(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2008-506317
(P2008-506317A)
(43)公表日　平成20年2月28日(2008.2.28)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 9/08	(2006.01)	H04L	9/00	601B	5B285
G06F 21/20	(2006.01)	H04L	9/00	601E	5J104
		G06F	15/00	330A	

審査請求 未請求　予備審査請求 未請求　（全 30 頁）

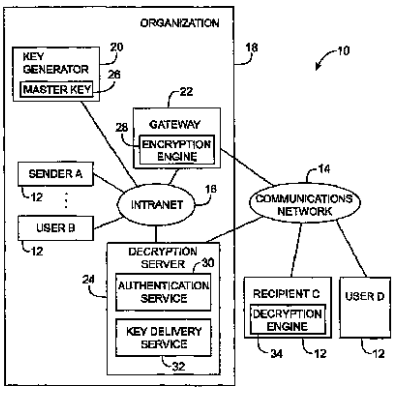
(21)出願番号　特願2007-520503 (P2007-520503)
(86)(22)出願日　平成17年7月5日(2005.7.5)
(85)翻訳文提出日　平成19年2月26日(2007.2.26)
(86)国際出願番号　PCT/US2005/024136
(87)国際公開番号　WO2006/007601
(87)国際公開日　平成18年1月19日(2006.1.19)
(31)優先権主張番号　10/887,721
(32)優先日　平成16年7月9日(2004.7.9)
(33)優先権主張国　米国(US)

(71)出願人　505295547
ボルテージ　セキュリティー，　インコーポレイテッド
アメリカ合衆国　カリフォルニア　９４３０４，　パロ　アルト，　アラストラデロ　ロード　１０７０，　スイート　１００
(74)代理人　100078282
弁理士　山本　秀策
(74)代理人　100062409
弁理士　安村　高明
(74)代理人　100113413
弁理士　森下　夏樹

最終頁に続く

(54)【発明の名称】導出鍵を用いたセキュアメッセージングシステム

(57)【要約】
対称メッセージ鍵を使用して、送信者と受信者との間で安全なメッセージ送信を行うことができる。対称メッセージは、組織において、鍵生成器を使用してマスター鍵から導出することができる。ゲートウェイは、導出鍵を使用して、発信メッセージを暗号化することが可能である。組織内の送信者は、組織の顧客である受信者にメッセージを送信することができる。受信者は、予め制定した信用証明書を使用して、組織内の暗号解読サーバーに対して認証を行うことができる。受信者には、暗号化メッセージを解読するための導出鍵のコピーが提供される。階層的アーキテクチャは、組織においてスーパーマスター鍵生成器が、組織の異なるユニット内の委譲鍵生成器に対するマスター鍵を導出するのに使用することが可能である。組織は、非顧客の対称メッセージ鍵を生成する、ポリシーサーバーを有することが可能である。



【特許請求の範囲】
【請求項１】
組織において、送信者が、通信ネットワークを通じて、前記組織の顧客である受信者にメッセージを送信するための方法であって、前記受信者は、受信者アイデンティティ（ＩＤ）を有し、前記方法は、
前記組織において、一方向関数であって、前記一方向関数の入力がマスター鍵および前記受信者ＩＤを含む、一方向関数を使用して、前記マスター鍵から前記メッセージを暗号化するための対称鍵を導出するステップと、
前記組織において、前記導出対称鍵を使用して前記メッセージを暗号化し、前記通信ネットワークを通じて、前記受信者に前記メッセージを送信するステップと、
前記受信者において、前記暗号化メッセージを受信するステップと、
前記受信者において、前記通信ネットワークを通じて、前記組織に導出対称鍵の要求をサブミットするステップであって、前記導出対称鍵の要求は前記受信者ＩＤを含む、ステップと、
前記通信ネットワークを通じて、前記組織に対して前記受信者を認証し、前記組織と前記受信者との間に安全な通信チャネルを確立するステップと、
前記受信者の前記導出対称鍵の要求に応えて、前記受信者が前記メッセージの解読において使用する前記導出対称鍵を生成して、前記安全な通信チャネルを通じて、前記受信者に前記導出対称鍵を提供するステップと、
を含む、方法。
【請求項２】
前記対称鍵を導出するステップは、前記対称鍵を導出するために、ハッシュ関数を使用するステップを含む、請求項１に記載の方法。
【請求項３】
前記対称鍵を導出するステップは、前記対称鍵を導出するために、デジタル署名機能を使用するステップを含む、請求項１に記載の方法。
【請求項４】
前記組織はゲートウェイを有し、前記メッセージを暗号化するステップは、前記ゲートウェイにおいて前記メッセージを暗号化するために、前記導出対称鍵を使用するステップを含む、請求項１に記載の方法。
【請求項５】
前記組織はゲートウェイおよび鍵生成器を有し、前記メッセージを暗号化するステップは、
前記組織において前記鍵生成器に前記受信者ＩＤを含む導出鍵の要求を提供するために、前記組織において前記ゲートウェイを使用するステップと、
前記ゲートウェイからの前記導出鍵の要求に応えて、前記一方向性関数を使用して、前記導出鍵を計算するために、前記鍵生成器を使用するステップと
を含む、請求項１に記載の方法。
【請求項６】
前記組織は、サーバーおよび鍵生成器を有し、前記組織に対して前記受信者を認証するステップは、前記受信者を認証するために前記サーバーを使用するステップを含み、前記受信者が前記メッセージの解読において使用する前記導出対称鍵を生成するステップは、前記サーバーからの導出鍵の要求に応えて、前記受信者に対する前記導出対称鍵を生成するために、前記鍵生成器を使用するステップを含む、請求項１に記載の方法。
【請求項７】
前記組織は暗号解読サーバーおよび鍵生成器を有し、前記通信ネットワークを通じて、前記受信者を認証し、前記組織と前記受信者との間に安全な通信チャネルを確立するステップは、前記暗号解読サーバーに対して前記受信者を認証し、前記暗号解読サーバーと前記受信者との間にセキュアソケットレイヤー（ＳＳＬ）リンクを確立するために、前記暗号解読サーバーを使用するステップを含み、前記受信者が前記メッセージの解読において

使用する前記導出対称鍵を生成するステップは、前記暗号解読サーバーからの導出鍵の要求に応えて、前記受信者に対する前記導出対称鍵を生成するために、前記鍵生成器を使用するステップを含み、前記受信者に暗号解読鍵を提供するステップは、前記ＳＳＬリンクを通じて、前記鍵生成器から前記受信者に前記暗号解読鍵を提供するために、前記暗号解読サーバーを使用するステップを含む、請求項１に記載の方法。

【請求項８】

組織において、送信者が受信者にメッセージを送信するための方法であって、前記組織は、ゲートウェイと、鍵生成器と、サーバーと、前記送信者、前記ゲートウェイ、前記鍵生成器、および前記サーバーが接続されるイントラネットと、を有し、前記受信者は、前記組織外にあり、前記受信者は、前記組織の顧客であり、前記受信者は、受信者アイデンティティ（ＩＤ）を有し、前記方法は、

ＨＭＡＣ関数であって、前記ＨＭＡＣ関数の入力がマスター鍵および前記受信者ＩＤを含む、ＨＭＡＣ関数を使用して、前記マスター鍵から前記メッセージを暗号化するための対称鍵メッセージを導出するために、前記鍵生成器を使用するステップと、

前記イントラネットを通じて、前記鍵生成器から前記ゲートウェイに前記導出対称鍵を提供するステップと、

暗号化メッセージを生成するために、前記導出対称鍵を使用して、前記ゲートウェイにおいて前記メッセージを暗号化するステップと、

インターネットを通じて、前記ゲートウェイから前記組織外の前記受信者に前記暗号化メッセージを提供するステップと、

前記受信者において、暗号化メッセージを受信するステップと、

前記サーバーに対して前記受信者を認証し、前記サーバーと前記受信者との間にセキュアソケットレイヤー（ＳＳＬ）リンクを確立するステップと、

前記受信者から前記サーバーに導出対称鍵の要求を提供するステップであって、前記導出対称鍵の要求は前記受信者ＩＤを含む、ステップと、

前記受信者ＩＤを使用して、前記イントラネットを通じて、前記鍵生成器から前記導出対称鍵を取得し、前記ＳＳＬリンクを通じて、前記鍵生成器から取得した前記導出対称鍵を前記受信者に提供するために、前記サーバーを使用するステップと、

前記受信者において、前記暗号化メッセージを解読するために、前記ＳＳＬリンクを通じて、前記サーバーによって提供された導出対称鍵を使用するステップと

を含む、方法。

【請求項９】

一方向性関数を使用して、スーパーマスター鍵から前記マスター鍵を導出するステップをさらに含む、請求項８に記載の方法。

【請求項１０】

複数のユニットを有する組織に対する安全な通信をサポートするために、階層的鍵生成器アーキテクチャを使用するための方法であって、前記組織は、スーパー鍵生成器と、複数の委譲鍵生成器と、を有し、前記方法は、

スーパーマスター鍵から複数の導出サブマスター鍵を生成するために、前記スーパー鍵生成器を使用するステップであって、各導出サブマスター鍵は、前記複数のユニットのうちのそれぞれ１つにおいて、前記委譲鍵生成器のうちのそれぞれ１つに提供される、ステップと、

前記ユニットのうちの所与の１つのユニットにおいて、前記所与のユニット内の送信者に、前記所与のユニットの顧客である前記組織外の受信者に安全に通信されるメッセージの作成を許可するステップであって、前記受信者は受信者アイデンティティ（ＩＤ）を有する、ステップと、

前記所与のユニットにおいて、一方向性関数であって、前記一方向性関数の入力がサブマスター鍵および前記受信者ＩＤを含む一方向性関数を使用して、その委譲鍵生成器に提供された前記サブマスター鍵からメッセージを暗号化するための対称鍵を導出するために、その所与のユニットの前記委譲鍵生成器を使用するステップと、

前記所与のユニットにおいて、前記導出対称鍵を使用して前記メッセージを暗号化し、通信ネットワークを通じて、前記受信者に前記メッセージを送信するステップと、
前記受信者において、前記暗号化メッセージを受信するステップと、
前記受信者において、前記通信ネットワークを通じて、前記所与のユニットに導出対称鍵の要求をサブミットするステップであって、前記導出対称鍵の要求は前記受信者ＩＤを含む、ステップと、
前記通信ネットワークを通じて、前記所与のユニットに対して前記受信者を認証し、前記所与のユニットと前記受信者との間に安全な通信チャネルを確立するステップと、
前記受信者が前記メッセージの解読において使用する前記導出対称鍵を生成するために、前記所与のユニットの前記委譲鍵生成器を使用して、前記安全な通信チャネルを通じて、前記受信者に前記所与のユニットからの前記導出対称鍵を提供するステップと
を含む、方法。
【請求項１１】
前記所与のユニットは、暗号解読サーバーを有し、前記所与のユニットに対して前記受信者を認証するステップは、予め制定した受信者信用証明書を使用して、前記暗号解読サーバーに対して前記受信者を認証するステップを含む、請求項１０に記載の方法。
【請求項１２】
前記メッセージを暗号化するステップは、前記送信者において、前記メッセージを暗号化するステップを含む、請求項１０に記載の方法。
【請求項１３】
前記導出対称鍵の要求をサブミットするステップは、前記所与のユニットの前記委譲鍵生成器の識別名を含む要求をサブミットするステップを含む、請求項１０に記載の方法。
【請求項１４】
前記スーパーマスター鍵から複数の導出サブマスター鍵を生成するステップは、前記スーパーマスター鍵および各ユニットに関連する名前を入力として使用して、ＨＭＡＣ関数に対する値を計算するステップを含む、請求項１０に記載の方法。
【請求項１５】
対称鍵の暗号技術を使用して、組織外の送信者と、組織内または前記組織の顧客である受信者との間の安全な通信をサポートする方法であって、
前記送信者と前記組織との間に安全な通信チャネルを確立するステップと、
前記組織において、マスター鍵から対称鍵を導出するステップと、
前記組織において、乱数Ｎを生成するステップと、
前記組織において、前記導出対称鍵および前記乱数Ｎに基づいて、非顧客対称メッセージ鍵を生成するステップと、
前記安全な通信チャネルを通じて、前記送信者に、前記非顧客対称メッセージ鍵および前記乱数Ｎを提供するステップと、
前記送信者において、前記受信者に対するメッセージを暗号化するために、前記非顧客対称メッセージ鍵を使用するステップと
を含む、方法。
【請求項１６】
前記送信者において、前記メッセージを暗号化するステップは、暗号文を生成し、前記方法は、前記組織外の前記送信者から前記受信者に前記暗号化メッセージを送信するステップをさらに含み、送信される前記暗号化メッセージは、前記暗号文および前記乱数Ｎを含む、請求項１５に記載の方法。
【請求項１７】
前記送信者において前記メッセージを暗号化するステップは、暗号文を生成し、前記方法は、
前記組織外の前記送信者から前記受信者に前記暗号化メッセージを送信するステップであって、送信される前記暗号化メッセージは、前記暗号文および前記乱数Ｎを含む、ステップと、

