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

特許第4486023号
(P4486023)

(45)発行日　平成22年6月23日(2010.6.23)　(24)登録日　平成22年4月2日(2010.4.2)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330G
H04L 9/10	(2006.01)	H04L	9/00	621A
G06K 19/10	(2006.01)	G06K	19/00	R
G06F 21/22	(2006.01)	G06F	9/06	660G
G06K 17/00	(2006.01)	G06K	17/00	S

請求項の数 4　(全 10 頁)

(21)出願番号　特願2005-312206(P2005-312206)
(22)出願日　平成17年10月27日(2005.10.27)
(62)分割の表示　特願2002-556349(P2002-556349)の分割
原出願日　平成14年1月11日(2002.1.11)
(65)公開番号　特開2006-120168(P2006-120168A)
(43)公開日　平成18年5月11日(2006.5.11)
審査請求日　平成17年10月27日(2005.10.27)
(31)優先権主張番号　01480003.1
(32)優先日　平成13年1月11日(2001.1.11)
(33)優先権主張国　欧州特許庁(EP)

(73)特許権者　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏
(74)復代理人　100106699
弁理士　渡部　弘道

最終頁に続く

(54)【発明の名称】無許可の人によるパーソナル・コンピュータの使用を防止するためのセキュリティ方法

(57)【特許請求の範囲】

【請求項１】

許可されたユーザが存在するメイン・コンピュータ装置を、前記許可されたユーザがリモート・コンピュータ装置からリモートで使用するのを許可するセキュリティ方法であって、

前記メイン・コンピュータ装置が、メイン秘密鍵と抽出可能なメイン公開鍵とメインＰＣ公開鍵とアプリケーション・ログオンのためのパスワードと第１のプロセッサを含み前記メイン・コンピュータ装置から取り外すことが可能なメイン・セキュリティ部分と、前記メイン・セキュリティ部分に含まれる前記メインＰＣ公開鍵および前記メイン秘密鍵とそれぞれＰＫＩ（公開鍵インフラストラクチャ）を構成するＰＣ秘密鍵および抽出可能なメイン公開鍵と、前記第１のプロセッサと認証データを交換する第２のプロセッサを含み前記コンピュータ装置から取り外すことができないＰＣセキュリティ・エリアとを有し、

前記メイン・セキュリティ部分を前記リモート・コンピュータ装置に挿入して、抽出可能なメイン公開鍵が実際に前記許可されたユーザに対応することを前記リモート・コンピュータ装置が確認するために、前記抽出可能なメイン公開鍵を前記メイン・セキュリティ部分から前記リモート・コンピュータ装置のリモートＰＣセキュリティ・エリア内の一時的鍵エリアに転送するステップを含み、

リモートＰＣ秘密鍵を保有する前記リモート・コンピュータ装置のリモートＰＣセキュリティ・エリアから、前記リモートＰＣ秘密鍵に対応するリモートＰＣ公開鍵をローカルＰＣ公開鍵として前記メイン・コンピュータ装置の前記メイン・セキュリティ部分に転送

