(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5660652号
(P5660652)
(45)発行日　平成27年1月28日(2015.1.28)　(24)登録日　平成26年12月12日(2014.12.12)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/20 131E
G09C 1/00 (2006.01)　　G09C 1/00 640E

請求項の数 28　(全 16 頁)

(21)出願番号　特願2014-519178 (P2014-519178)
(86)(22)出願日　平成24年6月29日 (2012.6.29)
(65)公表番号　特表2014-521152 (P2014-521152A)
(43)公表日　平成26年8月25日 (2014.8.25)
(86)国際出願番号　PCT/US2012/045057
(87)国際公開番号　WO2013/003782
(87)国際公開日　平成25年1月3日 (2013.1.3)
審査請求日　平成26年1月21日 (2014.1.21)
(31)優先権主張番号　13/174,558
(32)優先日　平成23年6月30日 (2011.6.30)
(33)優先権主張国　米国(US)

早期審査対象出願

(73)特許権者　507364838
クアルコム，インコーポレイテッド
アメリカ合衆国　カリフォルニア　９２１２１　サン　ディエゴ　モアハウス　ドライブ　５７７５
(74)代理人　100108453
弁理士　村山　靖彦
(74)代理人　100163522
弁理士　黒田　晋平
(72)発明者　チン・リ
アメリカ合衆国・カリフォルニア・９２１２１・サン・ディエゴ・モアハウス・ドライヴ・５７７５

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】アンチショルダーサーフィンの認証方法

(57)【特許請求の範囲】
【請求項１】
ストレージデバイスと、
ユーザが訪れるサーバサイトに関連付けられたユーザ名および第1のパスワードを受け取るユーザインターフェースと、
乱数を発生する乱数発生器と、
前記第1のパスワードおよび前記乱数に基づく関数を実行することによって第2のパスワードを生成し、
前記乱数、前記ユーザ名、および前記関連付けられたサーバサイトの前記ストレージデバイスへの記憶を命令する
プロセッサであって、
前記第1のパスワードおよび前記第2のパスワードが、クライアントデバイスに記憶されず、前記ユーザが自分のユーザ名および前記第2のパスワードを入力することによって前記サーバサイトにログオンしようと試みる場合、前記プロセッサが、前記ユーザ名および前記サーバサイトに関連付けられた前記乱数を前記ストレージデバイスから抽出し、前記第2のパスワードおよび前記乱数に基づく逆の前記関数を実行して前記第1のパスワードを生成し、前記第1のパスワードが前記ユーザによって入力された前記第2のパスワードと入れ替わり前記サーバサイトに送出されるようにさらに構成された、
プロセッサと
を備える、クライアントデバイス。

【請求項２】
前記関数が1対1マッピング関数である、請求項1に記載のクライアントデバイス。
【請求項３】
前記関数がブロック暗号アルゴリズムである、請求項1に記載のクライアントデバイス。
【請求項４】
前記ブロック暗号アルゴリズムが、高度暗号化標準(AES)の対称鍵暗号化演算であり、前記第2のパスワードが、鍵としての前記乱数および前記第1のパスワードを使用する前記対称鍵暗号化演算から出力される、請求項3に記載のクライアントデバイス。
【請求項５】
前記鍵としての前記乱数および前記第2のパスワードを用いて対称鍵解読演算を使用すると、前記出力として前記第1のパスワードがもたらされる、請求項4に記載のクライアントデバイス。
【請求項６】
前記ユーザが通常モードまたは保護モードのうちの1つを選択し、前記通常モードでは、前記ユーザが訪れる前記サーバサイトに関連付けられた前記第1のパスワードが前記ユーザによって入力されるのに対して、前記保護モードでは、前記ユーザが訪れる前記サーバサイトに関連付けられた前記第2のパスワードが前記ユーザによって入力される、請求項1に記載のクライアントデバイス。
【請求項７】
前記ユーザが訪れる前記サーバサイトが、インターネット上のウェブサイトである、請求項1に記載のクライアントデバイス。
【請求項８】
クライアントデバイス用の第2のパスワードを作成する方法であって、
ユーザが訪れるサーバサイトに関連付けられたユーザ名および第1のパスワードを受け取るステップと、
前記クライアントデバイスの乱数器を用いて、乱数を発生するステップと、
前記クライアントデバイスのプロセッサを用いて、前記第1のパスワードおよび前記乱数に基づく関数を実行することによって第2のパスワードを生成するステップと、
前記乱数、前記ユーザ名、および前記関連付けられたサーバサイトの記憶を命令するステップと
を含み、
前記第1のパスワードおよび前記第2のパスワードが、前記クライアントデバイスに記憶されず、前記ユーザが自分のユーザ名および前記第2のパスワードを入力することによって前記サーバサイトにログオンしようと試みる場合、前記ユーザ名および前記サーバサイトに関連付けられた前記乱数がストレージから抽出され、逆の前記関数が前記第2のパスワードおよび前記乱数に基づいて実行されて前記第1のパスワードを生成し、前記第1のパスワードが前記ユーザによって入力された前記第2のパスワードと入れ替わり前記サーバサイトに送出される、
方法。
【請求項９】
前記関数が1対1マッピング関数である、請求項8に記載の方法。
【請求項１０】
前記関数がブロック暗号アルゴリズムである、請求項8に記載の方法。
【請求項１１】
前記ブロック暗号アルゴリズムが、高度暗号化標準(AES)の対称鍵暗号化演算であり、前記第2のパスワードが、鍵としての前記乱数および前記第1のパスワードを使用する前記対称鍵暗号化演算から出力される、請求項10に記載の方法。
【請求項１２】
前記鍵としての前記乱数および前記第2のパスワードを用いて対称鍵解読演算を使用す

