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

特許第5844471号
(P5844471)

(45)発行日　平成28年1月20日(2016.1.20)　(24)登録日　平成27年11月27日(2015.11.27)

(51)Int.Cl.		F I		
G06F 13/00	(2006.01)	G06F	13/00	510A
G06F 21/30	(2013.01)	G06F	21/30	
G06F 21/10	(2013.01)	G06F	21/10	

請求項の数 30　(全 20 頁)

(21)出願番号	特願2014-530619 (P2014-530619)
(86)(22)出願日	平成24年2月16日 (2012.2.16)
(65)公表番号	特表2014-528129 (P2014-528129A)
(43)公表日	平成26年10月23日 (2014.10.23)
(86)国際出願番号	PCT/MY2012/000024
(87)国際公開番号	WO2013/043035
(87)国際公開日	平成25年3月28日 (2013.3.28)
審査請求日	平成26年12月3日 (2014.12.3)
(31)優先権主張番号	PI2011004430
(32)優先日	平成23年9月19日 (2011.9.19)
(33)優先権主張国	マレーシア(MY)

早期審査対象出願

(73)特許権者　505362399
イー－ロック・コーポレーション・エスディーエヌ・ビーエイチディー
マレーシア・５０４５０・クアラルンプール・ジャラン・ピナン・１９・ユーオーエー・センター・レベル・２６・ビジネス・スイート・１９Ａ－２６－３
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100064908
弁理士　志賀　正武
(74)代理人　100089037
弁理士　渡邊　隆
(74)代理人　100110364
弁理士　実広　信哉

最終頁に続く

(54)【発明の名称】インターネットベースのアプリケーションへのアクセスを制御する方法

(57)【特許請求の範囲】

【請求項１】

第１のインターネット利用可能デバイス（１）を介してのインターネットベースのアプリケーション（３）へのアクセスを制御する方法であって、アプリケーションは、アプリケーションの登録ユーザによる有効なログイン認証情報の提出を要求し、前記方法は：

ａ）ユーザに関連付けられた第２のインターネット利用可能デバイス（２）によってインターネットを介して送信される固有の認証コードを含むコマンドをコンピュータサーバ（４）で受信するステップを有していて、前記固有の認証コードの送信は、ユーザによって開始され、

ｂ）更に、受信した固有の認証コードとデータベースに格納された複数の固有の認証コードとを比較することによって、第２のデバイス（２）の身元を前記コンピュータサーバ（４）で判断するステップを有していて、各固有の認証コードは、アプリケーションの異なる登録ユーザに関連付けられ、

ｃ）更に、ステップｂ）で身元を有効に判断する時、前記コマンドに基づきアクセス制御ステータスを前記コンピュータサーバ（４）で設定するステップを有していて、アクセス制御ステータスは、ｉ）前記アプリケーション（３）へのアクセスを可能にするように、またはｉｉ）前記アプリケーション（３）へのアクセスを否定するように設定されることができ、

ｄ）更に、前記コンピュータサーバ（４）が、

ｉ）アクセス制御ステータスがアプリケーションへのアクセスを可能にするように設定さ

れる場合、前記第１のインターネット利用可能デバイスを介してのの有効なログイン認証情報の提出時にアプリケーション（３）へのアクセスを可能にし、
ｉｉ）アクセス制御ステータスがアプリケーションへのアクセスを否定するように設定される場合、前記第１のインターネット利用可能デバイスを介してのの有効なログイン認証情報の提出時でもアプリケーションへのアクセスを否定するステップを有している
ことを特徴とする方法。
【請求項２】
前記コンピュータサーバ（４）は、前記コマンドがアプリケーション（３）へのアクセスを可能にするためのものである時、ステップｃ）でアプリケーション（３）へのアクセスを可能にするようにアクセス制御ステータスを設定することを特徴とする請求項１に記載の方法。
【請求項３】
前記コンピュータサーバ（４）は、前記コマンドがアプリケーション（３）へのアクセスを否定するためのものである時、ステップｃ）でアプリケーション（３）へのアクセスを否定するようにアクセス制御ステータスを設定することを特徴とする請求項１に記載の方法。
【請求項４】
前記ステップａ）で受信したコマンドは、前記第２のインターネット利用可能デバイス（２）上でデバイスベースのアプリケーションを起動するユーザによって生成されることを特徴とする請求項１～３の何れか１項に記載の方法。
【請求項５】
前記固有の認証コードは、前記第２のインターネット利用可能デバイス（２）の一部分を成す固有の識別コードを含むことを特徴とする請求項４に記載の方法。
【請求項６】
前記固有の認証コードはまた、登録ユーザに関連付けられたユーザ識別子を含むことを特徴とする請求項５に記載の方法。
【請求項７】
前記固有の認証コードは、デバイスベースのアプリケーションによって暗号化されることを特徴とする請求項４～６の何れか１項に記載の方法。
【請求項８】
前記固有の識別コードは、前記第２のインターネット利用可能デバイス（２）の国際移動体装置識別番号（ＩＭＥＩ）、移動体装置識別番号（ＭＥＩＤ）、または電子シリアル番号（ＥＳＮ）であることを特徴とする請求項５～７の何れか１項に記載の方法。
【請求項９】
前記コンピュータサーバ（４）は、インターネットベースのアプリケーション（３）にリンクされた認証サーバであることを特徴とする請求項１～８の何れか１項に記載の方法。
【請求項１０】
前記第２のインターネット利用可能デバイス（２）は、移動式デバイスであることを特徴とする請求項１～９の何れか１項に記載の方法。
【請求項１１】
前記第１のインターネット利用可能デバイス（１）は、個人コンピュータデバイスであることを特徴とする請求項１～１０の何れか１項に記載の方法。
【請求項１２】
前記方法はまた、ステップｃ）の前に追加して：
第１および第２のインターネット利用可能デバイスの各地理的位置を前記コンピュータサーバ（４）で比較するステップと；
第１および第２のインターネット利用可能デバイスの地理的位置が互いに近接しているかを前記コンピュータサーバ（４）で判断するステップと；
を含むことを特徴とする請求項１～１１の何れか１項に記載の方法。

【請求項１３】
前記コマンドに基づきアクセス制御ステータスをコンピュータサーバ（４）で設定するステップｃ）はまた、第１および第２のインターネット利用可能デバイスの地理的位置が互いに近接していることの判断に依存することを特徴とする請求項１２に記載の方法。
【請求項１４】
前記コンピュータサーバ（４）で比較される各第１および第２のインターネット利用可能デバイスの地理的位置は、町および国情報であることを特徴とする請求項１２または１３に記載の方法。
【請求項１５】
前記第１のインターネット利用可能デバイス（１）の地理的位置は、ＩＰアドレス分析によって導出されることを特徴とする請求項１２～１４の何れか１項に記載の方法。
【請求項１６】
前記第２のインターネット利用可能デバイス（２）の地理的位置は、衛星信号、移動体通信基地局情報、およびWi-Fiアクセスポイント情報の１つまたは複数から導出されることを特徴とする請求項１２～１５の何れか１項に記載の方法。
【請求項１７】
登録ユーザに関連付けられたインターネット利用可能デバイス（５）を介してのインターネットベースのアプリケーション（３）へのアクセスを制御する方法であって、アプリケーションは、アプリケーションの登録ユーザによる有効なログイン認証情報の提出を要求し、前記方法は、
ａ） インターネット利用可能デバイス（５）によってインターネットを介して送信される固有の認証コードを含むコマンドをコンピュータサーバ（４）で受信するステップを有していて、前記固有の認証コードの送信は、ユーザによって開始され、
ｂ） 更に、受信した固有の認証コードとデータベースに格納された複数の固有の認証コードとを比較することによって、デバイス（５）の身元を前記コンピュータサーバ（４）で判断するステップを有していて、各固有の認証コードは、アプリケーションの異なる登録ユーザに関連付けられ、
ｃ） 更に、ステップｂ）で身元を有効に判断する時、前記コマンドに基づきアクセス制御ステータスを前記コンピュータサーバ（４）で設定するステップを有していて、アクセス制御ステータスは、ｉ）前記アプリケーション（３）へのアクセスを可能にするように、またはｉｉ）前記アプリケーション（３）へのアクセスを否定するように設定され、
ｄ） 更に、前記コンピュータサーバ（４）が、
ｉ）アクセス制御ステータスがアプリケーションへのアクセスを可能にするように設定される場合、前記インターネット利用可能デバイス（５）を介しての有効なログイン認証情報の提出時にアプリケーション（３）へのアクセスを可能にし、
ｉｉ）アクセス制御ステータスがアプリケーションへのアクセスを否定するように設定される場合、前記インターネット利用可能デバイスを介しての有効なログイン認証情報の提出時でもアプリケーションへのアクセスを否定するステップを有している
ことを特徴とする方法。
【請求項１８】
前記コンピュータサーバ（４）は、前記コマンドがアプリケーション（３）へのアクセスを可能にするためのものである時、ステップｃ）でアプリケーション（３）へのアクセスを可能にするようにアクセス制御ステータスを設定することを特徴とする請求項１７に記載の方法。
【請求項１９】
前記コンピュータサーバ（４）は、前記コマンドがアプリケーション（３）へのアクセスを否定するためのものである時、ステップｃ）でアプリケーション（３）へのアクセスを否定するようにアクセス制御ステータスを設定することを特徴とする請求項１７に記載の方法。
【請求項２０】

