(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3877640号
(P3877640)
(45)発行日　平成19年2月7日(2007.2.7)　(24)登録日　平成18年11月10日(2006.11.10)

(51)Int.Cl.		F I		
G06F 21/20	(2006.01)	G06F	15/00	330A
G06F 15/00	(2006.01)	G06F	15/00	310D
G06F 13/00	(2006.01)	G06F	13/00	351Z

請求項の数 14　(全 19 頁)

(21)出願番号	特願2002-129289(P2002-129289)
(22)出願日	平成14年4月30日(2002.4.30)
(65)公開番号	特開2003-30143(P2003-30143A)
(43)公開日	平成15年1月31日(2003.1.31)
審査請求日	平成14年9月26日(2002.9.26)
(31)優先権主張番号	60/287,488
(32)優先日	平成13年4月30日(2001.4.30)
(33)優先権主張国	米国(US)
(31)優先権主張番号	10/001,687
(32)優先日	平成13年10月23日(2001.10.23)
(33)優先権主張国	米国(US)

(73)特許権者　000005821
松下電器産業株式会社
大阪府門真市大字門真１００６番地
(74)代理人　100110364
弁理士　実広　信哉
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100108453
弁理士　村山　靖彦
(72)発明者　デニス・ブッシュミッチ
アメリカ合衆国・ニュージャージー・０８８７３・サマーセット・マットルック・プレイス・１８３

最終頁に続く

(54)【発明の名称】携帯用記憶装置を用いるコンピュータネットワークセキュリティシステム

(57)【特許請求の範囲】

【請求項１】

信用できるコンピュータネットワークへのアクセスを制御するためのセキュリティシステムにおいて、

前記信用できるコンピュータネットワークにアクセスするためのクライアントコンピュータと、

前記クライアントコンピュータから信用できるコンピュータネットワークへのアクセスを制御するゲートウェイと、

初期化時には、前記ゲートウェイにインストールされ、前記信用できるコンピュータネットワークへのアクセスのための認証時には、前記クライアントコンピュータにインストールされる携帯用記憶装置とを具備していて、

前記ゲートウェイは、要塞ホストを備えていて、この要塞ホストは、

前記携帯用記憶装置の初期化を実行する遠隔キー管理モジュールと、

安全なデータベースと、

前記信用できるコンピュータネットワークへのアクセスのための認証を実行する遠隔キー認証モジュールとを有していて、

前記携帯用記憶装置は、

プラグインソフトウェアモジュールと、

ユーザデータエリアとを有していて、

前記初期化時には、前記遠隔キー管理モジュールが、インデックスを付した１セットの

パスワードおよびインデックスを付した１セットのキーを生成し、
前記インデックスに基づいて各パスワードと各キーとを対応付けて、１セットのキー－パスワードペアを形成し、
１セットのパスワードをユーザデータエリアに格納し、
１セットのキー－パスワードペアを安全なデータベース内に格納し、
前記認証時には、遠隔キー認証モジュールが、安全なデータベースから、１つのインデックスおよびこのインデックスに対応するキーを取り出して、これらをプラグインソフトウェアモジュールに送信し、
プラグインソフトウェアモジュールが、ユーザデータエリアから、前記１つのインデックスに対応するパスワードを取り出し、
このパスワードを遠隔キー認証モジュールに送信し、
遠隔キー認証モジュールが、プラグインソフトウェアモジュールから送信されたパスワードと、安全なデータベース内に格納されていたキー－パスワードペアに含まれていたパスワードとを比較する
ことを特徴とするセキュリティシステム。
【請求項２】
前記初期化時には、前記遠隔キー管理モジュールは、キー－パスワードペアから、暗号化されたパスワードを計算し、この暗号化されたパスワードをユーザデータエリアに格納することを特徴とする請求項１に記載のシステム。
【請求項３】
前記認証時には、前記プラグインソフトウェアモジュールは、ユーザデータエリアから、前記１つのインデックスに対応する暗号化されたパスワードを取り出し、この暗号化されたパスワードを解読してパスワードを求め、このパスワードを遠隔キー認証モジュールに送信することを特徴とする請求項１に記載のシステム。
【請求項４】
前記携帯用記憶装置は、不揮発性メモリデバイスであることを特徴とする請求項１に記載のシステム。
【請求項５】
前記携帯用記憶装置は、光ディスクであることを特徴とする請求項１に記載のシステム。
【請求項６】
前記ゲートウェイは、信用できるコンピュータネットワークへの直接のアクセスを遮断する選別ルータを更に備えていることを特徴とする請求項１に記載のシステム。
【請求項７】
前記ゲートウェイは、クライアントコンピュータの代わりに信用できるコンピュータネットワークにアクセスするプロキシシステムを更に備えていることを特徴とする請求項６に記載のシステム。
【請求項８】
前記ゲートウェイは、信用できるコンピュータネットワークへのアクセスをアクティブセッションに限るアクティブセッション管理ミドルウェアを更に備えていることを特徴とする請求項１に記載のシステム。
【請求項９】
前記ゲートウェイは、信用できるコンピュータネットワークへのアクセスを所定の継続時間に限るアクティブセッション管理ミドルウェアを更に備えていることを特徴とする請求項１に記載のシステム。
【請求項１０】
前記プラグインソフトウェアモジュールは、クライアントコンピュータにアクセス可能となっていて、前記認証時にクライアントコンピュータに命令を与えることを特徴とする請求項１に記載のシステム。
【請求項１１】

