(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6727316号
(P6727316)

(45)発行日　令和2年7月22日(2020.7.22)　(24)登録日　令和2年7月2日(2020.7.2)

(51)Int.Cl.		F I		
H04W 12/08	(2009.01)	H04W	12/08	
H04W 8/18	(2009.01)	H04W	8/18	
H04L 9/14	(2006.01)	H04L	9/00	641
G06F 21/60	(2013.01)	G06F	21/60	320
H04W 88/16	(2009.01)	H04W	88/16	

請求項の数 23　(全 33 頁)

(21)出願番号　特願2018-539882(P2018-539882)
(86)(22)出願日　平成29年2月11日(2017.2.11)
(65)公表番号　特表2019-511149(P2019-511149A)
(43)公表日　平成31年4月18日(2019.4.18)
(86)国際出願番号　PCT/IB2017/050772
(87)国際公開番号　WO2017/137959
(87)国際公開日　平成29年8月17日(2017.8.17)
審査請求日　令和2年2月12日(2020.2.12)
(31)優先権主張番号　62/294,482
(32)優先日　平成28年2月12日(2016.2.12)
(33)優先権主張国・地域又は機関
米国(US)
(31)優先権主張番号　15/098,899
(32)優先日　平成28年4月14日(2016.4.14)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　518202356
ジェイピーユー．アイオー　リミテッド
ＪＰＵ．ＩＯ　ＬＴＤ
イスラエル国　４９５１１４８　ペタク　チクヴァ　インバー　１４　ピーオー　ボックス　４０９８
(74)代理人　100207837
弁理士　小松原　寿美
(74)代理人　100214640
弁理士　立山　千晶
(72)発明者　シュワルツ、ジョナサン
イスラエル国　６９６２６６０　テル　アビブ　モシェ　コル　ストリート　８

最終頁に続く

(54)【発明の名称】モバイル・セキュリティ・オフローダ

(57)【特許請求の範囲】

【請求項１】

モバイルセキュリティオフローダ（ＭＳＯＬ）であって、

コンピュータ上で動作し、モバイル無線ネットワーク内のモバイルデバイスから非暗号化データを受信して、前記非暗号化データから前記モバイルデバイスの固有のモバイルデバイス識別情報を決定するように構成されたモバイルデバイス識別用受信機コンポーネントと、

前記コンピュータ上で動作し、前記固有のモバイルデバイス識別情報を使用して、セキュリティプロファイルディレクトリから前記固有のモバイルデバイス識別情報に対応するセキュリティプロファイルを取得するように構成されたセキュリティプロファイルディレクトリインタフェースであって、前記固有のモバイルデバイス識別情報に対応する前記モバイルデバイスからのデータを暗号化するためのセキュリティプロトコルを識別する前記セキュリティプロファイルを取得する前記セキュリティプロファイルディレクトリインタフェースと、

１つまたは複数のプロセッサによって実行可能であり、前記セキュリティプロファイルで識別された前記セキュリティプロトコルを使用して前記非暗号化データを暗号化するように構成された暗号化エンジンと、

前記コンピュータ上で動作し、前記暗号化されたデータを、データ内で識別されたセキュアサーバにパケット交換ネットワークを介してルーティングするように構成されたパケット交換ネットワークインタフェースと、を備えるＭＳＯＬ。

【請求項２】
請求項１に記載のＭＳＯＬにおいて、
前記パケット交換ネットワークインタフェースはさらに、前記セキュアサーバから暗号化されたレスポンスデータを受信するように構成されており、前記暗号化エンジンはさらに、前記セキュリティプロファイルに基づいて前記暗号化されたレスポンスデータを復号化するように構成されている、ＭＳＯＬ。
【請求項３】
請求項２に記載のＭＳＯＬにおいて、
前記セキュリティプロファイルディレクトリインタフェースはさらに、前記ＭＳＯＬのキャッシュに前記セキュリティプロファイルを記憶するように構成されている、ＭＳＯＬ。
【請求項４】
請求項１に記載のＭＳＯＬにおいて、
前記モバイル無線ネットワークは２Ｇ／３Ｇネットワークであり、前記非暗号化データは、サービング汎用パケット無線サービス（ＧＰＲＳ）サポートノード（ＳＧＳＮ）を介して受信される、ＭＳＯＬ。
【請求項５】
請求項１に記載のＭＳＯＬにおいて、
前記モバイル無線ネットワークは４Ｇネットワークであり、前記非暗号化データはサービングゲートウェイ（ＳＧＷ）を介して受信される、ＭＳＯＬ。
【請求項６】
請求項１に記載のＭＳＯＬにおいて、
前記セキュリティプロファイルは、複数の固有のモバイルデバイス識別情報の間で共用され、前記複数の固有のモバイルデバイス識別情報を識別するフィールドを含む、ＭＳＯＬ。
【請求項７】
請求項１に記載のＭＳＯＬにおいて、
前記セキュリティプロファイルディレクトリは、対応するモバイルデバイスからのデータを暗号化するための異なるセキュリティプロトコルを識別する別のセキュリティプロファイルを含む、ＭＳＯＬ。
【請求項８】
方法であって、
コンピュータ上で動作するモバイルセキュリティオフローダ（ＭＳＯＬ）において、モバイル無線ネットワーク内のモバイルデバイスから符号分割多重アクセス（ＣＤＭＡ）、グローバル移動体通信システム（ＧＳＭ）、またはユニバーサル移動体通信システム（ＵＭＴＳ）を介して送信される非暗号化データを受信すること、
前記非暗号化データから前記モバイルデバイスの固有のモバイルデバイス識別情報を決定すること、
前記固有のモバイルデバイス識別情報を使用して、セキュリティプロファイルディレクトリから前記固有のモバイルデバイス識別情報に対応するセキュリティプロファイルを取得することであって、前記固有のモバイルデバイス識別情報に対応する前記モバイルデバイスからのデータを暗号化するためのセキュリティプロトコルを識別する前記セキュリティプロファイルを取得すること、
前記セキュリティプロファイルで識別された前記セキュリティプロトコルを使用して前記非暗号化データを暗号化すること、
前記暗号化されたデータを、データ内で識別されたセキュアサーバにパケット交換ネットワークを介してルーティングすること、を備える方法。
【請求項９】
請求項８に記載の方法において、
前記固有のモバイルデバイス識別情報は国際移動体加入者識別番号（ＩＭＳＩ）である

、方法。
【請求項１０】
請求項８に記載の方法において、
前記固有のモバイルデバイス識別情報は移動局国際加入者ディレクトリ番号（ＭＳＩＳＤＮ）である、方法。
【請求項１１】
請求項８に記載の方法において、
前記固有のモバイルデバイス識別情報は電話番号である、方法。
【請求項１２】
請求項８に記載の方法において、
前記セキュアサーバから暗号化されたレスポンスデータを受信すること、
前記セキュリティプロファイルに基づいて前記暗号化されたレスポンスデータを復号化すること、をさらに備える方法。
【請求項１３】
請求項１２に記載の方法において、
前記ＭＳＯＬのキャッシュに前記セキュリティプロファイルを記憶することをさらに備える方法。
【請求項１４】
請求項８に記載の方法において、
前記モバイル無線ネットワークは２Ｇ／３Ｇネットワークであり、前記非暗号化データは、サービング汎用パケット無線サービス（ＧＰＲＳ）サポートノード（ＳＧＳＮ）を介して受信される、方法。
【請求項１５】
請求項８に記載の方法において、
前記モバイル無線ネットワークは４Ｇネットワークであり、前記非暗号化データはサービングゲートウェイ（ＳＧＷ）を介して受信される、方法。
【請求項１６】
請求項８に記載の方法において、
前記セキュリティプロファイルは、複数の固有のモバイルデバイス識別情報の間で共用され、前記複数の固有のモバイルデバイス識別情報を識別するフィールドを含む、方法。
【請求項１７】
請求項８に記載の方法において、
前記セキュリティプロファイルディレクトリは、対応するモバイルデバイスからのデータを暗号化するための異なるセキュリティプロトコルを識別する別のセキュリティプロファイルを含む、方法。
【請求項１８】
モバイルセキュリティオフローダ（ＭＳＯＬ）であって、
コンピュータ上で動作し、モバイル無線ネットワークを介してモバイルデバイスから、セキュアサーバ上でログイン処理を開始するための要求を受信し、前記要求から前記モバイルデバイスの固有のモバイルデバイス識別情報を決定するように構成されたモバイルデバイス識別用受信機コンポーネントと、
前記コンピュータ上で動作し、前記固有のモバイルデバイス識別情報を使用して前記モバイルデバイスをセキュリティプロファイルディレクトリにより認証し、その認証に応答して前記セキュリティプロファイルディレクトリから認証情報を受信するように構成されたセキュリティプロファイルディレクトリインタフェースと、
前記コンピュータ上で動作し、１つまたは複数のプロセッサによって実行可能であり、前記ログイン処理を開始するための要求に前記認証情報を追加するように構成された認証情報追加コンポーネントと、
前記コンピュータ上で動作し、パケット交換ネットワークを介して前記セキュアサーバに前記ログイン処理を開始するための要求をルーティングするように構成されたパケット

交換ネットワークインタフェースと、を備えるＭＳＯＬ。
【請求項１９】
請求項１８に記載のＭＳＯＬにおいて、
前記パケット交換ネットワークインタフェースはさらに、前記セキュアサーバからログイン成功メッセージを受信して、前記モバイル無線ネットワークを介して前記モバイルデバイスに前記ログイン成功メッセージを転送するように構成されている、ＭＳＯＬ。
【請求項２０】
方法であって、
モバイルセキュリティオフローダ（ＭＳＯＬ）において、モバイル無線ネットワークを介してモバイルデバイスから、セキュアサーバ上でログイン処理を開始するための要求を受信すること、
前記要求から前記モバイルデバイスの固有のモバイルデバイス識別情報を決定すること、
前記固有のモバイルデバイス識別情報を使用して、前記固有のモバイルデバイス識別情報に対応する認証情報をセキュリティプロファイルディレクトリから取得すること、
前記ログイン処理を開始するための要求に前記認証情報を追加すること、
パケット交換ネットワークを介して前記セキュアサーバに、前記ログイン処理を開始するための要求をルーティングすること、を備える方法。
【請求項２１】
請求項２０に記載の方法において、
前記固有のモバイルデバイス識別情報は国際移動体加入者識別番号（ＩＭＳＩ）である、方法。
【請求項２２】
請求項２０に記載の方法において、
前記固有のモバイルデバイス識別情報は移動局国際加入者ディレクトリ番号（ＭＳＩＳＤＮ）である、方法。
【請求項２３】
請求項２０に記載の方法において、
前記セキュアサーバからログイン成功メッセージを受信して、前記モバイル無線ネットワークを介して前記モバイルデバイスに前記ログイン成功メッセージを転送することをさらに備える方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、概して、モバイル無線ネットワーキングに関する。具体的には、本開示は、モバイルセキュリティのオフロードを記載する。
【背景技術】
【０００２】
モバイルネットワークにより、デバイスは、国際標準団体によって規定されたネットワーク内で提供される基本サービスの一部として外部パケット交換ネットワーク（インターネットなど）に接続することができる。このような国際標準団体の例として、グローバル移動体通信システム（ＧＳＭ（登録商標））／ユニバーサル移動体通信システム（ＵＭＴＳ）／ロングタームエボリューション（ＬＴＥ）領域、時分割多重アクセス（ＴＤＭＡ）／符号分割多重アクセス（ＣＤＭＡ）／ＣＤＭＡ２０００ネットワーク、ＬｏＲａやＳＩＧＦＯＸなどの新たな低電力広域ネットワーク（ＬＰＷＡＮ）構想における第３世代パートナーシッププロジェクト（３ＧＰＰ）が挙げられる。
【０００３】
このようなシステムにおいて、モバイルデバイスとやり取りするパケットデータは、２Ｇネットワークの基地トランシーバ局（ＢＴＳ）や、３Ｇネットワークのノードｂ（ＮｏｄｅＢ）や、または４Ｇネットワークの拡張型ノードＢ（ｅＮｏｄｅＢ）などの要素に無

線ネットワークを介して送信される。その後、パケットデータは、２Ｇ／３Ｇネットワークのサービング汎用パケット無線サービス（ＧＰＲＳ）サポートノード（ＳＧＳＮ）や、４Ｇネットワークのサービングゲートウェイ（ＳＧＷ）や、または他のモバイルネットワークソリューションにおける同様のデバイスに向けてトンネルを使用して送信される。

【０００４】

すべてのモバイルデバイスからのＧＰＲＳトンネリングプロトコル（ＧＴＰ）トンネルは、２Ｇ／３ＧネットワークのゲートウェイＧＰＲＳサポートノード（ＧＧＳＮ）や、４ＧネットワークのＰＤＮゲートウェイ（ＰＧＷ）や、または他のモバイルネットワークソリューションにおける同様のデバイスに向けて集約される。これらのデバイスは、各接続における多数のトンネルを含む多くのイーサネット（登録商標）接続をマージする。

【０００５】

次いで、ＧＧＳＮまたはＰＧＷの責任下で、集約されたＧＴＰトンネルのトラフィックを多数のデータストリームに分散させ、すべての単一ストリームをモバイルデバイスによって最初に指定された外部パケット交換ネットワーク上の指定された宛先にルーティングする。

【０００６】

モノのインターネット（ＩｏＴ）分野の急増に伴い、これまで以上に多くの異なる種類のモバイルデバイスが使用されており、自動車、スマートシティセンサ、船積み用コンテナ、ベビーカーなどのより多くの種類のデバイスがモバイル通信コンポーネントを採用するに従ってこの傾向は高まる一方である。

【発明の概要】

【０００７】

多数の異なる種類のモバイルデバイスにおいて、通信およびデータのセキュリティへの脅威が増大している。携帯電話の設計者は通信セキュリティの専門家と言えるが、ベビーカーの設計者はそうとは言えない場合がある。これは、そのような異種製品に埋め込まれたモバイル通信コンポーネントが共通のセキュリティ問題に対処する可能性を低くする。

【０００８】

さらに、ＩｏＴデバイスは、一般には、安価でバッテリを節約するように設計されている。ＩｏＴデバイスでセキュリティ機能を実行するにはより複雑なＣＰＵ設計とより多くの電力消費が必要となるため、これらの目的と矛盾し得る。

【０００９】

殆どのモバイルネットワーク自体は安全であるが、インターネットは安全性の低い媒体であるため、通信がモバイルネットワークを離れてインターネットに入るときセキュリティに対する脅威が増大する。

【図面の簡単な説明】

【００１０】

【図１】ＧＳＭ（２Ｇ）および／またはＵＭＴＳ（３Ｇ）モバイルネットワークにおいてネットワーク通信をルーティングするための例示的な実施形態に従ったシステムを示すブロック図。

【図２】ＧＳＭ（２Ｇ）および／またはＵＭＴＳ（３Ｇ）モバイルネットワークにおいてネットワーク通信をルーティングするための例示的な実施形態に従ったシステムを示すブロック図。

【図３】例示的な実施形態に従ったＧＰＲＳサブネットワークサービスのプロトコルスタックを示すブロック図。

【図４】ＳＧＳＮ／ＳＧＷおよびＧＧＳＮ／ＰＤＮゲートウェイ（ＰＧＷ）を含むシステムを示すブロック図。

【図５】例示的な実施形態によるＭＳＯＬを詳細に示すブロック図。

【図６】例示的な実施形態による、モバイルデバイスパケット上でハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）暗号化を行う方法を示す相互作用図。