前記ステップａ）で受信したコマンドは、前記インターネット利用可能デバイス（５）上でデバイスベースのアプリケーションを起動するユーザによって生成されることを特徴とする請求項１７～１９の何れか１項に記載の方法。

【請求項２１】

前記固有の認証コードは、前記インターネット利用可能デバイス（５）の一部分を成す固有の識別コードを含むことを特徴とする請求項２０に記載の方法。

【請求項２２】

前記固有の認証コードはまた、登録ユーザに関連付けられたユーザ識別子を含むことを特徴とする請求項２１に記載の方法。

【請求項２３】

前記固有の認証コードは、デバイスベースのアプリケーションによって暗号化されることを特徴とする請求項２０～２２の何れか１項に記載の方法。

【請求項２４】

前記固有の識別コードは、デバイス（５）の国際移動体装置識別番号（ＩＭＥＩ）、移動体装置識別番号（ＭＥＩＤ）、または電子シリアル番号（ＥＳＮ）であることを特徴とする請求項２１～２３の何れか１項に記載の方法。

【請求項２５】

前記コンピュータサーバ（４）は、インターネットベースのアプリケーション（３）にリンクされた認証サーバであることを特徴とする請求項１７～２４の何れか１項に記載の方法。

【請求項２６】

前記インターネット利用可能デバイス（５）は、移動式デバイスであることを特徴とする請求項１７～２５の何れか１項に記載の方法。

【請求項２７】

インターネットベースのアプリケーションの登録ユーザによるインターネットベースのアプリケーションへのアクセスを制御するためのデバイスベースのアプリケーションを含む個人のインターネット利用可能デバイスであって、前記デバイスベースのアプリケーションは、

前記個人のインターネット利用可能デバイスの一部分を成す固有の識別コードを読み取り、

前記固有の識別コードを含むコマンドを生成して、コンピュータサーバへインターネットを介して送信するように適合され、前記コマンドは、ｉ）アプリケーションへのアクセスを可能にするためのものであり、またはｉｉ）アプリケーションへのアクセスを否定するためのものであり、

前記コンピュータサーバへ前記コマンドを送信するためのデバイスベースのアプリケーションの起動は、インターネットベースのアプリケーションへのアクセスを可能にするか、または不可にするユーザの意図を示すことを特徴とする個人のインターネット利用可能デバイス。

【請求項２８】

前記固有の識別コードは、前記個人のインターネット利用可能デバイスの国際移動体装置識別番号（ＩＭＥＩ）、移動体装置識別番号（ＭＥＩＤ）、または電子シリアル番号（ＥＳＮ）であることを特徴とする請求項２７に記載の個人のインターネット利用可能デバイス。

【請求項２９】

デバイスベースのアプリケーションはまた、個人のインターネット利用可能デバイスの地理的位置を判断し、コンピュータサーバへインターネットを介して地理的位置データを送信するように適合されることを特徴とする請求項２７または２８に記載の個人のインターネット利用可能デバイス。

【請求項３０】

地理的位置は、衛星信号、移動体通信基地局情報、およびWi-Fiアクセスポイント情報

の１つまたは複数から導出されることを特徴とする請求項２９に記載の個人のインターネット利用可能デバイス。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、オンラインサービスプロバイダのウェブサイト等のインターネットベースのアプリケーションへのアクセスを制御することに関する。

【背景技術】

【０００２】

インターネットの導入およびユーザに提供される前例のないアクセスに伴い、サービスプロバイダの全ての態様は、オンラインサービスの提供へ着実に向かってきている。オンラインバンキング、コマースサービス、ショッピング、ウェブベースのｅメールアカウント等は、現在すっかりありふれている。

【０００３】

ワイヤレスブロードバンドインフラストラクチャおよびサービスの導入および拡散はそれ以来、インターネットへの接続をユーザに提供するだけでなく、オンラインサービスの使用を拡張してきた。これはまた、ノート型個人コンピュータからインターネットおよびデータ機能を備えた移動式電話に至るまで、多数の製造者による多種多様な、携帯式インターネット利用可能なデバイスの開発および導入に対する推進力を提供してきた。

【０００４】

そのような携帯式デバイスの開発は、衰えることなく続き、過去１０年間、我々は、演算能力およびインターネット接続性において継続的に進化し継続的に向上した、インターネットをさらに改革した、スマートフォンとして知られる新世代の携帯式インターネット利用可能なデバイスの導入を見てきた。用語スマートフォンは一般に、進化した演算機能およびインターネット接続性を有する移動式電話に関して使用され、スマートフォンは現在ありふれており、日常生活の中核であり、それを取り囲んでいる。

【０００５】

しかし、この新規で前例のないインターネット接続レベルは、データセキュリティに関して並行した終わりのない仕事をもたらし、それは、ウェブページおよびオンラインデータベースを保護することだけでなく、インターネットベースのアプリケーション、特に金融または商業アプリケーションへのユーザによる安全なアクセスを保証することを含む。

【０００６】

インターネットを介したオンラインサービスの導入以来、オンラインサービスプロバイダは、基本的には特定のオンラインサービスに関するユーザの個人オンラインＩＤおよびパスワードの盗用を含む身元の盗用によるユーザアカウントへの違法なアクセスを得る方法を求める悪質なパーティに継続的に対処してきた。これらの悪質なパーティによって使用される周知の方法は、フィッシング、ファーミング、キーロギング、および介入者攻撃を含む。

【０００７】

フィッシングは、オンラインサービスのユーザを騙して、悪質なパーティによって作成された詐欺のウェブサイト（即ち、スプーフ）がオンラインサービスプロバイダの本当のウェブサイトであると信じさせ、後続的に個人オンラインＩＤおよびパスワードを悪質なパーティに暴露するプロセスに言及する。

【０００８】

実際、フィッシング攻撃は、詐欺のコンテンツを備えるｅメールで始まり、本当のウェブサイトの外観にかなり似せてあるかまたはコピーした詐欺のウェブサイトを何人かの受信者が訪問することを望んで、潜在的犠牲者に送信される。犠牲者はその後、騙されて自分のＩＤおよびパスワードを入力および提出し、悪質なパーティの手に落ちる。

【０００９】

ファーミングは、フィッシングの技術と同じ目的を持つＩＤ盗用のより高度な技術であ

る。詐欺のｅメールの配信およびユーザの無知を悪用することに代えて、ファーミングは、ユーザの身元が盗まれることになるよく似た詐欺のウェブサイトへ、本当のウェブサイトを訪問しようとするユーザを個別にそらす。

【００１０】

キーロギングは、ユーザが本当のウェブサイトにこれらログイン認証情報（login credentials）を提出する時、ユーザＩＤおよびパスワードを盗用するために使用される技術である。これは一般に、先ずユーザのキーストロークを記録するスパイウェアまたはトロイの木馬にユーザの個人コンピュータまたはインターネット利用可能なデバイスを感染させることによって達成される。記録されたキーストロークデータは、ユーザによって頻繁にタイプされたユーザＩＤおよびパスワードを含み、悪質なパーティへ定期的に送信される。

【００１１】

介入者攻撃は、ユーザと目標のオンラインサービスプロバイダのウェブサイトとの間にいわゆる中間者（ＭＩＭ）を置くことを含む。通常、ＭＩＭは、ユーザのログイン認証情報の盗用またはログインセッションの乗っ取りを求める悪質なパーティにユーザとオンラインサービスプロバイダのウェブサイトとの間の情報を中継することができる。

【００１２】

介入者攻撃の強みは、提供される全ての情報が正しく見えるので、ＭＩＭが実際にオンラインサービスプロバイダのウェブサイトであるとユーザが思い込み、同様にオンラインサービスプロバイダは、全てのログイン認証情報が正しいので、ユーザと直接対話していると想定することである。