ると、前記出力として前記第1のパスワードがもたらされる、請求項11に記載の方法。
【請求項１３】
前記ユーザが通常モードまたは保護モードのうちの1つを選択し、前記通常モードでは、前記ユーザが訪れる前記サーバサイトに関連付けられた前記第1のパスワードが前記ユーザによって入力されるのに対して、前記保護モードでは、前記ユーザが訪れる前記サーバサイトに関連付けられた前記第2のパスワードが前記ユーザによって入力される、請求項8に記載の方法。
【請求項１４】
前記ユーザが訪れる前記サーバサイトが、インターネット上のウェブサイトである、請求項8に記載の方法。
【請求項１５】
ユーザが訪れるサーバサイトに関連付けられたユーザ名および第1のパスワードを受け取るための手段と、
乱数を発生するための手段と、
前記第1のパスワードおよび前記乱数に基づく関数を実行することによって第2のパスワードを生成するための手段と、
前記乱数、前記ユーザ名、および前記関連付けられたサーバサイトの記憶を命令するための手段と
を備える、クライアントデバイスであって、
前記第1のパスワードおよび前記第2のパスワードが、前記クライアントデバイスに記憶されず、前記ユーザが自分のユーザ名および前記第2のパスワードを入力することによって前記サーバサイトにログオンしようと試みる場合、前記ユーザ名および前記サーバサイトに関連付けられた前記乱数がストレージから抽出され、逆の前記関数が前記第2のパスワードおよび前記乱数に基づいて実行されて前記第1のパスワードを生成し、前記第1のパスワードが前記ユーザによって入力された前記第2のパスワードと入れ替わり前記サーバサイトに送出される、
クライアントデバイス。
【請求項１６】
前記関数が1対1マッピング関数である、請求項15に記載のクライアントデバイス。
【請求項１７】
前記関数がブロック暗号アルゴリズムである、請求項15に記載のクライアントデバイス。
【請求項１８】
前記ブロック暗号アルゴリズムが、高度暗号化標準(AES)の対称鍵暗号化演算であり、前記第2のパスワードが、鍵としての前記乱数および前記第1のパスワードを使用する前記対称鍵暗号化演算から出力される、請求項17に記載のクライアントデバイス。
【請求項１９】
前記鍵としての前記乱数および前記第2のパスワードを用いて対称鍵解読演算を使用すると、前記出力として前記第1のパスワードがもたらされる、請求項18に記載のクライアントデバイス。
【請求項２０】
前記ユーザが通常モードまたは保護モードのうちの1つを選択し、前記通常モードでは、前記ユーザが訪れる前記サーバサイトに関連付けられた前記第1のパスワードが前記ユーザによって入力されるのに対して、前記保護モードでは、前記ユーザが訪れる前記サーバサイトに関連付けられた前記第2のパスワードが前記ユーザによって入力される、請求項15に記載のクライアントデバイス。
【請求項２１】
前記ユーザが訪れる前記サーバサイトが、インターネット上のウェブサイトである、請求項15に記載のクライアントデバイス。
【請求項２２】

クライアントデバイス用の第2のパスワードを作成する、コンピュータにより実行可能なコードを備えたコンピュータプログラムであって、
ユーザが訪れるサーバサイトに関連付けられたユーザ名および第1のパスワードを受け取ることと、
乱数を発生することと、
前記第1のパスワードおよび前記乱数に基づく関数を実行することによって第2のパスワードを生成することと、
前記乱数、前記ユーザ名、および前記関連付けられたサーバサイトの記憶を命令することと
を行うためのコードを含み、
前記第1のパスワードおよび前記第2のパスワードが、前記クライアントデバイスに記憶されず、前記ユーザが自分のユーザ名および前記第2のパスワードを入力することによって前記サーバサイトにログオンしようと試みる場合、前記ユーザ名および前記サーバサイトに関連付けられた前記乱数がストレージから抽出され、逆の前記関数が前記第2のパスワードおよび前記乱数に基づいて実行されて前記第1のパスワードを生成し、前記第1のパスワードが前記ユーザによって入力された前記第2のパスワードと入れ替わり前記サーバサイトに送出される、
コードを含むコンピュータプログラム。
【請求項２３】
前記関数が1対1マッピング関数である、請求項22に記載のコンピュータプログラム。
【請求項２４】
前記関数がブロック暗号アルゴリズムである、請求項22に記載のコンピュータプログラム。
【請求項２５】
前記ブロック暗号アルゴリズムが、高度暗号化標準(AES)の対称鍵暗号化演算であり、前記第2のパスワードが、鍵としての前記乱数および前記第1のパスワードを使用する前記対称鍵暗号化演算から出力される、請求項24に記載のコンピュータプログラム。
【請求項２６】
前記鍵としての前記乱数および前記第2のパスワードを用いて対称鍵解読演算を使用すると、前記出力として前記第1のパスワードがもたらされる、請求項25に記載のコンピュータプログラム。
【請求項２７】
前記ユーザが通常モードまたは保護モードのうちの1つを選択し、前記通常モードでは、前記ユーザが訪れる前記サーバサイトに関連付けられた前記第1のパスワードが前記ユーザによって入力されるのに対して、前記保護モードでは、前記ユーザが訪れる前記サーバサイトに関連付けられた前記第2のパスワードが前記ユーザによって入力される、請求項22に記載のコンピュータプログラム。
【請求項２８】
前記ユーザが訪れる前記サーバサイトが、インターネット上のウェブサイトである、請求項22に記載のコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明はアンチショルダーサーフィンの認証方法に関する。
【背景技術】
【０００２】
今日、(アクセス端末、リモート局、コンピューティングデバイスなどとしても知られる)クライアントデバイスの使用が普及している。そのようなクライアントデバイスは、固定(たとえば、デスクトップコンピュータ)またはモバイルのいずれかであり得る。そのようなモバイルデバイスは、ワイヤレス電話アクセス、インターネットアクセス、(個人

、企業、政府などの)コンピュータシステムへのアクセスをユーザに提供することができ、ユーザが、オンラインショッピング、オンラインバンキングなどのオンライン取引、ならびに、特定のロケーションへの地図の検索などの他のアプリケーションなどを実行することを可能にする。このようにして、今日のモバイルデバイスは、ワイヤレス通信、ならびに、非モバイルすなわち固定のコンピュータシステムに関連する通信およびインターネット機能のほとんどすべてを可能にする。そのようなモバイルデバイスの例には、(ノートブックとしても知られる)ラップトップコンピュータ、スマートフォン、携帯電話、携帯情報端末(PDA)、デジタルカメラ、タブレットコンピュータなどが含まれる。

【０００３】

パスワードは、ユーザがサーバサイトに接続するとき、個人情報および資産情報を保護するために広く使用される。そのような保護方法により、ユーザによって設定されたパスワードを使用して、サーバサイトへの接続および個人情報へのアクセスが可能になる。残念ながら、パスワードが露出されたとき、アタッカはパスワードを取得し、次いでユーザの個人情報および資産情報に潜在的にアクセスすることができる。パスワード保護を使用するそのようなサーバサイトの例には、銀行、店舗、工場、学校、データセンタなどに関係するサーバサイトが含まれる。

