(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7170661号
(P7170661)

(45)発行日　令和4年11月14日(2022.11.14)

(24)登録日　令和4年11月4日(2022.11.4)

(51)国際特許分類

Ｈ０４Ｌ　45/24　(2022.01)		Ｈ０４Ｌ	45/24
Ｈ０４Ｌ　67/12　(2022.01)		Ｈ０４Ｌ	67/12

ＦＩ

請求項の数　17　（全240頁）

(21)出願番号　特願2019-555116(P2019-555116)
(86)(22)出願日　平成30年4月2日(2018.4.2)
(65)公表番号　特表2020-516198(P2020-516198A)
(43)公表日　令和2年5月28日(2020.5.28)
(86)国際出願番号　PCT/US2018/025695
(87)国際公開番号　WO2018/187212
(87)国際公開日　平成30年10月11日(2018.10.11)
審査請求日　令和3年3月23日(2021.3.23)
(31)優先権主張番号　62/480,696
(32)優先日　平成29年4月3日(2017.4.3)
(33)優先権主張国・地域又は機関
米国(US)
早期審査対象出願

(73)特許権者　519358737
リスタット リミテッド
ベリーズ国ベルモパン・マウンテンビュー ブールバード・ガーデン シティ プラザ・スイート ５
(74)代理人　110001379
特許業務法人 大島特許事務所
(72)発明者　ウィリアムズ、リチャード・ケイ
アメリカ合衆国カリフォルニア州９５０１４・クパチーノ・ノリッジ アベニュー １０２９２
(72)発明者　ベルズン、イヴゲン
ウクライナ国キエフ・２０ビー・ステパナ バンデリー アベニュー
(72)発明者　ホルブ、オレクサンドル

最終頁に続く

(54)【発明の名称】　ハイパーセキュアラストマイル通信の方法及び装置

(57)【特許請求の範囲】

【請求項１】

クライアントデバイスからクラウドにデータパケットを送信する方法であって、

前記データパケットは通信に含まれ、

前記クラウドは複数のメディアノード及び複数のゲートウェイノードで構成されており、

当該方法は、

前記クライアントデバイスが、シグナリングサーバにコール要求を送信するステップであって、前記コール要求がコール先に関する連絡先情報を含む、該ステップと、

前記シグナリングサーバが、前記コール先と通信するための経路を決定するステップであって、前記経路が、第１のゲートウェイノードを含む第１の経路、第２のゲートウェイノードを含む第２の経路を含み、前記第１のゲートウェイノード、前記第２のゲートウェイノード、及び他のメディアノードはいずれも、前記第１の経路または前記第２の経路の全体を示す情報を有していない、該ステップと、

前記シグナリングサーバが、コマンド及び制御パケットを、前記クライアントデバイス、前記第１のゲートウェイノード、及び前記第２のゲートウェイノードにそれぞれ送信するステップであって、前記コマンド及び制御パケットは、前記クライアントデバイス、前記第１のゲートウェイノード、及び前記第２のゲートウェイノードによって送信されるルーティング指示パケットを含む、該ステップと、

前記クライアントデバイスが、前記コマンド及び制御パケットに応答して、前記通信に含まれる第１のデータパケットを前記クライアントデバイスから前記第１のゲートウェイ

ノードに送信し、かつ前記通信に含まれる第２のデータパケットを前記クライアントデバイスから前記第２のゲートウェイノードに送信するステップと、を含むことを特徴とする方法。

【請求項２】

前記第１のデータパケットは、前記クライアントデバイスから前記第１のゲートウェイノードに第１の物理媒体を介して送信され、

前記第２のデータパケットは、前記クライアントデバイスから前記第２のゲートウェイノードに第２の物理媒体を介して送信されることを特徴とする請求項１に記載の方法。

【請求項３】

前記第１の物理媒体が携帯電話リンクを含み、

前記第２の物理媒体がＷｉＦＩ（登録商標）チャネルを含むことを特徴とする請求項２に記載の方法。

【請求項４】

前記第１のデータパケットに第１のＩＰソースアドレスを提供するステップと、

前記第２のデータパケットに第２のＩＰソースアドレスを提供するステップとをさらに含むことを含む請求項２に記載の方法。

【請求項５】

前記第１のデータパケットに第１のＩＰソースアドレスを提供するステップと、

前記第２のデータパケットに第２のＩＰソースアドレスを提供するステップとをさらに含むことを含む請求項１に記載の方法。

【請求項６】

前記シグナリングサーバが、前記コマンド及び制御パケットを前記クライアントデバイス、前記第１のゲートウェイノード、及び前記第２のゲートウェイノードにそれぞれ送信する前に、前記シグナリングサーバは、前記コール先に関する前記連絡先情報を用いてネームサーバにコンタクトすることを特徴とする請求項１に記載の方法。

【請求項７】

前記コール先に関する前記連絡先情報は、前記コール先の機密ＩＤを含み、

前記ネームサーバは、前記機密ＩＤを前記コール先のＳＤＮＰアドレスに変換し、

前記シグナリングサーバは、前記クライアントデバイスから前記コール先に通信するための前記経路の決定時に、前記コール先の前記ＳＤＮＰアドレスを使用することを特徴とする請求項６に記載の方法。

【請求項８】

前記コール先に関する前記連絡先情報は、前記コール先の電話番号を含み、

前記ネームサーバは、前記電話番号を前記コール先の位置に最も近いゲートウェイノードのアドレスに変換し、

前記シグナリングサーバは、前記クライアントデバイスから前記コール先に通信するための前記経路の決定時に、前記コール先の位置に最も近いゲートウェイノードのアドレスを使用することを特徴とする請求項６に記載の方法。

【請求項９】

前記クライアントデバイスが前記クラウドにアクセスするたびに、前記ネームサーバに情報を渡すことを特徴とする請求項６に記載の方法。

【請求項１０】

前記シグナリングサーバが前記クライアントデバイスに送信する前記コマンド及び制御パケットは、前記第１のデータパケットを前記第１のゲートウェイノードに送信することを指示する第１のルーティング指示と、前記第２のデータパケットを前記第２のゲートウェイノードに送信することを指示する第２のルーティング指示とを含むことを特徴とする請求項１に記載の方法。

【請求項１１】

前記第１のゲートウェイノード及び前記第２のゲートウェイノードの各々は、前記クライアントデバイスと通信するための第１のアドレスと、前記クラウド内で通信するための

第２のアドレスとを有することを特徴とする請求項１０に記載の方法。
【請求項１２】
前記クライアントデバイスは、前記第１のデータパケット及び前記第２のデータパケットを前記第１のゲートウェイノード及び前記第２のゲートウェイノードにルータを介してそれぞれ送信し、
当該方法は、
前記第１のデータパケットに第１のＭＡＣソースアドレスを提供するステップと、
前記第２のデータパケットに第２のＭＡＣソースアドレスを提供するステップと、をさらに含むことを特徴とする請求項５に記載の方法。
【請求項１３】
複数のシグナリングサーバを提供するステップをさらに含み、
前記シグナリングサーバは、前記パケットを前記クライアントデバイスから前記コール先にルーティングするタスクを分割し、
前記複数のシグナリングサーバのいずれも、前記パケットの伝送ルートの全体を示す情報を有していないことを特徴とする請求項１に記載の方法。
【請求項１４】
前記第１のデータパケット及び前記第２のデータパケットに含まれる少なくとも１つのコンテンツを、隠蔽技術の組み合わせを用いて隠蔽するステップをさらに含み、
前記隠蔽技術は、暗号化、スクランブル化、ジャンクデータ挿入、分割及び／または混合を含み、かつ、所定のステートに基づいていることを特徴とする請求項１に記載の方法。
【請求項１５】
前記ステートは、時間、ノード番号、ネットワーク識別子、またはＧＰＳ位置を含むことを特徴とする請求項１４に記載の方法。
【請求項１６】
前記第１の物理媒体は、第１のキャリア周波数を使用して変調される携帯電話リンクを含み、
前記第２の物理媒体は、第２のキャリア周波数を使用して変調される携帯電話リンクを含むことを特徴とする請求項２に記載の方法。
【請求項１７】
前記第１の物理媒体は、第１のキャリア周波数を使用して変調されるＷｉＦｉ（登録商標）チャネルを含み、
前記第２の物理媒体は、第２のキャリア周波数を使用して変調されるＷｉＦｉ（登録商標）チャネルを含むことを特徴とする請求項２に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願への相互参照）
本出願は、２０１７年４月３日に提出された米国仮出願６２／４８０，６９６の優先権を主張し、２０１５年１月２６日に提出された米国仮出願第６２／１０７，６５０号の優先権を主張するものとして２０１５年７月２０日に提出された「セキュア動的通信ネットワーク及びプロトコル」という名称の米国出願第１４／８０３，８６９号の一部継続出願である。前述の各適用は、その全体が参照により本明細書に組み込まれている。
【０００２】
（技術分野）
本発明は、デバイス及びゲートウェイとネットワークまたはクラウドの間のハイパーセキュア「ラストマイル」通信を容易化する方法及び装置に関するものである。
【背景技術】
【０００３】
通信の手段を改善することにより、人類の初期の始まりから文明は進歩してきた。徒歩で、または馬に乗って移動する宅配便や配達員の使用から、電車、トラック、及び飛行機

による郵便配達を経て、電信、電話、無線、テレビ、コンピュータ、携帯電話、そしてインターネット、電子メール、及びワールド・ワイド・ウェブ（WWW）の出現に至り、より最近では、ソーシャルメディア、ボイスオーバーインターネット、マシン・ツー・マシン（Ｍ２Ｍ）接続、ＩｏＴ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｔｈｉｎｇ）、及びＩｏＥ（Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｅｖｅｒｙｔｈｉｎｇ）を通して、通信は常に当代の最新技術の活用において先駆けとなっている。それぞれの新しい時代の電気通信技術が採用されるとともに、接続される人々の数、及びそれらの人々の間で情報が運ばれる速度も増加している。

【０００４】

この傾向の影響は、歴史上のいかなるときと比較しても、人類がより接続されており、通信技術によって、私的、個人的、家族的、及び財政的情報が、接続することを意図された対象にのみ、安全かつ確実に配信されることを、人々が信頼、及び依存しているということである。知識、及び情報は数百万人の人々に数秒で配信されるようになり、友人や家族は、ボタンを押すだけで地球の反対側の人と連絡を取ることができる。「世界は非常に狭い場所になっている」と、しばしば言われている。

【０００５】

このような進歩は誰にとっても非常に有益であるが、我々が技術に対し重度に依存していることの皺寄せも存在する。例えば、地震、または荒天のときに通信システムが実行に失敗した場合、たとえ一時的であっても、「接続されていない」ことによって人々は混乱、またはパニックに陥りさえする。通信システム、またはメディアのサービス品質（ＱｏＳ）は、通信ネットワークの性能の重要な測定値である。人々の心の平和、金融資産、アイデンティティ、及びまさにその人生さえも、信頼でき、かつ安全な通信に依存している。

【０００６】

通信ネットワークのもう１つの検討ポイントは、プライバシー、安全性、及びセキュリティを、使用するクライアントに保証する能力である。通信技術が進化するにつれて、悪戯を起こし、システムを混乱させ、金銭を盗み、偶発的または悪意を持って他者に害を及ぼすことを意図する犯罪者及び「ハッカー」の知識も高度化している。クレジットカード詐欺、パスワード盗難、なりすまし、及び秘密情報、私的写真、ファイル、電子メール、テキストメッセージ、私的つぶやき（困らせるために盗まれたもの、または恐喝の犠牲）の無断公表は、現代のサイバー犯罪のいくつかの例にすぎない。

【０００７】

この特許出願時の、プライバシー侵害及びサイバー犯罪の注目すべき例を以下に列挙し、現代のオープン通信ネットワークにおけるセキュリティ問題の大流行を時系列に並べて示す。

・「ターゲット：少なくとも７千万人が巻き込まれた盗難情報」、ＣＮＢＣ、２０１４年１月１０日

・「ハッカーが高性能の冷蔵庫とテレビで悪意のある電子メールを送信」、ＢＧＲ、２０１４年1月２０日

・「サーモスタットがハッキングされ、Ｎｅｓｔ社とＧｏｏｇｌｅ社の秘密の論争が再開」、Ｓｌａｓｈ　Ｇｅａｒ、２０１４年6月２４日

・「アカウントのハイジャックはＬＩＮＥのデータセキュリティを疑問視する。無料の通話及びメッセージアプリケーションであるＬＩＮＥは、最近多発するデータセキュリティ侵害によって揺らいでいる。このアプリケーションでは、数百のユーザカウントがアカウントのユーザ以外の人間によって不正にアクセスされたことがわかった。」、日経アジアレビュー、２０１４年7月２日

・「ＮＳＡのデータスイープに一般のアメリカ人が巻き込まれる、報告クレーム」ＡＰ、２０１４年7月6日

・「スマートＬＥＤ電球がＷｉＦｉパスワードを流出させる」、ＢＢＣ　Ｎｅｗｓ、２０１４年7月8日

・「６人がＳｔｕｂＨｕｂ上でプライムチケット購入の詐欺にあった。ＳｔｕｂＨｕｂは、盗まれたパスワード及びクレジットカードの番号を使用して、ポップミュージックコン

サート及びヤンキースの試合の何千ものチケットを売買するハッカーのターゲットになった、とニューヨーク州当局は語った。」、Ｂｌｏｏｍｂｅｒｇ、２０１４年7月２４日
・「ＩｏＴは非常にハッキングを受けやすい、と研究が示す」、Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｂｕｓｉｎｅｓｓ Ｔｉｍｅｓ（www．ｉｂｔｉｍｅｓ．ｃｏｍ）
・「ロシアのハッカーが１０億以上のインターネットパスワードを収集する」、Ｎｅｗ Ｙｏｒｋ Ｔｉｍｅｓ、２０１４年8月5日
・「アメリカの秘密を暴露する新しい情報漏洩者、政府の結論」、ＣＮＮ、２０１４年8月6日
・「Ｇｏｏｇｌｅ社に買収されたＮｅｓｔ社のサーモスタットを、ハッカーは１５秒でルート化する」、Ｔｈｅ Ｅｎｑｕｉｒｅｒ（ｗｗｗ．ｔｈｅｉｎｑｕｉｒｅｒ．ｎｅｔ）、２０１４年8月１１日
・「標的を狙う同じマルウェアによってハッキングされたＤａｉｒｙ Ｑｕｅｅｎ社」、Ｃｈｒｉｓｔｉａｎ Ｓｃｉｅｎｃｅ Ｍｏｎｉｔｏｒ、２０１４年8月２９日
・「ヌード写真漏洩の被害者となった有名人―ｉＣｌｏｕｄアカウントのセキュリティ脆弱性」、ＣＢＳ Ｎｅｗｓ、２０１４年9月1日
「Ｈｏｍｅ Ｄｅｐｏｔ社は、クレジットカード侵害の最新のターゲットになり得る。Ｈｏｍｅ Ｄｅｐｏｔ社の侵害は、ターゲットよりはるかに大規模である可能性がある（４，０００万枚のカードが３週間にわたって盗まれていた）。」、Ｆｏｒｔｕｎｅ、２０１４年9月2日
・「ミステリアスな模造携帯電話のタワーが全米でコールを傍受している」、Ｂｕｓｉｎｅｓｓ Ｉｎｓｉｄｅｒ、２０１４年9月3日
・「ハッキング攻撃：銀行から小売へ、サイバー戦争の兆候は？」、Ｙａｈｏｏ Ｆｉｎａｎｃｅ、２０１４年9月3日
・「Ｈｏｍｅ Ｄｅｐｏｔ社が、アメリカとカナダの店舗で支払いシステムがハッキングされたことを認める」、Ｆｏｘ Ｎｅｗｓ、２０１４年9月9日
・「Ｙａｈｏｏは、監視に関してアメリカ政府と法廷闘争を行った」、ＣＢＳ／ＡＰ、２０１４年9月１１日
・「ハッカーにとって、あなたの医療記録はクレジットカードより価値が高い」、Ｒｅｕｔｅｒｓ、２０１４年9月２４日
・「赤警報：ＨＴＴＰがハッキングされた。何億もの人々が毎日依存するブラウザ接続を含むため、ＳＳＬ／ＴＬＳ（ＢＥＡＳＴ）攻撃に対するブラウザクラッシャは、最悪のハッキングにランク付けされる。」、ＩｎｆｏＷｏｒｌｄ、２０１４年9月２６日
・「Ｓｏｎｙ社のサイバー攻撃、最初の妨害行為は速やかに炎上した」、Ｎｅｗ Ｙｏｒｋ Ｔｉｍｅｓ、２０１４年１２月３０日

【０００８】

サイバー犯罪、セキュリティ違反、なりすまし、及びプライバシー侵害のペースが次第に上がっているように思われる中で、「これら全てのサイバー攻撃はどのようにして可能であり、サイバー攻撃を止めるためには何ができるのか」という疑問を投げかける。社会がより多くのプライバシー及びセキュリティを求めると同時に、消費者は、より高い接続性、より安価で高品質な通信、及び金融取引行為における更なる利便性も求めている。

【０００９】

最新の通信ネットワーク、データストレージ、及び、接続されたデバイスの性能及び脆弱性を理解するためには、現代の電子通信、無線通信、及び光通信が、ファイル、電子メール、テキスト、オーディオ、及びビデオ画像を含むデータをどのように操作、転送、及び記憶しているか理解することが、まず重要である。

【００１０】

回線交換電話ネットワーク操作

【００１１】

電子通信は、ワイヤ、無線、マイクロ波、または光ファイバ回線のネットワークに接続された様々なハードウェア構成要素、またはデバイスを含む。データストリームに情報の

「コンテンツ」を埋め込むため、またはエンコードするための様々な方法を使用し、このネットワークを通じて電気エネルギー、または電磁気エネルギーを送信することによって、情報は、あるデバイスから他のデバイスに渡される。理論的には、これらのネットワークの最大データレートは、物理法則によって光速で設定されるが、ほとんどの場合、データエンコーディング、ルーティング及びトラヒックコントロール、シグナル対雑音品質、及び、電気ノイズ、電磁的ノイズ、光学ノイズ、及び望ましくない電子寄生を克服する際の実用上の制限が、情報の流れを乱し、または妨げて、通信ネットワークの能力を理想的な性能のわずかな一部に制限する。

【００１２】

歴史的に、電子データ通信は、２つ以上の電気的に接続されたデバイスの間に通信の「回路」を形成する、専用の「配線による」電気的接続を使用し、最初に達成された。電信の場合、機械的なスイッチを使用して直流（ＤＣ）電気回路を手作業で作製し、電流を断ち、金属製のレバーを回転させ動かしたソレノイドを磁化し、送信者が押したスイッチのパターンと同様のパターンで、リスニングデバイス、または「中継機」をクリックする。送信者は、次に、制定された言語、すなわちモールスシグナルを使用して情報をパルス列にエンコードする。受信者は同様に、メッセージを理解するため、ドット、及びダッシュと呼ばれる一連の長短パルスであるモールスシグナルを理解する必要がある。

【００１３】

その後、アレクサンダー・グラハム・ベルは、電気的接続を介して音を伝えるために、現在は交流（ＡＣ）と呼ばれる「波動電流」の概念を用いて最初の電話を開発した。電話ネットワークは、電気回路によって接続された２つの電磁トランスデューサを含み、各電磁トランスデューサは、固定された永久磁石エンクロージャによって囲まれた可動振動版、及びコイル、すなわち「ボイスコイル」を含んでいた。トランスデューサに向かって話すと、音からの空気圧の変化により、ボイスコイルは、コイル内のＡＣ電流を誘導する周囲の磁界内で前後に移動する。聴取者側では、ボイスコイル内で流れる、経時変化する電流は、周囲の磁界に対面する同一の波形、及び経時変化する磁界を誘導し、音を捉えるトランスデューサと同じ方法で、ボイスコイルを前後に動かす。結果として生じる動きは、音を捉えるデバイスと同じ方法で音を再生する。現代の言葉では、トランスデューサが音を電流に変換するとき、マイクロホンとして操作し、トランスデューサが電流を音に変換するとき、スピーカーとして操作する。また、伝道された電気シグナルは、空気中の自然気圧波、すなわち音として運ばれるオーディオ波形に類似しているため、現代では、このような電気シグナルは、アナログシグナル、またはアナログ波形と呼ばれる。

【００１４】

説明したように、トランスデューサは話すこと、及び聞くことの両方に使われるため、会話では両者が話すときと聞くときとを知る必要がある。このようなシステムでは、糸で接続された２つの空き缶、すなわち糸電話と同様に、発信者は話すこと、及び聞くことを同時にはできない。「半二重」方式と呼ばれるこのような一方向動作は古典的であるように聞こえ得るが、トランシーバでの現代の無線通信において、及び「プッシュツートーク」すなわちＰＴＴと名付けられた現代の電話法において、実際に今でも一般に使われている。

【００１５】

のちの全二重（すなわち、双方向または送受信）電話は、別個のマイクロホンとスピーカーとを備えており、話すこと、及び聞くことを同時にできることが当たり前になった。しかし、現代でさえ、全二重電話通信を操作する場合には、フィートバック、つまり受信者の音声がマイクロホンによって拾い上げられ、発信者にフィードバックされ、紛らわしいエコー、ときには耳障りな異音が生じることになるという、長距離電話通信を特に悩ませる問題を防ぐために注意が必要である。

【００１６】

初期の電信システム、及び電話システムは、別の問題であるプライバシー問題に悩まされていた。これらの初期の通信ネットワークでは、ネットワークに接続される全ての人が

、望んでいないとしても、回路上で通信される全ての情報を耳にする。非都市部の電話ネットワークでは、これらの共有回路は「共同回線（ｐａｒｔｙ　ｌｉｎｅｓ）」として知られていた。その後、電話システムは急速にマルチ回線ネットワークに発展し、専用回線によって、電話局の支店個々の顧客の電話に直接接続された。支社の交換局内では、システムオペレータは、ジャンパケーブルを使用した交換機を介して発信者を相互に手動で接続し、また、ある支店を別の支店へ接続して最初の「長距離」電話サービスを形成する機能を有していた。電話「スイッチ」ネットワークを形成する大きな中継機の列は、次第に人間のオペレータに取って代わり、続いて真空管を含む電子スイッチに置き換えられた。

【００１７】

ベル研究所が１９５０年代後半にトランジスタを開発した後、電話と支店の交換機においては、壊れやすく高温の真空管は、トランジスタと最終的に集積回路とを含む低温稼動ソリッドステートデバイスに置き換えられた。ネットワークが成長するにつれて、電話番号は７桁のプレフィックス番号及びプライベート番号から桁を増やして拡大され、市外局番及び最終的には国際電話を扱うための国コードが含まれていた。音声通話を伝える銅ケーブルは、すぐに世界を覆い、海を渡った。ネットワークの規模に関わらず、操作の原理は一定であり、コールは、アナログシグナルによって伝えられる音声を伴う発信者と、電話スイッチによって決定されるコールの経路指定との間の直接的かつ電気的な接続、すなわち「回路」を表した。このような電話システムは、最終的には「回路交換電話ネットワーク」として知られることになったか、または基本電話システム、すなわちＰＯＴＳとして知られることになった。回線交換電話の採用は、１９８０年代にピークに達し、以後、次のセクションで説明する「パケット交換電話」に置き換えられた。

【００１８】

電話ネットワークとほぼ並行して進化し、１９２０年代には無線放送での定期的な無線通信が開始された。放送は一方向性であり、特定の政府認可周波数で無線放送局から発せられ、その特定の放送周波数、または無線局に同調した任意の数の無線受信機によって受信された。放送されたシグナルは、認可された無線スペクトルの専用部分に、それぞれ振幅変調（ＡＭ）方式、または、より後の周波数変調（ＦＭ）方式のいずれかを使用してアナログシグナルを搬送した。米国では、連邦通信委員会、すなわちＦＣＣが、このような認可された帯域の割り当て、及び規制の管理のために発展した。放送の概念は、無線伝送を使用したテレビ番組の放映へ拡大された。テレビ番組は、最初は白黒のコンテンツを含んでいたが、その後はカラーで放映された。その後、テレビシグナルも、マイクロ波衛星テレビ受信用アンテナによって、または同軸ケーブルを介してのどちらかで、人々の家に搬送されることができた。特定の放送周波数に同調した任意の視聴者が放送を受信することができるため、「マルチキャスト」という用語が、現在ではこのような一方向性のマルチリスナ通信のために使用されている。

【００１９】

無線放送の出現と同時に、最初の双方向通信が商用、及び軍用の海上船で始まった。第２次世界大戦の時代までには、無線は、送信機及び受信機を単一のユニットに結合させた携帯用無線トランシーバへ発展した。電話と同様に、初期の双方向無線送信は、「単信」方式で操作され、１つの無線チャンネルでは１つの無線のみ放送することができ、その間他の無線チャンネルは放送できなかった。異なる周波数の送信機及び受信機を結合させることによって、無線回線の両端で同時に送受信することが可能になり、２者間で全二重方式の通信が可能になった。

【００２０】

しかし、複数の相手からの重複送信を防ぐために、半二重、すなわちプッシュツートークと呼ばれるプロトコルがチャネル管理のために一般的に使用されており、先着順に特定のチャネルで、任意の者が独占的に送信することができる。アナログ変調を使用する業界標準の無線タイプには、アマチュア（ハム、またはＣＢ）無線、マリンＶＨＦ無線、航空交通管制用のＵＮＩＣＯＭ、及び個人トランシーバ通信用のＦＲＳが含まれる。これらの双方向無線ネットワークでは、無線機は特定の周波数の「チャンネル」を介してデータを

中央無線タワーへ送信し、タワーはそのシグナルを増幅して反復し、無線ネットワーク全体に送信する。放送地域に情報を伝える利用可能な周波数の数により、システムの総帯域幅、及び一度に無線ネットワーク上で独立して通信することができるユーザの数が設定される。

【００２１】

無線ネットワークの総容量を拡大して、より多くの発信者を処理するように、大きな領域をより小さな部分、すなわち無線「セル」に分割したセルラーネットワークの概念が１９７０年代に論証され、その後１０年以内に普及した。セルラーの概念は、無線タワーの放送圏をより狭い範囲、すなわちより短い距離に制限することであり、したがって、同じ周波数帯域を再利用して、異なるセルに存在する異なる発信者を同時に処理することができる。そのために、通信を「遮断する」、及び突然切断することなく、あるセルから隣接するセルに発信する人のハンドオフを管理するソフトウェアが作成された。ＰＯＴＳ、双方向性無線、無線及びテレビ放送のように、最初のセルラーネットワークは本質的にアナログであった。コールルーティングを制御するために、電話番号システムが採用され、適切な無線電気接続が決定された。この選択には、新しい無線セルラーネットワークを「有線の」従来型の電話システムに継ぎ目なく接続し、２つのシステム間の相互接続、及び相互運用性を提供するという利点も存在した。

【００２２】

１９８０年代には、無線放送及びテレビ放送に加えて、電話通信及び無線通信が、消費電力の削減及びバッテリ寿命の向上のため、シグナル対雑音品質の改善のため、データ及び音声付きのテキストを伝える必要性の問題に取り組み始めるために、アナログからデジタルへの通信方法及び通信フォーマットの避け難い移行を始めた。ＥＤＡＣＳ及びＴＥＴＲＡなどの無線フォーマットの出現と同時に、１対１、１対多、及び多対多の通信方式が可能になった。セルラー通信は、テレビ放送と同様に、ＧＰＲＳなどのデジタルフォーマットへも急速に移行した。

【００２３】

２０１０年までには、ほとんどの国が全てのアナログテレビ放送を中止したか、または中止の手続き中になった。放送テレビとは異なり、ケーブルテレビ事業者は、デジタルフォーマットに切り替える必要はなく、２０１３年まではアナログ及びデジタルシグナルのハイブリッド複合体を維持していた。ケーブルテレビのデジタルへの最終的な移行は、政府の基準ではなく商用の理由からであり、ネットワークの利用可能なチャンネルの数を拡大し、ＨＤ及びＵＨＤコンテンツを配信できるようにし、より多くのペイパービュー（ＰＰＶ、（「ユニキャスト」としても知られている））プログラミングを可能にし、高速デジタル接続サービスを顧客に提供するためであった。

【００２４】

アナログフォーマットからデジタルフォーマットへのグローバル通信ネットワークの移行を、インターネットの出現、より具体的にはインターネットプロトコル（ＩＰ）の普及と同一視することは一般的であるが、推進されていなければ、デジタルフォーマットへの転換は電話でのＩＰの商用的受諾に先行し、ＩＰ及び「パケット交換ネットワーク」（次のセクションで説明される）への通信の全世界的な移行を可能にする。

【００２５】

その結果生じる回線交換電話の進化は、各々が異なる技術を含む無線、セルラー、ＰＢＸ、及びＰＯＴＳ接続の融合とサブネットワークを含む「公衆交換電話ネットワーク」、すなわちＰＳＴＮである。例えば、ネットワークは、高帯域幅の幹線によって接続されて、ＰＯＴＳゲートウェイ、回線交換セルラーネットワーク、ＰＢＸ、及び双方向無線ネットワークへの有線接続を介して接続されるＰＳＴＮゲートウェイを含む。各サブネットワークは独立して操作でき、同様のデバイスを駆動する。

【００２６】

ＰＳＴＮはまた、ＡＭＰＳ、ＣＤＭＡ、及びＧＳＭ（登録商標）のアナログ及びデジタルプロトコルを実行する回線交換セルラーネットワーク１７に接続する。セルラー無線タ

ワーを介し、回線交換セルラーネットワークは、標準化されたセルラー無線を使用して、携帯電話などのモバイルデバイスに接続する。ＧＳＭ（登録商標）の拡張であるＧＰＲＳネットワークの場合には、回線交換セルラーネットワークは、タブレットにも接続することができ、同時に低速のデータ及び音声を伝える。ＴＥＴＲＡ及びＥＤＡＣＳなどの双方向無線ネットワークは、高出力の無線タワー及びＲＦ接続を介し、ＰＳＴＮをハンドヘルドの無線、及び、より大きいダッシュボード内のデスクトップの無線に接続する。警察官、救急車、救急救命士、消防署、さらには湾岸当局でも一般的に使用されているこのような双方向無線ネットワークは、プロフェッショナル通信ネットワーク及びサービスとも呼ばれており、消費者よりもむしろ、政府、地方自治体、及び緊急対応者を対象としている（注：本明細書で使用されるように、「デスクトップ」、「タブレット」及び「ノートブック」という用語は、それらの名前を有するコンピュータの略語として使用される。）。

【００２７】

コールルーティングを完了するために従来の電話番号を使用するＰＯＴＳゲートウェイ、回線交換セルラーネットワーク、及びＰＢＸとは異なり、双方向無線ネットワークは、専用ＲＦ無線チャンネル（電話番号ではなく）を使用して、無線タワー及び都合のよいモバイルデバイスの間の無線接続を築く。このように、プロフェッショナル無線通信サービスは、消費者の携帯電話ネットワークとは性質が異なり、独特のものである。

【００２８】

つまり、ＰＳＴＮネットワークは、柔軟に多様な技術のサブネットワークを相互接続する。まさにこの多様性によって、現在の回路交換ネットワークの本質的な弱点、つまりサブネットワーク間の相互運用性が定義される。様々なサブネットワークが任意の共通制御プロトコル及び言語と通信しないため、また各技術がデータ及び音声の伝達を異なる方法で処理するため、様々なシステムは、ＰＳＴＮのバックボーンまたは幹線を通じて電話をかける能力が限られていることを除いて、本質的に互換性がない。例えば、ニューヨーク市の世界貿易センターへの９月１１日のテロ攻撃の間、アメリカ全土から多くの緊急対応者がマンハッタンに集まって大惨事との戦いを支援しようと試みたが、無線通信システム及びトランシーバは他の州、及び都市からのボランティアとは互換性がないことを学んだだけであり、救援への努力を、集中化させて命令及び統制するよう管理することは不可能であった。無線の通信プロトコルで標準化が行われていないため、無線は相互に接続することが単純にできなかった。

【００２９】

さらに、回路交換電話ネットワークの直接的かつ電気的接続及びＲＦ接続、特にアナログまたは安全でないデジタルプロトコルを使用する場合、ＲＦスキャナを有するハッカーが、アクティブな通信チャンネルを見つけて、そのとき発生している会話に気付き、サンプリングし、聴き、傍受することは簡単である。ＰＳＴＮは、通信している当事者間の「継続的な」繋がり、すなわち回線を形成するため、ハッカーが接続を見極めて「盗聴」する時間は十分存在し、連邦裁判所の下で機能している政府によって合法的に盗聴を命じられるか、または非合法的な、禁じられた、または不認可の監視を実行するサイバー犯罪者または政府によって法律に反して盗聴される。合法的な、及び違法なスパイ及び監視の定義と、ネットワークオペレータによる協力遵守の義務とは、国によって大きく異なり、多数の国境を越えて経営しているＧｏｏｇｌｅ、Ｙａｈｏｏ、Ａｐｐｌｅなどのグローバル企業の間で激しい争点となっている。通信ネットワーク及びインターネットはグローバルであり、国境または境界は認識しないが、電子情報などを管理する法律はその土地特有であり、その時の国内及び国際的な通信、及び商業を管理する政府の監督官庁の対象である。

【００３０】

その合法性や倫理に関わらず、現在の電子スヌーピング及び監視は一般的であり、全ての道路や地下鉄の全ての道路の曲がり角、及び頭上に設置されたユビキタスセキュリティカメラの監視から、様々な国の国家安全保障課及び組織によって行われる巧みなハッキング及びコードクラッキングにまで及んでいる。全てのネットワークは脆弱であるが、ＰＳＴＮの古さ、及び不十分なセキュリティ対策のために、ハッキングすることが特に容易で

ある。このように、安全な最新ネットワークに接続されたＰＳＴＮでも、システム全体の弱点になり、セキュリティ違反及びサイバー犯罪に対する脆弱性を生み出す。それにもかかわらず、グローバルなＰＳＴＮネットワークを廃止し、ＩＰベースのパケット交換通信に完全に置き換えるには、数十年ではないにしても、やはり数年がかかる。パケットベースのネットワーク（以下に説明する）は、ＰＳＴＮネットワークより近代的であるが、それでも安全でなく、セキュリティ破壊、ハッキング、サービス拒否攻撃、及びプライバシー侵害の対象となる。

【００３１】

パケット交換通信ネットワーク操作

【００３２】

糸で接続された２つの空き缶、つまり糸電話が現代の回線交換電話の操作のメタファを象徴する場合、郵便局は、パケット交換通信ネットワークの同様なメタファを象徴する。テキスト、データ、音声、及びビデオは、ファイル及びデジタルデータのストリームに変換され、その後、ネットワークを介して配信されるデータの量子化された「パケット」に解析される。配信メカニズムは、データパケットの宛先及び送信元を一意に識別する電子アドレスに基づいている。フォーマット、及び通信プロトコルはまた、パケットに含まれるデータの性質に関する情報を含むよう設計され、パケットは、それが使用されるプログラムまたはアプリケーションに固有のコンテンツと、パケットを伝える物理的連結、及び電気的接続または無線接続を容易にするハードウェアとを含む。

【００３３】

１９６０年代に誕生したパケット交換ネットワークの概念は、ポスト・スプートニクの冷戦後のパラノイア時代に作られた。当時、米国国防総省（ＤｏＤ）は、間隔を置いた核ミサイル攻撃により米国の通信基盤全体が壊滅し、ソビエト連邦の先制攻撃に対応する能力が無効化される可能性があるという懸念、及び、攻撃などに対する脆弱性が実際に攻撃を引き起こす可能性があるという懸念を表明した。そのため、国防総省は、軍事施設間で情報を配信するネットワークの能力が、特定のデータリンク及びネットワーク内の多数のリンクの破壊によって妨げられない過剰な通信システム、すなわち格子状の「ネットワーク」の創設を支援した。アーパネット（ＡＲＰＡＮＥＴ）として知られるそのシステムは、インターネットの親、及び近代的なデジタル通信のイヴとなった。

【００３４】

パケット交換ネットワークの創設にも関わらず、最初の利用し易いウェブブラウザであるＭｏｓａｉｃ、ハイパーテキストによって定義されたウェブページの出現、ＷＷＷの急速な普及、及び電子メールの普及により、インターネットプラットフォームに世界的な支持が集まった１９９０年代になるまで、インターネットの爆発的な成長は発生しなかった。その基本的な考え方の１つである中央制御の欠如、すなわち中央メインフレームの必要性は、インターネットをある程度普遍的に推進したが、これは国や政府に止めることができなかった（または、グローバルな影響を十分に理解してさえいなかった）ため、また、ユーザベースが、新たに購入したパーソナルコンピュータを使用して消費者を含有したためである。

【００３５】

インターネットの成長によるもう１つの大きな影響は、ネットワークを介してデータパケットをルーティングするために使用されるインターネットプロトコル（ＩＰ）の標準化であった。１９９０年代半ばまでに、インターネットユーザは、データを伝達する同じパケット交換ネットワークが、音声を運ぶためにも使用され得ることを理解し、その後間もなく「ボイスオーバーインターネットプロトコル」、すなわちＶｏＩＰが誕生した。この概念は、インターネットにアクセスする任意の者がＶｏＩＰによって無料で通信することを理論的には可能にしたが、ネットワーク全体にわたって伝播に手間がかかる。すなわち待ち時間が生じ、音声品質が低下し、度々わかりにくくなる。「ラストマイル」での接続品質を改善するための、高速イーサネット（登録商標）リンク、高速ＷｉＦｉ接続、及び４Ｇデータの採用により遅延時間は改善されたが、インターネット自体は、データパケッ

トの正確な配信を確実にするために創設されたものであり、パケットを配信するために必要な時間を保証するものではなく、すなわちリアルタイムネットワークとして操作されるべく作成されていない。

【００３６】

そのため、高価な長距離通信事業者、すなわち「電話会社」の代わりにインターネットを使用するという夢は、スカイプ、ライン、カカオトーク、バイバーなどの「期待された」（ＯＴＴ）プロバイダの可用性にも関わらず、ほとんど果たされなかった。ＯＴＴ電話は、無制御の待ち時間、劣悪な音質、発信の停止、エコー、残響、フィードバック、不安定な音、及びしばしば発信を開始することさえできないことに起因する劣悪なサービス品質（ＱｏＳ）に悩まされている。ＯＴＴ通信の劣悪なパフォーマンスは、本質的にはＶｏＩＰベースのプロトコルの欠点ではなく、データが通る経路、または通信が直面する遅延をＯＴＴキャリアが管理できないネットワーク自体の欠点である。本質的に、ＯＴＴ通信はインターネットヒッチハイカーとして機能するため、ＯＴＴキャリアは性能またはＱｏＳを保証することができない。現在のＶｏＩＰベースの通信を最大限に活用できる企業は、待ち時間の少ないハードウェアベースの専用ネットワークを有する長距離電話事業者であり、皮肉にも、そのような動機が最も少ないのが、まさにその電話会社である。

【００３７】

固有のネットワーク余剰は別として、パケット交換通信の最大の長所の１つは、データがインターネットプロトコルと一致したパケットで配置され、インターネットに接続及びリンクされた通信デバイスが提供される限り、任意の送信元から任意の宛先へ情報を伝達する能力である。インターネットプロトコルは、どの情報が伝達されているか、またはどのアプリケーションがその情報を使用するかに注意または関心を示すことなく、宛先へペイロードを配信するネットワークの能力を管理し、カスタマイズされたソフトウェアインターフェイス及び高価な専用ハードウェアの必要性を完全に回避する。多くの場合、アプリケーションに関連したペイロードでさえ、予め定義されたフォーマットを確立している。例えば、電子メールを読むため、ブラウザ上でウェブページを開くため、写真やビデオを見るため、フラッシュファイルを見るため、またはＰＤＦドキュメントを読むためなどである。

【００３８】

その汎用的なファイル形式は、専用または企業固有のソフトウェアに依存しないため、インターネットは「オープンソース」の通信プラットフォームと見なすことができ、コンピュータから携帯電話、車から家電製品まで、これまでに接続された最も幅広いデバイスと通信することが可能である。この普遍的な接続を説明する最新のフレーズは、「Ｉｎｔｅｒｎｅｔ　ｏｆ　Ｅｖｅｒｙｔｈｉｎｇ」、すなわちＩｏＥである。

【００３９】

高速クラウドのサーバ、クラウドデータストレージを含むコンピュータの大規模アレイは、インターネットのクラウドを形成する無数の他のサーバ（図示せず）の間の高帯域幅接続、一般的には光ファイバによって相互接続される。クラウドのメタファは、どのサーバがクラウドの一部と見なされ、どのサーバがそうでないかを明確に定義する境界がないため、適切である。毎日、及び分単位でさえ、サーバはオンラインになり、メンテナンスのためにオフラインになることはあるが、インターネットの機能または性能への影響は何もない。これは、正しく重複した分散システムのメリットである。つまり、単一の制御点は存在せず、したがって単一の障害点も存在しない。

【００４０】

クラウドは、様々な有線、ＷｉＦｉ、またはワイヤレスリンクを介してユーザまたはデバイスに接続され得る。ワイヤレスパケット交換が可能な電話通信は、４Ｇ／ＬＴＥと同様にＨＳＵＰＡ及びＨＳＤＰＡを含むセルラープロトコル３Ｇを含む。ＬＴＥ、すなわちロングタームエボリューションは、セルが異なるプロトコルで動作している場合でさえ、あるセルから別のセルへの通話を継ぎ目なく引き渡す機能を含む、様々なセルラープロトコルの相互運用性を保証するネットワーク規格を指す。（注：定義の問題として、本明細

書で使用される「ラストマイル」は、タブレット、デスクトップ、または携帯電話などの任意のタイプのクライアントデバイスとクラウドサーバとの間のリンクを指す。）方向性として、「ファーストマイル」という用語は、データ送信元のデバイスとクラウドサーバとの間のリンクを特定するために使用されることもある。そのような場合、「ラストマイル」リンクも「ファーストマイル」である。

【００４１】

より短距離の通信のために、ＷｉＦｉアクセスポイントは、スマートフォン、タブレット、ノートブック、デスクトップ、または家電製品に接続し、家庭、カフェ、レストラン、及びオフィス内のローカライズされたワイヤレスアプリケーションで使用され得る。ＷｉＦｉは、シングルキャリア周波数仕様８０２．１１ａ、８０２．１１ｂ、８０２．１１ｇ、８０２．１１ｎ、及び最近では二重周波数帯８０２．１１ａｃフォーマット用のＩＥＥＥ定義規格に従って動作する通信を含む。単純な静的ログインキーに基づくＷｉＦｉセキュリティは、接続の不正アクセスを防ぐために主に使用されるが、データを盗聴またはハッキングから無期限に守ることを意図したものではない。

【００４２】

ルータは、ファイバ、同軸ケーブル、またはイーサネット（登録商標）により、ノートブック、デスクトップ、電話機、テレビに接続されるか、ツイストペア銅線の電話線により、ホテル、工場、オフィス、サービスセンター、銀行、及び家庭を含む、動かない、すなわち固定された、有線接続の市場へサービスを提供する販売時点端末に接続される。ファイバまたはケーブルが利用できない遠隔地域では、デジタル加入者線（ＤＳＬ）接続は今でも使用されるが、データ速度及び接続信頼性は劇的に損なわれる。全体として、ワイヤレス、ＷｉＦｉ、及び有線接続を介したアクセスを集計すると、インターネットに接続されたオブジェクトの数は、２０２０年までに世界中で２００億に達すると予測されている。

【００４３】

デバイス間の直接接続を確立及び維持する回路交換ネットワークとは対照的に、パレット交換通信は、アドレスを使用して、インターネットを介してパケットを宛先に「ルーティング」する。このように、パケット交換通信ネットワークでは、通信デバイス間の接続を維持する単一の専用回路はなく、またインターネットを介して伝わるデータも単一の一貫した経路を伝わることはない。各パケットは、相互接続されたコンピュータの迷路を通って、宛先に到達しなければならない。

【００４４】

パケット交換ネットワーク通信を使用したノートブックからデスクトップへのＩＰパケットのルーティングをした場合、ワイヤレス接続を介してノートブックからＷｉＦｉルータに送信される第１データパケットは、ＤＮＳサーバのアレイに向けられる。ＤＮＳは、ドメインネームサーバ（Ｄｏｍａｉｎ　Ｎａｍｅ　Ｓｅｒｖｅｒ）の頭字語である。ＤＮＳサーバのアレイの目的は、宛先デバイス、この場合ではデスクトップ、のテキスト名または電話番号をＩＰアドレスに変換することである。変換されると、ＩＰアドレスは、ＤＮＳサーバのアレイからソースアドレス、すなわちノートブックに戻される。通信端末を明確に識別するこのアドレスは、ネットワークを介してデータパケットをルーティング為に用いられる。

【００４５】

その後、ノートブックは、ＩＰデータパケットを組み立て、組み立てたＩＰデータパケットを宛先に順次送信し始め、まずＷｉＦｉ無線のワイヤレス接続を介してローカルＷｉＦｉルータへ届き、その後、宛先への中間ルータとして機能するルータ及びサーバのネットワークを横断する。ルータ及びコンピュータサーバネットワークは、インターネット内のノードとして、またはポイント・オブ・プレゼンス（ＰＯＰ）として機能する。すなわちインターネットにアクセス可能な限られた接続性のゲートウェイとして機能するルータネットワークを共に形成する。ＰＯＰとして動作するいくつかのルータまたはサーバは、少数の隣接デバイスのみを介してインターネットに接続するが、サーバは多数のデバイス

に相互接続され、「スーパーＰＯＰ」と呼ばれることもある。明快にするため、ネットワーク用語でのＰＯＰという用語は、電子メールアプリケーションで使用されるアプリケーション名のＰＯＰ、または普通の古い郵便局と混同されないよう注意する必要がある。

【００４６】

各ルータ、またはルータとして機能するサーバは、アドレス指定可能なＩＰアドレスと、可能であれば、より上位のルータがアドレス指定可能なアドレスとを識別するルーティングテーブルをメモリファイル内に含む。これらのルーティングテーブルは、インターネットに最初に接続されたときに自動的にダウンロードされ、全てのルータにインストールされる。通常、ネットワーク経由でパケットをルーティングする際にはダウンロードされない。ＩＰパケットが、ルータ、ＰＯＰ、またはスーパーＰＯＰに入ると、ルータはＩＰアドレスを十分に読み取り、一般的にはアドレスの最上位桁の数字で、パケットを宛先に届けるために、次に向ける場所がわかる。例えば、ニューヨークから東京に向かうパケットは、まずシカゴを経由し、その後サンフランシスコ、ロサンゼルス、またはシアトルのサーバを経由して東京に到着することができる。ルータ間を通るデータパケットの数、又ルータ間のデータレートは、インフラ設備及びネットワークトラフィックと負荷によるので、どのルートを通れば一番速く良いかを事前に決める事は不可能である。

【００４７】

パケット交換データを用いて、クライアント間の直接接続を確立及び維持する回路交換電話通信とは異なり、インターネットを俯瞰する普遍的な情報は存在せず、どの経路がパケットをルーティングするために最良、最適、または最速の経路であるかを決定することはできず、また、２つの連続するパケットが同じ経路をとるという保証さえ存在しない。このように、パケットは、パケットが通過するルータ及びサーバを操作する企業の優先順位に基づき、インターネットを介して経路を「発見」する。本質的に、各ルータには、ネットワークの状態に基づいて優先経路を定義する特定のルーティングテーブル及びルーティングアルゴリズムが含まれている。例えば、ルータの選択は、同じ企業が所有する他のルータへパケットを送ること、隣接するルータへの接続間のトラヒックのバランスをとること、次のルータへの最短遅延を探すこと、取引を戦略的なビジネスパートナーに向けること、または可能な限り多くの中間ルータを飛び越えることでＶＩＰクライアント向けの高速経路を作成することを優先させてもよい。パケットがルータに入ると、特定のＰＯＰによって行われたルーティング選択が、送信者またはネットワークサーバオペレータの最善の利益のために行われたか否かを知る方法は存在しない。

【００４８】

そのため、ある意味では、パケットが辿る経路はタイミング及び運の問題である。前述のニューヨークから東京へのルーティングの例では、ルーティング、及び結果的に生じるＱｏＳは、経路における小さな摂動、すなわち、いわゆる「バタフライ効果」と言われる非線型方程式であっても、実質的に変化させることができる。カリフォルニアで一時的にトラヒック量が多いため、ニューヨークからのパケットがシカゴの「ルータＡ」を通過し、カリフォルニアではなくメキシコシティに転送される場合を考察されたい。メキシコシティのルータは、その後ＩＰパケットをシンガポールに転送し、最終的に東京に送信する。送信された正に次のパケットは、シカゴの「ルータＢ」を経由してルーティングされるが、これはその時点でのトラヒックが少ないため、パケットをサンフランシスコに送信し、その後２回の経由のみで東京に直接送信するためである。このような場合、２番目のパケットは、最初の経路がより長い迂回経路を経由する前に、東京に到着する可能性がある。この例では、ライブビデオストリーミング、またはＶｏＩＰなどのリアルタイム通信のためにインターネットを使用する際の問題点を強調している。すなわち、インターネットは、送信時間を保証する、またはネットワークの送信遅延を制御するようには設計されていない。パケットが２台のサーバのみを経由するのか、または１５台のサーバを経由するのかにより、待ち時間は５０ミリ秒から１秒以上まで変化し得る。

【００４９】

インターネットのルーティング制御が不十分であることは、リアルタイムアプリケーシ

ョンにとって問題であり、特にＯＴＴ通信事業者にとっては劣悪なＱｏＳの問題である。つまりＯＴＴ事業者は、インターネットのインフラストラクチャ上に便乗することで、インターネットベースの電話を提供しようと試みている。ＯＴＴ事業者はルーティングを制御しないため、遅延またはネットワークの待ち時間を制御することができない。パケット交換通信のもう１つの問題は、検出されることなくデータを乗っ取ることが容易である点である。略奪者がパケットを傍受し、その送信元または宛先のＩＰアドレスを特定した場合、間に存在するルータからデータを傍受するために様々な方法を使用し、自身の非合法ネットワークを介してトラヒックを傍受またはリダイレクトして会話を見張り、暗号化されたファイルを壊すことさえできる。

【００５０】

パケットのルーティングに使用される（及び、略奪者がパケットを乗っ取るためにも使用される）送信元のＩＰアドレスと宛先のＩＰアドレス、及び他の重要な情報は、ＩＰパケット、ＩＰデータグラム又はＴＣＰ／ＩＰパケットと呼ばれるデジタルデータとして特定される。ＩＰパケットは、デバイス間の物理的接続、デバイスを共に繋ぐためにデータが編成される方法、パケットのネットワークルーティング、有用なデータ（ペイロード）が正確に配信されたことを保証する手段、及びペイロードに含まれるデータの種類を定義するデジタル情報を含み、ペイロードデータそのものは様々なアプリケーションプログラムによって使用される。

【００５１】

ＩＰパケットは、一連のシリアルデジタルビットとして順序通り送受信され、インターネットエンジニアリングタスクフォース、すなわちＩＥＴＦなどを含む様々な標準委員会によって確立された、インターネットプロトコルと呼ばれる特定の方法で編成されている。この標準規格は、予め定められたプロトコルに従う任意のＩＰパケットが、同じＩＰ規格に準拠する任意の接続されたデバイスと通信し、理解されることを保証する。インターネットに接続されたデバイス及びアプリケーションの通信及び相互運用性を保証することは、インターネットの品質証明であり、オープンソースイニシアチブ、すなわちＯＳＩの指針を表し、任意の企業、政府、または個人がインターネットを制御することや、アクセシビリティまたはその機能性を制限することを防ぐ。

【００５２】

ＯＳＩモデルは、７つの機能レイヤを含む抽象概念であり、ＩＰパケットのフォーマット、及びパケットの各セグメントがどのような用途に使用されているかを正確に規定している。ＩＰパケットの各部分、すなわち「セグメント」は、特定のＯＳＩレイヤの機能に適用されるデータに対応する。７つのＯＳＩの役割は以下の通りである。

【００５３】

レイヤ１：物理レイヤ、すなわちＰＨＹレイヤであるレイヤ１は、電気シグナル、ＲＦシグナル、及び光シグナルとしての通信の物理的性質を明確にするハードウェア固有の情報と、これらのシグナルを、通信システムを使用するためのビットに変換する方法とを含む。ＷｉＦｉ無線、イーサネット（登録商標）、シリアルポート、光ファイバ、３Ｇまたは４Ｇセルラー無線、ツイストペア銅線上のＤＳＬ、ＵＳＢ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ケーブルまたは衛星テレビ、またはオーディオ、ビデオ、またはマルチメディアコンテンツのデジタル放送などの特定の通信メディアをビットストリームに変換することは、ＰＨＹレイヤのタスクである。ＩＰパケットにおいて、プリアンブルは、レイヤ１データを表し、レイヤ１データを送受信するハードウェアにデータパケット、またはフレーム全体を同期させるために使用される。

【００５４】

レイヤ２：データリンクレイヤであるレイヤ２は、フレームとして配置されるビットを含み、ＰＨＹレイヤ１から配信されるビットストリームを解釈可能なデータに変換するルール及び手段を定義する。例えば、ＷｉＦｉ無線ベースのビットストリームは、８０２．１１ａ、８０２．１１ｂ、８０２．１１ｇ、８０２．１１ｎ、及び８０２．１１ａｃを含む任意の数のＩＥＥＥ定義規格に従うことができる。３Ｇ無線通信は、高速パケットアクセ

ス方法ＨＳＤＰＡまたはＨＳＵＰＡを使用して変調されてもよい。光ファイバ内の変調光、または同軸ケーブル上の電気シグナルは、ＤＯＣＳＩＳ　３規格などに従ってデータにデコードされることができる。ＩＰパケットにおいて、レイヤ２データは、そのペイロードを、先頭の「データリンクヘッダ」と後端の「データリンクトレーラ」を含めたデータグラムにカプセル化し、そのペイロードの配信の開始時及び終了時を定義するとともに、伝達プロセスにおいて何も失われていないことを保証する。レイヤ２データの重要な要素は、特定のイーサネット（登録商標）アドレス、ＲＦリンク、またはハードウェア固有のトランシーバリンクとの間でデータトラヒックを誘導するために使用されるＭＡＣ、すなわちメディアアクセスアドレスである。

【００５５】

レイヤ３：ネットワークまたはインターネットレイヤであるレイヤ３は、ＩＰパケットをルーティングするために使用されるＩＰ情報を含む「データグラム」と呼ばれるパケットを含み、該パケットは、パケット内に含まれるペイロードの性質に関する情報と同様に、ＩＰｖ４またはＩＰｖ６データ、及び対応するソースと宛先ＩＰアドレスとを含む。すなわち、使用されるトランスポートプロトコルのタイプは、トランスミッションコントロールプロトコル（ＴＣＰ）、ユーザデータグラムプロトコル（ＵＤＰ）、または他の何らかのものを含む。レイヤ３は、ループを防止する機能も含む。つまり、ＩＰパケットは決して転送されないが、消えることもない。レイヤ３パケットの特定のタイプであるＩＣＭＰは、ネットワークの状態を診断するために使用され、周知の「ピン（ｐｉｎｇ）」機能を含む。ＩＰパケットでは、レイヤ３は「ＩＰ」のヘッダを含み、トランスポートセグメントのヘッダ、及び上位レイヤのセグメントを含むペイロードをカプセル化する。

【００５６】

レイヤ４：トランスポートレイヤであるレイヤ４は、通信デバイス間の接続の性質を定義するデータのセグメントを含み、ＵＤＰによってコネクションレス通信のためのペイロードの最小限の記述要素、すなわちペイロードの大きさ、損失ビットの大きさ、及びどのアプリケーションサービス（ポート）が配信されたデータを使用するか、が定義される。ＵＤＰは、ペイロードの配信を確認せず、代わりにアプリケーションでエラーまたは消失データを確認するため、コネクションレスであると見なされる。ＵＤＰは通常、ブロードキャスト、マルチキャスト、ストリーミングなどの時間的制約のある通信のために使用され、パケットの再送信は選択肢にない。対照的に、ＴＣＰはパケットを確認することによって仮想接続を保証し、次のパケットが送信される前にペイロードが確実に配信され、破棄されたパケットは再送信される。ＴＣＰは、チェックサムを使用して配信されたパケットのデータ保全性も確認し、順序が狂ったパケットを元の順序で再構成するための規定を含む。ＴＣＰ及びＵＤＰの両方が、送信元ポート及び宛先ポート、上位レイヤサービスまたはアプリケーションの記述要素、例えばレイヤ４ペイロード内に含まれる情報に関連したウェブサーバ、または電子メールサーバを定義する。ＩＰパケットにおいて、レイヤ４はＴＣＰ／ＵＤＰのヘッダを含み、上位ＯＳＩレイヤ５、レイヤ６、及びレイヤ７によって使用されるコンテンツを含むデータ／ペイロードをカプセル化する。

【００５７】

レイヤ５、６、７：上位レイヤまたはアプリケーションレイヤであるレイヤ５、レイヤ６、レイヤ７は、データ／ペイロードとしてインターネットによって配信されるコンテンツを記述する。「アプリケーション」レイヤであるレイヤ７は、ＯＳＩモデルにおいて最高レベルを表し、オープンソース及び独自のアプリケーションソフトウェアの両方をサポートするために、６つの基礎となるＯＳＩレイヤに依存している。一般的に使用されるレベル７アプリケーションには、ＳＭＴＰ、ＰＯＰ、またはＩＭＡＰを使用した電子メール、ＨＴＴＰ（Ｃｈｒｏｍｅ、Ｓａｆａｒｉ、Ｅｘｐｌｏｒｅｒ、Ｆｉｒｅｆｏｘ）、ＦＴＰを使用したファイル転送、及びＴｅｌｎｅｔを使用したターミナルエミュレーションが含まれる。独自のアプリケーションには、Ｍｉｃｒｏｓｏｆｔ　Ｏｆｆｉｃｅ製品（Ｗｏｒｄ、Ｅｘｃｅｌ、ＰｏｗｅｒＰｏｉｎｔ）、Ａｄｏｂｅ　Ｉｌｌｕｓｔｒａｔｏｒ及びＰｈｏｔｏｓｈｏｐ（登録商標）、Ｏｒａｃｌｅ及びＳＡＰのデータベースアプリケーショ

ン、Ｑｕｉｃｋｅｎ、Ｍｉｃｒｏｓｏｆｔ Ｍｏｎｅｙ、及びＱｕｉｃｋＢｏｏｋｓの財務ソフトウェア、プラスオーディオ（ｐｌｕｓ ａｕｄｉｏ）及びビデオプレイヤ（ｉＴｕｎｅｓ、ＱｕｉｃｋＴｉｍｅ、Ｒｅａｌ Ｍｅｄｉａ Ｐｌａｙｅｒ、Ｗｉｎｄｏｗ Ｍｅｄｉａ Ｐｌａｙｅｒ、Ｆｌａｓｈなど）、及びＡｄｏｂｅ Ａｃｒｏｂａｔ Ｒｅａｄｅｒ、Ａｐｐｌｅ Ｐｒｅｖｉｅｗなどのドキュメントリーダが含まれる。レベル７のアプリケーションは、一般的に、テキスト、グラフィック＆ピクチャ、サウンド及びビデオ、ＸＭＬまたはＰＤＦなどのドキュメントプレゼンテーション、暗号化などのセキュリティ機能を含むレベル６の「プレゼンテーション」レイヤによって構文的に定義された埋め込みオブジェクトも利用する。レベル５の「セッション」レイヤは、１つのオブジェクトを他のプログラムファイルにインポートするなど、アプリケーション間の接続を確立し、セッションの開始及び終了を制御する。

【００５８】

前述のように、ＯＳＩの７レイヤモデルは各レイヤの機能を定義し、対応するＩＰパケットは各レイヤに関連するデータをカプセル化する。木の人形の中に別の人形が入っており、その人形の中にさらに別の人形が入っている、バブシュカ（ｂａｂｕｓｈｋａ）、すなわちロシアの入れ子人形に類似した方法で、１つのレイヤの中に他のレイヤが入っている。外部パケット、すなわちレイヤ１であるＰＨＹレイヤは、全ての上位レベルに関する情報を含むＩＰフレーム全体を定義する。このＰＨＹデータ内では、レイア２のデータフレームはデータリンクレイアを記述し、レイア３のデータフレームを含む。同様に、このデータフレームはインターネットレイアをペイロードとして記述し、レイア４のデータフレームはトランスポートレイアを記述する。トランスポートレイアは、レイア５、６、７のコンテンツを含む上層のデータをペイロードとして伝送する。

【００５９】

下位の物理レイヤ及びデータリンクレイヤはハードウェア固有であるが、ネットワーク情報及び転送情報を記述するＩＰパケット内でカプセル化された中間ＯＳＩレイヤは、ＩＰパケットの通信及び配信に使用されるハードウェアには完全に関知しない。さらに、トランスポートレイヤのペイロードとしてカプセル化された上位レイヤは、パケットがインターネット経由でルーティングまたは配信された方法とは完全に独立して適用及び操作するアプリケーションにのみ固有である。この分割により、各レイヤを本質的に独立して管理することが可能になり、パケットフォーマットの管理上の承認、及びパケットペイロードの実行可能性の確認を必要とすることなく無数の技術及びユーザの組み合わせがサポートされる。不完全、または不適切なＩＰパケットは、単に破棄される。このようにして、パケット交換ネットワークは、インターネットに接続された任意のデバイスまたはオブジェクト間で、一貫した方式で、異なる通信メディアを介して多様なアプリケーション関連情報をルーティング、転送、及び配信することができる。

【００６０】

結論として、回路交換ネットワークは、（１世紀前の従来型電話システムと同様に）通信している２人以上の当事者間の、単一の直接接続を必要とする。パケット交換ネットワーク通信は、文書、音声、ビデオ、及びテキストを複数のパケットに分解するが、それらのパケットを複数のネットワークパス（正確かつタイムリーな方法で配達するために最善の努力を払う郵便局に類似している）を介して配信し、その後、最初のコンテンツを再構築し、途中で何も失われていないことを確認する。下記の表は、公衆交換電話ネットワーク（ＰＳＴＮ）とパケット交換ＶｏＩＰの比較を要約である。

【００６１】

【表１】

ネットワーク	ＰＳＴＮ	インターネット
技術	回路交換	パケット交換
接続	専用の電気接続	インターネット上での各パケットのルーティング
データ配信	リアルタイム（回路）	ベストエフォート（パケット）
シグナル	アナログ又はデジタル	デジタル、ＩＰ、ＶｏＩＰ
コンテンツ	音声	音声、テキスト、データ、ビデオ
データ速度	遅い	速い
エラーチェック	なし、又は最小限	広範囲
断線の影響	通話の切断又は乱れ	通話の再ルーティング
電力不足の影響	ネットワークが電力を伝送	バッテリーのバックアップが必要

【００６２】
ＰＳＴＮはリアルタイム電気回路接続を使用して操作するが、パケット交換ネットワークコンテンツは、様々なトラック及び郵便集配人を使用して、到着が遅れた場合であっても最終的に手紙を配達する郵便局とは異なり、「ベスト・エフォート」方式を使用してコンテンツを配信し、パケット及びペイロードを配信する経路を見つける。パケット交換ネットワーク及びコミュニケーションは、「セキュア動的通信ネットワーク及びプロトコル」と呼ばれる特許の背景のセクションにその詳細が説明されている。
【００６３】
ネットワークの性能を考えるとき、いくつかの要因が考えられ、すなわち、
・データレート、すなわち帯域幅、
・サービスの質、
・ネットワークとデータのセキュリティ、
・ユーザのプライバシー
が考えられる。
【００６４】
上記の考慮事項のうち、データレートは数百万バイト／秒、すなわちＭｂｐｓで容易に定量化される。一方、サービス品質またはＱｏＳには、レイテンシー（待ち時間）、音質、ネットワーク安定性、断続的な動作または頻繁なサービス中断、同期や接続の失敗、信号強度の低下、アプリケーションの停止、緊急時の機能ネットワークの冗長性などを含むいくつかの要因を含まれる。サイバーセキュリティとサイバープライバシーは、サイバー犯罪、サイバー監視、ＩＰパケットスニッフィング、ＤｏＳ攻撃、プロファイリング、詐欺師、パケットハイジャッキング、サイバー感染、監視、サイバー犯罪者による管理及び侵入などを取り扱い、ネットワークへの攻撃及びデータトラフィックとコンテンツに許可されないアクセスを防御する。
【００６５】

ＱｏＳ（サービスの品質）

【００６６】

ＱｏＳとは、ネットワーク上のパフォーマンスであり、ネットワークのキャパシティ、帯域、レイテンシー、データ速度、スケーラビリティ、音品質、データインテグリティ、データビット誤り率や他のパフォーマンスに基づいたパラメータなどを使い示される。プログラム、ファイル、及びセキュリティ関連の検証では、データの正確さが重要な要素である。どの要素が重要かは、パケット交換ネットワークを介して運ばれるペイロードの性質によって決まる。対照的に、リアルタイムアプリケーションを含む音声及びビデオの場合、パケット配信時間に影響を及ぼす要因が重要である。品質要因と、それらがビデオ、音声、データ、テキストなどのさまざまなアプリケーションにどのように影響するかは、アプリケーションによる。一貫した高データレートＩＰパケット波形によって代表される良好なネットワーク状態は、最小時間遅延、明確に強い信号強度、信号歪み、安定動作、及びパケット伝送損失がないものである。

【００６７】

短期間の中断を伴うより低いデータレートのパケット波形による断続的なネットワークは、ビデオ機能に最も大きな影響を与え、不快なほど遅いビデオダウンロードを引き起こし、ビデオストリーミングを受け入れ難くする。ＩＰパケット波形によって例示される規則的な短時間の中断を伴いより低い実効データスループット速度を引き起こす輻輳したネットワークは、断続的な動き、ファジーな画像、及び不適切な着色及び輝度を伴ってビデオ映像をひどく劣化させるだけでなく、エコー、さらには会話やサウンドトラックから全体の削除さえ引き起こす。しかし、輻輳したネットワークでは、再ブロードキャストの要求を繰り返すことによってＴＣＰを使用してデータが供給され得る。不安定なネットワークは、予測できない期間の多数のデータ停止を伴う低いデータスループット率を示す。不安定なネットワークはまた、波形６１０Ｄにおいて濃い影の付いたパケットによって表される破損したＩＰパッケージを含み、これは、ＴＣＰベースのトランスポートでは再送が必要であり、ＵＤＰトランスポートでは単に破損したデータや不適切なデータとして破棄される。ネットワークの一部のレベルでは電子メールも断続的になり、ＩＭＡＰの同期は失敗する。軽量のデータフォーマットのため、ほとんどのＳＭＳ及びテキストメッセージは、ネットワークの輻輳が深刻な場合でも配信遅延が発生するものの転送されるが、添付情報はダウンロードされない。不安定なネットワークでは、全てのアプリケーションが失敗し、配信が予想されるファイルを待機するコンピュータまたは携帯電話の通常の動作フリーズすることさえある。このような場合、ビデオはフリーズし、音声が途切れて聞こえなくなり、数分以内に１０回以上もＶｏＩＰ接続が繰り返し落ち、場合によっては完全に接続できなくなる。同様に、電子メールは、コンピュータのアイコンがいつまでも回転し続ける形で、ストールまたはフリーズする。プログレスバーは完全に停止する。テキストメッセージもバウンスし、「配信不能」となる。

【００６８】

重要なサーバやスーパーＰＯＰの停電、過負荷の通話量、巨大なデータファイルやＵＨＤムービーの送信、一部のサーバやネットワークに対する重大なサービス拒否攻撃など、多くの要因がネットワークの不安定化につながる可能性があり、ネットワークのＱｏＳを追跡する重要な要因には、そのパケット廃棄率とパケットラテンシー（待ち時間）がある。廃棄パケットは、ＩＰパケットが配信されず、永久的なものとして「タイムアウト」した場合や、ルータまたはサーバがＩＰパケットのヘッダのチェックサムエラーを検出した場合に発生する。ＵＤＰを使用するパケットの場合、パケットは失われ、レイヤ７アプリケーションは、何かが失われたことを知るべく十分にスマートでなければならない。ＴＣＰがレイヤ４トランスポートに使用される場合、パケットは再送信のために要求され、潜在的にすでにオーバーロードされている可能性のあるネットワークへのロードをさらに追加する。

【００６９】

ＱｏＳ、伝搬遅延を決定する他の要因は、ノード間でのＩＰパケットの遅延として、ま

たは送信元から宛先への一方向に、あるいは送信元から宛先へ及び宛先から送信元への往復遅延として、いくつかの方法で定量的に測定することができる。ＵＤＰとＴＣＰのトランスポートプロトコルを使用したパケット配信に対する伝搬遅延の影響。インターモーダルネットワーク伝播遅延が増加すると、ＶｏＩＰ会話のような往復通信を実行するために必要な時間が長くなる。ＵＤＰトランスポートの場合、往復遅延は伝搬遅延とともに線形に増加する。長い伝播遅延はより高いビット誤り率と相関するので、失われたＵＤＰパケットの数は増加するが、ＵＤＰは破棄されたパケットの再送を要求するので、往復時間は遅延の増加に対して線形のままである。ＴＣＰトランスポートは、パケット配信を確認するために必要なハンドシェイクのために、ＵＤＰよりも送信される各パケットについて実質的により長い往復時間を示す。ビット誤り率が低いままであり、ほとんどのパケットが再送を必要としない場合、ＴＣＰ伝播遅延は、インターモーダル伝播遅延に対して線形に増加するが、より高いレート、すなわちＴＣＰのラインの傾きで増加する。しかしながら、通信ネットワークが伝搬遅延の増大につれて不安定になると、廃棄されたパケットの再送信のためのプロトコルの必要性のために、ＴＣＰ転送から生じる往復時間は指数関数的に増加する。したがって、ＶｏＩＰは、ＶｏＩＰやビデオストリーミングなどの時間の影響を強く受けるアプリケーションに対しては禁忌である。

【００７０】

全てのパケット通信は統計的であり、同じ伝搬時間を有する２つのパケットがないので、ネットワークの単一方向の待ち時間を推定する最良の方法は、同様のサイズの多数のＩＰパケットの往復時間を測定し、割って単一方向レイテンシーを推定することによる方法である。１００ｍｓ未満のレイテンシーは極めて良好であり、２００ｍｓまでは非常に良いと考えられ、３００ｍｓまでは許容可能と考えられる。インターネット上で実行されているＯＴＴアプリケーションが容易に遭遇する５００ｍｓの伝搬遅延に対して、その遅延はユーザにとって不快になり、通常の会話に干渉する。音声通信では、特に、そのような長い伝搬遅延は「悪いもの」として現れ、残響をもたらす可能性があり、「弦をはじいた様な」または金属的なサウンドの音声を作りだし、相手が相手の最後のコメントに応答するのを待っている間に通常の会話を中断し、壊れた理解できない音声を出力することがある。

【００７１】

明確化のために述べると、通信の片方向のレイテンシー（待ち時間）は、レイヤ３ＩＣＭＰユーティリティ（http://www.speedtest.netの無料ネットワークスピードテストなど）によって実行されるｐｉｎｇテストとは異なるが、これらの相違する理由は、一つにはＩＣＭＰパケットは実際のＩＰパケットに比べて一般的に軽量であるため、ｐｉｎｇテストではＴＣＰの「再送要求」機能を使用しないため、及びインターネット上パブリックネットワーク上でｐｉｎｇテストのルートが実際のパケットルートと一致する保証はないため、である。要するに、ｐｉｎｇが長い遅延を経験する場合、ネットワークにまたはデバイスとネットワークとの間のいずれかのリンク（例えばＷｉＦｉルータまたはラストマイル）に何らかの問題があるのだが、良好なｐｉｎｇの結果がでても、それ自体では、実際のパケットの伝播遅延の小ささを保証することはできない。

【００７２】

ネットワークセキュリティを向上させるために、ハッキング、スニッフィング、またはスパイ行為を防ぐために、暗号化と検証のメソッドが採用されることが多い。しかし、重い暗号化と複数の鍵の暗号化プロトコルは、会話相手のＩＤを絶えず再確認し、追加の遅延を作り出し、有効なネットワーク待ち時間を増加させ、セキュリティ向上の代価としてＱｏＳを低下させる。

【００７３】

サイバーセキュリティとサイバープライバシー

【００７４】

コミュニケーションにおける他の２つの主要な考慮すべき事項は、サイバーセキュリティとサイバープライバシーである。関連しているが、２つの問題は多少異なる。ネットワ

ークセキュリティ、コンピュータセキュリティ、セキュリティを確保した通信を含む「サイバーセキュリティ」は、コンピュータまたは通信ネットワーク、ネットワークアクセス可能なリソース、またはネットワークに接続されたデバイスに含まれるデータへの不正アクセス、誤用、変更、または拒否を監視、インターセプト、及び防止するための方法を含む。そのようなデータは、個人情報、バイオメトリックデータ、財務記録、健康記録、私的な通信及び記録、並びに私的な写真画像やビデオ記録を含み得る。ネットワークに接続されたデバイスには、デスクトップ、ファイルサーバ、電子メールサーバ、ウェブサーバ、データベース、個人データストレージ、クラウドストレージ、インターネット接続アプライアンス、ネット接続された車、個人が使用する公的共有デバイス（ＰＯＳターミナル、ガスポンプ、ＡＴＭ等）が含まれる。

【００７５】

明らかに、機密情報への不正アクセスを試みるサイバー犯罪者やコンピュータハッカーが犯罪を起こしている。違法に入手したデータに個人的な個人情報が含まれている場合、その攻撃は被害者の個人情報の侵害にもなる。しかし、逆にサイバー犯罪を必要とすることなくプライバシー流出が発生し、実際には阻止できない可能性がある。今日のネットワークに接続された世界では、セキュリティ侵害を必要とせずに、個人情報の不正使用が発生する可能性がある。多くの場合、１つの目的のためにデータを収集する企業は、別の目的のためにデータを使用することに関心のある他のクライアントにデータベースを販売することを選択することがある。マイクロソフト社がＨｏｔｍａｉｌ（登録商標）を購入したときですら、潜在的な顧客をスパムすることに関心のある広告主にメールリストを販売したことはよく知られていた。そのような行動がサイバープライバシーの侵害とみなされるべきか否かは、依然として意見の問題とされている。

【００７６】

インターネットプライバシー、コンピュータプライバシー、及びプライベートコミュニケーションを含む「サイバープライバシー」は、各人の非公開情報及び個人情報及びその使用（情報の収集、保存、表示または他人との共有を含む）をコントロールする個人の個人的権利または義務を含む。非公開個人情報には、身長、体重、年齢、指紋、血液型、運転免許証番号、パスポート番号、社会保障番号、または名前を知らなくても個人を識別するのに役立つ個人情報などの個人のＩＤ情報が含まれる。将来、個人のＤＮＡマップさえも法的記録の問題になる可能性がある。個人ＩＤ情報とは別に、いわゆる個人情報とは別の非公開の私的情報には、私たちが購入する服のブランド、頻繁にアクセスするウェブサイト、喫煙や飲酒の習慣の有無、銃の所有者か否か、運転する車の種類、それまでの病歴、家族には特定の病気や病気の病歴があるか否か、どんな種類の人に惹かれているかということさえ含まれる。

【００７７】

この個人情報は、個人の所得、税額、不動産訴訟、犯罪記録、交通違反、ソーシャルメディアサイトに掲載されたあらゆる情報に関連する公的記録と組み合わされて、利害関係者のための強力なデータセットを形成する。人口統計学的、個人的、財政的、生物医学的、行動傾向に関する情報を捕捉し、今日のパターン、傾向及び統計的相関関係のデータを採取する大規模なデータセットの意図的な収集を「ビッグデータ」という。保険会社、ヘルスケア、製薬会社、医療過誤弁護士などの医療業界は全て、ビッグデータとして保存されている個人情報に深い関心を持っている。自動車及び消費材製造企業は同様に、市場戦略及び広告予算の方向を決めるために、そのようなデータベースへのアクセスを望んでいる。最近の選挙では、投票者の意見や回避すべき政治的論争の争点をよりよく理解するために、政治家さえもビッグデータを参考にし始めている。

【００７８】

サイバープライバシーの問題は、今日のビッグデータが個人情報を取得しているか否かではなく、データセットがあなたの氏名を保持しているか否か、またはあなたの氏名が分からなくてもあなたを特定するための十分な個人情報を保持しているか否かではない。例えば、当初、米国政府は、民間医療アカウントが開設されると、医療費負担適正化法（Ａ

ＣＡ）に基づいて使用されたｈｅａｌｔｈｃａｒｅ．ｇｏｖウェブサイトによって収集された個人情報が破壊されると述べた。そして、最近発覚したこととして、米国政府のためのデータ収集を促進する第三者法人が、収集したデータを保持し使用する権利をもつという政府との契約に署名していたことが明らかになり、米国政府に預けられた非公開個人情報も実際に非公開ではないことが分かった。

【００７９】

最後に、同様の技術的手法を用いて政府と犯罪組織によって監視が行われていることを述べなければならない。犯罪者がそのようなデータを収集する法的権利を持っていないことは明らかであるが、権限のない政府の監視のケースは、国によって大幅に変わる。例えば米国のＮＳＡは、アップル、グーグル、マイクロソフトなどにクラウドやデータベースへのアクセスを提供するように繰り返し圧力をかけてきた。政府関係者でさえ、会話とコミュニケが盗聴され、傍受されている。マイクロソフトの一部門であるＳｋｙｐｅ（登録商標）が発信者のコンテンツを監視するか否か尋ねられたとき、Ｓｋｙｐｅ（登録商標）のＣＩＯは唐突に「ノーコメント」と答えた。

【００８０】

サイバー犯罪とサイバー監視の方法

【００８１】

サイバーセキュリティの関連に焦点を当てると、デバイス、ネットワーク、コンピュータデータへの不正アクセスを得るための多数の手段が存在する。サイバー犯罪を実行し、セキュリティを確保したネットワークに不正な侵入をするために使用されるさまざまなマルウェアとハッカーの技術がある。

【００８２】

例えば、インターネットに接続されたタブレットを使用する個人は、ビジネスオフィスの電話に電話をかけたり、テレビにメッセージを送信したり、電話で回線交換ＰＯＴＳネットワークを使用している国の友人に電話をかけたり、ウェブストレージからファイルをダウンロードしたり、電子メールサーバを介して電子メールを送信することができる。全てのアプリケーションがインターネットとグローバルな相互接続性を有する通常のアプリケーションを表しているが、ネットワーク全体を通じて監視、サイバー犯罪、詐欺、個人情報の盗難の機会が数多く存在する。

【００８３】

例えば、セルラー無線アンテナ及びＬＴＥ基地局を介して、または短距離無線アンテナ及び公衆ＷｉＦｉ基地局を介してネットワークに接続するタブレットの場合には、不正侵入者は無線リンクを監視することができる。同様に、ＬＴＥコールは、傍受用無線受信機またはスニファによって監視または「盗聴」することができる。同じスニファは、ＷｉＦｉ通信、及びケーブルＣＭＴＳとケーブルモデムとの間のケーブル上の受信端をモニタするように調整することができる。

【００８４】

一部の例では、ＬＴＥコールが、サイバーパイレーツ偽タワーによって傍受され、タブレットとセルラータワーとの間に迂回通信経路を確立することもできる。パケット交換ネットワークを介してルータ、サーバ、及びクラウドストレージへの送信を含む通信は、中間攻撃においても他人による攻撃を受ける。盗聴器は、ＰＳＴＮゲートウェイから電話機へのＰＯＴＳ回線上のコール、及びＰＢＸサーバからオフィス電話機への企業ＰＢＸ回線上のコールを傍受することができる。

【００８５】

一連のセキュリティ違反を行うことによって、スパイウェアは、タブレット、ルータ、ＰＳＴＮブリッジ、クラウドストレージ、ケーブルＣＭＴＳ、またはデスクトップにインストールできる。トロイの木馬のソフトウェアは、タブレットまたはデスクトップにインストールされ、パスワードをフィッシングする可能性がある。ワームも、特にコンピュータがアクティブＸ機能を有効にしたＭｉｃｒｏｓｏｆｔのオペレーティングシステムを実行している場合に、デスクトップを攻撃するために使用され得る。最後に、サービス拒否

攻撃を開始するために、ウイルスは、サーバやデスクトップやタブレットなど、ネットワークに接続された任意の数のデバイスを攻撃することができる。

【００８６】

通信ネットワーク及びインフラストラクチャの様々な部分に対して、各形態のマルウェアが動作する事が可能であり、それらのサイバー攻撃は、ウイルス、中間者攻撃、政府監視、及びサービス拒否攻撃を含み得る。通信ネットワークのラストマイルは、さらに広範はマルウェアやサイバー攻撃の機会を提供し、ローカルの電話会社／ネットワーク、ラストリンク、及びデバイスの３つのセクションに分かれている。ローカルの電話／ネットワークは、高速ファイバ、ルータ、ケーブルＣＭＴＳ、ケーブル／ファイバ、ケーブルモデム、ＷｉＦｉアンテナ、及びＬＴＥ無線タワーを含む。ネットワーク無線スニファのこの部分では、スパイウェア、ウイルス、及び中間者攻撃が全て可能である。

【００８７】

ラストリンクのデバイスへのローカル接続では、ネットワーク接続は、スパイウェア、無線スニファ、盗聴、及び偽タワーの影響を受ける有線リンク、ＷｉＦｉリンク、及びＬＴＥ／無線リンクを含む。例えば、タブレット、ノートブック、デスクトップ、スマートフォン、スマートテレビ、ＰＯＳ端末なども含むことができるデバイス本体は、スパイウェア、トロイの木馬、ウイルス、及びワームを含む多種の攻撃の対象となる。このような監視方法や装置は、市販されておりオンライン市場で、イーサネット（登録商標）ローカルエリアネットワーク、ＷｉＦｉデータや携帯電話のコミュニケーションを監視する端末が容易に入手できる。最近までは光ファイバクラウド接続のスニッフィングが脅威として特定されていなかったが、光通信のための非侵襲的なデータスニファ、すなわちファイバを切断する必要なく、一時的にであっても正常な動作が損なわれずに使用できるスニファが現在存在していることが明らかとなった。

【００８８】

ハッキングと監視方法の使用以外にも、携帯電話の会話やインターネット通信を監視するための多種多様な商用スパイウェアが容易に利用可能である。市販で売られているスパイウェアプログラムは、従業員、子供、及び配偶者の情報を有効利用するためにスパイする機能を広告している。この機能セットは驚くほど包括的であり、そこには電話、写真、ビデオ、ＳＭＳ／ＭＭＳテキスト、サードパーティのインスタントメッセージング、電子メール、ＧＰＳロケーショントラッキング、インターネット利用、アドレス帳、カレンダーイベント、バグ、コントロールアプリ、さらにはリモートコントロール機能等、驚くほど説得力のある数のサイバープライバシーを侵害する方法が含まれている。実際、サイバー攻撃は頻繁になり、毎日トラッキングされている。

【００８９】

サイバー攻撃を開始するには、一般に次のようないくつかの段階または技術の組み合わせが必要である。すなわち

・ＩＰパケットスニッフィング、
・ポートスキャン、
・プロファイリング、
・詐欺、
・パケットハイジャック、
・サイバー感染、
・監視、
・サイバーパイレーツサイト管理

等が必要である。

【００９０】

ＩＰパケットスニッフィング

【００９１】

サイバー犯罪者は、無線監視デバイスを使用して、ユーザ、そのトランザクション、及びそのアカウントに関する重要な情報を得ることができる。ＩＰパケットの内容は、２名

のユーザ間のパスのどこでも取得すなわち「スニッフィング」できる。例えば、ユーザがＩＰパケット内のファイル（例えば写真またはテキスト）を自分のノートブックからの携帯電話に送信すると、サイバーパイレーツは、送信者の最後のリンクをインターセプトし、送信者のローカルネットワークをインターセプトし、クラウドを監視し、受信者のローカル電話会社をインターセプトするか、または受信機の最後のリンクをインターセプトすることのいずれかによって、任意の数の場所でＩＰパケットを発見することができる。インターセプトされたＩＰパケットに含まれる観測可能なデータは、通信で使用されるデバイスのレイヤ２ＭＡＣアドレス、受信側の送信者のレイヤ３アドレス、すなわちパケットの宛先を含み、ＵＤＰ、ＴＣＰなどのトランスポートプロトコルが使用される。ＩＰパケットには、要求されているサービスのタイプを潜在的に定義している送受信デバイスのレイヤ４ポート番号と、データファイル自体も含まれており、ファイルが暗号化されていない場合には、ファイルに含まれるデータをサイバーパイレーツが直接読み取ることも可能となる。

【００９２】

ペイロードが暗号化されていない場合、口座番号、ログインシーケンス、パスワードなどのテキスト情報を読み取ることができ、それが価値あるものである場合、盗まれ、犯罪目的のために悪用されることがある。ペイロードにビデオや絵文字の情報が含まれている場合、コンテンツがどのレイヤ６アプリケーションフォーマットを採用しているかを判断するためにいくつかの追加作業が必要であるが、一度特定されれば、コンテンツを、閲覧、公開、またはおそらく通信相手の一方または両方を脅かすために使用することが可能となり得る。このようなサイバー攻撃は、サイバーパイレーツが個人的に通信相手を知ることはないため、「中間攻撃者」と呼ばれている。

【００９３】

前述したように、クラウド内のＩＰパケットルーティングは予測不可能なので、クラウドを監視することはより困難となり、すなわち監視が困難になる理由は、サイバーパイレーツはＩＰパケットの重要な情報に最初に遭遇したときに補足しなければならず、かつ後続のパケットが同じ経路とスニッフィングされたパケットに従わないことがあるからである。ラストマイルのデータを傍受することは、同じ会話を構成する一連の関連するパケットを観察する確率が高くなるが、その理由は、ローカルルータは通常、少なくともパケットが顧客自身のキャリア外のＰＯＰに到達するまで、所定のルーティングテーブルに従うからである。例えば、コムキャスト社のクライアントは、パケットがコムキャスト社の管理範囲及びカスタマーサービス領域を超えて地理的に移動するまで、完全にコムキャスト社が所有するネットワークを使用して、ルーティングチェーンの上にＩＰパケットを渡す可能性が高い。

【００９４】

同じ２つのＩＰアドレス間の連続したパケットが十分に長い間発生した場合、会話全体を細かく再現することができる。例えば、ＳＭＳテキストメッセージがラストマイルで同じネットワークを通過する場合、サイバーパイレーツは、ＩＰアドレス及びポート＃によって、テキストを運ぶ複数のＩＰパケットが、同じ２つのデバイス、すなわち携帯電話とノートブックの間の会話を表すことを特定することができる。従って、アカウント番号とパスワードが異なるメッセージでテキスト化されるか、または不完全に多くのパケットに送信されたとしても、パケット識別子の一貫性により、サイバーパイレーツは会話を再構築してアカウント情報を盗むことができる。アカウント情報を盗めば、オフショア銀行に送金することが可能となり、またはアカウントのパスワードとセキュリティに関する質問を変更することによって、つまり一時的にＩＤ盗難を使ってアカウント権限を奪うことさえできる。

【００９５】

ペイロードが暗号化されていても、ＩＰアドレス及びポート番号を含む残りのＩＰパケットは暗号化されない。十分なコンピューティングパワーにアクセスできるサイバーパイレーツは、多数のＩＰパケットを繰り返しスニッフィングした後、暗号のパスワードを破

るまで組織的に全ての組み合わせを試みる。鍵が破られると、パケット及び全ての後続のパケットは、サイバーパイレーツが解読して使用することが可能となる。「パスワード推測」によるログインパスワードのクラックの確率は、パケットスニッフィングが以下に説明するユーザ及びアカウント「プロファイリング」と組み合わされると大幅に向上する。「中間攻撃者」では、サイバーパイレーツが彼らに直接アクセスできないため、通信デバイスは通常は関与していないことに注意されたい。

【００９６】

ポートスキャン

【００９７】

デバイスに侵入するもう１つの方法は、そのＩＰアドレスを使用して多くのレイヤ４ポートを調べ、全ての要求が応答を受信するかどうかを確認することである。一旦サイバーパイレーツがパケットスニッフィングまたは他の手段からＩＰアドレスを有する携帯電話をターゲットデバイスとして特定すると、サイバーパイレーツは、携帯電話上のポートに対して一連の問い合わせを開始し、セキュリティの確保されていないポートすなわちオープンポート、サービス及び保守ポート、またはアプリケーションバックドアを探す。ハッカーの問い合わせプログラムは全てのポート番号を体系的に循環することができるが、攻撃は通常、ｐｉｎｇのためのポート＃７、ＦＴＰのためのポート＃２１、ｔｅｌｎｅｔターミナルエミュレーションのためのポート＃２３、シンプルメールのためのポート＃２５など、悪名高い脆弱なポートに焦点を当てて行われる。サイバーパイレーツは、パケットを送り応答が送信されるたびに、ターゲットデバイスのオペレーティングシステムに関する詳細を学習する。

【００９８】

ポートスキャンプロセスでは、サイバーパイレーツは本物のＩＤを公開したくないので、メッセージを受信するのに、個人として追跡できない偽装疑似アドレスを使用する。また、サイバー犯罪者は盗まれたコンピュータとアカウントを使用する可能性があるため、他の誰かがターゲットデバイスをハッキングしようとしているように見え、追跡された場合、調査者は彼らではない無罪の人にそれを戻す。

【００９９】

プロファイリング

【０１００】

ユーザとアカウントのプロファイリングとは、サイバーパイレーツが、公開されている情報を使用してターゲット、アカウント、及び個人履歴を調べて、パスワードを解読し、アカウントを特定し、資産を判定するプロセスである。ハッカーは、スニッフィングなどの手段を使用してターゲットのＩＰアドレスを取得すると、トレースルート・ユーティリティを使用してデバイスのアカウントのＤＮＳサーバを見つけることができる。その後、インターネット上の「Ｗｈｏ　ｉｓ」機能を利用することにより、アカウント所有者の氏名を見いだすことができる。プロファイリングでは、サイバー犯罪者がインターネット上を検索し、アカウント所有者に関する利用可能な全ての情報を収集する。情報源には、不動産取引、自動車登録、結婚と離婚、租税先取特権、駐車券、交通違反、犯罪記録などの公的記録が含まれる。多くの場合、大学や専門家のウェブサイトには、自宅住所、電子メールアドレス、電話番号、個人の生年月日が含まれている。Ｆａｃｅｂｏｏｋ、ＬｉｎｋｅｄＩｎ、Ｔｗｉｔｔｅｒなどのソーシャルメディアサイトを調査することで、サイバー犯罪者は重要な詳細情報を収集することができ、このような情報には、家族や友人、ペットの名前、前の自宅の住所、同級生、個人的な大事な出来事、恥ずかしい出来事、家族の秘密、そして個人的な敵を含む写真やビデオのファイルが含まれる。

【０１０１】

サイバーパイレーツの次のステップは、このプロファイルを使用して、プロファイルに基づいてユーザのパスワードを「推測」し、ターゲットデバイスと同じ個人の他のアカウントをハッキングすることである。一旦サイバー犯罪者が１つのデバイスのパスワードをクラッキングしてしまえば、人は記憶を容易にするためにパスワードを再利用する傾向が

あるため、サイバー犯罪者が他のアカウントに侵入する可能性は非常に高い。その時点で、人のＩＤを盗み、金銭を移動し、警察の捜査の対象にしてしまい、全ての資産を盗んで、その人の生活を本質的に破壊することが可能にもなり得る。例えば、本明細書の冒頭で説明したように、盗まれたアカウントから長いパスワードリストを収集するサイバー犯罪者は、同じパスワードとログイン情報を使用してコンサートやスポーツイベントへのプレミアムチケットを何百万ドルも違法に購入する。

【０１０２】

詐欺師

【０１０３】

サイバーパイレーツが誰かに偽装して、不正なサイバーセキュリティクレデンシャル情報を使用して通信やファイルにアクセスした場合、サイバーパイレーツは「詐欺師」として行動している。詐欺師タイプのサイバー攻撃は、サイバー犯罪者が個人アカウントに関する十分な情報またはアクセス権を所有して、被害者のアカウントを奪取し、不当に被害者の代理となって個人に対してメッセージを送信し、彼らがハッキングされたアカウントの所有者がそれを行ったと誤解させる形で発生し得る。最近、例えば、発明者の一人の個人的な友人が、彼女の「ＬＩＮＥ」パーソナルメッセンジャーアカウントをハッキングされた。アカウントを引き継いだサイバー犯罪者は、「車の事故があり、緊急融資のための資金が必要だ」という虚偽のメッセージを友人に送った。アカウントがハッキングされていることを知らないので、彼女の友人はリクエストが本当であり、彼女に急いで資金援助を行った。疑われるのを避けるためか、各友人に送られたリクエストは１，０００米ドル以下であった。幸運にも、送金する直前に、友人の一人が彼女に電話して送金情報を再確認したことで、詐欺が明らかになった。この電話がかけられなければ、これが詐欺師からのリクエストで、回線のアカウントの所有者がその名義で送金されたことも送金を要求されたことすら知らない状態だったと、誰も知ることはできなかったと思われる。

【０１０４】

別の形式の虚偽表示は、デバイスがセキュリティ特権を与えられ、サーバまたは他のネットワーク接続されたデバイスと情報を交換できるようになっており、サイバーパイレーツのデバイスが何らかの手段によって自らを認証されたサーバとして偽装する場合に発生し、犠牲者のデバイスは、サイバーパイレーツサーバへ詐欺サーバとは知らずにファイルや情報を委ねてしまうことになる。この方法は、バックアップクラウドが詐欺師のものであったことを除いて、有名人に通常のようにｉＣｌｏｕｄ（登録商標）を使ってプライベート画像ファイルをバックアップさせるために使用されたと言われている。

【０１０５】

詐欺師の別の形態は、人の電話または開いているブラウザに物理的にアクセスしている人が、電子メールを送信や電話への応答を行ったり、そこからさらに他の人のアカウントやデバイスからテキストメッセージを送信したりするなどの詐欺行為を行った場合に発生する。受信側は、既知のデバイスまたはアカウントに接続されているため、そのデバイスまたはアカウントを操作している人物が所有者であることを前提としている。詐欺の内容は、Ｆａｃｅｂｏｏｋに恥ずかしいコメントをフレンド投稿するといったいたずら的なもの、または誰かの配偶者が個人的な電話に返答するか、非公開にすべき性質の私的なテキストメッセージをインターセプトするような、より個人情報に関連する性質のものであり得る。この不正アクセスの結果が、嫉妬、離婚、報復的な訴訟につながる可能性がある。オフィスやカフェなどでトイレに行っている間にデバイスを一時的に監督しないままにすると、後の「感染」と題する部分で説明するように、詐欺師が個人情報や企業情報に素早くアクセスしたり、不正な電子メールを送信したり、ファイルを転送したり、マルウェアをデバイスにダウンロードする危険性がある。

【０１０６】

詐欺をベースにしたサイバー攻撃は、デバイスが盗難された場合にも重要である。このような場合では、たとえデバイスがログアウトしていても、泥棒はログインコードを破るのに十分な時間を有している。「ｆｉｎｄ　ｍｙ　ｃｏｍｐｕｔｅｒ」機能、すなわちサイ

バーパイレーツがデバイスに初めてログオンすると、ネットワーク上の盗難されたデバイスの位置を特定し、コンピュータのファイルを消去する機能は、もはや有効でなくなる。ハイテクに精通した犯罪者は現在、携帯電話やＷｉＦｉ接続がない場合にのみ、デバイスをアクティブにすれば良いことを知っているからである。このリスクは、パスラインセキュリティが単純な４桁の個人識別番号（ＰＩＮ）または暗証番号である携帯電話の場合に特に高いものとなる。わずか９９９９通りの組み合わせしかないので、ＰＩＮを破るのは時間の問題である。

【０１０７】

デバイスを保護するための重要な問題は、詐欺師のアクセスを防止することである。詐欺を防ぐには、一定の間隔でユーザのＩＤを認証し、必要な情報と特権にアクセスする権限があることを保証するための堅牢な手段が必要である。デバイスセキュリティはチェーン内の最も弱いリンクであることが多い。デバイスのセキュリティが破られるならば、堅牢なネットワークセキュリティの必要性が疑わしいものとなる。

【０１０８】

パケットハイジャック

【０１０９】

パケットハイジャックは、ネットワークを通過するパケットの正常なフローを悪意のあるデバイスを介して迂回させるサイバー攻撃を含む。

【０１１０】

例えば、もしルータの完全性がサイバーパイレーツからのサイバー攻撃によって損なわれた場合、ルータを通過するＩＰパケットは改訂したＩＰパケットに書き換えられ、ＩＰパッケージをサイバーパイレーツのデバイスの宛先アドレス及びポート番号に経路変更する。次いで、サイバーパイレーツのデバイスは、ＩＰパケットのペイロードから必要な情報を取得し、場合によってはＩＰパケットのペイロードの内容を変更する。不正なペイロードは、「感染」というトピックで後に説明するように、任意の数の種類の不正な犯罪を行ったり、情報を収集したり、マルウェアを携帯電話にダウンロードしたりするために使用される可能性がある。

【０１１１】

ハイジャックされたパケットは、元のＩＰパケットの送信元ＩＰアドレスとポート＃ように改変されるが、実際はそのパケットは新しい子となったルートを通過する。あるいは、ハイジャックされたＩＰパケットは、損なわれたルータに返され、その後、クラウドに送られる。サイバーパイレーツは、パケットハイジャックの犯罪の効果を最大限にするためにパケットハイジャック時にそのＩＤを隠す必要があるため、レイヤ３ＩＣＭＰ機能「ｔｒａｃｅｒｏｕｔｅ」でさえも通信の真の経路の特定が困難になるように、ＩＰパケットの真のルーティングを隠す。ただし、ハイジャックによりパケットルーティングに著しい遅延が追加された場合、異常な遅延がネットワークオペレータによる調査を促す可能性がある。

【０１１２】

サイバー感染

【０１１３】

サイバー攻撃の最も狡猾なカテゴリの１つは、情報を収集し、詐欺を行い、トラヒックをリダイレクトし、他のデバイスを感染させ、悪化させたり、閉鎖したりするマルウェアを標的デバイスまたはネットワークにインストールする「サイバー感染」すなわちサービス妨害をさせなくする状態を引き起こすことである。サイバー感染は、電子メール、ファイル、ウェブサイト、システム機能拡張、アプリケーションプログラム、またはネットワークを通じて広がる。マルウェアの１つの一般的なクラス「スパイウェア」は、あらゆる種類のトランザクション情報を収集し、それをサイバーパイレーツに渡す。「フィッシング」の場合には、慣れ親しんだログインページのように見えるウェブページやアプリケーションシェルがアカウントのログインや個人情報の入力を求め、得た情報をサイバーパイレーツに転送する。さらに他のマルウェア感染では、ハードウェアを制御することが可能

で、例えば前述のパケットハイジャックを実行するようにルータを制御する等を行う。このような場合、サイバーパイレーツは自分の目的のために有益な情報や制御を得ようとする。

【０１１４】

ウイルス、ワーム、トロイの木馬等のサイバー感染の別のクラスは、重要なファイルを上書きするか、または無意味な機能を繰り返し実行して、デバイスが通常の作業を行うのを防ぐように設計されている。基本的には、サービスを拒否したり、パフォーマンスを低下させたり、デバイスを完全に停止させたりする。これらの悪意のある感染は、本質的に破壊的であり、有害な目的、競合他社のビジネスにおいて通常の業務を行えなくする目的、または単純に可能であるかどうかを見たいと考えるハッカーの楽しみを動機として使用される。

【０１１５】

監視

【０１１６】

サイバー犯罪を超えた脅威と監視がある。そのような場合、私立探偵または知人を雇うかまたは強制して、音声の会話、データ交換、及び場所を監視するために、デバイスまたはプログラムをターゲットのパーソナルデバイスにインストールさせる。探偵は対象者がそれを知ることなくターゲットのデバイスに一時的にアクセスしなければならないので、捕まる危険性がより高い。例えば、ＳＩＭカードで、電話のネットワークアクセス特権をコピーすることができるが、同時にターゲットのコール及びデータトラヒックを監視するサイバー犯罪者に情報を送信させるものが市販されている。

【０１１７】

他の形式の監視には、カジノにあるものと同様に、人の行動や電話を監視する秘密のビデオカメラの使用が含まれる。ビデオ監視により、デバイスのパスワードすなわちＰＩＮは、ログインプロセス中にユーザのキーストロークを観察するだけで学習できる。十分なカメラがあれば、最終的にログインプロセスが記録される。疑いを起こさせずにカメラネットワークにアクセスするためには、サイバーパイレーツが建物、店舗、または通りにある既存のカメラ監視システムをハックし、他人のネットワークモニタへのアクセスを介して疑いをもたない犠牲者の行動を監視することができる。ビデオ監視とパケットスニッフィングを組み合わせることで、その後サイバー攻撃を開始するためのさらに包括的なデータセットが得られる。

【０１１８】

サイバーパイレーツによる管理（侵入）

【０１１９】

サイバーパイレーツが情報を得ることのできるもう１つの手段は、ハッキングし、デバイス、サーバ、またはネットワークのシステム管理権限にアクセスすることである。従って、システム管理者のログインをハッキングすることによって、あるユーザのアカウントに無許可でアクセスするのではなく、システムを使用しているユーザに知られずに、重要なアクセスと特権がサイバーパイレーツに利用可能になる。システム管理者はシステムの警察として働くので、その犯罪活動を把握できる者はいない。本質的には、腐敗した管理システムやネットワークでは、警察の取り締まりできる者がいない。

【０１２０】

結論

【０１２１】

インターネット、パケット交換ネットワーク、７層のオープンソースイニシアチブネットワークモデルの普遍的な採用による普遍性と相互運用性は、過去２０年にわたり、世界規模の通信が比類のない規模で拡大し、スマートフォンからタブレット、コンピュータ、スマートテレビ、車、さらには家電製品や電球に至るまで幅広く使用されることを可能にした。イーサネット（登録商標）、セルラー、ＷｉＦｉ、及びケーブルテレビの接続の基礎となるインターネットプロトコルすなわちＩＰの世界的な採用は、統一された通信が得

られただけでなく、できる限り多くのデバイスやシステムに侵入しようとするハッカーやサイバー犯罪者の課題を大幅に簡素化した。今日の通信ネットワークを攻撃するために利用可能なソフトウェアとハードウェアの方法が大量にあることを考えると、唯一の防御として単一のセキュリティ方法を用いるのは十分ではない。代わりに、高度なサイバー攻撃からの保護を確実にするために、全てのデバイス、ラストリンク、ローカルの電話／ネットワーク、及びクラウドネットワークを保護する体系的なアプローチが必要である。利用される方法は、ＱｏＳ、ネットワークレイテンシー、ビデオまたは音質を犠牲にすることなく、本質的なサイバーセキュリティとサイバープライバシーを提供するものでなければならない。暗号化は安全な通信とデータストレージでこの次世代を開発する上で重要な要素であるべきであるが、ネットワークのセキュリティは暗号化の方法論にのみ依存してはならない。

【発明の概要】

【課題を解決するための手段】

【０１２２】

本発明によれば、データ（広義には、テキスト、音声、映像、グラフィック、及び他の全ての種類のデジタル情報またはファイル）は、セキュア動的通信ネットワーク及びプロトコル（ＳＤＮＰ）ネットワークまたは「クラウド」を通じて伝送される。ＳＤＮＰクラウドは、世界中のあらゆる場所に配置されたサーバ、あるいは他の種類のコンピュータまたはデジタル装置（本明細書中では「サーバ」と総称する）にホストされた複数の「ノード」（「メディアノード」と呼ばれる場合もある）を含む。２以上のノードを、単一のサーバ上に配置することも可能である。一般的に、データは、メディアノード間で、光ファイバケーブルを通じて伝送される光、無線またはマイクロ波スペクトルの無線波、銅ワイヤまたは同軸ケーブルにより伝送される電気信号、あるいは衛星通信により伝送されるが、本発明は、デジタルデータをある地点から他の地点に伝送することができる任意の手段を幅広く含む。本発明に係るＳＤＮＰネットワークは、ＳＤＮＰクラウド、並びに、ＳＤＮＰクラウド及びクライアントデバイス間の「ラストマイル」リンクを含む。上記のクライアントデバイスとしては、例えば、セルフォン（スマートフォン）、タブレット、ノート型コンピュータ、デスクトップ（デスクトップ型コンピュータ）、モバイル電子機器、ＩｏＴ（Ｉｎｔｅｒｎｅｔ－ｏｆ－Ｔｈｉｎｇｓ）デバイスまたはアプリケーション、自動車または他の車両が挙げられる。ラストマイル通信はまた、セルフォン通信塔、家庭に接続されるケーブルまたはファイバ、及び公衆ＷｉＦｉルータを含む。ラストマイルでは、クライアントのデバイスと最も近いセルフォン通信塔又は他の再送信機の間のリンクを「ラストリンク」と呼ぶ。

【０１２３】

ＳＤＮＰクラウド内のメディアノード間で通信するときは、データは、固定長または可変長のデジタルビット列である「パケット」の形態で伝送され、スクランブル化、暗号化、分割、またはそれらと逆の処理であるアンスクランブル化、復号、混合などの技術を用いて偽装される。（注意：本明細書では、「または（ｏｒ）」は、文脈上他の意味を有する場合を除き、その接続詞的な意味（及び／または（ａｎｄ／ｏｒ））で使用される。）

【０１２４】

スクランブル化は、データパケット内のデータの配列順番を変更する。例えば、データパケット内にその順番に配列されたデータセグメントＡ、Ｂ、及びＣを、データセグメントＣ、Ａ、及びＢの順番に並べ替える。スクランブル化操作と逆の操作は、「アンスクランブル化」と呼ばれる。アンスクランブル化は、パケット内のデータの配列順番を元の配列順番（上記の例では、Ａ、Ｂ、Ｃの順番）に戻す。データパケットのアンスクランブル化操作と、それに続くスクランブル化操作との組み合わせを、「再スクランブル化」と称する。スクランブル化されたパケットを再スクランブル化するときは、パケットは、前回のスクランブル化操作のときと同一または異なる方法でスクランブル化される。

【０１２５】

第２の操作の「暗号化」は、パケット内のデータを、送信者及び他の認可された者、並

びに暗号化と逆の操作である「復号」を実施する者のみに理解可能なサイファテキストと呼ばれる形態に符号化することである。サイファテキストデータパケットの復号操作と、それに続く再度の暗号化操作との組み合わせを、本明細書中では「再暗号化」と称する。この再暗号化での暗号化操作は、一般的に、ただし必須ではないが、前回の暗号化のときと異なる方法を用いる。

【０１２６】

第３の操作の「分割」は、その名称が示すように、パケットを２以上のより小さなパケットに分割することを含む。分割と逆の操作である「混合」は、２以上の分割されたパケットを再結合して、元の単一のパケットに戻すことと定義される。以前に分割及び混合されたパケットの分割は、前回の分割操作のときと同一または異なる方法で行われる。分割操作及び混合操作の順番は可逆的であり、分割は混合によって元に戻すことができる。またその逆に、複数の入力を混合した出力は、分割することによってその構成要素（複数の入力）に戻すことができる。（注意：スクランブル化及びアンスクランブル化、暗号化及び復号、並びに分割及び混合は、互いに逆の処理なので、ある処理を実施するのに使用されるアルゴリズムまたは方法の情報は全て、それと逆の処理を実施するのに必要とされる。したがって、特定のスクランブル化、暗号化、または分割アルゴリズムについて言及するときは、そのアルゴリズムの情報により、それと逆の処理の実施が可能となることを理解されたい。）

【０１２７】

本発明によれば、ＳＤＮＰクラウドを通過するデータパケットは、スクランブル化または暗号化されるか、あるいはスクランブル化または暗号化の一方または両方と分割との組み合わせが施される。加えて、パケットを解読者にとってより複雑にするために、またはパケットを所定の長さにするために、「ジャンク（意味を持たない）」データがパケットに追加される。さらに、パケットは、パースされる、すなわち個別の部分（断片）に分割される。コンピュータ用語では、パース（ｐａｒｓｅ）は、コンピュータ言語の命令文、コンピュータ命令、またはデータファイルを、コンピュータにとって有用な複数の部分に分割することを意味する。パースはまた、命令またはデータパケットの目的を不明にするか、またはデータを特定のデータ長さを有するデータパケットに分割するのに用いられる。

【０１２８】

データパケットのフォーマットはインターネットプロトコルに従うが、ＳＤＮＰ内のクラウドでは、メディアノードのアドレスは、標準的なインターネットアドレスではない。すなわち、メディアノードのアドレスは、インターネットＤＳＮサーバによって識別することはできない。したがって、メディアノードは、インターネットを介してデータパケットを技術的には受信できるが、アドレスの認識または問い合わせに対しては応答できない。さらに、インターネットのユーザは、たとえメディアノードにコンタクトできたしても、メディアノードからは、該ノードへのアクセスに必要な識別認証情報を有していない偽者と認識されるので、メディアノード内のデータにアクセス及び分析することはできない。具体的には、メディアノードが、ＳＤＮＰネームサーバまたはそれと同等の機能を有するデバイス内の指定サーバ上で実行される有効なＳＤＮＰノードとして登録されていない限り、該ノードから他のＳＤＮＰメディアノードに送信されたデータパケットは、無視され廃棄されることとなる。同様に、ＳＤＮＰネームサーバに登録されたクライアントのみが、ＳＤＮＰメディアノードにコンタクトすることができる。登録されていないサーバと同様に、登録されたＳＤＮＰクライアント以外のソースから受信したデータパケットは、無視され、即座に廃棄される。

【０１２９】

「単一ルート」と呼ばれる比較的単純な実施形態では、データパケットは、ＳＤＮＰクラウド内の一連のメディアノードを介した単一ルートを通じて伝送され、クラウドに入るときに通るメディアノードでスクランブル化され、クラウドから出るときに通るメディアノードでアンスクランブル化される（この２つのノードは、「ゲートウェイノード」または「ゲートウェイメディアノード」と呼ばれる）。若干より複雑な実施形態では、パケッ

トは、各メディアノードで、前のメディアノードで使用されたものとは異なるスクランブル化方法を用いて再スクランブル化される。別の実施形態では、パケットは、クラウドに入るときに通るゲートウェイノードで暗号化、クラウドから出るときに通るゲートウェイノードで復号される。また、これに加えて、パケットは、クラウド内で通る各メディアノードで再暗号化してもよい。所与のノードは、パケットをスクランブル化または暗号化するときに毎回同一のアルゴリズムを使用するので、この実施形態は、「静的」なスクランブル化または暗号化と称する。

【０１３０】

パケットに２以上の操作（例えば、スクランブル化及び暗号化）を施す場合、それらと逆の操作は、元の操作の実施順と逆の順番で実施することが好ましい。例えば、パケットがスクランブル化された後に暗号化され、メディアノードから送信される場合、次のメディアノードに到着したパケットは、復号された後にアンスクランブル化される。パケットは、メディアノード内に存在するときにのみ、その元の形態に再生成される。パケットは、メディアノード間で伝送されるときは、スクランブル化、分割／混合、または暗号化されている。

【０１３１】

「マルチルート」データ伝送と呼ばれる別の実施形態では、パケットは、ゲートウェイノードで分割され、これにより生成された複数のパケットが、ゲートウェイノード以外はメディアノードを共有しない一連の「並列」な経路を通ってクラウドを横断する。複数のパケットはその後（一般的には出口のゲートウェイノードで）混合され、これにより元のパケットが再生成される。したがって、たとえハッカーが単一パケットの意味を理解できたとしても、ハッカーは、メッセージ全体の一部しか得ることはできない。また、パケットは、分割の前または後に、ゲートウェイノードでスクランブル化及び暗号化されてもよい。また、複数のパケットは、それが通過する各メディアノードにおいて、再スクランブル化または再暗号化されてもよい。

【０１３２】

さらなる別の実施形態では、パケットは、ＳＤＮＰクラウド内の単一ルートまたは一連の並列経路だけを通じてではなく、互いに交差する部分を多数含む複数の経路を通じて伝送される。この実施形態は、可能性がある経路のイメージがメッシュに似ているので、「メッシュ伝送」と称される。上述した実施形態と同様に、パケットは、ＳＤＮＰクラウド内の各メディアノードを通過するときに、スクランブル化、暗号化、及び分割／混合される。

【０１３３】

パケットがＳＤＮＰネットワークを通るルートは、メディアノードセグメント自体、または好ましくは「デュアルチャンネル」または「トリチャンネル」実施形態では専用のシグナリングサーバ上で実行される別個のシグナリングノードにより実施されるシグナリング機能により決定される。このシグナリング機能は、各パケットが送信クライアントデバイス（例えばセルフォン）から送信されるときに、そのパケットのルートを、ネットワークの状況（例えば伝搬遅延）並びにその通信の優先度及び緊急性に基づいて決定する。そして、そのルート上の各メディアノードに、そのノードがパケットを受信する予定であることを通知すると共に、そのノードが受信したパケットの宛先を指示する。各パケットはタグにより識別され、シグナリング機能は、各メディアノードに、そのノードから送信される各パケットにどのタグを付与するかを指示する。一実施形態では、データタグは、各データのサブパケットに添付されサブパケットの識別に使用されるデータフィールドであるＳＤＮＰヘッダまたはサブヘッダに含められ、各サブパケットは、パケット内の特定のデータ「スロット」に格納された、１または複数のソースからのデータセグメントを含む。任意の２つのメディアノード間でのデータ伝送中に、複数のサブパケットが、１つのより大きなデータパケット内に存在し得る。

【０１３４】

ルーティング機能は、分割及び混合機能と連携して行われる。パケットが分割された場

合には、各サブパケットのルートを決定すると共に、サブパケットが再結合（混合）されるノードに対してそのサブパケットを混合するように命令する必要があるためである。マルチルート実施形態では、ＳＤＮＰネットワークを横断して出口ゲートウェイノードに到着するまでに、パケットの分割及び混合は１回または複数回行われる。パケットを分割するノードとそのパケットを分割して生成するサブパケットの数の決定、及びそのサブパケットの伝送ルートとそのサブパケットを混合して元のパケットを再生成するノードの決定は全て、該シグナリング機能が別個のシグナリングサーバにより実施されるか否かに関わらず、シグナリング機能により制御される。分割アルゴリズムは、分割されるデータパケットのデータセグメントについて、各サブパケット内に含めるデータセグメント、並びにサブパケット内での各データセグメントの順番及び位置を指定する。混合アルゴリズムは、サブパケットを混合するノードにおいて、分割のときと逆の処理を実施して元のパケットを再生成する。当然ながら、シグナリング機能により再分割の命令を受けた場合、そのノードは、その分割処理を実施するときの時間及びステートに対応する、前の分割のときと別個の分割アルゴリズムに従ってパケットを再度分割する。

【０１３５】

シグナリング機能により、メディアノードが、複数のパケットを、それが分割されたパケット（サブパケット）であるかまたは互いに異なるメッセージに関連するかに関わらず、ネットワークを通じて「次のホップ」上の特定の宛先メディアノードに送信するように命令された場合、とりわけ、複数のサブパケットが次のホップのための共通の宛先メディアノードを共有する場合には、そのメディアノードは、その複数のパケットを結合して単一の大きなパケットを生成する（郵便局において、宛先が同一の複数の手紙を１つの箱に入れ、その箱をその宛先に送ることに似ている）。

【０１３６】

本発明の「動的」な実施形態では、ＳＤＮＰクラウド内の各メディアノードは、それを通る一連のパケットに対して、同一のスクランブル化、暗号化、または分割アルゴリズムまたは方法を使用しない。例えば、所与のメディアノードでは、あるパケットに対しては、特定のスクランブル化、暗号化、または分割アルゴリズムを使用してスクランブル化、暗号化、または分割を行い、その次のパケットに対しては、前回のとは別個のスクランブル化、暗号化、または分割アルゴリズムを使用してスクランブル化、暗号化、または分割を行う。この「動的」な操作により、ハッカーがパケットの解読に使用できる時間が非常に短くなり（例えば１００ミリ秒）、また、たとえパケットの解読に成功してもその情報はすぐに使えなくなるので、ハッカーが直面する困難性を著しく高めることができる。

【０１３７】

動的な実施形態では、各メディアノードは、いわゆる「ＤＭＺサーバ」に接続されている。ＤＭＺサーバは、ノードにおけるデータ伝送部分とは別個の部分と見なすこともでき、メディアノードがそれから出力されるパケットに対して適用する可能性があるスクランブル化、暗号化、及び分割アルゴリズムのリストまたはテーブルを含むデータベース（「セレクタ」）を有する。セレクタは、メディアノードですら知らず、かつ全てのＤＭＺサーバが所与の時点で同一のセレクタを有しているために「共有秘密」と呼ばれる多数の情報の一部である。

【０１３８】

メディアノードは、スクランブル化されたパケットを受信したとき、動的な実施形態では、そのパケットのアンスクランブル化に使用するアルゴリズムを該ノードに知らせるのに使用される「シード」も受信する。シードは、それ自体は意味を持たない偽装した数値であるが、頻繁に変更されるステート（例えば、前のメディアノードでパケットをスクランブル化したときの時間）に基づいている。前のノードがパケットをスクランブル化したときに、該ノードに接続されたＤＭＺサーバは、そのときのステートに基づいてシードを生成する。当然ながら、ステートは、該ノードに接続されたＤＭＺサーバがパケットのスクランブル化に使用するアルゴリズムを選択するのにも使用される。選択されたアルゴリズムは、送信側ノードに、そのパケットのスクランブル化方法に関する命令の形態で伝達

される。したがって、送信側ノードは、パケットのスクランブル化方法の命令と、次のメディアノードに伝送されるシードとの両方を受信する。ＤＭＺサーバ内で動作するシード生成器は、その処理が実施される時間でのステートに基づくアルゴリズムを使用してシードを生成する。シード生成器及びそのアルゴリズムは、メディアノードの共有秘密の一部であるが、生成されたシードは、秘密情報ではない。アルゴリズムにアクセスしない限り、数値シードは意味を持たないからである。

【０１３９】

したがって、パケットルート上の次のメディアノードは、スクランブル化されたパケットと、そのパケットに関連するステート（例えば、そのパケットがスクランブル化された時間）に由来するシードとを受信する。シードは、そのパケット自体に含めてもよいし、そのパケットが受信側ノードに送信される前に、そのパケットと同一のルートまたは別のルート（例えばシグナリングサーバ）を介して送信してもよい。

【０１４０】

シードの受信方法に関わらず、受信側ノードは、受信したシードをそれに接続されたＤＭＺサーバに送信する。ＤＭＺサーバは、共有秘密の一部であるスクランブル化アルゴリズムのセレクタまたはテーブルを有しているので、送信側ノードのＤＭＺサーバのセレクタと同様に、シードを使用して、パケットのスクランブル化に使用されたアルゴリズムを識別すると共に、受信側ノードにパケットのアンスクランブル化方法を指示することができる。したがって、受信側ノードは、スクランブル化されていない形態のパケットを再生成し、元のデータを復元することができる。一般的に、パケットは、次のノードに送信される前に、別のスクランブル化アルゴリズムに従って再びスクランブル化されることとなる。この場合、受信側ノードは、そのＤＭＺサーバからスクランブル化アルゴリズム及びシードを取得して、上記のプロセスを繰り返す。

【０１４１】

したがって、パケットは、ＳＤＮＰネットワークを通じて伝送されるに従って、各ノードで別個のスクランブル化アルゴリズムに従ってスクランブル化される。また、それと共に、各ノードにおいて、次のノードがそのパケットをアンスクランブル化することを可能にする新しいシードが生成される。

【０１４２】

本発明の別の実施形態では、実際のステート（例えば時間）が、ノード間で伝送される（すなわち、送信側ノードは受信側ノードにシードを送信する必要がない）。送信側メディアノードと受信側メディアノードとの両方に接続されたＤＭＺサーバは、任意の時点での識別アルゴリズムを含む隠し数字生成器（これも、共有秘密の一部である）を含む。送信側ノードに接続されたＤＭＺサーバは、可能性があるスクランブル化アルゴリズムのセレクタまたはテーブルからスクランブル化アルゴリズムを決定するための隠し数字を、ステートを使用して生成する。送信側ノードは、ステートを受信側ノードに送信する。シードとは異なり、隠し数字は、ネットワークを通じて送信されず、メディアノードとそのＤＭＺサーバとの間のプライベート通信を通じて送信される。受信側メディアノードが、入力データパケットに関するステートを受信したとき、該ノードに接続されたＤＭＺサーバ内の隠し数字生成器は、そのステートを使用して、同一の隠し数字を生成する。生成された数字は、セレクタまたはテーブルが、パケットのアンスクランブル化に使用するアルゴリズムを決定するのに使用される。ステートは、パケットに含めて伝送してもよいし、パケットを送信する前に、パケットの送信ルートと同一または別のルートを通じて送信側ノードから受信側ノードに伝送してもよい。

【０１４３】

動的暗号化及び分割に使用される技術は、動的スクランブル化に使用されたものと同様であるが、動的暗号化では、「鍵」がシードに追加して使用される。ＤＭＺサーバにより保持された共有秘密は、暗号化及び分割アルゴリズムのセレクタまたはテーブルと、鍵生成器とを含む。対称鍵暗号化の場合、送信側ノードは、受信側ノードに、該ノードのＤＭＺサーバで、パケットの暗号化に使用されたアルゴリズムを識別し、それによりファイル

を復号するのに使用される鍵を送信する。非対称鍵暗号化の場合、メディアノードは、情報を要求する。すなわち、まず、受信側ノードが、暗号化鍵を、送信されるデータパケットを含んでいる送信側ノードに送信する。そして、送信側メディアノードは、受信した暗号化鍵に従ってデータを暗号化する。暗号化鍵を生成する受信側メディアノードのみが、その暗号化鍵に対応する復号鍵を有しているので、その暗号化鍵を使用して生成されたサイファテキストを復号することができる。重要なことには、非対称暗号化では、暗号化に使用される暗号化鍵にアクセスしても、データパケットの復号方法に関する情報は得られない。

【０１４４】

分割の場合は、パケットを分割してサブパケットを生成したメディアノードから、そのサブパケットを混合するメディアノードにシードが送信される。この混合ノードに接続されたＤＭＺサーバは、受信したシードを使用して、分割アルゴリズム、すなわちサブパケットの混合に使用するアルゴリズムを決定する。

【０１４５】

上述したように、デュアルまたはトリチャンネル実施形態では、シグナリング機能は、シグナリングサーバと呼ばれる別個のサーバ群上で動作するシグナリングノードにより実施される。このような実施形態では、シード及び鍵は、送信側メディアノードから受信側メディアノードに直接送信されるのではなく、シグナリングサーバを介して送信される。したがって、送信側メディアノードは、シードまたは鍵をシグナリングサーバに送信する。上述したように、シグナリングサーバは、パケットのルートの決定に対して責任を負うので、シグナリングサーバは、各パケットが送信される次のメディアノードを知っている。

【０１４６】

ハッカーによるハッキングをより困難にするために、セレクタ内の可能性があるスクランブル化、分割、暗号化方法のリストまたはテーブルは、特定のシードまたは鍵に対応する方法が変更されるように、定期的に（例えば毎時間または毎日）シャッフルされる。したがって、所与のメディアノードにおいて、日１の時間ｔ１で生成されたパケットに対して使用される暗号化アルゴリズムは、日２の同じ時間ｔ１で生成されたパケットに対して使用される暗号化アルゴリズムとは異なり得る。

【０１４７】

各ＤＭＺサーバは、一般的に、同一の「サーバファーム」内の１または複数のメディアノードと物理的に接続されている。上述したように、メディアノードは、それに接続されたＤＭＺサーバに（例えば、そのパケットが生成された時間またはステートに基づく）シードまたは鍵を提供することにより、該ノードが受信したパケットに対して行う操作に関する指示（命令）を要求するが、メディアノードは、ＤＭＺサーバ内の共有秘密または他の任意のデータまたはコードにはアクセスできない。ＤＭＺサーバは、メディアノードからの要求に応答し、シードまたは鍵を使用して、メディアノードがパケットのアンスクランブル化、復号、または混合に使用するべき方法を決定する。例えば、パケットがスクランブル化されており、メディアノードがそれをアンスクランブル化する方法を知りたい場合、ＤＭＺサーバは、スクランブル化アルゴリズムのリスト（またはセレクタ）を検索して、シードに対応する特定のアルゴリズムを見つける。ＤＭＺサーバはその後、見つけたアルゴリズムに従ってパケットをアンスクランブル化するように、メディアノードに命令する。要するに、メディアノードは、シードまたは鍵に具現化された問い合わせをＤＭＺサーバに送信し、ＤＭＺサーバは、その問い合わせに応答してメディアノードに命令を送信する。

【０１４８】

メディアノード（ＤＮＳにより認識されるＩＰアドレスを有していないのにも関わらず）は、インターネットを介してアクセス可能であるが、ＤＭＺサーバは、メディアサーバに接続されたネットワークに対してワイヤまたは光ファイバを介したローカルネットワーク接続のみを有するインターネットからは完全に分離される。

【０１４９】

「単一チャンネル」の実施形態では、シード及び鍵は、送信側メディアノード及び受信側メディアノード間でデータパケット自体の一部として送信されるか、またはデータパケットの送信前に、データパケットの送信ルートと同一のルートを使用して、別個のパケットに含めて送信される。例えば、パケットを暗号化するときは、メディアノード＃１は、暗号化を実施したときの時間に基づく暗号化鍵をパケット内に含める。そして、暗号化鍵を含むパケットがメディアノード＃２に到着すると、メディアノード＃２は、該ノードに接続されたＤＭＺサーバに暗号化鍵を送信する。そして、ＤＭＺサーバは、受信した鍵を使用して、パケットを復号するための復号方法をセレクタから選択する。メディアノード＃２はその後、パケットをメディアノード＃３に送信する前に、ＤＭＺサーバにパケットの再暗号化方法を問い合わせる。繰り返すが、ＤＭＺサーバは、セレクタにより選択された暗号化方法をメディアノード＃２に知らせると共に、選択された暗号化方法に対応するステートを反映した鍵をメディアノード＃２に送信する。メディアノード＃２は、暗号化を実施し、暗号化されたパケット及び鍵を（個別にまたはパケットの一部として）メディアノード＃３に送信する。鍵はその後、同様の態様で、メディアノード＃３により、パケットを復号するのに使用される。この結果、ハッカーがパケットの解読に使用できる、単一の静的復号方法は存在しない。

【０１５０】

上記の例で、時間、すなわち動的な「ステート」状態を、シードまたは鍵に具現化される、スクランブル化、暗号化、または分割方法の決定因子として使用することは、一例にすぎない。任意の可変パラメータ、例えばパケットが通過したノードの数も、使用される特定のスクランブル化、暗号化、または分割方法を選択するためのシードまたは鍵についての「ステート」として使用することができる。

【０１５１】

「デュアルチャンネル」の実施形態では、シード及び鍵は、メディアノード間で直接的に送信されるのではなく、シグナリングサーバから構成されている第２の「命令及び制御」チャンネルを介してメディアノード間で伝送される。シグナリングノードはまた、メディアノードに、ルーティング情報を提供すると共に、パケットのルート上のメディアノードに、そのパケットの分割方法及び他のパケットとの混合方法を知らせる。また、シグナリングノードは、各メディアノードに対して、該ノードの次のメディアノードがそのパケットを認識することができるように、該ノードから送信される各パケットに識別「タグ」を付与するように命令する。シグナリングサーバは、所与のメディアノードに対して、該ノードにパケットを送信したメディアノードと、該ノードから送信されたパケットを受信するメディアノードとのみを知らせることが好ましい。これにより、どのメディアノードも、ＳＤＮＰクラウド内でのパケット伝送ルートの全体を知らない。いくつかの実施形態では、ルーティング機能は、２以上のシグナリングサーバで分割して行ってもよい。例えば、第１のシグナリングサーバで、特定のメディアノードへのルートを決定し、第２のシグナリングサーバで、その特定のメディアノードから別のメディアノードへのルートを決定し、このような処理を出口ゲートウェイノードまで続ける。これにより、どのシグナリングサーバも、データパケットのルーティングの全体を知らない。

【０１５２】

「トリチャンネル」の実施形態では、「ネームサーバ」と呼ばれる第３のサーバ群を使用して、ＳＤＮＰクラウド内の構成要素を識別し、ＳＤＮＰクラウドに接続されたデバイスの識別子及びそれに対応するＩＰまたはＳＤＮＰアドレスに関する情報を保存する。加えて、ネームサーバは、ＳＤＮＰクラウド内のメディアノードを頻繁にモニタし、例えば、アクティブなメディアノードの現在のリスト、及びクラウド内のメディアノードの全ての組み合わせについての伝搬遅延のテーブルを維持する。通信が開始される第１のステップでは、クライアントデバイス（例えばタブレット）は、ＩＰパケットをネームサーバに送信し、データ宛先または着呼者のアドレスまたは他の情報を要求する。さらに、デバイスがクラウドに最初に接続、すなわち登録されるときの最初のコンタクトとしての役割を果たすために、別個の専用ネームサーバが使用される。

【０１５３】
追加的な有益なセキュリティとして、互いに異なるセレクタ、シード及び鍵生成器、並びに他の共有秘密を有する個別のセキュリティ「ゾーン」が、単一のＳＤＮＰクラウド内に設けられる。互いに隣接するゾーンは、両ゾーンの共有秘密を保持し、一方のゾーンのルールに従うデータフォーマットを、他方のゾーンのルールに従うデータフォーマットに変換する能力を有するブリッジメディアノードにより接続される。
【０１５４】
同様に、例えば互いに異なるサービスプロバイダによりホストされた互いに異なるＳＤＮＰクラウド間の通信では、各クラウドのインターフェイスブリッジサーバ間に、全二重（すなわち双方向）通信リンクが形成される。各インターフェイスブリッジサーバは、各クラウドについての関連共有秘密及び他のセキュリティ情報にアクセスすることができる。
【０１５５】
本発明の重要な利点は、ＳＤＮＰネットワーク内に単一の制御ポイントが存在せず、ネットワーク内のどのノードまたはサーバも、ある通信がどのように行われ、どのように動的に変化するかについての完全な情報を持たないことである。
【０１５６】
例えば、シグナリングサーバ上で実行されるシグナリングノードは、通信が行われるルート（または、場合によっては、ルートの一部だけ）を知っているが、通信されるデータコンテンツにアクセスすることや、本当の発呼者またはクライアントを知ることはできない。さらに、シグナリングノードは、メディアノードのＤＭＺサーバ内の共有秘密にアクセスすることはできない。そのため、シグナリングノードは、送信中のデータパケットがどのように暗号化、スクランブル化、分割、または混合されたかを知ることはできない。
【０１５７】
ＳＤＮＰネームサーバは、発呼者の本当の電話番号またはＩＰアドレスを知っているが、通信中のデータまたは様々なパケット及びサブパケットのルーティングに対してアクセスすることはできない。シグナリングノードと同様に、ネームサーバは、共有秘密にアクセスすることはできない。したがって、ネームサーバは、送信中のデータパケットがどのように暗号化、スクランブル化、分割、または混合されたかを知ることはできない。
【０１５８】
メディアコンテンツを実際に伝送するＳＤＮＰメディアノードは、発呼者が誰であるか全く分からないし、様々な断片化されたサブパケットがＳＤＮＰクラウド内を伝送されるルートを知ることもできない。実際、各メディアノードは、該ノードに到着する予定のデータパケット（そのタグまたはヘッダにより識別される）と、そのデータパケットを次にどこに送信するか（すなわち、「次のホップ」）しか知らない。つまり、各メディアノードは、データがどのようにして暗号化、スクランブル化、混合、または分割されたか、または、ステート、数値シード、または鍵を使用して、そのファイルを復元するアルゴリズムをどのようにして選択するかは知らない。入力データパケットのデータセグメントを正しく処理するのに必要な情報は、ＤＭＺサーバだけが知っている。つまり、ＤＭＺサーバだけが、それの共有秘密、すなわちネットワークを通じてまたはメディアノード自体がアクセスできないアルゴリズムを使用して、正しい処理を行うことができる。
【０１５９】
本発明の別の発明的な側面は、ネットワーク遅延を減少させ、伝搬遅延を最小限に抑えることにより、優れたクオリティ・オブ・サービス（ＱｏＳ）を提供すること、並びに、データパケットのサイズを制御することにより、すなわち、単一の高帯域接続に依存するのではなく、クラウドを通じてより小さなデータパケットを並列に送信することにより、エコー及び通話切断を解消することである。ＳＤＮＰネットワークの動的ルーティングは、ネットワークのノードツーノード伝搬遅延の情報を使用して、ある通信についてのその時点での最良のルートを動的に選択する。別の実施形態では、優先度の高いクライアントのために、ネットワークは、レースルーティングを容易にし、複製のメッセージ断片化された形態でＳＤＮＰクラウドを通じて送信し、最も早いデータだけを選択して元の音声ま

たはデータコンテンツに復元することができる。

【０１６０】

本発明に係るＳＤＮＰシステムの様々な利点の中でも、並列及び「メッシュ伝送」実施形態では、パケットはＳＤＮＰクラウド内を伝送されるときに断片化され、それにより、たとえハッカーが個々のサブパケットまたはサブパケット群を解読できたとしても、ハッカーがメッセージを理解することを防止する。そして、「動的な」実施形態では、パケットに適用されるスクランブル化、暗号化、及び分割方法は、頻繁に変更されるので、ハッカーが、ある時点でパケットを連続的に解読することはできない。本発明の実施形態の様々な別の利点は、下記の説明を読むことにより、当業者には容易に明らかになるであろう。

