(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4680596号
(P4680596)
(45)発行日　平成23年5月11日(2011.5.11)　(24)登録日　平成23年2月10日(2011.2.10)

(51)Int.Cl.　F I
H04L 9/08 (2006.01)　H04L 9/00 601A

請求項の数 26 (全 14 頁)

(21)出願番号	特願2004-534408 (P2004-534408)
(86)(22)出願日	平成15年9月2日 (2003.9.2)
(65)公表番号	特表2005-537763 (P2005-537763A)
(43)公表日	平成17年12月8日 (2005.12.8)
(86)国際出願番号	PCT/US2003/027342
(87)国際公開番号	WO2004/023713
(87)国際公開日	平成16年3月18日 (2004.3.18)
審査請求日	平成18年7月12日 (2006.7.12)
(31)優先権主張番号	10/232,624
(32)優先日	平成14年9月3日 (2002.9.3)
(33)優先権主張国	米国(US)

(73)特許権者　502377350
ベリサイン・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　９４０４３　マウンテン・ビュー、イースト・ミドルフィールド・ロード　４８７
(74)代理人　100091351
弁理士　河野　哲
(74)代理人　100088683
弁理士　中村　誠
(74)代理人　100108855
弁理士　蔵田　昌俊
(74)代理人　100075672
弁理士　峰　隆司
(74)代理人　100109830
弁理士　福原　淑弘

最終頁に続く

(54)【発明の名称】公開鍵インフラストラクチャ内で秘密鍵を安全にエスクローするための方法およびシステム

(57)【特許請求の範囲】
【請求項１】
プロセッサと、このプロセッサに接続されているメモリとを備えているコンピュータを使用して公開鍵インフラストラクチャ内で秘密鍵をエスクローする方法において、
前記プロセッサを使用して、
１つの秘密鍵および１つの公開鍵を含む１つの鍵対を生成し、
セッション鍵を生成し、
このセッション鍵を使用して秘密鍵を暗号化し、
セッション鍵マスクを生成し、
暗号化された秘密鍵およびセッション鍵マスクを前記メモリに記憶し、
前記プロセッサの論理手段によってセッション鍵およびセッション鍵マスクを排他的オア処理することによってマスクされたセッション鍵を生成し、
マスクされていない前記セッション鍵を抹消し、
前記マスクされたセッション鍵およびデジタル証明書を前記プロセッサの配置された主位置とは異なる、秘密鍵を回復させる位置である補助位置に送信するステップを含んでいる秘密鍵をエスクローする方法。
【請求項２】
前記プロセッサはさらに、デジタル証明書を含む鍵回復リクエストを前記補助位置に送信し、
マスクされたセッション鍵を前記補助位置から受信し、

マスクされたセッション鍵およびセッション鍵マスクを排他的オアすることによりセッション鍵を再生し、
再生されたセッション鍵を使用して暗号化された秘密鍵を解読することにより秘密鍵を回復するステップをさらに含んでいる請求項１記載の方法。
【請求項３】
前記セッション鍵は対称鍵である請求項１記載の方法。
【請求項４】
前記セッション鍵を生成する前記ステップは、トリプルデータ暗号化規格および初期化ベクトルを使用するステップを含んでいる請求項１記載の方法。
【請求項５】
前記セッション鍵マスクは、セッション鍵に等しいビット長を有するランダムストリングである請求項１記載の方法。
【請求項６】
前記セッション鍵マスクは、セッション鍵に等しいビット長を有する擬似ランブムストリングである請求項１記載の方法。
【請求項７】
前記鍵回復リクエストは、複数のデジタル証明書を含んでいる請求項２記載の方法。
【請求項８】
解読された秘密鍵を対応した鍵対証明書と組合せるステップをさらに含んでいる請求項２記載の方法。
【請求項９】
前記鍵回復リクエストに関連した補助位置において監査トレイルを生成するステップをさらに含んでいる請求項２記載の方法。
【請求項１０】
プロセッサと、このプロセッサに接続されているメモリとを備えているこコンピュータに公開鍵インフラストラクチャ内で秘密鍵をエスクローする方法を実行させるように命令するプログラムにおいて、
前記プログラムは前記プロセッサに対して、
１つの秘密鍵および１つの公開鍵を含む１つの鍵対を生成し、
セッション鍵を生成し、
このセッション鍵を使用して秘密鍵を暗号化し、
セッション鍵マスクを生成し、
暗号化された秘密鍵およびセッション鍵マスクを前記メモリに記憶し、
セッション鍵およびセッション鍵マスクを排他的オア処理することによりマスクされたセッション鍵を生成し、
マスクされていないセッション鍵を抹消し、
マスクされたセッション鍵およびデジタル証明書を前記プロセッサの配置された主位置とは異なる、秘密鍵を回復させる位置である補助位置に送信するステップを実行させる命令を含んでいるプログラム。
【請求項１１】
プログラムはさらに、
デジタル証明書を含む鍵回復リクエストを前記補助位置に送信し、
マスクされたセッション鍵を前記補助位置から受信し、
マスクされたセッション鍵およびセッション鍵マスクを排他的オア処理することによったセッション鍵を再生し、
再生されたセッション鍵を使用することによって暗号化された秘密鍵を解読することにより秘密鍵を回復する動作をプロセッサに命令する請求項１０記載のプログラム。
【請求項１２】
前記セッション鍵は対称鍵である請求項１０記載のプログラム。
【請求項１３】