前記受信者において、前記非顧客メッセージ鍵を取得するために、前記乱数Ｎを使用するステップと
をさらに含む、請求項１５に記載の方法。
【請求項１８】
前記組織は、サーバーを有し、前記受信者は、受信者ＩＤを有し、前記送信者において前記メッセージを暗号化するステップは、暗号文を作成し、前記方法は、
前記組織外の前記送信者から前記受信者に前記暗号化メッセージを送信するステップであって、送信される前記暗号化メッセージは、前記暗号文および前記乱数Ｎを含む、ステップと、
前記受信者において、前記サーバーから前記非顧客メッセージ鍵を取得する際に、前記乱数Ｎを受信して、前記受信者ＩＤおよび前記乱数Ｎを使用するステップと
をさらに含む、請求項１５に記載の方法。
【請求項１９】
前記組織は、サーバーおよび鍵生成器を有し、前記受信者は、受信者ＩＤを有し、前記送信者において前記メッセージを暗号化するステップは、暗号文を生成し、前記方法は、
前記組織外の前記送信者から前記受信者に前記暗号化メッセージを送信するステップであって、送信される前記暗号化メッセージは、前記暗号文および前記乱数Ｎを含む、ステップと、
前記受信者において、前記サーバーから前記非顧客メッセージ鍵を要求するために、前記乱数Ｎを受信して、前記受信者ＩＤおよび前記乱数Ｎを使用するステップと、
前記サーバーにおいて、前記鍵生成器から前記導出対称鍵を取得するために、前記受信者ＩＤを使用して、前記鍵生成器からの前記導出対称鍵および前記受信者からの前記乱数Ｎを使用して、前記受信者に対する前記非顧客メッセージ鍵を計算するステップと
をさらに含む、請求項１５に記載の方法。
【請求項２０】
前記受信者は、受信者ＩＤを有し、前記マスター鍵から前記対称鍵を導出するステップは、前記導出対称鍵を生成するために、前記マスター鍵および受信者ＩＤにＨＭＡＣ関数を適用するステップを含む、請求項１５に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本願は、米国特許出願第１０／８８７，７２１号（２００４年７月９日出願）の優先権を主張する。
【０００２】
本発明は、暗号システムに関し、より詳しくは、導出鍵を使用した暗号システムに関する。
【背景技術】
【０００３】
電子メールメッセージのような敏感な電子通信の暗号化が望ましいことがしばしばある。
【０００４】
公開鍵暗号システムでは、２種類の鍵（公開鍵および秘密鍵）が使用される。送信者は、受信者の公開鍵を使用して、メッセージを暗号化することが可能である。各受信者は、その受信者に対するメッセージの解読に使用される、秘密鍵を有する。
【０００５】
対称鍵暗号機構では、メッセージの送信者は、メッセージの受信者がそのメッセージの解読に使用するものと同じ鍵を、そのメッセージの暗号化に使用する。対称鍵の暗号技術の利点は、対称鍵暗号化および暗号解読アルゴリズムが、計算上効率的なことである。
【０００６】
安全なメッセージの送信者および受信者は、多くの場合組織との既存の関係がある。例

えば、銀行は、その顧客の預金取引明細書を安全に送信したいと望む場合がある。別の例では、暗号化された預金取引明細書を受信する顧客は、問い合わせるために安全な電子メールメッセージをその銀行に返信したいと望む場合がある。

【発明の開示】

【発明が解決しようとする課題】

【０００７】

本発明の目的は、対称鍵を使用して安全な通信を容易にする、メッセージングシステムを提供することにある。

【課題を解決するための手段】

【０００８】

対称メッセージ鍵を使用して、送信者と受信者との間で安全なメッセージを送信することができる。組織は、マスター鍵から対称メッセージ鍵を導出する、鍵生成器を有することもある。鍵生成器は、マスター鍵および受信者のアイデンティティ情報（すなわち、受信者ＩＤ）に、ＨＭＡＣ関数のような一方向性関数または他のハッシュ関数を適用することによって、導出鍵を生成することができる。得られた導出鍵は、各受信者に固有である。導出鍵に障害が生じても、マスター鍵には障害は生じず、セキュリティの確保を支える。

【０００９】

送信者は、組織の顧客である受信者に対するメッセージを暗号化するために、導出鍵を使用することが可能である。受信者はその組織の顧客であるので、受信者と組織との間には既存の関係がある。したがって、その組織は、受信者を認証するために使用することができる、受信者の信用証明情報を有する。

【００１０】

受信者が暗号化メッセージを受信するとき、受信者は、組織に対して認証することができ、またそのメッセージを解読するために、導出鍵のコピーを要求することができる。導出鍵の要求は、受信者ＩＤを含む。受信者からの鍵要求が提供される受信者ＩＤは、導出鍵の新しいコピーを導出するために、鍵生成器により使用されることが可能である。この導出鍵の新しいコピーは、次いで安全な通信チャネルを通じて、受信者に提供することが可能である。受信者は、受信した導出鍵のコピーで暗号化メッセージを解読するために、受信者の装置上の暗号解読エンジンを使用することが可能である。

【００１１】

階層的鍵生成器のアーキテクチャは、複数の組織的ユニットを有する組織に対して使用することができる。各ユニットは、そのユニット内の送信者に対する導出対称鍵を生成する、委譲鍵生成器をそれぞれ有してもよい。組織は、スーパーマスター鍵を有する、スーパー鍵生成器を有することができる。スーパー鍵生成器は、各委譲鍵生成器に対するサブマスター鍵を導出することができる。

【００１２】

対称鍵の機構はまた、組織の顧客ではない組織外の送信者が、その組織内の受信者にメッセージを送ることができるようにするためにも使用することができる。組織は、マスター鍵および受信者ＩＤに基づいて、導出鍵を作成するための鍵生成器を有することができる。組織内のポリシーサーバーは、非顧客対称鍵を生成する（導出する）ために、導出鍵および乱数Ｎを使用することが可能である。

【００１３】

例えば、鍵生成器は、導出鍵を生成するために、マスター鍵および受信者ＩＤにＨＭＡＣ関数を適用することができる。ポリシーサーバーは、乱数Ｎを生成することが可能であり、また非顧客メッセージ鍵を生成するために、鍵生成器からの導出鍵および乱数Ｎに、ＨＭＡＣ関数を適用することが可能である。

【００１４】

送信者が組織内の受信者にメッセージを送りたい場合は、送信者およびポリシーサーバーは、安全なリンクを確立する。ポリシーサーバーは、安全なリンクを通じて、送信者に

非顧客メッセージ鍵を提供する。送信者は、非顧客メッセージ鍵を使用して、受信者に対するメッセージを暗号化する。送信者は、次いで受信者にＮの値を含む暗号化メッセージを送信する。受信者において、受信者は、ポリシーサーバーから非顧客メッセージ鍵のコピーを取得するために、受信者ＩＤおよびＮの値を使用することができる。受信者は、次いで送信者からの暗号化メッセージを解読することができる。

【００１５】

本発明の更なる特徴、性質、および様々な利点は、添付図面および以下の好適な実施態様の詳細な説明からより明らかになろう。

【発明を実施するための最良の形態】

【００１６】

本発明は、安全なメッセージングをサポートするためのシステムのような、暗号システムに関する。本発明はまた、当該のシステムを使用する方法にも関する。

【００１７】

図１のシステム１０内に示される種類の装置は、送信者と受信者との間の安全な通信をサポートするために使用することができる。送信者は、メッセージを送信するユーザーである。受信者は、メッセージを受信するユーザーである。ユーザーは、概してメッセージの送信および受信の両方を行えるので、所与のユーザーは、ある時には送信者となり、別の時には受信者となりうる。

【００１８】

システム１０内のいくつかのユーザーは、組織１８のような組織に属してもよい。他のユーザーは、異なる組織に属している場合もあれば、いかなる組織にも属していない場合がある。

【００１９】

図１の例では、送信者Ａおよびユーザー Ｂは、組織Ａに属するユーザーである。受信者ＣおよびユーザーＤは、組織Ａに属さないユーザーである。

【００２０】

システム１０内のいくつかのユーザーアクティビティは、人から人へ電子メールメッセージを送信するような、人の手の介入を伴う。例えば、個人的に構成したテキストメッセージを送信したい人は、そのメッセージが暗号化され、適切な受信者に送信される前に、そのメッセージを入力しなければならない。システム１０における他のユーザーアクティビティは、人の介入が概ね不要となるように、完全に自動化されてもよい。一例として、組織は、コンピュータを使用して、その顧客のそれぞれに自動的にメッセージを送信することができる。この種のシナリオでは、コンピュータは、一種のユーザー（すなわちこの例では送信者）としての機能を果たす。以下の説明では、人およびその装置の両方の説明に、「送信者」、「受信者」、および「ユーザー」という用語を使用する。

【００２１】

一例として電子メールメッセージを使用しているが、システムによって運ばれるメッセージは、電子メールメッセージでなくてもよい。メッセージは、電子メールメッセージ、インスタントメッセージ、または他の好適な電子的に伝達されるメッセージであってよい。メッセージには、送信者と受信者との間で電子的に伝達される、あらゆるデジタル情報（例、テキスト、グラフィックス、音声、ビデオ、コマンド、実行コード、データなど）が含まれてもよい。

【００２２】

システム１０内のユーザーは、装置１２を使用して互いに通信することができる。装置１２（およびシステム内の他のエンティティのための装置）には、例えば、パーソナルコンピュータ、ポータブルコンピュータ、ワークステーション、メインフレームコンピュータ、ローカルエリアネットワーク内でホストコンピュータを使用してインターネットに接続されるコンピュータ端末のようなネットワークコンピュータまたは端末、ハンドヘルドコンピュータ、携帯電話、または他の好適な電子装置のような計算機器が挙げられる。

【００２３】

図１の装置は、通信ネットワーク１４およびイントラネット１６内の通信経路によって相互接続することができる。

【００２４】

ネットワーク１４には、インターネットおよび他のワイドエリアネットワーク、１つ以上のイントラネット、ローカルエリアネットワーク、交換電話網、仮想プライベートネットワークのようなネットワーク、専用回線を含むネットワーク、有線または無線経路に基づくネットワーク、または他の好適なネットワーク技術を使用して形成された他のネットワークが挙げられる。

【００２５】

イントラネット１６のようなイントラネットは、特定の組織において、複数のユーザーをネットワーク化するために使用される、通信ネットワークである。例えば、図１のイントラネット１６は、組織１８に関連し、送信者ＡおよびユーザーＢに対する装置１２、鍵生成器２０、ゲートウェイ２２、および暗号解読サーバー２４のような、装置を相互接続するために使用される。イントラネット１６のようなイントラネットは、ローカルエリアネットワークでもワイドエリアネットワークでもよい。小企業の例示的イントラネットは、例えば、ｔｅｎ－ｓｅａｔイーサネット（登録商標）ネットワークとすることができる。大きな組織は、遠く離れた場所において複数のキャンパスを有するとすることができる。当該の組織のイントラネットは、インターネット上で、安全な経路によって互いにリンクされる各キャンパスにおいて、イーサネット（登録商標）ベースのローカルエリアネットワークから構築することができる。

【００２６】

システム１０は、鍵を生成するための、鍵生成器２０のような鍵生成器を有することができる。鍵生成器２０は、複数のユーザー固有の鍵をマスター鍵２６から導出することができる。

【００２７】

メッセージは、暗号化エンジンを使用して暗号化することができ、また暗号解読エンジンを使用して解読することができる。任意の好適な暗号アルゴリズムを、システム１０においてメッセージの暗号化および暗号解読に使用することができる。対称鍵暗号機構であることが好ましい。好適な対称鍵アルゴリズムには、ＡＥＳ（Ａｄｖａｎｃｅｄ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ；高度暗号化規格）、ＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ；データ暗号化規格）、トリプルＤＥＳなどが挙げられる。

【００２８】

１つの好適な機構では、組織１８の送信者からの全てのメッセージは、イントラネット１６およびゲートウェイ２２を介して、ネットワーク１４に転送される。ゲートウェイ２２は、メッセージを暗号化するための、暗号化エンジン２８を有することができる。受信者は、暗号化メッセージを受信した後に、受信者Ｃの暗号解読エンジン３４のような暗号解読エンジンを使用して、そのメッセージを解読することができる。

【００２９】

対称鍵の暗号技術では、暗号化および暗号解読オペレーションの両方に、同じ鍵が使用される。組織１８の外部の受信者Ｃのような受信者は、暗号化エンジン２８が、組織１８への鍵要求を行うことによって、暗号化に使用するゲートウェイ２２において、鍵のコピーを取得することができる。受信者は、鍵を入手すると、そのメッセージを解読して、その内容にアクセスするために、暗号解読エンジン３４のような暗号解読エンジンを使用することができる。

