(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4960883号
(P4960883)
(45)発行日　平成24年6月27日(2012.6.27)　(24)登録日　平成24年3月30日(2012.3.30)

(51)Int.Cl.　　F I
G06F 21/20 (2006.01)　　G06F 21/20 144D
H04L 9/32 (2006.01)　　H04L 9/00 673A

請求項の数 36　(全 46 頁)

(21)出願番号	特願2007-547085 (P2007-547085)	(73)特許権者	307043108
(86)(22)出願日	平成17年12月21日 (2005.12.21)		エミュー　ホールディングス　ピーティワイ　リミテッド
(65)公表番号	特表2008-524727 (P2008-524727A)		オーストラリア国　３０００　ビクトリア州　メルボルン　ロンズデール　ストリート　１８０　レベル　１５
(43)公表日	平成20年7月10日 (2008.7.10)	(74)代理人	100083806
(86)国際出願番号	PCT/AU2005/001923		弁理士　三好　秀和
(87)国際公開番号	WO2006/066322	(74)代理人	100095500
(87)国際公開日	平成18年6月29日 (2006.6.29)		弁理士　伊藤　正和
審査請求日	平成20年12月12日 (2008.12.12)	(74)代理人	100111235
(31)優先権主張番号	2004907210		弁理士　原　裕子
(32)優先日	平成16年12月21日 (2004.12.21)		
(33)優先権主張国	オーストラリア(AU)		

最終頁に続く

(54)【発明の名称】認証デバイスおよび／または方法

(57)【特許請求の範囲】
【請求項１】
通信ネットワークを介してユーザに対する遠隔サービスを認証する方法であって、
前記遠隔サービスを提供する遠隔サーバが、第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を獲得する工程と、
前記通信ネットワークを介して前記サービス認証符号を前記ユーザに伝達する工程と、
前記サービス認証符号を受信するか、または前記ユーザに付随する認証デバイスに前記サービス認証符号を入力する工程と、
前記認証デバイスが、第２の秘密鍵に基づき前記符号生成アルゴリズムと同じ符号生成アルゴリズムを使用して予期符号値を生成し、その後該予期符号値を前記サービス認証符号と比較する工程と、
前記比較に応じ、前記予期符号値が前記サービス認証符号と相関する場合に、前記認証デバイスが、前記遠隔サービスの真正性を前記ユーザに示す応答を生成する工程と
を含むことを特徴とする方法。
【請求項２】
前記遠隔サービスが電子商業サービスを含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記電子商業サービスがインターネット商業サービスを含むことを特徴とする請求項１に記載の方法。
【請求項４】

前記サービス認証符号を、前記遠隔サービスを提供する前記遠隔サーバに通信可能に接続する認証サーバが生成することを特徴とする請求項１に記載の方法。
【請求項５】
前記ユーザが提供する符号に関連する前記第１の秘密鍵を取り出すために、前記遠隔サービスにアクセスするために登録した各認証デバイスの符号、および前記各認証デバイスの符号に関連する前記第１の秘密鍵を含むデータベースへの前記ユーザが提供する符号の索引付けを行うことにより、前記第１の秘密鍵を取り出すことを特徴とする請求項１に記載の方法。
【請求項６】
前記ユーザが提供する符号が前記認証デバイスを唯一に特定することを特徴とする請求項５に記載の方法。
【請求項７】
前記サービス認証符号の前記生成が、前記第１の秘密鍵を符号化し、一回使用可能な認証符号を提供することを特徴とする請求項１に記載の方法。
【請求項８】
前記符号生成アルゴリズムの各インスタンスは、第１の擬似ランダム符号化シーケンス、および第２の擬似ランダム符号化シーケンスを使用し、前記第２の擬似ランダム符号化シーケンスが前記第１の擬似ランダム符号化シーケンスと同じシーケンス長を有することを特徴とする請求項７に記載の方法。
【請求項９】
前記第１の擬似ランダム符号化シーケンスは各文字が一度だけ現れる文字のシーケンスを含み、前記文字のシーケンスが前記第１の秘密鍵を導出する文字セットを形成し、従って前記第１の擬似ランダム符号化シーケンスが前記第１の秘密鍵の文字を備えることを特徴とする請求項８に記載の方法。
【請求項１０】
前記第２の擬似ランダム符号化シーケンスが、前記第１の秘密鍵と異なる文字セットの文字の配列を含むことを特徴とする請求項８に記載の方法。
【請求項１１】
前記サービス認証符号または前記予期符号値をそれぞれ生成するための前記符号生成アルゴリズムは、
前記第１の秘密鍵または前記第２の秘密鍵の文字に対応する前記第１の擬似ランダム符号化シーケンスにおける前記文字の位置を順次特定する工程と、
前記第１の擬似ランダム符号化シーケンスにおいて特定した前記文字の前記位置を、前記位置と同じシーケンス位置を有する前記第２の擬似ランダム符号化シーケンスの文字に対応付け、前記第２の擬似ランダム符号化シーケンスから文字セットを提供する工程と、
前記サービス認証符号を形成するように前記第２の擬似ランダム符号化シーケンスの前記文字セットを特定した順に配列する工程と
を含むことを特徴とする請求項８に記載の方法。
【請求項１２】
サービス認証符号を生成する場合は常に異なる第１および第２の擬似ランダム符号化シーケンスを使用し、同じサービス認証符号を再生成する見込みを削減することを特徴とする請求項８に記載の方法。
【請求項１３】
前記応答は、前記認証デバイスが前記遠隔サービスに対し前記ユーザを認証するユーザ認証符号を生成するために動作することを含むことを特徴とする請求項１に記載の方法。
【請求項１４】
前記ユーザに通常アクセスできないように前記認証デバイスのボード上のメモリに、前記第２の秘密鍵を格納することを特徴とする請求項１に記載の方法。
【請求項１５】
前記サービス認証符号は、前記サービス認証符号を生成する前記符号生成アルゴリズム

を、前記予期符号値を生成する前記符号生成アルゴリズムと同期させる特定情報を含むことを特徴とする請求項１に記載の方法。

【請求項１６】

前記第１の秘密鍵に基づき前記サービス認証符号を生成する前記符号生成アルゴリズム、および前記第２の秘密鍵に基づき前記予期符号値を生成する前記符号生成アルゴリズムは、前記第１の秘密鍵および前記第２の秘密鍵に基づき前記サービス認証符号および前記予期符号値をそれぞれ生成する同期符号化シーケンスを使用することを特徴とする請求項１に記載の方法。

【請求項１７】

サービス認証符号を生成する度毎に、前記符号化シーケンスを修正することを特徴とする請求項１６に記載の方法。

【請求項１８】

通信ネットワークを介してユーザに対する遠隔サービスを認証する方法であって、

前記遠隔サービスを提供する遠隔サーバが、第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を獲得する工程と、

前記通信ネットワークを介して前記サービス認証符号を前記ユーザに伝達する工程と、

前記サービス認証符号を受信するか、または前記ユーザに付随する認証デバイスに前記サービス認証符号を入力する工程と、

前記認証デバイスが、第２の秘密鍵に基づき前記符号生成アルゴリズムと同じ符号生成アルゴリズムを使用して予期符号値を生成し、その後該予期符号値を前記サービス認証符号と比較する工程と、

前記比較に応じ、前記予期符号値が前記サービス認証符号と相関する場合に、前記認証デバイスが、前記遠隔サービスの真正性を前記ユーザに示す応答を生成する工程と

を含み、

前記第１の秘密鍵に基づき前記サービス認証符号を生成する前記符号生成アルゴリズム、および前記第２の秘密鍵に基づき前記予期符号値を生成する前記符号生成アルゴリズムが、前記第１の秘密鍵および前記第２の秘密鍵に基づき前記サービス認証符号および前記予期符号値をそれぞれ生成する同期符号化シーケンスを使用することを特徴とする方法。

【請求項１９】

通信ネットワークを介して遠隔サービスのユーザと前記遠隔サービスを相互に認証する方法であって、

前記遠隔サービスを提供する遠隔サーバが、第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を獲得する工程と、

前記通信ネットワークを介して前記サービス認証符号を前記ユーザに伝達する工程と、

前記サービス認証符号を受信するか、または前記ユーザに付随する認証デバイスに前記サービス認証符号を入力する工程と、

前記認証デバイスが、第２の秘密鍵に基づき前記符号生成アルゴリズムと同じ符号生成アルゴリズムを使用して予期符号値を生成し、その後該予期符号値を前記サービス認証符号と比較する工程と、

前記比較に応じ、前記予期符号が前記サービス認証符号と相関する場合に、前記認証デバイスが、第３の秘密鍵に基づき符号生成アルゴリズムを使用してユーザ認証符号を生成する工程と、

前記通信ネットワークを介して前記ユーザ認証符号を前記遠隔サービスを提供する前記遠隔サーバに伝達する工程と、

前記遠隔サービス、またはその他のサービスを提供する前記遠隔サーバが、第４の秘密鍵に基づき生成した第２の予期符号値を獲得し、その後該第２の予期符号値を前記ユーザ認証符号と比較する工程と、

前記比較に応じ、前記第２の予期符号値が前記ユーザ認証符号と相関する場合に、前記遠隔サービスを提供する前記遠隔サーバが、前記ユーザにさらに前記遠隔サービスへアクセスすることを可能にする工程と

を含むことを特徴とする方法。
【請求項２０】
第１の秘密鍵に基づき符号生成アルゴリズムを使用してサービス認証符号を生成するサービス認証符号生成器手段であって、前記サービス認証符号の生成が、第１の擬似ランダム符号化シーケンス、および第１の擬似ランダム符号化シーケンスと同じシーケンス長を有する第２の擬似ランダム符号化シーケンスを使用して前記第１の秘密鍵を符号化する工程を含むサービス認証符号生成器手段、および通信ネットワークを介して前記サービス認証符号を遠隔ユーザに伝達する通信手段をサーバ上で実装するためのソフトウェアプログラムであって、
前記符号化する工程が、
前記第１の秘密鍵の文字に対応する前記第１の擬似ランダム符号化シーケンスにおける前記文字の位置を順次特定する工程と、
前記位置と同じシーケンス位置を有する前記第２の擬似ランダム符号化シーケンスの文字に特定した前記文字の前記シーケンス位置を対応付け、前記第２の擬似ランダム符号化シーケンスの文字セットを提供する工程と、
前記サービス認証符号を形成するように前記第２の擬似ランダム符号化シーケンスの前記文字セットを特定した順に配列する工程と
を含み、
前記サービス認証符号は、前記符号生成アルゴリズムが使用する前記第１および第２の擬似ランダム符号化シーケンスに従い変化し、
サービス認証符号を生成する場合には常に異なる第１および第２の擬似ランダム符号化シーケンスを使用し、同じサービス認証符号を再生成する見込みを削減することを特徴とするソフトウエアプログラム。
【請求項２１】
認証デバイス上で以下の手段を実装するためのソフトウエアプログラムであって、
遠隔サービスを提供する遠隔サーバが提供する第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を受信あるいは入力する入力手段と、
第２の秘密鍵に基づき前記符号生成アルゴリズムを使用して予期符号値を生成する生成器手段と、
前記予期符号値を前記サービス認証符号と比較する比較器手段と、
前記予期符号値の前記サービス認証符号との比較に従い、前記遠隔サービスの真正性を示す応答を生成する応答生成器手段と
を実装することを特徴とするソフトウエアプログラム。
【請求項２２】
遠隔サービスを提供する遠隔サーバが提供するサービス認証符号に基づき遠隔サービスの真正性を示す応答を認証デバイスのユーザに提供する認証デバイスであって、
第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成した前記サービス認証符号を受信あるいは入力する入力手段と、
第２の秘密鍵に基づき前記符号生成アルゴリズムと同じ符号生成アルゴリズムを使用して予期符号値を生成する生成器手段と、
前記予期符号値を前記サービス認証符号と比較する比較器手段と、
前記予期符号値の前記サービス認証符号との比較に従い、前記遠隔サービスの前記真正性を示す応答を生成する応答生成器手段と
を備えることを特徴とする認証デバイス。
【請求項２３】
各符号生成アルゴリズムは、第１の擬似ランダム符号化シーケンス、および第２の擬似ランダム符号化シーケンスを使用し、前記第２の擬似ランダム符号化シーケンスは、前記第１の擬似ランダム符号化シーケンスと同じシーケンス長を有することを特徴とする請求項２２に記載の認証デバイス。
【請求項２４】

前記第１の擬似ランダム符号化シーケンスは、各文字が一度だけ現れる文字のシーケンスを含み、前記文字のシーケンスは、前記第１の秘密鍵を導出する文字セットを形成し、従って前記第１の擬似ランダム符号化シーケンスは、前記第１の秘密鍵の文字を備えることを特徴とする請求項２３に記載の認証デバイス。

【請求項２５】

前記第２の擬似ランダム符号化シーケンスは、前記第１の秘密鍵と同じかまたは異なる文字セットの文字の配列を備えることを特徴とする請求項２３に記載の認証デバイス。

【請求項２６】

前記予期符号値をそれぞれ生成する前記符号生成アルゴリズムは、

前記第２の秘密鍵の文字に対応する前記第１の擬似ランダム符号化シーケンスにおける前記文字の位置を順次特定するステップと、

前記第１の擬似ランダム符号化シーケンスにおいて特定した前記文字の前記位置を、前記位置と同じシーケンス位置を有する前記第２の擬似ランダム符号化シーケンスの文字に対応付け、前記第２の擬似ランダム符号化シーケンスから文字セットを提供するステップと、

前記サービス認証符号を形成するように前記第２の擬似ランダム符号化シーケンスの前記文字セットを特定した順に配列するステップと

を備えることを特徴とする請求項２３に記載の認証デバイス。

【請求項２７】

サービス認証符号を生成する場合は常に異なる第１および第２の擬似ランダム符号化シーケンスを使用し、同じサービス認証符号を再生成する見込みを削減することを特徴とする請求項２３に記載の認証デバイス。

【請求項２８】

前記応答は、前記認証デバイスが前記遠隔サービスに対し前記ユーザを認証するユーザ認証符号を生成するために動作することを備えることを特徴とする請求項２２に記載の認証デバイス。

【請求項２９】

前記第２の秘密鍵を、前記ユーザに通常アクセスできないように前記認証デバイスのボード上のメモリに格納することを特徴とする請求項２２に記載の認証デバイス。

【請求項３０】

前記サービス認証符号は、前記ユーザ認証符号を生成する前記符号生成アルゴリズムを、前記予期符号値を生成する前記符号生成アルゴリズムと同期させる特定情報を備えることを特徴とする請求項２２に記載の認証デバイス。

【請求項３１】

前記第１の秘密鍵に基づき前記サービス認証符号を生成する前記符号生成アルゴリズム、および前記第２の秘密鍵に基づき前記予期符号値を生成する前記符号生成アルゴリズムは、前記第１の秘密鍵および前記第２の秘密鍵に基づき前記サービス認証符号および前記予期符号値をそれぞれ生成する同期符号化シーケンスを使用することを特徴とする請求項２２に記載の認証デバイス。

【請求項３２】

前記サービス認証符号を生成する度毎に、前記符号化シーケンスを修正することを特徴とする請求項３１に記載の認証デバイス。

【請求項３３】

通信ネットワークを介してユーザに対する遠隔サービスを認証する方法であって、

前記ユーザが、認証デバイスを動作させ、該認証デバイスから該認証デバイスに関連する唯一の識別符号を取り出す工程と、

前記通信ネットワークを介して前記唯一の識別符号を前記遠隔サービスを提供する遠隔サーバに伝達する工程と、

前記遠隔サービスを提供する前記遠隔サーバが、前記遠隔サービスにアクセスするために登録した認証デバイスの識別符号を備えるデータベースへの前記唯一の識別符号の索引

付けにより、前記データベースから取り出す前記第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を獲得する工程と、
前記通信ネットワークを介して前記サービス認証符号を前記ユーザに伝達する工程と、
前記サービス認証符号を受信するか、または前記ユーザに付随する認証デバイスに前記サービス認証符号を入力する工程と、
前記認証デバイスが、第２の秘密鍵に基づき前記符号生成アルゴリズムと同じ符号生成アルゴリズムを使用して予期符号値を生成し、その後該予期符号値を前記サービス認証符号と比較する工程と、
前記比較に応じ、前記予期符号値が前記サービス認証符号と相関する場合に、前記認証デバイスが、前記遠隔サービスの真正性を前記ユーザに示す応答を生成する工程と
を含むことを特徴とする方法。
【請求項３４】
通信ネットワークを介して遠隔サービスを使用する第１のユーザに対して第２のユーザの識別および／または信任情報を認証する方法であって、
前記第１のユーザが、請求項１に記載の方法を使用して前記遠隔サービスを認証する工程と、
前記遠隔サービスを有効に認証する場合、前記第１のユーザが、前記第２のユーザに関連するか、または前記第２のユーザが提供する第１の秘密鍵に基づき、前記第２のユーザの認証デバイスが生成したユーザ認証符号を提供する工程と、
前記通信ネットワークを介して前記ユーザ認証符号を前記遠隔サービスを提供する遠隔サーバに伝達する工程と、
前記遠隔サービスを提供する前記遠隔サーバが、第２の秘密鍵に基づき生成した予期符号値を獲得し、その後該予期符号値を前記第２のユーザの前記ユーザ認証符号と比較する工程と、
前記比較に応じ、前記予期符号値が前記ユーザ認証符号と相関する場合に、前記遠隔サービスを提供する前記遠隔サーバが、前記第２のユーザの真正性を示す応答を前記第１のユーザに提供する工程と
を含むことを特徴とする方法。
【請求項３５】
請求項２２に記載の認証デバイスを作成する方法であって、
ユーザが、作成されると認証デバイスとなる携帯デバイスにおいて、実行またはインストールするために、請求項２１に記載のソフトウエアプログラムを提供する遠隔サーバにアクセスする工程と、
前記遠隔サーバが、前記携帯デバイスに前記ソフトウエアプログラムを伝達する工程と、
前記携帯デバイスにおいて、前記ソフトウエアプログラムを実行するか、またはインストールして認証デバイスを作成する工程と
を含むことを特徴とする方法。
【請求項３６】
前記ソフトウエアプログラムを、
（ａ）ショートメッセージサービス、
（ｂ）電子メールサービス、または
（ｃ）パケットベース通信サービス、
を介して伝達することを特徴とする請求項３５に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザへの遠隔サービスを認証する方法およびデバイスに関する。典型的なアプリケーションでは、認証方法またはデバイスを通信ネットワークに接続するワークステーションを動作させるユーザに対してウェブサイトなどの遠隔サービスを認証するため

に使用することができる。一方、認証デバイスまたは方法は、また遠隔せービスに対してユーザの認証、または実際遠隔サービスおよびユーザを相互に認証するためにも使用することができる。

【背景技術】

【０００２】

従来の認証方法およびデバイスでは典型的に遠隔サービスに対するユーザの認証を可能にする。典型的には、従来の認証方法は、単にユーザからパスワードを要求することによりユーザを認証する遠隔サービスを伴う。

