(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7496996号
(P7496996)

(45)発行日　令和6年6月10日(2024.6.10)

(24)登録日　令和6年5月31日(2024.5.31)

(51)国際特許分類

Ｈ０４Ｌ	*9/14*	*(2006.01)*	Ｈ０４Ｌ　9/14
Ｈ０４Ｌ	*9/34*	*(2006.01)*	Ｈ０４Ｌ　9/34
Ｈ０４Ｌ	*45/00*	*(2022.01)*	Ｈ０４Ｌ　45/00

ＦＩ

請求項の数　24　（全151頁）

(21)出願番号　特願2022-183881(P2022-183881)
(22)出願日　令和4年11月17日(2022.11.17)
(62)分割の表示　特願2021-500581(P2021-500581)の分割
原出願日　令和1年7月10日(2019.7.10)
(65)公開番号　特開2023-22116(P2023-22116A)
(43)公開日　令和5年2月14日(2023.2.14)
審査請求日　令和4年11月17日(2022.11.17)
(31)優先権主張番号　62/696,160
(32)優先日　平成30年7月10日(2018.7.10)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　517413960
リスタット リミテッド
ウクライナ国キエフ０４０７３・２０ビー・ステパナ バンデリー アベニュー
(74)代理人　110001379
弁理士法人大島特許事務所
(72)発明者　ベルズン、イヴゲン
ウクライナ国キエフ０４０７３・２０ビー・ステパナ バンデリー アベニュー
(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
審査官　中里 裕正

最終頁に続く

(54)【発明の名称】　クラウド通信、コンピューティング、及びグローバル電子商取引のための分散型サイバーセキュアプライバシーネットワーク

(57)【特許請求の範囲】

【請求項１】

分散型通信及びコンピュータネットワークにおける安全な通信及びトランザクション処理の方法であって、

前記ネットワークは、デジタルデータのパケットを転送し処理することができるネットワーク接続されたデバイス上にホストされた複数のソフトウェアベースの通信ネットワークノードを含み、

前記方法は、

デジタルパケットの少なくとも一部が１つ以上の隠蔽方法によって不正アクセスから保護される形態で、パケットをネットワーク上で転送するステップであって、前記隠蔽方法は、データスクランブル、暗号化、分割、混合、及びジャンクデータ挿入を含む、該ステップと、

通信ノードのネットワークを介して、パケットの経路を動的に変更するステップとを含み、

１つ以上のノードがＨｙｐｅｒＣｏｎｔｒａｃｔ（以下、「ＨＰＣＴ」と記載。）を含むパケットを送信し、前記ＨＰＣＴはジョブ記述を含み、前記ジョブ記述は、データ、ソフトウェア、及び実行可能コードを、数字シード及び暗号鍵を含むセキュリティ認証情報とともに含むデジタルファイルから構成され、前記ＨＰＣＴは、前記ＨＰＣＴがノードを通過する際に変更することがあり得、

前記ＨＰＣＴは、前記ＨＰＣＴを受信するノードが前記ＨＰＣＴの前記ジョブ記述で指

定されたタスクまたは機能を実行できるように、前記ＨＰＣＴを受信するノードの動作を決定し、影響を与え、または制御する、
方法。
【請求項２】
請求項１に記載の方法であって、
各ＨＰＣＴは、前記ＨＰＣＴで指定されたジョブを実行するために必要な機能とリソースの提供に参加するネットワークノードを指定する、方法。
【請求項３】
請求項２に記載の方法であって、
前記ＨＰＣＴは、前記ＨＰＣＴの実行に際して前記ノードが実行するタスクを指定し、前記タスクは、ネームサーバ、オーソリティノード、またはタスクノードとして機能することを含む、方法。
【請求項４】
請求項２に記載の方法であって、
前記ＨＰＣＴは、前記ＨＰＣＴで指定された前記ノードであるプライマリノードがオフラインになった場合、または指定された役割や指定されたタスクを遂行できない場合に備えて、１つ以上のネットワークノードをバックアップ・ノードとして指定する、方法。
【請求項５】
請求項１に記載の方法であって、
前記ＨＰＣＴに含まれるジョブ仕様において、ノードが２人以上のユーザーまたは発信元のなか、または間でネットワークを介した通信を行うことが規定される、方法。
【請求項６】
請求項１に記載の方法であって、
前記ＨＰＣＴに含まれるジョブ仕様において、ネットワークキャリアや固定通信網に依存しない通信ノードのアドホック・ピアツーピアネットワークを形成する無線接続機能を有するデバイスや車両が規定される、方法。
【請求項７】
請求項１に記載の方法であって、
前記ＨＰＣＴに含まれるジョブ仕様において、ネットワークノードは、前記ジョブ記述に含まれるソフトウェア、アルゴリズム、または実行可能なコードを実行するために、分散型クラウドコンピューティングを行うことが規定される、方法。
【請求項８】
請求項１に記載の方法であって、
前記ＨＰＣＴに含まれるジョブ仕様において、ネットワークノードがＩｏＴデバイスや他のエッジデバイス間のコマンドとデータの流れを管理することが規定される、方法。
【請求項９】
請求項１に記載の方法であって、
前記ＨＰＣＴに含まれるジョブ仕様において、ネットワークノードが、冗長な不揮発性ストレージとして機能するデータまたはファイルを保存、保持することが規定される、方法。
【請求項１０】
請求項９に記載の方法であって、
前記データまたはファイルがネットワークノードに保存される前に、前記データまたはファイルを断片化するステップと、
前記データまたはファイルを、前記ネットワーク上の複数のノードに分散して保存するステップと、
断片化された前記データまたはファイルの復元に必要な暗号復号化キーを前記ジョブ記述のストレージデータとともに、前記ＨＰＣＴを生成、送信、または保持するノードに戻すステップと、
前記ＨＰＣＴを生成、送信、または保持する前記ノードに、断片化した前記データまた

はファイルを元の形に復元させるように、前記暗号復号化キーを使用して断片化された前記データまたはファイルを収集及びデフラグさせるステップと、
をさらに含む、方法。
【請求項１１】
請求項１０に記載の方法であって、
前記データまたはファイルを断片化する前に、前記データまたはファイルを暗号化する、またはスクランブルを施すステップと、
前記データまたはファイルの断片化後に、前記ＨＰＣＴを生成、送信、または保持する前記ノードに、断片化した前記データまたはファイルを元の形に復元させるように前記暗号復号化キーを使用して前記データまたはファイルの復号化、またはスクランブル解除を実施させるステップと、
をさらに含む、方法。
【請求項１２】
請求項１に記載の方法であって、
前記ネットワークノードは、種類が分化するメタモルフィックなものであり、
前記ＨＰＣＴは、
・前記ＨＰＣＴの前記ジョブ記述で指定されたタスクが完了するまで、どのネットワークノードをネームサーバノードに分化させるか、
・前記ＨＰＣＴの前記ジョブ記述で指定されたタスクが完了するまで、どのネットワークノードを権限ノードに分化させるか、及び
・前記ＨＰＣＴの前記ジョブ記述で指定されたタスクが完了するまで、どのネットワークノードをタスクノードに分化させるか、
を指定し、
前記ＨＰＣＴの前記ジョブ記述で指定されたタスクが完了した後、前記ＨＰＣＴで指定された前記ネームサーバノード、前記権限ノード、及び前記タスクノードが、未分化のネットワークに戻る、方法。
【請求項１３】
請求項１２に記載の方法であって、
各ＨＰＣＴは、数値シード及び暗号鍵のうちの１つ以上を含むセキュリティクレデンシャルを含み、前記数値シード及び前記暗号鍵により、選択されたネットワークノードが拡散クラウドストレージに断片データとして格納された情報にアクセスすることが可能になり、
前記ネームサーバノードは，知る必要がある場合にネームサーバ拡散クラウドにのみ格納されたネームサーバ関連データにアクセスすることが可能で、
前記権限ノードは，知る必要がある場合に権限ノード拡散クラウドにのみ格納されている権限ノード関連データにアクセスすることが可能で、
前記タスクノードは，知る必要がある場合にタスクノード拡散クラウドに保存されたタスクノード関連データにアクセスすることが可能である、方法。
【請求項１４】
請求項１に記載の方法であって、
前記ネットワーク接続されたデバイスは、異種であり、
前記方法は、
デバイスにインストールされたすべてのノードインスタンスを、その正確さと本物であることを証明する署名付きデジタルＣＡ証明書を使用して認証するステップであって、前記ＣＡ証明書がネットワークネイティブであり、前記ネットワークにのみ知られ、第三者または侵入者が利用できないＨｙｐｅｒＳｐｈｅｒｅ（以下、「ＨＰＳＲ」と記載。）固有のアイデンティティと署名を含む、該ステップをさらに含み、
前記ＨＰＣＴは、ネットワークリソースへのアクセスを求める加盟店やサービスプロバイダによって作成される、方法。
【請求項１５】

請求項１４に記載の方法であって、
前記ＣＡ証明書は、前記ＨＰＳＲネットワーク及び前記ＨＰＣＴを作成した前記加盟店またはサービスプロバイダによって認証され、デジタル署名される、該方法。
【請求項１６】
請求項１４に記載の方法であって、
前記ＨＰＳＲは、前記ＨＰＳＲネットワーク及び前記ＨＰＣＴを作成した前記加盟店またはサービスプロバイダによって認証され、デジタル署名される、該方法。
【請求項１７】
請求項１に記載の方法であって、
前記ＨＰＣＴは、ジョブ記述を指定し、前記ＨＰＣＴにおいて前記ネットワークノードに割り当てられたそれぞれのタスクを完了したネットワークノードに対する報酬の契約を含み、
前記ＨＰＣＴの実行は、
前記ネットワークを介したデータパケットの転送を含み、前記データパケットの転送が、データパケットの各ノード間ホップに対して一意の暗号ホップコードを生成する、方法。
【請求項１８】
請求項１７に記載の方法であって、
ノードにＨＰＣＴの実行への参加を、前記ＨＰＣＴの実行の証明としてその暗号化ホップコードを取り戻すことによって確認させるステップであって、前記ノードは、データパケットを伝送することの見返りとして、前記ＨＰＣＴで契約されている報酬の一部を受け取る、該ステップをさらに含む、方法。
【請求項１９】
請求項１８に記載の方法であって、
前記ノードは、前記ＨＰＣＴにおいて契約されている報酬の一部を、交換可能な暗号通貨で受け取り、
前記方法は、
前記ノードによる前記暗号ホップコードの取り戻しを永久的な動的有向非巡回グラフ（以下、「ＤｙＤＡＧ」と記載。）またはブロックチェーンに永久に記録するステップをさらに含む、方法。
【請求項２０】
請求項１８に記載の方法であって、
前記ノードが、前記ＨＰＣＴにおいて契約されている報酬の一部を、交換不可能な暗号通貨で受け取り、
前記方法は、
前記ノードによる前記暗号ホップコードの取り戻しを、前記交換不可能な暗号通貨として永久的なＤｙＤＡＧまたはブロックチェーンに永久に記録するステップと、
前記交換不可能な暗号通貨を、交換可能な暗号通貨に変換するステップと、
前記交換不可能な暗号通貨の交換可能な暗号通貨への変換を、永久的なＤｙＤＡＧまたはブロックチェーンに永久に記録するステップと、
を含む、方法。
【請求項２１】
請求項１に記載の方法であって、
データを、
デバイス名及びそれに対応するダイナミックアドレスを識別することを含むネームサーバ機能を実施するために使用されるデータ、
タスクノードのネットワーク上のデータパケットの経路を決定することを含むオーソリティノード機能を実施するために使用されるデータ、及び、
隠蔽アルゴリズムを使用してデータパケットのコンテンツを隠蔽することを含むタスクノード機能を実施するために使用されるデータ、
のいずれかのカテゴリに細分化するステップと、

前記ノードに、前記ネームサーバ機能、前記オーソリティノード機能、または前記タスクノード機能のいずれかを実施するために必要なデータを提供するステップと、
アルゴリズムに従って、前記各カテゴリのデータをファイルに断片化するステップであって、前記アルゴリズムは、時間を含むステートに基づいており、前記ファイルの一部または全部の断片化を解除するためには鍵を必要とする、該ステップと、
ノードに、
第１のステートに従って作成されたスクランブル化アルゴリズムに従って、受信パケット内のデータセグメントの順序を変更することによって、前記受信パケットをスクランブル化する隠蔽方法、及び、
第１のステートに従って作成された暗号化アルゴリズム及び暗号化鍵に従って、前記受信パケットを暗号化する隠蔽方法、
のうちの少なくとも１つを実施させる、該ステップと、
を含む、方法。
【請求項２２】
請求項２１に記載の方法であって、
前記断片化されたデータを複数のデバイスに格納するステップをさらに含み、
どの単一のデバイスにも、前記断片化前の前記データを再構築するのに十分なコンテンツが格納されない、方法。
【請求項２３】
請求項２１に記載の方法であって、
前記ネットワーク内のゲートウェイノードが、前記ネームサーバ機能を実施するために使用される前記データから宛先アドレスを要求する、方法。
【請求項２４】
請求項２１に記載の方法であって、
オーソリティノードが、ノード間のホップ時間のテーブルを含む拡散データクラウド内のデータにアクセスすることを可能にするために、ゲートウェイノードが、前記ネームサーバ機能を実施するために使用されるデータを、前記オーソリティノードに送信する、方法。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願の相互参照）
本出願は、２０１８年７月１０日に提出された米国仮出願第６２／６９６，１６０号の優先権を主張するものである。
【０００２】
本出願は、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日に提出された米国出願第１４／８０３，８６９号、すなわち２０１８年６月１２日に発行された米国特許第９，９９８，４３４号（以降、「ＳＤＮＰ特許」とも称する）の分割出願として２０１８年４月６日に提出された米国出願第１５／９４６，８６３号の一部継続出願である。
【０００３】
本出願はまた、２０１５年７月２０日に提出された上記米国出願第１４／８０３，８６９号、即ち２０１８年６月１２日に発行された米国特許第９，９９８，４３４号の一部継続出願であり、２０１７年４月３日に提出された米国仮出願第６２／４８０，６９６号の優先権を主張するものでもある、２０１８年４月２日に提出された米国出願第１５／９４３，４１８号の一部継続出願である。
【０００４】
前述の各出願は、その全体が参照により本明細書に組み込まれている。
【背景技術】
【０００５】

グローバルテレコミュニケーション、コンピュータネットワーキング、及びインターネットの到来は人間社会に多大なインパクトを与え、その影響は家庭、家族、仕事、娯楽、旅行、ソーシャライジングといった人々の日常生活のあらゆる側面に及んでいる。今日のインターネットは、エネルギー生産・配電制御、円滑な通信、交通システム、発送、製造（ロボット化など）、監視、法執行支援のように、社会的基盤としても欠かせない役割を果たしている。ネットバンキング、ＡＴＭ、電子送金、オンライン取引、ＰＯＳ（販売時点情報管理）などからも、フィンテックや電子商取引におけるインターネットの幅広い役割が見て取れる。デバイスのネットワーク接続、いわゆる「ＩｏＴ（モノのインターネット）」や、Ｖ２Ｉ（路車間）及びＶ２Ｖ（車車間）通信ネットワークによる自動車のネットワーク接続により、世界の隅々にまでインターネットの裾野が広がった。また近年は、デジタルアイデンティティ、分散台帳、ブロックチェーン、暗号通貨の出現によって、従来のブリック＆モルタル型の取引には相当するもののない、新たな形の電子商取引が誕生した。

【０００６】

インターネットはセキュリティやプライバシーを念頭に置いて開発されたものではなく、トランザクションやデータはインターネット上で転送されるため、ワールドワイドウェブではプライバシー、セキュリティ、及びデータインテグリティを保つ目的で、暗号化技術、暗号文、及び符号が広範に使用される。プライバシーを高める他の方法として、分散化、即ち中央制御、ネットワークオペレータ、及び信頼の置ける認証局への依存性を排除した手法があり、これらの手法では分散型アプリケーション（ｄアプリ）、即ちネットワークオペレータが存在しないＰ２Ｐ（ピアツーピア）ネットワーク上で、スマートコントラクトを利用して運用されるアプリケーションが使用される。スマートコントラクトとは、第三者の関与を受けずに契約の交渉や履行をデジタル的に推進、検証、実施するために採用された、暗号化及びブロックチェーンに基づく契約をいう。

【０００７】

プライバシー派の人々は、暗号化に基づく電子商取引は世界を変える技術であり、法的権威や政府機関が介在しなくても、信頼の置ける事業契約や個人的合意のトランザクション整合性が約束されると主張する。暗号化契約の潜在的適用分野は幅広く、電子記録サービス、電子購入契約、サプライチェーン管理、バンクレス送金、権利譲渡のブロックチェーン記録、弁護士を伴わない遺言状、信託、財産分与の執行など多岐にわたる。

【０００８】

中央銀行や認証局の手を借りずに「信頼の置ける」取引や契約を行えることから、契約者の経費削減（もしくは経費の完全撤廃）と契約の高速化・効率化の両立が可能となり、取引コストを抑えながら事業収益性を改善することができる。特に、法的及び金融的権限の分散化には、競争を促し、サービスを改善し、手数料を引き下げ、リスクをとりたがらない業界にイノベーションをもたらすという潜在的メリットがある。

【０００９】

特に金融業では、暗号化ブロックチェーン技術は独占的で、専制主義的で、難解で、時代遅れでさえある巨大金融機関の連携業務方式に取って代わる分散型の柔軟な選択肢として大きな魅力がある。中央権力への依存性がなくなるため、ブロックチェーン技術では金融取引の完全性と透明性を高め、安全な支払い、送金、電子商取引、保険契約を実現することができる。

【００１０】

金融業界に対する潜在的メリットだけでなく、ブロックチェーン技術はマーケティングチャネルとして、また柔軟な資金調達手段として、新興テック企業にとっても有益なことが既に証明されている。分散型ブロックチェーンに基づく契約は、潜在的に大きな力を持つ破壊的な市場の流れであり、サプライチェーン管理やサプライチェーン契約、監査に耐え得る記録、及びプロセスオートメーションを推進し、起業家を顧客やキャピタルファンディングに結び付けることにより、ＳＭＢ（中堅・中小企業）がそれより遙かに巨大な企業に効果的に対抗することを可能にする。分散化は、大企業がビッグデータへのアクセス

を仕切るのではないかという懸念に対する答えにもなる。これは、市場データのアクセスや制御を独占できる企業は一つとして存在しないためである。この点で、ブロックチェーンは事業の「民主化」をもたらす可能性を秘めている。

【００１１】

暗号化、分散化、スマートコントラクト、ブロックチェーン技術、及び暗号通貨をインターネット上に適切に展開し、それらを組み合わせて利用するには、個人及び企業をハッキングから保護し、少数企業による寡占的支配や違法なカルテルを阻止し、サイバー犯罪者による、疑うことを知らない消費者に対する詐欺やなりすまし犯罪を防ぐ必要があると言われる。政府による不正な監視を防止したり、（Ｇｏｏｇｌｅ（登録商標）、Ａｍａｚｏｎ（登録商標）、Ｆａｃｅｂｏｏｋ、Ｍｉｃｒｏｓｏｆｔのような）今日の巨大ネットワーク企業によるパーソナルプロファイリングを妨害する手段としても、同様の手法が宣伝されている。これら事業者の繁栄ぶりから、ブロックチェーンエンスージアストの中には、（ブロックチェーンは単一の不変な台帳から成り立っているため）詐欺への対抗やプライバシー保護だけでなく、インターネットの保護にもブロックチェーン技術を利用できるはずだと主張する者もいる。その背景には、ブロックチェーンそのものがセキュアで、ハッキングとは無縁だという前提がある。しかし、その主張は傾聴に値するものだろうか。ブロックチェーンを利用したとしても、今日の脆弱性が新しいものに置き換わるだけではないだろうか。

【００１２】

さらに言えば、今日における暗号化の広範な利用によって、オンライン詐欺、ハッキング、なりすまし犯罪、バンキング・送金詐欺、インフラ攻撃が実際に減少しているという主張には裏付けがあるのだろうか。トランザクション暗号化のセキュリティ上のメリットは幻想ではないだろうか。

【００１３】

Ｉ．ネットワークの脆弱性及び不完全性

【００１４】

データ漏洩、サイバー攻撃、遠隔監視についての報道が相次ぐ中、インターネットにはセキュリティがなく、プライバシーへの備えが不十分なことは広く知られている。２０１７年のサイバー犯罪の被害額は４，４５０億ドルを超えたと推定されている。２０１８年には、被害額は報告されたものだけでも史上最高の６，０００億ドルに達し、それ以外に報告されていないもの、露見していないものも存在する。さらに、２０１９年の被害額はその１．５倍に跳ね上がると見込まれている。このことから分かるように、暗号化ではサイバー攻撃に対抗できず、そのレベルは専門家が求める、または可能だと考える水準に達していない。

【００１５】

プライバシー攻撃はそれよりさらに蔓延しているが、盗まれた個人情報がどのように使われたかが定かではないケースも含まれるため、被害額の算定は難しい。ソーシャルメディア、販売店、個人信用調査機関、保険代理店、金融機関における顧客情報のぞんざいな扱いも一因ではあるが、アイデンティティ情報盗難では、インターネットがサイバー犯罪者にとっての絶好のプラットフォームとなるだけでなく、ターゲットの「プロファイリング」、即ちサイバー攻撃の効果を最大限に高めるための情報収集に便利な環境にもなっている。

【００１６】

よく知られているように、セキュリティとプライバシーを保つ秘策があると主張する「専門家」やベンダーは巷に溢れているが、それならなぜサイバー攻撃の数、頻度、被害が減るどころか、増える一方なのだろうか。少なくともその答えの一端は、ネットワーク脆弱性は複数の要因がからんだ多元的問題であることにある。これらの要因には、旧式のシステムに依存していること、通信リンク（サイバー攻撃の侵入ポイント）がセキュアではないこと、ソーシャルメディアに個人情報やプライベート情報が掲載され、そうするように推奨もされていること、クラウドが気軽に利用されてしまうことなどがある。また一般

に、データやトランザクションのセキュリティを保護する唯一の手段として、暗号化が（宗教的というほどではないにしろ）幅広く過信されていることも一因に挙げられる。

【００１７】

さらに、ブロックチェーン技術ならインターネットを保護できるという無邪気な主張も正しいとは言えない。ブロックチェーントランザクションはインターネット上で発生するため、インターネットの通信プロトコルＴＣＰ／ＩＰへの攻撃によって、ブロックチェーントランザクションはすべて攻撃に晒され、ブロックチェーンデータの漏洩や不可逆的改竄が引き起こされる危険性がある。トランザクションの実行にインターネットが使われることから、ブロックチェーンではインターネットを保護することはできない。

【００１８】

ネットワーク接続

【００１９】

サイバー攻撃の性質と、ネットワーク接続デバイスの脆弱性の原因をさらに理解するには、まず接続デバイスのアーキテクチャと動作原理を考える必要がある。図１には、オペレーティングシステムファームウェアとアプリケーションソフトウェア、及びそれらを実行するハードウェアプラットフォームからなるネットワーク接続デバイスの基本構成が示されている。このブロック図の記述は、高速サーバ、携帯電話機、ノートＰＣ、タブレット、ならびにＷｉＦｉ、Ｅｔｈｅｒｎｅｔ、衛星通信、及びＤＯＣＳＩＳ３（ケーブル通信）用ルータ、家電製品、ファクトリーオートメーション、セキュリティシステムなどで使用されるＩｏＴデバイス、及び自動車などの車両向け通信・制御モジュールに等しく当てはまる。

【００２０】

この図に示されているように、一般的デバイスのハードウェアは、マイクロコントローラやマイクロプロセッサといった演算コア３、ディスプレイ、キーパッド、タッチパネル、ポート、周辺機器、センサーのようなインターフェイスとの入出力接続から構成されるＩ／Ｏ　４、ならびにフラッシュメモリなどの不揮発性メモリ及びＤＲＡＭ、ＳＲＡＭなどのスクラッチパッドメモリから構成されるデータストレージ２から成り立っている。これらのハードウェアコンポーネントはハードウェア固有のデバイスドライバ１によって制御され、それがオペレーティングシステムカーネル６とともにデバイスのホストオペレーティングシステム（ＯＳ）を構成する。このうち、デバイスドライバ１は、メーカー固有のハードウェアコンポーネントの制御をハードウェアに依存しない汎用命令セットに変換し、オペレーティングシステムカーネル６は、デバイス上で通信やアプリケーションを実行できるように、ハードウェアコンポーネントのスケジューリングとリソース管理を行う。

【００２１】

この機能にはＯＳＩ通信スタックの管理が含まれ、この通信スタックは通信ネットワーク上の近接（ローカル）デバイスとの物理信号通信リンク１６を扱う物理ＰＨＹ及びＭＡＣ通信ブロック５、ローカルルータ経由で全体ネットワークやインターネットとの間で交換されるＴＣＰ／ＩＰデータグラム通信１５の管理に使用されるＴＣＰ／ＩＰブロック７、及びアプリケーションソフトウェアをホスティングする仮想マシン（即ちアプリケーション領域）として使用されるＯＳアプリケーションＶＭ　８から構成される。このソフトウェアアプリ領域では、ホストＯＳネイティブアプリケーション１１、オンラインアプリ１２、ローカルブロックチェーン処理ＢＣＰ　９、ブロックアプリケーションＢＣアプリ１０のような、あらゆる種類のソフトウェアアプリケーションを実行することができる。また、アプリケーション固有のドライバ及びアプリＵＩ／ＵＸ　１３は、アプリケーションとユーザとの間のユーザインターフェイス（ＵＩ）の制御、及びユーザが行った操作に対するデバイスの反応（ユーザエクスペリエンス即ちＵＸ）の管理を行う。

【００２２】

この図に示された統合システムは、ユーザからコマンドを受け取り、タスクを実行し、ＴＣＰ／ＩＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ－Ｃｏｎｔｒｏｌ－Ｐｒｏｔｏｃｏｌ／Ｉｎｔｅｒｎｅｔ－Ｐｒｏｔｏｃｏｌ）に準拠した他のデバイスと通信ネットワークを介して通

信することができる。７階層ＯＳＩ（Ｏｐｅｎ　Ｓｙｓｔｅｍｓ　Ｉｎｔｅｒｃｏｎｎｅｃｔｉｏｎ）標準に従った７つの抽象化層を備えることで、技術やメーカーが全く異なるデバイス間でのＴＣＰ／ＩＰによる相互運用が実現される。この相互運用性は、インターネットが人間社会に及ぼした多大な影響、及びインターネットによる今日の商取引実現の鍵となった機能である。ネットワーク通信のあらゆることが規定されていることから、ＯＳＩ開放型システム標準はインターネットの最大の弱点、即ちサイバー攻撃に対する全面的及び不可避の脆弱性をも表現している。

【００２３】

セキュリティ攻撃やプライバシー攻撃には様々な形があるため、その分類や整理を行える統一的な分類法は存在しない。とは言え、攻撃ベクトル（脆弱性）をいくつかの種類、即ち（Ａ）ネットワーク攻撃、（Ｂ）信頼関係攻撃、（Ｃ）データ漏洩、及び（Ｄ）ブロックチェーン攻撃に分類すると便利である。これらの攻撃は転送中のデータを横取りしたり、トランザクションを改竄したり、ネットワーク接続デバイスにマルウェアを感染させたりすることで行われる。

【００２４】

ネットワーク攻撃

【００２５】

ネットワーク攻撃とは、ネットワーク接続やネットワーク通信を介して行われるサイバー攻撃である。ネットワーク攻撃は、通信ネットワークやコンピュータネットワークに「不正アクセス」したり、これらのネットワークを監視することで、情報を入手したり、パケットトラフィックをリダイレクトしたり、企業活動に干渉（業務妨害）したり、詐欺、盗難、不正行為を働くことを指す。ＤＯＳ（サービス妨害）攻撃もネットワーク攻撃の一種と考えることができる。また、送金詐欺、取引詐欺、ＣＡ証明書詐欺のような信頼関係攻撃や、マルウェア拡散の手段としても、ネットワーク攻撃が頻繁に使用される。ネットワークスニッフィング、スヌーピング、スパイングが、プロファイリング、プライバシー攻撃、アイデンティティ情報漏洩に関与することもある。

【００２６】

サイバー攻撃を可能にしているネットワーク通信の特徴の一つに、ＴＣＰ／ＩＰにおけるパケットルーティングの方法がある。図２に示されているように、インターネットのようなパケット交換方式のデータネットワークでは、データは複数のデジタルデータパケット（データフレーム）としてネットワークに送出される。左から順に見ていくと、データパケット３７の先頭には、デバイスからネットワークへのローカル接続の確立に使用される情報が格納され、その後に、２つのＩＰアドレス及び１つのペイロードからなるデータグラムが続く。レイヤ１ヘッダーと呼ばれるＬ１データでは、ユーザデバイスをネットワークゲートウェイデバイスの電気的、光学的、または無線式リンク（物理信号層またはＰＨＹ層）に接続するために必要なタイミングが定義され、Ｌ２（レイヤ２）データでは、データ転送メディア及びＭＡＣ（メディアアクセス制御）アドレスの解釈に必要なデータプロトコル及びアドレスが記述される。例えば、図中のタブレット３０は、該当するＷｉＦｉ標準（８０２．１１ａｃなど）に従って、双方向マイクロ波無線リンクを介して、定められた周波数（１．８　ＧＨｚなど）で、ＯＦＤＭ（直交周波数分割多重）と呼ばれる特定の方式で変調されたデータを使用してＭＡＣアドレスを交換することにより、ＷｉＦｉルータ３１との無線リンクを確立する。

【００２７】

Ｌ１／Ｌ２ヘッダーの後には送信元ＩＰアドレスと宛先ＩＰアドレスが続く。送信元ＩＰアドレスでは（応答を返す先が受信側に分かるように）送信元デバイスのデジタルＩＰアドレスが定義され、宛先ＩＰアドレスではデータの最終的な受け取り先が定義される。図に示されているように、タブレット３０のＩＰアドレスはIP_{TB}であり、これが送信元ＩＰアドレスとなる。また、アドレスIP_{CP}は宛先ＩＰアドレスであり、これは携帯電話３６のＩＰアドレスを指す。データ転送時に、タブレット３０からルータ３１に渡されたデータパケット３７は、ＷｉＦｉルータ３１の内部にあるルーティングテーブル４０

で定められた情報に従って、クラウド４１上のサーバ３２ａかサーバ３３のどちらかに送出される。ルーティングテーブル４０によってサーバ３２ａが選択された場合は、データパケットはイントラクラウド接続３９を介してサーバ３２ｂへ、さらにサーバ３２ｃへと渡されて行き、最終的にクラウド４１からモバイルネットワーク通信塔３５を介して携帯電話３６に到達する。反対に、ルーティングテーブル４０によってサーバ３３が選択された場合は、無線リンク３８を介してサーバ３４へ、そこからさらにモバイルネットワーク通信塔３５、携帯電話３６へとルーティングが行われる。

【００２８】

（テーブル４０のような）ルーティングテーブルはサーバ３２ａ、３２ｂ、３２ｃ、３３、３４の内部にも存在し、それによってＷｉＦｉルータ３１で最初の通信パスが決定された後のルーティングが決められる。従って、タブレット３０にはデータパケット３７のインターネット上の転送経路を決める権限はない。例えばルータ３１で、マルウェアに感染したサーバを経由するパスが選択されたとすると、データパケット３７のセキュリティとペイロード整合性が危険に晒され、それ以降のすべてのパケットルーティングで、悪意のあるハイジャッキングや転送先書き換えが行われてしまう可能性がある。

【００２９】

従って、インターネットパケットルーティングがネットワーク攻撃のリスクに晒されていることには、（ｉ）通信の両方の側がＩＰアドレスで識別される、（ｉｉ）データパケットがネットワーク上でそのままの形で転送される、及び（ｉｉｉ）送信元デバイスはデータのネットワーク転送経路に影響を及ぼさないという３つの理由がある。加えて、ＴＣＰ／ＩＰデータグラムの内容は、「開放型システム間相互接続参照モデル」と題された１９８４年のＩＳＯ文書で標準化された、ＯＳＩ７階層モデルに基づく標準化されたフォーマットに従っているため、ハッカーらは容易にパケットの内容を分析し、脆弱性を特定できてしまう。

【００３０】

図３には、ＯＳＩ７階層通信スタック５０ａ及び５０ｂ、ならびにデータパケットの構成が示されている。運用時には、スタック５０ａ及び５０ｂの各層は、それより下位の層に処理を行わせ、それより上位の層のために処理を行う。従って、それぞれの層は、１つ下の層との間で、定められた規定に従ってデータ交換が行われている限りは、下位層でどのように処理が行われるかは気にしない。同様に、上位層についても、その層のための処理を行えていて、規定に従ってデータの送受信ができている限りは、上位層でデータがどのように利用・作成されるかは気にしない。このように、他の層についての詳細な知識を必要とすることのないように、層ごとの役割分担と通信機能切り分けが実現されている。

【００３１】

オープンアーキテクチャに抽象化層を採用すると、公正な競争が促される。ＳＭＢであっても、急成長しているインターネットやワールドワイドウェブ（ＷＷＷまたはウェブ）への自由な商用アクセスを行える。特定の企業、技術、政府によって方針を一方的に押し付けられたり、限を制約されることもない。インターネットに接続するうえで、登録も中央権力の承認も必要としない。ＯＳＩ標準に従って、あらかじめ定められた抽象化層を導入するだけで、他のネットワーク接続デバイスについての知識がなくても、デバイス間の信頼性の高いネゴシエーションと通信を行える。さらに詳しく言えば、ＯＳＩの７つの層はそれら全体を合わせて、物理インターフェイス（電気信号、電磁波、または光）、ならびに信号の解釈に使用されるデータ処理用ハードウェア及びソフトウェアを表現した単一の「プロトコルスタック」となる。運用時には、データはネットワーク接続デバイス間で受け渡され、それらのデータを、コンピューティング、データベース、ロボティクス、ＩｏＴ、及びセキュリティ分野のアプリケーションを実現するための、または汎用ハードウェア抽象化層（ＨＡＬ）としての、デバイスごとの独立した抽象化層で利用することができる。インターネットのプロトコルスタックは、ビジネスサービスや、非技術系のその他の業種、金融取引、バンキング、発送などにもリンクさせることができる。

【００３２】

以下の表に示されているように、ＯＳＩ　７階層モデルは、物理メディアを介してデバイスをネットワークに接続するための２つの下位層、インターネット上のパケットルーティングを制御する２つの中位層、及びネットワークアプリケーションの管理を行う３つの上位層から構成される。

【００３３】

【表１】

階層名	機能／特徴
７　アプリケーション層	ＡＰＩ、ＢＣ、ＰＫＩ、Ｔｅｌｎｅｔログイン、ファイル転送ＦＴＰ、ＣＡ証明書／Ｌ７処理、ＩＭＡＰメール処理、ＳＭＴＰ、ＤＣＯＭ演算、ＤＮＳ、ＤＨＣＰ、ＮＴＰ、ＴＬＳ／ＳＳＬネットワーキング
６　プレゼンテーション層	暗号カプセル化、圧縮、ＣＡ証明書／Ｌ６処理、符号化、変換、ＥＢＣＤＩＣ／ＡＳＣＩＩ、ＰＤＦ、ＭＰＥＧイメージ化、文書セキュリティ
５　セッション層	セッションイニシエーション、ＣＡ証明書／Ｌ５処理、アクセス権付与、全二重／半二重通信、セッション復元、ＳＯＣＫＳ、ＰＰＴＰトンネリング
４　トランスポート層	転送の信頼性とハンドシェーキング（ＴＣＰ／ＵＤＰ）、ポートアドレッシング、転送セキュリティセレクタ（ＳＳＬ／ＴＬＳ）
３　ネットワーク層	ＩＰｖ４／ＩＰｖ６、ＩＰルーティング、ＩＰアドレッシング、トラフィック制御、ＴＴＬ、ＩＣＭＰ、ＰＩＭマルチキャスト
２　データリンク層	Ｅｔｈｅｒｎｅｔ、ＷｉＦｉ、３Ｇ／ＬＴＥ、４Ｇ、５Ｇ、ＤＯＣＳＩＳ３プロトコル、セキュリティＷＥＰ、ＷＰＡ２に準拠したＭＡＣ（メディアアクセス制御）接続
１　物理（ＰＨＹ）層	タイミング制御、同期処理、デジタル（電子的）信号、無線信号、マイクロ波信号、光信号を含む、シンボル（ビット）としての信号転送

【００３４】

デバイス間の通信では、アプリケーション層で処理されたデータが必要に応じて暗号化された後、スタックの下位層へと渡されて行く。この一連の処理の中で、データは転送命令やＩＰアドレスルーティング情報とともにＩＰダイアグラムの中にカプセル化され、デ

ータリンク層（レイヤ２）固有のプロトコルを使用してＰＨＹ層から相手側デバイスに送られる。パケットが宛先ＩＰアドレス及び宛先ポートに届くと、検証と復号化の処理を経た後、それがスタックの上位層へと渡されて行き、アプリケーション層に到達して処理が行われる。７階層抽象化モデルは一般的なものだが、インターネットではＴＣＰ／ＩＰプロトコル及びＴＣＰ／ＩＰネットワークスタックが採用されている。ＴＣＰ／ＩＰはＴｒａｎｓｍｉｓｓｉｏｎ Ｃｏｎｔｒｏｌ Ｐｒｏｔｏｃｏｌ ／ Ｉｎｔｅｒｎｅｔ Ｐｒｏｔｏｃｏｌの頭字語である。

【００３５】

図３に示されているように、物理接続はＰＨＹ層（レイヤ１）でしか行われないが（実線部）、各通信デバイスペアはレイヤ単位で仮想的に動作し（点線部）、トランスポート層（レイヤ４）は相手側デバイスのトランスポート層（レイヤ４）と、セッション層（レイヤ５）は相手側のセッション層（レイヤ５）とのように、対応するレイヤ同士の間で通信が行われる。従って、セキュリティ脆弱性はデータ層ごとに存在する。特に、パケットのペイロードが格納されるレイヤ７データには、ユーザＩＤ情報、パスワード、ログインファイル、実行コード、ブロックチェーンデータ、暗号通貨などの情報が含まれるため、危険に晒されやすい。図３に示されたＴＣＰ／ＩＰデータの脆弱性の例としては、次のものが挙げられる。

・ＰＨＹデータ５１。レイヤ１データフレームの脆弱性（信号インターセプト、ジャミングなど）。

・ＭＡＣデータ５２。レイヤ２データフレームの脆弱性（ＩＤスニッフィング、パケットスニッフィング、プロファイリング、ＤｏＳ（サービス妨害）攻撃、ＷＰＡ／ＷＰＡ２（ＷｉＦｉ Ｐｒｏｔｅｃｔｅｄ Ａｃｃｅｓｓ）ハッキングなど）。

・ネットワークデータ５３。ＩＰルーティング、ＤＮＳネームサーバ、及び静的アドレッシングにおけるレイヤ３データグラムの脆弱性（ＭｉＭ（中間者）攻撃、パケットのハイジャッキング及びリルーティング、スニッフィング及びパケットレコーディング、スプーフィング（インポスター）攻撃、ＤｏＳ（サービス妨害）攻撃など）。

・トランスポートデータ５４。レイヤ４データグラムの脆弱性（静的及び事前割当（固定）ポート番号のポートバンギング、ＴＣＰプロトコルのエクスプロイト、ＳＳＬ／ＴＬＳのエクスプロイト及びブルートフォース暗号解読、メタデータ収集及びユーザプロファイリング、トラフィックモニタリング、ＤｏＳ（サービス妨害）攻撃など）。

・セッションデータ５５。アイデンティティ処理、信頼関係処理、及びアドホックネットワーク確立におけるレイヤ５セッションの脆弱性（ＣＡ（認証局）詐欺、暗号鍵窃取、マルウェアのインストール、プライバシー攻撃、ＭｉＭ（中間者）攻撃、ＤｏＳ（サービス妨害）攻撃など）。

・プレゼンテーションデータ５６。暗号化及び信頼関係処理に関するレイヤ６ペイロードの脆弱性（内容が暗号化されていない、暗号強度が弱い、暗号鍵窃取、プロファイリングによる暗号鍵推定、盗まれた暗号鍵を利用したＭｉＭ（中間者）攻撃、インポスターエクスプロイト、マルウェア攻撃（バックドア、キーロガー、トロイなど）、プライバシー攻撃、ＤｏＳ（サービス妨害）攻撃など）。

・アプリケーションデータ５７。データ及び内容に関するレイヤ７ペイロードの脆弱性（マルウェアのインストール、ＭｉＭ（中間者）攻撃、資産窃取、暗号通貨窃取、ウォレット窃取、ログインのエクスプロイト及びリダイレクト、ＯＳ乗っ取り、プライバシー攻撃及び信頼関係攻撃、ブロックチェーン攻撃、ブロックチェーン改竄、データベース改竄、アイデンティティ情報窃取、アカウントのブロッキング、アカウント奪取、ブロックチェーンに対するサラウンド攻撃及びＤｏＳ（サービス妨害）攻撃、アプリケーションに対するＤｏＳ（サービス妨害）攻撃など）。レイヤ７の脆弱なペイロードデータ５７ａには、ソフトウェアコード、ブロックチェーンデータ、スマートコントラクト ５７ｂを含む暗号通貨などがある。

【００３６】

メタデータ及びルーティングの脆弱性

【００３７】
ＴＣＰ／ＩＰ通信には、データパケットの中にデータグラムのルーティングに必要なデータを組み込む必要があり、その情報は転送中に参照できなければならないため暗号化することができないという、不可避の脆弱性が存在する。これらのデータとは、レイヤ１からレイヤ６までの伝送ブロック（サブパケット）の内容を指す。そこに収容されるデータ５１からデータ５６までは、インターネットのパケットルーティングに必要なため、暗号化されない。
【００３８】
このような、ＩＰパケットが横取りされた時に覗き見される可能性のある情報には、レイヤ２の送信元デバイスのＭＡＣアドレス（及び送信側のサブネット）、レイヤ３の送信元及び宛先ＩＰアドレス（実質的に通信者の身元情報）、使用されているデータ転送プロトコル（ＵＤＰ、ＴＣＰ）、レイヤ４の送信側及び受信側デバイスのポート番号（メール、ＶｏＩＰといったサービスタイプの判別が可能）、レイヤ５のデータ（通信者の認証を行い、「セッション」と呼ばれる継続的な情報交換を開始する処理に関係する情報）などがある。
【００３９】
これらのデータ全体をまとめて「メタデータ」という。政府職員はメタデータを定期的に監視、収集、保存して、対象者の行動の調査分析を行っている。国がネットワークトラフィックを監視できるのであれば、マフィア、ギャング、犯罪集団も、同じように敵対者のプロファイリングを行える。パケットのメタデータの中で本当に危険なのは送信元ＩＰアドレスである。特定のデバイスまで、そして最終的にはそのデバイスを使用している人物の身元まで辿ることのできる情報だからである。身元が知られてしまえば、その人物のデータトラフィックを監視し、行動パターンを分析し、ソーシャルメディアから当人の情報をさらに引き出し、最終的にはパスワードやＩＤ情報を盗んでアカウントを乗っ取ることができてしまう。
【００４０】
攻撃者が携帯電話ネットワークに不正にアクセスできたとすると、デバイスと通信している携帯電話基地局からの信号強度の強弱から、三角測量の要領で発信者の携帯電話の位置も知られてしまう。たとえＧＰＳをオフにしていたとしても、デバイスの位置が特定され、その動きを追跡されてしまうことになる。これは、犯罪者、ギャング、誘拐犯、人身売買人、猥褻犯が、次の犯行の時間と場所を選ぶうえで、警察を出し抜くのに極めて有効な情報となる。また、ＩｏＴクラウドがハッキングされたとすると、犯罪者が監視カメラを利用して警官の居場所を把握したり、その映像を参考にして、犯行に最適な時間と場所を選定したりすることが可能になる。
【００４１】
ユーザのプロファイリングを行わなかったとしても、ハッカーは暗号化されないレイヤ６のデータを調査することで、ペイロード暗号化のコーディングに関する情報を知ることができる。この情報から、ブルートフォース（総当たり）攻撃による暗号鍵解読、（誕生日、犬や猫によく付けられる名前のような）パスワード推定、対象者のデバイスへのスパイウェア感染といった手段がとられることになる。単純なブルートフォース攻撃は、プロファイリングを利用した攻撃に比べると成功の確率は低いが（後者では、攻撃者は対象者の個人情報を利用することができる）、最近のブルートフォースハッカーらはクラウドコンピューティングを導入し、数百万台のコンピュータの演算能力を駆使してパスワード推測や、コードの暗号鍵解読を行っている。クラウドコンピューティングを利用して、今日の最高速のスーパーコンピュータの演算能力を集約させると、「解読不可能」とされている暗号も驚くほど短時間で解読されてしまう。今後は量子コンピューティングの到来によって事態は一層悪化し、攻撃が一層容易になると予想される。
【００４２】
セッション層（レイヤ５）の脆弱性
【００４３】

インターネット通信には、レイヤ５のセッションを使用しないと通信の両者間のデータ交換を行えないという、特に本質的な弱点が存在する。ＴＣＰ／ＩＰの「セッション」機能を使用しなければ、ネットワーク経由で送出される各パケットが本物かどうかを１つ１つ確認しなければならない。それでは時間がかかり、インターネット通信速度が極端に低下してしまう。データトラフィック量も手に負えないほど増大し、リアルタイムの通信やビデオが不可能になってしまう。その代わりに、通信を開始する時に、暗号鍵を使用するか、信頼性ＣＡ（認証局）から発行される署名付きデジタル証明書を交換するかのどちらかの方法で、２台のデバイス間で情報交換を行い、チャネルを開くための「信頼関係」を築くという手法がとられる。

【００４４】

いったん信頼関係が築かれると、２台のデバイスは仮想チャネルで結ばれる。それ以降に適切なデジタル証明書を付けて送られたデータはすべて、真正なものとして「信用」され、疑われずに受け取られることになる。セッションの使用例の一つに、顧客が銀行口座にアクセスするために、銀行とのオンラインセッションを開くケースがある。その場合、ログインが行われた時に、口座所有者の身元確認が行われ、ＴＣＰ／ＩＰセッションが確立される。このセッションが開かれている間に実行される取引では、さらなる身元確認は必要とされず、ＩＤ認証は不要となる。

【００４５】

本質的に、セッションとは通信の両側のＩＰアドレス、及びセッション開始時に交換されるセッションセキュリティ証明書によって容易に識別可能なデバイス間通信チャネルである。もしハッカーが、セッション開始時に自分のデバイスをセッションに割り込ませる方法を見つけたとすると、送信側と受信側との間で受け渡される情報にすべてアクセスできてしまう。セッションのペイロードには、銀行口座番号、パスワード、個人資産、契約書、画像、映像、チャット履歴、企業機密情報、クレジット履歴、診療データ、納税情報、社会保障支払費、保険金受給記録などが含まれている可能性がある。不審に思わない通信者は、自分のコミュニケがハックされていることにまったく気付かないため、ＭｉＭ（中間者）攻撃またはパケットハイジャッキングと呼ばれるこの種の攻撃は、特に悪質性が高い。ＭｉＭ攻撃では、攻撃者が偽のＣＡ証明書を使用して認証を突破し、「不正セッション」トークンを使用して正当なセッションを開くことで、レイヤ５のセキュリティ機能をすべてすり抜ける手口が使われることもある。この手口は、かつて猛威を振るい、犯人自身のものも含めて世界中のコンピュータを感染させた悪名高いウイルス、Ｓｔｕｘｎｅｔの感染拡大に使われた。

【００４６】

トロイの木馬を利用して、メインアプリケーションの実行ファイル（ブラウザなど）と、そのセキュリティ機能やセキュリティライブラリとの間のコールを操作することで、証明書を盗み取る手口も存在する。ＳＳＨダウングレードエクスプロイトでは、攻撃者はクライアントとサーバを騙して、セキュリティの低いプロトコルを使わせたうえで攻撃を続行し、悪意のあるセッションを使用して情報収集や詐欺を働く。偽のセッションを開いて「セッション層マルウェア攻撃」を行い、ゼロデイエクスプロイト、タイムボム、ウイルス、ワームのようなマルウェアをシステムに送り込むことも可能である。

【００４７】

プレゼンテーション層（レイヤ６）攻撃

【００４８】

一般に、レイヤ６攻撃ではセキュリティ証明書と「暗号鍵」を盗む手口が使われる。これらの攻撃では、偽造証明書を使用してレイヤ５の認証を突破する手口と同じ手法が使われることが多い。暗号化は、セキュリティとプライバシーを保つ手段として、事実上すべてのインターネットデータパケットで利用されているため、レイヤ６やレイヤ７で転送される暗号鍵が攻撃されると、ほとんどのコミュニケがスパイングや犯罪に晒されてしまう。このようなエクスプロイトでは、セキュリティが破られ、プライバシー保護が一切効かなくなるだけでなく、プレゼンテーション層（レイヤ６）マルウェアによって、ＰＤＦリ

ーダー、メディアプレーヤー、広告ブロッカー、ディスクデフラグユーティリティのような一見無害に見えるユーティリティの形で、悪意のあるコードがインストールされてしまう可能性もある。

【００４９】

暗号鍵窃取の手口の一つとして、最初に接続が行われた時の、第三者の暗号鍵サーバからの１つまたは複数の暗号鍵の配布を察知する手法がある。例えば、「セキュア」だとされているパーソナルメッセンジャーから、インターネットを介してオープンに鍵が配布されたとする。この鍵が横取りされると、「Ｅ２Ｅ（エンドツーエンド）」暗号化のセキュリティが破られてしまう。また、Ｅ２Ｅ暗号化を破ることは不可能とされているが、Ｌｉｎｅ、ＫａｋａｏＴａｌｋ、ＷｈａｔｓＡｐｐ、ＷｅＣｈａｔといったＶｏＩＰパーソナルメッセンジャーがハッキングされたり、プライベートな通信が漏洩した事例が報告されている（Ｔｅｌｅｇｒａｍでさえハッキングの被害が報告されている）。

【００５０】

アプリケーション層（レイヤ７）攻撃

【００５１】

アプリケーション層攻撃では、アイデンティティ偽装（ＣＡ証明書詐欺及び信頼関係攻撃）、悪意のあるコード（マルウェア及びスパイウェア）、各種のサービス妨害攻撃など、多様な手口が使用される。ほとんどのレイヤ７攻撃は、ごまかし、即ちデジタル署名、偽のＳＳＨ鍵、または偽のＣＡ証明書を利用したアクセス権やシステム権限の奪取から始まる。サイバー攻撃者が偽のセキュリティ証明書によって認証を突破し、システムや暗号鍵にアクセスできるようになってしまえば、レイヤ７アプリケーションに残された保護手段は、アプリケーション自身に組み込まれたセキュリティ機能しかなくなってしまう。しかし、これらのアプリの多くはセキュリティ機能が貧弱か、もしくは全くなく、ＴＣＰ／ＩＰプロトコルスタックの機能に全面的に頼ってコンテンツと整合性の保護が行われている。

【００５２】

レイヤ７マルウェア攻撃では、ウイルスやワームを使用してシステムの乗っ取りや破壊が行われる。例えば、スパイウェア、フィッシング、キーロガー、及びトロイを用いた情報収集、バックドアを設置することによるセキュリティ突破、ランサムウェアのようなシステム制御権のあからさまな奪取、ファイルやプロセスの制御権の密かな奪取といった手口がある。その他に、（Ｓｔｕｘｎｅｔのような）ゼロデイエクスプロイトや、ファイルレスマルウェア感染を利用した手口も存在する。ストレージデバイスやデータベースが攻撃され、個人情報、クレジットカード情報、バンキングデータ、ログインファイルが盗み取られたり、口座や暗号ウォレットから暗号通貨が盗み出されることもある。

【００５３】

個人の写真やプライベートな文書を遠隔入手して、その窃取や恐喝を働く手口も存在する。内容や目的が不明なコンテンツやソフトウェアをインストールさせ、それを稼働中のプロセスやアプリケーションから起動させる手法も存在する。サイバー犯罪者が「クリプター」と呼ばれる特殊なソフトウェアを利用して、自身のマルウェアをウイルス対策ユーティリティから保護するケースもある。バックドア、ランサムウェア、ボットネット、スパイウェアなど、同様のサイバー攻撃法は携帯電話に対しても適用することができる。悪意のあるウェブサイトからダウンロードを行わせる、悪意のある暗号化されたペイロードをダウンロードさせる、アンチセキュリティ、アンチサンドボックス、アンチアナリストなどの手法を取り入れたステルスマルウェアによって検出をかいくぐるといった攻撃ベクトルが存在する。

【００５４】

サイバー犯罪者が効果的なアプリケーション層攻撃を行える方法はさらにある。その一つに、「ルートアクセス」によってデバイス、サーバ、またはネットワークのシステム管理者権限へのアクセス権を取得する手口がある。トロイなどを仕込んだり、悪意のあるアドウェアを送り込むことでルートアクセス権を取得し、大規模感染を引き起こしたり、情

報を盗んだり、アプリを密かにインストールして金儲けを行う。ユーザのアカウントに不正アクセスするのでなく、システム管理者のログインをハッキングすると、システムを利用するユーザについての知識がなくても、かなりのアクセス権と特権を奪うことができる。システム管理者はシステムの警察として振る舞うため、犯行を抑えるものは誰もいない。実質的に、管理体制が損なわれたシステムやネットワークでは、警察を取り締まれる者は存在しない。

【００５５】

ＰＣ及びサーバ、ならびに携帯電話に対するこの種の攻撃は、パイレート管理攻撃または侵入攻撃と呼ばれる。ユーザが携帯電話のオペレーティングシステムを改造して管理者特権を取得する、いわゆるジェイルブレイク（脱獄）やルート化は、サイバー犯罪を一層容易にする要因になっている。ルート化された携帯電話はマルウェアに無防備になる。極端なケースでは、攻撃者がデバイスの制御を完全に奪ってしまうこともある。特に、ＩｏＴ及びＶ２Ｘ通信アプリケーションでは、効果的なサイバー攻撃によって自律型自動運転車の制御が意図的または不意に奪われると、人命に関わる事態や事故に繋がる恐れがあり、影響が懸念される。

【００５６】

ＤｏＳ（サービス妨害）攻撃は、どの層でも実行可能であるが、アプリケーション層（レイヤ７）で実行されることが特に多い。これは、ＨＴＴＰ、ＦＴＰ、ＩＭＡＰ、Ｔｅｌｎｅｔ、ＳＭＰＴ／ＰＯＰ、ＩＲＣ、ＸＭＰＰ、ＳＳＨなど、攻撃対象になり得る多種多様なアプリケーションが数多く存在するためである。特に一般的な手口としては、Ｗｅｂサーバプロセスに対するＨＴＴＰ攻撃、及びＣＰＵプロセスに対するＷｅｂアプリケーション攻撃が挙げられる。

【００５７】

ＩＩ．アイデンティティ詐欺及び信頼関係攻撃

【００５８】

信頼関係攻撃は「インポスター（なりすまし）攻撃」と見なすことができる。犯人（またはそのデバイス）が他人（またはそのデバイス）の振りをして対象者のアイデンティティ情報、権限、アクセス権を奪取することで、不正取引を行ったり、正規のアプリケーションやユーティリティに見せかけたマルウェアをデバイスにインストールする。盗み取った情報を誰にも気付かれないうちに利用できるように、この攻撃はネットワーク攻撃や通信攻撃の直後に実行されることが多い。インポスターエクスプロイトに先立って、スパイングやパーソナルプロファイリングによる情報収集もよく行われる（ネットワーク攻撃やパケットスニッフィングの利用、スパイウェアやキーロガーのようなマルウェアによる物理デバイスへの干渉、ログインエクスプロイトなど）。偽造証明書を使用した資金移動（送金詐欺）や商品代金支払い（取引詐欺）といった、盗み取ったアイデンティティ情報を利用した金儲けも信頼関係攻撃の一種と言える。

【００５９】

信頼関係攻撃は、通信のどちら側も侵入に気付かないＭｉＭ（中間者攻撃）の形をとることが多い。例えば図４では、なりすまし犯４１ｃが発信側と受信側（ブラウザ４１ｂ及びＨＴＴＰＳセキュアサーバ４１ａ）の間にある通信ネットワークにノード４４を挿入し、偽の証明書を潜り込ませることで証明書認証手続きを欺こうとしている。セッションが通常通りに開かれ、ブラウザ４１ｂはＨＴＴＰＳサーバ４１ａに挨拶メッセージ（ｃｌｉｅｎｔ　ｈｅｌｌｏ　４２）を送出する。サーバ４１ｂがそれに応答し、真正なＳＳＬ証明書４３ａを返すと、なりすまし犯４１ｃはこのメッセージをパイレートノード４４のところで横取りし、代わりに窃取または偽造したＳＳＬ　ＣＡ証明書４３ｂをクライアントブラウザ４１ｂに渡す。このＣＡ証明書には、ＨＴＴＰＳサーバとの通信時における、クライアントブラウザ側での情報のエンコード方法が記述されている。

【００６０】

次に、クライアントはサーバに、暗号化に使用されるこのセッション専用の暗号鍵４５を返す。その後、ＨＴＴＰＳサーバ４１ａとの通信へのアクセス権を与える変更後の暗号

４６ａが、パイレートノード４４のところで横取りされ、パイレートノード４４とＨＴＴＰＳサーバ４１ａとの間に正式なセキュア通信リンク４７ａが確立される。同時に、パイレートノード４４はクライアントブラウザ４１ｂに改竄した暗号４６ｂを渡し、パイレートノード４４とブラウザ４１ｂとの間に正式なセキュア通信リンク４７ａが確立される。これで計略が完了し、その後はクライアントブラウザ４１ｂは、パイレートノード４４が当該チャネルのすべての通信に介入しているとは知らずに、リンク４７ａ及び４７ｂから構成される、セキュアではあるが偽のチャネルを介してＨＴＴＰＳサーバ４１ａと通信する。事実上、ＴＣＰ／ＩＰのセッションプロトコルが、安全かつ確実な犯行に荷担していると言える。

【００６１】

疑わしい認証局を信用してしまったり、改竄または偽造されたＣＡ証明書を受け入れてしまうことが、インターネット通信の完全性とセキュリティが損なわれるよくある原因となっている。このことは、ネットワーク接続デバイスが、マルウェアやスパイウェアを含んだファイルを信頼し、受け入れてしまう原因でもある。図５には、インターネットを利用したオンライン取引におけるＣＡ証明書の管理方法が示されている。ここに示された例では、顧客８０がオンライン販売業者８９とセキュアに取引を行おうとしている。業者８９宛てのＰＯ（購入注文書）８８が真正なものであることを証明するため、まず顧客８０はＲＡ（登録局）８３にプライベート情報８２を送る。登録局は当人のアイデンティティ情報８４が確かなものだと認め、認証局８５に通知を行う。その後、認証局８５は顧客８０にＣＡ証明書８６ａの複製を、及びＶＡ（検証局）９２に（ＣＡ証明書８６ａのデジタル署名付きの複製を含んだ）ＣＡ証明書８７を発行する。取引を行うため、顧客８１はＣＡ証明書８６ａとともにＰＯ　８８を業者８９に送付する。注文を受けた業者８９は、ＶＡ（検証局）９２との通信９１ａ及び９１ｂによってＣＡ証明書８６ａが本物であることを確認し、取引を履行する。

【００６２】

しかし、認証局（ＣＡ）８５や検証局（ＶＡ）９２が腐敗していたり、盗み出されたＣＡ証明書が使われたりすると、詐欺的プロセスが不当に認められてしまい、不正な金融取引がまかり通ったり、マルウェア感染が可能となってしまう。つまり、顧客及び業者は、認証局及び検証局が真面目で正直だと「信じ」なければならない。さらに悪いことに、ＣＡ証明書の多くは、すでに生成済みの証明書から生成されている。即ち、「ルート」証明書、中間証明書、「リーフ」証明書からなるファミリーツリーが形成され、同じ１つのルートＣＡ証明書から数多くのリーフ証明書が生まれている。この継承関係から「トラスト（信頼関係）チェーン」が形成され、取引で受け取られたリーフ証明書は、その起源を辿ると名高い認証局から発行された信頼の置けるルート証明書に行き着くため、それを根拠に真正なものと見なされる。しかし、中間証明書が得体の知れないところから発行されたものだったとしたら、リーフ証明書の真正さを本当に信用できるだろうか。

【００６３】

セッション開始時や取引の確認時に、改竄または偽造されたＣＡ証明書が使用されてしまうと、事実上検知も追跡も不可能な取引詐欺やデータ詐欺を行えてしまう。偽のＣＡ証明書を悪用した詐欺的プロセスの例には、送金詐欺、不正なオンライン取引及びＰｏＳ（販売時点管理）取引、アカウント奪取、ログインエクスプロイト、ログイン奪取、マルウェア配布などがある。この手口は、ネットワークのセキュリティ保護機能を回避するため、不正なデバイス、ドライブ、ＵＳＢキーからサーバやＰＣにアクセスする際にも使用することができる。

【００６４】

スパイング、ネットワーク攻撃、マルウェアの利用など、ＣＡ証明書を窃取する手段は多数存在する。コンピュータがバックドアトロイに感染すると、攻撃者は感染先のコンピュータへのフルアクセス権を取得することができる。そのコンピュータを完全に制御できるため、攻撃者は当該コンピュータ上のあらゆる情報を盗み出すことができる。

【００６５】

窃取の代わりに、明らかな悪用目的で偽のコードサイニングＣＡ証明書を偽造したり、ダークウェブからオンライン購入することも可能である。顧客から偽造証明書の作成依頼を受けたならず者業者は、まっとうな企業（またはその従業員）から盗み取ったデジタル証明書を使用して、高名なＣＡ証明書発行者から本物のＣＡ証明書を入手する。ほとんどの場合、騙されたビジネスオーナーやＣＡは、データが不法行為に使用された、または使用されていることに全く気付かない。偽造ＣＡ証明書の入手手段がどうであれ、サイバー犯罪者はそれを使用してマルウェアを拡散させ、インターネット経由で不正取引を行う。このようなマルウェアの中には、有益なウイルス対策ソフトウェアやディスククリーニングソフトウェアに見せかけたり、そのようなソフトだと大っぴらに宣伝されているものさえある。

【００６６】

偽造ＣＡ証明書の最も狡猾な使用事例の中に、マルウェア拡散が関わっているものがある。マルウェアに感染すると、犯罪行為、情報収集、またはサービス妨害を目的とした悪意のあるコードが標的デバイスにインストールされる。コンピューティングの初期の時代は、フロッピーディスク、ＣＤ、ＵＳＢデバイスのような記憶装置でウイルスが運ばれていたが、インターネット経由で配布された初のマルウェアエクスプロイトである１９８８年のＭｏｒｒｉｓワーム攻撃以降は、クラウドがコンピューティングデバイスやモバイルデバイスへの感染媒体となった。Ｍｏｒｒｉｓワームは、サイバー犯罪で初の有罪判決が下された事例であるだけでなく、インターネットや電子メールに内在している攻撃に対する脆弱性を浮き彫りにし、ユーザには警鐘を鳴らし、ハッカーには刺激を与えた。

【００６７】

検出や除去は極めて容易であったが、Ｍｏｒｒｉｓワームは効果的なサービス妨害攻撃によって、いかに大きな混乱を引き起せるかを明らかにした。それから３０年経った現在、ネットワーク感染エージェントの能力とステルス性は大きく進化し、メール、ウェブブラウザ（ＨＴＴＰエクスプロイト）、ファイル（ＦＴＰ）ダウンロード、広告ブロッカー、システムクリーンアップソフトウェア、ソフトウェアアップデート及びインストーラ、ＪａｖａＳｃｒｉｐｔ（登録商標）、ＡｃｒｏｂａｔＲｅａｄｅｒ（登録商標）及びＰＤＦリーダー、メディアファイルプレーヤー及びＦｌａｓｈ（登録商標）プレーヤー、パーソナルメッセンジャーなど、様々な攻撃ベクトルが生まれた。ほとんどのネットワーク配布型マルウェアエクスプロイトでは、信頼関係構築、検出回避、及びアクセス権取得のために、（上述の）偽造ＣＡ証明書が併用される。ユーザが悪意のあるＵＲＬに接続した時に、もしくはユーザがＵＲＬの綴りを間違えて入力することがあることを利用した「タイポスクワッティング」によって、ユーザを悪意のあるサイトに誘導した時に、アドウェアを介してシステムアクセス権を取得する手口も存在する。

【００６８】

インストールされたマルウェアは様々に動作する。サービス妨害攻撃、Ｆｏｒｋ爆弾、ランサムウェア、致命的ウイルス、及び多くのゼロデイエクスプロイトでは、引き起こされるシステム障害やシステムメッセージから、標的は感染したことにすぐに気付く。フィッシング、ログインエクスプロイト、キーロガー、スケアウェアのような対話型エクスプロイトでは、ユーザは騙されて個人的なプライベート情報を入力してしまい、悪人に知らせてしまう。スパイウェア、ルートキット、傍受、データスクレイパー、及びバックドア攻撃では、マルウェアは「痕跡を隠す」ため、抜け道を通って標的に密かに侵入し、検知を逃れ、自らの存在と出所の証拠をすべて消し去る。タイムボム、ロジックボムといった時限式のマルウェアは、しばらくの間は身を潜め、特定の状況になった時に作動して、標的デバイスにダメージを与えたり、他のデバイスへの感染を引き起こす。Ｆｒａｎｋｅｎｓｔｅｉｎマルウェアと呼ばれる、さらに高度な攻撃ベクトルは、攻撃の真意を隠すために、無害に見える一連の「良性バイナリ」の形で、悪意のあるコンポーネントを送り込む。その後、これらのコンポーネントは送り込まれた先で集合し、一つに結合して攻撃を開始する。

【００６９】

モバイルデバイスやモバイルアプリの急成長を受けて、サイバー犯罪者はスマートフォンやタブレットの攻撃に目を向けるようになった。侵入検知・防止機能がそれほど高度ではないこと、及びＰＣによく保存されるものより個人的な情報が含まれている傾向が高いことが、その動機の一部となっている。例えば、最近の研究によると、ウイルス対策アプリケーションに見せかけた（ＫｅｖＤｒｏｉｄという名称の）Ａｎｄｒｏｉｄ（登録商標）トロイが出回っていることが判明している。最新型のマルウェアは、以下に示すような極めて高度な機能を備えている。

・通話及び音声の録音
・インターネット閲覧履歴及びファイルの窃取
・ルートアクセス権（制御権）奪取
・通話履歴、ＳＭＳ、及びメールの窃取
・デバイスの位置情報収集（１０秒間隔）
・インストールされたアプリケーションのリスト収集

【００７０】

犯罪者、ギャング、犯罪シンジケートは、これらの機能を悪用することで、個人の居場所を追跡したり、音声・テキスト・メール通信を傍受したり、銀行取引詐欺を働いたり、恐喝・脅迫を行うことができる。このように、セキュリティが破られることでプライバシーが漏洩すると、サイバー犯罪の域を遙かに超えて、対象者が危険に晒されることになる。Ａｎｄｒｏｉｄ（登録商標）はオープンソースプラットフォームであるため、モバイルオペレーティングシステムを対象にしたマルウェア攻撃にとっての最大の標的となっている。これらの攻撃の大半は、ネットワーク接続（ＷｉＦｉまたはワイヤレス通信ネットワーク）を介して行われるが、Ａｎｄｒｏｉｄ（登録商標）フォンはマルチソース市場であるため、スマートフォンメーカーによって、バックドア、プリインストールマルウェアといったＯＥＭメーカー固有の脆弱性が仕込まれることもある。ｉＯＳ（登録商標）及びｉＰｈｏｎｅ（登録商標）は望まない侵入を受けにくいが、ｉＰｈｏｎｅ（登録商標）に対しても様々な攻撃ベクトルや攻撃法が報告されている。

【００７１】

インターネットを利用した攻撃を防げないことを想定し、ウイルスチェッカーやファイアウォールがサイバー犯罪への対抗策として利用される場合がある。しかし、今日のグローバル企業にとっては、遅延が大きく、扱いにくいＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）を利用すること以外に、各国に跨がるフットプリントを１つのファイアウォールでカバーする現実的手段は存在しない。さらに悪いことに、一般にウイルスチェッカーは、感染が起きた後に攻撃を検知することしかできない。しかも、断片バイナリ型のＦｒａｎｋｅｎｓｔｅｉｎマルウェアのような高度な攻撃は、検知の目から完全に逃れてしまう。従って、インターネットのようなオープンな公衆ネットワークを介したサイバー攻撃の防止が、相変わらず多くの研究の対象となっている。ネットワークで運ばれるマルウェアは、信頼の置ける商取引の重大な障害であり、個人のプライバシー及び身の安全に対する、増大し続けるリスクとなっている。

【００７２】

ＩＩＩ．　データ漏洩

【００７３】

米国保険福祉省によると、データ漏洩は「秘匿情報、保護情報、または機密情報が、適切な権限を持たない人物によって複製、転送、参照、窃取、または利用されるセキュリティ事案」とされている。データ漏洩は（前述の）ネットワーク通信のハッキングによって引き起こされるが、そのほとんどは「データファイルの盗み出し、または盗み取ったデータファイルの改竄」を目的としている。企業や政府のデータベース、ネット上のクラウドストレージ、または大型ストレージファームやサーバファームに保存されるこれらのデータには、アクティブレコード、定期的バックアップファイル、アーカイブデータ、カタストロフィックリカバリーファイルなどがある。

【００７４】

データ漏洩は、個人生活及び社会生活の両面で、現代社会のあらゆる側面に影響する。攻撃の対象となるものには、金融取引情報、商取引情報、企業機密、知的財産、顧客名簿、個人情報、社会保障・納税情報、政府職員情報、現役軍人情報、退役・予備役軍人情報、保険記録、クレジット明細、診療情報、ソーシャルメディアプラットフォームのファイル、画像のようなパーソナルクラウドストレージ上のプライベート情報などがある。中でも、クラウド上のバックアップストレージは、そこにプライベート情報が事実上すべて含まれているため、ハッカーにとって特に価値のある標的となっている。犯行の動機には、金儲け、スパイ活動、ＦＩＧ（Ｆｕｎ，　Ｉｄｅｏｌｏｇｙ，Ｇｒｕｄｇｅ：気晴らし、政治的理念、怨恨）などがある。例えばアイデンティティ情報漏洩では、犯人は社会保障情報、運転免許証、パスポート、住所、メールアドレス、電話番号などを盗み、それらの情報から偽のＩＤを作成して、犯罪を働いたり、テロ攻撃の取り締まりの目から逃れたりする。盗み出した情報を、迷惑メールの送り先としてスパム業者に売りつけることもある。業務情報や個人的プライベート情報の漏洩・流出から生じる、個人的及び事業的損害は計り知れない。

【００７５】

データ漏洩やデータストレージ攻撃では、大量の情報がまとめて盗まれることが多いが、対象を絞った攻撃も見られる。後者のケースでは、攻撃の価値や影響を最大限に高めるため、スパイングやプロファイリングが利用されていると推測される。特に悪質なデータベース攻撃としては、「アイデンティティ簒奪」が挙げられる。この攻撃では、犯人はデータベース上にある対象者のアイデンティティ情報を丸ごと書き換えるか抹消し、当人が存在しないかのように見せかけてＰＩＩ（個人識別情報）を乗っ取る。ハードコピー、バックアップストレージ、及び他のデータベースから当人のアイデンティティ情報を復元することはできるが、この処理には手間がかかり、個人や企業に大きな金銭的負担が生じてしまう。

【００７６】

データ漏洩の別の手口では、「トランザクションレコード攻撃」を行うことが可能となる。例えば、銀行のデータベースがトランザクション攻撃を受けると、口座にある資金が国外口座に送金または誤送金されてしまう。この不正送金の記録もすべて消去されてしまうため、ハードコピーがなければ、被害者には盗難の被害に遭ったことを証明する術はない。盗まれた資金が自分のものであることさえ証明できない。理論上、同様のデータベース攻撃は、保険データベース、企業、及び退役軍人援護局、社会保障局、連邦銀行といった政府機関に対しても起こり得る。ブロックチェーンであれば、一連のトランザクションを時間順に記録した消えない台帳を生成できるため、トランザクションレコード詐欺を減らすことができるが、それにはブロックチェーンの完全性（インテグリティ）がセキュアなことを保証できることが条件となる。

【００７７】

商用データベースの多くでは、独自インターフェイスと「セキュア」だとされているプロトコルが使用されている。そのため、データベース会社の多くが「我が社のデータベースは攻撃不能」と主張しているが、実際はそうではないことを示す確かな証拠がある。信頼関係攻撃やネットワーク攻撃と同様に、データ漏洩も起こり得るのは、暗号化への過信に原因がある。犯人は、暗号化を破らなくてもデータベースに侵入できる。ただアカウントのパスワードを盗み出したり、セキュリティの関門を迂回するだけでよい。例えば、「ＳＱＬインジェクション」と呼ばれるデータベースエクスプロイトがある。この手口では、攻撃者はウェブフォームの入力欄にＳＱＬ（Ｓｔｒｕｃｔｕｒｅｄ　Ｑｕｅｒｙ　Ｌａｎｇｕａｇｅ）コードを入力して、リソースへのアクセス権を取得したり、データ書き換えを行ったりする。自動化を通じて、「ブラックハット」と呼ばれるプロのハッカーらが、ＳＱＬインジェクションによってパスワード窃取、ワーム注入、データアクセスを行えるフリーウェアのハッカーツールを開発中だと言われている。これにより、動的コンテンツを使用したウェブアプリケーションの６０％が危険に晒される恐れがある。今日では、事実上すべてのデータベースやストレージファイルが、本質的にセキュアではない通信媒体

であるインターネット経由でアクセスされるため、この脆弱性をなくすことは不可能である。

【００７８】

ＩＶ．　ブロックチェーン攻撃

【００７９】

ブロックチェーン及び暗号通貨を使用した電子商取引は、暗号化ＤＬＴ（デジタル台帳技術）による記帳及び分散型のコンセンサス検証を用いた、分散型トランザクションプロセスから成り立っている。暗号化によってブロックチェーンの内容が保護されるため、これらのトランザクションは商業的、法的、及び個人的取引に適用することのできる、セキュアかつハッキング不可能な信頼性の高いプロセスであると広く主張されている。さらに、中央権力による制御が及ばない不変のデジタル台帳が使用されることから、ブロックチェーンではレコードのバックデーティング、改竄、ポスト訂正も行えない。

【００８０】

図６に示されているように、ブロックチェーントランザクション処理では、ブロックチェーン・アプリケーション６５によって、検証済みのトランザクション７０が実行され、ブロックチェーン祖先６０を使用して、トランザクションプロセスの検証、恒久記録、記帳が行われる。ブロックチェーンは、過去からの時間順に並べられたデジタル台帳であり、複数のインスタンスとしてクラウド、ネットワーク、システムに保存される。トポロジー的には、ブロックチェーンはメインブロック６１の「一繋がり」のチェーンからなる一次元有向非巡回グラフ（１Ｄ　ＤＡＧ）の形をとる。このメインチェーンの中に、孤立ブロック６３まで続くフォーク６２や、途絶えてしまったサイドチェーンが含まれる場合もあるが、それらすべてが順に並べられ、タイムスタンプが付けられる。「非巡回」という用語は、チェーンの中にループが形成されないことを意味する。即ち、サイドチェーンがチェーンの主軸に再結合して巡回ループを形成することはない。ループ、即ち巡回の形成が禁止されているのは、チェーンの最後尾に追加された新しいブロックより、その前のブロックの方が時間的に新しいという時間順のパラドックスが生まれる可能性があるためである。

【００８１】

一繋がりのブロックチェーンでは、残存し続けるアクティブなチェーンは１つしか存在しない。サイドチェーンは単純に途絶え、一般にメインチェーンの機能や目的に固有のものではない補足情報の記録に使用される。ブロックチェーンとそのブロックチェーン祖先６１は公開する（パブリック型にする）ことも、プライベート型のままにしておくこともできる。ブロックチェーントランザクションは、中央権威７１（銀行や政府など）による検証や、ノード集団の合議７２による分散的な確認を行える。

【００８２】

ブロックチェーンには暗号化データと非暗号化データの両方が含まれているため、パブリッククラウド上で公開したとしても、必ずしもプライバシー漏洩や公的開示には繋がらない。そうなるかどうかは、追加されたブロックの中で、データがどのように表現されているかに依存する。ブロックが暗号化されていなければ、ブロックチェーン祖先にアクセスできるすべての者がデータを読み出すことができる。反対に、ブロックが暗号化されていれば、暗号鍵を持つ者しか内容を参照できない。ブロックの生成時には、暗号化ハッシュ（入力に応じて変わる固定長の暗号文出力を生成する一方向性の暗号化）を用いて新しいブロックを生成するのが最も一般的である。暗号化ハッシュには復号鍵は存在しないが、ハッシュ値は固有の値をとるため、ハッシュの実際の内容を開示することなく、公の場で真正さを確認することができる。例えば、ファイルＸの内容を開示しなくても、ファイルＹの真正さを、２つのファイルのハッシュ値を比較する（即ちＨ（Ｘ）＝Ｈ（Ｙ）かどうかを調べる）ことで確認することが可能である。この２つのハッシュ値が同じであれば、ファイルＹの内容はファイルＸの内容と同一であると認められ、トランザクションを進行させることができる。反対に、ハッシュ値が異なっていれば（即ちＨ（Ｘ）≠Ｈ（Ｙ）であれば）、ファイルＸとファイルＹは同一ではない。ただし、ファイルＸのオーナーは

当該ファイルの内容を開示する必要はなく、相手側から機密情報が漏れる心配をする必要もない。

【００８３】

図６のブロックチェーントランザクションプロセスを再度参照すると、アプリケーション６５は、ブロックチェーンＢＡ　６０に追加する機密データファイルＤＦ　５６を生成する。次に、ブロックチェーンプロセッサ６７が、ファイルＤＦ　５６をＢＡ　６０に結合し、暗号文ファイルＨ（ＤＦ＋ＢＡ）からなるハッシュ６８、及び非暗号化プレーンテキストヘッダーファイル６９を生成する。その後、トランザクション検証７０で、Ｈ（ＢＡ）とＨ（ＤＦ＋ＢＡ）の値が比較され、アプリケーション６５が本当にファイルＤＦ　６６の生成元かつオーナーであることが確認される。この検証は、中央権威７１による承認、または分散システム上のノード集団７２のコンセンサスによって行うことができる。検証が成功すると、保留されていたトランザクションブロック６４がブロックチェーンＢＡ　６０の最後尾に追加される。

【００８４】

このブロックチェーン処理のすべてが、図１のＯＳアプリケーションＶＭ　８上のアプリケーションとして実行される。また、ブロックチェーントランザクションに関わるノード同士の通信１５は、ＴＣＰ／ＩＰ　７の最上位層、即ちアプリケーション層（レイヤ７）を使用して実行される。ブロックチェーン処理とその実行を「ブロックチェーンネットワーク」と称している一般向け技術記事もあるが、それは誤解を招く表現である。実際は、プロセス全体がデバイスのアプリケーションＶＭ上でホスティングされ、それがＴＣＰ／ＩＰを使用してインターネットを介して実行される。ＴＣＰ／ＩＰのすべての脆弱性が、ブロックチェーン処理にも等しく当てはまるため、巷の評判とは異なり、ブロックチェーンはネットワークセキュリティリスクと無縁ではない。

【００８５】

ブロックチェーン技術の適用事例の一つに、暗号通貨の生成と利用がある。ＰｏＷ（プルーフオブワーク）を用いた暗号通貨生成、即ち「マイニング」として知られているプロセスでは、デジタルプロセッサが演算集約的な力尽くの方法で、（次の素数を見つける、ハッシュ・ナンスパズルの答えを当てるといった）数学的問題を解く。答えが見つかると、その正しさがノード集団の合議によって確認され、それが正解だった場合のみ、結果がブロックチェーンの最後尾に追加され、新しく生成されたコインが報酬としてマイナーに支払われる。このプロセスは大量のエネルギーを消費する困難な処理であり、金銭的見返りが得られる保証は全くない。また、ブロックチェーンは一続きであるため、それが長くなるほどメモリ消費量が増大し、トランザクション取引に時間がかかるという問題も生じる。

【００８６】

さらに言えば、マイナーに報酬を与え、デジタルコインをウォレットや取引所に保管するというプロセス全体が、インターネットに内在しているセキュリティ脆弱性、及びインターネットのＴＣＰ／ＩＰ通信プロトコルへの全面的な依存性を悪用した盗難や取引詐欺の危険に満ちている。とは言え、分散型暗号通貨派の人々の多くは、「世界共通の金融・通貨ポリシーに各国政府が口出ししてくることに比べれば、犯罪の被害に遭った方がまだマシ」と考えている。

【００８７】

分散型ブロックチェーン及び暗号通貨トランザクションは、「信頼の置けない」システムで動いている、トランザクションを検証する中央権威がないとよく言われる。しかし、正確には分散型ブロックチェーンに信頼性がないわけではない。拠り所を１つの権威から、制御を分散させて単一システム障害点のリスクを排除した、ノード集団として振る舞う相互接続されたコンピュータノードのグループにシフトしているだけにすぎない。このような有益な点があるにも拘わらず、実際はブロックチェーントランザクションの改竄、暗号通貨窃取、セキュリティ及びプライバシー攻撃、犯罪の遂行、その他の悪意のあるオンライン行為など、攻撃の手口が数多く考案されている。

【００８８】
ブロックチェーンの分散型コンセンサスが信頼性に欠けることを、弱点として突く攻撃も存在する。ブロックチェーンや暗号通貨に対するサイバー攻撃では、基本的に金融詐欺、セキュリティ侵害、プライバシー攻撃が実行される。これらの攻撃は、スニッフィングなどの手段による暗号鍵奪取、ＤｏＳ攻撃、ブロックチェーントランザクション自体の直接的改竄などを利用して、ネットワーク層（レイヤ３）上で行われる。ブロックチェーン攻撃は、ブロックチェーン詐欺、暗号通貨窃取、マルウェア攻撃、プライバシー漏洩、ブロックチェーン非合法行為、スマートコントラクト詐欺といった数種類に大別することができる。
【００８９】
ブロックチェーン詐欺
【００９０】
ブロックチェーン詐欺では、犯人は主に金儲けを狙って、あらゆる手段で真正なトランザクションのタイムリーな検証を意図的に妨害し、犯行の発覚を防ごうとする。通常、このブロックチェーン攻撃では、ダブルスペンディングとレコードハッキングという、２種類のオンライン不正行為が使用される。「ダブルスペンディング」詐欺では、同じ暗号通貨でわざと２回支払いを行う。一方のトランザクションのみが真正なものであるが、もう一方の不正なトランザクションも通すには、犯人はシステム妨害、ミスディレクション、偽装といった様々な手段で発覚を防がなければならない。
【００９１】
例えば５１％攻撃では、ネットワークのマイニングハッシュレート、即ち演算能力の過半数を意図的に握ったマイナーグループが、ノード集団のコンセンサスプロセスに介入し、真正なトランザクションの承認を妨害する（その結果として不正なトランザクションの方が通ることになる）。５１％過半数攻撃に対する脆弱性は、分散型トランザクション検証で使用されるＰｏＷ（プルーフオブワーク）方式のコンセンサス形成手続きに大きな弱点があることを露呈させた。即ち、最も多くの演算能力を持つ者であれば、詐欺取引や脈絡のない支出から暗号通貨の完全性を守ることに関心がなくても、有無を言わさず決定権を握れるため、コンセンサスを支配することのできる犯人は正々堂々と詐欺を行えてしまう。
【００９２】
ダブルスペンディングの手口には、レース攻撃、フィニー攻撃、シビル攻撃、タイムジャッキング、及びその変種など、様々なものがある。特に、ビットコインのような通貨が成熟期に入って、マイナーに報酬として支払われる新造コインの数が減少して行き、トレーダーらの旨みがなくなると（いわゆるコモンズの悲劇）、たとえ過半数の議決権を握らなくても、マイニングモノポリーはトランザクションの迅速な処理を抑止することで、密かな詐欺を成功させる可能性を高めることができる。マイニングモノポリーのメリットを考えると、ＰｏＷ方式の暗号通貨が、かつて信じられていたほど分散化されていないのも不思議ではない。
【００９３】
「レコードハッキング」では、犯人は検証を受けていない不正なブロックをブロックチェーンに挿入するか、ブロックチェーンを悪用目的でハードフォークさせることで、ブロックチェーンの改竄を目論む。いったんブロックチェーンが改竄されてしまうと、それが次のトランザクションまでの間に拒絶されない限り、ダメージはほぼ不可逆なものとなる。修復するには、問題のイベントの前にハードフォークを作成し、メインブロックチェーンのブランチの巻き戻し（キャンセル）を行って、後続のトランザクションをすべて取り消さなければならない。使われてしまった暗号通貨は取り返せないため、このような修復は一般的ではなく、極めて面倒で、地域によっては違法性を問われる可能性もある。
【００９４】
ハードフォーク容認派の人々は、犯人の儲けを取り消すべきだ、即ち犯行の巻き戻しを行うべきだという立場を取る。しかし、そうしてしまうと、犯行の発生後に正当なトラン