【０００４】

特に、モバイルデバイスの出現により、しばしばモバイルデバイスは、ショルダーサーフィンアタックが発生する可能性がある混雑した場所で、個人取引を実施するサーバサイトにアクセスする。ショルダーサーフィンは、アタッカが、たとえば、誰かの肩越しに直接見ることによって(または他の手段によって)、モバイルデバイスで入力されたユーザ情報を直接観察して、機密情報を取得するセキュリティアタックである。パスワードベースの認証は、最も広く展開された認証方式の1つである。ショルダーサーフィンアタックは、パスワードベースの認証に対する重大な脅威である。

【０００５】

これの一例は、ユーザが自分のモバイルデバイスを用いて公共の場所(たとえば、会議室、コーヒーショップ、図書館、モールなど)で、サーバサイト(たとえば、銀行、店舗、工場、学校、データセンタなど)にある自分の専用アカウントにログインするときである。モバイルデバイスの画面、キーボードまたはユーザの手の動きは、アタッカにより完全に露出され見ることができる。アタッカの直接観察に基づいて、アタッカは、観察されたユーザ名およびパスワードを用いて、サーバサイトにある同じアカウントに後で首尾よくログインすることができる。多くのオンラインのアプリケーションおよびサービスが、クライアントサーバモデルでパスワードベースの認証を採用している。ユーザには、サーバエンドでの実装について制御の手立てはない。したがって、アタッカによるユーザ名、パスワード、およびユーザが自分のクライアントデバイスを用いて訪れるサーバサイトの潜在的な直接観察に基づくショルダーサーフィンアタックを防止する技法が求められている。

【発明の概要】

【課題を解決するための手段】

【０００６】

本発明の態様は、第2のパスワードを作成する、クライアントデバイス用の装置、システム、および方法に関することができる。クライアントデバイスは、ストレージデバイス、ユーザが訪れるサーバサイトに関連付けられたユーザ名および第1のパスワードを受け取るユーザインターフェース、乱数を発生する乱数発生器、ならびに、第1のパスワードおよび乱数に基づく関数を実行することによって第2のパスワードを生成し、乱数、ユーザ名、および関連付けられたサーバサイトのストレージデバイスへの記憶を命令するプロセッサを含むことができる。ユーザが自分のユーザ名および第2のパスワードを入力することによってサーバサイトにログオンしようと試みる場合、プロセッサはユーザ名およびサーバサイトに関連付けられた乱数をストレージデバイスから抽出し、第2のパスワードおよび乱数に基づく関数を実行して第1のパスワードを生成し、第1のパスワードはユーザ

によって入力された第2のパスワードと入れ替わりサーバサイトに送出される。

【図面の簡単な説明】

【０００７】

【図１】ワイヤレス通信システムの一例のブロック図である。

【図２】本発明の態様を実践できるシステムのブロック図である。

【図３】ユーザに第2のパスワードを提供するプロセスを示す流れ図である。

【図４】クライアントデバイスで第2のパスワードを利用する一例のブロック図である。

【図５】第2のパスワードを利用してサーバサイトにアクセスするプロセスを示す流れ図である。

【発明を実施するための形態】

【０００８】

「例示的」という言葉は、「例、実例、または例示として機能すること」を意味するために本明細書で使用される。「例示的」または「例」として本明細書に記載される任意の実施形態は、他の実施形態に比べて好ましいか、または有利であると必ずしも解釈されるべきではない。

【０００９】

図1を参照すると、ワイヤレス移動局(MS)102は、ワイヤレス通信システム100の1つまたは複数の基地局(BS)104と通信することができる。ワイヤレス通信システム100は、1つまたは複数の基地局コントローラ(BSC)106、およびコアネットワーク108をさらに含むことができる。コアネットワークは、適切なバックホールを介して、インターネット110および公衆交換電話網(PSTN)112に接続することができる。典型的なワイヤレス移動局には、ハンドヘルド電話またはラップトップコンピュータが含まれ得る。ワイヤレス通信システム100は、符号分割多元接続(CDMA)、時分割多元接続(TDMA)、周波数分割多元接続(FDMA)、空間分割多元接続(SDMA)、偏波分割多元接続(PDMA)、または当技術分野で知られている他の変調技法などのいくつかの多元接続技法のうちのいずれか1つを採用することができる。

【００１０】

ワイヤレスデバイス102は、任意の適切なワイヤレス通信技術に基づくか、または場合によっては任意の適切なワイヤレス通信技術をサポートする、1つまたは複数のワイヤレス通信リンクを介して通信することができる。たとえば、いくつかの態様では、ワイヤレスデバイスはネットワークと関連することができる。いくつかの態様では、ネットワークは、ボディエリアネットワークまたはパーソナルエリアネットワーク(たとえば、超広帯域ネットワーク)を備えることができる。いくつかの態様では、ネットワークは、ローカルエリアネットワークまたはワイドエリアネットワークを備えることができる。ワイヤレスデバイスは、たとえばCDMA、TDMA、OFDM、OFDMA、WiMAX、およびWi-Fiなどの様々なワイヤレス通信技術、プロトコル、または規格のうちの1つまたは複数をサポートするか、または場合によっては使用することができる。同様に、ワイヤレスデバイスは、様々な対応する変調または多重化方式のうちの1つまたは複数をサポートするか、または場合によっては使用することができる。したがって、ワイヤレスデバイスは、上記または他のワイヤレス通信技術を使用して、1つまたは複数のワイヤレス通信リンクを確立し、それを介して通信するのに適した構成要素(たとえばエアインターフェース)を含むことができる。たとえば、デバイスは、ワイヤレス媒体を介した通信を容易にする様々な構成要素(たとえば、信号発生器および信号処理器)を含むことができる、関連する送信機および受信機の構成要素(たとえば、送信機および受信機)を有するワイヤレス送受信機を備えることができる。

【００１１】

本発明の態様は、ユーザ名、パスワード、および、公共の場でモバイルクライアントデバイス102を利用してサーバサイトにアクセスするユーザが訪れるサーバサイトの直接観察に基づく、アタッカによるショルダーサーフィンアタックまたは他のタイプのアタックを防止することに関する。以下に記載される修正は、モバイルクライアントデバイス102

