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

特許第6105721号
(P6105721)

(45)発行日　平成29年3月29日(2017.3.29)　(24)登録日　平成29年3月10日(2017.3.10)

(51)Int.Cl.		F I		
G06F 21/33	(2013.01)	G06F	21/33	
G06F 21/64	(2013.01)	G06F	21/64	
H04M 11/00	(2006.01)	H04M	11/00	302

請求項の数 8　(全 33 頁)

(21)出願番号	特願2015-516018(P2015-516018)
(86)(22)出願日	平成25年5月6日(2013.5.6)
(65)公表番号	特表2015-528149(P2015-528149A)
(43)公表日	平成27年9月24日(2015.9.24)
(86)国際出願番号	PCT/US2013/039664
(87)国際公開番号	WO2013/184265
(87)国際公開日	平成25年12月12日(2013.12.12)
審査請求日	平成27年2月6日(2015.2.6)
(31)優先権主張番号	13/490,677
(32)優先日	平成24年6月7日(2012.6.7)
(33)優先権主張国	米国(US)

(73)特許権者　512193230
オーセンティファイ・インク
ＡＵＴＨＥＮＴＩＦＹ　ＩＮＣ.
アメリカ合衆国　６０６３１　イリノイ州　シカゴ　ウェスト・ヒギンズ・ロード　８７４５番地　２４０号
(74)代理人　100126675
弁理士　福本　将彦
(72)発明者　ピーター・ジョージ・タプリング
アメリカ合衆国　６００６８　イリノイ州　パーク・リッジ　ノース・ディー・ロード　１５００番地

最終頁に続く

(54)【発明の名称】企業トリガ式２ＣＨＫ関連付けの起動

(57)【特許請求の範囲】

【請求項１】

ネットワークを介するユーザと企業との間の商取引を安全に処理するようにセキュリティサーバを動作させる方法であって、

前記セキュリティサーバが、前記ネットワークを介して、現在において前記ユーザが前記ネットワークを介して認証されている企業の企業ネットワークサイトであって、かつ現在において前記ユーザのユーザ・ネットワーク・デバイスが前記ネットワークを介して接続されている企業ネットワークサイトから、前記ユーザ・ネットワーク・デバイスと前記セキュリティサーバとの間に前記ネットワーク上で安全な通信チャネルを起動するという前記企業の要求を受信することであって、前記ネットワーク以外を介して前記ユーザに接触するための連絡先情報を含む要求を、受信することと、

前記セキュリティサーバが、前記受信された起動要求に応答して、前記ネットワーク以外を介するとともに前記受信された連絡先情報に対応する、前記ユーザへの配信のために、起動コードを送信することと、

前記セキュリティサーバが、前記ユーザ・ネットワーク・デバイスから前記ネットワークを介して起動コードを受信することと、

前記セキュリティサーバが、前記受信された起動コードを前記送信された起動コードと比較して前記受信された起動コードを検証することと、

前記セキュリティサーバが、前記受信された起動コードの前記検証に基づいて、前記安全な通信チャネルを起動することと、を含む方法。

【請求項２】
セキュリティサーバが、前記ネットワークを介して、前記企業の識別子と、前記ユーザが前記企業を相手に始めることを希望するトランザクションの詳細とを含むトランザクション情報を受信することと、
前記セキュリティサーバが、前記受信されたトランザクション情報を、前記ユーザ・ネットワーク・デバイスへ前記安全な通信チャネルを介して送信することと、をさらに含む、請求項１に記載の方法。
【請求項３】
前記トランザクションへの有効なユーザ署名が前記企業ネットワークサイトによって要求され、
前記方法は、
前記セキュリティサーバが、前記受信されたトランザクション情報に基づいて、前記ユーザがトランザクション署名として用いるためのワンタイムパスワードを生成することと、
前記セキュリティサーバが、前記生成されたワンタイムパスワードを、前記安全な通信チャネルを介して前記ユーザ・ネットワーク・デバイスへ送信することと、をさらに含む、請求項２に記載の方法。
【請求項４】
ワンタイムパスワードは、前記セキュリティサーバおよび前記企業により共有されるが前記ユーザには知られておらず、かついかなる特定のユーザにも関連づけられていない秘密にも基づいて生成される、請求項３に記載の方法。
【請求項５】
前記企業は、第１の企業であり、前記トランザクション情報は、第１のトランザクション情報であり、
前記方法は、
前記セキュリティサーバが、前記ネットワークを介して、第２の企業の識別子と、前記ユーザが前記第２の企業を相手に始めることを希望する第２のトランザクションの詳細とを含む第２のトランザクション情報を受信することと、
前記セキュリティサーバが、受信された前記第２のトランザクション情報を、前記ユーザ・ネットワーク・デバイスへ前記安全な通信チャネルを介して送信することと、をさらに含む、請求項２に記載の方法。
【請求項６】
前記第２の企業の企業ネットワークサイトによって前記第２のトランザクションへの有効なユーザ署名が要求され、
前記方法は、
前記セキュリティサーバが、前記受信された第２のトランザクション情報に基づいて、前記ユーザによりトランザクション署名として使用されるための他のワンタイムパスワードを生成することと、
前記セキュリティサーバが、前記生成された他のワンタイムパスワードを、前記安全な通信チャネルを介して前記ユーザ・ネットワーク・デバイスへ送信することと、
前記セキュリティサーバが、前記ネットワークを介して前記第２の企業の前記企業ネットワークサイトから、前記有効に署名されたトランザクションを前記第２の企業の前記企業ネットワークサイトが前記ユーザ・ネットワーク・デバイスから受信したことの確認を受信することと、
前記セキュリティサーバが、前記安全な通信チャネルを介して前記ユーザ・ネットワーク・デバイスへ、前記第２の企業の前記企業ネットワークサイトが前記有効に署名されたトランザクションを受信したことの確認を送信することと、をさらに含む、請求項５に記載の方法。
【請求項７】
前記セキュリティサーバが、前記受信されたトランザクション情報を音声ストリームお

よび画像のうちの少なくとも一方へ組み込むことをさらに含み、前記送信されるトランザクション情報は、前記音声ストリームおよび前記画像のうちの前記少なくとも一方へ組み込まれた前記トランザクション情報である、請求項２に記載の方法。
【請求項８】
前記音声ストリームは、前記ユーザによる認識が可能な音声を有する音声ストリームであり、かつ前記画像は、前記ユーザが知るところの背景を有する画像である、請求項７に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セキュリティおよびプライバシに関する。より具体的には、本発明は、デスクトップおよび／またはラップトップコンピュータと互換性のあるハードウェア・プラグイン・デバイス、および／またはＡｐｐｌｅ　ｉＰｈｏｎｅｓ（商標）等のスマートモバイル通信デバイスを用いる、ウェブベースの署名を含むウェブベースのログインおよびトランザクション認証に関する。
【背景技術】
【０００２】
パスワード、ワンタイムパスワード（ＯＴＰ）、ハードウェアまたはソフトウェアスマートカード、他の技術を用いるユーザ認証は、全て、弱体に過ぎており、中間者（ＭＩＴＭ）攻撃またはマンインザブラウザ（ＭＩＴＢ）攻撃を受けやすいことが分かっているか、そうでなくとも扱いにくく高価すぎることが分かっている。ＯｐｅｎＩＤ、ＦａｃｅＢｏｏｋ　Ｃｏｎｎｅｃｔ、他等の技術に単一の署名を使用することは、攻撃者が、一旦マスターアカウントに不正侵入すると、次にはこの初回ログインに依存する他の全てのアカウントへ侵入できることから、問題を悪化させるだけである。さらに、攻撃者の焦点は、ログイン処理を破壊することから、高度な技術を用いて、ログイン行為後に侵入し、実行されているトランザクションを攻撃することへと移行している。これにより、トランザクション認証、即ちバックエンドのウェブサーバにおいて検分されるトランザクションがユーザの意図するものと同一であるかどうかを確認する行為、がますます重要となっている。
【０００３】
帯域外認証（ＯＯＢＡ）、即ちユーザへトランザクションを中継し、かつ代替形式の通信、例えば音声電話呼またはテキストメッセージの送信を用いて確認を得る技術は、有望な代替技術であるが、同じく頻繁に用いるには不便かつ高価すぎる。これは、極めて重要なトランザクションまたはパスワードの再設定のようなめったにない事象には有用である場合もあるが、大量のトランザクションに用いるには高価かつ煩雑すぎる。
【０００４】
最近では、これらの問題点のうちの幾つかに対処する革新的な新しい認証システムおよびプロトコルが開発されている。具体的には、一般に「２ＣＨＫ」と称されるシステムおよびプロトコルは、ユーザに、ウェブサイトへログインできるようにする（即ち、ウェブサイトに対するユーザの認証）、または、ウェブサイトとセキュリティサーバとの間で共有される秘密に基づいて、入力されたトランザクションにウェブサイトで電子的に署名できるようにするためのＯＴＰを提供することができる。特に有用である点は、２ＣＨＫは、ワンタイムパスワードによる安全性を提供するが、先行する全てのＯＴＰシステムおよびプロトコルが要求しているユーザ毎の共有秘密鍵を要求しない、という事実にある。
【０００５】
ユーザが商業者、銀行またはブローカのウェブサイト等の電子商取引ウェブサイトを閲覧する場合、ユーザがＰａｙＰａｌにより提供されるもの等の支払ボタンを目にすることは一般的である。ユーザがこの支払い機能をクリックすると、ユーザは、典型的には、支払いプロバイダと直接に双方向通信している。これは、ユーザは、支払いプロバイダに対して自らを認証するための認証情報を電子商取引サイトへは漏らさないことを意味する。

これは、ユーザが、ウェブサイトが提供するスマートフォンアプリを用いて電子商取引サイトと双方向通信しているときには、もはや利用できない重要な特徴である。したがって、２ＣＨＫは、バックエンドの認証サーバへの独立した安全な通信チャネルを有する、一般に「２ＣＨＫクライアント」と称される別の安全なクライアントアプリケーションを用いて実現することが可能である。２ＣＨＫクライアントは、コンピュータ装置上の専用ソフトウェアとして、またはブラウザをベースにしたアプリケーションとして、またはＩＰｈｏｎｅ等のスマートフォンを含む移動体通信デバイス上のアプリケーションとして実現することが可能である。

【０００６】

例えば、２ＣＨＫクライアントは、ユーザにトランザクションを知らせる、ユーザがトランザクションを追認／拒否できるようにする、かつ／またはユーザに、ユーザが商業者または銀行のウェブサイトアプリケーション等の他のアプリケーションにおいてトランザクションを承認するために使用できるトランザクション署名、即ちＯＴＰ、を提供する、の何れかを目的として、ユーザトランザクションを示すために使用されることが可能である。さらに、２ＣＨＫクライアントは、ユーザに、異なるウェブサイトまたは他のアプリケーションへログインするために使用できるＯＴＰを提供することもできる。実現の仕方に依存して、２ＣＨＫは、このようなＯＴＰを生成するための２つの別個の方法のうちの何れかを用いることができる。その一方では、ＯＴＰは、認証サーバによって提供され、もう一方では、２ＣＨＫクライアントが起動中に「シード付与」され、それによって、これは次に、バックエンド認証サーバとは如何なるつながりも無しでＯＴＰを生成することができる。

【０００７】

大量のスマートフォンによって、結果的に、様々なインタフェースを用いてスマートフォンへ取り付けることができる補助的なハードウェア品のマーケットが到来している。ＵＳＢポートおよび／またはケーブルを用いてコンピュータへプリンタを接続できることに酷似して、スマートフォンへも、例えばどこにでもあるヘッドフォンジャックを用いてデバイスを接続することができる。したがって、２ＣＨＫクライアントは、このような補助的ハードウェア上で実行されるように、かつこれにより、スマートモバイル通信デバイスと互換性のあるプラグインハードウェアおよびインターネット接続可能パーソナル・コンピュータ装置を用いて効率的かつ安全なログイン認証およびトランザクション承認を提供するように適合化されている。

【発明の概要】

【発明が解決しようとする課題】

【０００８】

本発明は、補助的ハードウェアを用いて実現する形態を含む、パーソナル・コンピュータ装置およびｉＰｈｏｎｅおよびｉＰａｄ等のスマートモバイル通信デバイス上での２ＣＨＫログイン認証および／またはトランザクション承認の実現において追加的な柔軟性を提供することができる、２ＣＨＫシステムおよびプロトコルのさらなる改良、および／または攻撃者に対する保護の強化に関する。

【０００９】

当業者には、本発明の追加の目的、優位点、新規特徴が、以下の詳細な説明を含む本開示からだけでなく、本発明の実施によっても明らかとなるであろう。以下、本発明を１つまたは複数の好適な実施形態を参照して説明するが、本発明がこれらに限定されないことは理解されるべきである。本明細書における教示を閲覧できる一般的な当業者には、本明細書に開示されかつクレームに記載されている発明の範囲に含まれる、かつ本発明が重要な有用性を有する可能性がある追加的な実施、変更および具現化ならびに他の利用分野が認識されるであろう。

【課題を解決するための手段】

【００１０】

本発明の態様によれば、セキュリティサーバは、インターネット等のネットワークを介

するユーザと企業との間の商取引を安全に処理するように動作させることが可能である。その実行に際して、セキュリティサーバは、ネットワークを介して、現在においてユーザがネットワークを介して接続されている企業から、ユーザとセキュリティサーバとの間にネットワーク上で安全な通信チャネルを起動するという企業側の要求を受信する。要求は、電話番号または携帯電話番号、メールアドレスまたは他の連絡先情報等の、ネットワーク以外でユーザに接触するための連絡先情報を含む。ユーザがネットワーク上で、典型的には、パーソナルコンピュータ、スマートフォンまたはスマートパッド等のユーザ・ネットワーク・デバイスによって代表され、かつ企業がネットワーク上で、典型的には、ウェブサイトサーバ等のネットワークサイトによって代表されることは認識されるであろう。

【００１１】

受信された起動要求に応答して、セキュリティサーバは、ネットワーク以外を介するとともに受信された連絡先情報に対応する、ユーザへの配信のために、起動コードを送信する。例えば、起動コードは、情報の配信に公衆交換電話網または携帯電話網を用いる帯域外認証事業者へ送信される場合もある。このような事業者は、好ましくは、ネットワーク上に代表されるものであるが、必須ではない。一方で、起動コードは、ユーザに手渡しする、または直接聴覚的に配信するために、任意数の方法で郵便事業者、民間宅配便業者またはメッセンジャーサービス業者へ送られる場合もあり、この場合、これらの事業者は、承認コードをユーザに、例えばインターネットであるネットワーク以外で配信することから、帯域外配信事業者となる。

【００１２】

次に、セキュリティサーバは、ユーザからネットワークを介して起動コードを受信し、受信された起動コードを検証するために、受信された起動コードを送信された起動コードと比較する。比較に基づいて起動コードが検証されると、セキュリティサーバは、セキュリティサーバとユーザとの間の安全な通信チャネルの起動をもする。例えば、これに続くユーザとセキュリティサーバとの間の通信は全て、起動コードに基づいて対称暗号鍵で暗号化されてもよいが、これは、この時点でユーザおよびセキュリティサーバの双方がこのコードを知っていることに起因する。