【０００３】

従って、ユーザにはユーザが望む、または正しい遠隔サービスと本当に通信しているのかを知る方法がない。従って、遠隔コンピュータが遠隔サービスの動作を真似ることができれば、ユーザは「騙され」るか、または「フィッシュされ」、ユーザが正しい遠隔サービスと通信していると考えるようになることがある。その結果、疑うことのないユーザは、そうでなければ合法的遠隔サービスにしか漏らさない、例えばそのＩＤおよびパスワードなどの情報を漏らすことがある。

【発明の開示】

【発明が解決しようとする課題】

【０００４】

従って、少なくともユーザに対して遠隔サービスを認証するのに適する認証デバイスおよび／または方法を提供することが本発明の目的である。

【０００５】

本発明に関して説明するために、本明細書には本発明に対する背景技術の説明を含む。これは、参照する文献が、本願の優先期日において公開され、既知であるか、または共通する一般的知見の一部であることを認めるものとするわけではない。

【課題を解決するための手段】

【０００６】

本発明は通信ネットワークを介してユーザに対する遠隔サービスを認証する方法を提供し、本方法は、

遠隔サービスが、第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を獲得する工程と、

通信ネットワークを介してサービス認証符号をユーザに伝達する工程と、

サービス認証符号を受信するか、またはユーザに付随する認証デバイスにサービス認証符号を入力する工程と、

認証デバイスが、第２の秘密鍵に基づき同じ符号生成アルゴリズムを使用して予期符号値を生成し、その後その予期符号値をサービス認証符号と比較する工程と、

その比較に応じ、予期符号値がサービス認証符号と相関する場合に、認証デバイスが、遠隔サービスの真正性をユーザに示す応答を生成する工程

とを含む。

【０００７】

認証デバイスが、遠隔サービスが真正であることをユーザに示す応答を生成するために、第１の秘密鍵は第２の秘密鍵と同じでなければならない。第１の秘密鍵が第２の秘密鍵と異なれば、予期符号値はサービス認証符号と異なろうし、従って認証デバイスは遠隔サービスを認証しないだろう。

【０００８】

ある実施形態では、遠隔サービスはユーザからの要求に応じて、データベースから取り出した第１の秘密鍵に基づき、サービス認証符号を生成した認証サーバからサービス認証符号を獲得する。ある実施形態では、要求はユーザに付随する認証デバイスを特定する符号(以後「起動符号」)を包含するメッセージを含む。その実施形態によれば、認証サーバは符号に関連する第１の秘密鍵を、遠隔サービスにアクセスするために登録した各認証デバイスの符号を包含するデータベースから取り出す。

【０００９】
ある実施形態では、第２の秘密鍵は認証デバイスと唯一に関連する秘密鍵である。
【００１０】
認証することができる遠隔サービスのタイプは変化するだろう。典型的には、遠隔サービスは電子商業サービスを含むだろう。当然、電子商業サービスはプログラム化コンピュータおよび通信技術を使用して、商品およびサービスの購入および販売を可能にする遠隔サービスである。ある実施形態では、遠隔サービスは金融取引（例えば、ウェブベース銀行取引サービス）を行う電子商業「ウェブベース」サービス、（電話口座管理サービスなどの）ユーザ口座管理サービス、株取引サービス、予約サービス、注文処理サービス、在庫管理サービス、オンライン・オークション・サービス、オンライン買い物サービス、電子メッセージングサービスを含むことができる。
【００１１】
適する通信技術に関しては、適する通信ネットワークは（ＴＣＰ／ＩＰローカル・エリア・ネットワーク、またはインターネットなどの）データ・パケット・ベース通信、無線アプリケーションプロトコル（wireless-application protocol、ＷＡＰ）ネットワーク、（公衆交換電話ネットワークなどの）電話ネットワークまたはその他の適する通信ネットワークをサポートするネットワークを含むことができる。当然、遠隔サービスおよび通信ネットワークの先の例は例示に過ぎず、制限するものと考えるものではない。さらに当然、実際の通信ネットワークは遠隔サービスのタイプおよびユーザがサービスにアクセスするためのそのサービスとユーザとの間の必要な相互接続性に依存するだろう。例えば遠隔サービスが、顧客のワークステーションによりユーザにアクセス可能なウェブベースサービスである実施形態では、通信ネットワークはインターネットでありうる。
【００１２】
ある実施形態では、サービス認証符号を生成する符号生成アルゴリズムを遠隔サービスが提供する。一方代替実施形態では、符号生成アルゴリズムを認証サーバが提供し、認証サーバは遠隔サービスから離れているが、遠隔サービスの要求に応じて認証サーバにアクセスでき、サービス認証符号を生成する。このような実施形態では、認証サーバはサービス認証符号を生成後、サービス認証符号を遠隔サービスに提供する。
【００１３】
ある実施形態では、サービス認証符号の生成は、サービス認証符号を提供するために第１の秘密鍵の符号化を伴う。サービス認証符号を提供するための第１の秘密鍵の符号化は適する符号生成アルゴリズムを使用して実行することができる。１つの適する符号生成アルゴリズムは第１の擬似ランダム符号化シーケンス、および第１の擬似ランダム符号化シーケンスと同じシーケンス長を有する第２の擬似ランダム符号化シーケンスを使用して第１の秘密鍵を符号化する。その実施形態によれば、サービス認証符号を生成する度毎に、符号生成アルゴリズムが異なる第１および第２の擬似ランダム符号化シーケンスを使用する。
【００１４】
ある実施形態では、第１の擬似ランダム符号化シーケンスは、第１の秘密鍵の文字を含む文字セットを形成する１つだけ生じる文字（例えば、アルファベット、数字および／またはアルファニューメリック文字など）のシーケンスを含む。即ち一実施形態では、第１の秘密鍵を第１の擬似ランダム符号化シーケンスを形成するのに使用するのと同じ文字セットから導出する。この点に関して、本明細書を通じて用語「文字セット」への言及は、数字文字、またはアルファニューメリック文字、またはアルファベット文字を含む文字セットへの言及であると理解すべきである。さらに、用語「１つだけ生じる」への言及は、各文字が一度だけ現れる文字セットへの言及であると理解すべきである。
【００１５】
ある実施形態では、第２の擬似ランダム符号化シーケンスは第１の秘密鍵と同じか、または異なる文字セットの文字の配列を含む。とはいえある実施形態では、第２の擬似ランダム符号化シーケンスは第１の擬似ランダム符号化シーケンスと同じシーケンス長を有す

る。この点に関して、本明細書を通じて用語「シーケンス長」への言及は、シーケンスにおける文字数に言及するものと理解すべきである。従って、１０文字を含む符号化シーケンスは１０のシーケンス長を有するだろう。

【００１６】

サービス認証符号および予期符号値を同じ符号生成アルゴリズムを使用して生成するので、符号生成アルゴリズムの各インスタンスは、同じ第１および第２の擬似ランダム符号化シーケンスを使用してサービス認証符号または予期符号値をそれぞれ生成する。

【００１７】

以上に記述したタイプの第１および第２の擬似ランダム符号化シーケンスを使用する符号生成アルゴリズムでは、サービス認証符号を生成する第１の秘密鍵の符号化は、

第１の秘密鍵の文字に対応する第１の擬似ランダム符号化シーケンスにおける文字の位置を順次特定する工程と、

特定した文字のシーケンス位置を同じシーケンス位置を有する第２の擬似ランダム符号化シーケンスの文字に対応付け、第２の擬似ランダム符号化シーケンスから文字セットを提供する工程と、

サービス認証符号を形成するために第２の擬似ランダム符号化シーケンスの文字セットを特定順に配列する工程

と含む。

【００１８】

ある実施形態では、サービス認証符号を生成する場合は常に、異なる第１および第２の擬似ランダム符号化シーケンスを使用し、同じサービス認証符号を再生成する見込みを削減する。従って一実施形態では、各サービス認証符号は実際上一回使用可能な符号である。

【００１９】

個々の符号生成の場合に使用する第１および第２の擬似ランダム符号化シーケンスを遠隔サービスにサービス認証符号を提供する符号生成アルゴリズムのインスタンスにより選択することができる。この点に関して、本明細書を通じて用語「符号生成の場合」への言及は、符号生成アルゴリズムの一度の繰り返しへの言及であると理解すべきである。

【００２０】

ある実施形態では、第１および第２の擬似ランダム符号化シーケンスを符号化するシーケンスのそれぞれの配列から選択し、サービス認証符号を生成するたび毎に異なる第１および第２の擬似ランダム符号化シーケンスを選択する。

【００２１】

第１および第２の擬似ランダム符号化シーケンスを配列要素として包含するそれぞれの配列を含む実施形態では、各配列は有限数の符号生成の場合をサポートすることにする。符号生成の場合の数は典型的にその配列における配列要素の数に対応するだろう。一実施形態では、配列における各シーケンスを使用してサービス認証符号を生成した後、各配列要素における各文字を配列要素内の異なる位置に制御可能に移し、それぞれの符号化シーケンスを変更する。

【００２２】

以前に記述したように、符号生成アルゴリズムの各インスタンスは、同じ第１および第２の擬似ランダム符号化シーケンスを使用してサービス認証符号または予期符号値をそれぞれ生成する。従って、個々の符号生成の場合に使用する第１および第２の擬似ランダム符号化シーケンスを、サービス認証符号を生成する符号生成アルゴリズムが選択する実施形態では、本方法は、

サービス認証符号を生成するのに使用する第１および第２の擬似ランダム符号化シーケンスを特定する特定情報をユーザに伝達する工程と、

特定情報を受信するか、またはユーザに付随する認証デバイスに特定情報を入力し、認証デバイスの符号生成アルゴリズムが使用して、第２の秘密鍵に基づき予期符号値の生成に使用する第１および第２の擬似ランダム符号化シーケンスを特定する工程

とをさらに含む。

【００２３】

サービス認証符号を、典型的に通信ネットワークがサポートする通信プロトコルを使用してユーザに伝達することにする。例えば、インターネットベースの遠隔サービスに対する通信は、サービス認証符号を提供するウェブページにユーザを接続するユニフォーム・リソース・ロケータ（uniform resource locator、ＵＲＬ）を含むＨＴＭＬファイルを含むことができる。あるいはサービス認証符号を、電子メールメッセージ、ショートメッセージサービス（Short Message Service、ＳＭＳ）のテキストメッセージ、サービス認証符号を読み上げる可聴メッセージ（例えば、ＭＰ３またはＷＡＶファイルベースのメッセージ）、ビデオベースのメッセージ、グラフィックメッセージ（例えば、ｊｐｅｇファイル）またはサービス認証符号を含むマルチメディア・メッセージング・プロトコルなどの別のメッセージング機構により伝達することができる。

【００２４】

ある実施形態では、遠隔サービスの真正性をユーザに示すために認証デバイスが生成する応答は、有効な認証信号をユーザに提供する認証デバイスを含む。再度、第１の秘密鍵および第２の秘密鍵が同じである場合にのみ、有効な認証信号を生成することにする。

【００２５】

別の実施形態では、遠隔サービスの真正性をユーザに示すために認証デバイスが生成する応答は、第３の秘密鍵に基づきユーザ認証符号を生成するために起動する認証デバイスを備える。

【００２６】

ある実施形態では、第３の秘密鍵は、ユーザの個人特定番号（personal identification number、ＰＩＮ）などのユーザに関連する秘密鍵である。ある実施形態では、ユーザ認証符号を遠隔サービスに対してユーザを認証するために使用する。

【００２７】

遠隔サービス対してユーザを認証するために、第３の秘密鍵に基づきユーザ認証符号を生成する実施形態では、ユーザ認証を、以前に記述したように同じ符号生成アルゴリズムを使用して実行することにするが、ユーザ認証サービスにアクセス可能な第４の秘密鍵に基づくことにする。ある実施形態では、ユーザ認証サービスを遠隔サービスが提供する。一方別の実施形態では、ユーザ認証サービスを認証サーバが提供し、ユーザ認証の結果を遠隔サービスに伝達する。

【００２８】

従って本発明は、また通信ネットワークを介して遠隔サービスに対するユーザを認証する方法を提供し、本方法は、

認証デバイスが、第３の秘密鍵に基づき符号生成アルゴリズムを使用してユーザ認証符号を生成する工程と、

通信ネットワークを介してサービス認証符号を遠隔サービスに伝達する工程と、

遠隔サービス、またはその他のサービスが、第４の秘密鍵に基づき生成した予期符号値を獲得し、その後予期符号値をユーザ認証符号と比較する工程と、

その比較に応じ、予期符号値がユーザ認証符号と相関する場合に、遠隔サービスがユーザにさらに遠隔サービスへのアクセスを可能にする工程

とを含む。

【００２９】

本発明は、また通信ネットワークを介して遠隔サービスのユーザおよび遠隔サービスを相互に認証する方法を提供し、本方法は、

遠隔サービスが、第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を獲得する工程と、

通信ネットワークを介してサービス認証符号をユーザに伝達する工程と、

サービス認証符号を受信するか、またはユーザに付随する認証デバイスにサービス認証符号を入力する工程と、

認証デバイスが、第２の秘密鍵に基づき同じ符号生成アルゴリズムを使用して予期符号値を生成し、その後予期符号値をサービス認証符号と比較する工程と、
その比較に応じ、予期符号がサービス認証符号と相関する場合に、認証デバイスが、第３の秘密鍵に基づき符号生成アルゴリズムを使用してユーザ認証符号を生成する工程と、
通信ネットワークを介してユーザ認証符号を遠隔サービスに伝達する工程と、
遠隔サービス、またはその他のサービスが、第４の秘密鍵に基づき生成した予期符号値を獲得し、その後予期符号値をユーザ認証符号と比較する工程と、
その比較に応じ、予期符号がユーザ認証符号と相関する場合に、遠隔サービスがユーザにさらに遠隔サービスへアクセスすることを可能にする工程
とを含む。

【００３０】
本発明は、またサーバにおいて実装する１以上のコンピュータ可読記憶媒体上で実施するソフトウエア構成を提供し、本サーバソフトウエア構成は、
第１の秘密鍵に基づき符号生成アルゴリズムを使用してサービス認証符号を生成するサービス認証符号生成器であって、サービス認証符号の生成が、第１の擬似ランダム符号化シーケンス、および第１の擬似ランダム符号化シーケンスと同じシーケンス長を有する第２の擬似ランダム符号化シーケンスを使用する第１の秘密鍵を符号化する工程を含むサービス認証符号生成器を含み、この符号化する工程は、
第１の秘密鍵の文字に対応する第１の擬似ランダム符号化シーケンスにおける文字の位置を順次特定する工程と、
同じシーケンス位置を有する第２の擬似ランダム符号化シーケンスの文字に特定した文字のシーケンス位置を対応付け、第２の擬似ランダム符号化シーケンスから文字セットを提供する工程と、
サービス認証符号を形成するように第２の擬似ランダム符号化シーケンスの文字セットを特定順に配列する工程とを含み、
且つ通信ネットワークを介してサービス認証符号を遠隔ユーザに伝達する通信ドライバを含み、
サービス認証符号は符号生成アルゴリズムが使用する第１および第２の擬似ランダム符号化シーケンスに従い変化し、サービス認証符号を生成する場合は常に異なる第１および第２の擬似ランダム符号化シーケンスを使用し、同じサービス認証符号を再生成する見込みを削減する。

【００３１】
本発明は、また認証デバイスにおいて実装する１以上のコンピュータ可読記憶媒体上で実施する認証デバイスソフトウエア構成を提供し、本認証デバイスソフトウエア構成は、
遠隔サービスが提供する、第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を受信するか、または入力する入力ドライバと、
第２の秘密鍵に基づき符号生成アルゴリズムを使用して予期符号値を生成する生成器と、
予期符号値をサービス認証符号と比較する比較器と、
予期符号のサービス認証符号との比較に従い、遠隔サービスの真正性を示す応答を生成する応答生成器
とを備える。

【００３２】
本発明は、また遠隔サービスが提供する、サービス認証符号に基づき遠隔サービスの真正性を示す応答を認証デバイスのユーザに提供する認証デバイスを提供し、本認証デバイスは、
第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を受信するか、または入力する入力手段と、
第２の秘密鍵に基づき符号生成アルゴリズムを使用して予期符号値を生成する生成器手段と、

予期符号値をサービス認証符号と比較する比較器手段と、
予期符号のサービス認証符号との比較に従い、遠隔サービスの真正性を示す応答を生成する応答生成器手段
とを備える。

【００３３】
ある実施形態では、遠隔サービスの真正性をユーザに示す、認証デバイスが生成する応答は、遠隔サービスに対してユーザを認証するためのユーザ認証符号の生成を起動する認証デバイスを備える。本実施形態では、ユーザ認証符号を遠隔サービスに伝達することができ、以前に記述したように同じ符号生成アルゴリズムを使用するが、第４の秘密鍵に基づき遠隔サービスがユーザを認証することを可能にする。

【００３４】
従って本実施形態では、本発明は認証デバイスを提供し、本認証デバイスは認証デバイスが後に認証デバイスの所有者またはユーザを認証するのに使用することにする遠隔サービスまたはその他のエンティティが提供する有効なサービス認証符号により起動する場合にのみその動作を可能にすることにする。これにより、ユーザが認証しようとするウェブサイト、またはエンティティの真正性の検証を保証し、その後ユーザにウェブサイト、またはエンティティに対する認証を要求するだろう。

【００３５】
結果として、スクラッチカードおよびある電子的な１回のパスワード（one-time passwords、ＯＴＰｓ）などの現在市場に入ろうとする他のデバイスと違い、ユーザを騙して機密情報を暴こうとする不正ウェブサイトまたはエンティティが、例えば６ディジットの認証符号を推測し、不正ウェブサイトまたはエンティティが、ユーザが取引しようと考える合法的遠隔サービスまたは他のエンティティであるかのごとく見せる見込みが減少するので、鍵情報を「フィッシュする」能力は相当削減する。

【００３６】
有利には、種々の秘密鍵を符号化するのに擬似ランダム符号化シーケンスを使用する本発明の実施形態は、トークン、スクラッチカードおよびＯＴＰｓなどのデバイスにおいて使用する数字アルゴリズムとは動きが異なる。このようなデバイスは複雑な素数に関係するアルゴリズムに基づき、アルゴリズムは時に数学的妥協になりやすいことがある。

【００３７】
ある実施形態では、認証デバイスをユーザが抱えることができる携帯デバイスに備えるか、またはインストールすることができる。別の実施形態では、また認証サーバを含み、認証サーバは遠隔サービスとユーザとの間で送信するデータを解釈し、遠隔サービスとユーザ双方の完全性を検証する。

【００３８】
本発明には、多様な異なるアプリケーションがあるものと考えられる。例えば、本発明は建物／制限エリアへの入場、オンライン選挙投票(例えば、選挙委任または企業役員会議に対する）、内部から、または離れた事務所の場所／自宅から企業ネットワークへのログオンおよび電子メールメッセージの合法的(不正なものとは違い）ソースからの発信認証の管理に適用することができる。

【００３９】
有利には、相互認証をサポートする本発明の実施形態をユーザが使用して、ユーザが他人またはエンティティを合法的に認証することができる遠隔サービスと通信していることをまず検証の後、別の人物(またはエンティティ)の特定情報または別の人物(またはエンティティ)に関係する他の情報を認証することができる。

