(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2006-520112
(P2006-520112A)
(43)公表日　平成18年8月31日(2006.8.31)

(51)Int.Cl.			F I			テーマコード（参考）
H04L	9/36	(2006.01)	H04L	9/00	685	5J104
H04L	9/08	(2006.01)	H04L	9/00	601B	

審査請求 未請求　予備審査請求 未請求　（全 60 頁）

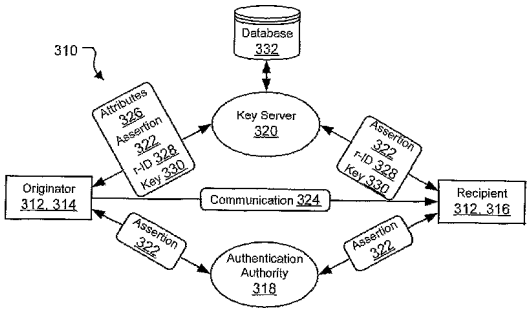
(21)出願番号	特願2004-555802 (P2004-555802)
(86)(22)出願日	平成15年11月26日 (2003.11.26)
(85)翻訳文提出日	平成17年7月14日 (2005.7.14)
(86)国際出願番号	PCT/US2003/037954
(87)国際公開番号	WO2004/049137
(87)国際公開日	平成16年6月10日 (2004.6.10)
(31)優先権主張番号	10/305,726
(32)優先日	平成14年11月26日 (2002.11.26)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/707,190
(32)優先日	平成15年11月25日 (2003.11.25)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/707,191
(32)優先日	平成15年11月25日 (2003.11.25)
(33)優先権主張国	米国(US)

(71)出願人　503140344
セキュア　データ　イン　モーション，インコーポレイテッド
アメリカ合衆国　カリフォルニア州　９４４０２，サン　マテオ，テンス　フロアー，エス．グラント　ストリート　１８７５
１８７５　Ｓ．Ｇｒａｎｔ　Ｓｔｒｅｅｔ，１０ｔｈ　Ｆｌｏｏｒ，Ｓａｎ　Ｍａｔｅｏ，ＣＡ　９４４０２　ＵＳＡ
(74)代理人　100079980
弁理士　飯田　伸行
(72)発明者　オルキン，テリー，エム．
アメリカ合衆国　カリフォルニア州　９５０３２，ロス　ガトス，リージェント　ドライブ　１０４

最終頁に続く

(54)【発明の名称】セキュリティ用キーサーバ、否認防止と監査を備えたプロセスの実現

(57)【要約】
キーサーバ（２１６、３２０、４２０）に基づくシステム（２１０、３１０、４１０）により、送信者と受信者参加者（２１２、３１２、４１２）は通信文（２１８、３２４、４２４）を安全に交換することができる。キーサーバ（２１６、３２０、４２０）は、参加者がメッセージの保護に使用する鍵を作成、保存、公開する。参加者は、キーサーバから提供された鍵（２２０、３３０、４３０）を使用して、暗号化形式の通信文を交換する。認証オーソリティ（３１８、４１８）からのアサーション（３２２、４２２）を使用して、参加者の証明書を確立することができる。正のイベントと負のイベント（３４２、３４４）と、復号化のための鍵の要求があったかどうか、あった場合にはそれはいつか、何回あったかを、制御イベント（３４０）に基づいて決定できる。キーサーバはまた、通信の送信者と受信者を、もっともらしい否認の実施が不可能で、容易に監査を行える形で確立するために、トランザクションＩＤに関連したアサーションからの情報を保存できる。



【特許請求の範囲】
【請求項１】
複数の参加者間でメッセージを安全に通信するシステムであって、前記メッセージがメッセージヘッダとメッセージコンテンツを有し、前記システムが、
前記参加者どうしをネットワーク経由で接続し、前記参加者間で、前記メッセージをメッセージヘッダに基づき伝送するメッセージルータ；および
会話鍵を保存し、前記参加者に公開するキーサーバを含み、前記会話鍵が、前記メッセージのメッセージコンテンツを保護するために使用されることを特徴とするシステム。
【請求項２】
前記保護が、暗号化とハッシングで構成される組のうち少なくとも１つの構成要素を含む、請求項１記載のシステム。
【請求項３】
前記メッセージを送信する前記参加者が送信元参加者であり；
前記メッセージを受信する前記参加者が宛先参加者であり；
前記キーサーバが新規の前記会話キーを、前記送信元参加者による要求に基づいて前記送信元参加者に公開し、これにより、前記送信元参加者がメッセージのメッセージコンテンツを、前記新規の前記会話鍵で保護することが可能になる、請求項１記載のシステム。
【請求項４】
前記キーサーバが、１つの前記要求に基づいて複数の前記新規の前記会話鍵を公開し、これにより、前記キーサーバに対して、前記会話鍵を公開するよう所望の度に要求する必要が回避される、請求項３記載のシステム。
【請求項５】
前記メッセージを送信する前記参加者が送信元参加者であり；
前記メッセージを受信する前記参加者が宛先参加者であり；
前記キーサーバが、前記送信元参加者による要求に基づいて、前記送信元参加者から新規の前記会話鍵を受領し、これにより前記キーサーバに前記会話鍵を提供し、前記キーサーバはこれを保存し、その後、前記宛先参加者に対して公開する、請求項１記載のシステム。
【請求項６】
前記キーサーバが、１つの前記要求に基づいて複数の前記新規の前記会話鍵を公開し、これにより、前記キーサーバに対して、前記会話鍵を提供するよう所望の度に要求する必要が回避される、請求項５記載のシステム。
【請求項７】
前記キーサーバが、前記宛先参加者による要求と、前記送信元参加者による許可とに基づいて、既存の前記会話鍵を前記宛先参加者に公開し、これにより、前記宛先参加者が、前記既存の前記会話鍵を使ってメッセージのメッセージコンテンツを処理できるようになる、請求項１記載のシステム。
【請求項８】
前記会話鍵に一意の識別子が関連付けられ、これにより前記宛先参加者が、メッセージのメッセージコンテンツを処理するために特定の前記会話鍵を要求する際に、前記キーサーバに前記識別子を提供できるようになる、請求項１記載のシステム。
【請求項９】
前記メッセージルータが、ヘッダ鍵を作成し、保存し、前記参加者に公開し、前記ヘッダ鍵が、メッセージのメッセージヘッダを保護するために使用される、請求項１記載のシステム。
【請求項１０】
前記ヘッダ鍵が、セキュアソケットレイヤとトランスポートレイヤセキュリティで構成される組のうち一方の構成要素に基づいている、請求項９記載のシステム。
【請求項１１】
前記ヘッダ鍵が、参加者のそれぞれで異なっている、請求項９記載のシステム。

【請求項１２】
会話が、複数の主題的に関連したメッセージのインスタンスの交換であり；
会話参加者が、前記会話に参加している参加者の組の構成要素であり；
前記会話参加者が、前記会話の、参加しているセッション期間中に、メッセージルータと少なくとも１つの継続的な接続を維持し；そして
前記ヘッダ鍵が前記それぞれのセッションで異なっている、請求項１１記載のシステム。
【請求項１３】
前記メッセージルータが、参加者の一人から、前記会話鍵を要求するメッセージのインスタンスを受信し、これを前記キーサーバへ送ることができ、さらに前記メッセージルータが前記キーサーバから、前記会話鍵を含んだメッセージのインスタンスを受信し、これを参加者の一人に送信することができ、これにより、前記キーサーバから参加者への前記会話鍵の公開が促進される、請求項１記載のシステム。
【請求項１４】
前記会話鍵を要求する前記メッセージのインスタンスが、鍵要求メッセージであり；そして
前記メッセージルータが、前記鍵要求メッセージのメッセージヘッダに基づいて、前記鍵要求メッセージを前記キーサーバに通信するか否かを決定する、請求項１３記載のシステム。
【請求項１５】
会話が、複数の主題的に関連したメッセージのインスタンスの交換であり；
会話参加者が、前記会話に参加している参加者の組のあるメンバーであり；
参加する参加者が、前記会話に参加しようとしている潜在的な前記会話参加者であり；
退出する参加者が、前記会話への参加を止めようとしている既存の前記会話参加者であり；
前記キーサーバが、前記会話のメッセージ内のサブセットのメッセージコンテンツを保護するための１つまたはそれ以上の前記会話鍵を作成し、保存し、公開し；そして
前記メッセージルータが前記キーサーバに、前記会話に前記参加する参加者または前記退出する参加者がいるか否かに基づいて、新規の前記会話鍵を今から公開するよう指示する、請求項１３記載のシステム。
【請求項１６】
ネットワーク内で、複数の参加者間でメッセージを安全に通信する方法であって、メッセージを送信する前記参加者が送信元参加者であり、メッセージを受信する参加者が宛先参加者であり、そして、メッセージがメッセージヘッダとメッセージコンテンツを備えており、前記方法が、
（ａ）送信元参加者にて：
（１）会話鍵を取得し；
（２）前記メッセージのメッセージコンテンツを、前記会話鍵に基づいて保護し、前記保護が、暗号化とハッシングで構成された組のうち少なくとも１つの構成要素を含み；そして
（３）前記メッセージをネットワークを介して宛先参加者に送信し；そして
（ｂ）宛先参加者にて：
（１）ネットワークを介して、前記送信元参加者から前記メッセージを受信し；
（２）やはりネットワーク内にあるキーサーバから前記会話鍵を取得し；そして、
（３）前記メッセージのメッセージコンテンツを、前記会話鍵に基づいて処理する（ここで前記処理は、復号とハッシュ分析のうちの少なくとも１つを含む）ことを特徴とする方法。
【請求項１７】
前記会話鍵が前記キーサーバで作成され、前記ステップ（ａ）（１）にて前記送信元参加者へ通信が行われる、請求項１６記載の方法。

【請求項１８】
複数の前記会話鍵が前記キーサーバで作成され、前記送信元参加者へ同時に通信が行われ、これにより、所望の度に、前記キーサーバに前記会話鍵を公開するよう要求する必要が回避される、請求項１７記載の方法。
【請求項１９】
前記会話鍵が前記送信元参加者で作成され、前記ステップ（ｂ）（２）の前に前記キーサーバへ通信が行われる、請求項１６に記載の方法。
【請求項２０】
複数の前記会話鍵が送信元参加者において作成され、前記キーサーバへ同時に通信が行われ、これにより、所望の度に、前記会話鍵を提供するよう送信者参加者に要求する必要が回避される、請求項１９記載の方法。
【請求項２１】
前記ステップ（ａ）（１）の前に、前記キーサーバにおいて、一意の識別子を前記会話鍵と関連付け；そして
前記ステップ（ｂ）（２）と同時に、宛先参加者の各々について、前記会話鍵が、前記一意の識別子に基づいて各々の宛先参加者に公開されることをさらに含む、請求項１９記載の方法。
【請求項２２】
前記ステップ（ａ）（３）の前に、前記メッセージのメッセージヘッダをヘッダキーに基づいて保護し；
前記ステップ（ａ）（３）の後、前記ステップ（ｂ）（１）の前に、やはりネットワーク内のメッセージルータにて、
メッセージを受信し；
メッセージヘッダを前記ヘッダキーに基づいて処理し；
前記メッセージヘッダを異なる前記ヘッダ鍵に基づいて保護し；そして
前記メッセージを、ネットワーク上で、これよりも先の宛先参加者へ送信し；そして
前記ステップ（ｂ）（１）の後に、前記メッセージのメッセージヘッダを前記異なる前記ヘッダ鍵に基づいて処理することをさらに含む、請求項１９記載の方法。
【請求項２３】
前記ヘッダ鍵のうち少なくとも１つが、セキュアソケットレイヤとトランスポートレイヤセキュリティで構成されている組の構成要素に基づいている、請求項２２記載の方法。
【請求項２４】
すべての前記ヘッダ鍵が前記参加者のそれぞれで異なっている、請求項２２記載の方法。
【請求項２５】
会話が複数の主題的に関連したメッセージのインスタンスの交換であり、会話参加者が前記会話に参加する参加者の組の構成要素であり、前記方法が、
前記会話参加が参加している会話の各セッションの期間中、前記メッセージルータとの少なくとも１つの継続的な接続を維持し；そして
前記セッションのそれぞれに異なる前記ヘッダ鍵を使用する、ことをさらに含む、請求項２４記載の方法。
【請求項２６】
前記ステップ（ａ）（１）と前記ステップ（ｂ）（２）が、やはりネットワーク内にあるメッセージルータを介して、前記キーサーバから前記会話鍵を要求する参加者を含む、請求項１９記載の方法。
【請求項２７】
前記会話鍵を要求するメッセージのインスタンスが、鍵要求メッセージであり、前記方法が、
前記メッセージルータが、前記鍵要求メッセージを前記キーサーバに通信するか否かを、前記鍵要求メッセージのメッセージヘッダに基づいて決定することをさらに含む、請求

項２６記載の方法。
【請求項２８】
会話が複数の主題的に関連したメッセージのインスタンスの交換であり、会話参加者が前記会話に参加する参加者の組の構成要素であり、参加する参加者が前記会話に参加しようとしている潜在的な前記会話参加者であり、退出する参加者が前記会話を離れようとしている既存の前記会話参加者であり、前記方法が、
前記メッセージルータが、前記会話が前記参加する参加者または前記退出する参加者を含むか否かに基づいて、新規の前記会話鍵を今から公開するよう前記キーサーバに指示することをさらに含む、請求項２６記載の方法。
【請求項２９】
通信イベントを決定するシステムであって、
通信を行っている参加者に鍵を公開するキーサーバを含み、ここで前記鍵が、通信文を暗号化する暗号鍵、または復号化する復号鍵であり、前記通信を行っている参加者が、通信文を作成しようとしている発信者と、前記通信文を見ようとしている受信者とを含み；そして
前記通信文の各々について、前記キーサーバが
識別子を割り当て；
前記識別子、対応する前記復号鍵、対応する制御イベントを含んだ記録をデータベースに保存し；
前記復号鍵のために、０、１つ、またはそれ以上の要求を受信し、前記要求が前記識別子を含み；そして
前記制御イベント、前記要求の受信数、いずれかの前記要求が受信された日時に基づいて、正のイベントと負のイベントで構成された少なくとも１つの構成要素を決定することを含むことを特徴とするシステム。
【請求項３０】
前記暗号鍵と前記復号鍵が同一である、請求項２９記載のシステム。
【請求項３１】
前記暗号鍵と前記復号鍵が異なる、請求項２９記載のシステム。
【請求項３２】
前記キーサーバが前記キーを生成することができる、請求項２９記載のシステム。
【請求項３３】
前記キーサーバが前記鍵を外部の送信元から受信できる、請求項２９記載のシステム。
【請求項３４】
前記外部送信元が前記発信者である、請求項３３記載のシステム。
【請求項３５】
前記キーサーバが、前記鍵を公開する前にアサーションを要求する、請求項２９記載のシステム。
【請求項３６】
前記制御イベントの少なくともいくつかが、前記発信者によって提供された属性に基づいて定義される、請求項２９記載のシステム。
【請求項３７】
後の前記通信に使用するだろうという推測のもとに、前記制御イベントの少なくともいくつかが前記データベースに事前に保存されている、請求項２９記載のシステム。
【請求項３８】
前記制御イベントの少なくともいくつかが、前記発信者以外の参加者から受信した属性に基づいて決定される、請求項３７記載のシステム。
【請求項３９】
前記制御イベントが、前記復号鍵を公開できるようになる時間を特定し、これにより、前記受信者が前記通信文を復号化できるようになるまでの遅延期間を特定する、請求項２９記載のシステム。

【請求項４０】
前記制御イベントが、それ以降は前記復号鍵が公開不能になる時間を特定し、これにより、その後は前記受信者がもはや前記通信文を復号化できなくなる失効日を特定する、請求項２９記載のシステム。
【請求項４１】
前記制御イベントが、前記復号鍵が前記受信者に公開されるべき回数を特定し、これにより、前記受信者が前記通信文を復号化できる回数を制限する、請求項２９記載のシステム。
【請求項４２】
前記キーサーバが、前記受信者のためのアサーションを要求し；そして
前記制御イベントが、前記復号鍵を前記受信者に公開する前に満たさなければならない少なくとも１つの条件を特定する、請求項２９記載のシステム。
【請求項４３】
前記キーサーバが、前記正のイベントまたは前記負のイベントのうち少なくとも１つに関するデータを、前記発信者と他のエンティティの内少なくとも一方に通信する、請求項２９記載のシステム。
【請求項４４】
前記他のエンティティが通知サーバである、請求項４３記載のシステム。
【請求項４５】
通信イベントを決定する方法であって、前記方法が、
（ａ）前記通信文を証明するためにリソースＩＤの第１の要求を受信し、前記第１の要求が、前記通信文の目的受信者の少なくとも１つの証明書を含み；
（ｂ）少なくとも１つの制御イベントを定義し、前記制御イベントが前記少なくとも１つの証明書を含み；
（ｃ）前記第１の要求に応答して前記リソースＩＤを提供し；
（ｄ）前記リソースＩＤと、前記制御イベントと、前記通信を復号化するための復号鍵とを保存し；
（ｅ）前記復号鍵のための第２の要求を監視し、前記第２の要求が前記リソースＩＤを含み、推定上の前記目的受信者の情報を証明し；
（ｆ）前記第２の要求が受信されると、これが前記制御イベントと一致するか否かを決定し、そして
（１）一致する場合は、
（ｉ）前記第２の要求に応答して前記復号鍵を提供し；そして
（ｉｉ）前記証明情報と正のイベントを前記リソースＩＤに関連して保存し、
（２）一致しない場合は；負のイベントを前記リソースＩＤに関連して保存し；そして
（ｇ）あるいは、前記目的とする受信者についての前記第２の要求が受信されない場合、負のイベントを前記リソースＩＤに関連して保存することを特徴とする方法。
【請求項４６】
前記ステップ（ｃ）が暗号鍵を提供することを含む、請求項４５記載の方法。
【請求項４７】
前記暗号鍵と前記復号鍵が同一である、請求項４６に記載の方法。
【請求項４８】
前記暗号鍵と前記復号鍵が異なる、請求項４６に記載の方法。
【請求項４９】
前記第１の要求が認証アサーションを含み、前記ステップ（ａ）が、前記ステップ（ｃ）で前記リソースＩＤを提供する前に、前記認証アサーションを検証する、請求項４５記載の方法。
【請求項５０】
前記制御イベントの少なくともいくつかが、前記通信の発信者が提供した属性に基づい

て定義される、請求項４５記載の方法。
【請求項５１】
前記制御イベントの少なくともいくつかが、通信においてその後の使用を予測して、前記ステップ（ａ）の前にあらかじめ保存される、請求項４５記載の方法。
【請求項５２】
前記制御イベントの少なくともいくつかが、前記発信者以外の参加者から受信した属性に基づいて決定される、請求項５１記載の方法。
【請求項５３】
前記制御イベントが、前記復号鍵が前記受信者に公開可能となる時間を特定する、請求項４５記載の方法。
【請求項５４】
前記制御イベントが、前記復号鍵が前記受信者に公開不能となる時間を特定する、請求項４５記載の方法。
【請求項５５】
前記制御イベントが、前記復号鍵を前記受信者に公開できる回数を特定する、請求項４５記載の方法。
【請求項５６】
前記第２の要求が、前記証明情報を含んだ認証アサーションを有し、ステップ（ｆ）が、前記復号鍵の提供の前に、前記認証アサーションを検証する、請求項４５記載の方法。
【請求項５７】
前記正のイベントと前記負のイベントの少なくとも１つに関するデータを、前記通信文の発信者と他のエンティティの内少なくとも１つへ通信するステップ（ｈ）をさらに含む、請求項４５記載の方法。
【請求項５８】
前記別のエンティティが通知サーバである、請求項５７記載の方法。
【請求項５９】
トランザクション送信元とトランザクション対象者が、否認不可能なトランザクションを交換する方法であって、方法が、
（ａ）前記トランザクションを証明するためにトランザクション識別子の第１の要求を受信し、前記要求が送信元認証アサーションを含み；
（ｂ）前記送信元認証アサーションを検証し；
（ｃ）前記トランザクション識別子と前記送信元認証アサーションからの情報とを保存し、これによりトランザクション送信元が、前記トランザクションの暗号化および送信の後に、もっともらしく否認できないようにする情報を確立し；
（ｄ）前記第１の要求に応答して前記トランザクション識別子を提供し、これにより、前記トランザクションと前記トランザクション識別子が前記トランザクション対象者へ送信され；
（ｅ）前記トランザクション対象者がトランザクションを受信すると、これを復号化するための復号鍵の第２の要求を受信し；前記第２の要求が、前記トランザクション識別子と対象者認証アサーションを含み；
（ｆ）前記対象者認証アサーションを検証し；
（ｇ）前記対象者認証アサーションからの情報を、トランザクション識別子と共に保存し；そして
（ｈ）前記第２の要求に応答して前記復号鍵を提供することでトランザクションの復号化が可能になり、これにより、トランザクション対象者がトランザクションの受信者であることをもっともらしく否認することを不可能にする情報を確立することを含むことを特徴とする方法。
【請求項６０】
前記ステップ（ｄ）が、トランザクションを暗号化するための暗号鍵を提供することも含む、請求項５９記載の方法。

【請求項６１】
前記方法が、
（ｉ）トランザクション送信元に関する送信元情報の情報要求を受信し、前記情報要求が前記トランザクション識別子を含み；
（ｊ）前記ステップ（ｃ）で、前記トランザクション識別子と共に保存された前記送信元認証アサーションからの前記情報を少なくともいくつか取り出し、ここから前記送信元情報を決定し；さらに、
（ｋ）前記情報要求に応答して前記送信元情報を提供する、ことをさらに含む、請求項５９記載の方法。
【請求項６２】
前記方法が、
（ｉ）対象者情報の情報要求を受信し、前記情報要求が前記トランザクション識別子と、前記トランザクションターゲットを証明する情報を含んでおり；
（ｊ）トランザクション対象者を証明する前記情報が、前記ステップ（ｇ）で保存されたトランザクション識別子と共に保存されている前記対象者認証アサーションからの前記情報のいずれかと一致するか否かを決定し、これから前記対象者情報を決定し；そして
（ｋ）前記情報要求に応じて前記対象者情報を提供する、ことをさらに含む、請求項５９記載の方法。
【請求項６３】
トランザクションを、前記トランザクションの起源であるトランザクション送信元による否認防止可能として確立する方法であって、前記方法が、
（ａ）前記トランザクションを証明するためのトランザクション識別子の要求を受信し、前記要求が送信元認証アサーションを含み；
（ｂ）前記送信元認証アサーションを検証し；
（ｃ）前記トランザクション識別子と前記送信元認証アサーションからの情報とを保存し；そして
（ｄ）前記要求に応答して前記トランザクション識別子を提供し、これにより、トランザクション送信元が前記トランザクションの起源であることをもっともらしく否認できないようにする情報を確立することを含むことを特徴とする方法。
【請求項６４】
前記ステップ（ｄ）が、前記トランザクションを暗号化するための暗号鍵を提供することも含む、請求項６３記載の方法。
【請求項６５】
前記方法が、
（ｅ）トランザクション送信元に関する送信元情報について情報要求を受信し、ここで前記情報要求が前記トランザクション識別子を含み；
（ｆ）ステップ（ｃ）で前記トランザクション識別子とともに保存された前記送信元認証アサーションから前記情報の少なくともいくつかを取り出し、ここから前記送信元情報を決定し；そして
（ｇ）前記情報要求に応答して前記送信元情報を提供する、ことを含む、請求項６３記載の方法。
【請求項６６】
前記送信元情報が、トランザクション送信元が実際に誰であるかを表している、請求項６５記載の方法。
【請求項６７】
前記ステップ（ｅ）で受信された前記情報要求が、トランザクション送信元であると思われる参加者を証明する情報も含み；
前記ステップ（ｇ）で提供された前記送信元情報が、前記参加者がトランザクション送信元であるか否かのみを表しているため、特にトランザクション送信元を証明することなく、前記情報要求に応答する、請求項６５記載の方法。