【００１３】

本発明の別の態様によれば、セキュリティサーバは、ネットワークを介して、企業の識別子と、ユーザがその企業を相手に始めることを希望するトランザクションの詳細とを含むトランザクション情報を受信する。トランザクションが事実上任意のタイプであり得ることは、理解されるであろう。インターネット等のネットワーク上で実行される一般的なトランザクションには、口座からの送金、株式または債券の購入および製品またはサービスの購入が含まれるが、これらに限定されない。このようなトランザクションのトランザクション詳細には、典型的には、口座番号、製品コード、送金される、または支払われる金額、およびトランザクションを明確に詳述するために適切と見なされる他の情報といった項目が含まれ、よって、後にユーザと企業との間にユーザが承認した内容に関する紛争は生じない。セキュリティサーバは、受信されたトランザクション情報をユーザへ安全な通信チャネルを介して送信する。トランザクションへの有効なユーザ署名が企業によって要求されると、セキュリティサーバは、受信されたトランザクション情報に基づいて、ユーザがトランザクション署名として用いるためのワンタイムパスワードを生成し、かつ生成されたワンタイムパスワードをセキュリティサーバから安全な通信チャネルを介してユーザへ送信する。ワンタイムパスワードは、好ましくは、セキュリティサーバおよび企業により共有されるがユーザには知られておらず、いかなる特定のユーザにも関連づけられていない秘密にも基づいて生成される。何れにしても、セキュリティサーバは、ネットワークを介して企業から、ユーザからの有効に署名されたトランザクションの企業による受信確認を受信する可能性もあるが、通常は受信しない。しかしながら、ワンタイムパスワードがユーザへ送信された後、ユーザは、セキュリティサーバから受信されたワンタイムパスワードを企業へ、好ましくはネットワークを介して送信する。

【００１４】

本発明のさらに他の態様によれば、この同じ安全な通信チャネルは、ユーザと様々な異なる企業との間のトランザクションに使用されることが可能である。したがって、セキュリティサーバは、ネットワークを介して、他の企業の識別子、およびユーザがこの他の企業と始めることを希望する他のトランザクションの詳細を含む他のトランザクション情報を受信することができる。その場合、セキュリティサーバは、この他のトランザクション情報をユーザへ同じ安全な通信チャネルを介して送信することができる。他の企業によってこの他のトランザクションへの有効なユーザ署名が要求されれば、セキュリティサーバは、受信された他のトランザクション情報に基づいて、ユーザによりトランザクション署名として使用されるための他のワンタイムパスワードを生成し、かつこの生成された他のワンタイムパスワードを安全な通信チャネルを介してユーザへ送信する。このワンタイムパスワードは、好ましくは、セキュリティサーバおよびこの他の第２の企業により共有されるがユーザにも第１の企業にも知られておらず、いかなる特定のユーザにも関連づけられていない秘密にも基づいて生成されることは留意されるべきである。何れにしても、セキュリティサーバは、次に、ネットワークを介して他の企業から、ユーザからの有効に署名されたトランザクションの他の企業による受信確認を受信し、かつ安全な通信チャネルを介してユーザへ、第２の企業が有効に署名されたトランザクションを受信したことの確認を送信する。

【００１５】

本発明のさらに他の態様によれば、セキュリティサーバは、受信されたトランザクション情報を音声ストリームおよび画像のうちの少なくとも一方へ組み込む、例えば埋め込んでもよく、この場合、送信されるトランザクション情報は、音声ストリームおよび画像のうちの少なくとも一方へ組み込まれたトランザクション情報となる。好ましくは、音声ストリームは、ユーザによる認識が可能な音声、例えばユーザ自身の声またはよく知られた有名人、例えばフランクリン・Ｄ・ルーズベルトまたはジョン・Ｆ・ケネディまたはロナルド・レーガンの声、を有する音声ストリームであり、画像は、予め選択された、例えばモナリザの絵等のユーザが知るところの背景を有する画像である。

【００１６】

また、本方法は、典型的には、ネットワークを介する通信を中継する１つまたは複数のポートと、先に述べたことを実行するようにプログラムされた論理、即ち必然ではないが典型的には実行可能なソフトウェア、を備えるプロセッサとを有するサーバによって実現されることも理解されるべきである。

【００１７】

また、セキュリティサーバは、ユーザからネットワークを介して、ユーザとセキュリティサーバとの間のネットワーク上での安全な通信チャネルを起動するための、ネットワーク以外を介してユーザに連絡するための連絡先情報を含むユーザの要求を受信することにより、ネットワークを介してのユーザと企業との間の商取引を安全に処理するために、段階的な起動を用いて動作することも可能である。このような場合、セキュリティサーバはこれに対応して、ネットワークを介してユーザへ、安全な通信チャネルが擬似的に起動されているという通知を送信する。後に、セキュリティサーバは、ネットワークを介して、企業の識別子と、ユーザがその企業を相手に始めることを希望するトランザクションの詳細とを含むトランザクション情報を受信する。これに応答して、セキュリティサーバは、ネットワーク以外を介するとともに受信された連絡先情報に対応する、ユーザへの配信のために、起動コードを送信する。先に論じたように、ネットワーク以外によるユーザへの配信には、帯域外認証事業者または他の何らかの事業者が包含されても良い。何れにしても、セキュリティサーバは、ユーザからネットワークを介して起動コードを受信し、受信された起動コードを送信された起動コードと比較して受信された起動コードを検証し、かつ受信された起動コードの検証に基づいて安全な通信チャネルを起動する。また、セキュリティサーバは、起動された安全な通信チャネルを介してユーザへトランザクション情報の送信をもする。

【００１８】

ユーザ・ネットワーク・デバイスは、ネットワークを介する商取引を安全に処理するために使用可能であるワンタイムパスワードを、持続的に保存されたシードを用いて生成するように動作することも可能である。そうするために、ユーザ・ネットワーク・デバイスは、ネットワークを介してセキュリティサーバへ、ユーザを識別するユーザ識別子と、ユーザ・ネットワーク・デバイスとセキュリティサーバとの間の安全な通信チャネルを起動する要求とを送信する。これに応答して、安全な通信チャネルが起動され、かつユーザ・ネットワーク・デバイスは、起動された安全な通信チャネルを介してセキュリティサーバからシードを受信する。シードは、送信されたユーザ識別子およびセキュリティサーバのみが知る秘密に対応する暗号鍵であり、これは続いて、例えばワンタイムパスワードを生成するために使用されることが可能であり、ワンタイムパスワードは次に、例えばネットワーク企業に対してユーザを認証する、またはネットワーク企業とのトランザクションに署名するために使用されることが可能である。受信されたシードは、ユーザ・ネットワーク・デバイスに持続的に格納されるが、安全な通信チャネルの起動期間が終了した後は削除される。即ち、シードは、安全な通信チャネルが再起動される度に再確立されるが、一旦再確立されると、安全な通信チャネルが機能している持続期間中は利用可能であり続ける。安全な通信チャネルが起動されている限り、ユーザ・ネットワーク・デバイスは、格納されたシードに基づいてワンタイムパスワードを生成することができる。

【図面の簡単な説明】

【００１９】

【図１】図１は、本発明による２ＣＨＫセキュリティシステムの構成要素を示す。

【図２】図２は、本発明による、補助的ハードウェアを除く図１のユーザ・コンピュータ装置を示す。

【図３】図３は、本発明による、補助的ハードウェアが接続されている図１のユーザ・コンピュータ装置を示す。

【発明を実施するための形態】

【００２０】

２ＣＨＫシステム

図１を参照すると、２ＣＨＫシステムは、好ましくは下記のうちの幾つか、または全てを含む：

・　デスクトップまたはラップトップコンピュータ、スマートフォンまたはスマートパッド等のユーザ・コンピュータ装置１００。これは、インターネット等のネットワークへ接続可能であって、キーボード、キーパッド、マウスまたはユーザ入力を入力する他の手段等の入力手段１０２と、（１）ウィンドウ１１０、以後「ウェブサイトウィンドウ」と称する、におけるウェブサイトに関連づけられるページ、以後「ウェブサイトページ」と称する、と、（２）ウィンドウ１２０、以後「セキュリティウィンドウ」と称する、内のセキュリティサーバに関連づけられるページと、（３）任意の所定の時間にユーザ・コンピュータ装置上で実行されている場合のある様々なアプリケーションのうちの何れかに関連づけられる他のページ、を表示できる画面１０５とを有する。

・　ウェブサイト１３０。典型的には、ネットワーク上にウェブサイトサーバによって代表され、ユーザはネットワークを介してこれにアクセスすることができ、ユーザがトランザクションにログインしている、またはトランザクションを実行している、もしくはそのログインまたは実行を希望しているウェブサイトであって、場合により、アプリケーション・プログラミング・インタフェース（ＡＰＩ）１３５および鍵管理ロジック－ＡＰＩ（ＫＭＬＷＳ）１３７を含む。実用的な実現形態では、典型的には、ネットワークを介してアクセス可能な複数の異なるウェブサイトが存在することとなることは理解されるべきである。

・　ネットワークを介してユーザがアクセスでき、かつ場合により鍵管理ロジック－サーバ（ＫＭＬＳ）１４７を含むセキュリティサーバ１４０。

・　帯域外認証サーバ１５０。以後、「ＯＯＢＡサーバ」と称する。

・　認証局（ＣＡ）１７０。

・　例えば従来型の固定電話である有線デバイス、または例えば携帯電話もしくはスマートフォンであるモバイルデバイス、他等のユーザ通信デバイス１６０。
・　ネットワークを介して確立される、ウェブサイト１３０とウェブサイトウィンドウ１１０との間で情報を伝達するための通信チャネル１３２。
・　ネットワークまたは他の手段を介して確立される、ウェブサイト１３０とセキュリティサーバ１４０との間で直接に情報を伝達するための任意選択の安全な通信チャネル１３４。
・　ネットワークを介して確立される、セキュリティサーバ１４０とウェブサイトウィンドウ１１０との間で情報を伝達するための通信チャネル１４２。
・　ネットワークを介して確立される、セキュリティサーバ１４０とセキュリティウィンドウ１２０との間で情報を伝達するための安全な通信チャネル１４４。
・　ネットワークまたは他の手段を介して確立される、セキュリティサーバ１４０とＯＯＢＡサーバ１５０との間で情報を伝達するための安全な通信チャネル１４６。
・　ネットワークまたは他の手段を介して確立される、セキュリティサーバ１４０とＣＡ１７０との間で情報を伝達するための安全な通信チャネル１４８。
・　ネットワーク以外によって確立される、ＯＯＢＡサーバ１５０とユーザ通信デバイス１６０との間で情報を伝達するための通信チャネル１５２。

【００２１】

図２を参照すると、ユーザ・コンピュータ装置１００は、好ましくは下記のうちの幾つか、または全てを含む：

・　中央処理装置（ＣＰＵ）２０５。
・　ネットワークを介してウェブサイト１３０およびセキュリティサーバと通信するための、モデムおよびポート等のネットワーク通信デバイス（ＮＣＤ）２０６。
・　（１）ウェブサイトウィンドウ１１０として機能するブラウザウィンドウを生成し、かつウェブサイト１３０および他のウェブサイト（不図示）から送信されるウェブサイトページを生成してウェブサイトウィンドウ１１０に表示するためと、（２）セキュリティウィンドウ１２０として機能するブラウザ・ポップアップ・ウィンドウを生成し、かつセキュリティサーバ１４０から送信されるページを生成してこのポップアップ・セキュリティ・ウィンドウ１２０に表示するために、ＣＰＵ２０５によって実行されることが可能なウェブ・ブラウザ・アプリケーション２０７。ブラウザ２０７により表示されるウェブサイトページは、以後、ウェブページと称される場合がある。
・　セキュリティウィンドウ１２０を作成し、かつ、セキュリティサーバ１４０から送信されるページを生成しかつ２ＣＨＫセキュリティウィンドウ１２０に表示するためにＣＰＵ２０５によって実行されることが可能なセキュリティアプリケーション２１０。以後、「２ＣＨＫクライアントアプリケーション」と称される場合もある。セキュリティアプリケーション２１０は、鍵管理ロジック－クライアント（ＫＭＬＣ）２１３を含んでもよい。
・　メモリおよび／またはハード・ドライブ・データ・ストアに実現されてもよい、プライベートストア２１０ａおよび２１２ａとパブリックストア２１０ｂとを含むローカルストレージ。
・　（１）ウェブサイトウィンドウ１１０を生成し、かつ、ウェブサイト１３０に関連づけられるウェブサイトページを生成しかつウェブサイトウィンドウ１１０に表示するためにＣＰＵ２０５によって実行されることが可能な、商業者または銀行アプリケーション等のウェブサイトアプリケーション２１２。実用的な実現形態では、各々がネットワークを介してアクセス可能な異なるウェブサイトに関連づけられる複数の異なるウェブサイトアプリケーションが存在し得ることは理解されるべきである。
・　テキストメッセージ送信のためのショート・メッセージ・サービス（ＳＭＳ）アプリケーション２１４。以後、「ＳＭＳＡ」と称されることがある。
・　ネットワークを介してｅメールを送受信するためのｅメールアプリケーション２１６。

・　コンピュータ装置上で作成される、またはネットワークを介してコンピュータ装置へ送信される文書を生成しかつウィンドウ（不図示）に表示するためにＣＰＵ２０５によって実行されることが可能な、Ａｄｏｂｅ　ＡｃｒｏｂａｔまたはＭｉｃｒｏｓｏｆｔ　Ｗｏｒｄ等の文書処理アプリケーション２１８。実用的な実現形態では、複数の異なる文書処理アプリケーションが存在し得ることは理解されるべきである。

・　補助的ハードウェア上で実行されるセキュリティアプリケーションとセキュリティサーバ１４０との間の通信のための安全なパイプラインを作成するためにＣＰＵ２０５によって実行されることが可能なプロキシアプリケーション。以後、「２ＣＨＫプロキシ・クライアント・アプリケーション」と称される場合もある。

・　コンピュータ装置１００を補助的ハードウェアへ通信可能に接続するためのポート２２２。

【００２２】

図３を参照すると、ユーザ・コンピュータ装置１００との間で通信可能に相互接続されかつ切断されてもよい補助的ハードウェア３００は、好ましくは下記のうちの幾つか、または全てを含む：

・　ディスプレイ画面３０２。

・　キーパッド、キーボード、マウスまたはユーザ入力の他の入力手段等の入力手段３０４。

・　中央処理装置（ＣＰＵ）３０５。

・　ディスプレイ画面３０２上にセキュリティウィンドウ１２０を作成し、かつ、セキュリティサーバ１４０から送信されるページを生成しかつセキュリティウィンドウ１２０に表示するためにＣＰＵ３０５によって実行されることが可能なセキュリティアプリケーション３１０。以後、「２ＣＨＫクライアントアプリケーション」と称される場合もある。セキュリティアプリケーション３１０は、ＡＰＩ３１１および鍵管理ロジック－クライアント（ＫＭＬＣ）３１３を含んでもよい。