【００３０】

暗号解読サーバー２４は、鍵に対する要求を処理するために使用することができる。認証サービス３０は、ユーザーに要求された鍵が提供される前に、ユーザーを認証するために使用することができる。キー配信サービス３２は、認証された要求元の鍵要求を満たすために使用することができる。

【００３１】
１つの好適なシナリオでは、ユーザーは、電子メールアプリケーション、ウェブブラウザエンジン（すなわち、組み込みのウェブブラウザ機能）を有する電子メールアプリケーション、ウェブブラウザアプリケーション、文書の作成および編集用アプリケーション、画像ビューア、メディアプレーヤなどのような、ソフトウェアアプリケーション（「クライアントソフトウェア」）を有する。暗号化および暗号解読エンジンの機能は、スタンドアロンの暗号化および暗号解読アプリケーションを使用して提供されても、あるいはこれらのアプリケーションと統合された暗号化および暗号解読ソフトウェアコンポーネントを使用して提供されてもよい。一例として、受信者が使用する電子メールプログラムのような電子メールプログラムは、暗号解読エンジンを有することができる。暗号化エンジンは、電子メールアプリケーション内のネイティブコードの一部として提供されても、あるいはプラグインモジュールとして組み込まれてもよい。別の例として、ゲートウェイ２２のようなゲートウェイの管理に使用されるソフトウェアが組み込みの暗号化エンジンを有してもよく、あるいは暗号化エンジンを独立したソフトウェアコンポーネントとして提供してもよい。
【００３２】
様々なコンピュータを、システム１０に使用することが可能である。例えば、計算機器は、各鍵生成器２０、ゲートウェイ２２、および暗号解読サーバー２４において、サーバーまたは他のコンピュータ機器の機能を実行するために使用することができる。サーバーはまた、認証局、メールサーバー、および他のエンティティの機能をサポートするために使用することが可能である。当該のサーバーは、送信者または送信者の組織と同じ場所に配置するか、独立した第三者のサービスとしてネットワーク１４に接続するか、ネットワーク１４のインフラの一部とするか、所与の受信者の組織と関連付けるか、受信者、鍵生成器、または他の装置と同じ場所に配置するか、またはこれらの場所うちの１つ以上で使用することができる。これらは、相互に排他的とする必要のない、単なる例示的機構である。
【００３３】
サーバーは、単一のコンピュータまたは複数のコンピュータを使用して形成することができる。複数のサーバーを、１つのコンピュータ上で実行することができる。必要に応じて、単一のサーバーの機能は、複数の異なる物理的な場所を通じて分配されるコンピュータによって提供することができる。システム１０内のサーバーを使用して実行される機能は、必要に応じて、概して他のコンピュータ機器の構成を使用して実行することができるが、これらの機能を実行するための計算機器は、「サーバー」または「サーバー群」と称することがある。
【００３４】
送信者は、メッセージを、任意の好適なメッセージングフォーマットを使用して、システム１０を通じて、所与の受信者に送信することができる。例えば、電子メールメッセージ、インスタントメッセージ（例、ＡＯＬインスタントメッセージ、Ｙａｈｏｏインスタントメッセージ、ＭＳＮメッセンジャインスタントメッセージ、および、ＩＣＱインスタントメッセージ、ＩＢＭ／Ｌｏｔｕｓセームタイムインスタントメッセージなど）、または他の電子メールメッセージを送信することができる。
【００３５】
システム１０のオペレーション中に、暗号解読サーバー２４のような特定のエンティティは、所与のパーティが、鍵を取得するための、新しいクライアントソフトウェア（例えば、暗号解読アルゴリズムを含む）をダウンロードするための、特定のメッセージの内容にアクセスするための、または他の機能を実行するための許可を有することを確認する必要がある場合がある。一般に、当該の認証および承認プロセスを行うエンティティは、任意の好適な手動または自動の手法を使用することが可能である。例えば、パーティは、そのパーティの正式なレターヘッドに関して、認証エンティティにレターのファックスまたはメールを求められる場合があるが、認証エンティティにおいて、要員または自動装置に

より信頼性が調査される。別の例として、バイオメトリック認証技術（例、指紋解析、眼球走査、手形または声紋解析、顔面の認識法、または対面による識別確認）を使用することが可能である。アイデンティティを確立するために、ハードウェアベースの機構（例、ハードウェアトークンに基づくもの）を使用してもよい。ユーザーは、予め定められたユーザー名およびパスワードの形式で、信用証明書を提供してもよい。認証局は、特定のパーティのアイデンティティの確認を助力する、デジタル証明書を作成することができる。デジタル署名（例えば、認証局からの署名、または秘密鍵を使用する他のエンティティ、および公開鍵を使用して確認できる他のエンティティからの署名）は、メッセージまたは他の署名された情報が特定のパーティに関連することを確認するために使用することができる。システム１０における認証プロセスは、Ｋｅｒｂｅｒｏｓチケットまたは他の承認の証明のようなチケットの生成を伴う場合がある。ユーザー認証オペレーションは、本願明細書において、受信者の信用証明情報や基となるユーザー名およびパスワード、またはユーザーにより入力されたその他の受信者の信用証明情報から導出されるか、またはこれに基づくチケット情報のような情報の区別を必要とせずに、一般的に記述されている。

【００３６】

認証情報および他の情報は、パーティ間（例、暗号解読サーバー２４とユーザーとの間）で安全に伝達されなければならない場合がある。システム１０において安全に情報を伝達するために、複数の異なる手法を使用することが可能である。例えば、情報は、セキュアソケットレイヤー（ＳＳＬ）プロトコルまたは他の好適な安全なプロトコル（例えばＴＬＳ）を使用する通信経路のような安全な通信経路を通じて、安全に伝達することができる。通信経路は、信頼できるパーティの制御下にある（例、通信経路が完全に組織１８内にあるため、物理的に信頼できるパーティの制御下にある）ため、信頼できる。情報は、安全でない（または安全な）リンクを通じて送信する前に、（例えばメッセージなどで）その情報を暗号化することによって、安全に送信することが可能である。

【００３７】

既存の暗号化機構とのインターフェースを容易にするため、または他の好適な理由で、メッセージの内容を暗号化するために第１の鍵を使用し、第１の鍵を暗号化するために第２の鍵を使用する、「ツーステップ」の暗号化技術を使用することが望ましい場合がある。暗号解読中に、第１の鍵の暗号化バージョンを解読するために、第２の鍵を使用するが、第２の鍵は、次いでメッセージの内容をアンロックするために使用することができる。これらのツーステッププロセス（および類似した高次のマルチステッププロセス）は、「純粋な」または「シングルステップ」の暗号化アルゴリズムよりも効率的な場合があり、必要に応じて使用することができる。明確にするため、本発明では、シングルステップアルゴリズムのコンテキストにおいて説明する。

【００３８】

公開鍵の暗号技術は、安全なメッセージングシステムにおいてしばしば使用される。公開鍵の暗号技術によって、送信者は、その受信者の公開鍵を使用して、受信者に対するメッセージを暗号化することができる。受信者は、暗号解読のためにマッチング秘密鍵を使用する。公開鍵の暗号技術は、概ね満足できるものであるが、送信者と受信者との間にすでに関係が存在するような環境においては、必要以上に扱いにくくなる場合がある。

【００３９】

組織１８が銀行であるような例示的シナリオを考察する。銀行は、安全に電子預金取引明細書を配信することが求められる、既存の一組の顧客を有する。銀行と顧客には、すでに互いに信頼できる関係がある。例えば、銀行は、その顧客にすでに割り当てたアカウント名および番号を有する。顧客が自分のアカウントを開いたときに、銀行は、社会保障番号情報、電話番号、親類の名前、生年月日、出生地、電子メールアドレスなどの情報を収集している。この情報は、銀行が顧客のアイデンティティを確認するために使用できる。銀行の顧客はまた、現金自動預払機から現金を引き出すための暗証番号（ＰＩＮ）、およびオンラインで銀行取引タスクを行う前の認証のためのユーザー名およびパスワードも有することが可能である。

【００４０】
この種の環境では、銀行およびその顧客は、見知らぬ者同士ではない。したがって、銀行およびその顧客は、送信者および受信者を互いに見知らぬものとして扱うことができるようにデザインされた、公開鍵の暗号技術のような暗号手法にのみ依存する必要がない。
【００４１】
本発明は、銀行とその顧客との間の先在する関係を活用することができる。公開鍵の暗号化ではなく、効率的な対称鍵の暗号化を使用することができる。銀行とその顧客との間の先在する関係はまた、認証および鍵配送のようなオペレーションを容易にするために使用することができる。
【００４２】
以下の説明において、組織１８は、企業または会社、あるいは他の好適な種類の企業体であってよい。組織のユーザーは、従業員、ボランティア、契約者、または組織（またはそれらの装置）の他の好適な種類のメンバーであってよい。組織内のユーザーは、イントラネット１６へのアクセス、およびゲートウェイ２２のようなイントラネット１６を使用した組織内に互いにネットワーク化された装置によって、組織外のユーザーと区別される。
【００４３】
組織外のユーザーの一部は、その組織とは関係のない、独立した第三者であってよい。
【００４４】
組織外の他のユーザーは、組織の顧客であってよい。例えば、上述のように、銀行の口座名義人は、銀行の顧客である。顧客は、クライアント、契約者、その組織で働く従業員と同じアクセス権を持たない臨時従業員、または顧客としてその組織と関連しているが、その組織自体の一員ではない顧客である、他の好適なユーザーであってよい。
【００４５】
ユーザーが、顧客として所与の組織と関連付けられた場合、ユーザーとその組織との間の関係は、本発明の安全な通信技術をサポートするために活用することができる。一般的なシナリオでは、銀行１８の自動預金取引明細書の配布サーバーは、受信者Ｃのような顧客である受信者に、暗号化した預金取引明細書メッセージを送信する。送信者Ａは、ゲートウェイ２２を介して各メッセージを送信する。ゲートウェイ２２は、対称鍵を使用して各メッセージを暗号化するために、暗号化エンジン２８を使用する。対称鍵は、鍵生成器２０によってマスター鍵２６から導出されるので、「導出鍵」と称する。多くの異なる鍵をこのように導出することができるため、導出鍵は、各受信者に対して一意に生成することが可能である。任意のユーザーの鍵は、必要に応じてユーザーＩＤから再導出することができるので、決定論的な鍵導出機構を使用することによって、導出鍵は、鍵生成器によって格納する必要がない。
【００４６】
ゲートウェイが、受信者Ｃの導出対称鍵を使用して、受信者Ｃに対するメッセージを暗号化した後、そのゲートウェイは、受信者Ｃに暗号化メッセージを中継することが可能である。暗号化メッセージは、通信ネットワーク１４を通じて、受信者Ｃに送達することが可能である。受信者Ｃは、暗号化メッセージを受信すると、メッセージの内容を解読するために暗号解読エンジン３４を使用できるように、組織Ａから導出鍵のコピーを取得することが可能である。
【００４７】
受信者Ｃは、鍵要求を暗号解読サーバー２４に送信することによって、受信者Ｃの導出鍵を取得することができる。受信者Ｃは銀行の顧客なので、認証サービス３０は、受信者Ｃを認証するために、受信者Ｃのアカウント名およびＰＩＮのような先在する受信者信用証明書を使用することが可能である。認証サービス３０が、受信者Ｃのアイデンティティを確認し、受信者Ｃが導出鍵のコピーの取得を許可されたと判断すると、受信者Ｃに対する導出鍵は、鍵配信サービス３２を使用して、受信者Ｃに送達することが可能である。
【００４８】

システム１０の設定、および導出鍵の要求に対する応答の際に伴われる例示的ステップを図２に示す。

【００４９】

設定オペレーションは、ステップ３６で行われる。設定中に、鍵生成器２０によってマスター鍵２６を生成することが可能である。マスター鍵２６は、例えば、十分なエントロピ（すなわち、マスター鍵のサイズと同数のエントロピ）を有するランダムな文字列から生成することが可能である。ランダムな文字列には、任意の好適なシンボルを含むことができる。一般に、数字、文字、および他のシンボルと、情報を表すための他の当該のスキームとの間には同等性がある。これらの異なる代表的なスキーム間の固有の同等性により、文字またはシンボルの数字への変換を伴う技術、または複数の数字または文字列を単一の数字または他の当該のオペレーションとして表すための技術は、本願明細書では詳述しない。鍵生成器は、マスターシークレットに障害が生じないように、安全なサーバー上で実行されることが好ましい。

【００５０】

マスター鍵２６の生成のような設定オペレーションが行われた後で、鍵生成器２０は、組織１８において、他の装置からの導出鍵に対する要求に応答することができる。導出鍵は、特定の目的のため（例、特定の受信者に対応するため）に、マスター鍵２６から導出される鍵である。１つまたは複数の導出鍵に障害が生じても、他の導出鍵に依存する他のオペレーションのセキュリティには障害が生じない。さらに、マスター鍵は、任意の一群の導出鍵から都合よく導出することができず、マスター鍵を保護する。