【０１６１】

一般的に、同様のセキュリティ技術が、ＳＤＮＰクラウドとクライアントデバイス（例えばセルフォン、タブレット）との間の「ラストマイル」に適用され得る。クライアントデバイスは、通常、クラウドから離れたセキュリティゾーンに位置するため、まずは、認証ＳＤＮＰクライアントにする必要がある。このステップは、一般的にはＳＤＮＰ管理サーバからのダウンロードにより、クライアントデバイスに、そのデバイスのセキュリティゾーンに特有のソフトウェアパッケージをインストールすることを含む。クライアントデバイスは、クラウド内のゲートウェイメディアノード（時にはゲートウェイとして呼ばれる。）を介して、ＳＤＮＰクラウドにリンクされる。このゲートウェイメディアノードは、クラウド及びクライアントデバイスのセキュリティゾーンの両方に関する共有秘密にアクセスすることができる。しかし、クライアントデバイスは、ＳＤＮＰクラウドに関する共有秘密にアクセスすることはできない。セキュリティレベルを高めるために、クライアントサーバ間で、シグナリングサーバを介して、シード及び鍵が直接的に送信される。したがって、送信側クライアントデバイスは、シード及び／または鍵を受信側クライアントデバイスに直接的に送信する。このような実施形態では、受信側クライアントデバイスが受信したパケットは、送信側クライアントデバイスから送信されたパケットと同一のスクランブル化または暗号化形式を有する。そのため、受信側クライアントデバイスは、送信側クライアントデバイスから受信したシード及び鍵を使用して、パケットのアンスクランブル化または復号を行うことができる。クライアントデバイス間でのシード及び鍵の直接的な送信は、ＳＤＮＰネットワーク自体の動的スクランブル化及び暗号化に加えて行われ、これにより、ネスト化セキュリティと呼ばれる高レベルのセキュリティを提供することができる。

【０１６２】

加えて、クライアントデバイスまたはそれと通信するゲートウェイノードは、データ種類が互いに同一のパケット（例えば、音声パケット、テキストメッセージファイル、ドキュメント、１つのソフトウェア）、またはデータ種類が互いに異なるパケット（例えば、音声パケットとテキストファイル、テキストパケットと動画または写真画像）を、そのパケットがＳＤＮＰネットワークに到着する前に混合し、出口ゲートウェイノードまたは宛先のクライアントは、混合されたパケットを分割して元のパケットを復元する。これは、ＳＤＮＰネットワークにおいて実施されるスクランブル化、暗号化、または分割に加えて行われる。このような場合、送信側クライアントデバイスは、受信側クライアントデバイスに、送信側クライアントデバイスまたはゲートウェイメディアノードで混合されたパケットを分割して元のパケットを再生成するためのパケットの分割方法を命令するシードを送信する。連続的な混合及び分割の実施は、線形順序の操作を含むか、または、クライアントがそれ自体のセキュリティ対策を実行し、かつＳＤＮＰもそれ自体のセキュリティ対策を実行するネスト化構造を用いる。

【０１６３】

ハッカーを更に混乱させるために、クライアントデバイスは、１回のコミュニケーションで、複数のパケット（又はサブパケット）を継続して異なったゲートウェイノードに送信し、又それらを異なった物理メディアリンク（セルラー、ＷｉＦｉ、イーサネット（登録商標）ケーブル）を介して送信する。このプロセスを、「マルチＰＨＹ」と呼ぶことも

ある。更に混乱させる為に、継続して送信されるパケットに異なった送信元アドレスを含め、ハッカーにより同じクライアントデバイスからパケットが送信されている事を発見されることを防止する。

【０１６４】

この発明は、電話会議に関しても進歩を成し遂げている。普通の電話会議では、パケットは全ての参加者に送られるが、この発明によると、何人かの参加者をミュートされる事ができ、クライアントデバイス又は他のノードからミュートされるべき参加者に対してパケットの送信を防止する事により会議電話から外される。本発明の別の実施形態では、データパケットがブロードキャストで全ての参加者に送られるが、異なった暗号方法を用いてそれを実施する。普通の会議電話では、データパケットは暗号化して全ての参加者に送られるが、それにより全ての参加者に復号鍵のコピーが送られてしまう。プライベートモード又はミュートモードでは、データパケットは、異なった暗号方法を用いて複数のユーザに送られ、選択されたユーザだけに復号鍵を送る事ができる。

【０１６５】

ＳＤＮＰネットワーク及びプロトコルを用いた通信で使われるセキュリティの仕組みは、ファイルとデータ保管のセキュリティにも適合である。ＳＤＮＰネットワークを介する通信は、典型的に、１つのクライアントデバイスから他のクライアントデバイスに、スクランブル化及び暗号化されたデータ、また、匿名の断片化されたデータの伝送を行うが、ファイルとデータの保管も、途中で通信を止め、クライアントデバイスが受信する事を希望するまで、１つか複数のバッファにファイルやデータを保管する事ができる。この分散化されたデータの保管を、ここで、時に非集約型データストレージを呼ぶ。

【図面の簡単な説明】

【０１６６】

以下に列記する図面において、同様の構成要素には概ね同様の参照符合が付されている。しかし、ある参照符合が付されたそれぞれの構成要素が、必ずしも同じ参照番号を有する別の構成要素と完全に同一であるとは限らないことに留意されたい。例えば、特定の参照符合が付された暗号化操作は、必ずしも同じ参照符合が付された別の暗号化操作と同一である必要はない。また、単一の参照符合によって集合的に特定されるネットワーク内のサーバなどの構成要素のグループは、必ずしも互いに同一である必要はない。

【図１】従来のネットワークを介するパケット転送を示す概略図

【図２Ａ】パケットスクランブル化プロセスを示す概略図

【図２Ｂ】パケットアンスクランブル化プロセスを示す概略図

【図２Ｃ】様々なパケットスクランブル化アルゴリズムを示す概略図

【図２Ｄ】静的パラメトリックパケットスクランブル化を示す概略図

【図２Ｅ】隠し数字を用いた動的スクランブル化を示す概略図

【図３】パケット再スクランブル化プロセスを示す概略図

【図４Ａ】パケット暗号化プロセスを示す概略図

【図４Ｂ】パケット復号プロセスを示す概略図

【図５】暗号化スクランブル化プロセスとそれと逆の処理を示す概略図

【図６】再スクランブル化・再暗号化を含むＤＵＳＥ再パケット化のプロセスを示す概略図

【図７Ａ】固定長パケットの分割プロセスを示す概略図

【図７Ｂ】固定長パケットの混合プロセスを示す概略図

【図８】様々なパケット混合方法を示す概略図

【図９Ａ】ＳＤＮＰのセキュリティ機能及び逆機能を示す概略図

【図９Ｂ】単一ルートのラストマイル通信の発着信データパケットに対するＳＤＮＰセキュリティ操作を示すブロック図

【図９Ｃ】マルチルートのラストマイル通信の発着信データパケットに対するＳＤＮＰセキュリティ操作を示すブロック図

【図９Ｄ】ＳＤＮＰクライアントデバイスにおけるオーディオ、ビデオ、テキスト、及びファイルコンテンツの作成、データパケットの準備、データパケットの認識、及びコンテ

ンツの再生を示すブロック図
【図９Ｅ】７層ＯＳＩモデルを用いた階層データのカプセル化を説明するＳＤＮＰデータパケットの解説図
【図９Ｆ】ＳＤＮＰペイロードの解説図表
【図９Ｇ】トライチャネル通信を使用するＳＤＮＰゲートウェイにおけるインバウンドのラストマイルデータパケット処理を示すブロック図
【図９Ｈ】単一チャネル通信を使用するＳＤＮＰゲートウェイにおけるインバウンドのラストマイルデータパケット処理を示すブロック図
【図９Ｉ】トライチャネル通信を使用するＳＤＮＰゲートウェイにおけるアウトバウンドのラストマイルデータパケット処理を示すブロック図
【図１０】ＳＤＮＰクラウドの概略図
【図１１】ＩＤ確認を伴わない安全でないラストマイル通信の例
【図１２】発信者のＩＤ検証を伴わない従来の電話システム（ＰＯＴＳ）を介した安全でないラストマイル通信
【図１３】ＩＤ検証を伴うが安全でないラストマイル通信の例
【図１４】オペレータベースのＩＤ検証を用いたアナログ公共サービス電話網（ＰＳＴＮ）を介した安全でないラストマイル通信
【図１５】ログインベースまたはトークンベースのＩＤ検証を用いた有線デジタルネットワーク上の安全でないラストマイル通信
【図１６】ＰＩＮまたはクレジットカードベースのＩＤ検証を用いた有線アナログネットワーク上の安全でないラストマイル通信
【図１７】ＩＤ検証をサポートできるハイパーセキュアラストマイル通信の例の概略図
【図１８】ＷｉＦｉワイヤレスネットワークを介したＩＤ検証可能なハイパーセキュアラストマイル通信
【図１９】セルラー無線ネットワークを介したＩＤ検証可能なハイパーセキュアラストマイル通信
【図２０】イーサネット（登録商標）有線ネットワークを介したＩＤ検証可能なハイパーセキュアラストマイル通信
【図２１】ケーブルネットワークを介したＩＤ検証可能なハイパーセキュアラストマイル通信
【図２２】ケーブル有線とホームＷｉＦｉワイヤレスネットワークを組み合わせたＩＤ検証可能なハイパーセキュアラストマイル通信
【図２３】ＩＤでペアリングされたセキュアＬＡＮの最終リンクに接続されたＩＤ検証可能なハイパーセキュア通信区間を含むラストマイル通信例の概略図
【図２４】有線でＩＤペアリングされた安全なデバイス及びＩＤ不明の安全でないデバイスに接続されたＩＤ検証可能なハイパーセキュア有線通信区間を含むラストマイル通信
【図２５】ＷｉＦｉ　ＬＡＮにより自宅と職場用にＩＤペアリングされＷＰＡで保護されたコンピューティング及び通信デバイスに接続されたＩＤ検証可能なハイパーセキュア有線通信区間を含むラストマイル通信
【図２６】ＷｉＦｉ　ＬＡＮによってＩＤペアリングされＷＰＡで保護されたホームＩｏＴデバイスに接続されたＩＤ検証可能なハイパーセキュア有線通信区間を含むラストマイル通信
【図２７】イーサネット（登録商標）またはＷｉＦｉ　ＬＡＮで企業向けのＩＤペアリングされ、ＷＰＡで保護されたデバイスに接続されたＩＤ検証可能なハイパーセキュア有線通信区間を含むラストマイル通信
【図２８】ＩＤペアリングされた安全な有線または安全な無線ＬＡＮラストリンクに接続されたＩＤ検証可能なハイパーセキュア通信区間を含むラストマイル通信の例の概略図
【図２９Ａ】ストマイル通信に適用可能なイーサネット（登録商標）及びＷｉＦｉを含む有線及び無線のハイパーセキュアブリッジの概略図
【図２９Ｂ】ラストマイル通信に適用可能な衛星及び自動車ネットワークを利用する有線

及び無線のハイパーセキュアブリッジの概略図
【図２９Ｃ】ラストマイル通信に適用可能なケーブル及びセルラーネットワークを利用する有線及び無線のハイパーセキュアブリッジの概略図
【図３０】衛星電話、飛行機、列車、船舶、及び家庭用衛星受信機（セットトップボックス）を含む各種デバイスへの衛星アップリンク及びダウンリンクを介したＩＤ検証可能なハイパーセキュア無線通信を含むラストマイル通信
【図３１Ａ】衛星接続機能を備えた機内航空機通信ネットワーク内でのデバイス間のラストリンクハイパーセキュア通信の例
【図３１Ｂ】航空機用衛星通信及びアンテナモジュールの例
【図３２】複数の衛星接続チャネルを備えた船上海洋クルーズ船通信ネットワークにおけるデバイス間のラストリンクハイパーセキュア通信の例
【図３３】無線及び衛星接続機能を備えた車載列車通信ネットワークにおけるデバイス間のラストマイルハイパーセキュア通信の例
【図３４】セルラーラストリンク接続を含む自動車テレマティクスモジュールへのハイパーセキュアラストマイル通信
【図３５】セルラー接続と車内ＷｉＦｉ接続デバイスを備えた自動車通信ネットワークのテレマティクスモジュール間のラストリンク通信の例
【図３６】セルラー接続を使用したハイパーセキュア車間通信の例
【図３７】マイクロ波、衛星、及びファイバネットワークを介したハイパーセキュアトランク回線通信
【図３８】ハイパーセキュア、セキュア、及び非セキュアな通信ネットワークのセキュリティ、ＩＤ検証、及び発信者の匿名性の機能比較
【図３９】静的ＩＰアドレスを使用した単一ルートラストマイルハイパーセキュア通信の概略図
【図４０Ａ】静的ＩＰアドレスを使用した単一ルートラストマイルハイパーセキュア通信のＩＰスタックの概略図
【図４０Ｂ】静的ＩＰアドレスを使用した単一ルートラストマイルハイパーセキュア通信の簡略図
【図４１】動的クライアントＩＰアドレスを使用した単一ルートラストマイルハイパーセキュア通信の概略図
【図４２Ａ】動的クライアントＩＰアドレスを使用した単一ルートラストマイルハイパーセキュア通信のＩＰスタック
【図４２Ｂ】動的クライアントＩＰアドレスを使用する単一ルートラストマイルハイパーセキュア通信の代替ＩＰスタック
【図４３】静的ＩＰアドレスを使用したマルチルートラストマイルハイパーセキュアの概略図
【図４４Ａ】シングルＰＨＹラストリンクを使用した静的ＩＰアドレスとのマルチルートラストマイルハイパーセキュア通信のＩＰスタック図
【図４４Ｂ】マルチＰＨＹラストリンクを使用した静的ＩＰアドレスとのマルチルートラストマイルハイパーセキュア通信のＩＰスタック図
【図４５】動的クライアントＩＰアドレスを使用したマルチルートラストマイルハイパーセキュア通信の概略図
【図４６Ａ】シングルＰＨＹラストリンクを使用した動的クライアントＩＰアドレスとのマルチルートラストマイルハイパーセキュア通信のＩＰスタック図
【図４６Ｂ】マルチＰＨＹラストリンクを使用した動的クライアントＩＰアドレスとのマルチルートラストマイルハイパーセキュア通信のＩＰスタック図
【図４７】動的クライアントＩＰアドレスを使用したマルチルートラストマイルハイパーセキュア通信の代替版の概略図
【図４８】動的クライアントＩＰアドレスを使用したマルチルートラストマイルハイパーセキュア通信の代替版のＩＰスタック図

【図４９】ＳＤＮＰペイロードを伝送するイーサネット（登録商標）通信のＩＰｖ４及びＩＰｖ６データグラムの解説図
【図５０Ａ】クライアントからＳＤＮＰクラウドへの通信で使用されるＩＰｖ４及びＩＰｖ６ラストリンクイーサネット（登録商標）パケットの解説図
【図５０Ｂ】クライアントからＳＤＮＰクラウドへの通信で使用されるＩＰｖ４及びＩＰｖ６ゲートウェイリンクイーサネット（登録商標）パケットの解説図
【図５０Ｃ】ＳＤＮＰクラウドからクライアントへの通信で使用されるＩＰｖ４及びＩＰｖ６ゲートウェイリンクイーサネット（登録商標）パケットの解説図
【図５０Ｄ】ＳＤＮＰクラウドからクライアントへの通信で使用されるＩＰｖ４及びＩＰｖ６ラストリンクイーサネット（登録商標）パケットの解説図
【図５１Ａ】静的クライアントアドレス指定による単一ルートのラストマイル通信で使用される連続イーサネット（登録商標）データパケット（要約）
【図５１Ｂ】動的なクライアントアドレス指定による単一ルートのラストマイル通信で使用される連続イーサネット（登録商標）データパケット（要約）
【図５１Ｃ】静的クライアントアドレス指定によるマルチルートラストマイル通信で使用される連続イーサネット（登録商標）データパケット（要約）
【図５１Ｄ】動的クライアントアドレス指定によるマルチルートラストマイル通信で使用される連続イーサネット（登録商標）データパケット（要約）
【図５２Ａ】イーサネット（登録商標）経由のＳＤＮＰラストマイルルーティングの要約表
【図５２Ｂ】イーサネット（登録商標）経由の単一ルートラストマイル通信のトポロジー
【図５２Ｃ】イーサネット（登録商標）経由のマルチルートラストマイル通信のトポロジー
【図５２Ｄ】イーサネット（登録商標）経由のマルチルートラストマイル通信のトポロジー
【図５３】ＳＤＮＰペイロードを伝送するＷｉＦｉ通信のＩＰｖ４及びＩＰｖ６の解説図
【図５４Ａ】クライアントからＳＤＮＰクラウドへの通信で使用されるＩＰｖ４及びＩＰｖ６ラストリンクＷｉＦｉパケットの解説図
【図５４Ｂ】クライアントからＳＤＮＰクラウドへの通信で使用されるＩＰｖ４及びＩＰｖ６ゲートウェイリンクＷｉＦｉパケットの解説図
【図５４Ｃ】ＳＤＮＰクラウドからクライアントへの通信で使用されるＩＰｖ４及びＩＰｖ６ゲートウェイリンクＷｉＦｉパケットの解説図
【図５４Ｄ】ＳＤＮＰクラウドからクライアントへの通信で使用されるＩＰｖ４及びＩＰｖ６ラストリンクＷｉＦｉパケットの解説図
【図５５】ＳＤＮＰペイロードを伝送する４Ｇセルラー通信のＩＰｖ４及びＩＰｖ６データグラムの解説図
【図５６Ａ】クライアントからＳＤＮＰクラウドへの通信で使用されるＩＰｖ４及びＩＰｖ６のラストリンク４Ｇセルラーデータパケットの解説図
【図５６Ｂ】ＳＤＮＰクラウドからクライアントへの通信で使用されるＩＰｖ４及びＩＰｖ６ラストリンク４Ｇセルラーパケットの解説図
【図５７Ａ】単一メディアのマルチＰＨＹラストリンク通信の解説図
【図５７Ｂ】混合メディアのマルチＰＨＹラストリンク通信の解説図
【図５７Ｃ】マルチＰＨＹラストリンク通信の代替実装の解説図
【図５８】マルチＰＨＹイーサネット（登録商標）経由で配信されるＩＰｖ６データグラムを使用したクライアントからＳＤＮＰクラウドへの連続するラストリンク通信の解説図
【図５９】マルチＰＨＹ　ＷｉＦｉ経由で配信されるＩＰｖ６データグラムを使用したクライアントからＳＤＮＰクラウドへの連続するラストリンク通信の解説図
【図６０】マルチＰＨＹ　４Ｇセルラーネットワーク経由で配信されるＩＰｖ６データグラムを使用したクライアントからＳＤＮＰクラウドへの連続するラストリンク通信の解説図
【図６１】イーサネット（登録商標）及びＷｉＦｉ経由のマルチＰＨＹ配信を使用するＩＰｖ６データグラムを使用したクライアントからＳＤＮＰクラウドへの連続するラストリンク通信の解説図
【図６２】ＷｉＦｉ及び４Ｇセルラーネットワーク経由のマルチＰＨＹ配信を使用したＩ

Ｐｖ６データグラムを使用した、クライアントからＳＤＮＰクラウドへの連続するラストリンク通信の解説図
【図６３】レイヤ１からレイヤ７の機能を示すＤＯＣＳＩＳケーブルモデム通信ネットワークのＯＳＩレイヤスタック構成の概略図
【図６４】ＳＤＮＰペイロードを伝送するケーブルシステム用に作成されたＤＯＣＳＩＳ３ベース通信パケットの解説図
【図６５Ａ】各種ＤＯＣＳＩＳ３プロトコルのスペクトル割り当てとキャリア変調方式の解説図
【図６５Ｂ】ＣＴＭＳとＣＭ間のＤＯＣＳＩＳ３．１通信シーケンスの解説図
【図６５Ｃ】ＤＯＣＳＩＳ３．１アップストリーム通信の解説図
【図６５Ｄ】ＤＯＣＳＩＳ３．１ダウンストリーム通信の解説図
【図６６】ラストマイル通信用の３ルートＳＤＮＰネットワークの概略図
【図６７】トライチャネルＳＤＮＰラストマイル通信における「コール要求」操作の概略図
【図６８】トライチャネルＳＤＮＰラストマイル通信における「アドレス要求」操作の概略図
【図６９】トライチャネルＳＤＮＰラストマイル通信における「アドレス配信」操作の概略図
【図７０】ＳＤＮＰコマンド及び制御パケット合成方法を示すフローチャート
【図７１】単一ルートのトライチャネルＳＤＮＰラストマイル通信における「ルーティング指示」操作の概略図
【図７２】ＳＤＮＰクライアントからＳＤＮＰクラウドへの単一ルートトライチャネルＳＤＮＰラストマイル通信における「ＳＤＮＰコール」操作の概略図
【図７３Ａ】ＳＤＮＰコールでのＳＤＮＰクラウド及びＳＤＮＰクライアントへのラストマイル３ルート通信の概略図
【図７３Ｂ】非ＳＤＮＰクライアントへの「コールアウト」として実装されたＳＤＮＰクラウドとラストマイルの３ルート通信の概略図
【図７４】マルチルートトライチャンネルＳＤＮＰラストマイル通信における「ルーティング指示」操作の概略図
【図７５Ａ】ＳＤＮＰクライアントからＳＤＮＰクラウドへの方向のマルチルート３チャネルＳＤＮＰラストマイル通信における「ＳＤＮＰコール」動作の概略図
【図７５Ｂ】ＳＤＮＰクラウドからＳＤＮＰクライアントへの方向のマルチルートトライチャネルＳＤＮＰラストマイル通信における「ＳＤＮＰコール」操作の概略図
【図７６】単一ルートトライチャネルＳＤＮＰラストマイル通信におけるグループコールの「ルーティング指示」操作の概略図
【図７７Ａ】ゾーンＵ１クライアントから他ゾーンのクライアントへの方向のＳＤＮＰマルチルートクラウドトランスポート及びＳＤＮＰラストマイル通信を使用する「ＳＤＮＰグループコール」の概略図
【図７７Ｂ】ゾーンＵ７クライアントから他ゾーンのクライアントへの方向のＳＤＮＰマルチルートクラウドトランスポート及びＳＤＮＰラストマイル通信を使用する「ＳＤＮＰグループコール」の概略図
【図７７Ｃ】ゾーンＵ９クライアントから、同じゾーン及び他のゾーンのクライアントへの方向のＳＤＮＰマルチルートクラウドトランスポート及びＳＤＮＰラストマイル通信を使用する「ＳＤＮＰグループコール」の概略図
【図７８】ＳＤＮＰクライアントとセキュリティのないＰＳＴＮデバイス双方に対するＳＤＮＰマルチルートクラウドトランスポート及びラストマイル通信を使用した「ＳＤＮＰグループコール」の概略図
【図７９Ａ】ＳＤＮＰグループコールにおける通常コールとプライベートコールの操作一覧表
【図７９Ｂ】ＳＤＮＰグループコールにおける通常コールとハイパープライベートコールの操作一覧表

【図８０Ａ】ＳＤＮＰ　ＰＴＴグループコールにおける通常及びプライベートのプッシュツートーク操作一覧表
【図８０Ｂ】ＳＤＮＰ　ＰＴＴグループコールにおける通常及びハイパープライベートのプッシュツートーク操作一覧表
【図８１】断片化データのハイパーセキュアファイルストレージにおける書き込み操作時のデータ伝送の概略図
【図８２Ａ】断片化データのハイパーセキュアファイルストレージにおける書き込み操作時のデータフローの概略図
【図８２Ｂ】断片化データのハイパーセキュアファイルストレージにおける読み取り操作のデータフローの概略図
【図８３】断片化データのハイパーセキュアファイルストレージにおける読み取り操作時のデータ伝送の概略図
【図８４Ａ】ＳＤＮＰクラウド接続ファイルストレージソリューションの例
【図８４Ｂ】ローカル及びクラウドに接続されたストレージサーバを含む分散ハイパーセキュアファイルストレージネットワークの概略図
【図８５Ａ】非冗長ハイパーセキュアファイルストレージのファイルマッピング（ＲＲＦ＝０）
【図８５Ｂ】読み取り冗長係数ＲＲＦ＝１のハイパーセキュアファイルストレージのファイルマッピング
【図８５Ｃ】読み取り冗長係数ＲＲＦ＝２のハイパーセキュアファイルストレージのファイルマッピング
【図８６】トライチャネルネットワーク通信を使用した分散ハイパーセキュアファイルストレージシステムのネットワークマップ
【図８７Ａ】分散ハイパーセキュアファイルストレージシステムでのファイル書き込み要求操作
【図８７Ｂ】分散ハイパーセキュアファイルストレージシステムでのファイルサーバ名要求操作
【図８７Ｃ】分散ハイパーセキュアファイルストレージシステムでのシグナリングサーバのプランニング操作
【図８７Ｄ】分散ハイパーセキュアファイルストレージシステムにおけるシグナリングサーバのクライアント側ラストマイル及びＳＤＮＰクラウドの書き込みルーティング指示
【図８７Ｅ】分散ハイパーセキュアファイルストレージシステムにおけるシグナリングサーバのストレージ側ラストマイル及びＳＤＮＰクラウドの書き込みルーティング指示
【図８８】分散ハイパーセキュアファイルストレージシステムでのファイル転送
【図８９Ａ】分散ハイパーセキュアファイルストレージシステムにおけるファイルストレージと書き込み操作を確認するリンク応答
【図８９Ｂ】分散ハイパーセキュアファイルストレージシステムにおけるファイルストレージサーバのリンク転送
【図８９Ｃ】ＦＳリンクを含むファイルストレージサーバ書き込み確認データパケット
【図８９Ｄ】クライアントのＳＤＮＰメッセンジャーでのファイルストレージ読み取りリンクの合成
【図９０Ａ】非冗長ＲＲＦ＝０のハイパーセキュアファイルストレージとＬＲＦ＝０の非冗長ＦＳリンクのファイルマップ
【図９０Ｂ】非冗長ＲＲＦ＝０のハイパーセキュアファイルストレージとＬＲＦ＝１の冗長ＦＳリンクのファイルマップ
【図９０Ｃ】非冗長ＲＲＦ＝１のハイパーセキュアファイルストレージとＬＲＦ＝１の冗長ＦＳリンクのファイルマップ
【図９１】ファイルストレージサーバとクライアントＦＳリンクの数の関数としてストレージの復元力を示すグラフ
【図９２】ＳＤＮＰエンコード及びＳＤＮＰデコード機能の概略図

【図９３Ａ】クライアント側にファイルセキュリティとハイパーセキュアファイル伝送機能があるＳＤＮＰ分散ファイルストレージの概略図
【図９３Ｂ】ネストされたファイルセキュリティとハイパーセキュアファイル伝送機能があるＳＤＮＰ分散ファイルストレージの概略図
【図９４】ＳＤＮＰ分散ファイルストレージの書き込み操作におけるハイパーセキュアエンコードの概略図
【図９５】ＳＤＮＰ分散ファイルストレージの読み取り操作におけるハイパーセキュアデコードの概略図
【図９６Ａ】ハイパーセキュアファイル読み取り操作におけるＡＡＡ操作のフローチャート
【図９６Ｂ】ハイパーセキュアファイル読み取り操作におけるファイルアクセスとＳＤＮＰ伝送のフローチャート
【図９７Ａ】分散ハイパーセキュアファイルストレージシステムにおけるファイル読み取り要求操作
【図９７Ｂ】分散ハイパーセキュアファイルストレージシステムにおけるファイルストレージサーバ名要求操作
【図９７Ｃ】分散ハイパーセキュアファイルストレージシステムにおけるストレージサーバ名配信及びシグナリングサーバのプランニング操作
【図９７Ｄ】分散ハイパーセキュアファイルストレージシステムにおけるシグナリングサーバのストレージ側ラストマイル及びＳＤＮＰクラウドルーティングの読み取り指示
【図９７Ｅ】分散ハイパーセキュアファイルストレージシステムにおけるシグナリングサーバのクライアント側ラストマイル及びＳＤＮＰクラウドの読み取りルーティング指示
【図９８】分散ハイパーセキュアファイルストレージシステムにおける読み取り操作中のストレージ側ファイルデコード
【図９９】分散ハイパーセキュアファイルストレージシステムでの読み取り操作中のファイルデータ転送
【図１００】分散ハイパーセキュアファイルストレージシステムでのリンク更新中のファイルデータ転送
【図１０１】ファイルの再配布に使用される分散ハイパーセキュアファイルストレージシステムでのファイルデータ転送
【図１０２】ＳＤＮＰテキストメッセージングのタイムスタンプ
【図１０３】ＳＤＮＰ登録通信のフローチャート
【図１０４Ａ】インターネットＯＴＴ通信におけるエンドツーエンドの暗号化
【図１０４Ｂ】ハイパーセキュア通信のエンドツーエンドの暗号化
【図１０５Ａ】発呼の目に見えない監視を実行するＳＤＮＰセキュリティエージェントによる「ＳＤＮＰコール」操作の概略図
【図１０５Ｂ】着呼の目に見えない監視を実行するＳＤＮＰセキュリティエージェントによる「ＳＤＮＰコール」操作の概略図
【図１０６】ＦＳリンクルーティングを秘密裏に監視するＳＤＮＰセキュリティエージェントを備えた分散ハイパーセキュアファイルストレージシステムにおけるファイルストレージサーバリンクの転送
【図１０７】マルチルートラストマイル通信を使用した発呼を秘密裏に監視するＳＤＮＰセキュリティエージェントによる「ＳＤＮＰコール」操作の概略図
【図１０８】ＳＤＮＰセキュリティエージェントの指定・承認手順のフローチャート
【図１０９】ＳＳ７の脆弱性の影響を受ける携帯電話から基地局への通信
【図１１０】電話番号の偽装によりＳＳ７攻撃を撃退するＳＤＮＰ通信
【図１１１】個別サーバでホストされているＳＤＮＰソフトウイッチベースのクラウドの接続性
【図１１２】共有サーバでホストされているＳＤＮＰソフトスイッチベースのクラウドの接続性
【図１１３】重複するネットワーク上でホストされているＳＤＮＰソフトスイッチベース

のクラウドの接続性
【図１１４】グローバルＳＤＮＰクラウド通信会社にアクセスするＳＤＮＰソフトスイッチベースのクラウドの接続性
【図１１５】ネストされたＳＤＮＰサブネットの例
【発明を実施するための形態】
【０１６７】
約１世紀半の回線交換電話の後、今日の通信システム及びネットワークは、全てこの１０年以内に、イーサネット（登録商標）、ＷｉＦｉ、４Ｇ／ＬＴＥ、及びＤＯＣＳＩＳ３データをケーブルと光ファイバ経由で伝送するインターネットプロトコルを使用したパケット交換通信に移行した。音声、テキスト、画像、ビデオ、及びデータを一括する利点は、信頼性の高いＩＰパケット配信を保証するための冗長パスの使用（つまりインターネットが最初に作られた理由）とともに、比類のないレベルのシステム相互運用性及びグローバルなコネクティビティなど数多くある。しかし、どんなイノベーションでも、新技術が生み出す課題の大きさは、得られるメリットに同程度となることが多い。
【０１６８】
既存の通信プロバイダの短所
【０１６９】
本開示の背景技術の欄全体にわたって詳述されたように、今日の通信は多くの欠点を有する。Ａ Ｔ＆Ｔ（登録商標）、Ｖｅｒｉｚｏｎ（登録商標）、ＮＴＴ（登録商標）、Ｖｏｄａｐｈｏｎｅ（登録商標）など世界の主要な長距離通信事業者が所有するカスタムデジタルハードウェアで構成されている今日の最高性能の通信システムは、一般的に優れた音声品質を提供するがコストが高く、そのようなコストには、高価な月額取扱料、接続料金、長距離料金、複雑なデータレートプラン、長距離ローミング料金、及び多数のサービス料が含まれる。これらのネットワークはプライベートであるため、実際のデータセキュリティは一般に知られておらず、セキュリティ侵害、ハッキング、侵入は通常は一般には報告されない。今日のプレスで報道された盗聴とプライバシー侵害の数を考えると、プライベートキャリア通信セキュリティは、プライベートクラウドではないにせよ、少なくともラストマイル接続では疑わしいままである。
【０１７０】
「インターネットサービスプロバイダ」すなわちＩＳＰは、グローバル・コミュニケーション・チェーンにおいて別のリンクを形成している。本発明の背景に記載されているように、ＶｏＩＰまたは「ボイスオーバーインターネットプロトコル」を使用してインターネットを介して運ばれる音声は、サービス品質またはＱｏＳの問題を抱えている。そのような問題としては、以下のものが挙げられる。
・パケット交換ネットワークであるインターネットは、適時にＩＰパケットを配信するように設計されておらず、低遅延で高ＱｏＳのリアルタイムアプリケーションをサポートするようには設計されていない。
・ＩＰパケットのルーティングに予期しない経路が発生すると、遅延が絶えず変化し、データエラー率が高いバーストが発生し、予期しないコール切断が起こる。
・ＩＰパケットルーティングは、インターネットサービスプロバイダ（ＩＰＳ）の裁量で行われ、ＩＰＳは、パケットがルーティングされるネットワークを制御し、ネットワークを通過する一般的なトラヒック接続品質の低下を犠牲にして、自己のネットワークの負荷を分散するためのルーティングの調整や、ＶＩＰクライアントに対する適切なサービスを行うことがある。
・ＬＩＮＥ（登録商標）、ＫａｋａｏＴａｌｋ（登録商標）、Ｖｉｂｅｒ（登録商標）などのオーバー・ザ・トップすなわちＯＴＴプロバイダは、インターネットにフリーライドし、インターネットのヒッチハイカーとして機能し、ネットワークやＱｏＳに影響を与える要因を制御できない。
・適度なデータレートでも妥協のない音声品質の音声を提供できないヘビーウェイトオーディオＣＯＤＥＣが使用される。

・ＴＣＰトランスポートプロトコルに基づくＶｏＩＰでは、ハンドシェーキングやＩＰパケットの再ブロードキャスト中に引き起こされる遅延のために遅延時間が大きくなり、音声が劣化する問題を生じる。補助無しのＵＤＰトランスポートは、ペイロードの完全性を保証しない。

【０１７１】

ＱｏＳの問題とは別に、現在のデバイスやネットワークのセキュリティは、グローバル通信の将来のニーズをサポートするにはまったく受け入れられないレベルである。セキュア動的通信ネットワーク及びプロトコルと名称されるアメリカ特許出願の背景技術の欄で詳述されているように、ネットワークセキュリティは、通信するデバイスに対するサイバー攻撃（スパイウェア、トロイの木馬、感染、フィッシングなど）、ラストリンクに対するサイバー攻撃（スパイウェア、ＩＰパケットスニッフィング、盗聴、サイバーパイレーツによる「偽」携帯電話タワーのコールインターセプトを含む）、及びラストマイル接続のローカルネットワークまた電話通信会社部分でのサイバー攻撃（スパイウェア、ＩＰパケットスニッフィング、ウイルスなどの感染、及びサイバーパイレーツの「中間攻撃」が関与）などの大規模な攻撃を受けやすい。クラウド自体は、ウイルスなどの感染による攻撃、中間攻撃を開始するサイバーパイレーツからの攻撃、サービス拒否攻撃、及び権限のない政府監視からの攻撃によって任意のクラウドゲートウェイでセキュリティを破ることによって不正なアクセスを受ける可能性がある。要約すると、今日の通信セキュリティは、サイバー犯罪者によって容易に悪用され、サイバー犯罪やサイバープライバシー侵害に有用な多数の脆弱性によって損なわれるが、そのような脆弱性として以下のものが挙げられる。

・宛先ＩＰアドレス、宛先ポート番号、及び宛先ＭＡＣアドレスを含むＩＰパケットの宛先の開示。

・送信元ＩＰアドレス、送信元ポート番号、及び送信元ＭＡＣアドレスを含む、ＩＰパケットの送信元の開示。

・採用されたレイヤ４トランスポートのタイプ、ポート番号によって要求されたサービスのタイプ、ＩＰパケットのペイロードにカプセル化されたアプリケーションデータの開示。

・暗号化されていないファイルにおける、個人及び機密情報、ログイン情報、アプリケーションパスワード、財務記録、ビデオ、写真などを含む、ＩＰパケットのペイロード。

・サイバーハッカーが暗号化されたファイルを壊す機会を繰り返すことを可能にする通信のダイアログ。

・ＦＴＰ、電子メール、及びウェブページベースの感染を使用して、スパイウェアやフィッシングプログラム、トロイの木馬を含むマルウェアを通信デバイスやルータにインストールする数多くの機会。

【０１７２】

インターネットプロトコルを使用するパケット交換通信ネットワークの根本的で本質的な弱点の要点を繰り返し述べると、任意の敵対者すなわちサイバーパイレーツがインターセプトしたＩＰパケットからは、ＩＰパケットに含まれるデータの作成にどのデバイスが関与していたか、ＩＰパケットがどこから来たのか、ＩＰパケットがどこに送られているか、どのようにデータが転送されているか（すなわちＵＤＰまたはＴＣＰのいずれか）、どのような種類のサービスが要求されているか（すなわちペイロード内にどのような種類のアプリケーションデータが含まれているか）を確認することができる。これに関して、サイバーパイレーツは、会話の「内容の前後関係」を判定し、暗号化を破る機会を高め、パスワードセキュリティを破り、ファイル、データ、及びペイロードコンテンツへの不正アクセスを得ることができる。

【０１７３】

暗号化

【０１７４】

前述のように様々なサイバー攻撃に対して防御するために、現在のネットワーク管理者、ＩＴプロフェッショナル、及びアプリケーションプログラムは、主にただ一つの防衛手

段である暗号化に依存している。暗号化とは、それにより「平文」とも呼ばれる認識可能なコンテンツ（可読テキスト、実行可能プログラム、可視ビデオ及び画像、または明瞭な音声）を、無意味な文字の文字列として表示される「暗号文」として知られる代替的ファイルタイプに変換する手段である。

【０１７５】

保護されていないファイルを暗号化されたファイルに変換する暗号化プロセスでは、暗号化の変換プロセスの見かけのパターンを明らかにせず、データを同等のテキスト要素に変更するための暗号アルゴリズムと呼ばれる論理アルゴリズムが使用される。暗号化されたファイルは、宛先デバイスによって受信されるまで通信ネットワークまたは媒体を介して送信される。ファイルを受信すると、その後、受信デバイスは、「復号化」として知られるプロセスを使用して元のコンテンツを明らかにするために符号化されたメッセージを復号化する。暗号化と解読の研究は、広く「暗号学」と呼ばれ、数理理論、集合理論、アルゴリズム設計などの数学の要素をコンピュータサイエンスや電気工学と融合させる。

【０１７６】

単純な「シングルキー」または「シンメトリックキー」暗号化技術では、ファイルの暗号化と復号化のプロセスでのロック解除のために、両者が前もって知っている単一のキーワードまたはフレーズを使用できる。例えば、第二次世界大戦では、公開された無線チャンネルで通信される潜水艦や海洋船は暗号化されたメッセージを使用していた。当初は、暗号化はシングルキーベースであった。連合国側の暗号学者は、コードパターンを分析することによって、暗号化キーワードまたはパターンを明らかにした後、知られることなく暗号化ファイルを読み取ることができた。暗号化の方法が複雑になるにつれて、手動でコードを破ることは困難になった。

【０１７７】

コードは、機械的な機械ベースの暗号に進化した。当時、コードを壊す唯一の方法は、暗号化機械を盗み、ファイルを暗号化するものと同じツールを使ってメッセージを解読することであった。その問題は、盗んだことを検知されることなく暗号化機械を盗む方法であった。コード機が盗まれたことが判明した場合、敵は単にコードを変更し、すでに動作中の暗号化機械を更新するだけで済む。この原則は今日でも有効であり、最も効果的なサイバー攻撃は、検知されないサイバー攻撃である。

【０１７８】

コンピュータ化と冷戦の到来により、暗号化はより複雑になったが、暗号化コードを解読するために使用されるコンピュータの速度も向上した。セキュリティを確保した通信の開発における各ステップでは、情報を暗号化するための技術とノウハウと、暗号化コードを解読する能力がほぼ足並みを揃えて開発されてきた。暗号化における次の進化の大きなステップは、１９７０年代の、今日も使用されているデュアルキー暗号化技術の革新である。最もよく知られているデュアルキー暗号化方式の１つは、開発者のＲｉｖｅｓｔ、Ｓｈａｍｉｒ、Ａｄｌｅｍａｎにちなんで命名されたＲＳＡ公開鍵暗号方式である。ＲＳＡの公開による認定にもかかわらず、同時代の開発者には同じ原則を独自に考案した者もいた。ＲＳＡは、公開されていない２つの大きな素数に基づいて２つの暗号鍵を使用する。この２つの素数を暗号鍵（ここではＥ鍵と呼ぶ）に変換するために１つのアルゴリズムが使用され、異なる２つの秘密素数を秘密復号鍵（ここではＤ鍵と呼ぶ）に変換するために異なる数学アルゴリズムが使用される。秘密素数を選択したＲＳＡユーザ（本明細書では「鍵発行者」と呼ぶ）は、ファイルを暗号化しようとする者に典型的には１０２４ｂから４０９６ｂのアルゴリズムで生成されたＥ鍵を配布すなわち「公開」する。この鍵は暗号化されていない形式で多くの当事者に配布される可能性があるため、Ｅ鍵は「公開鍵」として知られている。

【０１７９】

鍵発行者と通信したいと望む当事者は、一般に商用ソフトウェアの形で提供される公的に利用可能なアルゴリズムと共にこの公開Ｅ鍵を使用して、特定の鍵発行者に送信されるファイルを暗号化する。暗号化されたファイルを受信すると、鍵発行者は秘密のＤ鍵を使

用してファイルを復号化し、平文に戻す。一般的なデュアルキー方式とＲＳＡアルゴリズムの特有の特徴は、ファイルを暗号化するために使用された公開Ｅ鍵を復号化に使用できないことである。鍵発行者が所有する秘密のＤ鍵だけがファイルの復号化の能力を有する。

【０１８０】

ファイル暗号化及び復号化におけるデュアルキー、スプリットキー、またはマルチキー交換の概念は、ＲＳＡまたはいずれかのアルゴリズム方法に特に限定されず、通信方法を一連のステップとして方法論的に特定する。スイッチパケット通信ネットワークを介した通信を実現する際のデュアルキー交換を用いてみよう。例えば、携帯電話から安全なファイルを受信することを望むノートブックは、まず、暗号化のためのＥ鍵と、何らかのアルゴリズムを用いた復号化のためのＤ鍵の２つの鍵を生成する。次に、ノートブックは、ＩＰパケットを運ぶ公衆ネットワーク通信を使用して、Ｅ鍵を携帯電話に送る。ＩＰパケットは、暗号化されていない形式で、ノートブックのＭＡＣアドレス、ＩＰソースアドレス及びポートアドレスとともに、携帯電話の宛先ＩＰアドレス、ポート＃、及びトランスポートプロトコルＴＣＰ、並びにそのペイロードとしてのＥ鍵の暗号化されたコピーを含む。

【０１８１】

次に、携帯電話は、合意された暗号化アルゴリズムまたはソフトウェアパッケージを使用して、暗号アルゴリズム及び暗号化Ｅ鍵を使用して平文ファイルを処理して、セキュリティが確保された通信におけるＩＰパケットのペイロードとして運ばれる暗号化ファイルすなわち暗号文を、携帯電話からノートブックに送信する。アルゴリズムは、ＩＰパケットを受信すると、秘密復号鍵、すなわちＤ鍵を用いてファイルを復号する。Ｄ鍵はＥ鍵に対応するので、本質的にアルゴリズムは両方の鍵を認識し両鍵を用いて暗号文を復号化し、暗号化されていない平文６９７Ｂに戻す。ＩＰパケット６９６のペイロードは、暗号化されたファイル、すなわち暗号文の形で保護されているが、残りのＩＰパケットは暗号化されず、スニッフィング可能で、サイバーパイレーツにより読み出し可能であり、その部分には、ソースＩＰアドレス「ＣＰ」及びポート＃、宛先ＩＰアドレス「ＮＢ」及び関連ポート＃が含まれる。従って、ペイロード自体を開けない場合でも、通信を監視され得る。

【０１８２】

バーチャルプライベートネットワーク（ＶＰＮ）

【０１８３】

暗号化に依存するもう１つのセキュリティ方法は、「仮想プライベートネットワーク」すなわちＶＰＮのセキュリティ方法である。ＶＰＮでは、暗号化されたＩＰパケットを使用してネットワーク内にトンネルまたはセキュリティを確保したパイプ（セキュアパイプ）が形成される。ペイロードだけを暗号化するのではなく、ＩＰパケット全体が暗号化され、カプセル化されたパケットをあるＶＰＮゲートウェイから別のＶＰＮゲートウェイに送信するミュールすなわちキャリアとして機能する別の暗号化されていないＩＰパケットにカプセル化される。もともとは、ＶＰＮは、遠隔地に分散されたローカルエリアネットワークを接続するために使用され、例えば、ニューヨーク、ロサンゼルス、及び東京のプライベートネットワークを運営する企業が、ＬＡＮを相互接続して、１つのグローバルプライベートネットワークを共有しているかのように同じ機能を有するものとすることを望んでいる場合に使用されていた。

【０１８４】

基本的なＶＰＮ概念は、ふたつのデバイス間での暗号化された通信と考えられる。例えば、第１のサーバが、無線のＲＦ接続及び有線接続を介して多数のデバイスをサポートする１つのＬＡＮの一部として、コンテンツを含む「仮想プライベートネットワーク」、すなわち、ＶＰＮトンネルを介して第２のサーバに接続され、第２のサーバは、デスクトップ、ノートブック、及びＷｉＦｉ基地局への有線接続を有する。これらの比較的低い帯域幅のリンクに加えて、第１のサーバはまた、高帯域幅接続を介してスーパーコンピュータに接続する。その結果発生する通信は、外部ＩＰパケットの中にＶＰＮパッケトを含めた複数のデータパケットのシーケンスである。動作中、送信元ＩＰアドレス及びポート＃を指定するサーバＡからの外部ＩＰパケットは、宛先ＩＰアドレス及びポート＃でサーバＢ

に送信される。この外部ＩＰパケットは、第１のサーバと第２のサーバ間に通信を設定させ、データが通過するために暗号化されたトンネルを形成する。外部パケットのＶＰＮペイロードはラストマイルＩＰパケットを含み、送信元ＩＰアドレス「ＤＴ」及び対応するアドホックポート＃を有するデスクトップと、送信元ＩＰアドレス「ＮＢ」及び対応するアドホックポート＃を有するノートブックとの間の直接通信と、ファイル転送の要求とを提供する。

【０１８５】

仮想プライベートネットワークを使用してこの転送を安全に確立するためには、ＶＰＮトンネルが作成され、実際の通信が送信される前にセッションが開始される。企業の用途では、ＶＰＮトンネルはインターネット上でアドホックに運ばれるのではなく、一般に専用のＩＳＰまたはキャリアが自社のファイバ及びハードウェアネットワークを所有して運営されている。このキャリアは、多くの場合一定のコストに対して特定の帯域幅を保証するべくＶＰＮサービスを必要とする企業との年間または長期の契約を締結している。理想的には、サーバ間での通信は、高速専用リンクを用いて、ＶＰＮの性能、ＱｏＳ、またはセキュリティを妨げる中間すなわち「ラストマイル」接続なしで実施すべきである。

【０１８６】

動作中、従来のＶＰＮでは、ＶＰＮを作成するすなわち「ログイン」する第１ステップと、セキュリティを確保したパイプまたはトンネル内でデータを転送する第２のステップの２段階プロセスが必要である。トンネリングの概念は階層的に示されており、通信スタックによって搬送される外部ＩＰパケットは、レイヤ１からレイヤ４にＶＰＮ接続を形成し、レイヤ５を利用して仮想ＶＰセッション７２３を作成し、レイヤ６のプレゼンテーション層を利用して暗号化を容易化し、サーバ間のゲートウェイ・パイプへのＶＰＮゲートウェイを実現する。ＶＰＮ接続はインターネットプロトコルを使用してＩＰパケットを送信するが、ＶＰＮの物理レイヤ１及びＶＰＮデータリンクレイヤ２は一般に専用キャリアによってサポートされ、インターネット上での予測不可能なルーティングを使用しない。例えば、デスクトップ間のデバイス間通信として転送されるアプリケーションレイヤ７データは、あたかもＶＰＮが存在しないかのように通信を確立するために必要な７つのＯＳＩレイヤを全て含むトンネリングデータとして供給される。つまり、ＶＰＮは、その内部パケットを運ぶレイヤ７内で機能する通信プロトコルと考慮できる。

【０１８７】

動作中、１つの通信スタックからもうひとつの通信スタックに外部ＩＰパケットが移行すると、パケットの真のメッセージであるカプセル化データが開示するために開かれる。このようにして、ＶＰＮトンネルが通信の試みに先立って形成され、会話が終了した後に閉じなければならないことを除き、ＶＰＮトンネルの作成に使用される詳細とは無関係にエンドツーエンド通信が行われる。ＶＰＮトンネルを最初に開かないと、ＩＰパケットの盗聴、ハイジャック、感染などの影響を受けやすい暗号化されていないＩＰパケットの送信が発生する。会話が完了した後でＶＰＮを閉じないと、サイバー犯罪者に対し他人のＶＰＮトンネル内で違法行為を隠す機会を与え、インターセプトされた場合、罪のない人に対して刑事罰が科されることになる可能性がある。

【０１８８】

ＶＰＮは、複数のプライベートローカルエリアネットワークが専用の容量と帯域幅でプライベート接続を使用して相互に接続する一般的な方法であるが、公衆ネットワークとインターネットを介したＶＰＮの使用は両者間の通信に問題がある。ＶＰＮの１つの問題は、ＶＰＮ接続をパケットごとにではなく、使用する前に事前に確立する必要があることである。例えば、パケット交換ネットワークを介して接続されたＶｏＩＰコールでは、ある携帯電話が第２の携帯電話の意図された通話受信者に連絡する前に、ＶＰＮセッションを確立しなければならない。その為には、まずＶＰＮ接続アプリケーションを、発呼者の携帯電話の携帯に設置しなければならない。次に、発呼者は、典型的にサービスプロバイダであるＶＰＮホストにＩＰパケットを送信する。これらのパケットは、ルーティングを介して通過可能なラストマイルで運ばれる。例えば、携帯電話の無線通信から近くのＷｉＦ

ｉ基地局に運ばれ、次に有線通信によりローカルルータへ送られ、最終的にＶＰＮホストにたどり着く。発呼者の携帯電話とＶＰＮホスト間でのセッションが確立されると、発呼者の携帯電話はＶＰＮホストに対し、ＶＰＮトンネルを確立するよう指示を出す。このＶＰＮトンネルの部分はレイヤ５で促進され、レイヤ６により暗号化される。

【０１８９】

ＶＰＮ接続が設定されると、発呼者の携帯電話は、任意のＶｏＩＰ電話アプリを介して電話をかける。宛先電話が同じＶＰＮに接続されていない場合、アプリケーションは、最も近いＶＰＮホストから宛先携帯電話へラストマイルで「コールアウト」リンクを確立する必要がある。ＶｏＩＰアプリケーションがそれを行えない、または行うことが許可されていない場合、コールは失敗し、速やかに終了する。そうでない場合、内部側ＩＰパケットは、発呼側携帯電話と宛先携帯電話との間にアプリケーションレイヤ５セッションを確立し、ＩＰテストパケットが適切に解読され、理解可能であることを確認する。

【０１９０】

コールを行う（電話をかける）には、電話機内の電話キャリアのＳＩＭカードがＶＰＮトンネルと互換性がないため、コールは、電話機の通常のダイヤルアップ機能からではなく、電話機で実行されているレイヤ７アプリケーションからである必要がある。コールが開始されると、携帯電話は、その通信アプリケーションに従って音声の小片すなわち「スニペット」を表す一連のＩＰパケットを送信する。これらのパケットは、発呼者の携帯電話内のアプリケーションからＷｉＦｉリンクを介してＷｉＦｉ基地局に、次いで有線接続を介してルータに、そして最後に有線接続を介してＶＰＮホストに送られる。次に、データは、ＶＰＮトンネルを介してＶＰＮホストへの接続によりセキュリティを確保した状態で、ＶＰＮネットワークの宛先のデバイス、つまり、ＶＰＮゲートウェイに送信される。この例では、ＶＰＮトンネルは宛先携帯電話まで接続されず、発呼されているデバイスの手前で止まる。ＶＰＮゲートウェイ以降は、ＶＰＮキャリアが仲介していないので、データは暗号化されていない。一旦ＶＰＮトンネルを離れると、ＶＰＮホストは、宛先デバイスのラストマイル接続にデータを転送する。つまり、データを有線接続でルータに送り、有線接続によってローカルの携帯電話システムとタワーに送り、タワーは通常の２Ｇ、３Ｇ又は４Ｇを使った電話呼出しとしてコールを行う。携帯電話アプリから同じアプリを実行していない電話に電話をかける（コールする）プロセスをコールアウト機能と呼ぶ。

【０１９１】

後述の例は、公衆ネットワークを介してＶＰＮに接続する際の別の問題を浮き彫りにしている。ＶＰＮホストから発呼者へのラストマイルリンクは、ＶＰＮでカバーされていないので、セキュリティ、パフォーマンス、コールＱｏＳを保証するものではない。具体的には、発呼者のラストマイルの接続は、全て盗聴及びサイバー攻撃の対象となる。コールが完了し、発呼者が携帯電話を切ると、ＶＰＮリンクは終了しなければならず、ＶＰＮレイヤ５はＶＰＮセッションを終了し、発呼者の携帯電話はＶＰＮホストとの接続を断つ。

【０１９２】

コンピュータ間でのデータ転送の為に作られたＶＰＮネットワークを応用するのは、多数の問題点を発生させる。

・宛先ＶＰＮネットワークから宛先携帯電話へのラストマイル通信は、安全ではなくスニッフィングや監視されるリスクがある。

・発呼者の携帯電話とＶＰＮゲートウェイ間の通信は、発呼者がデータ通信のアプリケーションを用いている場合のみ安全性が確保できる。発呼者が電話線を用いてＶＰＮゲートウェイに接続する場合、つまりダイアルイン機能を使った場合は、発呼者の携帯電話と最も近いＶＰＮゲートウェイ間のラストマイル接続は安全ではなく、スニッフィングと監視されるリスクがある。

・最終的な端末間のコールは、両端末がデータ通信を用いている場合のみ安全性を確保する事ができ、電話線を用いる場合は、確保できない。また、コールを開始する前に、両端末が事前に同じＶＰＮに接続する事が要求される。

【０１９３】

この最後の点は、ＶＰＮコミュニケーションのパラドックスと言える。電話を受け取る側は、その前に、電話される事を知り、事前にネットワークに接続しなければならない。電話を受け取る事を事前に連絡し、コールがする前にＶＰＮに接続するように指示を出さなければならない。つまり、安全性を確保したコールをする前に、まず安全性が確保されていない電話を受け取らなければならない。安全性のないコールは、容易にハッキング、スニッフィング、又監視される。また、メタデータにより、誰が誰に電話しているか、また、何時に電話されたかが開示されてしまう。コールのメタデータは、ハッカーにとって、ハッキング対象とされている人の活動やプロフィールを知るのに非常に有効である。

【０１９４】

ただし、セキュリティに関する懸念を除外したとしても、ＶＰＮを介して電話をかけたり文書を送信したりすることは、以下の理由を含む何らかの理由で失敗しないという保証はない。

・ＶＰＮは、リアルタイムアプリケーション、ＶｏＩＰ、またはビデオをサポートために十分な低レイテンシーで動作しない可能性がある。

・発信者からＶＰＮゲートウェイまたはＶＰＮゲートウェイから通話受信者へのＶＰＮラストマイル接続は、リアルタイムアプリケーション、ＶｏＩＰまたはビデオをサポートするために十分な低レイテンシーで動作しない可能性がある。

・発呼者または意図された受信者への最も近いＶＰＮゲートウェイまでの距離、すなわち「ラストマイル」が非常に遠い可能性、場合によってはＶＰＮなしで通話受信者までの距離よりも遠く離れている可能性があり、これによりネットワークの不安定さ、未知のネットワークによる制御不能なルーティング、可変ＱｏＳ、及び接続の保護されていない部分での中間者攻撃の機会を多数提供することがある。

・ＶＰＮゲートウェイからコール受信者へのＶＰＮラストマイル接続では、「コールアウト」接続とパケット転送またはローカル電話会社へのサポートリンクをサポートしていない場合がある。

・地元の通信事業者または政府検閲官が、国家安全保障または法令遵守の理由で、既知のＶＰＮゲートウェイに出入りする通話または接続をブロックする可能性がある。

・企業のＶＰＮを使用すると、ＶｏＩＰ通話は会社の従業員と指定された許可されたユーザのみに限定され、金融取引やビデオストリーミングがブロックされたり、Ｙａｈｏｏ、Ｇｏｏｇｌｅなどのパブリックメールサーバへのプライベートメールがブロックされたり、ＹｏｕＴｕｂｅ（登録商標）、チャットプログラム、またはＴｗｉｔｔｅｒなどは企業のポリシーに従ってブロックされることがある。

・不安定なネットワークの場合、ＶＰＮオペレータによって手動でリセットされるまで、ＶＰＮが開かれ、発信者のデバイスに接続された常設セッションを保持することがある。これにより、後続の接続のための帯域幅が失われる、または接続料金が高額になる可能性がある。

【０１９５】

ネットワークの比較

【０１９６】

「オーバートップ」またはＯＴＴプロバイダによって提供される通信を、公衆ネットワークを使用してアドホックＶＰＮに接続する通信システムと比較すると、ＶＰＮリンクそれ自体以外では、両方の通信システムの大半はほぼ同じコンポーネントと接続を有している。具体的には、携帯電話、ＷｉＦｉ無線接続、ＷｉＦｉ基地局、有線接続、及びルータを含む発呼者の最後のマイルは、両方の実装において同じラストマイル接続を表す。同様に、相手方のラストマイルでは、発呼者の携帯電話、携帯電話接続、携帯電話基地局及びタワー、有線接続、及びルータは、インターネットバージョン及びＶＰＮバージョンの両方において同一である。主な相違点は、公衆ネットワークにおいて、ＶＰＮホスト間のセキュリティを確保された通信を構成するＶＰＮトンネルが、セキュリティが確保されていない通信接続を構成するサーバ及びルータに置き換えられていることである。別の相違点は、ＯＴＴ通信において、コールが即座に利用可能であり、ＶＰＮをセットアップし、コ

ールの前及び後にＶＰＮセッションを終了するために、ＶＰＮ追加ステップを使用する必要があることである。

【０１９７】

どちらの例でも、ラストマイル接続は、予期せぬコールのＱｏＳ、パケットスニッフィングを受けること、サイバー攻撃のリスクをもたらす。サーバ及びルータは、異なる場所の異なるＩＳＰによって管理される可能性が高いため、それらのサーバを既存の異なるクラウドとして解釈することができる。例えばＧｏｏｇｌｅ、Ｙａｈｏｏ、Ａｍａｚｏｎ、及びＭｉｃｒｏｓｏｆｔが所有し運営している公開ネットワークは、インターネットによって相互にリンクされているにもかかわらず、例えば「Ａｍａｚｏｎクラウド」は、互いに異なるクラウドと見なすことができる。

【０１９８】

比較的に普及していない競合ネットワークトポロジーであるピアツーピアネットワーク（ＰＰＮ）は、ルータまたはＩＳＰではなくＰＰＮによって管理されるパケットルーティングを備えた多数のピアから構成されるネットワークを含む。ピアツーピアネットワークは数十年にわたってハードウェアに存在していたが、インターネットサービスプロバイダの管理、コスト、規制を回避する手段としてこの概念を普及させたのはＮａｐｓｔｅｒであった。音楽著作権侵害のために米国政府の規制当局から訴えられたとき、Ｎａｐｓｔｅｒの創設者はそれをやめて、初期のＯＴＴキャリアＳｋｙｐｅに入った。その時、Ｓｋｙｐｅのネットワークは従来のＯＴＴからナップスターのようなＰＰＮに変換された。

【０１９９】

ＰＰＮ操作では、ＰＰＮへのログイン接続を行う全てのデバイスが、ＰＰＮに加わる１つのノードになる。例えば、ある地域において、ＰＰＮソフトウェアがインストールされた携帯電話がピアツーピアネットワークにログインすると、その地域の他の接続された全てのデバイスと同様にネットワークの一部となる。いずれかのデバイスによって呼び出されたコールは、１つのデバイスから別のデバイスに向かってホップして、目的地である別のＰＰＮ接続デバイスに到達する。例えば、ある携帯電話がそのＰＰＮ接続を使用して別のＰＰＮ接続デバイス（例えば、宛先携帯電話）を呼び出す場合、コールは、２者間のＰＰＮに物理的に配置された任意の装置を通る迂回経路に沿ってつながる。例えば、ある携帯電話から発するコールは、ＷｉＦｉによってＷｉＦｉ基地局を介して近くのデスクトップに、次に他の人のノートブックに、次にあるデスクトップから他のデスクトップに、最後に携帯電話基地局及びタワーを介して宛先携帯電話に接続する。このようにして、全てのルーティングはＰＰＮによって制御され、インターネットはルーティングの管理に関与しないものであった。両方の当事者が利用するので、ネットワークに接続するために使用されるＰＰＮソフトウェアは、ＶｏＩＰベースの音声通信のアプリケーションとしても機能する。

【０２００】

ある携帯電話が世界の反対側の非ＰＰＮ装置の携帯電話を呼び出そうとする場合、ルーティングは、特に海または山脈を越えてパケットを送信するために、いくつかのリンクでインターネットを必ず含むことがある。ある地域におけるルーティングの第１の部分は、以前の例と同様に、発呼者の携帯電話から開始し、ＷｉＦｉ基地局、デスクトップ、ノートブック、更に複数のデスクトップを介してルーティングされる。この時点で、最も近くのノートブックがネットワークに接続されている場合、コールはそれを介してルーティングされ、そうでない場合、コールは携帯電話基地局及びタワーを介して宛先携帯電話にルーティングされ、次に携帯電話基地局及びタワーに戻されてから、その先に送られる。

【０２０１】

通話が太平洋横断の場合には、コンピュータ及び携帯電話は海上でトラヒックを移送することができないので、通話はクラウド内のサードパーティのサーバ／ルータまでルーティングされ、更に別途のクラウド内のサードパーティのサーバ／ルータへの接続を通ってインターネットまで必然的にルーティングされることになる。例えば、宛先に近づくにあたって、コールはインターネットから出て、最初にデスクトップを介して宛先地域のＰＰ

Ｎに入り、ＷｉＦｉ、ノートブック、及び基地局に接続する。ＷｉＦｉはＰＰＮアプリを実行しないので、ＷｉＦｉに入る実際のパケットは、ＷｉＦｉサブネットにあるタブレットまたは携帯電話のいずれかに移動し、ＷｉＦｉに戻ってから有線接続を介して携帯電話基地局及びタワーに送信されなければならない。最後に、発呼者の携帯電話コールは、ＰＰＮ対応デバイスではない宛先携帯電話に接続する。これにより、ＰＰＮネットワークを出るため、接続はＰＰＮの「コールアウト」を構成する。このようなＰＰＮ方式を使用する場合、ＶＰＮのように、最初にＰＰＮログインを完了することによって、発呼側デバイスのＰＰＮネットワークへの登録を行う。その後、ＰＰＮアプリを使用してコールを発信することができる。ＰＰＮ方式の利点は、長距離通話を行うためにハードウェアがほとんどまたは全く必要ないことと、並びに、ＰＰＮに接続された全てのデバイスは、ＰＰＮオペレータをその状態、負荷及びレイテンシーに関して定期的に更新するので、ＰＰＮオペレータはパケットのルーティングを決定して遅延を最小限に抑えることができることである。

【０２０２】

この方式の欠点は、潜在的なセキュリティに対する脅威となり、コールレイテンシー及びコールＱｏＳに予測できない影響を及ぼす多くの未知ノードを含むネットワークをパケットが横断することである。そのため、パケット交換通信ネットワークでは、Ｓｋｙｐｅを除き、レイヤ３以上で動作するピアツーピアネットワークは一般的に採用されていない。

【０２０３】

アドホックＶＰＮプロバイダ、インターネットＯＴＴプロバイダ、及びＰＰＮピアネットワークの比較の概要を、対比させて以下の表に示す。

【０２０４】

【表２】

ネットワーク	仮想プライベート VPN	インターネット OTT	ピアツーピア PPN
ノード	公的/ホストされるサーバ	公的ルータ/サーバ	PPN ユーザ
ノードの能力	既知のインフラ	既知のインフラ	既知/未知混合未知
クラウド帯域幅	保証される	予測不可	予測不可
ラストマイル帯域幅	プロバイダ次第	プロバイダ次第	PPN 次第
レイテンシー	管理不可	管理不可	ベストエフォート
ネットワーク安定性	管理不可	管理不可、冗長	ベストエフォート
コール設定	複雑なログイン	要求なし	ログイン
ユーザ ID	ユーザ名	電話番号	ユーザ名
VoIP QoS	可変～良好	可変	可変
クラウドセキュリティ	暗号化ペイロードのみ	非暗号化	非暗号化
ラストマイルセキュリティ	非暗号化	非暗号化	非暗号化
スニッフィング可能部分	パケットヘッダ（クラウド） 全パケット（ラストマイル）	全パケット	全パケット

【０２０５】

前述された様に、ＶＰＮ及びインターネットは固定インフラストラクチャを構成するが、ピアツーピアネットワークのノードは、ログインしているユーザ及びＰＰＮに接続されているデバイスによって異なる。この表の内容から、ネットワークの高速長距離接続（例えば、海洋及び山脈を横切るネットワーク）は、ＶＰＮの場合にのみ契約上保証され、それ以外の場合には予測不可能である。ラストマイルの帯域幅は、インターネットプロバイダーとＶＰＮプロバイダ両方ともローカルプロバイダに依存しているが、ＰＰＮの場合は誰がログインしているかによって全く異なる。

【０２０６】

レイテンシー、すなわち連続して送信されるＩＰパケットの伝播遅延は、ＯＴＴ及びＶＰＮでは管理できないが、その理由は、プロバイダがラストマイルでのルーティングを制御するのではなく、ローカル通信会社またはネットワークプロバイダに依存しており、一方ＰＰＮは、特定の地域のその時間帯にオンラインになっているノード間でトラヒックを転送するためのベストエフォートを使用して、能力が限定されているからである。同様に、ネットワークの安定性については、ＰＰＮはネットワークを維持するためにトラヒックを再ルーティングする能力を有しているが、誰がログインしているかに左右される。一方、インターネットは本質的に冗長であり、配信を保証することはほぼ確実であるが、必ず

しも適時に配信されない。アドホックＶＰＮのネットワーク安定性は、ＶＰＮホストへの接続が許可されているノードの数によって異なる。これらのノードがオフラインになると、ＶＰＮは無効になる。

【０２０７】

コールセットアップの観点からは、インターネットは常に利用可能であり、ＰＰＮはコールを行う前にＰＰＮにログインする余分なステップを必要とし、ＶＰＮは複雑なログイン手順を伴うことがある。また、ほとんどのユーザは、ＶＰＮやＰＰＮで使用される別のログインＩＤではなく、ＯＴＴの電話番号の使用する機能を使いやすさの観点から有益と見いだしている。リストアップされた３つのネットワークは全て、一般に商用電話事業者を利用するよりはるかに遅れる可変ＶｏＩＰ　ＱｏＳに悩まされている。

【０２０８】

セキュリティの観点からは、３つの選択肢全てが悪く、ラストマイルは読み取り可能なアドレスとペイロードを有するパケットスニッフィングに完全にさらされている。ＶＰＮはクラウド接続の暗号化を提供するが、依然としてＶＰＮホストのＩＰアドレスを公開している。そのため、示されているネットワークの選択肢はいずれもセキュリティが確保されているとはみなされない。従って、暗号化は、レイヤ６プロトコルとして、またはレイヤ７アプリケーション自体の埋め込み部分としてハッキングやサイバー攻撃を防止するためにさまざまなアプリケーションで使用されている。

【０２０９】

暗号化に対する過剰な信頼

【０２１０】

ＩＰパケットを暗号化するかＶＰＮを確立するかにかかわらず、現在のネットワークセキュリティは、暗号化のみに依存しており、これは現代のパケット交換型の通信ネットワークの弱点の１つである。例えば、ＲＳＡ暗号化を攻撃する方法に関する多くの研究が行われている。素数を大きなサイズに制限することは、総当たり法を使用して解読Ｄ鍵コードを破る危険性を大幅に減少させるが、多項式因数分解法により、より小さな素数ベースの鍵に基づいて鍵を解くことに成功し得ることが実証された。「量子コンピューティング」の進化により、手ごろな時間でサイバー攻撃を行い、ＲＳＡベースの暗号鍵や他の暗号鍵を破壊する実用的な方法につながる懸念がある。

【０２１１】

これまでに存在していたコードの破損の危険に対抗するため、新しいアルゴリズムと、２００１年に米国ＮＩＳＴが採択した「高度暗号化標準」（ＡＥＳ暗号）などの「より大きな鍵」による暗号化方式が登場した。ラインダール暗号に基づいて、換字置換ネットワークとして知られる設計原理は、異なる鍵及びブロックサイズを使用する換字及び置換の両方を組み合わせる。現在の形では、アルゴリズムは１２８ビットの固定ブロック長を採用し、鍵長は１２８ビット、１９２ビット、及び５６ビットの可変長とし、それぞれに対応する、入力ファイル変換で使用されるラウンド回数は１０、１２、及び１４回とされている。実際問題として、ＡＥＳ暗号化は、ソフトウェアまたはハードウェアにおいて、任意の長さの鍵に対して、効率的かつ迅速に実行することができる。暗号方式では、２５６ビット鍵を使用するＡＥＳベースの暗号化をＡＥＳ２５６暗号化と呼ぶ。５１２ビット鍵を使用するＡＥＳ５１２暗号化も利用可能である。

【０２１２】

各新世代が、より良い暗号化方法を作り、より迅速にそれらを壊すべく暗号の水準を上げる一方、利益を得ようとするサイバー犯罪者は、暗号化されたファイルを破るために単にコンピューティングを使用するのではなく、目標に集中することが多い。前述のように、サイバーパイレーツは、パケットスニッフィングとポートスキャンを使用して、会話、企業サーバ、またはＶＰＮゲートウェイに関する貴重な情報を得ることができる。サイバープロファイリングにより、ネットワーク自体を攻撃するのではなく、企業のＣＦＯやＣＥＯのパーソナルコンピュータ、ノートブック、及び携帯電話のサイバー攻撃を開始する方が容易とも考えられる。埋め込みリンクを開くとマルウェアやスパイウェアを自動的に

インストールする電子メールを従業員に送信すると、その従業員が必ず接続して作業する必要のある「内部」からネットワークに入るので、ファイアウォールのセキュリティが完全に迂回されてしまう。

【０２１３】

データが変化せず、すなわち静的にネットワークを通過する場合にも、暗号化を破る可能性が高まる。例えば、図１のネットワークでは、パケット７９０、７９２、７９４、及び７９９内の基礎となるデータは、パケットがネットワークを通って移動するときに変更されないままである。図示された各データパケットは、作成時の元の順序から変更されていない、時間的に連続的に並べられたデータまたは音声のシーケンスを含む。データパケットの内容がテキスト形式の場合、シーケンス１Ａ－１Ｂ－１Ｃ－１Ｄ－１Ｅ－１Ｆの暗号化されていない平文ファイルを読むと、コミュニケ番号「１」の「読みやすい」テキストが得られる。データパケットの内容が音声である場合、シーケンス１Ａ－１Ｂ－１Ｃ－１Ｄ－１Ｅ－１Ｆ内の暗号化されていない平文ファイルを、対応する音声コーデック（本質的にソフトウェアベースのＤ／Ａ変換器）によって変換すなわち「再生」すると、オーディオファイル番号「１」の音声になる。

【０２１４】

いずれの場合においても、本開示を通じて、固定サイズのボックスによって表される各データスロットは、所定の数のビット、例えば２バイト（２Ｂ）長を有する。スロット当たりの正確なビット数は、ネットワーク内の各通信ノードが各データスロットのサイズを知っている限り柔軟に変えることができる。各データスロットに含まれているのは、音声、ビデオ、またはテキストのデータであり、これらは図面においては、数字とそれに続く文字によって特定される。例えば、図示のように、データパケット７９０の第１のスロットは、コンテンツ１Ａを含み、ここで数字「１」は特定の通信＃１を示し、文字「Ａ」は通信＃１のデータの第１部分を表す。同様に、データパケット７９０の第２のスロットは、コンテンツ１Ｂを含み、ここで数字「１」は特定の通信＃１を示し、文字「Ｂ」は通信＃１のデータの第２部分を表し、順序では１Ａの後にある。

【０２１５】

例えば、同じデータパケットが仮にコンテンツ「２Ａ」を含んでいた場合、データは、通信＃１とは無関係の異なる通信、具体的には通信＃２における第１のパケット「Ａ」を表す。同種の通信を含むデータパケット群である場合、例えば全てのデータが通信＃１用である場合は、異なる通信を混合するデータパケットよりも分析及び読み取りが容易である。データを適切な順序で順番に並べることで、サイバー攻撃者は、音声、テキスト、グラフィックス、写真、ビデオ、実行可能なコードなどのデータの性質を容易に解釈できる。

【０２１６】

さらに、図示された例では、パケットの送信元及び宛先ＩＰアドレスは一定であるため、すなわち、ゲートウェイサーバ２１Ａ及び２１Ｆに出入りするデータと同じ形式でネットワークを介して転送中にパケットが変更されないままであるため、また、基礎となるデータは変更しない為、ハッカーが、データパケットをインターセプトし、ファイルを分析して開くか、会話を聞く機会が増える。ただ単なる伝送及び単純なセキュリティ、つまり、保護する為に暗号化しか用いていないセキュリティは、サイバー攻撃の機会を増やす。何故なら、パケット交換型ネットワークとしての極端に簡素化されたインターネットの使用では、サイバー攻撃が成功する可能性が高くなるからである。

【０２１７】

<u>リアルタイムのネットワークと接続されたデバイスのセキュリティ確保</u>

【０２１８】

今日のパケット交換ネットワークを悩ましている過度のセキュリティ脆弱性に対処しながら、電話、ビデオ、及びデータ通信のサービス品質（ＱｏＳ）を向上させるために、ＩＰパケットルーティングを制御するための新しく革新的で体系的なアプローチ、すなわち個別の技術を含むグローバルネットワークを管理し、同時にエンドツーエンドのセキュリティを促進するアプローチが必要である。このような本発明のパケット交換ネットワーク

の目標は、以下の基準を含む。
１．リアルタイムの音声、ビデオ、及びデータトラヒックルーティングをネットワーク全体で動的に管理することを含む、グローバルなネットワークまたは長距離通信事業者のセキュリティとＱｏＳを保証すること。
２．通信ネットワークのラストマイルにおける「ローカルネットワークまたは電話会社」のセキュリティ及びＱｏＳを保証すること。
３．セキュリティが確保されていない回線に対するセキュリティを確保した通信の提供を含む、通信ネットワークの「ラストリンク」のセキュリティとＱｏＳを保証すること。
４．通信デバイスのセキュリティを保証し、不適格または不正なアクセスや使用を防ぐためにユーザを認証する。
５．不許可のアクセスを防止するために、デバイスまたはオンラインのネットワークまたはクラウドストレージにデータを格納する安全な手段の実現を容易化すること。
６．財務、個人、医療、バイオメトリックの全てのデータと記録を含む非公開の個人情報のセキュリティとプライバシーの保護を提供すること。
７．オンラインバンキング、ショッピング、クレジットカード、電子決済を含む全ての金融取引のセキュリティとプライバシーの保護を提供すること。
８．Ｍ２Ｍ（マシン・ツー・マシン）、Ｖ２Ｖ（ビークル・ツー・ビークル）、Ｖ２Ｘ（ビークル・ツー・インフラストラクチャ）通信を含む取引及び情報交換に、セキュリティ、プライバシー、及び必要に応じて匿名性を提供すること。

【０２１９】

上記の目標のうち、本開示に含まれる発明主題は、項目＃２に記載された第２のトピック、すなわち、「通信ネットワークのラストマイルにおけるローカルネットワークまたは電話会社のセキュリティ及びＱｏＳを保証すること。」に関する。このトピックは、リアルタイム通信パフォーマンスを犠牲にすることなく、ラストマイル接続のセキュリティを実現することと考えることができる。

【０２２０】

用語の説明

【０２２１】

文脈上別の解釈を必要としない限り、セキュリティを確保した動的ネットワークとプロトコルの記述で使用される用語は、以下の意味を有する。

【０２２２】

匿名データパケット：初めの送信元または最終宛先に関する情報が欠けているデータパケット。

【０２２３】

クライアントまたはクライアントデバイス：ラストマイルを介してＳＤＮＰクラウドに接続する端末。通常は携帯電話、タブレット、ノートブック、デスクトップ、またはＩｏＴデバイス。

【０２２４】

コンシールメント：スクランブル化、分割、ジャンクデータ挿入、暗号などのセキュリティ操作の組み合わせを用いて、ＳＤＮＰパケットのコンテンツ又はその一部を認識不可能にするエンコードのプロセス。

【０２２５】

復号（復号化）：データパケットを暗号文から平文に変換するために使用される数学的演算。

【０２２６】

非集約型データストレージ：複数の断片化されたファイルを異なるデータストレージノードに保管する前に、データファイルを断片化しそのコンテンツを隠蔽するプロセス。

【０２２７】

ＭＺサーバ：セレクタ、シードジェネレータ、キージェネレータ（鍵発生器）及びその他の共有の秘密の格納に使用されるＳＤＮＰネットワークまたはインターネットから直接

アクセスできないコンピュータサーバ。ＤＭＺは、「エアギャップ」サーバとも呼ばれ、有線ネットワークの接続またはアクセスのないコンピュータを指す。

【０２２８】

動的暗号化／復号化：データパケットがＳＤＮＰネットワークを通過する際に動的に変化する鍵に依存する暗号化及び復号化。

【０２２９】

動的混合（動的ミキシング）：ミキシングアルゴリズム（スプリットアルゴリズムの逆）が、混合データパケットが作成されるときの時間、状態、及びゾーンなどの状態に基づいてシードの関数として動的に変化するミキシングのプロセス。

【０２３０】

動的スクランブル化／アンスクランブル化：データパケットが作成された時間や作成されたゾーンなど、状態に応じて動的に変化するアルゴリズムに依存するスクランブル化とアンスクランブル化。

【０２３１】

動的分割：データパケットが複数のサブパケットに分割されるときの時間、状態、ゾーンなどの状態に基づいて、分割アルゴリズムがシードの関数として動的に変化する分割プロセス。

【０２３２】

暗号化：データパケットを平文から暗号文に変換するために使用される数学的演算。

【０２３３】

断片化データ転送：分割データと混合データのＳＤＮＰネットワークを介したルーティング。

【０２３４】

ジャンクデータ削除（または「デジャンキング」）：元のデータの復元のため、またはデータパケットの元の長さを回復するために、データパケットからジャンクデータを削除すること。

【０２３５】

ジャンクデータ挿入（または「ジャンキング」）：実際のデータ内容を難読化するため、またはデータパケットの長さを管理するために、意味のないデータをデータパケットに意図的に導入すること。

【０２３６】

鍵：秘密アルゴリズムを使用して鍵を生成する鍵生成器に時間などの状態を入力することによって生成される、偽装されたデジタル値。鍵は、セレクタからパケット内のデータを暗号化または復号化するアルゴリズムを選択するために使用される。鍵は、公的またはセキュリティを確保されていないラインを介して状態に関する情報を安全に渡すために使用できる。

【０２３７】

鍵交換サーバ：ネットワークオペレータのスパイ行為の可能性を防止するために、公開暗号鍵をクライアントに（特にクライアントが管理する鍵管理のため、すなわちクライアントベースのエンドツーエンド暗号化のため）、選択に応じて対称鍵暗号化を使用するサーバに配布するために使用される、ＳＤＮＰネットワークオペレータから独立したサードパーティにホストされるコンピュータサーバ。

【０２３８】

ラストリンク：クライアントのデバイスと、それが通信するネットワーク内の最初のデバイス（通常は無線タワー、ＷｉＦｉルータ、ケーブルモデム、セットトップボックス、またはイーサネット（登録商標）接続）との間のネットワーク接続。イーサネット（登録商標）通信の場合、ラストリンクは、物理的にケーブルモデム又は光ファイバモデムにケーブルで接続しているものを示す。ＷｉＦｉ接続の場合（例えば、喫茶店での接続）、ラストリンクは、ＷｉＦｉルータがＤＳＬ、ケーブル又は光ファイバネットワークと接続されている事を示す。無線セルラーネットワークの場合、ラストリンクは、セルラータワー

と携帯電話の間の無線リンク（例えば、３Ｇや４Ｇ／ＬＴＥ接続）を示す。
【０２３９】
ラストマイル：ラストリンクを含むＳＤＮＰゲートウェイ（又は他の種類のネットワーク又はクラウド）とクライアント間のネットワーク接続。通常、ラストマイルは、ローカル電話会社及びケーブルテレビ会社（例えば、コムキャストケーブル、ベライゾンモバイル、コリアテレコム、ブリティッシュテレコム等）が所有し管理するネットワークを介する通信を示す。
【０２４０】
混合（ミキシング）：異なるソース及びデータタイプからのデータの結合により、認識できないコンテンツを有する１つの長いデータパケット（または一連のより短いサブパケット）を生成すること。以前に分割されたデータパケットをミキシングさせて元のデータコンテンツを復元する場合もある。ミキシング操作には、ジャンクデータの挿入、削除、及び解析も含まれ得る。
【０２４１】
複数ＰＨＹ又はマルチＰＨＹ：複数の物理媒体（光ファイバと４Ｇ、異なるＷｉＦｉチャネルと波数、４ＧとＷｉＦｉ、イーサネット（登録商標）とＷｉＦｉなど）を介して関連したシーケンシャルデータパケットを交互転送する通信を指す。
【０２４２】
パース（構文解析）：データパケットを格納または送信のために短いサブパケットに分割する数値演算。
【０２４３】
ルータ：ＩＰヘッダに特定されている宛先アドレスへデータグラムをルーティングするデバイス。ＳＤＮＰネットワーク外でのデータルーティングに関しては、使用されているＩＰアドレスは有効なインターネットＩＰアドレス（つまり、ＤＮＳサーバにより認識されるアドレス）又はローカルネットワークプロバイダ（例えば、コムキャストが、所有しているケーブル／光ファイバネットワーク内の通信に、コムキャスト内部のＩＰアドレスを割り当てる。）により割り当てされたＮＡＴアドレスである場合がある。
【０２４４】
スクランブル化：データパケット内のデータセグメントの順序またはシーケンスがその自然順序から認識不可能な形式に変更される操作。
【０２４５】
分割：データパケット（または一連のシリアルデータパケット）が複数のサブパケットに分割され、多数の宛先にルーティングされる操作。分割操作には、ジャンクデータの挿入や削除も含まれ得る。
【０２４６】
ソフトスイッチ：通信スイッチ及びルータの機能を実行する実行可能コードを含むソフトウェア。
【０２４７】
ＳＤＮＰ：本発明に従って作られた高セキュリティの通信ネットワークを意味する「Ｓｅｃｕｒｅ Ｄｙｎａｍｉｃ Ｎｅｔｗｏｒｋ ａｎｄ Ｐｒｏｔｏｃｏｌ（セキュリティを確保した動的ネットワーク及びプロトコル）」の頭字語。
【０２４８】
ＳＤＮＰアドレス：ＳＤＮＰクラウド又はラストマイルを介してＳＤＮＰパケットをルーティングする為に用いられるアドレス。このアドレスは、次の宛先デバイスのアドホックＩＰアドレスであり、つまり、シングルホップを実行する為だけに必要な情報を含む。
【０２４９】
ＳＤＮＰ管理サーバ：実行可能コードと共有秘密をグローバルに、または特定のゾーンに分散するために使用されるコンピュータサーバ。
【０２５０】
ＳＤＮＰブリッジノード：１つのＳＤＮＰクラウド（又はゾーン）を異なるセキュリテ

ィクレデンシャル情報を持つ別のＳＤＮＰクラウド（又はゾーン）に接続するＳＤＮＰノード。
【０２５１】
ＳＤＮＰクライアントまたはクライアントデバイス：一般的にネットワークのラストマイルを介して接続するＳＤＮＰクラウドに接続するために、ＳＤＮＰアプリケーションを実行するネットワーク接続デバイス（通常は携帯電話、タブレット、ノートブック、デスクトップ、またはＩｏＴデバイス）。
【０２５２】
ＳＤＮＰクラウド：ＳＤＮＰ通信ノード操作を実行するためのソフトスイッチ実行可能コードを実行している相互接続されたＳＤＮＰサーバのネットワーク。
【０２５３】
ＳＤＮＰゲートウェイノード：ＳＤＮＰクラウドをラストマイルを介するクライアントデバイスに接続するＳＤＮＰノード。ＳＤＮＰゲートウェイノードは、ＳＤＮＰクラウドとラストマイルの少なくとも２つのゾーンにアクセスする必要がある。
【０２５４】
ＳＤＮＰメディアノード：シグナリングサーバまたはシグナリング機能（暗号化／復号、スクランブル化／アンスクランブル化、ミキシング／分割、タグ付け、およびＳＤＮＰヘッダ及びサブヘッダの生成を含む）を実行する別のコンピュータからの命令に従って、特定の識別タグを有する着信データパケットを処理するソフトスイッチ実行可能コード。ＳＤＮＰメディアノードは、特定のタグを有する着信データパケットを識別し、新たに生成されたデータパケットを次の宛先に転送する役割を果たす。
【０２５５】
ＳＤＮＰメディアサーバ：ＳＤＮＰメディアノードの機能をデュアルチャネル及びトライチャネル通信で実行し、シングルチャネル通信でＳＤＮＰシグナリングノード及びＳＤＮＰネームサーバノードのタスクを実行するソフトスイッチをホストするコンピュータサーバ。
【０２５６】
ＳＤＮＰネームサーバ：トライチャネル通信でＳＤＮＰネームサーバノードの機能を実行するソフトスイッチをホストするコンピュータサーバ。
【０２５７】
ＳＤＮＰネームサーバノード：ＳＤＮＰクラウドに接続された全てのＳＤＮＰデバイスの動的リストを管理するソフトスイッチ実行可能コード。
【０２５８】
ＳＤＮＰネットワーク：ＳＤＮＰクラウドだけでなく、ラストリンクとラストマイル通信を含む、クライアント－クライアント間の高セキュリティの通信ネットワーク全体。
【０２５９】
ＳＤＮＰノード：コンピュータサーバ上で動作するソフトウェアベースの「ソフトスイッチ」を含むＳＤＮＰ通信ノード、あるいはＳＤＮＰネットワークに接続され、メディアノード、シグナリングノード、またはネームサーバノードのいずれかのＳＤＮＰノードとして機能するハードウェアデバイス。
【０２６０】
ＳＤＮＰサーバ：ＳＤＮＰメディアサーバ、ＳＤＮＰシグナリングサーバ、またはＳＤＮＰネームサーバのいずれかを備え、適切なソフトスイッチ機能をホストしてＳＤＮＰノードとして動作するコンピュータサーバ。
【０２６１】
ＳＤＮＰシグナリングノード：当事者間のコールまたは通信を開始し、コール元（発呼元）基準及びノード間伝播遅延の動的テーブルに基づいて、断片化されたデータ転送の複数のルートの全てまたは一部を決定し、ＳＤＮＰメディアの着信および発信データパケットの管理方法。
【０２６２】

ＳＤＮＰシグナリングまたはシグナリングサーバ：デュアルチャネルおよびトライチャネルＳＤＮＰ通信でＳＤＮＰシグナリングノードの機能を実行し、デュアルチャネル通信でＳＤＮＰネームサーバノードの任務を実行するソフトスイッチをホストするコンピュータサーバ。

【０２６３】

ＳＤＮＰタグ：ソースアドレス、ＳＤＮＰ　ｚｉｐコード、又は着信データパケット又はそのサブパケットを識別する為に用いられたコード。

【０２６４】

セキュリティ操作：パケットが作成されたゾーン又は状態（ステート）に関連する状態に依存するセキュリティクレデンシャル情報を用いて隠蔽する（または隠蔽されたパケットのコンテンツを復旧する）為にデータパケットを変更する処理。

【０２６５】

セキュリティ設定またはセキュリティクレデンシャル情報：シードジェネレータやキージェネレータが、秘密アルゴリズムを、常に変化するネットワーク時間などの入力状態と共に使用して生成し、従ってパブリックまたはセキュリティが確保されていないラインを介して安全に送信することが可能な、シードや鍵などのデジタル値。

【０２６６】

シード（Ｓｅｅｄ）：秘密アルゴリズムを使用してシードを生成するシードジェネレータに、時間などの状態を入力することによって生成される偽装デジタル値。シードは、セレクタからパケット内のデータをスクランブル化または分割するためのアルゴリズムを選択するために使用される。シードは、パブリックまたはセキュリティが確保されていないラインを介して状態に関する情報を安全に渡すために使用できる。

【０２６７】

セレクタ：共有秘密情報の一部であるとともに、１つまたは複数のパケットのスクランブル化、アンスクランブル化、暗号化、復号、分割、またはミキシングのための特定のアルゴリズムを選択するためにシードまたは鍵と共に使用される可能性のある、スクランブル化、暗号化または分割アルゴリズムのリストまたはテーブル。

【０２６８】

共有秘密（情報）：ＳＤＮＰネットワークまたはインターネット経由でアクセスできないＤＭＺサーバにローカルに保存されるシードジェネレータ、キージェネレータ、ゾーン情報、およびアルゴリズムシャッフルプロセスで使用されるアルゴリズムのみならず、スクランブル化／アンスクランブル化、暗号化／復号化、および混合／分割アルゴリズムのテーブルまたはセレクタを含む、ＳＤＮＰノード操作に関する機密情報。

【０２６９】

シングルＰＨＹ：光ファイバ、イーサネット（登録商標）、ＷｉＦｉまたはセルラーネットワークなどの唯一の物理的メディアを介して関連したデータパケットを転送する通信。

【０２７０】

ステート（状態）：シードや鍵などのセキュリティ設定を動的に生成するために、また混合、分割、スクランブル化、暗号化などの特定のＳＤＮＰ操作のアルゴリズムを選択するために使用される、ロケーション、ゾーン、またはネットワーク時間などの入力。

【０２７１】

時間（Ｔｉｍｅ）：ＳＤＮＰネットワークを介して通信を同期させるために使用されるユニバーサルネットワーク時間。

【０２７２】

アンスクランブル化：スクランブル化されたデータパケット内のデータセグメントを元の順序またはシーケンスに復元するために使用されるプロセス。アンスクランブル化はスクランブル化の逆関数である。

【０２７３】

ゾーン：共通のセキュリティクレデンシャル情報と共有秘密を共有する特定の相互接続されたサーバのネットワーク。ラストマイル接続は、ＳＤＮＰクラウドとは別のゾーンを

含む。

【０２７４】

セキュア動的ネットワーク及びプロトコル（Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｎｅｔｗｏｒｋ　Ａｎｄ　Ｐｒｏｔｏｃｏｌ：ＳＤＮＰ）の設計

【０２７５】

リアルタイムでのパケット遅延を最小限に抑え、安定した呼接続を確実にし、かつ高信頼性の音声通信及び映像ストリーミングを伝送すると共に、パケット交換通信に対するサイバー攻撃及びハッキングを防止するために、本開示に係るセキュリティが確保された（以降、「セキュア」とも称する）動的ネットワーク及びプロトコル、すなわちＳＤＮＰは、下記の複数の処理原則に基づいて設計した。

・リアルタイム通信は、常に、遅延時間が最も短い経路を使用して行うべきである。

・データパケットの不正な検査またはスニッフィングによって、パケットの送信元、宛先、及びその内容が分からないようにすべきである。

・データパケットのペイロードは、適当な期間にハッキングされる危険を冒さずに、別個の暗号化アルゴリズムを使用して動的に再暗号化（すなわち、復号及びその後の再度の暗号化）するべきである。

・復号された後であっても、全てのデータパケットのペイロードは、複数の会話と、無関係なデータと、ジャンクパケットフィラーとの組み合わせを動的にスクランブル化することにより、依然として判読不能なペイロードである。

【０２７６】

上記のガイドラインの実施は、下記の様々な実施形態のいくつかまたは全てに含まれる様々なユニークな方法、機能、特徴、及び実行を含む。

【０２７７】

ＳＤＮＰは、インターネットを介してアクセスできないプロプライエタリコマンド及び制御ソフトウェアを使用して実現される通信会社（すなわち通信システム）のソフトスイッチ機能を含む、１または複数の専用クラウドを使用する。

・全てのクラウド内通信は、ＤＮＳにより認識されるＩＰアドレスではなく、ＳＤＮＰアドレス及び動的ポート（すなわちプロプライエタリＮＡＴアドレス）に基づいて、プロプライエタリクラウド内の専用のＳＤＮＰパケットルーティングを使用して行われる。ＳＤＮＰアドレスは、インターネットを通じてまたはＳＤＮＰクラウドの外部では、使用またはルーティングすることはできない。

・ＳＤＮＰネットワークは、全てのリアルタイム通信を、頻繁に識別し、遅延時間が最も短い経路を使用して動的にルーティングする。

・クラウドツークラウド及びラストマイル通信を除いては、セキュアまたはリアルタイム通信はＳＤＮＰクラウドの外部またはインターネットを介してルーティングされず、一般的に不可視アドレスによるシングルホップルーティングを使用する。

・データパケット内に含まれるルーティングデータは、互いに隣接する２つのデバイス間のシングルホップのためのルーティングを識別し、前の及び次のサーバのＳＤＮＰまたはＩＰアドレスのみを識別する。

・発呼者または着呼者の電話番号またはＩＰアドレス、すなわちクライアントの各ソースアドレス及び宛先アドレスは、ＩＰパケットのヘッダ内にも、暗号化されたペイロード内にも存在しない。

・命令及び制御に関連する共有秘密は、インターネットを介してアクセスできないセキュアＤＭＺサーバ内にインストールされたシステムソフトウェア内に存在する。

・ＳＤＮＰパケット通信は、互いに異なる３つのチャンネル、すなわち、ＳＤＮＰクラウド内のエレメントの識別に使用される「ネームサーバ」、コンテンツ及びデータのルーティングに使用される「メディアサーバ」、及びにパケット及び発呼の命令及び制御に使用される「シグナリングサーバ」を通じて行うことができる。

・ルーティング情報が、鍵及び数値シード（必要に応じて）と共に、発呼または通信の前に、かつコンテンツとは別個に、独立的なシグナリングチャンネルを通じて全ての参加メ

ディアサーバに供給される。シグナリングサーバは、メディアサーバに対して、ネットワークを横断するパケットの前の及び次の宛先のみを提供する。
・メディアパケットは、他のソースからの断片化されたデータ種類が異なるデータを含む他のパケットと動的に混合及び再混合された、会話、ドキュメント、テキスト、またはファイルの一部しか表さない断片化されたデータを含む。
・ファースト及びラストマイル通信を保護するために、シグナリングサーバ関連通信をメディア及びコンテンツ関連パケットから分離することを含む特別なセキュリティ方法が用いられる。
・パケット伝送は、コンテンツ種類依存性であり、音声及びリアルタイム映像またはストリーミングは改良型ＵＤＰに基づくが、パケット損失または遅延の影響を受けやすいシグナリングパケット、命令及び制御パケット、データファイル、アプリケーションファイル、システムファイル、及び他のファイルは、ＴＣＰ伝送を用いる。
・デバイスが本当のクライアントでありクローンではないことを確認すると共に、通信を行っている者がそのデバイスの真のオーナーであり偽者ではないことを認証するために、特定のセキュリティ及び認証方法が用いられる。
【０２７８】
ＶｏＩＰ及びリアルタイムアプリケーションにおいて低遅延及び高ＱｏＳを有するセキュア通信を確実にするために、本開示に係る「セキュア動的ネットワーク及びプロトコル（Ｓｅｃｕｒｅ Ｄｙｎａｍｉｃ Ｎｅｔｗｏｒｋ Ａｎｄ Ｐｒｏｔｏｃｏｌ）」すなわちＳＤＮＰは、下記の構成要素を含む本発明に係る「動的メッシュ」ネットワークを使用する。
・動的に適合可能なマルチパス、及び遅延を最小化したメッシュルーティング
動的なパケットスクランブル化
・パケット分割、混合、パース、及びジャンクビットパケットフィラー（ｊｕｎｋ ｂｉｔ ｐａｃｋｅｔ ｆｉｌｌｅｒｓ）を使用した動的な断片化
・ネットワークまたはクラウドの全体に渡っての動的なノード内ペイロード暗号化
アドレス偽装及びニーズツーノウ（ｎｅｅｄ－ｔｏ－ｋｎｏｗ）ルーティング情報による動的ネットワークプロトコル
・メディア及びコンテンツを、シグナリング、命令及び制御、及びネットワークアドレスから分離した複数チャンネル通信
・データ種類に特有のフィーチャ及びコンテキスチュアルルーティングによる動的に適合可能なリアルタイム通信プロトコル
・ユーザ鍵管理によるクライアント暗号化ペイロードのサポート
・混雑したネットワークでの高ＱｏＳのための軽量音声ＣＯＤＥＣ
【０２７９】
上述したように、ＳＤＮＰ通信は、マルチルートまたはメッシュ伝送に依存して、データパケットを動的にルーティングする。本発明に係るＳＤＮＰ通信では、インターネットＯＴＴ及びＶｏＩＰに使用される単一経路のパケット通信とは対照的に、データパケットのコンテンツは、情報を含んでいるコヒーレントパケットによって共通のソースまたは発呼者から直列的に搬送されるのではなく、断片化された形態で搬送される。複数のソース及び発呼者から送信されたコンテンツを動的に混合及び再混合することにより、データ種類が互いに異なるデータ、コンテンツ、音声、映像、及びファイルとジャンクデータフィラーとを組み合わせた不完全な断片が生成される。本開示に係るデータ断片化及び通信の利点は、暗号化及びスクランブル化されていないデータパケットであっても、それらはデータ種類が互いに異なる互いに無関係なデータの組み合わせであるため、解読するのはほぼ不可能だということである。
【０２８０】
断片化されたパケットの混合及び分割を、パケットスクランブル化及び動的暗号化と組み合わせることにより、動的に暗号化、スクランブル化、断片化されたデータのハイブイリッド化されたパケットは、そのデータの生成、パケット化、及び動的再パケット化に使

用された共有秘密、鍵、数値シード、時間、及びステート変数を持っていない任意の者または観察者には全く判読及び解読不能な意味を持たないパケットとなる。

【０２８１】

さらに、各パケットの断片化コンテンツと、それの生成に使用された秘密情報は、新しい断片及び新しいセキュリティ要素（例えば、変更されたシード、鍵、アルゴリズム、及び秘密情報）によりパケットが再構成されるまでの一秒足らずの間でのみ有効である。このように、サイバーパイレーツがステート依存性ＳＤＮＰデータパケットを解読するのに要する時間が制限されることにより、ＳＤＮＰのセキュリティはさらに高められる。サイバーパイレーツは、十分の１秒で何万年分（解読に要する時間の１２乗）もの計算を実行しなくてはならないためである。

【０２８２】

上述した方法の組み合わせは、静的な暗号化により実現されるセキュリティよりもはるかに高いレベルの多次元的なセキュリティを可能にする。したがって、本開示に係るセキュア動的ネットワーク及びプロトコルは、本明細書中では、「ハイパーセキュア（ｈｙｐｅｒ－ｓｅｃｕｒｅ）」ネットワークとも称す。

【０２８３】

デバイスパケットのスクランブル化

【０２８４】

本発明によれば、パケット交換網ネットワークを介したセキュア（セキュリティが確保された）通信は、ハッキング防止及びセキュリティ確保のいくつかの要素に依存し、そのうちの１つはＳＤＮＰパケットのスクランブル化を含む。ＳＤＮＰパケットのスクランブル化は、データセグメントの配列を並べ替えて、情報を判読不能で無益なものにすることを含む。図２Ａに示すように、スクランブル化されていないデータパケット９２３を、スクランブル化操作９２４（Ｓｃｒａｍｂｌｉｎｇ　Ｐｒｏｃｅｓｓ）により処理し、スクランブル化データパケット９２５を生成する。このスクランブル化操作９２４は、任意のアルゴリズム、数値的手法、またはシーケンシング手法を使用することができる。アルゴリズムは、静的な方程式であり得、例えばスクランブル化が実施された時間（ｔｉｍｅ）９２０などの「ステート（Ｓｔａｔｅ）」に基づく動的変数または数値シード、または、シード生成器（Ｓｅｅｄ　Ｇｅｎｅｒａｔｏｒ）９２１により例えばスクランブル化が実施された時間９２０などのステートに基づくアルゴリズムを使用して生成された数値シード（ｓｅｅｄ）９２９を含み得る。例えば、各データが、単調増加するユニークな数に変換される場合は、全てのシード９２９はユニークなものとなる。時間９２０及びシード９２９は、特定のアルゴリズムを選択及び識別するのに使用され、また、利用可能なスクランブル化方法、すなわちスクランブル化方法リスト９２２（Ｓｃｒａｍｂｌｉｎｇ　Ａｌｇｏｒｉｔｈｍｓ）から特定のスクランブル化操作９２４を選択するのにも使用される。データフロー図では、図示の便宜上、このパケットスクランブル化操作及びシーケンスは、パケットスクランブル化操作９２６（Ｐａｃｋｅｔ　Ｓｃｒａｍｂｌｉｎｇ）として概略的または記号的に表示する。

【０２８５】

図２Ｂは、スクランブル化操作９２４と逆の操作であるアンスクランブル化操作９２７（Ｕｎｓｃｒａｍｂｌｉｎｇ　Ｐｒｏｃｅｓｓ）を示す。このアンスクランブル化操作９２７は、スクランブル化データパケット９２５の生成に使用されたステート（時間）９２０及びそれに対応するシード９２９を再使用してスクランブル化を解除し、スクランブル化が解除されたデータである、スクランブル化されていないデータパケット９２３を生成する。パケットスクランブル化に使用されたものと同一のステート（時間）９２０を使用して、アンスクランブル化操作９２７では、スクランブル化方法リスト９２２から選択される、スクランブル化に使用されたものと同一のスクランブル化方法を再び使用しなければならない。スクランブル化アルゴリズムリスト９２２では「スクランブル化」という用語が用いられているが、このアルゴリズムテーブルは、「アンスクランブル化」の実施に必要とされる、スクランブル化と逆の操作を識別して選択するのに使用される。すなわち

、スクランブル化アルゴリズムリスト９２２は、データパケットのスクランブル化及びアンスクランブル化の両方に必要な情報を含んでいる。この２つの操作は、互いに逆の順番で実施される同一のステップを含むので、スクランブル化アルゴリズムリスト９２２は、「スクランブル化／アンスクランブル化」アルゴリズムリスト９２２と称することもできる。しかしながら、明確にするために、このテーブル（リスト）は、スクランブル化の機能についてのみ称し、それと逆の機能（アンスクランブル化）については称さないものとする。

【０２８６】

アンスクランブル化操作９２７の実施のために選択されたスクランブル化アルゴリズムが、パケットスクランブル化に使用されたアルゴリズムと一致しない場合、あるいは、シード９２９またはステート（時間）９２０が、スクランブル化が実施された時間と一致しない場合、アンスクランブル化操作は、元のスクランブル化されていないデータパケットの９２３の復号に失敗し、パケットデータが失われることとなる。データフローズ図では、図示の便宜上、このパケットアンスクランブル化操作及びシーケンスは、パケットアンスクランブル化操作９２８（Ｐａｃｋｅｔ　Ｕｎｓｃｒａｍｂｌｉｎｇ）として概略的または記号的に表示した。

【０２８７】

本発明によれば、スクランブル化操作が可逆的である限り、すなわち、各ステップを元の処理のときと逆の順番で繰り返すことにより、データパケット内の各データセグメントをその元の適切な位置に戻すことができる限り、スクランブル化操作の実施に数値アルゴリズムが使用される。数学的には、許容可能なスクランブル化アルゴリズムは、可逆的なものである。すなわち、例えば下記のように、関数Ｆ（Ａ）がその逆関数Ｆ－１（Ａ）を有するか、またはその逆関数に変換できる。

Ｆ－１［Ｆ（Ａ）］＝Ａ

【０２８８】

これは、関数Ｆにより処理されたデータファイル、配列、文字列、ファイル、またはベクターＡは、その後、逆関数Ｆ－１を使用して処理することにより、数値及び配列が壊れていない元の入力Ａに復号できることを意味する。

【０２８９】

このような可逆操作の例は、図２Ｃに示す静的スクランブル化アルゴリズムであり、ミラーリングアルゴリズム及び位相シフトアルゴリズムを含む。ミラーリングアルゴリズムでは、あるデータセグメントは、ミラーリング処理の係数すなわち「Ｍｏｄ」により定義された対称線を中心とした鏡像となるように、他のデータセグメントとスワップ（位置交換）される。図示したＭｏｄ－２ミラーリング（Ｍｏｄ－２　Ｍｉｒｒｏｒｉｎｇ）では、元の入力データパケット９３０の互いに連続する２つのデータセグメント毎にスワップされる。つまり、１番目及び２番目のデータセグメント間、３番目及び４番目のデータセグメント間、５番目及び６番目のデータセグメント間（以下同様）の位置、すなわち数学的には、１．５番目、３．５番目、５．５番目、・・・、（１．５＋２ｎ）の位置に位置する対称線を中心として、データセグメント１Ａ及び１Ｂの位置が交換され、データセグメント１Ｃ及び１Ｄの位置が交換され、データセグメント１Ｅ及び１Ｆの位置が交換され（以下同様）、これにより、スクランブル化された出力データパケット９３５が生成される。

【０２９０】

Ｍｏｄ－３ミラーリング（Ｍｏｄ－３　Ｍｉｒｒｏｒｉｎｇ）では、互いに連続する３つのデータセグメント毎に、その１番目及び３番目のデータセグメントの位置が交換され、それらの中間の２番目のパケットは元の位置から変更されない。したがって、データセグメント１Ａ及び１Ｃの位置が交換されるが、データセグメント１Ｂは元の位置（互いに連続する３つのデータセグメントにおける真ん中の位置）から変更されない。同様に、データセグメント１Ｄ及び１Ｆの位置が交換されるが、データセグメント１Ｅは元の位置（互いに連続する３つのデータセグメントにおける真ん中の位置）から変更されない。この

ようにして、スクランブル化されたデータパケット出力９３６が生成される。Ｍｏｄ－３ミラーリングでは、ミラーリングの対称線は、２番目、５番目、８番目、・・・、（２＋３ｎ）番目の位置に位置する。

【０２９１】

Ｍｏｄ－４ミラーリング（Ｍｏｄ－４　Ｍｉｒｒｏｒｉｎｇ）では、互いに連続する４つのデータセグメント毎に、１番目及び４番目のデータセグメントの位置が交換され、かつ２番目及び３番目のデータセグメントの位置が交換され、これにより、入力データパケット９３１からスクランブル化された出力データパケット９３７が生成される。したがって、データセグメント１Ａはデータセグメント１Ｄと位置が交換され、データセグメント１Ｂはデータセグメント１Ｃと位置が交換される。Ｍｏｄ－４ミラーリングでは、ミラーリングの対称線は、互いに連続する４つのデータセグメントにおける２番目のデータセグメントと３番目のデータセグメントとの間（例えば、２番目のデータセグメントと３番目のデータセグメントとの間、６番目のデータセグメントと７番目のデータセグメントとの間）の位置、すなわち数学的には、２．５番目、６．５番目、・・・、（２．５＋４ｎ）番目の位置に位置する。Ｍｏｄ－ｍミラーリング（Ｍｏｄ－ｍ　Ｍｉｒｒｏｒｉｎｇ）では、入力データパケット９３２のｍ番目のデータセグメントが、最初の、すなわち０番目のデータセグメントと位置が交換され、ｎ番目のデータセグメントが（ｍ－ｎ）番目のデータセグメントと位置が交換され、これにより、スクランブル化された出力データパケット９３８が生成される。

【０２９２】

図２Ｃには、フレームシフトと呼ばれる別のスクランブル化方法がさらに示されている。このフレームシフトでは、各データセグメントは、左側または右側に、１フレーム、２フレーム、またはそれ以上のフレームだけ位置がシフトされる。例えば、単一フレーム位相シフト（１－Ｆｒａｍｅ　Ｐｈａｓｅ　Ｓｈｉｆｔ）では、各データセグメントは、１フレームだけ位置がシフトされる。具体的には、１番目のデータセグメントは、２番目のデータセグメントの位置に位置がシフトされ、２番目のデータセグメントは、３番目のデータセグメントの位置に位置がシフトされ（以下同様）、これにより、スクランブル化された出力データパケット９４０が生成される。なお、入力データパケット９３０の最後のフレーム（図示した例では、フレーム１Ｆ）は、１番目のデータセグメント１Ａの位置に位置がシフトされる。

【０２９３】

２フレーム位相シフト（２－Ｆｒａｍｅ　Ｐｈａｓｅ　Ｓｈｉｆｔ）では、入力データパケット９３０の１番目のデータセグメント１Ａは、３番目のデータセグメント１Ｃの位置に２フレーム分位置がシフトされ、４番目のデータセグメント１Ｄは、スクランブル化された出力データパケット９４１の最後（６番目）のデータセグメントの位置に位置がシフトされる。そして、最後から２番目（５番目）のデータセグメント１Ｅは、１番目のデータセグメントの位置に位置がシフトされ、最後（６番目）のデータセグメント１Ｆは、２番目のデータセグメントの位置に位置がシフトされる。同様に、４フレーム位相シフト（４－Ｆｒａｍｅ　Ｐｈａｓｅ　Ｓｈｉｆｔ）では、入力データパケット９３０の各データセグメントは４フレーム分位置がシフトされ、１番目のフレーム１Ａはフレーム１Ｅと位置が交換され、フレーム１Ｂはフレーム１Ｆと位置が交換され、フレーム１Ｃはフレーム１Ａと位置が交換され（以下同様）、これにより、スクランブル化された出力データパケット９４２が生成される。最大フレーム位相シフト（Ｍａｘｉｍｕｍ　Ｐｈａｓｅ　Ｓｈｉｆｔ）の場合、１番目のフレームＡは最後のフレームと位置が交換され、２番目のフレーム１Ｂは１番目のフレームの位置に位置がシフトされ（すなわち、出力データパケット９４３の最初のフレームとなり）、３番目のフレームは２番目のフレームの位置に位置がシフトされる（以下同様）。１つのフレームが最大位相を超えて位相シフトされると、出力データは入力データから変化しない。図示した例は、位相シフトのシフト方向は右側である。このアルゴリズムでは、位相シフトのシフト方向は左側であってもよいが、その場合は、結果は異なるものとなる。

【０２９４】
本開示に係る上述したアルゴリズム及び同様の方法は、本明細書では、静的スクランブル化アルゴリズムと称する。スクランブル化操作が１回だけ行われ、それにより、入力データセットをユニークな出力に変換するからである。さらに、上述したアルゴリズムでは、スクランブル化の実施方法の決定は、データパケットの値に依存しない。図２Ｄに示すように、本発明によれば、パラメータ的なスクランブル化は、スクランブル化方法が、データパケット自体に含まれているデータに由来する値に基づいて、可能性があるスクランブル化アルゴリズム（例えば、Ｓｏｒｔ＃Ａ、Ｓｏｒｔ＃Ｂなど）のテーブルから選択されることを意味する。例えば、各データセグメントを、そのデータセグメントに含まれるデータの計算に基づいて、数値に変換することができると仮定する。データセグメントの数値を決定するための１つの可能性があるアプローチは、データセグメント内のビットデータの１０進数または１６進数相当値を用いることである。データセグメントが多重項を含む場合、数値相当値は、データセグメント中の数字を合計することにより求められる。データセグメントのデータはその後単一の数字または「パラメータ」に組み合わされ、その後、使用するスクランブル化方法の選択に用いられる。
【０２９５】
図示した例では、スクランブル化されていないデータパケット９３０は、ステップ９５０において、各データセグメントについての数値を含んでいるデータテーブル９５１にパラメータ的に変換される。図示のように、０番目のフレームであるデータセグメント１Ａは、数値「２３」を有し、１番目のフレームであるデータセグメント１Ｂは、数値「１２５」を有する（以下同様）。その後、ステップ９５２において、データパケット９３０全体についての単一のデータパケット値が抽出される。図示した例では、合計値９５３（Ｓｕｍ）の「１００２」は、テーブル９５１からの全データセグメント値の線形合計、すなわちパラメータ値を合算したものを示す。ステップ９５４では、このパラメータ値（すなわち合計値９５３）を条件テーブル（すなわち、ソフトウェアでは予め規定された条件付実行構文（ｉｆ－ｔｈｅｎ－ｅｌｓｅ　ｓｔａｔｅｍｅｎｔｓ））のセットと比較して、つまり、合計値９５３をテーブル９５５における多数の非重複数値範囲と比較して、使用するべきソートルーチンを決定する。この例では、パラメータ値「１２００」は、１０００から１４９９の範囲に入るので、ソート＃Ｃ（Ｓｏｒｔ＃Ｃ）を使用するべきであると決定される。ソートルーチンが選択されると、パラメータ値はもはや不要となる。スクランブル化されていない入力データ９３０はその後、ステップ９５６において、選択された方法でスクランブル化され、スクランブル化されたデータパケット出力９５９が生成される。図示した例では、テーブル９５７に要約されたソート＃Ｃは、各データセグメントの相対移動のセットを含む。このセットでは、スクランブル化されたデータパケット９５９の第１のデータセグメント、すなわち０番目のフレームは、左側に３フレーム分移動（３つシフト）するように定義されている。１番目のフレームは、元の位置から変更されない（すなわち移動しない）データセグメント１Ｂを含む。２番目のフレームは、元の位置から左側に２つシフトしたデータセグメント１Ｅを含む。３番目のフレームも同様であり、３番目のフレームは、元の位置から左側に２つシフトしたデータセグメント１Ｆを含む。スクランブル化されたデータパケット出力９５９の４番目のフレームは、元の位置から右側に２つシフトした（すなわち＋２移動した）データセグメント１Ｃを含む。５番目のフレームは、元の位置から右側に５つ位置がシフトした（すなわち＋５移動した）データセグメント１Ａを含む。
【０２９６】
このようにして、テーブル９５７に要約されたソート＃Ｃにより、各データセグメントは新しい位置に一意的に移動し、これにより、パラメータ的に決定されたスクランブル化データパケット９５９が生成される。スクランブル化データパケットをアンスクランブル化するときは、同一のソート方法（ソート＃Ｃ）を使用して、上記の処理を逆の順番で行う。アンスクランブル化操作を実施するために同一のアルゴリズムが選択されることを確実にするために、データパケットのパラメータ値９５３は、スクランブル化操作により変

更されない。例えば、各データセグメントのパラメータ値の線形合計を用いて、数の順番に関係なく、同一の数値が生成される。

【０２９７】

動的スクランブル化方法は、システムのステート（例えば、時間）を使用して、データパケットがスクランブル化されたときの条件を識別し、これにより、アンスクランブル化操作を実行するときに、スクランブル化のときと同一の方法を選択することが可能となる。図２Ｅに示したシステムでは、ステートを使用して、偽装数値シードが生成される。偽装数値シードは、パッケージの送信側または受信側デバイスに送信され、スクランブル化アルゴリズムをテーブルから選択するのに使用される。あるいは、ステート自体が送信側または受信側デバイスに送信され、送信側または受信側デバイスに配置された隠し数字生成器で、スクランブル化／アンスクランブル化アルゴリズムの選択に使用される隠し数字を生成するのに使用される。図２Ｅに示すこのような構成では、ステート（例えば時間）９２０は、隠し数字生成器９６０（Ｈｉｄｄｅｎ　Ｎｕｍｂｅｒ　Ｇｅｎｅｒａｔｏｒ）により隠し数字９６１（Ｈｉｄｄｅｎ　Ｎｕｍｂｅｒ：ＨＮ）を生成し、隠し数字８６１を用いてスクランブル化アルゴリズムリスト９６２からスクランブル化方法を選択するのに使用される。隠し数字９６１を使用してスクランブル化アルゴリズムテーブル９６２から選択されたアルゴリズムが使用して、スクランブル化操作９６３（Ｓｃｒａｍｂｌｉｎｇ）により、スクランブル化されていないデータパケット９３０をスクランブル化データパケット９６４に変換する。図２Ｆに示すように、ステート９２０は、隠し数字生成器９６０に、直接的に送信してもよいし、シード生成器９２１を経由して送信してもよい。

【０２９８】

スクランブル化アルゴリズムを選択するのに、数値シードのみを使用するのではなく、隠し数字を使用することの利点は、データストリームの分析により、すなわちスクランブル化データの繰り返しセットをそれに対応する数値シードと統計的に相関させることにより、スクランブル化テーブルがサイバー犯罪的に再構成される可能性を排除できることである。シードは、データストリーム中で可視的であり、それ故にスパイされることあるが、隠し数字生成器は、共有秘密に基づいて隠し数字「ＨＮ」を生成することができる。そのため、隠し数字ＨＮは、データストリーム中に存在せず、スパイまたはスニッフィングをされない。すなわち、隠し数字は、ネットワークを通じて送信されず、数値シードに基づきローカルで生成される。数値シードの目的は偽装であるため、隠し数字生成器でのこの数学的操作により、ハッカーを阻止するための追加的なセキュリティ層が得られる。

【０２９９】

アルゴリズムが選択されると、数値シードは、スクランブル化操作９６３のアルゴリズムにおける入力変数としても使用される。このように数値シードを２回使用することにより、ハッカーによる分析をさらに混乱させることができる。シードは、アルゴリズムを直接的に選択しないが、アルゴリズムと協働して、スクランブル化されたデータセグメントの最終的な配列を決定するからである。同様に、動的スクランブル化データパケットをアンスクランブル化するときは、シード９２９（またはステート（時間）９２０）を、スクランブル化を実施した通信ノード、デバイス、またはソフトウェアから、アンスクランブル化を実施するノードまたはデバイスに送信しなければならない。

【０３００】

本発明によれば、シード生成器９２１のアルゴリズム、隠し数字生成器９６０、及びスクランブル化アルゴリズムリスト９６２は、ＤＭＺサーバ（後述する）に格納された「共有秘密」情報を意味し、データパケットの送信者または受信者のいずれにも知られていない。共有秘密は、事前に設定されており、送信される通信データパケットには関連せず、例えば、共有秘密の漏出防止を確実にするために様々な認証手続きが行われるコードのインストール時に設定される。後述するように、１セットの盗まれた共有秘密によって、ハッカーが全通信ネットワークにアクセスしたり、リアルタイム通信を妨害したりすることができないように、共有秘密は「ゾーン」に限定される。

【０３０１】

任意の共有秘密に加えて、スクランブル化アルゴリズムがデータパケットの通過間で変化する動的スクランブル化では、「ステート」に基づくシードが、データのスクランブル化またはアンスクランブル化に必要とされる。シードの生成に使用されるステートに関する曖昧さが存在せず、かつデータパケットの前回のスクランブル化のときに使用されたステートを次のノードに知らせる何らかの手段が存在すれば、シードに基づくこのステートは、時間、通信ノード番号、ネットワーク識別子、さらにはＧＰＳ位置などの任意の物理的パラメータを含むことができる。シード生成器でシードを生成するのに使用されるアルゴリズムは共有秘密の一部であるので、ハッカーは、シードの情報から、そのシードがどのステートに基づいているかを知ることはできない。シードは、それ自体をデータパケットに埋め込むことにより、別のチャンネルまたは経路を通じて送信することにより、またはそれらの組み合わせなどにより、ある通信ノードから次の通信ノードに送信される。例えば、シードの生成に使用されたステートは、最初は乱数であり、その後は、データパケットが通信ノードを通過するたびに固定された数だけ増加するカウンタを含む。各カウントは、特定のスクランブル化アルゴリズムを表す。

【０３０２】

動的スクランブル化の一実施形態では、スクランブル化の第１のステップでは、乱数が、使用されるスクランブル化方法を選択するために生成される。この乱数は、データパケットのヘッダ、またはデータパケットにおける命令及び制御のために確保された、スクランブル化の影響を受けない部分に埋め込まれる。データパケットが次のノードに到着すると、データパケットに埋め込まれた数字は、通信ノードにより読み取られ、入力データパケットをアンスクランブル化するための適切なアルゴリズムを選択するためにソフトウェアで使用される。数字、すなわち「カウント」は、その後、１または予め定められた整数ずつ増やされ、パケットは、この新しい数字に関連するアルゴリズムに従ってスクランブル化される。そして、新しいカウントが、出力データパケットに格納され、前のカウントを上書きする。次の通信ノードでは、この処理が繰り返される。

【０３０３】

スクランブル化アルゴリズムを選択するための本開示に係るカウンタベース方法の別の実施形態では、最初のスクランブル化アルゴリズムを選択するために、乱数が生成され、この乱数は、「共有秘密」として、特定のデータパケットを送信するのに使用される全ての通信ノードに送信される。カウント（例えば０から始まる）が、データパケットのヘッダ、またはデータパケットにおける命令及び制御のために確保された、スクランブル化の影響を受けない部分に埋め込まれる。データパケットはその後、次の通信ノードに送信される。パケットが次の通信ノードに到着すると、そのサーバはカウントの数値を読み取り、そのカウントに初期の乱数を追加し、データパケットの前回のスクランブル化に使用されたスクランブル化アルゴリズムを識別し、それに従ってパケットをアンスクランブル化する。カウントはその後、その後、１または予め定められた整数ずつ増やされ、そのカウントは再び、データパケットのヘッダ、またはデータパケットにおける命令及び制御のために確保された、スクランブル化の影響を受けない部分に埋め込まれ、前のカウントを上書きする。共有秘密としての役割を果たす乱数は、通信データパケットに埋め込まれて送信されない。データパケットが次の通信ノードに到着すると、サーバは、乱数（共有秘密）を、データパケットから抽出した更新されたカウントの数値に追加する。この新しい数字は、前の通信ノードで入力パケットをスクランブル化するのに使用されたスクランブル化アルゴリズムを一意的に識別する。この方法では、意味を持たないカウント数のみが、サイバーパイレーツによりデータパケットのスクランブル化されていない部分から傍受され得るが、サイバーパイレーツにはそのデータが何を意味するか分からない。

【０３０４】

別の方法では、パケットのステート及びパケットのスクランブル化に使用されたアルゴリズムを知らせるのに、隠し数字が使用される。隠し数字は、経時的に変化するステートまたはシードを、一般的に数値アルゴリズムを含む共有秘密と組み合わせ、通信ノード間では送信されず、それ故に中間者攻撃またはサイバーパイレーツからスニッフィングまた

は見つかることがない秘密の数字、すなわち「隠し数字」を生成するのに使用される。この隠し数字はその後、スクランブル化に用いられるスクランブル化アルゴリズムを選択するのに使用される。ステートまたはシードは、隠し数字の計算に使用されるアルゴリズムを知らなければ意味を持たず、また、共有秘密アルゴリズムは、ネットワークまたはインターネットを介してアクセス不能なファイアウォールの背後に格納されるので、ネットワークトラヒックのモニタリングによってパターンが明らかになることはない。さらに複雑なことには、シードの位置により、共有秘密を表すことができる。一実施形態では、データパケットのスクランブル化されていない部分により伝送される、データスニッフィング可能な数字、例えば２７４８２５６７８２２５５２２１３は、その一部のみがシードを示す長い数字を含む。例えば、３番目から８番目までの数字がシードを示す場合、実際のシードは、２７４８２５６７８２２５５２２１３の全体の数字ではなく、一部の数字、すなわち４８２５６である。このシードは、その後、隠し数字を生成するために、共有秘密アルゴリズムと組み合わされる。そして、隠し数字は、ネットワークを通じて動的に変化するスクランブル化アルゴリズムを選択するのに使用される。

【０３０５】

ＳＤＮＰネットワークにおけるデータパケットのスクランブル化に関しては、出願日２０１５年７月２０日、「セキュア動的ネットワーク及びプロトコル（Ｓｅｃｕｒｅ Ｄｙｎａｍｉｃ Ｎｅｔｗｏｒｋ Ａｎｄ Ｐｒｏｔｏｃｏｌ）」、アメリカ出願番号１４／８０３，８６９で記述されている。ラストマイル通信におけるデータパケットのスクランブル化に関しては、本開示で更なる詳細が記述されている。

【０３０６】

前述されたように、ネットワークを横断するデータは、スクランブル化されたにも関わらず、「プレーンテキスト」（Ｐｌａｉｎｔｅｘｔ）と呼ぶことができる。実データがデータパケット中に存在している、すなわち、データパケットがサイファテキストに暗号化されていないからである。対照的に、サイファテキストでは、元のデータを含む文字列は、スクランブル化の有無に関わらず、暗号化鍵を使用して意味を持たない文字列に変換され、復号鍵を使用しない限りは、その元のプレーンテキストの形態には復元されない。本開示に係るＳＤＮＰベース通信における暗号化の役割は、下記の「パケット暗号化」のセクションにおいてさらに説明する。

【０３０７】

図３に示すように、ネットワークを通じた伝送中にデータパケットのデータセグメント配列を変更するためには、パケットの「再スクランブル化」が必要となる。このパケット再スクランブル化のプロセスは、スクランブル化データを新しいスクランブル化アルゴリズムにより再びスクランブル化する前に、スクランブル化データをそのアンスクランブル化状態に戻す。したがって、本明細書で使用される「再スクランブル化」という用語は、データパケットをアンスクランブル化した後に、一般的には別のスクランブル化アルゴリズムまたは方法により再びスクランブル化することを意味する。このアプローチにより、既にスクランブル化されているパッケージを再びスクランブル化することにより元のデータの復元に必要なデータセグメント配列が分からなくなることによって生じ得るデータ破損のリスクが避けられる。図示のように、パケットスクランブル化操作９２６により最初にスクランブル化された後に、スクランブル化データパケット１００８が「再スクランブル化」される。つまり、スクランブル化データパケット１００８は、まず、そのデータのスクランブル化に使用されたスクランブル化アルゴリズムと逆の処理を用いてアンスクランブル化操作９２８によりアンスクランブル化され、その後、スクランブル化操作９２６により、前回のスクランブル化操作９２６で使用されたものとは別のスクランブル化アルゴリズムを使用して、再びスクランブル化される。この結果生成された再スクランブル化データパケット１００９は、その前のスクランブル化データパケット１００８とは異なる。再スクランブル化操作１０１７は、アンスクランブル化とそれに続くスクランブル化との連続的な実施を含み、これを本明細書中では「ＵＳ再スクランブル化（ＵＳ Ｒｅｓｃｒａｍｂｌｉｎｇ）」と称する（ＵＳは、アンスクランブル化・スクランブル化（ｕｎｓ

ｃｒａｍｂｌｉｎｇ－ｓｃｒａｍｂｌｉｎｇ）の略語である）。元のデータパケット９３０を復元するためには、最終的なパケットアンスクランブル化操作９２８は、データパケットの最後の再スクランブル化に使用されたアルゴリズムと逆の処理の実施を必要とする。

【０３０８】

本発明によれば、データの静的及び動的スクランブル化により、スクランブル化されていないデータを判読不能な無意味な（意味を持たない）ものに変更し、音声を認識不能なノイズに並べ換え、テキストを無意味なものに並べ替え、画像を真っ白な画像（ｖｉｄｅｏ　ｓｎｏｗ）に変換し、コードを復元不能にスクランブル化することができる。スクランブル化だけによって、高いセキュリティを提供することができる。そして、本開示に係るＳＤＮＰ法では、スクランブル化は、ハッキング、サイバー攻撃、サイバーパイラシー、及び中間者攻撃から逃れるセキュア通信（セキュリティが確保された通信）を提供及び確保することができる１つの要素に過ぎない。

【０３０９】

パケット暗号化

【０３１０】

本発明によれば、パケット交換ネットワークを介したセキュア通信は、ハッキング防止及びセグメント確保のためのいくつかの要素に依存し、そのうちの１つはＳＤＮＰ暗号化を含む。上述したように、「隠す」、「秘密にする」、「見えなくする」を意味するギリシャ語に由来する暗号化は、一般的に「プレーンテキスト」と呼ばれる通常の情報またはデータを、秘密情報を使用しない限りは判読することはできない判読不能なフォーマットの「サイファテキスト」に変換する手段を表す。最近の通信では、この秘密情報は、一般的に、データの暗号化及び復号に使用される１またはそれ以上の「鍵」を共有することを含む。この鍵は、一般的に、アルゴリズム的に生成された擬似乱数を含む。「Ｃｒｙｐｔｏｎｏｍｉｃｏｎ」などの様々な暗号化技術のメリット及びデメリットについて論じた様々な文献または文章としては、現在、例えば、「Neal Stephenson (C) 1999」、「The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography、by Simon Singh (C) 1999」、「Practical Cryptography、by Niels Ferguson (C) 2013」、及び「Cryptanalysis: A Study of Ciphers and Their Solution、first published in 1939」などが入手可能である。

【０３１１】

暗号化または暗号のコンセプトは古くからあり当業者には公知であるが、本開示に係るセキュア動的ネットワーク及びプロトコルにおける暗号化法の応用はユニークなものであり、クライアント自体の暗号化から独立しており、ネットワークアーキテクチャ自体に対するエンドツーエンド暗号化（ｅｎｄ－ｔｏ－ｅｎｄ　ｅｎｃｒｙｐｔｉｏｎ）及びシングルホップノードツーノード動的暗号化（ｓｉｎｇｌｅ－ｈｏｐ　ｎｏｄｅ－ｔｏ－ｎｏｄｅ　ｄｙｎａｍｉｃ　ｅｎｃｒｙｐｔｉｏｎ）の両方を容易にする。ＳＤＮＰ通信は、暗号をどれだけ複雑にしても、十分な時間さえあれば、あらゆる静的暗号化ファイルまたはメッセージは最終的には破られてその情報が盗まれる、という基本的教訓に基づいて設計されている。この仮定は実際には不正確であるが、この仮定を証明または反証する必要はない。なぜならば、特定の暗号化法が失敗するまで待つと、許容不能な及び取り戻せない結果的被害が生じるからである。

【０３１２】

この代わりに、ＳＤＮＰ通信は、全ての暗号化ファイルは限られた「保存可能期間」を有するという前提に基づいている。これは、暗号化されたデータは有限の期間においてのみセキュリティが確保されており、秘密データは、所定の間隔で、理想的には最新式コンピュータで暗号を破るのに必要とされる時間の最も正確な見積もりよりもはるかに高い頻度で、動的に再暗号化しなければならないことを暗喩的に意味する。例えば、暗号処理装置の大きなサーバファームが所定の暗号を１年で破ることができると暗号学者により推測される場合は、ＳＤＮＰ通信では、データパケットを１秒毎または１００ミリ秒毎、すなわち暗号を破るための最高の技術よりも何桁も短い間隔で再暗号化する。したがって、Ｓ

ＤＮＰ暗号化は必然的に、動的すなわち経時変化的であり、また空間的にも、すなわちパケット交換ネットワークまたは地図上における通信ノードの位置に依存して変化し得る。このため、「再暗号化」または「再暗号化法」という用語は、データパケットを復元し、その後に、別の暗号化アルゴリズムまたは方法を用いて再び暗号化することを指す。

【０３１３】

このため、ＳＤＮＰ暗号化は、データを、暗号化されていないプレーンテキストからサイファテキストに繰り返し及び頻繁に変換し、情報を判読不能で無意味なものに改変することを含む。もし、所定のパケットのデータ暗号化が奇跡的に破られたとしても、ＳＤＮＰ動的暗号化方法を用いることにより、次のデータパケットでは全く異なる暗号化鍵または暗号が使用されるので、その暗号を破るためには、全く新しい労力が必要となる。個別に暗号化された各データパケットに含まれるコンテンツを制限することにより、不正アクセスのダメージの可能性を減らすことができる。破られたデータパケットに含まれるデータファイルの大きさを、サイバーパイレーツにとって意味をなすまたは有用となるには小さすぎるようにすることができるからである。さらに、動的暗号化を上述したＳＤＮＰスクランブル化方法と組み合わせることにより、通信のセキュリティを大幅に高めることができる。暗号化されていない形態でも、傍受されたデータファイルには、データセグメントの順番が無意味で判読不能となるようにスクランブル化されたデータ、音声、または映像の小さい断片しか含まれていない。

