(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第4914051号
(P4914051)

(45)発行日　平成24年4月11日(2012.4.11)　(24)登録日　平成24年1月27日(2012.1.27)

(51)Int.Cl.		F I		
H04L 9/32	(2006.01)	H04L	9/00	675B
G06F 15/00	(2006.01)	G06F	15/00	
H04L 9/10	(2006.01)	H04L	9/00	621A

請求項の数 22　(全 15 頁)

(21)出願番号	特願2005-301986 (P2005-301986)
(22)出願日	平成17年10月17日 (2005.10.17)
(65)公開番号	特開2006-148879 (P2006-148879A)
(43)公開日	平成18年6月8日 (2006.6.8)
審査請求日	平成20年10月17日 (2008.10.17)
(31)優先権主張番号	10/990,798
(32)優先日	平成16年11月17日 (2004.11.17)
(33)優先権主張国	米国(US)

(73)特許権者　500046438
マイクロソフト　コーポレーション
アメリカ合衆国　ワシントン州　９８０５２－６３９９　レッドモンド　ワン　マイクロソフト　ウェイ
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(72)発明者　ジェスパー　エム．ヨハンソン
アメリカ合衆国　９８０５２　ワシントン州　レッドモンド　ワン　マイクロソフト　ウェイ　マイクロソフト　コーポレーション内

最終頁に続く

(54)【発明の名称】パスワード保護

(57)【特許請求の範囲】

【請求項１】

パスワード保護モジュールを含むコンピュータにおいて、

前記パスワード保護モジュールが、パスワードと他のデータとを連結するステップと、

前記パスワード保護モジュールが、前記連結したパスワードと他のデータに基づいて値を生成するステップと、

前記パスワード保護モジュールが、前記値に鍵生成アルゴリズムを実行することによって、第１の非対称鍵ペアを形成するステップであって、前記値に前記鍵生成アルゴリズムを実行することにより、同一の出力が得られる、ステップと、

前記パスワード保護モジュールが、前記第１の非対称鍵ペアの公開鍵に基づいて、自己署名した擬似公開鍵証明書を生成するステップであって、前記擬似公開鍵証明書は、公開鍵インフラストラクチャ（ＰＫＩ）のフォーマットを有するが、ＰＫＩ証明書サーバによって発行されていない、ステップと、

前記パスワード保護モジュールが、前記擬似公開鍵証明書を認証サーバにエクスポートするステップと、

前記パスワード保護モジュールが、認証セッションに応答して、ディジタル署名ログインプロセスの一部として前記鍵生成計アルゴリズムを実行することによって、第２の非対称鍵ペアを形成し、前記第２の非対称鍵ペアの秘密鍵を使用して前記認証サーバに対する認証を行うステップであって、前記第１の非対称鍵ペアの秘密鍵と前記第２の非対称鍵ペアの秘密鍵は同一である、ステップと

を備えることを特徴とする方法。
【請求項２】
前記非対称鍵ペアは、ディフィー－ヘルマン、ＲＳＡ、ＤＳＡ、または非対称鍵ペアを生成するのに適した任意のその他のアルゴリズムに基づくことを特徴とする請求項１に記載の方法。
【請求項３】
前記パスワードは、平文パスワードであることを特徴とする請求項１に記載の方法。
【請求項４】
前記パスワードは、暗号化鍵交換プロトコルに応じて生成された弱いパスワードであることを特徴とする請求項１に記載の方法。
【請求項５】
前記他のデータは、ユーザプリンシパル名またはユーザに実質的に固有のその他の値であることを特徴とする請求項１に記載の方法。
【請求項６】
パスワードと他のデータとを連結するステップは、前記パスワードと前記他のデータとを暗号関数を介して組み合わせるステップを含むことを特徴とする請求項１に記載の方法。
【請求項７】
値を生成するステップは、前記連結したパスワードと前記他のデータに基づいて擬似乱数を生成するステップを含むことを特徴とする請求項１に記載の方法。
【請求項８】
パスワード保護モジュールを含むコンピュータに、
前記パスワード保護モジュールが、パスワードと他のデータとを連結するステップと、
前記パスワード保護モジュールが、前記連結したパスワードと他のデータに基づいて値を生成するステップと、
前記パスワード保護モジュールが、前記値に鍵生成アルゴリズムを実行することによって、第１の非対称鍵ペアを形成するステップであって、前記値に前記鍵生成アルゴリズムを実行することにより、同一の出力が得られる、ステップと、
前記パスワード保護モジュールが、前記第１の非対称鍵ペアの公開鍵に基づいて、自己署名した擬似公開鍵証明書を生成するステップであって、前記擬似公開鍵証明書は、公開鍵インフラストラクチャ（ＰＫＩ）のフォーマットを有するが、ＰＫＩ証明書サーバによって発行されていない、ステップと、
前記パスワード保護モジュールが、前記擬似公開鍵証明書を認証サーバにエクスポートするステップと、
前記パスワード保護モジュールが、認証セッションに応答して、ディジタル署名ログインプロセスの一部として前記鍵生成計アルゴリズムを実行することによって、第２の非対称鍵ペアを形成し、前記第２の非対称鍵ペアの秘密鍵を使用して前記認証サーバに対する認証を行うステップであって、前記第１の非対称鍵ペアの秘密鍵と前記第２の非対称鍵ペアの秘密鍵は同一である、ステップと
を実行させるためのプログラムを記録したことを特徴とするコンピュータ可読記録媒体。
【請求項９】
前記非対称鍵ペアは、ディフィー－ヘルマン、ＲＳＡ、ＤＳＡ、または非対称鍵ペアを生成するのに適した任意のその他のアルゴリズムに基づくことを特徴とする請求項８に記載のコンピュータ可読記録媒体。
【請求項１０】
前記パスワードは、平文パスワードであることを特徴とする請求項８に記載のコンピュータ可読記録媒体。
【請求項１１】
前記パスワードは、暗号化鍵交換プロトコルに応じて生成された弱いパスワードである