・　メモリおよび／またはハード・ドライブ・データ・ストアに実現されてもよい、プライベートストア３１２を含むローカルストレージ。

・　補助的ハードウェア３００が接続されるユーザ・コンピュータ装置１００のポート２２２と補助的ハードウェア３００との間で情報を送信するための、例えばＵＳＢケーブル、近距離無線通信（ＮＦＣ）、Ｂｌｕｅｔｏｏｔｈまたはヘッドフォンジャック、などを介して確立されるもの等の通信リンク３２０。

【００２３】

先に述べたように、セキュリティウィンドウ１２０は、コンピュータ装置１００の画面１０５上において、ブラウザアプリケーション２０７により作成されるポップアップ・セキュリティ・ウィンドウに、またはセキュリティアプリケーション２１０、即ち２ＣＨＫクライアントによって作成される非ブラウザ・セキュリティ・ウィンドウに表示されてもよい。また、セキュリティウィンドウ１２０は、補助的ハードウェア３００の画面３０２上において、セキュリティアプリケーション３１０、即ち２ＣＨＫクライアントによって作成される非ブラウザ・セキュリティ・ウィンドウにも表示されてもよい。セキュリティアプリケーション２１０は、様々な異なるフォームファクタのうちの何れによって実現されることも可能である。ある種類は、セキュリティウィンドウ１２０が、スマートフォンまたはスマートパッド等のモバイル・コンピュータ装置上のセキュリティアプリケーション２１０によって、例えば２ＣＨＫクライアントのスマートフォンアプリによって制御されることを企図している。別の種類は、セキュリティウィンドウ１２０が、デスクトップまたはラップトップコンピュータ等のより高性能のコンピュータ装置上のセキュリティアプリケーション２１０によって、例えば２ＣＨＫクライアントのパーソナルコンピュータ（ＰＣ）アプリケーションによって制御されることを企図している。さらに別の種類は、先に述べたように、セキュリティウィンドウ１２０が、通信機能を有するスマートカード等の専用または非専用補助的ハードウェア３００上で実行されるセキュリティアプリケーション２１０によって制御されることを企図している。後にさらに論じるように、これら

のフォームファクタは、単に、ブラウザを実行するユーザのＰＣとは独立していることによって、追加のセキュリティ層を提供する。スマートフォンは既に個人化され、かつ後述する技術によれば、ＯＴＰの生成はウェブサイト１３０およびセキュリティサーバ１４０のみが共有する秘密の使用に依存し、よってスマートフォンが特別な秘密を格納する、またはＯＴＰソフトウェアを実行する必要はないことから、スマートフォン上での実現が容易に達成されることは認識されるであろう。むしろ、ウェブサイト１３０およびセキュリティサーバ１４０のみが、必要な秘密を共有すればよく、かつセキュリティサーバ１４０およびウェブサイト１３０のみが、ユーザのログイン認証およびトランザクション署名に要求されるＯＴＰを生成すればよい。

【００２４】

本発明の所定の態様によれば、セキュリティアプリケーションまたは２ＣＨＫクライアント２１０は、プライベートストア２１０ａおよびパブリックストア２１０ｂの双方を用い、かつウェブサイトアプリケーション２１２も、パブリックストア２１０ｂのみならずプライベートストア２１２ａを用いる。後により詳細に論じるように、ＣＰＵ２０５は、通信チャネル１４２を介してセキュリティサーバ１２０と双方向通信するためにセキュリティアプリケーション２１０を実行することができ、かつ通信チャネル１３２を介してウェブサイト１３０と双方向通信しかつ通信チャネル１４２を介してセキュリティサーバ１２０と双方向通信するためにブラウザまたはウェブサイトアプリケーション２１２を実行することができる。

【００２５】

図３に示されているように、２ＣＨＫクライアント機能は、例えばＵＳＢケーブル、近距離無線通信（ＮＦＣ）、Ｂｌｕｅｔｏｏｔｈまたはヘッドフォンジャック、他を介してＰＣまたはスマートフォン等のコンピュータ装置へ、他の補助的なハードウェア製品に類似する方法で通信可能に取り付けられることが可能な専用または非専用補助的ハードウェア３００上で利用可能にされてもよい。補助的ハードウェアは、例えばスマートカード、安全な記憶装置、安全なディスプレイ装置、または証明書ストアまたは生体情報読取装置または指紋保護型記憶装置、他等の補助的識別情報の安全なソースを含む、任意のタイプであり得る。また、補助的ハードウェアは、ＰＣへ通信可能に取り付けることができるスマートフォンであり得ること、かつデスクトップ、ラップトップまたはスマート・モバイル・デバイスの代わりに、ゲーム装置、ＴＶ、ＤＶＤプレーヤ、他等の任意のインターネット接続デバイスがコンピュータ装置１００の代用にされることが可能でありかつ補助的ハードウェアのプロキシまたはコンジットとして機能する中間点となり得ることも理解されるべきである。補助的ハードウェア上に２ＣＨＫクライアント機能を保有すれば、結果的に、コンピュータ装置１００自体に対する攻撃を防護するための安全性をさらに高めることができる。

【００２６】

２ＣＨＫクライアント機能が補助的ハードウェア上に存在することにより、コンピュータ装置１００は（デスクトップまたはラップトップコンピュータであれ、スマートフォンまたはスマートパッドであれ）、基本的に、セキュリティサーバ１４０とコンピュータ装置１００へ取り付けられる補助的ハードウェアとの間でメッセージを運ぶためのコンジット（または、プロキシ）として行動している。即ち、コンピュータ装置１００上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０によって果たされる役割は、今度は代わりに、補助的デバイス上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント３１０によって果たされる。

【００２７】

補助的ハードウェア３００は、コンピュータ装置１００へポート２２２および通信リンク３２０を介して着脱可能式に接続される。セキュリティアプリケーション、即ち２ＣＨＫクライアント３１０は、ＣＰＵ３１５およびユーザによってプライベートストア３１２およびパブリックストア２１０ｂの双方で実行可能である。セキュリティアプリケーション、即ち２ＣＨＫクライアント３１０は、セキュリティサーバ１４０と、安全な通信チャ

ネル１４４、プロキシ２２０、ポート２２２および通信リンク３２０を介して双方向通信する。プロキシ／コンジットアプリケーション２２０は、通信リンク３２０、ポート２２２および通信チャネル１４４と共にセキュリティサーバ１４０とセキュリティアプリケーション２１０との間の安全な通信パイプラインとして機能するようにＣＰＵ２０５によって実行される。またこれは、通信リンク３２０およびポート２２２と共に、セキュリティアプリケーション３１０とコンピュータ装置１００上のパブリックストレージ２１０ｂとの間の通信パイプラインとしても機能する。したがって、セキュリティサーバ１４０とセキュリティウィンドウ１２０との間の通信が、「コンジット／プロキシ」として機能するコンピュータ装置１００によって読み取られる、または操作されることはない。言い替えれば、コンピュータ装置１００を介して補助的ハードウェアへ送られるデータは、補助的ハードウェア上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント３１０にしか読み取れないようにして暗号化または符号化される。

２ＣＨＫシステムの動作

【００２８】

動作には、次のような明確な５段階が存在する：（ｉ）セキュリティウィンドウ１２０のセットアップおよび個性化、これは、１回限りの処理である、（ｉｉ）ポップアップ・セキュリティ・ウィンドウであれ、２ＣＨＫセキュリティウィンドウであれ、セキュリティウィンドウ１２０の始動または起動、これは、使用毎のコンピュータへのログインと同様に、定期的に発生する、（ｉｉｉ）ユーザが、セキュリティサーバ１４０を介してユーザに対して自らを認証するウェブサイト１３０を閲覧する場合の、ユーザに対するウェブサイト１３０の認証、（ｉｖ）ユーザがウェブサイト１３０を閲覧する、またはウェブサイトアプリケーション２１２を起動する場合の、例えばログインを目的とする、セキュリティサーバ１４０によるユーザのウェブサイト１３０またはウェブサイトアプリケーション２１２に対する認証、および（ｖ）ユーザがウェブサイト１３０を閲覧するか又は、ウェブサイトアプリケーション２１２を用い、かつウェブサイト１３０との特定のトランザクションの開始を希望する場合の、トランザクションの承認またはトランザクション署名。

セットアップおよび個性化段階

【００２９】

ユーザは、その２ＣＨＫシステムとの関連付けを、１回限りの処理であるセットアップおよび個性化段階を介して開始する。セットアップするために、ユーザは、セキュリティサーバ１４０においてホストされるネットワークサイトを訪れる。セキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０が実現に利用されるのであれば、適用可能なセキュリティアプリケーションは、ユーザのコンピュータ装置１００へアップロードされ、かつコンピュータ装置１００上または補助的ハードウェア３００上へ、典型的には、適用可能なデバイス１００または３００上で利用可能な、例えばメモリ、ハードドライブまたは他のローカル・ストレージ・オプションであるローカルストレージ上へ、格納される。実現の仕方によっては、セキュリティアプリケーション２１０およびセキュリティアプリケーション３１０の双方が利用され、よってセットアップ処理中に双方がアップロードされる必要があることは理解されるべきである。ユーザは、個性化画像を選択する。この画像は、ユーザのコンピュータ装置１００上へクッキーを用いて局所的に格納される。これは、一般に、ユーザ毎、ユーザ・コンピュータ装置１００毎の１回限りの事象であって、ユーザが個性化画像の変更を希望する、またはローカルストレージが何らかの理由で削除される場合にのみ反復されることを要する。

始動および起動（セキュリティ・サーバ・ログイン）段階

【００３０】

起動は、典型的には周期的に発生し、例えば日に一度、ユーザがウェブの閲覧を開始する前に発生する。実現形態に依存して、ユーザは、起動処理を手動で開始することができ、あるいは、起動処理は、ユーザが２ＣＨＫシステムに参加するウェブサイト１３０を訪れた際に自動的に開始されても良い。この後、セキュリティサーバ１４０は、ＯＯＢＡサ

ーバ１５０を介するＯＯＢＡを通じたユーザの検証に基づいてセキュリティウィンドウ１２０を起動する。しかしながら、この段階では、望ましい場合には、ＯＯＢＡでない他の形式の検証が使用されることも可能であることは理解されるべきである。他の形式の検証が、２ＣＨＫシステムと既存のＯＴＰ配備との統合をより容易にする場合があることは認識されるであろう。

【００３１】

一般に始動のための「開放」モデルＯＯＢＡと称されるものを用いて、起動は、好ましくは、ユーザにより次のようにしてもたらされる。セキュリティサーバ１４０に対するユーザの検証に際しては、（１）ユーザが、その電話番号、例えば有線電話、携帯電話またはスマート携帯電話の電話番号を、例えばデスクトップコンピュータまたはスマートフォンであるユーザ・コンピュータ装置１００または補助的ハードウェア３００上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０またはブラウザアプリケーション２０７（セキュリティウィンドウがブラウザのポップアップ・セキュリティ・ウィンドウであれば）により表示されるセキュリティウィンドウ１２０へ入力するか、または（２）セキュリティアプリケーション２１０または３１０またはブラウザ２０７が、ユーザのコンピュータ装置１００から直接番号を入手する。入力された、または他の方法で入手された電話番号は、コンピュータ装置１００から通信チャネル１４４を介してセキュリティサーバ１４０へ、または、補助的ハードウェア３００から通信リンク３２０およびチャネル１４４を介してセキュリティサーバ１４０へ送信される。

【００３２】

セキュリティサーバ１４０は、ログインのセキュリティコードを、通信チャネル１４６を介してＯＯＢＡサーバ１５０へ伝達する。ＯＯＢＡサーバ１５０は、セキュリティサーバ１４０に対してユーザを認証するために、ユーザにログインのセキュリティコードを提供すべく通信チャネル１５２を介してユーザの携帯電話、スマートパッドまたはスマートフォン１６０と通信する。ＯＯＢＡサーバ１５０がユーザへ起動コードを伝達する手段には、テキストメッセージ、音声呼、ｅメール、または、セキュリティアプリケーション２１０または３１０またはブラウザ２０７がセキュリティサーバ１４０と通信する手段であるチャネルとは実質的に異なり、よって双方のチャネルへの不正侵入が実質的により困難になる、他の任意の通信チャネルが含まれることが可能であるが、これに限定されない。

【００３３】

通信チャネル１５２が、典型的にはその可能性が最も高いと思われる双方向性であれば、通信チャネル１５２は、場合により、ＯＯＢＡサーバ１５０によりアクセス可能で、共有秘密、居場所情報および生体情報識別子を含むが、これらに限定されない識別情報と比較するために、追加の認証情報を捕捉することにより、ユーザと双方向通信して起動コードの配信より前にユーザをより完全に認証するように利用されることが可能である。

【００３４】

セキュリティコードの鍵付きハッシュは、暗号化された通信チャネル１４４および妥当であればリンク３２０を介してセキュリティサーバ１４０へ送られる。セキュリティサーバ１４０に対するユーザのこのような検証は、当然ながら、セキュリティサーバ１４０がセキュリティウィンドウ１２０を介してユーザへ、例えばウェブサイトへのログインを目的として、またはウェブサイト１３０とのトランザクションを承認するために、ウェブサイト１３０に対する認証用に要求される認証情報を提供する前に実行される。

【００３５】

一方で、一般に「関連付け」ＯＯＢＡモデルと称されるものが始動に利用されれば、起動は、好ましくは、ユーザではなく企業、例えばウェブサイト１３０によってもたらされる。したがって、ユーザは、関連付けＯＯＢＡモデルにおけるセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０へ電話番号を入力する必要はなく、よって入力しない。代わりに、ユーザは、ブラウザアプリケーション２０７により伝達されるウェブサイト１３０の安全機構、またはユーザ識別子とパスワードとの組合せ等のウェブサイトアプリケーション２１２の安全機構を用いて企業へ、例えばウェブサイト１３

０へログインする。ユーザは、２ＣＨＫ関連付けを、ウェブサイトウィンドウ１１０におけるユーザのブラウザアプリケーション２０７またはウェブサイトアプリケーション２１２により提示されるウェブサイト１３０のウェブページから選択することによって要求する。

