(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7086327号
(P7086327)

(45)発行日　令和4年6月20日(2022.6.20)

(24)登録日　令和4年6月10日(2022.6.10)

(51)国際特許分類
H04L 9/08 (2006.01)

FI
H04L 9/08 B
H04L 9/08 F

請求項の数　18　外国語出願　（全24頁）

(21)出願番号　特願2018-11494(P2018-11494)
(22)出願日　平成30年1月26日(2018.1.26)
(65)公開番号　特開2018-121334(P2018-121334A)
(43)公開日　平成30年8月2日(2018.8.2)
審査請求日　令和3年1月12日(2021.1.12)
(31)優先権主張番号　62/450,968
(32)優先日　平成29年1月26日(2017.1.26)
(33)優先権主張国・地域又は機関
米国(US)

(73)特許権者　504375237
アマゾン テクノロジーズ インコーポレイテッド
Amazon Technologies, Inc.
アメリカ合衆国 ワシントン州 98109 シアトル テリー アベニュー エヌ 410
410 Terry Ave N, Seattle, WA 98109, U.S.A.
(74)代理人　100099623
弁理士　奥山 尚一
(74)代理人　100125380
弁理士　中村 綾子

最終頁に続く

(54)【発明の名称】　アプリケーション間でユーザ情報を安全に転送すること

(57)【特許請求の範囲】
【請求項１】
登録プロセス中に、ルート秘密鍵とリモート記憶ルート鍵とノード記憶ルート鍵とエスクロー鍵とを導出し、
前記ルート秘密鍵と前記リモート記憶ルート鍵と前記ノード記憶ルート鍵とを前記エスクロー鍵で暗号化し、
パスワードベース鍵を導出し、
前記エスクロー鍵を前記パスワードベース鍵で暗号化し、
前記暗号化されたルート秘密鍵と前記暗号化されたリモート記憶ルート鍵と前記暗号化されたノード記憶ルート鍵とを含む鍵エスクローバンドルを作成し、
前記鍵エスクローバンドルを第１のサーバに送信する
ように構成されるプロセッサと、
前記プロセッサに接続され、該プロセッサに命令を与えるように構成されるメモリと
を備えてなる、システム。
【請求項２】
前記暗号化されたエスクロー鍵は、前記サーバに送信される前記鍵エスクローバンドルに含まれるものである、請求項１に記載のシステム。
【請求項３】
前記登録プロセスは、ユーザ登録プロセスである、請求項１に記載のシステム。
【請求項４】

前記プロセッサは、
パスワードベース鍵導出関数を用いて前記パスワードベース鍵を導出するように構成される、請求項１に記載のシステム。
【請求項５】
前記プロセッサは、
ルートユーザ識別子とルート識別鍵対とを導出するように構成される、請求項１に記載のシステム。
【請求項６】
前記プロセッサは、
前記ルートユーザ識別子と前記ルート識別鍵対からのルート公開鍵とを前記第１のサーバに送信するように構成される、請求項５に記載のシステム。
【請求項７】
第１のデバイスにおいて、登録プロセス中に、ルート秘密鍵とリモート記憶ルート鍵とノード記憶ルート鍵とエスクロー鍵とを導出するステップと、
前記第１のデバイスによって、前記ルート秘密鍵と前記リモート記憶ルート鍵と前記ノード記憶ルート鍵とを前記エスクロー鍵で暗号化するステップと、
前記第１のデバイスにおいて、パスワードベース鍵を導出するステップと、
前記第１のデバイスによって、前記エスクロー鍵を前記パスワードベース鍵で暗号化するステップと、
前記第１のデバイスにおいて、前記暗号化されたルート秘密鍵と前記暗号化されたリモート記憶ルート鍵と前記暗号化されたノード記憶ルート鍵とを含む鍵エスクローバンドルを作成するステップと、
前記第１のデバイスによって、前記鍵エスクローバンドルを第１のサーバに送信するステップと
を含んでなる方法。
【請求項８】
前記暗号化されたエスクロー鍵は、前記サーバに送信される前記鍵エスクローバンドルに含まれるものである、請求項７に記載の方法。
【請求項９】
前記登録プロセスは、ユーザ登録プロセスである、請求項７に記載の方法。
【請求項１０】
パスワードベース鍵導出関数を用いて前記パスワードベース鍵を導出するステップを更に含む、請求項７に記載の方法。
【請求項１１】
前記第１のデバイスによって、ルートユーザ識別子とルート識別鍵対とを導出するステップを更に含む、請求項７に記載の方法。
【請求項１２】
前記第１のデバイスによって、前記ルートユーザ識別子と前記ルート識別鍵対からのルート公開鍵とを前記第１のサーバに送信するステップを更に含む、請求項１１に記載の方法。
【請求項１３】
少なくとも１つのプロセッサによって実行されると、
登録プロセス中に、ルート秘密鍵とリモート記憶ルート鍵とノード記憶ルート鍵とエスクロー鍵とを導出させ、
前記ルート秘密鍵と前記リモート記憶ルート鍵と前記ノード記憶ルート鍵とを前記エスクロー鍵で暗号化させ、
パスワードベース鍵を導出させ、
前記エスクロー鍵を前記パスワードベース鍵で暗号化させ、
前記暗号化されたルート秘密鍵と前記暗号化されたリモート記憶ルート鍵と前記暗号化されたノード記憶ルート鍵とを含む鍵エスクローバンドルを作成させ、
前記鍵エスクローバンドルを第１のサーバに送信させる

命令を含む、非一時的なコンピュータ可読媒体。
【請求項１４】
前記暗号化されたエスクロー鍵は、前記サーバに送信される前記鍵エスクローバンドルに含まれるものである、請求項１３に記載の非一時的なコンピュータ可読媒体。
【請求項１５】
前記登録プロセスは、ユーザ登録プロセスである、請求項１３に記載の非一時的なコンピュータ可読媒体。
【請求項１６】
パスワードベース鍵導出関数を用いて前記パスワードベース鍵を導出するための命令を含む、請求項１３に記載の非一時的なコンピュータ可読媒体。
【請求項１７】
ルートユーザ識別子とルート識別鍵対とを導出するための命令を含む、請求項１３に記載の非一時的なコンピュータ可読媒体。
【請求項１８】
前記ルートユーザ識別子と前記ルート識別鍵対からのルート公開鍵とを前記第１のサーバに送信するための命令を含む、請求項１７に記載の非一時的なコンピュータ可読媒体。
【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２０１７年１月２６日に出願された「Secure Communication Protocol」と題する米国仮特許出願第６２／４５０，９６８号の優先権を主張し、その全体が引用することにより本明細書の一部をなすものとする。また、本出願は、「Secure Configuration of an Application」と題する米国特許出願第　　号に関連し、その全体を引用することにより本明細書の一部をなすものとする。
【背景技術】
【０００２】
友人、家族、同僚、クライアント及び顧客と常に接続しておくために、ユーザは、複数のデバイス上に、メッセージングアプリケーション及び通話アプリケーション等の通信アプリケーションをインストールしている。これらの通信アプリケーションの幾つかによれば、ユーザは暗号化された通信を交換できるようになる。これらの通信アプリケーションに関する登録プロセスの一部として、アプリケーションは、ユーザに特有の秘密鍵を導出する場合がある。これらの秘密鍵は、エンドユーザだけが知っておくべきであり、信頼のルート（root of trust）を確立するために使用される場合がある。これに関して、通信アプリケーションの任意の後続のインストールによって、最初のインストールから任意の後続のインストールへの秘密鍵の転送中にセキュリティが損なわれるおそれがある。すなわち、秘密鍵が悪意のあるユーザによって取得されてしまったなら、悪意のあるユーザが正規のユーザに成りすまし、通信アプリケーションの自らのインスタンスを作成できることになる。これにより、悪意のあるユーザが、正規のユーザに代わってメッセージを送信できるようになり、及び／又は正規のユーザの会話を盗み聞きできるようになる。したがって、正規のユーザが、セキュア通信アプリケーションの最初のインストールからセキュア通信アプリケーションの後続のインストールに、自らの秘密鍵を安全に転送できるようにすることが当該技術分野において必要とされている。
【発明の概要】
【０００３】
本出願は、プロセッサと、命令を含むメモリとを含むシステムを記述する。プロセッサは、ルートユーザ識別子、ルート識別鍵対、ルート秘密鍵、リモート記憶ルート鍵、ノード記憶ルート鍵及びエスクロー鍵を導出することを含む登録プロセスを実行するように構成される。プロセッサは、ルート秘密鍵、リモート記憶ルート鍵及びノード記憶ルート鍵をエスクロー鍵で暗号化する。エスクロー鍵は、そして、パスワードベース鍵導出関数に従

って導出されたパスワードベース鍵で暗号化される。そして、プロセッサは、暗号化されたルート秘密鍵、暗号化されたリモート記憶ルート鍵及び暗号化されたノード記憶ルート鍵を含む鍵エスクローバンドルを作成し、ルートユーザ識別子、ルート公開鍵及び鍵エスクローバンドルをサーバに送信する。幾つかの例において、暗号化されたエスクロー鍵は、サーバに送信される鍵エスクローバンドル内に含まれる。

【０００４】

本出願の別の例によれば、方法は、ルートユーザ識別子と、ルート識別鍵対と、ルート秘密鍵と、リモート記憶ルート鍵と、ノード記憶ルート鍵と、エスクロー鍵とを導出することを含む登録プロセスを実行することを含む。その方法は、ルート秘密鍵とリモート記憶ルート鍵とノード記憶ルート鍵とをエスクロー鍵で暗号化し、そして、パスワードベース鍵導出関数に従って導出されたパスワードベース鍵でエスクロー鍵を暗号化する。その方法は、暗号化されたルート秘密鍵と暗号化されたリモート記憶ルート鍵と暗号化されたノード記憶ルート鍵とを含む鍵エスクローバンドルを作成し、ルートユーザ識別子とルート公開鍵と鍵エスクローバンドルとをサーバに送信する。

【０００５】

本開示の別の例は、登録プロセスを実行するための命令を含む非一時的コンピュータ可読媒体を含む。登録の一部として、ルートユーザ識別子と、ルート識別鍵対と、ルート秘密鍵と、リモート記憶ルート鍵と、ノード記憶ルート鍵と、エスクロー鍵とが導出される。ルート秘密鍵とリモート記憶ルート鍵とノード記憶ルート鍵とがエスクロー鍵を用いて暗号化される。エスクロー鍵は、その後、パスワードベース鍵導出関数に従って導出されたパスワードベース鍵で暗号化される。鍵が暗号化された後に、鍵エスクローバンドルが作成され、第１のサーバに送信される。

【０００６】

更に別の例によれば、本開示は、プロセッサ及びメモリを含むシステムを記述する。プロセッサは、サーバから、暗号化された鍵エスクローバンドルを検索するように構成される。これに関して、プロセッサは、サーバから、暗号化された鍵エスクローバンドルを要求し、その後に受信する。鍵エスクローバンドルは、ルート秘密鍵、リモート記憶ルート鍵、ノード記憶ルート鍵及びエスクロー鍵のうちの少なくとも１つを含む。次に、プロセッサはエスクロー鍵を取得し、エスクロー鍵を用いて、サーバから受信された暗号化された鍵エスクローバンドルを解読する。それに応じて、プロセッサは、解読された鍵エスクローバンドル内に含まれる情報を用いて、デバイス上でセキュア通信アプリケーションを使えるように設定する。幾つかの例において、暗号化された鍵エスクローバンドルは、異なるデバイスによって、サーバにアップロードされる。

