(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-171056
(P2004-171056A)
(43)公開日　平成16年6月17日(2004.6.17)

(51)Int.Cl.[7]		F I			テーマコード（参考）
G06F	15/00	G06F	15/00	330B	5B076
G06F	9/445	G06F	9/06	640A	5B085
H04L	9/32	H04L	9/00	673A	5J104

審査請求 有　請求項の数 10　OL　（全 15 頁）

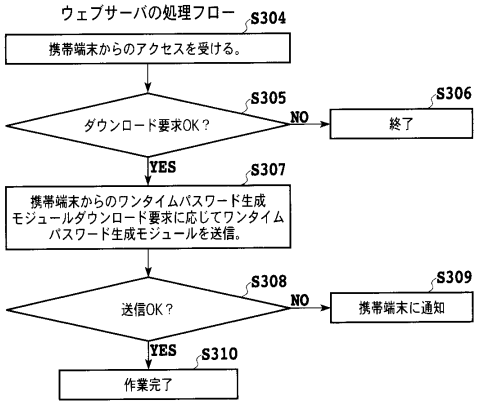
(21)出願番号　特願2002-332716(P2002-332716)
(22)出願日　平成14年11月15日(2002.11.15)

(71)出願人　500198841
アールエスエイ　セキュリティー　インコーポレーテッド
アメリカ合衆国　０１７３０　マサチューセッツ州　ベッドフォード　ミドルセックス　ターンパイク　１７４
(74)代理人　100077481
弁理士　谷　義一
(74)代理人　100088915
弁理士　阿部　和夫
(74)代理人　100106998
弁理士　橋本　傳一

最終頁に続く

(54)【発明の名称】ワンタイムパスワード生成プログラムの配布サーバ、配布方法および配布プログラム、コンピュータ読み取り可能な記録媒体ならびにワンタイムパスワード生成プログラムの配布システム

(57)【要約】
【課題】ソフトウェア管理の煩雑さや情報提供サーバの作業負担を解消するとともに、セキュリティ性を高めることの可能なワンタイムパスワード生成プログラムの配布サーバを提供する。
【解決手段】ワンタイムパスワード生成モジュールを記憶しているウェブサーバ３０は、携帯端末１０のユーザからのアクセスを受けると（Ｓ３０４）、ワンタイムパスワード生成モジュールのダウンロードを受け付けるための表示画面を携帯端末１０に表示させる。携帯端末１０からワンタイムパスワード生成モジュールのダウンロードが要求された場合、ウェブサーバ３０は、その携帯端末１０に対し、全てのユーザに共通のワンタイムパスワード生成モジュールをダウンロードする（Ｓ３０７）。
【選択図】　図８



【特許請求の範囲】
【請求項１】
携帯端末に対し、ユーザ識別子の入力を受けるステップと、前記入力を受けるステップにおいて入力されたユーザ識別子に基づいて、ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成するステップと、前記生成するステップにおいて生成されたワンタイムパスワードを表示部に表示するステップとを実行させるワンタイムパスワード生成プログラムを配布するためのワンタイムパスワード生成プログラムの配布サーバであって、
前記ワンタイムパスワード生成プログラムを記憶した記憶手段と、
前記携帯端末から前記ワンタイムパスワード生成プログラムのダウンロードの要求情報を受信する受信手段と、
前記受信手段による要求情報の受信に応じて前記記憶手段に記憶されたワンタイムパスワード生成プログラムを前記携帯端末にダウンロードするダウンロード手段と
を備えたことを特徴とするワンタイムパスワード生成プログラムの配布サーバ。
【請求項２】
請求項１に記載のワンタイムパスワード生成プログラムの配布サーバにおいて、前記ワンタイムパスワード生成プログラムは、前記携帯端末に対し、前記表示するステップにおける表示に基づいてユーザにより入力されたワンタイムパスワードを送信するステップを更に実行させることを特徴とするワンタイムパスワード生成プログラムの配布サーバ。
【請求項３】
携帯端末に対し、ユーザ識別子の入力を受けるステップと、前記入力を受けるステップにおいて入力されたユーザ識別子に基づいて、ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成するステップと、前記生成するステップにおいて生成されたワンタイムパスワードを表示部に表示するステップとを実行させるワンタイムパスワード生成プログラムを記憶したコンピュータを用いて、前記記憶されたワンタイムパスワード生成プログラムを配布する方法であって、
前記携帯端末から前記ワンタイムパスワード生成プログラムのダウンロードの要求情報を受信するステップと、
前記受信するステップにおいて受信した要求情報に応じて前記記憶されたワンタイムパスワード生成プログラムを前記携帯端末にダウンロードするステップとを備えたことを特徴とするワンタイムパスワード生成プログラムの配布方法。
【請求項４】
請求項３に記載のワンタイムパスワード生成プログラムの配布方法において、前記ダウンロードするステップは前記ワンタイムパスワード生成プログラムをバイト・コード形式でダウンロードすることを特徴とするワンタイムパスワード生成プログラムの配布方法。
【請求項５】
請求項３に記載のワンタイムパスワード生成プログラムの配布方法において、前記ダウンロードするステップは前記ワンタイムパスワード生成プログラムを暗号化してダウンロードすることを特徴とするワンタイムパスワード生成プログラムの配布方法。
【請求項６】
携帯端末に対し、ユーザ識別子の入力を受けるステップと、前記入力を受けるステップにおいて入力されたユーザ識別子に基づいて、ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成するステップと、前記生成するステップにおいて生成されたワンタイムパスワードを表示部に表示するステップとを実行させるワンタイムパスワード生成プログラムを記憶したコンピュータを用いて、前記記憶されたワンタイムパスワード生成プログラムを配布するためのワンタイムパスワード生成プログラムの配布プログラムであって、前記コンピュータに対し、
前記携帯端末から前記ワンタイムパスワード生成プログラムのダウンロードの要求情報を受信するステップと、
前記受信するステップにおいて受信した要求情報に応じて前記記憶された前記ワンタイム

