(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2015-519637
(P2015-519637A)
(43)公表日　平成27年7月9日(2015.7.9)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/31	(2013.01)	G06F	21/31		5B035
G06Q 20/40	(2012.01)	G06Q	20/40	110	5B072
G06F 21/34	(2013.01)	G06F	21/34		5K067
G06F 21/44	(2013.01)	G06F	21/44		
G06K 19/07	(2006.01)	G06K	19/07	230	

審査請求 未請求　予備審査請求 未請求　（全 42 頁）　最終頁に続く

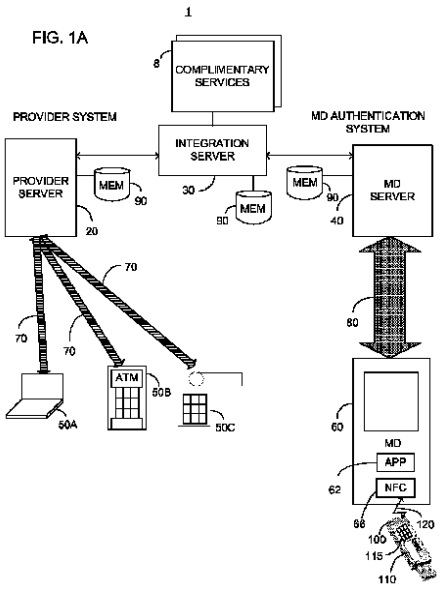
(21)出願番号　特願2015-505068 (P2015-505068)
(86)(22)出願日　平成25年4月10日 (2013.4.10)
(85)翻訳文提出日　平成26年12月3日 (2014.12.3)
(86)国際出願番号　PCT/IL2013/050318
(87)国際公開番号　WO2013/153552
(87)国際公開日　平成25年10月17日 (2013.10.17)
(31)優先権主張番号　13/442,861
(32)優先日　平成24年4月10日 (2012.4.10)
(33)優先権主張国　米国 (US)

(71)出願人　513290613
アクセルズ　テクノロジーズ　（２００９）　リミテッド
イスラエル国　４９５１１　ペタク　ティクバ、インバー　７
(74)代理人　100079108
弁理士　稲葉　良幸
(74)代理人　100109346
弁理士　大貫　敏史
(74)代理人　100117189
弁理士　江口　昭彦
(74)代理人　100134120
弁理士　内藤　和彦

最終頁に続く

(54)【発明の名称】モバイル機器による安全なトランザクションプロセスのためのシステム及び方法

(57)【要約】
ネットワークアドレスに関連するサーバと、利用者に関連する第１の装置であって、取得されるサーバのネットワークアドレスに応答して第１の通信チャネルを介してサーバと通信する、第１の装置と、第１の装置からサーバのネットワークアドレスを取得するように構成される、利用者に関連する第２の装置と、第２の通信チャネルを介して第２の装置と通信するモバイル機器サーバであって、第３の通信チャネルを介してサーバと通信する、モバイル機器サーバとから成り、モバイル機器サーバは、第２の通信チャネルを介して第２の装置からサーバのネットワークアドレスを取得し、サーバのネットワークアドレスを信頼できる情報源から取得し、それらのサーバのネットワークアドレスが一致する場合にのみ、第３の通信チャネルを介してトランザクションをサーバに承認するように構成される、装置によるトランザクションのセキュリティ強化をもたらすシステム。



【特許請求の範囲】
【請求項１】
装置によるトランザクションのセキュリティ強化をもたらすシステムであって、
ネットワークアドレスに関連するサーバと、
利用者に関連する第１の装置であって、第１の通信チャネルを介して前記サーバと通信し、前記サーバを介してトランザクションを要求し、前記サーバに関連するネットワークアドレスを取得するように構成される、第１の装置であり、、前記第１の通信チャネルは前記取得されたサーバに関連するネットワークアドレスに応答して確立される、第１の装置と、
前記利用者に関連する第２の装置であって、前記第１の装置と通信し、前記取得されたサーバに関連するネットワークアドレスを前記第１の装置から受信するように構成される、第２の装置と、
第２の通信チャネルを介して前記第２の装置と通信するモバイル機器サーバであって、第３の通信チャネルを介して前記サーバと通信する、モバイル機器サーバであり、
前記第２の通信チャネルを介して前記第２の装置から、前記取得され受信されたサーバに関連するネットワークアドレスを入力し、
前記サーバに関連するネットワークアドレスを信頼できる情報源から取得し、
前記取得され受信され入力されたサーバに関連するネットワークアドレスが、前記信頼できる情報源から取得された前記サーバに関連するネットワークアドレスと一致する場合にのみ、トランザクションを承認する
ように構成されるモバイル機器サーバと
を含む、システム。
【請求項２】
前記信頼できる情報源が前記サーバであり、前記サーバに関連するネットワークアドレスが前記第３の通信チャネルを介して前記サーバから取得される、請求項１に記載のシステム。
【請求項３】
前記信頼できる情報源が、前記モバイル機器サーバと通信するデータベースである、請求項１に記載のシステム。
【請求項４】
前記第１の通信チャネルが前記第２の通信チャネルと異なる、請求項１に記載のシステム。
【請求項５】
前記第１の装置及び前記第２の装置が単一の装置である、請求項１に記載のシステム。
【請求項６】
前記第１の装置及び前記第２の装置のうちの１つがユーザモバイル機器である、請求項１に記載のシステム。
【請求項７】
前記第１の装置及び第２の装置、前記ユーザ装置のうちの１つがコンピュータである、請求項１に記載のシステム。
【請求項８】
前記第１の装置がコンピュータであり、前記第２の装置がユーザモバイル機器である、請求項１に記載のシステム。
【請求項９】
前記第２の装置の前記第１の装置との通信が第４の通信チャネルを介し、前記第４の通信チャネルは前記第１、第２、及び第３の通信チャネルの何れとも異なる、請求項１に記載のシステム。
【請求項１０】
前記第４の通信チャネルが、無線認証通信及び近距離通信のうちの１つである、請求項９に記載のシステム。

【請求項１１】
前記第３の通信チャネルが、前記第１の通信チャネル及び前記第２の通信チャネルの何れとも異なる安全な通信チャネルである、請求項１に記載のシステム。
【請求項１２】
前記第２の装置と通信するように構成されるセキュリティ保護された要素を更に含み、前記セキュリティ保護された要素は、利用者のジェスチャに応答して、暗号化されたパスコードを前記第２の通信チャネルを介して前記モバイル機器サーバに提供するように構成される、請求項１に記載のシステム。
【請求項１３】
前記セキュリティ保護された要素と通信する入力装置を更に含み、前記入力装置を介した前記利用者のジェスチャにより、前記パスコードが前記セキュリティ保護された要素に与えられる、請求項１２に記載のシステム。
【請求項１４】
前記入力装置が専用の入力装置である、請求項１３に記載のシステム。
【請求項１５】
非接触要素を更に含み、前記セキュリティ保護された要素が前記非接触要素に含まれ、前記セキュリティ保護された要素と前記第２の装置との間の前記通信が前記非接触要素に応答したものである、請求項１３に記載のシステム。
【請求項１６】
前記モバイル機器サーバと通信する通知サーバを更に含み、前記第２の装置が自らの上にアプリケーションを有し、前記アプリケーションが前記通知サーバに応答し、前記アプリケーションが前記第１の装置のネットワークアドレス、及び前記取得され受信され入力されたサーバに関連するネットワークアドレスを提供するように構成される、請求項１に記載のシステム。
【請求項１７】
前記モバイル機器サーバと通信する追加のサーバを更に含み、前記追加のサーバは、前記第１の装置と前記サーバとの間の前記トランザクションの前記承認に応答して前記第１の装置との追加のトランザクションを承認するように構成される、請求項１に記載のシステム。
【請求項１８】
装置によるトランザクションのセキュリティ強化をもたらすシステムであって、
第１のサーバ、第２のサーバ、及びモバイル機器サーバと、
利用者に関連する第１の装置であって、第１の通信チャネルを介して前記第１のサーバと通信し、前記第１のサーバを介してトランザクションを要求する、第１の装置と、
前記利用者に関連する第２の装置と
を含み、
前記モバイル機器サーバが、第２の通信チャネルを介して前記第２の装置と通信し、第３の通信チャネルを介して前記第１のサーバと通信し、
前記第１のサーバからのトランザクション承認要求を入力し、
前記第２の通信チャネルを介して前記第２の装置を認証し、
前記第２の装置の認証に応答して前記第１の装置と前記第１のサーバとの間のトランザクションを承認し、
前記利用者に関連する前記第１の装置及び前記第２の装置のうちの１つと通信する前記第２のサーバからのトランザクション承認要求を入力し、
前記第１の装置と前記第１のサーバとの間の前記トランザクションの前記承認に応答して前記第２のサーバからの前記トランザクション承認要求を承認する
ように構成される、
システム。
【請求項１９】
前記第２のサーバが、前記第１の装置と前記第１のサーバとの間のトランザクション承

認履歴に応答して、前記利用者に関連する装置との追加のトランザクションを承認するように構成される、請求項１８に記載のシステム。
【請求項２０】
前記第１の装置及び前記第２の装置が単一の装置である、請求項１８に記載のシステム。
【請求項２１】
装置によるトランザクションのセキュリティ強化をもたらすシステムであって、
ネットワークアドレスに関連するサーバと、
利用者に関連する第１の装置であって、第１の通信チャネルを介して前記サーバと通信し、前記サーバを介してトランザクションを要求し、前記サーバに関連するネットワークアドレスを取得するように構成される、第１の装置であり、前記第１の通信チャネルを介した通信が、前記取得されたサーバに関連するネットワークアドレスに応答して確立される、第１の装置と、
前記利用者に関連する第２の装置であって、前記第１の装置と通信し、前記取得されたサーバに関連するネットワークアドレスを前記第１の装置から受信するように構成される、第２の装置と、
第２の通信チャネルを介して前記第２の装置と通信するモバイル機器サーバであって、第３の通信チャネルを介して前記サーバと通信する、モバイル機器サーバと
を含み、
前記サーバ及び前記モバイル機器サーバのうちの少なくとも１つが、
前記サーバに関連するネットワークアドレスを信頼できる情報源から取得し、
前記第２の通信チャネルを介して前記第２の装置から、前記取得され受信されたサーバに関連するネットワークアドレスを入力し、
前記取得され受信され入力されたサーバに関連するネットワークアドレスが、前記信頼できる情報源から取得される前記サーバに関連するネットワークアドレスと一致する場合にのみ、トランザクションを承認するように構成される、システム。
【請求項２２】
装置によるトランザクションのセキュリティ強化をもたらす方法であって、
第１のユーザ装置を提供するステップと、
サーバに関連するネットワークアドレスを取得するステップと、
第１の通信チャネルを介し、前記取得されたサーバに関連するネットワークアドレスに応答して前記第１のユーザ装置と前記サーバとの間の通信を確立するステップと、
第２の通信チャネルを介し、前記取得されたサーバに関連するネットワークアドレスを入力するステップと、
前記サーバに関連するネットワークアドレスを信頼できる情報源から取得するステップと、
前記信頼できる情報源から取得された前記サーバに関連するネットワークアドレスを前記取得され入力されたサーバに関連するネットワークアドレスと比較するステップと、
前記第２の通信チャネルを介して入力された前記サーバに関連するネットワークアドレスが、前記信頼できる情報源から取得された前記サーバに関連するネットワークアドレスと一致する場合にのみ、前記サーバに関連するトランザクションを承認するステップと
を含む、方法。
【請求項２３】
前記第１の通信チャネルが前記第２の通信チャネルと異なる、請求項２２に記載の方法。
【請求項２４】
前記信頼できる情報源が、前記第１の通信チャネル及び前記第２の通信チャネルと異なる第３の通信チャネル、及び安全なデータベースのうちの１つを含む、請求項２２に記載の方法。
【請求項２５】

第２のユーザ装置を提供するステップを更に含み、前記提供された第２のユーザ装置が前記取得されたサーバに関連するネットワークアドレスを前記第１のユーザ装置から取得し、前記取得され入力されたサーバに関連するネットワークアドレスが、前記提供された第２のユーザ装置によって前記第２の通信チャネルを介して伝達される、請求項２２に記載の方法。

【請求項２６】

前記提供される第２のユーザ装置が、前記取得されたサーバに関連するネットワークアドレスを前記第１のユーザ装置から非接触要素を介して受信する、請求項２５に記載の方法。

【請求項２７】

パスコードを暗号化するステップと、

前記暗号化したパスコードを前記第２の通信チャネルを介して伝送するステップと

を更に含む、請求項２２に記載の方法。

【請求項２８】

入力装置を提供するステップを更に含み、前記パスコードが、前記入力装置を介した利用者のジェスチャに応答して受信される、

請求項２７に記載の方法。

【請求項２９】

追加のサーバを提供するステップと、

前記サーバに関連する前記トランザクションを前記承認することに応答して、前記提供した追加のサーバに関連する追加のトランザクションを承認するステップと

を更に含む、請求項２２に記載の方法。

【請求項３０】

装置によるトランザクションのセキュリティ強化をもたらすシステムであって、

デジタル指紋に関連するサーバと、

利用者に関連する第１の装置であって、第１の通信チャネルを介して前記サーバと通信し、前記サーバを介してトランザクションを要求し、前記サーバに関連するデジタル指紋を取得するように構成される、第１の装置と、

前記利用者に関連する第２の装置であって、前記第１の装置と通信し、前記取得されたサーバに関連するデジタル指紋を前記第１の装置から受信するように構成される、第２の装置と、

第２の通信チャネルを介して前記第２の装置と通信するモバイル機器サーバであって、第３の通信チャネルを介して前記サーバと通信する、モバイル機器サーバとを含み、

前記モバイル機器サーバは、

前記第２の通信チャネルを介して前記第２の装置から、前記取得され受信されたサーバに関連するデジタル指紋を入力し、

前記サーバに関連するデジタル指紋を信頼できる情報源から取得し、

前記取得され受信され入力されたサーバに関連するデジタル指紋が、前記信頼できる情報源から取得された前記サーバに関連するデジタル指紋と一致する場合にのみ、トランザクションを承認する

ように構成される、

システム。

【請求項３１】

前記デジタル指紋がデジタル署名である、請求項３０に記載のシステム。

【請求項３２】

前記デジタル指紋がサーバの動的情報を含む、請求項３０に記載のシステム。

【発明の詳細な説明】

【技術分野】

【０００１】

技術分野

本開示は、一般にトランザクションシステムの分野に関し、とりわけモバイル機器を利用して安全なトランザクションを行うためのシステム及び方法に関する。

【背景技術】

【０００２】

背景技術

クレジットカードやデビットカードによる支払いは、消費者による支出の大部分に相当する。歴史的には、クレジットカードやデビットカードは磁気ストライプで符号化されており、かかる符号化は、磁気ストライプ上に符号化された情報を読み取るように構成されるトランザクション装置に応答してトランザクションを安全な方法で可能にする。磁気ストライプを読み取る装置は、典型的にはトランザクションネットワークを介してクレジットカードの発行者と通信し、クレジットカードの発行者が最終的にトランザクションを承認する。不都合なことに、クレジットカードやデビットカードは盗難に遭いやすく、利用者は盗まれてもかなりの期間にわたって気付かない場合がある。

【０００３】

技術の進歩により、近距離通信（ＮＦＣ）としても知られる、ＩＳＯ／ＩＥＣ７８１０及びＩＳＯ／ＩＥＣ１４４４３の下で定められるもの等、非接触スマートカードの開発に至った。一般的に無線認証（ＲＦＩＤ）という用語の下、他の規格又はプロトコルを満たす同様の技術が利用可能であり、ＲＦＩＤの範囲は、典型的にはＮＦＣの範囲と同程度に制限される。本明細書の全体を通して使用する用語、非接触要素（ＣＥ）は、ＮＦＣ、ＲＦＩＤ、又はＮＦＣと同程度の範囲を有する他の短距離通信規格のうちの何れかの下で動作する任意の短距離通信装置を指し、典型的にはＣＥが読取機に近接されることを必要とする。光学的に読取り可能なコードの利用が、特にＣＥの定義と共に本明細書に含まれる。かかるＣＥスマートカードはトランザクションに使用できるが、ＣＥスマートカードは約４ｃｍ以内の任意の読取機によって読み取ることができるので、セキュリティを向上させない。従って、ＣＥスマートカードは一般に低価値のトランザクションにしか使用されず、ＣＥスマートカード上には少ない金額が予めロードされ、この少ない金額は、制限に達するまでトランザクションごとに減らされる。

【０００４】

モバイル機器（ＭＤ）は、そのユビキタス性、並びに利用可能な画面及び入力装置により金融取引にますます利用されている。本明細書で使用するＭＤは、マルチメディア再生、ネットワーク上のデータ通信、音声通信等の個人的機能に使用される任意の電子ＭＤを含む。ＭＤの一実施形態は、移動通信装置、携帯電話、移動電話、ハンドフォン、ワイヤレスフォン、セルフォン、セルラフォン、セルラ電話、モバイルハンドセット、又はセル電話としても知られる移動局である。

【０００５】

ＩＥＥＥ８０２．１１の発展及びその結果生じた無線ネットワークの広範な確立と共に、セルラ電話の機能に加えて、利用可能な無線ネットワーク上で通信する様々なＭＤが開発されてきた。更に、無線ネットワーク上及び／又はセルラネットワーク上の両方でインターネットにアクセスする能力を有する様々なＭＤが開発されてきた。

【０００６】

利用者を識別して支出を請求するための関連手段を有するユビキタスＭＤは、電子ウォレットとしてＭＤを利用する機会を示す。移動局を使用することにより、サービス又は製品、具体的には電話利用又は通信時間以外の製品又はサービスに対する支払いを行うための幾つかの知られている方法がある。

【０００７】

ＭＤと連携するＣＥは、２つの主なグループ、つまりＭＤのＣＰＵ等、ＭＤのコントローラと通信する装置、及びＭＤのＣＰＵと通信しない装置へと発展した。ＭＤのＣＰＵと通信するＣＥの場合、「ＳＩＭ非接触要素」（ＳＣＥ）としても知られるＳＩＭカード上のＮＦＣ装置、ＮＦＣ装置を有するＳＤカード等の外部カード、ＳＩＭアドオン非接触要素（ＳＣＣＥ）、ＭＤのハードウェア内に見られるＮＦＣ装置等、様々な装置を見つける