【０３１４】

保存可能期間に関連するセキュリティの懸念を避けるために、ＳＤＮＰ暗号化は、動的であり、かつステート依存性である。図４Ａに示すように、プレーンテキスト９３０（Ｐｌａｉｎｔｅｘｔ）を含む暗号化されていないデータパケットは、暗号化操作１０２０（Ｅｎｃｒｙｐｔｉｏｎ　Ｐｒｏｃｅｓｓ）により処理され、これにより、サイファテキスト１０２４及び１０２５（Ｃｉｐｈｅｒｔｅｘｔ）を含む暗号化データパケットが生成される。サイファテキスト１０２４については、プレーンテキスト９３０のデータパケットは全体として暗号化され、データセグメント１Ａ－１Ｆは、単一のデータファイルとして扱われる。一方、サイファテキスト１０２５については、プレーンテキスト９３０のデータセグメント１Ａ－１Ｆは個別に暗号化され、他のデータセグメントと混合されない。プレーンテキストの第１のデータセグメント１Ａは、それに対応する第１のサイファテキストセグメント（説明目的のために図示した「７＄」で始まる長い文字列であり、図示しない長い文字列または数字を含む）に暗号化される。同様に、プレーンテキストの第２のデータセグメント１Ｂは、第２のサイファテキストセグメント（説明目的のために図示した「＊＾」で始まる長い文字列）に暗号化される。文字「７＄」及び「＊＾」は、記号、数字、アルファベットなどの無意味な文字列の先頭を意味しており、プレーンテキストソースの特定のデータまたは暗号化された文字列の長さについて限定または暗示するものではない。

【０３１５】

暗号化操作１０２０（Ｅｎｃｒｙｐｔｉｏｎ　Ｐｒｏｃｅｓｓ）は、利用可能な任意のアルゴリズム、暗号化方式、または暗号化方法を用いることができる。暗号化アルゴリズムは静的な方程式を示すが、一実施形態では、暗号化操作は、暗号化を行うときに、例えば時間９２０などの動的変数または「ステート」を使用する。また、暗号鍵生成器１０２１を使用して、暗号化を実施したときの時間９２０などのステートに依存する暗号化鍵（Ｅ鍵）１０２２を生成する。例えば、暗号化の日付及び時間が、ハッカー等が暗号化アルゴリズムを見つけた場合でも再生成することはできないＥ鍵を生成するための数値シードとして使用される。時間９２０または他の「ステート」はまた、利用可能な暗号化アルゴリズムのリストである暗号化アルゴリズムリスト１０２３（Ｅｎｃｒｙｐｔｉｏｎ　Ａｌｇｏｒｉｔｈｍｓ）から特定のアルゴリズムを選択するのに使用される。データフロー図では、図示の便宜上、このパケット暗号化操作及びシーケンスは、暗号化操作１０２６（Ｅｎｃｒｙｐｔｉｏｎ）として概略的または記号的に表示する。本開示を通じて、セキュア及び暗号化データは、パドロック（南京錠）によっても記号的に表される。特に、時計

の文字盤が上側に配置されたパドロックは、セキュア送信メカニズム、例えば、特定の時間間隔以内または特定の時間までに受信しなかった場合には暗号化ファイルは自己破壊され永久に失われることを示す。

【０３１６】

図４Ｂは、暗号化操作１０２０と逆の操作である復号操作１０３１を示す。この復号操作１０３１では、サイファテキスト１０２４（Ｃｉｐｈｅｒｔｅｘｔ）の生成に使用されたステート（時間または他のステート）９２０を再使用し、復号鍵生成器１０２１により生成された復号鍵（Ｄ鍵）１０３０と協働して暗号化を解除し、すなわちファイルを復号し、元のプレーンテキストデータパケット９９０（Ｐｌａｉｎｔｅｘｔ）を含む暗号化されていないデータを生成する。復号操作１０３１（Ｄｅｃｒｙｐｔｉｏｎ　Ｐｒｏｃｅｓｓ）では、パケットの暗号化のときに使用されたものと同一のステート（時間）９２０を使用して、暗号化のときに暗号化アルゴリズムリスト１０２３から選択されたものと同一の暗号化アルゴリズムを再び選択して使用する。暗号化アルゴリズムリスト１０２３では「暗号化」という用語が用いられているが、このアルゴリズムテーブルは、「復号」の実施に必要とされる、暗号化と逆の操作を識別して選択するのに使用される。すなわち、暗号化アルゴリズムリスト１０２３は、データパケットの暗号化及び復号の両方に必要な情報を含んでいる。この２つの操作は、互いに逆の順番で実施される同一のステップを含むので、このテーブル１０２３は、「暗号化／復号」アルゴリズムテーブル１０２３とも称することもできる。しかしながら、明確にするために、このテーブルは、暗号化の機能についてのみ称し、その反対の機能（復号）については称さないものとする。

【０３１７】

復号操作１０３１の実施のために選択された暗号化アルゴリズムが、パケット暗号化操作１０２０に使用されたアルゴリズムと逆のものと一致しない場合、ステート（時間）９２０が、暗号化のときの時間と一致しない場合、または、Ｄ鍵１０３０が、暗号化のときに使用されたＥ鍵１０２２に対して予め定められた数値関係を有さない場合、復号操作１０３１は、暗号化されていない元のデータ９９０の復元に失敗し、パケットデータは失われることとなる。データフロー図では、図示の便宜上、このパケット復号操作及びシーケンスは、復号化操作１０３２として概略的または記号的に表示する。

【０３１８】

前述したように、暗号化及び一般的な暗号化アルゴリズムにおける暗号化鍵及び復号鍵の使用に関する知識、とりわけ対称公開鍵暗号化、ＲＳＡ暗号化、ＡＥＳ２５６暗号化などは、当業者には一般的であり公知である。しかしながら、このような公知の暗号化方法を本開示に係るＳＤＮＰ通信システムへの適用にすると、本開示に係るＳＤＮＰ通信に特有の隠された情報、共有秘密、及び時間依存性の動的変数及びステートによって、ハッキングまたは暗号解読は困難になる。

【０３１９】

したがって、サイバーパイレーツがロバストな暗号化方法を最終的に破ることができるコンピュータ処理能力を有しているという、あり得そうにない場合でも、サイバーパイレーツは、復号操作の実施に必要な非公開または共有秘密としてＳＤＮＰネットワークに埋め込まれたいくつかの情報を欠いており、また、暗号が変更される前に、暗号を１秒足らずの間に破らなければならない。さらに、本開示に係るＳＤＮＰネットワークを横断する全てのデータパケットは、固有の鍵及び動的ステートに基づき決定される互いに異なる暗号化方法を使用する。欠けた情報、動的ステート、及び任意のパケットに含まれた限定された情報コンテンツの組み合わせにより、任意のデータパケットから盗まれた意味も持つデータを、サイバーパイレーツにとって困難で報われないものにする。

【０３２０】

ＳＤＮＰネットワークにおけるデータパケットの暗号化及び復号化は、前述された出願日２０１５年７月２０日、「セキュア動的ネットワーク及びプロトコル（Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｎｅｔｗｏｒｋ　Ａｎｄ　Ｐｒｏｔｏｃｏｌ）」、アメリカ出願番号１４／８０３，８６９で記述されている。ラストマイル通信におけるデータパケットの暗号法

に関しては、本開示で更なる詳細が記述されている。

【０３２１】

文章、動画ストリーム、または音声会話の全体を傍受して、コヒーレントデータシーケンスを再構成するためには、サイバー攻撃者は、１つだけではなく数千もの一連のＳＤＮＰパケットを連続的に破って復号しなければならない。動的な暗号化を、上述したデータパケットスクランブル化に関する方法と組み合わせることにより、一連のＳＤＮＰパケットを連続的にハッキングするという困難な作業がさらに困難になる。図５に示すように、暗号化及びスクランブル化されたデータパケット１０２４（Ｃｉｐｈｅｒｔｅｘｔ ｏｆ Ｓｃｒａｍｂｌｅｄ Ｄａｔａ Ｐａｃｋｅｔ）は、スクランブル化操作９２６と暗号化操作１０２６との連続的な組み合わせにより生成される。まず、スクランブル化操作９２６によりスクランブル化されていないプレーンテキストデータパケット９９０（Ｕｎ－ｓｃｒａｍｂｌｅｄ Ｐｌａｉｎｔｅｘｔ）をスクランブル化プレーンテキストデータパケット１００８（Ｓｃｒａｍｂｌｅｄ Ｐｌａｉｎｔｅｘｔ）に変換し、その後に、暗号化操作１０２６によりスクランブル化データパケットのサイファテキスト１０２４に変換する。スクランブル化パッケージの暗号化を繰り返すためには、上記と逆の操作を上記と逆の順番で行う。まず、復号操作１０３２によりスクランブル化プレーンテキストデータパケット１０３５（Ｓｃｒａｍｂｌｅｄ Ｐｌａｉｎｔｅｘｔ）に復号し、その後に、アンスクランブル化操作９２８によりスクランブル化されていないプレーンテキストデータパケット９９０（Ｕｎｓｃｒａｍｂｌｅｄ Ｐｌａｉｎｔｅｘｔ）を復元する。

【０３２２】

図示のように、スクランブル化及び暗号化は、セキュア通信を実現するための相補的な技術を表す。ネットワークを横断する暗号化されていないスクランブル化データは、データパケット内に実データが存在するので、すなわちパケットはサイファテキストに暗号化されていないので、「プレーンテキスト」と呼ばれる。暗号化データパケット、すなわちサイファテキストは、暗号化鍵を使用して無意味な文字列に変換され、対応する復号鍵を使用しない限りは元のプレーンテキストに復元することはできない、スクランブル化されたまたはスクランブル化されていない文字列を含む。使用されるアルゴリズムに依存して、暗号化鍵及び復号鍵は、同一の鍵、または予め定められた数学的関係で数学的に関連する別個の鍵であり得る。したがって、スクランブル化及び暗号化は、ＳＤＮＰ通信のための本発明に係るセキュア通信を実現するための相補的な技術を表す。

【０３２３】

スクランブル化及び暗号化の２つの方法は、暗号化されたスクランブル化データパケットから元のデータパケットを復元するときの順番が暗号化のときと逆の順番で行われることを除いて、互いに組み合わせて使用する場合でも別個のものとして見なすことができる。例えば、データパケット９９０をスクランブル化操作９２６によりスクランブル化した後に暗号化操作１０２６により暗号化した場合は、元のデータパケットに復元するためには、暗号化及びスクランブル化されたデータパケット１０２４を復号操作１０３２により復号した後にアンスクランブル化操作９２８によりアンスクランブル化する。数学的には、スクランブル化操作Ｆにより、ビットまたは文字の列を、それに対応するスクランブル化バーションにスクランブル化し、アンスクランブル化操作Ｆ－１により、スクランブル化を解除することは、下記のように表される。

Ｆ－１［Ｆ（Ａ）］＝Ａ

【０３２４】

同様に、暗号化操作Ｇにより、一連のプレーンテキストをそれに対応するサイファテキストに暗号化し、復号操作Ｇ－１により、暗号化を解除することは、下記のように表される。

【０３２５】

Ｇ－１［Ｇ（Ａ）］＝Ａ

したがって、

Ｆ－１｛Ｇ－１［Ｇ（Ｆ（Ａ））］｝＝Ａ

と表すことができる。各操作の順番が逆の順番で行われ、具体的には、暗号化及びスクランブル化されたパケット［Ｇ（Ｆ（Ａ））］を復号［Ｇ－１］することにより、スクランブル化されたプレーンテキストデータパケットＦ（Ａ）が復元され、その後、スクランブル化されたプレーンテキストパケットＦ（Ａ）のアンスクランブル化操作Ｆ－１により、元のデータパケットＡが復元されるからである。

【０３２６】

線形的方法を用いると仮定すると、各操作の順番は可逆的である。例えば、データパケットを暗号化した後にスクランブル化した場合は、元のデータパケットに復元するためには、スクランブル化サイファテキストをアンスクランブル化した後に複合される。すなわち、下記のように表される。

Ｇ－１｛Ｆ－１［Ｆ（Ｇ（Ａ））］｝＝Ａ

【０３２７】

各操作の順番を変更すると、元のデータパケットを復元することはできない。つまり、暗号化した後にスクランブル化したデータパケットを、アンスクランブル化する前に復号すると、元のデータパケットを復元することはできない。すなわち、下記のように表される。

Ｆ－１｛Ｇ－１［Ｆ（Ｇ（Ａ））］｝≠Ａ

【０３２８】

同様に、スクランブル化した後に暗号化したパケットを、復号する前にアンスクランブル化すると、元のデータパケットを復元することはできない。すなわち、下記のように表される。

Ｇ－１｛Ｆ－１［Ｇ（Ｆ（Ａ））］｝≠Ａ

【０３２９】

要約すると、プレーンテキストパケットを暗号化の前にスクランブル化した場合は、アンスクランブル化の前に復号しなければならない。また、プレーンテキストパケットをスクランブル化の前に暗号化した場合は、復号の前にアンスクランブル化しなければならない。

【０３３０】

スクランブル化及び暗号化はどの順番で行ってもよいが、本発明に係るＳＤＮＰ方法の一実施形態では、暗号化及び復号は、ネットワーク転送中にスクランブル化よりも頻繁に行われる。このため、図５に示すように、暗号化は、スクランブル化の後に行うべきであり、復号はアンスクランブル化の後に行うべきである。便宜上、パケットスクランブル化操作９２６と、それに続く暗号化操作１０２６との組み合わせを、スクランブル化・暗号化操作１０４１（Ｓｃｒａｍｂｌｅ　＆　Ｅｎｃｙｐｔ）と定義する。また、それと逆の、復号操作１０３２と、それに続くパケットアンスクランブル化操作９２８との組み合わせを、復号・アンスクランブル化操作１０４２（Ｄｅｃｒｙｐｔ　＆　Ｕｎｓｃｒａｍｂｌｅ）と定義する。これらの組み合わされた操作は、本発明に係る静的及び動的ＳＤＮＰ通信に用いられる。

【０３３１】

静的スクランブル化暗号化を用いて、任意の実装においてセキュリティを高める方法の１つは、各データパケットを、別個のスクランブル化及び／または暗号化方法（例えば、各データパケットが通信ネットワークに入るときの時間ｔ１でのステート、シード、及び／または鍵の変更を含む）を用いてスクランブル化及び／または暗号化を実施することである。

【０３３２】

しかしながら、よりロバストな別な方法は、データパケットがネットワークを横断するときに、データパケットの暗号化またはスクランブル化、あるいはその両方を動的に変更することを含む。ＳＤＮＰの完全な動的バージョンの実現に必要なデータ処理を容易にするためには、パケット交換通信ネットワークの各通信ノードを通過する各パケットを「再スクランブル化（すなわち、アンスクランブル化及びそれに続くスクランブル化）」及び

「再暗号化（すなわち、復号及びそれに続く暗号化）」するために、上記に定義した処理を組み合わせる必要がある。本明細書において使用される「再パケット」または「再パケット化」という用語は、パケットがアンスクランブル化の前に復号されるか、または復号された後にアンスクランブル化されるかに関わらず、「再スクランブル化」及び「再暗号化」の組み合わせを指すのに用いられる。いずれの場合でも、あるノードでのアンスクランブル化操作及び復号操作は、その前のノードでパケットをスクランブル化及び暗号化したときの順番と逆の順番で行わなければならない。すなわち、前のノードでパケットをスクランブル化した後に暗号化した場合は、現在のノードでは、パケットを復号した後にアンスクランブル化しなければならない。一般的に、パケットは、現在のノードから出力されるときに、スクランブル化した後に暗号化される。

【０３３３】

通信ノードでの「再パケット化」操作を図６に示す。通信ノードに入力されたサイファテキストデータパケット１０４０は、まず、復号操作１０３２により復号され、その後に、アンスクランブル化操作９２８によりアンスクランブル化される。これにより、元のパケットのコンテンツを含む、スクランブル化されていないプレーンテキストデータパケット９９０（Ｕｎｓｃｒａｍｂｌｅｄ　Ｐｌａｉｎｔｅｘｔ　（ｃｏｎｔｅｎｔ））が復元される。パケット内の任意の情報を検査、解析、分割、またはリダイレクトする必要がある場合、スクランブル化されていないプレーンテキストファイルは、そのような操作を行うのに最適なフォーマットである。そして、プレーンテキストデータパケット９９０は、スクランブル化操作９２６により再びスクランブル化された後、暗号化操作１０２６により再び暗号化され、これにより、新しいスクランブル化サイファテキストデータパケット１０４３が生成される。通信ノードに入力されたサイファテキストデータパケット１０４０の再パケット化操作では、復号、アンスクランブル化、スクランブル化、暗号化が連続的に行われるので、その頭文字を並べて、本発明に係る技術をＤＵＳＥ再パケット化操作１０４５（ＤＵＳＥ　Ｒｅ－Ｐａｃｋｅｔ）と称する。動的なセキュアネットワークでは、復号操作１０３２及びアンスクランブル化操作９２８を実施するために使用されるステート（時間）、復号鍵、及びシードは、スクランブル化操作９２６及び暗号化操作１０２６を実施するために使用されるステート（時間）、暗号鍵、及びシードとは異なることが好ましい。

【０３３４】

ＳＤＮＰネットワークにおけるデータパケットの再パケット化は、前述された出願日２０１５年７月２０日、「セキュア動的ネットワーク及びプロトコル（Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｎｅｔｗｏｒｋ　Ａｎｄ　Ｐｒｏｔｏｃｏｌ）」、アメリカ出願番号１４／８０３，８６９で記述されている。ラストマイル通信におけるデータパケットの再パケット化に関しては、本開示で更なる詳細が記述されている。

【０３３５】

<u>パケットの混合及び分割</u>

【０３３６】

本開示に係る動的なセキュア通信ネットワーク及びプロトコルの別のキー要素は、データパケットをサブパケットに分割して複数のルートに送信し、サブパケットを組み合わせて再構成し、完全なデータパケットを再構成する機能である。データパケット１０５４を分割操作１０５１（Ｓｐｌｉｔｔｉｎｇ（Ｕｎ－ｍｉｘｉｎｇ）Ｐｒｏｃｅｓｓ）により分割するプロセスを図７Ａに示す。分割操作１０５１は、アルゴリズム的なパース操作１０５２（Ｐａｒｓｅ）をジャンク操作１０５３（Ｊｕｎｋ）と組み合わせた操作であり、非データの「ジャンク」データセグメントを挿入または除去する機能を有する。ヒトゲノム内に存在するジャンクＤＮＡと同様に、ジャンクデータセグメントは、ジャンク操作１０５３により、データパケットの長さを延長または調節するために挿入され、また必要に応じて除去される。ジャンク操作１０５３は、パケットを満たすデータの量が不十分である場合に、とりわけ重要である。また、データパケットに挿入されたジャンクデータセグメントの存在は、サイバーパイレーツが実データをノイズと区別することを困難にする。

本明細書で使用される「ジャンク」パケットまたはデータセグメントは、意味を持たないデータ（ビット）だけで構成されるパケットまたはデータセグメントである。このようなジャンクビットをデータパケットのストリーム中に導入することにより、実データを多数の無意味なビットの中に埋没させることができる。

【０３３７】

パース操作１０５２の目的は、各構成要素を処理するために、データパケット１０５４をより小さなデータパケット（例えば、サブパケット１０５５及び１０５６）に分割することである。データパケット１０５４をより小さな部分に分割することにより、例えば、マルチパス伝送をサポートすること、すなわちデータパケットを複数の別個の経路を通じて伝送すること、及び別個の暗号化方法を用いたサブパケットの個別の暗号化を容易にすることなどの、固有の利点を提供することができる。

【０３３８】

分割操作は、任意のアルゴリズム、数値的方法、またはパース（ｐａｒｓｉｎｇ）方法を用いることができる。アルゴリズムは、静的方程式で表すか、または、動的変数または数値シードまたは「ステート」、例えば入力データパケット１０５４が多数のサブパケットにより最初に形成されたときの時間９２０、及びシード生成器９２１で生成された数値シード９２９（このシードもデータパケットの生成時の時間９２０などのステートに依存する）を含むことができる。例えば、各データが、単調増加する固有の数に変換される場合、各シード９２９は固有のものとなる。時間９２０及びシード９２９は、利用可能な方法のリスト、すなわち混合アルゴリズム１０５０（Ｍｉｘｉｎｇ　Ａｌｇｏｒｉｔｈｍｓ）から選択される特定のアルゴリズムを識別するのに使用される。パケット分割操作は、混合操作と逆の処理を含み、混合操作で特定のパケットの生成に使用されたアルゴリズムと正反対の順番で実行されるアルゴリズムを使用する。つまり、実施された操作は全て元に戻すことができるが、全てを１つのステップで行う必要はない。例えば、スクランブル化及び暗号化されたデータパケットは、復号しても、スクランブル化が保たれるようにしてもよい。分割操作１０５１で処理することにより、非分割データパケット１０５４は、複数のデータパケット、例えば固定長パケット１０５５及び１０５６に変換される。この操作をアルゴリズム的に実施するのに、パース操作１０５２が用いられる。データフロー図では、図示の便宜上、パース操作１０５２及びジャンク操作１０５３を含むこのパケット分割操作１０５１は、分割操作１０５７として概略的または記号的に表示する。

【０３３９】

したがって、本明細書で使用される「分割」という用語は、１つのパケットを２以上のパケットすなわちサブパケットに分割するパースを含む。また、「分割」という用語は、「パースされた」パケットまたはサブパケットにジャンクパケットまたはサブパケットを挿入すること、または、「パースされた」パケットまたはサブパケットからジャンクパケットまたはサブパケットを除去することを含む。

【０３４０】

分割操作と逆の操作であり、複数のパケット１０５５及び１０５６を混合して混合パケット１０５４を生成するパケット混合操作１０６０（Ｍｉｘｉｎｇ　Ｐｒｏｃｅｓｓ）を図７Ｂに示す。パケット分割操作と同様に、このパケット混合操作は、任意のアルゴリズム、数値的方法、または混合方法を用いることができる。アルゴリズムは、静的方程式で表すか、または、動的変数または数値シードまたは「ステート」、例えば入力データパケット１０５５及び１０５６が生成されたときの条件を特定するのに使用される時間９２０を含むことができる。データパケットの生成に使用される混合操作は、シード生成器９２１で生成された数値シード９２９（このシードも時間９２０などのステートに依存する）を使用することができる。時間９２０及びシード９２９は、利用可能な混合方法のリスト、すなわち混合アルゴリズム１０５０から選択される特定の混合アルゴリズムを識別するのに使用される。データフロー図では、図示の便宜上、このパケット混合操作１０６０を、混合操作１０６１として概略的または記号的に表示する。

【０３４１】

本発明によれば、パケット混合及びパケット分割は、可能性がある様々なアルゴリズムのうちの任意のものを用いて行うことができる。図８は、可能性がある３つの混合技術、連結方法（Ｃｏｎｃａｔｅｎａｔｉｏｎ）、交互配置方法（Ｉｎｔｅｒｌｅａｖｅｄ）、アルゴリズム的方法（Ａｌｇｏｒｉｔｈｍｉｃ）を示す。連結方法では、データパケット１０５６のデータセグメント配列を、データパケット１０５５の末端に追加して、混合パケット１０５４を生成する。交互配置方法では、データパケット１０５５及び１０５６のデータセグメントが交互に、すなわち、１Ａ、２Ａ、１Ｂ、２Ｂの順番で互い違いとなるように混合して、混合パケット１０５６を生成する。パケット混合に用いられる他の方法は、アルゴリズム的方法である。図示した例では、アルゴリズムは、交互的な鏡映対称（インターリーブ鏡映対称）を含み、データセグメントを、混合パケット１０６６の前半部分では、１Ａ、２Ａ、１Ｂ、２Ｂ、１Ｃ、２Ｃの順番で配置し、混合パケット１０６６の後半部分では、前半部分とは逆の順番で、すなわち２Ｄ、１Ｄ、２Ｅ、１Ｅ、２Ｆ、１Ｆの順番で配置する。

【０３４２】

ＳＤＮＰネットワークでのデータパケットの混合と分割の適用は、上記に参照される「セキュア動的通信ネットワーク及びプロトコル」という名称の米国出願第１４／８０３，８６９号に記載されている。図９Ａは、機能とそれに対応する逆の処理、すなわち逆機能、及び対応する機能の動的コンポーネント、すなわちデータパケットで実行されたときの各機能の状態または時間を含むＳＤＮＰ機能要素を要約するものである。ＳＤＮＰ機能には、パケットスクランブル化操作９２６及びその逆機能のパケットアンスクランブル化操作９２８を含むスクランブル化操作、分割操作１０５７及びその逆機能の混合操作１０６１を含む断片化操作、ジャンク挿入１０５３Ａとジャンク除去１０５３Ｂを含む偽装操作、及び暗号化操作１０２６及び復号化操作１０３２を含む暗号化操作が含まれる。これらの機能は全て、時間または状態変数９２０に従って一意に発生する。

【０３４３】

データパケットの混合と分割の適用は、ラストマイル通信におけるスクランブル化、アンスクランブル化、暗号化、復号化、及び偽装と共に、集合的にＳＤＮＰラストマイルセキュリティ操作を構成する。このＳＤＮＰラストマイルセキュリティ操作は「方向性」である。つまり、全ての発信データパケットに対して実行される操作は、着信データパケットに対して実行される操作とは異なる。

【０３４４】

ＳＤＮＰラストマイルセキュリティ操作もラストマイルに対して対称的かつ可逆的である。つまり、特定のラストマイルに固有の鍵、シード、共有秘密などのローカルセキュリティクレデンシャル情報が使用され、クライアントデバイスの送信データパケットで実行される操作はＳＤＮＰゲートウェイで元に戻すことができる。これは、一般的に逆機能、すなわち数学的逆またはクライアントデバイスによって元々実行された全ての機能操作を逆の順序で行うことで実行される。そのため、ＳＤＮＰゲートウェイは、ＳＤＮＰクラウド経由のルーティングの準備として元のコンテンツを回復するように有効化される。同様に、ラストマイルのゾーン固有のセキュリティクレデンシャル情報を通してクライアントデバイスに着信するデータパケットの場合、クライアントデバイスで実行されるＳＤＮＰラストマイルセキュリティ操作により、逆機能を逆の順序で実行することで、ＳＤＮＰゲートウェイで実行される各セキュリティ操作を取り消すことができる。このように、クライアントデバイスでは全ての着信データパケットの元のデータを回復することが可能である。

【０３４５】

ＳＤＮＰラストマイルセキュリティ操作は動的である。そして、これは、データパケットが準備された時点で使用されるパラメータ及び特定のラストマイルに固有の地域、地理、またはロケールを決定するため、場所や時間などのステートに依存する条件を使用してローカライズされる、すなわちゾーンに固有となる。ローカライズされることで、異なる地域の異なるラストマイル接続で実行されるデータパケットの準備で、同じコーディング

または同じセキュリティクレデンシャル情報が使用されることがなくなる。また、これらのラストマイルセキュリティクレデンシャル情報が、ＳＤＮＰクラウドで使用される認証情報とは常に異なるものとなる。さらに、動的であるため、データパケットの作成に使用されるステートが絶えず変化し、各データパケットで実行される実際のセキュリティプロセスがさらに難読化され、２つのデータパケットが同様にレンダリングされることがなくなる。

【０３４６】

各ラストマイル通信に固有の方向性の対称可逆かつ動的でローカライズされたセキュリティ操作の独自の組み合わせを適用することで、本発明に従って行われる動的スクランブル化、動的断片化、動的偽装、及び動的暗号化のアルゴリズムの適用により、単純な静的暗号化方式の使用では達成できないハイパーセキュア通信が保証される。わずか数十ミリ秒の持続時間で有効となる動的方法の適用を普及させることで、解釈がほぼ不可能となるだけでなく、ハッカーは別のパケットが到着する前にデータパケットを解読または解釈する暇がなくなる。実際には、ＳＤＮＰラストマイルセキュリティ操作は、ソフトウェア、ファームウェア、ハードウェア、専用セキュリティＩＣ、またはこれらの任意の組み合わせを使用して実行できる。

【０３４７】

無数のシーケンスの組み合わせが可能となるが、特にシングルルートラストマイル通信で使用されるシリアルＳＤＮＰペイロードのためのＳＤＮＰラストマイルセキュリティ操作の一例が図９Ｂに示されている。すなわち、この図では、クライアントデバイスから単一のＳＤＮＰゲートウェイへ通信が行われる。このプロセスには、発信データパケットと着信データパケットのための２方向の操作シーケンスが含まれる。図の上半分に示されるように、発信データパケットの場合、「送信されるデータ」が最初にパケットスクランブル操作９２６によりスクランブル化され、次にジャンクデータ１０５３Ａの挿入により偽装が実行される。場合によっては、パケット全体を完全にジャンクデータで構成することで、ハッカーによるデータマイニングの試みをさらに混乱させることができる。

【０３４８】

次に、これらのパケットはパース操作１０５２が使用される分割操作１０５７により複数の断片に分割され、暗号化操作１０２６に向けて個別に 送信される。次に、各断片が共通または個別の暗号鍵を使用して暗号化され、結果として生成される暗号文がデータパケット１１９９Ａとして示されるシリアルＳＤＮＰペイロードに配置される。そして、パケットは、ラストリンク及びラストマイルへの通信の準備として、ＩＰデータパケット、すなわち「ＩＰパケット準備」にフォーマットされる。実行される全ての操作は動的であり、特定の時間またはセキュリティプロセスの実行中に特定のステート９２０Ａで発生する。

【０３４９】

図の下半分に示されるように、着信データパケットの場合、シリアルＳＤＮＰペイロード１１９９Ｂを含むラストリンクからの着信データ、つまり「ＩＰパケット認識」からの着信データは、最初に断片的にまたは全体として解読操作１０３２により解読され、その後混合操作１０６１により実際のデータストリームに回復される。そして、データパケットからジャンクが除去され、すなわちジャンク除去操作１０５３Ｂによりデータパケットからジャンクデータが除去され、その後、パケットアンスクランブル操作９２８により「受信されたデータ」が回復される。着信データパケットで実行される全ての操作では、ＳＤＮＰゲートウェイでデータパケットが作成されたときに使用されたステート９２０Ｂを使用する必要がある。すなわち、これには特定の時間またはパケット生成時の特定のステート９２０Ｂに関する情報が含まれる。このステート情報は、シグナリングサーバによる別の通信を介して送信されるか、着信データパケットでプレーンテキストまたは静的暗号文として、すなわちＳＤＮＰラストマイルセキュリティ操作で既に知られている復号鍵と共に送信される。しかし、ステート９２０Ｂに含まれるステート情報を必要とする鍵を使用して、ステート９２０Ｂの詳細を暗号化することはできない。そうすると、コードを開

いて、独自のセキュリティクレデンシャル情報を使用できなくなるためである。
【０３５０】
図９Ｃには、具体的にマルチルートラストマイル通信で使用されるパラレルＳＤＮＰペイロードのためのＳＤＮＰラストマイルセキュリティ操作の一例が 示されている。すなわち、この図では、クライアントデバイスから複数のＳＤＮＰゲートウェイへ通信が行われる。前述のシングルルートと同様に、このプロセスには、発信データパケットと着信データパケットのための２方向の操作シーケンスが含まれる。図の上段に示されるように、発信データパケットの場合、「送信されるデータ」が最初にパケットスクランブル操作９２６によりスクランブル化され、次にジャンクデータ１０５３Ｃの挿入により偽装が実行される。場合によっては、パケット全体を完全にジャンクデータで構成することで、ハッカーによるデータマイニングの試みをさらに混乱させることができる。
【０３５１】
次に、これらのパケットはパース操作１０５２が使用される分割操作１０５７により複数のサブパケットに分割され、暗号化操作１０２６に向けて個別に送信される。次に、各断片が共通または個別の暗号鍵を使用して暗号化され、結果として生成される暗号文がデータパケット１１９９Ｃ、１１９９Ｄ、１１９９Ｅとして示される複数のＳＤＮＰペイロードに配置される。そして、パケットは、ラストリンク及びラストマイルへの通信の準備として、個別の区別できるＩＰデータパケット、すなわち「ＩＰパケット準備」にフォーマットされる。実行される全ての操作は動的であり、特定の時間またはセキュリティプロセスの実行中に特定のステート９２０Ｃで発生する。
【０３５２】
図の下段に示されるように、着信データパケットの場合、パラレルＳＤＮＰペイロード１１９９Ｆ、１１９９Ｇ、１１９９Ｈを含むラストリンクからの着信データ、つまり「ＩＰパケット認識」からの着信データは、最初に解読操作１０３２により区分的に解読され、その後混合操作１０６１により実際のデータストリームに回復される。そして、データパケットからジャンクが除去され、すなわちジャンク除去操作１０５３Ｄを使用してデータパケットからジャンクデータが除去され、その後、パケットアンスクランブル操作９２８により「受信されたデータ」が回復される。着信データパケットで実行される全ての操作では、ＳＤＮＰゲートウェイでデータパケットが作成されたときに使用されたステート９２０Ｄを使用する必要がある。すなわち、これには特定の時間またはパケット生成時の特定のステート９２０Ｄに関する情報が含まれる。このステート情報は、シグナリングサーバによる別の通信を介して送信されるか、着信データパケットでプレーンテキストまたは静的暗号文として、すなわちＳＤＮＰラストマイルセキュリティ操作で既に知られている復号鍵と共に送信される。
【０３５３】
ＳＤＮＰラストマイルセキュリティ操作では、着信データパケットと発信データパケットの両方に同じアルゴリズムまたは方法を使用する必要はない。図９Ｄに示されるように、発信データパケットではＳＤＮＰラストマイルセキュリティ操作１１９０Ａが使用され、着信データパケットではＳＤＮＰラストマイルセキュリティ操作１１９０Ｂが使用される。図の上半分に示されるように、発信データパケットには、トランスデューサまたはセンサーからのリアルタイムデータソースの任意の組み合わせを表すデータが含まれるか、通信前に作成されたファイルが含まれる。例えば、マイクロホン１１８０で電気信号に変換された音１１９８Ａ及びカメラ１１８１からのビデオ信号は、オーディオビデオＣＯＤＥＣ　１１８２Ａで同等のデジタルフォーマットに変換される。作成されるフォーマットには、一般的に、プレゼンテーションレイヤであるＯＳＩレイヤ６に従って、標準デバイスで解釈可能及び相互運用可能なｐｎｇ、ｐｉｃ、ｍｐｅｇ、ｍｏｖなどの標準フォーマットが関与する。標準のオーディオビデオフォーマットを使用することで、ファイルを開くために、送信元アドレスと宛先アドレスの間で独自のコードを送信する必要がなくなる。
【０３５４】
次に、オーディオビデオＣＯＤＥＣ　１１８２Ａのデジタル出力は、コンテンツミキサ

ー１１８４を使用して、仮想キーボード１１８３（タッチスクリーンで実現されるキーパッド）からのテキストデータ及びデータファイル１１７９Ａと混合される。そして、静的ファイルからのリアルタイムデータパケットを識別及びラベル付けするために、このミキサーからデータファイルがＳＤＮＰラストマイルセキュリティ操作１１９０Ａに送信され、ＳＤＮＰヘッダ情報がＩＰパケット準備操作１１９１Ａに提供される。そして、ＳＤＮＰラストマイルセキュリティ操作１１９０Ａにより、セキュアデータパケットがＩＰパケット準備操作１１９１Ａに渡され、これにより、次に、ＳＤＮＰシグナリングサーバ１６０３で受信されたルーティング指示に従って、ＳＤＮＰペイロードがＩＰデータパケットに埋め込まれる。データパケットは、マルチルートラストマイル通信用に複数のＩＰパケットに配信されるか、シリアルデータ文字列に連結されて、シングルルートラストマイル通信用の１つ以上のシリアルデータパケットに埋め込まれて収められる。次に、これらのパケットはクライアントＰＨＹ操作１１９２Ａに渡され、レイヤ１とレイヤ２データが追加されたＩＰデータパケットが完成する。

【０３５５】

図の下半分に示されている逆の操作では、クライアントＰＨＹ　１１９２Ｂで受信されたラストリンクからの着信データがＩＰパケット認識操作１１９１Ｂに渡され、これにより着信データが有効なメッセージまたは未知の悪意あるデータパケットとして識別される。有効なメッセージは、ＳＤＮＰタグ、シード、鍵、及びシグナリングサーバ１６０３によってクライアントデバイス及びＩＰパケット認識操作１１９１Ｂに事前に通信された他の識別子を使用して識別される。擬人的には、ＩＰパケット認識操作１１９１Ｂが有効な着信データパケットを期待し、さらには予測する。適切な識別がなく、予期されていないデータパケットは破棄され、それ以上開かれること、または処理されることはない。この方法では、ハッカーは自身のＩＤをＳＤＮＰクラウドに登録することなく、自身を偽装して有効なデータをいかなるＳＤＮＰノードにも送信することができなくなる。

【０３５６】

ＩＰパケット認識操作１１９１Ｂにより、有効なデータパケットがＳＤＮＰラストマイルセキュリティ操作１１９０Ｂに渡される。これにより、データパケットの実際のコンテンツ、すなわちビデオ、オーディオ、テキスト、及びデータファイルの連続して調整された組み合わせが含まれるデータを再構築するために必要な全ての操作が実行される。データパケットの作成で使用される混合操作を元に戻すデマルチプレクサであるコンテンツｄｅ－ｍｕｘ　１１９３（例えば他の発呼者の電話で実行される混合操作１１８４により作成されるシリアルデータファイルを分割する）は、様々なファイルタイプを分離するために使用される。コンテンツｄｅ－ｍｕｘ　１１９３の出力には、メッセンジャーウィンドウ１１９６に表示されるテキスト、データファイル１１７９Ａ、及びオーディオビデオＣＯＤＥＣ　１１８２Ｂに送信されるリアルタイムデータが含まれる。オーディオビデオＣＯＤＥＣ　１１８２Ｂにより、デジタルプレゼンテーションレイヤデータがライブビデオ画像１１９５に変換されるか、スピーカー１１９４を介して音１１９８Ｂに変換される。

【０３５７】

ラストマイルデータ転送の場合、データは図９Ｅに示されるように、バブシュカ（ｂａｂｕｓｈｋａ）というロシアの入れ子人形に類似した方法で、多層構造で埋め込むか、ラップする必要がある。したがって、ＳＤＮＰペイロード４３８は、トランスポートペイロード４３７を表す。これは、トランスポートヘッダ４３６と共にＩＰペイロード４３５を構成する。ＩＰペイロード４３５とＩＰヘッダ４３４の組み合わせは、ＭＡＣペイロード４３２に相当するＩＰデータグラムを表す。ＭＡＣヘッダ４３１及びＭＡＣフッター４３３内にＭＡＣペイロード４３２をラップすることで、物理レイヤ４９０に相当し、ＰＨＹレイヤ１コンテンツとも呼ばれるＭＡＣ「フレーム」が生成される。これは、電気信号、光、電波、マイクロ波などの物理媒で構成される。

【０３５８】

ＳＤＮＰルーティングでは、レイヤ２のＭＡＣヘッダ４３１により、ラストリンクのＭＡＣ接続、すなわちクライアントデバイスとラストマイルリンクの最初のデバイス間の接

続が記述される。クライアントデバイスとＳＤＮＰゲートウェイの送信元アドレスと宛先アドレスを使用することで、レイヤ３のヘッダ４３４により、ラストマイル経由のルーティングのエンドポイントが指定される。しかし、ラストマイルがＳＤＮＰクラウドの一部ではないため、ラストマイルを引き継ぐ正確なルートデータパケットは明示的に指定または制御できない。ＳＤＮＰラストマイル通信では、レイヤ４のトランスポートヘッダ４３６により、ＵＤＰがＳＤＮＰリアルタイムペイロードに使用されること、及び各パケットで使用されるアドホック割り当てＳＤＮＰポートアドレスが指定される。このアドレスは、ポートスキャン（ポート問い合わせ）サイバー攻撃戦略を阻止するために動的に変化する。

【０３５９】

ラストマイルＩＰパケットのペイロードであるＳＤＮＰペイロード４３８には、ゾーン情報、鍵、シードを含むＳＤＮＰプリアンブル１１９８、及び独立して暗号化された暗号文の複数のセグメントのシリアル文字列であるＳＤＮＰデータフィールド１１９９Ａが含まれる。暗号文の復号化されたフォーマットには、プレーンテキストファイル１１９７Ａ、１９９７Ｂ、及び１１９７Ｃが含まれ、それぞれに独自の一意のＳＤＮＰヘッダ及び対応するデータファイルデータ９１、データ９２、及びデータ９３が含まれる。個々のサブヘッダには、必要に応じてタグ、ｚｉｐ、アドレス、緊急性、及びＱｏＳデータを含む情報が含まれる。

【０３６０】

ＳＤＮＰプリアンブルとヘッダの役割は、使用されるコマンドと制御方法により異なる。三者ラストマイル通信では、シグナリングサーバから、コール、ファイル送信、またはセッションを開くための相互通信方法がクライアントデバイスとＳＤＮＰゲートウェイに対して指示される。そのため、メディアデータパケットが送信される前に、ＴＣＰ転送でコマンド及び制御データパケットを使用して両方のデバイスに指示が通信される。したがって、クライアントとＳＤＮＰゲートウェイ間のラストマイル通信に必要な最小限のデータは、着信パケットを識別するために使用されるタグまたはアドレスとなる。場合によっては、例えば、シグナリングサーバに到達できない場合、別の実施形態として、ＳＤＮＰデータパケットにより、そのプリアンブル及びパケットヘッダで追加のデータが伝送される。

【０３６１】

図９Ｆに示されるデータパケット及び付随する表１１７７は、ＳＤＮＰペイロード４３８内でＳＤＮＰ情報を運ぶために使用される１つの例示的なフォーマットを示すものである。データパケットには、ＳＤＮＰプリアンブル１１９８及び対応するデータフィールド「データＸフィールド」を有する１～８個のデータフィールドヘッダ１１７８Ｘが含まれる。「データ１フィールド」、「データ２フィールド」などの各データフィールドでは、対応するヘッダＨｄｒ　１、Ｈｄｒ　２などが先行し、音声、テキスト、ビデオ、写真、映画、ファイルなどのコミュニケコンテンツが伝送される。データフィールドの数値は、４ｂのロングフィールド＃によって決定される１～８、すなわちバイナリ０００１～バイナリ１１１１と様々に異なる。ＳＤＮＰプリアンブル１１９８とＳＤＮＰペイロード４３８の長さは、フィールド＃仕様の影響を受ける。１つのフィールドのみが選択された場合、すなわちフィールド＃＝０００１バイナリの場合、ＳＤＮＰプリアンブル１１９８にはＬ　Ｆｌｄ　１のみが含まれ（Ｌ　Ｆｌｄ　２～Ｌ　Ｆｌｄ　８は除外される）、ＳＤＮＰペイロード４３８にはＨｄｒ　１とデータ１フィールドのみが含まれる。最大８つのフィールドが選択された場合、すなわちフィールド＃＝１１１１バイナリの場合、ＳＤＮＰプリアンブル１１９８には８つの長さ指定Ｌフィールド１からＬフィールド８が含まれ、ＳＤＮＰペイロード４３８には８つのデータフィールドとヘッダが、Ｈｄｒ　１、データ１フィールド、Ｈｄｒ　２、データ２フィールド・・・Ｈｄｒ　８、データ８フィールドとして順番に含まれる。示されるように、ＳＤＮＰプリアンブル１１９８には、フィールド長の仕様Ｌ　Ｆｌｄ　１、Ｌ　Ｆｌｄ　２、Ｌ　Ｆｌｄ　８が含まれる。Ｌ　Ｆｌｄ　２とＬ　Ｆｌｄ　８の間にある小さなギャップは、シーケンスの継続を表すものであり、データのギャ

ップを表すものではない。
【０３６２】
Ｌ　Ｆｌｄ　Ｘで指定される各データフィールド長は、ゼロまたは０Ｂ（ヌルデータフィールド）からＦＦＦＦまたは６５，５３５Ｂの最大１６進数まで様々に異なる。イーサネット（登録商標）互換性における実用的な理由により、任意の１つのフィールドの最大データパケット長は１５００Ｂまたは１６進数０５ＤＣに制限することが好ましく、全てのデータフィールドの合計長は９０００Ｂまたは１６進数２３２８のジャンボパケットサイズを超えてはならない。各データフィールドに指定される長さは、個別に異なる場合がある。例えば、Ｌ　Ｆｌｄ　８＝００００の１６進数など、ゼロのフィールド長の場合は、対応するデータ８フィールドは削除されるが、対応するヘッダＨｄｒ　８は削除されない。ヘッダは、フィールド＃の指定によってのみ削除される。
【０３６３】
このＳＤＮＰプロトコルに従うと、様々なデータフィールドにわたるコンテンツの配分は非常に柔軟となる。単一の宛先に向けられたデータは、単一のデータフィールドに含まれる場合、または偽装目的で複数のデータフィールドに分割され、ジャンクデータとマージされる場合がある。データフィールドのサイズは個々に異なってもよい。純粋なジャンクデータを含むデータフィールドを含めること、またはジャンクデータのみを含むデータパケット全体を生成することもできる。しかし、効率的なパケットルーティングを行うには、異なる宛先をターゲットとするデータはそれぞれ独自のヘッダを有する個別のデータフィールドに分割する必要がある。
【０３６４】
ＳＤＮＰパケットフォーマットは、ＳＤＮＰクラウドなどの複数のクラウド及びゾーン間、またはラストマイル通信を含むＳＤＮＰネットワーク全体のエンドツーエンド転送に適用できる。ＳＤＮＰデータパケットの内容はネットワークを通過するときに変化するが、ＳＤＮＰパケットのフォーマットは変化しない。このフォーマットには最小限のデータオーバーヘッドしか含まれていないため、ＳＤＮＰデータパケットフォーマットは、大きなペイロードまたはタイムクリティカルなリアルタイム通信に等しく適用できる。パケットフォーマットは、双方向のデータフロー、すなわちラストマイルからＳＤＮＰゲートウェイへのデータフロー、及びＳＤＮＰクラウドへのデータフロー、または宛先クライアントデバイスへのラストマイル全体の転送のために、逆にクラウドから発せられてＳＤＮＰゲートウェイを出るデータパケットの配信に適用できる。
【０３６５】
動作中、ＳＤＮＰデータルーティングの方向は、図９ＥのＩＰヘッダ４３４内に記述されるネットワークレイヤ３の送信元アドレス及び宛先アドレスによって決定される。ルート上の次のメディアノードへの送信のためにメディアノードによりパケットが準備されるときに、各パケットに送信元アドレスと宛先アドレスがロードされる。トライチャネル通信では、パケットの宛先のＳＤＮＰまたはＩＰアドレスは、発信パケットの準備の前に、コマンド及び制御（Ｃ＆Ｃ）パケットとしてシグナリングサーバからメディアノードに配信される。一般的に、シグナリングサーバから、送信（送信者）デバイスと宛先（受信者）デバイスの両方を含む通信パスの全てのノードにＣ＆Ｃ指示を送信することができる。例えば伝搬遅延が長いリンクなど、シングルチャネル通信のみが利用可能な場合は、シグナリングサーバからメディアノードに対して、着信パケットまたはその処理について事前に警告を発信することができない。この場合、ルーティングアドレスはＳＤＮＰペイロード４３８の着信データパケット内で伝送される。このような場合、ルーティング、ステート情報、及びセキュリティクレデンシャル情報など、着信ＳＤＮＰパケットに含まれるデータフィールドを使用して着信パケットを処理する方法に関して、メディアサーバはデフォルトの指示に従って動作する。
【０３６６】
ペイロード４３８は、プリアンブル１１９８を含む読み取り可能な部分、及び「隠蔽されたフォーマット」のデータを含む読み取り不可能な部分１１９９ａの２つの部分で構成

される。このパケットのコンテンツについては、暗号化、スクランブル化、及び場合によってはジャンクデータの挿入など、任意の数のコンシールメント技術が使用され、そのコンテンツが隠される。使用可能なコンテンツ１１９７ａ、１９９７ｂ、及び１１９７ｃを抽出するには、コンシールメント方法を元に戻す必要がある。これらのパケットには、今後の発信パケットの宛先アドレスが含まれる。アドレスは、次のパケットが準備され暗号化されるまでの短時間のみ、隠蔽されていないフォーマットまたは復号化されたフォーマットで存在できる。

【０３６７】

説明されるように、ＳＤＮＰプリアンブル１１９８には、パケット全体に関連する情報が含まれる。データフィールドの仕様とは別に、図９Ｆには、ＳＤＮＰパケットが作成されるＳＤＮＰゾーン（例えばゾーンＵ１、２つの数値シード、及び２つの鍵など）を同じく含むＳＤＮＰプリアンブル１１９８が示されている。これらの鍵とシードは、スクランブル化／アンスクランブル化、ジャンク挿入／除去、混合／分割、暗号化／復号化プロセスで、ゾーン固有のセキュリティクレデンシャル情報として使用できる。シードと鍵は、データフィールドを開いて読み取る際に必要なセキュリティクレデンシャル情報を配信するための排他的な手段として、またはシグナリングサーバからクライアントデバイス及びＳＤＮＰゲートウェイに送信されるコマンド及び制御パケット、つまりコミュニケコンテンツをメディアパケットで伝送することに関与しないコンピュータのネットワークと組み合わせて使用できる。

【０３６８】

シードと鍵はセキュリティクレデンシャル情報の一部のみで構成されており、データにはそれらを使用するために必要な情報が欠如しているため、シードと鍵はパブリックに、すなわち暗号化されていないフォーマットで安全に配信できる。欠落しているセキュリティクレデンシャル情報の他の部分は、別のデータパケットで事前に送信される場合、またはアルゴリズムの共有秘密、ルックアップテーブル、ネットワーク経由では配信されず、かつメッセージの一部ではないコードが含まれる場合がある。暗号鍵は、送信者と受信者の両方が鍵を保持している場合の対称鍵の場合、または送信者を含むパブリックが暗号鍵にアクセスできるけれども受信者、すなわち暗号鍵を生成した当事者のみが復号化キーを保持する公開鍵の場合がある。さらに、全てのセキュリティクレデンシャル情報はＵ１などの特定のセキュリティゾーンに制限され、動的で、特定の期間または指定された時間内に使用されないと期限切れになるステートに制限される。例えば、セキュリティ操作に関してシグナリングサーバからＳＤＮＰデバイスに個別に指示が出される場合など、シード及び鍵データフィールドがセキュリティクレデンシャル情報として使用されない場合は、これらのフィールドには暗号鍵として表示される偽の数値が入力される。これにより、サイバー攻撃者はおとりのセキュリティ鍵の分析に時間を浪費することになる。

【０３６９】

ラストマイル通信では、クライアントデバイスとＳＤＮＰゲートウェイ間の中間ルータでは、転送されたデータパケットが処理、解釈、または開かれることはない。これは、これらがＳＤＮＰネットワークの一部ではなく、中に含まれるＳＤＮＰパケットデータを照会または解釈する機能がないためである。代わりに、全てのセキュリティ操作はＳＤＮＰクライアントとＳＤＮＰゲートウェイの２つのエンドポイントで排他的に実行される。これは、これらのデバイスのみがＳＤＮＰ通信ノードとして動作するためである。各エンドポイントでＳＤＮＰプロトコルが動的に実行されるため、ラストマイル通信はラストマイル全体でハイパーセキュアとなる。相手の発信者もＳＤＮＰソフトウェアを実行している場合は、その発信者のラストマイルも前述のＳＤＮＰ方法によって保護され、ハイパーセキュア通信が発信者間の「エンドツーエンド」で保証される。

【０３７０】

しかし、エンドデバイスがＳＤＮＰクライアントではない場合は、発信者に最も近いルータ、すなわちラストリンクルータをＳＤＮＰファームウェアで有効化する。この場合、ＳＤＮＰは有効化されないが、ＳＤＮＰが有効化されたルータで実行される特別な機能に

よりラストリンクを合理的に保護できる。この代替のラストリンクセキュリティ方法は、本開示の後続のセクションでより詳細に説明されており、本セクションでは詳述されない。説明されている方法は、ラストリンク通信の保護に適用できるが、ラストマイルの他の部分を保護するには不十分である。

【０３７１】

図９Ｆに示されるように、各ＳＤＮＰデータフィールドには、ＳＤＮＰデータフィールドヘッダ１１７８Ｘが付随している。これには、これが関連付けられるデータフィールドに一意に適用できるけれども、他のデータフィールドには役に立たない情報が含まれる。具体的には、開示される実施形態では、各ヘッダには、関連付けられたデータフィールド内に含まれるデータの種類を記述するデータタイプフィールド、特定のデータフィールドとその宛先を識別するために使用される宛先アドレスフィールド、ゾーン情報をあるゾーンから別のゾーンに転送するために使用されるフィールドゾーン、緊急性、及び配信情報が含まれる。示されるように、各ＳＤＮＰデータペイロード４３８には、１つのＳＤＮＰプリアンブル１１９８、及び１つ以上のＳＤＮＰデータフィールドヘッダ１１７８ｘ及び対応するデータｘフィールドが含まれる。ｘは個別のペイロードの数を示している。これは、ペイロードのサイズと緊急性に応じて５～５０の範囲となる。

【０３７２】

記述される情報のほとんどがシグナリングサーバからＳＤＮＰクライアントとＳＤＮＰゲートウェイに提供されるが、ラストマイルデータパケットで必ず伝送される基本コンポーネントが１つある。これは、データパケットを識別するために必要な「アドレスフィールド」またはタグである。ＳＤＮＰペイロードの宛先アドレス（図では「Ｄｅｓｔ　Ａｄｄｒ」と略記される）と呼ばれるフィールドには、あるデータフィールドと別のデータフィールドのＩＤを十分に区別できる一意の識別子を含めることができる。その目的は、空港における荷物や宅配便で配送される箱のタグ付けと追跡に使用されるバーコードの機能に似ている。データパケットを識別する際の競合を防ぐために識別子が一意となるように、例えばアドレスタイプには、数値タグ、ＳＤＮＰ　ｚｉｐ、ＩＰｖ４またはＩＰｖ６アドレス、ＮＡＴアドレス、さらにはＰＯＴＳの通常の電話番号を含めてもよい。宛先アドレスフィールドのサイズは、選択されたアドレスタイプの種類によって異なる。

【０３７３】

ルーティング中にパケットの匿名性を維持するために、実際の電話番号またはＩＰアドレスを使用するのではなく、ＳＤＮＰ宛先アドレスとしてＳＤＮＰ　Ｚｉｐコードなどの機密コードを使用することが推奨される。動作中、ＳＤＮＰクライアントからデータパケットがＳＤＮＰゲートウェイに到着するたびに、ＳＤＮＰペイロードが復号化され、次に宛先アドレスの識別について各データフィールドヘッダの検査が実施される。データパケットを復号化または処理して、パケット作成時に使用されるコンシールメント方法を元に戻すまで、データヘッダを検査することはできない。デュアルチャネルまたはトライチャネル通信の場合、図９Ｇに示されるように、シグナリングサーバ１６０３から、データパケットの到着予定及びそれに対応する識別マーキングとセキュリティクレデンシャル情報がＳＤＮＰゲートウェイに事前に通知される。そのため、ＳＤＮＰクライアントから送信されたラストマイル通信を含むデータパケット４３８ＡがＳＤＮＰゲートウェイで受信されると、ＳＤＮＰペイロードを暗号文からプレーンテキストデータパケット４３８Ｂに変換するため、ゲートウェイでＳＤＮＰラストマイルセキュリティ操作１１９０Ｄが実行される。セキュリティ操作とは、発信データパケットを変更してそのコンテンツのコンシールメントプロセス、及び着信データパケットを変更してそのコンテンツを明らかにするプロセスである。具体的には、着信データパケットで実行されるセキュリティ操作は、暗号化を解除する復号化、スクランブル化を元に戻すアンスクランブル化、挿入されたジャンクを取り去るジャンク除去、分解を元に戻す混合など、転送前に実行されるコンシールメント操作を元に戻すことによりコンテンツを回復するために使用される。これらのプロセスは、データパケット作成時のステートとゾーンに従って実行される。発信データパケットの場合、セキュリティ操作には、転送前にデータパケット作成時のステートとゾーンに

従って暗号化、スクランブル化、ジャンク挿入、及びパケット分割を実行することでデータパケットのコンテンツをコンシールメントする操作が含まれる。データパケット４３８Ａの暗号化されていないシード及び鍵データフィールドは、無視する、または暗号文を復号化するためにシグナリングサーバ情報と一緒にオプションで使用できる。結果の操作により、データフィールド１及びデータフィールドの宛先アドレス、データタイプ、緊急性、配信情報を含むＨｄｒ　１とラベル付けされた関連データフィールドヘッダ１１７Ｄが表示される。このような場合、宛先アドレスはルーティングアドレスではなく、単にＳＤＮＰ　Ｚｉｐ、すなわちパケットを識別するために使用されるタグで、特定の会話の一部である。

【０３７４】

シグナリングサーバ１６０３からの指示に一致するＳＤＮＰ　Ｚｉｐコードなど、識別された宛先フィールドを含む特定のデータフィールドが見つかると、データフィールドが抽出され、オプションでミキサー１１８４Ｚによって他の関連コンテンツと混合され、ＳＤＮＰパケット準備操作１１９１Ｚによって新しいＩＰまたはＳＤＮＰデータグラムに再度ラップされて次の宛先に配信される。クラウドに向かう新しいデータパケットには、新しいパケットの宛先とデータコンテンツであるＳＤＮＰペイロード４３５Ｚを含むＳＤＮＰヘッダ４３４Ｚが含まれる。ＩＰアドレスまたはＳＤＮＰアドレスとしてシグナリングサーバ１６０３からゲートウェイメディアノードに供給される宛先には、ＳＤＮＰクラウドノードとして動作する別のＳＤＮＰサーバを含めること、または別のＳＤＮＰクライアントへのラストマイル通信を含めることができる。このようなトライチャネル通信の場合、宛先アドレスは実際にはアドレスではなく、パケットを識別する手段であり、次の宛先はＳＤＮＰゲートウェイで既に認識されている。パケットの宛先がＳＤＮＰクラウドルーティングである場合は、次に、ラストマイルで使用されるＵ１認証情報ではなく、クラウドのＺ１セキュリティクレデンシャル情報に従って、ＳＤＮＰクラウドセキュリティ操作１１９０Ｚによりデータパケットが処理される。

【０３７５】

シングルチャネル通信の場合は、図９Ｈに示されるように、（ｉ）ローカルネットワークで動作するシグナリングサーバがない、（ｉｉ）シグナリングサーバが一時的にオフラインである、または（ｉｉｉ）シグナリングサーバがビジー状態で、時間内にパケットを先制的にルーティングできないといういずれかの理由により、目前に迫っているデータパケットとそのデータフィールドの到着の前に、シグナリングサーバからＳＤＮＰゲートウェイへの通知が行われない。このような場合、ＳＤＮＰクライアントからのデータパケット４３８Ａにより必要なセキュリティクレデンシャル情報ゾーンＵ１、シード１、シード２、鍵１、鍵２が伝送され、ＳＤＮＰラストマイルセキュリティ操作１１９０Ｄによって暗号文データパケット４３８Ａがプレーンテキストデータパケット４３８Ｂに変換されなければならない。特定のメディアノードでフィールドのコンテンツが必要でない場合も、標準のＳＤＮＰデータパケットフォーマットにより、これらのデータフィールドが予約される。例えば、データパケットの作成に使用される特定のコンシールメントプロセスで鍵２フィールドが使用されない場合は、そのフィールドのデータは無意味となり、宛先ノードで使用されることはない。それにも関わらず、データパケットにより、使用されるフィールドまたは使用されないフィールドに同じバイト数が予約されるため、全てのＳＤＮＰデータパケットのフォーマットは同種である。データパケット４３８Ａの暗号文が復号化されると、ＳＤＮＰゲートウェイにより、プレーンテキストデータパケット４３８Ｂから、データパケットデータ１フィールドのコンテンツ及び関連付けられたＨｄｒ　１フィールドヘッダ１１７８Ｄが抽出される。第一にトライチャネル通信で着信パケットが予期されていることを確認するため、第二に新しいＳＤＮＰアドレスを生成するためという２つの理由により、このデータパケットで、ＩＰパケット認識プロセス１１９１Ｄにより、Ｈｄｒ　１フィールドヘッダ１１７８ＤからのＡタイプと宛先アドレスのデータフィールドが組み合わされる。この新しいＳＤＮＰアドレスはＤタイプ、緊急性、配信フィールドと組み合わせられ、ＳＤＮＰパケット準備操作１１９１Ｚにより処理されて、発信データパ

ケットにＳＤＮＰヘッダ４３４Ｚが作成される。データ１フィールドのコンテンツも着信プレーンテキストデータパケット４３８Ｂから抽出され、そのコンテンツはオプションで１１８４Ｚと他の発信コンテンツと混合され、発信ＳＤＮＰペイロード４３５Ｚが作成される。その後、パケットは、転送の準備のためにＳＤＮＰクラウドセキュリティ１１９０Ｚによって処理される。このようにして、着信データパケットを識別し、必要に応じて転送アドレスを提供するために、アドレスフィールドでは複数の機能が実行される。

【０３７６】

シグナリングサーバからの指示を最初に受信せずに、メディアノードでデータパケットが受信された場合は、メディアノードは着信データパケットの処理方法及び発信データパケットの準備方法に関するデフォルトの指示に戻って動作する。メディアノードに未通知の着信パケットの処理方法に関する指示がない場合は、データパケットは破棄される。未識別のパケットの処理方法に関する指示がメディアノードで有効化されていない場合は、メディアノードでは最初にセキュリティクレデンシャル情報に従ってパケットが有効なＳＤＮＰパケットであることが確認され、これに応じて処理が実施される。しかし、例えば暗号化コード、シード、または送信元アドレスが無効であるために送信者を特定できない場合は、パケットは詐欺として破棄される。

【０３７７】

図９Ｆでは、「フィールドゾーン」とラベル付けされたパケットフィールドは、特定のフィールドが作成されたゾーンを示すものである。すなわち、例えばＵ１またはＵ２ゾーン設定で、過去の暗号化またはスクランブル化が実行されたかどうかである。ネスト化されたセキュリティプロトコルまたは他のネスト化されたコンシールメント方法の場合、データパケットのアンスクランブル化、復号化、またはコンシールメントの復元には、鍵、シード、時間、またはステートなどの追加情報が必要となる。この場合、「フィールドその他」とラベル付けされたパケットフィールドを使用して、フィールド固有の情報を伝送できる。一般的に、暗号化されたデータフィールドが次にスクランブル化される、または再度暗号化されるようなネスト化されたセキュリティプロトコルを除き、これらのフィールドは使用されない。ネスト化されたセキュリティ方法を使用して、データパケット準備と全く逆の順序でデータ回復を実行する場合は注意が必要である。そうしないと、コンテンツが永久に失われる。

【０３７８】

「データタイプ」とラベル付けされたパケットフィールドを使用する場合、コンテキスト固有のルーティングが容易化され、ビデオやライブビデオのような時間に敏感な情報を含むデータパケットから、リアルタイムの通信を要求することなく、データ、録画、テキスト、及びコンピュータファイルを区別する、すなわちリアルタイムルーティングと非リアルタイムルーティングとを区別することができる。データタイプには、音声、テキスト、リアルタイムビデオ、データ、ソフトウェアなどが含まれる。

【０３７９】

「緊急性」及び「デリバリ」とラベル付けされたパケットフィールドは共に、特定のデータフィールドのデータをルーティングする最良な方法を決定するために用いられる。緊急性には、遅い（ｓｎａｉｌ）、普通、優先、及び緊急のカテゴリが含まれる。デリバリには、通常、冗長、特別、及びＶＩＰのカテゴリを示すＱｏＳマーカが含まれる。本発明の１つの実施形態では、表１１７７に示されるように、様々なデータフィールドのバイナリサイズは、通信に必要となる帯域幅が最小となるように選択される。例えば、示されるように、データパケットが０～２００Ｂの範囲であり、データフィールドには２００Ｂの８パケットを含めることができるため、ＳＤＮＰパケットでは１，６００Ｂのデータを運ぶことができる。

【０３８０】

図９Ｇと図９Ｈの両方には、クライアントデバイスからゾーンＵ１のデータパケットがラストマイル経由でゲートウェイノードに送信される場合が示されている。次に、ゲートウェイノードにより着信データパケットが処理され、ゾーンＵ１セキュリティクレデンシ

ャル情報を使用して、行われたラストマイルセキュリティ及びコンシールメント方法が元に戻される。その後、ゲートウェイノードにより、混合プロセス１１８４Ｚでパケットのコンテンツが他のパケットのコンテンツと混合され、ゾーンＺ１のセキュリティクレデンシャル情報が使用され、ＳＤＮＰクラウドを介した転送にバインドされる新しいパケットが作成される。

【０３８１】

例えば、ＳＤＮＰクラウドからクライアントの電話（受信者）へ送信される場合など、ＳＤＮＰゲートウェイでクラウド（別のゲートウェイを含む）からのデータパケットが受信され、データパケットがクライアントデバイスに送信されるとき、同様のプロセスが使用される。図９Ｉに示されるように、デュアルチャネルまたはトライチャネル通信の場合、シグナリングサーバ２６０３から、クラウドからのデータパケットの到着予定及びそれに対応する識別マーキングとセキュリティクレデンシャル情報がＳＤＮＰゲートウェイに事前に通知される。そのため、ＳＤＮＰクラウドからのデータパケット２４３８ＡがＳＤＮＰゲートウェイで受信されると、ＳＤＮＰペイロードを暗号文からプレーンテキストデータパケット２４３８Ｂに変換するため、ゲートウェイでＳＤＮＰクラウドセキュリティ操作２１９０Ｄが実行される。データパケット２４３８Ａの非暗号のシード及び鍵データフィールドは、無視する、または暗号文を復号化するためにシグナリングサーバ情報と一緒にオプションで使用できる。データフィールドの使用は、パケットのペイロードをコンシールメントする際に使用されるアルゴリズムに依存する。例えば、暗号化が使用されていない場合は、暗号鍵を含むフィールドは無視される。

【０３８２】

結果の操作により、多数のデータフィールドが抽出される。後続の操作で、コンテンツ分割操作２１８４Ｚによりこれらのデータフィールドが分割され、認識操作２１９１Ｄによりデータフィールド１及びＨｄｒ　１とラベル付けされた関連データフィールドヘッダ２１１７Ｄを含む特定のコンテンツが抽出される。ヘッダＨｄｒ　１には、データフィールドの宛先アドレス、データタイプ、緊急性、配信情報が含まれる。次に、抽出されたデータフィールドは、次の宛先への配信のために、ＳＤＮＰパケット準備操作１１９１Ｚによって新しいＩＰまたはＳＤＮＰデータグラムに再度ラップされる。クラウドに向かう新しいデータパケットには、新しいパケットの宛先（個人の電話番号に対応するＩＰアドレス）とデータコンテンツ、ＳＤＮＰペイロード２４３５Ｚを含むＳＤＮＰヘッダ２４３４Ｚが含まれる。発信パケットは、クラウドで使用されるＺ１認証情報ではなく、ラストマイルのＵ１セキュリティクレデンシャル情報に従ってＳＤＮＰラストマイルセキュリティ操作２１９０Ｚにより処理される。

【０３８３】

シグナリングサーバが利用できない場合、すなわちシングルチャネル通信の場合は、デフォルトの指示として以前に配信された指示に従い、メディアノードで着信データパケットが処理される必要がある。このような場合、着信データパケットは、送信者が有効なＳＤＮＰクライアントであることを確認するために必要な基準（ＳＤＮＰ　Ｚｉｐコードまたは事前に決められた共有秘密として以前に配信された認証コードなど）が用いられる。パケットが有効であると判断された場合は、パケットはデフォルトの指示に従って処理される。そうでない場合は、パケットは破棄される。

【０３８４】

前述の方法は例示的なものであり、データパケットの処理とルーティングを特定のデータパケットフォーマットに制限することを意図するものではない。

【０３８５】

<u>通信におけるセキュリティ及びプライバシー</u>

【０３８６】

ラストマイル通信における重要な考慮事項は、セキュア通信とプライベートな通信の両方をサポートするネットワークの能力である。多くの場合、プライバシーとセキュリティは関連付けられるが、これらは同じものではない。通信において使用されるセキュリティ

という用語は、「認識可能なフォーマットの通信データへの不正アクセスを防ぐための規律」と見なされる。しかし、セキュリティは、個人または機関が通信にアクセスする、または通信を監視する権利を有する場合には適用されない。プライバシーは、「他者に観察または邪魔されることのない、及び世間の注目を浴びない状態または条件」と定義される。法律用語では、プライバシーは、自身の個人情報へのアクセスを制御する個人の権利と定義される。

【０３８７】

通信では、音声通話、ビデオ、テキスト、電子メール、パーソナルメッセージングなどにおける個人のプライバシー権は国によって大きく異なる。通信に法的に有効な方法でアクセスを提供する上で適用される政府規制に準拠する役割については、後続のセクションで説明する。これはさておき、理想的なネットワークと通信システムでは、通信のハッキングを防止する、すなわち完全にセキュアであり、かつ全ての通信が知る権利のある人物に限定される、すなわちプライベートであることを保証する必要がある。

【０３８８】

ネットワークのプライバシーとセキュリティ機能を評価する際は、ネットワークのラストマイルと接続されたデバイスを慎重に検討する必要がある。多くの場合、情報アクセス権の確立に使用されるセキュリティクレデンシャル情報により、ラストマイルと接続されたデバイスにおけるネットワークのセキュリティとプライバシーが左右される。すなわち、ラストマイルが最も脆弱な部分となる。通信ネットワークにおける以下４つの可能な組み合わせを考慮する必要がある。

・セキュアかつプライベートなネットワーク。個人の観点からは、これは理想的なネットワーク性能を示すもので、情報のセキュリティ及び個人のプライバシーの両方を保証するものである。極端に言えば、真にセキュアなプライベートネットワークとは、個人、政府、機関、または企業が有意義な通信を傍受すること、及び個人の行動、行為、連絡先や仲間、個人の嗜好、活動などに関するプライベートデータを取得できないことを意味する。プライバシー権を擁護する者は、理想的なセキュアプライベートネットワークを機密通信の至適基準と見なしているが、政府、セキュリティ組織、及び企業は通信の絶対的な自律性に問題があり、これにより個人が完全に秘密裏かつ無難に犯罪行為やテロに関与できるようになると見なしている。

・プライバシーを欠く非セキュアネットワーク。セキュアでなく、プライバシーの規定がないネットワーク（今日のインターネットＯＴＴ事業者など）は、通信チャネルを使用する個人、グループ、クラブ、企業、または政府に重大なリスクをもたらす。サイバーハッカーはコールやデータに簡単にアクセスできるため、悪意のある人物はこの情報を任意の目的に使用できる。悪戯仕掛け人やスパマーは非セキュア通信チャネルを乗っ取ることで、大混乱を招く、ネットワークをスパムで溢れさせる、サービス拒否攻撃を開始する、または有害な悪戯を展開することができる。イデオローグ、政治活動家、宗教カルトは非セキュア通信チャネルを利用することで、政変の促進、政府職員の失脚、暴動の唆し、政府打倒を目的として、機密情報を漏洩させることができる（数十万件に及ぶ政府の機密文書をウィキリークスが公開していることで、国際的な反響の嵐が発生するというシナリオを描く有名なフィクション映画「フィフス・エステート／世界から狙われた男」（ＤｒｅａｍＷｏｒｋｓ(c)２０１３）を参照されたい）。経済的動機のある組織犯罪やマフィアのサイバー犯罪者は、金銭犯罪、例えば窃盗、資金流用、詐欺、個人情報窃盗、マネーロンダリング、強奪、恐喝、他の重罪に焦点を合わせて攻撃を行う。麻薬カルテル、ギャング、テロリストのように恐喝や脅迫に関与する人物は、非セキュア通信を監視することで、暴行、誘拐、殺人、爆撃、またはテロ行為のような暴力犯罪を計画及び実施することを目的として、競合他社、敵、標的の被害者の位置、動き、行動を追跡することができる。最後に、個人的なサイバー攻撃の場合は、非セキュア通信を利用することで、社会保障番号、パスポート、銀行情報、クレジットカード情報、医療記録、他の個人機密情報といった個人情報を含むデータベースを不正にハッキングできる。

・プライバシーを欠くセキュアなネットワーク。プライバシーを欠くセキュアなネットワ

ークの例として、ＩＴ（情報技術）マネージャーまたはセキュリティ部門が、企業ネットワーク上で不適切または違法な通信が発生しないことを保証することを目的として、全ての企業通信を監視する権利と権限を有する企業アカウントが挙げられる。ネットワークはハッカーやサイバー犯罪者から保護されてはいるが、こうしたネットワークにおける通信はプライベートではなく、企業通信インフラストラクチャの不正な個人使用、企業スパイ、機密保持契約の違反、知的財産の不正開示（ＩＰ漏洩）、セクシュアルハラスメント、レギュレーションＦＤ（ｒｅｇ．　ＦＤ）違反、インサイダー取引、ＦＣＰＡ（連邦海外腐敗行為防止法）違反、汚職、贈収賄、詐欺、財務報告違反、証券違反などの不正行為を検出するために、許可された主体により監視される場合がある。企業通信の場合、企業は入社した個人に、自社の通信はプライベートではなく、企業の電話、電子メール、テキスト、パーソナルメッセージング、ＳＭＳ、及び他のコミュニケなどは監視される可能性があることを通知する。民事事件か刑事事件かに関わらず、訴訟手続が発生した場合は、個人情報が企業情報に混じっていたとしても、こうしたコミュニケが法廷に証拠として提出される可能性がある。本質的に、企業の従業員が企業の通信、デバイス、及びネットワークを個人的な使用に利用すると、（弁護士と依頼人の特権の場合を除いて）全ての情報は攻撃のかっこうの的となり、プライベートとは見なされなくなる。この理由及び他の理由から、Ｌｉｎｅ及びＫａｋａｏＴａｌｋなどの個人用メッセンジャーをビジネスと個人用に混合して使用すると、従業員がテキストチャット、写真、及びファイルの検査を防ぐためにプライバシー権を行使できないため、特に問題となる。

・半プライベートの非セキュアネットワーク。半プライベートの非セキュアネットワークとは、データを伝送するネットワークが盗聴などによりハッキングされる可能性があるにも関わらず、特定の条件が満たされていれば、セキュリティの欠如を問わず、プライベート取引を機密に実行できるネットワークを指す。この場合、ハッカーがコールを傍受しても発見できない共有秘密を使用する様々な手段により発信者のＩＤを確認することでプライバシーが確立される。プライベートの非セキュア通信の一般的な例として、音声による銀行取引が挙げられる。例えば「お客様が昨晩に食事をしたレストランの料金はクレジットカードで支払われています。どの都市で食事しましたか？」または「ワイナリーから定期的に請求書が届いています。どのワイナリーですか？」など、詐欺師が回答を知っている確率が低い質問を絶えず変更して発呼者に質問することで、発呼者のＩＤを確認する。別の質問例として、「小学校で気に入っていた先生の姓は何といいますか？」が挙げられる。こうしたＩＤ検証方法を良好に機能させるためには、銀行が非公開情報（クレジットカードの明細書など）にアクセスできるようにするか、またはクライアントが口座を開いた時点で、銀行とそのクライアントが電子的にではなく対面で共有秘密を確立する必要がある。発信者のＩＤが確認されると、クライアントは特定の操作を実行するように機関に指示でき、これによりサイバー犯罪者に利益がもたらされることはない。例えば、発信者が「１万ドルを普通預金から当座預金口座に移動する」といった指示を出すことができる。しかし、送金が別の銀行に送られる場合は、クライアントのプライバシーを保証するために、さらに厳密な検証を行う必要がある。いずれにせよ、電子的か聴覚的かに関わらず、プライバシーの確保は、通信で共有秘密が暴露されないという条件が満たされているかどうかに依存する。この条件が満たされなければ、全てのプライバシーが喪失し、口座が危険に曝される可能性がある。そのため、非セキュア回線における認証通信は、意味する条件付きプライバシーを意味する半プライベートを指す。別の例または非セキュアネットワーク経由の半プライベート通信として、セキュリティトークン、すなわち銀行が発行したものでクライアントのみが所有するデバイスを利用して実行されるものが挙げられる。デバイスにより生成された擬似乱数が銀行の担当者に通知され、当該担当者がその番号が銀行の承認済み番号と一致することを確認する。数字は８桁以上であるため、最初の試みで正しいコードが推測される可能性は非常に低い。間違ったトークン番号が伝えられた場合は、コールが終了し、口座が凍結され、そして不正行為対応部門に調査を促す警告が発せられる。この場合、非セキュアネットワークでプライバシーを確保することの重要性は、口座番号、ＰＩＮ、クレジットカード情報のような機密情報を口頭で明かすことなく通

信できるかどうかに依存する。すなわち、通信は半プライベートとなる。
【０３８９】
ＩＤ検証及びＡＡＡ
【０３９０】
セキュリティとプライバシーの概念は、正確かつ信頼性の高いＩＤ検証、すなわち発信者が本人であるということに依拠する。データと通信を有効に使用し、違法または未承認のアクセスを防止する上で、「認証」とも呼ばれるＩＤ検証が重要となる。国家安全保障、法執行機関、知的財産所有、企業、及び個人に関する権利において、信頼性の高いＩＤ検証は重要である。ＩＤ検証の重要性として、以下のような例が挙げられる。
・国家安全保障においては、犯罪者、スパイ、テロリスト、麻薬密売人、及び国家秘密の漏洩を企む人物や国家安保を脅かす人物のＩＤを追跡するために、発信者のＩＤ検証を行うことが重要となる。機密、秘密、または最高機密のコミュニケ、データ、ファイルへのアクセス、読み取り、または送信を許可されている個人を特定する上でも、これは同様に重要となる。
・法執行機関にとっては、強盗、放火、麻薬密売、密輸、売春や人身売買、強奪、脅迫、他の重罪などの犯罪行為に関与する個人または組織を識別するために、発信者のＩＤ検証を行うことが重要となる。警官、消防隊員、救急隊員、パークレンジャー、航空警察官、ＴＳＡや空港警備員、港湾局員、税関担当者、沿岸警備隊員など、法執行機関による認定を受けている個人を特定する上でも、これは同様に重要となる。
・映画スタジオなどの知的財産所有者にとっては、音楽、映画、書籍、ビデオなどの著作権で保護された材料の著作権侵害や不正配布に関与する個人、組織、及び事業体を識別するために、発信者のＩＤ検証を行うことが重要となる。知的財産及び著作物の有効かつ合法的な配布を確認する上でも、これは同様に重要となる。
・企業にとっては、重要な非公開情報の意図的または偶発的な開示を追跡し、商業スパイまたは知的財産の違法開示に従事する個人、及び詐欺または企業通信の個人使用のような他の犯罪を犯す個人を識別するために、従業員のＩＤ検証を行うことが重要となる。企業の機密情報を利用できる人物のＩＤ、及びアクセスできる特定データの種類を確認する上でも、これは同様に重要となる。例えば、マーケティング部門のスタッフの給与額を見るために、企業のエンジニアリング部門がマーケティング部門の人事記録にアクセスできるようなシステムがあってはならない。
・個人にとっては、通信相手が詐欺師ではないことを確認することで発信者の「プライバシー」を保証するために、ＩＤ検証を行うことが重要となる。
【０３９１】
したがって、ＩＤ検証の役割は、個人のＩＤを確認すること、すなわち主張通りの本人であることを認証し、ＩＤを偽る人物を特定及びブロックして、最終的に取り押さえることにある。「Ａｕｔｈｅｎｔｉｃａｔｉｏｎ、Ａｕｔｈｏｒｉｚａｔｉｏｎ、Ａｄｍｉｎｉｓｔｒａｔｉｏｎ」を表す「トリプルＡセキュリティモデル」または「ＡＡＡ」の最初の「Ａ」は、認証（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ）を指している。ＰＩＮコード、パスワード、指紋、トークン、クエリ応答方式などの多数の方法を使用して、個人の身元を確認し、システムにアカウントが存在することを検証することができる。
【０３９２】
認証されると、有効なユーザのＩＤを使用して、コミュニケ、データ、ファイル、システムなどへのアクセス権と特権が判断される。こうした特権とアクセス権は総称して、システムにより付与されるユーザの「認可（Ａｕｔｈｏｒｉｚａｔｉｏｎ）」と呼ばれる。すなわち、認証ユーザのみが、認可された通信、データ、ファイル、及びシステム機能にアクセスできる。したがって、認可は「特権」または「アクセス権」と同義となる。
【０３９３】
ＡＡＡの３番目の「Ａ」は「管理（Ａｄｍｉｎｉｓｔｒａｔｉｏｎ）」を表している。管理とは、従量課金制の管理などを目的として、ネットワークとファイルへの認可アクセスを記録し、ネットワーク、ファイル、及びシステムへの不正アクセスの試行を監視及び

報告することである。認証操作に必要なセキュリティクレデンシャル情報、ＰＩＮ、パスワードなどの変更を追跡する上でも、管理が重要となる。

【０３９４】

プライバシーを保証し、認可されていないユーザやネットワークオペレータによるネットワークの不正利用を防ぐ上で、ＡＡＡ検証を実行するネットワークの能力が最も重要となる。ユーザのＩＤを確認できないネットワークは全て、違法な操作に不正利用される可能性がある。ＯＴＴ通信には発信者ＩＤを検証する手段が存在しないため、許可されていないユーザによるネットワークの不正利用は避けられない問題となる。未確認ユーザによる不正アクセスとネットワーク通信、すなわち匿名性は、現代の通信における重大なリスクである。

【０３９５】

匿名性

【０３９６】

通信における匿名性の原則は、トレーサビリティなしに通信を図ることを目的として、発信者のＩＤを意図的に隠すことである。匿名通信のほぼ象徴的な例として公衆電話が挙げられる。公衆電話の支払は追跡不可能な現金であり、公衆電話番号は公開されており、そして誰でも電話を使用できる。すなわち、公衆電話では発呼者のＩＤは不明で、発呼者が主張通りの本人であることを確認する手段は存在しない。電話番号は電話帳に載っておらず、個人が番号を所有しているわけではないため、（高度な音声認識ソフトウェアを使用する場合を除き）発呼者のＩＤを識別する方法はない。携帯電話などの登録済みデバイスの場合は、電話番号からデバイス所有者のＩＤを追跡できるが、依然として発呼者のＩＤを隠すことはできる。例えば、盗んだ電話や従量制のＳＩＭカードを使用すれば、発呼者の実際のＩＤを隠すことが可能となる。または、ノートブック、タブレット、または携帯電話を公共のカフェでＷｉＦｉに接続することで、公衆電話や電話ボックスと同様の匿名性が得られる。

【０３９７】

一部のＯＴＴ事業者は、加入者のＩＤ検証なしで、ＶｏＩＰ電話サービスを有料電話として運用している。例えば、ＣＮＮ　Ｍｏｎｅｙの最近のオンラインレポート（http://money.cnn.com/2015/11/17/technology/isis-telegram/）には、「『Ｔｅｌｅｇｒａｍ』というアプリがジハード主義者の間で新たに人気を博している」と記されている。調査によると、パリテロ事件を密かに計画していたイスラム国（ＩＳＩＳ）テロリスト等はＴｅｌｅｇｒａｍアプリを連絡手段として活用していた。「Telegram founder knew Isis was using the app to communicate before Paris attacks（ＩＳＩＳがパリテロ事件の前にアプリを使用して通信していることをＴｅｌｅｇｒａｍの創設者は知っていた）」（http://www.independent.co.uk/life-style/gadgets-and-tech/news/telegram-knew-isis-communicate-paris-pavel-durov-a6742126.html）と題する記事には、Ｔｅｌｅｇｒａｍの創設者、パーヴェル・ドゥーロフ（Ｐａｖｅｌ　Ｄｕｒｏｖ）が「テロのような不良な事態が発生することへの恐怖よりも、プライバシーの権利のほうが重要である」と述べたと記されている。

【０３９８】

プライバシーと匿名性が犯罪行為に利用された別の報道事例として、ＢｉｔＴｏｒｒｅｎｔが挙げられる。これは、著作権で保護された材料を違法にダウンロードまたは共有するためによく使用されるアプリケーション及びデータネットワークである。ＣＮＮ　Ｍｏｎｅｙに掲載された記事「50,000 BitTorrent users sued for alleged illegal downloads（違法ダウンロード容疑でＢｉｔＴｏｒｒｅｎｔユーザ５万人を訴追）」（http://money.cnn.com/2011/06/10/technology/bittorrent_lawsuits/）によると、新しい海賊対処法の下、「ハート・ロッカー（Ｔｈｅ　Ｈｕｒｔ　Ｌｏｃｋｅｒ）」などの著作物を違法にダウンロードした容疑で同アプリのユーザ等が訴追されている。ネットワークオペレータのＢｉｔＴｏｒｒｅｎｔは、ネットワークユーザが個人的な活動のために行う行為に対する責任は負わないという公衆電話的な立場を取っている。言論の自由の擁護者

はこの姿勢を支持しているが、法執行機関、政府、国家安全保障機関、及び知的財産権の擁護者は、この姿勢を無謀かつ無責任であるとして激しく嫌悪している。問題の政治的側面に関係なく、通信システムで発信者検証を実行できない限り、匿名コールを停止することに関する議論は純粋に学術的なものに過ぎない。

【０３９９】

企業や事業体にとって、知的財産、開発技術、製品評価、製造ノウハウ、機密財務報告と財務予測、事業状況、販売予測、在庫と仕掛品、品質監査、取引と知的財産契約、顧客リスト、従業員記録、他の企業秘密といった企業機密データへのアクセスを管理する上で、発信者の検証と認証は特に重要となる。企業通信へのアクセスにおいては、従業員、請負業者、または役員に付与されるアクセス権はＩＤの確認に依存する。投資家との通話を含む電話会議では、通話への参加者のＩＤを確認し、知る必要のない人物が聞いていないことを確認するために、ＩＤ検証が重要となる。

【０４００】

皮肉なことに、発信者検証は犯罪者や企業スパイの行為を阻止するために使用できるが、同じＩＤ検証が発信者のプライバシーを保証するのにも有益に働く。コールまたはテキストチャットの双方当事者が何らかの規定された認証手順を介してお互いのＩＤを確認すれば、詐欺師はコールまたはそのデータにアクセスできなくなることから、攻撃からコールを保護することができる。

【０４０１】

最後に、匿名コールで匿名の発信者を区別するためには、区別を行う必要があるということを挙げておく。匿名の発信者とは、通信しているネットワークで自身の本当のＩＤを偽装する個人である。しかし、匿名コールでは、発信者のＩＤがネットワーク上で匿名というわけではなく、通信中の発信者のＩＤがコールデータパケットで難読化されているに過ぎない。ＳＤＮＰネットワークの登録アカウント所有者は、この開示に従って、ネットワークでＩＤと電話番号が知られていても、匿名データ転送を使用して電話をかけること、またはデータを送信することができる。このようにして、法を遵守する市民は、ＳＤＮＰネットワークオペレータからＩＤを隠すことなく、匿名で通信することが可能となる。発信者が通常のプライベートなコール、エンターテイメント、またはビジネスに従事している場合、ネットワークでＳＤＮＰネームサーバデータベースに格納されているＩＤが分かっていても、ＳＤＮＰコールは非公開でセキュアである。

【０４０２】

合法的な匿名コールの必要性の例として、ゲーマーのＩＤ、特に児童のＩＤを保護することが重要となるグローバルゲーミングが挙げられる。匿名性によりメリットがもたらされ得る別の例として、車車間（Ｖ２Ｖ）通信が挙げられる。交通状況を悪化させたドライバーの個人データを特定できれば、激怒した他のドライバーの報復の対象となる可能性があるが、匿名性を維持することで、こうしたリスクが排除される。対照的に、発信者が犯罪または他の悪意ある通信に関与している場合は、法執行者が（適用法に従って）コール及びデータ送信にアクセスできる。このように、ネットワークオペレータは、法を遵守する市民のＩＤやコール内容を公開することなく、裁判所命令と召喚状の要件を満たすことができる。

【０４０３】

要約すると、開示されるＳＤＮＰ通信方法を使用することで、識別可能なＳＤＮＰ加入者のみが匿名コールを発信できる。未確認発信者はＳＤＮＰネットワークにアクセスすることも、匿名コールを行うこともできない。

【０４０４】

国家安全保障及びプライバシー

【０４０５】

セキュアでプライベートな通信の性質は、政府の役割と法律を考慮するとさらに混乱する。どの国も、国内の通信を制御する主権を主張している。しかし、インターネット及び動的にルーティングされるパケット交換データネットワークの出現により、ネットワーク

の監視については技術的及び法的問題が山積みとなっている。懸念事項の１つとして、サーバ間のネットワークを「流れる」トラフィック監視に関する問題が挙げられる。つまり、データパケットが止まることなく国間を通過するということである。インターネットトラフィックは動的にルーティングされるため、サーバのネットワークによりどのようなデータパケットが伝送されているのかをネットワークオペレータは把握できない。もちろん、どのような国でもこの大量のバルクデータを傍受してデコードすることを試みることはできるが、暗号化されていることから、特にリアルタイムの監視の場合、暗号化鍵が分からなければアクセスすることは困難である。また、発信者は国内に居住していない可能性があるため、特定の国には召喚状の請求またはコールの発信に使用された暗号化鍵の要求を行う管轄権がない場合がある。このようにネットワークを流れるデータは、地球の大気を通過する電波トラフィックに似ている。電波が頭上を通過しても、これを止める実用的な方法は存在しない。同様に、国のインフラストラクチャをインターネットから完全に隔離すること以外に、ネットワークを流れるデータトラフィックを停止させる現実的な方法はない。

【０４０６】

通信を管理するより実用的なソリューションとして、ラストマイル通信に監視を集中することが挙げられる。すなわち、コールの送信元と宛先が国内にあるコールとコールデータを傍受及び監視するのである。このアプローチには、大量のデータトラフィックの傍受と比較して、（ｉ）データの規模が小さい、すなわち分析しやすい、（ｉｉ）ラストマイル通信事業者またはネットワークオペレータが所在している国の法律の対象となる、（ｉｉｉ）暗号化鍵の提出を求めて、ラストマイル通信事業者またはネットワークオペレータを召喚できる、（ｉｖ）ラストマイルネットワークに接続する条件として、発信者のデバイスに電子的な「登録」を強制し、その際に発信者に関する情報を放棄させることができる、（ｖ）ネットワークアドレス、ＧＰＳデータ、または無線信号の三角測量を使用して、ネットワークに接続されたデバイスの場所を把握できるといういくつかの利点がある。

【０４０７】

ネットワークを流れるデータ規制を執行する法的・技術的課題とは異なり、ラストマイル通信とコール終了に法律を適用することは、完全にラストマイルネットワークオペレータが所在する国の権利となる。国のプライバシー法に応じて、国の政府は、ラストマイル通信における必要なアクセスレベルを主張することができる。これには、以下の組み合わせが含まれる。

・相当の根拠に基づき裁判所から召喚状が発せられない限り、どのようなデータやコールでも監視する権利がない。裁判所命令により、コールまたはデータ通信を密かに監視する権利。

・裁判所命令なしで、任意の通話のメタデータを監視する権利。

・裁判所命令なしで、全てのコールとデータ通信を監視する権利。

・通信を傍受及び監視し、必要に応じて通信のいずれか、または全てをブロックする権利。

【０４０８】

例えば、米国などの様々な政府は、裁判所命令なしにコールの「メタデータ」を監視する権利を留保するという立場を取っている。メタデータには、発信者と発信先、コールの継続時間、呼び出し時に発信者が所在していた場所などに関するデータパケット情報が含まれており、実際のコールデータ自体にアクセスすることなく、こうした情報を得ることができる。本質的に、メタデータはＩＰパケットのデータヘッダで構成されるが、ペイロードではない。対照的に、コールとデータ通信を監視するには、ヘッダデータだけでなくペイロード自体にアクセスする必要がある。ペイロードが暗号化される可能性がある場合、マスター暗号化鍵が存在するのであれば、政府はネットワークオペレータに対してその鍵を提供するように要求することができる。プライバシー擁護者から提起される１つの問題として、政府の権力濫用が挙げられる。特に、ネットワークが単一セットのマスター暗号化鍵に依存している場合、裁判所命令に応じてその鍵が政府に提供されることで政府が特定個人を実際に監視できるようになるということは、たとえ裁判所命令がある個人また

は集団に制限されていたとしても、実際には政府が全員のコールを監視できるようになるということである。この問題では、時に「では誰が警察を取り締まるのか」という板挟みの状況が指摘される。

【０４０９】

別の考慮事項は、国際コールを行う個人のプライバシー権に関するものである。このような場合、発信者は、政府のアクセスに関連する法律が両方の発信者の場所、すなわち２つのラストマイルネットワークが発生する場所に依存することに注意する必要がある。米国から中国へのコールは、米国の発信者には米国の法律、他方の中国の発信者には中国の法律が適用される。こうした状況では、一方の政府によるコールアクセスが他方政府よりも大きい場合がある。そのため、プライバシー権が完全に保障されている国の発信者は、相手国の政府によってプライバシーが侵害されたと考える可能性があるが、その国にコールを発信しているため苦情を申し立てる法的根拠は存在しない。

【０４１０】

前回開示された動的通信ネットワーク及びプロトコルが使用される通信の場合は、ＳＤＮＰネットワークを通して匿名で転送される断片化及びスクランブル化されて動的に暗号化されたデータパケットのハイパーセキュアクラウド通信で流れるデータの傍受は事実上不可能である。そのため、ハイパーセキュアコールのプライバシーとセキュリティは、デバイスとラストマイル通信によって決定される。前述のＳＤＮＰ方法をラストマイル通信に適応させることで、本明細書に開示されるように、ハイパーセキュア通信及び高整合性のプライバシーが可能なラストマイルを実現できる可能性がある。

【０４１１】

さらに、ＳＤＮＰネットワークのセキュリティとプライバシーの設定を調整して、各国のラストマイル通信に適用される現地の法律に対応するメカニズムを開示している。これらの方法には、認可セキュリティ当局がコールデータをハッカーやサイバー犯罪者に曝すことなく、法律及び裁判所の措置に従って通信を監視できるようにする保護手段が含まれる。そのため、本明細書に開示されるハイパーセキュアラストマイル通信では、サイバー攻撃に対して脆弱な「バックドア」の使用は採用されていない。

【０４１２】

<u>ハイパーセキュアラストマイル通信の方法及び装置</u>

【０４１３】

エンドツーエンドのハイパーセキュリティを確保するには、断片化及びスクランブル化されて暗号化された匿名データパケットのＳＤＮＰクラウド内のルーティングに関する前述の方法の適用を、ラストマイル内の通信に同様に適応させる必要がある。データはＳＤＮＰオペレータによってホストされていないネットワークで運ばれる可能性があることから、パケットルーティングに従来型のＩＰパケットルーティングが含まれる場合があり、ラストマイルネットワークの本質的なセキュリティが、ラストマイルネットワークオペレータと共謀している可能性のあるサイバー犯罪者により知らないうちに侵害されている可能性があるため、ラストマイル通信の安全を確保することは特に問題である。

【０４１４】

本発明では、ラストマイル通信は必然的に、ＳＤＮＰクラウド内のデータパケットとは異なるパケットフォーマットを使用するデータクラウドネットワーク外のＩＰデータグラムの転送を伴う。図１０に示されるように、サーバ１２０１で構成されるＳＤＮＰクラウド（ソフトスイッチ対応ＳＤＮＰノードＭ$_{0,0}$からＭ$_{0,f}$として概略的に示す）により、例示的なデータパケット１２２２Ｂ、１２２２Ｃ、及び１２２２Ｆとして示されるＳＤＮＰデータグラムが使用され、ＶｏＩＰ、ビデオ、テキスト、及びデータが転送される。ＳＤＮＰデータグラムには、インターネットＩＰアドレスではなく、ＳＤＮＰレイヤ３送信元アドレス及び宛先アドレスが含まれる。ＳＤＮＰアドレスは、インターネットのＤＮＳネームサーバではなく、ＳＤＮＰネームサーバまたはＳＤＮＰネームサーバの機能を実行する他のサーバによってのみ認識されるという点でＩＰアドレスと異なる。

【０４１５】

上記の米国出願第１４／８０３，８６９号に記載されるように、ＳＤＮＰパケットはネットワークを移動する際に動的に変化し、更新されたルーティングアドレス及び共有秘密と動的な「ステート」（時間など）に従って常に変化するペイロードが実行される。例えば、ノードＭ０，０により送信されたデータパケット１２２２Ｂは、一意のＳＤＮＰアドレスと一意に暗号化されたペイロードを含むレイヤ３　ＳＤＮＰデータグラムＢで構成される。ダウンストリームのノードＭ０，１からのデータパケット１２２２Ｃ出力は、異なるＳＤＮＰアドレスと再暗号化されたペイロードを含むレイヤ３　ＳＤＮＰデータグラムＣで構成される。数十ミリ秒の後、同じペイロードがノードＭ０，ｆに到達する。これにより、データが処理され、ＩＰデータグラムＧを含むデータパケット１２２３Ｇがラストマイルに転送される。

【０４１６】

変更は定義されたステートに従って実行されるため、元のパケットデータは、実行された順序とは逆の順序で実行される一連の逆機能操作を実行することで復元できる。例えば、スクランブル化、ジャンク挿入（偽装）、及び暗号化の手順で構成されるＳＤＮＰ機能シーケンスは、対応する逆機能を実行するために機能の実行に使用されたのと同じステートを呼び出す場合は、逆の順番で復号化、ジャンク除去、及びアンスクランブル化により元に戻すことができる。パケットのステートデータは、パケットのペイロードに埋め込まれるか、またはパケットの前に送信されるかたちで時間、シード、または鍵として伝送される。ＳＤＮＰクラウド内のデータ転送と処理は、ＳＤＮＰクラウド固有の共有秘密とセキュリティクレデンシャル情報を使用して行われる。共有秘密とセキュリティクレデンシャル情報の共通セットを共有するメディアノードは、セキュリティ「ゾーン」と呼ばれる場合がある。ＳＤＮＰクラウド内で動作するセキュリティクレデンシャル情報に使用されるゾーンは、ＳＤＮＰクラウド外のユーザの通信で公開することはできない。そのため、全てのラストマイル通信には、ＳＤＮＰクラウドとは異なるＳＤＮＰセキュリティゾーンを含める必要がある。

【０４１７】

示される例では、対応するノード０，０及びＭ０，ｆをホストするサーバ１２０１Ａ及びサーバ１２０１Ｆは、ＳＤＮＰゲートウェイとして動作する。すなわち、ＳＤＮＰクラウド外部のデバイス及び他のクラウド内ＳＤＮＰノードと通信する。これらのゲートウェイからクラウド外部の通信デバイスへの通信は、「ラストマイル」通信を表す。したがって、ゲートウェイノードで、ＳＤＮＰクラウドと接続先のラストマイルネットワークの両方のゾーンセキュリティクレデンシャル情報が理解されており、パケットルーティング中のトランスレータとして機能させる必要がある。意味的には、ラストマイルという用語は、ＳＤＮＰクラウド外部の通信を意味する抽象概念であり、特に１マイルの距離を指すものではない。代わりに、ラストマイルという用語には、クライアントデバイスがＳＤＮＰクライアントとして動作しているかどうか、すなわちＳＤＮＰアプリケーションソフトウェアまたはファームウェアが実行されているかどうかに関わりなく、及びその距離に関係なく、クライアントデバイスとＳＤＮＰクラウド間の通信が含まれる。

【０４１８】

また、ラストマイルという用語は、コールが開始されるクライアントデバイス及びコール先のクライアントデバイスの両方に適用される。文字通り、発信者のデータはコールの「ラストマイル（ｌａｓｔ　ｍｉｌｅ）」ではなく「ファーストマイル（ｆｉｒｓｔ　ｍｉｌｅ）」を表すため、「ファーストマイル」と「ラストマイル」の区別は恣意的なものである。具体的には、二重変換またはＩＰ通信「セッション」では、コールを受信するデバイスは、必然的に発信者に応答を送信することにより、コールまたはセッション要求に応答する。したがって、双方向通信では、ファーストマイル接続は常に応答データパスのラストマイルとして機能する。本質的に、発信者のファーストマイルは、同時に応答のラストマイルとなる。そのため、本出願全体で定義される用語「ラストマイル」は、コールまたはコールセッションがいずれのデバイスから開始されたものかに関わりなく、ファーストマイルとラストマイルの両方を意味するものとする。

【０４１９】
ＳＤＮＰクラウド外部からＳＤＮＰクライアント以外の任意のデバイスへの通信は、必然的にＳＤＮＰデータグラムではなく、ＩＰデータグラムを使用して実行される。例として、図１０に示されるように、データパケット１２２３Ａは、ＳＤＮＰアドレスではなく、ＩＰアドレスを有するＳＤＮＰペイロードを使用して構築された「ＩＰデータグラムＡ」で構成される。同様に、ＩＰデータグラムＧは、ＩＰアドレスを使用してルーティングされたＳＤＮＰペイロードを含むデータパケット１２２３Ｇで構成される。送信元ＩＰアドレス及び宛先ＩＰアドレスとは、ルーティング先のネットワークで認識可能なＩＰｖ４またはＩＰｖ６アドレスを表すものである。ＩＰアドレスには、インターネットのＤＮＳサーバで認識されるインターネットアドレスが含まれる場合、またはローカルネットワークサービスプロバイダにより定義されたローカルネットワーク全体のルーティングに使用されるＮＡＴアドレスが含まれる場合がある。
【０４２０】
ラストマイル通信で使用されるハードウェアとファームウェアは大きく異なる場合があり、これには電話回線、ファイバ通信、ケーブルテレビネットワーク、３Ｇと４Ｇ無線ネットワーク、マイクロ波通信塔、及び衛星が含まれる場合があるため、ラストマイル通信の分析は、様々なレイヤ１物理ネットワーク及び採用されている対応レイヤ２データリンクフォーマットを考慮する必要がある。例えば、フォーマットにはアナログ（ＰＯＴＳ）、イーサネット（登録商標）、ＷｉＦｉ、３Ｇ、４Ｇ／ＬＴＥ、及びＤＯＣＳＩＳ３が含まれる。各ラストマイルの実装に対応するセキュリティ及びプライバシー機能は、ＳＤＮＰ「コールアウト」通信に関する以下のセクションで、ケースバイケースで検討される。
【０４２１】
非セキュア回線を介したＳＤＮＰコールアウト
【０４２２】
専門用語として、定義されたネットワークを出て別の（及び一般に異なる）ネットワークを介して転送されるコールは全て、一般的に「コールアウト」と呼ばれる。この用語は、データまたは音声があるネットワークを出て別のネットワークで転送されることを意味する。例えば、Ｓｋｙｐｅアプリケーションを実行しているクライアント間の通信は一般的にＳｋｙｐｅコールと呼ばれるが、Ｓｋｙｐｅクライアントから普通の電話番号または携帯電話番号にかけられる電話は、Ｓｋｙｐｅコールアウト機能または「Ｓｋｙｐｅアウト」コールと呼ばれる。一般的に、普通の電話へのコールアウトには、加入料または従量課金のいずれかとして、追加のコストがかかる。
【０４２３】
本文書の文脈において、非セキュアラストマイル接続を介したＳＤＮＰクライアントからＳＤＮＰクライアント以外の任意のデバイスへの通信は、本明細書では「ＳＤＮＰコールアウト」という定義された用語で表される。図１１は、非セキュアラストマイルへのＳＤＮＰコールアウトルーティングの２つの例を概略的に表したものである。上部の例では、電話や公衆電話６Ａなどのアナログデバイスへのアナログ信号を使用して通信が行われる。このような場合、ＳＤＮＰゲートウェイにはデジタルからアナログへの変換器が含まれている必要がある。そうでない場合は、モデムまたは変換デバイスがゲートウェイに追加される場合がある。情報は、データパケットではなく、アナログ信号１２２１によって伝送される。アナログ電話信号は音声の伝送には効率的であるが、高速データ通信には十分に対応していない。
【０４２４】
下部の例の場合、ＳＤＮＰコールアウトは、デジタルネットワークを介して、ＳＤＮＰクライアントとして有効化されていない、すなわちＳＤＮＰソフトウェアまたはファームウェアで有効化されていないデジタルデバイス（携帯電話３２など）に対して行われる。このような場合、一般的にインターネットプロトコルに従い、すなわち７レイヤＯＳＩモデルと一致するＩＰパケットフォーマットが使用され、データパケット１２２３により通話またはデータが伝送される。ＩＰデータグラムには、その送信元アドレスフィールド及

び宛先アドレスフィールドにＩＰアドレスまたはＮＡＴアドレスが含まれ、ペイロードとしてＩＰデータまたはＶｏＩＰデータが含まれる。デジタルパスには、ラストマイル接続に応じて異なるイーサネット（登録商標）、ＷｉＦｉ、４Ｇ／ＬＴＥなどの様々なフォーマットのデジタルデータが含まれる場合がある。

【０４２５】

いずれの例示的概略図でも、ラストマイル通信データはＳＤＮＰネットワーク外部で非セキュア通信チャネルまたはネットワークを介して運ばれるため、通話は安全でなく、ハッキング、スパイ、盗聴、他のサイバー攻撃の対象となる。本適用の背景に説明されるように、ツイストペア銅線、同軸ケーブル、ファイバ、イーサネット（登録商標）、ＷｉＦｉ、セルラー、衛星など、その種類に関わらず、暗号化のような特別なセキュリティ方式がエンドツーエンドのデータパスに挿入されていない限り、ラストマイルの非セキュア回線と接続は本質的に安全ではない。したがって、最もセキュアなデータクラウドまたはＶＰＮのセキュリティが、最も脆弱な部分（この例ではラストマイル）のせいで侵害される。特に単一の明確に定義された電気、マイクロ波、または電波接続では、暗号化によってもセキュリティは保証されない。セキュリティの欠如に加えて、例示的概略図では、ＩＤ検証のメカニズムが何も含まれていない。認証が可能でないため、ラストマイルにはプライバシーの保証がない。したがって、例示的概略図は、発信者のプライバシーが保証されない非セキュアラストマイルネットワークを表している。

【０４２６】

図１２では、デジタルネットワークサービスプロバイダＮＳＰがホストする有線またはファイバリンク２４を介して、公衆交換電話網またはＰＳＴＮゲートウェイ１Ａに接続し、ＳＤＮＰゲートウェイ１２０１Ａから非セキュアラストマイルへ、プライバシーの保証のないＳＤＮＰコールアウトが実行される。次に、ＰＳＴＮゲートウェイ１Ａは、アナログ通信接続４を介して従来型の電話システムＰＯＴＳスイッチ３にルーティングされる。その後、ＰＯＴＳスイッチ３から、ツイストペア線７を介して、家庭用電話６、コードレス電話システム５、または公衆電話６Ａに従来型の電話通話が行われる。ラストマイル全体が非プライベート及び非セキュアである。ＳＤＮＰデータグラムＡを含むデータパケット１２２２Ａの通信では、ＳＤＮＰネットワーク内でＳＤＮＰアドレス指定とＳＤＮＰペイロードが使用されるが、データがラストマイルに入ると、ハイパーセキュリティの利点が失われる。例えば、ＮＳＰネットワークでホストされる有線またはファイバリンク２４により伝送されるＩＰデータグラムＢを含むデータパケット１２２３Ｂでは、インターネットＤＮＳサーバで認識される従来型のＩＰアドレス指定が使用され、これにはサイバーパイレーツがスニッフィングできる従来型のＩＰペイロードが含まれる。アナログ回線４及び７では、アナログコールデータ１２２１として単純なアナログ音声信号が伝送されるため、同様に脆弱である。ＳＤＮＰゲートウェイでは非セキュアな非プライベートコールアウトをサポートできるが、ＳＤＮＰで保護されたコールをプライバシー規定のない非セキュアラストマイルネットワークに接続することは勧められない。

【０４２７】

ＩＤ検証を使用することで、前述の非セキュアラストマイル実装をわずかに改善することができる。図１３には、非セキュアラストマイルへのＳＤＮＰコールルーティングではあるが、２つの異なる種類の認証を使用する例が概略的に示されている。上部の例は、アナログまたはＰＯＴＳ回線を介したＳＤＮＰゲートウェイ１２２０Ａからのオフィスのデスクトップ電話機９へのＳＤＮＰコールアウトを示すものである。これに示されるように、オペレータ１２２５は認証を手動で実行して、アカウント所有者のＩＤ及びアカウントＩＤを確認する。認証されてはいるが、アナログ音声１２２１で行われるコールはセキュアではなく、会話で秘密またはアカウント情報が聴覚的に明らかにされない場合にのみプライベートとなる。すなわち、秘密が明らかにされなければ情報は非公開となるが、情報が明らかにされると、通信はもはやプライベートではなくなる。そのため、本明細書では、半プライベートという用語は、非セキュア回線を介した認証済みの通信、すなわち条件付きプライベート通信を指す。

【０４２８】
下部の例は、ＳＤＮＰゲートウェイ１２２０Ａから非セキュアデジタルラストマイルへのＳＤＮＰコールアウトを示すものである。ＩＰデータグラム１２２３によりデスクトップＰＣ　３６などの電子デバイスに伝送されるデータは非セキュアであるが、サイバー攻撃者がアクセスできないトークン１２２６などの電子的なＩＤ検証方法を使用して認証できる。回線が非セキュアで、スニッフィングできるため、デジタル対話でアカウント番号や機密データが漏れないように注意する必要がある。

【０４２９】
半プライベートの非セキュアコールの具体例を以下いくつかの例に示す。図１４には、ＳＤＮＰネットワークとオフィスのデスクトップ電話機９（プライベートバンカーの電話など）との間のＩＤ検証済みの非セキュアラストマイル通信が示されている。例えば、国際的に実行される場合、アカウント所有者／口座名義人のコールは、ＳＤＮＰネットワークでハイパーセキュア通信を使用して世界中にルーティングされ、最終的にＳＤＮＰゲートウェイ１２０１Ａを介してＳＤＮＰコールとしてラストマイルに接続される。コールの長距離部分は、ＳＤＮＰペイロードを有するＳＤＮＰデータグラムＡを含むデータパケット１２２２Ａなどの動的に変化するＳＤＮＰデータグラムを使用して実行される。次に、ＳＤＮＰゲートウェイ１２０１Ａで、データパケット１２２２Ａが、ＳＤＮＰデータグラムＡからデータパケット１２２３Ｂによって示されるＩＰデータグラムＢに変換される。ＳＤＮＰデータグラムＡとは異なり、ＩＰデータグラムＢにはスニッフィング可能なＩＰペイロードが含まれる。データパケット１２２３Ｂは、ネットワークサービスプロバイダ（ＮＳＰ）が運用する有線またはファイバリンク　２４によって、公衆交換電話網またはＰＳＴＮゲートウェイ１Ａに転送される。そして、このゲートウェイが、アナログコール１２２１を伝送するＰＯＴＳ回線４を介して企業の交換機８Ａに接続される。企業の交換機８Ａが、アナログ構内電話交換機またはＰＢＸ回線７Ａを介してデスクトップ電話機９に接続され、個人認証オペレータ１２２５にも接続される。コール中、口座名義人がデスクトップ電話機９でプライベートバンカーに連絡することになる。その際、どのような取引でもそれに従事する前に、個人認証オペレータ１２２５がコールに参加して発信者のＩＤを確認してから通話を終了するため、その後は発呼者のプライバシーが維持される。しかし、通話が非セキュアであるため、プライベートバンカーと口座名義人は両方共に、口座番号、パスワード、ＰＩＮなどの機密情報を口頭で明かさないように注意する必要がある。そのため、コールは半プライベート、すなわち条件付きプライベートとなる。

【０４３０】
図１５には、ＳＤＮＰネットワークとデスクトップコンピュータ３６との間のＩＤ検証済みの非セキュアラストマイル通信が示されている。デジタル通信セッションでは、いくつかのデジタルメディアで伝送されるＩＰデータグラムＢが使用され、デスクトップコンピュータ３６からＳＤＮＰゲートウェイ１２０１Ａへ通信が行われる。最初の区間では、イーサネット（登録商標）１０６Ａにより、ＩＰデータグラムＢを含むデータパケット１２２３Ｄが、デスクトップコンピュータ３６からイーサネット（登録商標）ベースのローカルルータ２７Ｂに伝送される。その後、ＩＰデータグラムＢを含むデータパケット１２２３Ｃが使用され、インターネットサービスプロバイダ（ＩＳＰ）の有線またはファイバリンク２４Ａ経由で、イーサネット（登録商標）ローカルルータからネットワークルータ２７へ通信が行われる。ネットワークルータ２７とＳＤＮＰゲートウェイ１２０１Ａ間のラストマイルの最終区間において、ＮＳＰが運用する有線またはファイバリンク２４のネットワークサービスプロバイダ回線により、ＩＰデータグラムＢを含むデータパケット１２２３Ｂが伝送される。ＩＰデータグラムが使用されるため、ラストマイルは非セキュアとなる。ログインウィンドウ１２２７及びセキュリティトークン１２２８のようなデジタル方式のＩＤ検証を認証に使用して、通信を半プライベートに維持することができる。詐欺師により利用されるのを防ぐために、これらのデジタル認証は１回限りの使用に制限する必要がある。例えば、トークンから番号が生成され、それが一旦アクセスに使用されると、その組み合わせはその後使用できなくなるため、ハッカーがトークンを傍受したとし

ても、当該トークンは有効期限が切れて無効になるため役には立たない。

【０４３１】

図１６には、ＩＤ検証済みの非セキュアラストマイル通信の他の例が示されている。この例では、ＳＤＮＰコールアウトとして、ＳＤＮＰゲートウェイ１２０１ＡからＰＯＳ端末３８及びガスポンプＰＯＳ端末３８Ａへ通信が行われる。示されているラストマイル通信は、ＩＰデータグラムＢを含むデータパケット１２２３Ｂをネットワークルータ２７に伝送するＮＳＰ有線またはファイバリンク２４、その後にデータパケット１２２３Ｃ内のＩＰデータグラムＢをＰＳＴＮブリッジ３Ａに伝送する有線またはファイバリンク２４Ａ、及びＰＯＳ端子３８及びガスポンプＰＯＳ端子３８Ａに接続されたアナログコール１２２１Ａとしてデジタル ＰＣＭ（パルスコード変調）データを伝送するＰＯＴＳまたはアナログ回線３０Ｂが続くデジタル及びアナログ接続が混合したものである。金融取引における認証は、電子検証に基づくスマートカード集積回路及び動的ＰＩＮ １２２８を含む銀行カードデータ１２２９に基づいている。認証には、ＳＤＮＰゲートウェイ１２０１Ａまたは別のラストマイルを介してＳＤＮＰネットワークに接続される金融機関１２３０による確認が含まれる。

【０４３２】

ハイパーセキュアラストマイル通信

【０４３３】

セキュア動的通信ネットワーク及びプロトコルの技術を採用することで、ハイパーセキュア通信をラストマイルで実現できる。ハイパーセキュリティを容易化するために、接続されたデバイスでＳＤＮＰコードを「ＳＤＮＰクライアント」として実行する必要がある。ＳＤＮＰクライアントは、接続された通信デバイスでホストされる操作指示、共有秘密、及びＳＤＮＰ接続情報で構成される。ＳＤＮＰクライアントには、オペレーティングシステムで実行されるソフトウェア、マイクロコントローラーまたはプログラマブルＩＣで実行されるファームウェア、または専用のハードウェアまたは集積回路が含まれる場合がある。図１７は、「ＳＤＮＰ接続」が使用されるラストマイルでのハイパーセキュア通信の例を概略的に表したものである。示されるように、ＳＤＮＰゲートウェイ１２０１Ａは、ＳＤＮＰクライアントを実行するデバイス、この例ではデスクトップコンピュータ３６で実行されるＳＤＮＰアプリ１３３５に接続される。ＳＤＮＰクライアントは、ハードウェア及びオペレーティングシステムに固有である。モバイルデバイスの場合、Ａｎｄｒｏｉｄ（登録商標）、ｉＯＳ、及びＷｉｎｄｏｗｓ（登録商標） Ｍｏｂｉｌｅを使用するモバイルデバイスプラットフォームごとに個別のアプリが必要となる。同様に、Ｗｉｎｄｏｗｓ（登録商標） １０、ＭａｃＯＳ、Ｕｎｉｘ（登録商標）、Ｌｉｎｕｘ（登録商標）などを含め、ノートブック、デスクトップＰＣ、及びサーバには、個別のＯＳ固有のアプリケーションが必要である。ＰＯＳ端末、ホットスポット、ＩｏＴなど、高レベルのオペレーティングシステムを備えていないデバイスにおけるＳＤＮＰクライアントのハードウェアホスティングでは、コードを実行するプログラマブルデバイスに適応させる必要がある。プログラマブル集積回路では、多くの場合、Ｑｕａｌｃｏｍｍ、Ｂｒｏａｄｃｏｍ、Ｉｎｔｅｌ、ＡＭＤ、ＮＶｉｄｉａ、Ｍｉｃｒｏｃｈｉｐなど、ＩＣベンダーに固有のチップ固有の開発環境でのプログラミングが必要になる場合がある。

【０４３４】

ＳＤＮＰゲートウェイ１２０１ＡとＳＤＮＰアプリ１３３５では、ＳＤＮＰペイロード１２２２を使用して通信が行われるため、パケットスニッフィングでは発信者のＩＤとコールペイロードが理解できなくなる。具体的には、ＳＤＮＰペイロード１２２２にはＤＮＳサーバによって認識されない送信元と宛先のＳＤＮＰ擬似アドレスが含まれ、ペイロードはスクランブル化、断片化、ジャンクデータ挿入との混合、及び動的に暗号化が可能なＳＤＮＰデータで構成される。ＳＤＮＰペイロード１２２２はＩＰデータグラム１２２３に埋め込まれる。これにより、ＳＤＮＰアドレスではなく、ラストマイル接続に使用されるセルラー、ケーブル、またはＩＳＰ事業者のネットワークのＩＰアドレスまたはＮＡＴアドレスを使用してラストマイルを介したルーティングが指示される。

【０４３５】
ＳＤＮＰベースのハイパーセキュアラスト通信のもう１つの側面として、全てのＳＤＮＰクライアントで本質的に認証とＩＤ検証を行えることが挙げられる。したがって、プライバシー機能は、ＡＡＡをサポートするためにプライバシーを実現するネットワークの能力に基づくのではなく、クライアントソフトウェアまたはファームウェアが検証プロセスを容易化するように設計されているかどうかに基づく。全てのハイパーセキュアラストマイルはＩＤ検証に対応しているため、以下のハイパーセキュアラストマイルの例はプライベート及び非プライベートのセキュア通信の両方に適用されることを理解する必要がある。したがって、半プライバシー機能を備えたセキュアでないラストマイルネットワークとは異なり、ハイパーセキュアラストマイルを介したプライベート通信は、ネットワークではなく、ＳＤＮＰクライアントによって決定され、ここではクライアントが望むあらゆるレベルの単一要素認証または多要素認証の手順をサポートできる。
【０４３６】
ハイパーセキュアコールの具体例を以下いくつかの例に示す。図１８には、ＳＤＮＰネットワーク及びＷｉＦｉラストリンクを備えた様々なセルラーモバイルデバイスの間のハイパーセキュアラストマイル通信が示されている。示されるように、ＳＤＮＰデータグラムＡとＳＤＮＰペイロードを含むデータパケット１２２２Ａは、ラストマイル通信のＳＤＮＰゲートウェイ１２０１Ａによって、同じくＳＤＮＰペイロードを含むＩＰデータグラムＢで構成されるデータパケット１２２３Ｂに変換される。ハイパーセキュアラストマイルでは、ＳＤＮＰクラウドで使用されるものとは異なる共有秘密、数値シード、暗号化鍵、及び他のゾーン固有のセキュリティクレデンシャル情報が利用されるため、ＩＰデータグラムＢのＳＤＮＰペイロードは、ＳＤＮＰデータグラムＡのＳＤＮＰペイロードとは異なる。言い換えると、あるセキュリティゾーンから別のセキュリティゾーンにペイロードが変更されることで、及びＳＤＮＰルーティング情報がＤＮＳサーバで認識されない送信元ＳＤＮＰアドレス及び宛先ＳＤＮＰアドレスとして埋め込まれることで、ＳＤＮＰゲートウェイ１２０１ＡでＳＤＮＰデータグラムがＩＰデータグラムに変換される。
【０４３７】
次に、ＳＤＮＰゲートウェイ１２０１Ａと通信デバイス、すなわちＳＤＮＰクライアントとして機能するタブレット３３と携帯電話３２の間のパケットルーティングを容易化するために、このゾーン固有のＳＤＮＰペイロードが、ラストマイルネットワーク固有のＩＰアドレス（ＮＡＴまたはインターネットアドレス）を含むＩＰヘッダを有するＩＰデータグラムパケットにラップされる。ラストマイルルーティングの中間デバイスはＳＤＮＰクライアントではないため、ＩＰデータグラムＢ内のＳＤＮＰペイロードの構造は、ラストマイルを移動する際に固定されたままとなる。言い換えると、データパケット１２２３Ｂ、１２２３Ｃ、及び１２２３Ｄは同一に構成されたデータグラムであり、全て同じＳＤＮＰペイロード（パケットがラストマイルに沿ってデバイスからデバイスにホップする際に変化しないペイロード）を有するＳＤＮＰデータグラムＢで構成される。簡単に要約すると、ＩＰデータグラムかＳＤＮＰデータグラムかに関係なく、ＳＤＮＰネットワークノードまたはＳＤＮＰクライアントでのみ、レベル３データグラムに埋め込まれたＳＤＮＰペイロードを再構築することが可能となる。
【０４３８】
示されるように、ＩＰデータグラムＢを含むデータパケット１２２３Ｂが、ＮＳＰが操作する有線またはファイバリンク２４によってネットワークルータ２７に伝送され、続いて同じくＩＰデータグラムＢを含むデータパケット１２２３Ｃが、ＩＳＰが操作する有線またはファイバリンク２４ＡによってＷｉＦｉルータ２６に伝送される。その後、両方ともＳＤＮＰアプリ１３３５Ａを実行する携帯電話３２及びタブレット３３といったモバイルデバイスのＷｉＦｉリンク　２９経由で、ＩＰデータグラムＢを含むデータパケット１２２３Ｄが使用され、ＷｉＦｉルータ２６によりラストリンク通信が容易化される。そのため、これらのデバイスは、ＩＰデータグラムＢを含むデータパケット１２２３Ｄに含まれるデータを解釈できるＳＤＮＰクライアントとして機能する。これには、復号化、ジャ

ンク除去、アンスクランブル化、及びペイロードのコンテンツを他のデータパケットからのデータ断片と混合することで、元のメッセージまたは音を再作成することが含まれる。

【０４３９】

図１９には、ＳＤＮＰネットワーク及びセルラー無線ラストリンクを備えた様々なセルラーモバイルデバイスの間のハイパーセキュアラストマイル通信が示されている。示されるように、ＩＰデータグラムＢを含むデータパケット１２２３Ｂが、ＮＳＰが操作する有線またはファイバリンク２４によってネットワークルータ２７に伝送され、続いて同じくＩＰデータグラムＢを含むデータパケット１２２３Ｃが、モバイルネットワーク事業者の有線またはファイバリンク２４Ｂによって携帯電話基地局１７に伝送され、セルラーネットワーク２５が作成される。その後、両方ともＳＤＮＰアプリ１３３５Ａを実行する携帯電話３２及びタブレット３３といったモバイルデバイスの３Ｇまたは４Ｇ／ＬＴＥセルラーリンク２８経由で、ＩＰデータグラムＢを含むデータパケット１２２３Ｄが使用され、携帯電話基地局１７によりラストリンク通信が容易化される。

【０４４０】

前述の例のように、ラストマイルルーティングの中間デバイスはＳＤＮＰクライアントではないため、ＩＰデータグラムＢ内のＳＤＮＰペイロードの構造は、ラストマイルを移動する際に固定されたままとなる。言い換えると、データパケット１２２３Ｂ、１２２３Ｃ、及び１２２３Ｄは同一に構成されたデータグラムであり、全て同じＳＤＮＰペイロード（パケットがラストマイルに沿ってデバイスからデバイスにホップする際に変化しないペイロード）を有するＳＤＮＰデータグラムＢで構成される。

【０４４１】

図２０には、ＳＤＮＰネットワーク及びイーサネット（登録商標）ラストリンクを備えた様々なテザー（非モバイル）デバイスの間のイーサネット（登録商標）ラストマイル通信が示されている。示されるように、ＩＰデータグラムＢを含むデータパケット１２２３Ｂが、ＮＳＰが操作する有線またはファイバリンク２４によってネットワークルータ２７に伝送され、続いて同じくＩＰデータグラムＢを含むデータパケット１２２３Ｃが、インターネットサービスプロバイダ（ＩＳＰ）の有線またはファイバリンク２４Ａによってイーサネット（登録商標）ルータ１０３Ａに伝送される。その後、ＳＤＮＰアプリ１３３５Ｃを実行するデスクトップコンピュータ３６及びＳＤＮＰファームウェア１３３５Ｂを実行するデスクトップ電話３７といったテザーデバイスのイーサネット（登録商標）１０６Ａ経由で、ＩＰデータグラムＢを含むデータパケット１２２３Ｄが使用され、イーサネット（登録商標）ルータ１０３Ａによりラストリンク通信が容易化される。ラストマイルにＳＤＮＰネットワークノードまたはＳＤＮＰクライアントがない場合、データパケット１２２３Ｂ、１２２３Ｃ、及び１２２３Ｄは同一に構成されたデータグラムであり、全て同じＳＤＮＰペイロード（パケットがラストマイルに沿ってデバイスからデバイスにホップする際に変化しないペイロード）を有するＳＤＮＰデータグラムＢで構成される。

【０４４２】

図２１には、ＳＤＮＰネットワーク及びケーブルサービスクライアントの間のハイパーセキュアラストマイル通信が示されている。示されるように、ＩＰデータグラムＢを含むデータパケット１２２３Ａが、ＮＳＰ有線またはファイバリンク２４によってケーブルＣＭＴＳ　１０１、ケーブルオペレータのコマンド、通信、及びコンテンツ配信センターに伝送される。このようなケーブルオペレータは、ケーブルテレビ、ペイパービュー、電話サービス、インターネット接続、ビジネスサービスといった幅広いサービスを提供している。次に、帯域幅及びリアルタイムサービスが最適化されるように、ＤＯＣＳＩＳ３及びトレリスフォーマット（本開示の背景で説明）に従って変調されたファイバまたは同軸が使用され、ＣＭＴＳ　１０１ヘッドユニットがケーブル１０６経由でクライアントに接続される。ケーブルオペレータは、クライアントに対して透過的に、データグラムフォーマットを維持するか、またはＩＰデータグラムを独自のデータグラムフォーマットにパッケージ化できる。本明細書でＣＭＴＳデータグラムＣと呼ばれるこれらのデータパケットでは、ケーブル固有のＮＡＴアドレス指定が使用され、ケーブル１０６での配信のために、

ＳＤＮＰペイロードがネスト化されたペイロードとしてデータパケット１２２４Ｃ内でカプセル化される。

【０４４３】

示されるように、ケーブルＣＭＴＳ　１０１によりＣＭＴＳデータグラムＣがケーブルモデム１０３にルーティングされる。その後、これにより、ラストリンク配信のための未変更のＳＤＮＰペイロードを有するＩＰデータグラムＢで構成されるペイロードデータパケット１２２３Ｂが抽出される。ＳＤＮＰクライアント対応デバイスへのラストリンクは、イーサネット（登録商標）１０６Ａ経由でＳＤＮＰクライアントアプリ１３３５Ｃを実行するデスクトップコンピュータ３６へ、またはツイストペア銅線７経由でＳＤＮＰクライアントファームウェア１３３５Ｂを実行するコードレス電話５Ａへなど、いくつかのフォーマットで発生する可能性がある。また、ケーブルＣＭＴＳ　１０１により、ＣＭＴＳデータグラムＣがケーブルモデム１０３にルーティングされ、その後、これにより、例えばＩＰデータグラムＢなどの元のＩＰデータグラムが抽出され、それと他のビデオコンテンツがケーブル１０６を介してケーブルテレビセットトップボックスに送信される。そして、ケーブルセットトップボックスから、ＩＰデータグラムＢとコンテンツがＨＤＭＩ（登録商標）－２　１０７経由で、ＳＤＮＰアプリ１３３５Ｄを実行するＵＨＤインタラクティブテレビ３９に転送される。または、ケーブルテレビセットトップボックス１０２でＳＤＮＰファームウェアをホストできる。

【０４４４】

図２２には、ＳＤＮＰネットワークとケーブルサービスプロバイダを介して接続されたＷｉＦｉホームネットワーク間のハイパーセキュアラストマイル通信が示されている。示されるように、ＩＰデータグラムＢを含むデータパケット１２２３Ｂが、ＮＳＰ有線またはファイバリンク２４Ａによってケーブル　ＣＭＴＳ　１０１、ケーブルオペレータのコマンド、通信、及びコンテンツ配信センターに伝送される。次に、有線またはファイバリンク２４Ａが使用され、同軸またはファイバ経由で、ＣＭＴＳ　１０１ヘッドユニットが特定のクライアントのケーブル（ＷｉＦｉ）モデムルータ１００Ｂに接続され、ＷｉＦｉアクセスポイント２６が作成される。データパケット１２２４Ｃのルーティングには、インターネットアドレスを有するＩＰデータグラム、またはＮＡＴアドレス指定を有する独自のＣＭＴＳデータグラムＣが含まれる場合がある。ＳＤＮＰゲートウェイ１２０１Ａとケーブル（ＷｉＦｉ）モデムルータ２６との間のルーティングは、ハイパーセキュアラストマイルの有線区間を表す。

【０４４５】

ホームネットワークの最後の区間には、ＩＰデータグラムＢを含むデータパケット１２２３Ｄによってケーブル（ＷｉＦｉ）モデムルータ２６を様々なホームデバイスにワイヤレスで接続するＷｉＦｉリンク２９が含まれる。エンドツーエンドのハイパーセキュリティを促進するには、こうしたデバイスは、デバイスにロードされたソフトウェアまたはファームウェアを使用するＳＤＮＰクライアントとして動作するものでなければならない。例えば、ノートブック３５及びデスクトップコンピュータ３６は、コンピュータアプリ１３３５Ｃを使用してＳＤＮＰクライアントとして動作し、携帯電話３２及びタブレット３３は、モバイルアプリ１３３５Ａを使用してＳＤＮＰクライアントとして動作する。ＩｏＴデバイス（この例では冷蔵庫３４Ｋ）は、制御システムにＳＤＮＰファームウェア１３３５Ｅがロードされている場合、ＳＤＮＰクライアントとして動作できる。しかし、こうしたデバイスにＳＤＮＰクライアントのソフトウェアを組み込まない場合、または組み込むことができない場合は、他の方法でエンドツーエンドのセキュリティを実現する必要がある。

【０４４６】

ＩＤペアのラストリンクセキュリティ

【０４４７】

接続されたデバイスがＳＤＮＰクライアントとして動作できない場合は、エンドツーエンドのハイパーセキュリティを保証することができない。この場合は、ＳＤＮＰリモート

ゲートウェイを使用してハイパーセキュリティ通信を拡張し、ラストリンクを除く通信のラストマイルをカバーできる。通信デバイスに直接接続されるラストマイルの部分であるラストリンクがＳＤＮＰホストとして有効化されていない場合は、ラストリンクの通信を容易にするために使用されるローカルエリアネットワーク（ＬＡＮ）を介してラストリンクセキュリティを保証する必要がある。図２３は、ラストマイル通信におけるＳＤＮＰリモートゲートウェイ１３５０の使用を概略的に表したものである。ＳＤＮＰリモートゲートウェイ１３５０には、リモートゲートウェイとして機能するためにＳＤＮＰファームウェア１３３５Ｈにより有効化される任意の通信デバイスが含まれる。したがって、ＳＤＮＰゲートウェイ１２０１ＡとＳＤＮＰリモートゲートウェイ１３５０との間のＳＤＮＰ接続は、ＩＰまたはＮＡＴソース及び宛先アドレスとＳＤＮＰペイロード１２２２を含むＩＰデータグラム１２２３Ａで構成される。ＳＤＮＰペイロード１２２２には、ＤＮＳサーバで認識されないＳＤＮＰアドレス及びラストマイルゾーン固有のセキュリティクレデンシャル情報を使用してネスト化されるＳＤＮＰペイロードが含まれる。このＳＤＮＰ接続は、ＩＤ検証と発信者のプライバシーをサポートできるハイパーセキュアである。

【０４４８】

ＳＤＮＰリモートゲートウェイ１３５０とＳＤＮＰクライアント以外の接続された任意のデバイス（デスクトップコンピュータ３６など）の間では、ローカルエリアネットワークまたはイーサネット（登録商標）、ＷｉＦｉ、他のプロトコルなどのＬＡＮ接続によって通信が実行される。ＬＡＮセキュリティプロトコル、及び通信デバイスとＳＤＮＰリモートゲートウェイ間のデバイスペアリングにより、セキュリティが容易化される。デバイスペアリングは、不正アクセスを防止するために、２つの通信デバイス間の認証シーケンスにより２つのデバイスのＩＤが確立されるプロセスである。

【０４４９】

図２４は、ＳＤＮＰ対応ルータ１３５１、すなわちＳＤＮＰファームウェア１３３５Ｈを実行するルータの使用により、リモートＳＤＮＰゲートウェイの機能が実行される例を示すものである。このゲートウェイにより、ＩＰデータグラムＡを含むデータパケット１２２３Ａが、ＩＰデータグラムＢを含むデータパケット１２２３Ｂに変換される。ＳＤＮＰファームウェア１３３５ＨではＩＰデータグラムＡに含まれるＳＤＮＰペイロードが解釈されるが、接続されたデバイスはＳＤＮＰクライアントではない。代わりに、ＳＤＮＰルータ１３５１により、ＳＤＮＰペイロードが従来型のＩＰペイロードに変換される。追加のセキュリティ方法をデバイスに導入しない限り、このラストリンクはセキュアとはならない。家庭で使用する場合は、ラストリンクが家庭内で発生するため、多くの場合、このセキュアでないデバイス接続は問題とはならない。ハッカーが物理的に家に侵入して盗聴しない限り、こうした有線接続をスニッフィングすることはできない。家庭内における非ＳＤＮＰデバイスへの有線のラストリンクの例には、例に示されるようにデスクトップコンピュータ３６に接続された、及びテレビ３９に接続されたモデム１０３ＣまたはＨＤＭＩ（登録商標）－２に接続されたイーサネット（登録商標）１０６Ａが含まれる。

