(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2014-531659
(P2014-531659A)
(43)公表日　平成26年11月27日(2014.11.27)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/20	131A	5J104
H04L 9/32	(2006.01)	H04L	9/00	673A	

審査請求 未請求　予備審査請求 未請求　（全 19 頁）

(21)出願番号	特願2014-531058 (P2014-531058)
(86)(22)出願日	平成24年9月21日 (2012.9.21)
(85)翻訳文提出日	平成26年3月17日 (2014.3.17)
(86)国際出願番号	PCT/CA2012/050661
(87)国際公開番号	WO2013/040713
(87)国際公開日	平成25年3月28日 (2013.3.28)
(31)優先権主張番号	61/538,114
(32)優先日	平成23年9月22日 (2011.9.22)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	13/623,641
(32)優先日	平成24年9月20日 (2012.9.20)
(33)優先権主張国	米国 (US)

(71)出願人　514066734
キネシス　アイデンティティ　セキュリティ　システム　インコーポレーテッド
カナダ国、ブイ７ティー　１ビー８、ブリティッシュ　コロンビア州、ウエスト　バンクーバー、５１８－１４８９　マリンドライブ
(74)代理人　100114775
弁理士　高岡　亮一
(74)代理人　100121511
弁理士　小田　直
(74)代理人　100191086
弁理士　高橋　香元

最終頁に続く

(54)【発明の名称】ユーザ認証のためのシステムおよび方法

(57)【要約】
ユーザの認証を可能にするシステムおよび方法が開示される。非機密性かつ一意のユーザ識別番号および一時的アクセスコードを使用することで、ユーザの認証を、任意の利用者パスワードまたはユーザ識別可能なデータを送信することから切り離し、さらに、関係性のない組織の間で何ら情報を交換することなく当該組織でユーザを認証する偏在的手段を提供する。
【選択図】図１

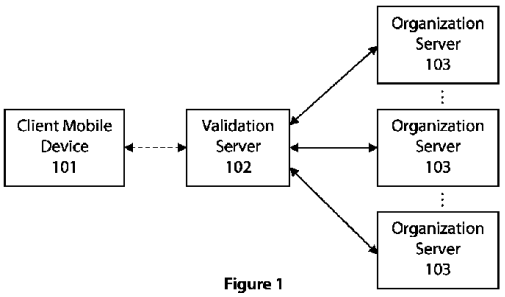


Figure 1

【特許請求の範囲】
【請求項１】
ユーザを認証する方法であって、
検証サーバで前記ユーザに対応する一意のユーザＩＤ番号および照合用暗号化キーを生成することと、
前記一意のユーザＩＤ番号および照合用暗号化キーをユーザ装置に送信することと、
前記ユーザ装置で前記暗号化キーに基づいて一時的アクセスコードを生成することと、
前記一意のユーザＩＤ番号および一時的アクセスコードを少なくとも１つの組織サーバに提供することと、
前記一意のユーザＩＤ番号および一時的アクセスコードを検証サーバに送信することと、
前記検証サーバで前記一意のユーザＩＤ番号および一時的アクセスコードの検証を実行して検証結果を得ることと、
前記少なくとも１つの組織サーバに前記検証結果を送信することと、
前記検証結果に基づいて前記少なくとも１つの組織で前記ユーザを認証することと、を含む、方法。
【請求項２】
前記一意のユーザＩＤ番号にマッチする前記暗号化キーを取得することと、第２のコードを前記一時的アクセスコードが生成されたときと同様に生成することと、前記第２のコードと前記一時的アクセスコードを比較して、肯定的検証結果または否定的検証結果の何れかを得ることと、をさらに含む、請求項１に記載の方法。
【請求項３】
前記少なくとも１つの組織サーバのクライアントデータベースを修正して、ユーザによる記録のため一意のユーザＩＤ番号用のフィールドを設けることをさらに含む、請求項１または請求項２に記載の方法。
【請求項４】
前記少なくとも１つの組織サーバから、前記ユーザ装置で動作可能なクライアントベースのセキュリティソフトウェアをダウンロードする命令を前記ユーザに提供することをさらに含む、請求項１～請求項３の何れか１項に記載の方法。
【請求項５】
前記検証サーバと前記ユーザ装置との時間同期を実行することをさらに含む、請求項１～請求項４の何れか１項に記載の方法。
【請求項６】
ユーザを認証するシステムであって、
前記ユーザにより操作可能であり、少なくとも１つのユーザ装置で動作可能なクライアントベースのセキュリティソフトウェアコンポーネントと、
少なくとも１つの検証サーバで動作可能なサーバベースの検証ソフトウェアコンポーネントと、
少なくとも１つのホスト組織サーバと、を備え、
前記サーバベースの検証ソフトウェアコンポーネントは、前記クライアントベースのセキュリティソフトウェアコンポーネントと通信して、前記少なくとも１つのユーザ装置上で前記ユーザに一意のユーザＩＤ番号および対応する暗号化キーを提供し、前記ホスト組織サーバは、認証要求を前記少なくとも１つの検証サーバに送信することによって、前記ユーザを認証し、前記サーバベースの検証ソフトウェアコンポーネントは、検証結果を生成する、システム。
【請求項７】
前記クライアントベースのセキュリティソフトウェアコンポーネントが、前記一意のユーザＩＤ番号および前記対応する暗号化キーに基づいて一時的アクセスコードを生成し、前記ユーザは、前記一意のユーザＩＤ番号および一時的アクセスコードを前記ホスト組織サーバに提供する、請求項６に記載のシステム。

【請求項８】
前記認証要求が、前記ユーザＩＤ番号および一時的アクセスコードを含む、請求項６または請求項７に記載のシステム。
【請求項９】
前記ホスト組織サーバが、前記サーバベースの検証ソフトウェアコンポーネントと通信する通信ソフトウェアコンポーネントを動作させる、請求項６～請求項８の何れか１項に記載のシステム。
【請求項１０】
前記少なくとも１つの装置が、前記クライアントベースのセキュリティソフトウェアコンポーネントを作動させるのに十分なコンピュータ計算および通信能力を備えたモバイル装置である、請求項６～請求項９の何れか１項に記載のシステム。
【請求項１１】
前記装置が、スマートフォン、タブレット型コンピュータ、ラップトップコンピュータ、個人用メディアプレーヤ、個人用娯楽用オーディオシステム、キオスクおよびスマートターミナルを含む前記群から選ばれる、請求項６～請求項１０の何れか１項に記載のシステム。
【請求項１２】
１つ以上のコンピュータ上で実行されるときに、コンピュータにユーザを認証する方法を遂行させる命令を記憶しているコンピュータ可読記憶媒体であって、前記方法は、
検証サーバで前記ユーザに対応する一意のユーザＩＤ番号および照合用暗号化キーを生成することと、
前記一意のユーザＩＤ番号および照合用暗号化キーをユーザ装置に送信することと、
前記ユーザ装置で前記暗号化キーに基づいて一時的アクセスコードを生成することと、
前記一意のユーザＩＤ番号および一時的アクセスコードを少なくとも１つの組織サーバに提供することと、
前記一意のユーザＩＤ番号および一時的アクセスコードを検証サーバに送信することと、
前記検証サーバで前記一意のユーザＩＤ番号および一時的アクセスコードの検証を実行して検証結果を得ることと、
前記少なくとも１つの組織サーバに前記検証結果を送信することと、
前記検証結果に基づいて前記少なくとも１つの組織で前記ユーザを認証することと、を含む、コンピュータ可読記憶媒体。
【請求項１３】
前記方法が、前記一意のユーザＩＤ番号にマッチする前記暗号化キーを取得することと、第２のコードを前記一時的アクセスコードが生成されたときと同様に生成することと、前記第２のコードと前記一時的アクセスコードを比較して、肯定的検証結果または否定的検証結果の何れかを得ることと、をさらに含む、請求項１２に記載のコンピュータ可読記憶媒体。
【請求項１４】
前記方法が、前記少なくとも１つの組織サーバのクライアントデータベースを修正して、ユーザによる記録のため一意のユーザＩＤ番号用のフィールドを設けることをさらに含む、請求項１２または請求項１３に記載のコンピュータ可読記憶媒体。
【請求項１５】
前記方法が、前記少なくとも１つの組織サーバから、前記ユーザ装置で動作可能なクライアントベースのセキュリティソフトウェアをダウンロードする命令を前記ユーザに提供することをさらに含む、請求項１２～請求項１４の何れか１項に記載のコンピュータ可読記憶媒体。
【発明の詳細な説明】
【技術分野】
【０００１】