ザクションを行ってしまっているコイン保有者が損をすることになる。反対派の人々の中には、そうすると損をする者、及び「買主が注意せよ」の原則を信奉し、「たとえ詐欺が起きたとしても、ブロックチェーンは不可逆であるべきだ」と考える哲学的ブロックチェーン純粋主義者がいる。

【００９５】

暗号通貨窃取

【００９６】

分散通貨を使用した商取引の今日のリスクの１つに、盗難が起きてしまうと、盗まれた資産を取り返す術がないことがある。攻撃によって、暗号通貨マイニング企業、モバイルウォレット、及びエンドポイント（デバイス）から、ならびにＷｉＦｉ経由で盗み出された資金は、既に合計数億ドルに達している。これらの暗号通貨窃取の多くは、マルウェアやスパイウェア（次節を参照）を用いた単純なパスワードハッキング、偽造ＣＡ証明書の悪用、暗号鍵窃取、パケットスニッフィング、不確かな第三者を信用してしまうこと、偽の取引所の利用、またはセキュアではないオンライン取引によって引き起こされている。

【００９７】

端的に言えば、セキュアではないインターネットでは、暗号通貨をオンライン盗難から守ることはできない。オンライン盗難の手口の一つに、ログインエクスプロイトを用いた暗号通貨ウォレットのフィッシングがある。この攻撃では、犯人はログインウィンドウを偽のウェブサイトにリダイレクトする。被害者はハッカーに渡ってしまうと気付かずに、パスワードとログイン情報を入力してしまう。犯人はその情報を使用して本物のサイトにログインし、資金を盗み出す。このようなエクスプロイトでは偽造ＳＳＬ証明書が使用される。インターネットを利用したログインエクスプロイトを確実に防ぐ手段はないが、サイトごとにパスワードを使い分ける、多要素認証を利用する、すべてのサイトのＳＳＬ証明書をチェックして、署名が本物かどうかを慎重に確認するなどの方法で、リスクをある程度軽減することができる。さらに言えば、資金の大半をオフラインの「コールドストレージ」に保存しておくことが望ましい。

【００９８】

ブロックチェーンマルウェア攻撃

【００９９】

ブロックチェーンに対するマルウェア攻撃も、デジタル通貨のリスクの一つとなっている。ＲＳＡ Ｃｏｎｆｅｒｅｎｃｅで発表された最近のレポートによると、ビットコインを盗み出すことを目的としたマルウェアは１４６種類存在する。例えば、キーストロークを記録したり、暗号通貨ウォレットのパスワードを盗んだり、スクリーンショットの撮影を行うトロイ、ウイルス、スパイウェアが存在する。中には、ビデオ画面の映像をハッカーにライブストリーミングするものさえある。対象者のコンピュータを感染させて、膨大な電気光熱費を当人にこっそりと負担させ、ＣＰＵに暗号コインの採掘を行わせる手口も存在する。マルウェアを感染させることでデバイスを乗っ取り、それをボットネット（マルウェアに感染したコンピュータから構成される大規模なネットワーク）に組み込んで、ブロックチェーン、暗号通貨ウォレット、及びその格納先のデバイスへの攻撃に利用する手口もある。

【０１００】

ウォレットとその内容の保護に使用される秘密暗号鍵が入ったファイル、ｗａｌｌｅｔ．ｄａｔを探し出すウイルスも存在する。ウォレットは暗号化することができるが、キーロガーが仕込まれてしまうと、パスワードを一回入力するだけで、ハッカーがウォレットを開けたり、暗号通貨を窃取（自分のアカウントに送金）したり、パスワードを変更して本人のアクセスを遮断することが可能となってしまう。いったん送金されてしまうと、コインの追跡性は完全に失われてしまう。また、暗号通貨の送金を横取りするマルウェアも存在する。このマルウェアは、コンピュータに密かに侵入して、何もせずに待機する。そして、感染先のデバイスでビットコインアドレスがコピーされた時に攻撃を開始して、ＩＰアドレスを変更し、コインの送金先をハッカーの口座に切り替える。さらに、特に攻撃

的な手口としてランサムウェアがある。これは、感染先のコンピュータやそのファイルのロックを解除することと引き替えに、ビットコインなどの暗号通貨での支払いを要求するマルウェアである。

【０１０１】

エンドポイント攻撃では、暗号通貨取引に関与しているデバイス（購入者や取引所のデバイス、交換するコインが入った暗号通貨ウォレットなど）に干渉することに特化したマルウェアが使用される。この攻撃は、ネットワーク上で取引の転送を行うノードではなく、取引の両端のデバイスに対して実行される。マルウェア対策のベストプラクティスとしては、完璧とは言えないものの、ファイアウォールやウイルス対策ソフトウェアを使用したり、専用のＰＣをオフラインで利用することが挙げられる。

【０１０２】

ブロックチェーンプライバシー漏洩

【０１０３】

当初は、取引の匿名性が暗号化ハッシュによって守られると信じられていたが、２０１３年にブロックチェーン専門家らによって、暗号化ブロックチェーンから氏名、口座番号といったプライベート情報が抽出される可能性があることが確認された。「非匿名化」と呼ばれるこのプロセスでは、（ブロックの共通性を見いだす）データパターン認識と、（アドレスを暴く）テスト取引分析を組み合わせることによって、暗号通貨ブロックチェーンの詳細分析が行われる。ブロックチェーンは、過去の全トランザクションの情報を記録したブロックから構成されているため、デジタル資産盗難のリスクがあるだけでなく、個人のプライバシー情報や金融取引情報が密かに流出する恐れもある。サイバー犯罪者は、流出したプライベート情報を、対象者のプロファイリング、暗号通貨窃取、アイデンティティ奪取、個人を狙った攻撃に利用することができる。また、ブロックチェーンレコードも、攻撃の標的を、より成功している暗号通貨トレーダーに絞るのに利用することができる。

【０１０４】

ブロックチェーンの秘匿名化に対する脆弱性は、管理方針と人々の行動に起因している。特に、アドレスの使い回しと、暗号通貨によるオンライン購入は危険性が高い。例えば、暗号通貨によるオンライン購入のケースでは、オンライン分析機能と広告機能を提供するサードパーティ製のトラッカーが、「ブロックチェーン上のトランザクションを一意に識別してユーザのＣｏｏｋｉｅにリンクさせ、そこからユーザの真の身元情報を引き出す」のに十分な情報を収集することができる。また、購入者が同じブロックチェーン上で複数回オンライントランザクションを実行すると、たとえ匿名化機能が使われたとしても、全トランザクションの情報を含めて、当人のアドレスのクラスタ全体が抽出されてしまう。このリスクとなり得る情報は消すことができず、かついつまでも残るため、過去に遡った攻撃を行うことができる。

【０１０５】

各種業界でのブロックチェーン記帳への移行が進むと、ブロックチェーンエクスプロイトによる個人的プライバシー情報に対する攻撃のリスクがますます大きな問題となる。特に、個人情報がブロックチェーンに保管されていることを全く知らない消費者が、アイデンティティ情報盗難の被害者となる可能性が心配される。この難題を解こうと、ブロックチェーンプライバシー漏洩問題とその対策についての研究がさかんに行われ、匿名性を保ちながらアカウンタビリティを高めるため、物理的実体を仮想的アイデンティティに紐付けすることなどが提案されている。しかし、現時点でのこれらの提案は、独創的ではあるものの、有力な実装、テスト手法、採用実績が全くなく、説得力に欠けている。このようなプライバシー保護されたブロックチェーンのトランザクション処理速度は、実用に即さないほど低速なものとなることが予想される。

【０１０６】

ブロックチェーン非合法行為

【０１０７】

ブロックチェーンでは、あらゆる種類のデータをブロックの中に組み込めるため、国や地域によっては違法性を問われる可能性のある、好ましくない情報でブロックチェーンが汚染される可能性がある。分散システムでは、ブロックチェーンに組み込まれる「任意コンテンツ」ファイルの事前確認及び承認を行う者は存在しない。従って、ブロックチェーンの内容を管理して、その適切性を判断したり、適切ではないものを拒絶したりする手段はない。このようなブロックチェーンに格納される内容の無制限性から、著作権違反、知的財産窃取、マルウェア、プライバシー侵害、政治的にセンシティブなコンテンツ、宗教的に好ましくない情報、違法なコンテンツといった、多くのリスクが生まれている。

【０１０８】

著作権違反とは、著作権で保護された作品（音楽作品、演劇作品、文学作品、芸術作品、及びその他の知的作品を含む原著作物）の頒布、違法ダウンロード、無断使用を言う。また、知的財産窃取とは、まだ公表されていない人間知性の無形の産物（出願中の特許、企業秘密、機密情報、事業計画、内約、及びその他の非公開創造物）の無断暴露、頒布、利用を指す。どちらの場合も、分散型ブロックチェーンの公的な回収は不可能なため、ＩＰ及び創作物のブロックチェーンへの流出によって生じた経済的損害の特定は難しい。ほとんどのユーザは、ブロックチェーン上に存在する違法物に気付かないため、国によっては、アップロード者の賠償責任を問う代わりに、違法物のダウンロードや使用の摘発を行い始めている。

【０１０９】

ブロックチェーンの任意コンテンツに伴う別のリスクの一つに、マルウェアの侵入がある。インターポールによると、「ブロックチェーンの仕組みは、マルウェアが入り込んで永久に居座る可能性があることを意味し、そのデータを消し去る手段は現時点では存在しない」とされ、グローバルなサイバー衛生が永久的に毀損される恐れがある。ブロックチェーンに潜む可能性のあるマルウェアとしては、ゼロデイエクスプロイト、タイムボム、トロイ、及び検出困難な分子ウイルスがある。いったん感染してしまうと、ブロックチェーンマルウェアの除去は不可能であり、永久的に取引リスクに晒され、ウイルス対策ソフトウェアの警告に絶えず悩まされることになる。政治的にセンシティブな情報や宗教に好ましくない情報のブロックチェーンへの注入は、それによる影響を受ける国やコミュニティに大きく依存する。ある国では神聖不可侵とされる政治的または宗教的見解が、別の国では冒涜と見なされる場合がある。宗教的に好ましくない内容やポルノの違法性も国によって異なる。ブロックチェーンのサイバー衛生を保つ裁定者は存在しないため、違法物や禁止物を含んだ暗号通貨を、それとは知らずに自国に輸入すると、重罪を課される可能性がある。脅迫、恐喝、トラフィッキングなどもブロックチェーンの非合法的な利用例であり、主権国家の国家安全保障及び国家安定性に対する脅威になり得る。

【０１１０】

スマートコントラクト詐欺

【０１１１】

スマートコントラクトは、ブロックチェーン技術の有益な利用及び悪用の両方の点で大きな可能性を持つ。スマートコントラクトは、ブロックチェーンに消せないように格納された実行可能なコンピュータプログラムを構成するデジタルコードから成り立っている。スマートコントラクトはシーケンシャルステートマシンとして動作し、検証可能な一連のタスクを実行して、各ジョブの合意済みの価値に基づいて、マイナー集団に暗号通貨を報酬として分配する。スマートコントラクトの概念は１９９６年から存在するが、Ｅｔｈｅｒｅｕｍによって、スマートコントラクトに基づく初のＢａａＳ（Ｂｌｏｃｋｃｈａｉｎ－ａｓ－ａ－Ｓｅｒｖｉｃｅ）が実現されるまでに、約２０年の歳月を要した。

【０１１２】

自らのプラットフォームとブロックチェーンの他社利用を可能にすることにより、Ｅｔｈｅｒｅｕｍはトレーディングにフォーカスした従来の暗号通貨との差別化を図っている。新技術への不信感、及びマスコミによる詐欺の事例の報道も手伝って、ＢａａＳの採用はなかなか進まず、市場への浸透は限られているが、特に証券、貿易金融、デリバティブ

取引、金融データ記録、保険、住宅ローン貸付といった金融工学（フィンテック）の分野では、大きな可能性を持つ適用事例が数多く生まれている。また、この技術はデジタルアイデンティティ、記帳、サプライチェーン管理、土地所有権記録、臨床試験管理、医学研究のような金融以外の分野にも適用することができる。

【０１１３】

ＢａａＳ支持派の人々は、スマートコントラクトならビジネス界の詐欺を防止できると言い、それに対して反対派は、スマートコントラクトではポンジスキームのような詐欺的エクスプロイトは防止できないことは明白と反駁する。実際に、今日のスマートコントラクトは疑念が払拭された状態ではなく、多くの問題を孕んでいる。例えば、元々プライバシーがない、攻撃を直ちに撃退できない、「瑕疵のある起草」テクニック及び（調査対象となったＥｔｈｅｒｅｕｍの１９，０００のスマートコントラクトのうちの４４％から見つかったとされる）エラーだらけのコードによって伝搬される脆弱性のために、エラーが次々と複製される傾向があるなどの問題がある。皮肉なことにブロックチェーンは、分散型サービス妨害攻撃を防ぐソリューションだと言う謳い文句に反して、ブロックチェーン技術を利用したビットコイントレードに対するＤＤｏＳ攻撃に対抗することはできない。

【０１１４】

Ｖ．プライバシーの問題

【０１１５】

前述のインターネット及びＴＣＰ／ＩＰのセキュリティ面の脆弱性に加えて、今日ではプライバシーも大きな問題となっている。即ち、個人や企業のデータの所有者は誰なのか、データの参照、配布、利用を所有者が制限することはできるのかという問題が生じている。Ｆａｃｅｂｏｏｋ、Ｉｎｓｔａｇｒａｍ、Ｔｗｉｔｔｅｒといったソーシャルメディアの急成長によって、人々が体験を分かち合ったり、仕事の宣伝を行う新たな手段が生まれた。しかし最近は、ソーシャルメディアの運営者がユーザの情報を収集し、広告業者やデータ分析企業に販売していることが明らかになっている。ビッグデータの世界では、個人の私的なデータは個人の物ではなく、そのデータへの他者からのアクセスを制限する権利も個人にはない。

【０１１６】

同様の問題はＡＷＳ、ＧＷＳ、Ａｚｕｒｅといった大規模コンピュータネットワークにも存在する。世界のデータトラフィックの余りにも多くの割合がこれらのネットワークで占められ、その２０２０年の年間売上高は１，０００億米ドルに達すると予想されている。これらのネットワークでも、どのような検索が行われたか、どの製品が購入されたか、どの販売店が利用されたか、誰と交流したかといった大量のユーザ情報が、本人の許可を取らずに、及び利用目的や販売先の開示を行わずに収集されている。メールアドレスや電話番号のような連絡先情報の、悪質な電話セールス業者やメールスパナーへの不正販売が、事実上すべての人々を悩ませているジャンクメールや自動音声勧誘電話の原因になっていると言われている。

【０１１７】

エドワード・スノーデン事件及び「ＮＳＡが国民を監視して、正当な理由なく通話内容を傍受（昔風の言い方ではワイヤータッピング）している」という彼の告発によって、国家がプライバシー侵害に関わっていることが広く知られることとなった。英国や中国のように、いかなる通話及びデータであっても、通話傍受及びデータ分析を警告なく行う場合があることを公に宣言している国もある。数週間前に、Ｈｕａｗｅｉのルータとスマートフォンに、メッセージや通話データを中国に送信する機能があることが明らかとなり、この事実が政治問題となった。

【０１１８】

企業のプライバシーも、今日盛んに議論されている話題の一つとなっている。販売店及び企業は、顧客の連絡先や販売情報が競争相手に渡ることを恐れて、顧客情報をデータ分析企業と共有しようとしない。新規顧客の獲得も大切だが、既存顧客との結び付きも強めたいと考える高級ブランドは、ビッグデータ企業が顧客の連絡先を入手してしまうと、そ

れがライバルブランドの手に渡ったり、得意先にスパムや勧誘メールが殺到するのではないかと心配する。

【０１１９】

米国のＨＩＰＡＡ（１９９６年医療保険の相互運用性と説明責任に関する法律）に基づく個人医療情報の保護、及び欧州のＧＤＰＲ（一般データ保護規則）で定められた個人行動に対するデータマイニングの禁止のように、プライバシー保護を定めた法律があるにも拘わらず、これらの法律の確実な行使を行える明確な手段は存在しない。現実にはソート及び利用に便利なように、データは暗号化されない状態で保管され、システムへのアクセス権を有するあらゆる者が、それらの情報に容易にアクセスすることができる。

【０１２０】

インターネットには「アイデンティティ」は存在しないため、プライバシー保護はほぼ不可能である。個人及び企業のデータや通信メタデータの法的所有者が誰なのかを特定できないため、それらの情報へのアクセスを行える者も定めることができない。プライバシー保護のためにはアイデンティティが必要なことは逆説的と言える。インターネットでは、誰もが誰もの振りをすることができるため、アイデンティティは意味を持たない。端的に言えば、個人情報及びプライベート情報の悪用が起きるのは、インターネットではそうすることが可能だからであり、それを阻止する規定が存在しないためである。

【０１２１】

Ｖ．分散化

【０１２２】

ウィキペディアでは「技術的分散化」が、商品及びサービスの生産及び消費の集中型から分散型への転換と定義されている。インターネットでは、この用語はクラウドコンピューティングのようなネットワークの運用方式、通信ネットワーク、及び電子商取引に適用される。分散化の経済的動機には、規模の経済の追求、需要と供給のバランス取り、競争促進、余力のあるリソースの活用などがある。

【０１２３】

未使用資産の経済的活用手段の一つに、「共有経済」と呼ばれる概念の利用がある。まず車の相乗りで一般的となり、その後ＵｂｅｒやＬｙｆｔの相乗りサービスで広まった共有経済は、十分に利用されていないリソースを、それを必要としている人々に利用させることにより、それらのリソースを活用する、即ち需要に供給を合わせる試みである。インベストペディアでは、共有経済は「商品またはサービスの利用権をＰ２Ｐ（ピアツーピア）方式で取得、提供、または共有する行為として定義される、しばしばコミュニティベースのオンラインプラットフォームによって実現される経済モデル」と定義されている。十分に活用されていないリソースを課題解決やサービス提供に生かすと同時に、天然資源の節約にもなるため、共有経済は環境的にも有益である。共有経済は、分散コンピューティング、クラウド通信、分散ストレージ、ブロックチェーンサービス、及び分散型通貨に等しく当てはめることができる。

【０１２４】

分散コンピューティング

【０１２５】

分散コンピューティングでは、１つのタスクを分割して、ネットワークで相互接続されたコンピュータのグループに分配する。サーバで構成されるプライベートクラウドを利用することが可能であるが、分散コンピューティングのメリットの一つは、コンピュータを所有することなく、それらのアクセスと利用を行えるため、演算キャパシティを無制限に利用できることにある。例えば図７Ａ及び７Ｂには、一週間及び任意の一日におけるコンピュータ及びサーバの使用及び未使用キャパシティが示されている。図７Ａでは、利用率を示す曲線５０から、午前８時から午後５時までを除く、１日の残りの１５時間は未使用の演算キャパシティ５１が大量に残存していることが分かる。世界を３つの時間帯に分けたとすると、一日のどの時間においても、世界の演算リソースの３分の２が使われないままとなっていることになる。また、図７Ｂに示されているように、演算リソースの１日の

平均利用時間５２は、月曜から木曜までは約９時間であるが、週末は３時間以下に落ち込む。即ち、未使用の演算キャパシティの一週間分の合計をとると、世界のどの時間帯においても、実際は全コンピュータの７３％が使われていないことになる。上記の分析では、暗号通貨マイナー、ゲーマー、ホームコンピュータ、及びＩｏＴデバイス（冷蔵庫、エアコン、ルータ、ＨＤＴＶ、どこにでもあるケーブルセットトップボックスなど）の膨大な演算キャパシティは無視されている。

【０１２６】

この使われていない演算キャパシティを、天気予報、暴風雨進路予想、気候モデリング、癌研究、地球接近天体（地球と衝突する可能性のある小惑星）の探査、宇宙研究、ＳＥＴＩ（地球外知的生命体探査）といった、膨大な演算を要する処理に役立てることができれば、最小限の社会的コストで、またあらゆる分野で、持続可能な進歩を成し遂げることができる。今日のインターネットを利用した共有経済の利用例の一つに、ＢＯＩＮＣ（Ｂｅｒｋｅｌｅｙ Ｏｐｅｎ Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ ｆｏｒ Ｎｅｔｗｏｒｋ Ｃｏｍｐｕｔｉｎｇ）がある。その演算能力は、２０１８年６月時点でボランティアリソースのみで平均２０ ＰＦＬＯＰＳ（接頭辞Ｐはペタ即ち10^{15}を表す）に達し、そこではＳＥＴＩ@Ｈｏｍｅ及びＭｉｌｋｙＷａｙ@Ｈｏｍｅ（それぞれＢＯＩＮＣの合計演算サイクル数の４％を消費）、パルサーの調査研究を行うＥｉｎｓｔｅｉｎ@Ｈｏｍｅ（ＢＯＩＮＣのクラウドコンピューティングキャパシティの約１５％を消費）といったプロジェクトが運営されている（ｈｔｔｐｓ：／／ｅｎ．ｗｉｋｉｐｅｄｉａ．ｏｒｇ／ｗｉｋｉ／ＦＬＯＰＳ）。効果的なクラウドコンピューティングの鍵となるのはアップ時間、即ちホストデバイスの常時稼働であるため、これらのデバイスはＡＣ電源で動作し、使われていない間も稼働し続ける。

【０１２７】

ノートＰＣ、タブレット、スマートフォンといったモバイルデバイスに搭載された演算リソースも膨大な量に上る。２０２０年までに、全世界のスマートフォン普及台数は３０億台を超えると予想されている（ｈｔｔｐｓ：／／ｗｗｗ．ｓｔａｔｉｓｔａ．ｃｏｍ／ｓｔａｔｉｓｔｉｃｓ／３３０６９５／ｎｕｍｂｅｒ－ｏｆ－ｓｍａｒｔｐｈｏｎｅ－ｕｓｅｒｓ－ｗｏｒｌｄｗｉｄｅ／）。最新世代のｉＰｈｏｎｅ（登録商標）にはＮＰＵニューラルプロセッサが搭載され、その演算能力は毎秒６，０００億浮動小数点演算数、即ち６００ ＧＦＬＯＰＳに達する。これを考慮すると、世界全体のスマートフォンの分散コンピューティングキャパシティの合計は、まもなく（600×10^{9} ＦＬＯＰＳ／デバイス）×（3×10^{9}台のデバイス）＝1.8×10^{21} ＦＬＯＰＳ、即ち約２ ＺＦＬＯＰＳ（Ｚはゼータの接頭辞、10^{21}を表す）と、ＢＯＩＮＣのボランティア方式のコンピューティングネットワークを５桁も上回るものとなろうとしている。

【０１２８】

今日のインターネットには、使われていない、または十分に利用されていないリソースを特定したり、ユーザがそういったリソースにアクセスできるようにする仕組みがないという問題がある。また、社会奉仕は素晴らしいことではあるが、来月の水道光熱費の工面に苦労している一般庶民が、いくら崇高な目的のためとはいえ、自らの演算サイクル数を気前よく提供するかどうかは極めて疑わしい。リソースを提供してくれたら報酬を支払おうと考える業者も存在するが、リソースを求めている業者を提供者（使用されていない演算サイクル数を提供する人々）に引き合わせたり、功績に見合った適正な報酬を支払う手段を提供するシステムや市場は存在しない。従って、今日のインターネットには、コンピューティング共有経済をサポートする能力はない。

【０１２９】

さらに言えば、コンピューティングデバイスやＩｏＴデバイスの多くが常時稼働しているため、所有者や社会に何の恩恵やメリットもなく、常に電力が消費されていることも問題となる。例えば、セットトップボックスの２０１７年の合計消費電力は、米国内だけでも２１ ＴＷｈ（テラワット時）に達する。これは５つの原子力発電所の発電量にほぼ匹敵するが、これらのデバイスは、ほとんどの時間は何もしていない。環境の持続可能性の

ためには、セットトップボックスにも、スマートフォンと同様の、及び共有経済で有益なコンピューティングのために使われているものと同じ電力管理システムの採用が必要となる。

【０１３０】

クラウド通信

【０１３１】

共有経済の可能性はクラウド通信にも及ぶ。数十年前は、一握りの電話会社が世界の通信トラフィックを独占していたが、インターネットとモバイルネットワークの出現によって、ＩＳＰ（インターネットサービスプロバイダ）や携帯キャリアが続々と誕生した。しかし近年は、ＩａａＳ（Ｉｎｆｒａｓｔｒｕｃｔｕｒｅ－ａｓ－ａ－Ｓｅｒｖｉｃｅ）、ＳａａＳ（Ｓｏｆｔｗａｒｅ－ａｓ－ａ－Ｓｅｒｖｉｃｅ）、及びＰａａＳ（Ｐｌａｔｆｏｒｍ－ａｓ－ａ－Ｓｅｒｖｉｃｅ）サービス市場の成長に伴い、少数のグローバルサプライヤ（主にＡＷＳ、Ａｚｕｒｅ、ＧＷＳ、及びＩＢＭ　Ｃｌｏｕｄ）への市場統合が急速に進んでいる。

【０１３２】

このクラウドの寡占化の進行は、インターネットから生まれた分散化のトレンドを逆転させるものであり、ネットワークトラフィック、データストレージ、及びデータ分析の独占的制御を、いかなる国民や政府の管轄下にもない特定の企業グループに集中させる結果となった。これらのメガ企業の成長を法令で縛ることも可能であるが、真の問題は、断片化したプラットフォームであるインターネットでは、民間企業のクラウドに代わるオープンソースの代替ソリューションは提供できず、ましてやオープンソース環境のセキュリティ問題を解決することなど不可能なことにある。しかし、もしグローバル通信ネットワークを共有経済の形で実現することができたとしたら、特にそのネットワークにモバイルフォンを取り込むことができたとすれば、民間企業のクラウドの寡占状態に十分に対抗できる見込みが生まれる。

【０１３３】

大規模サーバクラウドに対抗し得るグローバル通信ネットワークを実現するには、Ｐ２Ｐ（ピアツーピア）通信を導入することによって、ネットワークトラフィックの削減を図り、従量制クラウドサービスへの依存度を抑える必要がある。Ｐ２Ｐ通信の実現は農村部では非現実的であるが、人口の多い都市部であれば、ＱｏＳ（サービス品質）レベルの高いＰ２Ｐネットワークを実現できる可能性がある。実際に、１６億台のモバイルフォンが普及している中国では（ｈｔｔｐｓ：／／ｗｗｗ．ｔｈａｔｓｍａｇｓ．ｃｏｍ／ｃｈｉｎａ／ｐｏｓｔ／２７０９７／ｃｈｉｎａ－ｈａｓ－ｍｏｒｅ－ａｃｔｉｖｅ－ｍｏｂｉｌｅ－ｐｈｏｎｅｓ－ｔｈａｎ－ｐｅｏｐｌｅ）、人口よりも使われているモバイルフォンの方が多いことが２０１９年に報告されている。

【０１３４】

「広州市の数人の社会人に聞いたところによれば、彼らは仕事専用に１台、プライベート用にもう１台のモバイルフォンを保有している」（上記サイトより引用）。このような密なモバイルフォン台数をＰ２Ｐネットワークに取り込む仕組みは、今のところは存在しないが、ノード密度は既にサービスを実現する上で十分なレベルに達している。しかし、残念ながらＴＣＰ／ＩＰは、（特にハードウェアプラットフォームやオペレーティングシステムが異なる、多種多様なコンポーネントから構成される）アドホックネットワークの構築には適していない。

【０１３５】

Ｐ２Ｐ通信ネットワーク実現の可能性を持つもう一つの通信基盤にＶ２Ｖ（車車間）通信がある。ロサンゼルスでは、１２，５６１　ｋｍ^{2}の面積を有する都市部に６００万台の、即ち１平方キロメートル当たり約５００台の自動車が存在する。また上海では、６，３４１　ｋｍ^{2}の面積に３３０万台の自動車が密集し、こちらも１平方キロメートル当たりの台数は約５００台に及ぶ。このような密度であれば、有効なＰ２Ｐネットワークの実現に十分と言える。しかし残念ながら、上述のようにＴＣＰ／ＩＰは、アドホックネット

ワークを管理したり、データ中継を行うピアノードにパケットの内容を晒さずに、Ｐ２Ｐデータを転送する機能を有していない。

【０１３６】

分散型通貨

【０１３７】

Ｉｎｖｅｓｔｏｐｅｄｉａによれば、不換紙幣とは、「金などの商品による裏付けのない政府発行の通貨であり、法定不換紙幣は政府の中央銀行が通貨の印刷量を制御できるため、経済をより制御しやすいという性質がある」。政府と中央銀行は、需要と供給の真の市場力学によって設定されるのではなく、供給を制御し、恣意的、地政学的、利己的な利益に基づいて流通している通貨を恣意的に印刷したり、破棄したりすることで、通貨の価値を操作することができる。

【０１３８】

分散型通貨を開発しようとする初期の試みがやがて、世界初の暗号通貨であるビットコインの誕生につながった。数学的な課題を使用して新規トークンを生成するするマイニングと呼ばれる手法を用いることによって、ビットコインを新たに生成することが次第に困難になっていくため、流通するビットコインの数を事前に定義された量に制限される。新しいビットコインの供給を恣意的に制限することによって課せられた人為的な希少性が、その予測不可能な需要と相まって、ビットコインの価値は非常に不安定になり、ビットコインは実際の商取引には利用しづらい存在になってしまっている。商取引業者やサービス提供者は、日々変動する不確実な価値を持つ通貨を使って商売をすることはできない。

【０１３９】

また、今日の暗号通貨は生態学的に見て持続不可能である。環境保護主義者らは、今日実現されているような暗号通貨は、私たちの地球の天然資源を無闇に浪費する存在であると見なしている。２０１８年にビットコインとイーサリアムという２大暗号通貨のマイニングに消費された電力量は実に８３ＴＷｈにも達しており、これは地球上のエネルギー消費量が最も多い上位４０カ国を除くすべての国の年間エネルギー消費量を上回っている。このことが、暗号通貨が潜在的に有すると言われているが未だ証明されていないメリットと、そのエネルギー浪費というマイナスの性質とをどのように捉えるのかで大きな論争を引き起こしている。現在の暗号通貨は、プルーフオブワーク（ＰｏＷ）と呼ばれるマイニングとコンセンサスプロトコルに依存しているため、エネルギーの浪費の問題は解決できない。ＰｏＷは、もともと経済的な観点からハッカーがネットワークを攻撃しないようにするために開発された手法であり、意図的にエネルギー効率の良い設計になっている。

【０１４０】

暗号通貨のもうひとつの特徴は、分散型通貨システムにおける不正行為や二重支出を防ぐために必要な信頼できる経歴を確保するために、ブロックチェーン技術に密接に依拠している点が挙げられる。ビットコインの家系図の検証を可能にするために、トレーサビリティは、新規コインを生み出すすべてのマイニングイベント、コインのすべての転送、メインブロックチェーンに由来するすべてのハードフォークとソフトフォークを含め、その起源に至る範囲にまで及んでいる。記録管理がこのように徹底的になされるため次の３つの影響が表出することになった。すなわち、（ｉ）ブロックチェーンが過度に長くなる、（ｉｉ）解決時間（コインの真偽を確認するために必要な時間）に長い時間がかかる、そして（ｉｉｉ）取引に時間がかかりすぎた場合に受取人がコインの有効性の確認を徹底して行わなくなる、という点である。

【０１４１】

検証が不完全であれば、詐欺や二重支出の悪用が生まれる。ブロックチェーンが野放しにされている期間が長ければ長いほど、その長さはより長くなり、検証に要する時間も増大する。現在、新しいビットコインのサイズは１５６．４ＧＢもの長さであり、この数字は日増しに増大している。各ビットコインのメモリ要件は法外なもので、持ち運ぶには大すぎ、便利に使用できるものとは言えない。グローバルな取引が行われるたびに、ブロックチェーンは長くなり、コインを保存するために必要なメモリサイズは増大していく。新

しいブロックチェーンが加わるたびに増大するメモリサイズは、通常、実行されるトランザクションの種類に応じて０．５～１．０ＭＢの間とされている。

【０１４２】

現在の暗号通貨のもうひとつの大きな関心事は、スケーラビリティの問題である。プルーフオブワーク（ＰｏＷ）を使用してＰｏＷ暗号通貨を使用する人が増えれば増えるほど、単位ブロックチェーンは長くなり、使用するのが難しくなっていく。例えば、ビットコインが世界的な通貨になったと想定した場合、毎日何百ギガバイトものデータをブロックチェーンに追加していけば、ほとんど役に立たなくなることが研究で明らかになっている。議論のために、８ＭＢのブロックを完全に検証するのに１５０分かかると仮定すると、もしビットコインが世界的に支配的な通貨になった場合、そのブロックサイズは必然的に２．４ＧＢに膨れ上がり、検証に５１，０００分以上（２年以上）もの時間が経過してしまう。プルーフオブステーク（Ｐｒｏｏｆ－ｏｆ－Ｓｔａｋｅ）のような代替的なコンセンサスプロトコルも提案されているが、それらは主にブロックチェーンへの攻撃に関する問題に対処するためのものであって、速度・性能を向上させるというより、問題を解決するための手法なのだ。さらに、こうしたコンセンサス手法は、まだホワイトペーパーやカンファレンスの話題の範囲に留まっている。

【０１４３】

暗号通貨の今日の姿について端的に表現してみれば、実際の商取引で利用するには扱いにくく、安定性にかける金融商品といったところであろう。

【０１４４】

ＶＩ．結論

【０１４５】

結論として、インターネットは、世界中のいたるところに行き渡っているとはいえ、セキュリティを守り、プライバシーを保護し、電子商取引を可能にし、シェアリングエコノミーをサポートするためのプラットフォームとして設計されたものではなかった。インターネットの最大の弱点は、現在では完全に明らかになっている。すなわち、

・セキュリティなし
・プライバシーなし
・信頼性なし

【０１４６】

これらの問題は、いまだに問題であり続け、解決できないままである。暗号技術や証明書機関発行のデジタル署名を用いてこれらの欠陥を改善しようとする試みはいくつもあるが、サイバー犯罪の深刻さとその規模の絶え間ない拡大からも明らかなように、完全に失敗に終わっている。

【０１４７】

インターネットは、明らかに、リアルタイム通信、分散型クラウドコンピューティング、クラウドデータストレージ、クラウド接続デバイス、電子取引、電子商取引を安全かつ個人的に促進するグローバルなプラットフォームとしては適していない。ほとんどすべての近代的ネットワーク通信は、インターネットとしてグローバルに実現されていても、あるいはサブネットとしてローカルに実装されていたとしても、その基盤となる通信プロトコルにＴＣＰ／ＩＰを採用しているため、あらゆる通信や電子商取引は、この技術が本来的に持っている脆弱性にさらされている。この脆弱性は、データ伝送に使用される物理媒体が、光ファイバ、有線イーサネットネットワーク、無線ＷｉＦｉ　ＬＡＮ、セルラーネットワーク、ケーブル配信ネットワーク、衛星通信ネットワーク、その他のピアツーピアネットワークのいずれであっても、それには関係なく、常にそこにあるのだ。

【０１４８】

ＴＣＰ／ＩＰの脆弱性以外にも、デバイスのハードウェアや、物理層及びデータリンク通信層には、データパケット通信の内容やメタデータの傍受や操作、メモリ内のデータの破損、システムやアプリケーションソフトウェアの上書き、マルウェア、バックドア、スパイウェア、フィッシングソフトウェアの検出不能なインストール、オペレーティングシ

ステムの簒奪の可能性など、さらなるセキュリティやプライバシーのリスクが顕在化している。

【０１４９】

現在の通信システムやネットワークでは、暗号通貨の安全な取引、暗号通貨の安全な保管、偽物や盗まれた暗号通貨の不正使用の防止はもちろんのこと、分散型取引の検証が、有効な取引のタイムリーな実行を妨害・拒否したり、詐欺的取引を正当な取引として認証してしまうようプログラムされたサイバーボットによって乗っ取られないよう保護することは不可能なのである。現在の通信システムやネットワークでは、ひとつまたは複数のＯＳＩ通信層で行われるサービス拒否攻撃を回避することはできない。

【０１５０】

現在の通信システムやネットワークでは、信頼性の高いリアルタイム通信に必要な伝搬時間やネットワーク遅延を最小限に抑えたり、リアルタイムＱｏＳを保証したり、データパケットの性質やユーザの要求に合わせてデータパケットの伝送効率や冗長性、緊急性を調整したりすることはできない。今日のどの電子商取引システムも、ユーティリティートークンを使用した電子商取引のためのデジタル取引のコスト安定性を確保しつつ、市場の需要に基づく暗号通貨の変動性を求める投資家の欲求にも応えることはできない。

【０１５１】

現在の通信システムやネットワークでは、グローバルな通信、コンピューティング、データストレージの容量を効果的に再配分して、市場力学に沿った商業、研究、慈善活動の効用を最大化し、資源の過小利用やエネルギーの無駄な消費、グローバルなネットワーク資産やコンピューティングキャパシティの平等な管理を回避することはできない。現在の通信システムやネットワークでは、地球上のすべての人々のプライバシーを危険に晒す大規模なデータ侵害を効果的にブロックすることはできない。

【０１５２】

現在のネットワーク及びトランザクションの脆弱性のより詳細な説明及び分析は、２０１８年７月１０日に出願された「Ｔｈｅ　ＨｙｐｅｒＳｐｈｅｒｅ－ａ　Ｒｅａｌ－ｔｉｍｅ　Ｃｙｂｅｒｓｅｃｕｒｅ　Ｐｒｉｖａｃｙ　Ｎｅｔｗｏｒｋ　ｗｉｔｈ　Ｅｍｂｅｄｄｅｄ　ＤｙＤＡＧ　Ｄｕａｌ　Ｃｒｙｐｔｏｃｕｒｒｅｎｃｙ　ｆｏｒ　Ｇｌｏｂａｌ　ｅ－Ｃｏｍｍｅｒｃｅ」（ＨｙｐｅｒＳｐｈｅｒｅ　－　グローバル電子商取引を実現するＤｙＤＡＧデュアル暗号通貨内蔵リアルタイムサイバーセキュアプライバシーネットワーク）と題する仮特許出願６２／６９６，１６０に記載されており、参照により本書に含まれている。

【０１５３】

必要とされることは、クラウドベースの通信、ネットワーキング、コンピューティング、データストレージ、分散型暗号通貨に対するまったく新しいアプローチをとることで、既述のプライバシー、セキュリティ、パフォーマンス、社会的責任、持続可能性の問題に対処しながら、ネットワークとそれに接続されたデバイスの犯罪性、詐欺、ハッキングを抑制することなのである。実のところ、先見の明のあるインターネットの創設者であるティム・バーナーズ・リー（ワールドワイドウェブの創設者）やスティーブ・ウォズニアック（パーソナルコンピュータの発明者）でさえ、この無数の問題を解決するにはインターネットの完全な再構築が必要だと公言しているのである。

【発明の概要】

【課題を解決するための手段】

【０１５４】

本発明に従って、データはネットワークまたは「クラウド」を経由して、携帯電話またはノートブックコンピュータなどのクライアントデバイス間で転送される。クラウドには、サーバまたは他のタイプのコンピュータまたはデジタル機器上で個別にホストされている複数のノードが含まれる。ＳＤＮＰクラウド内のメディアノード間での転送中、データは固定長または可変長のデジタルビットの離散的文字列であるパケット形式をとる。

【０１５５】

ノードに導入されたソフトウェアは、「ネームサーバ」、「権限」、「タスク」の３つの機能を実現する。「ネームサーバ」機能は、クラウドに接続されているクライアント機器の動的なリストを管理する機能である。「タスク」機能は、クラウドを介してノードからノードへと進むパケットの受信と送信を行う機能である。「権限」機能は、クラウドを通過するパケットの各ルート（例えば、ノードＡからノードＢからノードＣへなど）を決定し、ルート上の各ノードに「コマンド及び制御」パケットを送信するほか、クラウドを通る「次のホップ」でどこにパケットを送信するかをノードに指示する。パケットは断片化されていてもよい。つまり、複数のサブパケットに分割されて別々の経路を移動し、宛先のクライアント装置で元のパケットに復元されもよい。パケット及びサブパケットは、ノードを通過する際に、様々なステートベースのアルゴリズムに従って、スクランブル化及び／または暗号化されてもよい。タスク機能は、受信パケットがどのアルゴリズムによってスクランブル解除または復号化されるべきか、及び送信パケットがどのアルゴリズムによって暗号化またはスクランブル化されるべきかを決定する機能と言うこともできる。

【０１５６】

ノードは「メタモルフィック」である。つまり、各ノードはネームサーバ、権限、タスクの機能を実行できるが、同時に複数の機能を実行することはないことを意味している。機能を実行していないノードは、「未分化」ノードと表現する。ノードにインストールされているソフトウェアにより、ネームサーバ機能、オーソリティ機能、タスク機能のいずれの機能が要求されているかを、ノードへの要求の性質から判断することができる。指定されたジョブが終了すると、ノードは次の実行要求を待機するために「未分化」状態に戻り、最後に行った動作に関する情報をすべて破棄する。

【図面の簡単な説明】

【０１５７】

【図１】ＴＣＰ／ＩＰ通信スタックを備えた計算機装置のブロック図である。

【図２】パケットルーティングのＴＣＰ／ＩＰデータグラムを示している。

【図３】ＴＣＰ／ＩＰ通信スタックとデータグラム構築の説明図である。

【図４】中間者攻撃（ＭｉＭ）によるインターネットパケットハイジャックを説明している。

【図５】インターネット認証局を示している。

【図６】インターネットブロックチェーンの処理を説明している。

【図７Ａ】１日当たりのサーバ及びコンピュータの容量を説明している。

【図７Ｂ】週当たりのサーバとコンピュータの容量を説明している。

【図８】ＳＤＮＰ（Ｓｅｃｕｒｅ Ｄｙｎａｍｉｃ Ｃｏｍｍｕｎｉｃａｔｉｏｎ Ｎｅｔｗｏｒｋ Ａｎｄ Ｐｒｏｔｏｃｏｌ）メッシュネットワークの一例を示している。

【図９】ＳＤＮＰメッシュネットワークの要素について説明している。

【図１０】メッシュ化されたネットワーク上でのＳＤＮＰルーティングのフローチャートである。

【図１１Ａ】ＳＤＮＰ登録動作の説明図である。

【図１１Ｂ】ＳＤＮＰネームサーバへの問い合わせ動作の説明図である。

【図１１Ｃ】ＳＤＮＰルーティング要求動作の説明図である。

【図１１Ｄ】ＳＤＮＰネットワークノード要求動作の説明図である。

【図１１Ｅ】ＳＤＮＰルーティング指示ディスパッチャの動作の説明図である。

【図１１Ｆ】ＳＤＮＰ第１パケットトランスポート動作の説明の図である。

【図１１Ｇ】ＳＤＮＰ第２パケットトランスポート動作の説明の図である。

【図１１Ｈ】ＳＤＮＰ第３パケットトランスポート動作の説明図である。

【図１１Ｉ】ＳＤＮＰ第４パケットトランスポート動作の説明図である。

【図１２Ａ】分散型ＳＤＮＰメッシュネットワークの一例を示す図である。

【図１２Ｂ】代替となる分散型ＳＤＮＰメッシュネットワークの一例を示す図である。

【図１２Ｃ】分散型ＳＤＮＰメッシュネットワークの要素を示す図である。

【図１２Ｄ】ＤｙＤＡＧメッシュネットワーク上での分散型ＳＤＮＰルーティングのフロ

ーチャート（その１）である。
【図１２Ｅ】ＤｙＤＡＧメッシュネットワーク上での分散型ＳＤＮＰルーティングのフローチャート（その２）である。
【図１３Ａ】分散型ＳＤＮＰ登録及びネームサーバによるクエリの動作説明図である。
【図１３Ｂ】分散型ＳＤＮＰルーティング要求の動作説明図である。
【図１３Ｃ】分散型ＳＤＮＰネットワークノード要求の動作説明図である。
【図１３Ｄ】分散型ＳＤＮＰ　Ｃ＆Ｃルーティング指示ディスパッチャの動作説明図である。
【図１３Ｅ】第１の分散型ＳＤＮＰデータグラムパケットトランスポートの動作説明図である。
【図１３Ｆ】第２の分散型ＳＤＮＰデータグラムパケットトランスポートの動作説明図である。
【図１３Ｇ】第３の分散型ＳＤＮＰデータグラムパケットトランスポートの動作説明図である。
【図１３Ｈ】第４の分散型ＳＤＮＰデータグラムパケットトランスポートの動作説明図である。
【図１４】ｄ'ＳＤＮＰ拡散データクラウドへのＨｙｐｅｒＮｏｄｅアクセスのための選択基準を示す図である。
【図１５Ａ】メタモルフィックＨｙｐｅｒＮｏｄｅの呼び出し開始のための｜ＮＳ｜ノードへの変換を説明する図である。
【図１５Ｂ】ａｎａｍｅサーバの拡散データクラウドデータから発信者ＩＤ情報をダウンロードして、分化された｜ＮＳ｜ノードへと変換する様子を示す図である。
【図１６Ａ】メタモルフィックなＨｙｐｅｒＮｏｄｅを経路計画用の｜Ａ｜ノードに変換する流れを示す図である。
【図１６Ｂ】ａｎａｍｅサーバの拡散データクラウドデータから発信者ＩＤ情報をダウンロードして、分化された｜Ａ｜ノードへと変換する様子を示す図である。
【図１６Ｃ】ネットワークホップ時間順にソートされた利用可能なタスクノードのｄ'ＳＤＮＰ権限ノードの処理方法を説明する図である。
【図１７Ａ】ルートディスパッチのためのメタモルフィックＨｙｐｅｒＮｏｄｅの｜Ａ｜ノードへの変換方法を示す図である。
【図１７Ｂ】選択されたＳＤＮＰアドレスに対応する現在のダイナミックＩＰアドレスをリストアップしたタスクノード変換テーブルのダウンロードを示している。
【図１８Ａ】｜Ａ｜ノードのコマンド＆制御（Ｃ＆Ｃ）ルーティングコマンドに対して、メタモルフィックなＨｙｐｅｒＮｏｄｅをルーティング用の｜Ｔ｜ノードに変換する様子を示す図である。
【図１８Ｂ】複数の動的コンシールメントアルゴリズム（シングルホップ暗号化サイファを含む）で構成されるｄ'ＳＤＮＰタスクノード共有秘密のダウンロードフローの説明図である。
【図１８Ｃ】受信パケット及び送信パケットに対して動的隠蔽方法を使用してデータグラムを処理するｄ'ＳＤＮＰタスクノードを示す図である。
【図１９】多層拡散データクラウドを模式的に示す図である。
【図２０】ＨｙｐｅｒＳｐｈｅｒｅの拡散データクラウドを実現し、アクセスするための様々な方法の図解である。
【図２１】非集約型データを用いた拡散型クラウドストレージの実現方法の図解である。
【図２２】ｄ'ＳＤＮＰネームサーバの拡散データクラウドストレージとアクセスキーの冗長ファイル管理の方法の図解である。
【図２３】ＨｙｐｅｒＮｏｄｅの動的特性に関してネームサーバの拡散データクラウドを更新するためのフローチャートである。
【図２４】ＨｙｐｅｒＳｐｈｅｒｅのタスクノードの分散型クラウドにおける動的メッシュデータルーティングのフローチャートである。

【図２５】ホップバイホップの状態に基づく動的隠蔽アルゴリズムを利用したｄ'ＳＤＮＰデータのパケット伝送の図解である。
【図２６】｜ＮＳ｜、｜Ａ｜、｜Ｔ｜の区別されたＨｙｐｅｒＮｏｄｅ間の分業を表すｄ'ＳＤＮＰデータグラムである。
【図２７】ＨｙｐｅｒＳｐｈｅｒｅの７層ＯＳＩ通信スタックと対応するｄ'ＳＤＮＰデータグラムを階層的に表現したものである。
【図２８】同種のＨｙｐｅｒＮｏｄｅをホストする異種クラウドのグラフである。
【図２９】通信、コンピューティング、データストレージ、及びクラウド接続デバイスを実行するソフトウェアで構成されるＨｙｐｅｒＳｐｈｅｒｅポータルの種類を図解している。
【図３０】パーソナルメッセンジャーの動作を示すＨｙｐｅｒＳｐｈｅｒｅ通信アプリケーションの一例を示す図である。
【図３１】ｄ'ＳＤＮＰデータグラムトランスポートのメッセンジャーペイロードの動的隠蔽の一例を示している。
【図３２Ａ】移動体（セルラー）キャリアネットワーク上の車両間インフラストラクチャ（Ｖ２Ｉ）ベースのネットワークのグラフである。
【図３２Ｂ】間接的な移動体ネットワークアクセスを維持する自律型アドホック車両対車両（Ｖ２Ｖ）ネットワークのグラフである。
【図３２Ｃ】モバイルネットワークアクセスから分離された完全自律型アドホック車両対車両（Ｖ２Ｖ）ネットワーク（マイクロクラウド）のグラフである。
【図３２Ｄ】モバイルネットワークアクセスから分離され、利用可能なＨｙｐｅｒＮｏｄｅにアクセスするために動的に再構成された完全自律型アドホック車両対車両（Ｖ２Ｖ）ネットワークのグラフである。
【図３２Ｅ】モバイルネットワークアクセスから分離され、利用可能なＨｙｐｅｒＮｏｄｅにアクセスするために動的に再構成された、完全自律型のアドホック車両対車両（Ｖ２Ｖ）ネットワークの更新されたグラフである。
【図３３Ａ】複数（８０２．１１互換）のＯＦＤＭ変調マイクロ波キャリアを用いたＨｙｐｅｒＳｐｈｅｒｅ　ＨｙＦｉ無線ルータの概略図である。
【図３３Ｂ】複数のマイクロ波無線チャネルと複数のＷｉＦｉプロトコルを介した断片化データ伝送を用いたＨｙＦｉルータｄ'ＳＤＮＰマルチＰＨＹ通信の一例を示す図である。
【図３４Ａ】ＩＥＥＥ　８０２．３互換（マルチＰＨＹ）通信の複数チャンネルが可能なＨｙｐｅｒＳｐｈｅｒｅ　Ｅｔｈｙｒｎｅｔ有線ルータの概略図である。
【図３４Ｂ】複数の８０２．３互換イーサネット媒体及びプロトコル上のｄ'ＳＤＮＰのフラグメント化データトランスポートを使用したイーサネットルータのマルチＰＨＹ通信の一例を示す図である。
【図３５Ａ】ケーブルモデム終端システム（ヘッドユニット）と複数のケーブルモデム（またはＳＴＢ）下流装置のためのｄ'ＳＤＮＰ対応通信スタックからなるＨｙｐｅｒＳｐｅｌｌｅケーブルシステムの概略図である。
【図３５Ｂ】トレリス符号化マルチチャネルＤＯＣＳＩＳ３ケーブル通信を採用したｄ'ＳＤＮＰフラグメント化データトランスポートの一例を示す図である。
【図３５Ｃ】ＤＯＣＳＩＳ３対応ケーブルモデム動作時の複数のｄ'ＳＤＮＰチャンネルとＨＤＴＶコンテンツのトレリス符号化の一例である。
【図３６Ａ】複数のキャリア周波数及びセルラープロトコル（４Ｇ及び５Ｇを例示）を介した断片化されたデータパケットのｄ'ＳＤＮＰトランスポートを使用したＨｙｐｅｒＳｐｅｌｉｃａｔｉｏｎモバイルネットワーク通信の概略図である。
【図３６Ｂ】複数のキャリア周波数及びセルラープロトコル（４Ｇ及び５Ｇを例示）を介した断片化されたデータパケットのｄ'ＳＤＮＰトランスポートを図解した、ＨｙｐｅｒＳｐｌｅａｔｉｏｎ対応モバイルネットワークへのエッジデバイス（携帯電話またはタブレット）のアクセスの概略図である。
【図３７Ａ】８０１．１１プロトコルに対応するマイクロ波通信を介したＨｙｐｅｒＳｐ

ｈｅｒｅ対応ＩｏＴデバイスの概略図である。
【図３７Ｂ】Ｄ'ＳＤＮＰネットワークからＩｏＴデータグラムのダウンロード及びアップロードコンテンツへのＤ'ＳＤＮＰネットワークを説明するＨｙｐｅｒＳｐｅｌｅ　ＩｏＴデバイスの概略図である。
【図３７Ｃ】ＩｏＴデバイスクラウドのＨｙｐｅｒＳｐｈｅｒｅ　ＨｙＦｉネットワーク制御を説明する概略図である。
【図３８Ａ】冗長ストレージ要素と復元機構を備えたクライアント所有のファイルの非集約型データストレージのためのハイパーセキュアクラウドの概略図である。
【図３８Ｂ】プライベートデータとコラボレーションファイルの両方を含むユーザ所有の拡散データクラウドのアクセス制御を説明する概略図である。
【図３９Ａ】ＨｙｐｅｒＳｐｈｅｒｅクラウドコンピューティングアプリケーションのＨｙｐｅｒＣｏｎｔｒａｃｔジョブ仕様を示すフローチャートである。
【図３９Ｂ】ＨｙｐｅｒＳｐｈｅｒｅクラウドコンピューティングアプリケーションのハイパーセキュアジョブの実行手順を示すフローチャートである。
【図４０】アカウント開設手順を説明している。
【図４１】オフラインルート証明書を使用してオンラインＣＡ証明書に署名する方法を示している。
【図４２】信頼できる検証済み証明書を使用して先行証明書に署名することにより、信頼チェーンを形成するプロセスを示している。
【図４３】信頼できる検証済み証明書を使用して先行証明書に署名することにより、信頼チェーンを形成するプロセスを示している。
【図４４】パーソナライズされたマルチツリーＤｙＤＡＧブロックチェーンを示している。
【図４５】循環型有向グラフと多次元有向グラフの比較を示す。
【図４６】ＤｙＤＡＧ（ｄｙｎａｍｉｃ　ａｃｙｃｌｉｃ　ｇｒａｐｈ）の２Ｄ及び３Ｄ表現を示す。
【図４７】タスクＨｙｐｅｒＮｏｄｅｓのＨｙｐｅｒＣｏｎｔｒａｃｔタスクベースの暗号通貨報酬を示す。
【図４８】ＨｙｐｅｒＳｐｈｅｒｅマーチャントＡＰＩが生成したＨｙｐｅｒＣｏｎｔｒａｃｔとプレッジを示す。
【図４９】鋳造とリサイクルによるハイパーコインの合成を示す。
【図５０】一時的かつ変更不可能なブロックチェーンのＨｙｐｅｒＣｏｎｔｒａｃｔの実行による、ＨｙｐｅｒＣｏｉｎのマイニングと陪審員による検証のフローチャートである。
【図５１】データパケットのトランスポート中の結合ハイパーノードホップコード（ＨＨＣ）生成を示す。
【図５２】一時的で取り消し不能なブロックチェーンのハイパーコントラクト実行による、ハイパーコインのリサイクルと陪審員検証のフローチャートである。
【図５３】ブロックチェーンのデフラグメンテーションを実行するためのＨｙｐｅｒＳｐｈｅｒｅプロセスシーケンスを示す。
【図５４】補助サイドチェーンの作成及び検証のためのＨｙｐｅｒＳｐｈｅｒｅブロックチェーンプロセスを示す。
【図５５】事前承認された支払いプロキシを容易にするワンタイムトランザクショントークン（ＯＴ^{3}）を使用するＨｙｐｅｒＳｐｈｅｒｅ支払い処理の概略図である。
【図５６】ＲＢＯＳ（ｒｅｐｌｉｃａｎｔ　ｂｌｏｃｋｃｈａｉｎ　ｏｂｓｅｒｖｅｒ　ｓｅｇｍｅｎｔｓ）を使用したＨｙｐｅｒＳｐｈｅｒｅの高速トランザクション検証とプライバシー保護の概略図である。
【図５７】陪審員のコンセンサスサラウンド攻撃を防止するためのハイパーノードトンネルの使用の概略図である。
【図５８】ＨｙｐｅｒＭｅｔａｌとＨｙｐｅｒＣｏｉｎの誓約によるＨｙｐｅｒＣｏｎｔｒａｃｔの実行によるＨｙｐｅｒＣｏｉｎのマイニングとリサイクルを含むＨｙｐｅｒＳｐｈｅｒｅ電子商取引の暗号経済学を示す。

【図５９】プラスとマイナスの経済的フィードバックメカニズムを含む、付加価値取引の経済的増幅表現を示すフローチャートである。
【発明を実施するための形態】
【０１５８】
通信を確保し、プライバシーを確保し、信頼されたビジネスと電子商取引をサポートするというインターネットの欠陥を克服するために、リアルタイム通信、データストレージ、クラウドコンピューティング、クラウド接続されたデバイス、及び電子サービスをサポートするグローバル電子商取引のための革新的かつ高度な分散型サイバーセキュア「プライバシー」ネットワークであるＨｙｐｅｒＳｐｈｅｒｅを紹介する。２０１８年7月１０日に出願した米国仮出願第６２／６９６，１６０号「Ｔｈｅ　ＨｙｐｅｒＳｐｈｅｒｅ－Ａ　Ｒｅａｌ－ｔｉｍｅ　Ｃｙｂｅｒｓｅｃｕｒｅ　Ｐｒｉｖａｃｙ　Ｎｅｔｗｏｒｋ　ｗｉｔｈ　Ｅｍｂｅｄｄｅｄ　ＤｙＤＡＧ　Ｄｕａｌ　Ｃｒｙｐｔｏｃｕｒｒｅｎｃｙ　ｆｏｒ　Ｇｌｏｂａｌ　ｅ－Ｃｏｍｍｅｒｃｅ」に記述したように、ＨｙｐｅｒＳｐｈｅｒｅは、分散型通信とグローバル電子商取引を可能にするためのオープンソースのビジネスプラットフォームと技術で構成されており、以下の機能を採用している。
・分散型のハイパーセキュアな通信
・ネットワークネイティブな認証局
・ＨｙｐｅｒＳｐｈｅｒｅブロックチェーン処理
・ネットワークネイティブな暗号通貨
これらの機能は、実行される各機能に固有の発明的事項を用いて促進される。分散型ネットワーク上でのハイパーセキュア通信の動作を理解するには、まず初めに前述の米国出願第１４／８０３，８６９号「Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｎｅｔｗｏｒｋ　ａｎｄ　Ｐｒｏｔｏｃｏｌ」（以下、「ＳＤＮＰネットワーク」または「ＳＤＮＰクラウド」と呼ぶ）に記載されているように、ネットワーク内の専用の単機能ノードによって実行される機能を考慮しなければならない。ＳＤＮＰクラウド外での通信は、「Ｍｅｔｈｏｄｓ　ａｎｄ　Ａｐｐａｒａｔｕｓ　ｆｏｒ　ＨｙｐｅｒＳｅｃｕｒｅ　Ｌａｓｔ　Ｍｉｌｅ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ」と題する前記米国出願第１５／９４３，４１８号に記載されている。
【０１５９】
Ａ．専用ノードでのＳＤＮＰルーティング
【０１６０】
図８は、エッジクライアントデバイスである携帯電話９５とノートブックコンピュータ９６からなるＳＤＮＰネットワークが、高速物理リンク１１０を使用して、ＳＤＮＰメディアノード１０６、ＳＤＮＰ信号サーバノード１０７、及びＳＤＮＰネームサーバノード１０８からなる専用の単機能ノードからなるＳＤＮＰクラウド１００を介して通信している様子を示している。携帯電話９５とＳＤＮＰクラウド１００との間のラストマイル通信は、セルタワー１０３ａ、１０３ｂと無線チャネル１１２ａ、１１２ｂとを含む移動体ネットワークを介して行われる。携帯電話９５は、インストールされたＳＤＮＰアプリケーション１０１を介してＳＤＮＰクラウド１００にアクセスする。ノートブック９６とＳＤＮＰクラウド１００との間のラストマイル通信は、ＷｉＦｉルータ１０５へのマイクロ波ラストリンク１１２ｃを介して発生し、これにより、ルータ１０４ａ、１０４ｂを介してラストマイル有線接続１１１ａ、１１１ｂを介してＳＤＮＰクラウド１００へのアクセスが完了する。ノートブック９６は、インストールされたＳＤＮＰアプリケーション１０２を介してＳＤＮＰクラウド１００にアクセスする。
【０１６１】
図９は、ＳＤＮＰネームサーバノード１０８、シグナリングサーバノード１０７、メディアノード１０６を含むＳＤＮＰネットワークを構成するリソースと、イーサネットルータ１０４、ＷｉＦｉルータ１０５を含み、ＴＣＰ／ＩＰルーティングテーブルを採用しているＳＤＮＰ非対応デバイスと、移動体通信事業者によるルーティングを管理するセルラー無線ネットワーク１０３とを図解している。

【０１６２】
ＳＤＮＰネームサーバノードは、電話番号、アカウント名、電子メールアドレス、またはその他の識別情報をデバイスのＩＰアドレスと照合するというネットワークのネームサーバの役割を実行するよう設計された専用の単一機能ソフトウェアで構成されている。ＳＤＮＰネームサーバに格納されているＩＰアドレスは動的なものである可能性があり、真のインターネットＤＮＳで認識されたアドレスではなく、ＮＡＴアドレスで構成されている場合もある。ＳＤＮＰネームサーバファイルは、デバイスの動的ＩＰアドレスが変更されるたびに、再登録プロセスによって更新される。図に示されているとおり、ＳＤＮＰネームサーバノード１０８は、任意の軽量サーバ１３０にインストールされ、サーバ１３０のＯＳアプリケーションＶＭ環境内で動作するＳＤＮＰネームサーバソフトウェア１３３を構成する仮想デバイスである。
【０１６３】
このように、ＳＤＮＰネームサーバノード１０８は、それをホストするサーバ１３０のハードウェアと同じものではない。ＳＤＮＰネームサーバノード１０８は、ＳＤＮＰルーティングを用いてＳＤＮＰクラウド内の他のノードと通信する。さらに、ＳＤＮＰネームサーバノード１０８は、インターネットのＤＮＳサーバに格納されていない動的データを保持する。ＳＤＮＰネームサーバノード１０８の機能は、ルックアップとアドレス変換のタスクに限定されており、パケットルーティングや、ＳＤＮＰクラウド１００内のメディアファイル（コンテンツ）の送信を行うことはない。ＳＤＮＰネームサーバノード１０８は、ＳＤＮＰネットワークを移動するいかなるメディアパケットの内容にもアクセスできず、またそこに存在するメディアパケットに適用される暗号化または隠蔽方法についても認識していない。ＳＤＮＰネームサーバノード１０８は、受信した問い合わせ、信号サーバノードに提供したデータ、またはどの信号サーバノードに提供したかの記録を保持しないという点で、（純粋にではないが）部分的にステートレスである。それは、ＳＤＮＰネットワーク名または郵便番号、電話番号、及び動的ＩＰアドレス間の変換テーブルを必然的に保持するという意味で、純粋にステートレスということではない。つまり、変換テーブルは動的であり、常に変化する動的ＩＰアドレスとポート番号が含まれており、それらが変更されたり、デバイスがＳＤＮＰクラウドにログインしたり、ログアウトするたびに更新される。ＳＤＮＰシグナルサーバノード（シグナリングサーバノードとも呼ばれる）は、パケットルーティングを指示し、パケットの伝搬遅延を最小限に抑えるタスクを実行するよう設計された専用の単一機能ソフトウェアで構成されている。
【０１６４】
ＳＤＮＰシグナルサーバノード（シグナリングサーバノードとも呼ばれる）は、パケットルーティングを指示し、パケットの伝搬遅延を最小限に抑えるタスクを実行するよう設計された専用の単一機能ソフトウェアで構成されている。ＳＤＮＰシグナルサーバノードは、一方的に、または同じ通信のルーティングを行う他のＳＤＮＰシグナルサーバノードと連携して、軽量なコマンド＆制御パケット（Ｃ＆Ｃ）を使用して、ＳＤＮＰメディアノードにルーティングコマンドを発行する。ＳＤＮＰシグナルサーバノードは、ホストデバイスの身元や所有権に関する知識を持たないＳＤＮＰネームサーバノードから取得したアドレスを使用する。示されているように、ＳＤＮＰシグナルサーバノード１０７は、任意の軽量サーバ１３０にインストールされ、サーバ１３０のＯＳアプリケーションＶＭ環境内で動作するＳＤＮＰシグナルサーバソフトウェア１３４からなる仮想デバイスである。
【０１６５】
このように、ＳＤＮＰ信号サーバノード１０７は、それをホストするサーバ１３０のハードウェアとは異なる。ＳＤＮＰシグナルサーバノード１０７は、ＳＤＮＰルーティングを用いてＳＤＮＰクラウド内の他のノードと通信する。ＳＤＮＰシグナルサーバノード１０７は、ＳＤＮＰネットワーク内の任意のデバイスの真の所有者に関する知識を持たず、発信者、着呼者、または他のエッジデバイスの身元に関する情報を持たない。また、ＳＤＮＰシグナルサーバノード１０７は、任意のＳＤＮＰメディアパケットの内容や、内部のペイロードがどのように隠されているか、または暗号化されているかに関しての情報も持

たない。ＳＤＮＰシグナルサーバノード１０７は、純粋にステートレスである。つまり、このノードは必要なときにいつでも起動され、ルーティングを実行するために必要な情報を収集し（単独で、または他のシグナルサーバノードと連携して）、コマンド＆制御（Ｃ＆Ｃ）パケットを選択されたメディアノードに分配し、その後、それまでに実行した情報をすべて破棄してしまう。シグナルサーバのステートレスな動作は、瞬間的健忘症と同じで、ネームサーバに要求したＩＰアドレスを記憶せず、最後に与えた指示やＣ＆Ｃパケットをどのメディアノードに送信したかも記憶していない。

【０１６６】

ＳＤＮＰメディアノードは、ＳＤＮＰネットワークを介してコンテンツ（メディア）のデータパケットを送信するタスクを実行するよう設計された専用の単一機能ソフトウェアで構成されている。メディアパケットのペイロードには、オーディオ、ビデオ、ソフトウェア、ブロックチェーン、暗号通貨、またはソフトウェアファイルの断片が含まれている場合がある。ＳＤＮＰメディアノードは、あるＳＤＮＰメディアノードから別のＳＤＮＰメディアノードにパケットを送信するシグナルルーティング命令をホップ単位で受信しており、個々のパケットがどこから送られてきて、どこに行き着くのかという情報を持たない。ＳＤＮＰメディアノードは、シグナリングサーバからＣ＆Ｃパケット内の命令を受信する。この命令には、ＳＤＮＰネットワークを通過するパケットのコンシールメントと内容をホップ単位で動的に変更するために使用される数値シードと暗号化鍵が含まれていることがある。

【０１６７】

図に示すとおり、ＳＤＮＰメディアノード１０６は２つの仮想デバイスで構成されている。一方の仮想デバイスは、高帯域幅サーバ１３１のＯＳアプリケーションＶＭ環境内で動作する任意の高帯域幅サーバ１３１にインストールされたＳＤＮＰメディアノードソフトウェア１３５で構成され、もうひとつの仮想デバイスは、エアギャップドサーバ１３０ａのＯＳアプリケーションＶＭ環境内で動作する任意の非ネットワーク（エアギャップド）サーバ１３０ａにインストールされたＤＭＺソフトウェア１３６で構成されている。エアギャップドコンピュータサーバ１３０ａは、インターネットを介して直接アドレス指定することはできず、さらにメディアノードソフトウェア１３５がアルゴリズムやコンシールメント方法などの特定の動的に変化するステートベースの情報のみを要求することができるファイアウォールまたは非武装地帯（ＤＭＺ）バリア１４０によってメディアノードとそのホストとから分離されている。

【０１６８】

このように、ＳＤＮＰメディアノード１０６は、サーバ１３１やエアギャップドＤＭＺサーバ１３０ａ、またはそれらをホストするハードウェアと同じものではない。ＳＤＮＰメディアノード１０６は、ＳＤＮＰルーティングを使用してＳＤＮＰクラウド内の他のノードと通信する。ＳＤＮＰメディアノード１０６は、ＳＤＮＰネットワーク内のデバイスの真の所有者に関する知識を持たず、発信者、受信者、または他のエッジデバイスの身元に関する知識を持たない。次のホップとその最後のホップを除いて、ＳＤＮＰメディアノード１０６はパケットの最終的な宛先またはパケットが出所についての情報を持たない。メディアノード１０６内であっても、認識している情報は限定的である。ＤＭＺソフトウェア１３６及びエアギャップドサーバ１３０ａは、ＳＤＮＰメディアノードソフトウェア１３５及び高帯域幅サーバ１３１によって処理または搬送されるメディアパケットの内容についての情報またはアクセス権を持たない。逆に、ＳＤＮＰメディアノードソフトウェア１３５は、ＤＭＺソフトウェア１３６が、メディアノード１０６によって搬送されるデータパケットのペイロードの内容を隠蔽するために、どのようにアルゴリズムを選択するか、またはファイル処理命令を選択するかに関する情報を一切持たない。

【０１６９】

全体として、メディアノード１０６はステートレスな方法で動作している。このため送信するメディアパケットの内容を保持せず、パケットのペイロードの複雑な動的編集である動的コンシールメントプロセスを実行する際に、そのパケットの出所、送信先、あるい

はそのコンテンツがどのように修正されたかといった情報を一切保持しない。ＤＭＺソフトウェアは準ステートレスである。これは、コンテンツの混合、分割、スクランブル、アンスクランブル、ジャンクデータの挿入と削除、暗号化と復号化などを含むコンシールメント処理のためのアルゴリズムのテーブルを記憶している必要があるが、アルゴリズムの選択と実行に使用されたステート、数値シード、暗号鍵を保有または見ることがないからである。サイバーセキュリティの分野では、ＤＭＺバリア１４０を越えた関係を、「ゼロ知識」と表現している。したがって、ＤＭＺサーバソフトウェア１３６に共有秘密として格納されているアルゴリズムが何らかの形で発見されたとしても（例えば、ミッションインポッシブルタイプの安全なサーバルームへのオンサイト侵入によって）、ＤＭＺサーバソフトウェア１３６は、メディアパケットのペイロードを処理するために使用されるステート変数、数値シード、及び暗号鍵を手にできないため、アルゴリズムの知識でコードを破ることはできない。さらに、受信パケットはスクランブルされ暗号化された情報のデータの断片しか含まないため、その元の内容を復号化する手段は存在しない。

【０１７０】

メディアパケットのトランスポートは、ＷｉＦｉルータ１０５、またはイーサネットルータ１０４のような非ＳＤＮＰ対応デバイスをまたいで、または無線ネットワーク１０３を介して発生する可能性もある。このケースは、発信者（エッジデバイス）とＳＤＮＰクラウドとの間の「ラストマイル通信」で特に起こりやすい。ＳＤＮＰパケットは７－ＯＳＩフォーマットに従っているため、ルータはＩＰアドレスをインターネット、サブネット、またはＮＡＴアドレスのための通常のＴＣＰ／ＩＰアドレスと見なし、パケットを通常のＴＣＰ／ＩＰパケットであるかのようにルーティングする。したがって、ＷｉＦｉルータ１０５を介したルーティングは、それぞれがＳＤＮＰノード対応デバイスに到達する前に、そのサブネットまたはＩＳＰプロバイダのルーティングテーブル１３７を採用し、通過する中間ルータはおそらくは１つないし２つを越えないであろう。

【０１７１】

同様に、イーサネットルータ１０４を介したルーティングは、それぞれがＳＤＮＰノード対応デバイスに到達するまで、ローカルＩＳＰプロバイダのルーティングテーブル１３８を使用する。無線ネットワーク１０３を介して、または同様にケーブルまたは衛星ネットワークを介してＳＤＮＰパケットを伝送する場合、ルーティングは、ネットワーク独自のネットワークルーティングテーブル１３９及びカスタムパケットフォーマット、例えば、３Ｇ、５Ｇ、衛星、またはＤＯＣＳＩＳ３プロトコルを使用して行われる。ネットワークアドレストランスレータ（ＮＡＴ）１３２は、専有パケットフォーマットをイーサネット互換のＴＣＰ／ＩＰパケットフォーマットに戻すために必要である。

【０１７２】

このように、ＳＤＮＰメディアパケットは、カスタムハードウェアや専用の独自所有のクラウドを必要とせずに、インターネットルータやＳＤＮＰノードのネットワークを介して伝送することができ、どのようなＴＣＰ／ＩＰネットワークにもＳＤＮＰクラウドをインストールすることができる。断片化された隠蔽パケットを非ＳＤＮＰ対応デバイス上で送信しても、通信セキュリティのリスクはないが、ネットワーク内のより長い遅延パスを通じてパケットをルーティングすることでパケットの伝搬遅延が増加し、通話品質のＱｏＳを低下させる可能性がある。

【０１７３】

図１０は、専用機能ＳＤＮＰノードを使用したＳＤＮＰ通信のシーケンスの一例である。ステップ２６０では、クライアントは携帯電話９５でホストされているＳＤＮＰクライアントアプリ１０１を介してセッションを開始する。このセッションは、ＶｏＩＰ電話、ビデオチャット、ビデオファイル、オーディオファイル、ファイル転送、トランザクションプロセス、グループチャット、会議通話などを含む、あらゆる種類の通信を構成することができる。ステップ２６１では、ＳＤＮＰクライアントアプリ１０１が、デフォルトのメディアノード１０６にアクセスし、その最寄りのネームサーバの動的ＩＰアドレスを得るためにネットワークにメッセージを送る。

【０１７４】
図１１Ａに示されている呼出の開始は、一般的にはラストマイル接続を介してクエリパケットをルーティングしている。この例では、無線リンク１１２ａを介してセルタワー１０３ａに接続し、その後、有線接続１２０を介して任意のＳＤＮＰメディアノード１０６に接続している。ある特定の地域内のすべてのメディアノードは、デフォルトでは、最も近いＳＤＮＰネームサーバノードのＳＤＮＰアドレスを知っている。これらのメディアノードは、ＳＤＮＰネットワークに参加する際に、自動登録プロセスの一部として、１つまたは複数のＳＤＮＰネームサーバのアドレスを学習する。メディアノードは、このネームサーバのＳＤＮＰアドレスをＳＤＮＰクライアントアプリ１０１に返す。
【０１７５】
図１１Ｂに示すステップ２６２において、ＳＤＮＰクライアントアプリ１０１は、次に有線接続１１３を介してＳＤＮＰネームサーバノード１０８にクエリを送出する。ＳＤＮＰネームサーバノード１０８は、次に、クライアントがコンタクトしようとしているデバイスまたは電話番号、すなわち受信者（または被呼者）の現在の動的ＳＤＮＰアドレスまたはＳＤＮＰジップコードを返す。別の方法、ただし安全性が低い方法では、クライアントアプリは、シグナルサーバノードのＳＤＮＰアドレスを取得し、それをネームサーバのプロキシとして動作させて着呼側のＳＤＮＰアドレスを取得させることができる。
【０１７６】
ステップ２６３に対応する図１１Ｃで、ＳＤＮＰクライアントアプリ１０１は、ＳＤＮＰシグナルサーバノード１０７にコンタクトして、着信側のＳＤＮＰアドレスまたはＳＤＮＰジップコードを有線接続１１４を介して送信する。図１１Ｄのステップ２６４では、ＳＤＮＰ信号サーバノード１０７は、有線接続１２１を介してＳＤＮＰネームサーバノード１０８にコンタクトし、ルーティングを実行しようとするすべてのメディアノードのＳＤＮＰアドレスを取得する。
【０１７７】
図１１Ｅに示すステップ２６５において、ＳＤＮＰ信号サーバノード１０７は、メディアパケットを送信するために選択したＳＤＮＰメディアノード１０６ａ～１０６ｆに、具体的には、有線接続１１５ａ～１１５ｆを使用して、それぞれＳＤＮＰメディアノード１０６ａ～１０６ｆに指示を送信するために、コマンド及び制御（Ｃ＆Ｃ）パケットをディスパッチする。また、状態情報、数値シード、暗号鍵も引き渡す。ステップ２６６では、ＳＤＮＰメディアノード１０６ａ～１０６ｆのネットワークを介して、発信側ＳＤＮＰアプリ１０１から着信側ＳＤＮＰアプリ１０２へのメディアパケットのデータ転送が開始される。
【０１７８】
ＳＤＮＰの動的ルーティングは、図１１Ｆ～１１Ｉに示されているとおり、各連続するデータパケットの変化するパスによって例示される。具体的には、図１１Ｆでは、携帯電話９５のクライアントアプリ１０１からの第１のデータパケットは、無線リンク１１２ａを介して携帯電話タワー１０３ａに運ばれ、その後、有線１１６によって第１のメディアノード１０６ａに運ばれ、ＳＤＮＰクラウド１００のメッシュネットワークへのゲートウェイとして機能する。このゲートウェイＳＤＮＰノードは、次に、データパケットの内容に対して特定のステートベースのシングルホップコンシールメント操作を実行してから、このパケットをＳＤＮＰメディアノード１０６ｃに転送し、そこでこのプロセスを繰り返し、同パケットをＳＤＮＰメディアノード１０６ｄに送り、ルータ１０４ａ、ＷｉＦｉルータ１０５、及び無線リンク１１２ｃによって運ばれ、ノートブック９６によってホストされたＳＤＮＰクライアント１０２とのラストマイル通信のためのクラウドゲートウェイとして機能する。
【０１７９】
図１１Ｇに示すように、携帯電話９５のクライアントアプリ１０１からの第２のデータパケットは、無線リンク１１２ａを介して携帯電話タワー１０３ａに運ばれ、その後、有線１１７によってＳＤＮＰクラウド１００のゲートウェイメディアノード１０６ｂに送ら

れる。ゲートウェイノード１０６ｂは、次にデータパケットの内容に対して特定のステートベースのシングルホップコンシールメント操作を実行し、このパケットをＳＤＮＰメディアノード１０６ｅに転送してこのプロセスを繰り返し、パケットをＳＤＮＰメディアノード１０６ｄに送り、ルータ１０４ａ、ＷｉＦｉルータ１０５、及び無線リンク１１２ｃによって送られ、ノートブック９６によりホストされているＳＤＮＰクライアント１０２との同じラストマイル通信へのクラウドゲートウェイとして機能する。

【０１８０】

図１１Ｇに示すように、携帯電話９５のクライアントアプリ１０１からの第３のデータパケットは、無線リンク１１２ａを介して携帯電話タワー１０３ａに送られ、その後、有線１１８によってＳＤＮＰクラウド１００のゲートウェイメディアノード１０６ｃに送られる。ゲートウェイノード１０６ｃは、次に、データパケットの内容に対して特定のステートベースのシングルホップコンシールメント操作を実行し、パケットをＳＤＮＰメディアノード１０６ｄに転送し、これがノートブック９６によってホストされるＳＤＮＰクライアント１０２とのラストマイル通信のためのクラウドゲートウェイとして機能し、パケットをルータ１０４ｂ、ＷｉＦｉルータ１０５、及び無線リンク１１２ｃを経由して送信される。この場合、ラストマイルのルーティングは動的に変更される。

【０１８１】

最後の図１１Ｉでは、携帯電話９５内のクライアントアプリ１０１からの第４のデータパケットは、無線リンク１１２ｂを介して携帯電話タワー１０３ｂに運ばれ、その後、有線１１９により、ＳＤＮＰクラウド１００のゲートウェイメディアノード１０６ａに送られる。ゲートウェイノード１０６ａは、次に、データパケットの内容に対して特定のステートベースの単一ホップコンシールメント操作を実行し、パケットをＳＤＮＰメディアノード１０６ｅに転送し、次にメディアノード１０６ｆに転送し、これがノートブック９６によってホストされるＳＤＮＰクライアント１０２とのラストマイル通信のためのクラウドゲートウェイとして機能し、パケットをルータ１０４ａそして１０４ｂ、ＷｉＦｉルータ１０５、及び無線リンク１１２ｃを経由して送信される。この場合、ファーストマイル及びラストマイルのルーティングはともに動的に変更される。

【０１８２】

再び図１０を参照すると、ステップ２６８でセッションが終了するまで、ステップ２６７でクライアントアプリ１０２と１０１の間で双方向の対話が行われている。すでに説明したように、ＳＤＮＰクラウド及びラストマイルルーティング、パケットセキュリティクレデンシャル情報、及びパケット内容は、中央の制御なしに動的かつ連続的に変更される。これもすでに説明したとおり、ＳＤＮＰネットワークは専用リソースを使用してメッシュネットワークを構成している。ここで、特定のサーバはＳＤＮＰネームサーバノード１０８、ＳＤＮＰシグナルサーバノード１０７、またはＳＤＮＰメディアノード１０６ａ～１０６ｆなどの機能のいずれかひとつのみをホストするように設定されている。

【０１８３】

ＳＤＮＰ通信はすでに説明したように、ネームサーバ、シグナルサーバ、及びメディアノードとしての役割を果たすよう別々のノードを使用しており、それぞれが別々の専用デバイス上でホストされている。そのため、ネットワークの運用には、３つのクラスのノードすべてのハードウェアホストが永続的に利用可能な状態を維持することが必要となる（つまり、常に稼働状態になっていてアクセス可能であること）。グローバルサーバクラウドは、ソフトウェアホストがオフラインになった場合や、単一のサーバのトラフィックが一定レベルを超えた場合、アクティブなサーバにインストールされているソフトウェアの新しいインスタンスを起動することで、永続的可用性を容易に維持することができる。

【０１８４】

アドホックネットワーク、ピアツーピアネットワーク、モバイルネットワークなどの不確実なリソースで構成されるネットワークでは、シグナルサーバノードやネームサーバノードの必要な管理機能が常時利用できるとは限らないことが、通信の信頼性に悪影響を与えることがある（たとえメディアノードが十分に冗長化されていて停電に耐えられるとし

ても）。このようなケースでは、すべての機能がホストされ、常時オンラインを保証するために、完全に分散化されたＳＤＮＰクラウドの実現が必要となる。

【０１８５】

しかし、ＳＤＮＰネットワーク運用の分散化では、機能性とハイパーセキュリティの両方を維持するために、いくつかの創意工夫を凝らした方法を使用する必要がある。

【０１８６】

Ｂ．分散型ＳＤＮＰハイパーセキュア通信

【０１８７】

ＳＤＮＰ通信の機能性とハイパーセキュリティの両方を維持するためには、ＳＤＮＰネットワークの分散型実装は、固定インフラストラクチャ上にホストされた専用機能ノードを使用したＳＤＮＰ通信と同じ管理原則、特に「知識ゼロ」（より正確には「不完全な知識」）の原則を遵守しなければならない。

・デバイスやユーザＩＤにアクセスできるノードは、ネットワークを介したデータパケットのルーティングを知るべきではない。

・デバイスやユーザＩＤにアクセスできるノードは、データパケット通信の内容を知るべきではない。

・いかなるノードもデータパケットのペイロード内容を知るべきではない。

・データパケットをルーティングするノードは、データパケットのペイロードの所有者の身元を知るべきはない。

・データパケットを送信するどのノードも、パケットのペイロードの所有者の身元を知るべきではない。

・データパケットを送信するノードは、着信パケットを識別し、発信パケットを次のノードの宛先に誘導するために必要なシングルホップ情報を除いて、パケットルーティング情報にアクセスしてはならない。