【請求項６８】
前記ステップ（ｃ）がまた、トランザクションの復号化に使用できる復号鍵も保存し；そして
ステップ（ｇ）が、前記復号鍵も提供し、これにより、前記情報要求を行った参加者が、たとえ前記参加者がトランザクション送信元またはトランザクションの対象者でない場合でも、トランザクションの復号化を容易に実施できるようになる、請求項６５記載の方法。
【請求項６９】
前記ステップ（ｅ）で受信された前記情報要求がトランザクションも含み；そして
前記ステップ（ｇ）が、前記情報要求に応答して前記送信元情報を提供する前に、前記トランザクションを復号化することを含む、請求項６５記載の方法。
【請求項７０】
前記ステップ（ｅ）で受信された前記情報要求がトランザクション送信元であると思われる参加者を証明する情報も含み；そして
前記ステップ（ｇ）で提供された前記送信元情報が、前記参加者がトランザクション送信元であるか否かのみを示しており、これにより、前記トランザクション送信元を特に証明することなく前記第２の要求に応じる、請求項６９記載の方法。
【請求項７１】
前記ステップ（ｇ）が、前記情報要求への前記応答に、復号化した形式のトランザクションを提供することも含み、これにより、前記情報要求を行っている参加者が、トランザクション送信元またはトランザクションの対象者でない場合でも、トランザクションのコンテンツを確認できるようになる、請求項６９記載の方法。
【請求項７２】
トランザクションを、前記トランザクションの受信者であるトランザクション対象者による否認防止可能として確立する方法であって、トランザクション識別子がトランザクションを識別し、復号鍵が、あらかじめ保存されているトランザクションを復号化することが不可能であり、前記方法が、
（ａ）復号鍵の要求を受信し、ここで前記要求がトランザクション識別子と対象者認証アサーションとを含み；
（ｂ）前記対象者認証アサーションを検証し；
（ｃ）前記対象者認証アサーションからの情報を前記トランザクション識別子と共に保存し；そして
（ｄ）前記要求に応答して前記復号鍵を提供し、これにより、トランザクション対象者がトランザクションの受信者であることをもっともらしく否認できないようにする情報を確立することを含むことを特徴とする方法。
【請求項７３】
前記方法が、
（ｅ）対象者情報の情報要求を受信し、ここで前記情報要求が前記トランザクション識別子と、トランザクション対象者を証明する情報とを含み；
（ｆ）前記ステップ（ｃ）にて前記トランザクション識別子と共に保存された前記対象者認証アサーションからの前記情報の少なくともいくつかを取り出し、これから前記対象者情報を判断し；そして
（ｇ）前記情報要求に応答して前記対象者情報を提供する、ことをさらに含む、請求項７２記載の方法。
【請求項７４】
前記ステップ（ｇ）が前記復号鍵を提供することも含み、これにより、前記情報要求を行っている参加者が、たとえトランザクション送信元またはトランザクション対象者でない場合にも、トランザクションの復号化を容易に実施できるようになる、請求項７３記載の方法。
【請求項７５】

前記ステップ（ｅ）で受信された前記情報要求がトランザクションも含み；そして
前記ステップ（ｇ）が、前記識別情報を提供する前に、前記トランザクションを復号化する、請求項７３記載の方法。
【請求項７６】
前記ステップ（ｇ）が、前記情報要求への前記応答において、復号形式の前記トランザクションを提供することも含み、これにより、前記情報要求を行っている参加者が、トランザクション送信元またはトランザクション対象者でない場合にも、トランザクションのコンテンツを確認することが容易になる、請求項７５記載の方法。
【請求項７７】
トランザクション送信元とトランザクション対象者がトランザクションを交換する、否認不可能なシステムであって、
コンピュータ化されたキーサーバ含み；
前記キーサーバが、トランザクション識別子を要求する第１の要求をネットワーク経由で受信するのに適しており、ここで前記第１の要求が送信元認証アサーションを含み；
前記キーサーバが、前記トランザクションの復号化に使用する復号鍵を要求する第２の要求をネットワーク経由で受信するのに適しており、ここで前記第２の要求が、前記トランザクション識別子と対象者認証アサーションとを含み；
前記キーサーバが、前記送信元認証アサーションと前記対象者認証アサーションとを検証するのに適しており；
前記キーサーバが、前記トランザクション識別子と、前記送信元認証アサーションからの情報とを、前記対象者アサーションからの情報に関連してデータベースに保存するのに適しており；
前記キーサーバが、前記第１の要求に対して、前記トランザクション識別子を含む第１応答を、前記ネットワーク経由で提供するのに適しており；そして
前記キーサーバが、前記第２の要求に対して、前記復号鍵を含む第２応答を、前記ネットワーク経由で提供するのに適しており、これにより、トランザクション送信元が、前記トランザクションの暗号化および送信した後に、もっともらしく否認することを不可能にし、前記トランザクション対象者が、前記復号鍵を提供された後に、もっともらしく否認することを不可能にする情報を確立することを特徴とするシステム。
【請求項７８】
前記キーサーバがさらに、前記トランザクションを暗号化するための暗号鍵を前記第１応答において提供するのに適している、請求項７７記載のシステム。
【請求項７９】
前記キーサーバがさらに、前記トランザクション送信元に関する送信元情報の情報要求を受信するのに適しており、ここで前記情報要求が前記トランザクション識別子を含み；
前記キーサーバがさらに、前記データベースから、前記トランザクション識別子と共に保存されている、前記送信元認証アサーションからの前記情報を取り出し、ここから前記送信元情報を判定するのに適しており；そして
前記キーサーバがさらに、前記情報要求に応答して前記送信元情報を提供するのに適している、請求項７７記載の方法。
【請求項８０】
前記キーサーバがさらに、対象者についての情報要求を受信するのに適しており、ここで前記情報要求が、前記トランザクション識別子と、前記トランザクション対象者を識別する情報とを含み；
前記キーサーバがさらに、前記トランザクション対象者を証明する前記情報が、トランザクション識別子と共に保存された前記対象者認証アサーションからの前記情報のいずれかと一致するか否かを判断し、ここから前記対象者情報を判断するのに適しており；そして
前記キーサーバがさらに、前記情報要求に応じて前記対象者情報を提供するのに適している、請求項７７記載のシステム。

【請求項８１】
トランザクションを、その起源であるトランザクション送信元による認証否認可能として確立するシステムであって、
コンピューター化されたキーサーバを含み、
前記キーサーバが、トランザクションを識別するトランザクション識別子の要求をネットワーク経由で受信するのに適しており、ここで前記要求が送信元認証アサーションを含み；
前記キーサーバが、前記送信元認証アサーションを検証するのに適しており；
前記キーサーバが、前記トランザクション識別子と、前記送信元認証アサーションからの情報をデータベースに保存するのに適しており；そして
前記キーサーバが、前記トランザクション識別子を含んだ返答を前記ネットワーク経由で提供し、これにより、前記トランザクション送信元が、前記トランザクションを暗号化および送信した後で、もっともらしく否認することを不可能にする情報を確立するのに適していることを特徴とするシステム。
【請求項８２】
前記キーサーバがさらに、前記返答に含まれたトランザクションを暗号化するための暗号鍵を提供するのに適している、請求項８１記載のシステム。
【請求項８３】
前記キーサーバがさらに、トランザクション送信元に関する送信元情報の要求を受信するのに適しており、ここで前記情報要求が前記トランザクション識別子を含み；
前記キーサーバがさらに、前記トランザクション識別子と共に保存されている前記送信元認証アサーションからの情報を、前記データベースから取り出し、ここから前記送信元情報を判断するのに適しており；そして
前記キーサーバがさらに、前記情報要求に応答して前記送信元情報を提供するのに適している、請求項８１記載のシステム。
【請求項８４】
トランザクションを、その受信者であるトランザクション対象者による否認防止可能として確立するシステムであって、ここでトランザクション識別子がトランザクションを識別し、前記トランザクションの復号化に使用される復号鍵がデータベース内にあらかじめ保存されており、前記システムが、
コンピュータ化されたキーサーバを含み、
前記キーサーバが、前記復号鍵の要求をネットワーク経由で受信するのに適しており、ここで前記要求が前記トランザクション識別子と対象者認証アサーションとを含み；
前記キーサーバが、前記対象者認証アサーションを検証するのに適しており；
前記キーサーバが、前記対象者認証アサーションからの情報を、前記トランザクションと共にデータベース内に保存するのに適しており；
前記キーサーバが、前記復号鍵を含んだ返答を、前記ネットワーク経由で提供し、これにより、前記トランザクション対象者がもっともらしく否認することを不可能にする情報を確立するのに適していることを特徴とするシステム。
【請求項８５】
前記キーサーバがさらに、対象者情報についての情報要求を受信するのに適しており、ここで前記情報要求が、前記トランザクション識別子と、前記トランザクション対象者を証明する情報とを含み；
前記キーサーバがさらに、前記トランザクション識別子と共に保存されている前記対象者認証アサーションから前記情報の少なくともいくつかを取り出し、ここから前記対象者情報を判断するのに適しており；そして
前記キーサーバがさらに、前記情報要求に応答して前記対象者情報を提供するのに適している、請求項８４記載のシステム。

【発明の詳細な説明】

【技術分野】
【０００１】
本発明は、一般に、インターネットを含むネットワーク上で通信が行われるメッセージのセキュリティの提供、より詳細には、メッセージに関連したイベントを決定し、これを監査し、メッセージを否認防止可能にするための情報の確立に関する。
【背景技術】
【０００２】
実質的にすべての電子通信媒体のユーザが、このようなシステム内に保存されている通信文の安全性について考えてみたことがある。これに関しては様々な理由があり、とてもここで扱いきれる数ではないのだが、そのうちの数例は、複雑なテクノロジーへの依存によらなければならないもの、未知で恐らくは信頼できない仲介機関への依存によらなければならないもの、かつ、通信伝送距離と、我々が到達しようとしている巨大な人口に起因する電子ネットワークにおける匿名性の増加によるものである。
【０００３】
既存の通信システムがセキュリティメカニズムを確立し、ユーザから信頼されるようになるまでには長い時間がかかった。米国では従来の郵便制度が良い例である。我々が投函した郵便物は、往々にして物理的に非常に安全な容器内に入れられる。次に、郵便物は集配され、分類され、配送され、最終的に、受取人によって内容物が回収される、似たような容器へと配達される。差出人の容器と受取人の容器の間で郵便物を取り扱う人々は、我々にとって周知であり、非常に信頼できると考えられている単一組織（少なくとも米国内）の一部である。我が国の郵便システムのセキュリティが稀に間違いを起こした時でさえ、この間違いを検出して修正するメカニズムが整っている。
【０００４】
不幸なことに、我々の多くは、電子通信の安全性については郵便システムに全く及ばない程度の信頼しか抱いていないが、その理由は、これが現代ネットワーク内で、送信者と受信者の間でやりとりされるためである。一般に、我々は、電子メール、インスタントメッセージ、ビデオ会議、共同文書などのようなメッセージの送信および受信のための「容器」の安全性を維持していると、我々の知識の範囲内だけで信じている。これは、これらの容器が、我々個人の物理的管理範囲内にあるパーソナルコンピュータ（ＰＣ）、ワークステーション、インターネット機器などであるためである。また、我々は通常、こうした容器どうし間の、電子媒体内で起こっていることは管理できないと思っている。例えば、送信者と受信者が賢くならない限り、安全化されていないメッセージを受信およびコピーしてしまう悪人は潜在的にいくらでもいるのである。さらに悪いことに、多くの場合、電子通信文はその通過過程において紛失されたり、悪意によって改ざんされ、不当にでっち上げられて全く別のものにされてしまう可能性がある。
【０００５】
電子メッセージセキュリティの問題は深刻であり、既に多大な注目を浴びている。セキュリティの侵害を罰し、侵害を思いとどまらせるために、少なくとも電子メールメッセージについては既に法的なメカニズムが配備され、その処罰は重くなり続けている。しかしながら、電子メッセージが遠距離の高速移動という非常に有益な機能を有するということは、同時に、電子メッセージがこうした法的努力を潜在的に妨害し、ユーザの秘密を確実に危機に陥れる可能性があることを意味する。
【０００６】
古い技術は、最新電子媒体で使用するために再生、拡大され続けているが、これらは多くの場合、安全性を高めるために、従来の郵便システムと組み合わせて長いこと使用されてきたものの応用形である。したがって、我々は暗号技術への関心とその使用の蘇生を見ているのである。
【０００７】
電子通信を安全化する既存のシステムの多くは扱い難いか、十分に信用されていないか、あるいはその両方である。現代の電子通信を可能かつ効率的にしたこの電子システムが

、多数の従来の暗号システムを旧式にし、または少なくとも非常に疑わしいものにしている。これと最新性が同じ、またはより高いコンピュータシステムは、多数の退屈なオペレーションを実質的に平行な方法でスタガリングする能力を備えており、過去の多くの強力な暗号システムはもはや信頼できないものとして示されている。

【０００８】

しかし、電子通信を安全化する新規のシステムが登場している。過去２５年間において、一般に「公開鍵インフラストラクチャ」（ＰＫＩ）と呼ばれる、公開鍵と秘密鍵に基づくシステムが導入され、その開発が急速に進み、最近では使用されてきた。これらのシステムは現在非常に普及しているが、その使用は未熟かつ不当であると思われる。

【０００９】

ＰＫＩシステムの基礎は、一般に１９７０年代中頃に、Massachusetts Institute of TechnologyのRon Rivest、 Adi Shamir、 Leonard Adlemanの貢献によってもたらされた。この貢献の結果開発された、一般にＲＳＡアルゴリズムとして知られているものは、プリンシパルに公開鍵と秘密鍵の両方を割り当てる暗号技術である。公開鍵は全員に公開されるが、秘密鍵は秘密性を保持される。使用される鍵は、時として数百桁の大きな素数と、大きな数字の数学的因数分解の難しさが存在するＲＳＡアルゴリズムの固有の強度の両方である。

【００１０】

メッセージを安全に送信するには、そのメッセージを、その宛先受信者（ここではプリンシパル）の公開鍵を使って暗号化する。次に、受信者のみが、自分の秘密鍵を使ってそのメッセージを復号化および読み出すことができる。この単純なシナリオでは、誰もが受信者にメッセージを送信で、受信者のみがそのメッセージを読むことができる。

【００１１】

ＰＫＩ手法のより有用な特徴は、送信者もプリンシパルになることができ、この送信者のみが送信できるメッセージ、すなわち認証防止メッセージを送信することができることである。このために、送信者は、自分の秘密鍵を使ってメッセージ（多くの場合、長いメッセージの内の一部分のみ）を暗号化する。これにより、その送信者の公開鍵を使用してしかそのメッセージを解読できないため、受信者は、送信者とされている者が実は問題となっている送信者、人物であることを知ることができる。

【００１２】

実際に、ＰＫＩシステムでは送信者と受信者の両方がプリンシパルであることが多い。送信者は自分の秘密鍵を使って「署名」を暗号化し、この署名をメッセージに嵌め込み、さらにこれを受信者の公開鍵を使って暗号化する。これにより、メッセージが受信者以外の人物から保護される。受信者のみが、自分の秘密鍵を使ってそのメッセージを復号化でき、受信者はこの復号化が済むと、さらに送信者の公開鍵を使って署名だけを復号化する。この方法で、受信者は、送信者が否認することを禁止された、署名の送信元である本人であると知って安心できる（さらに、無条件にメッセージ全体が本物であるとわかるが、しかし、メッセージ全体のハッシュといったものを署名に一意に含めることでより安全になる）。

【００１３】

しかし、ＰＫＩは「インフラストラクチャ」という用語を使用しているとおり、この普及した暗号システムには大規模なサポートシステムが必要である。公開鍵は公開されなければならず、これにより、メッセージを送信したい人物が目的のメッセージ受信者用の鍵を決定することができる。さらに、公開鍵は指定された期間（例えば1年間）だけ認証され、その後は更新する必要がある。最後に、秘密鍵が危険にさらされた場合、または危険にさらされた疑いがある場合には、対応する秘密鍵を破棄しなければならない。したがって、すべての通信参加者は、公開鍵をメッセージの暗号化または署名の検証に使用する前に、公開鍵の破棄状態を調べる必要がある。通常、これらの作業は「認証局」によって取り扱われる。そのため、不幸にも現在、我が国の競争社会の市場において実証されているとおり、複数の認証局が加入を求めて競い合い、潜在的なユーザを完全に混乱させる結果

を引き起こす。さらに、公開鍵のライフサイクル（作成、配布、更新、破棄）によって、展開シナリオが複雑かつ管理不能なものになる可能性がある。

【００１４】

例えば、自分達の間だけで安全な通信を実現したいと願う小規模グループどうしで、また、否認の心配がない場合には、認証局を使用せずに公開および秘密鍵システムを実施することはもちろん可能である。しかし、適切に実証されたＲＳＡアルゴリズムの、またはこれに関連した初期公開に対する我が国の政府の反応は、完全に拘束から解放された社会が政府の社会を守る能力への脅威になりかねないという非常に否定的なものである。ほとんどの統治機関が、この超強力な暗号技術の使用を完全に抑制することは今や遅すぎるであろうが、このような統治機関が、本当に適切な場合のみに開封できる暗号システム（多くの場合「キーエスクロウ」システムと呼ばれる）を今後さらに受け入れる可能性がある。

【００１５】

さらにＰＫＩには、これ以外にも、その使用性と効率性に関連した問題がいくつかある。鍵は、通常平均的な人間が記憶できる能力を超える、非常に大きなものであるため、その扱いが難しい。鍵を扱うためだけに、マシンに基づく記憶装置と使用メカニズムを採用しなければならない。これは、複数のシステムにかけてのモバイル使用と、揮発性メモリからの削除後の修復にとって非常に重要であり、これによって、秘密鍵を格納するために必要な効率的に物理鍵となるものの保護に関連したさらに多くの問題が生じる。さらに、ＰＫＩのような受信者に基づく鍵システムは扱い難い場合がある。例えば、宛先受信者が複数である場合、その各々について公開鍵を取得し、各々メッセージコピーを暗号化するためにそれぞれ別個に使用する。これは、宛先メッセージ受信者のリストが大きくなるに従い、非常に重大な計算上の負担を包含しかねない。したがって、実際の使用上での一般的な例では、まず、１つの対称鍵を使ってメッセージを暗号化する。次に、各受信者の公開鍵を使ってメッセージ鍵を複数回暗号化する。これにより、メッセージ自体が一度だけ暗号化される。複数回暗号化されるのはメッセージ鍵である。

【００１６】

したがって、従来技術の暗号システムとＰＫＩシステム、およびこれらを採用する電子メッセージシステムは多くの恩恵を提供する。しかし不幸にも、これらでさえもまだ不十分であることがわかった。このようなシステムを改良し、増設し、さらには交換することが望ましいことが次々と明白になったため、本発明の発明者が「セキュア電子メールシステム」と「セキュリティサーバシステム」を開発した。これらは、米国特許第６，５８４，５６４号、米国特許出願第１０/３０５，７２６号においてそれぞれ網羅されており、本明細書中ではその全体が参照により組み込まれている。

【００１７】

上述の手法は、大幅に改良されたデジタルメッセージ通信であるが、それでもまだ改良の余地はある。例えば、多くのビジネスがデジタル通信を使用して、顧客、供給業者、共同経営者、その他のビジネス提携者とのビジネスを遂行している。デジタル通信（例えば電子メール、企業内インスタントメッセージング（ＥＩＭ）など）は、非デジタル通信（例えば書類郵便物）と同様、スタンドアロンプロセスではまずない。多くの場合、デジタル通信は総体的なビジネスプロセスの流れの１ステップであり、１つのビジネスイベントによって誘発される。例えば、金融ブローカー企業が、顧客の追加証拠金支払いの期日が来たと判断したとき、顧客に通知する必要がある。ブローカー企業は顧客に電話をかけて適切な処置を行うことができる。顧客がその通知を開封したか否かを判断するビジネス能力があれば、顧客に電話で確認する工程に大きく影響する。この例では、顧客が通知を開封したことを企業側が証明できれば、顧客に電話をかけて追及する必要はない。これにより顧客に確認する電話の数が減り、企業の節約につながる。

【００１８】

例示の目的で電子メールを使用して技術背景を説明する。電子メールは、トランザクション（電子メール）、トランザクション発信者（電子メールの送信者）、トランザクショ

ン対象者（一人またはそれ以上の電子メール受信者）が常に関与するため、この説明に適している。さらに、送信者と受信者が相互に対して直接通信を行わない、分断された環境を仮定する。電子メールを読み出すことにより１つのイベントが構成され、さらに、指定された期間内に電子メールの読み出しを行わない場合にも1つのイベントが構成される。このようなイベントの知識は、企業および他の状況の両方において特に有用である。

【００１９】

例えばビジネスプロセスの文脈にて上述したような、既存のデジタルメッセージ通信システムには多数の制限がある。例えば、これらのシステムは透明性でない。公開鍵インフラストラクチャ（ＰＫＩ）のような既存の技術では、通信が行われたデータの受領の通知にユーザが参加する必要がある。これはアクションおよびアクションの欠如のどちらもサポートしていない。既存の技術では、こうしたシステムの使用によって提供される情報は、通信が行われたデータの受信に関する情報だけである。受信の欠如に関する情報は提供されない。さらに、既存のシステムは分断されていない。こうしたシステムが使用する既存の技術、例えばウェブに基づく通信では、通信データの送信者が受信者と直接接続する必要がある。さらに、受信者の自発的な参加を要する。例えば、受信確認電子メールでは受信者の自発的参加が必要である。受信者が通信文の受信を通知しないことを選択した場合、発信者はこのイベントと、通信文を受信していない受信者とを区別することが全くできない。既存のシステムはこの制限により、不当にも、発信者が制御するシステムではなく、受信者が制御するシステム、または全く制御されないシステムになってしまう。さらに、ＰＫＩに基づく電子メールのような既存技術では、発信者は、いつ受信者にデータを読めるようにするかを制御できない。メッセージが送信されれば、受信者はその到着と同時にこれを読むことができる。さらに既存のシステムは、通信データの容量によって制約されている場合が多い。ウェブに基づく通信のような既存技術は、通信データのサイズに依存している。データのサイズが大きいほど、より大容量のメモリ、基礎システムのより高い処理能力が必要になる。これによって、予測される通信システム能力の管理が難しくなると思われる。

【００２０】

したがって、ビジネス通信を含む、しかし必ずしもこれに限定されないデジタル通信に関連したイベントの決定に関する限り、従来技術の暗号システム、特にＰＫＩシステムは不十分であることが証明された。

【００２１】

上述した手法は、デジタル通信の利用に伴う問題をすべて述べていない。一般的な従来技術のシステムは、本発明者による過去の発明品と同様に、通信の否認防止と監査という、２つの特に難しい問題を検討する方法についてそれほど説明していない。

【００２２】

否認防止または監査のいずれかを提供する既存のデジタルメッセージ通信用システムには多数の規制がある。例えば、これらのシステムは透明性でない。ＰＫＩのような技術は、ユーザに秘密鍵を保持させ、これを活発に使用して署名を生成させる負担を課す。さらに、参加者はトランザクションがコピーを有することを証明するか、あるいはトランザクション署名者のデジタル証明書を取り出す必要がある。またさらに、既存の技術は、否認防止と監査のいずれにも何のサービスも提供しない。ＰＫ－Ｉに基づく技術は、すべての参加者（トランザクションの発信者と対象者の両方）が信頼する公開鍵インフラストラクチャを使用しなければならない。ＰＫＩ技術以外の技術（例えば、データベースでのトランザクションログの保存）は、完全に異なるメカニズムを使用し、ＰＫＩと相互動作しない。そのため、既存のシステムはＰＫＩに基づく技術またはＰＫＩ技術以外の技術を使用するが、両方と実質的に相互動作することが不可能であり、またその必要もない。さらに、既存の技術は単一レベルの強度の否認防止しか提供していないが、その場合、異なる程度は通常、状況を変えるために適当である。例えば、ＰＫＩでは否認防止の強度は、その基礎となる証明書の確実性のレベルに等しい。トランザクション実行中の参加者は、異なる確実性を有する異なる証明書を使用することで強度を変更することしかできない。さら

に既存の技術は、否認防止と監査に厳しい信頼規則を課している。例えば、ＰＫＩシステムでは、トランザクションを検証する参加者は、署名者の証明書を信頼しなければならない。ＰＫＩシステム以外のシステムでは、検証者は、トランザクションログを保持するシステムを信頼しなければならない。

【００２３】

したがって、従来技術の暗号およびＰＫＩシステムは、デジタルメッセージ通信における否認防止および監査の問題を十分に解決できていない。

【特許文献１】米国特許第６，５８４，５６４号明細書

【特許文献２】米国特許出願第１０/３０５，７２６号明細書

【発明の開示】

【発明が解決しようとする課題】

【００２４】

したがって、本発明の目的は、インターネットのようなネットワーク上で通信が行われるメッセージに安全性を提供することである。

【００２５】

簡潔に言えば、本発明の一つの好ましい実施形態は、メッセージがメッセージヘッダとメッセージコンテンツを備える場合に、複数の参加者間でメッセージを安全に通信するシステムである。このシステムでは、メッセージルータが、参加者どうしをネットワーク経由で接続し、参加者間で、メッセージをそのメッセージヘッダに基づいて配送する。キーサーバは参加者に会話鍵を作成、保存、公開するが、この会話鍵は、メッセージのメッセージコンテンツを暗号化、復号化するために使用される。

【００２６】

簡潔に言えば、本発明の別の好ましい実施形態は、ネットワーク上の複数の参加者間で安全に通信する方法である。メッセージ送信する参加者は送信元参加者であり、メッセージを受信する参加者は宛先参加者である。メッセージは、メッセージヘッダとメッセージコンテンツを備える。この方法では、送信元参加者が、やはりネットワーク上にあるキーサーバから会話鍵を取得する。次に、送信元参加者は、この会話鍵に基づいて、メッセージのメッセージコンテンツを暗号化する。その後、メッセージをネットワーク経由で宛先参加者に送信する。すると、宛先参加者が、送信者参加者からのメッセージをネットワーク経由で受信する。宛先参加者は、上記のキーサーバから会話鍵を取得する。最後に、宛先参加者は、この会話鍵に基づいてメッセージのメッセージコンテンツを復号化する。

【００２７】

簡潔に言えば、本発明の別の好ましい実施形態は、通信イベントを決定するシステムである。通信参加者に鍵を公開するためにキーサーバを設けており、鍵は、通信文を暗号化する暗号鍵、または復号化する復号鍵であり、通信参加者には通信文を作成しようとする発信者と、通信文を見ようとする受信者が含まれる。キーサーバは、各通信文にさらに識別子を割り当て、識別子、対応する復号鍵、対応する制御イベントを含んだ記録をデータベースに保存する。さらにキーサーバは、各通信文につき、復号鍵を要求するゼロ、１つ、またはそれ以上の要求を受信し、ここで、これらの要求は識別子を含んでいる。さらに、キーサーバは、各通信文について、制御イベントと、受信した要求の数、または要求の受信時間に基づいて、正のイベントと負のイベントで構成された少なくとも１つの構成要素のセットを決定する。