信用できるコンピュータネットワークへのアクセスを制御するためのセキュリティシステムを用いて、前記アクセスを認証する方法において、
前記セキュリティシステムは、
前記信用できるコンピュータネットワークにアクセスするためのクライアントコンピュータと、
前記クライアントコンピュータから信用できるコンピュータネットワークへのアクセスを制御するゲートウェイと、
初期化時には、前記ゲートウェイにインストールされ、前記信用できるコンピュータネットワークへのアクセスのための認証時には、前記クライアントコンピュータにインストールされる携帯用記憶装置とを具備していて、
前記ゲートウェイは、要塞ホストを備えていて、この要塞ホストは、
前記携帯用記憶装置の初期化を実行する遠隔キー管理モジュールと、
安全なデータベースと、
前記信用できるコンピュータネットワークへのアクセスのための認証を実行する遠隔キー認証モジュールとを有していて、
前記携帯用記憶装置は、
プラグインソフトウェアモジュールと、
ユーザデータエリアとを有していて、
前記方法は、
前記初期化時には、前記遠隔キー管理モジュールが、インデックスを付した１セットのパスワードおよびインデックスを付した１セットのキーを生成し、
前記インデックスに基づいて各パスワードと各キーとを対応付けて、１セットのキー－パスワードペアを形成し、
１セットのパスワードをユーザデータエリアに格納し、
１セットのキー－パスワードペアを安全なデータベース内に格納し、
前記認証時には、遠隔キー認証モジュールが、安全なデータベースから、１つのインデックスおよびこのインデックスに対応するキーを取り出して、これらをプラグインソフトウェアモジュールに送信し、
プラグインソフトウェアモジュールが、ユーザデータエリアから、前記１つのインデックスに対応するパスワードを取り出し、
このパスワードを遠隔キー認証モジュールに送信し、
遠隔キー認証モジュールが、プラグインソフトウェアモジュールから送信されたパスワードと、安全なデータベース内に格納されていたキー－パスワードペアに含まれていたパスワードとを比較する
ステップを有していることを特徴とする方法。
【請求項１２】
前記初期化時には、前記遠隔キー管理モジュールは、ユーザが提供したPINを用いて、キー－パスワードペアから、暗号化されたパスワードを計算し、この暗号化されたパスワードをユーザデータエリアに格納し、
前記認証時には、前記プラグインソフトウェアモジュールは、ユーザデータエリアから、前記１つのインデックスに対応する暗号化されたパスワードを取り出し、ユーザが提供したPINを用いて、この暗号化されたパスワードを解読してパスワードを求め、このパスワードを遠隔キー認証モジュールに送信する
ことを特徴とする請求項１１に記載の方法。
【請求項１３】
前記携帯用記憶装置は、PINを使用前に暗号化するために用いられるセッションキーを格納する保護されたエリアを更に有していることを特徴とする請求項１２に記載の方法。
【請求項１４】
前記認証後に、更に、アクティブセッションを確立し、かつ、このアクティブセッションを、所定の継続時間に限ることを特徴とする請求項１１に記載の方法。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、一般に、コンピュータネットワークセキュリティシステムに関する。特に、本発明は、遠隔地にいる認証されたユーザによる、遠隔クライアントを介した、安全なアクセスを可能にするセキュリティシステムに関する。前記遠隔クライアントは、ユーザが生成するワンタイムパスワードを格納している携帯用記憶装置を利用する。
【０００２】
【従来の技術】
コンピュータネットワークが伝搬したウイルス及びウォームが拡散する中で、また、コンピュータネットワークへの不法侵入が増加する中で、コンピュータのセキュリティに、今日、かなりの関心が集まっている。高度な技術を持つネットワーク管理者は、そのような攻撃を防止するために、安全なファイアウォールを構築する。しかし、大部分のホームネットワークコンピュータユーザを含む、あまり高度な技術を持っていないシステム管理者は、はるかに耐性が低いセキュリティ対策しかとっていない。すなわち、現在、多くのホームコンピュータネットワークは、全く無防備である。コンピュータネットワークのセキュリティは、複雑な問題であり、多くのホームネットワークユーザは、彼らのネットワークが攻撃から保護されることを保証するための技術を持っていないし、訓練も受けていない。
【０００３】
【発明が解決しようとする課題】
本発明は、非常に安全で、かつ使い易いネットワークセキュリティの解決方法を提供する。本発明は、ホームネットワークセキュリティに適用するのに理想的であり、ネットワーク管理者は、多くの訓練を受ける必要がなく、また、セキュリティ問題に関する多くの経験も必要ない。
【０００４】
【課題を解決するための手段】
本発明は、１セットのワンタイムパスワードを保持する携帯用記憶装置を用いる。ホームネットワーク内の安全で有利な地点からのシステムソフトウェアを用いて、ユーザは、１セットのワンタイムパスワードを生成し、携帯用記憶装置に格納する。携帯用記憶装置は、遠隔クライアントコンピュータ内にインストールされるか、または遠隔クライアントコンピュータに接続され、これにより、この遠隔クライアントコンピュータは、ホームネットワークとの安全な接続を、確立かつ認証することができる。各パスワードは、１回だけ使用される。また、ホームネットワーク内のセッション管理ソフトウェアは、セッションを所定の長さの時間（例えば３０分）に制限することができる。ホームネットワークと遠隔クライアント間の通信は、なるべく安全なチャネルを介して行うが、このチャネルを介したワンタイムパスワードの通信は、更に、暗号化された形のユーザPIN番号を用いて保護される。このPIN番号は、プラグインモジュールを用いている遠隔クライアントで暗号化される。前記プラグインモジュールは、暗号化に用いるキーを引き出すために、携帯用記憶装置内の保護エリアにアクセスする。
【０００５】
好ましい実施形態は、選別ルータとして機能するファイアウォールを備えるホームゲートウェイの形をとる。選別ルータは、ホームネットワーク上のコンテンツにアクセスするための全ての要求を遮断する。ホームネットワークと関連している全てのURLは、直接、外部からアクセスすることができないので、保護されたURLとして維持される。遠隔クライアントは、認証後であっても、ホームネットワークを、直接、指し示すURLを送出することはできない。認証されると、ホームネットワークと通信するために、認証された遠隔クライアントに代わってウェブプロキシシステムが用いられる。プロキシシステムは、URLの変更及び検証処理と共に動作する。URL変更処理によれば、ウェブプロキシシステムが、信用できるドメイン資源による正しい照会を可能にする。一方、URL検証処理によれば

、クライアントの信頼性が検証される。URL変更処理は、それぞれの認証されたクライアント、及び、それぞれの認証されたセッションに対して、唯一のものである。このように、ある認証されたクライアント、または、あるセッションのために変更されたURLは、他のクライアントによって再使用されることはなく、さらに、同一のクライアントであっても、後のセッションのために再使用されることもない。

【０００６】

好ましい実施形態においては、認証機能は、ホームゲートウェイの一部を形成している要塞ホストシステムによって実現される。要塞ホストは、遠隔キー認証処理を実行するためのソフトウェアを備えていて、これにより、遠隔クライアントは、携帯用記憶装置から得られたワンタイムパスワードを用いて自身を認証する。また、要塞ホストは、上述したURL検証及び変更機能を実現する。

【０００７】

本発明は、このように、管理が容易でありながら、高いレベルのセキュリティを提供する。ユーザが遠隔クライアントコンピュータからホームネットワークにアクセスするために必要な全てのもの（ユーザの個人認証(identification)番号を除く）は、携帯用記憶装置に格納される。好ましい実施形態においては、この記憶装置は、適切なブラウザプラグインソフトウェアを備えていて、それは、遠隔クライアントコンピュータのブラウザが、認証処理を実行することを可能にする。前記認証処理は、適切なワンタイムパスワードにアクセスし、このパスワードを使用する処理を含んでいる。

【０００８】

キーを配布するための信用できる第三者機関のソースに頼る他のセキュリティシステムと異なり、本発明は、ユーザが、信用できるホームネットワークサイトで設定ソフトウェアを操作することにより、自身のキーを作成することを可能にする。ユーザは、設定ソフトウェアを用いて、携帯用記憶装置を設定し、この携帯用記憶装置に１セットのワンタイムパスワードを供給する。

【０００９】

設定ソフトウェアは、また、ゲートウェイと接続された安全なデータベース内に、対応するセットの認証コードをインストールする。このように、ゲートウェイと携帯用記憶装置の両方が、認証を実行するために必要な、対応するキーを供給する。これは、いかにして、遠隔クライアントがホームネットワークにアクセスすることを可能にするキーを、前記遠隔クライアントに、安全に配布するかという問題を解決する。