【背景技術】

【０００２】

今日の世界では、仮想的かつ非個人的な方法を介した情報送信が、絶えず行なわれている。送信者または受信者は、送信データの大多数を機密的であると考えており、場合によっては、結果として不正にその情報を得ようとする試みが頻繁に行なわれることになるような重要性を有したものと考えている。これは、政府、企業および個人にとってますます深刻な懸念点になってきた。

【０００３】

今日、データ保護のために一般的に認められている方法は、遍在する「パスワード」、「パスフレーズ」、「ＰＩＮ」および多くの他の類似の手法である。パスワードは、保護すべきデータと一緒に、またはデータのそれぞれの所有者で管理されることが非常に多い。このような習慣またはユーザのその他の習慣は、パスワードベースのセキュリティ対策の大きな弱点となっている。

【発明の概要】

【発明が解決しようとする課題】

【０００４】

パスワードは、繰り返し送信されているデータの静的部分であり、すなわち、窃盗に対して容易な標的を示す。あるいは、システムがパスワードの頻繁な変更を求めることで、ユーザによる予測可能なパターン化、またはパスワードの忘却および喪失が助長され、これは、結果的に非効率性、さらには、パスワード回復措置費用の増加をもたらす。

【課題を解決するための手段】

【０００５】

本発明は、情報の守秘義務を維持し、従来型のパスワードセキュリティ手段の前述の短所に対処するユーザＩＤ用セキュリティシステムを提供する。より詳細には、本発明は、個人情報窃盗を防止するためのものであり、完全に安全で、暗号解読またはハッキングされることなく、その上、個人識別を必要とするいかなる状況での使用にもほぼ普遍的に適応可能なシステムを実現するものである。

【０００６】

本発明のシステムは、処理能力を備えた様々なハードウェアプラットホーム（例えばサーバコンピュータ、個人用コンピュータ、ラップトップ、携帯電話、個人用メディアプレーヤ、キオスク、ターミナル、飛行機、列車、船の個人用娯楽システムなど）で使用され得るが、好適な実施形態は、通常、ほとんどの時間または常時ユーザに保持されるモバイルコンピュータ装置（例えば個人用携帯電話）、およびユーザから遠く離れておよび少なくとも１つのホスト組織から遠く離れて位置する少なくとも１つのコンピュータサーバにおいて実施される。

【０００７】

本システムは、少なくとも１つの検証サーバにインストールおよび維持され、いかなるユーザまたはホスト組織からも独立している、サーバベースの検証ソフトウェアと、ユーザのモバイル装置にインストールされるクライアントベースのセキュリティソフトウェアと、任意選択で、少なくとも１つのホスト組織のサーバ（例えば法人サーバ、ウェブサイトサーバなど）で動作する通信ソフトウェアコンポーネントと、を備えている。用語「ユーザ」、「クライアント」および「顧客」は、以下の説明では同義的に使われている。ユーザは、一意のユーザＩＤ（識別）番号を、クライアントセキュリティソフトウェアコンポーネントを介して得ることによってシステムに登録する。この単一の非機密性のユーザＩＤ番号は、本発明のシステムを使用して機密保護コード識別機構を実施し、そのような

データの保全性を維持する任意の組織で共有され得る。いかなる個人ユーザ情報も要求されることは決してなく、ユーザがシステムに登録して使用するための時間および労力は、非常に少ない。

【０００８】

部分的にユーザＩＤ番号に基づき、クライアントセキュリティソフトウェアは、ユーザのモバイル装置で所定の時間間隔毎に生成される一時的アクセスコードをユーザに提供する。データにアクセスする方法（コンピュータ、キーパッドなど）に応じて、所有者は、検証のために組織にアクセス番号を送信する。所定の時間間隔が経過した後、一時的アクセスコードは失効し、新しい一時的アクセスコードが、生成される。ユーザおよび組織のどちらも、後成の一時的アクセスコードを予測する能力は持っていない。

【０００９】

この新規な検証の方法は、視覚識別が可能ではない仮想世界において理想的なものにし、これは、第１または第２の何れの検証においても使用することができる。

【００１０】

好ましい実施形態では、本発明は、処理能力を有するモバイル装置（例えば携帯電話、個人メディアプレーヤ）に、ダウンロード可能なクライアントセキュリティアプリケーションソフトウェアの形態で、少なくとも１つのサーバで動作可能なサーバ検証ソフトウェアとして、および任意選択で、少なくとも１つのホスト組織のサーバで動作可能な通信ソフトウェアコンポーネントとして提供されている。

【発明の効果】

【００１１】

有利なことに、個人的ユーザ情報をユーザが入力する必要はなく、個人情報は、クライアントセキュリティソフトウェアを動作させている装置内に保持されておらず、個人情報が、モバイル装置との間で送信されることがない。

【００１２】

本発明の別の利点として、いったん登録されると、クライアントセキュリティソフトウェアは、装置が、任意の組織のサーバへのネットワーク接続を維持する必要がない。すなわち、ユーザは、任意選択で通信ソフトウェアコンポーネントを動作させ、本発明の検証サーバと連通して検証サーバとクライアントモバイル装置の間で何ら情報が交換されることなく、いかなる参加組織に対しても認証することが可能である。さらなる利点として、クライアントセキュリティソフトウェアの１つの例は、関係性のない組織のサーバでの認証にも使用することができ、関係性のない組織のサーバ間で何ら情報が交換されることがない。

【００１３】

本発明のこの『汎用的な』機能は、ホストサイト間で情報を共有する必要なく、異なるホスト組織サイトおよび関係のないホスト組織サイトでの認証を可能にし、個人と組織とに同じようにきわめて低コストのセキュリティシステムを実現する。コストをさらに低減するため、本発明は、既存のソフトウェアインフラストラクチャおよびハードウェアインフラストラクチャを、ほとんどまたは全く修正せずに使用する。