【０４５０】

ＳＤＮＰ接続とハイパーセキュア通信はＳＤＮＰルータ１３５１までしか拡張されないため、有線接続のセキュリティを実現するには、ラストリンクが認証と暗号化に依存することになる。イーサネット（登録商標）の場合、このようなセキュリティでは、レイヤ１からレイヤ３で動作するｉＳＣＳＩなど、認証デバイス間の暗号化を利用する仮想ローカルエリアネットワーク操作またはＶＬＡＮのように、任意の数のセキュリティ方法（http://www.computerweekly.com/feature/iSCSI-security-Networking-and-security-options-available）を利用できる。または、「ＩＰセキュリティ」またはＩＰＳｅｃフレームワークを使用して、レイヤ４からレイヤ６の方法を使用してセキュリティを実現できる。元々はデータストレージ向けとして開発され、業界規格としてシスコによって推進されたＩＰＳｅｃには、２つのセキュリティモードがある。「認証ヘッダ」モードでは、受信デバイスでデータの送信者を認証できる。このモードでは、データフィールドは暗号化されるが、ヘッダでは認識可能なＩＰアドレスが使用される。トンネルモードとも呼ば

れるカプセル化セキュリティペイロード（ＥＳＰ）では、ＩＰヘッダを含むＩＰパケット全体が暗号化され、新しい非暗号化ＩＰパケットにネスト化されるため、ルーティングが適切に機能し、パケットが正しいネットワーク宛先に伝送される。

【０４５１】

いずれの場合も、セキュリティは、デバイスのネットワークへの接続を許可する認証デバイスに依存する。例えば、コンピュータ、共有ストレージドライブ、ＩｏＴ、及び他のデバイスに接続されるパーソナルネットワークなどのホームネットワークでは、ネットワークに接続されるハードウェアが頻繁に変更されることはない。このような場合、基本的に、認証にはネットワークまたはルータにアクセスするデバイスの登録プロセスが含まれる。特定のユーザのＩＤを識別するのではなく、このタイプの認証はデバイス間、すなわちデバイスからデバイスへの間で行われ、一般的にはデバイスタグ、名前、またはＩＤ番号の使用により、接続が承認されたデバイスが識別及び認識される。ネットワーク接続の確立には、デバイスが最初に相互に導入され、ユーザが接続を承認された後のセットアップ段階が含まれる。そして、有線デバイスが物理的に他のデバイスに接続されるたびに、またはＷｉＦｉの場合は２つのデバイスが互いの範囲内に入るたびに、自動認証シーケンスが実行される。本明細書ではＩＤペアリングと呼ばれるこのセットアップ段階は、デバイス登録、デバイスボンディング、デバイスペアリング、ペアリング、またはペアボンディングとも呼ばれる場合がある。Ｂｌｕｅｔｏｏｔｈ（登録商標）ヘッドフォンを携帯電話に接続するデバイス、またはＢｌｕｅｔｏｏｔｈ（登録商標）携帯電話を車のハンズフリーオーディオシステムにペアリングするデバイスでも、同様のプロセスが使用される。プロトコルには、チャレンジハンドシェイク認証プロトコルまたはＣＨＡＰ、Ｋｅｒｂｅｒｏｓ　Ｖ５、シンプルな公開鍵の汎用的なセキュリティサービスアプリケーションプログラミングインターフェイス（ＧＳＳＡＰＩ）、セキュアリモートパスワード（ＳＲＰ）、及びリモート認証ダイヤルインユーザサービス（ＲＡＤＩＵＳ）が含まれる。ＲＡＤＩＵＳなどの方法は、破られた暗号化方法に依存するが、それでも他の技術と組み合わせて使用されている。

【０４５２】

イーサネット（登録商標）通信ではイーサネット（登録商標）モデム１０３ＣなどのＩＤペアデバイスが保護されるが、ツイストペア銅線コンダクタ７を介してコードレス電話５Ａ及びデスクトップ電話３７に伝送されるアナログ電話信号で構成されるモデムの出力の場合、ラストリンクはセキュアではない。さらに、コードレス電話５Ａの通信フォーマットはセキュアではなく、傍受及び監視の対象となる。このため、セキュア通信で家庭の電話を使用することは勧められない。

【０４５３】

ビデオコンテンツの配信も、セキュリティにおいては関心の対象となる。例えば、ＳＤＮＰルータ１３５１のＨＤＴＶ　３９への通信では、高解像度マルチメディアインターフェイス（ＨＤＭＩ（登録商標））、ＤｉｓｐｌａｙＰｏｒｔ（ＤＰ）、デジタルビジュアルインターフェイス（ＤＶＩ）、及びあまり人気はないがギガビットビデオインターフェイス（ＧＶＩＦ）などのビデオ通信フォーマット、または統合デジタルインターフェイス（ＵＤＩ）は、通常、ＨＤＴＶまたはディスプレイモニターへの物理的な接続で構成される。元々この接続とそのデータのセキュリティは、著作権で保護された材料の違法な複製と配布の防止を焦点として、映画スタジオとコンテンツプロバイダの関心事となっていた。ビデオリンクのセキュリティを維持するためにＩｎｔｅｌ　Ｃｏｒｐ．が開発したセキュリティプロトコルの１つに、高帯域幅デジタルコンテンツ保護（ＨＤＣＰ）（https://en.wikipedia.org/wiki/High-bandwidth_Digital_Content_Protection）というものがある。元々このシステムは、ＨＤＣＰで暗号化されたコンテンツが未許可のデバイスで再生されるのを防ぐことを目的するものであった。このシステムでは、コンテンツが送信される前に、テレビ受信機またはディスプレイの認証が確認される。したがって、ＤＨＣＰでは、認証によってライセンスのないデバイスによるデータ受信が防止され、データの暗号化によって情報の盗聴が防止され、そして侵害されたデバイスの鍵は取り消される。

【０４５４】
ＨＤＣＰでは、認証により、すなわちＩＤペアリングを使用して、モデムからテレビへのコンテンツの流れを保護できる。しかし、スマートテレビの出現により、データフローが双方向となった。リビジョン１．４以降、テレビからモデムまたはセットトップボックスへのアップストリームデータフローを容易化する手段として、ＨＥＣまたはＨＤＭＩ（登録商標）イーサネット（登録商標）チャネルとして知られる高速双方向データチャネルがＨＤＭＩ（登録商標）に組み込まれるようになった。このデータチャネルでは、１００ＭＣ／ｓｅｃイーサネット（登録商標）経由でＨＤＭＩ（登録商標）に接続されたデバイスからデータを送受信できるため、ＩＰテレビなどのＩＰベースアプリケーションに対応できる。ＨＤＭＩ（登録商標）イーサネット（登録商標）チャネルにより、インターネット対応のＨＤＭＩ（登録商標）デバイスで、個別のイーサネット（登録商標）ケーブルを必要とせずに、ＨＤＭＩ（登録商標）リンクを介してインターネット接続を共有できる。そのため、同じセキュリティプロトコルとイーサネット（登録商標）で利用可能なＩＤペアリングを使用して、ＨＤＭＩ（登録商標）経由でセキュア通信を容易化できる。
【０４５５】
図２５には、ＳＤＮＰ対応ＷｉＦｉルータ１３５２、すなわちＳＤＮＰファームウェア１３３５Ｊを実行するＷｉＦｉルータの使用により、リモートＳＤＮＰゲートウェイの機能が実行される例が示されている。このゲートウェイにより、ＩＰデータグラムＡを含むデータパケット１２２３Ａが、ＩＰデータグラムＢを含むデータパケット１２２３Ｂに変換される。ＳＤＮＰファームウェア１３３５ＪではＩＰデータグラムＡに含まれるＳＤＮＰペイロードが解釈されるが、接続されたデバイスはＳＤＮＰクライアントではない。代わりに、ＳＤＮＰ　ＷｉＦｉルータ１３５２によりＳＤＮＰペイロードが従来型のＩＰペイロードに変換され、ＷｉＦｉアクセスポイント２６が使用されて、接続されたデバイスとのワイヤレス通信が行われ、ＷｉＦｉリンク２９を介した通信が容易化される。追加のセキュリティ方法をデバイスに導入しない限り、このラストリンクはセキュアとはならない。家庭やオフィスにおけるＷｉＦｉ通信の場合、遠方からでもデータパケットがスニッフィングされる可能性があるため、セキュリティが懸念事項となる。ＷｉＦｉ接続された家庭デバイス及びオフィスデバイスの例には、デスクトップコンピュータ３６、ノートブック３５、タブレット３３、携帯電話３２、スピーカー３４Ｂ、プリンタ／スキャナ３４Ａ、及び共有データドライブ３４Ｃが含まれる。
【０４５６】
接続されたデバイスとＳＤＮＰゲートウェイ（すなわちＳＤＮＰ　ＷｉＦｉルータ１３５２）との間のセキュリティは、旧ＷＰＡとそのセキュアでない前身のＷＰＥの代替であるＷｉＦｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓ　ＷＰＡ－ＩＩまたはＷＰＡ２（ＩＥＥＥ８０２．１１ｉ－２００４）など、任意の数の業界標準プロトコルを使用して達成される。ＷＰＡ２通信はＣＣＭＰを使用して保護される。ＣＣＭＰは、１２８ビット鍵と１２８ビットブロックサイズでのＡＥＳ処理に基づく「Counter Mode Cipher Block Chaining Message Authentication Code Protocol」の頭文字である。ＣＣＭＰでは、データの機密性が提供され、認証が必要となり、アクセス制御が設定される。認証には、セットアップ時のＩＤペアリングが含まれる。再ペアリングは手動で実行する必要がある。ＣＣＭＰセキュリティは優れてはいるが、ハイパーセキュアではなく、ＳＤＮＰクライアントにより得られる匿名データパケットとＳＤＮＰ通信の動的な性質に欠ける。
【０４５７】
図２６は、ホームネットワークでＩｏＴに接続されたデバイスの例である。この例では、ＳＤＮＰ対応ＷｉＦｉルータ１３５２、すなわちＳＤＮＰファームウェア１３３５Ｊを実行するＷｉＦｉルータの使用により、リモートＳＤＮＰゲートウェイの機能が実行される。このゲートウェイにより、ＩＰデータグラムＡを含むデータパケット１２２３Ａが、ＩＰデータグラムＢを含むデータパケット１２２３Ｂに変換される。ＳＤＮＰファームウェア１３３５ＪではＩＰデータグラムＡに含まれるＳＤＮＰペイロードが解釈されるが、ＩｏＴに接続されたデバイスはＳＤＮＰクライアントではない。代わりに、ＳＤＮＰ　Ｗ

ｉＦｉルータ１３５２によりＳＤＮＰペイロードが従来型のＩＰペイロードに変換され、そしてＷｉＦｉアクセスポイント２６からのＷｉＦｉリンク２９が使用され、ワイヤレスで、接続されたデバイスとの通信が行われる。追加のセキュリティ方法が実装されていない限り、特にＷｉＦｉデータパケットが遠方からスニッフィングされる可能性があるため、このラストリンクはセキュアではない。家庭でＷｉＦｉに接続されたＩｏＴデバイスの例には、セントラルヒーティングとエアコン３４Ｄ、照明３４Ｇ、ブラインド３４Ｆ、大型家電３４Ｋ、ポータブル及び室内ＨＶＡＣ　３４Ｅ、ガレージドア３４Ｌ、ホームモニタリング３４Ｊ、及びホームセントラルセキュリティシステム３４Ｈが含まれる。

【０４５８】

接続されたデバイスとＳＤＮＰゲートウェイ（すなわちＳＤＮＰ　ＷｉＦｉルータ１３５２）との間のセキュリティは、ＣＣＭＰを用いる前述のＷｉＦｉ　Ｐｒｏｔｅｃｔｅｄ　Ａｃｃｅｓｓプロトコル ＷＰＡ２など、任意の数の業界標準プロトコルを使用して、データの機密性を確保し、認証を要求し、アクセス制御を設定することで達成される。ＷＰＡ２では、ＩＤペアリング、レイヤ２プロトコルとして実装されたデバイス検証を使用してセキュリティが達成される。この方法には手動認証方法が含まれるため、扱いにくい。

【０４５９】

ＩｏＴ通信のために、ローカルエリアネットワークで使用される代替プロトコル「ＡｌｌＪｏｙｎフレームワーク」と呼ばれる近接ネットワークが最近導入された。このフレームワークでは、デバイスが検知され、セッションが作成され、そしてセキュア通信が容易化される。このフレームワークは、ＷｉＦｉ、イーサネット（登録商標）、シリアルバス通信、電力線ＰＬＣなど、多数のレイヤ２トランスポートレイヤを使用してＩｏＴデバイスの接続性をサポートするように設計されている。アプリケーションは、Ｌｉｎｕｘ（登録商標）、Ｗｉｎｄｏｗｓ（登録商標）、ＭａｃＯＳ、Ａｎｄｒｏｉｄ（登録商標）、ｉＯＳ、ＲＴＯＳリアルタイムオペレーティングシステム、オープンソース開発環境Ａｒｄｕｉｎｏを含む多数のプラットフォームで動作するＣ、Ｃ＋＋、Ｏｂｊ．Ｃ、及びＪａｖａ（登録商標）に基づいている。

【０４６０】

ＡｌｌＪｏｙｎに準拠したアプリケーションでは、相互の認証が行われ、暗号化されたデータが交換されて、エンドツーエンドのアプリケーションレベルのセキュリティが実現する。認証とデータ暗号化は、アプリケーションレイヤ７で実行される。ルータレイヤとも呼ばれるトランスポートレイヤ２では、アプリケーションエンドポイント間でセキュリティ関連のメッセージが送信されるが、セキュリティロジック自体は実装されない。アプリケーションレイヤ７にも「認証リスナー」と呼ばれるコールバック機能が実装され、これによりＰＩＮ、パスワード、または認証証明書を使用する認証が容易化される。セキュリティは、ＡＥＳ１２８ピアツーピア暗号化を使用して達成される。ＷＰＡと同様に、ＡｌｌＪｏｙｎでは、コマンド及び制御シーケンスの実行前に、認証プロセスでＩＤペアリングが使用される。サポートされる認証方法には、事前共有鍵（ＰＳＫ）、セキュアリモートパスワード（ＳＲＰ）鍵の交換、またはユーザ名とパスワードを使用するログオンが含まれる。このプロトコルでは、（ｉ）認証なし、（ｉｉ）事前に交換された鍵による認証、及び（ｉｉｉ）Ｘ．５０９　ＥＣＤＳＡ証明書による認証のＥＣＤＨＥ（Ｅｌｌｉｐｔｉｃ　Ｃｕｒｖｅ　Ｄｉｆｆｉｅ-Ｈｅｌｌｍａｎ　Ｅｐｈｅｍｅｒａｌ）鍵交換もサポートされている。

【０４６１】

同じ技術を企業に適用できる。図２７は、ホームネットワークでＩｏＴに接続されたデバイスの例である。この例では、ＳＤＮＰ対応ＷｉＦｉ及びイーサネット（登録商標）ルータ１３５２Ｚ、すなわちＳＤＮＰファームウェア１３３５Ｊを実行するイーサネット（登録商標）及びＷｉＦｉルータの使用により、リモートＳＤＮＰゲートウェイの機能が実行される。このゲートウェイにより、ＩＰデータグラムＡを含むデータパケット１２２３Ａが、ＩＰデータグラムＢを含むデータパケット１２２３Ｂに変換される。ＳＤＮＰファームウェア１３３５ＪではＩＰデータグラムＡに含まれるＳＤＮＰペイロードが解釈され

るが、ＩｏＴに接続されたデバイスはＳＤＮＰクライアントではない。代わりに、ＳＤＮＰ及びイーサネット（登録商標）ＷｉＦｉルータ１３５２ＺによりＳＤＮＰペイロードが従来型のＩＰペイロードに変換され、ＷｉＦｉリンク２９及びイーサネット（登録商標）１０６Ａの両方が使用されて、接続されたデバイスとの通信が行われる。

【０４６２】

追加のセキュリティ方法が実装されていない限り、特にＷｉＦｉデータパケットが遠方からスニッフィングされる可能性があるため、このラストリンクはセキュアではない。ＷｉＦｉに接続されたＩｏＴビジネスデバイスの例には、セントラルヒーティングとエアコン３４Ｄ、照明３４Ｇ、監視システム３４Ｊ、セキュリティシステム３４Ｈ、ＰＯＳ端末３８、タブレット３３などのＷｉＦｉホットスポットに接続されたデバイスが含まれる。企業の有線接続デバイスは事業の性質に依存する。銀行業では、デバイスにはイーサネット（登録商標）接続のＡＴＭマシン３８Ｄが含まれる。ガソリンスタンドでは、デバイスには、例としてイーサネット（登録商標）接続のガスポンプ３８Ａが含まれる。

【０４６３】

要約すると、ラストリンクは、ＳＤＮＰリモートゲートウェイと通信する非ＳＤＮＰクライアントで保護できる。このように、ラストマイルの大半はハイパーセキュアであり、ラストリンクではＩＤペア暗号化セキュリティが使用されている。

【０４６４】

ＳＤＮＰブリッジ通信

【０４６５】

前述のように、ＳＤＮＰクラウド外のラストマイルデータ転送では、必ずＩＰデータグラム、すなわちインターネットの送信元アドレスと宛先アドレスを使用するか、ネットワークオペレータのＮＡＴアドレスを使用するデータパケットが使用される。例えば、オフィスビル内で運用している場合、またはサーバでＳＤＮＰソフトスイッチをホストするローカルネットワークサービスプロバイダと協力して運用している場合など、プライベートネットワークの場合は、ＳＤＮＰデータグラムを利用してラストマイルの一部でハイパーセキュア通信を実現することもできる。

【０４６６】

前述のように、ハイパーセキュア通信ではサーバに依存してＳＤＮＰソフトスイッチソフトウェアまたはファームウェアがホストされ、ＳＤＮＰクラウド内のＩＰデータグラムではなく、ＳＤＮＰデータグラムと匿名アドレスを使用して通信が行われるため、これらのＳＤＮＰソフトスイッチ対応サーバは、ＳＤＮＰノード表記$M_{0,0}$、$M_{0,1}$、$M_{1,0}$、$M_{1,1}$などで指定されるＳＤＮＰノードと呼ばれる。上記の米国出願第１４／８０３，８６９号でも、ＩＰデータグラムが他のＳＤＮＰクラウドにルーティングされるＳＤＮＰゲートウェイであるＳＤＮＰブリッジで接続された複数の独立ＳＤＮＰクラウド間の通信が開示されている。

【０４６７】

ＳＤＮＰブリッジの概念は、ラストマイル通信の一部に同様に適応させることができる。ラストマイル内にＳＤＮＰサブネットワークまたはミニクラウドを作成するには、ＳＤＮＰブリッジソフトウェアまたはファームウェアで２つ以上のサーバを有効化する必要がある。エンドデバイス、すなわち発信側のデバイスで動作するＳＤＮＰクライアントソフトウェアまたはファームウェアとは異なり、ＳＤＮＰブリッジ操作は最終接続として動作するのではなく、データのルーティングに使用される。そのため、２つ以上の隣接するＳＤＮＰブリッジは、スタンドアロンのＳＤＮＰブリッジネットワーク、ＳＤＮＰミニクラウド、またはＳＤＮＰアドホックネットワークとして動作させることができる。開示されるように、ＳＤＮＰブリッジ機能は、ＷｉＦｉルータのブリッジモード操作のレイヤ２ディスクリプションの構造に類似したレイヤ３ディスクリプションを表す。ＳＤＮＰブリッジまたはＳＤＮＰブリッジネットワーク内では、ＳＤＮＰデータグラムを使用して通信が行われる。ＳＤＮＰブリッジまたはＳＤＮＰブリッジネットワーク外からＳＤＮＰブリッジへの通信では、ＳＤＮＰペイロードを有するＩＰデータグラムが使用される。

【０４６８】
図２８の例示的概略図には、ラストマイル通信内のＳＤＮＰブリッジの操作が示されている。これは、ＳＤＮＰゲートウェイ１２０１Ａを有するＳＤＮＰネットワーク、ＳＤＮＰファームウェア１３３５Ｈと１３３５Ｊをそれぞれ実行するＳＤＮＰブリッジルータ１３５０と１３５２Ｚで構成されるＳＤＮＰブリッジ、及びＳＤＮＰクライアントではない接続クライアントデバイス（この例ではノートブック３５として示される）で構成される。示されるように、ＳＤＮＰゲートウェイ１２０１ＡとＳＤＮＰブリッジ１３５０との間の通信は、ＩＰアドレスとＳＤＮＰペイロードを含むＩＰデータグラム１２２３Ａが使用されるセキュアな接続から構成される。ＳＤＮＰペイロード１２２２Ａには、ゾーン固有のセキュリティクレデンシャル情報を使用してエンコードされたＳＤＮＰルーティング情報とセキュアなＳＤＮＰペイロードが含まれる。そのため、ＩＰアドレスルーティングが使用されていても、ＳＤＮＰペイロードを使用してハイパーセキュアが実現する。
【０４６９】
ＳＤＮＰブリッジ接続内、すなわちＳＤＮＰブリッジルータ１３５０とＷｉＦｉ対応ＳＤＮＰブリッジルータ１３５２Ｚの間では、ハイパーセキュア通信はＳＤＮＰデータグラム１２２２Ｂを使用して行われる。ＳＤＮＰルーティング情報は、ＳＤＮＰペイロード１２２２Ａに含まれるＳＤＮＰアドレス指定から抽出される。ＳＤＮＰブリッジとＳＤＮＰ接続にはラストマイル通信のハイパーセキュア有線区間が含まれ、ここではＩＤ検証とアカウント検証をサポートでき、プライバシーがサポートされる。
【０４７０】
ＳＤＮＰブリッジルータ１３５２Ｚから非ＳＤＮＰクライアントデバイス、すなわちノートブック３５への接続では、ＷｉＦｉまたはイーサネット（登録商標）のいずれかのローカルエリアネットワークで、ＩＰアドレスとＩＰペイロードを有するＩＰデータグラム１２２３Ｂが利用される。ハイパーセキュアではなくても、このラストリンクのセキュリティは、ｉＳＣＳＩ、ＩＰＳｅｃ、ＷＰＡ、ＡｌｌＪｏｙｎなど、前述のイーサネット（登録商標）及びＷｉＦｉセキュリティプロトコルのいずれかによって保護できる。
【０４７１】
任意の数の物理媒体（ｐｈｙｓｉｃａｌ　ｍｅｄｉｕｍ）により伝送される任意の２つのＳＤＮＰ対応デバイス間でＳＤＮＰブリッジを実装できる。つまり、ＳＤＮＰブリッジングは、レイヤ１　ＰＨＹとレイヤ２トランスポートレイヤの具現から不可知的に操作されるレイヤ３プロトコルである。例えば、図２９Ａに示される最上部の概略図は、イーサネット（登録商標）（有線）ブリッジ経由で、ＳＤＮＰデータグラム１２２２が使用されて、それぞれＳＤＮＰファームウェア１３３５Ｈを実行する２つのＳＤＮＰブリッジイーサネット（登録商標）ルータ１３５１Ａから行われる通信を示したものである。中央の概略図には、それぞれにイーサネット（登録商標）及びＷｉＦｉ通信が可能で、ＳＤＮＰファームウェア１３３５Ｊを実行する２つのＳＤＮＰブリッジルータ１３５２Ｚが示されている。ＷｉＦｉ（ワイヤレス）ブリッジ経由で、ＳＤＮＰデータグラム１２２２が使用されて、このＳＤＮＰブリッジルータから通信が行われる。最下部の概略図には、イーサネット（登録商標）（有線）ブリッジ経由で、ＳＤＮＰデータグラム１２２２が使用されて、ＳＤＮＰファームウェア１３３５Ｈを実行するＳＤＮＰブリッジイーサネット（登録商標）ルータ１３５１Ａから、イーサネット（登録商標）及びＷｉＦｉ通信が可能で、かつＳＤＮＰファームウェア１３３５Ｊを実行するＳＤＮＰブリッジルータ１３５２Ｚに対して行われる通信が示されている。このように、ラストマイルのＳＤＮＰクラウド外で動作している場合でも、２つ以上のＳＤＮＰ対応ルータで構成されるＳＤＮＰブリッジから、建物全体またはプライベートネットワーク全体にＳＤＮＰデータグラムをルーティングまたは配信できる。
【０４７２】
ＳＤＮＰブリッジは、ケーブルテレビシステムなどの独自のハードウェアを使用してシステムに拡張できる。例えば、図２９Ｂに示される最上部の概略図では、ＳＤＮＰファームウェアまたはソフトウェア１３３５Ｌを実行してケーブルＣＭＴＳ　ＳＤＮＰブリッジ

１０１として動作するように２つのケーブルＣＭＴＳ「ヘッド」サーバが変更されている。ケーブルまたはファイバ（有線）ブリッジ経由で、ＳＤＮＰデータグラム１２２２が使用され、このサーバから通信が行われる。ＳＤＮＰブリッジは、ＣＭＴＳヘッドから加入者の自宅まで拡張できる。中央の概略図に示されるように、ケーブル（同軸）ブリッジ経由で、ＳＤＮＰデータグラム１２２２が使用され、ＳＤＮＰファームウェアまたはソフトウェア１３３５Ｌを実行するケーブルＣＭＴＳ　ＳＤＮＰブリッジ１０１から、ＳＤＮＰファームウェア１３３５Ｍを実行するケーブルテレビセットトップボックスまたはケーブルモデム１０２へ通信が行われる。この方法で、ＳＤＮＰブリッジにより、ハイパーセキュア通信を自宅またはオフィスに拡張する。

【０４７３】

開示されるＳＤＮＰブリッジ方法は、無線ネットワークを介したデータ転送にも使用できる。図２９Ｂの最下部の概略図には、ＳＤＮＰファームウェアまたはソフトウェア１３３５Ｎを実行し、携帯電話基地局ＳＤＮＰブリッジ１７Ｘと１７Ｙとして機能する２つの携帯電話基地局と無線タワーが示されている。セルラーブリッジ２５Ｘと２５Ｙを含むセルラーネットワーク経由で、ＳＤＮＰデータグラム１２２２が使用され、これらの携帯電話基地局と無線タワーからワイヤレスで通信が行われる。図２９Ｃに示される上部の概略図には、ＳＤＮＰファームウェアまたはソフトウェア１３３５Ｏを実行し、地上衛星間リンクＳＤＮＰブリッジ９２Ｃとして機能する地上マイクロ波基地局が示されている。ＳＤＮＰデータグラム１２２２が使用され、ＳＤＮＰファームウェアまたはソフトウェア１３３５Ｐを実行する軌道衛星、すなわち衛星ＳＤＮＰブリッジ９３に対して、マイクロ波衛星ブリッジとしてこの地上マイクロ波基地局から通信が行われる。次に、衛星から加入者または他の衛星へ通信が行われる。

【０４７４】

ＳＤＮＰブリッジ通信は、自動車をピアツーピアアドホック通信ネットワークとして使用する自動車アプリケーションに適合できる。図２９Ｃの下部の概略図には、自動車の無線ブリッジ経由で、ＳＤＮＰデータグラム１２２２が使用され、ＳＤＮＰファームウェア１３３５Ｆを実行する自動車１３９０Ａのテレマティックスモジュールから、ＳＤＮＰファームウェア１３３５Ｆを実行する近くの自動車１３９０Ｂへ行われる通信が示されている。ＳＤＮＰファームウェアが有効化されたそれぞれの自動車では、動的テレマティックスＳＤＮＰブリッジネットワークの別の通信ノードが形成される。この通信では、特定の自動車またはドライバーに送信される情報ではなく、セルラータワーがローカルに存在しない場合でも、高速道路に沿って情報を渡すことができる通信ネットワークが形成される。

【０４７５】

ＳＤＮＰブリッジネットワークの概念は、広い地域における通信、及び自動車、トラック、緊急車両、列車、飛行機、ボート、海洋船が関与する輸送及び運送で特に有益である。特に、広域にわたる通信範囲を実現するには、衛星ネットワークが必要となる。通常、システムには衛星ブリッジまたはバックホールと呼ばれる衛星オペレータとのネットワーク接続が含まれ、衛星配信とも呼ばれるそのクライアントと加入者に衛星がリンクする。図３０は、ＳＤＮＰハイパーセキュア通信に適応される様々な衛星接続を概略的に表したものである。示されるように、ＳＤＮＰデータグラムＡ及びＳＤＮＰペイロードを含むデータパケット１２２２Ａを伝送する有線接続９４Ａが使用され、ＳＤＮＰゲートウェイ１２０１Ａから、ＳＤＮＰファームウェアまたはソフトウェア１３３５Ｏを実行する地上衛星アンテナ皿９２Ｃへ通信が行われる。ここから、同じＳＤＮＰデータグラムＡがデータパケット１２２２Ｂとして、衛星ブリッジ９５Ａ経由で、ＳＤＮＰファームウェアまたはソフトウェア１３３５Ｐを実行するサテライト９３に中継される。

【０４７６】

ＳＤＮＰからの様々なクライアントへのハイパーセキュア通信データパケットの配信により、ＳＤＮＰペイロードを含むデータパケット１２２２ＣとＳＤＮＰデータパケットＡが衛星９３に含まれる。衛星通信は双方向であり、衛星９３から地上クライアントへのダウンリンクでは、アップリンク接続よりも高い信号強度と高速のデータレートが可能とな

る。言い換えると、クライアントの応答よりも高いデータレートかつより強力な信号強度で、衛星から地上クライアントへの送信が可能となる。衛星９３から加入者へのリンクの例には、ＳＤＮＰファームウェア１３３５Ｔを実行するディッシュインターネット加入者９２Ｇへの衛星リンク９５Ｂ、ＳＤＮＰファームウェア１３３５Ｓを実行する衛星電話９２Ｆ、ＳＤＮＰファームウェア１３３５Ｇを実行する高速列車１３６０Ｃに配置された衛星アンテナアレイ９２Ｈ、ＳＤＮＰファームウェア１３３５Ｒを実行する海洋船１３６０Ｂに配置された衛星アンテナアレイ９２Ｅ、及びＳＤＮＰファームウェア１３３５Ｑを実行する航空機１３６０Ａに配置された衛星アンテナアレイ９２Ｄが含まれる。

【０４７７】

船舶、航空機、列車などの大型車両の場合、各システムにより、このハイパーセキュア衛星通信リンクが独自の内部通信システムまたはローカルエリアネットワークに接続される。例えば、図３１Ａには、航空機１３６０Ａの胴体に配置され、ＳＤＮＰファームウェア１３３５Ｘを実行する衛星アンテナモジュール９２Ｄから、ＳＤＮＰソフトウェア１３３５Ｚを実行する通信中央サーバ１３６１に接続される民間航空機の例が示されている。通信中央サーバ１３６１は、機器１３６７、データレコーダとブラックボックス１３６８、メディアストレージモジュール１３６３、及びオプションでＳＤＮＰファームウェア１３３５Ｌを実行するＷｉＦｉルータモジュール１３６２を含む様々なシステムにリンクする。ＷｉＦｉホットスポット通信をサポートするため、ＷｉＦｉルータモジュール１３６２から、航空機全体に配置されたＷｉＦｉアンテナ１３６１のアレイに接続される。図３１Ｂの例に示されるように、無線ベースの飛行制御を除く全ての通信は、アンテナモジュール９２Ｄを使用して、共通の衛星通信リンクを介して行われる。アンテナモジュールには、衛星送信アンテナ１３６０Ａ、衛星受信アンテナ１３６８Ａ、アンテナ制御ユニット１３６９、及び４０Ｗ電圧調整器１３７０が含まれる。衛星放送の電力と信号強度はアンテナ放送の強度とアップリンク機能よりも大きいため、衛星受信アンテナ１３６８Ａは衛星送信アンテナ１３６０Ａよりも小さくなる。

【０４７８】

海洋船の衛星通信では、高高度衛星及び低高度軌道衛星を含む衛星通信の複数の帯域が利用される。例えば、図３２には、Ｋｕバンド衛星アンテナ１３８３Ａ、低高度軌道衛星アンテナ１３８３Ｂと１３８３Ｃを含む複数帯域の通信の使用例が示されている。高高度衛星はアップリンク機能を提供しないか、またはその機能があっても限りがあるが、静止軌道を含め、これにより非常に高い高度から広範囲をカバーできる。マップ１３８４に示されるように、高度が高いため、各衛星がカバーできるエリアはかなり大きくなる。マップ１３８５に示されるように、低高度軌道衛星はカバーできるエリアが小さいためにより多くの衛星が必要となる。そのため、放送エリアをカバーするためのコストが高くなる。船舶の進路によっては、衛星の軌道上の位置に応じて、低高度軌道衛星へのアクセスが断続的になる場合がある。

【０４７９】

Ｋｕバンド衛星アンテナ１３８３Ａは主にテレビと映画コンテンツの配信に使用されるため、通常、ＳＤＮＰセキュリティは必要ない。追跡と位置決めは、アンテナ制御１３８３により実行される。衛星アンテナ１３８３Ａからのマルチチャネルデータは、Ｌバンドマルチスイッチ１３８１に供給され、信号がテレビ受信機とチューナー１３８２にルーティングされる固定ビデオ放送データとデジタルビデオ放送ＤＶＢデータに分離される。ビデオコンテンツは中央通信サーバ１３８０に供給される。しかし、セキュア通信が必要な場合は、Ｋｕバンド衛星アンテナ１３８３ＡをＳＤＮＰソフトウェアの実行に適合できる。

【０４８０】

対応するＳＤＮＰファームウェア１３３５Ｕ及び１３３５Ｖを実行する低高度軌道衛星アンテナ１３８３Ｂ及び１３８３Ｃからのデータの場合、衛星アンテナからの情報がＳＤＮＰソフトウェア１３３５Ｚを実行する中央通信サーバ１３８０に中継される。通信システムでは、土地の範囲内で、ＳＤＮＰファームウェア１３３５Ｎを実行する携帯電話基地局１７によりホストされる４Ｇ／ＬＴＥセルラーネットワーク２５を使用する通信も可能

となる。サーバ１３８０を介した通信は、ＳＤＮＰファームウェア１３３５Ｌを実行するＳＤＮＰ　ＷｉＦｉルータ１３６２により船舶全体に配信される。ＷｉＦｉアクセスポイント２６のＷｉＦｉホットスポット通信は、ＷｉＦｉアンテナ１３６１により船舶全体に配信される。ＳＤＮＰアプリ１３３５を実行する携帯電話３２などのＳＤＮＰクライアントとの通信により、エンドツーエンドのハイパーセキュア通信が容易化される。ＳＤＮＰクライアントとして有効化されていないデバイスは、ＷＡＰ、ＡｌｌＪｏｙｎ、または他のセキュリティプロトコルを使用するＩＤペアリングに依存する必要がある。

【０４８１】

図３３には、高速列車に適用されるマルチバンド通信のアプリケーションが示されている。示されるように、ＳＤＮＰゲートウェイ１２０１Ａに接続されたＳＤＮＰソフトウェア１３３５Ｚを実行する列車データセンターサーバ１３８０から、衛星マイクロ波９５Ｂ、４００ＭＨｚ無線１３７２、及び６０ＧｈｚマイクロＷ波１３７３を含む複数ＰＨＹ接続を介して、高速列車１３６０Ｃへ通信が行われる。ＳＤＮＰ通信中、ＳＤＮＰデータセンター１３８０から、ＳＤＮＰファームウェア１３３５Ｄを実行する衛星アンテナ９２Ｃを介して、ＳＤＮＰファームウェア１３３５Ｐを実行する衛星９３にデータが中継される。衛星から、ＳＤＮＰソフトウェア１３３５Ｙを実行するサーバ１３６１に接続された列車アンテナアレイ１３８３Ｖへ通信が行われる。ＳＤＮＰデータセンター１３８０から、列車の線路に沿って一定間隔で配置された４００ＭＨｚアンテナ１３８１または６０ＧＨｚアンテナ１３８２を介して、代替の通信が行われる。また、これらの衛星から、ＳＤＮＰソフトウェア１３３５Ｙを実行する列車通信ＳＤＮＰサーバ１３６１に接続されたアンテナアレイ１３８３Ｂへ通信が行われる。次に、ＳＤＮＰサーバ１３６１で受信された通信は、ＷｉＦｉブリッジ１３３５Ｚによって列車全体に配信され、ＷｉＦｉホットスポットとしてクライアントに配信される。

【０４８２】

自動車及び業務トラック輸送における通信機能は多面的で、以下が含まれる。

・音声通信
・ナビゲーション、マップ、道路情報、アラート
・エンターテイメント、ホットスポットサービス、インフォテインメント
・ワイヤレス支払、通行料
・救急サービス、けん引車サービス
・衝突回避
・発車係のスケジューリング（プロフェッショナル、ライドシェアリング）

【０４８３】

自動運転車、すなわち無人運転には追加機能が必要である。主に「テレマティックス」モジュールと呼ばれるＣＤＭＡ（２．５Ｇ）制御中央ユニットなどの旧式のセルラーネットワークに基づくと、既存の自動車システムは、ハッキング、サイバー攻撃、及びプライバシー攻撃を受けやすいことが分かっている。この脆弱性を排除するには、多額の費用をかけずにネットワーク全体を保護する必要がある。すなわち、財政的に、新しいネットワークをインストールするという選択肢はない。代わりに、セキュリティ方法はレイヤ３からレイヤ７に展開されるため、セキュリティインフラストラクチャをハードウェアネットワークに重ねる必要がある。この戦略は、本明細書に開示されるＳＤＮＰラストマイルの実装に適合する。

【０４８４】

図３４には、車両とＳＤＮＰクラウド間の典型的なハイパーセキュアラストマイル接続が示されている。以前のラストマイル接続と同様に、ラストマイル全体でパケットの転送に関係する特定のデータキャリアは、場所によって著しく異なる場合がある。そのため、図には、関係するデータキャリアに関係なく、ハイパーセキュア通信を表す例が示されている。示されるように、ネットワークサービスプロバイダ（ＮＳＰ）が管理する有線またはファイバリンク２４を介して、ネットワークルータ６７Ａに接続されるＳＤＮＰゲートウェイ１２０１Ａで、ＳＤＮＰデータグラムＡを含むデータパケット１２２２Ａが、ＳＤ

ＮＰペイロードを含むＩＰデータグラムＢで構成されるデータパケット１２２３Ａに変換される。次に、ネットワークルータ６７Ａから、モバイルネットワークオペレータ（ＭＮＯ）が所有または運営する有線またはファイバリンク２４Ａを介して、ＩＰネットワークグラムＢがデータパケット１２２３Ｂとして、携帯電話基地局１７にルーティングされる。そして、セルラーネットワーク２５経由で、地域のモバイルネットワークオペレータに応じて２．５Ｇ、３Ｇ、３．５Ｇ、４Ｇ／ＬＴＥのいずれかでセルラーリンク２８が使用され、ＳＤＮＰペイロードを含むＳＤＮＰデータグラムＢで構成されるデータパケット１２２３Ｃとして、ＩＰデータパケットＢから自動車１３９０Ａのテレマティックスモジュールへ通信が行われる。その後、テレマティックスモジュール内で動作するＳＤＮＰファームウェア１３３５Ｆにより、着信データパケット１２２３Ｃに埋め込まれたＳＤＮＰペイロードが解釈され、ハイパーセキュア通信リンクが完成する。そのため、自動車のセルラーラストリンクは、ハイパーセキュアラストマイル通信の一部として機能する。

【０４８５】

図３５に示されるように、自動車１３９０Ａのテレマティックスモジュールで、インフォテインメントインターフェイス１３７７によって制御される様々な機能のためにセキュアな情報が利用される。また、内蔵ＷｉＦｉホットスポット１３６２Ｄからも、それぞれＩＰデータグラムＢとＩＰデータグラムＣを含むデータパケット１２２３Ｂと１２２３Ｃが配信される。ＩＰデータグラムＢには、ＳＤＮＰアプリ１３３５を実行する携帯電話３２Ｂなどの任意のＳＤＮＰクライアントへのエンドツーエンドのハイパーセキュア通信を容易化するＳＤＮＰペイロードが含まれる。従来型のＩＰペイロードのみが使用されるＩＰデータグラムＣは安全性が低くなるが、携帯電話３２Ａ及びタブレット３３Ａなど、ＳＤＮＰクライアントとして動作しないデバイスで動作する。ＩＤペアリングを使用して、ＷＰＡ、ＡｌｌＪｏｙｎ、または他のプロトコルにより、非ＳＤＮＰデバイスのラストリンクセキュリティを改善できる。

【０４８６】

自動車通信におけるもう１つの重要な機能として、Ｖ２Ｖ通信とも呼ばれる車車間通信の機能が挙げられる。Ｖ２Ｖ通信の目的は、主に衝突回避である。しかし、本明細書に開示されるＳＤＮＰ方法に従うと、Ｖ２Ｖ通信はハイパーセキュアアドホックピアツーピアネットワークとして機能させることもできる。図３６には、車車間ＳＤＮＰ通信が示されている。この図では、ＳＤＮＰファームウェア１３３５Ｆを実行する自動車１３９０Ａ、１３９０Ｂ、及び１３９０Ｃで、相互及びＳＤＮＰゲートウェイ１２０１Ａに接続された携帯電話基地局１７とのピアツーピアネットワークが形成される。車車間通信は、ＩＰデータグラムまたはＳＤＮＰデータグラムのいずれかを使用して実行できる。

【０４８７】

ＳＮＰクライアントまたはゲートウェイから非ＳＤＮＰデバイスへ通信が行われる場合、通信はＩＰデータグラムを使用して行われる。例えば、ＳＤＮＰゲートウェイ１２０１Ａで、ＳＤＮＰペイロードを含むＳＤＮＰデータグラムＡが、埋め込まれたＳＤＮＰペイロードを含むＩＰデータグラムＢで構成されるデータパケット１２２３Ａに変換される。示されるように、２．５Ｇまたは３Ｇのセルラーリンク２８Ａ経由で、埋め込まれたＳＤＮＰペイロードを含むＩＰデータグラムＢで構成されるデータパケット１２２３Ｂが使用され、携帯電話基地局１７から自動車１３９０Ａへ通信が行われるが、同じく埋め込まれたＳＤＮＰペイロードを含むＩＰデータグラムＢで構成されるデータパケット１２２３Ｃが使用されて、３．５Ｇまたは４Ｇ／ＬＴＥのセルラーリンク２８Ｂ経由で、自動車１３９０Ｃへ通信が行われる場合もある。このように、ＳＤＮＰペイロードは、データパケットの伝送に使用されるネットワークとは無関係に配信される。

【０４８８】

ＳＤＮＰファームウェア１３３５Ｆが有効化されている自動車では、アドホックピアツーピアＳＤＮＰブリッジまたはブリッジネットワークが形成される場合がある。例えば、ＩＰデータグラムではなく、ＳＤＮＰデータグラムＣを含むデータパケット１２２２Ｂが使用されて、Ｖ２Ｖ無線リンク１３９１Ａ経由で、自動車１３９０Ａから自動車１３９０

Ｂへ通信が行われる。同様に、Ｖ２Ｖ無線リンク１３９１Ｂ経由で、ＳＤＮＰデータグラムＤを含むデータパケット１２２２Ｃが使用されて、自動車１３９０Ｂから自動車１３９０Ｃへ通信が行われる。これはＩＰデータグラムに依存しない。使用されるデータグラムの種類に関係なく、埋め込まれたコンテンツは、ＳＤＮＰペイロードを使用するハイパーセキュアのままとなる。

【０４８９】

ＳＤＮＰアドホックＶ２Ｖネットワークのもう１つの機能として、トンネリング機能を実行する能力が挙げられる。すなわち、車車間を通過するデータが監視または解釈されないようにデータを渡すことができる。自動車１３９０Ｃが範囲外であるためにセルラーリンク２８Ｂに障害が発生した場合は、代替パスとして、携帯電話基地局１７でＳＤＮＰブリッジネットワークが利用され、セルラーリンク２８Ａ、Ｖ２Ｖ無線リンク１３９１Ａ、最後にＶ２Ｖ無線リンク１３９１Ｂを介して同じ発信者に接続される。データ転送中、データパケット１２２３Ｂ、１２２２Ｂ、及び１２２２Ｃは、ＩＰデータグラムＢからＳＤＮＰデータグラムＣに、そして最終的にＳＤＮＰデータグラムＤに変更される。自動車１３９０Ｃを意図したＳＤＮＰペイロードは宛先自動車用に一意に作成されているため、自動車１３９０Ｂとそのドライバーは、アドホックネットワークを介してデータパケット１２２２Ｂが中継されていても、ＳＤＮＰデータグラムＣのコンテンツをハッキングまたは監視することができない。

【０４９０】

従来型のラストマイル通信とは別に、同じＳＤＮＰブリッジ技術を使用して、ハイパーセキュリティを用いて長距離、すなわちデジタルトランク通信で大量のデータを送信できる。図３７には、こうした例が３つ示されている。すなわち、マイクロ波トランク９８、ファイバトランク９０、及び衛星トランク９５Ａと９５Ｂである。この機能はＳＤＮＰクラウドの一部と見なすことができるが、単一のデータルートがラストマイル通信のルートに似ているため、ハイパーセキュリティを保証するために同様の方法を採用している。例えば、ＳＤＮＰファームウェア１３３５Ｗを実行するマイクロ波タワー９６Ａと９６Ｂを介したマイクロ波トランク９８経由で、ＳＤＮＰデータグラムを含むデータパケット１２２２を使用して、ＳＤＮＰソフトウェア１３３５Ｚを実行するサーバ２１Ａと２１Ｂから通信を行うことができる。また、ファイバトランク９８経由で、ＳＤＮＰデータグラムを含むデータパケット１２２２を使用して、サーバ２１Ａと２１Ｂから直接通信を行うこともできる。グローバル通信（例えば、太平洋を横断するデータリンク）では、両方ともＳＤＮＰファームウェア１３３５Ｕを実行する地球基地の衛星アンテナ９２Ａと９２Ｂを使用して、マイクロ波衛星トランク９５Ａと９５Ｂにより、サーバ２１Ａと２１Ｂから、ＳＤＮＰファームウェア１３３５Ｖを実行する衛星９３に通信を行うことができる。ファイバとマイクロ波タワーの例のように、衛星トランク通信では、ＳＤＮＰデータグラムを含むデータパケット１２２２が利用される。

【０４９１】

結論として、ラストマイル通信で提供されるセキュリティ及びプライバシー機能は、２つの通信デバイスに依存しているということが挙げられる。図３８は、４つの異なる組み合わせを対比したものである。下から上へとセキュリティとプライバシーが向上する。それぞれで、（ｉ）セキュリティ：コミュニケへの不正アクセスを防止する能力、（ｉｉ）ＩＤ検証：ユーザを認証し、ＩＤに基づいてアクセスと特権を調整する能力、及び（ｉｉｉ）匿名性：監視から発信者のＩＤを隠す能力という３つの要素が考慮されている。

【０４９２】

最下部の例では、スニッフィング可能なＩＰアドレスとＩＰペイロードを有するＩＰデータグラムを含むデータパケット１２２３Ｃが使用され、ＳＤＮＰゲートウェイ１３９５から、セキュリティ対策を全く欠く非ＳＤＮＰクライアントへオープンに通信が行われる。そのため、ラストマイル接続はセキュアでもプライベートでもない。下から２番目の例では、ＳＤＮＰゲートウェイ１３９５から、デバイス認証及びＩＤペアリング機能を提供する非ＳＤＮＰクライアントへ通信が行われる。この通信では、スニッフィング可能なＩ

ＰアドレスをＩＰデータグラムを含むデータパケット１２２３Ｂが用いられるが、ＩＤペアのデバイスのみで復号化が可能となる暗号文を含む暗号化されたペイロードが使用される。通信はプライベートではなく、匿名性もないが、少なくとも限られた期間はセキュリティが強化される。

【０４９３】

上から２番目の例では、データパケット１２２３ＡにＩＰデータグラム内のＳＤＮＰペイロードが含まれる場合は、任意のブリッジまたはルータ１３９７を介して、ＳＤＮＰゲートウェイ１３９５から通信がルーティングされることで、ハイパーセキュリティが実現できる。達成されるセキュリティのレベルは、ルータではなくエンドデバイスのみに依存する。最上部の例の場合、ＳＤＮＰアドレス指定を有するＳＤＮＰデータグラムを含むデータパケット１２２２、すなわちインターネットＤＮＳネームサーバで認識されない送信元アドレスと宛先アドレス、及びＳＤＮＰセキュアペイロードを使用して行われるＳＤＮＰゲートウェイ１３９５とＳＤＮＰクライアント１３９６間の通信は、優れたセキュリティ、完全なプライバシー条件、及び匿名パケットルーティングを備えたハイパーセキュア通信となる。

【０４９４】

ハイパーセキュアラストマイルのパケットルーティング

【０４９５】

使用されるレイヤ１物理ハードウェア及びレイヤ２データリンクのアルゴリズムと方式に関係なく、ＳＤＮＰクライアントまたはＳＤＮＰブリッジとＳＤＮＰゲートウェイ間のパケットルーティングは、ＩＰデータグラムに依存して、ラストマイル全体にデータパケットが伝送及びルーティングされる。ＳＤＮＰシグナリングサーバからの指示によるＳＤＮＰクラウド内のデータルーティングとは異なり、ＳＤＮＰクラウドまたはそのシグナリングサーバで、ラストマイルを通過するＩＰデータグラムが制御されることはない。そのため、ラストマイルでの伝播遅延には多少のばらつきが予想される。幸いラストマイル通信の距離と可能なルート数が制限されているため、グローバル通信のエンドツーエンドの総伝播遅延に比べると、この不確実性はそれほど高くない。ラストマイルの変化性による総伝播遅延のはらつきは、総遅延の１０％未満であると推定される。

【０４９６】

図３９には、固定ＩＰアドレスが使用されるＳＤＮＰクライアント１４００とＳＤＮＰゲートウェイ１４０１間のシングルルートラストマイル通信が示されている。ＩＰデータグラム１４０５には、$M_{0,0}$（ＳＤＮＰゲートウェイ）の宛先ＩＰアドレス、及びデータパケットの$C_{1,1}$の送信元ＩＰアドレス、すなわちＳＤＮＰクライアントが含まれる。ラストリンク通信は、ルータ１４０２Ａへのシングルルート１４０４として行われる。データは、任意の数のルータＲを介してルーティングされる（例えば、ルータ１４０２Ｂから$M_{0,0}$へ）。

【０４９７】

ラストマイルネットワーク接続の代替の表し方として、ＰＨＹ、データリンク、及びネットワーク接続をＯＳＩレイヤ１、２、３として表すＩＰスタックとして各通信デバイスを示すことができる。例えば、図４０Ａは、静的ＩＰアドレスが使用されるシングルルートラストマイルハイパーセキュア通信のＩＰスタック図である。このように、ＷｉＦｉルータを含むルータ１４０２Ａ及びイーサネット（登録商標）ルータである１４０２Ｂを介して、ＳＤＮＰクライアント$C_{1,1}$を含むクライアントデバイスから、ＳＤＮＰゲートウェイ$M_{0,0}$を含むＳＤＮＰゲートウェイ１４０１へのシングルルートラストマイル接続１４０９が確立される。クライアントデバイス１４００が、ラストリンク１４０４を介してルータ１４０２Ａに接続される。ここでは、クライアントＩＰスタック１４１１のＰＨＹレイヤ１物理接続及び対応するデータリンクレイヤ２が、ルータＩＰスタック１４１２Ａの対応するレイヤ１とレイヤ２に接続される。

【０４９８】

次に、ルータ１４０２Ａが、イーサネット（登録商標）経由でルータ１４０２Ｂに接続

される。ここでは、ＷｉＦｉルータのＩＰスタック１４１２ＡのＰＨＹレイヤ１物理接続と対応するデータリンクレイヤ２が、イーサネット（登録商標）ルータＩＰスタック１４１２Ｂの対応するレイヤ１とレイヤ２に接続される。最後に、ルータ１４０２Ｂが、イーサネット（登録商標）経由でＳＤＮＰゲートウェイサーバ１４０１に接続される。ここでは、イーサネット（登録商標）ルータのＩＰスタック１４１２ＢのＰＨＹレイヤ１物理接続と対応するデータリンクレイヤ２が、ゲートウェイのＩＰスタック１４２２の対応するレイヤ１とレイヤ２に接続される。動作中、妨害されずにルータからデータが伝送されるように、ネットワークレイヤ３　ＩＰデータグラムは、透過的に１つのＩＰスタックから別のＩＰスタックへ、具体的にはＩＰスタック１４１１のレイヤ３から１４１２Ａへ、次に１４１２Ｂへ、最後に１４２２へと流れる。このように、データが物理的に複数のデバイスを通過する場合でも、ネットワークではＩＰデータグラムがシングルルートデータとして仮想ラストマイル接続１４０９により伝送される。

【０４９９】

言い換えると、レイヤ３ネットワークデータは、ＩＰデータグラムの伝送に使用される物理接続とは無関係にラストマイルを流れる。すなわち、レイヤ３ラストマイル通信は、データ転送に使用される基礎のレイヤ１とレイヤ２の実装には不可知的に動作する。この原則は、図４０Ｂの概略図のように、中間ノードを削除して簡略化された形式で表すことができる。これには、ＩＰスタック１４１１と対応するコンピューティング＆データストレージ機能１４１０の間、ＩＰスタック１４２２と対応するコンピューティング＆データストレージ機能１４２１の間で行われるデータ転送の通信をそれぞれに含むクライアントデバイス１４００とＳＤＮＰゲートウェイサーバ１４０１が含まれる。データパケット配信プロセスで使用される媒体またはルータの数に関係なく、ＩＰデータグラム１４０５はラストマイル接続１４０９を流れる。したがって、ラストマイルは「データ構造」、すなわちＩＰデータグラムがデバイス間で転送されるあらゆる物理的手段を意味する抽象概念と見なすことができる。しかし、発信者の接続デバイスには、確立できない通信リンクのアップストリームルータに接続できる能力が必要であるため、ラストリンクには物理的な意味がある。例えば、ＷｉＦｉ接続機能のみを備えたタブレットコンピュータを使用する発信者がＷｉＦｉを使えるカフェにいて、発信者がＷｉＦｉネットワークへのＷＰＡパスワードを持っていない場合はラストリンクを確立できず、発信者はラストマイルであるＳＤＮＰクラウドに接続することができない。または、コールを発信することができない。

【０５００】

ラストマイル通信におけるもう１つの考慮事項として、ＩＰデータグラム１４０５のペイロードに、トランスポートレイヤ４データ、セッションレイヤ５データ、プレゼンテーションレイヤ６データ、アプリケーションレイヤ７データなど、上位のＯＳＩレイヤ全ての情報が含まれることが挙げられる。ＵＤＰまたはＴＣＰ転送プロトコルの選択に必要なレイヤ４データを除き、ＩＰデータグラムのペイロードに含まれる残りのデータは、開示されるＳＤＮＰ通信に固有であり、自体がＳＤＮＰソフトウェアまたはファームウェアを実行しない限り、ラストマイルに沿って動作するルータでは解釈されない。したがって、ラストマイルネットワーク自体が様々なデバイス、キャリア、及びネットワークオペレータの組み合わせで構成される場合でも、エンドデバイス、すなわち発信者またはＳＤＮＰクライアント及びＳＤＮＰゲートウェイでのみラストマイル通信が解釈される。

【０５０１】

ＳＤＮＰペイロードはスクランブル化、断片化、ジャンクデータの挿入と除去、ステート依存のフォーマット、及び動的暗号化を含む多数の秘密により保護されているが、ラストマイルネットワークを通過するＩＰデータグラムのＩＰアドレスでは、必然的にクライアントデバイス１４００及びＳＤＮＰゲートウェイサーバ１４０１の送信元アドレスと宛先アドレスが明かされる。ラストマイルにある程度の匿名性を提供するには、アドレス偽装が有益である。すなわち、ＩＰデータグラムの送信元アドレスと宛先アドレスを動的に変更することで、サイバー攻撃者を誤った方向に誘導できる。ＩＰ偽装は、発信者の接続デバイスのＩＰアドレスを動的に変更すること（本明細書では「動的クライアントアドレ

ス指定」と呼ぶ）、または複数のＳＤＮＰゲートウェイと通信すること、すなわちマルチルートラストマイル通信により実現できる。

【０５０２】

説明されるＩＰアドレス偽装の最初の方法には、順次データパケットの送信元アドレスを動的に変更することが含まれる。図４１に示されるように、連続して送信されるＩＰデータグラムＡ、Ｂ、及びＣは、３つの異なる送信元アドレスで構成される。具体的には、ＩＰデータグラムＡ　１４０５Ａには送信元ＩＰアドレス$C_{1,1}$、ＩＰデータグラムＢ　１４０５Ｂには送信元ＩＰアドレス$C_{1,2}$、ＩＰデータグラムＣ　１４０５Ｃには送信元ＩＰアドレス$C_{1,3}$が含まれる。したがって、ルータ１４０２Ａに入るパケットは全てＳＤＮＰクライアント１４００から発せられるが、クライアントの送信元アドレス$C_{1,n}$は動的に変化するため、実際のＩＰアドレスが難読化され、複数の通信デバイスのように見える。この「見せかけ」を完成させるには、動的送信元アドレスに対応するように、通信デバイスのＭＡＣアドレスも変更する必要がある。

【０５０３】

この方法は、ＩＰスタックを使用して、図４２Ａに示されている。この図では、ＷｉＦｉとイーサネット（登録商標）が使用され、デバイス１４００、１４０２Ａ、１４０２Ｂ、１４０１から、対応するＩＰスタック１４１１Ｎ、１４１２Ａ、１４１２Ｂ、１４２２を介して通信が行われるが、ＳＤＮＰクライアントのネットワークレイヤ３　ＩＤに$C_{1,1}$、$C_{1,2}$、$C_{1,3}$という複数のＩＰアドレスが含まれる。その結果、図４２Ｂのラストリンクの概略図に示されるように、ルータ１４０２Ａに入る順次データパケットは、１つのデバイスではなく、３つの異なるクライアントデバイスから送信されたように見える。共有ＰＨＹレイヤはＷｉＦｉの標準周波数で構成され、デバイスを接続するデータリンクレイヤは８０２．１１ａｃまたは８０２．１１ｎなどの確立された規格に従う。

【０５０４】

ネットワーク接続１４０８に沿ってルータデバイス１４０２Ａに送信されるＩＰデータグラム１４０５Ｎは、固定宛先ＩＰアドレスＩＰ　$M_{0,0}$及び順次送信元アドレスＩＰ　$C_{1,1}$、ＩＰ　$C_{1,2}$、ＩＰ　$C_{1,3}$などで構成される。これは、ｎ＝１，２，３とするＩＰ　$C_{1,n}$の数学表記で表したもので、これにより各順次パケットが一意に識別される。各順次ＩＰパケットには、対応するペイロードＳＤＮＰ　１、ＳＤＮＰ　２、ＳＤＮＰ３なども含まれる。この説明では、数学的な略記法「ＩＰ　$C_{1,n}$」を使用して各ＩＰアドレスを参照しているが、ＩＰアドレスはＩＰｖ４またはＩＰｖ６の国際規格に従って作成された実際のＩＰアドレスで構成され、予約済みのＩＰアドレスは除外されていることに注意されたい。

【０５０５】

セキュリティを強化するもう１つのオプションとして、ラストマイルでマルチルートパケット転送を使用する方法が挙げられる。ＳＤＮＰクラウド内のデータ転送と同様の方法で、マルチルートラストマイル通信では、オーディオと順次データがパース及び断片化されてから個別のパケットに分割され、異なるＳＤＮＰゲートウェイにアドレス指定される。図４３には、静的ＩＰアドレスが使用されるマルチルートデータ転送の例が示されている。この図では、ＳＤＮＰクライアント１４００から、複数のゲートウェイ１４０１Ａ、１４０１Ｂ、及び１４０１Ｃへ通信が行われる。示されるように、最初のデータパケット１４０５Ａは、送信元ＩＰアドレス$C_{1,1}$及び宛先アドレス$M_{0,0}$を含むペイロードＳＤＮＰ１で構成される。データパケット１４０５Ａは、ルータ１４０２Ａ及び１４０２Ｂを介して、ラストリンク１４０４Ａ経由でＳＤＮＰゲートウェイ１４０１Ａにルーティングされる。同様に、２つ目のデータパケット１４０５Ｂは、送信元ＩＰアドレス$C_{1,1}$及び宛先アドレス$M_{0,1}$を含むペイロードＳＤＮＰ　２で構成される。データパケット１４０５Ｂは、ルータ１４０２Ｃを介して、ラストリンク１４０４Ｂ経由でＳＤＮＰゲートウェイ１４０１Ｂにルーティングされる。３つ目のデータパケット１４０５Ｃは、送信元ＩＰアドレス$C_{1,1}$及び宛先アドレス$M_{0,3}$を含むペイロードＳＤＮＰ３で構成される。データパケット１４０５Ｃは、ルータ１４０２Ｄ及び１４０２Ｅを介して、ラストリンク

１４０４Ｃ経由でＳＤＮＰゲートウェイ１４０１Ｃにルーティングされる。

【０５０６】

クライアントデバイス１４００と示される３つのゲートウェイ１４０１Ａ、１４０１Ｂ、１４０１Ｃのいずれかとの間のパスで、ＩＰデータグラムは複数のラストリンク１４０４Ａ、１４０４Ｂ、１４０４Ｃを介して、複数のルータ１４０２Ａ、１４０２Ｂ、１４０２Ｃにルーティングされる。これらのルータには、（ｉ）ＷｉＦｉまたはイーサネット（登録商標）など、同一の物理媒体が使用される完全に独立したルータ、（ｉｉ）ＤＯＣＳＩＳ３ケーブルモデムの複数のトレリスチャネルなど、共通のハードウェアデバイスの複数のルータチャネル、または（ｉｉｉ）例えば１つはＷｉＦｉ経由、もう１つは３Ｇ経由など、通信に使用される異なる物理媒体が含まれ得る。

【０５０７】

例えば、図４４Ａは、共通のＰＨＹラストリンク１４０４経由で、静的ＩＰアドレスが使用されるマルチルートラストマイルハイパーセキュア通信のＩＰスタック図である。動作中、共通のＰＨＹ、データリンク、及びネットワークレイヤが使用され、単一のデバイス接続として、ＳＤＮＰクライアント$C_{1,1}$からルータ１４０１Ａ、１４０２Ｂ、及び１４０２Ｃへ通信が行われる。アドレス偽装は、静的クライアントアドレスＩＰ　$C_{1,1}$を含む連続したＩＰデータグラムを使用して実行されるが、ＳＤＮＰゲートウェイアドレスＩＰ　$M_{0,0}$、ＩＰ　$M_{0,1}$、及びＩＰ　$M_{0,3}$が変更される。パケットのミスダイレクションは、アルゴリズム的またはランダムに行うことができる。例えば、クライアントデバイス１４００から送信されるデータグラム１０個目ごとにそれをＳＤＮＰサーバ１４０１Ｃに送信し、クライアントデバイス１４００からの１０個目の送信データグラムに宛先アドレスＩＰ　$M_{0,3}$及び送信元ＩＰアドレスＩＰ　$C_{1,1}$を含めることができる。ＳＤＮＰゲートウェイサーバ１４０１Ｃからの返信は、リバースパスで、すなわち送信元ＩＰアドレスＩＰ　$M_{0,3}$及び宛先アドレスＩＰ　$C_{1,1}$で、クライアントデバイス１４００に返される。

【０５０８】

示されるように、クライアントデバイス１４００とルータ１４０２Ａ、１４０２Ｄ、１４０２Ｃとの間のＰＨＹ及びデータリンクは、例えばＷｉＦｉなどの単一の媒体で構成される。ラストリンク接続は３つに分かれる単一の線として表されるが、物理接続は全て、並列配線を作成するために使用される電気的なＹコネクタではなく、ポイントツーポイントで行われることを理解する必要がある。代わりに、図の接続は接続の効果を示すことを意味するものである。すなわち、クライアントＩＰスタック１４１１のＰＨＹレイヤから、１つのＰＨＹ接続が３つに拡張される。つまり、ＩＰスタック１４１２Ａ、１４１２Ｃ、及び１４１２ＤのＰＨＹレイヤに接続される。機能的には、このラストリンクは３つの入力拡張機構への単一の出力として動作する。ここでは、ルータ機能が１つの共通の電子機器に含まれているか、個別のルータに分割されているかに関係なく、１つのクライアントが３つのルータ機能に接続される。示されるように、ラストリンク１４０４は、ケーブル、ファイバ、ＷｉＦｉ、イーサネット（登録商標）、セルラーのいずれかの単一タイプの通信媒体で構成されることに注意されたい。

【０５０９】

しかし、ラストマイルの残りの部分は、ラストリンクと同じであるとは限らず、任意の媒体で構成される。代替のラストリンクには、独立したルータに接続される複数の異なるＰＨＹレイヤが含まれる。こうした実装が図４４Ｂに示されている。図には、複数ＰＨＹのラストリンク経由で、静的ＩＰアドレスを使用してマルチルートラストマイルハイパーセキュア通信を実行するＩＰスタックが示されている。具体的には、クライアントデバイス１４００は静的クライアントアドレスＩＰ　$C_{1,1}$の共通ネットワークレイヤ３インターフェイスを使用して動作するが、ＩＰスタック１４１１Ａ、１４１１Ｂ、及び１４１１Ｃとして表される個別のレイヤ１及びレイヤ２インターフェイスが使用される。動作中、ＩＰスタック１４１１Ａはラストリンク１４０４Ａを介してルータ１４０２Ａに接続され、送信元アドレスＩＰ　$C_{1,1}$及び宛先アドレスＩＰ　$M_{0,0}$を含むＩＰデータグラム

がルータ１４０２Ｂまで伝送される。同様に、ＩＰスタック１４１１Ｂはラストリンク１４０４Ｂを介してルータ１４０２Ｃに接続され、送信元アドレスＩＰ　$C_{1,1}$及び宛先アドレスＩＰ　$M_{0,1}$を含むＩＰデータグラムが伝送される。ＩＰスタック１４１１Ｃはラストリンク１４０４Ｃを介してルータ１４０２Ｄに接続され、送信元アドレスＩＰ　$C_{1,1}$及び宛先アドレスＩＰ　$M_{0,3}$を含むＩＰデータグラムがルータ１４０２Ｅまで伝送される。

【０５１０】

動的送信元アドレス指定とマルチルートデータ転送の組み合わせが図４５に示されている。この図では、動的送信元アドレスが使用され、ＳＤＮＰクライアント１４００から複数のゲートウェイ１４０１Ａ、１４０１Ｂ、及び１４０１Ｃへ通信が行われる。このように、最初のデータパケット１４０５Ａは、動的な送信元ＩＰアドレス$C_{1,1}$及び宛先アドレス$M_{0,0}$を含むペイロードＳＤＮＰ１で構成される。データパケット１４０５Ａは、ルータ１４０２Ａ及び１４０２Ｂを介して、ラストリンク１４０４Ａ経由でＳＤＮＰゲートウェイ１４０１Ａにルーティングされる。同様に、２つ目のデータパケット１４０５Ｂは、動的な送信元ＩＰアドレス$C_{1,2}$及び宛先アドレス$M_{0,1}$を含むペイロードＳＤＮＰ２で構成される。データパケット１４０５Ｂは、ルータ１４０２Ｃを介して、ラストリンク１４０４Ｂ経由でＳＤＮＰゲートウェイ１４０１Ｂにルーティングされる。３つ目のデータパケット１４０５Ｃは、動的な送信元ＩＰアドレス$C_{1,3}$及び宛先アドレス$M_{0,3}$を含むペイロードＳＤＮＰ３で構成される。データパケット１４０５Ｃは、ルータ１４０２Ｄ及び１４０２Ｅを介して、ラストリンク１４０４Ｃ経由でＳＤＮＰゲートウェイ１４０１Ｃにルーティングされる。

【０５１１】

そのため、連続する各データパケットには変化するＳＤＮＰペイロードが含まれ、動的に変化する送信先アドレスが使用されて、各データパケットが異なるラストリンクを介して一意のＳＤＮＰゲートウェイにルーティングされる。複数のラストリンク、すなわちラストリンク１４０４Ａ、１４０４Ｂ、及び１４０４Ｃ経由でデータを転送するには、トレリスエンコーディングを備えたＤＯＣＳＩＳ３ケーブルモデムなど、複数のＩＰ入力を有する単一のルータか、複数の帯域のＷｉＦｉ、または無線とＷｉＦｉの組み合わせ、あるいは有線とワイヤレス通信の他の組み合わせなど、複数の形式の媒体を使用する。一例として、図４６Ａに、シングルＰＨＹラストリンク１４０４経由で、動的クライアントＩＰアドレスが使用されるマルチルートラストマイルハイパーセキュア通信のＩＰスタックが示されている。クライアントデバイス１４００は、ＩＰスタック１４１１Ａに示されるようなレイヤ１とレイヤ２通信を含む共有物理インターフェイスを示している。ネットワークレイヤ３については、ＩＰスタック１４１１ＡでＳＤＭＰゲートウェイ$M_{0,0}$に宛てられたクライアントアドレス$C_{1,1}$、ＩＰスタック１４１１ＢでＳＤＭＰゲートウェイ$M_{0,1}$に宛てられたクライアントアドレス$C_{1,2}$、ＩＰスタック１４１１ＣでＳＤＭＰゲートウェイ$M_{0,3}$に宛てられたクライアントアドレス$C_{1,3}$が生成される。

【０５１２】

図４６ＢのＩＰスタック図に示されるように、同じマルチルートアプローチを、動的クライアントアドレス指定及び複数ＰＨＹの最終レイヤと組み合わせることができる。示されるように、クライアントデバイス１４００には、ＩＰアドレスＩＰ　$M_{0,0}$、ＩＰ　$M_{0,1}$、ＩＰ　$M_{0,3}$を有するＳＤＮＰゲートウェイに対して、対応するラストリンク１４０４Ａ、１４０４Ｂ、１４０４Ｃ経由で、対応するＩＰアドレスＩＰ　$C_{1,1}$、ＩＰ　$C_{1,2}$、ＩＰ　$C_{1,3}$を有するＩＰデータグラムを伝送する３つのＩＰスタック１４１１Ａ、１４１１Ｂ、１４１１Ｃが含まれる。

【０５１３】

多くの場合、ラストリンクは、最初のルータ以降はマルチルートデータ転送が使用される単一のルートで構成される。図４７では、ラストリンク１４０４を介して、ＳＤＮＰクライアント１４００から単一のルータ１４０２Ａへ通信が行われる。ルータ１４０２Ａ以降は、動的送信元アドレスが使用され、データパケットが複数のゲートウェイ１４０１Ａ

、１４０１Ｂ、及び１４０１Ｃに伝送される。この実装では、最初のデータパケット１４０５Ａは、動的な送信元ＩＰアドレス$C_{1,1}$及び宛先アドレス$M_{0,0}$を含むペイロードＳＤＮＰ１で構成される。データパケット１４０５Ａは、ルータ１４０２Ａ及び１４０２Ｂを介して、ラストリンク１４０４経由でＳＤＮＰゲートウェイ１４０１Ａにルーティングされる。

【０５１４】

同様に、２つ目のデータパケット１４０５Ｂは、動的な送信元ＩＰアドレス$C_{1,2}$及び宛先アドレス$M_{0,1}$を含むペイロードＳＤＮＰ　２で構成される。データパケット１４０５Ｂは、ルータ１４０２Ａ及び１４０２Ｃを介して、ラストリンク１４０４経由でＳＤＮＰゲートウェイ１４０１Ｂにルーティングされる。３つ目のデータパケット１４０５Ｃは、動的な送信元ＩＰアドレス$C_{1,3}$及び宛先アドレス$M_{0,3}$を含むペイロードＳＤＮＰ３で構成される。データパケット１４０５Ｃは、ルータ１４０２Ａ、１４０２Ｄ、及び１４０２Ｅを介して、ラストリンク１４０１経由でＳＤＮＰゲートウェイ１４０１Ｃに連続的にルーティングされる。そのため、連続する各データパケットには変化するＳＤＮＰペイロードが含まれ、動的に変化する送信先アドレスが使用されて、各データパケットが共通のラストリンクを介して一意のＳＤＮＰゲートウェイにルーティングされる。

【０５１５】

このラストマイル接続は、ＩＰスタックを使用して、図４８に示されている。この図では、ルータ１４０２Ａのみにつながるラストリンク１４０４を有するＳＤＮＰクライアントデバイス１４００のＩＰスタック１４１１から、ネットワークレイヤ３のデータパケットが、３つの異なるネットワークアドレス、具体的にはＩＰ　$C_{1,1}$、ＩＰ　$C_{1,2}$、ＩＰ　$C_{1,3}$を含むスタック１４１２Ａに送信される。そのため、クライアントデバイス１４００は実際には単一のクライアントで構成されるが、ルータ１４０２Ａでは３つの個別のクライアントとして認識される。ＩＰデータグラムがルータ１４０２Ａに到達すると、ＩＰデータグラムが分割され、異なるルート経由で異なる宛先ゲートウェイに伝送される。例えば、送信元アドレスＩＰ　$C_{1,1}$を有するパケットは、ルータ１４０２Ｂを介して宛先ＩＰ　$M_{0,0}$へ、送信元アドレスＩＰ　$C_{1,2}$を有するパケットはルータ１４０２Ｃを介して宛先ＩＰ　$M_{0,1}$へ、送信元アドレスＩＰ　$C_{1,3}$を有するパケットはルータ１４０２Ｄ及び１４０２Ｅを介して宛先ＩＰ　$M_{0,3}$へルーティングされる。特定の動的クライアントアドレス$C_{1,n}$を有するデータパケットを特定のＳＤＮＰゲートウェイに伝送するルーティングテーブルは、事前に固定することなく、動的に変更できる。ＩＰアドレスをパケットごとに割り当てることができれば、明らかに無関係なデータパケットが実は全て２つの発信者間の単一の断片化された通信の一部であるという事実がさらに難読化される。

【０５１６】

ラストマイルルーティングの物理的実現

【０５１７】

ラストマイルの物理的実現には、イーサネット（登録商標）、ＷｉＦｉ、セルラー、またはＤＯＣＳＩＳ３対応のケーブルとファイバリンクなど、様々な媒体を介した通信が含まれる。使用する媒体に関係なく、ラストマイルにおけるデータパケットのルーティングは、主に以下３つの変数によって制御される。

・通信デバイスの媒体アクセス制御（ＭＡＣ）アドレス
・ＩＰデータグラムの送信先ＩＰアドレス
・ＩＰデータグラムの宛先ＩＰアドレス

【０５１８】

したがって、ラストマイル通信で各ホップを実行するために使用される物理媒体、すなわちレイヤ１及びレイヤ２情報はＭＡＣアドレスにより制御され、クライアントデバイスとＳＤＮＰゲートウェイ、すなわちラストマイルはＩＰアドレスにより識別される。ハイパーセキュア通信で使用されるペイロードは、セキュア動的通信ネットワーク及びプロトコルに従い定義されたプロトコルに従うが、ラストマイルの中間デバイス、すなわちクラ

イアントデバイスとゲートウェイ間のパケットのルート上のルータ及び他のデバイスにはＳＤＮＰ実行可能コードが備わっていないため、こうしたデバイスではＳＤＮＰ機能を実行することができない。したがって、ＳＤＮＰペイロードは、ラストマイルのハイパーセキュアデータパケットのルーティングには影響しない。

【０５１９】

一例として、ラストマイル通信におけるイーサネット（登録商標）の使用が挙げられる。図４９は、ＳＤＮＰラストマイル通信について前述した図９Ｅのイーサネット（登録商標）データパケットを適応させ、ＳＤＮＰペイロードを伝送するイーサネット（登録商標）通信のＩＰｖ４とＩＰｖ６データグラムを図で示したものである。示されるように、レイヤ１イーサネット（登録商標）パケット１８８には、データフレームヘッダ、すなわちプリアンブル１８０、開始フレームデリミタＳＦＤ１８１、及びレイヤ２イーサネット（登録商標）パケット１８９が含まれる。イーサネット（登録商標）パケット１８９には、宛先ＭＡＣアドレス１８２と送信先ＭＡＣアドレス１８３、ＶＬＡＮ実装のためのオプションの８０２．１Ｑタグ１８４、使用されるデータリンクのタイプの指定に使用されるイーサタイプフィールド１８５（イーサネット（登録商標）ＩＩまたはＩＥＥＥ８０２．３に基づく長さ指定）、及びデータリンクパケット全体の３２ビットＣＲＣチェックサムを含むフレームチェック１８６が含まれる。イーサネット（登録商標）パケット１８９には、ＩＰデータグラムのＳＤＮＰコンテンツ１４３０のカプセル化に使用される可変長ＭＡＣペイロード１８７も含まれる。具体的には、ＭＡＣペイロード１８７には、ＩＰヘッダ４３４及びトランスポートヘッダ４３６とＳＤＮＰペイロード１４３０で構成されるＩＰペイロード４３５が含まれる。

【０５２０】

ＩＰヘッダ４３４は、バイナリ４を含むプロトコルフィールド４４７またはバイナリ６を含むプロトコルフィールド４４８よる決定に基づいてＩＰデータグラムがＩＰｖ４かＩＰｖ６プロトコルのいずれに従うかによって異なる。プリアンブル４４０と４４４には両方とも、ＴＣＰ、ＵＤＰ、またはメンテナンス機能ＩＣＭＰとＩＧＭＰなど、使用されるレイヤ４転送方法の決定に使用されるトランスポートヘッダフラグ４７０が含まれる。具体的には、セキュア動的通信ネットワーク及びプロトコルに従って、ソフトウェア及びデータファイルにはＴＣＰ転送が使用され、ＶｏＩＰ及びビデオなどのリアルタイムデータにはＵＤＰが使用される。トランスポートヘッダ４３６の長さとフォーマットは、トランスポートヘッダ４７０に応じて異なる。ＩＰヘッダ４３４には、ＩＰｖ４の送信元アドレス４４１と宛先アドレス４４２、またはＩＰｖ６の送信元アドレス４４５と宛先アドレス４４６が含まれる。

【０５２１】

イーサネット（登録商標）パケットのラストマイルルーティングは、ＩＰアドレスとＭＡＣアドレスの両方に依存する。図では、ＭＡＣ　$C_{1,1}$またはＩＰ　$M_{0,0}$のように、ＩＰまたはＭＡＣアドレスが指し示すデバイスの例示的な名称で表されている。ここでは、明確化を目的として、数値アドレスの代わりに、イーサネット（登録商標）フォーマットのインターネットプロトコルに従って作成された数値アドレスを表す記号名が使用されている。ＩＰアドレスＩＰ　$C_{1,1}$は異なる形式に従い、ＩＰｖ４名及びＩＰｖ６名に異なるバイト数が使用されていることに注意されたい。さらに、ＭＡＣアドレスのフォーマットは、使用されるレイヤ２データリンクプロトコルによって異なる。そのため、セルラー無線のＭＡＣアドレスＭＡＣ　$C_{1,1}$は、ＷｉＦｉまたはイーサネット（登録商標）により通信する同じデバイスのＭＡＣアドレスとは異なる。ＭＡＣアドレスはＩＰアドレスには関係がない。すなわち、同じクライアントのＩＰアドレスとＭＡＣアドレスには関係がない。

【０５２２】

図５０Ａ～図５０Ｄに、イーサネット（登録商標）パケットの順次ラストマイルルーティングが示されている。各図には、２つのイーサネット（登録商標）パケットが含まれる。上部のパケットはＩＰｖ４データグラムで構成され、下部のパケットはＩＰｖ６データ

グラムで構成される。ＩＰｖ４とＩＰｖ６では異なるフィールド長の異なるフォーマットが使用されるため、同じペイロードが伝送される場合でも、通常、表示される２つのイーサネット（登録商標）パケットは同じ長さにはならない。通信シーケンスの最初のステップで、ＳＤＮＰペイロードＡはラストリンク１４０４を介してＳＤＮＰクライアント１４００からルータ１４０２Ａに移動し、そしてゲートウェイリンク１４１４を介してＳＤＮＰゲートウェイ１４０１に移動する。ＳＤＮＰゲートウェイからクライアントへの応答では、ＳＤＮＰペイロードＧがゲートウェイリンク１４１４を介してＳＤＮＰゲートウェイ１４０１からルータ１４０２Ａに移動し、そしてラストリンク１４０４を介してクライアント１４００に移動する。ＳＤＮＰクライアント１４００は数値ＭＡＣアドレスＭＡＣ　$C_{1,1}$及び数値ＩＰアドレスＩＰ　$C_{1,1}$を有し、ルータ１４０２Ａは数値ＭＡＣアドレスＭＡＣ　Ｒを有し、ＳＤＮＰゲートウェイは数値ＭＡＣアドレスＭＡＣ　$M_{0,0}$及び数値ＩＰアドレスＩＰ　$M_{0,0}$を有する。ルータ１４０２ＡのＩＰアドレスは、データパケットでは使用されない。

【０５２３】

ＳＤＮＰデータグラムのパケットルーティングがＳＤＮＰネットワークによって完全に制御されるＳＤＮＰクラウドとは異なり、ＩＰデータグラムが使用されるラストマイル通信では、ＳＤＮＰペイロードが解釈されること、またはルーティングに影響を与えることがない。つまり、ラストマイルで転送される各通信には、固定送信元ＩＰアドレス及び固定宛先ＩＰアドレスが含まれる。イーサネット（登録商標）パケットの送信に使用される物理媒体またはチャネルは、ラストマイルの各通信ノードを接続するＭＡＣアドレスにより管理される。例えば、図５０Ａには、送信元ＭＡＣアドレスＭＡＣ　$C_{1,1}$、宛先ＭＡＣアドレスＭＡＣ　Ｒ、送信元ＩＰアドレスＩＰ　$C_{1,1}$、宛先アドレスＩＰ　$M_{0,0}$、及びＳＤＮＰペイロードを含むルータ１４０２Ａへのシングルｐｈｙルーティングに使用されるＩＰｖ４及びＩＰｖ６ラストリンクイーサネット（登録商標）パケットが示されている。図５０Ｂには、対応するイーサネット（登録商標）により、パケットゲートウェイリンク１４１４を介してＳＤＮＰペイロードＡが転送される図が示されている。示されるように、送信元ＩＰアドレスと宛先ＩＰアドレスはＩＰ　$C_{1,1}$及びＩＰ　$M_{0,0}$から変更されないが、送信元ＭＡＣアドレスと宛先ＭＡＣアドレスは元の値からＭＡＣ　Ｒ及びＭＡＣ　$M_{0,0}$に変更される。

【０５２４】

ＳＤＮＰゲートウェイ１４０１からクライアント１４００への応答通信では、ＳＤＮＰペイロードＧが同じネットワークを逆の順序で、すなわち送信元アドレスと宛先アドレスが入れ替わる場所を通過する。図５０Ｃに示されるように、送信元ＩＰアドレスと宛先ＩＰアドレスはそれぞれＩＰ　$M_{0,0}$とＩＰ　$C_{1,1}$で構成され、ＭＡＣアドレスには送信元アドレスＭＡＣ　$M_{0,0}$及び宛先アドレスＭＡＣ　Ｒが含まれる。図５０Ｄに示されるラストリンク通信では、ＭＡＣアドレスは送信元アドレスＭＡＣ　Ｒ及び宛先アドレスＭＡＣ　$C_{1,1}$に変更されるが、送信元ＩＰアドレスと宛先ＩＰアドレスはＩＰ　$M_{0,0}$及びＩＰ　$C_{1,1}$から変更されない。

【０５２５】

ＳＤＮＰクライアントからのラストマイル通信を表す便利な手段の１つとして、送信元ＭＡＣアドレス、宛先ＭＡＣアドレス、送信元ＩＰアドレス、宛先ＩＰアドレス、ＳＤＮＰペイロードを含むデータフィールドで構成される「簡略化された」データパケットを利用する方法が挙げられる。簡略化された形式は、任意の通信「セッション」、すなわちラストマイルを介してＳＤＮＰゲートウェイに送信される連続データパケットの構築及びその応答におけるデータフローを示す上で便利である。例えば、図５１Ａの上部には、ＳＤＮＰクライアントからＳＤＮＰゲートウェイに送信される連続のイーサネット（登録商標）パケットが示されている（短縮化された形式で表示）。各行は、ＳＤＮＰペイロード、Ａ、Ｂ、Ｃを含む連続したデータパケットを表している。左端の列はラストリンクのデータパケット、右の列はゲートウェイリンクを介して同じペイロードを伝送するデータパケットを示している。示されるように、全てのパケットには、送信元ＩＰアドレスとしてＩ

Ｐ　Ｃ$_{1,1}$、宛先ＩＰアドレスとしてＩＰ　Ｍ$_{0,0}$が指定されている。ＩＰアドレスのペアが１つしか使用されないため、本明細書ではこのラストマイルはＳＤＮＰシングルルートラストマイル通信と呼ばれる。さらに、連続したデータパケットを伝送するためにＳＤＮＰクライアント１４００により使用される送信元ＩＰアドレスは変化しないため、ラストリンクでは「静的クライアントアドレス指定」が使用される。

【０５２６】

各通信ノードとその近隣ノードとのレイヤ２相互接続が容易化されるように、ラストマイルの異なるセグメントのＭＡＣアドレスは必然的に変更される。示されるように、クライアントからルータに向かってラストリンクを通過する全ての連続パケットでは、送信元ＭＡＣアドレスＭＡＣ　Ｃ$_{1,1}$及び宛先ＭＡＣアドレスＭＡＣ　Ｒが使用される。連続したデータパケットではクライアントに単一のＭＡＣアドレスが使用されるため、ラストリンクは単一の物理媒体、すなわちシングルＰＨＹラストリンクで構成される。ゲートウェイリンクを介した転送では、送信元ＭＡＣアドレスＭＡＣ　Ｒと宛先ＭＡＣアドレスＭＡＣ Ｍ$_{0,0}$が使用される。

【０５２７】

そのため、示されるデータパケットにはＳＤＮＰペイロードが含まれるが、ラストマイルでのルーティングでは必然的にスニッフィング可能なＭＡＣアドレスとＩＰアドレス、すなわち不正聴取者の監視により解釈できるアドレスが使用される。同一の送信元ＩＰアドレスと宛先ＩＰアドレスを有するパケットを追跡することで、不正聴取者はデータパケットが同じ会話またはセッションの一部である可能性が高いと推測でき、ＳＤＮＰペイロードを開けなくても、コール時間、ファイルサイズ、データレートなどのメタデータを収集して、発信者のプロファイルを作成できる。さらに、比喩的にはパンくずリストのように、ハッカーはＭＡＣアドレスとＩＰアドレスを追跡することで、コールの発信元をエンドデバイス、つまりクライアントデバイスまで追跡できる可能性があるため、発信者を個人的に特定できる。

【０５２８】

本明細書で開示されるように、クライアントデバイスへの追跡を防止し、関連するコールパケットを難読化し、そしてメタデータの収集を抑制する上で優れた方法は、ラストマイル及びラストリンク通信でＭＡＣアドレスとＩＰアドレスを動的に変更することである。こうした独創的な偽装の方法には以下が含まれる。

・ラストリンクＭＡＣアドレスを動的に変更することで、変化する通信媒体を介してデータパケットを送信する。これは、本明細書では「マルチＰＨＹラストリンク」通信と呼ばれる。

・クライアントデバイスのＩＰアドレスのＩＤを動的に変更することで、発信者を偽装する。これは、「動的クライアントアドレス指定」と呼ばれる。

・異なるＳＤＮＰゲートウェイＩＰアドレスとの間における通信のＩＰアドレスを動的に変更することで、ラストマイルにおける連続データパケットの通信パスを変更する。これは、「マルチルートラストマイル」通信と呼ばれる。

【０５２９】

マルチＰＨＹ、動的クライアントアドレス指定、及びマルチルートラストマイル通信を組み合わせることで、どのパケットが同じコールまたはセッションの一部であるかを理解できるのはＳＤＮＰ発信者とＳＤＮＰゲートウェイのみとなるため、ラストマイルとラストリンク通信の追跡とトレースが非常に困難になる。これらの方法は、個別にでも、組み合わせても使用できる。

【０５３０】

例えば、図５１Ａの下半分には、静的クライアントアドレス指定によるシングルルートラストマイル通信でのマルチＰＨＹラストリンク通信の使用が示されている。示されるように、各行は、ＳＤＮＰクライアントからＳＤＮＰゲートウェイへの通信で使用されるデータパケットのペアで構成される。左側はラストリンクデータパケット、右側はゲートウェイリンクデータパッケージを表している。３つの行は３つの連続したメッセージを表し

ている。一番上の行には最初のデータセット「ＳＤＮＰペイロードＡ」、中央の行にはＳＤＮＰペイロードＢが含まれ、一番下の行はＳＤＮＰペイロードＣを含む連続データパケットの３番目を表している。静的クライアントアドレス指定によるシングルルートラストマイル通信では、連続する全てのデータパケットで、静的クライアントアドレスＩＰ　$C_{1,1}$及び固定宛先ＩＰアドレスＩＰ　$M_{0,0}$が使用される。

【０５３１】

マルチＰＨＹラストリンク通信を実行するには、すなわちラストリンクのデータを複数の物理媒体にルーティングするには、順次データパケットにおけるＳＤＮＰクライアントのＭＡＣアドレスを動的に変更する必要がある。各ＭＡＣアドレスは、イーサネット（登録商標）１００ＢＡＳＥ－Ｔ及び１０００ＢＡＳＥ－Ｔ接続など、特定のＰＨＹレイヤに対応する。物理媒体が３つの場合、パケットでクライアントのＭＡＣアドレスがＭＡＣ　$C_{1,1}$からＭＡＣ　$C_{1,2}$へ、そしてＭＡＣ　$C_{1,3}$へと動的に変更される。媒体が２つしかない場合は、パターン認識を回避するため、ＭＡＣ　$C_{1,1}$、ＭＡＣ　$C_{1,2}$、ＭＡＣ　$C_{1,2}$、ＭＡＣ　$C_{1,1}$、ＭＡＣ　$C_{1,2}$、ＭＡＣ　$C_{1,1}$、ＭＡＣ　$C_{1,2}$、ＭＡＣ　$C_{1,1}$など、ＭＡＣアドレスをランダムパターンで変更することができる。送信元ＭＡＣアドレスは変化するが、ラストリンクの宛先ＭＡＣアドレスはＭＡＣ　Ｒとして一定に維持することができる。ラストリンクの全てのマルチＰＨＹパスは同じルータで終端するため、ラストマイルの残りの部分を通るデータパスは、シングルルート通信として固定されたままとなる。言い換えると、ラストリンクではマルチＰＨＹ接続が使用されるが、ラストマイルは単一のゲートウェイを介してＳＤＮＰクラウドに入り、ラストマイルはシングルルート通信で構成される。

【０５３２】

マルチＰＨＹアプローチではある程度の偽装が実現するが、共通のクライアントＩＰアドレスが共有されるため、特定のコールからのデータパケットのパケットスニッフィングが依然として可能となる。この検知方法は、動的なクライアントアドレス指定（クライアントが送信する各パケットでＩＰアドレスを変更する操作）を使用して妨害できる。一例として、図５１Ｂに、シングルルートラストマイル通信におけるクライアント動的ＩＰアドレス指定の使用が示されている。上部のデータパケットのセットはシングルＰＨＹラストリンク接続、下部のデータパケットのセットはマルチＰＨＹ実装を示している。ＳＤＮＰシングルルートラストマイル通信では、シングルＰＨＹ方法かマルチＰＨＹ方法のいずれが使用されるかに関わらず、ＳＤＮＰゲートウェイの宛先ＩＰアドレス４４２は、全てのデータパケットで数値ＩＰ　$M_{0,0}$に固定されたままとなる。

【０５３３】

示されるように、動的クライアントアドレス指定の場合、ＳＤＮＰペイロードＡを伝送するデータパケットでは動的に選択された送信元ＩＰアドレス４４１（ＩＰ　$C_{1,1}$を含む）、ＳＤＮＰペイロードＢを伝送するデータパケットでは動的に選択された送信元ＩＰアドレス（ＩＰ　$C_{1,2}$を含む）、ＳＤＮＰペイロードＣを伝送するデータパケットでは動的に選択された送信元ＩＰアドレス（ＩＰ　$C_{1,3}$を含む）などのように使用される。動的に選択されるアドレスの数は、特にＩＰｖ６でほぼ無制限である。さらに、ＩＰアドレスは一定時間（例えば１秒）再利用されるため、アドレスがリサイクルされる前に発生する場合がある。シングルＰＨＹラストリンクでの動的クライアントアドレスの場合、送信元ＩＰアドレスが変更されても、送信元ＭＡＣアドレス１８３の値、この例ではＭＡＣ　$C_{1,1}$は一定に保たれる。マルチＰＨＹラストリンクでの動的クライアントアドレスの場合、送信元ＭＡＣアドレス１８３の値はＭＡＣ　$C_{1,1}$からＭＡＣ　$C_{1,2}$、そしてＭＡＣ　$C_{1,3}$へと連続的に変化する。クライアントの変化するＭＡＣアドレスとその動的ＩＰアドレスの間には、特に数学的な対応はない。

【０５３４】

動的クライアントアドレス指定は、異なるユーザから送信されたメッセージで構成されているように見えるが、データパケットは依然としてシングルルートでラストマイルのほとんどを通過する（マルチＰＨＹ実装のラストリンクを除く）。ラストマイル通信のパケ

ットスニッフィングを混乱させるより高度な方法として、「マルチルート」通信の採用が挙げられる。マルチルート通信では、クライアントとＳＤＮＰクラウドの接続に複数のＳＤＮＰゲートウェイＩＰアドレスが使用される。ＳＤＮＰネットワークルーティングはシグナリングサーバにより規定され、各パケットのＳＤＮＰタグの識別が使用されるため、データが単一のゲートウェイを介してＳＤＮＰクラウドに入るか、複数のゲートウェイを介してＳＤＮＰクラウドに入るかに関係なく、ＳＤＮＰクラウドからパケットを宛先にルーティングできるようになる。図５１Ｃには、静的クライアントアドレス指定によるマルチルートラストマイル通信の使用が示されている。ラストリンクに示される全てのデータパケットでは、クライアントの送信元ＩＰアドレス４４１は数値ＩＰ　$C_{1,1}$で静的のままとなるが、ＳＤＮＰペイロードＡ、Ｂ、Ｃを含む連続データパケットではＩＰ　$M_{0,0}$からＩＰ　$M_{0,1}$、そしてＩＰ　$M_{0,3}$へと宛先ＩＰアドレス４４２が動的に変化する。ＳＤＮＰゲートウェイのＩＰアドレスはランダムに選択されるのではなく、ＳＤＮＰシグナリングサーバにより「選択」され、一時的に発信者に近いゲートウェイ、すなわちＳＤＮＰクライアントと特定のＳＤＮＰゲートウェイ間の統計的伝播遅延が最小のゲートウェイを表す。この例では、動的宛先アドレスは、ＰＨＹ接続に関係なく変化する。例えば、上部のデータパケットのセットはラストリンクの数値ＭＡＣ　$C_{1,1}$を有するクライアント送信元ＭＡＣアドレス１８３とのシングルＰＨＹラストリンク接続、下部のデータパケットのセットは異なる媒体間で、ＭＡＣ　$C_{1,1}$、ＭＡＣ　$C_{1,2}$、ＭＡＣ　$C_{1,3}$など、送信元ＭＡＣアドレスが変更されるマルチＰＨＹ実装を示している。クライアントの変化するＭＡＣアドレスとＳＤＮＰゲートウェイの宛先ＩＰアドレスの間には、対応するパターンまたは数学的な関係はない。

【０５３５】

最も効果的なレベルの偽装を実現するには、動的クライアントアドレス指定とマルチルートラストマイル通信を組み合わせる。図５１Ｄには、シングルＰＨＹラストリンクの実装（図の上部）及びマルチＰＨＹラストリンクバージョン（図の下部）の両方におけるこのセキュリティ機能の新しい組み合わせが示されている。下部に示される完全に動的なバージョンでは、送信元ＩＰアドレス４４１はＩＰ　$C_{1,1}$からＩＰ　$C_{1,2}$、そしてＩＰ　$C_{1,3}$へと動的かつランダムに変化し、ＳＤＮＰゲートウェイの宛先ＩＰアドレス４４２はＩＰ　$M_{0,0}$からＩＰ　$M_{0,1}$、そしてＩＰ　$M_{0,3}$へと独立して変化する。伝播遅延が最小限に抑えられるように、ＳＤＮＰゲートウェイアドレスはＳＤＮＰシグナリングサーバにより選択され、動的クライアントアドレスは無関係な方法で変更される。前例のように、上部のデータパケットのセットはラストリンクの数値ＭＡＣ　$C_{1,1}$を有するクライアント送信元ＭＡＣアドレス１８３とのシングルＰＨＹラストリンク接続、下部のデータパケットのセットは異なる媒体間で、ＭＡＣ　$C_{1,1}$、ＭＡＣ　$C_{1,2}$、ＭＡＣ　$C_{1,3}$など、送信元ＭＡＣアドレスが変更されるマルチＰＨＹ実装を示している。クライアントの変化するＭＡＣアドレスとクライアントまたはＳＤＮＰゲートウェイの変化するＩＰアドレスの間には、対応するパターンまたは数学的な関係はない。しかし、マルチルートラストマイル通信では、全てのデータが単一のルータＲに集められるのではなく、マルチＰＨＹラストリンクから３つの異なるルータR_1、R_2、R_3に有利に接続できる。

【０５３６】

図５２Ａの表には、静的クライアントアドレスとシングルＰＨＹラストリンクを有するシングルルートラストマイルで構成される最も安全性の低い実装（表の最後の１０行目に表示）から、動的送信先アドレス指定とマルチルートラストマイル通信を有するマルチＰＨＹラストリンクにより実現する優れた偽装（表の最上部の１行目に表示）に至るまで、前述の１０種類のラストマイル偽装がまとめられている。表はセキュリティの強度の順に並べられている。表記$C_{1,n}$、$M_{0,n}$、R_nは、ＳＤＮＰクライアント、ＳＤＮＰゲートウェイ、及びラストリンクルータの動的に変化するアドレスを指している。動的アドレスに相関性はない。７行目～１０行目にはシングルルートラストマイル通信、すなわち単一のゲートウェイ$M_{0,0}$が使用される通信、１行目～６行目には複数のゲートウェイとのマルチルートラストマイル通信が示されている。網掛けされた１行目と４行目を除き、ラ

ストリンク通信はＭＡＣアドレスＲを有する単一のルータに接続される。対照的に、マルチルート通信として、網掛けされた１行目と４行目は動的ＭＡＣアドレスR_nを有する複数のルータに接続されるマルチＰＨＹラストリンク通信を表している。

【０５３７】

図５２Ｂには、シングルＰＨＹラストリンクの静的クライアントアドレス指定、マルチＰＨＹラストリンクの静的クライアントアドレス指定、シングルＰＨＹラストリンクの動的クライアントアドレス指定、及びマルチＰＨＹラストリンクの動的クライアントアドレス指定という４つの組み合わせで、シングルルートラストマイル通信の動作が位相幾何学的に示されている。各ボックスには、使用されるデータパスを示す３つの連続したデータパケット通信が示されている。実線はデータパケットフロー、点線は使用されていないが可能性のあるパスを表している。網掛けされた円はラストマイル通信で使用される通信ノード、空の円は未使用の通信ノードを表している。示されるように、全ての例で、ラストマイルデータはルータＲとＳＤＮＰゲートウェイ$M_{0,0}$間の単一接続を介してルーティングされて終端に達する。

【０５３８】

左上に示されるシングルＰＨＹラストリンク経由の静的クライアントアドレス指定の場合、連続する各パケットは、不変のＩＰアドレスによりラストマイル全体で同じパスを通る。左下に示されるマルチＰＨＹラストリンク経由の静的クライアントアドレス指定の場合、連続する各パケットは、動的に変化するＭＡＣアドレスの指定に従ってラストリンクで異なるパスを通る。ラストマイルの残りの部分は、不変のＩＰアドレスで指定されたシングルルートで構成される。単一ルート転送ではあるが、ラストリンクの物理媒体を変更すると、発信者の追跡がより困難になる。右上に示されるシングルＰＨＹラストリンク経由の動的クライアントアドレス指定の場合、連続する各パケットは、不変の宛先ＩＰアドレスとラストリンクの一定のクライアントＭＡＣアドレスに従って、ラストマイル全体で同じパスを通る。代わりに、動的送信元ＩＰアドレスの変更により、クライアントＩＤを変更することで、偽装が実現する。右下の動的クライアントアドレス指定とマルチＰＨＹラストリンクの両方が使用されるシングルルート通信の場合、全てのパケットが単一のＳＤＮＰゲートウェイにルーティングされても、クライアントのＭＡＣアドレスと送信先ＩＰアドレスが動的かつランダムに変化する。

【０５３９】

動的クライアントアドレス指定は、クライアントデバイスで１つ以上の一時的なアドホックＩＰアドレスが使用されるプロセスである。このプロセスには２つの段階がある。１つ目の段階では、デバイスが最初にネットワークにログオンする際、最も近いルータに接続されて、ローカルサブネットにその存在が登録される。次に、ルータから同じサブネット上にある最も近いＤＨＣＰサーバに接続がリダイレクトされる。Ｄｙｎａｍｉｃ Ｈｏｓｔ Ｃｏｎｆｉｇｕｒａｔｉｏｎ Ｐｒｏｔｏｃｏｌの頭字語であるＤＨＣＰは、ＩＰアドレスを動的に割り当てるために使用されるネットワーク管理プロトコルである。登録プロセスでは、クライアントデバイスに１つ以上のＩＰアドレスがダウンロードされ、そのアドレスが通信データレジスタに保存される。新しいセッションを開始するか新しいアドレスを要求することで、割り当てられたＩＰアドレスがローカルＤＨＣＰサーバによって更新されるまで、これらのＩＰアドレスを使用してクライアントデバイスから通信が行われる。アドレスは特定のサブネット内で動的に発行されるため、クライアントデバイスのＩＰアドレスはインターネットアドレスではない。

【０５４０】

クライアントデバイスからコールが発信される、またはＳＤＮＰネットワークにログオンする第２段階では、ＳＤＮＰサーバの静的ＩＰアドレスに基づいて、デバイスがＳＤＮＰシグナリングサーバに自動的に接続される。ＳＤＮＰサーバで着信メッセージが受信されると、アドホックＩＰアドレスまたはアドレスがＳＤＮＰネームサーバにアップロードされる。次に、ＳＤＮＰネームサーバから、それぞれの一時ＩＰアドレスの擬似コードとして、ＳＤＮＰアドレスが割り当てられる。動作中、ルーティングの直前に、パケットの

ＳＤＮＰ送信元アドレスがローカルのアドホックＩＰアドレスに置き換えられる。ＳＤＮＰ動的アドレス指定の場合、送信元アドレスが変化してパケットが繰り返し送信されることで、クライアントデバイスのＩＤが偽装される。このように、動的偽装により、クライアントデバイスの実際のＩＤを隠すことができる。

【０５４１】

ＳＤＮＰゲートウェイに到達すると、発信パケットの送信元アドレスからクライアントＩＰアドレスが破棄され、代わりにゲートウェイサーバのＳＤＮＰアドレスに置き換えられる。次に、各発信ＳＤＮＰパケットで、転送の直前に、デバイスのローカルＩＰアドレスがローカルのアドホックＩＰアドレスと交換される。送信元ＩＰアドレスと宛先ＩＰアドレスが一定で、応答が必要となるインターネットパケット転送とは異なり、ＳＤＮＰ転送では各ホップで新しいＩＰアドレスが使用される。そのため、ＳＤＮＰメッセージが最終的に宛先に到達する時点で、クライアントデバイスの送信元アドレスがデータパケットに含まれない。代わりに、シグナリングサーバから、応答のリターンパスに関する情報が宛先デバイスに通知される。

【０５４２】

図５２Ｃには、静的クライアントアドレス指定と動的クライアントアドレス指定、及びシングルＰＨＹラストリンクとマルチＰＨＹラストリンクの４つの組み合わせで、「マルチルート」ラストマイル通信の動作が位相幾何学的に示されている。各マルチルート通信では、宛先ＩＰアドレス、すなわちＳＤＮＰゲートウェイは常に変化する。つまり、ラストマイルルートは異なる入力でＳＤＮＰクラウドに接続される。左側の列では、クライアントアドレスは静的のままとなる。つまり、発信者のＩＤは変更されない。左上の例では、ラストリンクでシングルＰＨＹ接続が使用される。つまり、この場合もクライアントのＭＡＣアドレスが静的のままとなる。異なる宛先ゲートウェイと通信が行われても、ラストリンク物理媒体とクライアントＩＰアドレスが変化しないため、ラストマイルはコールトレースの影響を受けやすくなる。データパケットの転送に使用されるラストリンク媒体を変更するか、または発信者のＩＰアドレスの実際のＩＤを隠すことで、この弱点を補うことができる。

【０５４３】

左下の例では、ラストリンクにマルチＰＨＹ接続が使用される。つまり、クライアントのＭＡＣアドレスが動的に変化する。このようなアプローチにより、クライアントのＩＤが静的ＩＰアドレスに維持されるという事実を補うことができる。エンドツーエンドのマルチルートラストマイル通信の一部として、連続的なパケットが個別のＳＤＮＰゲートウェイに到達できるように、一意の各ラストリンクが個別のルータに接続される。そのため、最初のパケットは、一意のＰＨＹ媒体を介して、静的アドレスＩＰ　$C_{1,1}$のクライアントからＭＡＣアドレスＭＡＣ　R_1のルータにルーティングされ、その後最終的にＩＰアドレスＩＰ　$M_{0,0}$のＳＤＮＰゲートウェイにルーティングされる。同一のクライアントアドレスＩＰ　$C_{1,1}$の２番目のパケットは、一意のＰＨＹ媒体を介して、メディアアドレスＭＡＣ　R_2の別のルータにルーティングされ、その後最終的にＩＰアドレスＩＰ　$M_{0,1}$のＳＤＮＰゲートウェイにルーティングされる。同様に、静的クライアントＩＰアドレス$C_{1,1}$の３番目のパケットは、一意のＰＨＹ媒体を介して、メディアアドレスＭＡＣ　R_3のルータにルーティングされ、その後ＳＤＮＰゲートウェイ$M_{0,3}$にルーティングされる。複数のルータを使用すると、単一の送信先ＩＰアドレスを有するクライアントが使用されるにも関わらず、複数のＰＨＹラストリンクの便宜的な使用により、完全に別個の軌道でラストマイルパケットが伝送される。

【０５４４】

右上に示される別の実装形態では、単一のＭＡＣアドレスとＰＨＹ接続が使用されるが、クライアントのＩＤは動的に変化する。示されるように、クライアントのＩＰアドレスはＩＰ　$C_{1,1}$からＩＰ　$C_{1,2}$、そしてＩＰ　$C_{1,3}$へと動的に変化するが、物理媒体は送信元メディアアドレスＭＡＣ　$C_{1,1}$及び宛先アドレスＭＡＣ　Ｒで一定に維持される。次に、ＳＤＮＰシグナリングサーバにより決定されるランダムな順序で、データが

ゲートウェイM０，０、M０，１、M０，３に転送される。

【０５４５】

３つのラストマイル偽装方式全て、すなわちマルチＰＨＹラストリンクと動的クライアントアドレス指定が使用される複数ルート通信を組み合わせることで、優れたセキュリティが実現する。これは、図５２Ｃの右下に示されている。ここでは、マルチＰＨＹラストリンクと複数のルータが使用され、送信されたデータパケットが、複数のルートを介して、動的ＩＰアドレスを有するクライアントから複数のＳＤＮＰゲートウェイに伝送される。示されるように、動的送信元ネットワークアドレスＩＰ　Ｃ１，１を有するクライアントからの最初のパケットは、送信元メディアアドレスＭＡＣ　Ｃ１，１及び宛先メディアアドレスＭＡＣ　Ｒ１により定義されるマルチＰＨＹラストリンクにより、複数のルート経由で宛先ＩＰ　M０，０に送信される。動的に選択された送信元ネットワークアドレスＩＰ　Ｃ１，２を有するクライアントからの２番目のデータパケットは、送信元メディアアドレスＭＡＣ　Ｃ１，２及び宛先メディアアドレスＭＡＣ　Ｒ２により定義されるマルチＰＨＹラストリンクにより、複数のルート経由で宛先ＩＰ　M０，１に送信される。動的に選択された送信元ネットワークアドレスＩＰ　Ｃ１，３を有するクライアントからの３番目のデータパケットは、送信元メディアアドレスＭＡＣ　Ｃ１，３及び宛先メディアアドレスＭＡＣ　Ｒ３により定義されるマルチＰＨＹラストリンクにより、複数のルート経由で宛先ＩＰ　M０，３に送信される。このように、クライアントＩＰアドレス、ＳＤＮＰゲートウェイＩＰアドレス、クライアントのＭＡＣアドレス、及びルータのＭＡＣアドレスの組み合わせが全てランダムかつ動的に変化するため、コールトレースとメタデータの収集がほぼ不可能となる。

【０５４６】

複数のゲートウェイへの動的ＩＰアドレス指定、マルチＰＨＹ転送、及びマルチルート転送によるクライアントデバイスのＩＰアドレス偽装及びラストマイルルーティングの難読化は、クライアントデバイスまたはシグナリングサーバによって決定できる。ミスダイレクションプロセスは、乱数生成または他の擬似ランダムアルゴリズムを使用して実現できる。重要な原則は、ルーティングと転送の変化を予測不能にすることである。

【０５４７】

図５２Ｄには、複数ルート経由のイーサネット（登録商標）パケットのラストマイルデータ転送について、２つのやや強度の低いバージョンが示されている。左側の図では、静的クライアントアドレス指定とマルチＰＨＹラストリンク接続が使用される。右側の図では、動的クライアントアドレス指定とマルチＰＨＹラストリンク接続が使用される。この実装と図５２Ｃに示されるマルチＰＨＹバージョンは、図５２Ｃのバージョンではデータ転送を複数のルータに分散させるのではなく、単一のルータＲが使用されるという点で異なる。要するに、ラストリンク接続で単一のルータが使用されるマルチルート転送では、クライアントからの順次データが複数の物理媒体、すなわちマルチＰＨＹラストリンクに分散されてから、単一のルータＲで再収集される。そして、この共通ルータから異なる宛先ＩＰアドレスにより定義される複数のＳＤＮＰゲートウェイへのラストマイルにおける複数のゲートウェイリンク及び他の並列セクション（図示なし）を含むラストマイルの残りの部分にデータが送信される。

【０５４８】

ＳＤＮＰクライアントとＳＤＮＰゲートウェイ間のラストマイル通信には、イーサネット（登録商標）の付属として、ＷｉＦｉワイヤレス通信を使用することもできる。ＷｉＦｉ通信では、特にイーサネット（登録商標）データパケットを使用する場合、３つまたは４つのＭＡＣアドレス（無線リンクに２つ、有線ネットワーク接続に１つまたは２つ）を有するデータパケットが必要である。図５３には、ＳＤＮＰラストマイル及びラストリンク通信に適合させた同じＷｉＦｉパケットフォーマットが示されている。ラストリンク通信に適用できるアクセスポイントとして必要となるのは、３つの６Ｂの長さのＭＡＣアドレスのみである。具体的には、受信無線基地局または「受信機」のＭＡＣアドレス１フィールド２３５、送信無線基地局または「送信機」のＭＡＣアドレス２フィールド２３６、

及びＷｉＦｉルータへの有線ネットワーク接続のＭＡＣアドレスを含むＭＡＣアドレス３フィールド２３７、すなわちイーサネット（登録商標）または「ネット」である。動作中、受信機と送信機データフィールドにロードされるＭＡＣアドレスの数値は、（ｉ）無線で受信されてイーサネット（登録商標）に転送されるデータパケットか、または（ｉｉ）無線通信に変換されるイーサネット（登録商標）上の着信データかが決定される「Ｔｏ ＤＳ」／「Ｆｒｏｍ ＤＳ」の方向設定に依存する。ＭＡＣアドレス４データフィールド２３９はオプションであり、ＷｉＦｉデバイスが「無線配信モード」で無線ブリッジとして使用される場合にのみ使用される。こうしたモードは、セルラーまたはマイクロ波ネットワークの代替手段として、砂漠などの長距離のラストマイル通信で使用できるが、一般的なＳＤＮＰラストマイルにおけるＷｉＦｉ通信の使用は、通常、ＳＤＮＰクライアントへのラストリンク接続に焦点が当てられる。そのため、本明細書におけるＳＤＮＰ技術はワイヤレス配信モードルーティングにも同様に適用できることを理解した上で、以下の説明では、ＷｉＦｉルータのアクセスポイントモードに焦点が当てられている。

【０５４９】

イーサネット（登録商標）データパケットと同様に、プリアンブル２３０と開始フレームデリミタＳＦＤ ２３２には、データとデバイスを同期するためのレイヤ１データが含まれる。物理レイヤ収束手続きＰＬＣＰ ２３２には、レイヤ１とレイヤ２の情報（関連するパケット長、データレート、ヘッダのエラーチェックなど）が混在する。ＩＥＥＥ８０２．１１規格に従って、残りのデータフィールドには、フレーム制御２３３（これにより、ＳＤＮＰペイロードの伝送に使用されるタイプである管理、制御、予約、または「データ」としてＷｉＦｉバージョンパケットタイプが指定される）を含むレイヤ２データリンク情報が含まれる。

【０５５０】

持続時間＆ＩＤ ２３４にはＮＡＶ持続時間が含まれる。ただし、ＷｉＦｉデバイスが電力節約モードになっている場合は、このフィールドにはステーションＩＤが含まれる。ＮＡＶまたはネットワーク割り当てベクトルは、ワイヤレス通信システムの電力節約モードに使用される仮想キャリア検知メカニズムである。ＮＡＶ持続時間は、一定レートでゼロまでカウントダウンするカウンタと見なすことができる。これにより、媒体が検知され、無線がアイドル状態か、まだ通信中であるかが判断される。アイドルモードでは、カウンタによりＮＡＶ持続時間が繰り返し数えられ、注意を要する無線通信アクティビティが検知されたかどうかが確認される。シーケンス制御または「シーケンス」フィールド２３８には、レイヤ２パケットフレームを定義するパケットシーケンスとフラグメントナンバーが含まれる。フレームチェック２４０には、データパケット全体の３２ビットＣＲＣチェックサム、すなわちエラーチェックデータリンクトレーラが含まれる。

【０５５１】

ＷｉＦｉペイロード２４１は、ＷｉＦｉペイロードの伝送に使用される０Ｂから２，３１２Ｂの長いデータフィールドである。ＳＤＮＰラストマイル通信では、このフィールドには、ＩＰヘッダ４３４、トランスポートヘッダ４３６、ＳＤＮＰペイロード４３５など、ラストマイル通信で使用されるＩＰデータグラムが含まれる。

【０５５２】

ＩＰヘッダ４３４は、バイナリ４を含むプロトコルフィールド４４７またはバイナリ６を含むプロトコルフィールド４４８よる決定に基づいてＩＰデータグラムがＩＰｖ４かＩＰｖ６プロトコルのいずれに従うかによって異なる。プリアンブル４４０と４４４には両方とも、ＴＣＰ、ＵＤＰ、またはメンテナンス機能ＩＣＭＰとＩＧＭＰなど、使用されるレイヤ４転送方法の決定に使用されるトランスポートヘッダフラグ４７０が含まれる。具体的には、セキュア動的通信ネットワーク及びプロトコルに従って、ソフトウェア及びデータファイルにはＴＣＰ転送が使用され、ＶｏＩＰ及びビデオなどのリアルタイムデータにはＵＤＰが使用される。トランスポートヘッダ４３６の長さとフォーマットは、トランスポートヘッダフラグ４７０に応じて異なる。ＩＰヘッダ４３４には、ＩＰｖ４の送信元アドレス４４１と宛先アドレス４４２、またはＩＰｖ６の送信元アドレス４４５と宛先ア

ドレスと４４６が含まれる。

【０５５３】

イーサネット（登録商標）データパケットと同様に、ＷｉＦｉパケットのラストマイルルーティングはＩＰアドレスとＭＡＣアドレスの両方に依存し、ＩＰアドレスまたはＭＡＣアドレスが指し示すデバイスの象徴的な名称で表されている。図５４Ａ～図５４Ｄには、ＷｉＦｉパケットの順次ラストマイルルーティングが示されている。各図には、２つのＷｉＦｉパケットが含まれる。上部のパケットはＩＰｖ４データグラムで構成され、下部のパケットはＩＰｖ４データグラムで構成される。ＩＰｖ４とＩＰｖ６では異なるフィールド長の異なるフォーマットが使用されるため、同じペイロードが伝送される場合でも、通常、表示される２つのＷｉＦｉパケットは同じ長さにはならない。

【０５５４】

通信シーケンスの最初のステップで、ＳＤＮＰペイロードＡはＷｉＦｉ無線媒体として、ラストリンク１４０４を介してＳＤＮＰクライアント１４００からＷｉＦｉ基地局／ルータ１４０２Ｗに移動し、そしてＢＳリンク１４１５を介して有線でルータ１４０２Ｘに移動する。次に、ゲートウェイリンク１４１４を介して、データパケットがルータ１４０２ＸからＳＤＮＰゲートウェイ１４０１に伝送される。ＳＤＮＰゲートウェイからクライアントへの応答では、ＳＤＮＰペイロードＧがゲートウェイリンク１４１４を介して有線でＳＤＮＰゲートウェイ１４０１からルータ１４０２Ｘへ、次にＢＬリンク１４１５を介してＷｉＦｉルータ１４０２Ｗへ、そしてＷｉＦｉ無線が通信媒体として使用され、ラストリンク１４０４を介してクライアント１４００へと移動する。ＳＤＮＰクライアントは数値ＭＡＣアドレスＭＡＣ　$C_{1,1}$及び数値ＩＰアドレスＩＰ　$C_{1,1}$を有し、ＷｉＦｉルータ１４０２Ｗは数値ＭＡＣアドレスＭＡＣ　Ｗを有し、ルータ１４０２Ａは数値ＭＡＣアドレスＭＡＣ　Ｒを有し、ＳＤＮＰゲートウェイは数値ＭＡＣアドレスＭＡＣ　$M_{0,0}$及び数値ＩＰアドレスＩＰ　$M_{0,0}$を有する。ＷｉＦｉルータ１４０２Ｗ及び有線ルータ１４０２ＸのＩＰアドレスは、示されるように、ラストマイル通信では必要ない。

【０５５５】

ＳＤＮＰデータグラムのパケットルーティングがＳＤＮＰネットワークによって完全に制御されるＳＤＮＰクラウドとは異なり、ＩＰデータグラムが使用されるラストマイル通信では、ＳＤＮＰペイロードが解釈されること、またはルーティングに影響を与えることがない。つまり、ラストマイルで転送される各通信には、固定送信元ＩＰアドレス及び固定宛先ＩＰアドレスが含まれる。無線通信でＷｉＦｉパケットの送信に使用される物理媒体またはチャネル、及び有線通信でイーサネット（登録商標）パケットの送信に使用される物理媒体またはチャネルは、ラストマイルの各通信ノードを接続するＭＡＣアドレスにより管理される。

【０５５６】

例えば、図５４Ａには、ラストリンク１４０４を介したＷｉＦｉルータ１４０２Ｗへのシングルｐｈｙ無線ルーティングに使用されるＩＰｖ４及びＩＰｖ６ラストリンクＷｉＦｉパケットが示されている。これには、送信機ＭＡＣアドレスＭＡＣ　$C_{1,1}$及び受信機ＭＡＣアドレスＭＡＣ　Ｗが含まれる。次に、ＢＳリンク有線１４１５経由で、ＷｉＦｉルータ１４０２Ｗから、「ネット」ＭＡＣ宛先アドレスＭＡＣ　Ｒを有するイーサネット（登録商標）ルータ１４０２Ｘにルーティングされる。レイヤ３ネットワークルーティングには、エンドデバイス、すなわち送信元ＩＰアドレスＩＰ　$C_{1,1}$を有するＳＤＮＰクライアント１４００及び宛先アドレスＩＰ　$M_{0,0}$を有するＳＤＮＰゲートウェイ１４０１のみが含まれる。イーサネット（登録商標）データパケットとは異なり、ＷｉＦｉパケットには送信機または送信元無線ＭＡＣアドレスＭＡＣ　$C_{1,1}$、受信機または無線宛先ＭＡＣアドレスＭＡＣ　Ｗ、及びイーサネット（登録商標）「ネット」アドレスＭＡＣ　Ｒの３つのアドレスが含まれる。このデータ送信の方向では、有線ルータ１４０２ＸはＷｉＦｉルータデバイスのネットワーク宛先として機能する。そのため、ＷｉＦｉデータパケットにより、ＷｉＦｉ無線ラストリンク１４０４及びイーサネット（登録商標）有線ＢＳリンク１４１５の２つの媒体が指定される。図５４Ｂには、対応するイーサネット（登録

商標）により、パケットゲートウェイリンク１４１４を介してＳＤＮＰペイロードＡが転送される図が示されている。示されるように、送信元ＩＰアドレスと宛先ＩＰアドレスはＩＰ　$C_{1,1}$及びＩＰ　$M_{0,0}$から変更されないが、送信元ＭＡＣアドレスと宛先ＭＡＣアドレスは元の値からＭＡＣ　Ｒ及びＭＡＣ　$M_{0,0}$に変更される。

【０５５７】

応答通信には、宛先ＩＰアドレスと送信元ＩＰアドレスの交換、及びそれに応じたＭＡＣアドレスの調整が含まれる。図５４Ｃは、ゲートウェイリンク１４１４を介したＳＤＮＰゲートウェイ１４０１から有線ベースのルータ１４０２Ｘへのデータ転送に使用されるＩＰｖ４及びＩＰｖ６イーサネット（登録商標）パケットが示されている。レイヤ３データグラム情報について、ＩＰ送信元アドレス４４１にはＳＤＮＰゲートウェイ１４０１のネットワークアドレス、すなわちＩＰ　$M_{0,0}$が含まれ、ＩＰ宛先アドレスにはクライアントのアドレスである値ＩＰ　$C_{1,1}$が含まれる。ゲートウェイリンクイーサネット（登録商標）パケットのＭＡＣアドレスは、送信元アドレス１８３ではＭＡＣ　$M_{0,0}$、宛先ＭＡＣアドレス１８２ではＭＡＣ　Ｒとなる。

【０５５８】

図５４Ｄには、有線ＢＳリンク１４１５及びＷｉＦｉ無線ベースのラストリンク１４０４のＩＰｖ４及びＩＰｖ６　ＷｉＦｉパケットが示されている。ネットワークレイヤ３ルーティングには、送信元アドレス４４５及び宛先アドレス４４６として、ＳＤＮＰゲートウェイ１４０１アドレスＩＰ　$M_{0,0}$及びＳＤＮＰクライアントアドレスＩＰ　$C_{1,1}$が含まれる。「ネット」とラベル付けされたＭＡＣアドレスフィールド２３７の機能は、無線モードに従って変化する。ここに示される送信モードでは、このフィールドには、無線の着信データの有線送信元のイーサネット（登録商標）ＭＡＣアドレス、すなわちＷｉＦｉアクセスポイントにデータパケットを送信するルータ１４０２Ｘの数値ＭＡＣ　Ｒが含まれる。前述の図５４Ａに示される受信機モードでは、このフィールドにより、無線パケットとして受信されてイーサネット（登録商標）パケットに変換されるデータのイーサネット（登録商標）宛先が定義される。示される例では、「ネット」フィールド２３７には、送信モードと受信モードの両方において、ルータ１４０２Ｘと同じＭＡＣアドレス、すなわちＭＡＣ　Ｒが含まれる。つまり、ＷｉＦｉアクセスポイントではラストマイル接続に単一のイーサネット（登録商標）ルータが使用される。

【０５５９】

オプションとして、ラストマイル経由のマルチルート通信では、ＷｉＦｉアクセスポイントで受信されるデータパケットのルーティング、すなわち受信モードで使用される有線ルータは、ＷｉＦｉアクセスポイントから送信されるデータパケットのルーティング、すなわち送信モードで使用される有線ルータとは異なる場合がある。例えば、受信モードの無線パケットのネットワークＭＡＣアドレス２３７には数値ＭＡＣアドレスＭＡＣ　R_1が含まれ、送信モードではデータが別のルータ接続ＭＡＣ　R_2に変更される場合がある。つまり、オプションとして、ＢＳリンクは方向依存性のマルチＰＨＹ実装で構成できる。送信モードでは、ＷｉＦｉルータ１４０２ＷからＳＤＮＰクライアント１４００へのシングルＰＨＹ無線１４０４ラストリンクルーティングに使用されるラストリンクＷｉＦｉパケットには、数値ＭＡＣ　Ｗの送信機ＭＡＣアドレス２３６及び数値ＭＡＣ　$C_{1,1}$の受信機ＭＡＣアドレス２３５が含まれる。このデータ送信の方向では、有線ルータ１４０２Ａは、ＷｉＦｉルータデバイスから送信されるデータの送信元として機能する。そのため、ＷｉＦｉデータパケットにより、ＷｉＦｉ無線ラストリンク１４０４及びイーサネット（登録商標）有線ＢＳリンク１４１５の２つの媒体が指定される。

【０５６０】

セルラーネットワークは、ＳＤＮＰラストマイル通信に適応できる別の形式のワイヤレス通信である。セルラーネットワークでは、受信イーサネット（登録商標）パケットを無線固有の媒体アクセス制御（ＭＡＣ）パケットにパーティションが再設定される。多重に（ＴＤＭＡ）、符号分割で（ＣＤＭＡ）、またはコンテンツが複数のサブチャネル周波数に拡散されて（ＯＦＤＭ）、データが送受信される場合がある。直交周波数分割多重方式

（ＯＦＤＭ）に基づく４Ｇ／ＬＴＥ通信の場合、レイヤ２データパケットは、全てレイヤ２内の埋め込みサービスデータユニット（ＳＤＵ）の３つの異なるレベルにスタックされる。具体的には、最下位レベルは、ＰＨＹレイヤ１データを含む２０個のタイムスロット３００にまたがるＭＡＣヘッダ３０３とパディング３０５と共にシングルフレームＭＡＣ ＳＤＵ ３０４を含むＰＨＹ ＰＤＵ ２９９で構成される。ＭＡＣ ＳＤＵ ３０４には、無線リンク制御またはＲＬＣ ＳＤＵ ３０８が含まれる。

【０５６１】

無線リンク制御（ＲＬＣ）は、３Ｇ（ＵＭＴＳ）及び４Ｇ／ＬＴＥ（ＯＦＤＭ）ベースの電話で使用されるレイヤ２プロトコルである。無線リンク制御の機能は、３つのモード、すなわち確認済みモード、未確認モード、透過モードのいずれかで上位層の要求に応答し、エラー検出、エラー修正、重複検出、及び指定された形式に応じたデータのパケット化を提供する。データのパケット化には、ＲＬＣデータＰＤＵの並べ替えと再セグメント化に加えて、ＲＬＣ ＳＤＵの連結、セグメント化、及び再組み立てが含まれる。例えば、無線オーバーヘッド機能を実行する時間が割り当てられた後は、単一フレームＲＬＣ ＳＤＵ ３０８では、ペイロードを伝送する持続時間とデータファイルサイズが不可避的に制限される。したがって、単一フレームＲＬＣ ＳＤＵ ３０８は、セグメントに分割され、異なるＲＬＣレイヤ２フォーマット（マルチフレームＲＬＣ ＳＤＵ ３１９）にマッピングされる必要がある。

【０５６２】

図５５に示されるように、マルチフレームＲＬＣ ＳＤＵ ３１９の様々なＫ、Ｋ＋１、Ｋ＋２セグメント３１３、３１４、３１５などへの単一フレームＲＬＣ ＳＤＵ ３０８のマッピングは１対１では行われない。例に示されるように、単一フレームＲＬＣ ＳＤＵ ３０８のマッピングは、Ｋ＋２セグメント３１５の中央で終了する。代わりに、残りのＫ＋１セグメントの未送信部分が新しい単一フレームＲＬＣ ＳＤＵ ３１２で送信されるが、これは無線クロック同期に必要なパディング時間３１０が許可された後、及びＲＬＣヘッダ３１１が処理した後でのみ発生する。この方法では、Ｋ＋２スロットにカプセル化されたデータの送信は、データフローが中断されなかったかのように、中断されたところから正確に再開される。操作的には、４Ｇは、ＤＶＤチャプターの途中でＤＶＤエンコードされた映画の再生を一時停止し、他の機能を実行するためにしばらく待機してから、一時停止した場所から正確に再生を再開する操作に似ている。そのため、データコンテンツは失われず、セルラーシステムのＲＦデータ配信レートはパケットオーバーヘッド（ＰＤＵヘッダなど）以外の無駄な無線帯域幅がなくなるように最大化され、クロック同期パディング時間３１０によるデータレートの低下が最小限に抑えられる。

【０５６３】

マルチフレームＲＬＣ ＳＤＵ３１９により、各Ｋセグメントと１対１の対応でＰＤＣＰ ＰＤＵ３２０がカプセル化される。例えば、Ｋのセグメント３１３ではＰＤＣＰヘッダ３２１Ａ及びデータ３２３を含むＩＰペイロードが伝送され、（Ｋ＋１）のセグメント３１４ではＰＤＣＰヘッダ３２１Ｂ及びデータ３２４を含むＩＰペイロードが伝送され、（Ｋ＋２）のセグメント３１５ではＰＤＣＰヘッダ３２１Ｃ及びデータ３２５を含むＩＰペイロードが（以下同様に）伝送される。ＰＤＣＰという用語は、３Ｇ及び４Ｇ／ＬＴＥ通信プロトコルで指定されるＰａｃｋｅｔ Ｄａｔａ Ｃｏｎｖｅｒｇｅｎｃｅ Ｐｒｏｔｏｃｏｌの頭字語であり、これにより、圧縮、暗号化、整合性保証、ユーザと制御データ転送などの機能が実行される。ＰＤＣＰヘッダは、ユーザデータ、制御データなど、転送されるデータのタイプによって異なる。

【０５６４】

４Ｇデータパケットのデータ転送では連続的に連結されたデータストリームが運ばれるため、ペイロードサイズはイーサネット（登録商標）及びＷｉＦｉデータパケットのように定義された長さのブロックに量子化されることはない。代わりに、対応するレイヤ２データセグメント３１３、３１４、３１５・・・により伝送されるデータフィールド３２３、３２４、３２５・・・は、ＩＰヘッダ４３４及びトランスポートヘッダ４３６とＳＤＮ

Ｐペイロード１４３０を含むＩＰペイロード４３５のように、任意のサイズのペイロードに増分的に対応できる。さらに、ＯＦＤＭベースの通信では、各タイムスロットでは複数の周波数サブキャリアで同時にデータが伝送される。つまり、ＴＤＭＡのように、単一チャネルにおける持続時間によって総データスループットが単純に決定されるわけではない。しかし、便宜上、多くの場合、ＩＰデータグラムのサイズを、イーサネット（登録商標）またはＷｉＦｉ標準のサイズと一致するように維持すると便利である。

【０５６５】

示されるように、ＩＰヘッダ４３４は、バイナリ４を含むプロトコルフィールド４４７またはバイナリ６を含むプロトコルフィールド４４８よる決定に基づいてＩＰデータグラムがＩＰｖ４かＩＰｖ６プロトコルのいずれに従うかによって異なる。プリアンブル４４０と４４４には両方とも、ＴＣＰ、ＵＤＰ、またはメンテナンス機能ＩＣＭＰとＩＧＭＰなど、使用されるレイヤ４転送方法の決定に使用されるトランスポートヘッダフラグ４７０が含まれる。具体的には、セキュア動的通信ネットワーク及びプロトコルに従って、ソフトウェア及びデータファイルにはＴＣＰ転送が使用され、ＶｏＩＰ及びビデオなどのリアルタイムデータにはＵＤＰが使用される。トランスポートヘッダ４３６の長さとフォーマットは、トランスポートヘッダ４７０に応じて異なる。ＩＰヘッダ４３４には、ＩＰｖ４の送信元アドレス４４１と宛先アドレス４４２、またはＩＰｖ６の送信元アドレス４４５と宛先アドレスと４４６が含まれる。