【００３６】

例えば、ユーザは、マスクされたアドレスまたは電話番号、即ちウェブサイト１３０が事前に入手可能なものであってユーザには完全に示されないアドレスまたは電話番号、例えば４１５．６８０．ｘｘｘｘ等である連絡先情報を含む識別情報を選択することによって、２ＣＨＫ関連付けを要求するように求められる場合もある。このような場合、ウェブサイト１３０は、例えば有線電話または携帯電話の番号である電話番号を有する関連付け要求を、ユーザの認証および起動においてセキュリティサーバ１４０により使用されるためにセキュリティサーバ１４０へ送る。望ましい場合には、連絡先情報は、電話呼によってユーザに連絡するための情報の代わりに、ユーザにより選択される、好ましくはマスクされた適用可能な識別情報を有する、手渡し、ＮＦＣ／Ｂｌｕｅｔｏｏｔｈ交換または知識ベースの認証（ＫＢＡ）照会、他によってユーザに連絡するための情報であることも可能であることは留意されるべきである。あるいは、ユーザは、２ＣＨＫ関連付けを、単に２ＣＨＫ起動ボックスをクリックするだけで要求するように求められる場合もある。このような場合、ウェブサイト１３０は、所望されれば、ユーザの認証および起動においてセキュリティサーバにより使用されるための企業起動コードを生成し、かつこれをセキュリティサーバ１４０へ送ることができる。

【００３７】

ウェブサイト１３０またはウェブサイトアプリケーション２１２は、関連付け要求を、好ましくは選択された完全な連絡先情報、例えば選択された完全な電話番号、例えば４１５．６８０．００００、またはユーザ識別情報（ユーザによって選択されたものではない）を含む識別情報および企業起動コードと共に、適宜、ウェブサイトウィンドウ１１０とセキュリティサーバ１４０との間の通信チャネル１３２および１４２を介して、またはウェブサイト１３０とセキュリティサーバ１４０との間の直接的な安全な通信チャネル１３４を介してセキュリティサーバ１４０へ送信する。

【００３８】

この時点から、セキュリティサーバ１４０は、ＯＯＢＡ比較用に利用可能な識別情報および恐らくはＯＯＢＡ比較の起動コードがこれでセキュリティサーバおよび企業の双方から到来することを除いて、「開放」モデルと全く同様に進行する。識別情報または識別コードは、好ましくは妥当な企業への妥当な要求に固有のものであり、同時的に、エンドユーザへ例えば公衆交換電話網（ＰＳＴＮ）を介して配信されかつセキュリティサーバ１４０内に格納される。セキュリティサーバ１４０は、セキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０によるセキュリティサーバ起動コードおよび妥当であれば企業起動コードの配信を待機し、かつこれらのコードを受信した時点で、セキュリティアプリケーション、即ち２ＣＨＫクライアント２１０又は３１０を、例えばウェブサイト１３０である企業からの特定の要求へ結び付ける。即ち、セキュリティコードの鍵付きハッシュは、暗号化された通信チャネル１４４および妥当であればリンク３２０を介してセキュリティサーバ１４０へ送られる。受信されたコードに基づいてセキュリティサーバによりユーザが検証されれば、セキュリティサーバ１４０とセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０との間のさらなる通信は、通信チャネル１４４および妥当であれば通信リンク３２０が安全であるように、起動コードを用いて暗号化される。ここで、当然ながら、このようなセキュリティサーバ１４０に対するユーザの検証は、ユーザがウェブサイト１３０に対する認証に要求される認証情報を例えばウェブサイトへのログインを目的として提供した後に、但し、セキュリティサーバ１４０がユーザにセキュリティウィンドウ１２０を介して、安全な通信チャネル１４４および妥当であれば通信リンク３２０上で送信される認証情報であって、ウェブサイト１３０とのトランザクションを承認するために要求される認証情報を提供する前に実行される。

【００３９】
２ＣＨＫシステムを用いたユーザと企業との間の関連付けの重要性は、特定の企業の特定のアカウント／関係性へ結び付けることにある。したがって、ここでは、企業が処理を制御して、セキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０が特定のアカウントに関連づけられることを許し、又は可能にする。
【００４０】
ＯＯＢＡを介してユーザが検証されると、セキュリティウィンドウ１２０が起動されて、ユーザのコンピュータ装置１００または補助的ハードウェア３００上の比較的小さいスペースを占有する。セキュリティウィンドウ１２０を始動する行為は、セキュリティサーバ１４０がユーザのコンピュータ装置１００または補助的ハードウェア３００上へローカル・セッション・オブジェクト、例えばセッションクッキーを仕掛ける結果ももたらす。この時点で、セキュリティサーバ１４０は、セキュリティサーバ１４０が何らかのユーザ識別子、例えばＯＯＢＡに使用される電話番号によって識別するユーザに開放された、機能中の安全な通信チャネル１４４を有する。
【００４１】
通信チャネル１４４上で送信される情報の暗号化には、２つのレベルが存在する。第１に、全てのトラフィックがＳＳＬ上で実行される。第２に、全てのトラフィックは、アプリケーションレベルにおいても、セキュリティサーバ１４０へログインするためにユーザにより使用されるセキュリティから導出される鍵を用いて暗号化される。セキュリティウィンドウ１２０およびセキュリティサーバ１４０はＳＳＬ上で通信していることから、ＥＶ－ＳＳＬ証書の使用が極めて好ましいことは留意されるべきである。ＳＳＬおよびＥＶ－ＳＳＬ証書は共に、当業者には周知でありかつ理解されている。
【００４２】
コンピュータ装置１００または補助的ハードウェア３００がスマートフォンまたは他のスマートモバイル通信デバイスである場合、所定の動作は、望ましい場合には、スマートフォンの所定の一般的な機能および性能を利用するように実現されてもよい。
【００４３】
例えば、ＯＯＢＡサーバ１５０にとっては、セキュリティコードをユーザへテキストメッセージで伝達することが有益である場合がある。このような場合、ユーザは、ＳＭＳＡ２１４を介してログインのセキュリティコードを有するテキストメッセージを受信した後、セキュリティサーバ１４０へログインするために、即ちセキュリティサーバ１４０に対して検証するために、受信されたログインのセキュリティコードを、スマートフォン１００上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０によって、またはスマートフォン１００へ接続される補助的ハードウェア３００上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント３１０によって提示されるセキュリティウィンドウ１２０へ入力することができる。幾つかのスマートフォンプラットフォーム上において、セキュリティアプリケーション２１０は、望ましい場合には、着信するテキスト・メッセージ・ストリームからログインのセキュリティコードを検索し、かつまたログインのセキュリティコードをセキュリティウィンドウ１２０へ自動記入するように構成されることが可能であって、ユーザに対する利便性がさらに高められる。
【００４４】
何れにしても、セキュリティサーバ１４０からセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０への返信メッセージは、転送されたセキュリティコードが有効であれば、セッションクッキー、「ノンスログイン」と呼ばれる乱数および有効期間（ＴＴＬ）である。セッションクッキーは、非公開で、適宜プライベートストア２１０ａまたは３１２に格納される。ノンスログインおよびＴＴＬは、カスタムペーストボード、セキュリティアプリケーション、またはパブリックストア２１０ｂ内に生成される２ＣＨＫクライアントのパブリックペーストボード上に公開して格納される。ユーザがその焦点をセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０へ向けると、セキュリティアプリケーション２１０は、ＴＴＬが時間切れになっていな

いことを保証するために、常にノンスおよびＴＴＬをチェックする。

【００４５】

ユーザが一旦セキュリティサーバ１４０へログインすると、ユーザは次に、ウェブサイトアプリケーション２１２またはブラウザアプリケーション２０７等の他のアプリケーションの使用を開始し、かつ必要に応じてセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０へ戻ってもよい。

【００４６】

先に述べたように、ユーザは、この２ステップ起動を、例えば（ｉ）ユーザの電話番号または携帯電話番号を、適宜ユーザのコンピュータ装置１００または補助的ハードウェア３００上で実行されるセキュリティアプリケーション２１０または３１０によって提示されるセキュリティウィンドウ１２０へ入力し、かつ（ｉｉ）入力された番号においてＯＯＢＡサーバ１５０から起動コードを音声またはテキストメッセージによって受信し、かつ受信された起動コードを、セキュリティサーバ１４０へ転送して返すためにセキュリティウィンドウ１２０へ入力すること、によって完了する。ステップ（ｉｉ）は、ステップ（ｉ）に続いて直ちに発生し、この後、ユーザは、２ＣＨＫシステムを介してトランザクションを受信できる状態になる。

【００４７】

しかしながら、ＯＯＢＡサーバ１５０は、セキュリティサーバ１４０から受信する起動コードを（音声またはテキストメッセージを介して）電話番号宛に、その番号について何ら知識もないまま送信していることから、潜在的問題が発生する可能性もある。これにより、システムがなりすまし攻撃を受けやすくなるものではないが、システムが、例えば攻撃者が地元のピザ配送所の番号を入力し、ユーザが続いて、例えば地元のピザ配送所であるウェブサイトにより転送された例えばピザの注文であるトランザクションを承認せずに拒絶する、という迷惑攻撃を受けやすくなる可能性はある。即ち、開放モデルでは、攻撃者がセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０へユーザの電話番号を入力して起動を開始させる可能性もある。これは、技術的に言えば攻撃ではないが、ユーザは結果的に、ＯＯＢＡサーバから迷惑コールまたはテキストを受信する。

【００４８】

この潜在的な問題点は、上述の起動処理を起動ステップが時差式に実行されるように修正することにより、改善されることが可能である。より具体的には、ユーザは、時差式の起動を用いて電話番号を通常の方法で適宜、ユーザのコンピュータ装置１００または補助的ハードウェア３００上で実行されるセキュリティアプリケーション２１０または３１０により提示されるセキュリティウィンドウ１２０へ入力する。しかしながら、入力された番号においてＯＯＢＡサーバ１５０から起動コードを直ちに受信するのではなく、ユーザは、入力された番号において、ユーザが「擬似的に起動されている」こと、およびこの起動は後に完成されることを通知される。後に、例えばウェブサイト１３０である企業が電話番号により識別されるユーザへのトランザクションの送信を希望する時点で、例えばウェブサイト１３０である企業は、トランザクション、およびユーザを識別する電話番号をセキュリティサーバ１４０へ送る。セキュリティサーバ１４０が「擬似的に起動されている」状態にあるその電話番号（と装置との組合せ）を有していれば、セキュリティサーバ１４０は、まず、ＯＯＢＡサーバ１５０へ起動コードを送ってユーザの起動を正常に完了させる。起動の完了後、セキュリティサーバ１４０は、通信チャネル１４４を介してユーザのコンピュータ装置１００上のセキュリティウィンドウ１２０へトランザクションを送る。ユーザは、この時点で完全に起動されていて、起動の完了を要求しないことから、この後、後続のトランザクションは通常の方式で処理される。

ウェブサイト認証段階

【００４９】

２ＣＨＫシステムに参加するウェブサイト１３０は、ブラウザ２０７により閲覧されるウェブページまたはウェブサイトアプリケーション２１２により提示されるウェブサイト

ページに、２ＣＨＫシステムにアクセスするためのコードを埋め込む。典型的には、これは、ｉＦｒａｍｅ内部のＪａｖａｓｃｒｉｐｔコードの形式となる。コードは、セキュリティサーバ１４０へ先に仕掛けられたローカル・セッション・オブジェクトを転送する行為の要求に従って、セキュリティサーバ１４０へ届く。

【００５０】

セキュリティサーバ１４０は、ｉＦｒａｍｅからの要求のＲｅｆｅｒｒｅｒまたはＯｒｉｇｉｎタグを、許可／禁止サイトの既知のホワイトリストおよび／またはブラックリストに照らしてチェックする。これは、次に、ｉＦｒａｍｅに応答し、かつ同時に自らが通信状態にあるセキュリティウィンドウ１２０に信号で伝える。信号は、２つの部分からなり、第１の部分は、ウェブサイト１３０が「良い」か「悪い」か、またはセキュリティサーバ１４０はウェブサイト１３０を「知らない」ことを示す。信号の第２の部分は、（ウェブサイト１３０が正規のものであれば）セキュリティウィンドウ１２０およびｉＦｒａｍｅへ送られるランダム画像である。ウェブサイト１３０が正規であれば、ユーザのセキュリティウィンドウ１２０は、ウェブサイト１３０が「良い」ものであるという視覚的合図（例えば、緑色の光）を有し、かつランダム画像を示す。ｉＦｒａｍｅも、同様の視覚的合図を示し、かつ極めて重要な点として、同じランダム画像も示す。ウェブサイト１３０がブラックリストに存在していれば、セキュリティウィンドウ１２０は、ウェブサイト１３０が「悪い」ものであることを示す視覚的合図（例えば、赤色光）を示す。

【００５１】

偽のセキュリティウィンドウを生成することによって２ＣＨＫシステムを破ろうとする攻撃者は、個性化画像を知り得ないことに起因して阻まれる。また、ｉＦｒａｍｅに視覚的合図を表示しようとする攻撃者は、セキュリティウィンドウ１２０へ送られるランダム画像を知らないことに起因して成功しない。最後に、偽のウェブサイトは、ブラウザによって点検されることから、ＲｅｆｅｒｒｅｒまたはＯｒｉｇｉｎタグを操作することができない。

ユーザ認証（例えば、ウェブサイトへのログイン）段階

【００５２】

好ましくは、始動の間、ユーザはセキュリティサーバ１４０に対し、セキュリティサーバ１４０の要求で電話番号を所有していることを証明するためにＯＯＢＡサーバ１５０により実行されるＯＯＢＡ技術を用いて認証される。これが発生した後、セキュリティサーバ１４０は、ウェブサイト１３０からのユーザ識別アサーション要求に応えることができる。これを実行するために、セキュリティサーバ１４０、および２ＣＨＫシステム内の個々のウェブサイト１３０は、２ＣＨＫシステムに参加していてこのウェブサイトを訪れる全てのユーザに関して、異なる共有秘密について事前に合意している。即ち、セキュリティサーバおよび各ウェブサイト１３０は、いかなるユーザにも他のウェブサイトにも知られておらず、かついかなる特定のユーザにも関連付けられていない共有秘密を有する。

【００５３】

ユーザが、認証を要求するウェブサイト１３０またはウェブサイトアプリケーション３１２に存在し、かつウェブサイト１３０またはウェブサイトアプリケーション２１２がこの要求をセキュリティサーバ１４０へ伝達する場合、セキュリティサーバ１４０は、ログインＯＴＰ、即ちログイン認証情報を、このウェブサイト１３０と共有される秘密および望ましい場合には所定の他の情報の関数として計算する。例えば、ＯＴＰは、タイムスタンプまたはカウンタベースのＯＴＰアルゴリズムにも基づいて構築することができ、時間またはカウンタ値は、セキュリティサーバ１４０によってウェブサイト１３０またはウェブサイトアプリケーション２１２へ伝達され、または潜在的に、何らかの合意された公式を用いて確定的に計算される。セキュリティサーバ１４０は、次に、計算されたＯＴＰを、例えばユーザのセキュリティウィンドウ１２０に表示するためにブラウザアプリケーション２０７またはセキュリティアプリケーション２１０、即ち２ＣＨＫクライアントへ伝達する。ユーザは、ウェブサイト１３０またはウェブサイトアプリケーション２１２に対してユーザを認証するために、この表示されたログインＯＴＰを、ユーザのコンピュータ