ことができる。本明細書では「埋込みＣＥ」（ＥＣＥ）装置として表す上記の装置群は、ＣＥ読取機がＣＥ装置と直接通信し、その通信がＭＤのＣＰＵの如何なる動作にも依存しない応用では、ＭＤのＣＰＵに接続されないＣＥ装置と同じ方法で使用することができる。ＣＥがＭＤのディスプレイ上に表示される光学的に読み取り可能なコードを含む場合、ＭＤは本質的にＥＣＥ装置であることを指摘しておく。

【０００８】

ＭＤのＣＰＵに接続されないＣＥのグループは、ＮＦＣ又はＲＦＩＤタグ、ステッカ、キーフォブ、ＭＤに取り付けることができる光学的に読み取り可能なコード、及び他のフォームファクタを含み得る。従ってこのようなＣＥは、ＭＤに関して固定されると、ＣＥのすぐ近くにある読取機によって読み取られる識別番号を提供するために利用することができる。

【０００９】

トランザクションシステムがより洗練され、より広く使用されるようになったので、不正なトランザクションの発生も増加している。ポータブルコンピュータ等のユーザ装置が成功裏にハッキングされており、それにより、パスワード及び／又は他の任意の入力情報が不正なハッカーによって不正に取得される可能性があるので、バンキングサイトやショッピングサイト等の安全なウェブサイトへのアクセスが問題になっている。同様に、インターネットカフェのコンピュータ等の共用コンピュータから安全なウェブサイトにアクセスすると、疑いをもたない利用者のユーザ名及びパスワードの両方が漏洩する可能性がある。

【００１０】

ＭＤ上に不正にロードされたキーロガーソフトウェアは、パスワード等のユーザ情報を簡単に取得し、それらを通信リンクを介して非承認の相手に転送することができる。介入者攻撃は、実際のトランザクションサーバを偽のトランザクションサーバに置き換え、それによりユーザ情報を取得する。

【発明の概要】

【発明が解決しようとする課題】

【００１１】

従来技術によって提供されておらず、必要とされているものは、ＭＤと連携して安全なトランザクションを行い、それによりセキュリティの向上を利用者に提供するためのシステム及び方法である。好ましくは、かかるシステム及び方法は、許可されたネットワークアドレスとの通信が確認される場合にのみトランザクションを許可するように構成される。

【課題を解決するための手段】

【００１２】

発明の概要

上記の解説及び他の考察に鑑みて、本開示は、安全なトランザクションを行う従来の及び現在の方法の欠点の一部又は全てを克服するための方法及び機器を提供する。この方法及び機器の他の新たな及び有用な利点も本明細書に記載し、当業者によって理解可能である。

【００１３】

一例示的実施形態では、少なくとも２つの独立した通信チャネルが設けられる。ユーザ装置が、プロバイダサーバと通信を確立するために使用される、サーバに関連するネットワークアドレスを取得する。モバイル機器サーバがプロバイダサーバと通信し、データベースや安全な通信リンク等の信頼できる情報源から、プロバイダサーバのネットワークアドレスを取得する。モバイル機器サーバは、プロバイダサーバと通信するためにユーザ装置によって利用されるネットワークアドレスを、第２の通信チャネルを介してユーザ装置から入力する。トランザクションは、入力アドレスが信頼できる情報源から取得されるアドレスに一致する場合にのみ承認される。

【００１４】

一実施形態では、トランザクションを要求するユーザ装置がモバイル機器であり、別の実施形態では、ユーザ装置が、トランザクションプロバイダサーバとの通信を試みるコンピュータ又は他の装置である。一実施形態では、モバイル機器サーバによって一致が確認され、別の実施形態では、トランザクションプロバイダサーバによって一致が確認される。

【００１５】

一実施形態では、モバイル機器と通信する非接触要素上でユーザ名及び／又はパスワードが入力され、モバイル機器との通信が非接触要素と共にセキュア要素によって暗号化される。一実施形態では、ユーザ装置のネットワークアドレス、及びトランザクションプロバイダサーバと通信するためにユーザ装置によって利用されるネットワークアドレスを、ユーザ装置が非接触要素によってモバイル機器に伝達する。更に別の実施形態では、ユーザ装置のネットワークアドレス、及びトランザクションプロバイダサーバと通信するためにユーザ装置によって利用されるネットワークアドレスを、ユーザ装置がＮＦＣ通信や赤外線通信等の短距離通信によってモバイル機器に伝達する。

【００１６】

独立して、装置によるトランザクションのセキュリティ強化をもたらすシステムを提供し、このシステムは、ネットワークアドレスに関連するサーバと、利用者に関連する第１の装置であって、第１の通信チャネルを介してサーバと通信し、サーバを介してトランザクションを要求し、サーバに関連するネットワークアドレスを取得するように構成される第１の装置であり、第１の通信チャネルは取得されたサーバに関連するネットワークアドレスに応答して確立される、第１の装置と、利用者に関連する第２の装置であって、第１の装置と通信し、取得されたサーバに関連するネットワークアドレスを第１の装置から受信するように構成される、第２の装置と、第２の通信チャネルを介して第２の装置と通信するモバイル機器サーバであって、第３の通信チャネルを介してサーバと通信する、モバイル機器サーバであり、第２の通信チャネルを介して第２の装置から、取得され受信されたサーバに関連するネットワークアドレスを入力し、サーバに関連するネットワークアドレスを信頼できる情報源から取得し、取得され受信され入力されたサーバに関連するネットワークアドレスが、信頼できる情報源から取得されるサーバに関連するネットワークアドレスと一致する場合にのみ、トランザクションを承認するように構成される、モバイル機器サーバとを含む。

【００１７】

一実施形態では、信頼できる情報源がサーバであり、サーバに関連するネットワークアドレスが第３の通信チャネルを介してサーバから取得される。別の実施形態では、信頼できる情報源が、モバイル機器サーバと通信するデータベースである。

【００１８】

一実施形態では、第１の通信チャネルが第２の通信チャネルと異なる。別の実施形態では、第１の装置及び第２の装置が単一の装置である。

【００１９】

一実施形態では、第１の装置及び第２の装置のうちの１つがユーザモバイル機器である。別の実施形態では、第１の装置及び第２の装置、ユーザ装置のうちの１つがコンピュータである。

【００２０】

一実施形態では、第１の装置がコンピュータであり、第２の装置がユーザモバイル機器である。別の実施形態では、第２の装置の第１の装置との通信が第４の通信チャネルを介し、第４の通信チャネルは第１、第２、及び第３の通信チャネルのどれとも異なる。或る更なる実施形態では、第４の通信チャネルが、無線認証通信及び近距離通信のうちの１つである。

【００２１】

一実施形態では、第３の通信チャネルが、第１の通信チャネル及び第２の通信チャネルの何れとも異なる安全な通信チャネルである。別の実施形態では、このシステムが、第２

の装置と通信するように構成されるセキュリティ保護された要素を更に含み、セキュリティ保護された要素は、利用者のジェスチャに応答して、暗号化されたパスコードを第２の通信チャネルを介してモバイル機器サーバに提供するように構成される。

【００２２】

或る更なる実施形態では、このシステムが、セキュリティ保護された要素と通信する入力装置を更に含み、入力装置を介した利用者のジェスチャにより、パスコードがセキュリティ保護された要素に与えられる。或る更なる実施形態では、入力装置が専用の入力装置である。別の更なる実施形態では、このシステムが非接触要素を含み、セキュリティ保護された要素が非接触要素に含まれ、セキュリティ保護された要素と第２の装置との間の通信が非接触要素に応答したものである。

【００２３】

一実施形態では、このシステムが、モバイル機器サーバと通信する通知サーバを更に含み、第２の装置が自らの上にアプリケーションを有し、そのアプリケーションは通知サーバに応答して、第１の装置のネットワークアドレス、及び取得され受信され入力されたサーバに関連するネットワークアドレスを提供するように構成される。別の実施形態では、このシステムが、モバイル機器サーバと通信する追加のサーバを更に含み、追加のサーバは、第１の装置とサーバとの間のトランザクションの承認に応答して第１の装置との追加のトランザクションを承認するように構成される。

【００２４】

別の独立した実施形態では、装置によるトランザクションのセキュリティ強化をもたらすシステムを提供し、このシステムは、第１のサーバ、第２のサーバ、及びモバイル機器サーバと、利用者に関連する第１の装置であって、第１の通信チャネルを介して第１のサーバと通信し、第１のサーバを介してトランザクションを要求する、第１の装置と、利用者に関連する第２の装置とを含み、モバイル機器サーバは、第２の通信チャネルを介して第２の装置と通信し、第３の通信チャネルを介して第１のサーバと通信し、モバイル機器サーバは、第１のサーバからのトランザクション承認要求を入力し、第２の通信チャネルを介して第２の装置を認証し、第２の装置の認証に応答して第１の装置と第１のサーバとの間のトランザクションを承認し、利用者に関連する第１の装置及び第２の装置のうちの１つと通信する第２のサーバからのトランザクション承認要求を入力し、第１の装置と第１のサーバとの間のトランザクションの承認に応答して第２のサーバからのトランザクション承認要求を承認するように構成される。

【００２５】

一実施形態では、第２のサーバが、第１の装置と第１のサーバとの間のトランザクション承認履歴に応答して、利用者に関連する装置との追加のトランザクションを承認するように構成される。別の実施形態では、第１の装置及び第２の装置が単一の装置である。

【００２６】

或る独立した実施形態では、装置によるトランザクションのセキュリティ強化をもたらすシステムを提供し、このシステムは、ネットワークアドレスに関連するサーバと、利用者に関連する第１の装置であって、第１の通信チャネルを介してサーバと通信し、サーバを介してトランザクションを要求し、サーバに関連するネットワークアドレスを取得するように構成される、第１の装置であり、第１の通信チャネルを介した通信が、取得されたサーバに関連するネットワークアドレスに応答して確立される、第１の装置と、利用者に関連する第２の装置であって、第１の装置と通信し、取得されたサーバに関連するネットワークアドレスを第１の装置から受信するように構成される、第２の装置と、第２の通信チャネルを介して第２の装置と通信するモバイル機器サーバであって、第３の通信チャネルを介してサーバと通信する、モバイル機器サーバとを含み、サーバ及びモバイル機器サーバのうちの少なくとも１つが、サーバに関連するネットワークアドレスを信頼できる情報源から取得し、第２の通信チャネルを介して第２の装置から、取得され受信されたサーバに関連するネットワークアドレスを入力し、取得され受信され入力されたサーバに関連するネットワークアドレスが、信頼できる情報源から取得されるサーバに関連するネット

ワークアドレスと一致する場合にのみ、トランザクションを承認するように構成される。

【００２７】

別の独立した実施形態では、装置によるトランザクションのセキュリティ強化をもたらす方法を提供し、この方法は、第１のユーザ装置を提供するステップと、サーバに関連するネットワークアドレスを取得するステップと、第１の通信チャネルを介し、取得されたサーバに関連するネットワークアドレスに応答して第１のユーザ装置とサーバとの間の通信を確立するステップと、第２の通信チャネルを介し、取得されたサーバに関連するネットワークアドレスを入力するステップと、サーバに関連するネットワークアドレスを信頼できる情報源から取得するステップと、信頼できる情報源から取得されたサーバに関連するネットワークアドレスを取得され入力されたサーバに関連するネットワークアドレスと比較するステップと、第２の通信チャネルを介して入力されたサーバに関連するネットワークアドレスが、信頼できる情報源から取得されたサーバに関連するネットワークアドレスと一致する場合にのみ、サーバに関連するトランザクションを承認するステップとを含む。

【００２８】

一実施形態では、第１の通信チャネルが第２の通信チャネルと異なる。別の実施形態では、信頼できる情報源が、第１の通信チャネル及び第２の通信チャネルと異なる第３の通信チャネル、及び安全なデータベースのうちの１つを含む。

【００２９】

一実施形態では、この方法が、第２のユーザ装置を提供するステップであって、取得されたサーバに関連するネットワークアドレスを第１のユーザ装置から受信する、第２のユーザ装置を提供するステップを更に含み、取得され入力されたサーバに関連するネットワークアドレスが、提供された第２のユーザ装置によって第２の通信チャネルを介して伝達される。或る更なる実施形態では、提供される第２のユーザ装置が、取得されたサーバに関連するネットワークアドレスを第１のユーザ装置から非接触要素を介して受信する。

【００３０】

別の実施形態では、この方法が、パスコードを暗号化するステップと、暗号化したパスコードを第２の通信チャネルを介して伝送するステップとを更に含む。或る更なる実施形態では、この方法が、入力装置を提供するステップを更に含み、パスコードが、入力装置を介した利用者のジェスチャに応答して受信される。

【００３１】

一実施形態では、この方法が、追加のサーバを提供するステップと、サーバに関連するトランザクションを承認することに応答して、提供した追加のサーバに関連する追加のトランザクションを承認するステップとを更に含む。

【００３２】

或る独立した実施形態では、装置によるトランザクションのセキュリティ強化をもたらすシステムが提供され、このシステムは、デジタル指紋に関連するサーバと、利用者に関連する第１の装置であって、第１の通信チャネルを介してサーバと通信し、サーバを介してトランザクションを要求し、サーバに関連するデジタル指紋を取得するように構成される、第１の装置と、利用者に関連する第２の装置であって、第１の装置と通信し、取得されたサーバに関連するデジタル指紋を第１の装置から受信するように構成される、第２の装置と、第２の通信チャネルを介して第２の装置と通信するモバイル機器サーバであって、第３の通信チャネルを介してサーバと通信する、モバイル機器サーバであり、第２の通信チャネルを介して第２の装置から、取得され受信されたサーバに関連するデジタル指紋を入力し、サーバに関連するデジタル指紋を信頼できる情報源から取得し、取得され受信され入力されたサーバに関連するデジタル指紋が、信頼できる情報源から取得されるサーバに関連するデジタル指紋と一致する場合にのみ、トランザクションを承認するように構成される、モバイル機器サーバとを含む。

【００３３】

一実施形態では、デジタル指紋がデジタル署名である。別の実施形態では、デジタル指

紋がサーバの動的情報を含む。
【００３４】
以下の図面及び説明から、本発明の更なる特徴及び利点が明らかになる。
【００３５】
図面の簡単な説明
本発明をより良く理解し、本発明を実施し得る方法を示すために、同じ番号が全体を通して対応する要素又は部分を指す添付図面を専ら例としてこれから参照する。
【００３６】
これから図面を詳しく具体的に参照するが、図示する詳細は例であり、本発明の好ましい実施形態を例示的に解説するためのものに過ぎず、本発明の原理及び概念的側面について最も有用且つ容易に理解される説明と思われる内容を提供するために示すことを強調しておく。この点において、本発明を基本的に理解するのに必要である以上に本発明の構造的詳細を詳しく図示する試みは行わず、説明を図面と共に解釈すれば、本発明の幾つかの形態を実際にどのように実施できるのかが当業者に明らかになる。
【図面の簡単な説明】
【００３７】
【図１Ａ】統合サーバと連携して有利な区分化を行い、それによりプロバイダシステムと共に使用するための帯域外認証を可能にする、トランザクションシステムの一実施形態の高レベルブロック図を示す。
【図１Ｂ】プロバイダ帯域上で私的なユーザ名又はパスワードを伝えることなしに安全なログイン機能をユーザ装置に提供するための、図１Ａのトランザクションシステムの動作の一例示的実施形態の高レベル流れ図を示す。
【図１Ｃ】統合サーバと連携して有利な区分化を行い、ＮＦＣ対応装置によりセキュリティ強化を更にもたらすトランザクションシステムの一実施形態の高レベルブロック図を示す。
【図１Ｄ】ＭＤキーパッド上で私的なユーザ名又はパスワードをタイプすることなしに安全なログイン機能をユーザ装置に提供するための、図１Ｃのトランザクションシステムの動作の一例示的実施形態の高レベル流れ図を示す。
【図１Ｅ】統合サーバと連携して有利なセキュリティを提供し、ネットワークアドレスの一致を確認することによりセキュリティ強化を更にもたらすトランザクションシステムの一実施形態の高レベルブロック図を示す。
【図２Ａ】２台の装置を利用するネットワーク通信にセキュリティの改善を提供するシステムの高レベルブロック図を示す。
【図２Ｂ】帯域外ログインによりセキュリティの向上をもたらすための、図２Ａのシステムの動作の第１の実施形態の高レベル流れ図を示す。
【図２Ｃ】アドレスを比較することに応答してセキュリティの向上をもたらすための、図２Ａのシステムの動作の第２の実施形態の高レベル流れ図を示す。
【図３Ａ】モバイル機器サーバと連携して有利なセキュリティを提供し、モバイル機器との多重帯域通信を利用して幾つかのネットワークアドレスの一致を確認することによりセキュリティ強化を更にもたらすトランザクションシステムの一実施形態の高レベルブロック図を示す。
【図３Ｂ】モバイル機器サーバと連携してネットワーク応用の有利なセキュリティを提供し、計算装置との多重帯域通信を利用して幾つかのネットワークアドレスの一致を確認することによりセキュリティ強化を更にもたらすトランザクションシステムの一実施形態の高レベルブロック図を示す。
【図３Ｃ】ネットワークアドレスの一致を用いた高度なセキュリティをもたらすための、図３Ａ、図３Ｂのトランザクションシステムの動作の高レベル流れ図を示す。
【図３Ｄ】アドレスに応答してシングルサインオン機能を提供するための、図３Ａのトランザクションシステムの動作の高レベル流れ図を示す。
【図３Ｅ】認証履歴に応答してシングルサインオン機能を提供するための、図３Ａのトラ