での修正に関するだけで、サーバサイトの修正は必要としないことに留意されたい。さらに、例として、モバイルクライアントデバイス102は、ラップトップコンピュータ、スマートフォン、携帯電話、携帯情報端末(PDA)、デジタルカメラ、モバイルコンピュータなどであり得るし、通常ワイヤレスデバイスと呼ぶことができる。しかしながら、本発明の態様は有線デバイスにも関係する。以下、ワイヤレスデバイスまたは有線デバイス、固定またはモバイルのいずれでもあり得るクライアントデバイス102という用語が利用される。

【００１２】

詳細には、本発明の態様は、ユーザ用の第2のパスワードを作成する装置、方法、およびシステムに関する。たとえば、クライアントデバイス102は、ストレージデバイス、ユーザが訪れる特定のサーバサイトに関連付けられたユーザ名および第1のパスワードを受け取るユーザインターフェース、乱数を発生する乱数発生器、ならびにプロセッサを備えることができる。プロセッサは、第1のパスワードおよび乱数に基づく関数を実行することによって第2のパスワードを生成し、乱数、ユーザ名、および関連付けられたサーバサイトのストレージデバイスへの記憶を命令するために使用することができる。第2のパスワードの生成後、ユーザが自分のユーザ名および第2のパスワードを入力することによって特定のサーバサイトにログオンしようと試みる場合、プロセッサはユーザ名およびサーバサイトに関連付けられた乱数をストレージデバイスから抽出することができる。次いで、プロセッサは、第2のパスワードおよび乱数に基づく関数を実行して第1のパスワードを生成し、第1のパスワードはユーザによって入力された第2のパスワードと入れ替わり、ユーザが特定のサーバサイトにアクセスできるようにそのサーバサイトに送出される。このようにして、クライアントデバイス102は、アンチショルダーサーフィンの認証機構として働く。

【００１３】

図2を参照すると、図2は、本発明の態様を実践できるシステム101のブロック図である。詳細には、システム101は、ユーザ用の第2のパスワードを作成できるクライアントデバイス102を含む。クライアントデバイス102は、ディスプレイデバイス142、ユーザインターフェース140、乱数発生器132、およびプロセッサ130を含むことができる。ディスプレイデバイス142は、モバイルデバイス、携帯電話、携帯情報端末、ラップトップコンピュータなどのクライアントデバイス102上の典型的なディスプレイデバイスであり得る。ユーザインターフェース140は、通常クライアントデバイス102とともに使用されるキーパッド、キーボード、または別のタイプのユーザ入力デバイスであり得る。

【００１４】

一態様では、クライアントデバイス102は、以下で説明されるように、第2のパスワードを作成し利用するための命令を実行するように構成された、プロセッサ130およびメモリ131を含むことができる。メモリ131はプロセッサ130に結合されて、プロセッサ130による実行用の命令を記憶することができる。このようにして、クライアントデバイス102は、命令を実行して第2のパスワードの作成および第2のパスワードの利用を実施するように構成される。

【００１５】

ユーザインターフェース140は、ユーザによってアクセスされようとする特定のサーバサイト103(たとえば、ウェブサイト)に関連付けられたユーザ名150、サーバサイト識別子152、および第1のパスワード153を受け取ることができる。乱数発生器132は、ユーザ名150およびサーバサイト指示子152に関連付けられるべき乱数160を発生することができる。

【００１６】

プロセッサ130は、第1のパスワード153および乱数160に基づく関数を実行することによって、第2のパスワードを生成することができる。プロセッサ130は、ユーザ名150、乱数160、および関連付けられた指定のサーバサイト152を、表162の一部としてストレージデバイス134に記憶するように命令することができる。図2に示されたように、表162は、他の情報とともに複数のユーザ名150、サーバサイト152、および関連付けられた乱数160を含

むことができる。

【００１７】

生成された第2のパスワード154は、次いでユーザが第2のパスワードを有するように、ディスプレイデバイス142上でユーザに表示することができる。次いで第2のパスワード154は、ユーザが訪れるサーバサイト103およびユーザによって入力されたパスワードをアタッカが直接観察しようとする可能性があるエリアで、ユーザが自分のクライアントデバイス102を利用するときに、使用することができる。

【００１８】

一態様では、第1のパスワード153をユーザの通常パスワードと呼ぶことができ、第2のパスワード154をユーザの保護パスワードと呼ぶことができる。また、乱数160は安全な乱数であり得る。

【００１９】

以下に記載されるように、ユーザが自分のユーザ名150および第2のパスワード154を入力することによって、特定のサーバサイト103にログオンしようと試みるとき、プロセッサ130は、ユーザ名150およびサーバサイト152に関連付けられた乱数160をストレージデバイスから抽出する。プロセッサは、第2のパスワード154および乱数160に基づく関数を実行して第1のパスワード153を生成し、第1のパスワード153は、ユーザによって入力された第2のパスワードと入れ替わり、アクセスのために特定のサーバサイト103に送出される。

【００２０】

第1のパスワード153または第2のパスワード154のいずれも、モバイルクライアントデバイス102に記憶されないことに留意されたい。さらに、ユーザは、自分が使用する第2のパスワード154を作成するために、秘密用の専用環境内でクライアントデバイス102を有することができることに留意されたい。このようにして、ユーザだけが第1のパスワード153および第2のパスワード154を知り、どちらもクライアントデバイス102によって記憶されず、したがってアタッカによってアクセスできない。

【００２１】

一態様では、ユーザが自分の第2のパスワード154を作成しているとき、ユーザはサーバサイト103に実際にログオンする必要がない。この実装形態では、ユーザは自分のユーザ名150、サーバサイト指示子152、および第1のパスワード153をローカルに入力し、プログラム(たとえば、ソフトウェア、ファームウェア、またはミドルウェア)を実装するプロセッサは、前述のように、ディスプレイデバイス142上でユーザに表示するための第2のパスワード154を生成する。このプロセスでは、乱数160、サーバサイト152、およびユーザ名150は、ストレージデバイス134に記憶される。したがって、このプロセスはオフラインで遂行することができる。しかしながら、それは、クライアントデバイス102がサーバサイト103と通信するように、有線またはワイヤレスでリンク170を介して、インターフェース136によりオンラインでも実施することができる。インターフェース136は、ワイヤレスリンク(たとえば、図1)を介してサーバ103と通信できる送信機および受信機を含むワイヤレスインターフェース、ならびに/または、有線リンク(たとえば、ケーブルシステム、PSTN、他のリンク、およびそれらの組合せ)を介して通信して、サーバ103と通信する有線インターフェースであり得る。