装置１００上へブラウザ２０７またはウェブサイトアプリケーション２１２によって表示されているユーザ資格認定情報を要求するウェブサイトページの適切な部位に（例えば、切り取りおよび貼り付けまたはタイプ打ちによって）入力する。

【００５４】

入力されたログインＯＴＰを受信した後、ウェブサイト１３０は、セキュリティサーバ１４０と共有する秘密を用いてＯＴＰを再計算することによりユーザを認証する。したがって、２ＣＨＫシステムは、従来のＯＴＰシステムにおける全ての安全特性を有し、しかも、各ユーザとの間に共有される秘密を要求せず、かつＯＴＰを生成する目的で共有秘密を必要とするのはセキュリティサーバ１４０およびウェブサイト１３０のみであるという圧倒的な優位点を有する。

【００５５】

例えば、ある実用的なアプリケーションにおいて、ユーザは、ウェブサイト１３０における所定の情報にアクセスするために、ブラウザ２０７またはウェブサイトアプリケーション２１２を用いてウェブサイトウィンドウ１１０へ要求を入力する。要求は、ウェブサイトウィンドウ１１０から通信チャネル１３２を介してウェブサイト１３０へ送信される。ウェブサイト１３０は、この要求をセキュリティサーバ１４０へ、適宜、ユーザのブラウザアプリケーション２０７またはウェブサイトアプリケーション２１２を介し通信チャネル１３２および１４２を介して、または任意選択のウェブサイト１３０とセキュリティサーバ１４０との間の直接的な通信リンク１３４を介して、の何れかによって送信する。

【００５６】

セキュリティサーバ１４０は、ウェブサイト１３０に対してユーザを認証するために、ウェブサイトへログインするための個人識別番号（ＰＩＮ）と称される場合もあるログインＯＴＰを計算する。ログインＯＴＰは、セキュリティサーバ１４０がこの特定のウェブサイト１３０と共有する秘密の関数として計算される。先に述べたように、この共有される秘密は、ユーザの知らないものであり、かつユーザまたは他のいかなる特定ユーザにも関連付けられているものではない。セキュリティサーバ１４０は、次に、このログインＯＴＰをユーザのセキュリティウィンドウ１２０へ安全な通信チャネル１４４を介して送信する。

【００５７】

ユーザは、このログインＯＴＰを切り取って、ウェブサイトウィンドウ１１０内のウェブブラウザ２０７またはウェブサイトアプリケーション２１２によって表示されるウェブサイトページへ貼り付け、または切り取り・貼り付けに代えてコピーし、かつログインＯＴＰは、通信チャネル１３２を介してウェブサイト１３０へ送信される。

【００５８】

ウェブサイト１３０は、独自に、セキュリティサーバ１４０と共有する秘密を用いてログインパスワードを計算し、かつこれをユーザから受信されるものと比較する。両者が一致すれば、ウェブサイト１３０は、セキュリティサーバ１４０がアクセスを要求してきたユーザと同じユーザ（即ち、ユーザのふりをしている、セキュリティサーバ１４０への途中で要求を傍受した他の誰かではない）を認証している、と確信することができる。さらに、セキュリティサーバ１４０は、ユーザのログインＯＴＰを独立したチャネル１４４内に示していることから、要求のユーザ確認が得られる。

【００５９】

セキュリティアプリケーション、即ち２ＣＨＫクライアント２１０は、他のアプリケーション、例えばウェブサイトアプリケーション２１２または非ブラウザアプリケーション２１８と最も適切な方法を用いて通信するようにプログラムされ得ることは留意されるべきである。

【００６０】

スマートフォンによる実現形態の固有の優位点は、ｉＰｈｏｎｅのオペレーティングシステム上のパブリックペーストボード等のパブリック共有記憶装置を用いる能力にある。したがって、ユーザがウェブサイトアプリ２１２へアクセスするという自身の希望を確認

し、かつセキュリティサーバがログインＯＴＰ、即ちユーザのログイン認証情報をセキュリティアプリ２１０へ通信チャネル１４４を介して送信した後、セキュリティアプリは、このログインＯＴＰをウェブサイトアプリ２１２へスマートフォン共有記憶装置２１０ｂを用いて転送する。しかしながら、望ましい場合には、ユーザは、ＯＴＰを自動的に記入してもらうのではなく、ログインＯＴＰをセキュリティウィンドウ１２０からウェブサイトアプリ２１２によって表示されるウェブサイトページへ手動でコピーするように要求される可能性もあることは理解されるべきである。何れの場合も、表示されたウェブサイトページにＯＴＰが記入された後、ユーザが「ログイン完了」をクリックすると、ウェブサイトアプリ２１２は、通信チャネル１３２を介してウェブサイト１３０へログインＯＴＰを送る。

【００６１】

ノンスログインおよびＴＴＬは、有益なことには、パブリック記憶装置２１０ｂにおけるセキュリティアプリ、即ち２ＣＨＫクライアント２１０のパブリックペーストボードへ書き込まれることが可能である。ログインＯＴＰは、有益なことには、ペーストボードへ、マーチャントｉｄ．ＰＩＮと称される場合もある、ウェブサイト識別子とＰＩＮとの組合せを用いて書き込まれることも可能である。マーチャントｉｄ．ＰＩＮは、先に書き込まれたあらゆるマーチャントｉｄ．ＰＩＮへ上書きされる。また、ウェブサイトアプリケーション２１２は、ユーザの、または任意の特定ユーザに関連づけられる、有効なＴＴＬを伴うログインノンスを有するセキュリティアプリケーション２１０のパブリックペーストボードが存在するかどうかをチェックすることも留意されるべきである。存在しなければ、それはユーザに、ユーザが２ＣＨＫシステムにログインしているようには思われないことを知らせる。

【００６２】

ログイン認証の場合、セキュリティアプリ、即ち２ＣＨＫクライアント２１０は、商業者および認証要求に関する情報をセキュリティサーバ１４０へ送信する。送信は、ログインノンスを含む。ウェブサイトアプリ２１２は、セキュリティアプリケーション、即ち２ＣＨＫクライアント２１０のペーストボードをポーリングして新しいマーチャントｉｄ．ＰＩＮが存在するかどうかを確認する。ウェブサイトアプリケーション２１２は、これを見つけると、ウェブサイト１３０へストリングおよびログインＯＴＰの送信を行う。ウェブサイト１３０は、ログインＯＴＰに関するその固有の検証を行った後に、成功または失敗メッセージを戻す。

トランザクション承認（例えば、トランザクション署名）段階

【００６３】

ウェブサイト１３０は、ユーザのブラウザ１１０から確認を希望するというトランザクション要求を受信すると、先に論じたように、トランザクション情報をセキュリティサーバ１４０へ、ユーザのブラウザ１１０を介して、またはウェブサイト１３０とセキュリティサーバ１４０との間の直接的な通信チャネル１３４を介して、の何れかで送る。セキュリティサーバ１４０は、次に、このトランザクション情報をユーザのセキュリティウィンドウ１２０へ、トランザクションへのユーザ署名として機能するトランザクションＯＴＰ、即ちトランザクション署名と共に転送する。トランザクションＯＴＰは、セキュリティサーバ１４０により、セキュリティサーバ１４０とウェブサイト１３０との間で共有される秘密、およびトランザクション情報、および望ましい場合には、タイムスタンプまたはカウンタベースのＯＴＰアルゴリズム等の他の情報に基づいて計算される。先に述べたように、共有される秘密は、ユーザには知られず、かついかなる特定ユーザにも関連付けられるものではない。即ち、ユーザ毎の共有秘密に対する要求事項は存在しない。

【００６４】

ユーザは、このトランザクションＯＴＰ、即ちトランザクション署名を、ウェブサイトウィンドウ１１０を介してウェブサイト１３０へ転送する。

【００６５】

ウェブサイトは、トランザクションＯＴＰ、即ちトランザクション署名を再計算し、ウ

ェブサイト１３０により計算されたＯＴＰとウェブサイトウィンドウ１１０から受信されたＯＴＰとが一致すれば、ウェブサイトは、ユーザがトランザクションを追認したことを確信することができる。

【００６６】

実用的なアプリケーションにおいて、ウェブサイト１３０を訪れているユーザは、ブラウザアプリケーション２０７またはウェブサイトアプリケーション２１２によりウェブサイトウィンドウ１１０によって表示されているウェブサイト１３０のウェブページからトランザクション、例えば「アリスに１００ドル支払う」を選択し、これがウェブサイトウィンドウ１１０から通信チャネル１３２を介してウェブサイト１３０へ送信される。ウェブサイト１３０は、このトランザクションをセキュリティサーバ１４０へ、適宜、通信チャネル１３２および１４２を介したユーザのブラウザ２０７を介して、またはウェブサイト１３０とセキュリティサーバ１４０との間の直接的な通信チャネル１３４を介して、の何れかで送信する。

【００６７】

セキュリティサーバ１４０は、トランザクション署名、即ちトランザクションＯＴＰを、（ｉ）トランザクション詳細、（ｉｉ）その特定のウェブサイト１３０と共有する秘密、および場合により他の情報、の関数として計算する。セキュリティサーバ１４０は、次に、このトランザクション署名をユーザのセキュリティウィンドウ１２０へ通信チャネル１４４を介して、かつ妥当であれば通信リンク３２０を介して送信する。

【００６８】

ユーザは、このトランザクション署名を切り取って、ブラウザ２０７またはウェブサイトアプリケーション２１２によりウェブサイトウィンドウ１１０に表示されるウェブサイト１３０のウェブサイトページへ貼り付け、または切り取り・貼り付けに代えてコピーし、このトランザクション署名は、通信チャネル１３２を介してウェブサイト１３０へ送信される。ウェブサイト１３０は、独自にトランザクション署名を、（ｉ）トランザクション詳細、（ｉｉ）セキュリティサーバ１４０と共有する秘密、および妥当であれば他の情報を用いて計算し、これを、ユーザから受信されたものと比較する。２つのトランザクション署名が一致すれば、ウェブサイト１３０は、セキュリティサーバ１４０は送信したものと同じトランザクション（即ち、セキュリティサーバ１４０への途中で操作されたトランザクションではない）を目にしていることを確信することができ、かつセキュリティサーバ１４０はユーザにトランザクションを独立したチャネル１４４において示していることから、トランザクションのユーザ追認も得られていることを確信することができる。

【００６９】

要約すれば、ユーザと、識別プロバイダとして作用するセキュリティサーバ１４０と、ネットワーク上で行われる、ウェブサイトにおけるユーザによる製品購入または送金等のトランザクションの場合の依拠当事者であるウェブサイト１３０との間の結び付きは、著しく強化される。繰り返すが、本システムがＯＴＰの全ての安全特性を有し、しかも、各ユーザとの間の共有秘密を必要とせず、かつトランザクションへの署名として使用されるＯＴＰを生成する目的で共有秘密を必要とするのはセキュリティサーバ１４０およびウェブサイト１３０等の各ウェブサイトのみである、という著しい優位点を有することは理解されるべきである。同じく先に述べたように、実際のＯＴＰは、望ましい場合には、タイムスタンプまたはカウンタベースのＯＴＰアルゴリズム（例えば、時間またはカウンタ値がセキュリティサーバ１４０によってウェブサイト１３０へ伝達されるように使用されるアルゴリズム）に基づいて構築されることも可能であり、または潜在的に、何らかの合意された公式を用いて確定的に計算されることが可能である。

【００７０】

また同じく、先にも述べたように、コンピュータ装置１００がスマートフォンまたは他のスマートモバイル通信デバイスである場合、所定の動作は、望ましい場合には、所定の一般的なスマートフォン機能および性能を利用するように達成されてもよい。

【００７１】

スマートフォンにより達成することの固有の優位点は、ｉＰｈｏｎｅのオペレーティングシステム上のパブリックペーストボード等のパブリック共有記憶装置を用いる能力にある。したがって、ウェブサイトアプリ２１２は、通信チャネル１４２を介してトランザクションをセキュリティサーバ１４０へ送信し、かつまた、ユーザにセキュリティウィンドウ１２０におけるトランザクションの承認も求める。これは、トランザクションを承認するためにＰａｙＰａｌ（商標）等の支払いウェブサイトへユーザがリダイレクトされることに類似する。セキュリティサーバ１４０は、トランザクションを、ユーザへ提示するために通信チャネル１４４を介してセキュリティアプリ、即ち２ＣＨＫクライアント２１０へ送信する。ユーザがセキュリティサーバ１４０に対してトランザクションを進めるというその希望を追認し、かつセキュリティサーバがトランザクションＯＴＰ、即ちトランザクション署名を、セキュリティアプリ、即ち２ＣＨＫクライアント２１０へ通信チャネル１４４を介して送信した後、セキュリティアプリ２１０は、スマートフォン共有記憶装置２１０ｂを用いてウェブサイトアプリ２１２へトランザクションＯＴＰを転送する。しかしながら、望ましい場合には、ユーザは、ＯＴＰを自動的に記入してもらうのではなく、トランザクションＯＴＰをセキュリティウィンドウ１２０からウェブサイトアプリ２１２によって表示されるウェブサイトウィンドウに提示されるページへ手動でコピーするように要求される可能性もあることは理解されるべきである。何れの場合も、表示されたウェブサイトページにＯＴＰが記入された後、ユーザが「ログイン完了」をクリックすると、ウェブサイトアプリ２１２は、通信チャネル１３２を介してウェブサイト１３０へトランザクションＯＴＰを送る。

【００７２】

ログインＯＴＰの場合と同様に、トランザクションＯＴＰも、有益なことには、ウェブサイト商業者識別子、即ちマーチャントｉｄおよびＰＩＮの組合せを用いてペーストボードへ書き込まれることが可能である。マーチャントｉｄ．ＰＩＮは、先に書き込まれたあらゆるマーチャントｉｄ．ＰＩＮに上書きされる。また、ウェブサイトアプリ２１２は、セキュリティアプリ、即ち２ＣＨＫクライアント２１０のパブリックペーストボードが存在するかどうかをチェックし、存在すれば、ペーストボードをポーリングして新しいトランザクションＯＴＰが存在するかどうかを確認することも留意されるべきである。ウェブサイトアプリ２１２は、これを見つけると、ウェブサイト１３０へ送信を行う。ウェブサイト１３０は、トランザクションＯＴＰに関するその固有の検証を行った後に、成功または失敗メッセージを戻す。

【００７３】

セキュリティウィンドウに表示する目的でセキュリティサーバのブラウザアプリケーション２０７またはセキュリティアプリケーション２１０または３１０から送信されるトランザクション情報の完全性をさらに保護するために、トランザクション情報は、検出、特に送信される情報の一部のみの検出もなしには改竄が困難であるプレゼンテーション形式を利用して送られることが可能である。この点に関して、改竄は、テキストよりも音声記録および画像の方が遙かに困難である。