して、前記メイン・セキュリティ部分と前記リモートＰＣセキュリティ・エリアの間のセキュリティ通信を確立し、
さらに、ユーザが前記リモート・コンピュータ装置にゲストとしてログオンするステップと、
前記メイン・セキュリティ部分に含まれる前記メイン秘密鍵と前記メインＰＣ公開鍵、および前記ＰＣセキュリティ・エリアに含まれる抽出可能なメイン公開鍵と前記ＰＣ秘密鍵を利用して前記パスワードを前記ＰＣセキュリティ・エリアに転送しアプリケーション・ログオンするステップと
を有するセキュリティ方法。
【請求項２】
前記メイン・セキュリティ部分が、前記メイン・コンピュータ装置の部分を構成するキーボードのキーまたはマウス・ボタンである請求項１に記載のセキュリティ方法。
【請求項３】
前記メイン・セキュリティ部分が、ＰＣＭＣＩＡカードである、請求項１または請求項２に記載のセキュリティ方法。
【請求項４】
前記ＰＣセキュリティ・エリアが、前記メイン・コンピュータ装置のマザーボードである、請求項１ないし請求項３のいずれか一項に記載セキュリティ方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザの裁量でユーザのコンピュータ装置の盗難およびハッキングを防止するシステムおよび手順に関し、より詳細には、無許可の人によるパーソナル・コンピュータの使用を防止するためのセキュリティ・システムに関する。
【背景技術】
【０００２】
パーソナル・コンピュータ、ポータブル・コンピュータ、または他のハンドヘルド・コンピュータなどのコンピュータ装置が、ハッカーや泥棒の目標になることから、重要なデータを保護し、あるいは無許可の人によるコンピュータの使用を防止するためにパスワードが使われている。このようなパスワードは、コンピュータ間で安全な通信を確立するのに用いる暗号化鍵および認証鍵と共に用いられる。今日、機密データを暗号化して、これらのデータをアンロック鍵をもたない人が読み取れないようにするプログラムをコンピュータにインストールすることは、可能である。しかし、鍵をどこかに記憶する必要があり、またこの鍵が複雑でなければ、見破られてしまう。
【０００３】
新技術の不断の発展にもかかわらず、パスワードは、依然として最も普及したセキュリティ・ツールであり、また、最もよく乱用され、多くの場合、攻撃者が解読するのが最も簡単である。パスワードは、ある種のセキュリティ・パラドックスを示している。最良のパスワードは、推量するのが最も難しく、長く、ランダムである。残念なことに、これらのパスワードは、また記憶するのが最も大変である。また、大部分のエキスパートは、電子メール、電子商取引、または他のアカウントごとに異なるパスワードを使用し、それらを定期的に変えるよう強く勧めている。その結果、ほとんどの人が簡単に推量できるパスワードを選択し、あるいはそれをコピーや盗用のできる場所に書き留めている。
【０００４】
この難問に対する答えは、パスワード・セーフ（password safes）を使用することである。これらのプログラムは、長い、複雑な、またはランダムなパスワードを記憶するスペースを提供し、次にそれが盗み出されないように暗号化を行う。パスワード・セーフには、ランダムなパスワードを生成するものさえある。しかしそれらのパスワードは、ディスク上にあり、ソフトウェアを起動するパスワードも必要としている。
【０００５】

暗号化（暗号手法）と、ユーザ認証、装置認証またはデータ認証による伝送においてセキュリティは、公開鍵インフラストラクチャ（Public Key Infrastructure）（ＰＫＩ）を用いて実現できる。ＰＫＩ暗号化では、ユーザが公開鍵および秘密鍵という１対の鍵を持っている。それらの名前が示すように、秘密鍵は、個人専用に保持され、公開鍵は、他のユーザに配布される。秘密鍵の所有者は、他の誰とも秘密鍵を共有しない。個々のユーザの公開鍵と秘密鍵は、一方の鍵が他方にきちっとリンクするように、複雑な数学的構造を介して関連付けられる。この関係は、公開／秘密鍵ベースの暗号化を機能させるのにきわめて重大である。

【０００６】

公開鍵は、メッセージを暗号化するベースとして使用され、一方、秘密鍵は、受領者が暗号化されたメッセージを解読するのに必要である。秘密鍵の持参者だけがメッセージを解読できる。暗号化を行った人でさえ、秘密鍵を知らないために、暗号化したばかりのメッセージを解読できないことがある。

【０００７】

デジタル署名では、一般に２つの異なる鍵を使用する。一方の鍵は、デジタル署名を作成し、あるいはデータを一見しただけでは理解できない形に変換するためのものである。他方は、デジタル署名を確認し、またはメッセージをその元の形に戻すためのものである。このような２種の鍵を利用するコンピュータ装置およびソフトウェアは、しばしば、「非対称暗号システム（asymmetric cryptosystem）」と称される。

【０００８】

デジタル署名用の非対称暗号システムの鍵は、署名者だけが知り、デジタル署名の作成に使用する秘密鍵と称するものと、普通、より多くの人に知られ、デジタル署名の確認に使用する公開鍵と称するものである。受領者は、デジタル署名が署名者のものであることを確認するのに、対応する公開鍵を持たなければならない。多くの人が署名者のデジタル署名を確認する必要がある場合、公開鍵は、おそらくそれらの人々がその鍵を簡単に取得できるオンライン・リポジトリまたはディレクトリ内で発表することにより、それらの人々すべてに配布されなければならない。

【０００９】

前記１対の鍵は、数学的に関連付けられているが、非対称暗号システムがデジタル署名に対し安全に設計され実装されている場合、一方の鍵から他方を導出するのは、計算上不可能である。

【００１０】

多くの人々は、所与の署名者の公開鍵を知っていて、それを用いて署名を確認するが、署名者の秘密鍵を発見し、それを用いてデジタル署名を偽造することはできない。

【発明の開示】

【発明が解決しようとする課題】

【００１１】

したがって、本発明の主な目的は、許可されたユーザが所有するメイン・コンピュータ装置を無許可の人が使用するのを防止する、公開鍵インフラストラクチャ（ＰＫＩ）に基づく、セキュリティ・システムを提供することである。