【００４０】
それ故一実施形態では、本発明はまた別の人物またはエンティティの特定情報および／または信任情報を検証する方法およびシステムを提供する。例えば、本発明を使用して、規制団体(例えば、消費者および事業問題事務局）から認可状態情報を取得することができる商人、ユーザ、および遠隔サービス間の認証に参加することにより、商人（例えば電

気工事者）が適切に認可されていることを検証することができる。別の例により、かつ相互認証をサポートする実施形態に関して、本発明を使用して、就職志願者が「Ｘ大学」の学位を保有していることを検証することができる。さらに別の例によれば、本発明を切符販売システムの一部として切符販売目的に対する旅行者の特定情報を認証することに使用することができる。

【００４１】

それ故本発明は、また通信ネットワークを介して遠隔サービスを使用する第１のユーザに対する第２のユーザの特定情報および／または信任情報を認証する方法を提供し、本方法は、

第１のユーザが、以上に記述した認証方法を使用して遠隔サービスを認証する工程と、

遠隔サービスを有効に認証する場合、第１のユーザが、第２のユーザに関連するか、または第２のユーザが提供する秘密鍵に基づき、第２のユーザの認証デバイスが生成したユーザ認証符号を提供する工程と、

通信ネットワークを介してユーザ認証符号を遠隔サービスに伝達する工程と、

遠隔サービスが、秘密鍵に基づき生成した予期符号値を獲得し、その後予期符号値を第２のユーザのためのユーザ認証符号と比較する工程と、

その比較に応じ、予期符号がユーザ認証符号と相関する場合、遠隔サービスが、第２のユーザの真正性を示す応答を第１のユーザに提供する工程

とを含む。

【００４２】

当然、以上の例は本発明の可能なアプリケーションの非制限的例として提示した。種々の実施形態における本発明には、以上に特定したものを越える範囲のエリアにアプリケーションがありうることを理解すべきである。実際、本発明は認証が一方向（いずれかの方向の)か、または相互（両方向)であろうと、ユーザと遠隔サービスとの間の認証を含む広い範囲のアプリケーションに適用することができると考えられる。

【００４３】

次に、本発明を添付の図面に図示する種々の実施形態に関して記述することにする。とはいえ当然、以下の記述は以上の記述の一般性を制限するものではない。

【発明を実施するための最良の形態】

【００４４】

本発明の実施形態による遠隔サービスとユーザ１０２との間の認証システム１００を図１に示す。システム１００は遠隔サービス１０４、および通信ネットワーク１０８を介して遠隔サービス１０４が提供するサービス認証符号を受信するために、ユーザが運用可能な認証デバイス１０６を備える。

【００４５】

本明細書に示す通信ネットワーク１０８は（インターネットなどの）グローバル・コンピュータ・ネットワークであり、グローバル・コンピュータ・ネットワークは遠隔サービス１０４を提供する（本明細書では遠隔サーバ１１２として示す）ネットワークデバイス１１０、ユーザが運用可能なデバイス１１４および認証サーバ１１６を含み、以上のそれぞれは通信ネットワーク１０８の他の要素と両立可能であり、かつ通信ネットワーク１０８の他の要素と接続し、遠隔サーバ１１２、ユーザが運用可能なデバイス１１４および認証サーバ１１６の間の通信を可能にする。通信ネットワーク１０８をグローバル・コンピュータ・ネットワークに関して記述することにするが、当然通信ネットワーク１０８をそのように制限する必要はない。実際、本発明の別の実施形態によるシステム１００を、公衆地上移動ネットワーク（ｐｕｂｌｉｃ　ｌａｎｄ　ｍｏｂｉｌｅ　ｎｅｔｗｏｒｋ、ＰＬＭＮ）、公衆交換電話ネットワーク（ｐｕｂｌｉｃ　ｓｗｉｔｃｈｅｄ　ｔｅｌｅｐｈｏｎｅ　ｎｅｔｗｏｒｋ、ＰＳＴＮ）、または通信ネットワークを相互にネットワーク化した種々のタイプの組み合わせなどの他のタイプの通信ネットワーク１０８を使用して、配備することができる。当然、ネットワークデバイス１１０およびユーザデバイス１１４は使用する通信ネットワーク１０８のタイプに従い変化するだろう。

【００４６】
認証サーバ１１６は単一処理ユニット（単一サーバなどの）または適するオペレーティングシステムを備える一群のより小さな目的集中型デバイスを備えることができる。適するオペレーティングシステムはウインドウズ（Windows(登録商標)）、リナックス（Linux）またはソラリス（Solaris）を含むことができる。この点に関して、言葉「サーバ」を使用する場合、物理的サーバ（即ち、個別の機械）、またはバーチャルサーバ（即ち、同じ物理的機械における２以上の機能）、またはサービスまたは一群のサーバ／サービス（即ち、負荷平衡、冗長性および規模拡張性を可能にする複数の物理的またはバーチャルデバイス）を意味する。
【００４７】
図示する実施形態では、認証サーバ１１６を使用することができ、通信ネットワーク１０８を介してユーザ１０２に対して遠隔サービス１０４を認証する、および／または遠隔サービス１０４に対してユーザ１０２を認証する。
【００４８】
図２は、認証デバイス１０６に関する実施形態のブロック図を示す。図示するように、認証デバイス１０６はプロセッサ２００、オンボードメモリ２０２、（入力値をキー入力するキーパッド２０８などの）入力手段２０４および電力供給２０６を伴う消費者または事務デバイスであることができ、消費者または事務デバイスは移動電話機、（ＨＰＩＰＡＱｓ、パームパイロット（Palm Pilots）および同類などの）パーソナルデータアシスタントおよび製造会社またはユーザのいずれかがインストールするソフトウエアプログラム２１０を伴う携帯音楽プレーヤ、またはカスタム化デバイス（スマートカードなど）を備えるが、これらに限らない。ソフトウエアプログラム２１０を、プロセッサが実行可能な命令セットの形式でオンボードメモリ２０２上に格納する。
【００４９】
プロセッサ２００は命令セットにおいて提供する入力ドライバを実行し、入力手段２０４をユーザが動作させることを可能にし、サービス認証符号を受信するか、またはサービス認証符号を認証デバイス１０６に入力する。現実施形態の場合、プロセッサ２００はテキサスインストゥルメント社のＭＳＰ‐４３０である。一方当然、任意の適するプロセッサを使用することができる。
【００５０】
一度受信、または入力すると、プロセッサ２００は、認証デバイスに関連する秘密鍵に基づきサービス認証符号を生成するのに使用したのと同じ符号生成アルゴリズムを使用して、予期符号値を生成する。プロセッサ２００は、また命令セットを実行し、予期符号値をサービス認証符号と比較し、予期符号値のサービス認証符号との比較に従い、遠隔サービスの真正性を、示す応答を生成する比較器手段を提供する。図示するように、入力手段２０４は、また入力値の再キー入力を可能にするクリアボタン２１２、認証サーバ１１６が提供するサービス認証符号を入力した後に使用する認証デバイス１０６のロックを外すアンロックボタン２１４を備える。図示する認証デバイス１０６の入力手段２０４は、また「ＡＣＴ」２２０ボタンを含み、「ＡＣＴ」２２０ボタンを押すとユーザ認証符号を生成する起動符号、即ちユーザのＰＩＮの入力後にユーザのＰＩＮを符号化する「ＰＩＮ」２２２ボタンを示す。
【００５１】
図示するように、ＬＣＤ表示装置などの出力表示装置２２４を、また提供し、命令などの情報をユーザに提供し、入力を目立たせる。
【００５２】
応答手段を、また提供し、応答手段は、本明細書ではサービス認証符号が予期符号値と相関しない場合に点灯する赤いＬＥＤ表示器２１６およびサービス認証符号が予期符号値と相関する場合に点灯する緑のＬＥＤ表示器２１８を備える一組の表示器として示す。図示する認証デバイス１０６は一組のＬＥＤの形式における応答手段を備えるが、当然任意の適する応答手段を使用することができる。例えば別の実施形態では、応答手段は、認証

デバイス１０６が遠隔サービス１０４を認証することを示す音を生成する可聴音生成器を備えることができる。

【００５３】

実行可能なプログラム命令２１０に加えて、実施形態では認証デバイス１０６が有するオンボードメモリ２０２は、また以下のリストにおいて特定するような事前プログラムデータ項目を含む。以下のリストが例示に過ぎないことを理解すべきである。

【００５４】

１．　起動符号；

２．　認証デバイス１０６に関連する秘密鍵（以後、「ＤＰＩＮ」と呼ぶ）；

３．　遠隔サービスの認証のための第１の擬似ランダム符号化シーケンス（以後、「デバイス調査シーケンス（Device Challenge Sequence、ＤＣＳ）」と呼ぶ）；

４．　遠隔サービスの認証のための第２の擬似ランダム符号化シーケンス（以後、「デバイス符号化シーケンス（Device Encoding Sequence、ＤＥＳ）」と呼ぶ）；

５．　ユーザ認証のための第１の擬似ランダム符号化シーケンス（以後、「ユーザ調査シーケンス（User Challenge Sequence、ＵＣＳ）」と呼ぶ）；

６．　ユーザ認証のための第２の擬似ランダム符号化シーケンス（以後、「ユーザ符号化シーケンス（User Encoding Sequence、ＵＣＳ）」と呼ぶ）；

７．　符号化シーケンス変位シーケンス（Encoding Sequence Displacement Sequence、ＥＳＤＳ）；

８．　符号化シーケンス変位シーケンス参照（Encoding Sequence Displacement Sequence Reference、ＥＳＤＳＲＥＦ）；

９．　調査シーケンス変位シーケンス（Challenge Sequence Displacement Sequence、ＣＳＤＳ）；

１０．　調査シーケンス参照（Challenge Sequence Reference、ＣＳＲＥＦ）；

１１．　符号化シーケンス参照（Encoding Sequence Reference、ＥＳＲＥＦ）；および

１２．　ＰＩＮ変位符号（PIN Displacement Codes、ＰＤＣ）：

以上に掲げるデータ項目のそれぞれの機能に関する短い要約を以下の記述において提示する。

【００５５】

１．起動符号：

起動符号は、各認証デバイス１０６に対して唯一であるｘディジットのアルファニューメリック符号であり、遠隔サービスまたは認証サーバ１１６による認証デバイス１０６の登録、および遠隔サービスまたは認証サーバ１１６からの応答の起動の双方のための手段として使用する。起動符号の使用を後にさらに詳細に記述することにする。

【００５６】

起動符号は、あらゆる適する符号化方式を含むことができる。ある実施形態では、起動符号は文字セットから抜き出す６ディジット符号の文字を含み、文字セットは（０と１とのありうる混同のため、多分「Ｏ」と「Ｉ」の両方を利用しない）２４のアルファ文字および全てが「０」と「９」との間の１０ディジットを含む。このような方式は１５，４５０億個の組み合わせ（３４ｘ３４ｘ３４ｘ３４ｘ３４ｘ３４）を提供しよう。

【００５７】

以下の記述では、６ディジットの起動符号である次の実施例「ＲＦ６Ｄ９Ｓ」を使用することにする。

【００５８】

２．デバイスＰＩＮ（ＤＰＩＮ）：

ＤＰＩＮは擬似ランダムｘディジット符号であり、この符号は、符号が関係する認証デバイス１０６に対して静的に留まる。このＤＰＩＮは認証デバイス１０６と唯一に関連する符号である。起動符号とＤＰＩＮとの間には相関はない。

【００５９】

遠隔サービス１０４の認証中に、ＤＰＩＮを認証サーバ１１６と認証デバイス１０６との間で通信するサービス認証符号の構成要素として使用する。

【００６０】

ある実施形態では、ＤＰＩＮは４文字の数字シーケンスを含む。このようなシーケンスはシーケンスを推測する１／１００００のチャンスを呈する。以下の実施例では、「６７９４」の４ディジットのＤＰＩＮを使用することにする。

【００６１】

３．デバイス調査シーケンス（ＤＣＳ）符号：

各ＤＣＳは符号であり、この符号を認証デバイス１０６のＤＰＩＮに基づき認証デバイス１０６が予期符号値の生成において使用する。認証デバイス１０６は典型的に複数の唯一のＤＣＳ符号を格納することにする。現実施形態では、各ＤＣＳ符号は繰り返すことのない数字文字のシーケンスを含む。以下の実施例では、ＤＣＳ符号の次の４実施例、「２１９６７５８３０４」、「０１２３４５６７８９」、「６３８７１０９２４５」および「８２５３６１４７０９」を使用することにする。

【００６２】

４．デバイス符号化シーケンス（ＤＥＳ）：

ＤＥＳは複数のサービス認証符号を認証するのに使用する擬似ランダム符号化シーケンスである。ＤＥＳの長さは実際上重要ではないが、文字の後続する変位が与えられると、この数が小さいほど、変位の複雑度が増し、従ってサービス認証符号のより大きな数のサービス認証符号が必要になる。

【００６３】

典型的には、ＤＥＳの長さは５００乃至１０００シーケンスビットであるとする。この範囲の長さでは５０乃至１００回の使用を可能にし、その後変位が必要になろう。一方ある実施形態では、ＤＥＳは少なくとも５０回の認証サイクルを可能とするように少なくとも５００ディジットの長さを有する。以下の実施例では、２０ディジットのＤＥＳも有する（２つのサービス認証符号の検証が可能になろう）次の実施例、「７３６１９４８２６４０１９４８２７３５１」を使用することにする。

【００６４】

５．ユーザ調査シーケンス（ＵＣＳ）符号：

ある実施形態では、ＵＣＳ符号を使用し、ユーザが入力するユーザＰＩＮを符号化し、それによりユーザ認証符号を提供する。現実施形態では、ＵＥＳにおいて複数の１０ディジットが存在する限り多数回ＵＣＳ符号を使用する。

【００６５】

一方複雑度が加わるのは、このようなＵＣＳ符号の循環使用でありえ、従って暗号化の観点からＯＴＰｓとＵＥＳとの間のありうる相関をさらに削除する。

【００６６】

ユーザが入力するユーザＰＩＮを符号化する手段として、ＵＣＳ符号を使用する。以下の実施例では、ＵＣＳの次の４実施例、「６３８７１０９２４５」、「８２５３６１４７０９」、「２１９６７５８３０４」および「０１２３４５６７８９」を使用することにする。

【００６７】

６．ユーザ符号化シーケンス（ＵＥＳ）：

ＵＥＳはｘユーザが選択するＰＩＮを符号化するのに使用する擬似ランダム符号化シーケンスである。５０人のユーザが選択するＰＩＮの符号化を可能にするように、このシーケンスは少なくとも５００ディジットの長さであることが好ましい。

【００６８】

ＤＥＳの場合のように、ＵＥＳの長さを実際には問題にすべきではない。とはいえ、変位シーケンスを複雑にし過ぎることを避けるために、ＵＥＳは好ましくは５００乃至１００ディジットの間のシーケンス長を有し、従って５０乃至１００回の間の使用を可能にすべきである。

【００６９】
１０００ディジットのＵＥＳは凡そ３２ｘ１０^{１５３０}の可能な変形を提供するであろう。以下の実施例では、次の２０ディジットのＵＥＳの実施例、「Ａ２３ＣＴＢＬＭ４Ｓ５ＲＴ７Ｐ６ＳＪＫ９」を使用することにする。実施例の２０ディジットのＵＥＳはユーザの選択したＰＩＮの符号化を２回可能にするであろう。
【００７０】
７．符号化シーケンス変位シーケンス（ＥＳＤＳ）：
ある実施形態では、ＥＳＤＳ変位シーケンスを使用し、「新しい」ＤＥＳおよびＵＥＳを生成する。
【００７１】
一方、新しいＤＥＳおよびＵＥＳも定義することができる、ＤＥＳおよびＵＥＳ自体のように長いシーケンスを避けるために、ＥＳＤＳを実際上何度か繰り返す。例えば、５００乃至１０００ディジットのＤＥＳおよびＵＥＳに対して、ＥＳＤＳは実際上５乃至１０の間の変位符号を必要とする１００ディジットの符号であるべきである。
【００７２】
ｘ個のＥＳＤＳは、一度ＥＳＤＳをｘ回使用するとＤＥＳおよびＵＥＳ双方を変位させる（この値に達するのに１０で除算するＤＥＳおよびＵＥＳに使用するｘにより）。
【００７３】
ｘ個の変位シーケンスのそれぞれは、ＤＥＳおよびＵＥＳ双方の変位を可能にするのに使用するｘ（例えば、１００）ディジットの数字のシーケンスに基づく。
【００７４】
例えば、５つの１００ディジットのＥＳＤＳシーケンスを使用して、それぞれ１００ディジットのＤＥＳおよびＵＥＳに対して使用する各ＥＳＤＳにより５００ディジットのＤＥＳおよびＵＥＳを変位させることがきよう。ｘディジットの各シーケンスは、１とシーケンス長を構成するのに使用するｘとの間の各数字のディジットを使用してランダムに生成する数字のシーケンスである。例えば、１００ディジットのＥＳＤＳは１乃至１００の間の全ての数を構成するであろう。以下の実施例では、２０ディジットであるＥＳＤＳが有する次の３つの実施例を使用することにする。
【００７５】
１．　０６．１６．０９．１３．０１．０３．１９．１２．１８．１４．０５．０８．０７．１０．０２．１７．２０．１１．１５．０４．
２．　０７．２０．０９．０２．１１．０８．１６．０１．１０．１５．０３．１７．０５．１４．０４．１２．１９．０６．１８．１３
３．　１０．０４．１４．０１．２０．０５．１３．０９．０３．１２．１７．０８．１１．１９．０２．１８．０６．１６．０７．１５．
８．ＥＳＤＳの参照（ＥＳＤＳＲＥＦ）：
ＥＳＤＳＲＥＦは、使用するＤＥＳおよびＵＥＳの変位シーケンスを反映し、予め「１」とするが、変位シーケンスが終了する度に１だけ増加する。それ故、５個のＥＳＤＳがあれば、ＥＳＤＳＲＥＦは１と５の間で循環するであろう。
【００７６】
９．シーケンス変位シーケンスの調査（ＣＳＤＳ）：
ＣＳＤＳはｘディジットＤＥＳおよびＵＥＳ双方の第１のディジットを確立するのに使用する数字符号を含み、それにより各シーケンスで利用可能なｘ個の第１の１０ディジットのブロックを確立する。例えば、３つの「２０」ディジットＣＳＤＳの数は６、１３、１７を含む。別の実施例では、５つの「５００」ＣＳＤＳの数は０８３，１３６，２７６，３４３，４３５を含む。
【００７７】
１０．ＣＳＤＳの参照（ＣＳＤＳＲＥＦ）：
それ故１と使用するＣＳＤＳの総数の間を循環することにするＣＳＤＳＲＥＦが、使用するＣＳＤＳの数を反映する。従って、ＣＳＤＳＲＥＦは使用するＣＳＤＳを反映し、予