・データを送信するどのノードも、パケットのステートに基づく動的コンシールメントを決定するために使用される選択プロセスを知るべきではない。

・データを運ぶどのノードも、意味のある、あるいは有用な量のペイロードデータフラグメントを含まないものとする。

分散型ＳＤＮＰネットワークは、ネットワークを形成するために利用可能なリソースがどのようなものであるかを知ることなく、これらの基準に準拠したハイパーセキュアなトランスポートを実行しなければならない。このような要件とは、どのＨｙｐｅｒＮｏｄｅも、以下のような重要な役割をすべて果たすことができなければならないということを意味している：すなわち、（ｉ）ネームサーバのデバイスＩＤ管理、（ｉｉ）シグナルサーバのディスパッチャ機能、そして（ｉｉｉ）あるタスクで得たデータを別のタスクに持ち込むことなく、メディアノードのハイパーセキュアなデータ転送。

【０１８８】

分散型ＳＤＮＰネットワークトポロジー

【０１８９】

分散型ＳＤＮＰネットワーク（またはd'ＳＤＮＰクラウド）の一例を図１２Ａに示す。これは、高速有線接続２１０を介して通信する｜ＨＮ｜とラベル付けされたハイパーノード２０６を実現するためのシングルインスタンスタイプのソフトウェアをホストするサーバのＩＳＰホストクラウド２００で構成されている。理解しやすくするため、文章中のノード名には、ノードＩＤの前後に縦線を付けて｜ＸＸ｜のように表記する（図では括弧は外してある）。すべてのハイパーノード２０６は、機能と能力が同一の実行可能コードをホストするサーバで構成されている。そのため、ＨｙｐｅｒＳｐｈｅｒｅ通信セッションを開始する前に、ＨｙｐｅｒＮｏｄｅｓ　２０６ｘ、２０６ｙ、２０６ｚ、及び２０６ａは、一般的なＨｙｐｅｒＮｏｄｅ　２０６のすべてのインスタンスは、均質なＳＤＮＰノードのクラウドとして同一の動作をする。

【０１９０】

図に示すように、クラウド２００は、携帯電話タワー１０３ａ、１０３ｂからなるモバ

イルネットワークを介して携帯電話９５に接続し、それぞれセルラーネットワーク無線リンク１１２ａ、１１２ｂを使用して、別のクラウド（ラストマイル）通信を実現する。携帯電話９５は、専用機能ＳＤＮＰ実装においてＳＤＮＰソフトウェア１０１と同様の接続性を実現できるソフトウェアであるインストール済みのD'ＳＤＮＰソフトウェアクライアントＨｙｐｅｒＳｐｈｅｒｅゲートウェイノード｜ＨＧ｜２０１を介して、ＨｙｐｅｒＳｐｈｅｒｅクラウドにアクセスすることができる。同様に、クラウド２００とノートブック９６との間のラストマイル接続は、イーサネットルータ１０４ａ、有線接続１１１ａ、ＷｉＦｉルータ１０５、及び８０２．１１マイクロ波ラストリンク１１２ｃを介して促進される。

【０１９１】

分散型ＳＤＮＰ通信に特有の代替実施形態では、クラウド２００とノートブック９５との間のハイパーセキュアなラストマイル接続は、ＳＤＮＰ対応のＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜２０４ｂ、ＳＤＮＰ対応のＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜２０５への有線接続２１１ｂ、及び８０２．１１マイクロ波ラストリンク２１２ｃを介して実現することができる。タブレット９６は、インストールされたＳＤＮＰソフトウェア、多機能ＨｙｐｅｒＳｐｈｅｒｅゲートウェイノード｜ＨＧ｜２０２を介してＨｙｐｅｒＳｐｈｅｒｅクラウド２１０にアクセスする。ＨｙｐｅｒＳｐｈｅｒｅルータソフトウェアを使用すると、デバイスがラストマイル通信を行うすべてのクラウドの外側で動作している場合でも、あらゆるコンポーネントがＨｙｐｅｒＮｏｄｅのすべての機能を使用して動作できるようになる。

【０１９２】

クラウド２００内のすべてのＨｙｐｅｒＮｏｄｅｓ｜ＨＮ｜が通信を開始する前に同じであること、クライアントのＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜ソフトウェアがＨｙｐｅｒＮｏｄｅの多くの機能をエミュレートしていること、そしてまた一部のルータがＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜としてＳＤＮＰ対応である事実を踏まえると、ＨｙｐｅｒＮｏｄｅのグループが共通のＩＳＰやネットワークプロバイダによって提供されているか、固定ネットワーク、共通のインフラストラクチャ、またはネットワークバックボーン上でホストされているかという相違には意味がない。ＨｙｐｅｒＳｐｈｅｒｅの分散型ネットワークでは、すべてのノードは同等の価値を持っている。この点を考慮して、図１２Ｂには、クラウド２００の表現を除去した上で同じＨｙｐｅｒＳｐｈｅｒｅのネットワークを図解した。

【０１９３】

ＨｙｐｅｒＮｏｄｅｓをホストするすべてのデバイス（ＨｙｐｅｒＳｐｈｅｒｅルータやＨｙｐｅｒＳｐｈｅｒｅゲートウェイを含む）は、基本的には同じ方法で動作し、異種混在ホストデバイスの上にホストされたノードの同種ネットワークを形成する。このようにして、ＨｙｐｅｒＳｐｈｅｒｅは、ホストプラットフォームのデバイスに完全には依存しない均一なクラウドを運用する ― これは完全自律分散型通信ネットワークを実現するために必要な重要な基準である。つまり、分散型ネットワークでは、クラウドやラストマイル通信などというものは存在せず、ＨｙｐｅｒＮｏｄｅ、ＨｙｐｅｒＳｐｈｅｒｅルータ、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイはすべて対等なパートナーとみなされる。ＨｙｐｅｒＳｐｈｅｒｅのクラウドはどこにでもあり、遍在しているのである。

【０１９４】

さらに、ネットワークトラフィックの増加に伴ってパフォーマンスが低下し、トラフィックジャムや遅延の原因となる固定インフラストラクチャネットワークと異なり、ＨｙｐｅｒＳｐｈｅｒｉｃクラウドは動的で分散化されている。クラウドに参加するＨｙｐｅｒＮｏｄｅｓの数が増えれば増えるほど、その組み合わせが増え、ネットワークのパフォーマンスとＱｏＳ（サービス品質）の向上につながる。

【０１９５】

ＨｙｐｅｒＳｐｈｅｒｅネットワークコンポーネント

【０１９６】

図１２Ｃは、ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６、クライアントＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜２０１、及びＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜２０５を含むＨｙｐｅｒＳｐｈｅｒｅネットワークの構成要素と、ＷｉＦｉルータ｜１０５、イーサネットルータ｜１０４、及びモバイル無線ネットワーク｜１０３を含む非ＳＤＮＰ対応の構成要素を示している。ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６、クライアントＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜２０１、及びＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜２０５の３つのコンポーネントノードはすべて「メタモルフィック」であり、特定のネットワーク機能に対する現在の需要に基づいて機能を変更することができる。

【０１９７】

特に、メタモルフィックＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６は、サーバ、コンピュータ、スマートフォン、タブレット、ノートブック、自動車、またはＩｏＴデバイスからなるホストデバイス２３１にインストールされたＨｙｐｅｒＮｏｄｅソフトウェアで構成されている。メディアノード、シグナルサーバノード、ネームサーバノードが別々の実行可能なアプリケーションソフトウェアで構成されている、以前に開示された機能専用のＳＤＮＰネットワークとは異なり、ｄ'ＳＤＮＰコードでは、すべてのＨｙｐｅｒＮｏｄｅは、前述の３つの機能のいずれかを実行することができるが、１つの条件がある。それは、特定のＨｙｐｅｒＮｏｄｅは３つの機能（タスク、ネームサーバ、オーソリティノードの機能）のうちの１つしか同時には実行できないということである。数学的には、この機能は次の式で定義される。

【０１９８】

【数１】

$$|HN| = |T| \oplus |NS| \oplus |A|$$

【０１９９】

ここで、

【０２００】

【数２】

$$\oplus$$

【０２０１】

（以降、「〇」と表記する）は「排他的論理和」を表すブール論理記号で、一方または他方を意味するが、両方を意味しない関数である。

【０２０２】

未分化ＨｙｐｅｒＮｏｄｅは、通信セッションを開始するための命令を受信した時点で、以下の３つの分化ＨｙｐｅｒＳｐｈｅｒｅノードタイプのいずれかに変化（モーフィング）する必要がある。

・タスクノード｜Ｔ｜は、データパケットを搬送し（専用機能ＳＤＮＰメディアノードのメディアノードと同様の操作）、データグラムペイロードの動的コンシールメントを実行するために使用される。専用機能ＳＤＮＰトランスポートでは、エアギャップＤＭＺサーバが動的コンシールメントのための指示を提供する。開示されたｄ'ＳＤＮＰの実施形態では、これらの指示は、分散型ＤＭＺサーバまたはｄ'ＤＭＺ（本開示で後述する）からディスパッチされなければならない。

・権限ノード｜Ａ｜は、ネットワークトラフィックを指示し（専用機能ＳＤＮＰネットワークにおいてシグナルサーバノードが行うのと同じ機能）、コンセンサスベースのピアの陪審によるトランザクションの検証に従事するために使用される（後述のブロックチェーンの機能）。専用機能ＳＤＮＰトランスポートでは、リアルタイムデータルーティングに必要なノードＳＤＮＰのノードアドレス間でデータが通過するのにかかる時間を記述したネットワーク伝搬遅延テーブルが、シグナルサーバノードにすべて（または一部）格納さ

れる。
・電話番号やクライアントＩＤをダイナミックＩＰアドレス、ＳＤＮＰアドレス、ＳＤＮＰジップコードに変換するために使用されるネームサーバノード｜ＮＳ｜。専用機能のＳＤＮＰネットワークとは異なり、ＨｙｐｅｒＳｐｈｅｒｅのネームサーバデータベースは分散化・非集約化されており、１つのサーバやストレージデバイスに物理的に配置されていない、エーテルのような多次元データ構造で構成されている。
【０２０３】
セッションが開始された時点で、ＨｙｐｅｒＮｏｄｅは、説明されている３種類のノードのうちのひとつに変態するため、ＨｙｐｅｒＮｏｄｅは「メタモルフィック」と呼ばれる。この語は、「あるものの形や性質が全く異なるものに変化する」という意味の英単語メタモルフォーゼの形容詞形である。未分化なＨｙｐｅｒＮｏｄｅが単機能のＨｙｐｅｒＮｏｄｅに変態することは、未分化な幹細胞が組織特異的な細胞型に変化することに似ている。しかし、生物学的類似体とは異なり、ＨｙｐｅｒＳｐｈｅｒｅでは、変態は可逆的なプロセスである。分化したＨｙｐｅｒＮｏｄｅは、指定されたタスクを完了すると、未分化な前駆体に戻り、次の仕事を待機する。この意味で、ネットワークリソースとして機能するＨｙｐｅｒＮｏｄｅの数も、あるＨｙｐｅｒＮｏｄｅのネットワーク参加の可能性も無尽蔵と言える。
【０２０４】
要約すると、すべてのＨｙｐｅｒＮｏｄｅｓ｜ＨＮ｜は、最初は未分化でメタモルフォーゼの状態であるにもかかわらず、ジョブ中にノードはＨｙｐｅｒＳｐｈｅｒｉｃネームサーバ｜ＮＳ｜、ディスパッチ及びシグナルサーバ機能を実行するオーソリティノード｜Ａ｜、メディアノード機能を実行するタスクノード｜Ｔ｜のいずれかに変態し、ジョブを完了した後に未分化な｜ＨＮ｜の形に戻る。メタモルフォーゼの間、未分化ノードは一時的に、拡散した、すなわち非集約型のまたは冗長なデータベース層（後述）から必要な情報をダウンロードし、定義されたジョブを実行した後、未分化｜ＨＮ｜状態に戻り、ダウンロードした情報やそれが行ったすべてのことを忘却してしまう。ステートレス動作と称する動作記憶喪失とは、ＨｙｐｅｒＮｏｄｅがノウハウを一時的に限って保持しているだけであって、ノードの命名、パケットルーティング、ペイロードの内容などの情報を同時に保持し続けることはないことを意味している。ステートレスオペレーションとは、ノードが｜ＮＳ｜、｜Ａ｜、｜Ｔ｜のいずれかの機能を実行できても、同時に複数の機能を実行することはできないことを意味している。
【０２０５】
また、ＨｙｐｅｒＮｏｄｅはそのホストプロセッサとメモリのリソースを使用するが、それが処理するデータや、実行するタスクに関する情報をホストと共有することはない。これはサンドボックス化と呼ばれる手法で、ホストＯＳが実行するアプリケーションからホストＯＳを保護する方法である。ただし、ＨｙｐｅｒＮｏｄｅのソフトウェアは対称的にサンドボックス化されていて、ＨｙｐｅｒＮｏｄｅがデバイスホストと相互に対話したり、そのデバイスホストから情報を取得したりすることはできない。逆に、ＨｙｐｅｒＮｏｄｅをホストしているデバイスは、ＨｙｐｅｒＮｏｄｅが伝送するネットワークトラフィックと相互作用することはできない（あるいは、理解することすらできない）。ＨｙｐｅｒＮｏｄｅはステートレスに動作し、ホストデバイスのメモリにその動作に関する記録を残さない。つまり、ＨｙｐｅｒＮｏｄｅに割り当てる計算能力（計算サイクル）をデバイスが決定するだけでなく、ノードとデバイスがお互いに干渉することもなく、どのデバイスでもＨｙｐｅｒＮｏｄｅをホストすることができるのである。
【０２０６】
この対称的サンドボックス化により、ＨｙｐｅｒＮｏｄｅは、アプリケーションをサポートしたり、クライアント固有の機能を実行したりするためのユーザインターフェイスとして動作することができない。デバイスのアプリケーション境界を越えてデータを搬送するためには、特別なソフトウェアインターフェイスが必要である。具体的には、アプリケーションまたはクライアントがＨｙｐｅｒＳｐｈｅｒｉｃクラウドにアクセスできるよう

、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイＨＧ　２０１の動作を容易化するために特別なアプリケーションソフトウェア２３２がデバイス、例えば携帯電話９５（または他の任意のエッジデバイス）にインストールされる。ウィキペディアによれば、エッジデバイスとは、「企業またはサービスプロバイダのコアネットワークへのエントリーポイントを提供するデバイス」である。たとえば、ルータ、ルーティングスイッチ、統合アクセスデバイス（ＩＡＤ）、マルチプレクサ、及びさまざまなメトロポリタンエリアネットワーク（ＭＡＮ）やワイドエリアネットワーク（ＷＡＮ）のアクセスデバイスなどがある。ＨｙｐｅｒＳｐｈｅｒｅの用語では、エッジデバイスとは、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイソフトウェアをホストするあらゆるデバイスを指している。例えば、パソコン、ゲーム、タブレット、スマートフォン、ＩｏＴデバイス、自動車、その他のユーザが制御するネットワーク接続コンポーネントなどが挙げられる。

【０２０７】

ＵＮＩＸ（登録商標）、Ｌｉｎｕｘ（登録商標）、ＭａｃＯＳ（登録商標）、Ｗｉｎｄｏｗｓ（登録商標）、ｉＯＳ（登録商標）、Ａｎｄｒｏｉｄ（登録商標）などの主要なオペレーティングシステム上で動作するように設計された汎用ソフトウェアであるＨｙｐｅｒＮｏｄｅとは異なり、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイの機能は、銀行のログインポータル、ＰＯＳ端末、工場の制御システム、自動車のインフォテインメントシステム、ホームセキュリティシステム、ホームＩｏＴクラウドなど、それが可能にするアプリケーションと必然的に対話することになる。この統合されたリンクを促進するために、ＨｙｐｅｒＳｐｈｅｒｅ固有のアプリケーションプログラミングインターフェイス（ＡＰＩ）とソース開発キット（ＳＤＫ）に加えて、あらかじめ用意された特別なインターフェイスとソフトウェアユーティリティ（ライブラリ）が重要なエンジニアリングツールとなっている。具体的には、ＨｙｐｅｒＳｐｈｅｒｅのアプリケーションプログラミングインターフェイス（ＨＡＰＩ）の要素として、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイＨＧ２０１は、ユーザアプリケーションがＨｙｐｅｒＳｐｈｅｒｅ分散型ネットワークや他のＨｙｐｅｒＮｏｄｅｓとコンタクトして通信するための定義済みリンク、言語、及びプロトコルが提供されている。ユーザアプリケーションは、ＨｙｐｅｒＳｐｈｅｒｅ　Ｓｏｆｔｗａｒｅ　Ｄｅｖｅｌｏｐｍｅｎｔ　Ｋｉｔ（ＨＳＤＫ）を使用して開発する。

【０２０８】

ほとんどの場合、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイＨＧ　２０１　は、ＨｙｐｅｒＳｐｈｅｒｅへの専用のインターフェイス及び　ＡＰＩ　として動作しますが、状況によっては、ゲートウェイがメタモルフィックなものになることもある。ＨｙｐｅｒＳｐｈｅｒｅゲートウェイのメタモルフィックな応用例のひとつに、アドホックなピアツーピアネットワークの形成がある（後述）。言い換えると、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイは、ＨｙｐｅｒＮｏｄｅとして動作し、限定的な方法でＨｙｐｅｒＳｐｈｅｒｉｃクラウドとデバイスとの間で特定の種類のデータを交換することができる。ただし、ＨｙｐｅｒＮｏｄｅゲートウェイは自律的なコードとして動作するのではなく、マーチャントやサービスプロバイダのアプリケーションソフトウェアに統合されている。

【０２０９】

ＨｙｐｅｒＮｏｄｅソフトウェアのもうひとつのバージョンとして、ＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜がある。ＳＤＮＰ通信は通常、ネットワークレイヤ３からアプリケーションレイヤ７までの間で動作するが、ＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜のソフトウェアには、ＰＨＹレイヤ１とＭＡＣレイヤ２のセキュリティをオプションで管理するための規定が含まれている。ＨｙｐｅｒＳｐｈｅｒｅルータ２０５は、イーサネットルータ１０４などの従来のルータハードウェアとＨｙｐｅｒＳｐｈｅｒｅダイナミックルータソフトウェア２３３を組み合わせて構成され、ＳＤＮＰ対応の有線ルータ２３４（本明細書では「イーサネット」ルータと定義されている）を実現する。また上記の代わりに、ＨｙｐｅｒＳｐｈｅｒｅ動的ルータソフトウェア２３３と組み合わせたＷｉＦｉルータ１０５を使用して、本明細書で「ＨｙＦｉ」ルータと定義しているＳＤＮＰ対応ＷｉＦｉ無線ルータ２３５を実現する方法もとることができる。

【０２１０】
ＨｙｐｅｒＳｐｈｅｒｅルータソフトウェアは、ネットワークレイヤ３通信を確立または許可する前にセキュリティとユーザ検証を管理しているため、固定インフラストラクチャネットワークや高速クラウドの外部でのラストマイル通信において特別な利点がある。このような機能は、｜ＨＲ｜ノードは認識できないノードを完全に無視するため、サービス拒否（ＤｏＳ）攻撃の阻止に役立つ。ＨｙｐｅｒＳｐｈｅｒｅルータには以下のように多くの利点がある。
・ＨｙｐｅｒＳｐｈｅｒｅルータは、ＨｙｐｅｒＳｐｈｅｒｅ権限ノードから受け取ったＳＤＮＰルーティング命令（シグナルサーバ機能を実行）に従って、ＨｙｐｅｒＳｐｈｅｒｅデータグラムを送信している。ルータの静的ルーティングテーブルはパケットのルーティングを決定しない。
・権限ノードがリモートでルーティングを制御しているため、ラストマイル通信であっても、ＨｙｐｅｒＳｐｈｅｒｅデータグラムを迂回したり、乗っ取ることはできません。
・ＨｙｐｅｒＳｐｈｅｒｅルータは、ホップ遅延をネットワークに報告して、ＨｙｐｅｒＳｐｈｅｒｅの権限ノード（シグナルサーバ機能）がラストマイル通信の最低伝搬遅延パスを決定できるようにしている。
・ＨｙｐｅｒＳｐｈｅｒｅルータは、ＳＤＮＰ動的コンシールメント処理をサポートし、動的なセキュリティクレデンシャル情報を解釈する。
・ＨｙｐｅｒＳｐｈｅｒｅルータは、ＨｙｐｅｒＳｐｈｅｒｅルータとクライアントデバイスのＨｙｐｅｒＳｐｈｅｒｅゲートウェイとの間の最後のリンク通信において、動的セキュリティパラメータのリフレッシュレートをより高くサポートし、動的セキュリティの質を向上させている。
・ＨｙｐｅｒＳｐｈｅｒｅルータは、ＨｙｐｅｒＳｐｈｅｒｅルータとクライアントデバイスのＨｙｐｅｒＳｐｈｅｒｅゲートウェイ間のラストリンク通信において共有秘密をサポートし、動的コンシールメントの質を向上させている。
【０２１１】
例えば、図１２Ａに示す、Ｅｔｈｙｒｎｅｔ ＨｙｐｅｒＳｐｈｅｒｅルータ２０４ｂ及びＨｙＦｉ ＨｙｐｅｒＳｐｈｅｒｅルータ２０５を介したハイパーセキュア通信では、従来のルータを介したデータ転送よりも高いパフォーマンスのラストマイル接続が可能になっている。しかし、多くの場合、発信元（エッジデバイス）とＳＤＮＰクラウドとの間のラストマイル通信は、不可避的にＷｉＦｉルータ１０５やイーサネットルータ１０４などのＳＤＮＰ対応デバイス以外のデバイスを介して、または無線ネットワーク１０３を介して、メディアパケットを搬送することもある。
【０２１２】
ＳＤＮＰパケットは７－ＯＳＩフォーマットに従うため、非ＳＤＮＰルータはＩＰアドレスをインターネット、サブネット、またはＮＡＴアドレスの通常のＴＣＰ／ＩＰアドレスとして解釈してパケットを通常のＴＣＰ／ＩＰパケットであるかのようにルーティングし、パケットがＨｙｐｅｒＳｐｈｅｒｉｃであることに気づかない。もう一度図９に戻ると、ＷｉＦｉルータ１０５を介したトラフィックは、上記の理由で、ディスパッチャベースのルーティングではなくルーティングテーブル１３７を採用している。同様に、イーサネットルータ１０４は、各パケットがＳＤＮＰノード対応デバイスに到達するまで、ローカルＩＳＰプロバイダのルーティングテーブル１３８を使用する。有線通信では、ＳＤＮＰパケットは各パケットがＨｙｐｅｒＮｏｄｅに到達する前に、ひとつまたは２つ以上の中間ルータを通過することはないと考えられる。無線ネットワーク１０３上の（またはケーブルまたは衛星ネットワーク上でも）ＳＤＮＰパケットの伝送の場合、通信事業者の独自のネットワークルーティングテーブル１３９及びカスタムパケットフォーマット（例えば、３Ｇ、４Ｇ、５Ｇ、衛星、またはＤＯＣＳＩＳ３プロトコル）を使用してルーティングが行われる。ネットワークアドレストランスレータ（ＮＡＴ）１３２は、独自のパケットフォーマットを有線接続用のイーサネット互換ＴＣＰ／ＩＰパケットフォーマットに戻すために必要である。

【０２１３】
このようにして、ＳＤＮＰメディアパケットをインターネットルータとＳＤＮＰノードのネットワークを介して伝送することができ、カスタムハードウェアや専用の私有クラウドは不要となるため、ＳＤＮＰクラウドを任意のＴＣＰ／ＩＰネットワークに導入することが可能になる。断片化された隠蔽パケットを非ＳＤＮＰ対応デバイス上で送信しても、通信セキュリティがリスクに晒されることはないが、ネットワークで遅延パスが長くなりパケットのルーティングで伝搬遅延が増大し、通話のサービス品質（ＱｏＳ）を低下させる可能性がある。
【０２１４】
分散型ＳＤＮＰネットワークの運用
【０２１５】
分散型ＳＤＮＰネットワークにおけるデータパケットのルーティングは、専用のＳＤＮＰノード上の固定インフラストラクチャで構成される以前のルーティングと同様、動的なセキュリティ規定を使用したメッシュネットワーク経由の匿名の断片化データ転送方法を採用しているのだが、分散型メッシュネットワークでは、データを搬送するために利用できるノードは、ネットワークオペレータの監視なしで完全に自律的に常に変化する。図１２Ｄ及び１２Ｅは、「ｄ'ＳＤＮＰネットワーク」とも呼ばれる分散型ＳＤＮＰネットワークの例を挙げてその動作を図解している。分散化メッシュネットワーク上での対応するパケットルーティングを図１３Ａ～図１３Ｈに示す。
【０２１６】
図１２Ｄのステップ２７０にて、携帯電話９５でホストされているＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜２０１ａがｄ'ＳＤＮＰネットワークとのセッションを開く。ステップ２７１ａでは、ＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１が、ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｘにコンタクトして、通話受信者のＳＤＮＰアドレスを取得する。ステップ２７１ｂでは、ＨｙｐｅｒＮｏｄｅ ｜ＨＮ｜２０６ｘは、ＨｙｐｅｒＳｐｈｅｒｅネームサーバノード｜ＮＳ｜２３６ａに変態する。図１３Ａに示すように、ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｘは、次にセルタワー１０３ａへの無線リンク１１２ａを介し、またＨｙｐｅｒＳｐｈｅｒｅネームサーバノード｜ＮＳ｜２３６ａへの有線接続２５０を介してＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１ａとの接続を確立する。ステップ２７２ａにおいて、ＨｙｐｅｒＳｐｈｅｒｅネームサーバノード｜ＮＳ｜２３６ａは、受信者のＳＤＮＰアドレスをＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１に渡す。ステップ２７２ｂで、ＨｙｐｅｒＳｐｈｅｒｅネームサーバノード｜ＮＳ｜２３６ａは、未分化なＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｘに戻る。
【０２１７】
ステップ２７３ａでは、ＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１は、受信者ＳＤＮＰアドレスを未分化ＨｙｐｅｒＮｏｄｅ ２０６ｚに渡し、ステップ２７３ｂで、権限ノード｜Ａ｜ ２３７に変態する。図１３Ｂに示すプロセスでは、データは無線リンク１１２ａを介してセルタワー１０３ａに転送され、有線接続２５１を介して権限ノード｜Ａ｜２３７に転送される。
【０２１８】
ステップ２７４ａで、権限ノード｜Ａ｜２３７は、未分化なＨｙｐｅｒＮｏｄｅ ２０６ｙにコンタクトして、タスクノードアドレスのＳＤＮＰアドレスを取得し、ステップ２７４ｂでＨｙｐｅｒＮｏｄｅ ２０６ｙはＨｙｐｅｒＳｐｈｅｒｅネームサーバノード｜ＮＳ｜２３６ｂに変態する。図１３Ｃのステップ２７５で、ＨｙｐｅｒＳｐｈｅｒｅネームサーバノード｜ＮＳ｜ ２３６ｂは、要求されたアドレステーブルを、有線接続２５２を介してＨｙｐｅｒＳｐｈｅｒｅ権限ノード｜Ａ｜２３７に配信する。
【０２１９】
図１２Ｅのステップ２７６ａに対応する図１３Ｄで、ＨｙｐｅｒＳｐｈｅｒｅ権限ノード｜Ａ｜２３７は、未分化のＨｙｐｅｒＮｏｄｅ２０６を有線接続２５３ａ～２５３ｈ上

で選択するためのルーティング命令を送信し、それにより、ステップ２７６ｂでは、それらをそれぞれＨｙｐｅｒＳｐｈｅｒｅタスクノード｜Ｔ｜２３８ａ～２３８ｈに変換する。ただし、微分化前のＨｙｐｅｒＳｐｈｅｒｅタスクノード２３８ｄ及び２３８ｅは、ＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜２０４ｂ及び２０５を構成しており、ＩＳＰクラウド２００によってホストされているノードではない。

【０２２０】

図１２Ｅでは、ステップ２７７ａに対応して、第１のＳＤＮＰデータパケットが、ＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１から無線リンク１１２ａを介してセルタワー１０３ａに転送され、その後、有線２５４を介してタスクノード｜Ｔ｜２３８ａ、２３８ｃ、２３８ｆに転送されてから、イーサネットルータ１０４ａ、ＷｉＦｉルータ１０５、及びＷｉＦｉマイクロ波リンク１１２ｃを介してＨｙｐｅｒＳｐｈｅｒｅゲートウェイ２０２に転送される。図１３Ｆでは、第２のＳＤＮＰデータパケットは、ＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１から無線リンク１１２ａを介してセルタワー１０３ａに転送され、その後、有線２５５を介してタスクノード｜Ｔ｜２３８ｂ、２３８ｇ、２３８ｆに転送された後、イーサネットルータ１０４ａ、ＷｉＦｉルータ１０５、ＷｉＦｉマイクロ波リンク１１２ｃによってＨｙｐｅｒＳｐｈｅｒｅゲートウェイ２０２に転送される。

【０２２１】

図１３Ｇでは、３番目のＳＤＮＰデータパケットが、ＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１から無線リンク１１２ａを介してセルタワー１０３ａに転送され、その後、有線２５６を介してタスクノード｜Ｔ｜２３８ｃ、２３８ｆ、２３８ｆに転送された後、ＨｙｐｅｒＳｐｈｅｒｅ　イーサネットルータのタスクノード２３８ｄ、ＨｙｐｅｒＳｐｈｅｒｅ　ＨｙＦｉルータ２３８ｅに転送され、最後にハイパーセキュアなマイクロ波リンク２１２ｄを介してＨｙｐｅｒＳｐｈｅｒｅゲートウェイ２０２に転送される。図１３Ｈでは、第４のＳＤＮＰデータパケットが、ＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１から無線リンク１１２ｂを介してセルタワー１０３ｂに転送された後、有線２５７を介してタスクノード｜Ｔ｜２３８ａ、２３８ｇ、２３８ｈに転送され、続いてイーサネットルータ１０４ａ、ＨｙｐｅｒＳｐｈｅｒｅイーサネットルータタスクノード２３８ｄ、ＨｙｐｅｒＳｐｈｅｒｅ　ＨｙＦｉルータ２３８ｅ、及びハイパーセキュアなマイクロ波リンク２１２ｄによってＨｙｐｅｒＳｐｈｅｒｅゲートウェイ２０２に転送される。

【０２２２】

もう一度図１２Ｅに戻ると、断片化されたデータの転送のシーケンスは、ゲートＨｙｐｅｒＳｐｈｅｒｅ　ＨＧ　２０１から集合タスクノード２３８を介して２０２までの通信を説明している。ステップ２７７ｂで断片化データパケットが送信された後、タスクノード２３８は未分化ＨｙｐｅｒＮｏｄｅｓ｜ＨＮ｜に戻る。その後、プロセス２７８では、ステップ２７９でセッションが終了するまで、ゲートウェイ装置２０１と２０２との間の双方向の対話が繰り返される。

【０２２３】

メタモルフィックＨｙｐｅｒＮｏｄｅの運用

【０２２４】

ＨｙｐｅｒＳｐｈｅｒｅでは、メタモルフィックなＨｙｐｅｒＮｏｄｅの運用を実装するために２つの手段がある。第一の手段では、｜ＮＳ｜、｜Ａ｜、及び｜Ｔ｜の機能からなる３つの別々の実行コードファイルが、同じサーバまたはホスト装置に読み込まれる。各機能ノードはホストデバイスのＭＡＣアドレスをアップロードする。ＨｙｐｅｒＮｏｄｅがタスクの実行を依頼されると、まずは同じＭＡＣアドレスを持つ他の単機能ノードをチェックして、同じクライアントのためにジョブを実行しているかどうかを確認する。もし実行中であれば、ＨｙｐｅｒＮｏｄｅは新しいジョブの受け入れを拒否する。例えば、ＭＡＣアドレス｛００：Ａ０：Ｃ９：１４：Ｃ８：２９｝でホストされているタスクＨｙｐｅｒＮｏｄｅ｜Ｔ｜がクライアントゲートウェイノード２０１のためにデータパケット

を送信している場合、同じＭＡＣアドレスを持つ｜Ａ｜ノードが同じクライアントデバイス、すなわちクライアントゲートウェイノード２０１のためにルーティングを実行するための要求は拒否される。

【０２２５】

もうひとつのより効率的な方法では、メタモルフィックＨｙｐｅｒＮｏｄｅの排他機能を、セレクタ機能を含む単一の実行コードに統合することができる。この独創的な方法は図１４にて図解した。サーバ２３０にインストールされたＨｙｐｅｒＮｏｄｅソフトウェア２３１によって実現されたＨｙｐｅｒＮｏｄｅ ｜ＨＮ｜２０６には、｜Ｔ｜、｜Ａ｜、｜ＮＳ｜のいずれかのノードとして動作する実行コードが含まれており、セレクタ２９０を使用してＨｙｐｅｒＮｏｄｅの動作を任意の時間に３つの機能のうちのひとつのみに制限している。

【０２２６】

一実施形態では、ＨｙｐｅｒＮｏｄｅ２０６は、ジョブ明細２９１、数値シード２８１、及び暗号鍵２８２を含む、ＨｙｐｅｒＣｏｎｔｒａｃｔ２８０と呼ばれるデジタルファイルの形でジョブオーダーを受信する。ジョブ明細は、ＨｙｐｅｒＮｏｄｅ ２０６がタスクノードであるべきか、権限ノードであるべきか、またはネームサーバノードであるべきかを決定するために、セレクタ２９０に必要な情報となる。前掲のルーティング例では、メタモルフィックＨｙｐｅｒＮｏｄｅ ２０６ｘがＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１の要求時にネームサーバ機能を実行するよう命令を受けると、未分化Ｈｙｐｅｒｎｏｄｅ ２０６ｘが拡散データクラウド２８３ａからデータをダウンロードし、｜ＮＳ｜ノード２３６ａに変態する。

【０２２７】

同様に、メタモルフィックＨｙｐｅｒＮｏｄｅ ２０６ｚがＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１の要求時に権限ノード機能を実行するよう命令を受けると、未分化｜ＨＧ｜２０６ｚが拡散データクラウド２８３ｂからデータをダウンロードし、｜Ａ｜ノード２３７に変態する。拡散データクラウド２８３ａからダウンロードして｜Ａ｜ノード２３７を生成するために使用したデータは、｜ＮＳ｜ノード２３６ａを生成するために使用したダウンロードデータとは異なる。したがって、ネームサーバノードと権限ノードは分化しており、必要に応じて拡散データクラウドから異なる情報にアクセスしている。

【０２２８】

その後、メタモルフィックＨｙｐｅｒＮｏｄｅ ２０６ｙが権限ノード｜Ａ｜２３７の要求によりネームサーバ機能を実行する命令を受けると、｜ＨＮ｜２０６ｙは拡散データクラウド２８３ａからデータをダウンロードして｜ＮＳ｜ノード２３６ｂに変態する。拡散データクラウド２８３ａからダウンロードして｜ＮＳ｜ノード２３６ｂを生成するためにダウンロードしたデータは、｜ＨＮ｜２０６ｘを生成するために使用したデータと同じではない。このようにして、２つのネームサーバインスタンスは区別され、必要に応じて必要な情報のみにアクセスする。

【０２２９】

最後に、メタモルフィックＨｙｐｅｒＮｏｄｅ ２０６ａは、権限ノード｜Ａ｜２０７の要求に応じてタスクノードルーティング指示を実行するように指示を受けると、未分化｜ＨＮ｜２０６ａは、拡散データクラウド２８３ｃからデータをダウンロードして｜Ｔ｜ノード２３８に変態する。拡散データクラウド２８３ｃからダウンロードして｜Ｔ｜ノード２３８を生成するためにダウンロードしたデータは、｜Ａ｜ノード２３７または｜ＮＳ｜ノード２３６ａまたは２３６ｂを生成するために使用したダウンロードデータとは異なる。このように、タスクノード、権限ノード、及びネームサーバノードは、すべて分化され、相互に排他的であり、純粋に「知る必要があるときにのみ」拡散データクラウドから異なる情報にアクセスする。

【０２３０】

ＨｙｐｅｒＳｐｈｅｒｅの重要な革新性は、「拡散型」の非集約型データクラウドを利

用して、専用のストレージデバイスを使用せずにグローバルに情報を共有できる点にある。非集約型データストレージとは、データを小さな単位（ジグソーパズルのピースのようなもの）に断片化し、ＨｙｐｅｒＳｐｈｅｒｅの分散型クラウドに分散したローカルストレージデバイスに格納したものを指す。書き込み、読み込み、検索、リフレッシュなど、ＨｙｐｅｒＳｐｈｅｒｅの非集約型データストレージの動作については、本明細書で後述する。つまり、ＨｙｐｅｒＳｐｈｅｒｅの非集約型・拡散型データクラウドに格納されているデータは、権限のあるＨｙｐｅｒＮｏｄｅのみが必要に応じてアクセスできるデータであるということである。

【０２３１】

図１５Ａは、メタモルフィックＨｙｐｅｒＮｏｄｅの動作時における拡散型クラウドストレージの役割を例示している。最左端の列では、ＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１が、メタモルフィックＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｘからネームサーバ情報を要求している。アクセスを許可するＨｙｐｅｒＣｏｎｔｒａｃｔ２８０からの数値シード２８１は、｜ＨＮ｜２０６ｘに渡される。一実施形態では、数値シードが、格納データの作成ステート、すなわちデータが格納された時のステート変数を定義している。このアクセス要求には、要求がタイムリーであることを確認するために使用されるステート２８４を含めることもでき、例えば、認証期間が満了していないことを確認するために使用する。ステートは、時間、場所、セキュリティゾーン、または他の動的に変化するパラメータで構成することができる。

【０２３２】

中央の列に示されている次のステップでは、未分化の｜ＨＮ｜２０６ｘが、暗号化鍵２８２を使用して、または（後述の）デジタルＣＡ証明書を使用して、要求を認証するためにネームサーバノードの拡散データクラウド２８３ａとの間で安全なチャネルを確立している。図１５Ａの右端の列では、要求されたデータが検出され、コンパクトなファイルに集約され、拡散データクラウド２８３ａから｜ＨＮ｜２０６ｘに渡され、直ちに分化したネームサーバＨｙｐｅｒＮｏｄｅ｜ＮＳ｜２３６ａに変態する。ネームサーバＨｙｐｅｒＮｏｄｅ｜ＮＳ｜２３６ａは、その後、要求されたＮＳデータ２８５（この場合は発信者ＩＤ情報）を、要求元のＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１に渡す。

【０２３３】

図１５Ｂに示すように、拡散データリコールには、エッジデバイスの連絡先情報、例えば、発信者が通話を希望する電話番号２８５ａ（着呼者）が含まれ、これは、ネームサーバ拡散データクラウド層２８３ａからデータを抽出するために使用され、デバイスのＳＤＮＰアドレス、ＳＤＮＰのジップコード、その時点での着呼者の動的ＩＰアドレスを含むネームサーバ｜ＮＳ｜ファイル２８５ｂに含まれる着呼者ＩＤ情報を抽出するために使用される。このファイルには、ルーティングの優先度、コスト、冗長性などを決定するために使用される「ＶＩＰデータ」という名称のついたカスタムないしアプリケーション固有の情報が含まれていてもかまわない。

【０２３４】

図１６Ａの左端の列では、ＨｙｐｅｒＳｐｈｅｒｅクライアントゲートウェイ｜ＨＧ｜２０１の要求により、メタモルフィックなＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｚに、｜ＮＳ｜データ２８５ｂで指定された呼び出しＩＤへの呼び出しを行う意図を通知している。アクセスを許可するＨｙｐｅｒＣｏｎｔｒａｃｔ　２８０からの数値シード２８１が｜ＨＮ｜２０６ｚに渡される。一実施形態では、数値シードが格納データの作成ステート、すなわちデータが格納された時のステート変数を定義している。このアクセス要求には、要求がタイムリーであることを確認するために使用されるステート２８４を含めることもでき、例えば、認証期間が満了していないことを確認するために使用する。ステートは、時間、場所、セキュリティゾーン、またはその他の動的に変化するパラメータで構成することができる。

【０２３５】

中央の列に示されている次のステップでは、未分化の｜ＨＮ｜２０６ｚが、暗号化鍵２８２を使用して、または（後述の）デジタルＣＡ証明書を使用して、要求を認証するために権限ノードの拡散データクラウド２８３ｂとの間で安全なチャネルを確立している。図１６Ａの右端の列では、要求されたデータが特定され、ネットワークホップ時間を含むコンパクトな｜Ａ｜データファイル２８６ａに集約され、拡散データクラウド２８３ｂから｜ＨＮ｜２０６ｚに渡され、直ちに権限ノード｜Ａ｜２３７で構成される分化ＨｙｐｅｒＮｏｄｅに変態する。

【０２３６】

図１６Ｂに示すように、拡散データリコールでは、発信者ＩＤ情報｜ＮＳ｜データ２８５ｂを使用して、権限ノード拡散データクラウド層２８３ｂからデータにアクセスし、ネームサーバ｜Ａ｜ファイル２８６ａに含まれるネットワークホップ時間情報が抽出される。このファイルには、２つのＳＤＮＰアドレス間の潜在的に関連性のあるノード間伝播遅延のリストと、特定のホップ、具体的には発信者と受信者の間の一般的なパス内のホップに関して最後に記録された伝送時間が格納されている。このテーブルには、任意の２つのＳＤＮＰアドレス間の伝搬遅延のランク付けされていないリストが含まれており、ミリ秒（ｍｓ）単位の伝搬遅延は１６進数形式で表されている。例えば、遅延時間"２Ｂ　ｈｅｘ"は４３ミリ秒に相当する。なお、ＳＤＮＰアドレスは、図のようにＩＰｖ６で表現することも、ＩＰｖ４形式で表現することもできる。

【０２３７】

図１６Ｃでは、ルーティングオプション３０９をランク付けして選択するためのアルゴリズムが、編集２８６ａを簡略化されたテーブル２８６ｂに修正するために使用されている。選択及び順位付けプロセスは、"Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｃｏｍｍｕｎｉｃａｔｉｏｎ　Ｎｅｔｗｏｒｋ　ａｎｄ　Ｐｒｏｔｏｃｏｌ"（完全な動的通信ネットワークとプロトコル）と題される米国特許第９，９９８，４３４号に記載されているアルゴリズムを使用している。このアルゴリズムについては、本明細書では再度言及しない。ルーティング選択プロセスからの出力により、パケットルーティングに潜在的に役立つタスクノードのＳＤＮＰアドレスのリスト２８６ｃが得られる。

【０２３８】

図１７Ａの左端の列では、テーブル２８６ｃが｜Ａ｜ノード２３７からメタモルフィックＨｙｐｅｒＮｏｄｅ　２０６ｙに転送され、このノードは、数値シード２８１及びステート２８４が（このセッションで２回目の）ネームサーバノード拡散データクラウド２８３ａに接触することに関連して、中央の列に示されているように、暗号鍵２８２を使用してＨｙｐｅｒＮｏｄｅ　２０６ｙとの間で安全なリンクを確立している。これに応答して、右端の列に示されているように、ネームサーバノード拡散データクラウド２８３ａは、データをＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｙにダウンロードし、これは瞬時にネームサーバノード｜ＮＳ｜２３６ｂに変態し、タスクノードＩＤテーブルが記述された｜ＮＳ｜データファイル２８７ａを権限ノード｜Ａ｜２３７に渡す。

【０２３９】

図１７Ｂに示すように、拡散データリコールでは、ランクソートされたタスクノードデータ２８６ｃが使用され、ネームサーバ拡散データクラウドレイヤ２８３ａからデータにアクセスし、ネームサーバ｜ＮＳ｜ファイル２８７ａに含まれるタスクノードＩＤ情報が抽出される。このファイルには、要求された各ＳＤＮＰアドレスとそれに対応するＳＤＮＰのジップコードとその時点での動的ＩＰアドレスの変換テーブルを含むリストが含まれている。

【０２４０】

図１８Ａの左端の列では、テーブル２８７ａは次に｜Ａ｜ノード２３７からメタモルフィックなＨｙｐｅｒＮｏｄｅ　２０６ｗに転送され、このノードは、数値シード２８１及びステート２８４と関連して、タスクノード拡散データクラウド２８３ｃにコンタクトし、中央の列に示されているように、暗号鍵２８２を使用してＨｙｐｅｒＮｏｄｅ　２０６ｗとの間で安全なリンクを確立する。これに応答して、右端の列に図にあるように、ネー

ムサーバノード拡散データクラウド２８３ｃは、｜Ｔ｜データファイル２８７ｂ内の共有秘密をＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｗにダウンロードすると同時に、データを搬送する準備ができたタスクノード２３８ａに即座に変態する。

【０２４１】

図１８Ｂに示すとおり、拡散データリコールでは、タスクノードＩＰデータ２８７ａを使用してタスクノード拡散データクラウド層２８３ｃからデータにアクセスし、タスクノード｜Ｔ｜ファイル２８７ｂに含まれる共有秘密が抽出される。このファイルには、図１８Ｃのタスクノード３２０として図解されているように、着信データパケット３２１ａを処理するために必要なアルゴリズム２９９ａと、発信データパケット３２１ｂを処理するために使用されるアルゴリズム２９９ｂとを含む、分散型ＤＭＺアルゴリズム、すなわちｄ'ＤＭＺ動的コンシールメントアルゴリズムのリストが含まれている。「メディアノード」操作を実行するタスクノードの機能的操作については、前記米国特許第９，９９８，４３４号にその説明が記述されている。

【０２４２】

拡散データクラウド

【０２４３】

図１９に示すとおり、非集約型データとして格納されている拡散データクラウド２８３は、３つのタイプのデータまたはサブクラウド、すなわちネームサーバクラウド２８３ａ、権限ノードクラウド２８３ｂ、及びタスクノードクラウド２８３ｃに細分化されている。特定のノードタイプに分化すると、メタモルフィックＨｙｐｅｒＮｏｄｅ２０６は、必要に応じて、その対応する拡散データクラウド層とのみ相互作用するように制限される。例えば、ネームサーバノードに分化すると、｜ＮＳ｜ＨｙｐｅｒＮｏｄｅ　２３６は、ネームサーバクラウド２８３ａに関連する拡散データクラウド２８３からのみデータにアクセスすることができ、権限ノードクラウド２８３ｂまたはタスクノードクラウド２８３ｃからはアクセスすることができない。クライアントＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜ゲートウェイ要求は別にして、ネームサーバ｜ＮＳ｜ノードは、権限ノード２３７としか通信できないが、タスクノード２３８とは通信できない。

【０２４４】

権限ノードに分化すると、｜Ａ｜ＨｙｐｅｒＮｏｄｅ　２３７は、権限ノードクラウド２８３ｂに関連する拡散クラウド２８３からのみデータにアクセスすることができ、ネームサーバクラウド２８３ａやタスクノードクラウド２８３ｃからはアクセスすることができない。クライアントＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜ゲートウェイ要求は別にして、権限｜Ａ｜ノード２３７は、ネームサーバＨｙｐｅｒＮｏｄｅ　２３６から情報を要求し、コマンド及び制御（Ｃ＆Ｃ）パッケージの命令をタスクＨｙｐｅｒＮｏｄｅ２３８に伝達することができる。

【０２４５】

タスクノードに分化すると、｜Ｔ｜ＨｙｐｅｒＮｏｄｅ　２３８は、タスクノードクラウド２８３ｃに関連する拡散クラウド２８３からのみデータにアクセスすることができ、ネームサーバクラウド２８３ａや権限ノードクラウド２８３ｂからはアクセスできない。クライアントＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜ゲートウェイ要求は別にして、タスク｜Ｔ｜ノード２３８は、権限ノードＨｙｐｅｒＮｏｄｅ　２３７からコマンド及び制御（Ｃ＆Ｃ）命令を受け取ることができるが、ネームサーバ｜ＮＳ｜ＨｙｐｅｒＮｏｄｅ　２３６と直接通信することはできない。

【０２４６】

拡散クラウドデータを検索し呼び出すためのいくつかの考え得る方法が、図２０に図解されている。これには、左端の列に示された階層型ネームサーバ３００、中央の列にあるＲＡＩＤ冗長メモリ３０１、及び右端の列にある非集約型ストレージ３０２である。階層化ネームサーバ３０７では、サーバ３０７に格納されたデータフラグメントは、最初にサーバ３０６でソートされてより大きなファイルに集約され、最終的にサーバ３０６で１つのファイルにマージされる。ファイルは、検索と並べ替えに使用される暗号化されていな

い部分と、ユーザＩＤ情報を含む隠蔽または暗号化されたペイロードとで構成される。メタモルフィックＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｘからの要求に応答して、ネームサーバ３０５は、暗号化または隠蔽されたファイルを復号化プロセス２８７に渡し、復号化キー２８２と組み合わせてデータのロックを解除して｜ＨＮ｜２０６ｘにこれをロードし、ノードを分化されたＨｙｐｅｒＮｏｄｅ｜（この場合はネームサーバ｜ＮＳ｜２３６ａ）に変態するようトリガする。

【０２４７】

ＲＡＩＤ冗長メモリ３０１では、データドライブ３０８に格納されたデータフラグメントはデフラグされ、サーバ３０５に読み込まれる。続いてサーバ３０５は隠蔽されたデータを復号化プロセス２８７に渡し、復号化キー２８２と組み合わせてデータのロックを解除し、｜ＨＮ｜２０６ｘに読み込ませ、ノードを分化されたＨｙｐｅｒＮｏｄｅに変態させる。

【０２４８】

別の方法として、非集約型クラウド３０２では、クラウドサーバ３０７に格納されたデータ断片がデフラグされてサーバ３０５にロードされ、このサーバ３０５では、隠蔽されたデータが復号化プロセス２８７に渡され、復号化キー２８２と組み合わせてデータのロックが解除され、｜ＨＮ｜２０６ｘにロードされ、ノードが分化されたＨｙｐｅｒＮｏｄｅ（この場合はネームサーバ｜ＮＳ｜２３６ａ）にモーフィングされるようにトリガされる。

【０２４９】

図２１に示すとおり、断片化されたペイロードパケットの拡散データストレージは、前述のパズルピースのメタファーを用いて図解されている。断片化されたストレージでは、未処理データ（例えば、サウンド、ビデオ、ピクチャ、ファイル、プログラムなど）からなるオリジナルのメディアコンテンツは、決定的な相互接続及び相互関係を有する要素を含んでいる。オリジナルのファイルコンテンツ３２５は、わずかでも乱れが生じると、機能を破壊し、ファイルを復元不可能な状態にする可能性がある。ファイル格納プロセスにおいて、オリジナルファイルコンテンツ３２５は、ステップ３２６において、ステートベースのデジタル命令またはＨｙｐｅｒＣｏｎｔｒａｃｔ　２６０に従って、アルゴリズム的に断片化される。その後、断片化された日付要素３２７は、分離された構成要素３２７ａ（またはサブファイル）に分割され、別個のファイル記憶媒体３０８に格納され、拡散データ記憶３０１を集合的に表現する。保存プロセスにおいて、暗号鍵３２９が生成され、データの所有者またはＨｙｐｅｒＣｏｎｔｒａｃｔの作成者に送信され、データを再呼び出しできるようになる。

【０２５０】

図２２は、ネームサーバデータの冗長ファイル保存について図解している。例えば、更新されたネームサーバデータ３３０ａ、３３０ｂ、３３０ｃの解析ファイルは、ネームサーバノード｜NS_{13}｜、｜NS_{92}｜、｜NS_{46}｜からなる複数のストレージサーバ３３１、３３２、３３３に書き込まれ、総称して拡散型ネームサーバクラウドストレージ３０２を実行する。このように、データ３３０ａからなるファイル解析ファイル１は｜NS_{13}｜と｜NS_{46}｜との両方に冗長的に格納され（図示せず）、データ３３０ｂからなるファイル解析ファイル２は｜NS_{92}｜と｜NS_{46}｜との両方に冗長的に格納され、データ３３０ｃからなるファイル解析ファイル３は｜NS_{13}｜と｜NS_{92}｜との両方に冗長的に格納される。

【０２５１】

｜NS_{13}｜のファイル１とファイル３、｜NS_{92}｜のファイル２とファイル３、｜NS_{46}｜のファイル１とファイル２の保存は、それぞれファイルストレージアクセスリンクキー３１９ａ、３１９ｂ、３１９ｃを自動的に生成し、これらはそれぞれサーバ３３４ａと３３４ｂにホストされているネームサーバノード｜NS_{21}｜と｜NS_{77}｜、その他（図示せず）に冗長的に保存される。いずれかの｜ＮＳ｜ストレージノードがオフラインになると、データは別のネームサーバノードにクローニングされる。一実施形態では、各

｜ＮＳ｜ノードは、現在オンラインになっているバックアップサーバをリストアップした動的ＨｙｐｅｒＣｏｎｔｒａｃｔを発行し、維持する。サーバがオフラインになると、ＨｙｐｅｒＣｏｎｔｒａｃｔは自動的にデータを別のサーバにクローニングし、その後、新しいバックアップＨｙｐｅｒＣｏｎｔｒａｃｔを発行し続ける。

【０２５２】

ネームサーバ拡散クラウドが記憶するネームサーバデータベースを更新する処理は、データ記憶リソースがオンラインになったり、消滅したりするたびに実行される。図２３に示すとおり、登録処理は、リソースに変更があるたびに実行される。例えば、新しいＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ｐがＨｙｐｅｒＳｐｈｅｒｅネットワークに参加すると、この情報がネームサーバノード｜ＮＳ｜２０７ｍにそのノードを登録するように通知する。ノード登録の開始処理は、直接行うこともできるが、「ｈｅｌｌｏ」プロセスの一部として権限ノードを使用して行うこともできる。新しいノードの動的ＩＰアドレスを受信し、新しいＳＤＮＰアドレスとＳＤＮＰジップコードを割り当てた後、ネームサーバ拡散データクラウドはデータベースの関連部分をストレージサーバ３３３にホストされている｜ＮＳ｜２０７ｎにダウンロードし、そこでは、新しいコンテンツ３３０ｐがファイルに追加されるように解析ファイル３３０ａが作成される。このファイルは次に、ファイル３３０ｒや３３０ｓのような複数の断片に再解析することにより、｜ＮＳ｜２０７ｎによる保存のためのステップ３２８で処理されてから、ネームサーバノードの拡散データクラウド３８３ａにアップロードされる。同時に、修正されたリンクキー３２９ｂがネームサーバ｜ＮＳ｜２０７ｐに転送され、ネームサーバ運用要求に使用される。

【０２５３】

一方、ＨｙｐｅｒＮｏｄｅ　２０６ｐは、ネットワーク内の｜ＮＳ｜２０７ｍや他のノードとの接続性を確保するために、定期的なネットワークブロードキャスト、すなわちｐｉｎｇを開始する。もしｐｉｎｇが何度か失敗した場合、登録プロセスが繰り返され、アクティブなノードのネームサーバリストからノード｜ＨＮ｜２０６ｐが削除される。

【０２５４】

分散型メッシュネットワークセキュリティ規定

【０２５５】

分散型ＳＤＮＰネットワークにおけるデータ通信のセキュリティには、多くの革新的な手法が利用されている。これらの手法は、前記米国特許第９，９９８，４３４４号に開示されているものと類似しているが、専用機能のネットワークノード、中央権限、またはネットワークオペレータを持たない分散化された運用に合わせて適応されている。すなわち、

・「分業」。どのＨｙｐｅｒＮｏｄｅも、意味のあるペイロードを取り出すために必要とされるすべての情報にアクセスすることができないことを意味している。すなわち、｜ＮＳ｜ノードはＨｙｐｅｒＮｏｄｅのアイデンティティに関する情報を持っているが、ペイロードやｄ'ＳＤＮＰデータパケットのルーティングに関する知識はまったくなく、｜Ａ｜ノードはパケットのルーティングを制御しているが、ＨｙｐｅｒＮｏｄｅユーザのアイデンティティやペイロードのコンテンツに関する知識もなく、また｜Ｔ｜ノードはコンテンツを搬送するが、ＨｙｐｅｒＮｏｄｅユーザのアイデンティティやパケットの最終的なルーティングに関する知識を持たない。ＨｙｐｅｒＮｏｄｅｓは次のホップ先を知っているだけで、エッジデバイスや発信者の身元については全く認識していない。

・「ＤＭＺ（エアギャップ）」共有秘密。データパケットを搬送する｜Ｔ｜ノードが、ペイロードの内容を暗号化または難読化するための隠蔽アルゴリズムがどのように選択されているかについて一切の情報を持たないことを意味する。コンシールメントアルゴリズムと暗号は、拡散ＤＭＺクラウドに事前にインストールされているゼロデイコンポーネントであり、通信セッションに先立って存在している。

・「メタモルフィックハイパーノード」。専用の機能ノードを使用する必要がないため、特定のハイパーノードの役割は｜Ａ｜，｜Ｔ｜，｜ＮＳ｜機能の間で常に変化するため、機能に特化した攻撃機会を防止することができる。

・「動的ＨｙｐｅｒＳｐｈｅｒｅネームサーバ｜ＮＳ｜」。ネットワーク上に登録されて

いるすべてのＳＤＮＰノードのＨｙｐｅｒＳｐｈｅｒｅの現在のリストが格納されているインターネットのＤＮＳネームサーバとは関係のないデータベース。ノードのリストは、｜ＮＳ｜拡散クラウドに保存され、データパケットを転送するタスクノードでは利用できない（このため、フィッシングを防止するための役割分担は維持される）。
・「フラグメント化されたデータ転送」。ファイルを小さなスニペット（サブパケット）に解析し、そのスニペットをデータパケットにしてメッシュ化されたネットワーク上で送信しているため、ハッカーがパケットをひとつ傍受したとしても、パケットのペイロードから有用なコンテンツを抽出することはできない。
・「メッシュ化ルーティング」。ネットワーク伝搬遅延のタイムリーな知識に基づいてデータパスを動的に変更する。情報はセッションのルーティングを担当する権限ノード以外はアクセスできない拡散型｜Ａ｜データクラウドに保存され更新される。
・「ディスパッチャベースのパケットルーティング」。｜Ａ｜ノードは、ネットワーク内の次の宛先へのシングルホップのみを実行するための情報を各タスクノードに通知することでデータパケットをルーティングしている。
・「匿名データパケット」。各ＳＤＮＰデータグラムは、データパケットの元の送信元や最終的な宛先、すなわち｜ＮＳ｜拡散クラウドから取得したＳＤＮＰノードの動的ＩＰアドレスからなる名前を明らかにすることなく、シングルホップ（すなわちパケットを送信しているノード）のＩＰ送信元アドレスとパケットの次の宛先のＩＰアドレスのみを表示する。データパケットの匿名性は、サイバーターゲットをプロファイリングしたり、攻撃手法を開発するためのパターン化された行動を識別したりする上で、メタデータの収集を無意味にする。
・「動的なセキュリティ認証情報とアルゴリズム」。参加するタスクノードが知る必要があることに基づいてアクセス可能な｜Ｔ｜拡散クラウドに安全に保存されたステートベースの共有秘密を使用することで、コンシールメントの方法（スクランブル、暗号化、ジャンク化、分割、及びそれらのアンチ機能を含む）を変更する。
・「ステートレスノード操作」。分化したＨｙｐｅｒＮｏｄｅは、指定されたジョブを完了すると未分化なメタモルフィック状態に戻り、最後のアクション（またはそのアクションの実行に関連したデータ）に関するすべての情報を破棄する。
【０２５６】
メタモルフィックなＨｙｐｅｒＮｏｄｅと、権限ノードが発行したコマンド及び制御パケットを実行するメッシュ化された動的ルーティングを組み合わせることで、ＨｙｐｅｒＳｐｈｅｒｅ内のパケットルーティングは、中央の権限やネットワークオペレータに依らず、予測不可能な形で実行される。本明細書に開示されているような自律的な「メッシュルーティング」を使用した分散型ＳＤＮＰ通信では、データトラフィックの指示やネットワークの管理にオペレータが関与しないため、ネットワークのセキュリティが向上する。クライアント｜ＨＧ｜３５０ａから｜ＨＧ｜３５０ｂに送信される３つの連続したパケットの分散型ＳＤＮＰルーティングの例を図２４に示す。左側の列では、データは安全な接続３５２ａを通じてタスクノード｜Ｔ｜３５１ｄに渡され、次に安全な接続３５２ｂを通じてクライアント｜ＨＧ｜３５０ｂに渡る。権限ノードは、権限ノード拡散クラウドからダウンロードした伝搬遅延データに基づいてパケットルーティングを決定する。
【０２５７】
分散型ＳＤＮＰ通信の第２の特徴は、動的なセキュリティ及びコンシールメント技術の使用である。例えば、安全な接続３５２ｄと３５２ｅのセキュリティクレデンシャル情報とコンシールメントアルゴリズムは、固有のシングルホップ数値シード、暗号鍵、及び動的なステート条件の採用を含めて異なっている。その結果、暗号を破り、動的セキュリティを破るという事実上不可能な操作を１００ｍｓ（データが安全な接続３５２ｄを通過するのにかかる時間）で達成したとしても、１００ｍｓ後には、データが全く異なるセキュリティ方法と鍵を使用して安全な接続３５２ｅを介して転送されるため、全プロセスを再度１００ｍｓ後に行う必要がある。
【０２５８】

分散型ＳＤＮＰ通信における動的セキュリティについては、図２５でさらに詳しく説明している。この図で、ノード｜Ｔ１｜からノード｜Ｔ２｜へのデータパケットの転送に使用されるセキュリティ方法３５２ｄは、ホストデバイスのハードウェアと一致するＭＡＣレイヤ２アドレス３９０ａからなるデータパケットと、ネームサーバ拡散クラウド｜ＮＳ｜から供給されるＨｙｐｅｒＮｏｄｅ｜Ｔ１｜と｜Ｔ２｜のＳＤＮＰアドレスに対応する動的ＩＰアドレスからなる送信元及び宛先ルーティングアドレス３９１ａと３９１ｂから構成されている。また、トランスポートレイヤ４基準（例としてＴＣＰとして示される）３９３ａと、認証、承認、管理のシーケンスからなるＡＡＡ検証でＣＡデジタル証明書を介して双方の身元を確認するセッションを検証するためにセッションレイヤ５データ３９４ａが使用されている。成功したセッション検証は、データパケットの残りの部分の処理を開始するために必要とされる。ＳＤＮＰ固有のセキュリティ認証情報は、プレゼンテーションフィールド３９５ａ及びアプリケーションデータフィールド３９８ａでデータグラムと共に運ばれる。

【０２５９】

時間t_1のようなステート変数、ゾーンＹのセキュリティ手段、及び暗号鍵１と数値シードＹ１のようなステート変数からなるプレゼンテーションレイヤ６のデータフィールド３９５ａは、その後、プロセス３９６ａにおいて、他のシードまたは鍵データ（セッションのルーティングを担当する権限ノードからのコマンド＆制御（Ｃ＆Ｃ）パケットによってデータルーティングに先立って配信される）と結合される。この情報は、タスクノード拡散クラウド｜Ｔ｜から供給されるセキュリティアルゴリズムと組み合わせて使用され、コンシールメントアルゴリズム３９７ａを実行して、受信ファイルデータを脱処理（回復）し、新たに隠蔽されたデータ３８９ａに変換するために使用される。

【０２６０】

全体の処理は、シングルホップセキュリティ手段３５２ｄから手段３５２ｅへのデータの引き渡しに伴い、タスクＨｙｐｅｒＮｏｄｅ｜T_2｜３５１ｂによって繰り返される。したがって、ＭＡＣアドレス３９０ａは、デバイスホストノード｜T_2｜が送信元ＭＡＣアドレスとなり、デバイスホストノード｜T_3｜が宛先アドレスとなるよう３９０ｂに更新される。データグラムの送信元ＩＰアドレスは、ＳＤＮＰノード｜T_1｜３９１ａの動的ＩＰアドレスから、ＳＤＮＰノード｜T_2｜３９８ｂの動的ＩＰアドレス、すなわちＤＩＰ｛ＳＤＮＰ｜T_2｜｝に変更される。同様に、データグラムの宛先ＩＰアドレスは、ＳＤＮＰノード｜T_2｜３９１ｂの動的ＩＰアドレスから、ＳＤＮＰノード｜T_3｜または３９１ｃの動的ＩＰアドレス、すなわちＤＩＰ｛ＳＤＮＰ｜T_3｜｝の動的ＩＰアドレスに変更される。Ｌ４トランスポートデータフィールド３９３ｂは、適切なダイナミックポート番号で更新され、ＣＡデジタル署名及びクレデンシャルは、新たなＡＡＡ検証プロセスなしにＬ５フィールド３９４ｂに保持される。

【０２６１】

次に、レイヤ６のＳＤＮＰデータ３９５ｂは、時刻t_2、ゾーンＹ（変更なし）、暗号鍵２（新しい鍵）、更新された数値シードＹ２を含む新しいセキュリティ認証情報に更新される。同時にＣ＆Ｃパケットは、ｄ'ＤＭＺタスククラウド拡散データ｜Ｔ｜として格納された新しい隠蔽３９７ｂアルゴリズムへのリンクをダウンロードする。その結果、１００ミリ秒前の前身の３９８ａから認識できない隠蔽ペイロード３９８ｂが変更される。

【０２６２】

図２４に示すようなデータ断片化及びトランスポートでは、単一のパケット内に含まれるデータは、元のメディアコンテンツのほんの一部を表しているに過ぎない。元のファイルを構成するすべてのパケットを収集しなければ、データファイルアセンブリの再構成を行うことができない。すなわち、暗号化されたファイル全体がなければ、平文ソースの復号化及び復元を行うことはできない。また、前述のメッシュ化された動的ルーティングであるため、単一のノードに対する攻撃では、元の暗号化ファイルを収集して再構築するために必要なパケットをすべて傍受することができない。例えば、同図の中央の列では、データパケットは、従来のルーティングとは全く異なるルーティングであるセキュア接続３

５２ｃ、３５２ｄ、３５２ｅ、３５２ｆを用いて、タスクノード３５１ａ、３５１ｂ、３５１ｃを介して転送される。右端の列で、データは安全な接続３５２ｇを介してタスクノード３５１ｃにルーティングされ、続いて接続３５２ｈを介してタスクノード３５１ｂにルーティングされ、接続３５２ｉを介してタスクノード３５１ｄにルーティングされ、最後に安全な接続３５２ｊを介してクライアントゲートウェイ３５０ｂにルーティングされる。

【０２６３】

図２６は、任意のひとつのデバイスや記憶媒体への知識の集中を防ぐためのハイパーセキュア通信における分業の原理を示している。パケットルーティングにおいて、動的ＩＰアドレス４０１を有するネームサーバノード｜ＮＳ｜４００は、ステップ４０４の間に、ステップ４０６の動的ＩＰアドレス４０６を有する｜Ａ｜ノード４０５から送信されたデータグラムのペイロード４０８内の宛先ＩＰアドレス４０７及びＣ＆Ｃ（コマンド及び制御命令）にロードされるＳＤＮＰアドレスからＩＰアドレスへの変換テーブルを含むペイロード４０３を携えて、ＩＰ宛先アドレス４０２で権限ノード｜Ａ｜にデータグラムを送信する。Ｃ＆Ｃ命令ファイルは、タスクノード｜$Ｔ_1$｜３５１ａに転送され、ノード｜$Ｔ_1$｜の送信元ＩＰアドレス３９１ａ、ノード｜$Ｔ_2$｜の宛先ＩＰアドレス３９２ａ、セキュリティクレデンシャル情報からなるＳＤＮＰ情報３９５ａ、及び暗号化されたペイロード３９８ａからなるメディアパケットを構築し、次の宛先に転送することを記述している。このようにして、｜ＮＳ｜ノード４００、｜Ａ｜ノード４０５、及び｜Ｔ１｜ノード３５１ａは、どのようなジョブを実行すべきかをノードに指示するために必要な情報のみを共有する。情報交換の対象を知る必要のあるコンテンツに限定することと分業を組み合わせることで、デバイス上または分散型ＳＤＮＰネットワーク上での組織的な攻撃を混乱させる。

【０２６４】

ＤＮＰ通信プロトコルを表現するひとつの方法に、インターネットのＴＣＰ／ＩＰプロトコルを表現するのに使用されるのと同じ７層ＯＳＩ抽象化モデルの使用がある。そこで、図２７に、ネットワークレイヤ３データ４２３及びトランスポートレイヤ４データ４２４で構成される分散型ＳＤＮＰルーティングを実行するため、ＳＤＮＰデータグラム４２０を使用して、別々のＳＤＮＰスタック４２８及び４２９を介して通信する２つのデバイスを示した。ＳＤＮＰのハイパーセキュアデータトランスポートの上には、セッションレイヤ５データ４２５、プレゼンテーションレイヤ６データ４２６、及びアプリケーションレイヤ７データ４２７があり、クライアントアプリケーション、オンラインアプリケーション、及びブロックチェーン・アプリケーションをサポートするＨｙｐｅｒＮｏｄｅの操作を容易にしている。このように、ＨｙｐｅｒＳｐｈｅｒｅ通信は、ＰＨＹレイヤ１データ４２１及びＭＡＣレイヤ２データ４２２に関係なく、レイヤ３～レイヤ７を用いて行われる（ＳＤＮＰ対応のＨｙｐｅｒＳｐｈｅｒｅルータを実現する場合を除く）。

【０２６５】

ネットワークレイヤ３とトランスポートレイヤ４を介して実行されるルーティングは完全に分散化されているため、ＨｙｐｅｒＳｐｈｅｒｅルーティングはオープンソースではないとは言え、メッシュ化された動的ネットワーク上のトランスポートは自律分散型であるため、誰の制御も受けず、またパケットルーティングが監視されることさえない。さらに、分散型システムであるため、ネットワークオペレータ、政府、またはハッカーが、パケットルーティングを迂回したり、ネットワーク操作を乗っ取ることもできない。自律型ネットワークユーティリティは別にしても、レイヤ５からレイヤ７で利用可能なＨｙｐｅｒＮｏｄｅのユーザ機能はオープンソースであり、ユーザはＨｙｐｅｒＳｐｈｅｒｅをプラットフォームとして、独自の認証、セキュリティ、アプリケーションを開発し実施することができる。

【０２６６】

ＳＤＮＰプロトコルスタックのネットワークレイヤ３で表されるように、分散型ＳＤＮＰパケットのＩＰアドレスは動的（頻繁に変更される）であるだけでなく、ＨｙｐｅｒＳ

ｐｈｅｒｅルーティングでは、インターネットのドメインネームサーバ（ＤＮＳ）が使用されていない。その代わりに、動的ＩＰアドレスをユーザの身元情報、電話番号、物理デバイス、ＭＡＣアドレスなどとリンクするＳＤＮＰネームサーバ機能が、ｄ'ＳＤＮＰネームサーバ拡散｜ＮＳ｜クラウドを介して完全に分散化された方法で実現されており、メタモルフィックＨｙｐｅｒＮｏｄｅを介してアクセスし、ＨｙｐｅｒＳｐｈｅｒｅ｜Ａ｜オーソリティノードを介してのみ実行される。ＨｙｐｅｒＳｐｈｅｒｅ　ＩＰデータグラムでは、シングルホップの送信元と送信先のＩＰアドレスのみが指定されるが、パケットの送信元や最終的な送信先は公開されない。

【０２６７】

匿名データパケットを使用してＳＤＮＰパケットの真の送信元と送信先を難読化することで、通話の送信元を追跡することができなくなり、クライアントをプロファイリングから保護することができる。意味のあるパケットルーティングアドレスがなければ、ハッカーはスニッフィングや監視によってどのパケットが互いに関連しているかを判断することはできない。メタデータの監視やＤＯＳ攻撃をさらに困難にするため、トランスポートレイヤ４のＳＤＮＰプロトコルは、特定のポート番号や定義されたサービス（電子メールやＦＴＰなど）を持たないアドホックな動的ポートアドレスを採用しているため、攻撃者はパケットの内容をコンテキストから分析することはできない。さらにまた、ＳＳＬやＴＬＳのトランスポートセキュリティ（攻撃に対して脆弱であることが知られている）を使用するのではなく、ｄ'ＳＤＮＰトランスポートセキュリティがクラウド内でホップバイホップベースで実行されるトンネリングプロトコル（ＩＰＳｅｃなど）によって実行される。

【０２６８】

ＨｙｐｅｒＳｐｈｅｒｅのトランスポートプロトコルは、ＱｏＳ（サービス品質）を最大化するため、ペイロードの性質に応じてＴＣＰとＵＤＰの両方の伝送方式を採用している。ソフトウェアコードやコンテンツ配信などの信頼性の高いペイロード配信には伝送制御プロトコル（ＴＣＰ）が採用されている一方、音声やライブ映像、その他のリアルタイム（ＲＴ）通信にはユーザデータグラムプロトコル（ＵＤＰ）が採用されている。さらに、ＲＴデータグラムは、ネットワークの最短伝搬遅延パスを介して権限ノード｜Ａ｜によってルーティングされる。ＴＣＰルーティングは、より高い冗長度で信頼性を最大化することに焦点を当てた「高整合性」配信用として予約されている。

【０２６９】

時間の影響を受けにくいＴＣＰパケットは、ＵＤＰパケットとは全く異なるメッシュ化されたルート経由でルーティングされることが多い。前述の方法を使用することで、分解されたデジタルコンテンツ、会話、メディア、またはトランザクションセッションの不正な再構築を防止することができる。このように、ＳＤＮＰネットワークの動作は、データを断片化し、単一のパケットを同じタスクノードを介してのみルーティングすることによって、ネットワーク内の任意の単一ノードで運ばれるコンテンツを制限することで、シングルポイント攻撃を混乱させる。

【０２７０】

「ＨｙｐｅｒＮｏｄｅホップコード」、つまりＨＨＣ　４３４の生成は、ＳＤＮＰパケットトランスポートの卓越した機能のひとつである。ＨＨＣは、ブロックチェーンアプリ、ハイパーコントラクト、ＢａａＳ（Ｂｌｏｃｋｃｈａｉｎ－ａｓ－ａ－ｓｅｒｖｉｃｅ）におけるブロックチェーン処理に必要とされ、トークンや暗号通貨の取引に使用される、パケット転送中に付随的に作成される一過性のブロックチェーンである。これらはデータパケットの分散型動的メッシュデータルーティングの一部として生成されるため、ＨＨＣ　４３４には、偽造や複製を撃退するランダム化された暗号化ハッシュ値が含まれている。

【０２７１】

プライバシーを確保するため、ＨｙｐｅｒＳｐｈｅｒｅは、レイヤ５データ４２５を使用して各セッション（及びそこから得られるコンテンツ）を非公開化する。セッションデータには、ＡＡＡログインダイアログを介した身元確認、権限ノードが発行した｜Ａ｜コ

マンド＆制御（Ｃ＆Ｃ）パケット、及びデジタルＣＡ証明書に基づく信頼されたデバイスとトランザクション（後述）を介して配信されるセキュリティクレデンシャル情報が含まれる。

【０２７２】

ｄ'ＳＤＮＰネットワーク動作のもうひとつの属性では、データパケットのペイロード４２７の内容を隠蔽し、不正アクセスを防止するために、セキュリティクレデンシャル情報とアルゴリズムを含む権限ノードが発行した｜Ａ｜コマンド及び制御（Ｃ＆Ｃ）パケットをプレゼンテーションレイヤ６データ４２６と組み合わせて使用されている。ステートベースのセキュリティとは、ＳＤＮＰデータグラムを保護するために使用されるセキュリティ手法とクレデンシャルが、そのステートに応じて変化する手法を指している。セキュリティの「ステート」とは、データパケットが作成された時点で存在するステートのことであり、ネットワーク時刻、場所、セキュリティゾーンなどが含まれる。ＨｙｐｅｒＳｐｈｅｒｅにおけるパケットのコンシールメントは、データパケットが時空間ネットワークを通過する際に実行されるさまざまなステートベースのセキュリティメカニズムを使用してペイロードを変更することで実現される。

・動的な分割と混合。
・動的なスクランブルとスクランブル解除。
・動的な暗号化と復号化［３９８］［３９９］
・ジャンクデータ（またはパケット）の動的な挿入と削除
・時間とゾーンに依存したステート

【０２７３】

分散型ＳＤＮＰペイロードセキュリティは、ハイパーノードがメタモルフィックであり、ＤＭＺサーバが拡散型クラウド上で実現されることを除いては、前記米国特許第９，９９９８，４３４４号で開示された固定インフラストラクチャＳＤＮＰプロトコルと同様のステートベースのセキュリティアルゴリズム及びクレデンシャルを使用した動的コンシールメント手法を採用している。前述のとおり、ステートベースの動的コンシールメントに関しては図２５及び図２６に図解されているが、セキュリティクレデンシャル情報、アルゴリズム、及びペイロードの内容は、ネットワーク時間に依存し、ＳＤＮＰコマンド及び制御パケット４３１で配信されるホップ毎に変化する。動的ステートはさらに、ＨｙｐｅｒＳｐｈｅｒｉｃクラウド内のゾーン、地理的領域（サブネット）にさらに細分化される。

【０２７４】

上記の方法を使用すると、ＨｙｐｅｒＳｐｈｅｒｅを通過する２つのパケットが同じ構造を持つことはない。つまり、万が一、２つのパケットが同じ会話またはセッションの一部であると識別できたとしても、そのパケットは同じステートベースのセキュリティクレデンシャル情報（鍵、シード、タグ、ジップ）を持たず、同じフラグメント化、スクランブリング、暗号化、またはジャンクデータアルゴリズムを使用していないのである。言い換えれば、２つの関連するデータグラムを特定したとしても、ハッカーが安全なメッセージコンテンツを再構築する確率を向上させることにはつながらないのである。このため、本明細書に開示される動的セキュリティは、ネットワークのステートが時間と共に常に変化するＤＡＧ（有向非巡回グラフ）の動的バージョンであるＤｙＤＡＧで構成されている。ＤｙＤＡＧの動作及びその技術的実現は、ＨｙｐｅｒＳｐｈｅｒｅルーティング、コマース、及びブロックチェーン（本明細書で後述）の基本的な構成要素である。

【０２７５】

ＳＤＮＰデータグラム４２０のペイロード４２７は、リアルタイムデータ（ライブ映像、オーディオ）、写真や映像などのメディアコンテンツ、アプリケーションコード（ソフトウェアディストリビューション）、及び暗号鍵やＣＡ証明書などを含むユーザ及びアプリケーション固有のレイヤ７セキュリティクレデンシャルを含むファイル４３０など様々な種類のコンテンツを含むことができる。｜Ａ｜ルーティングタスクにおいて、ペイロード４２７は、Ｃ＆ＣパケットＣ４３１のようなＳＤＮＰのコマンド＆制御命令を含むことができる。ペイロード４２７はまた、実行可能コード（ＨｙｐｅｒＣｏｎｔｒａｃｔ　４３

２）、ＤＬＴ／ＢＣデータベース４３３上のトランザクション、及びＨｙｐｅｒＣｏｉｎ４３４、ビットコイン、及びその他のデジタル資産などのトークンまたは暗号通貨を含む多数のブロックチェーン関連ファイルを安全に配信することができる。

【０２７６】

ＨｙｐｅｒＳｐｈｅｒｉｃノードの展開

【０２７７】

図２８に示すとおり、ＨｙｐｅｒＮｏｄｅｓ　３８０は任意のホストデバイスにインストールして、それをＨｙｐｅｒＳｐｈｅｒｉｃノードに変換することができる。デバイスは、サーバ３７０、デスクトップコンピュータ３８４、及び暗号通貨マイニングマシン３６１を含む高性能ＡＣ電源システムを含むことができる。その他の適切なデバイスとしては、低性能であっても、ＷｉＦｉルータ３６８、イーサネットルータ３６９、ゲーミングコンソール３６５、ＨＤＴＶ　３６７、及びＩｏＴデバイス（例えばスマート冷蔵庫３６６）が含まれる。タブレット３６１や携帯電話３６０などのモバイル機器は、豊富なコンピューティング能力を有しているが、バッテリ寿命は限られている。自動車３７１や商用トラック３７２などの車両は、密な通信グリッドを形成する可能性があり、特にモバイルネットワークに障害が発生した場合に価値がある。

【０２７８】

ハードウェアの取得やインストールを一切必要とせず、完全にソフトウェアをベースにした相互運用可能なハイパーセキュアハイパフォーマンスクラウドを実現する意義は、ＨｙｐｅｒＮｏｄｅの総数が、地上のあらゆる商用ネットワーク、さらにはＡＷＳ、ＧＷＳ、Ａｚｕｒｅ（ＨｙｐｅｒＮｏｄｅもホストしている）をも凌駕するほど急速に拡大する可能性があることを意味している。ただし、大規模な商用クラウドと異なり、ＨｙｐｅｒＳｐｈｅｒｅは、パソコン、スマートフォン、インターネットルータ、ゲーム機、ビットコインマイナー、ＨＤＴＶ、ＩｏＴデバイス（冷蔵庫など）、車やトラックなどからサポートを得ることもできる。

【０２７９】

今日のインターネットは、２億台のサーバを使用し、１０億台のネットワーク接続されたＰＣをサポートしている。携帯電話の利用者は世界人口の６６％を占め、５０億人が９０億の契約を結んでいる。つまり、地球上の人口よりも１０億人多い契約数、つまり多くの人が複数の携帯電話を持っていることになる。さらに、現在のＩｏＴデバイスは２７０億台で、２０２４年までに６００億台を超えると予想されている（ｈｔｔｐｓ：／／ｗｗｗ．ｓｔａｔｉｓｔａ．ｃｏｍ／ｓｔａｔｉｓｔｉｃｓ／４７１２６４／ｉｏｔ－ｎｕｍｂｅｒ－ｏｆ－ｃｏｎｎｅｃｔｅｄ－ｄｅｖｉｃｅｓ－ｗｏｒｌｄｗｉｄｅ／）。

【０２８０】

前述のように、ＨｙｐｅｒＳｐｈｅｒｅへのアクセスは、ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜２０６ソフトウェアベースの自律型ネットワーク要素、クライアントのアプリケーションに組み込まれたＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜２０１、またはＬ１／Ｌ２物理接続を管理するＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜２０５で構成されている。図２９に示すとおり、便宜上、これらのＨｙｐｅｒＳｐｈｅｒｉｃソフトウェアのインスタンスを総称して「ＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェア３８０」と呼ぶことがある。また、ＨｙｐｅｒＳｐｈｅｒｅポータルは、主要なホストＯＳごとに利用可能な汎用ソフトウェアで構成されているが、その機能の性能は、ホストデバイスのハードウェアに基づいて異なる。特に、ＨｙｐｅｒＳｐｈｅｒｅポータルは、通信－ネットワーキング３８１、分散コンピューティング３８２、拡散型クラウドデータストレージ３８３、及びＩｏＴクラウド接続性３８４に合わせて最適化することができる。

・クライアントエッジデバイス（携帯電話３６０など）、ネットワークルータ、及び商用サーバクラウド（図示せず）を含む通信ネットワークコンポーネント３８１で構成されるＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェア３８０は、最小限のコンピューティングを実行するが、可能であれば、光ファイバ回線及びマイクロ波無線リンク、ギガビットイーサネットルータ、８０２．１１ａｃなどの高速ＷｉＦｉ、及び４Ｇまたは５Ｇモバイルネ