ンザクションシステムの動作の高レベル流れ図を示す。
【発明を実施するための形態】
【００３８】
実施形態の説明
少なくとも１つの実施形態を詳しく説明する前に、本発明は、以下の説明の中で記載し又は図中に示す構成の詳細及び構成要素の配置にその応用が限定されないことを理解すべきである。本発明は、他の実施形態にも適用可能であり、又は様々な方法で実践し若しくは実行することができる。更に、本明細書で使用する表現及び用語は説明目的であり、限定的であると見なすべきではないことを理解すべきである。具体的には、本明細書で使用するとき、接続されるという用語は直接的な接続に限定することを意図せず、如何なる種類の通信も含み、中間装置又は中間構成要素を制限なしに認める。
【００３９】
以下の説明では、モバイル機器（ＭＤ）という用語は、これだけに限定されないが移動局を含む、マルチメディア再生、ネットワーク上のデータ通信、音声通信等の個人的機能に使用される任意の電子モバイル機器を含む。明瞭にするために、移動局という用語は、基地局のネットワークを介した移動音声通信又は移動データ通信に使用される任意の移動通信装置、携帯電話、移動電話、ハンドフォン、ワイヤレスフォン、セルフォン、セルラフォン、セルラ電話、セル電話、又は他の電子装置を指す。以下の説明では、特定の実施形態においてセルラ通信、とりわけＧＳＭ（登録商標）（global system for mobile communication）の例を用いて通信を説明するが、本発明の範囲はこの点で限定されず、使用される通信方法は、これだけに限定されないが、ＵＭＴＳ（Universal Mobile Telecommunications System）、ＩＥＥＥ８０２．１１、ＩＥＥＥ８０２．１６ｘ、及びＣＤＭＡを含む任意の適切な通信プロトコルに基づき得ることが理解される。
【００４０】
本明細書の全体を通して、「復号」及び「解読」という用語は区別なく使用し、同じ意味を有する。同様に、本明細書の全体を通して、「暗号化」及び「符号化」という用語も区別なく使用し、同じ意味を有する。本明細書で使用するとき、「トランザクション」という用語は、金融取引並びに様々なウェブサイトへのログインを制限なしに含むことを意図する。
【００４１】
図１Ａは、支払手段認証方法及び／又はユーザ認証方法を制限なしに含む従来技術の認証方法の有利な区分化を行い、それにより柔軟性の向上をもたらす、トランザクションシステム１の一実施形態の高レベルブロック図を示す。トランザクションシステム１は、５０Ａ、５０Ｂ、５０Ｃ等の装置、一括して装置５０の何れか又は全てとすることができる装置と通信するプロバイダサーバ２０であって、通信はプロバイダ帯域７０によって行われる、プロバイダサーバ２０と、統合サーバ（ＩＳ）３０と、ＩＳ３０と通信する補足サービス８と、ＭＤサーバ４０と、好ましくはＭＤ６０に関連するメモリ上のアプリケーション６２をオンボードで実行するＭＤ６０であって、アプリケーション６２はＭＤ６０の計算装置上で実行される、ＭＤ６０とを含む。ＭＤ６０は、ＮＦＣ通信インターフェイス６６を更に示す。トランザクションシステム１は、セキュリティ保護された要素（ＳＥ）１１０が内部に埋め込まれたＵＳＢドングルとして制限なしに図示する非接触要素（ＣＥ）１００を更に含み、ＣＥ１００は、一実施形態ではキーパッド１１５、画面、及び機能ボタンを含む。ＭＤ６０は、範囲を超えることなしにＳＥ１１０（不図示）を更に含むことができる。ＮＦＣリーダ６６とＣＥ１００との間の通信は、ＮＦＣ帯域１２０を介する。
【００４２】
ＭＤサーバ４０とＭＤ６０との間の通信は、顧客帯域８０を介して行われ、顧客帯域８０は典型的にはプロバイダ帯域７０とは別であり異なる。プロバイダサーバ２０、ＩＳ３０、及びＭＤサーバ４０のそれぞれは、データを記憶し、必要に応じて命令を操作するためのメモリ９０が関連付けられ、本明細書に記載の方法を実行し、サービスを提供するた

めのプロセッサを更に示す。メモリ９０は、制限なしに関連する装置の内部メモリ又は外部メモリとすることができる。非限定的な一実施形態では、プロバイダサーバ２０、ＩＳ３０、及びＭＤサーバ４０が単一のサーバによって実装される。

【００４３】

プロバイダサーバ２０は、コンピュータ５０Ａ、ＡＴＭ５０Ｂ、及びゲート５０Ｃといった装置５０により利用者にサービスを提供するように構成される、従来技術で知られているプロバイダシステムを実装する。ＭＤサーバ４０は、アプリケーション６２、好ましくはＳＥ１１０と連携し、ＭＤ６０によるログインや購入等の金融サービスを提供するための、従来技術で知られているＭＤ認証システムを実装する。一実施形態では、ＳＥ１１０がＭＤ６０に組み込まれて設けられ、別の実施形態では、ＳＥ１１０が制限なしにＣＥ１００に組み込まれて設けられる。プロバイダサーバ２０は、ＩＳ３０と連携して以下で更に説明する高度な機能を更に提供する。

【００４４】

プロバイダサーバ２０と様々な装置５０との間の従来技術による認証は独自のものであり、不正を防ぐために努力を継続的に維持しなければならない。プロバイダ帯域７０によるプロバイダサーバ２０及び様々な装置５０の構成は、プロバイダシステムとして知られている。プロバイダサーバ２０は、インターネットによって実装することができる水平に線影を付けた双方向矢印として示すプロバイダ帯域７０を介し、各ユーザ装置５０と双方向通信する。更に、この水平に線影を付けた双方向矢印は、双方向通信セッションを示す。一例示的実施形態では、プロバイダ帯域７０を介した通信がアドレスを利用して行われる。

【００４５】

ＭＤサーバ４０とＭＤ６０との間の従来技術による認証は独自のものであり、不正を防ぐために努力を継続的に維持しなければならない。ＭＤ６０は、典型的には限られた数のＭＤサーバ４０に制約されており、ＭＤサーバ４０は、従来技術によればそのそれぞれのアプリケーションがそれぞれＭＤ６０上に記憶されており、従ってＭＤ６０は、セキュリティ対策を伴う独自の及び面倒な導入過程なしにＭＤサーバ４０を自由に選択することができない。顧客帯域８０によるＭＤサーバ４０及びＭＤ６０の構成は、ＭＤ認証システムとして知られている。アプリケーション６２は、一般に「モバイルウォレット」として知られる。顧客帯域８０は、点で埋められた双方向矢印として図示しており、無線ＬＡＮやＩＥＥＥ８０２．１１対応接続等、ＭＤ６０とＭＤサーバ４０との間のデータ接続によって実装することができる。更に、点で埋められた双方向矢印は、一例示的実施形態ではアドレスを利用して行われる双方向通信セッションを示す。本明細書に記載のＭＤサーバ４０は、ＩＳ３０と連携して以下で更に説明する高度な機能を更に提供する。

【００４６】

以下で更に説明するように、ＩＳ３０は、プロバイダシステムとＭＤ認証システムとの間の結合を有利に且つ革新的に提供する。具体的には、ＩＳ３０はプロバイダサーバ２０及びＭＤサーバ４０のそれぞれと双方向通信し、従来技術の区分化を保ちながら高度なサービスを提供する。

【００４７】

かかる区分化は、ＩＳ３０と連携し、従来技術の認証プロトコルとの統合を有利に実現し、プロバイダのサービスのユビキタス性を高め、セキュリティを強化し、費用節減に貢献しながらＭＤ６０に基づく利用者の経験を向上させる。トランザクションシステム１は、１つ又は複数のＭＤサーバ４０をサポートできるのでオープンシステムであり、従ってプロバイダサーバ２０は、既定の及び事前に組み込まれた１組の認証ベンダに依存しない。更に、トランザクションシステム１は、少なくとも１つのＭＤ認証システム４０を用いて複数のプロバイダサーバ２０及び複数のユーザＭＤ６０をサポートすることができる。ＭＤサーバ４０は、好ましくは全てのプロバイダサーバ２０にシングルサインオンを提供し、従ってトランザクションシステム１は、複数のプロバイダサーバ２０に対して１つのＭＤサーバ４０を示すことができる。

【００４８】
動作面では、ＩＳ３０は、プロバイダサーバ２０とＭＤサーバ４０との統合を実現し、具体的には、及び以下で説明するように、ＩＳ３０は、ＭＤサーバ４０がプロバイダサーバ２０に認証を与えることを可能にし、それによりプロバイダサーバ２０が装置５０にサービスを提供できるようにする。ＮＦＣ通信インターフェイス６６と通信するＣＥ１００により、好ましくは高度なセキュリティが提供される。
【００４９】
一部の更なる詳細では、プロバイダサーバ２０が、インターネットによって実装することができるプロバイダ帯域７０を介してユーザ装置５０と双方向通信し、装置５０がユーザＰＣ５０Ａによって具体化され得るオンラインバンキングシステム、自動販売機システムによって具体化されるＡＴＭ５０Ｂ、及び／又はゲート５０Ｃ等のアクセス制御システム等の多くのシステムのうちの１つによって具体化され得る。従来技術によるプロバイダサーバ２０は、典型的には磁気クレジットカード承認機器等の装置５０における利用者が資格情報を提示することに基づく内部認証方法を含む。更に、装置５０のデータ入力装置において利用者の識別情報又はパスワードを入力する必要があり得る。しかし、上記のように、とりわけユーザＩＤ及びパスワードの使用を含む資格情報を提供する要件は、装置５０上にひそかにロードされたキーロガーソフトウェア等の不正な攻撃に利用者をさらす。以下で更に説明するように、ＩＳ３０の動作は、機密性の高い資格情報を装置５０において提供する必要なしに、プロバイダサーバ２０からユーザ装置５０にサービスを安全に提供できるようにする。
【００５０】
その代わりに、著しく低レベルの識別情報をプロバイダ帯域７０内で利用し、この識別情報は、漏洩しても機密性の高い資格情報が漏洩するよりも著しく低い損害しか引き起こさないものである。例えば、低レベルの識別情報の漏洩は、迷惑行為による損害を引き起こす可能性はあるが、直接的な金銭的損害を引き起こすことはできない。本明細書では、かかる識別情報を保護なし識別情報と呼び、それは保護なし識別情報の漏洩が最小限の損害しか引き起こさないからである。保護なし識別情報は、トランザクションシステム１を安全なユーザ認証に導く。一実施形態では、プロバイダサーバ２０が、複数のＩＳ３０と制限なしに通信することができる。特定の実施形態では、保護なしＩＤを装置５０によってプロバイダサーバ２０に与えることが、制限なしにキーパッド上でデータを入力すること、音声識別、又はＲＦＩＤ、ＮＦＣ、Ｂｌｕｅｔｏｏｔｈ（登録商標）、Ｉ．Ｒ、バーコードの読取り等の短距離無線に基づく情報を読み取ることのうちの１つ又は複数によって行われる。
【００５１】
ＭＤサーバ４０は、ＭＤ６０の利用者からの認証要求、及び受信される任意の応答の認証を少なくとも含む認証サービスを提供する。ＭＤサーバ４０による認証は、ユーザＭＤ６０と連携して実現され、１つ又は複数の認証要素及び帯域外認証を含むことができる。任意選択的にＭＤ６０は、以下で更に説明するように、トランザクションシステム１によって実現されるセキュリティレベルの向上に寄与するセキュリティソフトウェアがインストールされたＳＥ（不図示）を含む。
【００５２】
ＩＳ３０は、利用者が複数のＭＤサーバ４０によって制限なしに認証されることを可能にする、オープンシステムとして機能することを可能にする。一実施形態では、ユーザＭＤ６０が複数のアプリケーション６２を含み、特定のアプリケーション６２との通信に応じて認証を行うように複数のＭＤサーバ４０のそれぞれが構成される。別の実施形態では、単一のアプリケーション６２との通信に応じて認証を行うように複数のＭＤサーバ４０が制限なしに構成される。トランザクションシステム１は、更に説明するように、１つ又は複数のＭＤサーバ４０と連携して補助的なユーザ認証サービスをプロバイダサーバ２０に提供する。ＩＳ３０と通信する補足サービス８は、クーポンや広告サービス等の高度なサービスをＩＳ３０に供給する。一実施形態では、ＩＳ３０がＭＤサーバ４０に埋め込ま

れ、別の実施形態では、プロバイダサーバ２０及びＩＳ３０の両方がＭＤサーバ４０に埋め込まれる。トランザクションシステム１は、保護なしユーザ識別情報を捕捉するために、装置５０と連携してプロバイダサーバ２０によって使用されるプロトコルとは無関係に、高度なトランザクションのセキュリティを実行するように好ましくは構成される。統合サーバ３０は、利用者の事前設定、利用者のアプリケーション６２から生じるトランザクション前の時間表示、及びプロバイダサーバ２０の好みを含む複数のパラメータの１つに応答し、複数のＭＤサーバ４０の少なくとも１つを選択するようにプログラムされ得る。

【００５３】

ＩＳ３０に対してプロバイダサーバ２０が起こす認証要求は、認証過程を支援するための所望の認証の種類及びトランザクション情報を含むことができる。かかるトランザクション情報は、装置５０に関する位置情報を有利に含むことができ、その位置情報は、好ましくはＭＤ６０の物理的位置の位置情報に一致するとＭＤサーバ４０によって確認される。ここで、位置情報の脈絡で使用するとき、一致するという用語は、位置が正確に一致することは必要とせず、好ましくは位置決定誤差を考慮に入れる所定の範囲内で位置が一致することを示し、その誤差の量は更に位置に依存し得る。

【００５４】

認証の種類には、利用者がもっているもの、利用者が知っていること、利用者がどこにいるのか、利用者が通信している当事者、認証リスクスコア、支払認証、利用者の履歴、利用者の詳細、及びＭＤ６０の詳細を制限なしに含み得る、利用者の真正性の指示のうちの何れか又は全てが含まれ得る。一実施形態では、プロバイダサーバ２０が、認証過程の一環としてプロバイダサーバ２０に関連するパスワードをＭＤ６０上で入力するように利用者に要求することができる。

【００５５】

上記のように、プロバイダサーバ２０、ＩＳ３０、及びＭＤサーバ４０のそれぞれはプロセッサを示し、上記のように、範囲を超えることなしに内部メモリ又は外部メモリとすることができるメモリ９０と通信する。メモリ９０は、以下で説明するように、プロバイダサーバ２０、ＩＳ３０、及びＭＤサーバ４０それぞれの動作用の命令が記憶される非一時的なコンピュータ可読媒体を示す。メモリ９０は、必要に応じてデータの記憶域を提供するために更に利用することができる。様々なメモリ９０が物理的に不同である必要はなく、様々なメモリ９０は、範囲を超えることなしに単一のクラウドサーバ上に実装することができる。

【００５６】

図１Ｂは、プロバイダ帯域７０上で私的なユーザ名又はパスワードを伝えることなしに安全なログイン機能をユーザ装置５０Ａに提供するための、トランザクションシステム１の動作の一例示的実施形態の高レベル流れ図を示す。この実施形態は、インターネットカフェのパーソナルコンピュータ（ＰＣ）等、ユーザ装置５０Ａが利用者一人の所有物でない場合にとりわけ有用だが、これは決して限定的であることは意図しない。明瞭にするために、各段階間の矢印は図１Ａの帯域の情報に一致する方法で印付けしてあり、従ってプロバイダ帯域７０内のフローは水平に線影を付けた矢印として示し、顧客帯域８０内のフローは点で埋められた矢印として示し、ＩＳ３０とプロバイダサーバ２０又はＭＤサーバ４０との間のフローは実線として示してある。特定の段階は、上記のようにそれぞれのメモリ９０上に記憶される命令に応答して実行される。このフローは、最初のログイン後に行われるトランザクションに関するトランザクション認証等、更なる例示的実施形態に対し、適切に適合させて適用できることに留意すべきである。このフローは、とりわけユーザ装置５０Ａに関して説明するが、これは決して限定的であることは意図しない。同様のフローを、ユーザ装置５０Ｂ及び５０Ｃに制限なしに等しく適用することができる。

【００５７】

段階１０００で、ユーザ装置５０Ａが提供帯域７０を介してプロバイダサーバ２０の特定の資源、ページ、又はサイトにアクセスし、本明細書で更に説明するユーザＭＤ６０を介した信頼できるＩＳ３０による利用者のログイン承認等、トランザクションの承認を要

求する。ログインの承認がユーザＭＤ６０によるものかの制限はなく、認証要求前の所定の時間内の少なくとも１つの他の信頼できるエンティティによるユーザ認証等、ＩＳ３０によって集められた情報に基づくプロバイダ２０とＩＳ３０との間で合意される如何なる承認も、範囲を超えることなしに利用することができる。明瞭にするために、ユーザＭＤ６０による承認を、専ら非限定的な例として以下で更に詳述する。任意選択的に、プロバイダサーバ２０によってユーザ装置５０Ａに提供される初期ログインページは簡単なＯＯＢＬロゴを提示し、このロゴは、選択時にログインが信頼できるエンティティによって承認され、利用者がユーザＭＤ６０によってログインを完了することを信頼できるエンティティが要求し得ることを利用者に知らせるものである。このＯＯＢＬロゴは、明瞭にするためにユーザ装置５０Ａの表示部分上に示される。或いは、特定のトランザクションではログインがＯＯＢＬによるものに制約される。ユーザ装置５０Ａは、好ましくは、ローカルメモリ上のユーザ装置５０Ａを識別する記憶済みクッキー情報を提供する。任意選択的に、提供されるクッキー情報は、シリアル番号や他の設定データ等のコンピュータ識別情報を含む。プロバイダサーバ２０は、任意選択的にユーザ装置５０のインターネットプロトコルアドレスに応答し、ユーザ装置５０の位置情報を決定する。プロバイダサーバ２０の特定のページ又はサイトは、制限なしに金融機関、小売商、又はサービスサプライヤに関連することができる。

【００５８】

段階１０１０で、プロバイダサーバ２０が、利用者が制限なしに選択する任意のＩＤとすることができ、少なくともＩＳ３０又はＭＤサーバ４０に登録されているユーザＩＤ、好ましくは保護なしユーザＩＤをユーザ装置５０Ａに要求する。一例示的実施形態では、保護なしユーザＩＤとして電子メールアドレスが利用され、別の実施形態では、ユーザＭＤ６０のＭＳＩＳＤＮ等の電話番号が利用される。保護なしユーザＩＤをユーザＭＤ６０に更に関連する少なくとも１つのＭＤサーバ４０に関連付けるＩＳ３０との事前登録は、好ましくは事前登録段階において行われ、好ましくは保護なしユーザＩＤと異なるユーザ名及びパスワードが定められ、保護なしユーザＩＤに関連するＭＤサーバ４０によってアクセス可能なメモリ９０の一部分に記憶される。ＳＥ１１０の１つ又は複数の識別情報及び／又はＳＥ１１０の暗号化鍵を保護なしユーザＩＤに関連付けるために、事前登録が更に利用される。