め「１」とする。
【００７８】
１１．ＣＳの参照（ＣＳＲＥＦ）：
ＣＳＲＥＦは使用するＵＣＳおよびＤＣＳ符号を反映し、予め「１」とする。これは各変位シーケンスの後か、または加わる複雑度のため、各ログオンに対して循環することができよう。さらに大きな複雑度に対して、ＣＳＲＥＦを各変位シーケンスに対して１だけ増加することができようが、その場合ＵＣＳおよびＤＣＳ符号のそれぞれを一度使用すると、その場合ＵＣＳおよびＤＣＳ符号はユーザがログオンする度に循環できよう。
【００７９】
１２．符号化シーケンス参照（ＥＳＲＥＦ）：
ＥＳＲＥＦを使用して、ユーザ１０２が認証サーバ１１６から発生したものでない有効なサービス認証符号を入力する、ありそうも無い場合にも、認証デバイス１０６が認証サーバ１１６との同期に留まることを保証する。
【００８０】
１３．ＰＩＮ変位符号
ある実施形態では、ＰＤＣを使用してバーチャルＰＩＮを作成し、バーチャルＰＩＮを認証デバイス１０６の各ｘ回の使用後に変更する。ユーザが選択するユーザＰＩＮが４，５、または６ディジットのＰＩＮであるに関わらず、ＰＤＣを使用して毎回唯一の６ディジットのＰＩＮに到達するように選択する実際のユーザのＰＩＮを変更することになろう。
【００８１】
ＤＥＳおよびＵＥＳ変位シーケンスを使用すれば毎回、ｘ個のＰＤＣを使用し、ｘ回認証デバイス１０６を使用する度に、ｘ個のＰＤＣを単純に使用し、ユーザの選択するＰＩＮを変更し、それによりバーチャルに新しいＰＩＮを作成することになろう。変更により負の値を生じる場合、同じ数字のディジットを使用してこれを正の値に変更することになろう。ＰＤＣは完全にランダムである。
【００８２】
ＰＤＣは複雑度の追加をもたらし、不要なメモリを占有することがある。当然その影響は、ユーザが認証デバイス１０６を使用する度に、ユーザのＰＩＮを単にバーチャルＰＩＮに変更し、次いでバーチャルＰＩＮを符号化することになろうが、本明細書の目的に対しては、ＰＤＣの使用を詳細には記述していない。
【００８３】
認証サーバの構成要素およびデータ
認証サーバ１１６を備えるシステムの実施形態を図２Ａに示す。この実施形態では、生成サーバ２２６はＤＰＩＮを生成し、これを認証デバイス１０６および認証サーバ１１６にロードする。このデータを次いでデータのエンドユーザに分配する。コピーが作成され、電話機、ＰＤＡ、インターネットのデバイスまたは同類にダウンロードされようと、現実施形態では１つのコピーをユーザの格納装置２３０に、１つをエンド認証デバイス１０６に送信する。
【００８４】
起動符号およびユーザの格納装置２３０のアドレスをディレクトリサーバ２２８に送信し、起動符号およびユーザの格納装置２３０のアドレスを次に宛先変更サーバ２３０が読み取るか、または更新する。
【００８５】
図示する実施形態においてログインを試行すると、宛先変更サーバ２３０はディレクトリサーバ２２８（またはディレクトリのローカルコピー）を読み、ＤＰＩＮのサーバ側バージョンを格納する認証サーバ／クラスター１１６に認証要求を送信する。例えば、ユーザは遠隔サービス１０４を通じてログオンすることができ、遠隔サービス１０４は次に銀行、即ち認証デバイス１０６をユーザ１０４に発給した発給組織に要求を宛先変更する。このような工程は「連結」を可能にする。

【００８６】
認証サーバ１１６は符号生成アルゴリズムのための計算機能を実行し、ユーザに付随するユーザ格納装置に変数の現状態および同類を格納する。
【００８７】
この節では、認証サーバ１１６に格納する各認証デバイス１０６に関係するデータ構成要素を記述する。以下のリストは例示に過ぎないことを理解すべきである。
【００８８】
１．　起動符号；
２．　認証サーバ１１６により登録し、従って遠隔サービスにアクセスするために登録する認証デバイス１０６に関連する秘密鍵（ＤＰＩＮ）。
【００８９】
３．　遠隔サービスの認証のための第１の擬似ランダム符号化シーケンス（以後、「デバイス調査シーケンス（Device Challenge Sequence、ＤＣＳ）」と呼ぶ）；
４．　遠隔サービスの認証のための第２の擬似ランダム符号化シーケンス（以後、「デバイス符号化シーケンス（Device Encoding Sequence、ＤＥＳ）」と呼ぶ）；
５．　ユーザ認証のための第１の擬似ランダム符号化シーケンス（以後、「ユーザ調査シーケンス（User Challenge Sequence、ＵＣＳ）」と呼ぶ）；
６．　ユーザ認証のための第２の擬似ランダム符号化シーケンス（以後、「ユーザ符号化シーケンス（User Encoding Sequence、ＵＣＳ）」と呼ぶ）；
７．　符号化シーケンス変位シーケンス（Encoding Sequence Displacement Sequence、ＥＳＤＳ）；
８．　符号化シーケンス変位シーケンス参照（Encoding Sequence Displacement Sequence Reference、ＥＳＤＳＲＥＦ）；
９．　調査シーケンス変位シーケンス（Challenge Sequence Displacement Sequence、ＣＳＤＳ）；
１０．　調査シーケンス参照（Challenge Sequence Reference、ＣＳＲＥＦ）；
１１．　符号化シーケンス参照（Encoding Sequence Reference、ＥＳＲＥＦ）；および
１２．　ＰＩＮ変位符号（PIN Displacement Codes、ＰＤＣ）：
図３は、ユーザ１０２に対して遠隔サービス１０４を認証する方法３００のフローチャート３００を示す。
【００９０】
図示するように、方法３００は遠隔サービス１０４が第１の秘密鍵に基づき符号生成アルゴリズムを使用して生成したサービス認証符号を獲得する工程３０２を含む。
【００９１】
工程３０４において、サービス認証符号を通信ネットワークを介してユーザ１０２に伝達する。
【００９２】
工程３０６において、サービス認証符号を次いで受信するか、またはサービス認証符号をユーザ１０２に付随する認証デバイスに入力する。
【００９３】
工程３０８において、認証デバイス１０６は第２の秘密鍵（この場合ＤＰＩＮ）に基づき同じ符号生成アルゴリズムを使用して予期符号値を生成し、その後工程３１０において予期符号値をサービス認証符号と比較する。
【００９４】
最後に工程３１２においてその比較に応じ、予期符号がサービス認証符号と相関する場合、認証デバイスは遠隔サービス１０４の真正性をユーザ１０２に示す応答を生成する。第１の秘密鍵と第２の秘密鍵が同じであれば、当然認証デバイス１０６が生成する予期符号は遠隔サービス１０４が提供するサービス認証符号とのみ相関するだろう。従って、遠隔サービス１０４が第２の秘密鍵（即ち、ＤＰＩＮ）と同じ鍵以外のものを使用して生成

したサービス認証符号を獲得すれば、その場合サービス認証符号は予期符号と相関しないだろう。

【００９５】

図４は、遠隔サービス１０４に対してユーザ１０２を認証する方法４００のフローチャートを示す。図示するように、方法４００は認証デバイス１０６が第３の秘密鍵（この場合、ユーザが入力する個人特定番号）に基づき符号生成アルゴリズムを使用してユーザ認証符号を生成する工程４０２を含む。

【００９６】

工程４０４において、サービス認証符号を、通信ネットワークを介して遠隔サービス１０４に伝達する。工程４０６において、予期符号値を第４の秘密鍵に基づき認証サーバ１１６が生成する。

【００９７】

工程４０８において、予期符号値をユーザ認証符号と比較する。最後に、かつその比較に応じ、予期符号がユーザ認証符号と相関する場合に、工程４１０において遠隔サービス１０４はユーザ１０２がさらに遠隔サービス１０４へアクセスするのを認める。

【００９８】

第３の秘密鍵と第４の秘密鍵が同じであれば、当然認証サーバ１１６が生成する予期符号は認証デバイス１０６が提供するユーザ認証符号とのみ相関するだろう。従って、認証デバイス１０６が第４の秘密鍵と同じ鍵以外のもの（即ち、ユーザの登録するＰＩＮ以外のもの）を使用して生成したサービス認証符号を提供すれば、その場合ユーザ認証符号は予期符号と相関しないだろう。

【００９９】

認証処理フロー

一般的に言えば、以下の処理の幾つかまたは全てを本発明の実施形態による方法、またはデバイスを利用する認証サービスの一部として実装することができる：

１．　認証サーバ１１６により認証デバイス１０６を最初に登録するユーザ登録処理；
２．　ユーザにその認証デバイス１０６を使用して遠隔サービス１０４を認証することを可能にする「通常のログオン」処理；
３．　各ＵＥＳおよびＤＥＳを使用した後、各ＵＥＳおよびＤＥＳのディジットを制御可能に移動させる「変位処理」；
４．　ユーザＰＩＮを再設定する処理；および
５．　複数のサービス環境における認証方法または認証デバイスの適用性を認める１以上の処理；

以上およびその他の処理の以下の実施例を例示の目的で提示する。

【０１００】

実施例１：認証サーバによる認証デバイスの初期登録

認証デバイス１０６をユーザ１０２に提供することができ、その後認証デバイス１０６を使用してアクセスすることができる遠隔サービス１０４に対し認証デバイス１０６を登録する。

【０１０１】

このような実施形態では、ユーザ１０２はユーザＩＤおよびパスワードなどの既存の信任情報を使用して遠隔サービス１０４に「ログオンする」ことができる。ログオンすると、ユーザ１０２は次いで認証サーバ１１６により認証デバイス１０６を登録することを選択することができる。認証サーバ１１６による認証デバイス１０６の登録は典型的に以下の工程を含むだろう：

１．　起動および検証フェーズ；
２．　ユーザＰＩＮの選択；および
３．　ユーザ情報の登録。

【０１０２】

以上の各工程を以下にさらに詳細に記述する。

【０１０３】

起動および検証

認証サーバ１１６により認証デバイス１０６を登録するために、認証サーバ１１６はユーザの認証デバイス１０６のための起動符号（この実施例では：「ＲＦ６Ｄ９Ｓ」）を提供することをユーザ１０２にまず促すだろう。以前に記述したように、「ＡＣＴ」ボタン２２０(図に参照)を押すことにより、起動符号を認証デバイス１０６の表示装置上に表示することができる。

【０１０４】

起動符号を提供した後、認証サーバ１１６は次にサービス認証符号により応答し、ユーザ１０２が、入力した起動符号に基づいて示した認証デバイス１０６を実際に有していることを検証することができる。

【０１０５】

このサービス認証符号（ＳＡＣ）は、認証符号に基づき認証サーバ１１６が取り出す符号化ＤＰＩＮ（この実施例では：「６７９４」）を含む。この点に関して、認証サーバ１１６は各発給認証デバイス１０６に対する起動符号の指標および関連するＤＰＩＮを維持する。従って起動符号を受信すると、認証サーバ１１６は受信起動符号に関連するＤＰＩＮを取り出すことができる。

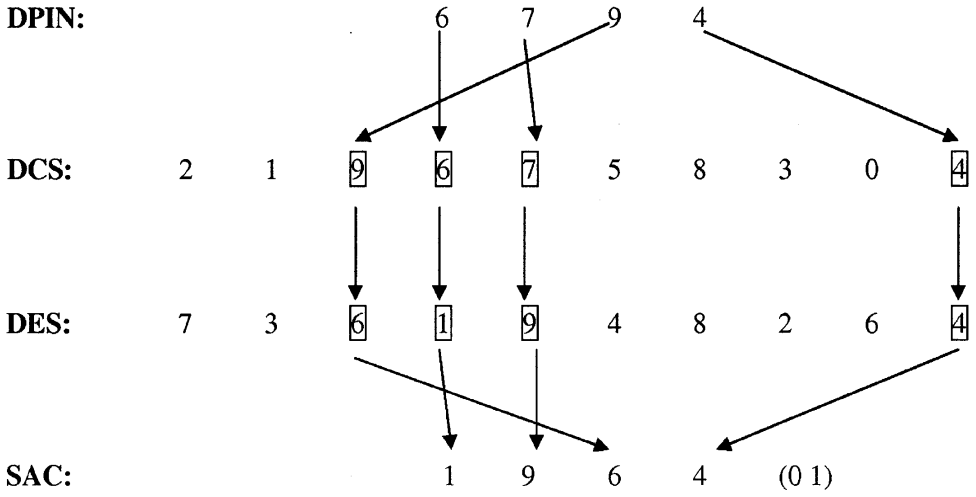
【０１０６】

サービス認証符号は、またＥＳＲＥＦを含み、ＥＳＲＥＦは初期登録の時点では、数「０１」であろう。従って、現実施形態では符号化ＤＰＩＮと合わせて、サービス認証符号は６ディジット符号である。

【０１０７】

実施例によれば、「７３６１９４８２６４０１９４８２７３５１」（即ち２つの１０ディジットシーケンス)の実施例である２０ディジットのＤＥＳ、および「０１」のＥＳＲＥＦを持つＣＳＲＥＦが反映するＤＣＳ符号（この実施例では「１」を反映する実施例：「２１９６７５８３０４」）を使用し、サービス認証符号を以下のようにＤＥＳの最初（「０１」）の１０ディジットに対してＤＣＳ符号を使用して取り出したＤＰＩＮを符号化することにより生成するであろう。

【表１】



【０１０８】

ユーザ１０２は次いで提供されたサービス認証符号を認証デバイス１０６に入力する。

【０１０９】

認証デバイス１０６は、ＤＥＳの第１の１０ディジットブロック（サービス認証符号の最後の２ディジットが「０１」であろうとすれば）および認証デバイス１０６において格

納するＤＣＳ符号に対して認証デバイス１０６に格納するようにＤＰＩＮを（即ち、認証デバイス１０６に関連するＤＰＩＮ）符号化する。

【０１１０】

６ディジットのサービス認証符号（この実施例では：「１９６４０１」）を入力すると、認証デバイス１０６は、次に認証デバイス１０６に関連するＤＰＩＮを使用して、認証デバイス１０６が生成した予期符号の対応するディジットに対しサービス認証符号の最初の４ディジットを比較する。

【０１１１】

現実施例では、これを認証デバイス１０６上の「ＶＥＲ」ボタン（図示せず）を押すことにより達成する。認証デバイス１０６は、またサービス認証符号の最後の２ディジットがＥＳＲＥＦ＋１に等しいことを調べるであろう。

【０１１２】

サービス認証符号を認証すれば、緑のＬＥＤ２１８(図２参照)が点灯し、「ＰＩＮを入力してください」を認証デバイスの表示装置上に表示する。次に、ＥＳＲＥＦを次のサービス認証符号のために１だけ増加させる。一方、サービス認証符号を認証しなければ、赤いＬＥＤ２１６(図２参照)が点灯し、「もう一度試行してください」、または類似のメッセージを認証デバイスの表示装置２２４(図２参照)上に表示する。

【０１１３】

サービス認証符号が何回か失敗すれば、遠隔サービス１０４が有効でないか、またはユーザ１０２が使用している認証デバイス１０６が起動符号に対応する正しいものでない、かのいずれかである。

【０１１４】

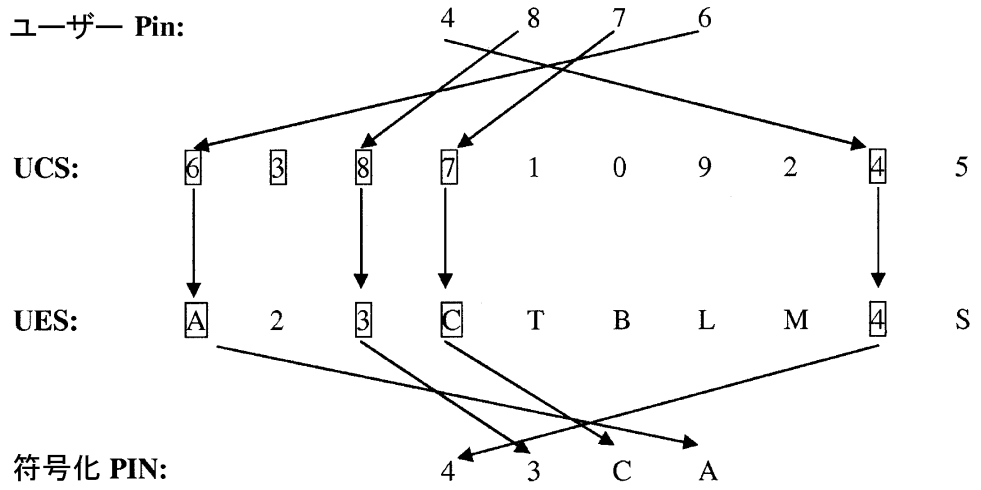
ＰＩＮの選択

ユーザ１０２は、次に唯一のユーザＰＩＮを選択、入力し、次いで「ＰＩＮ］ボタン２２２（図２参照）を押すはずである。認証デバイス１０６は次にＵＥＳの１０ディジットの第１のブロックおよび第１のＵＣＳ符号を使用して符号化ユーザＰＩＮを生成するであろう。

【０１１５】

実施例によれば、「Ａ２３ＣＴＢＬＭ４Ｓ５ＲＴ７Ｐ６ＳＪＫ９」である実施例の２０ディジットのＵＥＳ、および認証符号と共に提供されるように－「０１」のＤＥＳブロックを持つＣＳＲＥＦ（例えば、「６３８７１０９２４５」）に対応するＵＣＳ符号を使用して、ユーザＰＩＮ（この実施例では：４８７６）を以下のように符号化するであろう。

【表２】



【０１１６】

ユーザ１０２が符号化ＰＩＮ一度入力すると、認証サーバ１１６はユーザＰＩＮを復号

化し、復号化ＰＩＮを将来のユーザ認証に使用するために格納する。

【０１１７】

追加処理を使用して、ＵＥＳの第２の１０ディジットブロックに対してユーザＰＩＮを符号化することによりユーザＰＩＮを検証することができる。一方、これはユーザを混乱させ、ユーザＰＩＮを忘れた場合、Ｑ＆Ａ機能（後にさらに詳細に説明するように）の存在により、ユーザが確実にＰＩＮを再設定することを認めるであろう。さらに、認証デバイス１０６は論理を保持し、最初のユーザＰＩＮが２度目のユーザＰＩＮの入力と同じであることを保証するには２回目のユーザＰＩＮを入力することを要求することにより、ユーザＰＩＮを符号化する前に、ユーザの選択したユーザＰＩＮを検証することができよう。

【０１１８】

Ｑ＆Ａ

ユーザＰＩＮの選択を完了すると、ユーザ１０２は次に従来タイプのＱ＆Ａに基づく処理にその詳細情報を登録することができる。Ｑ＆Ａに基づく処理から導出する質問を使用して、再設定処理を取り巻く安全性を判断することができる。

【０１１９】

認証サーバ１１６による登録処理を成功裡に完了すると、－認証デバイス１０６を登録しようとする第３のパーティに特定である－ユーザのユーザＩＤを認証サーバ１１６に送信するであろう。