【０００７】

本開示の別の例は、サーバから、暗号化された鍵エスクローバンドルを検索するための方法を記述する。その方法は、クライアントデバイスから、サーバに送信されている鍵エスクローバンドルを要求することから開始する。クライアントデバイスは、暗号化された鍵エスクローバンドルをサーバから受信し、エスクロー鍵を取得し、エスクロー鍵を用いて、サーバから受信された暗号化された鍵エスクローバンドルを解読する。解読された鍵エスクローバンドルから、ルート秘密鍵とリモート記憶ノード鍵とノード記憶ルート鍵とが検索される。ルート秘密鍵とリモート記憶ノード鍵とノード記憶ルート鍵とを用いて、セカンダリデバイス上でセキュア通信アプリケーションが構成される。

【０００８】

本開示によって例示される別の実施形態は、暗号化された鍵エスクローバンドルをサーバから検索するための命令を含む非一時的コンピュータ可読媒体を含む。その命令は、クライアントデバイスからサーバに鍵エスクローバンドル要求を送信する。その要求に応答して、クライアントデバイスは、サーバから暗号化された鍵エスクローバンドルを受信する。その命令は、エスクロー鍵を取得することを含み、エスクロー鍵を用いて、サーバから受信された暗号化された鍵エスクローバンドルを解読する。解読された鍵エスクローバンドルから、ルート秘密鍵とリモート記憶ノード鍵とノード記憶ルート鍵とが取得され、セ

カンダリデバイスを構成するために使用される。
【０００９】
本発明の種々の実施形態は、以下の詳細な説明及び添付の図面に開示される。
【図面の簡単な説明】
【００１０】
【図１】セキュア通信が交換される環境の一例を示す図である。
【図２】セキュアコラボレーションアプリケーションを用いて、暗号化された通信を送信及び受信するクライアントデバイスを示す図である。
【図３】セキュア通信プラットフォームでユーザが登録するための例示的なプロセスを示す図である。
【図４】鍵エスクローバンドルを作成し、鍵エスクローバンドルをサーバ上に記憶するための例示的なプロセスを示す図である。
【図５】セキュア通信プラットフォームでデバイスを登録するための一例を示す図である。
【図６】鍵合意プロトコルの一部として短期鍵のプールを生成するためのプロセスの一例を示す図である。
【図７】セカンダリデバイスを使えるように設定するためのプロセスの一例を示す図である。
【図８Ａ】本開示の一実施形態による、暗号化された通信を送信するためのプロセスを示す図である。
【図８Ｂ】本開示の一実施形態による、暗号化された通信を送信するためのプロセスを示す図である。
【図８Ｃ】本開示の一実施形態による、暗号化された通信を送信するためのプロセスを示す図である。
【図９Ａ】本開示の一実施形態による、暗号化された通信を受信し、解読するためのプロセスを示す図である。
【図９Ｂ】本開示の一実施形態による、暗号化された通信を受信し、解読するためのプロセスを示す図である。
【図１０】第１のユーザと第２のユーザとの間の終端間暗号化通信のためのモバイルインターフェースの一例を示す図である。
【図１１】２つのユーザ間の終端間暗号化通信のためのインターフェースの説明のための例を示す図である。
【発明を実施するための形態】
【００１１】
本開示は、複数のデバイス上でセキュア通信アプリケーションの複数のインスタンスを使えるように設定するためのシステム及び方法を記述する。セキュア通信アプリケーションの複数のインスタンスが使えるように設定されると、ユーザは、それら全てのデバイスにわたって、暗号化された通信を送信及び受信することができる。
【００１２】
本開示は、プロセス、装置、システム、組成物、非一時的コンピュータ可読記憶媒体上に具現されるコンピュータプログラム製品、及び／又はプロセッサに結合されるメモリに記憶され、及び／又はプロセッサに結合されるメモリによって与えられる命令を実行するように構成されるプロセッサ等のプロセッサを含む、種々の方法で実現することができる。これらの実施態様、又は本開示がとる場合がある任意の他の形態が、技法と呼ばれる場合がある。一般に、開示されるプロセスのステップの順序は、本開示の範囲内で変更される場合がある。他に明示されない限り、タスクを実行するように構成されるものとして説明されるプロセッサ又はメモリ等の構成要素は、所与の時点においてそのタスクを実行するように一時的に構成される汎用構成要素として、又はそのタスクを実行するために製造される専用の構成要素として実現される場合がある。本明細書において使用されるときに、「プロセッサ」という用語は、コンピュータプログラム命令等のデータを処理するように構成される１つ以上のデバイス、回路及び／又は処理コアを指している。

【００１３】
本開示の１つ以上の実施形態の詳細な説明が、本開示の原理を例示する添付の図面とともに以下に与えられる。本開示は、そのような実施形態に関連して説明されるが、本開示はいかなる実施形態にも限定されない。本開示の範囲は、特許請求の範囲によってのみ限定され、本開示は、数多くの代替形態、変更形態及び均等形態を含む。本開示を完全に理解してもらうために、以下の説明において数多くの具体的な細部が記述される。これらの細部は、例示する目的で与えられており、本開示は、これらの具体的な細部のうちの幾つか又は全てを用いることなく、特許請求の範囲に従って実施することができる。明確にするために、本開示に関連する技術分野において既知である技術資料は、本開示を無用に不明瞭にしないように、詳細には説明されない。

【００１４】
図１は、セキュア通信が交換される環境の一実施形態を示す。具体的には、図１は、ネットワーク１１２を介して、サーバ１００上に位置するセキュア通信プラットフォーム１２０に接続される第１のクライアントデバイス１１６及び第２のクライアントデバイス１１８を示す。

【００１５】
通常、セキュア通信は、送信者のメッセージをカプセル化するセキュアメッセージデータグラムを用いて交換される。また、そのデータグラムによって、暗号化情報、ハードウェアバインディング情報、メッセージセキュリティ制御、及び解読情報等の情報が、（適用可能なだけ）複数の受信者に対して、そのメッセージとともに安全に移動できるようになる。また、セキュアメッセージデータグラムは、自らのオペレーティングシステム（例えば、Ｌｉｎｕｘ（登録商標）、ｉＯＳ及びＷｉｎｄｏｗｓ）、スマートフォンプラットフォーム（例えば、ｉＰｈｏｎｅ（登録商標）、Ａｎｄｒｏｉｄ、Ｗｉｎｄｏｗｓ、Ｂｌａｃｋｂｅｒｒｙ等）及びデバイスタイプ（例えば、モバイルスマートフォン、タブレット、ラップトップ、デスクトップ等）にかかわらず、ユーザが通信することができるように、クロスプラットフォームサポートを提供する。本明細書において説明される技法を使用するとき、意図したデバイス上の意図したアカウントのみが、そのメッセージを解読することができる。したがって、例えば、セキュア通信プラットフォーム１２０は、メッセージを解読することができない。後に更に詳細に説明されるように、本明細書において説明される技法を使用するとき、メッセージ参加者は、同期して通信する（例えば、全ての参加者がオンライン状態にあるか、又は別の方法でプラットフォーム１２０と通信することができる）にしても、非同期で通信する（例えば、少なくとも１人の参加者がオフライン状態にあるか、又は別の状況でプラットフォーム１２０と通信していない）にしても、フォワード秘密セキュア通信チャネル（forward secret secure communication channel）を保持することができる。

【００１６】
図１に示されるように、セキュア通信プラットフォーム１２０は、サーバ１００上に実現することができる。サーバ１００は、プロセッサ１０２と、メモリ１０４と、ユーザディレクトリ１０６と、セキュア通信プラットフォーム１２０とを含みうる。これに関して、サーバ１００は、スタンドアローンサーバ、企業サーバ、又はサーバファーム若しくはクラウドコンピューティング環境内に位置するサーバでありうる。幾つかの実施形態において、サーバ１００は、ソフトウェア・アズ・ア・サービス（ＳａａＳ：Software as a Service）として企業にセキュア通信プラットフォーム１２０を提供するように構成されるバーチャルマシンを運用するクラウドサービスプロバイダでありうる。

【００１７】
プロセッサ１０２は、メモリ１０４、ユーザディレクトリ１０６及びセキュア通信プラットフォーム１２０とインタラクトすることができる任意の従来のプロセッサでありうる。これに関して、プロセッサ１０２は、プロセッサ、マルチプロセッサ、マルチコアプロセッサ、又はその任意の組み合わせを含みうる。代わりに、プロセッサ１０２は、特定用途向け集積回路（ＡＳＩＣ）又はフィールドプログラマブルゲートアレイ（ＦＰＧＡ）等の

専用コントローラでありうる。
【００１８】
メモリ１０４は、プロセッサ１０２によって実行される場合があるか、又は別の方法で使用される場合がある命令及びデータを含む、プロセッサ１０２によってアクセス可能な情報を記憶する。メモリ１０４は、ハードドライブ、固体ドライブ、メモリカード、フラッシュドライブ、ＲＯＭ、ＲＡＭ、ＤＶＤ又は他の光ディスク、及び他の書込み可能や読出し専用メモリ等の、電子デバイスの助けを借りて読み出すことができるデータを記憶する非一時的コンピュータ可読媒体又は任意の他の適切な媒体を含む、プロセッサによってアクセス可能な情報を記憶することができる任意のタイプの媒体でありうる。メモリ１０４は、短期的又は一時的な記憶装置及び長期的又は持続的な記憶装置を含みうる。幾つかの実施形態によれば、メモリ１０４は、セキュア通信プラットフォーム１２０によってアクセス可能なストレージエリアネットワーク（ＳＡＮ）を含みうる。
【００１９】
ユーザディレクトリ１０６は、ディレクトリサービスを提供することができる任意のデータベース又はテーブルでありうる。例えば、ユーザディレクトリは、従業員の氏名、ユーザ名、電子メールアドレス、電話番号、部署情報等を含む企業ディレクトリを含みうる。代わりに、ユーザディレクトリ１０６は、セキュア通信プラットフォーム１２０のユーザのユーザ情報を維持管理するデータベース又はテーブルでありうる。これに関して、ユーザディレクトリ１０６は、暗号化される場合がある。幾つかの実施形態において、ユーザディレクトリ１０６は、ハッシュ化されたユーザ名のテーブル、ａｐｐＩＤのテーブル及びセキュア通信アプリケーションのためのデバイスＩＤのテーブルを含むセキュアディレクトリとしての役割を果たすことができる。したがって、ユーザディレクトリ１０６を用いて、ユーザ、システム、ネットワーク、サービス及びアプリケーションについての情報を共有することができる。幾つかの実施形態によれば、ユーザディレクトリ１０６は、ライトウェイトディレクトリアクセスプロトコル（ＬＤＡＰ）を含みうる。
【００２０】
図１は、プロセッサ１０２、メモリ１０４、ユーザディレクトリ１０６及びセキュア通信アプリケーション１２０をサーバ１００上に位置するものとして示すが、プロセッサ１０２及びメモリ１０４は、複数のプロセッサ及びメモリを含む場合があり、それらは物理的に同じハウジング内に収容される場合があるか、又は物理的に同じハウジング内に収容されない場合がある。例えば、メモリ１０４は、ストレージエリアネットワーク（ＳＡＮ）等の、データセンターのサーバファーム内に位置するハードドライブ又は他の記憶媒体でありうる。したがって、プロセッサ、コンピュータ又はメモリを参照することは、並列に動作する場合があるか、又は並列に動作しない場合があるプロセッサ又はコンピュータ又はメモリの集合を参照することを含むことは理解されるであろう。さらに、ユーザディレクトリ１０６は、処理エンジン１０２及びメモリ１０４とは物理的に別のハウジング内に位置することができる。さらに、セキュア通信プラットフォーム１２０は、複数のサーバにわたって分散する場合がある。
【００２１】
セキュア通信プラットフォーム１２０は、セキュア通信アプリケーションのユーザのための通信の交換を助長するように構成することができる。本明細書において使用されるときに、「通信」及び「メッセージ」は、テキストメッセージ、チャットルームメッセージ、制御メッセージ、コマンド、電子メール、ドキュメント、オーディオビジュアルファイル、ショートメッセージサービスメッセージ（ＳＭＳ）、音声通話（すなわち、ＶＯＩＰ）及びビデオ通話を含む、様々な形態をとることができる。さらに、メッセージ及び／又は通信のコンテンツは、クレジットカードセキュリティ、パスワード保護、ディレクトリ及びストレージドライブ保護、ビデオオンデマンドセキュリティ、オンラインゲーム、ギャンブル、音楽電子配信、ビデオ、ドキュメント、オンライン学習システム、データベース、クラウドストレージ及びクラウド環境、銀行取引、投票処理、軍事通信、医療記録セキュリティ、医療用移植デバイスと医者との間の通信等の電子トランザクションに関連する