【００２８】

簡潔に言えば、本発明の別の好ましい実施形態は、通信イベントを決定する方法である。通信文を証明するリソースＩＤの第１の要求が受信され、ここで、この第１の要求は、その通信の目的とされる受信者の少なくとも１つの証明書を含んでいる。少なくとも１つの制御イベントが定義されるが、この制御イベントは少なくとも１つの証明書を含んでいる。第１の要求に応答してリソースＩＤが提供される。リソースＩＤ、制御イベント、通信文を復号化する復号鍵が記憶される。復号鍵を要求する第２の要求が監視されるが、ここで、この第２の要求はリソースＩＤと、推定上目的とされる受信者についての証明情報

を含んでいる。第２の要求を受信したら、制御イベントと一致するか否かが判断される。一致した場合には、第２の要求に応答して復号鍵が提供され、証明情報と正のイベントがリソースＩＤに関連して記憶される。受信した第２の要求が一致しない場合には、負のイベントがリソースＩＤに関連して記憶される。あるいは、目的の受信者について第２の要求が受信されない場合には、負のイベントがリソースＩＤに関連して記憶される。

【００２９】

簡潔に言えば、本発明の別の好ましい実施形態は、トランザクション送信元とトランザクション対象者が、否認不可能なトランザクションを交換する方法である。トランザクションを証明するためのトランザクション識別子を要求する第１の要求が受信され、ここで、この要求は送信元認証アサーションを含んでいる。次に、送信元認証アサーションが検証される。トランザクション識別者と、送信元認証アサーションからの情報が保存され、これにより、トランザクション送信元が、トランザクションを暗号化および送信した後には、もっともらしく否認できないようにする情報が確立される。第１の要求に応答してトランザクション識別子が提供されるので、トランザクションとトランザクション識別子をトランザクション対象者に送信することができる。復号鍵の第２の要求がトランザクション対象者によって受信されると、トランザクションを復号化するための復号鍵の第２の要求が受信されるが、この場合、第２の要求はトランザクション識別子と対象者認証アサーションを含む。次に、対象者認証アサーションが検証される。対象者認証アサーションからの情報もトランザクション識別子と共に保存される。次に、第２の要求に応答して復号キーが提供されるため、トランザクションを復号化することができ、これにより、トランザクション対象者が、トランザクションの受信者であることをもっともらしく否認できないようにする情報が確立される。

【００３０】

簡潔に言えば、本発明の別の好ましい実施形態は、トランザクションを、トランザクションの発信者であるトランザクション送信元による否認防止可能なものとして確立する方法である。トランザクションを証明するトランザクション識別子の要求が受信されるが、この要求は送信元認証アサーションを含んでいる。次に、送信元認証アサーションが検証される。トランザクション識別子と、送信元認証アサーションからの情報が保存される。さらに、この要求に応答してトランザクション識別子が提供され、これにより、トランザクション送信元がトランザクションの発信元であるということをもっともらしく否認できないようにするための情報が確立される。

【００３１】

簡潔に言えば、本発明の別の好ましい実施形態は、トランザクションを、トランザクションの受信者であるトランザクション対象者による否認防止可能を確立する方法であり、ここで、トランザクション識別子がトランザクションを識別し、また、トランザクションの復号化に使用できる復号鍵が事前に保存されている。復号鍵の要求が受信され、ここで、この要求はトランザクション識別子と対象者認証アサーションを含んでいる。次に、対象者認証アサーションが検証される。対象者認証アサーションからの情報を、トランザクション識別子と共にデータベースに保存される。この要求に応答して復号鍵が提供され、これにより、トランザクション対象者が、トランザクションの受信をもっともらしく否認できないようにする情報が確立される。

【００３２】

簡潔に言えば、本発明の別の好ましい実施形態は、トランザクション送信元とトランザクション対象者が、否認不能なトランザクションを交換するためのシステムである。このシステムは、コンピュータ化されたキーサーバを設けている。キーサーバは、トランザクション識別子にトランザクションを識別させる第１の要求をネットワーク経由で受信するのに適しており、ここで、この第１の要求は送信元認証アサーション含んでいる。さらにキーサーバは、トランザクションの復号化に使用できる復号鍵の第２の要求をネットワーク経由で受信するのに適しており、ここで、この第２の要求は、トランザクション識別子と対象者認証アサーションを含んでいる。さらにキーサーバは、送信元認証アサーション

と対象者認証アサーションを検証するのに適している。さらに、関連するトランザクション識別子、送信元認証アサーションからの情報、対象者認証アサーションからの情報をデータベースに保存するのに適している。キーサーバはさらに、トランザクション識別子を含んだ第１の返答を、第１の要求に対してネットワーク経由で提供するのに適している。さらにキーサーバは、復号鍵を含んだ第２の返答を、第２の要求に応答してネットワーク経由で提供し、これにより、トランザクション送信元が、トランザクションを暗号化および送信した後にもっともらしく否認できないようにする情報を確立し、さらに、トランザクション対象者が、復号鍵を受信した後にもっともらしく否認できないようにするのにも適している。

【００３３】

簡潔に言えば、本発明の別の好ましい実施形態は、トランザクションを、トランザクションの発信者であるトランザクション送信元による否認防止が可能なものとして確立するシステムである。このシステムは、コンピュータ化されたキーサーバを備えている。キーサーバは、トランザクション識別子にトランザクションを識別させる要求をネットワーク経由で受信するのに適しており、ここで、この要求はソース認証アサーションを含む。さらにキーサーバは、送信元認証アサーションを検証するのにも適している。さらに、トランザクション識別子と、送信元認証アサーションからの情報をデータベースに保存するのにも適している。キーサーバはさらに、トランザクション識別子を含んだ返答をネットワーク経由で提供し、これにより、トランザクション送信元が、トランザクションを暗号化および送信した後にもっともらしく否認できないようにする情報を確立するのに適している。

【００３４】

簡潔に言えば、本発明の別の好ましい実施形態は、トランザクションを、トランザクションの受信者であるトランザクション対象者による否認防止が可能なものとして確立するシステムであって、ここで、トランザクション識別子は、トランザクションを証明し、トランザクションの復号に使用できる復号鍵がデータベース内に事前に保存されている。このシステムは、コンピュータ化したキーサーバを設けている。キーサーバは、復号鍵の要求をネットワーク経由で受信するのに適しており、ここで、この要求は識別子と対象者認証アサーションを含んでいる。さらにキーサーバは、対象者認証アサーションを検証するのにも適している。また、対象者認証アサーションからの情報を、トランザクション識別子と共にデータベースに保存するのにも適している。キーサーバはさらに、復号鍵を含んだ返答をネットワーク経由で提供し、これにより、トランザクション対象者がもっともらしく否認できないようにする情報を確立するのにも適している。

【００３５】

本発明の利点は、安全性の高いメッセージ通信を提供することである。本発明は、強力な鍵管理技術を使って、送信者と受信者、またはコラボレーション参加者の間でメッセージを保護する。これにより、高度のメッセージ改ざん検出と送信者による否認防止が得られる。しかし、本発明は、実際に安全化されたメッセージのコンテンツを検査することを全く必要とせずに、そのすべての機能を提供するものである。

【００３６】

本発明の別の利点は、使用者の負担を最小にすることである。このためにユーザが複雑なインストールや構成を行う必要はなく、プレインストールされているか、あるいはユーザによる高速インストールが可能になっており、すべての構成オプションにデフォルトが設けられている。特に、本発明は、企業やその他の組織が、メンバーのメッセージを保護し、共同作業を促進するために、容易に実現できるようになっている。

【００３７】

本発明の別の利点は、単純な登録スキームを採用しており、登録やインストールの完了後すぐに使用することができる。これらの、およびその他の特徴のために、本発明を使って作成したセキュアメッセージの対象受信者は、事前に登録されている必要がない。送信者がセキュアメッセージを作成および送信すると、本発明は、目的受信者が登録されてい

ない旨を検出して、登録の催促を行う。

【００３８】

本発明の別の利点は、特に、安全なコラボレーション通信を容易化することである。送信者と受信者、またはコラボレーション参加者で構成された大きなグループの会話を安全化でき、さらに、新規ユーザが会話に参加する、または既存のユーザが会話から退出する度に、容易にその安全性を変更することができるため、会話の過去的および将来的な秘密性（バックおよびフォワードシークレシー）を実現できる。

【００３９】

本発明の別の利点は、これがイベントに基づくものであり、アクションイベントと非アクションイベント（すなわち正のイベントと負のイベント）の両方をサポートすることである。既に一般に使用されている方法で通信文を開封および表示する場合以外に、受信者による自発的な動作は必要ない。

【００４０】

本発明の別の利点は、制御を強化できることであり、この制御は発信者側に基づくものであり、通信文の実際の発信者または発信者を越えるオーソリティによって設定される。特に、この制御は、初回表示時、最終表示時、さらに、再び通信文を表示できる回数を設定できる。

【００４１】

本発明の別の利点は、分断された通信が可能になることである。本発明が使用する技術では、通信文の発信者が受信者と直接接続する必要がない。上述したように、発信者は、受信者がまだ見ることが許可されない通信文を送信できる。受信者が（通信文の表示により、または通信文の表示に何らかの形で失敗することにより）表示関連のイベントをトリガすると、これが記録されるか、または発信者または別の適切な参加者に肯定的に報告されるため、これらの人物がこれを適切に対処できる。

【００４２】

本発明の別の利点は、ユーザにとってその大部分が透明性であることである。本発明の中心的機能は公開/秘密鍵暗号化スキームに依存しないが、しかし、本発明をある補助的な関連において便利にするため、また、より安全にするために、そのいくつかの要素にこのスキームを採用することは可能である。本発明によって使用される技術では、ユーザが、例えば公開鍵インフラストラクチャ（ＰＫＩ）を設定および採用して、これに付随する負担を負う必要がなく（しかし、所望であればＰＫＩを使用することもできる）、そしてユーザが通信文受信の通知を行う必要もない。

【００４３】

本発明の別の利点は、公開/秘密鍵システムと違い、メッセージへの鍵を、受信の度にいったん暗号化する必要がないことである。同様に、安全化したメッセージのコンテンツも、メッセージがルータおよびハブを通過する際、受信の度にいったん復号化する必要がない。そのため、実行される暗号化および復号化の回数は、受信者の数、および通信に使用されるリソースの数とは無関係である。

【００４４】

本発明の別の利点は、公開/秘密鍵システムと異なり、秘密鍵を常駐させる場所に依存しないことである。ユーザは、他の参加者との安全なコラボレーションにどこからでも参加できる。

【００４５】

本発明の別の利点は、メモリと、基礎となるハードウェアの処理能力に重い負担をかけることなく、大容量データを扱うことを可能にしながら、さらに、従来技術の手法と同等またはこれを超えるセキュリティを提供できることである。

【００４６】

本発明の別の利点は、否認防止および監査の両方にそれぞれ一回サービスを提供することである。

【００４７】

本発明の別の利点は、異なる状況に対応して異なる程度が適切であるとき、否認防止のための複数の強度レベルを使用できることである。

【００４８】

さらに、本発明の別の利点は、ユーザへの負担がなく、また、すべてのトランザクション対象者について、鍵、デジタル証明書、およびこれらのデータを検索するためのディレクトリを事前に取得する必要性に依存しておらず、そのため、すべてのトランザクション実行中の参加者が柔軟性のない一貫したスキームを使用する必要がないことである。

【００４９】

本発明のこれらの目的およびこれ以外の目的は、本明細書中で説明する、また、いくつかの図面で例証しているように、本発明を実施する現在最良の形態の説明と、好ましい実施形態の産業上の利用可能性を考慮することで、当業者にとって明白になるであろう。

【００５０】

本発明の目的および利点は、添付の図面および表と共に、以下に示す詳細な説明から明白になるであろう。

【００５１】

発明を実施するための最良の形態

本発明の好ましい実施形態は、鍵交換、およびこれに基づく安全な提携通信を実現するシステム、キーサーバイベントを使用してビジネス処理を実現するシステム、認証アサーションとキーサーバを使用して否認防止および監査を実現するシステムである。本明細書中の多数の図面、特に図９、図１１、図１５に示すように、本発明の実施形態を参照符号２１０、３１０、４１０で表している。本発明について説明を開始する前に、まず、安全なメッセージ通信を実現するためのキーサーバの背景について説明する。

【００５２】

図１は、セキュア電子メールシステム１０における情報の流れを示す概略外観図である。送信者１２が、セキュア電子メールシステム１０を使用して、一人またはそれ以上の受信者１６に対してセキュア電子メール１４を送信する。この送信を完遂するには、送信者１２は、セキュア電子メール１４の作成および送信に適した送信ユニット１８を使用し、受信者１６は、このセキュア電子メール１４の受信および表示に適した受信ユニット２０を使用する。さらに、セキュア電子メールシステム１０は、本質的に従来型の電子メールサーバ２２、送信ユニット１８および受信ユニット２０内のソフトウェアモジュール２６（図３）と共にセキュア電子メールシステム１０の一次の新規エレメントを構成するセキュリティサーバ２４（先述したようにキーサーバ形式のもの）を実装している。

【００５３】

送信ユニット１８と受信ユニット２０は、ハードウェアとソフトウェアの適切な組み合わせである。これは、同種または異種のハードウェアであってよく、図１では、送信ユニット１８と第１受信ユニット２０ａをパーソナルコンピュータ（ＰＣ）として示し、第２受信ユニット２０ｂをインターネット機器として示すことで、これを強調している。

【００５４】

送信ユニット１８は送信機能の装備が必須であり、また、多くの場合、セキュア電子メール１４の構成にも使用される。しかし、構成機能は必ずしも必須の機能ではなく、例えば、標準メッセージが事前に保存されている携帯電話のようなインターネット機器を使用することも可能である。受信ユニット２０は、セキュア電子メール１４を受信できることが必須であり、また、場合によりメッセージ構成およびその他の機能を搭載できる。

【００５５】

必要なソフトウェアに関しては、送信ユニット１８と受信ユニット２０の各々に、適切な電子メールタイプのアプリケーションと、適例のソフトウェアモジュール２６を実装することが必要である。この電子メールタイプのアプリケーションは、従来型の電子メール・アプリケーションであってよく、あるいは、電子メール機能を統合したブラウザ、または、従来のブラウザで動作する電子メール・アプレットであってもよい。次に、ソフトウェアモジュール２６についてより詳細に説明するが、複数のソフトウェアモジュール２６

を、送信ユニット１８または受信ユニット２０で最初に使用する際にほぼ同時にインストールできる点を述べておく。

【００５６】

図１では、複数の受信者１６への送信にセキュア電子メールシステム１０を使用できることを強調するために、第１受信機１６ａと第２受信機１６ｂの両方を図示している。そのため、共通の電子メール宛先指定規定、例えば「Ｔｏ：宛先」、「Ｃｃ：（コピー）」、「Ｂｃｃ：（ブラインドコピー）」など、さらに、セキュア電子メールシステム１０を使用して、複数の受信者１６のリストに同時に送信を行うことができる。

【００５７】

次に述べる総体的な説明に備え、送信者１２と第１受信者１６Ａがセキュア電子メールシステム１０に登録されており、送信ユニット１８と第１受信ユニット２０ａには、適例のソフトウェアモジュール２６が実装され、セキュア電子メールシステム１０にてそれぞれの機能で動作すると仮定する。さらに、第２受信者１６ｂは、セキュア電子メールシステム１０に未登録であり、また、第２受信ユニット２０ｂにはセキュア電子メールシステムがまだ実装されていないと仮定する。

【００５８】

さらに図１の概観は、一般的なインターネットのようなネットワーク環境３０で、セキュア電子メール１４を送信するための主要な段階を示す。段階３２では、送信者１２がセキュア電子メール１４を送信しようと決める。そのため、従来またはその他の方法といった何らかの方法で電子メールメッセージを構成する。

【００５９】

段階３４では、送信者１２は、「送信」命令の代わりに「安全な送信」命令を使用して、セキュア電子メール１４の送信を要求する。しかし、安全でない電子メールメッセージを電子メールサーバ２２へ直接送信するのではなく、まず送信ユニット１８がセキュリティサーバ２４に接触して、様々なデータアイテムを提供する（この段階および他の段階で使用されるデータアイテムについては先述のとおりである）。次に、セキュリティサーバ２４が送信者１２を認証し、このセキュア電子メール１４用の一意のメッセージ鍵とＩＤを送信ユニット１８に返送する。また、セキュリティサーバ２４は、このトランザクションのための様々なデータアイテムを、後の使用のために記録する。送信ユニット１８は、メッセージ鍵を使用して、セキュア電子メール１４を暗号化する。暗号化された、または暗号化されていないメッセージ本体がセキュリティサーバ２４に送信されることは絶対にない。

【００６０】

段階３６において、セキュリティサーバ２４は、受信者１６が登録済みであるか否かを判断する。既に登録されている場合には、ここで第１受信者１６ａのみについてそうであるように、受信者１６についてこの段階が終了する。しかし、受信者１６が未登録の場合には、ここで第２受信者１６ｂについてそうであるように、登録が試みられる。登録を試みるために、セキュリティサーバ２４は電子メールメッセージを第２受信者１６ｂに送信して、まもなく暗号化されたメッセージが届き、このメッセージを読むためには登録が必要である旨を知らせる。次に、第２受信者１６ｂは、セキュリティサーバ２４から送信されたこの電子メールに含まれているユニバーサル・リソース・ロケータ（ＵＲＬ）を入力して、セキュリティサーバ２４で登録のためのルーチンを追従することができる。第２受信ユニット２０ｂには、セキュア電子メール１４を受信または復号するのに必要なソフトウェアモジュール２６が既に実装されているか、または登録プロセスの一部としてこのようなソフトウェアが提供される。第２受信者１６ｂが登録を済ませ、第２受信ユニット２０ｂが必要なソフトウェアモジュール２６のインストールを完了すると、この段階は終了する。

【００６１】

あるいは、セキュア電子メール１４内で段階３６を飛ばして次に進むこともできる。セキュア電子メール１４自体に、受信者１６が追従できる単純な形式のユニバーサル・リソ

ース・ロケータ（ＵＲＬ）を含めることが可能である。そのため、セキュリティサーバ２４は受信者１６が登録済みであるか否かを考慮する必要がない。送信者１２は、既に説明したように、セキュア電子メール１４を作成および送信することができ、受信者１６は、自分が登録済みであるか否かに対処し、このセキュア電子メール１４が到着したらこれを読むことができる。

【００６２】

段階３８において、送信ユニット１８は、暗号化されたセキュア電子メール１４を送信する。これは、送信者にとって本質的に透過的またはシームレスであってよく、また、暗号化されたセキュア電子メール１４を従来の電子メールタイプのアプリケーションに送信し、自動的に適切な「送信」命令を出すことで、送信ユニット１８のソフトウェアモジュール２６内でこれを取り扱うことができる。次に、セキュア電子メール１４は、従来の方法で電子メールサーバ２２へ進み、各宛先受信者１６のインボックスに到着する。注目すべき点は、セキュア電子メール１４の本体が、送信ユニット１８と受信ユニット２０の間で通信が行われている間の全般にわたって暗号化された状態にあることである。場合により、この最中に件名を暗号化してもよい。

【００６３】

段階４０において、セキュア電子メール１４が、各受信者１６のインボックスに到着する。受信者１６が自分の受信ユニット２０を使用してセキュア電子メール１４を開封すると、受信ユニット２０用のソフトウェアモジュール２６が、このセキュア電子メール１４が暗号化されていることを検出する。ソフトウェアモジュール２６は、その構成により、受信者１６にパスワードを催促するか、または既に知っているパスワードを使用することができる。

【００６４】

最後に、段階４２で、受信ユニット２０がセキュリティサーバ２４に接触し、受信者１６用のメッセージＩＤとデータ（パスワードを含む）を提供する。セキュリティサーバ２４は、受信者１６が（オリジナルメッセージ内の受信者のリストにより決定されているとおりに）認証された受信者であると仮定し、メッセージ鍵を受信ユニット２０に提供する。場合により、セキュリティサーバ２４は、セキュリティ電子メール１４が何らかの形式に変更された旨の表示を提供することもできる。受信ユニット２０が、このメッセージ鍵を用いてセキュア電子メール１４を復号化すると、受信者１６がこれを読めるようになる。

【００６５】

図２ａ～図２ｃは、セキュア電子メールシステム１０が使用できる電子メールフォーム５０を示す。図２ａは、従来の送信フォーム５２ａである。図２ｂは、送信フォーム５２ａと本質的に同一であるが、セキュア電子メールシステム１０で扱えるように変更された送信フォーム５２ｂである。図２ｃは、セキュア電子メールシステム１０で使用できる従来の受信フォーム５４である。

【００６６】

送信フォーム５２ａ～５２ｂの両方は、受信者ＩＤフィールド５６、件名フィールド５８、本体フィールド６０を含んでいる。さらに、これらの両方のフォームは従来型の送信ボタン６２を含んでいる。図２ａの送信フォーム５２ａ（従来型）と図２ｂの送信フォーム５２ｂ（変更型）の唯一の違いは、後者が送信セキュリティボタン６４を含んでいる点である。いくつかの実施形態では、送信ボタン６２を安全送信ボタン６４に変更することが望ましいかもしれないが、これが一般的になる見込みはない。図２ｃの受信フォーム５４は、受信ＩＤフィールド５６（宛先：とＣｃ：）、件名フィールド５８、本体フィールド６０、そして送信者ＩＤフィールド６６も含んでいる。これらのフォーム内に含まれた多様なフィールドを理解することは、後続の説明を理解するために役立つ。

【００６７】

図３は、送信ユニット１８と受信ユニット２０で使用されるソフトウェアモジュール２６を示すブロック図である。セキュア電子メールシステム１０の多くの実施形態において

、ソフトウェアモジュール２６は、送信ユニット１８と受信ユニット２０の両方に実装されているものと同一であってよいが、これは必須ではなく、これ以外のモジュールを使用することが可能である。ソフトウェアモジュール２６は、セキュア電子メールシステム１０の「クライアント」側のコンポーネントとして見ることができる。

【００６８】

この図は、また、ソフトウェアモジュール２６を送信ユニット１８および受信ユニット２０にインストールする様々な使用可能な方法を示している。プレインストールされているオプション４４を使用することで、送信ユニット１８または受信ユニット２０にロードされている内在の電子メールタイプ・アプリケーションを、すでに搭載されているソフトウェアモジュール２６に付随させることが可能である。従来の電子メール専用アプリケーションまたはウェブに基づく電子メール・アプリケーションは、このプレインストール済みのオプション４４を有利に使用することができる。

【００６９】

セキュア電子メールシステム１０の主要な目的は、その使用の容易化であり、セキュア電子メールシステム１０をウェブに基づく電子メール・アプリケーションと共に使用することで、新規ユーザにとっては操作が特に容易になり、既存の上達したインターネットユーザにとってはその操作が単純化される。現在、多くのインターネット・サービス・プロバイダ（ＩＳＰ）がブラウザ・アプリケーション・ソフトウェアをユーザに提供している。その一例はアメリカオンライン（ＡＯＬ（登録商標））であり、ＡＯＬでは、あらかじめ構成された「プライベートラベル」ブラウザ・アプリケーションをユーザに提供している。プレインストールされているオプション４４によって、セキュア電子メールシステム１０をプライベート・ラベル・ブラウザに含め、設定に伴うあらゆる負担を最小化することが可能になる。あらゆる構成オプションにデフォルト設定を設定することができ、これにより送信者１２と受信者１６は、場合によりソフトウェアモジュール２６を望みどおりに適合させることができるようになる。

【００７０】

あるいは、ユーザがインストールしたオプション４６を使用してもよく、この場合、ソフトウェアモジュール２６が送信者１２と受信者１６、すなわちエンドユーザによって、送信ユニット１８、受信ユニット２０の各々にインストールされる。このユーザがインストールしたオプション４６により、プライベート・ラベル・アプリケーションを使用していない多数のインターネットユーザがセキュア電子メールシステム１０を使用することが可能になる。

【００７１】

ユーザがインストールしたオプション４６は、多くの応用形にて実現することができる。ある応用形４６ａは、ソフトウェアモジュール２６をプラグインとして永久インストールするというものである。別の応用形４６ｂは、例えばＹａｈｏｏ！（商標）のような特定のウェブポータルを使用して入手したＪａｖａアプレットのようなセキュア電子メールシステム１０を使用する度に、ソフトウェアモジュール２６をアプレットとして一時的に「インストール」するものである。さらに別の応用形４６ｃは、スクリプト・ドリブン・インストール、すなわち、区画化されたプラグイン・タイプのインストールではなく、本質的に従来型のフルブローン・ソフトウェア・アプリケーション・インストールである。さらに別の応用形４６ｄは、上述したインストール、または全く新規のインストール手法の組み合わせであってよい。

【００７２】

これらの応用形４６ａ～４６ｄは、セキュリティサーバ２４（図１）のような、密接に制御されたサーバからダウンロードを実施することができる。あるいは、これらの内のいくつかは、他の手段による配布、例えばコンパクトディスク（ＣＤ）からのソフトウェアモジュールのローディングを含んでよい。ＣＤは、プライベート・ラベル・アプリケーション、特にプライベート・ラベル・ブラウザを配布する一般的な方法である。プレインストールされたオプション４４に従って既にインストールしたソフトウェアモジュール２６