ットワークで構成される高速ネットワークを横断する高帯域幅の接続性を必要とする。ＨｙｐｅｒＳｐｈｅｒｅポータルをホストする固定インフラストラクチャの重要な要件の１つは、安定した信頼性の高い電源、つまり高いアップタイムと永続的な可用性である。
・ＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェア３８０は、ピアツーピア（Ｐ２Ｐ）または車両間（Ｖ２Ｖ）通信もサポートしている。ピア通信は、固定の有線またはモバイルインフラストラクチャへのアクセスができない場合（山間部を走行する場合など）や、ネットワークがオフラインの場合（自然災害時など）に重要な存在となる。ＨｙｐｅｒＳｐｈｅｒｉｃのピア通信では、携帯電話や自動車などの利用可能なリソースを募集したり、利用可能なものを徴発したりしながら、遍在するネットワーク上での通信とは必然的に異なる動作をすることになる。有線のインフラがまったくない地方の地域では、ＨｙｐｅｒＳｐｈｅｒｅ通信は、キャリア周波数の低い携帯電話、衛星ネットワーク、極端な場合にはドローンがホストする無線接続、またはＣＯＷ（セル－オン－ホィールズ）ネットワークに依存しなければならない。性能とＱｏＳは別として、ＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェア３８０は、それらをホストする物理ネットワークに依存しない方法で動作するが、唯一の条件は、ＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェアがデバイスホストのＯＳと互換性が必要という点である。
・分散コンピューティングコンポーネント３８２を構成するＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェア３８０は、実質的なコンピューティング能力（一般的には、１秒間に数百万回の浮動小数点演算（ＭＦＬＯＰまたは数百万回の浮動小数点演算）で測定される）及びスクラッチパッドメモリ（揮発性メモリ、すなわちＲＡＭ）の十分な容量を有するデバイスを採用し、メモリスワップ（読み取り／書き込みサイクル）のアンドゥなしで計算を実行することができる。ホストには、高速商用サーバやサーバファーム、または多数のパーソナルコンピュータ３６４の集合体を含めてもよい。他の高性能ホストとしては、暗号通貨のマイニングコンピュータ及びゲーミングコンピュータなどがある。最も有益なコンピューティングリソースは、高いアップタイムとネットワークの可用性のために一定の電力を維持する。とはいえ、適切に管理されている世界のスマートフォンの膨大な数（９Ｂ）は、膨大な計算量が必要になる可能性を表しており、この問題は、各サブタスクがデバイスの充電あたりのバッテリ寿命よりも多くの時間を必要としないこと、あるいは圧倒的な揮発性メモリ容量が必要とされない限り解消されない。
・拡散型クラウドストレージ３８３を構成するＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェア３８０は、大容量のサーバファーム（それに相当する大規模なメモリ容量を有する）または多数の小容量のオンライン接続メモリデバイスのいずれかを採用している。容量の小さいストレージでは、断片化やメモリのメンテナンスが必要になる。
・ＩｏＴクラウド接続デバイス３８４を構成するＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェア３８０は、計算、ストレージ、または通信帯域幅の需要がほとんどない軽量のデバイスで構成されている。ただし、例えば防犯カメラなどのリモートデバイスは低消費電力を必要としている。しかし、ＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェアは、ホストに大きな電力を必要としないため、当然ながらＩｏＴとの互換性があり、環境に優しいものとなっている。

【０２８１】

分散型ＳＤＮＰハイパーセキュア通信

【０２８２】

分散型ｄ'ＳＤＮＰハイパーセキュア通信のユースケースの例としては、以下が挙げられる。
・ＨｙｐｅｒＳｐｈｅｒｅ　ｄ'ＳＤＮＰメッセンジャーアプリ
・ＨｙｐｅｒＳｐｈｅｒｅ　Ｖ２Ｖアドホックピアネットワーク
・ＨｙｐｅｒＳｐｈｅｒｅマルチバンド通信
・ＨｙｐｅｒＳｐｈｅｒｅ　ｏｖｅｒ　５Ｇモバイルネットワーク
・ＨｙｐｅｒＳｐｈｅｒｅ分散コンピューティング
・ＨｙｐｅｒＳｐｈｅｒｅ拡散型データクラウドストレージ

・ＨｙｐｅｒＳｐｈｅｒｅクラウド接続デバイス
前記各アプリケーションには、特定のアプリケーションに必要なタスクを実行するために必要な発明的事項が含まれている。
【０２８３】
ＨｙｐｅｒＳｐｈｅｒｅ　ｄ'ＳＤＮＰメッセンジャーアプリ
【０２８４】
ＨｙｐｅｒＳｐｈｅｒｅ通信の１つの適用機能は、パーソナルメッセンジャーアプリケーションでハイパーセキュアなテキスト、音声、及びビデオを提供することである。図３０に示すとおり、ｄ'ＳＤＮＰ対応のパーソナルメッセンジャー４４７は、分散型ＳＤＮＰクラウド４４０を介してパーソナルメッセンジャー４４３と通信する。パーソナルメッセンジャー４４７は、マイク４５０１及びスピーカ４５０ｂとインターフェイスする携帯電話またはタブレット（図示せず）上にホストされたｄ'ＳＤＮＰメッセンジャーアプリ４４８で構成されている。パーソナルメッセンジャーには、ｄ'ＳＤＮＰクラウド４４０へのアクセスを提供する埋込みＨｙｐｅｒＳｐｈｅｒｅゲートウェイソフトウェアＨＧ４４９が含まれている。このゲートウェイは、ＨｙｐｅｒＳｐｈｅｒｅネームサーバ拡散クラウド上でのメッセンジャーとデバイスの登録を容易にし、他のｄ'ＳＤＮＰ通信アプリとの通信セッションを開くための接続ダイアログを管理する。
【０２８５】
メッセンジャー４４７から４４３への通話では、マイク４５０ａからの音声は、デジタル化され、断片化され、スクランブル化され、暗号化されてから（共有鍵４４２を使用して）、複数のパケットに分割される。ｄ'ＳＤＮＰクラウド４４０内でのデータ転送の間、データパケットは、ＨｙｐｅｒＮｏｄｅｓ４４１上の断片化されたデータパケットの動的メッシュ転送方式で転送され、データグラムは最終的にメッセンジャーアプリ４４３内に埋め込まれたＨｙｐｅｒＳｐｈｅｒｅゲートウェイ４４５に到達する。一連の関連するデータグラムが受信され、再結合され、復号化され、スクランブル解除されると、デジタル音声パケットはアナログ信号に変換され、スピーカ４４６ｂを駆動する。通常のＶｏＩＰテレフォニーでは、パーソナルメッセンジャー４４３のマイク４４６ａからメッセンジャー４４７のスピーカ４５０ｂへのメッセージの同時送信によって全二重会話が行われる。それぞれの連続したパケットは、ディスパッチャとして機能する｜Ａ｜ノードの指示のもとで、ｄ'ＳＤＮＰクラウド４４０を介して固有の軌跡をたどる。
【０２８６】
メッセンジャーのセキュリティは、２つの無関係なプロセスで実現される。すなわち、一方はエッジデバイスを含むクラウド４４００の外部で実行され、他方はクラウド４００の内部で自律的に機能する。図３１に示す一実施形態では、エッジセキュリティは、２つのメッセンジャー間で直接転送される１つ以上の暗号化キー４４２を使用した暗号化により実現される。図に示されるとおり、音声波形４５１ａは、暗号化されていない（平文とも表現される）ファイル４５１ｂに変換された後、鍵４４２を使用してプロセス４５２で暗号化され、結果として暗号文４５１ｃが得られる。エッジ暗号化ファイル４５１ｃは、ｄ'ＳＤＮＰクラウドを介して転送された後、アプリケーション４４３に転送され、プロセス４５３で暗号化されていない（平文の）ファイル４５１ｂに復号され、最終的にオーディオ波形４５１に戻される。
【０２８７】
ネットワーク４４０の関与なしに直接転送される暗号鍵４４２を含むので（例えば、鍵を直接転送することによって、または音声、ビデオ、または音楽の無害なデータストリームに隠されて）、エッジ暗号化はネットワークセキュリティとは別に、発信者に対するプライバシーの利益を促進する。どのような場合でも、鍵の転送は、通信セッションを開始する数日前、数週間前、または数ヶ月前に行うべきであり、エッジ共有秘密を使用した暗号化チャネルの使用が検出されないようにする。
【０２８８】
分散型ＳＤＮＰクラウド内のセキュリティには、エッジセキュリティとは別のプロセス

が含まれている。エッジセキュリティとは異なり、ダイナミッククラウドセキュリティは、いかなる当事者の参加も必要としない。ネットワークオペレータの関与なしに自律的に発生する。図３１は、ネットワークトランスポート中に動的に変化するｄ'ＳＤＮＰデータグラムの内容を示している。ｄ'ＳＤＮＰクラウド４４０内のセキュリティ規定は、動的なセキュリティ認証情報及び共有秘密（通信セッションの開始前に交換される秘密情報）を使用してホップバイホップで適用される。例えば、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜４４９によるデータの処理は、状態Ｓ１に従って行われるスクランブル動作４５３及び暗号化動作４５４でなされる。ステート$Ｓ_1$は、スクランブル動作が発生した時間、タスクノードがＨｙｐｅｒＣｏｎｔｒａｃｔからジョブを受け付ける時間、デバイスのセキュリティ領域、またはこれらのいくつかの組み合わせや他の時間によって変化するパラメータに基づいていてもよい。

【０２８９】

操作４５３によりパケット４５１ｃをスクランブルすることによって、データパケット４５１ｄが得られる。その後、このデータパケットは暗号化され、断片化される（データペイロードや他のパケットデータにアルゴリズムに従ってジャンクデータが挿入される）。このパケットは、暗号化されて無意味なジャンクデータで汚染されるだけでなく、他の通信セッションの内容と混合される。結果として得られるデータパケット４５１ｅは、断片化データの一部が、メッシュネットワークを介して複数の異なる経路に流れるため、その祖先の系統（パケット４５１ｄ）の完全な内容を欠いている。関連性のないデータまたはジャンクデータは、図では本文中の空の四角形□で表現されている。

【０２９０】

ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜４４１ａは、ステート$Ｓ_1$に従って復号化プロセス４５５でパケット４５１ｅを復号化する。この結果、元のデータパケット４５１ｂとはまったく似ていないデータパケットの断片化され暗号化されていない残骸が復元されることになる。ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜４４１ａは、その後、ステート$Ｓ_2$に従って、データパケットのペイロードを新たに暗号化する。したがって、データパケット４５１ｅを復号化する方法を知っていても、データパケット４５１ｇの復号化には何の役にも立たない。復号化プロセス４５７（ステート$Ｓ_2$を使用）とそれに続く暗号化プロセス４５８（ステート$Ｓ_3$を使用）は、｜ＨＮ｜４４１ｂ及びその他の中間ハイパーノード（図示せず）にて以下が達成されるまで繰り返される。すなわち、出口ゲートウェイノード｜ＨＧ｜４４５がメッシュ化ネットワークからの関連するすべての着信パケットからジャンクを除去して結合し、続いてファイルをアルゴリズム的にマージし、そのコンシールメント処理で使用された最後のステート（ここではステートＳ３）に従って、結果として得られたパケットを復号化する（スクランブル化されたパケット４５１ｄを回復する）。復元されたパケット４５１ｄはまだスクランブル状態であるので、暗号を破り、復号化プロセス４５９をエミュレートするブルートフォース攻撃をしかけても、ハッカーが受信ファイルの復号化に成功したかどうかを知る方法がないので、完全に非生産的である。

【０２９１】

最後のステップで、パケット４５１ｄは、メッセンジャーアプリケーション４４３に埋め込まれたＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜４４５内でスクランブル解除され、エッジ暗号化プロセスによって、まだ暗号化されているデータパケット４５１ｃが復元される。その後、エッジユーザキー４４２の保持者のみが、パケットを復号化して平文ファイル４５１ｂを抽出することができる。

【０２９２】

ＨｙｐｅｒＳｐｈｅｒｅ　Ｖ２Ｖアドホックピアネットワーク

【０２９３】

メッシュ自律ネットワークの分散化のもうひとつの利点は、固定インフラやモバイルネットワークに障害が発生した場合でも、瞬時に自律的なピアツーピア（Ｐ２Ｐ）や車車間ネットワーク（Ｖ２Ｖ）を形成できることである。前述のように、エッジデバイスとｄ'ＳＤＮＰクラウドとの間のインターフェイスは、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイと呼

ばれる多機能ソフトウェアポータルである。対称的にサンドボックス化されたＨｙｐｅｒＮｏｄｅがホストから分離されているのとは異なり、｜ＨＧ｜ノードは、ホストのデバイスからアプリケーションデータにアクセスすることができる。例えば、図３２Ａでは、自動車のグループ４７５、４７６、４７７、及び４７８が、それぞれ無線リンク４７１、４７２、４７３、及び４７４を介してモバイルネットワークのセルタワー４７０と通信している。

【０２９４】

セルタワー４７０は、車４７５、４７６、及び４７７にホストされた対応するＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜４７５ａ、４７６ａ、及び４７７ａに接続されたＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜４７０ａで有効になっているため、無線リンク４７１、４７２、及び４７３は、ＨｙｐｅｒＳｐｈｅｒｅのノード間パケットルーティングを採用しているため、きわめて安全である（クラウドでホストされたＨｙｐｅｒＮｏｄｅが動作するのと同じ）。この意味で、ＨｙｐｅｒＳｐｈｅｒｅのクラウドはエッジデバイスに至るまで網羅している。言い方を変えれば、ネットワークレイヤ３では、ｄ'ＳＤＮＰネットワークの実装では、ラストマイル通信のようなものは存在しない。なお、車４７８はＨｙｐｅｒＳｐｈｅｒｅゲートウェイをホストしていないので、無線リンク４７４は安全ではない。

【０２９５】

学術的な観点では、ＨｙｐｅｒＮｏｄｅゲートウェイは、セルラーネットワークがネットワークのバックボーンとして利用可能な場合でも、ピアツーピア（Ｐ２Ｐ）ネットワーク（自動車の場合は車両間（Ｖ２Ｖ）ネットワーク）として動作することが議論されている。このピア通信機能は、ＨｙｐｅｒＳｐｈｅｒｅポータル（ノード、ルータ、ゲートウェイ）が相互に信頼しているだけなので、ネットワークレイヤ３でも独自に可能である。この意味で、すべてのＨｙｐｅｒＳｐｈｅｒｅノードは、隣接するノードとの動的な自律型ＶＰＮとして動作するが、ＨｙｐｅｒＳｐｈｅｒｅのノード間トンネルは、｜Ａ｜ノードのディスパッチャ機能を介して作成される。つまり、ｄ'ＳＤＮＰクラウドでは、仮想トンネルはアプリケーションのレイヤ７（従来のＶＰＮの動作方法）ではなく、レイヤ３のトンネル上に形成される。また、通信を行う前にＶＰＮを確立する必要がある。ｄ'ＳＤＮＰクラウドのノードは、他のノードとの間で自律的かつ自動的にハイパーセキュアなリンクを形成する。

【０２９６】

図３２は、ネットワークインフラストラクチャが存在しない場合のｄ'ＳＤＮＰクラウドのＶ２Ｖネットワークへの自然な適応を示している。例えば、車４７６、４７７、及び４７８が山脈の麓を走行する場合、それらはセルラーネットワーク接続から遮断される可能性がある。しかし、車４７５がまだセルタワー４７０に接続できている場合、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜ノード４７５ａ、４７６ａ、及び４７７ａは、介在する車の｜ＨＧ｜ノードを介して、セルタワー４７０及びＨｙｐｅｒＳｐｈｅｒｅルータ４７０ａへの接続を維持するＶ２Ｖピアネットワークを自発的に招集する。その結果、車両からインフラストラクチャ（Ｖ２Ｉ）リンク４７１及びＶ２Ｖリンク４８０、４８１は、いずれもハイパーセキュアである。車両｜ＨＧ｜４７７からのデータがセルタワー｜ＨＲ｜ノード４７０ａに転送されたとしても、中間の車両｜ＨｙｐｅｒＳｐｈｅｒｅゲートウェイ４７５ａ及び４７６ａは、転送されているデータを検査することができない。ＨｙｐｅｒＳｐｈｅｒｅゲートウェイノードが存在しなければ、車両４７８はタワーの守備範囲を超えるとすべての接続を失う。

【０２９７】

図３２では、車４７５、４７６、及び４７７がすべてセルタワー４７０の範囲外で走行している。このような場合、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイは、自然発生的に完全に自立したＶ２Ｖネットワークに変化し、ハイパーセキュアなチャネル４８０及び４８１を介した接続を維持する。Ｖ２Ｖ通信は、特に悪天候時には、衝突を防止し、差し迫った危険を他の車に警告するために重要である。

【０２９８】
アドホックＶ２Ｖネットワークは、車両間の無線範囲への出入に応じてリソースの追加・削除を完全に自律的に行う。例えば、図３２Ｄで、｜ＨＧ｜ノード４８５ａの別の車両４８５が他の車両の近傍に進入している。ＨｙｐｅｒＳｐｈｅｒｅゲートウェイノード４７５ａと４７７ａは、｜ＨＧ｜ノード４８５ａに接続するためのハイパーセキュアリンク４８３と４８４を瞬時かつ自発的に追加する。図３２Ｅでは、車４７６が道路を離れたので、Ｖ２Ｖピアネットワークから除去されている。可能な限り最良のＱｏＳの接続性を維持するために、｜ＨＧ｜ノード４７５ａは、｜ＨＧ｜ノード４７７ａへのハイパーセキュアリンク４８６を自動的に確立する。
【０２９９】
ＨｙｐｅｒＳｐｈｅｒｅマルチバンド通信
【０３００】
ｄ'ＳＤＮＰクラウド通信の重要な原則のひとつは、メッシュネットワーク内の複数のパスにまたがってなされる断片化データ転送である。複数のサーバで構成される固定インフラストラクチャのクラウドでは、これらのパスはＨｙｐｅｒＮｏｄｅの様々な組み合わせを表現できるが、エッジデバイスへの接続では、複数のＰＨＹ接続を介してさまざまなパケットを送信することで、さらなる冗長性とセキュリティを実現することができる。
【０３０１】
そのような一実施形態は、図３３Ａに示すように、無線アクセスポイントの形で構成され、イーサネットＭＡＣアクセス５００とマルチバンドＷｉＦｉ無線機５０１との間のブリッジを形成する。このアクセスポイントは、３つの通信スタック５０２、５１３ａ、５１３ｂを組み合わせて、イーサネット５０１とマイクロ波無線機５１５ａ、５１５ｂとの間のルーティングを容易にする。ホストプラットフォームは、ドライバインターフェイス５０６を介してホストプロセッサ５０８に、ドライバインターフェイス５０５を介してローカルデータストレージ（不揮発性メモリ）に、ドライバインターフェイス５０３を介して８０２．３（イーサネット）通信スタック５０２のＰＨＹレイヤ１に、ドライバインターフェイス５１１ａを介して無線Ａの８０２．１１（ＷｉＦｉ）通信スタック５１３ａのＰＨＹレイヤ１に、そしてドライバインターフェイス５１１ｂを介して無線Ｂの８０２．１１（ＷｉＦｉ）通信スタック５１３ｂのＰＨＹレイヤ１に接続されたインターフェイス回線及び無線ホストカーネル（以下「カーネル」と称する）５０９で構成されている。
【０３０２】
イーサネット接続５０１から渡されたデータパケットは、通信スタック５０２によって解釈され、データリンクレイヤ２データ５０４を介してカーネル５０９に渡される。ｄ'ＳＤＮＰ権限ノードによって受信されたルーティング命令に従って、ＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜ノード５１０は、受信パケットを処理し、それを解析して個別のペイロードにする。これらのペイロードは次いで異なるＩＰアドレス及びＭＡＣアドレスを持つパケットにアセンブルされ、一方は、データリンクレイヤ接続５１２ａ及び５１４ａを介して無線機５１５ａに転送され、キャリア周波数ｆＡを有するアンテナ５１６ａを介してブロードキャストされる。
【０３０３】
もうひとつのペイロードは、データリンクレイヤ接続５１２ｂ及び５１４ｂを介して無線５１５ｂに転送され、キャリア周波数ｆＢでアンテナ５１６ｂを介してブロードキャストされる。上記のシーケンスでは、着信イーサネットパケットが複数の無線キャリア周波数に分割されて送信されることを説明しているが、全二重通信及びテレフォニーでは、このプロセスは双方向性である。例えば、一旦受信された複数のＷｉＦｉ無線信号は、処理され混合された後、分割され、共通のＭＡＣアドレスを共有するが、別々のＩＰアドレスでイーサネット５０１を通じて複数のパケットとして送信される。
【０３０４】
ＨｙｐｅｒＳｐｈｅｒｅ対応ＷｉＦｉルータ（以下、ＨｙＦｉルータと呼ぶ）では、独自の方法でデータパケットを混合し分割して複数のキャリア周波数を介して送受信するプ

ロセスを実行する。図３３Ｂはこの方法を例示した図であり、イーサネット有線５２２からＨｙＦｉルータ３６８に運ばれたデータパケットは、例えば２．４ＧＨｚチャネル５２１ａ、５ＧＨｚチャネル５２１ｂ、及び９００ＭＨｚチャネル５２１ｃからなるマルチＰＨＹマイクロ波無線リンクを介して、分割されて携帯電話３６０に送信される。パケットの構築は、｜ＨＲ｜ルータ５１０及び｜ＨＧ｜ゲートウェイ５２０からなるＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェアを使用して管理されている。以下の説明では、ＭＡＣアドレス及びＩＰアドレスについては、便宜上、略号Ｌ２はデータリンクレイヤ２、Ｌ３はネットワークレイヤ３を意味するものとする。本実施例では、２つの無線リンクと１つのイーサネット接続を示しているが、性能への影響を最小限に抑えつつ、無線ルータ及び有線ルータのチャネル数を増やしてもよい。

【０３０５】

イーサネットパケット５３０は、ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜（図示せず）をホストするサーバから、Ｌ２送信元アドレス５３０ｂ（値ＭＡＣ｜ＨＮ｜を有する）及びＬ３送信元アドレス５３０ｃ（値ＩＰ｛ＳＤＮＰ｜ＨＮ｜｝を有する）にルーティングされる。イーサネットパケット５３０は、Ｌ２宛先アドレス５３０ａ（値ＭＡＣ｜ＨＲ｜を有する）及びＬ３宛先アドレス５３０ｄ（値ＩＰ｛ＳＤＮＰ｜ＨＲ｜｝を有する）で、ルータノード｜ＨＲ｜５１０をホストするＨｙｐｅｒＳｐｈｅｒｅ　ＨｙＦｉルータ３６８にルーティングされる。ブランクフィールド５３０ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。イーサネットパケット５３０のペイロード５３０ｆは、ＳＤＮＰ１及びＳＤＮＰ２サブパケットの両方を含んでいる。明確化のために、用語ＳＤＮＰ｜ＨＮ｜はＨｙｐｅｒＮｏｄｅ｜ＨＮ｜のＳＤＮＰアドレスであり、一方、値ＩＰ｛ＳＤＮＰ｜ＨＮ｜｝はＨｙｐｅｒＮｏｄｅ｜ＨＮ｜をホストするデバイスの動的ＩＰアドレスであり、アドレスＳＤＮＰ｜ＨＮ｜に関連付けられている。

【０３０６】

ペイロード処理及びコンシールメント処理の後、ＷｉＦｉパケット５３１は、ＨｙｐｅｒＳｐｈｅｒｅ　ＨｙＦｉルータ３６８のホスティングルータノード｜ＨＲ｜５１０から、Ｌ２送信元アドレス５３１ｂ（チャネルＣ用の値ＭＡＣ｜ＨＲＣ｜を有する）及びＬ３送信元アドレス５３１ｃ（ＨＲ１が第１ＩＰアドレスである値ＩＰ｛ＳＤＮＰ｜ＨＲ１｜｝を有する）で、スマートフォン３６０のホスティングゲートウェイ｜ＨＧＣ｜５２０にルーティングされる。ＷｉＦｉパケット５３１は、Ｌ２宛先アドレス５３１ａ（チャネルＣ用の値ＭＡＣ　｜ＨＧＣ｜）とＬ３宛先アドレス５３０ｄ（値ＩＰ｛ＳＤＮＰ｜ＨＧ１｜｝）で、スマートフォン３６０のホスティングゲートウェイ｜ＨＧＣ｜５２０にルーティングされる。ブランクフィールド５３１ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。ＷｉＦｉパケット５３１のペイロード５３１ｆは、ＳＤＮＰ１及びＳＤＮＰ２サブパケットの両方を含んでいる。

【０３０７】

ペイロード処理及びコンシールメント処理の後、ＷｉＦｉパケット５３２は、ＨｙｐｅｒＳｐｈｅｒｅ　ＨｙＦｉルータ３６８のホスティングルータノード｜ＨＲ｜５１０から、Ｌ２ソースアドレス５３２ｂ（チャネルＡ用の値ＭＡＣ｜ＨＲＡ｜を有する）及びＬ３ソースアドレス５３２ｃ（ＨＲ２は第２ＩＰアドレスである値ＩＰ｛ＳＤＮＰ｜ＨＲ２｜｝を有する）でルーティングされる。ＷｉＦｉパケット５３２は、Ｌ２宛先アドレス５３２ａ（チャネルＡ用の値ＭＡＣ　｜ＨＧＡ｜を有する）とＬ３宛先アドレス５３２ｄ（値ＩＰ｛ＳＤＮＰ｜ＨＧ２｜｝を有する）で、スマートフォン３６０のホスティングゲートウェイ｜ＨＧＡ｜５２０にルーティングされる。ブランクフィールド５３２ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。ＷｉＦｉパケット５３１のペイロード５３２ｆは、ＳＤＮＰ２及びＳＤＮＰ２サブパケットの両方を含んでいる。

【０３０８】

ｄ'ＳＤＮＰのパケットルーティングの方法は、８０２．３（Ｇｂイーサネット）などの有線通信にも同様に適用される。図３４Ａは、複数のイーサネットＭＡＣアドレス５７５ａ、５７５ｂ、及び５７５ｃの間にブリッジを形成するＨｙｐｅｒＳｐｈｅｒｅ対応の有

線ルータ５７０を示している。ルータブリッジは、３つの通信スタック５７７ａ、５７７ｂ、及び５７７ｃを組み合わせており、イーサネット接続５７６ａ、５７６ｂ、及び５７６ｃ間のルーティングを容易にしている。ホストプラットフォームは、ホストプロセッサ５７４、ローカルデータストレージ（不揮発性メモリ）５７３、及び８０２．３（イーサネット）通信スタック５７９ａ、５７９ｂ、及び５７９ｃのＰＨＹ層１に接続されたインターフェイス回線及び無線ホストカーネル（以下、「カーネル」と言う）５７１で構成される。

【０３０９】

イーサネット接続のいずれかによって搬送されるデータパケット、例えば５７６ｂは、対応する通信スタック５７７ｂによって解釈され、Ｌ２データリンク５７８ｂを介してカーネル５７１に渡される。d'ＳＤＮＰ権限ノードによって受信されたルーティング命令に従って、ＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ｜ノード５７２は、受信パケットを処理し、それを解析して個別のペイロードにする。これらのペイロードは次に、異なるＩＰアドレス及びＭＡＣアドレス（任意）を有するパケットに組み立てられ、例えば、未使用のイーサネットチャネル５７６ａ及び５７６ｃを介して転送される。

【０３１０】

物理媒体は、銅ツイストペアケーブルから、赤外光の様々な波長のより一般的な光ファイバまで選択肢がある。プロトコル自体もまた、データレートが１００Ｍｂ／ｓから１０００Ｍｂ／ｓ（いわゆるＧｂイーサネット）まで、ケーブル長が５０ｋｍから数ｍまでと使用することができる。例えば、複数のイーサネットプロトコルは、一旦受信されると、処理され、混合され、分割され、別個のＩＰアドレス及び別個のＭＡＣアドレスでイーサネット接続５７６ａ～５７６ｃを介して複数パケットとして送信される。

【０３１１】

ＨｙｐｅｒＳｐｈｅｒｅ対応ＷｉＦｉルータ（以下、Ｅｔｈｙｒｎｅｔルータと呼ぶ）では、独自の方法でデータパケットを混合・分割し、複数のキャリア周波数にて送受信するプロセスを実行する。この断片化トランスポート手法では、図３４Ｂに例示されているように、イーサネット有線５５６によって搬送されたデータパケットは、Ｅｔｈｙｒｎｅｔクワッドチャネルルータ３６９によって受信され、分割された後、新しいペイロードに再結合され、複数のハイパーセキュアチャネルを介してルータ｜ＨＲ１｜により転送される。この有線チャネルは、１００ＢＡＳＥ－ＫＸ（銅線）で構成されるチャネル５５５ａ、２２０ｍの光ファイバに限定される１０００ＢＡＳＥ－ＳＸからなるチャネル５５５ｂ、そして１０ｋｍまでのファイバ通信をサポートできるチャネル５５５ｃの１００００ＢＡＳＥ－ＢＸ１０を含んでいてもよい。

【０３１２】

Ｅｔｈｙｒｎｅｔパケットの宛先は、ＨｙｐｅｒＳｐｈｅｒｅの｜Ａ｜権限ノードのディスパッチャ機能によって決定されるパケットルーティングに依存している。例としては、パーソナルコンピュータ５５２がホストする｜ＨＧ｜ゲートウェイ５５１ａ、サーバ５５３がホストする｜ＨＮ｜ＨｙｐｅｒＮｏｄｅ　５５１ｂ、高帯域幅ルータ５５４がホストする｜ＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ２｜などが挙げられる。パケットの構築は、｜ＨＲ１］ルータ５５０、｜ＨＧ｜ゲートウェイ５５１ａ、｜ＨＮ２｜ＨｙｐｅｒＮｏｄｅ　５５１ｂ、または｜ＨＲ２］ルータ５５１ｃで構成されるＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェアを使用して管理される。前出のＷｉＦｉの例と同様、簡略化のためにＬ２とはデータリンクレイヤ２、Ｌ３とはネットワークレイヤ３を意味するものとする。この例では、イーサネットの有線接続を３つ示しているが、ルータのチャンネル数を増やしても、機器の性能にはほとんど影響はない。

【０３１３】

もう一度図３４Ｂに戻ると、着信イーサネットパケット５６０は、Ｌ２ソースアドレス５６０ｂ（値ＭＡＣ｜ＨＮ１｜を有する）及びＬ３ソースアドレス５６０ｃ（値ＩＰ｛ＳＤＮＰ｜ＨＮ１｜｝を有する）において、ＨｙｐｅｒＮｏｄｅ｜ＨＮ１｜（図示せず）をホストするサーバからルーティングされている。イーサネットパケット５６０は、Ｌ２宛

先アドレス５６０ａ（値はＭＡＣ｜ＨＲ１｜）及びＬ３宛先アドレス５６０ｄ（値はＩＰ｛ＳＤＮＰ｜ＨＲ１｜｝）でルータノード｜ＨＲ１｜５５０をホストするＨｙｐｅｒＳｐｈｅｒｅ Ｅｔｈｙｒｎｅｔルータ３６９にルーティングされる。ブランクフィールド５６０ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。イーサネットパケット５６０のペイロード５６０ｆには、サブパケットＳＤＮＰ１とＳＤＮＰ２の両方が含まれている。

【０３１４】

ペイロード処理及びコンシールメント処理の後、ＷｉＦｉパケット５６１は、ＨｙｐｅｒＳｐｈｅｒｅ ＨｙＦｉルータ３６９のホスティングルータノード｜ＨＲ１｜５５０から、Ｌ２送信元アドレス５６１ｂ（値ＭＡＣ｜ＨＲ１｜を有する）及びＬ３送信元アドレス５３１ｃ（ＨＲ１が第１のＩＰアドレスである値ＩＰ｛ＳＤＮＰ｜ＨＲ１｜｝を有する）で、スマートフォン３６０のホスティングゲートウェイ｜ＨＧＣ｜５２０にルーティングされる。Ｅｔｈｙｒｎｅｔパケット５６１は、Ｌ２宛先アドレス５６０ａ（値はＭＡＣ｜ＨＲ１｜）及びＬ３宛先アドレス５６１ｄ（値はＩＰ｛ＳＤＮＰ｜ＨＲ１｜｝）でルータノード｜ＨＲ１｜５５１ｃをホストするＨｙｐｅｒＳｐｈｅｒｅ Ｅｔｈｙｒｎｅｔルータ５５４にルーティングされる。空のフィールド５１１ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。ＷｉＦｉパケット５６１のペイロード５６１ｆには、ＳＤＮＰ１及びＳＤＮＰ２サブパケットの両方が含まれている。

【０３１５】

ペイロード処理及びコンシールメント処理の後、ＷｉＦｉパケット５６２は、ＨｙｐｅｒＳｐｈｅｒｅ ＨｙＦｉルータ３６９のホスティングルータノード｜ＨＲ１｜５５０から、Ｌ２送信元アドレス５６２ｂ（値ＭＡＣ｜ＨＲ１｜を有する）及びＬ３送信元アドレス５６１ｃ（ＨＲ１が第１のＩＰアドレスである値ＩＰ｛ＳＤＮＰ｜ＨＲ１｜｝を有する）で、スマートフォン３６０のホスティングゲートウェイ｜ＨＧＣ｜５２０にルーティングされる。ＷｉＦｉパケット５６２は、Ｌ２宛先アドレス５３２ａ（チャネルＡ用の値ＭＡＣ｜ＨＧ｜を有する）とＬ３宛先アドレス５６２ｄ（値ＩＰ｛ＳＤＮＰ｜ＨＧ２｜｝を有する）で、スマートフォン５５２のホスティングゲートウェイ ｜ＨＧ｜５５１ａにルーティングされる。空のフィールド５６２ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。ＷｉＦｉパケット５６２のペイロード５６２ｆには、ＳＤＮＰ２及びＳＤＮＰ２サブパケットの両方が含まれている。

【０３１６】

また、ＨｙｐｅｒＳｐｈｅｒｅ通信の別の例として、家庭や企業を高速な有線接続に接続するために使用されるケーブルモデムがある。本明細書で既述のＨｙＦｉ ルータや Ｅｔｈｙｒｎｅｔルータと同様、ケーブルやファイバを介したＤＯＣＳＩＳ－３を使用したコンテンツ配信は、パケット交換技術を使用して全二重動作が可能な双方向性を備えている。ケーブル事業者は、ＤＯＣＳＩＳ－３と呼ばれる特殊なプロトコルを使用して、ファイバケーブルと同軸ケーブルのハイブリッドネットワーク上でコンテンツ配信と高帯域幅通信トラフィックを管理している。これは「Ｄａｔａ Ｏｖｅｒ Ｃａｂｌｅ Ｓｅｒｖｉｃｅ Ｉｎｔｅｒｆａｃｅ Ｓｐｅｃｉｆｉｃａｔｉｏｎ」の頭文字で構成された略語で、ユニキャストＨＤＴＶ、サブスクリプションＨＤＴＶ（放送テレビコンテンツを含む）、ペイパービューＨＤＴＶ、ウェブストリーミングサービスを含むインターネット、オーディオ、ビデオ（メディア）コンテンツオーディオのダイナミックな組み合わせをサポートするよう設計された国際電気通信規格である。ＣａｂｌｅＬａｂｓは２０１７年１０月、１０Ｇｂ／ｓの対称速度をサポートする「ＤＯＣＳＩＳ－３．１ Ｆｕｌｌ Ｄｕｐｌｅｘ」（略してＤ３．１－ＦＤ）仕様を発表した。

【０３１７】

ケーブルテレビは衰退の一途をたどっているビジネスを象徴しているが、インターネットビデオストリーミングサービスの登場により、ケーブルシステムが提供する高帯域幅に対する新たな需要が生まれている。この傾向は、グローバルなインターネット・クラウド・アズ・ア・サービス（ＣａａＳ）プロバイダとケーブルネットワーク事業者の間で新た

な提携を余儀なくされており、家庭や商業者へのラストマイル・パフォーマンスを向上させている。例えば、Ｇｏｏｇｌｅ－Ｃｏｍｃａｓｔは、スターバックス（登録商標）のようなグローバルな主要顧客企業向けに大規模なケーブルネットワークを展開しており、スターバックス（登録商標）は自社の音楽チャンネルを全拠点にブロードキャストしている。多くのインターネットトラフィックは、安全ではない公衆ＷｉＦｉを使用しているコーヒーショップチェーンのクライアントから来ているため、サイバー犯罪の可能性は非常に大きい。このように、ケーブルネットワーク上のプライバシーとセキュリティ保護は、現代のネットワーキングにおいて重要な考慮事項なのである。

【０３１８】

ＰＨＹレイヤで情報を送信するために電気信号またはマイクロ波信号の代わりに光を採用することで、特に光ファイバは、他の形態の通信と比較して優れた帯域幅をもたらす。ケーブル分配システムにおけるＤＯＣＳＩＳ３のＯＳＩ通信スタックを図３５Ａに示す。この図では、仕様に従ってレイヤ１のＰＨＹ接続及びレイヤ２のデータリンクが説明されている。ＤＯＣＳＩＳ仕様は、ネットワークレイヤ３データの使用に関しては不可知である。

【０３１９】

全二重高帯域幅通信と組み合わせたコンテンツ配信及びビデオストリーミングを提供するために、ケーブル配信サービスでは、ケーブルモデム（ＣＭ）６０１またはセットトップボックス（ＳＴＢ）６０２からなる複数のクライアント装置と組み合わせたケーブルモデム終端装置（ＣＭＴＳ）６２１と呼ばれるマルチチャンネルアップストリーム装置をクライアントの家庭や企業に配置する方法を採用している。具体的には、ケーブルモデム終端装置ＣＭＴＳ６２１及びそれに対応する通信スタック６２０は、有線６２３を介してクラウドサーバ６２５及びインターネットクラウド６２５に接続されたレイヤ１のＰＨＹネットワークインターフェイス６２７を使用するか、または代替的にビデオヘッドエンド、ＩＰＴＶ、またはＶｏＩＰシステム（図示せず）を含む様々なメディア及びコンテンツソースに接続されたレイヤ１のＰＨＹネットワークインターフェイス６２７を使用している。ネットワークインターフェイス６２５とデータリンクレイヤ６２８の組み合わせには、ＣＭＴＳ　６２１のデバイスインターフェイス通信スタックが含まれている。

【０３２０】

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６２９を介して、具体的にはリンクレベル制御ＬＬＣ　６６９に引き渡される。リンクレベル制御ＬＬＣ　６６９は、ＩＥＥＥ仕様８０２．２にしたが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６３０によって変更されて限定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。次いで、データパケットは、ケーブルモデム及びセットトップボックスに分配するためのケーブルＭＡＣ６３１アドレスを含めるよう、ＤＯＣＳＩＳ３に従ってフォーマットされる。

【０３２１】

次に、レイヤ１　ＰＨＹケーブルインターフェイス６３２は、同軸ケーブル６１９ｂまたは光ファイバ６１９ａのいずれかからなるケーブル分配ネットワーク６１９を介して、ケーブルモデムＣＭ６０１またはセットトップボックスＳＴＢ６０２の通信スタック６００内の対応するレイヤ１　ＰＨＹケーブルインターフェイス６１８にデータフレームを送信する。

【０３２２】

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６１７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６１６に渡し、最終的にハードウェア非依存のリンクレイヤ制御ＬＬＣ　６２２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６１３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の仕様にしたがってデバイス独立リンクレイヤ制御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６１３またはＷｉＦｉ　８０２．１１　ＭＡＣブロック６１２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、８０２．１１　ＭＡＣブロック６１２からＷｉＦｉ　ＰＨＹレイヤ１無線インターフェイス６１０に渡され、ＷｉＦｉ無線６０５で送信される。有線接続の場合、データパケットは、スマートＨＤＴＶ６０４ａまたはデスクトップ６０４ｂに接続するために、ＨＳＤ＆ＩＰＴＶＭＡＣブロック６１３からイーサネットまたはＨＤＭＩ（登録商標）インターフェイスブロック６１１に渡される。

【０３２３】

ネットワークインターフェイス６２７、イーサネット６１１、及びＷｉＦｉ　６１０への外部接続のため、ケーブルネットワークはＴＣＰ／ＩＰベースのネットワークと同じセキュリティ脆弱性に悩まされることになる。その結果、ＨｙｐｅｒＳｐｈｅｒｅルータソフトウェアをインストールすることで、ＤＯＣＳＩＳ３プロトコルを変更することなく、ハイパーセキュアな通信が可能になる。具体的には、ＣＭＴＳ６２１のネットワークポートを確保するために、通信スタック６２０にＨｙｐｅｒＳｐｈｅｒｅルータソフトウェア｜ＨＲ１｜６２３がインストールされている。同様に、イーサネット６１１　及びＷｉＦｉ６１０　のポートセキュリティを確保するため、ＨｙｐｅｒＳｐｈｅｒｅルータソフトウェア｜ＨＲ２｜６０３ａ及び｜ＨＲ３｜が、ＣＭ　６０１　またはＳＴＢ　６０２のいずれかにインストールされている。結果として得られるＨｙｐｅｒＳｐｈｅｒｅを有効にしたハイパーセキュアケーブルネットワークは、図３５Ｂに示されるとおり、ＣＭＴＳ　６２１によってホストされたＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ１｜６２３、ＳＴＢ　６０２によってホストされたルータ｜ＨＲ２｜６０３ａ、及びＣＭ　６０１によってホストされたルータ｜ＨＲ３｜６０３ｂで構成されている。

【０３２４】

ｄ'ＳＤＮＰクラウド内の他のＨｙｐｅｒＮｏｄｅｓ（図示せず）との通信は、ＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ１｜６２３が、イーサネット６３４を介してＨｙｐｅｒＳｐｈｅｒｅとのセキュアな有線通信を容易にする。ケーブルモデム６０１とノートブック３６３との間のＷｉＦｉ通信リンク６４２は、図に示すように、対応するホストデバイスにインストールされたソフトウェアＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ３｜６０３ｂ及びＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ３｜６３９によって確保される。同様にインストールされたＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェアは、セットトップボックス６０２にホストされているルータ｜ＨＲ２｜６０３ａとノートブック３６３にホストされているＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ２｜６４０との間のイーサネットリンク６４２、及びＩＰＴＶ　３６４ａにホストされている｜ＨＲ２｜とゲートウェイ｜ＨＧ２｜６３８との間のイーサネットリンク６４１ｂなど、その他のラストリンク接続を保護する。ただし、ＨＤＴＶ　３６４ｂへのＨＤＭＩ（登録商標）接続６４１ａは、クライアントデバイスがＨｙｐｅｒＳｐｈｅｒｅポータルソフトウェアを欠いているため、安全ではない。

【０３２５】

本発明のもうひとつの卓越した実施形態は、トレリス符号化６４５と呼ばれるケーブル固有のデータ変調方式が関係している、ファイバリンク６１９ｙを介したＣＭＴＳ６２１とクライアントデバイスＣＭ６０１との間、及びファイバ接続６１９ｘを介したＳＴＢ６０２との間のハイパーセキュアな通信に関するものである。トレリス符号化６４５を採用するためにｄ'ＳＤＮＰルーティングを適応させることにより、共通のＰＨＹレイヤ（光ファイバ）を共有するケーブル分配内で、異なるＩＰアドレスとＭＡＣアドレスを送ることができる。ＷｉＦｉで使用されるＯＦＤＭ、または４Ｇ／ＬＴＥ及び５Ｇ通信で使用されるＯＦＤＭＡと同様に、ＤＯＣＳＩＳ３通信は、情報を符号化して送信する電磁放射のマイクロ波または光スペクトルの中で、直交する複数の周波数、すなわち重複しない周波数を採用している。トレリス符号化方式では、各チャンネルに具体的に専用のコンテンツを

割り当てるのではなく、需要に応じて利用可能なすべての周波数チャンネルに動的に映像と高速データを割り当てる。

【０３２６】

図３５Ｃに示すとおり、トレリス符号化６４５では、ファイバ帯域幅が変調キャリアチャネル（Ａ～Ｇとして示されている）と順次固定間隔のタイムスロットに分割される。例えば、チャネルＢ及びＣ６４７ａ上で搬送されたオンデマンド映像は、タイムスロット２０で単一のチャネルＤ６４７ｂに再割り当てされる。トレリス符号化の動的機能は、別個のＩＰアドレス及びパケット固有のセキュリティ規定を有するｄ'ＳＤＮＰデータグラムを伝送するよう適合させることができる。例えば、チャネルＡ　６４６ａで伝送されたＳＤＮＰ｜ＨＲ３｜データは、タイムスロット２２でチャネルＢ　６４６ｂに変化する。同時に、全く異なるセキュリティクレデンシャル情報及びアルゴリズムを使用して、ＳＤＰ｜ＨＲ２｜データ６４８ａは、断片化されたデータ転送を使用して、チャネルＦ及びＧにわたって分割されて伝送される。タイムスロット２５において、キャリアは断片化されたデータ６４８ｂ及び６４８ｃを含むチャネルＥ及びＧに再割り当てされる。そのため、複数のＷｉＦｉキャリア周波数またはイーサネットケーブルを介してｄ'ＳＤＮＰパケットを送信するのと同様の方法で、ＤＯＣＳＩＳ３はハイパーセキュアな通信のためのｄ'ＳＤＮＰトランスポートに対応している。

【０３２７】

データパケットを混合及び分割し、複数のチャネルで送受信する　ＨｙｐｅｒＳｐｈｅｒｅプロセスは、携帯電話及びワイヤレスネットワークに適用される。この断片化トランスポート手法は図３６Ａにて例を使って次のように説明されている。イーサネット有線６７４によって伝送されたデータパケットは、モバイルネットワークセルタワー４７０によって受信され、その後、ＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ１｜６７０によって処理され、１．９ＧＨｚの無線キャリア６７１ａ、６００ＭＨｚの無線キャリア６７１ｂ、及び２．５ＧＨｚの無線キャリア６７１ｃを介したブロードキャストに使用される。キャリア６７１ａは、携帯電話タワー６７２ａがホストするＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ２｜に接続する。キャリア６７１ｂとキャリア６７１ｃは、両方とも携帯電話タワー６７３ｂによってホストされているＨｙｐｅｒＳｐｈｅｒｅルータ｜Ｈ３２｜にルーティングされる。

【０３２８】

セルラールーティングは、ＰＨＹレイヤ１及びリンクレイヤ２データと移動体キャリアのネットワークによって定義される変調方式（２Ｇ、３Ｇ／ＬＴＥ、ＨＳＤＰＡ、ＨＳＵＰＡ、５Ｇ）及びキャリア周波数を採用するが、任意の移動体ネットワークパケットの最終的な宛先は、ＨｙｐｅｒＳｐｈｅｒｅの｜Ａ｜権限ノードのディスパッチャ機能によって決定されるパケットルーティングに依存している。もう一度図３６に戻ると、着信イーサネットパケット６８０は、Ｌ２送信元アドレス６８０ｂ（値ＭＡＣ｜ＨＲ１｜）及びＬ３送信元アドレス６８０ｃ（値ＩＰ｛ＳＤＮＰ｜ＨＮＲ｜｝）において、ＨｙｐｅｒＮｏｄｅ｜ＨＮ｜（図示せず）をホストするサーバからルーティングされている。イーサネットパケット６８０は、Ｌ２宛先アドレス６８０ａ（値ＭＡＣ｜ＨＲ１｜）及びＬ３宛先アドレス６８０ｄ（値ＩＰ｛ＳＤＮＰ｜ＨＲ１｜｝）でルータノード｜ＨＲ１｜６７０をホストするＨｙｐｅｒＳｐｈｅｒｅ　Ｅｔｈｙｒｎｅｔルータ４７０にルーティングされる。ブランクフィールド６８０ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。イーサネットパケット６８０のペイロード６８０ｆには、サブパケットＳＤＮＰ１とＳＤＮＰ２の両方が含まれている。

【０３２９】

ペイロード処理及びコンシールメント処理の後、パケット６８１は、携帯電話タワー４７０のホスティングルータノード｜ＨＲ１｜６７０から、Ｌ２送信元アドレス６８１ｂ（値ＭＡＣ｜ＨＲ１｜）及びＬ３送信元アドレス６８１ｃ（値ＩＰ｛ＳＤＮＰ｜ＨＲ１｜｝、ＨＲ１は最初のＩＰアドレス）でルーティングされる。モバイル５Ｇパケット６８１は、無線リンク６７１ｃを介して、Ｌ２宛先アドレス６８１ａ（値ＭＡＣ｜ＨＲ３｜）とＬ

３宛先アドレス６８１ｄ（値ＩＰ｛ＳＤＮＰ｜ＨＲ３｜｝）で、セルタワー６７２ｂホスティングルータ｜ＨＲ３｜６７３ｂにルーティングされる。空のフィールド６８１ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。ＷｉＦｉパケット６８１のペイロード６８１ｆには、ＳＤＮＰ１及びＳＤＮＰ２サブパケットの両方が含まれている。

【０３３０】

同様に、ペイロード処理及びコンシールメント処理の後、４Ｇ無線パケット６８１は、携帯電話タワー４７０のホスティングルータノード｜ＨＲ１｜６７０から、Ｌ２送信元アドレス６８１ｂ（値ＭＡＣ｜ＨＲ１｜）及びＬ３送信元アドレス６８１ｃ（値ＩＰ｛ＳＤＮＰ｜ＨＲ１｜｝、ＨＲ１は２番目のＩＰアドレス）でルーティングされる。モバイル４Ｇパケット８６２は、Ｌ２宛先アドレス６８２ａ（値ＭＡＣ｜ＨＲ２｜）及びＬ３宛先アドレス６８２ｄ（値ＩＰ｛ＳＤＮＰ｜ＨＲ２｜｝）でルータノード｜ＨＲ２｜６７３ａをホストする携帯タワー６７２ａにルーティングされる。空のフィールド６８２ｅは、分かりやすくするためにＬ４～Ｌ６データを空白のままにしてある。モバイル４Ｇパケット６８２のペイロード６８２ｆには、ＳＤＮＰ２サブパケットのみが含まれている。

【０３３１】

マルチＰＨＹモバイルネットワーク上での断片化データ転送は、タワーツータワー（Ｔ２Ｔ）通信及び大陸間ルーティングには有用であるが、同じ方法を今後登場する５Ｇ装備の携帯電話及びタブレットに適用することも可能である。この断片化トランスポート手法は図３６Ｂにて例を使って次のように説明されている。タブレット３６２及びＨｙｐｅｒＳｐｈｅｒｅゲートウェイ７００によって搬送されるデータパケットは、１．９ＧＨｚの無線キャリアチャネル７０１ａ、６００ＭＨｚの無線キャリアチャネル７０１ｂ、及び２．５ＧＨｚの無線キャリアチャネル７０１ｃを介してブロードキャストされる。キャリア６７１ａは、携帯電話タワー７０２ａがホストするＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ２｜に接続する。キャリア７０１ｂとキャリア７０２ｃは、両方とも携帯電話タワー７０２ｂによってホストされているＨｙｐｅｒＳｐｈｅｒｅルータ｜ＨＲ３｜にルーティングされる。

【０３３２】

図に示されているとおり、携帯電話３６２及びＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜７００からのモバイル５Ｇデータパケット７１０、７１１、７１２の伝送は、３つの異なるキャリア７０１ａ、７０１ｂ、及び７０１ｃをまたいで行われる。

【０３３３】

５Ｇパケット７１０を伝送するキャリア７０１ｂは、値ＭＡＣ｜ＨＧ１｜のＬＳ送信元アドレス７１０ｂからなり、ここでＨＧ１は携帯電話７００の６００ＭＨｚ帯を表す。このパケットのＬ２宛先７１０ａのアドレスは、ＨｙｐｅｒＳｐｈｅｒｅルータ７０３ｂによって割り当てられたＭＡＣ｜ＨＲ３｜である。Ｌ３送信元アドレス７１０ｃからＬ３宛先アドレス７１０ｄへのデータパケット７１０のネットワークルーティングは、ソースの動的ＩＰアドレスをＩＰ｛ＳＤＮＰ｜ＨＧ｜｝、宛先の動的ＩＰアドレスをＩＰ｛ＳＤＮＰ｜ＨＲ３｜｝として使用して行われる。

【０３３４】

５Ｇパケット７１２を伝送するキャリア７０１ａは、値ＭＡＣ｜ＨＧ３｜のＬＳ送信元アドレス７１２ｂで構成され、ここでＨＧ３は携帯電話７００の６００ＭＨｚ帯を表す。パケットのＬ２宛先７１２ａは、ＨｙｐｅｒＳｐｈｅｒｅルータ７０３ａによって割り当てられたアドレスであるＭＡＣ｜ＨＲ２｜である。Ｌ３送信元アドレス７１２ｃからＬ３宛先アドレス７１２ｄへのデータパケット７１２のネットワークルーティングは、送信元の動的ＩＰアドレスをＩＰ｛ＳＤＮＰ｜ＨＧ｜｝、宛先の動的ＩＰアドレスをＩＰ｛ＳＤＮＰ｜ＨＲ２｜｝として行われる。

【０３３５】

５Ｇパケット７１１を伝送するキャリア７０１ｃは、値ＭＡＣ｜ＨＧ２｜のＬＳ送信元アドレス７１１ｂからなり、ここでＨＧ２は携帯電話７００の２．５　ＧＨｚ帯を表す。

このパケットのＬ２宛先７１１ａのアドレスは、ＨｙｐｅｒＳｐｈｅｒｅルータ７０３ｂによって割り当てられたＭＡＣ｜ＨＲ４｜である。Ｌ３送信元アドレス７１１ｃからＬ３宛先アドレス７１１ｄへのデータパケット７１１ａのネットワークルーティングは、送信元のＳＤＮＰアドレス（動的ＩＰアドレスではなく）をＳＤＮＰ［ＨＧ］、宛先をＳＤＮＰ［ＨＲ３］として行われる。このように、ルーティングは必ずしもダイナミックＩＰアドレスに依存しない。

【０３３６】

ＨｙｐｅｒＳｐｈｅｒｅクラウド接続デバイス

【０３３７】

分散型ＳＤＮＰルーティングもまた、ＩｏＴデバイスのセキュリティを確保するために実装することができる。図３７Ａに示すとおり、ＩｏＴクラウド接続デバイス７８０は、ＷｉＦｉ無線７８０ｃと、ＩｏＴホストカーネル７８１、マイクロコントローラ７８４、ローカル不揮発性メモリ７８３、電源７９２、ロードドライバ７９３、８０２．１１ａｈ互換無線７８６、及び２つの通信スタック７８８ａ、７８８ｂを含むホストデバイス７８０ａから構成される。動作中、アンテナ７８５で受信した信号は復調されてデジタルデータ７８７に変換され、接続部７９０ａを介してＩｏＴカーネル７８１に渡される。データリンク情報７８９ａは、次にＨｙｐｅｒＮｏｄｅゲートウェイ７８２によって処理され、制御命令７８９ａは、通信スタック７８８ｂのデータリンク層に渡され、ＰＨＹデジタルデータ７９０ｂを制御信号７９１に変換する情報を解釈して、電源７９２によって給電された負荷ドライバ７９３を介して負荷を駆動するための制御信号７９１に変換される。

【０３３８】

図３７Ｂに示すとおり、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイ７８２は、ＩｏＴデバイス７８０の不正な制御、ＩｏＴ負荷７９０の制御、または低レベルの「ダム」ＩｏＴデバイスの侵入によるネットワークの不正侵害を防止する。ＨｙｐｅｒＳｐｈｅｒｅを制御プラットフォームとして使用することで、ＨｙｐｅｒＮｏｄｅｓ｜ＨＮ｜７９５は、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜７８２対応のＩｏＴデバイスにコマンド７９５ａとソフトウェアダウンロードを送信することができるが、ＨｙｐｅｒＮｏｄｅｓ｜ＨＧ｜７８２からローカルネットワークへのアップロードはデータ７９７のみに限定される。コマンド及び情報要求７９９は、不正アクセスを表しており、これはサンドボックス保護７９９によってブロックされる。

【０３３９】

ＨｙｐｅｒＳｐｈｅｒｅで保護されたＩｏＴネットワークの例示している図３７Ｃにおいて、ワイヤレスルータ３６８は、ＨｙｐｅｒＳｐｈｅｒｅルータソフトウェア｜ＨＲ１｜７５１によってＨｙＦｉが有効化されており、ネットワーク全体を不正侵入から保護している。スマート冷蔵庫３６６、ＩＰＴＶ　３６４ａ、サーモスタットまたはＨＶＡＣコントローラ　７５０ａ、セキュリティカメラ　７５０ｂ、ＩｏＴドアロック　７５０ｃ及び制御可能な照明　７５０ｄなどのＩｏＴデバイスは、それぞれＩｏＴ埋め込みＨｙｐｅｒＳｐｈｅｒｅゲートウェイＨＧ３　７５３ａ～ＨＧ８　７５３ｆによって保護され、保護ＨｙｐｅｒＳｐｈｅｒｅゲートウェイＨＧ２　７５２ｃ及びＨＧ１７５２ａを含むタブレット３６２またはパーソナルアシスタント７５１にインストールされたアプリケーションソフトウェアによって制御される。信頼されたＨｙＦｉゾーン外にあるＩｏＴデバイスの安全な制御は、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ９｜７５４をホストする有線接続のデスクトップ３６４を使用する方法で実現できる。または、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ９｜７５４を介して、セルタワー７０２ａを介してサーバ３７０がホストするＨｙＰｅｒＮｏｄｅ｜ＨＮ｜７５５を介してハイパーセキュアなネットワークを促進するＨｙｐｅｒＳｐｈｅｒｅゲートウェイ７５６を介して実現することも可能である。

【０３４０】

ＨｙｐｅｒＳｐｈｅｒｅ拡散型データクラウドストレージ

【０３４１】

図３８は、ネームサーバデータの冗長ファイル保存について図解している。例えば、ク

ライアントファイル８０１ａ、８０１ｂ、８０１ｃの解析ファイルは、タスクノード｜Ｔ１｜、｜Ｔ２｜、｜Ｔ３｜からなる複数のストレージサーバ８０２、８０３、８０３に書き込まれ、まとめてクライアントデータ８００の拡散クラウドストレージに格納する。このように、データ８０１ａからなる解析ファイル１は、｜Ｔ１｜と｜Ｔ３｜、及びその他（図示せず）に冗長的に格納され、データ８０１ｂからなる解析ファイル２は、｜Ｔ２｜と｜Ｔ３｜及びその他に冗長的に格納され、データ８０１ｃで構成される解析ファイル３は、｜Ｔ１｜と｜Ｔ３｜、及びその他に冗長的に格納されている。

【０３４２】

｜Ｔ１$_3$｜内へのファイル１とファイル３の格納、｜Ｔ２｜内へのファイル２とファイル３の格納、及び｜Ｔ３｜内へのファイル１とファイル２の格納により、それぞれファイルストレージアクセスリンクキー８０５、８０６、及び８０７が自動的に生成され、これらはそれぞれサーバ８０８及び８０９にホストされているクライアントＨｙｐｅｒＳｐｈｅｒｅゲートウェイデバイス｜ＨＧ１｜及び｜ＨＧ２$_7$｜、及びその他（図示せず）に冗長的に格納される。任意の｜Ｔ｜ストレージノードがオフラインになると、データは別のネームサーバノードにクローニングされる。一実施形態では、各｜Ｔ｜ノードは、現在オンラインになっているバックアップサーバをリストアップした動的ＨｙｐｅｒＣｏｎｔｒａｃｔを発行し、維持する。サーバがオフラインになると、ＨｙｐｅｒＣｏｎｔｒａｃｔは自動的にデータを別のサーバにクローニングし、その後、新しいバックアップＨｙｐｅｒＣｏｎｔｒａｃｔを発行し続ける。

【０３４３】

図３８Ｂに示すように、ＨｙｐｅｒＳｐｈｅｒｅに格納されたユーザのために格納・分解されたデータは、例えば、データの所有者がＨｙｐｅｒＳｐｈｅｒｅゲートウェイ｜ＨＧ｜８２０を使用して、ユーザ拡散データクラウド８１０への書き込み８１１及び読み取りアクセス８１２を促進する場合、または代替手段として、クラウドへの書き込み８１３及び読み取り８１４のアクセスを共同作業者のゲートウェイデバイス｜ＨＧ２｜８２１と共有する場合、またはゲートウェイデバイス｜ＨＧ３｜８２２を介してレビューアに読み取り８２３のアクセス権を提供する場合など、プライベートな使用のために保持することができる。

【０３４４】

ＨｙｐｅｒＳｐｈｅｒｅ分散コンピューティング

【０３４５】

ＨｙｐｅｒＳｐｈｅｒｅによるハイパーセキュアな通信クラウドは、d'ＳＤＮＰクラウド上での安全かつ迅速なデータ転送を促進するクラウドコンピューティングにも適している。図３９Ａに示すように、ゲートウェイ｜ＨＧ｜８４０を介してＨｙｐｅｒＳｐｈｅｒｅポータルを構成するサーバ８３１上にホストされたクラウドコンピューティングアプリケーションは、ＨｙｐｅｒＣｏｎｔｒａｃｔ　８５０によって、ジョブ記述８５１で定義された一連のタスク（タスク、サブルーチン、行列計算、ジョブ割り当てを含む）で構成されるコンピューティングジョブに関する指示を、数値シード８５２、暗号鍵８５３、及びステート８５４を含むセキュリティ関連情報とともに受け取る。ゲートウェイノード｜ＨＧ｜８４０は、次に、選択された多数のタスクノード８４２、８４３、８４４等にジョブを割り当てる。

【０３４６】

図３９Ｂに示すように、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイノード｜ＨＧ｜８４０は、その後、インストールされたＨｙｐｅｒＮｏｄｅｓがタスクノード｜Ｔ２｜８４２～｜Ｔ７｜８４７に変身するサーバ８３２～８３７との間で、安全なセッションリンクと通信チャネルを確立する。ジョブ命令及びセキュリティクレデンシャル情報はまた、ジョブ実行中にファイルをアップロード及びダウンロードするために、タスクノードが分散コンピューティング拡散データクラウド８５０にアクセスすることを可能にする。

【０３４７】

ＨｙｐｅｒＳｐｈｅｒｅ分散通信の概要

【０３４８】
パブリック－プライベートネットワーク
【０３４９】
ＨｙｐｅｒＳｐｈｅｒｅの独自の接続性は、インターネット上では不可能な相互運用性と分散型アプリケーションをサポートする単一の共通通信プラットフォームを使用して、上記のような電子的ビジネスプロセスを容易化する。ＴＣＰ／ＩＰ上で実行されるパブリックネットワーク上でホストされる通信やトランザクションとは異なり、ＨｙｐｅｒＳｐｈｅｒｅはインターネットとは独立して動作するが、グローバルでダイナミックなリアルタイムメッシュネットワークを使用してインターネットと共存する。d'ＳＤＮＰネットワークは動的で、需要の変化に応じて地域のリソースを自動的に拡張または縮小し、データパケットのルーティングが最短の伝搬遅延パスで行われることを保証する。このようにして、ＨｙｐｅｒＳｐｈｅｒｅのネットワーク通信は、音声通信やライブ映像のリアルタイム性能とＱｏＳ（サービス品質）の優秀性を維持している。ＨｙｐｅｒＳｐｈｅｒｅ通信では、単純な暗号化技術をはるかに超えた動的なネットワーク通信方式が使用されており、データパケットをさまざまに変化するルートで送信したり、常に変化する暗号化とセキュリティ方法で構成される匿名データパケットを使用し、アクセスや監視を防止する「ハイパーセキュア」なプロトコルを採用している。
【０３５０】
ＨｙｐｅｒＳｐｈｅｒｅは、これらの技術を音声、ビデオ、テキスト、ビデオ通信、分散コンピューティングタスク、そしてまたＨｙｐｅｒＳｐｈｅｒｅの金融取引にも同様に適用し、これによってネットワークトラフィックの「意味のある」監視を防止しながら、ユーザの身元を難読化し、データパケットの最終的な送信元と送信先をカモフラージュし、中間者（ＭｉＭ）攻撃を確実に阻止する。ＨｙｐｅｒＳｐｈｅｒｅのネットワークは、インターネットと並行して共存しており、携帯電話ネットワークやインターネットと物理層の接続を共有しているが、それ以外は完全に独立した並列システムとして動作する。
【０３５１】
ＨｙｐｅｒＳｐｈｅｒｅネットワークを物理的に実現するには、ＨｙｐｅｒＳｐｈｅｒｅノードポータルの異種クラウド、つまりＨｙｐｅｒＮｏｄｅｓ、ＨｙｐｅｒＳｐｈｅｒｅルータ、ＨｙｐｅｒＳｐｈｅｒｅゲートウェイからなるＨｙｐｅｒＳｐｈｅｒｅへの接続が必要とされる。これらのノードは、あらゆるコンピューティングデバイスや通信デバイスにダウンロードされたアプリケーションソフトウェアで構成されており、グローバルサーバネットワークから家庭用ＰＣ、スマートフォンからＩｏＴ電球まで、あらゆるサイズのデバイスに対応している。ＨｙｐｅｒＳｐｈｅｒｅのノード数は、ユーザの採用率に比例して自然に増加するため、導入のためのインフラストラクチャへの投資は不要で、カバレッジの拡大、機能の向上、パフォーマンスの向上のための資本支出も不要である。そのため、ＨｙｐｅｒＳｐｈｅｒｅのネットワークは、個人や企業であれば誰でもＨｙｐｅｒＮｏｄｅをダウンロードしてアクティブにすることで参加できるという意味ではパブリックであるが、すべてのデータ転送をプライベートなネットワークとしてルーティングしセキュリティを確保している。このように、パブリックなＨｙｐｅｒＳｐｈｅｒｅの中にプライベートクラウドが共存しているにもかかわらず、大人数のユーザが完全分散型のプライベートネットワークとしてプライベートな通信をやりとりすることができる。その意味で、ＨｙｐｅｒＳｐｈｅｒｅは逆説的に、「パブリックプライベート」ネットワークと称することもできる。
【０３５２】
さらに別の言い方をすれば、パブリックＨｙｐｅｒＳｐｈｅｒｅ内でアドホックの仮想プライベートネットワーク（ＶＰＮ）のように動作するが、電話をかけたりファイルを送信したりする前にＶＰＮを確立する手間が要らないプライベートなＨｙｐｅｒＳｐｈｅｒｅクラウドと説明することもできよう。公開ホスト型プライベートクラウドは、自己起動型ＶＰＮ、または自律型ＶＰＮと表現することができる。この同じ自己起動メカニズムは、アドホックなピアツーピアネットワークを構築に使用することができる。この場合、ク

ラウドから切り離されたＨｙｐｅｒＮｏｄｅは、たとえ近くにセルラーネットワークやＷｉＦｉネットワークが存在しなくても、接続先となるＨｙｐｅｒＮｏｄｅをホストするデバイスを自動的に見つけようとする。検出された各デバイスはクラウド接続が再確立されるまで、順番に他のＨｙｐｅｒＮｏｄｅホストデバイスを探索する。

【０３５３】

つまり、ＨｙｐｅｒＮｏｄｅは、ＨｙｐｅｒＳｐｈｅｒｅのネットワークを形成するものであって、ＨｙｐｅｒＮｏｄｅをホストする物理デバイスではない。１つのサーバや共通のハードウェア上に共存できるＨｙｐｅｒＮｏｄｅの数に制限はない。例えば、ＨｙｐｅｒＳｐｈｅｒｅは、特定のＡＷＳサーバ上で独自のＨｙｐｅｒＮｏｄｅを直接起動できるが、ＡＷＳサービスの通常のクライアントがＡＷＳクラウド上や同じサーバ上に独自のＨｙｐｅｒＮｏｄｅをインストールして起動することに何の制約もない（ただし、クライアントが独自のデータトラフィックをＡＷＳに支払っていなければならない）。商用クラウドでホスティングされているＨｙｐｅｒＮｏｄｅと、同じクラウドを利用しているクライアントは、それぞれ別個のデジタル署名と所有者を持っているため、ＨｙｐｅｒＳｐｈｅｒｅは、ＨｙｐｅｒＮｏｄｅを独立したリソースサプライヤとみなし、さらには競合他社とみなす。

【０３５４】

例えば、ＡＷＳクラウド・アズ・アサービス（ＣａａＳ）のクライアントが、ＡＷＳクラウドサービスを利用してＨｙｐｅｒＣｏｎｔｒａｃｔの事業をＡＷＳクラウドサービスと競合しているケースが考えられる。デジタル証明書であるＣＡ証明書によって一意に識別されたものとみなすため、２つのＨｙｐｅｒＮｏｄｅは競合する独立したベンダーとして表示されることになる。暗号経済学では、通常の商取引と同様に、競争が激化すれば自ずとコストを押し下げられ、資本効率が向上する。

【０３５５】

ステートレスメッシュルーティング

【０３５６】

ＨｙｐｅｒＮｏｄｅｓは、中央集権的な制御を一切行わない匿名のデータパケットを使用して、メッシュ化されたネットワーク上でＨｙｐｅｒＳｐｈｅｒｅを介してデータパケットをルーティングする。ディスパッチャベースの通信システムおよびプロトコルとして、ＨｙｐｅｒＮｏｄｅｓのジョブには、相互に関連しながらも独立して実行される３つの機能のうちの１つが含まれている。

・ネームサーバノードまたは｜ＮＳ｜ノードと呼ばれる、データの転送またはタスクの実行に選択されたデバイスとハイパーノードを識別する。

・データパケットのルーティングを決定し、タスクを実行するＨｙｐｅｒＮｏｄｅｓに指示を与えるとともに、タスクが完了したかどうかを確認する。

・データを転送したり、タスクを実行したりすることで、タスクノードまたは｜Ｔ｜ノードと呼ばれている（オリジナルのＳＤＮＰ特許ではメディアノードと呼ばれている）。

【０３５７】

本出願が一部継続出願となっているオリジナルのＳｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｎｅｔｗｏｒｋ　ａｎｄ　Ｐｒｏｔｏｃｏｌ（ＳＤＮＰ）特許出願に記載されているように、専用機能ＳＤＮＰノードを介した３チャンネル通信は、ＳＤＮＰネームサーバノードをホストするネームサーバまたはデバイス、ＳＤＮＰシグナリングサーバノードをホストするシグナリングサーバまたはデバイス、ＳＤＮＰメディアサーバノードをホストするメディアサーバまたはデバイス、およびＤＭＺサーバのオフライン機能をホストするＤＭＺサーバまたはデバイス、別名「エアギャップドコンピュータ」を利用している。これらの電子資産、つまり「リソース」を組み合わせることで、今日のネットワークでは他に類を見ないハイパーセキュアな通信、マルチレベルのセキュリティ、および優れたパフォーマンスを実現する。ＳＤＮＰ特許出願では、ネームサーバ機能、シグナルサーバ機能、メディアサーバ機能、共有秘密をサポートするＤＭＺサーバの４つの主要機能を特定のコンピュータでホストしている。通話のルーティング、コンテンツ、デバイスアドレスなどの情報を１台

のコンピュータがすべて把握しているわけではないため、パケット伝送は安全である。
【０３５８】
ネットワーク管理者は、ＳＤＮＰノードの動的なリアルタイム動作を傍受することはできないが、コンピュータに特定のタイプのＳＤＮＰノードがロードされ、実行コードの展開と割り当てにネットワーク管理者が責任を負うという事実は、ＳＤＮＰネットワークの展開が完全に分散化されていないことを意味している（ネットワークのメッシュルーティング操作は分散化されているが）。対照的に、ｄ'ＳＤＮＰを使用すると、ＨｙｐｅｒＳｐｈｅｒｅによるネットワークおよびＳＤＮＰプロトコルの実装は完全に分散化されているが、これはネットワーク管理者が特定のサーバでどのような機能がホストされているかを常に把握できないことを意味している。
【０３５９】
この完全に分散化された機能を実現するために、ＨｙｐｅｒＳｐｈｅｒｅは、機能専用のＳＤＮＰノードを、新たに公開されたメタモルフィックＨｙｐｅｒＮｏｄｅに置き換えている。メタモルフィックＨｙｐｅｒＮｏｄｅは、前述のＳＤＮＰ機能であるネームサーバ、シグナルサーバ、メディア（タスク）サーバの機能のいずれか１つを実行することができるが、特定の会話ではこれらの機能のうち１つしか実行できない。例えば、メタモルフィックＨｙｐｅｒＮｏｄｅは、ある会話ではタスクノードサービスを実行し、別の呼び出しではオーソリティノード（シグナルサーバ）として動作し、別のトランザクションではネームサーバ｜ＮＳ｜機能として機能することができるが、同じ呼び出しやセッションでタスク、ネームサーバ、オーソリティノードのうち２つ以上の機能を実行することはできない。論理的には、この機能は○で象徴される「排他的なＯＲ'関数」と考えることができる。数学的には、メタモルフィックなＨｙｐｅｒＮｏｄｅ関数｜ＨＮ｜は、「１つまたは複数ではないが別のもの」からなる機能ステートを意味しているか、または
【０３６０】
【数３】

$$|MHN| = (|NS| \oplus |A| \oplus |T|)$$

【０３６１】
のように、「１つまたは複数ではないが別のもの」からなる機能ステートを意味している。ＳＦの格言から採用された「メタモルフ」という用語は、何か別のものに変化する能力、すなわちモーフィングを意味している。
【０３６２】
この意味では、呼び出しやトランザクションが開始されると、メタモルフィックなＨｙｐｅｒＮｏｄｅは３つの機能のうちの１つとして機能するように選択される（｜ＮＳ｜，｜Ａ｜，｜Ｔ｜ＨｙｐｅｒＮｏｄｅ）。３つの機能のうちの１つを実行するように選択された場合、同じジョブ内で他の２つの機能を実行することができないように自動的に除外される。このようにして、単一のＨｙｐｅｒＮｏｄｅに情報が集中することはない。一実施形態では、メタモルフィックなＨｙｐｅｒＮｏｄｅのジョブ選択は、ＨｙｐｅｒＳｐｈｅｒｅ　Ｍａｒｋｅｔｐｌａｃｅと呼ばれる分散型ＡＩベース環境でのＨｙｐｅｒＣｏｎｔｒａｃｔネゴシエーション中に行われ、その際にＨｙｐｅｒＮｏｄｅがネームサーバ、オーソリティノード、タスクノードとして機能する資格があるかどうかが決定される。この選択プロセスでは、実際に必要とされる数よりも多くのＨｙｐｅｒＮｏｄｅが選択される。これらの余分な「バックアップ」ＨｙｐｅｒＮｏｄｅｓは、選択されたＨｙｐｅｒＮｏｄｅがオフラインになった場合や、割り当てられた役割を果たせなくなった場合に備えて予備として保持される。
【０３６３】
与えられた役割に選択されると、ＨｙｐｅｒＮｏｄｅは、ＨｙｐｅｒＳｐｈｅｒｅの分散データストレージに保存されているデータにアクセスして、割り当てられたタスクを実

行するために必要な情報を取得する。集約されたデータストレージ層は、ＤＭＺサーバのように動作し、格納されているデータをインターネットから直接呼び出したり、読み取ったりすることはできない。ＨｙｐｅｒＮｏｄｅだけが、データを分解されたデータストレージ層からデータを取り出すことができる。ＨｙｐｅｒＮｏｄｅが特定のタイプのＨｙｐｅｒＮｏｄｅに設計変更される際、ＨｙｐｅｒＣｏｎｔｒａｃｔはＨｙｐｅｒＮｏｄｅに、分解されたデータ保存層から関連情報を抽出するために必要なコードを提供する。例えば、｜ＮＳ｜ＨｙｐｅｒＮｏｄｅはルーティングを行うために必要なノードリストにアクセスする。｜Ｔ｜ＨｙｐｅｒＮｏｄｅは必要なステートベースの隠蔽アルゴリズムを抽出し、｜Ａ｜ＨｙｐｅｒＮｏｄｅは伝播遅延にアクセスする。比喩的に言えば、ＨｙｐｅｒＮｏｄｅのメタモルフォーゼのプロセスは、ヒトの幹細胞の生物学的分化に似ている。幹細胞の細胞学的な分化は、分化を開始するためのテンプレートとして使用される環境に基づいている。同様に、メタモルフィックなＨｙｐｅｒＮｏｄｅは、ＨｙｐｅｒＣｏｎｔｒａｃｔから受け取ったテンプレートと、分解されたデータ記憶層からアクセスした情報に基づいて分化する。他のＨｙｐｅｒＮｏｄｅはタスクを実行するためではなく、ブロックチェーンのオブザーバーとして機能することで取引を確認するために使用されている。

【０３６４】

メタモルフィックＨｙｐｅｒＮｏｄｅのもう一つの重要な特徴は、「ステートレス」な動作である。タスクを完了した直後、ＨｙｐｅｒＮｏｄｅは受け取った情報や指示をすべて忘れ、瞬間的な記憶喪失を経験し、自動的に未分化なメタモルフィックＨｙｐｅｒＮｏｄｅに戻る。

【０３６５】

マスター暗号化キーなし

【０３６６】

ＨｙｐｅｒＳｐｈｅｒｅは、分散制御されたメッシュ型ネットワークで構成されているため、隠蔽メカニズムの実行は、マスター暗号化キーを使用してローカルに行われる。そのため、各｜Ｔ｜ＨｙｐｅｒＮｏｄｅは、次の予想される受信データパケットと次の送信データパケットに関連してのみ、知る必要があるベースで復号化キーと暗号化キーを受信する。言い換えれば、暗号化と隠蔽はホップバイホップで行われ、ネットワークトラフィックやその内容を解読するためのマスター復号鍵は存在しない。このアプリケーションで後述する動的有向非周期グラフ（ＤｙＤＡＧ）として動作するパケットルーティングでは、ルートやセキュリティクレデンシャル情報を変更するたびに、ＨｙｐｅｒＮｏｄｅのステートが繰り返されることはない。万が一、１つのデータパケットが同じノードを２回通過したとしても、ノードのステートとセキュリティクレデンシャル情報は変更されている。この機能は、ネットワークパケットを共通のサーバに流用しようとすると、コンテンツが読めなくなることを意味している。

【０３６７】

個人、グループ、企業は、ＨｙｐｅｒＳｐｈｅｒｅ、そのネットワーク、およびその運営を所有または管理していない。その代わりに、ＨｙｐｅｒＳｐｈｅｒｅは、企業、民間、研究機関のリソースを集約した非営利の分散型組織として機能している。固定の運営コストがほぼゼロの参加メンバーによる自律的なネットワークを構成しており、商人やサービスプロバイダは、必要に応じてリソースプロバイダと契約して支払いを行うが、ＨｙｐｅｒＳｐｈｅｒｅ　ＦｏｕｎｄａｔｉｏｎはＨｙｐｅｒＳｐｈｅｒｉｃの取引には一切関与しない。

【０３６８】

このようにして、ＨｙｐｅｒＳｐｈｅｒｅのネットワークは、リソースプロバイダで構成されている。これは、所有者のために収入を得るデバイスの異種コミュニティであり、所有者とＨｙｐｅｒＳｐｈｅｒｅのユーザベースのプライバシー保護に相互に関心を持っている。分散型アプリケーションと混同されないように、完全分散型ネットワークでは、パケットルーティングやネットワークセキュリティは、中央の権限を持たずに動的に実行される。その代わりに、トラフィック管理、パケット隠蔽アルゴリズムおよび方法、セキ

ュリティクレデンシャル情報および暗号鍵の発行などのタスクを動的にノード間で共有している。実際、ネットワークの暗号化とパケット隠蔽はステートベースであるため、マスターキーは一切存在しない。その代わり、動的なセキュリティは、データパケットがＨｙｐｅｒＳｐｈｅｒｉｃクラウドを通過する際に、ホップバイホップで動的に発生する「ステートベース」のものである。

【０３６９】

Ｃ．ＨｙｐｅｒＳｐｈｅｒｅのアイデンティティとプライバシーに関する規定

【０３７０】

個人情報保護

【０３７１】

データパケットは匿名でネットワークを通過するが、ＨｙｐｅｒＮｏｄｅは登録ユーザを代表しており、ＨｙｐｅｒＮｏｄｅがネットワークに参加するたびに、その個人または企業のアイデンティティが検証され認証される。金融取引のトレーサビリティを容易にすることで、ＨｙｐｅｒＮｏｄｅユーザの専門的なＩＤ登録は、犯罪者がＨｙｐｅｒＳｐｈｅｒｅを不正に使用して犯罪、マネーロンダリング、人身売買、恐喝、テロリズムに関与することを抑制する。ＨｙｐｅｒＳｐｈｅｒｅは、「アイデンティティが責任を喚起する」というポリシーを採用することで、インターネットの匿名性の問題を回避し、通信内容が非公開のままであっても、ユーザのアイデンティティが金融取引まで追跡できることを保証することで、「公衆電話」という比喩的な問題を克服している。ユーザ登録は各ＨｙｐｅｒＮｏｄｅを識別するが、ステートレスなネットワーク運用は、ネットワークオペレータでさえネットワークトラフィックやパケットの内容を監視することができないため、個人やビジネスのプライバシーを保証する。

【０３７２】

ＨｙｐｅｒＳｐｈｅｒｅにおけるアイデンティティは、デジタルで検証されたデジタル証明書、つまり「署名された」デジタルＣＡ証明書で構成されるデジタル証明書信頼チェーンを使用して確認される。このようなシステムで生成される「ネットワークネイティブ」なＣＡ証明書は、ＨｙｐｅｒＳｐｈｅｒｅ独自のものである。このＣＡ証明書は、デバイス、ＨｙｐｅｒＮｏｄｅｓ、暗号通貨ウォレット、ソフトウェアのインストール、永久ブロックチェーン取引（資産の借方と借方の記録）の確認と認証など、ＨｙｐｅｒＳｐｈｅｒｅでは数え切れないほどの方法で使用されている。

【０３７３】

ネットワークネイティブ証明書局

【０３７４】

ＨｙｐｅｒＳｐｈｅｒｅは、ユーザとそのデバイスのためにＩＤ－トラストチェーンを生成する際に、独自のネットワークネイティブ証明書局として機能する。アカウントの設定時には、ＨｙｐｅｒＳｐｈｅｒｅは、まず最初に、検証済みの「真のアイデンティティ」の所有者として、または偽名を使用して、親の「アイデンティティ」証明書を確立する。銀行取引、資産管理、法律上およびビジネス上の取引の目的では、ユーザの真の身元は、Ｋｎｏｗ－ｙｏｕｒ－ｃｌｉｅｎｔ　ａｎｔｉ－ｍｏｎｅｙ－ｌａｕｎｄｅｒｉｎｇ（ＫＹＣ／ＡＭＬ）の身元確認手順によって確立されなければならない。

【０３７５】

図４０のアカウント開設プロセスでは、個人のアイデンティティと、その個人のアイデンティティトラストチェーンであるＣＡ証明書との間に、取消不能なリンクが確立される。本発明の一実施形態では、個人のアイデンティティ文書９００は、暗号化ハッシュを使用してプライベート情報に変換され、ハッシュＩＤ９０１を生成し、これは、セキュリティ上の理由からオフラインで保存されている親ＨｙｐｅｒＳｐｈｅｒｅ証明機関、具体的には「アカウント」ＣＡ９０２を生成するために使用される。ＣＡ９０２を発行するために不明のサードパーティの認証局を採用する代わりに、ＨｙｐｅｒＳｐｈｅｒｅは、システムＣＡ証明書９０３を介してシステム固有のデジタル暗号検証を提供する。システム証明書９０３は、オフラインでＨｙｐｅｒＳｐｈｅｒｅの拡散型クラウドストレージに保存

されるため、ドキュメント９０３は読み取り可能だが、破損や修正のリスクはない。
【０３７６】
次に、システム署名されたＣＡ証明書９０３は、第２要素認証を含む可能性のあるグループ証明書９０４に署名するために使用される。ＨｙｐｅｒＳｐｈｅｒｅで生成されたグループＣＡ証明書９０４は、ＨｙｐｅｒＳｐｈｅｒｅの外部で複製することはできない。そのデジタル署名をハッシュＩＤ９０１と組み合わせることにより、発行ペアレンタルアカウントＣＡ証明書９０２は、ＨｙｐｅｒＳｐｌｅａｃｅの外部から偽造することができなくなる。ＨｙｐｅｒＳｐｈｅｒｅ内から偽造を実行したり、配布しようとする者は検知され、その行動はＩＤ、アカウント、資産を追跡することができる。この不正防止機能は、ＨｙｐｅｒＳｐｈｅｒｅで生成されたトラストチェーンに特有のものである。
【０３７７】
その後、アカウント証明書９０２は、ルート証明書９０５ａおよび９０５ｂを生成するために使用される。図４１に示すように、オフラインのルート証明書９０５ｂは、次に、オンラインＣＡ証明書９０６に署名するために使用され、この証明書９０６は、順番に、「リーフ」または「発行」証明書９０７（資産のＨｙｐｅｒＳｐｈｅｒｅブロックチェーン記録に署名するために使用される）を生成するために使用され、ウォレット、契約、デバイス、およびインストールされたソフトウェア（ＨｙｐｅｒＮｏｄｅｓなど）を検証および署名するために使用される９０８ｎとしてまとめて複数のＣＡを生成するために使用される。
【０３７８】
アカウントが検証可能な真のＩＤを使用して作成されたものであるか偽名で作成されたものであるかにかかわらず、アカウントとそのトラストチェーンは、ＨｙｐｅｒＮｏｄｅｓが存在するすべてのハードウェアにデジタル署名を行う（したがって接続されている）。真のＩＤアカウントでは、最上位の個人ＣＡ証明書である「親」ＣＡ証明書９０２は、画像スキャン、バイオメトリクス、署名などによって証明される、パスポート、運転免許証、社会保障番号などのＩＤ文書にリンクされている。先行する証明書に署名するために信頼された検証済み証明書を使用して信頼チェーンを形成するプロセスは、図４２および図４３に図示されている。アカウントのセットアップ中に銀行、適格加盟店、または信頼できる第三者機関によって実行される場合、独立した確認手順は、アカウントＣＡ証明書９１０を作成するＩＤ検証の複数のソースを使用して、個人または法人の合法的な身元を確認し裏付ける。信頼された身元が確立されると、アカウント所有者は、ＨｙｐｅｒＳｐｈｅｒｅが発行する「ルート」証明書を取得することができる。
【０３７９】
承認されたルート証明書により、その所有者は、特定の取引に署名したり、特定のデバイスを認証したりするために、プロディジー証明書９１２とサブディジー証明書９１３を有用なものにすることができる。このようにして、個人またはそのデバイスは、個人の身元を明らかにしたり、身元盗難のリスクを冒したりすることなく商取引に従事することができるようになる。図４２に示すように、アカウント所有者の身元証明書（親のＣＡ証明書）９１０は、個人のルート証明書を生成するために使用される。次にＩＤ証明書９１０はアカウント所有者のルート証明書９１１に署名し、そのルート証明書は、１つまたは複数の中間証明書９１２（ＩＭ　ＣＡ証明書）、最終的にはリーフ（エンドエンティティ）証明書９１３に署名して承認するために使用される。ＩＤ証明書９１０とそのルートＣＡ証明書９１１は、下位証明書に署名するために一度使用された後は、先行するＣＡ証明書が破損した場合に備えて、バックアップとしてコールドストレージ（オフラインまたは拡散クラウド）に置くことができる。ＣＡ証明書は、証明書のサブジェクトに指定された者が公開鍵を所有していることを確認するものである。署名プロセスにおいて、各証明書はその公開鍵を部下、すなわち発行者に渡し、その部下は公開鍵を用いて機密情報を暗号化して署名局に返す。このようにして秘密鍵を使って、署名局はファイルを復号化することができ、公開鍵の所有者は署名局だけであることを証明することができる。
【０３８０】