場合がある。メッセージ及び／又は通信の交換は、後に更に詳細に説明される。
【００２２】
セキュア通信プラットフォーム１２０は、規格に準拠し、安全な通信を提供しながら、安全な既存のシステムに容易に統合される暗号化通信を提供することができる。これに関して、セキュア通信プラットフォーム１２０は、ユーザディレクトリ１０６等の、既存の識別システムと統合することができる。さらに、セキュア通信プラットフォーム１２０は、企業データ保持及びサポートシステムのためのビルトインサポートを含みうる。
【００２３】
また、セキュア通信プラットフォーム１２０は、データベース１３０も含みうる。データベース１３０は、様々なテーブル内に情報を記憶するリレーショナルデータベースでありうる。これに関して、データベース１３０は、ユーザが他のユーザを見つけ、他のユーザと通信できるようにするために、プラットフォーム１２０のユーザごとの記録を含みうる。したがって、データベース１３０は、ユーザの鍵エスクローバンドルを含む、ルート識別子１３２のテーブル、ノード識別子１３４のテーブル、短期鍵１３６のプール、ユーザプロファイル情報１３８のテーブルを含みうる。さらに、ユーザプロファイル情報は、ユーザが通信することができる相手を管理するために、プライバシーモード及びプライバシーリストエントリを記憶することができる。さらに、データベース１３０は、通信１４０のテーブルを含みうる。すなわち、セキュア通信プラットフォームは、テーブル１４０内に所定の時間にわたって通信を記憶することができる。例えば、通信が受信されるとき、セキュア通信プラットフォームは、通信１４０のテーブル内に通信を記憶し、受信者に、プッシュ通知等のアラートを与えることができる。それに応じて、受信者は、テーブル１４０内に記憶された自分の通信を取得するために、セキュア通信プラットフォームにアクセスすることができる。好ましい実施形態において、テーブル１４０は、３０日間、通信を記憶することができる。しかしながら、これは、業界標準規格に基づいて、及び／又は規制方針に準拠するために、必要に応じて調整することができる。
【００２４】
図１にはデータベースが示されるが、暗号化通信の交換を容易にするために、他の技法を用いて、プラットフォーム１２０によって使用される情報を記憶することができる。例えば、通信のテーブルは、データベース１３０内に記憶する代わりに、メモリ１０４等の別の記憶装置内に記憶することができる。代わりに、データベース１３０内に含まれる情報は、データベース１３０とユーザディレクトリ１０６との間で分割することができる。これに関して、データベース１３０及びユーザディレクトリ１０６は、情報を交換するためのインターフェースを有することがある。さらに、データベース１３０内であるか、別の適切な場所であるかにかかわらず、プラットフォーム１２０上に更なる情報を安全に記憶することができる。
【００２５】
セキュア通信プラットフォーム１２０は、第１のクライアントデバイス１１６及び第２のクライアントデバイス１１８と通信するための１つ以上のインターフェース１２２を含みうる。一例として、プラットフォーム１２０は、クライアントデバイス上にインストールされたアプリケーションと通信するように構成されるアプリケーションプログラミングインターフェース（ＡＰＩ）を提供することができる。また、プラットフォーム１２０は、ウェブインターフェース、又は種々のオペレーティングシステム（ＯＳ）上で実行される、デスクトップ及びラップトップ用のスタンドアローンソフトウェアプログラム等の、他のタイプのインターフェースを提供することもできる。ウェブインターフェースによって、クライアントデバイスのユーザは、別個にインストールされる通信アプリケーションを必要とすることなく、（互いとの通信、又は他のユーザとの通信にかかわらず）通信を安全に交換できるようになる場合がある。スタンドアローンソフトウェアプログラムによって、ユーザは、各ユーザによってダウンロードされたソフトウェアを介して、セキュア通信を交換できるようになる場合がある。幾つかの実施形態によれば、プラットフォーム１２０は、１つ以上のインターフェース１２２を介して、マスタークロック時間を利用でき

るようになる場合がある。マスタークロック時間は、メッセージの安全な有効生存期間（ＴＴＬ：time-to-live）値を強制するためにクライアントアプリケーションによって使用される場合がある。ＴＴＬ値を用いて、（例えば、受信者による）通信アクセスに関する時間制約を（例えば、メッセージ送信者に代わって）強制することができる。

【００２６】

クライアントデバイス１１６及び１１８等のクライアントデバイスのユーザは、本明細書において説明される技法を用いて互いに安全に通信することができる。例えば、第１のクライアントデバイス１１６及び第２のクライアントデバイス１１８はそれぞれ、セキュア通信アプリケーション１４６及び１４８を介して、本明細書において説明されるセキュア通信プラットフォーム１２０及び技法を使用することができる。図１に示されるように、クライアントデバイスは、ラップトップ、スマートフォン若しくはタブレット等のモバイルデバイス、又はデスクトップコンピュータ若しくはサーバ等のコンピューティングデバイスでありうる。上記で言及されたように、本明細書において説明されるセキュア通信アプリケーションはクロスプラットフォーム通信を可能にし、それにより、種々のデバイスのユーザがシームレスに通信できるようにする。さらに、各ユーザは、複数のデバイスにわたって通信アプリケーションの異なるインスタンスを有する場合がある。すなわち、デバイス１１６のユーザは、デバイス１１６と、ラップトップ等のセキュア通信アプリケーションのコピーを含む、ユーザが所有する場合がある任意の他のデバイスとの両方においてメッセージを受信できる場合がある。幾つかの実施形態において、クライアントデバイス１１６及び１１８は、ユーザのパーソナルデバイスでありうる（すなわち、個人所有機器持ち込み（ＢＹＯＤ：bring your own device）シナリオ）。代わりに、クライアントデバイスは、適用可能な場合には、ゲームコンソール、カメラ／ビデオレコーダ、ビデオプレーヤ（例えば、ＤＶＤ、ブルーレイ、レッドレーザ、光学及び／又はストリーミング技術を組み込む）、スマートＴＶ、及び他のネットワーク接続電化製品等の他のタイプのデバイスを含みうる。

【００２７】

クライアントデバイス１１６及び１１８のユーザ間の通信は、ネットワーク１１２を介して交換することができる。ネットワーク１１２は、種々の構成を含むことができ、インターネット、ワールドワイドウェブ、イントラネット、仮想プライベートネットワーク、ローカルイーサネット（登録商標）ネットワーク、１つ以上の企業に所有権がある通信プロトコルを用いるプライベートネットワーク、セルラー及びワイヤレスネットワーク（例えば、ＷｉＦｉ）、インスタントメッセージング、ＨＴＴＰ及びＳＭＴＰ、並びに上記の種々の組み合わせを含む、種々のプロトコルを使用することができる。

【００２８】

後に更に詳細に説明されるように、プロセッサ１０２は、セキュア通信プラットフォーム１２０の代わりに複数のタスクを実行することができる。さらに、プラットフォーム１２０がタスクを実行すると説明されるときにはいつでも、プラットフォーム１２０又は企業サーバ１００の単一の構成要素、又は構成要素のサブセット、又は全ての構成要素が協調して、タスクを実行する場合がある。例えば、プラットフォーム１２０は、デバイスのユーザから受信されたＥＣＤＨ公開鍵のプール内の鍵のうちの１つを「予約」鍵と指定することができる。プラットフォーム１２０によって実行される別のタスクは、新たな鍵が使用されるときに、それらの鍵をユーザの公開鍵のプールに追加するのを容易にすることを含みうる。プラットフォーム１２０によって実行される更に別のタスクは、必要に応じて、ユーザの公開鍵プールのサイズを動的に調整することを含みうる。

【００２９】

上記のセキュア通信プラットフォームを使用するために、ユーザは、自らのクライアントデバイス上にセキュア通信アプリケーションをダウンロードし、インストールしなければならない。図２は、セキュアコラボレーションアプリケーションを介してセキュリティプラットフォーム１２０にアクセスすることができる例示的なクライアントデバイス２００を示す。これに関して、クライアントデバイス２００は、バス２１６によって全て相互接

続される、プロセッサ２０２と、メモリ２０４と、ディスプレイ２０６と、Ｉ／Ｏユニット２０８と、暗号（「クリプト」）アクセラレータ２１２と、ネットワークインターフェース２１４とを含む。