【００１４】

このような利点およびその他の利点は、以下に記載する図および詳細説明により明白となるであろう。

【図面の簡単な説明】

【００１５】

【図１】本発明の一実施形態によるセキュリティシステムを示す例示的なブロック図である。

【図２】本発明の一実施形態によるユーザ登録プロセスを示す例示的なフローチャートである。

【図３】本発明の一実施形態によるユーザログインプロセスを示す例示的なフローチャートである。

【図４】本発明の一実施形態による、モバイル装置でのクライアントセキュリティソフトウェアを示す例示的な図である。
【図５】本発明の一実施形態による、モバイル装置でのクライアントセキュリティソフトウェアを示す例示的な図である。
【図６】本発明の一実施形態による、モバイル装置でのクライアントセキュリティソフトウェアを示す例示的な図である。
【図７】本発明の一実施形態による、モバイル装置でのクライアントセキュリティソフトウェアを示す例示的な図である。
【図８】本発明の一実施形態による、モバイル装置でのクライアントセキュリティソフトウェアを示す例示的な図である。
【図９】本発明の一実施形態による、モバイル装置でのクライアントセキュリティソフトウェアを示す例示的な図である。
【図１０】本発明の一実施形態による、モバイル装置でのクライアントセキュリティソフトウェアを示す例示的な図である。
【発明を実施するための形態】
【００１６】
本発明のさまざまな実施形態を、図を参照しながら詳述するが、図中の同一の参照符号は、いくつかの図を通じて類似の部品を示す。さまざまな実施形態に関する言及は、本発明の範囲を限定するものではなく、本発明の範囲は、添付の特許請求の範囲によってのみ限定される。さらに、本明細書に記載されているいかなる例も、制限することを目的としたものではなく、本願発明に関する多くの可能な実施形態のいくつかを記載しているにすぎない。
【００１７】
以下の説明は、当業者であれば本発明を実行し、使用することができるように提示されており、本発明の特殊用途との関連で提供されている。当業者であれば開示される実施形態に加えられるさまざまな修正は、容易に明白であり、本明細書において画定される一般原則は、本発明の範囲を逸脱することなく他の実施形態および応用例に適用することができる。さまざまな実施形態および例に関する言及は、本発明の範囲を限定するものではなく、本発明の範囲は、添付の特許請求の範囲によってのみ限定される。さらに、本明細書に記載されているいかなる例も、制限することを目的としたものではなく、本願発明に関する多くの可能な実施形態のいくつかを記載しているにすぎない。
【００１８】
本発明の本実施形態が実例として実行されるプログラム環境には、汎用コンピュータまたは携帯型コンピュータなどの特殊目的装置が含まれる。そのような装置（例えば、プロセッサ、メモリ、データ記憶、ディスプレイ）の詳細は、明瞭さを期するため、省略され得る。
【００１９】
さらに、本発明の技術は、さまざまな技術を用いて実施することができることを理解されたい。例えば、本明細書に記載される方法は、コンピュータシステムで動作するソフトウェアで実施することも、またはマイクロプロセッサまたは他の特別に設計された特定用途向け集積回路、プログラマブル論理デバイスの組み合わせ、またはさまざまなそれらの組み合わせの何れかを利用しているハードウェアで実施することができる。詳細には、本明細書において記載されている方法は、適切なコンピュータ可読媒体上にある一連のコンピュータ実行可能命令によって実施することができる。適切なコンピュータ可読媒体には、揮発性（例えば、ＲＡＭ）および／または不揮発性（例えば、ＲＯＭ、ディスク）メモリ、搬送波および送信媒体（例えば、銅線、同軸ケーブル、光ファイバ媒体）が含まれる。例示的な搬送波は、ローカルネットワーク、インターネットまたは何らかの他の通信リンクなどの公にアクセス可能なネットワークに沿ってデジタルデータストリームを伝達している、電気的、電磁的、または光学的信号という形態をとり得る。
【００２０】

したがって、一態様において、本発明は、ユーザを認証する方法を提供し、当該方法は、検証サーバでユーザに対応する一意のユーザＩＤ番号および照合用暗号化キーを生成することと、一意のユーザＩＤ番号および照合用暗号化キーをユーザ装置に送信することと、ユーザ装置で暗号化キーに基づいて一時的アクセスコードを生成することと、一意のユーザＩＤ番号および一時的アクセスコードを少なくとも１つの組織サーバに提供することと、一意のユーザＩＤ番号および一時的アクセスコードを検証サーバに送信することと、検証サーバで一意のユーザＩＤ番号および一時的アクセスコードの検証を実行して検証結果を得ることと、少なくとも１つの組織サーバに検証結果を送信することと、検証結果に基づいて少なくとも１つの組織でユーザを認証することと、を含む。本方法は、一意のユーザＩＤ番号にマッチする暗号化キーを取得することをさらに含んでいてもよく、第２のコードを一時的アクセスコードが生成されたときと同様に生成することと、第２のコードと一時的アクセスコードを比較して、肯定的検証結果または否定的検証結果の何れかを得ることと、をさらに含んでもよい。本方法は、少なくとも１つの組織サーバのクライアントデータベースを修正して、ユーザによる記録のため一意のユーザＩＤ番号用のフィールドを設けることをさらに含んでもよい。本方法は、少なくとも１つの組織サーバから、ユーザ装置で動作可能なクライアントベースのセキュリティソフトウェアをダウンロードする命令をユーザに提供することをさらに含んでもよい。本方法は、検証サーバとユーザ装置との時間同期を実行することをさらに含んでもよい。

【００２１】

別の態様では、本発明は、ユーザを認証するシステムを提供し、当該システムは、ユーザにより操作可能であり、少なくとも１つのユーザ装置で動作可能なクライアントベースのセキュリティソフトウェアコンポーネントと、少なくとも１つの検証サーバで動作可能なサーバベースの検証ソフトウェアコンポーネントと、少なくとも１つのホスト組織サーバと、を備え、サーバベースの検証ソフトウェアコンポーネントは、クライアントベースのセキュリティソフトウェアコンポーネントと通信して、少なくとも１つのユーザ装置上でユーザに一意のユーザＩＤ番号および対応する暗号化キーを提供し、ホスト組織サーバは、認証要求を少なくとも１つの検証サーバに送信することによって、ユーザを認証し、サーバベースの検証ソフトウェアコンポーネントは、検証結果を生成する。クライアントベースのセキュリティソフトウェアコンポーネントは、一意のユーザＩＤ番号および対応する暗号化キーに基づいて一時的アクセスコードを生成することができ、ユーザは、一意のユーザＩＤ番号および一時的アクセスコードをホスト組織サーバに提供する。認証要求は、ユーザＩＤ番号および一時的アクセスコードを含んでもよい。ホスト組織サーバは、サーバベースの検証ソフトウェアコンポーネントと通信する通信ソフトウェアコンポーネントを動作させることができる。少なくとも１つの装置は、クライアントベースのセキュリティソフトウェアコンポーネントを作動させるのに十分なコンピュータ計算および通信能力を備えたモバイル装置でもよい。さらに、装置は、スマートフォン、タブレット型コンピュータ、ラップトップコンピュータ、個人用メディアプレーヤ、個人用娯楽用オーディオシステム、キオスクおよびスマートターミナルを含む群から選ぶことができる。

【００２２】

ユーザＩＤ番号は、本発明のユーザごとに一意の識別子である。これは、ユーザまたはクライアントが、ユーザの識別性またはクライアントの識別性を保護するために本発明を使用する任意の組織と共有する必要がある唯一の数である。ユーザＩＤ番号は、ユーザによって機密扱いされる必要は無く、単独では、ユーザを特定することはできない。ユーザＩＤ番号が、モバイル装置を通じ、無線接続を介してインターネットへ取得されれば最も好ましく、これが、最も便利な方法である。好都合なことに、送信が必要なデータ量は、１ＭＢ未満と少なく、好ましくは１００ＫＢ未満、より好ましくは１０ＫＢ未満であれば、最も好ましくは１ＫＢ未満である。ユーザＩＤ番号は、任意のホスト組織から独立して維持される検証サーバから取得される。