パスワード生成プログラムを前記携帯端末にダウンロードするステップと
を実行させることを特徴とするワンタイムパスワード生成プログラムの配布プログラム。
【請求項７】
請求項６に記載のワンタイムパスワード生成プログラムの配布プログラムにおいて、前記ダウンロードするステップは前記ワンタイムパスワード生成プログラムをバイト・コード形式でダウンロードすることを特徴とするワンタイムパスワード生成プログラムの配布プログラム。
【請求項８】
請求項７に記載のワンタイムパスワード生成プログラムの配布プログラムにおいて、前記ダウンロードするステップは前記ワンタイムパスワード生成プログラムを暗号化してダウンロードすることを特徴とするワンタイムパスワード生成プログラムの配布プログラム。
【請求項９】
請求項６ないし８のいずれかに記載のワンタイムパスワード生成プログラムの配布プログラムを記録したことを特徴とするコンピュータ読み取り可能な記録媒体。
【請求項１０】
ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成する携帯端末であって、
ユーザ識別子を入力する入力手段と、
前記入力手段から入力されたユーザ識別子に基づいてワンタイムパスワードを生成する生成手段と、
前記生成手段により生成されたワンタイムパスワードを表示する表示手段と
を有する携帯端末と、
請求項１または２に記載のワンタイムパスワード生成プログラムの配布サーバと
を備えたことを特徴とするワンタイムパスワード生成プログラムの配布システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明はワンタイムパスワード生成プログラムの配布サーバ、配布方法および配布プログラム、コンピュータ読み取り可能な記録媒体ならびにワンタイムパスワード生成プログラムの配布システムに関し、より詳細には、ネットワーク上においてユーザ認証（本人認証）に用いられるワンタイムパスワードを携帯端末で生成するためのワンタイムパスワード生成プログラムの配布サーバ、配布方法および配布プログラム、コンピュータ読み取り可能な記録媒体ならびにワンタイムパスワード生成プログラムの配布システムに関する。
【０００２】
【従来の技術】
ワンタイムパスワード認証システムでは、固定パスワードのようにユーザだけが知っている要素だけではなく、第二の要素、すなわち、誰にも予測がつかず、ログインのたびごとに一度限り有効となるワンタイムパスワードを用い、これらを組み合わせてユーザ認証を行う。
【０００３】
ユーザがパーソナルコンピュータなどを用いてインターネットを利用する際におけるワンタイムパスワードの生成には、従来より以下のような方法が採用されている。
（ａ）ワンタイムパスワード生成のための専用のハードウェア（認証トークン（Ｔｏｋｅｎ））をユーザに配布する方法。ユーザは、そのハードウェアを操作してワンタイムパスワードを生成する。
（ｂ）ワンタイムパスワード生成のためのソフトウェアをパーソナルコンピュータにインストールしておく方法。ユーザは、パーソナルコンピュータ上でそのソフトウェアを実行してワンタイムパスワードを生成する。
（ｃ）ウェブサーバ上に配置されたワンタイムパスワード生成モジュールにパーソナルコンピュータからアクセスし、ウェブサーバ上でワンタイムパスワードを生成して、それを

パーソナルコンピュータにダウンロードする方法。
【０００４】
上記従来の方法（ａ）ではハードウェアの配布が必要になる。また、（ｂ）ではソフトウェアのインストール作業の手間や管理などの点で煩雑な面がある。また、（ｃ）では、ハードウェアの配布やソフトウェアの場合の煩雑さに関する問題は解決するが、ワンタイムパスワードを生成するためにウェブサーバにアクセスする際には、毎回同じ固定パスワードを用いることとなる。このため、ワンタイムパスワードという一度限りしか有効でないパスワードを使用することによって守られているセキュリティという意義が、実質的には失われることになってしまう。
【０００５】
このような問題に鑑み、ハードウェアの配布等に伴う煩雑さを解消しながらセキュリティの向上を図るため、さまざまな技術が開発されている。
【０００６】
例えば、特許文献１には、ユーザからの依頼に基づきワンタイムパスワードを表示するためのＪＡＶＡ（登録商標）プログラムを作成し、作成した実行オブジェクトをプログラムダウンローダブルな携帯端末にダウンロードするワンタイムパスワード認証システムが記載されている。
【０００７】
また、特許文献２には、クライアント側から端末固有の情報を含む情報取得申請を行うと、サーバ側がユーザＩＤおよびワンタイムパスワード作成プログラムを含む情報取得情報を生成してクライアント側に提供する方法が記載されている。
【０００８】
【特許文献１】
特開２００２－１３２７２８号公報
【０００９】
【特許文献２】
特開２００１－６７３２０号公報
【００１０】
【発明が解決しようとする課題】
しかしながら、従来したような携帯端末に固有の実行オブジェクトをダウンロードする方式では、ユーザからの依頼に基づきユーザ固有のプログラムを作成し、更にその作成が完了したことをユーザに通知するという煩雑な手続が必要となるという問題があった。
【００１１】
また、ワンタイムパスワード生成プログラムの提供を受けるためにクライアント側から送信される情報取得申請を利用する従来の方法では、ネットワークを介して端末固有の情報が送信される場合、セキュリティを十分に確保できないという問題があった。更に、このような情報提供支援方法は、ワンタイムパスワードを用いた認証と、ワンタイムパスワードの配布とをともに情報提供サーバで行わなければならず、情報提供サーバの作業負担が大きいという問題があった。
【００１２】
本発明は、従来のワンタイムパスワード配布システムが有する上記問題点に鑑みてなされたものであり、その目的とするところは、プログラムモジュールの作成および通知に伴う管理の煩雑さや情報提供サーバの作業負担を解消するとともに、セキュリティ性を高めることの可能なワンタイムパスワード生成プログラムの配布サーバ、配布方法および配布プログラム、コンピュータ読み取り可能な記録媒体ならびにワンタイムパスワード生成プログラムの配布システムを提供することである。
【００１３】
【課題を解決するための手段】
このような目的を達成するために、請求項１に記載の発明は、携帯端末に対し、ユーザ識別子の入力を受けるステップと、前記入力を受けるステップにおいて入力されたユーザ識