【０１２０】

次に、ユーザ１０２が別の第３のパーティにより使用するためにその認証デバイス１０６を登録すると、ユーザが為す必要があろう全てのことは、その起動符号を提供し、そのユーザＰＩＮを検証することである。ユーザがその個々のサービスに対して認証する場合に使用するために、第３のパーティは次いでユーザのＩＤを認証デバイス１０６に送信することができよう。従って、既に行ったＱ＆Ａ処理を繰り返す必要はないであろう。

【０１２１】

この処理により、認証デバイス１０６を同じ程度の安全性を提供しつつ、複数の遠隔サービスに使用することが可能になるであろう。

【０１２２】

実施例２Ａ：正常ログオン

ユーザ１０２は、認証デバイス１０６上の「ＡＣＴ」ボタンを押し、取り出した起動符号を入力することにより、認証デバイス１０６が認証手段を提供する個々の遠隔サービス１０４にログオンする。

【０１２３】

遠隔サービス１０４は、次に起動符号を認証サーバ１１６に送るだろう。認証サーバ１１６は次いでサービス認証符号により応答し、ユーザ１０２が有していることを示した認証デバイス１０６を実際に有していることを入力起動符号に基づき検証する。

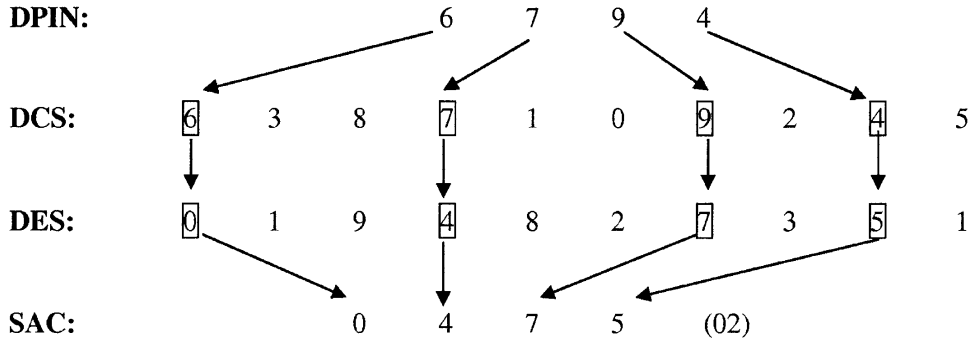
【０１２４】

サービス認証符号をユーザ１０２に送信する時点で、タイマがスタートし、ユーザの符号化ユーザＰＩＮの有効性を所定の時間の間、例えば６秒に制限することができる。これは、幽霊ウェブサイトがサービス認証符号に整合することに成功することがあれば、符号化ユーザＰＩＮが使用されることを防止し、また攻撃者がアクセスを得るためには規定時間のフレーム内に応答しなければならないとする場合に、媒介者が攻撃する機会をある程度制限するであろう。

【０１２５】

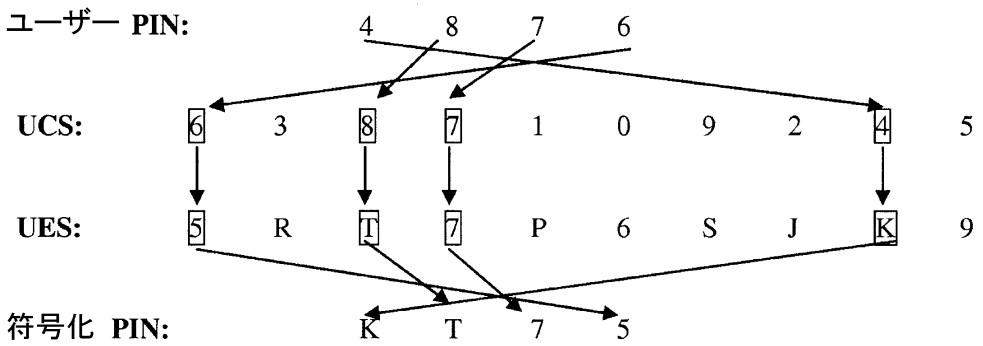
このサービス認証符号の構成に、符号化ＤＰＩＮ（この実施例では：「６７９４」）および認証サーバ１１６に接続するたびに＋１だけ増加するであろう－ＥＳＲＥＦを含む。符号化ＤＰＩＮおよびＥＳＲＥＦは、あわせて６ディジットのサービス認証符号を作成する。

【０１２６】
実施例によれば、「７３６１９４８２６４０１９４８２７３５１」（即ち２つの１０ディジットシーケンス)の実施例である２０ディジットのＤＥＳ、および適するＤＣＳおよび「０２」のＥＳＲＥＦを持つ、例えば「６３８７１０９２４５」であるＣＳＲＥＦを使用し、以下のようにＤＥＳの第２（「０２」）の１０ディジットに対してＤＣＳ符号を使用してＤＰＩＮを符号化することにより、サービス認証符号を生成するであろう。
【表３】



【０１２７】
ユーザ１０２は、次にサービス認証符号を認証デバイス１０６に入力しなければならず、次いで認証デバイスはＤＥＳが持つ第２の１０ディジットのブロック（サービス認証符号の最後の２ディジットが「０２」であったので）に対し、かつ認証デバイス上に格納する適当なＤＣＳ符号を使用して、認証デバイス１０６上に格納するＤＰＩＮを符号化する。
【０１２８】
サービス認証符号、この実施例では「０４７５０２」を入力すると、認証デバイス１０６は次いで、最初の４ディジット（この例では：「０４７５」）が、認証デバイス１０６が認証デバイス１０６に関連するＤＰＩＮを使用して生成するものと整合することを調べるであろう。
【０１２９】
現実施形態では、これを「ＶＥＲ］ボタンを押すことにより達成する。
【０１３０】
再度、サービス認証符号を認証すれば、緑のＬＥＤ２１８(図２参照)が点灯するだろうし、「ＰＩＮを入力してください」の助言、または同類を認証デバイス１０６の表示装置上に表示する。サービス認証符号を認証しなければ、赤いＬＥＤ２１６(図２参照)が点灯するだろうし、助言「もう一度試行してください」、または別の適するメッセージを認証デバイスの表示装置２２４(図２参照)上に表示する。
【０１３１】
ＰＩＮ入力
一度遠隔サービス１０４を認証すれば、ユーザ１０２は、次いでその唯一のユーザＰＩＮを入力し、次に「ＰＩＮ］ボタン２２２（図２参照)を押すことができる。
【０１３２】
認証デバイス１０６は次にＵＥＳが持つ１０ディジットの第２のブロックおよび適するＵＣＳ符号を使用する。実施例によれば、「Ａ２３ＣＴＢＬＭ４Ｓ５ＲＴ７Ｐ６ＳＪＫ９」である実施例の２０ディジットのＵＥＳ、および認証符号において提供されるように－「０２」のＥＳＲＥＦを持つ適当なＵＣＳ符号、例えば「６３８７１０９２４５」を使用して、ユーザＰＩＮ（この実施例では：４８７６）を以下のように符号化するであろう。

【表４】



【０１３３】

ユーザ１０２は、次いで直接的または間接的かのいずれかにより符号化ユーザＰＩＮを認証サーバ１１６に提供し、認証サーバ１１６は次に認証サーバ１１６に格納するか、または認証サーバ１１６にアクセス可能なユーザＰＩＮと符号化ユーザＰＩＮを整合させることを試行する。現実施形態ではこれを、認証サーバ１１６が以前に認証サーバ１１６に送った起動符号のためのＤＰＩＮを取り出し、認証デバイス１０６が認証デバイス１０６に関連するＤＰＩＮを符号化するのに使用した同じＵＣＳおよびＵＥＳを使用して、そのＤＰＩＮを符号化することにより達成する。

【０１３４】

符号化ユーザＰＩＮが整合すれば、認証サーバ１１６は適するユーザＩＤを第３のパーティに送信し、肯定的な検証とともに第３のパーティの認証を求める。整合しなければ、認証サーバはユーザに再試行することを求め、３度失敗した後試行をＱ＆Ａシーケンスに移すであろう。

【０１３５】

実施例２Ｂ：２次連結登録

認証デバイスの発給者以外である２番目の第３のパーティが、ユーザ１０２が遠隔サービス１０４に対して自らを認証する手段としてその認証デバイス１０６を使用するのに利用可能になると、ユーザ１０２は簡単な登録処理に従うことができよう。

【０１３６】

まず、ユーザ１０２は第３のパーティの規格および安全性要求に従いユーザＩＤおよびパスワードなどのその既存の信任情報を使用してウェブサイトなどの遠隔サービス１０４にログオンするだろう。ログオンすると、ユーザ１０２は次いでその認証デバイス１０６を、登録することを選択するだろう。

【０１３７】

起動および検証

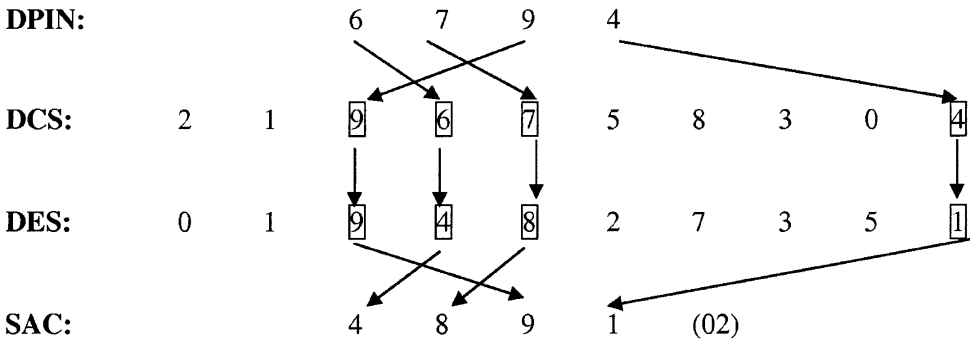
遠隔サービス１０４は、ユーザ１０２に起動符号（この実施例では：「ＲＦ６Ｄ９Ｓ」を求めてまず助言するはずである。再度、これを認証デバイス１０６の表示装置において「ＡＣＴ」ボタンを押すことにより獲得する。一度認証サーバ１１６に提供されると、認証サーバ１１６は次いでサービス認証符号により応答し、ユーザ１０２が有していることを示した認証デバイス１０６を、実際に有していることをユーザが入力した起動符号により検証することができる。

【０１３８】

サービス認証符号の構成に、符号化ＤＰＩＮ（この実施例では：「６７９４」）および－２次登録の時点では少なくとも「０２」より大きく、－共に６ディジットのサービス認証符号を作成するであろう、ＥＳＲＥＦを含む。例えば、「７３６１９４８２６４０１９４８２７３５１」の実施例である２０ディジットのＤＥＳ、および「０２」のＥＳＲＥＦ

を持つＣＳＲＥＦ（この実施例では「２１９６７５８３０４」の実施例であるＤＣＳを反映する「２」）が反映するＤＣＳ符号を使用し、以下のようにＤＥＳの第２（「０２」）の１０ディジットに対してＤＣＳ符号を使用してＤＰＩＮを符号化することにより、サービス認証符号を生成するであろう。

【表５】



【０１３９】

ユーザ１０２は、次いでこのサービス認証符号を認証デバイス１０６に入力し、認証デバイスは、次いで認証デバイス１０６において再度格納するＤＣＳ符号を使用して、ＤＥＳが持つ第２の１０ディジットのブロック（サービス認証符号の最後の２ディジットが「０２」であろうとして）に対して認証デバイス１０６において格納するＤＰＩＮを符号化するだろう。

【０１４０】

６ディジットのサービス認証符号（この実施例では：「４８９１０２」）を入力すると、認証デバイス１０６は、次に最初の４ディジットが認証デバイス１０６において符号化したものと整合するかを調べるであろう。図示する実施形態では、これを「ＶＥＲ」ボタンを押すことにより達成する。認証デバイス１０６は、またサービス認証符号の最後の２ディジットがＥＳＲＥＦ＋１に等しいかを調べるであろう。

【０１４１】

サービス認証符号を認証すれば、緑のＬＥＤ２１８(図２参照)が点灯するだろうし、「ＰＩＮを入力してください」を認証デバイスの表示装置において表示することができようし、ＥＳＲＥＦを次のサービス認証符号のために１だけ増加させるであろう。サービス認証符号を認証しなければ、赤いＬＥＤ２１６(図２参照)および「もう一度試行してください」、または適するメッセージを認証デバイスの表示装置２２４(図２参照)上に表示することができよう。遠隔サービス認証が何回か失敗すれば、これは遠隔サービスが有効でないか、またはユーザ１０２が使用している認証デバイス１０６が起動符号に対応する正しいものでないか、のいずれかであることを示唆するであろう。

【０１４２】

ＰＩＮ入力

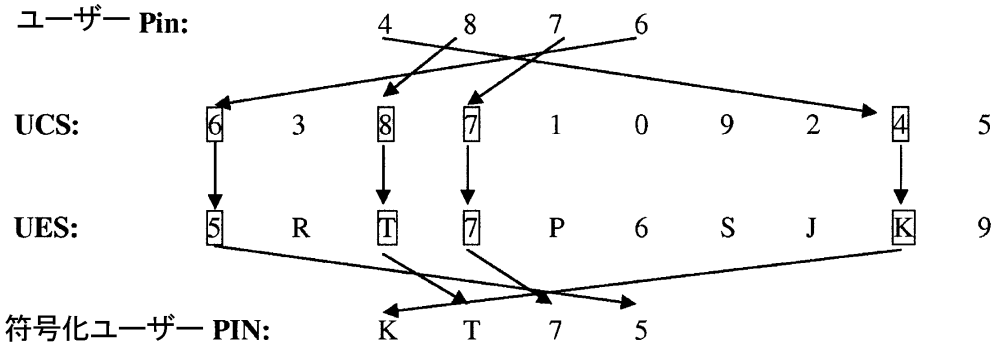
認証サーバ１１６が、ユーザ１０２が既に登録していることを判断できたであろう（その起動符号により）とすれば、その場合認証サーバ１１６はユーザＰＩＮをユーザ１０２が選択しなければならないとは考えないであろうが、認証サーバ１１６に対して最初に自らを登録する時に使用するために既に選択したであろうその実際のユーザＰＩＮを入力するものと考えるであろう。

【０１４３】

ユーザ１０２は、次にその唯一のユーザＰＩＮを入力し、次いで「ＰＩＮ」ボタン２２２(図２参照)を押すはずである。認証デバイス１０６は、次いでＵＥＳが持つ１０ディジットの適するブロックおよび適するＵＣＳ符号を使用するであろう。例えば、「Ａ２３ＣＴＢＬＭ４Ｓ５ＲＴ７Ｐ６ＳＪＫ９」である実施例の２０ディジットのＵＥＳ、および－

サービス認証符号と共に提供されるように、「０２」のＥＳＲＥＦを有する「６３８７１０９２４５」のＵＣＳ符号を使用して、ＰＩＮ（この実施例では：「４８７６」）を以下のように符号化するであろう。

【表６】



【０１４４】

一度ユーザ１０２が符号化ユーザＰＩＮを入力すると、認証サーバ１１６は認証サーバ１１６において同じＰＩＮを符号化した符号化ＰＩＮと整合させることができる。

【０１４５】

認証サーバ１１６による登録処理を成功裡に完了すると、－認証デバイス１０６を登録しようとする第３のパーティに特定である－ユーザのユーザＩＤを認証サーバ１１６に送信するであろう。

【０１４６】

符号化ユーザＰＩＮが整合しなければ、ユーザにＰＩＮを再試行することを求め、３度失敗した後試行をＱ＆Ａシーケンスに移すであろう。

【０１４７】

実施例３：変位処理

ＤＥＳ、ＤＣＳ、ＵＣＳおよびＵＥＳシーケンスをそれぞれ包含する個々の配列を含む実施形態では、各配列はその配列における配列要素の数に相当する有限数の符号生成イベントをサポートすることができる。従って、配列における各シーケンスを使用してサービス認証符号を生成した後、配列の各配列要素における各文字を配列要素内における異なる位置に制御可能に移動させ、それによりそれぞれのシーケンスを変更することができる。

【０１４８】

このように図示する実施形態では、認証方法は幾つかの変位シーケンスに基づいて動作し、変位シーケンスはＤＥＳおよびＵＥＳを一度の使用後実際上変更する。

【０１４９】

実施例である２０ディジットのＤＥＳおよびＵＥＳ（完全ｘディジットシーケンスに反して）、および実施例であるＥＳＤＳおよびＣＳＤＳを使用して、認証方法は以下のように動作するであろう：

１．　ＥＳＲＥＦの調査により‐各サービス認証符号が成功すると１だけ増分した、ＥＳＲＥＦが‐１０＋１により除算したＤＥＳおよびＵＥＳに等しいことが判明すると、特定するであろうＤＥＳおよびＵＥＳが持つ２つの１０ディジットのブロックを使用する場合、以下の工程が生じるであろう：

２．　ＤＥＳおよびＵＥＳ双方を変位させるであろう。図５に示すように、これをＥＳＤＳＲＥＦに対応するＥＳＤＳを使用することにより達成するであろう。例えば、ＥＳＤＳＲＥＦが「１」であったとすれば、第１のｘディジットのＥＳＤＳを使用し、このシーケンスに従いＤＥＳおよびＵＥＳ双方を変位させるであろう。ＤＥＳおよびＵＥＳ双方の実施例である２０ディジットを構成する各「ブロック」をこのシーケンスに従い変位させる

であろう。実施例である２０ディジットのＥＳＤＳをＤＥＳおよびＵＥＳに対して使用すると、ＥＳＤＳは以下の結果を得るであろう：

ＥＳＤＳ：０６．１６．０９．１３．０１．０３．１９．１２．１８．１４．０５．０８．０７．１０．０２．１７．２０．１１．１５．０４

変位は各文字が移動するであろう場所を反映する以上のシーケンスに基づいて動作する。以上の実施例では、ＤＥＳまたはＵＥＳの最初の文字を６の位置に移動させ、第２の文字を１６の位置に移動させ、第３の文字を９の位置、などに移動させるであろう。

【０１５０】

３．　図６に図示する実施例に示すように、ＥＳＤＳＲＥＦに基づき対応するＥＳＤＳを持つＤＥＳおよびＵＥＳを変位させた後、各シーケンスを次にＣＳＤＳＲＥＦが示すように５つのＣＳＤＳの１つを使用してさらに変位させることができよう。例えば、ＣＳＤＳＲＥＦにおける「１」の値により示すように３つの内の最初のものを反映し、２０ディジットのＤＥＳおよびＵＥＳに使用する３つの実施例であるＣＳＤＳの１つを使用して、ＤＥＳおよびＵＥＳを以下のように変位させるであろう：

・ＣＳＤＳＲＥＦ＝「１」であれば、３つの実施例である２０ディジットに関係するＣＳＤＳの最初のものを使用するであろう（「６」）。ＤＥＳおよびＵＥＳに使用する各文字を６文字前方に移動させ、変化を反映し、それによりＤＥＳおよびＵＥＳ双方の第１の文字を変位させ、さらに暗号上危険に晒す危機を排除するであろう。