前記セッション鍵の生成は、トリプルデータ暗号化規格および初期化ベクトルを使用して行われる請求項１０記載のプログラム。
【請求項１４】
前記セッション鍵マスクは、セッション鍵に等しいビット長を有するランダムストリングである請求項１０記載のプログラム。
【請求項１５】
前記セッションマスクは、セッション鍵に等しいビット長を有する擬似ランブムストリングである請求項１０記載のプログラム。
【請求項１６】
前記鍵回復リクエストは、複数のデジタル証明書を含んでいる請求項１１記載のプログラム。
【請求項１７】
プログラムはさらに、
前記解読された秘密鍵は対応した鍵対証明書と組合せて使用される請求項１１記載のプログラム。
【請求項１８】
プログラムはさらに、
前記鍵回復リクエストに関連した補助位置において監査トレイルを生成させる請求項１１記載のプログラム。
【請求項１９】
ネットワークに結合され、主データベースおよび鍵管理サーバを含む主位置と、ネットワークに結合され、補助データベースおよび制御局を含む補助位置とを備えている公開鍵インフラストラクチャ内で秘密鍵をエスクローするシステムにおいて、
前記主位置の前記鍵管理サーバは、
１つの秘密鍵および１つの公開鍵を含む１つの鍵対を生成し、
セッション鍵を生成し、
このセッション鍵を使用して秘密鍵を暗号化し、
セッション鍵マスクを生成するように構成され、
前記主データベースは暗号化された秘密鍵およびセッション鍵マスクを記憶するように構成され、
前記鍵管理サーバはさらに前記セッション鍵および前記セッション鍵マスクを排他的オア処理してマスクされたセッション鍵を生成し、マスクされていないセッション鍵を抹消する手段と、
マスクされたセッション鍵およびデジタル証明書を補助データベース中に記憶するために補助位置に送信する手段とを具備している秘密鍵をエスクローするシステム。
【請求項２０】
前記主位置の前記プロセッサはさらに、
デジタル証明書を含む鍵回復リクエストを補助位置に送信し、
マスクされたセッション鍵を補助位置から受信し、
前記プロセッサはマスクされたセッション鍵およびセッション鍵マスクを排他的オア処理することによってセッション鍵を再生し、再生されたセッション鍵を使用して暗号化された秘密鍵を解読することにより秘密鍵を回復するように構成されている請求項１９記載のシステム。
【請求項２１】
前記セッション鍵は対称鍵である請求項１９記載のシステム。
【請求項２２】
前記セッション鍵は、トリプルデータ暗号化規格および初期化ベクトルを使用して生成される請求項１９記載のシステム。
【請求項２３】
前記セッション鍵マスクは、セッション鍵に等しいビット長を有するランダムストリン

グである請求項１９記載のシステム。
【請求項２４】
前記セッション鍵マスクは、セッション鍵に等しいビット長を有する擬似ランブムストリングである請求項１９記載のシステム。
【請求項２５】
前記鍵回復リクエストは、複数のデジタル証明書を含んでいる請求項２０記載のシステム。
【請求項２６】
前記主位置のプロセッサはさらに、解読された秘密鍵を対応した鍵対証明書と組合せるように構成されている請求項２０記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、一般に、公開鍵暗号化に関する。とくに、本発明の実施形態は、回復データに対して分散形記憶アーキテクチャを使用する秘密鍵のエスクローに関する。
【背景技術】
【０００２】
インターネットおよびＥコマースの人気は高まり続けているため、セキュリティの問題は最も重要な関心事である。オンライン取引が伝統的な取引に代わるものとして成立するためには、パーティの間の接続を秘密に対して保護するメカニズムが重要である。公開鍵インフラストラクチャにおいて、各パーティは、公開された１つの鍵（公開鍵）と秘密の保持された別の鍵（秘密鍵）から形成されたある鍵対を必要とする。公開鍵はデジタル証明者中に配置され、自分が公開鍵の所有者だと主張している者が本当にそうであることを検証するために十分に成文化されたデジタル署名アルゴリズム（ＤＳＡ）のようなアルゴリズムを使用して署名される。いくつかのアプリケーションは、所有者が鍵対を生成してデジタル証明書自体を発生することを可能にするが、セキュリティがとくに重要であるアプリケーションにおいては、公開鍵対の所有者の身元を検証するために証明機関（ＣＡ）と呼ばれる第３のパーティが使用されることが多い。
【発明の開示】
【発明が解決しようとする課題】
【０００３】
多くの場合、ＣＡは登録機関（ＲＡ）を使用して、そのデジタル証明書がその鍵対の所有者に発行されたか否かを決定する。ＲＡは、一般に鍵エスクローと呼ばれる所有者の秘密鍵のバックアップコピーを保持することが多い。明らかに、秘密鍵のエスクロー化されたコピーは、偶発的な発覚を回避するように安全に秘密保護されて記憶され、保護されなければならない。したがって、許可されていないパーティが秘密鍵にアクセスすることが非常に困難なものになるように秘密鍵を安全にエスクローすることが必要とされている。
【０００４】
いくつかの鍵エスクロー方法が開発されているが、ある問題が残っている。図１および１２乃至１４は、従来技術の鍵エスクロー方法を示し、これらの問題を強調している。とくに、図１は公開鍵インフラストラクチャを示しており、ここにおいて、エンドユーザ130はネットワーク160による秘密に対して安全な接続を介して主位置140によってある鍵対132を提供される。鍵管理サーバ（ＫＭＳ）180は、鍵対132中の秘密鍵の１つの暗号化された変形である鍵回復記録（ＫＲＲ、または暗号化された秘密鍵）20と、回復データ22とを主位置140に配置された主データベース24中に記憶することが認められる。この暗号化された秘密鍵20を安全に保護するためにセッション鍵が使用される。
【０００５】
図１４は、回復データ22（図１）を構成する従来技術の方法を示している。一般に、セッション鍵およびパスワードは、３つのエンティティ：鍵回復コーディネータ（ＫＲＣ）、鍵回復オフィサ（ＫＲＯ）および鍵回復エージェント（ＫＲＡ）の公開鍵で暗号化され