【００１３】

介入者攻撃は明らかに、無防備なユーザが介入者を通して追加の認証情報を実際に提出することに気付かないので、追加の認証コードを提出するようにユーザに要求する多数の２要素認証手法を回避することができる進化した攻撃形式である。

【００１４】

現在、上記説明したＩＤ盗用の形式に対する多数の周知の対応策があるが、ほとんどは、問題に対して部分的な解決策を提供するだけであり、実装するのに面倒であり、コストがかかるだけである。例えば：

－　スパムフィルタは、ｅメールベースのフィッシングを防ぐのに効果があるだけで、ファーミングには効果がない。

－　質疑応答チャレンジレスポンス（question and answer challenge response）は、ユーザが無知であることを通じて騙されて情報を暴露することがあるので、未だフィッシングには脆弱である。

－　既知の秘密テキストまたはユーザの画像を表示することによるサーバ識別は、キーロギングを防ぐことはなく、ユーザとオンラインサービスプロバイダのウェブサーバとの間に介入者がいることを単に見落とす。

－　トークンベースの認証（ハードウェアトークンおよびＳＭＳベースのトークンの両方）は、フィッシングおよびファーミングを共に防ぐが、進化した介入者攻撃には未だ脆弱である。

－　クライアントデジタル証明書およびスマートカードは、堅牢な認証ソリューションであるが、指数関数的に増加し続ける非常に多くのインターネット利用可能なデバイスが使用されていること、およびインターネットの急速に拡大する接続性および使用量を考慮する時、大規模なシステムを管理するには面倒であり、そのようなシステムに配置するにはコストがかかる。

【００１５】

ＷＯ２００７／０５０９３２Ａ２は、インターネットベースのアプリケーションへのアクセスを制御する方法、特に帯域外のシグナリング、特に電話ネットワークを介してインターネットベースのアプリケーションへのアクセスを制御するシステムおよび方法を開示する。ＷＯ２００７／０５０９３２Ａ２では、インターネットベースのアプリケーション

に対する詐欺または権限のない使用の可能性は、電話の使用を介してユーザのログイン認証情報のプロセスを可能にするかまたは拒否する能力をユーザに与えることによって、低減される。

【００１６】

電話ネットワークに関して開示されたシステムおよび方法に依存すると、ユーザが電話をかけるように要求するという欠点があり、故に頻繁に移動するユーザにとって特に重要かもしれない追加のコストが生じる。もう１つの欠点は、ユーザがいくつかのコードシーケンスに慣れているかまたは記憶している必要があることで、同様に問題であると考えられる。また、一連のキーストロークを入力する必要性は、さらなる努力を要求し、誤った数字を入力しやすく、システムエラーをもたらすことがあり、または少なくとも手続を繰り返す必要がある。

【００１７】

上記周知の対応策の明らかな欠点に鑑みて、ユーザの既存のログイン認証情報を補うためにインターネットベースのアプリケーションへのアクセスを制御する方法に対する解決されていないニーズがあり、それは、大規模かつ妥当なコストで開発でき、上記説明した従来技術に改良をもたらす。

【発明の概要】

【課題を解決するための手段】

【００１８】

本発明の１つの実施形態では、第１のインターネット利用可能なデバイス（望ましくは、個人コンピュータ、ノートＰＣ、またはタブレット等の個人コンピュータデバイス）を使用して登録ユーザによって有効なログイン認証情報の提出を要求するインターネットベースのアプリケーションへのアクセスを制御する方法は、ユーザが先ず、ユーザに関連付けられた第２のインターネット利用可能なデバイス（好ましくは、スマートフォンなどの移動式デバイス）によって固有の認証コードを含むコマンドのインターネットを介する送信を開始することを含む。

【００１９】

コマンドは、第２のデバイス上でデバイスベースのアプリケーションを起動する登録ユーザによって生成されてもよい。コマンドは、固有の認証コードとデータベースに格納されたそのコードのリストとを比較することによって、第２のインターネット利用可能なデバイスの身元を判断する認証サーバによって受信される。各コードは、特定の登録ユーザに関連付けられる。

【００２０】

固有の認証コードは、第２のデバイスに不可欠な固有の識別コードを含んでもよい。

【００２１】

登録ユーザの身元を有効に判断する時、認証サーバは、受信したコマンドに基づきアクセス制御ステータスを設定する。制御ステータスに基づき、サーバは、第１のインターネット利用可能なデバイスを介して有効なログイン認証情報の提出時にアプリケーションへのアクセスを判断する。

【００２２】

登録ユーザは、インターネットベースのアプリケーションにログインしたい時、アクセスを可能にするコマンド、またはインターネットベースのアプリケーションのログアウト後、権限のないアクセスを防ぐためにインターネットベースのアプリケーションへのアクセスを否定するコマンドを送信することができる。

【００２３】

もう１つの実施形態では、インターネットベースのアプリケーションへのアクセスを制御する方法は、第１および第２のインターネット利用可能なデバイスの各地理的位置を比較し、受信したコマンドに基づきアクセス制御ステータスを設定する前、両デバイスの地理的位置が互いに近接しているかを判断する認証サーバの追加的手続を含む。

【００２４】

現世代の携帯式デバイスによって提供される進化した機能性および高レベルのインターネット接続性に鑑みて、登録ユーザはもしかしたら、分離したデバイス（通常、個人コンピュータまたはノートＰＣ）の代わりに、インターネットベースのアプリケーションにアクセスするために、同一のインターネット利用可能なデバイス（通常、スマートフォン等の携帯式デバイス）を利用するかもしれない。

【００２５】

故に、本発明の別の実施形態では、登録ユーザは、インターネットベースのアプリケーションにアクセスし、固有の認証コードを含むコマンドの送信のために同じデバイスを利用する。

【００２６】

そのような実施形態では、登録ユーザに関連付けられたインターネット利用可能なデバイスを使用して登録ユーザによって有効なログイン認証情報の提出を要求するインターネットベースのアプリケーションに対する自分のデバイス上でのアクセスを制御する方法は、ユーザが先ず、デバイスによって固有の認証コードを含むコマンドの送信を開始することを含む。

【００２７】

受信したコマンドは、デバイス上でデバイスベースのアプリケーションを登録ユーザが起動することにより生成され、各コードが特定の登録ユーザに関連付けられるので、固有の認証コードとデータベースに格納されたそのコードのリストとを比較することによって、インターネット利用可能なデバイスの身元を判断する認証サーバによって受信される。

【００２８】

固有の認証コードは、デバイスに不可欠な固有の識別コードを含んでもよい。

【００２９】

登録ユーザの身元を有効に判断する時、認証サーバは、受信したコマンドに基づきアクセス制御ステータスを設定し、制御ステータスに基づき、インターネット利用可能なデバイスを介して有効なログイン認証情報の提出時にアプリケーションへのアクセスを判断する。

【００３０】

登録ユーザは、インターネットベースのアプリケーションにログインしたい時、アクセスを可能にするためのコマンド、またはインターネットベースのアプリケーションのログアウト後、権限のないアクセスを防ぐためにインターネットベースのアプリケーションへのアクセスを否定するコマンドを送信してもよい。

【００３１】

この実施形態では、受信したコマンドは、インターネット利用可能なデバイス上でデバイスベースのアプリケーションを起動する登録ユーザによって生成され、固有の認証コードは、使用したデバイスに不可欠な固有の識別コードを含む。

【００３２】

全ての実施形態では、好ましい実施形態で説明した固有の認証コードは、登録ユーザに関連付けられたユーザ識別子からなってもよく、追加のセキュリティのためにデバイスベースのアプリケーションによって暗号化されてもよい。

【００３３】

固有の識別コードは、使用したデバイスの種類に依存してもよく、デバイスの国際移動体装置識別番号（ＩＭＥＩ）、移動体装置識別番号（ＭＥＩＤ）、または電子シリアル番号（ＥＳＮ）でもよい。代わりに、デバイスがBluetooth（登録商標）対応である場合、デバイスの固有のBluetooth（登録商標）アドレスが使用されてもよい。

【００３４】

簡単に言うと、本発明は、２要素認証手法（two-factor authentication scheme）の１つの概念として、スマートフォン等のありふれたインターネット利用可能なデバイスの新規な使用法によって、インターネットベースのアプリケーションへのアクセスを“スイッチオン”および“スイッチオフ”する方法を提供する。