【課題を解決するための手段】

【００１２】

したがって、本発明は、許可されたユーザが所有するパーソナル・コンピュータなどのメイン・コンピュータ装置の無許可の人による使用を防止する、セキュリティ・システムに関し、このシステムは、前記メイン・コンピュータ装置の部分であり、前記許可された人がそこから取り外すことができ、少なくとも取り外し可能なメイン秘密鍵およびＰＣ公開鍵を含む取り外し可能なセキュリティ部分と、前記メイン・コンピュータ装置の取り外し不可能な部分であり、少なくともＰＣ秘密鍵および抽出可能なメイン公開鍵を含むＰＣセキュリティ・エリアとを含み、このＰＣ秘密鍵および抽出可能なメイン公開鍵の対が、それぞれ取り外し可能なメイン秘密鍵およびＰＣ公開鍵の対と共に公開鍵インフラストラ

クチャ（ＰＫＩ）を構成し、取り外し可能なセキュリティ部分とＰＣセキュリティ・エリアの両方に、既に取り外されたセキュリティ部分がリモート・コンピュータ装置に挿入され、取り外し可能なセキュリティ部分とＰＣセキュリティ・エリアの相互認証を実行することによって、許可されたユーザが前記メイン・コンピュータ装置に記憶されたデータにアクセスすることができるようにする処理手段を含む。

【発明を実施するための最良の形態】

【００１３】

図１を参照すると、本発明の主な原理は、取り外し可能なセキュリティ部分１０およびＰＣセキュリティ・エリア１２を組み合わせて使用することになる。取り外し可能なセキュリティ部分１０は、それが接続されているコンピュータ装置において一意である。この取り外し可能なセキュリティ部分１０がないと、コンピュータ装置、およびメモリ、ハードディスク、様々な周辺装置など、それに含まれるまたは接続された装置がすべて使用できない。この部分は、キーボードのキー、または一体化したマウス・ボタン、すなわち小さな情報表示エリアまたはＬＥＤエリアまたはＰＣＭＣＩＡカードを含むブロックとすることができる。後者のケースでは、ＰＣＭＣＩＡスロットの１つは、他の目的に使用することができない。もう１つの機能、ＰＣセキュリティ・エリア１２は、オペレーティング・システムおよびインストール済みのアプリケーションを含めてコンピュータ装置ハードウェア／ファームウェアの任意の部分である。一般に、このＰＣセキュリティ・エリアは、コンピュータ装置のマザーボード、あるいはコンピュータ装置の他の必須なボードまたはカードに含まれ、取り外すことはできない。

【００１４】

取り外し可能なセキュリティ部分１０は、一体化した通信ポートを有するマイクロプロセッサとすることができるプロセッサ１４と、外部読み取りに対して保護されたメモリ１６（プロセッサ１４内で一体化されたメモリでもよい）と、ＰＣセキュリティ・エリア１２に送られたデータを暗号化または認証するためにプロセッサ１４が使用するソフトウェア・アプリケーションであるＰＫＩチェッカ１８とを含む。保護されたメモリ１６は、取り外し可能なメイン秘密鍵２０、ＰＣ公開鍵（コンピュータ装置の公開鍵）２２、および他の鍵またはパスワード２４を格納している。

【００１５】

同様に、ＰＣセキュリティ・エリア１２は、通信ポートを介してプロセッサ１４と通信するプロセッサ２６と、取り外し可能なセキュリティ部分１０に送られるデータを暗号化または認証するために使用されるソフトウェア・アプリケーションであるＰＫＩチェッカ２８と、プロセッサ２６内で一体化することもできる保護されたメモリ３０とを含む。保護されたメモリ３０は、抽出可能なメイン公開鍵３２（取り外し可能なセキュリティ部分１０の公開鍵）、ＰＣ秘密鍵３４、および他の鍵またはパスワード３６を格納している。

【００１６】

許可されたユーザがコンピュータ装置から以前に取り外した取り外し可能なセキュリティ部分１０が、コンピュータ装置内の正しい場所に再度置かれたとき、ＰＣセキュリティ・エリア１２との相互認証が以下に説明するように自動的に行われる。このチェックが完了したとき、プロセッサ２６は、アプリケーションの認証または暗号化をチェックするＯＳまたはアプリケーション・パスワード用の入出力バスにより、ＰＣシステム３８へのアクセスを開始することができる。この瞬間に、プロセッサ１４または２６のいずれも暗号化または認証の実行を助けることができる。さらに、コンピュータ装置システム３８は、リモート・ユーザなど外部ユーザを確認するために、プロセッサ２６に対する通信をオープンすることができる。