ることが認められる。主位置140（図１）において管理者により１つのパスワードが提供され、鍵管理サーバ（ＫＭＳ）180（図１）によってセッション鍵が発生される。回復データ22は時として鍵回復ブロック（ＫＲＢ）と呼ばれる。再び図１を参照すると、秘密鍵を回復するためには、上述した管理者のような許可された鍵回復担当者がその管理者により与えられた候補パスワードと共に回復データ22を補助位置26に配置された鍵回復サーバに送信することが認識されるであろう。候補パスワードは、回復リクエストを行っている管理者が補助位置26によりセッション鍵を提供される前に、回復データ22中に含まれているパスワードと一致しなければならない。

【０００６】

したがって、図１２に示されているように、処理ブロック28において秘密鍵がセッション鍵によって暗号化され、処理ブロック30において、回復データ22および暗号化された秘密鍵20は主位置（図１）に記憶される。図１３に示されているように、秘密鍵を回復するために、ブロック32において回復データ22および暗号化された秘密鍵20が主位置メモリから検索され、ブロック34において回復データ22および証明書パスワードは補助位置26に送信される。鍵回復サーバ（ＫＲＳ）36は、ＫＲＣ、ＫＲＯおよびＫＲＡ公開鍵を使用して回復データ22を解読し、管理者によって提供された候補パスワード38は解読された回復データ22中に含まれているパスワードと一致するか否かを決定する。そうである場合、セッション鍵40が補助位置26から主位置140に送信される。ブロック36において受信されると、ブロック42において暗号化された秘密鍵はセッション鍵40に基づいて解読される。その結果が秘密鍵44であり、これはエンドユーザ130（図１）に再送信されることが可能である。

【０００７】

上述した方法はある環境においては満足できるものであるが、改善の余地がかなり残されている。たとえば、暗号化された秘密鍵20と回復データ22の両者を主位置140に記憶することにより、秘密鍵を回復するためにパスワードメカニズムが必要になる。しかしながら、担当者の変更およびセキュリティの継続的な問題は、パスワード変更がしばしば必要であることを意味している。たとえば、ある特定の管理者が秘密鍵に対する回復データ中に含まれたパスワードを提供し、それに続いて主位置140による使用を止めた場合、その管理者のパスワードは変更されなければならない。このような状態が発生したとき、ＫＲＢ22全体が新しいパスワードと共に再度発生されなければならない。担当者の変更に基づいてＫＲＢを選択的に再度発生することは管理上複雑であり、また不便である。したがって、パスワードが要求されない公開鍵インフラストラクチャ内で秘密鍵へのアクセスを制限することが必要とされている。

【０００８】

別の問題は、回復データ22の秘密を保護するために暗号化を使用することに関する。とくに、ＫＲＣ、ＫＲＯおよびＫＲＡ鍵対には、補助位置26により１以上の外部ソースから獲得されることが多いデジタル証明書が必要である。たとえば、１つの市販のシステムにおいて、デジタル証明書はＫＲＯ／ＫＲＣ／ＫＲＡ暗号化／解読コードのプロバイダから獲得されなければならない。補助位置26が証明書を受信したとき、それらは構成ファイルに埋込まれ、この構成ファイルがＫＭＳ180（図１）に転送され、暗号化を行うことのできるツールキットと共にインストールされる。しかしながら、証明書の期限が切れていたとき、ツールキットはもはや暗号化を行って回復データ22を発生することはできない。新しい現在の証明書をタイミングよく獲得することは、複雑で不便である可能性が高い。その結果、新しい構成ファイルを獲得できるまで、時としてクロックリセットのような望ましくない手段に頼らざるを得ない。補助位置26が上述した外部ソースから証明書を獲得しなければならないとき、結果はとくに深刻である。したがって、十分なセキュリティレベルを維持しながら証明書によるセッション鍵のパスワードで保護された暗号化を必要としない回復データを発生する方法を提供する必要がある。

【課題を解決するための手段】

【０００９】

本発明は、１つの秘密鍵および１つの公開鍵を含む１つの鍵対を生成し、セッション鍵を生成し、このセッション鍵を使用して秘密鍵を暗号化し、セッション鍵マスクを生成し、暗号化された秘密鍵およびセッション鍵マスクを記憶し、セッション鍵およびセッション鍵マスクを排他的オアすることによってマスクされたセッション鍵を生成し、そのセッション鍵を抹消し、マスクされたセッション鍵およびデジタル証明書を補助位置に送信するステップを含んでいる公開鍵インフラストラクチャ内で秘密鍵をエスクローする方法を提供する。

【発明を実施するための最良の形態】

【００１０】

本発明の実施形態の種々の利点は、以下の明細書、添付された請求の範囲および添付図面を参照することにより当業者に明らかになるであろう。

図２を参照すると、公開鍵インフラストラクチャが示されており、ここで秘密鍵エスクローが本発明の１実施形態にしたがって実施される。一般に、このインフラストラクチャは、回復データに対して分散形記憶アーキテクチャを使用し、パスワードの必要性をなくしている。ここに記載されている実施形態は主として広域ネットワーク（ＷＡＮ）およびインターネットに関して説明されているが、これら実施形態はそれに限定されないことが認識されるであろう。実際に、ここに記載されている原理は、セキュリティが関係する任意のネットワーク環境において有用であることが可能である。それらもかかわらず、これら実施形態が特有に適切なものとなるインターネット用途の多くの特徴が存在する。