【００３５】
ログイン認証情報は、登録ユーザが一意的に知っている何かとして機能し、デバイスまたは第２のデバイスは、登録ユーザが一意的に有している何かとして機能し、固有のデバイスのシリアルコードを参照する等により識別可能である。
【００３６】
別の局面では、本発明は、インターネットベースのアプリケーションの登録ユーザによってインターネットベースのアプリケーションへのアクセスを制御するためのデバイスベースのアプリケーションを含む個人のインターネット利用可能なデバイスを提供し、デバイスベースのアプリケーションは、デバイスに不可欠な固有の識別コードを読み取り、固有の識別コードを含むコマンドを生成し、コンピュータサーバへインターネットを介して送信するように適合され、コンピュータサーバへ前記コマンド信号を送信するためのデバイスベースのアプリケーションの起動は、インターネットベースのアプリケーションへのアクセスを可能にするかまたは否定するユーザの意図である。
【００３７】
さらに別の局面では、本発明は、インターネットベースのアプリケーションの登録ユーザによるインターネットベースのアプリケーションへのアクセスを制御するために個人のインターネット利用可能なデバイス上で使用するためのデバイスベースのアプリケーションを提供する。アクセスが有効な時、インターネットベースのアプリケーションは次いで、同じデバイスまたは別のインターネット利用可能なデバイスを介してアクセスされてもよい。
【００３８】
本発明のこの曲面の実施形態では、デバイスベースのアプリケーションは、それがインストールされたデバイスの位置を判断し、アクセス制御プロセスの一部として位置データを送信するように適合される。
【００３９】
本発明は故に、ユーザがアプリケーションにアクセスしたい時はいつでも、インターネットベースのアプリケーションへのアクセスを可能にするコマンドを、インターネットを介して単に送信することで、および任意の悪質なパーティによる権限のないアクセスを防ぐために、全ての他の時間でインターネットベースのアプリケーションへのアクセスを否定するコマンドを、インターネットを介して送信することで、インターネットベースのアプリケーション（インターネットバンキングウェブサイト等）へのアクセス制御をユーザに許可することによって、有効なログイン認証情報の提出を要求するインターネットベースのアプリケーション上でのフィッシング、ファーミング、キーロギング、および介入者攻撃に対処する新規な方法を提供する。
【図面の簡単な説明】
【００４０】
【図１】図１は、ユーザが先ず、第１のインターネット利用可能なデバイスによってインターネットベースのアプリケーションへのアクセスを可能にするために第２のインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第１の実施形態を示すフローチャートである。
【図２】図２は、ユーザが先ず、インターネットベースのアプリケーションへのアクセスを否定するために、第２のインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第１の実施形態を示すフローチャートである。
【図３】図３は、第１および第２のデバイスの地理的位置が互いに近接している場合、ユーザが先ず、第１のインターネット利用可能なデバイスによってインターネットベースのアプリケーションへのアクセスを可能にするために第２のインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第２の実施形態を示すフローチャートである。
【図４】図４は、第１および第２のデバイスの地理的位置が互いに近接していない場合、ユーザが先ず、第１のインターネット利用可能なデバイスによってインターネットベース

のアプリケーションへのアクセスを可能にするために第２のインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第２の実施形態を示すフローチャートである。
【図５】図５は、ユーザが先ず、インターネット利用可能なデバイスによってインターネットベースのアプリケーションへのアクセスを可能にするためにインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第３の実施形態を示すフローチャートである。
【図６】図６は、ユーザが先ず、インターネットベースのアプリケーションへのアクセスを否定するためにインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第３の実施形態を示すフローチャートである。
【発明を実施するための形態】
【００４１】
第１の実施形態では、方法は、第１のインターネット利用可能なデバイス１を介して登録ユーザによって有効なログイン認証情報の提出を要求するインターネットベースのアプリケーション３へのアクセスを制御することを含み、方法は：
ａ）　ユーザに関連付けられた第２のインターネット利用可能なデバイス２によってインターネットを介して送信される固有の認証コードを含むコマンドをコンピュータサーバ４で受信するステップであって、そのコードの送信は、ユーザによって開始される、受信するステップと；
ｂ）　データベースに格納される複数のそのコードと受信したコードとを比較することによって第２のデバイス２の身元（identity）をコンピュータサーバ４で判断するステップであって、各コードがアプリケーションの異なる登録ユーザに関連付けられた、判断するステップと；
ｃ）　ステップｂ）で身元を有効に判断する時、前記コマンドに基づきアクセス制御ステータスをコンピュータサーバ４で設定するステップと；
ｄ）　アクセス制御ステータスに基づき、第１のデバイス１を介して有効なログイン認証情報の提出時にアプリケーション３へのアクセスをコンピュータサーバ４で判断するステップと；を含む。
【００４２】
インターネットベースのアプリケーション３にアクセスする登録ユーザによって使用される第１のインターネット利用可能なデバイス１は通常、個人コンピュータ、ノートＰＣ、またはタブレットでもよい。
【００４３】
登録ユーザによってアクセスされるインターネットベースのアプリケーション３は通常、インターネットバンキングウェブサイト等のオンラインサービスプロバイダのウェブサイトでもよい。ログイン認証情報は通常、ユーザＩＤおよびパスワードからなる。
【００４４】
コマンドを送信するために登録ユーザによって使用される第２のインターネット利用可能なデバイス２は通常、登録ユーザに属するスマートフォン等の携帯式または移動式デバイスでもよい。
【００４５】
第２のインターネット利用可能なデバイス２によって送信されるコマンドは、第２のインターネット利用可能なデバイス上のデバイスベースのアプリケーションを登録ユーザが起動することによって生成される。第２のインターネット利用可能なデバイスが通常スマートフォンなので、デバイスベースのアプリケーションは、“app”として共通に知られる専門のスマートフォンアプリケーションの形式をとることができる。
【００４６】
デバイスベースのアプリケーションは、オンラインサービスプロバイダのウェブサイト３にユーザアカウントを登録するプロセスの一部としてユーザに提供され、それはまた、ユーザおよびユーザの第２のインターネット利用可能なデバイス２に関連付けられる識別

子にユーザのアカウントを関連付けることを含む。実際、オンラインサービスプロバイダは、登録ユーザ毎にユーザ識別子およびスマートフォン識別子のセキュアデータベースを維持し、それは、登録ユーザの身元を判断および認証するために使用される。

【００４７】

コンピュータサーバ４は通常、前の段落で言及したセキュアデータベースへのアクセスを有するオンラインサービスプロバイダのウェブサイトにリンクされた認証サーバでもよく、一方で、他のサーバ配置は、当業者によって想定されうる。

【００４８】

ユーザ識別子は一般に、ユーザＩＤまたはパスワード等の登録ユーザのログイン認証情報の形式をとることができる。実際、ユーザのログイン認証情報の任意の１つまたは両方は、ユーザ識別子として使用されてもよい。

【００４９】

第２のインターネット利用可能なデバイス２によって送信されるコマンドが含む認証コードは次いで、第２のデバイスに不可欠な固有の識別コードを含んでもよく、また好ましくは、同様に登録ユーザに関連付けられたユーザ識別子を含んでもよい。

【００５０】

認証コードが含む情報の重要性に鑑みて、送信されたコマンドは、追加のセキュリティのためにデバイスベースのアプリケーションによって暗号化されてもよい。利用可能な通常の暗号化手法は、ＳＨＡ－１ハッシュ関数、または次世代暗号規格（ＡＥＳ）アルゴリズムでもよい。

【００５１】

固有の識別コードは、第２のインターネット利用可能なデバイス２の種類に依存でき、例えば第２のインターネット利用可能なデバイスの国際移動体装置識別番号（ＩＭＥＩ）、移動体装置識別番号（ＭＥＩＤ）、または電子シリアル番号（ＥＳＮ）でもよい。代わりに、デバイスがBluetooth（登録商標）対応である場合、デバイスの固有のBluetooth（登録商標）アドレスが使用されてもよい。

【００５２】

ここで説明される第１の実施形態は、第１および第２のインターネット利用可能なデバイスの地理的位置をさらに比較することによって、追加の認証レベルを提供してセキュリティをさらに高めるように修正されてもよい。

【００５３】

本発明の第２の実施形態では、第１のインターネット利用可能なデバイス１を介して登録ユーザによって有効なログイン認証情報の提出を要求するインターネットベースのアプリケーション３へのアクセスを制御する方法はまた、ステップｃ）の前に：