【図７】例示的な実施形態による、モバイルデバイスパケット上でＴＬＳ暗号化を行う方

法を示す相互作用図。
【図８】例示的な実施形態による、モバイルデバイスパケット上でＶＰＮ暗号化を行う方法を示す相互作用図。
【図９】例示的な実施形態による、ショートメッセージングサービス（ＳＭＳ）パケット上でＴＬＳ暗号化を行う方法を示す相互作用図。
【図１０】例示的な実施形態による、音声呼上でセッション・イニシエーション・プロトコル・オーバーＴＬＳ（ＳＩＰＳ）／セキュア・リアルタイム・プロトコル（ＳＲＴＰ）暗号化を行う方法を示す相互作用図。
【図１１】例示的な実施形態による、ネットワーク認証情報をログイン処理に追加するＭＳＯＬを示す相互作用図。
【図１２】例示的な実施形態による、ネットワーク認証情報をログイン処理に追加可能なＭＳＯＬを示すブロック図。
【図１３】本明細書に記載の種々のハードウェアアーキテクチャとともに使用可能な代表的なソフトウェアアーキテクチャを示すブロック図。
【図１４】機械可読媒体（例えば、機械可読記憶媒体）から命令を読み込み本明細書に記載の方法のうちの任意の１つ以上を実行可能な、いくつかの例示的な実施形態によるマシンの構成要素を示すブロック図。
【発明を実施するための形態】
【００１１】
限定ではなく一例として、いくつかの実施形態を添付図面の図に示す。以下の説明は、例示的な実施形態を具体化する例示的なシステム、方法、技術、命令シーケンス、および演算マシンプログラム製品を含む。以下の説明では、説明の目的で、本発明の主題の種々の実施形態の理解をもたらすために多数の特定の詳細を述べる。しかしながら、本発明の主題の実施形態がこれらの特定の詳細なしに実施され得ることは当業者には明らかであり得る。概して、周知の命令インスタンス、プロトコル、構造、および技術は詳細には示されていない。
【００１２】
例示的な実施形態では、インターネットなどのパケット交換ネットワークに対する通信が行われる際にモバイルデバイスから無線ネットワークを介して送信される通信を保護するべくすべてのセキュリティ方法および暗号化を実行するように設計されたモバイル・セキュリティ・オフローダのコンポーネントに対し、セキュリティ方法および処理が、モバイルデバイスからオフロードされる。
【００１３】
図１は、ＧＳＭ（２Ｇ）および／またはＵＭＴＳ（３Ｇ）モバイルネットワークにおいてネットワーク通信をルーティングするための例示的な実施形態に従ったシステム１００を示すブロック図である。システム１００は、１つまたは複数のモバイルデバイス１０２Ａ～１０２Ｄを含む。各モバイルデバイス１０２Ａ～１０２Ｄは、セルトランシーバとして一般に知られる無線通信機を有する任意のタイプのデバイスとすることができる。モバイルデバイス１０２Ａ～１０２Ｄは、例えば、スマートフォン、タブレットコンピュータ、コネクティッド自動車、センサ、警報システムなどを含む。
【００１４】
各モバイルデバイス１０２Ａ～１０２Ｄは、無線通信を介してモバイルネットワークに接続する。図１は、モバイルネットワークの２つの別々の例示的な種類を示している。１つはＧＳＭベースのモバイルネットワークである。ＧＳＭベースのモバイルネットワークでは、モバイルデバイス１０２Ａ，１０２Ｂは、基地トランシーバ局（ＢＴＳ）１０４Ａ，１０４Ｂと無線通信を介して接続する。ＢＴＳ１０４Ａ，１０４Ｂは、無線インタフェースの終端ノードである。各ＢＴＳ１０４Ａ，１０４Ｂは１つ以上のトランシーバを含み、無線インタフェースの暗号化を行う。
【００１５】
各ＢＴＳ１０４は、次いで基地局コントローラ（ＢＳＣ）１０６と通信する。典型的に

は、ＢＳＣ１０６は、その制御下に数百のＢＴＳ１０４Ａ，１０４Ｂを有する。ＢＳＣ１０６は、モバイルデバイス１０２Ａ，１０２Ｂに無線リソースを割り当て、周波数を管理し、ＢＴＳ１０４間のハンドオーバを制御するように動作する。ＢＳＣ１０６は、コンセントレータとしても機能することができ、これにより、ＢＳＣ１０６への多くの低容量の接続がより少ない数の接続に低減されるようになる。

【００１６】

同図に示される２つ目の種類のモバイルネットワークは、ユニバーサル移動体通信システム（ＵＭＴＳ）ベースのモバイルネットワークである。ＵＭＴＳベースのモバイルネットワークは、広帯域符号分割多重アクセス（Ｗ－ＣＤＭＡ）の無線アクセス技術を使用する。ここで、モバイルデバイス１０２Ｃ，１０２Ｄは、ノードＢ（ＮｏｄｅＢ）１０８Ａ，１０８Ｂと無線通信を介して接続する。ノードＢ１０８Ａ，１０８Ｂは、無線インタフェースの終端ノードである。各ノードＢ１０８Ａ，１０８Ｂは１つ以上のトランシーバを含み、無線インタフェースの暗号化を行う。各ノードＢ１０８Ａ，１０８Ｂは、符号を適用してＣＤＭＡベースのＵＭＴＳネットワーク内のチャネルを記述するように構成されている。一般に、各ノードＢ１０８Ａ，１０８Ｂは、ＢＴＳ１０４Ａ，１０４ＢがＧＳＭネットワークに対して実行するのと同様の機能をＵＭＴＳネットワークに対して実行する。

【００１７】

各ノードＢ１０８Ａ，１０８Ｂは、次いで無線ネットワークコントローラ（ＲＮＣ）１１０と通信する。典型的には、ＲＮＣ１１０は、その制御下に数百のノードＢ１０８Ａ，１０８Ｂを有する。ＲＮＣ１１０は、モバイルデバイス１０２Ｃ，１０２Ｄに無線リソースを割り当て、周波数を管理し、ノードＢ１０８Ａ，１０８Ｂ間のハンドオーバを制御するように動作する。ＲＮＣ１１０は、コンセントレータとしても機能することができ、これにより、ＲＮＣ１１０への多くの低容量の接続がより少ない数の接続に低減されるようになる。

【００１８】

同図には、２つの異なるモバイルネットワークの種類が示されているが、本開示で説明される概念は、単一のネットワークの種類のみを有するシステムにも適用され得るものであり、さらには、図１に示されるネットワークの種類に加えてまたはそれに代えて多数のネットワークの種類を有するシステムにも適用され得る。

【００１９】

ＢＴＳ１０４Ａ，１０４Ｂおよび／またはノードＢ１０８Ａ，１０８Ｂは、ネットワーク内のすべてのパケット交換データを処理するサービングＧＰＲＳサポートノード（ＳＧＳＮ）１１２に接続する。典型的なシステム１００においては、実際に２つの形式のＧＰＲＳサポートノード（ＧＳＮ）が存在する。ここでは、第１の種類はＳＳＧＮであり、その地理的サービスエリア内のＢＴＳ１０４Ａ，１０４ＢやノードＢ１０８Ａ，１０８Ｂとの間でデータパケットの配信を典型的には行う。追加のタスクは、パケットルーティングおよび転送、モビリティ管理（着脱およびモビリティ管理）、論理リンク管理、および課金機能を含み得る。

【００２０】

いくつかの例示的な実施形態では、ＳＧＳＮ１１２に関して上述した機能は、簡略化のためにここには示されていないが、サービングゲートウェイ（ＳＧＷ）によって実行される。いくつかの他の例示的な実施形態では、いくつかの他のタイプのデバイスがＳＧＳＮ１１２に関して上述した機能を実行することができる。ＳＧＳＮ１１２およびＳＧＷを含むこれらのデバイスの種類を総称して「アグリゲータ」または「パケットアグリゲータ」と呼ぶことができる。

【００２１】

データパケットは、モバイルデバイス１０２Ａ～１０２Ｄから、インターネット１１４などの外部パケット交換データネットワークに向けて上流に送信される。ＳＧＳＮ１１２は、モバイルデバイス１０２Ａ～１０２Ｄからのデータパケットを集約して、それらを第２の種類のＧＳＮであるゲートウェイＧＰＲＳサポートノード（ＧＧＳＮ）１１６に送信

する。ＧＧＳＮ１１６は、ＧＰＲＳネットワークと、インターネット１１４などの外部パケット交換ネットワークとの間のインターネットワーキングを行う。外部ネットワークから見ると、ＧＧＳＮ１１６はＧＰＲＳインフラストラクチャを外部ネットワークから隠すので、ＧＧＳＮ１１６はサブネットワークへのルータである。ＧＧＳＮ１１６は、特定のユーザ宛のデータを受信すると、ユーザがアクティブであるかどうかをチェックする。ユーザがアクティブである場合、ＧＧＳＮ１１６は、モバイルユーザにサービスするＳＧＳＮ１１２にデータを転送する。モバイルユーザが非アクティブである場合、データは破棄される。ＧＧＳＮ１１６は、ＧＰＲＳネットワーク内のユーザ端末のモビリティを可能にするアンカーポイントである。

【００２２】

このシステム１００を介して送信されるデータを保護するために、モバイルデバイス１０２Ａ～１０２Ｄは、セキュアソケット層（ＳＳＬ）、トランスポート層セキュリティ（ＴＬＳ）、仮想プライベートネットワーク（ＶＰＮ）などの方法を使用してデータを暗号化することができる。そして、この暗号化は、ＢＴＳ１０４Ａ，１０４ＢまたはノードＢ１０８Ａ，１０８Ｂと、ＢＳＣ１０６またはＲＮＣ１１０と、ＳＧＳＮ１１２と、ＧＧＳＮ１１６とを含むネットワーク内のすべてのコンポーネント、および最終的にはインターネット１１４を介してセキュアサーバ１１８に至るまで維持される。しかしながら、この方法は、暗号化機構を用いてモバイルデバイス１０２Ａ～１０２Ｄをプログラミング／設計する必要があるため、モバイルデバイス１０２Ａ～１０２Ｄのコストおよび電力の利用を増加させる。また、モバイルデバイス１０２Ａ～１０２Ｄをインターネット１１４上の悪意のあるデバイスから保護するためには、内部ファイアウォールを維持する必要がある。

【００２３】

図２は、ＧＳＭ（２Ｇ）および／またはＵＭＴＳ（３Ｇ）モバイルネットワークにおいてネットワーク通信をルーティングするための例示的な実施形態に従ったシステム２００を示すブロック図である。図２の種々のコンポーネントは、モバイル・セキュリティ・オフローダ（ＭＳＯＬ）２０２および対応するセキュリティプロファイルディレクトリ２０４の追加を除いて、図１のものと同様である。図２では、モバイルデバイス１０２Ａ～１０２Ｄ自体に対してセキュリティ暗号化は実行されず、モバイルデバイス１０２Ａ～１０２Ｄは、モバイルネットワークを介して、暗号化されていないトラフィックをＭＳＯＬ２０２に向けて送信し、このトラフィックの保護をモバイルネットワークプロバイダのセキュリティプロトコルに委ねる。次いで、ＭＳＯＬ２０２は、セキュリティ・プロファイル・ディレクトリ２０４から、送信側のモバイルデバイス１０２Ａ～１０２Ｄに対応するセキュリティプロファイルを取得する。送信側のモバイルデバイス１０２Ａ～１０２Ｄは、国際移動体加入者識別番号（ＩＭＳＩ）または移動局国際加入者ディレクトリ番号（ＭＳＩＳＤＮ）などの、加入者識別番号モジュール（ＳＩＭ）またはユニバーサル集積回路カード（ＵＩＣＣ）カード識別子に基づいて識別され得る。対応するセキュリティプロファイルに基づいて、ＭＳＯＬ２０２は、どのようにトラフィックを暗号化しそれを暗号化の形態でセキュアサーバ１１８に送るかを知る。暗号化は、ＳＳＬ、ＴＬＳ、ＶＰＮなどの方法を使用してＭＳＯＬ２０２上で実行され得る。これにより、モバイルデバイス１０２Ａ～１０２Ｄ自体のセキュリティおよび暗号化を行う必要性を除去する。いくつかの例示的な実施形態では、ＭＳＯＬ２０２は、格納されたセキュリティプロファイルに基づいてモバイルデバイス１０２Ａ～１０２Ｄのための外部ファイアウォールを提供することもできる。

【００２４】

図３は、例示的な実施形態に従ったＧＰＲＳサブネットワークサービスのプロトコルスタックを示すブロック図である。同図には、モバイルデバイス（ＭＳ）３００、基地局（ＢＳ）３０２、ＳＧＳＮ３０４、およびＧＧＳＮ３０６が示されている。ＧＴＰ３０８は、Ｇｎインタフェースを用いてＳＧＳＮ３０４とＧＧＳＮ３０６との間で使用されるプロトコルである。これはレイヤ３トンネリングプロトコルである。ネットワーク内外のユー

ザには、行われる処理は通常のＩＰサブネットワークのように見える。アプリケーション３１０は、ＩＰ３１２を介して通信し、ＧＰＲＳネットワークおよびＧＧＳＮ３０６を介して実行される。ＧＧＳＮ３０６とＳＧＳＮ３０４との間で移動するパケットは、ＧＴＰ３０８を使用する。このようにＧＰＲＳの外側に位置するＩＰアドレスは内部バックボーンに対処する必要はない。ＳＧＳＮ３０４上では、ＵＤＰ３１４およびＩＰ３１２は、ＧＴＰ３０８によって実行される。

【００２５】

サブネットワーク依存コンバージェンスプロトコル（ＳＮＤＣＰ）３１６および論理リンク制御（ＬＬＣ）３１８は、ＳＧＳＮ３０４とＭＳ３００との間で組み合わせて使用される。ＳＮＤＣＰ３１６は、ユーザプレーンＧＰＲＳプロトコルスタックの最上層である。ＳＮＤＣＰ３１６は、データを平坦化して無線チャネル上の負荷を低減する。ＳＮＤＣＰ３１６の主な目的は、ネットワークプロトコルデータユニット（ＰＤＵ）をバッファリングおよびセグメント化し、ヘッダを各セグメントに追加して、セグメントをＬＬＣ３１８に供給して送信させることである。パケットを暗号化することによって生成される安全な論理リンクはＬＬＣ３１８によって提供され、移動体が単一のＳＧＳＮ３０４の下にある限り、同じＬＬＣ３１８のリンクが使用される。また、ＳＮＤＣＰ３１６は、圧縮および解凍を実行する。この目的は、無線送信が要求されるデータの量を低減することにある。従って、ＳＮＤＣＰ３１６の多くは、圧縮関連機能のためのパケットデータネットワーク（ＰＤＮ）プロトコルに関する特定の詳細を認識する。また、ＳＮＤＣＰ３１６は、ＰＤＰコンテキスト、およびＰＤＰタイプやＱｏＳなどの対応する情報についても認識し得る。この情報は、ＰＤＰコンテキストアクティベーションプロシージャ中に与えられる。

【００２６】

ＬＬＣ３１８の機能は、データ送信の完全性を管理し保証することである。ＬＬＣ３１８は、ネットワーク層プロトコルのサービスに対してデータリンク層のリンクを提供する。これは、ネットワークコンピュータ上に存在するサービスに対するＬＬＣサービスアクセスポイントによって実現される。さらに、配信リクエストまたはサービスのためのＬＬＣ制御フィールドが存在する。また、ＬＬＣ３１８は、パケットの暗号化および解読を実行し得る。

【００２７】

図４は、ＳＧＳＮ／ＳＧＷ４０２およびＧＧＳＮ／ＰＤＮゲートウェイ（ＰＧＷ）４０４を含むシステム４００を示すブロック図である。例示的な実施形態では、ＳＧＳＮ／ＳＧＷ４０２は図１のＳＧＳＮ１１２とすることができ、ＧＧＳＮ／ＰＧＷ４０４は図１のＧＧＳＮ１１６とすることができる。ＳＧＳＮ／ＳＧＷ４０２は、モバイル無線ネットワークからＧｎインタフェースポートを介してＧＧＳＮ／ＰＧＷ４０４にデータを転送する。Ｇｎは、ＧＰＲＳトンネリングプロトコル（ＧＴＰ）トンネルで構成されている。ＧＴＰ３０８は、トンネルを制御するＧＴＰ－Ｃと実際のユーザトラフィックデータであるＧＴＰ－Ｕとに分割される。

【００２８】

オンライン課金システム（ＯＣＳ）４０６は、Ｇｙ参照ポイントを介してＧＧＳＮ／ＰＧＷ４０４に接続する。ＯＣＳ４０６は、特定のトンネルに帯域幅に関する割り当てがあるかどうかをＧＧＳＮ／ＰＧＷ４０４に通知する請求システムであり、ユーザ毎の実際のサービスプランおよび口座残高に基づいてトンネリングを許可または禁止する。オンライン課金は２つのサブ機能、すなわちレーティングと単位判定とを有する。それらはともに集中型または分散型として実装することができる。

【００２９】

レーティングとは、単位判定機能によって算出される非貨幣単位の計算のことである。単位判定とは、サービス配信の開始前に割り当てられる非貨幣単位（サービス単位、データ量、時間およびイベント）の数の計算のことである。