【００１０】

以下の記述と、付随の図を参照すれば、本発明と、その目的及び利点が、更に完全に理解されるであろう。

【００１１】

【発明の実施の形態】

本発明は、詳細な記述、及び、付随の図から、更に十分に理解されるであろう。

【００１２】

図１は、好ましい実施形態の概観を示すシステムブロック図である。

【００１３】

図２は、図１に示したシステムにおける、好ましいゲートウェイの基本的な構成を示すブロック図である。

【００１４】

図３は、図２に示したゲートウェイの動作を理解するために有益なデータフロー図である。

【００１５】

図４は、図２に示したゲートウェイにおける、認証及びプロキシモジュールを示す、さらに詳細なブロック図である。

【００１６】

図５は、図２に示したゲートウェイにおける、ワンタイムパスワード認証メカニズムを示

すブロック図である。
【００１７】
図６は、好ましい認証処理の詳細を示すブロック図である。
【００１８】
図７は、好ましい認証処理を理解するために有益なデータフロー図である。
【００１９】
図８は、認証処理を示すシーケンス図である。
【００２０】
図９は、図２にも示したゲートウェイのブロック図であって、好ましい実施形態のウェブプロキシ機能を示している。
【００２１】
図１０は、ウェブプロキシモジュールの構成要素のブロック図であり、ユニフォームリソースロケータ(URL)の検証及び変更機能を示している。
【００２２】
図１１は、携帯用記憶装置を初期化もしくは設定するための好ましい処理を示している。
【００２３】
図１２は、認証のためにクライアントブラウザプラグインを用いる方法における、更に詳細な動作を示すブロック図である。
【００２４】
以下の好ましい実施形態の記述は、単に現存している具体例を示すものであって、本発明と、その応用または使用を限定するものではない。
【００２５】
安全なネットワークアクセス構成の具体的な手段を図１に示す。遠隔クライアント20は、ホームネットワーク22と、インターネット24のような敵意のある（安全性が低い）ネットワークを介して通信する。ホームネットワーク22は、１台のコンピュータのように簡単なものであってもよいし、フルスケールのローカルエリアネットワークのように複雑なものであってもよい。本発明は、特に、高度な技術を持っていないユーザによる使用に適しているので、図１に示したホームネットワークは、サーバ26と、プリンタ28と、１組のデスクトップもしくはラップトップコンピュータ30とを備える、かなり簡単なローカルエリアネットワークとなっている。なお、ここには、簡単なホームネットワークが示されているが、本発明の原理を、オフィスや公共機関や大学等に見られる、より大きなネットワークに、容易に拡張することが可能だということは、明らかである。
【００２６】
セキュリティの観点から見ると、ホームネットワーク22は、信用できるネットワークである。一方、インターネット24は、敵意のあるネットワークである。ホームネットワークのシステムオペレータは、認証されたユーザのみが、このホームネットワークにアクセスし、そのサービスを使うことができるように、このホームネットワークを設定することができる。しかし、ホーム管理者は、インターネット24に対しては、同様の制御を行うことができない。従って、敵意のある側から信用できる側を分離するために、本発明は、ゲートウェイ装置32を備えている。ゲートウェイ装置の詳細については、より十分に後述する。本質的に、このゲートウェイは門番としての役割を果たし、認証されていないホームネットワークへのアクセスを全て遮断する。ゲートウェイ装置は、また、認証処理を仲介する機能を有している。これによって、遠隔クライアント20は、自身を認証し、その結果、ホームネットワーク22上のサーバ26にアクセスすることが可能になる。
【００２７】
本発明の認証メカニズムのキーとなる構成要素は、携帯用記憶装置(device)34である。そのような装置が、図１に２つ示されている。１つはAに配置されていて、もう１つはBにおける遠隔クライアントによって用いられている。ゲートウェイ装置は、携帯用記憶装置を初期化かつ設定するための適切な記録装置36を備えている。携帯用記憶装置34は、様々な形をとることができ、CD-ROM、DVD、CD-R、DVD-RAM、フラッシュメモリ、及び、その他の

ハードディスクを用いた媒体、または、固体メモリを含んでいる。図１には、例として、CD-ROMが示されている。

【００２８】

本発明の１つの形態によれば、いかなる携帯用記憶装置も、遠隔キー格納メカニズムとしての働きをすることができる。しかし、ここでの好ましい実施形態においては、携帯用記憶装置が安全な保護されたエリアを有することによって、保護レベルが、さらに追加されている。この保護されたエリアの詳細については、より十分に後述する。

【００２９】

携帯用記憶装置34は、安全なキーの配布メカニズムとして機能する。ユーザは、ホームネットワークの境界線内で、携帯用記憶装置を初期化かつ設定する。更に具体的には、好ましい実施形態において、ユーザは、ゲートウェイ内に構成されている、携帯用記憶装置に対する安全なインターフェースを用いて、これを達成する。そして、前記携帯用記憶装置は、厳格に制御された安全な方式で、ゲートウェイ上で動作する、安全なソフトウェアモジュールを用いる。好ましい実施形態において、ゲートウェイは、キーが格納される安全なデータベースを備えている。このデータベースは、同様に、厳格に制御された安全な存在であって、ゲートウェイ上で動作する安全なソフトウェアモジュールによってのみアクセスされる。

【００３０】

将来、分散された環境の全域で、インターフェース及びソフトウェアモジュールのセキュリティを維持することを可能にする、安全な手段が開発されれば、携帯用記憶装置を初期化及び設定する機能、及び、安全なデータベースを保守する機能は、ゲートウェイ以外の、信用できるドメイン内のコンピュータシステムを用いて実現してもよい。

【００３１】

初期化後、携帯用記憶装置は、ユーザによって、世界中のどこにあるコンピュータに運ばれてもよい。あるコンピュータ（例えば、遠隔クライアント20）内に、携帯用記憶装置をインストールすることによって、そのコンピュータは、ホームネットワーク22との通信のために自身を認証することが可能になる。ここでの好ましい実施形態においては、初期化中に、携帯用記憶装置に対してワンタイムパスワードが付与される。それ以降、使用の間、プラグインプログラムが、これらのワンタイムパスワードにアクセスすることは、より十分に説明されるであろう。プラグインプログラムは、遠隔クライアント20上に既に存在するウェブブラウザソフトウェアによる使用に適した、プログラムモジュールまたはアプレットであってもよい。プラグインソフトウェアによって、遠隔クライアントは、認証のために必要なメッセージの交換に関与することが可能になる。好ましい実施形態においては、インターネット24を通り抜ける安全なパイプライン38を確立するために、安全なソケット層(SSL)が用いられる。

【００３２】

図２を参照すれば、ゲートウェイ装置32は、パケットをフィルタにかける選別ルータ42を備えるファイアウォール40を実現する。このルータは、全ての遠隔クライアントが、ホームネットワーク22上のいかなるホストにも、直接、アクセスすることができないように設定される。選別ルータが、次に、遠隔キー認証機能46及びウェブプロキシ（代理）機能48を実現する要塞ホスト44と通信することは、以下で更に十分に論じられるであろう。本質的に、要塞ホスト44は、携帯用記憶装置から得られる適切なワンタイムパスワードを用いる認証を要求する。結局、情報をファイアウォールを通して得るためには、遠隔クライアントは、21に図示された、遠隔キーに基づく認証処理に正常に関与しなければならない。

【００３３】

いったん認証が正常に完了したら、要塞ホストは、URLアドレス変換及びクライアント検証の任務を、ウェブプロキシ機能48の一部として実行する。特に、遠隔クライアントから伝送されるURLは、認証されたクライアントから来るものとして検証され、かつ、そのクライアント固有の方法で変更される。ウェブプロキシシステムは、その認証されたクライアントのためのアクティブ状態が存在するかどうかを決定するために、アクティブ状態ミ

ドルウェア(図４におけるASSM72)を調査する。もし存在するのであれば、ウェブプロキシシステムは、遠隔クライアントに代わって、信用できるホームネットワークにアクセスする。特に、アドレス変換機能は、各クライアントに対して固有のものである。すなわち、URLの再使用は禁止されているので、認証されたクライアントのためのURLが詐欺師によって傍受されて再使用されるようなシステム攻撃は、阻止される。この処理については、後に、図９に関連して更に詳細に述べる。

【００３４】

図３を参照すれば、いかにして、遠隔クライアントが、ホームネットワーク内に格納された情報へのアクセスを可能にするかを、よりよくイメージすることができる。図３には、データフロー図が示されていて、いかにして、ホームネットワーク内の情報へのアクセスが達成されるかが示されている。遠隔クライアントは、インターネット上に、SSL接続のような、安全なチャネル50を確立する。符号52で図示されているように、選別ルータ42は、ファイアウォールとして動作し、ホームネットワークに関連するURLを常に遮断する。ただし、この選別ルータ42は、ファイアウォールを経由する一定の通信を許容する。これは、すなわち、認証及びそれに続くウェブプロキシ機能を用いる通信のために必要なものである。そして、選別ルータは、要塞ホスト44と通信する。これは、第１に、セッション管理及び認証のためであり、第２に、認証後のウェブプロキシ任務のためである。

【００３５】

要塞ホストは、ワンタイムパスワードを用いる認証を要求するセッションマネージャを備えている。さらに安全性を高めるために、セッションマネージャは、セッションの長さを制御し、所定の時間（例えば３０分）後、セッションを終了させる。これらの制御機能は、符号54に図示されている。符号56に図示されているように、セッションマネージャは、携帯用記憶装置内のプラグインソフトウェアとの連係によって、認証機能を実現させる。

【００３６】

携帯用記憶装置には、符号58に図示された、ユーザ設定の一部としてのワンタイムパスワードが付与される。具体的には、ゲートウェイが、ユーザPINを用いて、特定のユーザのために個人専用とされた乱数及びランダムなキーを生成する。PINは、このように、暗号化方程式の要素になる。具体的には、PINと、キーKiとの排他的論理和(XOR)がとられる。野蛮かつ暴力的な攻撃によるユーザPINの漏洩を避けるために、この好ましい実施形態においては、ワンタイムパスワードを生成するために必要な要素のうちの１つであるユーザPINの暗号化された形を用いる。ユーザが提供したPINを暗号化するために用いられる値は、特別な対称のキーKsである。Ksは、ゲートウェイによって生成され、携帯用記憶装置内の保護されたエリアに格納される。正しく認証された携帯用記憶装置、及び、正しく認証された携帯用記憶装置のユーザのみが、Ksを引き出すために、保護されたエリアにアクセスすることができる。