【００５９】

段階１０２０で、段階１０１０の要求に応答し、利用者が保護なしユーザＩＤをユーザ装置５０Ａによって与える。任意選択的な段階１０３０では、与えられた保護なしユーザＩＤを、上記のプロバイダサーバ２０Ａによってアクセス可能なメモリ内に記憶される既定の保護なしユーザＩＤと突き合わせて検証する。検証時間やユーザ装置５０Ａの位置等、複数の補足的パラメータを検証手続きに適用しても良い。保護なしユーザＩＤが検証されない場合、段階１１８０で、ログイン失敗メッセージを生成し、ユーザ装置５０Ａの表示装置上に表示する。

【００６０】

段階１０４０で、「信頼できるＩＳによってログインせよ」メッセージ、又は「ユーザＭＤによってログインせよ」等のより具体的な命令をプロバイダサーバ２０によってユーザ装置５０Ａに伝送し、ユーザ装置５０Ａの表示装置上に表示し、それにより、一実施形態ではユーザＭＤ６０上でログインを続行するように利用者を促し、ユーザＭＤ６０は、以下の段階１０７０で説明するように好ましくは更なるログイン命令を自動で表示する。代替的実施形態では、利用者の介入なしにＭＤサーバ４０がユーザＭＤ６０にチャレンジを発行することをＩＳ３０が要求し、成功した場合にだけログイン命令に進む。

【００６１】

段階１０５０では、段階１０２０の保護なしユーザＩＤ、及び段階１０００の任意選択的な求めた位置情報を、認証要求としてプロバイダサーバ２０によりＩＳ３０に伝送する。ＩＳ３０は、プロバイダサーバ２０とＩＳ３０との間で交渉された所定のリスク規則に従って認証要求を管理し、所定のリスク規則に応答し、段階１１６０に関して以下で説明

するように利用者のログインを直接承認するか、又は以下の段階１０６０以降に関して以下で説明するようにユーザＭＤ６０によるログインに進むかを決定する。

【００６２】

段階１０６０で、ＩＳ３０が、段階１０２０の保護なしユーザＩＤ、及び段階１０００の位置情報等の任意選択的な求めたパラメータを含むＭＤによるログイン要求をＭＤサーバ４０に伝送する。

【００６３】

段階１０７０で、ＭＤサーバ４０がログイン認証要求をＭＤ６０に伝送し、ＭＤ６０は好ましくはユーザＭＤ６０のアプリケーション６２をトリガし、ユーザＭＤ６０の表示装置上に更なるログイン命令を自動で表示する。或いは、利用者がＭＤアプリケーション６２を起動して更なるログイン命令を表示しても良い。一実施形態では、ＭＤサーバ４０が、利用者の介入なしに通知サーバ（不図示）によってアプリケーション６２をトリガする。

【００６４】

段階１０８０で、段階１０７０でのＭＤサーバ４０からの認証要求に応答し、ＭＤ６０が、ユーザＭＤ６０の位置情報及び識別情報をＭＤサーバ４０に与え、その識別情報は、制限なしにクッキー、ＩＭＳＩ、ＩＭＥＩ、ＢＴ　ＩＤ等、ユーザＭＤ６０に固有であり、ＭＤサーバ４０によって検証可能なＭＳＩＳＤＮや他の識別情報又は他の識別情報群とすることができる。好ましくは、ユーザＭＤ６０上で実行され、ユーザＭＤ６０のローカルメモリ上に記憶されるアプリケーション６２は、ＭＤサーバ４０へのアクセスを行い、上記のデータを提供する。更に好ましくは、ユーザＭＤ６０とＭＤサーバ４０との間の情報伝送は、セキュアソケットレイヤ（ＳＳＬ）リンクによるものである。

【００６５】

段階１０９０で、段階１０４０～段階１０６０に関して上記で説明したように、ＭＤサーバ４０がユーザＭＤ６０の受信済みの識別情報及び位置情報を全ての待ち状態のログイン認証要求と比較し、一致する待ち状態のログイントランザクションを探す。上記のように、待ち状態のトランザクションの何れかのユーザＩＤが、ユーザＭＤ６０の受信済み識別情報に一致するかどうか、即ち相互参照されるかどうかを判定するために、ＭＤサーバ４０のメモリ９０が、段階１０１０に関して上記で説明したユーザＩＤの相互参照、及びユーザＭＤ６０の識別情報を含むことを理解すべきである。不正を防ぐために、好ましくは位置情報が一致を求めて更に比較される。上記のように、位置情報の一致は正確である必要はなく、それはとりわけユーザＭＤ６０の位置情報がピンポイント精度を提供しない三角測量によって提供され得るからであり、ユーザ装置５０の位置情報が同様にピンポイント精度を提供しないＩＰアドレスによって与えられ得るからである。従って、位置の一致の広義の定義を好ましくは利用し、それにより、物理的にあり得ない位置の不一致だけが、不一致結果をトリガするように設定される。任意選択的に、範囲を超えることなしに位置フィルタをバイパスさせることができる。但し、識別情報の一致は正確であり、任意の相互参照を含むことを意図する。従って、受信される識別情報は、変換、復号、又は相互参照後に記憶済みの識別情報に合致する場合、記憶済みの識別情報と一致するとしてよい。

【００６６】

段階１０９０で、ユーザＭＤ６０の識別情報及び位置情報が待ち状態のログイントランザクションに一致する場合、段階１１００で、ＭＤサーバ４０が、ＳＥ１１０のパスコード情報及び識別情報をユーザＭＤ６０に要求する。任意選択的に、利用者がもっているものでセキュリティ要素を強化するために、ＭＤサーバ４０がユーザＭＤ６０に対してＳＭＳチャレンジを行う（不図示）。更なる詳細では、ＭＤサーバ４０が、英数字コードを任意選択的に含むＳＭＳメッセージをユーザＭＤ６０に伝送することができ、上記のユーザＭＤ６０のアプリケーションの実行が、好ましくは受け取った英数字コードを返すことによってＳＭＳチャレンジに応答する。上記のＳＭＳチャレンジ及び応答は、モバイル金融取引の当業者に知られており、従って簡潔にするために本明細書では更に詳述しない。

【００６７】
段階１１１０で、利用者がＰＩＮ等のパスコードをＣＥ１００の入力装置１１５上で入力し、ＣＥ１００をＭＤ６０に近接させる。或いは、範囲を超えることなしにユーザ名及びパスワードの両方をユーザＭＤ６０の入力装置上で入力することができる。ＭＤ６０の入力装置上への利用者の入力ジェスチャ、又はＣＥ１００をＮＦＣ通信インターフェイス６６に近接させることに応答し、段階１１２０で、ユーザＭＤ６０が好ましくはＳＥ１１０の鍵によって暗号化されるパスコード及びＳＥ１１０の識別情報をＮＦＣ帯域１２０を介して受信する。段階１１３０で、ＭＤ６０が受信した識別情報及びパスコードをＭＤサーバ４０に伝送する。この伝送は、範囲を超えることなしに任意選択的なＳＥ１００オンボードＭＤ６０によって更に符号化され得る。一実施形態では、ユーザ名、パスワード、及びＳＥ識別情報がＭＤサーバ４０を使って事前登録され、従ってプロバイダサーバ２０と通信することなしにＭＤサーバ４０によって検証され得る。代替的実施形態では、ユーザ名及びパスワードが制限なしにＩＳ３０又はプロバイダサーバ２０に登録され、適切なサーバによって検証が行われる。代替的実施形態では、ユーザ名が要求されず、パスワード及び好ましくはＳＥ１１０の識別情報だけが利用者に要求される。一実施形態では、任意選択的なＳＭＳチャレンジの一部に応答した情報に応答して符号化される、ユーザ名及びパスワードがユーザＭＤ６０から伝送される。更に、ユーザＭＤ６０からの情報も制限なしに同様に符号化することができる。

【００６８】
段階１１４０で、受信済みのユーザ名、パスワード、及びＳＥ　ＩＤを検証し、それがＭＤサーバ４０上の記憶済みユーザ名、パスワード、及びＳＥ　ＩＤに一致することを確認する。受信済みのユーザ名及びパスワードが検証される場合、段階１１５０で、ＭＤサーバ４０が「ログインが完了しました。ユーザ装置によって続けて下さい」等のメッセージをユーザＭＤ６０に伝送し、段階１１３０の伝送されたユーザ名及びパスワードに応答してプロバイダサーバ２０にログインできるようにするために、ＭＳサーバ４０はＩＳ３０に認証を更に伝送する。検証メッセージは、好ましくは検証メッセージの一部として伝送されるＭＤ６０の識別情報により、段階１０００の待ち状態のトランザクションとマッチされる。

【００６９】
段階１１６０で、ＩＳ３０が、利用者を識別するために利用される認証方法の指示、ユーザＭＤ６０の識別情報、及び検証用の確認コードを含む認証メッセージをプロバイダサーバ２０に伝送する。

【００７０】
段階１１７０で、プロバイダサーバ２０が、段階１１６０の受信済み認証メッセージに応答し、所望のユーザページをユーザ装置５０Ａに伝送する。ユーザ名及びパスワード情報はプロバイダ帯域７０内で伝送されておらず、顧客帯域８０内で独占的に伝送されており、それによりセキュリティを改善していることに留意すべきである。

【００７１】
段階１０３０で保護なしＩＤの検証に失敗した場合、段階１０９０でユーザＭＤ６０と位置とが一致しない場合、又は段階１１４０でユーザ名及びパスワードの検証に失敗した場合、段階１１８０で、ログインの試みが失敗する。好ましくは、ログイン失敗の通知が、ユーザＭＤ６０及びユーザ装置５０Ａの両方に伝送される。

【００７２】
一実施形態では、ＭＤ６０によるユーザ装置５０Ａ上のログイン認証は、段階１０２０の前に、利用者が能動的に開始し又はＭＤアプリケーション６２によりＭＤサーバ４０にログインすることによって始まり得る。

【００７３】
従って、図１Ｂのトランザクションフローは、３つの帯域、つまりプロバイダ帯域、発行者帯域、及びＳＥ１１０を読み取るように構成される別のＮＦＣ帯域の隔離を実現する。更に、第２の「利用者がもっているもの」、即ちＳＥ１１０の識別情報を設けることに

より、セキュリティが強化される。好ましくはセキュリティ保護されたキーパッド上で入力され、暗号化され、それにより不正なキーロガーソフトウェアによるアクセスが遮られるパスワードであって、「利用者が知っていること」を表す、パスワードによって、及び追加で位置確認を使用し、「利用者がどこにいるのか」を追加することによって、セキュリティが更に強化される。

【００７４】

上記の内容は決してＳＥ１１０の単一の不変のＩＤに限定されることを意図せず、ＳＥ１１０は、ＭＤサーバ４０及びＩＳ３０の１つに事前登録された鍵に基づく疑似乱数生成器を搭載し得る。従って、範囲を超えることなしにワンタイムパスワード（ＯＴＰ）がＳＥ１１０から更に提供され、図１Ｂのトランザクションフローの一部として検証されても良い。好ましくは、ＯＴＰは、有効時間と共にＮＦＣ帯域１２０を介してユーザＭＤ６０に提供される。

【００７５】

範囲を超えることなしに、画像選択等の他の手段を利用し、セキュリティを更に強化することができる。

【００７６】

図１Ｃは、統合サーバ３０と連携して有利な区分化を行い、ＣＥ１００によりセキュリティ強化を更にもたらすトランザクションシステム１５０の一実施形態の高レベルブロック図を示す。トランザクションシステム１５０は、明瞭にするためにポータブルコンピュータとして制限なしにユーザ装置５０Ａしか図示していないことを除き、トランザクションシステム１とあらゆる点で同じである。更に、ＣＥ１００は、ＭＤ６０及びユーザ装置５０Ａの両方と通信するように構成される。一実施形態では、ＣＥ１００がＵＳＢ形式で構成され、それによりユーザ装置５０Ａにすぐ接続できるようになっている。別の実施形態では、図１Ｄに関して以下で更に説明する操作の流れを可能にするために、ユーザ装置５０ＡがＮＦＣ又は他の近距離通信機能を備える。

【００７７】

図１Ｄは、ユーザＭＤ６０のキーパッド上で私的なユーザ名又はパスワードをタイプすることなしに安全なログイン機能をユーザ装置５０Ａに提供するための、トランザクションシステム１５０の動作の一例示的実施形態の高レベル流れ図を示す。更に、以下で更に説明するように、ＮＦＣ帯域１２０、プラグイン、及び／又はＮＦＣ帯域１２０Ａによって提供されるネットワークアドレス情報に応答し、追加のセキュリティがもたらされる。

【００７８】

段階１３００で、上記の図１Ｂの段階１０００～段階１０９０を実行する。以下で更に説明するように、好ましくは、プロバイダサーバ２０は、自らが使用するネットワークアドレス、並びにユーザ装置５０Ａに通じるネットワークアドレスに関する情報を検証のために提供する。段階１３１０で、ＭＤサーバ４０が、安全なパスワード、ネットワークアドレス、ＳＥ識別情報、及び任意選択的に段階１０００の待ち状態のログイントランザクションに利用されるトランザクション情報を得るための要求をユーザＭＤ６０に伝送する。

【００７９】

段階１３２０で、利用者の入力ジェスチャがＣＥ１００のキーパッド１１５において受け付けられ、それによりＰＩＮ等のパスコードを受け取る。パスコードは、好ましくは暗号化されてＳＥ１１０によって受信され、ローカルメモリ内に記憶される。

【００８０】

段階１３３０で、ＣＥ１００をユーザ装置５０Ａと通信状態に置く。一実施形態では、ＣＥ１００がユーザ装置５０Ａのそれぞれの ＵＳＢ（ユニバーサルシリアルバス）ポートに差し込まれ、別の実施形態では、ＣＥ１００がユーザ装置５０Ａのそれぞれの ＮＦＣ通信装置に近接される。更に別の実施形態では、ＣＥ１００が、ユーザ装置５０ＡとＢｌｕｅｔｏｏｔｈ通信又は赤外線通信する。ユーザ装置５０Ａと通信状態に置かれることに応答し、段階１３４０で、ＳＥ１１０が、ＳＥ１１０の識別情報と共に暗号化されたパスコ

ードをユーザ装置５０Ａに伝送する。従って、パスコードがユーザ装置５０Ａ上で入力されることはなく、キーロギングソフトウェアによって傍受することはできない。ＣＥ１００は、汎用ソフトウェアを実行しない専用装置であり、従ってキーロギングソフトウェアの影響を受けない。ユーザ装置５０Ａは、自らが通信するネットワークアドレスの一覧をＣＥ１００に伝送し、その一覧は、プロバイダサーバ２０に接続するのに利用されるアドレス及びユーザ装置５０Ａのアドレスを少なくとも含む。当業者に知られているように、この一覧はユーザ装置５０Ａのプロセッサから入手することができる。ユーザ装置５０Ａは、ユーザ装置５０Ａの識別情報をＣＥ１００に更に伝送し、任意選択的に、トランザクション情報を更に伝達する。図１Ｃに示すように、ユーザ装置５０ＡとＣＥ１００との間の双方向通信は、ＮＦＣ又はＵＳＢ帯域１２０Ａを介する。

【００８１】

段階１３５０で、ユーザ装置５０Ａが、受信済みのＳＥ識別情報、暗号化されたパスコード、及びトランザクション情報を、一例示的実施形態ではウェブサーバであるプロバイダサーバ２０に伝送する。プロバイダサーバ２０は、受け取った情報を統合サーバ３０に転送する。

【００８２】

段階１３６０で、ＣＥ１００をＭＤ６０に近接させ、段階１３７０で、ＣＥ１００がＳＥ１１０の識別情報、暗号化されたパスコード、ユーザ装置５０Ａから取得されたネットワークアドレス、及び任意選択的なトランザクション情報をＭＤ６０、とりわけアプリケーション６２に、ＮＦＣ通信インターフェイス６６を介して、即ちＮＦＣ帯域１２０上で伝送する。ＣＥ１００がユーザ装置５０Ａから接続を絶たれる必要はないが、ユーザ装置５０Ａとの接続は要求されていない。

【００８３】

段階１３８０で、受信したＳＥ１１０の識別情報、暗号化されたパスコード、ネットワークアドレス、及び任意選択的なトランザクション情報を、ＭＤ６０からＭＤサーバ４０に顧客帯域８０を介して伝送する。この伝送は、範囲を超えることなしに、任意選択的なＳＥ１１０オンボードＭＤ６０によって更に符号化されても良い。更に、ユーザＭＤ６０が、好ましくはユーザＭＤ６０の識別情報をＭＤサーバ４０に伝送する。

【００８４】

段階１３９０で、受信したパスコード及びＳＥ　ＩＤを検証し、それがＭＤサーバ４０上の記憶済みのパスコード及びＳＥ　ＩＤと一致することを確認する。更に、段階１０００の受信済みアドレスと一致するものとして、受信したアドレスを検証する。この文脈内の、一致するという用語は、プロバイダサーバ２０によって承認された再アドレス指定又は転送を考慮して比較することを意味する。受信したＳＥ　ＩＤ、パスコード、及びアドレスが検証された場合、段階１４００で、ＭＤサーバ４０が、ユーザＭＤ６０の受信済み識別情報又はプロバイダサーバ２０に知られているマップされた等価物を、デジタル署名等の検証情報と共にＩＳ３０に伝送する。

【００８５】

段階１４１０で、ＩＳ３０が、利用者を識別するために利用される認証方法の指示、段階１０００のオープントランザクション要求とマッチさせるための段階１０００の受信済み識別情報、及び検証用の確認コードを含む認証メッセージをプロバイダサーバ２０に伝送する。

【００８６】

段階１４２０で、プロバイダサーバ２０が、段階１４１０の受信済み認証メッセージに応答し、所望のユーザページをユーザ装置５０Ａに伝送し、又は所望のトランザクションを許可する。プロバイダ帯域７０内で伝送されたパスワード情報はＣＥ１００によって暗号化されており、顧客帯域８０内で暗号化されて伝送されており、それによりセキュリティを大幅に改善していることに留意すべきである。更に、キーストロークロギングに遭いやすいＭＤ６０のキーパッド上及び装置のキーパッド５０Ａ上で如何なる情報も入力されていない。更に、ネットワークアドレスの検証によって介入者攻撃が防がれる。