その後、認証局は発行者の身元情報に秘密鍵の暗号化されたバージョンで署名し、それを発行者に引き渡す。証明書の発行者は、下位の証明書にデジタル署名を行い、ルート証明書と親のＣＡ証明書に遡る信頼の連鎖を作成する。ＨｙｐｅｒＳｐｈｅｒｅでは、制御する証明書にはアカウント所有者のＩＤが含まれるが、ＩＭ証明書およびリーフ証明書では、ユーザのプライバシーをさらに保護するために仮名のＩＤが使用されることがあるＣＡ証明書は、個人のプライバシーを保護するだけでなく、不正行為を防止することもできる。親証明書から共通の系統を共有するすべての派生ＣＡ証明書は、親証明書の所有者のアカウントとデバイスにのみ有用である。アカウントのログイン情報が盗まれたとしても、泥棒はアカウント所有者の個人ＣＡ証明書の血統を自分のデバイスやアカウントと照合することはできない。アカウント所有者とその署名者が協力して詐欺行為を行った場合、犯罪捜査では、取り返しのつかないアイデンティティトラストチェーンを介して、必ず共謀関係が発見され、暴かれることになる。

【０３８１】

本発明の代替実施形態（図４３に示す）では、グループＣＡ証明書９１４と所有者の公開鍵９１５の組み合わせを使用して、エンドエンティティ証明書９１７を生成するために使用される検証済み中間証明書９１６を生成する。

【０３８２】

このように、ＨｙｐｅｒＳｐｈｅｒｅ　ｉｄｅｎｔｉｔｙは、アカウントのセキュリティ、トランザクションの完全性、および個人のプライバシーを保護しながら、犯罪を阻止する。ＨｙｐｅｒＳｐｈｅｒｅでは、ユーザは、ＩＤ－トラストチェーンにアクセスして、追加のコストや遅延なしにＡＡＡ検証済みトランザクションを実行することができる。ここでは、（ｉ）証明書が有効な署名であるかどうかを最初にチェックし、（ｉｉ）確認されたユーザの対応するトランザクションプロセスを承認し、最後に（ｉｉｉ）ブロックチェーンに新しいブロックを追加するなど、関連するすべてのレコードを更新する。

【０３８３】

ネットワークで生成されたＣＡ証明書、アイデンティティの検証、および超安全な公開鍵インフラストラクチャ（ＰＫＩ）暗号を使用したデジタル署名のユニークな組み合わせにより、ＨｙｐｅｒＳｐｈｅｒｅは、パブリッククラウド上にネイティブに展開されるエンタープライズグレードのＣＡ証明書のパイオニアとしての地位を確立している。これに対して、インターネット上でのエンタープライズレベルのＣＡ認証は、脆弱性とコストの両方を抱えており、１つの証明書につき数百ドルのコストがかかることも珍しくない。また、インターネットはＣＡ証明書の真の出所を確認できないため、検出されないインターネット詐欺が横行し、マルウェアの感染が蔓延している。ＨｙｐｅｒＳｐｈｅｒｅは、安全性の高い「プライバシー」ネットワークとしての先駆的な展開により、デバイス、ＨｙｐｅｒＮｏｄｅｓ、アカウント、ブロックチェーン、トランザクション、およびウォレットのデジタル署名付き認証に、アイデンティティトラストチェーンと検証済みのＣＡ－ｃｅｒｔｉｆｉｃａｔｅの系統を組み合わせることで、個人のアイデンティティとプライバシーを保護する。プライバシーネットワークの保護規定は、以下のような無数の方法で動作する。

・アカウントのマッピングを防ぐために、アドホックな動的ＩＰアドレスと動的ポート番号を介して、暗号化されたＩＤに動的に割り当てられている。

・デバイス、ＨｙｐｅｒＮｏｄｅｓ、およびＨｙｐｅｒＷａｌｌｅｔｓのトランザクションの信頼できる動的署名のためのパーソナルネットワークで生成されたＣＡ証明書で、偽者攻撃、証明書詐欺、および仮想通貨の盗難を阻止する。

・個人ＣＡ証明書を使用したセッションベースの証明書交換により、セッションダイアログを保護し、盗聴を防止する。

・アイデンティティベースの秘密鍵交換機能と分散型セッションベースの証明書を組み合わせたエンドツーエンドの暗号化により、ＳＤＮＰクラウドの運用に依存しない個人のプライバシーを確保する。

・フォレンジック攻撃やコンテンツの再構築を防ぐために、デバイスやＨｙｐｅｒＮｏｄ

ｅｓ（クラウドポータル）上の通話、ファイル、コミュニケ、暗号通貨取引の記録を含まないステートレスなＨｙｐｅｒＮｏｄｅｓ。
・完全に分散制御された分散型ネットワークで、すべてのトランザクションやデータのルーティングにマスターキーやシステム権限のない秘密鍵を使用することで、電子的に、あるいはシステム担当者などのオフライン攻撃によるネットワークの簒奪を防ぐことができる。
・暗号通貨取引のためのアクセスが制限された個人所有のマルチツリーブロックチェーンと、動的有向非周期グラフ（ＤｙＤＡＧ）で構成された記録保持は、オブザーバーがマスターブロックチェーンをバックトレースすることでプライバシー漏洩のリスクを排除する。
・ブロックチェーンの取引の完全性を保証しながら、バックトレース、詐欺、ブロックチェーン攻撃を防ぐために、ブロックチェーンの証明書へのアクセスを制限されたブロックチェーンの分散化された隠蔽された（特定できない）陪審員を介して、レプリカントブロックチェーンオブザーバーセグメント（ＲＢＯＳ）のトランザクションの検証を行うことができる。
・新たに開示されたデバイス、シーケンシャル量子キーまたは（ＳＱＫ）を使用したルート回復機能は、オンラインサイバー攻撃による悪意のある者の簒奪にアイデンティティトラストチェーンを晒すことなく、アカウントの復元を容易にする。

【０３８４】

ＨｙｐｅｒＳｐｈｅｒｅの外部で不正な証明書を生成しようとする不正な試みを防止するために、ネットワークでは、各ユーザアカウントをグループにリンクするシステムレベルの証明書権限も容易にしている。図４３に示すように、追加のプライバシー保護のために、中間ＣＡ証明書では、所有者のルート証明書９１５から１つ目と、システムで生成されたグループ証明書９１４から２つ目の証明書という、二重署名を使用して、多要素認証を利用することができる。この２つ目の認証により、不正行為を防止するだけでなく、ビジネス取引における共謀者による不正行為からの保護も強化される。いずれにしても、ＨｙｐｅｒＳｐｈｅｒｅは、犯罪者が取引を行うのに適したプラットフォームではない。アカウント情報は、裁判所の命令または召喚令状に基づいて、法執行機関が権限のある管轄区域に対して無期限に発見することができる。

【０３８５】

同様に、仮名口座は、ＩＤベースの所有権を持つため、法的な機密ビジネスに従事する際には便利であるが、ＨｙｐｅｒＳｐｈｅｒｅでは、法律を踏みにじったり、そのエージェントから逃れたりするための導管にはならない。ＨｙｐｅｒＳｐｈｅｒｅでは、銀行業務に必要な仮名口座から真のＩＤ口座へのすべての送金が、ブロックチェーン上に記録される。ＨｙｐｅｒＳｐｈｅｒｅのもう１つの要素は、トポロジカルトラストネットワークの斬新な利用である。前述の方法では、ネットワークで生成されたＣＡ証明書と、詐欺や盗難の対象とならないＩＤ－トラストチェーンを使用した強力な暗号防御に依存しているが、すべての攻撃に対して免疫があるシステムはない。このため、ＨｙｐｅｒＳｐｈｅｒｅのアーキテクチャでは、トポロジカルトラストネットワーク、つまり「トラストレイヤリング」を採用して、個人のアカウントやデバイスへの侵入が成功した場合の潜在的な被害を制限している。

【０３８６】

図４４は、ＨｙｐｅｒＳｐｈｅｒｅのトポロジカルトラストネットワークの階層構造を示している。最も安全な部分であるセキュリティコアには、アカウント所有者のＩＤベースの「ルート証明書」９２０が格納されている。これを使用して「中間」ＣＡ証明書（図示せず）を生成した後、ルート証明書９２０はオフラインで銀行の金庫などの「コールドストレージ」９２１に保存され、アカウントの不正利用を防止する。優れたＩＤベースのプライバシー保護の欠点としては、破損または紛失したルートＣＡ証明書は永久に回復できなくなる可能性があることだ。ＨｙｐｅｒＳｐｈｅｒｅでは、ルートＣＡ証明書のプライバシーを保護しつつ、その回復可能性を確保す９２２るために、ここで初めて導入された新しい暗号鍵、シーケンシャル量子鍵（ＳＱＫ）を採用している。

【０３８７】
ＳＱＫは、量子物理学から適応された手法、すなわち、システムを観察することでそのステートが変化するプロセスである量子オブザーバー効果を採用している。この効果には、量子もつれも含まれる。これは、ある粒子の状態に影響を与えるものがあれば、そのもつれたペアにも影響を与える。ＳＱＫは、最終的には量子電子デバイスを使用して実現されるかもしれないが、ＨｙｐｅｒＳｐｈｅｒｅでは、ＨｙｐｅｒＳｐｈｅｒｅの階層化された仮想ネットワーク層全体で実現される多次元ソフトウェアを使用して、その量子的な振る舞いをエミュレートすることができる。例えば、ある実施形態では、ＳＱＫキーの実装は、多数のキーセグメント（セル）で構成されており、それぞれのキーセグメントにはＡＳＣＩＩ英数字が含まれている。証明書アクセスパスコードの暗号化されたバージョンを構成するＳＱＫ鍵には、ユーザが選択したコンポーネントとシステムが生成したコンポーネントの両方が含まれる。ＳＱＫ復号化には、所有者のパスフレーズを知り、正確な順序で読み書きシーケンスを実行する必要がある。すべてのセグメントが適切な読み書きシーケンスで閲覧修正された場合にのみ、ルート証明書復旧プロセスへのアクセスがアンロックされる。単一のシーケンスのミスステップや入力エラーを犯すと、入力がすでに失敗していることを明らかにすることなく、行き止まりや無意味なチャレンジレスポンスダイアログが次々と表示されてしまいる。このように、ミスディレクションはハッカーのＣＰＵサイクルを消費し、時間、エネルギー、お金を浪費することになる。ＱＳＫは多次元的なものであり、ＨｙｐｅｒＳｐｈｅｒｅのユーザレベルでは、パスフレーズとは異なる長さの暗号化パスワードとして表示されるため、適切な読み書きシーケンスがなければ、パスフレーズを知っていても意味がない。パスフレーズの欠落した部分は、少なくとも３つの異なる仮想ネットワーク層に存在し、適切な順序が入力された場合にのみ表示される。このように、ＳＱＫセグメントフィールドの長さは可変であり、エントリが作成されたり、表示されたりすると、その外観は変化する。この可変キー長機能により、サイバー攻撃者は、自分が探しているパスフレーズの長さを推測することができなくなる。例えば、入力フィールドの長さが一定の１６セグメントで、各セグメントが３７文字の英数字（２６文字、１０個の数字、１個のヌル入力）のうちの１つを構成する場合、１次元のブルートフォース侵入が成功する確率は、使用される仮想ネットワークの次元ごとに10^{25}対１をはるかに超えている。しかし、パスコードエントリのセグメント長が変化すると、ブルートフォース攻撃を使用してパスフレーズを発見する確率は指数関数的に増加する。ＳＱＫの動作については、別の出版物や特許出願で詳しく説明する。

【０３８８】
図４４に戻り、オフラインストレージ９２１（エアギャップまたはＤＭＺセキュリティとしても知られている）を超えて、ＨｙｐｅｒＳｐｈｅｒｅでは、トポロジカルな信頼ネットワークを、信頼されたネットワーク９２３、保護されたネットワーク９２４、信頼されていないネットワーク９２５の３つのゾーンに分割している。信頼されたネットワーク９２３では、ＨｙｐｅｒＳｐｈｅｒｅのネットワークネイティブのリーフＣＡ証明書９２６ａ、９２６ｂが、ネットワークに接続されたすべてのデバイス（９２７ａ、９２７ｂ、９２７ｃ）とインストールされたすべてのＨｙｐｅｒＮｏｄｅｓ９２８ａ～９２７ｃに署名するために使用される。同じデバイスが、企業ネットワーク、大学のクラウド、サイバーカフェのサブネット、インターネッ９３０などの信頼されていないネットワークと相互作用する場合でも、ＨｙｐｅｒＳｐｈｅｒｅの対称的なＨｙｐｅｒＮｏｄｅｓのサンドボックス化により、ＨｙｐｅｒＣｏｎｔｒａｃｔの実行に対する侵入や監視を防ぐことができる。また、別のリーフ証明書９２６ｂを使用して、アカウント所有者の信頼できるＨｙｐｅｒＷａｌｌｅｔ９３１に暗号通貨やその他のデジタル資産を格納して署名することもできる。しかし、この信頼された資産９３１は、オンラインおよびＰＯＳトランザクション、モバイルおよびその他のアプリケーション、ユーザ、または独立したデジタル通貨取引所の保護されていないネットワークと直接やりとりすることはない。その代わり、すべての取引は、ユーザの個人的な信頼されたＨｙｐｅｒＷａｌｌｅｔ９３１とは別に、一時的なウォレット９３２からなる保護されたネットワーク９２４を介して処理される。この

一時的なウォレット９３２は、ワンタイムトランザクショントークンであるOT^3プロキシ９３３を使用してトランザクション９３５を実行し、ベンダーやユーザがＨｙｐｅｒＳｐｈｅｒｅアカウント所有者のＨｙｐｅｒＷａｌｌｅｔ９３１やそのブロックチェーンにアクセスすることを防ぐ。このように、ＨｙｐｅｒＳｐｈｅｒｅに組み込まれたトポロジカルトラストネットワークは、トランザクション９３５の両当事者を、第三者に対する不正行為や盗難から、またお互いに対する不正行為からも保護する。

【０３８９】

Ｄ．ＨｙｐｅｒＳｐｈｅｒｅブロックチェーン処理

【０３９０】

ＤＡＧ（有向非周期グラフ）

【０３９１】

インターネットの基本的なセキュリティ上の欠陥はさておき、ウェブ上での仮想通貨取引は、誰もがアクセスできる単一の共同ブロックチェーンに依存しているため、脆弱性が生じている。これとは対照的に、ＨｙｐｅｒＳｐｈｅｒｅでは、共通のパブリックブロックチェーンの使用を完全に排除し、代わりに、個人のＩＤベースの所有権を持つ複数の接続されたブロックチェーンを採用している。ピアコンセンサスによるトランザクションの整合性を確保するために、ブロックチェーンの相互接続性は、有向非周期グラフ（ＤＡＧ）と呼ばれるマルチツリーデータ構造を使用して促進される。

【０３９２】

ＨｙｐｅｒＳｐｈｅｒｅは、このＤＡＧデータ構造の新しいバリエーションを採用している。このＤＡＧデータ構造は、暗号通貨の生成、支払い、転送だけでなく、ネットワーク操作、断片化されたデータの転送、分解されたデータの保存、およびＩＤ－トラストチェーンにも使用されている。ＤＡＧがＨｙｐｅｒＳｐｈｅｒｉｃオペレーションにどのように適用されるかをよりよく理解するために、まず最初にグラフ理論－グラフの特性と応用に関する数学的理論－を考える必要がある。数学では、グラフという言葉にはいくつかの解釈があるが、最も広い意味では、グラフとは、頂点と頂点のペアを結合する辺の集合体である。物理学、生物学、化学、電子工学、コンピュータサイエンス、通信、商業などの多様な分野に適用可能なグラフは、接続性、関係性、階層性、プロセスについてのトポロジカルな洞察を提供する。トポロジーの１つのクラスである「有向」グラフは、シーケンス情報を含むプロセス、フロー、アルゴリズムを記述するのに特に適している。図４５に様々な形態で示されている有向グラフ９５０は、方向性を示すベクトル（矢印）を用いた辺によって接続された頂点を持つグラフから構成されている。このように、少なくとも１つのグラフサイクル（頂点がそれ自身から到達可能な辺と頂点の経路、すなわちループ）を含むグラフを環状グラフと呼ぶ。理論物理学では、周期的なプロセスの例として、カルノエンジン、可逆的等温ガス膨張プロセス（熱力学エンジンの熱を仕事に変換する効率の上限をモデル化するために使用される）がある。各カーノットサイクルでは、温度とエントロピーは同じループを繰り返し、システムは前回のサイクルから変更されずに元のステートに戻る。これらは検出されない詐欺や盗難を犯す機会を提供し、変更の記録なしで過去を変更するための手段を提供するため、電子商取引では、周期的なプロセスが問題となっている。このため、会計では、誤った元帳のエントリを変更することはできないが、代わりに、変更の日付を記録したデビットとクレジットのペアで構成される新しいエントリとして修正されることになる。

【０３９３】

従来の会計台帳と同様に、ブロックチェーンとＤＡＧは「サイクル」を含まないシーケンシャルレコードで構成されており、トランザクションは一方向に進み、同じ頂点に戻ることはない。ＤＡＧの他の例としては、先祖代々の家系図、単一の起源やインデックスケースから感染症が蔓延する疫学的なグラフ、各世代の先祖が自分の子孫に続くコンピュータマルウェアの拡散などがある。

【０３９４】

ウェブ上では、ブロックチェーンとＤＡＧは異なる概念であり、ＤＡＧはブロックチェ

ーンよりも本質的に優れた新しい概念であることが示唆されているが、より正確な説明としては、ブロックチェーンは１本の木からなる１次元のＤＡＧ９５１であるということである。言い換えれば、ブロックチェーンはＤＡＧの縮退形であり、１次元で進化するチェーンなのだ。ＤＡＧは２次元にも存在する。単一の側鎖を持つブロックチェーン９５２は、単一の共通の木からなる２次元ＤＡＧの些細なケースである。グラフ用語では、木は共通の祖先に接続された頂点で構成されている。２Ｄマルチツリー ＤＡＧは、単純に共通の頂点と異なる頂点を含む複数の独立した木９５３を含むＤＡＧであることになる。概念的には、シングルチェーン（１Ｄ　ＤＡＧ）ブロックチェーンに対するマルチツリーＤＡＧの利点は「並列性」であり、コンテンツを分割し、複数の「相互接続された」ブロックチェーンにトランザクションを分散させることができる。従来のブロックチェーンと比較して、並列処理は、トランザクション効率の向上、チェーン長の短縮、ストレージ需要の低下、トランザクション処理の高速化などの可能性を提供する。単一の共同ブロックチェーンを複数の相互接続されたブロックチェーンに変換することは、正しい方向への一歩であるとはいえ、ブロックチェーン技術の今日の暗号通貨の問題を解決するだけではない。

【０３９５】

仮想通貨は、ＤＡＧが提供するトランザクション処理の効率化とは無関係に、ノンチェインハッシュの謎解きに依存しているため、根本的にエネルギーと時間の効率が悪いままである。さらに、インターネット上のすべての仮想通貨取引は、ブロックチェーンのコンセンサス攻撃、プライバシー侵害、詐欺、仮想通貨の盗難などのセキュリティと信頼の攻撃に対して脆弱なまま変わらない。仮想通貨をＤＡＧに変換するだけでは、クリプトウォレットの盗難やブロックチェーン攻撃を防ぐことはできない（そして、今後防ぐこともできない）。セキュリティ、プライバシー、クリプト経済的なトランザクションの完全性に対する総合的なアプローチだけが、インターネットで流行しているサイバー窃盗や詐欺を克服することを望むことができる。

【０３９６】

前述のように、ＨｙｐｅｒＳｐｈｅｒｅは、Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｎｅｔｗｏｒｋ＆Ｐｒｏｔｏｃｏｌの技術、方法、および装置に従って行われるステートベースの通信に基づいている。グラフ理論では、ＨｙｐｅｒＮｏｄｅがタスクを実行したり、トランザクションを実行したりするたびに、その瞬間の頂点のステートが時空間的に異なることを意味する。このように、ＨｙｐｅｒＳｐｈｅｒｅは、時空間ネットワークを独自に構成している。したがって、ＨｙｐｅｒＳｐｈｅｒｅ内のすべてのトランザクションは、動的でステートに依存し、時間と場所に応じて常に変化する。マルチツリーＤＡＧの特徴をＳＤＮＰベースの動的時空間ネットワーク上で動作するように適応させるために、ＨｙｐｅｒＳｐｈｅｒｅでは、新しいグラフトポロジーである動的有向非周期グラフ（ＤｙＤＡＧ）を初めて採用した。ＤｙＤＡＧトポロジーでは、頂点は、ｉｄｅｎｔｉｔｙ（頂点名または頂点番号）とｓｔａｔｅ（ステート）の２つの特徴によって定義される。ステートとは、頂点が動作し、他の頂点と相互作用するためのルールを定義する条件である。ＨｙｐｅｒＳｐｈｅｒｅでは、頂点のステートには、時間、常駐するセキュリティゾーン、およびその他の位置情報が含まれる。そのため、ステートが異なる限り、同じ頂点を再訪しても循環ループにはならない。

【０３９７】

例えば、カルノサイクルでは、システムが頂点に戻るたびに、頂点のステートは前のサイクルと全く同じであるため、各繰り返しループは周期的である。対照的に、ＳＦ超大作「バックトゥザフューチャーパートＩＩ」のタイムトラベルは、非周期的な時空間動作の例である。物語の中では、登場人物のドック・ブラウンとマーティ・マクフライは、彼らの旅行中に全く何も変更されないことを期待して、彼らのデロリアンのタイムマシンで未来に旅行する。その後もとの時間と場所に戻ると、全てが恐ろしく馴染みのないものであることが分かった。比喩的に言えば、頂点v_xは以前と同じであったにもかかわらず、ステートs_yは予期せぬ変化を遂げていたのだ。この意味で、ＨｙｐｅｒＳｐｈｅｒｅは意図的に常に予期せぬ方法でステートを変化させており、パターンを識別しようとするサ

イバーハッカーを混乱させる。また、図４６に示すように、（ｖ$_1$，ｓ$_1$）から（ｖ$_2$，ｓ$_2$）、（ｖ$_1$，ｓ$_2$）から（ｖ$_1$，ｓ$_2$）までのトランザクションで構成されるＤｙＤＡＧシーケンス９５３は、ステートがｓ$_1$≠ｓ$_2$である限り、周期的なグラフを構成しない。三次元ＤｙＤＡＧを平面投影した二次元のグラフ９５４では周期的に見えるが、三次元では螺旋状や螺旋状９５５に描かれているので、ステート空間が周期的ではないことがわかる。本質的には、ネットワークは自律的に、解析が不可能なほどの速さで、取り返しのつかない変化の連続を示しているのである。ステート変数を含めることで、２Ｄマルチツリー ＤＡＧは、優れたパフォーマンス、整合性、セキュリティを備えた３Ｄ ＤｙＤＡＧブロックチェーンになる。ＨｙｐｅｒＳｐｈｅｒｅは、このＤｙＤＡＧの原理をＨｙｐｅｒＳｐｈｅｒｅ内でいくつかの方法で適用している。

・ステートベースのセキュリティクレデンシャル情報とアルゴリズムを用いた超安全なＳＤＮＰ通信

・アクティブで冗長なＨｙｐｅｒＮｏｄｅｓからなる分散ネットワーク上でのデータ転送により、ネットワークの回復力を向上させながら、伝搬遅延を最小限に抑えることができる（後述）。

・Ｐｅｒｓｏｎａｌ ＣＡ－ｃｅｒｔｉｆｉｃａｔｅベースのＩＤ－Ｔｒｕｓｔ－Ｃｈａｉｎを使用して、ＨｙｐｅｒＳｐｈｅｒｅに接続されたデバイスやＨｙｐｅｒＮｏｄｅｓの包含または失効を記録し、アクセスと権限を制御する。

・永久ＤｙＤＡＧブロックチェーントランザクション、ＲＢＯＳオブザーバー、ＯＴ^{3}プロキシペイメントプロセッサーに署名し、管理するために使用される個人ＣＡ証明書ベースのアイデンティティトラストチェーン。

・ＨｙｐｅｒＷａｌｌｅｔｓの永久ＤｙＤＡＧデータに署名し、管理するために使用される個人ＣＡ証明書ベースのアイデンティティトラストチェーン。

・契約誓約のＨｙｐｅｒＣｏｎｔｒａｃｔジョブ実行、タスク実行、陪審員のコンセンサス、鋳造または溶融リサイクル（再鋳造）によるＨｙｐｅｒＣｏｉｎ生成に使用される一過性のＤｙＤＡＧブロックチェーン（'ｔＢＣ'）。

【０３９８】

ネットワーク運用におけるＤｙＤＡＧの使用に関しては、ＳＤＮＰクラウドは本質的に４層のＨｙｐｅｒＮｏｄｅリソースプロバイダで構成されるダイナミックＤＡＧを形成している。ノードは、暗号通貨の獲得を希望する採掘者の数に基づいてネットワークに追加され、ローカルネットワークの混雑やＤｏＳ攻撃が発生した場合には、自動的にノードがインスタンス化される。各インスタンスでは、ネットワークに参加するＨｙｐｅｒＮｏｄｅｓの数が増えれば増えるほど、クラウドの冗長性が高まり、データルーティングのための最短伝搬遅延パスを見つけて使用する際のネットワークの効率が向上する。グラフ理論の用語では、ＳＤＮＰネットワークの動作は、メッシュ化されたマルチパスルーティングのための時空間的な目的地指向の動的有向非周期グラフを表している。ノード密度に応じてスケーリングされるもう一つの利点は、設定ミス、障害、停電、自然災害、攻撃に耐えながら、ネットワークが許容可能なレベルのＱｏＳ（サービス品質）を維持する能力である回復力である。ネットワークの回復力は、参加しているノードの数に応じて非線形に変化する。理論的には、結合接続の総数はノード数ｎに比例してスケールするが、多数のノードではｎ－（ｎ－１）／２の関係でｎ^{2}に近づくが、多くの接続は周期的なものとして除外される。ＤｙＤＡＧでは、ノードの再利用は真のサイクリックではないが（ステートが異なるため）、リアルタイムネットワークでは、短いホップ数だけが低い伝搬遅延を実現する上で価値があり、低消費電力のルーティングを実現する上で有益である。ＤＡＧの代表的なモデルは、'ｎ'ノード上のｋ個のアウトフローの（出口エッジ）からなる再帰方程式によって、組み合わせの数"ａ"を記述する。

【０３９９】

【数４】

$$a_n = \sum_{k=1}^{n} (-1)^{k-1} \binom{n}{k} 2^{(n-k)} a_{n-k}$$

【０４００】
ここで示された二項式では、利用可能なパスの数はネットワーク内の参加ノードの母集団に比例して増加する。この式は理想化された順列母集団ｎ－（ｎ－１）／２よりも現実的だが、ダイナミックＤＡＧの特定の特徴を具現化しているわけではない。例えば、ＤＡＧでは除外されていたサイクリックループが、ＤｙＤＡＧではステート変化によりサイクリックにならない場合がある。逆に、非常に高いトランザクションレートでトランザクションを実行しているノードでは、一部のノードは（少なくとも短時間の間は）静的ＤＡＧの要素として振る舞うことがあり、それにより、いくつかの可能性のあるループ（流出）がサイクリックなものとしてツリー母集団から除外すべきである。また、数学的に言えば、遠距離のリモートノードは有効なＤｙＤＡＧツリーを構成するが、リアルタイムネットワークでは、許容できないほど長い伝搬遅延が発生するため、除外されなければならない（発信側からあまりにも遠く離れているため、ネットワークに参加しても全く輸送に役立たないという意味である）。言い換えれば、時空間的なＤｙＤＡＧグラフでは、これらのツリーは除外されなければならないということである。
【０４０１】
マルチツリーＤｙＤＡＧブロックチェーン
【０４０２】
暗号通貨の生成やブロックチェーン取引の安全性、完全性、スピードを確保するためには、ブロックチェーンのサイズと長さを制限し、制御不能な成長を避け、未知のユーザからの侵入を防ぐために、限定されたメンバーを関与させる必要がある。ビットコインやＥｔｈｅｒｅｕｍなどで使用されている既存のブロックチェーン技術は、グローバルな許可のない参加を伴う単一のパブリックな「共同」ブロックチェーンを採用している。
【０４０３】
共用の許可のないブロックチェーンは、プライバシーの漏洩、盗難、コンテンツの汚染、違法性の対象にもなる。結果として生じるパブリックブロックチェーンは、ＨｙｐｅｒＳｐｈｅｒｅの設計目標や運用目標を満たすには、あまりにも面倒で、時間がかかり、攻撃に対して脆弱性がある。長い間のブロックチェーンの弱点や脆弱性を回避するために、ＨｙｐｅｒＳｐｈｅｒｅでは、ブロックチェーン処理、暗号通貨トランザクション、トラフィック管理のために、全く新しいブロックチェーン構造と制御システムを採用している。静的グラフ理論から動的リアルタイムプロセスに適応したＤｙＤＡＧ数学、グラフ理論、制御アルゴリズムは、動的メッシュデータルーティングのガバナンス、ＨｙｐｅｒＣｏｎｔｒａｃｔの実行、高速ブロックチェーントランザクション、ＨｙｐｅｒＳｐｈｅｒｅ暗号通貨生成、Ｅコマースなど、ＨｙｐｅｒＳｐｈｅｒｉｃの運用全体に広く採用されている。
【０４０４】
従来のシングルチェーン台帳とは対照的に、図４１に示すＤｙＤＡＧブロックチェーン９５５はパーソナライズされたマルチツリー型であるため、ブロックチェーンの長さが制限され、ストレージの需要が減り、トランザクションの解決率が向上する。これらの明らかな性能上の利点に加え、ＤｙＤＡＧブロックチェーンは堅牢であり、トランザクション検証のための改ざん防止のコンセンサスを保証する。
【０４０５】
従来の暗号通貨におけるグローバルな共同許可のないシングルチェーンブロックチェーンとは異なり、ＨｙｐｅｒＳｐｈｅｒｅのＤｙＤＡＧブロックチェーンのさまざまなツリーは「個人」（共同ではない）であり、各ブロックチェーンは、ＩＤ－トラストチェーンを介して個人または企業の所有権を持っている。ＤｙＤＡＧブロックチェーンには、一過

性のブロックチェーン（ｔＢＣ）、つまり契約の実行に使用される期間限定の台帳と、金融取引を不変に記録し、法的記録を埋め込むために使用される永久（恒久）ブロックチェーン（ＢＣ）の両方がある。ユニタリーブロックチェーンの実装と同様に、ＤｙＤＡＧブロックチェーン上のすべてのトランザクションにはタイムスタンプが押され、バックデートや修正の対象とならないシーケンシャルなトランザクションの記録が不変に記録される。しかし、共同のユニタリーパブリックブロックチェーンとは異なり、ＤｙＤＡＧブロックチェーンツリーはそれぞれ個人や企業の所有物が異なるため、取引を行うブロックチェーンや企業を相互にリンクさせる仕組みが必要となる。

【０４０６】

図４９に示すように、このリンクは、すべてのクレジット９７４が別のブロックチェーン上のデビット９７３に対応しているブロックチェーンの一般的な会計の二列クレジット／デビット元帳の概念を適用することで実現されている。ＨｙｐｅｒＳｐｈｅｒｅでは、ブロックチェーンからブロックチェーンへの資産移転はすべて、買い手、売り手、陪審員、代替陪審員などの参加者を指定したＨｙｐｅｒＣｏｎｔｒａｃｔｓ９６４を通じて実行される。契約が完了すると、すべてのクレジット／デビット取引が記録され、支払者のＤｙＤＡＧブロックチェーン上ではデビットとして、支払者のプライベートブロックチェーン上ではクレジットとしてタイムスタンプが押される。パブリックブロックチェーンの場合、修正されたＤｙＤＡＧは、ハッカーや泥棒から所有者の正体を守るために、偽名を使用してＨｙｐｅｒＳｐｈｅｒｅ上で公開される。これらの偽名によって所有者の本当の個人や企業の身元が明らかになることはないが、犯罪捜査や民事訴訟の場合には、偽名のブロックチェーン所有者が本当の身元を追跡することができる。ＨｙｐｅｒＳｐｈｅｒｅは、プライベートなブロックチェーンをサポートすることも可能である。買い手が内蔵の保護規定を放棄しない限り、プライベートブロックチェーンに記録されたトークンは、ＨｙｐｅｒＳｐｈｅｒｅの暗号通貨に直接転送することはできない。代わりに、そのようなトークンは、銀行または独立したデジタル通貨取引所を通じて、フィアット通貨に交換し、その後、ＨｙｐｅｒＭｅｔａｌまたはＨｙｐｅｒＣｏｉｎｓのいずれかを購入するために使用する必要がある。

【０４０７】

Ｅ．ＨｙｐｅｒＳｐｈｅｒｅ　Ｃｒｙｐｔｏｅｃｏｎｏｍｉｃ　Ｐｌａｔｆｏｒｍ

【０４０８】

ＨｙｐｅｒＳｐｈｅｒｅは、分散型電子商取引のための完全分散型ネットワークおよびエコスフィアとして動作する。ＨｙｐｅｒＳｐｈｅｒｅの加盟店とリソースプロバイダの間の取引は、中央の権限を持たないピアツーピアベースで行われ、報酬（報酬）は当事者間で直接やり取りされる。公開された完了したトランザクションのブロックチェーン台帳は、ＨｙｐｅｒＳｐｈｅｒｅ内のピアの陪審員によって検証可能である。ＨｙｐｅｒＳｐｈｅｒｅ加盟店の顧客は、加盟店が提供するサービスによって異なる。ＨｙｐｅｒＳｐｈｅｒｅ加盟店が提供するサービスには、ＨｙｐｅｒＳｅｃｕｒｅクラウド通信、クラウドコンピューティング、クラウドデータストレージ、ネットワーク接続されたデバイス、クラウドベースの電子サービスなどがある。

【０４０９】

Ｃｌｏｕｄ－ａｓ－ａ－Ｓｅｒｖｉｃｅ（ＣａａＳ）プロバイダであるＨｙｐｅｒＳｐｈｅｒｅは、商業的科学的な取り組みを幅広くサポートするための超安全なプラットフォームを提供している。しかし、商業的なＣａａＳプロバイダとは異なり、ＨｙｐｅｒＳｐｈｅｒｅはホストのトランザクションとは距離を置いたプラットフォームとして運営されており、（少額のルーティング料を除けば）ＨｙｐｅｒＳｐｈｅｒｅを利用したサービス、トランザクション、ビジネスの当事者ではない。つまり、ＨｙｐｅｒＳｐｈｅｒｅは、ユーザやリソースプロバイダと競合することはない。そのため、ＨｙｐｅｒＳｐｈｅｒｅは、より正確にはＰｌａｔｆｏｒｍ－ａｓ－ａ－Ｓｅｒｖｉｃｅプロバイダと表現されている。

【０４１０】

ＨｙｐｅｒＳｐｈｅｒｅ　Ｐｌａｔｆｏｒｍ－ａｓ－ａ－Ｓｅｒｖｉｃｅ
【０４１１】
非営利の独立したＰｌａｔｆｏｒｍ－ａｓ－ａ－Ｓｅｒｖｉｃｅとして、ＨｙｐｅｒＳｐｈｅｒｅは、経済的、商業的、科学的、そして慈善活動の多様な取り組みを、対立することなくサポートすることができる。ＨｙｐｅｒＳｐｈｅｒｅは、加盟店が提供するサービスと参加者の想像力によってのみ制限されるため、銀行・金融、製造業、マーケティング、商品化・販売、流通、ヘルスケア／医療、エネルギー／エコロジー、輸送・輸送、安全・セキュリティ、教育、研究・開発、科学、情報ストレージなど、事実上あらゆる分野のビジネスや研究を支援することができる。ＨｙｐｅｒＳｐｈｅｒｅは、次のような今日最もホットなハイテクビジネスの多様なトピックをサポートする独自のアプローチのｅコマースを提供する。
・クラウドコンピューティングとリアルタイム通信
・ビッグデータ
・人工知能（ＡＩ）
・セキュリティとプライバシー
・分散型デジタル通貨
・エネルギー効率
【０４１２】
上記の取り組みでＨｙｐｅｒＳｐｈｅｒｅプラットフォームが提供するサービスについては、以下で詳しく説明する。
【０４１３】
クラウドコンピューティングとリアルタイム通信
【０４１４】
クラウドコンピューティングとクラウドベースの通信の約束は、接続性をインターネットに依存していることに悩まされている。当初から、インターネットはファイルの信頼性の高い冗長配信のために作られたが、リアルタイムのネットワークとしては決して作られていなかった。そのため、Ｌｉｎｅ、ＫａｋａｏＴａｌｋ、ＷｈａｔｓＡｐｐなどのクラウドベースの通信は信頼性が低く、通話が途絶えたり、遅延や「ネットワークの不安定性」と呼ばれる現象に悩まされることがある。ネットワークの遅延が数百ミリ秒にもなると、コンピュータの計算よりも１０億倍も遅くなることがあるため、サーバはネットワーク接続の再確立や更新されたデータファイルの転送を待つ間、すべての時間を費やしてしまうことになる。ＨｙｐｅｒＳｐｈｅｒｅは、特許取得済みのリアルタイムダイナミックネットワークとプロトコルを採用することで、これらの問題に対処している。
【０４１５】
ビッグデータ
【０４１６】
大規模なデータセットを分析または保存するということは、１つのドライブまたはメモリファームに、１つの場所に驚異的な量の個人データやプライベートデータが格納されている可能性があることを意味する。これらの大規模な記録に対する攻撃や不正侵入に成功すると、詐欺的な取引、個人情報の窃盗、恐喝、恐喝、さらには個人攻撃に国民がさらされることになる。近年、政府、クレジットカード、クレジットビューロー、保険会社、加盟店のデータベースに対するハッキングが成功したことで、何億人もの人々が盗まれたデータからの個人攻撃や金融攻撃にさらされている。この問題は、今日のビッグデータのファイル構造への移行や、ｉＣｌｏｕｄ（登録商標）、Ａｍａｚｏｎ　Ｄｒｉｖｅ、Ｇｏｏｇｌｅ　Ｄｒｉｖｅ（登録商標）、ｉＤｒｉｖｅ、Ｂｏｘ．ｃｏｍ、Ｄｒｏｐｂｏｘ（登録商標）などのオンラインおよび個人向けクラウドストレージへの移行に伴い、さらに悪化することが予想される。ＨｙｐｅｒＳｐｈｅｒｅは、ファイルのコンテンツを何百ものデバイスに冗長的に分散させたデータストレージを使用して、ストレージドライブへの攻撃に対抗する。このアプローチにより、ハッカーがファイルのすべての構成要素を探し出して収集したり、元のコンテンツを復元するために断片を再構築したりすることを不可能

にする。
【０４１７】
人工知能
【０４１８】
人工知能は急速に進化しているが、今日のコンピュータサイエンスの中ではまだ十分に活用されていない分野でもある。まず大規模な計算能力を蓄積しなければ、この分野の進歩は遅々として進まないと予想されている。人工知能は、ＨｙｐｅｒＳｐｈｅｒｅにおいて２つの役割を果たしている。１つ目は、イネーブル技術として、ＨｙｐｅｒＳｐｈｅｒｅのマーケットプレイスでＡＩを採用し、ＨｙｐｅｒＳｐｈｅｒｅの加盟店とＨｙｐｅｒＳｐｈｅｒｅのリソースプロバイダとの間で自律的に雇用契約の交渉を行う。このようにして、ＡＩは、ＨｙｐｅｒＳｐｈｅｒｅの中央権限の懸念を排除し、スケジューリングは（ディスパッチャのように）実行するが、トランザクションやその検証の当事者としては動作しない。第二に、分散コンピューティングリソースとオープンソースアーキテクチャを持つＨｙｐｅｒＳｐｈｅｒｅは、ＡＩ技術研究のための魅力的なクラウドプラットフォームになると期待している。
【０４１９】
セキュリティとプライバシー
【０４２０】
国際的なビジネスや電子商取引のための世界のプラットフォームであるインターネットは、本質的に安全ではない。インターネットをベースとした通信や電子商取引が登場して以来、サービス拒否攻撃、ワーム、ウイルス、スパイウェア、パケットリダイレクト、偽セルタワー、キーストロークロガー、パケットスニッファ、ゼロデイ攻撃、ポートスニッファ、その他のマルウェアなど、サイバー攻撃は数え切れないほど記録されている。さらに、データパケットはパケットの送信元と送信先に関する情報を特定するため、メタデータ解析を利用してユーザのプロファイリングに基づいた攻撃を行うことができる。これとは対照的に、ＨｙｐｅｒＳｐｈｅｒｅは、動的ルーティングによる匿名の断片化されたデータ伝送を使用している。パケットの内容、セキュリティクレデンシャル情報、およびルーティングは１秒の数分の１単位で動的に変化するため、ネットワーク伝送を追跡してＨｙｐｅｒＳｐｈｅｒｅで関連するパケットをキャプチャし、それらを解読してペイロードを抽出した後、元の内容を再構築することは事実上不可能だ（たった一度でも）。また、通信全体をハッキングするためには、ＨｙｐｅｒＳｐｈｅｒｅ内の各ノードを常に監視し、新しいパケットが変化するスピードよりも速いペースで前述のハッキングシーケンスを実行する必要がある。このように、ＨｙｐｅｒＳｐｈｅｒｅの動的なセキュリティ手法により、ネットワークは中間者攻撃を受けないようになっている。そのため、純粋に暗号化ベースのインターネット通信とは異なり、ＨｙｐｅｒＳｐｈｅｒｅの通信は、中央制御やシステムの暗号化キーを一切持たないハイパーセキュアな通信となっている。
【０４２１】
分散型デジタル通貨
【０４２２】
既存の暗号通貨は、コイン所有者の購買力に影響を与える投機による急激な価格変動に容赦なく直面している。ビットコインの価格変動は、１日の取引で２７％もの変動が発生している。その他の仮想通貨の懸念事項としては、コインの採掘に必要な費用の上昇と時間の長期化（いわゆる「コモンズの悲劇」）、ネズミ講やねずみ講、信頼性の低い取引所、コイン取引に使用されるインターネットベースの通信のハッキング、ＩＣＯ創設者の不審な退場、インサイダー取引、証券詐欺、ＩＤ窃盗、マネーロンダリング、麻薬取引、セキュリティ、倫理、デジタル通貨の完全性と価値に関するその他の実質的な懸念が挙げられる。このように、今日の暗号通貨は、消費者、企業、銀行、国際商取引などの日常生活ではほとんど、あるいはまったく役割を果たさない怪しげな金融商品となっている。ＨｙｐｅｒＳｐｈｅｒｅは、ネットワークを介したデータ転送の一部として、自律的に生成されたトークンを使用している。トークンは使用証明に基づいて生成されるため、リソース

プロバイダがタスクやジョブを完了するたびに、ネズミ講や５１％攻撃、コモンズの悲劇（Ｔｒａｇｅｄｙ　ｏｆ　ｔｈｅ　Ｃｏｍｍｏｎｓ）などの影響を受けずに造幣プロセスを行うことができる。

【０４２３】

エネルギー効率

【０４２４】

現在の暗号通貨のマイニングでは、膨大なエネルギー（現在では世界の年間消費電力量の０．１５％以上）を無駄に消費し、新しい暗号通貨を生成する以外には、ほとんど、あるいは全く有益な目的を持たない計算タスクを実行している。ＨｙｐｅｒＳｐｈｅｒｅでは、ネットワークを介したデータ転送の一部として、自律的に生成されたトークンを使用している。この方法は、ビットコインの生成に使用されるプルーフオブワークベースのマイニングに比べて、トークンの消費電力が１２桁も少なくて済む。

【０４２５】

ＨｙｐｅｒＳｐｈｅｒｅ設計アーキテクチャ

【０４２６】

ＨｙｐｅｒＳｐｈｅｒｅの設計目標は、ユーザのプライバシーを保護し、トランザクションの完全性を確保しながら、グローバルなユーザコミュニティをサポートする電子商取引のためのオープンソースプラットフォームを容易にすることである。そのために、ＨｙｐｅｒＳｐｈｅｒｅの設計手法は、以下の５つの基本的なコンセプトに基づいている。

・アイデンティティ
・セキュリティ
・個人情報の取り扱いについて
・保全
・責任の所在

【０４２７】

ＨｙｐｅｒＳｐｈｅｒｅの設計は、このような基本原則に則ったコンピュータネットワークおよび通信クラウドとして、他のネットワークやクラウドと比較して圧倒的に優れた運用上の指揮・制御を実現している。インターネットは、その性質上、接続されている未知のデバイスに制御を委ねている。インターネットに接続されたデバイスは、パケットのルーティング、データ転送で採用される（または無視される）セキュリティ方法、さらにはパケットのコンテンツやメタデータに誰がアクセスしたり、監視したりできるかを決定する。このように、悪質な行為者は、クラウドの匿名性によって保護された状態で、さまざまな手段を使って他のユーザに窃盗、プライバシー侵害、その他の悪質な行為を結果を伴わずに行わせることができる。

【０４２８】

比喩的に言えば、この点ではインターネットは「公衆電話」として機能し、誰もがネットワークや他のユーザに個人情報を明かさずに匿名で通信できることを意味する。さらに悪いことに、身元を確認したり、自信を持って信頼を確立したりする能力がないため、詐欺師は比較的簡単にインターネットを利用して、発見されずに他人のユーザの個人情報を詐取することができる。多くの場合、インターネット攻撃は、ネットワークの中で最も安全性の低いコンポーネントであるＩｏＴデバイスから開始することができる。このように、冷蔵庫、スマートＴＶ、サーモスタット、調光可能な「スマート」電球は、ネットワーク全体とそのユーザの整合性とセキュリティを損なう可能性があり、目の肥えたサイバー犯罪者が選択する攻撃ベクトルとなる。対照的に、ＨｙｐｅｒＳｐｈｅｒｅは、すべてのユーザと接続されたコンポーネントを識別して承認することで、ネットワークへのアクセスを明示的に制御する。ＨｙｐｅｒＮｏｄｅｓと呼ばれるソフトウェアベースのネットワークポータルを通じて、ＨｙｐｅｒＳｐｈｅｒｅは、プロセスと通話の開始を管理し、さまざまなデータタイプ（音声、テキスト、ビデオ、ソフトウェアなど）の処理を制御し、データパケットのルーティングを指示し、セキュリティ隠蔽アルゴリズムとセキュリティクレデンシャル情報を選択し、プロセスを検証する。

【０４２９】
　また、組み込みの暗号通貨トランザクションを慎重に精査し、ネットワーク運用を管理して高いサービス品質（ＱｏＳ）を確保し、接続されたデバイスとユーザのアイデンティティを慎重に検証する。ＨｙｐｅｒＳｐｈｅｒｅでは、セキュリティとプライバシーは別のメカニズムで対処されている。ＨｙｐｅｒＳｐｈｅｒｉｃのセキュリティは、インターネット通信を強化するのではなく、独自の専用通信プロトコルであるＳＤＮＰ（Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｎｅｔｗｏｒｋ＆Ｐｒｏｔｏｃｏｌ）を利用することで実現している。そのため、ＨｙｐｅｒＳｐｈｅｒｅは、従来のインターネットセキュリティの脆弱性や欠陥の影響を受けることはない。
【０４３０】
　ＳＤＮＰ通信は、ドイツ、アラブ首長国連邦、および様々な海運港当局の自治体や緊急サービス向けのプライベートネットワーク上に展開された実績があり、専門的な通信やプライベートネットワークで１５年以上の経験を持つ実証済みの実地試験済み技術を使用して運用されている。イラク戦争中に米軍で使用されたＳＤＮＰ通信は、ＦＩＰＳ１４０－２規格に準拠したプライベート無線ネットワーク上で軍事レベルのセキュリティを提供できることが確認されている。ここで説明するＨｙｐｅｒＳｐｈｅｒｅの設計目標は、同じ技術をパブリックネットワークオープンソースで展開し、エンタープライズグレードの認証局と組み込みネットワークネイティブの暗号通貨を組み合わせたものである。これらの目的の簡単な概要と、ＨｙｐｅｒＳｐｈｅｒｅがどのように問題に対処しているかについては、以下を参照のこと。
【０４３１】
　ＨｙｐｅｒＳｐｈｅｒｅ　Ｉｄｅｎｔｉｔｙ
【０４３２】
　インターネットとは対照的に、ＨｙｐｅｒＳｐｈｅｒｅでは、ユーザが匿名であることはない。個人または企業を問わず、すべてのユーザは、対応する固有のＨｙｐｅｒＳｐｈｅｒｅ　ＩＤを保持しており、他のユーザの閲覧からプライベートに保護されている。この個人または企業のＨｙｐｅｒＳｐｈｅｒｅ　ＩＤは、ユーザのデバイス、ＨｙｐｅｒＮｏｄｅクラウドポータル、アカウント、およびウォレットを、ＨｙｐｅｒＳｐｈｅｒｅネットワークで生成されたＣＡ証明書で構成されるアイデンティティトラストチェーンに恒久的にリンクさせる。インターネットは、盗難や詐欺の対象となるサードパーティの証明書機関に依存している。これに対して、ＨｙｐｅｒＳｐｈｅｒｅは、独自のネットワーク固有のＣＡ証明書を生成する。図４０に示すように、前述のように、すべてのＩＤ－トラストチェーンは、ＨｙｐｅｒＳｐｈｅｒｅのマスター証明書９０３によって署名されたＣＡ証明書のみを使用し、自己署名された証明書やサードパーティの証明書はすべて信頼されていないものとして拒否する。ユーザのＣＡ証明書を対応するＩＤ－トラストチェーンにリンクすることで、盗まれた証明書や不正な証明書は、ユーザのＣＡ証明書の他のインスタンスとは一致せず、不正が検出され、不正な証明書が関与するすべてのトランザクションが拒否される。
【０４３３】
　ＨｙｐｅｒＳｐｈｅｒｅのセキュリティ
【０４３４】
　ＨｙｐｅｒＳｐｈｅｒｅのエンタープライズグレードの認証局による本人確認は重要だが、それだけでは、ネットワークへの侵入を防ぐには不十分である。データを保護し、トランザクションの完全性を維持し、暗号通貨の盗難や詐欺を防ぐために、ＨｙｐｅｒＳｐｈｅｒｅでは、軍事レベルの「ハイパーセキュア」なデータ転送と、特許取得済みのＳＤＮＰ（Ｓｅｃｕｒｅ　Ｄｙｎａｍｉｃ　Ｎｅｔｗｏｒｋ＆Ｐｒｏｔｏｃｏｌ）に準拠した多層的なセキュリティ機能を採用している。パケット転送処理には暗号化が採用されているが、ＳＤＮＰプロセスは暗号化だけに依存しているわけではなく、優れたセキュリティ保護を実現している。その代わり、ハイパーセキュア通信では、匿名データパケットの断片化された伝送の原理と、動的なルーティングと隠蔽が組み合わされている。ＨｙｐｅｒＳ

ｐｈｅｒｅにおけるＳＤＮＰデータ転送は、そのプロトコルに従って、（ｉ）ネットワーク内の単一ノードを通過するデータ量を制限し、（ｉｉ）パケットの真の送信元と送信先を難読化し、（ｉｉｉ）データパケットの内容を隠蔽し、（ｉｖ）すべてが変更される前にセキュリティ規定を破って攻撃を開始する時間を制限する（新しいセキュリティクレデンシャル情報、アルゴリズム、パケットルーティング、内容など）。

【０４３５】

最後に説明した「時間」を制限するセキュリティ手法は、より正確にはダイナミックルーティングとコンシールメントと呼ばれ、サイバー犯罪者にとっては、ハッキングが成功しても有効な時間がほんの数秒に制限され、その後は攻撃者が最初からやり直さなければならないため、特にフラストレーションがたまり、コストもかかる。ルーティングや隠蔽の方法の変更は永続的に変化するため、万が一サイバー攻撃者がパケットに侵入したとしても、次のパケットがどこにあるのか、どのようにルーティングされているのかを把握することができない。ＨｙｐｅｒＳｐｈｅｒｅのメッシュ化されたネットワークでは、２つの連続したパケットが同じノードを通過することはまずない。また、ＳＤＮＰデータパケットには断片化されたデータが含まれているため、たとえ攻撃者がパケットの暗号を破ることができたとしても（１／１０秒の１秒間に１００年分のブルートフォース復号を完璧に実行する必要がある）、それに対応する他の断片がなければ、復号化されたパケットの断片化された内容は不完全で意味がなく、まったく役に立たないものとなり、ＨｙｐｅｒＳｐｈｅｒｅのクラウドやネットワークトラフィックに対するさらなる攻撃を阻止することができない。

【０４３６】

ＨｙｐｅｒＳｐｈｅｒｅのプライバシー

【０４３７】

プライバシーとは、どのような情報を誰と共有するかをコントロールする権利のことである。セキュアなネットワークが自動的にプライバシーを保証するわけではない。プライバシーの確保は、単にセキュリティを容易にするだけではなく、より厳格で厳しいものとなる。そのため、ＨｙｐｅｒＳｐｈｅｒｅは、ＳＤＮＰセキュアネットワーク機能だけに頼って、プライベートな通信やファイルを保証するわけではない。代わりに、プライバシーネットワークでは、ハッキングや監視の防止に加えて、個人コンテンツや個人情報へのアクセスを必要に応じて制御し、「検証可能な身元」を利用してアクセスを制限する必要がある。

【０４３８】

検証可能なＩＤによる認証は、匿名性を利用して、偽者が真のＩＤを難読化したり、目的を偽ったり、個人や企業に対する悪意のある攻撃を密かに行うことを防ぐ上で特に重要な役割を果たす。プライバシーネットワークとして機能するために、ＨｙｐｅｒＳｐｈｅｒｅは、接続プロセスでユーザとデバイスの身元を確認するという原則を利用している。つまり、ネットワークネイティブのＣＡ証明書を使用して、ユーザに特権情報へのアクセスを許可する前に、個人やデバイスの信頼を確立することができる。ＨｙｐｅｒＳｐｈｅｒｅのプライバシー規定では、ハイパーセキュリティだけでなく、インターネット上では不可能な、アイデンティティトラストチェーンと検証済みのＣＡ証明書の系統を高度に組み合わせて、個人のアイデンティティと個人情報を保護している。これらの保護機能には、デバイス、ＨｙｐｅｒＮｏｄｅｓ、アカウント、ブロックチェーン（ＢＣ）、ＨｙｐｅｒＣｏｎｔｒａｃｔのトランザクション、およびウォレットのデジタル署名付き認証が含まれており、中間のＩＭの親とは異なる発行（リーフ）証明書を採用している。強力な暗号防御に加えて、前述の方法は、偽造の対象とならないＨｙｐｅｒＳｐｈｅｒｉｃネットワークネイティブのＣＡ証明書とＩＤ－ｔｒｕｓｔ－ｃｈａｉｎを独自に採用している。ＩＤベースのプライバシー保護の欠点の１つは、何らかのバックアップ手段がないと、破損したり紛失したりしたルートＣＡ証明書が永久に復元できなくなる可能性があるということである。これは、ＨｙｐｅｒＳｐｈｅｒｅが革新的なソリューションであるＱｕａｎｔｕｍ　ＳｅｑｕｅｎｔｉａｌＫｅｙまたはＱＳＫで対処する問題で、こちらについては

後段で説明する。

【０４３９】

ＨｙｐｅｒＳｐｈｅｒｅトランザクションの完全性

【０４４０】

超安全なグローバル電子商取引のためのプライバシーネットワークとして、トランザクションの完全性は、安全なネットワーク運用、ユーザ認証、アイデンティティトラストチェーン、確実なＨｙｐｅｒＣｏｎｔｒａｃｔの実行、検証可能な暗号通貨トランザクションに依存している。ＨｙｐｅｒＳｐｈｅｒｅにおけるトランザクションの完全性を確保するためには、（ｉ）詐欺的な（偽の）仮想通貨の生成を防止すること、（ｉｉ）二重支出や窃盗を目的としたブロックチェーン攻撃を防止すること、（ｉｉｉ）ＨｙｐｅｒＳｐｈｅｒｅのユーティリティやクリプトエコノミクスに影響を与える仮想通貨の価値の不安定化を回避すること、（ｉｖ）迅速なトランザクション処理と解決を確保することなど、いくつかの重要なメカニズムが必要となる。

【０４４１】

ＨｙｐｅｒＳｐｈｅｒｅの責任

【０４４２】

ＨｙｐｅｒＳｐｈｅｒｅの最終的な考慮点は、個人のプライバシー、財政的、倫理的、生態学的責任への原則的な献身である。ネットワーク暗号マスターキーを持たない断片化されたデータ転送を使用する完全分散型ネットワークであるＨｙｐｅｒＳｐｈｅｒｅの運用は、ユーザの機密性と個人のプライバシーを自然に保護する。動的なメッシュ化された伝送のため、パケットスニッフィング、監視、メタデータ監視を利用したプライバシー攻撃は、まったく生産的ではない。

【０４４３】

ＨｙｐｅｒＳｐｈｅｒｅでは、個人データはネットワークではなく、ユーザが所有する。ユーザがサービスプロバイダにアクセスまたは配布する権利を付与しない限り、加盟店は、ＨｙｐｅｒＳｐｈｅｒｅクライアントの個人情報を取得したり、知ったり、共有したり（または盗み取ったり）することはできない。さらに、仮名のリーフＣＡ証明書を使用することで、クライアントは個人データを一切公開したり、ＩＤ窃盗のリスクを負うことなく電子商取引を行うことができる。ＩＤベースのＣＡ証明書と高度な多要素認証および生体認証を組み合わせることで、ユーザのアカウント、ブロックチェーン、ウォレット、および個人データは、検査、データ収集、攻撃、または簒奪の対象とはならない。

【０４４４】

ＨｙｐｅｒＳｐｈｅｒｅは、ネットワークの合法的な使用において個人のプライバシーを保護するが、ＨｙｐｅｒＳｐｈｅｒｅの発明者および推進者は、犯罪行為、金融およびビジネス詐欺、プライバシー攻撃、窃盗、およびテロリズムのすべての行為を非難している。倫理的な通信ネットワークとして、ＨｙｐｅｒＳｐｈｅｒｅは、セッションの終着点であるＨｙｐｅｒＮｏｄｅｓ、つまり当事者間の取引が発生したり終了したりする場所の法的管轄権に従って、法の執行をサポートする。メッシュ化されたネットワーク上での断片的なデータ転送とステートレスなノード操作のため、ターミナスノード以外では、有用なコンテンツやメタデータは利用できない。

【０４４５】

環境面では、ＨｙｐｅｒＳｐｈｅｒｅは、世界初の最も環境に優しい仮想通貨の生成方法である。無駄なパズルやゲームを解くためだけに膨大なエネルギーを浪費し、貴重な資源を消費し、大きな二酸化炭素排出量を示すＰｏＷ暗号通貨とは異なり、ＨｙｐｅｒＳｐｈｅｒｅの暗号通貨はエネルギー効率が高く、ネットワークを介したデータ転送を共生メカニズムとして利用して、新しい暗号通貨を生成する。そのため、ＨｙｐｅｒＳｐｈｅｒｅのＰｒｏｏｆ－ｏｆ－Ｐｅｒｆｏｒｍａｎｃｅ補助合成と軽量ブロックチェーンは、Ｂｉｔｃｏｉｎ、Ｅｔｈｅｒｅｕｍ、およびそれらのサイドチェーン誘導体などのＰｒｏｏｆ－ｏｆ－Ｗｏｒｋ暗号通貨の１兆分の１（10^{-12}）のエネルギーを消費する。既存の、あるいは架空のトークンや暗号通貨の生成スキームと比較して、ＨｙｐｅｒＳｐｈｅｒ

ｅの補助的な暗号通貨の作成方法は、世界初のエコロジーフレンドリーで環境的に持続可能な仮想通貨を象徴している。最後に、ＨｙｐｅｒＳｐｈｅｒｅの可能性は、営利を目的とした商業的・個人的なプロジェクトに限定されるものではなく、すべての社会経済的グループに広がっている。たとえば、ＨｙｐｅｒＳｐｈｅｒｅは、研究を支援したり、新世代の起業家の資金調達を促進したり、さまざまな慈善事業や慈善事業を促進したりするために活用することができ、遺言や信託の実行、遺産計画における潜在的な役割などが考えられる。

【０４４６】

建築の概要

【０４４７】

要約すると、ここに開示されている「ＨｙｐｅｒＳｐｈｅｒｅ」は、デジタル通貨の完全性と不安定性、ネットワークセキュリティ、リアルタイムパフォーマンス、エネルギー効率の悪さといった問題を克服した、電子商取引のための新しいデュアルデジタルトークンベースの非中央集権型グローバル電子マーケットプレイスから構成されている。ＨｙｐｅｒＳｐｈｅｒｅは、グローバルな超安全なプライベートネットワーク（インターネットとは別個に独立したクラウドでありながら、同じハードウェア上に共存するクラウド）上で動作し、環境に優しいクラウドベースのコンピューティング、データストレージ、リアルタイム通信、安全なネットワーク接続デバイス、およびｅサービスをＨｙｐｅｒＳｐｈｅｒｅ内の任意のユーザに提供する。

【０４４８】

ＨｙｐｅｒＳｐｈｅｒｅの有益な機能

【０４４９】

仮特許に記載されているように、ＨｙｐｅｒＳｐｈｅｒｅは、インターネットのグローバルな機能と、一流のプロフェッショナルコミュニケーション、プライベートネットワーク、ＶＰＮ（仮想プライベートネットワーク）、ダイナミックリアルタイムネットワーク、グローバルテレフォニー、軍事レベルのサイバーセキュリティ、エンタープライズレベルの認証局、信頼されたトランザクション、本質的なプライバシー保護、プライベートブロックチェーンの最高の機能を融合させた、オープンソースのハイブリッドクラウドプラットフォームである。ＨｙｐｅｒＳｐｈｅｒｅは、リアルタイムデータルーティング、トラフィック管理、暗号通貨生成、ブロックチェーントランザクション実行の斬新な方法で、完全に独自のものとなっている。運用中は、タスクは自律的に実行され、ネットワークオペレータの支援を受けずに補助的に実行される。ルーティングは、事前に定義された（静的な）ルーティングテーブルに依存することなく、ネットワークの状況に基づいて動的に行われる。その代わりに、ＨｙｐｅｒＳｐｈｅｒｅは、ネットワークの伝播遅延を最小限に抑え、安全かつ迅速にトランザクションを実行するように設計された動的なメッシュルーティングを採用した完全な分散型システムを表している。

【０４５０】

ＨｙｐｅｒＳｐｈｅｒｅは、信頼性の高い固定およびバックボーンネットワーク、ダークファイバおよびバックホール、ワイヤレス、アドホックピアツーピア通信の有益な機能を、ＡＩベースの分散型マーケットプレイスを組み合わせることで、ネットワークのパフォーマンスとクライアントのパフォーマンスおよびコスト目標との間のベストマッチを動的に分析し、把握することができる。ネットワークの結節密度はユーザ数に応じて増加するため、「ＨｙｐｅｒＳｐｈｅｒｅを利用する人が多ければ多いほどパフォーマンスが向上する」という、固定型のネットワーククラウドとは正反対の特徴を持っている。

【０４５１】

ＨｙｐｅｒＳｐｈｅｒｅは、ネットワークネイティブ（組み込み型）の暗号通貨を生成して使用する点で特にユニークである。インターネットでは、従来の暗号通貨は、コストがかかり、エネルギーを浪費するＰｒｏｏｆ－ｏｆ－Ｗｏｒｋの謎解きを使用して「採掘」されていた。これとは対照的に、ＨｙｐｅｒＳｐｈｅｒｅでの仮想通貨の生成は、図４７に示すように、データパケットがクラウドを通過する際に付随的に生成される「鋳造」

がある。ＰｏＷの採掘者の不確実なリターンとは異なり、ＨｙｐｅｒＳｐｈｅｒｅのリソースプロバイダは、あらかじめ交渉されたＨｙｐｅｒＣｏｎｔｒａｃｔｓ９６４に従って、完了したトランザクションをサポートするための保証された報酬を受け取る。コインの生成はネットワークの運用と並行して行われるため、暗号通貨の鋳造には、通信やコンピューティングのタスクに必要な有用な作業を完了させるために費やされるエネルギーを超えて、事実上、追加のエネルギーは一切使用されることはない。エネルギー効率が良く、環境に優しいだけでなく、クラウドでのデータ転送によってネットワークネイティブのブロックチェーンを動的に生成することで、偽造を防ぐことができる。動的ブロックチェーン合成を用いた暗号通貨の生成は、ＨｙｐｅｒＳｐｈｅｒｅの外では真似のできないノード間のデータ転送プロセスで構成されている。また、暗号通貨はネットワークネイティブであるため、ブロックチェーンをインターネットのハッキング、盗難、詐欺、オンライン取引のリスクにさらすことなく、ＨｙｐｅｒＷａｌｌｅｔｓに転送して保持し、ＨｙｐｅｒＳｐｈｅｒｅで再利用することができる。

【０４５２】

ＨｙｐｅｒＳｐｈｅｒｅアクセスは、特殊なハードウェアを必要とせず、完全にソフトウェアベースで提供されている。スマートフォン、ノートブック、デスクトップＰＣ、ゲームプラットフォーム、スマートＴＶ、ＩｏＴなどのユーザインターフェイスは、Ｗｉｎｄｏｗｓ（登録商標）、ＭａｃＯＳ（登録商標）、Ｌｉｎｕｘ（登録商標）、Ｕｎｉｘ（登録商標）、ｉＯＳ（登録商標）、Ａｎｄｒｏｉｄ（登録商標）などの主要なオペレーティングシステムをサポートしている。企業、企業、研究機関、大学は、個人のデバイスを介してＨｙｐｅｒＳｐｈｅｒｅにアクセスし、プライベートサーバやネットワークへのアクセスを容易にすることができる。つまり、便利で費用対効果の高いＢＹＯＤ（Ｂｒｉｎｇ－Ｙｏｕｒ－Ｏｗｎ－Ｄｅｖｉｃｅ）接続を可能にすると同時に、企業のＩＴ部門のセキュリティ規定や制御をサポートする。また、デバイスのクラスタは、ＨｙｐｅｒＳｐｈｅｒｅ内のプライベートネットワークとして、つまり、公共の場でホストされているプライベートネットワークとしても動作する。ＨｙｐｅｒＳｐｈｅｒｅのユーザは、次のような役割を含め、いくつかの方法でトランザクションを行うことができる。

・リソース提供者－ＨｙｐｅｒＮｏｄｅポータルソフトウェアを１つ以上のデバイスにダウンロードすることで、個人、企業、機関がＨｙｐｅｒＳｐｈｅｒｅにリソースを提供し、その対価としてＨｙｐｅｒＣｏｉｎ暗号通貨を獲得することができる。

・加盟店およびサービスプロバイダ－ＨｙｐｅｒＳｐｈｅｒｅ　ＡＰＩで生成されたアプリケーションまたはユーザインターフェイスを作成することで、加盟店およびサービスプロバイダ９５８は、通信、コンピューティング、ストレージ、クラウド接続デバイス、またはｅサービスや製品を顧客に提供することができる（顧客がＨｙｐｅｒＳｐｈｅｒｅのクライアントではない場合でも）。

・ユーザ－加盟店やサービスプロバイダ９５８の顧客であるユーザ９５９は、ＨｙｐｅｒＳｐｈｅｒｅのリソースを利用して、フィアット通貨での支払いや、獲得した、または商業的に取得したＨｙｐｅｒＣｏｉｎ仮想通貨を使用することができる。

【０４５３】

階層的には、インターネット上で動作するソフトウェアをＯＴＴ（Ｏｖｅｒ－ｔｈｅ－Ｔｏｐ）アプリケーションとして採用するのではなく、ＨｙｐｅｒＳｐｈｅｒｅはインターネットと共存し、リソース、物理ネットワーク、ラストマイルキャリア、データリンクを共有している。この意味で、ＨｙｐｅｒＳｐｈｅｒｅは本質的にインターネットの「オンザサイド」（ＯＴＳ）で動作し、部分的に重複するピアネットワークを表現している。さらに、ＨｙｐｅｒＳｐｈｅｒｅは、クラウドとユーザのデバイス間のラストマイル接続には不可知であり、ＷｉＦｉ、イーサネット、ＤＯＣＳＩＳ－３、ワイヤレス（３Ｇ／ＬＴＥ、４Ｇ、５Ｇ）など、あらゆる媒体とシームレスに互換性がある。優れたセキュリティと内蔵されたネイティブ暗号通貨に加え、ＨｙｐｅｒＳｐｈｅｒｅは「プライバシーネットワーク」として、ネットワーク固有の仮名ＩＤを独自に採用し、個人アカウント情報を保護する。デジタル署名されたＣＡ証明書を使用して、個人的なトランザクションの実

行、ＨｙｐｅｒＣｏｎｔｒａｃｔｓのオープン、ネットワークリソースの配信、暗号通貨の取引を行うことで、ＨｙｐｅｒＳｐｈｅｒｅのユーザは、潜在的な攻撃に自分の正体を晒すことなく、電子商取引を行うことができる。これは、レプリカントブロックチェーンオブザーバーセグメント（ＲＢＯＳ）１０６３（図５６）と呼ばれる、ブロックチェーンのバックトレースやプライバシーの漏洩を防ぎながらトランザクションを検証するために使用される限られた長さのブロックチェーンミラーである。もう１つの発明的要素であるワンタイムトランザクショントークン（ＯＴ^{3}）１０４１（図５５）は、単一使用の一時的なトランザクション支払いメカニズムを採用しており、支払者のサードパーティトランザクションプロセッサが支払者のブロックチェーンから個人情報を盗み出すことを防ぐ。電子商取引において、ＨｙｐｅｒＳｐｈｅｒｅはインターネット上で以下のような多くのメリットを提供する。

・リアルタイムの音声・映像コンテンツを匿名、安全、プライベートに転送する機能：通信やセキュアなメッセンジャーサービスを提供するサービスプロバイダに必要な機能。

・電子メール、データベース、プライベートメディアコンテンツ、ソフトウェアを含む、匿名で安全かつプライベートに高品位なデータファイルを転送する機能：安全な電子メール、データベースサービス、顧客のコンタクト管理、オンラインコラボレーションプラットフォームのプロバイダが必要とする機能。

・研究者やオンラインクラウドコンピューティングプロバイダを支援する分散型クラウドコンピューティングの実行を匿名、安全、非公開で派遣、管理、照合する機能。

・データを匿名、安全、そしてプライベートに転送、保存、リコールする機能は、ビッグデータ分析に必要な機能であり、オンラインおよびクラウドストレージサービスの提供者によって必要とされている。

・クラウド接続されたデバイスに対するセキュリティとプライバシー攻撃を防ぎながら、クラウド接続されたデバイスのコマンドアンドコントロール（Ｃ＆Ｃ）指示を匿名、安全、非公開で伝送する機能：ＩｏＴデバイスのユーザやサービスプロバイダにとって重要な機能とプライバシー機能。

・ネットワークネイティブの動的ブロックチェーンを構成する仮想通貨仲介者を使用して、金融取引、支払い、または送金を安全かつ偽名で実行する能力。

・加盟店向けの様々な電子サービスを匿名で、安全に、そしてプライベートに実行することができる。

・ユーザの正体を明らかにしたり、個人情報や個人情報への不正アクセスや販売を可能にすることなく、仮名データの使用を促進し、パーソナライズされたＡＩベースのレコメンデーションを促進する機能。ＨｙｐｅｒＳｐｈｅｒｅでは、ユーザは個人データを所有しており、加盟店やネットワークではない。

・ＨｙｐｅｒＳｐｈｅｒｅクラウド内にセキュアに展開された加盟店が運営するハイパーセキュアプライベートオーバーレイネットワークを形成する機能である。例としては、完全にサンドボックス化された処理を使用して企業および個人のプライバシーとデータの整合性を保護する。

・ラストマイルサブネットを動的にトンネルしてサービス拒否攻撃を回避したり、安全ではないネットワークやクラウドにユーザの身元を晒すことなくインターネットにアクセスしたりする機能である。

・個人ＣＡ証明書アイデンティティベースの所有権検証とネットワークベースの盗難防止規定を使用して、様々な形態の暗号通貨（ハイパーコイン、ビットコイン、イーサを含む）を安全に受け入れ、転送し、プライベートなハイパーウォレットに保持する機能。

・ＨｙｐｅｒＳｐｈｅｒｅの加盟店やスタートアップにＢｌｏｃｋｃｈａｉｎ－ａｓ－ａ－Ｓｅｒｖｉｃｅ（ＢａａＳ）を提供できること。

・ブロックチェーンをベースにした様々な企業、サービス、スタートアップのためのプラットフォームとして、仮想通貨やトークンの提供をサポートすることができる。

前述の特徴は、ＨｙｐｅｒＳｐｈｅｒｅの無数の有益な特徴のほんの一部を説明したものである。

【０４５４】
ＨｙｐｅｒＳｐｈｅｒｅビジネスサービス
【０４５５】
開示されているように、ＨｙｐｅｒＳｐｈｅｒｅは、オープンソースの電子通信および電子商取引環境であり、参加者は、需要を創造し、取引およびその需要を満たすために必要なリソースを供給することによって積極的に貢献している。非営利のＬｉｎｕｘ（登録商標）　Ｆｏｕｎｄａｔｉｏｎがセキュアコンピューティングのためのオープンソースのプラットフォームを提供しているのと同様の役割を果たすように、ＨｙｐｅｒＳｐｈｅｒｅは、ハイパーセキュアネットワーキング、通信、クラウドコンピューティング、および電子商取引のための完全に分散化されたオープンソースのプライバシープラットフォームを容易にするように設計されている。比喩的に言えば、ＨｙｐｅｒＳｐｈｅｒｅは、通信と電子商取引のＬｉｎｕｘ（登録商標）になるように設計されている。
・クラウド型のハイパーセキュア通信。
・分散コンピューティング。
・クラウドデータの保管とデータバックアップを細分化。
・ネットワークに接続された（ＩｏＴ）セキュアなデバイス、および
・無数のオンライン電子サービス、オンライン、電子取引。
【０４５６】
ハイパースフェリッククラウド通信
【０４５７】
ＨｙｐｅｒＳｐｈｅｒｉｃクラウド通信において、加盟店は、ネットワークの独自のセキュリティを利用して、個人をターゲットとした脆弱性（企業や役員、役員など）を含む個人、企業、法人に対して、ＨｙｐｅｒＳｅｃｕｒｅテレフォニー、電話会議通話、テキストメッセージング、ライブビデオ、ハイパーセキュア電子メールを提供することができる。また、ＨｙｐｅｒＳｐｈｅｒｅを利用して、政府やその関係者、警察、緊急サービス、港湾局、国防、国土安全保障などに向けて、ＦＩＰＳ－１４０に準拠した専門的な通信サービスを提供することもできる。企業は、大企業内のプライベートビジネスネットワークや、輸送・海運業界でＨｙｐｅｒＳｐｈｅｒｅを利用することができる。
【０４５８】
ハイパースフェリッククラウドコンピューティング
【０４５９】
ＨｙｐｅｒＳｐｈｅｒｉｃクラウドコンピューティングでは、加盟店は、ＨｙｐｅｒＳｐｈｅｒｅを利用して、小規模企業や公認会計士向けにローカルソースのオンラインビジネスコンピューティングを提供したり、病院や診療所向けに医療画像の解析のためのクラウドコンピューティングサービスを提供したりすることができる。ビッグデータプロジェクトでは、ＨｙｐｅｒＳｐｈｅｒｅの分散コンピューティング機能により、企業、政府機関、研究機関に無制限のコンピューティングリソースを、クライアントの予算に応じた価格とパフォーマンスで提供することができる。ビッグデータプロジェクトには、疫学研究、ＤＮＡ解析、ヒトゲノム研究、気候・気象モデリング、マクロ経済学、地殻変動や火山活動の予測、ＮＥＯ（地球近傍天体）の特定、高エネルギー物理学や素粒子研究、ＳＥＴＩ（地球外知的生命体の探索）などの慈善事業などがある。
【０４６０】
ＨｙｐｅｒＳｐｈｅｒｉｃクラウドストレージ
【０４６１】
ＨｙｐｅｒＳｐｈｅｒｉｃの分散型データクラウドストレージでは、個人の写真やビデオのハイパーセキュアな細分類されたストレージ、金融データの企業アーカイブ、保険の医療記録や医療画像、税務や会計記録、企業のＩＴバックアップサービス、図書館のコンテンツのアーカイブストレージ、映画のアーカイブ、希少書のアーカイブストレージなど、個人、企業、政府、市民のクライアントに低コストで分散型の大規模なデータストレージを提供することができる。データのデジタルコンテンツはネットワーク上に拡散され、

別の場所に保存されているため、記憶装置や施設の手入れに成功しても何の有用な情報も得られないという利点がある。さらに、データの細分化がどのように発生したかについての情報は、保存されたメディアファイルには含まれていない。

【０４６２】

ＨｙｐｅｒＳｐｈｅｒｉｃネットワークに接続されたデバイス

【０４６３】

ＨｙｐｅｒＳｐｈｅｒｉｃネットワーク接続デバイスでは、加盟店はＨｙｐｅｒＳｐｈｅｒｅを採用して、家庭、商業、輸送、政府機関、インフラストラクチャのアプリケーションで使用されるデバイスに安全な接続を提供することができる。インターネットに接続されたデバイス（Ｉｎｔｅｒｎｅｔ　ｏｆ　ＴｈｉｎｇｓまたはＩｏＴと呼ばれる）は、ハッキングやさまざまなＩＤ攻撃の対象となることはよく知られている。ＨｙｐｅｒＳｐｈｅｒｅ対応のＷｉＦｉハブを採用することで、ＨｙｐｅｒＳｐｈｅｒｅ　ｏｆ　Ｔｈｉｎｇｓ（ＨＳｏＴ）接続デバイスは、外部からの侵入や制御の乗っ取りを防ぐことができる。パーソナルＨＳｏＴ接続デバイスには、防犯カメラやホームセキュリティシステム、制御用ＩｏＴデバイスやパーソナルアシスタント、家電製品、サーモスタット、エンターテイメントデバイスやホームエンターテイメントネットワーク、音声起動型デバイス、ラジコンスピーカーなどがある。

【０４６４】

職場でのＨＳｏＴ接続デバイスの用途には、共有ドライブ、プリンター、会議用ディスプレイ画面、ＨＶＡＣシステム、照明とブラインド制御、アラームシステム、セキュリティシステム、ビルメンテナンスなどが含まれる。ファクトリーオートメーションや発電所では、ネットワーク接続されたデバイスには、監視カメラ、センサー、モニター、ロック、フェイルセーフシステム、バックアップシステム、ガス・空気モニター、バイオセンサー、非常照明、非常システムなどが含まれる。インフラストラクチャプリケーションには、カメラ、交通流センサー、交通信号機、高速道路のメータリングおよび通勤車線照明、大量輸送機関のセキュリティセンサ、無線コントローラパーキングメータ、スマートペイフォンなどが含まれる。コネクティッドカーや自動走行車は、セキュリティとプライバシーが厳密に重要なネットワーク接続デバイスやもう一つの幅広いクラスのアプリケーションを表している。車載およびスマートハイウェイのアプリケーションには、車両間（Ｖ２Ｖ）、車両間インフラ（Ｖ２Ｘ）、さらに広くは車両間（Ｖ２Ｅ）通信が含まれる。

【０４６５】

ＨｙｐｅｒＳｐｈｅｒｉｃ　ｅ－Ｓｅｒｖｉｃｅｓ

【０４６６】

ＨｙｐｅｒＳｐｈｅｒｉｃ　ｅ－ｓｅｒｖｉｃｅｓでは、加盟店はＨｙｐｅｒＳｐｈｅｒｅの本質的なセキュリティを収益化して、銀行、輸送、通信、エネルギー、セキュリティ、財務、医療、緊急対応、防衛用途など、リスクの高い業界に安全なサービスを提供することができる。アプリケーションには、クレジットカードリーダー、リモートＡＴＭ、モバイルバンキングおよび決済、ディスパッチャベースの専門的な通信サービス、ＨＩＰＡ準拠の医療機器およびファイル、軍事および政府アプリケーション向けのＦＩＰＳ－１４０準拠サービス、ケーブルおよび衛星テレビ加入者サービスの代替としてのオンラインＤＲＭ準拠の動画配信など、業界特有のカスタマイズされたサービスが含まれる。上記のようなアプリケーションでは、ＨｙｐｅｒＳｐｈｅｒｅを使用することで、インターネットベースの通信や商取引では保証が困難であったり、不可能であったりするような、安全な取引を顧客ベースに提供することが可能になる。

【０４６７】

その他のＨｙｐｅｒＳｐｈｅｒｅの機能

【０４６８】

ＨｙｐｅｒＳｐｈｅｒｅのその他のユニークな発明的特徴としては、暗号通貨生成のためのグリーンな方法、パブリック－プライベートネットワークとしてのインターネットとの共存、分散型データパケットルーティングのための斬新な方法、ユーザのアイデンティ

ティと資産所有権のプライバシー保護を容易にする能力、および斬新なデュアル仮想通貨ベースのクリプト経済システムなどが挙げられる。インターネットと比較した場合、ＨｙｐｅｒＳｐｈｅｒｅは電子商取引においてユニークな能力を持ち、以下のような特徴を持つハイパーセキュアなプラットフォームである。
・環境に優しい自律接続型の暗号通貨＆デジタルトークン
・官民完全分散型リアルタイムネットワーク
・ステートレスメッシュネットワーク上での分散型データパケットルーティング
・マスター暗号鍵を持たない分散型ＤｙＤＡＧネットワーク
・プライバシーが保護されたアイデンティティと所有権
・バンクレス取引のための組み込み型暗号通貨（ＨｙｐｅｒＳｐｈｅｒｅ　ｃｒｙｐｔｏｅｃｏｎｏｍｉｃｓ）

【０４６９】
ハイパースフィア市場

【０４７０】
ＨｙｐｅｒＳｐｈｅｒｅマーケットプレイス

【０４７１】
ＨｙｐｅｒＳｐｈｅｒｅは、Ｅコマースプラットフォームとして、ハードウェア、インフラストラクチャ、研究開発、サイバーセキュリティ開発への設備投資なしに、リアルタイムのサイバーセキュアなネットワーク通信とクラウドコンピューティングに取り組むことができる。ＨｙｐｅｒＳｐｈｅｒｅの加盟店およびサービスプロバイダは、個人所有のリースや契約上の義務であるサーバ、ＶＰＮ、または専用のダークファイバチャネルの容量に依存するのではなく、ＨｙｐｅｒＣｏｎｔｒａｃｔｓを使用して、独立したリソースプロバイダ（ＨｙｐｅｒＮｏｄｅの所有者）を募集し、契約することで、ネットワーク通信を容易にし、取引を実行することができる。人工知能と機械学習を使用して、分散型のＨｙｐｅｒＳｐｈｅｒｅ　Ｍａｒｋｅｔｐｌａｃｅが、各契約を完了させるために必要なＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダを勧誘し、調達する。