【００２３】

本発明のクライアントセキュリティソフトウェアコンポーネントがモバイル装置にダウ

ンロードされ、ユーザが、検証サーバによってユーザＩＤ番号を割り当てられれば、識別システムが、無限数の組織またはユーザＩＤの申請に対して機能するようになる。好都合なことに、任意のホスト組織で通信ソフトウェアコンポーネントを動作させているサーバは、さまざまな組織のさまざまなサーバ間で何ら通信を求められることなく一意のユーザＩＤ番号を、検証サーバを介してユーザに提供することができる。

【００２４】

好都合なことに、ほとんどすべての場合、既存のハードウェアおよびソフトウェア（ユーザ用および組織用の両方）は、本発明を利用するのに十分である。本発明は、ユーザ情報またはデータに関する組織の内部データベースを置き換えるものではないことに留意されたい。むしろ、本発明の一時的アクセスコードを、従来型のパスワードまたはピン番号の代わりに使用することができる。しかし、他の従来型のセキュリティメソッドとは異なり、ユーザ定義可能情報を保護するためにすでに実施されている既存のセキュリティ対策以上に、ユーザＩＤ番号は、実施する何らかの追加的なセキュリティ対策（またはセキュリティソフトウェア）が実装されることを必要としない。このことは、実装の費用が代替セキュリティメソッドよりはるかに低いことから、本発明を利用するどのような組織にとっても大きな利点である。

【００２５】

当業者であれば理解されるように、本発明は、ホスト組織でなく、ユーザがセキュリティのキー態様を制御することを可能にする。すなわち、従来型のセキュリティでは、ホスト組織が、ユーザアクセス用のパラメータの全てを提供し、そうしたパラメータをユーザに付与する。本発明の場合、その逆の例もあり、ユーザが、ホスト組織にすべてのパラメータを提供する。セキュリティ上の大部分の攻撃は、個人ユーザではなく、ホスト組織のサーバに保管されているデータを対象としているので、これは、セキュリティに重要な利点を提供する。例えば、ユーザは、ユーザが望むのであればいつでも、どのような理由であっても新しいユーザＩＤ番号を要求することができる。例えば、ユーザは、彼の／彼女の古いユーザＩＤ番号が、危険に曝される（例えば、彼（女）らのモバイル装置が盗まれた、無くなった、および新しいものに取り換えられた）と思う場合もあり、あるいは、セキュリティの安心感を増すために定期的に数字を変更することを所望してもよい。新しいユーザＩＤの要求は、即時的かつ実用的であり、結果的にユーザまたはホスト組織を混乱させることはほとんどまたは全くない。好都合なことに、本発明のシステムおよび方法は、サーバからの認証プロセスと任意のパスワードを切り離し、ユーザデータおよび情報は、ホスト組織によって保管されている。

【００２６】

図１は、一実施形態による本発明のシステムを示す。詳細には、クライアントモバイル装置１０１が設けられており、これは、双方向の破線矢印で示すように、検証サーバ１０２とのみ通信して新しいユーザＩＤ番号および暗号化キーを取得する。１つ以上のホスト組織サーバ１０３は、クライアントモバイル装置１０１とではなく、検証サーバ１０２と通信して、後で詳しく述べるように、ホスト組織サーバ１０３への入力（例えば手動で）を行うユーザを確認および認証する。当業者であれば理解されるように、システムは、図１には図示されていないが、任意の数の検証サーバおよびクライアントモバイル装置を備えていてもよい。

【００２７】

別の実施形態では、図示しないが、検証サーバおよび組織サーバとが、共通であってもよい。すなわち、サーバベースの検証ソフトウェアコンポーネントは、ホスト組織のサーバで直接動作しても、またはホスト組織内の別のサーバで動作してもよい。容易に理解されるように、この代替の構成では、さまざまな組織間の連絡または連携が、一意のユーザＩＤ番号の相互接続を保証するのに必要となる。

【００２８】

図２および図３は、本発明の一実施形態による、ユーザ登録プロセスおよびユーザログインプロセスをそれぞれ示す例示的なフローチャートであり、以下に、インターネットを

介したホスト組織のウェブサイトへのユーザ認証に関して、説明する。

【００２９】

図２を参照すると、ホスト組織は、本発明のシステムを実施するために最初に登録を開始する（２０１）。ホスト組織は、顧客またはユーザ／クライアントごとのユーザＩＤ番号を保持するためにクライアントデータベースにフィールド（例えば長さ７バイトの）追加する（２０２）。ホスト組織は、ツールを提供して、一意のユーザＩＤ番号を組織のデータベースに記録し、さらに、ユーザのモバイル装置にクライアントセキュリティソフトウェアをダウンロードおよびインストールする場所および方法に関して、そのユーザに通知およびリンクを送る（２０３）。好ましくは、この通知は、ユーザへの電子メールである。さらに、ホスト組織は、ウェブサイトログインページを修正して、ユーザ認証に関して、従来のパスワードを使用するのか、または本発明のユーザＩＤ番号を使用するのかの選択を求める（２０４）。

【００３０】

ユーザは、提供されたリンクに従ってダウンロードを行い、クライアントセキュリティソフトウェアをユーザのモバイル装置にインストールする（２０６）。次に、ユーザは、モバイル装置をパスコードで保護し（２０７）、クライアントセキュリティソフトウェアをパスコードで保護して（２０８）、ユーザインストールおよび登録プロセスを完了させる。モバイル装置のパスワード保護は、任意選択であるが、特にモバイル装置が、（例えばスマートフォンへの電子メールにより）ホスト組織サーバからも通知を受信することが、最良の形態として推奨される。最終的に、ユーザは、後で詳しく述べるように、クライアントセキュリティソフトウェアを利用して一意のユーザＩＤ番号を取得し（２０９）、ユーザＩＤ番号をホスト組織のウェブサイト上のユーザ個人用プロファイルに提供する（２１０）。

【００３１】

サーバベースの検証ソフトウェアは、現在の日時を使用して一意のユーザＩＤ番号を作成する。好ましくは、この番号は、１６進数値として作成され、設定された桁数に短縮されることで、サーバベースの検証ソフトウェアおよびクライアントセキュリティソフトウェアのプロバイダのみが知る番号方式が作成される。次いで、ユーザＩＤ番号が、周知の暗号化技法を用いて暗号化され、好ましくは２５６ビット以上の有効な暗号化キーが生成される。ユーザＩＤ番号および暗号化キーの両方が、検証サーバから直接モバイル装置に送信される。好ましくは、ユーザＩＤ番号は、ユーザしか閲覧できない。

【００３２】

クライアントセキュリティソフトウェアは、上記のモバイル装置に付与された暗号化キーを使用して現在の日時を暗号化することで、一時的アクセスコードを生成する。計算結果は、好ましくは一連の算術演算（例えば加算と減算）によって修正され、好ましくは４桁から８桁の数字、最も好ましくは６桁の数字である、短縮された数が生成され、これは一時的アクセスコードである。

【００３３】

図３を参照すると、本発明の好適な実施形態のユーザ識別が示される。ホスト組織およびユーザは、共に上述のように登録を行なう（２２０、２２１）。ユーザは、まずクライアントセキュリティソフトウェアにパスコード（好ましくは、さらに、ユーザのモバイル装置を解除するための追加のパスコード）を入力する必要がある（２２２）。クライアントセキュリティソフトウェアは、一時的アクセスコードを生成および表示する（２２３）。ユーザは、別のコンピュータ装置上で、または同じモバイル装置自体でウェブブラウザを使用してホスト組織のウェブサイトログインページに進む（２２４）。