ことを特徴とする請求項８に記載のコンピュータ可読記録媒体。
【請求項１２】
前記他のデータは、ユーザプリンシパル名またはユーザに実質的に固有のその他の値であることを特徴とする請求項８に記載のコンピュータ可読記録媒体。
【請求項１３】
パスワードと他のデータとを連結するステップは、前記パスワードと前記他のデータとを暗号関数を介して組み合わせるステップを含むことを特徴とする請求項８に記載のコンピュータ可読記録媒体。
【請求項１４】
値を生成するステップは、前記連結したパスワードと前記他のデータに基づいて擬似乱数を生成するステップを含むことを特徴とする請求項８に記載のコンピュータ可読記録媒体。
【請求項１５】
プロセッサと、
前記プロセッサに結合され、前記プロセッサによって実行可能なコンピュータプログラム命令であって、
パスワードと他のデータとを連結するための命令と、
前記連結したパスワードと他のデータに基づいて値を生成するための命令と、
前記値に鍵生成アルゴリズムを実行することによって、第１の非対称鍵ペアを形成するための命令であって、前記値に前記鍵生成アルゴリズムを実行することにより、同一の出力が得られる、命令と、
前記第１の非対称鍵ペアの公開鍵に基づいて、自己署名した擬似公開鍵証明書を生成するためのコンピュータプログラム命令であって、前記擬似公開鍵証明書は、公開鍵インフラストラクチャ（ＰＫＩ）のフォーマットを有するが、ＰＫＩ証明書サーバによって発行されていない、命令と、
前記擬似公開鍵証明書を認証サーバにエクスポートするための命令と、
認証セッションに応答して、ディジタル署名ログインプロセスの一部として前記鍵生成計アルゴリズムを実行することによって、第２の非対称鍵ペアを形成し、前記第２の非対称鍵ペアの秘密鍵を使用して前記認証サーバに対する認証を行うための命令であって、前記第１の非対称鍵ペアの秘密鍵と前記第２の非対称鍵ペアの秘密鍵は同一である、命令と
を備えたメモリと
を備えたことを特徴とするコンピューティングデバイス。
【請求項１６】
前記非対称鍵ペアは、ディフィーヘルマン、ＲＳＡ、ＤＳＡ、または非対称鍵ペアを生成するのに適した任意のその他のアルゴリズムに基づくことを特徴とする請求項１５に記載のコンピューティングデバイス。
【請求項１７】
前記パスワードは、平文パスワードであることを特徴とする請求項１５に記載のコンピューティングデバイス。
【請求項１８】
前記パスワードは、暗号化鍵交換プロトコルに応じて生成された弱いパスワードであることを特徴とする請求項１５に記載のコンピューティングデバイス。
【請求項１９】
前記他のデータは、ユーザプリンシパル名またはユーザに実質的に固有のその他の値であることを特徴とする請求項１５に記載のコンピューティングデバイス。
【請求項２０】
パスワードと他のデータとを連結するための前記コンピュータプログラム命令は、前記パスワードと前記他のデータとを暗号関数を介して組み合わせるための命令を含むことを特徴とする請求項１５に記載のコンピューティングデバイス。

【請求項２１】
値を生成するための前記コンピュータプログラム命令は、前記連結したパスワードと前記他のデータに基づいて擬似乱数発を生成するための命令を含むことを特徴とする請求項１５に記載のコンピューティングデバイス。
【請求項２２】
パスワードと他のデータとを連結する連結手段と、
前記連結したパスワードと他のデータに基づいて値を生成する生成手段と、
前記値に鍵生成アルゴリズムを実行することによって、第１の非対称鍵ペアを形成する形成手段であって、前記値に前記鍵生成アルゴリズムを実行することにより、同一の出力が得られる、形成手段と、
前記第１の非対称鍵ペアの公開鍵に基づいて、自己署名した擬似公開鍵証明書を生成する生成手段であって、前記擬似公開鍵証明書は、公開鍵インフラストラクチャ（ＰＫＩ）のフォーマットを有するが、ＰＫＩ証明書サーバによって発行されていない、生成手段と、
前記擬似公開鍵証明書を認証サーバにエクスポートするエクスポート手段と、
認証セッションに応答して、ディジタル署名ログインプロセスの一部として前記鍵生成計アルゴリズムを実行することによって、第２の非対称鍵ペアを形成し、前記第２の非対称鍵ペアの秘密鍵を使用して前記認証サーバに対する認証を行う認証手段であって、前記第１の非対称鍵ペアの秘密鍵と前記第２の非対称鍵ペアの秘密鍵は同一である、認証手段と
を備えたことを特徴とするコンピューティングデバイス。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、パスワードの保護および認証に関する。
【背景技術】
【０００２】
セキュリティに対応したオペレーティングシステムは、ユーザを認証する能力を必要とする。ユーザ認証はいくつかの方法で行うことができる。ユーザ認証は、その最も単純な形態では、ユーザ認証子とユーザ識別の何らかの組合せに基づいている。ユーザ認証子は、パスワードなど、ユーザの知っている固有のものから得られる。より最近の洗練された多層の認証機構（ｍｕｌｔｉ－ｆａｃｔｏｒ ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｍｅｃｈａｎｉｓｍｓ）はまた、ユーザの有しているもの（通常は、何らかの形態のハードウェアで表されるトークン）、ユーザの何か（指紋や網膜パターンなどの生体認証子）、またはこの３つの何らかの組合せにも依拠している。しかし、このような多層の認証システムにおいても、特定のオペレーションにはパスワードが使用され、したがってパスワードを管理および格納する必要がある。パスワード、またはパスワードから派生する何らかの表現を格納することは、難しい問題である。
【０００３】
パスワードの格納には様々な技法が使用されてきたが、すべての技法はいくつかの弱点を有し、こうした弱点によりこれらの技法は、格納されたパスワードに対する攻撃がより洗練され攻撃者に利用可能なコンピュータハードウェアがより高速になるにつれて、適さないものになる。例えば、パスワードを格納する最も単純なスキームの１つは、単にパスワード自体を格納することである。しかし、このようなシナリオでは、パスワードのリストをうまく入手した攻撃者は、すぐにすべてのパスワードを使用することができる。このような制止されないアクセスに対抗するために、システムは、Ｒｏｔ－１３やＢａｓｅ－６４に基づく操作などの単純な数学的な操作でパスワードを不明化しようとした。あるいは、固定鍵を使用してパスワードを暗号化した。しかし、格納されたパスワードへのアクセスを有し、アルゴリズムまたは固定鍵の知識を有する者なら誰でも、簡単に平文パスワードを決定できるので、これらの技法は簡単に可逆となる。