【００２２】

図3を簡単に参照すると、ユーザに第2のパスワードを提供するプロセス300を例示する流れ図が示される。ブロック302で、ユーザは第2のパスワードを作成する機能を選択する。次いで、ユーザは、ユーザインターフェース140を介して、自分のユーザ名150、特定のサーバサイト152、および自分の第1のパスワード153を入力する(ブロック304)。次いで、乱数160が発生される(たとえば、安全な乱数)(ブロック306)。プロセッサ130は、第1のパスワード153および乱数に基づく関数を実行することによって、第2のパスワード154を生成する(ブロック308)。

【００２３】

たとえば、第2のパスワード154は、第1のパスワード153および乱数160の関数であり得

る。第2のパスワードは、式:第2のパスワード=f(第1のパスワード,乱数)によって決定することができる。次に、プロセス300はユーザ名150、サーバサイト152、および乱数160をストレージデバイス134に記憶する(ブロック310)。次いで、第2のパスワード154がディスプレイデバイス142上でユーザに表示される(ブロック312)。

【００２４】

一態様では、関数(f)は、ブロック暗号アルゴリズムなどの1対1マッピング関数であり得る。特定の一態様では、ブロック暗号アルゴリズムは、高度暗号化標準(AES)の対称鍵暗号化演算であり得るし、そこでは第2のパスワード154は、鍵としての乱数160および平文として第1のパスワード153を使用する対称鍵暗号化演算から出力される。さらに、後でより詳細に記載されるように、第1のパスワード153を決定するために、鍵としての乱数160および第2のパスワード154を使用する対称鍵解読演算(f^{-1})は、出力として第1のパスワードをもたらす。

【００２５】

また図4を参照すると、クライアントデバイス102で第2のパスワード154を利用する一例が示される。図4に示されたように、ユーザは、クライアントデバイス102のユーザインターフェース140を介して、自分のユーザ名150、サーバサイト指示子152、および第2のパスワード154を入力することによって、特定のサーバサイト103にログオンしようと試みることができる。プロセッサ130は、ユーザ名150およびサーバサイト152に関連付けられた乱数160をストレージデバイス134から抽出し、第2のパスワード154および乱数160に基づく関数を実行して第1のパスワード153を生成し、第1のパスワード153はユーザによって入力された第2のパスワードと入れ替わり、特定のサーバサイト103に送出される。詳細には、サーバサイト103へのアクセスは、ユーザ名150および第1のパスワード153を用いて、インターフェース136およびリンク170を介して行われる。ユーザ名150および第1のパスワード153は、非表示の暗号化されたフォーマットであり得る。また、前述のように、リンク170は、ワイヤレスリンクもしくは有線リンク、またはそれらの組合せであり得る。

【００２６】

操作時、ユーザは通常モードまたは保護モードのうちの1つを選択することができる。通常モードでは、ユーザが訪れようとしている特定のサーバサイト103用の第1のパスワード153およびサーバサイト指示子152が、ユーザインターフェース140を介してユーザによって入力され、通常操作が行われる。一方、保護モードでは、ユーザが訪れようとしている特定のサーバサイト103に関連付けられたサーバサイト指示子152および第2のパスワード154が、ユーザインターフェース140を介してユーザによってクライアントデバイス102に入力される。様々な態様では、プロセッサ130は、ミドルウェア、ソフトウェア、ファームウェア、またはそれらの組合せと連携して動作することができる。また、例として、ユーザが訪れるサーバサイト103は、銀行、店舗、企業、学校、データセンタなどの、インターネット上のサーバサイトまたはウェブサイトであり得るし、認証用のパスワードが必要とされる任意のタイプのネットワーク(たとえば、公衆、専用、企業、政府などのネットワーク)を介することができる。さらに、これらのサーバサイトへのアクセスは、ワイヤレスリンクおよび/または有線リンクならびにそれらの組合せを介して行うことができる。

【００２７】

図5を簡単に参照すると、第2のパスワード154を利用してサーバサイト103にアクセスするプロセス500を例示する流れ図が示される。決定ブロック502で、ユーザは通常モードまたは保護モードを選択する。通常モードが選択された場合、クライアントデバイス102は通常の処理を進める(ブロック504)。しかしながら、ユーザにより保護モードが選択された場合、ユーザは、自分のユーザ名150、サーバサイト指示子152、および第2のパスワード154を入力することによって、サーバサイト103にログオンする(ブロック506)。ユーザ名150およびサーバサイト指示子152に関連付けられた乱数160(たとえば、安全な乱数)が抽出される(ブロック508)。

【００２８】

次に、第2のパスワードに基づく関数を実行することによって、第1のパスワード153が生成される(ブロック510)。たとえば、第1のパスワードは、式:第1のパスワード=f^{-1}(第2のパスワード,乱数)によって得ることができる。第1のパスワード153が第2のパスワード154と入れ替わり、インターフェース136を介してリンク170を経てサーバサイト103に送出される(ブロック512)。たとえば、サーバサイト103へのアクセスは、暗号化された非表示の形の第1のパスワードを用いて行うことができる。次いで、ユーザはサーバサイト103にアクセスすることができる(ブロック514)。

【００２９】

関数(f)は1対1マッピング関数であり得る。一態様では、関数はブロック暗号アルゴリズムであり得る。特定の一態様では、ブロック暗号アルゴリズムは、高度暗号化標準(AES)の対称鍵暗号化演算である。前述のように、第2のパスワードは、鍵として乱数を、平文として第1のパスワードを使用する対称鍵暗号化演算から出力される。第1のパスワードに関して、鍵としての乱数および第2のパスワードを用いて対称鍵解読演算(f^{-1})を使用すると、出力として第1のパスワードがもたらされる。多種多様な異なるタイプのアルゴリズムが利用できることを諒解されたい。

【００３０】

特定の一態様では、ミドルウェアモジュールがクライアントデバイス102によって使用することができ、クライアントデバイス102では、ミドルウェアモジュールの機能は、ユーザ名およびパスワードのフィールドを含むサーバ/ウェブのフォームを検査および処理することである。ミドルウェアは、特定のサーバサイトへの保護されたアクセスをサポートするように構成することができる。ミドルウェアは、通常モードおよび保護モードの2つのモードで動作することができる。ミドルウェアは、保護モードによって使用されて第2のパスワード154を生成するために、サーバサイト指示子152によって指定された特定のサーバサイト103用にユーザによって入力された第1のパスワード153を設定するユーザ画面を提供することができる。ミドルウェアは、最初に乱数160を生成することができ、次いで、ユーザによって入力される第1のパスワード153を要求することができる。代替として、クライアントデバイス102は、乱数発生器132を実装する他のタイプのハードウェア、ファームウェア、またはソフトウェアを含むことができる。ミドルウェアは、第1のパスワード153および乱数160の関数として第2のパスワード154を計算することができる。次いで、ミドルウェアは、乱数160、ユーザ名150、およびサーバサイト指示子152のストレージデバイス134への記憶を命令することができる。