【００３０】

プロセッサ２０２は、クライアントデバイス２００の構成要素とインタラクトすることができる任意のプロセッサでありうる。例えば、プロセッサ２０２は、プロセッサ、マルチコアプロセッサ、マルチコアプロセッサ、ＡＲＭプロセッサ、ＡＳＩＣ若しくはＦＰＧＡ等の専用コントローラ、又はその任意の組み合わせを含みうる。メモリ２０４は、プロセッサ２０２及び／又はクリプトアクセラレータ２１２によって実行される場合があるか、又は別の方法で使用される場合がある命令及びデータを含む、プロセッサ２０２によってアクセス可能な情報を記憶することができる。例えば、メモリ２０４は、アプリケーション２２４等の命令を記憶することができる。好ましい実施形態において、アプリケーション２２４は、音声通話及びビデオ通話に参加し、暗号化されたコンテンツを共有し、暗号化された通信を交換する能力をユーザに提供するセキュアコラボレーションアプリケーションでありうる。暗号化された通信は、直接通信（例えば、送信者と受信者との間の一対一通信）、グループチャット、又はセキュアチャットルーム通信を含みうる。メモリ２０４によって記憶されるデータは、データベース２３４を含みうる。データベース２３４は、拡張暗号化規格（ＡＥＳ：Advanced Encryption Standard）等の暗号化アルゴリズムと、これ以降、ローカル記憶鍵と呼ばれる２５６ビット鍵とによって暗号化することができる。幾つかの実施形態において、データベース２３４は、セキュアコラボレーションアプリケーション２２４に関連する情報を記憶することができる。例えば、データベース２３４は、鍵情報、ユーザ情報、友人情報及び通信等の、セキュアコラボレーションアプリケーションに関連する情報をインデックス化することができる。これに関して、メッセージ識別子、送信者のユーザ名のハッシュ、送信者のアプリケーション識別子のハッシュ、受信者のユーザ名のハッシュ、受信者のアプリケーション識別子のハッシュ、通信暗号鍵、及び各通信のタイムスタンプを含む、セキュアコラボレーションアプリケーションによって送信及び受信される通信が、データベース２３４に記憶される場合がある。したがって、メモリ２０４は、ハードドライブ、固体ドライブ、メモリカード、フラッシュドライブ、ＲＯＭ、ＲＡＭ、ＤＶＤ又は他の光ディスク、並びに他の書込み可能及び読出し専用メモリ等の、電子デバイスの助けを借りて読み出すことができるデータを記憶する非一時的コンピュータ可読媒体又は任意の他の適切な媒体を含む、上記の情報を記憶することができる任意のタイプの媒体でありうる。さらに、メモリ２０４は、短期的又は一時的な記憶装置及び長期的又は持続的な記憶装置を含みうる。

【００３１】

ディスプレイ２０６は、情報を視覚的に提示することができる任意の電子デバイスでありうる。スマートフォン及びタブレット等のモバイルデバイスにおいて、ディスプレイ２０６は、タッチスクリーンディスプレイでありうる。したがって、ディスプレイ２０６は、ユーザ入力を検出し、データを出力するＩ／Ｏユニット２０８と一体化することができる。コンピューティングデバイスにおいて、ディスプレイ２０６は、モニタに接続するように構成される、ＶＧＡ、ＤＶＩ又はＨＤＭＩ（登録商標）出力等の出力とすることができる。Ｉ／Ｏユニット２０８は、ユーザから入力を受信できる場合がある。上記で言及されたように、Ｉ／Ｏユニット２０８は、ユーザから入力を受信するために、タッチスクリーンディスプレイと協働することができる。代わりに、Ｉ／Ｏユニットは、キーボード、マウス、モニタ、プリンタ等の入力デバイス及び出力デバイスとインタラクトすることができるインターフェースでありうる。さらに、Ｉ／Ｏユニット２０８は、デバイスの向き及び環境要因を判断するために、少なくとも１つの加速度計、グローバルポジショニング衛星（ＧＰＳ）システム、磁力計、近接センサ、周囲光センサ、湿度センサ、ジャイロスコープ等を含みうる。

【００３２】

クリプトアクセラレータ２１２は、鍵生成、乱数発生、暗号化／解読、署名生成、署名検

証等の暗号演算を実行することができる、専用ハードウェア、ソフトウェア又はその任意の組み合わせとすることができる。好ましい実施形態において、クリプトアクセラレータ２１２は、プロセッサ２０２の代わりに暗号演算を実行するように構成される専用プロセッサである。これに関して、アプリケーション２２４は、クリプトアクセラレータ２１２を使用して、後に更に詳細に説明されるセキュア通信機能を提供することができる。

【００３３】

ネットワークインターフェース２１４は、クライアントデバイス２００をネットワーク１２に接続することができる専用ハードウェア、ソフトウェア又はその任意の組み合わせとすることができる。これに関して、ネットワークインターフェース２１４は、種々の構成を含み、イーサネット、ＴＣＰ／ＩＰ、ＡＴＭ、セルラー及びワイヤレス通信プロトコル（例えば、８０２．１１、ＬＴＥ）、インスタントメッセージング、ＨＴＴＰ及びＳＭＴＰ、並びに上記の種々の組み合わせを含む、種々の通信プロトコルを使用することができる。

【００３４】

セキュア通信アプリケーションをインストールした後に、ユーザは、自分自身及び自らの第１のデバイスをセキュア通信プラットフォームで登録しなければならない。図３は、セキュア通信プラットフォームでユーザが登録するためのプロセス３００を示す。プロセス３００は、ブロック３１０において、ルートユーザ識別子（ＩＤｒ）を導出することから開始する。好ましい実施形態において、ルートユーザ識別子（ＩＤｒ）は、第１のユーザがセキュア通信プラットフォームとネゴシエートするユーザ名である。代わりの例において、ルートユーザ識別子（ＩＤｒ）は、システム管理者等の第三者によって割り当てられる識別子でありうる。これらの実施形態によれば、ルートユーザ識別子（ＩＤｒ）は、企業、団体又は政府ログイン情報に関連付けられる場合がある。幾つかの例において、ルートユーザ識別子（ＩＤｒ）は、ユーザに割り当てられるランダム識別子でありうる。ランダム識別子は、セキュア通信アプリケーションによって生成され、セキュア通信プラットフォームによって確認される場合がある。代わりに、ランダム識別子は、セキュア通信プラットフォームによってユーザに割り当てられる場合がある。

【００３５】

ブロック３２０において、セキュア通信アプリケーションが、ユーザのためのルート識別鍵対（Ｋｒ、ＰＫｒ）を生成する。ルート識別鍵対は、非対称導出関数を用いて生成される長期非対称鍵対でありうる。好ましい実施形態において、ルート識別鍵対は、第１のＰ－５２１曲線を用いて、楕円曲線暗号法（ＥＣＣ：elliptic curve cryptography）に従って生成される。ブロック３３０において、セキュア通信アプリケーションが、リモート記憶ルート鍵（Ｋｒｓ）を生成する。リモート記憶ルート鍵は、セキュア通信アプリケーションによってランダムに生成される対称鍵である。リモート記憶ルート鍵を用いて、セキュア通信アプリケーションのアカウントレベルバックアップを暗号化することができる。すなわち、ＡＥＳ－ＧＣＭ等の任意の対称暗号化アルゴリズムを用いて、アカウント情報をリモート記憶ルート鍵で暗号化し、セキュア通信プラットフォーム上に記憶することができる。次に、ブロック３４０において、セキュア通信アプリケーションが、ノード記憶ルート鍵（Ｋｎｓｒ）を生成する。ノード記憶ルート鍵は、ユーザのデバイス上に記憶されるデータを暗号化するためにランダムに生成され、使用される。ユーザデバイス上に記憶されるデータは、任意の対称暗号化アルゴリズム、好ましくはＡＥＳ－ＧＣＭに従って暗号化することができる。ブロック３５０において、セキュア通信アプリケーションが、エスクロー鍵（Ｋｅ）を導出する。エスクロー鍵はランダムに生成される。後に更に詳細に説明されるように、エスクロー鍵を用いて、セキュア通信プラットフォームにアップロードされ、記憶される、ユーザを識別するために使用される複数の鍵を含むユーザ情報を暗号化する。セキュア通信アプリケーションがルート公開鍵（ＰＫｒ）及びルートユーザ識別子（ＩＤｒ）をセキュア通信プラットフォームに送信するとき、ブロック３６０においてユーザ登録が完了する。ルート公開鍵（ＰＫｒ）及びルートユーザ識別子（ＩＤｒ）を受信するのに応答して、セキュア通信プラットフォームは、ユーザのために、データ

ベース１３０内に新たなエントリを作成する。

【００３６】

ユーザが複数のデバイスを有するか、又は自らのデバイスを取り替える場合、ユーザを識別する鍵を後続のデバイスに安全に転送する必要がある。図４は、これらの鍵をセキュア通信プラットフォームに安全にアップロードするためのプロセス４００を示す。ブロック４１０において、ルート秘密鍵（Ｋｒ）、リモート記憶鍵（Ｋｒｓ）及びノード記憶ルート鍵（Ｋｎｓｒ）がエスクロー鍵（Ｋｅ）で暗号化される。好ましくは、ルート秘密鍵（Ｋｒ）、リモート記憶鍵（Ｋｒｓ）及びノード記憶ルート鍵（Ｋｎｓｒ）は、ＡＥＳ－ＧＣＭ等の対称暗号化アルゴリズムを用いて暗号化される。ブロック４２０において、セキュア通信アプリケーションが、ユーザのパスワードから鍵を導出する。パスワードベース鍵は、スクリプト等のパスワードベース鍵導出関数を用いて生成される。ブロック４３０において、導出されたパスワードベース鍵でエスクロー鍵が暗号化される。ブロック４４０において、セキュア通信アプリケーションが、暗号化されたルート秘密鍵、暗号化されたリモート記憶鍵（Ｋｒｓ）及び暗号化されたノード記憶ルート鍵を含む鍵エスクローバンドルを作成する。幾つかの実施形態によれば、暗号化されたエスクロー鍵は、セキュア通信アプリケーションによって生成され、セキュア通信プラットフォームにアップロードされる鍵エスクローバンドル内に含まれる場合がある。代わりに、暗号化されたエスクロー鍵は、ユーザのデバイス上に、非一時的コンピュータ可読媒体上に、又は第三者リポジトリでローカルに記憶することができる。ブロック４５０において、鍵エスクローバンドルが、サーバに送信される。サーバ上で、鍵エスクローバンドルは、セキュア通信プラットフォームのデータベース内に記憶され、その中で、ユーザのプロファイルに関連付けられ、ユーザからの要求時に利用可能になる。後に更に詳細に論じられるように、ユーザの鍵で後続のインストールを使えるように設定するために、セキュア通信アプリケーションの後続のインストールがサーバから鍵エスクローバンドルを要求する場合がある。より安全な実施態様では、ブロック４５０はスキップされる場合がある。これに関して、ユーザは、鍵エスクローバンドルを後続のインストールに転送しなければならない。これは実施するのがより難しい場合があるが、より高い度合いのセキュリティを提供することになる。

【００３７】

上記で言及されたように、登録プロセスの一部が、セキュア通信プラットフォームでユーザのデバイスを登録することを含む。デバイス登録は、ユーザ登録が行われた後の第１のデバイス上を含む、新たなデバイス上でユーザがセキュア通信アプリケーションにログインする任意の時点で行われる。図５は、セキュア通信プラットフォームでデバイスを登録するための例示的なプロセス５００を示す。

【００３８】

デバイス登録は、セキュア通信アプリケーションがノード識別鍵対（Ｋｎ、ＰＫｎ）を生成するブロック５１０において開始する。ノード識別鍵対は、非対称導出関数を用いて生成される長期非対称鍵対でありうる。好ましい実施形態において、ノード識別鍵対は、第２のＰ－５２１曲線を用いて、ＥＣＣに従って生成される。ノード識別鍵対は、セキュア通信アプリケーションのインスタンスに固有である。これに関して、ユーザが幾つかのデバイス上でセキュア通信アプリケーションをインストールした場合には、各デバイスは、自らの固有のノード識別鍵対を有することになり、その一方で、ルート識別鍵対はインストールごとに同じになる。