【０００４】
より洗練された一方向暗号関数（ＯＷＦ：ｏｎｅ－ｗａｙ　ｃｒｙｐｔｏｇｒａｐｈｉｃ　ｆｕｎｃｔｉｏｎ）が、上で論じた弱点に対応するために導入された。ＯＷＦは、暗号アルゴリズムを使用して、パスワードを不明化し格納する。格納されたパスワードに関する最も共通するタイプの攻撃は、ブルートフォース攻撃、または辞書／ブルートフォースの何らかのタイプのハイブリッド攻撃であり、この場合、攻撃者はパスワードを推測し、適切なＯＷＦを用いてパスワードを符号化し、それを格納された値と比較しなければならない。この２つがマッチした場合は、正しいパスワードが見つかったことになる。残念ながら、いくつかのＯＷＦパスワード暗号化アルゴリズムは、今日では暗号的に安全ではなく、その他のアルゴリズムは、今日では暗号的に安全と考えられるものの、近い将来には安全でなくなる可能性が高い。特に、分散型の協調した攻撃を考えるとそうである。
【０００５】
従来のＯＷＦパスワード不明化技法（ＯＷＦ　ｐａｓｓｗｏｒｄ　ｏｂｆｕｓｃａｔｉｏｎ　ｔｅｃｈｎｉｑｕｅｓ）は、他の理由でも、パスワードを安全に格納する能力がかなり限られている。最も重要な問題は、格納された認証子（パスワードハッシュ）が、ユーザを認証するのに使用されるのと同じ値であるということである。言い換えれば、唯一の秘密は認証子、すなわちパスワード表現またはハッシュであり、それが表すパスワードではない。論考の目的で、用語「ハッシュ」は、パスワードが不明化されているか否かにかかわらず、格納されたパスワード表現を指すのに使用する。
【発明の開示】
【発明が解決しようとする課題】
【０００６】
一線式のパスワード認証アルゴリズム（ｏｎｅ－ｗｉｒｅ　ｐａｓｓｗｏｒｄ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ）は、探知され、クラックされることがある。ネットワーク上の認証シーケンスは、捕捉され、パスワードの判定またはクラックするのに使用される可能性がある。捕捉された情報はパスワード表現自体に対してさらにもう１つの暗号変換を経ているので、このような攻撃を仕掛けるのは難しい。しかし、暗号的に安全な格納アルゴリズムを使用することは可能だが、一線式のアルゴリズムは、格納された値のブルートフォーシングに対して脆弱なままとなる。そしてこの値が、上の段落で述べたように平文パスワードの代わりに使用される可能性がある。
【課題を解決するための手段】
【０００７】
パスワード保護のためのシステムおよび方法について説明する。一態様では、パスワードと他のデータを組み合わせることによって、非対称鍵ペアを決定論的に形成する。非対称鍵ペアの公開鍵を外部デバイスにエクスポートする。非対称鍵ペアの秘密鍵を使用して、外部デバイスに対する後続の認証を実効する。
【０００８】
図面において、構成要素の参照番号の左端の桁は、その構成要素が最初に現れる特定の図を識別している。
【発明を実施するための最良の形態】
【０００９】
（概要）
従来のほぼすべてのパスワード格納システムは、単純な攻撃の対象となる。例えば、ソルト（ｓａｌｔ）されていないパスワードハッシュは、事前に計算されたハッシュ攻撃に対して脆弱である。この攻撃では、攻撃者は、いくつかのパスワードに対応するパスワードハッシュのセットを事前に計算する（ソルトは、短い値を取って、ハッシュに先立ってそれをパスワードに加えるプロセスである）。次いで、セキュリティが破られ、パスワードデータベースが得られると、盗んだハッシュを事前に計算したハッシュと比較して、基礎をなすパスワードを数秒で得ることができる。基本的に、これは「一度クラックすればどこでも使える（ｃｒａｃｋ　ｏｎｃｅ，ｕｓｅ　ｅｖｅｒｙｗｈｅｒｅ）」攻撃であり

、一方、従来のパスワード攻撃は、パスワードを推測し、ハッシュを実行時に計算することに基づいている。

【００１０】

いくつかのケースでは、攻撃者は、システムを危険にさらすためにパスワードを実際にリバースエンジニアリングする必要はない。一部には、これは、格納されたパスワードを表すハッシュを攻撃者が直接使用することができる既存のチャレンジレスポンスプロトコル（ｃｈａｌｌｅｎｇｅ　ｒｅｓｐｏｎｓｅ　ｐｒｏｔｏｃｏｌ）の構造のためである。ハッシュを直接使用するパスワード攻撃は、「パスザハッシュ（ｐａｓｓ－ｔｈｅ－ｈａｓｈ）」攻撃として知られている。これらは、チャレンジレスポンス認証システム中では使用される秘密はハッシュだけであるという基本的な事実に依拠している。ハッシュを有する攻撃者は、ハッシュを、認証チャレンジに正しく応答し、このハッシュで表されるパスワードのユーザとして認証するツール中で使用することができる。近年のほぼすべてのコンピュータ認証システムは、パスザハッシュ攻撃の対象となり、いくつかのシステムは、他のシステムよりもずっと脆弱である。「パスザハッシュ」攻撃は、ハッシュを得るのに必要な計算を超える計算を行うどんな必要からも完全に独立している。したがって、また、パスワード格納システムがパスワード自体と同じくらい安全であるという従来の想定とは対照的に、パスワード格納システムはパスワード自体ほど安全ではない。攻撃者がハッシュにアクセスできる場合、強いパスワードは、弱いパスワードに勝る何らの追加的なセキュリティも提供しない。これが発生すると、すべてのパスワードハッシュは、それらが表す平文パスワードと等化である。

【００１１】

Ｒａｉｎｂｏｗ　Ｃｒａｃｋなどの新たに出現したツールが、既存のパスワード格納アルゴリズムの弱点を際立たせるために広く使用されている。Ｒａｉｎｂｏｗ　Ｃｒａｃｋは、パスワードをクラックするためにすべてのハッシュを実行時に計算する代わりにハッシュを事前に計算することができるという古い考え方を最適化した、自由に利用可能な一実装である。実行時に、盗んだハッシュを格納されたものと比較することができ、単純な検索によってマッチメークすることができる。より多くの人が、パスワードがどのようにして格納され、使用されるかを調べ始めているので、より多くの労力がこれらのタイプの攻撃に費やされるかもしれないと想定するのは論理的である。現在、ハッシュにアクセスできる攻撃者に対して、このようなパスワード攻撃を打ち負かす唯一の知られている方法は、スマートカードまたはトークンベースの認証システムの使用によるものである。しかし、スマートカードの実装形態を構築することの実装上の困難は、スマートカードが完全にパスワードに取って代わることは当面ないことを意味している。