【００１７】

取り外し可能なセキュリティ部分１０の保護されたメモリ１６は、図２により詳細に図示されている１組の記憶域を含む。この記憶域は、いずれかの鍵を格納するが、この鍵は、鍵自体でもこれらの鍵を含む完全な証明書でもパスワード・エリアでもよい。

【００１８】

すなわち、記憶域は以下のものを格納している。
・取り外し可能なセキュリティ部分１０を識別するための一意の秘密鍵である取り外し可能なメイン秘密鍵４０。一連番号に類似しているが、ずっと複雑で読み取り難い。この秘密鍵４０は、それ自体を接続されたコンピュータ装置に対して識別し、コンピュータ装置がこの秘密鍵４０でしか解読できない暗号化されたメッセージをこの部分に送れるようにするために取り外し可能なセキュリティ部分１０によって使用される。
・コンピュータ装置に対応し、この環境でセキュリティ部分１０の使用許可を要求するなど、ＰＣセキュリティ・エリア１２に送られるメッセージを暗号化するのに使用される、メインＰＣ公開鍵４２。この鍵は、ＰＣセキュリティ・エリア１２からのメッセージを認証するのにも使用される。
・ユーザによって生成され、以下に説明するように、ある種のアプリケーションに対してこのコンピュータ装置上で認可される他のセキュリティ部分に送信される秘密鍵である、共用秘密鍵４４。
・取り外し可能なセキュリティ部分１０を、このセキュリティ部分１０が属するコンピュータ装置とは異なるコンピュータ装置上で識別するために使用されるＰＣ公開鍵である、ローカルＰＣ公開鍵４６。
・取り外し可能なセキュリティ部分を、このセキュリティ部分が属するコンピュータ装置とは異なるコンピュータ装置上で識別するための一意な秘密鍵である、取り外し可能なローカル秘密鍵４８。この鍵は、以下に説明するように、ローカルＰＣ公開鍵と共に、可能なゲスト・コンピュータに対応する１組の鍵を形成する。これらの鍵は、多数のコンピュータ装置が接続できるように複製することができる。
・メイン・コンピュータ装置とのローカル接続での使用に、またはリモート接続に必要なパスワードを格納するメイン・パスワード・エリア５０。
・以下に説明するように、取り外し可能なセキュリティ部分が、他のコンピュータ装置上で許可されるときに、ゲスト・モードで使用されるローカル・パスワード・エリア５２。許可されたユーザは、コンピュータ装置それ自体の上ではなく、取り外し可能なセキュリティ・エリア上に、そのすべてのパスワードを保持するよう望むことができる。
・安全なＩＰＳｅｃトンネル（IPSec tunnel）を構築するなど、ある種のアプリケーションに対して使用できる鍵である、アプリケーション秘密鍵５４。この鍵は、暗号化および／または認証を行うためのＰＫＩ手順を実施するのにも使用できる。多数のこのようなフィールドが、取り外し可能なセキュリティ部分で利用可能である。

【００１９】

ＰＣセキュリティ・エリア１２の保護されたメモリ３０は、取り外し可能なセキュリティ部分１０に含まれる機能と類似の機能を含む。
・取り外し可能なセキュリティ部分１０の公開鍵であり、取り外し可能なセキュリティ部分１０によって解読される暗号化メッセージを送るために、コンピュータ装置によって使用される、抽出可能なメイン公開鍵５６。
・取り外し可能なメイン秘密鍵４０と抽出可能なメイン公開鍵５６との対とともに、メインＰＣ公開鍵４２と対を組んで取り外し可能なセキュリティ部分１０を認証するＰＣ秘密鍵５８。
・暗号化されたメッセージを他の外部装置に送るために、コンピュータ装置によって使用されるコンピュータ装置の公開鍵である、ＰＣ公開鍵６０。この鍵は、取り外し可能なセキュリティ部分１０のメインＰＣ公開鍵４２と同じであってもよい。事実、取り外し可能なセキュリティ部分１０が、コンピュータ装置と対応するもの（メイン・セキュリティ部分を持つメイン・コンピュータ装置）である場合は、同じである。
・以下に説明するように、他の取り外し可能なセキュリティ部分がメイン・コンピュータ装置上に置かれるとき、秘密鍵を記憶するのに使用される一時的鍵を格納することができる、一時的（ＴＥＭＰ）鍵エリア６２。
・以下に説明するように、メイン・コンピュータ装置上に置かれた他の取り外し可能なセキュリティ部分に送られる公開鍵である、共用公開鍵６４。