【００３４】

ホスト組織のウェブサイトログインページは、ユーザ認証に関して、従来のパスワードを使用するのか、または本発明のユーザＩＤ番号を使用するのかの選択を求める（２２５）。ユーザは、ユーザＩＤ番号認証を選び（２２６）、ユーザのモバイル装置のクライアントセキュリティソフトウェアに、ユーザによってホスト組織のウェブサイトログインペ

ージへ入力された一時的アクセスコードに関する情報を求める（２２７）。任意選択で、モバイル装置を用いてホスト組織のウェブサイトに進む場合、一時的アクセスコードが、ログインページに自動的に挿入され得る。

【００３５】

ホスト組織のウェブサイトサーバは、通信ソフトウェアコンポーネントを介して、確認および検証のため検証サーバに一時的アクセスコードおよびユーザＩＤ番号を送信する（２２８）。返信検証結果が、ホスト組織の通信ソフトウェアコンポーネントに提供され（２２９）、この結果に基づいて、ユーザは、ホスト組織のウェブサイトへのアクセスを許可される（２３０）、またはユーザは、がアクセスを拒否され（２３１）、一時的アクセスコードを再入力する必要が生じる（２２７）。段階２３１と段階２２７の再入力の間で十分な時間が経過した場合には、提供された一時的アクセスコードは、新しい数に変わっている。

【００３６】

サーバベースの検証ソフトウェアは、一時的アクセスコードおよびユーザＩＤ番号が提供されており、識別検証用クライアントセキュリティソフトウェアと同じ段階を実行する。すなわち、ユーザＩＤ番号を使用して、検証サーバが以前生成した対応する暗号化キーを調べる。次に、暗号化キーを使用して、コードが、現在の日時を用いて生成される。計算結果は、上で開示した同じ一連の算術演算によって修正され、短縮された数を形成し、次いで、この数が一時的アクセスコードと比較される。その結果得られる数が一時的アクセスコードと一致する場合には、検証サーバは、検証の確認をホスト組織のウェブサイトサーバ上の通信ソフトウェアコンポーネントに送信する。

【００３７】

残りの図（図４から図１０）には、モバイル装置で動作可能なクライアントセキュリティソフトウェアの本発明の好適な実施形態が記載されている。

【００３８】

メイン画面

図４を参照すると、モバイル装置１０１のクライアントセキュリティアプリケーションソフトウェアが示される。メイン画面は、好ましくは毎分１回の設定された時間間隔で更新される新しい一時的アクセスコード１００を示す。一時的アクセスコード１００は、数または英数字コードとして提供され得る。この時間間隔は、長くても短くてもよく、さらに可変でもよい。一時的アクセスコード１００は、モバイル装置で生成され、送信されず、モバイル装置１０１のみにローカルに保持される。クロック１１０は、時間間隔でカウントダウンし、図４では６０秒と示されている。クロック１１０で色が変化することで、一時的アクセスコード１００の失効時間が近いことをユーザに通知ことができる。例えば、緑－アンバー－赤の色彩設計が採用され得る。右側のソフトキー１３０を選択すると、オプションメニューが表示され、左のソフトキー１２０を選択すると、アプリケーションを終了することができる。

【００３９】

オプション

図５を参照すると、（１）ユーザＩＤを見る、（２）新しいユーザＩＤ、（３）ユーザＩＤを削除するおよび（４）時間を同期する、のオプション１３１がユーザに示される。モバイル装置１０１で所望のオプションを選択するには、オプションをスクロールし、ソフトキーメニュー１４０で『次』を選択する。

【００４０】

ユーザＩＤ番号の閲覧

図６を参照すると、「（１）ユーザＩＤを見る」が選択されて、ユーザＩＤ番号１５０が表示される。ユーザＩＤは、機密保持される必要はなく、ユーザまたはユーザのモバイル装置に関連していない。『完了』というソフトキー１４１を押すと、ユーザは、オプション１３１に戻る。

【００４１】

新しいユーザＩＤ番号の取得

図７を参照すると、確認１６０の後、モバイル装置１０１は、検証サーバから新しいユーザＩＤ番号１５０を取得する。ユーザＩＤ番号１５０は、モバイル装置１０１上に既に存在する場合には、上書きされる。メニュー１４２で『はい』を選択すると、ユーザＩＤ番号１５０が、検証サーバ（例えばインターネットへの無線接続）へのデータ接続を経てモバイル装置１０１にコピーされる。メニュー１４２で『いいえ』を選択すると、オプション１３１に戻る。データ接続にアクセスすることが許容される場合には、ユーザへの問い合わせを行なうことが可能である。これにより、ユーザが何らかの移動サービス料を最適化し、データ送信を確認することが可能になる。好都合なことに、送信が必要なデータ量は、１ＭＢ未満と少なく、好ましくは１００ＫＢ未満、より好ましくは１０ＫＢ未満、最も好ましくは１ＫＢ未満である。

【００４２】

図８を参照すると、新しいユーザＩＤ番号１５０がモバイル装置１０１にコピーされるときの、結果１７０の確認が示される。『ｏｋ』と示されたソフトキー１４３を押すと、ユーザはメイン画面に戻り、新しい一時的アクセスコート１００が表示される（図４参照）。ユーザは、オプションメニュー１３０に従って進み、オプション１３１下で「（１）ユーザＩＤを見る」を選択することで、新しいユーザＩＤ番号１５０を見ることができる。

【００４３】

新しいユーザＩＤ番号１５０を受信した後、ユーザは、自身の識別を希望することを任意の組織に提示しなければならない。同様に、その同じ組織が、同じユーザのファイルに以前のユーザＩＤ番号を持っていた場合には、新しいユーザＩＤ番号が取得されたことを、ユーザが通知しなければならない。

【００４４】

ユーザＩＤ番号の削除

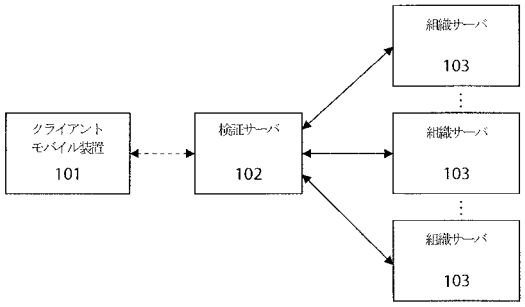
図９を参照すると、オプション１３１から「（３）ユーザＩＤを削除する」を選択すると、装置に保管されている任意のユーザＩＤ番号１５０が削除される。作業の確認１６１が、ユーザに示され、ソフトキーオプション１４４下で『はい』を選択すると、ユーザＩＤ番号が削除される。好ましいことに、ユーザＩＤ番号１５０の削除は、セキュリティを高めるために永続的であり、その結果、検索が不可能となり、新しいユーザＩＤ番号１５０のみが取得されるようになる。