【０１５１】

４．　次に、新しいＤＥＳおよびＵＥＳを確立すると、以下の変更が次に生じるであろう：

・ＥＳＤＲＥＦを＋１だけ増加させるであろう。これがＥＳＤＳＲＥＦの総数より大きければ、ＥＳＤＳＲＥＦを「１」に設定するであろう；

・ＣＳＲＥＦを＋１だけ増加させるであろう。これがＣＳＲＥＦの総数より大きければ、ＣＳＲＥＦを「１」に設定するであろう（複雑さが増すために、暗号使用者が試行し、シーケンスを作成することができよう能力を無効にするために、ＣＳＲＥＦは単純に１と各ログオンに使用するＵＣＳおよびＤＣＳの総数との間を循環することができようことに注意されたい）；

・ＥＳＲＥＦを「０１」に設定するであろう。

【０１５２】

以上の実施例はＤＥＳおよびＵＥＳと同じ長さであるＥＳＤＳに関係する。ＤＥＳおよびＵＥＳが、例えば１００ディジットであり、ＥＳＤＳがそれぞれ１００ディジットであれば、種々のＥＳＤＳを使用して、ＣＳＤＳに関連する最終変位処理の前にＤＥＳおよびＵＥＳの各１００ディジットのブロックを変位させるであろう。

【０１５３】

当然、認証デバイス１０６と認証サーバ１１６との間の符号同期を維持するために、変位処理は認証デバイスおよび認証サーバ双方において同期する必要がある。同期化の後、認証デバイス１０６は、ユーザが次回に認証する必要のある場合に備えるであろう。

【０１５４】

変位処理が完了した後に次にユーザがログオンする際に、以下のデータを使用して、処理を適する位置に付かせる：

・　ＤＥＳおよびＵＥＳ双方を、位置１における新しい開始文字により変位させ、配列するだろう；

・　ＣＳＲＥＦを１とＣＳＲＥＦの総数との間の値に設定し、ＣＳＲＥＦの総数はサービス認証符号の認証およびユーザのＰＩＮの符号化において使用する適当なＵＣＳおよびＤＣＳ符号を参照するであろう；

・　認証サーバが提示する次のサービス認証符号は最後の２文字を「０１」に再設定させ、ＤＥＳおよびＵＥＳ双方が持つ１０ディジットの第１のブロックを使用することを示すであろう。

【０１５５】

一度ＤＥＳおよびＵＥＳ双方の変位が完了すると、ＣＳＤＳは次に各シーケンスの最初の１０ディジットを使用するための開始点を再配列する手段として、全シーケンスを変位させることができよう。これは結果として以下の暗号化上の複雑さになるであろう。

【０１５６】

１．　経験のある暗号使用者が最初の１００回のログオンに使用したＯＴＰを全て獲得したとしても（１０００ディジットのＵＥＳに基づいて）、４ディジットのＰＩＮを４ディジットのパスワードに符号化し、各１０ディジットのブロックの内の４ディジットのみを使用したであろうとすれば、暗号使用者は１０００ディジットのシーケンスにおける文字の４０％を獲得したに過ぎないであろう。これは２文字のみ、例えば「３５５３」をＰＩＮに使用する場合にはただの２０％に減少することがありえよう。

【０１５７】

２．　これは、各符号化パスワード内において使用するディジットのそれぞれが対応するサービス認証符号において使用する任意のディジットでありうることを意味するであろう。従って、最初の１００回のログオンに対しては何も漏らさないであろう。

【０１５８】

３．　ＥＳＤＳＲＥＦに対応するＥＳＤＳを使用し、１０００文字全ての複雑な変位に従うと、その場合新しい開始点をＣＳＤＳＲＥＦに対応するＣＳＤＳが定義することになり、従って実際上新しい１０００ディジットのＵＥＳを提供するであろう。

【０１５９】

４．　次いで、暗号使用者が次の１００のＯＴＰのそれぞれを捉えたとしても、暗号使用者は試行し、シーケンスのベースにするデータの２０％乃至４０％を、再言すれば得るに過ぎないであろう。一方、これら追加の１００のＯＴＰを種々のサービス認証符号に対して作成したであろうし、それにより２つの間の「可能な」相関を失い、複雑さはかなり大きくなったであろう。

【０１６０】

５．　理論的には暗号使用者が第１の１００のＯＴＰから何も得なかったとしても、暗号使用者は、その場合３６０万の可能なサービス認証符号シーケンスのそれぞれに対して動作する第２の32×10^{1530}のＵＥＳを試行し、見ることができ、そこで暗号使用者は可能な開始点として１０００ディジットのそれぞれを試行しなければならず、それにより使用する第１の32×10^{1530}ディジットのＵＥＳに対して同じＰＩＮを反映したであろう可能な３６０万のサービス認証符号を判断するであろう。不幸にして暗号使用者は、また少なくとも２７の繰り返すＵＥＳ文字と戦わねばならないことになり（１０００ディジットのＵＥＳに基づいて）、このＵＥＳ文字は複数の誤った実在するサービス認証符号を作成するだろうし、暗号使用者が成功したと考えることができる頃には、変位シーケンスが再び生じるだろうし、サービス認証符号もまた変化するだろう。

【０１６１】

１．　従って概念的には、過去のＵＥＳの一部を計算し、可能性のあるパターンおよび有力なＰＩＮを確立することは可能であるが、このような解析を行うデータは過去のものであらねばならず、従って変位シーケンスが生じるたびに古くなる。

【０１６２】

実施例４：ユーザＰＩＮの再設定

ユーザ１０２がログオンを試行して３回失敗するか、またはそのユーザＰＩＮを忘れたと恐らく悟るかのいずれかの場合、ユーザを自動的にＱ＆Ａ機能に移動させることにする。

【０１６３】

その場合、処理は次のようであろう：

１．　ユーザが単純にそのユーザＰＩＮを忘れ、ＰＩＮを再設定することを望めば、ユーザにその起動符号を入力することを求めるであろう。ユーザが何回か失敗した（例えば、３回）としても、起動符号は既に提供されているであろう；

２、　起動符号を認証サーバ１１６に送り、認証サーバ１１６はサービス認証符号をユーザ１０２に提示するであろう。
【０１６４】
３．　ユーザ１０２はサービス認証符号を検証し、ランダムに選択したＰＩＮ（認証サーバ１１６が選択した）をその認証デバイス１０６に入力するように助言をうけるであろう。
【０１６５】
４．　ユーザは次いで符号化ＰＩＮを入力し、これを認証サーバ１１６に提出するであろう。
【０１６６】
５．　ＰＩＮが、ユーザが正しい認証デバイス１０６を有していることを示せば、ユーザ１０２にＱ＆Ａ処理を提供する。
【０１６７】
６．　Ｑ＆Ａ処理が成功裡に完了すると、ユーザ１０２に新しいユーザＰＩＮを選択することを求めることになるであろうし、ユーザＰＩＮがＱ＆Ａ処理にアクセスしようとするものでなければ、認証サーバ１１６は、その場合ユーザ１０２が認証デバイスの発給者か、またはユーザがアクセスを得ようと試行するパーティと接触するのに十分な所定の時間の間ユーザを締め出すであろう。
【０１６８】
７．　Ｑ＆Ａ処理に失敗すると、ユーザはその認証デバイスを再度使用可能にするために、ユーザ１０２が信頼するソースを訪れねばならないことになるはずであり、そのために１００ポイントの調査が必要になるであろう。
【０１６９】

実施例５：複数サービス環境における認証方法およびデバイスの適用性
　一実施形態では、種々の信頼レベルか、または信頼範疇により表す信頼関係に基づき、ユーザ１０２は複数の遠隔サービスへのアクセスにその単一の認証デバイス１０６を使用することができる。例えば、認証方法は以下のように信頼範疇に基づくことができる：
信頼レベル３：
　ユーザ１０２が銀行または適当な小売店で担当者が認証した「１００」の調査ポイントを完了すると、信頼レベル３の範疇を達成することができる。
【０１７０】
　ユーザ１０２がインターネット銀行取引に新規であり、その認証デバイス１０６を取得するために支店を訪ね、その時点で銀行が１００ポイントの調査を行い、その支店の遠隔サービスにユーザを登録するであろう場合は、信頼レベル３の範疇を即座に達成することができよう。
【０１７１】
　あるいは、ユーザ１０２が信頼レベル３の範疇を達成することを望み、ユーザが既に認証デバイス１０６を持っていれば、ユーザ１０２は１００ポイントの調査を完了するために、銀行または適するように信頼するソースを訪ねなければならないでだろうが、その時点でユーザの詳細情報を認証デバイス１０６において更新できよう。
【０１７２】
信頼レベル２：
　ユーザ１０２が確実な方法で以前の信任情報を取得しているサービスを介してその認証デバイス１０６を登録する場合、信頼レベル２を達成することができる。
【０１７３】
　例えば、インターネット銀行取引に使用した既存ユーザＩＤおよびパスワードは、郵送などのある確実な手段によってかまたは支店においてユーザ１０２に提供したに過ぎなかったであろう。それ故、ユーザ１０２は特定情報の取り扱いが以前管理されていたと思われる機密性の厳しいサービスにログオンしようとするであろう。

【０１７４】
同様に、オンライン購入または電話など、カードがない場合にクレジットカード保持者を検証するのに使用する情報は、ユーザのみがカードによって種々の唯一の符号にアクセスするはずであるので、信頼レベル２の範疇と思われるであろう。
【０１７５】
信頼レベル１：
ユーザがオンライン・オークション・ウェブサイトなど、遠隔サービスに使用する認証デバイス１０６を取得するのであれば、そのユーザ１０２の初期登録は特定情報の取り扱いまたは管理のない自己登録の簡単な処理であったであろう。それ故、認証デバイス１０６はその個々のサービスに対してその個人がその後行う全ての取引に対してさらに安全性を加えるであろうが、その真の特定情報を検証する手段は存在しないであろう。
【０１７６】
登録前にユーザを検証するのに使用する信任情報が、信頼レベル２の下で詳述したようにある形式の特定情報の管理により提供される限り、信頼レベル２のサービス提供業者が使用するためにユーザの認証デバイス１０６を登録することにより、ユーザを信任レベル１から信任レベル２へ上げることができよう。同様に、ユーザが銀行かまたは適するように信頼するソースを訪ね、そこで‐条件および規約が適用するであろう１００ポイントの調査を実行することができれば、ユーザ１０２を信頼レベル３に上げることができよう。
【０１７７】
全てのサービス提供業者間で合意する２次特定情報が、ユーザ１０２をそれぞれの口座と関連付けることを可能にするのに十分唯一であらねばならないであろうことに注意するのは重要である。例えば、以前に記述したオンライン・オークション・ウェブサイトは１００ポイントの調査を確実に口座に結合することができるであろう手段を選択しなければならないであろうし、同様に銀行は、キャッシュカード口座または類似のものなど‐ユーザを検証する適切な手段と思われるであろうある形式の特定情報を規定する必要があるであろう。
【０１７８】
信頼レベル３ｖ：
第４の信頼レベルを、また規定することができようが、第４の信頼レベルは処理手段では達成できないであろう。問題であるか、または不正目的に使用されているその認証デバイス１０６を使用することなく、ユーザ１０２が予め規定する数の認証サイクルを完了した場合、この信頼レベルを達成することができよう。このような手法は漸進的信頼関係を提供するであろうし、漸進的信頼関係は信頼レベル２の範疇より強いと思われるが、信頼レベル３の範疇ほど強くはないであろう。一方時に、個々のデバイスを使用し、ユーザ状態を信頼レベル３ｖに更新する集約的サービスにより容認可能と見ることができよう。
【０１７９】
認証デバイス１０６が個々のサービスを使用する所定の数を超えると、オンライン認証報告を生成することができよう。各サービスは、その場合遠隔サービス１０４とのユーザの活動に基づき対応するユーザ１０２を「信頼する」用意がどの程度あるかを判断することができよう。
【０１８０】
ユーザが所定の使用数を超えた全てのサービスによりユーザ１０２を容認する場合、ユーザが１００ポイントの調査を全て完了していなくとも‐信頼レベル３Ｖへの漸進的昇格は、信頼レベル３Ｖのユーザを受け入れることに合意した‐信頼レベル３のサービスにユーザがアクセスすることを可能にするのに適当とみなすことができよう。
【０１８１】
以上に記述したタイプの信頼モデルを使用する本発明の実施形態は、さらにバーチャル特定情報の管理を提供することができ、それによるシステムの使用により、取引の合法性および所定の取引量に基づく所与のユーザの特定情報に関する信頼性に繋がることができるであろうと考えられる。

【０１８２】

実施例６：相互動作可能な認証デバイスの信頼レベル登録

次の節では、各信頼レベルの登録処理を説明し、また信頼レベル１の状態の達成に関連する処理フローを強調する。

【０１８３】

郵便局、消費者用電子機器店および同類などの‐認証デバイス１０６を取得する‐認証デバイス１０６を確実な方法で提供することに必ずしもならないかもしれない‐多くの変形および手段があるとすれば、本発明の実施形態は、登録が生じるであろう、規定された処理およびそれに従い第３のパーティの遠隔サービス提供業者に関係する適切な信頼レベルを提供する。本質的に、信頼レベル１にある認証デバイスを持つユーザはより高いレベルのサービスにアクセスすることはできないであろう。

【０１８４】

信頼レベル３の範疇：

信頼レベル３をユーザは以下の４つの方法で達成することができよう：

（ｉ）　銀行、政府機関または郵便局および同類などの信頼するソースが提供するサービスへのアクセスを得ることを望む新規ユーザ１０２；

（ii）　以上に規定したように、信頼するソースによる１００ポイントの調査（「１００ポイント調査」）を行う既存ユーザ１０２；

（iii）　ユーザ１０２を、登録し、信頼する認証デバイスサービスが認証することができる唯一の特定情報を有するサービスにユーザ１０２がアクセスを得るのに使用していた認証デバイス１０６をユーザが失う場合；および

（iv）　ユーザ１０２がそのＰＩＮおよびその自らの質問への答えを忘れ、Ｑ＆Ａ処理を完了できない場合；

これら種々の手法のそれぞれを、次により詳細に記述することにする。

【０１８５】

（ｉ）　新規ユーザ

即座に信頼レベル３の範疇を達成するために、ユーザ１０２は銀行、政府機関または郵便局または同類などの信頼するオンラインサービスに自らを登録しようとしなければならないであろう。

【０１８６】

ユーザ１０２は信頼するサービス‐例えば銀行の支店‐を尋ね、そのサービスへ登録することを求めるであろう。

【０１８７】

支店代表者はその場合「１００」ポイントの調査および認証登録処理の両方を完了する必要があるであろう。

【０１８８】

「１００」ポイントの調査は標準処理であるが、認証管理コンソールにおいて図的に表し、支店代表者が全て必要な工程を完了したことを確かめることができよう。信頼するソースが、個人に関係する、銀行口座などの既存口座を持たねばならないであろう‐ユーザの特定情報を検証するために「１００」ポイントの調査を完了すると、支店代表者は次に登録処理に従うことによりユーザの認証デバイス１０６を登録することができるであろう。

【０１８９】

これには、ＰＩＮを選択することを可能にするように、取得した（「マークを付けた」）認証デバイス１０６の起動符号の入力およびサービス認証符号の入力を必要とするであろう。この処理を完了すると、入力を支店代表者がディジタル的に「署名」することができようし、その時以後、ユーザ１０２は次いで信頼レベル３の状態を持つその認証デバイス１０６により対応するオンラインサービスにアクセスするであろう。

【０１９０】

また、認証デバイス１０６と信頼するサービス提供業者との間で予め合意し、キャッシュカード口座番号または類似のものなどの‐唯一の特定情報を入力しなければならないであろう。これは「１００」ポイントの調査を越え、かつその上の２次の特定情報であるであろうものであり、これは、ユーザ１０２がその認証デバイス１０６を失くすか、またはその個人的質問への答えを忘れ、新規デバイスを獲得するか、またはその口座を再設定するために、別の信頼するソースを訪ねればならなかった（以下のiiiおよびivで規定する）場合に必要になるであろう。

【０１９１】

初期登録を行い、認証デバイスを提供する信頼するソースは、またユーザの主要なサービス提供業者になるであろう。

【０１９２】

ii）　「１００」ポイントの調査

登録した認証デバイスのユーザ１０２が信頼レベル３の状態を得ることを望んだ場合、ユーザは認証デバイスを登録した、銀行、政府機関または郵便局などの信頼するソースを訪ねる必要があるであろう。

【０１９３】

信頼するソースに、ユーザを既に登録したサービスがあれば、ユーザはソースと共有した口座に対する「１００」ポイントの調査を検証することができるであろうため、ユーザは「１００」ポイントの調査処理全体を完了することができるであろう。これは、ユーザ１０２が信頼レベル２の範疇として以前に既に自らをオンラインで登録し、その後本人が遠隔サービス提供業者を訪ね、その信頼レベル範疇を変更した場合に生じることがありえよう。

【０１９４】

代表者は、合意したサービス特定情報（キャッシュカード番号、などなどの）および／またはその認証デバイスの起動符号によりユーザの認証デバイス口座にアクセスすることができるであろう。認証サーバは次に「１００」ポイントの調査を達成する要求条件の全てを要約するであろう。

【０１９５】

代表者は、次に認証サーバが発給したその認証デバイスおよびサービス認証符号に基づき１回のＰＩＮを提供することによりユーザ自身を認証デバイスに対して成功裡に検証することをユーザに要求することができよう。この処理を完了すると、ユーザを信頼レベル３のユーザとして登録するであろう。

【０１９６】

ユーザ１０２が、口座を持たない信頼するソースを訪ねた場合、ソースは依然「１００」ポイントの調査を行うことができよう。

【０１９７】

そのような場合、ユーザ１０２は認証デバイス１０６とユーザ１０２が口座を登録した遠隔サービス１０４との間で詳細化したような唯一の特定情報を提供するであろう。代表者は次に認証デバイス管理コンソールにログオンし、適切なサービスを探し、ユーザが保持する‐キャッシュカード、運転免許証などの情報が、それぞれのサービスに対して登録したものであることを検証することができよう。認証サーバ１１６は次に「１００」ポイントの調査のための要求条件およびまた代表者が調べようとする遠隔サービス１０４が、代表者が署名したものとして要求するであろう、その他の詳細情報の要点を共に示すことができよう。

【０１９８】

この工程を完了すると、代表者は次に検証のさらなる手段としてユーザの認証デバイスＰＩＮを入力することをユーザに要求し、次いで入力にディジタル署名することにより詳細情報を検証することができよう。ユーザはその場合信頼レベル３の状態を獲得するであろう。

【０１９９】

iii）　失くしたデバイス

ユーザ１０２がその認証デバイス１０６を失くす場合、ユーザはその認証デバイス１０６の使用を登録した信頼するサービスから別のデバイスを獲得するか、または銀行または郵便局などの信頼するソースであらねばならないであろう‐登録する別のサービスを訪ねることができよう。