・取り外し可能なセキュリティ部分１０のメイン・パスワード・エリア５０に記憶されたパスワードと交換できる、またはこれらのパスワードの更新に使用できるＰＣパスワードを含む、ＰＣパスワード・エリア６６。

【００２０】

コンピュータ装置システム３８は、取り外し可能なセキュリティ部分１０が認識されたとき、ＰＣパスワード・エリア６６またはメイン・パスワード・エリア５０に何が記憶されているか、比較によってログイン・パスワードを確認するオペレーティング・システム・ログオンである、ＯＳログオン６８を含んでいる。これには、アプリケーションが、取り外し可能なセキュリティ部分１０内のメイン・パスワード・エリア５０中のパスワードを必要とするときに使用されるアプリケーション・ログオン７０、およびやはり取り外し可能なセキュリティ部分１０内のアプリケーション秘密鍵５４を使用するＰＫＩアプリケーション７２が含まれる。

【００２１】

図３に、取り外し可能なセキュリティ部分１０の代わりに、他の取り外し可能なセキュリティ部分を、メイン・コンピュータ装置と共に使用するケースを示す。このような場合、最初のステップは、取り外し可能なメイン・セキュリティ部分をメインのコンピュータ装置に挿入することにある。取り外し可能なセキュリティ部分は、一方では取り外し可能なメイン秘密鍵４０と抽出可能なメイン公開鍵５６との対、他方ではメインＰＣ公開鍵４２とＰＣ秘密鍵５８との対のおかげで、先に述べたように認証される。

【００２２】

次に、取り外し可能なセキュリティ部分１０のメモリ１６内の共用秘密鍵４４が、ＰＣセキュリティ・エリアのメモリ３０の一時的鍵エリア６２にコピーされる。その後、取り外し可能なセキュリティ部分１０を、コンピュータ装置から取り外し、取り外し可能なゲスト・セキュリティ部分で置き換えることができる。もちろん、後者のゲスト・セキュリティ部分の同一性は、外部の一連番号を使って、対応する公開鍵を記憶するサーバによってチェックされる。その後、一時的鍵エリア６２内の鍵が、取り外し可能なゲスト・セキュリティ部分のメモリ７６内の取り外し可能なローカル秘密鍵７４にロードされる。したがって、取り外し可能なゲスト・セキュリティ部分の取り外し可能なローカル秘密鍵７４が、コンピュータ装置の共用公開鍵６４と一致し、互いに通信できるようになる。

【００２３】

最後に、コンピュータ装置は、双方向の安全なリンクを完成するために、そのＰＣ公開鍵６０を取り外し可能なゲスト・セキュリティ部分のメモリ７６に、ローカルＰＣ公開鍵７８として記憶する。いたんこのリンクが確立すると、取り外し可能なゲスト・セキュリティ部分のローカル・パスワード・エリア８０を、コンピュータ装置システムのＯＳゲスト・ログオン８２のために、コンピュータ装置のＰＣパスワード・エリア６６を介して使用することができる。

【００２４】

本発明の他の適用例は、取り外し可能なメイン・セキュリティ部分を、メイン・コンピュータ装置に挿入する代わりに、リモート・コンピュータあるいはゲスト・コンピュータ装置に挿入するときである。図４に、このようなケースで実施されるプロセスを示す。図では、双方向矢印はエンティティ間の関係を表し、バスはデータ転送を意味する。図２で用いられる参照項目は、取り外し可能なメイン・セキュリティ部分またはメイン・コンピュータ装置のＰＣセキュリティ・エリアの異なるエリアなど、同じエンティティを表すときは同じままであることに留意されたい。

【００２５】

基本的に、取り外し可能なセキュリティ部分１０とゲスト・コンピュータ装置セキュリティ・エリア８４との接続は、セキュリティ部分の側で、取り外し可能なメイン秘密鍵４０を使用して、対応する公開鍵をそのとき抽出可能なメイン公開鍵５６’を格納しているリモートの一時的鍵エリア９０に送信することによって行われる。取り外し可能なメイン秘密鍵４０と抽出可能なメイン公開鍵５６’が同時に生成される。抽出可能なメイン公開

鍵５６’は、リスクなしに外部装置に提供でき、たとえリモート・コンピュータ装置またはゲスト・コンピュータ装置がよく知られたコンピュータ装置でなくとも、それに公開鍵を与えるのには問題がない。さらに、各ユーザは、ある種のルールを定義して、秘密鍵と公開鍵の両方を定期的に変更することができ、また、以前の公開鍵を変更するために、反対側の機器を新しい鍵で更新することができる。