でアプリケーションを配布するのではなく、単純に、ユーザが自分でインストールしたオプション４６を介してインストールするか否かを決定できるオプションとして、ソフトウェアモジュール２６をアプリケーション配布ＣＤに含めることができる。

【００７３】

しかし、ソフトウェアモジュール２６をオンライン上で入手することにより、周縁的な利点が得られる。送信者１２と受信者１６は、同時にセキュア電子メールシステム１０に正式登録され、他の正規手続き、例えば暗号化技術の受諾および使用が可能になる認証を遵守できる。

【００７４】

応用形４６ａ～４６ｄは、各々異なる度合いで、アップグレードオプションを容易化することもできる。例えば、ソフトウェアモジュール２６は、セキュリティサーバ２４と接触する度に、バージョン情報をその通信の一部分として含めることができる。複雑な実施形態では、ソフトウェアモジュール２６は、アップグレードが利用可能になると、セキュリティサーバ２４またはその他の場所から自己アップグレードを実行する自己アップグレード型であってよい。複雑性の低い実施形態、または再認証が必要な場合には、アップグレードを実施する方法に関する情報を送信することができる。例えば、アップグレードサイトＵＲＬを含んだ電子メールメッセージを、送信者１２または受信者１６に対して送信できる。

【００７５】

図３も、送信者１２と受信者１６が、ソフトウェアモジュール２６内で変更できるいくつかの構成オプション４８を示す。すべてでなければほとんどの状況において、適切なデフォルトの提供が可能であるが、しかし、上達したユーザは、または特定の状況においては、これらの設定を変更することが有利な場合もある。該してこのような構成オプション４８は、セッションの種類に無関係に一貫していなければならない一方で、優れたセキュリティの実施を一貫すれば、構成オプション４８は単にマシンと関連するのではなく、ユーザと関連するはずである。そのため、複数の送信者１２または受信者１６が同一の送信ユニット１８または受信ユニット２０を使用できる場合、ユーザは、独立した個人的な構成を設定することができるようになる。

【００７６】

構成オプション４８の特定の設定例は、件名暗号化設定４８ａ、キャッシュパスワード設定４８ｂ、キャッシュ時間設定４８ｃ、有効期限設定４８ｄ、最大読み出し設定４８ｅ、その他４８ｆを含んでよい。

【００７７】

件名暗号化設定４８ａは、ソフトウェアモジュール２６がセキュア電子メール１４の件名フィールド５８（図２ａ～図２ｃ）、本体フィールド６０を暗号化するか否かの制御を行う。デフォルトでは通常、件名を暗号化しないようになっている。

【００７８】

キャッシュパスワード設定４８ｂによって、アプリケーション・セッションの度（例えばブラウザセッションの度）にパスワードが一回要求されるか、あるいは、プロンプトが必要に応じて毎回パスワードを要求するかのいずれかを指定することが可能になる。一般に、デフォルトでは、パスワードをキャッシュするようになっているが、次に記述するように、これは、キャッシュ時間設定４８ｃと組み合わせ、より安全な方法で実施することで機能する。安全性をさらに高めるために、パスワードをメモリ内でのみキャッシュし、ディスクに対しては絶対にキャッシュを行わないようにすることもできる。

【００７９】

キャッシュ時間設定４８ｃはキャッシュパスワード設定４８ｂと協働して、パスワードをキャッシュできる最大時間を制御する。これについてのデフォルト値および許可される最大値は８時間であってよい。その後、送信者１２がキャッシュ時間設定４８ｃを短縮することができるが、セキュリティ性を劣化させてしまう程にこの時間を長く設定することは許されない。

【００８０】
有効期限設定４８ｄによって、送信者１２は、いつセキュリティサーバ２４（図１）がメッセージ鍵を破棄して、セキュア電子メール１４を読み出し不能にするべきかを特定することが可能になる。セキュア電子メールシステムの多くの実施形態では、有効期限を明確に強制実施するのではなく、ある十分長い期間（恐らくは数年間）の後に、恐らくセキュリティサーバ２４が有効期限の強制実施を行う必要がある状態にデフォルト設定されている。
【００８１】
最大読み出し設定４８ｅは、各受信者１６が１通のセキュア電子メール１４を開封し、読む回数、すなわち、一人の受信者１６に対してメッセージ鍵が送付される回数を特定指定する。ゼロ、つまり無制限にデフォルト設定することができる。
【００８２】
もちろん、さらに別の構成オプション４８を設けることができ、図３に、これを強調するためにその他４８ｆの要素を示す。
【００８３】
ソフトウェアモジュール２６を送信ユニット１８にインストールすると、メッセージ構成シナリオとメッセージ送信シナリオに使用することが可能となる。後述の説明では、ソフトウェアモジュール２６がプラグイン・タイプの応用形４６ａである場合のプライベート・ラベル・ブラウザを使用するが、当業者は、基本となる原理が、セキュア電子メールシステム１０を使用できる他のシステムへの拡大が可能であることを理解するだろう。
【００８４】
図４はセキュア電子メール１４が送信（または受信）されているか否かを判断するための、ソフトウェアモジュール２６の好ましい手法を示すブロック図である。送信ユニット１８内のソフトウェアモジュール２６は、ページ７２のストリーム７０を検査し、送信者１２が作成したセキュア電子メール１４を構成しているものを探す。ストリーム７０を検査するある方法では、ソフトウェアモジュール２６が、ページ７２のＵＲＬがある一定の構造、例えば“*mail.privatelabel.com*/Compose*”（ここで、*はあらゆるパターンに適合できる）を含んでいるかどうかを調べる。ソフトウェアモジュール２６による別の検査方法は、ページ７２のＨＴＭＬコンテンツがある一定の認識可能な（静的）パターン、例えば、「構成」という名称のフォームタグを含んでいるか否かを判断するものである。ソフトウェアモジュール２６はまた、ＭＩＭＥタイプを使用して、代行受信できるページ７２を識別することも可能である。実際に候補のページ７２ａが見つかると、これがストリーム７０から除去され、説明したとおりに処理されて、処理済みのページ７２ｂとしてストリーム７０内の元の場所に配置される。
【００８５】
ソフトウェアモジュール２６が、元の場所に戻されるページ７２が構成タイプ候補ページ７２ａであると判断すると、この候補ページ７２ａを、少なくとも１つの新規制御である安全送信ボタン６４（図２ｂ）を含むよう変更する必要がある。所望であれば、この１つのボタンに加えて他の制御を追加することもできるが、あくまでも任意である。
【００８６】
セキュア電子メール１４を送信することが望ましい時に、送信者１２は、従来の送信ボタン６２を操作するのではなく、安全送信ボタン６４を「押す」（要するに、マウスクリックで操作する）。安全送信ボタン６４を操作すると、ソフトウェアモジュール２６が、電子メールサーバ２２に投函できる状態の、電子メールの様々なフィールドを含むページ７２（またはフォーム）を代行受信し、これらフィールドのいくつかを変更する。この変更が完了すると、ソフトウェアモジュール２６が、送信者１２が送信ボタン６２を押した場合に第１に起こったであろう状態と全く同一の望ましい動作（投函または送信）を実行する。この場合の唯一の違いは、セキュア電子メール１４内のいくつかのフィールドに含まれる値が異なる、つまり暗号化されている点である。
【００８７】

発明者の現時点で好ましい実施形態では、２つのフィールドのみが典型的に変更されている。本体フィールド６０は、常に暗号化によって変更される。そして、構成設定、特に上述の件名暗号化設定４８ａに従い、件名フィールド５８を変更することもできる。

【００８８】

暗号化処理および復号処理の考察を行う前に、セキュア電子システム１０によって使用される様々なデータアイテムについて説明することが適切である。図５は、セキュア電子メールシステム１０によって使用されるテーブルを含むデータベース１００の図である。セキュリティサーバ２４（図１）の主要な構成要素は、このデータベース１００である。登録された送信者１２と受信者１６は、このデータベース１００内でユーザとしてまとめて処理され、送信者１２と受信者１６のためのデータがユーザテーブル１０２に保存される。

【００８９】

ユーザテーブル１０２は、userId１０２ａ、password１０２ｂ（実際には、先述した好ましい実施形態における実パスワードのハッシュバージョン）、salt１０２ｃ、status１０２ｄのためのフィールドを各々有する記録を含んでいる。

【００９０】

ユーザエイリアステーブル１０３は、ユーザテーブル１０２に密接に関連し、emailAddress１０３a、userId１０３ｂ（ユーザテーブル１０２内のユーザＩＤ　１０２ａと関連的にリンクしている）のためのフィールドを各々有する記録を含んでいる。

【００９１】

データベース１００は送信済みメールテーブル１０４も含んでいる。このテーブルには、messageId１０４ａ、senderId１０４ｂ、dateSent１０４ｃ、numRecipients１０４ｄ、messageKey１０４ｅ、maxDeliveries１０４ｆ、expiration１０４ｇ、sealSalt１０４ｈ、subject１０４ｉ、lastRead１０４ｊ、およびdeliverAfter１０４ｋのフィールドを各々有する記録を含んでいる。

【００９２】

受信者テーブル１０６も提供される。図５に見られるように、送信済みメールテーブル１０４内のメッセージＩＤ１０４ａは、受信者テーブル１０６内のメッセージＩＤ１０６ａと関連的にリンクしている。したがって、この受信者テーブル１０６は、各々のセキュア電子メール１４に特定されている受信者１６のためのデータを含んでいる。さらに受信者テーブル１０６は、receiverAddr１０６ｂ、firstRequest１０６ｃ、およびnumRequests１０６ｄのためのフィールドを有する記録を含む。

【００９３】

図６ａ～図６ｆは、好ましい実施形態で使用されるデータフィールドのテーブルである。図６ａ～図６ｄ中のテーブルは、セキュア電子メールシステム１０のコア動作にとって重要であるのに対し、図６ｅ～図６ｆは、セキュア電子メール１０の任意の特徴に関連している。

【００９４】

図６ａ～図６ｄのテーブル内のテキストは、ここでさらに詳細に説明する１次フィールドと共に、いくつかの特定のフィールドを記述している。図６ａは、図５のユーザテーブル１０２である。これには、セキュア電子メールシステム１０に登録されている各ユーザ、つまり送信者１２または受信者１６のためのデータ記録が含まれている。各ユーザは、登録時にUserId（userId１０２ａ）を割り当てられ、Password（password１０２ｂ）を選択し、このパスワードがここに保存される。好ましいPassword（password１０２ｂ）の値はＨ（ｐ＋ｓ）であり、ここでｐはクリアテキストパスワードであり、ｓは、クリアテキストパスワードと連結したsalt（salt102c）である。図６ｂは、図５のsentMailテーブル１０４である。このテーブルには、セキュア電子メールシステム１０内の各セキュア電子メール１４のためのデータ記録が含まれている。図６ｃは、図５の受信者テーブル１０６である。このテーブルには、セキュア電子メールシステム１０が配送できる各セキュア電子メール１４のための宛先データが含まれている。送信された各セキュア電子メール１４

の各々の受信者１６（個人またはリストグループ）に関する記録がこのテーブル内で生成されるため、セキュア電子メールシステム１０内でこのテーブルが最も大きくなることが予想される。FirstRequest（firstRequest１０６ｃ）内のフィールドヌル値は、受信者１６がセキュア電子メール１４の読み出しをまだ要求していないことを意味する。図６ｄは、図５のユーザエイリアステーブル１０３である。このテーブルには、各々の所与のユーザ（ユーザテーブル１０２中でuseId１０２ａと関連的にリンクしているuserId１０３ｂ）に関してわかっているすべての電子メールアドレス（emailAddress１０３ａ）のデータが含まれている。そのため、複数の電子メールアドレスまたはエイリアスから、シングルユーザが判明することがある。

【００９５】

図６ｅ～図６ｆのフィールドに関しては、以下の説明以上に詳細な説明を省く。これらのテーブルはオプション特徴によって使用されるものであり、また、テーブル中に十分詳細な記述があるため、当業者はこれらフィールドの使用を理解できる。図６ｅは、電子メール配布リストの使用を可能にするデータのテーブルである。このテーブルにより、ユーザは配布リストを作成できる。所有者はこのリストを常に更新できるが、所有者が実際にこのリストのメンバーである必要はない。この後者の特徴は、リスト管理者にとって特に便利である。そして、図６ｆは、配布リストの使用を許可するために使用されるデータのテーブルである。このテーブルには、各配布リストのメンバーに関するデータが含まれる。

【００９６】

図５、図６ａ～図６ｆに示したデータ以外のための、他のテーブルおよびフィールドの使用ももちろん可能であり、また、いくつかのセキュア電子メールシステム１０の実施形態では、上述したフィールドのいくつかをオプションにしたり、省略してもよい。

【００９７】

メッセージを暗号化する前に、ソフトウェアモジュール２６は送信者１２のパスワードを取得する必要がある。このパスワードがキャッシュされ、キャッシュ時間設定４８ｃを超えない場合にはこのステップが完了する。それ以外の場合には、ソフトウェアモジュール２６が、送信者１２にパスワードの入力を催促するダイアログボックスを表示する。例えば、パスワードのみをアスタリスクで表示したり、送信者に送信を中止するべくキャンセルを許可する従来のパスワード取り扱い機能が提供される。

【００９８】

好ましい実施形態では、送信者１２と受信者１６のパスワードは、ユーザテーブル１０２に保存されているパスワード１０２ｂと違うものである。代わりに、強化されたセキュリティオプションとしてユーザがパスワードを選択し、このパスワードとソルト１０２ｃがセキュリティサーバ２４によってハッシュされ、パスワード１０２ｂが取得できる。ユーザが選択したパスワードがセキュリティサーバ２４へ送られ、そこでパスワードとソルト１０２ｃをハッシュし、パスワード１０２ｂがデータベース１００に保存される。ユーザのパスワードのクリアテキストは、セキュリティサーバ２４に保存されず、オリジナルパスワードなしでの計算が不可能な、計算されたハッシュだけが保存される。

【００９９】

このようにして、セキュリティサーバ２４に実際のユーザパスワードが知られることは決してないし、知り得る方法もない。次に、このオプションについてさらに詳細に説明する。

【０１００】

パスワード１０２ｂを取得すると、ソフトウェアモジュール２６は暗号化と実際の送信を実施できるようになる。ソフトウェアモジュール２６は、送信者１２を認証し、セキュア電子メール１４の暗号化に使用するmessageKey１０４ｅを送り戻すよう求める要求を、セキュアソケットレイヤ（ＳＳＬ）プロトコルを介してセキュリティサーバ２４に送信する。次に、ソフトウェアモジュール２６がこのメッセージの本体フィールド６０（および場合により、件名フィールド５８）を暗号化し、この結果が別個に符号化されて、セキュ

ア電子メール１４が作成される。

【０１０１】

セキュアソケットレイヤ（ＳＳＬ）の使用については上述した。本発明のセキュア電子メールシステム１０の目的は、その使用の容易性であるため、発明者によるこの好ましい実施形態はＳＳＬを採用している。これは、現在の産業界で安全と考慮され、一般的なブラウザに広く利用されているが、今日の平均的なインターネットユーザはそうとは知らずにこれを使用している。しかし、ＳＳＬの使用は必須ではないことが理解されるべきである。代わりに、これ以外のセキュリティプロトコルを使用してもよい。

【０１０２】

次の表記は、下記の説明において使用されているものである。

K_m ＝ 電子メールに関連したワンタイムの一意キー；

P_s ＝ 送信者のパスワード；

P_r ＝ 受信者のパスワード；

$\{p\}_k$ ＝ キーｋで暗号化したｐ；

$\{p\}_{ssl}$ ＝ ＳＳＬセッションキーで暗号化したｐ；

$H_{(p)}$ ＝ ｐの一方向ハッシュ。

【０１０３】

図７は、現在好ましい暗号化のプロセス１２０を示すフローチャートである。送信者１２がセキュア電子メール１４を送信する準備ができた時点で、本体フィールド６０内に平文が入力されたＨＴＭＬ送信フォーム５２ｂ（図２ｂ）が表示されている。ここで、送信者１２はセキュリティサーバ２４に登録済みであり、この送信者のブラウザには適切なソフトウェアモジュール２６がインストールされていると仮定する。また、送信者１２は、ブラウザのみを使用してセキュア電信メール１４を送信するものと仮定する。セキュリティの性質は、使用する実際のメールクライアントに関係なく同一でなければならず、そして、これを用いることで以下の説明を単純化することができる。

【０１０４】

先述したように、送信者１２は、セキュア電子メールの投函準備ができると、送信フォーム５２ｂ上の安全送信ボタン６４を選択する。これがステップ１２２、つまり暗号化プロセス１２０の開始を構成する。

【０１０５】

ステップ１２４では、送信ユニット１８内で、以下の情報をソフトウェアモジュール２６へ送信するスクリプトが実行される。

送信者１２の電子メールアドレス（emailAdress103a）；

宛先；フィールド、ＣＣ；フィールド、ＢＣＣ；フィールドのコンテンツ（receiver Addr106bの例）；

件名フィールド５８のコンテンツ；そして

本体フィールド６０のコンテンツ。

【０１０６】

ステップ１２６では、ソフトウェアモジュール２６が送信者１２のパスワードをまだ知らない場合に、送信者１２のパスワードを催促する。送信の度にパスワードを入力するかどうかは、これが場合によっては非常に面倒な作業であるため、セキュリティポリシーの選択の問題となる。送信者１２がブラウザセッションを開いた状態で維持した場合、ソフトウェアモジュール２６内でユーザのパスワード、さらにパスワード１０２ｂをキャッシュすることで危険を招く可能性がある。このポリシーによって、多くの場合、送信者１２はこのオプションの構成方法を選択できるようになるが、その一方で、例えば公共キオスクのような場所で、各セキュア電子メール１４へのパスワードの入力が常に要求されるべき場合もある。

【０１０７】

ステップ１２８では、ソフトウェアモジュール２６がＸＭＬ文書を下記の形式で作成し、これは暗号化されるものである：

```
<?xml version="1.0"encoding="ASCII"/>
<emailPart random="randomNum"length="numChars"
mic="messageIntegrityCode">
<subject>subject</subject>
<body>body</body>
</emailPart>.
```

【０１０８】
この場合、ランダム要素は、クラッキング防止性があり、また、コンテンツ内では同一の電子メールでも、安全化の実行後には違ったものにしてしまうために使用されるランダム数であり；長さ要素が本体フィールド６０中の文字数であり；ｍｉｃ要素は、本体フィールド６０のハッシュを取って作成したメッセージの整合性コードであり；件名要素は件名フィールド５８のコンテンツであり；そして本体要素は本体フィールド６０のコンテンツである。

【０１０９】
ステップ１３０では、ソフトウェアモジュール２６が、セキュリティサーバ２４に対してＳＳＬ　ＨＴＴＰ（ＨＴＴＰＳ）接続を開き、セキュリティサーバに下記の情報を送信する：

送信者１２のemailAddress１０３ａ；
送信者１２のパスワード１０２ｂ；
対象受信者１６のリスト（receiverAddr１０６ｂ、および潜在的なnumRecipients１０４ｄ）；
メッセージの件名フィールド５８（件名１０４ｉ）；
計算されたハッシュのリスト、本体用のもの、Ｈ（ｂ）、そして各付属物のもの　Ｈ（a_1），Ｈ（a_2）．．．Ｈ（a_n）；そして、
有効期限または受信者毎の許容最大送信数といったオプション構成情報。

【０１１０】
ステップ１３２では、セキュリティサーバ２４が、認証サブプロセスの結果に従って前進する。

１）送信者１２のemailAddress１０３ａがわかっていない場合、暗号化プロセス１２０が、知っているemailAddress１０３ａを決定するか、または停止する。emailAddress１０３ａは様々な理由から未知である。ある一般的な例は、送信者１２がセキュリティサーバ２４の新規加入者であるというものである。この場合、送信者１２がその場で登録を行えるようにするための別個のブラウジングウィンドウを開くよう、ソフトウェアモジュール２６が指示を受けることができる。別の理由は、ユーザのエラーのためにemailAddress１０３ａが未知となっているというものである。このようなエラーの単純な原因は、複数のユーザが同じブラウザを共用しているためである。その後、送信者１２は自分の証明を明確にするよう要求できる。

２）送信者１２のパスワード１０２ｂが不正確である場合、ソフトウェアモジュール２６は、パスワード１０２ｂを再び催促するか（恐らくは限られた回数のみ）、送信者１２に送信動作を中止させる（これによって送信者はオリジナルのＨＴＭＬ送信フォーム５２ｂへと戻る）よう指示される。

３）送信者１２がセキュア電子メール１４の送信を許可されていない場合は、暗号化プロセス１２０も停止することができる。これは管理上の理由で実施できる。例えば、送信者１２が料金を未払いである場合や、あるユーザがこの暗号化サービスを使用することを阻止するよう裁判所命令が出ている場合などに実施される。この場合、拒絶の理由をダイアログボックスに入力し、これが承認されると、ユーザがオリジナルのＨＴＭＬ送信フォーム５２ｂへ戻れるようになる（恐らくは、その代わりに送信ボタン６２を使用するため、そして、メッセージを従来の電子メールとして送信するために）。

【０１１１】
あるいは、送信者１２は認証されたと考慮し、現在意図されているセキュア電子メール

１４の送信を許可され、このステップ１３２は首尾よく完了する。

【０１１２】

ステップ１３４では、セキュリティサーバ２４が記録を作成し、sentMailテーブル１０４に保存する。特に、messageId１０４ａ（ｍ）と、messageKey１０４ｅ（k_m）と、送信されているセキュア電子メール１４の各部分について計算されたシール（ｓＬｉｓｔ）とに一意の値が生成される。セキュリティサーバ２４が、sList内のシールをH（H(H(x)+s+t+m+N_m)+N_m）として計算する。要素ｓは、送信者１２のuserId１０２ａ;tは日付および時間（またdateSent104cとしてsentMailテーブル１０４に保存される）；ｍはmessageId１０４ａ；NmはsealSalt１０４ｈ（この特別なセキュア電子メール１４のために生成されたランダム数であるが、messageKey１０４ｅとは別のもの）；Ｈ（ｘ）はハッシュＨ（ｂ）、ソフトウェアモジュール２６から受信したＨ（a1）、Ｈ（a2）... Ｈ（a_n）の組である。sListのコンテンツは再計算可能であるべきなので、これを保存する必要はない。

【０１１３】

ステップ１３６では、セキュリティサーバ２４が送信ユニット１８のソフトウェアモジュール２６に対して、{ｍ，K_m，ｓＬｉｓｔ}$_{SSL}$形式の情報のＳＳＬパケットで応答する。

【０１１４】

ステップ１３８では、ソフトウェアモジュール２６がmessageId１０４ａ（ｍ）、messageKey１０４ｅ（Ｋｍ）を抽出し、ｓＬｉｓｔからシールし、上記のＸＭＬ文書および各添付ファイルをmessageKey１０４ｅで暗号化するべく前進する。次に、ソフトウェアモジュール２６が、送信ユニット１８内のメモリからこの鍵を破棄する。詳細には、ソフトウェアモジュール２６が下記の汎用形式を有するメッセージフォームを作成する：

```
------ BEGIN SECURECORP SECURED EMAIL ------
<securecorp:messagePart id = "m">
<encryptedPart>encrypted body</encryptedPart>
<seal>seal</seal>
</securecorp:messagePart>
------ END SECURECORP SECURED EMAIL ------
```

【０１１５】

セキュア電子メール１４のこの部分に暗号化された本体が含まれている場合には、生ビットストリーム（暗号化後）から符号化されたストリームに変換されるので、暗号化した本体要素は印刷可能な（ASCII）文字の行で構成される。これが添付ファイルである場合には必要ない。

【０１１６】

最後に、ステップ１４０にて、ソフトウェアモジュール２６が、送信者１２が送信フォーム５２ｂ内の送信ボタン６２を押した場合に最初に起こるのと同じ動作を実行する。これにより電子メールサーバ２２に投函を行う（恐らくは、例えばYahoo！（商標）、Hotmail（商標）などの電子メール使用可能なウェブサーバを介して行う）。違いは、投函されているフォームの本体フィールド６０内の値が、上述のとおりに暗号化および符号化された状態にある点である。同様に、あらゆる付属物が上述のとおり暗号化される。従来の電子メールサーバ２２またはウェブサーバの観点からすると、本体が訳のわからない文章の一群でできた通常の電子メールメッセージのように見える。その後、セキュア電子メール１４は、通常のインターネットメールシステム上で伝送され、様々な宛先に到達する。

【０１１７】

上述の説明では添付ファイルについてそれほど詳細に網羅していないが、添付ファイルの扱いも同様に容易である。好ましい実施形態では、添付ファイルの各々は本体フィールド６０とほぼ同様に扱われるが、ＸＭＬでラップされない、または符号化（ＡＳＣＩＩに変換）されない点が異なる。その代わり、プロトコルバージョン情報；本体のものと同様の新規の長さ要素；セキュア電子メール１４の本体に使用されているものと同じmessageI

ｄ１０４ａのコピー；この添付ファイル本体のハッシュを取って作成した新規のｍｉｃ要素；シール（上述したsListのもの）を含んだバイナリヘッダが追加される。次に、この添付ファイルが、ヘッダが追加されたセキュア電子メール１４の本体に使用したものと同じmessageKey１０４ｅを使用して暗号化され、この暗号化されたものが通常の方法で電子メールサーバ２２にアップロードされる。