【００５１】

導出鍵の要求に応答するプロセスは、ステップ３８、４０、および４２を伴う。これらのステップは、一般に、破線３７で示されるように、ステップ３６の設定オペレーションとは異なる時間に行われる。導出鍵の要求を生成することができる組織１８のエンティティは、ゲートウェイ２２、暗号解読サーバー２４、およびユーザー１２を含むことが可能である。鍵生成器２０から直接に導出鍵を要求するユーザーは、暗号化エンジン２８のようなゲートウェイ上の暗号化エンジンを使用せずに、クライアントソフトウェア内の暗号化エンジンを使用して、暗号化を行うことが可能である。したがって、ゲートウェイ２２のようなゲートウェイを使用することはオプションであり、その組織のポリシーによって規定される。ゲートウェイを有するシステムでは、ゲートウェイは、暗号化エンジン２８で使用する導出鍵を要求することができる。暗号解読サーバー２４は、組織外のユーザーに代わって鍵を要求することが可能である。鍵要求は、イントラネット１６を通じて、鍵生成器２０に提供することが可能である。

【００５２】

ステップ３８で、鍵生成器２０は、ゲートウェイ２２、暗号解読サーバー２４、または送信者Ａなどの組織内のユーザーのような、組織内の信頼できるエンティティからの要求を受信する。導出鍵の要求は、これらの信頼できるエンティティによってのみ承認されることが好ましい。導出鍵は特定のユーザー（例えば顧客）に固有であるので、導出鍵の要求は、ユーザー識別子（ユーザーＩＤ）を含むことが好ましい。例えば、受信者に対するメッセージを暗号化するために、導出鍵が要求されている場合、その鍵に対する要求は、受信者のアイデンティティに関する情報（すなわち、受信者ＩＤ）を含まなければならない。

【００５３】

ステップ４０で、鍵生成器２０は、要求された導出鍵を計算する。要求された導出鍵は、その要求において提供された受信者ＩＤに対して一意のものである。必要に応じて、導出鍵は、他の点において一意とするか、または受信者のＩＤ情報を含まないようにすることが可能である。例えば、導出鍵は、セキュリティを強化するために、特定の日付または日付範囲に対して一意とすることが可能である。各メッセージは、鍵生成器の負担を非常に増加させることになるが、導出鍵が、受信者およびメッセージの両方に対して一意となるように、それ自身が関連する導出鍵を有するように要求することができる。導出鍵は、

電子メールアドレス（一種のユーザーＩＤ）またはドメイン名の情報に基づいて生成することができる。明確にするため、現在の説明は、主に、導出鍵がユーザーＩＤに基づいてマスター鍵から導出される機構に重点を置いている。しかし、これは、単なる例示的なものである。導出鍵を導出するときには、鍵生成器２０は、任意の好適な入力を使用することが可能である。

【００５４】

マスター鍵および受信者ＩＤから導出鍵を生成するために、鍵生成器２０は、任意の好適な一方向性関数を使用することができる。一例として、鍵生成器２０は、式１のハッシュ関数のようなハッシュ関数を使用して、受信者Ａ（ｄｋｅｙＡ）に対する導出鍵を計算することができる。

ｄｋｅｙＡ＝ＨＭＡＣ（ｍａｓｔｅｒ－ｋｅｙ：ｒｅｃｉｐｉｅｎｔ＿ＩＤ）（１）

式１において、ｍａｓｔｅｒ－ｋｅｙは、マスター鍵２６であり、ｒｅｃｉｐｉｅｎｔ＿ＩＤは、受信者のアイデンティティに関する情報である。値ｄＫｅｙＡは、導出対称鍵である。関数ＨＭＡＣは、周知の鍵付ハッシュメッセージ認証コード関数である。本願明細書の式１および他の式に使用される記号において、コロンの前にある関数の引数は、暗号関数（ここでは、ＨＭＡＣ関数）によって使用される鍵情報である。コロンの後の引数は、非鍵情報（この場合は受信者ＩＤ）を表す。

【００５５】

式１の関数を使用して、鍵生成器２０は、受信者のアイデンティティの鍵付ハッシュ値を計算することができる。ただし、式１の鍵導出関数は、単なる例示的なものである。導出鍵を受信者ＩＤに対して一意のものにしながら、マスター鍵の秘密性を保つために、マスター鍵および受信者ＩＤに機能することができる、任意の好適な一方向性関数を使用することが可能である。個々の導出鍵に固有のあらゆる情報の格納を鍵生成器に要求せずに、送信者および受信者の導出鍵のコピーが一致するように、好適な一方向性関数は、決定論的となる。また、（一例として）ユーザーＸに対する要求が、ユーザーＹに対して偶発的または敵対的に導出鍵を生成しないように、好適な一方向性関数は、衝突に抵抗性のあるものとなる。好適な一方向性関数には、ハッシュ関数、鍵付ハッシュ関数、デジタル署名関数などが挙げられる。

【００５６】

導出鍵の要求に応えて導出鍵を生成した後に、ステップ４２で、鍵生成器２０は、要求元に導出鍵を提供することができる。鍵生成器４０は、例えば、組織のイントラネット１６を通じて、ゲートウェイ２２、組織１８内の送信者、または暗号解読サーバー２４に、導出鍵を送信することができる。イントラネット１６は、組織１８によって制御されるため、安全であるとみなせる。

【００５７】

導出鍵は、ゲートウェイ２２、組織１８内の送信者、または暗号解読サーバー２４によって（例えば、タイムスタンプされた導出鍵が期限切れになるまで）、ローカルに格納することができる。このように、ローカルキャッシュ内に導出鍵を格納することで、鍵生成器２０が処理する導出鍵の要求数を減じることができる。ローカル記憶装置を使用する場合、導出鍵の要求元は、鍵が必要なときに、導出鍵のコピーのためのローカル記憶装置を確認することができる。ローカル記憶装置において現在のバージョンの導出鍵が利用できる場合は、鍵生成器２０に対する鍵要求を行う必要はない。

【００５８】

メッセージの暗号化および組織１８内から組織１８の顧客である外部の受信者への送信の際に関連する例示的ステップを図３に示す。

【００５９】

ステップ４４で、送信者Ａのような組織１８の送信者は、組織１８の顧客である受信者Ｃのような受信者に安全に送信される、メッセージを作成する。送信者のクライアントソフトウェアがメッセージ内容を作成してもよく、またメッセージの内容を、別の好適なソースから送信者Ａが取得してもよい。

【００６０】
ステップ４６で、送信者Ａは、受信者にメッセージを送信する。一例として、送信者Ａの電子メールクライアントは、イントラネット１６を通じて、受信者に宛てた電子メールメッセージを送信することができる。イントラネット１６は安全であるとみなされるので、概してこの時点で、メッセージを暗号化する必要はない。
【００６１】
ステップ４８で、送信者からの発信メッセージをゲートウェイ２２が受信することができる。ゲートウェイは、メッセージ管理ソフトウェア、または暗号化ポリシー、ウイルススキャンポリシー、アーカイブポリシー、などのようなポリシーを実行するために使用される、他の好適なソフトウェアを有することができる。ゲートウェイは、各メッセージをどのように処理するのかを判断するために、これらのポリシー、およびメッセージ内容情報、ソースおよび宛先アドレス情報、ヘッダ情報、などのようなメッセージ属性情報を使用することができる。例えば、ゲートウェイは、特定のメッセージを暗号化する必要があるかどうかを判断するために、各受信者の電子メールアドレスのドメイン名部分を調査することができる。
【００６２】
あらゆる好適な暗号化ポリシーは、ゲートウェイ２２を使用して実行することが可能である。例えば、ゲートウェイ２２は、全ての発信メッセージを暗号化すること、特定の受信者またはリストの受信者（すなわち、特定の顧客）に送信されるメッセージを暗号化すること、その電子メールアドレスが所定のドメイン名を含むメッセージを暗号化すること、メッセージの状態または組織に関連付けられた日付に基づいて、受信者へのメッセージを暗号化すること、などが可能である。
【００６３】
ゲートウェイ２２が、そのメッセージを暗号化する必要があると判断した場合、ゲートウェイ２２は、鍵生成器２０から、暗号解読プロセスのための好適な導出鍵を取得することができる。適切な導出鍵がローカルに利用できる場合、ゲートウェイ２２は、ローカルに格納されたバージョンの導出鍵を使用することができる。適切な導出鍵がローカルに利用できない場合、ゲートウェイは、ステップ５０で、導出鍵の要求を生成し、イントラネット１６を通じて、鍵生成器２０に導出鍵の要求を提供する。導出鍵の要求は、受信者のアイデンティティを含む。任意の好適なフォーマットは、導出鍵の要求において、鍵生成器に受信者のアイデンティティ情報を提供するために使用することができる。例えば、受信者のアイデンティティ情報は、受信者ＩＤ（例、受信者Ｃの電子メールアドレス、または受信者Ｃの電子メールアドレスに基づいた情報）の形式で提供することができる。
【００６４】
ステップ５２で、鍵生成器２０は、導出鍵の要求の受信および処理を行う。導出鍵は、図２のステップ３８、４０、および４２のプロセスを使用して生成することができる。導出鍵を生成した後に、導出鍵を、イントラネット１６を通じて、ゲートウェイ２２に提供することができる。
【００６５】
ステップ５４で、ゲートウェイ２２は、鍵生成器２０から導出鍵を受信する。ゲートウェイは、次いで、暗号文を生成するために、暗号化エンジン２８を使用してメッセージ内容を暗号化することができる。暗号化エンジン２８は、ＡＥＳのような対称鍵暗号化アルゴリズムを使用する対称鍵暗号化エンジンとするか、または他の好適な暗号化アルゴリズムを使用することができる。暗号化エンジン２８への入力は、受信者および非暗号化メッセージ内容の導出鍵を含む。暗号化エンジン２８の出力は、含む暗号化バージョンのメッセージ（暗号文）を含む。
【００６６】
ステップ５６で、ゲートウェイ２２は、受信者Ｃに暗号化バージョンのメッセージを中継することができる。暗号化メッセージは、受信者Ｃが受信する前に、１つ以上のメールサーバー（組織１８の内部および外部のメールサーバーを含む）１つ以上のメールサーバ

ーを通過する場合がある。

【００６７】

暗号化メッセージの受信および解読の際に関連する例示的ステップを図４に示す。

【００６８】

ステップ５８で、受信者（この例では受信者Ｃ）は、通信ネットワーク１４を通じて、メッセージを受信する。メッセージは、受信者の装置１２上で動作している受信者のクライアントソフトウェアによって受信することができる。

【００６９】

受信者のクライアントソフトウェアが、ローカルキャッシュ内で利用できる適切な導出鍵のコピーを有する場合、クライアントソフトウェアは、メッセージを解読するために、その導出鍵を使用することができる。導出鍵をローカルに利用できない場合、受信者は、組織１８から導出鍵のコピーを取得することができる。

【００７０】

特に、ステップ６０で、受信者は、導出鍵の要求を生成し、暗号解読サーバー２４に導出鍵の要求を提供することができる。導出鍵の要求を作成するために、任意の好適な機構を使用することができる。例えば、送信者Ａまたはゲートウェイ２２のクライアントは、発信メッセージ内にクリックできるリンク（例えばウェブリンク）を自動的に含むことが可能である。受信者Ｃがメッセージを受信するとき、メッセージ内の命令は、受信者Ｃに、そのリンクをクリックするように促すことができる。リンクをクリックすることで、受信者Ｃのウェブブラウザまたは他の好適なクライアントソフトウェアに、通信ネットワーク１４を通じて、特定のウェブアドレスに特定の情報を送信するように命令することができる。送信される情報は、受信者のアイデンティティ情報を含むこと、および導出鍵の要求としての機能を果たすことが可能である。ウェブアドレスは、暗号解読サーバー２４に関連付けることができる。これは、導出鍵の要求を暗号解読サーバー２４に提供することが可能な１つの例示的方法である。必要に応じて、任意の好適な機構を使用することができる。

【００７１】

ステップ６２で、暗号解読サーバー２４は、受信者を認証することによって導出キーの要求を処理し、サーバー２４と受信者Ｃの装置との間に安全な通信チャネルを確立することができる。必要に応じて、任意の好適な認証技術を使用することができる。例えば、受信者のクライアントは、ユーザー名およびパスワード情報の形式で、暗号解読サーバーに受信者信用証明書を提供することができる。ユーザー名およびパスワード情報は、例えば、組織１８が銀行であれば、銀行アカウント名情報およびＰＩＮ情報となりうる。認証プロセス中、暗号解読サーバーは、受信者信用証明書を確認するために、認証サービス３０を使用する。受信者信用証明書が、組織に保持されている信用証明情報と一致する（および導出鍵の要求内の受信者ＩＤと一致する）場合、暗号解読サーバー２４は、導出鍵を要求している受信者が、その受信者の導出鍵のコピーの取得を許可されていると判断することができる。認証プロセス中に、サーバー２４および受信者Ｃの装置１２は、安全な通信チャネル（例えば、ＳＳＬリンク）を確立する。この安全な通信チャネルは、導出鍵の配信に使用することができる。