－　第１のおよび第２のインターネット利用可能なデバイスの各地理的位置をコンピュータサーバ４で比較するステップと；

－　第１および第２のインターネット利用可能なデバイスの地理的位置が互いに近接しているかをコンピュータサーバ４で判断するステップと；

の追加のステップを含んでもよい。

【００５４】

第２の実施形態では、受信したコマンドに基づきアクセス制御ステータスをコンピュータサーバ４で設定するステップ（即ち、ステップｃ））はまた、所定の閾値内で、第１および第２のインターネット利用可能なデバイスの地理的位置が互いに近接していることの判断に依存してもよい。ここで使用されるように、用語“近接”は、２つの位置が同じであることを含んでもよい。

【００５５】

通常、個人コンピュータ、ノートＰＣ、またはタブレットである第１のインターネット利用可能なデバイス１の地理的位置は、町および国レベルの地理的位置情報が導き出されるデバイスのＩＰアドレスの分析を介して認証サーバによって判断されてもよい。

【００５６】

第２のインターネット利用可能なデバイス２の地理的位置は、デバイスベースのアプリケーションによって抽出されて第２のデバイスによって送信される衛星信号（例えば、ＧＰＳ座標）、移動体通信基地局情報、およびWi-Fiアクセスポイント情報のようなデータの形式で認証サーバによって受信される。受信したデータ情報は、町および国レベルの情報の形式で第２のデバイスの地理的位置を認証サーバに提供する。

【００５７】

第２のインターネット利用可能なデバイス２は、追加のチェックとして使用される最新情報を認証サーバに提供するために、デバイスベースのアプリケーションが起動されている限り、デバイスの地理的位置情報を繰り返し送信する。１つの実施形態では、アクセスを可能にするためにデバイスベースのアプリケーションを起動する時、主要なアクセスコマンドは、一度に送信され、その後地理的位置データの送信が繰り返される。地理的位置データを組込む信号のフォーマットは、特に第２のデバイスの固有の識別コードおよび／またはユーザのユーザ識別子を含むことによって、アクセスコマンド信号のフォーマットに類似してもよい。

【００５８】

当業者であれば、本発明の範囲および対象内にある地理的位置情報を分析、抽出、および比較するための他の適切な技法に多分想到できるだろう。

【００５９】

第２のインターネット利用可能なデバイスによって送信される地理的位置情報は、追加のセキュリティのために暗号化されてもよい。利用可能な通常の暗号化手法は、ＳＨＡ－１ハッシュ関数、または次世代暗号規格（ＡＥＳ）アルゴリズムでもよい。

【００６０】

図１は特に、登録ユーザが先ず、第１のインターネット利用可能なデバイスによってインターネットベースのアプリケーションへのアクセスを可能にするために、第２のインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第１の実施形態を示す。

【００６１】

オンラインサービスプロバイダのウェブサイト３（インターネットバンキングアカウント等）の登録ユーザが第１のインターネット利用可能なデバイス１（自分の個人コンピュータ等）を介して自分のオンラインアカウントにアクセスしたい時、登録ユーザは先ず、自分のオンラインアカウントへのアクセスを可能にするために、第２のインターネット利用可能なデバイス２（自分のスマートフォン等）からインターネットを介してコマンドを送信することができる。

【００６２】

アクセスを可能にするためのコマンドは、コマンドが含む固有の認証コードとデータベースに格納されたそのコードのリストとを比較することによって、第２のインターネット利用可能なデバイス２の身元を判断する認証サーバ４によって受信される。第２のインターネット利用可能なデバイス２が実際に登録ユーザに属することを判断する時、認証サーバ４は、ユーザが自分のオンラインアカウントにアクセス可能になる前、登録ユーザによって提出されたログイン認証情報が有効であることを検証することによって登録ユーザの身元を判断することができる。

【００６３】

登録ユーザは即ち、ユーザのオンラインアカウントへのアクセスが許可される前に認証される自分の有効なログイン認証情報を、第１のインターネット利用可能なデバイス１を介して提出することに追加して、第２のインターネット利用可能なデバイス２を使用して自分のオンラインアカウントへのアクセスを“スイッチオン”する。

【００６４】

図２は特に、登録ユーザが先ず、インターネットベースのアプリケーションへのアクセスを否定するために第２のインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第１の実施形態を示す。

【００６５】
オンラインサービスプロバイダのウェブサイト３（インターネットバンキングアカウント等）の登録ユーザが自分のアカウントへのアクセスを否定したい時、登録ユーザは先ず、自分のオンラインアカウントへのアクセスを否定するために第２のインターネット利用可能なデバイス２（自分のスマートフォン等）からコマンドを送信することができる。
【００６６】
アクセスを否定するためのコマンドは、コマンドが含む固有の認証コードとデータベースに格納されたそのコードのリストとを比較することによって、第２のインターネット利用可能なデバイス２の身元を判断する認証サーバによって受信される。第２のインターネット利用可能なデバイス２が実際に登録ユーザに属することを判断する時、認証サーバ４は、登録ユーザのオンラインアカウントへのアクセスを否定することができる。この後、有効なログイン認証情報をも提出するための登録ユーザまたは任意の他のパーティによる任意の試みは、許可されている登録ユーザのオンラインアカウントへのアクセスをもたらさないことができる。
【００６７】
登録ユーザは即ち、第２のインターネット利用可能なデバイス２を使用して自分のアカウントへのアクセスを“スイッチオフ”する。一度アクセスが否定されると、第１のインターネット利用可能なデバイス１を介する任意のログイン認証情報の提出は、有効であるか、さもなければ拒絶されうる。
【００６８】
図３は特に、第１および第２のデバイスの地理的位置が互いに近接している場合、第１のインターネット利用可能なデバイスによってインターネットベースのアプリケーションへのアクセスを可能にするために、登録ユーザが先ず、第２のインターネット利用可能なデバイスによってコマンド送信を開始する時の、本発明の第２の実施形態を示す。
【００６９】
オンラインサービスプロバイダのウェブサイト３（インターネットバンキングアカウント等）の登録ユーザが第１のインターネット利用可能なデバイス１（自分の個人コンピュータ等）を介して自分のオンラインアカウントにアクセスしたい時、登録ユーザは先ず、自分のオンラインアカウントへのアクセスを可能にするために、第２のインターネット利用可能なデバイス２（自分のスマートフォン等）からコマンドを送信することができる。

【００７０】
アクセスを可能にするためのコマンドは、コマンドが含む固有の認証コードとデータベースに格納されたそのコードのリストとを比較することによって、第２のインターネット利用可能なデバイス２の身元を判断する認証サーバ４によって受信される。
【００７１】
認証サーバ４はまた、第１および第２のインターネット利用可能なデバイスの地理的位置を判断し、２つのデバイスが互いに近接しているかを比較することができる。
【００７２】
これは認証サーバ４が、第１のインターネット利用可能なデバイスのＩＰアドレスを分析し、ＩＰアドレスから町および国レベルの地理的位置情報を導出し、町および国レベルの地理的位置情報の形式で第２のインターネット利用可能なデバイスによって送信されたＧＰＳ座標、移動体通信基地局情報、およびWi-Fiアクセスポイント情報等のデータを受信することによって行われる。
【００７３】
第２のインターネット利用可能なデバイス２が実際に登録ユーザに属することを判断し、第１および第２のインターネット利用可能なデバイスの両方が互いに近接していることを判断する時、即ち２つのデバイスに関して町および国の情報が集計されているこの特定の実施形態において、認証サーバ４は、ユーザが自分のオンラインアカウントにアクセス可能になる前、登録ユーザによって提出されたログイン認証情報が有効であることを検証