【００２６】

異なるエンティティ間でのすべての更新、あるいは鍵の送信は、装置ＩＤと公開鍵を含む証明書を用いて行うことができる。これらの証明書は、信用されるエンティティである認証局（ＣＡ）サーバによって証明される。したがって、このようなＣＡサーバを認証サーバとして使用することができる。これらのサーバは、例えば、カスタマのすべての装置のすべての公開鍵を知っており、したがってそれらの鍵が安全な通信を互いに構築できるようにすることができる。このＣＡで発行された証明書だけを信用することが共通のルールと言える。

【００２７】

この方法を用いると、ユーザ・セキュリティ部分とリモート・コンピュータ装置の間で相互認証（cross authentication）が行われた後、リモート・コンピュータ装置は、このシステム内で何らかのログオンの実行を最終的に受け入れるため、公開鍵がこのユーザに実際に対応しているかどうかを確認することができる。ユーザのセキュリティ部分は、リモート・コンピュータ装置の安全に通信するためにＰＣ公開鍵を受け取る必要がある。リモート・コンピュータ装置は、（リモートＰＣ秘密鍵８８と一致する）そのリモートＰＣ公開鍵８６をセキュリティ部分１０のメモリ１６内にあるフィールド、ローカルＰＣ公開鍵４６に転送する。この段階で、ゲスト・コンピュータ装置とセキュリティ部分の間で安全な通信を確立することができる。その後、ユーザは、リモート接続を可能にするプロファイル内のリモート・コンピュータ装置に、ゲストとしてログオンできる。

【００２８】

あるタイプの接続は、ＣＡに接続してリモート・コンピュータ装置の同一性を確認してから、この環境でより多くのことを行うというものである。そのケースでは、リモートＰＣ公開鍵８６の確認が行われる。

【００２９】

このような相互接続の主な目的は、ユーザがそのメイン・コンピュータ装置に安全な方式でアクセスできるようにすることである。メインＰＣセキュリティ・エリアへの接続は、図２に示す主な１組の鍵、すなわち、セキュリティ部分側の取り外し可能なメイン秘密鍵４０およびメイン公開鍵４２と、メイン・コンピュータ装置側の抽出可能なメイン公開鍵５６およびＰＣ秘密鍵５８を用いて確立される。リモート・コンピュータ装置は、抽出可能なメイン・セキュリティ部分とそのメイン・コンピュータ装置の間のデータ通信を、たとえそれぞれの公開鍵を知らなくとも、それがＰＫＩの基本原理であるので、解読するのは不可能である。

【００３０】

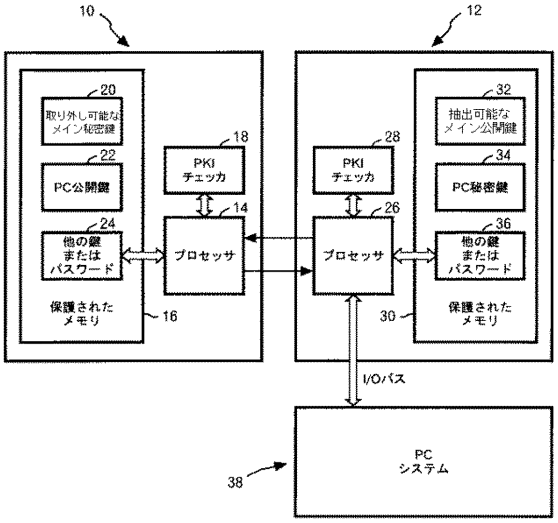
最後に、この安全なチャネルを介して、メイン・パスワード・エリア５０に記憶されているすべてのパスワードを使用し、メイン・コンピュータ装置のセキュリティ・エリア上のＰＣパスワード・エリア６６にそれを安全に転送し、通常のログオンのためにそれをアプリケーション・ログオン７０として使用することができる。この場合、リモート・コンピュータ装置は、ローカル機器と見なされる。この段階で、共用のシークレット（secret）鍵を交換して、ＰＫＩ通信よりも計算用資源を使用せずに、メイン・コンピュータ装置とリモート・コンピュータ装置の間で安全な通信チャネルを確立することができる。