【０５６６】

ＩＰｖ６データグラムが使用される４Ｇ通信の例として、図５６Ａには、セルラータワー及び基地局１４０２Ｑへのセルラー無線１４０４ラストリンクルーティングが示されている。具体的には、送信元ＭＡＣフィールド３００Ａでは、ＲＬＣ　ＰＤＵにより、セルラー送信元メディアアドレスがクライアントデバイスであるＭＡＣ　$C_{1,1}$として定義される。同様に、宛先ＭＡＣフィールド３００Ｂでは、セルラータワー及び基地局を表すＭＡＣ　ＢＳとしてセルラー受信機メディアアドレスが指定される。レイヤ３ネットワークルーティングは、ラストマイルエンドデバイス、すなわち送信元データフィールドに示される送信元ＩＰアドレスＩＰ　$C_{1,1}$を有するＳＤＮＰクライアント１４００、及び宛先アドレス$M_{0,0}$を有するＳＤＮＰゲートウェイ１４０１のみで構成される。前述のように、データフィールド３２３、３２４、３２５は、必ずしもＩＰｖ６データグラムデータペイロードの特定のセクションに対応するわけではない。ここでは、データフィールド３２３は、送信元ＩＰアドレス４４５、宛先ＩＰアドレス４４６、及びトランスポートヘッダ４３６を含むＳＤＮＰペイロードＡ　４３５の一部で構成される。データフィールド３２４及び３２５では、ＳＤＮＰペイロード４３５の未送信の残りの部分が伝送される。

【０５６７】

図５６Ｂには、セルラータワー及び基地局１４０２Ｑからモバイルクライアントデバイス１４００へのセルラーラストリンク１４０４経由の応答メッセージＳＤＮＰペイロードＧのデータパケットが示されている。ここでは、以前のデータパケットからの送信元アドレスと宛先アドレスが交換される。すなわち、セルラー送信元メディアアドレス３００Ａにメディアアドレス ＭＡＣ　ＢＳがロードされ、セルラー宛先メディアアドレス３００Ｂがクライアントの ＭＡＣアドレス、ＭＡＣ　$C_{1,1}$に、ＩＰＶ６データグラムの送信元ＩＰフィールド４４５がＩＰ　$M_{0,0}$に、そして宛先ＩＰフィールド４４５がＩＰ　$C_{1,1}$に設定される。ＢＳリンク１４１５を介したネットワークルータ１４０２Ｘとセルラータワー及び基地局１４０２Ｑとの間のルーティングでは、前例と一致するイーサネット（登録商標）データパケットが使用される。

【０５６８】

ラストリンクを介したマルチＰＨＹ通信には、様々な組み合わせで使用される前述の媒体のいずれかを含めることができる。マルチＰＨＹ実装には、同一または異なるデータレートでデータを伝送し、かつＵＳＢ、イーサネット（登録商標）１０ＢＡＳＥ－Ｔ、１００ＢＡＳＥ－Ｔ、１０００ＢＡＳＥ－Ｔ、ＤＯＣＳＩＳ３などの共通または異なるレイヤ２プロトコルを使用する複数の有線接続を含めることができる。有線物理媒体はイーサネ

ット（登録商標）またはＵＳＢ準拠のネットワークケーブル、同軸ケーブル、光ファイバ、またはＤＳＬ用のツイストペア銅線接続で構成できるが、性能は低下する。

【０５６９】

ワイヤレスマルチＰＨＹ通信には、無線周波数帯及びマイクロ波帯で実行されるＷｉＦｉ、セルラー、衛星、または独自の無線フォーマットの組み合わせを含めることができる。ワイヤレスラストリンク通信には、Ｂｌｕｅｔｏｏｔｈ（登録商標）などの短距離技術または日本のＰＨＳなどのマイクロセルラーネットワークを含めることもできる。ワイヤレスプロトコルには、アナログのＴＤＭＡ、ＧＳＭ、ＣＤＭＡ、ＵＭＴＳ、ＯＦＤＭ、または８０２．１１ａ、８０２．１１ｂ、８０２．１１ｇ、８０２．１１ｎ、８０２．１１ａｃなどのＷｉＦｉプロトコルを含む２Ｇ、２．５Ｇ、３Ｇ、４Ｇ／ＬＴＥのセルラーフォーマット、及び衛星通信またはカスタム無線リンクの独自のフォーマットが含まれる。レイヤ２プロトコルはレイヤ１の物理媒体によって異なるため、本開示の文脈で使用される用語「マルチＰＨＹ通信」は、ＯＳＩ物理レイヤとデータリンクレイヤの両方の組み合わせ、すなわちレイヤ１とレイヤ２の組み合わせを意味し、レイヤ１物理媒体のみを意味する主張に限定するものと解釈されるべきではない。

【０５７０】

図５７Ａには、イーサネット（登録商標）、ＷｉＦｉ、携帯電話の実装を含め、共通レイヤ２プロトコルが使用されるマルチＰＨＹ通信の例が示されている。最上部のマルチＰＨＹイーサネット（登録商標）の例では、それぞれ１００ＢＡＳＥ－Ｔと１０００ＢＡＳＥ－Ｔを実行する有線またはファイバリンク２４Ａと２４Ｂで構成される２つのイーサネット（登録商標）ケーブルが使用され、ルータ２７からデスクトップコンピュータ３６へ通信が行われる。ラストマイルにおけるハイパーセキュア通信が容易化されるように、ＳＤＮＰソフトウェア１３３５Ｃを実行するデスクトップ３６が示されている。

【０５７１】

中央のマルチＰＨＹ　ＷｉＦｉの例では、２．４ＧＨｚで８０１．１１ｎプロトコルを実行するＷｉＦｉリンク２９Ａ、及び５ＧＨｚの８０２．１１ａｃで通信するＷｉＦｉリンク２９Ｂとして示される２つのＷｉＦｉチャネルを通して、ＷｉＦｉルータ１００からノートブック３５へ通信が行われる。マルチＰＨＹモードで動作させるためには、ノートブックの内蔵マルチバンドアンテナ２６Ｂにより、ノートブック３５で複数の周波数で同時に信号を送受信できるようになっている必要がある。同様に、マルチバンドアンテナ２６により、ＷｉＦｉルータで複数の周波数で同時に信号を送受信できるようになっている必要がある。ラストマイルにおけるハイパーセキュア通信が容易化されるように、ＳＤＮＰソフトウェア１３３５Ｃを実行するノートブック３５が示されている。

【０５７２】

最下部のマルチＰＨＹセルラー通信の例では、対応する周波数１．８ＧＨｚ及び９００ＭＨｚのセルラーリンク２８Ａと２８Ｂを含む２つの異なる無線チャネルが使用され、マルチバンドセルラータワー１８Ａを介して、携帯電話基地局１７からタブレット３９へ同時に通信が行われる。示される例では、セルラーリンクは４Ｇ／ＬＴＥネットワークで構成される。示されるように、内蔵マルチバンドアンテナ１８Ｂにより、タブレット３９で複数の周波数で信号を同時に送受信できるようになっている必要がある。ラストマイルにおけるハイパーセキュア通信が容易化されるように、ＳＤＮＰアプリ１３３５Ａを実行する　タブレット３９が示されている。

【０５７３】

共通レイヤ２プロトコルが使用されるこうしたマルチＰＨＹ通信では、ハッカーはそれぞれに独自のセキュリティが含まれる２つの異なるレイヤ２データリンクに物理的にアクセスする必要があるため、これによりサイバー攻撃を混乱させることができる。さらに、クライアントがＳＤＮＰソフトウェア１３３５Ｃ、ＳＤＮＰアプリ１３３５Ａ、またはＳＤＮＰファームウェア１３３５Ｂ（図示なし）を実行している場合、マルチＰＨＹ接続でのＳＤＮＰペイロードのルーティングでは一意の動的セキュリティ認証情報が使用されるため、リアルタイムのハッキングによるＳＤＮＰパケットの傍受及び解釈は非常に困難と

なる。

【０５７４】

図５７Ｂには、混合のレイヤ１媒体とレイヤ２プロトコルが使用されるマルチＰＨＹ通信の例が示されている。この例では、ラストリンクデータの伝送に携帯電話、ＷｉＦｉ、衛星システムの組み合わせが使用される。最上部の混合媒体マルチＰＨＹ通信の例では、１００ＢＡＳＥ－Ｔイーサネット（登録商標）有線またはファイバリンク２４Ｂ及び５ＧＨｚで動作する８０２．１１ａｃ　ＷｉＦｉリンク２９Ｂの組み合わせが使用され、ＷｉＦｉルータ１００からデスクトップコンピュータ３６へ通信が行われる。ラストマイルにおけるハイパーセキュア通信が保証されるように、ＳＤＮＰソフトウェア１３３５Ｃを実行するデスクトップ３６が示されている。この例は、有線とワイヤレス通信の組み合わせである。この場合、ワイヤレスパケットスニッフィングでは有線データを傍受または監視できない。イーサネット（登録商標）とＷｉＦｉを混合したこのマルチＰＨＹラストリンクの分散方式は、アクセスが制限されたサーバルームに安全に収納されているプライベートサーバと通信する建物またはキャンパス内のセキュアなデスクトップコンピュータで構成される企業オフィスネットワークの展開に特に適している。

【０５７５】

図５７Ｂの中央の混合媒体によるマルチＰＨＹ通信の例では、２つの異なる無線技術が使用され、マルチバンドアンテナ１８Ｃを内蔵した携帯電話３２から通信が行われる。例として５ＧＨｚの８０２．１１ｎプロトコルが使用され、１つのＰＨＹ接続でＷｉＦｉリンク２９ＣからＷｉＦｉルータ１００及びアンテナ２６へ通信が行われる。２番目のＰＨＹ接続であるセルラーリンク２８Ｃでは、４Ｇ／ＬＴＥプロトコルで動作する１．８ＧＨｚキャリアが使用され、セルラータワー２５及び基地局１７へのラストリンク接続が容易化される。セルラータワー２５とＷｉＦｉアンテナ２６は無関係なシステムで動作するため、このマルチＰＨＹアプローチでは、ラストリンクの複数の物理媒体により伝送されるデータパケット間の関係が完全に隠される。ラストマイルにおけるハイパーセキュア通信が保証されるように、ＳＤＮＰアプリ１３３５Ａを実行する携帯電話３２が示されている。

【０５７６】

図５７Ｂの最下部の例には、セルラーと衛星を組み合わせたマルチＰＨＹラストリンク通信を実現する同様の方法が示されている。２つの長距離無線ネットワーク経由で、ＳＤＮＰアプリ１３３５Ａを実行する衛星／携帯電話３２Ｚから、１．８　ＧＨｚでセルラーリンク２８Ｄを介してセルラータワー２５及び基地局１７へ、そして例として１．９　ＧＨｚで衛星リンク９５Ｗを介して通信衛星９２へ通信が行われる。次に、広帯域リンク９５Ｘを介して、衛星９２から地上衛星アンテナ及び基地局９２Ｂへ通信が行われる。これは、クライアント通信と同じ周波数であるとは限らない。

【０５７７】

図５７Ｃには、別の様々なマルチＰＨＹ通信が示されている。この例では、共通プロトコルは共有されるが、周波数分割により複数の同時通信チャネルが可能な複数の物理媒体が挙げられている。こうしたシステムでは、動作の負荷が大きくなるほど、すなわちメディアの帯域幅とスループット能力を使用するユーザが多くなるほど性能が低下するため、高帯域幅の媒体が必要となる。このように帯域幅が非常に広い媒体で、現在利用できるものは３つのみである。すなわち、（ｉ）同軸ケーブルを使用するＤＯＣＳＩＳ３ケーブルシステム、（ｉｉ）光ファイバを使用するＤＯＣＳＩＳ　３ケーブルシステム、及び（ｉｉｉ）マルチＧＨｚの低高度軌道衛星通信システムである。具体的には、上部のマルチＰＨＹケーブルシステムの図では、複数の帯域が使用され、ＤＯＣＳＩＳ３プロトコルを実行する同軸またはファイバ１０５を介して、ＳＤＮＰファームウェア１３３５Ｍを実行するセットトップボックスまたはケーブルモデム１０２ＢからケーブルＣＭＴＳ　１０１へ通信が行われる。

【０５７８】

下部の図には、独自の通信プロトコルでフォーマットされた複数のキャリアバンド９５Ｚが使用され、ＳＤＮＰアプリ１３３５Ａを実行する衛星対応携帯電話３２Ｚから通信衛

星９２へ通信が行われるマルチＰＨＹ衛星ネットワークが示されている。衛星９２と地上衛星アンテナ及び基地局９２Ｂ間の通信では、数千の通話が混合されるトランクラインプロトコル９５Ｘが使用されることで、ハッカーが特定の通話を識別及び傍受することが困難となり、クライアントリンク９５Ｚにおける複数帯域でのマルチＰＨＹ通信の使用によりクライアントのハイパーセキュア通信が保証される。

【０５７９】

図５８には、マルチＰＨＹラストリンクルーティングで使用されるデータパケットの別の例が示されている。この図では、例としてそれぞれプロトコル１００ＢＡＳＥ－Ｔ及び１０００ＢＡＳＥ－Ｔを実行するイーサネット（登録商標）有線またはファイバリンク２４Ａと２４Ｂを含む２つの個別のＰＨＹ接続を介して、ＳＤＮＰクライアント１４００からルータ１４０２Ａへ通信が行われる。次に、ゲートウェイリンク１４１４を介して、ルータ１４０２ＡがＳＤＮＰゲートウェイ１４０１に接続される。両方のイーサネット（登録商標）パケットにより、送信元ＩＰアドレス４４５、すなわちクライアントデバイスがＩＰ　$C_{1,1}$として、ＳＤＮＰゲートウェイの宛先ＩＰアドレス４４６がＩＰ　$M_{0,0}$として定義される。有線またはファイバリンク２４Ａにより実現するＰＨＹ経由でルーティングされるイーサネット（登録商標）パケットＡには、ＭＡＣ　Ｒを含む宛先ＭＡＣアドレス１８２及びＭＡＣ　$C_{1,1}$を含む送信元ＭＡＣアドレス１８３が含まれる。有線またはファイバリンク２４Ｂにより実現するＰＨＹ経由でルーティングされるイーサネット（登録商標）パケットＢには、ＭＡＣ　Ｒを含む宛先ＭＡＣアドレス１８２及びＭＡＣ　$C_{1,2}$を含む異なる送信元ＭＡＣアドレス１８３が含まれる（これにより、代替ＰＨＹ接続が定義される）。

【０５８０】

送信元メディアアドレスがＭＡＣ　$C_{1,1}$からＭＡＣ　$C_{1,2}$に変化することで、イーサネット（登録商標）通信が２．６ＧＨｚの１００ＢＡＳＥ－Ｔ接続から１０００ＢＡＳＥ－Ｔ接続にリダイレクトされる。動作中、ＳＤＮＰクライアントデバイス１４００からのデータパケットは断片化され、次にＳＤＮＰアルゴリズム及び共有秘密に従ってＳＤＮＰペイロードＡとＳＤＮＰペイロードＢに配分される。有線またはファイバリンク２４Ａ経由のイーサネット（登録商標）パケットＡで伝送されるＳＤＮＰペイロードＡ、及び有線またはファイバリンク２４Ｂ経由のイーサネット（登録商標）パケットＢで伝送されるＳＤＮＰペイロードＢにより、断片化されたデータがマルチＰＨＹラストリンクを介して転送される。

【０５８１】

図５９には、マルチＰＨＹラストリンクルーティングで使用されるデータパケットの別の例が示されている。この図では、例としてそれぞれ２．４ＧＨｚの８０２．１１ｎプロトコル及び５ＧＨｚの８０２．１１ａｃプロトコルが使用され、ＷｉＦｉリンク２９Ａ及び２９Ｂを含む２つの別個のＰＨＹ接続を介して、ＳＤＮＰクライアント１４００からＷｉＦｉルータ１４０２Ｗへ通信が行われる。次に、ＢＳリンク１４１５を介して、ルータ１４０２Ｗがルータ１４０２Ｘに接続され、ゲートウェイリンク１４１４を介して、ルータ１４０２ＸがＳＤＮＰゲートウェイ１４０１に接続される。両方のＷｉＦｉパケットにより、送信元ＩＰアドレス４４５、すなわちクライアントデバイスがＩＰ　$C_{1,1}$として、ＳＤＮＰゲートウェイの宛先ＩＰアドレス４４６がＩＰ　$M_{0,0}$として定義される。ＷｉＦｉリンク２９Ａにより実現するＰＨＹ経由でルーティングされるＷｉＦｉパケットＡには、ＭＡＣ　$C_{1,1}$を含む無線送信機送信元ＭＡＣアドレス２３６、ＭＡＣ　Ｗを含む無線受信機宛先ＭＡＣアドレス２３５、及びＭＡＣ　Ｒを含むネットワーク宛先ＭＡＣ　２３７が含まれる。ＷｉＦｉリンク２９Ｂにより実現するＰＨＹ経由でルーティングされるＷｉＦｉパケットＢには、ＭＡＣ　$C_{1,2}$を含む無線送信機送信元ＭＡＣアドレス２３６、ＭＡＣ　Ｗを含む無線受信機宛先ＭＡＣアドレス２３５、及びＭＡＣ　Ｒを含むネットワーク宛先ＭＡＣ　２３７が含まれる。

【０５８２】

送信元メディアアドレスがＭＡＣ　$C_{1,1}$からＭＡＣ　$C_{1,2}$に変化することで、送

信が２．６ＧＨｚのＷｉＦｉ無線から５ＧＨｚトランシーバにリダイレクトされる。動作中、ＳＤＮＰクライアントデバイス１４００からのデータパケットは断片化され、次にＳＤＮＰアルゴリズム及び共有秘密に従ってＳＤＮＰペイロードＡとＳＤＮＰペイロードＢに配分される。ＷｉＦｉリンク２９Ａ経由のＷｉＦｉパケットＡで伝送されるＳＤＮＰペイロードＡ、及びＷｉＦｉリンク２９Ｂ経由のＷｉＦｉパケットＢで伝送されるＳＤＮＰペイロードＢにより、断片化されたデータがマルチＰＨＹラストリンクを介して転送される。

【０５８３】

図６０には、マルチＰＨＹラストリンクルーティングで使用されるデータパケットのさらに別の例が示されている。この図では、例としてそれぞれ１．８ＧＨｚの４Ｇ／ＬＴＥプロトコル及び９００ＭＨｚの４Ｇ／ＬＴＥプロトコルが使用され、セルラーリンク２８Ａ及び２８Ｂを含む２つの個別のＰＨＹ接続を介して、ＳＤＮＰクライアント１４００からセルラータワー１４０２Ｑへ通信が行われる。次に、ＢＳリンク１４１５を介して、ルータ１４０２Ｑがルータ１４０２Ｘに接続され、ゲートウェイリンク１４１４を介して、ルータ１４０２ＸがＳＤＮＰゲートウェイ１４０１に接続される。両方のセルラー無線パケットにより、送信元ＩＰアドレス４４５、すなわちクライアントデバイスがＩＰ　$C_{1,1}$として、ＳＤＮＰゲートウェイの宛先ＩＰアドレス４４６がＩＰ　$M_{0,0}$として定義される。セルラーリンク２８Ａにより実現するＰＨＹ経由でルーティングされるセルラーパケットＡには、ＭＡＣ　$C_{1,1}$を含む無線送信機送信元ＭＡＣアドレス３００Ａ及びＭＡＣ　ＢＳを含むセルラータワー宛先ＭＡＣアドレス３００Ｂが含まれる。セルラーリンク２８Ｂにより実現されるＰＨＹ経由でルーティングされるセルラーパケットＢには、ＭＡＣ　$C_{1,2}$を含む無線送信機送信元ＭＡＣアドレス３００Ａ及びＭＡＣ　ＢＳを含むセルラータワー宛先ＭＡＣアドレス３００Ｂが含まれる。

【０５８４】

送信元メディアアドレスがＭＡＣ　$C_{1,1}$からＭＡＣ　$C_{1,2}$に変化することで、送信が１．８ＧＨｚの４Ｇ／ＬＴＥセルラー無線から９００ＭＨｚにリダイレクトされる。動作中、ＳＤＮＰクライアントデバイス１４００からのデータパケットは断片化され、次にＳＤＮＰアルゴリズム及び共有秘密に従ってＳＤＮＰペイロードＡとＳＤＮＰペイロードＢに配分される。ＷｉＦｉリンク２８Ａ経由のセルラーパケットＡで伝送されるＳＤＮＰペイロードＡ、及びＷｉＦｉリンク２８Ｂ経由のセルラーパケットＢで伝送されるＳＤＮＰペイロードＢにより、断片化されたデータがマルチＰＨＹラストリンクを介して転送される。

【０５８５】

前述のように、マルチＰＨＹ通信には異種の媒体を含めることもできる。その場合、各接続のデータパケットを、対応する物理媒体のレイヤ２プロトコルに従ってフォーマットする必要がある。例えば、図６１には、イーサネット（登録商標）とＷｉＦｉを含むハイブリッドラストリンク通信が示されている。この図では、例としてそれぞれ５ＧＨｚの１００ＢＡＳＥ－Ｔ及び８０２．１１ａｃが使用され、イーサネット（登録商標）有線またはファイバリンク２４ＡとＷｉＦｉリンク２９Ｂを含む２つの個別のＰＨＹ接続を介して、ＳＤＮＰクライアント１４００からＷｉＦｉルータ１４０２Ｗへ通信が行われる。次に、ＢＳリンク１４１５を介して、ルータ１４０２Ｗがルータ１４０２Ｘに接続され、ゲートウェイリンク１４１４を介して、ルータ１４０２ＸがＳＤＮＰゲートウェイ１４０１に接続される。両方のＷｉＦｉパケットにより、送信元ＩＰアドレス４４５、すなわちクライアントデバイスがＩＰ　$C_{1,1}$として、ＳＤＮＰゲートウェイの宛先ＩＰアドレス４４６がＩＰ　$M_{0,0}$として定義される。有線またはファイバリンク２４Ａにより実現するＰＨＹ経由でルーティングされるイーサネット（登録商標）Ａには、ＭＡＣ　$C_{1,1}$を含む送信元ＭＡＣアドレス１８３及びＭＡＣ　Ｗを含む宛先ＭＡＣアドレス１８２が含まれる。ＷｉＦｉリンク２９Ｂにより実現するＰＨＹ経由でルーティングされるＷｉＦｉパケットＢには、ＭＡＣ　$C_{1,2}$を含む無線送信機送信元ＭＡＣアドレス２３６、ＭＡＣ　Ｗを含む無線受信機宛先ＭＡＣアドレス２３５、及びＭＡＣ　Ｒを含むネットワーク宛先ＭＡＣ

２３７が含まれる。

【０５８６】

送信元メディアアドレスがＭＡＣ　Ｃ$_{1,1}$からＭＡＣ　Ｃ$_{1,2}$に変化することで、送信がイーサネット（登録商標）からＷｉＦｉにリダイレクトされる。動作中、ＳＤＮＰクライアントデバイス１４００からのデータパケットは断片化され、次にＳＤＮＰアルゴリズム及び共有秘密に従ってＳＤＮＰペイロードＡとＳＤＮＰペイロードＢに配分される。有線またはファイバリンク２４Ａ経由のイーサネット（登録商標）パケットＡで伝送されるＳＤＮＰペイロードＡ、及びＷｉＦｉリンク２９Ｂ経由のＷｉＦｉパケットＢで伝送されるＳＤＮＰペイロードＢにより、断片化されたデータがマルチＰＨＹラストリンクを介して転送される。

【０５８７】

図６２は、ＷｉＦｉ通信とセルラー通信で構成されるハイブリッド型ラストリンク通信の仕組みを示している。ここで、ＳＤＮＰクライアント１４００は２つの異なる物理接続を通じて２つの異なる無線基地局に接続している。具体的には、Ｗｉｆｉリンク２９Ａは２．４ＧＨｚ、８０２．１１ｎのＷｉＦｉルータ１４０２Ｗに、セルラーリンク２８Ｂはキャリア周波数帯９００ＭＨｚ、４Ｇ／ＬＴＥでステーション１４０２Ｑに接続している。ルータ１４０２Ｗと１４０２Ｑは、それぞれＢＳリンク１４１５Ａ及び１４１５Ｂを介してルータ１４０２Ｘに接続し、ルータ１４０２Ｘはゲートウェイリンク１４１４を介してＳＤＮＰゲートウェイ１４０１に接続している。ＷｉＦｉと４Ｇセルラーのパケットはいずれも、接続元ＩＰアドレス４４５、つまりクライアントデバイスをＩＰ　Ｃ$_{1,1}$と定義し、ＳＤＮＰゲートウェイの接続先ＩＰアドレス４４６をＩＰ　Ｍ$_{0,0}$と定義している。ＷｉＦｉリンク２９Ａを構成する接続を介して物理層でルーティングされるＷｉＦｉパケットＡは、ＭＡＣ　Ｃ$_{1,1}$を構成するトランスミッタＭＡＣ無線接続元アドレス２３６、ＭＡＣ　Ｗを構成するＭＡＣ無線受信機接続先アドレス２３５、及びＭＡＣ　Ｒを構成するＭＡＣネットワーク接続先２３７が含まれる。ＷｉＦｉリンク２９Ｂによって実現される物理層接続としてルーティングされるセルラーＢには、ＭＡＣ　Ｃ$_{1,2}$を構成するＭＡＣ接続元アドレス３００Ｂ、及びＭＡＣ　ＢＳを構成するＭＡＣ接続先３００Ｂが含まれる。

【０５８８】

ＭＡＣ　Ｃ$_{1,1}$からＭＡＣ　Ｃ$_{1,2}$に接続先メディアアドレスを変更すると、送信はＷｉＦｉ　ＬＡＮからセルラーネットワークにリダイレクトされる。動作中、ＳＤＮＰクライアントデバイス１４００からのデータパケットは断片化されてから、ＳＤＮＰアルゴリズム及び共有秘密に従ってＳＤＮＰペイロードＡ及びＳＤＮＰペイロードＢに割り当てられる。マルチＰＨＹラストリンクを介した断片化されたデータの転送は、ＷｉＦｉリンク２９Ａを介してＷｉＦｉパケットＡにより搬送されるＳＤＮＰペイロードＡと、セルラーリンク２８Ｂでセルラーパケットにより搬送されるＳＤＮＰペイロードＢによって実行される。

【０５８９】

マルチＰＨＹ通信には物理メディアを用いる形式もあり、この場合は様々な周波数で多数のチャネルをサポートし、各々のデータパケットに異なるプロトコルを使用することができる。このような実装は、ＳＤＮＰソフトウェアを実行するＤＯＣＳＩＳ３ベースのケーブル配信システムを使用することで簡素化できる。ＳＤＮＰ対応のＤＯＣＳＩＳ３ケーブル配信システムのＯＳＩＤ通信スタックを図６３に示す。この図には、レイヤ１のＰＨＹ接続及びレイヤ２のデータリンクに加え、ケーブルモデム終端装置ＣＭＴＳ　１０１、及びケーブルモデムＣＭ　１０３やセットトップボックスＳＴＢ　１０２といったケーブル接続装置をカバーするレイヤ３のネットワークが示されている。具体的には、ケーブルモデム終端システム装置ＣＭＴＳ　１０１及びその関連スタック３７８には、クラウドサーバ２２及びインターネット２０、あるいはビデオヘッドエンド、ＩＰＴＶシステム、またはＶｏＩＰシステム（図示せず）に接続されるレイヤ１　ＰＨＹネットワークインターフェイス３６１が含まれている。ネットワークインターフェイス３６１とデータリンク層３

６６の組み合わせは、ＣＭＴＳ　１０１のデバイスインターフェイス通信スタック３７８に含まれている。データリンクレイヤ２では、データはネットワークインターフェイス通信スタックからケーブルネットワークインターフェイス通信スタックへと、転送機能３７０を介して、具体的にはリンクレベル制御ＬＬＣ　３６９に引き渡される。リンクレベル制御８０２．２　ＬＬＣ　３６９は、ＩＥＥＥ仕様８０２．２に従って定義された非ハードウェア依存プロトコルで構成されている。このパケットデータは次に、リンクセキュリティ３６８によって変更されて基本的なパケットセキュリティが施される。これは主にペイパービューユニキャストブロードキャストなどのコンテンツの不正視聴の防止を目的として行われる。

【０５９０】

その後、レイヤ１　ＰＨＹケーブルインターフェイス３６２は、同軸ケーブル１０４または光ファイバ９１のいずれかで構成される配信ネットワーク１０２を介して、ケーブルモデムＣＭ１０３またはセットトップボックスＳＴＢ１０２内の対応するレイヤ１　ＰＨＹケーブルインターフェイス３６３にデータフレームを送信する。ケーブルインターフェイス３６３は、ケーブルモデムＣＭ１０３またはセットトップボックスＳＴＢ１０２のＯＳＩＯ通信スタック３７９として示されるケーブルネットワークインターフェイスのＰＨＹ層を表す。データパケットを受信すると、ケーブルＭＡＣインターフェイス３７１はケーブルのＭＡＣアドレスを解釈し、そのペイロードを復号のためにリンクセキュリティ３７２に渡し、最終的にハードウェア非依存のリンク層制御８０２．２　ＬＬＣ　３７３に渡して解釈可能にする。ＣＭまたはＳＴＢケーブルネットワーク通信スタックへの入力データは次に、トランスペアレントブリッジング３７４を介してＣＭまたはＳＴＢデバイスインターフェイス通信スタック（具体的にはＩＥＥＥ　８０２．２の仕様に従ってデバイス独立リンク層制御８０２．２　ＬＬＣ　３７５）へと渡される。このパケットは次にＨＳＤ＆ＩＰＴＶ　ＭＡＣブロック３７６またはＷｉＦｉ　８０２．１１　ＭＡＣブロック３７７に渡され、パケットのＭＡＣアドレスが更新される。ＷｉＦｉ通信の場合、データパケットは次にＷｉＦｉアンテナ２６で送信するため、８０２．１１　ＭＡＣブロック３７７からＷｉＦｉ　ＰＨＹレイヤ１無線インターフェイス３６５に渡される。有線接続の場合、データパケットは、ＴＶ　３９またはデスクトップ３６に接続するため、ＨＳＤ及びＩＰＴＶ　ＭＡＣブロック３７６からイーサネット（登録商標）またはＨＤＭＩ（登録商標）インターフェイスブロック３６４に渡される。

【０５９１】

ＰＨＹ層とデータリンク層は、すでに説明したように、ＣＭＴＳから任意の数のケーブルモデム（ＣＭ）への接続を確立する。ＣＭＴＳ通信スタック３７８内及びＣＭ通信スタック３７９内では、データパケットは、ケーブルネットワークまたはインターネットのＤＮＳネームサーバによって認識されるＩＰアドレスを使用して、ＩＰデータグラムＩＰｖ４、ＩＰｖ６またはＩＣＭＰｖ６として、ＯＳＩレイヤ３のレイヤ３６０Ａと３６０Ｂ内でそれぞれ準備される。ラストマイル通信では、ＳＤＮＰの接続元または接続先のＩＰアドレスを持つＩＰｖ４またはＩＰｖ６データパケットを使用するＳＤＮＰデータグラムは通常、使用できない。これは、ＳＤＮＰソフトウェアまたはファームウェアによって有効にされていない接続デバイスは、ＳＤＮＰデータグラムのルーティングアドレスを解釈することができないからである。

【０５９２】

ケーブルモデムネットワーク内のトランスポートレイヤ４の動作は、デバイスによって異なる。ＣＭＴＳ　１０１の場合、ＯＳＩ通信スタック３７８のレイヤ４トランスポートレイヤ１４２０は、その動作にリアルタイム通信を必要とするため（例えば　ビデオデータのストリーミング）、ＵＤＰを排他的に使用する。このことから、ケーブル通信１０２は、インターネットよりもＳＤＮＰリアルタイムネットワーク的と言える。ケーブルモデムは、クライアント（つまり、エンド通信デバイス）としてインターネットともケーブルネットワークとも相互運用性があるため、ＣＭ　１０３またはＳＴＢ　１０２のＯＳＩ通信スタック３７９のレイヤ４トランスポート層１４２０Ｂは、リアルタイム運用にはＵＤＰ

を使用し、インターネットデータにはＴＣＰを使用している。このような使用法は、ＶｏＩＰ　ｏｖｅｒ　Ｉｎｔｅｒｎｅｔを使用するＯＴＴキャリアにとっては好ましくない。ケーブルネットワークでは、ＩＰデータグラムをデータとして解釈し、ＴＣＰとトランスポートプロトコルを自動的に使用するため、リアルタイム通信のＱｏＳ、レイテンシー、及び伝播遅延に問題を発生させるからである。　この問題は、ＳＤＮＰ対応のケーブルモデムでは発生しない。ＣＭまたはＳＴＢがＳＤＮＰファームウェアやソフトウェアを実行しているとき、ＳＤＮＰソフトウェアは、ＴＣＰの使用をいつ保証し（ソフトウェアやファイルに対して）、いつ保証しないのか（つまり、リアルタイムデータに対して）を状況に応じて決定している。

【０５９３】

アプリケーション層、つまりＯＳＩ層５～７は、ＣＭＴＳ　１０１ではトランスポート層のオペレーション１４２０Ａの上、ＣＭ　１０３またはＳＴＢ　１０２ではトランスポート層１４３０Ｂの上に位置している。ＣＭＴＳ　１０１では、これらのアプリケーションは通常、ＩＰネットワーク上の情報接続デバイスを収集及び整理するためのインターネット標準プロトコルであるＳＮＭＰ　１４３１Ａなどの通信タスクを処理する。その他の機能として、ＤＨＣＰｖ４　１４３２Ａ及びＤＨＣＰｖ６　１４３３Ａがある。ＤＨＣＰ（動的ホスト構成プロトコルの頭字語）は、動的に生成された（非静的）ＩＰアドレス、デフォルトゲートウェイ、及びサブネットマスクなどの必要なルーティング情報をＩＰホストに自動的に提供するクライアントとサーバの両方のプロトコルである。インターネットの生成に特有のものであるが（つまり、ＩＰｖ４またはＩＰｖ６）、ＮＡＴゲートウェイやＳＮＭＰなどの動的ＩＰアドレス生成機能は汎用的であり、ＣＭＴＳ　１０１とＣＭ　１０３の両方、またはＳＴＢ　１０２のＤＯＣＳＩＳ３ケーブルシステムに等しく適用される。

【０５９４】

本明細書で開示されるセキュア動的通信ネットワーク及びプロトコルのアプリケーション層の実装は、ＣＭＴＳ　１０１オペレーティングシステム上で動作するＳＤＮＰファームウェア１４３０Ａとして実現される場合、以下を含む任意の数のユニークなタスクを実行できる。

・ＳＤＮＰペイロード１４３０を解釈せずにパススルーとして動作。この場合、ＣＭ　１０３を有効にしてＳＤＮＰペイロードをオープンし読み取る必要がある。つまり、ＣＭ　１０３はＳＤＮＰクライアントでなければならない。

・ラストマイルリモートＳＤＮＰゲートウェイとして動作。つまり、ＳＤＮＰペイロードのコンテンツを解釈し、ＣＭ　１０３に転送するためにコンテンツをＤＯＣＳＩＳ３固有のメッセージ（リンクセキュリティを含む）に変換する。このような場合、ＣＭ　１０３はＳＤＮＰクライアントソフトウェアまたはファームウェアを実行する必要はない。

・ラストマイルＳＤＮＰブリッジとして動作。ＩＰデータグラムをＳＤＮＰデータグラムに変換し、ＳＤＮＰデータグラムをＣＭ　１０３に送出する。この場合、ＣＭ　１０３はＳＤＮＰクライアントソフトウェアまたはファームウェアを実行してＳＤＮＰブリッジに接続する必要がある。つまり、アドホックＳＤＮＰ「フローティング」ネットワークを形成する必要がある。

【０５９５】

図に示されるように、ＣＭ１０３及びＳＴＢ１０２のＯＳＩ通信スタック３７９には、前出の通信関連アプリケーションＳＮＭＰ１４３１Ｂ、ＤＨＣＰｖ４　１４３２Ｂ、及びＤＨＣＰｖ６　１４３３Ｂをはじめとする、ＯＳＩレイヤ５～７として分類される多くのアプリケーションが含まれている。もうひとつの機能であるユーティリティＴＦＴＰ　１４３４Ｂ（簡易ファイル転送プロトコル）は、主にＤＯＣＳＩＳ３でソフトウェア及びソフトウェアの更新版をＣＭＴＳからケーブルネットワーク全体にわたるケーブルモデム及びセットトップボックスにダウンロードする手段として使用される。ケーブルネットワークでは、ＨＴＴＰ　１４３５Ｂ、すなわちハイパーテキスト転送プロトコルが、主にスマートテレビで有用な動的メニューの表示に使用される。その他のアプリケーション（「Ｏｔｒ」１４３６Ｂと略記されている）としては、ゲームアプリ、診断、ＩＰＴＶアプリ、

ビデオ録画機能などが存在する。ＣＭ　１０３またはＳＴＢ　１０２で実行されているＳＤＮＰファームウェア１４３０Ｂが拡張され、ＣＭＴＳ　１０１がＳＤＮＰソフトウェアを実行しているかどうかに関係なく、ハイパーセキュアラストマイル通信とすべてのユーザ及びラストリンクとの接続が確立される。

【０５９６】

図６４は、ＳＤＮＰペイロード１４３０を配信するように適合化されたＤＯＣＳＩＳ３データパケットの構造を示している。図に示されるように、ＰＨＹレイヤ１は、可変長及び可変持続時間の物理メディアデバイスフレーム３９０を含み、プリアンブル３９１、可変長ペイロードまたはコードワード３９２、及びガードタイム３９３を含むデータリンクレイヤ２　ＭＡＣデータを含んでいる。プリアンブル３９１は、通信の方向に応じて、アップストリームプリアンブルまたはダウンストリームプリアンブルのいずれかを含む。アップストリームプリアンブルの場合、プリアンブル３９１は、物理メディアデバイスＰＭＤヘッダ３９８、ＭＡＣヘッダ３９９Ａ、及びデータＰＤＵ４００Ａを含む。ダウンストリームプリアンブルの場合、プリアンブル３９１は、ＭＰＥＧヘッダ４０１、ＭＡＣヘッダ３９９Ｂ、及びデータＰＤＵ４００Ｂを含む。アップストリームプリアンブルのデータＰＤＵ　４００Ａとダウンストリームプリアンブルのデータ　ＰＤＵ　４００Ｂは、ＭＡＣ宛先アドレス（ＤＡ）４０３ＢとＭＡＣ送信元アドレス（ＳＡ）４０３Ａを含む。可変長ペイロード３９２のコンテンツは、ショートコードワード３９４またはロングコードワード３９７を含むことができる。

【０５９７】

ショートコードワード３９４は、データＡを有するペイロード３９５Ａ及びＦＥＣ　Ａを有するエラー訂正３９６Ａを含む。ロングコードワード３９７の場合、ペイロードは、データＡ、データＢ、及びデータＣを搬送する複数のペイロードブロック３９５Ａ、３９５Ｂ、及び３９５Ｃに分割される。各ペイロードは、対応するデータＦＥＣ　Ａ、ＦＥＣ　Ｂ、及びＦＥＣ　Ｃを有する独自のエラーチェックブロック３９６Ａ、３９６Ｂ、及び３９６Ｃを含む。エラーチェック後、ＤＯＣＳＩＳ３から配信されたデータは、ロングコードワードの場合にはデータブロック３９５Ａ、３９５Ｂ、及び３９５Ｃを含み、ショートコードワードの場合はデータブロック３９５Ａのみを含む。データＡ、データＢ、及びデータＣの組み合わせは、ひとつの連続するＩＰデータグラム、この例ではひとつのＩＰｖ６データグラムにまとめられる。これには、ＩＰ送信元アドレス４４５、ＩＰ宛先アドレス４４６、及びＳＤＮＰペイロード１４３０を含むデータフィールド４３５、及びレイヤ４データを含むトランスポートヘッダ４３６が含まれる。このように、ＤＯＣＳＩＳ３は、パケット交換データプロトコルを使用して、ケーブルネットワーク上でデータを柔軟に配信する。

【０５９８】

図６５Ａに示されるように、データパケットはハイブリッドケーブルファイバネットワーク上の複数のチャネル、つまり、異なる周波数で伝送される。ＤＯＣＳＩＳ３．０では、データチャネルの周波数範囲は５ＭＨｚ～１，００２ＭＨｚであり、これにはアナログＴＶ信号１４４０（トライアングル）、ＱＡＭデータ１４４１、及び「ダイプレクサー」制御チャネル１４４３が含まれる。ＤＯＣＳＩＳ　３．１のフェーズ１では、周波数範囲が１，２１８ＭＨｚに拡張されるとともに、ＤＯＣＳＩＳ３．１データチャネル１４４２が追加されて、主にＱＡＭに割り当てられている現行チャネルより上の周波数帯域におけるＯＦＤＭ変調を容易化している。

【０５９９】

ＯＦＤＭは、チャネルの間隔をより狭くできる点で、ＱＡＭ変調方式よりも好まれている。変調方式を比較すると、ＱＡＭ周波数分布１４４５Ａは、ＯＦＤＭ周波数分布１４４５Ｂよりもスペクトル成分の裾が広くなっている。具体的には、f_0からf_{-50}までのスペクトル側波帯幅、すなわちキャリアエッジから信号が-５０ｄＢ低下する周波数までの帯域幅は、ＱＡＭ周波数分布１４４５Ａで４．３正規化周波数単位だが、ＯＦＤＭ周波数分布１４４５Ｂではわずか０．４正規化周波数単位である。スペクトルの幅が狭いため、よ

り多くの通信チャネルを同じスペクトルに収めることができ、ネットワーク全体の帯域幅と最大総データレートが増加する。ＤＯＣＳＩＳ　３．１のフェーズ２の展開では、周波数範囲が１，７９４ＭＨｚに拡張されている。ＱＡＭデータ１４４１に元々割り当てられていた帯域の多くは、ＯＦＤＭデータ１４４２に明示的に割り当てられた新しいチャネルに置き換えられる。

【０６００】

ＤＯＣＳＩＳ対応のケーブルネットワークでは、１つのＣＭＴＳユニットで多くのＣＭをサポートし利用可能なチャネルを管理できる。ＣＭＴＳは必要に応じてダウンストリーム通信とチャネル選択を動的に割り当てることができるが、アップストリーム通信では、複数のＣＭが同時にデータを送信しようとする状況に容易に対応できるようにするため、コンテンション管理が必要となる。そのため、各モデムは、データを送信する前にＣＭＴＳからアップリンクチャネルを要求しなければならない。このプロセスを図６５Ｂに示す。このプロセスは、ＳＤＮＰアプリ１３３５Ｌを実行するＣＭＴＳ１０１とＳＤＮＰファームウェア１３３５Ｍを実行するＣＭ１０３との間で行われる一連の通信操作で構成されている。マルチＰＨＹ通信でのＩＰデータグラムのルーティングでは、ＩＰアドレス「ＩＰ　ＣＭＴＳ」と「ＩＰ　ＣＭ１」、及び複数のＭＡＣアドレスを使用する。例えば、ＣＭ１０３には「ＭＡＣ　ＣＭ１」、ＣＭＴＳ　１０１には「ＭＡＣ　ＣＭＴＳ１」、「ＭＡＣ　ＣＭＴＳ２」、「ＭＡＣ　ＣＭＴＳ３」、及び「ＭＡＣ　ＣＭＴＳ４」を使用する。周波数対時間のグラフを示す最上部の図で、ＣＭ　１０３は、専用チャネル上でＲＱＳＴ　１４４５Ａの送信要求を出す。

【０６０１】

応答が得られないと、２番目のＲＱＳＴ　１４４５Ｂが送信され、ＭＡＰデータパケット１４４６の形式で、別のチャネル上のＣＭＴＳ　１０１から応答を得る。ＭＡＰデータパケット１４４６のコンテンツは、ＣＭ１０３に送信するタイミングと、アップストリーム通信に使用できるチャネルを指示するものである。ＭＡＰデータパケット１４４６を受信した後、ＣＭ１０３は、アップリンクデータパケット１４４７Ａ及び１４４７Ｂの２つのチャネル上を並行して流れるそれ自身のアップストリームデータを送信する。中央の図に示されている２つのチャネルで同時に送信されるデータの分割のことを、チャネルボンディングと呼んでいる。チャネルボンディングは、ＣＭＴＳとＣＭ間の通信帯域幅とデータレートを増加させる手段である。また、使用可能な帯域幅が未使用にならないようにするための動的な手段でもある。下の図で、ＣＭＴＳ　１０１は４つのチャネル（１４４８Ａ、１４４８Ｂ、１４４８Ｃ、１４４８Ｄ）をチャネルボンディングし、並行して、かつ異なる期間のデータを送信することによって応答する。

【０６０２】

ハイブリッドファイバケーブルネットワークを介したアップストリームとダウンストリームの両通信では、帯域幅は複数のチャネル間で動的に割り当てられ、「ミニスロット」と呼ばれる小さな時間セグメントに分割される。図６５Ｃは、ＣＭ１０３からＣＭＴＳ１０１へのアップストリーム通信を示している。このようなアップストリーム通信には、一般的にひとつのメッセージまたは送信要求が含まれている。図の例では、合計５つのタイムミニスロットで構成される周波数ｆ１及びｆ２でデータが送信される。図の通り、ミニスロット１、２、及び３はＫ、（Ｋ＋１）、及び（Ｋ＋２）の時間間隔で周波数ｆ１で送信され、ミニスロット４及び５はＫ及び（Ｋ＋１）の時間間隔で周波数ｆ２で送信され、（Ｋ＋２）では送信されない。要約形式で示されているアップストリームデータパケット１４５０Ａは、ＩＰ送信元アドレス「ＩＰ　ＣＭ１」及びラストマイル通信のＩＰ宛先アドレス、すなわちサーバ１２０１Ａによってホストされるネットワークのゲートウェイノードである「ＩＰ　$M_{0,0}$」を指定している。

【０６０３】

ラストリンク通信の場合、アップストリームデータパケット１４５０Ａは、ケーブルモデムの送信元ＭＡＣアドレスとして「ＭＡＣ　ＣＭ１」を指定し、またＰＨＹ媒体、この場合はＭＡＣ宛先「ＭＡＣ　ＣＭＴＳ１」として周波数f_1のチャネルを指定する。ＳＤ

ＮＰペイロードＡを含むデータパケット１４５０Ａは、まとめて１つのデータパケットとペイロードを伝送しているにもかかわらず、合計３つのミニスロット、すなわちミニスロット１、２、及び３を占有する。ただし、これら３つのミニスロット全体で１つのデータパケット及びペイロードを伝送する。これと対照的に、ミニスロット４とミニスロット５にはそれぞれ１つのデータパケットのみが含まれる。つまり、１４５０Ｂ及び１４５０Ｃにそれぞれ対応するデータＳＤＮＰペイロードＢとＳＤＮＰペイロードＣが含まれている。データパケット１４５０Ａと同様、パケット１４５０Ｂと１４５０Ｃはいずれも、ＳＤＮＰクラウドの宛先ＩＰアドレス、具体的にはＳＤＮＰゲートウェイノード$M_{0,0}$を指定している。

【０６０４】

ただし、ＭＡＣ宛先アドレスに関しては、最初のパケットと同じＭＡＣアドレスと物理メディアを指定するのではなく、パケット１４５０Ｂと１４５０Ｃの両方がＭＡＣ宛先アドレス「ＭＡＣ　ＣＭＴＳ２」を指定する。このアドレスを使用して、データパケット１４５０Ｂ及び１４５０Ｃをデータパケット１４５０Ａとは異なる周波数（この場合は周波数f_1ではなく周波数f_2）で伝送するように指定できる。これらの周波数の実際の値は、ＣＭＴＳ　１０１によって動的にマッピングされ、具体的には指定されない。したがって、ＤＯＣＳＩＳ３対応システムはマルチＰＨＹソリューションであり、単一のＣＭＴＳユニットで複数の周波数で、２５６　ＱＡＭやＯＦＤＭなどの複数のプロトコルを使用してケーブルモデムまたはセットトップボックスと同時通信が可能である。

【０６０５】

ＤＯＣＳＩＳ３システムの一般的なケースと同様にＣＭ及びＣＭＴＳがどのデータパケットが共通のキャリアチャネルまたは周波数を使用するかを決定できるようにするのではなく、ラストマイル通信の開示されたセキュアな動的通信ネットワーク及びプロトコルに従い、ＳＤＮＰクライアントＣＭ　１０３は異なるＭＡＣ宛先アドレスを指定して、複数の周波数とチャネルでの通信（つまりマルチＰＨＹの運用）を強制する。ＣＭ　１０３のデータパケット１４５０Ａ及び１４５０Ｂ／Ｃは、別々の宛先ＭＡＣアドレス、すなわちそれぞれＭＡＣ　ＣＭＴＳ１及びＭＡＣ　ＣＭＴＳ２を指定しているため、これらのデータパケットはラストリンクを介してマルチＰＨＹ動作を自動的に起動する。代替手段として、ＣＭＴＳが一意のチャネル割り当てを要求する別の容易な方法をとる場合（例えば、コマンドや制御要求を用いるなど）、ＭＡＣアドレスを使用してマルチＰＨＹ通信を呼び出す方法の代わりに、この代替手段を用いることができる。

【０６０６】

図６５Ｄは、ＣＭＹＳ１０１からＣＭ１０３へのダウンストリームデータフロー図、マルチＰＨＹダウンストリーム通信において高データレートを達成するためのボンディングの使い方を示している。図に示されるように、すべてのデータパケットは、「ＩＰ　ＣＭＴＳ」の送信元ＩＰアドレス、「ＩＰ　ＣＭ１」の宛先ＩＰアドレス、及び「ＭＡＣ　ＣＭ１」のＭＡＣ宛先アドレスを指定している。マルチＰＨＹ通信は、ＣＭＴＳ　１０１のＭＡＣ送信元アドレスの指定によって制御される。図のように、ＳＤＮＰペイロードＧを含むデータパケット１４５０Ｇは、ミニスロット１５及び１６でデータを伝送する周波数f_6での通信に対応するＭＡＣ送信元アドレス「ＭＡＣ　ＣＭＴＳ６」を指定している。データパケット１４５０ＨはＳＤＮＰペイロードＨを含み、ミニスロット１７及び２０でデータを伝送する周波数f_7の通信に対応するＭＡＣ送信元アドレス「ＭＡＣ　ＣＭＴＳ７」を指定している。ＳＤＮＰペイロードＩを含むデータパケット１４５０Ｉは、ミニスロット２１、２２、及び２３でデータを伝送する周波数f_8での通信に対応するＭＡＣ送信元アドレス「ＭＡＣ　ＣＭＴＳ８」を指定している。最後に、ＳＤＮＰペイロードＪを含むデータパケット１４５０Ｊは、ミニスロット番号２４及び２５でデータを伝送する周波数f_9での通信に対応するＭＡＣ送信元アドレス「ＭＡＣ　ＣＭＴＳ９」を指定している。このようにして、関連するデータパケットと関連性のないデータパケットを、マルチＰＨＹメソッドを使用して、チャネルの競合や同時アップストリームデータとのデータ衝突なしに、ＣＭＴＳ　１０１からＣＭ　１０３に並行して送信することができる。

【０６０７】
ハイパーセキュアコールルーティング
【０６０８】
本明細書で開示したセキュア動的通信ネットワーク及びプロトコルに従ってなされるハイパーセキュアコールルーティングは、コマンド及び制御のための３つの方法のいずれかを使用して実行できる。
・トライチャネル通信。通話または通信のルーティングは３セットのサーバ、すなわち音声、ビデオ、またはデータファイルの伝送用のＳＤＮＰメディアサーバ、通話のルーティングを選択するためのＳＤＮＰシグナリングサーバ、及び電話番号と対応するＳＤＮＰアドレスとの動的マッピングを格納するためのＳＤＮＰネームサーバによって制御される。
・デュアルチャネル通信。通話または通信のルーティングは２組のサーバ、すなわち音声、ビデオ、またはデータファイルの伝送用のＳＤＮＰメディアサーバ、及び通話のルーティングをするとともに、電話番号と対応するＳＤＮＰアドレスとのマッピングを行うＳＤＮＰネームサーバによって制御される。
・シングルチャネル通信。データトランスポート、ルート計画、及びＳＤＮＰアドレスマップがすべて単一のサーバセットによって実行される。
【０６０９】
一般に、トライチャネル通信では、ひとつのサーバセットに通話に関するすべての情報が含まれてはいないため、サイバー攻撃に対する耐性が向上する。ただし、どの場合でも、ＳＤＮＰネットワークは分散処理を利用して、特定のサーバに格納する情報を制限している。さらに、シングル、デュアル、またはトライチャンネル通信によるデータ転送中、ＳＤＮＰメディアサーバは４つ目のタイプのサーバであるＤＭＺサーバに接続する。ＤＭＺサーバは、スクランブル、分割、ミキシング、ジャンクデータの挿入・削除、暗号化など、ＳＤＮＰデータペイロードの処理に必要なＳＤＮＰ共有秘密の格納に使用される。動作中、メディアサーバが受信した着信データパケットはＤＭＺサーバに送られ、そこでデータパケットが変更されてからメディアサーバに戻される。メディアサーバは、データパケットの変更方法や、データの処理に使用されたロジックやアルゴリズムについては認識しない。ＤＭＺサーバに保存されている実行可能コードとテーブルは、コードを分析できないよう暗号化されている。また、ＤＭＺサーバはネットワークまたはインターネットに接続せずにオフラインで動作する。
【０６１０】
次図は、トライチャネルＳＤＮＰ通信の実装の一例と、ネットワークを介した通話の開始またはファイルの送信に使用されるシーケンスを示している。デュアルチャネル通信の動作は、トライチャネル通信からの若干の変更版と見ることができ、ＳＤＮＰネームサーバの機能がシグナリングサーバに組み込まれている。シングルチャネル通信は、３つの操作すべてをＳＤＮＰ通信ノードとして動作する多機能サーバのネットワークに統合することで構成される。
【０６１１】
ＳＤＮＰクラウド内の断片化されたデータ転送は通常、動的メッシュルーティングを使用して実行されるが、ラストマイル通信で利用できるルーティングオプションは少ない。具体的には、連続データパケットは（ｉ）単一のＳＤＮＰゲートウェイにルーティングされるか（つまり、単一ルートのラストマイル通信）または、（ｉｉ）複数のＳＤＮＰゲートウェイにルーティングされるか（マルチルートのラストマイル通信）、のいずれかである。その他のラストマイルルーティングの選択肢には、動的送信元アドレッシングとマルチＰＨＹラストリンク接続がある。これらの配信オプションは、シグナリングサーバで生成されるＩＰデータパケット内で指定される。これらのＳＤＮＰデータパケットは、送信元及び宛先のＩＰアドレスとＭＡＣアドレスを指定している事実があるにもかかわらず、ある特定のデータパケットがラストマイル通信で通過する正確なパスを知ることはできない。その代わり、中間のパスは、ＳＤＮＰシグナリングサーバではなく、ローカルネットワークオペレータ、モバイルネットワークオペレータ、及びラストマイルのサービスを提

供するネットワークサービスプロバイダが所有するデバイス、ルータの動作によって判別される。したがって、ラストマイル通信は、両端は固定されているが、それらの間には無数の独特な形状のパスが存在する縄跳びの縄に似ている。

【０６１２】

より詳しく解説すれば、単一ルート、複数ルート、及びメッシュルート通信という用語は、メディアパケットのパスを意味する。つまり、パスの「コンテンツ」が発信者間を往来する経路を意味している。一方、トライチャネル、デュアルチャネル、及びシングルチャネル通信とは、ＳＤＮＰノードのネットワーク上での伝送を管理するために使用されるコマンド及び制御システムを指している。前記を前提として、以下の一連の図は、本開示のセキュア動的通信ネットワーク及びプロトコルに従って、電話をかける、または通信を開始する際に使用される一連のステップ、すなわち「プロセス」を示している。

【０６１３】

図６６は、ＳＤＮＰクライアント１６００、ＩＰルータ１６０２Ａ、１６０２Ｂ、及び１６０２Ｃ、シグナリングサーバ１６０３Ａ、ＳＤＮＰネームサーバ１６０４Ａ、及びＳＤＮＰゲートウェイ１６０１からなるトライチャネル通信のための単一ルートのラストマイルネットワークの抽象的表現である。これらのコンピュータサーバは、図に示されるように、ＳＤＮＰクライアント$C_{1,1}$、ルータＲ、ＳＤＮＰシグナリングサーバノードＳ、ＳＤＮＰネームサーバノードＮＳ、及びＳＤＮＰゲートウェイノード$M_{0,0}$で構成されるネットワークノード名とＩＰアドレスによるネットワーク通信を容易にするために使用されるＳＤＮＰ通信ノードをホストする。ネットワーク接続１６１０はクライアント$C_{1,1}$とそれに最も近いルータ１６０２Ａとの間のラストリンクを円滑化し、ネットワーク接続１６１１はＳＤＮＰゲートウェイ$M_{0,0}$とそれに最も近いルータ１６０２Ｂとの間のゲートウェイリンクを円滑化し、ネットワーク接続１６１２はＳＤＮＰシグナリングサーバ１６０３Ａとそれに最も近いルータ１６０２Ｃとの間のゲートウェイリンクを円滑化し、そしてネットワーク接続１６１６は、トポロジ的に隣接するルータ１６０２Ａ及び１６０２Ｃに相互接続する。ルータのＩＰアドレスは、ＩＰデータグラムでは送信元アドレスまたは宛先アドレスとして使用されないため、レイヤ３のすべてのルータにはルータであることを示す表記として「Ｒ」が使用される。レイヤ１及びレイヤ２の説明では、各ルータに一意のＩＤが付与されているが、このことはＩＰネットワークのレイヤ３のコールルーティングの説明と密接な関係があるわけではない。ＳＤＮＰシグナリングサーバ１６０３Ａ（ノードＳ）は、ネットワーク接続１６１３を介してＳＤＮＰネームサーバ１６０４Ａ（ノードＮＳ）に接続し、また複数のネットワーク接続１６１４を介してＳＤＮＰクラウドノード$M_{0,n}$に接続する。シグナリングサーバ１６０３Ａは、ネットワーク接続１６１５を介して他のシグナリングサーバ（図示せず）にも接続する。

【０６１４】

ＳＤＮＰネットワークを使用してコールを行う（つまり、「セッション」を確立する）とは、ＳＤＮＰクライアントによる発呼から始まる以下の一連の手順を実行することである。

１．ＳＤＮＰコール（またはコールアウト）要求
２．ＳＤＮＰアドレス要求
３．ＳＤＮＰアドレス配信
４．ＳＤＮＰルーティング指示
５．ＳＤＮＰコール（またはコールアウト）の開始

【０６１５】

最初のステップ「コール要求」は図６７に示す通りである。ここで、発信者、すなわちアドレス「ＩＰ　$C_{1,1}$」のクライアント１６００が、ＩＰデータグラム１６２０を用いてパス１６１０、１６１６、及び１６１２を介してアドレス「ＩＰ　Ｓ」のシグナリングサーバ１６０３Ａにアクセスする。データグラムのコマンド及び制御ペイロード６２１には、ＴＣＰを使用してデータの正確性を保証するレイヤ４データトランスポートが含まれ、配信、緊急度、セキュリティクレデンシャル情報、及びコールする相手すなわち「受信

者」の連絡先情報など、いくつものコールパラメータが指定されている。別のＳＤＮＰクライアントを呼び出す場合（つまり「ＳＤＮＰコール」の場合）、この連絡先情報には、コール対象のクライアントの機密ＩＤ（ＣＩＤ）、クライアントのＳＤＮＰ電話帳に存在するデータが含まれる。「コールアウト」（ＳＤＮＰクライアントではない相手へのコール）の場合は、連絡先情報には電話番号が含まれる。ＳＤＮＰクライアントのＣＩＤは本質的に匿名であり、ＳＤＮＰネームサーバのみが認識しているが、電話番号は偽装されない。被コール側のプライバシーを保護するため、Ｃ＆Ｃペイロード内の電話番号は暗号化される。代替手段として、Ｃ＆Ｃペイロード１６２１全体を暗号化することもできる。Ｃ＆Ｃペイロード１６２１は暗号文の形式でも構わないが、ＩＰデータグラム１６２０のＩＰアドレスは暗号化できない。暗号化されると、ルータ１６０２Ａ及び１６０２Ｃはデータグラムをルーティングできないからである。

【０６１６】

２番目のステップである「ＳＤＮＰアドレス要求」を図６８に示す。ここで、アドレス「ＩＰ　Ｓ」のＳＤＮＰシグナリングサーバは、ＩＰデータグラム１６２２のパス１６１３を介してアドレス「ＩＰ　ＮＳ」のＳＤＮＰネームサーバに接続する。データグラムのコマンド及び制御ペイロードは、レイヤ４データトランスポートをＴＣＰとして定義し、コール先（受信者）のＣＩＤまたは暗号化された電話番号を含む。ＳＤＮＰコールの場合、ネームサーバ１６０４Ａは、ＣＩＤをコール先のクライアントのＳＤＮＰアドレスに変換する。コールアウトの場合、ネームサーバ１６０４Ａは受信者の電話番号を復号してから、受信者の位置に最も近いＳＤＮＰゲートウェイのＳＤＮＰアドレスに変換する。図６９に示す通り、ネームサーバ１６０４Ａはこの後、ＩＰデータグラム１６２３内のクライアントまたはゲートウェイのＳＤＮＰアドレスを送信元アドレス「ＩＰ　ＮＳ」からアドレス「ＩＰ　Ｓ」のシグナリングサーバ１６０３Ａに渡す。

【０６１７】

シグナリングサーバ１６０３Ａは、発信者と受信者のＳＤＮＰアドレスを利用して、受信者がＳＤＮＰクライアントの場合はハイパーセキュア接続として、受信者がＳＤＮＰクライアントでない場合は最も近いＳＤＮＰゲートウェイへ、コールをルーティングする。図７０に、ルーティング指示を準備し、発信者の接続を成立させるために必要とされるすべてのメディアノードにこれらの指示を配信するプロセスを示す。図に示す通り、Ｃ＆Ｃペイロード１６２１Ａの配信及び緊急度フィールドに含まれる発信者の配信要求は、アカウント情報の検証が完了した後、操作１６５０に示されるように、データグラムの配信方法を選択するために使用される。配信方法には、普通、ＶＩＰ、保証、または特別のカテゴリがあり、パケットまたはサブパケットのルーティングに影響する（パケットが分割または断片化される場合）。例えば、ＶＩＰ配信では、データ転送に最速ルートが使用されるが、他のクライアントによる同じルートの読み込みは最小限に抑制される。保証伝送では、重複したデータパケットフラグメントがネットワークを介して送信され（つまり、冗長性を使用）、最速パケットのタイムリーな配信を保証し、遅延パケットを無視する。Ｃ＆Ｃペイロード１６２３Ａから得られるＳＤＮＰアドレスデータと組み合わせて、操作１６５１は、発信者から受信者のＳＤＮＰアドレスへの、または受信者がＳＤＮＰクライアントでない場合は受信者に最も近いゲートウェイに、最適なルートをマッピングする。Ｃ＆Ｃペイロード１６２１Ａに含まれる緊急性要求データは、遅い（ｓｎａｉｌ）配信（急ぐ必要がない）、普通配信、優先配信、緊急配信など、伝播遅延が減少する順などの基準でパッケージの緊急性操作１６５２の選択に使用される。

【０６１８】

緊急性要求情報はその後、操作１６５３によるルーティングの選択、及びサブパケットルーティングのゾーンの選択に使用される。これらのパラメータは、任意の該当するセキュリティクレデンシャル情報１６２１Ｂとともに、操作１６６０を通じてルーティングコマンドと制御パケットを合成する。これらのＣ＆Ｃデータパケットは、ＴＣＰ指定レイヤ４トランスポートを使用してラストマイルの参加通信ノードに配信されるが、リアルタイムデータの配信に使用される場合には、レイヤ４トランスポートプロトコルとしてＵＤＰ

を使用するルーティング情報が含まれる。例えば、ゾーンＵ１セキュリティクレデンシャル情報に従って作成されるラストマイルルーティングは、クライアントノードＣ$_{1,1}$からＳＤＮＰゲートウェイノードＭ$_{0,0}$へのデータのルーティングに使用されるＣ＆Ｃペイロード１６２６を含むＩＰデータグラム１６２５として生成される。ＩＰデータグラム１６２５は、ＴＣＰデータトランスポートを使用してＳＤＮＰクライアントに配信されるが、「ラストマイルルーティングＵ１」というタイトルのＣ＆Ｃペイロード１６２６には、パケットをリアルタイムでルーティングするために使用されるデータが含まれているため、レイヤ４トランスポートメカニズムとしてＵＤＰを使用する必要がある。ＳＤＮＰ　Ｃ＆Ｃパケット合成操作１６６０では、ＳＤＮＰクラウド内のノードにＴＣＰデータパケットとして配信される多数の他のＣ＆Ｃメッセージも生成される。クラウド命令データパケットの一例として、ＳＤＮＰ　Ｍ$_{0,0}$からＳＤＮＰ　Ｍ$_{0,1}$へのデータのルーティングに使用されるＣ＆Ｃペイロード１６２８Ａを含むＩＰデータグラム１６２７Ａがある。図７１に示されるように、これらのＳＤＮＰルーティング指示パケットは、シリアル接続１６１２、１６１６、１６１０を介してクライアントノードＣ$_{1,1}$を含むメディアノードに、またＳＤＮＰゲートウェイノードＭ$_{0,0}$に、さらにまた接続１６１４を介してＳＤＮＰクラウド内の他のノードに配信される。

【０６１９】

コールの開始を図７２に示す。この図で、ＳＤＮＰデータ（サウンド、ビデオ、テキスト等）を含むメディアＳＤＮＰデータグラム１６３０は、Ｃ＆Ｃデータパケット１６２６を含むＩＰヘッダに追加され、ＩＰ　Ｃ$_{1,1}$からＩＰ　Ｍ$_{0,0}$へ、そしてＳＤＮＰクライアント１６００からラストリンクネットワーク接続１６０１を介してルータ１６０２Ａ及び１６０２Ｂにルーティングされ、最後にゲートウェイリンク１６１１を介してＳＤＮＰゲートウェイ１６０１に到達する。識別タグ、セキュリティゾーン、プリアンブル、及びＳＤＮＰデータフィールドを合わせて、メディアＳＤＮＰデータグラム１６３０に含まれるＳＤＮＰメディアパケットのペイロードが構成される。

【０６２０】

前述のＳＤＮＰコール、すなわちＳＤＮＰゲートウェイＭ$_{0,0}$から、ＳＤＮＰアプリ１３３５Ａを実行する携帯電話３２を含むＳＤＮＰクライアントＣ$_{7,1}$へのハイパーセキュアコールのルーティングを、図７３Ａの簡略化したネットワーク図に示す。メディアＳＤＮＰペイロードＡ及びヘッダ１６２８Ａを含むＳＤＮＰデータグラム１６３１Ａは、ＳＤＮＰアドレスＭ$_{0,0}$及びＭ$_{0,1}$のメディアノード間でルーティングされる。ただし、ＳＤＮＰゲートウェイ１６０１には、２つのアドレス、すなわちラストマイル通信用のＩＰアドレス「ＩＰ　Ｍ$_{0,0}$」と、ＳＤＮＰクラウド内の通信用のＳＤＮＰアドレス「ＳＤＮＰ　Ｍ$_{0,0}$」がある。各ＳＤＮＰデータグラムのコンテンツは、パケットがＳＤＮＰクラウドを通過するときに変化するため、ＳＤＮＰメディアペイロードＡ、Ｂ、及びＣに含まれるサウンド、ビデオ、及びテキストなどのコンテンツは同じでないことは明らかで、２０種類の会話またはコミュニケからのコンテンツが含まれることがある。ＳＤＮＰクラウド内のデータルーティング及びパケットセキュリティのメカニズムは、前掲の米国特許出願第１４／８０３，８６９号「Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｎｅｔｗｏｒｋ　ａｎｄ　Ｐｒｏｔｏｃｏｌ（安全で動的な通信ネットワークとプロトコル）」に開示されており、それにはＳＤＮＰクラウドを匿名で移動するデータパケットのコンテンツと暗号化が動的かつ継続的に変化し、やがてクライアントのデバイスに収束する仕組みが記述されている。

【０６２１】

それによって、メディアＳＤＮＰペイロードＢ及びヘッダ１６２８Ｂを含むＳＤＮＰデータグラム１６３１Ｂは、ＩＰアドレスＩＰ　$_{0,4}$及びＭ$_{0,f}$　のメディアノード間でルーティングされる。ＳＤＮＰゲートウェイ１６０１Ｂを介してＳＤＮＰクラウドを出るデータは、ＳＤＮＰデータグラムからＩＰデータグラム１６３２に変換される。ヘッダ１６２８Ｃ及びＳＤＮＰメディアペイロードＣを含むＩＰデータグラム１６３２は、ラストマイルを構成するゾーンＵ２のセキュリティクレデンシャル情報を使用する。次いで、Ｉ

Ｐデータグラム１６３２は、有線またはファイバリンク２４を通しラストマイルを介してネットワークルータ２７にルーティングされ、その後、セルラーネットワーク２５及びセルラーリンク２８を介して携帯電話３２にルーティングされる。携帯電話３２はＳＤＮＰクライアントであるため、ラストマイルを介した通信はハイパーセキュアの状態が維持される。この簡素化された例では、クラウドからラストマイルに到達するすべてのデータパケットは、単一のＳＤＮＰゲートウェイ１６０１Ｂからルーティングされる。実際には、複数のＳＤＮＰゲートウェイをラストマイルデータルーティングに使用できる。

【０６２２】

「コールアウト」でのラストマイル通信を図７３Ｂに示す。ＳＤＮＰクラウドを介したルーティングは、ＳＤＮＰクライアントへのコールに使用される場合と同じＳＤＮＰデータグラム１６３１Ａ及び１６３１Ｂを使用するが、ＳＤＮＰゲートウェイ１６０１ＢはＳＤＮＰソフトウェアを実行する最後のサーバである。したがって、コールアウトにおけるラストマイル通信では、非ＳＤＮＰペイロードが含まれるＩＰデータグラムが使用される。つまり、ＩＰデータグラム１６３５は、ゲートウェイＩＰ　$M_{0,0}$からＩＰアドレスＩＰ　$C_{7,9}$のＰＳＴＮにルーティングされ、ＶｏＩＰの形式で音声が伝送される。ＰＳＴＮは、電話番号とサウンドパケット１６３６のアナログサウンドを使用して、ＶｏＩＰのコールフォーマットを従来の電話のコールフォーマットに変換する。このような場合、ラストマイルはハイパーセキュア通信を構成しない。

【０６２３】

図７４に示すマルチルートのラストマイル通信において、ＳＤＮＰシグナリングサーバ１６０３Ａによって配信されるコマンド及び制御データパケットには、データリンク１６１２及び１６１０を介してクライアント１６００に送信されるＣ＆Ｃデータパケット１６２５Ｘ、データリンク１６１４Ｘを介してＳＤＮＰゲートウェイ１６０１Ｘに送信されるＣ＆Ｃデータパケット１６２７Ｘ、及びデータリンク１６１４Ｙ上のＳＤＮＰゲートウェイ１６０１Ｙに送信されるＣ＆Ｃデータパケット１６２７Ｙが含まれる。他のＣ＆Ｃデータパケット（図示せず）は、データリンク１６１４Ｘを介して、メディアノードをホストする他のサーバに送信される。Ｃ＆Ｃデータパケット１６２５Ｘは、アドレス「ＩＰ　Ｓ」からアドレス「ＩＰ　$C_{1,1}$」に送信され、これにはラストマイルルーティングＵ１を構成するＣ＆Ｃペイロードが含まれている。ラストマイルルーティングＵ１には、２つの異なるルーティング指示が含まれている。１つはタグ１とプリアンブル１を含む「ＩＰ　$C_{1,1}$」から「ＩＰ　$M_{0,0}$」までの指示、もう１つはタグ２及びプリアンブル２「ＩＰ　$C_{1,1}$」から「ＩＰ　$M_{0,1}$」までの指示が含まれる。例に示されるように、ＳＤＮＰクラウド内の通信ノードに送信されるＣ＆Ｃデータパケットには、指示ＳＤＮＰクラウドルーティング１の指示を含む「ＩＰ　Ｓ」から「ＩＰ　$M_{0,0}$」に送信されるデータパケットと、ＳＤＮＰクラウドルーティング２の指示を含む「ＩＰ　$M_{0,1}$」に送信されるデータパケットが含まれている。

【０６２４】

ＳＤＮＰグループコール

【０６２５】

図７５Ａに示される、ＳＤＮＰクライアント１６００から複数のＳＤＮＰゲートウェイへのラストマイルメディアパケットルーティングには、それぞれのヘッダ１６２６Ｘ及び１６２６Ｙ、ならびにＳＤＮＰメディアペイロードＳＤＮＰデータＸ及びＳＤＮＰデータＹを含む２つのデータパケット１６３０Ｘ及び１６３０Ｙが含まれる。タグ１及びプリアンブル１を含むデータヘッダ１６２６Ｘはアドレス「ＩＰ　$C_{1,1}$」からアドレス「ＩＰ　$M_{0,0}$」にルーティングされ、タグ２及びプリアンブル２を含むデータヘッダ１６２６Ｙはアドレス「ＩＰ　$C_{1,1}$」からアドレス「ＩＰ　$M_{0,1}$」にルーティングされる。

【０６２６】

マルチルート通信によりＳＤＮＰクラウドからクライアントへ逆方向に流れるデータには、図７５Ｂに示されるように、ヘッダ１６２６Ｕ、タグ８、プリアンブル８、ＳＤＮＰデータＵ、送信元アドレスＳＤＮＰゲートウェイアドレス$M_{0,0}$、及び宛先アドレス「Ｉ

Ｐ　Ｃ$_{0,0}$」を含むデータパケット１６３０Ｕが含まれる。同時に、このデータには、ヘッダ１６２６Ｖ、タグ９、プリアンブル９、ＳＤＮＰデータＶ、宛先アドレスＳＤＮＰゲートウェイアドレスＭ$_{0,1}$、及び宛先アドレス「ＩＰ　Ｃ$_{0,0}$」を含むデータパケット１６３０Ｖも含まれる。ＳＤＮＰクライアント１６００で実行されているＳＤＮＰアプリケーションプログラムは次に、着信データパケットＳＤＮＰデータＵ、ＳＤＮＰデータＶ、及びその他を結合して、メッセージテキストや音声（サウンド）を再作成する。

【０６２７】

ルーティング指示のＣ＆Ｃデータパケット配信は、３方向またはグループコール、グループメッセージング、及びその他のマルチクライアント通信を開始するように拡張できる。このようなグループコミュニケまたは「会議通話」では、クライアントメッセージが複数の受信者に同時に送信される。このグループ機能は、グループコールを要求する発信者によって呼び出され、最初に接続先とするクライアントのグループを定義し、続いてシグナリングサーバによって呼び出され、個々のグループコールに関連付けられたデータパケットのルーティングを処理する方法を必要なメディアノードに指示する。グループコールルーティング指示の一例を図７６に示す。ここで、シグナリングサーバ１６０３Ｐは、データリンク１６１４Ａを介してＳＤＮＰクライアント１６００Ａに、またデータリンク１６１４Ｚを介してＳＤＮＰクラウド内の多数のメディアサーバ１６００Ｚにルーティング指示を送信する。

【０６２８】

そのため、ラストマイルルーティングＵ１を含むＴＣＰデータパケット１６２７Ａは、アドレス「ＩＰ　Ｓ１」のシグナリングサーバ１６０３ＰからアドレスＩＰ　Ｃ$_{1,1}$」のＳＤＮＰクライアントに配信され、発信者とのグループコールを「セットアップ」する。例示するＴＣＰデータパケット１６２７Ｚによって表されるＣ＆Ｃデータパケットは、シグナリングサーバアドレス「ＩＰ　Ｓ１」から様々な宛先アドレス「ＩＰ　Ｍ$_{0,y}$」までのデータリンク１６１４Ｚを介してゾーンＺ１のＳＤＮＰクラウド全体に同時に配布される（ここで、ｙは整数変数を表す）。全体として、ＳＤＮＰクラウドのルーティング指示により、ＳＤＮＰクラウド全体の発信者のゲートウェイから、呼び出されるＳＤＮＰクライアントに最も近い２つ以上の他のＳＤＮＰゲートウェイへのパケットルーティングを確立する。

【０６２９】

例に示す通り、他のＳＤＮＰクライアントは異なる地理的地域に配置されている場合があり、ゾーンＵ７とＵ９などの個別のセキュリティゾーン内にある場合がある。場合によっては、これらのクライアントはシグナリングサーバ１６０３Ｐから十分に離れている可能性があるため、別の信号サーバ１６０３Ｑを使用してこれらのＳＤＮＰクライアントのパケットルーティングを計画できる。シグナリングサーバ１６０３Ｑは、ゾーンＵ９のルーティング指示をデータリンク１６１４Ｍを介してＳＤＮＰクライアント１６００Ｍに、データリンク１６１４Ｌを介してＳＤＮＰクライアント１６００Ｌにそれぞれ通信する。例えば、Ｃ＆Ｃデータパケット１６２５Ｍは、「ＩＰ　Ｓ４」のシグナリングサーバからそのアドレス「ＩＰ　Ｃ$_{9,1}$」のＳＤＮＰクライアント１６００Ｍにラストマイルルーティング指示Ｕ９を伝達する。別のＣ＆Ｃデータパケット（図示せず）も同様に、アドレス「ＩＰ　Ｃ$_{9,4}$」のＳＤＮＰクライアントに送信される。ラストマイルルーティングＵ７の指示を含むデータパケット１６２７Ｈは、データリンク１６１４Ｈを介して、「ＩＰ　Ｓ４」のシグナリングサーバ１６０３ＱからアドレスＩＰ　Ｃ$_{7,1}$」のクライアント１６００Ｈに送信される。

【０６３０】

ノードＳ１及びＳ４のシグナリングサーバ１６０３Ｐ及び１６０３Ｑも、データリンク１６１３Ｚを介してＣ＆Ｃデータパケットとして情報を交換する。この情報は、ルーティングのどの部分がシグナリングサーバ１６０３Ｐによって実行され、どの部分がシグナリングサーバ１６０３Ｑによって実行されるかを確立するために使用され、ルーティングタスクを複数のシグナリングサーバに分割する。例において、シグナリングサーバノードＳ

１はゾーンＵ１及びＳＤＮＰクラウドのラストマイルルーティングを管理し、シグナリングサーバノードＳ４はゾーンＵ７及びＵ９でのラストマイル通信を管理する。

【０６３１】

通話中またはコミュニケ中のデータルーティングを図７７Ａに示す。ここで、データパケット１６３０ＡのＳＤＮＰデータ１によって送られる音声は、ヘッダ１６２６Ａにより、ＩＰアドレス「ＩＰ　$C_{1,1}$」の発信者から最も近いＳＤＮＰゲートウェイメディアノード$M_{0,0}$にルーティングされる。このデータパケットはＳＤＮＰクラウドトランスポート用に再パケット化され、ゲートウェイメディアノード$M_{0,4}$及び$M_{0,8}$に送信される。ＳＤＮＰクラウド内でパケットルーティングがとるパスは、電話会議の参加者には不明であり、中央での制御はできず、ネットワークの状態に応じて動的に変化する。この例では、ＳＤＮＰクラウド内のすべてのＳＤＮＰデータパケットは、匿名のアドレス指定及び動的暗号化に加え、ジャンクデータの挿入及び削除による動的スクランブリング、ミキシング、分割などの技術を活用した断片化メッシュデータ伝送を利用している。例に示す通り、クラウドトランスポートは、ＳＤＮＰゲートウェイノード$M_{0,0}$の着信通信を他のゲートウェイに（この例では、ＳＤＮＰゲートウェイノード$M_{0,4}$及び$M_{0,8}$）に向ける。

【０６３２】

発信者の音声を運ぶデータパケット１６３０Ｈ、すなわちＳＤＮＰデータ１は、ゲートウェイノード$M_{0,4}$を出て、ヘッダ１６２６Ｈを用い、ゾーンＵ７セキュリティクレデンシャル情報を使用して、「ＩＰ　$M_{0,4}$」のメディアノードから「ＩＰ　$C_{7,1}$」のクライアント１６００Ｈにルーティングされる。ヘッダ１６２６Ｈは、図７６で説明するように、メディアデータパケットを準備する前に、Ｃ＆Ｃデータパケット１６２７Ａ内のクライアント１６００Ａに付与されている。このようにして、リアルタイムデータを伝送するすべてのメディアパケットは、コンテンツのデータ伝送の準備が整った時点で遅延なく準備することができる。リアルタイムネットワークで優れたＱｏＳを実現するには、動的データのタイムリーなルーティングが欠かせない。これができなければ、許容できないほど長い伝播遅延が生じる可能性がある。

【０６３３】

ＳＤＮＰクラウドを介してルーティングされると、ＳＤＮＰデータ１ペイロードはゾーンＵ９の電話会議参加者（すなわちＳＤＮＰクライアント１６００Ｍ及び１６００Ｌ）に、つまりゲートウェイメディアノード$M_{0,8}$からクライアントＩＰアドレス「ＩＰ　$C_{9,1}$」及び「ＩＰ　$C_{9,4}$」に送られる。これらのラストマイルデータパケット１６３０Ｍ及び１６３０Ｌには、同じ会話に関連付けられたコンテンツの認識に使用される識別パケットタグ、ｔａｇ８及びｔａｇ９を指定するヘッダ１６２６Ｍ及び１６２６Ｌ、ＳＤＮＰ埋め込み指示、鍵、シードなどの伝達に使用されるプリアンブル９情報、及びレイヤ４トランスポートにＵＤＰを要求するために使用される「Ｌ４」データフィールドが含まれる。シグナリングサーバから送られるデータルーティング指示はその精度を保証するためにＴＣＰトランスポートプロトコルを使用しているが、メディアパケットコンテンツはリアルタイムデータであるため、ＴＣＰの代わりにより相応しいＵＤＰレイヤ４プロトコルを使用する。

【０６３４】

図７７Ｂは同じ会話を示している。ここでは、ゾーンＵ７のクライアント１６００Ｈからコンテンツが発生する。つまり、クライアント$C_{7,1}$が会話を開始する。このデータをクライアント$C_{1,1}$からの音声コンテンツと比較するため、ペイロードはすべてのデータパケット内で「ＳＤＮＰデータ５」として識別される。ペイロードが一意であることを別にすると、前図からの唯一の変更点は、データパケット１６３０Ｈと１６３０Ａのラストマイルの送信元及び宛先のＩＰアドレスが逆になっていることである。具体的には、ゾーンＵ７のＳＤＮＰユーザの場合、データパケット１６３０Ｈの送信元ＩＰアドレスはＩＰ　$C_{7,1}$に変更され、その宛先はＳＤＮＰゲートウェイアドレスＩＰ　$M_{0,4}$になっている。ゾーンＵ１の場合、データパケット１６３０Ａの送信元ＩＰアドレスはＩＰ　$C_{1,1}$

に変更され、その宛先はＳＤＮＰゲートウェイアドレスＩＰ　Ｍ$_{0,0}$に変わる。複数の電話会議参加者が同時に発話し、クライアントノードＣ$_{7,1}$を含む他の通話参加者に送信されるＳＤＮＰクライアントノードＣ$_{1,1}$からのデータパケットが、クライアントノードＣ$_{7,1}$に対して同時に発生し、クライアントノードＣ$_{1}$、$_{1}$に応答することがあることを想定しておかなければならない。

【０６３５】

ラストマイル通信のネットワークレベル３では、反対方向のトラフィックのデータ衝突は発生しない。ただし、物理リンク層とデータリンク層の１及び２では、ラストマイル通信に時間多重化を使用することで、同じ通信リンクの競合を回避できる。ただし、この調停は、通信が音声パケットの遅延のない全二重通信のように見えるほど高速に行われる。図７７Ａ及び図７７Ｂでは共に、ゾーンＵ９のクライアントのデータフローの方向（クラウドからクライアントへのデータフロー）は変更されていない。ただし、図７７Ｃでは、ゾーンＵ９クライアントノードＣ９，１が会話を開始する。この場合、クライアントノードＣ$_{9,4}$、Ｃ$_{1,1}$、及びＣ$_{7,1}$はすべて、音声、つまりＳＤＮＰ音声データ６の受信者になる。

【０６３６】

図７８に示す代替実施形態では、グループ通話は、ＳＤＮＰクライアントへのＳＤＮＰ通話と、通常の電話番号への「コールアウト」通話の混在が可能である。図７７Ａに示した通話またはコミュニケと同様、データパケット１６３０ＡのＳＤＮＰデータ１によって送られる音声は、ヘッダ１６２６Ａにより、ＩＰアドレス「ＩＰ　Ｃ$_{1,1}$」の発信者からメディアノードＭ$_{0,0}$を含む最も近いＳＤＮＰゲートウェイにルーティングされる。このデータパケットはＳＤＮＰクラウドトランスポート用に再パケット化され、ゲートウェイメディアノードＭ$_{0,4}$及びＭ$_{0,8}$に送信される。

【０６３７】

例に示す通り、クラウドトランスポートは、ＳＤＮＰゲートウェイノードＭ$_{0,0}$の着信通信を他のゲートウェイに（この例では、ＳＤＮＰゲートウェイノードＭ$_{0,4}$及びＭ$_{0,8}$）に向ける。発信者の音声を運ぶデータパケット１６３０Ｈ、すなわちＳＤＮＰデータ１は、ゲートウェイノードＭ$_{0,4}$を出て、ヘッダ１６２６Ｈを用い、ゾーンＵ７セキュリティクレデンシャル情報を使用して、「ＩＰ　Ｍ$_{0,4}$」のメディアノードから「ＩＰ　Ｃ$_{7,1}$」のクライアント１６００Ｈにルーティングされる。ＳＤＮＰデータ１ペイロードは、ゲートウェイメディアノードＭ$_{0,8}$を介して電話会議の参加者にも配信される。このＳＤＮＰゲートウェイからのラストマイル通信は、２種類の接続で構成される。具体的には、ＳＤＮＰクライアント１６００Ｍへのハイパーセキュア接続、及びＶｏＩＰまたはパケットプロトコルを使用しない従来の電話システムを含むＰＳＴＮ　１への非セキュアな「コールアウト」接続である。アドレス「ＩＰ　Ｃ$_{9,1}$」のゾーンＵ９　ＳＤＮＰクライアントに送られるラストマイルデータパケット１６３０Ｍ及びＵ９には、同じ会話に関連付けられたコンテンツの認識に使用されるパケット識別子タグｔａｇ９を指定するヘッダ１６２６Ｍ、ＳＤＮＰ埋め込み指示、鍵、シードなどの伝達に使用されるプリアンブル９情報、及びレイヤ４トランスポートにＵＤＰを要求するために使用される「Ｌ４」データフィールドが含まれる。

【０６３８】

ゲートウェイノードＭ$_{0,8}$はまた、ＩＰパケット１６３５をアドレスＩＰ　Ｃ$_{7,9}$のＰＳＴＮ　１にも送信する。この場合、ＳＤＮＰデータ１を含むペイロードを送信するのではなく、ＩＰペイロードはＶｏＩＰサウンドパッケージに変換されており、パケットスニッフィングによって傍受される可能性がある。そこで、電話交換システムＰＳＴＮ　１は、この保護されていないＩＰパケットを、ＰＯＴＳデータ１６３６（被コール電話番号とそれに続く電話３７とＰＳＴＮ　１との間の連続アナログ回線接続を含む）で示される電話３７へのアナログＰＯＴＳ電話接続に変換する。この接続及びその他のコールアウト接続はハイパーセキュアではないため、コールアウトラストリンクによって送信されるコンテンツは、ハッキング、盗聴、及びその他の監視技術の危険に晒される。クライアント

のアクセス特権を定義する階層構造が実装されていない限り、コール全体のセキュリティは最も弱いリンクによって危険にさらされ、例えばグループコールの参加者全員がすべてを聞くことができてしまいかねない。

【０６３９】

この点を、図７９Ａの表に例示する。ここで、グループコールは、ＳＤＮＰネットワーククライアントノード$C_{1,1}$、$C_{7,1}$、$C_{9,1}$、及び$C_{9,4}$上のハイパーセキュアな参加者と、電話番号「Ｐｈ＃１」及び「Ｐｈ＃２」の参加者で構成される。図の示すように、ＳＤＮＰクライアント$C_{1,1}$はグループのホストであり、ＳＤＮＰクライアント$C_{7,1}$、$C_{9,1}$は参加者であり（つまり、これらの参加者は他の参加者の発話を聞き、自身も話すことができる）、ＳＤＮＰクライアント$C_{9,4}$は「リスナー」である（聞くことはできるが、話せない、つまり参加者にその声が聞かれることはない）。コールアウト電話番号「Ｐｈ＃１」の参加者は聞き取りと発言が可能な参加者でもあり、一方、「Ｐｈ＃２」の発信者はコールアウト「リスナー」としてのみ許可され、グループコールでの発言はできない。グループホストは、コールのセットアップ時に、これらの聴取・発話特権、つまりユーザ認証を規定する。

【０６４０】

「通常コール」というタイトル欄の表を再度確認し、グループコールの全員、つまりホストによって承認された発信者がコールを聞くことができることに注意する。通話へのハッキングを試みる発信者や、ホストにより承認されていない発信者には、通話に接続したり、強制的に通話に参加したりすることはできず、また通話が発生していることを判別することもできない。同じ方法はグループチャットにも適用される。グループチャットの参加者は、メッセージを読み書きすることはできる一方、表示専用メンバーはコメントを読むことだけができ、チャット上に自分のテキストを挿入することはできない。

【０６４１】

本開示に従ってなされたネットワークアクセスを制御するための認証並びＩＤ確認により、ＳＤＮＰシステムは、従来のグループチャット及びグループ通話では利用できなかったプライバシー機能を実現している。この機能は、プライベートモードを選択することで呼び出される。例えば、テキストメッセージシングや発言の前にカギマークやその他のプライバシーアイコンをクリックするなど。このような場合、通信は認証済みのＳＤＮＰクライアントにのみ送られ、認証によってまだ身元が確認されていないＳＤＮＰクライアントには送られない。さらに、安全でないデバイスのコールアウトリスナーまたは参加者にも送信されない。この点は、前述の表で明確に示されている。「非認証ＳＤＮＰクライアント」欄にあるプライベートコールでは、すべてのグループコールクライアントがマイクとスピーカーの両方をミュート（消音化）されている。一方、「認証ＳＤＮＰクライアント」欄では、すべてのＳＤＮＰクライアントは聴くことができ、参加者$C_{1,1}$、$C_{7,1}$、及び$C_{9,1}$は聴くことに加えて話すこともできる。しかし、すべてのコールアウトデバイスはマイクとスピーカーの両方がミュートされているため、認証されたＳＤＮＰクライアントのみがプライベートモードで聞き取りやコメントができる。このようにして、身元が保証された複数のＳＤＮＰクライアントとのグループコールや、未知の相手とのコールアウト接続でのグループコールで、コールアウトデバイスに機密情報を晒すことなく、通話の公開部分に相互に参加できる。「コールアウト」発信者をプライベートディスカッションから除外するには、発言やテキスト送信の前にＳＤＮＰ参加者にプライベートアイコンをクリックさせるだけでよい。プライベートディスカッションが終わったら、プライベートボタンを元に戻すことで、コールアウト発信者は再接続される。コールアウト発信者が切断されている間（つまり基本的に「保留」になっている間）、ＳＤＮＰシステムは待機中の音楽を再生したり、無音にしたり、ホワイトノイズ（海や雨の音など）を再生したりできる。

【０６４２】

グループチャットのテキストメッセージも同じ方法で管理できる。通常のグループチャットでは、すべてのテキストメッセージがＳＤＮＰクライアントデバイスのＳＤＮＰアプ

リに送信され、ＳＭＳテキストメッセージによってすべてのコールチャットメンバーに送信される。テキストメッセージは、参加者のみが送信できる。「リスナー」または「読み取り専用」チャットメンバーから送信されたテキストメッセージは無視され、チャットグループには転送されない。参加者がメッセージを送信する前に鍵アイコンまたはプライバシーアイコンをクリックすると、メッセージはＳＤＮＰクライアントにのみ送信され、コールアウトクライアントには送信されない。プライベートメッセージを受信するＳＤＮＰクライアントの場合、自分の身元が認証されると、メッセージが読み取り用で表示される。クライアントの身元が認証されてなければ、メッセージはボカされたり、覆われたり、隠されたり、鍵などのアイコンで表示されたりする。クライアントが認証手順を踏んで身元が確認されれば、正常に表示される。

【０６４３】

身元の認証とＳＤＮＰネットワークシステム認証によって規制されるプライバシー特権と組み合わせることで、単にデバイスをハッキングするだけでは、グループチャットやグループコールでもプライベートテキストを開いたり、プライベートコールを盗聴したりすることはできなくなる。この機能は、ローカルでハッキングされる可能性のある情報であるデバイスのセキュリティパラメータのみに依存することでは保証できない。偽のセキュリティや身元資格情報はシステムログと一致せず、無効なＳＤＮＰクライアントとして拒否されるため、システムパラメータをハックする壁は非常に高い。

【０６４４】

グループコールやグループチャットの実行時のプライバシーもさらに強化できる。図７９Ｂの表にあるハイパーセキュアラストマイルのこの独特の実施形態は、本明細書ではハイパープライベートコールまたはハイパープライベートチャットと称している。ハイパープライバシーを使用するには、発信者またはメッセージが４つの基準に準拠している必要がある。

・グループコールのコミュニケのすべての受信者は、コールアウトデバイスではなく、ＳＤＮＰクライアントでなければならない。

・通話またはテキストは、それが通話なのかテキストなのか画像なのかに拘わらず、ハイパープライベートコミュニケとして事前に選択しておかなければならない。

・グループコールまたはグループチャットのコミュニケの受信者は、接続を認証して身元を確認しておく必要がある。

・ハイパープライベートコミュニケの受信者は、「プライベート」参加者またはプライベートリスナーとして事前に選択しておく必要がある。

【０６４５】

最初の３つの基準は、前記のグループコールにおけるプライベートパーティの例と基本的に同じだが、４番目の基準である、ハイパープライベートコールまたはテキストを受信する資格のある発信者を「プライベート」ＳＤＮＰクライアントとして読み込むことを求める要件はすばらしく、機密情報へのアクセスをさらに強化している。例えば、表に示されるように、ＳＤＮＰ参加者クライアントＣ$_{1,1}$及びＣ$_{7,1}$、及びＳＤＮＰリスナークライアントＣ$_{9,4}$はすべて、グループコールの「プライベート」パーティとして指定されている。一方、ＳＤＮＰクライアントＣ$_{9,1}$は参加者としてのみ指定され、プライベート参加者としては指定されていない。定義により、コール参加者またはリスナーはプライベートパーティとしては登録できない。

【０６４６】

前例にあるように、通常のコール中、すべての参加者、つまりＳＤＮＰクライアントＣ$_{1,1}$、Ｃ$_{7,1}$、及びＣ$_{9,1}$、及びコールアウト参加者Ｐｈ＃１は、すべての会話を聴き、すべてのテキストメッセージを読み、またいつでも発言し、テキストメッセージを送ることができる。一方、クライアントＣ$_{9,3}$、Ｐｈ＃２を含む「リスナー」は、すべての会話を聴き、テキストを読むことができるが、グループコールまたはチャットで発言したり、メッセージを送信したりすることはできない。ただし、ハイパープライベートコールでは、スイッチまたはアイコンを選択してハイパープライベートコミュニケを指定すると

、グループコールまたはチャットの認証されていないパーティはすべて自動的にブロックされると共に、「プライベート」パーティ以外のすべてのパーティが無効になる。さらにまた、すべてのコールアウト接続及び非認証ユーザも無効化される。そのため、操作中、プライベート参加者がプライバシーアイコンを選択すると、プライベート参加者（プライベートグループのホストを含む）のみがグループを表示し、閲覧し、会話し、テキストを送ることができる。他のすべての参加者のマイクとスピーカーはミュートされ、同様にテキストまたは添付ファイルをグループに対して送受信することはできない。具体的には、ハイパープライベートモードでは、認証されれば、クライアントＣ$_{1}$、$_{1}$及びＣ$_{7}$、$_{1}$のみが聞き取りと会話の両方、及びテキストの読み書きを行うことができ、一方、プライベートクライアントＣ$_{9}$、$_{4}$は会話の聞き取りまたはグループテキストの読み取りのみができる。

【０６４７】

上記のラストマイルルーティング制御機能を使用すると、グループコールとグループチャットを様々な方法で管理できる。例えば、グループコールのホストは、誰を通話またはグループに参加できるようにするか、誰が会話をしテキストを送信できるようにするか、また誰が聞き取りと読み取りのみができるようにするかを決定できる。標準のプライベートコールでは、プライベートモードを選択することにより、すべてのＳＤＮＰクライアントは（一旦認証されると）、標準の非プライベートグループ通信中と同じ権限でコミュニケに参加できる。ハイパープライベートモードでは、プライベート参加者及びプライベートリスナーとして定義されたＳＮＤＰクライアントのみハイパープライベートモード操作中にコミュニケートできる。

【０６４８】

ハイパープライベートコミュニケの一部として、すなわちプライベート参加者またはリスナーとして誰に資格を与えるか、および誰に与えないかの選択方法は、いくつかの方法で設定できる。アドホックハイパープライベートグループ通信では、グループホストがプライベートコールの発信者と非発信者を決定する。ＳＤＮＰの「システム定義」のハイパープライベートグループ通信では、ＳＤＮＰネットワークオペレータが、プライベートコールの発信者と非発信者を事前に決定する。ルールベースのハイパープライベートグループ通信では、ＳＤＮＰネットワークは、誰がプライベート発信者になる資格があるか、誰がないかを決定するルールを定義している。これらのルールは企業の雇用リストに基づいている場合がある。例えば、副社長以上がハイパープライベートコールに参加できる、など。政府やセキュリティ組織では、基準は米国のセキュリティクリアランス、パスポート番号、警察バッジ番号などによって設定される場合がある。本開示で定義されたＳＤＮＰ対応のラストマイル通信方法は、これらの例示したシナリオのいずれかをサポートしてもよいし、他の基準を使用して集団を２つのグループに分け、それによってハイパープライベートコミュニケへのアクセス権を持つグループとそうでないグループを設定できる。

【０６４９】

この概念は複数のグループに拡張できるが、一般的に階層型アクセス基準のほうが、テレフォニーよりもディスパッチャベースのプロフェッショナル通信システムにより適している。プロフェッショナル通信に対するＳＤＮＰ手法の適用については従って、この適用では言及しない。

【０６５０】

グループ通話の課題のひとつに、全員が同時に話そうとする問題がある。会話がオーバーラップすると、話が混乱し、聞き取りにくくなり、不要な停滞も生じる。この問題は、プッシュツートーク機能（トランシーバやＣＢ無線をエミュレートする機能）を使用することで解決できる。プッシュツートークまたはＰＴＴ操作では、一度に１人の参加者のみが発言できる。参加者が会話を希望する場合、スイッチを押すと、ネットワークマイク上の他のすべてがミュートされ、グループコールの他のすべての参加者が聞き取りのみのモードになる。図８０Ａ内の表に示されるように、通常のＰＴＴ会話では、ホストがＰＴＴボタンを押すと（「ホストＰＴＴ」列を参照）、グループコールよりも優先度が上がり、

トークボタンを押した発信者を含め、他のすべての発信者に優先されることになる。コールアウト電話接続を含む他のすべての発信者は、マイクが自動的にミュートされ、リスナー専用モードになる。ホストがＰＰＴボタンを押さなかった場合、「その他のＰＴＴ」というラベルの列に示されるように、ＰＴＴ機能は先着順に他のＳＤＮＰ参加者に引き渡される。リスナーやコールアウトデバイスとして指定されたＳＤＮＰノード（Ｃ９，４、Ｐｈ＃１など）は、ＰＴＴの会話を聴くことができるが、グループコール全体ではそのマイクがミュートされる。

【０６５１】

ネットワークに対して身元の認証を受けた発信者を識別するＳＤＮＰラストマイル機能を使用することで、ＰＴＴ機能をプライベートプッシュツートーク機能に拡張することができる。プライバシー機能またはプライバシーアイコンが選択されると、認証されていない参加者はすべてグループコールから除外され、彼らのスピーカーとマイクがミュートされる。コールアウト接続は本質的に認証できないため、同様にミュートされる。ミュートは双方向であるため、除外された参加者は会話を聞くことができず、マイクも切断される。認証された参加者の場合、操作は通常のＰＴＴと同じ優先度である。すなわち、ホストは優先的に話すことができ、それ以外の場合は認証された参加者が先着順にＰＴＴ通話機能を呼び出すことができる。

【０６５２】

図８０Ｂの表は、ＰＴＴ機能に拡張できるハイパープライベートグループコールの概念を示している。通常の操作では、ＰＴＴ機能は前述のケースと同じである。しかし、ハイパープライベートモードでは、以前にプライベート参加者またはプライベートリスナーとして指定された認証済みの当事者のみ、ハイパープライベート会話に参加できる。例えば、ハイパープライベートモードでは、ＳＤＮＰクライアントＣ９，１及びＣ９，５は、プライベート参加者またはリスナーとして以前に登録されていなかったため、話すことも、聴くこともできない。同様に、すべてのコールアウト接続デバイスは、ハイパープライベートモードの操作中はミュートされる。このようにして、ＰＴＴグループコールの様々な関係者へのアクセスを明示的に制御できる。ミュートとは、一部の参加者（コールアウトリスナーなど）を、会話の音声を運ぶデータパケットの受信から除外しつつ、ミュートされていない参加者にデータパケットを供給し続けるプロセスのことである。本開示の方法では、データパケットは、通常の会話のすべての参加者に個別に送信され、クライアントのユーザによってミュートが有効化されたときには、リストのサブセットにのみ送信される。

【０６５３】

本発明の別の実施形態では、データパケットは、グループコールのすべての参加者にブロードキャストモードで送信されるが、異なる暗号化方法を使用している。通常の電話会議の場合、データパケットは、すべての参加者が復号鍵のコピーを保持する暗号化方式を使用してすべてのユーザに送信される。プライベートモードまたはミュートモードでは、ユーザにブロードキャストされるデータパケットは異なる暗号化を利用し、選択されたユーザのみが復号鍵を共有している。この復号鍵を持つ参加者は電話会議に参加でき、この鍵を持たない参加者は参加できない。ブロードキャストパケットを使用することの利点は、個別のパケット要求を送信する場合に比べてラストマイル通信に必要とされる帯域幅が少なくて済むことである。さらに別の実施形態では、ひとつのパケットがゲートウェイに送信され、このパケットをシグナリングサーバが複製して通常のコールモードですべての参加者に配信し、プライベートまたはミュートモードで発信者を選択する。

【０６５４】

ハイパーセキュアファイルストレージ

【０６５５】

「セキュア動的通信ネットワーク及びプロトコル」は、テレフォニー及びリアルタイムデータ転送用のハイパーセキュア通信システムとして発明され開発されたものであり、ＳＤＮＰネットワーク及びプロトコルに本来的に備わっているセキュリティ機構により、ハイパーセキュアファイル及びデータストレージに最適なものとなっている。ごく簡単に説

明すると、ハイパーセキュアコールで、ある発信者から別の発信者に対してスクランブル化され暗号化されたデータが匿名の断片化データとして送信される場合、言い換えると、あるＳＤＮＰクライアントから別のＳＤＮＰクライアントへのエンドツーエンド通信が行われる場合、ハイパーセキュアファイル及びデータストレージとは、データ送信が途中で停止し、再コールがかかるまで無期限にバッファに保存される、そのような形態の通信と考えることができる。ハイパーセキュア分散ファイルストレージは、非集約型データストレージとも称される。

【０６５６】

このストレージはパケット配信の途中で停止する通信であるというこの簡素化された説明は、それが最初に現れたときよりも技術的にはより正確な表現である。上記で参照されている米国特許出願第１４／８０３，８６９号では、他のパケットが到着するまでの一時的なデータパケットのバッファリングが明示的に開示され、その動作が記述されていた。ＳＤＮＰクラウドのノード内でのバッファリングは月単位ではなくミリ秒単位で行われ、ＳＤＮＰシステムは情報を失うことなくデータを待機または保持し、元のコンテンツを回復する機能を備えている。当然ながら、このような単純化された実装では、ディレクトリ、メニュー、ファイルのリサイクル、セキュリティクレデンシャル情報の更新、その他の機能など、長期的なファイル管理に必要とされる一部の機能が欠落している。

【０６５７】

クライアントから断片化データストレージネットワークへのデータ伝送の一例を図８１に示す。図に示されるように、ＩＰアドレスＩＰ　$C_{1,1}$のＳＤＮＰクライアント１７００Ａは、ＳＤＮＰクラウドを介して、対応するＩＰアドレスＩＰ　$F_{7,1}$、ＩＰ　$F_{9,1}$、及びＩＰ　$F_{9,4}$のＳＤＮＰファイルストレージサーバ１７００Ｈ、１７００Ｍ、及び１７００Ｌに一連のデータパケットを転送する。操作中、クライアントノード$C_{1,1}$は、アドレスＩＰ　$C_{1,1}$からＳＤＮＰゲートウェイ$M_{0,0}$に、ヘッダ１７２６Ｘと一連のデータパケット１７３０Ｘを送信する。データパケット１７３０Ｘは、データパケット１７３０Ｈ、１７３０Ｌ、及び１７３０Ｍと、それぞれに対応するヘッダ１７２６Ｈ、１７２６Ｌ、及び１７２６Ｍと共に例示されている。精度を確保するため、レイヤ４トランスポートはＵＤＰではなくＴＣＰを使用している。これらのパケットには、ルーティング用にパケットを識別するために使用されるＳＤＮＰ　Ｚｉｐまたはタグ Ｘの形式で表されるその他のＩＤが含まれている。データパケット１７３０Ｈ、１７３０Ｌ、及び１７３０Ｍの場合、それぞれタグ１、タグ２、及びタグ３である。各パケットのペイロード部分には、例えば３つに断片化されたファイルＳＤＮＰファイル１、ＳＤＮＰファイル２、及びＳＤＮＰファイル３に、それぞれ一意のデータが含まれている。このラストマイルのセキュリティクレデンシャル情報は、ゾーンＵ１情報とそれに対応するプリアンブル１を使用している。

【０６５８】

データパケットは、ＳＤＮＰクラウドに入ると、その身元情報とシグナリングサーバ（図示せず）の命令に従って別の宛先にルーティングされる。ＳＤＮＰファイル１を運ぶ、ヘッダ１６２６Ｈ及びタグ１を含むデータパケット１７３０Ｈは、ＳＤＮＰゲートウェイノード$M_{0,4}$にルーティングされる。ＳＤＮＰゲートウェイノード$M_{0,4}$は次に、ゾーンＵ７のセキュリティクレデンシャル情報を使用して、パケット１７３０Ｈをファイルストレージノード$F_{7,1}$にルーティングする。一方、ＳＤＮＰファイル２を運ぶタグ２をＩＤとするパケット１７３０Ｌは、ＳＤＮＰゲートウェイノード$M_{0,8}$に単独でルーティングされる。次に、ＳＤＮＰゲートウェイノード$M_{0,8}$は、ゾーンＵ９のセキュリティクレデンシャル情報を使用して、パケット１７３０Ｌをファイルストレージノード$F_{9,4}$にルーティングする。

【０６５９】

ほぼ同時に、ＳＤＮＰファイル３を運ぶ、タグ３をＩＤとして付与されたパケット１７３０Ｍは、ＳＤＮＰゲートウェイノード$M_{0,8}$にも単独でルーティングされるが、必ずしもタグ２をＩＤとして付与されたデータパケット１７３０Ｌと同じメッシュルーティング

パスを使用しない。ＳＤＮＰゲートウェイノード$M_{0,8}$はさらに、同じくゾーンＵ９のセキュリティクレデンシャル情報を使用して、タグ３を付与されたパケット１７３０Ｍをファイルストレージノード$F_{9,1}$にルーティングする。

【０６６０】

このようにして、ＳＤＮＰファイル１はゾーンＵ７のセキュリティクレデンシャル情報を使用してファイルストレージノード$F_{7,1}$に配信され、ＳＤＮＰファイル２及びＳＤＮＰファイル３は、ゾーン９のセキュリティクレデンシャル情報を使用してファイルストレージノード$F_{9,4}$及び$F_{9,1}$にそれぞれ配信される。これらのファイルはクライアントノード$C_{1,1}$が所有しているが、クライアントはこれらのファイルの内容をエンコードし保護するために使用されるセキュリティクレデンシャル情報に対するアクセス権を有していない。どのファイルストレージノードにもすべてのデータが含まれてはいないこと、またデータを所有しているクライアントはデータの保存時に使用されるセキュリティ認証情報へのアクセス権がないことから、ハッカーがファイルの内容を盗むことは、次の理由から困難である：（ｉ）ファイルの内容に一貫性がなく、使用不可能な断片に分割されている、（ｉｉ）すべてのファイルが異なるセキュリティクレデンシャル情報を使用してデータをスクランブル化し暗号化している、（ｉｉｉ）すべてのファイルが異なる場所及び異なるラストマイルネットワークに保存されている、（ｉｖ）これらの様々な保存データが同じＳＤＮＰソースファイルからのものであることを知る方法が存在しない。ファイルストレージサーバを含むゾーンは、「ストレージ側」ゾーンとも称され、ファイルの所有者が存在しているゾーン（つまりＳＤＮＰクラウドの反対側のゾーン）と区別されることがある。この定義により、ゾーンＵ１はＳＤＮＰクライアントゾーンであり、「ファイル所有者」ゾーンとも呼ばれ、一方、ゾーンＵ７及びＵ９は「ストレージ側」ゾーンとなる。

【０６６１】

ファイルストレージ上でのＳＤＮＰネットワーク通信プロトコルの適用方法について「書き込み操作」を例として図８２Ａのフローチャートで説明する。ここでは、ＳＤＮＰクライアントとファイル所有者は自分のデータをハイパーセキュアファイルストレージサーバに保存、つまり書き込む一般的な手順を示している。図に示されるように、ＳＤＮＰクライアント１７００Ａは、ＳＤＮＰ分割操作１０５７及びパース（構文解析）機能１０５２を使用して未パースファイル１７０５を分割し、マルチパートファイルまたはドキュメントを生成する。この例では、パースされたファイル１７０６Ａ、１７０６Ｂ、１７０６Ｃで構成される３パートのファイルである。必要があれば、ファイルのコンテンツを分割する前にスクランブル化しておいてもよい。これら３つのファイルは、無関係のデータまたはコミュニケとしてＳＤＮＰネットワークを介して転送される。ＳＤＮＰネットワークを介して最終宛先にルーティングするための手順は、ハイパーセキュアラストマイル通信に関して本明細書で開示し、ＳＤＮＰクラウド内のメッシュルーティングについてすでに説明した方法と同じ方法を使用している。具体的には、ラストマイルハイパーセキュアトランスポート１７０７は、ゾーンＵ１に従ってセキュリティクレデンシャル情報を使用している。ＳＤＮＰクラウドのハイパーセキュアメッシュトランスポート１７０８は、ゾーンＺ１セキュリティクレデンシャル情報を採用している。これらのハイパーセキュアデータ伝送操作は大きなブロックとして表されるが、パケット転送は、本開示において説明されるルータ、サーバ、及びソフトスイッチのネットワーク全体にわたり、マスターキー、中央制御、及びパケットの内容へのアクセス権のない分散システムを使用して行われる。

【０６６２】

ゾーンＵ１のラストマイルルーティングでは、限られた数のルーティング選択肢を含むインフラストラクチャを介してデータパケットの送信を行うことができるが、マルチＰＨＹラストリンクルーティング、複数のＳＤＮＰゲートウェイへの順次パケットルーティング、及び動的送信元アドレッシングの使用（つまりクライアントのＩＰアドレスの名前の変更）などを含むハイパーセキュアラストマイル通信に関して説明した方法は、ハイパーセキュアファイルストレージ操作にも同様に適用できる。データパケットがＳＤＮＰクラウドに到達すると、そのトランスポートは、スクランブル化され動的に暗号化されたデー

タを使用した匿名メッシュルーティングを使用して、ファイルコンテンツはもとより、この通信に関連するメタデータの監視をも防止する。最終的には、３つのデータパケットはすべて、異なるＳＤＮＰファイルストレージサーバ１７００Ｈ、１７００Ｍ、及び１７００Ｌに到達し、それぞれ異なるセキュリティゾーンのＳＤＮＰノードＦ$_{7,1}$、Ｆ$_{9,1}$、及びＦ$_{9,4}$に配置される。ネットワークトランスポート後、パースされたファイル１は、ゾーンＵ７ファイルセキュリティ操作１７０９Ａに従って処理され、ＳＤＮＰファイルストレージノードＦ$_{7,1}$に格納される。パースされたファイル２及び３は、ゾーンＵ９ファイルセキュリティ操作１７０９Ｂ及び１７０９Ｃに従って処理され、ＳＤＮＰファイルストレージノードＦ$_{9,1}$及びＦ$_{9,4}$に格納される。このように、１つのファイルにすべてのデータが含まれることはなく、１つのセキュリティクレデンシャル情報ですべてのコンポーネントファイルのロックを解除して元のファイルを再作成することはできない。

【０６６３】

図８２Ｂに示すハイパーセキュア保存ファイルの「読み取り操作」では、ファイルストレージサーバとＳＤＮＰクライアント（つまりファイルの所有者）との間のデータ転送の順序が逆になっている。ハイパーセキュアファイルの読み取りは、ファイルが最初に逆の順序で保存されたプロセスを元に戻す処理であり、次のように行われる：（ｉ）各ストレージサーバ内のパースされたファイルを識別、（ｉｉ）パースされた各ファイルからローカルストレージセキュリティ対策部を削除、（ｉｉｉ）回復された各パースされたファイルを、ＳＤＮＰクラウド及びハイパーセキュアラストマイルを介してＳＤＮＰクライアントに戻す、（ｉｖ）様々な関連コミュニケからパースされたファイルを収集、（ｖ）クライアントのローカルセキュリティクレデンシャル情報を使用してパースされたファイルをマージし、適切にスクランブルを解除して、元のファイルを回復する。

【０６６４】

ハイパーセキュアファイルの「読み取り操作」をさらに詳しく説明するため、ファイルストレージノードＦ$_{7,1}$に保存されているファイルストレージサーバ１７００Ｈの関連コンテンツが、ゾーンＵ７ファイルセキュリティ操作１７０９Ａを使用して処理され、パースされたファイル１が回復されている。パースされたファイル２または３とは無関係に、パースされたファイル１は、ゾーンＺ１セキュリティクレデンシャル情報を使用してハイパーセキュアトランスポート操作１７０８により、またそれに続いてゾーンＵ１のラストマイルハイパーセキュアトランスポート操作１７０７により、簡略形式で示されるＳＤＮＰクラウドを用いてＳＤＮＰクライアントノードＣ$_{1,1}$に戻される。同時に、ファイルストレージノードＦ$_{9,1}$に保存されているファイルストレージサーバ１７００Ｍの関連コンテンツが、ゾーンＵ９ファイルセキュリティ操作１７０９Ｂを使用して処理され、パースされたファイル２が回復される。パースされたファイル１または３とは無関係に、パースされたファイル２は、ゾーンＺ１セキュリティクレデンシャル情報を使用してハイパーセキュアトランスポート操作１７０８により、またそれに続いてゾーンＵ１のラストマイルハイパーセキュアトランスポート操作１７０７により、簡略形式で示されるＳＤＮＰクラウドを用いてＳＤＮＰクライアントノードＣ$_{1,1}$に戻される。一方、ファイルストレージノードＦ$_{9,4}$に保存されているファイルストレージサーバ１７００Ｌの関連コンテンツは、ゾーンＵ９ファイルセキュリティ操作１７０９Ｃを使用して処理され、パースされたファイル３が回復される。パースされたファイル１または２とは無関係に、パースされたファイル３は、ゾーンＺ１セキュリティクレデンシャル情報を使用してハイパーセキュアトランスポート操作１７０８により、またそれに続いてゾーンＵ１のラストマイルハイパーセキュアトランスポート操作１７０７により、簡略形式で示されるＳＤＮＰクラウドを用いてＳＤＮＰクライアントノードＣ$_{1,1}$に戻される。

【０６６５】

読み取り操作中の３つのパースされたファイルの独立したパケットルーティングを図８３に例示する。ここで、サーバノード１７００Ｈは、ＳＤＮＰファイル１とＩＤ「タグ７」を含むデータパケット１７３１Ｈを、ＴＣＰトランスポートを使用して、ファイルストレージアドレスＩＰ　Ｆ$_{7,1}$からアドレスＩＰ　Ｍ$_{0,4}$のＳＤＮＰゲートウェイサーバ

に送信する。パケット１７３１Ｈには、以前にトライチャネル通信でシグナリングサーバによって配信されたコマンド及び制御パケットで提供されたプリアンブル７とその他の情報を含むヘッダ１７２７Ｈが含まれている。

【０６６６】

一方、サーバノード１７００Ｌは、ＳＤＮＰファイル２とＩＤ「タグ９」を含むデータパケット１７３１Ｌを、ＴＣＰトランスポートを使用して、ファイルストレージアドレスＩＰ　$F_{9,4}$からアドレスＩＰ　$M_{0,8}$のＳＤＮＰゲートウェイサーバに送信する。パケット１７３１Ｌには、以前にトライチャネル通信でシグナリングサーバによって配信されたコマンド及び制御パケットで提供されたプリアンブル９とその他の情報を含むヘッダ１７２７Ｌが含まれている。サーバノード１７００Ｍは、ＳＤＮＰファイル１とＩＤ「タグ８」を含むデータパケット１７３１Ｍを、ＴＣＰトランスポートを使用して、ファイルストレージアドレスＩＰ　$F_{9,1}$からアドレスＩＰ　$M_{0,8}$のＳＤＮＰゲートウェイサーバへ送信する。

【０６６７】

パケット１７３１Ｍには、以前にトライチャネル通信でシグナリングサーバによって配信されたコマンド及び制御パケットで提供されたプリアンブル９とその他の情報を含むヘッダ１７２７Ｍが含まれている。３つのデータパケット１７３１Ｈ、１７３１Ｌ、１７３１Ｍは、ゾーンＺ１セキュリティクレデンシャル情報を使用してＳＤＮＰクラウドを通過し、ＳＤＮＰクラウドサーバ１７０１ＵがホストするＳＤＮＰゲートウェイ$M_{0,0}$から最終的に出現する。ここで、これらのデータパケットは対応するゾーンヘッダ１７２７Ｘ及びゾーンＵ１セキュリティクレデンシャル情報を使用して連続データパケット１７３１Ｘで順次、アドレスＩＰ　$C_{1,1}$のクライアントデバイス１７００Ａに送られる。

【０６６８】

図８２Ｂをもう一度見てみよう。３つのパース済みファイル１、２、３、すなわち１７０６Ａ、１７０６Ｂ、１７０６Ｃが独立したルーティングを使用してＳＤＮＰクライアントデバイス１７００Ａに送られた後、これらのファイルはミキシング操作１０６１により単一のパースされていないファイル１７０５にマージされ、その後、該当する場合には、ゾーンＵ１セキュリティクレデンシャル情報に従ってスクランブル解除操作が実行される（図示せず）。

【０６６９】

追加のファイルサーバ操作を追加して保存データを保護する方法をとるのではなく、セキュリティ操作１７０９Ａ、１７０９Ｂ、及び１７０９Ｃが実際にＳＤＮＰクラウドと対応するストレージサーバ１７００Ｈ、１７００Ｍ、及び１７００Ｌの間のラストマイルハイパーセキュア通信を構成している。ＳＤＮＰ通信プロトコルを使用したレイヤ３のネットワーク接続ツールとして、ＳＤＮＰファイルストレージは、ジャンクデータ挿入やジャンクファイルなどのデータ偽装手法の使用を含め、複数の分散型不揮発性データドライブにスクランブル化、断片化、及び暗号化されたデータを保存しており、本質的にハイパーセキュアである。前述のデータセキュリティ方法とは別に、本明細書で開示するハイパーセキュアストレージでは、意味のあるメタデータ、ファイル所有者への追跡可能性、ファイルが配信された経路、あるいはまた元のソースファイルから不明な構成要素を保持している任意の他のファイルストレージサーバの身元情報などが一切含まれない匿名ファイル名が使用されている。

【０６７０】

ＳＤＮＰネットワークの相互運用性、ストレージサーバの物理的実現など、レイヤ１のＰＨＹ実装とレイヤ２のトランスポートは別として、プロトコルはストレージ機能、アクセス時間、またはグローバルアクセシビリティに影響することなく大きく変わる可能性がある。図８４Ａは、ＳＤＮＰファイルストレージサーバの物理的な実装例を示している。一番上の構成例はＳＤＮＰゲートウェイ１７０１ＢがルータＲ７を介してＳＤＮＰファイルサーバに接続されている。ネットワークのパフォーマンスを高め、攻撃に対するレジリエンシー（回復力）を高めるため、中央の構成例は、光ファイバ９１を使用してＳＤＮＰ

ゲートウェイ１７０１ＢとＳＤＮＰファイルストレージサーバ１７４０Ａとを直結し、ルータを介在させていない。一番下の例では、ファイルストレージサーバは、サーバコントローラ１７４０Ｂとストレージドライブ１７４０Ｃ及び１７４０Ｄを装備し、より大きなメモリアレイを追加できるようになっている。これらのドライブには、ハードディスクドライブや、フラッシュドライブベースの不揮発性メモリなど任意のメディアを導入することができる。アクセス制限を強化するため、ＳＤＮＰゲートウェイとＳＤＮＰファイルストレージサーバを物理的に同じ場所に配置し、それらの接続にはファイバリンクのみを使用している。これらの設備は同じ部屋を共有することも可能であり、例えば、保管室に物理的に固定し、施設に入る人物に対しては厳格に管理されたアクセス制御と監視が行われる。

【０６７１】

図８４Ｂはさらに、断片化されたデータファイルの一部がファイル所有者のサイトでローカルに保存できることを示している。図に示されるように、ファイル所有者のデスクトップ３６は、（ｉ）サーバ１７０１Ａ上のＳＤＮＰゲートウェイノード$M_{0,0}$に接続されたＷｉＦｉルータ１３５２を介してアクセスされるローカルファイルストレージサーバ１７４０Ａ、（ｉｉ）ＳＤＮＰゲートウェイノード$M_{0,4}$に接続されたファイルストレージサーバ１７４０Ｂ、及び（ｉｉｉ）ＳＤＮＰゲートウェイノード$M_{0,8}$に接続されているファイルストレージサーバ１７４０Ｃ、などのように、分散化されたファイルをいくつかのデバイスにまたがり保存できる。データは分散されたドライブ１７４０Ａ、１７４０Ｂ、１７４０Ｃに保存され断片化されているため、ローカルファイルサーバ１７４０Ａとファイル所有者デスクトップ３６が同じＷｉＦｉ　１３５２を共有しているとしても、ノートブック３５、タブレット３３、携帯電話２９などの他のデバイスは保存されているファイルにアクセスすることはできない。

【０６７２】

非冗長ハイパーセキュアファイルマッピングと呼ばれる、ひとつのファイルの各パース部分を別々のファイルストレージサーバに一意に格納するプロセスを図８５Ａに示す。この図に示されるように、ＳＤＮＰクライアントノード$C_{1,1}$を含むクライアントデバイス１７００Ａは、パースされたファイル１７０６Ａをファイルストレージサーバ１７００Ｈに、パースされたファイル１７０６Ｂをファイルストレージサーバ１７００Ｍに、そしてパースされたファイル１７０６Ｃをファイルストレージサーバ１７００Ｌにそれぞれ排他的に格納しており、これらはストレージノード$F_{7,1}$、$F_{9,1}$、及び$F_{9,4}$とパースされたファイル１、２、及び３との間の１対１のファイルマッピングに対応している。これらのファイルの配信にはハイパーセキュアラストマイル通信を使用して、データの転送とその保存の安全を確保する。非冗長ファイルマッピングには、ファイルストレージサーバのいずれかが一時的または永続的に失われると、ファイルのアクセスと回復が困難になる、という欠点がある。本明細書の観点から、「復元力」及び「復元性がある」という用語を、保存されたデータへの保証された、かつタイムリーなアクセス、すなわち保存されたデータが失われない、またはアクセスが相当な期間にわたって損なわれない信頼性があることを表すために使用している。このことから、ここに示されている非冗長型のハイパーセキュアファイルマッピングは、あるひとつのポイントで障害が発生すると、ファイルアクセスに問題が生じるため、復元力が低下することを表している。復元力の弱さは、同じデータが複数のファイルストレージサーバに保存されているような冗長システムによって克服することができる。

【０６７３】

データストレージシステムの復元力を説明または評価するもうひとつの指標として、本明細書で定義している読み取り冗長係数ＲＲＦがある。この指標は、一次データストレージが利用できない場合にデータアクセスを提供するバックアップシステムの数を定義するために使用する。この例では、一意のデータ毎にひとつの場所が設けられている。これにより、読み取りの冗長性係数はゼロ、すなわち数学的にはＲＲＦ＝０となる。つまり、シングルポイント接続、すなわちファイルサーバの障害が発生すると、ファイル所有者がフ

ァイルを読み取れなくなるため、一時的または永続的なデータ損失が発生する可能性がある。

【０６７４】

図８５Ｂは、読み取り冗長性係数がＲＲＦ＝１であるファイルマッピングを示している。この例では、パースされたファイル１はファイルストレージサーバノードＦ$_{9,4}$及びＦ$_{7,1}$に格納され、パースされたファイル２はファイルストレージサーバノードＦ$_{9,1}$及びＦ$_{7,1}$に、そしてパースされたファイル３はファイルストレージサーバノードＦ$_{9,4}$及びＦ$_{9,1}$に格納されている。このような実装であれば、ファイルストレージサーバノードＦ$_{9,1}$が機能しなくなったり使用できなくなったりした場合でも、パースされたファイル３にはファイルストレージサーバノードＦ$_{9,4}$から、パースされたファイル２にはファイルストレージサーバノードＦ$_{7,1}$からそれぞれアクセスできる。そのため、いずれかひとつのストレージノードに障害が発生しても、ハイパーセキュアファイルへの読み取りアクセスができなくなることはない。図８５Ｃは、ＲＲＦ＝２のハイパーセキュアファイルマッピングである。このファイルマッピングにはファイルストレージサーバ１７００Ｌ、１７００Ｍ、及び１７００Ｈが含まれているが、ファイルストレージサーバ１７００Ｊ、１７００Ｅ、及び１７００Ｆからなる２つ目のグループを追加して、それぞれに対応するファイルストレージサーバノードＦ$_{8,2}$、Ｆ$_{4,4}$、及びＦ$_{6,8}$が用意されている。こうして、ファイルストレージサーバ１７００Ｊはファイルストレージサーバ１７００Ｌのバックアップ、ファイルストレージサーバ１７００Ｅはファイルストレージサーバ１７００Ｍのバックアップ、そしてファイルストレージサーバ１７００Ｆはファイルストレージサーバ１７００Ｈのバックアップとしてそれぞれの役割を果たすことになる。図に示されている例は３つのセクションにパースされたファイルで構成されているが、必要に応じてドキュメントはより多くのセクションに分割できる。ハイパーセキュアストレージを保証するため、元ファイルの分割数は２つ未満にすべきではなく、理想的には３つ以上にすることが推奨される。

【０６７５】

ハイパーセキュアファイルストレージを使用して冗長ファイルを保存及び読み取るプロセスを説明するため、ストレージプロセスを円滑化するために使用されるＳＤＮＰネットワーク上にオーバーレイされたコミュニケ及びファイルの転送機能のトランザクションシーケンスを説明することにする。図８６のネットワークには、例として、クライアントノードＣ$_{1,1}$を実装するクライアントデバイス１７００Ａ、ルータ１７０２Ｇ、ＳＤＮＰノードＳを実装するシグナリングサーバ１７１５、ＳＤＮＰノードＮＳを実装するネームサーバ１７１４、ＳＤＮＰクラウドノードＭ$_{0,0}$、Ｍ$_{0,4}$、及びＭ$_{0,8}$を実装するクラウドサーバ１７０１Ｕ、及びＳＤＮＰファイルストレージノードＦ$_{7,1}$、Ｆ$_{9,4}$及びＦ$_{9,1}$をそれぞれ実現するＳＤＮＰファイルストレージサーバ１７００Ｈ、１７００Ｌ、及び１７００Ｍが含まれている。

【０６７６】

図８７Ａでは、アドレス「ＩＰ　Ｃ$_{1,1}$」のクライアントデバイス１７００Ａは、Ｃ＆Ｃペイロード１７１１Ａを含み、ファイルサイズとセキュリティ及び冗長性の要求レベルの記述を含むデータパケット１７１０Ａにより、アドレス「ＩＰ　Ｓ」のシグナリングサーバ１７１５にファイル書き込み要求を出す。図８７Ｂでは、シグナリングサーバ１７１５は、データパケット１７１０Ｂをネームサーバ１７１４に送信して、ファイルストレージサーバノードＦ$_{7,1}$、Ｆ$_{9,4}$、及びＦ$_{9,1}$のＩＰアドレスまたはＳＤＮＰアドレスを要求する。使用するファイルアドレスサーバノードの選択は、ストレージノードのリストからランダムに選択する方法と、クライアントの近くで利用可能なノードまたは災害のない地域で利用可能なノードなどの地理的条件に基づいて選択する方法がある。選択は、ノードの未使用メモリ容量、ファイルストレージノードへの伝播時間、ノードの稼働時間の信頼性評価、その他の考慮事項などのパフォーマンスパラメータに基づいて行うこともできる。図８７Ｃでは、ネームサーバ１７１４は、ファイルストレージサーバノードＦ$_{7,1}$、Ｆ$_{9,4}$、及びＦ$_{9,1}$のＩＰまたはＳＤＮＰアドレスを含むシグナリングサーバ１

７１５のデータパケット１７１０Ｃを送信する。シグナリングサーバ１７１５は次に、ファイルストレージサーバ１７００Ｈ、１７００Ｌ、及び１７００Ｍへのパースされたファイルのラストマイル及びメッシュクラウドによる配信を計算する。

【０６７７】

図８７Ｄでは、シグナリングサーバ１７１５は、データパケット１７１０Ｄをクライアントデバイス１７００Ａに送信し、このパケットは、アドレス「ＩＰ　Ｓ」からルータ１７０２Ｇを介して「ＩＰ　$Ｃ_{1,1}$」にルーティングされる。データパケット１７１１ＤにはＣ＆Ｃペイロード１７１１Ｄが含まれている。このペイロードにはクライアントゾーンのゾーンＵ１で間もなく行われるファイル転送のラストマイルルーティングが指示されている。具体的には、タグ１、タグ２、及びタグ３で各パケットが指定され（簡略化してタグＸと表記）、アドレス「ＩＰ　$Ｃ_{1,1}$」から、「ＩＰ　$Ｍ_{0,0}$」のＳＤＮＰゲートウェイへの複数パケットのルーティング情報が含まれている。同時に、シグナリングサーバ１７１５は、データパケット１７１０ＥをＳＤＮＰゲートウェイ１７０１Ｕに送信する。このパケットはアドレス「ＩＰ　Ｓ」から「ＩＰ　$Ｍ_{0,0}$」にルーティングされる。このパケットには、ＩＤタグＸを持つパケットのゾーンＺ１セキュリティクレデンシャル情報を使用するＳＤＮＰクラウドルーティングを示すＣ＆Ｃペイロード１７１１Ｅが含まれている。このケースでは、ＳＤＮＰゲートウェイアドレス「ＳＤＮＰ　$Ｍ_{0,0}$」からクラウド内の次のノードまで、すなわちアドレス「ＳＤＮＰ　$Ｍ_{0,5}$」（図示せず）までのルートである。「セキュア動的通信ネットワーク及びプロトコル」に従い、メッシュ式匿名断片化トランスポートを使用したＳＤＮＰクラウド全体のデータパケットのルーティングは、リアルタイムネットワークの現在の状態に基づいて動的に選択される。具体的には、ＳＤＮＰゲートウェイに送られてくるリアルタイムデータパケットのＳＤＮＰクラウド内でのルーティングは、ＳＤＮＰクラウド内のノード間の伝播遅延と、シグナリングサーバが割り当てた各リアルタイムデータパケットの緊急度に依存している。

【０６７８】

図８７Ｅのシグナリングサーバ１７１５は、ストレージ側にあるラストマイルノード、すなわちゾーンＵ７及びＵ９にＣ＆Ｃデータパケットを送信する。図に示されるように、データパケット１７１０Ｆは、ＳＤＮＰゲートウェイ$Ｍ_{0,4}$に送信される。パケットはアドレス「ＩＰ　Ｓ」から「ＩＰ　$Ｍ_{0,4}$」にルーティングされ、Ｃ＆Ｃペイロード１７１１Ｆには、タグ１のデータパケットがゲートウェイノード$Ｍ_{0,4}$に送られ、受信後にラストマイルアドレス「ＩＰ　$Ｆ_{7,1}$」に転送されることが示されている。２番目のデータパケット１７１０Ｇは、シグナリングサーバ１７１５からアドレス「ＩＰ　$Ｆ_{7,1}$」のファイルストレージサーバ１７００Ｈに転送される。ゾーンＵ７のストレージのＣ＆Ｃペイロードは、送信元アドレス「ＩＰ　$Ｍ_{0,4}$」からのＩＤタグ１を含む着信パケットを定義するが、ノードの機能はストレージであり、通信ではないため、宛先フィールドは空のまま、つまりヌル値が埋め込まれている。コマンド及び制御データパケットがネットワークに配信されると、ファイル転送が実行される。