【０２００】

ユーザの認証デバイス１０６が可能にするサービスをユーザに再度可能にするために、新規認証デバイス１０６を提供する代表者は「１００」ポイントの調査を行い、またユーザがその認証デバイス１０６を登録した‐代表者自らのデータベースと対照してユーザの唯一の特定情報を検証するか、‐または特定情報が、ユーザ１０２を登録した別の遠隔サービス１０４の特定情報と整合することを確かめなければならないであろう。

【０２０１】

ユーザ１０２が、その認証デバイス１０６の使用を登録した信頼するサービスから認証デバイス１０６を取得しようとした場合、代表者は「１００」ポイントの調査を実行し、唯一のサービス特定情報を検証することができよう。一方、認証デバイス管理コンソールにおける再使用可能化処理は唯一の特定情報と共に新規デバイスの起動符号を提出することを単に要求するであろうし、認証サーバ１１６はユーザの古い認証デバイス１０６から新規デバイスへユーザの詳細情報を伝送し、その後元のデバイスを解約することができよう。

【０２０２】

ユーザ１０２がその認証デバイス１０６を失くしただけであろうとすれば、認証サーバ１１６による特定の追加手段としてユーザにまたそのユーザＰＩＮを提出することを求めるであろう。

【０２０３】

ユーザ１０２が、その認証デバイス１０６を既に登録した信頼するサービスによりその認証デバイス１０６を再使用可能化しようとするであろうとすれば、再使用可能化は即座であり、ユーザ１０２は認証デバイス１０６を実際上使用して、ユーザが以前に登録した全てのサービスにアクセスすることができよう。

【０２０４】

さらに、必要な１００ポイントの調査を完了すると、信頼レベルの範疇を信頼レベル３に移すことができよう。

【０２０５】

さらに、認証デバイス１０６を、小売販売店により販売するために利用するのであれば、ユーザ１０２はその新規認証デバイス１０６を既に購入したであろう故、代表者はユーザが持ち込むどのような認証デバイス１０６も使用することができよう。認証サービスは、ユーザ１０２を再可能にするために起動符号を入力した時間を調べ、認証デバイス１０６が誰か他により既に使用されていないか、または動作不能にされているかを確かめ、このようにして失くしたか、または盗まれたデバイスが再使用されることを防ぐであろう。

【０２０６】

ユーザ１０２が、ユーザが登録していない信頼するサービスを訪ねる場合、代表者は「１００」ポイントの調査を行い、ユーザが既に登録したサービスの唯一の特定情報を検証するであろう。ユーザ１０２がその認証デバイス１０６を単に失くしたであろうとすれば、ユーザにまた認証サーバによる特定の追加手段としてそのユーザＰＩＮを提出することを求めるであろう。

【０２０７】

ユーザはその場合認証デバイスを登録し、最可能化することができよう。

【０２０８】

iv）　Ｑ＆Ａの完了不可能

ユーザ１０２が、そのＱ＆Ａを完了することができなければ、ユーザは登録認証デバイスが信頼するサービスを訪ねる必要があるであろう。

【０２０９】
信頼するサービスだけが「１００」ポイントの調査を行い、認証サービス管理コンソールと対照してユーザ１０２の特定情報を検証することができよう。
【０２１０】
以上の（iii）（即ち、遺失デバイス）の場合のように、ユーザ１０２が、ユーザがその認証デバイス１０６を登録したサービスを提供する信頼するソースに行けば、代表者は「１００」ポイントの調査を行い、認証デバイスの起動符号、サービス認証符号およびユーザのための新規ＰＩＮの選択を使用することにより認証デバイス１０６を再使用可能化することができよう。
【０２１１】
ユーザ１０２が、ユーザ１０２が登録していないオンラインサービスを提供する登録認証デバイスが信頼するソースに行けば、信頼するソースは「１００」ポイントの調査を行い、唯一の認証デバイスサービス特定情報と対照して検証することができよう。同時に、これらは、特定情報およびユーザが特定情報を提供した遠隔サービスとの個人の関係を確かめるには十分であるであろう。結果として、ユーザ１０２をその新規デバイスにより再使用可能化することができよう。
【０２１２】
さらに、ユーザ１０２が再度初めてログオンすると、ユーザが最初のときのころの新規質問および個人的答えを忘れたであろうとすれば、ユーザに新規質問および個人的答えを提出することを求めることになろう。
【０２１３】

実施例６：認証デバイスの処理
以下の実施例は、１次および２次両方のサービスを通じてユーザ１０２がその認証デバイス１０６を登録することができる種々の方法、およびその認証デバイス１０６を引き続き使用することを確実にするために典型的に従う必要があるであろう処理を説明する。ある実施形態では、このような処理は以下の実施例を含むことができるが、これに制限されることはない：
１．　認証デバイスの配備；
２．　認証デバイスの登録；
３．　複数デバイスの登録；および
４．　ユーザの認証デバイスの取得
これらの処理のそれぞれを次に詳細に記述することにする。
【０２１４】
１．　認証デバイスの配備：
この節では、ユーザが信頼レベルの範疇に従い認証デバイスを登録するか、または獲得することができる手法を概説する。
【０２１５】
信頼レベル３：
以上で説明したようにある実施形態では、ユーザ１０２が即座に信頼レベル３の範疇を獲得することができる唯一の手法は、信頼するソースに自ら現れ、以下の「１００」ポイントの調査によりその認証デバイス１０６を実際に獲得することであろう。
【０２１６】
一方、標準認証デバイス１０６を「手に入れること」に加えて、ユーザ１０２は、また以下のような幾つかの方法の１つで、認証デバイス１０６をユーザに提供することを要求することができよう：
１．　移動電話機などの移動デバイスへの送信。これは、ユーザが自らを登録するか、または新規認証デバイスを（その以前のものを失くして）獲得する際に、ユーザ１０２がその移動電話機の詳細情報を提供することを伴うであろう。このような方法で提供される場合、認証デバイス１０６を、ユーザに対して始めて「マークを付ける」はずである「ソフ

トウエアデバイス」として提供するだろう故、ユーザは登録の過程でそのユーザＰＩＮを選択することができる。ＳＭＳまたは類似のものを介して認証デバイス１０６を受け取ると、ユーザ１０２は認証デバイス１０６にログオンするユーザＰＩＮを既に有しているであろう；または

２．　ＨＰｉＰＡＱハンドヘルドコンピュータなどの別の媒体に新規ソフトウエアデバイスをダウンロードすることを望むユーザ１０２に関して、ユーザ１０２がダウンロード可能なソフトウエアデバイスの貯蔵場所にアクセスし、そのそれぞれに新たに登録した認証デバイス１０６を結合することにより、認証デバイス１０６を分配することができる。この手法でユーザがその認証デバイス１０６を登録するのを手伝う人物は、ユーザが選択する恐らく標準的、一回使用可能なパスワードを伴う起動符号によりソフトウエアデバイスへのリンクを提供することができよう。ユーザはまたその認証デバイスのＰＩＮを選択することができるであろう。ユーザに提供される起動符号およびユーザが選択した標準的、１回のパスワードを使用して、ユーザ１０２がその後認証サーバ１１６にログオンする場合、これによりユーザ１０２がそのソフトウエアデバイスにアクセスすることが可能になり、次いでソフトウエアデバイスを、ユーザはそのＨＰｉＰＡＱまたは類似の媒体にダウンロードすることができよう。このデバイスのために既に選択したＰＩＮにより、ユーザ１０２は認証デバイスを使用することができ、信頼レベル３の範疇を破らなかったであろう唯一の人物である。

【０２１７】

信頼レベル２：

以下の黒点はユーザ１０２が信頼レベル２の関係下において認証デバイス１０６を獲得するであろう方法を強調する：

・ユーザＩＤおよびパスワードなどの既存信任情報を使用して、ユーザが対応するサービスにログオンした際に認証デバイスを要求した後、認証デバイスを郵便でユーザ１０２に物理的に送付することができよう。同様に、ユーザ１０２はクレジットカードの詳細情報など唯一の既存特定情報に基づき認証デバイス１０６を要求することができ、次いで認証デバイスを認証デバイスそれぞれに対し遠隔サービスのデータベースにおいて保持するアドレスへただ郵送するであろう；

・クレジットカードの詳細情報など既存信任情報または提供された既存特定基準を使用して、サービスに署名契約した後、ユーザ１０２は「ソフトウエアデバイス」をＳＭＳによりユーザ１０２へ送信することを要求することができよう；または

・ユーザ１０２は認証デバイス１０６を、ダウンロードすることを要求し、ユーザが認証デバイスをＨＰｉＰＡＱなどのユーザが選ぶ媒体にインストールすることができよう。

【０２１８】

以上に規定する全ての例証では、認証デバイスを保持する媒体に関わらず、認証サービス登録処理は、ユーザが認証デバイスを所有している場合と同じであろう。

【０２１９】

信頼レベル１：

認証サービスが、ユーザ１０２は、ユーザが述べる者であると単に想定するであろうとすれば、信頼レベル１の範疇の認証デバイス１０６を取得するために、管理であるべきものは何もないであろう。ユーザが自ら登録でき、あらゆる個人の詳細情報を入力できるとすれば、口座を一度設定すると、このレベルの管理は口座が危険に晒されることを単に防止するだけである。

【０２２０】

以上で詳述したように、信頼するソースからの既存信任情報を使用して、ユーザの認証デバイスを登録することにより、ユーザ１０２は何時でも信頼レベル１の範疇の関係から信頼レベル２の範疇の関係へ移行することができよう。同様に、信頼するソースを訪ね、「１００」ポイントの調査を完了することにより、ユーザはまた信頼レベル３の範疇の関係へ移行することができよう。

【０２２１】

全ての例証には、ユーザ１０２が小売販売店から認証デバイス１０６を購入するのを妨げる何物もないであろうことに注意されたい。一方、信頼レベルの関係は登録処理に依存するであろう。

【０２２２】

信頼レベル１の範疇の関係が存在することができる一方、改善された信頼レベルのユーザ範疇に値するであろう認証デバイスの分配に関する安全な手段を、遠隔サービスが配備することができることに注目することは、また重要である。とはいえ信頼レベル１の範疇の関係は優れて自己登録および信頼に基づくので、これは遠隔サービス提供業者間で合意しなければならないであろう。それ故、ユーザが提供する詳細情報は不正でありえ、信頼レベル２の範疇の分類には信頼することができないであろう。本質的に、信頼レベル１の範疇を超えて増大する信頼レベルの分類の唯一の安全な活用は、信頼レベル３の範疇を達成することでなければならないであろう。

【０２２３】

以上を見ると、それ故少なくとも信頼レベル２の範疇の関係により既に発給した認証デバイスをてこ入れすることが、信頼レベル１のサービス提供業者の最大の関心事において不可避であるであろう。

【０２２４】

２．　認証デバイスの登録

以下の節では、ユーザがその認証デバイスの登録の過程で従うであろう登録処理の実施例およびユーザの信頼レベルの範疇への依存性を概説する。

【０２２５】

信頼レベル３の登録：

ユーザ１０２が銀行または郵便局などの信頼するサービス提供業者に入ると、ユーザが最終的に使用するのをやめる認証デバイス１０６の媒体に関わらず、ユーザ１０２は標準登録処理に従うだろう。この処理の実施例を以下のように記述する：

１．　ユーザ１０２は信頼するサービス提供業者のオンラインサービスにアクセスするその希望を示すであろう。この実施例では、オンライン銀行取引サービスを使用した；

２．　銀行代表者は「１００」ポイントの調査を完了し、個人と個人が遠隔サービス提供業者と共有する口座との間に明確な繋がりを確立するであろう。この繋がりは認証サービスと銀行との間で以前に確立した唯一の特定情報であろう；

３．　銀行代表者は次に認証サービス管理に対して認証を行い、ユーザ１０２が選択する認証デバイスの媒体に依存して‐幾つかの異なる方法によりユーザを登録することができよう；

４．　ユーザ１０２が物理的デバイスを受け取ることを選択すれば、銀行代表者は認証デバイスの起動符号および唯一の特定情報の詳細を入力し、これらの情報をその後ユーザがその認証デバイスを失くした場合に要求するであろう。ユーザ１０２に、次いで‐物理的デバイスを検証するために、‐認証サーバ１１６が発給したサービス認証符号を入力することを要求し、次にＰＩＮを選択することを要求するであろう。ユーザは次いで信頼レベル３のユーザとして遠隔サービスにアクセスすることができるであろう。最初にユーザがログオンする場合、ユーザはＱ＆Ａ処理を経なければならないであろうことに注意されたい；

５．　ユーザ１０２が認証デバイス１０６をその移動電話機に配信することを望めば、銀行代表者は認証サーバから引き出す起動符号にその移動電話機の番号を連結する必要があるであろう。これは、またユーザがそのユーザＰＩＮをオンラインで選択することを可能にし、従ってソフトウエアデバイスをその後認証サーバがその移動電話機に配信する場合に、ユーザはユーザが選択したユーザＰＩＮを使用してログオンすることができるであろう。ユーザにまたＱ＆Ａ処理を完了することを助言するであろうことに注意されたい；

６．　ユーザ１０２がソフトウエアデバイスとして認証デバイスを獲得し、そのＰＤＡまたはＨＰｉＰＡＱなどにインストールすることを望めば、銀行代表者は再度個人に連結するであろう起動符号を引き出すであろう。ユーザにそのユーザＰＩＮを入力することを要

求すると同様に、代表者はまた１回の標準パスワードを要求するであろう。この１回の標準パスワードを、ユーザが後にログオンする場合、その認証デバイスにアクセスし、認証デバイスをダウンロードするためにその認証デバイスサービスにアクセスすることができるであろうという、その起動符号に関する注意と共にユーザに与えるであろう。その後、認証デバイスは次いでユーザが選択した正しいＰＩＮよってのみ動作し、ユーザにＱ＆Ａ処理を完了することを強いるであろう。

【０２２６】

信頼レベル２の登録：

信頼レベル２の範疇のユーザとして登録するために、ユーザ１０２は、郵便によるか、小売販売店からか、そのサービス提供業者から手に入れたか、または同類であったにせよ、可能と思われる手法で認証デバイス１０６を獲得できたと仮定しなければならない。ユーザの信頼レベル２の範疇を決めるのはその場合認証デバイスを登録する手法である。

【０２２７】

信頼レベル２の範疇への要点は、ユーザ１０２がユーザのみが使用すると思われる信任情報を既に与えられているであろうことである。例えば、インターネット銀行取引サービスへのアクセスに使用する既存信任情報またはクレジットカード詳細情報である。このような信任情報をある管理された配信機構の下にあるユーザに提供したであろうことに注意することは重要である。一方認証サービスの目的に対して、ありそうではあるが信任情報が正しい人の手に落ちたと想定することはできない。

【０２２８】

認証デバイスを登録すると、ユーザ１０２はオンライン銀行取引サービスなどの既存信頼レベル２のサービスにログオンするか、またはクレジットカードおよび同類などのユーザに唯一と考えられる情報がユーザにあることを保証するかいずれかをしなければならないであろう。

【０２２９】

ログオンするか、または唯一の信任情報を提示すると、個々の信頼レベル２の範疇であるサービスはユーザを登録のために認証サーバに移すことができよう。

【０２３０】

認証サーバ１１６はユーザのデバイス起動符号を要求し、それに対して認証サーバはサービス認証符号を返信するであろう。このサービス認証符号には２つの目的があり、即ちユーザ１０２が認証サービスと通信していることを確信することを可能にすることおよび認証デバイス１０６が認証サーバ１１６と同期することを保証することである。

【０２３１】

ユーザ１０２は、ユーザが認証サービスと通信していること確信すると、次に標準登録処理に従いＰＩＮを選択し、Ｑ＆Ａ処理を完了するであろう。これらの課題を完了すると、認証サービスは遠隔サービスに制御を返し、ユーザは遠隔サービスに対してその認証デバイスを登録しようとするであろう。遠隔サービス１０４は次いで唯一の特定情報を返信し、唯一の特定情報に対して、ユーザがその信頼レベルの範疇を変更することを望むか、またはユーザがその認証デバイス１０６を失くしたか、またはその自らのＱ＆Ａｓに答えることができなかった場合に、将来のユーザ検証を行うことができよう。

【０２３２】

信頼レベル１の登録：

信頼レベル１の範疇のユーザとして登録するためには、ユーザ１０２はユーザが述べる者であるかを確証する必要はない。オンライン・オークション・ウェブサイトなどの自己登録を必要とするサービスに対して、個人が、個人が述べる者であることを保証する手段はない。

【０２３３】

一方、インターネット上の取引に簡単なユーザＩＤおよびパスワードを利用する全ての口座を危険に晒すことを可能にする現在の恐れ故に、認証サービスは、このような口座に一人の個人およびその対応する認証デバイスのみがアクセスすることを保証するであろう

。
【０２３４】
信頼レベル１である範疇の自己登録の目的に対して、ユーザ１０２が郵便によるか、小売販売店からか、そのサービス提供業者または同類から手に入れたかであったにせよ、可能と思われる手法で認証デバイスを獲得することができたであろうと再度想定しなければならない。ユーザの信頼レベル１の範疇を決めるのはその場合認証デバイスを登録する手法である。
【０２３５】
信頼レベル１の範疇への要点は、ユーザ１０２がその完全性を保証する以前の手段を提示しなかったであろうことであり、従ってその特定情報を信頼レベル２または３の範疇に関係する取引およびサービスには信頼できないことである。
【０２３６】
認証デバイス１０６を登録すると、ユーザ１０２はユーザが自己登録の過程で最初に獲得した信任情報を使用して、オンライン・オークション・ウェブサイトなど既存の信頼レベル１の範疇であるサービスにいずれにせよログオンしなければならないであろう。さらに今度は、ユーザはまた信任レベル１の範疇のサービスが全てのユーザが有するであろうと考えるであろう、唯一の特定情報の形式を持つ必要があるであろう。この理由は、信頼するソースにおいてその後の再使用可能化および信頼レベルの範疇の更新を可能にするためである。
【０２３７】
古い信任情報を使用してログオンするか、または新しくユーザの自己登録処理を完了するかのいずれかを行うと、個々の信頼レベル１の範疇であるサービスは登録のためにユーザ１０２を認証サーバへ移すことができよう。
【０２３８】
認証サーバ１１６はユーザのデバイス起動符号を要求し、それに対して認証サーバはサービス認証符号を返信するであろう。このサービス認証符号には２つの目的があり、即ちユーザが認証サービスと通信していることを確信することを可能にすることおよび認証デバイスが認証サーバ１１６と同期することを保証することである。
【０２３９】
ユーザ１０２は、ユーザが認証サービスと通信していること確信すると、次に標準登録処理に従いＰＩＮを選択し、Ｑ＆Ａ処理を完了するであろう。これらの課題を完了すると、認証サービスは遠隔サービスに制御を返し、ユーザは遠隔サービスに対してその認証デバイスを登録しようとするであろう。遠隔サービス１０４は次いで将来のユーザ検証を行うことができるであろう、唯一の特定情報を返信するであろう。
【０２４０】
３．　複数デバイスの登録：
信頼レベルサービスの関係に対してユーザの認証デバイスを既に登録していると、その場合ユーザ１０２は認証サービス「ファミリー」における全ての他のサービスにその認証デバイス１０６を使用することから利益を得ることができるであろう。とはいえ、ユーザが登録することができるであろう遠隔サービス１０４は、その既存信頼レベルの状態およびユーザが自らを認証する手段に依存するであろう。
【０２４１】
信頼レベル３の状態：
ユーザ１０２が信頼レベル３のユーザとして既に登録していれば、ユーザは認証サービス「ファミリー」における全てのサービスに登録することができるであろう。
【０２４２】
全ての例証において、ユーザ１０２はその認証デバイス１０６による登録を選択することができるであろう。ユーザが登録することを望む遠隔サービスはその場合ユーザの起動符号を要求することができ、要求を認証サービスに対して行い、ユーザの信頼レベルの範疇を確立するであろう。ユーザが信頼レベル３のユーザでなかったならば、代替処理に従