【００１２】

パスワード保護のための以下のシステムおよび方法は、例えば、暗号的に安全な公開鍵を使用することにより、特定ユーザについて格納されたものがそのユーザの認証に使用されることになるものとは異なるようにすることによって、従来のパスワード格納技法に関して前述した弱点のそれぞれに対処する。パスワード保護のためのシステムおよび方法についてのこれらおよび他の態様を、次に図１から４に関してより詳細に説明する。

【００１３】

（例示的なシステム）

図１に、パスワード保護のための例示的なシステム１００を示す。コンピューティングシステム１００はコンピューティングデバイス１０２を含み、このデバイスは、プログラムモジュール１０４、およびプログラムデータ１０６を含む。プログラムモジュール１０４は、例えばパスワード保護モジュール１０８を含む。パスワード保護モジュール１０８は、信用機構（ｔｒｕｓｔ　ｍｅｃｈａｎｉｓｍ）の必要のない擬似証明書ソリューション（ｐｓｅｕｄｏ－ｃｅｒｔｉｆｉｃａｔｅ　ｓｏｌｕｔｉｏｎ）を実装して、パスワード１１２から格納されたパスワード表現１１０を生成する。擬似証明書ソリューションは、本当の公開鍵インフラストラクチャ（ＰＫＩ）と区別するためにこのように名付けられている。ＰＫＩでは、すべての証明書は証明書サーバによって発行され、証明書サーバに

よって署名されて、認証性および妥当性が証明される。証明書サーバの証明書はそれ自体、別の証明書サーバによって発行することができるので、全システムが、ツリーの形態をとる信用階層を生成する。システムのあるエージェントがツリーの特定のノードを信用すると、このエージェントはまた、ツリーの中でこの信用されるノードよりも下にある何らかのエンティティによって発行された証明書のどんな者も信用することになる。システム１００の擬似証明書の実装形態では、証明書はこのような中央権限から発するのではなく、また証明書サーバによって署名されることもない。証明書は、ＰＫＩで使用されるのと同じ形態をとるが、これは単に、公開暗号鍵と秘密暗号鍵のセットをパッケージするのに都合のよい方法にすぎない。しかし、公開鍵と秘密鍵のペアを証明書に格納することによって、１つの特異な利点が得られる。すなわち、我々のシステムは、ＰＫＩ用に設計されたすべての既存の認証システムを生成することができるという利点である。証明書は自己署名され、したがって、信用階層の一部ではないことは別として、ＰＫＩでの使用に完全に有効である。

【００１４】

システム１００は、１０２４ビット、２０４８ビット、４０９６ビットセキュリティなど、鍵の長さとして定義されるセキュリティのレベルを実装する。鍵を生成するために、パスワード保護モジュール１０８は、ユーザ識別子（例えばユーザプリンシパル名（ＵＰＮ）やその他何らかの任意のユーザに関連付けられたデータ）を平文パスワード１１２と組み合わせる。この組合せは、単純な連結からなるものとしたり、この２つに暗号ハッシュを適用するなど、任意の数のその他のプロセスからなるものとしたりすることができる。説明の目的で、このオペレーションの結果を「その他のデータ」１１４の「組合せ結果」として示す。一実装形態では、ｅメールアドレスフォーマットのシステムユーザの名前（ＵＰＮ）が、ユーザ識別子として使用される。別の実装形態では、ユーザ識別子は、システムユーザを表す任意の値である。その使用がシステム内で一貫しており、例示的なシステムがすべての可能な値を許容する限り、具体的な値は問題ではない。２人のユーザのパスワードが同一であっても２人が同じ格納されたパスワード値を持たないようにするために、ユーザ識別子を使用してパスワードをソルトする。

【００１５】

パスワード保護モジュール１０８は、上記の組合せ結果を使用して、秘密鍵および関連する公開鍵を生成する。一実装形態では、パスワード保護モジュール１０８は、組合せ結果を秘密の鍵ｘとして使用し、関連するディフィーヘルマン（Ｄｉｆｆｉｅ－Ｈｅｌｌｍａｎ）公開鍵を$y = g^x \mod p$として計算する。ここで、ｇおよびｐは利用されるビットセキュリティのレベル（例えば１０２４ビット、２０４８ビットなど）に対応するビット長の整数である。これらの整数は所定またはランダムとすることができる。一実装形態では、整数は、システム１００にわたって様々な鍵の長さの使用を許容するために公開鍵証明書１２０の一部である。ＲＳＡ、ＤＳＡ、楕円曲線法など、その他の鍵生成手法を使用することもできよう。

【００１６】

一実装形態では、パスワード保護モジュール１０８は、ｙをユーザの公開鍵として使用し、任意選択でパラメータｇおよびｐを含む所望の任意の公開鍵証明書フォーマットを使用して公開鍵証明書１２０を作成する。公開鍵証明書は、ユーザまたはエンティティに関連付けられたデータのディジタル署名と共に、人名／ｅメールアドレス／肩書／電話番号、および／またはその他などの識別情報と共に、非対称鍵ペアの公開部分（「公開鍵」）を指定のフォーマットに収容する構造である。公開鍵証明書は、識別証明書とも呼ばれる。公開鍵証明書は、認証サーバに格納される。このような認証サーバの例を、図４のリモートコンピュータ４８０として示す。任意のディレクトリまたはユーザ識別システムを使用して、この公開鍵証明書を格納することができる。パスワード保護モジュール１０８は、公開鍵証明書１２０を利用して、手持ちのシステム中で証明書ベースの認証の確立された規則に従って、ユーザ／エンティティを認証する。このような認証セッションの例を、以下に図２を参照しながら説明する。