【００１１】

一般に、エスクローの時点で、保護された秘密鍵20は第１の回復データ48と共に主位置46に配置されたメモリに記憶される。秘密鍵は、その秘密鍵をセッション鍵で暗号化することによって、あるいは秘密鍵とセッションマスクとの間で排他的オア（ＸＯＲ）動作を行うことによって保護されることができる。いずれの場合も、秘密鍵はセッション値（すなわち、鍵またはマスク）を使用して保護される。メモリは主データベース50として示されているが、別の記憶構成が可能であることを認識すべきである。たとえば、保護された秘密鍵20は第１の回復データ48から分離されたデータベース中に記憶されてもよいし、あるいは情報は、データベースフォーマットではない１以上の基本電子ファイルとして記憶されることが可能である。メモリは動的ランダムアクセスメモリ（ＤＲＡＭ）、Ｒａｍｂｕｓ（登録商標）ＲＡＭ（ＲＤＲＡＭ）、静的ＲＡＭ（ＳＲＡＭ）、フラッシュメモリ、ハードディスク、光ディスク、磁気光ディスク、ＣＤ-ＲＯＭ、デジタルバーサタイルディスク、ＤＶＤ、非揮発性メモリ、またはそれらの任意の組合せであることが可能であることもまた認識すべきである。

【００１２】

第２の回復データ52は補助位置54に送られ、ここで秘密鍵の回復を可能にするために第１の回復データ48および第２の回復データ52が一緒に使用されることができる。以下さらに詳細に説明するように、第１の回復データ48はマスクであることが可能であり、第２の回復データ52はマスクされたセッション値であることが可能であり、セッション値とマスクとの間でＸＯＲ動作を行うことによってセッション値が保護される。第１の回復データはまた、セッション値をマスク鍵で暗号化することによりセッション値が保護されるマスク鍵であることが可能である。さらに、ネットワーク160による主位置46と補助位置54との間の通信は、よく知られている技術にしたがって秘密保護に対して安全な接続により鍵管理サーバ（ＫＭＳ）56および制御局58によって容易に行われる。制御局58は第２の回復データ52を補助データベース59に記憶し、この補助データベース59は上述された任意の許容可能な機械読取り可能な媒体内に構成されることができる。

【００１３】

図３は、鍵エスクロープロセスの１つの方法を主位置46の視点からさらに詳細に示している。とくに、処理ブロック60において、鍵対の秘密鍵がセッション鍵により暗号化される。ブロック62において、第１の回復データ48および暗号化された秘密鍵20が主位置46に記憶される。処理ブロック64において、第２の回復データ52が補助位置54に送信され、こ

の補助位置54において第１の回復データ48および第２の回復データ52が秘密鍵の回復を可能にする。

【００１４】

図４を参照すると、第１の回復データ48（図３）および暗号化された秘密鍵20を主位置46（図３）に記憶する１つの方法がブロック63においてさらに詳細に示されている。とくに、ブロック66においてマスク49が発生され、ここにおいて第１の回復データはマスク49を含んでいる。ブロック68において、マスク49とセッション鍵70との間で排他的オア（ＸＯＲ）動作が行われる。ＸＯＲ動作の結果、マスクされたセッション鍵（ＭＳＫ）53が生成され、ここにおいて第２の回復データはＭＳＫ53を含んでいる。したがって、マスク49は主位置46（図３）に記憶され、ＭＳＫ53は補助位置54（図３）に送られて記憶される。この時点で、セッション鍵70はもはや必要とされず、ブロック74において破壊される。１つの方法において、セッション鍵70を保持しているメモリ位置が０にされて消去される。

【００１５】

マスクおよびセッション鍵は典型的に、１２８ビットのような同じビット長を有している。マスク49はランダムまたは擬似ランダムストリング発生アルゴリズムのいずれかによって発生されることができることがさらに認識されるであろう。示されているマスク49は、十分に成文化された米連邦情報処理規格（ＦＩＰＳ）１４０-１および１４０-２を満足させなければならない。

【００１６】

したがって、図３および４に示されている処理ブロックは、ＫＭＳ56（図２）内のプロセッサによりアクセス可能な機械読取り可能な記憶媒体中に記憶された鍵エスクロー命令のセットとして実施されることができる。ＫＭＳ56はさらに、十分に成文化された鍵発生方法にしたがって鍵対を発生すると共にセッション鍵を発生するように構成されることが可能であることもまた認識すべきである。たとえば、トリプルデータ暗号化規格（３ＤＥＳ）および初期化ベクトル（ＩＶ）は、対称セッション鍵を生成するために使用されることができる。図５は、エスクロープロセスを要約した鍵エスクローデータフロー76を示している。

【００１７】

図６を参照すると、エスクロー化された秘密鍵を回復する１つの方法が示されている。一般に、ブロック78において、第１の回復データ48および暗号化された秘密鍵20が主位置46に配置されたメモリから検索される。処理ブロック80において、第２の回復データ52が補助位置54から受信される。ブロック82において、暗号化された秘密鍵20は第１の回復データ48および第２の回復データ52に基づいて解読される。すでに説明したように、１つの方法において、第１の回復データ48はマスクであり、第２の回復データはマスクされたセッション鍵である。