【０１１８】

添付ファイルへのこの手法には多くの利点がある。添付ファイルの検証メカニズムがセキュア電子メール１４内部で実施され、これに適用可能なセキュリティ特徴によって保護されるため、添付ファイルを扱うこの手法によってセキュリティサーバ２４のデータベース１００が必ずしも妨害されることはない。また、あらゆる数の添付ファイルのサポートが可能である。各添付ファイルは、暗号化を実行するソフトウェアモジュール２６内に送られるオブジェクトに追加される。各添付ファイルは、メッセージの本体と同じmessageKey１０４ｅを用いて暗号化され、各添付ファイルのハッシュは同じアルゴリズムを用いて計算できる。各添付ファイルにフルヘッダを付与することで、各添付ファイルを他の添付ファイルとは別に、さらには本体と別に復号化することが可能になる。添付ファイルを別々にすることにより、特に変更された添付ファイルがあるか否かを判断できる。セキュア電子メール１４のこれ以外の部分での通常動作は、たとえ添付ファイルを有するセキュア電子メール１４への返信時のように、添付ファイルが故意に含まれていない場合でも実施することができる。

【０１１９】

上述したように、セキュア電子メール１４は、通常の電子メールシステムを介して各受信者１６のインボックスへ到達する。受信者１６は例によって、ブラウザの、受信した全メッセージの一覧が表示されている画面へ進むことができる。メッセージ一覧上をクリックすると、ブラウザは、その中のメッセージでフォーマットされたページを送信できるようになる。しかし、これには適切なソフトウェアモジュール２６が存在することが必要である。

【０１２０】

受信ユニット２０にソフトウェアモジュール２６をインストールすれば、これをメッセージの受信/読み出しシナリオに使用する準備が整う。以下の説明では、プラグイン変形４６ａのソフトウェアモジュール２６を用いたプライベート・ラベル・ブラウザも使用されているが、さらに当業者は、この基本となる原理を、セキュア電子メールシステム１０を使用しているこれ以外のシステムにも拡大できることを容易に理解するだろう。

【０１２１】

簡単に図４に戻ると、同図はさらに、セキュア電子メール１４が受信されているか否かを判断するためのソフトウェアモジュール２６への好ましい手法も様式的に示している。受信ユニット２０内のソフトウェアモジュール２６が、セキュア電子メール１４を含むものがあるかどうか、ページ７２のストリーム７０を検査する。ソフトウェアモジュール２６がページ７２にセキュア電子メール１４が含まれているか否かを判断する方法は、“------- BEGIN SECURECORP SECURED EMAIL -------”タイプのタグについて走査を実行するというものである。この作業は、それ以上処理されるべきでないページを送信する待ち時間を最短化することで、迅速に実施できる。実際の候補ページ７２ａが見つかった場合、このページはストリーム７０から除去され、今説明したとおりに処理され、処理済のページ７２ｂとしてストリーム内に戻されることで、受信者１６がこのページを読むことが可能になる。

【０１２２】

図８は、好ましい復号化プロセス１５０を示すフローチャートである。ここでも同様に、受信者１６の受信ユニット２０上で実行されているブラウザ内にソフトウェアモジュール２６が既にインストールされており、受信者１６がセキュリティサーバ２４に登録済みであると仮定する（セキュリティサーバ２４は、恐らく、未登録のあらゆる受信者に対して既に電子メールを生成している）。受信者１６がセキュア電子メール１４（つまり、暗

号化プロセス１２０に従って作成された、安全化およびシールされたＸＭＬ文書）を選択すると、ソフトウェアモジュール２６が、セキュア電子メール１４を受信者１６によって読み出し可能なものにするために、復号化動作を実行する。これがステップ１５２、つまり復号プロセス１５０の開始を構成する。

【０１２３】

ステップ１５４では、受信者１６がパスワードを取得する。セキュリティサーバ２４は送信者１２と受信者１６の両方をユーザとして扱い、送信者１２と受信者１６の両方がユーザテーブル１０２（図５）内への同等のエントリを有する点を思い出されたい。まだパスワード１０２ｂがキャッシュされていない場合には、受信者１６がパスワードの入力を催促される。パスワードのキャッシング、催促などの規則は送信の場合と同様である。

【０１２４】

ステップ１５６にて、ソフトウェアモジュール２６がmessageId１０４ａを抽出し、受信したメッセージを（符号化されている場合には）復号化し、（まだ暗号化された状態の）本体フィールド６０を抽出する。

【０１２５】

ステップ１５８にて、以下の情報がセキュリティサーバ２４へ（ＳＳＬ経由で）送られる：

受信者１６の電子メールアドレス（emailAddress１０３ａ）；
受信者１６のpassword１０２ｂ；そして
messageId１０４ａ。

【０１２６】

ステップ１６０では、セキュリティサーバ２４が、認証サブプロセスの結果に従って先に進む。

１）　password１０２ｂを決定するために、セキュリティサーバ２４がsalt１０２ｃで受信者のパスワードのハッシュを実行する。

２）　受信者１６のemailAddress１０３ａとの関連に一部基づき、パスワード１０２が検証される。この認証部分が失敗した場合、受信者１６に正確なパスワード１０２ｂの入力、または復号プロセス１５０の中止を催促する応答がソフトウェアモジュール２６に送信される。

３）　受信者１６がこのセキュア電子メール１４を読むことを許可されているか否かが判断される。このためには、受信者１６の電子メールアドレスが、特定のmessageId１０６ａの受信者テーブル１０６内のreceiverAddr１０６ｂと一致しなければならず、numRequests１０６ｄが、このセキュア電子メール１４のmaxDeliveries１０４ｆよりも少なくなくてはならず、さらに、expiration１０４ｇが、このメッセージの有効期限が既に切れている旨を示すものでなければならない。この許可が失敗すると、受信者に通知が送られ、さらに、セキュア電子メール１４を復号化することなく復号プロセス１５０を終了するよう要求する応答がソフトウェアモジュール２６に送信される。

【０１２７】

これら検査のいずれかが失敗した場合、ブラウザページは、単純に、暗号化されたデータを含んでいないかのような表示を行える、つまり、本体フィールド６０が通常そうであるように理解不能な訳のわからない文字の羅列として表示することができる点に留意すべきである。しかし、送信者ＩＤフィールド６６、様々な受信者ＩＤフィールド５６、そして、恐らくは（構成により）件名フィールド５８を依然として理解不能にしておくことができる。そのため、受信者１６は、送信者１２または他の受信者１６と接触して、そのセキュア電子メール１４が重要であるか、また、セキュア電子メールシステム１０外部での処置が適切であるか否かを判断することができるようになる。これらの検査が成功すると、この受信者１６は認証されたと考慮され、このステップ１６０が終了する。

【０１２８】

ステップ１６２では、セキュリティサーバ２４がmessageKey１０４ｅを、ＳＳＬ経由で受信者１６のソフトウェアモジュール２６へ返送する。

【０１２９】
ステップ１６４では、ソフトウェアモジュール２６が、これと同じmessageKey１０４ｅと、暗号化する際に使用した基本プロセスを逆にしたものを用いて、セキュア電子メール１４を復号化する。
【０１３０】
ステップ１６６では、ソフトウェアモジュール２６がセキュア電子メール１４の妥当性チェックを実行する。このために、セキュリティサーバ２４との第２ラウンドの通信が実施される。ソフトウェア２６はセキュア電子メール１４の各部分の新規ハッシュを生成し、これらのハッシュと、各メッセージ部分に含まれているシールとをセキュリティサーバ２４に送信する。次に、セキュリティサーバ２４が、ハッシュ内の送信されたものに基づいて新規シールを計算し、これをシール内の送信されたものと比較する。これらの間に相違があれば、そのセキュア電子メール１４が認証されないものであることを示す。次に、セキュリティサーバ２４が、セキュア電子メール１４の認証性に関する表示を、ソフトウェアモジュール２６へ返送する。
【０１３１】
最後に、ステップ１６８にて、暗号化されたメッセージが配置されていたセキュア電子メール１４の平文本体フィールド６０を表示するＨＴＭＬ受信フォーム５４が受信者１６に対して示される。さらに、セキュリティサーバ２４からの認証性に関する表示が負であった場合には、ソフトウェアモジュール２６は、これに関して受信者１６に提案するメッセージも表示する。
【０１３２】
また、好適な実施形態では、複合プロセス１５０の最適化として、ソフトウェアモジュール２６がmessageKey１０４ｅをキャッシュすることで、同一のセッション中に、セキュリティサーバ２４にアクセスすることなく同じメッセージを再び読むことができる。しかし、これは読み出し動作のみに適用され、messageKey１０４ｅがディスク上に保存されることはない。
【０１３３】
あらゆる添付ファイルの復号化は、これと同じmessageKey１０４ｅと、同じ基本プロセスを用いて単純に実行される。前述したとおりバイナリヘッダを使用している点と、添付ファイル内の情報が符号化されていない点のみが異なる。
【０１３４】
要するに、好適な実施形態のソフトウェアモジュール２６は：ＨＴＭＬページを提供する前に、該ページを代行受信およびパースし；ＨＴＭＬページを提供する前に、該ページを選択的に変更し；ＨＴＭＬフォームおよびページからデータを抽出し；安全な手段（例えば安全なＨＴＴＰ、ＳＳＬ）を使ってデータをセキュリティサーバへ送信し；同一のアルゴリズムを使用して対称な鍵暗号化および復号を実行し（例えばBlowfish対称鍵暗号/復号）；ハッシングを実行し（例えばSecured hash algorithm one, SHA-1）；（パスワード入力、構成、エラーメッセージ、シール検証結果のための）ダイアログボックスを表示し；好ましくは自己更新型である。
【０１３５】
前出の暗号化プロセス１２０と復号プロセス１５０の基礎となるセキュリティ特徴にはさらに何らかの分析が含まれる。セキュリティサーバ２４のオペレータは、送信者のemailAdress１０３ａがpassword１０２ｂと関連するべきであるため、認証の目的から送信者１２を知っている。password１０２ｂがあるべきとおりに、つまり、その保持者にしか知られない方法で扱われた場合、セキュリティサーバ２４のオペレータは、この送信者１２のみが特定のセキュア電子メール１４を送信できたと確信できる。しかし、送信者１２が信用されている必要は少しもない。セキュリティサーバ２４のオペレータはさらに、最初にseaSalt１０４ｈを保存することで、その送信者１２を含む何人であってもセキュア電子メール１４をその送信後に変更することは不可能である旨を確信することができる。追加のセキュリティ特徴として、暗号化したsealSalt１０４ｈをデータベース１００に保存

し、共用や、セキュリティサーバ２４から持ち出すことを絶対に許可しないようにしてもよい。送信者１２の認証（password１０２ｂの提出によって行う）の後に、ＳＳＬ鍵で本体と添付ファイルのハッシュ（Ｈ（ｂ）、Ｈ（ａ））を暗号化することで、セキュア電子メール１４に署名しているのは送信者１２であると判断することが可能になる。セキュリティサーバ２４は、送信者１２の実パスワードのハッシュのみをpassword１０２ｂとして保存しているので、セキュリティサーバ２４のオペレータでさえ送信者１２の代わりにセキュア電子メール１４に不正に署名することは全く不可能である。

【０１３６】

messageKey１０４ｅは対称であり、外部エンティティ、つまりセキュリティサーバ２４がこれを保存しているので、何者かが例えばデータベース１００に侵入して、セキュア電子メール１４の代行受信と、さらにそのmessageKey１０４ｅの入手の両方を実行すれば、その人物はセキュア電子メール１４を復号化できてしまう。興味深いことに、この内の一方しか入手できなければ復号化は行えない。messageKey１０４ｅを公開鍵で暗号化すれば、この手法をさらに強化できる。所与のセキュア電子メール１４をクラッキングするために必要なmessageKey１０４ｅを入手するには適切な秘密鍵を要するため、これでデータベース１００への侵入も役に立たなくなる。したがって、データベース１００への総当たり攻撃も実行不可能となる。さらに、セキュリティサーバ２４のオペレータが必要な秘密鍵を可能な限り実ハードウェア内に置くことができ、これにより、採用している実マシンに物理的にアクセスしない限りデータベース１００への侵入が実質的に不可能になる。

【０１３７】

セキュア電子メール１４を読むことは、その送信よりも単純である。ここで唯一の問題は、復号に使用するシングルキー（messageKey１０４ｅ）をメッセージ毎に設けている点である。そのため、ソフトウェアモジュール２６内において、鍵が受信者のマシン上でノーガードとなり、これにアクセスできる瞬間がある。しかし、これによって可能になるのは、受信者１６が読み出しを許可された最新のセキュア電子メール１４を読むことだけである。そのため、この場合に危険が生じるのは、無許可の人物がメモリ内の鍵に短時間アクセスできた場合だけである。これを実行することは非常に困難であり、この方法で鍵を盗めるならば、復号化したメッセージも一緒にいとも簡単に（それ以上ないほど簡単に）盗めてしまうということになる。それなら鍵などに関心を持たないだろう。要するに、これはセキュリティリスクではないのである。

【０１３８】

シールを使用することで、信頼できる第三者の公証人として機能するセキュリティサーバ２４のオペレータを介した否認防止が得られる。特に、裁判官は、メッセージが、セキュリティサーバ２４のオペレータにシール、メッセージのハッシュ、送信者１２の名称（userId１０２ａをマッピングするため）を付与することで実際に送信者１２から送信されたものか否かを判断できる。好適な実施形態について説明したとおり、受信者１６はシールを、そのシールと、受信したメッセージのハッシュをセキュリティサーバ２４に送信することで、これが本物であると検証することができる。（送信者１２が、実際に書き、特定のセキュア電子メール１４を送信したことを証明する。）その後、セキュリティサーバ２４がこれに関連して保証を提供する。セキュリティサーバ２４にて、３つの既知の数量に基づいてこのシールを再計算するために使用して、このシールが本物であるか否かを判断する。この技術は「秘密鍵による否認防止」として知られており、Kaufma等による"Network Security: Private Communication in Public World", Prentice-Hall, 1995, pp. 343-44により示唆されている。

【０１３９】

ここで説明した実施形態におけるセキュリティの多くがＳＳＬの強度に基づくことが明白である。現在これが基準として受け入れられているようなので、ここでは、送信者１２のpassword１０２ｂとmessageKey１０４ｅの両方がＳＳＬ経由で送信されるという事実を心配することはない。しかし、セキュア電子メールシステム１０のセキュリティの強度はＳＳＬに依存するものではない。通信チャネルを保護するためのより安全なプロトコルの

利用が可能になっており（例えば、Transport Layer SecurityまたはＴＬＳ）、セキュア電子メールシステム１０はこのようなプロトコルを容易に使用できる。

【０１４０】

ここまで、主にセキュア電子メールシステム２０のプレゼンテーションについて説明してきた。しかし、このキーサーバの概念は、安全な通信に伴う問題に取り組む様々なソリューションを構築および展開するためにさらに一般的に使用することができる。たとえば、この手法はさらに、特に企業内インスタントメッセージング（ＥＩＭ）、ビデオ会議、安全なリアルタイム文書編集を促進できる。これらは、メッセージコンテンツを伝送またはルーティングするためにメッセージヘッダを採用した通信スキームの単なる追加例であり、キーサーバはこのような通信スキームのいずれとも効率的に使用することができる。

【０１４１】

このキーサーバによって提供されるソリューションは、組織間での共同使用にも特に適している。組織は、キーサーバを使用することで、その構成要素に技術と媒体の贅沢な組み合わせを介して自由かつ容易に共同させながら、最も厳しいセキュリティの必要性を満たすことができる。

【０１４２】

以下の用語は、本明細書の以降の説明をとおして頻繁に使用されるものであるため、ここで便宜性のために定義しておく：

秘密保護 -- データの場所に関係なく（例えば、送信中または記憶装置内）、許可された受信者しかデータを見ることができないようにする。

会話鍵 -- 会話データを保護する対称鍵。会話データは１つの送信元から１つまたはそれ以上の宛先へ流れる。

ハブ -- メッセージを処理し、このメッセージを適切な宛先へ中継するネットワークサーバ。

整合性保護 -- 送信中または記憶装置内にあるデータへの無許可の変更を確実に検出する。

参加 -- コラボレーションへの参加を開始する。

キーサーバ -- 保護鍵を保持しており、これらを許可されたユーザに公開するネットワークサーバ。

退出 -- コラボレーションへの参加を中止する。

ヘッダ鍵 -- メッセージのヘッダを保護する対称鍵。ヘッダ鍵はハブと各スポークの間で個別に確立される。

メッセージ -- コラボレーション参加者間で交換されるデータの基本ユニット。メッセージは「ヘッダ」と「コンテンツ」の２つの部分で構成されている。

メッセージコンテンツ -- コラボレーション参加者によって生成されるデータであり、１つまたはそれ以上の他の参加者へ宛てて送信される。

メッセージヘッダ -- メッセージルータがコンテンツをその宛先へ伝送する上で補助をするデータ。

保護 -- 秘密および整合性の保護。

スポーク -- データの送信者または受信者；スポークはデータの中継を行わない。

トランスクリプト -- コラボレーションのある部分の記録。

【０１４３】

図９は、セキュリティサーバシステム２１０の主要な構成要素を示す概略ブロック図である。ほぼ汎用化されているが、この実施形態は企業におけるコラボレーション通信に特に適している。ここで、主要な構成要素にはコラボレーション参加者２１２、１つまたはそれ以上のメッセージルータ２１４、１つまたはそれ以上のキーサーバ２１６が含まれる。したがって、この場合のコラボレーション参加者２１２は、図１の送信ユニット１８、受信ユニット２０に等しい。メッセージルータ２１４は、図１の電子メールサーバ２２（または従来型のルータ）に等しい。しかし、先述したように、ここでのメッセージルータ２１４は、特にセキュリティサーバシステム２１０を使用している企業の制御下にあって

よい。図９のキーサーバ２１６は、図１のセキュリティサーバ２４に等しい。
【０１４４】
コラボレーション参加者２１２は、メッセージ２１８の送信元（送信元参加者２１２ａ）および/または宛先（宛先参加者２１２ｂ）先述のように、会話鍵２２０は、メッセージ２１８のコンテンツを保護するために使用される。
【０１４５】
メッセージルータ２１４は、メッセージ２１８を目的のコラボレーション参加者２１２へ伝送する。メッセージ２１８は実際には複数のメッセージルータ２１４を通過するであろうが、図面中では１つのメッセージルータ２１４（または電子メールサーバ２２、およびセキュア電子メール１４が通過するであろう使用可能なルータ）のみを概念形成的に示している。複数のメッセージルータ２１４を設けている場合には、その各々が、コラボレーション参加者２１２を見るのと同様に他のメッセージルータ２１４を「見る」。コラボレーション参加者２１２の各々が、少なくとも１つのメッセージルータ２１４（または「最も近い」メッセージルータ２１４）との継続的な接続を維持する。
【０１４６】
キーサーバ２１６は会話鍵２２０を作成するか、または送信元２１２ａの参加者から会話鍵２２０を受信する。その後、キーサーバ２１６がこの会話鍵２２０を保存し、コラボレーション参加者２１２である参加者に公開する（恐らくは認証および許可後に行うが、様々なスキームを使用でき、関連性があるかどうかはここでの主題ではない）。さらにキーサーバ２１６も会話鍵２２０を大量に作成/保存でき、要求に応じて任意数を公開できる。そのため、サーバクラス装置であるクライアント（例えば電子メールゲートウェイ）が会話鍵２２の組を大量に入手でき、また、キーサーバ２１６に一意の会話キー２２０を毎回要求する必要なく、この中からそれぞれ唯一の鍵を使って各メッセージ２１８を保護できる。
【０１４７】
以下の説明を単純化するために、暗号化と復号を主な保護の例として使用する。鍵で暗号化/復号化することで、メッセージの秘密性が保護される。しかし、これは単に１つの保護の利用可能な例でしかない点を理解すべきである。鍵を使用したメッセージダイジェスト（ハッシュされたメッセージ認証コード、またはＨＭＡＣとしても知られている）を用いてメッセージの整合性を保護したり、両タイプの保護を適用することができる。例えば、キーサーバ２１６は２５６ビット鍵を作成し、これを送信元の参加者２１２ａに公開することができる。これにより、送信元の参加者２１２ａは第１の１２８ビットを暗号化に、第２の１２８ビットをＨＭＡＣに使用できる。
【０１４８】
会話鍵２２０を暗号化またはハッシュへの使用後に、解読またはハッシュ分析のためにこれを回収する必要があるので、キーサーバ２１６は各会話鍵２２０の一意ＩＤと関連している。一意ＩＤ、またはこれから導出できる何かが、保護された各メッセージ２１８と共に普通文で送信される。そのため、コラボレーション参加者２１２がキーサーバ２１６に会話鍵２２０の要求を提出すると、キーサーバ２１６が要求された会話鍵２２０を含んだ返信をコラボレーション参加者２１２に送信する。キーサーバ２１６は汎用体であり、任意タイプのアプリケーションについて会話鍵２２０を扱うために使用できる。これによって、コラボレーション参加者２１２とキーサーバ２１６の間のセッションが安全なセッションとなる。
【０１４９】
図１と図９は、オプションであるが、非常に便利な特徴を図示する主要な点において異なる。図１では、電子メールサーバ２２とセキュア電子サーバ２４を、直接通信しないものとして示している。このスキームは、例えば電子メールサーバ２２（またはその代用品としてのメッセージハブ）が従来のものである場合に効果を発揮する。これに対して図９では、メッセージルータ２１４とキーサーバ２１６を、直接通信するものとして示している。このスキームは、メッセージルータ２１４がセキュリティサーバシステム２１０内で

機能するように設計されている場合に効果を発揮する。そのため、メッセージルータ２１４は、コラボレーション参加者が会話に参加または会話から退出する際に新規の会話鍵２２０を作成するようキーサーバ２１６に指示するエンティティであってよい。

【０１５０】

図１０は、セキュリティサーバシステム２１０におけるメッセージ２１８の典型的な流れを示す概略ブロック図である。メッセージ２１８は、メッセージヘッダ２２２とメッセージコンテンツ２２４を含む。

【０１５１】

メッセージヘッダ２２２は、メッセージルータ２１４がメッセージをその宛先、つまり１つまたはそれ以上の宛先参加者２１２ｂへ伝送する際に補助となるデータを含む。以下はメッセージヘッダ２２２内に含まれる要素の例である：

宛先 -- メッセージの宛先。

送信元 -- メッセージの起源。

日付 -- メッセージ作成日時。

メッセージＩＤ -- そのメッセージのための一意のＩＤ。

コンテンツ長 -- コンテンツの長さ。

コンテンツタイプ -- ＭＩＭＥタイプのコンテンツ。

優先順位 -- メッセージの優先順位。

【０１５２】

メッセージコンテンツ２２４は、送信元の参加者２１２ａによって生成され、１つまたはそれ以上の宛先参加者２１２ｂに宛てられたデータを含む。もちろん、コラボレーションの最中に複数のメッセージ２１８を交換する場合、コラボレーション参加者２１２は、送信元参加者２１２ａとしての役割りを変更でき、頻繁にこの変更を行う。メッセージルータ２１４はメッセージコンテンツ２２４を検査しない。［コンテンツフィルタリングやウィルススキャンのような特別なサービスが、メッセージコンテンツがその宛先に転送される前にこれを検査できる。しかし、これはオプションサービスであり、メッセージルーティングとは別のものである。］

【０１５３】

図１０はまた、図示されたセキュリティサーバシステム２１０の実施形態が、実際にデータ保護のために2タイプのキーをどのように使用するかも示している。ここでも、保護は秘密性、整合性、またはその両方に関連している。第一に、メッセージルータ２１４が各コラボレーション参加者２１２と共にヘッダ鍵２２６を確立する。このヘッダ鍵２２６はメッセー２１８のメッセージヘッダ２２２を保護する。メッセージルータ２１４とコラボレーション参加者２１２の間で接続がなされる度に、異なるヘッダ鍵２２６が使用される。キーサーバ２１６はヘッダ鍵２２６の作成、保存、管理を行わない。さらに、ヘッダ鍵２２６は一時的なものであり、メッセージルータ２１４とコラボレーション参加者２１２の間でのセッションの継続時間を超えて有効性を維持することはない。第二に、会話鍵２２０はメッセージ２１８のコンテンツを保護する。あらゆるプロセス（コラボレーション参加者２１２またはメッセージルータ２１４）が会話鍵２２０を作成する（要求し、許可される）ことが可能である。この２つの鍵の手法を使用することで、送信元から宛先までの間において、効率的かつ安全性の高いメッセージ２１８の配布が可能になる。

【０１５４】

この２つの鍵の使用は、会話鍵２２０に等しい１つの鍵のみを使用する図１に示したスキームとも異なる。ヘッダ鍵の使用はオプションであるが、その使用によって安全性が高まる。例えば、メッセージルータ２１４を制御している企業はこの追加的レベルの安全性を付加して、メッセージヘッダ２２２内の情報をも安全化してしまうことを望むかもしれない。