【００３０】

オンライン課金については、即時イベント課金（ＩＥＣ）、単位予約によるイベント課

金（ＥＣＵＲ）、および単位予約によるセッション課金（ＳＣＵＲ）の３つの場合を区別することができる。

【００３１】

ＩＥＣは、自動引き落とし処理を伴い、この処理では金融口座に適切な手数料が即座に引き落とされる。ＥＣＵＲでは、金融単位がサービス配信に先立って予約され、サービス配信の完了後に金融口座引き落とし処理が実行される。ＳＣＵＲでは、金融単位がセッション監視に先立って予約され、セッション終了の完了後に金融口座引き落とし処理が実行される。

【００３２】

オフライン課金システム（ＯＦＣＳ）４０８は、Ｇｚ参照ポイントを介してＧＧＳＮ／ＰＧＷ４０４に接続する。ＯＦＣＳ４０８は、後払い呼び出し詳細記録（ＣＤＲ）処理に関する請求システムである。オフライン課金は、ネットワークリソース使用の課金情報がそのリソース使用と同時に収集される処理である。この課金情報は、その後、一連の論理課金機能に渡される。この処理の最後に、ＣＤＲファイルがネットワークによって生成され、このＣＤＲファイルは、加入者請求および／またはインターオペレータ会計（または統計などの追加機能）のためにネットワーク事業者の請求ドメインに転送される。請求ドメインは典型的には、オペレータの請求システムまたは請求仲介デバイスなどの後処理システムを含む。

【００３３】

オフライン課金機能は例えば、課金トリガ機能（ＣＴＦ）、課金データ機能（ＣＤＦ）、および課金ゲートウェイ機能（ＣＧＦ）を含む。ＣＴＦは、ネットワークリソース使用の観測に基づいて課金イベントを生成する。ＣＴＦは主に、ネットワーク要素内の課金可能イベントに関する情報を収集して、この情報を対応する課金イベントに組み込み、これらの課金イベントをＣＤＦに送信する。ＣＴＦは２つの機能ブロック、すなわちアカウントメトリック収集とアカウントデータ転送とからなる。アカウントメトリック収集は、ネットワークユーザによって確立されたサービスイベントまたはセッションの呼び出し、またはそれら呼び出し（サービスイベントまたはセッション）に関するユーザトラフィックの処理、またはこれらの呼び出し（サービスイベントまたはセッション）を通じたユーザへのサービス配信のためのシグナリング機能を監視する。アカウントデータ転送は、収集したアカウントメトリックを受信し、それらメトリックのうちの１つ以上のセットから課金可能イベントの発生を判定してその検出した課金可能イベントに一致する課金イベントを組み立て、Ｒｆインタフェースを介して課金データ機能にその課金イベントを転送する。

【００３４】

ＣＤＦは、Ｒｆ参照ポイントを介してＣＴＦから課金イベントを受信する。ＣＤＦは、次いで課金イベントに含まれる情報を使用してＣＤＲを構築する。ＣＤＦによって生成されたＣＤＲは、Ｇａインタフェースポイントを介して課金ゲートウェイ機能（ＣＧＦ）に直ちに転送される。ＣＧＦは、Ｇａインタフェースを介したＣＤＦからのほぼリアルタイムでのＣＤＲ受信、ＣＤＲ前処理、検証、ＣＤＲの統合および（再）フォーマット、ＣＤＲエラー処理、永続的なＣＤＲストレージ、ＣＤＲルーティングおよびフィルタリング、ＣＤＲファイル管理、および請求ドメインへのＣＤＲファイル転送などの機能を実行する。

【００３５】

パケットデータネットワーク４１０は、Ｇｉ参照ポイントを介してＧＧＳＮ／ＰＧＷ４０４に接続する。パケットデータネットワーク４１０は、モバイルデバイス３００がデータを送信することができる公衆または私設のデータネットワークである。ポリシーおよび課金ルール機能（ＰＣＲＦ）４１２は、Ｇｘ参照ポイントを介してＧＧＳＮ／ＰＧＷ４０４に接続し、ＧＧＳＮ／ＰＧＷ４０４内でデータフローポリシーを実施する方法の一部をなす。ＰＣＲＦ４１２は、ルールを収集してそれらをＧＧＳＮ／ＰＧＷ４０４に渡す役割を果たす。ＰＣＲＦ４１２は、サービスデータフロー検出、ゲーティング（パケットのブ

ロッキングまたは許可）、ＱｏＳ制御、および課金に関するネットワーク制御を提供する。ＰＣＲＦ４１２は、例えば、サービス情報が加入者情報と一致しないとき、アプリケーション３１０から受信したリクエストを拒否することができる。

【００３６】

ＰＣＲＦ４１２は、Ｓｐ参照ポイントを介して加入者プロファイルリポジトリ（ＳＰＲ）４１４に接続する。ＳＰＲ４１４は、典型的にはＰＤＮ毎を基準に記憶された加入者および加入者情報を含み、加入者の許可されたサービス、加入者の許容ＱｏＳに関する情報、加入者の課金関連情報、および加入者カテゴリなどの情報を含み得る。ＰＣＲＦ４１２は、ＳＰＲ４１４にアクセスして、関連する各ユーザのプロファイルを問い合わせることができる。アプリケーション機能（ＡＦ）４１６は、Ｒｘ参照ポイントを介してＰＣＲＦ４１２に接続し、外部アプリケーションロジックによりＰＣＲＦの規則を変更可能とする。

【００３７】

ＧＧＳＮ／ＰＧＷ４０４は、ポリシー実施ルール機能（ＰＣＥＦ）４１８を使用して、ＰＣＲＦ４１２によって作成された規則を実施する。ＧＧＳＮ／ＰＧＷ４０４は、ＶＰＮ、ネットワークアドレス変換（ＮＡＴ）、および基本ファイアウォールの確立だけでなく基本ルーティング機能を可能にするが、これらのサービスはすべて、ネットワークオペレータ構成に基づいており、この機能のいずれもサービスの実際のベアラ（モバイルデバイス３００およびその所有者、ならびに所有者を雇用する企業または他の組織、総称して顧客として知られる）によって変更されるようにエクスポートされない。また、これらは、モバイルデバイス３００からの特定のパケットトラフィックではなく、内部ネットワーク要素と外部ネットワーク要素との接続に向けられている。また、ＰＣＲＦ４１２は、ブラックリスト（例えば、禁止されたモバイルデバイス３００、ネットワークロケーション、トラフィックタイプなどのリスト）を使用してセキュリティルールを実施する。

【００３８】

図５は、例示的な実施形態によるＭＳＯＬ２０２を詳細に示すブロック図である。ＭＳＯＬ２０２は、データをＭＳＯＬ２０２に送信したモバイルデバイス３００を識別するように動作するモバイルデバイス識別コンポーネント５００を含み得る。データは、ＨＴＴＰリクエスト、ＴＣＰパケット、音声呼、ＳＭＳメッセージなどを含む任意の数の異なる種類の通信を含み得る。モバイルデバイス識別コンポーネント５００は、データ自体に少なくとも部分的に基づいて、どのモバイルデバイス３００がデータを送信したかを判定することができる。例えば、データは、モバイルデバイス３００のＩＭＳＩまたは同様の固有識別情報を識別するフィールドを含み得る。あるいは、音声呼の場合、音声呼に付随するメタデータは、発呼者ＩＤ機構を介して電話番号などの固有識別情報を含み得る。モバイルデバイス識別コンポーネント５００は、モバイルデバイス３００の識別情報の形態に関係なく、この識別情報をセキュリティプロファイルディレクトリインタフェース５０２に転送し得る。このセキュリティプロファイルディレクトリインタフェース５０２は、セキュリティプロファイルディレクトリ２０４に対する、モバイルデバイス識別情報に対応するプロファイルのリクエストを生成するように動作し得る。

【００３９】

対応するプロファイルは、セキュリティプロファイルディレクトリ２０４からセキュリティプロファイルディレクトリインタフェース５０２に返される。そして、プロファイルは、プロファイルからの情報を使用してデータを暗号化するように動作する暗号化エンジン５０４に送られる。プロファイルのフォーマットは、実装に依存して、さらには、セキュアサーバ１１８への送信のために使用される暗号化方式に基づいて大きく変わり得る。いくつかの例示的な実施形態では、例えば特定の個別セキュリティプロファイル内の情報が別の個別セキュリティプロファイル内の情報と正確に一致し得る場合（例えば、２人の個人が全く同じセキュリティ暗号化のパラメータを使用する場合など）があるとしても、各モバイルデバイス識別情報は、対応する個別セキュリティプロファイルを有する。その場合、セキュリティプロファイルは、そのセキュリティプロファイルのフィールドに適用

する特定のモバイルデバイス識別情報をリストすることができ、このリストをセキュリティプロファイルディレクトリ２０４によって検索することで、必要に応じてセキュリティプロファイルを取得することができる。他の例示的な実施形態では、対応するセキュリティプロファイルは、複数のモバイルデバイス識別情報の間で共有され得る。その場合、セキュリティプロファイルは、そのセキュリティプロファイルが適用されるグループまたは識別情報の範囲を特定し得る。このグループまたは識別情報の範囲をセキュリティプロファイルディレクトリ２０４によって検索することで、必要に応じてセキュリティプロファイルを取得することができる。

【００４０】

なお、いくつかの例示的な実施形態では、モバイルオペレータおよび／またはエンド加入者は、コマンドラインインタフェース、ウェブインタフェース、またはＡＰＩなどの１つまたは複数の異なる種類のインタフェースを介して、プロファイルディレクトリを変更することができる。

【００４１】

暗号化エンジン５０４は、ソフトウェアコンポーネント、ハードウェアコンポーネント、またはそれらのいくつかの変形形態とすることができる。特定の種類の暗号化は、ソフトウェアよりもハードウェアで実装するほうが有益となる場合がある。いくつかの例示的な実施形態では、暗号化エンジン５０４は、セキュリティプロファイル内の情報に基づいて複数の異なる種類の暗号化を処理するように設計されている。

【００４２】

最も簡単な形態では、セキュリティプロファイルは、モバイルデバイス１０２からセキュアサーバ１１８へのデータを暗号化するために使用する暗号化規格を識別し得る。例えば、セキュリティプロファイルは、モバイルデバイス１０２からセキュアサーバ１１８へのデータを暗号化するためにＨＴＴＰＳ、ＴＬＳ、ＶＰＮ、またはセキュアリアルタイム転送プロトコル（ＳＲＴＰ）暗号化を使用すべきであることを識別し得る。ただし、いくつかの場合には、セキュリティプロファイルは、認証情報（例えば、証明書、ユーザ名、パスワード）やセキュリティパラメータ（例えば、暗号化レベル、サブフォーマット）や他の接続パラメータなどのデータを暗号化する方法に関する追加の詳細を含み得る。

【００４３】

ＨＴＴＰＳプロファイルは例えば、プロファイルの名前、プロファイルが関係するモバイルデバイス識別情報、種々のＨＴＴＰＳセキュリティフィールド（例えば、実行されるセキュリティチェックのチェックリスト）、および種々のＨＴＴＰＳパラメータフィールド（例えば、リモートロギング）を含み得る。

【００４４】

ＴＬＳプロファイルは例えば、プロファイルの名前、プロファイルが関係するモバイルデバイス識別情報、種々のＴＬＳセキュリティフィールド（例えば、最小プロトコル方法、暗号、証明書認証）、および種々のＴＬＳパラメータフィールド（例えば、ノンス（nonce）有効時間、トランスポートタイプ）を含み得る。

【００４５】

ＶＰＮプロファイルは例えば、プロファイルの名前、プロファイルの記述、プロファイルが関係するモバイルデバイス識別情報、種々のＶＰＮセキュリティフィールド（例えば、クライアント認証方法、パスワードの永続的有効化）、および接続パラメータを識別する種々のＶＰＮパラメータフィールド（例えば、自動ネットワーク検出の有効化、最大送信単位のサイズ、接続失敗を示す前の待機時間、ホストＩＤチェックの有効化）を含み得る。

【００４６】

セキュアサーバ１１８から応答が受信されると、暗号化エンジン５０４は、同じセキュリティプロファイルを使用して、その応答を解読フォーマットに解読するように動作し得る。この解読された応答は、モバイルデバイス３００に転送され得る。実際には、ＭＳＯＬ２０２は、多くの異なるモバイルデバイス３００からだけでなく、多くの異なるセキュ

アサーバ１１８から多くのデータを受信し得る。このため、いくつかの例示的な実施形態では、取得されたセキュリティプロファイルを記憶するためにＭＳＯＬ２０２上にキャッシュ（図示略）が維持され得る。このキャッシュは、一時的スケジュール（例えば、プロファイルがキャッシュに維持されている期間）またはセッションスケジュール（例えば、セッションが対応するモバイルデバイス３００とセキュアサーバ１１８との間で維持される限りセキュリティプロファイルがキャッシュに維持される）に基づいてパージされ得る。

【００４７】

図６は、例示的な実施形態による、モバイルデバイスパケット上でハイパーテキスト転送プロトコルセキュア（ＨＴＴＰＳ）暗号化を行う方法６００を示す相互作用図である。この方法６００は、モバイルデバイス（ＭＤ）６０２と、ＭＤ６０２が接続されたモバイルネットワーク６０４と、ＭＳＯＬ６０６と、セキュリティプロファイルディレクトリ（ＳＰＤ）６０８と、インターネット６１０と、セキュアサーバ６１２とを利用する。動作６１４において、ＨＴＴＰリクエストがモバイルデバイス６０２からモバイルネットワーク６０４に送信され、動作６１６において、そのＨＴＴＰリクエストがＭＳＯＬ６０６に転送される。動作６１８において、ＭＳＯＬ６０６は、ＳＰＤ６０８にデバイスプロファイルを要求する。この動作は、ＩＭＳＩなどのＭＤ６０２の固有識別子を識別し、その固有識別子をＳＰＤ６０８に転送することを含み得る。そして、動作６２０において、ＳＰＤ６０８は、ＨＴＴＰＳ暗号化プロファイルを返す。ＨＴＴＰＳ暗号化プロファイルは、ＩＭＳＩなどの固有識別子によって識別されるＭＤ６０２に対応するものであり得る。動作６２２において、ＭＳＯＬ６０６は、このＨＴＴＰＳ暗号化プロファイルを使用してＨＴＴＰリクエストを暗号化し、ＨＴＴＰＳリクエストを形成する。動作６２４において、ＭＳＯＬ６０６は、このＨＴＴＰＳリクエストをセキュアサーバ６１２に向けてインターネット６１０に送信し、動作６２６において、セキュアサーバ６１２は、そのＨＴＴＰＳリクエストを受信する。次に、セキュアサーバ６１２は、ＨＴＴＰＳ復号化を実行してリクエストを読み取り、それに応じて動作することでＨＴＴＰレスポンスを形成し、ＨＴＴＰレスポンスをＨＴＴＰＳレスポンスとして暗号化し得る。そして、動作６２８において、ＨＴＴＰＳレスポンスが送信され、動作６３０において、そのＨＴＴＰＳレスポンスがＭＳＯＬ６０６で受信される。次に、ＭＳＯＬ６０６は、動作６３２においてデバイスプロファイルを使用してＨＴＴＰＳレスポンスを復号化し、動作６３４において、その復号化によって得られたＨＴＴＰレスポンスをモバイルネットワーク６０４に送信する。そして、動作６３６において、モバイルネットワーク６０４は、ＨＴＴＰレスポンスをＭＤ６０２に転送する。

【００４８】

図７は、例示的な実施形態による、モバイルデバイスパケット上でＴＬＳ暗号化を行う方法７００を示す相互作用図である。この方法７００は、モバイルデバイス（ＭＤ）７０２と、ＭＤ７０２が接続されたモバイルネットワーク７０４と、ＭＳＯＬ７０６と、セキュリティプロファイルディレクトリ（ＳＰＤ）７０８と、インターネット７１０と、セキュアサーバ７１２とを利用する。動作７１４において、ＴＣＰトラフィックがモバイルデバイス７０２からモバイルネットワーク７０４に送信され、動作７１６において、そのＴＣＰトラフィックがＭＳＯＬ７０６に転送される。動作７１８において、ＭＳＯＬ７０６は、ＳＰＤ７０８にデバイスプロファイルを要求する。この動作は、ＩＭＳＩなどのＭＤ７０２の固有識別子を識別し、その固有識別子をＳＰＤ７０８に転送することを含み得る。そして、動作７２０において、ＳＰＤ７０８は、ＴＬＳ暗号化プロファイルを返す。ＴＬＳ暗号化プロファイルは、ＩＭＳＩなどの固有識別子によって識別されるＭＤ７０２に対応するものであり得る。動作７２２において、ＭＳＯＬ７０６は、セキュアサーバ７１２とのＴＬＳハンドシェイクを開始し、このＴＬＳハンドシェイクは、動作７２４において、インターネット７１０を介してセキュアサーバ７１２によって受信される。動作７２６において、セキュアサーバ７１２は、ハンドシェイクレスポンスをＭＳＯＬ７０６に送信し得る。そして、このハンドシェイクレスポンスは、動作７２８において、インターネ