【００３１】

さらなる例として、操作時、保護モードでは、ユーザはウェブフォームに第2のパスワード154を入力し、ミドルウェアはウェブフォームから第2のパスワードを抽出し、記憶された乱数160を取り出し、第1のパスワード153を計算する。ミドルウェアは、第2のパスワード154を第1のパスワード153と入れ替え、サーバサイト103に要求を送出する。一方通常モードでは、ウェブフォームは、いかなる修正もなしにサーバに送信される。ミドルウェア、ファームウェア、ソフトウェア、またはハードウェアの任意の組合せが、本発明の態様を実装するために利用できることを諒解されたい。

【００３２】

本発明の態様は、サーバサイト103でのいかなる修正も必要としない。さらに、第1のパスワード153または第2のパスワード154のいずれも、クライアントデバイス102に記憶されない。それゆえ、アタッカがユーザによって入力された第2のパスワード154およびユーザ名150を観察しても、アタッカは、同じ乱数160がなければ、まだサーバサイト103にログオンすることができない。したがって、クライアントデバイス102を侵害して同じ乱数を取得すること、第2のパスワードを取得すること、および同じプログラムをインストールすることをすべて同時に行うことによって、アタッカが認証プロセスをバイパスするリスクは比較的低い。さらに、情報漏洩が起きた可能性があるとユーザが考えた場合はいつでも、ユーザは、新しい乱数160を用いて新しい第2のパスワード154を再生成することができる。したがって、本発明の態様は、1)第2の(たとえば、保護された)パスワード、およ

び2)乱数を有するデバイスに基づく2要素認証を提供する。当業者には知られているように、2要素認証は1要素認証とは対照的に、認証の2つのレベルまたは2つのインスタンスを必要とし、したがって、2要素認証は第2のセキュリティレイヤを追加する。

【００３３】

本明細書の教示は、様々な装置(たとえば、デバイス)に組み込む(たとえば、それらの装置内に実装するか、またはそれらの装置によって実行する)ことができる。たとえば、本明細書で教示された1つまたは複数の態様は、電話(たとえば、携帯電話)、携帯情報端末(「PDA」)、エンターテインメントデバイス(たとえば、音楽デバイスもしくはビデオデバイス)、ヘッドセット(たとえば、ヘッドフォン、イヤピースなど)、マイクロフォン、医療用デバイス(たとえば、生体センサ、心拍数モニタ、歩数計、EKGデバイスなど)、ユーザI/Oデバイス(たとえば、時計、リモートコントロール、照明スイッチ、キーボード、マウスなど)、タイヤ圧モニタ、コンピュータ、POSデバイス、エンターテインメントデバイス、補聴器、セットトップボックス、または任意の他の適切なデバイスに組み込むことができる。

【００３４】

これらのデバイスは、様々な電力要件およびデータ要件を有する場合がある。いくつかの態様では、本明細書の教示は、(たとえば、インパルスベースの信号方式および低デューティサイクルモードの使用により)低電力アプリケーションでの使用に適合することができ、(たとえば、高帯域パルスの使用による)比較的高いデータレートを含む様々なデータレートをサポートすることができる。

【００３５】

いくつかの態様では、ワイヤレスデバイスは、通信システム用のアクセスデバイス(たとえば、Wi-Fiアクセスポイント)を備えることができる。そのようなアクセスデバイスは、たとえば、有線またはワイヤレスの通信リンクを介した、別のネットワーク(たとえば、インターネットまたはセルラーネットワークなどのワイドエリアネットワーク)への接続を提供することができる。したがって、アクセスデバイスは、別のデバイス(たとえば、Wi-Fi局)が他のネットワークまたは何らかの他の機能にアクセスすることを可能にすることができる。さらに、デバイスのうちの1つまたは両方は携帯型であるか、または場合によっては比較的非携帯型であり得ることを諒解されたい。

【００３６】

情報および信号は、様々な異なる技術および技法のいずれかを使用して表現できることを、当業者は理解されよう。たとえば、上記の説明全体にわたって言及され得るデータ、命令、コマンド、情報、信号、ビット、シンボル、およびチップは、電圧、電流、電磁波、磁界もしくは磁性粒子、光場もしくは光学粒子、またはそれらの任意の組合せによって表現することができる。

【００３７】

本明細書で開示された実施形態に関連して記載された様々な例示的な論理ブロック、モジュール、回路、およびアルゴリズムステップは、電子ハードウェア、コンピュータソフトウェア、または両方の組合せとして実装できることを、当業者はさらに諒解されよう。ハードウェアとソフトウェアのこの互換性を明確に示すために、様々な例示的な構成要素、ブロック、モジュール、回路、およびステップが、概してそれらの機能に関して上述された。そのような機能がハードウェアとして実装されるか、またはソフトウェアとして実装されるかは、特定の適用例および全体的なシステムに課される設計制約に依存する。当業者は、記載された機能を特定の適用例ごとに様々な方法で実装できるが、そのような実装の決定は、本発明の範囲からの逸脱を生じるものと解釈すべきではない。

【００３８】

本明細書で開示された実施形態に関連して記載された様々な例示的な論理ブロック、モジュール、および回路は、汎用プロセッサ、デジタル信号プロセッサ(DSP)、特定用途向け集積回路(ASIC)、フィールドプログラマブルゲートアレイ(FPGA)もしくは他のプログラマブル論理デバイス、個別ゲートもしくはトランジスタ論理、個別ハードウェア構成要素

、または、本明細書に記載された機能を実行するように設計されたそれらの任意の組合せで、実装または実行することができる。汎用プロセッサはマイクロプロセッサであり得るが、代替として、プロセッサは、任意の従来のプロセッサ、コントローラ、マイクロコントローラ、または状態機械であり得る。プロセッサはまた、コンピューティングデバイスの組合せ、たとえば、DSPとマイクロプロセッサとの組合せ、複数のマイクロプロセッサ、DSPコアと連携する1つもしくは複数のマイクロプロセッサ、または任意の他のそのような構成として実装することができる。