【００７２】

ステップ６４で、暗号解読サーバー２４が、要求元の受信者（この例では受信者Ｃ）が導出鍵のコピーの取得を許可されたと判断した後で、暗号解読サーバー２４は、導出鍵を要求して鍵生成器２０から取得することができる。暗号解読サーバー２４によって作成される鍵要求は、イントラネット１６を通じて作成し、受信者ＩＤを含むことができる。暗号解読サーバー２４は、鍵生成器２０と同じ組織であるので、鍵生成器２０は、暗号解読サーバーを信頼する。それに応じて、鍵生成器２０は、導出鍵を生成するために、暗号解読サーバーからの受信者ＩＤ情報、およびステップ３８、４０、および４２（図２）の導出鍵生成プロセスを使用することが可能である。導出鍵は、イントラネット１６を通じて、暗号解読サーバーに提供することができる。

【００７３】
ステップ６４で、暗号解読サーバー２４が、鍵生成器２０から受信者Ｃに対する導出鍵を取得した後に、ステップ６６で、暗号解読サーバー２４は、通信ネットワーク１４を通じて、受信者Ｃに導出鍵を提供することができる。暗号解読サーバー２４は、ステップ６２で確立された安全な通信チャネルを使用して（例えば、ＳＳＬリンクを通じて）、受信者Ｃに安全に導出鍵を提供することができる。
【００７４】
ステップ６８で、受信者Ｃは、安全な通信チャネルを通じて、暗号解読サーバー２４から導出対称鍵を受信する。受信者は、次いで暗号化メッセージを解読する（すなわち、暗号文を解読する）ために、暗号解読エンジン３４を使用することができる。暗号解読エンジン３４への入力は、暗号化バージョンのメッセージ（すなわち、暗号文）、および受信者Ｃの導出鍵である。暗号解読エンジン３４の出力は、非暗号化バージョンのメッセージ内容である。
【００７５】
暗号解読エンジン２４は、暗号化エンジン２８によって使用された同じ種類の暗号アルゴリズム（ＡＥＳを使用した対称鍵暗号解読アルゴリズムなど）を使用する。この種の対称鍵機構に関しては、受信者がメッセージを解読するために使用する導出鍵は、送信者が（ゲートウェイ２２において暗号化エンジン２８を使用して）メッセージを暗号化するために使用した導出鍵と同じである。暗号解読エンジン３４は、スタンドアロンのソフトウェアパッケージの一部とするか、または既存のクライアントソフトウェアに（例えば、電子メールクライアントへのプラグインなどとして）組み込むことが可能である。
【００７６】
必要に応じて、受信者は、導出鍵のコピーを要求する代わりに、組織１８に暗号化メッセージの解読を要求することができる。この種類の機構では、暗号解読サーバーは、暗号解読エンジン３４のような暗号解読エンジンを含むことができる。受信者は、暗号解読サーバー２４に導出鍵の要求を行うのではなく、暗号解読サーバー２４に暗号解読の要求を行うことができる。暗号解読の要求は、受信者のＩＤを含むことができる。暗号化バージョンのメッセージは、暗号解読の要求とともに、または他の好適な機構を使用して、暗号解読サーバー２４に提供することが可能である。受信者の認証の成功に続いて、暗号解読サーバー２４は、鍵生成器２０から導出鍵を取得し、メッセージの内容を解読するために、ローカルな暗号解読エンジンを使用することができる。解読されたメッセージの内容は、認証プロセス中に、ＳＳＬリンクのような安全なリンクを通じて、受信者に提供することができる。
【００７７】
大きな組織では、組織の種々の構成要素が互いを信頼しなければならない範囲を制限するために、階層的機構を使用することが有用となりうる。例えば、組織は、北アメリカのユニットおよびヨーロッパのユニットを有することができる。北アメリカのユニットの従業員は、その組織内の１つの鍵生成器に関連付けることが可能である。ヨーロッパのユニットの従業員は、その組織内の別の鍵生成器に関連付けることが可能である。この種類の機構によって、平行および独立したセキュリティ機構を同じ組織内に保持することができるため、セキュリティが強化される。例えば、１つの鍵生成器のマスター鍵に障害が生じた場合であっても、他の鍵生成器によって保護された通信は、その安全性が保持される。
【００７８】
階層的セキュリティ機構はまた、組織へのイントラネット１６の導入をより容易にすることも可能である。例えば、ある場所において、ローカルなイーサネット（登録商標）に接続される全てのエンティティは、互いに信頼することができ、別の場所において、ローカルなイーサネット（登録商標）に接続される全てのエンティティは、互いに信頼することができる。各イーサネット（登録商標）ネットワークは、その関連する場所に対するローカルなイントラネットを形成することが可能であるが、（一例として）各ローカルなイントラネットには、それぞれの委譲された鍵生成器が提供されるので、同じレベルの信頼

性およびセキュリティとともに、２つの場所をネットワーク化する必要はない。

【００７９】

図２に関して説明した導出鍵機構は、各委譲鍵生成器に対するマスター鍵を導出するために使用することができる。スーパーマスター鍵は、これらのマスター鍵を導出するために使用することができる。導出マスター鍵のそれぞれは、組織のより小さな部分に関連付けられるので、それらをサブマスター鍵と称する場合がある。委譲鍵生成器は、組織内、または他の相異なるユニット内（例えば、地理的領域、管理レベルまたは他の状態、組織系統、従業員の職務など、によって分割されるユニット）の独立したビジネスユニットの制御下に配置することができる。

【００８０】

各組織的ユニットがそれ自体の委譲鍵生成器を有すると、その委譲鍵生成器は、関連する顧客に対する導出鍵を生成するために使用することができる。例えば、組織において、北アメリカのユニットは、北アメリカのユニットの顧客に対する鍵を導出するために、北アメリカのユニットの鍵生成器を使用することができる。ヨーロッパのユニットの鍵生成器は、ヨーロッパのユニットの顧客に対する鍵を導出するために使用することが可能である。この種類のシナリオにおける顧客は、必ずしも排他的であるというわけでないが、かなり異なることになる（すなわち、顧客は、北アメリカのユニットおよびヨーロッパのユニットの両方の顧客となる場合があり、その場合、顧客は、それぞれの導出鍵を使用して、各ユニットと情報をやり取りする）。

【００８１】

階層的な鍵生成器のアーキテクチャでは、スーパー鍵生成器は、スーパーマスター鍵（マスター鍵と呼ぶ場合もある）を有し、各委譲鍵生成器は、導出されたマスター鍵（マスター鍵またはサブマスター鍵と呼ぶこともある）を有する。単一のスーパーマスター鍵を使用することにより、ゲートウェイ２２のような単一のゲートウェイは、全ての送信を暗号化するために使用することができる。

【００８２】

階層的なアーキテクチャを鍵生成器に対して使用した、例示的システム１０の図を図５に示す。スーパー鍵生成器７０は、マスター鍵７２を有する。スーパー鍵生成器７０は、組織１８（図１）によって運営され、組織の種々のユニットに対するサブマスター鍵を導出するために使用することができる。図５では、２つの組織的ユニット（ユニットＥおよびユニットＦ）が示されている。一般に、組織は、任意の適当な数のユニットを有することが可能である。

【００８３】

１つの好適な機構によって、組織のユニットは、通信ネットワーク１４を介してスーパー鍵生成器７０と相互接続されるが、これはイントラネットまたは他の好適なネットワークであってよい。この種の機構によって、スーパー鍵生成器７０は、ユニットに導出マスター鍵を電子的に配信することができる。必要に応じて、導出マスター鍵はまた、（例えば、ディスクまたは他の媒体で）手動で配信することも可能である。

【００８４】

組織は、スーパー鍵生成器７０を制御して、スーパーマスター鍵７２の秘密性を確認する。各ユニットは、それ自体の委譲鍵生成器を有し、それぞれが、スーパーマスター鍵から導出されたそれ自体のサブマスター鍵を有する。図５の例では、ユニットＥは、委譲鍵生成器２０Ｅを有する。委譲鍵生成器２０Ｅは、ユニットＥの送信者および顧客に対する導出鍵を生成するために、サブマスター鍵２６Ｅを使用する。サブマスター鍵２６Ｅは、システム設定オペレーション中に、スーパー鍵生成器７２によってスーパーマスター鍵７２から導出されたものである。ユニットＦは、委譲鍵生成器２０Ｆを有する。委譲鍵生成器２０Ｆは、導出鍵を生成するために、サブマスター鍵２６Ｆを使用する。サブマスター鍵２６Ｆは、スーパーマスター鍵７２から導出されたものである。

【００８５】

階層的な鍵生成器機構は、任意の適当な数の層を有することができる。例えば、それぞ

れが導出されたマスター鍵の更なる層を有する、鍵生成器の更なるサブ層をユニットＥのサブユニットに提供することができる。明確にするため、本発明は、組織の単一のスーパー鍵生成器が、組織内の種々のユニットに対する導出サブマスター鍵を生成する、二層の機構に関して説明する。

【００８６】

階層的な鍵生成器のアーキテクチャは、種々のシステム構成において使用することができる。例えば、システム１０は、（図１のゲートウェイ２２のような）中央ゲートウェイを有することができる。中央ゲートウェイは、全ての発信メッセージに対する情報センターとして機能することができ、メッセージを暗号化するための（図１の暗号化エンジン２８のような）暗号化エンジンを有することができる。中央ゲートウェイ内の暗号化エンジンは、種々の受信者の導出鍵を使用して、メッセージを暗号化することができる。導出鍵は、委譲鍵生成器によって中央ゲートウェイに提供することができる。

【００８７】

図５に示される例示的機構では、ゲートウェイを使用しない。むしろ、各送信者は、発信メッセージを暗号化するために、暗号化エンジンを有するクライアントソフトウェアを使用する。

【００８８】

標準的なシナリオでは、その組織の特定のユニット内のユーザーは、そのユニットの顧客に、暗号化メッセージを送信するように要求する。例えば、ユニットＥの送信者Ｘが、ユニットＥの顧客である受信者Ｙへの暗号化メッセージの送信を要求する。送信者Ｘは、委譲鍵生成器２０Ｅから、受信者Ｙのメッセージを暗号化するための導出鍵を取得する。暗号化メッセージは、通信ネットワーク１４を通じて、受信者Ｙに送信される。受信者Ｙは、導出鍵の要求を生成する。導出鍵の要求は、組織によって処理され、要求された導出鍵は、メッセージを解読するために、受信者Ｙに提供される。

【００８９】

階層的な鍵生成器のアーキテクチャに基づいて、１つ以上の暗号解読サーバーをシステム１０内で使用することができる。

【００９０】

１つの好適な機構では、中央暗号解読サーバーは、受信者からの導出鍵の要求を処理するために使用される。各受信者の導出鍵の要求は、受信者を識別する情報を含む。各受信者の導出鍵の要求はまた、どのユニットの鍵生成器が、送信者がメッセージを暗号化する際に使用した、導出鍵を生成するために使用されたのかを識別する情報を含むこともできる。中央暗号解読サーバーは、どの委譲鍵生成器が導出鍵を作成したかについて判断するために、この情報を処理することができる。中央暗号解読サーバーは、次いで組織の適切なユニット内の委譲鍵生成器に鍵要求を送ることができる。

【００９１】

必要に応じて、暗号解読サーバーは、各ユニットに提供することが可能である。この種類の機構を図５に示す。ユニットＥ内の暗号解読サーバー２４Ｅは、委譲鍵生成器２０Ｅから導出鍵を取得するために使用される。委譲鍵生成器２０Ｅからの導出鍵は、ユニットＥ内の送信者からのメッセージを解読するために、ユニットＥの顧客に提供される。ユニットＦ内の暗号解読サーバー２４Ｆは、委譲鍵生成器２０Ｆから導出鍵を取得するために使用される。委譲鍵生成器２０Ｆからの導出鍵は、ユニットＦの送信者からのメッセージを解読するために、ユニットＦの顧客によって使用される。

【００９２】

送信者と受信者との間の安全なメッセージングをサポートするための、図５のシステム１０のような階層的な鍵生成器機構を有するシステムの使用の際に伴われる例示的ステップを図６に示す。