別子に基づいて、ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成するステップと、前記生成するステップにおいて生成されたワンタイムパスワードを表示部に表示するステップとを実行させるワンタイムパスワード生成プログラムを配布するためのワンタイムパスワード生成プログラムの配布サーバであって、前記ワンタイムパスワード生成プログラムを記憶した記憶手段と、前記携帯端末から前記ワンタイムパスワード生成プログラムのダウンロードの要求情報を受信する受信手段と、前記受信手段による要求情報の受信に応じて前記記憶手段に記憶されたワンタイムパスワード生成プログラムを前記携帯端末にダウンロードするダウンロード手段とを備えたことを特徴とする。

【００１４】

また、請求項２に記載の発明は、請求項１に記載のワンタイムパスワード生成プログラムの配布サーバにおいて、前記ワンタイムパスワード生成プログラムは、前記携帯端末に対し、前記表示するステップにおける表示に基づいてユーザにより入力されたワンタイムパスワードを送信するステップを更に実行させることを特徴とする。

【００１５】

また、請求項３に記載の発明は、携帯端末に対し、ユーザ識別子の入力を受けるステップと、前記入力を受けるステップにおいて入力されたユーザ識別子に基づいて、ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成するステップと、前記生成するステップにおいて生成されたワンタイムパスワードを表示部に表示するステップとを実行させるワンタイムパスワード生成プログラムを記憶したコンピュータを用いて、前記記憶されたワンタイムパスワード生成プログラムを配布する方法であって、前記携帯端末から前記ワンタイムパスワード生成プログラムのダウンロードの要求情報を受信するステップと、前記受信するステップにおいて受信した要求情報に応じて前記記憶されたワンタイムパスワード生成プログラムを前記携帯端末にダウンロードするステップとを備えたことを特徴とする。

【００１６】

また、請求項４に記載の発明は、請求項３に記載のワンタイムパスワード生成プログラムの配布方法において、前記ダウンロードするステップは前記ワンタイムパスワード生成プログラムをバイト・コード形式でダウンロードすることを特徴とする。

【００１７】

また、請求項５に記載の発明は、請求項３に記載のワンタイムパスワード生成プログラムの配布方法において、前記ダウンロードするステップは前記ワンタイムパスワード生成プログラムを暗号化してダウンロードすることを特徴とする。

【００１８】

また、請求項６に記載の発明は、携帯端末に対し、ユーザ識別子の入力を受けるステップと、前記入力を受けるステップにおいて入力されたユーザ識別子に基づいて、ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成するステップと、前記生成するステップにおいて生成されたワンタイムパスワードを表示部に表示するステップとを実行させるワンタイムパスワード生成プログラムを記憶したコンピュータを用いて、前記記憶されたワンタイムパスワード生成プログラムを配布するためのワンタイムパスワード生成プログラムの配布プログラムであって、前記コンピュータに対し、前記携帯端末から前記ワンタイムパスワード生成プログラムのダウンロードの要求情報を受信するステップと、前記受信するステップにおいて受信した要求情報に応じて前記記憶された前記ワンタイムパスワード生成プログラムを前記携帯端末にダウンロードするステップとを実行させることを特徴とする。

【００１９】

また、請求項７に記載の発明は、請求項６に記載のワンタイムパスワード生成プログラムの配布プログラムにおいて、前記ダウンロードするステップは前記ワンタイムパスワード生成プログラムをバイト・コード形式でダウンロードすることを特徴とする。

【００２０】

また、請求項８に記載の発明は、請求項７に記載のワンタイムパスワード生成プログラム

の配布プログラムにおいて、前記ダウンロードするステップは前記ワンタイムパスワード生成プログラムを暗号化してダウンロードすることを特徴とする。

【００２１】

また、請求項９に記載の発明は、コンピュータ読み取り可能な記録媒体であって、請求項６ないし８のいずれかに記載のワンタイムパスワード生成プログラムの配布プログラムを記録したことを特徴とする。

【００２２】

また、請求項１０に記載の発明は、ワンタイムパスワード生成プログラムの配布システムであって、ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成する携帯端末であって、ユーザ識別子を入力する入力手段と、前記入力手段から入力されたユーザ識別子に基づいてワンタイムパスワードを生成する生成手段と、前記生成手段により生成されたワンタイムパスワードを表示する表示手段とを有する携帯端末と、請求項１または２に記載のワンタイムパスワード生成プログラムの配布サーバとを備えたことを特徴とする。

【００２３】

【発明の実施の形態】

以下、図面を参照し、本発明の実施の形態について詳細に説明する。

【００２４】

以下の説明では、インターネットに接続して情報の収集を行い、必要に応じてワンタイムパスワードの入力が要求されるコンピュータを「パーソナルコンピュータ」と称し、ワンタイムパスワードを生成するためのワンタイムパスワード生成モジュールを格納するコンピュータを「携帯端末」と称して、両者を区別して説明するが、本発明はこれに限定されない。