【００７４】

例えば、複雑な音声操作ソフトウェアおよびユーザが認識可能な同じ音声へのアクセスまたは知識の双方を有する攻撃者でなければ、セキュリティサーバ１４０において作成された、ユーザが認識可能な特有の音声で発生される「ジョンへの１０００ドルの支払いに同意する場合は、３４５６７を入力してください」という言い回しの音声記録を「エバンへの１０００ドルの支払いに同意する場合は、３４５６７を入力してください」に変更することは極めて困難であると思われる。セットアップの間にユーザにより選択されるもの等の特有の音声または背景画がユーザとの双方向通信において一貫して使用されれば、如何なる変更もユーザによってより容易に検出されるものと思われる。

【００７５】

本発明の別の態様によれば、トランザクション詳細は、ユーザには理解できるが連続したテキストよりも操作が困難な形式で提示される。例えば、トランザクション詳細は、セ

キュリティウィンドウ１１０において、トランザクション詳細が内部に埋め込まれたユーザ認識可能音声の音声ストリームとして、またはトランザクション詳細が内部に埋め込まれたユーザ認識可能背景を利用する画像として提示されることが可能である。さらに、情報は、先に述べたように、セキュリティウィンドウ１１０において、音声ストリームおよびピクチャの双方を含むマルチメディア提示として提示されることが可能である。この場合、ユーザは次に、提示されたトランザクション詳細とユーザがトランザクション詳細であると理解するものとが一致するか否かを決定する前に、この提示からトランザクション詳細を抽出するように要求される。またさらに、セキュリティサーバは、コンテンツを、例えば感知された、または決定されたリスクに依存して、テキストのみ、または画像のみ、または音声ストリームのみ、または画像と音声ストリームとを含むマルチメディア、またはマルチメディアのオプションが付いたテキスト、またはテキストのオプションが付いたマルチメディア、他を含む様々な方法のうちの任意の方法で提示するように構成されることが可能である。

【００７６】

また、２ＣＨＫシステムは、ユーザが開始するトランザクション用に適合されることも可能である。しかしながら、このようなトランザクションは、典型的には、２ＣＨＫシステムとの関連付けを有するユーザ、即ちセキュリティサーバ１４０との間に事前に確立されかつ現時点で機能している関連付けを有するユーザに限定される。また、ユーザが開始するトランザクションも、典型的には、２ＣＨＫシステムとの関連付けを有する企業、即ちセキュリティサーバ１４０と共に２ＣＨＫログインおよび／またはトランザクションＯＴＰの生成に使用される秘密を共有する企業等の、セキュリティサーバ１４０との間に事前に確立されかつ現時点で機能している関連性を有する企業に限定される。

【００７７】

より具体的には、このモデルにおいて、エンドユーザは、セキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０を介して、例えばウェブサイト１３０により代表される存在である企業とのトランザクションを開始する。これを行うために、ユーザは、先に述べたように、そのコンピュータ装置または補助的ハードウェア上のセキュリティアプリケーション２１０または３１０を起動する。

【００７８】

起動段階が首尾良く完了した後、ユーザは、例えばセキュリティウィンドウ１２０において利用可能な参加企業のプルダウンリストから、ユーザが開始を希望するトランザクションの相手企業を選択することができる。またユーザは、例えばセキュリティウィンドウ１２０において利用可能なプルダウンリストから、開始されるべきトランザクションのタイプ、例えば送金、残高照会、商品購入、情報受信またはクーポン入手、他、も選択する。ユーザは、次に、セキュリティウィンドウ１２０においてこのトランザクションタイプに関連する情報を入力し、送信を押す。企業およびトランザクションタイプの識別に加えて、関連するトランザクション情報は、例えば、（ｉ）転送されるべき金額、送金元口座および送金先口座の口座番号、または（ｉｉ）残高照会が希望される口座の口座番号、または（ｉｉｉ）購入されるべき商品の識別子、その価格およびその配送先であり得る。メッセージおよびコンテンツの構成は、例えば、クイックレスポンス（ＱＲ）コードまたはＮＦＣスキャンから拾い出されてもよい。

【００７９】

入力されたトランザクション情報は、通信チャネル１４４を介して、かつ妥当であれば通信リンク３２０を介してセキュリティサーバ１４０へ送信される。セキュリティサーバは、次に、このトランザクション情報を例えばウェブサイト１３０である適切な企業へ通信チャネル１３４を介して転送する。所定の実現形態において、セキュリティサーバは、トランザクション情報と共に、ユーザに関するリスク情報も送信することが望ましい場合がある。何れにしても、企業は、例えばログイン認証およびトランザクション署名のためのユーザによるセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３２０の進行中の使用に基づいて、適用可能なユーザと２ＣＨＫシステムとの間に既存の

関連付けが存在することを通知されるか、事前に気づかされている。したがって、企業は、要求者との信用（２ＣＨＫ関連付け）を有する存在、即ちセキュリティサーバ１４０から、認識可能なコンテンツを有する構造化されたメッセージにおいてトランザクション要求を受信するのが有利である。

【００８０】

例えばウェブサイト１３０である企業は、トランザクション要求を受け入れるか拒絶することができ、かつ通信チャネル１３４を介してセキュリティサーバ１４０へステータスを返す。セキュリティサーバ１４０は、このステータスメッセージをセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０へ通信チャネル１４４を介して、かつ妥当であれば通信リンク３２０を介して送る。セキュリティアプリケーションは、ステータスメッセージをセキュリティウィンドウ１２０においてユーザに提示する。

【００８１】

望ましい場合には、例えばウェブサイト１３０である企業は、トランザクション要求を受け入れる、または拒絶する前に、ＯＯＢＡ、ＫＢＡまたはテキストメッセージのトランザクションＯＴＰによるユーザの追加認証も要求してもよい。その場合、ユーザは、（ｉ）セキュリティウィンドウ１２０において、要求された情報（例えば、ユーザがＯＯＢＡサーバ１５０を介してセキュリティサーバ１４０から受信したトランザクションＯＴＰ、または例えばウェブサイト１３０である企業から直接受信したテキストメッセージ内のトランザクションＯＴＰ）を入力するか、または（ｉｉ）企業から直接電話を受ける。ＯＴＰが入力されれば、これは、セキュリティウィンドウ１２０からセキュリティサーバ１４０を介して例えばウェブサイト１３０である企業へ転送される。

【００８２】

例えばウェブサイト１３０である企業は、返されたＯＴＰに基づいて、またはユーザが電話呼を取ることに基づいてトランザクションを完了するか否かを決定し、通信チャネル１３４を介してセキュリティサーバ１４０へステータスを返す。セキュリティサーバ１４０は、次に、このステータス情報を、セキュリティウィンドウ１２０における表示のためにセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０または３１０へ送る。

問い合わせ型トランザクション

【００８３】

「問い合わせ型」トランザクションは、ユーザが、自分がユーザであると言う者であることについてさらに大きな信頼を与えるために実行されることが可能である。より具体的には、「問い合わせ型」トランザクションは、セキュリティサーバ１４０に対し、安全な通信チャネル１４４を利用して、企業が、共有秘密、居場所情報および生体情報識別子を含むが但しこれらに限定されないウェブサイト１３０によるアクセスが可能な識別情報と、比較できる追加的な認証情報を、捕捉するように要求することによって、識別の結び付きにおいて適用可能な企業を「堅固にする」、即ち適用可能な企業にさらなる信頼を与えるために、例えばウェブサイト１３０である任意の企業によりセキュリティサーバ１４０へ通信チャネル１３４またはチャネル１３２および１４２を介して、任意の後続する時間に、即ち起動後に送られることが可能である。

【００８４】

例えばウェブサイト１３０である企業は、指標としてユーザの電話番号またはそのハッシュを用いて、通知／追認／署名／問い合わせトランザクションを送ることができる。したがって、複数の関連付けを用いて識別の結び付きを堅固にすることができる。

【００８５】

例えば、ユーザが既にセキュリティサーバ１４０によって検証されかつ安全な通信チャネル１４４が確立された後の任意の時点で、ウェブサイト１３０は、安全な通信チャネル１３４または通信チャネル１３２および１４２を介してセキュリティサーバ１４０へ問い合わせを送信し、ユーザに、「あなたの郵便番号は何ですか？」または「好きな色は何ですか？」または「あなたの企業パスワードは何ですか？」等の１つまたは複数の質問また

は企業自体が、ユーザとの間に既に有する個別の関連性を介して企業が知る情報に基づいてセキュリティサーバ１４０により安全な通信チャネル１４４を介して通信相手であるユーザを別個に認証できるようにする他の何らかの１つまたは複数の問い合わせをすることができる。セキュリティサーバ１４０は、受信された企業の問い合わせを、セキュリティウィンドウ１２０においてユーザへ提示するために、安全な通信チャネル１４４を介してユーザへ送信する。ユーザは、提示された企業の問い合わせに対する回答をセキュリティウィンドウ１２０に入力し、セキュリティアプリケーションは、安全な通信チャネル１４０を介するセキュリティサーバ１４０への回答の送信を指令する。セキュリティサーバ１４０は、さらに、受信された回答をウェブサイト１３０へ、安全な通信チャネル１３４を介して、またはチャネル１３２および１４２を介して送信する。ウェブサイト１３０は、次に、受信された回答を、ユーザをさらに認証するために、即ちユーザが実際に、自分がユーザであると言う者であることをさらに追認するために知っている問い合わせに対する正解と比較する。

システムアーキテクチャの柔軟性

【００８６】

本システムは、ウェブサイト１３０が任意の所定のトランザクションに適するフォームファクタを要求または選択することを可能にする柔軟なアーキテクチャで実現されることが可能である。例えば、ユーザは、２つ以上の異なるタイプのコンピュータ装置上に、例えばそのスマートフォン、デスクトップおよび／または補助的ハードウェア上で同時に実行されるセキュリティウィンドウ１１０を同時に有することができる。大部分のトランザクションは、そのデスクトップのセキュリティウィンドウ１１０へ送られることが可能（それが遙かに便利）であるが、よりリスクの高いトランザクションは、そのスマートフォンのセキュリティウィンドウ１１０へ送られることが可能である。最もリスクの高いトランザクションは、その補助的ハードウェアへと送られる場合もある。

【００８７】

再度、図１を参照すると、図示されているように、各ウェブサイト１３０は、ウェブサイト１３０上で動作可能なセキュリティアプリケーションのプログラミングインタフェース（ＡＰＩ）１３５を有するのが有利である。ユーザが任意のウェブサイト１３０を訪れている場合、ユーザは、セキュリティＡＰＩ１３５を用いて、セキュリティウィンドウ１１０を介してセキュリティサーバ１４０へ暗号化されたトランザクションを送ることによりトランザクション認証を要求することができる。

【００８８】

先に述べたように、セキュリティウィンドウ１１０は、少なくとも３つのフォームファクタ、即ち（１）デスクトップまたはラップトップ・コンピュータ装置上で実行されるブラウザアプリケーション２０７によって制御され、ソフトウェアのダウンロードを必要としないポップアップ・セキュリティ・ウィンドウ、（２）スマートフォンまたは他のスマートモバイル通信デバイス上、または補助的ハードウェア上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０（「セキュリティアプリ」２１０と称されることが多い）によって制御されるセキュリティウィンドウ、および（３）デスクトップまたはラップトップ・コンピュータ装置上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０によって制御されるセキュリティウィンドウ、のうちの任意の１つで実現されることが可能である。

【００８９】

同一のユーザは、有益なことには、異なる時間に異なるフォームファクタを用いることができる。例えば、セキュリティアプリケーション、即ち２ＣＨＫクライアント２１０をデスクトップ上にインストールしていて、ほとんどの時間にこれを用いるユーザは、他の何らかのデスクトップにあるブラウザ・ポップアップ・セキュリティ・ウィンドウを用いることができる（ローミング）。所定の高リスクのトランザクションでは、ウェブサイトは、ユーザのスマートフォン上で実行されるセキュリティアプリ２１０によって制御されるセキュリティウィンドウ１２０上にトランザクションを示すことを要求する場合もあり

、一方で大部分のトランザクションは、ユーザのデスクトップ上で実行されるセキュリティアプリケーション２１０によって制御されるセキュリティウィンドウ１２０に示される。ソフトトークンとは異なり、セキュリティウィンドウ１２０または２ＣＨＫクライアント自体は、いかなるユーザ秘密をも含まない。フォームファクタに依存して、セキュリティウィンドウ１２０は、ブートアップ時間においてユーザに対して自動的に開始されることが可能であり、または、例えばデスクトップまたはスマートフォン上、または例えばブラウザ・ポップアップ・バージョンの場合のブックマーク上で実行されるセキュリティアプリケーション、即ち２ＣＨＫクライアント２１０に対しては、ユーザがアプリケーションアイコンをクリックすることによって手動で開始されることが可能である。

【００９０】

先に詳しく論じたように、ユーザは、セキュリティウィンドウ１２０に表示されるログインＯＴＰまたはトランザクションＯＴＰを切り取って、ＯＴＰを要求する、ブラウザ２０７またはウェブサイトアプリケーション２１２により表示されるウェブサイトウィンドウ１１０へ貼り付ける、または他の方法で挿入することができる。ユーザは、セキュリティウィンドウ１２０を介してセキュリティサーバ１４０へ、トランザクションが有効／無効であることを、例えばユーザがトランザクションを進めることを希望する、またはトランザクションの確認を拒絶する、という確認を行なうことによって伝えることもできる。しかしながら、セキュリティウィンドウ１２０が単にユーザにトランザクションを示すためにも使用され得ることは認識されるべきである。したがって、セキュリティウィンドウ１２０は、異なる形式を取ることができき、例えば、ある形式では、ユーザにトランザクションの表示を提示しかつユーザにウェブサイトへログインする、またはウェブサイトとのトランザクションに署名するためのＯＴＰを提供し、別の形式では、ユーザにトランザクションの表示を提示しかつユーザによるトランザクションの確認を要求し、かつさらに別の形式では、単にユーザにトランザクションの表示を提示し、ユーザはさらなる行動を何ら要求されない。

【００９１】

ウェブサイト１３０へ参加すると、セキュリティＡＰＩ１３５は、下記の機能ステップを遂行するように実行されるのが有利である。

１．ウェブサイト１３０がｔｒａｎｓａｃｔｉｏｎ＿ｒｅｑｕｅｓｔ（）ＡＰＩを呼び出し、ｔｒａｎｓａｃｔｉｏｎ＿ｒｅｑｕｅｓｔ（）ＡＰＩは暗号化されたｔｒａｎｓａｃｔｉｏｎ＿ｒｅｑｕｅｓｔを返す。トランザクション自体（単にトランザクションＯＴＰの要求でもあり得る）に加えて、ウェブサイト１３０は、（ｉ）単にユーザにトランザクションを表示すること、または（ｉｉ）ユーザがセキュリティウィンドウ１１０において「ＯＫ」をクリックする、またはユーザがセキュリティウィンドウ１１０に表示されるトランザクションを承認するという何らかの対応する指示を提供することを保証すること、または（ｉｉｉ）トランザクション署名を入手すること、の何れを希望するかを示す。