【００９３】

ステップ７４で、設定オペレーションを行う。ユニットＥおよびユニットＦが一部である組織は、種々の委譲鍵生成器に対する導出マスター鍵を生成するために、スーパー鍵生

成器７０を使用する。スーパー鍵生成器７０は、式２ａを使用して、スーパーマスター鍵７２からサブマスター鍵２６Ｅを導出することが可能である。

ｓｕｂ－ｍａｓｔｅｒ＿ｋｅｙ＿Ｅ＝ＨＭＡＣ（ｓｕｐｅｒ＿ｍａｓｔｅｒ＿ｋｅｙ：ｕｎｉｔＥ）　（２ａ）

式２ａでは、ｓｕｂ－ｍａｓｔｅｒ＿ｋｅｙ＿Ｅは、図５のサブマスター鍵２６Ｅの値である。ｓｕｐｅｒ＿ｍａｓｔｅｒ＿ｋｅｙは、スーパー鍵生成器７０によって保持される、スーパーマスター鍵７２の値である。ｕｎｉｔＥは、鍵生成器２０Ｅの名前である。図２に関して説明したように、鍵生成器２０Ｅのような委譲鍵生成器に対する導出マスター鍵を生成するために、任意の好適な一方向性の鍵導出関数を使用することができる。式２ａの例では、ＨＭＡＣ関数を使用する。

【００９４】

サブマスター鍵の導出プロセスは、組織内の全てのユニットに対して繰り返される。例えば、スーパー鍵生成器７０は、式２ｂを使用して、スーパーマスター鍵７２から図５のサブマスター鍵２６Ｆを導出することができる。

ｓｕｂ－ｍａｓｔｅｒ＿ｋｅｙ＿Ｆ＝ＨＭＡＣ（ｓｕｐｅｒ＿ｍａｓｔｅｒ＿ｋｅｙ：ｕｎｉｔＦ）　（２ｂ）

マスター鍵のｓｕｂ－ｍａｓｔｅｒ＿ｋｅｙ＿Ｅおよびｓｕｂ－ｍａｓｔｅｒ＿ｋｅｙ＿Ｆは、安全に配信することができ、図５に示されるように、それぞれの委譲鍵生成器２０Ｅおよび２０Ｆによってローカルに格納することができる。スーパー鍵生成器７０は、安全なイントラネットを介して、委譲鍵生成器２６Ｅおよび２６Ｆとネットワーク化することが可能である。これによって、鍵は、組織内の信頼できる経路を通じて配信するか、または他の好適な通信ネットワーク１４を介して安全に配信することが可能になる。

【００９５】

式２ａおよび２ｂ、または他の好適な鍵導出関数を使用して、委譲鍵生成器のサブマスター鍵を導出することによって、委譲鍵生成器を設定した後に、メッセージは、ステップ７６、７８、８０、８２、８４、および８６で安全に送信することができる。ステップ７６、７８、８０、８２、８４、および８６は、破線７５で示されるように、ステップ７４の設定オペレーションとは異なる時間に行うことができる。

【００９６】

ステップ７６で、ユニットＥ内の送信者Ｘのような送信者は、ユニットＥの顧客である受信者Ｙのような所望の受信者に対する導出鍵を取得する。送信者のクライアントソフトウェアは、ユニットＥ内のイントラネット１６を通じて、委譲鍵生成器に対する導出鍵の要求を行うことによって、メッセージの暗号化に使用する適切な導出鍵２０Ｅを取得することができる。送信者によって作成される鍵要求は、メッセージの対象となる受信者に関する情報を含む。

【００９７】

この例では、対象となる受信者は受信者Ｙであるので、鍵要求は、受信者Ｙに対する受信者ＩＤのような受信者Ｙを識別する情報（例、ｒｅｃｉｐｉｅｎｔ＿Ｙ＿ＩＤ）を含むことができる。委譲鍵生成器は、次いで、式３を使用するか、または図２に関して説明したように、他の好適な鍵導出関数を使用して、ローカルに導出した鍵を計算することができる。

ｋｅｙ＿Ｙ＝ＨＭＡＣ（ｓｕｂ－ｍａｓｔｅｒ＿ｋｅｙ＿Ｅ：ｒｅｃｉｐｉｅｎｔ＿Ｙ＿ＩＤ）　（３）

式３では、ｓｕｂ－ｍａｓｔｅｒ＿ｋｅｙ＿Ｅは、ユニットＥのユーザーおよびそれらの関連する顧客に対する導出鍵の生成において、委譲鍵生成器２０Ｅによって使用される。ｒｅｃｉｐｉｅｎｔ＿Ｙ＿ＩＤは、メッセージの対象となる受信者を識別する情報である。Ｋｅｙ＿Ｙは、導出鍵である。Ｋｅｙ＿Ｙを計算した後に、委譲鍵生成器２０Ｅは、要求元の送信者にｋｅｙ＿Ｙを提供する。要求元の送信者におけるクライアントソフトウェアは、受信者に対するメッセージを暗号化するためにＫｅｙ＿Ｙを使用する、図１の暗号化エンジン２８のような暗号化エンジンを含む。クライアントソフトウェアは、次いで受

信者に暗号化メッセージを送信する。

【００９８】

暗号化メッセージは、メッセージ（暗号文）の暗号化された内容を含み、また受信者がメッセージを解読するための導出鍵（Ｋｅｙ＿Ｙ）のコピーを要求したときに、受信者が交信するための適切なユニット（すなわち、この例では、委譲鍵生成器２０Ｅおよび暗号解読サーバー２４Ｅを含むユニットＥ）を識別する非暗号化情報を含む。委譲鍵生成器およびそのユニットを識別する情報には、任意の好適な機構を使用して、メッセージを提供することが可能である。例えば、送信者Ｘにおけるクライアントソフトウェアは、ｒｅｃｉｐｉｅｎｔ＿Ｙ＿ＩＤを含む発信メッセージ内にウェブリンクを自動的に組み込み、また委譲鍵生成器２０Ｅおよび／または暗号解読サーバー２４Ｅに対する一意の名前を自動的に組み込む。ウェブリンクはまた、受信者が鍵要求によって暗号解読サーバー２４Ｅと交信する際に使用することができる、暗号解読サーバー２４Ｅに関連するウェブアドレス情報（例、ドメイン名）を含むことも可能である。受信者は、このウェブリンクをクリックして、受信者のウェブブラウザを使用して、暗号解読サーバー２４Ｅへの鍵要求を開始することができる。

【００９９】

ステップ７８で、受信者Ｙが、ネットワーク１４を通じて、送信者Ｘから暗号化メッセージを受信した後に、受信者Ｙは、導出鍵の要求を生成して、暗号解読サーバー２４Ｅにこの要求を提供する。鍵要求は、受信者を識別する情報（例、ｒｅｃｉｐｉｅｎｔ＿Ｙ＿ＩＤ）を含む。鍵要求はまた、暗号解読サーバーが、適切な委譲マスター鍵サーバーに導出鍵の要求を送るのを助力する情報も含むことが可能である。例えば、鍵要求は、受信者にメッセージとともに送信された、適切な委譲マスター鍵サーバーの名前を含むことが可能である。

【０１００】

中央暗号解読サーバーが存在する環境では、適切な委譲鍵生成器の名前に関する情報は、要求された導出鍵のコピーに対してどの委譲鍵生成器が交信するのかを判断するために使用することが可能である。委譲鍵生成器と暗号解読サーバーとの間に一対一の対応のある、図５に示される種類の機構では、受信者は、暗号解読サーバーのうちの特定の１つに導出鍵を送信するために、組み込まれたウェブリンク内の情報を使用することが可能である。これは、その要求に関連する委譲鍵生成器を暗黙に定義する役目をする。

【０１０１】

ステップ８０で、暗号解読サーバー２０Ｅは、受信者Ｙを認証して、暗号解読サーバー２０Ｅと受信者Ｙとの間に安全なチャネル（例、ＳＳＬリンク）を確立する。Ｋｅｙ＿Ｙのコピーを取得するために受信者Ｙの承認が確認されると、暗号解読サーバー２０Ｅは、ｋｅｙ＿Ｙに対する鍵要求を生成するために委譲鍵生成器２０Ｅを識別する、要求内の情報を使用することが可能である。鍵要求は、Ｋｅｙ＿Ｙを生成するために委譲鍵生成器２０Ｅが式３を使用できるように、ｒｅｃｉｐｉｅｎｔ＿Ｙ＿ＩＤを含む。

【０１０２】

ステップ８２で、委譲鍵生成器２０Ｅは、暗号解読サーバー２４Ｅから鍵要求を受信する。委譲鍵生成器２０Ｅおよび暗号解読サーバー２４Ｅは、同じイントラネット１６を通じて、同じユニット内で動作するので、暗号解読サーバー２４Ｅは、委譲鍵生成器２０Ｅによって信頼される。したがって、委譲鍵生成器２０Ｅは、受信者Ｙに対する導出鍵を生成する。特に、委譲鍵生成器２０Ｅは、Ｋｅｙ＿Ｙを導出するために、受信者のアイデンティティ（ｒｅｃｉｐｉｅｎｔ＿Ｙ＿ＩＤ）および式３のサブマスター鍵２６Ｅに関する要求からの情報を使用することが可能である。委譲鍵生成器２０Ｅは、次いで、ユニットＥ内のイントラネット１６を通じて、暗号解読サーバー２４Ｅに安全にＫｅｙ＿Ｙを提供することが可能である。

【０１０３】

ステップ８４で、暗号解読サーバーは、暗号解読サーバー２４Ｅと受信者Ｙとの間の安全な通信チャネルを通じて、受信者ＹにＫｅｙ＿Ｙを提供する。

【０１０４】
ステップ８６で、受信者Ｙは、暗号文を解読して、非暗号化バージョンのメッセージ内容にアクセスするために、図１の暗号解読エンジンのような暗号解読エンジン３４およびＫｅｙ＿Ｙを使用する。
【０１０５】
必要に応じて、各ユニットは、そのユニット内の送信者からの発信メッセージを暗号化するためのゲートウェイを有することができる。各ユニット内の委譲鍵生成器は、暗号化に必要な導出鍵を生成することができる。
【０１０６】
複数のユニット内の送信者からの発信メッセージを暗号化するために、グローバルゲートウェイが使用される機構では、スーパー鍵生成器７０は、式４ａおよび４ｂを使用して、導出鍵を生成することができる。
Ｕｎｉｔ＿ｊ＿ｋｅｙ＝ＨＭＡＣ（ｓｕｐｅｒ＿ｍａｓｔｅｒ＿ｋｅｙ：ｕｎｉｔ＿ｊ）　（４ａ）
$key_{j,k}$＝ＨＭＡＣ（Ｕｎｉｔ＿ｊ＿ｋｅｙ：ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ）　（４ｂ）
式４ａおよび４ｂでは、サブマスター鍵Ｕｎｉｔ＿ｊ＿ｋｅｙを生成するために、スーパー鍵生成器を使用するが、これは次いで、メッセージの対象となる受信者（この例では受信者ｋ）と、適切なユニットおよび鍵生成器（この例ではユニットｊおよび鍵生成器ｊ）との両方に固有である、導出鍵$Key_{j,k}$を生成するために、受信者ｋに対する受信者アイデンティティ（ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ）と組み合わせられる。
【０１０７】
必要に応じて、階層的な機構は、サブ分割受信者アイデンティティに使用することが可能である。例えば、そのＩＤがｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤであり、ｍａｓｔｅｒ＿ｋｅｙのマスター鍵を有する組織の顧客である受信者ｋに関連する、ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ＿１、ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ＿２などのような、複数のサブアイデンティティが存在する場合がある。ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤの各サブ受信者に対する導出鍵は、式５、６ａ、および６ｂのような式を使用して計算することが可能である。
Ｋｅｙ＿ｋ＝ＨＭＡＣ（ｍａｓｔｅｒ＿ｋｅｙ：ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ）　（５）
Ｋｅｙ＿ｋ＿１＝ＨＭＡＣ（Ｋｅｙ＿ｋ：ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ＿１）　（６ａ）
Ｋｅｙ＿ｋ＿２＝ＨＭＡＣ（Ｋｅｙ＿ｋ：ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ＿２）　（６ｂ）
式５は、マスター鍵および受信者ｋのアイデンティティから、導出鍵Ｋｅｙ＿ｋを計算するために使用することができる。式６ａは、受信者ｋに対する鍵およびｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ＿１のアイデンティティに基づいて、受信者のサブアイデンティティｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ＿１に対する導出鍵を計算するために使用することができる。式６ｂは、受信者のサブアイデンティティｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ＿２に対する導出鍵を計算するために使用することができる。ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤに関連する他の受信者サブアイデンティティに対する導出鍵も、同様に計算することが可能である。ＨＭＡＣ関数は、式５、６ａ、および６ｂの鍵を導出するために使用される。図２に関して説明したように、必要に応じて、他の好適な鍵導出関数を使用することが可能である。
【０１０８】
組織は、受信者のアイデンティティｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤを認識してさえいればよい。しかし、組織の外部では、各サブ受信者に対する導出鍵は、ｒｅｃｉｐｉｅｎｔ＿ｋ＿ＩＤ（すなわちＫｅｙ＿ｋ）に対する導出鍵を使用して計算することができる。これによって、Ｋｅｙ＿ｋは、組織外の受信者ｋによって管理される一群のユーザーに対するマスター鍵として使用できるようになる。
【０１０９】