【００３７】

具体的には、携帯用記憶装置は、それがインストールされるか、挿入されるか、あるいは接続される読取装置によって認証されるはずであり、ユーザは、プラグインモジュールによって促された後に、PINを入力することによって認証されるはずである。

【００３８】

いったんセッションマネージャが認証されたセッションを確立すれば、符号60で図示されているように、URLアクセス要求は、ウェブプロキシ機能と共に用いられるURL検証及び変更機能によって処理される。そして、ウェブプロキシは、信用できるホームネットワークと通信し、遠隔クライアントの代わりに情報あるいは資源を取得するが、このとき、変更されたURL、すなわち、特定の認証されたクライアントのために検証及びカスタマイズされたURLを用いる。

【００３９】

ゲートウェイのプロキシ動作及びクライアント認証モジュールの連係動作の詳細が、図４に示されている。ここでの好ましい実施形態においては、ゲートウェイ32は、正当な証明書を持つ唯一の装置であり、また、SSLウェブプロキシサーバ48を備える唯一のホストで

ある。このSSLプロキシサーバは、全ての遠隔クライアントがホームコンテンツへアクセスする際に用いる唯一の存在である。選別ルータで展開される、パケットをフィルタにかける方法が、適切に設定される。すなわち、ウェブプロキシに向けられたhttpsの通信データの流れのみが、パケットフィルタを通過し、その他の通信データの流れは、全て阻止される。

【００４０】

処理は、遠隔クライアント20が、ゲートウェイに対して、直接のhttpsのURL要求を送出することによって始まる。この要求は、ユーザIDを含んでいる。この時点で、遠隔クライアント及びゲートウェイの遠隔キー認証モジュール70は、ワンタイムパスワードの使用に基づく認証処理に貢献する。この認証については、後に詳細に述べる。

【００４１】

認証が成功したら、ゲートウェイのアクティブセッション管理ミドルウェア(ASMM)72内に、「クライアント－ゲートウェイセッション状態(CGSS)」が確立される。各セッションの開始時に、ASMM72と対応付けられたセッション継続時間タイマが、ゼロにリセットされる（例えば、W=30分を超えないように）。それから、ASMM72は、安全なユーザデータベース73から、ユーザ固有のパラメータを取り出す。（図３における符号58のように、）ユーザが携帯用記憶装置を設定するとき、この安全なユーザデータベースには、ワンタイムパスワードに関する情報が、密かに格納される。この秘密情報及びその他のCGSSパラメータは、認証及びURL有効性検査処理の間、使用される。

【００４２】

具体的には、認証後に、ASMM72は、ウェブプロキシサーバ48のSSLウェブプロキシ部に、74のようなURL有効性検査と結合した適切なウェブプロキシ処理を行うことを指示すると共に、76のような双方向性のURL変更処理を実行することを指示する。これらの処理は、図１０に関連して更に十分に後述される。

【００４３】

ユーザセッション（提案されている時間は30分）の満了後、ウェブプロキシシステムは、（テンプレートページデータベース78からの）カスタムページを、遠隔クライアントに送信する。このことは、新しい、携帯用記憶装置に基づく認証が行われなければならないことを示している。遠隔ユーザは、また、以下のような要求を送出することによって、クライアント－ゲートウェイセッション(CGSS)を、はっきりと解消することもできる。

https://gw_host/?UserID=db&TearDown=on

すると、ASMM72は、クライアント－ゲートウェイセッション状態(CGSS)を解消し、かつ、ウェブプロキシシステムに対して、「古い」SSLセッションを再開しないように指示する。新しいSSLセッションを確立し、携帯用記憶装置に基づく認証の全工程(full round)を実行し、そして、新しいCGSSを確立するためには、全ての(full)SSLハンドシェイクが、再度、クライアント及びプロキシによって行われなければならない。いったんCGSSが解消されれば、ウェブコンテンツのプロキシ処理が、「外部の」要求に応じて行われることはなく、要求されたURLは、それらの認証された有効性検査に落ちてしまうことは、重要な、注目すべきことである。

【００４４】

好ましい実施形態においては、プロキシ任務を遂行するゲートウェイ32は、正当なIPアドレスを必要とする唯一のホストである。残りのホームホストは、それらのIPアドレスを、内部で管理されたアドレスプールから、DHCP及びネットワークアドレス変換(NAT)のようなメカニズムを用いて取得する。

【００４５】

ここで、好ましい実施形態の全体構成を念頭において、好ましい遠隔キー認証処理の詳細を、図５～８を参照して述べる。図５を参照すれば、認証は、遠隔キー認証モジュール46によって仲介される。ここでの好ましい実施形態は、少なくとも128ビットの強度の暗号を利用していて、これは、全てのセッションキー(Ki, Ks)が、少なくとも128ビット長であることを意味している。使用の前に、キーは、後に図１１に関連して詳述するキー管理

システムによって生成される。

【００４６】

好ましい実施形態において、我々は、ランダムな暗号パラメータを生成するために、「真の」乱数発生器を必要とする。提案されたシステムのセキュリティ状況の多くは、暗号化のためのワンタイムパスワード及びキーとして用いられる、ランダムシーケンスによる。このような発生器は、例えば、外部温度や、ネットワーク接続及び多くの他の外部資源に関する情報を考慮に入れ、何らかの強力なハッシュ機能（例えばMD5）を用いて、これらを相互に結合する。

【００４７】

携帯用記憶装置に基づく認証処理が、図６に示されている。遠隔キーの初期化段階の間、「将来の」遠隔ユーザは、物理的にホームゲートウェイのすぐ近くにいなければならない。ユーザは、キーカード（あるいはCD媒体）を、初期化手続き及びそれに続くキーカードへのワンタイムパスワードの転送のために、ゲートウェイの中に挿入しなければならない。遠隔キーカード初期化処理が、図１１に示されていて、後に詳述される。この初期化段階の間に、ゲートウェイは、１セット（例えばN=100）のランダムなパスワード(Si)を単純に生成し、ランダムなキー(Ki)によってそれらを暗号化し、そして、それらが４桁のPINのユーザ情報に依存するようにする（そして、前記PINは、保護されたエリアに格納された対称のキー(Ks)によって保護される）。そして、これらの暗号化されたパスワード(Ei)は、携帯用記憶装置内に格納されるので、旅行に出る遠隔クライアントによって持ち運び可能となる。パスワード(Si)及び対応するキー(Ki)は、遠隔キー認証モジュール70（図４）によるアクセスのために、ゲートウェイの安全なデータベース内に格納される。

【００４８】

図６を参照すれば、以下に列挙されたステップに従って、認証処理が進行する。

ステップ(1)　遠隔クライアントは、そのユーザIDを、https要求内のゲートウェイに送信する。

ステップ(2)　このステップでは、ゲートウェイが、遠隔クライアントに、秘密の対応するキー(Ki)の値と共に、カウンタ値(i)を送信する。

ゲートウェイは、成功したユーザ認証の数を示すカウンタ値(i)を保持する。もしN=100であれば、カウンタ値は、100から1に向かって減少する。もしカウンタ値が0に達したら、キーカードを再び初期化しない限り、そのユーザIDに対して、それ以上の認証は許可されない。

ステップ(3)　クライアントのブラウザプラグインソフトウェアは、下記の式に従って、ワンタイムパスワード(Ei)を解読する。

【数１】

$$S_i = D_{Ki \oplus Eks(PIN)}(E_i)$$

プラグインは、Siをゲートウェイのキーカード認証モジュールに送信する。

【００４９】

この時点で、遠隔キー認証モジュール70（図４）は、クライアントから受信した値Siを、その安全なデータベース73（図４）内に格納されていた値と比較する。もし、それらが一致したら、ASMM72は、使用量カウンタの値(i)を減少させると共に、ゲートウェイのASMM72（図４）内にCGSSを確立する。