【００３１】

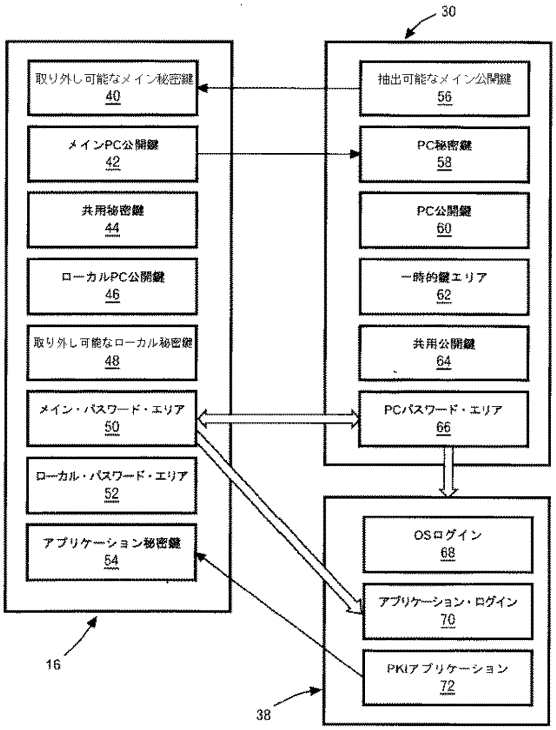
さらに、アプリケーションは、図１ですでに説明したように動作することができる。すなわち、ＰＫＩアプリケーション７２は、アプリケーション秘密鍵５４に記憶した鍵を、図４には示されていないが、各セキュリティ部分および各セキュリティ・エリアに存在す

るＰＫＩチェッカの助けで使用することができる。
【図面の簡単な説明】
【００３２】
【図１】取り外し可能なセキュリティ部分、ＰＣセキュリティ・エリア、およびコンピュータ装置システムとのリンクを持つ、本発明によるセキュリティ・システムを示すブロック図である。
【図２】メイン・コンピュータ装置上に取り外し可能なセキュリティ部分を接続した場合に取り外し可能なセキュリティ部分、ＰＣセキュリティ・エリア、およびコンピュータ装置システムの間の対話を示す略図である。
【図３】メイン・コンピュータ装置上に取り外し可能なゲスト・セキュリティ部分を接続した場合に、取り外し可能なメイン・セキュリティ部分、ＰＣセキュリティ・エリア、取り外し可能なゲスト・セキュリティ部分、およびコンピュータ装置システムの間の対話を示す略図である。
【図４】リモート・コンピュータ装置上に取り外し可能なメイン・セキュリティ部分を接続した場合に、取り外し可能なセキュリティ部分、メインＰＣセキュリティ・エリア、ゲストＰＣセキュリティ・エリア、メイン・コンピュータ装置システム、およびゲスト・コンピュータ装置システムの間の対話を示す略図である。
【符号の説明】
【００３３】
１０ 取り外し可能なセキュリティ部分
１４ プロセッサ
１６ 保護されたメモリ
１８ ＰＫＩチェッカ
２０ 取り外し可能なメイン秘密鍵
２２ ＰＣ公開鍵
２４ 他の鍵またはパスワード
２６ プロセッサ
２８ ＰＫＩチェッカ
３０ 保護されたメモリ
３２ 抽出可能なメイン公開鍵
３４ ＰＣ秘密鍵
３６ 他の鍵またはパスワード
３８ ＰＣシステム

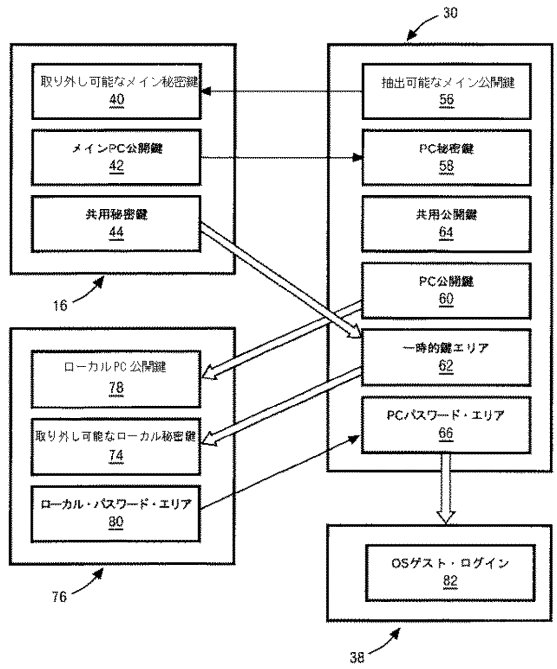
【図１】


10
12
20
取り外し可能な
メイン秘密鍵
22
PC公開鍵
24
他の鍵
または
パスワード
保護された
メモリ
16
18
PKI
チェッカ
14
プロセッサ
28
PKI
チェッカ
26
プロセッサ
32
抽出可能な
メイン公開鍵
34
PC秘密鍵
36
他の鍵
または
パスワード
保護された
メモリ
30
I/Oバス
PC
システム
38