ット７１０を介してＭＳＯＬ７０６によって受信される。
【００４９】
動作７３０において、ＭＳＯＬ７０６は、ＴＬＳ暗号化プロファイルを使用してＴＣＰトラフィックを暗号化し、ＴＣＰｏｖｅｒ ＴＬＳトラフィックを形成する。動作７３２において、ＭＳＯＬ７０６は、このＴＣＰｏｖｅｒ ＴＬＳトラフィックをセキュアサーバ７１２に向けてインターネット７１０に送信し、動作７３４において、セキュアサーバ７１２は、そのＴＣＰｏｖｅｒ ＴＬＳトラフィックを受信する。次に、セキュアサーバ７１２は、ＴＬＳ復号化を実行してそのトラフィックを読み取り、それに応じて動作することでＴＣＳトラフィックのレスポンスを形成し、それをＴＣＰｏｖｅｒ ＴＬＳトラフィックとして暗号化し得る。そして、動作７３６において、ＴＣＰｏｖｅｒ ＴＬＳトラフィックが送信され、動作７３８において、そのＴＣＰｏｖｅｒ ＴＬＳトラフィックがＭＳＯＬ７０６で受信される。次に、ＭＳＯＬ７０６は、動作７４０においてＴＣＰｏｖｅｒ ＴＬＳトラフィックを復号化し、動作７４２において、その復号化によって得られたＴＣＰトラフィックをモバイルネットワーク７０４に送信する。そして、動作７４４において、モバイルネットワーク７０４は、ＴＣＰトラフィックをＭＤ７０２に転送する。
【００５０】
図８は、例示的な実施形態による、モバイルデバイスパケット上でＩＰＳＥＣ暗号化などのＶＰＮ暗号化を行う方法８００を示す相互作用図である。この方法８００は、モバイルデバイス（ＭＤ）８０２と、ＭＤ８０２が接続されたモバイルネットワーク８０４と、ＭＳＯＬ８０６と、セキュリティプロファイルディレクトリ（ＳＰＤ）８０８と、インターネット８１０と、セキュアサーバ８１２とを利用する。動作８１４において、ＩＰトラフィックがモバイルデバイス８０２からモバイルネットワーク８０４に送信され、動作８１６において、そのＩＰトラフィックがＭＳＯＬ８０６に転送される。動作８１８において、ＭＳＯＬ８０６は、ＳＰＤ８０８にデバイスプロファイルを要求する。この動作は、ＩＭＳＩなどのＭＤ８０２の固有識別子を識別し、その固有識別子をＳＰＤ８０８に転送することを含み得る。そして、動作８２０において、ＳＰＤ８０８は、ＶＰＮ暗号化プロファイルを返す。ＶＰＮ暗号化プロファイルは、ＩＭＳＩなどの固有識別子によって識別されるＭＤ８０２に対応するものであり得る。動作８２２において、ＭＳＯＬ８０６は、セキュアサーバ８１２とのＶＰＮ接続開始を行う。このＶＰＮ接続開始は、動作８２４において、インターネット８１０を介してセキュアサーバ８１２によって受信される。動作８２６において、セキュアサーバ８１２は、ＭＳＯＬ８０６にＶＰＮ接続レスポンスを送信し得る。このＶＰＮ接続レスポンスは、動作８２８において、インターネット８１０を介してＭＳＯＬ８０６によって受信される。
【００５１】
動作８３０において、ＭＳＯＬ８０６は、ＶＰＮ暗号化プロファイルを使用してＩＰトラフィックを暗号化し、ＩＰｏｖｅｒ ＶＰＮトラフィックを形成する。動作８３２において、ＭＳＯＬ８０６は、このＩＰｏｖｅｒ ＶＰＮトラフィックをセキュアサーバ８１２に向けてインターネット８１０に送信し、動作８３４において、セキュアサーバ８１２は、そのＩＰｏｖｅｒ ＶＰＮトラフィックを受信する。次に、セキュアサーバ８１２は、ＶＰＮ復号化を実行してそのトラフィックを読み取り、それに応じて動作することでＩＰトラフィックのレスポンスを形成し、それをＩＰｏｖｅｒ ＶＰＮトラフィックとして暗号化し得る。そして、動作８３６において、ＩＰｏｖｅｒ ＶＰＮトラフィックが送信され、動作８３８において、そのＩＰｏｖｅｒ ＶＰＮトラフィックがＭＳＯＬ８０６で受信される。次に、ＭＳＯＬ８０６は、動作８４０においてＩＰｏｖｅｒ ＶＰＮトラフィックを復号化し、動作８４２において、その復号化によって得られたＩＰトラフィックをモバイルネットワーク８０４に送信する。そして、動作８４４において、モバイルネットワーク８０４は、ＩＰトラフィックをＭＤ８０２に転送する。
【００５２】
図９は、例示的な実施形態による、ショートメッセージングサービス（ＳＭＳ）パケット上でＴＬＳ暗号化を行う方法９００を示す相互作用図である。この方法９００は、モバ

イルデバイス（ＭＤ）９０２と、ＭＤ９０２が接続されたモバイルネットワーク９０４と、ＭＳＯＬ９０６と、セキュリティプロファイルディレクトリ（ＳＰＤ）９０８と、インターネット９１０と、セキュアサーバ９１２とを利用する。動作９１４において、ＳＭＳメッセージがモバイルデバイス９０２からモバイルネットワーク９０４に送信され、動作９１６において、そのＳＭＳメッセージがＭＳＯＬ９０６に転送される。この動作は、シグナリングシステム７（ＳＳ７）またはショートメッセージピアツーピア（ＳＭＰＰ）ベアラのいずれかを介して実行され得る。動作９１８において、ＭＳＯＬ９０６は、デバイスプロファイルをＳＰＤ９０８に要求する。この動作は、ＩＭＳＩなどのＭＤ９０２の固有識別子を識別し、その固有識別子をＳＰＤ９０８に転送することを含み得る。そして、動作９２０において、ＳＰＤ９０８は、ＴＬＳ暗号化プロファイルを返す。ＴＬＳ暗号化プロファイルは、ＩＭＳＩなどの固有識別子によって識別されるＭＤ９０２に対応するものであり得る。動作９２２において、ＭＳＯＬ９０６は、セキュアサーバ９１２とのＴＬＳハンドシェイクを開始し、このＴＬＳハンドシェイクは、動作９２４において、インターネット９１０を介してセキュアサーバ９１２によって受信される。動作９２６において、セキュアサーバ９１２は、ＴＬＳハンドシェイクレスポンスをＭＳＯＬ９０６に送信し得る。このＴＬＳハンドシェイクレスポンスは、動作９２８において、インターネット９１０を介してＭＳＯＬ９０６によって受信される。

【００５３】

動作９３０において、ＭＳＯＬ９０６は、ＴＬＳ暗号化プロファイルを使用してＳＭＳメッセージを暗号化し、ＴＣＰｏｖｅｒ ＴＬＳによるＳＭＳトラフィックを形成する。動作９３２において、ＭＳＯＬ９０６は、このＴＣＰｏｖｅｒ ＴＬＳによるＳＭＳトラフィックをセキュアサーバ９１２に向けてインターネット９１０に送信し、動作９３４において、セキュアサーバ９１２は、そのＴＣＰｏｖｅｒ ＴＬＳによるＳＭＳトラフィックを受信する。次に、セキュアサーバ９１２は、ＴＬＳ復号化を実行してそのＳＭＳメッセージを読み取り、それに応じた動作、例えば、そのＳＭＳメッセージを受信者に向けて転送し、その受信者からＳＭＳレスポンスを受信し得る。そして、セキュアサーバ９１２は、ＴＬＳを使用してＳＭＳレスポンスを暗号化し、ＴＣＰｏｖｅｒ ＴＬＳによるＳＭＳレスポンスのトラフィックを形成し得る。そのＴＣＰｏｖｅｒ ＴＬＳによるＳＭＳレスポンスが動作９３６において送信され、動作９３８においてＭＳＯＬ９０６で受信される。次に、ＭＳＯＬ９０６は、動作９４０においてＴＣＰｏｖｅｒ ＴＬＳによるＳＭＳトラフィックを復号化し、動作９４２において、その復号化によって得られたＳＭＳレスポンスをモバイルネットワーク９０４に送信する。そして、動作９４４において、モバイルネットワーク９０４は、そのＳＭＳレスポンスをＭＤ９０２に転送する。

【００５４】

図１０は、例示的な実施形態による、音声呼上でセッション・イニシエーション・プロトコル・オーバーＴＬＳ（ＳＩＰＳ）／セキュア・リアルタイム・プロトコル（ＳＲＴＰ）暗号化を行う方法１０００を示す相互作用図である。この方法１０００は、モバイルデバイス（ＭＤ）１００２と、ＭＤ１００２が接続されたモバイルネットワーク１００４と、ＭＳＯＬ１００６と、セキュリティプロファイルディレクトリ（ＳＰＤ）１００８と、インターネット１０１０と、セキュアサーバ１０１２とを利用する。動作１０１４において、システム番号に対する音声呼がモバイルデバイス１００２からモバイルネットワーク１００４に向けて開始され、動作１０１６において、その音声呼がＭＳＯＬ１００６に転送される。動作１０１８において、ＭＳＯＬ１００６は、デバイスプロファイルをＳＰＤ１００８に要求する。この動作は、ＩＭＳＩなどのＭＤ１００２の固有識別子を識別することを含み得る。そして、動作１０２０において、ＳＰＤ１００８は、ＳＴＲＰ暗号化プロファイルを返す。ＳＴＲＰ暗号化プロファイルは、ＩＭＳＩなどの固有識別子によって識別されるＭＤ１００２に対応するものであり得る。動作１０２２において、ＭＳＯＬ１００６は、セキュアサーバ１０１２へのＳＩＰインビテーションを開始し、動作１０２４において、このＳＩＰインビテーションが、インターネット１０１０を介してセキュアサーバ１０１２によって受信される。このＳＩＰインビテーションは暗号化されていてもよ

い。動作１０２６において、セキュアサーバ１０１２は、ＳＩＰレスポンス２００ＯＫメッセージをＭＳＯＬ１００６に送信し得る。そして、動作１０２８において、このＳＩＰレスポンス２００ＯＫメッセージが、インターネット１０１０を介してＭＳＯＬ１００６によって受信される。

【００５５】

動作１０３０において、ＭＳＯＬ１００６は、ＳＲＴＰ暗号化プロファイルを使用して音声呼を暗号化し、ＳＲＴＰトラフィックを形成する。動作１０３２において、ＭＳＯＬ１００６は、このＳＲＴＰトラフィックをセキュアサーバ１０１２に向けてインターネット１０１０に送信し、動作１０３４において、セキュアサーバ１０１２は、そのＳＲＴＰトラフィックを受信する。次に、セキュアサーバ１０１２は、ＳＲＴＰ復号化を実行して音声呼を受信し、それに応じた動作、例えば、その音声呼を受信者に向けて転送し、その受信者から音声呼レスポンスを受信し得る。そして、セキュアサーバ１０１２は、ＳＲＴＰを使用してその音声呼レスポンスを暗号化し、ＳＲＴＰレスポンスのトラフィックを形成し得る。そして、そのＳＲＴＰレスポンスのトラフィックが動作１０３６において送信され、動作１０３８においてＭＳＯＬ１００６で受信される。次に、ＭＳＯＬ１００６は、動作１０４０においてＳＲＴＰトラフィックを復号化し、動作１０４２において、音声呼レスポンスをＴＣＰトラフィックとしてモバイルネットワーク１００４に送信する。そして、動作１０４４において、モバイルネットワーク１００４は、そのＴＣＰトラフィックをＭＤ１００２に転送する。

【００５６】

モバイルデバイス１００２は、リモートサーバ、クラウドサービス、または他のリモートサービスにサインインする必要があり得る。サインインするためには、デバイスがクラウドサーバに接続して、所定のユーザ名またはデバイス識別情報、場合によってはパスワードを使用するサインイン処理が発生する。しかしながら、識別情報およびパスワードはデバイス自体に記憶されているため、サインイン処理は非常に安全ではなく、この情報を使用してそのデバイスになりすましてリモートサーバにハッキングするハッカーによってそれらが取得される可能性がある。例示的な実施形態では、「ネットワークベースのトラストアンカー」の概念が導入される。ネットワークベースのトラストアンカーは、セキュアサーバ１０１２が確かめることができるＭＳＯＬ１００６のいくつかの特徴であって、モバイルデバイス１００２が誰であると主張しているのかを意味する。例示的な実施形態では、モバイルデバイス１００２は、ＳＩＭカードを使用してモバイルネットワークに対して認証する。そして、ＭＳＯＬ１００６は、確かに実際のデバイスであることを確認するために、デバイスのログインを実行するかまたはログインに認証情報を追加し得る。モバイルデバイス１００２がログインを実行しようとする際には、モバイルデバイス１００２がＭＳＯＬ１００６にログインの要求を送信するか、またはネットワークがその要求をインターセプトしてＭＳＯＬ１００６にルーティングする。そして、ＭＳＯＬ１００６は、その要求がモバイルネットワーク１００４を介して実際の認証されたモバイルデバイス１００２から来たものであることを識別して、ログインを実行するかまたはログインに追加の認証情報を追加することにより、セキュサーバ１０１２は、そのログインが想定されていたデバイスから来たものであるという完全に肯定的な認識を得ることができる。このような認証情報は、認証の有効性を強化するためにセキュアサーバ１０１２と予め共有されてもよい。

【００５７】

図１１は、例示的な実施形態による、ネットワーク認証情報をログイン処理に追加するＭＳＯＬを示す相互作用図である。この方法１１００は、モバイルデバイス（ＭＤ）１１０２と、ＭＤ１１０２が接続されたモバイルネットワーク１１０４と、ＭＳＯＬ１１０６と、セキュリティプロファイルディレクトリ（ＳＰＤ）１１０８と、インターネット１１１０と、セキュアサーバ１１１２とを利用する。動作１１１４において、ＭＤ１１０２上でログイン処理が開始される。動作１１１６において、モバイルネットワーク１１０４は、このログイン処理の開始を受信し、それをＭＳＯＬ１１０６にルーティングまたは再ル

ーティングする。動作１１１８において、ＭＳＯＬ１１０６はＳＰＤ１１０８にアクセスすることによってデバイスを認証し、動作１１２０において、ＳＰＤ１１０８は認証情報を返す。そして、動作１１２２において、ログイン処理が、そのログイン処理に追加された認証情報を用いてこのＭＳＯＬ１１０６によって開始される。動作１１２４において、セキュアサーバ１１１２は、認証情報を有するログイン処理を受信すると、その認証情報を使用してモバイルデバイス１１０２にログインする。動作１１２６において、セキュアサーバ１１１２はログイン成功メッセージを送信し、動作１１２８において、このログイン成功メッセージがＭＳＯＬ１１０６によって受信される。そして、動作１１３０において、ＭＳＯＬ１１０６は、このログイン成功メッセージをＭＤ１１０２に向けて送信し、動作１１３２において、ＭＤ１１０２は、そのログイン成功メッセージを受信する。

【００５８】

図１２は、例示的な実施形態による、ネットワーク認証情報をログイン処理に追加することが可能なＭＳＯＬ１２００を示すブロック図である。ＭＳＯＬ１２００は、モバイルデバイス識別コンポーネント１２０２を含み得る。このモバイルデバイス識別コンポーネント１２０２は、セキュアサーバ１１１２に向けてログイン処理の要求（ＭＳＯＬ１２００によってインターセプトされる）を送信したモバイルデバイス１１０２を識別するように動作する。この識別情報の一部には、ＩＭＳＩＡなどの、モバイルデバイス１１０２のネットワーク識別情報が含まれ得る。セキュリティプロファイルディレクトリインタフェース１２０４は、その識別情報をセキュリティプロファイルディレクトリ２０４に渡す。このセキュリティプロファイルディレクトリ２０４は、その識別情報に基づいて認証情報を作成し、その認証情報をＭＳＯＬ１２００に返信するように動作する。次に、認証情報追加コンポーネント１２０６は、その認証情報をログイン処理の要求に追加して、ログイン処理を開始する。次に、パケット交換ネットワークインタフェース１２０８は、パケット交換ネットワークを介してセキュアサーバ１１１２にログイン処理の開始要求をルーティングする。