【００２５】

本発明にかかる配布システムは、図１に示すように、携帯端末１０と、ウェブサーバ３０と、認証サーバ２０と、業務サーバ６０と、パーソナルコンピュータ８０により構成されている。図１において、携帯端末１０は、携帯電話パケット網４０を介してインターネット５０に接続し、本発明にかかる配布システムの他の構成要素たるウェブサーバ３０および業務サーバ６０にアクセスすることができる。パーソナルコンピュータ８０は、携帯端末１０のユーザにより使用されるコンピュータであり、インターネット５０に接続されている。インターネット５０は、ＴＣＰ／ＩＰによる常時相互接続の他、ダイヤルアップ接続などによる一時的な接続、パソコン通信サービス、ＵＵＣＰなどのＴＣＰ／ＩＰ以外のプロトコルによる接続を含むネットワークである。

【００２６】

認証サーバ２０および業務サーバ６０は企業内ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）７０を介してインターネットに接続され、互いにデータを送受信できるように構成されている。業務サーバ６０は、ワンタイムパスワードをパーソナルコンピュータ８０から受信し、そのワンタイムパスワードを認証サーバ２０に送信し、ユーザ認証を依頼する。ここで、パーソナルコンピュータ８０から送信される情報は、携帯端末１０に表示されたワンタイムパスワードに基づいてユーザにより入力されたものである。

【００２７】

そして、業務サーバ６０は、認証サーバ２０から返された認証結果に基づいて、パーソナルコンピュータ８０からのアクセスを許可し、サービスを提供する。

【００２８】

本発明にかかる配布システムは、ユーザが携帯端末１０を用いてインターネット５０に接続し、ワンタイムパスワード生成モジュールを携帯端末１０上にダウンロードするためのシステムであり、上述のワンタイムパスワード認証システムを基調とする。このシステムでは、携帯端末１０がワンタイムパスワード生成モジュールの実行に基づき、ユーザ識別子の入力を受け、そのユーザ識別子に基づいてワンタイムパスワードを生成し、生成されたワンタイムパスワードを表示部に表示する。

【００２９】
すなわち、携帯端末１０を用いてネットワークに接続し、情報収集およびその際に必要とされるワンタイムパスワードの生成および送信を全て同一の携帯端末から行う場合であっても、同様に本発明を適用できる。この場合、ワンタイムパスワード生成プログラムは、ワンタイムパスワードの生成のみならず、携帯端末１０に対し、ユーザにより入力されたワンタイムパスワードを送信する処理も実行することになる。
【００３０】
なお、携帯端末１０は、ユーザの所有物または専有物であるが、パーソナルコンピュータ８０は、ユーザの所有物または専有物であるとは限らない。一のユーザが複数のパーソナルコンピュータを使用する場合があるとともに、一のパーソナルコンピュータを複数のユーザで共有する場合がある。
【００３１】
以下に、本発明にかかる配布システムの各構成要素たる携帯端末１０、認証サーバ２０およびウェブサーバ３０について詳述する。
【００３２】
（携帯端末１０）
まず、携帯端末１０について説明する。本発明にかかる配布システムにおける携帯端末１０は、ユーザが携帯することが可能であり、インターネット５０にアクセスして情報を送受する機能を有する端末である。このような携帯端末としては、図１に示したインターネット接続機能を有するものがある。なお、携帯電話などの無線通信手段を介してネットワークに接続可能なノート型パーソナルコンピュータやパームトップ型パーソナルコンピュータやナビゲーションシステムなども、広い意味でここでいう携帯端末に含まれる。
【００３３】
携帯端末１０の構成の一例を、図２を参照しながら説明する。携帯端末１０は、図２のブロック図に示すように、入力部１１と、通信部１２と、格納部１３と、モジュール実行部１４と、表示部１５とを含んで構成されている。
【００３４】
入力部１１は、数字キー（０、１、…、９など）や文字キー（ひらがな、片仮名、英文字など）などのキーや、ユーザが音声を入力するための音声入力部などを含む。ユーザはこれらのキーを組み合わせて電子メールを作成したり、音声入力部から音声による指示を入力することにより、ワンタイムパスワード生成モジュールの要求を行う。
【００３５】
また、ユーザはこれらのキーを組み合わせることにより、ワンタイムパスワード生成モジュールのダウンロード元のアドレス、「シード」と称されるワンタイムパスワード生成に利用される情報、あるいは「ＰＩＮ（Ｐｅｒｓｏｎａｌ　Ｉｄｅｎｔｉｆｉｃａｔｉｏｎ　Ｎｕｍｂｅｒ）」と称されるワンタイムパスワードの入力などを行うことができる。ここで、シードとは、ワンタイムパスワードを作り出すために必要な所定桁数のランダムな数字を時間とともに発生させるための元となるデータファイルで、ワンタイムパスワード生成モジュールに固有の値である。
【００３６】
なお、ダウンロード元のアドレスとして、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）を使用することができる。
【００３７】
また、ダウンロード元のアドレス、およびシードは、電話や、ウェブサーバ３０とは独立した端末から携帯端末１０に向けて送信される電子メール等の手段を使用してユーザに通知されるものとすることができる。
【００３８】
通信部１２は、携帯端末１０と図１に示した携帯電話パケット網４０との間の通信を行う。携帯端末１０のユーザは、通信部１２を介して、ワンタイムパスワード生成モジュールのダウンロードを行う。携帯端末の一般的な機能である電話機能や電子メール機能につい

ても、通信部１２を介して実現される。

【００３９】

モジュール格納部１３には、通信部１２を介してダウンロードされたワンタイムパスワード生成モジュールが格納される。ワンタイムパスワード生成モジュールは、一度限り有効なワンタイムパスワードを生成するためのモジュールである。ワンタイムパスワード生成モジュールは、一度ダウンロードして、モジュール格納部１３に格納しておくことにより、ワンタイムパスワードの生成に繰り返し使用することができる。なお、モジュール格納部１３は、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）により構成される。