【００３９】

本明細書で開示された実施形態に関連して記載された方法またはアルゴリズムのステップは、直接ハードウェアで、プロセッサによって実行されるソフトウェアモジュールで、またはその2つの組合せで具現化することができる。ソフトウェアモジュールは、RAMメモリ、フラッシュメモリ、ROMメモリ、EPROMメモリ、EEPROMメモリ、レジスタ、ハードディスク、リムーバブルディスク、CD-ROM、または当技術分野で知られている任意の他の形態の記憶媒体に常駐することができる。例示的な記憶媒体は、プロセッサが記憶媒体から情報を読み取り、記憶媒体に情報を書き込むことができるように、プロセッサに結合される。代替として、記憶媒体はプロセッサと一体である場合がある。プロセッサおよび記憶媒体はASICに常駐することができる。ASICはユーザ端末に常駐することができる。代替として、プロセッサおよび記憶媒体は、ユーザ端末に個別構成要素として常駐することができる。

【００４０】

1つまたは複数の例示的な実施形態では、記載された機能は、ハードウェア、ソフトウェア、ミドルウェア、ファームウェア、またはそれらの任意の組合せに実装することができる。コンピュータプログラム製品としてソフトウェアに実装された場合、機能は、1つまたは複数の命令またはコードとしてコンピュータ可読媒体上に記憶するか、またはコンピュータ可読媒体を介して送信することができる。コンピュータ可読媒体は、ある場所から別の場所へのコンピュータプログラムの転送を可能にする任意の媒体を含む、コンピュータ記憶媒体とコンピュータ通信媒体の両方を含む。記憶媒体は、コンピュータによってアクセスできる任意の利用可能な媒体であり得る。限定ではなく例として、そのようなコンピュータ可読媒体は、RAM、ROM、EEPROM、CD-ROMもしくは他の光ディスクストレージ、磁気ディスクストレージもしくは他の磁気ストレージデバイス、または、命令もしくはデータ構造の形態で所望のプログラムコードを搬送もしくは記憶するために使用でき、コンピュータによってアクセスできる、任意の他の媒体を含むことができる。また、いかなる接続もコンピュータ可読媒体と適切に呼ばれる。たとえば、ソフトウェアが、同軸ケーブル、光ファイバケーブル、ツイストペア、デジタル加入者回線(DSL)、または赤外線、無線、およびマイクロ波などのワイヤレス技術を使用して、ウェブサイト、サーバ、または他のリモートソースから送信される場合、同軸ケーブル、光ファイバケーブル、ツイストペア、DSL、または赤外線、無線、およびマイクロ波などのワイヤレス技術は、媒体の定義に含まれる。本明細書で使用するディスク(disk)およびディスク(disc)は、コンパクトディスク(disc)(CD)、レーザディスク(disc)、光ディスク(disc)、デジタル多用途ディスク(disc)(DVD)、フレキシブルディスク(disk)、およびブルーレイディスク(disc)を含み、ディスク(disk)は、通常、磁気的にデータを再生し、ディスク(disc)は、レーザで光学的にデータを再生する。上記の組合せもコンピュータ可読媒体の範囲内に含まれるべきである。

【００４１】

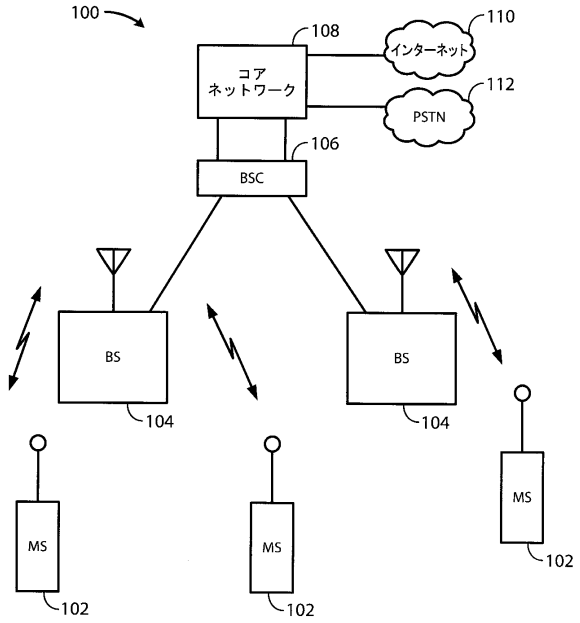
開示された実施形態の前の説明は、いかなる当業者も本発明を作成または使用することを可能にするために提供される。これらの実施形態への様々な修正が当業者には容易に明らかになり、本明細書で規定された一般原理は、本発明の趣旨または範囲を逸脱することなく、他の実施形態に適用することができる。したがって、本発明は、本明細書に示された実施形態に限定されるものではなく、本明細書で開示された原理および新規の特徴に一致する最大の範囲を与えられるものである。

【符号の説明】

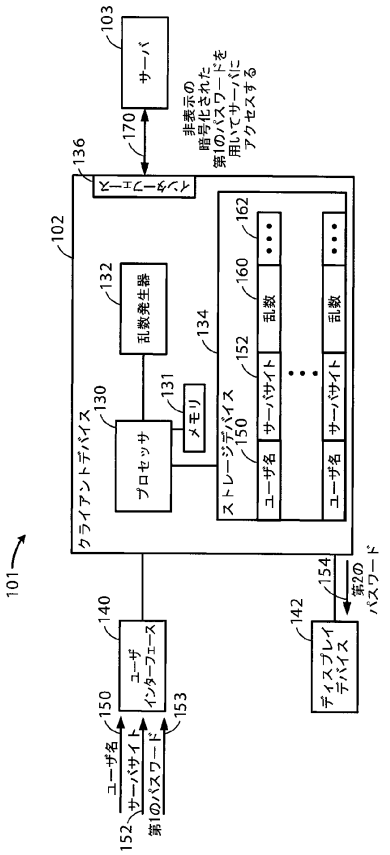
【００４２】

100　ワイヤレス通信システム
101　システム
102　ワイヤレス移動局(MS)
103　サーバサイト
104　基地局(BS)
106　基地局コントローラ(BSC)
108　コアネットワーク
110　インターネット
112　公衆交換電話網(PSTN)
130　プロセッサ
131　メモリ
132　乱数発生器
134　ストレージデバイス
136　インターフェース
140　ユーザインターフェース
142　ディスプレイデバイス
150　ユーザ名
152　サーバサイト
153　第1のパスワード
154　第2のパスワード
160　乱数
162　表
170　リンク
300　ユーザに第2のパスワードを提供するプロセス
500　第2のパスワードを利用してサーバサイトにアクセスするプロセス