【００５９】

ＭＳＯＬ１２００およびＭＳＯＬ２０２は、別々のコンポーネントであってもよく、またはいくつかの実施形態では、そのすべての機能を実行するＭＳＯＬ２０２やＭＳＯＬ１２００内のすべてのコンポーネントを有する一体化したＭＳＯＬであってもよい。

【００６０】

［モジュール、コンポーネント、およびロジック］

本明細書において、特定の実施形態は、ロジックまたは多数のコンポーネント、モジュール、またはメカニズムを含むものとして記載される。モジュールは、ソフトウェアモジュール（例えば、機械可読媒体上に具現化されたコード）またはハードウェアモジュールのいずれかに相当し得る。「ハードウェアモジュール」は、特定の動作を実行可能な有形のユニットであり、特定の物理的方法で構成または配置され得る。種々の例示的な実施形態では、１つまたは複数のコンピュータシステム（例えば、スタンドアロンコンピュータシステム、クライアントコンピュータシステム、またはサーバコンピュータシステム）またはコンピュータシステムの１つまたは複数のハードウェアモジュール（例えば、プロセッサまたはプロセッサ群）は、本明細書で説明される特定の動作を実行するように動作するハードウェアモジュールとしてソフトウェア（例えば、アプリケーション３１０またはアプリケーション部分）によって構成され得る。

【００６１】

いくつかの実施形態では、ハードウェアモジュールは、機械的に、電子的に、またはそれらの任意の適切な組み合わせで実装され得る。例えば、ハードウェアモジュールは、特定の動作を実行するように恒久的に構成された専用の回路またはロジックを含み得る。例えば、ハードウェアモジュールは、フィールドプログラマブルゲートアレイ（ＦＰＧＡ）または特定用途向け集積回路（ＡＳＩＣ）などの専用プロセッサとすることができる。また、ハードウェアモジュールは、特定の動作を実行するべくソフトウェアによって一時的に構成されたプログラマブルロジックまたは回路を含み得る。例えば、ハードウェアモジ

ュールは、汎用プロセッサまたは他のプログラマブルプロセッサによって実行されるソフトウェアを含み得る。このようなソフトウェアによって構成されると、ハードウェアモジュールは、構成された機能を実行するべく固有に調整された特定のマシン（またはマシンの特定のコンポーネント）となり、汎用プロセッサではなくなる。専用化されかつ恒久的に構成された回路か、または一時的に構成された回路（例えば、ソフトウェアによって構成された回路）にてハードウェアモジュールを機械的に実装する決定はコストおよび時間を考慮して推進され得る。

【００６２】

したがって、「ハードウェアモジュール」という用語は、有形のエンティティであって、物理的に構成されているか、恒久的に構成されている（例えば、ハードウェアに組み込まれている）か、あるいは特定の方法で動作するようにまたは本明細書に記載の特定の動作を実行するように一時的に構成されている（例えば、プログラムされている）エンティティを包含するものと理解され得る。本明細書で使用する「ハードウェア実装モジュール」は、ハードウェアモジュールを指す。ハードウェアモジュールが一時的に構成される（例えば、プログラムされる）実施形態を考慮して、各ハードウェアモジュールが任意のある時点で構成またはインスタンス化される必要はない。例えば、ハードウェアモジュールが、専用プロセッサとなるようにソフトウェアによって構成された汎用プロセッサを含む場合、その汎用プロセッサは、異なる時間にそれぞれ異なる専用プロセッサ（例えば、異なるハードウェアモジュールを含む）として構成されてもよい。したがって、ソフトウェアは、特定のプロセッサまたはプロセッサ群を構成して、例えば、ある時間にはある特定のハードウェアモジュールを構築するとともに、異なる時間には異なるハードウェアモジュールを構築する。

【００６３】

ハードウェアモジュールは、他のハードウェアモジュールに情報を供給するとともに、他のハードウェアモジュールから情報を受信することができる。したがって、記載された複数のハードウェアモジュールは通信可能に結合されているとみなすことができる。複数のハードウェアモジュールが同時に存在する場合、その複数のハードウェアモジュールのうちの２つ以上の間の信号伝送によって（例えば、適切な回路およびバスを介して）通信が実現され得る。複数のハードウェアモジュールが異なる時間に構成またはインスタンス化される実施形態では、そのようなハードウェアモジュール間の通信は、例えば、それら複数のハードウェアモジュールがアクセスするメモリ構造内の情報の記憶と取得を通じて実現され得る。例えば、１つのハードウェアモジュールは、動作を実行して、その動作の出力をそのハードウェアモジュールと通信可能に結合されたメモリデバイス内に記憶することができる。その後、さらなるハードウェアモジュールは、メモリデバイスにアクセスして、その記憶された出力を取得して処理することができる。また、ハードウェアモジュールは、入力デバイスまたは出力デバイスとの通信を開始して、リソース（例えば、情報の集合）上で動作することもできる。

【００６４】

本明細書に記載される例示的方法の種々の動作は、関連する動作を実行するように一時的に構成される（例えば、ソフトウェアによって）かまたは恒久的に構成される１つまたは複数のプロセッサによって少なくとも部分的に実行され得る。一時的に構成されているかまたは恒久的に構成されているかによらず、このようなプロセッサは、本明細書に記載される１つまたは複数の動作または機能を実行するように動作するプロセッサ実装モジュールを構成し得る。本明細書で使用される「プロセッサ実装モジュール」は、１つまたは複数のプロセッサを使用して実装されるハードウェアモジュールを指す。

【００６５】

同様に、本明細書に記載される方法は、ハードウェアの一例である特定のプロセッサまたはプロセッサ群を用いて、少なくとも部分的にプロセッサ実装され得る。例えば、方法の動作の少なくとも一部は、１つまたは複数のプロセッサまたはプロセッサ実装モジュールによって実行され得る。さらに、１つまたは複数のプロセッサは、「クラウドコンピュ

ーティング」環境において、または「サービスとしてのソフトウェア」（ＳａａＳ）として、関連動作の性能をサポートするように動作し得る。例えば、動作の少なくともいくつかは、ネットワーク（例えば、インターネット１１１０）および１つまたは複数の適切なインタフェース（例えば、アプリケーションプログラムインタフェース（ＡＰＩ））を介してアクセス可能な一群のコンピュータによって（例えばプロセッサを含むマシンとして）実行され得る。

【００６６】

特定の動作の性能は、単一のマシン内に備えられているだけでなく、複数のマシンにわたって配備されて、プロセッサ間で分散されてもよい。いくつかの例示的な実施形態では、プロセッサまたはプロセッサ実装モジュールは、単一の地理的位置（例えば、家庭環境、オフィス環境、またはサーバファーム内）に配置されてもよい。他の例示的な実施形態では、プロセッサまたはプロセッサ実装モジュールは、複数の地理的位置にわたって分散されてもよい。

【００６７】

［マシンおよびソフトウェアアーキテクチャ］

図１～１２に関連して説明したモジュール、方法、アプリケーション３１０などは、いくつかの実施形態では、マシンおよび関連するソフトウェアアーキテクチャの文脈で実装される。以下の節では、開示された実施形態での使用に適した代表的なソフトウェアアーキテクチャおよびマシン（例えば、ハードウェア）アーキテクチャを説明する。

【００６８】

ソフトウェアアーキテクチャは、特定の目的に合わせて調整されたデバイスおよびマシンを作成するためにハードウェアアーキテクチャと共に使用される。例えば、特定のソフトウェアアーキテクチャと結合された特定のハードウェアアーキテクチャは、携帯電話やタブレットデバイスなどのモバイルデバイス１１０２を形成する。わずかに異なるハードウェアおよびソフトウェアアーキテクチャは「モノのインターネット」で使用するためのスマートデバイスをもたらす一方、別の組み合わせはクラウドコンピューティングアーキテクチャ内で使用するためのサーバコンピュータを生成する。当業者は、本明細書に含まれる開示と異なる文脈で本発明の主題を実施する方法を容易に理解できるため、このようなソフトウェアおよびハードウェアアーキテクチャのすべての組み合わせはここでは提示されていない。

【００６９】

［ソフトウェアアーキテクチャ］

図１３は、本明細書に記載の種々のハードウェアアーキテクチャとともに使用可能な代表的なソフトウェアアーキテクチャ１３０２を示すブロック図１３００である。図１３はソフトウェアアーキテクチャ１３０２の非限定的な例に過ぎず、本明細書に記載の機能を容易にするために多くの他のアーキテクチャが実装可能であることが理解され得る。ソフトウェアアーキテクチャ１３０２は、図１４のマシン１４００などのハードウェア上において実行され得る。マシン１４００は、とりわけ、プロセッサ１４１０、メモリ／ストレージ１４３０、およびＩ／Ｏコンポーネント１４５０を含む。代表的なハードウェア層１３０４が示されており、このハードウェア層１３０４は、例えば、図１４のマシン１４００を表すことができる。代表的なハードウェア層１３０４は、関連する実行可能命令１３０８を有する１つまたは複数の処理ユニット１３０６を含む。実行可能命令１３０８は、図１～図１２の方法やモジュールなどの実装を含むソフトウェアアーキテクチャ１３０２の実行可能命令を表す。また、ハードウェア層１３０４はメモリおよび／またはストレージモジュール１３１０を含み、このモジュール１３１０も実行可能命令１３０８を有する。ハードウェア層１３０４は、他のハードウェア１３１２も含み、このハードウェア１３１２は、マシン１４００の一部として図示されている他のハードウェアなどのハードウェア層１３０４の任意の他のハードウェアを表す。

【００７０】

図１３の例示的なアーキテクチャにおいて、ソフトウェアアーキテクチャ１３０２は、

各層が特定の機能を提供するレイヤスタックとして概念化され得る。例えば、ソフトウェアアーキテクチャ１３０２は、オペレーティングシステム１３１４、ライブラリ１３１６、フレームワーク／ミドルウェア１３１８、アプリケーション１３２０、およびプレゼンテーション層１３４４などのレイヤを含むことができる。動作上、レイヤ内のアプリケーション１３２０および／または他のコンポーネントは、ソフトウェアスタックを介してアプリケーションプログラミングインタフェース（ＡＰＩ）コール１３２４を呼び出し、そのＡＰＩコール１３２４に応答して、メッセージ１３２６として示されるレスポンスや戻り値などを受け取ることができる。図示されたレイヤは本質的に代表的なものであり、すべてのソフトウェアアーキテクチャがすべてのレイヤを有しているわけではない。例えば、いくつかのモバイルまたは専用のオペレーティングシステム１３１４は、フレームワーク／ミドルウェア１３１８を提供し得ないが、他のものはそのようなレイヤを提供し得る。他のソフトウェアアーキテクチャは、追加のレイヤまたは異なるレイヤを含み得る。

【００７１】

オペレーティングシステム１３１４は、ハードウェアリソースを管理し、共通のサービスを提供し得る。オペレーティングシステム１３１４は、例えば、カーネル１３２８、サービス１３３０、およびドライバ１３３２を含み得る。カーネル１３２８は、ハードウェア層と他のソフトウェア層との間の抽象レイヤとして機能し得る。例えば、カーネル１３２８は、メモリ管理、プロセッサ管理（例えば、スケジューリング）、コンポーネント管理、ネットワーキング、セキュリティ設定などを行い得る。サービス１３３０は、他のソフトウェア層のための他の共通サービスを提供し得る。ドライバ１３３２は、基礎とするハードウェアを制御またはインタフェースする役割を果たし得る。例えば、ドライバ１３３２は、ディスプレイドライバ、カメラドライバ、Ｂｌｕｅｔｏｏｔｈ（登録商標）ドライバ、フラッシュメモリドライバ、シリアル通信ドライバ（例えば、ユニバーサルシリアルバス（ＵＳＢ）ドライバ）、Ｗｉ－Ｆｉ（登録商標）ドライバ、オーディオドライバ、電力管理ドライバなどをハードウェア構成に依存して含み得る。

【００７２】

ライブラリ１３１６は、アプリケーション１３２０および／または他のコンポーネントおよび／またはレイヤによって利用され得る共通のインフラストラクチャを提供し得る。ライブラリ１３１６は典型的には、他のソフトウェアモジュールが、基礎とするオペレーティングシステム１３１４の機能（例えば、カーネル１３２８、サービス１３３０、および／またはドライバ１３３２）と直接的にインタフェースするよりも簡易な方法でタスクを実行可能とする機能を提供する。ライブラリ１３１６は、メモリ割り当て関数、文字列操作関数、数学関数などの関数を提供し得るシステムライブラリ１３３４（例えば、Ｃ標準ライブラリ）を含み得る。また、ライブラリ１３１６は、メディアライブラリ（例えば、ＭＰＥＧ４、Ｈ．２６４、ＭＰ３、ＡＡＣ、ＡＭＲ、ＪＰＧ、ＰＮＧなどの種々のメディアフォーマットの提示および操作をサポートするライブラリ）、グラフィックスライブラリ（例えば、ディスプレイ上のグラフィックコンテンツに２Ｄおよび３Ｄをレンダリングするために使用され得るＯｐｅｎＧＬフレームワーク）、データベースライブラリ（例えば、種々のリレーショナルデータベース機能を提供し得るＳＱＬｉｔｅ）、ウェブライブラリ（例えば、ウェブブラウジング機能を提供し得るＷｅｂＫｉｔ）などのＡＰＩライブラリ１３３６を含み得る。また、ライブラリ１３１６は、アプリケーション１３２０および他のソフトウェアコンポーネント／モジュールに多くの他のＡＰＩを提供するための多種多様な他のライブラリ１３３８を含み得る。

【００７３】

フレームワーク／ミドルウェア１３１８（ミドルウェアと呼ぶ場合もある）は、アプリケーション１３２０および／または他のソフトウェアコンポーネント／モジュールによって利用され得るより高いレベルの共通インフラストラクチャを提供し得る。例えば、フレームワーク／ミドルウェア１３１８は、種々のグラフィックユーザインタフェース（ＧＵＩ）機能、高レベルのリソース管理、高レベルの位置サービスなどを提供し得る。フレームワーク／ミドルウェア１３１８は、アプリケーション１３２０および／または他のソフ

トウェアコンポーネント／モジュールによって利用され得る広範囲な他のＡＰＩを提供することができ、そのいくつかは特定のオペレーティングシステム１３１４またはプラットフォームに固有とすることができる。

【００７４】

アプリケーション１３２０は、内蔵アプリケーション１３４０および／または第三者アプリケーション１３４２を含む。代表的なビルトインアプリケーション１３４０は例えば、連絡先アプリケーション、ブラウザアプリケーション、ブックリーダーアプリケーション、位置アプリケーション、メディアアプリケーション、メッセージングアプリケーション、および／またはゲームアプリケーションを含み得るが、これらに限定されない。第三者アプリケーション１３４２は、任意の内蔵アプリケーション１３４０および多種多様の他のアプリケーションを含み得る。特定の例では、第三者アプリケーション１３４２（例えば、特定のプラットフォームのベンダー以外のエンティティによってＡｎｄｒｏｉｄ（商標）またはｉＯＳ（商標）ソフトウェア開発キット（ＳＤＫ）を使用して開発されたアプリケーション）は、ｉＯＳ（商標）、Ａｎｄｒｏｉｄ（商標）、Ｗｉｎｄｏｗｓ（登録商標）フォンなどのモバイルオペレーティングシステム１３１４上、または他のモバイルオペレーティングシステム１３１４上で実行するモバイルソフトウェアとすることができる。この例では、第三者アプリケーション１３４２は、オペレーティングシステム１３１４などのモバイルオペレーティングシステムによって提供されるＡＰＩコール１３２４を呼び出すことで、本明細書に記載の機能を容易化することができる。