【００３９】

ブロック５２０において、セキュア通信アプリケーションが、ローカル記憶デバイス鍵（Ｋｌｓｄ）を導出する。ローカル記憶デバイス鍵は、対称暗号化によって、ユーザのデバイス上にローカルに記憶されるデータを保護する。これに関して、ローカル記憶デバイス鍵は、鍵導出関数を通してノード記憶ルート鍵及びデバイスデータを合成することによって生成される。好ましい実施形態において、鍵導出関数は、根底にあるハッシュ関数としてのＳＨＡ－２５６を伴うＨＭＡＣ鍵導出関数である。後続のインストールにおいて、セキュア通信アプリケーションは、後に更に詳細に論じられるように、セキュア通信プラッ

トフォームから、ノード記憶ルート鍵を取得する。デバイスデータは、インストールされるハードウェア又はオペレーティングシステムソースから導出され、アプリケーションインストールにわたって固有であり、一定であるデバイス特有データ及び／又は識別子を含む。例えば、デバイスデータは、ハードドライブ識別子、マザーボード識別子、ＣＰＵ識別子、及びワイヤレス、ＬＡＮ、Ｂｌｕｅｔｏｏｔｈ（登録商標）及び光カードのためのＭＡＣアドレス、構成情報、又は上記の組み合わせを含みうる。

【００４０】

ブロック５３０において、セキュア通信アプリケーションが、ノード識別子（ＩＤｎ）を生成する。ノード識別子は、ＳＨＡ２５６を用いて擬似ランダムバイトの組をハッシュすることによって生成されるランダム識別子である。ノード識別子は、セキュア通信アプリケーション、及びそれが関連付けられるデバイスを識別するために、セキュア通信プラットフォームによって使用される。ブロック５４０において、セキュア通信アプリケーションが、ルート識別秘密鍵を用いて、ノード識別公開鍵の第１の署名を生成する。好ましい実施形態において、セキュア通信アプリケーションは、楕円曲線デジタル署名アルゴリズム（ＥＣＤＳＡ）に従って、署名を生成する。ブロック５５０において、ノード識別子（ＩＤｎ）、ノード公開鍵（ＰＫｎ）及びノード識別公開鍵の第１の署名（ＳＫｒ（ＰＫｎ））がサーバに送信される。セキュア通信プラットフォームは、ノード識別子（ＩＤｎ）、ノード公開鍵（ＰＫｎ）及びノード識別公開鍵の第１の署名（ＳＫｒ（ＰＫｎ））をセキュア通信プラットフォーム上のユーザのプロファイル内に記憶する。

【００４１】

ユーザ登録及びデバイス登録の両方が完了した後に、セキュア通信アプリケーションの各インスタンスが、非対称鍵対のプールを作成する。これらの鍵対は、鍵合意プロトコルの一部として使用され、セキュア通信アプリケーションが、暗号化された通信を受信し始めることができるようにする。セキュア通信アプリケーションが暗号化された通信を受信し始めると、非対称鍵対のプールは枯渇し、補充される必要がある。図６は、短期非対称鍵対のプールを追加するための方法６００を示す。

【００４２】

ブロック６１０において、セキュア通信アプリケーションが、短期非対称鍵対（ＫＥｎ及びＰＫＥｎ）のプールを生成する。好ましい実施形態において、短期非対称鍵対は、第３のＰ－５２１曲線に従って、ＥＣＣに従って生成される。ブロック６２０において、固有識別子（ＩＤｋｅｎ）が各鍵対（ＫＥｎ及びＰＫＥｎ）に割り当てられる。次に、ブロック６３０において、セキュア通信アプリケーションが、ノード識別秘密鍵（Ｋｎ）を用いて短期公開鍵（ＰＫＥｎ）ごとの署名を計算する。短期公開鍵ごとの署名は、ＥＣＤＳＡを含む、任意の標準的な署名生成アルゴリズムに従って生成することができる。ブロック６４０において、短期公開鍵（ＰＫＥｎ）がそれぞれ、その固有識別子及び対応する署名とともに、サーバにアップロードされる。それに応じて、サーバは短期公開鍵のプールをセキュア通信プラットフォーム上のユーザのプロファイル内に記憶する。短期秘密鍵の対応するプールは、ローカル記憶デバイス鍵で暗号化され、割り当てられたその固有識別子とともに、ユーザのデバイス上に安全に記憶される。

【００４３】

上記で言及されたように、プロセス６００は、ユーザの最初のユーザ登録及びデバイス登録後に最初に実行される。プロセス６００は、新たなデバイス登録ごとに繰り返される。最後に、図６に示される方法は、非対称鍵のプールが枯渇するときに必要に応じて繰り返すことができる。後に更に詳細に説明されるように、送信側セキュア通信アプリケーションが公開鍵のうちの１つを使用するとき、セキュア通信プラットフォームは、セキュア通信プラットフォーム上の入手可能な鍵のプールから公開鍵を除去する。プールが使い果たされた場合、プールを補充することができるまで、プール内の最後の鍵が再利用されることになる。

【００４４】

上記で論じられたように、ユーザが、１つ以上のセカンダリデバイス上にセキュア通信ア

プリケーションをダウンロードし、インストールする場合がある。本明細書において説明される暗号化技法によれば、ユーザは、ユーザ及びユーザの第１のデバイスのためのユーザの初期登録中に作成されたルート識別子及び鍵を用いて、１つ以上の第２のデバイスを構成しなければならないであろう。図７は、１つ以上のルート識別子及び鍵を用いてセカンダリデバイスを使えるように設定するためのプロセスを示す。

【００４５】

セキュア通信アプリケーションをセカンダリデバイスにダウンロードした後に、ユーザはそのルート識別子（例えば、ユーザ名）及びパスフレーズを入力する。ブロック７１０において、セキュア通信アプリケーションが、ルート識別子及びパスフレーズを受信する。ブロック７２０において、セキュア通信アプリケーションが、セキュア通信プラットフォームから鍵エスクローバンドルを要求する。鍵エスクローバンドル要求は、セキュア通信プラットフォームがデータベースを探索し、鍵エスクローバンドルが存在するか否かを判断できるようにするために、ルート識別子、又は何らかの他の固有識別子を含みうる。鍵エスクローバンドルがデータベース内に存在しない場合には、セキュア通信プラットフォームは、存在しないことをセキュア通信アプリケーションに通知し、セキュア通信アプリケーションが鍵エスクローバンドルを提供することを要求する。これに関して、セキュア通信アプリケーションは上記の技法に従う。しかしながら、鍵エスクローバンドルがサーバ上に記憶される場合には、ブロック７３０において、セキュア通信アプリケーションが、暗号化された鍵エスクローバンドルをサーバから受信する。

【００４６】

ブロック７４０において、セキュア通信アプリケーションが、エスクロー鍵を取得する。幾つかの例によれば、エスクロー鍵は、パスフレーズ導出鍵で暗号化され、鍵エスクローバンドルとともにセキュア通信プラットフォームに記憶される。セキュア通信アプリケーションは、受信されたパスフレーズからパスフレーズ導出鍵を導出し、セキュア通信プラットフォームから受信された暗号化された鍵エスクローバンドル内で受信された暗号化されたエスクロー鍵を解読する。他の例において、ユーザは第１のデバイスからエスクロー鍵を取得することができる。例えば、エスクロー鍵は、ＵＳＢドライブを介して、第１のデバイスから第２のデバイスに転送することができる。代わりに、エスクロー鍵は、電子メール、テキストメッセージ又は第三者リポジトリ等の異なるチャネルを介して送信される場合がある。これらの例において、エスクロー鍵は、第１のデバイスから転送される前に、パスフレーズ導出鍵で暗号化することができる。したがって、第２のデバイスは、パスフレーズ導出鍵を計算し、エスクロー鍵を解読する。正しいパスワードのみがエスクロー鍵を解読することができ、解読されたエスクロー鍵を用いて、鍵エスクローバンドルの内容を解読することができるので、これは、不正の目的のためにセキュア通信アプリケーションを使えるように設定する悪意のあるユーザに対する更なるセキュリティ機構を表す。

【００４７】

ブロック７５０において、セキュア通信アプリケーションが、エスクロー鍵を用いて、暗号化された鍵エスクローバンドルを解読する。鍵エスクローバンドルは、ＡＥＳ等の対称暗号化アルゴリズムに従って暗号化することができる。ブロック７６０において、第２のデバイス上のセキュア通信アプリケーションが、解読された鍵エスクローバンドル内に含まれる情報を用いて構成される。これに関して、第２のデバイス上のセキュア通信アプリケーションは、解読された鍵エスクローバンドルから、ルート秘密鍵（Ｋｒ）、リモート記憶ルート鍵（Ｋｒｓ）及びノード記憶ルート鍵（Ｋｎｓｒ）を取得する。鍵エスクローバンドルをアンパックした後に、セキュア通信アプリケーションは、解読された鍵エスクローバンドルから取得された情報を用いてデバイス登録を完了することができる。これにより、１つのユーザデバイスから別のユーザデバイスに複数の鍵を安全に転送できるようになり、それにより、両方のデバイスが、同じ信頼できるルート識別子に基づいて、セキュア通信を送信及び受信できるようになる。さらに、これは、後続のインストールごとに秘密鍵の新たな組を生成するようにユーザに要求することになる従来技術のシステムからの改善を表す。したがって、本明細書において説明される技法によれば、後続のアプリケ