【００１７】
（例示的な手順）
図２に、パスワード保護のための例示的な手順を示す。例示的な説明のために、図２の操作を図１のコンポーネントに関して説明する（図面において、構成要素の参照番号の左端の桁は、その構成要素が最初に現れる特定の図を識別する）。ブロック２０２で、パスワード保護モジュール１０８（図１）は、ユーザ識別子を平文パスワード１１２と組み合わせる。説明のために、このオペレーションの結果を「その他のデータ」１１４の「組合せ結果」として示している。ユーザ識別子の使用は、同じパスワードを有する２人のユーザが異なる鍵を得るようにするためのソルトとして働く。ブロック２０４で、パスワード保護モジュール１０８は、組合せ結果から非対称鍵ペア１１８（公開鍵と秘密鍵のペア）を決定論的に生成する。すなわち、このプロセスは、同じ入力で同じ方式を繰り返すことができ、同じ出力に達する。
【００１８】
より詳しくは、パスワード保護モジュール１０８は、ディフィー－ヘルマン公開鍵$y = g^x \bmod p$など、秘密データから公開鍵を計算する。他の実施形態では、非対称鍵生成プロセスの一部として、組合せデータを使用して擬似乱数発生器に決定論的にシードを提供することができる。
【００１９】
ブロック２０６で、パスワード保護モジュール１０８は、非対称鍵ペア１１８の公開鍵を、図４のリモートコンピュータ４８０によって表されるような外部デバイスにエクスポートする。ブロック２０８で、非対称鍵ペアの秘密鍵を使用して、外部デバイスに対する後続の認証を実効する。認証は、任意のタイプの公開鍵ベースの認証方式に基づく。
【００２０】
例えば、このパスワード保護のためのシステムおよび方法は、ベロヴィン／メリット（Ｂｅｌｌｏｖｉｎ／Ｍｅｒｒｉｔｔ）暗号化鍵交換（ＥＫＥ：Ｅｎｃｒｙｐｔｅｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ）プロトコルと共に使用することができる。まず、ＥＫＥプロトコルのディフィー－ヘルマンバージョンと、それが達成するものについて説明する。クライアントとサーバが、公開の素数モジュラスｐおよび公開のジェネレータｇについて合意していると想定する。クライアントは、ランダムな値Ａを選択し、一時的なディフィー－ヘルマン値$X = g^A \bmod p$を生成し、この値Ｘをサーバに送ることによって開始する。サーバは、ランダムな値Ｂを生成し、$Y = g^B \bmod p$を形成し、これを、クライアントによって復号できるように暗号化する。すなわちＺ＝Ｅ（Ｙ）とする。サーバは、強い共有鍵$K = X^B \bmod p$も計算する。
【００２１】
サーバは、ランダムなノンスＢ’を生成し、これを強い対称鍵Ｋで暗号化して、Ｕ＝Ｋ（Ｂ’）を形成する（やや表記法を乱用している）。サーバは、ＺおよびＵをクライアントに送る。クライアントは、Ｚを復号してＹを得て、同じ強い共有鍵Ｋを$K = Y^A \bmod p$として計算する。次いでクライアントは、ランダムなノンスＡ’を生成し、Ｖ＝Ｋ（Ａ’，Ｂ’）をサーバに送る。サーバはＶを復号し、Ｂ’が正しいことをチェックする。Ｂ’が正しいと仮定すると、サーバはＷ＝Ｋ（Ａ’）をクライアントに送る。クライアントはＷを復号し、Ａ’が正しいことをチェックする。Ａ’が正しいと仮定すると、強い共有Ｋは今や認証されており、後続の通信に使用することができる。前２つの段落で、強い共有鍵Ｋを生成するためディフィー－ヘルマン鍵交換を、その最も単純な形で説明した。ＥＫＥの従来の使用は、クライアントとサーバが弱いパスワードだけを共有するときであり、暗号化（Ｚ＝Ｅ（Ｙ））は通常、弱いパスワードを鍵として使用する対称暗号で行われる。ノンスを介して継続することで、ＥＫＥが弱いパスワードに関するオフライン攻撃を防止することが明らかである。
【００２２】
上記に照らして、また一実装形態では、パスワード１１２は弱いパスワードであり、システム１００は、弱いパスワード１１２から非対称鍵ペア１１８を生成することによって

ＥＫＥを実施する。

【００２３】

図３に、図１の非対称鍵ペアに基づく公開／秘密鍵証明書を作成し使用して証明書ベースのログオンを実行するための例示的な手順を示す。例示的な説明のために、図３の操作を図１のコンポーネントに関して説明する（図面において、構成要素の参照番号の左端の桁は、その構成要素が最初に現れる特定の図を識別する）。ブロック３０２で、パスワード保護モジュール１０８は、ｙをユーザの公開鍵として使用して、所望の任意の公開鍵証明書フォーマットを使用した公開鍵証明書１２０を作成する。ブロック３０４で、パスワード保護モジュール１０８は、公開鍵証明書１２０を認証サーバに格納する。ブロック３０６で、認証セッションの間に、パスワード保護モジュール１０８は、オペレーション２０２から２０６を実行することによって、公開－秘密鍵ペア１１８を計算する。ブロック３０８で、パスワード保護モジュール１０８は、従来のディジタル証明書で使用されるであろうものと同一の認証ログオンプロセスを実行する。これは技術的には、利用可能な任意の証明書ベースのログオン技法を用いて実行することができる。一実装形態では、証明書ベースのログオン技法はディジタル署名アルゴリズム（ＤＳＡ：Ｄｉｇｉｔａｌ　Ｓｉｇｎａｔｕｒｅ　Ａｌｇｏｒｉｔｈｍ）機構である。

【００２４】

（例示的な動作環境）

必須ではないが、このパスワード保護のためのシステムおよび方法を、パーソナルコンピュータによって実行されるコンピュータ実行可能命令（プログラムモジュール）の一般的なコンテキストで説明する。プログラムモジュールは一般に、特定のタスクを実行するか特定の抽象データ型を実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。このシステムおよび方法を前述のコンテキストで説明するが、以下に述べる動作および操作はハードウェア中で実施することもできる。

【００２５】

図４に、完全にまたは部分的に実施することのできるパスワード保護のための適切なコンピューティング環境の例を示す。例示的なコンピューティング環境４００は、図１の例示的なシステムならびに図２および３の例示的な操作のための適切なコンピューティング環境の一例にすぎず、ここに述べるシステムおよび方法の使用または機能の範囲についていかなる限定を意味するものではない。またコンピューティング環境４００は、コンピューティング環境４００に示すコンポーネントのいずれか１つまたは組合せに関していかなる依存や要件を有するものと解釈すべきでもない。

【００２６】

本明細書で説明した方法およびシステムは、多くの他の汎用または専用コンピューティングシステム、環境、または構成で機能する。使用に適する可能性のある周知のコンピューティングシステム、環境、および／または構成の例には、限定しないがパーソナルコンピュータ、サーバコンピュータ、マルチプロセッサシステム、マイクロプロセッサベースのシステム、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータや、これらのシステムまたはデバイスのいずれかを含む分散コンピューティング環境などが含まれる。ハンドヘルドコンピュータやその他のコンピューティングデバイスなど、リソースの限られたクライアントで、このフレームワークのコンパクトなまたはサブセットのバージョンを実施することもできる。本発明は、タスクが通信ネットワークを介してリンクされたリモート処理デバイスによって実行される分散コンピューティング環境で実施される。分散コンピューティング環境では、プログラムモジュールは、ローカルとリモートの両方のメモリ記憶デバイスに位置することができる。