【００７５】

アプリケーション１３２０は、内蔵オペレーティングシステム機能（例えば、カーネル１３２８、サービス１３３０、および／またはドライバ１３３２）、ライブラリ（例えば、システムライブラリ１３３４、ＡＰＩライブラリ１３３６、およびその他のライブラリ１３３８）、フレームワーク／ミドルウェア１３１８を利用することで、システムのユーザと対話するためのユーザインタフェースを作成することができる。代替的または追加的に、いくつかのシステムでは、ユーザとの対話は、プレゼンテーション層（プレゼンテーション層１３４４など）を介して行われてもよい。これらのシステムでは、アプリケーション／モジュールの「ロジック」は、ユーザと対話するアプリケーション／モジュールの側面からは分離され得る。

【００７６】

いくつかのソフトウェアアーキテクチャは、仮想マシンを利用する。図１３の例では、これは仮想マシン１３４８によって示されている。仮想マシン１３４８は、アプリケーション／モジュールがあたかもハードウェアマシン（例えば、図１４のマシン１４００など）上で実行しているかのように実行可能なソフトウェア環境を形成する。仮想マシン１３４８は、ホストオペレーティングシステム（図１３のオペレーティングシステム１３１４）によってホストされ、必ずしもそうではないが典型的には、仮想マシン１３４８の動作に加えてホストオペレーティングシステム（すなわち、オペレーティングシステム１３１４）とのインタフェースを管理する仮想マシンモニタ１３４６を有する。ソフトウェアアーキテクチャは、オペレーティングシステム１３５０、ライブラリ１３５２、フレームワーク／ミドルウェア１３５４、アプリケーション１３５６、および／またはプレゼンテーション層１３５８などの仮想マシン１３４８内で実行される。仮想マシン１３４８内で実行されるソフトウェアアーキテクチャのこれらの層は、上述した対応する層と同じであってもよいし、異なっていてもよい。

【００７７】

［例示的なマシンアーキテクチャおよび機械可読媒体］

図１４は、機械可読媒体（例えば、機械可読記憶媒体）から命令１４１６を読み込み本明細書に記載の方法のうちの任意の１つ以上を実行可能な、いくつかの例示的な実施形態によるマシン１４００の構成要素を示すブロック図である。具体的に、図１４は、コンピュータシステムの例示的な形態によるマシン１４００の概略図を示し、同図における命令１４１６（例えば、ソフトウェア、プログラム、アプリケーション１３５６、アプレット

、アプリケーション、または他の実行可能コード）は、上述したエンドポイント（例えば、モバイルデバイス１１０２や、外部ネットワーク内のデバイス）に対して上述した方法をマシン１４００による実行可能とする。命令１４１６は、プログラムされていない一般的なマシン１４００を、説明および図示した機能を説明した方法で実行するようにプログラムされた特定のマシンに変換する。代替の実施形態では、マシン１４００は、スタンドアロン装置として動作するか、または他のマシンに結合（例えば、ネットワーク接続）されてもよい。ネットワーク展開の場合、マシン１４００は、サーバ・クライアントネットワーク環境内のサーバマシンまたはクライアントマシンの能力で動作し得るか、またはピアツーピア（または分散型）ネットワーク環境内のピアマシンとして動作し得る。マシン１４００は、サーバコンピュータ、クライアントコンピュータ、パーソナルコンピュータ（ＰＣ）、タブレットコンピュータ、ラップトップコンピュータ、ネットブック、セットトップボックス（ＳＴＢ）、パーソナルデジタルアシスタント（ＰＤＡ）、環境メディアシステム、携帯電話、スマートフォン、モバイルデバイス１１０２、ウェアラブルデバイス（例えば、スマートウォッチ）、スマートホームデバイス（例えば、スマート電化製品）、他のスマートデバイス、ウェブ電化製品、ネットワークルータ、ネットワークスイッチ、ネットワークブリッジ、または、命令１４１６を順番に実行可能なもしくはマシン１４００が実行すべき動作を指定する命令１４１６を実行可能な任意のマシン１４００を含み得るが、これらに限定されない。さらに、単一のマシン１４００のみが示されているが、「マシン」という用語は、本明細書に記載の方法のうちの１つ以上を実行するための命令１４１６を個別にまたは共に実行するマシン１４００の集合を含むと解釈され得る。

【００７８】

マシン１４００は、プロセッサ１４１０、メモリ／ストレージ１４３０、およびＩ／Ｏコンポーネント１４５０を含み得る。これらは、バス１４０２などを介して互いに通信するように構成され得る。例示的な実施形態では、プロセッサ１４１０（例えば、中央処理装置（ＣＰＵ）、縮小命令セット演算（ＲＩＳＣ）プロセッサ、複合命令セット演算（ＣＩＳＣ）プロセッサ、グラフィックス処理装置（ＧＰＵ）、デジタル信号プロセッサ（ＤＳＰ）、特定用途向け集積回路（ＡＳＩＣ）、無線周波数集積回路（ＲＦＩＣ）、別のプロセッサ、またはそれらの任意の適切な組み合わせ）は、例えば、命令１４１６を実行可能なプロセッサ１４１２およびプロセッサ１４１４を含み得る。「プロセッサ」という用語は、命令１４１６を同時に実行可能な２つ以上の独立したプロセッサ１４１２，１４１４（「コア」と呼ぶ場合もある）を含み得るマルチコアプロセッサ１４１２，１４１４を含むことを意図している。図１４は複数のプロセッサ１４１０を示しているが、マシン１４００は、単一コアを備える単一プロセッサ１４１２，１４１４、マルチコアを備える単一プロセッサ１４１２，１４１４（例えば、マルチコアプロセッサ１４１２，１４１４）、単一コアを備えるマルチプロセッサ１４１２，１４１４、マルチコアを備えるマルチプロセッサ１４１２，１４１４、またはそれらの任意の組み合わせを含み得る。

【００７９】

メモリ／ストレージ１４３０は、メインメモリまたは他のメモリストレージなどのメモリ１４３２と、ストレージユニット１４３６とを含み得る。これらは双方ともにバス１４０２などを介してプロセッサ１４１０にアクセス可能である。ストレージユニット１４３６およびメモリ１４３２は、本明細書に記載の方法または機能のうちの任意の１つ以上を具現化する命令１４１６を記憶する。命令１４１６は、マシン１４００によるその実行中において、メモリ１４３２内、ストレージユニット１４３６内、プロセッサ１４１０の少なくとも１つの内部（例えば、プロセッサ１４１２，１４１４のキャッシュメモリ内）、またはそれらの任意の適切な組み合わせ内に、完全にまたは部分的に存在し得る。したがって、メモリ１４３２、ストレージユニット１４３６、およびプロセッサ１４１０のメモリは、機械可読媒体の例である。

【００８０】

本明細書で使用される場合、「機械可読媒体」は、命令１４１６およびデータを一時的または恒久的に記憶可能な装置を意味し、ランダムアクセスメモリ（ＲＡＭ）、リードオ

ンリーメモリ（ＲＯＭ）、バッファメモリ、フラッシュメモリ、光学媒体、磁気媒体、キャッシュメモリ、他のタイプの記憶装置（例えば、消去可能なプログラム可能リードオンリーメモリ（ＥＥＰＲＯＭ））、および／またはそれらの任意の適切な組み合わせを含み得るが、これらに限定されない。「機械可読媒体」という用語は、命令１４１６を記憶可能な単一の媒体または複数の媒体（例えば、集中型または分散型データベース、または関連するキャッシュおよびサーバ）を含むと解釈されるべきである。また、「機械可読媒体」という用語は、マシン（例えば、マシン１４００）による実行のための命令（例えば、命令１４１６）を記憶または伝送可能な任意の媒体または複数の媒体の組み合わせを含み、マシン１４００の１つまたは複数のプロセッサ（例えば、プロセッサ１４１０）によって命令１４１６が実行されると、命令１４１６は、本明細書に記載の方法のうちの１つ以上をマシン１４００により実行させるものであると解釈されるべきである。したがって、「機械可読媒体」とは、単一のストレージ装置またはデバイスだけでなく、複数のストレージ装置またはデバイスを含む「クラウドベース」のストレージシステムまたはストレージネットワークも指す。

【００８１】

Ｉ／Ｏコンポーネント１４５０は、入力を受信し、出力を提供し、出力を生成し、情報を送信し、情報を交換し、測定結果を取得するなどの多種多様なコンポーネントを含み得る。特定のマシンに含まれる特定のＩ／Ｏコンポーネント１４５０は、マシン１４００のタイプに依存し得る。例えば、携帯電話などのポータブルマシンは、タッチ入力デバイスまたは他のそのような入力機構を含む可能性が高いが、ヘッドレスサーバマシンは、そのようなタッチ入力デバイスを含まない可能性が高い。Ｉ／Ｏコンポーネント１４５０は、図１４には示されていない多くの他のコンポーネントを含み得ることが理解され得る。Ｉ／Ｏコンポーネント１４５０は機能に従ってグループ分けされており、以下の説明を単に簡単にするためのものであり、このグループ分けは決して限定的ではない。種々の例示的な実施形態では、Ｉ／Ｏコンポーネント１４５０は、出力コンポーネント１４５２および入力コンポーネント１４５４を含み得る。出力コンポーネント１４５２は、視覚コンポーネント（例えば、プラズマディスプレイパネル（ＰＤＰ）、発光ダイオード（ＬＥＤ）ディスプレイ、液晶ディスプレイ（ＬＣＤ）、プロジェクタ、または陰極線管（ＣＲＴ）などのディスプレイ）、音響コンポーネント（例えば、スピーカー）、触覚コンポーネント（例えば、振動モータ、抵抗機構）、他の信号発生器などを含み得る。入力コンポーネント１４５４は、英数字入力コンポーネント（例えば、キーボード、英数字入力を受け取るように構成されたタッチスクリーン、光学キーボード、または他の英数字入力コンポーネント）、ポイント式の入力コンポーネント（例えば、マウス、タッチパッド、トラックボール、ジョイスティック、モーションセンサ、または他のポインティング機器）、触覚入力コンポーネント（例えば、物理的ボタン、タッチまたはタッチジェスチャの位置および／または力を提供するタッチスクリーン、または他の触覚入力コンポーネント）、オーディオ入力コンポーネント（例えば、マイクロフォン）などを含み得る。

【００８２】

さらなる例示的な実施形態では、Ｉ／Ｏコンポーネント１４５０は、多様なコンポーネントのうち、バイオメトリックコンポーネント１４５６、モーションコンポーネント１４５８、環境コンポーネント１４６０、または位置コンポーネント１４６２を含み得る。例えば、バイオメトリックコンポーネント１４５６は、表現（例えば、手による表現、顔による表現、声による表現、身体のジェスチャ、または目の追跡）の検出、生体信号（例えば、血圧、心拍数、体温、汗、または脳波）の測定、人の識別（例えば、音声識別、網膜識別、顔識別、指紋識別、または脳波に基づく識別）などを行うためのコンポーネントを含み得る。モーションコンポーネント１４５８は、加速度センサコンポーネント（例えば、加速度計）、重力センサコンポーネント、回転センサコンポーネント（例えば、ジャイロスコープ）などを含み得る。環境コンポーネント１４６０は、例えば、照明センサコンポーネント（例えば、光度計）、温度センサコンポーネント（例えば、周囲温度を検出する１つまたは複数の温度計）、湿度センサコンポーネント、圧力センサコンポーネント（

例えば、気圧計）、音響センサコンポーネント（例えば、背景雑音を検出する１つまたは複数のマイクロフォン）、近接センサコンポーネント（例えば、近くの物体を検出する赤外線センサ）、ガスセンサ（例えば、安全のために有害ガスの濃度を検出したり大気の汚染を検出したりするためのガス検出センサ）、または周囲の物理的環境に対応する示唆、測定結果、または信号を提供可能な他のコンポーネントを含み得る。位置コンポーネント１４６２は、位置センサコンポーネント（例えば、全地球測位システム（ＧＰＳ）受信機コンポーネント）、高度センサコンポーネント（例えば、高度を導出可能な空気圧を検出する高度計または気圧計）、方向センサコンポーネント（例えば、磁力計）などを含み得る。

【００８３】

通信は、広範囲の技術を使用して実装され得る。Ｉ／Ｏコンポーネント１４５０は、マシン１４００をネットワーク１４８０またはデバイス１４７０にそれぞれカップリング１４８２，１４７２を介して結合するように動作可能な通信コンポーネント１４６４を含み得る。例えば、通信コンポーネント１４６４は、ネットワークインタフェースコンポーネントまたはネットワーク１４８０とのインタフェースを行う他の適切なデバイスを含み得る。さらなる例において、通信コンポーネント１４６４は、有線通信コンポーネント、無線通信コンポーネント、セルラー通信コンポーネント、近距離通信（ＮＦＣ）コンポーネント、Ｂｌｕｅｔｏｏｔｈ（登録商標）コンポーネント（例えば、Ｂｌｕｅｔｏｏｔｈ（登録商標）Ｌｏｗ　Ｅｎｅｒｇｙ）、Ｗｉ－Ｆｉ（登録商標）コンポーネント、および他の手法を介して通信を提供する他の通信コンポーネントを含み得る。デバイス１４７０は、別のマシンまたは多種多様な周辺デバイス（例えば、ユニバーサルシリアルバス（ＵＳＢ）を介して結合された周辺デバイス）のうちの任意のものとすることができる。

【００８４】

さらに、通信コンポーネント１４６４は識別子を検出してもよく、識別子を検出するように動作可能なコンポーネントを含んでもよい。例えば、通信コンポーネント１４６４は、無線周波数識別（ＲＦＩＤ）タグリーダーコンポーネント、ＮＦＣスマートタグ検出コンポーネント、光学リーダーコンポーネント（例えば、ユニバーサルプロダクトコード（ＵＰＣ）バーコードなどの１次元バーコード、クイックレスポンスコード（ＱＲコード（登録商標））などの多次元バーコード、アズテックコード（ＡｚｔｅｃＣｏｄｅ）、データマトリックス（Ｄａｔａ　Ｍａｔｒｉｘ）、データグリフ（Ｄａｔａｇｌｙｐｈ）、マキシコード（ＭａｘｉＣｏｄｅ）、ＰＤＦ４１７、ウルトラコード（ＵｌｔｒａＣｏｄｅ）、ＵＣＣ　ＲＳＳ－２Ｄバーコード、および他の光学コードなどを検出するための光学センサ）、または音響検出コンポーネント（例えば、タグ付き音響信号を識別するためのマイクロフォン）を含み得る。さらに、インターネットプロトコル（ＩＰ）ジオロケーションによる位置、Ｗｉ－Ｆｉ（登録商標）信号三角測量による位置、ＮＦＣビーコン信号の検出による位置などの特定の位置に種々の情報が通信コンポーネント１４６４を介して配置され得る。

【００８５】

［伝送媒体］

種々の例示的な実施形態では、ネットワーク１４８０の１つまたは複数の部分は、アドホックネットワーク、イントラネット、エクストラネット、仮想プライベートネットワーク（ＶＰＮ）、ローカルエリアネットワーク（ＬＡＮ）、無線ＬＡＮ（ＷＬＡＮ）、広域ネットワーク（ＷＡＮ）、無線ＷＡＮ（ＷＷＡＮ）、メトロポリタンエリアネットワーク（ＭＡＮ）、インターネット１１１０、インターネット１１１０の一部、公衆交換電話網（ＰＳＴＮ）の一部、基本電話サービス（ＰＯＴＳ）ネットワーク、携帯電話ネットワーク、無線ネットワーク、Ｗｉ－Ｆｉ（登録商標）ネットワーク、別の種類のネットワーク、または２つ以上のそのようなネットワークの組み合わせとすることができる。例えば、ネットワーク１４８０またはネットワーク１４８０の一部は、無線またはセルラーネットワークを含むことができ、カップリング１４８２は、符号分割多重アクセス（ＣＤＭＡ）接続、グローバル移動体通信システム（ＧＳＭ（登録商標））接続、または他の種類のセ

ルラーまたは無線カップリングとすることができる。この例では、カップリング１４８２は、シングルキャリア無線伝送技術（１ｘＲＴＴ）、エボリューションデータ最適化（ＥＶＤＯ）技術、汎用パケット無線サービス（ＧＰＲＳ）技術、ＧＳＭエボリューション拡張データレート（ＥＤＧＥ）技術、３Ｇを含む第三世代パートナーシッププロジェクト（３ＧＰＰ）、第四世代無線（４Ｇ）ネットワーク、ユニバーサル移動体通信システム（ＵＭＴＳ）、高速パケットアクセス（ＨＳＰＡ）、マイクロ波アクセス世界規模相互運用性（ＷｉＭＡＸ（登録商標））、ロングタームエボリューション（ＬＴＥ）規格、種々の規格設定組織によって規定された他のもの、他の長距離プロトコル、または他のデータ転送技術など、種々の種類のデータ転送技術のうちのいずれかを実装し得る。