受信者の階層は、好適な数の層を有することができる。式５、６ａ、および６ｂの例は、二層スキームを伴う。さらに、システム１０は、必要に応じて、受信者の階層および鍵生成器の階層を有することが可能である。

【０１１０】

本発明の別の側面は、認証された導出鍵に関する。特に、ゲートウェイのない環境において、導出鍵を認証できることが望ましい場合がある。ゲートウェイのないシステムでは、送信者は、発信メッセージを暗号化できるようになる前に、導出鍵を取得しなければならない。送信者が、偶発的または悪意のある送信エラーによる誤った導出鍵を取得する場合、または鍵生成器になりすました攻撃者が、送信者に偽の鍵を提供する場合には、問題が生じる可能性がある。認証された導出鍵は、要求した鍵を適切に取得した送信者および受信者を保証するために使用することができる。

【０１１１】

鍵の認証に使用することが可能な１つの好適な技術は、デジタル署名を使用するものである。この状況では、ＨＭＡＣベースのバージョンの式１は、式１’となる。

ｄｋｅｙＡ＝ｓｉｇｎ（ｐｒｉｖａｔｅ－ｋｅｙ：ｒｅｃｉｐｉｅｎｔ＿ＩＤ）　（１’）

式１’では、式１の鍵付ハッシュ関数は、決定論的なデジタル署名関数「ｓｉｇｎ」に置き換えられている。さらに、式１のマスター鍵は、私的な鍵（秘密鍵）に置き換えられている。式１’は、システム１０内の式１と同じ導出鍵生成関数の役目を果たすが、それによって、エンティティは、それらが取得する導出鍵を認証することが可能になる。

【０１１２】

秘密鍵に対応する公的な鍵（公開鍵と呼ぶ）は、公的にアクセス可能となる。公開鍵は、例えば、通信ネットワーク１４を通じて、公開鍵および／または組織１８にアクセス可能な組織の内部または外部の好適なサーバー上に公開鍵を配置することによって、発行することができる。公開鍵はまた、（例えば、イントラネット１６に接続された内部サーバー上に公開鍵を配置することによって）組織内のエンティティだけにアクセス可能とすることもできる。

【０１１３】

この鍵認証プロセスを使用するシステムでは、導出鍵（ｄｋｅｙＡ）は、式７の認証オペレーションを使用して確認することができる。

ｖａｌｉｄ＝ｖｅｒｉｆｙ（ｐｕｂｌｉｃ－ｋｅｙ：ｒｅｃｉｐｉｅｎｔ＿ＩＤ，ｄＫｅｙＡ）　（７）

式７では、関数「ｖｅｒｉｆｙ」は、公開鍵、およびｒｅｃｉｐｉｅｎｔ＿ＩＤおよびｄＫｅｙＡの値に基づいて、パラメータｖａｌｉｄを計算するために使用される。ｄＫｅｙＡが正当な導出鍵でない場合、パラメータｖａｌｉｄは誤ったものとなり、送信者または他のエンティティは、その導出鍵を使用しないことがわかる。パラメータｖａｌｉｄが真である場合、導出鍵は正当なものである。ｓｉｇｎのようなデジタル署名関数の非偽造性により、秘密鍵に関する知識がなければ、導出鍵の計算は実行不可能である。関数「ｓｉｇｎ」は、決定論的（または確定的に作用するために適切に、デランダマイズされる）であり、送信者および受信者の両方が、式１’を使用した場合に、同じ導出鍵を計算するようにする。

【０１１４】

上述のシステムによって、組織内の送信者は、組織の顧客である受信者に暗号化メッセージを送信することができる。受信者は、暗号化メッセージの解読に使用する適切な導出対称鍵のコピーを取得するために、組織と交信することができる。受信者（送信者としての役割を果たす）はまた、組織に対してメッセージを暗号化するために、導出対象鍵を使用することもできる（例えば、受信者は、組織内の送信者に暗号化した応答メッセージを返信することができる）。

【０１１５】

組織の外部の者でその組織の顧客ではない送信者は、組織内の受信者またはその組織の

顧客である受信者に暗号化メッセージを送信したい場合がある。この送信者は組織に属していないので、送信者は、組織がその顧客を認証できる同じ方法でその送信者を認証できるようにする、前もって制定された関係を持たない。

【０１１６】

非顧客である送信者が、組織の受信者またはその組織の顧客である受信者に安全なメッセージを送信できるように使用することが可能な、例示的システムを図７に示す。

【０１１７】

図７のシステム１０では、鍵生成器２０は、導出鍵を生成するために使用されるマスター鍵２６を有する。組織１８の顧客である受信者Ｑに暗号化メッセージの送信を望む送信者Ｐは、メッセージを暗号化するために、鍵生成器２０から導出鍵を使用することができる。メッセージは、送信者の装置１２において、またはゲートウェイ２２によって暗号化することができる。受信者Ｑが暗号化メッセージを受信するとき、受信者Ｑは、暗号解読サーバー２４から導出鍵のコピーを要求することができる。暗号解読サーバー２４は、受信者Ｑを認証して、鍵生成器２０から導出鍵のコピーを取得することができる。暗号解読サーバー２４は、次いで安全なチャネルを通じて、受信者Ｑに導出鍵を提供することができる。受信者Ｑは、送信者Ｐからの暗号化メッセージを解読するために、導出鍵を使用することができる。受信者Ｑはまた、送信者Ｐに対する新しいメッセージ（例えば、送信者Ｐの元のメッセージに応答する応答メッセージ）を暗号化するために、導出鍵を使用することもできる。送信者Ｐは、導出鍵のコピーを有する（またはそれを取得することができる）ので、送信者Ｐは、受信者Ｑの暗号化した応答を解読することができる。

【０１１８】

受信者Ｑとは異なり、送信者Ｓは、組織１８の顧客でない。送信者Ｓと組織１８との間には先在する関係がないので、組織１８は、送信者Ｓを認証する際に使用する信用証明書を持たない。したがって、送信者Ｓは、受信者Ｑが暗号解読サーバー２４に対して認証できるのと同じ方法で導出鍵を取得するために、暗号解読サーバー２４に対して認証することができない。送信者Ｓは組織１８の一員ではないので、送信者Ｓに受信者Ｑの導出鍵を委任することは望ましくない。

【０１１９】

本発明によれば、組織１８には、ポリシーサーバー８８が提供される。ポリシーサーバー８８は、図７の例では独立したサーバーとして示されているが、必要に応じて、ポリシーサーバー８８は、ゲートウェイ２２の一部として、暗号解読サーバー２４の一部として、鍵生成器２０の一部として、または組織１８に属する他のエンティティの一部として、使用することが可能である。ポリシーサーバーは、送信者Ｓのような非顧客送信者に対する導出鍵の生成を処理する。送信者Ｓは、その組織の顧客であるか、または組織１８の送信者への安全なメッセージの送信を望む場合に、当該の非顧客メッセージ鍵を取得することができる。

【０１２０】

図７の例示的受信者Ｒは、組織１８内に位置するが、受信者Ｒはまた、組織の顧客である受信者Ｑのような受信者である場合がある。

【０１２１】

非顧客の送信者Ｓが、メッセージを暗号化して、受信者Ｒのような受信者に安全なメッセージを送信する際に伴われる例示的ステップを図８に示す。

【０１２２】

ステップ９０で、送信者Ｓは、メッセージを受信者Ｒに送信するための鍵を要求するために、ポリシーサーバー８８と交信する。送信者Ｓは、例えば、ポリシーサーバー８８に関連するウェブページにアクセスするために、送信者Ｓの装置上で動作しているウェブブラウザを使用することが可能である。

【０１２３】

ステップ９２で、送信者のウェブブラウザは、ポリシーサーバーを認証する。標準的なウェブブラウザは、（例えば、ポリシーサーバーのウェブページに関連する証明書を確認

することによって）この種の認証を行うために、公開鍵インフラ（ＰＫＩ）技術を使用するための組み込み機能を有する。ポリシーサーバーを認証するプロセス中に、ポリシーサーバー８８と送信者Ｓとの間に安全な通信チャネル（例、ＳＳＬリンク）が確立される。

【０１２４】

送信者Ｓからの鍵要求は、対象となる受信者のアイデンティティ（ｒｅｃｉｐｉｅｎｔ＿Ｒ＿ＩＤ）に関する情報を含む。

【０１２５】

ステップ９４で、ポリシーサーバー８８は、鍵生成器２０から送信者Ｓのための導出対称鍵（Ｄｅｒ＿Ｋｅｙ）を要求して取得する。ポリシーサーバー８８はまた、乱数Ｎを生成する。数字Ｎは真ランダムとする必要はないが、当該の数字のそれぞれは、各受信者に対して一度だけ使用されることが好ましい。例えば、当該の手法は、クロックまたはカウンタを保持するために、それぞれ鍵生成器を必要とするが、Ｎは、タイムスタンプまたはカウンタに基づくことが可能である。ポリシーサーバー８８によって作成される鍵要求は、受信者のアイデンティティに関する情報（すなわち、送信者Ｓによって提供されたｒｅｃｉｐｉｅｎｔ＿Ｒ＿ＩＤの値）を含む。鍵生成器２０は、式８を使用して、導出鍵Ｄｅｒ＿Ｋｅｙを計算することができる。

Ｄｅｒ＿Ｋｅｙ＝ＨＭＡＣ（ｍａｓｔｅｒ－ｋｅｙ：ｒｅｃｉｐｉｅｎｔ＿Ｒ＿ＩＤ）　（８）

式８では、マスター鍵は、鍵生成器２０のマスター鍵であり、ｒｅｃｉｐｉｅｎｔ＿Ｒ＿ＩＤは、受信者Ｒに対する固有の識別子である。式８のＨＭＡＣ関数（および、本願明細書における他の鍵導出式）は、単なる例示的なものである。任意の好適なハッシュ関数または他の一方向性関数は、図２に関して説明したように、Ｄｅｒ＿Ｋｅｙを導出するために使用することが可能である。

【０１２６】

ステップ９６で、ポリシーサーバー８８は、非顧客メッセージ鍵Ｋｅｙ－Ｎの値を計算するために、導出鍵Ｄｅｒ＿Ｋｅｙおよび乱数Ｎを使用する。ポリシーサーバー８８は、図２に関して説明したように、任意の好適な鍵導出関数を使用することが可能である。例えば、ポリシーサーバー８８は、式９を使用して、非顧客メッセージ鍵Ｋｅｙ－Ｎを生成することができる。

Ｋｅｙ－Ｎ＝ＨＭＡＣ（Ｄｅｒ＿Ｋｅｙ：Ｎ）　（９）

ステップ９８で、ポリシーサーバー８８は、安全なチャネルを通じて、送信者Ｓに非顧客の対称メッセージ鍵Ｋｅｙ－Ｎを提供する。

【０１２７】

ステップ１００で、送信者Ｓは、受信者Ｒに対するメッセージを暗号化するために、非顧客メッセージ鍵Ｋｅｙ－Ｎを使用する。送信者Ｓは、暗号文を生成するために、送信者Ｓの装置上の暗号化エンジンを使用して、そのメッセージを暗号化することができる。

【０１２８】

ステップ１０２で、送信者Ｓは、組織１８の受信者Ｒに暗号化メッセージを送信する。送信者は、ステップ１００で作成した暗号文および暗号化メッセージの一部としてＮの値の両方を送信するか、または暗号文および関連する送信におけるＮを提供することができる。送信者Ｓから受信者Ｒに送信されるＮの値は、暗号化されていない。

【０１２９】

送信者Ｓからのメッセージを解読する際に関連する例示的ステップを図９に示す。

【０１３０】

ステップ１０４で、受信者Ｒは、非暗号化値Ｎおよび暗号文を含む、暗号化メッセージを受信する。

【０１３１】

ステップ１０６で、受信者Ｒは、ポリシーサーバーから導出鍵Ｄｅｒ＿Ｋｅｙのコピーを要求するか、または、可能な場合は、単純にそれを受信者のローカルキャッシュから取り出す。鍵要求は、鍵生成器がどの鍵を生成すべきかがわかるように、受信者Ｒのアイデ

ンティティ（ｒｅｃｉｐｉｅｎｔ＿Ｒ＿ＩＤ）を含む。ステップ１０６中に、受信者は、ポリシーサーバーに対して認証を行う。認証中に、受信者Ｒとポリシーサーバー８８との間に、安全な通信チャネル（例、ＳＳＬリンク）が確立される。