【００５０】

もし、侵入者が、単にユーザIDをゲートウェイに何回も送信することによって、全てのパスワードスペースを使い果たすことができるのであれば、サービス拒否(DOS)の状態に陥ってしまう。これを防止するために、この好ましい実施形態では、ユーザの認証に成功した後に、はじめて、カウンタを減算させる。更に、我々は、時間ウィンドウ(W)を提案する。その中では、最大３回の認証の試みが許される。もし、不成功に終わった試みの数が３回に達したら、そのユーザのための、それ以上の認証の試みは、その時点でのW内では

許されない。ウィンドウWの具体的な長さとしては、5分を提案する。

【００５１】

認証処理の更に完全な理解のために、ここで、図７及び８を参照する。図７は、いったん適切な情報がゲートウェイから受信された後に、遠隔クライアントで行われる処理を示している。図８は、幾分高いレベルにおける同じ処理を示していて、認証処理に関与する様々な実体の間で伝送されるメッセージのやりとりを示している。

【００５２】

遠隔クライアントとゲートウェイ間の通信は、遠隔クライアントが、テンプレートページデータベースに格納されたページから生成されるか、または提供されるログインページにアクセスすることによって開始される。これは、プラグインモジュールを起動させ、このプラグインモジュールは、ユーザに対して、自身のログイン名またはユーザIDを入力するように促す。そこで、ユーザが、自身のユーザIDを入力すると、この情報は、ゲートウェイに送信され、ここで、IDがASSMミドルウェアによってチェックされると共に、そのユーザに適合するi及びKiの値を引き出すために、安全なデータベースがアクセスされる。いったん、これらの値が引き出されると、認証処理を開始する準備が整う。

【００５３】

認証処理は、ゲートウェイが、プラグインモジュールを用いて作動している遠隔クライアントに、インデックス値i及びキーの値Kiを伝達することによって開始される。図７及び８の200に、この１回目の情報(i, Ki)のやりとりが示されている。プラグインモジュールは、このインデックス値iを、ワンタイムパスワードのテーブルE1...Ei中での指標として用いる。なお、これらは、暗号化されたパスワードである。図７の202において、暗号化されたパスワードEiが、プラグインモジュールによって引き出される。

【００５４】

一方、プラグインモジュールは、204において、ユーザに対して、自身の秘密のPIN番号を入力するように促す。そこで、ユーザは、206において、秘密のPINを入力する。この好ましい実施形態においては、ユーザPINは、平文の形では用いられない。その代りに、PINは暗号化され、暗号化されたPINが、暗号化されたワンタイムパスワードを解読するために必要なキーを生成する際の１つの要素として用いられる。208に示したように、ユーザPINは、携帯用記憶装置内の保護されたエリアに格納されていた値Ksを用いて暗号化される。保護されたエリアへのアクセスは、携帯用記憶装置の認証を経た後にのみ、可能になる。

【００５５】

プラグインモジュールは、210で、暗号化されたセッションキーKsを取り出し、そして、208で、ユーザが提供したPINを暗号化するために、それを用いる。このように、処理におけるこの段階で、プラグインモジュールは、ワンタイムパスワードを生成するために必要な３個の情報、すなわちKs、Ei及びKiを持っている。インデックス値iは、202で、暗号化されたワンタイムパスワードEiの中から選択された１つを取り出すために用いられる。暗号化されたPINであるE_{Ks}は、排他的論理和(XOR)動作を通して、値Kiと結合され、その結果は、暗号化されたワンタイムパスワードEiを解読するために用いられる。解読処理を、図７の214に示す。解読処理は、図７の216に示すように、単一のワンタイムパスワードSiを生成する。それから、このワンタイムパスワードは、218で、ゲートウェイに返送される。すると、ゲートウェイは、このワンタイムパスワードを、安全なデータベース（図４における安全なデータベース73）内に格納されていたワンタイムパスワードと比較し、遠隔クライアントであるのか、あるいは、安全な通信を進めるための認証がなされていないものであるのかを検証することができる。

【００５６】

前述したように、安全な信用できるネットワークとの直接の通信の全ては、選別ルータ40によって遮断されている。適切な認証が行われた後のプロキシシステムのみが、信用できるネットワークへアクセスして、遠隔クライアントの代わりに、情報及びサービスを取得することができる。そのタスクを実行する際に、プロキシシステムは、URLの有効性検査及び変更の処理を実行する。これらの有効性検査及び変更の処理の詳細を、図９及び１０

に示す。

【００５７】

遠隔クライアントとホームのホストとの間の通信が、SSLに基づく暗号化によって保護されているという事実にもかかわらず、我々は、適切に認証されたクライアントのみが、正当なURLを送出することが可能な当事者になれることを保証するという方法で、セキュリティを更に強化することを提案する。このアプローチは、たとえSSLチャネルが侵入者によって損なわれたとしても、全てのURLを「防弾」状態に保つことができる。

【００５８】

各ウェブページは、ウェブプロキシを通過して、遠隔クライアントに至るので、ホームサイトに対する、それぞれの内部のhref照会先は、図１０に示したURL変更モジュール90によって、下記のように書き直される。

【数２】

$$\text{https://gateway\_host/home\_host/MSB/}_{64}\{MD5_{128}((\text{0riginal\_URL}\|\text{User\_ID})\oplus S_i\}/\text{Original\_URL/?UserID=db, where } S_i = D_{Ki\oplus Eks(PIN)}(E_i)$$

【００５９】

そして、この照会先がURLになり、遠隔クライアントは、このURLを受信し、かつ、ウェブプロキシサーバに対する要求の中に、このURLを含ませる。全体の処理を、図１０に示す。変更されたURLが遠隔クライアントからゲートウェイに到着したとき、URL検証（有効性検査）モジュール92は、その信頼性を検証する。それから、URL変更モジュールが、このURLを、下記のような通常の形に変換する。

http://home_host/0riginal_URL

これは、ウェブプロキシが信用できるホームネットワーク上に発する要求になる。なお、URL変更処理が、双方向性のものであることに注目すべきである。遠隔クライアントから入って来るURLは、（認証において、）そのクライアント固有の方法で変更される。同様に、遠隔クライアントに送出されるURLは、同じ変更規則を用いて変更される。

【００６０】

Siが、ある遠隔クライアントセッション（W=30分）の間のみ有効であれば、たとえ基礎をなすSSL接続が損なわれても、侵入者が獲得したURLは、いかなる将来のセッションにおいても照会の役には立たない。

【００６１】

ワンタイムパスワードを遠隔クライアントに安全に配布する携帯用記憶装置は、ネットワークセキュリティシステムの重要な部分を形成している。上述したように、このシステムは、ゲートウェイに備えられた初期化及び設定ソフトウェアを用いて、ユーザが、自身の携帯用記憶装置を簡単に設定できるように設計されている。ここで、携帯用記憶装置の設定の詳細を、図１１を参照して説明する。

【００６２】

ユーザは、遠隔地からのログインを可能にするために、前もって、携帯用記憶装置（遠隔キー）を初期化する必要があり、そのためには、携帯用記憶装置を、ゲートウェイ32における記録装置36のスロットに挿入しなければならない。携帯用記憶装置としてCD/DVD媒体を用いる場合には、ゲートウェイ装置は、携帯用媒体の「ユーザ」エリア及び「保護された」エリアに情報を格納することが可能なCD/DVDライタを装備していなければならない。その処理が、図１１に示されている。遠隔キー管理モジュール70（図４）が、遠隔キー初期化処理を実行する。

【００６３】

おのおのの携帯用記憶装置の初期化処理の間に、ゲートウェイは、１セット（N個）の数値であるユーザワンタイムパスワード(Si)を生成する（図１１におけるステップ(1)）。これらは、乱数発生器から得られた単なる乱数である。これに加えて、ゲートウェイは、

N個のランダムキー(Ki)を生成すると共に、各ワンタイムパスワードと各キーとのペア結合を形成する（図１１におけるステップ(2)）。

【００６４】

ステップ(3)において、ゲートウェイの遠隔キー管理モジュールは、ユーザ側の認証プラグインソフトウェアから、ユーザPINを取得し、ランダムなKsを生成し（ステップ(4)）、キーカードを認証し、そして、携帯用記憶装置の保護されたエリアにKsを格納する（ステップ(5)）。