することによって登録ユーザの身元を判断することができる。
【００７４】
図４は特に、第１および第２のデバイスの地理的位置が互いに近接していない場合、第１のインターネット利用可能なデバイスによってインターネットベースのアプリケーションへのアクセスを可能にするために、登録ユーザが先ず、第２のインターネット利用可能なデバイスによってコマンドの送信を開始する時の、本発明の第２の実施形態を示す。
【００７５】
オンラインサービスプロバイダのウェブサイト３（インターネットバンキングアカウント等）の登録ユーザが第１のインターネット利用可能なデバイス１（自分の個人コンピュータ等）を介して自分のオンラインアカウントにアクセスしたい時、登録ユーザは先ず、自分のオンラインアカウントへのアクセスを可能にするために、第２のインターネット利用可能なデバイス２（自分のスマートフォン等）からコマンドを送信することができる。
【００７６】
アクセスを許可するためのコマンドは、コマンドが含む固有の認証コードとデータベースに格納されたそのコードのリストとを比較することによって、第２のインターネット利用可能なデバイス２の身元を判断する認証サーバ４によって受信される。
【００７７】
認証サーバ４はまた、第１および第２のインターネット利用可能なデバイスの地理的位置を判断し、２つのデバイスが互いに近接しているかを比較することができる。
【００７８】
第２のインターネット利用可能なデバイス２が実際に登録ユーザに属することを判断し、第１および第２のインターネット利用可能なデバイスの両方が互いに近接していないことを判断する時、即ち２つのデバイスに関する町および国情報が集計されていないこの特定の実施形態において、認証サーバ４は、登録ユーザによって提出されたログイン認証情報が有効であるかに関係なく、ユーザのオンラインアカウントへのアクセスを否定することができる。
【００７９】
図３および図４に示す本発明の第２の実施形態では、登録ユーザは、オンラインアカウントへのアクセスが許可される前に認証された自分の有効なログイン認証情報を第１のインターネット利用可能なデバイスを介して提出することに追加して、自分のオンラインアカウントへのアクセスを“スイッチオン”するために、第１のインターネット利用可能なデバイスに近接していなければならない第２のインターネット利用可能なデバイスを使用する。
【００８０】
本発明の利用はしかしながら、インターネットベースのアプリケーションへのアクセスを制御する方法において、第１および第２のインターネット利用可能なデバイスの両方を登録ユーザが利用することに限定されない。
【００８１】
スマートフォン等の現世代の携帯式インターネット利用可能なデバイスの高機能性およびそのデバイスの高レベルのインターネット接続性を考えると、登録ユーザがインターネットベースのアプリケーションにアクセスするために単一のデバイスを所有し、および／または利用することを好むだけである可能性が大いにありえる。
【００８２】
この可能性は、本発明の第３の実施形態で考慮される。
【００８３】
本発明の第３の実施形態では、方法は、インターネット利用可能なデバイス５を介して登録ユーザによって有効なログイン認証情報の提出を要求するインターネット利用可能なアプリケーション３へのアクセスを制御することを含み、方法は：
ａ）　インターネット利用可能なデバイス５によってインターネットを介して送信される固有の認証コードを含むコマンドをコンピュータサーバ４で受信するステップであって、

そのコードの送信は、ユーザによって開始される、受信するステップと、
ｂ）　受信したコードとデータベースに格納された複数のそのコードとを比較することによって、デバイスの身元をコンピュータサーバ４で判断するステップであって、各コードは、アプリケーションの異なる登録ユーザに関連付けられる、判断するステップと；
ｃ）　ステップｂ）で身元を有効に判断する時、前記コマンドに基づきアクセス制御ステータスをコンピュータサーバ４で設定するステップと；
ｄ）　デバイスを介して有効なログイン認証情報の提出時にアプリケーション３へのアクセスを、アクセス制御ステータスに基づきコンピュータサーバ４で判断するステップと；
を含む。

【００８４】

登録ユーザによってアクセスされるインターネットベースのアプリケーション３は通常、インターネットバンキングウェブサイト等のオンラインサービスプロバイダでもよい。

【００８５】

コマンドを送信するために登録ユーザによって利用されるインターネット利用可能なデバイス５は通常、登録ユーザに属するスマートフォンまたはタブレット等の個人携帯式デバイスでもよい。

【００８６】

インターネット利用可能なデバイス５によって送信されるコマンドは、デバイス上でデバイスベースのアプリケーションを起動する登録ユーザによって生成される。インターネット利用可能なデバイス５は通常、スマートフォンなので、デバイスベースのアプリケーションは、“app”として共通に知られる専門のスマートフォンアプリケーションの形式をとることができる。

【００８７】

デバイスベースのアプリケーションは、オンラインサービスプロバイダのウェブサイトにユーザアカウントを登録するプロセスの一部としてユーザに提供され、それはまた、ユーザおよびユーザのインターネット利用可能なデバイスに関連付けられた識別子とユーザのアカウントとを関連付けることを含むことができる。実際、オンラインサービスプロバイダは、登録ユーザ毎にユーザ識別子およびスマートフォン識別子のセキュアデータベースを維持でき、それは、登録ユーザの身元を判断および認証するために使用できる。

【００８８】

コンピュータサーバは通常、前の段落で言及したセキュアデータベースへのアクセスを有するオンラインサービスプロバイダのウェブサイトにリンクされた認証サーバ４でもよく、一方で、他のサーバ配置は、当業者によって想定されうる。

【００８９】

ユーザ識別子は一般に、ユーザＩＤおよびパスワード等の登録ユーザのログイン認証情報の形式をとることができる。

【００９０】

インターネット利用可能なデバイス５によって送信されたコマンドが含む認証コードは次いで、デバイスに不可欠な固有の識別コードを含んでもよく、好ましくは登録ユーザに関連付けられたユーザ識別子も同様に含む。

【００９１】

本発明の第１の実施形態のように、認証コードはまた、追加されたセキュリティのためにデバイスベースのアプリケーションによって暗号化されてもよい。

【００９２】

固有の識別コードは、インターネット利用可能なデバイスの種類に依存でき、例えば第２のインターネット利用可能なデバイスの国際移動体装置識別番号（ＩＭＥＩ）、移動体装置識別番号（ＭＥＩＤ）、または電子シリアル番号（ＥＳＮ）でもよい。代わりに、デバイスがBluetooth（登録商標）対応である場合、デバイスの固有のBluetooth（登録商標）アドレスが使用されてもよい。

【００９３】

図５は特に、同じデバイスによってインターネットベースのアプリケーションへのアクセスを可能にするために、登録ユーザが先ず、インターネット利用可能なデバイス（自分のスマートフォン等）によってインターネットを介してコマンドの送信を開始する時の、本発明の第３の実施形態を示す。

【００９４】

オンラインサービスプロバイダのウェブサイト３の登録ユーザがインターネット利用可能なデバイス５を介して自分のオンラインアカウントにアクセスしたい時、登録ユーザは先ず、自分のオンラインアカウントへのアクセスを可能にするために、インターネット利用可能なデバイスからコマンドを送信することができる。

【００９５】

アクセスを可能にするためのコマンドは、コマンドが有する固有の認証コードとデータベースに格納されたそのコードのリストとを比較することによって、インターネット利用可能なデバイス５の身元を判断する認証サーバ４によって受信される。インターネット利用可能なデバイス５が登録ユーザに実際に属することを判断する時、認証サーバ４は、ユーザが自分のオンラインアカウントにアクセス可能になる前に、登録ユーザによって提出されたログイン認証情報が有効であることを確認することによって、登録ユーザの身元を判断することができる。

【００９６】

登録ユーザは即ち、ユーザのオンラインアカウントへのアクセスが許可される前に認証された自分の有効なログイン認証情報を、デバイスを介して提出することに追加して、自分のオンラインアカウントへのアクセスを“スイッチオン”するためにインターネット利用可能なデバイス５を使用する。

【００９７】

図６は特に、インターネットベースのアプリケーションへのアクセスを否定するために、登録ユーザが先ず、インターネット利用可能なデバイス（自分のスマートフォン等）によってコマンドの送信を開始する時の、本発明の第３の実施形態を示す。

【００９８】

オンラインサービスプロバイダのウェブサイト３の登録ユーザが自分のアカウントへのアクセスを否定したい時、登録ユーザは先ず、自分のオンラインアカウントへのアクセスを否定するために、インターネット利用可能なデバイス５からコマンドを送信することができる。

【００９９】

アクセスを否定するためのコマンドは、コマンドが含む固有の認証コードとデータベースに格納されたそのコードのリストとを比較することによって、インターネット利用可能なデバイス５の身元を判断する認証サーバ４によって受信される。インターネット利用可能なデバイス５が実際に登録ユーザに属することを判断する時、認証サーバ４は、登録ユーザのオンラインアカウントへのアクセスを否定することができる。この後、有効なログイン認証情報をも提出するための登録ユーザまたは任意の他のパーティによる任意の試みは、許可される登録ユーザのオンラインアカウントへのアクセスをもたらさないことができる。

【０１００】

登録ユーザは即ち、自分のアカウントへのアクセスを“スイッチオフ”するためにインターネット利用可能なデバイスを使用する。一度アクセスが否定されると、インターネット利用可能なデバイス５を介する任意のログイン認証情報の提出は、有効であるか、さもなければ拒絶されうる。