【０４７２】
図４８に示すように、ＨｙｐｅｒＣｏｎｔｒａｃｔｓ９６４は、ＨｙｐｅｒＳｐｈｅｒｅの契約に精通したソフトウェアエンジニアが「ハードコーディング」することもでき、ＡＰＩインターフェイス９４８やテンプレートを使用して自動または準自動で生成することもできる。これらのＨｙｐｅｒＳｐｈｅｒｅサービスユーティリティ９４９は、ＨｙｐｅｒＣｏｉｎの販売、資産の転送、ＰＯＳ取引、デバイスへのＨｙｐｅｒＮｏｄｅｓのインストール、ＨｙｐｅｒＮｏｄｅクラスタの作成、ＨｙｐｅｒＷａｌｌｅｔｓへの署名など、一般的に実行される特定のプロセスを、実行可能なコードを一4致させるために、ＨｙｐｅｒＳｐｈｅｒｅは、分散型の電子マーケットプレイスであるＨｙｐｅｒＳｐｈｅｒｅ　Ｍａｒｋｅｔｐｌａｃｅを利用している。ＨｙｐｅｒＳｐｈｅｒｅ　Ｍａｒｋｅｔｐｌａｃｅの運用では、リソースを募集し、すべての当事者が相互に納得できる条件を交渉する。契約解決プロセスに参加するＨｙｐｅｒＮｏｄｅｓは、定義上、ＨｙｐｅｒＣｏｎｔｒａｃｔの当事者ではない。交渉が完了すると、ブローカーノードは、実行可能な契約を仲介する役割を果たしたとして、ＨｙｐｅｒＣｏｎｔｒａｃｔに追加される。ＨｙｐｅｒＭｅｔａｌの報酬は、ＨｙｐｅｒＣｏｎｔｒａｃｔが成功裏に実行された場合にのみ支払われる。

【０４７３】
ＨｙｐｅｒＳｐｈｅｒｅの加盟店やサービスプロバイダの要件を、ＨｙｐｅｒＣｏｎｔｒａｃｔで指定された条件や成果物を満たすことを望むリソースプロバイダと一致させるために、ＨｙｐｅｒＳｐｈｅｒｅは、分散型の電子マーケットプレイスであるＨｙｐｅｒＳｐｈｅｒｅ　Ｍａｒｋｅｔｐｌａｃｅを利用している。ＨｙｐｅｒＳｐｈｅｒｅ　Ｍａｒｋｅｔｐｌａｃｅの運用では、リソースを募集し、すべての当事者が相互に納得できる条件を交渉する。契約解決プロセスに参加するＨｙｐｅｒＮｏｄｅｓは、定義上、ＨｙｐｅｒＣｏｎｔｒａｃｔの当事者ではない。交渉が完了すると、ブローカーノードは、実行可

能な契約を仲介する役割を果たしたとして、ＨｙｐｅｒＣｏｎｔｒａｃｔに追加される。ＨｙｐｅｒＭｅｔａｌの報酬は、ＨｙｐｅｒＣｏｎｔｒａｃｔが成功裏に実行された場合にのみ支払われる。

【０４７４】

リソースプロバイダ（ハイパーノード）

【０４７５】

ＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダは、ＨｙｐｅｒＣｏｎｔｒａｃｔｓ（加盟店が提供するタスク、成果物および報酬を説明する電子契約）に規定されたパフォーマンス要件に従って、通信機能、コンピューティング機能、ストレージ機能を加盟店に提供する。ＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダとは、ＨｙｐｅｒＳｐｈｅｒｅにアクセスするためのソフトウェアベースのポータルであるＨｙｐｅｒＮｏｄｅの運用をホストする、ネットワークに接続された通信デバイスのことである。ＨｙｐｅｒＮｏｄｅｓは、信頼できるアプリストアやＨｙｐｅｒＳｐｈｅｒｅのウェブサイトからダウンロードできる。身元確認のために、ＨｙｐｅｒＮｏｄｅの所有者は、デジタル署名を使用して、特定の親のＣＡ証明書およびＩＤ信頼チェーンによる所有権を確認する。

【０４７６】

稼働中、完了したトランザクションに参加しているアクティブなＨｙｐｅｒＮｏｄｅは、その貢献度に応じて直ちにＨｙｐｅｒＣｏｉｎ暗号通貨を獲得する。貢献の価値と報酬は、市場の需要だけでなく、ＨｙｐｅｒＮｏｄｅのホストデバイスの本質的な能力、スピード、信頼性などにも左右される。ＨｙｐｅｒＮｏｄｅｓは、単一のハードウェアホスト上での動作に限定されるものではなく、特定の永久ブロックチェーンおよび親ＣＡ証明書にリンクされた共有アカウントを形成するデバイスのクラスタで構成されていてもよい。具体的には、ＨｙｐｅｒＳｐｈｅｒｅでは、リソースプロバイダは、ホストの性能、速度、容量、およびアップタイム能力に基づいて、ＨｙｐｅｒＮｏｄｅ所有者の４つの層に細分化されている。

・１stＴｉｅｒ：Ａｚｕｒｅ、ＡＷＳ、ＧＷＳ、ＩＢＭクラウドサービスなど、高速で大容量のグローバルサーバネットワークが高可用性を発揮する。

・２ndＴｉｅｒ：ＩＳＰ、ケーブルネットワーク、ビットコインマイナファームなどの高速ローカルサーバクラウドなど、

・3rdＴｉｅｒ：パソコン、ゲーム機、スマートテレビ、ルータなどの中速交流電源のパソコンやＣＰＵ、そして

・４thＴｉｅｒ：ノートパソコン、タブレット、スマートフォン、ゲーム、家電などのモバイルＩｏＴデバイスなど

【０４７７】

リソースプロバイダの特定の層への加盟店のアクセスと価格設定は、加盟店のＨｙｐｅｒＣｏｎｔｒａｃｔに規定されているコストとパフォーマンスの要件、および需給の市場力学によって決定される。ＨｙｐｅｒＣｏｎｔｒａｃｔの実行中、担保された支払い（ＨｙｐｅｒＭｅｔａｌまたはＨｙｐｅｒＣｏｉｎで行われる）は、アカウント所有者の対応するブロックチェーン上に記録される。ＨｙｐｅｒＣｏｎｔｒａｃｔが完了し、陪審員による確認が行われると、ＨｙｐｅｒＮｏｄｅは、ＨｙｐｅｒＣｏｎｔｒａｃｔで指定された契約に従ってＨｙｐｅｒコインを採掘する。

【０４７８】

ＨｙｐｅｒＳｐｈｅｒｅ加盟店（サービスプロバイダ）

【０４７９】

ハイパーコントラクト

【０４８０】

ＨｙｐｅｒＳｐｈｅｒｅ内でのトランザクションは、ＨｙｐｅｒＮｏｄｅのリソースプロバイダからの成果物の提供を求め、契約上規定するために、ＨｙｐｅｒＳｐｈｅｒｅの加盟店やサービスプロバイダが発行するＨｙｐｅｒＣｏｎｔｒａｃｔｓと呼ばれる、デジタルで指定された手続きを使用して行われている。図４７に示すように、すべてのＨｙｐ

ｅｒＣｏｎｔｒａｃｔは、ジョブの仕様９６４ａと、契約の成功に参加したリソースプロバイダ（陪審員やバックアップノードを含む）への支払いのために予約された報酬９６４ｂ、つまり誓約された報酬を記述したＨｙｐｅｒＭｅｔａｌまたはＨｙｐｅｒＣｏｉｎの報酬契約から構成されている。透明性を提供し、ブロックチェーン攻撃を混乱させるために、コンセンサスベースの検証に使用される陪審員には、公開メンバーと隠蔽されたメンバーの両方が含まれる。ジョブリソースを募り、参加を促すために、ＨｙｐｅｒＳｐｈｅｒｅの加盟店やサービスプロバイダは、ジョブの仕様に沿ってＨｙｐｅｒＣｏｎｔｒａｃｔに報酬の契約書を添付する。

【０４８１】

契約は、一度取り付けられると、加盟店のブロックチェーンから一時的に隔離され、削除され、契約の完了または失敗までの間、実質的にデジタルエスクローに保持される。次に加盟店は、ＨｙｐｅｒＮｏｄｅｓによって実行されるＡＩベースのアルゴリズムを使用した分散型マーケットであるＨｙｐｅｒＳｐｈｅｒｅ　Ｍａｒｋｅｔｐｌａｃｅに提案書を提出する。入札プロセスは、さまざまなサイレントオークション手法を用いて反復的に行われ、参加者、陪審員、バックアップなどの必要なリソースがすべてコミットされるまで継続される。承諾された契約は、指定された通りに実行される。報酬も同様に、契約上の義務に応じて支払われる。

【０４８２】

シェアリングエコノミー

【０４８３】

ＨｙｐｅｒＳｐｈｅｒｅ自体が、通信やトランザクションが発生する電子的なフレームワークおよびエコスフィアとして機能する。異種分散型ネットワークを構成するＨｙｐｅｒＳｐｈｅｒｅクラウドは、パブリッククラウドや営利目的のプライベートクラウドと同じサーバ、マイクロ波タワー、衛星、ファイバネットワーク、ダークファイバチャネル、ルータを使用して、インターネットと共存している。同様に、ＨｙｐｅｒＳｐｈｅｒｅの「ラストマイル」は、ローカルＩＳＰのイーサネット回線やファイバ回線、ケーブルネットワーク、２Ｇ、３Ｇ／ＬＴＥ、４Ｇ、５Ｇネットワークを経由してルーティングされており、新たなインフラストラクチャや専用のインフラストラクチャを導入する必要はない。ユーザのデバイスへの最後のリンクには、イーサネット、ＷｉＦｉ、携帯電話、またはユーザが参加するアドホックピアツーピア（Ｐ２Ｐ）や車両間（Ｖ２Ｖ）ネットワークなど、利用可能な接続性があれば何でも利用できる。ＨｙｐｅｒＳｐｈｅｒｅでは、ネットワーク操作は、中央の権限もマスター暗号化キーも管理するセキュリティクレデンシャル情報もない、完全に分散化された操作で構成されている。つまり、ユーザは、ＨｙｐｅｒＳｐｈｅｒｅがどのようにして通信やトランザクションのセキュリティとプライバシーを実現しているのかを知ることができない。

【０４８４】

加盟店（サービスプロバイダ）、リソースプロバイダのどちらでも、ユーザは、ＨｙｐｅｒＮｏｄｅと呼ばれるソフトウェアまたはファームウェアベースのネットワークポートをインストールするだけで、ＢＹＯＤ（Ｂｒｉｎｇ－ｙｏｕｒ－ｏｗｎ－ｄｅｖｉｃｅ）ハードウェアを使用してＨｙｐｅｒＳｐｈｅｒｅに接続することができる。ＨｙｐｅｒＮｏｄｅは、デバイスがＨｙｐｅｒＳｐｈｅｒｅにアクセスし、他のＨｙｐｅｒＮｏｄｅ所有者にアクセスできるようにするだけでなく、ネットワーク内の通信ノードとしても機能する。ＨｙｐｅｒＳｐｈｅｒｅに新しいＨｙｐｅｒＮｏｄｅが接続されるたびに、ＨｙｐｅｒＳｐｈｅｒｅのサイズ、密度、容量、性能が拡張される。この意味で、ＨｙｐｅｒＳｐｈｅｒｅは、ユーザ、商人、リソースプロバイダによって構成されるネットワークである「Ｔｈｅ　ｐｅｏｐｌｅ's　ｎｅｔｗｏｒｋ」なのである。

【０４８５】

大規模なクラウドオペレーターであるＡＷＳ、ＧＣＰ、Ａｚｕｒｅ、Ｆａｃｅｂｏｏｋ、およびグローバルな電話事加盟店であるＡＴ＆Ｔ、ＮＴＴ、Ｖｅｒｉｚｏｎ、Ｔ－Ｍｏｂｉｌｅとは異なり、ＨｙｐｅｒＳｐｈｅｒｅは、ホストするビジネストランザクション

の当事者でも受益者でもない。その代わり、加盟店は、データの転送や所定のタスクの実行に関与するＨｙｐｅｒＮｏｄｅｓに対してのみ支払いを行うことで、リソースに資金を提供する。特定の種類のトランザクションを処理するための少額のトランザクション料金を除いて、ＨｙｐｅｒＳｐｈｅｒｅは報酬を受け取ったり、そのプラットフォーム上で実行されるサービスの価格を設定したりしない。その代わり、ＨｙｐｅｒＳｐｈｅｒｅのサービスのコストは、ＨｙｐｅｒＮｏｄｅの所有者であるリソースプロバイダと、ネットワーク、ストレージ、またはコンピューティングリソースを求める加盟店やサービスプロバイダとの間の交渉によって決定される。

【０４８６】

ある実施形態では、これらのタスクは、人工知能（ＡＩ）ベースのマーケットプレイスを介して、利用可能な（オンラインの）ＨｙｐｅｒＮｏｄｅｓに割り当てられ、様々なリソースプロバイダのキャパシティや能力と加盟店の要求をマッチングさせる。別の実施形態では、実行されるべきタスクが特定され、そのようなサービスの実行に同意する参加ＨｙｐｅｒＮｏｄｅｓがＨｙｐｅｒＣｏｎｔｒａｃｔと呼ばれるデジタル契約で割り当てられる。第３の実施形態では、ＨｙｐｅｒＣｏｎｔｒａｃｔは、ＡＩベースのＨｙｐｅｒＳｐｈｅｒｅ Ｍａｒｋｅｔｐｌａｃｅで電子的に交渉される。ＨｙｐｅｒＣｏｎｔｒａｃｔｓを提供するＨｙｐｅｒＮｏｄｅｓは、パフォーマンス、信頼性、容量、可用性によって分類された４つの階層のＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダのうちの１つで構成されている。

・Ｔｉｅｒ－１リソースプロバイダ：Ｔｉｅｒ－１リソースプロバイダは、信頼性が高く、大容量、高帯域幅のクラウド通信、クラウドコンピューティング、およびクラウドストレージのサプライヤーで構成されている。Ｔｉｅｒ－１プロバイダは、ＨｙｐｅｒＳｐｈｅｒｅマーケットプレイスのジョブ契約、つまりＨｙｐｅｒＣｏｎｔｒａｃｔｓを利用して、最高のＨｙｐｅｒＭｅｔａｌ支払い価格でプレミアムなパフォーマンスを提供している。Ｔｉｅｒ－１リソースには、ＡＷＳ、Ａｚｕｒｅ、ＧＣＰなどがある。Ｔｉｅｒ－１リソースは、「パフォーマンスが保証され、支払いが保証されている」というビジネスモデルで運営されており、ジョブ完了時にＨｙｐｅｒＭｅｔａｌをＨｙｐｅｒＣｏｉｎに変換し、ＨｙｐｅｒＣｏｉｎを即座にフィアット通貨に交換する可能性が高い。統計的には、Ｔｉｅｒ－１リソースプロバイダは、商業的な有料サービスを提供するプレミアムＨｙｐｅｒＳｐｈｅｒｅ加盟店や、音声やライブビデオなど、遅延や伝搬遅延に敏感なリアルタイムアプリケーションなど、パフォーマンスが要求されるアプリケーションにサービスを提供することが期待されている。

・Ｔｉｅｒ－２リソースプロバイダ：Ｔｉｅｒ－２リソースプロバイダは、グローバルな遍在性や可用性が保証されていないが、大容量かつ高帯域幅のコンピューティングプラットフォームとインターネットプロバイダで構成されている。Ｔｉｅｒ－２リソースプロバイダは、Ｔｉｅｒ－１リソースプロバイダと比較して競争力のある商業的に積極的な料金設定がされており、高スループットのクラウド接続、高速なクラウド接続コンピューティング、大容量ストレージを提供する。例としては、地元のＩＳＰ、ケーブル通信事加盟店、大学のサーバファーム、再目的化された大容量ビットコイン採掘加盟店などが挙げられる。ＨｙｐｅｒＳｐｈｅｒｅマーケットプレイスで交渉されるＴｉｅｒ－２リソースプロバイダ向けのＨｙｐｅｒＣｏｎｔｒａｃｔｓは、固定報酬とボーナス報酬のＨｙｐｅｒＭｅｔａｌ報酬の組み合わせで構成されている。ＨｙｐｅｒＭｅｔａｌのボーナス報酬は、市場競争やプロバイダの業績によって異なる。ＨｙｐｅｒＣｏｎｔｒａｃｔの履行のためにＨｙｐｅｒＭｅｔａｌで支払いを受けると、受け取ったＨｙｐｅｒＭｅｔａｌは自動的に、ＨｙｐｅｒＳｐｈｅｒｅの互換性のある仮想通貨であるＨｙｐｅｒＣｏｉｎｓに変換される。Ｔｉｅｒ－２ＨｙｐｅｒＮｏｄｅｓは、投機目的でＨｙｐｅｒＣｏｉｎを保有することができるが、Ｔｉｅｒ－２ＨｙｐｅｒＮｏｄｅｓは、ＨｙｐｅｒＣｏｉｎの価格変動を避けるために、ＨｙｐｅｒＣｏｉｎをすぐに再利用したり、現金化したりする傾向がある。また、Ｔｉｅｒ－２リソースプロバイダは、（ｉ）ＨｙｐｅｒＣｏｉｎを現在の市場レートでフィアット通貨に交換し、（ｉｉ）現在のクオンツ（ビットレート）コストで

ＨｙｐｅｒＭｅｔａｌを購入するというタンデム通貨交換プロセスを通じて、ＨｙｐｅｒＣｏｉｎをＨｙｐｅｒＭｅｔａｌに交換することを選択することもできる。なお、ハイパーコインを直接購入するためには、「オプション契約」に関する政府の厳しい規制を受けなければならない。

・Ｔｉｅｒ－３リソースプロバイダ：Ｔｉｅｒ－３リソースプロバイダは、パーソナルコンピュータ、小型サーバ、プライベートオンラインストレージファーム、ＨｙｐｅｒＮｏｄｅ対応ルータ（ＨｙｐｅｒＳｐｏｔなど）のような、有線接続または高稼働率のデバイスで構成されるオポチュニスティックプロバイダで構成されている。Ｔｉｅｒ－３リソースは、オンラインショッピングサイト、地域サービス、写真、ファイル、メディアコンテンツのオンラインバックアップおよびストレージなど、通信遅延の影響をあまり受けないＨｙｐｅｒＳｐｈｅｒｅ加盟店に使用される。また、Ｔｉｅｒ－３リソースは、コンピューティングリソースにアクセスできない学生、研究者、新興企業、起業家を支援するために慈善活動に利用されることもある。Ｔｉｅｒ－３リソースプロバイダのためのＨｙｐｅｒＣｏｎｔｒａｃｔｓは、ＨｙｐｅｒＳｐｈｅｒｅマーケットプレイスで交渉されるもので、契約とボーナスのＨｙｐｅｒＭｅｔａｌ報酬が混在しており、需要が高い時期にはＨｙｐｅｒＭｅｔａｌ報酬が保証される可能性が高くなる。Ｔｉｅｒ－３リソースプロバイダは、多くの場合、収入を補ったり、運営コストを削減したりすることを希望する個人や小規模企業で構成されている。ＨｙｐｅｒＣｏｎｔｒａｃｔを満たすためにＨｙｐｅｒＭｅｔａｌで支払いを受けると、受け取ったＨｙｐｅｒＭｅｔａｌは自動的に、ＨｙｐｅｒＳｐｈｅｒｅが保有する増殖性のある仮想通貨であるＨｙｐｅｒＣｏｉｎｓ（ハイパーコイン）に変換される。Ｔｉｅｒ－３ＨｙｐｅｒＮｏｄｅｓはいつでもＨｙｐｅｒＣｏｉｎｓをフィアット通貨に交換することができるが、Ｔｉｅｒ－１やＴｉｅｒ－２プロバイダに比べて支払い時に「キャッシュアウト」する可能性が低く、投資目的でＨｙｐｅｒＭｅｔａｌを保有する傾向が強く、仮想通貨のアップサイドの可能性のために資本損失のリスクを負うことになる。

・Ｔｉｅｒ－４リソースプロバイダ：Ｔｉｅｒ－４リソースプロバイダは、携帯電話、タブレット、ノートブックコンピュータ、自動車などのモバイルデバイスで構成されており、ＨｙｐｅｒＳｐｈｅｒｅクラウドへの接続時間が限られている。これらのデバイスは主に、ＨｙｐｅｒＳｐｈｅｒｅの通信メッシュ密度を高めるために使用されており、特に、ピアツーピアネットワークや、セルタワーへのアクセスが制限されていたり、妨げられている可能性のある農村部や都市部の密集地で使用されている。ＨｙｐｅｒＳｐｈｅｒｅマーケットプレイスで交渉されるＴｉｅｒ－４リソースプロバイダ向けのＨｙｐｅｒＣｏｎｔｒａｃｔｓは、ボーナスのＨｙｐｅｒＭｅｔａｌ報酬が自動的にＨｙｐｅｒＣｏｉｎに変換されたもので、その価値は需要の多い時期や地域に応じて変化する。Ｔｉｅｒ－４ＨｙｐｅｒＮｏｄｅｓは、いつでもＨｙｐｅｒＣｏｉｎをフィアット通貨に交換することができるが、他のＴｉｅｒ－４リソースプロバイダに比べて、支払い時に「キャッシュアウト」することは少なく、投資目的でＨｙｐｅｒＣｏｉｎを保有する傾向が強く、仮想通貨のアップサイドの可能性のために資本損失のリスクを負うことになる。

【０４８７】

ＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダは、携帯電話、ノートブック、パーソナルコンピュータ、および会社のコンピュータを活用して、毎日の３分の２以上はアイドル状態になっているデバイスから収入を得ることができる。リソースプロバイダには、給料を増やしたり、電話や光熱費を削減したいと考えている一般の人々が含まれている。ゲーマーは、ゲームをしていないときは、コンピューティングパワーと挑戦者のグローバルネットワークへのアクセスと引き換えに、彼らがアクティブなときにゲーム体験を強化するために彼らのリソースを共有することができる。ビットコインの採掘者は、ビットコイン市場の収益性が継続的に低下しているため、ハードウェア投資の代替手段を見つけることができる。大学は、ワークロードのバランスを取り、コストを削減し、ピークパフォーマンスを向上させるために、研究用コンピュータを他の研究機関と共有することができる。大企業は、ＨｙｐｅｒＳｐｈｅｒｅの顧客にアクセスすることで、負荷を改善することがで

きる。

【０４８８】

ＨｙｐｅｒＳｐｈｅｒｅの加盟店は、ＨｙｐｅｒＳｐｈｅｒｅを使用して製品やサービスを顧客に提供する独立した企業である。一実施形態では、ＨｙｐｅｒＳｐｈｅｒｅ Ｍａｒｋｅｔｐｌａｃｅは、ＡＩ（人工知能）ベースのトランザクションエコスフィアで構成されており、クラウドに接続されたサプライヤーに対して加盟店の需要をマッチングする。つまり、ＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダは、ＨｙｐｅｒＳｐｈｅｒｅの加盟店に対してタスクを実行し、契約を実行する。加盟店は、クライアントに対して、企業間（Ｂ２Ｂ）および消費者間（Ｂ２Ｃ）のサポートなどのサービスを提供する。ＨｙｐｅｒＳｐｈｅｒｅはプラットフォームであり、企業ではないため、消費者は、ＨｙｐｅｒＳｐｈｅｒｅ加盟店を通さない限り、ＨｙｐｅｒＳｐｈｅｒｅを利用したり、ＨｙｐｅｒＳｐｈｅｒｅにアクセスしたりすることはできない。商用企業は、ＨｙｐｅｒＳｐｈｅｒｅを使用することで、インターネットよりも効率的に競争を行うことができる。

【０４８９】

ＨｙｐｅｒＳｐｈｅｒｉｃ ｅコマースへの参加を希望する個人や企業は、投資やインフラストラクチャ費用なしに、加盟店、リソースプロバイダ、またはその両方としてＨｙｐｅｒＳｐｈｅｒｅに積極的に参加することができる。ＨｙｐｅｒＳｐｈｅｒｅの加盟店として、企業はＨｙｐｅｒＳｐｈｅｒｅの無限のリソースにすぐにアクセスし、競争力のあるコストで国際ビジネスやグローバルマーケティングに取り組むことができる。ＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダとして、コンピュータネットワーク事加盟店、ビットコイン採掘者、地域のＩＳＰプロバイダ、ケーブルネットワーク事加盟店、パーソナルコンピュータ、あるいはスマートフォンの所有者は、フルタイムまたはパートタイムでＨｙｐｅｒＳｐｈｅｒｅに通信資産やコンピューティング資産を提供することで、利益を得ることができる。ＨｙｐｅｒＳｐｈｅｒｅ加盟店の顧客は、加盟店が提供するサービスによって異なる。ＨｙｐｅｒＳｐｈｅｒｅ加盟店のお客様は、加盟店が提供するサービスによって異なる。ＨｙｐｅｒＳｐｈｅｒｅがサポートする事業には、以下のようなものがある。

【０４９０】

ＨｙｐｅｒＳｐｈｅｒｅデジタル通貨

【０４９１】

ＨｙｐｅｒＳｐｈｅｒｅで使用されるデジタルトークンには、ＨｙｐｅｒＭｅｔａｌトランザクショントークンとＨｙｐｅｒＣｏｉｎユーティリティートークンの２種類の暗号通貨がある。ＨｙｐｅｒＭｅｔａｌとＨｙｐｅｒＣｏｉｎｓの目的は、商人やリソースプロバイダがＨｙｐｅｒＳｐｈｅｒｅで電子商取引を行うための手段を容易にすることである。

【０４９２】

ハイパーコイン／仮想通貨

【０４９３】

ＨｙｐｅｒＳｐｈｅｒｅの取引可能な暗号通貨およびユーティリティートークンであるＨｙｐｅｒＣｏｉｎｓは、完全に互換性のある取引媒体であり、下記の機能を備えている。

・銀行や独立したデジタル通貨取引所で売買されていること。

・リソースプロバイダ（ＨｙｐｅｒＮｏｄｅｓ）が、タスクを完了し、ＨｙｐｅｒＣｏｎｔｒａｃｔｓを満たすための報酬として、ＨｙｐｅｒＭｅｔａｌから採掘されていること。

・タスクを完了し、ＨｙｐｅｒＣｏｎｔｒａｃｔｓを実行するために、リソースプロバイダ（ＨｙｐｅｒＮｏｄｅｓ）と契約し、支払いを行うために使用され、暗号通貨は新しいＨｙｐｅｒＣｏｉｎ（新しいデジタル暗号ＩＤを有する）にリサイクルされる。

【０４９４】

銀行の独立したデジタル通貨取引所で購入または販売され、オプションでＨｙｐｅｒＳｐｈｅｒｅで使用されるＨｙｐｅｒＣｏｉｎは、本質的に不安定であり、需給市場の力学の影響を受ける。逆に、ＨｙｐｅｒＳｐｈｅｒｅから直接購入したＨｙｐｅｒＭｅｔａｌ

は、ＨｙｐｅｒＳｐｈｅｒｅ内でのサービス契約のみを目的としており、販売、物々交換、仮想通貨化することはできない。リスクのある加盟店は、リソースプロバイダと契約するためにＨｙｐｅｒＭｅｔａｌを採用する必要がある。リスクのあるリソースプロバイダが報酬としてＨｙｐｅｒＣｏｉｎを鋳造した場合は、直ちに、他のＨｙｐｅｒＳｐｈｅｒｅ加盟店からサービスを購入するためにＨｙｐｅｒＣｏｉｎを使用するか、またはデジタル通貨取引所でＨｙｐｅｒＣｏｉｎをフィアット通貨に交換する必要がある。

【０４９５】

ＨｙｐｅｒＣｏｉｎを保有することには、経済的なリスクが伴いる。ＨｙｐｅｒＳｐｈｅｒｅでの有用性は別として、投資手段としてのＨｙｐｅｒＣｏｉｎの価値は、市場の動向に依存するため不明である。購入者が長期にわたってＨｙｐｅｒＣｏｉｎｓを保有している場合、ＨｙｐｅｒＣｏｉｎｓの価格が上昇する可能性や、ＨｙｐｅｒＣｏｉｎｓ保有者が購入した価格よりも高い価格でＨｙｐｅｒＣｏｉｎｓを売却できる可能性があるという保証はない。本発明の一実施形態では、ＨｙｐｅｒＣｏｉｎｓを販売するためには、購入者またはトークン保有者がＨｙｐｅｒＳｐｈｅｒｅに積極的に参加している必要があり、１つ以上のコンピューティングデバイスまたは通信デバイスにＨｙｐｅｒＮｏｄｅをダウンロードし、所定の期間ＨｙｐｅｒＳｐｈｅｒｅに積極的に接続する必要がある。また、ＨｙｐｅｒＮｏｄｅがアクティブに接続されていないと、関連するＨｙｐｅｒＣｏｉｎｓは、基準が満たされるまで販売または交換の対象とはならない。なお、他の実施形態では、取引手数料が徴収されるが、ユーザがアクティブなＨｙｐｅｒＮｏｄｅを所有している必要はない。

【０４９６】

ハイパーメタルトークン

【０４９７】

ＨｙｐｅｒＳｐｈｅｒｅの非取引可能な内部暗号通貨であるＨｙｐｅｒＭｅｔａｌユーティリティートークンは、ＨｙｐｅｒＣｏｎｔｒａｃｔトランザクションを作成して実行し、タスクやマイクロタスクを成功裏に完了させた場合に報酬を支払うことを誓約するという、単一の目的のために使用される。ＨｙｐｅｒＭｅｔａｌは、ＨｙｐｅｒＳｐｈｅｒｅからフィアット通貨で購入することができ、また、認定されたデジタル通貨取引所（ＤＣＥ）を通じて購入することができるが、販売したり、物々交換したりすることはできない。ＨｙｐｅｒＭｅｔａｌの購入価格（フィアット通貨での価格）は、ネットワークのビットコストによって設定される。ビットコストは、１ｓｔＴｉｅｒリソースプロバイダの正規化された加重平均コストであり、ＨｙｐｅｒＣｏｉｎの取引価格とは無関係である。ＨｙｐｅｒＭｅｔａｌはＨｙｐｅｒＣｏｎｔｒａｃｔｓの補償金を質入れするためにのみ使用でき、取引はできないため、ＨｙｐｅｒＭｅｔａｌの購入価格は比較的安定しており、投機的な価格変動の影響を受けない。

【０４９８】

トレーダーが誘導する価格変動から切り離された加盟店やリソースプロバイダは、企業のＨｙｐｅｒＳｐｈｅｒｉｃオペレーションに資金を供給するためにＨｙｐｅｒＭｅｔａｌを、投機家がコストを押し上げ、ビジネスやサプライチェーンを不安定化させるというリスクなしに、蓄積・保有することができる。また、ＨｙｐｅｒＭｅｔａｌの購入価格は１ｓｔＴｉｅｒサプライヤーのビットレートによって設定されているため、ＨｙｐｅｒＭｅｔａｌを購入することは、商業的には最高性能のネットワークへのアクセスを保証することと同等のものである。ＨｙｐｅｒＳｐｈｅｒｅの経済成長に伴う購買力をディスカウントすることで、商人は自力では調達できないような価格でリソースにアクセスすることができる。

【０４９９】

ＨｙｐｅｒＭｅｔａｌは、ＨｙｐｅｒＳｐｈｅｒｅ内でのみ使用される純粋な取引であるため、投機や通貨の変動の対象とはならない。ＨｙｐｅｒＭｅｔａｌは、ＨｙｐｅｒＳｐｈｅｒｅ内で電子商取引を行うことによってのみ、ＨｙｐｅｒＣｏｉｎに変換することができる。ＨｙｐｅｒＭｅｔａｌの購入価格は、ＨｙｐｅｒＣｏｉｎｓの取引価格ではな

く、コンピューティングや通信のビットレートコストの指標である「クアンツ」とも呼ばれるＴｉｅｒ１リソースプロバイダの実際のビットレートコストによって決定される。

【０５００】

このように、フィアット通貨からＨｙｐｅｒＣｏｉｎへの為替レートは、ＨｙｐｅｒＭｅｔａｌの購入に必要なＨｙｐｅｒＣｏｉｎの為替レートと同様に変動する可能性があるが、国際的なフィアット通貨とＨｙｐｅｒＣｏｉｎの間の正味の為替レートは、実質的なビットレートコストまたはクラウドサービスの量でのみ変動する。ＨｙｐｅｒＣｏｉｎｓが高くなれば、一定量のＨｙｐｅｒＭｅｔａｌの取引トークンを購入するために必要なユーティリティートークンが少なくなり、逆に、ＨｙｐｅｒＣｏｉｎｓの取引価格が下がれば、同じ量のトランザクショントークンを調達するために、より多くのユーティリティートークンが必要になる。ハイパーコインの市場価格にかかわらず、国際通貨でのハイパーメタルの等価購入価格は比較的一定であり、実質的には世界の電力コストに比例して変動する。

【０５０１】

デュアルトークンエコノミー

【０５０２】

開示されているＨｙｐｅｒＳｐｈｅｒｅ経済は、同時に２つの形態のデジタルトークンまたは仮想通貨で運営されている。それは、ＨｙｐｅｒＳｐｈｅｒｅ加盟店がリソースを調達したり、タスクをスケジュールしたりするためにＨｙｐｅｒＳｐｈｅｒｅマーケットプレイス内で使用するＨｙｐｅｒＭｅｔａｌと、ＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダがタイムリーにジョブを完了したり、ＨｙｐｅｒＳｐｈｅｒｅ経済環境に関与したりすることで報酬を得るために使用する「ＨｙｐｅｒＣｏｉｎｓ」である。ＨｙｐｅｒＳｐｈｅｒｅリソースプロバイダは、タスクを完了することでのみ、ＨｙｐｅｒＭｅｔａｌをＨｙｐｅｒＣｏｉｎｓに変換（鋳造）することができる。ＨｙｐｅｒＳｐｈｅｒｅでは、タスクを完了してＨｙｐｅｒＭｅｔａｌをＨｙｐｅｒＣｏｉｎｓに変換するプロセスである鋳造作業は、他の暗号通貨のマイニングと類似しているが、２つのデジタル通貨が作成され、もう１つが破壊される。ビットコインのマイニングとは異なり、ハイパーコインのマイニングは、資源提供者が商人のためにタスクやジョブ、契約を完了させることをベースにしている。鋳造は、ギャンブルや賭博をベースにしていない。

【０５０３】

ＨｙｐｅｒＳｐｈｅｒｅのユニークなイノベーションの１つであるデュアル仮想通貨システムのコンセプトの商業的価値は、ＨｙｐｅｒＣｏｉｎがＨｙｐｅｒＳｐｈｅｒｅ内での電子商取引の実質的なコストに影響を与えることなく、任意の価値に変動することができるということである。リスクを抱える加盟店は、ＨｙｐｅｒＣｏｉｎの購入と同時にＨｙｐｅｒＭｅｔａｌへの交換を行うことで、現在の懸念を解消し、ＨｙｐｅｒＣｏｉｎの高騰に賭けることを望む加盟店は、ＨｙｐｅｒＣｏｉｎを保有してからＨｙｐｅｒＭｅｔａｌと交換することができ、ＨｙｐｅｒＣｏｉｎの取引価格が上昇した場合にＨｙｐｅｒＭｅｔａｌの購買力が向上することを期待することができる（上昇しない可能性もある）。このように、ＨｙｐｅｒＳｐｈｅｒｅは、投機的で保守的な事業主や加盟店を満足させることができる。

【０５０４】

デジタル通貨生成

【０５０５】

図４９に示されているように、ＨｙｐｅｒＣｏｉｎは、ＨｙｐｅｒＭｅｔａｌをＨｙｐｅｒＣｏｉｎに変換するプロセスである鋳造９６０と、ＨｙｐｅｒＣｏｉｎを新しいＨｙｐｅｒＣｏｉｎにリサイクル９６１（溶解）する方法の２つの方法で生成することができる。このプロセスでは、ＨｙｐｅｒＣｏｎｔｒａｃｔ９６４の支払い誓約は参加しているＨｙｐｅｒＮｏｄｅｓの間で均等に配分され、新しいＨｙｐｅｒＣｏｉｎを合成するために使用される。支払いがＨｙｐｅｒＭｅｔａｌ９７０ａとして誓約された場合、ＨｙｐｅｒＣｏｎｔｒａｃｔ９６４はその誓約をＨｙｐｅｒＮｏｄｅ９６２のオーナーのＨｙｐｅ

ｒＭｅｔａｌブロックチェーン９６５ａに転送し、ロックする（９７１ａ）。契約の実行とコンセンサスの後、誓約はロックが解除され（９７２ａ）、ＨｙｐｅｒＮｏｄｅ９６２オーナーの個人的なＨｙｐｅｒＭｅｔａｌブロックチェーン上でデビット９７３として記録され、同じアカウントオーナーのＨｙｐｅｒＣｏｉｎブロックチェーン９５６ｂ上で対応するクレジット９７４として入力される。ＨｙｐｅｒＣｏｉｎリサイクル９６１の場合、誓約９７０ｂはＨｙｐｅｒＣｏｉｎブロックチェーン９６６に入力され、ＨｙｐｅｒＣｏｎｔｒａｃｔ９６４が完了するまで保持される。その後、ＨｙｐｅｒＣｏｉｎは溶解され（９７５）、新しい暗号コードで再発行され、古いコインが新しいコイン９７５にリサイクルされる。造幣９６０またはリサイクル９６１のいずれの場合も、参加しているＨｙｐｅｒＮｏｄｅｓ９６２または９６３は、契約の完了時に新しいＨｙｐｅｒＣｏｉｎ９７５を自動的に生成する。生成されたハイパーコインは、売却、譲渡、ウォレットへの移動が可能である。

【０５０６】

接続型ＢＣ生成

【０５０７】

ＨｙｐｅｒＳｐｈｅｒｅのユニークな機能の一つは、銀行やクレジットカードを使わずに、電子商取引、オンラインショッピング、ビジネス取引、送金をサポートできることである。その代わりに、ＨｙｐｅｒＳｐｈｅｒｅは、独自のネットワーク内蔵仮想通貨、すなわちデジタルトークンを利用しており、国際通貨や電信送金、従来のクレジットカードベースの決済メカニズムを利用した電子商取引のコスト、複雑性、遅延、非効率性を排除している。これらのデジタルトークンの生成は、データパケットがＨｙｐｅｒＳｐｈｅｒｅの独自のダイナミックネットワークを通過する際に、自律的に、かつ連動して行われる。ある実施形態では、データがネットワークを通過する際に、参加するＨｙｐｅｒＮｏｄｅｓに固有の暗号コードが配布される。

【０５０８】

ネットワーク運用中、クラウド内のデータホップごとに、一時的または一時的なブロックチェーンで構成される暗号コードが変更される。ネットワークトラフィックの伝送やタスクの実行へのＨｙｐｅｒＮｏｄｅｓの参加を証明するために使用されるこの検証コードは、ＨｙｐｅｒＮｏｄｅホップコード（ＨＨＣ）と呼ばれている。トークンの生成はネットワークが実際の作業を行う際に付随して行われるため、無意味なマイニング作業にエネルギーを浪費することはない。その代わりに、デジタルトークンは、タスクやジョブ、契約を完了したリソースプロバイダへの報酬として「鋳造」される。この新しいＰｏＰ（Ｐｒｏｏｆ－ｏｆ－Ｐｅｒｆｏｒｍａｎｃｅ）メカニズムは、ビットコインのマイニングで消費される必要なエネルギーは１兆分の１以下、世界初の環境に優しいデジタルトークンの生成を表している。発行されたトークンの販売や譲渡は、公開されたブロックチェーンの台帳に記録され、同加盟店の陪審員によって簡単に検証することができる。新しいハイパーコントラクトを開始するために、デジタルトークンまたはその一部はリサイクルされ、新しい取引、仕事、契約の支払いに使用される。

【０５０９】

ＨｙｐｅｒＮｏｄｅホップコード（ＨＨＣ）トークンの生成は、ＨｙｐｅｒＣｏｉｎやＨｙｐｅｒＭｅｔａｌの生成やトランザクション処理に限定されない。ＨｙｐｅｒＳｐｈｅｒｅを利用した加盟店向けの偽造防止デジタルトークンの生成にも、同様の手法を用いることができる。このＨｙｐｅｒＮｏｄｅ　Ｈｏｐ　Ｃｏｄｅｓという機能、つまりＴａａＳ（ｔｏｋｅｎｓ－ａｓ－ａ－ｓｅｒｖｉｃｅ）を利用した加盟店向けのサービスとしてのデジタルトークンの生成、配布、検証を行うことは、ＨｙｐｅｒＳｐｈｅｒｅにしかできないことである。生成方法が過渡的なブロックチェーン（ｔＢＣ）と永久的なブロックチェーン（ＢＣ）のいずれかの合成を伴うため、ＴａａＳの特徴は、ＢａａＳ（Ｂｌｏｃｋｃｈａｉｎ－ａｓ－ａ－ｓｅｒｖｉｃｅ）の特殊版と考えることができる。ＨｙｐｅｒＳｐｈｅｒｉｃ　ＴａａＳでカスタム生成されたトークンは、顧客の忠誠心を表すリワードトークン、購入時の割引クーポン、頻繁に旅行に行く人へのマイレージや特典、ゲーム

のパフォーマンスを表すゲームリワード、アーティストのファンクラブ会員のための優先チケット、バックステージパス、ミート＆グリーティングＶＩＰ特典、情報リクエストやクレジットカードの申請を完了させるためのショッパーリワードなど、さまざまな目的に利用することができる。

【０５１０】

ＨｙｐｅｒＣｏｉｎの鋳造

【０５１１】

暗号通貨の不正生成や改ざんされた検証を防ぐために、ＨｙｐｅｒＳｐｈｅｒｅでは、新しいコインの生成にマイニングを使用していない。数値パズルや暗号パズルのＰｒｏｏｆ－ｏｆ－Ｗｏｒｋソリューションを検証するために、無名の採掘加盟店や腐敗しやすい陪審員を信用するのではなく、ＨｙｐｅｒＳｐｈｅｒｅは、ＨｙｐｅｒＮｏｄｅｓのネットワークによって実行される信頼性の高い内部プロセスを介して、暗号通貨を合成している。この生成方法は、外部のオブザーバーからは観測することができず、パケットスニッフィングの対象にもなることなく、またＰｏＷの非暗号ハッシュパズルの解法とも無関係である。そのユニークな実装では、仮想通貨の生成は、追加のエネルギーや労力を必要とせずに、ＨｙｐｅｒＣｏｎｔｒａｃｔｓの実行中のデータ伝送中に、ネットワーク操作の本質的な一部として付随的に発生する。

【０５１２】

ＨｙｐｅｒＳｐｈｅｒｅの運用では、マルチツリーのＤｙＤＡＧブロックチェーンを使用して、暗号通貨を生成したり、所有権を記録したりしている。ＤｙＤＡＧには、目的や用途に応じて、「永久」ブロックチェーンと「一過性」ブロックチェーンがある。永久ブロックチェーン（ＢＣ）は、対応する親証明書から派生したアイデンティティトラストチェーンの系統を使用して、現存する暗号通貨を個人のＣＡ証明書にリンクさせることで、所有権を確立する。

【０５１３】

対照的に、一過性のブロックチェーン（Ｔｒａｎｓｉｔｏｒｙ　Ｂｌｏｃｋｃｈａｉｎｓ）または「ｔＢＣ」は、ハイパーコントラクトの実行、暗号通貨の合成、参加しているリソースプロバイダへの報酬の分配に使用される一時的な分散型台帳である。永久ブロックチェーンの永続性とは異なり、一過性のブロックチェーンのタスクが完了すると、そのブロックチェーンは破壊される。この方法では、永久ブロックチェーンは、不必要で無関係なブロックを運んで負担になることはない。ＨｙｐｅｒＳｐｈｅｒｅにおけるすべての暗号通貨の合成は、リソースプロバイダとそのクライアントであるサービスプロバイダや加盟店との間のビジネスアグリーメントであるＨｙｐｅｒＣｏｎｔｒａｃｔ（ハイパーコントラクト）から始まる。各ＨｙｐｅｒＣｏｎｔｒａｃｔは、仕事の仕様と、誓約の成功に参加したリソースプロバイダのために確保された報酬を記述した報酬誓約で構成されている。ＨｙｐｅｒＣｏｎｔｒａｃｔの誓約書は、ＨｙｐｅｒＭｅｔａｌまたはＨｙｐｅｒＣｏｉｎｓの２種類の暗号通貨で作成することができる。

【０５１４】

ＨｙｐｅｒＭｅｔａｌ誓約をＨｙｐｅｒＣｏｉｎｓに変換して鋳造するプロセスが、図５０に示されている。示されているように、縦線は、ＨｙｐｅｒＮｏｄｅの所有者９７０ｃ～９７３ｃによって保持され、所有者の対応するＣＡ－ｃｅｒｔｉｆｉｃａｔｅ９７０ｄ～９７３ｄベースのＩＤ－ｔｒｕｓｔ－ｃｈａｉｎによって署名された永久ブロックチェーン９２０ａ及び９７０ｂ、９７１ａ及び９７１ｂ、９７２ａ及び９７２ｂ、９７３ａ及び９７３ｂを表している。参加するＨｙｐｅｒＮｏｄｅｓ９７０ｃ～９７３ｃの役割は、名前、サーバ｜ＮＳ｜、権限｜Ａ｜、ジョブ実行のためのタスク｜Ｔ｜ノード、または権限｜Ａ｜ノードが、陪審員合意のオブザーバーとして参加しているメタモルフィック機能によって表されている。各参加ノードは２つのＤｙＤＡＧ永久ブロックチェーンを持ち、１つはＨｙｐｅｒＭｅｔａｌ取引用９７０ａ、９７１ａ、９７２ａ、及び９７３ａ、もう１つはＨｙｐｅｒＣｏｉｎ取引用９７０ｂ、９７１ｂ、９７２ｂ、及び９７３ｂとなっている。ＤｙＤＡＧマトリックスでは、これらの永久ブロックチェーンに新しいブロック

が追加され、上から下へと順番に並べられ、それに応じてタイムスタンプが押されている。同じ図では、横向きの矢印が一過性のブロックチェーンであるｔＢＣ９７６、９７８ｅ、９７８ｆ、９８２、及び、９８３ａ～９８３ｄを表している。一過性のブロックチェーンは、無常的に順次実行され、永久ブロックチェーンを修正し、その後破棄される。描かれているように、ＨｙｐｅｒＣｏｉｎ生成の造幣プロセスは、左から右へとタスクが実行され、上から下へと順番に行われる。ハイパーコントラクトに示されている順番に記載されているように、これらのプロセスには以下のマイルストーンが含まれている。

・ハイパーコントラクトの誓約時刻t_{mp}（９７５）
・ＨｙｐｅｒＣｏｎｔｒａｃｔタスクの実行時間Δt_t（９７７）
・時刻t_cにおけるハイパーコントラクトのコンセンサス（９７９）
・ハイパーコインの造幣時間t_g（９８１）

【０５１５】

この時間t_{mp}、でのＨｙｐｅｒＭｅｔａｌの誓約書９７５では、分散型ＨｙｐｅｒＳｐｈｅｒｅ　Ｍａｒｋｅｔｐｌａｃｅが契約書のネゴシエーションを正常に完結し、その時点で加盟店スポンサーはＨｙｐｅｒＭｅｔａｌの誓約書（９８５ｄ）をコミットされた契約参加者に配布し、実際にＨｙｐｅｒＭｅｔａｌを転送することなく、保留中のトランザクションとしてブロックチェーン９７０ａ、９７１ａ、９７２ａ、９７３ａに記録する。このようにして、誓約書は二重支出を防ぐために通貨をロック（９８６）することで、ブロックチェーン版のエスクローのような役割を果たす。ＨｙｐｅｒＣｏｎｔｒａｃｔの実行（９７７）は一定期間にわたって行われる。つまり、ＨｙｐｅｒＮｏｄｅがＨｙｐｅｒＣｏｎｔｒａｃｔのジョブ仕様に従って一連のタスク（またはサブタスク）を実行する間隔Δt_tの間に行われる。データトランジットとマイクロタスクの実行の間、各ＨｙｐｅｒＮｏｄｅは暗号化されたレシート、つまり、それ以前のＨｙｐｅｒＮｏｄｅのホップコードまたはＨＨＣを含む一連のハッシュ化されたブロックを含む一過性のブロックチェーン（９７８ｅ）を受け渡する。

【０５１６】

図５１に示すように、ＨｙｐｅｒＮｏｄｅ９９１、９９２ａ、９９２ｂ、９９２ｃはデータパケットのＳＤＮＰベースのルーティング命令の一部として、これらの暗号コード９４４ｂ、９４４ｃ、９４４ｄ、９４４ｅを自律的に生成する。作業が完了すると、各ＨｙｐｅｒＮｏｄｅは自身の暗号ブロックを一過性のブロックチェーンに追加する。その後、ＨｙｐｅｒＮｏｄｅは新しいより長いブロックチェーンを次のノードに転送し、次のノードはこのプロセスを繰り返す。このようにして、各ＨｙｐｅｒＮｏｄｅは自分が参加していることの反論の余地のない証拠を持っている。例えば、タスクノード｜Ｔ｜９９２ｂが一過性のブロックチェーンtBC_1を受信し、HHC_3のハッシュを受け取った後、修正された一過性のブロックチェーンtBC_2を次のＨｙｐｅｒＮｏｄｅ９９２ｃに転送する。このようにして、偽者の可能性を排除した自己矛盾しないブロックの文字列が生成される。ＳＤＮＰネットワークで生成されたＨｙｐｅｒＮｏｄｅのホップコードHHC_x９９５ｂ、９９５ｃ、９９５ｄと暗号ハッシュ関数ｈ（ｘ）を代数的に表現すると、次のようになる。

【０５１７】

【数５】

$$tBC_j = h(HHC_j) + tBC_{j-1}$$

【０５１８】

このプロセスでは、ＨｙｐｅｒＣｏｎｔｒａｃｔ自体がＨｙｐｅｒＣｏｎｔｒａｃｔの実行で使用される一過性のブロックチェーンの初期ブロック、つまりtBC_0＝ｈ（ＨＣ'）９９４ａを形成する。データパケットが連続してＨｙｐｅｒＮｏｄｅｓ９９１、９９２ａ、９９２ｂ、９９２ｃを通過すると、一過性ブロックチェーンtBC_j９４４ｂ、９４

４ｃ、９４４ｄ、９４４ｅのコピーが堆積される。終着ノードに到達すると、最終的な完全長の一過性ブロックチェーン$_{t}$ＢＣ$_{f}$９４４ｅが、タスクの完了を確認するためにＨｙｐｅｒＣｏｎｔｒａｃｔのイニシエータに返却される。完全長の$_{t}$ＢＣ$_{f}$ブロックチェーンは、チェックをするためＨｙｐｅｒＣｏｎｔｒａｃｔで指定されたｊｕｒｙ－ｏｆ－ｐｅｅｒｓに同時に転送される。図５０に戻って、時刻t_cでは、ｊｕｒｙ－ｏｆ－ｐｅｅｒｓによるコンセンサスがＲＢＯＳ（レプリカントブロックチェーンオブザーバーセグメント）（例えば、９８０ｄ）を使用して契約の実行９７９を確認し、バックトレースの可能性を排除して検査を容易にする。ＨｙｐｅｒＣｏｎｔｒａｃｔの完了、ピアレビュー、コンセンサスが確認されると、参加したすべてのＨｙｐｅｒＮｏｄｅオーナーは、透過的ブロックチェーンtBC_0、tBC_1、tBC_2を確立したコピーを使用して、その貢献度に応じた報酬を受け取ることができる。一旦確認されると、一過性のブロックチェーンは自動的に変換、指定された数のＨｙｐｅｒＣｏｉｎ９８４に鋳造され、ＨｙｐｅｒＮｏｄｅオーナーの永久ブロックチェーン９７０ｂ、９７１ｂ、９７２ｂ、９７３ｂに記録される。参加ノードが実際のタスクを実行する際に貢献度を証明する暗号通貨の作成は、Ｐｒｏｏｆ－ｏｆ－ＰｅｒｆｏｒｍａｎｃｅまたはＰｏＰと呼ばれている。時刻t_gにＨｙｐｅｒＮｏｄｅのパフォーマンスが証明されると（９８１）、ＨｙｐｅｒＭｅｔａｌは（無制限のコードを使用して）アンロックされ（９８５）、ＨｙｐｅｒＭｅｔａｌの誓約と、有効なピアレビューされた出所を証明する一過性のブロックチェーンｔＢＣ　９８３ａ、９８３ｂ、９８３ｃ、９８３ｄのハッシュを含む新しいコードが生成される。鋳造プロセスは、ＨｙｐｅｒＭｅｔａｌの永久ブロックチェーンＢＣ　９７０ａ、９７１ａ、９７２ａ、９７３ａからのアンロック９８５と引き落とし９８６、ＨｙｐｅｒＣｏｉｎの永久ブロックチェーンＢＣ　９７０ｂ、９７１ｂ、９７２ｂ、９７３ｂへのクレジット９８７としてグラフィカルに描かれている。一度鋳造されたＨｙｐｅｒＣｏｉｎは、国際的なフィアット通貨に変換されたり、ＨｙｐｅｒＳｐｈｅｒｅで資源を募るために使用されたりする可能性がある。

【０５１９】

図５２に示すＨｙｐｅｒＣｏｉｎリサイクルでは、ＨｙｐｅｒＣｏｎｔｒａｃｔの誓約がＨｙｐｅｒＣｏｉｎ（ＨｙｐｅｒＭｅｔａｌではない）で行われる。この誓約は、ＨｙｐｅｒＮｏｄｅのパーペチュアルＨＣブロックチェーン９７０ｂ、９７１ｂ、９７２ｂ、９７３ｂ上で保留中のトランザクションとして記録される（実際にＨｙｐｅｒＣｏｉｎを転送することはない）。契約交渉時にＨｙｐｅｒＣｏｉｎをデジタルエスクローにロックすることは（９８９）、ＨｙｐｅｒＣｏｉｎが代替可能で流動資産として取引可能であるため、支出の二重化を防ぐために特に重要である。リサイクル契約のタスク実行９７７と陪審員のコンセンサス９７９リサイクル契約の実行は、新しいＨｙｐｅｒＣｏｉｎ９８４ａが生成される契約完了時のt_g９８１ａを除き、鋳造の契約と同様の方法で行われる。リサイクルプロセスでは、元の誓約されたＨｙｐｅｒＣｏｉｎｓの暗号ＩＤが破壊され、ＨｙｐｅｒＳｐｈｅｒｅ分類法で「溶解」された後、新しいデジタルＩＤを持つ新しいＨｙｐｅｒＣｏｉｎｓとして再鋳造される（ＨＣ永久ブロックチェーン９７０ｂ、９７１ｂ、９７２ｂ、９７３ｂ上では、借方９９８と同時貸方９９９として描かれている）。新たに鋳造された暗号通貨と同様に、リサイクルされたＨｙｐｅｒＣｏｉｎｓは、ＨｙｐｅｒＮｏｄｅのホップコードHHC_jとオリジナルのＨｙｐｅｒＣｏｎｔｒａｃｔ　ＨＣから派生した暗号化ハッシュ値ｈ（ｘ）に基づくデジタルＩＤを採用している。ＨｙｐｅｒＮｏｄｅによって再鋳造されたＨｙｐｅｒＣｏｉｎｓの量は、ＨｙｐｅｒＣｏｎｔｒａｃｔでは＃ＨＣｎｅｗ＜＃ＨＣｐｌｅｄｇｅであるため、リサイクルによる減少により、流通しているＨｙｐｅｒＣｏｉｎｓの量を自然に減らすので、ＨｙｐｅｒＣｏｎｔｒａｃｔ上で誓約されたＨｙｐｅｒＣｏｉｎｓの数よりも少なくなる。このため、ＨｙｐｅｒＳｐｈｅｒｅのリサイクルプロセスは、エントロピー（情報の損失）であり、保守的とは言えない。

【０５２０】

その他のブロックチェーンプロセス

【０５２１】
他の人よりも先に難解なパズルを解くことができた幸運な採掘者のみに報酬を支払う仮想通貨のマイニングとは異なり、Ｐｒｏｏｆ－ｏｆ－Ｐｅｒｆｏｒｍａｎｃｅでは、ＨｙｐｅｒＣｏｎｔｒａｃｔの成功に参加したすべてのＨｙｐｅｒＮｏｄｅｓは、契約上保証されたリターンを採掘者として受け取ることができる。また、これはＳＤＮＰネットワークの運用と並行して行われるため、ＨｙｐｅｒＣｏｉｎｓの鋳造とリサイクルは、基本的に通信や電子商取引そのものを行うよりも電気エネルギーを消費しない。本質的には、ＨｙｐｅｒＳｐｈｅｒｉｃ暗号通貨の合成は、実質的にエネルギーを全く無駄にすることがない。ＨｙｐｅｒＳｐｈｅｒｅでの仮想通貨生成およびトランザクション処理を十分に理解し、これらのプロセスがＢｉｔｃｏｉｎ、Ｅｔｈｅｒｅｕｍ、および従来のブロックチェーン・アプリケーションとどのように異なるかを理解するには、デバイスのシステムアーキテクチャを考慮することが重要である。図３４に示すように、コンピュータまたは通信デバイスは、Ｗｉｎｄｏｗｓ（登録商標）、ＭａｃＯＳ（登録商標）、Ｌｉｎｕｘ（登録商標）、Ａｎｄｒｏｉｄ（登録商標）、またはｉＯＳ（登録商標）などの「オペレーティングシステム」（ＯＳ）を使用してソフトウェアアプリケーションをサポートしている。オペレーティングシステムは、典型的には複数のＣＰＵ、メモリ、およびデバイス接続を含むハードウェアとドライバからなるプラットフォーム上でホストされている。動作中の「カーネル」は、ハードウェアとアプリケーション環境（曖昧さを避けるために、ここではアプリケーション環境と呼ぶ）の間のインターフェイス、すなわちリエゾンとして機能するＯＳのためのリソーススケジューリングとタスク管理を提供する。アプリケーション環境は、ＡＰＩ、ＵＩ／ＵＸ、データベース、ビジネス、電子メール、ＶｏＩＰメッセンジャー、リモートアクセスゲートウェイ、ＩｏＴ、Ｗｅｂアプリなどを含む様々なソフトウェアをホストしている。今日のほとんどのアプリはネットワークに対応しており、Ｉｎｔｅｒｎｅｔ－ｏｆ－Ｅｖｅｒｙｔｈｉｎｇ（ＩｏＥ）接続を容易にしている。

【０５２２】
図示されているように、オペレーティングカーネルはアプリケーション環境と基盤となるハードウェアプラットフォームの両方と直接対話する。カーネルはまた、通信プロトコルスタック、特にアプリケーションレイヤ７を介して、レイヤ１．５（ＰＨＹレイヤ１とデータリンクレイヤ２の間に存在する界面準レイヤ）と相互作用する。動作中、ＰＨＹレイヤ１で受信した信号は、レイヤ２に渡され、ジョブスケジューリングのためにＯＳカーネルに同時に転送される。カーネルは、アプリケーションレイヤ７との相互作用により、デバイスＯＳ上（アプリケーションハビタット内）で動作するソフトウェアをサポートするために、タスクのスケジューリングを行いる。このような仕組みを説明する際には、アプリケーションレイヤ７（ＳＤＮＰやＴＣＰ／ＩＰプロトコルスタック内）の主な通信の役割と、コンピュータのアプリケーションプログラム（ＯＳのアプリケーション環境内で動作する）の機能を区別することが重要である。具体的には、アプリケーションレイヤ７のデータパケットは、特定のアプリケーションに高レベルのネットワーク接続性を提供するが、ＯＳがホストするアプリケーションから独立して動作することはできない。その意味で、アプリケーションのハビタットは、アプリケーションレイヤ７のすぐ上にあるＯＳＩプロトコルスタックの上に位置している。抽象化されたレイヤの用語で言うと、アプリケーションレイヤ７は、その上のアプリケーションハビタットで動作するソフトウェアをサポートし、ソフトウェアはレイヤ７から提供された情報に依存してサポートを行う、と言える。機能するためには、ソフトウェアとデータパケットのペイロードの種類、構文、バージョンなどが一致している必要がある。例えば、データベースソフトウェアがデバイスにインストールされていない場合、レイヤ７上で受信したＳＱＬ命令は認識されず、応答されない。

【０５２３】
ウェブ上の分散、コラボレーション、ハイパーメディア情報のためのハイパーテキスト転送プロトコル（ＨＴＴＰ）コンテンツを運ぶデータパケットは、ＨＴＭＬやＸＭＬを解釈できるブラウザアプリケーションなしでは全く役に立たない。同様に、従来の暗号通貨

ブロックチェーンでは、レイヤ７ペイロードとして受信したトランザクションは、対応するアプリケーションのサポートなしに、既存のブロックチェーンに新しいブロックを変更したり、追加したりすることはできない。従来のブロックチェーンおよび暗号通貨のトランザクションはすべて、プロトコルスタックの一部ではなく、完全にホストＯＳのアプリ環境内で発生する。ＨｙｐｅｒＳｐｈｅｒｅへのネットワークポータルとして、ＨｙｐｅｒＮｏｄｅｓはＳＤＮＰプロトコルスタックとＯＳアプリ環境にまたがり、ネットワークおよび伝送レイヤ３および４、ＳＤＮＰアプリケーションレイヤ７、ＯＳアプリ環境内のＡＰＩおよびＵＩ／ＵＸと直接通信する。ブロックチェーン処理では、ＨｙｐｅｒＳｐｈｅｒｅは完全に独自のもので、ネットワークレイヤ３の一部としてＨＨＣ暗号ＨｙｐｅｒＮｏｄｅホップコードを生成し、この情報をブロックチェーンプロセッサ「ＢＣＰ」で使用する。そしてＢＣＰは、ＢａａＳ（Ｂｌｏｃｋｃｈａｉｎ ａｓ ａ Ｓｅｒｖｉｃｅ）や各種ブロックチェーンアプリを含むブロックチェーンアプリをサポートする。ＢＣＰ、ＢａａＳ、およびＢＣアプリは、ＨｙｐｅｒＭｅｔａｌやＨｙｐｅｒＣｏｉｎのトランザクションを促進するために使用されるが、処理エンジンは、ＨｙｐｅｒＳｐｈｅｒｅのユーザがカスタム暗号通貨を作成したり、サービスプロバイダの事業のトークン化を行う際のサービスとしても使用することができる。

【０５２４】

ＨｙｐｅｒＳｐｈｅｒｅのマルチレイヤ暗号通貨生成は、ＯＳＩプロトコルスタックのレイヤ７以上のＯＳａｐｐ－ｅｎｖｉｒｏｎで実行されるアプリケーションとして処理される従来のブロックチェーンとは全く異なるものであり、簡単に区別できる。このような理由から（他にも数え切れないほどの理由から）、このような従来型のブロックチェーンプロセッサは、「プロトコル」や「ネットワーク」というよりも、「アプリ」と呼ぶ方が正確である。これとは対照的に、ＨｙｐｅｒＳｐｈｅｒのＢＣＰブロックチェーンプロセッサは、ＳＤＮＰプロトコルスタックの一部として存在し、新しい暗号通貨の鋳造や電子商取引の実行時にネットワークネイティブの操作として動作するため、本当の意味でプロトコルとみなすことができる。つまり、ＢＣＰの操作はＨｙｐｅｒＳｐｈｅｒｅネットワークネイティブであるため、ブロックチェーンの処理は迅速に行われるが、トランザクション検証のためのピアコンセンサス速度によってのみ制限される。ＨｙｐｅｒＳｐｈｅｒｅの暗号通貨は、その迅速な処理能力にもかかわらず、偽造が困難なのは、ＯＳＩ Ｓｅｓｓｉｏｎ、Ｐｒｅｓｅｎｔａｔｉｏｎ、Ａｐｐｌｉｃａｔｉｏｎ Ｌａｙｅｒｓ５、６、７からは観測できないＳＤＮＰネットワーク操作に固有の暗号ホップコードを採用しているからである。これらのコードには、ＨｙｐｅｒＣｏｎｔｒａｃｔの情報（誓約書のハッシュとタイムスタンプを含む）と、独自のＨｙｐｅｒＮｏｄｅホップコードのシーケンスの組み合わせが含まれている。さらに、純粋に内部でのコイン生成と、隠蔽された（非公開の）陪審員のため、仮想通貨の偽造者は、ネットワークで生成されたブロックチェーンのコンテンツを一致させたり、予測したりすることができない。

【０５２５】

ネットワークネイティブのブロックチェーン処理や短い長さのＤｙＤＡＧブロックチェーンとは別に、トランザクション速度を向上させるもう一つの方法として、ブロックチェーンのデフラグという独自の方法がある。ハードディスクドライブ（ＨＤＤ）のデフラグに似た方法で、ブロックチェーンのデフラグのプロセスでは、利用可能な暗号通貨をブロックチェーンの末端に移動させる。ＤｙＤＡＧブロックチェーンの底部付近に流動通貨を再配置することで、その後のトランザクションの検証は、確認のために非常に短いＲＢＯＳセグメントのみを必要とし、検証を迅速化し、バックトレースを完全に防ぐことができる。図５３に示されているように、ブロックチェーンの処理中、新しいブロックチェーンは、資産の貸方か借方のどちらを構成するかに関係なく、チェーンの最後にのみ追加される。ブロックチェーン資産は、ラストインファーストアウトまたはＬＩＦＯプロセスを使用して処理され、最後に取得したコインが最初に使用されるので、トランザクション時間を最小化する。示されているように、時刻t_2では、時刻t_1で追加（１０１０）された通貨が消費（１０１１ａ、１０１１ｂ）される。時刻t_3では、現在の引き落とし（１０

１２ｂ）を容易にするために、さらに早い入金（１０１２ａ）を見つけて確認しなければならない。時刻t_6では、当座負債（１０１４ｂ）を資金調達するために必要な資産は、過去のはるか昔からの預金（１０１４ａ）を特定する必要があり、断片的な取引１０１９で構成されているため、ＲＢＯＳが長くなり、取引の解決に時間がかかる。

【０５２６】

この難問を解決するには、ブロックチェーンを「ａｓ　ｙｏｕ　ｇｏ（必要に応じて）」方式でクリーンアップすることである。つまり、他のトランザクションが発生しておらず、スピードが重要でない時、都合の良い時にデフラグされたアセットを削除することである。時間t_4からt_6までのシーケンスで示されているデフラグプロセスでは、足止めされた資産を特定し、ブロックチェーンの最後にこれらの資産を再配置する。追加されたブロックは永久的なものなので、以前のエントリを変更する手段はない。代わりに、ＢＣのデフラグ処理では、時刻t_4で示されているように、借方と貸方のペア１０１５を記録することで、ブロックチェーンに「ゼロ」を追加する。検証中、新しい借方１０１５ｂは以前の預金（１０１４ａ）をキャンセルし、時刻t_2に示すようにチェーンの末端に新しい資産（１０１５ｃ）が移動する。そして、時刻t_6に支払い（１０１６）が行われると、資産（１０１５ｃ）はすでにブロックチェーンの末端に位置しており、コンパクトで迅速なトランザクションが実装される。ブロックチェーン管理のもう一つの要素として、補助ブロックチェーンの利用がある。共同ブロックチェーンでは、任意のファイルがメインブロックチェーンに追加されるが、ＨｙｐｅｒＳｐｈｅｒｅでは、図５４に示すようにＤｙＤＡＧブロックチェーンを使用することで、メインブロックチェーン１０２０の整合性を妨げることなく、コンテンツを補助的なサイドチェーン１０２１として実装することができる。

【０５２７】

メインブロックチェーンに任意のブロックを書き込む機能がなければ、ユーザはトランザクションブロックチェーンを不快な内容や違法な内容で汚染することを防ぐことができる。その代わりに、メインブロックチェーン１０２０は補助ブロックチェーン１０２１にリンクするポインタ１０２２を記録するだけで、文書化の目的に有用な暗号通貨トランザクション以外のエントリ１０２３ａ、１０２３ｂをサポートする。ドキュメントがトランザクション１０２４ａをサポートしている場合、そのようなコンテンツは、独立した陪審員１０２６によるＲＢＯＳ１０２５の検証チェックに含めることができる。

【０５２８】

サイドチェーンが完成すると、サイドチェーンは終了し、メインブロックチェーンに２番目のエントリを記録する。２番目のエントリ（１０２７ｂ）は異なる動的な状態で発生するため、ＤｙＤＡＧサイドチェーンは周期的なループを形成しない。同じ補助的なサイドチェーンメカニズムは、暗号トランザクションとは関係のない文書化のために使用することができ、ＢＣアプリを介して実行コードのサブルーチン呼び出しにも使用することができる。これらのプロセスは、任意に、ブロックチェーンの時空間的な状態に並行してプロセスを継続しながら、メインブロックチェーン上のサブルーチンのプロセス状態に関する更新を記録することができ、それにより、チューリング完全プロセスの実行の見通しを可能にする。

【０５２９】

セキュアウォレット

【０５３０】

ＨｙｐｅｒＳｐｈｅｒｅアカウントとは、特定の親であるＣＡ証明書が所有するデバイス資産、デバイス、およびＨｙｐｅｒＷａｌｌｅｔｓを指す。特に、特定の所有者のＨｙｐｅｒＳｐｈｅｒｅアカウントには、そのデバイス、登録されたＨｙｐｅｒＮｏｄｅｓまたはＨｙｐｅｒＮｏｄｅクラスタ、ＨｙｐｅｒＭｅｔａｌ永久ブロックチェーン、ＨｙｐｅｒＣｏｉｎ永久ブロックチェーン、およびＨｙｐｅｒＷａｌｌｅｔｓが含まれる。これらの要素の所有権をデジタル署名し、検証するために、仲介するＣＡ証明書を任意の数だけ使用することができる。ＨｙｐｅｒＳｐｈｅｒｅアカウントの所有者が獲得したＨｙｐ

ｅｒＮｏｄｅの収入はすべて、複数のＨｙｐｅｒＷａｌｌｅｔｓのいずれかに転送されない限り、個人のＨｙｐｅｒＣｏｉｎブロックチェーン上に残る。さらに、ＨｙｐｅｒＷａｌｌｅｔｓは、ＨｙｐｅｒＳｐｈｅｒｅ ａｓ ａ Ｂｌｏｃｋｃｈａｉｎ－ａｓ－ａ－Ｓｅｒｖｉｃｅ（ＢａａＳ）を利用して、Ｈｙｐｅｒコイン以外の暗号通貨を保有することができる。ＨｙｐｅｒＣｏｉｎｓの造幣以外にも、ＨｙｐｅｒＳｐｈｅｒｅアカウントへの資産の出し入れはすべてＯＴ^{3}プロキシメディエーターを介して行われる。

【０５３１】

買取＆ＯＴ^{3}プロキシ

【０５３２】

前述のように、ＨｙｐｅｒＳｐｈｅｒｅアカウントへの資産の出入りはすべて、ワンタイムトランザクショントークンまたはＯＴ^{3}プロキシと呼ばれる特別な一過性のブロックチェーンを使用して実行される。このプロキシは、仲介者とその記録が取消不能に解消された後のトランザクション中にのみ存在する。特に、ＨｙｐｅｒＣｏｉｎｓの販売中や、オンラインやＰＯＳでの購入時の支払いとしてＨｙｐｅｒＣｏｉｎｓを使用する際の盗難やバックトレースを防ぐために、所有者のブロックチェーンへの直接のアクセスは許可されていない。その代わりに、２段階の転送プロセスが採用されており、まずブロックチェーンがワンタイムトランザクショントークンメディエーターまたはＯＴ^{3}プロキシに移動され、次に第２段階として、商品または通貨（暗号または不換紙）と引き換えにプロキシから加盟店または買い手に暗号通貨が転送される仕組みになっている。すべてのＯＴ^{3}プロキシが仲介する取引の間、最初のステップでは、支払い者であるＨｙｐｅｒＣｏｉｎ保有者が、アカウントまたはＨｙｐｅｒＷａｌｌｅｔからＯＴ^{3}プロキシに指定された数のＨｙｐｅｒＣｏｉｎを移動することを要求する必要がある。

【０５３３】

図５５に示すように、プロセスは、要求者がＯＴ^{3}転送ＨｙｐｅｒＣｏｎｔｒａｃｔを開くことで始まる。次にＨｙｐｅｒＣｏｎｔｒａｃｔは陪審員（１０５１）を特定し、オーナーのＨｙｐｅｒＣｏｉｎブロックチェーン（またはＨｙｐｅｒＷａｌｌｅｔ）１０４０から十分な長さのレプリカントブロックチェーンオブザーバーセグメント（ＲＢＯＳ）１０４３を作成し、支払い者が要求されたトランザクションを実行するのに十分な資産を保有していることを確認する。検証されると、要求されたＨｙｐｅｒＣｏｉｎは、所有者の永久ＨｙｐｅｒＣｏｉｎブロックチェーン１０４０から引き落とされ、一過性のＯＴ^{3}ブロックチェーン１０４１に貸方として記録される。支払い者１０５０は、隠蔽された陪審員１０５１を見ることができないため、またＲＢＯＳブロックチェーンをチェックしている陪審員も知らないため、５１％、サイバーボット、またはＳｙｂｉｌ攻撃を実行して二重支出に関与することができない。同様に、支払者１０５０はＲＢＯＳ１０４３のデータを改ざんしたり、破損させたりすることもできない。

【０５３４】

次のステップは、受取人である商品やサービスを販売している加盟店、またはＨｙｐｅｒＣｏｉｎ購入者の誠実さを確認することである。これは、ＰＯＳ取引の場合は本人が直接行うか、エスクローエージェント（不動産の場合）を介して行うか、または取引が決済されるまでＯＴ^{3}プロキシ１０４１のリリースをタイムロックすることで行うことができる（例：ビットコインの支払いの有効性が確認されるまで）。トランザクションの整合性が確認された後、ＯＴ^{3}プロキシはＨｙｐｅｒＣｏｉｎデジタルコードを加盟店または買い手に転送（１０４２ａ、１０４２ｂ、１０４２ｃ）してからプロキシは閉じられる。このようにＯＴ^{3}プロキシを介して、どちらの当事者も直接対話することはなく、詐欺やバックトレースを犯すことはできない。プロキシ仲介者はまた、より遅いブロックチェーンの検証と転送プロセスが実際の電子商取引に先行することができるため、取引の解決を加速させる。最後に、ＯＴ^{3}プロキシは、ＨｙｐｅｒＳｐｈｅｒｅアカウント所有者が個人のＨｙｐｅｒＣｏｉｎブロックチェーンやＨｙｐｅｒＷａｌｌｅｔを公開することがないため、トランザクション詐欺のリスクにさらされる総資産を制限する。

【０５３５】

レプリカントブロックチェーンオブザーバーセグメント（ＲＢＯＳ）

【０５３６】

アカウント所有者のブロックチェーンからの個人情報の盗難や漏洩を防ぎながら、トランザクションの完全性を管理するために、ＨｙｐｅｒＳｐｈｅｒｅでは、レプリカントブロックチェーンオブザーバーセグメント（ＲＢＯＳ）と呼ばれるユニークで独創的な方法を使用している。ホストのブロックチェーンの限られた長さのコピーで構成されるＲＢＯＳは、トランザクションを承認するのに十分な長さだが、短すぎて過去の履歴をバックトレースできなかったり、不注意でプライバシーが漏洩したりすることがある。

【０５３７】

ＨｙｐｅｒＳｐｈｅｒｉｃトランザクションにおける陪審員コンセンサスのためのＲＢＯＳ１０６３の使用例を図５６に示す。どのようなトランザクションでも、あらゆる規模の陪審員コンセンサスをサポートするために、複数のＲＢＯＳを採用することができる。トランザクションの完了後、対応するＲＢＯＳ１０６３は破棄され、ハッシュ化されたブロックチェーンに記録され、プライバシーを保護しながら、トランザクションの完全性とトレーサビリティを確保し、二重支出を防止する。

【０５３８】

マントを纏った陪審員

【０５３９】

ＨｙｐｅｒＳｐｈｅｒｅのもう１つのユニークな機能は、ＨｙｐｅｒＮｏｄｅのソースポータルとリモートポータルの間にアドホックトンネル通信、つまりダイナミックシングルホップＶＰＮを確立できることである。これらのプライベートトンネルの目的は、輻輳によるＱｏＳの低下に苦しむサブネットからトラフィックを迂回させ、ネットワークやＤｏＳ攻撃やＳｙｂｉｌ攻撃などのブロックチェーントランザクションに対するサイバー攻撃を回避することにある。この方法は、制御されていないラストマイルリンク上での超安全な通信を確保するためにも使用できる。

【０５４０】

図５７に示すように、ＨｙｐｅｒＮｏｄｅインターポータルトンネル１０８２が確立されると、データは、急行列車が停止せずに（または速度を落とさずに）ローカル列車の停車場を通過するように、中間ノードが処理することなく、ダイレクトルーティングを使ってリモートポータル１０８１に流れるようになる。ＨｙｐｅｒＮｏｄｅトンネル通信の応用は、サイバー攻撃を撃退する上で特に価値がある。例えば、サービス妨害攻撃が疑われるような局地的なネットワークの混雑が急激に増加した場合、攻撃を受けているノードは、受信パケットのサポートを一時的に中断し（またはオプションでキューバッファを開く）、攻撃を受けているデバイスやサブネットの手の届かないところにトンネル１０８２を確立してから、リモートポータル１０８１との間のトラフィックをリダイレクトする進行中のすべてのセッションを再確立することができる。この応答方法では、ＤｏＳが新たな着信コールやセッションの確立を遅らせることを防ぐことはできないが、ソース１０８０がサイバーボット１０８３ａに囲まれている場合でも、囲まれたノードが優先的に安全へのオープンな新しいリンクを確立することができる。サイバーボット１０８３はＳＤＮＰプロトコルを解釈するための動的なセキュリティクレデンシャル情報を欠いているため、リモートのＨｙｐｅｒＮｏｄｅポータル１０８１の位置を追跡することができない。ＨｙｐｅｒＮｏｄｅのトンネリングは、Ｓｙｂｉｌ、５１％、ＤｏＳの方法などのブロックチェーン攻撃を回避するために、暗号通貨取引を保護する上で特に価値がある。ハイパーコントラクトで隠蔽された陪審員を指定することで、取引当事者は、どのＨｙｐｅｒＮｏｄｅがアセットおよびトランザクションのコンセンサス検証を行っているのかを知ることができない。さらに、ＨｙｐｅｒＮｏｄｅトンネル１０８２を介して隠蔽された陪審員に接続することで、彼らのポータル間通信は特権的なものとなり、他のネットワークノードによるメタデータの監視やハッキングの対象とはならない。ＨｙｐｅｒＮｏｄｅのトンネリングは、卓越したトランザクションセキュリティを求めるＨｙｐｅｒＮｏｄｅによって、あるいはＤｏＳ攻撃を検知した場合に自動的に実行される。攻撃が検知されると、トンネ

ルトラフィックはすべてのローカルトラフィックよりも優先される。継続的なセッションは、サイバーボット攻撃者に気づかれることなく、リモートノードを経由して再開される。

【０５４１】

ＨｙｐｅｒＳｐｈｅｒｅは、エンドツーエンドで実行されるトンネリングもサポートしている。ポート間トンネリングとは異なり、エンドツーエンドのトンネリングでは、通信当事者は、セッションの開始や通話とは無関係に、事前に暗号化キーを交換する。理想的には、ネットワークを介在させることなく、２つのデバイス間で鍵を交換することができる。エンドツーエンド暗号化を適用することで、ＳＤＮＰのセキュリティプロトコルとは独立してＨｙｐｅｒＳｐｈｅｒｅでの個人のプライバシー保護が容易になる。

【０５４２】

多次元プロパティには、以下のようなものがある。

・データパケットのブルートフォースコード解読に量子コンピューティングを使用しても、パケット内に含まれる不完全なデータは、ネットワークトラフィックの海の中で関連するデータグラムを識別するのに役立つメタデータを欠いているため、意味がなくなる。

・データパケットのブルートフォースコード解読に量子コンピューティングを使用しても、セキュリティクレデンシャル情報や隠蔽アルゴリズムは動的で、解読するよりも早く変化するため、他のデータパケットの解読には役立たない。

・ＨｙｐｅｒＳｐｈｅｒｅのメタモルフィックなＨｙｐｅｒＮｏｄｅは、ステートレスである。つまり、タスクを実行しても、そのタスクが何をしたかはすぐに忘れてしまい、検査するための記録は残らない。

・データの転送はメッシュ化されたネットワーク上で行われ、動的な隠蔽方法を使用してホップバイホップで保護されている。つまり、データトラフィックコンテンツ、さらにはメタデータを検査できるマスターキーはない。

・ルーティングは光速に近い速度でネットワークを移動する動的なものであるため、ハッカーの介入（同じ速度で移動する）はパケットを追いかけることができない。ハッカーのパケットがＨｙｐｅｒＮｏｄｅに到着する頃には、ＤｙＤＡＧのメッシュ化されたルーティングの状態は変化しており、比喩的に言えば、昨日の天気予報を読むようなものである。

・ＨｙｐｅｒＣｏｎｔｒａｃｔ実行におけるＤｙＤＡＧ ｔｒａｎｓｉｔｏｒｙ ｂｌｏｃｋｃｈａｉｎｓ（ｔＢＣ）の応用は、各タスクが完了した後にステートレスで破壊されるため、すでに破壊された記録を破るためにスーパーコンピューティングを使用することはできない。

・ＤｙＤＡＧパーペチュアルブロックチェーン（ＢＣ）は、仮名のアイデンティティを使用したマルチツリーのアイデンティティトラストチェーンによってプライバシーが保護されている。つまり、仮の名前での所有者を本当のＩＤＣＡ証明書にリンクする手段はない。

【０５４３】

一般的に、ＨｙｐｅｒＳｐｈｅｒｅは、ネットワーク操作、パケット伝送、およびセキュリティクレデンシャル情報に時間と状態に基づく動的な変化を採用し、ＳＤＮＰ時空間メッシュネットワークへの侵入が成功する確率、またはＨｙｐｅｒＳｐｈｅｒｉｃトランザクション処理に対する侵入が成功する確率を大幅に低下させている。これは、任意のデータグラムがコードブレークされない可能性があるということではなく、パケットの内容が限られており、寿命が短く、コンテキストメタデータがないため、攻撃の被害が限定的であることを意味している。

【０５４４】

シーケンシャルクオンタムキー

【０５４５】

失われたルートＣＡ証明書を回復し、破損したアカウントのＩＤを復元するために、ＨｙｐｅｒＳｐｈｅｒｅには、最後の手段として、ここではシーケンシャル量子鍵（ＳＱＫ）として紹介されている独自の暗号化デバイスが含まれている。ＳＱＫが適切にデコードされると、その所有者は、ルートＣＡ認証書を開いて復元し、破損したアカウントの正当な所有権を取り戻すことができる。観察者が観察することで観察された現実に影響を与え

るという量子オブザーバー効果の原理に基づいて、シーケンシャル量子キーでは、キーの内容を忠実に再現するだけでなく、各セルが表示され入力されるシーケンスを正確に実行する必要がある（比喩的には多次元ルービックキューブのように）。シーケンスが間違って実行された場合、適切な組み合わせが現れることはない。オブザーバー効果により、ブルートフォース攻撃がより困難になる一方で、関連性のないメディアコンテンツのパスフレーズのアーカイブとシーケンスをユーザが分離できるようになる。

【０５４６】

暗号経済学

【０５４７】

一般的に受け入れられている定義はないが、本稿の文脈では、「ｃｒｙｐｔｏｅｃｏｎｏｍｉｃｓ」という用語を最も単純な解釈で使用し、暗号通貨の使用を含む電子商取引を意味する。この文脈では、暗号通貨ベースの取引および電子商取引には、暗号通貨の生成、分散型金融取引、陪審員のコンセンサスに基づく取引の検証、スマートコントラクトの実行、および暗号インセンティブが含まれる。過去１０年間で、暗号通貨、ブロックチェーン技術、スマートコントラクトの出現は、特に資金調達、ベンチャーキャピタル、銀行、資本の分散化、情報管理のための企業の覇権に挑戦するなど、ビジネスに深遠で有益な影響を与えてきた。これらの成果にもかかわらず、主要なビジネス分野、特にリスクの高い分野では、仮想通貨やブロックチェーン技術の応用や商業的な受け入れは予想通りには進んでいない。以下に説明するように、多くの問題が今日の暗号ベースの経済モデルを悩ませている。