【００８６】

命令１４１６は、ネットワークインタフェースデバイス（例えば、通信コンポーネント１４６４に含まれるネットワークインタフェースコンポーネント）を介した伝送媒体を用いるとともに多数の周知の転送プロトコル（例えば、ハイパーテキスト転送プロトコル（ＨＴＴＰ））を利用したネットワーク１４８０を介して送信または受信され得る。同様に、命令１４１６は、デバイス１４７０へのカップリング１４７２（例えば、ピアツーピア結合）を介した伝送媒体を用いて送信または受信され得る。「伝送媒体」という用語は、マシン１４００により実行するための命令１４１６を記憶、符号化、または伝搬可能な任意の無形媒体を含むと解釈され得るものであり、デジタルまたはアナログ通信信号、またはそのようなソフトウェアの通信を容易化する他の無形媒体を含む。伝送媒体は、機械可読媒体の一実施形態である。

【００８７】

以下に番号を付した実施例は実施形態である。

［１］モバイルセキュリティオフローダ（ＭＳＯＬ）であって、

モバイル無線ネットワーク内のモバイルデバイスから非暗号化データを受信して、前記非暗号化データから前記モバイルデバイスのモバイルデバイス識別情報を決定するように構成されたモバイルデバイス識別コンポーネントと、

前記モバイルデバイス識別情報を使用して、セキュリティプロファイルディレクトリから前記モバイルデバイス識別情報に対応するセキュリティプロファイルを取得するように構成されたセキュリティプロファイルディレクトリインタフェースであって、前記モバイルデバイス識別情報に対応する前記モバイルデバイスからのデータを暗号化するためのセキュリティプロトコルを識別する前記セキュリティプロファイルを取得する前記セキュリティプロファイルディレクトリインタフェースと、

１つまたは複数のプロセッサによって実行可能であり、前記セキュリティプロファイルで識別された前記セキュリティプロトコルを使用して前記非暗号化データを暗号化するように構成された暗号化エンジンと、

前記暗号化されたデータをデータ内で識別されたセキュアサーバにパケット交換ネットワークを介してルーティングするように構成されたパケット交換ネットワークインタフェースと、を備えるＭＳＯＬ。

【００８８】

［２］実施例１のＭＳＯＬにおいて、

前記パケット交換ネットワークインタフェースはさらに、前記セキュアサーバから暗号化されたレスポンスデータを受信するように構成されており、前記暗号化エンジンはさらに、前記セキュリティプロファイルに基づいて前記暗号化されたレスポンスデータを復号化するように構成されている、ＭＳＯＬ。

【００８９】

［３］実施例２のＭＳＯＬにおいて、

前記セキュリティプロファイルディレクトリインタフェースはさらに、前記ＭＳＯＬのキャッシュに前記セキュリティプロファイルを記憶するように構成されている、ＭＳＯＬ。

【００９０】

［４］実施例１または２のＭＳＯＬにおいて、
前記モバイル無線ネットワークは２Ｇ／３Ｇネットワークであり、前記非暗号化データはサービング汎用パケット無線サービス（ＧＰＲＳ）サポートノード（ＳＧＳＮ）を介して受信される、ＭＳＯＬ。
【００９１】
［５］実施例１または２のＭＳＯＬにおいて、
前記モバイル無線ネットワークは４Ｇネットワークであり、前記非暗号化データはサービングゲートウェイ（ＳＧＷ）を介して受信される、ＭＳＯＬ。
【００９２】
［６］実施例１～５のうちのいずれか１つのＭＳＯＬにおいて、
前記セキュリティプロファイルは、複数のモバイルデバイス識別情報の間で共用され、前記複数のモバイルデバイス識別情報を識別するフィールドを含む、ＭＳＯＬ。
【００９３】
［７］実施例１～６のうちのいずれか１つのＭＳＯＬにおいて、
前記セキュリティプロファイルのデータベースは、対応するモバイルデバイスからのデータを暗号化するための異なるセキュリティプロトコルを識別する別のセキュリティプロファイルを含む、ＭＳＯＬ。
【００９４】
［８］方法であって、
モバイルセキュリティオフローダ（ＭＳＯＬ）において、モバイル無線ネットワーク内のモバイルデバイスから非暗号化データを受信すること、
前記非暗号化データから前記モバイルデバイスのモバイルデバイス識別情報を決定すること、
前記モバイルデバイス識別情報を使用して、セキュリティプロファイルディレクトリから前記モバイルデバイス識別情報に対応するセキュリティプロファイルを取得することであって、前記モバイルデバイス識別情報に対応する前記モバイルデバイスからのデータを暗号化するためのセキュリティプロトコルを識別する前記セキュリティプロファイルを取得すること、
前記セキュリティプロファイルで識別された前記セキュリティプロトコルを使用して前記非暗号化データを暗号化すること、
前記暗号化されたデータをデータ内で識別されたセキュアサーバにパケット交換ネットワークを介してルーティングすること、を備える方法。
【００９５】
［９］実施例８の方法において、
前記モバイルデバイス識別情報は国際移動体加入者識別番号（ＩＭＳＩ）である、方法。
【００９６】
［１０］実施例８の方法において、
前記モバイルデバイス識別情報は移動局国際加入者ディレクトリ番号（ＭＳＩＳＤＮ）である、方法。
【００９７】
［１１］実施例８または９の方法において、
前記モバイルデバイス識別情報は電話番号である、方法。
［１２］実施例８～１１のうちのいずれか１つの方法において、
前記セキュアサーバから暗号化されたレスポンスデータを受信すること、
前記セキュリティプロファイルに基づいて前記暗号化されたレスポンスデータを復号化すること、をさらに備える方法。
【００９８】
［１３］実施例１２の方法において、
前記ＭＳＯＬのキャッシュに前記セキュリティプロファイルを記憶することをさらに備

える方法。
【００９９】
［１４］実施例８～１３のうちのいずれか１つの方法において、
前記モバイル無線ネットワークは２Ｇ／３Ｇネットワークであり、前記非暗号化データはサービング汎用パケット無線サービス（ＧＰＲＳ）サポートノード（ＳＧＳＮ）を介して受信される、方法。
【０１００】
［１５］実施例８～１３のうちのいずれか１つの方法において、
前記モバイル無線ネットワークは４Ｇネットワークであり、前記非暗号化データはサービングゲートウェイ（ＳＧＷ）を介して受信される、方法。
【０１０１】
［１６］実施例８～１５のうちのいずれか１つの方法において、
前記セキュリティプロファイルは、複数のモバイルデバイス識別情報の間で共用され、前記複数のモバイルデバイス識別情報を識別するフィールドを含む、方法。
【０１０２】
［１７］実施例８～１５のうちのいずれか１つの方法において、
前記セキュリティプロファイルのデータベースは、対応するモバイルデバイスからのデータを暗号化するための異なるセキュリティプロトコルを識別する別のセキュリティプロファイルを含む、方法。
【０１０３】
［１８］ＭＳＯＬであって、
モバイル無線ネットワークを介してモバイルデバイスから、セキュアサーバ上でログイン処理を開始するための要求を受信し、前記要求から前記モバイルデバイスのモバイルデバイス識別情報を決定するように構成されたモバイルデバイス識別コンポーネントと、
前記モバイルデバイス識別情報を使用して前記モバイルデバイスをセキュリティプロファイルディレクトリにより認証し、その認証に応答して前記セキュリティプロファイルディレクトリから認証情報を受信するように構成されたセキュリティプロファイルディレクトリインタフェースと、
１つまたは複数のプロセッサによって実行可能であり、前記ログイン処理を開始するための要求に前記認証情報を追加するように構成された認証情報追加コンポーネントと、
パケット交換ネットワークを介してセキュアサーバに前記ログイン処理を開始するための要求をルーティングするように構成されたパケット交換ネットワークインタフェースと、を備えるＭＳＯＬ。
【０１０４】
［１９］実施例１８のＭＳＯＬにおいて、
前記パケット交換ネットワークインタフェースはさらに、前記セキュアサーバからログイン成功メッセージを受信して、前記モバイル無線ネットワークを介して前記モバイルデバイスに前記ログイン成功メッセージを転送するように構成されている、ＭＳＯＬ。
【０１０５】
［２０］方法であって、
ＭＳＯＬにおいて、モバイル無線ネットワークを介してモバイルデバイスから、セキュアサーバ上でログイン処理を開始するための要求を受信すること、
前記要求から前記モバイルデバイスのモバイルデバイス識別情報を決定すること、
前記モバイルデバイス識別情報を使用して、前記モバイルデバイス識別情報に対応する認証情報をセキュリティプロファイルディレクトリから取得すること、
前記ログイン処理を開始するための要求に前記認証情報を追加すること、
パケット交換ネットワークを介してセキュアサーバに、前記ログイン処理を開始するための要求をルーティングすること、を備える方法。
【０１０６】
［２１］実施例２０の方法において、

前記モバイルデバイス識別情報は国際移動体加入者識別番号（ＩＭＳＩ）である、方法。

【０１０７】

［２２］実施例２０または２１の方法において、

前記モバイルデバイス識別情報は移動局国際加入者ディレクトリ番号（ＭＳＩＳＤＮ）である、方法。

【０１０８】

［２３］実施例２０～２２のうちのいずれか１つの方法において、

前記セキュアサーバからログイン成功メッセージを受信して、前記モバイル無線ネットワークを介して前記モバイルデバイスに前記ログイン成功メッセージを転送することをさらに備える方法。

【０１０９】

［２４］命令を伝搬する機械可読媒体であって、

前記命令がマシンのプロセッサによって実行されるとき、前記命令により、実施例８～１７，２０～２３のうちのいずれか１つの方法を前記マシンに実行させる、機械可読媒体。

【０１１０】

［用語］

本明細書を通して、複数のインスタンスは、単一のインスタンスとして記載されるコンポーネント、動作、または構造を実装することができる。１つまたは複数の方法の個々の動作を別々の動作として図示および説明しているが、それら個々の動作のうちの１つ以上が同時に実行されてもよく、それら動作が図示の順序で実行される必要はない。例示的な構成において、別々のコンポーネントとして提示されている構成および機能は、組み合わせの構成またはコンポーネントとして実装されてもよい。同様に、単一のコンポーネントとして提示されている構成および機能は、別々のコンポーネントとして実装されてもよい。これらおよび他の変形、変更、追加、および改良は、本明細書の主題の範囲内に含まれる。

【０１１１】

本発明の主題の概要を特定の例示的な実施形態を参照して記載したが、これら実施形態に対して、本開示のより広い範囲から逸脱することなく種々の変形および変更を行うことが可能である。本発明の主題のそのような実施形態は、本明細書では、単に便宜上の目的のために「発明」という用語によって個別にまたは総称して言及され得るが、この出願の範囲を任意の単一の開示または発明の概念に自発的に限定するものではなく、実際には２つ以上が開示される。

【０１１２】

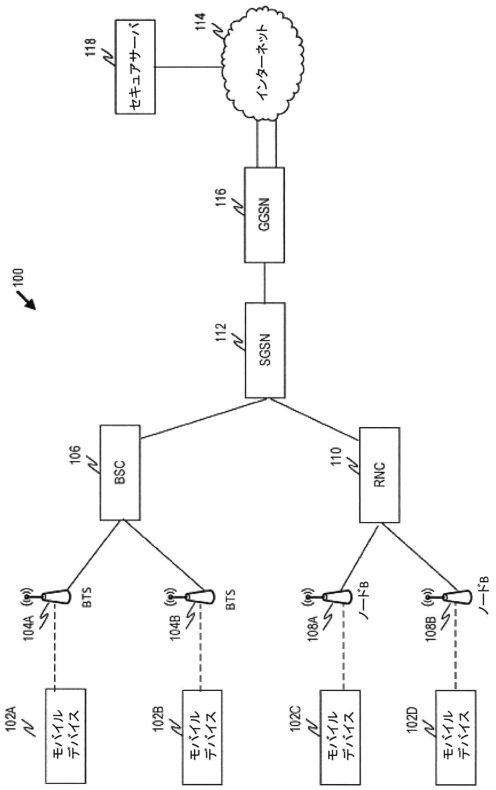
本明細書に示す実施形態は、当業者が開示された教示を実施できるように十分に詳細に記載されている。本開示の範囲から逸脱することなく、構造的および論理的な置換および変更を行い得るように他の実施形態を使用したり他の実施形態から導出したりすることができる。したがって、本詳細な説明は、限定的な意味で解釈されるべきではなく、種々の実施形態の範囲は、添付の特許請求の範囲と、そのような特許請求の範囲により与えられる等価物の全範囲とによってのみ規定される。

【０１１３】

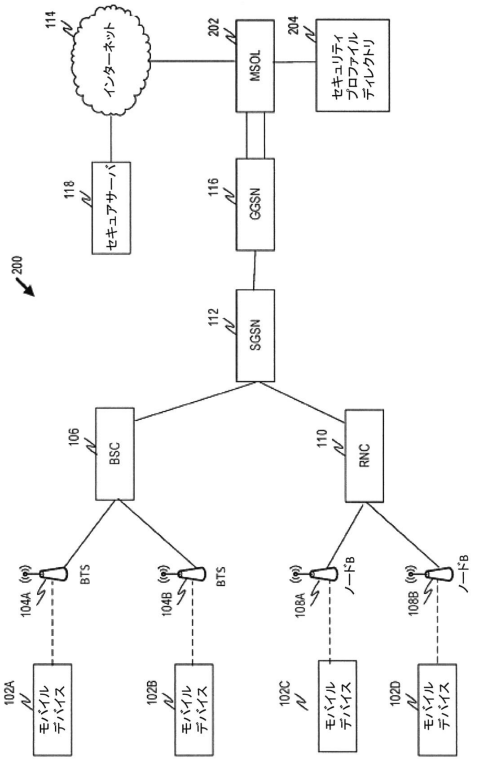
本明細書で使用される場合、「または」という用語は包括的または排他的な意味で解釈され得る。さらには、本明細書に記載されるリソース、動作、または構造に対して、複数のインスタンスが単一のインスタンスとして提供されてもよい。また、種々のリソース間、動作間、モジュール間、エンジン間、およびデータストア間の境界はいくぶん恣意的であり、特定の動作は特定の例示的な構成の文脈で示されている。機能の他の割り当ても想定されており、本開示の種々の実施形態の範囲内に含まれ得る。概して、構成例で、別個のリソースとして提示されている構造および機能は、組み合わせの構造またはリソースとして実装されてもよい。同様に、単一のリソースとして提示されている構造および機能は

、別個のリソースとして実装されてもよい。これらおよび他の変形、変更、追加、および改良は、添付の特許請求の範囲によって代表される本開示の実施形態の範囲内に含まれる。したがって、明細書および図面は、限定的ではなく例示的なものとみなされるべきである。