【０１０１】

ここで説明した本発明の実施形態では、実際にユーザアカウントを登録するプロセスは通常、オンライン手続きでもよく、それによりユーザは先ず、個人コンピュータ、ノートＰＣ、またはタブレット（即ち、第１のインターネット利用可能なデバイス）を介してオンラインサービスプロバイダのウェブサイト（即ち、インターネットベースのアプリケー

ション）にアクセスして、新たなユーザアカウントを作成する。ウェブサイトは次いで、ウェブサイトに登録されたスマートフォン（即ち、第２のインターネット利用可能なデバイス）をユーザが有するかをチェックすることができる。

【０１０２】

オンラインサービスプロバイダのウェブサイトに登録されたスマートフォンをユーザが有していない場合、ユーザは、スマートフォンプラットフォームによって提供されるオフィシャルアプリケーションレポジトリから“app”（即ち、デバイスベースのアプリケーション）をダウンロードするように催促および案内される。

【０１０３】

ユーザがスマートフォンに“app”をインストールした後、オンラインサービスプロバイダのウェブサイトは、ユーザのユーザＩＤ、認証サーバのインターネットアドレス、およびユーザの固有の登録コードを含むテキストメッセージをユーザのスマートフォンに送信して、オンラインサービスプロバイダのウェブサイトに自分のスマートフォンを登録する。テキストメッセージに含まれる情報は、改ざんを防ぐために暗号化される。

【０１０４】

“app”は次いで、テキストメッセージのコンテンツを使用してユーザのスマートフォンの登録を実行することができ、故にユーザアカウントを登録するプロセスを完了する。

【０１０５】

ここで説明された本発明の実施形態では、固有の認証コードは、登録ユーザのユーザＩＤおよびスマートフォンのシリアル番号（例えば、ＩＭＥＩ）、万国標準時（ＵＴＣ）フォーマットのタイムスタンプ、および暗号化手法で使用されるＳＨＡ－１ハッシュ関数に属する制御シグネチャを含む。ユーザＩＤおよびスマートフォンのＩＭＥＩナンバーは、固有の識別コードとして使用される。タイムスタンプは、第２の実施形態に適用可能な連続的に送信された地理的位置情報が最新であるかをチェックするための追加情報を提供する。制御シグネチャは、固有の認証コードに含まれた暗号化情報が改ざんまたは漏えいされていないことを保証する。

【０１０６】

ここで説明した本発明の実施形態では、第１および第２の実施形態における第２のインターネット利用可能なデバイス、または第３の実施形態における単一のインターネット利用可能なデバイスによって送信されたアクセスを可能にするためのコマンドの有効性は、登録ユーザによって所定期間起動されなかった後、失効またはタイムアウトになる。インターネットベースのアプリケーションへのアクセスの許可はまた、アクセスを可能にするためのコマンドが有効なままであることに依存し、認証サーバは故に、登録ユーザによって提出されたログイン認証情報が有効であるとして受け取られ、扱われるべきかを判断する時、アクセスを可能にするためのコマンドが失効したかを判断するように要求される。

【０１０７】

本発明は、ここで説明された実施形態に限定されず、その説明は、本発明の例示目的であり、可能な改良または修正は、本発明の範囲から逸脱しないで直ちに明らかとなる。一例として、説明された実施形態は、ユーザがインターネットベースのアプリケーションにアクセスしたい時はいつでも、選択的にアクセスをスイッチオンすることに関するが、ステータスが通常、デフォルトによってオンに設定されることも本発明の範囲内である。ユーザは次いで、自分のセキュリティに対する潜在的または実質的な違反が検出された場合、アクセスをスイッチオフするためにデバイスベースのアプリケーションを起動することによってアプリケーションへのアクセスを単純に妨げる。別の例として、地理的位置データの使用に関する実施形態において、位置の比較は、アクセスを可能にするための必要条件として定期的に行われるというよりも、単に特定の状況で行われてもよい。例えば、サービスプロバイダまたはコンピュータサーバは、ＩＰアドレスまたはユーザが通常インターネットベースのアプリケーションにアクセスするアドレスを格納してもよい。次いで、地理的位置のチェックは、予め使用および格納されていないＩＰアドレスからユーザがアプリケーションにアクセスを試みる場合、それは、疑わしい権限のないアクセスが試みら