【００６５】

ステップ(6)において、ゲートウェイの遠隔キー管理モジュール75（図５）は、各ペア結合(Si, Ki)について、下記の値を計算する。

【数３】

$$Ei = E_{ki \oplus Eks(PIN}(S_i)$$

これらの値は、ステップ(7)において、携帯用記憶装置のユーザデータエリアに格納される。

【００６６】

最後に、ユーザID、ユーザPIN、Ks、及びOTPキー－パスワードペア(Si, Ki)が、遠隔キー認証モジュール70及びASMMモジュール72（図４参照）による将来の照会のために、図４の安全なデータベース(73)内に格納される。

前述のステップのうちのいずれかが、何らかの理由で失敗すると、携帯用記憶装置の初期化処理の全体が失敗となる。

【００６７】

いったん、携帯用記憶装置がキーによって初期化されれば、世界中のどこへでも、ユーザは、それを持ち運び、適切な装備のコンピュータを用いて、ゲートウェイとの安全なクライアント－サーバ通信を行うことができる。ここでの好ましい実施形態においては、遠隔クライアントコンピュータは、（例えば、携帯用記憶装置によって運ばれた）プラグインソフトウェアモジュールをアップロードもしくはインストールする 。プラグインソフトウェアモジュールは、認証を行うのに必要なメッセージの交換にあずかるように、クライアントコンピュータを設定する。また、プラグインソフトウェアモジュールは、遠隔クライアントコンピュータが、ゲートウェイからの情報及びユーザPINを用いて生成されたキーを用いて、携帯用記憶装置に格納されたパスワードのうちの１つを選択して解読することによって、適切なワンタイムパスワードを生成することを可能にする。この好ましい実施形態においては、暗号化された形のユーザPINが、選択されたワンタイムパスワードの解読のために必要なキーを生成するために用いられる。ユーザが平文の形で提供したユーザPINは、携帯用記憶装置内の保護されたエリアに格納されたセッションキーを用いて暗号化される。暗号化されたPINに基づいて認証を行えば、安全なSSLチャネルを通して伝達される情報への野蛮で暴力的な攻撃に対するシステムの脆弱性を減少させることができるので、この好ましい実施形態を更に安全にすることができる。

【００６８】

この好ましい実施形態は、遠隔クライアントのウェブブラウザに対する、いかなる変更をも防止するように設計されている。しかしながら、クライアントのために、前述した携帯用記憶装置に基づく認証処理を実行するためには、ブラウザは、前記携帯用記憶装置にアクセスして、いくらかの補助的な暗号の計算を行うことが可能なプラグインモジュールからの援助を必要とする。図１２に、ブラウザ－プラグイン－ゲートウェイ間の連係の詳細を示す。

【００６９】

図１２のステップ(1)において、遠隔クライアントは、ゲートウェイに、下記の照会を送信する。この照会は、これに続くOTP交換のためにSSLセッションを確立することが必要で

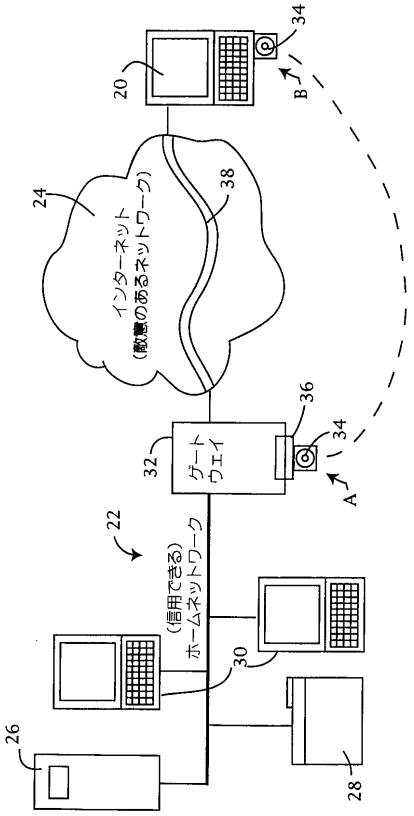
あることを示していて、かつ、クライアントのユーザIDを含んでいる。
http://gw_host/?UserID=user_name
【００７０】
ステップ(2)において、図４に示した遠隔キー認証モジュール70は、<OBJECT>タグを含み、かつ、プラグインのパラメータ列として渡される、プラグイン名、及び、(i)及び(Ki)の値を示しているページによって応答する。この時点で、プラグインは、ユーザの小型装置(widget)を「ポップアップ」し、クライアントにユーザPINを要求する。そして、それが、携帯用記憶装置の、Ei、及び、保護されたエリアからのKsの値にアクセスし、かつ、下記のワンタイムパスワードの値を計算する。
【数４】

$$S_i = D_{Ki \oplus Eks(PIN)}(E_i)$$

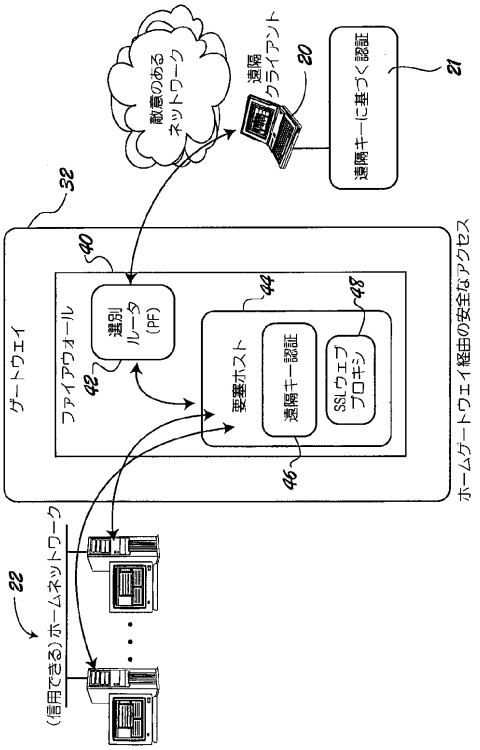
この値は、ステップ(3)で、下記のような形で、同じSSLチャネル経由で、遠隔キー認証モジュールに返送される。
https://gw_host/?UserID=db&Si=123456789ABCDEF0FEDCBA9876543210.
【００７１】
好ましくは、プラグインモジュールは、ゲートウェイの製造業者によって署名されていて、不正操作がきかないようになっているべきである。クッキーの使用もまた、可能である。例えば、クッキーは、ユーザ認証に関与する、クライアントのヘルパーアプリケーションによって変更されてもよい。
【００７２】
【発明の効果】
以上より、本発明が、ユーザにとって使い易く、便利で、かつ非常に安全なシステムを提供し、コンピュータシステムまたはコンピュータネットワークとの安全な通信を実現することが明らかになった。本発明の記述は、単に、現存している具体例に過ぎず、従って、本発明の要旨から逸脱しない変形は、本発明の範囲内にあると解釈されるべきである。そのような変形は、本発明の真意及び範囲からはずれていると見なされるべきではない。
【図面の簡単な説明】
【図１】　好ましい実施形態の概観を示すシステムブロック図である。
【図２】　図１に示したシステムにおける、好ましいゲートウェイの基本的な構成を示すブロック図である。
【図３】　図２に示したゲートウェイの動作を理解するために有益なデータフロー図である。
【図４】　図２に示したゲートウェイにおける、認証及びプロキシモジュールを示す、さらに詳細なブロック図である。
【図５】　図２に示したゲートウェイにおける、ワンタイムパスワード認証メカニズムを示すブロック図である。
【図６】　好ましい認証処理の詳細を示すブロック図である。
【図７】　好ましい認証処理を理解するために有益なデータフロー図である。
【図８】　認証処理を示すシーケンス図である。
【図９】　図２にも示したゲートウェイのブロック図であって、好ましい実施形態のウェブプロキシ機能を示している。
【図１０】　ウェブプロキシモジュールの構成要素のブロック図であり、ユニフォームリソースロケータ(URL)の検証及び変更機能を示している。
【図１１】　携帯用記憶装置を初期化もしくは設定するための好ましい処理を示している。
【図１２】　認証のためにクライアントブラウザプラグインを用いる方法における、更に詳細な動作を示すブロック図である。