ーションをより効率的に、そして安全にインストールできるようになる。
【００４８】
セキュア通信プラットフォームによって提供されるセキュア通信は、より理解が進むと、ユーザ間通信ではなく、ノード間通信を提供すると理解することができる。上記で論じられたように、単一のユーザが複数の関連するデバイス上で実行されるセキュア通信アプリケーションを有する場合がある。通信を送信することを目的とする場合、セキュア通信アプリケーションの各インスタンスはノードと見なされるべきである。例えば、３つのデバイスを有する第２のユーザにメッセージを送信する、２つのデバイスを有する第１のユーザは、４つのノード、すなわち、第２のユーザに関連付けられる３つのデバイス及び第１のユーザの第２のデバイスに、暗号化されたメッセージを送信している。図８Ａ～図８Ｃは、この原理に従って、暗号化された通信を送信するためのプロセス８００を示す。
【００４９】
ブロック８０５において、送信側デバイスのセキュア通信アプリケーションが、セキュア通信プラットフォームから、１つ以上の受信側ユーザのプロファイル情報を検索する。これに関して、送信側セキュア通信アプリケーションは、セキュア通信プラットフォームから、受信側ユーザのプロファイル情報を要求することができる。これは、例えば、送信側ユーザが通信を構成し始めるときに行われる場合がある。ユーザプロファイル情報は、ユーザのルート識別公開鍵（ＰＫｒ）、ユーザのデバイスノードのリスト、デバイスごとのノード識別公開鍵（ＰＫｎ）、及びノードごとの署名付きノード識別公開鍵（ＳＫｒ（ＰＫｎ））を含む。次に、ブロック８１０において、送信側セキュア通信アプリケーションが、受信側ユーザデバイス及び送信者のデバイスの共同体に基づいて、受信ノードのリストを構築する。ブロック８１５において、送信側セキュア通信アプリケーションが、セキュア通信プラットフォームから、受信側デバイスごとの署名付き短期公開鍵及びその関連する固有識別子を検索する。幾つかの実施形態によれば、署名付き短期公開鍵及び関連する固有識別子は、受信側ユーザのプロファイル情報とともに取得することができる。ブロック８２０において、送信側セキュア通信アプリケーションが、セキュア通信プラットフォームから受信された短期公開鍵ごとに署名チェーンの正当性を確認する。これに関して、短期公開鍵の署名はノード識別公開鍵を用いて、ＥＣＤＳＡ等の署名検証アルゴリズムに従って認証される。ノード識別公開鍵の署名はルート識別公開鍵を用いて検証され、ルート識別公開鍵は、予想されるユーザ識別に対応する。署名チェーンが無効である場合には、セキュア通信アプリケーションは、セキュア通信プラットフォームから、１つ以上の受信側ユーザのプロファイル情報を要求することができる。代わりに、セキュア通信アプリケーションは、通信を破棄し、無効の署名チェーンを有する１つ以上の受信側ノードとの通信を拒否することができる。署名チェーンが有効である場合には、セキュア通信アプリケーションは、１つ以上の受信者ノードに送信する通信を準備し続ける。
【００５０】
ブロック８２５において、送信側セキュア通信アプリケーションが、ランダムメッセージペイロード暗号鍵（Ｋｐａｙｌｏａｄ）を生成する。好ましい実施形態において、第１のメッセージペイロード暗号鍵は、送信側クライアントのデバイスから導出された擬似ランダムバイトの第１の組に鍵導出関数（例えば、ＨＫＤＦ）を適用することによって生成される２５６ビット鍵である。擬似ランダムバイトの第１の組は、デバイスドライバから取得された短期環境雑音、及び他のカーネル演算から導出することができる。例えば、種々のセンサ（例えば、少なくとも１つの加速度計、グローバルポジショニング衛星（ＧＰＳ）システム、磁力計、近接センサ、周囲光センサ、湿度センサ及びジャイロスコープ）からのデータを擬似ランダムバイトの第１の組として使用することができる。
【００５１】
ブロック８３０において、送信側セキュア通信アプリケーションが、パケットヘッダ暗号鍵（Ｋｈｅａｄｅｒ）を計算する。好ましい実施形態において、パケットヘッダ暗号鍵は、ルート識別子をセキュア通信アプリケーションのノード識別子と合成し、両方のデータセットを鍵導出関数に通すことによって計算される。ブロック８３５において、送信側セ

キュア通信アプリケーションが、短期鍵対（ＫＥｓ、ＰＫＥｓ）を生成する。ブロック８４０において、送信側セキュア通信アプリケーションが、受信者ノードごとに鍵暗号化鍵（ＫＥＫ）を計算する。鍵暗号化鍵は、

【数１】

$$KEK=KDF\left(DH\left(KE_{s}、PKE_{n}\right)\|ID_{n\_r}\right)$$

に従って計算される。これに関して、送信側セキュア通信アプリケーションは、送信側セキュア通信アプリケーションが生成した短期秘密鍵と、セキュア通信プラットフォームから受信された受信側ノードの短期公開鍵とを用いて共有秘密鍵（shared secret）を導出する。好ましい実施形態において、共有秘密鍵はディフィーヘルマン（Diffie-Hellman）に従って導出される。共有秘密鍵及び受信側ノードのノード識別子を鍵導出関数に入力して、通信を受信者のセキュアコラボレーションアプリケーションに実効的に結び付ける鍵暗号化鍵を導出する。これは、受信側ノードだけが通信にアクセスできるようにすることによって、セキュリティを改善する。すなわち、鍵暗号化鍵を生成するために使用される鍵は、セキュア通信アプリケーションの特定のインストールに固有であるので、受信者は、デバイス間で通信を転送できなくなるが、それでもメッセージを解読することができる。ブロック８４０は、１つ以上の受信者のデバイスごとに繰り返される。

【００５２】

１つ以上の受信者のデバイスごとに鍵暗号化鍵を計算した後に、ブロック８４５において、送信側セキュア通信アプリケーションが受信者ノードごとに鍵交換データを作成する。鍵交換データは、受信者ノードのための鍵暗号化鍵で暗号化されたランダムメッセージペイロード暗号鍵（Ｋｐａｙｌｏａｄ）と、送信側ノードのノード識別子と、受信側ノードの短期公開鍵に割り当てられた固有識別子（ＩＤｋｅｎ）とを含む。したがって、ブロック８４５は、受信者ノードごとに繰り返されることになる。

【００５３】

ブロック８５０において、送信側セキュア通信アプリケーションが、受信者ノードごとの鍵交換リストを作成する。例えば、セキュア通信アプリケーションは、ブロック８４５において生成された情報の鍵交換データブロブのそれぞれを合成して、鍵交換リストを作成することができる。ブロック８５５において、送信側セキュア通信アプリケーションが、暗号化されたパケットヘッダを生成する。これに関して、送信側セキュア通信アプリケーションは、鍵交換リスト及び送信者の短期公開鍵をヘッダ暗号鍵で暗号化することによって、暗号化されたパケットヘッダを作成する。好ましい実施形態において、鍵交換リスト及び送信者の短期公開鍵は、ＡＥＳ等の対称暗号化アルゴリズムによって暗号化される。

【００５４】

暗号化されたパケットヘッダを生成した後に、送信側セキュア通信アプリケーションは、送信するためのパケットコンテンツを準備し始める。ブロック８６０において、送信側セキュア通信アプリケーションは、通信メタデータを作成する。通信メタデータは、通信に含まれるコンテンツのタイプを識別することができる。さらに、通信メタデータは、通信の短期性を含みうる。すなわち、送信者は、通信のための有効生存期間を指定することができる。有効生存期間が満了した後、受信側ノードは、通信にアクセスできなくなる。

【００５５】

ブロック８６５において、送信側セキュア通信アプリケーションが、暗号化されたメッセージペイロードを作成する。暗号化されたメッセージペイロードは、ランダムメッセージペイロード暗号鍵を用いて、対称暗号化アルゴリズムによって、メッセージメタデータ及びメッセージコンテンツを暗号化することによって作成される。ブロック８７０において、送信側セキュア通信アルゴリズムがパケット署名を作成する。パケット署名は、署名生成アルゴリズムに従って、暗号化されたパケットヘッダ及び暗号化されたメッセージペイロードにノード識別秘密鍵を適用することによって生成される。ブロック８７５において

、送信側セキュア通信アプリケーションが、バージョン情報、暗号構成情報、暗号化されたパケット、暗号化されたパケットヘッダ及びパケット署名を含む、シリアライズされたパケットを作成する。ブロック８８０において、送信側セキュア通信アプリケーションが、シリアライズされたパケットを、１つ以上の受信者ノードに配信するために、セキュア通信プラットフォームに送信する。このようにして、セキュア通信プラットフォームは、単一のパケットを受信し、単一のパケットを１つ以上の受信者ノードに配信する。

【００５６】

セキュア通信プラットフォームは、１つ以上の受信側ノードのそれぞれに、受信側ノードが新たな通信を受信したという、プッシュ通知等のアラートを与える。セキュア通信アプリケーションは、セキュア通信プラットフォームと交信し、新たな通信をそれらのデバイスにダウンロードする。図９Ａ及び図９Ｂは、受信側ノードにおいて、暗号化された通信を受信し、解読するための方法９００を示す。

【００５７】

ブロック９０５において、受信者ノードが、送信側ノードから、シリアライズされたパケットを受信する。シリアライズされたパケットを受信することは、アラート又は通知を受信するのに応答して、セキュア通信プラットフォームからシリアライズされたパケットを検索することを含む。さらに、受信者ノードは、通信コンテンツを解読するのに適した鍵材料を識別する責任を担う。このために、ブロック９１０において、受信側ノードがセキュア通信プラットフォームから送信側ノードについての情報を取得する。その情報は、送信側ノードの識別子（ＩＤｎ＿ｓ）、そのノードのルートの識別子（ＩＤｒ＿ｓ）及び送信側ノードのユーザプロファイル情報を含む。

【００５８】

通信及び送信者についての情報を取得した後に、ブロック９１５において、受信側ノード上のセキュア通信アプリケーションが、パケットをデシリアライズし、適切なバージョン及び暗号構成を設定する。ブロック９２０において、受信側ノード上のセキュア通信アプリケーションが、パケット署名を検証する。これに関して、暗号化されたパケットヘッダ及び暗号化されたパケットペイロードの署名が認証され、ノード識別公開鍵の署名がルート識別公開鍵を用いて検証され、ルート識別公開鍵は予想されるユーザ識別に対応する。署名のうちのいずれかが無効である場合には、受信側ノード上のセキュア通信アプリケーションは、受信されたパケットを解読するのを中止し、そのパケットを破棄することができる。代わりに、受信側ノード上のセキュア通信アプリケーションは、解読プロセスを継続し、通信のコンテンツを検証できなかったという通知をユーザに与えることができる。署名が正当であると確認された場合には、受信側ノードのセキュア通信アプリケーションは解読プロセスを継続する。

【００５９】

ブロック９２５において、受信側ノード上のセキュア通信アプリケーションが、セキュア通信プラットフォームから受信された送信者のプロファイル情報から、パケットヘッダ暗号鍵（Ｋｈｅａｄｅｒ）を計算する。上記で論じられたように、パケットヘッダ暗号鍵は、送信者のルート識別子（ＩＤｒ＿ｓ）及び送信者のノード識別子（ＩＤｎ＿ｓ）から導出される。ブロック９３０において、受信側ノードのセキュア通信アプリケーションが、導出されたパケットヘッダ暗号鍵を用いてパケットヘッダを解読し、送信者の短期公開鍵（ＰＫＥｓ）及び鍵交換リストを取得する。

【００６０】

ブロック９３５において、受信側ノードのセキュア通信アプリケーションが、ノード識別子（ＩＤｎ＿ｒ）を用いて、解読された鍵交換リストから鍵交換データを検索する。具体的には、受信側ノードは、暗号化されたペイロード鍵（ＥＫＥＫ（Ｋｐａｙｌｏａｄ））、受信側ノードのノード識別子（ＩＤｎ）及び受信側ノードの短期公開鍵の固有識別子（ＩＤｋｅｎ）を取得する。ブロック９４０において、受信側ノードのセキュア通信アプリケーションが、固有識別子（ＩＤｋｅｎ）を用いて、受信側ノード上のローカル記憶装置から鍵交換のために送信側ノードによって使用された短期鍵対（ＫＥｎ、ＰＫＥｎ）を識