【００２７】

図４を参照すると、パスワード保護のための例示的なシステムは、例えば図１のシステム１００を実装するコンピュータ４１０の形態の汎用コンピューティングデバイスを含む。以下に述べるコンピュータ４１０の態様は、図１のクライアントコンピューティングデバイス１０２の例示的な実装形態である。コンピュータ４１０のコンポーネントには、限

定しないが、処理ユニット４２０と、システムメモリ４３０と、システムメモリを含む様々なシステムコンポーネントを処理ユニット４２０に結合するシステムバス４２１とを含むことができる。システムバス４２１は、様々なバスアーキテクチャのいずれかを用いた、メモリバスまたはメモリコントローラ、周辺バス、ローカルバスを含め、いくつかのタイプのバス構造のいずれかとすることができる。限定ではなく例として、このようなアーキテクチャには、ＩＳＡ（Ｉｎｄｕｓｔｒｙ Ｓｔａｎｄａｒｄ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＭＣＡ（Ｍｉｃｒｏ Ｃｈａｎｎｅｌ Ａｒｃｈｉｔｅｃｔｕｒｅ）バス、ＥＩＳＡ（Ｅｎｈａｎｃｅｄ ＩＳＡ）バス、ＶＥＳＡ（Ｖｉｄｅｏ Ｅｌｅｃｔｒｏｎｉｃｓ Ｓｔａｎｄａｒｄｓ Ａｓｓｏｃｉａｔｉｏｎ）ローカルバス、ＰＣＩ（Ｐｅｒｉｐｈｅｒａｌ Ｃｏｍｐｏｎｅｎｔ Ｉｎｔｅｒｃｏｎｎｅｃｔ）バス（メザニンバスとも呼ばれる）などを含むことができる。

【００２８】

コンピュータ４１０は通常、様々なコンピュータ可読媒体を含む。コンピュータ可読媒体は、コンピュータ４１０によってアクセスできる任意の利用可能な媒体とすることができ、揮発性と不揮発性の媒体、リムーバブルと非リムーバブルの媒体の両方が含まれる。限定ではなく例として、コンピュータ可読媒体には、コンピュータ記憶媒体および通信媒体を含むことができる。コンピュータ記憶媒体には、コンピュータ可読命令、データ構造、プログラムモジュール、その他のデータなどの情報を格納するための任意の方法または技術で実現された、揮発性と不揮発性、リムーバブルと非リムーバブルの媒体を含む。コンピュータ記憶媒体には、限定しないがＲＡＭ、ＲＯＭ、ＥＥＰＲＯＭ、フラッシュメモリまたはその他のメモリ技術、ＣＤ－ＲＯＭ、ディジタル多用途ディスク（ＤＶＤ）またはその他の光ディスクストレージ、磁気カセット、磁気テープ、磁気ディスクストレージまたはその他の磁気記憶デバイスが含まれ、または所望の情報を格納するのに使用できコンピュータ４１０によってアクセスできるその他の任意の媒体が含まれる。

【００２９】

通信媒体は通常、コンピュータ可読命令、データ構造、プログラムモジュール、またはその他のデータを、搬送波またはその他のトランスポート機構などの変調データ信号に具現するものであり、任意の情報送達媒体が含まれる。用語「変調データ信号」は、信号中に情報を符号化するように１つまたは複数の特性を設定または変更した信号を意味する。限定ではなく例として、通信媒体には、有線ネットワークや直接配線接続などのワイヤ媒体と、音響、無線周波数、赤外線などのワイヤレス媒体およびその他のワイヤレス媒体とが含まれる。以上のいずれかの組合せもコンピュータ可読媒体の範囲に含まれるべきである。

【００３０】

システムメモリ４３０は、読取り専用メモリ（ＲＯＭ）４３１やランダムアクセスメモリ（ＲＡＭ）４３２など、揮発性および／または不揮発性メモリの形態のコンピュータ記憶媒体を含む。ＲＯＭ４３１には通常、起動中などにコンピュータ４１０内の要素間で情報を転送するのを助ける基本ルーチンが入ったＢＩＯＳ（ｂａｓｉｃ ｉｎｐｕｔ／ｏｕｔｐｕｔ ｓｙｓｔｅｍ）４３３が格納されている。ＲＡＭ４３２は通常、処理ユニット４２０によってすぐにアクセス可能で、そして／または現在操作されている、データおよび／またはプログラムモジュールを収容する。限定ではなく例として、図４は、オペレーティングシステム４３４、アプリケーションプログラム４３５、その他のプログラムモジュール４３６、プログラムデータ４３７を示している。

【００３１】

コンピュータ４１０は、その他のリムーバブル／非リムーバブル、揮発性／不揮発性コンピュータ記憶媒体を含むこともできる。例にすぎないが図４には、非リムーバブルな不揮発性の磁気媒体に対して読み書きするハードディスクドライブ４４１と、リムーバブルな不揮発性の磁気ディスク４５２に対して読み書きする磁気ディスクドライブ４５１と、ＣＤ ＲＯＭやその他の光媒体などリムーバブルな不揮発性の光ディスク４５６に対して読み書きする光ディスクドライブ４５５を示している。この例示的な動作環境で使用でき

るその他のリムーバブル／非リムーバブル、揮発性／不揮発性コンピュータ記憶媒体には、限定しないが磁気テープカセット、フラッシュメモリカード、ディジタル多用途ディスク、ディジタルビデオテープ、半導体ＲＡＭ、半導体ＲＯＭなどが含まれる。ハードディスクドライブ４４１は通常、インタフェース４４０などの非リムーバブルメモリインタフェースを介してシステムバス４２１に接続され、磁気ディスクドライブ４５１および光ディスクドライブ４５５は通常、インタフェース４５０などのリムーバブルメモリインタフェースでシステムバス４２１に接続される。