【００８７】
段階１３８０で検証に失敗した場合、段階１４３０で、ログインの試みが失敗する。好ましくは、ログイン失敗の通知が、ユーザＭＤ６０及びユーザ装置５０Ａの両方に伝送される。
【００８８】
図１Ｅは、統合サーバ３０と連携して有利なセキュリティを提供し、ネットワークアドレスの一致を確認することによりセキュリティ強化を更にもたらすトランザクションシステム２００の一実施形態の高レベルブロック図を示す。トランザクションシステム２００は、ユーザＭＤ６０と様々な装置５０Ａ、５０Ｂ、５０Ｃのそれぞれとの間でＮＦＣ帯域、ＵＳＢ帯域、又は他の短距離通信によってもたらされ得る通信帯域１２０が提供されることを除き、トランザクションシステム１とあらゆる点で同様である。
【００８９】
動作面では、ユーザＭＤ６０が、現在の通信に使用されるネットワークアドレスの一覧、及びパスコードをそれぞれの装置５０に与える。与えられるパスコードは、任意選択的にＭＤ６０のオンボードＳＥ（不図示）によって暗号化される。ユーザＭＤ６０がそれぞれの装置５０に近接され、ユーザＭＤ６０は、ユーザＭＤ６０のネットワークアドレス、及びＭＤサーバ４０との通信に利用されるアドレス、並びに任意選択的に暗号化されたユーザパスコードを、ＮＦＣ通信インターフェイス６６を介してそれぞれの装置５０に提供する。更に、ユーザＭＤ６０がそれぞれの装置５０に近接されることに応答し、それぞれの装置５０が、通信に利用されるネットワークアドレスの一覧、トランザクションの量、及び番号等の受取人情報をユーザＭＤ６０に与える。従って、ＩＳ３０、ＭＤサーバ４０、又はプロバイダサーバ２０のどれもが、両方の帯域、即ち帯域７０及び帯域８０のネットワークアドレスを比較し、それらのネットワークアドレスが互いに一致する場合にのみ、要求されたトランザクションを承認するように構成され得る。
【００９０】
従って一実施形態では、利用者がユーザＭＤ６０によってＡＴＭ５０Ｂにログインし、ユーザＭＤ６０から受信されるプロバイダサーバ２０のネットワークアドレスがプロバイダサーバ２０の既知の通信アドレスに合致することに応答し、統合サーバ３０がトランザクションを承認する。
【００９１】
図２Ａは、２台のユーザ装置を利用するネットワーク通信にセキュリティの改善を提供するシステム３００の高レベルブロック図を示す。図２Ｂ～図２Ｃは、システム３００の動作の一実施形態の高レベル流れ図をそれぞれ示し、以下で更に詳しく説明する。
【００９２】
システム３００は、セキュリティモジュール３２０をその中に含むサーバ３１０と、モバイル機器サーバ（ＭＤＳ）３３０と、通知サーバ（ＮＳ）３４０と、ポータブルコンピュータとして制限なしに図示するユーザ装置５０Ａと、アプリケーション６２、ＮＦＣ通信インターフェイス６６を有し、ＣＥ１００と通信するユーザＭＤ６０とを含み、ＣＥ１００はその内部にＳＥ１１０、及び好ましくは入力装置１１５が埋め込まれる。ＮＦＣ通信インターフェイス６６とＣＥ１００との間の通信は、上記のように好ましくはＮＦＣ帯域１２０を介し、ＣＥ１００とユーザ装置５０Ａとの間の通信は、好ましくはＵＳＢ帯域１２０Ａを介する。一実施形態では、ＭＤ６０をユーザ装置５０Ａに近接させることに応答し、ユーザＭＤ６０とユーザ装置５０Ａとの間の通信がＮＦＣを介する。ＭＤＳ３３０とユーザＭＤ６０との間の通信は、点で埋められた双方向矢印として図示する無線ネットワーク３５０を介してであり、通知サーバＮＳ３４０とＭＤ６０との間の通信は、破線で示す通信経路３６０を介してである。ユーザ装置５０Ａとセキュリティサーバ３２０との間の通信は、線で埋められた双方向矢印として図示するセキュアソケットトンネリングプロトコル（ＳＳＴＰ）リンク３７０として示す、安全なトンネリング又はＶＰＮプロトコルによってである。セキュリティサーバ３２０は、ポイントツーポイントトンネリングプロトコル（ＰＰＴＰ）や、インターネットプロトコルセキュリティレイヤ２トンネリング

プロトコル（ＩＰＳＥＣ／Ｌ２ＴＰ）を含む様々なセキュリティのレベルを提供する。任意選択的に、セキュリティサーバ３２０は仮想私設網（ＶＰＮ）を更に支援するが、これは費用を増加させる。不都合なことにＶＰＮサーバは費用が高く、セキュリティの強化をもたらすものの、ＶＰＮサーバはセキュリティチェーン内の１つのリングに過ぎず、ＶＰＮサーバと通信する様々なユーザ装置等、セキュリティチェーンの他の部分は不正プログラムに対して脆弱であり、その結果ＶＰＮサーバのセキュリティは損なわれる。サーバ３１０は、一実施形態では安全な通信リンクである通信リンク３２５を介してＭＤＳ３３０と通信し、ＭＤＳ３３０はＮＳ３４０と通信する。

【００９３】

帯域という用語は、多くの場合は通信経路と区別なく使用し、従って２つの独立した通信経路は、２つの帯域通信としても知られる。

【００９４】

以下で更に説明するように、多重帯域通信により、セキュリティの強化がもたらされる。一例示的実施形態では、アドレスを確認することが、更に強化されたセキュリティをもたらす。

【００９５】

次に図２Ｂを参照し、システム３００の動作の第１の実施形態が示されている。段階３０００で、ユーザ装置５０Ａが、好ましくはユーザ名及びパスワード又はパスコードを提供することにより、サーバ３１０にログインする。一実施形態では、利用者の識別情報だけがサーバ３１０に提供される。段階３０１０で、サーバ３１０がユーザ名及びパスワードを確認し、通信リンク３２５を介し、ユーザ名情報を含む帯域外ログイン（ＯＯＢＬ）承認要求をＭＤＳ３３０に要求する。段階３０２０で、サーバ３１０が、好ましくは、ユーザＭＤ６０と連携してログインを進めるべきことを示すメッセージをユーザ装置５０Ａに伝送する。

【００９６】

段階３０３０で、段階３０１０の受信済みユーザ名に応答し、ＭＤＳ３３０が、ＭＤＳ３３０と相互認証するためのメッセージを、ユーザＭＤ６０のプロセッサ上で実行されるアプリケーション６２に好ましくはＮＳ３４０を介して伝送する。一実施形態では、相互認証後、ＭＤＳ３３０のメッセージがアプリケーション６２を更に起動し、ユーザＭＤ６０の表示部分上にログイン画面を表示させる。別の実施形態では、アプリケーション６２が、利用者に知らせることなしにＮＳ３４０からのメッセージに応答する。段階３０４０で、ユーザＭＤ６０が、位置情報、ＭＳＩＳＤＮ等のユーザＭＤ６０の識別情報、及び承認コードをＭＤＳ３３０に伝送する。アプリケーション６２がログイン画面を表示した場合、好ましくはＭＤＳ３３０及びサーバ３１０の１つに事前登録されたユーザ承認コードが更に伝送される。

【００９７】

段階３０５０で、ユーザＭＤ６０の受信済み識別情報を知られている識別情報と比較し、応答しているユーザＭＤ６０が、段階３０１０の受信済みログイン情報に関連することを確実にする。更に、期待される値との一致を確かめるために受信済みの位置情報を確認する。上記のように、物理的にあり得ない不一致だけが好ましくは却下される。

【００９８】

段階３０５０で受信済みのＩＤ及び位置情報が正当であると確認される場合、段階３０６０で、ＭＤＳ３３０が検証メッセージをサーバ３１０に伝送する。段階３０７０で、サーバ３１０が、ＳＳＴＰリンク３７０等のリンクの１つを介したサーバ３１０とユーザ装置５０Ａとの間の通信を承認する。

【００９９】

任意選択的な段階３０８０で、トランザクションのハイライトがサーバ３１０からＭＤＳ３３０に伝送され、ユーザＭＤ６０のディスプレイ上に、ユーザＭＤ６０にプッシュされる。或る特定の実施形態では、セキュリティを確保するために、ユーザ装置５０Ａによって行われているトランザクションの種類の指示がユーザＭＤ６０に伝送され、その表示

装置上に好ましくは時系列順に表示される。この指示は、好ましくは利用者が容易に見直せるように図表によって表わす方法で、好ましくはセッションの始まりから行われた他の操作に対して時系列順に表示される。ＭＤ６０の利用者が、ＭＤ６０の動作とユーザＭＤ６０上に表示される時系列順情報との間に食い違いがあることに気付いた場合、攻撃が確認され、利用者はサーバ３１０から接続を絶つことができる。任意選択的に、利用者は、ＭＤ６０により、又はウェブセッションを終了することにより、不正の疑いにつき更なる操作情報を要求することができる。別の実施形態では、５０Ａのユーザ装置の利用者によって実際には行われていない操作の指示がＭＤ６０上に表示されていないことを利用者が確認し、それはかかる指示が不正攻撃の表れの可能性があるからである。好ましくは、利用者がユーザ装置５０Ａ又はＭＤ６０によってサーバ３１０をログオフするまで、ＭＤ６０のモニタリングはアクティブのままである。

【０１００】

段階３０５０で、ユーザＭＤ６０の識別情報が正当であると確認されない場合、又は位置情報が期待される値と一致しない場合、段階３０９０で、トランザクションが失敗し、ユーザ装置５０Ａのログイン特権が拒否されたことを表示するメッセージが、好ましくはユーザＭＤ６０に送信される。

【０１０１】

従って図２Ｂのフローは、ＯＯＢＬ、継続的な帯域外監視により、ユーザ装置５０Ａとサーバ３１０との間の高度なセキュリティを提供する。

【０１０２】

図２Ｃは、アドレスを比較することに応答して、更にはＣＥ１００と連携してセキュリティの向上をもたらすための、図２Ａのシステムの動作の第２の実施形態の高レベル流れ図を示す。段階４０００で、パスワード又はＰＩＮ等のパスコードをＣＥ１００の入力装置１１５に入力する。好ましくは、入力されるパスワードは、ＣＥ１００のＳＥ１１０によって受信され、ＳＥ１００によって暗号化され、暗号化された形式で記憶される。ＳＥ１１０による暗号化は、好ましくはＳＥ１１０上に記憶される１つ又は複数の鍵に応じたものである。段階４０１０で、ユーザ装置５０Ａが利用者のジェスチャに応じてサーバ３１０にアクセスする。段階４０２０で、サーバ３１０がユーザ装置５０Ａにメッセージを送信し、そのメッセージは、ＣＥ１００を用いて安全な暗号化済みパスワードによってログインするために、ユーザ装置５０Ａの表示部分上に表示される。

【０１０３】

段階４０３０で、ＣＥ１００とユーザ装置５０Ａとの間の通信が確立される。一実施形態では、ＣＥ１００をＣＥ１００のＵＳＢポートに差し込むことによって通信が確立され、別の実施形態では、ＣＥ１００をユーザ装置５０のＮＦＣ通信インターフェイスに近接させることによって通信が確立される。ＳＥ１１０がユーザＭＤ６０に、好ましくは提供されたセキュリティ保護されたキーパッド１１５と共に埋め込まれる更に別の実施形態では、ユーザＭＤ６０を装置５０Ａに近接させることによって通信が確立される。従って、ＣＥ１００とユーザ装置５０との間の通信は、特定の通信帯域である通信リンク１２０を介する。段階４０４０で、段階４０００の暗号化されたパスワードが、通信帯域１２０Ａを介してユーザ装置５０Ａに伝送される。ＳＥ　ＩＤとして知られるＳＥ１１０の識別情報が、通信帯域１２０Ａを介してユーザ装置５０Ａに更に伝送される。ユーザ装置５０Ａは、ユーザ装置５０Ａの識別情報及び現在使用中のアクティブネットワークアドレスの一覧をＣＥ１００に伝送し、更に任意選択的に位置情報を伝送する。かかるアクティブネットワークアドレスの一覧は、ローカルアドレス、即ちユーザ装置５０Ａに現在関連するネットワークアドレスと、外部アドレス、即ちユーザ装置５０Ａが現在通信中のアドレスとを含む。一実施形態では、段階４０００の暗号化されたパスワードが通信帯域１２０Ａを介してユーザ装置５０Ａに伝送されず、代わりに、以下で説明するようにＭＤ６０にだけ伝送される。

【０１０４】

段階４０５０で、ユーザ装置５０Ａが、段階４０４０の受信済みの暗号化されたパスワ

ード、段階４０４０の受信済みＣＥ　ＩＤ、ユーザ装置５０Ａの識別情報、及び任意選択的な位置情報をサーバ３１０に伝送する。サーバ３１０は、受信済みの暗号化されたパスワードを復号してその妥当性を確認すること等により、受信した情報を可能な限り検証する。サーバ３１０は、自らの関連するネットワークアドレス、ユーザ装置５０Ａの受信済み識別情報、ＳＥ　ＩＤ、及び位置情報を、ＯＯＢＬを実行する要求と共に通信リンク３２５を介してＭＤＳ３３０に更に送信する。段階４０６０では、サーバ３１０が、好ましくは、ユーザＭＤ６０によってログインするためのメッセージをユーザ装置５０Ａに伝送する。

【０１０５】

段階４０７０では、上記のように安全なログインを得るための要求を、ＭＤＳ３３０がＮＳ３４０を介してユーザＭＤ６０に伝送し、この要求は、好ましくはユーザＭＤ６０とＣＥ１００との間の通信を確立するようにユーザＭＤ６０の利用者を促す。一実施形態では、ＣＥ１００をＭＤ６０のＮＦＣ通信インターフェイス６６に近接させることによって通信が確立されるが、これは決して限定的であることを意図しない。

【０１０６】

段階４０８０で、段階４０７０のプロンプトに応答してＣＥ１００とユーザＭＤ６０との間の通信が確立され、ＣＥ１００が、ＣＥ１００のＩＤ、段階４０００の暗号化されたパスワード、ネットワークアドレス、任意選択的な位置情報、及び段階４０５０で受信されるユーザ装置ＩＤをＭＤ６０のアプリケーション６２に伝送する。

【０１０７】

段階４０９０で、アプリケーション６２が、段階４０８０の受信済み情報を通信リンク３５０を介してＭＤＳ３３０に伝送する。段階４１００で、ＭＤＳ３３０が、段階４０７０でサーバ３１０から受信される情報との一致について、位置情報の一致や、ＣＥ１００のＩＤ、ユーザ装置５０の識別情報、暗号化されたパスワード、ネットワークアドレスの一致等、受信済み情報を検証する。一実施形態では、ＭＤＳ３３０が暗号化されたパスワードを検証のためにサーバ３１０に転送する。

【０１０８】

段階４１００で、ＭＤ６０から受信される全ての情報がサーバ３１０から受信される情報と一致する場合、段階４１１０で、ＭＤＳ３３０が検証メッセージをサーバ３１０に伝送する。段階４１２０で、サーバ３１０が、ＳＳＴＰリンク３７０等のリンクの１つを介したサーバ３１０とユーザ装置５０Ａとの間の通信を承認する。

【０１０９】

任意選択的な段階４１３０で、トランザクションのハイライトがサーバ３１０からＭＤＳ３３０に伝送され、ユーザＭＤ６０のディスプレイ上に、ユーザＭＤ６０にプッシュされる。具体的には、セキュリティを確保するために、ユーザ装置５０Ａによって行われているトランザクションの種類の指示がユーザＭＤ６０に伝送され、その表示装置上に好ましくは時系列順に表示される。この指示は、好ましくは利用者が容易に見直せるように図表によって表わす方法で、好ましくはセッションの始まりから行われた他の操作に対して時系列順に表示される。ＭＤ６０の利用者が、ＭＤ６０の動作とユーザＭＤ６０上に表示される時系列順情報との間に食い違いがあることに気付いた場合、攻撃が確認され、利用者はサーバ３１０から接続を絶つことができる。任意選択的に、利用者は、ＭＤ６０により、又はウェブセッションを終了することにより、不正の疑いにつき更なる操作情報を要求することができる。別の実施形態では、５０Ａのユーザ装置の利用者によって実際には行われていない操作の指示がＭＤ６０上に表示されていないことを利用者が確認し、それはかかる指示が不正攻撃の表れの可能性があるからである。好ましくは、利用者がユーザ装置５０Ａ又はＭＤ６０によってサーバ３１０をログオフするまで、ＭＤ６０のモニタリングはアクティブのままである。

【０１１０】

段階４１００で何らかの不一致が生じた場合、段階４１４０で、トランザクションが失敗し、ユーザ装置５０Ａのログイン特権が拒否されたことを表示するメッセージがユーザ

ＭＤ６０に送信され得る。

【０１１１】

上記の内容は、ＭＤＳ３３０が承認を行う実施形態において説明してきたが、これは決して限定的であることを意図しない。承認は、サーバ３１０、又はセキュリティサーバ３２０により範囲を超えることなしに同様に行われ得る。

【０１１２】

従って図２Ｃのフローは、ＯＯＢＬ、継続的な帯域外監視、及びネットワークアドレスに応じた高度なセキュリティにより、ユーザ装置５０Ａとサーバ３１０との間の高度なセキュリティを提供する。

【０１１３】

図３Ａは、モバイル機器サーバ（ＭＤＳ）３３０と連携して有利なセキュリティを提供し、ＭＤ６０との多重帯域通信を利用して幾つかのネットワークアドレスの一致を確認することによりセキュリティ強化を更にもたらすトランザクションシステム４００の一実施形態の高レベルブロック図を示す。トランザクションシステム４００は、クラウドコンピューティング環境４１０と、クラウドコンピューティング環境４１０内になくても良いプロバイダサーバ２０と、ＳＥ１１０及び入力装置１１５を有するＣＥ１００とを更に含む。クラウドコンピューティング環境４１０は、複数の独立したプロバイダサーバ２０、ＭＤＳ３３０、及びＮＳ３４０を含む。ＭＤ６０は、ＭＤのプロセッサ上でそれぞれ実行され、ローカルメモリ（不図示）上に記憶される、アプリケーション６２及びアプリケーション４６２を含む。一実施形態では、アプリケーション６２がＭＤＳ３３０に関連し、アプリケーション４６２がクラウドプロバイダサーバ２０に関連する。各プロバイダサーバ２０は、それぞれの通信リンク３２５を介してＭＤＳ３３０と通信する。