【００４０】

モジュール実行部１４では、モジュール格納部１３に格納されたワンタイムパスワード生成モジュールを実行してワンタイムパスワードを生成する。ワンタイムパスワード生成モジュールは、後述するように、携帯端末１０においてバイト・コード形式でダウンロードされる。ここで、バイト・コードとは、ＪＡＶＡ（登録商標）言語で記述されたソースファイルをコンパイラを用いて変換した中間言語のコードをいう。

【００４１】

表示部１５は、モジュール実行部１４で生成されたワンタイムパスワードを表示する。携帯端末１０のユーザは、表示部１５に表示されたワンタイムパスワードを用いて本人認証を行うことができる。すなわち、携帯端末１０のユーザは、ワンタイムパスワード生成モジュールが格納された携帯端末１０を、ワンタイムパスワード生成のためのハードウェア（認証トークン（Ｔｏｋｅｎ））の代わりとして機能させることができる。

【００４２】

以上説明した携帯端末１０の構成は一例に過ぎない。特に、図２において、本実施の形態に直接関係のないその他の機能を遂行する構成要素については省略して説明しているが、当業者であれば、各種の変更例または修正例に想到し得ることは明らかである。

【００４３】

次いで、携帯端末１０における処理フローを、図３を参照しながら説明する。携帯端末１０のユーザが、パーソナルコンピュータを用いてインターネットに接続し、例えば、遠隔地にある他のコンピュータにアクセスして情報を取得する際に、ワンタイムパスワードが要求される場合がある。かかる場合に備えて、携帯端末１０のユーザは、予め、本発明にかかる配布システムを利用して、ワンタイムパスワードを生成するためのワンタイムパスワード生成モジュールを携帯端末１０にダウンロードし、格納しておく。かかる場合における携帯端末１０における処理フローを、図３を参照しながら説明する。

【００４４】

まず、ワンタイムパスワード生成モジュールのダウンロードを希望する携帯端末１０のユーザに対し、ダウンロード元、すなわちワンタイムパスワード生成モジュールが格納されているウェブサーバ３０のアドレスが、電話または電子メール等の手段により通知される。

【００４５】

携帯端末１０のユーザは、通知されたアドレスを指定することにより、ウェブサーバ３０にアクセスする（ステップＳ１０４）。携帯端末１０には、ワンタイムパスワード生成モジュールのダウンロードを受け付けるための表示画面が表示され（ステップＳ１０５）、ダウンロードを要求しない場合には、処理を終了する（ステップＳ１０６）。

【００４６】

図４は、携帯端末１０が、ウェブサーバ３０により管理されるウェブページをアクセスしたときの表示画面の一例を示すものである。ここで、表示画面上の操作により、ワンタイムパスワード生成モジュールのダウンロードを行うよう要求すると、ウェブサーバ３０より携帯端末１０に対し、ワンタイムパスワード生成モジュールがダウンロードされる（図３のステップＳ１０７）。ウェブサーバ３０では、ダウンロードが成功したかが確認され（ステップＳ１０８）、ダウンロードに失敗した場合には、ウェブサーバ３０よりその旨が通知される（ステップＳ１０９）。

【００４７】
なお、上記のワンタイムパスワード生成モジュールのダウンロード要求は一例に過ぎず、どのような手段を用いて行うようにしても良いが、携帯端末１０を用いて要求を行えるシステム構成とすることが好ましい。かかる観点から、電子メールもしくは電話によりワンタイムパスワード生成モジュールのダウンロード要求を行うものとしても良い。
【００４８】
以上のようにして、携帯端末１０はワンタイムパスワード生成モジュールを取得することができる。携帯端末１０のユーザはワンタイムパスワード生成モジュールを起動する。そして、電話または電子メール等の手段により通知されたシードを携帯端末１０に入力し（ステップＳ１０３）、ワンタイムパスワード生成モジュールの動作確認を行う（ステップＳ１１０）。ワンタイムパスワード生成モジュールの動作が確認できた後、携帯端末１０のユーザは、ワンタイムパスワード生成モジュールを使用して、ワンタイムパスワードを生成し、これをユーザ認証（本人認証）に用いることができる（ステップＳ１１３）。
【００４９】
以上説明した処理フローを経て、携帯端末１０のユーザは、ワンタイムパスワード生成モジュールを使用してワンタイムパスワードを生成し、これをユーザ認証（本人認証）に用いることができる。
【００５０】
なお、上述の携帯端末１０の機能は携帯端末本来の機能として予め携帯端末に組み込まれるようにしても良い。あるいは、携帯端末１０にオプション的にプログラムを組み込むことにより上述の機能を実現するようにしても良い。この場合、プログラムは、記録媒体に記録することにより、有体物の形で流通させることが可能である。
【００５１】
（ワンタイムパスワード生成モジュール）
上述の携帯端末１０上で稼働するワンタイムパスワード生成モジュールについて説明する。ワンタイムパスワード生成モジュールは携帯端末１０上で稼働するアプリケーション（ＪＡＶＡ（登録商標）アプレット）であり、上述のようにウェブサーバ３０より携帯端末１０にダウンロードされる（ステップＳ１０７）。そして、携帯端末１０に対し、ユーザ識別子の入力を受ける処理、入力されたユーザ識別子に基づいて、ネットワーク上でのユーザ認証に用いられるワンタイムパスワードを生成する処理、および生成されたワンタイムパスワードを表示部に表示する処理を実行させる。
【００５２】
かかるワンタイムパスワード生成モジュールは、このＪＡＶＡ（登録商標）アプレットはＪａｖａ（登録商標）言語により作成され、コンパイルされてウェブサーバ３０にバイト・コード形式で格納されている。
【００５３】
図５は、ワンタイムパスワード生成モジュールを起動した際の、携帯端末１０に表示されるシード情報入力画面を示している。ここで、入力部１１を操作して、表示画面上の入力欄５０２にシードを入力すると、オフラインでワンタイムパスワードを生成するプログラムが完成する。シードを入力する処理は、初期処理として一度だけ行う処理である。
【００５４】
図６は、ワンタイムパスワード生成モジュールを使用してワンタイムパスワードを生成した際の、携帯端末１０上の表示画面を示している。ここでは、ワンタイムパスワードＯＴＰとして、６桁の数字「２４２９０４」が表示されている。
【００５５】
（認証サーバ２０）
次いで、認証サーバ２０について説明する。認証サーバ２０はシードを予め格納しており、業務サーバ６０から送信されたパスワードと、予め格納されたシードとに基づいてユーザ認証を行う機能を有するサーバである。
【００５６】