【００４５】

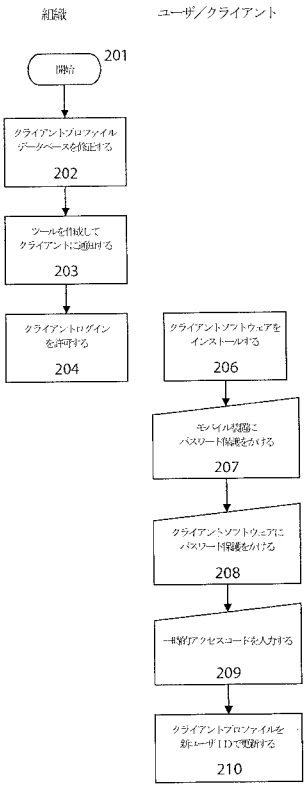
時間の同期

図１０を参照すると、オプション１３１から「（４）時間を同期する」を選択すると、確実に、一時的アクセスコード１００が、正確に検証されるようになる。時間同期は、サーバとモバイル装置１０１の間でデータ接続を介して実施される。作業の確認１６２が、ユーザに示され、ソフトキーオプション１４５下で『はい』を選択すると、時間を自動的に同期させる。データ接続にアクセスすることが許容される場合には、ユーザへの問い合わせを行なうことが可能である。ソフトキーオプション１４５下で『いいえ』を選択すると、ユーザは前の画面に戻る。この時間同期は、モバイル装置１０１自体のクロックとは無関係であり、本発明のクライアントアプリケーションソフトウェアに限定される。タイミング機構は、ユーザおよび組織から一様に見えなくなっており、このため、容易に暗号解読またはハッキングされることがないので、このことは有益である。

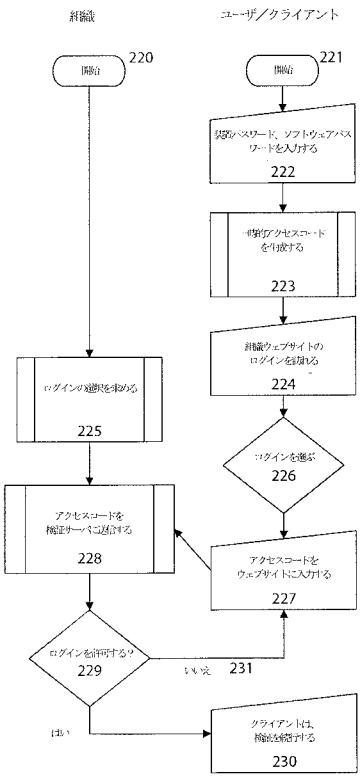
【図１】


クライアント
モバイル装置
101
検証サーバ
102
組織サーバ
103
組織サーバ
103
組織サーバ
103

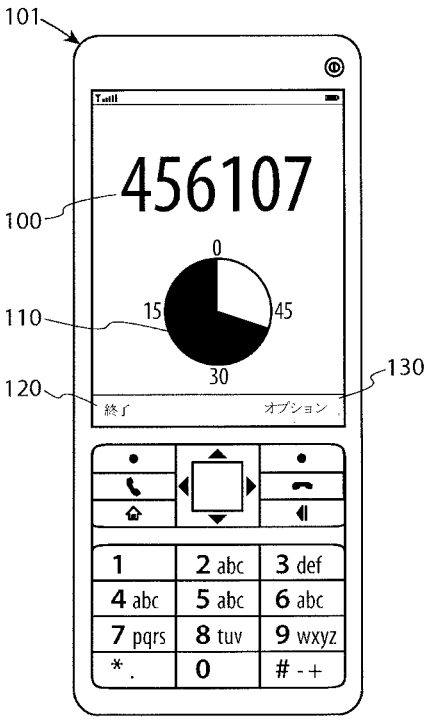
【図２】


組織
ユーザ／クライアント
開始
201
クライアントプロファイル
データベースを作成する
202
ツールを作成して
クライアントに通知する
203
クライアントログイン
を許可する
204
クライアントソフトウェアを
インストールする
206
モバイル装置に
パスワード保護をかける
207
クライアントソフトウェアに
パスワード保護をかける
208
一時的アクセスコードを入力する
209
クライアントプロファイルを
新ユーザIDで更新する
210

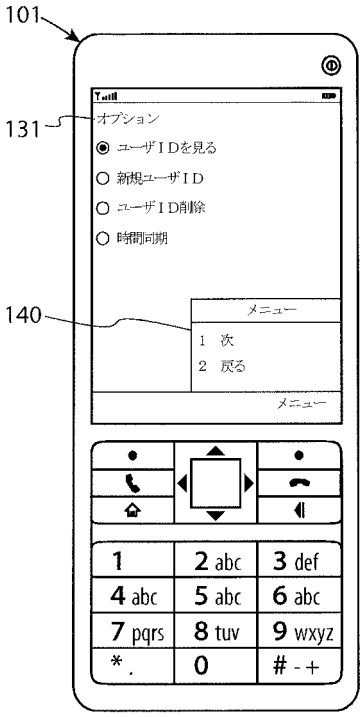
【図３】


組織
ユーザ／クライアント
開始
220
開始
221
装置パスワード、ソフトウェアパス
ワードを入力する
222
一時的アクセスコード
を作成する
223
組織ウェブサイトの
ログインを開く
224
ログインの選択を求める
225
ログインを選ぶ
226
アクセスコードを
検証サーバに通信する
228
アクセスコードを
ウェブサイトに入力する
227
ログインを許可する？
229
いいえ
231
はい
クライアントは、
検証を確定する
230

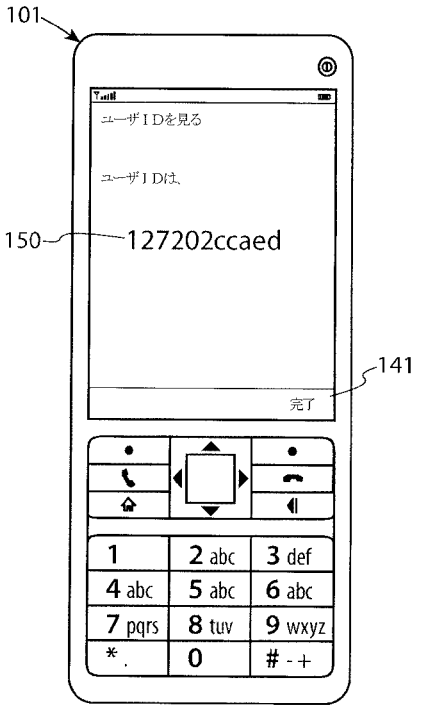
【図４】


101
100
110
120
130
456107
0
15
45
30
終了
オプション
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
- +

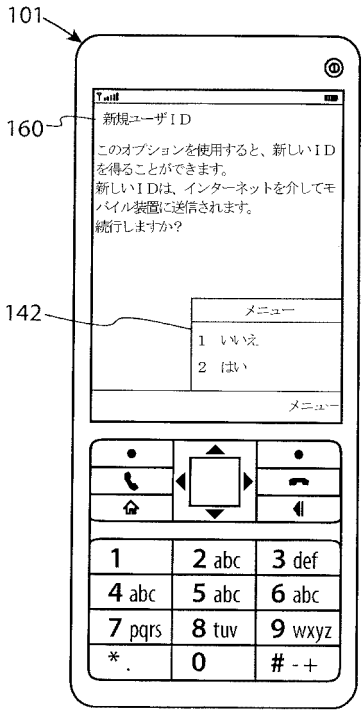
【図５】


101
131
オプション
ユーザＩＤを見る
新規ユーザＩＤ
ユーザＩＤ削除
時間同期
140
メニュー
1 次
2 戻る
メニュー
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
-+