【０１５５】

メッセージルータ２１４がその任務を実行するには、メッセージ２１８のメッセージヘッダ２２２のみを処理するだけでよい。図１０では、メッセージルータ２１４は、通信す

るコラボレーション参加者２１２に従い、異なるヘッダ鍵２２６（K_{H1}、K_{H2}、K_{H3}、またはK_{H4}）を使用する。メッセージ２１８のメッセージコンテンツ２２４は、無変更のまま単純にメッセージルータ２１４を通り、次に、宛先の参加者２１２ｂが、メッセージ２１８のメッセージコンテンツ２２４を解読し、その整合性を検証するために、同一の会話鍵２２０（K_c）を要求および使用する。各メッセージルータ２１４は、メッセージコンテンツ２２４全体の整合性を検証することなくメッセージ２１８を次のメッセージルータ２１４へ「流す」ことができるため、この方法でヘッダ鍵２２６を会話鍵２２０から分離することが有利である。これは、人工的にメッセージを管理可能なブロックに分け、各ブロックを個々に暗号化する必要があるＳＳＬおよびＩＰＳｅｃとは対照的である。

【０１５６】

メッセージルータ２１４は、将来的および過去的な秘密性を提供するために、以下のイベントが生じた場合、会話鍵２２０を変更または「ロールオーバ」できる。新規のコラボレーション参加者２１２が会話に参加した場合、メッセージルータ２１４が会話鍵２２０が変更されたことを知る。このイベントが発生する前に通信が行われたメッセージ２１８はすべて、過去の会話鍵２２０を使用して暗号化された状態を維持し、また、デフォルトでは、これらのメッセージ２１８が新規のコラボレーション参加者２１２に対して利用可能にされることはない。同様に、既存のコラボレーション参加者２１２が会話を退出する場合（例えば、メッセージルータ２１４との接続を切断する場合）、このイベント後に通信が行われたすべてのメッセージ２１８は新規の会話鍵を使用して暗号化される。デフォルトでは、退出するコラボレーション参加者２１２はこの会話鍵２２０を使用できないようになっている。セキュリティサーバシステム２１０の好ましい実施形態では、トランスプリプトは、暗号化された状態で記憶装置に保存される。そのため、コラボレーション中のイベントのシーケンスによっては（つまり、参加および退出動作）、会話の異なる部分を暗号化するための複数の会話鍵２２０が存在する場合もある。

【０１５７】

例えばコラボレーション参加者２１２が多数いる場合に、会話鍵２２０ロールオーバプロセスを、図９、図１０中のこの実施形態の企業のコラボレーションテーマと一致するように最適化することができる。一般に、メッセージルータ２１４は、実際の（暗号化した）メッセージコンテンツ２２４にアクセス不能であっても、メッセージコンテンツ２２４が実際の物であるか否かを判断することはできる。例えば、メッセージヘッダ２２２内の情報がこれを表すものであってよく、あるいは、メッセージコンテンツ２２４がなくてもよい。メッセージルータ２１４は、この情報を用いて、会話鍵２２０のロールオーバを、次の実際のメッセージ２１８に遭遇するまで変更することができる。これにより、複数のコラボレーション参加者２１２が新規の会話に参加できるようになり、参加の度に会話鍵２２０が自動的にロールオーバされないようになる。その代わり、実際のメッセージ２１８の送信時に会話鍵２２０がロールオーバされる。同様に、複数のコラボレーション参加者２１２が既存の会話を退出し、会話鍵２２０が次の実際のメッセージ２１８が送信されるまでロールオーバされないようにすることができる。

【０１５８】

次の説明は、セキュリティサーバシステム２１０の実現のいくつかの新規概念を制限なく要約したものである。このセキュリティサーバシステム２１０は、１つの会話鍵２２０を割り当ておよび使用してデータの保護を行うが、そのデータが存在する限りこの１つの会話鍵２２０を使い続けることが可能である。この１つの会話鍵２２０を使用することで、メッセージルータ２１４はメッセージ２１８を解読および再暗号化する必要がなくなる。これにより、メッセージ２１８の非常に効率的なルーティングが可能となり、スケーラブルで企業クラスのコラボレーションシステムを実現できる。

【０１５９】

これと対照的に、既存の技術は、データがその起源から複数の宛先へ送信される際に、複数の鍵を使用して、（秘密性および整合性に関連して）データを保護する。典型的な実現は、セキュアソケットレイヤ/トランスポートレイヤセキュリティ（ＳＳＬ/ＴＬＳ）プ

ロトコル、またはＩＰＳＥＣプロトコルを採用している。ＳＳＬ/ＴＬＳを使用することで、各メッセージをその起源において暗号化し、このメッセージをルーティングするサーバ（つまりハブ）において復号化し、該ハブにおいて再暗号化し、最後に最終的な宛先において復号化することが必要になる。

【０１６０】

また、セキュリティサーバシステム２１０は、将来的および過去的な秘密性を容易に維持することもできる。新規コラボレーション参加者２１２の参加時、または既存のコラボレーション参加者２１２のコラボレーション退出時に、会話鍵２２０を変更できる。これにより、新規ユーザが参加以前のコラボレーションデータのどの部分にもアクセスできず、同様に、会話を退出したユーザは退出後にはそのコラボレーションにアクセスできないことがすべてのコラボレーション参加者２１２に保証される。たとえ攻撃者がセキュティサーバシステム２１０との接続状態を維持し、メッセージ２１８を受信しても、攻撃者は、これらメッセージ２１８のメッセージコンテンツ２２４を復号化するための会話鍵２２０を取得することはできない。

【０１６１】

これと対照的に、既存の技術では秘密性の維持を接続状態に頼っている。つまり、ハブに接続していないユーザはコラボレーションデータを受信できない。これは下級ユーザが使用するにはよいが、上級の攻撃者からコラボレーションデータを保護するには安全な技術ではない。

【０１６２】

セキュリティサーバシステム２１０は、効率的なマルチユーザ参加も可能にする。メッセージルータ２１４において会話鍵２２０による暗号化または複合を行わないことにより、メッセージルータ２１４における暗号化および復号の回数を最小化する。実際、メッセージルータ２１４においてコラボレーションデータに適用される暗号化および復号の回数は、コラボレーション参加者２１２の数には関係ない。

【０１６３】

これと対照的に、既存の技術では、ユーザ数が増えるとパフォーマンスに劣化が生じてしまう。このようなパフォーマンス劣化には多くの要因が貢献するが、主な要因は、システムの各構成要素によって実行される保護動作の数である。既存の技術は、セッション鍵を使用してコラボレーションデータを保護する。この既存技術では、セッション数がユーザ数と比例し、必要な保護動作がユーザ数と共に増加するため非効率である。

【０１６４】

セキュリティサーバシステム２１０は、同一のコラボレーションまたはセッション内で複数の安全なスレッドを実行することもできる。これは、コラボレーションデータ（メッセージコンテンツ２２４）が、セッション鍵よりはむしろ会話鍵２２０を使用して保護されているからである。そのため、許可されたコラボレーション参加者２１２の組によっては、１つのセッションで複数の会話鍵２２０を使用できる。

【０１６５】

既存の技術は、コラボレーションデータを保護するためにセッション鍵を使用する。そのため、同じコラボレーション内における会話の複数のスレッドを保護するには複数のセッションが必要となる。これにより、システムが柔軟性に欠け、非効率なものとなってしまう。

【０１６６】

さらにセキュリティサーバシステム２１０では、トランスクリプトの扱い方法も洗練されている。該システム２１０は、コラボレーションの最中およびコラボレーション後に、同じ会話鍵の組を使用してメッセージコンテンツ２２４を保護する。これにより、より柔軟で安全性の高いコラボレーションシステムが得られる。

【０１６７】

セッション鍵を使用する技術は、セッション鍵は一時的なものであり、コラボレーション終了と同時に失効するため、コラボレーションデータのトランスクリプトを保護する技

術は厳密性を有する。

【０１６８】

また、セキュリティサーバシステム２１０は、これ以外の既存のセキュリティ技術を今説明したように改良する。すべてのセキュリティ機能に公開鍵インフラストラクチャ（ＰＫＩ）を使用するコラボレーション技術によって、システムが非効率で厳密なものになる。ＰＫＩを用いてコラボレーションデータの保護を行うには、参加者全員がＰＫＩデジタル証明書を持っている必要がある。これと対照的に、セキュリティサーバシステム２１０は、ＰＫＩ証明書を、任意のコラボレーション参加者２１２を認証するために使用することができる。しかし、ＰＫＩ証明書を所有する必要はない。そのため、自分の認証性を十分なレベルで証明できるコラボレーション参加者２１２はコラボレーションに参加できる。

【０１６９】

ＩＰＳｅｃに基づいたコラボレーション技術は、個々のセキュリティアソシエーション（ＳＡ）を使用する必要がある。第一に、ＳＡは一時的なものであり、事実上、ＳＡ鍵は送信中のコラボレーションデータしか保護できない。第二に、ＳＡは送信元/宛先のペアに指定されている。したがって、ハブ－スポークモデルに基づいて動作するコラボレーションアプリケーション（例えばインスタントメッセージング）は、情報が複数のＳＡ間で送信される際にデータの保護を要する。これと対照的にセキュリティサーバ２１０は、同じベース技術を使用して、送信中および記憶装置保存中（つまりトランスクリプト）のコラボレーションデータ（メッセージコンテンツ２２４）を保護する。

【０１７０】

ＳＳＬ/ＴＬＳを使用するコラボレーション技術には複数のＳＳＬ/ＴＬＳセッションが必要である。第一に、セッションは一時的なものであり、事実上、セッション鍵は送信中のコラボレーションデータしか保護できない。第二に、セッションはクライアント/サーバのペアに指定されている。したがって、ハブ‐スポークモデルに基づいて動作するコラボレーションアプリケーション（例えばインスタントメッセージング）は、情報が複数のセッション間で送信される際に情報データの保護を要する。これと対照的に、セキュリティサーバシステム２１０は、同一のベース技術を使用して、送信中および記憶装置保存中（つまりトランスクリプト）のコラボレーションデータを保護する。

【０１７１】

図１１は、通信システム３１０が４つの基本構成要素、すなわち通信を行っている参加者３１２（発信者３１４または受信者３１６）、認証オーソリティ３１８、キーサーバ３２０がどのように構成されているかを示すブロック図である。

【０１７２】

一般に、発信者３１４と受信者３１６が、認証オーソリティ３１８に接触し、自己を認証する。しかし、発信者３１４の認証オーソリティ３１８は、受信者３１６の認証オーソリティ３１８と同一であっても、異なっていてもよい。通信を行っている参加者３１２は、認証オーソリティ３１８に指定されたプロトコルを使用する（例えばＴＬＳ上のユーザＩＤおよびパスワード、２ファクタ認証、ＰＫＩ証明書を使用するチャレンジ/応答プロトコルなど）。認証が成功すると、認証オーソリティ３１８が通信を行っている参加者３１２に認証アサーション３２２を発行する。認証オーソリティ３１８はこのアサーション３２２に署名する（一般にＰＫＩ秘密鍵を使用して行う）。すべてのアサーション３２２はそれぞれ異なっている。

【０１７３】

次に、発信者３１４は、１つまたはそれ以上の受信者３１６に送信したい通信文３２４用のデータを有している。発信者３１４はキーサーバ３２０に接触し、そのアサーション３２２と、目的の通信文３２４用の属性３２６を提出する。この属性３２６については以降でより詳細に説明するが、属性３２６は、通信文３２４のための目的受信者３１６のリストを含んでいる。

【０１７４】

キーサーバ３２０は、発信者３１４からのアサーション３２２を確認する。その後、将来の通信文３２４にリソースＩＤ３２８を割り当て、通信文３２４の暗号化に適した鍵３３０を作成し、リソースＩＤ３２８と鍵３３０を発信者３１４へ戻す。場合により、発信者３１４は鍵３３０をキーサーバ３２０へ送信し、この鍵３３０をリソースＩＤ３２８と関連付けるよう要求することができる。この最中に、キーサーバ３２０はリソースＩＤ３２８、鍵３３０、アサーション３２２、属性３２６を、管理しているデータベース３３２に保存する。

【０１７５】

次に発信者３１４は、鍵３３０を使用してデータを暗号化し、リソースＩＤ３２８を普通文で追加することによって通信文３２４を構成する。その後、発信者３１４が、従来の手段を使ってこの通信文３２４をすべての受信者３１６に送信する。発信者３１４は、キーサーバ３２０または認証オーソリティ３１８のいずれにも通信文３２４を送信する必要は全くなく、またほとんどの実施形態において送信していない点に留意すべきである。

【０１７６】

各受信者３１６はキーサーバ３２０から、暗号化された通信文３２４の復号に適した鍵３３０を受信する必要がある。通信文３２４は普通文でのリソースＩＤを含んでいるため、受信者３１６はそのアサーション３２２とリソースＩＤ３２４をキーサーバ３２０に提供する。次にキーサーバ３２０が、この受信者３１６からのアサーション３２２を確認する。さらに、先に発信者３１４が属性３２６提供した宛先受信者３１６のリストを使用して、その受信者３１６が、リソースＩＤ３２８が指定するその通信文３２４の宛先の受信者であるか否かを調べる。この属性３２６内に、これ以外に、先述した鍵３３０を使用可能にするための基準がさらに含まれている場合には、キーサーバ３２０はこれらの基準が一致するか否かも調べる。その後、キーサーバ３２０が受信者３１６に鍵を提供する。

【０１７７】

最後に、受信者３１６が鍵３３０を使って通信文３２４を復号化する。これと同時に、復号が成功したか否かにより、また場合により、通信文３２４内に含まれている暗号化チェックサムを比較することにより、通信文３２４のコンテンツの整合性が実証される。このようなチェックサムは、リソースＩＤ３２８と共に通信文の普通文の部分に含まれていてよいが、より典型的には、暗号化された部分に通信文３２４のコンテンツと共に含まれる。このようなチェックサムは、通信文３２４全体の異なる各部分も包括できる。例えば、通信文３２４のコンテンツ部分のみから導出でき、または、該通信文３２４の別の部分から導出できる。電子メール形式の通信文３２４である場合の一例には、チェックサム内に件名と暗号化時を含むものが挙げられる。この方法では、受信者３１６は、普通文で送信された件名部分が変更されたものであるか、または通信文３２４の到着が過度に遅れていないかを知ることができる。

【０１７８】

テーブル１は、キーサーバ３２０が保有するデータベース３３２のコンテンツのスキーマを示す。resourceIDフィールドは直線形であり、これまで説明してきたのはリソースＩＤ３２８である。ResourceTypeフィールドは、鍵３３０が作成されるアプリケーションタイプの範囲を提供する。例えば、電子メールとインスタントメッセージングが別々の送信者タイプを使用できる。これにより、別々のアプリケーションが、リソースＩＤ３２８の一意性を一致させる必要性から解放される。ResourceＩＤフィールドとResourseTypeフィールドの組み合わせは常に一意である。ResourseKeyは単純に鍵３３０であり、やはり既に説明済みである。鍵３３０が対称鍵である場合は１つのResourceKeyだけが必要である、つまり、同じ鍵３３０が発信者３１４と受信者３１６によって使用される。さらに通信システム３１０の実施形態は非対称鍵を使用することもできる。この場合には、キーサーバ３２０が発信者３１４に暗号化鍵３３０を提供するのであれば、発信者３２４は、この暗号化鍵３３０のためのResourEncryptKeyフィールドを有し、さらに、受信者３１６に提供されるはずの復号鍵３３０を保存するためのResourceDecryptKeyフィールドを有する。発信者３１４が鍵の生成を行う場合には、暗号化鍵および復号鍵３３０の両方、または復

号鍵３３０のみをキーサーバ３２０に送信できる。

【０１７９】

スキーマについての説明をさらに続けるが、KeySizeフィールドはオプションである。１つのサイズの鍵を独占的に使用できるが、これに限定されるものではない。あるユーザは、より大型の鍵が提供する非常に強力な暗号化を希望するかもしれないし、他のユーザは、より小型の鍵が提供する処理負担の軽減を希望するかもしれない。別の考察として、リソースのクラッキングがより強力になるに従って鍵が大型化する傾向にある。この傾向はこれからも継続しそうであり、そのため実施形態は、古い鍵サイズとアップグレード版の鍵サイズに対応するためだけに、異なる鍵サイズを扱う必要があるかもしれない。

【０１８０】

さらにKeyCreatorフィールドもオプションである。キーサーバ３２０のみが鍵３３０を作成する、または常に発信者３１４が鍵３３０を作成する実施形態を利用できる。このフィールドを設けることにより、これらのうちいずれか一方の実施形態が許容される、または鍵３３０が時にキーサーバ３２０によって作成され、時に発信者３１４によって作成される混合配置が許容される。もちろん、ある実施形態にこのような機能を設けることで、どの配置を使用するか指定するため、または特定の発信者３１４に使用されるべき配置を指定するために用いられている手段が制限されることはない。

【０１８１】

大部分の実施形態がKeyOwnerフィールドを設けていることが予測される。発信者３１４は鍵３３０の「所有者」であり、このフィールドの使用の一例として、キーサーバ３２０がスキーマのコンテンツを便利な方法で変更することを促進するものが挙げられる。例えば、企業コンテキスト内で、発信者３１４が、鍵３３０がたった今退出したばかりの受信者３１６に関連付けされることを防止したいと希望する。あるいは、発信者３１４は、受信者３１６が休暇中であることを知ったため、例えば最初に指定された期間よりも長い期間、鍵３３０の公開を許可したいかもしれない。さらにKeyOwnerフィールドは、キーサーバ３２０が、他の参加者からの要求に応答することを許可するが、しかしこれは恐らく適切な場合のみである。例えば、政府機関キーサーバ３２０に、参加者発信者３１４に既に発行されているすべての鍵３３０を凍結し、それ以上鍵を発行しないよう要求できる。または、裁判所が、発信者３１４と受信者３１６の間の陰謀の証拠を調べるべく通信文３２４を復号化するために、鍵３３０の公開を命令するかもしれない。

【０１８２】

KeyOwnerフィールドを故意に設けない、または設けてはいるが単に使用していないということも可能である。キーサーバ３２０は、鍵３３０を「匿名の」発信者３１４、さらには「匿名の」受信者３１６に提供するかもしれない。キーサーバ３２０は、任意の発信者３１４が単に要求を行った場合に、鍵３３０とリソースＩＤ３２８をその最も単純な形式において提供することができ；次に、キーサーバ３２０は、単に要求およびリソースＩＤ３２８の提供を行った任意の受信者３１６に対して、その鍵３３０（または、非対称暗号化を使用している場合にはこれに関連する鍵）を提供できる。あるいは、匿名の発信者３１４が目的の受信者３１６を指定することにより、キーサーバ３２０がその非匿名受信者３１６のみに鍵３３０を公開できるようにする。さらにキーサーバ３２０は、発信者３１４と受信者３１６のいずれか一方、または両方から、アサーション３２２を要求する、またはしないかもしれない。例えば、キーサーバ３２０が、単に有効なアサーション３２２を提供されたことを根拠に、通信を行っている参加者３１２に鍵３３０を提供または公開するかもしれない。

【０１８３】

やはりスキーマの説明を続けると、DateCreatedフィールドは理論的にオプションであるが、その用途は明確であり、また一般的には提供および使用される。スキーマ内のこれ以外のフィールドには、発信者３１４が提出した属性に反応して設定されたものであり、また、テーブル１の記述と、これらがイベントとどのように関連するかについての説明から明白となるはずである。

【０１８４】
通信システム３１０により、３組のビジネスイベントの構成が可能になる。制御イベント３４０（図１２）は、受信者３１６が通信文３２４を見ることができる時間およびその回数を制御するために発信者３１４が実行した動作の組で構成されている。正のイベント３４２（図１３）は、受信者３１６が実行した動作の組で構成されている。また、負のイベント３４４（図１４）は受信者３１６から実行が予想されたが、まだ開始されていない動作の組で構成されている。
【０１８５】
キーサーバ３２０は、発信者３１４が提供した属性３２６に基づいて制御イベント３４０を設定する。次に、キーサーバ３２０は、そのデータベース３３２内の情報、および受信者３１６との通信またはその欠如に基づいて、正のイベント３４２と負のイベント３４４の両方を決定する。
【０１８６】
受信者３１６が通信文３２４を見るためには、復号鍵３３０を認証し、これをキーサーバ３２０から取り出すことを思い出されたし。通信文３２４の発信者３１４はこの鍵３３０の「所有者」であり、各受信者３１６が復号鍵３３０を取り出せる時間と回数についての制御イベント３４０を作成するために、属性３２６を設定できる。この機能を可能にする属性は、キーサーバ３２０がデータベース３３２内に保有しているReleaseAfterフィールド、ExpireOnフィールド、NumReleaseフィールドである。
【０１８７】
図１２は、制御イベント３４０に関連した情報の流れを示すブロック図である。矢印付きの線３５２は、属性３２６が発信者３１４からキーサーバ３２０まで、さらにそのデータベース３３２内へ流れる様子を示す。
【０１８８】
図１３は、正のイベント３４２に関連した情報の流れを示すブロック図である。矢印付きの線３５４は、鍵３３０（ResourceＩＤと受信者のアサーション３２２を含む）の要求が受信者３１６からキーサーバ３２０へ流れ、また、これに関する情報がキーサーバ３２０のデータベース３３２内へ流れる様子を示す。キーサーバ３２０は、所与の受信者３１６が鍵３３０を取り出せる時間およびその回数を記憶する。これは、特定の受信者３１６が特定の時間に実行した動作を示す正のイベント３４２を作成するための支持として機能する。この機能性を可能にする属性は、キーサーバ３２０のデータベース３３２内のLast Releaseフィールド、NumReleasedフィールドである。
【０１８９】
別の矢印付きの線３５６は、キーサーバ３２０が、受信者３１６が復号鍵３３０を取り出せる時間を通知サーバ３４６（キーサーバ３２０と別個に示しているが、この限りではない）に知らせる様子を示す。次に、通知サーバ３４６は、複数の矢印線３５８で示すフォローアップ動作を、複数の利用可能な宛先に向けて発信できる。例えば、通知サーバ３４６がマーケティング部署のシステムに通知し、次に、このシステムがマーケティング代表者に、見込み客（受信者３１６）に電話をしてフォローアップを行うよう警告できる。
【０１９０】
図１４は、負のイベント３４４に関する情報の流れを示すブロック図である。負のイベント３４４に発信するには、キーサーバ３２０のデータベース３３２内のLastReleasedフィールドとExpectedRequestフィールド内の属性を使用する。同図中の仮想矢印線３６０（破線）は、受信者３１６からキーサーバ３２０までの発生しなかった情報の流れと、さらに、ここでも、矢印付き線３５６と複数矢印付き線３５８が、これによって発生するキーサーバ３２０から通知サーバ３４６までの情報の流れを示す。受信者３１６が所与の時間までに鍵３３０の要求に失敗すると、キーサーバ３２０が通知サーバ３４６に信号を発信し、その後、通知サーバ３４６がフォローアップ動作を発信できる。例えば、通知サーバ３４６が顧客コールセンター内のシステムに通知し、次に、このシステムは顧客サービス代表者に、顧客（受信者３１６）に電話をかけて通信文３２４のコンテンツを口頭で伝

えるように警告できる。

【０１９１】

図１５は、本発明の通信システム４１０の実施形態が４つの基本構成要素、つまりトランザクション実行中の参加者４１２（発信元４１４または対象者４１６）、認証オーソリティ４１８、キーサーバ４２０を使用できるブロック図を示す。

【０１９２】

トランザクション実行中の参加者４１２は認証オーソリティ４１８と通信して自己認証を行う。トランザクション実行中の参加者４１２は、認証オーソリティ４１８に指定されたプロトコル（例えば、トランスポートレイヤセキュリティ上のユーザＩＤおよびパスワード、２ファクタ認証、ＰＫＩ証明書を使用するチャレンジ/応答プロトコルなど）を使用する。認証が成功すると、認証オーソリティ４１８がトランザクション実行中の参加者４１２に認証アサーション４２２を発行する。認証オーソリティ４１８がこのアサーション４２２に署名をする（一般に、ＰＫＩ秘密鍵を使用して行う）。アサーション４２２はトランザクション実行中の参加者４１２の証明書；認証オーソリティ４１８の証明書；認証アサーション４２２の有効期間；任意の承認データを含んでおり、これらは、トランザクション実行中の参加者４１２がアサーション４２２の正当な所有者であることを証明するためにキーサーバ４２０によって使用される。この認証データの一例に、その秘密鍵がトランザクション実行中の参加者に知られている一時的な公開鍵がある。トランザクション実行中の参加者４１２は、この秘密鍵を作成し、これに対応する公開鍵が自分に属すると主張して欲しいと、認証プロトコルを介して認証オーソリティ４１８に要求することができる。あるいは、認証オーソリティ４１８は鍵のペアを作成し、秘密鍵をトランザクション実行中の参加者に安全に伝送し、これに関連する公開鍵が、このトランザクション実行中の参加者４１２に属すると主張できる。認証オーソリティ４１８が秘密鍵について知ることがないため、一般には前者の方法が好ましい。