認証サーバ２０によるワンタイムパスワード認証について説明する。ユーザはパーソナルコンピュータ８０を使用して業務サーバ６０にアクセスし、携帯端末１０上に表示されたワンタイムパスワードを見て、ワンタイムパスワードを入力する。業務サーバ６０は、パーソナルコンピュータ８０から受信したワンタイムパスワードを認証サーバ２０に送信し、認証を要求する。認証サーバ２０は、受信したワンタイムパスワードに基づいて、ユーザの認証を行う。ここで、ユーザが認証されなかった場合、認証サーバ２０と携帯端末１０の通信部１２との間で同期をとる場合がある。認証サーバ２０による認証の結果は、業務サーバ６０に通知される。このようにして、他の不正ユーザからのアクセスチェックが行われる。

【００５７】

なお、認証サーバ２０および業務サーバ６０の機能は、通常コンピュータにプログラムを組み込むことにより実行される。この場合、プログラムは、記録媒体に記録することにより、有体物の形で流通させることが可能である。なお、認証サーバ２０および業務サーバ６０は、専用のハードウェアとして構成される場合もある。本発明にかかる配布システムは以上のように構成されている。

【００５８】

（ウェブサーバ３０）

ウェブサーバ３０は、上述した携帯端末１０とインターネット上で接続されており、図４の一例で示したウェブページを管理することにより、携帯端末１０へのワンタイムパスワード生成モジュールのダウンロードを行うサーバである。ウェブサーバ３０は本発明のワンタイムパスワード生成プログラムの配布サーバとして機能する。

【００５９】

ウェブサーバ３０の構成の一例を、図７を参照しながら説明する。ウェブサーバ３０は、図７のブロック図に示すように、ワンタイムパスワード生成モジュールを予め記憶したモジュール記憶部３２と、携帯端末１０からワンタイムパスワード生成モジュールのダウンロードを要求する情報を受信する受信部３３と、ワンタイムパスワード生成モジュールを出力するモジュール出力部３４を含んで構成されている。

【００６０】

ウェブサーバ３０は、携帯端末１０からアクセス可能なウェブページの管理サーバである。モジュール記憶部３２に予め記憶されているワンタイムパスワード生成モジュールは全てのユーザに共通のものであり、ウェブページ上の操作により、ダウンロード作業を行うことができる。なお、モジュール記憶部３２にワンタイムパスワード生成モジュールを記憶させる方法としては、ＣＤ－ＲＯＭ等の記録媒体を使用して供給する方法や、ネットワークを介して外部からウェブサーバ３０に送信する方法等を使用することができる。

【００６１】

図４は、携帯端末１０上に表示されたウェブページの一例を示している。携帯端末１０のユーザは、ウェブページ上で、ワンタイムパスワード生成モジュールをダウンロードするか否かを選択することができる。

【００６２】

次いで、ウェブサーバ３０における処理フローを、図８を参照しながら説明する。ワンタイムパスワード生成モジュールを記憶しているウェブサーバ３０は、携帯端末１０のユーザからのアクセスを受けると（ステップＳ３０４）、ワンタイムパスワード生成モジュールのダウンロードを受け付けるための表示画面を携帯端末１０に表示させる。携帯端末１０からワンタイムパスワード生成モジュールのダウンロードが要求されない場合（ステップＳ３０５）には、処理を終了する（ステップＳ３０６）。

【００６３】

携帯端末１０からワンタイムパスワード生成モジュールのダウンロードが要求された場合、ウェブサーバ３０は、全てのユーザに共通のワンタイムパスワード生成モジュールをモジュール記憶部３２から読み出す。そして、読み出されたワンタイムパスワード生成モジュールをモジュール出力部３４から出力することで、携帯端末１０に対するダウンロード

を行う（ステップＳ３０７）。ワンタイムパスワード生成モジュールのダウンロードに失敗した場合（ステップＳ３０８）には、ウェブサーバ３０より携帯端末１０に対しその旨が通知される（ステップＳ３０９）。

【００６４】

なお、ワンタイムパスワード生成モジュールは、携帯端末１０においてインストール作業の必要がなく即座に実行可能な形式、例えばバイナリ形式で携帯端末１０に出力（ダウンロード）することが好ましい。これにより、インストール作業の手間やソフトウェアの管理の煩雑さを解消することができ、ユーザビリティが高い。また、ソースコード解析などのハッキングにも強いという利点がある。

【００６５】

また、ウェブサーバ３０が、携帯端末１０からのアクセスに対し、ワンタイムパスワード生成モジュールを該携帯端末に出力する際の通信は、例えばＳＳＬ（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔｓ　Ｌａｙｅｒ）暗号化通信などにより、暗号化されて行われることが好ましい。

【００６６】

以上説明した処理フローを経て、ウェブサーバ３０による携帯端末１０へのワンタイムパスワード生成モジュールのダウンロード作業が完了する（ステップＳ３１０）。

【００６７】

このようにして、ワンタイムパスワード生成プログラムを記憶しておき、携帯端末からワンタイムパスワード生成プログラムのダウンロードの要求情報を受信し、要求情報の受信に応じて、記憶されたワンタイムパスワード生成プログラムを携帯端末にダウンロードする処理が実現される。