別し、検索する。
【００６１】
記憶装置から短期鍵対を取得した後に、ブロック９４０において、受信側ノード上のセキュア通信アプリケーションが鍵暗号化鍵を計算する。具体的には、受信側ノードは、受信側ノードの短期秘密鍵及び送信側ノードの短期公開鍵を用いて、共有秘密鍵を計算する。共有秘密鍵及び受信側ノードのノード識別子を鍵導出関数に入力して、鍵暗号化鍵を生成する。ブロック９４５において、受信側ノードのセキュア通信アプリケーションが、暗号化されたペイロード暗号鍵を解読する。ブロック９５０において、解読されたペイロード暗号鍵を用いて、メッセージを解読する。詳細には、セキュア通信アプリケーションは、解読されたメッセージから、メッセージメタデータ及びメッセージコンテンツを取得する。ブロック９５５において、受信側ノードのセキュア通信アプリケーションが、解読されたメッセージをユーザに与える。ブロック９６０において、メッセージペイロードが、受信側ノードのローカル記憶デバイス鍵で暗号化され、受信側ノード上のローカル記憶装置内に記憶される。
【００６２】
メッセージコンテンツが解読された直後に、送信者及び受信者の短期鍵対及びペイロード暗号鍵等の、持続期間が短い鍵が削除される。セキュア通信アプリケーションは、メッセージメタデータに従って動作を実行することになる。例えば、暗号化された各メッセージは、満了時間又は有効生存期間（ＴＴＬ）値に関連付けられる場合があり、その時間以降、セキュア通信アプリケーションはメッセージを削除しなければならない。したがって、セキュア通信アプリケーションは、満了時間又はＴＴＬ値を強制し、それが満了した後にメッセージを削除することになる。
【００６３】
図１０は、第１のユーザと第２のユーザとの間の終端間暗号化通信のためのモバイルインターフェース１０００の一例を示す。インターフェース１０００はタイトルフィールド１０１０を含む。ユーザがセキュアチャットルームに参加しているとき、セキュアチャットルームのタイトルが表示されることになる。同様に、ユーザが一対一通信に参加しているとき、他方の参加者の名前が表示されることになる。インターフェース１０００は、テキスト検索を実行する能力をユーザに提供する検索フィールド１０２０を含みうる。さらに、インターフェース１０００は、ユーザが安全な音声通話又はビデオ通話に参加できるようにする通話オプションフィールド１０３０を含みうる。インターフェース１０００は、着信及び発信する通信を表示するテキストウィンドウ１０４０と、テキストを入力し、ファイルをアップロードするテキストインターフェース１０５０とを含む。
【００６４】
図１１は、２つのユーザ間の終端間暗号化通信のためのデスクトップインターフェース１１００の説明のための例を示す。インターフェースルーム１１００がフィールド１１０５内にユーザ情報を表示する。これに関して、インターフェース１１００は、フィールド１１０５によって示されるようなＶｅｒｎｉｃｉｏｕｓ　Ｋｎｉｄｓに属する。フィールド１１１０は、ユーザがその参加者であるセキュアチャットルームを表示し、一方、フィールド１１１５はユーザの一対一通信を示す。例示されるように、Ａｒｔｈｕｒ　Ｓｌｕｇｗｏｒｔｈの名前がハイライトされ、Ａｒｔｈｕｒ　Ｓｌｕｇｗｏｒｔｈとの一対一通信が表示されることを示す。これは、他方のユーザの名前を表示するヘッダフィールド１１３０内にも表示される。セキュアチャットルームが選択された場合には、ヘッダフィールド１１３０がセキュアチャットルームの名前を表示することになる。さらに、インターフェース１１００は、検索フィールド１１３５、ＴＴＬステータスフィールド１１４０及び通話オプションフィールド１１４５を含みうる。検索フィールド１１３５は、インターフェース１１００内で行われる通信のためのテキスト検索を行う能力をユーザに提供する。ＴＴＬステータスフィールド１１４０は、ユーザが、セキュアチャットルームにおいて送信されるメッセージの満了時間を変更できるようにする。通話オプションフィールド１１４５は、ユーザが、暗号化された音声通話又はビデオ通話に参加できるようにする。また

、インターフェース１１００は、着信及び発信する通信を表示するテキストウィンドウ１１４５を含む。最後に、インターフェース１１００は、ユーザがテキストを入力し、ファイルをアップロードできるようにするウィンドウ１１５０を含む。

【００６５】

上記の実施形態は、明確に理解してもらうために幾らか詳細に説明されてきたが、本開示は、提供される細部に限定されない。本開示を実施する数多くの代わりの方法がある。開示される実施形態は例示であり、限定するものではない。

【図面】

【図１】

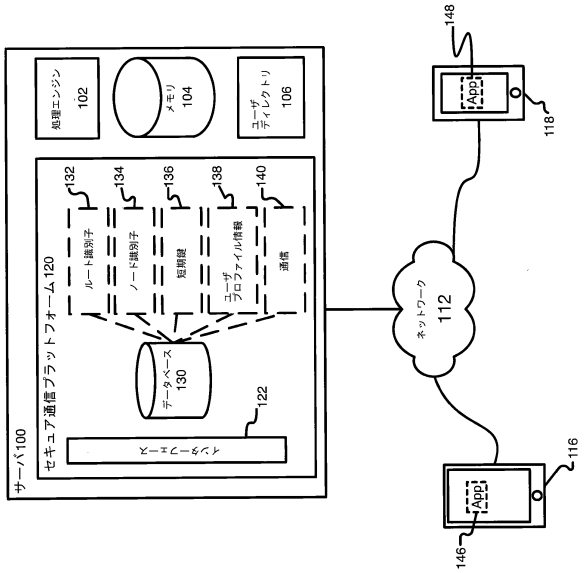
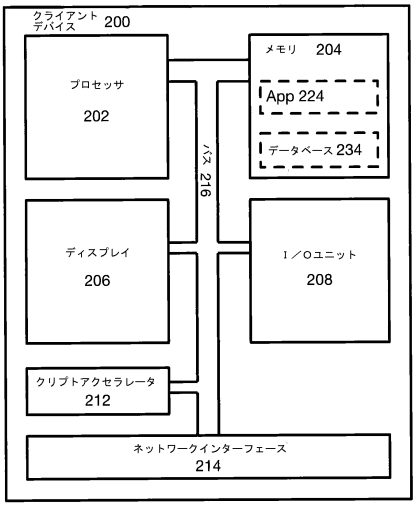