【０１３２】

ポリシーサーバー８８および受信者がどちらも組織内にある場合、受信者を認証するプロセスは暗黙的なものとなりうる（例えば、ポリシーサーバー８８は、鍵要求が、その組織のイントラネットを通じて、ポリシーサーバーと交信している組織のユーザーからのものであることを確認するだけでよい）。必要に応じて、（例えば、ポリシーサーバーによって受信者Ｒの信用証明書の認証を伴う）より大規模な認証技術を使用することが可能である。この種類の認証手法は、例えば、受信者が、組織１８のユーザーではなく、受信者Ｑのような組織１８の顧客である場合に使用することが可能である。

【０１３３】

必要に応じて、ポリシーサーバーはまた、受信者が、信頼できるソースから要求鍵を取得していることを確認するために、（例えばＰＫＩ手法を用いることによって）受信者によって認証することも可能である。

【０１３４】

ステップ１０８で、ポリシーサーバーは、鍵生成器２０から導出鍵Ｄｅｒ＿Ｋｅｙを要求するために、受信者の鍵要求から受信者ＩＤ（ｒｅｃｉｐｉｅｎｔ＿Ｒ＿ＩＤ）の情報を使用する。

【０１３５】

ステップ１１０で、鍵生成器２０は、ポリシーサーバーに対するＤｅｒ＿Ｋｅｙを生成するために、式８（または他の好適な関数）を使用する。

【０１３６】

ステップ１１２で、ポリシーサーバー８８は、安全なチャネルを通じて、受信者に導出鍵Ｄｅｒ＿Ｋｅｙを提供する。

【０１３７】

ステップ１１４で、受信者は、（例えば、式９または他の適切な一方向性関数を使用して）非顧客メッセージ鍵Ｋｅｙ－Ｎの値を計算するために、送信者Ｓから受信したＮの値およびポリシーサーバー８８からの導出鍵（Ｄｅｒ＿Ｋｅｙ）を使用する。（ポリシーサーバーが送信者に対するＫｅｙ－Ｎを計算するときに使用する式は、受信者がＫｅｙ－Ｎを計算するときに使用する式と一致しなければならない）。

【０１３８】

ステップ１１６で、受信者は、暗号文を解読してそのメッセージの内容にアクセスするために、非顧客メッセージ鍵Ｋｅｙ－Ｎを使用する。

【０１３９】

上記の説明は、単に本発明の原理を例証したにすぎず、当業者は、本発明の範囲および精神から逸脱することなく、様々な変更を行うことができる。

【図面の簡単な説明】

【０１４０】

【図１】本発明による、送信者と受信者との間で安全なメッセージを伝達することが可能な、例示的システムの図である。

【図２】本発明による、図１に示される種類のシステムの設定、および導出鍵の要求を満たす際に関連する、例示的ステップのフローチャートの図である。

【図３】本発明による、図１に示される種類のシステムを使用した、安全なメッセージの暗号化および送信の際に関連する、例示的ステップのフローチャートの図である。

【図４】本発明による、図１に示される種類のシステムを使用した、安全なメッセージの受信および解読の際に関連する、例示的ステップのフローチャートの図である。

【図５】本発明による、鍵生成器が、関連する鍵生成器に対するマスター鍵（サブマスター鍵）を作成できるようにする、例示的な階層的機構の図である。

【図６】本発明による、安全なメッセージを送受信するための、図５に示される種類のシ

ステムの設定および使用の際に関連する、例示的ステップのフローチャートの図である。
【図７】本発明による、組織の顧客ではない送信者が、組織において受信者に安全なメッセージを送信できるようにするために使用することが可能な、例示的システムの図である。
【図８】本発明による、安全なメッセージを暗号化して受信者に送信するための、図７に示される種類のシステムにおいて送信者が使用することが可能な、例示的ステップのフローチャートの図である。
【図９】本発明による、送信者から安全なメッセージを受信して解読するために、図７に示される種類のシステムにおいて受信者が使用することが可能な、例示的ステップのフローチャートの図である。

【図１】

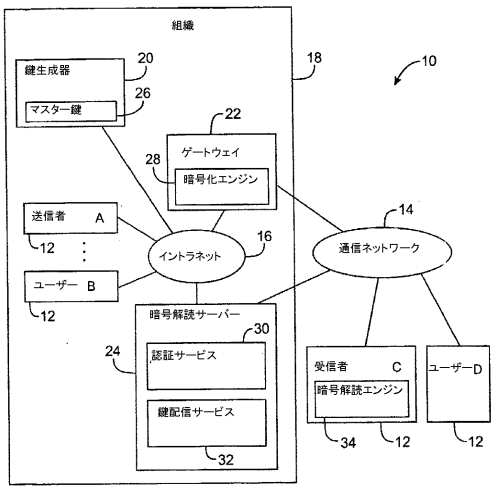


FIG. 1

【図２】

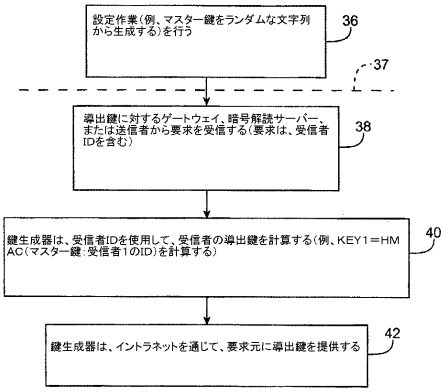


FIG. 2

【図３】

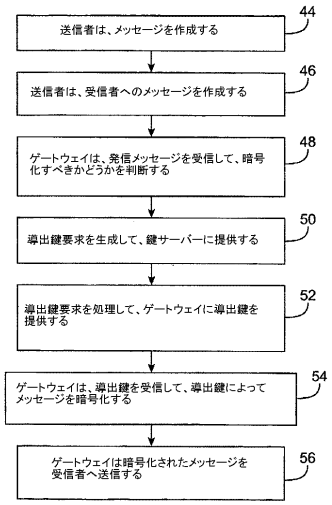


FIG. 3

【図４】

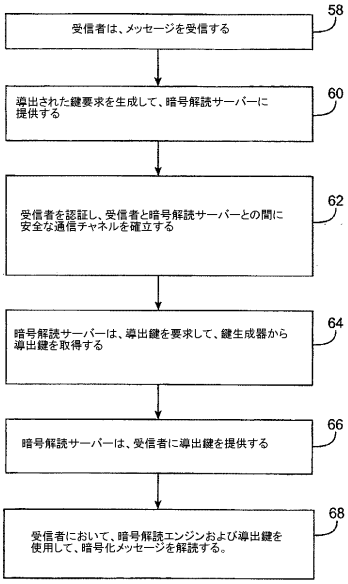


FIG. 4

【図５】

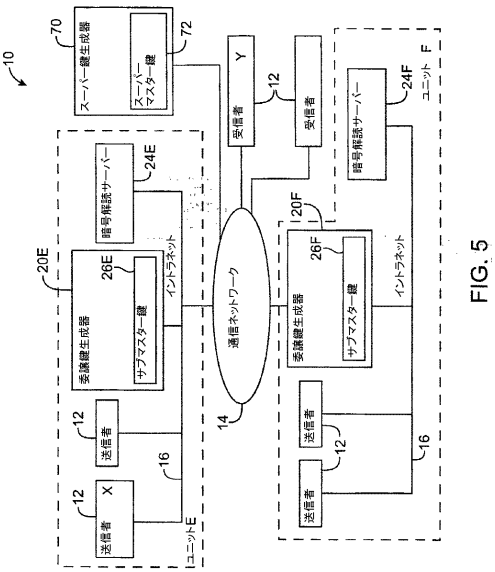


FIG. 5

【図６】

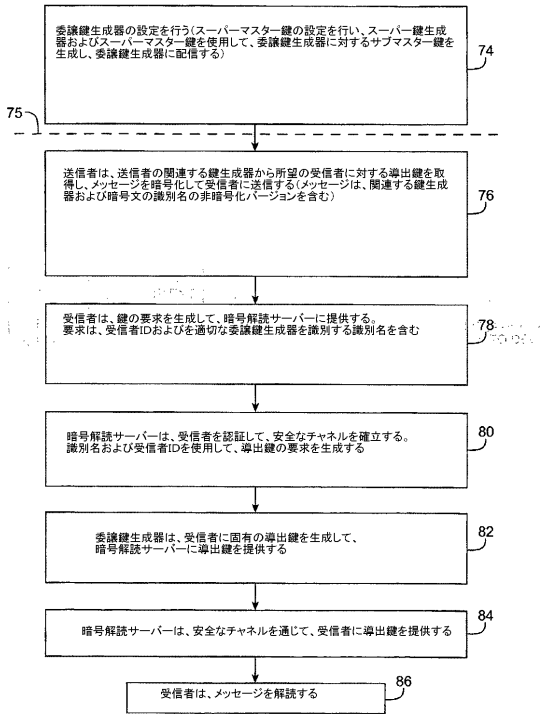


FIG. 6

【図７】

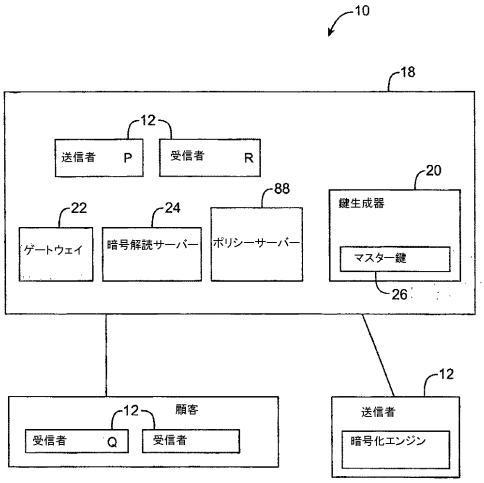


FIG. 7

【図８】

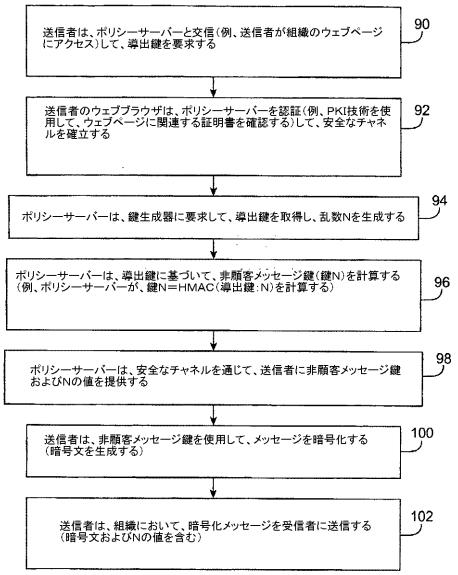


FIG. 8

【図９】

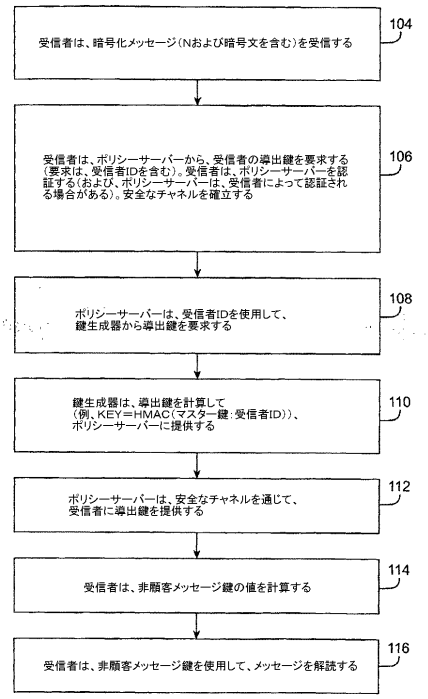


FIG. 9

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US05/24136

A. CLASSIFICATION OF SUBJECT MATTER
IPC: G06F 12/14(2006.01)

USPC: 713/152
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 713/152

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST SEARCH (USPAT; USPGPUB; EPO; JPO; DERWENT; IBM_TDB)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,584,564 B2 (Olkin et al.) 24 June 2003, Figures 1-6, Column 3, line 30 through Column 19, line 45.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
04 August 2006 (04.08.2006)

Date of mailing of the international search report
12 SEP 2006

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (571) 273-3201

Authorized officer
Baotran N. To

Telephone No. 571-272-3581

Form PCT/ISA/210 (second sheet) (April 2005)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IS,IT,LT,LU,LV,MC,NL,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SM,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 アッペンツェラー, ギド
アメリカ合衆国 カリフォルニア ９４０２５, メンロ パーク, ノエル ドライブ １０３５, アパートメント エフ
(72)発明者 ボイエン, ザビエル
アメリカ合衆国 カリフォルニア ９４３０３, パロ アルト, ミッドタウン コート ３１５ ２７２１
(72)発明者 シュピース, テレンス
アメリカ合衆国 カリフォルニア ９４４０４, サン マテオ, ホウォーフサイド ロード ８２６

Fターム(参考) 5B285 AA04 BA07 CA02 CA12 CA41 CA43 CA45 CB47 CB52 CB55
CB56 CB62 CB63 CB72 CB83 CB92 CB93
5J104 AA16 EA15 EA16 MA05 PA07