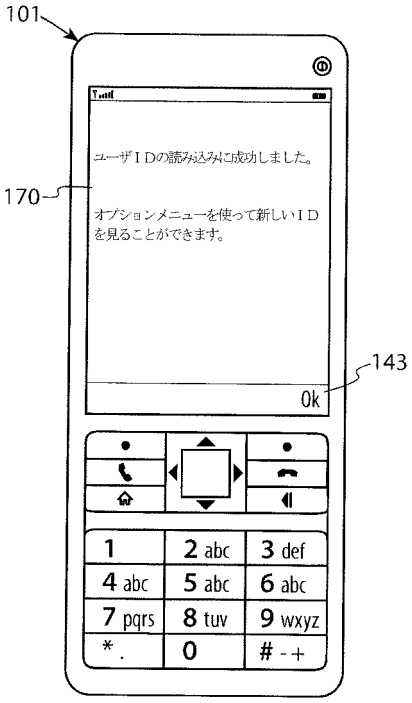
【図６】


101
ユーザＩＤを見る
ユーザＩＤは、
150
127202ccaed
141
完了
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
-+

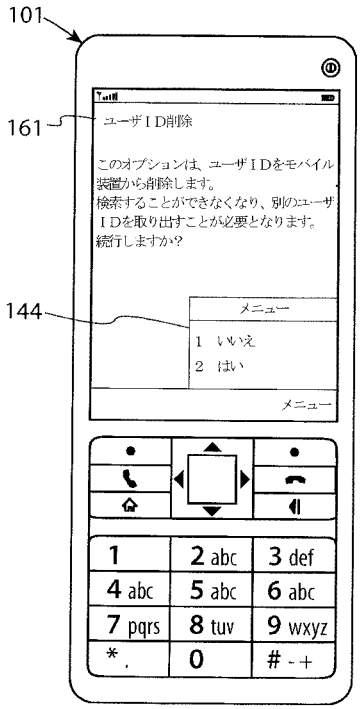
【図７】


101
160
新規ユーザＩＤ
このオプションを使用すると、新しいＩＤを得ることができます。
新しいＩＤは、インターネットを介してモバイル装置に送信されます。
続行しますか?
142
メニュー
1 いいえ
2 はい
メニュー
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
-+

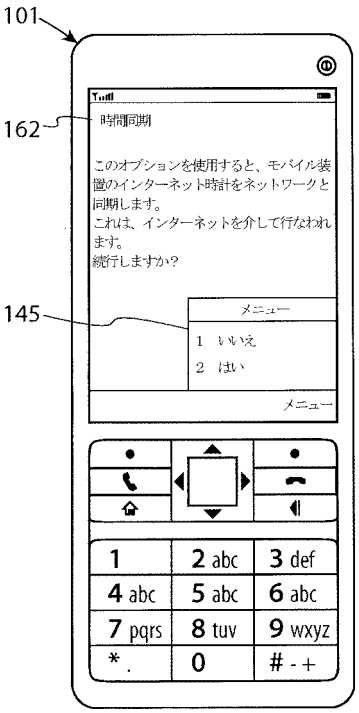
【図８】


101
ユーザＩＤの読み込みに成功しました。
170
オプションメニューを使って新しいＩＤを見ることができます。
143
Ok
1
2 abc
3 def
4 abc
5 abc
6 abc
7 pqrs
8 tuv
9 wxyz
*.
0
-+

【図９】



【図１０】



【手続補正書】
【提出日】平成26年7月28日(2014.7.28)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
コンピュータにより実施される、ユーザを認証する方法であって、
検証サーバで前記ユーザに対応する一意のユーザＩＤ番号および照合用暗号化キーを生成することと、
前記一意のユーザＩＤ番号および照合用暗号化キーをユーザ装置に送信することと、
前記ユーザ装置で前記暗号化キーに基づいて一時的アクセスコードを生成することと、
前記一意のユーザＩＤ番号および一時的アクセスコードを、独立ホスト組織によって個別に維持される、少なくとも１つのコンピュータ上で動作するように構成されている少なくとも１つの組織サーバに提供することと、
前記一意のユーザＩＤ番号および一時的アクセスコードを、前記少なくとも１つの組織サーバから前記検証サーバに送信することと、
前記一意のユーザＩＤ番号にマッチする前記暗号化キーを生成すること、および第２のコードを、前記一時的アクセスコードが生成されたのと同様に前記検証サーバ上に生成することと、
前記検証サーバで、前記第２のコードと前記一時的アクセスコードを比較することによって前記一意のユーザＩＤ番号および一時的アクセスコードの検証を実行して、検証結果を得ることと、

前記少なくとも１つの組織サーバに前記検証結果を送信することと、
前記検証結果に基づいて前記少なくとも１つの組織で前記ユーザを認証することと、を含み、
前記検証サーバは、前記独立ホスト組織およびそれらのそれぞれの組織サーバから独立して離れている第１の組織によって維持される、少なくとも１つのコンピュータ上で動作するように構成されており、
前記一意のユーザＩＤは、非機密的であり、前記独立ホスト組織のそれぞれと共有されている、方法。
【請求項２】
前記少なくとも１つの組織サーバのクライアントデータベースを修正して、ユーザによる記録のため一意のユーザＩＤ番号用のフィールドを設けることをさらに含む、請求項１に記載の方法。
【請求項３】
前記少なくとも１つの組織サーバから、前記ユーザ装置で動作可能なクライアントベースのセキュリティソフトウェアをダウンロードする命令を前記ユーザに提供することをさらに含む、請求項１に記載の方法。
【請求項４】
前記検証サーバと前記ユーザ装置との時間同期を実行することをさらに含む、請求項１に記載の方法。
【請求項５】
（以前に提示されたもの）
ユーザを認証するコンピュータシステムであって、
前記ユーザにより操作可能であり、少なくとも１つのユーザ装置で動作可能なクライアントベースのセキュリティソフトウェアコンポーネントと、
第１の組織によって維持される、少なくとも１つのコンピュータ上で動作するように構成されている少なくとも１つの検証サーバで動作可能なサーバベースの検証ソフトウェアコンポーネントと、
独立ホスト組織によって個別に維持される、少なくとも１つのコンピュータ上で動作するように構成されている少なくとも１つのホスト組織サーバと、を備え、
前記サーバベースの検証ソフトウェアコンポーネントは、前記クライアントベースのセキュリティソフトウェアコンポーネントと通信して、前記少なくとも１つのユーザ装置上で前記ユーザに一意のユーザＩＤ番号および対応する暗号化キーを提供し、
前記クライアントベースのセキュリティソフトウェアコンポーネントは、前記一意のユーザＩＤ番号および前記対応する暗号化キーに基づいて一時的アクセスコードを生成し、
前記ユーザは、前記一意のユーザＩＤ番号および一時的アクセスコードを前記少なくとも１つのホスト組織サーバに提供し、
前記少なくとも１つのホスト組織サーバは、前記ユーザＩＤ番号および一時的アクセスコードを備えている認証要求を前記少なくとも１つの検証サーバに送信することによって、前記ユーザを認証し、
前記サーバベースの検証ソフトウェアコンポーネントは、前記一意のユーザＩＤ番号にマッチする前記暗号化キーを生成し、第２のコードを、前記一時的アクセスコードが生成されたのと同様に前記検証サーバ上に生成し、
前記サーバベースの検証ソフトウェアコンポーネントは、前記第２のコードと前記一時的アクセスコードを比較することから、検証結果を生成し、
前記検証結果は、前記検証サーバから前記少なくとも１つのホスト組織サーバに送信され、
前記第１の組織によって維持される前記少なくとも１つのコンピュータは、前記独立ホスト組織およびそれらのそれぞれの組織サーバから独立して離れており、
前記一意のユーザＩＤは、非機密的であり、前記独立ホスト組織のそれぞれおよびそれらのそれぞれのホスト組織サーバと共有されている、システム。