【符号の説明】
20 遠隔クライアント（クライアントコンピュータ）
21 遠隔キーに基づく認証処理
22 ホームネットワーク（信用できるコンピュータネットワーク）
24 インターネット
26 サーバ
28 プリンタ
30 コンピュータ
32 ゲートウェイ
34 携帯用記憶装置
36 記録装置
38 パイプライン
40 ファイアウォール
42 選別ルータ
44 要塞ホスト
46 遠隔キー認証機能
48 ウェブプロキシ機能
70 遠隔キー認証モジュール
72 アクティブセッション管理ミドルウェア(ASMM)
73 安全なデータベース
74 URL有効性検査
75 遠隔キー管理モジュール
76 URL変更処理
78 テンプレートページデータベース
90 URL変更モジュール
92 URL検証（有効性検査）モジュール

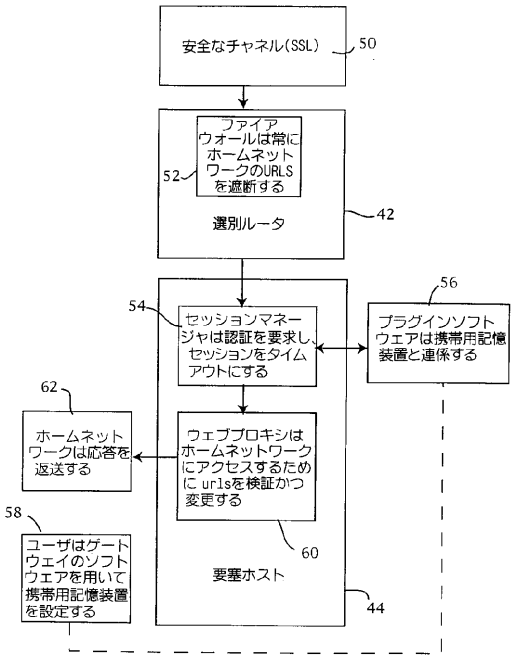
【図１】


20
34
B
24
インターネット
(敵意のあるネットワーク)
38
36
34
A
32
ゲート
ウェイ
22
(信用できる)
ホームネットワーク
30
26
28

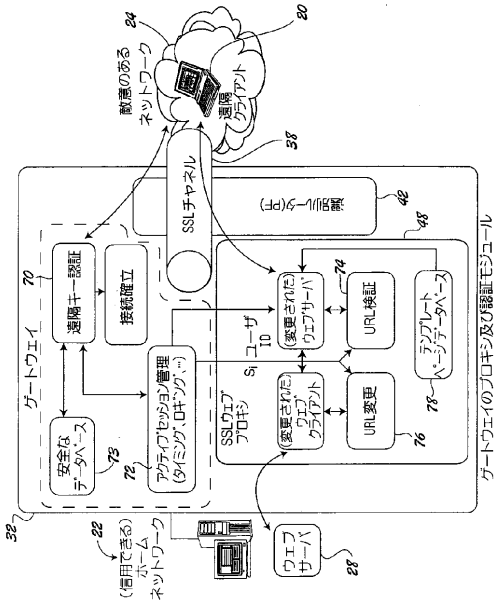
【図２】


敵意のある
ネットワーク
遠隔
クライアント
20
遠隔キーに基づく認証
21
32
ゲートウェイ
ファイアウォール
42
選別
ルータ
(PF)
40
要塞ホスト
44
遠隔キー認証
SSLウェブ
プロキシ
48
46
ホームゲートウェイ経由の安全なアクセス
22
(信用できる)ホームネットワーク

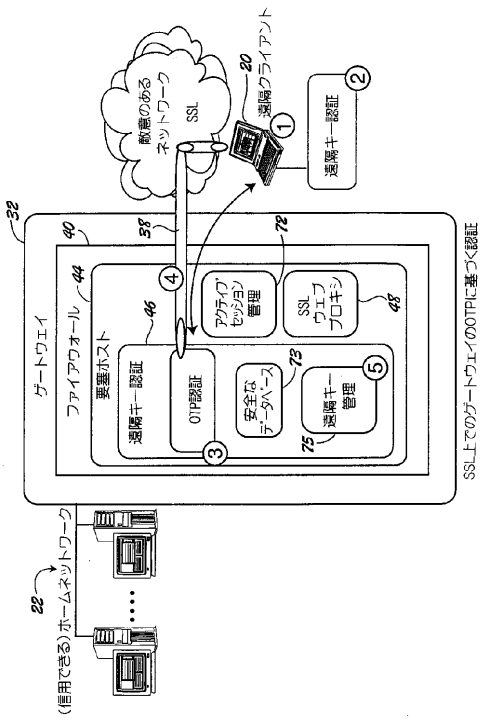
【図３】


安全なチャネル(SSL)
50
ファイア
ウォールは常に
ホームネット
ワークのURLS
を遮断する
52
選別ルータ
42
54
セッションマネー
ジャは認証を要求し、
セッションをタイム
アウトにする
56
プラグインソフト
ウエアは携帯用記憶
装置と連係する
62
ホームネット
ワークは応答を
返送する
ウェブプロキシは
ホームネットワーク
にアクセスするため
にurlsを検証かつ
変更する
60
58
ユーザはゲート
ウェイのソフト
ウエアを用いて
携帯用記憶装置
を設定する
要塞ホスト
44

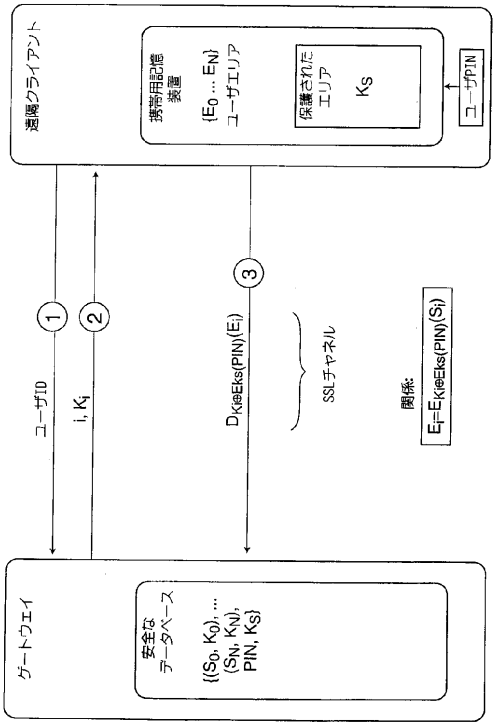
【図４】


敵意の
ネットワーク
24
20
遠隔
クライアント
38
SSLチャネル
選別ルータ(PF)
42
48
ゲートウェイ
70
遠隔キー認証
接続確立
ユーザ
ID
Si
(変更された)
ウェブサーバ
74
URL検証
テンプレート
ページデータベース
78
SSLウェブ
プロキシ
アクティブセッション管理
(タイミング、ログイン、…)
安全な
データベース
72
(変更された)
ウェブ
クライアント
URL変更
76
ゲートウェイのプロキシ及び認証モジュール
32
22
(信用できる)
ホーム
ネットワーク
ウェブ
サーバ
28

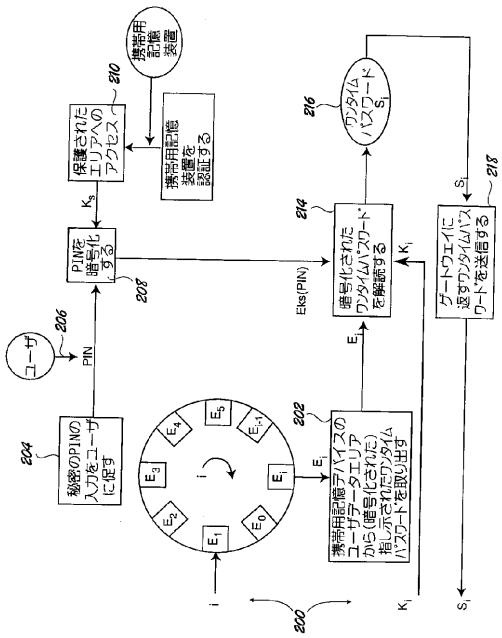
【図５】


敵意のあるネットワーク
SSL
20
遠隔クライアント
遠隔キー認証
32
40
38
72
44
ゲートウェイ
ファイアウォール
46
要塞ホスト
遠隔キー認証
OTP認証
アクティブセッション管理
SSLウェブプロキシ
48
安全なデータベース
73
遠隔キー管理
75
SSL上でのゲートウェイへのOTPに基づく認証
22
(信用できる)ホームネットワーク