【０１１４】

図３Ｂは、ＬＡＮ、イントラネット、又は広域ネットワークを制限なしに含み得るネットワーク応用にセキュリティ強化をもたらす、トランザクションシステム４５０の高レベルブロック図を示す。トランザクションシステム４５０は、制限なしに固定局又は携帯計算装置とすることができるユーザ装置５０Ａを示す。多重帯域通信を利用してネットワークアドレス情報の一致を確認することに応じて、セキュリティの強化がもたらされる。ユーザＭＤ６０の代わりにユーザ装置５０Ａを設けることを除き、トランザクションシステム４５０はシステム４００と同様である。アプリケーション６２及びアプリケーション４６２は、それぞれユーザ装置５０Ａ上で実行され、ユーザ装置５０Ａは、点で埋められた双方向矢印として図示するネットワーク接続３５０を介してＭＤＳ３３０と通信し、破線で示す通信経路３６０を介してＮＳ３４０と更に通信する。簡単且つ明瞭にするために、ＭＤＳ３３０と通信するプロバイダサーバ３１０を１つだけ図示するが、これは決して限定的であることを意図せず、トランザクションシステム４００に関して上記で説明したように、範囲を超えることなしに複数のプロバイダサーバ３１０を設けても良い。

【０１１５】

図３Ｃは、ネットワークアドレスの一致を用いた高度なセキュリティをもたらすための、図３Ａ及び図３Ｂのそれぞれのトランザクションシステム４００、４５０の動作の高レベル流れ図を示し、明瞭にするために図３Ａ、図３Ｂ、及び図３Ｃを一緒に説明する。段階５０００で、トランザクションシステム４００内のユーザＭＤ６０又はトランザクションシステム４５０のユーザ装置５０Ａが、関連するユーザ名及び任意選択的なパスワードを任意選択的にアプリケーション６２を利用して供給し、複数のプロバイダサーバ２０、３１０のうちの特定の１つにログインする。ユーザＭＤ６０又はユーザ装置５０Ａは更に、好ましくはハードウェア識別情報や位置情報等の属性を制限なしに提供する。従ってトランザクションシステム４００では、ユーザ名及びパスワードが、帯域１として図示し、棒塗りつぶし双方向矢印として示す第１の通信チャネルを介して伝送される。ユーザＭＤ６０又はユーザ装置５０Ａとの間の通信は、プロバイダサーバ２０、３１０のアドレスがユーザＭＤ６０、ユーザ装置５０Ａによって取得されることに応答して行われる。アドレスは、利用者のジェスチャにより、ウェブアドレス又は制限なしに他の入力フォームを入

力することによって取得され得る。

【０１１６】

段階５０１０で、段階５０００のアドレス指定されたサーバが、受信済みのユーザ名及び任意選択的にパスワードを検証し、ユーザ名、任意選択的にユーザ装置５０Ａ又はユーザＭＤ６０のそれぞれに関する位置情報、実際のネットワークアドレス、段階５０００のアドレス指定されたサーバに関連するアドレス等の識別情報を含む、ＯＯＢＬ要求をＭＤＳ３３０に伝送する。任意選択的に、ログイン要求に関連しているというユーザ装置５０Ａ、ユーザＭＤ６０に関連するアドレス及びポートを制限なしに含む、検証に使用される追加情報が提供される。ＭＤＳ３３０との通信は、それぞれの通信リンク３２５を介して行われる。従って、プロバイダサーバ２０、３１０のアドレスは、制限なしにプロバイダサーバ２０、３１０等の信頼できる情報源を介してＭＤＳ３３０に伝送される。別の実施形態では、プロバイダサーバ２０、３１０のアドレスが、図３ＡではＤＢ３６０として図示する、ＭＤＳ３００と通信するデータベース内に記憶される。信頼できる情報源という用語は、ＭＤＳ３３０によって使用される可能性があり、プロバイダサーバ２０、３１０によって拒否され得ない任意の通信を含むことを意図する。

【０１１７】

段階５０３０で、ＭＤＳ３３０が、情報クエリをユーザ装置５０Ａ、ユーザＭＤ６０に好ましくはＮＳ３４０を介して伝送する。ユーザＭＤ６０、ユーザ装置５０Ａにおいて情報クエリを受信すると、アプリケーション４６２が好ましくは自動でアクティブになり、情報クエリに応答する。段階５０５０で、アプリケーション４６２及びＭＤＳ３３０が、ここでは帯域２で示す通信チャネル３５０を介して認証を好ましくは互いに行う。段階５０６０で、アプリケーション４６２が、好ましくはアドレス指定されたサーバのネットワークアドレスを含むログイン情報、好ましくはログイン通信情報をユーザ装置５０Ａ、ユーザＭＤ６０のプロセッサ及び／又は関連する記憶場所から任意選択的にアプリケーション６２を利用して受け取り、ユーザ装置５０Ａ、ユーザＭＤ６０、位置情報の属性等の他の関連情報、及び好ましくはハードウェアや周辺機器のシリアル番号等の他の識別情報を取得し、取得した情報を、ここでは帯域２で示す通信チャネル３５０を介してＭＤＳ３３０に伝送する。取得されるログイン情報は、ローカルアドレス、即ちユーザ装置５０Ａ、ユーザＭＤ６０に関連するネットワークアドレス及びポートと、外部アドレス、即ちユーザ装置５０Ａ、ユーザＭＤ６０が通信しているアドレス及びポートとを含む。ログイン情報は、デジタル指紋、デジタル署名、及びサーバの動的指紋情報を制限なしに更に含み得る。従って、ログイン情報の入力は、プロバイダサーバ２０、３１０との通信に利用される段階５０００の取得済みアドレスを含む。受信されるログイン情報は、ＭＤＳ３３０内に入力される。

【０１１８】

段階５０７０で、ＭＤＳ３３０が、入力されたログイン情報を段階５０１０の要求情報と比較する。具体的には、識別情報を確認するために、受信済みの任意の識別情報を受信済みの属性と比較する。更に、好ましくはアドレス指定されたサーバのネットワークアドレスを含み、好ましくはデジタル署名を含み、任意選択的にサーバの動的指紋情報を制限なしに含む、ログイン情報、好ましくはログイン通信情報の一覧を、一致要求内の情報と比較する。従って、段階５０１０で信頼できる情報源から取得されたプロバイダサーバ２０、３１０に関連するアドレスが、段階５０００のプロバイダサーバ２０、３１０に関連する取得された受信済み入力ネットワークアドレスと比較される。アドレスが一致しない場合、即ち段階５０１０の要求のアドレスが、段階５０６０内で伝送されるアドレス内で見つからない場合、帯域１のリンクが直接的でないとみられ、介入者攻撃等の不正攻撃が疑われる。任意選択的に、段階５０６０でアプリケーション４６２が取得した位置情報を、段階５０１０のそれぞれのサーバが取得した位置情報との一致に関して更に確認する。

【０１１９】

段階５０７０で、段階５０６０のアドレス及びポートを含む入力ログイン情報が、段階５０１０の信頼できる情報源から取得されたアドレスの何れかと一致することをＭＤＳ３

３０が見出す、即ち段階５０１０のアドレスが段階５０６０のアドレスの一覧内で見つかり、他の任意の識別情報が同様に一致する場合、段階５０９０で、ＭＤＳ３３０が段階５０１０のそれぞれのサーバに検証メッセージを伝送する。それに応答し、段階５１００で、段階５０１０のサーバ、即ちそれぞれのプロバイダサーバ２０又はサーバ３１０が、段階５０００のユーザＭＤ６０にサービスを提供できるようにする。

【０１２０】

段階５０７０で一致しない場合、段階５１１０でログインが失敗し、段階５０１０のサーバがアクセスを拒否する。

【０１２１】

従って図３Ｃのトランザクションフローは、単一のユーザＭＤ６０又はユーザ装置５０Ａのそれぞれに、２帯域セキュリティとしても知られる、強化された多重通信チャネルセキュリティを提供する。

【０１２２】

上記の内容は、ユーザ名及びパスワードがユーザ装置５０Ａ、ユーザＭＤ６０上に直接与えられ、帯域１を介して伝送される実施形態において説明してきたが、これは決して限定的であることを意図しない。ユーザ名及び／又はパスワードは、範囲を超えることなしにユーザ装置５０Ａ、ユーザＭＤ６０上のアプリケーション６２又はＳＥによって暗号化されても良い。同様に、上記のようにパスワードは、範囲を超えることなしにＣＥ１１０の入力装置１１５上に入力され、ＳＥ１１０によって暗号化され、ＮＦＣ通信によってアプリケーション４６２に伝送され得る。かかる実施形態では、キーロガーソフトウェアは、有利には利用者のパスワードをひそかに取得することができない。

【０１２３】

上記の内容は、ＮＳ３４０を設け、検証がＭＤＳ３３０によって遂行される実施形態において説明してきたが、これは決して限定的であることを意図しない。別の実施形態ではＮＳ３４０を設けず、ＭＤＳ３３０が全ての通信を遂行する。別の実施形態では、ＭＤＳ３３０に関して上記で説明した情報に応答し、アプリケーション４６２及びプロバイダサーバ２０又はサーバ３１０それぞれのうちの１つによって検証が行われる。ＭＤＳ３００は、範囲を超えることなしにプロバイダサーバ２０のうちの１つ又はサーバ３１０に組み込むことができ、又はクラウドコンピューティング環境４１０の外側に設けても良い。上記の内容は、記載したトランザクションがログインアクセスである実施形態において説明してきたが、これは決して限定的であることを意図しない。別の実施形態では、トランザクションがアクセスではなく、即ち貨幣的トランスファーである。この実施形態では、段階５０００のログイン情報をＰＩＮコード等の他の種類のユーザ入力情報で置き換えることができ、又は全く含めなくても良い。

【０１２４】

図３Ｄは、シングルサインオン機能を提供するための、図３Ａのトランザクションシステムの動作の高レベル流れ図を示す。とりわけ、プロバイダサーバ２０の１つ又は複数は、信頼できるサードパーティエンティティによる検証等、一定の条件下でログインにユーザ名及びパスワードを要求しない場合があり、ユーザ名及びパスワードの代わりにＭＤＳ３３０による検証を承認してアクセスを提供することができる。図３Ｄは、特に図４Ａのトランザクションシステム４００に関して説明しているが、これは決して限定的であることを意図しない。

【０１２５】

段階５５００で、特定のＭＤＳ３３０のシングルサインオン（ＳＳＯ）の承認に応答し、ユーザＭＤ６０が、アクセスを承認する要求を使ってアプリケーション６２によりそれぞれの通信リンク３２５を介してプロバイダサーバ２０にログインする。或る特定の実施形態では、ＳＳＯに応答してアクセスを承認する要求が、選択されたプロバイダサーバ２０によって示されるページ上に表示されるアイコンをクリックすることに応じたものである。トランザクションシステム４００内で認められるＭＤＳ３３０の数に制限はないので、好ましくは特定のＭＤＳ３３０が識別される。特定のＭＤＳ３３０に関するユーザ名が

提供されるが、プロバイダサーバ２０に関するユーザ名及びパスワードは好ましくは提供されない。上記のようにハードウェア識別情報、位置、アドレス等が示される、ユーザＭＤ６０の属性が読み取られる。

【０１２６】

段階５５１０で、プロバイダサーバ２０が、段階５０１０に関して上記で説明したようにネットワークアドレス情報、属性情報、及びＭＤＳ３３０に登録されたユーザ名を含むＳＳＯ要求を、識別されたＭＤＳ３３０に送信する。

【０１２７】

段階５５３０で、ＭＤＳ３３０と通信して記憶されるデータに基づいてアドレスに変換されるユーザ名に応答し、ＭＤＳ３３０が、ＮＳ３４０を介してユーザＭＤ６０にセッションＩＤを伝送する。ユーザＭＤ６０においてセッションＩＤを受信すると、アプリケーション４６２が好ましくは自動でユーザ入力を必要とすることなしにアクティブになり、セッションＩＤに応答する。段階５５５０で、アプリケーション４６２及びＭＤＳ３３０が、ここでは帯域２で示す通信チャネルを介して相互認証を行う。段階５５６０で、アプリケーション４６２が、ユーザＭＤ６０のプロセッサ及び／又は関連する記憶場所からネットワークアドレスを読み取り、ＭＤ６０や位置情報の属性等の他の関連情報、及び好ましくはハードウェアや周辺機器のシリアル番号等の他の識別情報を取得し、読み取った情報を帯域２を介してＭＤＳ３３０に伝送する。取得されるアドレスは、ローカルアドレス、即ちユーザＭＤ６０に関連するネットワークアドレスと、外部アドレス、即ちユーザＭＤ６０が通信しているアドレスとを含む。

【０１２８】

段階５５７０で、ＭＤＳ３３０が、受信した情報を段階５０１０の要求情報と比較する。具体的には、識別情報を確認するために、受信済みの任意の識別情報を受信済みの属性と比較する。更に、アドレスの一覧を、一致要求内のアドレスと比較する。アドレスが一致しない場合、即ち段階５５１０の要求のアドレスが、段階５５６０内で伝送されるアドレス内で見つからない場合、帯域１のリンクが直接的でないとみられ、介入者攻撃等の不正攻撃が疑われる。任意選択的に、段階５５６０でアプリケーション４６２が取得した位置情報を、段階５５１０のプロバイダサーバ２０が取得した位置情報との一致に関して更に確認する。

【０１２９】

段階５５７０で一致する場合、任意選択的な段階５５８０で、所定の時間制限内にユーザ名及びパスワードを伴う有効なログインが生じたかどうかを判定するために、ＭＤＳ３３０が承認されたプロバイダサーバ２０を確認する。検証はＭＤＳ３３０により複数のプロバイダサーバ２０に対して行われるので、有効なログインごとに、より多くのセキュリティ値がＭＤＳ３３０において蓄積されることを理解すべきである。従って、所定の期間にわたり複数回ログインに成功したユーザＭＤ６０は、たまにしかログインしていないユーザＭＤ６０よりも信頼され得る。検証の確立規則は、サービスプロバイダ２０とＭＤＳ３３０との間で予め定められる。例えば規則が、任意選択的な段階５５８０で、少なくとも１つの信頼できるエンティティ及び所定の期間を伴う少なくとも１回の有効なログインが見つかることである場合、段階５５９０で、ＭＤＳ３３０が検証メッセージ及び承認の詳細を段階５５１０の要求側プロバイダサーバ２０に伝送する。それに応答して、段階５６１０で、プロバイダサーバ２０が、段階５０００のユーザＭＤ６０にサービスを提供できるようにする。

【０１３０】

段階５５７０で一致しない場合、又は任意選択的な段階５５８０で適切なログインを識別できない場合、段階５６５０でログインが失敗し、プロバイダサーバ２０がアクセスを拒否する。

【０１３１】

従って、図３Ｃのトランザクションフローは、ＭＤＳ３３０に応答してＳＳＯ機能を提供する。

【０１３２】
次に図３Ｃの段階５０７０を参照し、図３Ｄの技法をここに適用できることを理解すべきである。従って、ＭＤＳ３３０は、ユーザ装置５０Ａ又はユーザＭＤ６０の検証履歴を制限なしに考慮するように構成され得る。検証はＭＤＳ３３０により複数のプロバイダサーバ２０に対して行われるので、それぞれの有効なログインは、ＭＤＳ３３０において蓄積されるユーザＭＤ６０のセキュリティ値を高める。従って、所定の期間にわたり複数回ログインに成功したユーザＭＤ６０は、たまにしかログインしていないユーザＭＤ６０よりも信頼され得る。従って一実施形態では、高セキュリティのプロバイダサーバ２０が、追加のログインハードルとして検証されたログインの証跡を要求し得る。

【０１３３】
図３Ｅは、履歴情報に基づくサインオン機能を提供するための、図３Ａのトランザクションシステムの動作の高レベル流れ図を示す。とりわけ、プロバイダサーバ２０の１つ又は複数は、信頼できるサードパーティエンティティによる検証等、一定の条件下でログインにユーザ名及びパスワードを要求しない場合があり、ユーザ名及びパスワードの代わりにＭＤＳ３３０による検証を承認してアクセスを提供することができる。図３Ｅは、特に図４Ａのトランザクションシステム４００に関して説明しているが、これは決して限定的であることは意図せず、包括的な履歴サインオン機能を提供することができる。

【０１３４】
段階５７００で、ユーザＭＤ６０が、それぞれの通信リンク３７０を介し、好ましくはアプリケーション４６２により、プロバイダサーバ２０へのアクセスを要求する。トランザクションシステム４００内で認められるＭＤＳ３３０の数に制限はないので、好ましくは特定のＭＤＳ３３０が識別される。特定のＭＤＳ３３０に関するユーザ名が提供されるが、プロバイダサーバ２０に関するパスワードは好ましくは提供されない。上記のようにハードウェア識別情報、位置、アドレス等が示される、ユーザＭＤ６０の属性が読み取られる。一実施形態では、ユーザ装置５０Ａがプロバイダサーバ２０へのアクセスを要求する。

【０１３５】
段階５７１０で、プロバイダサーバ２０が、ユーザＭＤ６０の属性、アドレス、属性情報、ＭＤＳ３３０に登録されたユーザ名等の他の任意選択的な情報を含む承認要求を、識別されたＭＤＳ３３０に送信する。

【０１３６】
段階５７２０で、プロバイダサーバ２０に事前に登録された条件に応答し、ＭＤＳ３３０が、ユーザＭＤ６０に関する履歴的な認証の詳細を取得し、現在の認証レベルを突き止める。

【０１３７】
段階５７３０で、ユーザＭＤ６０の現在の認証レベルが、プロバイダサーバ２０に関する事前登録された条件と比較される。現在の認証レベルが、事前登録された履歴的サインオン承認の所要の条件レベルを上回り、そのためユーザＭＤ６０の相互認証がプロバイダサーバ２０によって要求されない場合、段階５７６０で、履歴的な認証の詳細に応じてＭＤＳ３３０がユーザＭＤ６０を認証する。認証に成功した場合、段階５７７０で、ＭＤＳ３３０が検証情報及び承認の詳細をプロバイダサーバ２０に伝送し、認証の詳細を関連するメモリ内に更に記憶する。

【０１３８】
段階５７８０で、プロバイダサーバ２０が伝送された検証情報及び承認情報を確認し、段階５７９０で、プロバイダサーバ２０が、段階５７７０の伝送された検証情報及び承認情報に応答してユーザＭＤ６０とのトランザクションを可能にする。