２．暗号化されたトランザクションは、次に、セキュリティサーバ１４０へ、ユーザのブラウザ２０７またはウェブサイトアプリケーション２１２を介して、またはセキュリティサーバ１４０とウェブサイト１３０との間の直接的な通信チャネル１３４を介して直に、の何れかで伝えられる。

３．セキュリティサーバ１４０は、トランザクションを復号し、真正性を検証しかつ次に、ユーザへのセキュリティウィンドウ１１０におけるトランザクションの表示を指令する。先に述べたように、トランザクション署名が要求されていれば、セキュリティサーバ１４０は、トランザクションＯＴＰを計算し、かつそのトランザクションＯＴＰのセキュリティウィンドウ１１０におけるユーザへの表示も指令する。

４．セキュリティサーバ１４０は、次に、暗号化されたｔｒａｎｓａｃｔｉｏｎ＿ｒｅｓｐｏｎｓｅを準備し、最初の送信に応答してこれをブラウザ２０７またはウェブサイトアプリケーション２１２へ送り返し、ブラウザ２０７またはウェブサイトアプリケーション２１２は、次に暗号化されたｔｒａｎｓａｃｔｉｏｎ＿ｒｅｓｐｏｎｓｅをウェブサイト１３０へ送信する。

５．ウェブサイト１３０は、次に、ｔｒａｎｓａｃｔｉｏｎ＿ｖｅｒｉｆｙ（）ＡＰＩを呼び出し、ｔｒａｎｓａｃｔｉｏｎ＿ｖｅｒｉｆｙ（）ＡＰＩは、結果をそのウェブサイトへ返す。

暗号鍵の管理

【００９２】

２ＣＨＫシステムの要は、ユーザのコンピュータ装置１００、例えばユーザのＰＣまたはスマートモバイル通信デバイス上のセキュリティウィンドウ１２０と、セキュリティサーバ１４０との間に安全な暗号化されかつ独立した通信チャネル１４４を確立することである。

【００９３】

暗号鍵の生成は、次のようにして達成されてもよい。セキュリティウィンドウ１２０が起動された後の何らかの時点で、ＫＭＬＣ２１３または３１３は、秘密鍵／公開鍵ペア、例えばＤｕ／Ｐｕを生成し、かつ秘密鍵Ｄｕを安全に（典型的には、メモリに）、例えばプライベートストレージ２１０ａまたは３１２に格納する。ＫＭＬＣ２１３または３１３は、公開鍵Ｐｕをセキュリティサーバ１４０へ安全なチャネル１４４および妥当であればリンク３２０を介して送り、セキュリティサーバ１４０において、送信は、ＫＭＬＳ１４７によって傍受される。ユーザの公開鍵Ｐｕを含むデジタル証明書（「Ｃｅｒｔ」）は、ＫＭＬＳ１４７によって準備され、次の２つのうちの一方が発生する。

【００９４】

ＫＭＬＳ１４７が中間またはルート認証局として行動することができれば、これは、証明書に署名し、かつ署名された証明書をＫＭＬＣ２１３または３１３へ返し、ＫＭＬＣ２１３または３１３は、これをプライベートストレージ２１０ａまたは３１２等で局所的に（好ましくは、メモリに）保持する。例えば、ＫＭＬＳ１４７は、Ｃｅｒｔにその秘密／公開鍵ペアＤｓ／Ｐｓのうちの秘密鍵Ｄｓで署名することができ、よって、［Ｃｅｒｔ］ＤｓがＫＭＬＣ２１３または３１３へ安全なチャネル１４４および妥当であればリンク３２０を介して返される。

【００９５】

一方で、ＫＭＬＳ１４７が「登録局」として行動すれば、これは、通信チャネル１４８を介して外部の認証局１７０へ証明書要求を転送し、認証局１７０は、証明書を作成しかつこれを同じ通信チャネルを介してＫＭＬＳ１４７へ返す。ＫＭＬＳ１４７は、次に、通信チャネル１４４を介して証明書をＫＭＬＣ２１３または３１３へ転送し返し、ＫＭＬＣ２１３または３１３は、これを局所的に（好ましくは、メモリに）、例えばプライベートストレージ２１０ａまたは３１２内に保持する。このような場合、Ｃｅｒｔは、認証局によりその秘密／公開鍵ペアＤｃａ／Ｐｃａのうちの秘密鍵Ｄｃａで署名され、よって［Ｃｅｒｔ］ＤｃａがＫＭＬＳ１４７へ返される。ＫＭＬＳ１４７は、次に、受信された署名入りＣｅｒｔ、即ち［Ｃｅｒｔ］Ｄｃａを安全なチャネル１４４を介して、および妥当であればリンク３２０を介してＫＭＬＣ２１３または３１３へ転送する。

【００９６】

何れの例においても、発行されるＣｅｒｔは、比較的短命、即ち一時的であって、２ＣＨＫセッション自体の寿命に一致することが好ましい。鍵の生成を起動と同時的にして単純化することにより、デジタル証明書および秘密鍵を局所的に長い期間に渡って格納する必要性が回避される。

【００９７】

状況によっては、後により詳しく論じるように、秘密鍵および証明書は、同じコンピュータ装置１００上の他のアプリケーション、例えばブラウザ２０７または例えば文書プロセッサ２１８である非ブラウザアプリケーションによって必要とされてもよい。基本的なオペレーティングシステムが、ＭＳ　Ｗｉｎｄｏｗｓ（商標）またはＡｐｐｌｅ　ＭａｃＯＳ（商標）がそうであるように、標準的な鍵ストアをサポートしていれば、ＫＭＬＣ２１３または３１３に、鍵を鍵ストアへ格納しかつ適宜これらを削除するというタスクが課される可能性がある。

【００９８】
公開鍵暗号化に適する上述の鍵、即ち非対称鍵の生成に加えて、鍵管理システムは、対称鍵も生成しかつ配分することができる。これの要は、ＫＭＬＳ１４７内に組み込まれる関数Ｓｈａｒｅｄ＿Ｓｅｃｒｅｔ＿Ｇｅｎｅｒａｔｏｒ（）であり、これは、入力としてユーザＩＤ（おそらくは、ユーザの有線または携帯電話番号）、セキュリティサーバ１４０のみに知られる長寿命の秘密および他の種々雑多のパラメータ等のファクタを取り入れ、かつ出力としてｓｈａｒｅｄ＿ｓｅｃｒｅｔ　Ｋを生成する。所定の入力セットに関しては、同じ共有秘密が確定的に計算される点に留意することが重要である。ＫＭＬＳ１４７に対しては、認証された異なる存在が、ＫＭＬＳ１４７へ妥当な入力パラメータを提供することにより、妥当な対称鍵を提供するように要求することができる。
【００９９】
アプリケーションに依存して、鍵管理ロジックは、上述の非対称（即ち、公開）鍵暗号化方式および対称鍵暗号化方式の機能の一方または双方を利用する場合があることに留意されたい。
【０１００】
以下、鍵管理を２ＣＨＫアーキテクチャの上へ層化し得る有益な方法について、幾つかの例を述べる。
【０１０１】
第１の例は、デジタル署名に関する。デジタル署名を必要とするアプリケーションでは、ユーザは、秘密鍵およびデジタル証明書、即ちユーザの識別と認証局により証明された公開鍵との結び付きを提供される必要がある。セキュリティサーバを含むいかなる第三者にも知られていないこのような秘密鍵の使用は、ある種のアプリケーションに必要である強力な否認防止を提供する。以下、公開鍵暗号化方式で作成される産業協定署名を、「デジタル署名」と称する。当業者には理解されるように、かつ先に論じたように、先に述べたトランザクションＯＴＰ等の共有秘密を用いる基本的な対称暗号化方式に基づくトランザクション署名は、通常「電子署名」と称される。
【０１０２】
別の例は、鍵の配布に関連する。
【０１０３】
さらに別の例は、暗号化文書の配布に関連する。ユーザへ暗号化されたファイル、例えば証券取引明細書のＰＤＦが送られると、ユーザは、ファイルの暗号化に使用された鍵を提供される必要がある。
【０１０４】
これらの全ての例において、鍵管理は、システムのコスト高に直結し、かつ間接的にセキュリティに影響する。鍵の生成、配布および保持が、同時的に必要となる。鍵は、紛失、改竄または盗難の可能性があることから、鍵管理は通常、コストの重大な部分を占め、かつシステムの脆弱な点となる。
【０１０５】
鍵管理システムをその鍵生成機能を含めて記述したが、鍵管理機能の利用方法は、以下の３つのアプリケーション例によってさらに理解されるであろう。
【０１０６】
第１の例は、デジタル署名のための２ＣＨＫシステムの使用に対処する。所定のアプリケーションでは、公開鍵暗号化方式を用いるデジタル署名が電子トランザクション署名より適切であるとされている。デジタル署名を達成するために、エンドユーザは、ブラウザ２０７またはウェブサイトアプリケーション２１２を用いて閲覧し、かつウェブサイト１３０とのトランザクションを実行する。ウェブサイト１３０は、ＫＭＬＷＳ１３７を用いて、必要とされる「デジタル署名」によるトランザクション署名を要求する。この要求は、安全なバックエンド通信チャネル１３４上でＫＭＬＳ１４７へ送られる。この要求は、次に、デジタル署名が必要とされていることの指示と共にＫＭＬＳ１４７から安全なチャネル１４４、および妥当であればリンク３２０を介してＫＭＬＣ２１３または３１３へ送

られる。トランザクション署名、即ちトランザクションＯＴＰは、場合により、セキュリティサーバ１４０によって生成され、かつデジタル署名要求と共に、セキュリティウィンドウ１２０に表示するために持続的で安全な通信チャネル１４４および妥当であればリンク３２０を介してセキュリティアプリケーション２１３または３１３へ送られ、次いで、ユーザのコンピュータ装置１００、例えばユーザのＰＣまたはスマートフォン、他に表示される。

【０１０７】

セキュリティウィンドウ１２０は、通常通りユーザにトランザクションを示し、かつ場合により、ユーザにトランザクションＯＴＰ、即ち電子署名を、ブラウザアプリケーション２０７またはウェブサイトアプリケーション２１２によって表示されるウィンドウ１１０へコピーするように要求する。並行して、ＫＭＬＣ２１３または３１３は、トランザクションのハッシュ（「ＨａｓｈＴｒａｎ」）を計算し、かつ先にメモリに格納されたユーザの秘密鍵Ｄｕを用いてデジタル署名を計算する。結果は、［ＨａｓｈＴｒａｎ］Ｄｕとなる。この処理は、舞台裏で、またはトランザクションへの署名に同意するようにユーザに求めることによって、発生する可能性もある。何れの場合も、秘密鍵Ｄｕは、ハッシュされたトランザクション［ＨａｓｈＴｒａｎ］へ適用される。デジタル署名されたトランザクションのハッシュ［ＨａｓｈＴｒａｎ］Ｄｕは、次に、安全な通信チャネル１４４および妥当であればリンク３２０を介してＫＭＬＣ２１３または３１３からＫＭＬＳ１４７へ、デジタル証明書［Ｃｅｒｔ］Ｄｓまたは［Ｃｅｒｔ］Ｄｃａと共に送られる。

【０１０８】

ＫＭＬＳ１４７は、場合により、ユーザの公開鍵Ｐｕをデジタル署名［ＨａｓｈＴｒａｎ］Ｄｕへ適用してＨａｓｈＴｒａｎを取得し、かつこれを独自に生成されたＨａｓｈＴｒａｎと比較することにより、署名の検証を遂行することができる。検証遂行の有無に関わらず、ＫＭＬＳ１４７は、署名、即ち［ＨａｓｈＴｒａｎ］Ｄｕおよび証明書、即ち［Ｃｅｒｔ］Ｄｓまたは［Ｃｅｒｔ］Ｄｃａを、安全なチャネル２３４を介してＫＭＬＡＰＩ４２０へ転送する。

【０１０９】

ＫＭＬＷＳ１３７は、ハッシュＨａｓｈＴｒａｎを再計算し、かつデジタル証明書Ｃｅｒｔに含まれるユーザの公開鍵Ｐｕを用いて署名を検証することができる。したがって、ＫＭＬＷＳ１３７は、ＫＭＬＳ１４７の公開鍵Ｐｓを［Ｃｅｒｔ］Ｄｓへ適用し、または認証局公開鍵Ｐｃａを［Ｃｅｒｔ］Ｄｃａへ適用してＰｕを回復する。ＫＭＬＷＳ１３７は、次に、回復されたＰｕを［ＨａｓｈＴｒａｎ］Ｄｕへ適用してＨａｓｈＴｒａｎを回復し、かつこれを独自に生成されたＨａｓｈＴｒａｎと比較して署名を検証する。

【０１１０】

上述の説明では、ハッシュがＫＭＬＣ２１３または３１３において作成されることに留意されたい。これは、ＫＭＬＷＡ１３７またはＫＭＬＳ１４７においても同じく容易に作成される可能性もあるが、これらの存在は各々、その真正について確信を得るためにハッシュを再計算する可能性が高い。

【０１１１】

この例では、トランザクション全体がセキュリティウィンドウ１２０に至る。一方で、この手法を用いて文書に署名する必要があれば、ＫＭＬＣ２１３または３１３に秘密鍵および公開鍵をユーザのコンピュータ装置１００上で利用可能な鍵ストアへ格納させるように、機能を拡張することが可能であり、これにより、鍵は、他のアプリケーション、例えばスマートフォンアプリを含むブラウザまたは非ブラウザアプリケーションで利用可能になる。ＫＭＬＣ２１３または３１３は、ユーザ鍵を適時鍵ストアから削除することを担当すると思われる。

【０１１２】

第２の例では、２ＣＨＫシステムが鍵配布に使用される。ｅメールのように、データが格納および転送システムにおいて暗号化されかつ受信者へ転送されることは、頻繁に発生する。例えば、法規は、財務諸表または健康記録等の文書がｅメールへの添付ファイルと

して送信される場合、これらを必ず暗号化して送信することを求めている。多くのアプリケーション、例えばＷｉｎＺｉｐ（商標）およびＡｃｒｏｂａｔ　Ｒｅａｄｅｒ（商標）は、埋込みパスワードをベースとする暗号化機能を有する。すると、復号パスワードをどのようにしてユーザへ送信するか、に関して問題が生じる。１つの手法は、共有パスワードに対して事前に合意することである。この手法の欠点は、不正侵入されたパスワードを用いて多くの文書が復号される可能性があることにあるが、複雑なパスワードを要求することもまた、ユーザがパスワードを忘れる可能性が高いために困難である。以下、２ＣＨＫ鍵管理を用いてこの問題点を解決する３手法について述べる。