【０６７９】

図８８は、ファイルのハイパーセキュアストレージ中にフラグメント化データトランスポートについて説明している。ここで、クライアント１７００Ａは、アドレス「ＩＰ　$Ｃ_{1,1}$」からアドレス「ＩＰ　$Ｍ_{0,0}$」のＳＤＮＰゲートウェイまでＴＣＰデータトランスポートで、ＳＤＮＰデータファイル１、２、及び３を含む一連のデータパケット１７１２Ｘを送る。各データパケットには一意の識別子ＩＤ、つまりタグ１、タグ２、及びタグ３が含まれている。これらのファイルは、その後、ＳＤＮＰクラウドを介して他のゲートウェイ、つまりＳＤＮＰゲートウェイノード$Ｍ_{0,4}$及び$Ｍ_{0,8}$に転送される。ゲートウェイノード$Ｍ_{0,4}$に到着するＳＤＮＰデータ１を含むパケットは、データパケット１７１２Ａで、ゾーンＵ７セキュリティクレデンシャル情報とＴＣＰを使用してアドレス「ＩＰ　$Ｍ_{0,4}$」から「ＩＰ　$Ｆ_{7,1}$」に転送される。一方、ゲートウェイノード$Ｍ_{0,8}$に到着するデータ２及びデータ３パケットは、データパケット１７１２Ｂ及び１７１２Ｃで、ゾーンＵ９セキュリティクレデンシャル情報を使用して、アドレス「ＩＰ　$Ｍ_{0,8}$」からアド

レス「ＩＰ　Ｆ９，４」及び「ＩＰ　Ｆ９，１」にそれぞれ転送される。ストレージには、ドライブのデータスキャンを防ぐために、ファイルサーバ内にローカル暗号化機能が含まれる場合もある。この暗号化プロセスはローカルで実行され、ＳＤＮＰのセキュリティ対策とは関係がない。データパケットのコンテンツであるＳＤＮＰデータ１、ＳＤＮＰデータ２、ＳＤＮＰ　３には、保存対象の実際の断片化されたファイルが含まれている。

【０６８０】

各データパケット内のプリアンブル、例えばデータパケット１７１２Ａのプリアンブル１には、対称鍵暗号化操作の一部としてクライアントにより提供される暗号鍵が含まれる場合もある。対称鍵暗号化を使用して、ＳＤＮＰクライアントノードＣ１，１は、暗号化用と復号化用のスプリットキーを生成する。対称暗号鍵は、この例では、データパケット１７１２Ａによって配信されるファイルストレージサーバノードＦ７，１に提供される。将来、クライアントが保存されているファイルの内容の読み取りまたはアクセスを要求するたびに、ファイルストレージサーバノードＦ７，１は、この暗号鍵を使用して要求されたファイルを暗号化してからクライアントに送り返す。当該クライアントのみが関連する復号鍵を保持しているため、他のクライアントが読み取ったこのファイルを開くことはできない。この方法では追加の保護層が提供されるが、欠点もある。ひとつのクライアントしか読み取り操作としてファイルにアクセスできないため、元のクライアントデバイスが盗難、損傷、または紛失した場合には、冗長アクセスをしやすくするために必要とされるクライアントファイルの複数の「所有者」を使用できない。

【０６８１】

データ転送やファイル保存のプロセスを実行する際に、シグナリングサーバ１７１５は、「リンク応答」メッセージルーティングに関する指示をファイル保存サーバ１７００Ｈ、１７００Ｌ、及び１７００Ｍに送信する。リンク応答とは、書き込み操作が成功し、パースされた各ファイルの保存が完了したことをクライアントに確認するデータパケットとＣ＆Ｃペイロードである。これらのメッセージは、転送及びパースされたファイルの保存に関係する各ファイルストレージサーバから独立して、クライアントファイル所有者に送信される。ファイルサーバは、互いについての知識がなく独立して書き込み確認応答をクライアントに送信し、この書き込み通信応答は、書き込み操作時の運用状態とは異なる一意の状態を含む独立したセキュリティクレデンシャル情報を使用して送信される。これらのリンク応答メッセージのルーティングは、ファイルの転送に使用されるものと同じルーティングパスの逆方向が必ずしも使用されるわけではない。これらの応答は、ファイル所有者を見つけるためのトレースバックとしてサイバー攻撃者によって使用されかねない。その代わりに、リンク応答はパケットＩＤを使用して、保存されているファイルが同じファイルの一部であり、同じ断片化された書き込み操作の一部として保存されていることをクライアントに対して明らかにする。

【０６８２】

動作中、シグナリングサーバは、リンク応答メッセージのルーティングを、ファイルストレージサーバ、クライアントファイル所有者、及びリンク応答メッセージルーティングに関与するすべての中間ＳＤＮＰノードに送信する。シグナリングサーバ１７１５は、図８９Ａの例に示されるように、コマンド及び制御ペイロードを含むデータパケットを使用して、リンク応答メッセージルーティングを調整する。この例で、ファイルストレージサーバ１７００Ｈは、アドレスＩＰ　Ｆ７，１からアドレスＩＰ　Ｍ０，４への「リンク１応答」ルーティングのためのヘッダデータを含むＣ＆Ｃペイロード１７２２Ｇを含むデータパケット１７２１Ｇを受信する。ＳＤＮＰゲートウェイノードＭ０，４は、アドレス「ＳＤＮＰ　Ｍ０，４」からＳＤＮＰクラウド内の別のノード（この場合はアドレス「ＳＤＮＰ　Ｍ０、１４」）へのタグ１データパケットのルーティングを記述しているＣ＆Ｃペイロード１７２２Ｆを含むデータパケット１７１２Ｆを受信する。同様に、シグナリングサーバ１７１５は、アドレス「ＩＰ　Ｆ９，１」から「ＩＰ　Ｍ０，８」への「リンク３応答」のタグ３のパケットラストマイルルーティング指示を含むファイルストレージサーバ１７００Ｍのデータパケット１７２１Ｍを送信する。ファイルデータパケットとそれらに対応する

リンク応答メッセージのストレージ側のラストマイルルーティングは同じまたは類似している場合があるが、ＳＤＮＰクラウドを介した応答メッセージのルーティングは、ＳＤＮＰクラウドの動的性質のため、ほぼ同じではない。

【０６８３】

参加ファイルストレージサーバノードからのリンク応答メッセージの実際のルーティングを図８９Ｂに示す。この図のように、ファイルストレージサーバ１７００Ｈは、タグ１によって識別され、ペイロード「ＦＳリンク１」を含むデータパケット１７２０Ａで応答する。このパケットは、ゾーンＵ７のセキュリティクレデンシャル情報を使用して、アドレス「ＩＰ　$F_{7,1}$」からアドレス「ＩＰ　$M_{0,4}$」のＳＤＮＰゲートウェイにルーティングされる。ＳＤＮＰゲートウェイから、タグ１のデータパケットは、ＳＤＮＰクラウドを介してアドレス「ＳＤＮＰ　$M_{0,0}$」のクライアント側ゲートウェイにルーティングされる。ここで、アドレスはラストマイルデータパケット１７２０Ｘに変換されてから、ＴＣＰトランスポート、ゾーンＵ１セキュリティ認証情報、及びタグ１のデータ、つまりプリアンブル１とＦＳリンク１を使用して、アドレス「ＩＰ　$M_{0,0}$」から「ＩＰ　$C_{1,1}$」にルーティングされる。

【０６８４】

同様にして、ファイルストレージサーバ１７００Ｌは、タグ２によって識別され、ペイロード「ＦＳリンク２」を含むデータパケット１７２０Ｂを応答として返す。このパケットは、ゾーンＵ９のセキュリティクレデンシャル情報を使用して、アドレス「ＩＰ　$F_{9,4}$」からアドレス「ＩＰ　$M_{0,8}$」のＳＤＮＰゲートウェイにルーティングされる。ＳＤＮＰゲートウェイから、タグ２で識別されたデータパケットは、ＳＤＮＰクラウドを介してアドレス「ＳＤＮＰ　$M_{0,0}$」のクライアント側ゲートウェイにルーティングされる（ルーティングは図示せず）。ここで、アドレスがラストマイルデータパケット１７２０Ｘに変換されてから、データパケットはＴＣＰトランスポート、ゾーンＵ１セキュリティ認証情報、及びタグ２のデータ、つまりプリアンブル２とＦＳリンク２を使用して、アドレス「ＩＰ　$M_{0,0}$」から「ＩＰ　$C_{1,1}$」にルーティングされる。

【０６８５】

タグ３によって識別され、ペイロード「ＦＳリンク３」を運ぶパースされた３番目のファイルが、データパケット１７２０Ｃを介してファイルストレージサーバ１７００Ｍから送信される。このタグ３パケットは、ゾーンＵ９のセキュリティクレデンシャル情報を使用して、アドレス「ＩＰ　$F_{9,1}$」からアドレス「ＩＰ　$M_{0,8}$」のＳＤＮＰゲートウェイにルーティングされる。ＳＤＮＰゲートウェイから、タグ３データパケットは、ＳＤＮＰクラウドを介してアドレス「ＳＤＮＰ　$M_{0,0}$」のクライアント側ゲートウェイにルーティングされる。ここで、アドレスがラストマイルデータパケット１７２０Ｘに変換されてから、ゾーンＵ１のセキュリティ認証情報を使用し、タグ３のデータ、すなわちプリアンブル３とＦＳリンク３を運ぶＴＣＰトランスポートを使用して、アドレス「ＩＰ　$M_{0,0}$」から「ＩＰ　$C_{1,1}$」にルーティングされる。

【０６８６】

図８９Ｃは、ファイルストレージサーバ１７００Ｈからクライアント及びファイル所有者に戻されるＦＳリンクデータパケット１７２０Ａのコンテンツの例を示している。図に示されるように、データパケットには、セキュリティゾーンＵ７で作成されたＩＤタグ１を含むパケットでＴＣＰを使用するアドレス「ＩＰ　$F_{7,1}$」からアドレス「ＩＰ　$M_{0,4}$」のＳＤＮＰゲートウェイへのラストマイルルーティングが記述されている。応答プリアンブル１７１９Ａには、データペイロード１７４１Ａの説明に加えて、クライアントに配信されるＦＳリンクデータパケット１７２０Ａのセキュリティを実行または強化するために使用されるオプションのセキュリティクレデンシャル情報も含まれている。ただし、トライチャンネル通信では、応答プリアンブル１７１９Ａに含まれる応答セキュリティクレデンシャル情報は通常不要であり、以降にハイパーセキュアの保存ファイルにアクセスして開くためにクライアントが使用するクレデンシャル情報とは無関係である。クライアントからファイルストレージノード$F_{7,1}$に格納されているファイルへのリンクを作成

するために必要なアクセスクレデンシャル情報は、代わりにデータフィールド１７４１Ａ内に格納されており、以下の内容が含まれる。
・断片化されたファイルの該当部分が保存されているファイルストレージサーバを識別するために必要な一意のネットワークタグ、ＳＤＮＰアドレス、または擬似アドレス。
・「ストレージ側」のセキュリティゾーン（クライアントのゾーンではない）でファイルをエンコードするために使用されるセキュリティクレデンシャル情報を定義するゾーンの説明。
・保存前のファイルのエンコード中に使用された数値シードまたは時間またはステート９２０を含むことができるシード１。
・保存操作の一部としてファイルエンコーディングを実行するために使用される数値シード９２９を含むことができるシード２。
・ゾーンＵ７の「ストレージ側」の暗号化を解読するための復号鍵１０３０を含む鍵１。この鍵は、ファイルストレージサーバの一部として動作するＤＭＺサーバに保持されている共有秘密と組み合わせて使用したり、数値シードなどの別のセキュリティクレデンシャル情報と組み合わせたりしてのみ操作できる部分的な復号鍵を表すことができる。
・クライアントに送信され、対称鍵暗号化を使用してクライアントからファイルストレージサーバに安全な命令を送信するために使用される暗号鍵１０２２を含む鍵２。
・クライアントが保存方法を明らかにすることなく、保存ファイルを識別できるようにするために使用されるファイル名またはその他の情報。

【０６８７】

前述のデータパケットは説明目的で用いられたものであり、データパケットの内容を、例示されているものとまったく同じ要素または形式に限定するものとみなしてはならない。ＳＤＮＰクライアントノード$C_{1,1}$にて受け取られるＦＳリンク１７２０Ｘは、断片化されたファイルの保存に参加しているファイルストレージサーバから受領した後、クライアントのデバイスのファイルリンクを作成するために処理される。図８９Ｄに示されるように、この操作により、複合操作１７５３を使用してＦＳリンク１７４１Ａ、１７４１Ｂ、及び１７４１Ｃが組み合わされて、ＦＳリンク集約体「ファイルストレージ読み取りリンク」１７５４が生成される。ファイルストレージリンク１７５４は、クライアントのハイパーセキュアテキストメッセンジャまたはファイル管理システムにポストされ、ハイパーセキュアファイルをシングルボタンで簡単に呼び出すことができるようにする。ハイパーセキュア操作はユーザから見えない。ファイルの所有者は、ファイルが実際に分散ファイルストレージシステム全体にわたって断片化、エンコード、及び保存されている事実を考慮する必要はない。ファイルの再コールは、ファイルがローカルに存在しているかのように行われる。したがって、ＦＳリンクは、分散ファイルストレージシステム全体に保存されているすべてのファイルにアクセスするための重要な要素である。

【０６８８】

ＦＳリンク通信の簡略化した表現を図９０Ａに示す。ここでは、３台のファイルストレージサーバすべてがそれぞれのＦＳリンクをクライアントノード$C_{1,1}$及び対応するクライアントデバイス１７００Ａに送信する。具体的には、ファイルストレージサーバ１７００ＨはＦＳリンク１を、ファイルストレージサーバ１７００ＭはＦＳリンク２を、ファイルストレージサーバ１７００ＬはＦＳリンク３を送信する。クライアントデバイス１７００Ａ内では、クライアントノード$C_{1,1}$のＳＤＮＰアプリソフトウェアが、３つの入ＦＳリンク１、２、及び３をまとめて、保存ファイルへのひとつのリンクを形成している。この結合されたリンクは、ファイルストレージの確認としてＳＤＮＰメッセンジャーに表示される。非冗長ファイル管理では、ＦＳリンク情報はクライアントデバイスにのみ送信される。ユーザファイル管理の場合、ファイルの格納が要求された時点、または確認メッセージの受信時にファイルリンクに名前を付けることができる。

【０６８９】

ファイルストレージリンクは、シグナリングサーバを介してではなく、ファイルストレージサーバからクライアントに直接送られるため、リンクを持つクライアントのみが当該

ファイルにアクセスできる。このＦＳリンクは、断片化されたファイルを呼び出して読み取るために必要となる。ＦＳリンクがなければ、保存ファイルとその内容は永久に失われ、不可逆的に回復不能となる。ＦＳリンクが失われてしまうリスクを低減するための代替手段として、ＦＳリンクを２つのクライアントデバイス、すなわちクライアントデバイスとその補助デバイス、に送信する方法がある。補助デバイスは、クライアントが所有する２番目のデバイス、あるいはビジネスケースでは会社が所有する２番目のデバイスとすることも考えられる。さらに別の考え方として、独自のログインセキュリティとユーザＩＤ検証機能を備えたもう一台のサーバを第２のデバイスとしてもよい。

【０６９０】

本明細書に従って作成された断片化された分散格納ファイルへの冗長リンクアクセスは、読み出し冗長性のあるファイルストレージシステム（すなわちＲＲＦ≧１）、及び非冗長性ファイルストレージシステムの両方に適用できる。図９０Ｂに、読み出し冗長性のない（ＲＲＦ＝０）ハイパーセキュア分散メモリシステムにおける冗長リンクの使用例を示す。このようなシステムでは、パースされたファイル１７０６Ａ、１７０６Ｂ、及び１７０６Ｃと、それらに対応するファイルストレージサーバ１７００Ｈ、１７００Ｍ、及び１７００Ｌとの間のファイルマッピングは冗長構成ではない。図に示されるように、ＦＳリンク１、２、及び３は、２つのクライアントデバイス、すなわちＳＤＮＰクライアントノード$C_{1,1}$をホストする１７００Ａと、バックアップクライアントノード$C_{2,1}$をホストする補助クライアントデバイス１７００Ｂに送信される。これらのＦＳリンクのうちの１つが失われた場合、または何らかの理由で使用できなくなった場合、バックアップクライアントのＦＳリンクをファイルの回復に使用できる。この点で、このＳＤＮＰ分散ストレージシステムは、単一リンクの冗長性を備えた非冗長読み出し実装、すなわちＲＲＦ＝０及びＬＲＦ＝１である。

【０６９１】

読み出し冗長性とリンク冗長性の両方を備えたハイパーセキュアメモリの例を図９０Ｃに示す。この図で、パースされたファイル１、２、及び３はそれぞれ２つのファイルストレージサーバにマップされている。つまり、読み出し冗長性係数ＲＲＦ＝１を実現している。また、各ＦＳリンクが２つのクライアントに送られ、リンク冗長性係数ＬＲＦ＝１を実現している。読み出し及びリンクの両方に関連する障害に対するストレージシステムの耐性は、システムが全体的なストレージ冗長性係数ＳＲＦ＝１を持つ真の冗長ハイパーセキュアファイル管理システムと見なされることを意味する。本開示では、ストレージの冗長性係数ＳＲＦを、ＲＲＦとＬＲＦの最低値に等しい冗長性係数として定義している。例えば、ＲＲＦ＝０及びＬＲＦ＝１の場合、ＳＲＦ＝０となる。もしＲＲＦ＝３及びＬＲＦ＝２であれば、全体的なストレージの冗長性係数はＳＲＦ＝２となる。全体的なシステムＳＲＦ＝３を実現するには、各パースされたファイルを４つの別個のファイルストレージサーバ（前記図８５Ｃ参照）に保存し、ＦＳリンクを４つの別個のクライアントに送信する必要がある。

【０６９２】

したがって、全体的なストレージ冗長性係数ＳＲＦは、障害からの分散ストレージシステムの復元力の直接的な尺度となる。この原理は、図９１のグラフに要約されている。グラフの横軸はファイルストレージシステムで使用されるファイルストレージサーバの数を示し、縦軸は個別のクライアントに送信されるＦＳリンクの数を示している。図に示されるように、単一のファイルストレージサーバには冗長性はない。つまり、ＲＲＦ＝０である。ファイルストレージデバイスの数を増やせば読み取りの冗長性は向上するが、リンクの冗長性には影響しない。逆に、単一のクライアントにリンクを送信してもリンクの冗長性は得られない。つまり、利用可能なファイルストレージサーバの数に関係なくＬＲＦ＝０となる。いずれの場合も、つまり、１つのストレージサーバまたは１つのクライアントリンクでは、全体としてストレージ冗長係数はＳＲＦ＝０である。つまり、Ｌ形の領域に図示されているように、ファイルストレージシステムには復元力がないことを意味している。

【０６９３】
図に示す通り、前述のように３つに分割されたパースされたファイルを３つのファイルストレージサーバに保存すると、読み出し冗長性係数はＲＲＦ＝１となる。少なくとも２つのクライアントがＦＳリンクを受信すると、ＬＲＦ≧１のリンク冗長性が実現される。ＬＲＦ＝１またはＲＲＦ＝１のいずれかの組み合わせにより、ＳＲＦ＝１であるＬ字型領域１７２４Ｂが得られる。つまり、ある程度のシステム復元力が得られる。６台のサーバが使用されている場合であっても、ＦＳリンクが２つのクライアントにしか送信されない場合には、システムは限られた程度の復元力、つまりＳＲＦ＝１しか得られない。
【０６９４】
ＦＳリンクを３つのクライアントに送信し、６つのストレージサーバにデータを冗長的に保存することにより、領域１７２４Ｃは、かなり堅牢なストレージ復元力であるＳＲＦ＝２を達成する条件を定義している。領域１７２４Ｄは、復元力がさらに強化されたＲＦ＝３を示しており、６つのファイルストレージサーバと、鍵を受信する４つのクライアントを使用している。左下隅（一番下の行と一番左の列）ストレージの復元力が最も低く、右上隅のストレージの復元力が最も高くなっている。
【０６９５】
本開示に従って作成されたハイパーセキュア分散ファイルストレージは、ＳＤＮＰ通信から多くの独創的な要素を状況に合わせて順応、すなわち再利用することによって、長期的な持続可能なセキュリティを実現する。こうした独創的な要素には次のようなものが挙げられる。
・ファイルをパースし、断片化されたコンテンツを、ネットワークに接続されていない多数のファイルストレージサーバに配布する、
・ＤＮＰがマスターキーを用いずに暗号化した匿名の断片化データ転送を動的にスクランブルするエンドツーエンドのハイパーセキュア通信を使用してクライアントとファイルストレージサーバ間でファイルを転送する、
・トレージサーバが保存データを最初に断片化及びエンコードするときに使用されるクライアントのセキュリティクレデンシャル情報にアクセスできない方法、つまりファイルストレージサーバがファイルをデコード、アクセス、または読み取るために必要とされる「クライアント側」のラストマイルセキュリティクレデンシャル情報を保持しない方法で、ファイルストレージサーバに断片化されたファイルを保存する、
・オプションとして、クライアント（ファイル所有者）が、セキュリティリンクを用いる方法を別として、格納データをデコードするために必要とされるセキュリティクレデンシャル情報を持たない方法、すなわち「クライアントサイド」のラストマイルには、ファイルをローカルでエンコードするために使用される「ストレージ側」のラストマイルセキュリティクレデンシャル情報を保持しない方法を用いて、ストレージサーバで断片化ファイルをエンコードする、
・ファイルを見つけて開くために必要なファイルストレージリンクの数を制限し、ファイル所有者のクライアントデバイス及びすべての冗長またはバックアップデバイスへのリンクに対するユーザクセスを制限する、
・ファイルリンクを実行し、読み取りまたは消去操作を呼び出すには、クライアントの多要素認証と身元検証を求める、
・匿名データパケットルーティングと匿名ファイル名の使用。データの再呼び出しにファイルリンクを使用することで、ハイパーセキュリティファイルストレージの場所または符号化に関する情報が明らかにされず、ファイルリンクを除き、ルーティング情報がＳＤＮＰネットワークやハイパーセキュアファイルストレージシステムにも保存されない、
・非公開のファイルサーバの場所を使用し、クライアント、ＳＤＮＰネットワーク、またはその他のストレージサーバには情報が存在しない匿名ＩＤを使用して、断片化されたファイルを複数のストレージサーバに分散する、
・分散型ストレージのファイルルーティングの計画作成に使用されるＳＤＮＰシグナリングサーバが、ファイルのエンコードに使用される断片化ファイルの内容やセキュリティク

レデンシャル情報にアクセスせず、またファイルコンテンツの転送に使用されるＳＤＮＰメディアノードがクライアントまたはファイルストレージサーバのＩＤまたはアドレスを含まないシングルホップＳＤＮＰデータパケットを使用する、トライチャネル通信を採用する、
・ファイルへの定期的なアクセスや反復アクセスがなされた後には、動的なファイル名の変更とデータの再配置を実施し、ファイルの書き換え操作の際にはセキュリティクレデンシャル情報を作成しなおす、
・ファイルストレージサーバのディレクトリをローカルで暗号化し、ファイルの解析を阻止する。

【０６９６】

上記により、識別可能なファイルＩＤの除去、ネットワーク全体に分散した断片化ファイルの使用（おそらく世界規模で）、そしてゾーン固有のセキュリティクレデンシャル情報の使用により、ファイルストレージリンクへのアクセスなしでは実現できないハイパーセキュアな保存ファイルへのアクセスとその再構築が可能になる。これらのＦＳリンクは、その数が制限され、ＳＤＮＰ通信システムのみを介して配信されるため、身元検証によってその安全性がさらに強化される。

【０６９７】

ハイパーセキュアファイルストレージの前記機能の実行の概略は、既出の図９Ａに示した機能シンボルを用いたハイパーセキュア通信と同様の方法で表すことができる。説明を簡素化するため、図９２の上のイラストに示されるように、ステートまたは時間９２６Ｃを使用するスクランブル化９２６、ジャンクデータ挿入１０５３、パース１０５２及び分割１０５７、及び暗号化１０２６の任意の組み合わせを、ＳＤＮＰエンコード機能１７５０で表すことができる。同様に、デコード機能１７５１は、ステートまたは時間９２６Ｂを使用した暗号化１０３２、ミキシング１０６１、ジャンクデータ除去１０５３Ｂ、及びアンスクランブル化９２８をまとめたものである。

【０６９８】

前述のセキュリティ機能を用いて、図９３Ａの上部のイラストに、クライアント側のエンコーディングによる分散ファイルストレージのプロセスを示す。図に示されるように、ファイル１７０５は、ＳＤＮＰクライアント$C_{1,1}$を実現するために使用されるクライアントデバイス１７００Ａ内でパースされたファイル１７０６を作成するためのパースされた１０５２と分割された１０５７である。結果として得られた断片化ファイルは次に、本明細書で開示される方法に従って実行されるラストマイル通信のＳＤＮＰエンコード操作１７５０ＢによってゾーンＵ１のセキュリティクレデンシャル情報を使用してエンコードされる。順次またはマルチルートのラストマイル通信で送信される断片化ファイルはこの後、ＳＤＮＰゲートウェイ$M_{0,0}$に届き、ゾーンＵ１のセキュリティクレデンシャル情報に従ってＳＤＮＰデコード操作１７５１Ｃを使用してデコードされ、パースされたファイル１７０６を回復する。パースされたファイル１７０６は、ＳＤＮＰクラウドのゾーンＺ１セキュリティ認証情報に従い、ＳＤＮＰエンコード操作１７５０Ｃによって再エンコードされる。メッシュトランスポート中、ＳＤＮＰクラウドで一連のゾーンＺ１でのデコード及びエンコード操作（図示せず）の実行後、最終データパケットは、例えばゲートウェイ$M_{0,8}$などそれぞれのＳＤＮＰゲートウェイに到着し、そこでＳＤＮＰデコード操作１７５１Ｄによりパースされたファイル１７０６が回復され、続いてゾーンＵ９セキュリティクレデンシャル情報に従ってＳＤＮＰエンコード操作１７５０Ｄにより再エンコードされる。この例では、次にパースされたファイル１７０６が２つのファイルに断片化（分割）され、これらのファイル２と３はＳＤＮＰデコード機能１７５１Ｅにより回復され、ファイルストレージサーバ１７４０Ｂと１７４０Ｃにそれぞれ保存される。この方法では、ファイルストレージサーバに保存されているデータファイルは断片化されるが、そうでなければ（ローカルドライブの暗号化を除く）、これらのドライブデータのサイバー攻撃によってアクセス可能になってしまう。そのため、ファイルの断片化と分散ストレージによってセキュリティを実現している。

【０６９９】
図９３Ａの下部のイラストに示されているプロセスを使用することで、より高いレベルのファイルセキュリティが達成される。ここには、完全なクライアント側エンコーディングによる分散ファイルストレージのプロセスが示されている。図に示されるように、ファイル１７０５は、ＳＤＮＰエンコード操作１７５０Ａによって処理され、ＳＤＮＰクライアント$C_{1,1}$を実現するために使用されるクライアントデバイス１７００Ａ内のスクランブル化され、暗号化され、パースされたファイル１７０６を作成する。操作１７５０Ａには、ファイル１７０６を３つの断片化ファイル１、２、及び３に分割する操作も含まれる。断片化されたファイル１、２、及び３は次に、本出願で開示される方法に従って実行されるラストマイル通信のためのＳＤＮＰエンコード操作１７５０Ｂにより、ゾーンＵ１セキュリティクレデンシャル情報を使用してエンコードされる。順次またはマルチルートのラストマイル通信で送信されたこれらの断片化ファイルはこの後、ＳＤＮＰゲートウェイ$M_{0,0}$に届き、スクランブル化され、暗号化され、パースされたファイル１７０６を回復するゾーンＵ１のセキュリティクレデンシャル情報に従ってＳＤＮＰデコード操作１７５１Ｃを使用してデコードされる。パースされたファイル１７０６は次に、ＳＤＮＰクラウドのゾーンＺ１セキュリティクレデンシャル情報に従い、ＳＤＮＰエンコード操作１７５０Ｃによって再エンコードされる。

【０７００】
メッシュ伝送中、ＳＤＮＰクラウドで一連のゾーンＺ１でのデコード及びエンコード操作（図示せず）の実行後、最終データパケットが、例えばゲートウェイ$M_{0,8}$などそれぞれのＳＤＮＰゲートウェイに到着し、そこでＳＤＮＰデコード操作１７５１Ｄによりパースされたファイル１７０６を回復し、続いてゾーンＵ９セキュリティクレデンシャル情報に従ってＳＤＮＰエンコード操作１７５０Ｄを使用してこのファイルを再エンコードする。スクランブル化、暗号化、パースされたファイル１７０６の断片化ファイル２及び３は、この後、ＳＤＮＰデコード機能１７５１Ｅを使用して回復され、ファイルストレージサーバ１７４０Ｂ及び１７４０Ｃにそれぞれ保存される。したがって、このファイルは断片化された分散ストレージだけでなく、スクランブル化、ジャンクデータ、及びクライアントのセキュリティゾーンのみが知っている暗号化の組み合わせによっても保護される。同様に、ファイル１はＳＤＮＰクラウドを介してゲートウェイ$M_{0,4}$に転送され、図８８のパケット１７１２Ａに示す通りに、ゾーンＵ７のファイルストレージ１７００Ｈに格納される。

【０７０１】
説明したこれら２つの例において、図９３Ｂのイラストに示されているように、最後のＳＤＮＰデコード操作１７５１Ｅを除去することにより、より高度なセキュリティを実現できる。このようにして、ファイルストレージサーバに保存されるファイルは、ゾーンＵ９セキュリティクレデンシャル情報を使用してＳＤＮＰエンコード操作１７５０Ｄによりエンコードされた状態を維持する。図の上側のイラストでは、ファイルはクライアントによって断片化されているが、エンコードはゾーンＵ９のストレージ側のセキュリティクレデンシャル情報に従って行われる。図の下側のイラストでは、ファイルはクライアント側のセキュリティクレデンシャル情報Ｕ１に従ってエンコードされ、ゾーンＵ９のストレージ側のセキュリティクレデンシャル情報に従って２回目のエンコードが行われる。断片化された分散ファイルストレージによって保護に加えて、このような二重にエンコードされたファイルは、ゾーンＵ９セキュリティクレデンシャル情報によってエンコードされたファイルの中にＵ１セキュリティクレデンシャル情報によってエンコードされたファイルが含まれるため、ネストされたハイパーセキュリティストレージと表現される。本明細書で開示しているネストされたセキュリティの利点は、保存されたファイルを開くために必要な情報がクライアントにもストレージサーバにも存在しないことである。

【０７０２】
ハイパーセキュリティ非集約型ファイルストレージを実装する例示的な方法の概要を図９４に示す。この図に示す例では、ハイパーセキュア通信とＳＤＮＰクラウドルーティン

グ用に使用されているエンコードとデコードを除去し、ファイルエンコードの正味の効果のみを示している。左上隅は、クライアントゾーンの断片化のケースを示している。ここで、ドキュメントはゾーンＵ１のセキュリティクレデンシャル情報に従って断片化されているが、ネットワークのストレージ側によって課される追加のセキュリティ対策は存在しない。左下隅は、クライアントゾーンでのエンコーディングのケースを示している。ここで、ドキュメントは操作１７５０Ｂによってエンコードされる。すなわち、ネットワークＵ１のセキュリティクレデンシャル情報に従ってスクランブル化、ジャンク化、フラグメント化、及び暗号化される。ただし、ネットワークのストレージ側ではセキュリティ対策は行われていない。

【０７０３】

右上隅は、クライアントゾーンＵ１でのフラグメント化のケースを示しているが、ＳＤＮＰエンコードの追加のステップ、つまりスクランブル化、ジャンク挿入、フラグメント化、及び暗号化が、ゾーンＵ９に従ってストレージ側に導入されている。右下隅は、完全にネストされたハイパーセキュアファイルストレージの例である。ファイルは、ゾーンＵ１のクライアント側セキュリティクレデンシャル情報を使用したＳＤＮＰエンコード操作１７５０Ｂに従ってエンコード及びフラグメント化され、その後、ストレージ側のラストマイルのゾーン９のセキュリティクレデンシャル情報に従ってファイルが２回エンコードされる。

【０７０４】

ファイルを呼び出して読み取るには、データの再呼び出しに、図９５に示されるように、正確に逆順にエンコードを実行する逆機能を含むセキュリティ操作を使用する必要がある。左上のケースでは、クライアントゾーンの断片化されたデータを呼び出すために、異なるファイルストレージサーバから呼び出されたパースされたファイル１７０６が、マージ操作１０６１を使用して再結合され、元のファイル１７０５を回復する。左下はクライアントゾーンのエンコードされたデータを再呼び出しするケースで、ここでは異なるファイルストレージサーバから再呼び出しされたパースされたファイル１７０６が、ミキシング、復号化、アンスクランブル化を含む分割操作１７５０Ｂの完全な逆機能であるＳＤＮＰデコード操作１７５１Ｈを使用して回復され、元のファイル１７０５にアクセスする。ストレージゾーンでエンコードされ、クライアントゾーンで断片化されたファイルの右上のケースでは、逆方向の操作が次のように実行される。まず最初に、ＳＤＮＰデコード操作１７５１Ｆを実行してゾーンＵ９セキュリティ操作の結果を取り消してパースされたファイル１７０６を回復し、続いてファイルマージ操作１０６１によりゾーンＺ１セキュリティクレデンシャル情報に従って行われたファイル分割操作１０５７の結果を取り消す。

【０７０５】

完全にネストされたハイパーセキュアファイルを読み取る右下の例では、異なるファイルストレージサーバに格納されているデータが、ゾーンＵ９のセキュリティクレデンシャル情報を使用してＳＤＮＰデコード操作１７５１Ｄによって、デコード、スクランブル化、ジャンク化、パース、及び暗号化された状態のマルチパートファイル１７０６を再構成する。次に、ゾーンＺ１固有のＳＤＮＰデコード操作１７５１Ｈは、エンコーダー１７５０Ｂの順次逆機能、すなわちミキシング（混合）、復号化、アンスクランブル化の操作を実行し、元のファイル１７０５を呼び出す。ファイルを回復するために順次逆機能を実行する操作は、当該ファイルの作成時に使用された一連の操作を逆の順序で実行する必要がある。例えば、エンコードが、分割、スクランブル化、及び暗号化の順に行われた場合、逆の機能であるデコードは、復号、アンスクランブル化、及びミキシング（混合）の順に操作を実行する必要がある。ただし、データパケットの順次エンコードが、スクランブル化、暗号化、そしてパケット分割の順に行われた場合、逆の機能であるデコードは、ミキシング、復号化、そして最後にアンスクランブル化の順に操作を行う必要がある。

【０７０６】

ファイルの呼び出し、すなわち「ファイル読み取り操作」を実行するには、クライアントが「ファイルストレージ読み取りリンク」をクリックして集約型ファイルリンクを呼び

出し、システムのハイパーセキュアファイルストレージシステムに格納されているファイルを呼び出して読み取るために必要な手順を開始する。読み取りプロセスでは、図９６Ａに示す以下の手順が実行される。
・ファイル所有者とクライアント１７００Ａまたは許可ユーザは、ＳＤＮＰ対応ハイパーセキュアメッセンジャ１１９６、ファイルマネージャ、またはその他のＳＤＮＰ対応インターフェイスなどのＳＤＮＰアプリケーションで「ファイルストレージ読み取りリンク」をクリックする。
・ダイアログインターフェイス１７６５、またはオプションでコマンドライン命令を使用して、クライアント１７００Ａはファイル要求１７６１を指定する。これには、ファイルの読み取り、ファイルの編集（書き込み権限でファイルのコピーを作成）、ファイルの消去（削除）、リンクの更新（セキュリティクレデンシャル情報の再発行）、またはファイルの再配布（ファイル断片を異なるファイルストレージサーバに移動し、ファイル所有者クライアントに新しいファイルストレージ読み取りリンクを発行）といった操作が含まれる。
・「クライアントの検証」操作１７６２では、ＳＤＮＰシグナリングサーバ１７１５が、ファイル（認証）を要求する１つまたは複数のクライアントの身元を確認する。ダイアログボックス１７６７を使用して、クライアントは、ＰＩＮ、及びオプションでデバイスまたはセキュリティトークンの検出などの２番目の要素を使用して身元を確認する必要がある。別の方法として、同じクライアントが所有する別のデバイスにＳＭＳテキストを送信することもできる。複数のクライアントによるアクセス承認を必要とするファイルの場合、すべてのユーザの身元を検証しなければならない（マルチ認証）。
・「特権の検証」操作１７６３では、シグナリングサーバ１７１５は、要求側クライアント１７００Ａが読み取りまたは読み取り／消去特権（許可）で要求ファイルへのアクセスを許可されていることを確認する。結果がダイアログボックス１７６８に表示されてから、ユーザがファイルのダウンロードまたは読み取りを希望しているかどうかを確認する。身元の確認がとれなかった場合、要求側は再試行するように指示される場合がある。指定した試行回数に達すると、ファイル管理者１７００Ｚ（存在する場合）に失敗した試行が通知され、アカウントがロックされる。ダイアログボックスは、この問題をファイル管理者に伝えるよう当該ユーザに通知することがある。または、ハッキングの疑いがある場合は、ダイアログボックスが空白になったり、ＳＤＮＰアプリケーションからユーザが完全に追い出されたりすることさえある。
・文書要求管理操作１７６４では、ＳＤＮＰシグナリングサーバ１７１５は、ファイルアクセス管理者にファイルアクセス要求とその要求（管理）の性質についてファイルストレージ管理者１７００Ｚに通知する。この管理手順は次のいずれかとなる。（ｉ）完全にスキップされる、（ｉｉ）ファイルアクセス管理者のアカウントにファイルアクセス要求を記録する、（ｉｉｉ）ファイルストレージ管理者にメッセージを送り、試行されたファイルアクセスについて直ちに通知する、または（ｉｖ）ファイルを要求しているクライアントにアクセス許可を与える前に、ダイアログボックス１７６９を介してファイルストレージ管理者の承認を求める。

【０７０７】

これらの認証、承認、及び管理（ＡＡＡ）ステップの後、承認が得られると、クライアントは図９６Ｂのフローチャートに示すステップを使用してファイルへのアクセス要求を行う（この図では説明用に読み取り要求として使用）。これらの手順には以下が含まれる。
・読み取り要求操作１７７０では、要求側クライアント１７００Ａはファイル読み取り要求をＳＤＮＰシグナリングサーバ１７１５に送信する。
・ストレージサーバ名要求操作１７７１において、ＳＤＮＰシグナリングサーバ１７１５は、ファイルストレージサーバ名要求をＳＤＮＰネームサーバ１７１４に送り、関連するファイルストレージサーバ（例えば、ファイルストレージサーバ１７００Ｍ）の現在のＳＤＮＰアドレスを要求する。ＳＤＮＰのメソッドに従って、ＳＤＮＰクライアント（ファイルサーバを含む）のＳＤＮＰアドレスは、少なくとも１日に１回は変更され、長期的な

クライアントの長期的なトレーサビリティから保護される。
・ストレージ名配信操作１７７２において、ＳＤＮＰネームサーバ１７１４は、要求されたファイル名「ＦＳアドレス」をＳＤＮＰシグナリングサーバ１７１５に配信し、それに従ってＳＤＮＰシグナリングサーバはファイル呼び出しルーティングを設定する。
・ルーティング指示操作１７７３で、ＳＤＮＰシグナリングサーバは、ファイルルーティング指示をクライアント１７００Ａ、サーバ１７００ＵなどのＳＤＮＰクラウド内のノード、及びファイルストレージサーバに対して送信する。このとき、ステートまたは時間９２０、数値シード９２３、復号鍵１０３０、及びオプションの暗号鍵１０２２（対称鍵暗号化通信で使用）を含むゾーンＵ９セキュリティクレデンシャル情報を用いる。
・ローカルファイルリカバリ操作１７７４では、ファイルの作成に固有の状態ないし時間情報を含む適用可能なセキュリティ認証情報を利用して、すべてのストレージ側ラストマイルのＤＭＺサーバが、パースされたファイルをデコードし、回復し、伝送するための準備としてこのデータを１つ以上のデータパケットにまとめる。
・ファイル配信操作１７７５では、パースされた各ファイルが、ＳＤＮＰシグナリングサーバのルーティング指示に従い、ＳＤＮＰネットワークを介した独立した配信を使用して、要求元クライアントに配信される。例えば、ファイルストレージサーバ１７００Ｍがそのファイルをクライアント１７００Ａに送信する。
・受信したパースされたデータファイルは、クライアントゾーンのセキュリティ認証情報に従ってさらにデコードされ、このパースされたファイルはマージされ、表示または転送が可能な元のパースされたファイルが再作成される。

【０７０８】

これらの手順は、以下の一連の図に示されている。図９７Ａにおいて、アドレス「ＩＰ Ｃ$_{1,1}$」のクライアントデバイスは、データパケット１８１０Ａを使用してアドレス「ＩＰ Ｓ」のシグナリングサーバ１７１５に対してファイル読み取り要求を出す。この要求には、ＴＣＰ伝送、ファイルに関連するヘッダ情報、及び２つ以上のＦＳリンクを指定するＣ＆Ｃペイロード１８１１Ａが含まれる。ＦＳリンクには、ルーティングのためにＳＤＮＰアドレスまたはＩＰアドレスに変換する必要があるタグないし疑似アドレスを用いて、保存されたファイル断片の場所が匿名で記述されている。ただし、シグナリングサーバ１７１５は、これらの名前付きユーザＩＤの現在のＳＤＮＰアドレスを知らないため、ＳＤＮＰネームサーバ１７１４に現在の情報を要求する必要がある。図９７Ｂで、シグナリングサーバ１７１５は、データパケット１８１０Ｂをネームサーバ１７１４に送信して、ファイルストレージサーバノードＦ$_{7,1}$、Ｆ$_{9,4}$、及びＦ$_{9,1}$のＩＰアドレスまたはＳＤＮＰアドレスを要求する。図９７Ｃでは、シグナリングサーバ１７１４は、データパケット１８１０Ｃをネームサーバ１７１４に送信して、ファイルストレージサーバノードＦ$_{7,1}$、Ｆ$_{9,4}$、及びＦ$_{9,1}$のＩＰアドレスまたはＳＤＮＰアドレスを要求する。シグナリングサーバ１７１５は次に、ファイルストレージサーバへのパースされたファイルのラストマイル及びメッシュクラウドによる配信を計算する。

【０７０９】

図９７Ｄのシグナリングサーバ１７１５は、ストレージ側にあるラストマイルノード、すなわちゾーンＵ７及びＵ９にＣ＆Ｃデータパケットを送信する。図に示されるように、データパケット１８１０Ｇは、アドレスＳのシグナリングサーバ１７１５から、アドレス「ＩＰ Ｆ$_{7,1}$」のファイルストレージサーバ１７００Ｈに転送され、「ファイル１読み取り命令」１８１１Ｇを含むＣ＆Ｃペイロードを運ぶ。このパケットは、Ｕ７セキュリティクレデンシャル情報を使用して、アドレス「ＩＰ Ｆ$_{7,1}$」からアドレス「ＩＰ Ｍ$_{0,4}$」のＳＤＮＰゲートウェイにＩＤタグ１のファイルを送信するようファイルストレージサーバに指示する。同時に、データパケット１８１０Ｆは、ＳＤＮＰゲートウェイＭ$_{0,4}$に送信される。このパケットはアドレス「ＩＰ Ｓ」から「ＩＰ Ｍ$_{0,4}$」にルーティングされ、Ｃ＆Ｃペイロード１８１１Ｆを含んでおり、タグ１を含むデータパケットがゲートウェイノードＭ$_{0,4}$によって期待されていること、データパケットの受信後にＺ１セキュリティクレデンシャル情報を用いてＳＤＮＰクラウドで、例えばアドレスＳＤＮＰ

Ｍ０，３１に転送されることが伝達される。
【０７１０】
２番目のデータパケット１８１０Ｉは、「ファイル３読み取り命令」を含むＣ＆Ｃペイロード１８１１Ｉを含んでおり、アドレス「ＩＰ　Ｓ」のＳＤＮＰシグナリングサーバ１７１５からアドレス「ＩＰ　Ｆ９，１」のファイルストレージサーバ１７００Ｍに送信される。この命令は、ファイルストレージサーバ１７００Ｍに、ＩＤタグ３を持つファイルを、ゾーンＵ９セキュリティクレデンシャル情報を使用してアドレスＩＰ　Ｍ０，８のＳＤＮＰゲートウェイに送信するように指示している。他のＣ＆Ｃパケット（図示せず）は、他のファイルストレージサーバ及びゲートウェイ（ノードＦ９、４、Ｍ０、８など）、及びＳＤＮＰクラウド内のノードに同様に送信される。
【０７１１】
図９７Ｅでは、シグナリングサーバ１７１５は、データパケット１８１０Ｄをクライアントデバイス１７００Ａに送信する。このパケットはアドレス「ＩＰ　Ｓ」からルータ１７０２Ｇを介して「ＩＰ　Ｃ１，１」にルーティングされる。データパケット１８１０Ｄは、ゾーンＵ１セキュリティクレデンシャル情報を使用して、アドレス「ＩＰ　Ｍ０，０」のＳＤＮＰゲートウェイ１７０１Ｕからタグ１、タグ２などのＩＤを持つ複数の着信データパケットが予期されることをクライアントに通知するＣ＆Ｃペイロード１８１１Ｄを含む。同時に、シグナリングサーバ１７１５は、データパケット１８１０ＥをＳＤＮＰゲートウェイ１７０１Ｕに送信する。このパケットはアドレス「ＩＰ　Ｓ」から「ＩＰ　Ｍ０，０」にルーティングされる。このパケットには、ＳＤＮＰクラウド内から転送されるタグ１、タグ２、及びタグ３パケットとして識別される着信データパケットに適用可能なゾーンＵ１のラストマイルルーティング用のＣ＆Ｃペイロード１８１１Ｅが含まれる。
【０７１２】
コマンド及び制御データパケットがネットワークに配信されると、ファイル転送が実行される。この転送の最初のステップを図９８に示す。ここで、ＦＳリンク３を含むデータパケット１７４１Ｒは、例示されている状態９２０、数値シード９２９、復号鍵１０３０、及び暗号鍵１０２２などの情報をＳＤＮＰデコード動作１７５１Ｒに提供する。ＳＤＮＰデコード操作１７５１Ｒのため、この情報はＤＭＺサーバ１７５２によって処理され、パケット復号化１０３２Ｒ、ミキシング１０６１Ｒ、ジャンク除去１０５３Ｒ、及びアンスクランブル化９２８Ｒなどの共有秘密を含む機能を実行する。これらの実行はすべて状態９２０、すなわちパースされたファイルが最後にエンコードされたときの状態で行われる。暗号鍵１０２２は、ファイルをデコードするために特に必要ではないが、パースされたファイルをクライアント及びファイル所有者に返送するための対称鍵暗号化に使用することができる。
【０７１３】
図９９に、ファイルのルーティング及びデータ伝送について示す。ここでは、ＴＣＰデータパケット１７２０ＡでＵ７セキュリティクレデンシャル情報を用いてアドレス「ＩＰ　Ｆ７，１」から「ＩＰ　Ｍ０，４」にファイル１が送信され、ＴＣＰデータパケット１７２０ＢでＵ９セキュリティクレデンシャル情報を使用してアドレス「ＩＰ　Ｆ９，４」から「ＩＰ　Ｍ０，８」にファイル２が送信され、ＴＣＰデータパケット１７２０ＣでＵ９セキュリティクレデンシャル情報を使用してアドレス「ＩＰ　Ｆ９，１」から「ＩＰ　Ｍ０，８」にファイル３が送信される。ＳＤＮＰクラウドを介した伝送の後（図示せず）、一連のデータパケット１７２０Ｘが、アドレス「ＩＰ　Ｍ０，０」のＳＤＮＰゲートウェイからクライアントアドレス「ＩＰ　Ｃ１，１」に配信される。
【０７１４】
読み取り操作では、データは「読み取り専用」形式でＳＤＮＰアプリにロードされる。ファイルがＳＤＮＰアプリケーション内でサンドボックス化されている限り、ファイルはＳＤＮＰアプリケーションとネットワークの機能によって保護され、デバイスのオペレーティングシステムのログイン手順や脆弱なセキュリティ対策には依存しない。私的文書への読み取り専用アクセスの必要性が企業の間で広まっている。企業の財務、法務、製造、

エンジニアリング、品質管理などの部門によって作成されるファイルの多くが、読み取り専用の内容であることを表す資料の例となっている。多くの場合、これらの企業の社内ファイルは、公開前に審査のために企業の幹部に転送、つまり電子的に配布する必要がある。

【０７１５】

配布された情報の偶発的または時期尚早の公開は計り知れない影響があり、企業にとって深刻な経済的または法的な影響、さらには役員に対する個人的責任を伴う。例えば、上場企業の未公表の財務報告は、公開されるまでは厳密に機密が維持されている。米国では、規制ＦＤ、すなわち「公正な開示」とは、優先権なしに万人に対して同時に情報が公開されなければならないことを意味している。外部の当事者が公開前にこのような情報にアクセスした場合、それは規制ＦＤへの違反となる。会社が文書の機密性を維持及び保証する義務を怠ったために規制ＦＤ違反が発生したと裁判所が判断した場合、会社はその違反により罰せられる可能性があり、役員は、選択的開示に起因するインサイダー取引でない場合であっても、個人的に責任を問われる可能性がある。

【０７１６】

ＳＤＮＰアプリ内では、取得したファイルは区分化（サンドボックス化）されて、あるアカウントＩＤから別のアカウントＩＤへのデータの転送ができないように保護される。例えば、ファイルは、ビジネスアカウントと個人アカウントとの間で交換できない。読み取り者の承認特権に応じて、ユーザは取得したファイルをＳＤＮＰアプリケーションからダウンロードして、デバイスメモリのエンコードされていないストレージにダウンロードすることが許可される場合とされない場合がある。ＳＤＮＰ対応アプリケーションの外部でファイルをダウンロードすると、ファイルとそれに含まれるデータのセキュリティが侵害される。ＳＤＮＰアプリケーション内にあるデータの場合、アクセスが制御され、ユーザのアクションが制限され、デバイスとＳＤＮＰネットワークがいずれもユーザの身元を確認しなければならない。このような多層型の多要素認証を打ち破るのは、携帯電話を開くために必要な単純な４桁のピンを無効化するのに比べ、はるかに困難である。それとは対照的に、ファイルがコンピュータ、タブレット、または携帯電話にダウンロードされてしまうと、不正アクセスを防止したり、アクセスした人物を特定したり、ファイルのコピーを作成した人物を特定することはほぼ不可能となってしまう。

【０７１７】

そのため、ＳＤＮＰ通信を使用して、ファイル所有者は機密の文書やファイルをロック、つまりコンパートメント化することができる。これで、文書やファイルを他人が読むことはできるが、携帯電話にはダウンロードできないようになる。追加の手順を使用して、ＬＣＤディスプレイのスクリーンショットまたは写真撮影を防止することも可能である。セキュリティやプライバシーが求められないその他のケースでは、取得したファイルをＳＤＮＰアプリから携帯電話のメモリへ転送することが可能になり、制限なく使用できる。

【０７１８】

編集操作では、編集可能な形式のファイルがデバイスにダウンロードされ、ファイルの編集に必要なアプリケーションプログラムに渡される。ファイル要求とデータ交換の実行に関しては、ＳＤＮＰネットワーク操作でのファイル読み取り要求とファイル編集要求との基本的な相違は、クライアントのＳＤＮＰアプリケーションの操作である点を除けば、存在しない。つまり、ＳＤＮＰネットワークでのデータ転送という観点からは、これらの操作は機能的に同じである。したがって、読み取り操作と編集操作の違いは、主にアプリケーション固有のファイルで構成されるレイヤ５からレイヤ７の実行にあると考えることができる。

【０７１９】

取得したファイルを編集するアプリケーションには、（ｉ）デバイスのオペレーティングシステムにネイティブであるが、ＳＤＮＰアプリケーションの外部で動作するデバイス埋め込みアプリケーション（Ｓｉｍｐｌｅｔｅｘｔなど）、（ｉｉ）デバイスのオペレーティングシステム上にあるが、ＳＤＮＰアプリケーションの外部で実行されるサードパーティアプリケーション（例えば、Ｍｉｃｒｏｓｏｆｔ　Ｗｏｒｄ、Ａｄｏｂｅ　Ａｃｒｏｂ

ａｔなど）、または（ｉｉｉ）ＳＤＮＰアプリケーション内で実行され、デバイスまたはそのオペレーティングシステムから直接にはアクセスできない安全なアプリケーションが挙げられる。例えば、企業のプレスリリースはＳＤＮＰアプリケーションサンドボックス内で編集できるが、携帯電話のメモリにはダウンロードできない。ビジネスのセキュリティを維持するための追加の対策として、会社が所有するすべてのファイル、すなわちＳＤＮＰビジネスアカウントコンパートメントにサンドボックス化されているファイルは、同じＳＤＮＰアプリケーション内で実行されている場合であっても、ユーザの個人ＳＤＮＰアカウントには転送できない。

【０７２０】

編集後、編集されたファイルをＳＤＮＰのファイルストレージサーバに保存しても、当該ファイルの所有者が具体的にそうするように要求しない限り、既存のファイルは上書きされない。代わりに、当該ファイルの最初のバージョンに加えて２番目のバージョンが保存され、以前のバージョンを削除するには、当該ユーザがそのファイルに対して消去操作を実行する必要がある。ハイパーセキュアファイルストレージはＩＤ検証を必須としているため、編集されたファイルを保存するプロセスには、専用のハイパーセキュアネットワーク通信機能を備えていないファイルストレージでは利用できない独自のシステム機能が含まれる場合がある。このようなユニークな機能のひとつに、ファイルに署名して日付を入れる（またはアジアなら印鑑を押す）ために使用される署名検証機能がある。署名機能には、文書所有者及び元の文書作成者に送信される登録済み受領書が含まれる場合がある。

【０７２１】

本明細書に従って作成されたハイパーセキュアデータストレージの場合、消去操作は、既存のパースされたファイルをすべて乱数で上書きし、さらにオプションで１時間後にもう一度乱数の上書きを実行して、保存されているビットの電荷または磁場の小さいが潜在的に検出可能なアナログ変動をさらに念を入れて曖昧化する。ファイルレコードも上書きされて、データドライブのファイルレコードが複雑に乱される。データとファイルレコードを消去した後、クライアントのデータリンクは、ＳＤＮＰシステムの自己破壊メッセージ機能を使用してクライアントデバイス内で破壊され、ＦＳリンクのすべての残余データはＳＤＮＰシステムから破棄される。ただし、ファイルシステム管理者がサードパーティのソフトウェアを使用してユーザ単位の活動を追跡していた場合、管理者は、削除されたファイル自体にはアクセスできなくても、ファイルの所有者及び作成日、ファイルを誰がいつアクセスしたか、いつ消去されたかなど、ファイルの履歴に関するメタデータを保持することができる。

【０７２２】

ＳＤＮＰネットワークとハイパーセキュアラストマイル機能は、個人アカウントのプロファイルとは異なる企業アカウントの機能や操作手順をサポートすることもできる。前述のように、個人アカウントの消去操作では、ジャンクデータのファイルへの書き換え、ファイルの存在を表すドライブ上のインデックスレコードの消去、自己破壊メッセージを使用したファイルの以前の断片化された格納場所を指し示すすべてのＦＳリンクの破壊などが行われる。ただし、企業アカウントの場合、ファイルストレージ管理者は、ファイルを完全に破棄するために事前の承認が必要とされる場合がある。例えば、図９６Ａのダイアログボックス１７６９と同様の承認プロセスを使用する（ただし、ファイルの所有者ではなく管理者に送られる）。

【０７２３】

会社のファイル管理者がファイルの削除を許可しないことを選択した場合、次のようなシナリオが発生することが考えられる。（ｉ）ファイル所有者にファイルが削除されないことが通知され、ファイル読み取りリンクがＳＤＮＰアプリケーションまたはＳＤＮＰコミュニケータのメッセージ履歴に保持される、（ｉｉ）ファイルが削除されないことがファイル所有者に通知され、例えば「アーカイブ目的」のために保存されるが、ＳＤＮＰシステムの自己メッセージ破壊プロビジョン機能を使用して、ＳＤＮＰアプリケーションから個人のファイル読み取りリンクが削除される、つまり、ファイル所有者がファイルを削

除しようとすると、ファイルストレージ管理者しかこのファイルを呼び出せなくなる、または（ｉｉｉ）ファイル所有者の個人ファイル読み取りリンクは、ＳＤＮＰシステムの自己メッセージ破壊プロビジョン機能を使用してＳＤＮＰアプリケーションから削除されるが、ファイル所有者には当該ファイルが会社によって保持されていることは通知されない。

【０７２４】

本明細書で開示された匿名の断片化分散ファイルストレージシステムの動作に固有のラストマイルハイパーセキュリティにより、「ファイルストレージ読み取りリンク」がなければ、ファイルストレージ管理者であっても格納されたファイルを取り出すことはできない。管理者がファイルにアクセスするためには、そのファイルが保存または編集されるたびに、対応するファイルストレージ読み取りリンクが必ず必要なのである。企業アカウントではこのレベルの監視が可能だが、すべてのファイルに対するすべての変更を追跡することで生じる膨大な量のデータに対処するのは、どのようなファイル管理システムでも容易なことではない。本明細書で開示されているように、本ＳＤＮＰシステムで可能なインテリジェントフィルタリングは、試行されたファイル消去のみを追跡する。このアプローチでは、管理者はファイルの作成を監視せず、ファイルの削除の試行のみを追跡する。ファイル所有者がファイルを削除しようとすると、そのときのみ、対応するファイルストレージの読み取りリンクが、承認またはアーカイブ目的で管理者のデータベースまたはコンソールに転送される。

【０７２５】

データベースのサイズは、監視が必要とされる特定の従業員及び請負業者を指定することでさらに最小化できる。例えば、企業が財務監査または特許訴訟に関与することになった場合、通常はすべての関係当事者は関連するデータやファイルを消去しないよう通告される。本明細書で開示しているＳＤＮＰファイルストレージシステムによって有効化されたファイル管理機能を使用して、調査に関連するスタッフによるファイル消去の試行はすべて、そのログを取り、「その時点で」ファイルストレージリンクのコピーをファイルストレージ管理者に、または場合によっては独立した調査者に送信することにより追跡できる。このような方法は、監視対象のデータの量を制限するとともに、不正行為の隠蔽の試みを示唆する疑わしい活動を自然な形で管理者に警告するため、有益である。クライアントとファイル所有者のデバイス自体の破壊によるファイルストレージ名リンクの偶発的または悪意のある消失を防止するため、前述の冗長ファイルストレージリンクの使用は欠かせない。企業の場合、バックアップコピーは、セキュリティで保護されたオフィス内のコンピュータ、または会社の中央サーバに保持されているかもしれない。

【０７２６】

例えば国家安全保障に関わるなど、極めて強固なセキュリティが求められる場合、ファイルの消去には次のような複数の手順を用いる方法が使用されるであろう。（ｉ）ファイルをランダムデータで上書きする、（ｉｉ）ストレージドライブから他のすべてのファイルを他のストレージデバイスにコピーする、（ｉｉｉ）ドライブを一括消去する、（ｉｖ）ドライブを再フォーマットする、（ｖ）ドライブのストレージフィールドを乱数で上書きする、及びオプションとして（ｖｉ）必要に応じて保存されているファイルをコピーする。従来のようなファイルデータの上書きと異なり、一括消去プロセスでは、読み書き記憶媒体自体に影響を与え、その電気的、磁気的、または光学的特性を分子レベルで自然にランダム化する。磁気ドライブの一括消去には大きな電磁石を使用できるが、フラッシュの一括消去にはＩＣを高温にしたり、場合によっては高い動作電圧で電離放射線を照射したりする必要がある。磁気光学ドライブは、高磁場を使用して一括消去することができる。再書き込み可能型光学ドライブは、ディスクフォーマットトラックに対して横方向にスキャンされる明るいスキャンレーザーを使用することで一括消去できる。いずれにしても、一括消去は、消去後のストレージメディアにデータがまったく存在しなくなり、ストレージメディアが破損して二度と使用できなくなるリスクがある極端な例である。

【０７２７】

ハイパーセキュア分散ファイルストレージシステムのもう１つの重要な要素は、ファイ

ルデータとリンクアクセスの整合性の維持である。リンクが偶発的に失われないようにするには、その時々にファイルストレージの読み取りリンクを再確立、すなわち再確認し、セキュリティ認証情報を再発行することが有益となる。本明細書で「リンク更新」コマンドと呼んでいるこのプロセスは、クライアントから手動または自動で開始することができ、また事前定義された時間間隔でファイルストレージサーバから開始することもできる。クライアントから開始された要求の場合、ＳＤＮＰシグナルサーバはコマンド及び制御パケットを対応するサーバに送信する。図１００に示されるようにリンクの更新が開始されると、ファイルは、それらが以前にゾーンＵ９セキュリティクレデンシャル情報を用いて作成された時間t_1の「古い」ステートであるステート３２０ＸでＳＤＮＰデコード操作１７５１Ｆにより読み取られデコードされる。ファイルは次に、時間t_2で新しいステート９２０Ｙを使用してＳＤＮＰエンコード操作１７５０Ｄにより再エンコードされ、ストレージドライブに保存される。更新されたストレージリンク（例：ＦＳリンク３）はこの後、ＳＤＮＰネットワークを介してファイル所有者であるクライアントデバイス１７００Ａに返送される。結果として得られたファイルには、時間t_2でゾーンＵ９のセキュリティクレデンシャル情報を用いて更新されたエンコードデータが格納される。ただし、元のファイルの作成とパースに使用されたゾーンＵ１のクライアントのセキュリティクレデンシャル情報は更新されない。このファイルを読み取るには、読み取り操作で最初に時間t_2に対応する状態でゾーンＵ９セキュリティクレデンシャル情報を使用してファイルをデコードしてから、クライアントノード$C_{1,1}$に転送した後、ファイルが最初に作成された時間に関連付けられたゾーンＺ１のセキュリティクレデンシャル情報を使用してファイルをデコードする必要がある。

【０７２８】

セキュリティを強化するためのもうひとつの対策として、ファイルの再配布操作により、選択したファイルストレージリンクのすべてのパースされたファイルを新しい、または異なるファイルストレージサーバに移動する方法がある。この操作では、パースされたファイルをまったく新しいサーバに送信するか、またはファイルを既存のストレージノード間で再配布することができる。いずれの場合も、セキュリティクレデンシャル情報が更新され、新しいファイルＦＳリンクが発行され、ファイルへのアクセス権のあるクライアントに送られる。この操作を図１０１に例を使って示す。ここで、ゾーンＵ７のファイルストレージＳＤＮＰノード$F_{7,1}$のコンテンツは、そのファイルが作成された時間t_1、ステート９２０Ｘを使用してＳＤＮＰデコード操作１７５１Ｈによりデコードされる。ファイルは次に、ＳＤＮＰネットワーク（図示せず）を介してファイルストレージＳＤＮＰノード$F_{9,4}$に転送され、そこで時刻ｔ２に対応するステート９２０ＹとしてゾーンＵ９セキュリティクレデンシャル情報を使用してＳＤＮＰエンコード操作１７５０Ｌによってエンコードされる。この後、ファイルは保存され、更新されたＦＳリンク２がファイル所有者とファイルアクセス権を持つ他のクライアントに送信される。

【０７２９】

上記のファイル転送と並行して、ゾーンＵ９のファイルストレージＳＤＮＰノード$F_{9,4}$の内容は、このファイルが作成されたときの時間t_1、ステート９２０Ｘを用いてＳＤＮＰデコード操作１７５１Ｌによってデコードされる。ファイルは次に、ＳＤＮＰネットワーク（図示せず）を介してファイルストレージＳＤＮＰノード$F_{9,1}$に転送され、そこで時刻t_2に対応するステート９２０ＹとしてゾーンＵ９セキュリティクレデンシャル情報を使用してＳＤＮＰエンコード操作１７５０Ｍによってエンコードされる。この後、ファイルは保存され、更新されたＦＳリンク３がファイル所有者とファイルアクセス権を持つ他のクライアントに送信される。同様にして、ゾーンＵ９のファイルストレージＳＤＮＰノード$F_{9,1}$の内容は、このファイルが作成されたときの時間t_1、ステート９２０Ｘを用いてＳＤＮＰデコード操作１７５１Ｍによってデコードされる。ファイルは次に、ＳＤＮＰネットワーク（図示せず）を介してファイルストレージＳＤＮＰノード$F_{7,1}$に転送され、そこで時刻t_2に対応するステート９２０ＹとしてゾーンＵ７のセキュリティクレデンシャル情報を使用してＳＤＮＰエンコード操作１７５０Ｈによってエンコードされ

る。この後、ファイルは保存され、更新されたＦＳリンク１がファイル所有者とファイルアクセス権を持つ他のクライアントに送信される。このようにして、３つのファイルすべてが再配置され、新しいセキュリティクレデンシャル情報が発行され、アクセスが承認されたクライアントに対して、更新されたＦＳリンク１、２、３に基づいて新しいファイルストレージ読み取りリンクが発行される。

【０７３０】

ハイパーセキュアファイルストレージシステムによって実行されるもうひとつの必要とされるメンテナンス機能は、ライブリンクのないファイル、つまり「ゾンビファイル」の有無を確認するために使用される操作である。この操作は、クライアントやファイル所有者ではなく、ファイルストレージサーバが開始することを除いて、リンクの更新操作と似ている。この操作中、各ファイルストレージサーバは、ファイルが最後にアクセスされてからの時間を追跡する。ファイルに対する最後の操作が、指定された時間間隔を超えた場合（例えば、１ヶ月間活動がない等）、ファイルストレージサーバはクライアントに接続して、リンクがまだアクティブかどうかを確認する。ファイルストレージサーバは、ＦＳリンクをクライアントに送信するために使用された方法と同じ方法で、クライアントに接続できる。ファイルが保存されるとき、ファイルストレージサーバはクライアントのＳＤＮＰ　ｚｉｐまたは擬似アドレスを保持する。

【０７３１】

指定された時間内にアクティビティが発生しなかった場合、ファイルストレージサーバはＳＤＮＰシグナリングサーバに接続して、リンクが依然としてアクティブであることを再確認する要求を送信する。次に、ＳＤＮＰシグナリングサーバは、参加している各ファイルストレージサーバに対するＦＳリンク検証要求の配信ルートを計画する。各ファイルストレージサーバは、ＳＤＮＰネットワーク経由でクライアントにこの要求を送信する。参加しているすべてのＳＤＮＰクライアントノードは、デバイスにファイルリンクがまだ存在することを確認して応答する。ファイルリンクが確認された場合、その時点でクライアントにはリンクの更新を実行するオプションがある。ただし、デバイスが応答しない場合、つまりアクティブなファイル読み取りリンクが存在していない場合には、ファイルストレージサーバは管理者にファイルリンクが古くなっているか失われていることを通知し、１～３ヶ月といった期間の経過後に所有者不明のゾンビファイルは永久かつ取消不能な方法で消去される。

【０７３２】

登録通信

【０７３３】

本明細書に従って行われるＳＤＮＰ通信のもうひとつの特徴に、「登録通信」を配信または保存するネットワーク機能がある。登録通信では、コミュニケのハイパーセキュア配信や、署名付きタイムスタンプ付きメッセージとしてのファイルのハイパーセキュア保存が行われ、法的有効性を確立する目的で通信に電子署名（ｅ－ｓｉｇｎ）及び電子スタンプ（ｅ－ｃｈｏｐ）を行う機能がある。登録通信には、「証明付きメッセージ」を送信する機能も含まれる。これはハンドシェイク方式で実行され、署名またはスタンプの捺されたタイムスタンプ付きの返信を使用して文書またはファイルの受領を確認する。すべての登録通信は、クライアントデバイスのＳＤＮＰアプリケーションによって開始されるが、ラストマイル通信、つまりＳＤＮＰネットワークのラストマイルを介して行われる通信を通じて認証される。クライアントがスタンプ確認を不正に変更しようとすると、スタンプ確認のメッセージとネットワーク記録との間に矛盾が生じる。

【０７３４】

ＳＤＮＰ通信では「ステート」が使用されているため、つまり、時間とその他のユニークな変数を使用してコミュニケとファイルストレージとでメッセージ固有のセキュリティ認証情報を確立しているので、タイムスタンプはＳＤＮＰ通信にとって本質的に備わる機能となっている。このことが図１０２のＳＤＮＰコミュニケータアプリケーションウィンドウ１８００で例示されている。ここでは、送受信される各テキストメッセージには、メ

ッセージが送信されるタイミング、受信されるタイミング、読み取られるタイミングを示す、それぞれに対応するタイムスタンプ１８０１Ａと１８０１Ｂがある。ＳＤＮＰシグナリングサーバによって確立されたグローバルな時間参照を含む時間情報は、ラストマイルネットワークを介してクライアントに配信される。次に、ＳＤＮＰクライアントアプリはこのタイムスタンプを情報表示に統合する。

【０７３５】

登録通信では、コミュニケはプロセスの一部として正式のタイムスタンプを生成する。登録通信プロセスの一例を図１０３に示す。この図では、ハイパーセキュアメッセージが実行され、オプションの添付ファイルステップ１８０２が開始される。この操作には、ダイアログボックス１８０３が使用され、メッセージまたはファイルを送信するクライアント、すなわち送信者が、メッセージにファイルを添付するかどうかを選択し、もし添付することにした場合は、ディレクトリブラウザを使用してファイルを見つける。次に、コマンドダイアログ１８０４を使用して登録メッセージを送信するが、このときダイアログボックス１８０５に従って通常の配信を使用するか登録配信を使用するかを選択する。次に、メッセージは本発明に従って実装されたハイパーセキュア通信を使用して送信される。

【０７３６】

「メッセージ受理」ステップ１８０６で、受信側は、メッセージにアクセスするために身元を確認し、受け取るメッセージとファイルの受理を確認する認証済み受領書を送信するために必要とされる一連の手順を実施する。このプロセスは、受信側クライアントに身元の確認を求める受領認証操作１８０７から始まる。受信側の身元が認証されなければ、受信側はメッセージにはアクセスできず、メッセージは破棄され、送信者に認証ステップの失敗が通知される。このようにして、送信側は、受信側のデバイスが盗難にあった可能性があることを示す警告を受けることができる。受信側の身元が確認されると、受信側は、受領承認操作１８０８により、受信するメッセージと添付ファイルを受け入れるか拒否するかの判断を求められる。メッセージの受信が拒否された場合、その旨が送信者に通知される。

【０７３７】

受信側が肯定応答を選択してメッセージを受け入れる場合、受領管理ステップ１８０９を実行し、電子署名（ｅ－ｓｉｇ）を選択するか、電子スタンプ／印（ｅ－ｃｈｏｐ）を選択することによって、メッセージ受領の署名を行わなければならない。送信側は必要なオプションを指定することができる。国によっては、電子スタンプと電子署名の両方がなければ法的拘束力が発生しない場合がある。続いて表示されるダイアログボックス（図示せず）で、ユーザはデバイスのファイルディレクトリで自分の電子署名または電子スタンプを指定するように指示される。また代替手段として、音声の録音ないしビデオの録画を確認用に使用することもできる。受信側は、録音ないし録画時に読み上げる内容を指示される。メッセージへの署名を終えると、そのメッセージを受信者は読むことができ、添付ファイルは送信者の要件に応じて、その場で表示したり、ダウンロードしたりすることができるようになる。

【０７３８】

文書の受領時には、メッセージ受信者を特定する署名＋タイムスタンプ入りメッセージ受領書１８１１、受信した埋め込みテキストと添付ファイル名、メッセージの受信日時、ｅ－ｓｉｇ、ｅ－ｃｈｏｐ、音声記録、音声＋ビデオ記録、またはそれらのいずれかの組み合わせが、確認応答送信操作１８１０で送信される。アーカイブ受領オプション１８１２で、送信者は署名付きタイムスタンプ付きのメッセージ受領書１８１１のコピーをシステムのハイパーセキュアファイルストレージシステムに保存することができる。これにより、送信者はメッセージの呼び出しに必要なファイル読み取りリンク１８１３を受け取ることができる。代替手段として、送信者のデバイスにメッセージ受領書１８１１をダウンロードできる場合もある。

【０７３９】

暗号化ベースのセキュリティの問題

【０７４０】
政府のセキュリティ機関は、今日の企業詐欺、ＩＰ窃盗、サイバー犯罪、ハッキング、犯罪組織、麻薬カルテル、マフィア、ヤクザ、ジハード主義者、及びテロリスト等が溢れるこの世界において、発信者に追跡不可能な匿名通信を提供する通信システム、すなわち、暗号化を使用してデータを保護し、発信者（比喩的には公衆電話）の身元を隠すあらゆる通信システムは、ネットワークオペレータ、アプリケーション開発者、及びデバイスメーカーにとって無謀で無責任な商慣行である、と主張している。
【０７４１】
残念なことに、セキュリティの実現を暗号化に依存している通信は、犯罪者と法を遵守する市民の双方を同様に保護するという事実が存在する。前述のように、このテーマは、ＩＳＩＳテロリストの犯罪活動、Ｔｅｌｅｇｒａｍと呼ばれる電話アプリケーションプログラムを使用した彼らによるパリやベルギーでのテロ行為に関する無数のニュース記事でも注目されるようになっている。本明細書では、エンドユーザベースの暗号化とも呼ばれるエンドツーエンドの暗号化を使用して安全な通信を促進している。復号鍵は通信を行う送受信者間でのみ保持され、介在するネットワークまたはそのオペレータはこれを保持しないため、エンドツーエンドの暗号化はセキュリティ機関にとって特に面倒な存在である。Ｔｅｌｅｇｒａｍに反発するセキュリティ機関は、大きな鍵によるエンドツーエンドの暗号化は、テロリストがオープン通信を使用して密かに活動することを可能にする国家的、さらには世界的なセキュリティリスクであると主張している。Ｔｅｌｅｇｒａｍを支持する議論は、何があっても個人のプライバシーを支持する。
【０７４２】
２０１５年１２月２日にカリフォルニア州サンバーナーディーノでの銃撃で１４人が死亡、２２人が負傷した事件に関して、連邦裁判事がＦＢＩに有利な判決を下し、犯人が所有していたと思われる携帯電話の「ロックを解除」するようＡｐｐｌｅ社に命じたことから、プライバシーに関する議論が再燃した。２０１６年2月１７日のワシントンポスト誌の「Ａｐｐｌｅ社は、サンバーナーディーノの襲撃に関連しているｉＰｈｏｎｅ（登録商標）の暗号解除に関するＦＢＩの要求に断固抵抗すると断言」と題する記事。Ａｐｐｌｅ社と同社ＣＥＯは、裁判所の命令に従うことを拒否するいくつかの理由を挙げた。この記事は（https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html）から入手できる。
【０７４３】
最も注目すべきは、警察が令状を取得したとしても、Ａｐｐｌｅ社自身が復号鍵を保持しないようにセキュリティが設計されているため（このことは本質的にエンドツーエンドの暗号化というもうひとつの悪夢を呼び起こす）、法執行機関のためにより新しいｉＰｈｏｎｅ（登録商標）のロック解除はできないのだと強く主張したことである。Ａｐｐｌｅ社は、当該携帯電話のユーザ、またはその携帯電話のパスワードを知っている者だけが携帯電話のロックを解除できると主張した。一方、政府は、暗号化機能のロックを解除する必要はなく、ログイン試行が１０回失敗した後に携帯電話のメモリを消去する機能を無効にすることだけを求めている、と反論した。オンラインでの声明の中で、Ａｐｐｌｅ社のＣＥＯであるティム・クックは、そのような行為はｉＰｈｏｎｅ（登録商標）のセキュリティを危険にさらすものであると反論した。氏は、声明の中で「一度作成してしまえば、その技術は何度でも使用でき、あらゆるデバイスで使用できてしまう」と述べている。物理的な世界であれば、レストランや銀行から店舗や家にいたるまで、何億もの錠前を開くことができるマスターキーができてしまうことに相当する。分別のある人間ならば、そんなことは受け入れられないであろう。氏はさらに次のように続けた。「この命令に反対することは、私たちにとって気軽にできることではない。私たちは、米国政府による行き過ぎと思われるものに直面し、発言しなければならないと感じているのだ」。
【０７４４】
Ａｐｐｌｅ社が主張した最後のポイントは、米国司法省がその権限を超えていた点であ

り、技術的な立場ではなく法的な主張であった点であり、それは国家が何らの理由もなく、通信の内容を監視したり、個人のプライバシーを侵害したりする権利などないという憲法主義者やプライバシー擁護者の心情を的確に代弁している。このサンバーナーディーノのケースは明白な理由という条件を満たしているが、議論されている通信デバイスを開くことができる汎用的なバックドアを作成するという考えは、当局による乱用を招く。Ｔｈｅ　Ａｔｌａｎｔｉｃ誌は、２０１６年２月２３日の記事で、「Ａｐｐｌｅ社は正しい：ＦＢＩは多くのｉＰｈｏｎｅ（登録商標）に侵入したいと考えている」と、Ａｐｐｌｅ社の主張を擁護した。同日、英ガーディアン誌も、「ＦＢＩが多くのｉＰｈｏｎｅ（登録商標）へのアクセスを求めている、とＡｐｐｌｅ社が主張」、とレポートした。

【０７４５】

このとき、同じプライバシー保護の立場が米国議会によってとられたのは、奇妙なことであった。３月１日、ガーディアン誌の「米議会がＡｐｐｌｅ社にｉＰｈｏｎｅ（登録商標）のロック解除を強制することは『愚か者の使い』であるとＦＢＩに伝えた」と題するフォローアップ記事を出し、米国の議員等が米国司法省によるプライバシーへの過剰な関与や侵害を非難していることを伝えた。サンフランシスコで開催されたＲＳＡカンファレンスでは、Ｍｉｃｒｏｓｏｆｔ社の法務顧問であるブラッド・スミス氏が、「地獄への道は裏口から始まる」と語った。スミス氏は、「この重要なケースでＡｐｐｌｅ社と一緒に立ち向かう」ために、この会合に出席していたコンピュータセキュリティ業界の人々を挑発した。

【０７４６】

この騒ぎの間、ＮＳＡの内部告発者であるエドワード・スノーデン氏を含む多くのセキュリティ専門家は、携帯電話のロックを解除することはＦＢＩが主張したほど難しくないという立場を表明していた。スノーデン氏は、モスクワからのビデオリンクを通じて、Ｇｒｅａｔ　Ｄｅｍｏｃｒａｃｙ会議（３月８～９日）のＣｏｍｍｏｎ　Ｃａｕｓｅ　Ｂｌｕｅｐｒｉｎｔに対して、次のように語っている。「ＦＢＩは、Ａｐｐｌｅ社が携帯電話のロックを解除するための『排他的な技術的手段』を持っていると言っている。敬意を表して言いましょう、それはでたらめだ」。事件が法廷に持ち込まれる前に、ＦＢＩは、ロックされたｉＰｈｏｎｅ（登録商標）に侵入する方法をすでに発見したと報告した。２０１６年３月２９日、米フォーチュン誌はこう伝えている。「ＦＢＩはＡｐｐｌｅ社に対して、ｉＰｈｏｎｅ（登録商標）をどのようにクラックしたのかを伝えないかもしれない」と。

【０７４７】

Ａｐｐｌｅ社対ＦＢＩ事件の法的及び地政学的な影響は広範囲に及んでいる。ＦＢＩが先例となって、今後は他の国々でも、海外に旅行する米国市民が所持する携帯電話を含め、ネットワークに接続されているすべての通信デバイスのバックドアを要求することが予想される。さらに、ｉＰｈｏｎｅ（登録商標）のハッキングが成功した今、犯罪者は常にこれらの方法を発見または再発明して、新たな形態のサイバー犯罪や個人情報の盗難に手を染めていくことになるだろう。犯罪者に出し抜かれないために、政府は犯罪者と同じ手法を使って監視とスパイ活動を拡大しようとしかねず、また同じ政府内の様々な部門が、同様の方法を用いて互いの活動をスパイすることさえ起こり得る。関連する話として、様々な政府がエンドツーエンド通信で使用される暗号化のレベルを制限することを検討している。

【０７４８】

全体としては、こうした出来事は、公有財産の中で現在利用できる既存のセキュリティ手法のどの組み合わせも、セキュリティとプライバシーの両方を保証することなく、少なくとも犯罪者とテロリストを支援することもない、という認識を明らかに強化している。この問題は、ネットワークセキュリティとエンドツーエンドセキュリティ、それに関連する発信者のプライバシーの双方の実現を暗号化だけに頼っていることに起因している。暗号鍵のビットサイズを大きくすることでテキスト、音声、またはファイルのセキュリティを強化すると、コミュニケのセキュリティが強化され、これを破ることがそれまでよりも困難になる。強化されたセキュリティは、セキュリティとプライバシーを維持し、個人情

報の盗難に対処して、企業や法を遵守する市民を保護してくれる。しかし残念ながら、強化されたセキュリティは犯罪者やテロリストであっても監視の目から彼らを保護し、何も咎められず不可視の状態で彼らが活動することを可能にしてしまうのである。

【０７４９】

このことを、図１０４Ａに示す。ここで、発信者１８２５Ａは、様々な経路からのサイバー攻撃に苦しむインターネット１８２１などの安全でないネットワークを介して、受信者１８２５Ｑと通信している。つまり、このネットワークには脆弱性という巨大な「攻撃面」が存在している。攻撃対象領域を減らすために、暗号化１０２６と復号化１０３２を使用して、ネットワーク１８２１よりも小さな攻撃対象領域を持つ暗号化されたパイプまたはトンネル１８２０を形成する。問題は、使用する暗号鍵の大きさを決定することである。表１８２４に示されるように、暗号鍵が大きいほど、より多くの組み合わせが得られるため、暗号の解読が困難になる。暗号化は次の２つの目的に使用される：（ｉ）中間者攻撃を防ぐためのネットワークセキュリティを提供するため、及び（ｉｉ）エンドツーエンドのセキュリティを通じて発信者のプライバシーを保証するためである。線分１８２３に示されるように、ネットワークセキュリティを改善すると、エンドツーエンドのセキュリティがそれと同等に向上する。高度なネットワークセキュリティは悪意のある部外者の攻撃を防ぐのに有益だが、過剰なエンドツーエンドの暗号化は両刃の剣となる。鍵のサイズが大きい場合、例えば、ＡＥＳ２５６またはＡＥＳ５１２が採用されていると、システムは「極秘」のネットワークパフォーマンスを提供し、それに伴って自然に発信者にも同じグレードのセキュリティを提供する。しかし、発信者が犯罪者やテロリストである疑いがあっても、ネットワークオペレータも政府も発信者の活動を検出・監視することはできない。

【０７５０】

鍵サイズの得失評価は複雑だ。暗号鍵が小さすぎれば、犯罪者はネットワークとそのユーザをターゲットとして攻撃できてしまうし、暗号鍵が大きすぎれば、犯罪者はネットワークを使用して違法行為を隠したり、詐欺や不正行為の捜査官による検出活動を妨害したりできるからだ。企業環境においては、エンドツーエンドの暗号化により、従業員の業務活動の監視や、企業調査や知的財産訴訟への準拠が妨げられるため、企業のセキュリティポリシーがこのような暗号化を完全に拒否するケースが見られる。

【０７５１】

どのサイズの鍵が解読可能で、どのサイズの鍵が安全かを判断することさえ困難であり、その状況は技術の進化とともに変化していく。もう一度、表１８２４を参照すると、総当り攻撃で解析する必要のある可能な組み合わせの数は、暗号の鍵サイズの関数として計算される。１６ビット鍵には６５ｋの組み合わせしかないが、５６ビット鍵には10^{16}の組み合わせがあり、１２８ビット鍵には10^{38}を超える組み合わせがある。さらに、２５６ビット鍵には１２８ビット鍵よりも３９桁大きい数の組み合わせがある。パターン認識の使用を無視すると、総当り攻撃はあらゆる組み合わせを試みてコードを解読する。「総当り攻撃に対するＡＥＳの安全性」というタイトルのＥＥＴｉｍｅｓの記事で（http://www.eetimes.com/document.asp/doc_id=1279619）、著者は１０．５ペタフロップスが可能な２０１２年頃のスーパーコンピュータが総当り攻撃を実行するのに必要な時間を見積もっている。ペタフロップスは、１秒間に１，０００兆回または10^{15}回の浮動小数点演算、すなわち１，０００テラフロップスである。そのため、５６ビット鍵の計算所要時間はわずか３９９秒、１２８ビット鍵の計算所要時間は1.02×10^{18}年、１９２ビット鍵の計算所要時間は1.872×10^{37}年、２５６ビット鍵では3.31×10^{56}年となる。

【０７５２】

総当たり攻撃を仕掛けるのに必要な時間も変化している。この文書が書かれて以来、世界最速のコンピュータの速度はすでに3倍に達している。２０１５年7月３０日付けのＢＢＣニュースの記事『スーパーコンピュータ：オバマ大統領、世界最速コンピュータの実現を命じる』によると、調査官は、次世代のスーパーコンピュータの目標速度は、その時

点での記録保持マシンの２０倍の速度、すなわち１エクサフロップ（１秒あたり１京回の浮動小数点演算）の演算能力のあるマシン、と報告している。このことは、暗号を解読するのに必要な時間が、年を追うごとに減少し続けていくことを意味している。暗号を解読するさらなる新しいアプローチとして、ビットコインのマイニングに使われている方法である超並列処理を採用する方法がある。１台のスーパーコンピュータを使用する代わりに、数千～数百万台のコンピュータを同時に使用することで、攻撃を同時進行させ、解読時間を劇的に短縮できる。今日の最速のマイクロプロセッサの能力はすでに１．１テラフロップスを突破しているので、３万台のクラス最高レベルのマイクロプロセッサが連動すれば、現時点で世界最高速のコンピュータに匹敵する速度が得られるのだ。エクサフロップの演算能力を持つコンピュータを実現するために必要なマイクロプロセッサは１００万個にすぎない。専用のＡＳＩＣはセキュリティをさらに侵食する可能性があるが、量子コンピューティングはさらにそれをはるかに超えて何桁も高速に変えることが確実である。

【０７５３】

結論として、サイズの大きな鍵によるエンドツーエンド暗号化は、通信のプライバシーとセキュリティを実現するための優れたソリューションとは言えない。ＳＤＮＰネットワーク及びハイパーセキュアラストマイル通信によって可能になる代替アプローチは、本明細書で開示している通り、ネットワークセキュリティからエンドツーエンドの暗号化を分離する。図１０４Ｂに示されるように、それぞれの発信者と受信者を表すＳＤＮＰクライアント１７００Ａと１７００Ｑとの間の通信は、ＳＤＮＰネットワーク１８３１によって行われる。ネットワークの小さな攻撃対象領域は、動的スクランブル化、断片化、ジャンク挿入、及び制御のための３チャネル通信を使用してルーティングされるホップバイホップの暗号化を使用する匿名マルチルート及びメッシュデータ転送によって実現される。ラストマイル通信及びＳＤＮＰクラウド内のすべてのホップでは、セキュリティクレデンシャル情報が動的に変化するが、このプロセスは、ＳＤＮＰエンコード操作１８３２及びＳＤＮＰデコード操作１８３３を用い簡略化形式で表現されている。

【０７５４】

表１８３４で説明し、線分１８３０で示すように、これらの方法は様々な組み合わせで、暗号化のみに依存することなく、秘密または極秘の暗号化標準と同等のセキュリティを実現している。線分１８３０はフラットであるため、ｙ軸に表示されるエンドツーエンドの暗号化とｘ軸に表示されるネットワークセキュリティの間に相互依存性がないことを示している。その代わりに、様々なＳＤＮＰセキュリティ方式を適用することにより、ネットワークセキュリティレベルをケースＡからケースＤに調整できる。これらのセキュリティ操作はＳＤＮＰソフトウェアによって実行されるが、発信者と受信者はいずれもＳＤＮＰネットワーク１８３１及びその様々なセキュリティゾーンを経由してデータパケットが転送される際にセキュリティクレデンシャル情報が使用されていることに気付かない。特に、会話中のクライアントは、ラストマイルネットワークの暗号鍵の交換に参加していることを意識することはない。分散ネットワークとしては、ＳＤＮＰクラウド内での暗号化の使用はラストマイルセキュリティとは関係がなく、システムのマスターキーは存在しない。そのため、ＳＤＮＰネットワーク１８３１のセキュリティは、暗号化１０２６及び復号化１０３２によって実行されるエンドツーエンドの暗号化には依存せずに暗号化されたパイプ、すなわちトンネル１８２０を生成する。

【０７５５】

ＳＤＮＰネットワーク１８３１で使用される暗号化では、エンドツーエンド暗号化トンネル１８２０と同じサイズの鍵を使用する必要はない。グラフに示されるように、エンドツーエンド暗号化の商用及び企業のセキュリティアプリケーションは、ＳＤＮＰクラウド内のシングルホップ動的暗号化にＡＥＳ２５６が使用されている場合でも、点線１８３５で示す１２８ｂキー暗号化（ＡＥＳ１２８など）を使用できる。実際のところ、エンドツーエンドの暗号化では、ネットワークセキュリティを損なうことなくＲＳＡまたはその他の暗号を利用できる。ＳＤＮＰネットワーク１８３１は、エンドツーエンドの暗号化トンネル１８２０が存在しない場合であっても、ＦＩＰＳ１４０－２軍事グレードセキュリテ

ィに準拠したＡＥＳ暗号化によって保護される。前述のように、ＳＤＮＰネットワーク１８３１は、すべての外部のサイバー攻撃及び中間者攻撃を防止する。エンドツーエンドの暗号化されたトンネル１８２０は、ネットワークオペレータや他の「内部」からのハッキングによる介入から発信者を保護する。これに関して、本開示のエンドツーエンド暗号化は、データパケットの転送セキュリティを達成するためではなく、主に発信者のプライバシーを保証するために使用される。

【０７５６】

ネットワークのセキュリティを危険にさらすことなく、エンドツーエンド暗号化の強度を増減できるほか、排除することもできるため、この手法は幅広いアプリケーションに適応できる。例えば、点線１８３５で示されている１２８ｂキー暗号化が中小企業や個人の使用には厳しすぎる場合であれば、個人のプライバシーを犠牲にすることなくビット数を減らすことができる。軍事用途または政府用途では、暗号鍵の長さを必要に応じて１９２ｂ、２５６ｂ、または５１２ｂに増やすことができる。これに関して、本開示のＳＤＮＰシステムは、現在の暗号化ベースの通信の欠陥を克服し、代替アプリケーション、デバイス、またはネットワークでは利用できない機能を提供する。

【０７５７】

セキュリティ管理

【０７５８】

ＳＤＮＰ通信のもう１つの重要な特徴に、セキュリティ管理に対する独自のアプローチがある。セキュリティ管理は、次のような多くの状況で必要とされる。

・ＨＲポリシーまたは従業員の調査に従って実施された従業員のコミュニケーションの監視、

・財務監査、法定会計、財務報告などをサポートする従業員のコミュニケーションの監視と記録、

・合併買収の一環としての会社間コミュニケーションの文書化、

・ＩＰまたは企業訴訟の一部としての会社間コミュニケーションの文書化、

・召喚状及び犯罪捜査に基づくコミュニケ及び文書の要求に対する対応、

・アカウント情報、通話とメッセージの監視、及び国家安全保障に関するファイルアクセスの法的命令への順守。

【０７５９】

適切な承認を得ることでＳＤＮＰネットワーク管理者は、通信の監視とデータ監視を目的として、指定された「ＳＤＮＰセキュリティエージェント」へのＳＤＮＰネットワークトラフィックのアクセスを促進できる。ＳＤＮＰセキュリティエージェントが確立並びに有効化されるプロセスには、監視アクティビティの前に必ず実行される多層的な承認及び認証プロセスが含まれる。乱用を防ぐため、監視を開始できる個人は存在せず、ＳＤＮＰネットワーク管理者でさえもその権限はない。中央制御がなく、マスターネットワーク鍵がなく、ＤＭＺサーバで、オフラインで動作するゾーン固有のセキュリティクレデンシャル情報を使用して実行される動的ＳＤＮＰエンコード及びデコードを使用する分散ネットワークとしてのＳＤＮＰ通信の動的な性質により、データを回復したり、会話を遡及的に再呼び出したりするメカニズムは存在しない。データは、通常１００ミリ秒未満の短い期間のみＳＤＮＰネットワーク内に存在する。分散システムとして、ＳＤＮＰネットワークは設計上、中央制御機能が本質的に存在しないため、事前呼び出しのメタデータも存在しない。そのため、ＳＤＮＰネットワークは推測的なセキュリティ監視のみをサポートしている。つまり、コミュニケをインターセプトする前に、指定されたＳＤＮＰセキュリティエージェントによる監視を確立する必要がある。

【０７６０】

さらに、ＳＤＮＰクラウド内での断片化メッシュ通信は動的に行われるため、クラウド内、つまりＳＤＮＰゲートウェイを超えたＳＤＮＰノードは、ひとつの完全な会話を収めたデータパケットを伝送しない。ほとんどのノードは、ルーティングの変更前に、５％未満のデータしか伝送せず、通常は一度に１０ミリ秒しか伝送しない。ＳＤＮＰ通信に従っ

て、動的ルーティングは常に異なるメディアサーバを介して通信をリダイレクトする。そのため、クラウドアクセスはコミュニケの復旧や監視には不向きである。ＳＤＮＰクラウドのデータパケットは、捕捉することはできるが、無関係な音、データ、会話、及びジャンクデータなどの無用な寄せ集めデータで構成されている。その代わりに、指定されたＳＤＮＰセキュリティエージェントによる監視は、クライアントデバイス内、あるいは、できればＳＤＮＰゲートウェイ内のいずれかで関連データパケットの完全なセットが必ず通過するラストマイル通信でのみ生産的に行うことができる。

【０７６１】

セキュリティ監視中のデータパケットルーティングの例を図１０５Ａに示す。ここでは、ＳＤＮＰセキュリティエージェント１８４０は、ＳＤＮＰクライアントデバイス１６００ＡとＳＤＮＰクライアントデバイス１６００Ｈの間の会話を監視している。この会話は、ＳＤＮＰクライアントデバイス１６００Ａからラストマイルルータ１６０２Ｇを通じてＳＤＮＰゲートウェイ１７０１ＵにＳＤＮＰクラウド経由で送られるデータパケットを用いて発生するが、クライアントデバイス１６００Ａから送信されたデータパケットはＳＤＮＰゲートウェイ１７００Ｕによって閉じられ、指定されたＳＤＮＰセキュリティエージェント１８４０に安全にルーティングされる。具体的には、ＵＤＰでの伝送中、ラストマイルデータパケット１６３０Ａは、アドレス「ＩＰ　$C_{1,1}$」のＳＤＮＰクライアントからアドレス「ＩＰ　$M_{0,4}$」のＳＤＮＰゲートウェイから出てくるアドレス「ＩＰ　$M_{0,0}$」のＳＤＮＰゲートウェイにＳＤＮＰデータ１を伝送し、ゾーンＵ７ラストマイル経由でＳＤＮＰクライアントアドレス「ＩＰ　$C_{7,1}$」に配信される。許可された監視期間中、クローン化されたＳＤＮＰデータ１が安全にＳＤＮＰアドレス「ＩＰ　ＳＡ」でセキュリティエージェント１８４０　ＳＤＮＰに配信される。複製された監視データパケット１８４１は、複製されたデータクローンが発信者には見えないことを除き、ＳＤＮＰグループコールと同じ方法で動作する。発信者は、したがって自分が監視されていることに気づかない。

【０７６２】

セキュリティの監視は、着信呼に対しても有効である。図１０５Ｂで、ＳＤＮＰデータ７は、アドレス「ＩＰ　$C_{7,1}$」のクライアントデバイス１６００Ｈからアドレス「ＩＰ　$M_{0,4}$」のＳＤＮＰゲートウェイに送信される。ＳＤＮＰクラウドからの伝送の後、データはアドレス「ＩＰ　$M_{0,0}$」のＳＤＮＰゲートウェイから２つの宛先に配信される。最初の宛先であるアドレス「ＩＰ　$C_{1,1}$」のクライアント１６００Ａは、ＳＤＮＰデータ７を含む応答データパケット１６４０Ａを受信する。２番目の宛先であるＳＤＮＰセキュリティエージェント１８４０は、データパケット１８４２を介してクローンデータ「ＳＤＮＰデータ７」を含む同じペイロードを受信する。データパケット１８４２の配信は発信者からは見えないため、発信者は監視されていることに気付かない。

【０７６３】

同じ方法は、断片化された分散ファイルストレージの監視にも適用できる。ただし、セキュリティエージェントは断片化されたデータファイルを捕捉するのではなく、関連するＦＳリンクのコピーを受信するだけで済む。このような例が図１０６に示されている。ここで、ＳＤＮＰファイルストレージデバイス１７００Ｈは、アドレス「ＩＰ　$F_{1,1}$」からゲートウェイアドレス「ＩＰ　$M_{0,4}$」へのＦＳリンク１を含むデータパケット１７４０Ｈを送信する。クローン化ペイロード「ＦＳリンク１」は、ゲートウェイアドレス「ＩＰ　$M_{0,0}$」から送信されたデータパケット１８４３によって、アドレス「ＩＰ　ＳＡ」のＳＤＮＰセキュリティエージェント１８４０にも配信される。リアルタイム通信の場合と同様に、ファイル所有者であるクライアント１６００Ａは、ＳＤＮＰセキュリティエージェントによって監視されていることに気付かない。

【０７６４】

同じ監視メカニズムは、データパケットが複数のＳＤＮＰゲートウェイを介してＳＤＮＰクラウドに出入りするマルチルートラストマイル通信でも有効である。このケースを図１０７に示す。ここで、クライアントデバイス１６００Ａからのラストマイル通信は、ペ

イロードＳＤＮＰデータ１を含む分割データパケット１６３０Ａと、それぞれＳＤＮＰゲートウェイ１７０１Ｕ及び１７０１Ｖを介してクラウドに入るペイロードＳＤＮＰデータ２を運ぶデータパケット１６３０Ｂを含む。ＳＤＮＰクラウドでのルーティング後、データパケットは再結合され、結合されたデータＳＤＮＰデータ３を含むペイロードを持つ単一のデータパケット１６３０Ｌとしてクラウドから出現する。動作中、アドレス「ＩＰ　Ｍ０，０」及び「ＩＰ　Ｍ０，１１」のＳＤＮＰゲートウェイはシグナリングサーバからの指示により、クライアントノードＣ１，１からの着信ＳＤＮＰデータ１及びＳＤＮＰデータ２のクローンを作成し、それらをアドレス「ＩＰ　ＳＡ」のＳＤＮＰセキュリティエージェント１８４０に転送する。クローン化されたデータは、セキュリティエージェントがそれ自身の独自のセキュリティゾーン、すなわち他のいかなるデバイスにも利用できないクレデンシャル情報を使用するゾーンＳＡで動作することを除き、すべてのＳＤＮＰデータ転送に使用される方法と同じハイパーセキュアな方法を使用して、データパケット１８４１Ａ及び１８４１Ｂで送信される。そのため、指定されたセキュリティエージェントが特定の会話を監視したという記録や証拠は一切残らない。

【０７６５】

ＳＤＮＰの監視活動は秘密裏に行われており、本質的に検出不可能な不可視の電話会議と同等であるため、ＳＤＮＰシステムが独立した確認方法を採用して、ネットワーク監視の使用を承認及び確認し、監視の実行を許可されたＳＤＮＰセキュリティエージェントを指定及び確認することが重要である。ＳＤＮＰセキュリティエージェントには、ネットワーク管理者を除く任意のＳＤＮＰクライアントを使用できる。システム破損に対する保護策として、ＳＤＮＰネットワークオペレータやＳＤＮＰ管理者は、ＳＤＮＰセキュリティエージェントとして機能することは許可されていない。つまり、ネットワークを管理しているユーザは、脅しや恐喝にあったとしても、自分自身の使用のためにその機能を破壊することはできないのである。

【０７６６】

ＳＤＮＰセキュリティエージェントには、個人、政府代理人、政府指定代理人、または法務官が任命されることがある。指定されたセキュリティエージェントに特に必要とされる資格は、適用される現地法に従い、会社または国によって異なる。ＳＤＮＰセキュリティエージェントの監視ハードウェアには、通信デバイス、または記録、データストレージ、高度な復号化機能を備えたコンピュータサーバが使用される。ＳＤＮＰネットワークから指定されたＳＤＮＰセキュリティエージェントに送信されるすべての通信は、クライアント自身のコミュニケと同じハイパーセキュア通信で転送されるため、セキュリティ監視は、承認されたセキュリティエージェントによる監視を除き、通話の機密性または発信者のプライバシーを侵害しない。

【０７６７】

さらに、権限の与えられたＳＤＮＰエージェントの監視と許可された機能の実装は、いかなる方法であってもネットワークの整合性とセキュリティを損なわない。運用の詳細やＤＭＺ共有秘密が、ネットワークオペレータやセキュリティエージェントに公開されることはない。ＳＤＮＰシステムの操作は、人間のオペレータの介入や関与なしに自動的かつ自律的に行われており、ＤＭＺサーバはオンラインアクセスを通じて入手することのできないゾーン固有の資格情報を用いてセキュリティが確保されている。したがって、セキュリティの監視により、システムのセキュリティが低下したり、ＳＤＮＰネットワークがサイバー攻撃に対して脆弱になったりすることはない。

【０７６８】

データペイロードは、発信者が作成したものと同じ形式でＳＤＮＰセキュリティエージェントに配信される。ＳＤＮＰセキュリティエージェントへの配信の一部として、すべてのネットワークＳＤＮＰエンコードがデコードされるため、配信されたデータパケットにはネットワークセキュリティの対策情報が一切含まれていない。ただし、クライアントがエンドツーエンド暗号化を採用している場合、ＳＤＮＰセキュリティエージェントは、クライアントがネットワークとエンドツーエンド復号鍵を共有すること、またはＳＤＮＰネ

ットワークからアクセス可能な独立したキーサーバユーティリティを使用することに事前に同意しない限り、クライアントのエンドツーエンド暗号化を解除する必要がある。繰り返すが、このようなエンドツーエンドの暗号鍵と復号鍵は、主にプライバシー保護のためにＳＤＮＰの手法に含まれており、ＳＤＮＰの動的エンコード機能で使用される暗号化とは無関係である。

【０７６９】

不正使用を監視するリスクを最小限に抑えるために、指定されたＳＤＮＰセキュリティエージェントを確立し承認してクライアントまたはクライアントグループを監視するために使用されるＳＤＮＰ管理は、多段階プロセスとなっている。ＳＤＮＰシステムには監視を実行するための対策が含まれているが、この機能の合法的な適用は、ネットワークオペレータ、ネットワーク管理者、及び認可機関ないし認可代理機関の責任で行われる。これらの当事者は、監視が合法的に、かつ当該国の法律に準拠して行われることを保証する責任を個人的に負っている。

【０７７０】

監視の必要性は、様々な状況から発生し得る。企業では、内部告発者からの苦情やセクシャルハラスメントの申し立てにより、人事部門の調査が開始されたり、法廷会計が急遽行われたりする可能性がある。訴訟に関連する裁判所の召喚状（口外禁止命令を含むこともある）もまた監視を必要とする場合がある。企業の問題では、会社のＳＤＮＰネットワークを使用した通信は一般に会社のコミュニケに限定され、プライベート及び個人の通信は対象外である。ほとんどの国では、犯罪の意図が疑われる場合を除き、プライベートな通信は保護されている。国家安全保障や法執行活動の場合、発信者の公的及び私的双方のＳＤＮＰアカウントが監視の対象になる場合がある。このような場合、会社向けの企業ＳＤＮＰネットワークオペレータは会社の通信の監視プロセスを実装する一方、独立した電気通信ＳＤＮＰネットワークオペレータが発信者側の私的通信の監視を実行できる唯一のプロバイダとなる。政府が民間人の通信の監視を開始するためには、裁判官承認の召喚状を提出しなければならない国もあれば、政府には事実上すべての私的通信を監視する権限があると主張する国もある。国際通信の場合、どの法律が適用されるのか、通話の監視を有効にする上でのネットワークの立場をどうすべきなのかを判断することはさらに難しい。

【０７７１】

監視を可能にするために使用されるＡＡＡプロセスの一例を図１０８に示す。クライアントの監視を承認するプロセスには、監視操作の設定に使用されるネットワーク管理者１８５０、クライアントの監視を担当するセキュリティエージェント１８４０、及び監視プロセスの承認に使用される３つの承認エージェント１８５１Ａ、１８５１Ｂ、１８５１Ｃが含まれ、できればネットワークオペレータまたはネットワーク管理者から自律的かつ独立して動作することが望ましい。このプロセスは、調査または裁判所命令に応えて、ネットワーク管理者１８５０が監視要求１８６２を求めることから始まる。管理者は、コマンドダイアログボックス１８６２を使用して、監視が要請されている個人の電話番号を指定する。要求が複数の個人で構成されるグループを監視することである場合、すべての関係者を各々の電話番号と共に一人ずつファイルに入力しシステムにアップロードできる。

【０７７２】

承認ステップ１８６３では、ネットワーク管理者１８５０は、例示的なダイアログボックス１８６４を使用して監視機能を実行するために推奨される候補セキュリティエージェント１８４０を識別する。企業の場合、個人は人事部長、法律顧問、監査委員会のメンバー、独立会計事務所の代表者、または独立調査員である場合がある。訴訟の場合、セキュリティエージェントは、法務官、地区弁護士、ＦＢＩエージェント、またはその他の正式に任命された調査委員会メンバー（例えば、政府の違法行為の場合の特別検察委員会調査パネルなど）が考えられる。次に、システムはＳＤＮＰネームサーバ１７１４をチェックして、セキュリティエージェントがＳＤＮＰアカウントを有し、会社またはネットワークオペレータによって指定されたルールに準拠していることを確認する。国家安全保障に関係する場合には、承認される前に、提案されたセキュリティエージェントの資格情報と犯

罪歴の追加調査が行われる場合がある。

【０７７３】

セキュリティエージェントが承認されると、承認ステップ１８６５で監視要求が承認エージェント１８５１Ａ、１８５１Ｂ、及び１８５１Ｃに転送され、承認エージェントは、監視対象者の名前または説明、または監視を実行するよう任命されたセキュリティエージェントの名前と地位、監視調査の予想期間、及び調査の理由が含まれるダイアログボックス１８６６に列挙される情報を確認する。各承認エージェントは、要求を受諾することも、拒否することもできる。ネットワークオペレータまたは会社のルールにより、承認エージェントの全員一致の承認に基づいて、または単純な過半数の決議により、監視操作が承認されるかどうかが決定される。承認機関の身元は、企業の場合は明らかにされ得るが、刑事事件の場合などでは、ＳＤＮＰネットワークの匿名通信機能によって匿名のまま明らかにされない場合がある。

【０７７４】

監視が承認されると、管理ステップ１８６７にて、クライアントのデータベース１８６８がネームサーバ１７１４で更新され、監視対象のＳＤＮＰクライアントにタグが付けられ、セキュリティエージェントとして承認されたＳＤＮＰクライアント、この例ではデータの網掛け行が識別される。このデータベースのＳＤＮＰアドレスは、監視対象のクライアントと指定されたセキュリティエージェントとの同じ関係を維持するために、ＳＤＮＰアドレスがシャッフルされるタイミングで毎日一緒に更新される。調査日程が満了すると、監視リンクは自動的に切断される。管理ステップ１８６９では、ＳＤＮＰセキュリティエージェント１８４０にリンクが送信され、識別された監視対象のクライアントの進行中のすべての通信を受信できるようにする。エージェントがこの情報をどのように使用するかは、ＳＤＮＰネットワーク操作の問題ではない。セキュリティエージェントによる個人情報の不正な公開は、セキュリティエージェントが全責任を負う犯罪となる場合がある。

【０７７５】

本発明の監視方法により、ＳＤＮＰネットワークは、法を遵守する市民のための安全な通信媒体を維持しながら、不正行為と潜在的なテロ活動の犯罪捜査をサポートできる。ＳＤＮＰネットワークは、無実の民間人のプライバシーを危険にさらしたり、ＳＤＮＰグローバル通信ネットワークのセキュリティを危険にさらしたりすることなく、裁判所命令に準拠して当局に私的なクライアント通信を安全に配信できる。裁判所の命令を尊重するためにバックドアまたはマスターキーが使用されていないため、ＳＤＮＰネットワークを介した今後の通信は匿名かつハイパーセキュアのまま維持される。このようにして、安全な動的通信ネットワークとプロトコル及びそのハイパーセキュアラストマイル通信は、他の手段では不可能なセキュリティ機能を提供でき、ＯＴＴ及びほぼすべてのメッセンジャー及びコミュニケータアプリで採用されているエンドツーエンド暗号化に過度に依存することで生じる犯罪やテロを支援するリスクを完全に回避できる。

【０７７６】

ＳＳ７脆弱性の克服

【０７７７】

Ａｐｐｌｅ社とＦＢＩの論争が通信やセキュリティ業界にとってさほど問題ではなかったとしても、米テレビ番組「６０　Ｍｉｎｕｔｅｓ」のエピソード（http://www.cbsnews.com/news/60-minutes-hacking-your-phone/）は、従来のワイヤレス電話の信号制御チャネルであるＳＳ７（Ｓｉｇｎａｌｉｎｇ　Ｓｙｓｔｅｍ　７）の深刻なセキュリティ脆弱性を明らかにした。この番組で明らかに示されているように、ＳＳ７の脆弱性により、すべてのスマートフォンと接続デバイスがパケットスニッフィングとサイバー攻撃にさらされる可能性があり、個人の電話番号を知るだけで、携帯電話での会話を盗聴したり、ＳＭＳテキスト、添付ファイル、画像を閲覧したりできる。

【０７７８】

Ｓｉｇｎａｌｉｎｇ　Ｓｙｓｔｅｍ　７（ＳＳ７）は、１９７５年に開発されたテレフォニーシグナリングプロトコルで、世界中のあらゆる形態のデジタルテレフォニーで使用さ

れている。ＳＳ７は、ＰＨＹレイヤ１、データリンクレイヤ２、及びネットワークレイヤ３で動作するメッセージ伝送部分、すなわち「ＭＴＰ」で構成され、コールのルーティングを処理する。エンドツーエンドのルーティングは、トランスポートレイヤ４で動作するシグナリング接続制御部、すなわち「ＳＣＣＰ」により管理されている。このプロトコルには、課金、ローミング、及び通話認証に関連する多数のアプリケーションレイヤ７機能も含まれている。ＳＳ７プロトコルは、どうしても必要なものとは言え、攻撃に対して非常に脆弱であり、従来型のテレフォニーの安全を確保する上で深刻なリスクとなる。

【０７７９】

２０１６年４月（https://en.wikipedia.org/wiki/Signalling_System_No._7）、米国議会監視委員会は次のような報告を行った。「この脆弱性の応用は、個人のターゲットを監視する犯罪者から、米国企業への産業スパイ行為を行う外国企業、さらには米国政府関係者を監視する国家まで無限に広がる恐れがある。（中略）この脆弱性は、個人のプライバシーだけでなく、米国のイノベーション、競争力、国家安全保障にも深刻な影響を及ぼす。テキストメッセージを使用した多要素認証を始めとするデジタルセキュリティの多くの革新的技術が役に立たなくなる可能性がある。」

【０７８０】

ＳＳ７のサイバー攻撃は基本的にパケットスニッフィングのカテゴリに分類され、ＳＳ７情報の固有のフォーマットを手引として使用してコンテンツとメタデータの両方を傍受する。ＳＳ７プロトコルは基本的に、パケット情報の解釈に使用される情報テンプレートを提供している。図１０９に示されるように、問題はＳＩＭカード、すなわち「加入者識別モジュール」から始まる。ＳＩＭカードには、加入者とそのアカウントに関する様々な種類の個人情報が含まれている。図に示されるように、一般にネットワークプロバイダから発行されるキャリアＳＩＭカード１８８０は、アンテナ２５Ａ、２５Ｂ、及び２５Ｃと、それらに対応する無線リンク２８Ａ、２８Ｂ、及び２８Ｃによって示されるセルラーネットワークに対して携帯電話３２を識別するために使用される。各ＳＩＭカードには、それを国際的に識別するために使用される１８桁または１９桁の番号である一意の識別子、すなわちＩＣＣＩＤまたは「集積回路カードＩＤ」、が含まれている。国際携帯電話加入者ＩＤまたはＩＭＳＩは、個々のオペレータネットワーク、すなわちＳＩＭカードが機能するホームネットワークを識別する。ローカルネットワークプロバイダは、ＩＭＳＩ番号を使用してＳＩＭカードと通信し、通話を確立する。

【０７８１】

ＳＩＭカードには、ＳＩＭカードの発行国を識別するための「運用地域識別コード」またはＭＣＣの３桁の数字も含まれている。携帯電話から国際電話をかける場合には、ダイヤルシーケンスの一部としてＭＣＣが必要とされる。ＭＣＣの一例としては、米国の３１０～３１６、英国の２３４～２３５、中国の４６０、フランスの２０８、ロシアの２５０、ドイツの２６２、カナダの３０２、ブラジルの７２４などが挙げられる。ＭＣＣは、「モバイルネットワークコード」、すなわちＭＮＣと組み合わせて使用して、ＳＩＭカードを発行したネットワークプロバイダを識別する。これらのコードの完全なリストは、「https://en.wikipedia.org/wiki/Mobile_country_code」に一覧が掲載されている。ＳＩＭカードには、加入者とＳＩＭが動作するネットワークのタイプを一意に定義するための１５桁の「移動局国際加入者電話番号」、すなわちＭＳＩＳＤＮも含まれている。ＳＩＭカードには、ユーザの電話番号に加え、電話やテキストの発着信とその時刻と日付の記録を収めたＳＭＳテキストディレクトリも保持されている。近年、キャリアはモバイル決済を容易にするために、いわゆるセキュア要素を備えた専用のＳＩＭカードを使用してクレジットカードの資格情報を保存するようになっている。

【０７８２】

ＭＣＣ、ＭＮＣ、及びＭＳＩＳＤＮコードは接続プロセスの一部として送信されるため、ＳＳ７への侵入とパケットスニッフィングにより、ＳＩＭカードの母国とキャリア、及び加入者の関連電話番号を簡単に特定することができる。送信データ１８８１は、電話帳、オンライン情報、またはソーシャルメディアを介して、つまりプロファイリングを通じ

て、発信者の身元を追跡するために簡単に使用できる。ひとたび身元を特定し、関連付けが完了すれば、電話番号とＳＩＭを使用して、加入者が世界中のどこに移動しても、加入者の活動を監視することができる。暗号化は、基礎となるコール情報またはメタデータを覆い隠すことはしない。エンドツーエンドの暗号化を使用しても、データパケットは同じ会話からのものであると簡単に識別され、その後の解読試行のために捕捉・保存されてしまう。

【０７８３】

メタデータとコンテンツは別として、発信者の場所もＳＳ７の脆弱性によって侵害される。セルラーネットワークでは、電話はローカル基地局にメッセージを送信し、特定の基地局で利用可能であることを識別する。これらの登録パケットは定期的に送信される。これらのパケットを監視することにより、電話がかかっていない場合やＧＰＳがオフになっている場合でも、特定のＳＩＭカードを使用している電話の位置を、電話中でなくても、またＧＰＳの設定がオンになっていなくても特定することができる。このような方法で、加入者の位置と移動は、加入者に知られずに追跡できる。

【０７８４】

ＳＳ７が本来的に持っているこの脆弱性にもかかわらず、安全な動的通信ネットワークとプロトコルに従って実行されるハイパーセキュアラストマイル通信は、ラストリンクで意味のあるコールデータを不明瞭化することによってＳＳ７攻撃を撃退する。特に、ハイパーセキュアラストマイル通信は、次のような従来の電話通信またはＯＴＴインターネット通信に比べて、セキュリティ上の大きな利点がある。

・ハイパーセキュアラストマイル通信では、コールやメッセージを受け取る側の電話番号またはＩＰアドレスが、相手がＳＤＮＰクライアントでなくても、明らかにされないのである。

・ハイパーセキュアラストマイル通信では、順次データパケットが同じコールの一部であるのか、あるいはまた異なる宛先と関連性のないデータパケットを表しているのかを識別しない。

・データパケットのコールの特異性を隠すことにより、ハイパーセキュアラストマイル通信はコール時間に関するメタデータを不明瞭化する。

・ハイパーセキュアラストマイル通信は、ペイロードを動的にエンコードし、パケットコンテンツへの不正アクセスを防ぎ、音声、ビデオ、テキスト通信、写真、ファイル、その他のコンテンツのプライバシーを保護する。

【０７８５】

したがって、すでに説明したとおり、開示された安全な動的通信ネットワークとプロトコル及びハイパーセキュアラストマイル通信を使用した通信では、ＳＳ７の脆弱性の影響を受けることがない。ＳＤＮＰ通信は独自のプロトコルを使用して実行され、エンコードされたペイロードによって伝送されるため、２Ｇ、３Ｇ、４Ｇ／ＬＴＥテレフォニーなどのオープンで暗号化されていないチャネルで伝送されるパケットであっても、ＳＤＮＰデータパケットから通話データやコンテンツを抽出することはできない。したがって、パケットスニッフィングを使って、ＳＤＮＰのコーディングや断片化されたデータ転送に対してサイバー攻撃の開始しようとしても効果は得られない。

【０７８６】

ＳＤＮＰの偽装機能

【０７８７】

上記を考慮すると、ＳＳ７の脆弱性がＳＤＮＰ通信に与える唯一の影響は、発信者の位置を明らかにする点である。携帯通信会社のＳＩＭの電話番号は各ユーザのＩＤにリンクされているため、携帯電話の電源を入れると、電話がかかっていない場合でも、必ず最寄りの携帯電話基地局との通信が発生する。この基地局の情報は、ＧＰＳをオフにしても、ユーザの位置を三角測量し、加入者の移動を追跡するために使用できる。こうした未承認の追跡はＳＳ７に依存しているため、従来の携帯電話会社のＳＩＭカードを使用しているデバイスは、ＳＤＮＰクライアントとして動作しているデバイスであっても、位置追跡に

対して脆弱である。

【０７８８】

図１１０の簡素化したネットワーク概略図に示す通り、本開示で示すところの「ＳＤＮＰ偽装機能」と称するハイパーセキュアラストマイル通信の強化により、加入者の追跡は完全に阻止される。この機能を実装するには、通常の携帯電話会社のＳＩＭカード１８８０をＳＤＮＰ　ＳＩＭカード１８８２に置き換える。ＳＤＮＰ　ＳＩＭカードは、加入者ではなくＳＤＮＰネットワークオペレータに登録されるため、ＳＤＮＰ　ＳＩＭカード１８８２には個人の加入者情報は記録されない。ＳＤＮＰ　ＳＩＭカード１８８２は、ネットワークにアクセスできる点はプリペイドＳＩＭカードに似ているが、個人情報は一切含まれていない。代わりに、アカウント所有者の個人情報はすべてＳＤＮＰネットワークのネームサーバ内に安全に保存されており、ハッカーがアクセスしたり、サイバー攻撃を受けたりすることはない。

【０７８９】

動作中、ＳＤＮＰの偽装機能は、ＳＤＮＰネットワークオペレータのみが認識しているＳＩＭカード１８８２を使用することにより、所有者の本当の身元を隠す。このように、ＳＩＭカード内に含まれる電話番号は、携帯電話３２と基地局２５Ｂとの間にＰＨＹレイヤ１とデータリンクレイヤ２の接続２８Ｂを確立するために使用されるが、ルーティングは行わない。代わりに、ラストマイルルーティングのデータパケットの送信元アドレスと宛先アドレスが、ＳＤＮＰシグナリングサーバ１６０３Ａからの指示に従って、ＳＤＮＰアプリ１３３５Ａ及びＳＤＮＰゲートウェイ１６０１Ａによって管理される。

【０７９０】

ＳＤＮＰゲートウェイ１６０１Ａを介してルーティングされるＳＤＮＰアプリからのコールは、ＳＩＭカード番号とは異なる番号で表示される。物理ＳＩＭカード番号からＳＤＮＰ電話番号へのこの変換は、ＳＤＮＰネームサーバ１６０４Ａによって実行される。コールのルーティング中に変換テーブル１８８５に従ってＳＤＮＰの電話番号をＳＩＭの電話番号に変換することですべてのユーザに対して物理ＳＩＭカード番号を偽装する。ＳＤＮＰの偽装機能を使用すると、電話の所有者の本当の身元が完全に隠される。ＳＤＮＰクライアントに電話をかけるには、外部の発信者は、自分がＳＤＮＰクライアントでなくても、ＳＤＮＰの番号に電話をかける。ＳＤＮＰネットワークは、このコールを、ＳＩＭカードの電話番号を公開することなく、ＳＤＮＰクライアントに自動的にルーティングする。同様に、ＳＤＮＰクライアントは、ＳＤＮＰ以外の相手先にコールを発信し、このコールの受信者にはＳＩＭカード番号ではなく、ＳＤＮＰ番号からの着信コールが表示される。このようにして、ＳＤＮＰはインターネット通信のＮＡＴゲートウェイと同様の電話機能を実行する。唯一の違いは、ＳＤＮＰシステムはリアルタイムネットワークであり、インターネットはそうではないことだけが異なる。

【０７９１】

携帯電話３２の真のユーザＩＤはコール２８Ｂによっては明らかにならないため、携帯電話の位置を三角測量しても、そのユーザとすべての通信が匿名のままであるため役に立たない。そのため、身元不明の携帯電話の位置を追跡しても、ハッカーにとって有益なことは何もなく、ＳＳ７の脆弱性は回避される。ＳＤＮＰクライアントが海外を旅行している場合、この旅行者は現地のプリペイドＳＩＭカードを購入し、ＳＤＮＰ番号にリンクできる。ＳＤＮＰ加入者は引き続きＳＤＮＰ電話番号にかけられたコールを受信するが、ラストリンクの通信はローカルＳＩＭカードを使用して発生するため、ローミング料金が回避される。このようにして、ひとつのＳＤＮＰ電話番号を、長距離通話料なしでグローバル番号として使用することができる。

【０７９２】

ＳＤＮＰサブネット

【０７９３】

ＳＤＮＰ通信クラウドは、ソフトウェアベースの通信ノードである独自のソフトスイッチを使用して、プライベートまたは公にホストされているあらゆる相互接続コンピュータ

のネットワーク全体にリモート展開できる。サーバネットワークの例には、Ｍｉｃｒｏｓｏｆｔ、Ｇｏｏｇｌｅ、及びＡｍａｚｏｎの各社がホストするような、私企業が所有し公に貸与されるネットワークが含まれる。図１１１は、２つの別個のサーバネットワークに展開された２つのＳＤＮＰクラウドを示している。この図に示されるように、サーバ１９０１Ａ、１９０１Ｂ、１９０１Ｃ、及び１９０１Ｄで構成されるＳＤＮＰクラウドは、それぞれＳＤＮＰ通信ノードＭ$_{0,0}$、Ｍ$_{0,4}$、Ｍ$_{0,7}$、及びＭ$_{0,8}$をホストしている。第２のＳＤＮＰクラウドはサーバ１９０２Ａ、１９０２Ｂ、及び１９０２Ｃで構成され、それぞれＳＤＮＰノードＭ$_{10,0}$、Ｍ$_{10,1}$、及びＭ$_{10,2}$をホストしている。これらのクラウドはそれぞれゾーンＺ０とゾーンＺ１０の別々のセキュリティクレデンシャル情報を利用するため、２つのＳＤＮＰクラウドは完全に区別され、情報を直接には共有できない。ただし、ＳＤＮＰアプリ１３３５を実行している携帯電話３２として示されている単一のＳＤＮＰクライアントは、それが異なるコンピューターサーバリースプロバイダによってホストされている場合であっても、両方のクラウドに適切に認証されてアクセスできる。例に示されるように、ＳＤＮＰクライアントＣ$_{1,1}$は、ルータ１９１０を介したハイパーセキュアラストマイル通信を使用してゾーンＺ０クラウドのＳＤＮＰゲートウェイノードＭ$_{0,7}$にアクセスし、また同じルータ１９１０を介してハイパーセキュアラストマイル通信を使用してゾーンＺ１０クラウドのＳＤＮＰゲートウェイノードＭ$_{10,0}$にアクセスでき、両者の会話やデータパケットが混じり合うリスクがない。

【０７９４】

２つの独立したクラウドへのアクセスは、共通のコミュニケータアプリケーションＵＩ／ＵＸ　１９２０を介して行われる。各クラウドへのアクセスは、個別のダイアログサンドボックス１９２１Ａ及び１９２１Ｂにコンパートメント化されている。情報は個人アカウントのサンドボックス１９２１Ａから携帯電話にダウンロードできるが、ビジネスアカウントのサンドボックス１９２１Ｂからデータをエクスポートする方法は、企業と企業のセキュリティ管理に依存する。

【０７９５】

デバイスをＳＤＮＰクラウドに接続するには、ＳＤＮＰアプリを、ソフトウェアまたはファームウェアとしてそのデバイスにインストールする必要がある。インストールは次のように行われる：（ｉ）アプリケーションのダウンロード、（ｉｉ）ＳＤＮＰネットワークで生成された認証コードによるデバイスＩＤの確認、（ｉｉｉ）個人識別クレデンシャル情報の確立、及び（ｉｖ）特定のＳＤＮＰクラウドへの参加への承認の取得。一旦有効化されると、ＳＤＮＰアプリケーションは、独立したＳＤＮＰクラウドへのハイパーセキュアラストマイル接続を構築する。多くの場合、ビジネスアカウントのＩＤ確認とユーザ認証は、個人アカウントのアクセスに必要なものよりも複雑であり、多要素認証方法が必要になる場合もある。

【０７９６】

ＳＤＮＰ通信はソフトウェアベースであり、通信クラウド毎にそれぞれのセキュリティクレデンシャル情報が使用されるため、同じサーバでホストされている場合でも、インストールされているＳＤＮＰ通信ネットワーク同士間での相互作用が存在しない。ゾーン固有のセキュリティクレデンシャル情報によってカスタマイズされた各ＳＤＮＰクラウドが一意に定義されるため、２つのＳＤＮＰクラウドは異なるので、データを直接共有することはできない。都合がよいことに、複数のＳＤＮＰクラウドを同じサーバまたはサーバネットワーク内に共存させることができ、データ漏洩のリスクもない。ビジネスネットワークへのアクセスは、クラウド所有者の要件に従って定義されている通り制御されている。そのため、共通のホストサーバを共有する場合、２つのアカウントと通信クラウドの混在は禁止されており、２つの異なるネットワークに接続するために２つの異なる電話が必要な場合と同じセキュリティで運用される。ゾーン固有のＳＤＮＰクラウド、つまり「サブネット」の自律性を図１１２でさらに詳しく示す。この図で、サーバ１１２１Ａ、１９０１Ｂ、１９０１Ｃ、１９０１Ｄが同時に２つのクラウドをホストしている。一方のクラウドはゾーンＺ０のＳＤＮＰ通信ノードＭ$_{0,0}$、Ｍ$_{0,4}$、Ｍ$_{0,7}$、及びＭ$_{0,8}$、及び他

方のクラウドはゾーンＺ７　ＳＤＮＰ通信ノードＭ$_{7,0}$、Ｍ$_{7,4}$、Ｍ$_{7,7}$、及びＭ$_{7,8}$で構成されている。同じサーバ内で動作しているにもかかわらず、ＳＤＮＰで確立されたプロトコルを使用するハイパーセキュア通信では、直接的なデータ交換を防止できる。したがって、アクセスは、直接的なクラウド間データ交換ではなく、ラストマイル通信によって管理される。

【０７９７】

ＳＤＮＰ通信は、個人的にリースされた一般に利用可能なサーバに限定されず、様々な種類の企業ないし政府機関向けにカスタマイズすることも可能である。実際に、民間企業は多くの場合、とりわけ業務に不可欠なアプリケーションでは、独自のネットワークをホストすることを好む。プライベートネットワークの例としては、ＦｅｄＥｘ、Ｗａｌｍａｒｔ、ＩＢＭなどが挙げられる。機密保持のため、研究機関、大学、及び医療センターで利用されるネットワークも、組織が独自にホストすることが多い。プライベートサーバネットワークはこの他にも次のような目的のホスティングに採用されることも多い。すなわち、ＳａｌｅｓＦｏｒｃｅ．ｃｏｍ、Ｂｏｘ．ｃｏｍ、Ｄｒｏｐｂｏｘ、ｅＴｒａｄｅ、ＳＡＰなどのグローバルビジネスクラウドアプリケーション、ｅＢａｙ、Ａｍａｚｏｎ．ｃｏｍ、Ｐｒｉｃｅｌｉｎｅ．ｃｏｍ、ｅ－Ｉｎｓｕｒａｎｃｅなどの電子コマースプラットフォーム及び比較ショッピングネットワーク、ＹｏｕＴｕｂｅ（登録商標）、Ａｍａｚｏｎ　Ｐｒｉｍｅ、Ｎｅｔｆｌｉｘ、Ｈｕｌｕ、Ｃｏｍｃａｓｔ　Ｘｆｉｎｉｔｙなどのメディアストリーミングサービス、そしてＦａｃｅｂｏｏｋ、Ｔｗｉｔｔｅｒ、Ｓｎａｐｃｈａｔなどのソーシャルメディアなどである。

【０７９８】

より規模の大きい企業では、ＩＴ部門が親組織や子会社に対して個別のネットワークを運用することを選択する場合があるだろう。ただし、多くの民間企業では、インフラストラクチャのコストがネットワーク設計の重要な要素と見られている。ＳＤＮＰシステムは、２つの完全に異なるハードウェアベースのシステムをサポートするのではなく、別個の共有サーバリソースの組み合わせを使用してネットワークを展開する機能を会社組織に提供する。図１１３に示されるように、２つの法人、例えば親会社とその子会社は、別々のサーバと共有サーバの両方で構成されるひとつのサーバネットワークを共同でホストする。具体的には、サーバ１９０３、１９０４Ｂ、１９０４Ｃ、及び１９０４Ｄは、親企業エンティティのためにゾーンＺ７の通信ノードＭ$_{7,0}$、Ｍ$_{7,4}$、Ｍ$_{7,7}$、及びＭ$_{7,8}$をそれぞれホストし、一方、サーバ１９０１Ａ、１９０１Ｂ、１９０１Ｃ、及び１９０３は会社の現地法人のためにゾーンＺ０の通信ノードＭ$_{0,0}$、Ｍ$_{0,4}$、Ｍ$_{0,7}$、Ｍ$_{0,8}$をそれぞれホストする。図に示されるように、サーバ１９０３は、例えば、親エンティティのための２つのＳＤＮＰ通信ノード、すなわちノードＭ$_{7,0}$と、子会社のためのノードＭ$_{0,8}$をホストする。サーバ１９０３とその他のサーバ（図示せず）が両方のエンティティで共有されている場合でも、セキュリティクレデンシャル情報が異なるため、親会社と子会社のＳＤＮＰクラウド間で直接データが共有されることはない。従業員は通常、雇用主のクラウドのみにアクセスするように制限されているが、役員の場合は両方のクラウドへのアクセスが必要になる場合がある。ＳＤＮＰコミュニケータアプリＵＩ／ＵＸ　１９２０で示されるような適切に承認されたユーザには、様々な法人向けの個別のダイアログサンドボックス１９２１Ｃ及び１９２１Ｄが含まれている。このようにして、一台の携帯電話またはタブレットで、ユーザが複数の携帯電話を持っているかのように、データが混在してしまうリスクを伴わずに、異なる法人の複数のＳＤＮＰクラウドにアクセスできる。

【０７９９】

ラストマイルハイパーセキュアセキュリティクレデンシャル情報を使用して複数のＳＤＮＰクラウドへのアクセスを有効化または禁止するＳＤＮＰアプリのマルチプロファイル機能は、ひとつのＳＤＮＰアプリからその数に限りなくアカウントプロファイルをサポートする。例えば、図１１４では、ＳＤＮＰクライアントＣ$_{1,1}$は、ＳＤＮＰノードＭ$_{99,1}$からＭ$_{99,5}$をそれぞれホストするサーバ１９０９Ａから１９０９Ｅを含むゾーンＺ９９のグローバルＳＤＮＰ　ｔｅｌｃｏを介して、長距離料金なしで国際電話を発信でき

るだけでなく、例えば、ＳＤＮＰノードＭ９，０、Ｍ９，４、及びＭ９，８をホストするサーバ１９０５Ａ、１９０５Ｂ、及び１９０５Ｃで構成されるゾーンＺ９のコーポレートクラウドなどの他のクラウドへのアクセスも可能であり、さらにまたＳＤＮＰノードＭ９，０、Ｍ０，４、及びＭ０，８をそれぞれホストするサーバ１９０１Ａ、１９０１Ｂ、１９０１Ｃを介してゾーンＺ０クラウドの加入者を呼び出すこともできる。特定のクラウドへのアクセス権限は、ＳＤＮＰゲートウェイへのラストマイル通信を通じて適用され、システムのＳＤＮＰシグナリングサーバと、許可ユーザの管理に使用されるＳＤＮＰネームサーバによって管理される。