【０１３９】
段階５７６０で認証に成功しなかった場合、段階５８００でアクセスが拒否される。

【０１４０】
段階５７３０で、現在の認証レベルが、事前登録された履歴的サインオン承認の所要の

条件レベルを下回り、そのためユーザＭＤ６０の相互認証がプロバイダサーバ２０によって要求される場合、段階５７４０で、ＭＤＳ３３０が、ユーザＭＤアプリケーション６２を呼び起こす認証要求を好ましくはＮＳ３４０を介してＭＤ６０に伝送する。段階５７５０で、プロバイダサーバ２０の所要の認証レベルに応じて、ユーザＭＤ６０とＭＤＳ３３０との間で相互認証が行われる。段階５７６０で、上記のようにＭＤＳ３３０がユーザＭＤ６０を認証する。

【０１４１】

上記の内容は、ネットワークアドレスに応じた認証に関して特に説明したが、これは決して限定的であることを意図しない。ネットワークアドレスの代わりに、範囲を超えることなしにデジタル署名等のデジタル指紋を利用することができる。一実施形態では、デジタル指紋がサーバの動的情報を含む。

【０１４２】

明確にするために別々の実施形態の文脈で説明した本発明の特定の特徴は、単一の実施形態において組み合わせて提供しても良いことが理解される。逆に、簡潔にするために単一の実施形態の文脈で説明した本発明の様々な特徴は、個別に又は任意の適切な副組合せによって提供することもできる。

【０１４３】

特記しない限り、本明細書で使用した全ての技術及び科学用語は、本発明が属する技術分野の当業者によって一般に理解されるのと同じ意味を有する。本明細書に記載のものと同様の又は等価の方法を本発明の実行又は試験に使用することができるが、本明細書では適切な方法を記載した。

【０１４４】

本明細書で言及した全ての刊行物、特許出願、特許、及び他の参考文献は、参照によりその全体を援用する。矛盾する場合、定義を含む本明細書が優先する。加えて、材料、方法、及び例は例示的に過ぎず、限定的であることを意図しない。

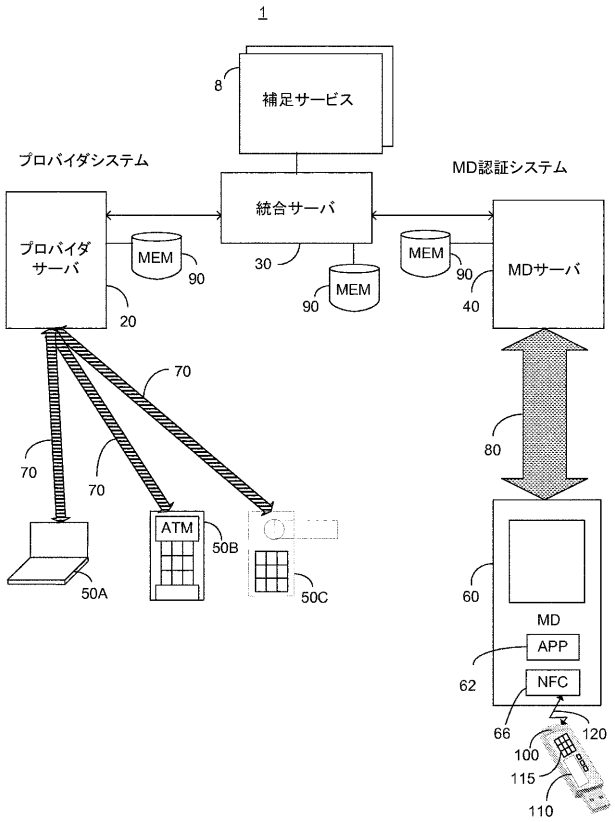
【０１４５】

本明細書で使用した「含む(include)」、「含む(comprise)」、「有する(have)」という用語、及びそれらの活用語は、「含むが、必ずしもそれだけに限定されない」ことを意味する。「接続される(connected)」という用語は、直接接続に限定されず、中間装置を介した接続をとりわけ含む。

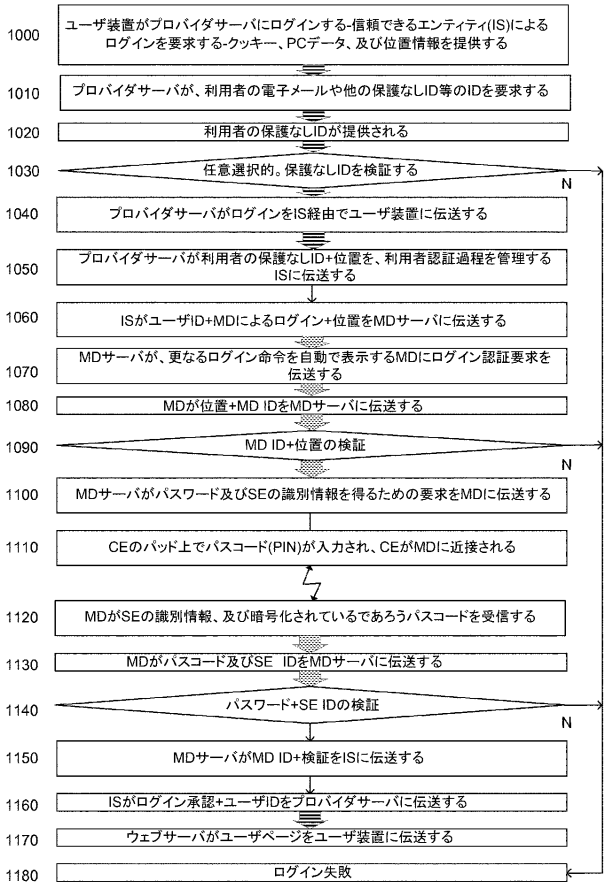
【０１４６】

当業者は、本発明が具体的に図示し、上記で説明した内容に限定されないことを理解されよう。むしろ、本発明の範囲は添付の特許請求の範囲によって定められ、上記の様々な特徴の組合せ及び副組合せの両方、並びに上記の説明を読めば当業者なら思い浮かぶだろうその改変形態及び修正形態を含む。