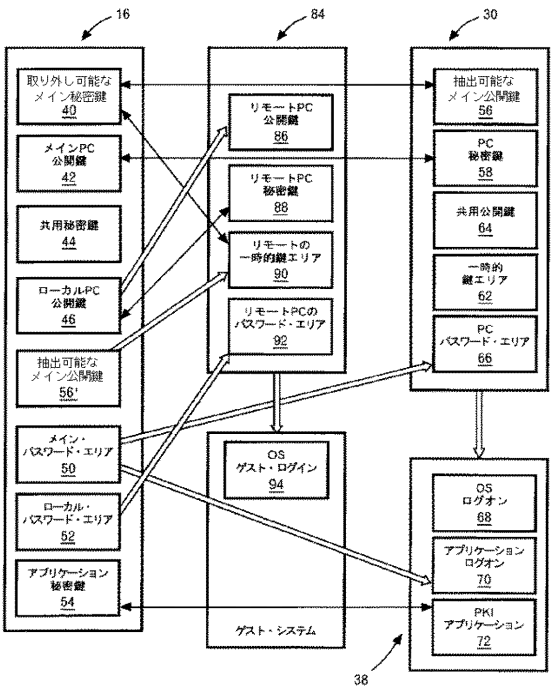
【図２】


30
取り外し可能なメイン秘密鍵
40
メインPC公開鍵
42
共用秘密鍵
44
ローカルPC公開鍵
46
取り外し可能なローカル秘密鍵
48
メイン・パスワード・エリア
50
ローカル・パスワード・エリア
52
アプリケーション秘密鍵
54
16
抽出可能なメイン公開鍵
56
PC秘密鍵
58
PC公開鍵
60
一時的鍵エリア
62
共用公開鍵
64
PCパスワード・エリア
66
OSログイン
68
アプリケーション・ログイン
70
PKIアプリケーション
72
38

【図３】


30
取り外し可能なメイン秘密鍵
40
メインPC公開鍵
42
共用秘密鍵
44
16
ローカルPC公開鍵
78
取り外し可能なローカル秘密鍵
74
ローカル・パスワード・エリア
80
76
抽出可能なメイン公開鍵
56
PC秘密鍵
58
共用公開鍵
64
PC公開鍵
60
一時的鍵エリア
62
PCパスワード・エリア
66
OSゲスト・ログイン
82
38

【図４】


16
84
30
取り外し可能な
メイン秘密鍵
40
メインPC
公開鍵
42
共用秘密鍵
44
ローカルPC
公開鍵
46
抽出可能な
メイン公開鍵
56'
メイン・
パスワード・エリア
50
ローカル・
パスワード・エリア
52
アプリケーション
秘密鍵
54
リモートPC
公開鍵
86
リモートPC
秘密鍵
88
リモートの
一時的鍵エリア
90
リモートPCの
パスワード・エリア
92
OS
ゲスト・ログイン
94
ゲスト・システム
抽出可能な
メイン公開鍵
56
PC
秘密鍵
58
共用公開鍵
64
一時的
鍵エリア
62
PC
パスワード・エリア
66
OS
ログオン
68
アプリケーション
ログオン
70
PKI
アプリケーション
72
38

フロントページの続き

(74)復代理人 100077584
弁理士 守谷 一雄
(72)発明者 ベナユン、アラン
フランス エフ－０６８００ カーニュ・シュル・メール シュマン・デ・コレット ２２－２
アンパス・デュ・クロ・ルノワール
(72)発明者 ル、ペネ、ジャン、フランソワ
フランス ０６１００ ニース ルート・ド・ゲロ シュマン・ド・ラ・セレナ １１
(72)発明者 フィーシ、ジャック
フランス エフ－０６７００ サン・ロラン・デュ・ヴァル アヴニュ・ポール・セザンヌ ６６
ル・ローズ・ガーデン－バティマン－ベー
(72)発明者 ロワ、パスカル
フランス エフ－０６４１０ ビオ ルート・ダンティブ ラ・ノリア ニュメロ ２９

審査官 田中 慎太郎

(56)参考文献 特開平１１－２０５３０８（ＪＰ，Ａ）
特開２０００－１７２４１２（ＪＰ，Ａ）
特開平０９－１１４９４６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２０
Ｇ０６Ｆ ２１／２２
Ｇ０６Ｋ １７／００
Ｇ０６Ｋ １９／１０
Ｈ０４Ｌ ９／１０