【０１９３】

先述したように、送信元４１４が認証オーソリティ４１８を有し、アサーション４２２を受信する。次に、送信元４１４が、一般にはトランザクション実行中の参加者４２４を１つまたはそれ以上の対象者４１６と通信させたいと望む直前に、キーサーバ４２０と通信する。キーサーバ４２０がトランザクション４２４にトランザクションＩＤ４２８を割り当て、そのトランザクション４２４のための暗号化鍵４３０を作成する。（暗号化鍵４３０は、復号に使用できるものと同一の鍵３４０かもしれないし、そうでないかもしれない。）任意で、送信元４１４が鍵４３０をキーサーバ４２０へ送信して、その鍵４３０をトランザクション４２４と関連付けるよう要求する。キーサーバ４２０が送信元４１４の鍵４３０、トランザクションＩＤ４２８、アサーション４２２のすべてを、キーサーバ４２０が保有するデータベース４３２内に保存する。最後に、送信元４１４が、鍵４３０を使用して、トランザクション４２４内でデータの秘密性と整合性を保護し、このトランザクション４２４を対象者４１６へ送信する。この送信は、認証オーソリティ４１８またはキーサーバ４２０のいずれかを介さない、全く従来の手段によって実施することができる。

【０１９４】

通信システム４１０は、送信元４１４のアサーション４２２を、トランザクション４２４を保護するトランザクションＩＤ４２８および鍵４３０と関連付けることによって起源の否認防止を達成する。これにより、鍵４３０がトランザクション４２４と送信元を「暗号化的に」バインドする。例えば、トランザクション４２４が電子メール内で具現化される実施形態では、その電子メールの起源である送信元４１４が、特定の認証方法で特定の認証オーソリティ４１８において認証されたことを証明するために通信システム４１０を使用する。

【０１９５】

送信元４１４が後にトランザクション４２４の否認を試みた場合、これと競争しようとしている参加者が様々な方法で前進することができる。この参加者が対象者４１６である

場合には、トランザクションＩＤ４２８と推定上の送信元４１４の証明書をキーサーバ４２０に提供して、キーサーバ４２０に、この推定上の送信元４１４が、トランザクションＩＤ４２８に関連したアサーション４２２を提供したことを承認するよう要求する。あるいは、対象者４１６がトランザクションＩＤ４２８のみを提供して、キーサーバ４２０にそのトランザクションＩＤ４２８を受信した送信元４１４が誰であったかを質問してもよい。

【０１９６】

もちろん、送信元４２０またはこれ以外の参加者は、対象者４１６がトランザクション４２４の起源を妥当に確認したことをまだ簡単に認めたくないかもしれない。しかし、問題解決側の参加者はトランザクション実行中の参加者４１２（送信元４１４または対象者４１６）以外の者、例えば仲裁者、裁判所、または銀行である可能性もある。ここで、次にこの参加者がトランザクションＩＤ４２８をキーサーバ４２０に提供し、そのトランザクションＩＤ４２８の発行のためにアサーション４２２を提供した送信元４１４は誰であるか、また、トランザクション４２４を復号化して、その整合性を検証するのはどの鍵４３０であるかについて通知される。鍵４３０がトランザクション４２４を復号化し、その整合性を検証する場合には、起源についての質問は解決する。あるいは、恐らくより一般的には、この参加者がトランザクション４２４とトランザクションＩＤ４２８の両方をキーサーバ４２０に提供することができ、キーサーバ４２０が、トランザクション４２４を復号化して、その整合性を検証したのがその鍵４３０であるか否かを判断することができ、その後、キーサーバ４２０がその旨を通知することができる。ここで、推定上の送信元４１４の証明書もキーサーバ４２０に提供でき、その後、キーサーバ４２０は、その推定上の送信元４１４がトランザクションＩＤ４２８に関連したアサーション４２２を提供したか否かを確認する（つまり、イエス、ノーで応答する）ことができる。

【０１９７】

さらに先述したように、トランザクション対象者４１６は、認証オーソリティ４１８（しかし、送信元４１４が使用したものと同一である必要はない）を有し、さらにアサーション４２２を受信する。次に、対象者４１６は、トランザクション４２４内のデータを解読して、その整合性を実証するために、キーサーバ４２０から復号鍵３３０を取り出す必要がある。キーサーバ４２０は、このために鍵３３０を公開する前に、対象者４１６のアサーション４２２を保存し、トランザクションＩＤ４２８との関連付けを行う。

【０１９８】

このように、通信システム４１０は、対象者４１６のアサーション４２２をトランザクションＩＤ４２８、トランザクション４２４を保護している鍵３３０と関連付けすることで、受信の否認防止を達成する。例えば、トランザクション４２４が電子メール内で具現化される実施形態では、対象者４１６がその電子メールを受信および開封し、また特定の認証方法により、特定の認証オーソリティ４１８において認証されたことを証明するために、通信システム４１０を使用することができる。

【０１９９】

後に対象者４１６がトランザクション４２４の受信を否認しようと試みた場合には、トランザクションＩＤ４２８と対象者４１６の証明書をキーサーバ４２０に提供して、対象者４１６が鍵４３０を要求し、対象者４１６が有効なアサーション４２２をその要求の一部分として提出し、そしてその時に対象者４１６が鍵の提供を受けたことを確認するよう要求することで、問題は簡単に解決する。これにより、対象者４１６が、トランザクション４２４を開けるために実際に鍵４３０を使用したかどうかの問題のみが残る。しかし上述したように、トランザクション実行中の参加者４１２からの要求は、一般にソフトウェア（例えば、図３のソフトウェアモジュール２６）によって扱われる。そのため、少なくとも対象者４１６に関しては、鍵４３０の受信とその使用を容易に自動化し、両方を同時に実行するようにすることができる。これにより、鍵４３０を受信した対象者４１６が、同じ鍵４３０を使用してトランザクション４２４を開いたであろうという、解決が非常に困難な推測ができる。

【０２００】
キーサーバ４２０は、送信元４１４およびすべての対象者４１６のアサーション４２２をそのデータベース４３２内に永久に保存する。通信システム４１０がこれらのアサーション４２２をトランザクションＩＤ４２８と関連付けるため、データベース４３２を使用して、トランザクション４２４の起源であるイベントと、各トランザクション４２４の受信を再構成できる。これは、総合的な監査システムの基本として機能する。
【０２０１】
図１６は、通信システム４１０が、後の否認防止および監査目的のために、データベース４３２内でデータを確立できる適切なプロセス４５０を示すフローチャートである。プロセス４５０はステップ４５２にて開始するが、ここで、認証オーソリティ４１８とキーサーバ４２０の存在が推測され、また、送信元４１４は、認証オーソリティ４１８からアサーション４２２を既に取得している。
【０２０２】
ステップ４５４では、キーサーバ４２０へ要求が送信される。多くの実施形態において、この要求は送信元４１４が直接行うであろうと予測されるが、しかし、技術上の理由からして送信元４１４の代理で仲裁者がこれを行なうこともできる（もちろん、これを許可しないための優れたポリシー上の理由があってよい）。この要求には、送信元４１４のアサーション４２２、予想されるトランザクション４２４に関する情報が含まれる（例えば表１参照）。先述したように、このような情報は少なくとも対象者４１６を証明し、さらに、このトランザクションについて許可される復号鍵４３０の公開回数および個数を設定することができる。送信元４１４が復号鍵４３０を提供した場合には、要求にさらにこの復号鍵４３０が含まれる。
【０２０３】
ステップ４５６では、キーサーバ４２０が、送信元４１４のアサーション４２２有効であるか否か（また、少なくとも最小のこれ以外の情報、例えば少なくとも１つの対象者４１６が証明されているといった情報が提供されているか否か）が判断される。有効でない場合には、ステップ４５８にて、キーサーバ４２０が、特定の実施形態にとって適切と思われる処置を実行する。判断の失敗は悪意のないエラーによって起こる可能性があるため、多くの実施形態では要求の修正を少なくとも１回は許可すると予想される。もちろん、キーサーバ４２０は、試みられた要求をすべてデータベース４３２に記録している。
【０２０４】
ステップ４５６で、プロセス４５０が継続すべきであると決定された場合、ステップ４６０にて、キーサーバ４２０がトランザクションＩＤ４２８（図中では“ｔ－ｉｄ”）を割り当て、これを送信元４１４のアサーション４２２、復号鍵４３０と共にデータベース４３２に保存する。設計または構成の問題として、暗号化鍵４３０と復号鍵４３０は同一であっても、同一でなくてもよい点を思い出されたし。これらの鍵が異なる場合、キーサーバ４２０は、所望であればその両方を保存できる。
【０２０５】
ステップ４６２にて、キーサーバ４２０が、トランザクションＩＤ４２８と、さらに暗号化鍵４３０を提供するのであればこれも一緒に提供することで要求に応答する。
【０２０６】
図１６では、トランザクション４２４を暗号化、送信、受信するためのステップを示していない。簡略化の目的で、ここでは、これらをそのラベルが示すとおりに処理し、それ以降の詳細な説明を以下に示す。
【０２０７】
ステップ４６４では、対象者４１６がトランザクション４２４を受信し、認証オーソリティ４１８からアサーション４２４を既に取得していると仮定する。このステップにはさらに、キーサーバ４２０による別の要求の受信が含まれる。多くの実施形態では、この要求が対象者４１６によっても直接行われているが、しかし、技術上の理由からして仲裁者がこの要求を行うことも可能である。この要求には、トランザクション４２４および対象

者４１６のアサーションと共に提供されたトランザクションＩＤ４２８も含まれる。
【０２０８】
ステップ４６６では、キーサーバ４２０が、対象者４１６のアサーション４２２が有効であるか否か（また、トランザクションＩＤ４２８が、現在対象者４１６が見ることを許可されているトランザクション４２４用のものであるか否か）を判断する。有効でない場合は、ステップ４６８にて、キーサーバ４２０が適切と思われる処置を実行する。ここでも、判断の失敗は悪意のないエラーによって起こる可能性があるため、多くの実施形態では要求の修正を少なくとも１回は許可すると予想される。しかし、キーサーバ４２０はここでも、試みの要求をすべてデータベース４３２に保存できる。
【０２０９】
ステップ４６６にて、プロセス４５０が継続すべきと判断された場合、ステップ４７０にて、キーサーバ４２０が対象者４１６のアサーション４２２をデータベースに保存され、トランザクションＩＤ４２８、対象者４１６の証明書と関連付けされる。
【０２１０】
ステップ４７２にて、キーサーバ４２０が、トランザクションＩＤ４２８に関連して保存してあった復号鍵４３０を取り出し、さらに、この復号鍵４３０を提供することでこの要求に応じる。
【０２１１】
最後に、ステップ４７４にて、プロセス４５０が終了する。この状態で、否認防止および監査の目的からデータベース４３２内にデータが確立されている。恐らく、しかし非常に高い確率で、通信システム４１０が対象者４１６について、要求/応答処理を自動化するソフトウェア（例えば、図３のソフトウェアモジュール２６）を使用した場合、トランザクション４２４が復号化および表示される。
【０２１２】
上述したように、暗号化鍵４３０を使用する動作は、トランザクション４２４と送信元４１４を「暗号的に」バインドする。しかし、次に、これとは別の手法、およびこれら手法の適切な応用形、さらに代表的な例証について説明する。
【０２１３】
公開/秘密鍵システムを採用している場合、送信元４１４は、キーサーバ４２０に提出するアサーション４２２内に公開鍵（復号鍵４３０）を含めることができる。次に、送信元４１４が、関連の秘密鍵（暗号化鍵４３０）を使用してトランザクション４２４を暗号化することで、トランザクション４２４に効率的に「署名」するため、トランザクション４２４を否認することはできない。これは、ＰＫＩシステムが否認防止を達成する方法と概念上類似するが、この手法ではキーサーバ４２０を採用し、追加の恩恵の取得を許可している。
【０２１４】
暗号化と復号化の両方に１つの鍵を使用する場合には、送信元４１４とキーサーバ４２０が協働して、送信元４１４から送信されたトランザクション４２４を証明するための「シール」を作成できる。この手法には多数の応用形が可能であり、現在発明者が好ましいとする応用形を以下に示す。この中の多くの特徴はオプションである。
【０２１５】
ここでは、前述したように、送信元４１４がキーサーバ４２０からトランザクションＩＤ４２８と暗号化キー４３０を要求し、キーサーバ４２０がこれらと、鍵作成タイムスタンプ、送信元４１４の証明書を提供する。［一般にこの証明書は電子メールアドレスであるが、これに限定はされない。例えば、キーサーバ４２０が、送信元４１４を証明するためにその顧客番号を使用してもよい。多くの場合、送信元４１４は「その」証明を十分よく知っているが、キーサーバ４２０からこれを「オウム返し」し、その完全に同一のコピーを次のステージに使用することで、起こり得るエラーを回避できる。］次に、送信元４１４がトランザクション４２４のためのデータ、トランザクションＩＤ４２８、タイムスタンプ、証明書を組み合わせてハッシュを生成する。送信元４１４がこのハッシュを「ソ

ルト」、つまりランダムに生成された数で暗号化し、この暗号化されたハッシュがシールになる。

【０２１６】

次に、送信元４１４がトランザクション４２４用のデータを暗号化し、これが対象者４１６に実際に送信されるものとなる。ここで、送信元４１４がシールとソルトを作成する点に留意すること。送信元４１４はシールをキーサーバ４２０に送信するが、トランザクションまたはソルトは送信しない。送信元４１４は各対象者４１６に、暗号化され、ソルトを含むが（好ましくは）シールを含まないトランザクション４２４を送信する。

【０２１７】

対象者４１６はこのトランザクションを受信すると、トランザクションＩＤ４２８とそのアサーション４２２をキーサーバ４２０に送信する。すべて整っていれば、キーサーバ４２０が復号鍵４３０、鍵作成タイムスタンプ、送信元４１４の証明書、シールを返送する。対象者４１６は、この復号鍵４３０トランザクション４２４を復号化し、ソルトにアクセスし、次に、送信元４１４がシール作成のために使用するプロセスを再度作成する。対象者４１６はトランザクション４２４用のデータ、トランザクションＩＤ４２８、タイムスタンプ、証明書を組み合わせてハッシュを生成する。続いて、このハッシュをソルトで暗号化する。その結果が、送信元４１４が作成し、現在キーサーバ４２０から提供されているシールと一致した場合には、送信元４１４はトランザクション４２４を否認できない。さらにこれにより、対象者４１６がトランザクション４２４と接続し、復号鍵４３０を使ってこれを暗号化し、後にこのトランザクション４２４が送信元４１４から送信されたものであると主張されることを防止できる。

【０２１８】

図１７は、データベース４３２に確立されたデータを、送信元４１４が試みた否認に対抗するために使用する適切なプロセス４８０を示すフローチャートである。

【０２１９】

ステップ４８２にて、プロセス４８０が開始する。データはトランザクション４２４として既にデータベース４３２内に確立されていると仮定する。

【０２２０】

ステップ４８４にて、キーサーバ４２０、またはこれ以外の、少なくともデータベース４３２への読み出しアクセスを有するシステムに対して、送信元４１４を証明する要求が行われる。このような要求は、潜在的に対象者４１６、またはこのトランザクション４２４を何らかの方法で証明できる別の参加者から出される（もちろん、所望であればポリシーによってこれに制限を課すこともできる）。最も一般的には、トランザクションＩＤ４２８によって証明を行われるが、別のデータを使用して、データベース４３２を検索し、トランザクションＩＤ４２８を決定することができる（例えば、鍵４３０、アサーション４２２、実際のトランザクション実行中の参加者４１２証明情報、トランザクション４２４送信または受信回数など）。

【０２２１】

ステップ４８６にて、送信元４１４が最初に提供し、トランザクションＩＤ４２８に関連してこれまでずっと保存されていたアサーション４２２を検査することで、送信元４１４の証明が決定される。

【０２２２】

ステップ４８８にて、送信元４１４を検証することによりこの要求への返答が為される。しかし、この返答と実証の性質は多様な形式であってよい。例えば、この返答は単純に送信元４１４を証明するものであってもよい。あるいは、要求に注意すべき送信元４１４が含まれている場合、応答に「はい」または「いいえ」による返答のみを含め、実際の証明を提供しないようにしてもよい。恐らく適切な状況においてのみ（例えば裁判所の命令）、応答にトランザクション４２４用の復号鍵４３０を含めることもできる。または、やはり適切な状況においてのみであるが、要求に暗号化したトランザクション４２４を含めて、返答に復号化したトランザクション４２４を含めることも可能である。

【０２２３】
最後に、ステップ４９０にてプロセス４８０が終了する。送信元４１４はそれ以上、トランザクション４２４をもっともらしく否認することはできない。
【０２２４】
図１８は、データベース４３２内に確立されたデータを、対象者４１６によって試みられた否認に対抗するべく使用するための、適切なプロセス５００を示すフローチャートである。
【０２２５】
ステップ５０２において、プロセス５００が開始する。トランザクション４２４のためにデータが既にデータベース４３２内に確立されていると仮定する。
【０２２６】
ステップ５０４において、その対象者４１６がトランザクション４２４を受信した旨を証明する要求が、キーサーバ４２０、または、少なくともデータベース４３２への読み出しアクセスを有する別のシステムに対して行われる。このような要求は送信元４１４、または対象のトランザクション４２４と推測される対象者４１６を同じ方法で証明できる他の参加者（ポリシー考察の対象）から出される。最も一般的には、証明はトランザクションＩＤ４２８によるものであるが、やはりここでも、データベース４３２の検索に、さらにこれ以外のデータを潜在的に使用することが可能である。
【０２２７】
ステップ５０６において、対象者４１６がトランザクション４２４を受信したか、これを特定の回数受信したか、またはこれを１つまたはそれ以上の特定回数受信したか否かを、対象者アサーション４２２と、トランザクションＩＤ４２８に関連して保存されていたこれ以外のデータ（例えば表１を参照）とを検査することによって判断する。対象者４１６のアサーション４２２を含んでいない場合、または、含んではいるが、他の基準が一致しない場合には、ステップ５０８において、対象者に適切な返答が行われる。
【０２２８】
あるいは、データベース４３２が、対象者４１６のアサーション４２２がトランザクションＩＤ４２８に関連して存在することを反映し、さらに、他の任意の基準が一致する場合には、ステップ５１０にて、この場合に要求に対して適切な返答が行われる。
【０２２９】
返答と、実証の性質は多様な形式であってよいと留意すべきである。例えば、返答は、対象者４１６が対象のトランザクション４２４用の復号鍵４３０を要求し、これが提供されたことを単純に実証するものであってよい。あるいは、その要求が行われ、実施形態が許可した場合、返答は、対象者４１６に復号鍵４３０が何回提供されたか、そしていつ提供されたかを知らせるものとなる。また、この返答は、恐らく適切な状況においてのみ、やはり復号鍵４３０を含むこともできる。または、この要求は、ここでもやはり恐らく適切な状況においてのみ、暗号化したトランザクション４２４を含むことができる。
【０２３０】
最後に、ステップ５１２において、プロセス５００が終了する。この時点では、対象者４１６はトランザクション４２４をもっともらしく否認することはできない。
【０２３１】
送信元４１４と対象者４１６の間でのトランザクション４２４の通過を監査する場合には、データベース４３２にはこれに適した長いデータが含まれる。このようなデータがタイムスタンプと共に保存され、データベース４３２内に保存され続ける限り、監査要求への応答は、ルックアップとレポート生成の直接的なタスクであるべきである。
【０２３２】
これまで様々な実施形態について説明してきたが、これらが限定的ではなく、例示のみの方法で提示されたことを理解すべきである。したがって、好ましい実施形態の広がりおよび範囲は上述の例示的実施形態のいずれによっても制限されるべきでないが、添付の特許請求項およびその等価物に従ってのみ定義されるべきである。

【０２３３】
産業上の利用可能性
本明細書中で、セキュリティサーバシステム２１０、通信システム３１０、通信システム４１０を例にとって例証された本発明は、インターネットのような最新のネットワーク環境での使用に非常に適している。
【０２３４】
特にインターネットは、主として無制御および無規制のワイルドな未知の領域であるため、その使用には注意が必要であると広く考えられてきた。さらに、変化が迅速で、理解に限界があり、また、テクノロジーの実現が不十分であれば、恐らく最も精通した適任者でさえも危険にさらされてしまう環境としても広く考えられてきた。こうした考えが実際にどの程度正しいかはさておき、インターネット上での通信のセキュリティに関して言えば、その秘密性が危険にさらされ、その危険は増大していることは否定できない。
【０２３５】
本発明はメッセージを保護することで、秘密性、整合性、またはその両方を達成し；キーサーバイベントを使用してビジネスプロセスを実現し；そして、認証アサーションとキーサーバを使用して否認防止および監査を実現する。
【０２３６】
本発明は、通信文（例えば、メッセージやトランザクション）を送信する参加者と、このような通信文を受信する参加者の両方が容易に使用できる。これらの通信を行っている参加者は、自分が使用している何らかのハードウェア、例えばコンピュータ、インターネット機器などで、単純なソフトウェアモジュールを実行できる。
【０２３７】
本発明は、従来技術のシステムに伴うユーザにとっての複雑性を著しく克服する。主要なセキュリティ要素には、キーサーバに適したあらゆる手段により認証されたあらゆるユーザが、会話鍵を使用できるようにするものが挙げられる。これは単純なパスワード、デジタル証明書、生体認証などであってよい。この簡略化は、主流である最新の公開/秘密鍵スキームに対抗する目立ったものであり、この場合、送信者と受信者は互いの証明された公開鍵のディレクトリに頼らなければならず、すべての参加者がこのようなディレクトリに事前登録され、表示されている必要がある（ディレクトリは複数。これは、このようなシステムの競合オペレータが多数存在するためである）。さらに現在主流のスキームは、その初期設定の煩わしさ以上の理由で好まれていない。このスキームは、多くの場合数百桁もある複雑な鍵を使用するので保存することができず、このような複雑な事前に保存されている鍵にアクセスする何らかの手段を備えたシステム以外に使用できない。例えば、公共キオスクでの公開/秘密鍵システムの唯一実用的な使用方法は、ユーザが鍵保存装置用のハードウェア補助品、例えばスマートカードを採用するというものである。本発明の実施形態は、ハードウェア補助品が不要であり（場合により使用することは可能）、そして、ユーザを少しの事前設定システムのみに必ずしも「束縛」する必要がない。
【０２３８】
本発明はまた、既存のインターネット環境において容易かつ経済的に実現可能である。追加的な物を採用することはほとんどないか、全くない。セキュリティサーバまたはキーサーバを別のサーバハードウェアに組み込むことさえも可能である。本発明の実施形態の構成も、現在ソフトウェアおよび通信技術を実践している技術者の範囲内にある。本発明はさらに、その動作環境である、基礎となるインターネット環境に大きな変更を加える必要がない点に注目すべきである。送信者と受信者の間に通信が発生し、本質的に従来のものと同様に扱われ、従来の経路をとおり、本質的に標準の機材を使用する。
【０２３９】
本発明はまた、企業および他の組織が共同の通信を提供する増え続ける必要性を特に検討する。これを例証するためにセキュリティサーバシステム２１０を用いることにより、電子メール、インスタントメッセージング、ビデオ会議、マルチパーティ文書編集、これに関しては、メッセージヘッダ２２２とメッセージコンテンツ２２４を含む実質的にあら

ゆるメッセージ２１８をどのように安全化できるかについて説明してきた。潜在的に多数のコラボレーション参加者２１２によって会話を実施することができ、この会話では、関連するテーマについての多くのメッセージ２１８が安全かつ効率的に交換される。あるいは、コラボレーション参加者２１２は、このような共同会話で相互にやり取りするメッセージ２１８の送信元と宛先であってよい。セキュリティサーバシステム２１０は、会話の最中にレベルの高いセキュリティを維持し、メッセージコンテンツ２２４と、任意でさらにメッセージヘッダ２２２を安全化する。さらに、会話に参加・退出するコラボレーション参加者２１２を効率的に扱うことで、従来技術のシステムが果たせなかった基準化機能を提供することができる。

【０２４０】

本明細書中では、通信システム３１０を、キーサーバイベントを使用してビジネスプロセスを実現するためにどれほど適しているかを示す例として使い、本発明を説明してきた。説明したように、本発明は、通信文３２４の発信者３１４によって、または実際の発信者３１４に代わってこれらの設定を行う別の参加者によって使用される制御イベント３４０の組を使用する。次に、通信文３２４は暗号化された状態で１人またはそれ以上の受信者３１６へ送信される。受信者３１６が通信文３２４、制御イベント３４０への件名の表示を行おうとした場合に、正のイベントが記載される。あるいは、一人またはそれ以上の受信者３１６が表示の試みにさえ失敗したために、または、表示許可の前に行われる制御イベント３４０による確認に失敗したために、通信文３２４を見ることができなかった場合には、負のイベント３４４が記載される。

【０２４１】

正のイベント３４２と負のイベント３４４を再検査する能力、またはこれらに基づいて動作をトリガする機能は相当に実用的である。例えば、受信者３１６との通信を所望している、ビジネスおよび他のエンティティを代表する発信者３１４が、制御イベント３４０を使って、通信文３２４を最初にいつ見ることができるか、どのような頻度で見ることができるか、またいつまで見ることができるのかを指定できる。発信者３１４と他の適当な参加者は、正のイベント３４２に基づき、各受信者３１６がその通信文３２４をいつ、何回見たかを判断することができる。あるいは、発信者３１４と他の適当な参加者は、負のイベント３４２に基づいて、所与の受信者３１６による通信文３２４表示の試みが全く行われていない、または受信者３１６による通信文３２４表示の試みの失敗が全くないと判断することができる。