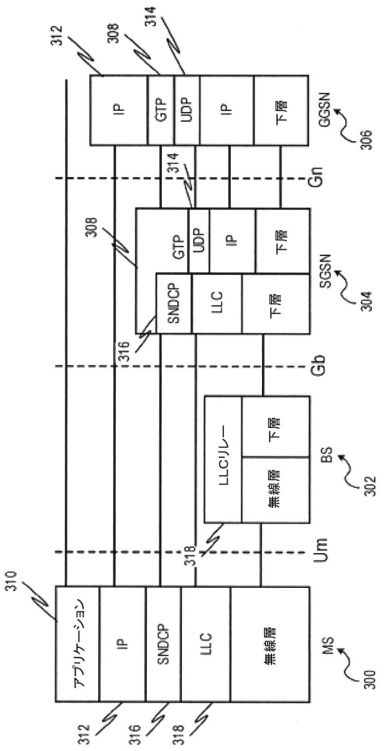
【図１】



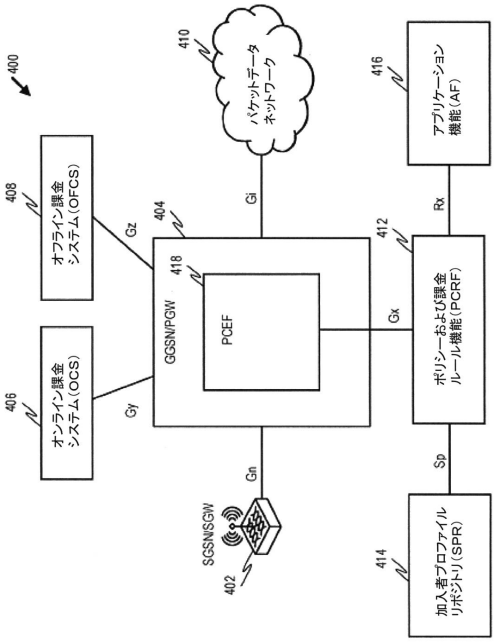
【図２】



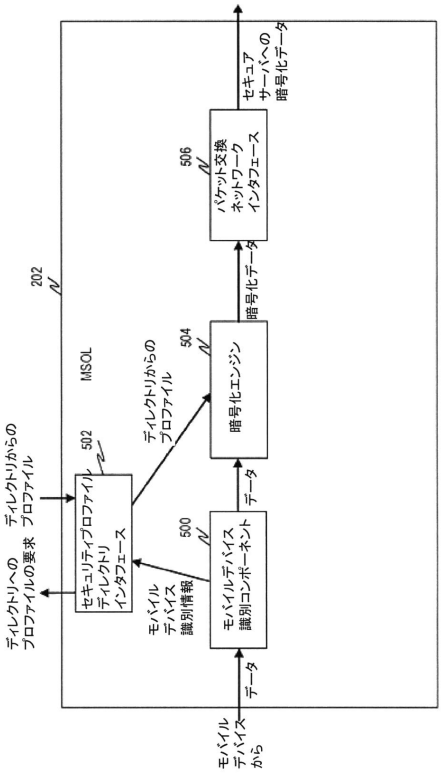
【図３】


アプリケーション
IP
SNDCP
LLC
無線層
MS
300
BS
302
SGSN
304
GGSN
306
GTP
UDP
下層
LLCリレー
Gn
Gb
Um
310
312
314
316
318

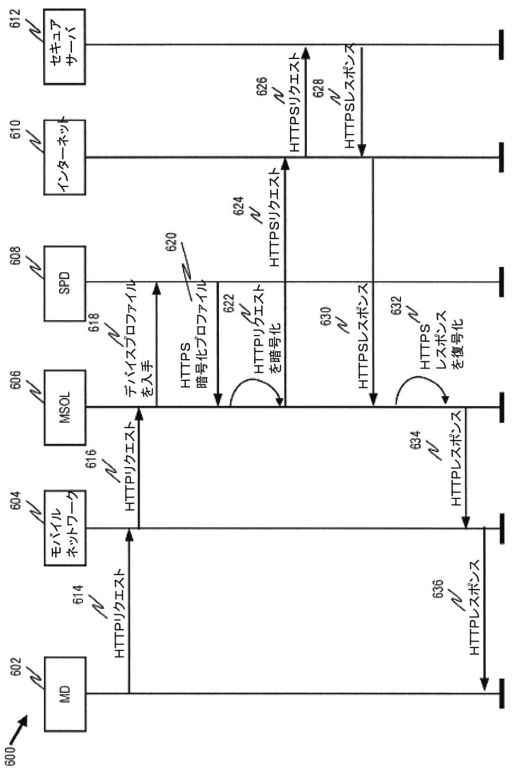
【図４】


400
パケットデータネットワーク
410
アプリケーション機能(AF)
416
オフライン課金システム(OFCS)
408
オンライン課金システム(OCS)
406
GGSN/PGW
404
PCEF
418
ポリシーおよび課金ルール機能(PCRF)
412
加入者プロファイルリポジトリ(SPR)
414
SGSN/MSGW
402
Gz
Gy
Gi
Gx
Rx
Sp
Gn

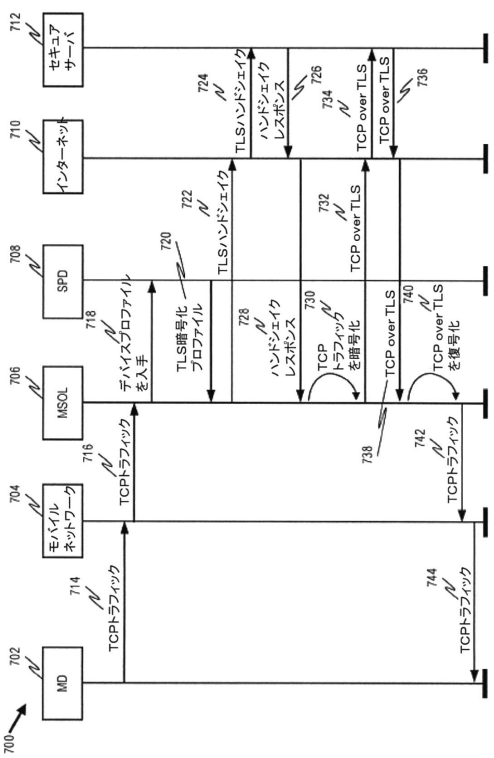
【図５】


MSOL
202
セキュリティプロファイル
ディレクトリインタフェース
502
モバイルデバイス識別コンポーネント
500
暗号化エンジン
504
パケット交換ネットワークインタフェース
506
ディレクトリからのプロファイル
ディレクトリへのプロファイルの要求
モバイルデバイス識別情報
データ
暗号化データ
セキュアサーバへの暗号化データ
モバイルデバイスから

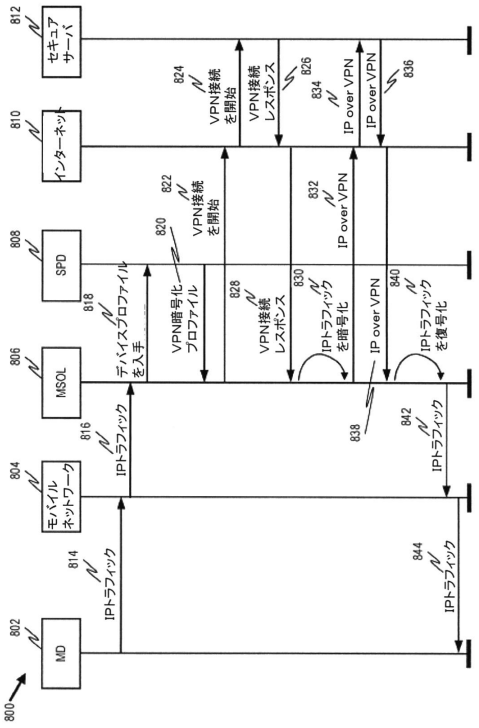
【図６】


600
MD
602
モバイルネットワーク
604
MSOL
606
SPD
608
インターネット
610
セキュアサーバ
612
HTTPリクエスト
614
HTTPリクエスト
616
デバイスプロファイルを入手
618
HTTPS暗号化プロファイル
620
HTTPリクエストを暗号化
622
HTTPSリクエスト
624
HTTPSリクエスト
626
HTTPSレスポンス
628
HTTPSレスポンス
630
HTTPSレスポンスを復号化
632
HTTPレスポンス
634
HTTPレスポンス
636

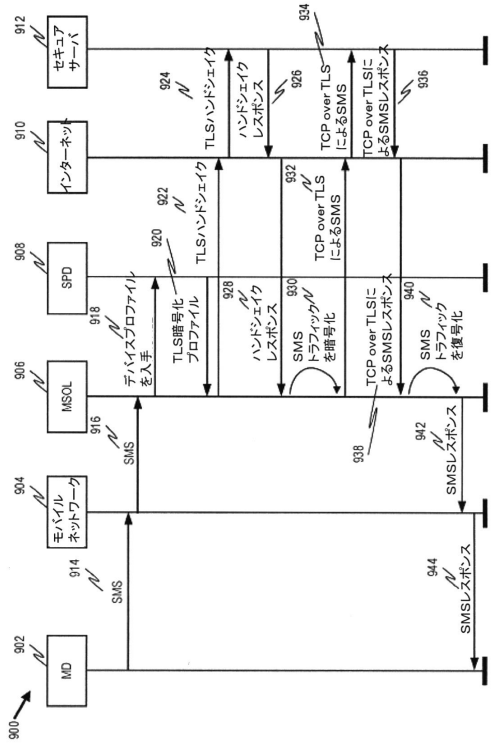
【図７】


700
MD
モバイルネットワーク
MSOL
SPD
インターネット
セキュアサーバ
TCPトラフィック
デバイスプロファイルを入手
TLS暗号化プロファイル
TLSハンドシェイク
ハンドシェイクレスポンス
TCP over TLS
TCPトラフィックを暗号化
TCPトラフィックを復号化

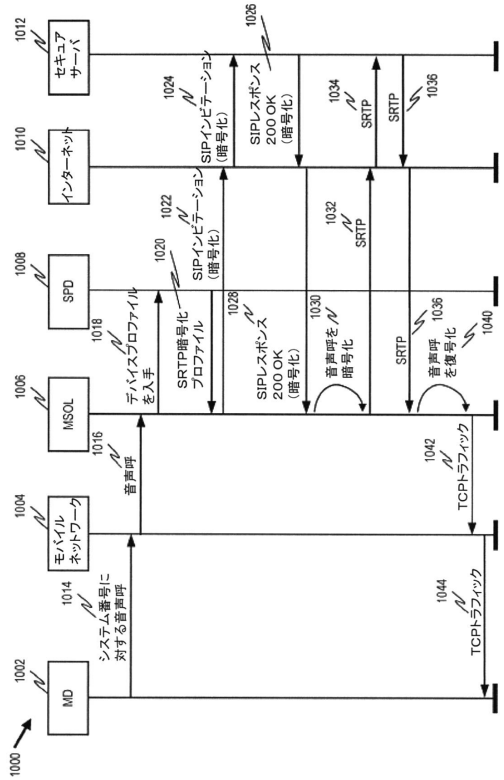
【図８】


800
MD
モバイルネットワーク
MSOL
SPD
インターネット
セキュアサーバ
IPトラフィック
デバイスプロファイルを入手
VPN暗号化プロファイル
VPN接続を開始
VPN接続レスポンス
IP over VPN
IPトラフィックを暗号化
IPトラフィックを復号化

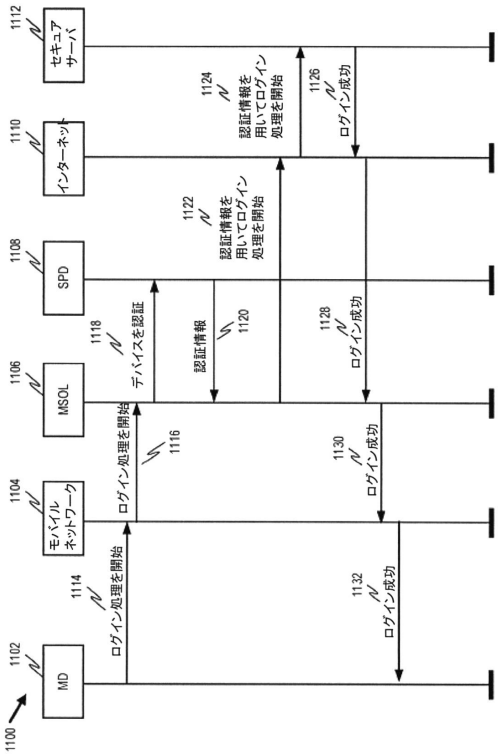
【図９】


900
MD
モバイルネットワーク
MSOL
SPD
インターネット
セキュアサーバ
SMS
SMSレスポンス
デバイスプロファイルを入手
TLS暗号化プロファイル
TLSハンドシェイク
ハンドシェイクレスポンス
SMSトラフィックを暗号化
TCP over TLSによるSMS
TCP over TLSによるSMSレスポンス
SMSトラフィックを復号化

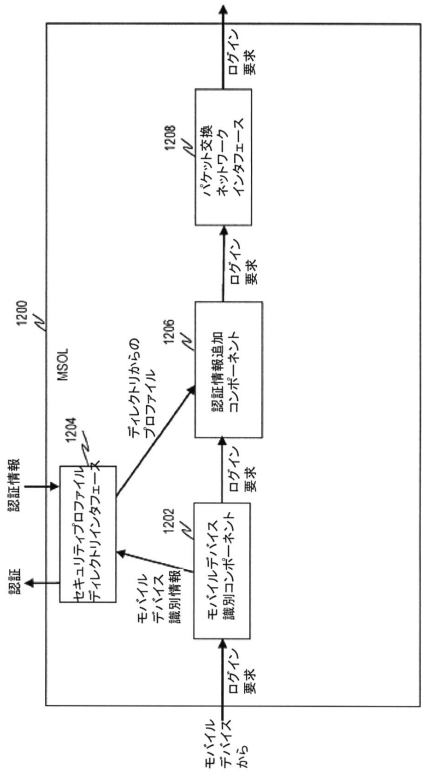
【図１０】


1000
MD
モバイルネットワーク
MSOL
SPD
インターネット
セキュアサーバ
音声呼
システム番号に対する音声呼
TCPトラフィック
デバイスプロファイルを入手
SRTP暗号化プロファイル
SIPインビテーション（暗号化）
SIPレスポンス 200 OK（暗号化）
SRTP
音声呼を暗号化
音声呼を復号化

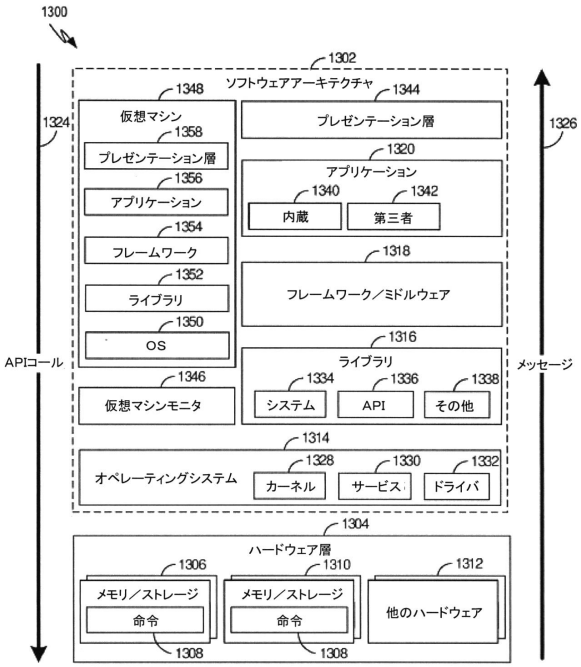
【図１１】



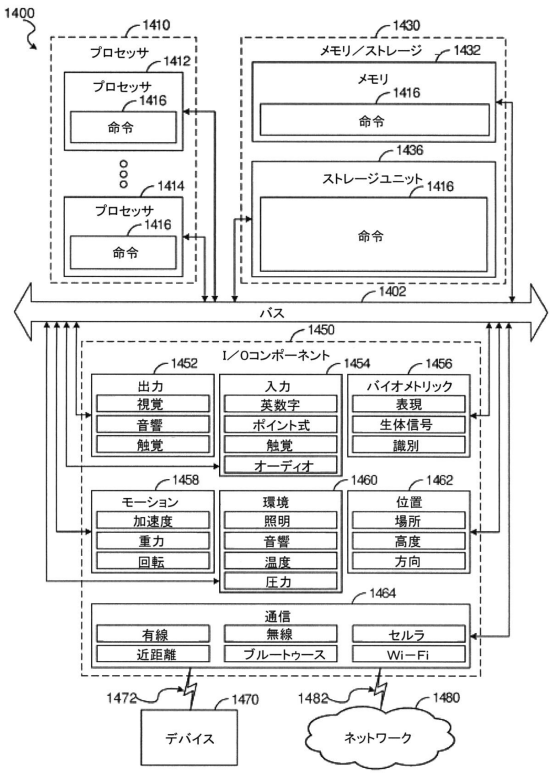
【図１２】



【図１３】



【図１４】



フロントページの続き

早期審査対象出願

(72)発明者　マルカ、フランク
イスラエル国　４０３３９２６　クファ　ヨナ　シガロン　ストリート　４６　ピーオービー　７０８１

審査官　石田　信行

(56)参考文献　特表２０１５－５１１４３４（ＪＰ，Ａ）
米国特許出願公開第２０１１／０２８９３０８（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｂ　　７／２４－　７／２６
Ｈ０４Ｗ　　４／００－９９／００
Ｇ０６Ｆ　２１／６０
Ｈ０４Ｌ　　９／１４
３ＧＰＰ　ＴＳＧ　ＲＡＮ　ＷＧ１－４
ＳＡ　ＷＧ１－４
ＣＴ　ＷＧ１、４