【００１８】

したがって、図７は、暗号化された秘密鍵20を解読する１つの方法をブロック83においてさらに詳細に示している。とくに、ブロック84においてＸＯＲ動作がマスク49とＭＳＫ53との間で行われることが認められ、ここで、ＸＯＲ動作の結果、マスク49を使用してＭＳＫ53が導出されて元のセッション鍵70が得られる。ブロック86において、暗号化された秘密鍵20が主位置に配置されたメモリから検索され、ブロック88において、暗号化された秘密鍵20がセッション鍵70に基づいて解読される。処理ブロック90において、解読された秘密鍵44は対応した鍵対証明書と組合せられて、管理者またはエンドユーザへの伝送のために１つのファイルにされる。したがって、上記の回復手順は鍵回復命令のセットとして実施され、また、ＫＭＳ56（図２）内のプロセッサによってアクセス可能である機械読取り可能な記憶媒体に記憶されることができる。図８は、鍵回復プロセスを要約する鍵回復データフロー94を示している。

【００１９】

図９を参照すると、公開鍵インフラストラクチャ内において秘密鍵へのアクセスを制限する方法96が示されており、ここにおいて、暗号化された秘密鍵は主位置に記憶されてい

る。この方法96は、秘密鍵が主位置でエスクロー化されている期間中その完全性を維持するために補助位置によって実施されることができる。処理ブロック98において、マスクされたセッション鍵（ＭＳＫ）が補助位置に記憶されることができる。ＭＳＫは、秘密鍵の回復を可能にする。既知の方法では、鍵回復データの全てが主位置に記憶され、単に、暗号化されたセッション鍵および鍵回復データを検証および解読のために補助位置に送信するに過ぎないことを認識すべきである。本発明の１実施形態においては、ＭＳＫを補助位置に記憶することにより、パスワード保守および証明書期限切れに関する多くの問題が事前に取り除かれる。

【００２０】

とくに、ブロック100において、鍵エスクローリクエスタ（たとえば、登録機関ＲＡ）は管理者証明書に基づいて認証されることができる。ブロック104において、その認証された鍵エスクローリクエスタが鍵エスクロー特権と関連付けられていることが検証される。これに関して、デジタル証明書を発行した多くの補助位置は、システム構成を変更する能力、証明書を許可／拒否する能力、および特権を変更する能力のような管理者に対する特権のセットを維持することができる。鍵回復を特権として追加することにより、補助位置は鍵エスクローおよび回復プロセスを既存の認証方式の中に組込むことができる。ブロック102において、ＭＳＫは秘密保護に対して安全なソケット層（ＳＳＬ）接続のような安全なエスクロー接続を介して認証された秘密鍵エスクローリクエスタから受信される。

【００２１】

ブロック106において、管理者証明書に基づいて鍵回復リクエスタを認証することにより鍵回復が実施されることができる。処理ブロック108において、認証された鍵回復リクエスタは鍵回復特権と関連付けられているか否かが決定される。鍵回復特権が検証された場合、ＭＳＫは補助位置に配置されたメモリから検索され、ブロック110において、安全な回復接続を介して認証された鍵回復リクエスタに送信される。また、このブロック110においては、この送信は将来の参照のために監査トレイルに記録される。

【００２２】

図１０を参照すると、鍵エスクローリクエスタを認証する１つの方法がブロック101においてさらに詳細に示されている。とくに、鍵エスクローが許可される前に多数の管理者自身を補助位置に対して認証することを彼等に要求することによりセキュリティが追加されることができる。したがって、ブロック112において、第１の管理者証明書に基づいて第１の鍵エスクローリクエスタが認証され、ブロック114において、第２の管理者証明書に基づいて第２の鍵エスクローリクエスタが認証され、ブロック116においては、第ｎの鍵エスクローリクエスタが同様に認証される。同様に、図１１は、鍵回復リクエスタを認証する１つの方法をブロック107において示すと共に鍵回復特権を検証する１つの方法をブロック109において示している。ブロック118において第１の鍵回復リクエスタが認証され、ブロック119においてその第１の鍵回復リクエスタは鍵回復特権と関連付けられていることが検証される。ブロック120において第２の鍵回復リクエスタの認証が行われ、ブロック121においてその第２の鍵回復リクエスタは鍵回復特権と関連付けられていることが検証される。このプロセスは、ブロック122および123における第ｎの鍵回復リクエスタに対するものまで続行する。

【００２３】

上述した実施形態は、既知の鍵回復システムより秘密の保守が安全で容易であることができる。各エスクロー鍵を回復するためにどのパスワードが必要とされるかを記憶しなければならない代りに、主位置はそれらの既存の位置上の管理者証明書を使用するだけで彼等自身を制御局に対して認証することができる。そうしたときに、彼等は、鍵回復を行うことを許可されたことを証明することができる。秘密鍵は依然として主位置においてエスクロー化されており、補助位置に対して決して明らかにされない利点があることを認識することが重要である。さらに、主位置からのある情報と補助位置からのある情報とは１つの鍵を回復するために組合せられなければならないため、鍵回復の分離性質が保存される。主データベースが侵入者により盗まれた場合、それは任意の鍵の回復に対して計算的に