【００６８】

なお、ウェブサーバ３０の機能は、通常コンピュータにプログラムを組み込むことにより実行される。この場合、プログラムは、記録媒体に記録することにより、有体物の形で流通させることが可能である。なお、ウェブサーバ３０は、専用のハードウェアとして構成される場合もある。本発明にかかる配布システムは以上のように構成されている。

【００６９】

次いで、本発明にかかる配布システムにかかるワンタイムパスワード生成モジュールの配布方法（以下、本配布方法という。）について、図９を参照しながら説明する。図１０は、本配布方法の全体的な流れを時系列的に示したものである。

【００７０】

図９に示したように、まず、携帯端末１０のユーザは、ウェブサーバ３０にアクセスし（ステップＳ４）、ウェブサーバ３０からワンタイムパスワード生成モジュールをダウンロードする（ステップＳ５）。図１０は、上記各ステップＳ４およびＳ５を時系列的に示したものである。

【００７１】

本実施形態にかかるワンタイムパスワード生成プログラムの配布方法は以上のとおりである。各ステップの詳細については、本配布システムの説明として上述したとおりであるので、ここでは重複説明を省略する。

【００７２】

以上、添付図面を参照しながら本発明にかかるワンタイムパスワード生成プログラムの配布サーバ、配布方法および配布プログラム、コンピュータ読み取り可能な記録媒体、ワンタイムパスワード生成プログラムの配布システム、ならびにその関連技術についての好適な実施形態について説明したが、本発明はかかる例に限定されない。当業者であれば、特許請求の範囲に記載された技術的思想の範疇内において各種の変更例または修正例に想到し得ることは明らかであり、それらについても当然に本発明の技術的範囲に属するものと了解される。

【００７３】

【発明の効果】

以上説明したように、本発明によれば、ソフトウェア管理の煩雑さや情報提供サーバの作業負担を解消できるとともに、セキュリティ性が高められたワンタイムパスワード生成プログラムの配布サーバ、配布方法および配布プログラム、コンピュータ読み取り可能な記録媒体ならびにワンタイムパスワード生成プログラムの配布システムが提供される。

【図面の簡単な説明】

【図１】本発明にかかるワンタイムパスワード生成モジュールの配布システムのシステム構成の一例を示すブロック図である。

【図２】本発明にかかる携帯端末の構成の一例を示すブロック図である。

【図３】本発明にかかる携帯端末における処理の一例を示すフローチャートである。

【図４】本発明にかかるウェブサーバが管理するウェブページの一例を示す図である。

【図５】本発明にかかるワンタイムパスワード生成モジュールを起動した際の、携帯端末上の表示画面の一例を示す図である。

【図６】本発明にかかるワンタイムパスワード生成モジュールを使用してワンタイムパスワードを生成した際の、携帯端末上の表示画面の一例を示す図である。

【図７】本発明にかかるウェブサーバの構成の一例を示すブロック図である。

【図８】本発明にかかるウェブサーバにおける処理の一例を示すフローチャートである。

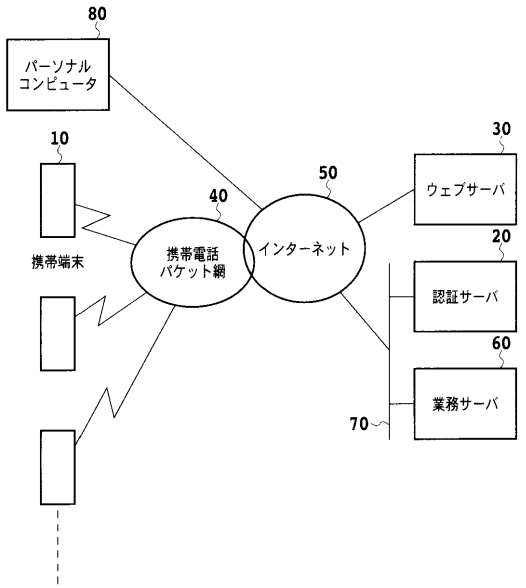
【図９】本発明にかかるワンタイムパスワード生成モジュールの配布方法の一例を概略的に示す図である。

【図１０】本発明にかかるワンタイムパスワード生成モジュールの配布方法を時系列的に示す通信シーケンス図である。

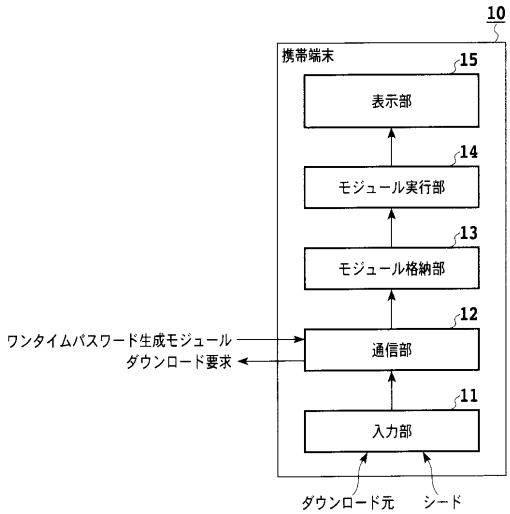
【符号の説明】

１０　携帯端末
１１　モジュール入力部
１２　通信部
１３　モジュール格納部
１４　モジュール実行部
１５　表示部
２０　認証サーバ
２１　受信部
２３　通知部
２４　データベース
３０　ウェブサーバ
３２　モジュール記憶部
３３　受信部
３４　モジュール出力部
ＯＴＰ　ワンタイムパスワード
４０　携帯電話パケット網
５０　インターネット
６０　業務サーバ
７０　企業内ＬＡＮ
８０　パーソナルコンピュータ