【００３２】

以上に論じ図４に示したドライブおよびそれらに関連するコンピュータ記憶媒体は、コンピュータ４１０のコンピュータ可読命令、データ構造、プログラムモジュール、その他のデータのストレージを提供する。例えば図４には、ハードディスクドライブ４４１がオペレーティングシステム４４４、アプリケーションプログラム４４５、その他のプログラムモジュール４４６、プログラムデータ４４７を格納しているのが示されている。これらのコンポーネントは、オペレーティングシステム４３４、アプリケーションプログラム４３５、その他のプログラムモジュール４３６、プログラムデータ４３７と同じものとすることも、異なるものとすることもできることに留意されたい。アプリケーションプログラム４３５は、例えば図１のプログラムモジュール１０４を含む。プログラムデータ４３７は、例えば図１のプログラムデータ１０６を含む。ここでは、オペレーティングシステム４４４、アプリケーションプログラム４４５、その他のプログラムモジュール４４６、プログラムデータ４４７が少なくとも異なるコピーであることを示すために、異なる番号を付けてある。

【００３３】

一実装形態では、ユーザは、キーボード４６２、マウスやトラックボールやタッチパッドと一般に呼ばれるポインティングデバイス４６１などの入力デバイスを介して、コンピュータ４１０にコマンドおよび情報を入力することができる。その他の入力デバイス（図示せず）には、マイクロフォン、ジョイスティック、ゲームパッド、衛星アンテナ、スキャナなどを含めることができる。これらおよび他の入力デバイスは、システムバス４２１に結合されたユーザ入力インタフェース４６０を介して処理ユニット４２０に接続されることが多いが、パラレルポート、ゲームポート、１３９４／Ｆｉｒｅｗｉｒｅ、ＡＧＰ（ａｃｃｅｌｅｒａｔｅｄ ｇｒａｐｈｉｃｓ ｐｏｒｔ）、ユニバーサルシリアルバス（ＵＳＢ）など、その他のインタフェースおよびバス構造で接続されてもよい。

【００３４】

コンピュータ４１０は、リモートコンピュータ４８０など１つまたは複数のリモートコンピュータへの論理接続を用いて、ネットワーク化された環境で動作する。リモートコンピュータ４８０は、パーソナルコンピュータ、サーバ、ルータ、ネットワークＰＣ、モバイルコンピューティングデバイス、ピアデバイス、またはその他の一般的なネットワークノードとすることができ、図４にはメモリ記憶デバイス４８１だけが示してあるが、その特定の実装形態に応じて、コンピュータ４１０に関して上述した要素の多くまたはすべてを含むことができる。図４に示す論理接続は、ローカルエリアネットワーク（ＬＡＮ）４７１およびワイドエリアネットワーク（ＷＡＮ）４７３を含むが、その他のネットワークを含むこともできる。このようなネットワーキング環境は、オフィス、企業全体のコンピュータネットワーク、イントラネット、インターネットでよくみられる。

【００３５】

ＬＡＮネットワーキング環境で使用されるとき、コンピュータ４１０は、ネットワークインタフェースまたはアダプタ４７０を介してＬＡＮ４７１に接続される。ＷＡＮネットワーキング環境で使用されるとき、コンピュータ４１０は通常、インターネットなどのＷＡＮ４７３を介して通信を確立するためのモデム４７２またはその他の手段を含む。モデム４７２は内蔵でも外付けでもよく、ユーザ入力インタフェース４６０またはその他の適切な機構を介してシステムバス４２１に接続することができる。ネットワーク化された環境では、コンピュータ４１０に関して示したプログラムモジュールまたはその一部をリモ

ートのメモリ記憶デバイスに記憶することができる。限定ではなく例として、図４には、リモートアプリケーションプログラム４８５がメモリデバイス４８１上にあるのが示されている。図示したネットワーク接続は例示的なものであり、コンピュータ間で通信リンクを確立するための他の手段を使用することもできる。

【００３６】

（結び）

パスワード保護のためのシステムおよび方法について、構造上の特徴および／または方法上のオペレーションもしくは動作に特有の言葉で説明したが、添付の請求項で定義される実装形態は、説明した特定の特徴または動作に必ずしも限定されないことを理解されたい。したがって、これらの具体的な特徴および動作は、特許請求の範囲に記載された主題を実現する例示的な形態として開示されている。