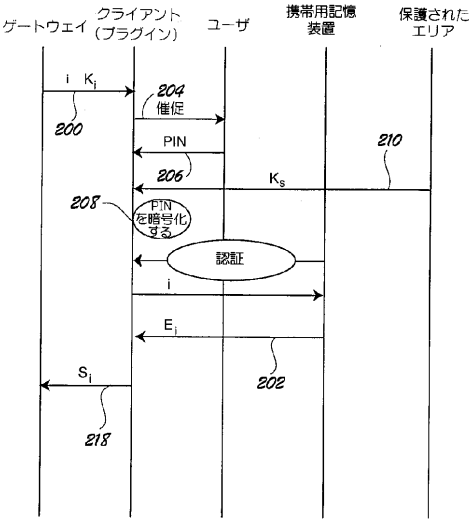
【図６】


遠隔クライアント
携帯用記憶装置
{E0 ... EN}
ユーザエリア
保護されたエリア
KS
ユーザPIN
ユーザID
i, Ki
DKieEks(PIN)(Ei)
SSLチャネル
関係:
EI=EKieEks(PIN)(Si)
ゲートウェイ
安全なデータベース
{(S0, K0), ... (SN, KN), PIN, KS}

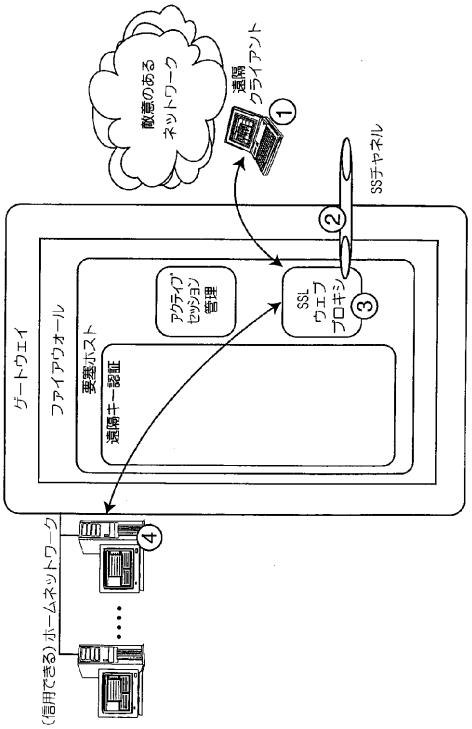
【図７】


携帯用記憶装置
210
保護されたエリアへのアクセス
携帯用記憶装置を認証する
Ks
PINを暗号化する
208
ユーザ
206
PIN
204
秘密のPINの入力をユーザに促す
Eks(PIN)
暗号化されたワンタイムパスワードを解読する
214
216
ワンタイムパスワード Si
Si
218
ゲートウェイに返すワンタイムパスワードを送信する
Ei
202
携帯用記憶デバイスのユーザデータエリアから(暗号化された)指し示されたワンタイムパスワードを取り出す
Ki
i
220

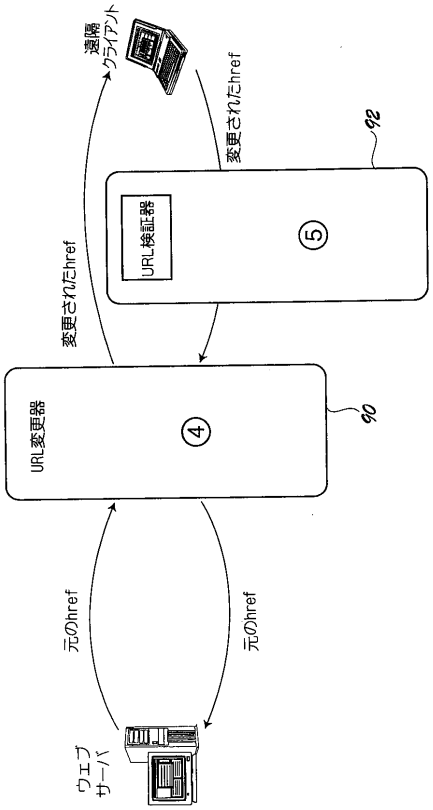
【図８】


ゲートウエイ
クライアント(プラグイン)
ユーザ
携帯用記憶装置
保護されたエリア
i Ki
200
204
催促
PIN
206
Ks
210
208
PINを暗号化
認証
i
EI
202
Si
218

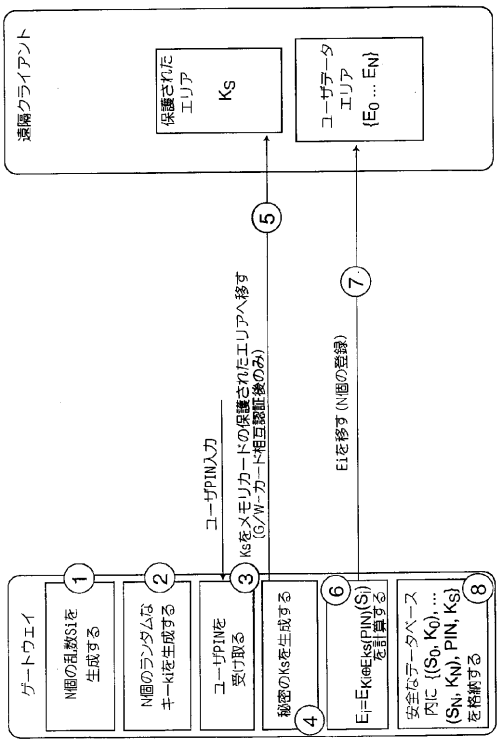
【図９】



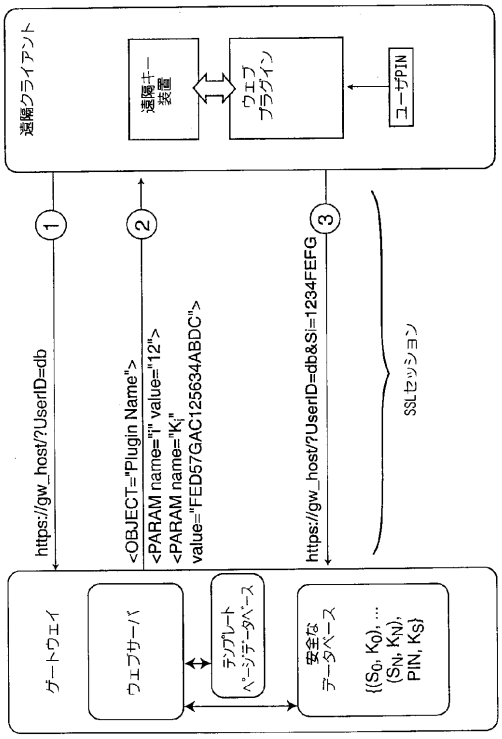
【図１０】



【図１１】



【図１２】



フロントページの続き

(72)発明者　ナサー・メモン
アメリカ合衆国・ニュージャージー・０７７３３・ホルムデル・ダコタ・コート・６
(72)発明者　サスヤ・ナラヤナン
アメリカ合衆国・ニュージャージー・０８６４８・ローレンスヴィル・タウン・コート・ノース・１２２４

審査官　永野　志保

(56)参考文献　特開２０００－２００３１５（ＪＰ，Ａ）
特開平０７－１４０８９７（ＪＰ，Ａ）
特開平０８－２２７３９７（ＪＰ，Ａ）
特開２００１－０５１９３２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20
G06F 13/00