【０８００】

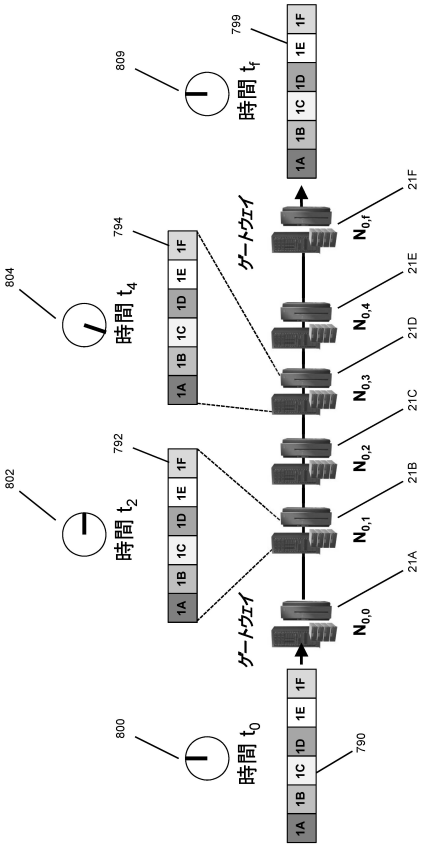
ＳＤＮＰ通信は、政府やセキュリティの分野に必要とされる高度なセキュリティとアクセスが制限されているネットワークでも同様に適用できる。例えば、米国では、地方及び州の法執行機関、ＦＢＩ、米国防軍、米国国家安全保障局、米国の各軍隊（個別及び共同）、米国国務省などの様々な組織が、セキュリティによる制限付き通信を、議会及び立法のサーバネットワークと供に必要としている。他の国々も同様に、様々な政府機関向けに個別のネットワークをホストしている。

【０８０１】

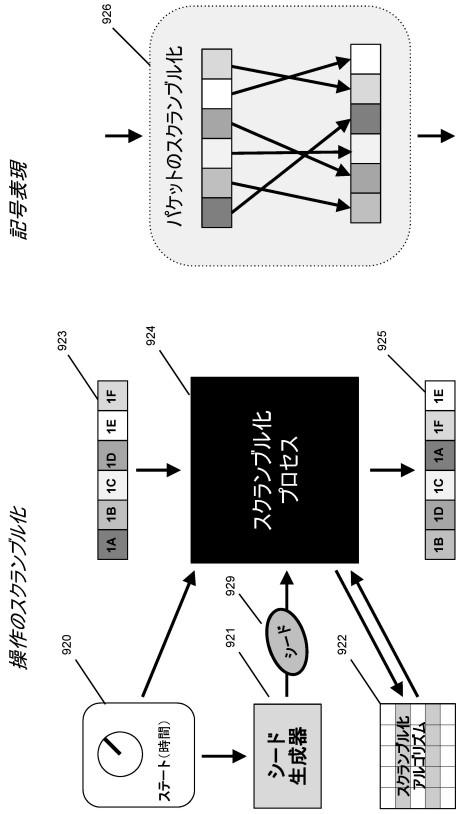
「知る必要がある人にのみ知らせる」方針で特定のクラウドへのアクセスをサポートするため、ＳＤＮＰ通信の方法と技術を活用して、ネストされたサブネットアーキテクチャを実装することができる。図１１５はネストされたＳＤＮＰクラウド構造の例で、これはＳＤＮＰ通信ノードＭ０，０、Ｍ０、４、Ｍ０、５、Ｍ０、９をそれぞれホストするリースされたコンピュータサーバ１９０７Ａから１９０７Ｄで構成されるひとつのセキュアクラウドとして示されている。この外側のネットワーク「シェル」での通信は、ゾーンＺ０のセキュリティクレデンシャル情報を含み、ＳＤＮＰコミュニケータ１９２０に表示される「秘密」レベルのダイアログサンドボックス１９１２Ｅに表示される。ネストされたクラウドには、政府がホストするサーバ１９０６Ａ、１９０６Ｂ、１９０６Ｃ、及び対応するＳＤＮＰサーバノードＭ８、０、Ｍ８、２、Ｍ８、４を含むゾーンＺ８のセキュリティクレデンシャル情報による強化されたセキュリティ内部コアも含まれている。クライアントＣ１，１がゾーンＺ８コアにアクセスするには、「トップシークレット」の安全許可が必要とされ、強化された通信サンドボックス１９２１Ｆを介して通信する必要がある。この技術の政府による応用例のひとつは米国国務省にあり、ゾーンＺ８でのトップシークレット通信は大使及び国務長官によるアクセスに制限されており、世界中の他の米国大使館スタッフはゾーンＺ０のセキュリティクレデンシャル情報を用いたハイパーセキュアの「トップシークレット」通信しか利用できない。

【図面】

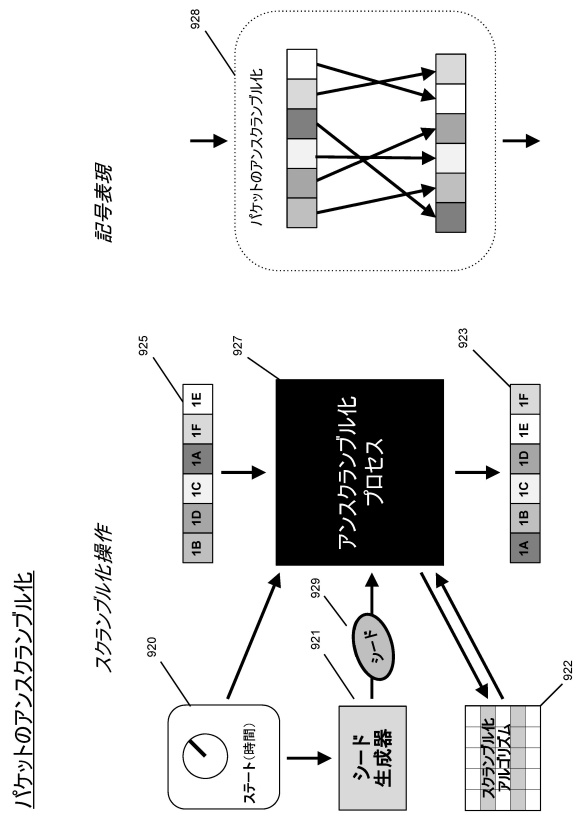
【図１】



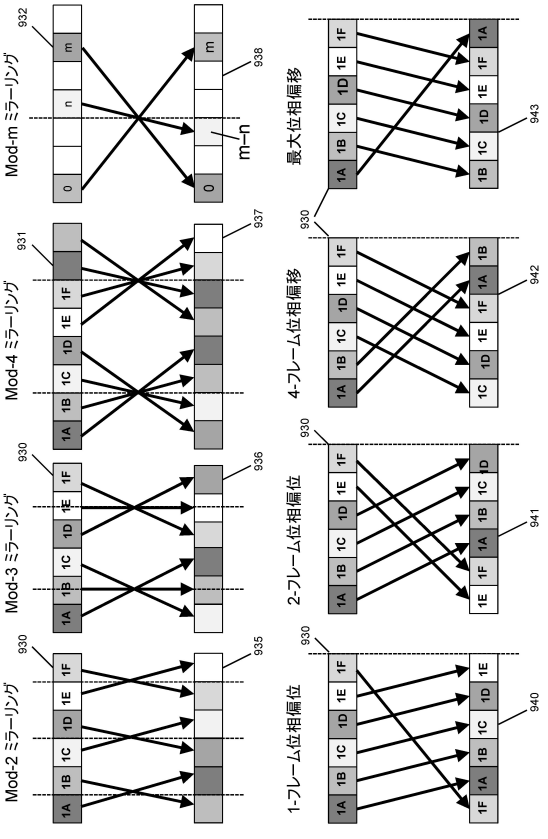
【図２Ａ】



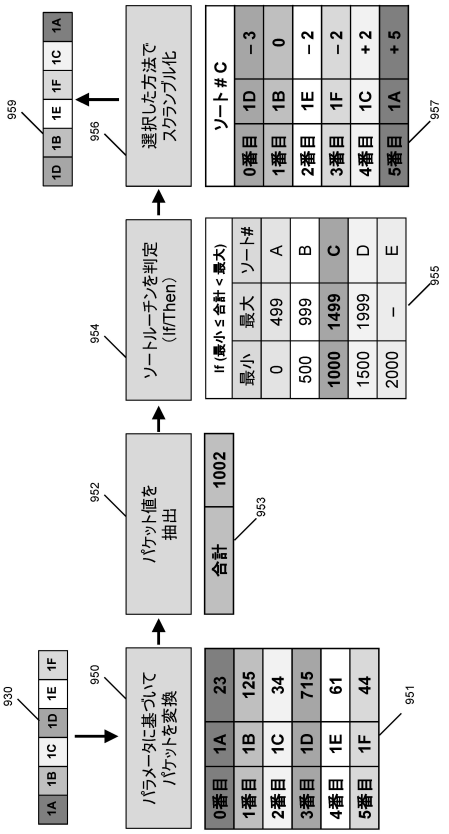
【図２Ｂ】



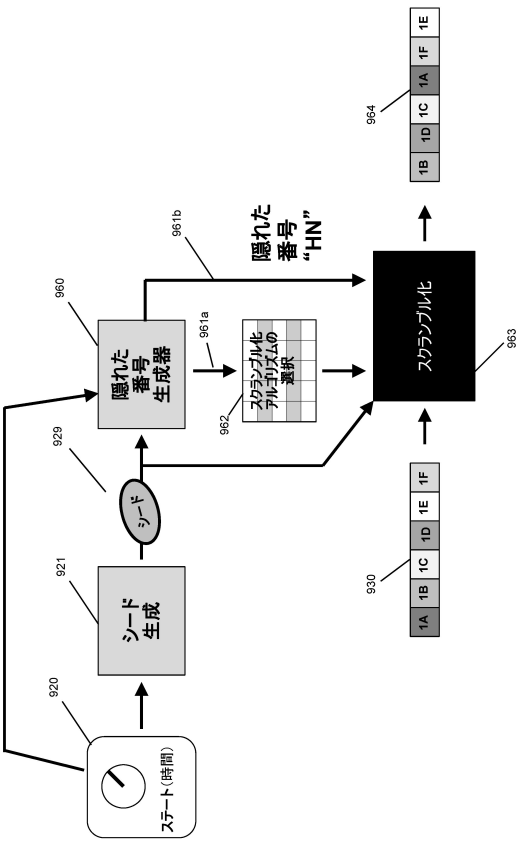
【図２Ｃ】



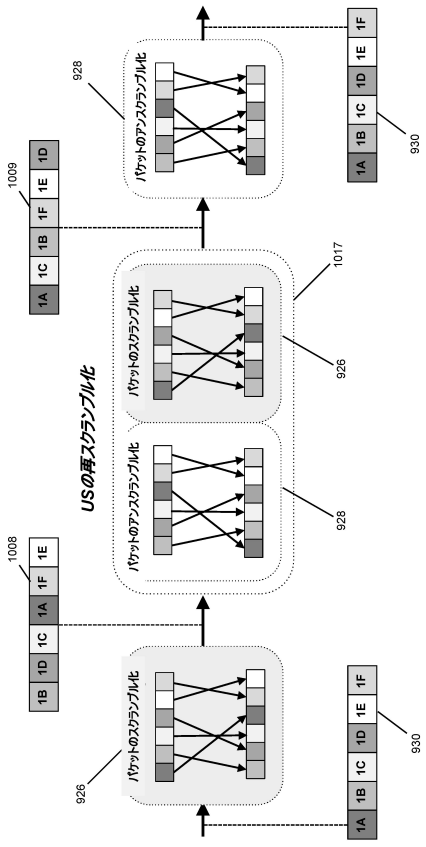
【図２Ｄ】



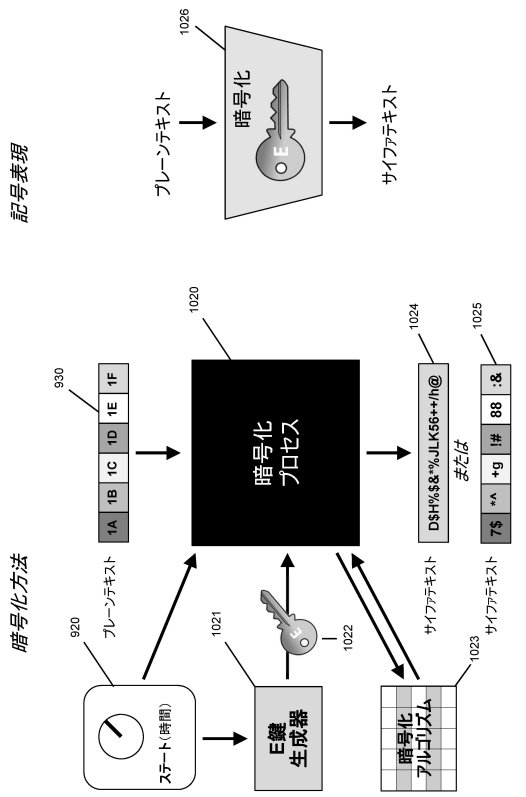
【図２Ｅ】



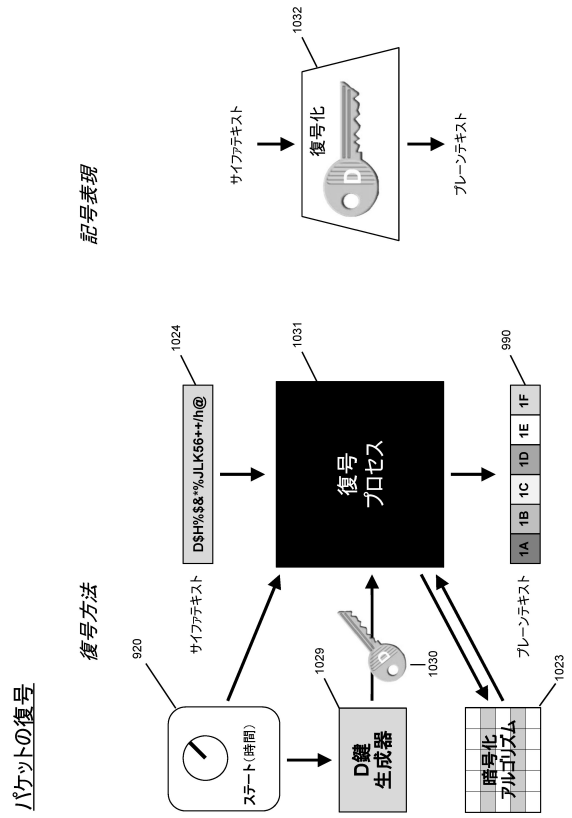
【図３】



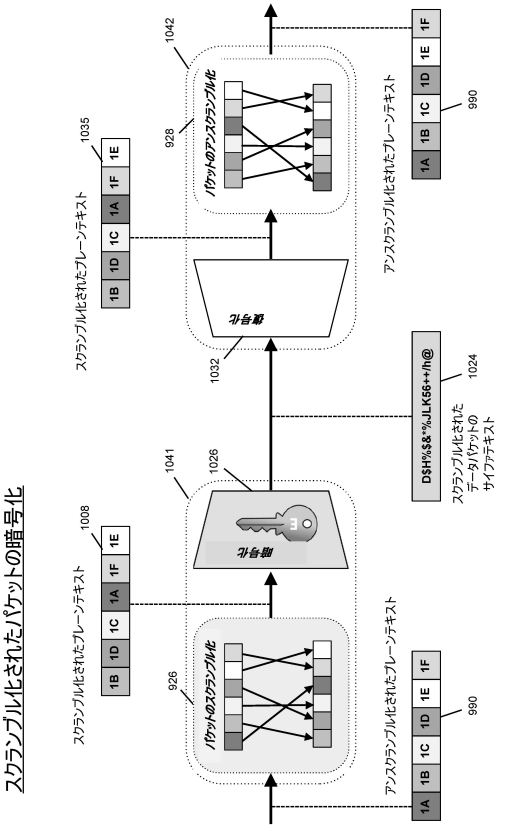
【図４Ａ】



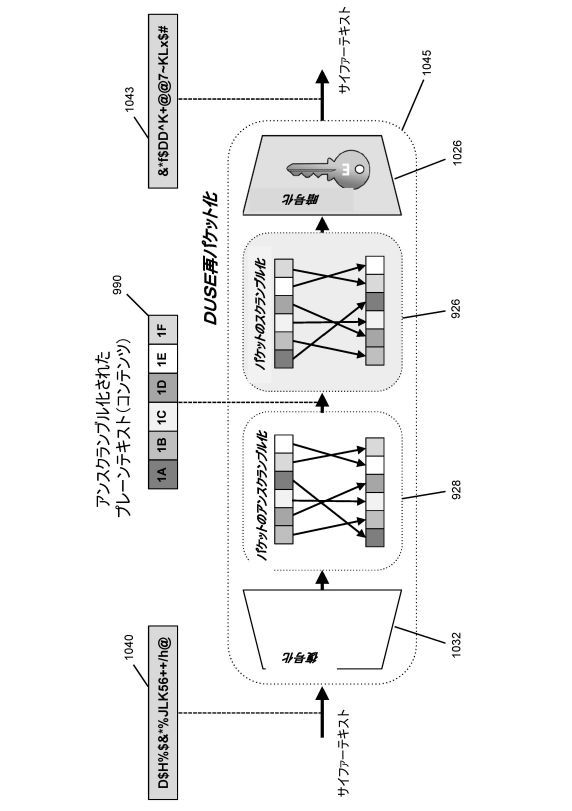
【図４Ｂ】


パケットの復号
記号表現
復号方法
サイファテキスト
復号化
プレーンテキスト
1032
1024
D$H%$&*%JLK56++/h@
1031
復号
プロセス
990
1A 1B 1C 1D 1E 1F
920
ステート(時間)
1029
D鍵
生成器
1030
暗号化
アルゴリズム
1023

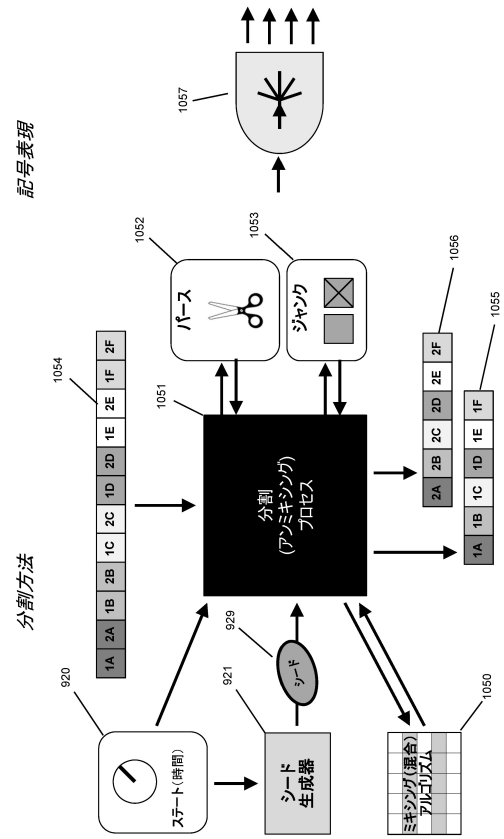
【図５】


スクランブル化されたパケットの暗号化
スクランブル化されたプレーンテキスト
1008
1A 1B 1C 1D 1E 1F
パケットのスクランブル化
926
暗号化
1026
1041
アンスクランブル化されたプレーンテキスト
990
1042
928
1035
1032
DS#%$&*%JLK56++/h@
1024
スクランブル化された
データパケットの
サイファテキスト

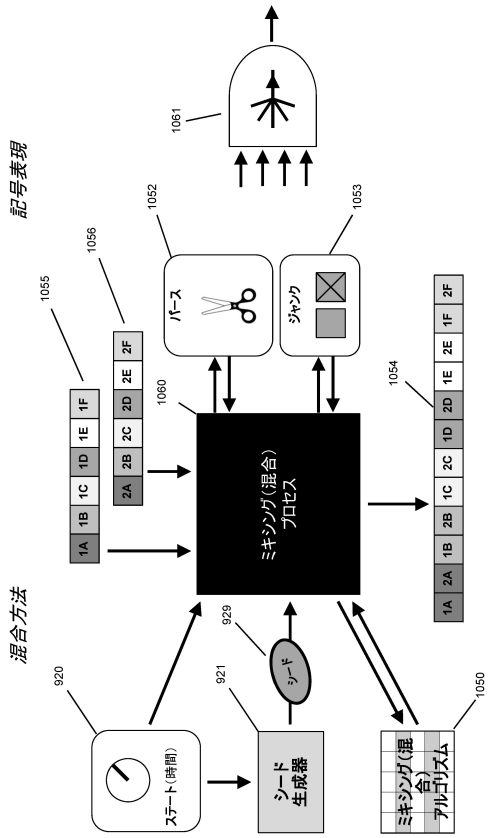
【図６】


DUSE再パケット化
アンスクランブル化された
プレーンテキスト(コンテンツ)
990
1A 1B 1C 1D 1E 1F
1040
D$H%$&*%JLK56++/h@
サイファーテキスト
1043
&'!$DD^K+@@7~KL;$#
1045
1026
926
928
1032

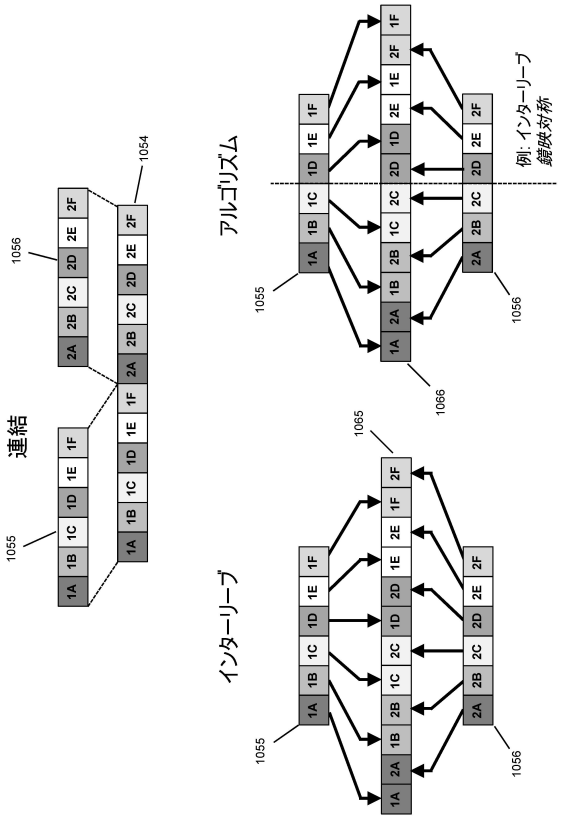
【図７Ａ】


記号表現
分割方法
1057
1052
パース
1053
シャンク
1056
1054
1A 2A 1B 2B 1C 2C 1D 2D 1E 2E 1F 2F
1051
分割
(アンミキシング)
プロセス
2A 2B 2C 2D 2E 2F
1A 1B 1C 1D 1E 1F
1055
920
ステート(時間)
921
シード
生成器
929
シード
1050
ミキシング(混合)
アルゴリズム

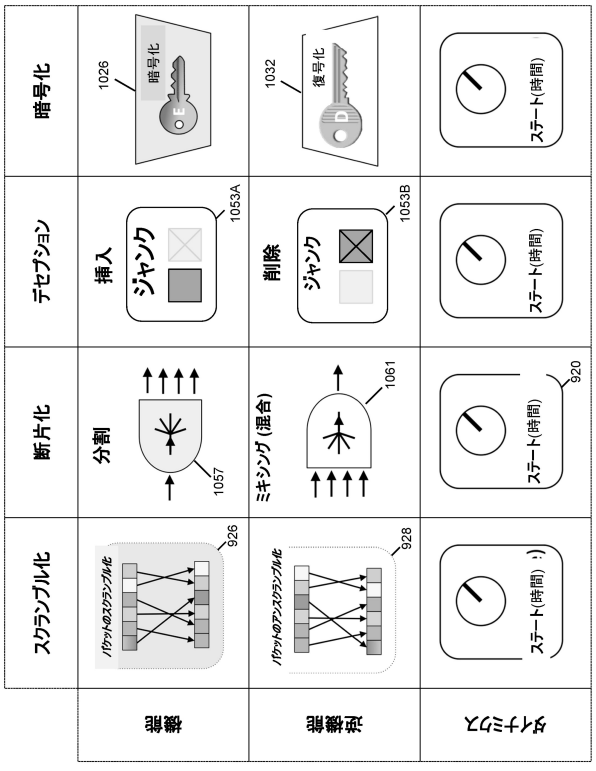
【図７Ｂ】



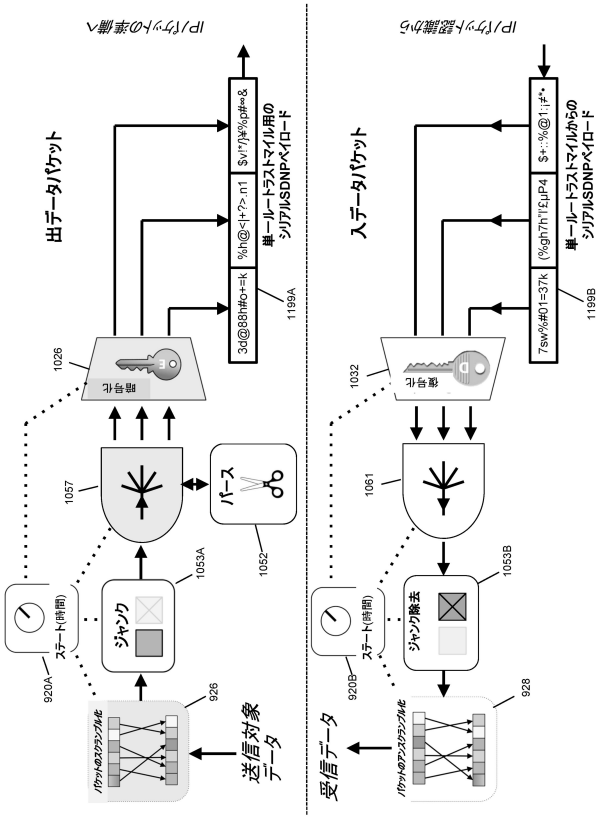
【図８】



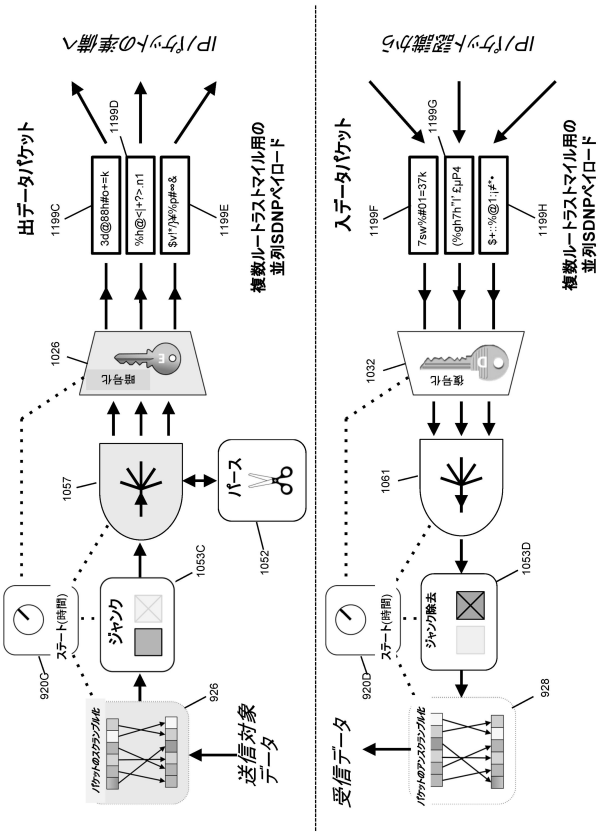
【図９Ａ】



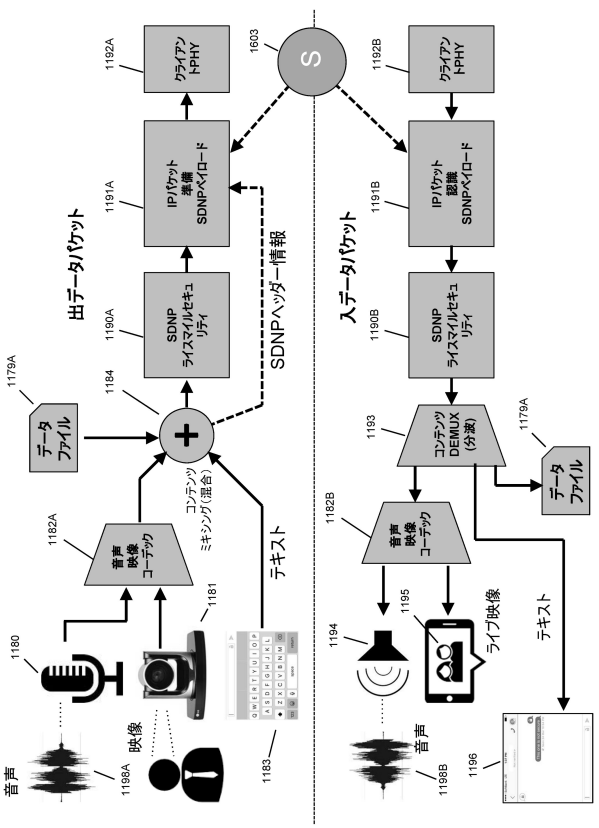
【図９Ｂ】



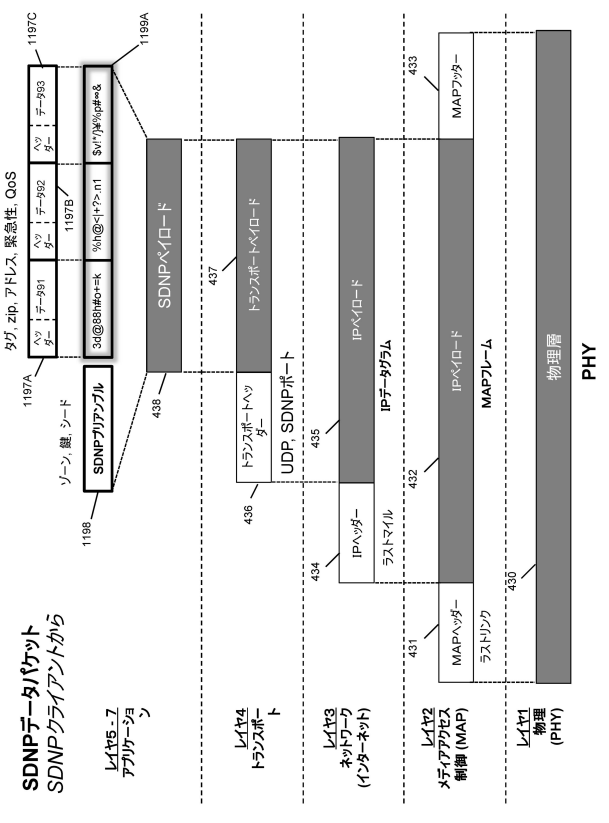
【図９Ｃ】



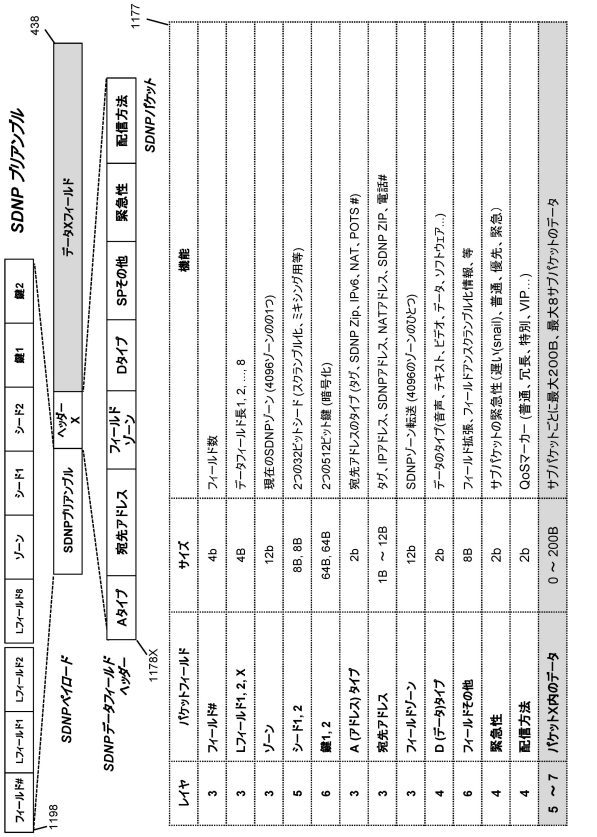
【図９Ｄ】



【図９Ｅ】

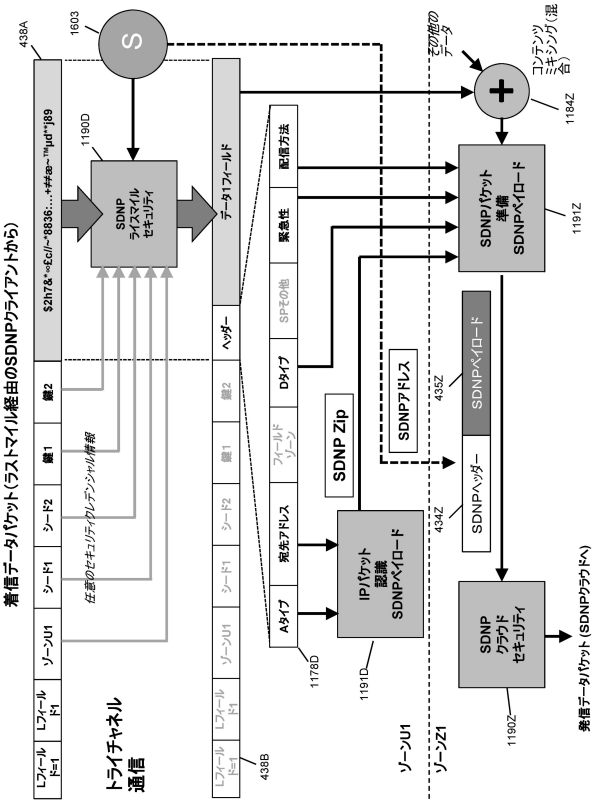


【図９Ｆ】

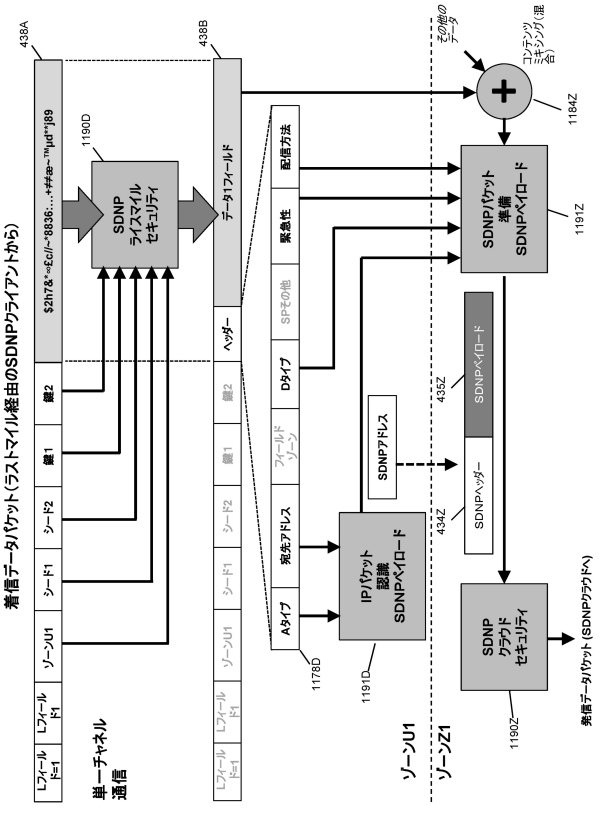


レイヤ	パケットフィールド	サイズ	機能
3	フィールド#	4b	フィールド数
3	Lフィールド1, 2, X	4B	データフィールド長1, 2, ... 8
3	ゾーン	12b	現在のSDNPゾーン(4096ゾーン/0.01つ)
5	シードF1, 2	8B, 8B	2つの32ビットシード(スクランブル化、ミキシング用等)
6	鍵1, 2	64B, 64B	2つの512ビット鍵(暗号化)
3	A (アドレス) タイプ	2b	宛先アドレスのタイプ(タグ、SDNP Zip、IPv6, NAT, POTS #)
3	宛先アドレス	1B ~ 12B	タグ、IPアドレス、SDNPアドレス、NATアドレス、SDNP ZIP、電話#
3	フィールドゾーン	12b	SDNPゾーン転送 (4096のゾーン/0.01とつ)
4	D (データ) タイプ	2b	データのタイプ(音声、テキスト、ビデオ、データ、ソフトウェア...)
6	フィールドその他	8B	フィールド拡張、フィールドデスクランブル化情報、等
4	緊急性	2b	サブパケットの緊急性(遅い(snail)、普通、優先、緊急)
4	配信方法	2b	QoSマーカー(普通、冗長、特別、VIP...)
5 ~ 7	パケットXPRのデータ	0 ~ 200B	サブパケットごとに最大200B、最大8サブパケットのデータ

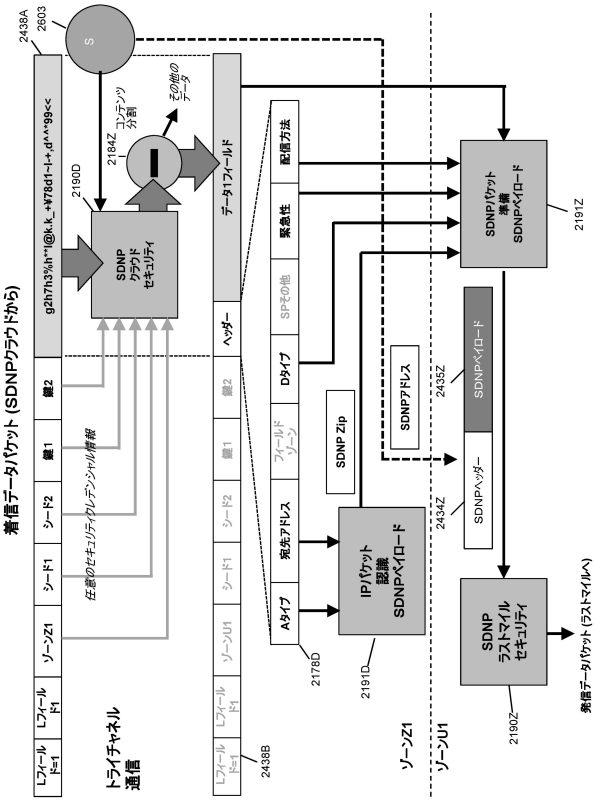
【図９Ｇ】



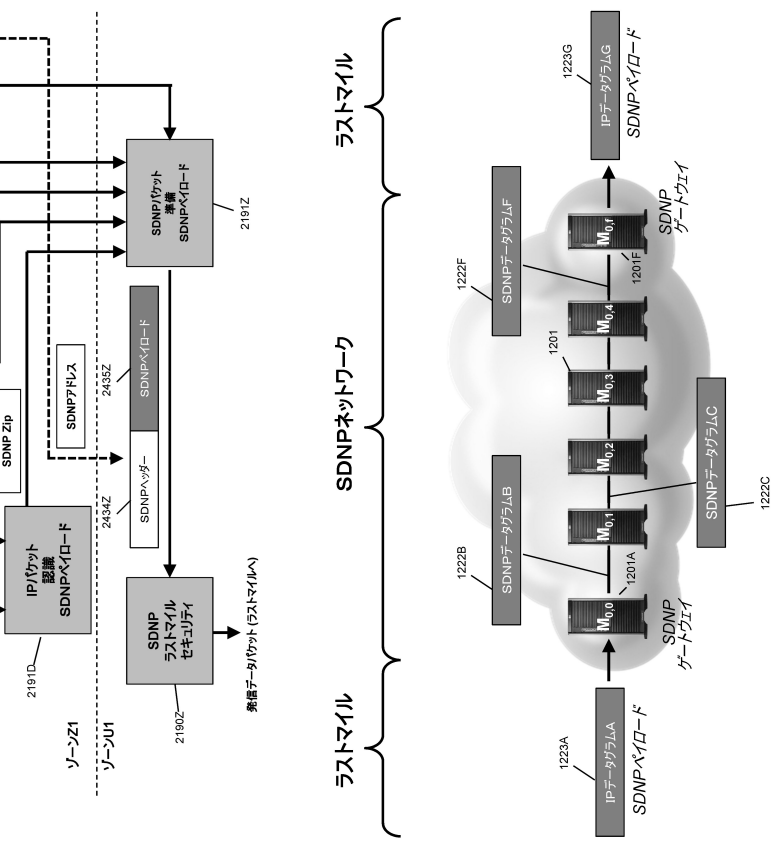
【図９Ｈ】



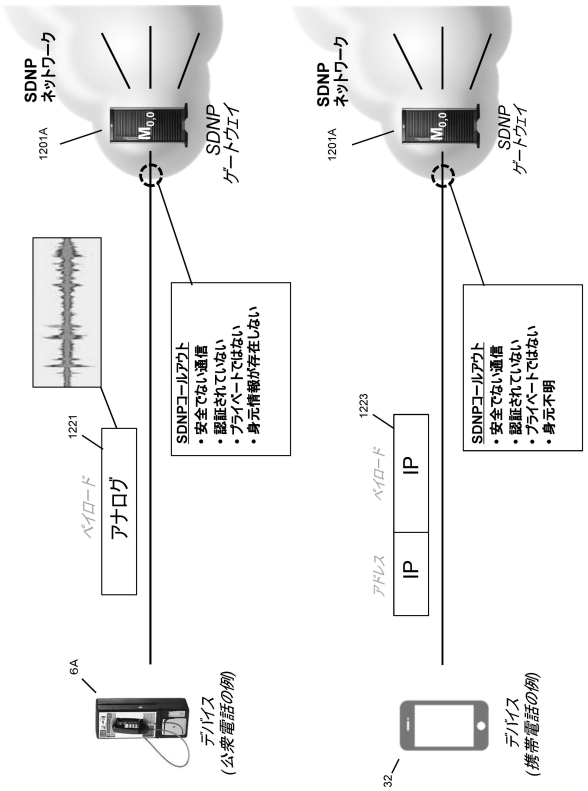
【図９Ｉ】



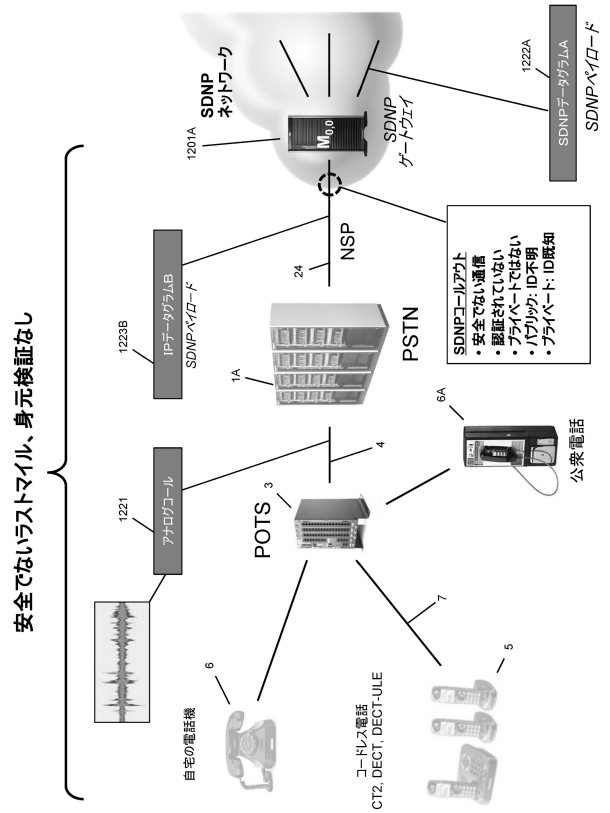
【図１０】



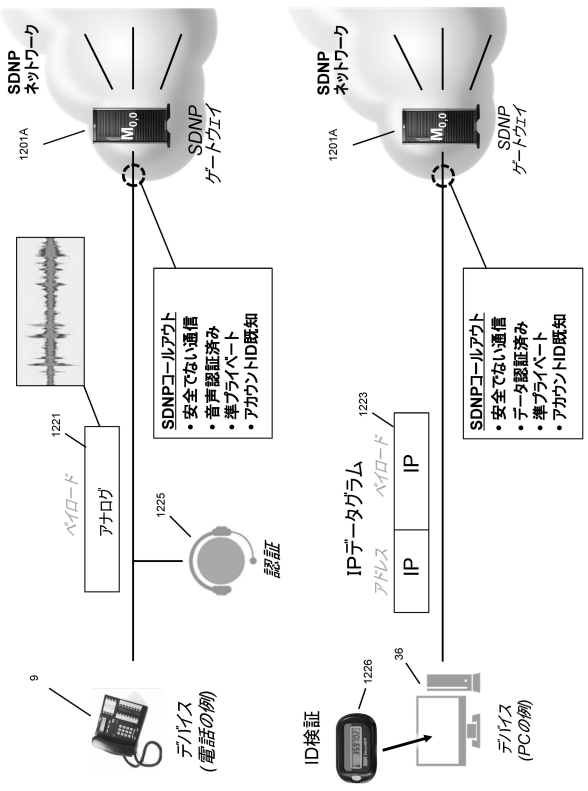
【図１１】



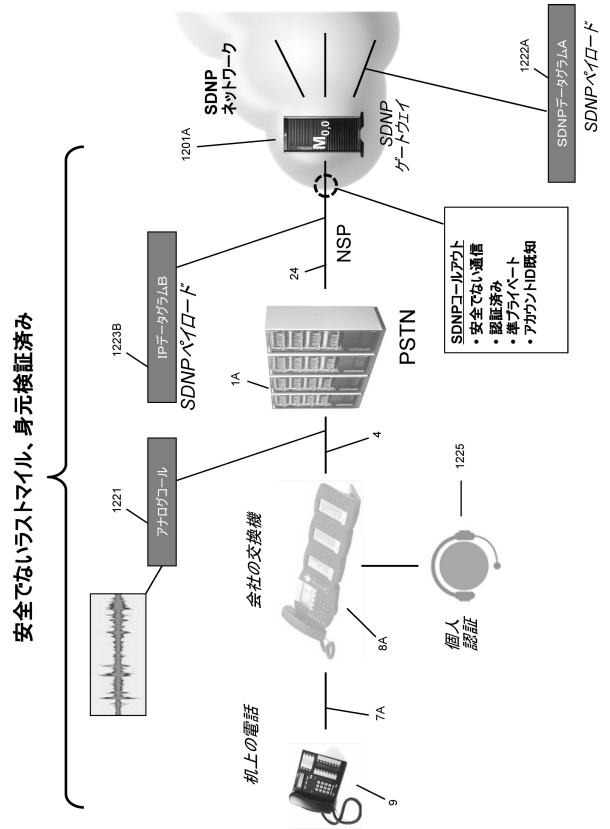
【図１２】



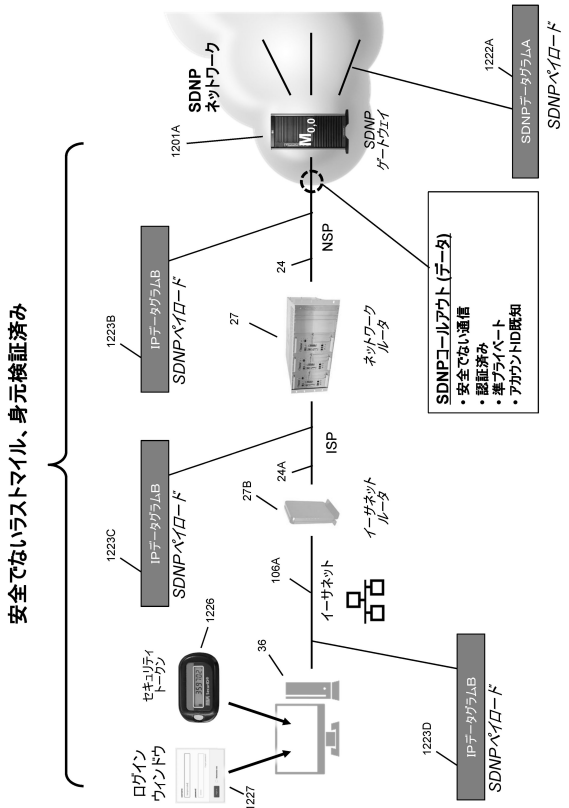
【図１３】



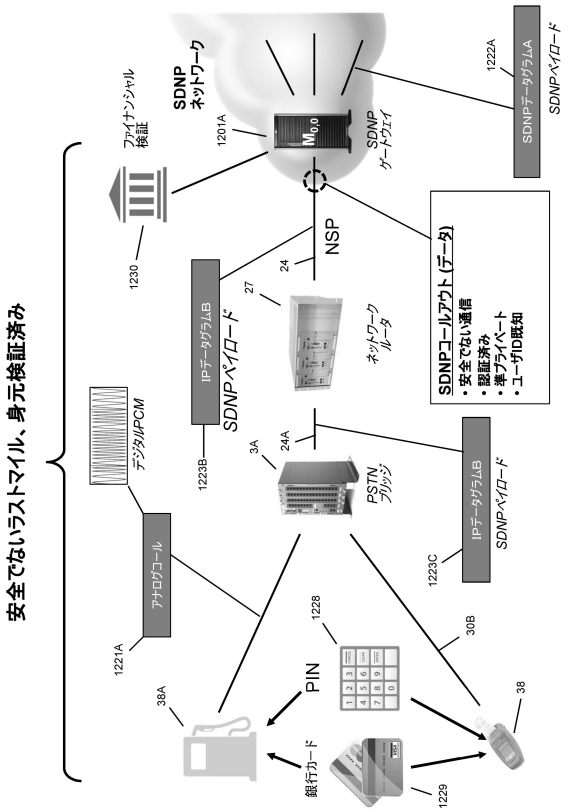
【図１４】



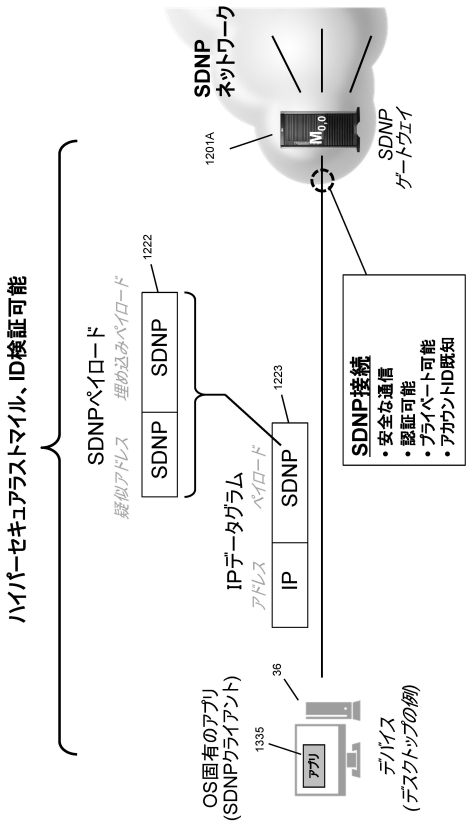
【図１５】



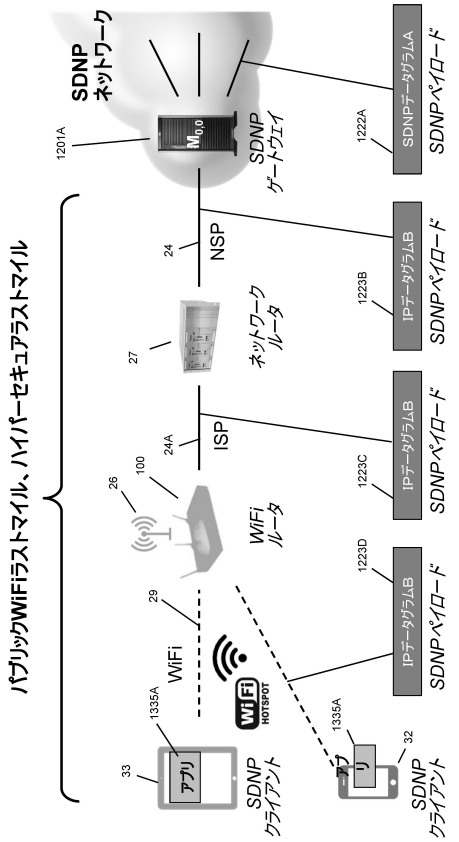
【図１６】



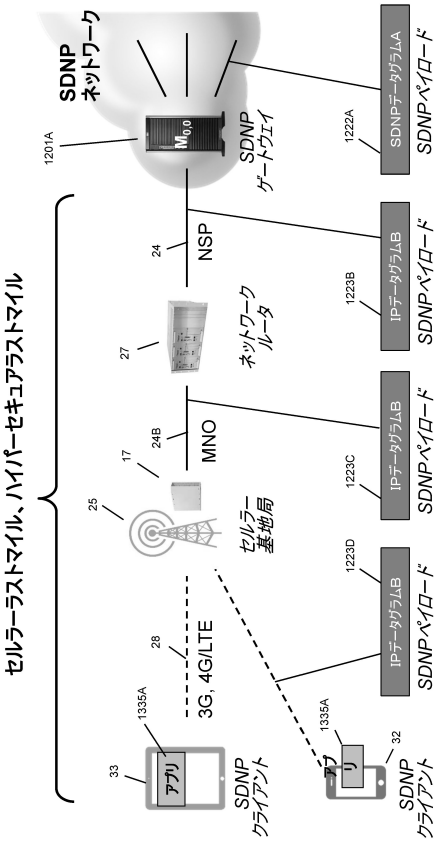
【図１７】



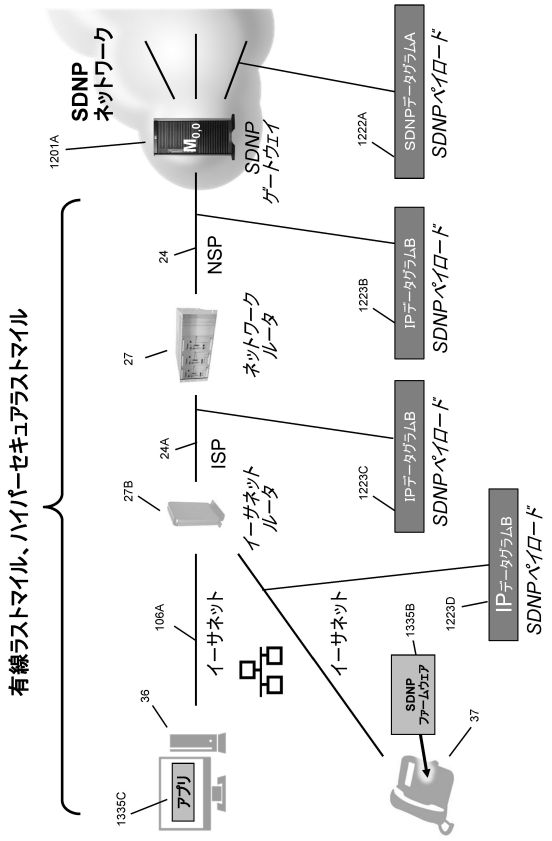
【図１８】



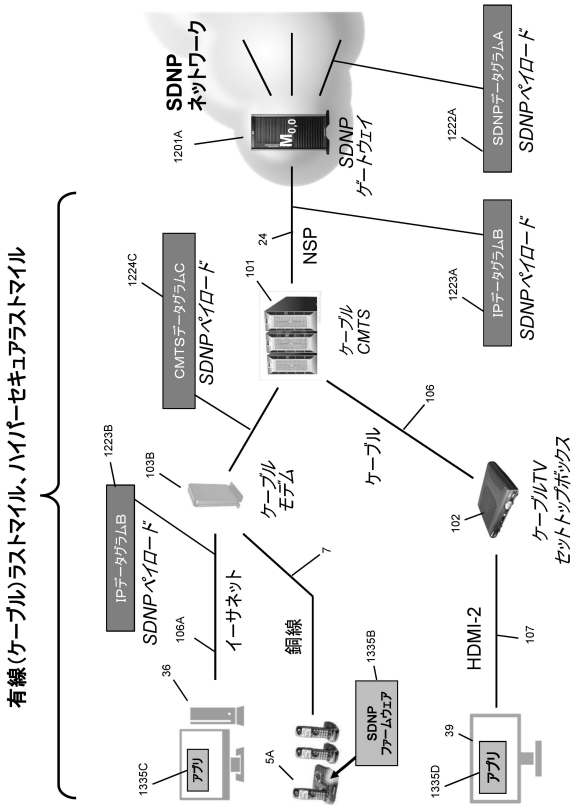
【図１９】



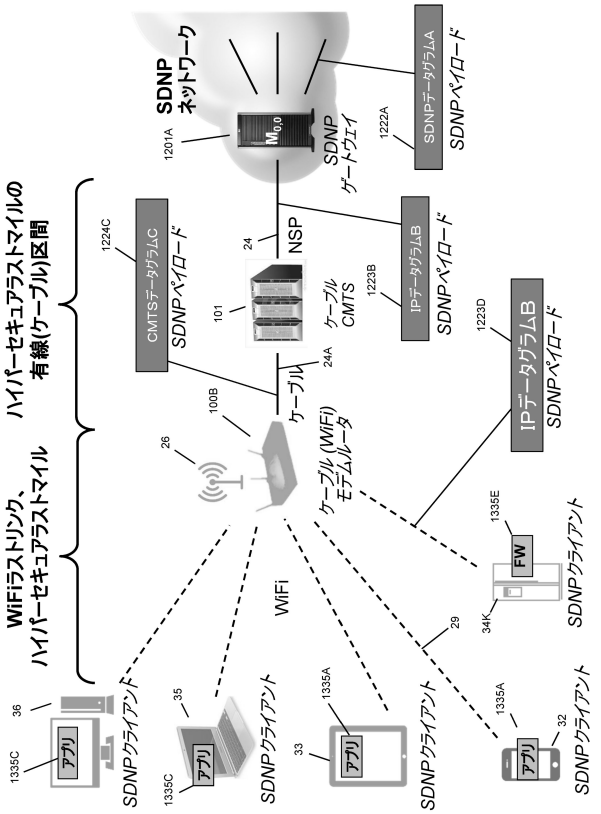
【図２０】



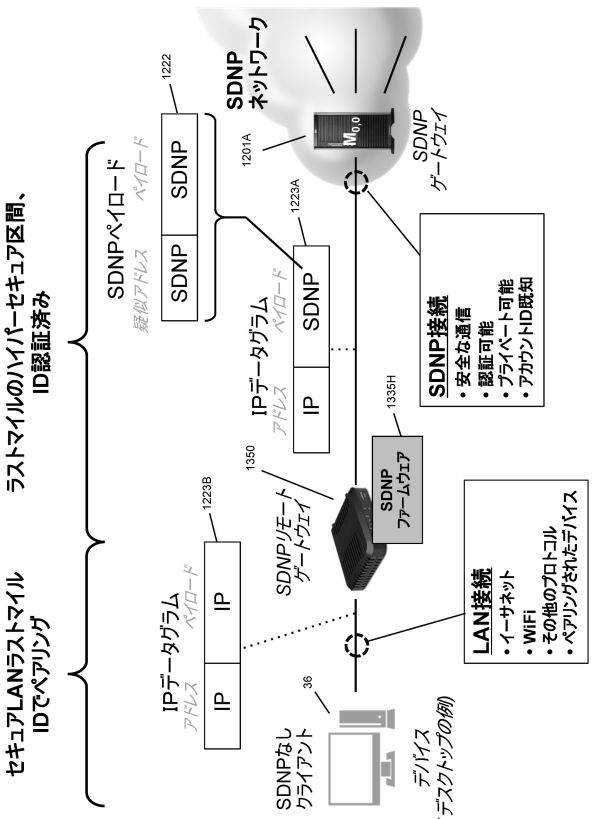
【図２１】



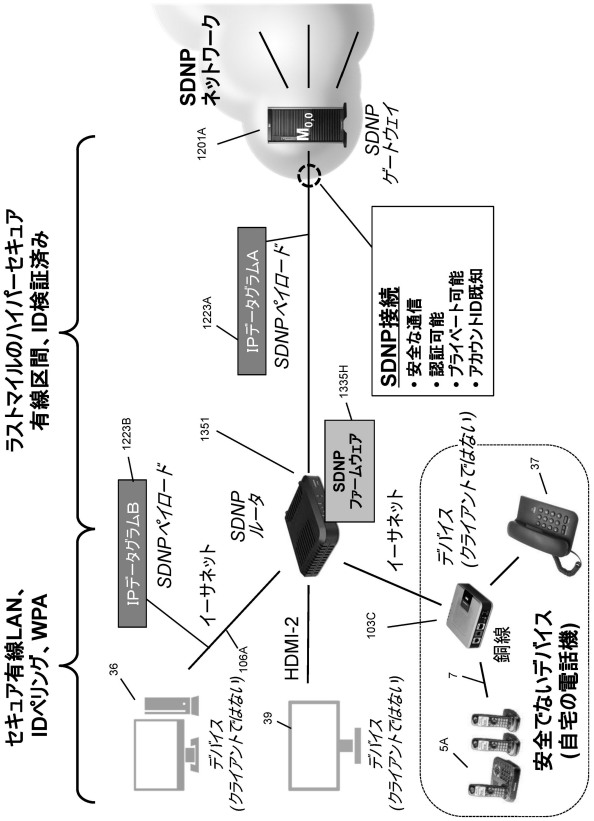
【図２２】



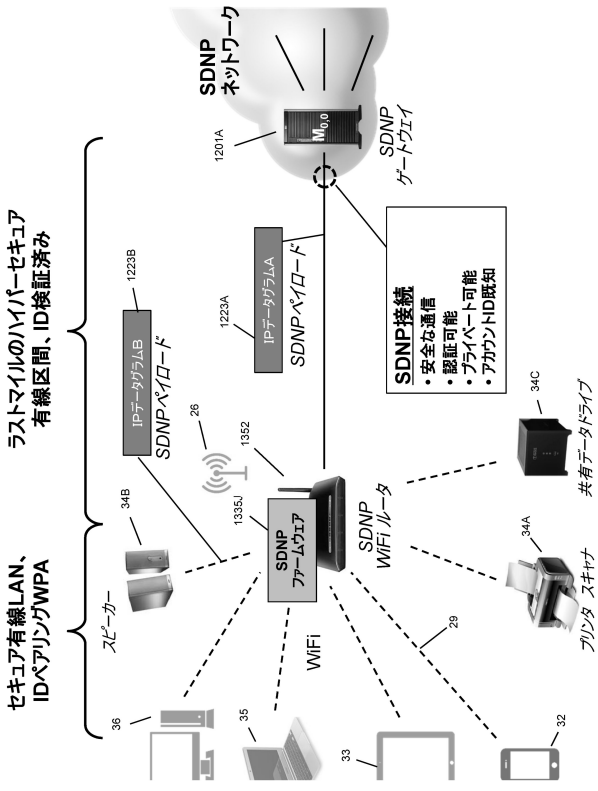
【図２３】



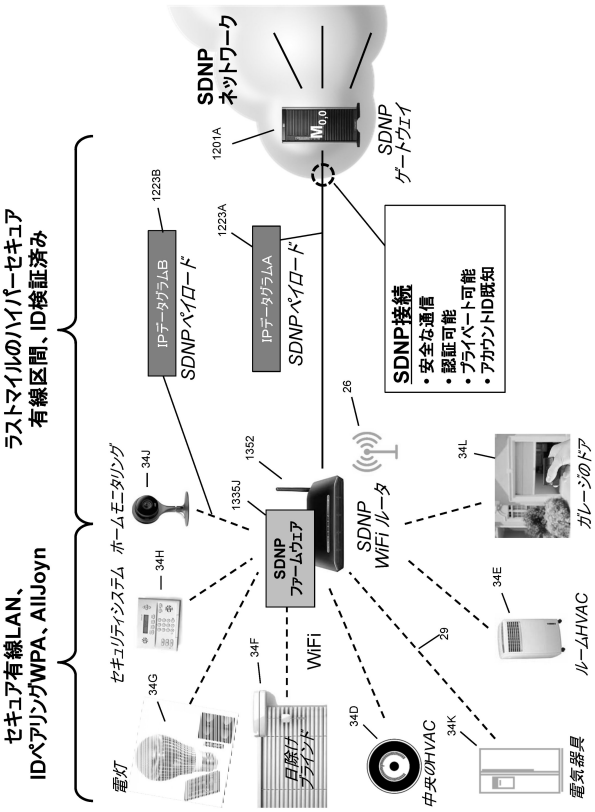
【図２４】



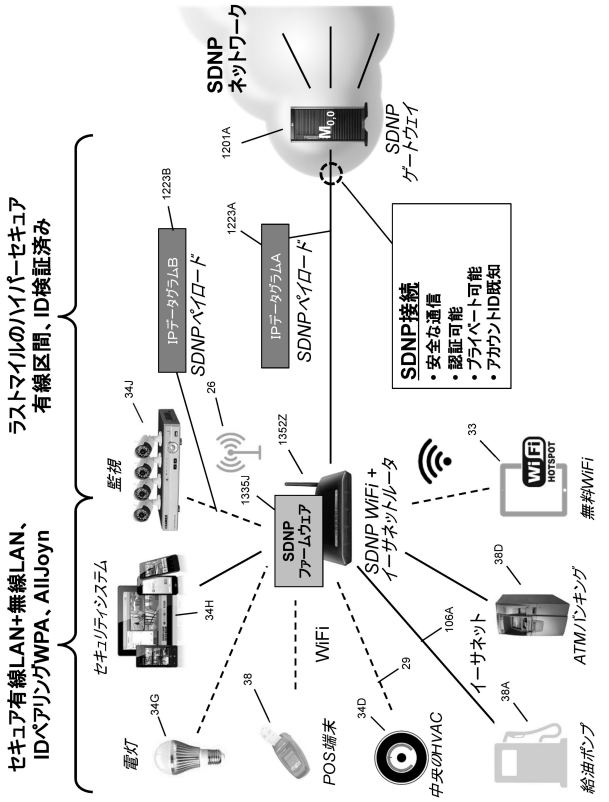
【図２５】



【図２６】

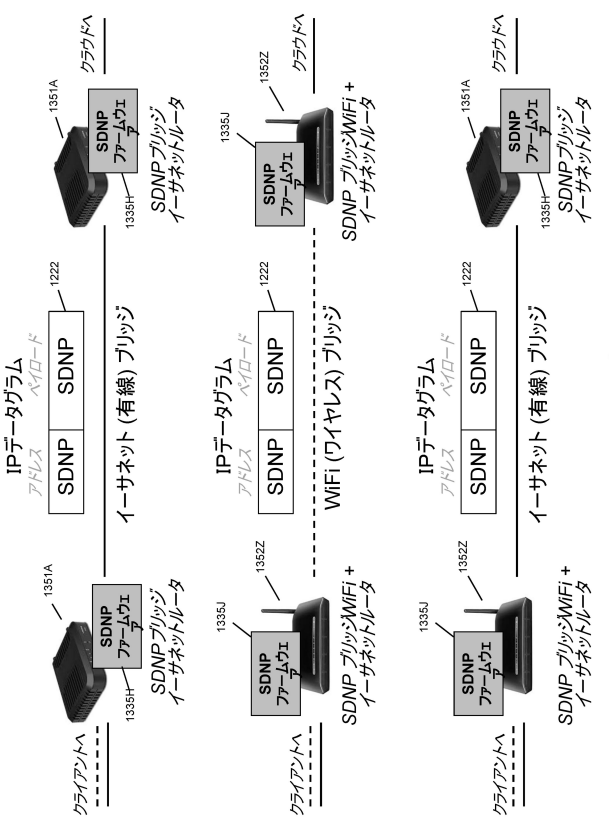


【図２７】



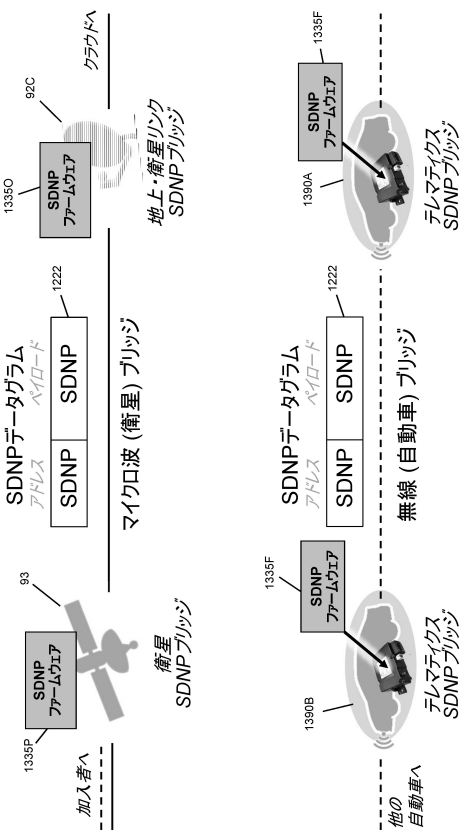
【図２８】

【図２９Ａ】

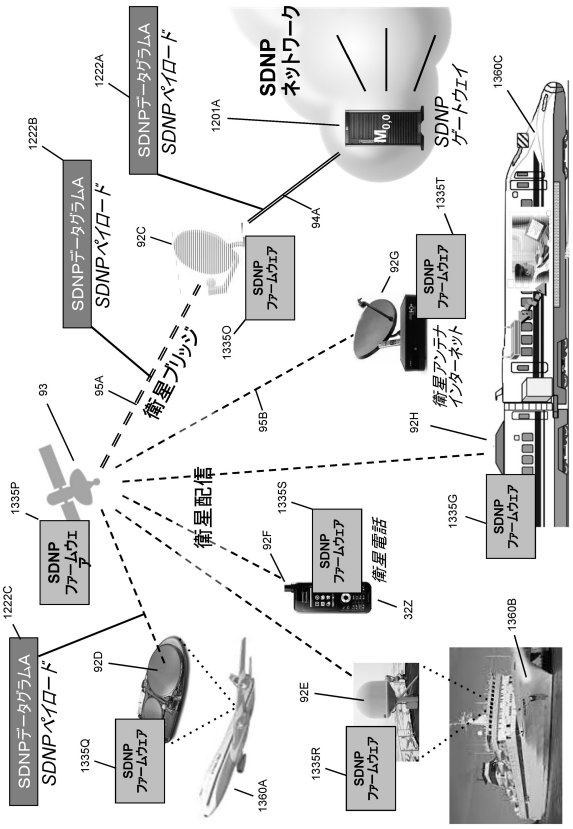


【図２９Ｂ】

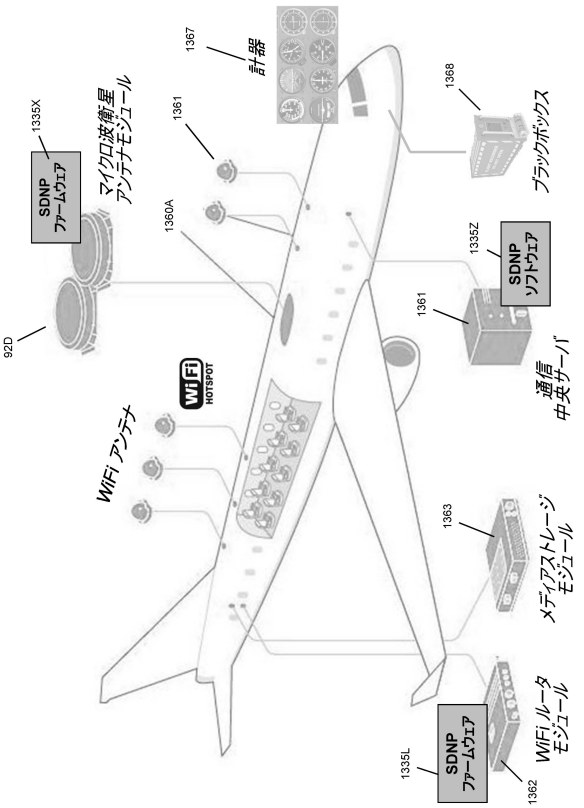
【図２９Ｃ】



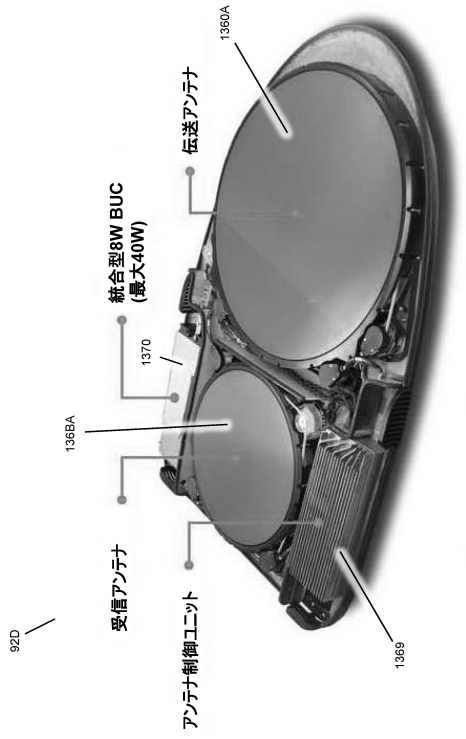
【図３０】



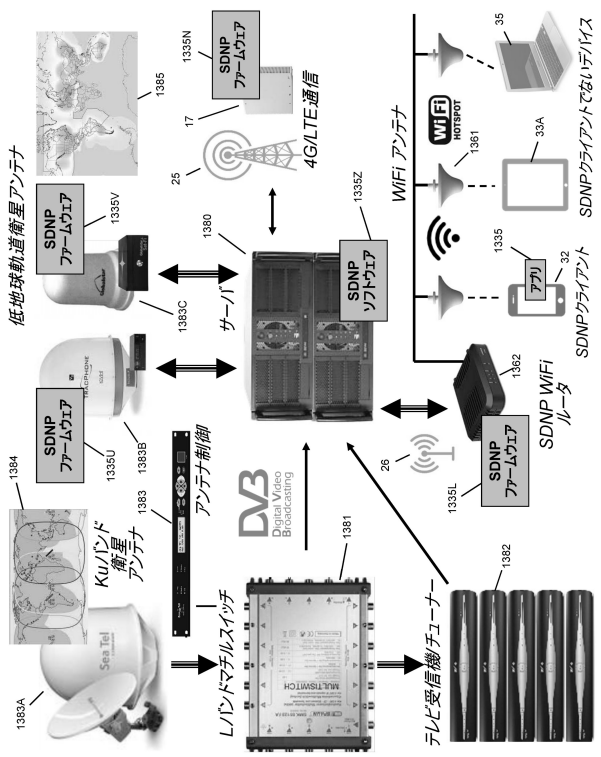
【図３１Ａ】



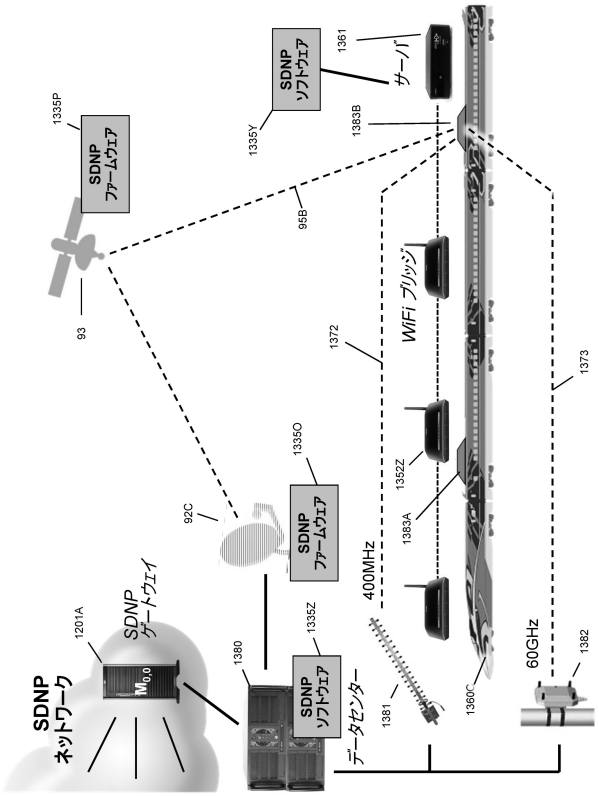
【図３１Ｂ】



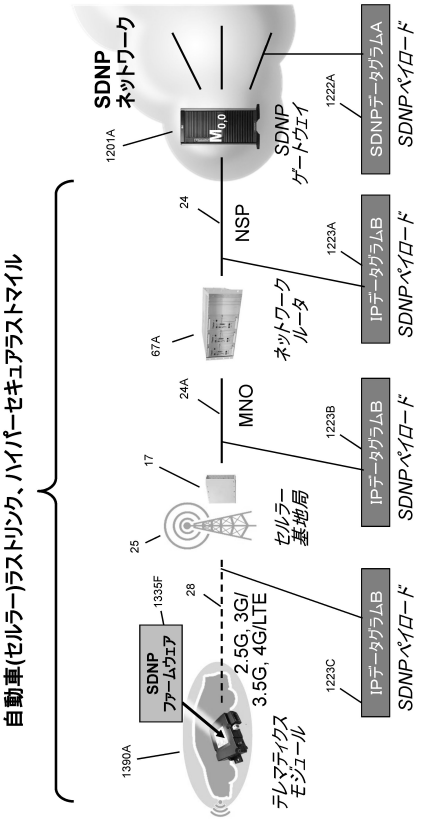
【図３２】



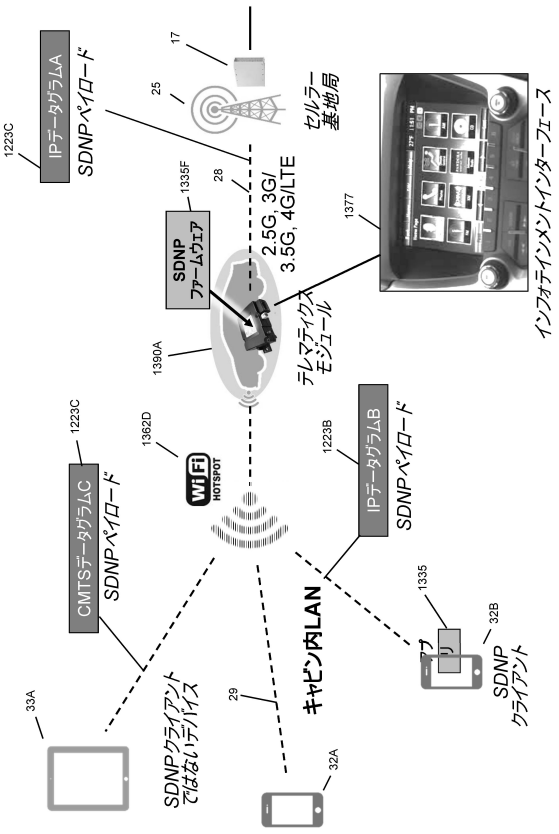
【図３３】



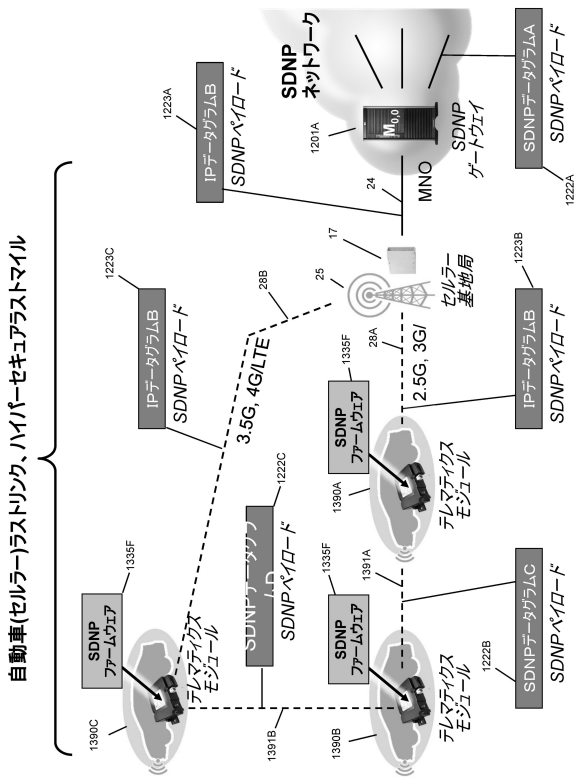
【図３４】



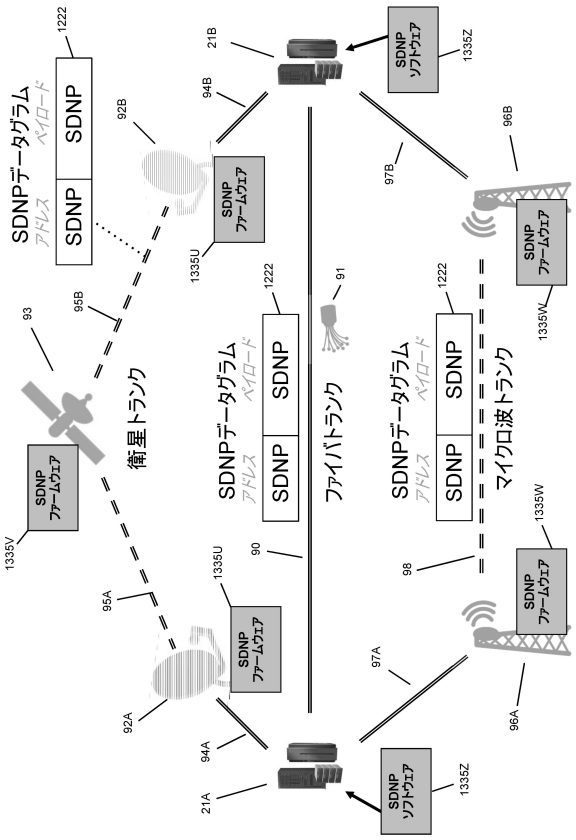
【図３５】



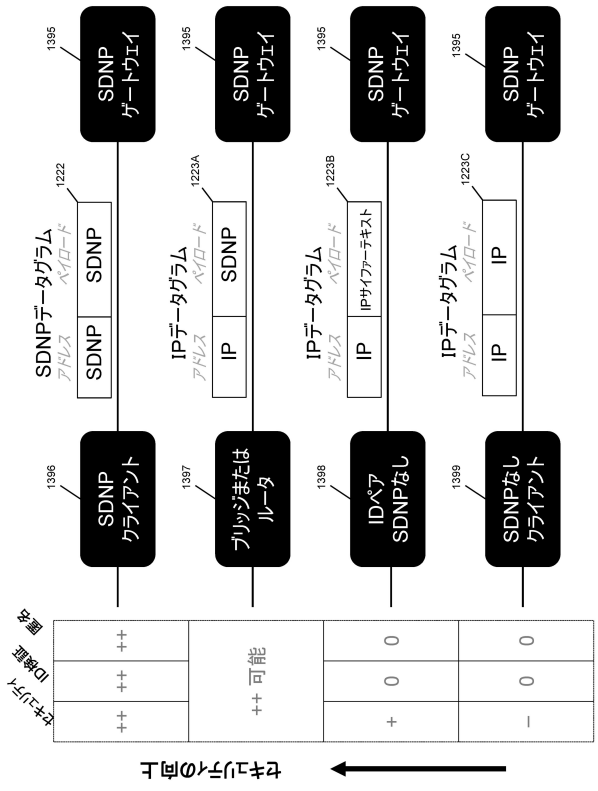
【図３６】



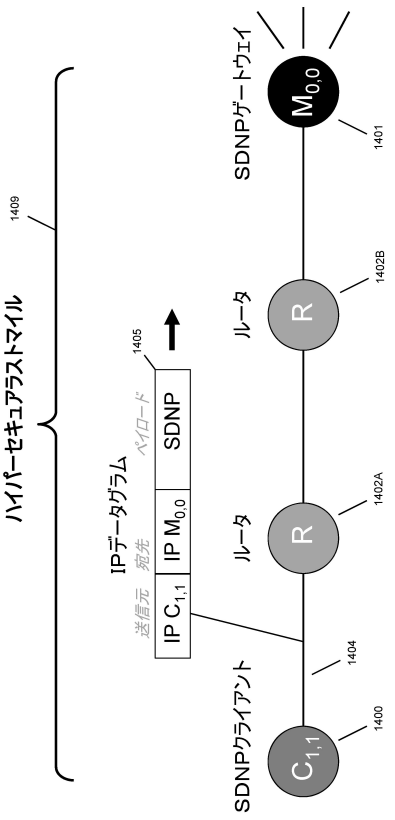
【図３７】



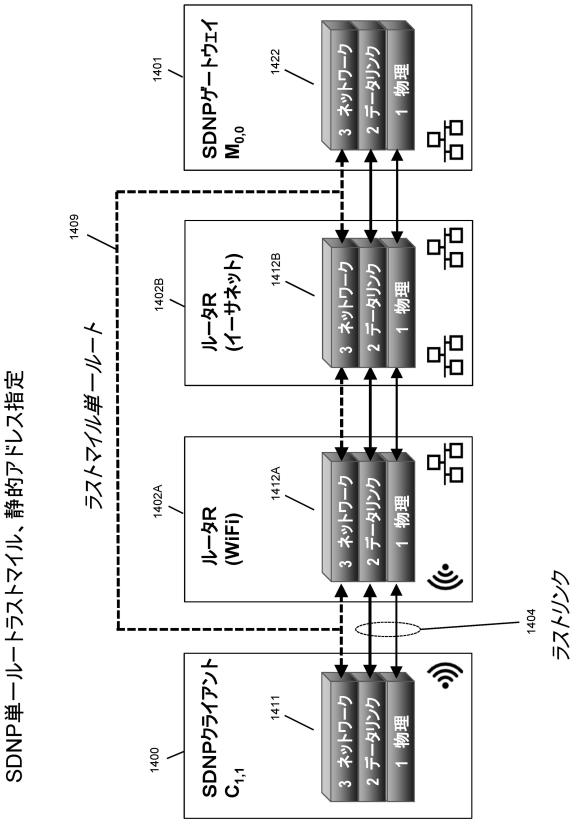
【図３８】



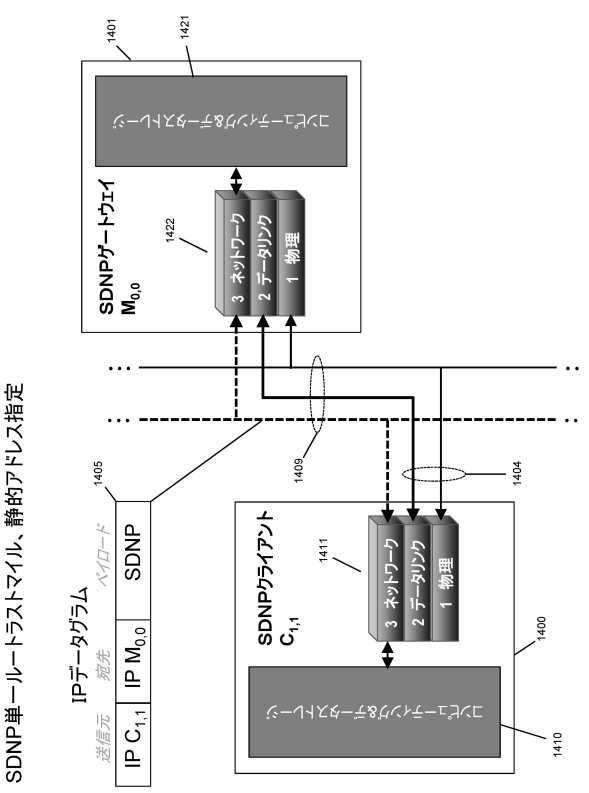
【図３９】



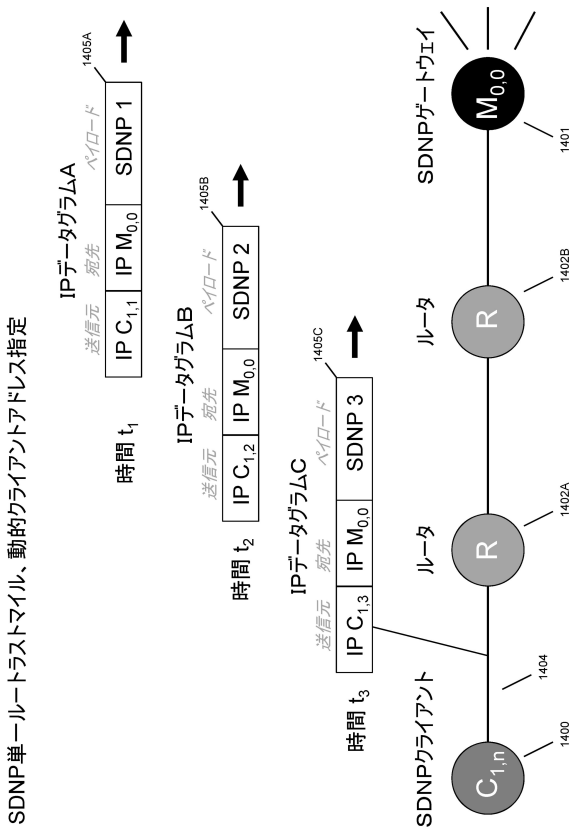
【図４０Ａ】



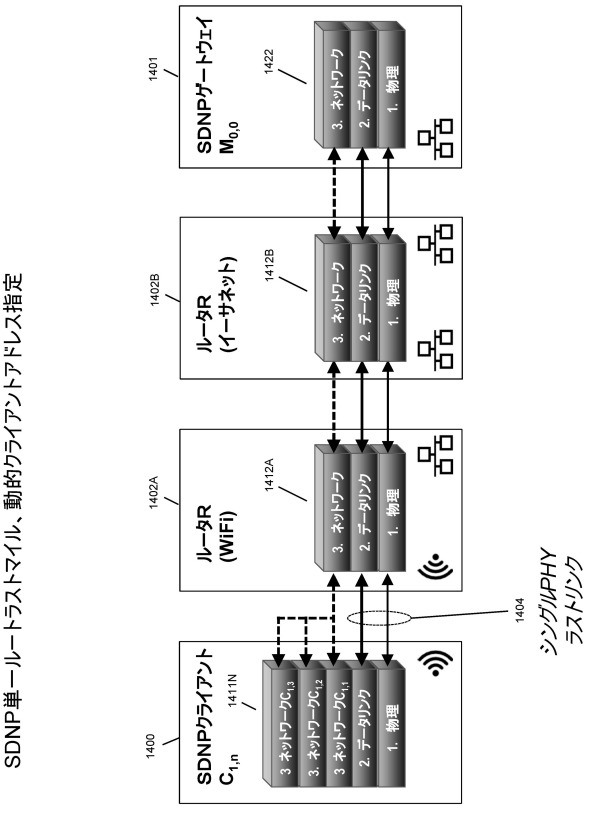
【図４０Ｂ】



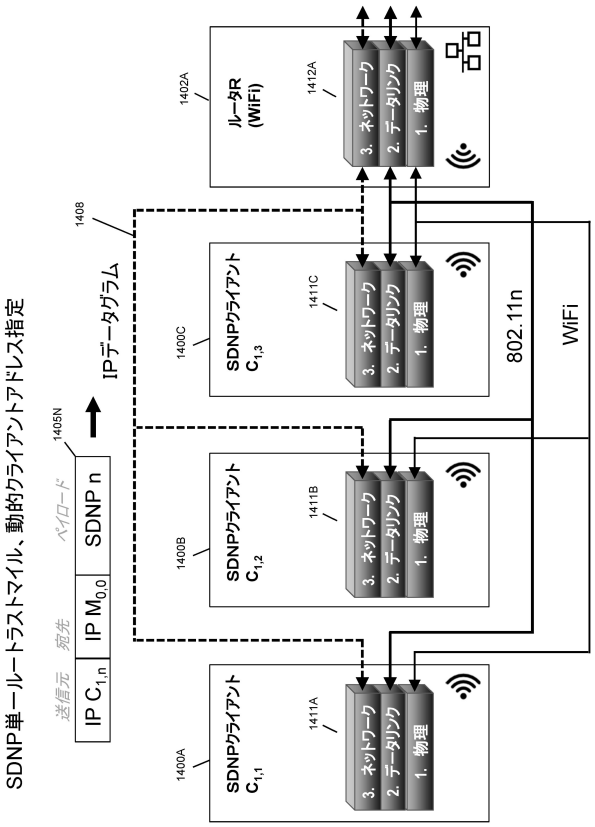
【図４１】



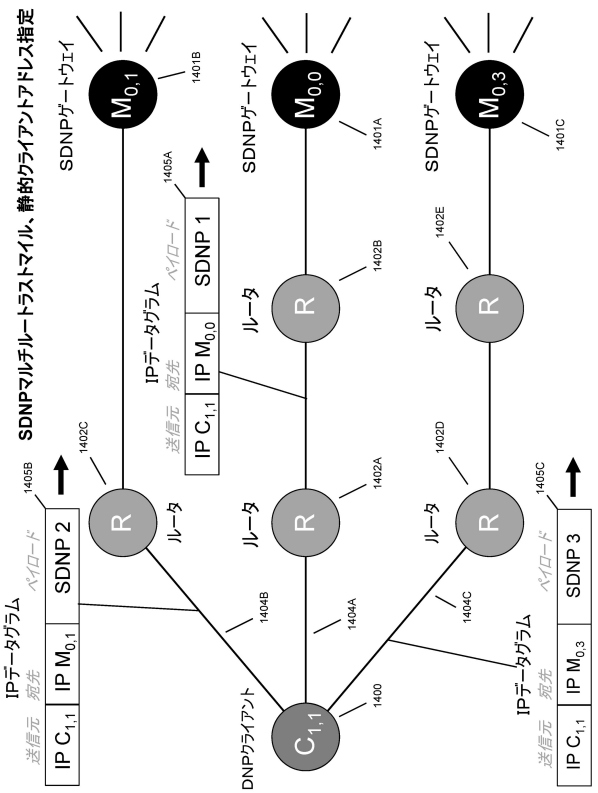
【図４２Ａ】



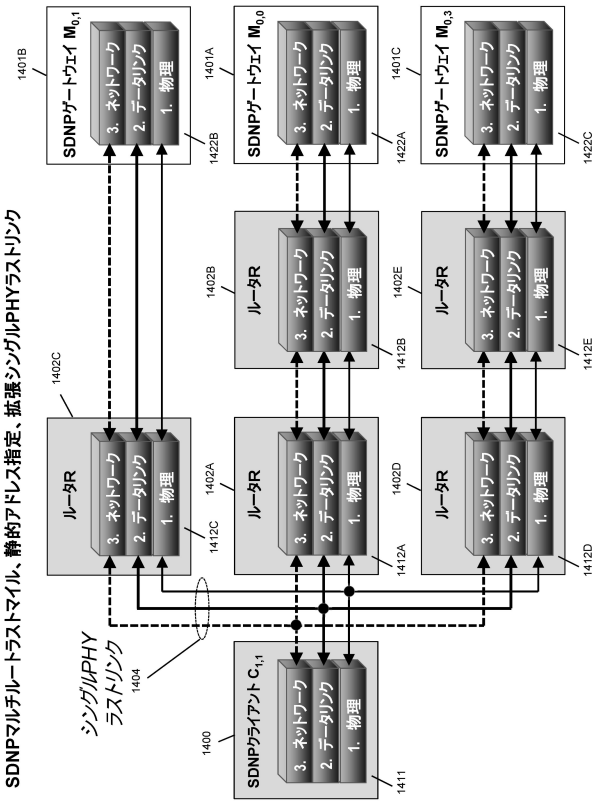
【図４２Ｂ】



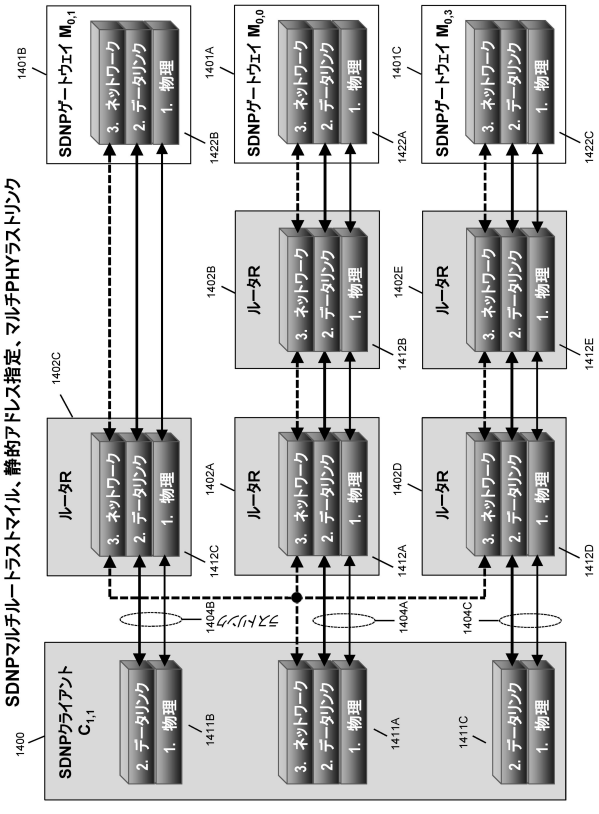
【図４３】



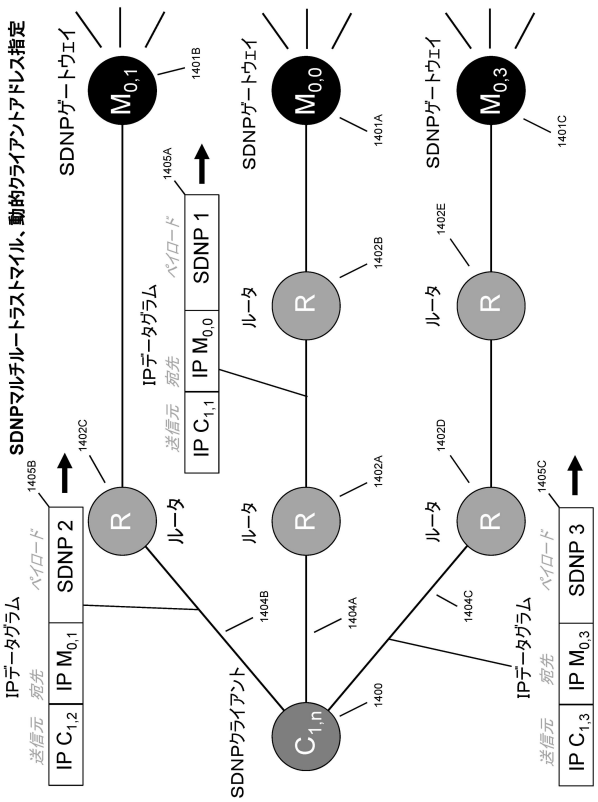
【図４４Ａ】



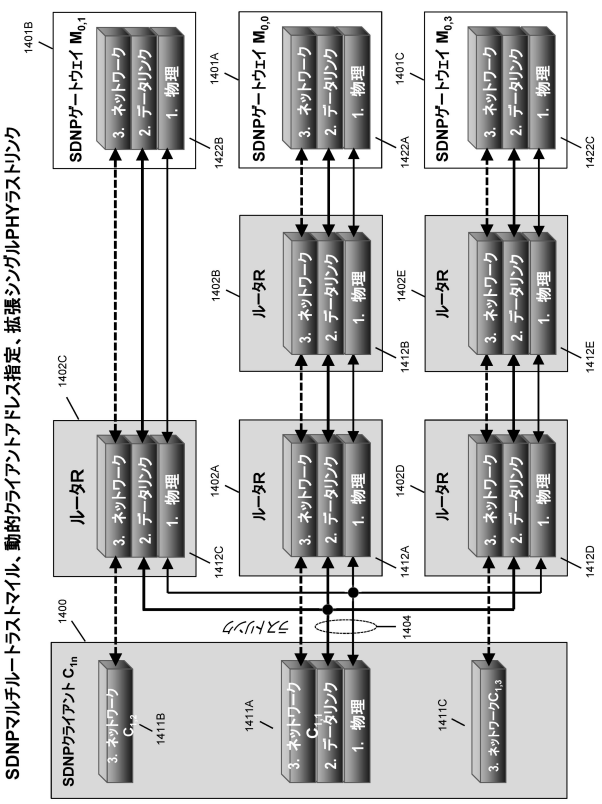
【図４４Ｂ】



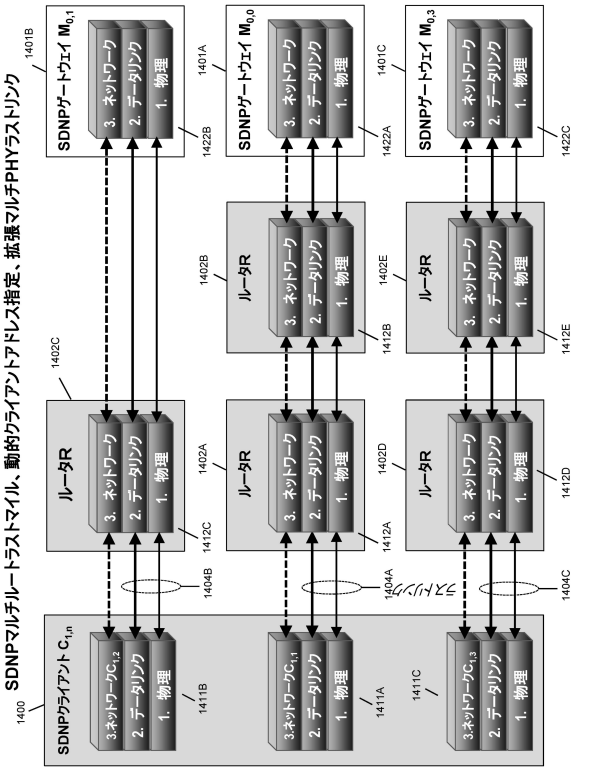
【図４５】



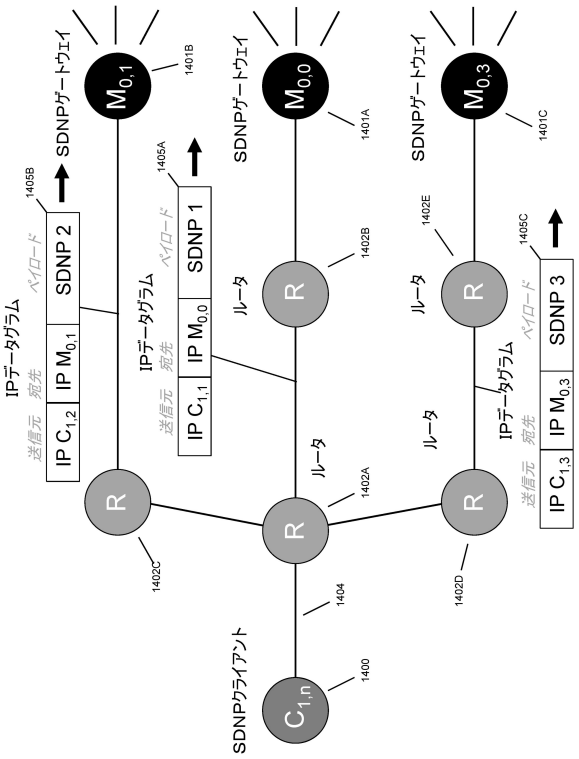
【図４６Ａ】



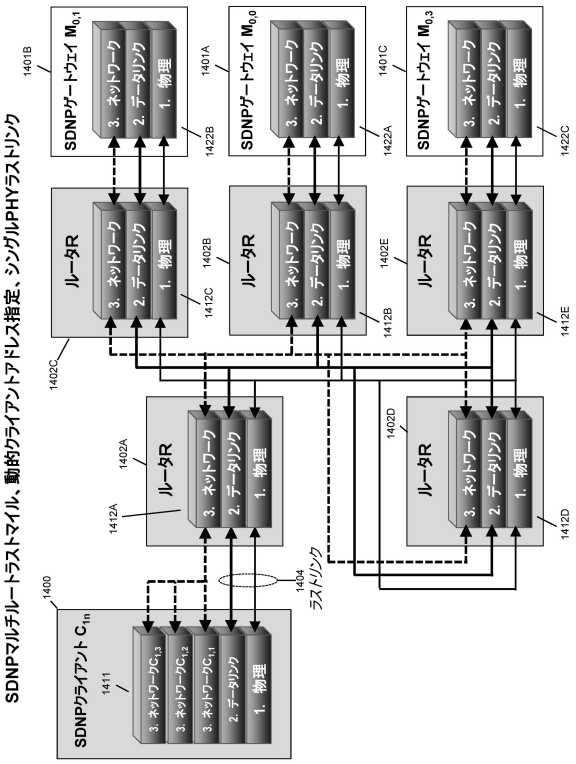
【図４６Ｂ】



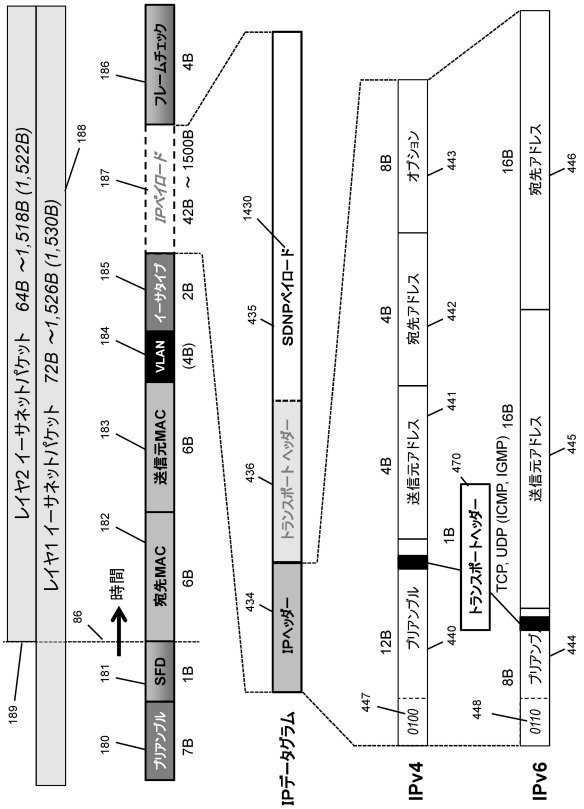
【図４７】



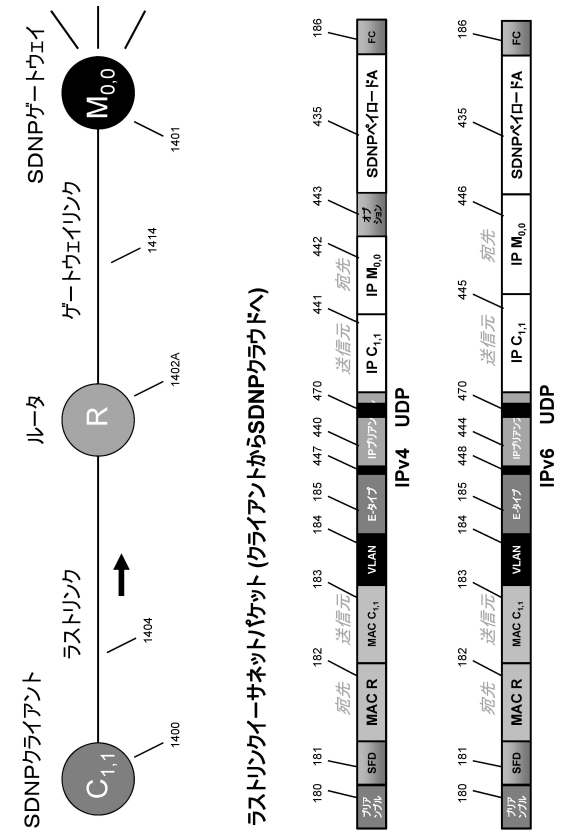
【図４８】



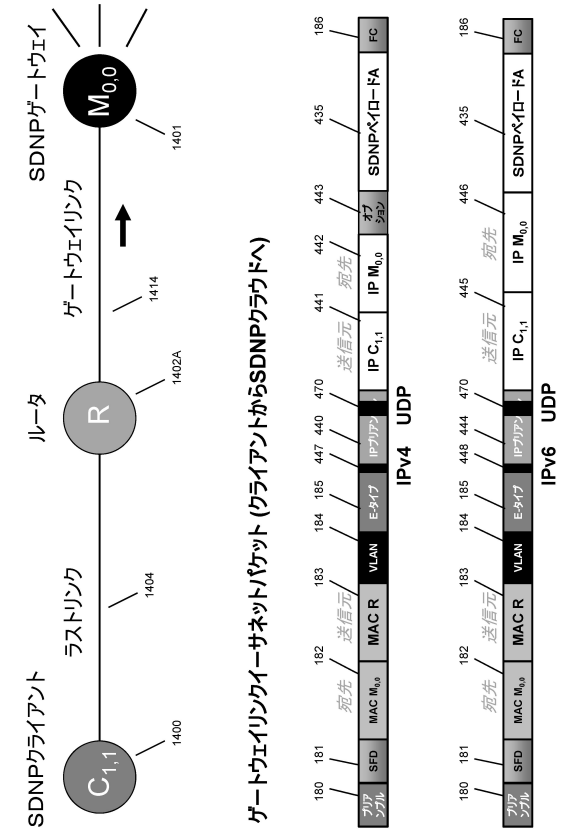
【図４９】



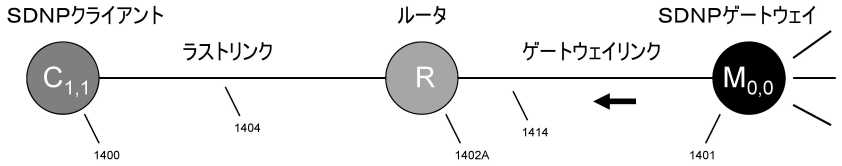
【図５０Ａ】



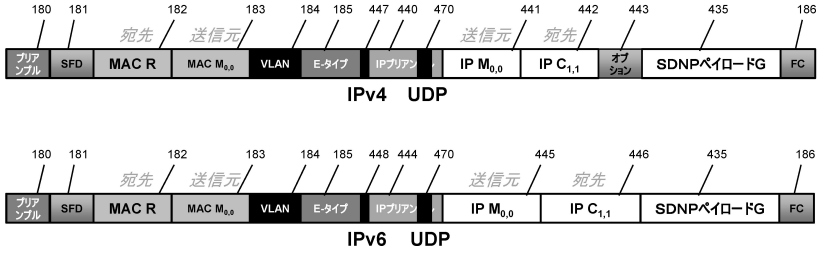
【図５０Ｂ】



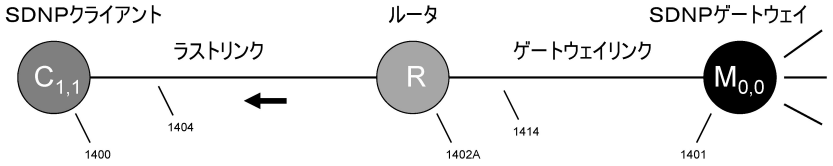
【図５０Ｃ】



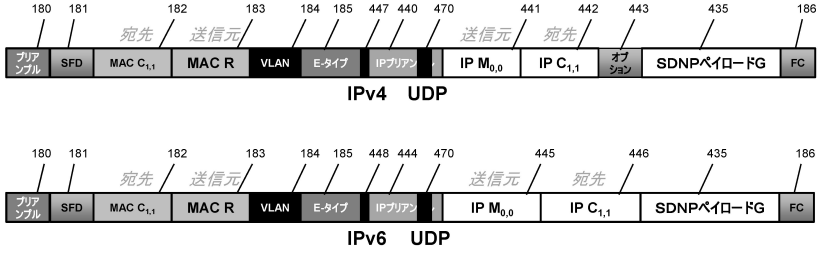
ゲートウェイリンクイーサネットパケット (SDNPクラウドからクライアントへ)



【図５０Ｄ】

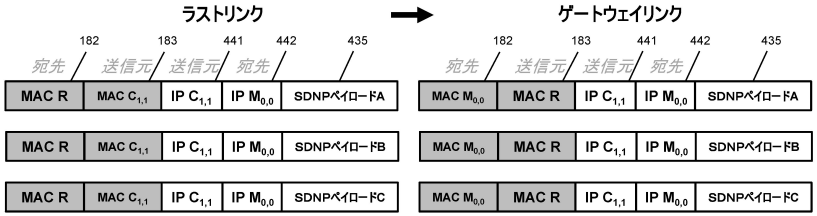


ラストリンクイーサネットパケット (SDNPクラウドからクライアントへ)

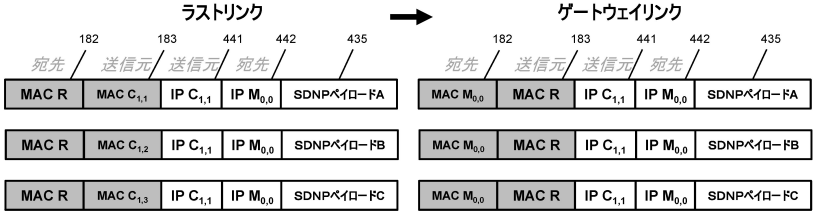


【図５１Ａ】

SDNP単一ルートラストマイル、静的クライアントアドレス指定、シングルPHYラストリンク

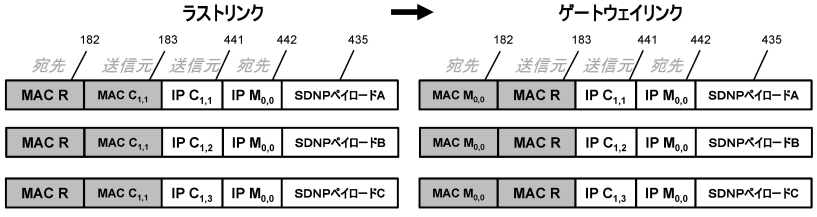


SDNP単一ルートラストマイル、静的クライアントアドレス指定、マルチPHYラストリンク

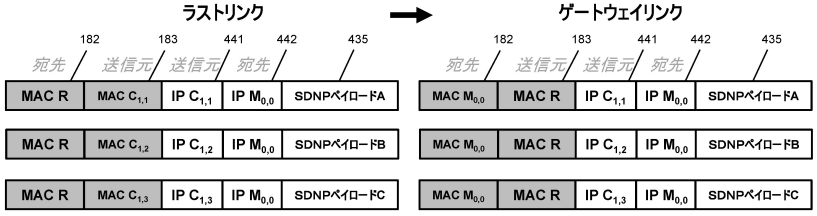


【図５１Ｂ】

SDNP単一ルートラストマイル、動的クライアントアドレス指定、シングルPHYラストリンク



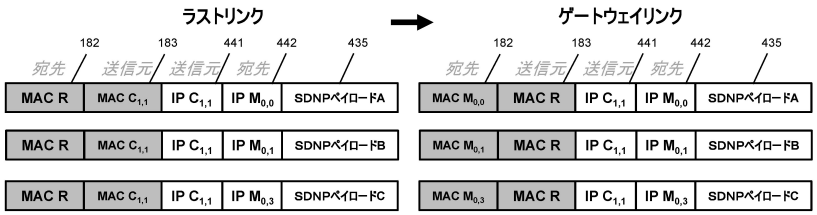
SDNP単一ルートラストマイル、動的クライアントアドレス指定、マルチPHYラストリンク



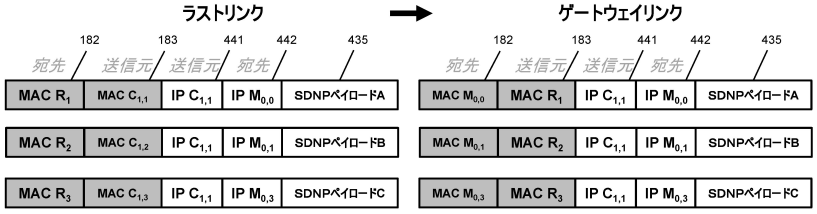
10 20 30 40 50

【図５１Ｃ】

SDNP単一ルートラストマイル、静的クライアントアドレス指定、シングルPHYラストリンク

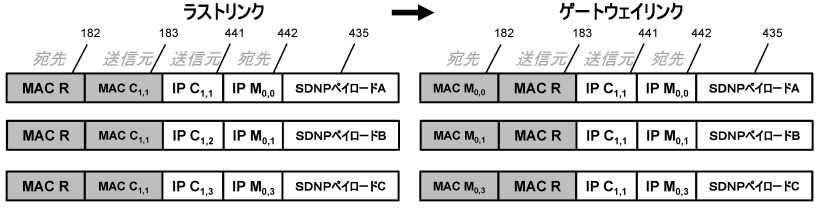


SDNPマルチルートラストマイル、静的クライアントアドレス指定、マルチPHYラストリンク

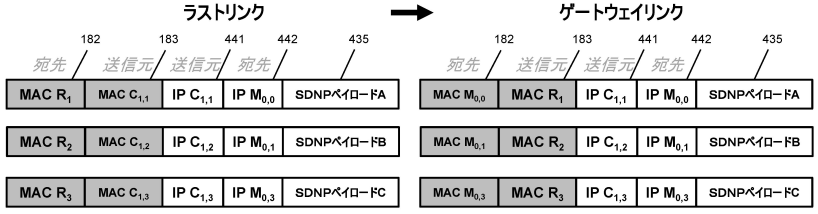


【図５１Ｄ】

SDNPマルチルートラストマイル、動的クライアントアドレス指定、シングルPHYラストリンク



SDNPマルチルートラストマイル、動的クライアントアドレス指定、マルチPHYラストリンク

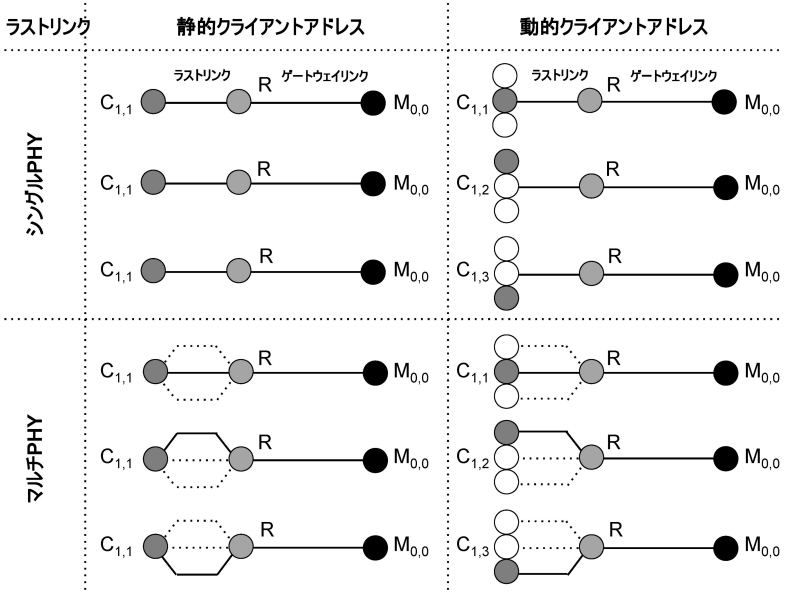


【図５２Ａ】

イーサネット経由のSDNPラストマイルルーティング

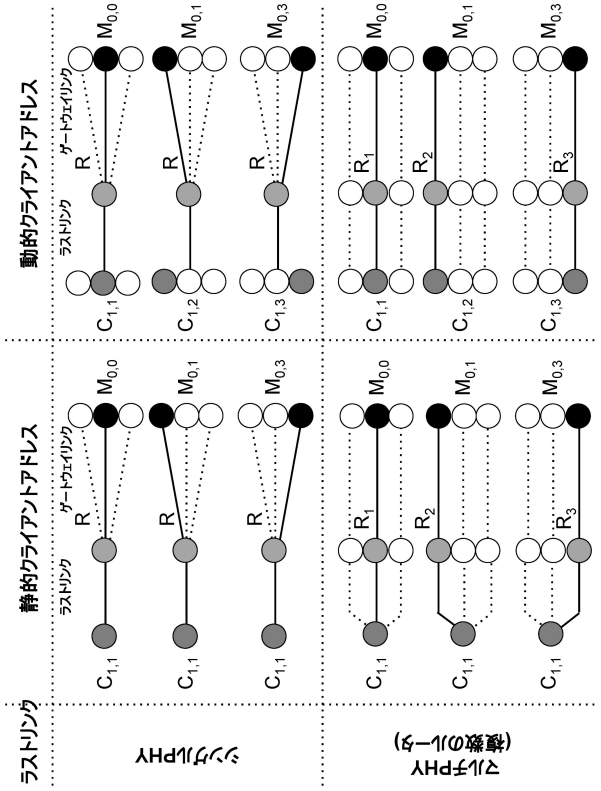
#	ルート	クライアントアドレス	ラストリンク	IP送信元	IP宛先	MACクライアント
1	複数	動的	マルチPHY	可変 $C_{1,n}$	複数 ゲートウェイ $M_{0,n}$	MAC $C_{1,n}$ ～ R_n
2	複数	動的	マルチPHY	可変 $C_{1,n}$		MAC $C_{1,n}$ ～ R
3	複数	動的	シングルPHY	可変 $C_{1,n}$		MAC $C_{1,1}$ ～ R
4	複数	静的	マルチPHY	固定 $C_{1,1}$		MAC $C_{1,n}$ ～ R_n
5	複数	静的	マルチPHY	固定 $C_{1,1}$		MAC $C_{1,n}$ ～ R
6	複数	静的	シングルPHY	固定 $C_{1,1}$		MAC $C_{1,1}$ ～ R
7	単一	動的	マルチPHY	可変 $C_{1,n}$	単一 ゲートウェイ $M_{0,0}$	MAC $C_{1,n}$ ～ R
8	単一	動的	シングルPHY	可変 $C_{1,n}$		MAC $C_{1,1}$ ～ R
9	単一	静的	マルチPHY	固定 $C_{1,1}$		MAC $C_{1,n}$ ～ R
10	単一	静的	シングルPHY	固定 $C_{1,1}$		MAC $C_{1,1}$ ～ R

【図５２Ｂ】

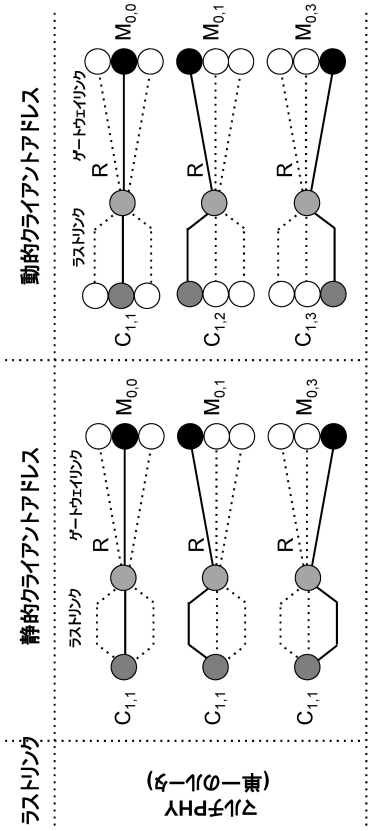


10 20 30 40 50

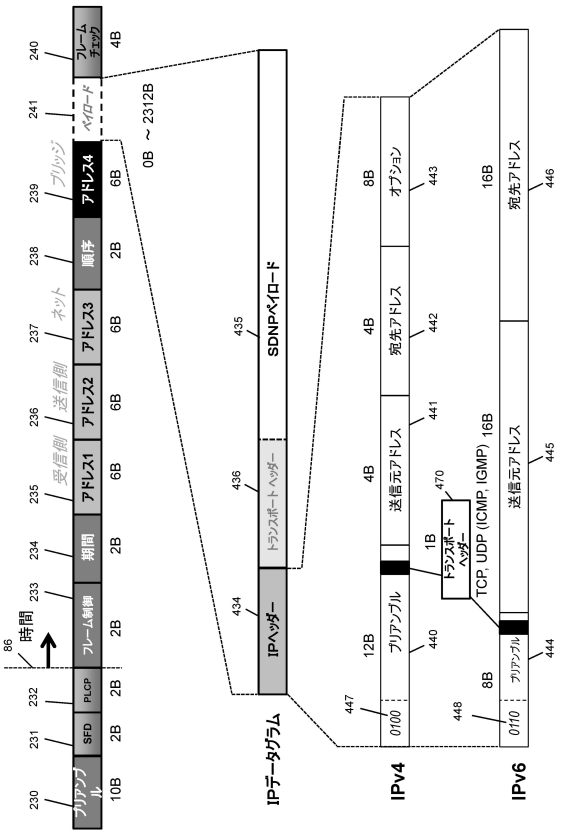
【図５２Ｃ】



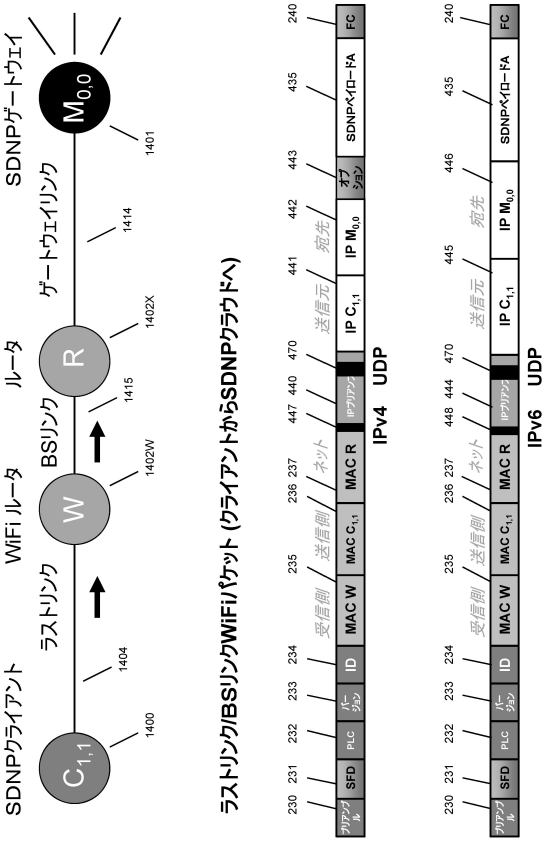
【図５２Ｄ】



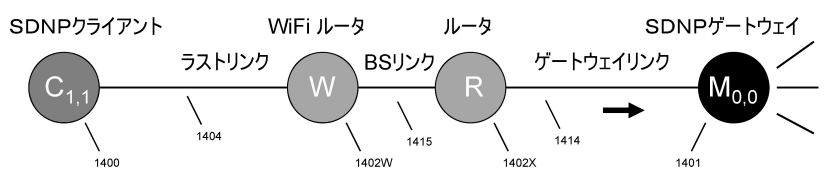
【図５３】



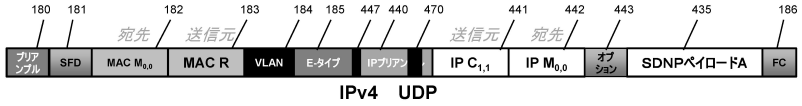
【図５４Ａ】



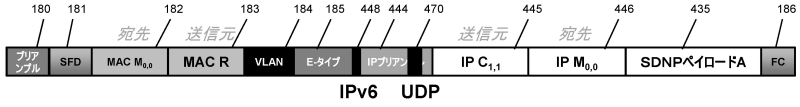
【図５４Ｂ】



ゲートウェイリンクイーサネットパケット (クライアントからSDNPクラウドへ)

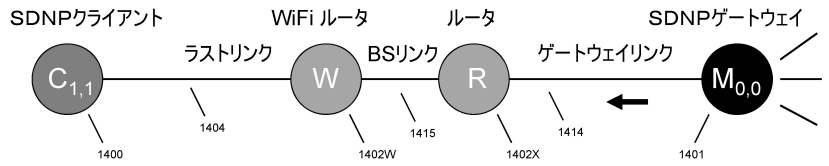


IPv4 UDP

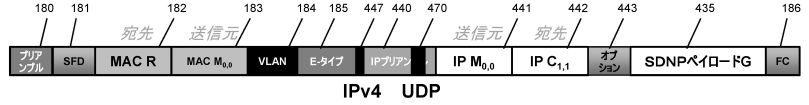


IPv6 UDP

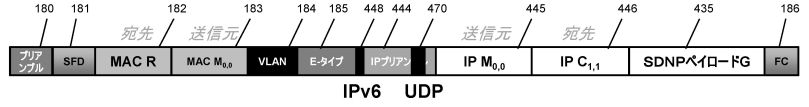
【図５４Ｃ】



ゲートウェイリンクイーサネットパケット (SDNPクラウドからクライアントへ)

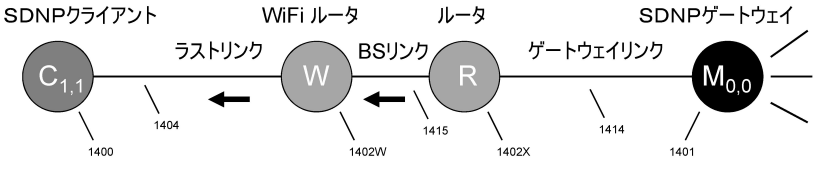


IPv4 UDP

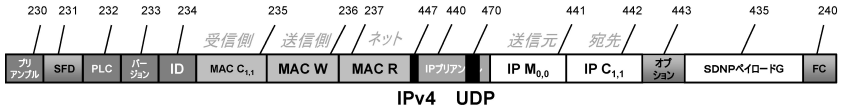


IPv6 UDP

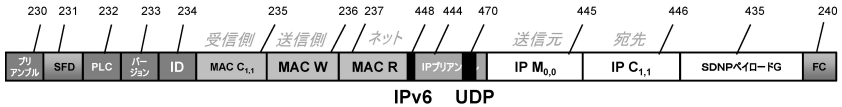
【図５４Ｄ】



BSリンク/ラストリンクWiFiパケット (SDNPクラウドからクライアントへ)