実行不可能であることが可能である。彼等が１つの鍵を何とか回復することができても、その情報が別の鍵を回復する助けを何等提供するものではない。

【００２４】

本発明の１実施形態は以下のように説明されることができる。第１の位置は、１２８ビットの対称鍵であってもよい第１の鍵を有するクライアントコンピュータである。別の鍵サイズもまた可能である。対称鍵は、クライアントのハードドライブ上の記憶されている貴重で取り扱いに注意を要するデータを暗号化するために使用される。その鍵が失われ、あるいは破壊された場合、そのデータをハードドライブから回復することは困難であり、あるいは不可能である。クライアントは、技術的に知られているＤＥＳアルゴリズムを使用して第１の鍵を１２８ビットの第２の鍵で暗号化し、暗号化された第１の鍵を得る。クライアントは、時としてナンス（ｎｏｎｃｅ）と呼ばれる乱数を発生する。このナンスはマスクとして機能し、セキュリティのために一般に一度だけ使用される情報の一部である。クライアントは第２の鍵およびナンスに関してＸＯＲ動作を行ってマスクされた第２の鍵を獲得する。その後、クライアントはそのナンスおよび暗号化された第１の鍵を記憶し、第２の鍵を、たとえば、それをメモリから完全に、かつ永久的に抹消する等によって破壊する。クライアントはマスクされた第２の鍵を補助位置に送信し、この補助位置は信頼できる鍵回復サーバである。クライアントは、第２の位置からマスクされた第２の鍵のコピーをリクエストする任意のエンティティを認証するために特定クライアント要求を実施するように、および、または第２の位置がマスクされた第２の鍵のコピーをリクエスタに送信する前にある特定クライアント条件が満足されることを確実にするように第２の位置に命じることができる。たとえば、信頼できる第３パーティにより署名されたデジタル証明書を使用してリクエスタの身元（アイデンティティ）が検証された場合、マスクされた第２の鍵が第２の位置により受信された後１２０日以内にリクエストが受信された場合、また、リクエスタがそのクライアントの会社の情報テクノロジースタッフのメンバーまたはクライアント自身である場合にのみ、クライアントは、第２の位置がマスクされた第２の鍵のコピーをそのリクエスタに送信することを要求することが可能である。

【００２５】

８０日後に第１の鍵がクライアントにおいて偶発的に削除され、そのクライアントがハードドライブ上に記憶された暗号化されたデータにアクセスすることができなくなった場合、そのクライアントは、信頼できる第３のパーティにより発行されたそのクライアントのデジタル証明書と共にマスクされた第２の鍵に対するリクエストを第２の位置に送信する。第２の位置はデジタル証明を検証し、そのリクエストが１２０日の範囲内に受信されたことを確認するためにチェックし、をそのリクエスタがクライアント自身であることを検証する。第２の位置はマスクされた第２の鍵をそのクライアントに送信する。クライアントはマスクされた第２の鍵およびナンスに関してＸＯＲ動作を行って第２の鍵を獲得し、この第２の鍵は暗号化された第１の鍵を解読するために使用される。このようにして、クライアントは失われた第１の鍵を回復する。

【００２６】

本発明は、当業者によって認識されるその他種々の実施形態を含むことが可能であり、上記に与えられた特定の実施形態に限定されない。鍵は、秘密鍵を使用してその鍵を暗号化し、その秘密鍵を２つのデータ部分（第１および第２の部分）に変換してその両者が秘密鍵を回復するために必要とされるようにすることにより回復可能にされる。秘密鍵自身は抹消される。２つの各データ部分は異なった位置に記憶され、それらを再結合するにはある定まった要求が満足されなければならない。それらが再結合されたとき、秘密鍵は回復され、暗号化された鍵を解読するために使用される。このようにして、元の鍵が回復される。

【００２７】

上記の説明から、当業者は本発明の実施形態の広範囲にわたる技術が種々の形態で実施されることができることを認識することが可能である。したがって、実施形態は特定の例との関連で説明されているが、図面、明細書および請求の範囲の検討により他の修正が当

業者に明らかになるため、本発明の実施形態の真の技術的範囲はそれに制限されてはならない。

【図面の簡単な説明】

【００２８】

【図１】本発明の実施形態の理解に有用な、公開鍵インフラストラクチャ内で秘密鍵へのアクセスを制限する従来技術の方法を示す概略図。

【図２】本発明の１実施形態による公開鍵インフラストラクチャの一例のブロック図。

【図３】秘密鍵をエスクロー化する本発明の１実施形態による方法の一例のフローチャート。

【図４】第１の回復データと暗号化された秘密鍵を主位置に記憶する本発明の１実施形態によるプロセスの一例のフローチャート。

【図５】本発明の１実施形態による鍵エスクローデータフローの一例のブロック図。

【図６】秘密鍵を回復する本発明の１実施形態による方法の一例のフローチャート。

【図７】暗号化された秘密鍵を解読する本発明の１実施形態によるプロセスの一例のフローチャート。

【図８】本発明の１実施形態による鍵回復データフローの一例のブロック図。

【図９】公開鍵インフラストラクチャ内で秘密鍵へのアクセスを制限する本発明の１実施形態による方法の一例のフローチャート。

【図１０】鍵エスクローリクエスタを認証する本発明の１実施形態によるプロセスの一例のフローチャート。

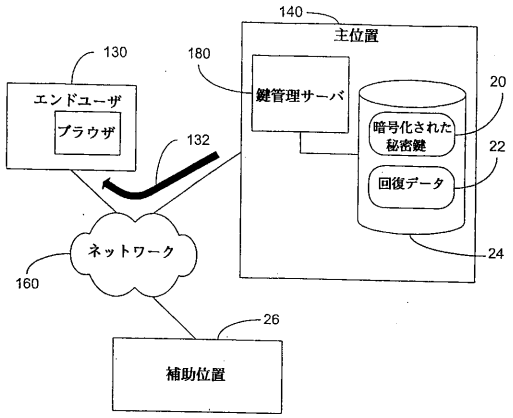
【図１１】鍵回復リクエスタを認証する本発明の１実施形態によるプロセスの一例のフローチャート。