FIG. 1

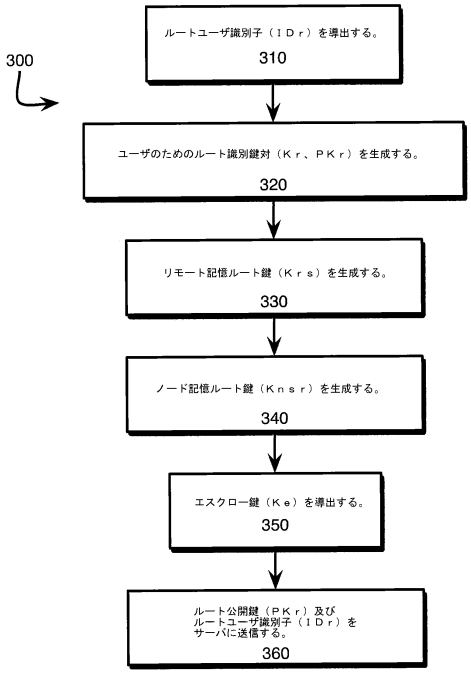
【図２】

FIG. 2



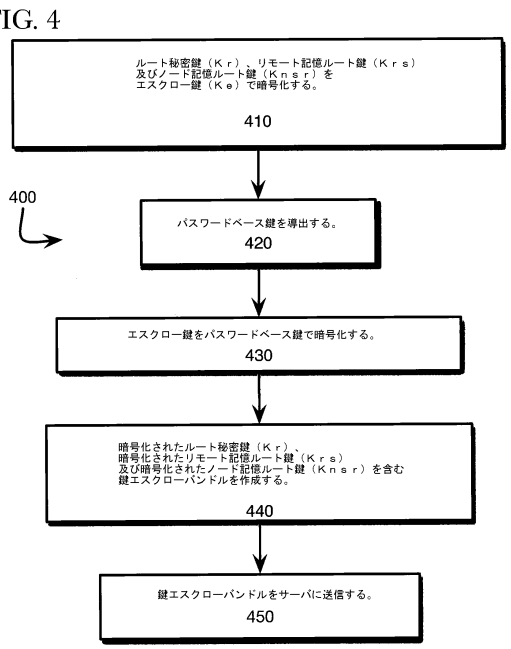
【図３】

FIG. 3



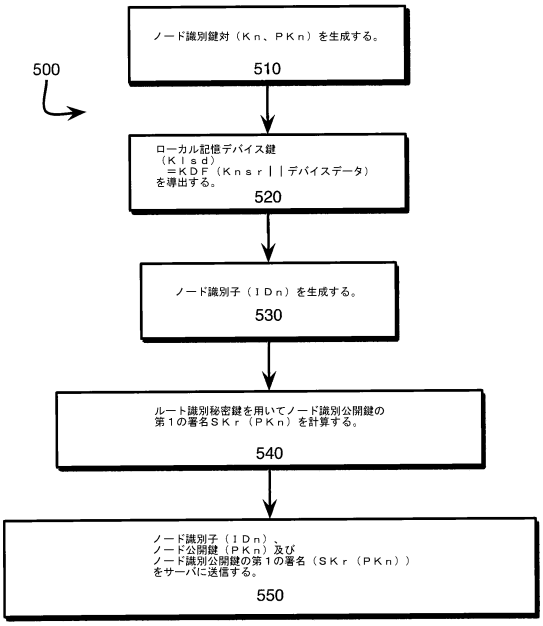
【図４】

FIG. 4



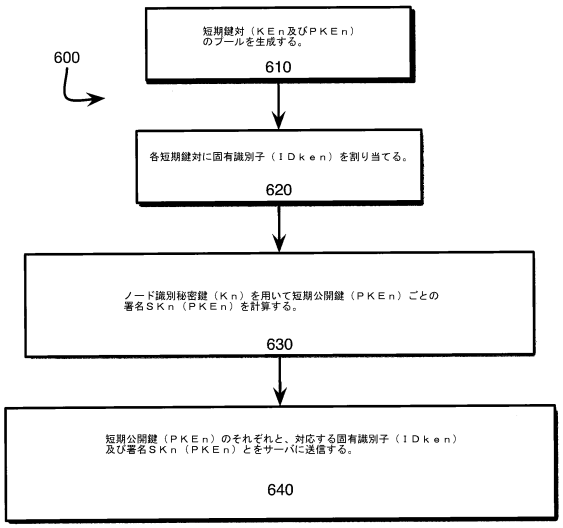
【図５】

FIG. 5



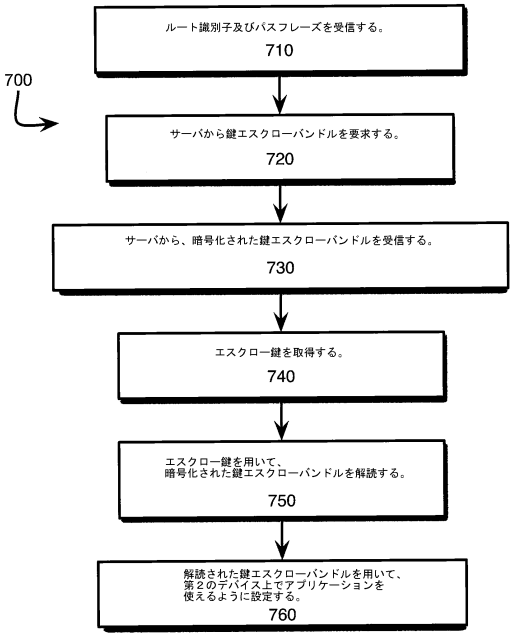
【図６】

FIG. 6



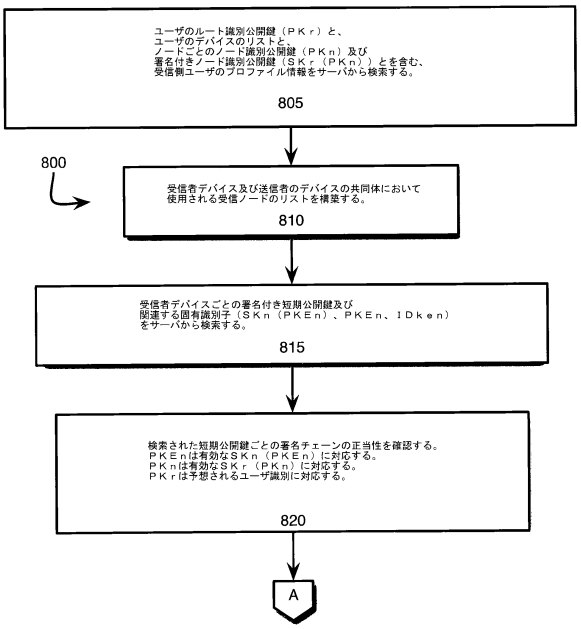
【図７】

FIG. 7



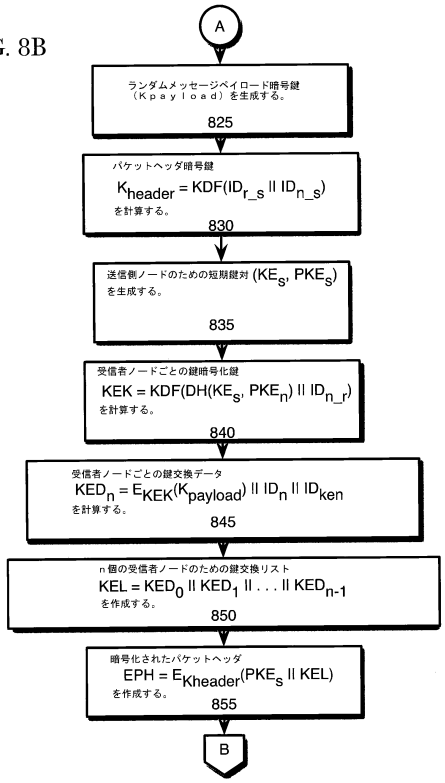
【図８Ａ】

FIG. 8A



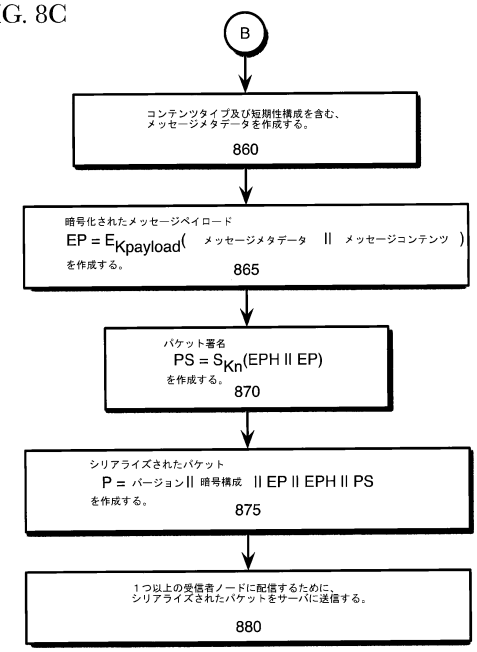
【図８Ｂ】

FIG. 8B



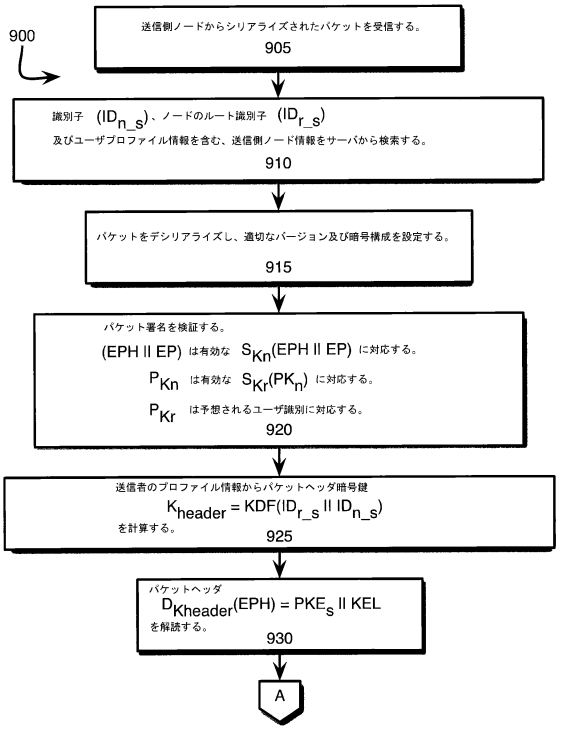
【図８Ｃ】

FIG. 8C



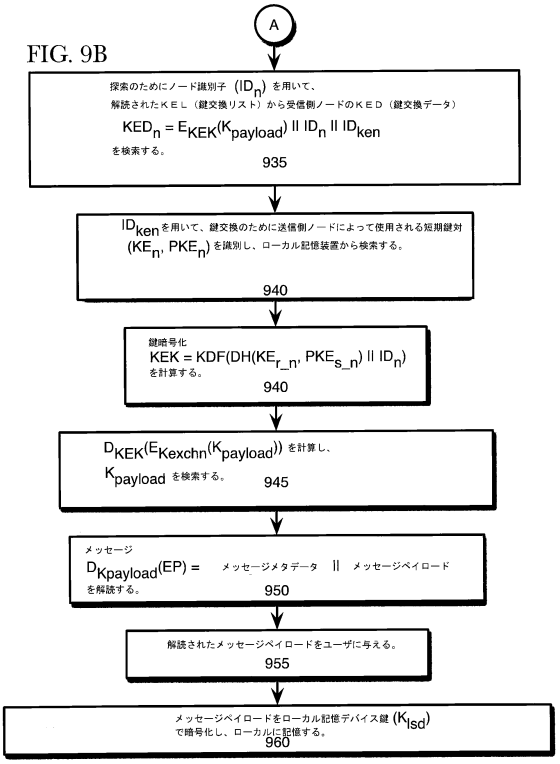
【図９Ａ】

FIG. 9A



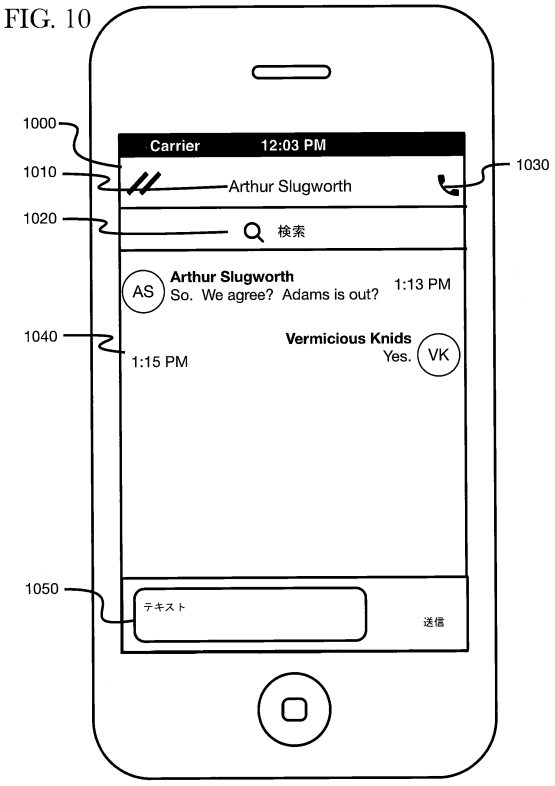
【図９Ｂ】

FIG. 9B



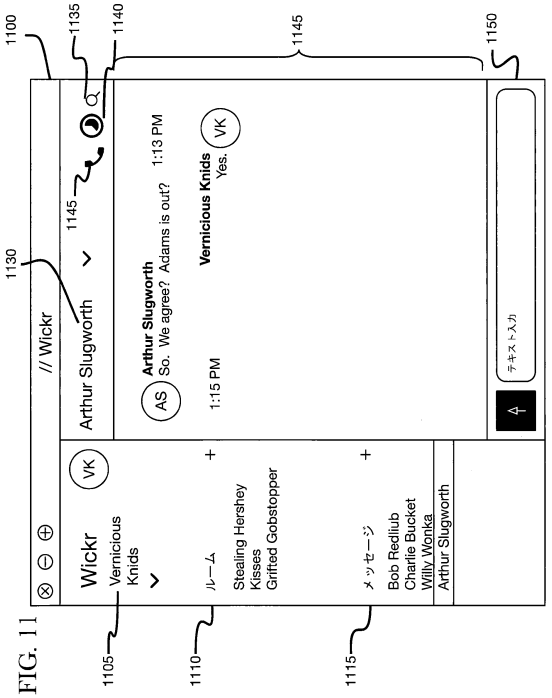
【図１０】

FIG. 10



【図１１】

FIG. 11



フロントページの続き

(74)代理人　100142996
弁理士　森本 聡二
(74)代理人　100166268
弁理士　田中 祐
(74)代理人　100180231
弁理士　水島 亜希子
(74)代理人　100096769
弁理士　有原 幸一
(72)発明者　トーマス・マイケル・リーヴィ
アメリカ合衆国ニューヨーク州１０００１，ニュー・ヨーク，ウェスト・サーティーファースト・ストリート ２５４，サード・フロア
(72)発明者　クリストファー・エイ・ハウエル
アメリカ合衆国ニューヨーク州１０００１，ニュー・ヨーク，ウェスト・サーティーファースト・ストリート ２５４，サード・フロア
審査官　松平 英
(56)参考文献　米国特許出願公開第２０１６／００７２７８５（ＵＳ，Ａ１）
米国特許出願公開第２０１５／００５２３５９（ＵＳ，Ａ１）
特開平１１－２０２７６５（ＪＰ，Ａ）
特表２００９－５１５３９３（ＪＰ，Ａ）
特開２００５－２０８８４１（ＪＰ，Ａ）
特開２００７－５２６３３（ＪＰ，Ａ）
(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ１２／１４
２１／００－２１／８８
Ｇ０９Ｃ １／００－５／００
Ｈ０４Ｋ １／００－３／００
Ｈ０４Ｌ ９／００－９／４０