【０５４８】

（１）暗号経済１．０の問題点

【０５４９】

すべての現在の暗号通貨ベースの商取引、すなわちｃｒｙｐｔｏｅｃｏｎｏｍｉｃｓ１．０は、特定の基本的な共通点と関連する欠陥や脆弱性に依存している。

・すべての取引はインターネット上で発生し、固有のセキュリティ脆弱性（中間者攻撃、信頼攻撃、ウイルス感染など）の対象となる。

・ＣＡ証明書に基づく識別が盗まれたものか不正なものかを判断したり、マルウェアの感染（破損した証明書を介して配信されたもの）を防ぐための確実な方法はない。

・ブロックチェーンに対する約１５０の攻撃が知られており、その多くは窃盗、詐欺、二重支出が関与している。

・サイバー犯罪や仮想通貨犯罪の大部分は、特に多国籍企業のハッキングが絡んだものは処罰されないが、その理由の一つには、法務当局がサイバー犯罪に対処するための設備が整っていないことや、司法の管轄権の問題もある。

・共謀者とサイバーボットのピア投票制御により、様々な悪用、５１％攻撃、ネズミ講などが、疑う余地のないコイン保有者やトレーダーに悪用される可能性がある。

・破損したスマートコントラクトは、影響を与えることなく詐欺やねずみ講に使われてしまいる。

・従来の仮想通貨の生成は、その設計上、根本的にエネルギー効率が悪く、エコ的に有害である。

【０５５０】

最後の箇条書きは、ｃｒｙｐｔｏ－ｅｃｏｎｏｍｙ　１．０のエコロジカルな課題を強調している。本質的には、ビットコインのマイニングの基礎となるＰｒｏｏｆ－ｏｆ－Ｗｏｒｋは、もともと暗号通貨のためではなく、攻撃者が攻撃を開始するためにエネルギーを浪費し、お金を費やすことを強制することで、サービス拒否攻撃を間引くために作成された。残念なことに、同じメカニズムは今、すべてのＰｏＷの仮想通貨を生成するために使用されている（そして当然のことながら）エネルギーの膨大な量を無駄にしている。また、話題になっているにもかかわらず、Ｐｒｏｏｆ－ｏｆ－Ｓｔａｋｅのようなコンセンサスベースの暗号通貨のような代替品は、広く普及していない。さておき、前述の懸念から、ｃｒｙｐｔｏｅｃｏｎｏｍｉｃａｌｌｙいくつかの主要な基本的な欠陥が含まれてお

り、ｃｒｙｐｔｏ－ｅｃｏｎｏｍｙ　１．０の悩みの種となっている。
・Ｐｒｏｏｆ－ｏｆ－Ｗｏｒｋ世代の仮想通貨は、人為的に作られたコイン不足（報酬が減少する生産量の制限）に依存しており、カウントダウンが価格変動を煽り、悪用を招く。
・不正なブロックでブロックチェーンの整合性を「転覆」することを目的としたブロックチェーンからのハードフォークは、メインチェーン上で競合する有効なトランザクションとサイドフォークの間で激しい法的論争を巻き起こす。
・今日の暗号通貨は、実際には何もしていない。暗号通貨のマイニングと取引から、ハッシュナンスの謎解きを使用して、電子商取引や任意の実際の製品を提供する上では何の関係もないのである。
・長く重たいブロックチェーン暗号通貨は、今日の迅速な電子商取引の必要性とは相容れない（悪化の一途をたどる）取引レートに悩まされている。
・直接的なブロックチェーン決済を繰り返し使用すると、ブロックチェーンやウォレットがバックトレースや盗難に晒される。
・現在のスマートコントラクトは、全会一致のコンセンサスが必要であるため、最も遅い参加者により、連続的な取引レートが制限されている。
・ＰｏＷの暗号通貨、特にビットコインとイーサのボラティリティは、取引に興味のない事加盟店が暗号通貨を保有することを妨げ、取引時にのみ暗号通貨を購入することを余儀なくされている。
・ブロックチェーン攻撃は非常に定期的に発生している。熟練した加害者がブロックチェーンのブロック全体を制御することで、コインの所有者は自分たちの暗号通貨へのアクセスを無名の加害者に奪われてしまうことになり、法的な手段や手段もなく、損失を回復したり、正義を求めたり、加害者を特定したりすることすらできなくなる。

【０５５１】

最後の２つの箇条書きは、暗号経済学の現状のリスクを浮き彫りにしている。特に加盟店や企業は、（ｉ）価格があまりにも不安定で、（ｉｉ）長期間保持されている場合、盗まれる可能性が高すぎるため、暗号通貨を調達し、長期間保持することができない。このため、仮想通貨のユーザは、スポット取引や同時売買取引でのみデジタル資産を購入し、同時に使用することを余儀なくされる。もう一つの問題は、通貨の安定性である。取引ベースのボラティリティと相まって、仮想通貨の平均価格の絶え間ない上昇は、企業の運営コストを不安定にするため、商取引のための媒体として仮想通貨を検討している企業にとっては特に不穏なものとなる。よく引用される謝罪文の一つである（ビットコインの投資家を鼓舞することを意図している）「５，０００万ドルのピザ」の逸話は、２０１０年に２枚のピザを１０，０００ビットコイン購入したという真実の物語を詳述している。これは２０１７年１１月の価値に直すと、購入はピザ1枚５０，０００，０００ドル相当になる。なお、６ヶ月後にはビットコインはその価値の２５％を失った。このようなボラティリティは、迅速な富を求める投機家を鼓舞するかもしれないが、企業や企業にとっては、乱暴に不安定な通貨の見通しは、常にその有用性を制限し、任意の本当の商業的な採用を妨げる恐ろしいものである。

【０５５２】

（２）二重暗号通貨のｅコマース

【０５５３】

「Ｃｒｙｐｔｏ－ｅｃｏｎｏｍｙ　１．０」の落とし穴を回避するために、ＨｙｐｅｒＳｐｈｅｒｅのｃｒｙｐｔｏｅｃｏｎｏｍｉｃシステムでは、個人ブロックチェーンの所有権を持つ独自に実装されたデュアル暗号通貨システム、つまり他のユーザと共有されないブロックチェーンを採用している。トランザクションの完全性を確保し、ピア間の信頼を確立するために、ＨｙｐｅｒＳｐｈｅｒｅのブロックチェーンは、動的な（ＤｙＤＡＧ）マルチツリー構造で他のブロックチェーンと不可分にリンクされている。ＨｙｐｅｒＳｐｈｅｒｅの暗号経済学はシンプルで、マイニングもハッシュも必要なく、パズルを解く必要もない。サービスプロバイダや商人は、ＨｙｐｅｒＣｏｎｔｒａｃｔｓを発行して、フィアット貨幣またはＨｙｐｅｒＣｏｉｎのいずれかを使用して通信、コンピューティン

グ、ストレージ機能を獲得する。図５８に示すように、ＨｙｐｅｒＳｐｈｅｒｅ１１００のリソースプロバイダ（ＨｙｐｅｒＮｏｄｅの所有者）は、リソースを加盟店に供給することで、鋳造１１０２ａまたはリサイクル１１０２ｂによってＨｙｐｅｒＣｏｉｎｓを獲得する。ＨｙｐｅｒＣｏｉｎの「鋳造」１１０２ａのためのＨｙｐｅｒＣｏｎｔｒａｃｔｓ１１０４では、加盟店１１０３は、フィアット貨幣１１１０で購入したＨｙｐｅｒＭｅｔａｌ１１０５を使用して（ＨｙｐｅｒＣｏｉｎ取引所を経由して）、ＨｙｐｅｒＭｅｔａｌ１１０５での支払いを契約で誓約する。契約が成功すると、リソースプロバイダ（１１０１）は、リリースされたＨｙｐｅｒＭｅｔａｌの誓約金を、各ＨｙｐｅｒＮｏｄｅの相対的な貢献度に応じて比例配分されたＨｙｐｅｒＣｏｉｎ１１１２に自動的に鋳造する。また、ＨｙｐｅｒＣｏｉｎの「リサイクル」を目的としたＨｙｐｅｒＣｏｎｔｒａｃｔｓ１１０４では、加盟店が契約によりＨｙｐｅｒＣｏｉｎでの支払いを誓約する（以前に獲得または購入したＨｙｐｅｒＣｏｉｎ１１０２ｂを使用）。契約が成功裏に完了すると、リソースプロバイダはオリジナルのＨｙｐｅｒＣｏｉｎ１１０２ｂを溶解し、各ＨｙｐｅｒＮｏｄｅの相対的な貢献度に応じて比例配分された新しいＨｙｐｅｒＣｏｉｎ１１１２にリサイクルする。新たに生成されたＨｙｐｅｒＣｏｉｎには、小規模なファイルと迅速なトランザクションを維持するための新しいデジタル暗号ＩＤが含まれている。リサイクルを通じて、ＨｙｐｅｒＣｏｉｎ保有者と消費者は、デジタル通貨の交換を必要とせずに、稼いだＨｙｐｅｒＣｏｉｎ暗号通貨１１１２ｂや購入したＨｙｐｅｒＣｏｉｎ暗号通貨をすぐに使用して直接商人に支払うことができ、高額な交換手数料を回避することができる。対照的に、鋳造するＨｙｐｅｒＣｏｎｔｒａｃｔｓを使用することで、加盟店はＨｙｐｅｒＣｏｉｎの取引や投機による市場の変動リスクを冒すことなく、ＨｙｐｅｒＭｅｔａｌ１１０５を保有または使用して事業を行うことができる。

【０５５４】

（３）ＨｙｐｅｒＳｐｈｅｒｅ　Ｃｒｙｐｔｏｅｃｏｎｏｍｉｃｓ

【０５５５】

ＨｙｐｅｒＳｐｈｅｒｅは、独自の暗号通貨生成方法、デュアル暗号通貨システム、実質的な電子商取引を容易にする実用性を備えており、Ｃｒｙｐｔｏ－ｅｃｏｎｏｍｙ　１．０の基本的な限界を克服している。

・ＨｙｐｅｒＳｐｈｅｒｅは、完全に分散化された方法で運用されるユーザコミュニティ所有のクラウド上で、クラウドベースの通信、コンピューティング、ストレージ、デバイスとクラウドの接続性、電子サービスを含む有意義なＥコマースを提供する。

・ＨｙｐｅｒＳｐｈｅｒｉｃ　ｃｒｙｐｔｏｃｕｒｒｅｎｃｙは、ネットワークネイティブのデジタルトークンを組み込んだもので、フィアット貨幣ベースの取引のような煩雑さを伴うことなく、ＨｙｐｅｒＳｐｈｅｒｅで意味のある電子商取引を行うために使用される。

・ＨｙｐｅｒＳｐｈｅｒｉｃの仮想通貨の生成は、人工的な希少性のデジタル資産を作成するために無用なパズルを解くマイニングを伴わない。

・ＨｙｐｅｒＣｏｉｎは、ＨｙｐｅｒＮｏｄｅｓをデバイス（またはデバイスのクラスタ）上でホストしている個人、企業、事業体が自動的に獲得するもので、ＨｙｐｅｒＮｏｄｅが参加しているＨｙｐｅｒＣｏｎｔｒａｃｔｓが成功した際に報酬が支払われる。

・ＨｙｐｅｒＮｏｄｅｓはＢＹＯＤにも対応しており、ビジネスアカウントと個人アカウントを共通のプラットフォーム上で共存させることができ、ファイルやデータが混在することもなく、（個人所有のデバイスを除いて）設備投資も不要である。

・ビットコインの採掘者とは異なり、ハイパーコイン採掘者は暗号通貨を生成するために大量のエネルギーを消費したり、一定の報酬やＲＯＩのない採掘装置への設備投資のリスクを負う必要がない。

・加盟店やサービスプロバイダは、ＨｙｐｅｒＭｅｔａｌを購入、保管、段階的に使用して、ＨｙｐｅｒＳｐｈｅｒｉｃの運用資金を調達することができ、その結果、ＨｙｐｅｒＣｏｉｎの価格変動がネットワーク利用に与える影響を回避することができる。

・リスク許容度の高いトレーダー、投資家、投機家は、制限なくＨｙｐｅｒＣｏｉｎを自

由に売買することができ、ＨｙｐｅｒＣｏｉｎの価格変動やボラティリティから恩恵を受ける可能性がある。

【０５５６】

図５９には、ＨｙｐｅｒＳｐｈｅｒｅの経済モデルが簡略化されているが、資本注入とＨｙｐｅｒＣｏｉｎのリサイクルの両方を通じた経済成長の推進力を概略的に表している。このように、ＨｙｐｅｒＳｐｈｅｒｅ１１００は、ＨｙｐｅｒＣｏｎｔｒａｃｔを完了させるためのタスクを実行するリソースプロバイダであるＨｙｐｅｒＮｏｄｅｓの運用を通じて、経済的価値を生み出している。ＨｙｐｅｒＳｐｈｅｒｉｃの運営による経済成長の推進力は、次の２つの方法で明らかになる。（ｉ）製品の創出やサービスの提供を通じて実現する、商人やサービスプロバイダの企業価値ΔＥＶの増加、（ｉｉ）ＨｙｐｅｒＮｏｄｅの所有者に支払われる新しいＨｙｐｅｒＣｏｉｎ（ＨＣ）の鋳造。つまり、サービス提供者やリソース提供者（ＨｙｐｅｒＳｐｈｅｒｅユーザのコミュニティ）がＨｙｐｅｒＳｐｈｅｒｉｃ電子商取引の経済的利益者であり、大手通信会社やソーシャルメディア企業ではなく、ＨｙｐｅｒＳｐｈｅｒｅプラットフォームでもないのである。ＨｙｐｅｒＳｐｈｅｒｅの経済的利益は、造幣とリサイクル（溶融）という２つのプロセスを使用して発生する。

【０５５７】

鋳造時には、フィアット通貨１１１０という形でＨｙｐｅｒＳｐｈｅｒｅに新たな資本が注入され、ＨｙｐｅｒＭｅｔａｌ１１０５に変換されてから「増幅」し、企業価値ΔＥＶ（１１３１）とＨｙｐｅｒＣｏｉｎ価値V_{HC}１１３２からなる付加価値が（ΔＥＶ＋V_{HC}）という代数的な形で生み出される。造幣時には、ＨｙｐｅｒＣｏｉｎは、受け取ったコインの枚数ＨＣと自由市場のＨｙｐｅｒＣｏｉｎ交換レートＨＸＲに基づいて、即時のＨｙｐｅｒＣｏｉｎ価値V_{HC}を持つ（ここで、ＶＨＣ＝(ＨＣ・ＨＸＲ）。コイン１１３２ａが稼いだコインを同時に売却する場合（１１３４）、ＨｙｐｅｒＣｏｉｎの取引価格ＨＸＲの変動性、つまり特定の国のフィアット通貨への交換レートは、ＨｙｐｅｒＮｏｄｅの所有者が稼ぐフィアット通貨の利益の要因にはならない。模式的に説明すると、鋳造による価値の創出は、ＨｙｐｅｒＮｏｄｅに担保されたＨｙｐｅｒＭｅｔａｌ（ＨＭ）１１０５の量（差分増幅器への入力として示されている）と、新しいＨｙｐｅｒＣｏｉｎを鋳造するＨｙｐｅｒＮｏｄｅ１１３０の増幅価値利得A_v（交渉された各ＨｙｐｅｒＣｏｎｔｒａｃｔで指定された報酬値）のみに依存している。ＨｙｐｅｒＭｅｔａｌの購入価格（１１１１）はネットワークの（比較的安定した）ビットコストに基づいているため、ＨｙｐｅｒＣｏｉｎの取引価格の変動は、獲得したＨｙｐｅｒＣｏｉｎには影響を与えない（差分増幅器によって増幅されないコモンモードノイズとしてグラフィカルに表現される挙動）。要約すると、鋳造では、ＨｙｐｅｒＭｅｔａｌ１１０５は、需給市場のダイナミクスに基づいて、様々な数のＨｙｐｅｒＣｏｉｎ１１３２に変換される（システムのゲイン）。

【０５５８】

ＨｙｐｅｒＮｏｄｅ１１３０）アンプへの２つ目の経済的入力である「ＨｙｐｅｒＣｏｉｎのリサイクル」は、新しいＨｙｐｅｒＣｏｉｎを生産するのではなく、古いコイン１１３２ｂを溶かしてリサイクルし、より少ない量の新しいコインを生成する。アンプ１１３０への負の入力として表示されているが、リサイクル（１１３５）によって流通するＨｙｐｅｒＣｏｉｎｓ数が減るため、加盟店はＨｙｐｅｒＳｐｈｅｒｅに新たな資金を投入することなく商行為を行うことができる。リサイクルの際には、初期のＨｙｐｅｒＣｏｉｎｓ（ＨＣ）の量は、より少ない量（β　ＨＣ）に減少する（なお、ここでβは０％から１００％の範囲であり、保持されている。つまりリソースプロバイダに支払われ、流通し続けているＨｙｐｅｒＣｏｉｎの割合を表す）。リサイクルの結果として流通するＨｙｐｅｒＣｏｉｎの価値変化は、ΔV_{HC}＝（ＨＣ－ＨＸＲ）（１－β）で与えられ、その一部は商品やサービスとして商取引業者やサービス提供者に届けられる。企業価値の変化はＨｙｐｅｒＣｏｉｎ価値の変化$\Delta EV \propto \Delta V_{HC}$に比例するが、一定の比率に従うのではなく、市場の状況によって変化する。要約すると、リサイクルはＨｙｐｅｒＳｐｈｅｒｅ

の経済を成長させないが、不況期には電子商取引を促進する。溶解はまた、負の経済フィードバックとしても機能し、ハイパーコインの一部を着実に流通から取り出すことで、暗号経済的に安定性を向上させる。

【０５５９】

ＨｙｐｅｒＣｏｉｎの溶融による安定化効果と、経済成長に応じた新しい通貨の生成能力を組み合わせることで、ＨｙｐｅｒＳｐｈｅｒｅは、ＨｙｐｅｒＣｏｉｎの取引価格の変動に影響を受けず、安定したクローズドループシステムでダイナミックな電子商取引をサポートすることが可能になる。景気が拡大している時期には、資源を求める加盟店による新たな資金注入により、ＨｙｐｅｒＳｐｈｅｒｅのＨｙｐｅｒＭｅｔａｌ１１０５とＨｙｐｅｒＣｏｉｎ１１３２の両方のマネーサプライが増加し、市場の需要の拡大をサポートする。景気後退期には、新たな資金注入が減少するため、ＨｙｐｅｒＳｐｈｅｒｅ経済は自然に収縮し、未使用のＨｙｐｅｒＭｅｔａｌ１１０５が消費され、最終的にはＨｙｐｅｒＣｏｉｎ１１３２ｂがリサイクルされることで、流通するコインが減少し、市場での売却に対抗して通貨が安定するようになる。このようにして、ＨｙｐｅｒＳｐｈｅｒｅの暗号経済は、ビジネス企業というよりも、国に近い形で運営されている。

【０５６０】

コミュニティ

【０５６１】

ＨｙｐｅｒＳｐｈｅｒｅは、情報の独占的な制御を禁止し、ネットワーク帯域幅の不当な確保を阻止することを目的とした規制や立法の取り組みをはるかに超えて、経済的には「ネット中立性」の真髄を体現している。ＨｙｐｅｒＳｐｈｅｒｅの分散型クラウドネットワークは、ＨｙｐｅｒＮｏｄｅｓをホストする企業や一般市民によって所有・運営されており、ＨｙｐｅｒＳｐｈｅｒｅはまさに人々のネットワークとなっている。この点で、ＨｙｐｅｒＳｐｈｅｒｅは、現在の暗号経済学とは比較にならないほどユニークな存在となっている。

【０５６２】

複数のサーバ、コンピュータ、モバイルデバイスを所有している個人、企業、研究機関は、ＨｙｐｅｒＮｏｄｅポータルソフトウェアを各コンポーネントデバイスにダウンロードし、それらを「クラスタ」として単一のＩＤ－トラストチェーンが所有する１つのアカウントにリンクさせることができる。デバイスをクラスタリングすることの利点は２つある。第一に、クラスタが獲得したＨｙｐｅｒＣｏｉｎ暗号通貨の収益をすべて単一のブロックチェーンに割り当て、グループのより大きな利益のために使用することができる。第二に、クラスタ化されたデバイスで実行される通信やタスクは、安全な相互接続性を確立するためにＨｙｐｅｒＳｐｈｅｒｅに支払われる報酬を必要とせず、単一の接続デバイスとして動作する。このようにして、企業は、パブリックなＨｙｐｅｒＳｐｈｅｒｅネットワーク内に仮想的なプライベート企業ネットワークを作成して運用することができ、プライベートな機能を持ちながらも、機会があればリソースを募ったり、暗号通貨を獲得したりすることができる。デバイスクラスタリングのもう１つの機会は、ゲームコミュニティにある。グローバルなゲームコミュニティでも、デバイスクラスタリングの恩恵を受けることができる。特定のゲームのためのアドホックなソサエティを作成し、ＨｙｐｅｒＳｐｈｅｒｅ上で動作する独自のパブリック－プライベートネットワークを使用する。このような場合、ＨｙｐｅｒＳｐｈｅｒｅは、ＨｙｐｅｒＣｏｉｎやＨｙｐｅｒＭｅｔａｌの暗号通貨とは別に、ゲーマーのためのトークン化プラットフォームとしても利用することができる。

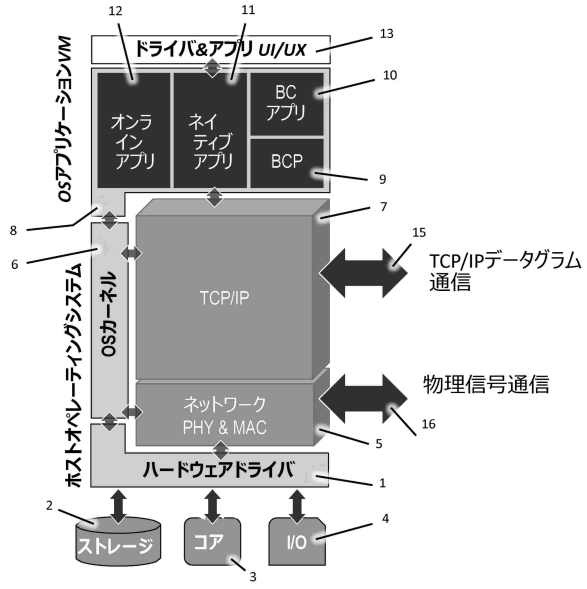
【０５６３】

また、ＨｙｐｅｒＳｐｈｅｒｅはコラボレーションもサポートしている。たとえば、２つの大学がそれぞれ独自のＨｙｐｅｒＮｏｄｅクラスタを運用している場合、ＨｙｐｅｒＣｏｎｔｒａｃｔを使用して、お互いの支援や協力を得ることができる。このように、協力の状況を定義するＨｙｐｅｒＣｏｎｔｒａｃｔでは、大学が他大学から計算能力を借りることができるタイミングと、支払うべき対価が指定されている。ＨｙｐｅｒＳｐｈｅｒ

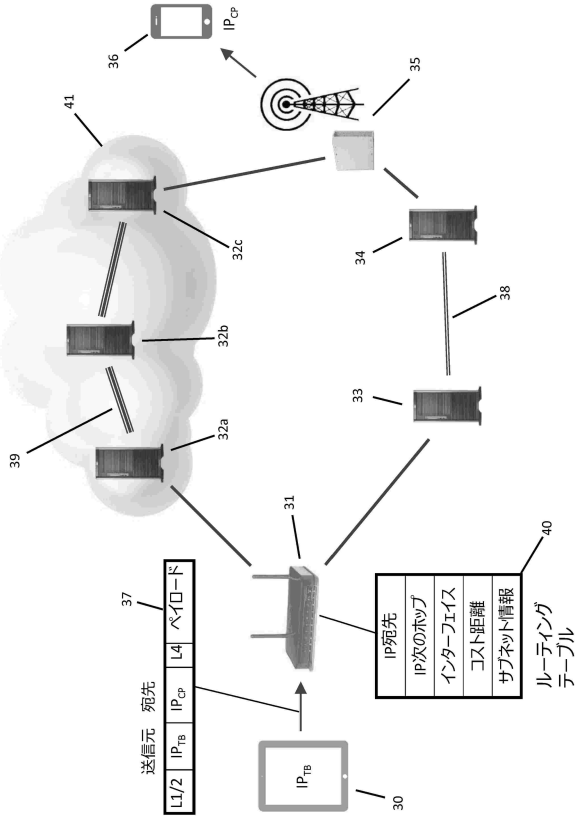
ｅを利用することで、サーバファーム、ビットコインのマイニングファーム、スーパーコンピュータの遊休容量を無駄にする必要がなくなり、代わりに、地球とその住民が直面している複雑な計算集約型の課題の解決に貢献することができるようになる。最後に、ＨｙｐｅｒＳｐｈｅｒｅは、慈善団体や非営利団体を支援することができる。寄付金は、サービスの支払いに使われたり、元の寄付金よりも多くの仮想通貨資産を生成できるＨｙｐｅｒＮｏｄｅホスティングプラットフォームに資金を提供したりすることができる。つまり、寄付を「増幅」してより大きな利益を得ることができるのだ。

【図面】

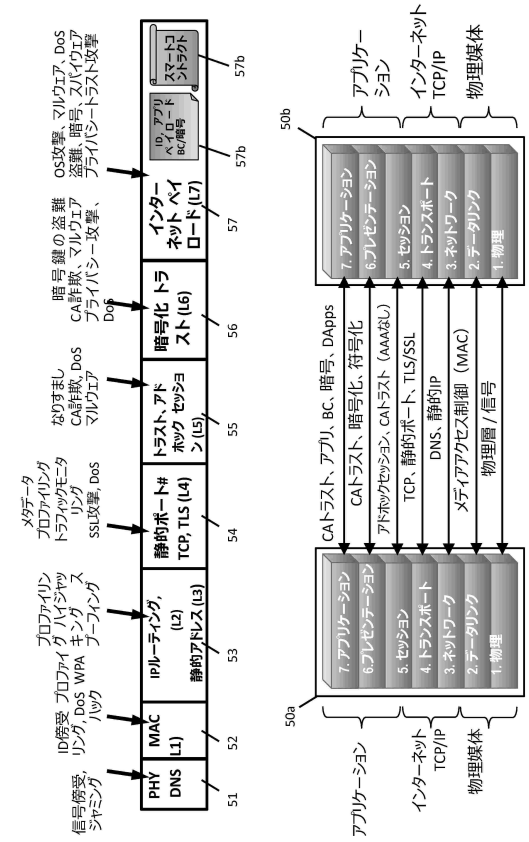
【図１】



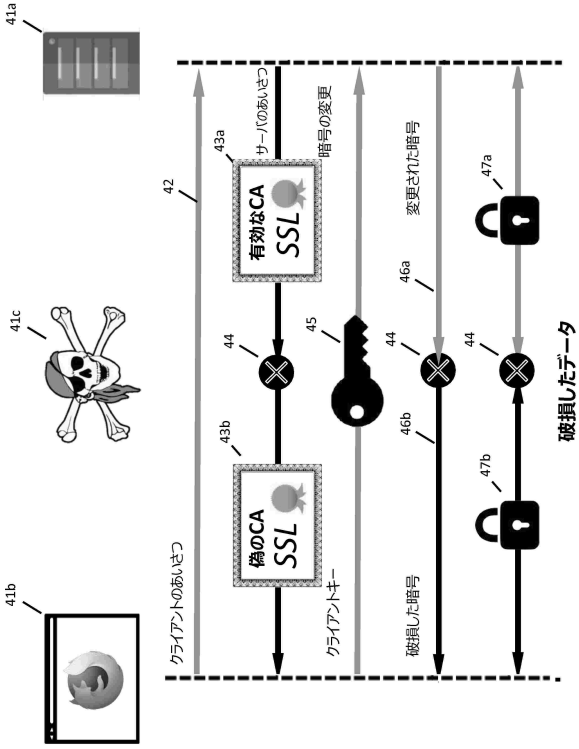
【図２】



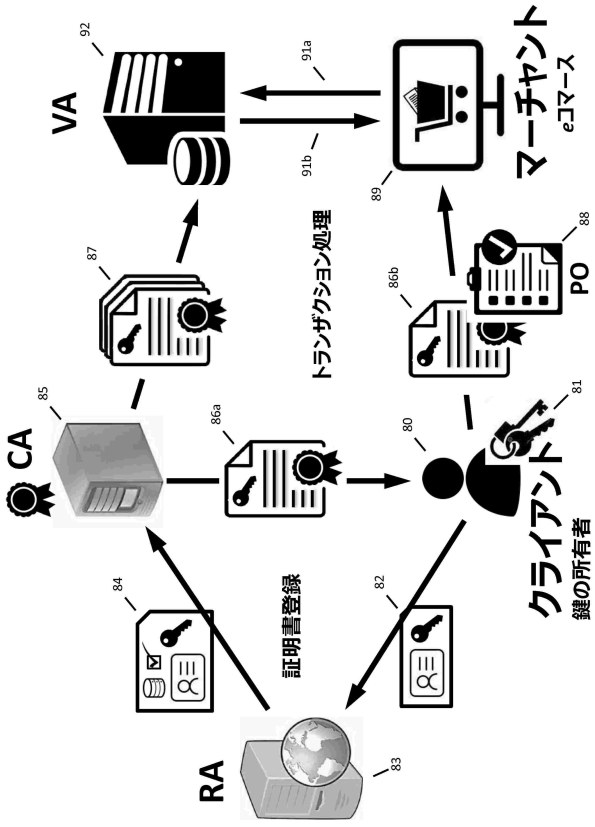
【図３】


PHY
DNS
MAC (L1)
IPルーティング, (L2)
静的アドレス (L3)
静的ポート# TCP, TLS (L4)
トラスト、アドホック セッション (L5)
暗号化 トラスト (L6)
インターネット ペイロード (L7)
51
52
53
54
55
56
57
57b
信号傍受, ジャミング
ID傍受, リンク, DoS
プロファイリング ハイジャック WPA キング ブーフィング ハッシュ
メタデータ プロファイリング トラフィックモニタ リンク SSL攻撃, DoS
なりすまし CA詐欺, DoS マルウェア
暗号鍵の盗難 CA詐欺、マルウェア プライバシー攻撃、 DoS
OS攻撃、マルウェア、DoS 盗難、暗号、スパイウェア プライバシートラスト攻撃
50a
50b
CAトラスト、アプリ、BC、暗号、DApps
CAトラスト、暗号化、符号化
アドホックセッション、CAトラスト（AAAなし）
TCP、静的ポート、TLS/SSL
DNS、静的IP
メディアアクセス制御（MAC）
物理層 / 信号
アプリケーション
インターネット TCP/IP
物理媒体

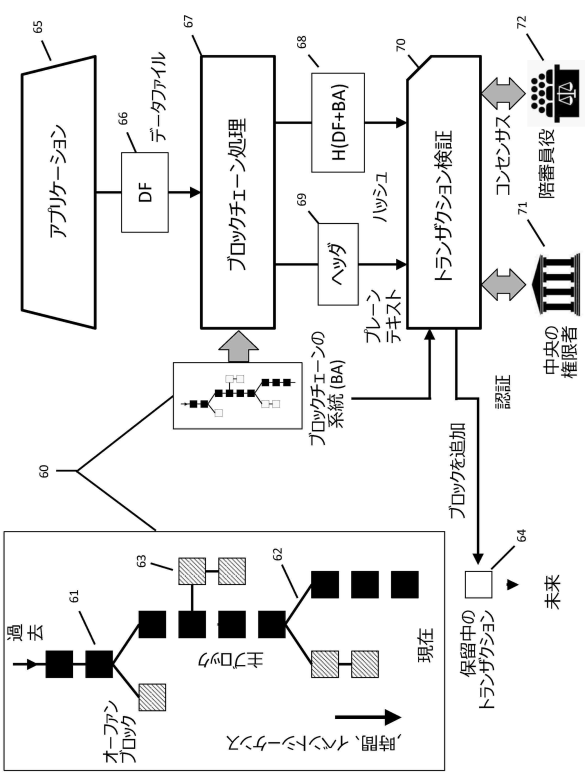
【図４】


41a
41b
41c
42
43a
43b
44
45
46a
46b
47a
47b
有効なCA SSL
偽のCA SSL
サーバのあいさつ
暗号の変更
変更された暗号
破損した暗号
クライアントのあいさつ
クライアントキー
破損したデータ

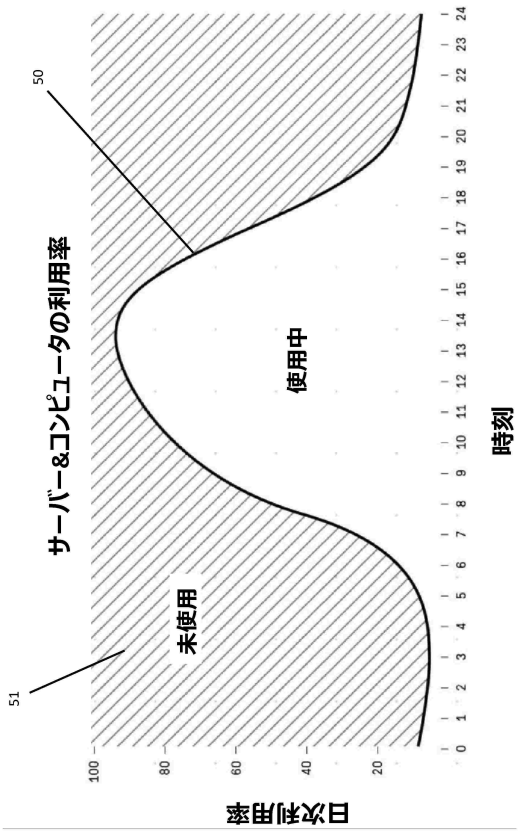
【図５】


CA
VA
RA
マーチャント
eコマース
PO
クライアント
鍵の所有者
証明書登録
トランザクション処理
81
82
83
84
85
86a
86b
87
88
89
91a
91b
92

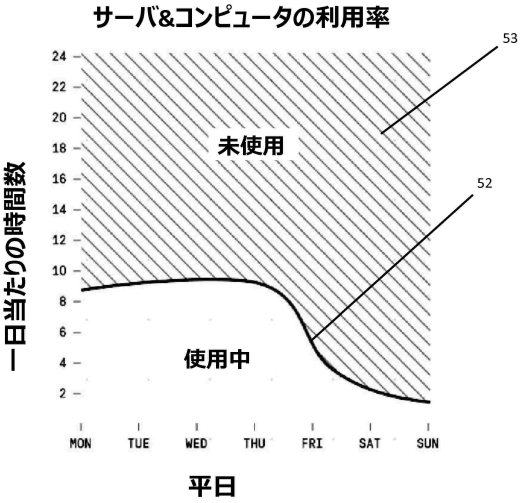
【図６】


アプリケーション
DF
データファイル
ブロックチェーン処理
H(DF+BA)
ヘッダ
ハッシュ
ブロックチェーンの系統 (BA)
プレーンテキスト
トランザクション検証
コンセンサス
陪審員役
中央の権限者
認証
ブロックを追加
保留中のトランザクション
未来
現在
過去
ブランチ
オーファンブロック
60
61
62
63
64
65
66
67
68
69
70
71
72

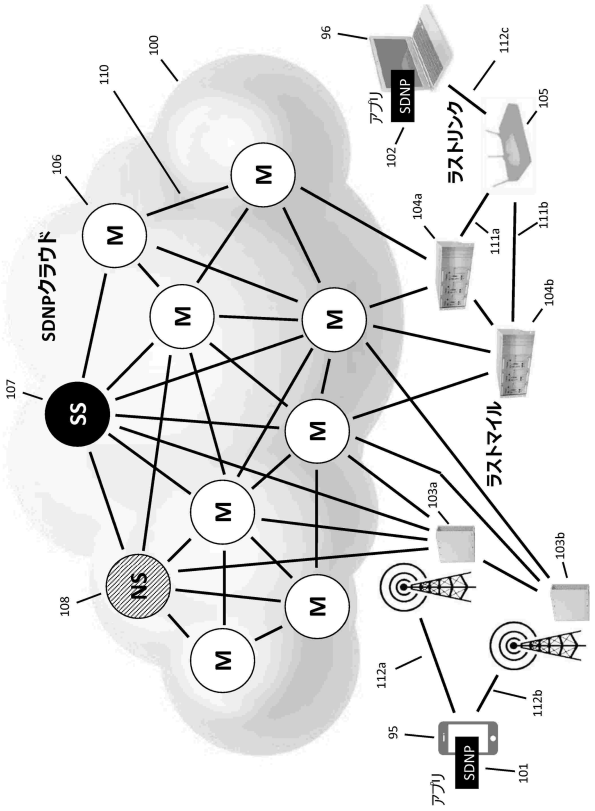
【図７Ａ】



【図７Ｂ】



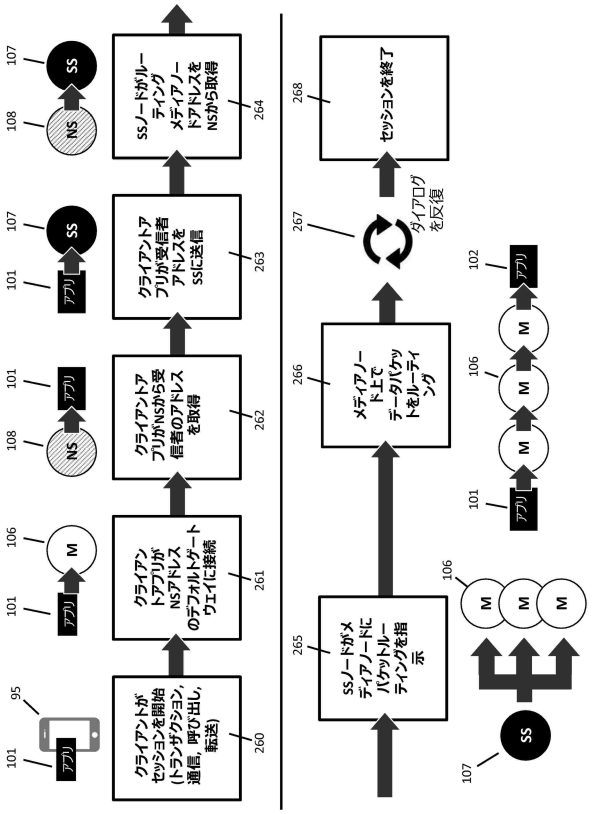
【図８】



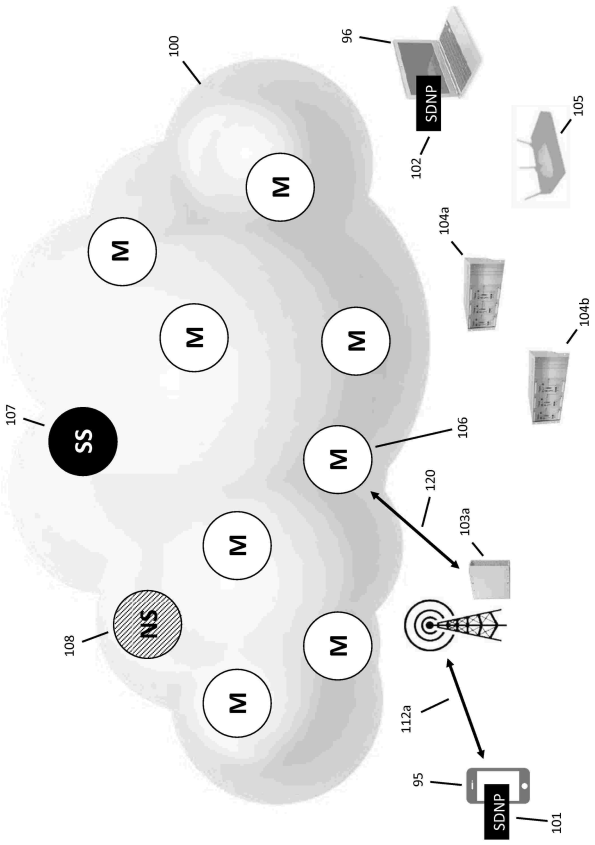
【図９】

コンポーネント	名称	実装	プロトコル
108 NS	SDMPネームサーバノード	130 SDNP NSソフトウェア 133	SDNP ルーティング
107 SS	SDMPシグナルサーバノード	130 SDNP SSソフトウェア 134	SDNP ルーティング
106 M	SDNPメディアノード＋DMZ	130a DMZソフトウェア 136 140 131 SDNP Mソフトウェア 135	SDNP ルーティング
105	WiFiルータ	ISPネットワークルーティングテーブル 137	TCP/IP ルーティング
104	イーサネットルータ	ISPネットワークルーティングテーブル 138	TCP/IP ルーティング
103	無線ネットワーク	132 NAT モバイルネットワークルーティング 139	無線通信事業者のルーティング

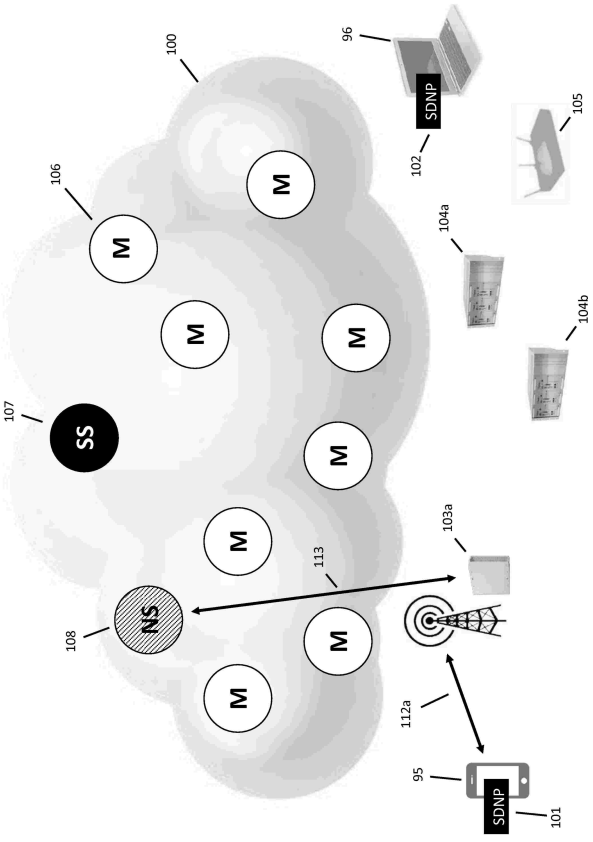
【図１０】



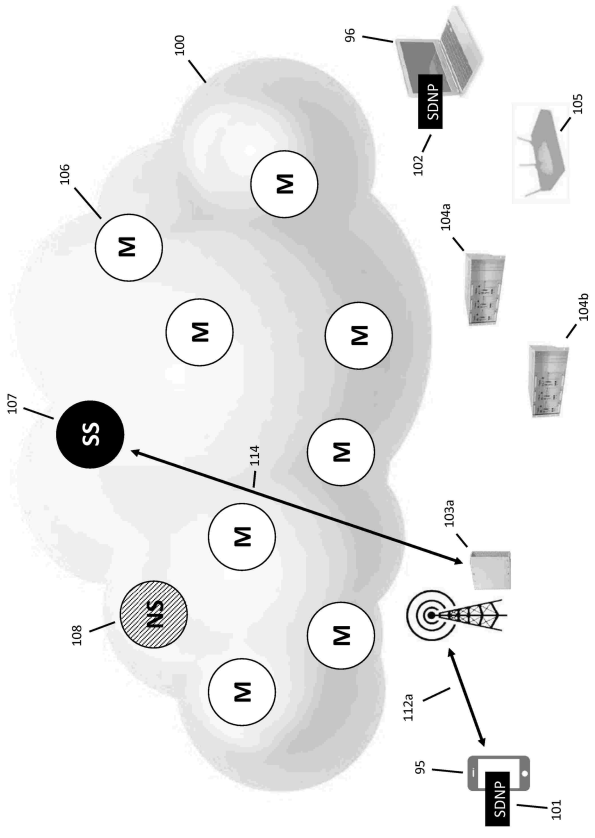
【図１１Ａ】



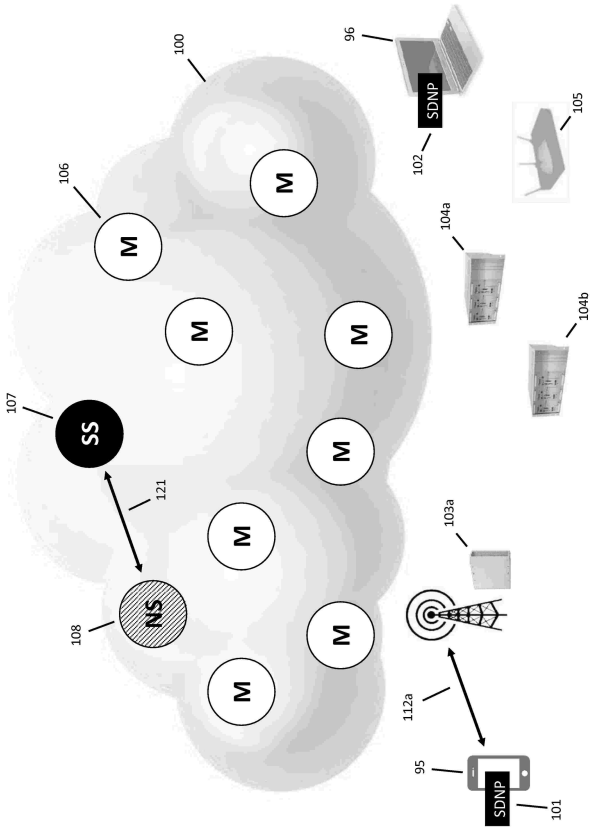
【図１１Ｂ】



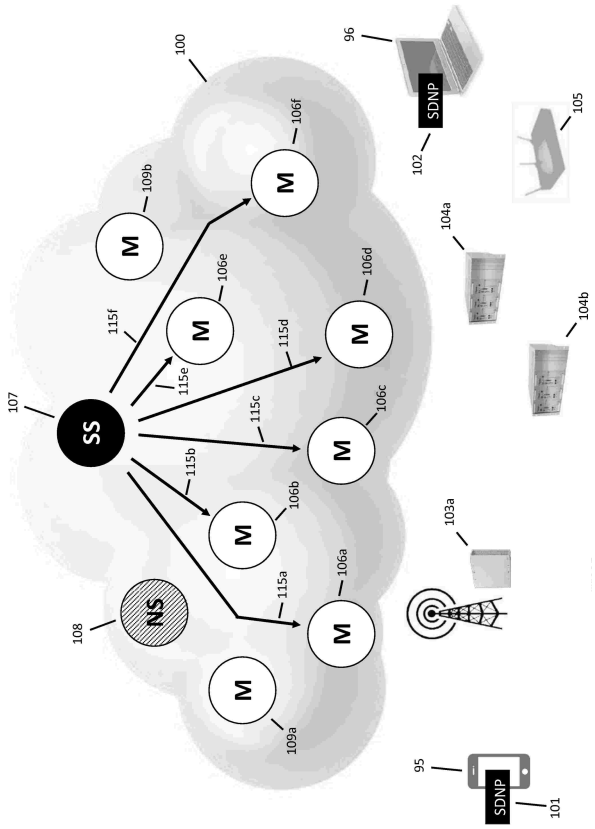
【図１１Ｃ】



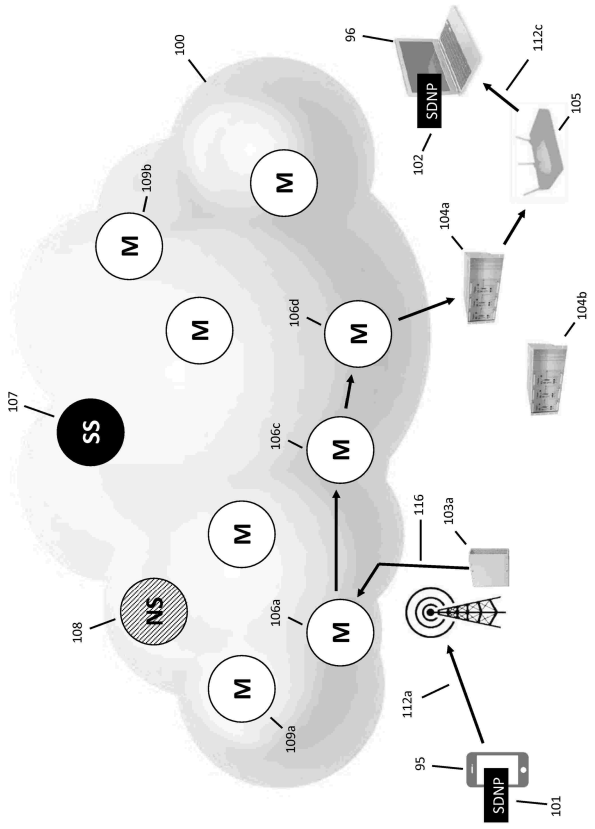
【図１１Ｄ】



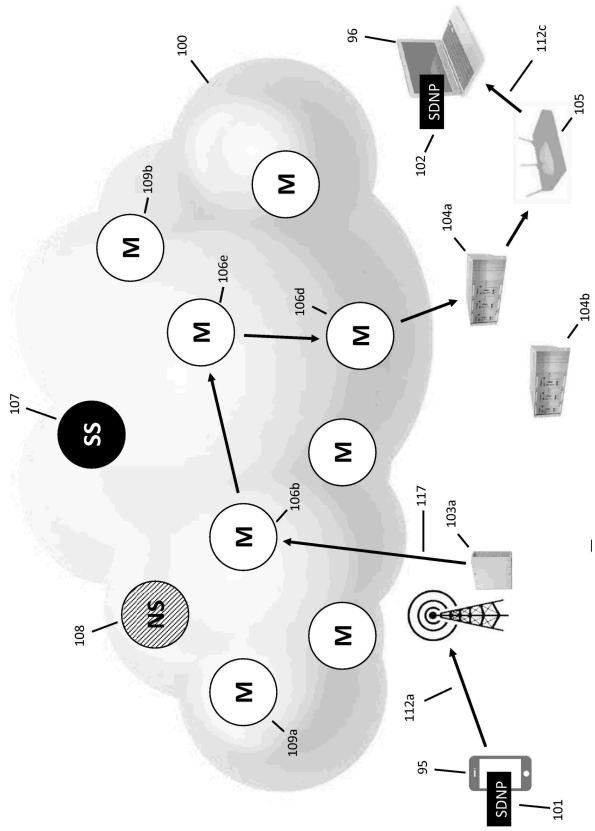
【図１１Ｅ】



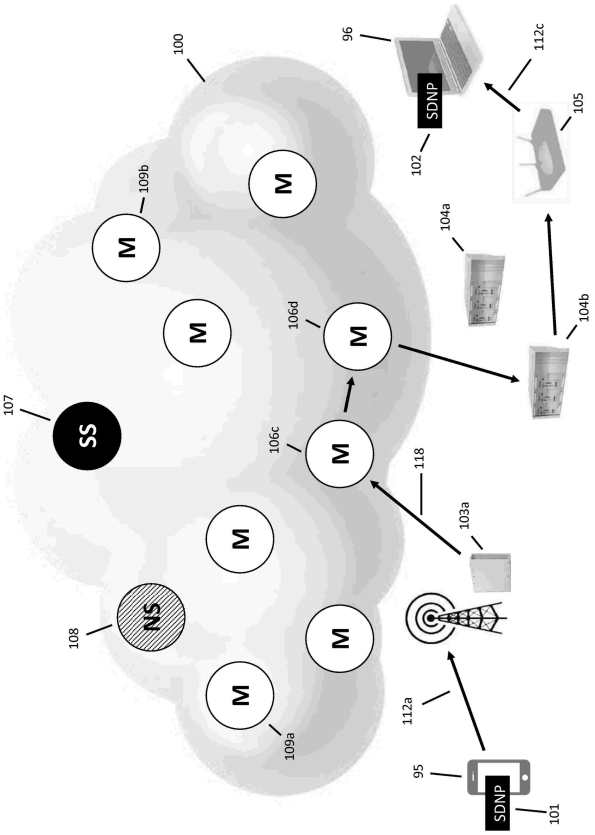
【図１１Ｆ】



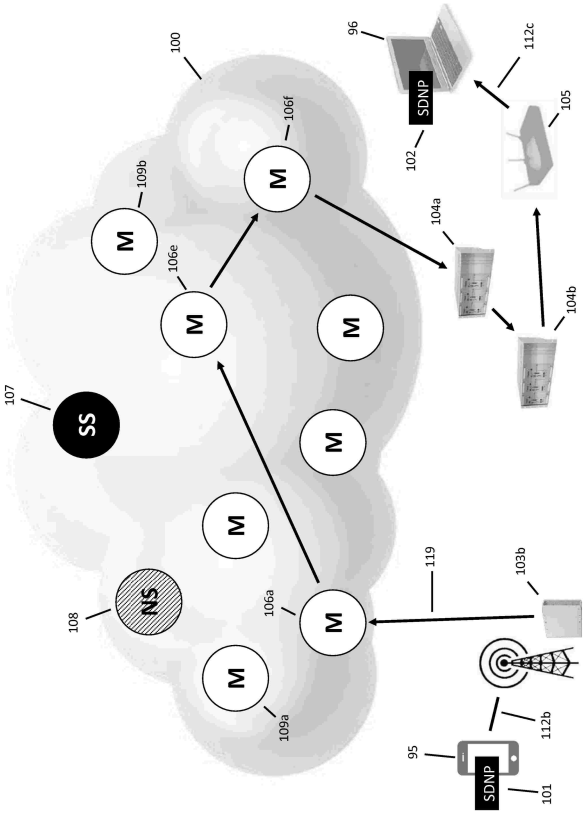
【図１１Ｇ】



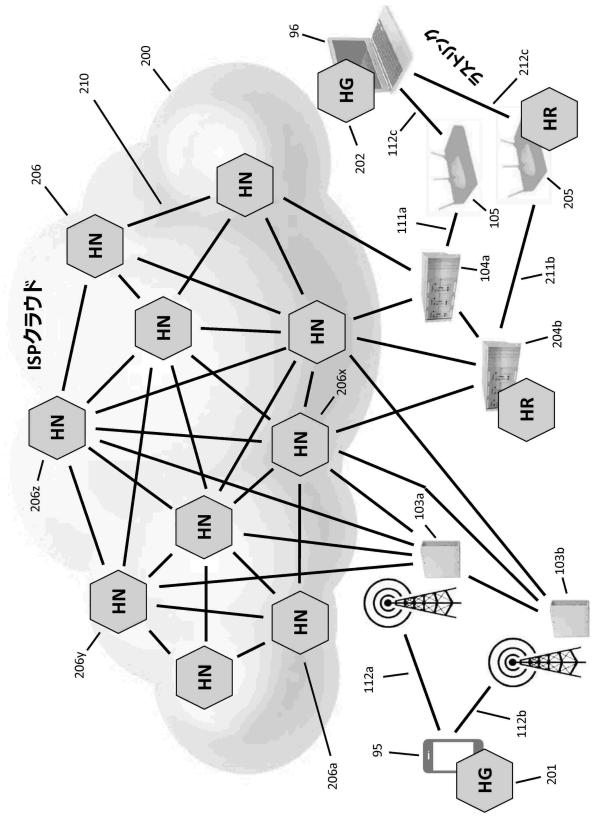
【図１１Ｈ】



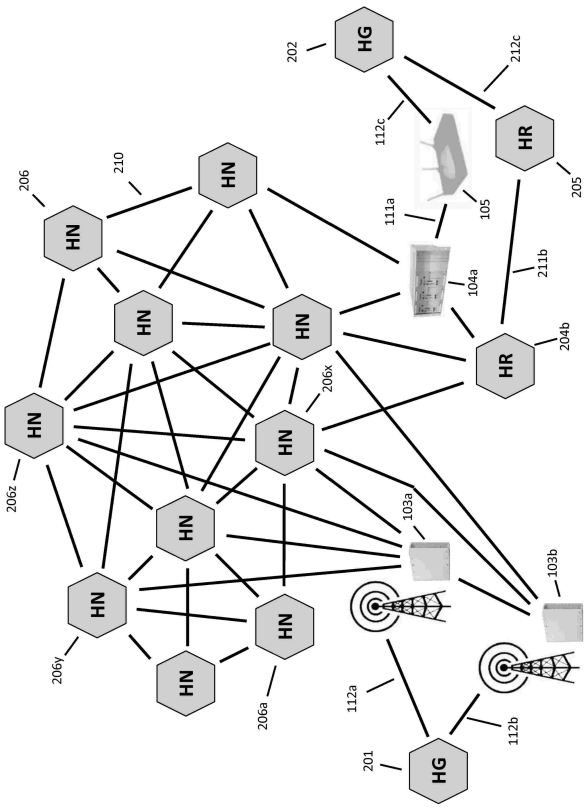
【図１１Ｉ】



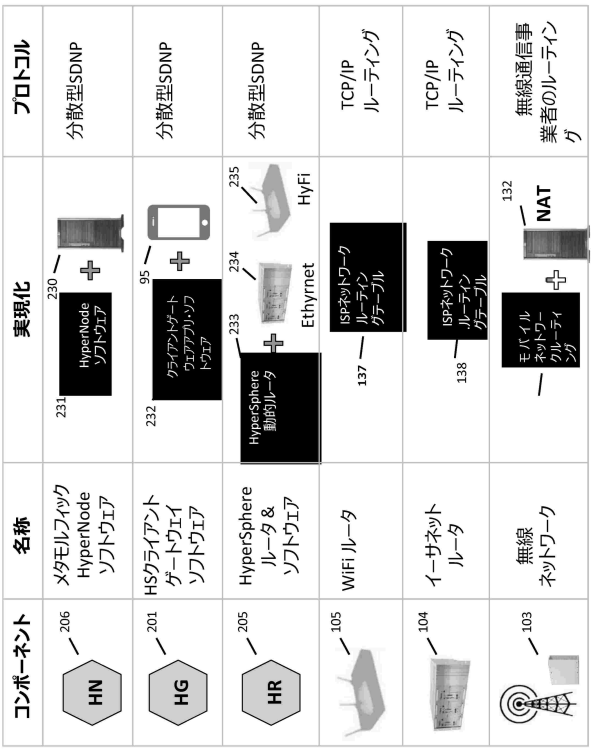
【図１２Ａ】



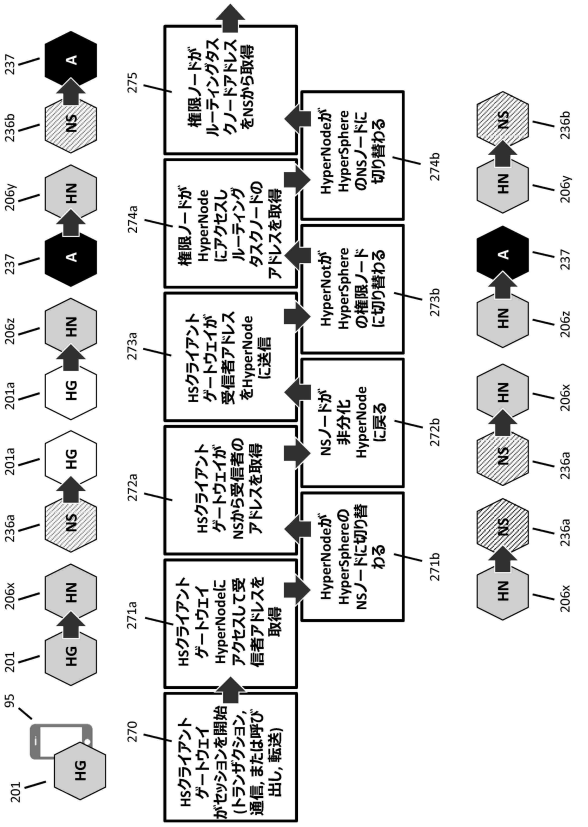
【図１２Ｂ】



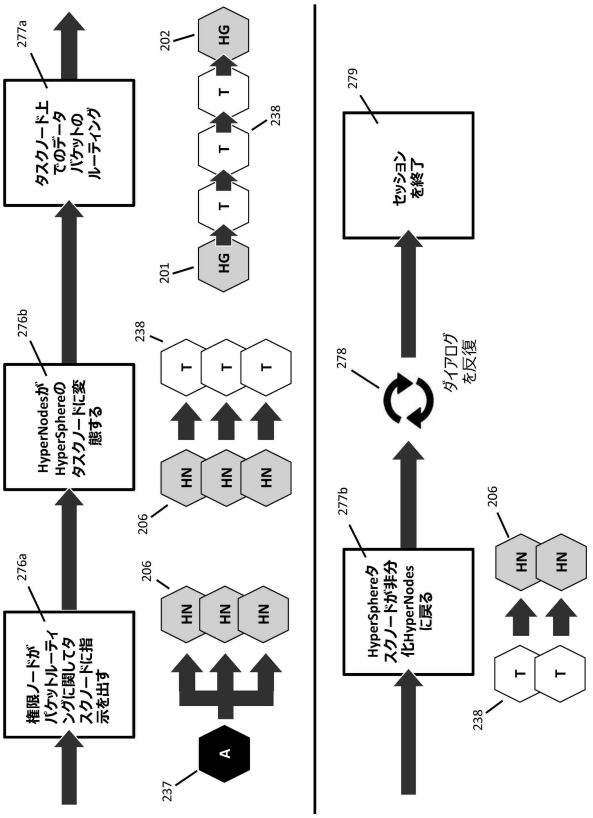
【図１２Ｃ】



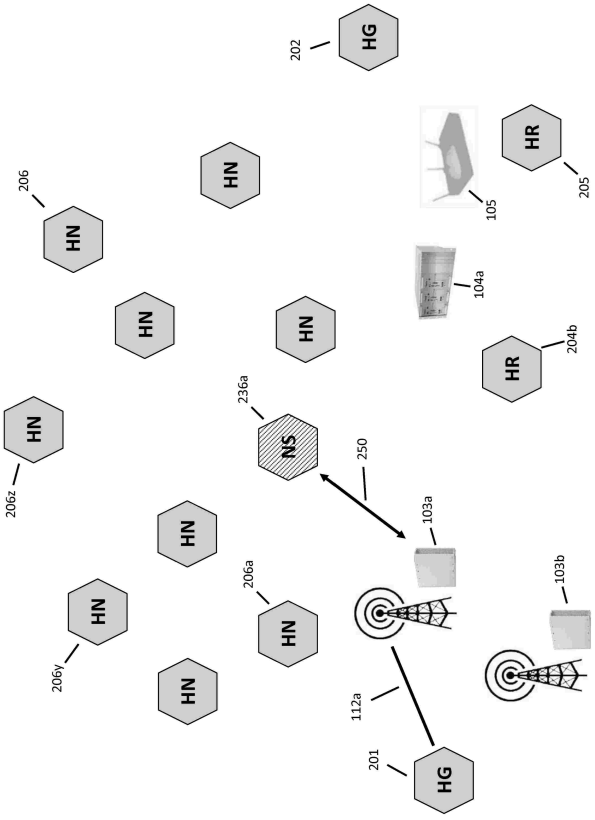
【図１２Ｄ】



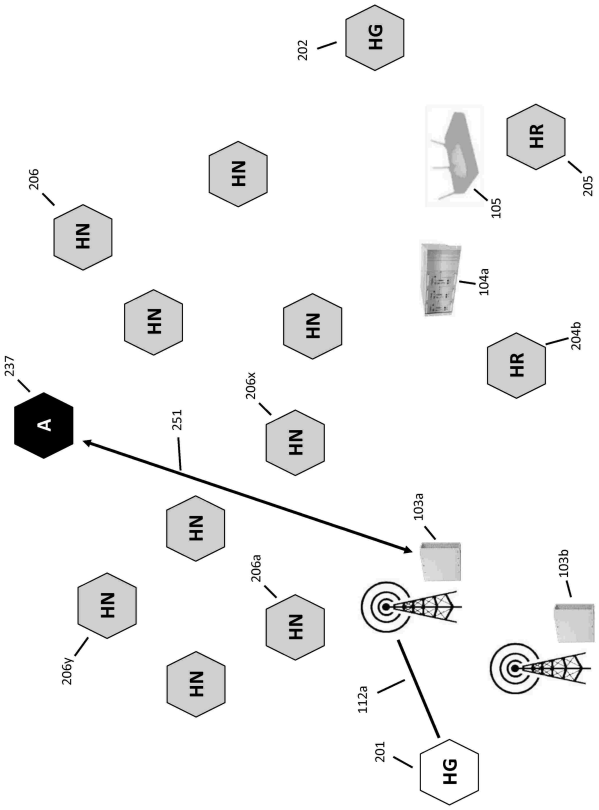
【図１２Ｅ】



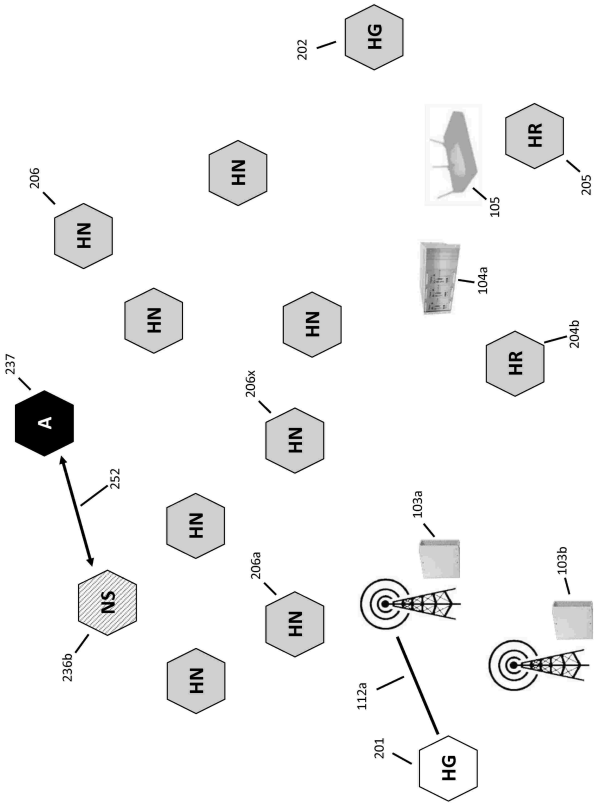
【図１３Ａ】



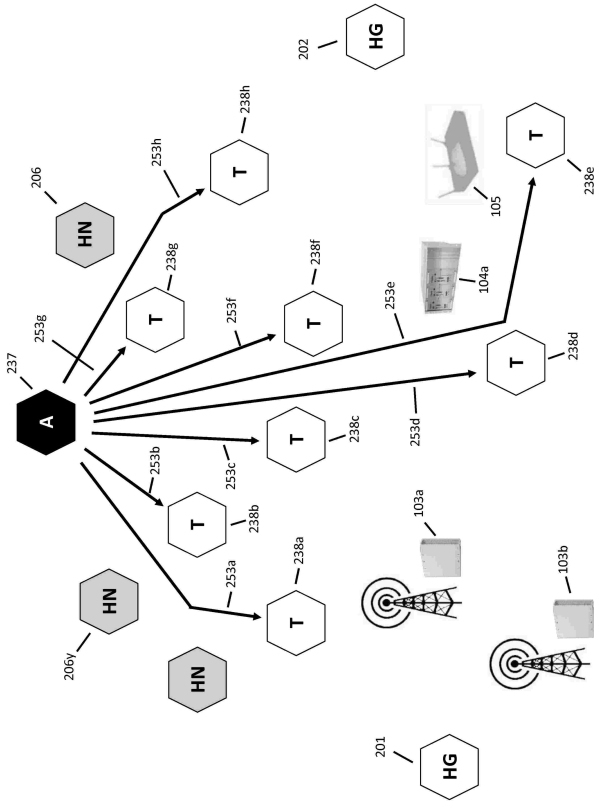
【図１３Ｂ】



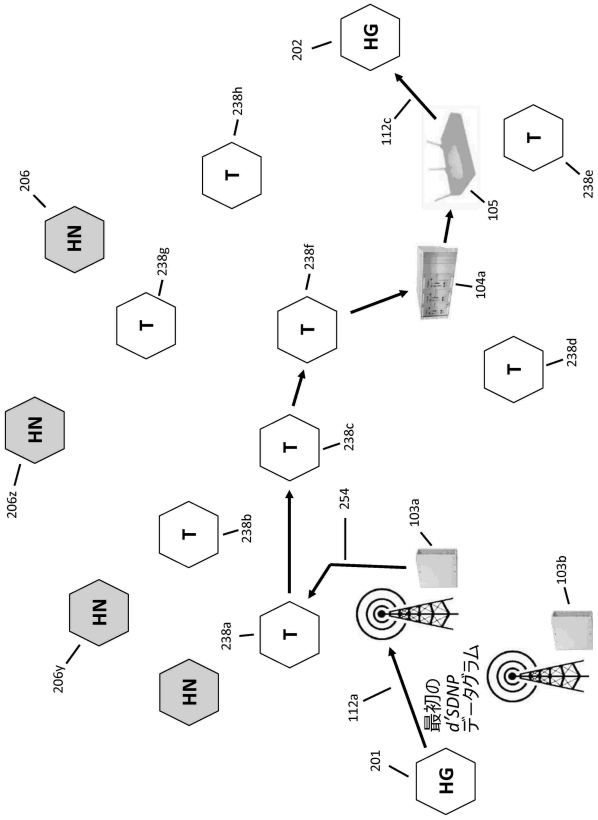
【図１３Ｃ】



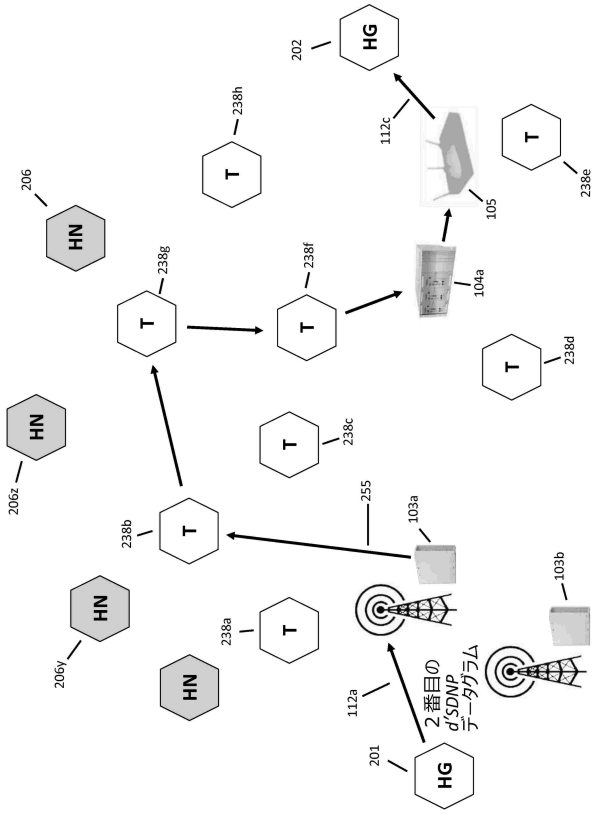
【図１３Ｄ】



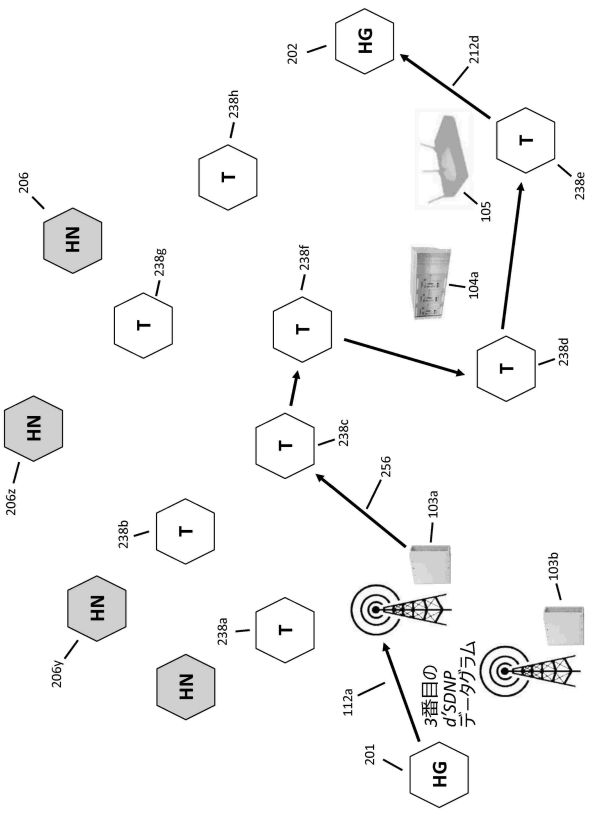
【図１３Ｅ】



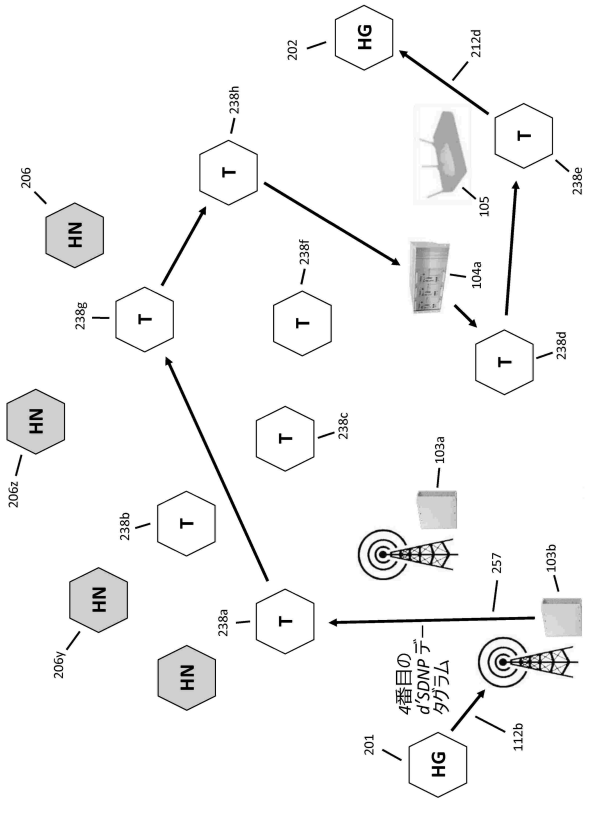
【図１３Ｆ】



【図１３Ｇ】



【図１３Ｈ】



【図１４】

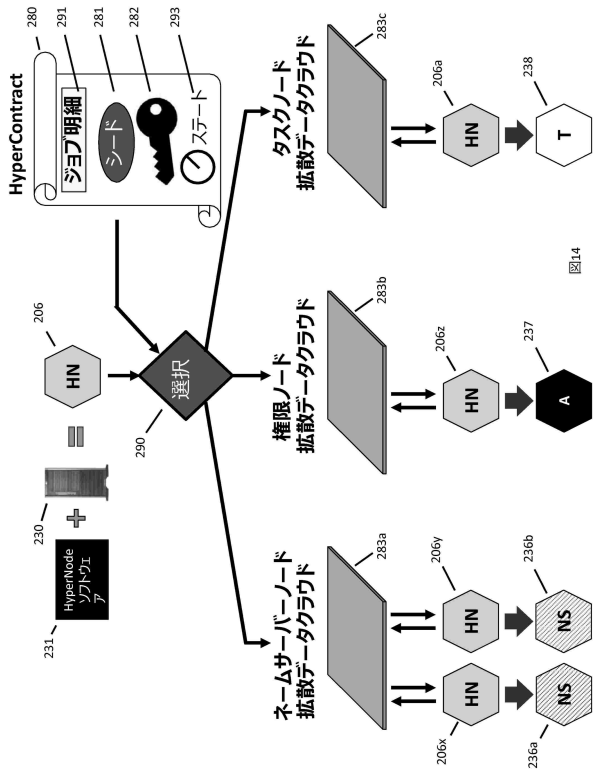
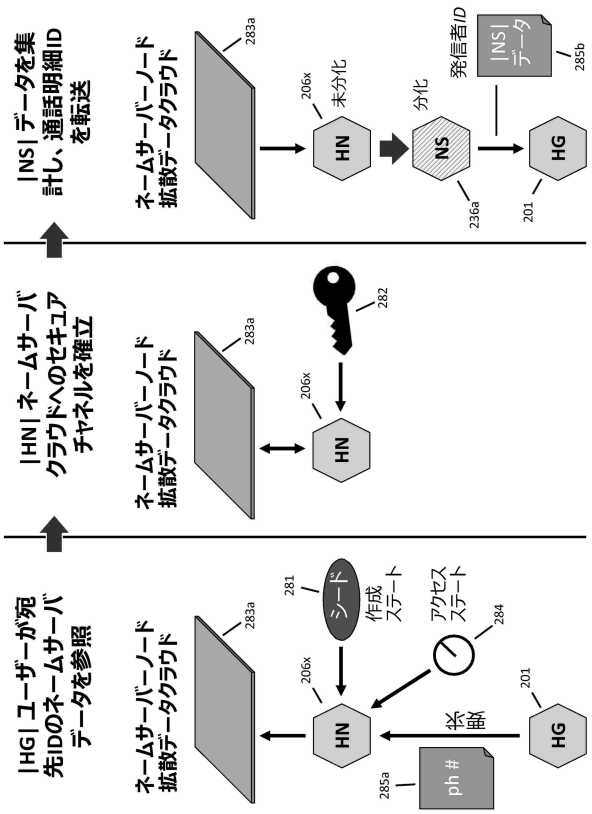
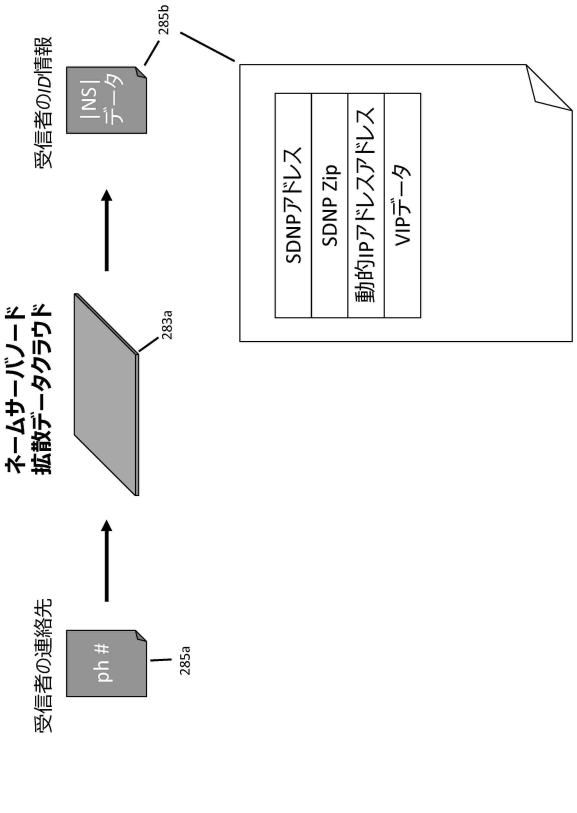