【０１１３】

第１の手法では、例えば一意のＤｏｃｕｍｅｎｔＩＤによって一意に識別された文書が、ウェブサイト１３０により、ＰＩＮ、例えば英数字８文字のＰＩＮから導出される鍵を用いて暗号化され、次いで、例えばｅメールを介してユーザへ送られる。この議論のの目的においては、ＤｏｃｕｍｅｎｔＩＤは、送信者識別、受信者識別および文書識別の特定の組合せに関連づけられる一意の値である。ユーザが文書を何らかの非ブラウザアプリケーション２１８を用いて、典型的には、例えばＷｉｎＺｉｐ（商標）およびＡｃｒｏｂａｔ　Ｒｅａｄｅｒ（商標）であるそのＰＣ上のソフトウェアアプリケーションを用いて開くと、プログラムは、ウェブサイト１３０へ、ユーザが特定の文書を読もうとしていることを示す信号を送る。アプリケーション２１８が、代わりにブラウザ２０７であることも可能ではあるが、本議論のの目的においては、これは、非ブラウザソフトウェアであることが想定されている。

【０１１４】

ウェブサイト１３０は、ＤｏｃｕｍｅｎｔＩＤにより参照された文書を最初に暗号化したＰＩＮを検索し、次いで、ＫＭＬＷＳ１３７を用いてこのＰＩＮをセキュリティサーバ１４０へ通信リンク１３４を介して送る。セキュリティサーバ１４０は、ＫＭＬＳ１４７を用いてＰＩＮをＫＭＬＣ２１３または３１３へ通信チャネル１４４および妥当であればリンク３２０を介して転送し、ＰＩＮは、次に、セキュリティウィンドウ１２０内でユーザへ表示される。

【０１１５】

ユーザは、ＰＩＮをアプリケーション２１８へコピーし、復号が通常通りに進行する。一般に、アプリケーション２１８の変更が要求されないことは注目されるべきである。開かれた時点でウェブサイト１３０へのメッセージをもたらす能力は、多くのアプリケーション（例えば、Ａｄｏｂｅ　Ｒｅａｄｅｒ）へ既に埋め込まれている機能である。

【０１１６】

上述の手法における１つの欠点は、ウェブサイト１３０がＤｏｃｕｍｅｎｔＩＤおよびＰＩＮのリストを保持しなければならないことにある。

【０１１７】

この問題点を解決する一方法は、第２の手法を用い、かつ各文書の暗号化に用いる鍵を、ＤｏｃｕｍｅｎｔＩＤおよびウェブサイト１３０にのみ知られる長期間の秘密を入力として取る関数の結果とすることである。この方法では、鍵は、第１の手法で説明したように、ユーザが文書を開こうとした後に動的に生成されることが可能である。

【０１１８】

第２の手法の欠点は、文書が開かれるとウェブサイト１３０が利用可能であってオンラインになる、という想定が存在することにある。文書を生成して配布するある種のシステムは、バックエンドのバッチシステムであることから、この想定は、必ずしも適用可能でない場合がある。

【０１１９】

第３の手法では、２ＣＨＫ鍵管理の共有秘密生成機能を用いて、この問題点を次のように解決することができる。

【０１２０】

ウェブサイト１３０は、セキュリティサーバ１４０へ、暗号化を望むＤｏｃｕｍｅｎｔ

ＩＤを一度に一つずつ、またはより高い可能性としてバッチファイルで、の何れかで送る。この議論の目的においては、ファイルは、送信者ＩＤおよび受信者ＩＤ等のエンベロープ情報を含むことが想定される。ＫＭＬＳ１４７は、上述のＳｈａｒｅｄ＿Ｓｅｃｒｅｔ＿Ｇｅｎｅｒａｔｏｒ（）を用いてＤｏｃｕｍｅｎｔＩＤ毎に暗号鍵を計算する。例えばあるＤｏｃｕｍｅｎｔＩＤに対して鍵Ｋ１、他のＤｏｃｕｍｅｎｔＩＤに対して鍵Ｋ２、さらに他のＤｏｃｕｍｅｎｔＩＤに対して鍵Ｋ３、他、である。これらの鍵は、次に、ＫＭＬＳ１４７によってウェブサイト１３０へ返される。ウェブサイト１３０は、次に、個々の文書を妥当な鍵で暗号化し、かつ暗号化された文書を例えばｅメールを介して個々の妥当なユーザへ送る。

【０１２１】

妥当なユーザは、他のデスクトップソフトウェア２１８を用いて文書を開き、これにより、鍵要求が安全なウェブ接続（不図示）上で直接にセキュリティサーバ１４０へもたらされる。これが、セキュリティウィンドウ１２０を介さない非ブラウザアプリケーション２１８からセキュリティサーバ１４０への直接接続である点は留意されるべきである。

【０１２２】

この動作により、ＫＭＬＳ１４７は、Ｓｈａｒｅｄ＿Ｓｅｃｒｅｔ＿Ｇｅｎｅｒａｔｏｒ（）を用いて妥当な暗号鍵、例えばＫ１、Ｋ２、Ｋ３、他を再計算する結果となる。妥当な鍵は、次に、安全なチャネル１４４および妥当であればリンク３２０を介してＫＭＬＣ２１３または３１３へ送られ、先に述べたように、非ブラウザアプリケーション２１８により表示されるウィンドウへコピーするためにセキュリティウィンドウ１２０内でユーザに表示される。

【０１２３】

上述の説明は、非ブラウザ・ソフトウェア・アプリケーション２１８（例えば、Ａｃｒｏｂａｔ　Ｒｅａｄｅｒ）を用いて行ったが、ブラウザをベースとするウェブアプリケーションでも同じ機能を使用することができる。

暗号鍵のシード付与

【０１２４】

ユーザがワンタイムパスワード生成ツールまたはトランザクション認証ツールの何れかのためにトークン認証ツールを提供されると、ユーザのトークンは、共有秘密鍵を提供される必要がある。当業者は、この意味合いにおいて、共有秘密鍵が「シード」として特徴づけられる場合が多いことを認識するであろう。ＯＴＰおよびトランザクション認証トークンの「シード付与」には、先に述べた２ＣＨＫ鍵管理も使用されることが可能である。ＯＴＰおよびトランザクション認証トークン認証ツールは、全て、トークンに格納されかつバックエンドシステムにも格納される鍵を必要とする。これらの鍵（一般に、「シード」と称される）は、コストおよび複雑さをもたらす。２ＣＨＫ鍵管理は、この手順を大幅に単純化するために使用されることが可能である。

【０１２５】

この議論の目的においては、トークン認証ツール（不図示）は、ハードウェア、ソフトウェアまたは携帯電話アプリとして実現されることが想定される。トークンは、シードが存在しない（または、シードのリフレッシュが要求される）不活性状態で始動する。要求は、ユーザによりセキュリティウィンドウ１２０内部から、またはトークンから直接、通信チャネル１４４を介してセキュリティサーバ１４０へ、またはシードの付与を要求する外部ウェブサイト１３０へ、の何れかで行われる。ユーザを識別する幾つかの一意の識別子は、適宜セキュリティサーバ１４０またはウェブサイト１３０へ提供される。

【０１２６】

セキュリティサーバ１４０内部のＫＭＬＳ１４７は、一意のＵｓｅｒＩＤ、およびＫＭＬＳ１４７にのみ知られる長期間の秘密を含む他の情報を、Ｓｈａｒｅｄ＿Ｓｅｃｒｅｔ＿Ｇｅｎｅｒａｔｏｒ（）への入力として使用し、そのユーザのための一意のシード（即ち、鍵）を生成する。例えば、起動時毎にシードを「シード付与」することは、ユーザの電話番号（または他のＩＤ）および２ＣＨＫ事業者にのみ知られる秘密に基づいてシード

を生成することを含む可能性がある。このようなシードは、起動毎に生成し直されるが、生成される度に同じ値を有する。しかしながら、幾分か修正されたアルゴリズムを用いることにより、起動毎に異なる値を有するシードを生成することも可能である。

【０１２７】

このシードは、安全なチャネル２４４および妥当であればリンク３２０を介してＫＭＬＣ２１３または３１３へ送り返され、次に、セキュリティウィンドウ１２０においてユーザへ表示される。ユーザは、シードをソフトウェアまたはスマートフォンアプリのトークンへ入力する。実際のシードが、ユーザが入力するシードを変換する関数によって生成され得ることは、留意されるべきである。また、ハードウェアの場合、これは、トークンがキーパッドを有する場合に限って機能することも認識されるであろうが、実際に、大部分のトランザクション認証ツールはキーパッドを有する。

【０１２８】

上述の一変形例として、トランザクション認証ツールは、セキュリティアプリケーション２１０または３１０内へ機能の一部として直に組み込まれることが可能である点に注目されたい。一見して、この点の理論的根拠は明白ではないかもしれないが、ＥＭＶ／ＣＡＰ等の既存システムとの互換性は、この手法に理論的根拠を与える。トランザクション認証ツールのこのオンデマンドのシード付与は、付与のコストを大幅に単純化する。

【０１２９】

先に述べたように、補助的ハードウェア上のセキュリティアプリ、即ち２ＣＨＫクライアント３１０も、ＯＴＰトークンを生成するために先に述べた技術を用いて「シード付与」されることが可能である。これは、補助的ハードウェアがもはやコンピュータ装置１００へ接続されていない場合でも、これでＯＴＰを補助的ハードウェア上で安全に生成できることを意味する。これまでは、コンピュータ装置１００へ接続された補助的ハードウェア３００によるシード付与関連動作について詳述したが、以下、コンピュータ装置１００から外されている補助的ハードウェア３００によってこれらの動作をどの程度確実に実行できるかについて述べる。この議論の目的においては、トークン認証ツール（不図示）は、ハードウェアとして、ソフトウェアとして、または補助的ハードウェアアプリとして実現されることが想定される。

【０１３０】

トークンは、シードが存在しない（または、シードのリフレッシュが要求される）不活性状態で始動する。補助的ハードウェア３００がコンピュータ装置１００から外された後、コンピュータ装置１００へ接続された補助的ハードウェア３００によって受信されて格納されたシードは、望ましい場合には、セキュリティアプリ、即ち２ＣＨＫクライアント３１０により、補助的ハードウェア３００の画面３０２に表示されるセキュリティウィンドウ１２０においてユーザに示されることが可能である。ユーザは、次に、シードを補助的ハードウェア３００のＣＰＵ３０５によって実行されるトークン生成ツール（不図示）に入力することができる。この場合もやはり、実際のシードは、ユーザが入力するシードを変換する関数によって生成されてもよいことに留意する。また、ハードウェアトークン生成ツールの場合、これは、トークン生成ツールがキーパッドを有する場合に限って機能することも認識されるであろうが、実際に、大部分のトランザクション生成ツールはキーパッドを有する。

【０１３１】

先に述べたように、ＯＴＰの「シード付与」は、各起動時、即ち始動および起動ステージの間のシードを用いて実行される。具体的には、シード、即ち鍵は、ユーザの電話番号または他のユーザ識別子、およびセキュリティサーバ１４０にのみ知られる秘密に基づいて生成される。このシードは、起動時毎に生成し直されるが、同じ値を有することになる。

【０１３２】

ある代替手法は、最初の関連付けにおいて、即ちセットアップおよび個性化段階の間にシードを生成し、かつこのシードを局所的かつ持続的に、全体として又は部分的に、格納

することである。したがって、この代替手法では、シードは、新規起動毎に、再生成される必要がなく、その全体が再生成される必要もない。この手法の主たる利点は、攻撃者が自動転送または他の何らかの機構を用いてユーザの電話番号を盗み、かつ新規に起動しても、攻撃者がシードを知ることにはならない点にある。したがって、このシードを用いてトランザクションＯＴＰが生成されても、このシードを有していない攻撃者は阻止されることとなる。

【図１】

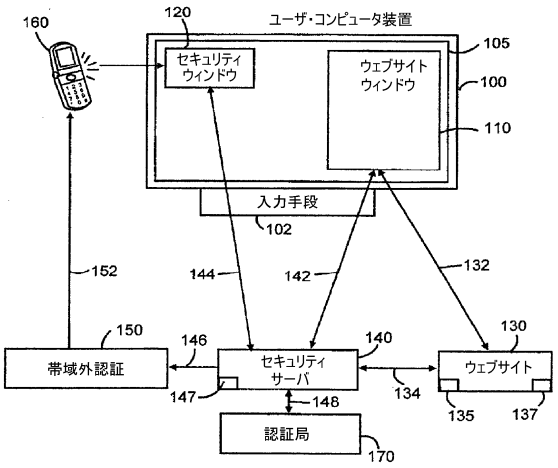

図1

【図２】

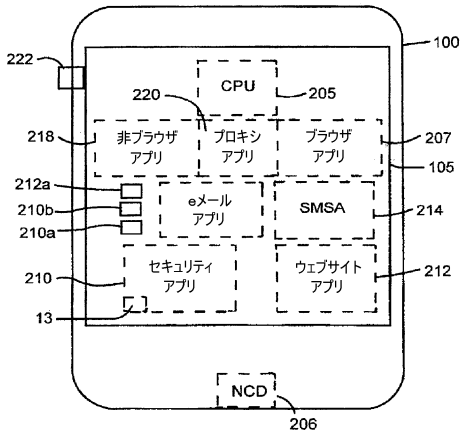

図2

【図３】

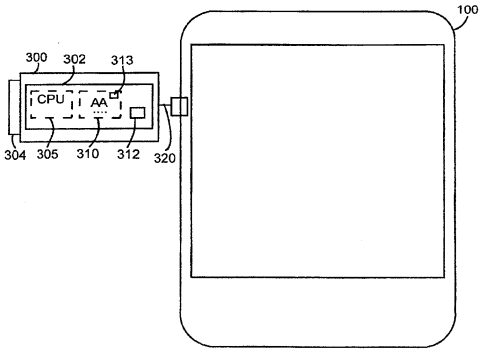

図3

フロントページの続き

(72)発明者　アンドリュー・ロバート・ロルフ
アメリカ合衆国　６０１１８　イリノイ州　イースト・ダンディー　ウェント・アベニュー　５３７番地　２４０号
(72)発明者　ラヴィ・ガネサン
アメリカ合衆国　３３４１０　フロリダ州　パーム・ビーチ・ガーデンズ　ガーデンズ・パークウェイ　３６１０番地　１２０４Ａ号

審査官　岸野　徹

(56)参考文献　特表２００３－５３４５８９（ＪＰ，Ａ）
特表２０１０－５３１５０６（ＪＰ，Ａ）
特表２０１３－５２７７０８（ＪＰ，Ａ）
特表２０１３－５１８３４８（ＪＰ，Ａ）
米国特許出願公開第２０１１／０１８５４０５（ＵＳ，Ａ１）
米国特許出願公開第２０１１／００２９４３６（ＵＳ，Ａ１）
米国特許出願公開第２０１１／０２６５１４９（ＵＳ，Ａ１）
米国特許出願公開第２０１１／０２８３３４０（ＵＳ，Ａ１）
特表２０１０－５１８５１５（ＪＰ，Ａ）
米国特許出願公開第２００９／０３２８１７０（ＵＳ，Ａ１）
特開２００２－０４１３９８（ＪＰ，Ａ）
特開２００６－１０９４５５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３３
Ｇ０６Ｆ　２１／６４
Ｈ０４Ｍ　１１／００