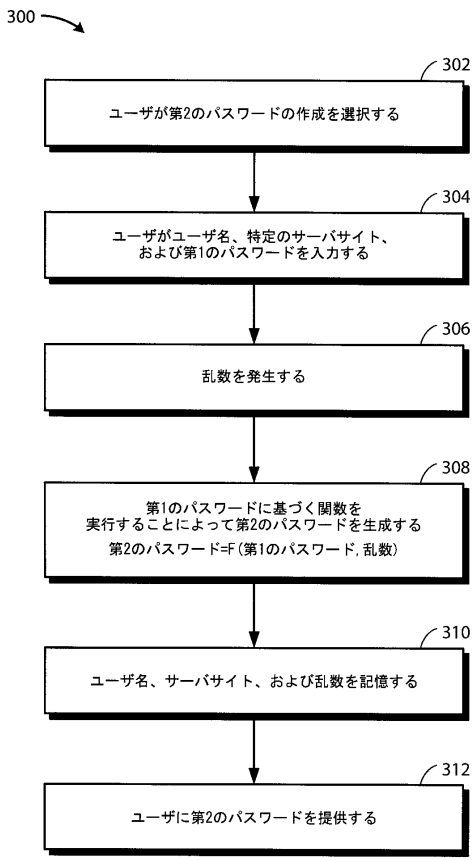
【図１】


100
108
コア
ネットワーク
110
インターネット
112
PSTN
106
BSC
BS
104
BS
104
MS
102
MS
102
MS
102

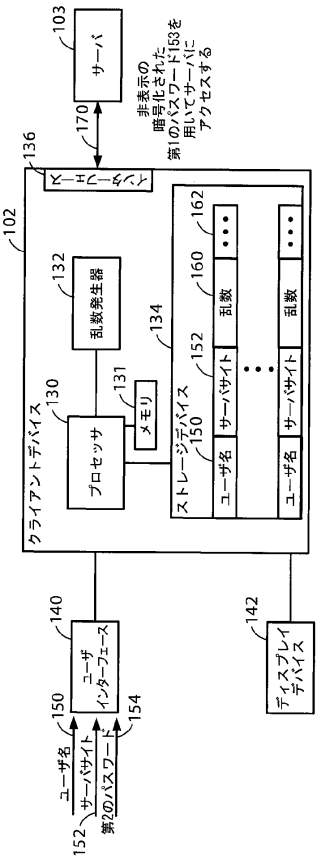
【図２】


103
サーバ
非表示の
暗号化された
第1のパスワードを
用いてサーバに
アクセスする
170
136
ドーエビーをベト
102
162
132
乱数発生器
134
160
乱数
152
サーバサイト
150
ユーザ名
ストレージデバイス
131
メモリ
130
プロセッサ
クライアントデバイス
101
154
第2の
パスワード
140
ユーザ
インターフェース
142
ディスプレイ
デバイス
150
ユーザ名
153
サーバサイト
第1のパスワード
152

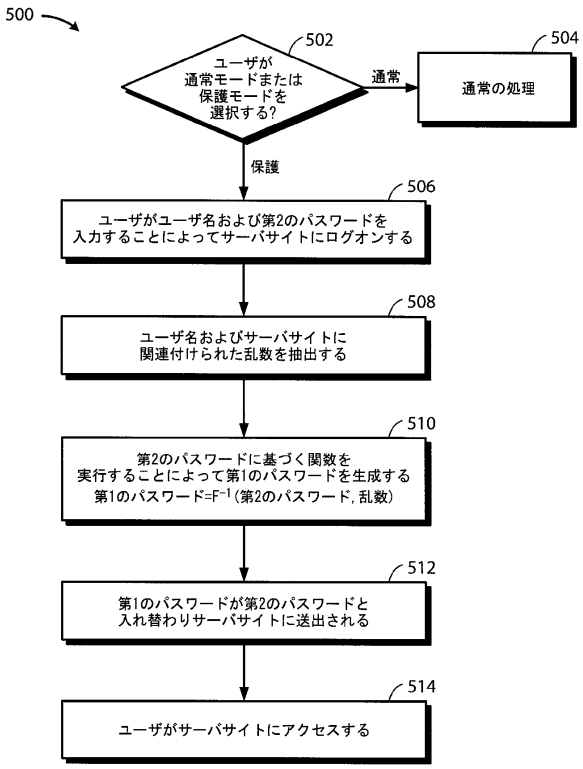
【図３】


300
302
ユーザが第2のパスワードの作成を選択する
304
ユーザがユーザ名、特定のサーバサイト、
および第1のパスワードを入力する
306
乱数を発生する
308
第1のパスワードに基づく関数を
実行することによって第2のパスワードを生成する
第2のパスワード=F(第1のパスワード, 乱数)
310
ユーザ名、サーバサイト、および乱数を記憶する
312
ユーザに第2のパスワードを提供する

【図４】


103
サーバ
非表示の
暗号化された
第1のパスワード153を
用いてサーバに
アクセスする
170
136
ドーエビーをベト
102
162
132
乱数発生器
134
160
乱数
152
サーバサイト
150
ユーザ名
ストレージデバイス
131
メモリ
130
プロセッサ
クライアントデバイス
140
ユーザ
インターフェース
142
ディスプレイ
デバイス
150
ユーザ名
154
サーバサイト
第2のパスワード
152

【図５】


500
502
ユーザが
通常モードまたは
保護モードを
選択する?
通常
504
通常の処理
保護
506
ユーザがユーザ名および第2のパスワードを
入力することによってサーバサイトにログオンする
508
ユーザ名およびサーバサイトに
関連付けられた乱数を抽出する
510
第2のパスワードに基づく関数を
実行することによって第1のパスワードを生成する
第1のパスワード=F-1(第2のパスワード, 乱数)
512
第1のパスワードが第2のパスワードと
入れ替わりサーバサイトに送出される
514
ユーザがサーバサイトにアクセスする

フロントページの続き

(56)参考文献 特開２００７－３５０４１（ＪＰ，Ａ）
特開２００１－３０６５１３（ＪＰ，Ａ）
特開２００８－５３７１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０９Ｃ　１／００