れていることを示す可能性があるので、呼出される。

【符号の説明】

【０１０８】

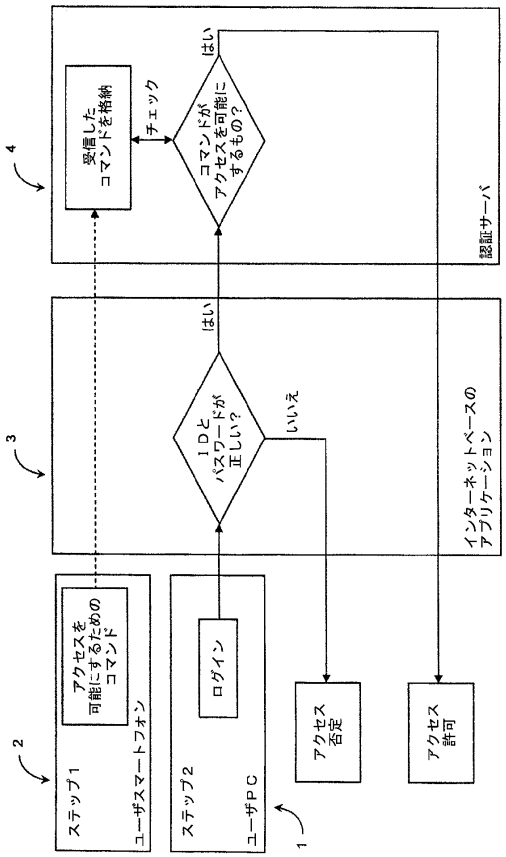
１　ユーザＰＣ

２　ユーザスマートフォン

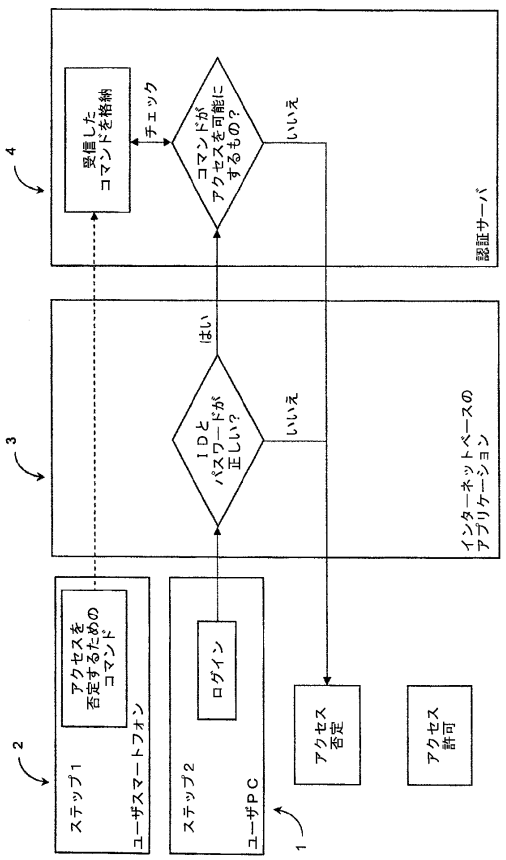
３　インターネットベースのアプリケーション

４　認証サーバ

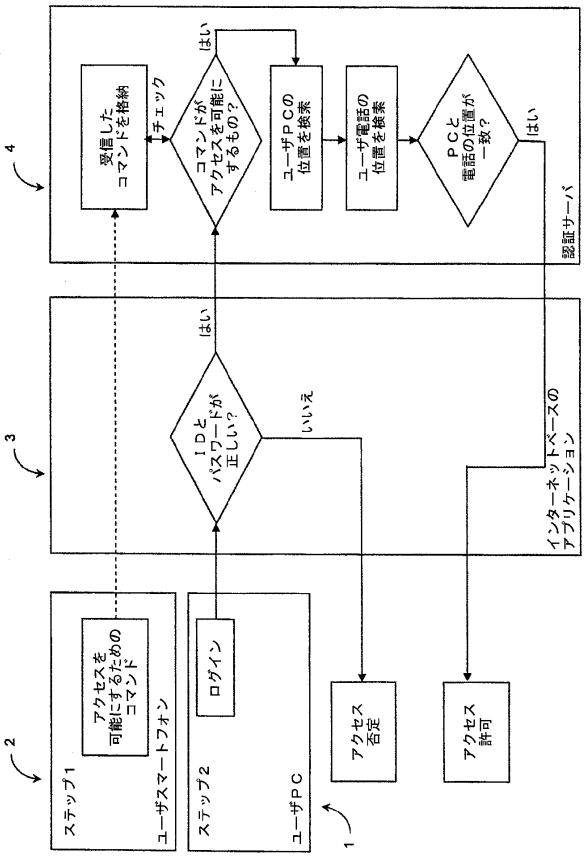
【図１】



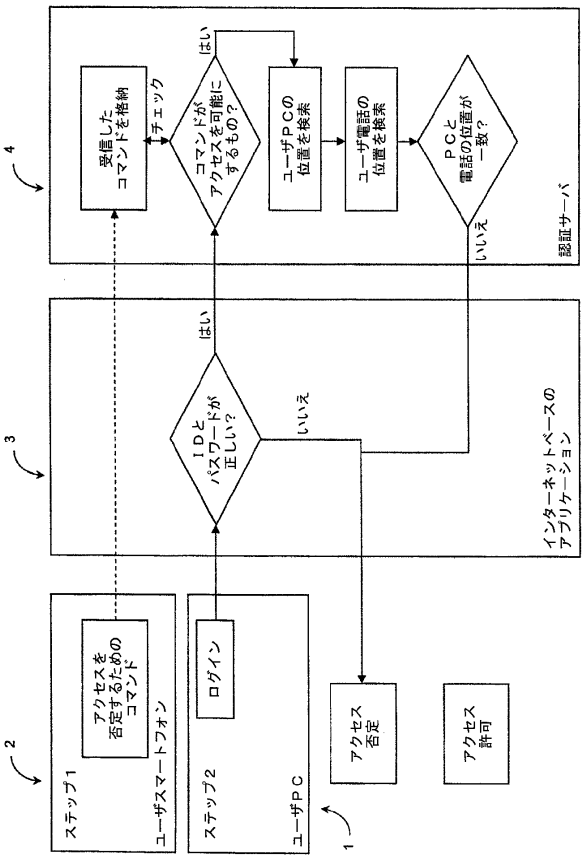
【図２】



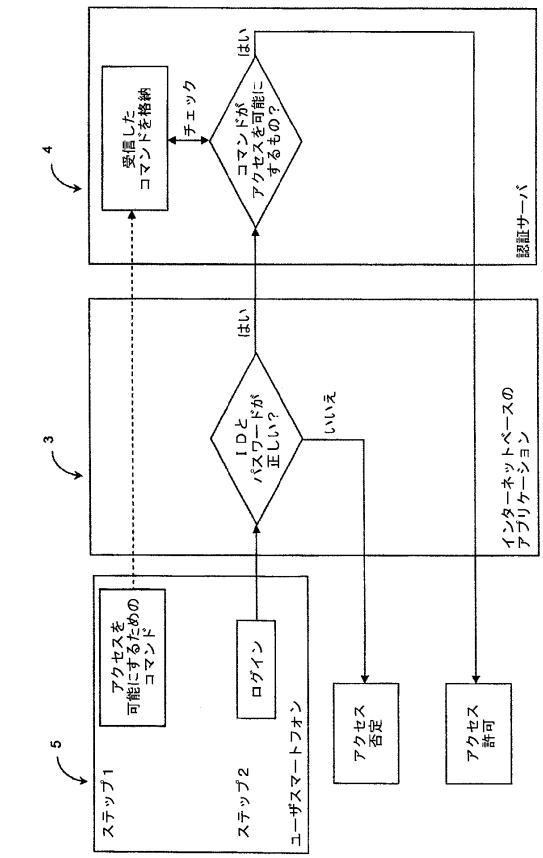
【図３】


1
2
ステップ1
アクセスを可能にするためのコマンド
ユーザスマートフォン
ステップ2
ログイン
ユーザＰＣ
3
インターネットベースのアプリケーション
IDとパスワードが正しい？
はい
いいえ
4
認証サーバ
受信したコマンドを格納
チェック
コマンドがアクセスを可能にするもの？
はい
ユーザＰＣの位置を検索
ユーザ電話の位置を検索
ＰＣと電話の位置が一致？
はい
アクセス否定
アクセス許可

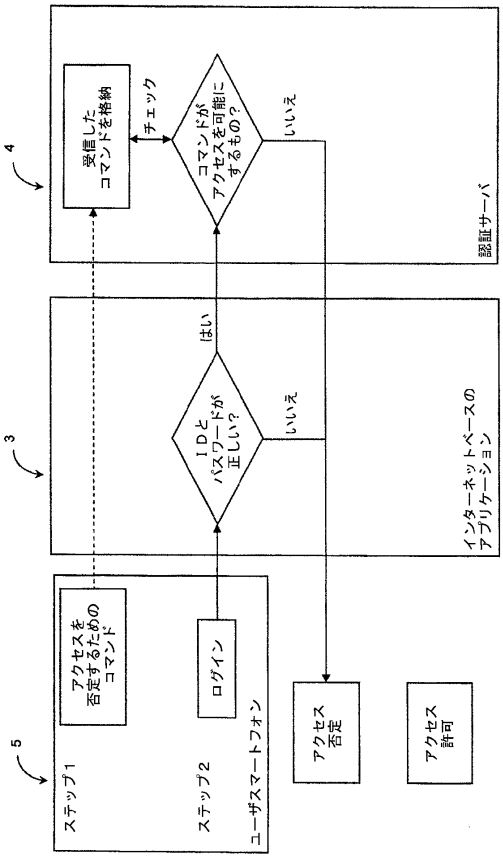
【図４】


1
2
ステップ1
アクセスを否定するためのコマンド
ユーザスマートフォン
ステップ2
ログイン
ユーザＰＣ
3
インターネットベースのアプリケーション
IDとパスワードが正しい？
はい
いいえ
4
認証サーバ
受信したコマンドを格納
チェック
コマンドがアクセスを可能にするもの？
はい
ユーザＰＣの位置を検索
ユーザ電話の位置を検索
ＰＣと電話の位置が一致？
いいえ
アクセス否定
アクセス許可

【図５】


5
ステップ1
アクセスを可能にするためのコマンド
ステップ2
ログイン
ユーザスマートフォン
3
インターネットベースのアプリケーション
IDとパスワードが正しい？
はい
いいえ
4
認証サーバ
受信したコマンドを格納
チェック
コマンドがアクセスを可能にするもの？
はい
アクセス否定
アクセス許可

【図６】


5
ステップ1
アクセスを否定するためのコマンド
ステップ2
ログイン
ユーザスマートフォン
3
インターネットベースのアプリケーション
IDとパスワードが正しい？
はい
いいえ
4
認証サーバ
受信したコマンドを格納
チェック
コマンドがアクセスを可能にするもの？
いいえ
アクセス否定
アクセス許可

フロントページの続き

(72)発明者　チク・ウェン・レオン
マレーシア・５０４５０・クアラルンプール・ジャラン・ピナン・１９・ユーオーエー・センター・レベル・２６・ビジネス・スイート・１９Ａ－２６－３・イーロック・コーポレーション・エスディーエヌ・ビーエイチディー内
(72)発明者　チー・フー・ラウ
マレーシア・５０４５０・クアラルンプール・ジャラン・ピナン・１９・ユーオーエー・センター・レベル・２６・ビジネス・スイート・１９Ａ－２６－３・イーロック・コーポレーション・エスディーエヌ・ビーエイチディー内
(72)発明者　ユエン・レン・コン
マレーシア・５０４５０・クアラルンプール・ジャラン・ピナン・１９・ユーオーエー・センター・レベル・２６・ビジネス・スイート・１９Ａ－２６－３・イーロック・コーポレーション・エスディーエヌ・ビーエイチディー内
(72)発明者　タウ・ウェイ・ファン
マレーシア・５０４５０・クアラルンプール・ジャラン・ピナン・１９・ユーオーエー・センター・レベル・２６・ビジネス・スイート・１９Ａ－２６－３・イーロック・コーポレーション・エスディーエヌ・ビーエイチディー内
(72)発明者　フン・シン・チョン
マレーシア・５０４５０・クアラルンプール・ジャラン・ピナン・１９・ユーオーエー・センター・レベル・２６・ビジネス・スイート・１９Ａ－２６－３・イーロック・コーポレーション・エスディーエヌ・ビーエイチディー内

審査官　坂東　博司

(56)参考文献　米国特許出願公開第２０１０／０２９９７３１（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００
Ｇ０６Ｆ　２１／１０
Ｇ０６Ｆ　２１／３０