わなければならないであろう（以下を参照）。

【０２４３】

ユーザ１０２が信頼レベル３の範疇のユーザであることを認証すると、サービス認証符号を提供し、そのユーザＰＩＮの入力を要求することにより、認証サーバ１１６はユーザが認証デバイス１０６の合法的所有者であることを保証することができよう。この工程を成功裡に完了することにより、認証デバイス１０６が遠隔サービスに符号を返信することが可能になり、遠隔サービスに対してユーザ１０２が登録しようとして、その個々のサービスの要求条件を満たす適切な詳細情報を完了することを可能にするであろう。

【０２４４】

遠隔サービスの登録処理が完了すると、遠隔サービスは、次にユーザがその認証デバイスを失くしたか、またはその自らの質問に答えることができなかった場合に、ユーザの再検証を可能にするために認証サーバがその後に使用するのに必要な唯一の特定情報を提供するはずである。

【０２４５】

ユーザがこの時点において不正な詳細情報を入力することが可能であるとしても、ユーザが信頼レベル３の範疇のユーザであるとすれば、認証デバイスを使用して行う将来のあらゆる活動を合法的なユーザに向けて追跡することができよう。

【０２４６】

信頼レベル２の状態：

ユーザ１０２が信頼レベル２の範疇のユーザであるとしても、ユーザはなおユーザが登録することを考える信頼レベル２の範疇のサービスから信任情報を直接獲得する必要があるか、またはクレジットカードなどの唯一の信任情報を既に持っている必要があるであろう。

【０２４７】

このような詳細情報を現在行われているように郵便で送れば、その場合ユーザはこれらの信任情報を使用してログオンし、次にその認証デバイスを登録することができよう。他方、ユーザが、ユーザが登録することを考える遠隔サービスを訪ねることに決めれば、ユーザはサイトにおいてこれを行うことができるであろうし‐以前に説明したように‐、結果としてその信頼レベルの状態を信頼レベル３に変更するであろう。

【０２４８】

ユーザ１０２に信任情報を送信したかまたは信頼レベル２のサービスに対する既存信任情報を既に持っていると仮定すると、ユーザはそのような信任情報を使用して、ログオンし、次いでユーザはその認証デバイスを登録することを要求することができるであろう。

【０２４９】

ユーザが登録することを望む遠隔サービスは次にユーザの起動符号を要求することができ、次いで登録を完了するために、認証サーバに制御を移すことができよう。一方この例証では、ユーザが既に登録されており、ユーザはサービス認証符号およびユーザＰＩＮの検証情報を提示することによりその特定情報を検証する必要があるだけであろうことを確証しているので、認証サーバ１１６は初期認証デバイスの登録処理に従わないであろう。

【０２５０】

認証サーバ１１６は次いで信頼レベル２の範疇のサービスに成功する符号を返送することができ、信頼レベル２の範疇のサービスは次に、ユーザがその認証デバイスを失くしたか、またはその自らの質問に答えることができなかった場合に、ユーザ１０２の再検証を可能にするために認証サーバ１１６がその後に使用するのに必要な唯一の特定情報を提供するであろう。

【０２５１】

信頼レベル１の状態：

デバイスを信頼レベル１の範疇のサービスに登録するために、ユーザ１０２は、ユーザが既に持っているかもしれない既存の自己登録信任情報を使用するかまたは遠隔サービスの自己登録処理を完了することができよう。いずれにしろ、ユーザ１０２は、ユーザが遠

隔サービス１０４にその認証デバイス１０６を登録することを望むことを示すであろう。これが行うであろうことの全ては、現在の恐れにより口座を危険に晒すことがありうる事実を制限することであり、認証デバイスを登録しようとする人物に対する口座の使用を制限するであろう。

【０２５２】

ユーザが登録することを望む遠隔サービス１０４は次いでユーザの起動符号を要求し、次に登録を完了するために認証サーバ１１６に制御を移すことができよう。一方この例証では、ユーザは既に登録されており、ユーザはサービス認証符号およびユーザＰＩＮの検証情報を提示することによりその特定情報を検証する必要があるだけであろうことを確証しているので、認証サーバ１１６は初期認証デバイスの登録処理に従わないであろう。

【０２５３】

認証サーバ１１６は次いで信頼レベル１の範疇のサービスに成功する符号を返送することができ、信頼レベル１の範疇のサービスは、次にユーザがその認証デバイス１０６を失くしたか、またはその自らの質問に答えることができなかった場合に、ユーザ１０２の再検証を可能にするために認証サーバ１１６がその後に使用するのに必要な唯一の特定情報を提供するであろう。

【０２５４】

ユーザの認証デバイスの取得：

ある実施形態では、認証デバイス１０６をユーザ１０２が取得するか、または獲得することができる２つの主要な手段がある、即ち：

１．　「物理的」認証デバイス‐物理的デバイスは誰がデバイスを提供することを決めようと、資本経費を必要とするであろう。これは認証サービス「ファミリー」における信頼レベルサービスのいずれかかまたはこのようなデバイスを一般に利用可能にすることを望む小売販売店でありうる。

【０２５５】

３．　「ソフトウエア」認証デバイス‐ソフトウエアデバイスを認証サーバ１１６からのダウンロードとしてか、または対応するサービスからのダウンロードとして利用可能にすることができる。このデバイスの手段を利用することは、資本経費は即座にではないが、ユーザがそのソフトウエアデバイスを必要とするのに要する時間に亘って広がることを意味しよう。

【０２５６】

実施例７：認証デバイスの既存処理への連結

認証デバイス１０６を「ビザによる検証」または「マスタカードの安全な符号」などの既存サービスの使用により既存処理へ連結することができよう。

【０２５７】

ユーザ１０２がこのようなサービスにより使用するためにその認証デバイス１０６を登録することを望む場合、ユーザが信頼レベル２の信任情報を持っているであろうことに基づき、現在実施されているように、ユーザ１０２は遠隔サービスにアクセスすることができるであろう。

【０２５８】

現在、これらのサービスは信頼レベル２の信任情報に基づきクレジットカードにおいて利用可能である。一方、ユーザ１０２が追加工程としてその認証デバイス１０６を登録するのであれば、遠隔サービス１０４はその場合静的パスワードをオンラインで入力しなければならないのに反して、支払い手段として本処理を利用することができよう。

【０２５９】

「ビザによる検証」および「マスタカードの安全な符号」などのサービスをクレジットカードの詳細情報をオンラインで入力する必要を避けるために導入したが、このタイプのサービスはなお「フィッシング」および／またはユーザのパスワードを得るためのキーストロークによるログインを許し、それによりオンライン支払いを不正に行うことができる

ことを許す。
【０２６０】
このように、遠隔サービスは唯一の特定情報としてユーザのクレジットカードの詳細情報を認証デバイスに提供することができるであろう。ユーザ１０２が支払いに認証デバイス１０６を使用することを選ぶ場合、遠隔サービス１０４はその場合１回のユーザＰＩＮにより支払いを認証する認証サーバ１１６に連絡をするであろう。
【０２６１】
以上を見ると、本発明はユーザ１０２が、ユーザが取引を行っていると信じる遠隔サービスおよび／またはエンティティと通信していることを検証するのを手伝うために適用可能な認証方法およびデバイスを提供することが認識されるであろう。現在の恐れが、幽霊ウェブサイト、「フィッシング」およびユーザが通信していると信じる合法的エンティティであるかの罪を犯す不正者によりユーザを騙して、その個人信任情報を暴くことができるので、これは反幽霊的で反社会工学的特徴を表す。
【０２６２】
さらに、唯一の１回のサービス認証符号をユーザ１０２に提供することにより、遠隔サービス１０４および／またはエンティティは効果的にユーザに対して自らを認証しようとし、その後業務をオンラインで取引する。
【０２６３】
以上の記述を見ると、当然本発明の実施形態による認証方法および／またはデバイスは３つの要因の認証方法および／またはデバイスを提供し、その中でユーザの特定情報に関する認証および／または検証を確認するには、以下の唯一の工程を成功裡に完了しなければならない。
【０２６４】
１．　ユーザ１０２がその特定情報を検証することを望む、遠隔サービス１０４か、またはその他のエンティティからの有効な認証サービス符号の提供。ある実施形態では、これは認証デバイス１０６が動作することを可能にするだろうし、無効な認証サービス符号は認証デバイス１０６を動作不能にするだろう。
【０２６５】
２．　認証デバイス１０６が符号化し、ユーザ１０２が認証しようとする遠隔サービス１０４か、またはその他のエンティティへの入力のために表示するか、または遠隔サービス１０４か、またはその他のエンティティへ中継して返送するユーザ自らの唯一のユーザＰＩＮを認証デバイス１０６に入力するユーザ１０２。
【０２６６】
３．　遠隔サービスおよび／またはエンティティへの符号化ユーザＰＩＮの入力。
【０２６７】
さらに、本発明の実施形態による認証デバイス１０６をユーザの選択に応じて移動電話機、ＰＤＡまたは類似のものにインストールするためにソフトウエアの形式で提供することができる。
【０２６８】
有利には、ユーザは登録の時点で認証デバイスを起動することができ、ユーザが認証デバイスを登録しようとする遠隔サービスが提供する既存信任情報により登録するまで認証デバイスは役立たないままであるので、本発明の実施形態による認証デバイス１０６は処理を開始する前に「準備をし」なくとも良い。
【０２６９】
以前に記述したように、認証デバイスは現存し、その他の場合には複数のデバイスを配備することが必要であろう複数の検証および認証処理との簡単な統合を可能にすることができる。簡単な登録処理により、安全性を必要とし、電話銀行取引、オンライン購入、手動特定および手形小切手の検証および同類など現在問題である多くの機能を行うために、ユーザはただ単一の認証デバイスを持っていればよいであろう。
【０２７０】

さらに、認証デバイス製品は、既存認証処理が強いる信頼関係に基づき漸進的特定を可能にすることができる。特に、ユーザの特定は即座である処理よりむしろ漸進的処理であることができよう。このような処理により、代替製品が動作するためにユーザの特定情報の瞬時の検証を必要とするこのような変化への現在の禁止要因を相殺するかなり経済的な利益を提供しうると考えられる。

【０２７１】

以上に記述したように、本発明の実施形態において提供するようなＱ＆Ａの特徴を、ユーザがその認証デバイスを物理的に所有しないかぎり、ユーザはそのＱ＆Ａにアクセスできないであろうことにより追加する。従って、認証デバイスがなければユーザはＱ＆Ａ処理を完了できないであろう故、質問へのアクセスを獲得する手段は本発明の実施形態が持つ安全性をさらに改善する。

【０２７２】

また、認証サーバはユーザがその認証デバイスを使用することができる時刻を決めることをまた可能にし、従って各ユーザにとってバーチャルで、固有の開いている時間を提供することができると考えられる。従って一実施形態では、ユーザは認証デバイスを使用することができる「開いている時間」を決めることができる。この実施形態によれば、この時間外ではログオンすることは可能でないであろう。ユーザが時間を変更することを望む場合、ユーザはユーザが予め規定する、開いている時間をそのように変更するまで待たねばならないであろう。それ故完全な制御はユーザにある。

【０２７３】

最後に、本明細書に記載する構成に対して、本発明の範囲内でもあるその他の変形および修正が存在することがあることは理解されるだろう。

【図面の簡単な説明】

【０２７４】

【図１】本発明の実施形態による方法の実行に適するシステムのシステムブロック図である。

【図２】本発明の実施形態による認証デバイスのブロック図である。

【図２Ａ】本発明による認証サーバを備えるシステムの実施形態のブロック図である。

【図３】本発明の実施形態に従う方法におけるユーザに対する遠隔サービスを認証する工程を記述するフローチャートである。

【図４】本発明の実施形態に従う方法における遠隔サービスに対するユーザを認証する方工程を記述するフローチャートである。

【図５】本発明の実施形態に従い擬似ランダム符号化シーケンスを変位させる変位処理の実施例を図示するテーブルである。

【図６】本発明の実施形態に従い擬似ランダム符号化シーケンスをさらに変位させるさらなる変位処理の実施例を図示するテーブルである。

【図１】

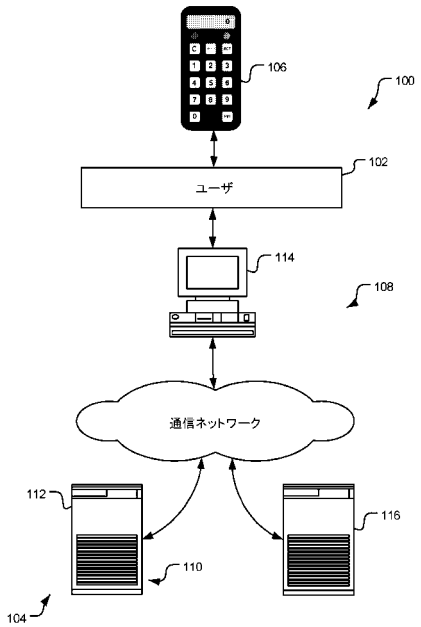


FIGURE 1

【図２】

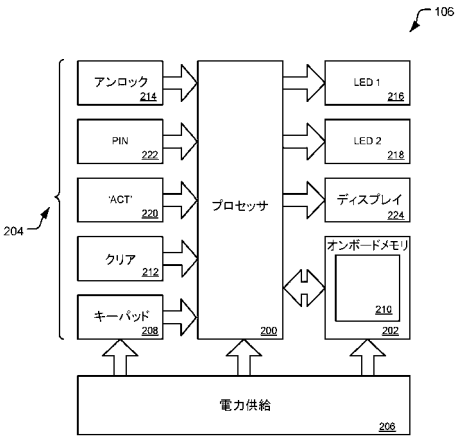


FIGURE 2

【図２Ａ】

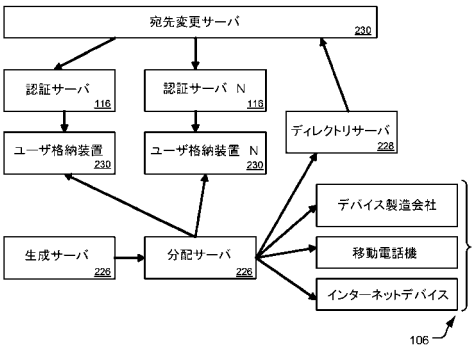


FIGURE 2A

【図３】

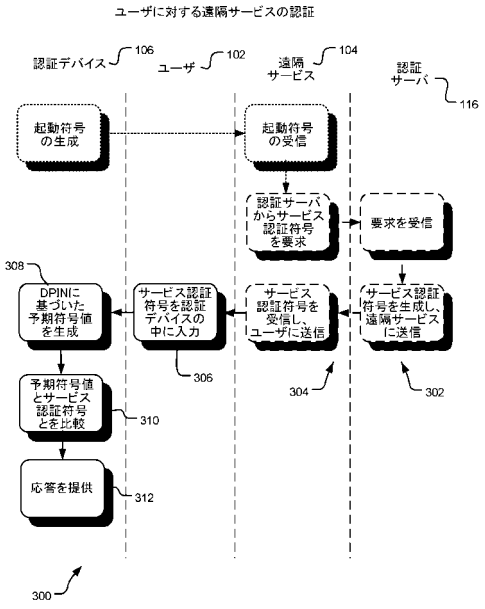


FIGURE 3

【図４】

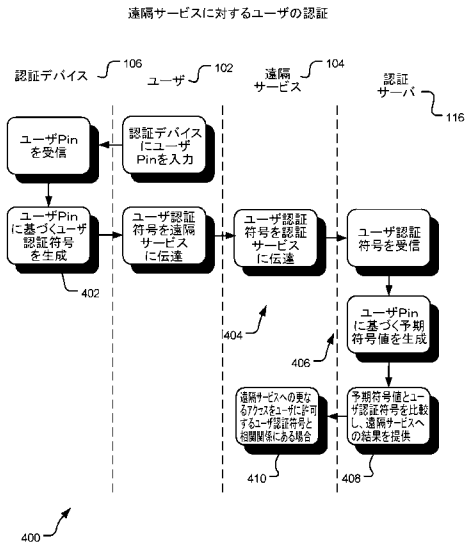


FIGURE 4

【図５】

ESDS	06	16	09	13	01	03	19	12	18	14	05	08	07	10	02	17	20	11	15	04
位置	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
DES	7	3	6	1	9	4	8	2	6	4	0	1	9	4	8	2	7	3	5	1
変位DES	9	8	4	1	0	7	9	1	6	4	3	2	1	4	5	3	2	6	8	7
UES	A	2	3	C	T	B	L	M	4	S	5	R	T	7	P	6	S	J	K	9
変位UES	T	P	B	9	5	A	T	R	3	7	J	M	C	S	K	2	6	4	L	S

FIGURE 5

【図６】

位置	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
第１変位DES	9	8	4	1	0	7	9	1	6	4	3	2	1	4	5	3	2	6	8	7
最終変位DES	5	3	2	6	8	7	9	8	4	1	0	7	9	1	6	4	3	2	1	4
第１変位UES	T	P	B	9	5	A	T	R	3	7	J	M	C	S	K	2	6	4	L	S
最終変位UES	K	2	6	4	L	S	T	P	B	9	5	A	T	R	3	7	J	M	C	S

FIGURE 6

フロントページの続き

(72)発明者 ヒューイット、 サイモン チャールズ ヒューズ
オーストラリア国 ３１０６ ビクトリア州 テンプルストウ スミス ロード ６５
(72)発明者 ベンダー、 ジェイソン フレデリック
オーストラリア国 ５０６４ サウスオーストラリア州 グレン オズモンド バイン レーン ３
(72)発明者 レノン、 ジェイムズ エバン
オーストラリア国 ５００７ サウスオーストラリア州 ブロンプトン フローレンス クレセント ４８

審査官 和田 財太

(56)参考文献 特開２００４－３０４７５１（ＪＰ，Ａ）
米国特許第６７９９２７２（ＵＳ，Ｂ１）
国際公開第２００２／０７９９６０（WO，Ａ１）
国際公開第２００１／０３１８４０（WO，Ａ１）
国際公開第２０００／０５６００９（WO，Ａ１）
英国特許出願公開第２３８７９９９（ＧＢ，Ａ）
英国特許出願公開第２３６９４６９（ＧＢ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
G06F 21/20-21/24
H04L 9/32