【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第７部門第３区分
【発行日】平成18年12月14日(2006.12.14)

【公表番号】特表2006-520112(P2006-520112A)
【公表日】平成18年8月31日(2006.8.31)
【年通号数】公開・登録公報2006-034
【出願番号】特願2004-555802(P2004-555802)
【国際特許分類】
Ｈ０４Ｌ　9/36　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６８５
Ｈ０４Ｌ　9/00　６０１Ｂ

【手続補正書】
【提出日】平成18年10月26日(2006.10.26)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【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、暗号化又はハッシングの少なくとも１つからなる保護を前記メッセージのメッセージコンテンツに適用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は、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３】
前記メッセージルータは、ヘッダ鍵を作成し、保存し、前記参加者に公開し、前記ヘッダ鍵は、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４】
前記ヘッダ鍵は、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３記載のシステム。
【請求項５】
前記ヘッダ鍵は、参加者のそれぞれで異なっている請求項３記載のシステム。
【請求項６】
会話は、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；
会話参加者は、前記会話に参加している参加者の組の構成要素であり；
前記会話参加者は、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
前記ヘッダ鍵は、前記それぞれのセッションで異なっている請求項５記載のシステム。

【請求項７】
前記メッセージルータは、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は、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８】
会話は、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；
会話参加者は、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；
参加する参加者は、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；
退出する参加者は、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；
前記キーサーバは、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は前記キーサーバに、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７記載のシステム。
【請求項９】
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り、そして、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ており、前記方法は、
（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、前記保護は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１０】
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、前記会話鍵は、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９記載の方法。
【請求項１１】
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９記載の方法。

【請求項１２】
すべての前記ヘッダ鍵は前記参加者のそれぞれで異なっている請求項１１記載の方法。
【請求項１３】
会話は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、会話参加者は前記会話に参加する参加者の組の構成要素であり、前記方法は、
前記会話参加者は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１２記載の方法。
【請求項１４】
前記会話鍵を要求するメッセージのインスタンスは鍵要求メッセージであり、前記方法は、
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９記載の方法。
【請求項１５】
会話は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、会話参加者は前記会話に参加する参加者の組の構成要素であり、参加する参加者は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、退出する参加者は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、前記方法は、
前記メッセージルータは、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９記載の方法。
【請求項１６】
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、前記通信を行っている参加者は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、前記キーサーバは
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、前記要求は前記識別子を含み；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１７】
前記キーサーバは、前記鍵を公開する前にアサーションを要求する請求項１６記載のシステム。
【請求項１８】
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１６記載のシステム。
【請求項１９】
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１６記載のシステム。
【請求項２０】
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１９記載のシステム。
【請求項２１】

前記制御イベントは、それ以降は前記復号鍵を公開できるようになる時間を構成するセットの要素を特定し、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し、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を特定し、前記復号鍵は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１６記載のシステム。

【請求項２２】

前記キーサーバは、前記受信者のためのアサーションを要求し；そして

前記制御イベントは、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１６記載のシステム。

【請求項２３】

前記キーサーバは、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１６記載のシステム。

【請求項２４】

通信イベントを決定する方法であって、前記方法は、

（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の要求は、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、前記制御イベントは前記少なくとも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の要求は前記リソース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）或いは、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２５】

前記ステップ（ｃ）は暗号鍵を提供することを含む請求項２４記載の方法。

【請求項２６】

前記第１の要求は認証アサーションを含み、前記ステップ（ａ）は前記ステップ（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２４記載の方法。

【請求項２７】

前記制御イベントの少なくともいくつかは、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２４記載の方法。

【請求項２８】

前記制御イベントの少なくともいくつかは、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２４記載の方法。

【請求項２９】

前記制御イベントの少なくともいくつかは、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２８記載の方法。

【請求項３０】

前記制御イベントは、前記復号鍵が前記受信者に公開可能となる時間を構成するセットの要素を特定し、それ以降は前記復号鍵が前記受信者に公開不能になる時間を特定し、前記復号鍵が前記受信者に公開されるべき回数を特定する請求項２５記載のシステム。

【請求項３１】

前記第２の要求は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）は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２４記載の方法。

【請求項３２】

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２４記載の方法。

【請求項３３】

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、方法は、

（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、前記要求は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は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は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は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の要求は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は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３４】

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、前記方法は、

（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、前記要求は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は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３５】

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はトランザクションを識別し、復号鍵は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、前記方法は、

（ａ）復号鍵の要求を受信し、ここで前記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は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３６】
トランザクション送信元とトランザクション対象者は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；
前記キーサーバは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の要求は送信元認証アサーションを含み；
前記キーサーバは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の要求は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；
前記キーサーバは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；
前記キーサーバは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；
前記キーサーバは前記第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
前記キーサーバは前記第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は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は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３７】
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、
前記キーサーバは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、ここで前記要求は送信元認証アサーションを含み；
前記キーサーバは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；
前記キーサーバは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
前記キーサーバは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は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３８】
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は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はデータベース内にあらかじめ保存されており、前記システムは、
コンピュータ化されたキーサーバを含み、
前記キーサーバは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、ここで前記要求は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；
前記キーサーバは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；

前記キーサーバは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；

前記キーサーバは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は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。