【請求項６】
前記ホスト組織サーバが、前記サーバベースの検証ソフトウェアコンポーネントと通信する通信ソフトウェアコンポーネントを動作させる、請求項５に記載のシステム。
【請求項７】
前記少なくとも１つの装置が、前記クライアントベースのセキュリティソフトウェアコンポーネントを作動させるのに十分なコンピュータ計算および通信能力を備えたモバイル装置である、請求項５に記載のシステム。
【請求項８】
前記装置が、スマートフォン、タブレット型コンピュータ、ラップトップコンピュータ、個人用メディアプレーヤ、個人用娯楽用オーディオシステム、キオスクおよびスマートターミナルを含む前記群から選ばれる、請求項５に記載のシステム。
【請求項９】
１つ以上のコンピュータ上で実行されるときに、コンピュータにユーザを認証する方法を遂行させる命令を記憶している非一時的コンピュータ可読メモリであって、前記方法は、
検証サーバで前記ユーザに対応する一意のユーザＩＤ番号および照合用暗号化キーを生成することと、
前記一意のユーザＩＤ番号および照合用暗号化キーをユーザ装置に送信することと、
前記ユーザ装置で前記暗号化キーに基づいて一時的アクセスコードを生成することと、
前記一意のユーザＩＤ番号および一時的アクセスコードを、独立ホスト組織によって個別に維持される、少なくとも１つのコンピュータ上で動作するように構成されている少なくとも１つの組織サーバに提供することと、
前記一意のユーザＩＤ番号および一時的アクセスコードを、前記少なくとも１つの組織サーバから前記検証サーバに送信することと、
前記一意のユーザＩＤ番号にマッチする前記暗号化キーを生成すること、および第２のコードを、前記一時的アクセスコードが生成されたのと同様に前記検証サーバ上に生成することと、
前記検証サーバで、前記第２のコードと前記一時的アクセスコードを比較することによって前記一意のユーザＩＤ番号および一時的アクセスコードの検証を実行して、検証結果を得ることと、
前記少なくとも１つの組織サーバに前記検証結果を送信することと、
前記検証結果に基づいて前記少なくとも１つの組織で前記ユーザを認証することと、を含み、
前記検証サーバは、前記独立ホスト組織およびそれらのそれぞれの組織サーバから独立して離れている第１の組織によって維持される、少なくとも１つのコンピュータ上で動作するように構成されており、
前記一意のユーザＩＤは、非機密的であり、前記独立ホスト組織のそれぞれと共有されている、非一時的コンピュータ可読メモリ。
【請求項１０】
前記方法が、前記少なくとも１つの組織サーバのクライアントデータベースを修正して、ユーザによる記録のため一意のユーザＩＤ番号用のフィールドを設けることをさらに含む、請求項９に記載の非一時的コンピュータ可読メモリ。
【請求項１１】
前記方法が、前記少なくとも１つの組織サーバから、前記ユーザ装置で動作可能なクライアントベースのセキュリティソフトウェアをダウンロードする命令を前記ユーザに提供することをさらに含む、請求項９に記載の非一時的コンピュータ可読メモリ。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CA2012/050661

A. CLASSIFICATION OF SUBJECT MATTER
IPC: ***H04L 9/32*** (2006.01) , ***H04L 9/08*** (2006.01) , *H04W 12/06* (2009.01)
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC: ***H04L*** (2006.01), ***H04W*** (2006.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic database(s) consulted during the international search (name of database(s) and, where practicable, search terms used)
Canadian Patent Database, TotalPatent, IEEExplore, Google
Keywords: one-time password, OTP, access code, ID, mobile, validat*, two factor authentication, 2FA, authenticat*, application, pin, server

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y	US 2007/0130463 A1 (LAW et al.), 7 June 2007 (07-06-2007) see para. [0035], [0036], [0038], [0041], [0043-0048], [0050], [0052], [0056], [0061] and [0062]	1, 3, 6-12 and 14 2, 4, 5, 13 and 15
Y	US 2011/0197266 A1 (CHU et al.), 11 August 2011 (11-08-2011) see para. [0012], [0013] and [0036]	2, 4, 5, 13 and 15
A	WO 2009/018564 A1 (ASHBY), 5 February 2009 (05-02-2009) see entire document	1-15
A	WO 2007/102823 A1 (FOT et al.), 13 September 2007 (13-09-2007) see entire document	1-15
A	US 2011/0162054 A1 (SAXENA et al.), 30 June 2011 (30-06-2011) see entire document	1-15

[ ] Further documents are listed in the continuation of Box C. [X] See patent family annex.

* Special categories of cited documents :
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 March 2013 (26-03-2013)	02 April 2013 (02-04-2013)

Name and mailing address of the ISA/CA	Authorized officer
Canadian Intellectual Property Office Place du Portage I, C114 - 1st Floor, Box PCT 50 Victoria Street Gatineau, Quebec K1A 0C9 Facsimile No.: 001-819-953-2476	Jamie Hayami (819) 934-2670

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CA2012/050661

Patent Document Cited in Search Report	Publication Date	Patent Family Member(s)	Publication Date
US2007130463A1	07 June 2007 (07-06-2007)	TW200802025A	01 January 2008 (01-01-2008)
		US2007125838A1	07 June 2007 (07-06-2007)
		US2007125840A1	07 June 2007 (07-06-2007)
		WO2007067349A1	14 June 2007 (14-06-2007)
		WO2007067350A1	14 June 2007 (14-06-2007)
		WO2007067351A1	14 June 2007 (14-06-2007)
US2011197266A1	11 August 2011 (11-08-2011)	US7904946B1	08 March 2011 (08-03-2011)
WO2009018564A1	05 February 2009 (05-02-2009)	US2009172795A1	02 July 2009 (02-07-2009)
		US8296834B2	23 October 2012 (23-10-2012)
WO2007102823A1	13 September 2007 (13-09-2007)	BRPI0621455A2	13 December 2011 (13-12-2011)
		CN101427510A	06 May 2009 (06-05-2009)
		CN101427510B	11 May 2011 (11-05-2011)
		EP1997270A1	03 December 2008 (03-12-2008)
		MX2008011277A	25 November 2008 (25-11-2008)
		US2011314290A1	22 December 2011 (22-12-2011)
		US8261087B2	04 September 2012 (04-09-2012)
US2011162054A1	30 June 2011 (30-06-2011)	None	

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC

(72)発明者 ベル，ジョナサン ジー.
カナダ国、ブイ７ティー １ビー８、ブリティッシュ コロンビア州、ウエスト バンクーバー、５１８－１４８９ マリン ドライブ，キネシス アイデンティティ セキュリティ システム インコーポレーテッド
(72)発明者 ジェニングス，ケニス ダブリュー.
カナダ国、ブイ７ティー １ビー８、ブリティッシュ コロンビア州、ウエスト バンクーバー、５１８－１４８９ マリン ドライブ，キネシス アイデンティティ セキュリティ システム インコーポレーテッド

Ｆターム(参考) 5J104 AA07 AA16 AA32 AA41 EA04 EA08 JA03 KA01 KA04 KA21
MA01 NA02 NA36 NA38 PA07