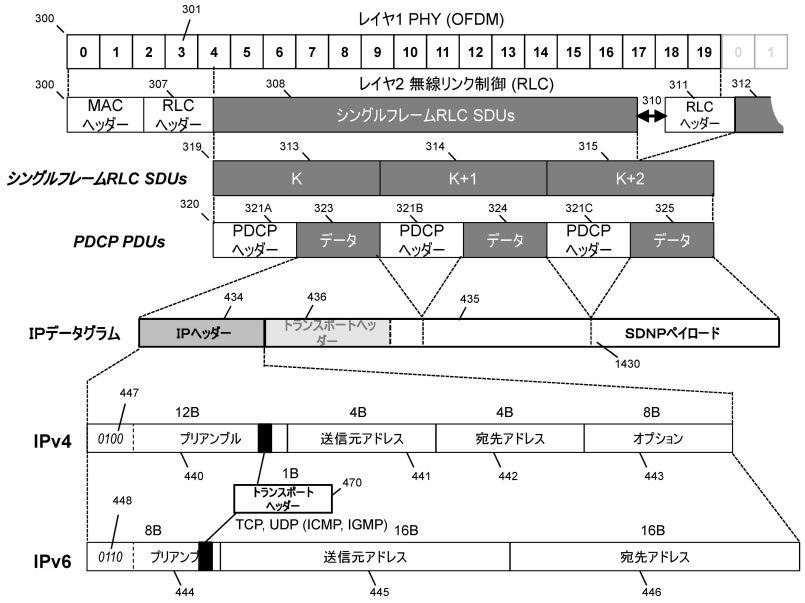


IPv4 UDP

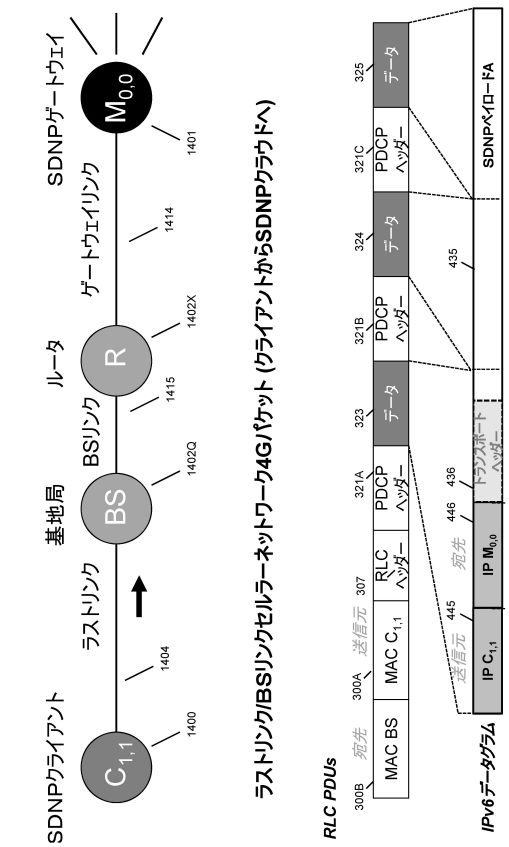


IPv6 UDP

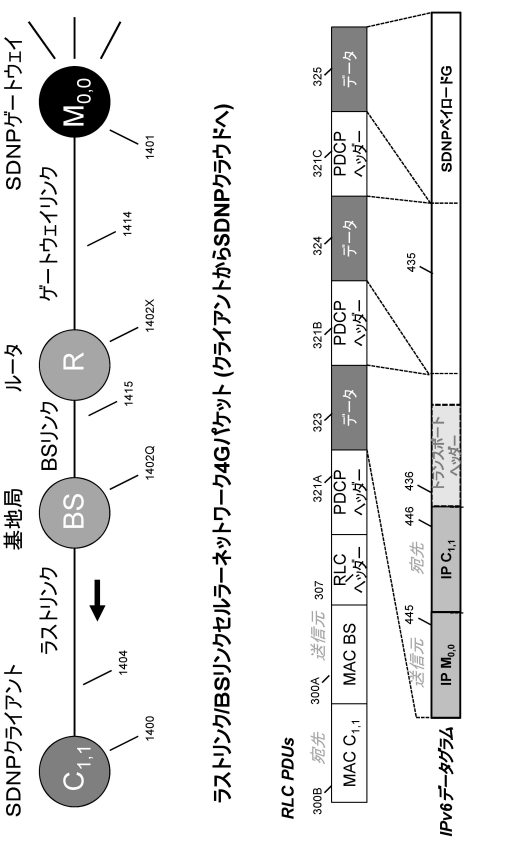
【図５５】



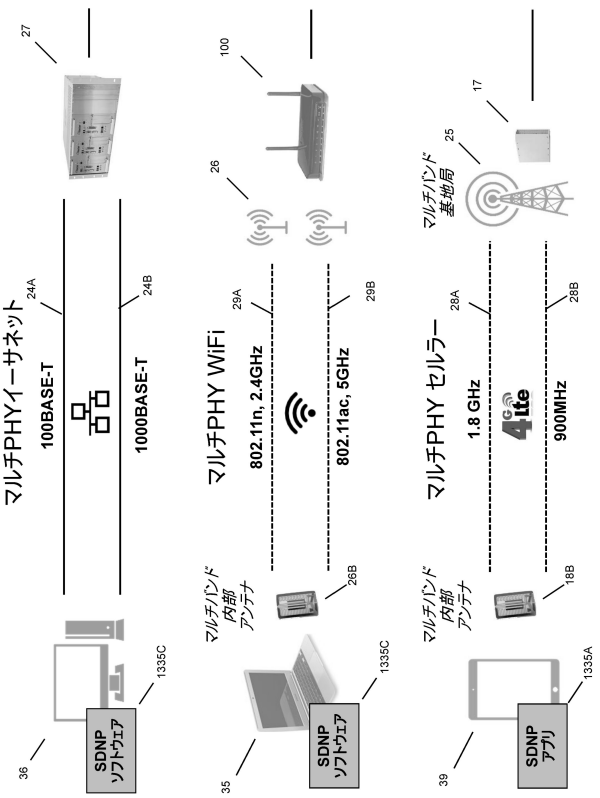
【図５６Ａ】



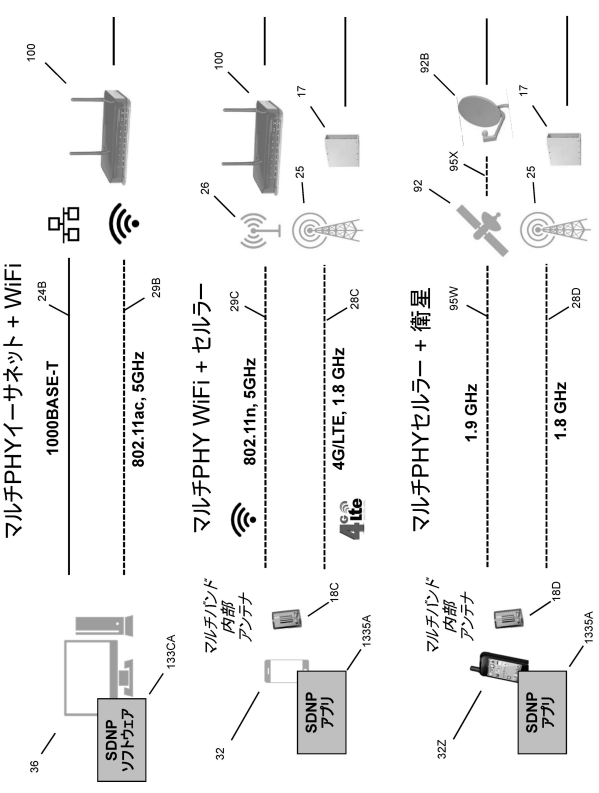
【図５６Ｂ】



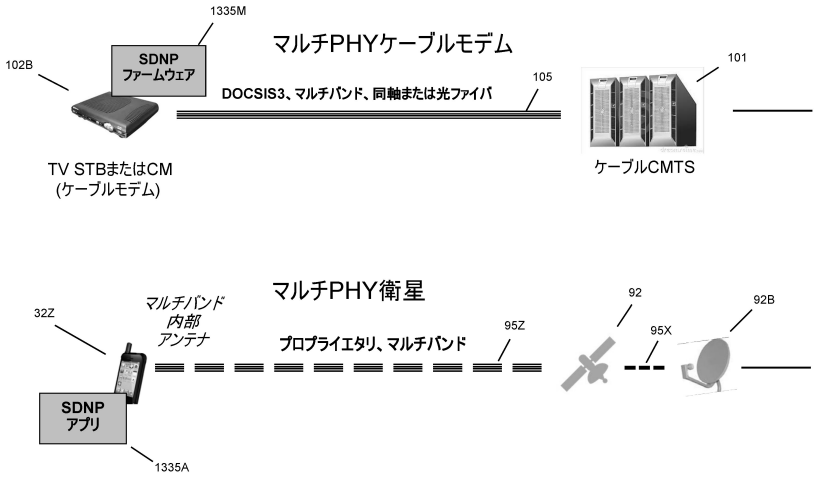
【図５７Ａ】



【図５７Ｂ】

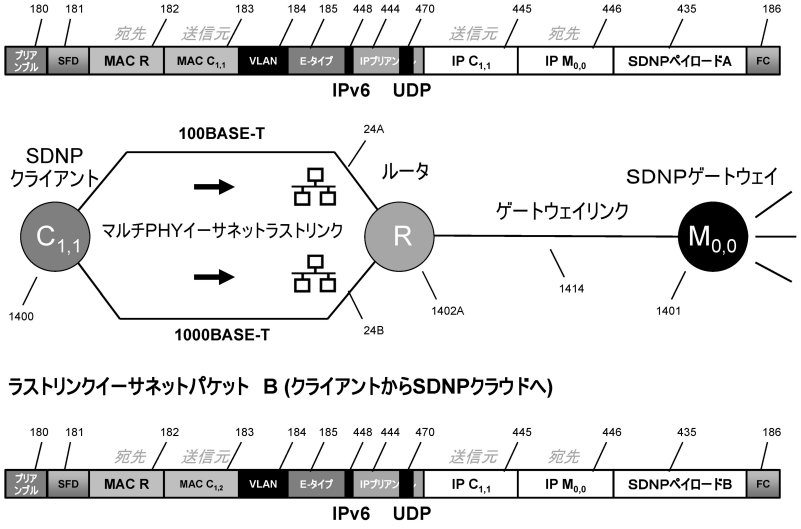


【図57C】



【図58】

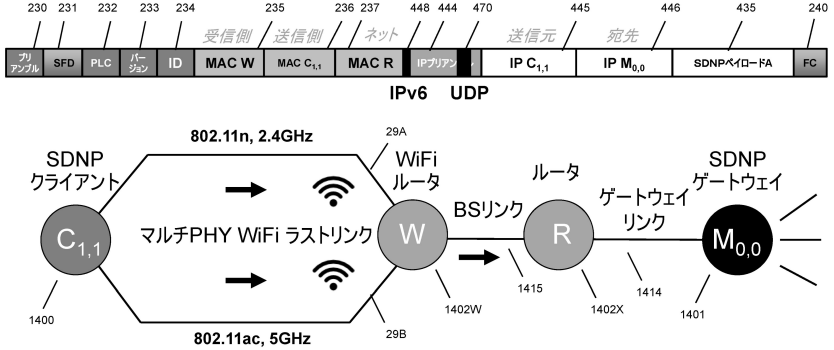
ラストリンクイーサネットパケット A (クライアントからSDNPクラウドへ)



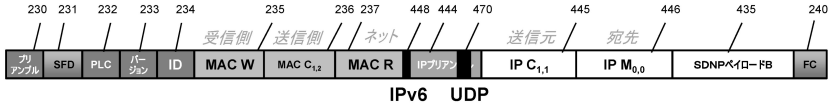
ラストリンクイーサネットパケット B (クライアントからSDNPクラウドへ)

【図59】

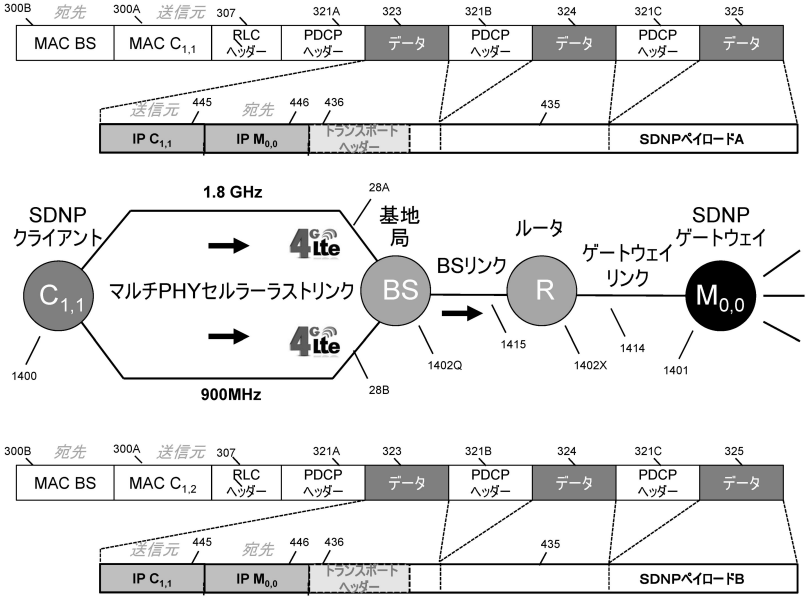
ラストリンク/BSリンクWiFiパケット A (クライアントからSDNPクラウドへ)



ラストリンク/BSリンクWiFiパケット B (クライアントからSDNPクラウドへ)



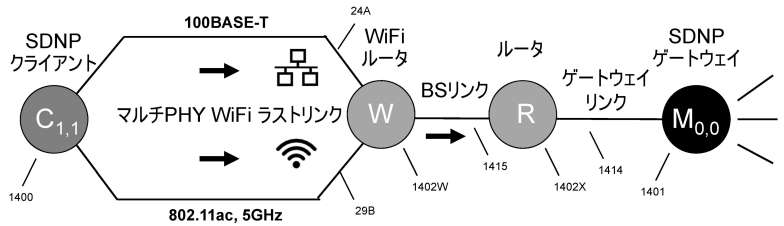
【図60】



【図６１】

ラストリンクイーサネットパケット A (クライアントからSDNPクラウドへ)



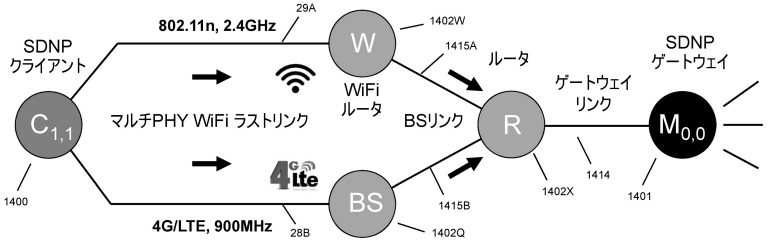


【図６２】

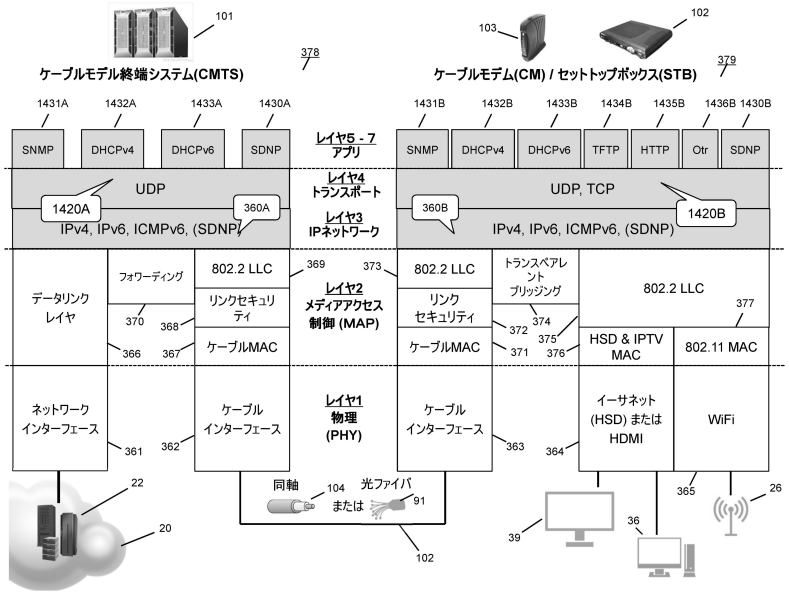
ラストリンク/BSリンクWiFiパケット A (クライアントからSDNPクラウドへ)



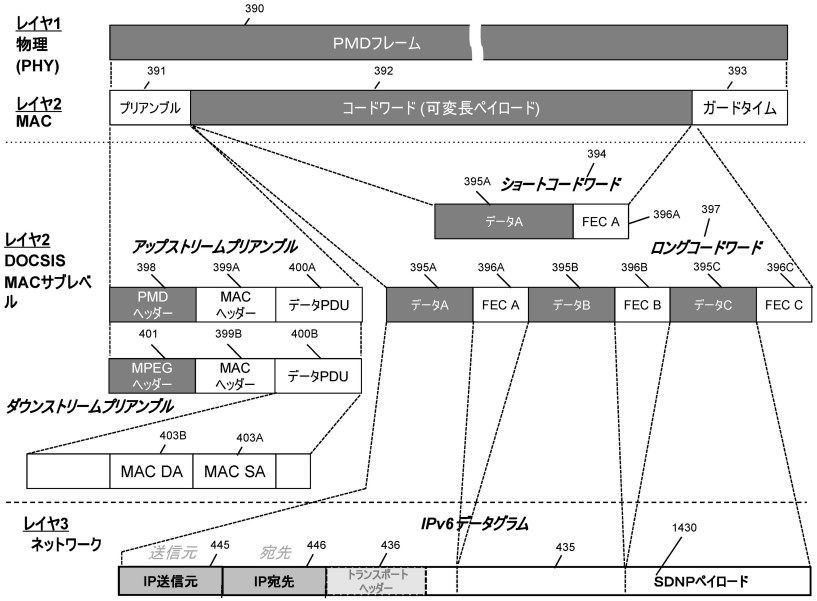
IPv6 UDP



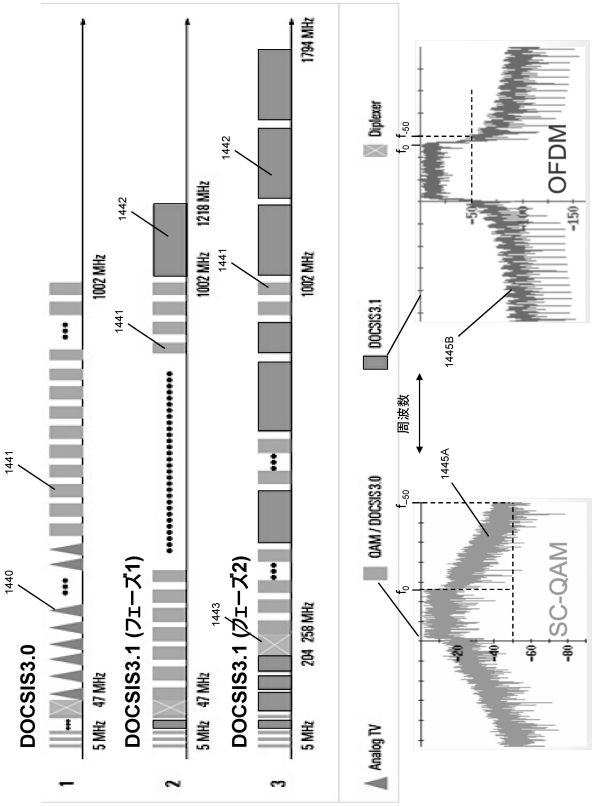
【図６３】



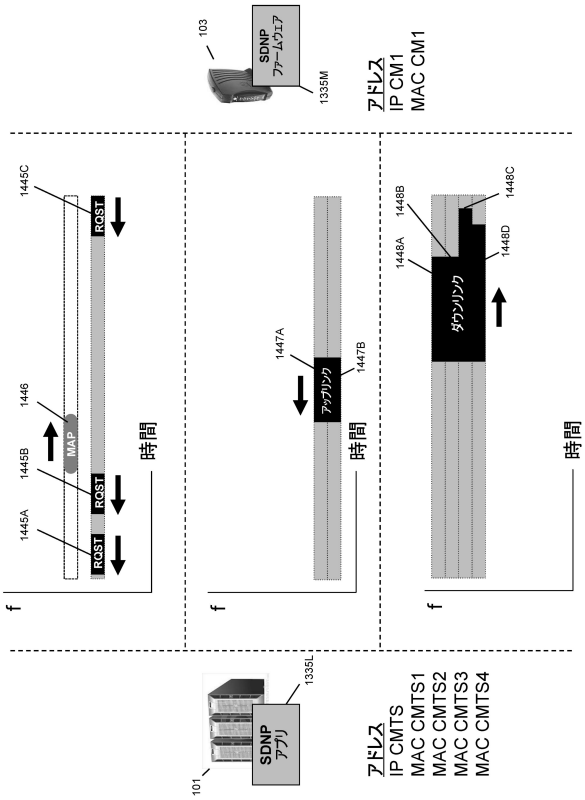
【図６４】



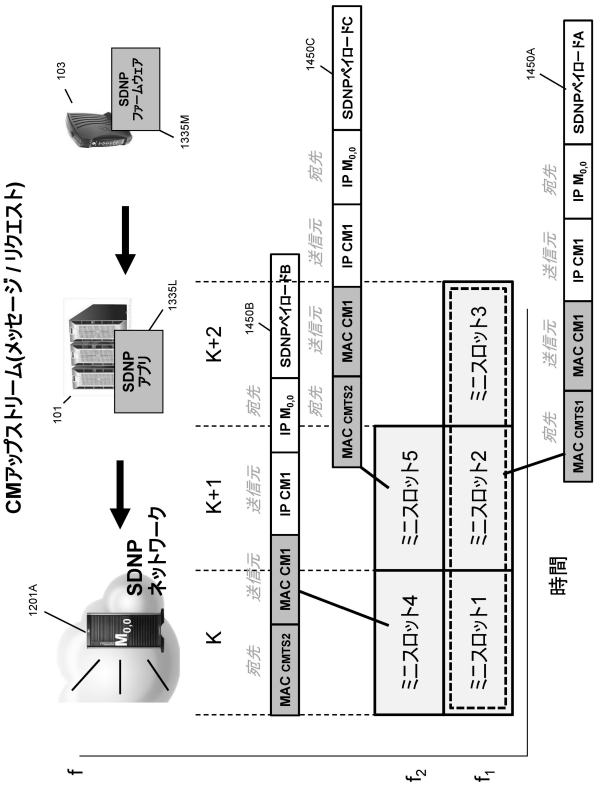
【図６５Ａ】



【図６５Ｂ】

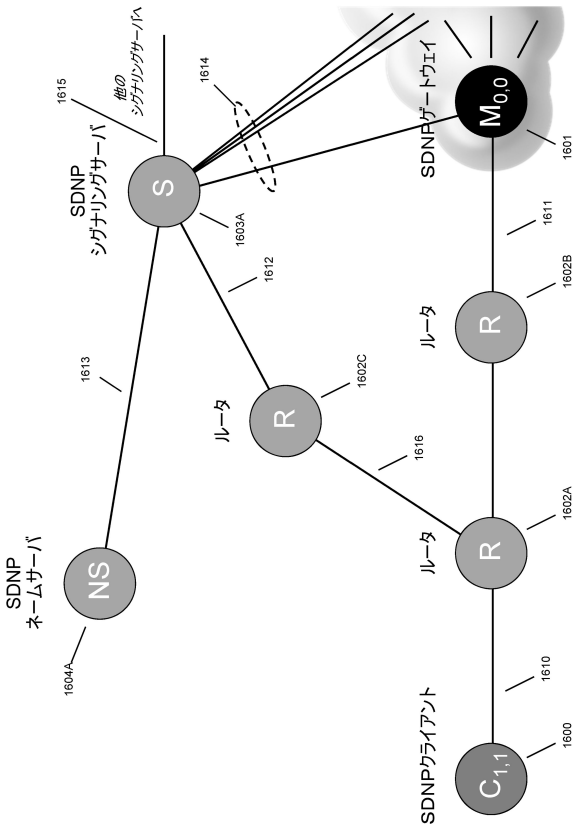


【図６５Ｃ】

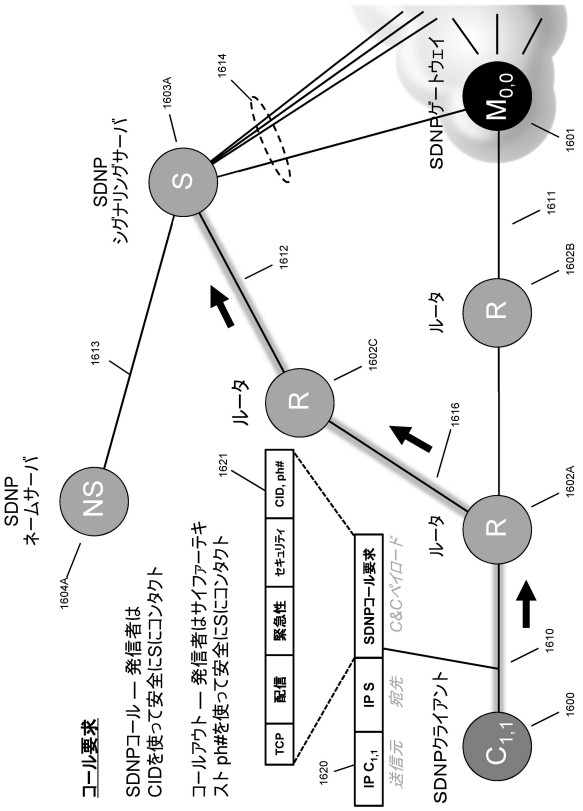


【図６５Ｄ】

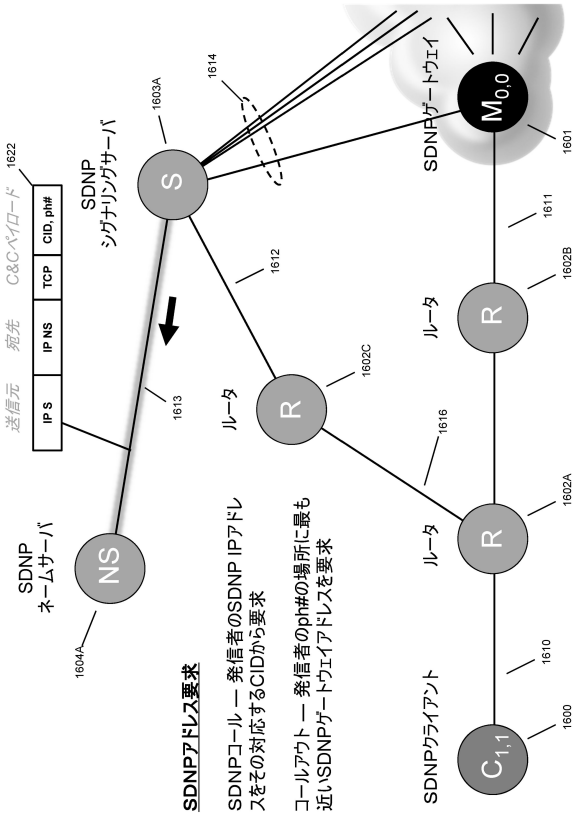
【図６６】



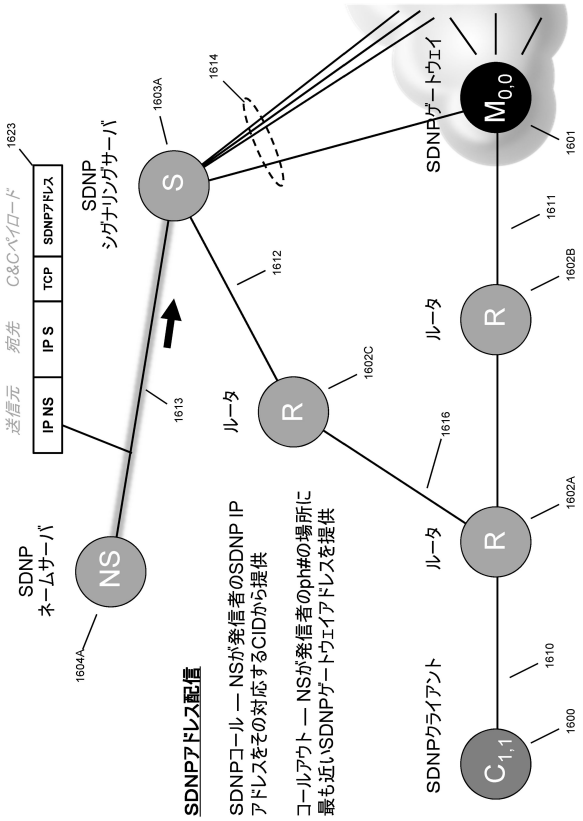
【図６７】



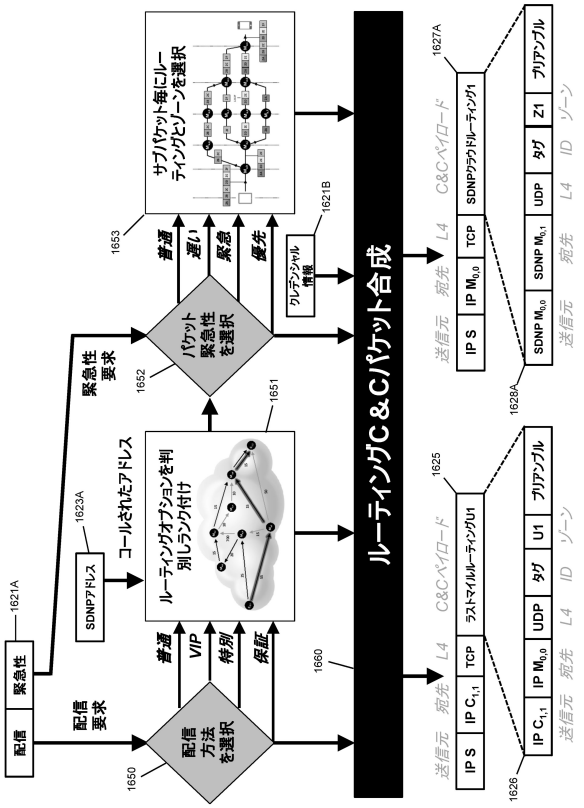
【図６８】



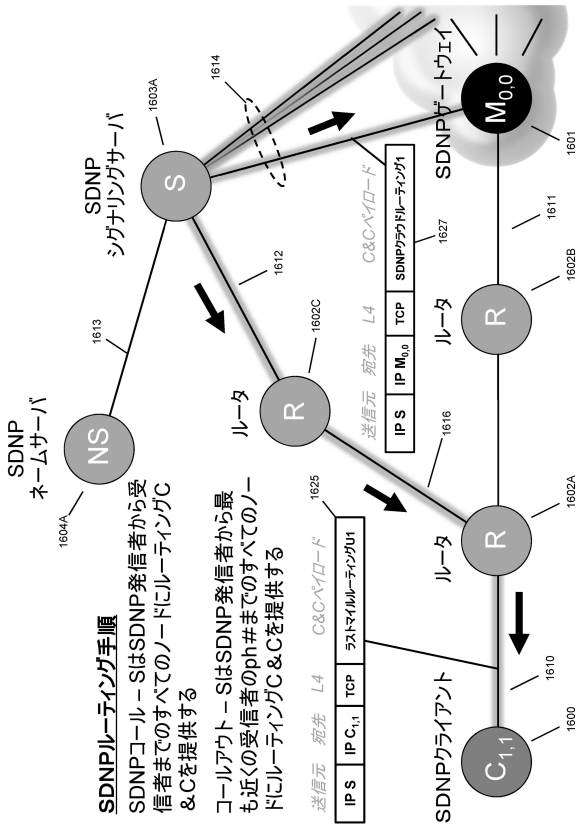
【図６９】



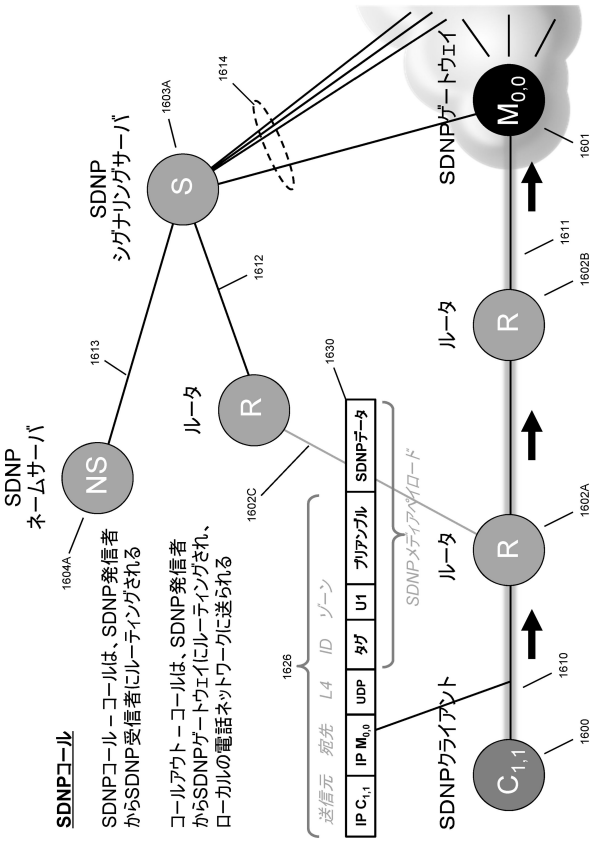
【図７０】



【図７１】

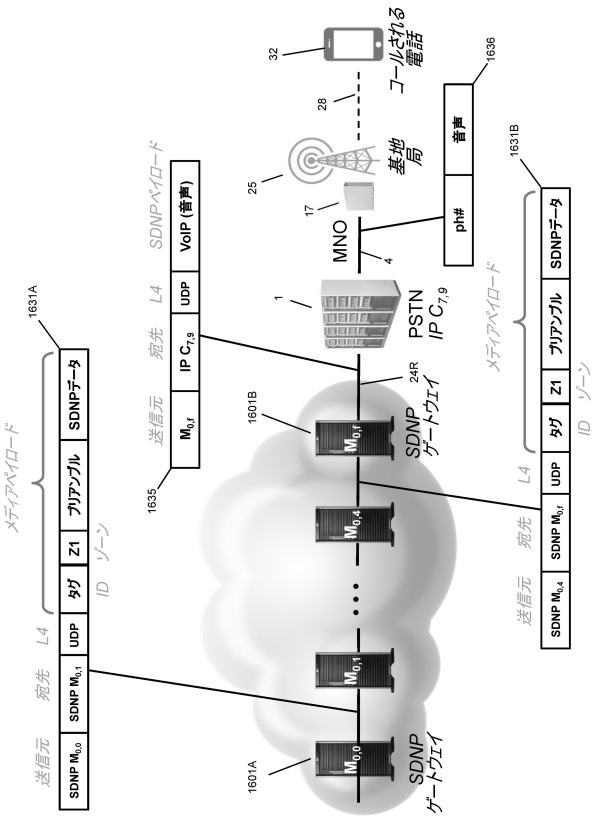


【図７２】

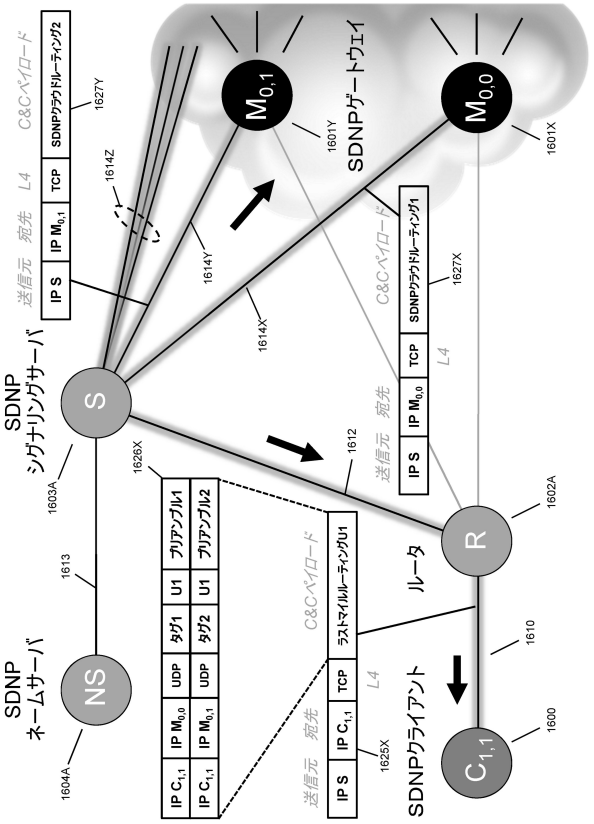


【図７３Ａ】

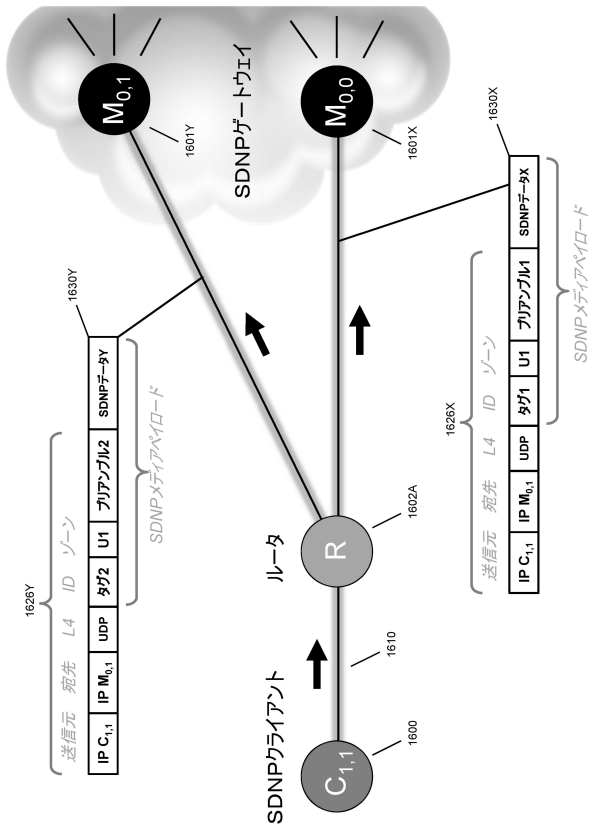
【図７３Ｂ】



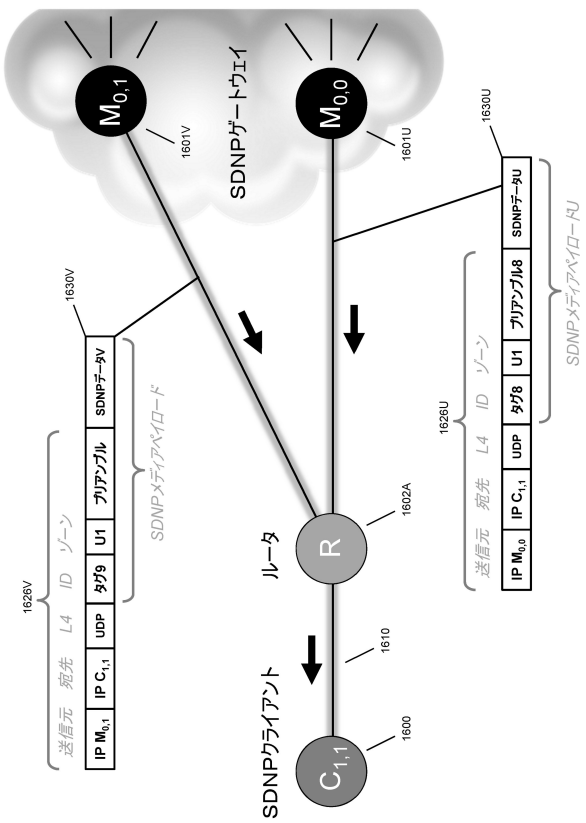
【図７４】



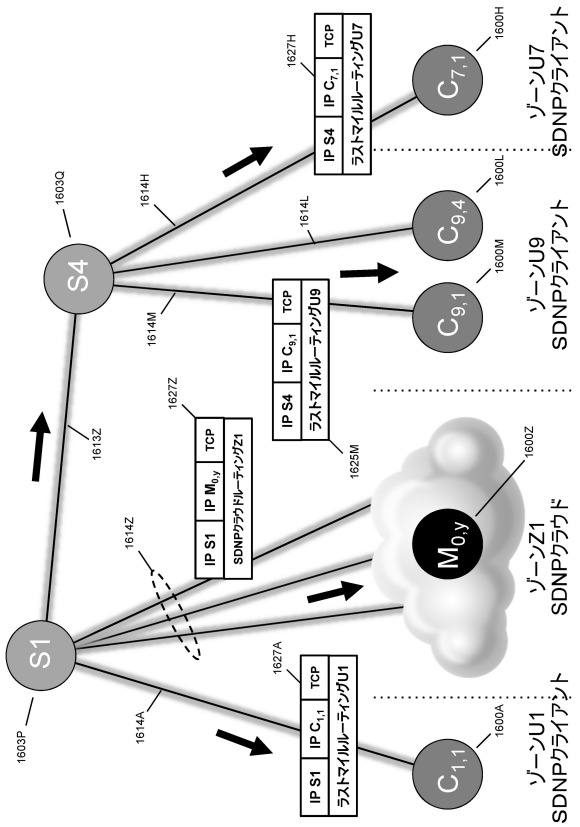
【図７５Ａ】



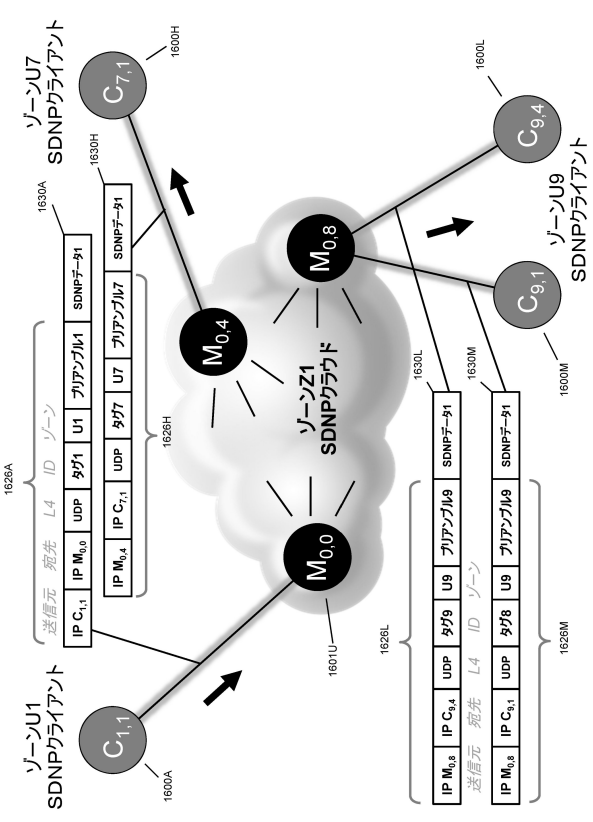
【図７５Ｂ】



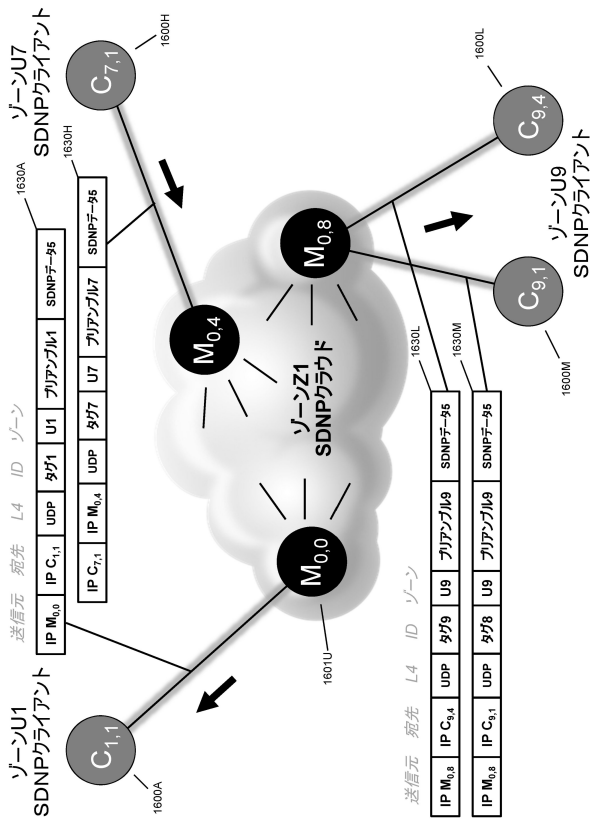
【図７６】



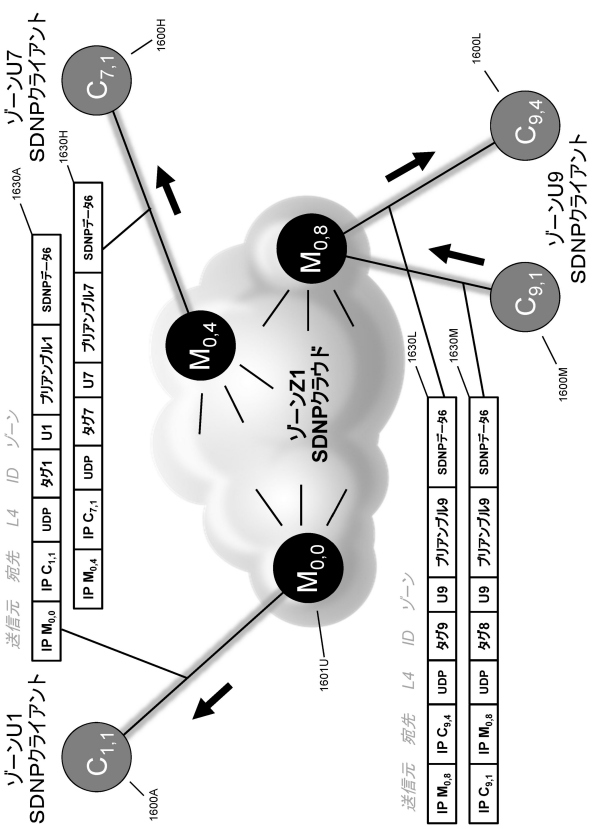
【図７７Ａ】



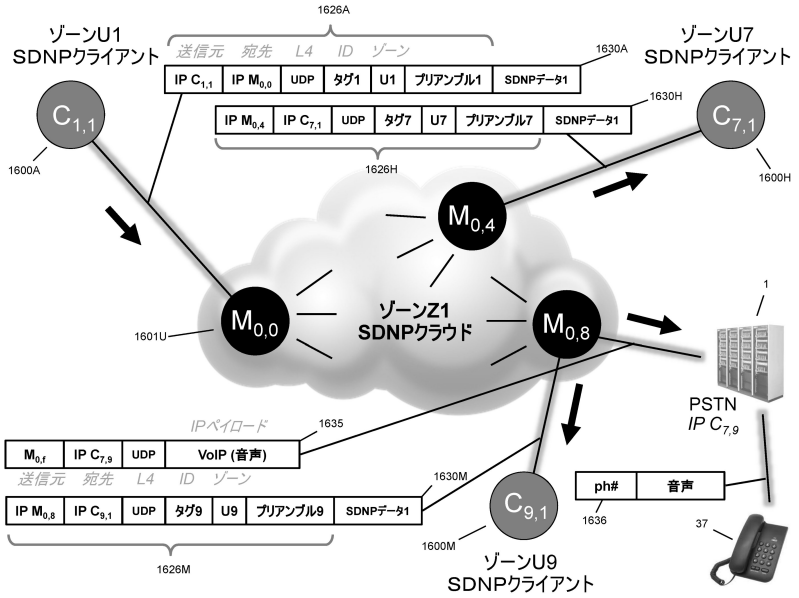
【図７７Ｂ】



【図７７Ｃ】



【図７８】



【図７９Ａ】

グループコールクライアント		通常コール	プライベートコール	
ネットワークノード	ユーザ認証	すべての参加者	認証済みSDNPクライアント	未認証のSDNPクライアント
$C_{1,1}$	SDNPクライアント *グループホスト*	聴取、発話	聴取、発話	–
$C_{7,1}$	SDNPクライアント *参加者*	聴取、発話	聴取、発話	マイク、スピーカー共にミュート
$C_{9,1}$	SDNPクライアント *参加者*	聴取、発話	聴取、発話	
$C_{9,4}$	SDNPクライアント *リスナー*	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	
Ph #1	コールアウト *参加者*	聴取、発話	マイク、スピーカー共にミュート	
Ph #2	コールアウト *リスナー*	聴取のみ、マイクはミュート	マイク、スピーカー共にミュート	

【図７９Ｂ】

グループコールクライアント		通常コール	ハイパープライベートコール	
ネットワークノード	ユーザ認証	すべての参加者	認証済みSDNPクライアント	未認証のSDNPクライアント
$C_{1,1}$	SDNPクライアント *プライベートグループホスト*	聴取、発話	聴取、発話	–
$C_{7,1}$	SDNPクライアント *プライベート参加者*	聴取、発話	聴取、発話	マイク、スピーカー共にミュート
$C_{9,1}$	SDNPクライアント *参加者*	聴取、発話	マイク、スピーカー共にミュート	
$C_{9,4}$	SDNPクライアント *プライベートリスナー*	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	
$C_{9,5}$	SDNPクライアント *リスナー*	聴取のみ、マイクはミュート	マイク、スピーカー共にミュート	
Ph #1	コールアウト *参加者*	聴取、発話	マイク、スピーカー共にミュート	
Ph #2	コールアウト *リスナー*	聴取のみ、マイクはミュート	マイク、スピーカー共にミュート	

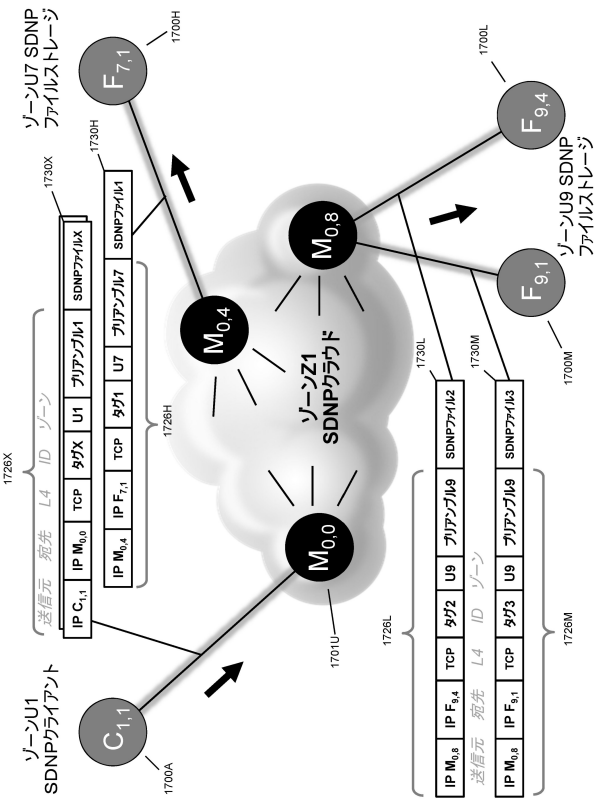
【図８０Ａ】

PTTグループコールクライアント		通常のプッシュツートーク		プライベートなプッシュツートーク		
ネットワークノード	ユーザ認証	ホストPTT	その他のPTT	認証済みホストPTT	認証済みその他のPTT	未認証のパーティ
$C_{1,1}$	SDNPクライアント グループホスト	**発話、** 優先ミュート	聴取のみ、マイクはミュート	**発話、** 優先ミュート	聴取のみ、マイクはミュート	–
$C_{7,1}$	SDNPクライアント 参加者	聴取のみ、マイクはミュート	**発話、** 他者をミュート	聴取のみ、マイクはミュート	**発話、**ミュート すべての他者	マイク、スピーカー共にミュート
$C_{9,1}$	SDNPクライアント 参加者	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	
$C_{9,4}$	SDNPクライアント リスナー	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	
$C_{9,5}$	SDNPクライアント リスナー	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	
Ph #1	コールアウト	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	マイク、スピーカー共にミュート	マイク、スピーカー共にミュート	

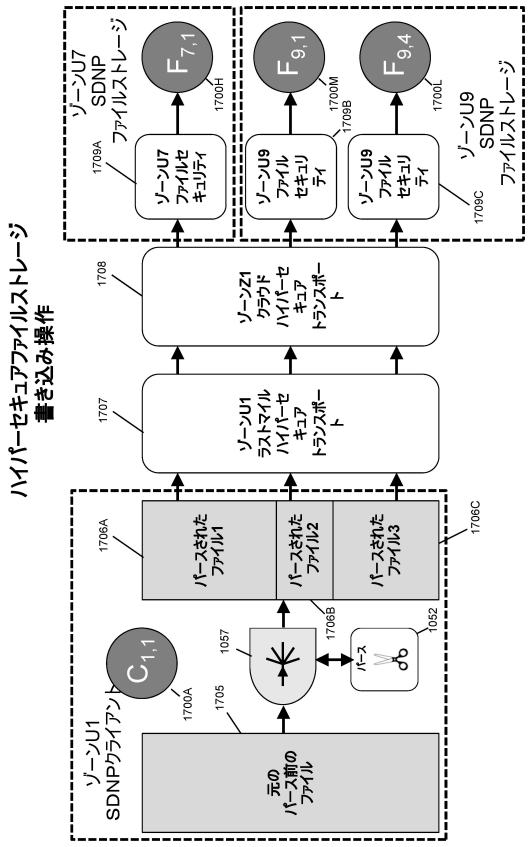
【図８０Ｂ】

PTTグループコールクライアント		通常のプッシュツートーク		ハイパープライベートなプッシュツートーク			
ネットワークノード	ユーザー認証	ホスト PTT	その他の PTT	認証済み ホストPTT	認証済み その他のPTT	未認証の パーティ
$C_{1,1}$	SDNP クライアント グループホスト	発話、優先ミュート	聴取のみ、マイクはミュート	発話、優先ミュート	聴取のみ、マイクはミュート	–
$C_{7,1}$	SDNP クライアント プライベート参加者	聴取のみ、マイクはミュート	発話、他者をミュート	聴取のみ、マイクはミュート	発話、他者をミュート	マイク、スピーカー共にミュート
$C_{9,1}$	SDNP クライアント 参加者	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	マイク、スピーカー共にミュート	マイク、スピーカー共にミュート	
$C_{9,4}$	SDNP クライアント プライベート リスナー	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	
$C_{9,5}$	SDNP クライアント 聴取のみ	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	マイク、スピーカー共にミュート	マイク、スピーカー共にミュート	
ph#	コールアウト	聴取のみ、マイクはミュート	聴取のみ、マイクはミュート	マイク、スピーカー共にミュート	マイク、スピーカー共にミュート	

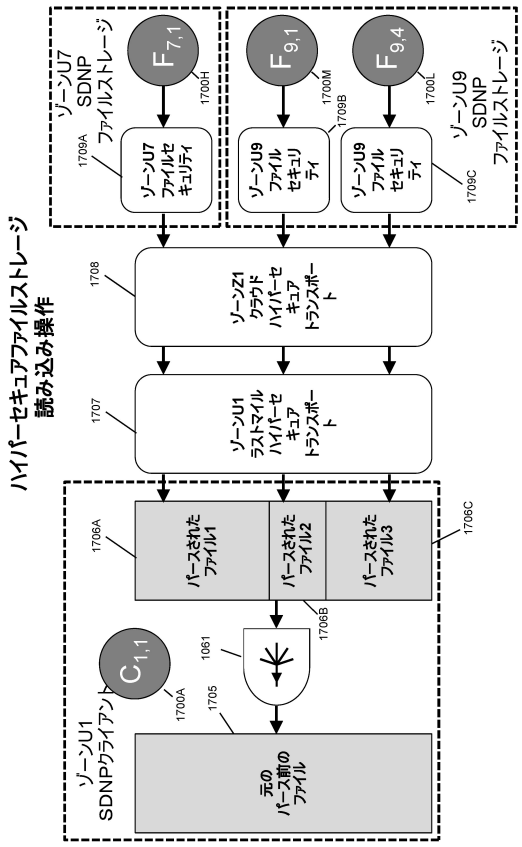
【図８１】



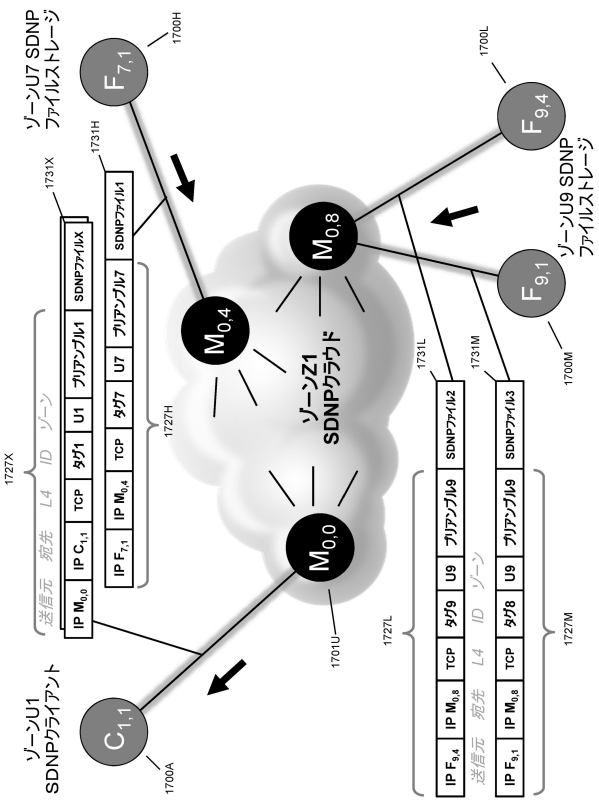
【図８２Ａ】



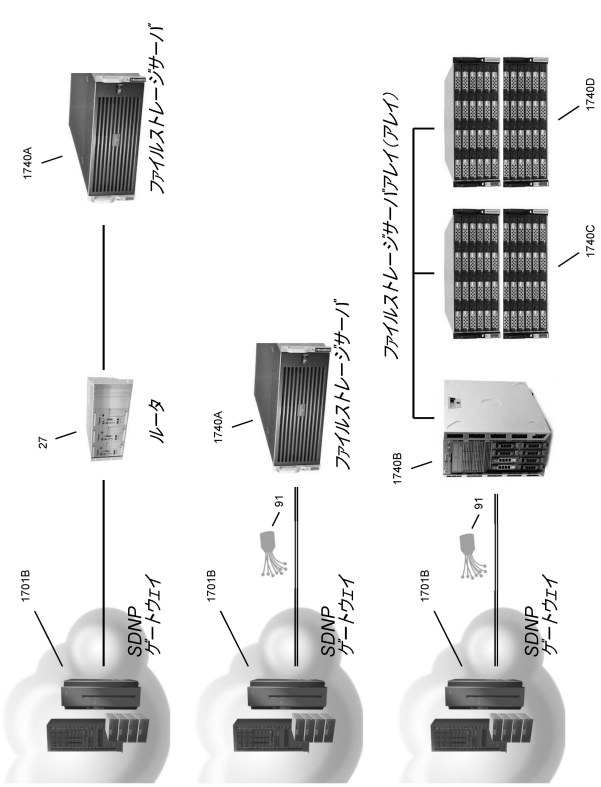
【図８２Ｂ】



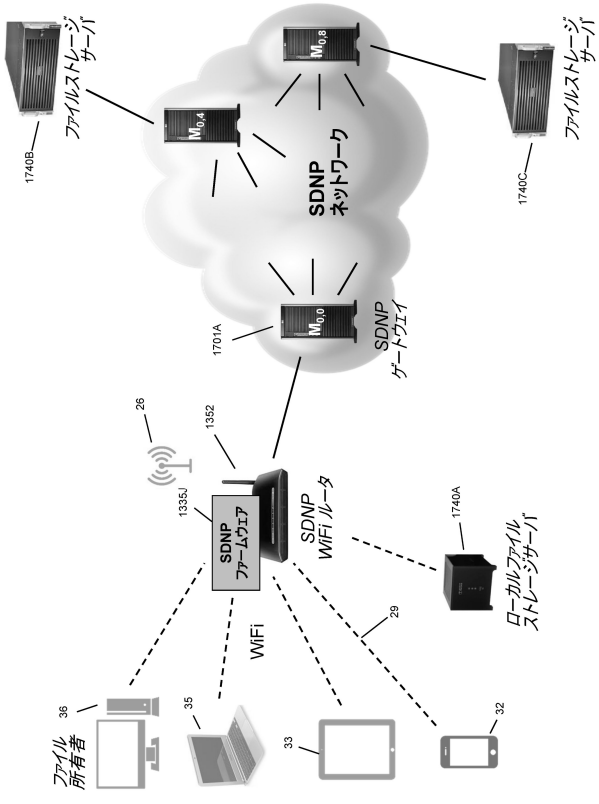
【図８３】



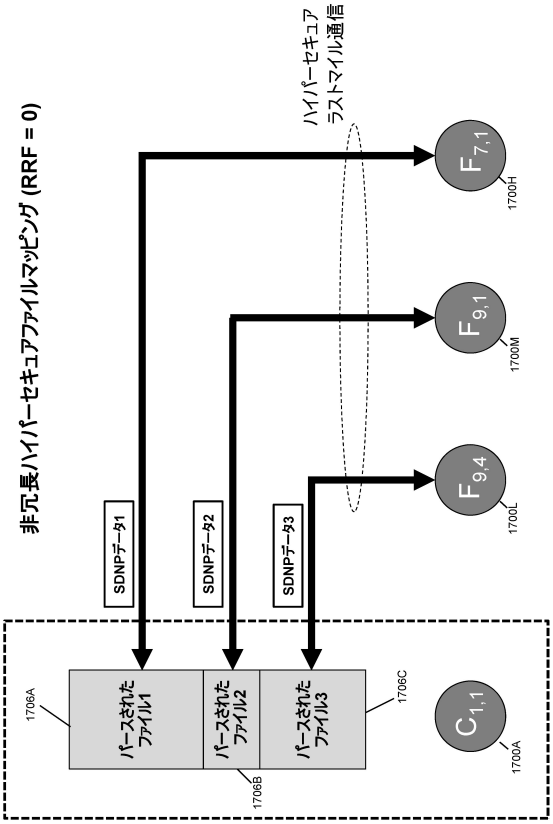
【図８４Ａ】



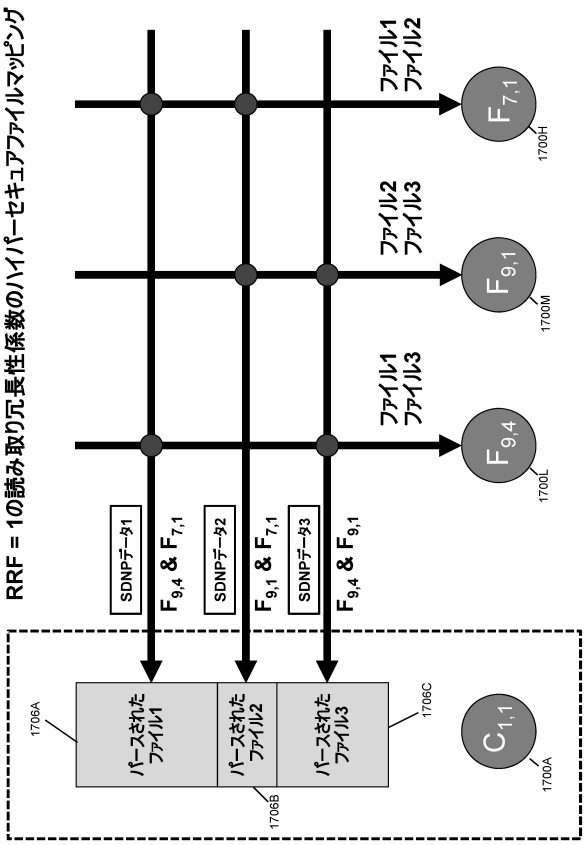
【図８４Ｂ】



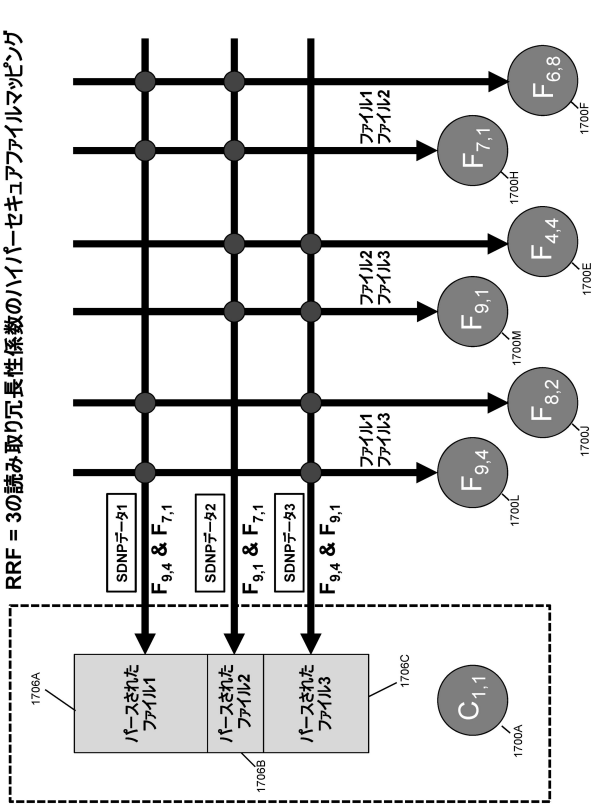
【図８５Ａ】



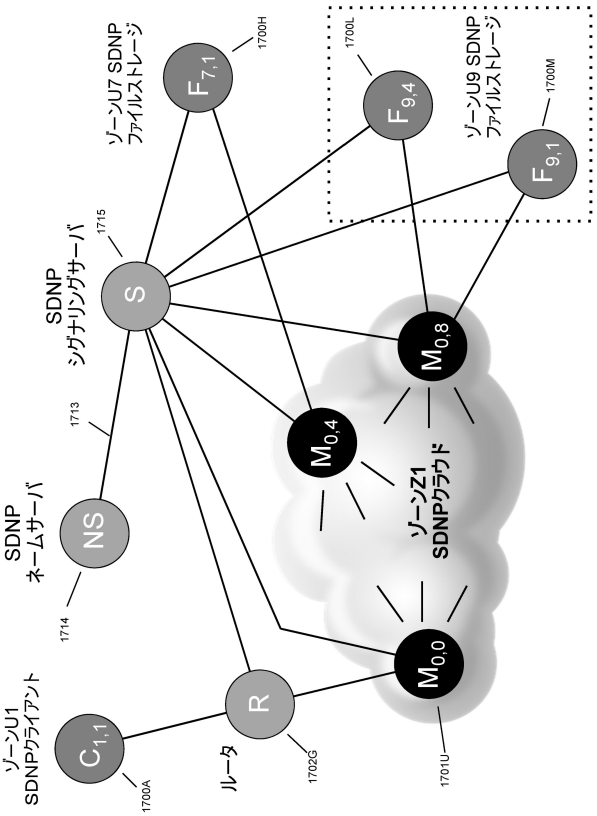
【図８５Ｂ】



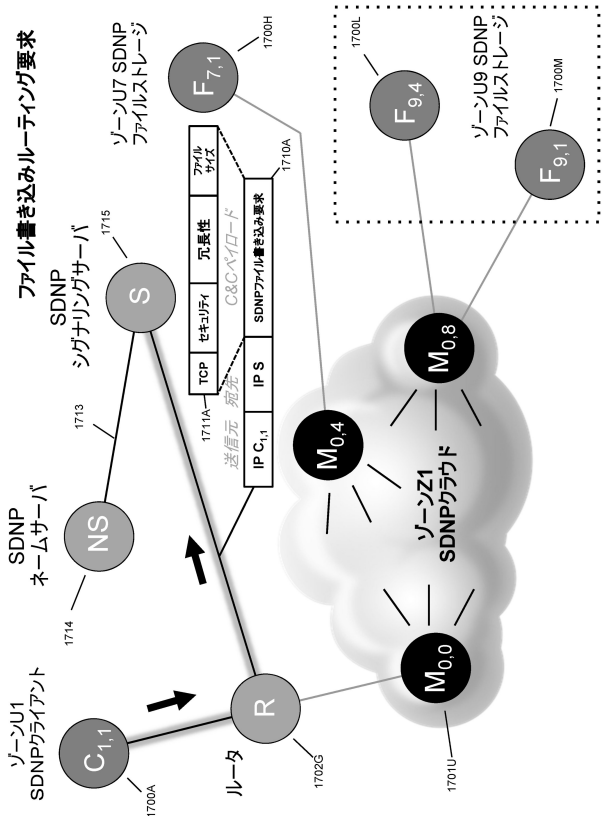
【図８５Ｃ】



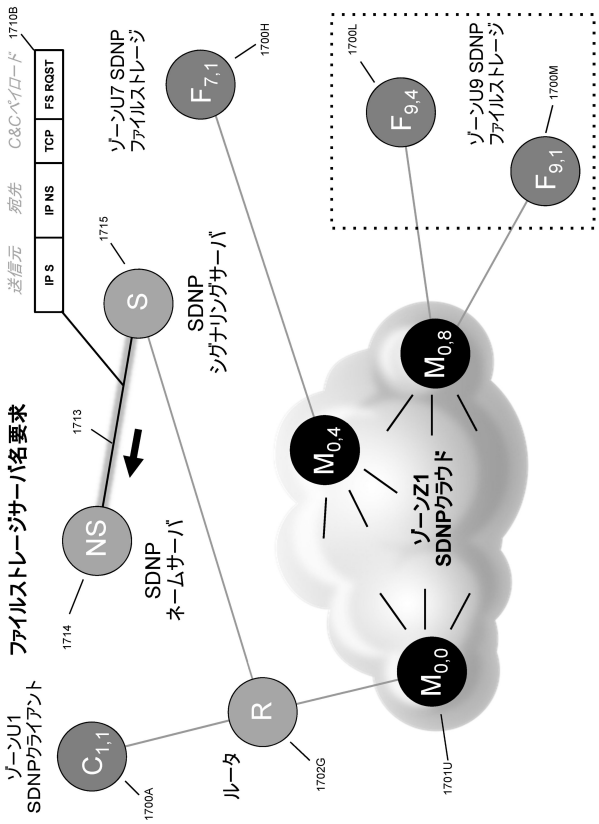
【図８６】



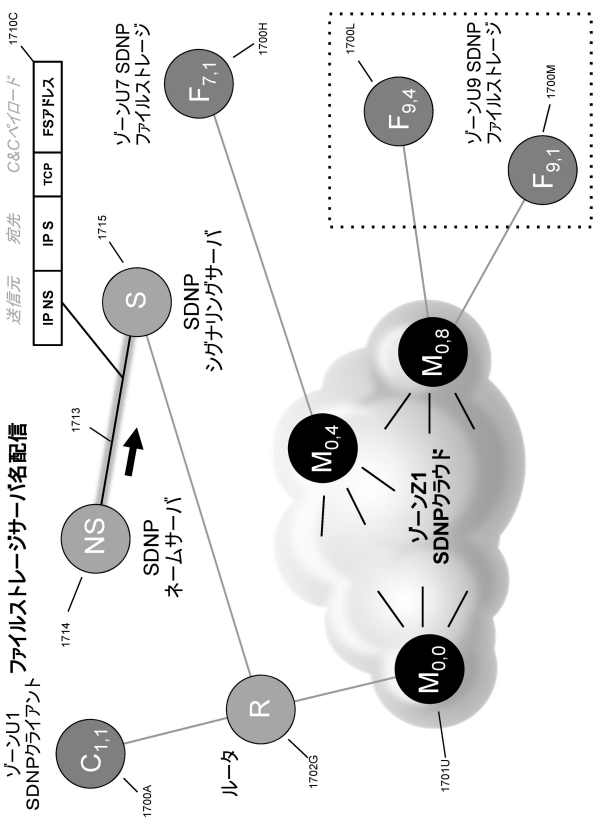
【図８７Ａ】



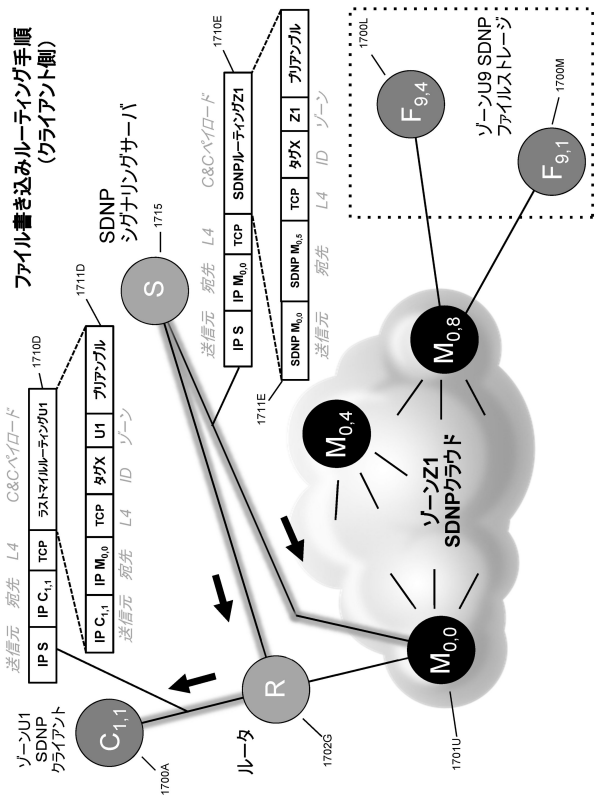
【図８７Ｂ】



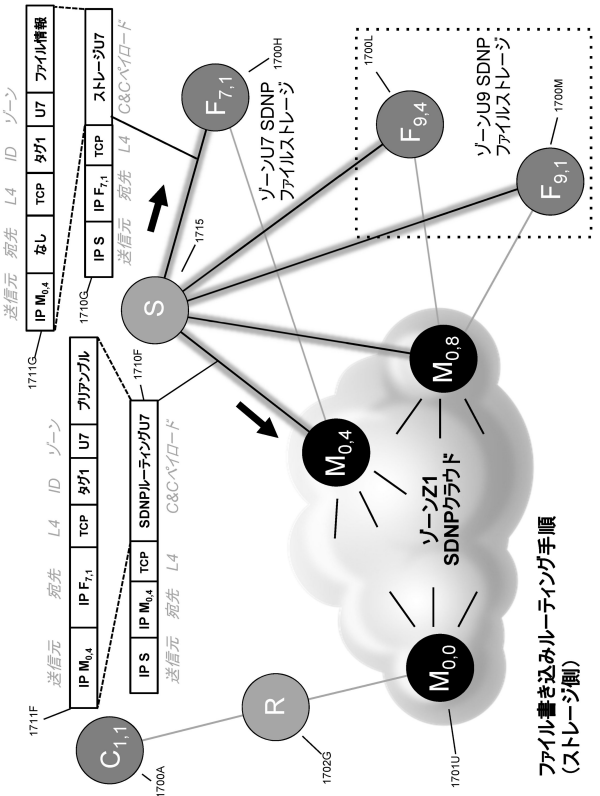
【図８７Ｃ】



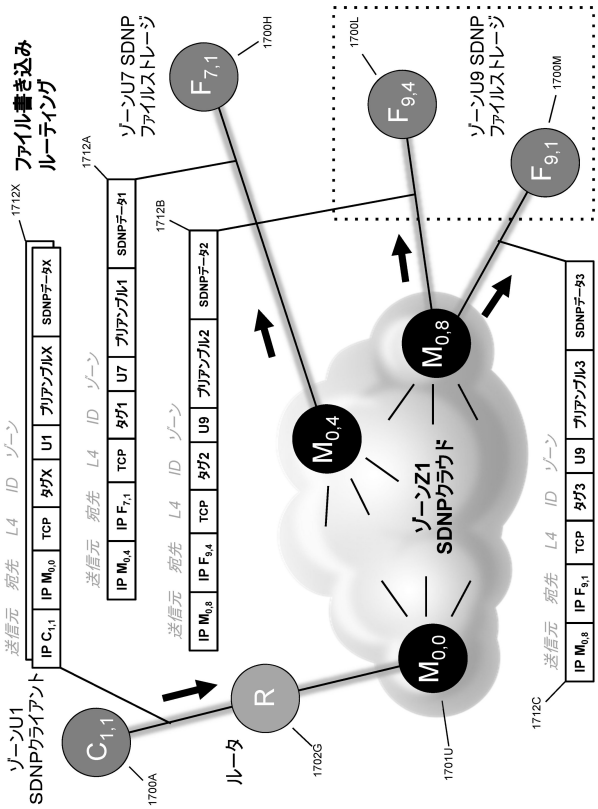
【図８７Ｄ】



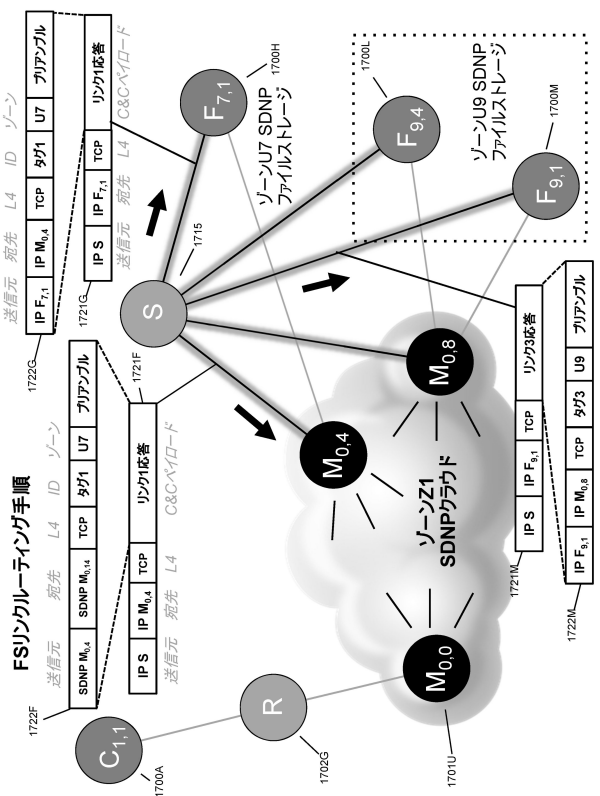
【図８７Ｅ】



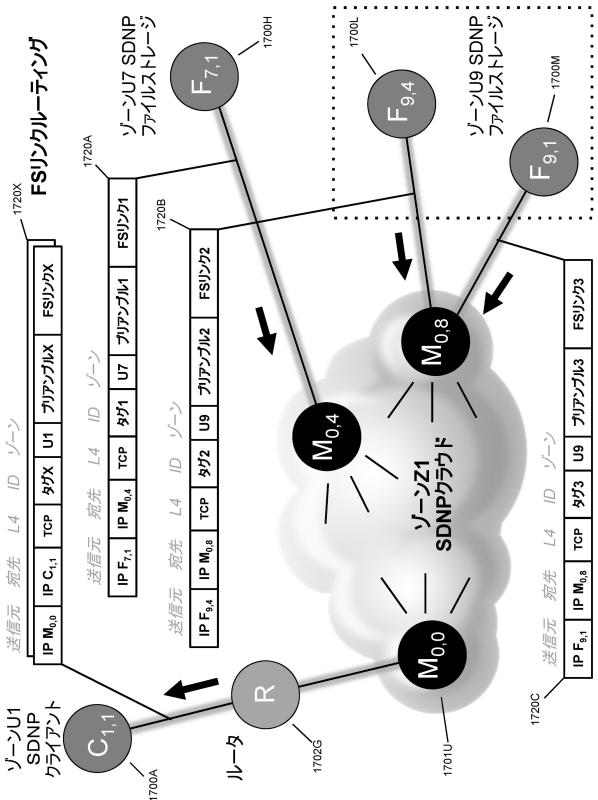
【図８８】



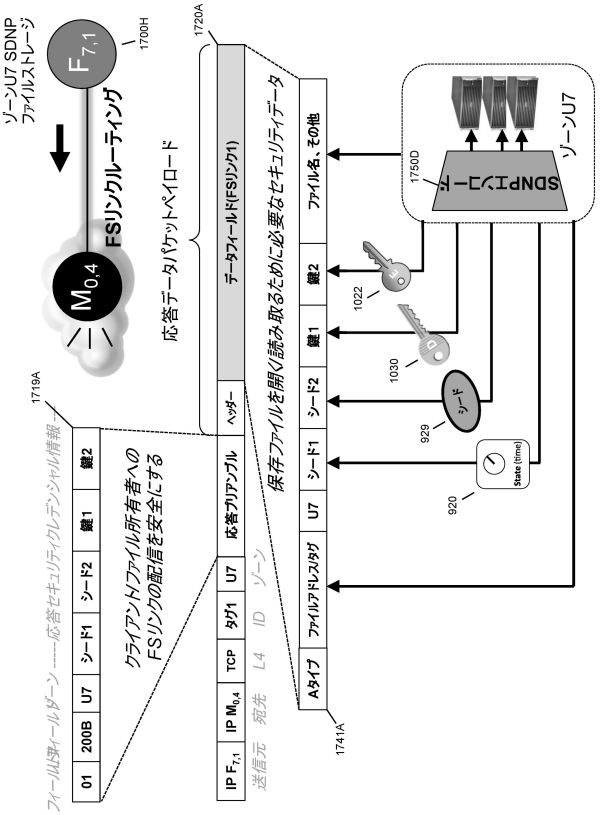
【図８９Ａ】



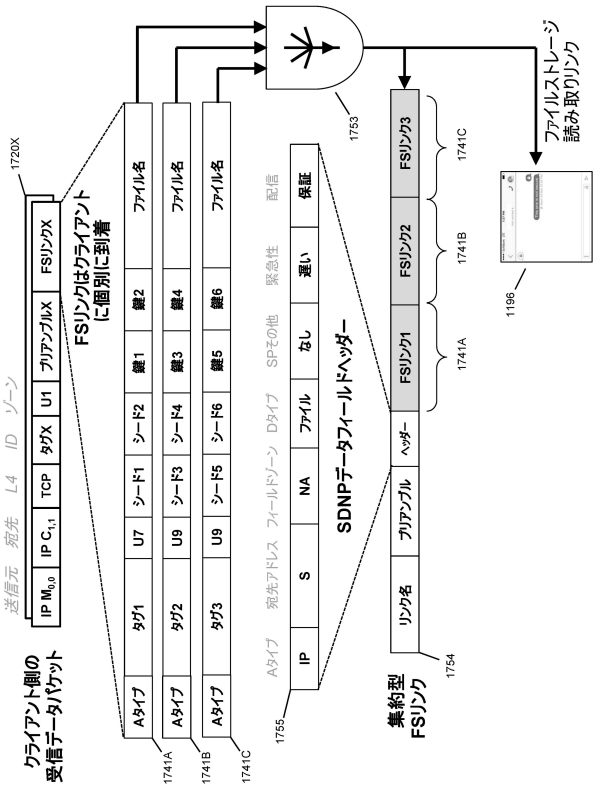
【図８９Ｂ】



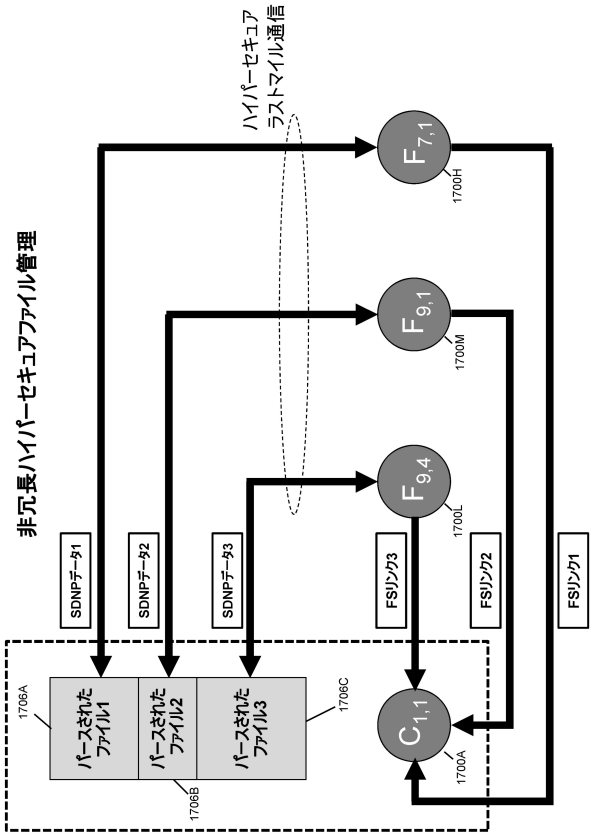
【図８９Ｃ】



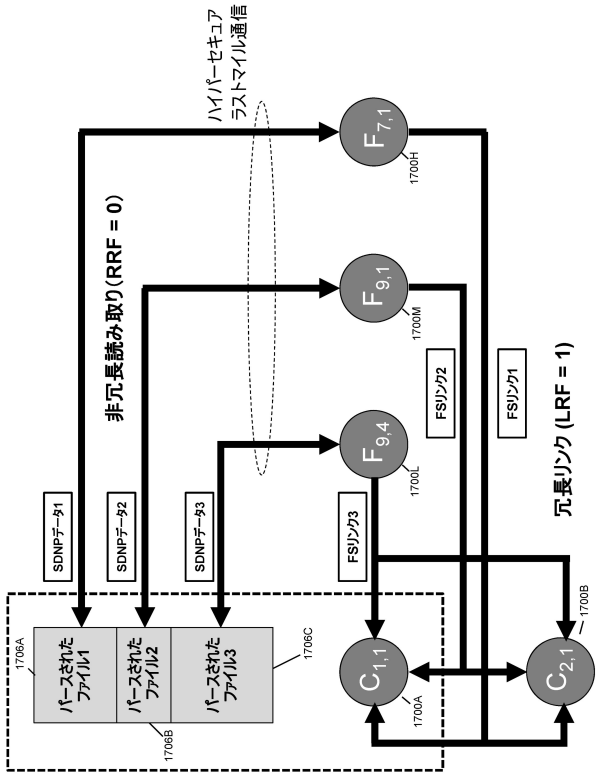
【図８９Ｄ】



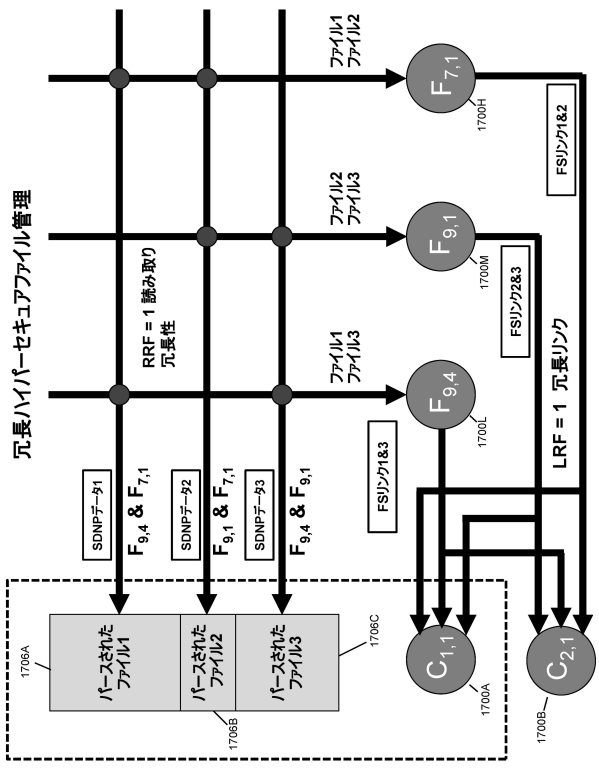
【図９０Ａ】



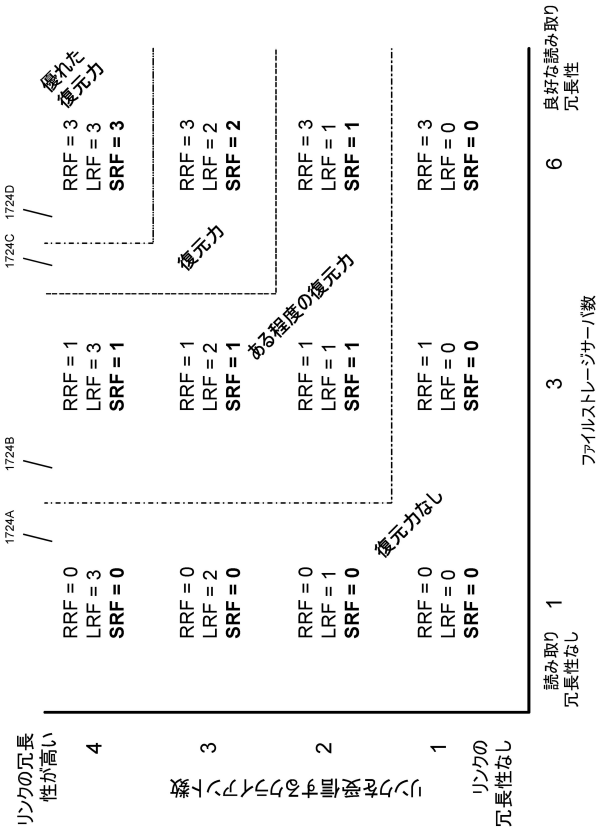
【図９０Ｂ】



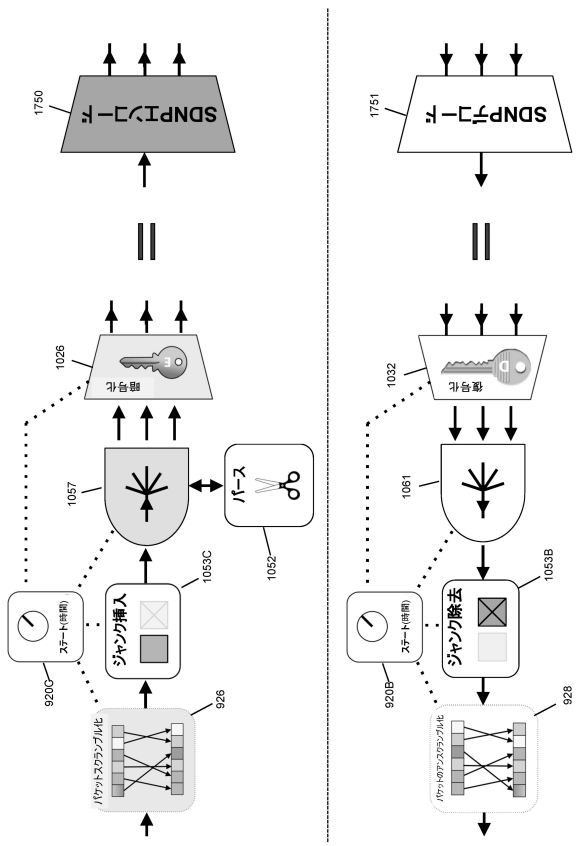
【図９０Ｃ】



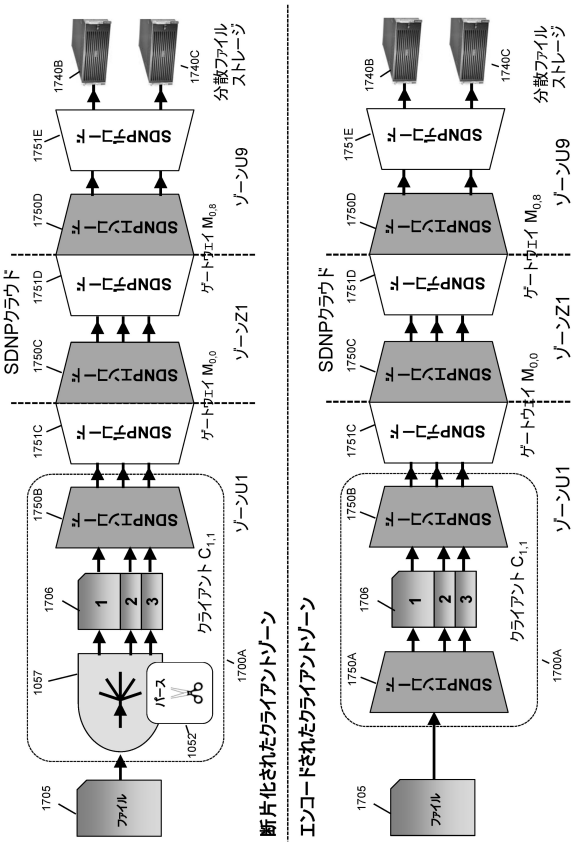
【図９１】



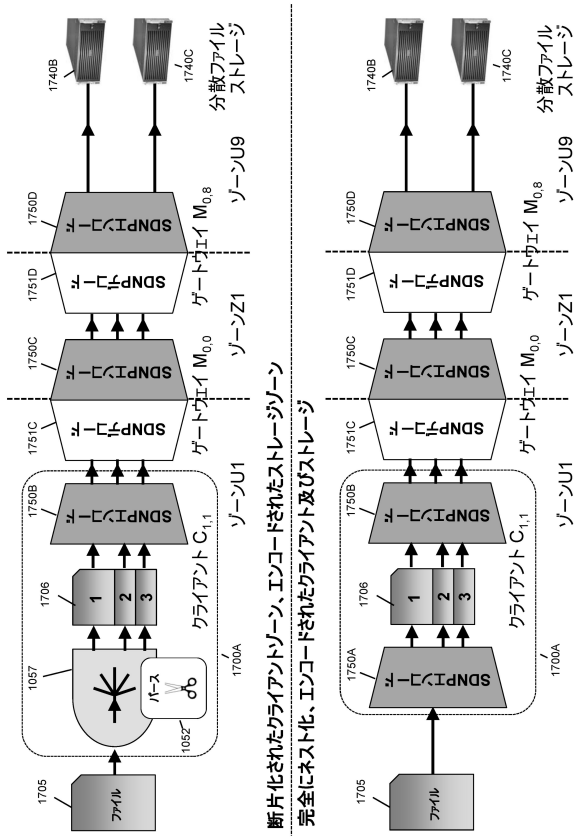
【図９２】



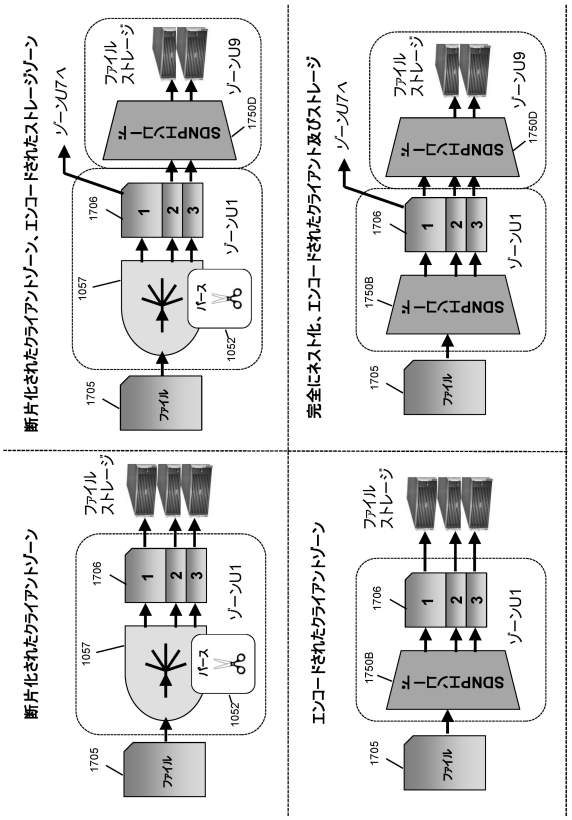
【図９３Ａ】



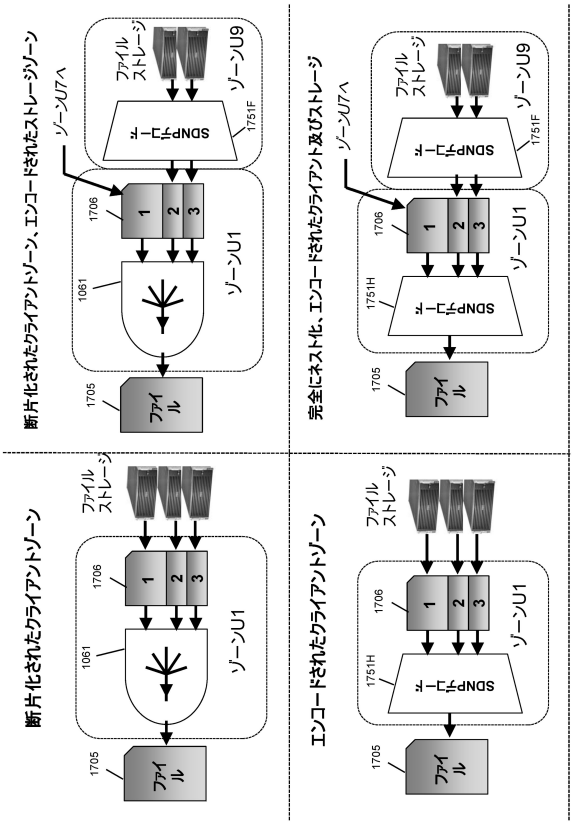
【図９３Ｂ】



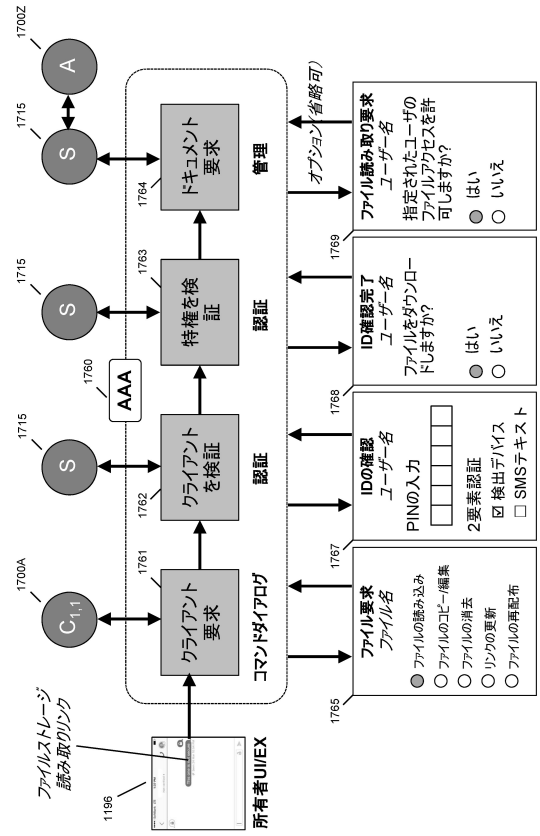
【図９４】



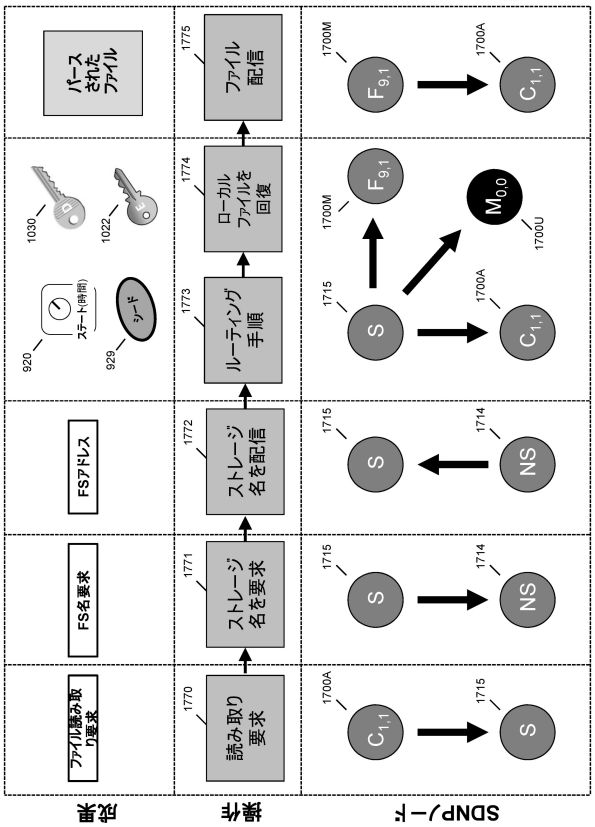
【図９５】



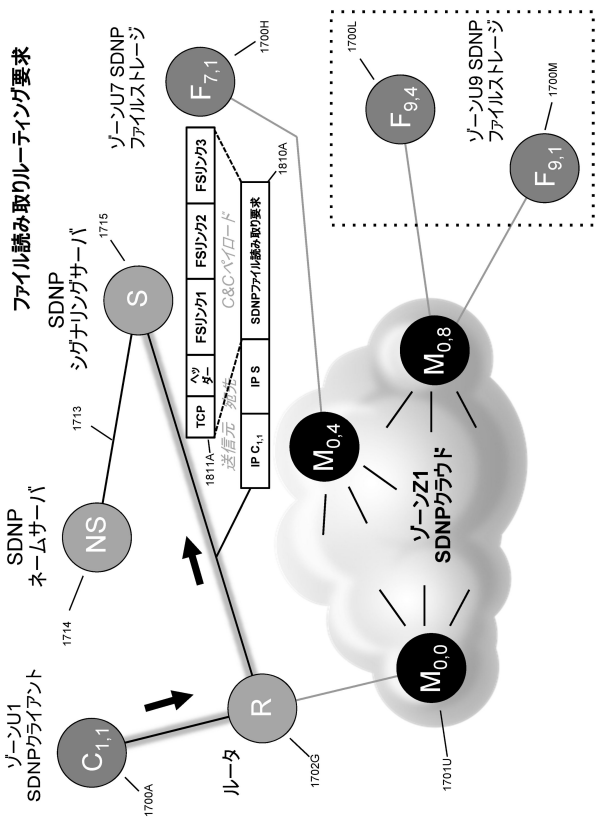
【図９６Ａ】



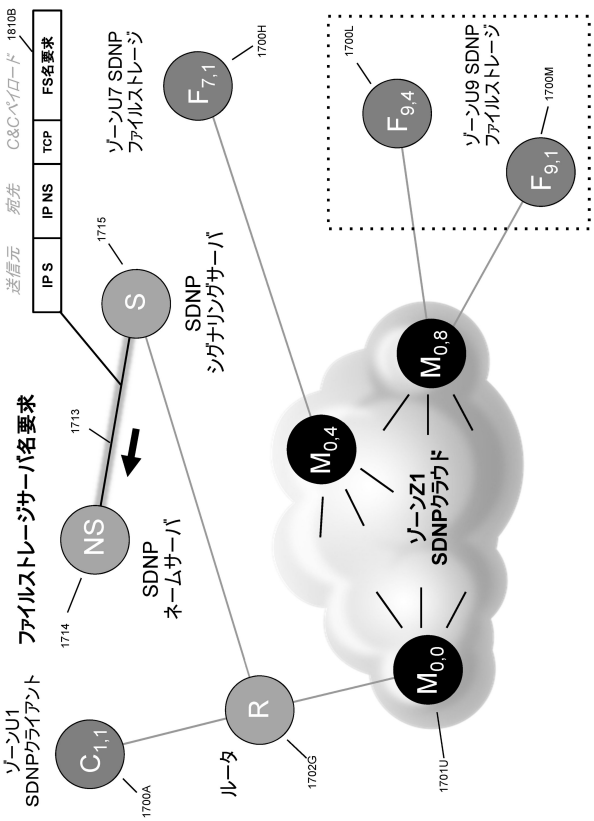
【図９６Ｂ】



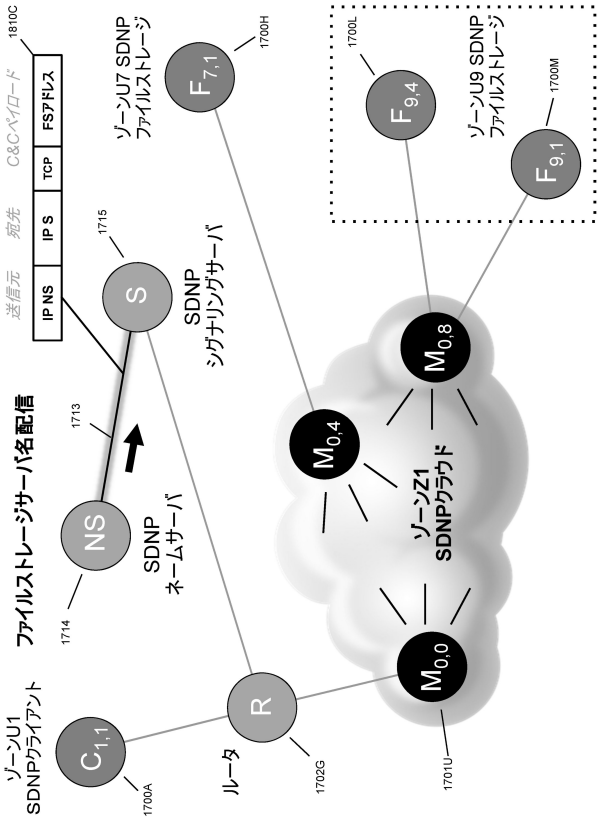
【図９７Ａ】



【図９７Ｂ】

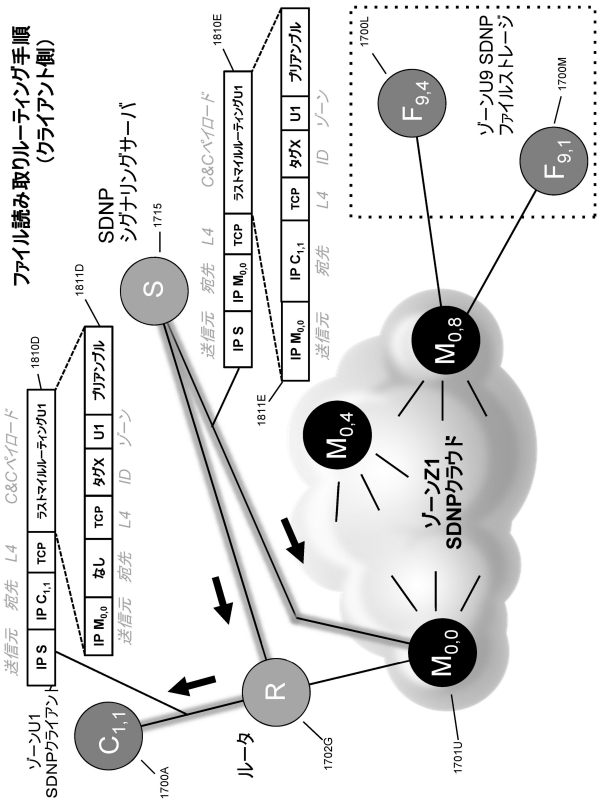


【図９７Ｃ】

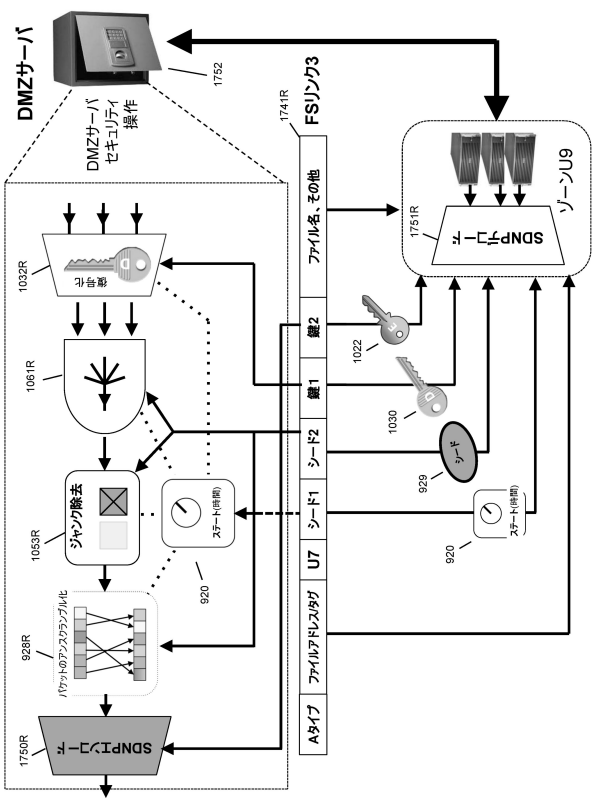


【図９７Ｄ】

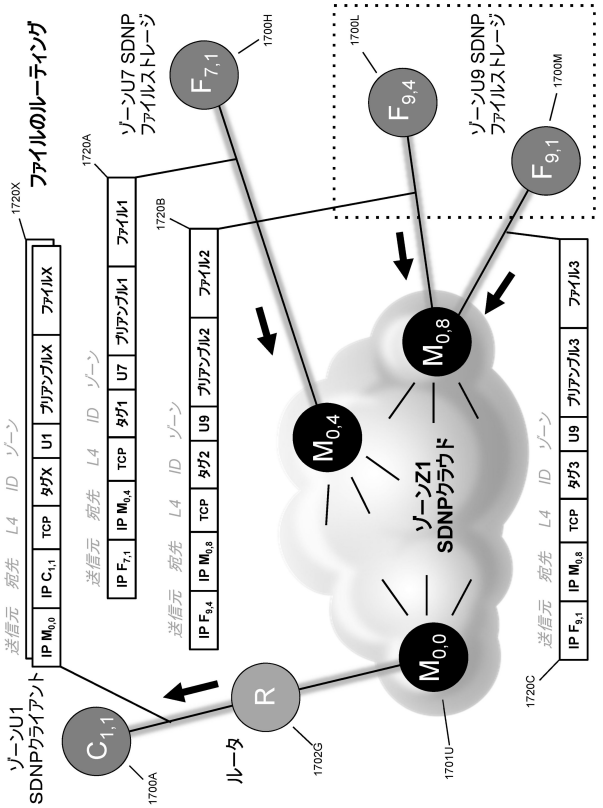
【図９７Ｅ】



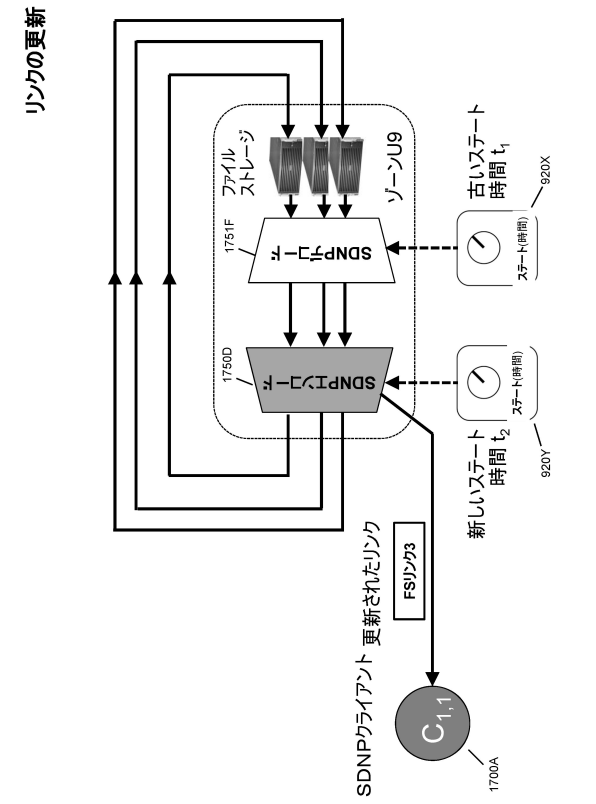
【図９８】



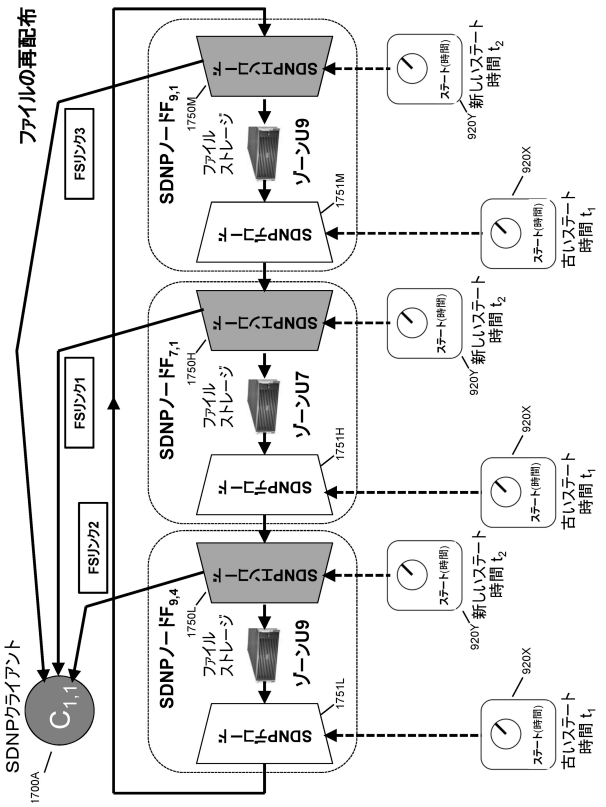
【図９９】



【図１００】



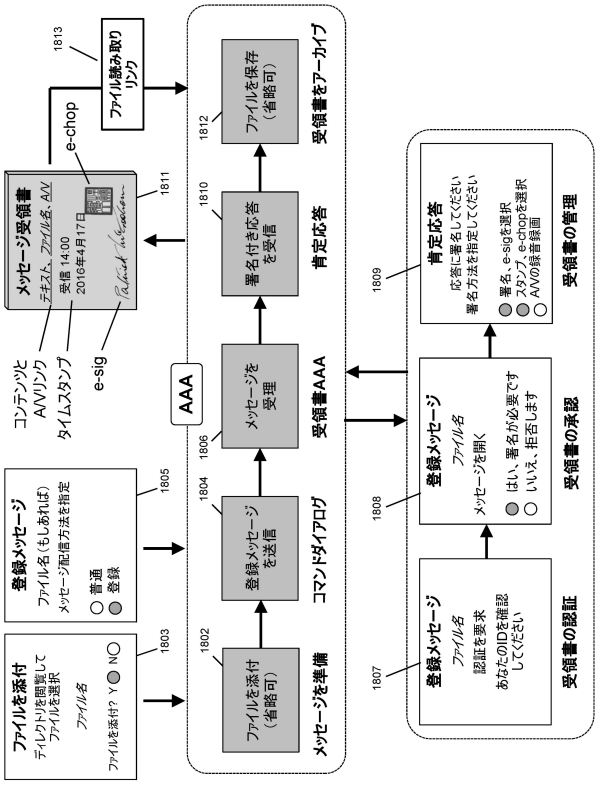
【図１０１】



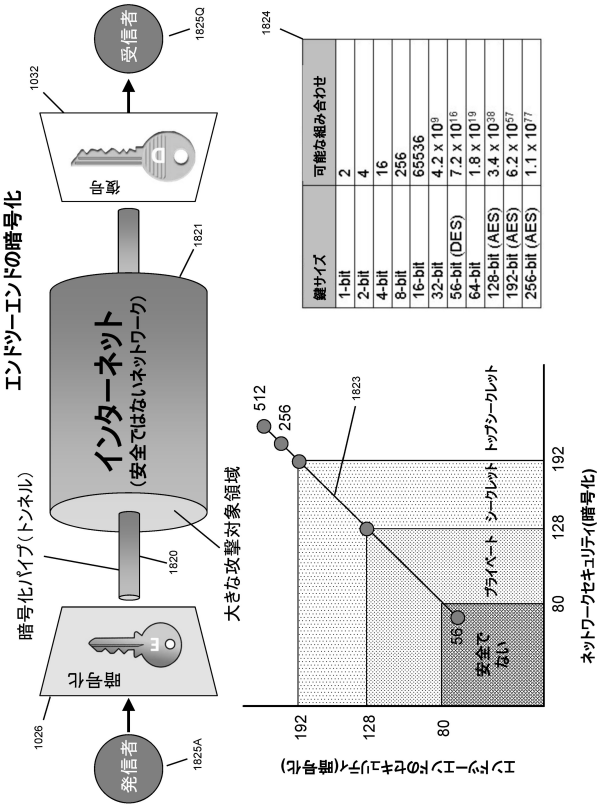
【図１０２】



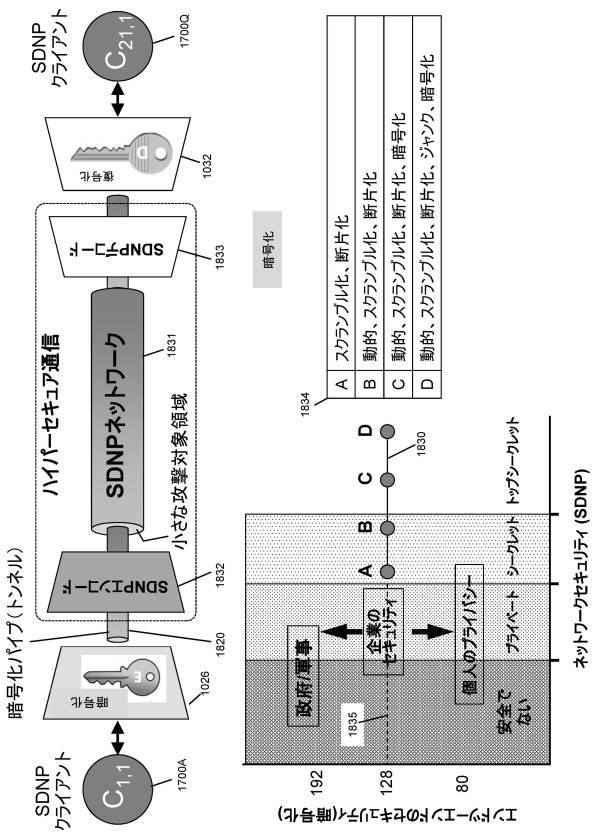
【図１０３】



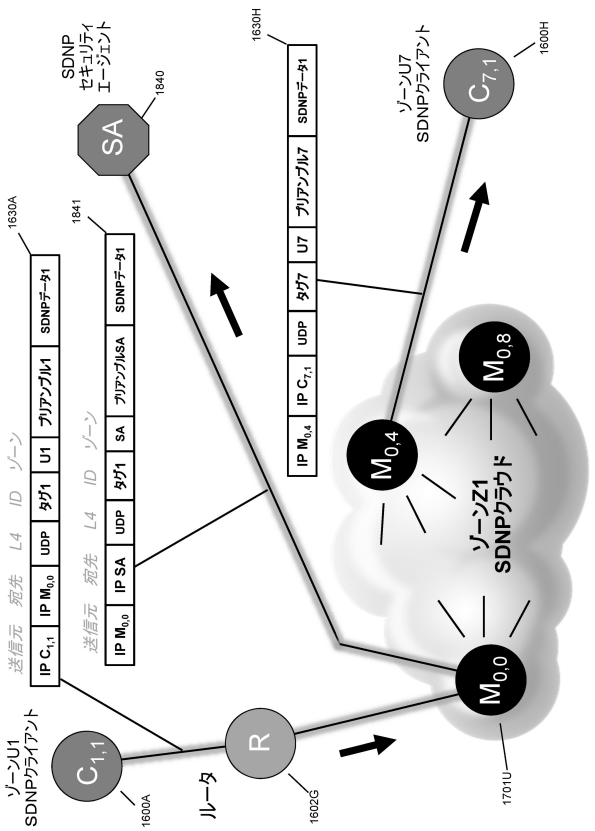
【図１０４Ａ】



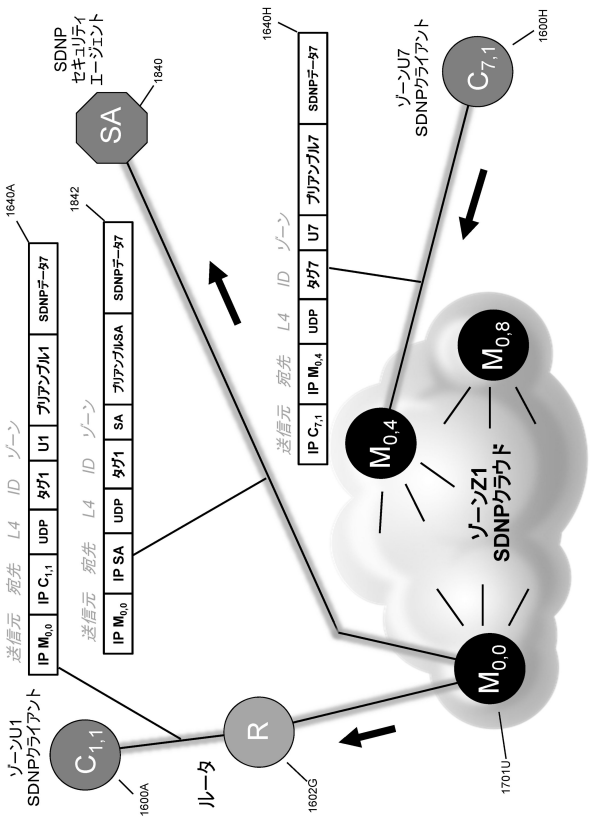
【図１０４Ｂ】



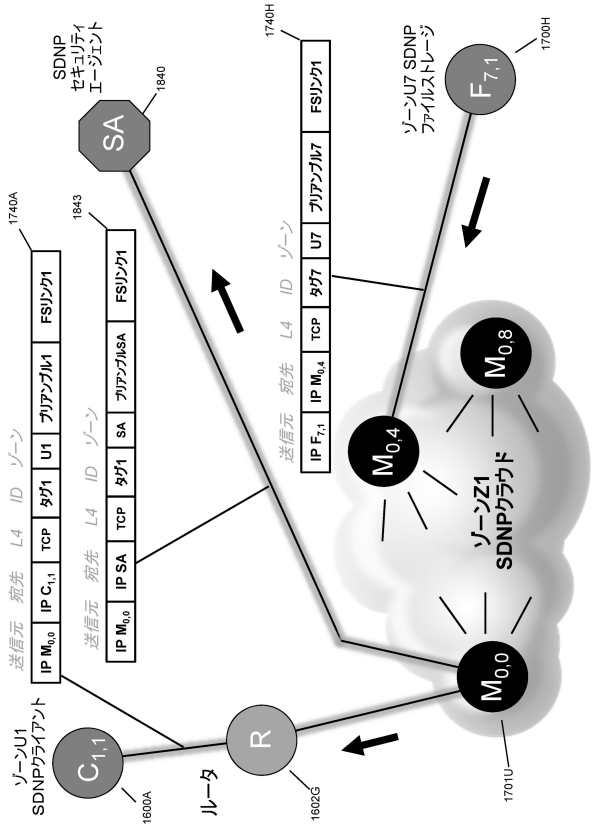
【図１０５Ａ】



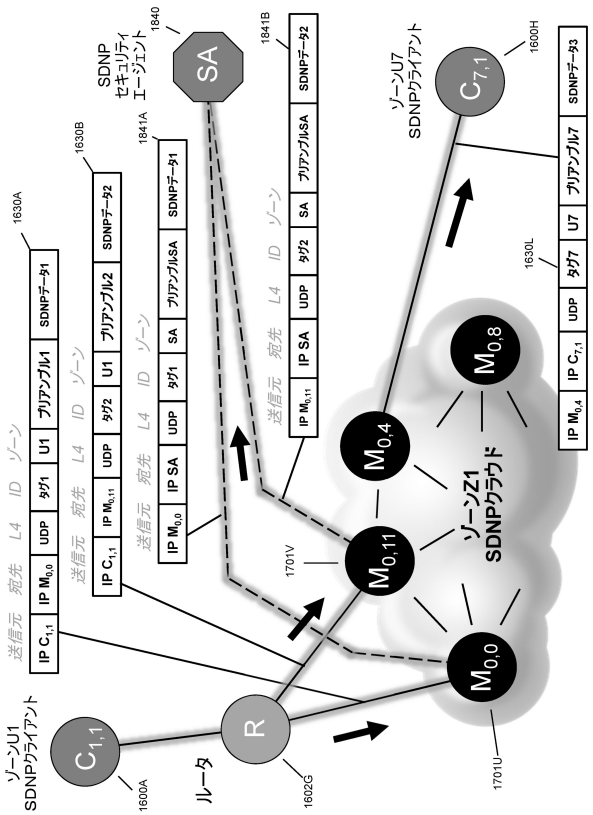
【図１０５Ｂ】



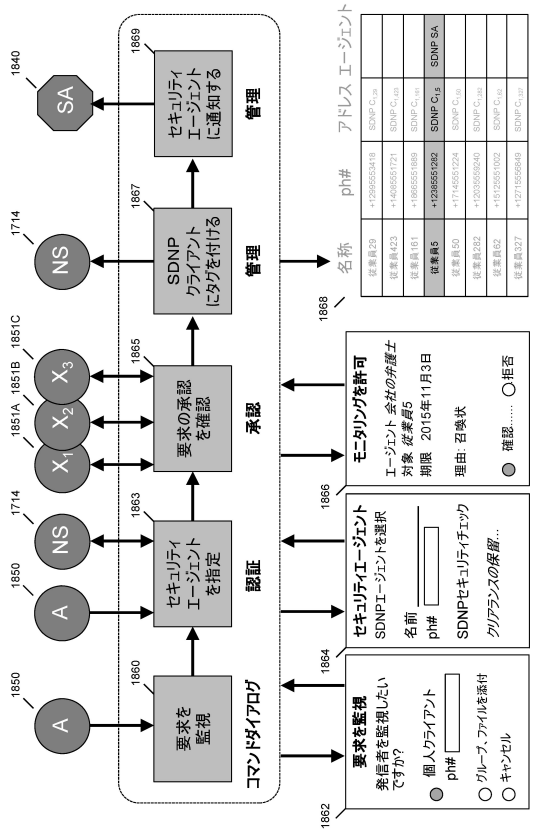
【図１０６】



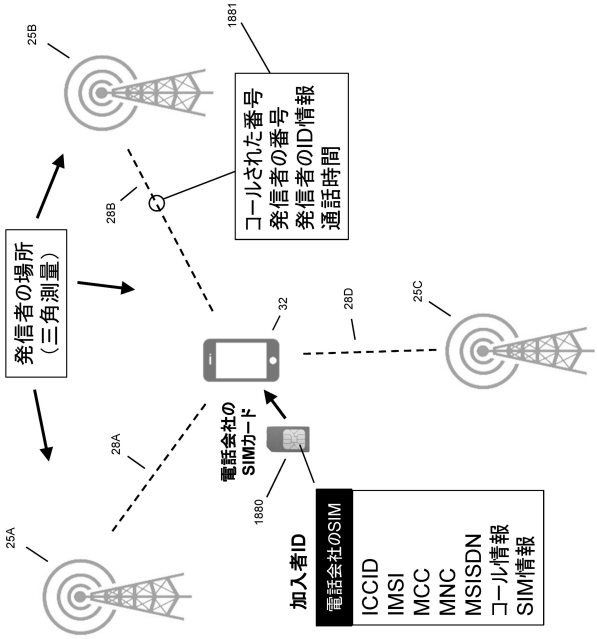
【図１０７】



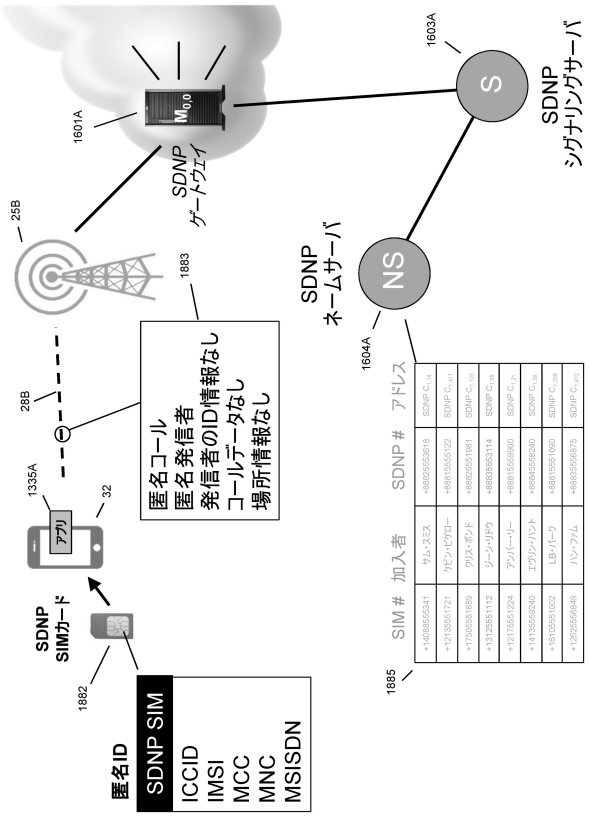
【図１０８】



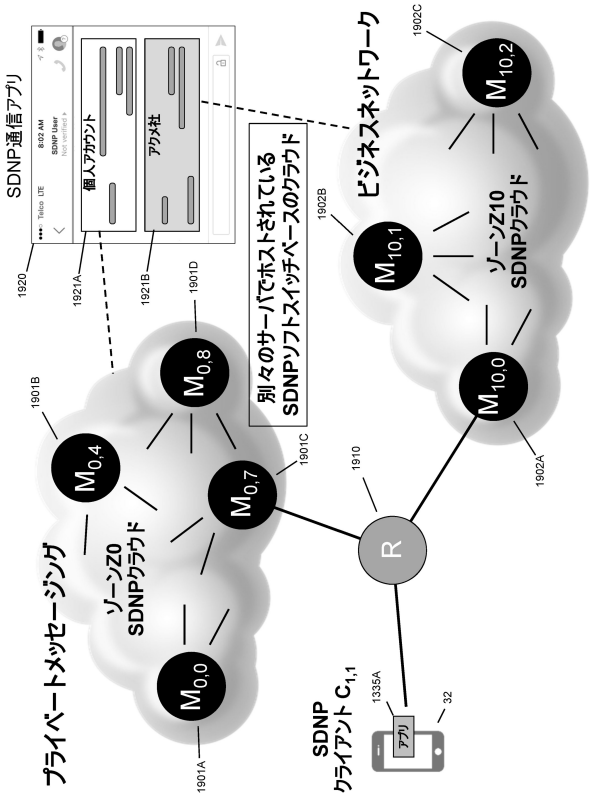
【図１０９】



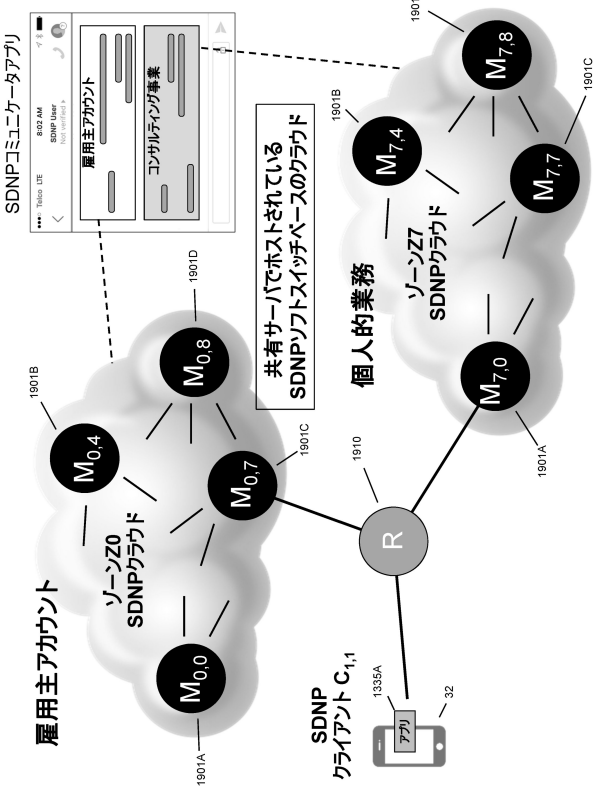
【図１１０】



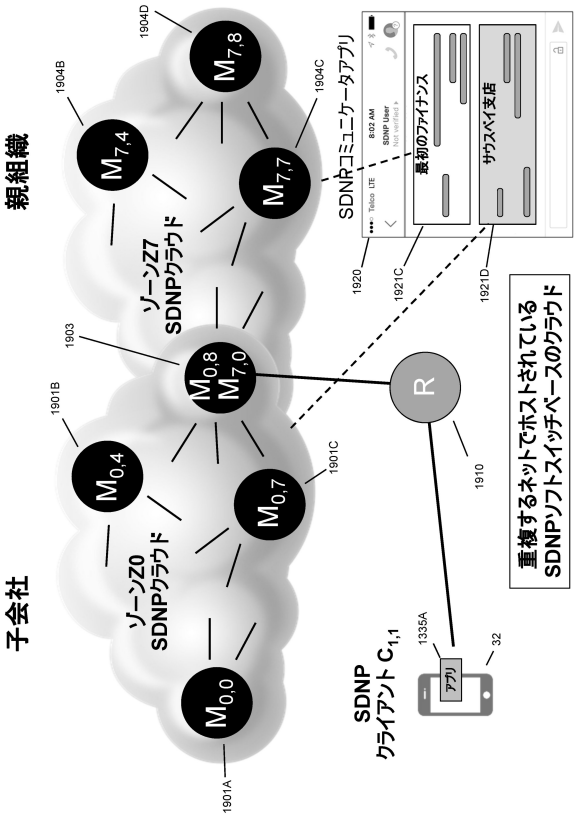
【図１１１】



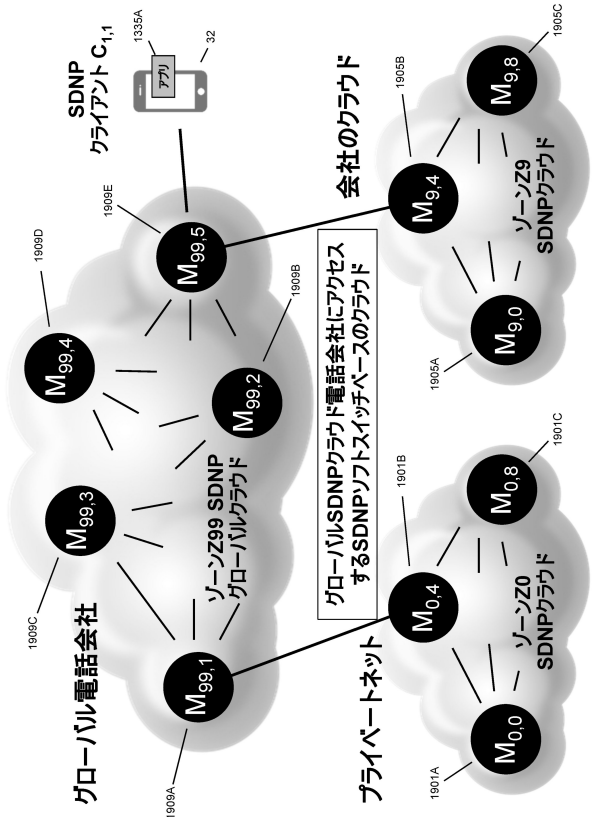
【図１１２】



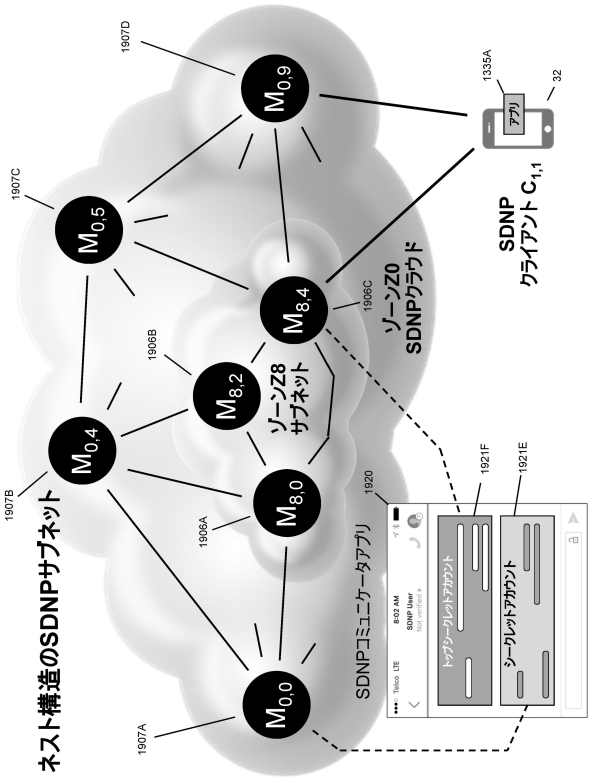
【図１１３】



【図１１４】



【図１１５】


1907D
1907C
1907B
1907A
1906A
1906B
1906C
1335A
32
アプリ
$M_{0,9}$
$M_{0,5}$
$M_{0,4}$
$M_{0,0}$
$M_{8,4}$
$M_{8,2}$
$M_{8,0}$
ネスト構造のSDNPサブネット
ゾーンZ8
サブネット
ゾーンZ0
SDNPクラウド
SDNP
クライアント $C_{1,1}$
1920
1921F
1921E
SDNPコミュニケータアプリ
トップシークレットアカウント
シークレットアカウント

フロントページの続き

ウクライナ国キエフ・２０ビー・ステパナ バンデリー アベニュー

審査官　野元 久道

(56)参考文献　米国特許出願公開第２０１６／０２１９０２４（ＵＳ，Ａ１）
特開２０１３－０４２４４５（ＪＰ，Ａ）
特表２０１３－５２５８７６（ＪＰ，Ａ）
特開２０１４－２３０１０４（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　４５／００
Ｈ０４Ｌ　６７／００