【０２４２】

再び背景技術部分の、金融ブローカー企業が、顧客が追加証拠金の通知を受け取ったかどうかを判断する必要がある場合の例に戻ると、従来技術のシステムが果たせない部分で本発明が容易に成果を発揮する様子を見ることができる。顧客（受信者３１６）は、通知（通信文３２４、例えば電子メール）を見る際に正のイベント３４２を自動的に作成しているので、通知の受信を確認上知らせる手間を負うことがない。さらに、ブローカー企業（発信者３１４）は、顧客が通知を読んだ旨の返答を迅速に受けることができ、それ以上の不必要な行動をとる手間を追うことがない。あるいは、顧客は、設定された期間中に通知の表示に失敗した際に負のイベント３４２を自動的に作成するので（制御イベント３４０）、ブローカー企業は適切な行動を起すことができる。

【０２４３】

本明細書中では、通信システム４１０を、認証アサーションとキーサーバを使用して否認防止および監査を実現するためにどれだけ適しているかを示す例として使い、本発明を例証してきた。説明したように、従来技術の手法は、デジタル通信の使用に伴うすべての懸念を検討していない。特に、トランザクションの否認防止および監査に伴う２つの特に厄介な問題について検討していない。

【０２４４】

本発明は、トランザクション実行中の参加者、トランザクション送信元、対象者に対して大いに透過的である。トランザクション実行中の参加者の認証された証明書を使用して

、両方の参加者からの否認防止を実現する。さらに、トランザクション実行中の参加者からの情報、またはトランザクション実行中の参加者の完全な認証アサーションを継続的に保存することにより、同じシステムを用いて否認防止と監査の両方を提供できる。これに対して、既存の技術（例えば、公開鍵インフラストラクチャ、ＰＫＩ）では、ユーザに秘密鍵を管理させ、これを署名生成のために活発に使用させる。さらに、トランザクションの検証を必要とするある参加者はトランザクション署名者のデジタル証明書のコピーを取得するか、あるいはトランザクション署名者のデジタル証明書を取り出さなくてはならない。さらに、このような既存の技術は、否認防止と監査の両方に有効な１つのサービスの提供を行わない。

【０２４５】

本発明に依然としてＰＫＩを組み込むことはできるが、ＰＫＩが必要なわけではない。トランザクション送信元、対象者、またはその両方が、ＰＫＩを含む任意の方法を使用して、起源と受信の否認防止を行える。さらに、トランザクション送信元が用いる方法は、トランザクション対象者が用いる方法と同一であっても、違うものでもよい。これに対して、ＰＫＩに基づく技術では、すべての参加者（トランザクション送信者および対象者）が信頼するインフラストラクチャを使用する必要がある。さらに、非ＰＫＩ技術（例えば、トランザクションログをデータベースに保存する）はＰＫＩとは完全に異なる機構を使用し、ＰＫＩと相互動作することがない。

【０２４６】

本発明は、様々な度合いの強度を提供できる。これは、トランザクション実行中の参加者の認証に伴う強度の度合いに関連する。認証の強度を増すことで（例えば、uswerＩＤ/passwordから２ファクタ認証までにかけて）、トランザクション実行中の参加者が、否認防止強度をダイナミックかつ自動的に増加する。これに対し、多くの従来技術では、否認防止強度のレベルは１つしかない。例えば、ＰＫＩでは、否認防止の強度は、基本である証明書の確実性のレベルに等しい。ここでは、参加者は、異なる証明書を使用して、異なるレベルの確実性を得ることでしか強度の変更を行えない。

【０２４７】

本発明はまた、特定の信用規則を強化することができる。これにより、ビジネス関係に追随した柔軟な信用規則が可能になる。例えば、ある組織が、各トランザクション実行中の参加者を認証する規則を強化することにより、自己の認証アサーションのみを信頼する規則を強化できる。または、組織は、自己のキーサーバを所有および管理する規則を強化することにより、自己の監査サーバのみを信頼する規則を強化することが可能である。これに対して、多くの従来技術は、否認防止と監査のための、柔軟性のない信頼規則しか提供できない。ここで再びＰＫＩを例に用いると、これに基づいたシステムにおいて、取引の証明を行う参加者は、署名者の証明書を信頼するしかない。従来技術による非ＰＫＩに基づくシステムでは、証明者は、トランザクションログを維持するシステムを信頼するしかない。

【０２４８】

上述の、およびそれ以外の理由から、本発明は産業に幅広く適用されると予測され、かつ、本発明の商業的実用性は広範囲にわたり、長期間継続するであろうと予測される。

【０２４９】

テーブル１は、　キーサーバが管理するデータベースのコンテンツのスキーマである。

No	フィールド	タイプ	記述
1.	ResourceID	ストリング	この通信に割り当てた一意ＩＤ
2.	ResourceType	整数	アプリケーションタイプ (例えば、電子メール、インスタントメッセージングなど)
3.	ResourceKey	バイナリ	暗号鍵
4.	KeySize	整数	鍵のサイズ
5.	KeyCreator	ストリング	鍵作成者のＩＤ
6.	KeyOwner	ストリング	鍵所有者のＩＤ
7.	DateCreated	日付	鍵作成日付および時間
8.	ReleaseAfter	日付	鍵を公開できるようになる日付および時間（各受信者毎）
9.	ExpireOn	日付	鍵が公開不能になる日付および時間（各受信者毎）
10.	LastRelease	日付	最後に鍵が公開された日付および時間（各受信者毎）
11.	ExpectedRequest	日付	鍵の要求が予想される日付および時間（各受信者毎）
12.	NumReleased	整数	鍵が公開された回数（各受信者毎）
13.	NumReleases	整数	鍵を公開できる回数（各受信者毎）

テーブル１

【図面の簡単な説明】

【０２５０】

【図１】例証的なセキュア電子メールシステムに関係する情報の総体的な流れを示す略概外観図である。

【図２ａ】図１の実施例で使用できる電子メールフォームを示し、従来の送信フォームである。

【図２ｂ】図１の実施例で使用できる電子メールフォームを示し、図１の実施形態と協働するよう変更した送信フォームである。

【図２ｃ】図１の実施例で使用できる電子メールフォームを示し、従来の受信フォームである。

【図３】図１の送信および受信ユニットで使用できるソフトウェアモジュールを示すブロック図である。

【図４】セキュア電子メールが受信されたものか、受信されたものかを判断するためのソフトウェアモジュールの手法を様式的に示すブロック図である。

【図５】図１のセキュリティサーバが使用できるテーブルを含むリレーショナルデータベースの図である。

【図６ａ】ここで使用するフィールドの記述を備えた図５のテーブルであり、ユーザデータのテーブルである。

【図６ｂ】ここで使用するフィールドの記述を備えた図５のテーブルであり、メッセージデータのテーブルである。

【図６ｃ】ここで使用するフィールドの記述を備えた図５のテーブルであり、宛先データ

のテーブルである。
【図６ｄ】ここで使用するフィールドの記述を備えた図５のテーブルであり、ユーザ用のエイリアスデータのテーブルである。
【図６ｅ】ここで使用するフィールドの記述を備えた図５のテーブルであり、図６ｅはオプションの配布リストデータのテーブルである。
【図６ｆ】ここで使用するフィールドの記述を備えた図５のテーブルであり、こうした配布リストのメンバーデータのテーブルである。
【図７】図１の実施形態で使用できる暗号化プロセスを示すフローチャートである。
【図８】図１の実施形態で使用できる復号化プロセスを示すフローチャートである。
【図９】安全なコラボレーションおよび鍵交換のための一般的な実施形態の主要構成要素を示す略ブロック図である。
【図１０】図９の一般的形態における典型的なメッセージの流れを示す概略ブロック図である。
【図１１】４つの基本構成要素を使用するプロセスイベントを決定できる通信システムのブロック図である。
【図１２】制御イベントに関連した情報の流れを示すブロック図である。
【図１３】正のイベントに関連した情報の流れを示すブロック図である。
【図１４】負のイベントに関連した情報の流れを示すブロック図である。
【図１５】通信システムの別の実施形態が４つの基本構成要素を使用する様子を示すブロック図である。
【図１６】図１５の通信システムが、後の否認防止および監査目的のために、データベース内にデータを確立するために使用できる、適切なプロセスを示すフローチャートである。
【図１７】送信元による否認の試みに対抗するために、データベース内に確立されたデータを使用できる適切なプロセスを示すフローチャートである。
【図１８】対象者による否認の試みに対抗するために、データベース内に確立されたデータを使用できる適切なプロセスを示すフローチャートである。

【図１】

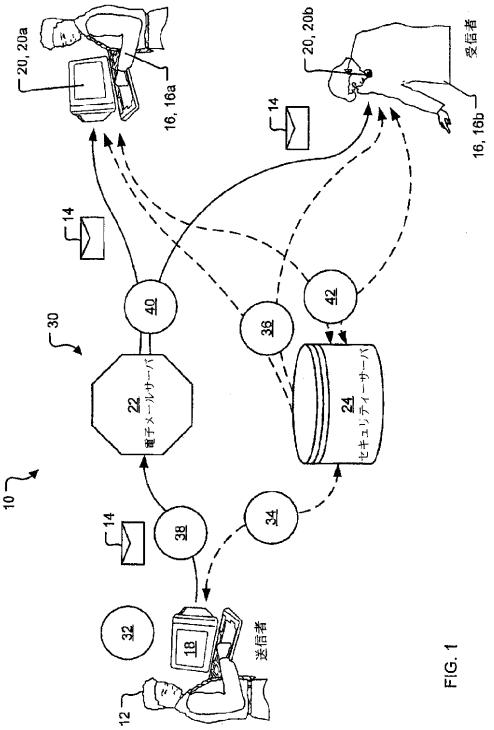


FIG. 1

【図２ａ】

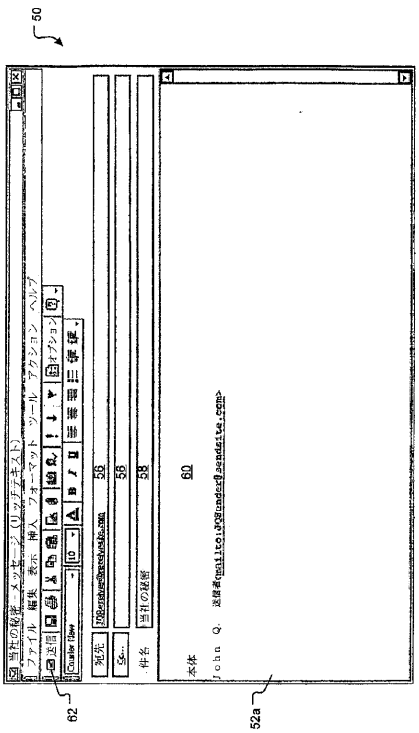


FIG. 2a

【図２ｂ】

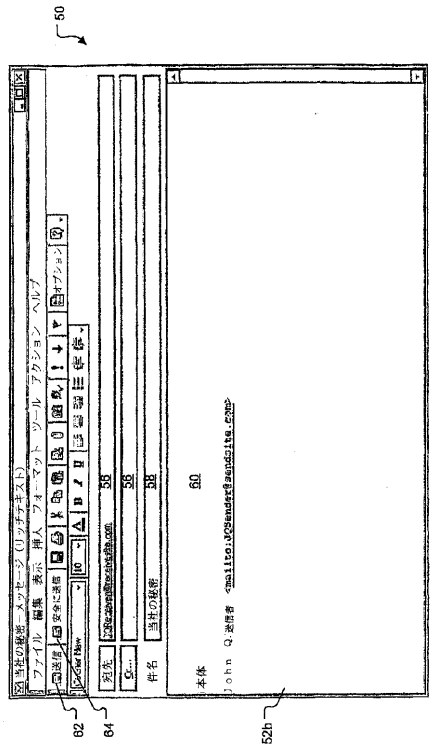


FIG. 2b

【図２ｃ】

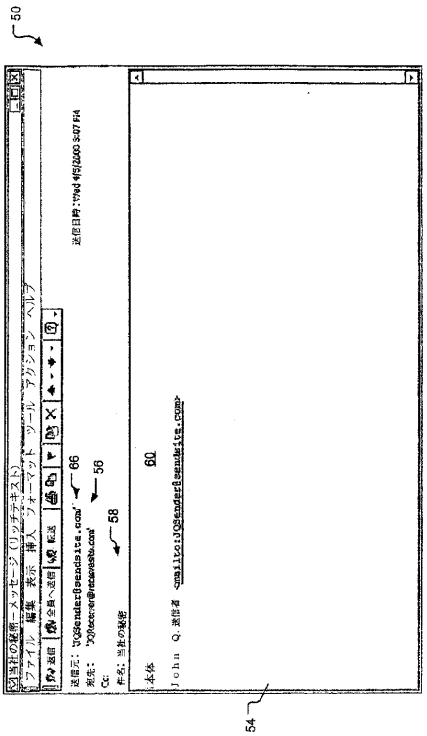


FIG. 2c

【図３】

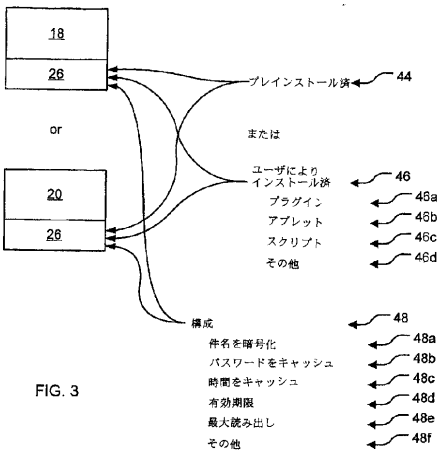


FIG. 3

【図４】

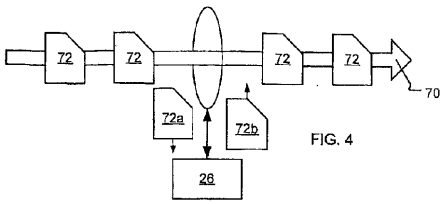


FIG. 4

【図５】

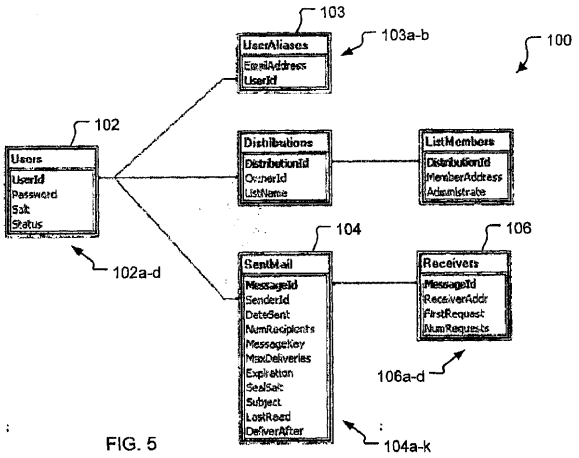


FIG. 5

【図６ａ】

FIG. 6a: ベーシックユーザ情報テーブル（Ｕｓｅｒｓ）

カラム名	タイプ	記述
UserId	整数	内部ユーザ識別子
Password	行	ユーザのパスワードのハッシュ
Salt	整数	ハッシュ前にパスワードに追加されたソルト
Status	バーチャー	ユーザの最新登録/使用状況

【図６ｂ】

FIG. 6b: 送信済メッセージテーブル（ＳｅｎｔＭａｉｌ）

カラム名	タイプ	記述
MessageId	整数	一意電子メール識別子
SenderId	整数	インターネット送信者識別子（ユーザへの参照）
DateSent	日付	入力された時間および日付記録
NumRecipients	整数	メッセージが送信された受信ユーザ数
MessageKey	行	メッセージの暗号化/復号化に使用した鍵
MaxDeliveries	整数	各ユーザに鍵が送信される最大回数
Expiration	日付	メッセージがそれ以降配送されない時間
SealSalt	整数	シールを形成するためにハッシュに追加された秘密ソルト
Subject	バーチャー	メッセージの件名
LastRead	日付	最後にメッセージが読まれた日付
DeliverAfter	日付	メッセージを読めるようになる日付

【図６ｃ】

FIG. 6c: 電子メール宛先（Ｒｅｃｅｉｖｅｒｓ）

カラム名	タイプ	記述
MessageId	整数	電子メールメッセージの識別子（ＳｅｎｔＭａｉｌを参照）
ReceiverAddr	整数	受信者の電子メールアドレス
FirstRequest	日付	受信者が最初に読み出しを試みる時間
NumRequests	整数	受信者が読み出しを要求した回数

【図６ｄ】

FIG. 6d: 別のユーザ識別子（ＵｓｅｒＡｌｉａｓｅｓ）

カラム名	タイプ	記述
EmailAddress	バーチャー	別の電子メールアドレス
UserId	整数	Ｕｓｅｓテーブルへの参照

【図６ｅ】

FIG. 6e: 配布リストマスター（Ｄｉｓｔｒｉｂｕｔｉｏｎｓ）

カラム名	タイプ	記述
DistributionId	整数	一意リスト識別子
OwnerId	整数	リストの所有ユーザ（Ｕｓｅｒｓへの参照）
ListName	バーチャー	このリストの電子メールアドレス

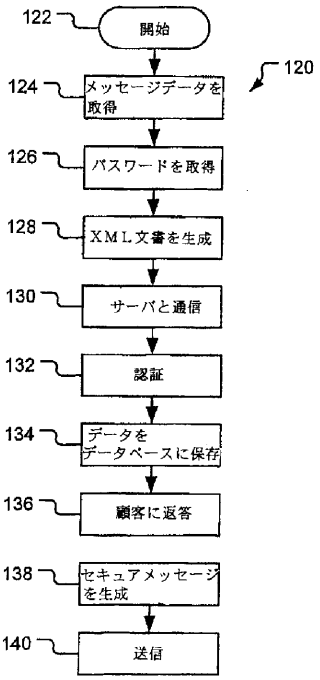
【図６ｆ】

FIG. 6f: 配布リストメンバー（ＬｉｓｔＭｅｍｂｅｒｓ）

カラム名	タイプ	記述
DistributionId	整数	Ｄｉｓｔｒｉｂｕｔｉｏｎｓへの参照
MemberAddress	バーチャー	リスト上のエイリアス名
Administrate	チャー	Ｙ＝メンバーはリストを更新できる　Ｎ＝できない

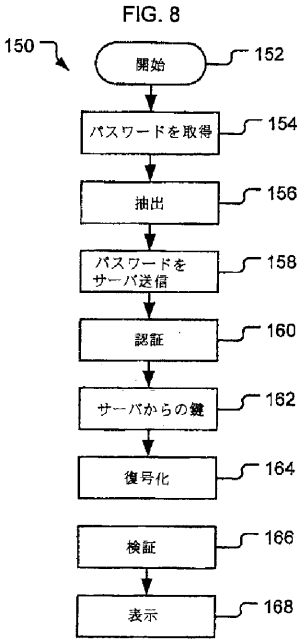
【図７】

FIG. 7



【図８】

FIG. 8



【図９】

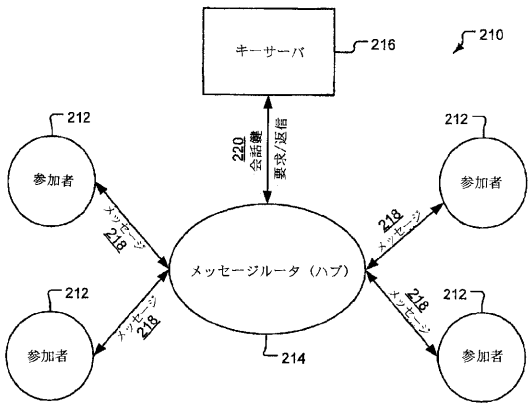


FIG. 9

【図１０】

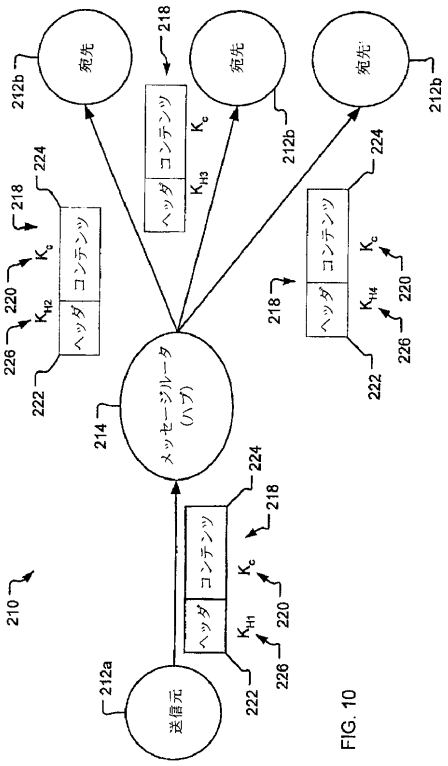


FIG. 10

【図１１】

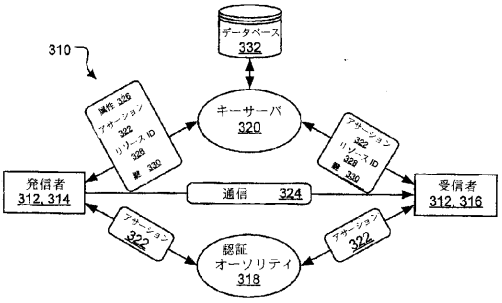


FIG. 11

【図１２】

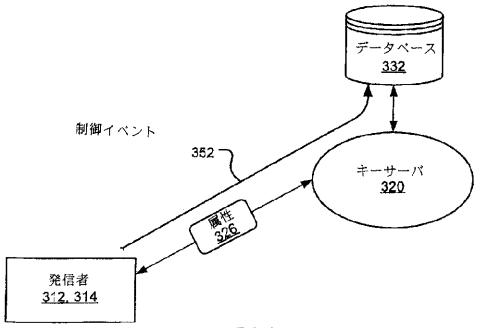


FIG. 12

【図１３】

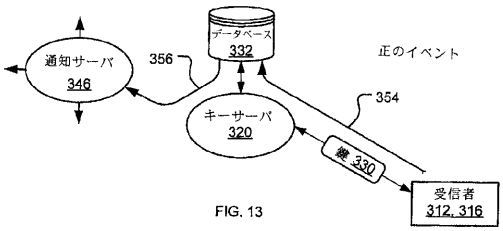


FIG. 13

【図１４】

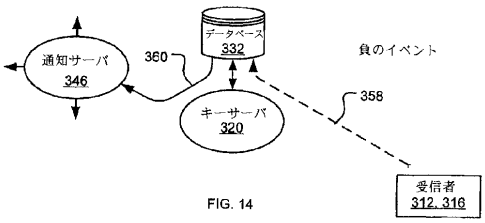


FIG. 14

【図１５】

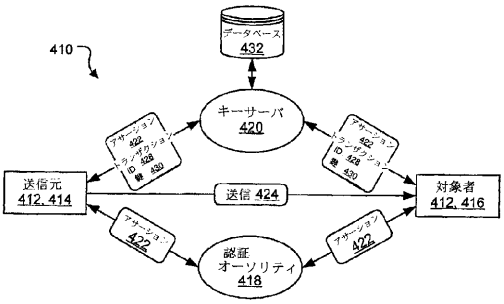


FIG. 15

【図１６】

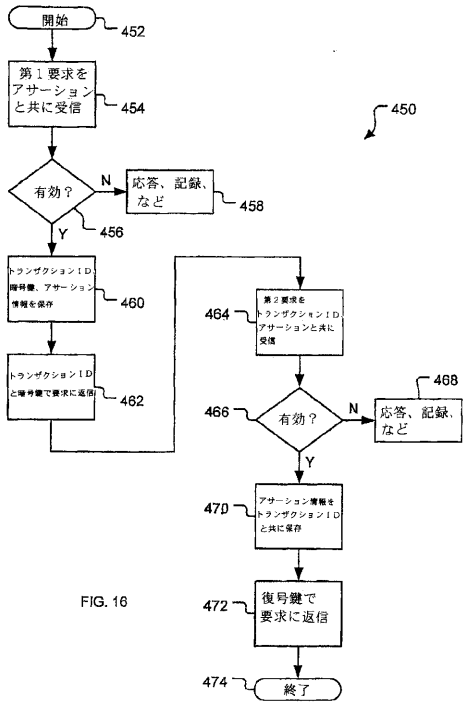


FIG. 16

【図１７】

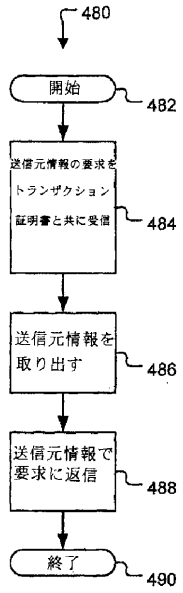


FIG. 17

【図１８】

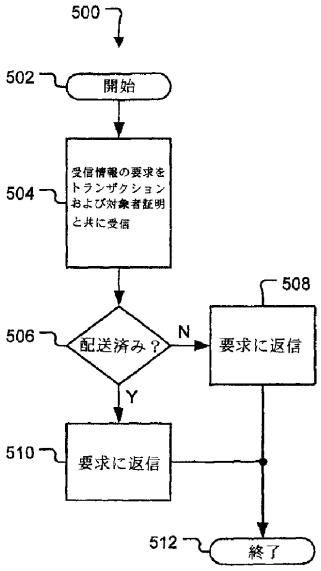


FIG. 18

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,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,IT,LU,MC,NL,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,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
ＪＡＶＡ

(72)発明者 モレイ，ジャハーンシャー
アメリカ合衆国 カリフォルニア州 ９００６７，ロサンゼルス，アパートメント ４１７，センチュリー パーク レーン ２１２２

Ｆターム(参考) 5J104 AA01 AA16 EA01 EA04 EA15 EA16 JA03 MA05 NA02 NA37
PA07