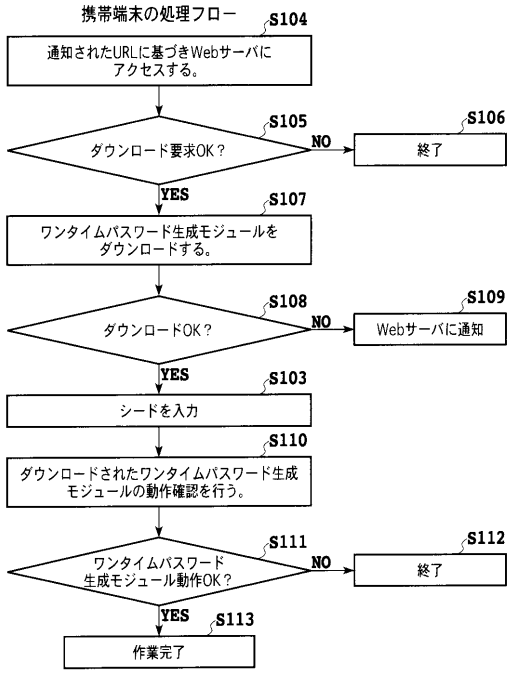
【図１】


80
パーソナル
コンピュータ
10
携帯端末
40
携帯電話
パケット網
50
インターネット
30
ウェブサーバ
20
認証サーバ
60
業務サーバ
70

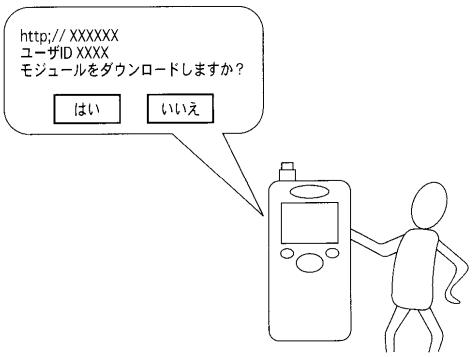
【図２】


10
携帯端末
15
表示部
14
モジュール実行部
13
モジュール格納部
12
通信部
11
入力部
ワンタイムパスワード生成モジュール
ダウンロード要求
ダウンロード元
シード

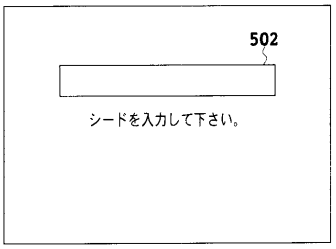
【図３】


携帯端末の処理フロー
S104
通知されたURLに基づきWebサーバに
アクセスする。
S105
ダウンロード要求OK？
NO
S106
終了
YES
S107
ワンタイムパスワード生成モジュールを
ダウンロードする。
S108
ダウンロードOK？
NO
S109
Webサーバに通知
YES
S103
シードを入力
S110
ダウンロードされたワンタイムパスワード生成
モジュールの動作確認を行う。
S111
ワンタイムパスワード
生成モジュール動作OK？
NO
S112
終了
YES
S113
作業完了

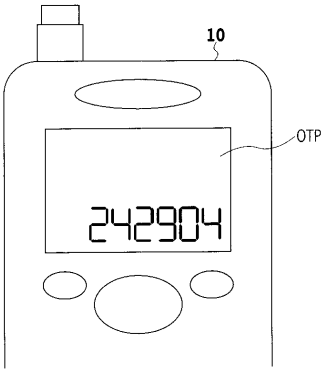
【図４】


http;// XXXXXX
ユーザID XXXX
モジュールをダウンロードしますか？
はい
いいえ

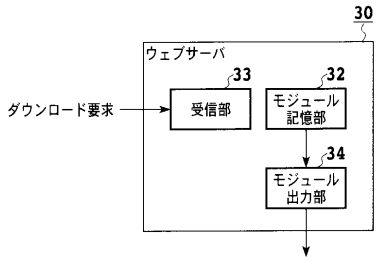
【図５】


502
シードを入力して下さい。

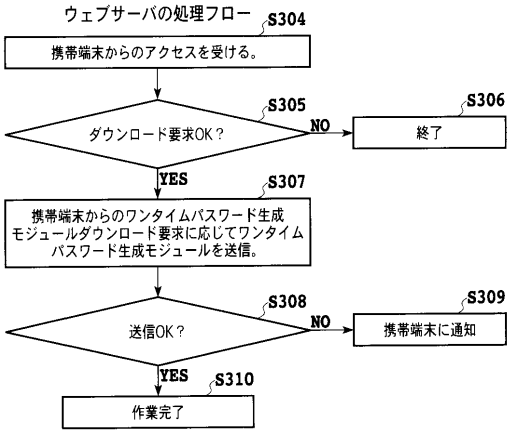
【図６】



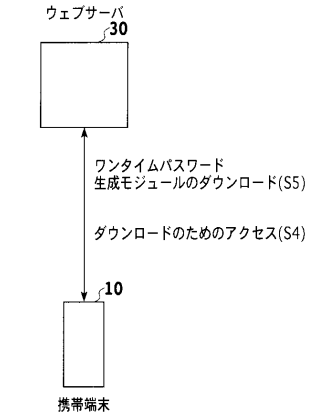
【図７】



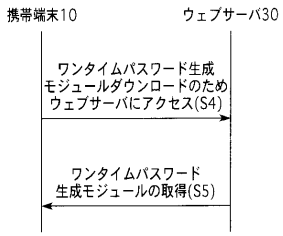
【図８】



【図９】



【図１０】



フロントページの続き

(72)発明者　中島　伸之
東京都千代田区丸の内１丁目３番１号　東京銀行協会ビルヂング１３階　アール・エス・エー・セキュリティ株式会社内

Ｆターム(参考) 5B076 BB06 FB01
5B085 AE03
5J104 AA07 KA02 KA04 KA06 KA21 NA05 NA27 PA01 PA07