【図面の簡単な説明】

【００３７】

【図１】パスワード保護のための例示的なシステムを示す図である。

【図２】パスワード保護のための例示的な手順を示す図である。

【図３】ディジタル署名ログオン操作のための公開鍵および秘密鍵証明書を生成するための例示的な手順を示す図である。

【図４】パスワード保護を完全にまたは部分的に実施することのできる適切なコンピューティング環境の一例を示す図である。

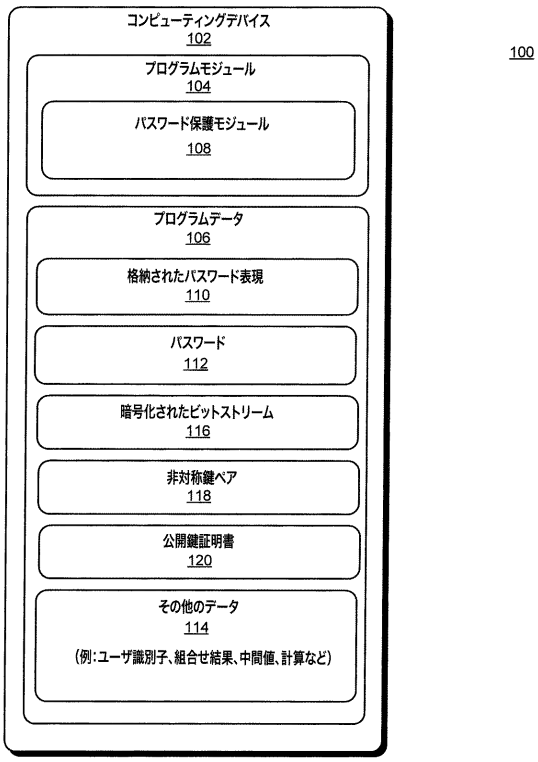
【符号の説明】

【００３８】

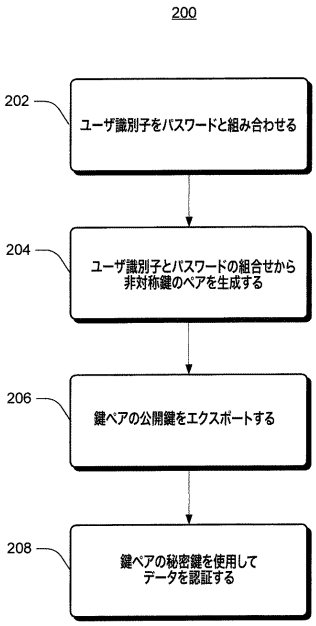
１００　コンピューティングシステム
１０２　コンピューティングデバイス
１０４　プログラムモジュール
１０６　プログラムデータ
１０８　パスワード保護モジュール
１１０　格納されたパスワード表現
１１２　パスワード
１１４　その他のデータ
１１６　暗号化されたビットストリーム
１１８　非対称鍵のペア
１２０　公開鍵証明書
４００　コンピューティング環境
４１０　コンピュータ
４２０　処理ユニット
４２１　システムバス
４３０　システムメモリ
４３１　ＲＯＭ
４３２　ＲＡＭ
４３３　ＢＩＯＳ
４３４　オペレーティングシステム
４３５　アプリケーションプログラム
４３６　その他のプログラムモジュール
４３７　プログラムデータ
４４０　非リムーバブル不揮発性メモリインタフェース
４４１　ハードディスクドライブ
４４４　オペレーティングシステム
４４５　アプリケーションプログラム
４４６　その他のプログラムモジュール
４４７　プログラムデータ

４５０　リムーバブル不揮発性メモリインタフェース
４５１　磁気ディスクドライブ
４５２　磁気ディスク
４５５　光ディスクドライブ
４５６　光ディスク
４６０　ユーザ入力インタフェース
４６１　マウス
４６２　キーボード
４７０　ネットワークインタフェース
４７１　ローカルエリアネットワーク
４７２　モデム
４７３　ワイドエリアネットワーク
４８０　リモートコンピュータ
４８１　メモリデバイス
４８５　リモートアプリケーションプログラム
４９０　ビデオインタフェース
４９５　入出力周辺インタフェース

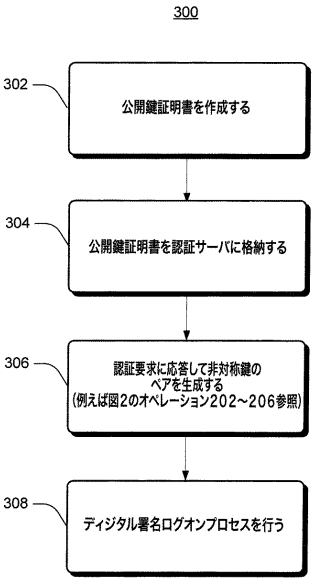
【図１】



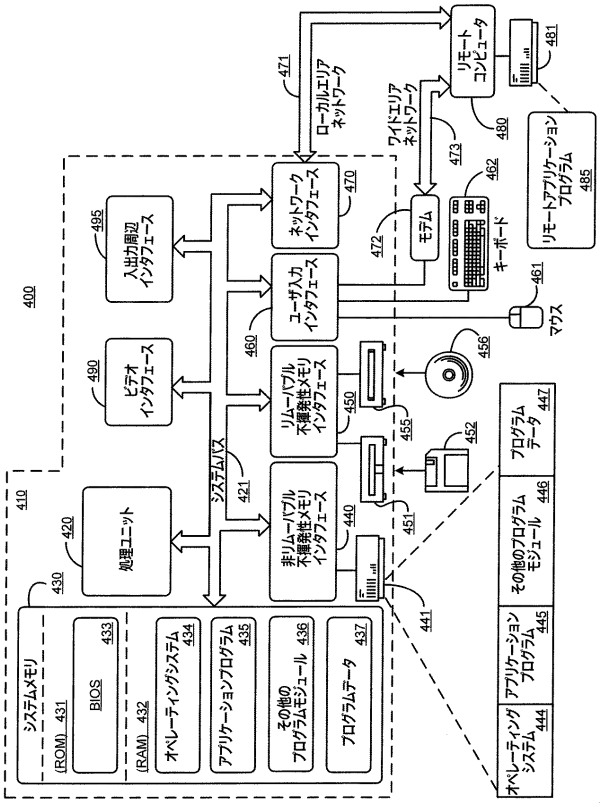
【図２】



【図３】


300
302
公開鍵証明書を作成する
304
公開鍵証明書を認証サーバに格納する
306
認証要求に応答して非対称鍵の
ペアを生成する
(例えば図2のオペレーション202～206参照)
308
ディジタル署名ログオンプロセスを行う

【図４】


400
410
420
処理ユニット
430
システムメモリ
(ROM) 431
BIOS 433
(RAM) 432
オペレーティングシステム 434
アプリケーションプログラム 435
その他のプログラムモジュール 436
プログラムデータ 437
システムバス 421
ビデオインタフェース 490
入出力周辺インタフェース 495
ネットワークインタフェース 470
ユーザ入力インタフェース 460
リムーバブル不揮発性メモリインタフェース 450
非リムーバブル不揮発性メモリインタフェース 440
ローカルエリアネットワーク 471
ワイドエリアネットワーク 473
モデム 472
リモートコンピュータ 480
リモートアプリケーションプログラム 485
キーボード 462
マウス 461
オペレーティングシステム 444
アプリケーションプログラム 445
その他のプログラムモジュール 446
プログラムデータ 447

フロントページの続き

(72)発明者 ジョシュ ディー. ベナロウ
アメリカ合衆国 ９８０５２ ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイクロソフト コーポレーション内

審査官 青木 重徳

(56)参考文献 特開平０８－２７４７６９（ＪＰ，Ａ）
特表２００２－５３５７４０（ＪＰ，Ａ）
特開２００４－１５９１５９（ＪＰ，Ａ）
特開平０９－２３１１７４（ＪＰ，Ａ）
特開２０００－２１５３７９（ＪＰ，Ａ）
特表平０８－５１２４４５（ＪＰ，Ａ）
柴田陽一，中村逸一，曽我正和，田窪昭夫，西垣正勝，“メカニズムベースＰＫＩ”，コンピュータセキュリティシンポジウム２００３，日本，社団法人情報処理学会，２００３年１０月２９日，第２００３巻，第１５号，ｐ．１８１－１８６
Steven M. Bellovin, Michael Merritt, “Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks”, IEEE Computer Society Symposium on Research in Security and Privacy, [online], １９９２年 ５月, p.72-84, [retrieved on 2011-09-15]. Retrieved from the Internet, ＵＲＬ, <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=213269>

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ ９／３２
Ｇ０６Ｆ １５／００
Ｈ０４Ｌ ９／１０