図14

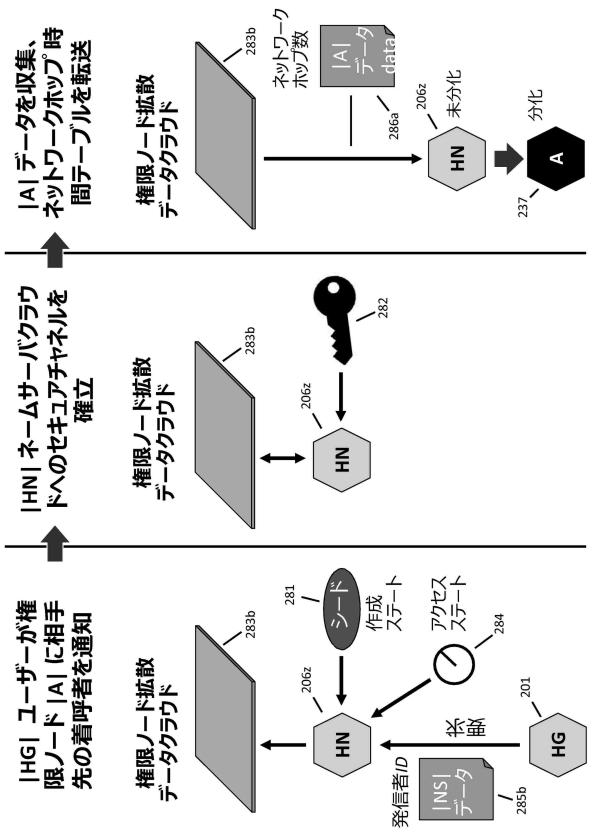
【図１５Ａ】



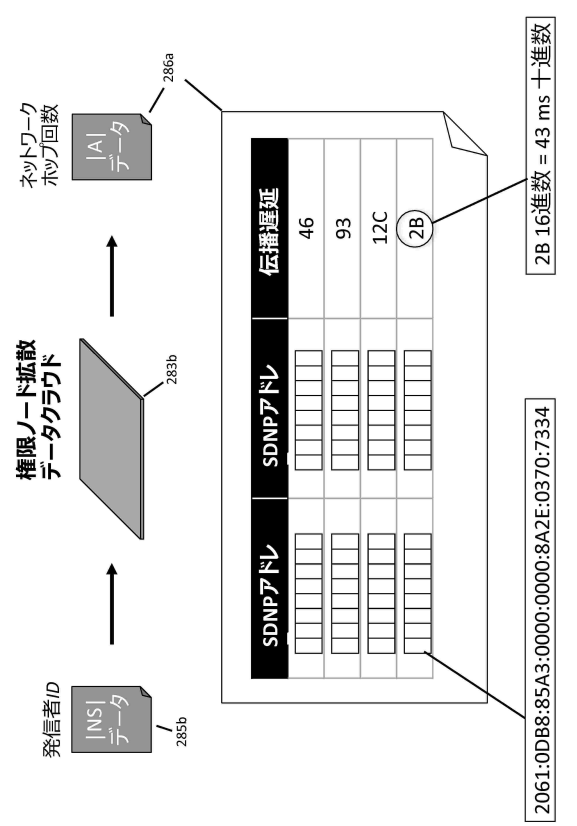
【図１５Ｂ】



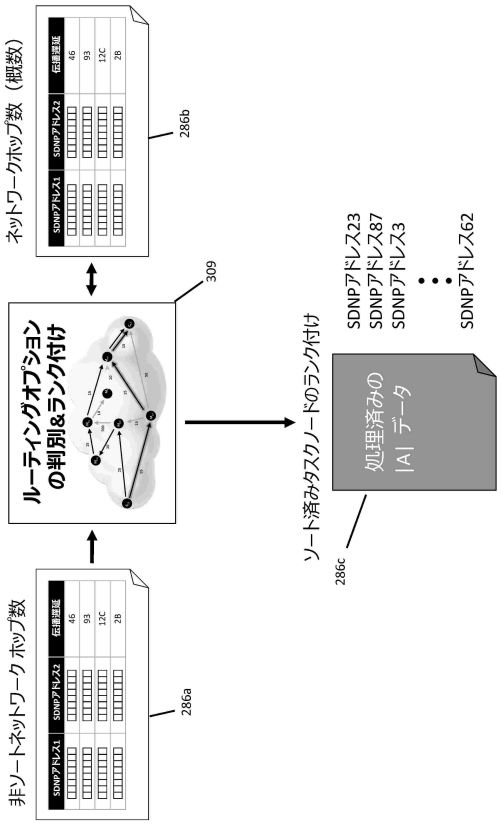
【図１６Ａ】



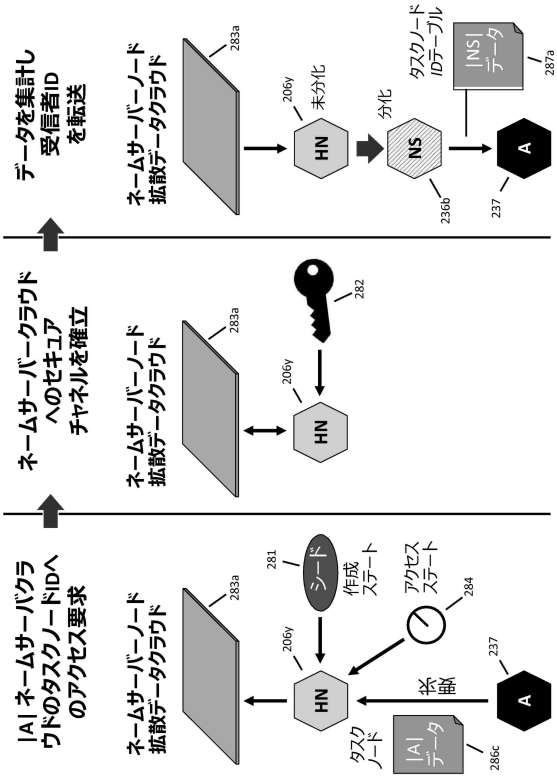
【図１６Ｂ】



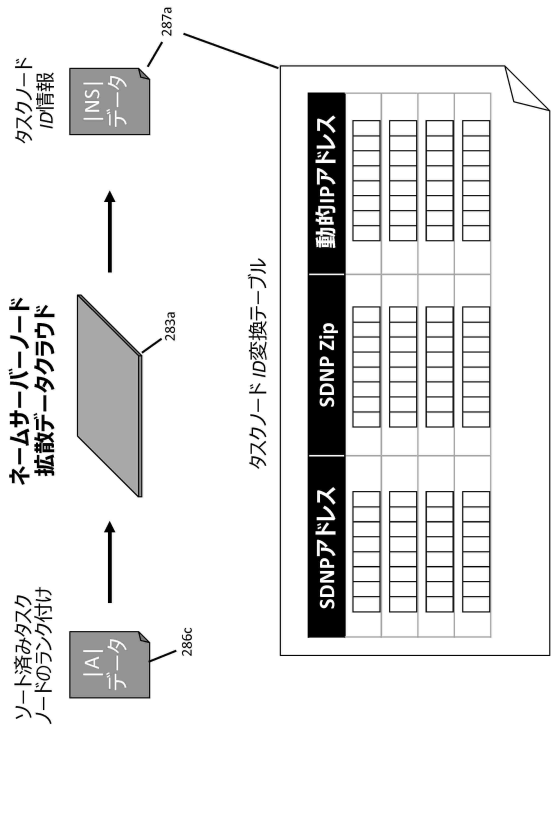
【図１６Ｃ】



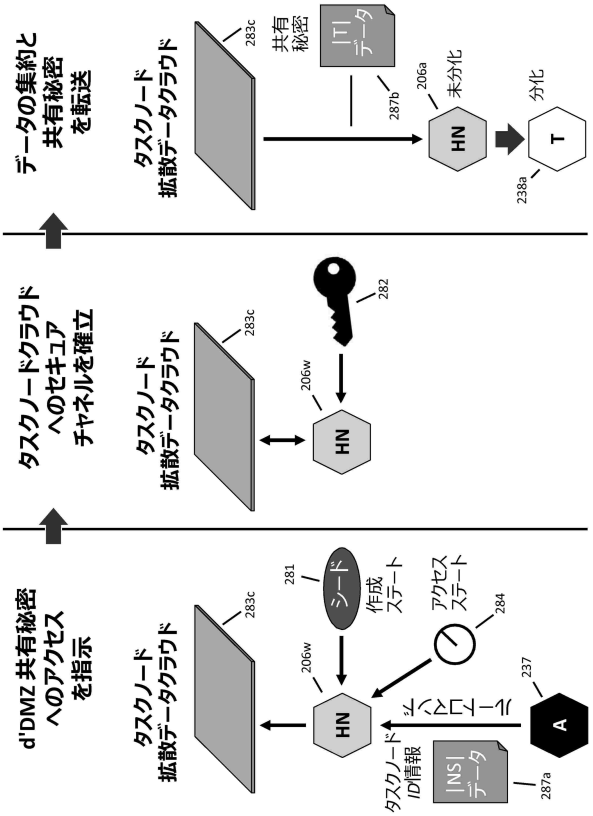
【図１７Ａ】



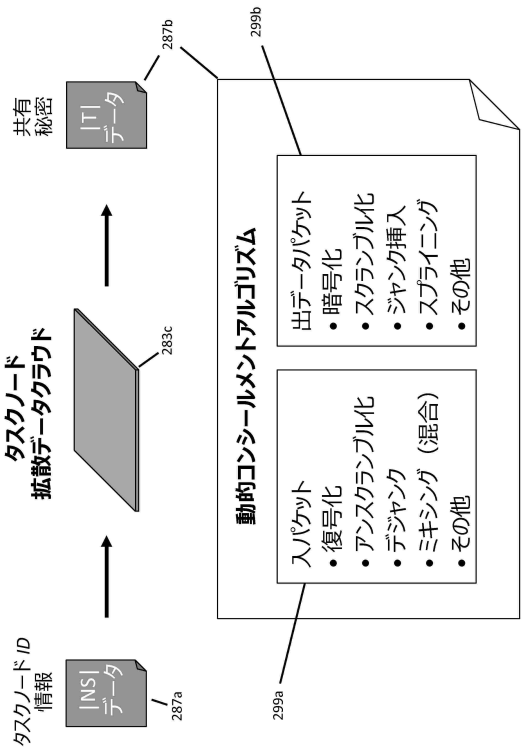
【図１７Ｂ】



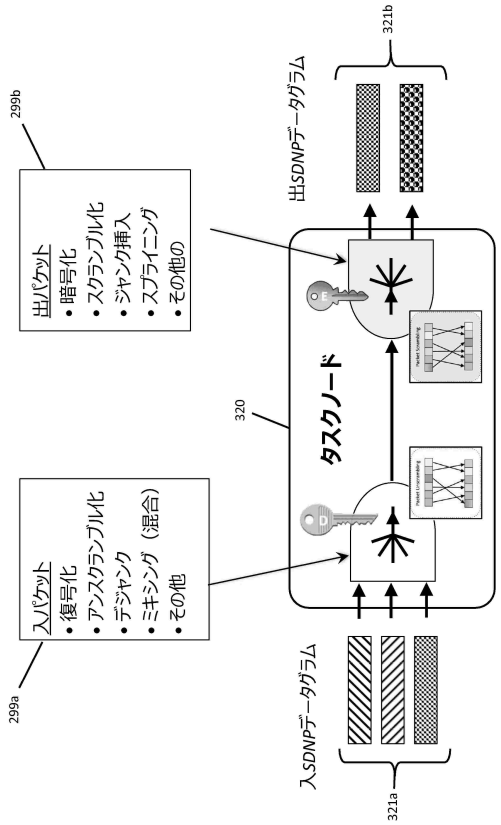
【図１８Ａ】



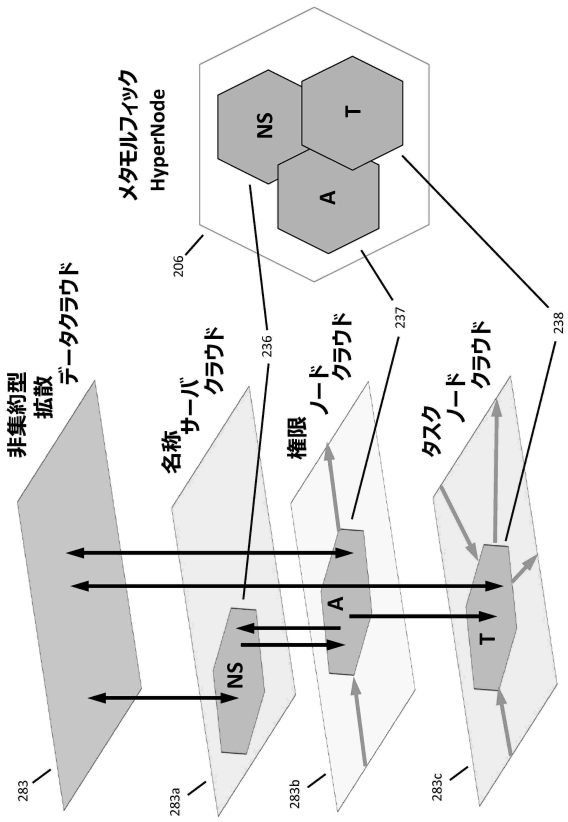
【図１８Ｂ】



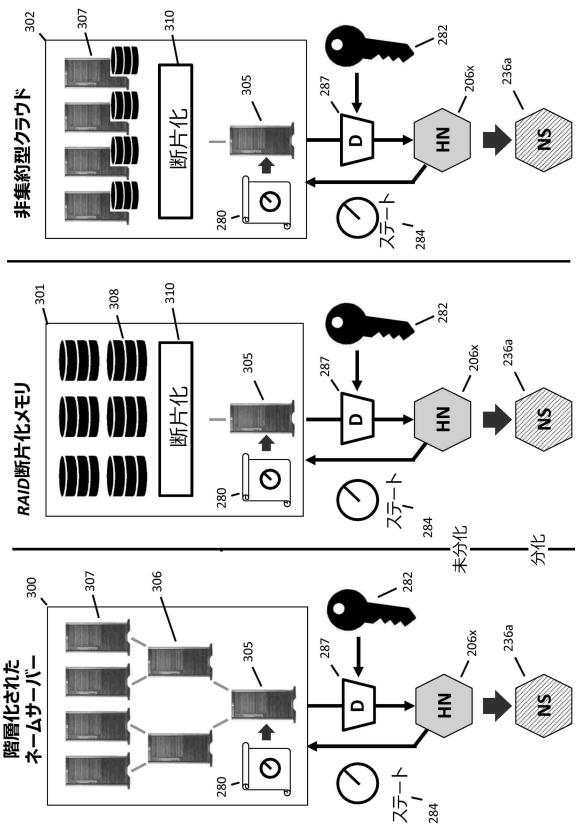
【図１８Ｃ】



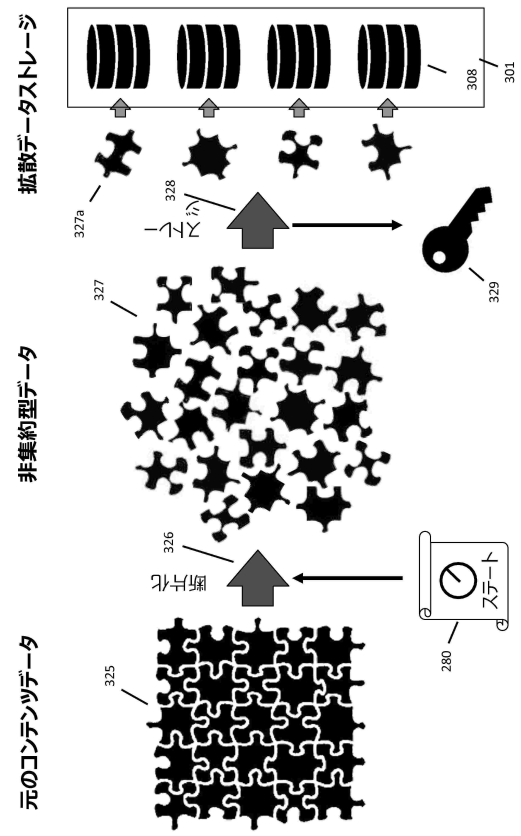
【図１９】



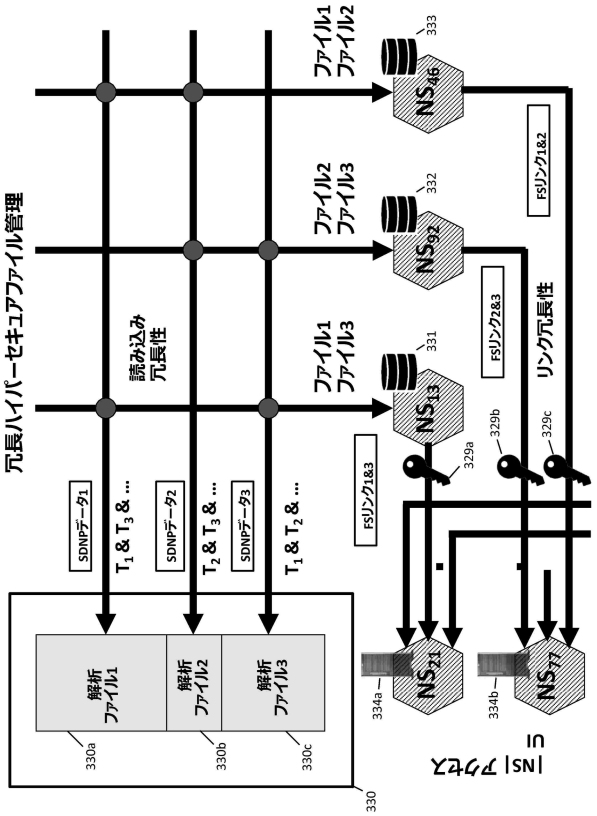
【図２０】



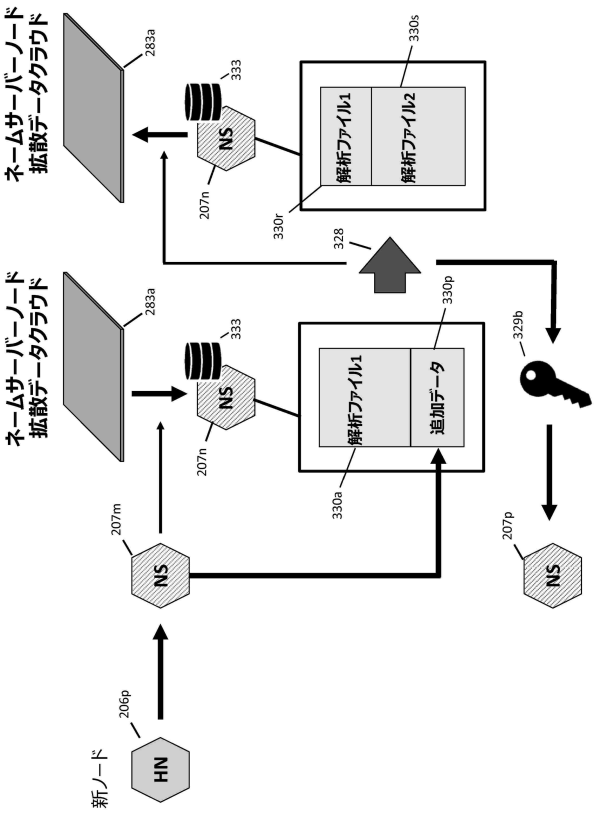
【図２１】



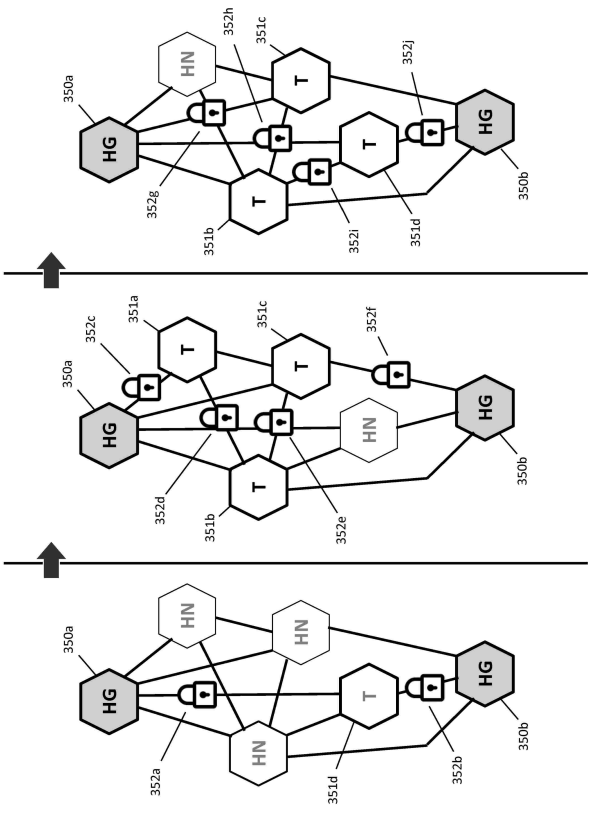
【図２２】



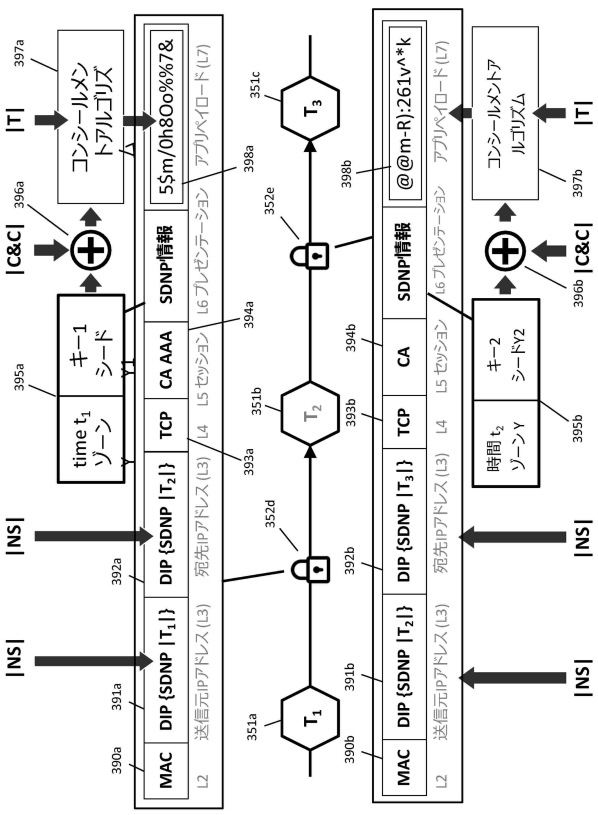
【図２３】



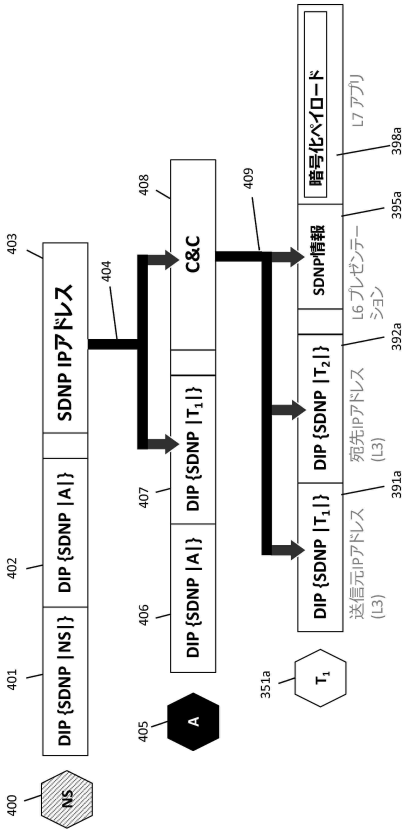
【図２４】



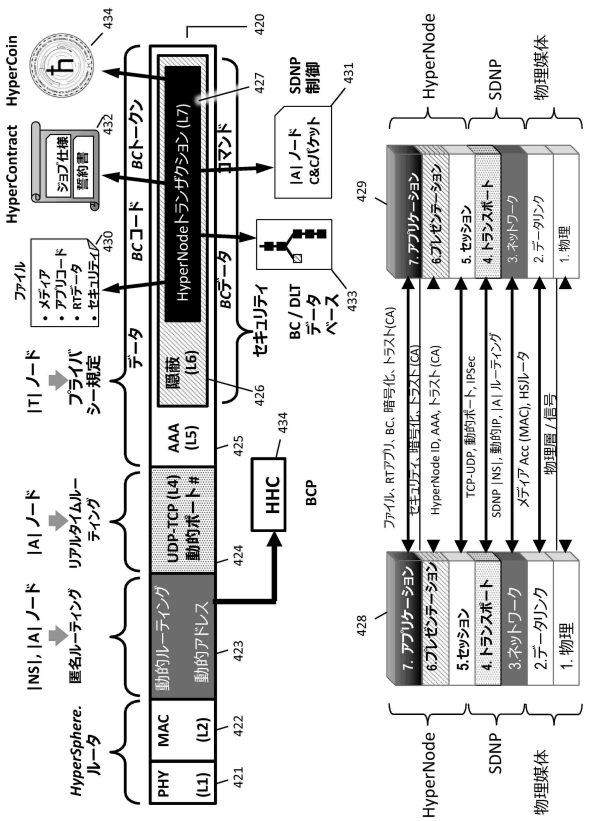
【図２５】



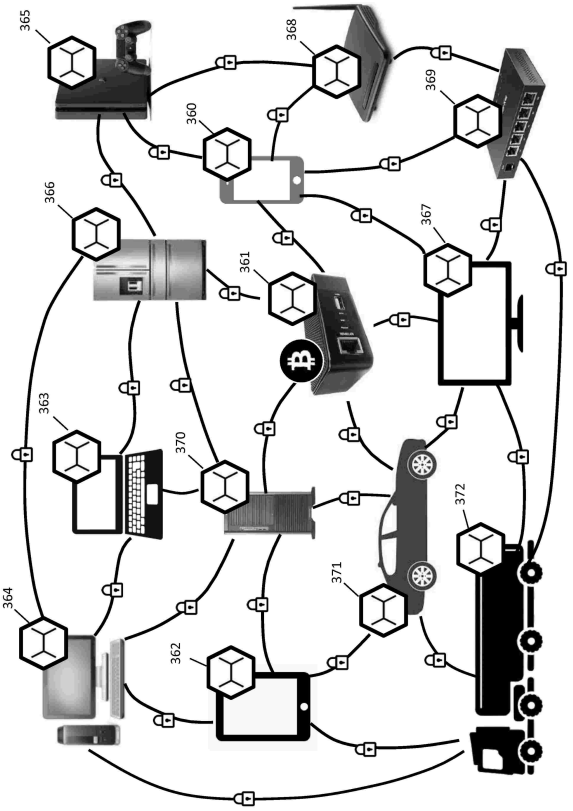
【図２６】



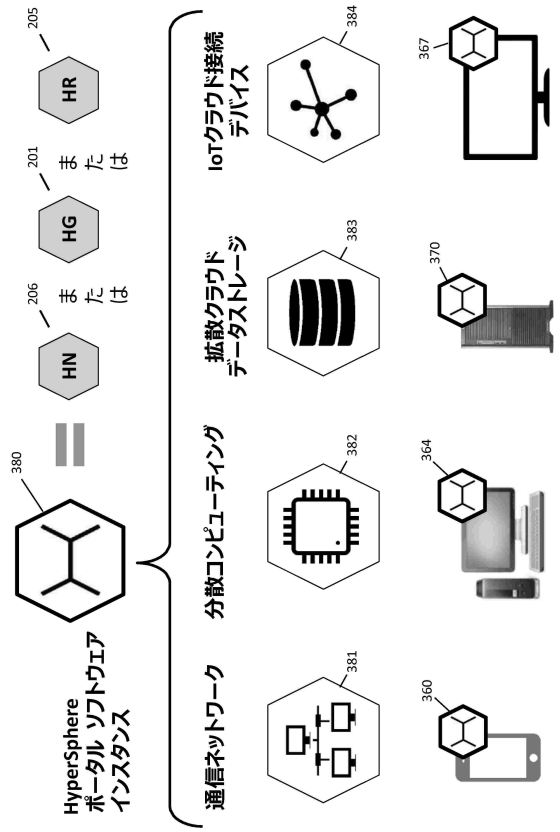
【図２７】



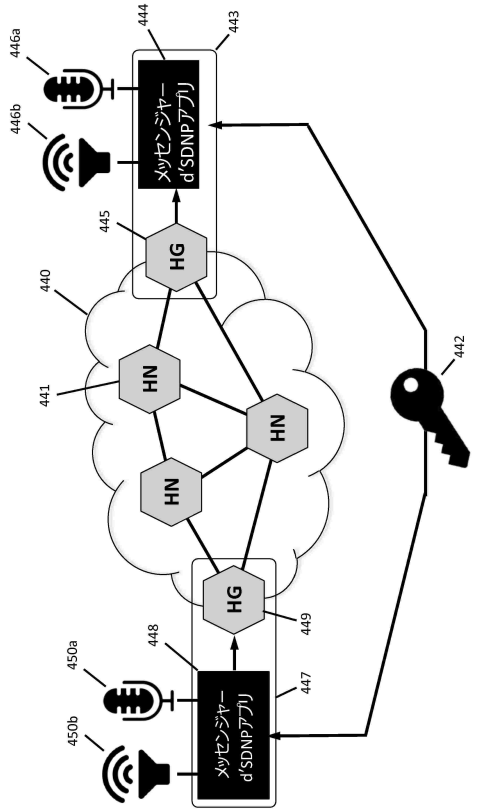
【図２８】



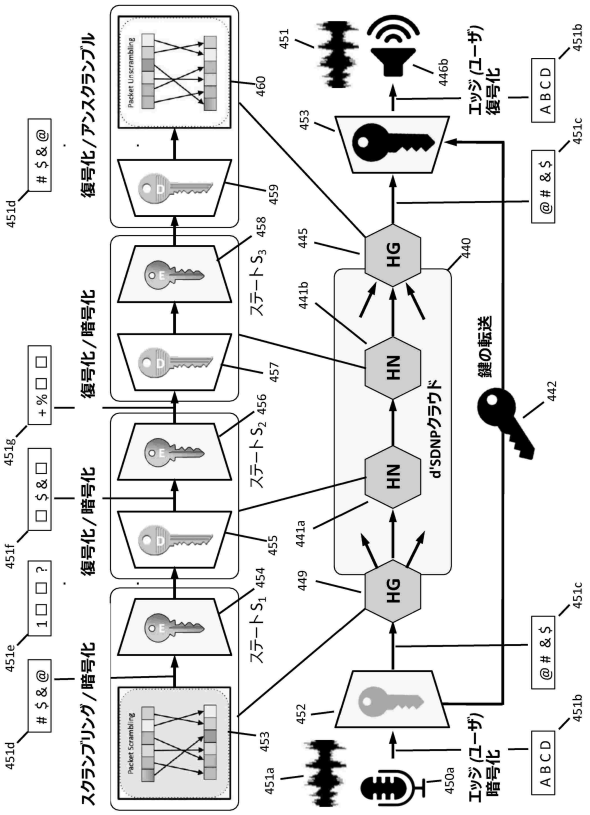
【図２９】



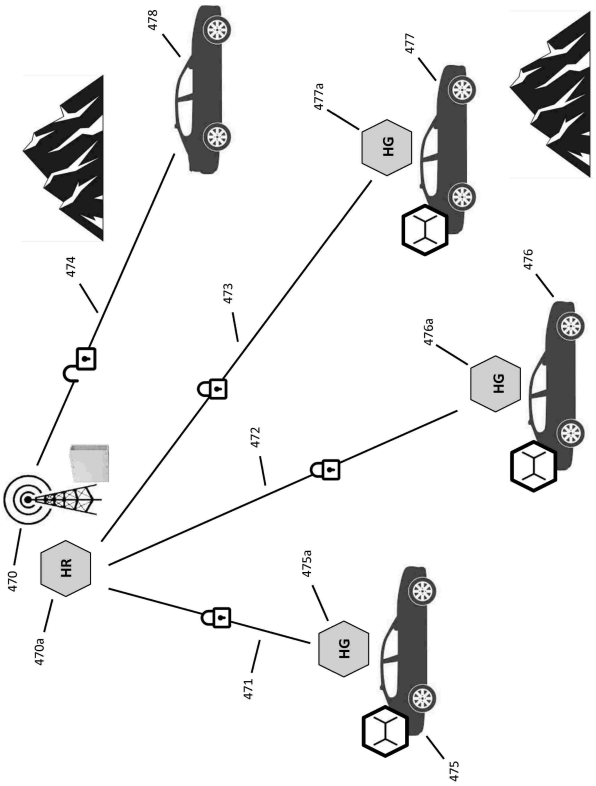
【図３０】



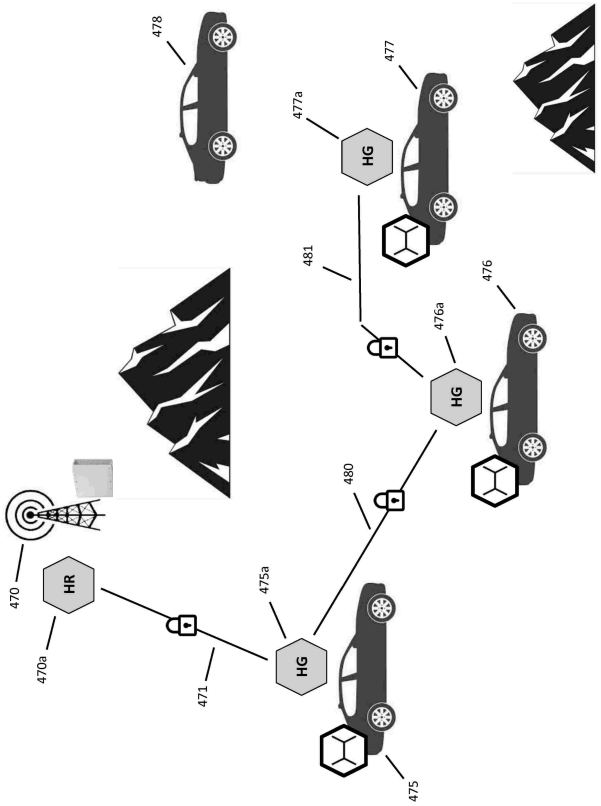
【図３１】



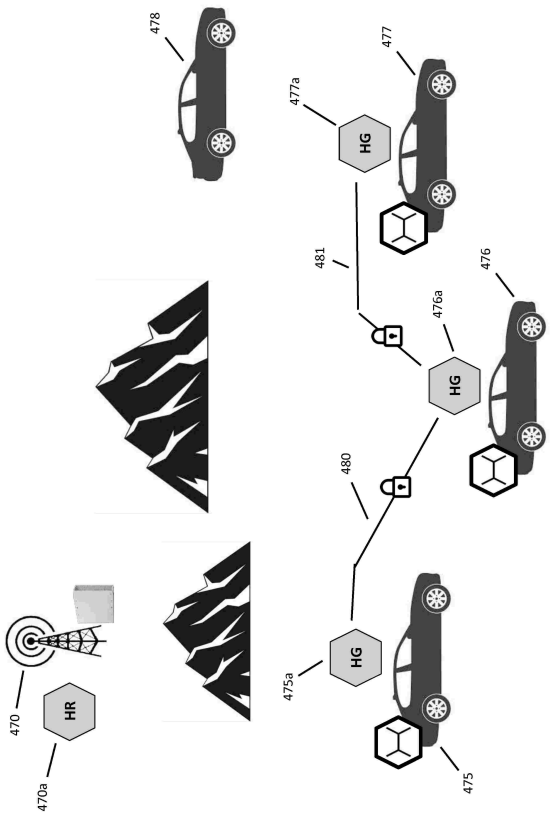
【図３２Ａ】



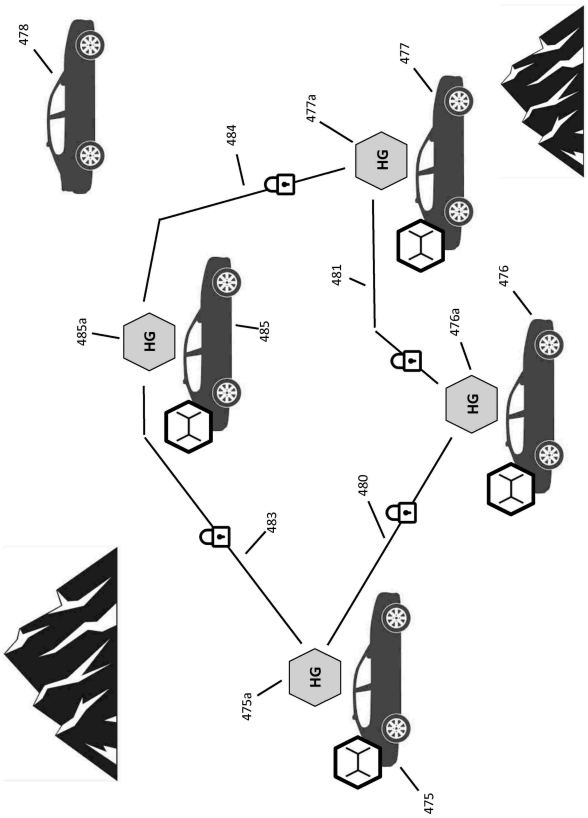
【図３２Ｂ】



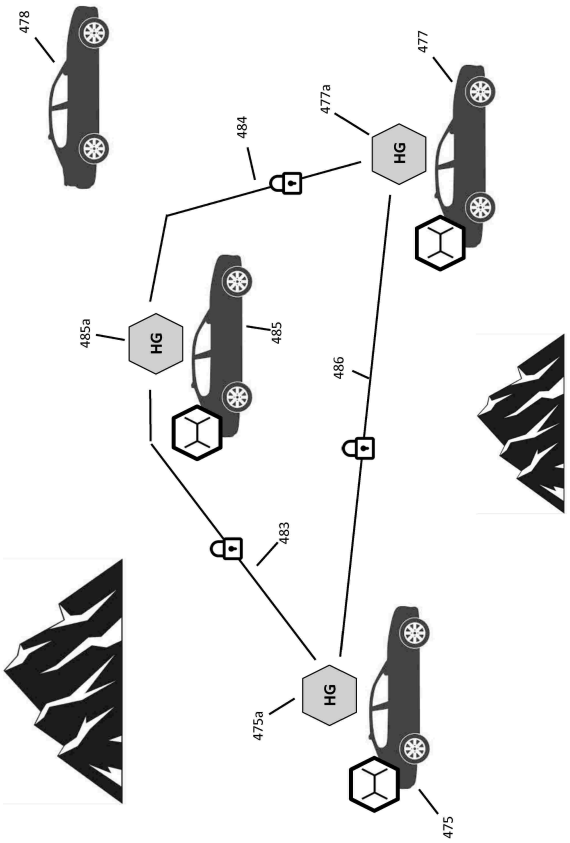
【図３２Ｃ】



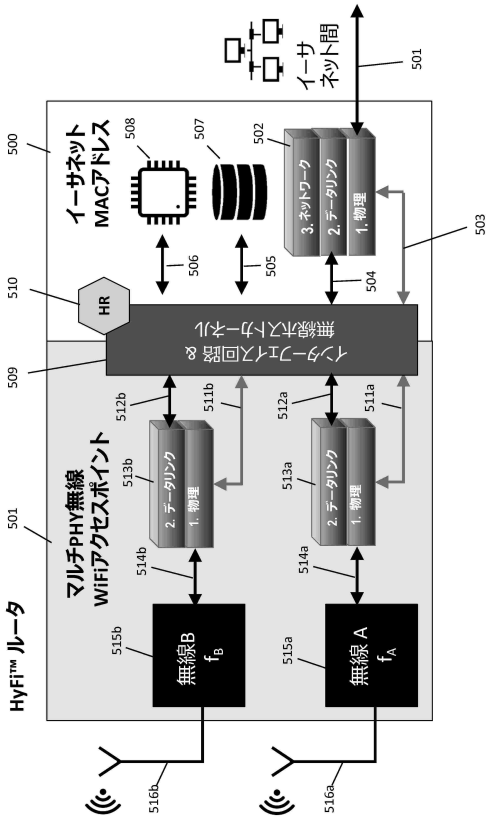
【図３２Ｄ】



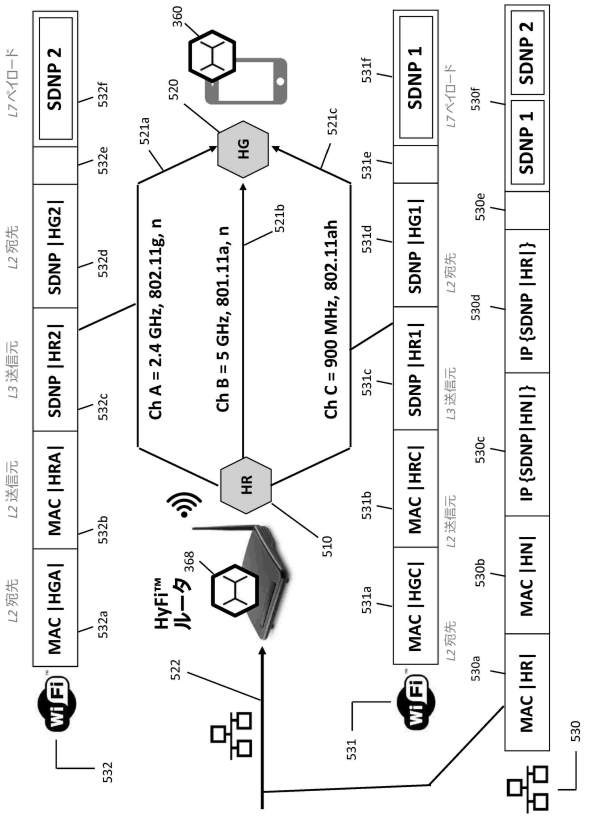
【図３２Ｅ】



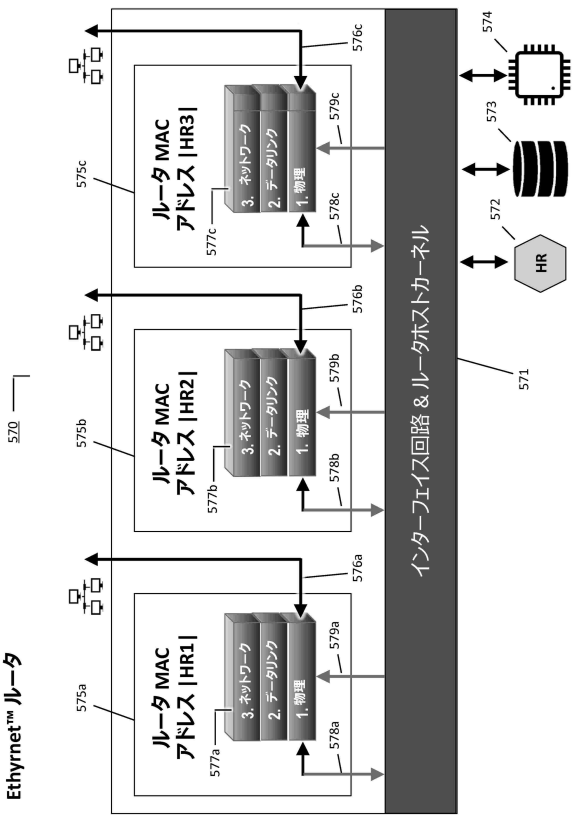
【図３３Ａ】



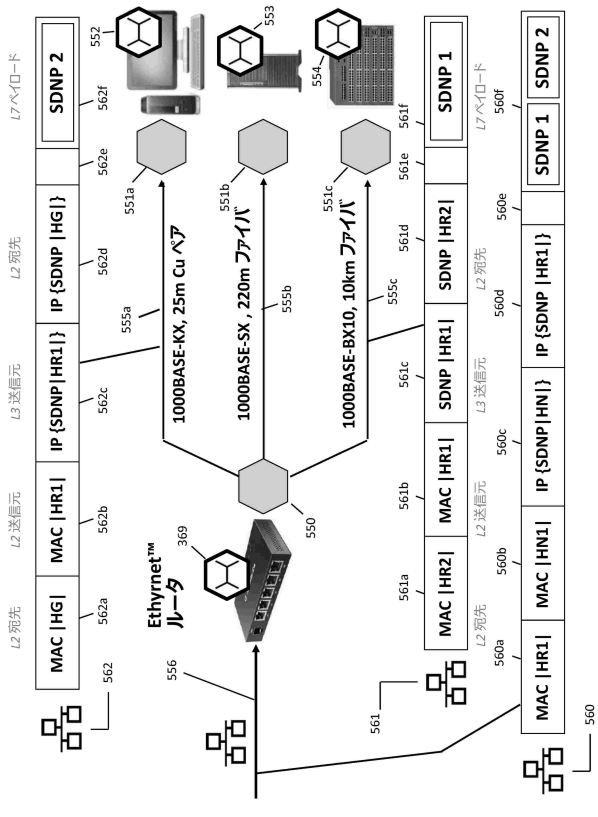
【図３３Ｂ】



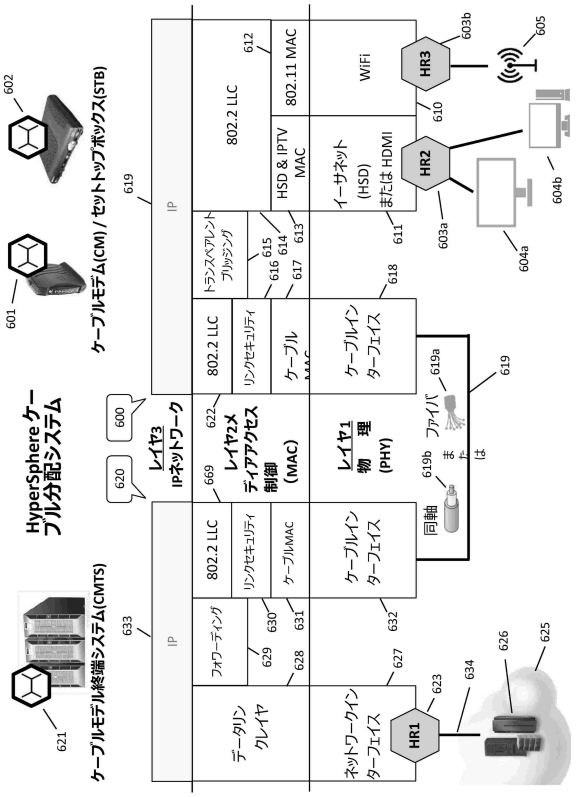
【図３４Ａ】



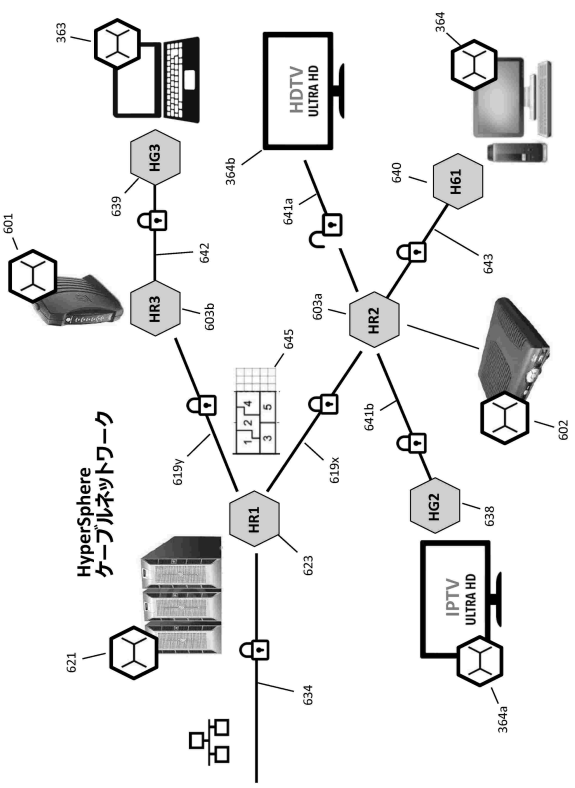
【図３４Ｂ】



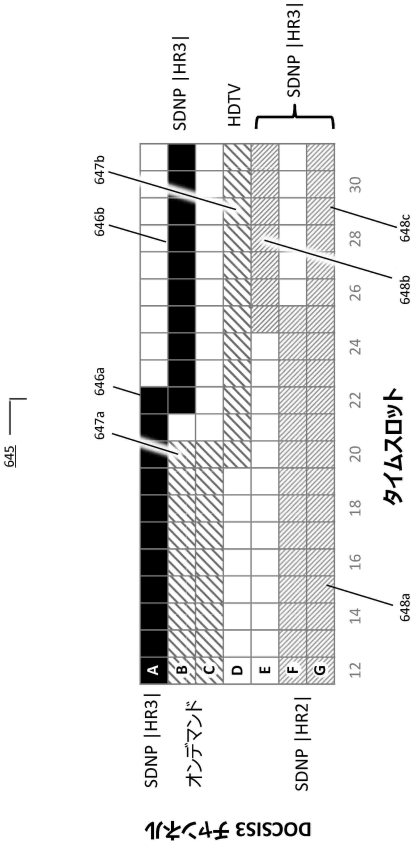
【図３５Ａ】



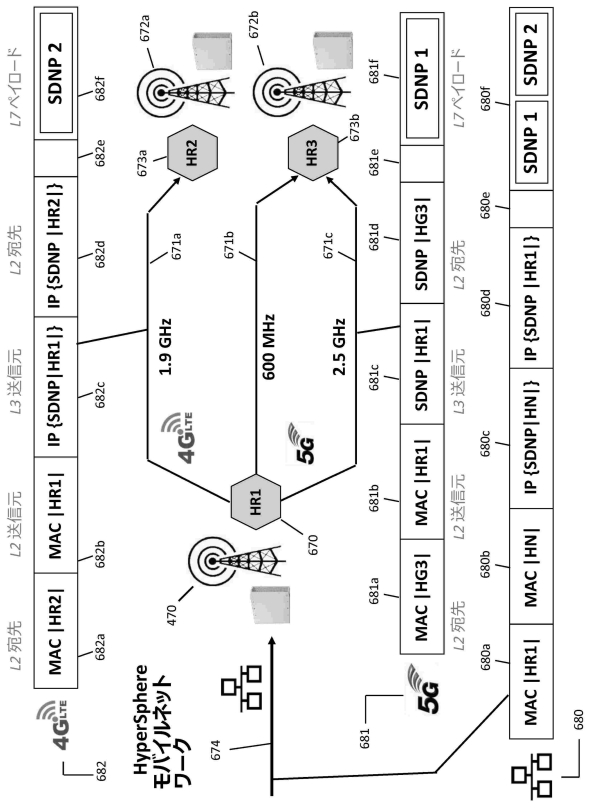
【図３５Ｂ】



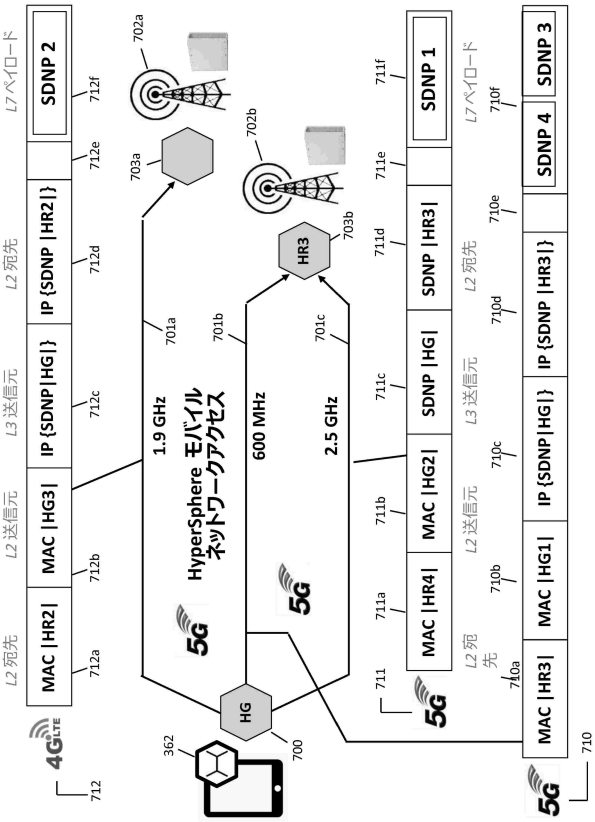
【図３５Ｃ】



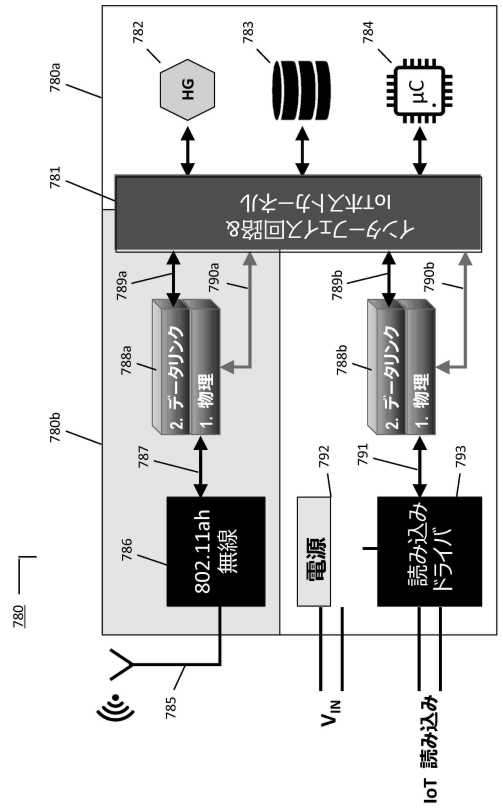
【図３６Ａ】



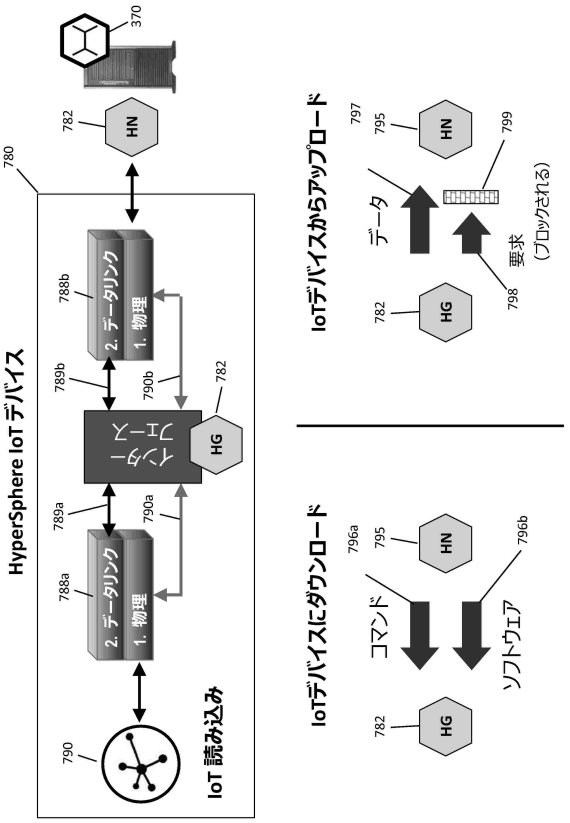
【図３６Ｂ】



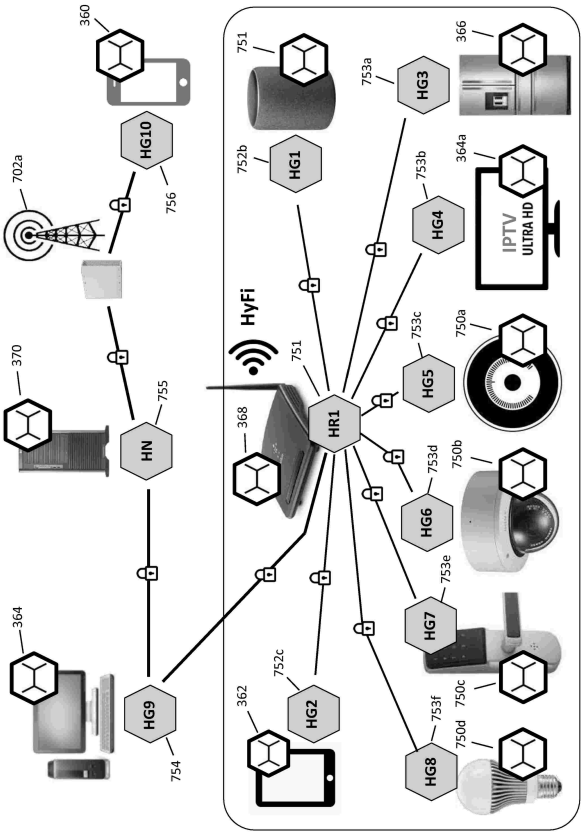
【図３７Ａ】



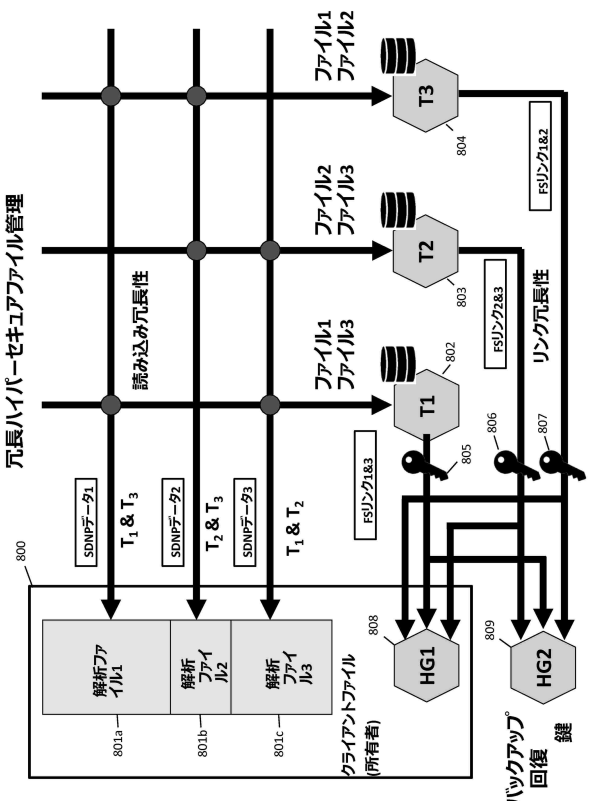
【図３７Ｂ】



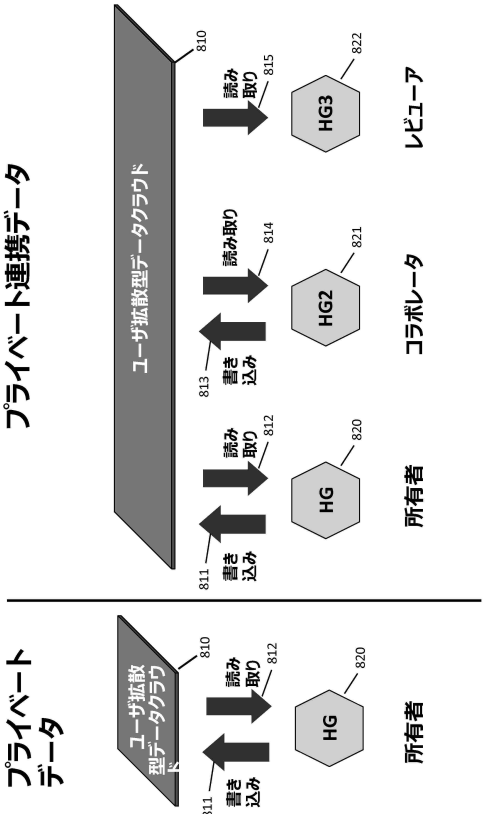
【図３７Ｃ】



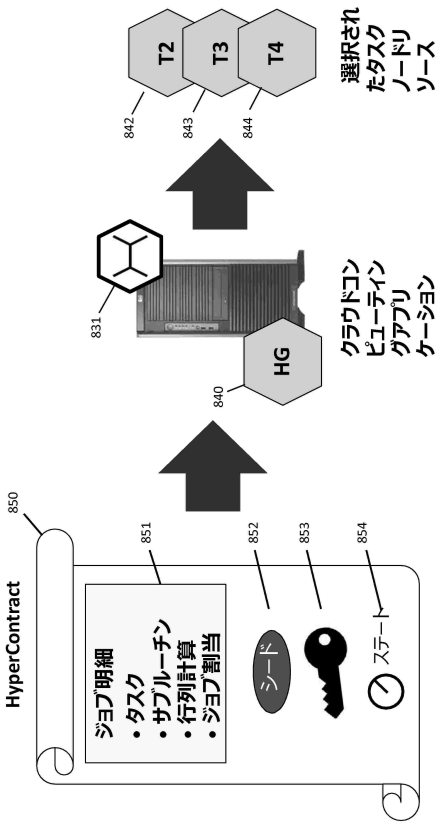
【図３８Ａ】



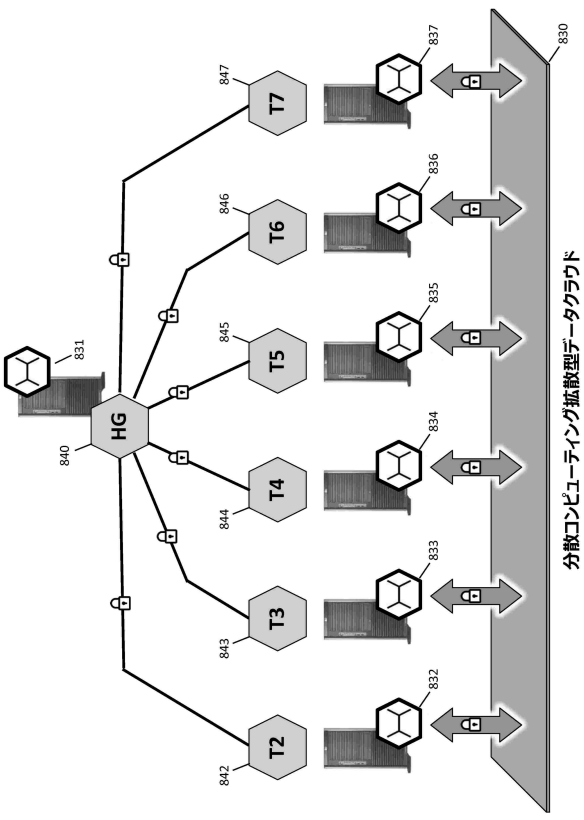
【図３８Ｂ】



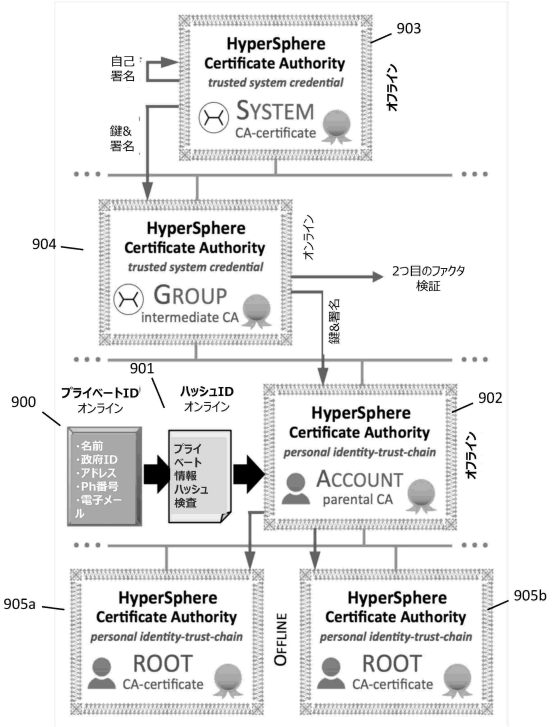
【図３９Ａ】



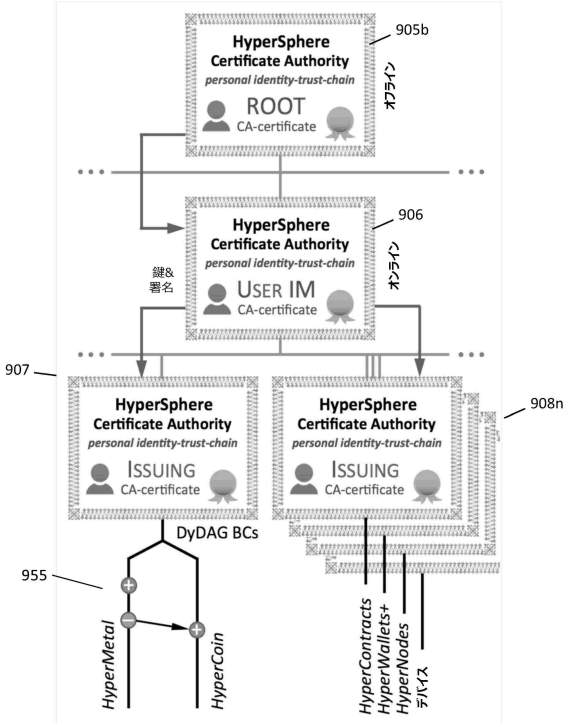
【図３９Ｂ】



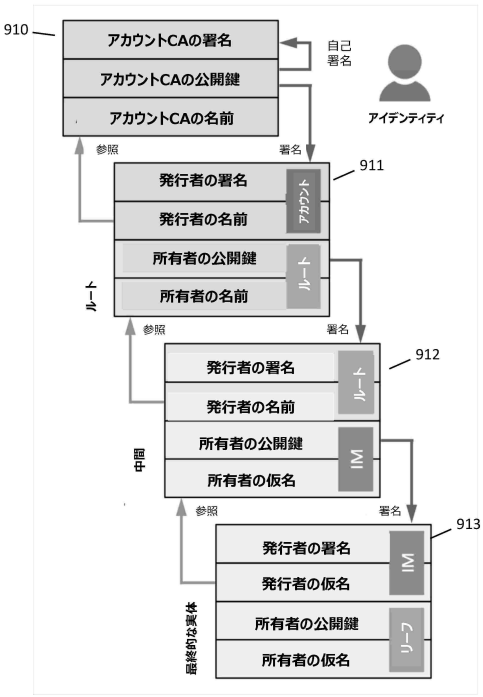
【図４０】



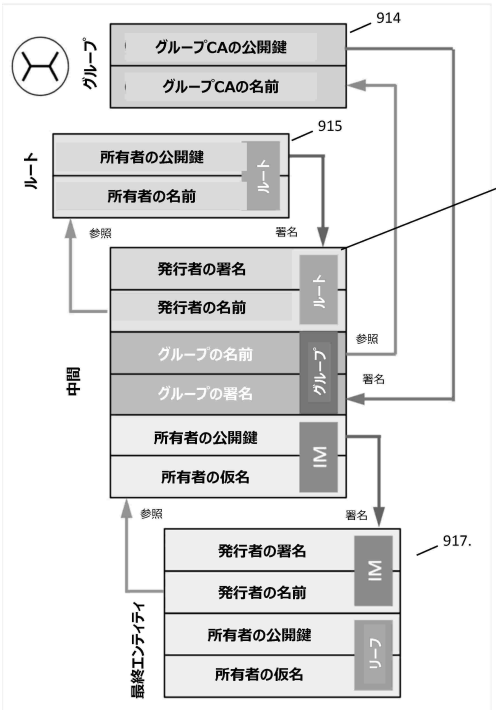
【図４１】



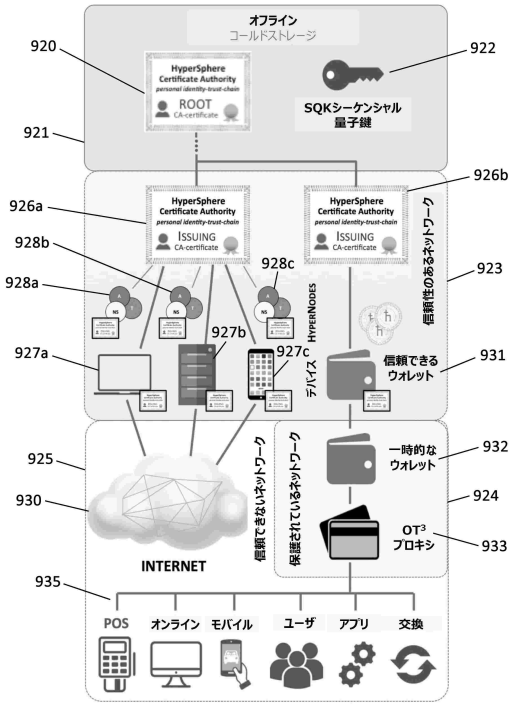
【図４２】



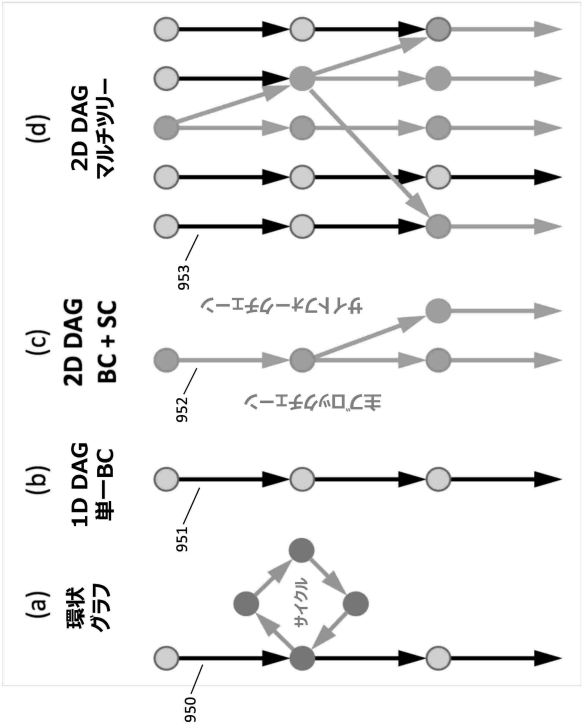
【図４３】



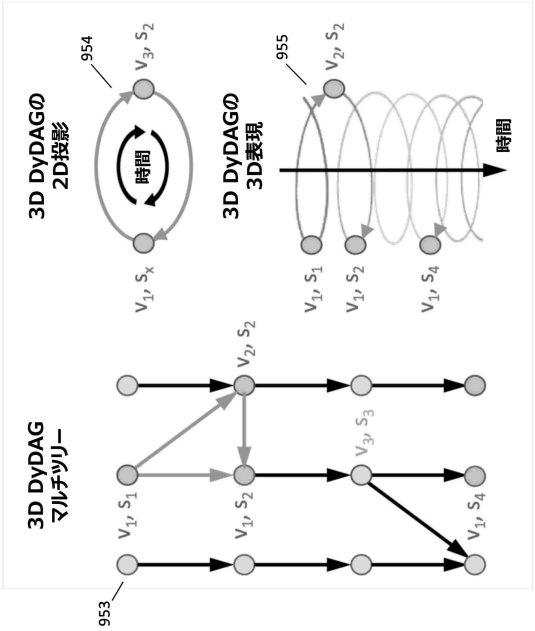
【図４４】



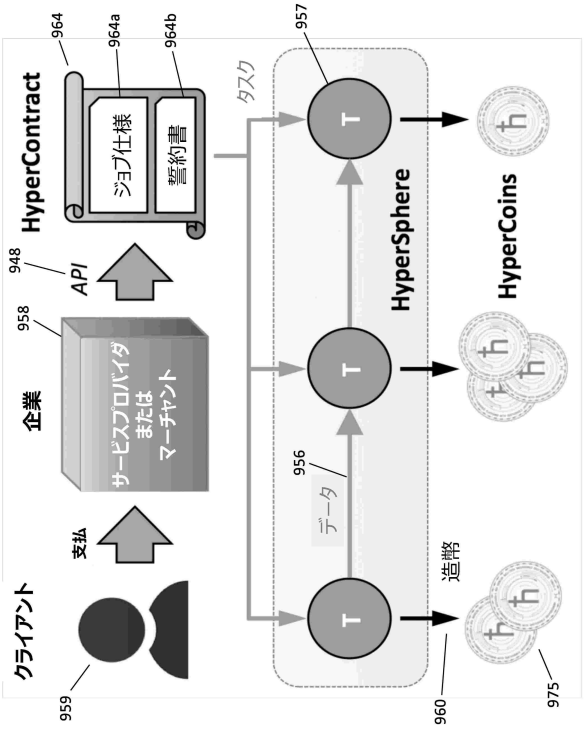
【図４５】



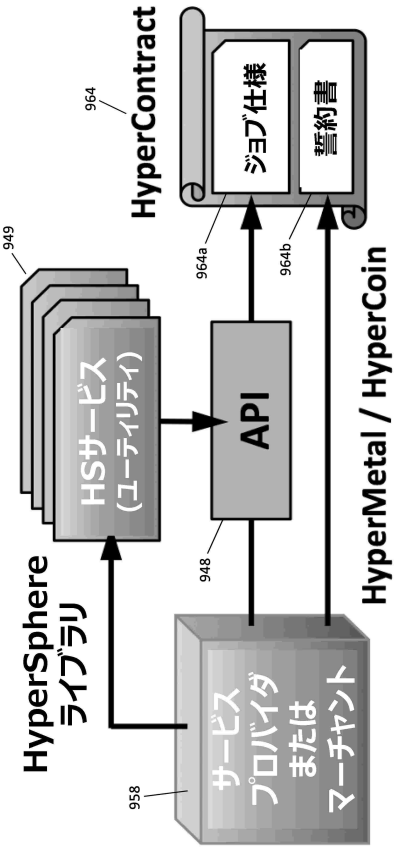
【図４６】



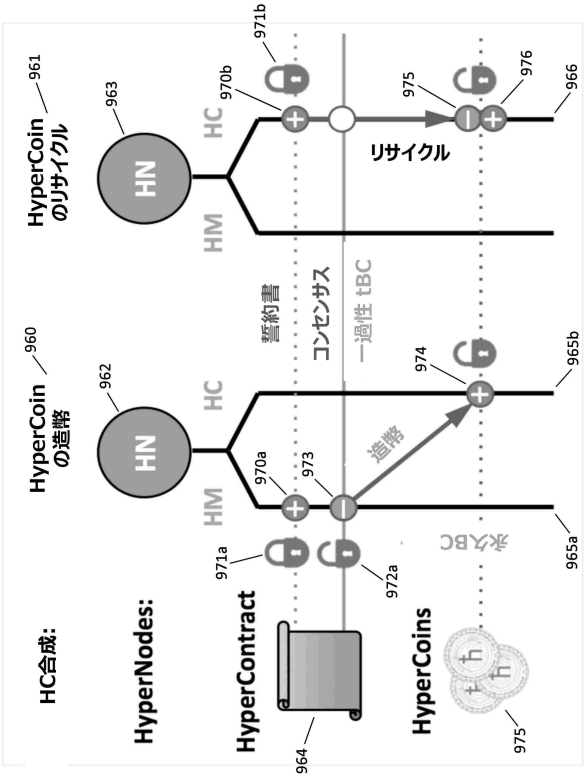
【図４７】



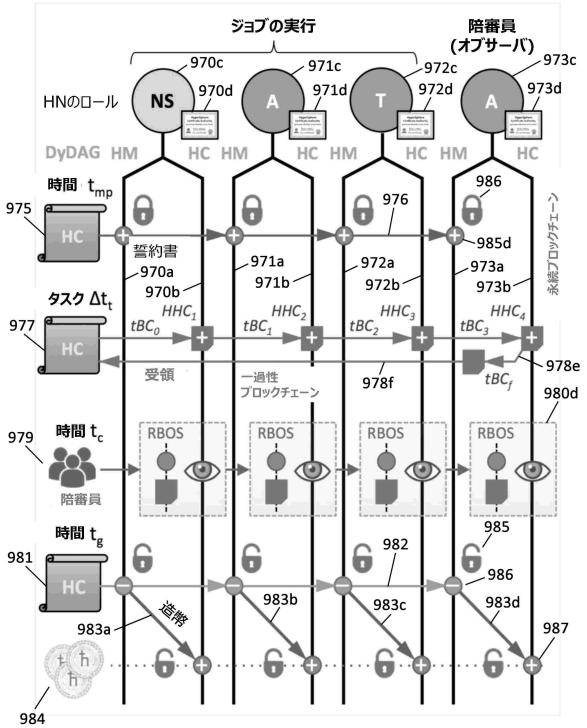
【図４８】



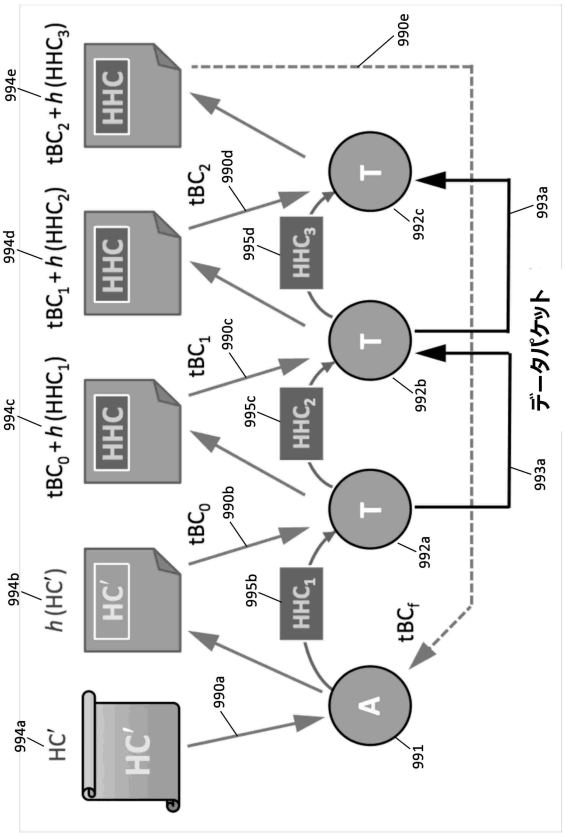
【図４９】



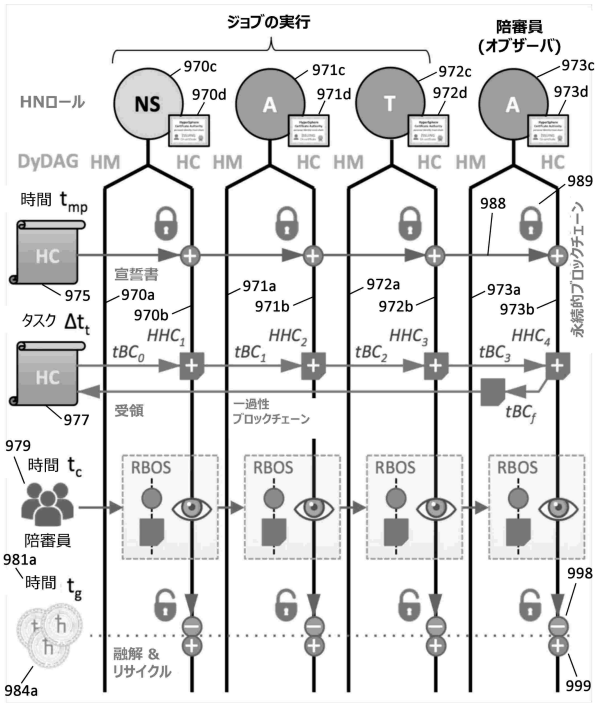
【図５０】



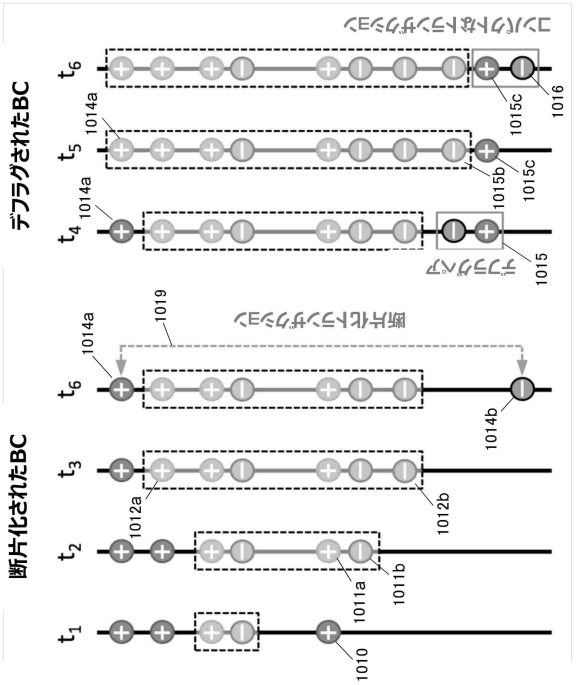
【図５１】



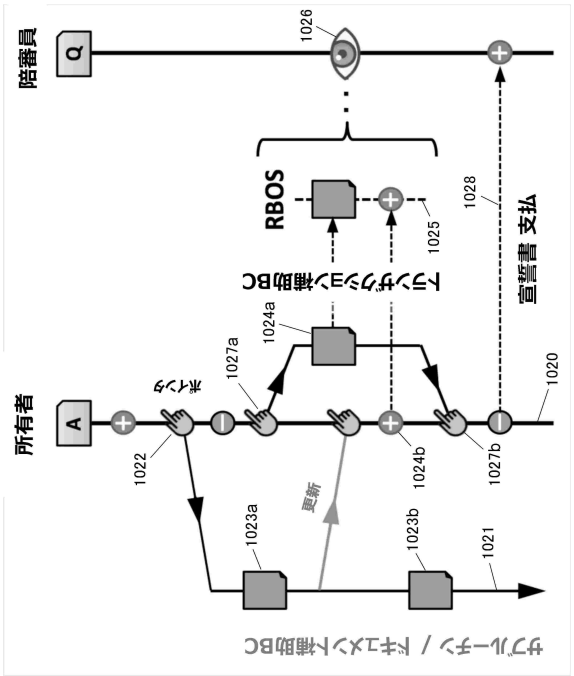
【図５２】



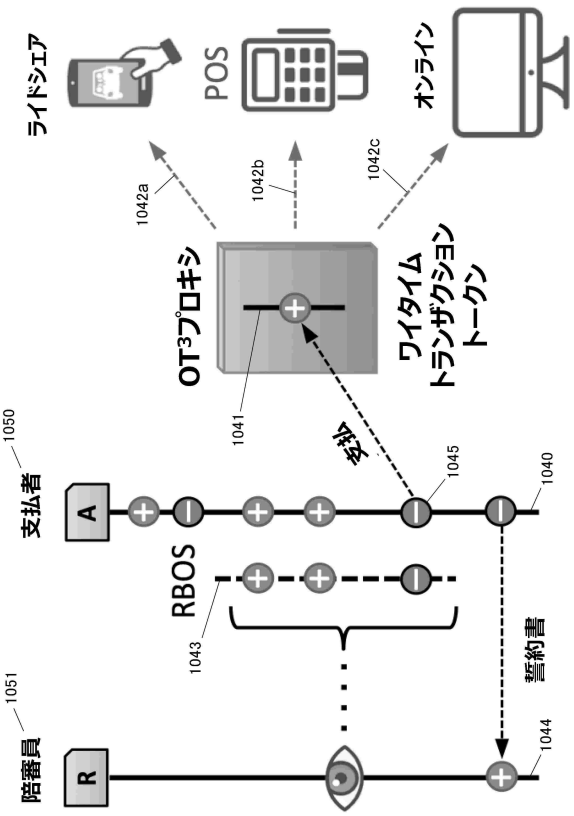
【図５３】



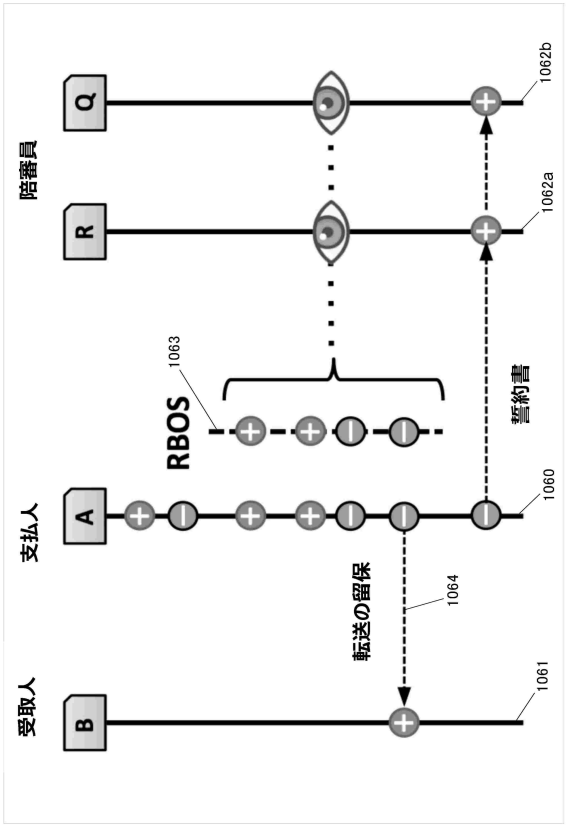
【図５４】



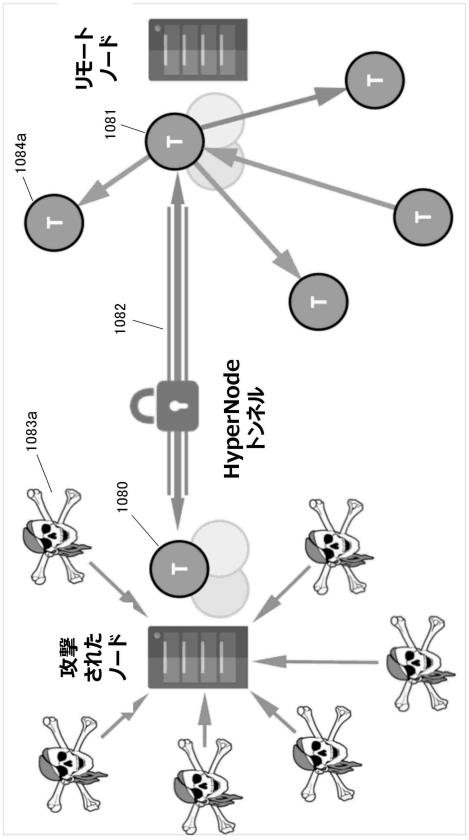
【図５５】



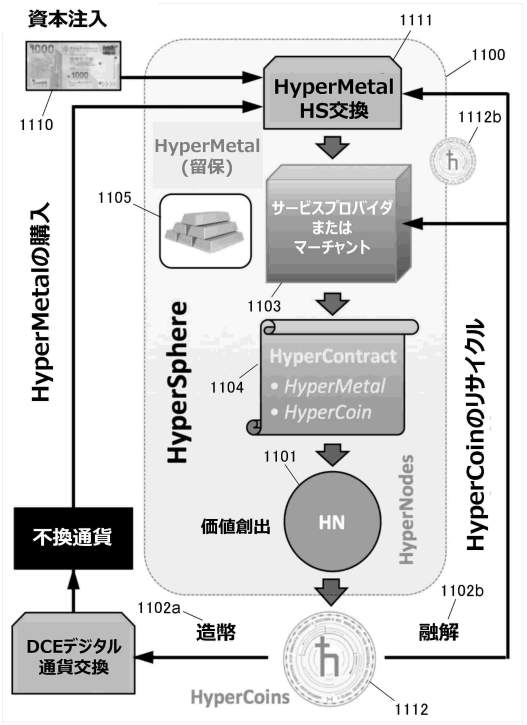
【図５６】



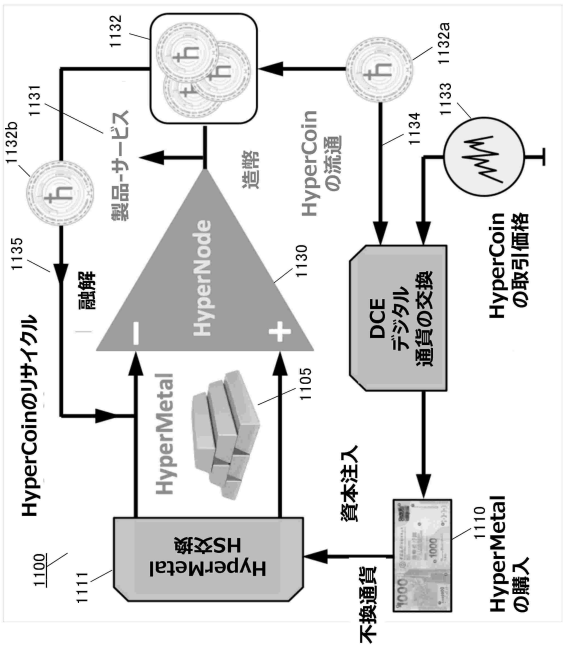
【図５７】



【図５８】



【図５９】



フロントページの続き

(56)参考文献 特表２０１８－５１２０９９（ＪＰ，Ａ）
特開２０１８－０１９４００（ＪＰ，Ａ）
特開２０１６－１５２４２９（ＪＰ，Ａ）
特開２０１６－１２７３２１（ＪＰ，Ａ）
特表２００２－５２９７７９（ＪＰ，Ａ）
特表２００２－５２３８０９（ＪＰ，Ａ）
特開平０４－３６０４３８（ＪＰ，Ａ）
国際公開第２０１８／０１１６０７（ＷＯ，Ａ１）

(58)調査した分野 (Int.Cl.，ＤＢ名)
Ｈ０４Ｌ ９／１４
Ｈ０４Ｌ ９／３４
Ｈ０４Ｌ ４５／００