【図１２】本発明の実施形態の理解に有用な、公開鍵インフラストラクチャ内で秘密鍵へのアクセスを制限する従来技術の方法を示す概略図。

【図１３】本発明の実施形態の理解に有用な、公開鍵インフラストラクチャ内で秘密鍵へのアクセスを制限する従来技術の方法を示す概略図。

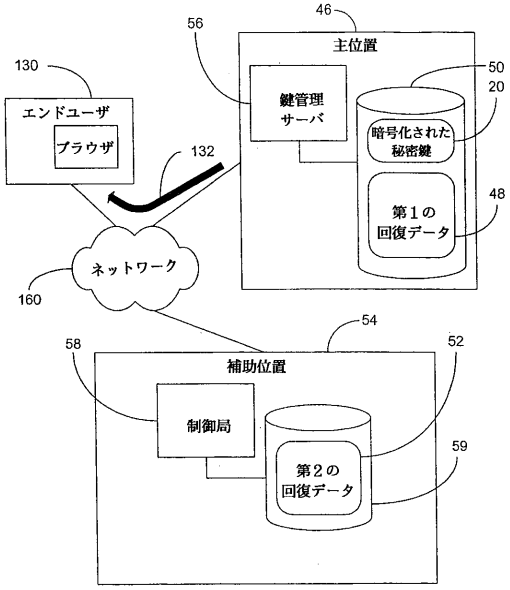
【図１４】本発明の実施形態の理解に有用な、公開鍵インフラストラクチャ内で秘密鍵へのアクセスを制限する従来技術の方法を示す概略図。