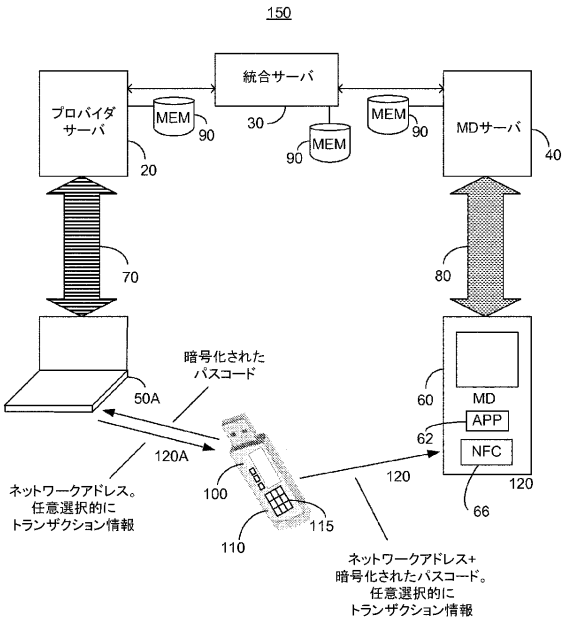
【図１Ａ】



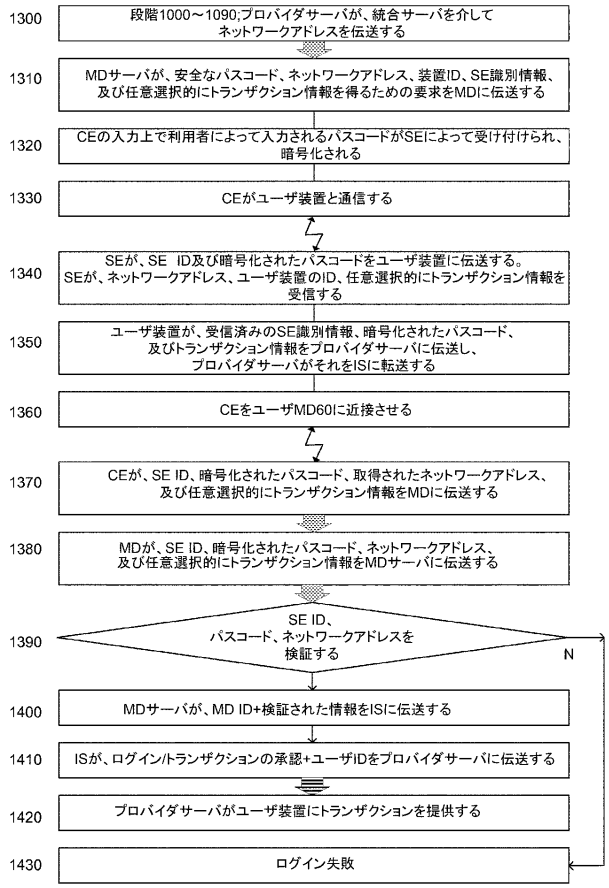
【図１Ｂ】



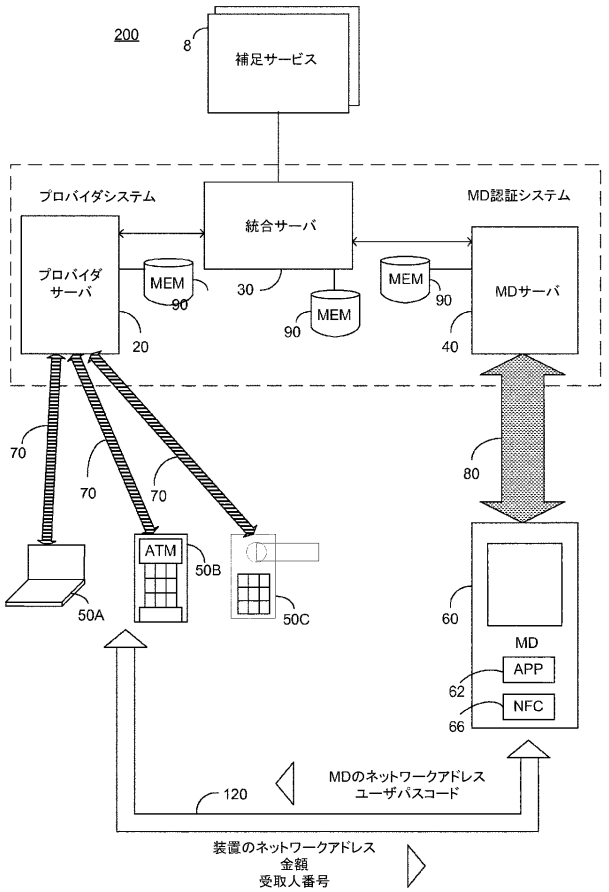
【図１Ｃ】



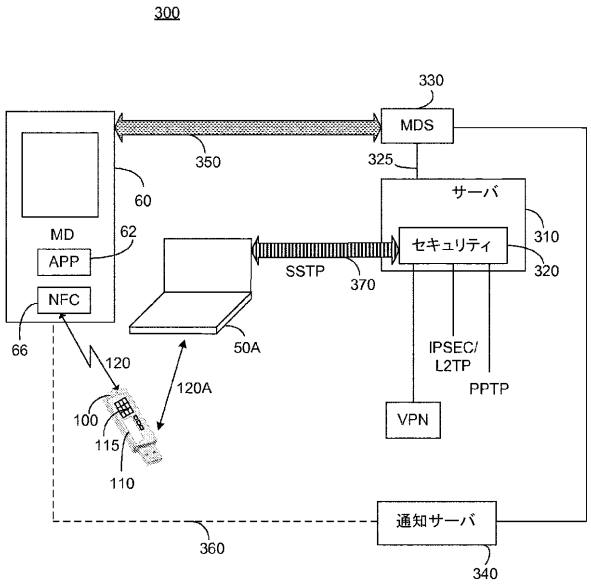
【図１Ｄ】



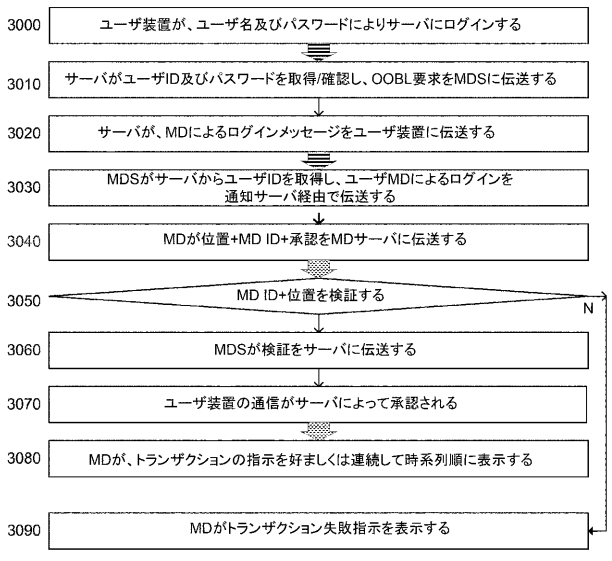
【図１Ｅ】



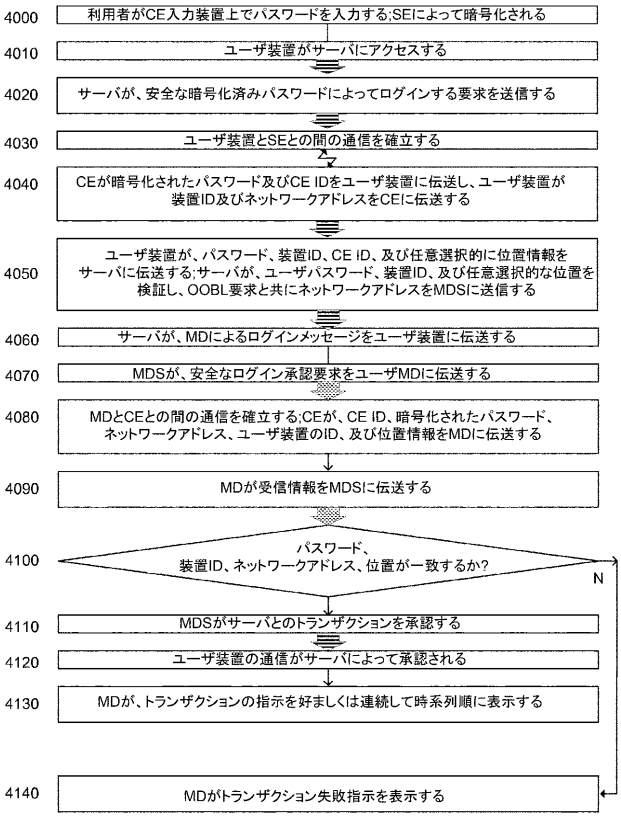
【図２Ａ】



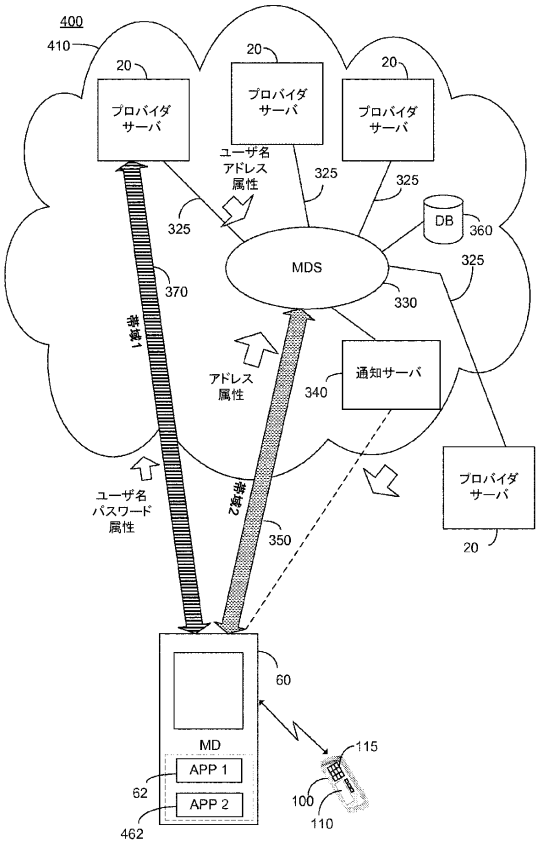
【図２Ｂ】



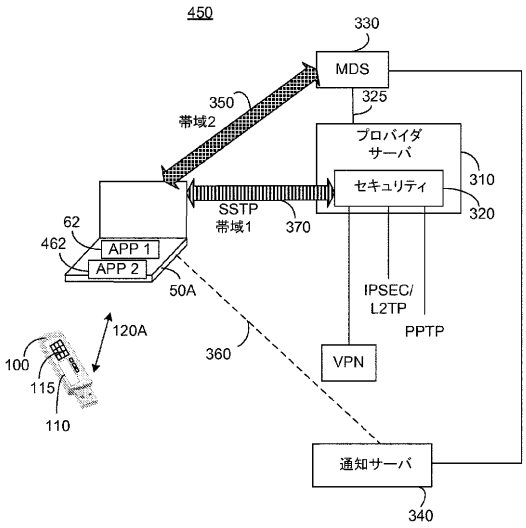
【図２Ｃ】



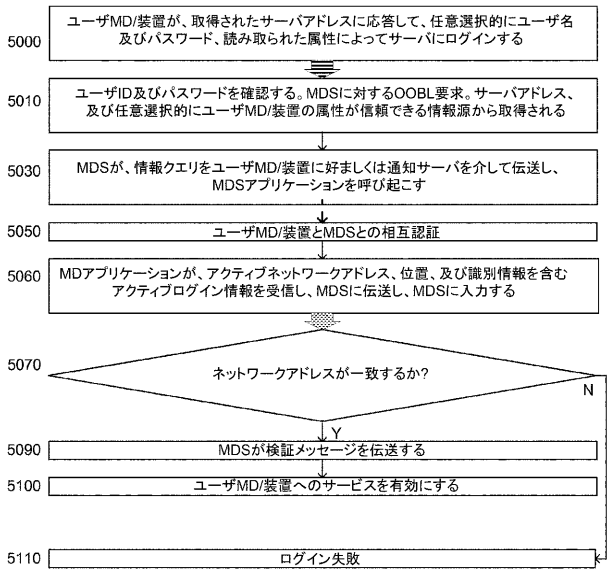
【図３Ａ】



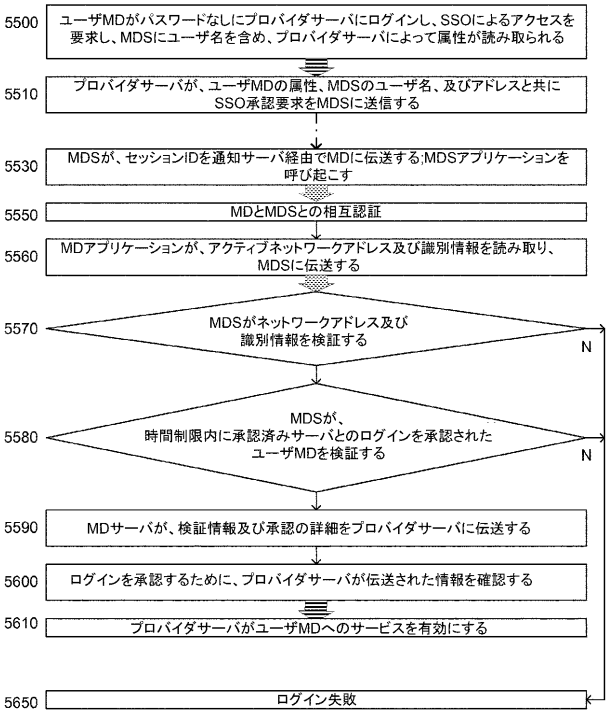
【図３Ｂ】



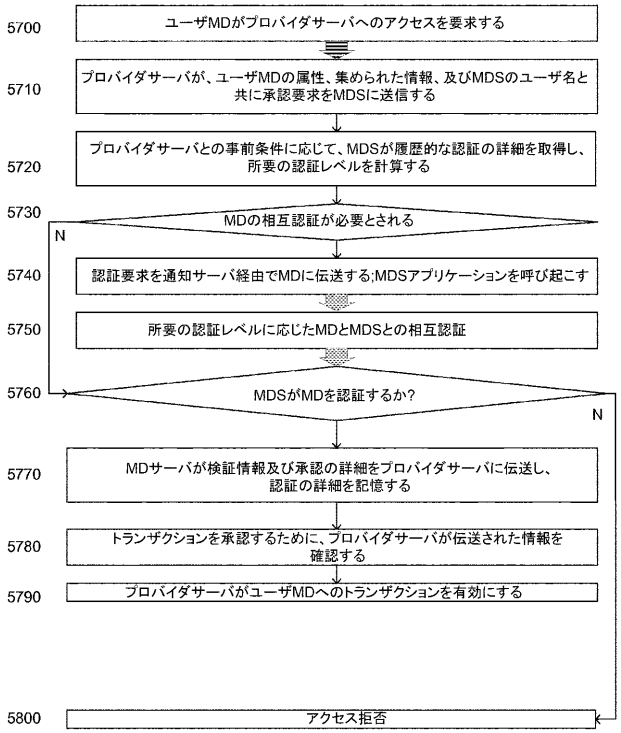
【図３Ｃ】



【図３Ｄ】



【図３Ｅ】



【手続補正書】
【提出日】平成26年12月11日(2014.12.11)
【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】
メモリ又はプロセッサ装置の少なくとも１つで実装されるモバイル機器サーバであって、ネットワークを介してプロバイダサーバに動作可能に結合されるように構成され、前記プロバイダサーバに関連する資源に計算装置を介してアクセスするための利用者からの要求を表す信号を前記プロバイダサーバから受信するように構成され、
前記利用者からの前記要求に関連するチャレンジを表す信号を、前記計算装置と別であり前記利用者に関連するモバイル計算装置にネットワークを介して送信するように構成され、
前記チャレンジに対する応答を表す信号を前記モバイル計算装置から受信するように構成され、
（１）前記計算装置の位置、及び（２）前記モバイル計算装置の位置を識別するように構成され、
前記計算装置の前記位置を前記モバイル計算装置の前記位置と比較し、位置関係の識別情報を生成するように構成され、
前記位置関係の識別情報が第１の既定の基準を満たし、前記チャレンジに対する前記応答が第２の既定の基準を満たす場合、前記利用者の肯定的な承認を表す信号を前記プロバイダサーバに対して、及び前記チャレンジに対する前記応答に基づいて送信するように構

成される、モバイル機器サーバ
を含む、装置。
【請求項２】
前記応答が、利用者から与えられる応答である、請求項１に記載の装置。
【請求項３】
前記応答が、前記モバイル計算装置において実行されるアプリケーションを介して提供される、利用者から与えられる応答である、請求項１に記載の装置。
【請求項４】
前記応答が、利用者から与えられるパスコード、又は前記モバイル計算装置に一意に関連する識別情報の少なくとも１つを含む、請求項１に記載の装置。
【請求項５】
前記要求がトランザクションの種類を有し、前記要求の前記トランザクションの種類が第１の既定のポリシ基準を満たす場合、前記チャレンジを表す前記信号を送信するように前記モバイル機器サーバが構成され、前記要求の前記トランザクションの種類が第２の既定のポリシ基準を満たす場合、前記利用者の肯定的な承認を表す前記信号を送信するように前記モバイル機器サーバが構成され、前記第２の既定のポリシ基準は、前記第１の既定のポリシ基準と異なる、請求項１に記載の装置。
【請求項６】
前記第１の既定の基準が、前記プロバイダサーバによって少なくとも部分的に定められる、請求項１に記載の装置。
【請求項７】
前記第１の既定の基準が、前記利用者によって少なくとも部分的に定められる、請求項１に記載の装置。
【請求項８】
前記モバイル機器サーバが、第１の期間中に前記計算装置の前記位置を前記モバイル計算装置の前記位置と比較するように構成され、前記第１の期間後に始まる第２の期間中に、及び前記位置関係の識別情報が第３の既定の基準を満たすことに基づき、前記チャレンジを表す前記信号を送信するように構成される、請求項１に記載の装置。
【請求項９】
前記資源にアクセスするための、前記利用者からの前記要求を表す前記信号が、安全でない通信チャネルを介して前記第１の計算装置から送信される、請求項１に記載の装置。
【請求項１０】
前記計算装置が第１の計算装置であり、前記応答が、前記第１の計算装置及び前記モバイル計算装置とは別の第２の計算装置において生成される第１のパスコードの表現を含み、
前記モバイル機器サーバが、前記第１のパスコードの前記表現を、前記第２の計算装置において生成され、前記第１の計算装置から受信される第２のパスコードの表現と比較するように構成され、
前記第１のパスコードの前記表現が前記第２のパスコードの前記表現と合致する場合、前記第１のパスコードの前記表現が前記第２の既定の基準を満たす、
請求項１に記載の装置。
【請求項１１】
前記利用者からの前記要求を表す前記信号が、前記計算装置において生成される、請求項１に記載の装置。
【請求項１２】
前記モバイル機器サーバは、前記要求が既定のポリシ基準を満たす場合、前記利用者からの前記要求に関連する前記チャレンジを表す前記信号を送信するように構成される、請求項１に記載の装置。
【請求項１３】
プロセッサによって実行される命令を表すコードを記憶する非一時的なプロセッサ可読

媒体であって、前記コードが、
プロバイダサーバの資源に計算装置を介してアクセスするための利用者からの要求を表す信号を前記プロバイダサーバから、及びネットワークを介して受信することであって、前記要求は複数の既定のトランザクションの種類からの、及び前記プロバイダサーバによって少なくとも部分的に定められるトランザクションの種類を有する、受信すること、
複数の既定のポリシ基準から既定のポリシ基準を前記トランザクションの種類に基づいて識別することであって、前記複数の既定のトランザクションの種類からのそれぞれのトランザクションの種類は、前記複数の既定のポリシ基準からの既定のポリシ基準に関連する、識別すること、
前記要求の前記トランザクションの種類が、前記複数の既定のポリシ基準からの第１の既定のポリシ基準を満たす場合、前記利用者からの前記要求に関連するチャレンジを表す信号を、前記計算装置と別であり前記利用者に関連するモバイル計算装置にネットワークを介して送信すること、及び
前記要求の前記トランザクションの種類が、前記複数の既定のポリシ基準からの第２の既定のポリシ基準を満たす場合であって、前記第２の既定のポリシ基準は前記第１の既定のポリシ基準と異なる、第２の既定のポリシ基準を満たす場合、前記チャレンジを表す前記信号を送信することなしに、前記利用者の肯定的な承認を表す信号を前記プロバイダサーバに送信すること
を前記プロセッサに行わせるためのコードを含む、非一時的なプロセッサ可読媒体。
【請求項１４】
肯定的な承認を表す前記信号を前記プロセッサに送信させる前記コードが、前記モバイル計算装置を介した利用者の介入なしに、前記利用者の肯定的な承認を表す前記信号を前記プロセッサに送信させるコードを含む、請求項１３に記載の非一時的なプロセッサ可読媒体。
【請求項１５】
前記チャレンジが第１のチャレンジであり、前記第１のチャレンジが第１の認証の種類に関連し、前記コードが、
前記要求の前記トランザクションの種類が、前記複数の既定のポリシ基準からの第３の既定のポリシ基準を満たす場合であって、前記第３の既定のポリシ基準は前記第１の既定のポリシ基準と異なり、第２のチャレンジが前記第１のチャレンジと異なる、第３の既定のポリシ基準を満たす場合、前記利用者からの前記要求に関連する前記第２のチャレンジを表す信号を前記モバイル計算装置に送信すること、及び
前記第２のチャレンジに対する応答が有効な応答である場合、前記利用者を承認すること
を前記プロセッサに行わせるためのコードを更に含む、請求項１３に記載の非一時的なプロセッサ可読媒体。
【請求項１６】
前記複数の既定のポリシ基準が、前記プロバイダサーバによって少なくとも部分的に定められる、請求項１３に記載の非一時的なプロセッサ可読媒体。
【請求項１７】
前記複数の既定のポリシ基準が、前記利用者によって少なくとも部分的に定められる、請求項１３に記載の非一時的なプロセッサ可読媒体。
【請求項１８】
前記計算装置が第１の計算装置であり、前記コードが、
前記チャレンジに対する応答を表す信号を前記モバイル計算装置から受信することであって、前記チャレンジに対する前記応答は、前記第１の計算装置及び前記モバイル計算装置とは別の第２の計算装置において生成される第１のパスコードの表現を含む、受信すること、
前記モバイル計算装置から受信される前記第１のパスコードを、前記第２の計算装置において生成され、前記第１の計算装置から受信される第２のパスコードの表現と比較する

こと、及び
（１）前記第１のパスコードの前記表現が前記第２のパスコードの前記表現と合致し、（２）前記要求の前記トランザクションの種類が、前記複数の既定のポリシ基準からの第１の既定のポリシ基準を満たす場合、前記利用者の肯定的な承認を表す信号を前記プロバイダサーバに送信すること
を前記プロセッサに行わせるためのコードを更に含む、請求項１３に記載の非一時的なプロセッサ可読媒体。
【請求項１９】
前記コードが、
前記計算装置の位置、及び前記モバイル計算装置の位置を識別すること、及び
前記計算装置の前記位置を前記モバイル計算装置の前記位置と比較し、位置関係の識別情報を生成すること
を前記プロセッサに行わせるためのコードを更に含み、
前記プロバイダサーバに送信することを前記プロセッサに行わせる前記コードが、前記位置関係の識別情報が既定の位置基準を満たす場合、前記利用者の肯定的な承認を表す前記信号を前記プロバイダサーバに送信することを前記プロセッサに行わせるコードを含む、
請求項１３に記載の非一時的なプロセッサ可読媒体。
【請求項２０】
プロセッサによって実行される命令を表すコードを記憶する非一時的なプロセッサ可読媒体であって、前記コードが、
プロバイダサーバの資源に第１の計算装置を介してアクセスするための利用者からの要求を表す信号を前記プロバイダサーバから、及びネットワークを介して受信すること、
前記利用者からの前記要求に関連するチャレンジを表す信号を、前記第１の計算装置と別であり前記利用者に関連するモバイル計算装置にネットワークを介して送信すること、
前記チャレンジに対する応答を表す信号を前記モバイル計算装置から受信することであって、前記応答は、前記第１の計算装置及び前記モバイル計算装置とは別の第２の計算装置において生成される第１のパスコードの表現を含む、受信すること、
前記モバイル計算装置から受信される前記第１のパスコードを、前記第２の計算装置において生成され、前記第１の計算装置から受信される第２のパスコードの表現と比較すること、及び
前記第１のパスコードの前記表現が前記第２のパスコードの前記表現と合致する場合、前記利用者の肯定的な承認を表す信号を前記プロバイダサーバに送信すること
を前記プロセッサに行わせるためのコードを含む、非一時的なプロセッサ可読媒体。
【請求項２１】
前記第２の計算装置が非接触要素である、請求項２０に記載の非一時的なプロセッサ可読媒体。
【請求項２２】
前記第１のパスコードの前記表現が、近距離通信（ＮＦＣ）又はユニバーサルシリアルバス（ＵＳＢ）の少なくとも１つを介して前記第２の計算装置から前記モバイル計算装置に送信される、請求項２０に記載の非一時的なプロセッサ可読媒体。
【請求項２３】
前記資源にアクセスするための、前記利用者からの前記要求を表す前記信号が第１の通信チャネルを介して送信され、前記チャレンジに対する前記応答を表す前記信号が前記第１の通信チャネルを介して送信され、前記第２のパスコードの前記表現が、前記第１の通信チャネルとは別の第２の通信チャネルを介して前記第１の計算装置から送信され、前記第１の通信チャネル又は前記第２の通信チャネルのうちの少なくとも１つが安全ではない、請求項２０に記載の非一時的なプロセッサ可読媒体。
【請求項２４】
アクセスするための前記利用者からの前記要求を表す前記信号が、前記第１の計算装置

において生成される、請求項２０に記載の非一時的なプロセッサ可読媒体。
【請求項２５】
メモリ又はプロセッサ装置の少なくとも１つで実装されるモバイル機器サーバであって、ネットワークを介してプロバイダサーバに動作可能に結合されるように構成され、前記プロバイダサーバに関連する資源にモバイル計算装置によってアクセスするための利用者からの要求を表す信号を、前記モバイル計算装置から、並びに第１の通信チャネル及び前記プロバイダサーバを介して受信するように構成され、
前記利用者からの前記要求に関連するチャレンジを表す信号を、前記モバイル計算装置に送信するように構成され、
前記チャレンジに対する応答を表す信号を前記モバイル計算装置から、及び第２の通信チャネルを介して受信するように構成され、
（１）第１の属性を表し、前記第１の通信チャネルを介して受信される指示、及び（２）第２の属性を表し、前記第２の通信チャネルを介して受信される指示を識別するように構成され、
前記第１の属性を表す前記指示を、前記第２の属性を表す前記指示と比較し、チャネル合致識別情報を生成するように構成され、
前記チャネル合致識別情報が既定の基準を満たす場合、前記利用者の肯定的な承認を表す信号を前記プロバイダサーバに送信するように構成される、モバイル機器サーバ
を含む、装置。
【請求項２６】
前記応答が、利用者から与えられる応答である、請求項２５に記載の装置。
【請求項２７】
前記モバイル機器サーバは、前記要求が既定のポリシ基準を満たす場合、前記利用者からの前記要求に関連する前記チャレンジを表す前記信号を前記モバイル計算装置に送信するように構成される、請求項２５に記載の装置。
【請求項２８】
前記既定の基準が第１の既定の基準であり、前記モバイル機器サーバが、前記チャレンジに対する前記応答が第２の既定の基準を満たす場合、前記利用者の前記肯定的な承認を表す前記信号を前記プロバイダサーバに送信するように構成される、請求項２５に記載の装置。
【請求項２９】
前記第１の属性又は前記第２の属性のうちの少なくとも１つが、前記モバイル計算装置の識別情報又は前記モバイル計算装置に関連する位置情報のうちの少なくとも１つを含む、請求項２５に記載の装置。
【請求項３０】
前記モバイル機器サーバが、前記利用者からの前記要求に関連する前記チャレンジを表す前記信号を、通知サーバを含む第３の通信チャネルを介して前記モバイル計算装置に送信するように構成される、請求項２５に記載の装置。

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No
PCT/IL2013/050318

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06Q20/42 G06Q20/32
ADD.

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)
G06Q

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

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/156436 A1 (FISHER MICHELLE [US] ET AL) 5 July 2007 (2007-07-05) abstract	1-32
X	WO 2006/090392 A2 (RSA SECURITY INC [US]; KLEIN AMIT [IL]; GOLAN ZOHAR [IL]) 31 August 2006 (2006-08-31) abstract	1-32
X	US 2007/055749 A1 (CHIEN DANIEL [US]) 8 March 2007 (2007-03-08) abstract	1-32
X	WO 2010/140876 A1 (BEMOBILE SDN BHD [MY]; HO CHING WEE [MY] INFINITIUM SOLUTIONS SDN BHD) 9 December 2010 (2010-12-09) abstract	1-32

-/--

[X] 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
23 July 2013	31/07/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Van Dop, Erik

Form PCT/ISA/210 (second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

International application No
PCT/IL2013/050318

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2007/107044 A1 (YUEN PHILIP [US] ET AL) 10 May 2007 (2007-05-10) abstract -----	1-32

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/IL2013/050318

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2007156436 A1	05-07-2007	US 2007156436 A1	05-07-2007
		US 2010161403 A1	24-06-2010
WO 2006090392 A2	31-08-2006	EP 1866783 A2	19-12-2007
		JP 2008532133 A	14-08-2008
		US 2008147837 A1	19-06-2008
		WO 2006090392 A2	31-08-2006
US 2007055749 A1	08-03-2007	US 2007055749 A1	08-03-2007
		WO 2007030764 A2	15-03-2007
WO 2010140876 A1	09-12-2010	NONE	
US 2007107044 A1	10-05-2007	NONE	

Form PCT/ISA/210 (patent family annex) (April 2005)

フロントページの続き

(51)Int.Cl.		F I		テーマコード（参考）
G06K 7/10	*(2006.01)*	G06K	7/10	100
H04W 12/06	*(2009.01)*	H04W	12/06	
H04W 84/10	*(2009.01)*	H04W	84/10	110

(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 ワイナー，アヴィシュ ヤコブ
イスラエル国，テル アビブ ６９１２７１１，ボイヤー ストリート １２
(72)発明者 ネマン，ラン
イスラエル国，ラマト ガン ５２２８６０１，バッダー ストリート ４

Ｆターム(参考) 5B035 BA06 BB09
5B072 CC39 DD10
5K067 AA30 BB21 DD17 EE02 EE04 EE10 EE12 EE16 EE35 EE39
FF02 HH17 HH22 HH23