【図１】

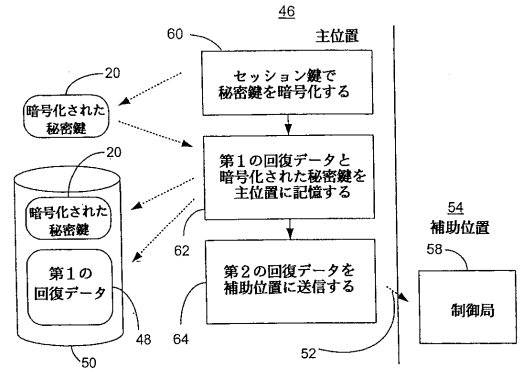


（従来技術）

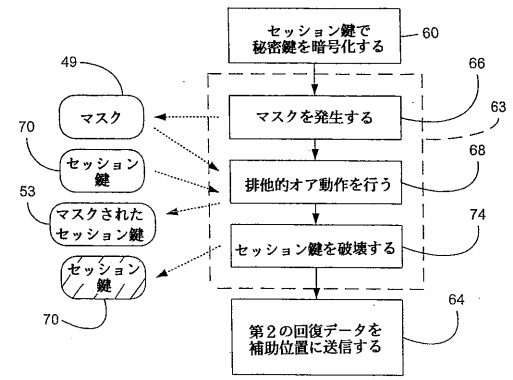
【図２】



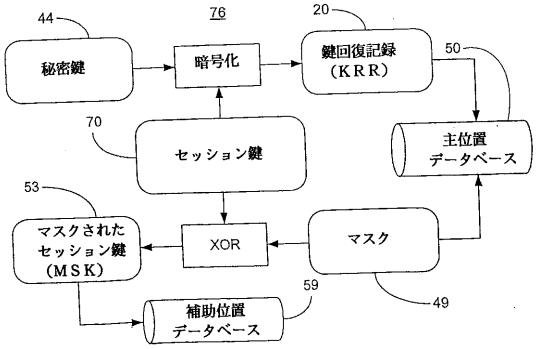
【図３】



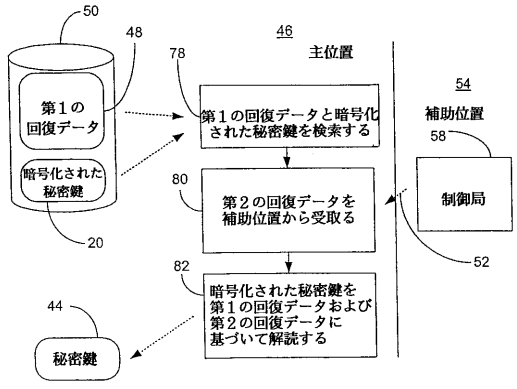
【図４】



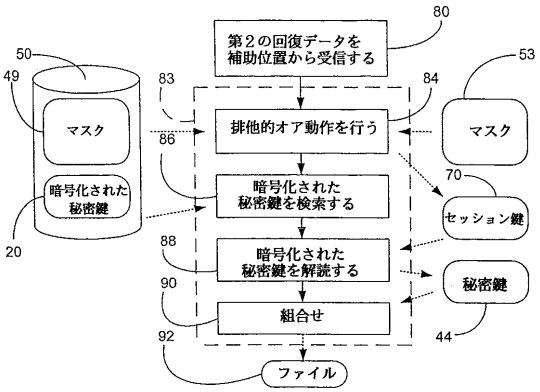
【図５】



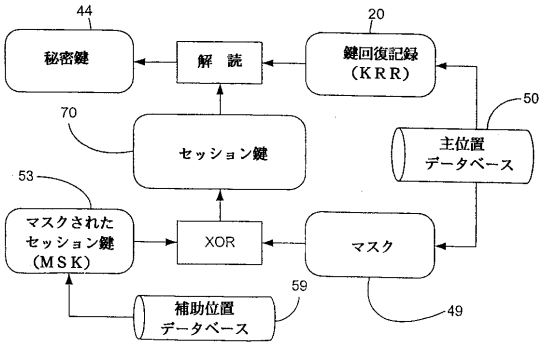
【図６】



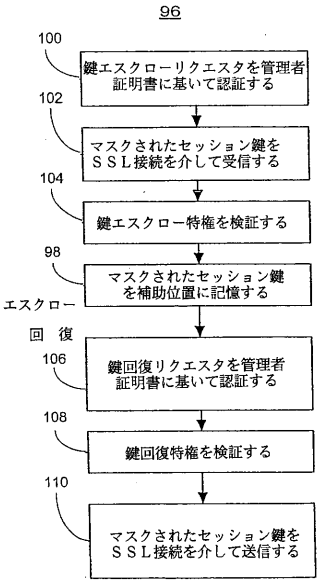
【図７】



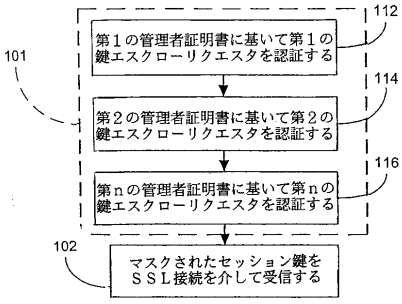
【図８】



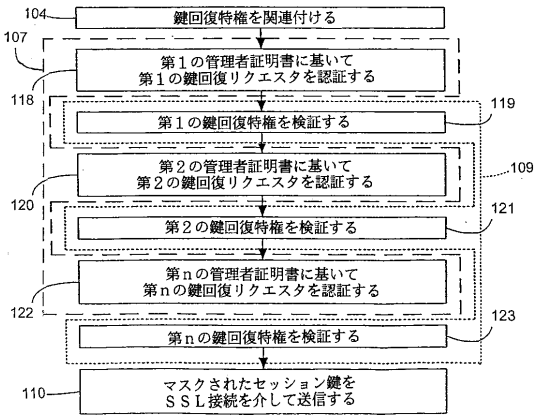
【図９】



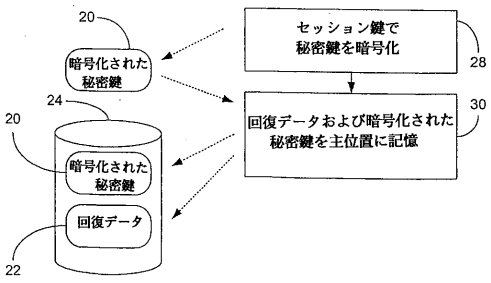
【図１０】



【図１１】

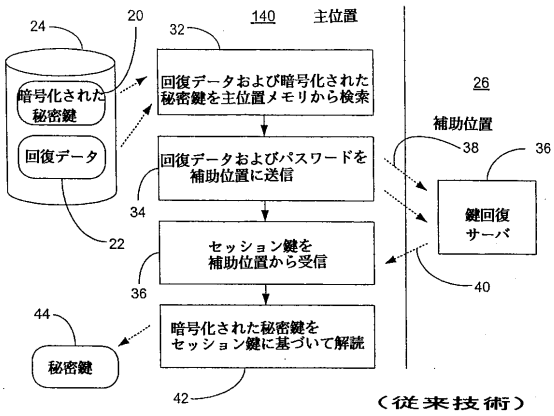


【図１２】



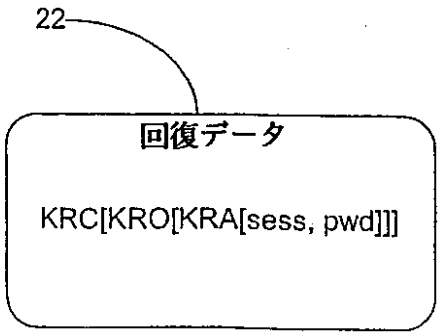
（従来技術）

【図１３】



（従来技術）

【図１４】



（従来技術）

フロントページの続き

(74)代理人 100084618
弁理士 村松 貞男
(74)代理人 100092196
弁理士 橋本 良郎
(72)発明者 アンドリュース、リチャード・エフ.
アメリカ合衆国、カリフォルニア州 ９４０２５、メンロ・パーク、レランド・アベニュー ２７９
(72)発明者 ファン、ジヨン
アメリカ合衆国、カリフォルニア州 ９４０８５、サニーベール、ナンバーディー１０２７、エスカロン・アベニュー １０００
(72)発明者 ルアン、トム・チ・ション
アメリカ合衆国、カリフォルニア州 ９５１２９、サン・ホセ、アイビー・レーン ６４４７

審査官 青木 重徳

(56)参考文献 米国特許第０６３７０２５１（ＵＳ，Ｂ１）
米国特許第０６３３５９７２（ＵＳ，Ｂ１）
特表平０９－５０７７２９（ＪＰ，Ａ）
特表平１１－５０６２２２（ＪＰ，Ａ）
特開２００１－２６８０６７（ＪＰ，Ａ）
特開平１０－１７７３４１（ＪＰ，Ａ）
特開２０００－１５１５７４（ＪＰ，Ａ）
池野信一，小山謙二，“現代暗号理論”，日本，社団法人電子情報通信学会，１９９７年１１月１５日，初版第６刷，ｐ．５４－５６，６０－６２
鬼頭宏幸，関野公彦，“社内システム向けキーリカバリシステムの開発”，ＮＴＴ技術ジャーナル，日本，社団法人電気通信協会，１９９９年１０月 １日，Ｖｏｌ．１１，Ｎｏ．１０，ｐ．５２－５３
鬼頭宏幸，植田広樹，関野公彦，“鍵寄託型キーリカバリシステムの設計と評価”，第５９回（平成１１年後期）全国大会講演論文集（３） データベースとメディア ネットワーク，日本，社団法人情報処理学会，１９９９年 ９月２８日，４Ｔ－３，ｐ．３・３９３－３・３９４

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 9/08