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

特許第5164204号
(P5164204)

(45)発行日　平成25年3月21日(2013.3.21)　(24)登録日　平成24年12月28日(2012.12.28)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/20 131A
H04L 9/32 (2006.01)　　H04L 9/00 673D

請求項の数 15　(全 20 頁)

(21)出願番号　特願2008-75279(P2008-75279)
(22)出願日　平成20年3月24日(2008.3.24)
(65)公開番号　特開2009-230482(P2009-230482A)
(43)公開日　平成21年10月8日(2009.10.8)
審査請求日　平成23年2月8日(2011.2.8)

(73)特許権者　506301140
公立大学法人会津大学
福島県会津若松市一箕町大字鶴賀字上居合
９０番地
(74)代理人　100118094
弁理士　殿元　基城
(72)発明者　林　隆史
福島県会津若松市一箕町大字鶴賀字上居合
９０番地　公立大学法人会津大学内

審査官　市川　武宜

最終頁に続く

(54)【発明の名称】ワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置。

(57)【特許請求の範囲】
【請求項１】
ワンタイムパスワードを出力する情報通信装置と、該情報通信装置より前記ワンタイムパスワードを受信して前記情報通信装置の認証判断を行う認証判断装置とを備えるワンタイムパスワード認証システムであって、
前記情報通信装置は、
乱数情報を生成する乱数生成手段と、
時刻検出を行うための時刻検出手段と、
前記乱数生成手段により生成された乱数情報と、前記時刻検出手段により検出された時刻情報とに基づいて前記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手段と、
前記時刻検出手段による前記時刻情報の検出時に、前記乱数生成手段により生成された乱数情報を前記認証判断装置に出力する乱数情報出力手段と、
前記ワンタイムパスワード生成手段により生成されたワンタイムパスワードを前記認証判断装置に出力するワンタイムパスワード出力手段と
を有し、
前記認証判断装置は、
前記乱数情報および前記ワンタイムパスワードを受信する情報受信手段と、
前記情報受信手段により前記乱数情報を受信した時の時刻検出を行う受信時刻検出手段と、

該受信時刻検出手段により検出された時刻情報と前記情報受信手段により受信された乱数情報とに基づいて認証用ワンタイムパスワードを生成する認証用ワンタイムパスワード生成手段と、
該認証用ワンタイムパスワード生成手段により生成された認証用ワンタイムパスワードと、前記情報受信手段により受信されたワンタイムパスワードとを比較して前記情報通信装置に対する認証判断を行う認証判断手段と
を有することを特徴とするワンタイムパスワード認証システム。
【請求項２】
前記乱数生成手段は、物理的現象を利用して乱数情報を生成する物理乱数生成装置により構成されることを特徴とする請求項１に記載のワンタイムパスワード認証システム。
【請求項３】
前記情報通信装置は、前記乱数情報および前記ワンタイムパスワードの暗号化処理を行う暗号化手段を有し、
前記認証判断装置は、前記暗号化手段により暗号化された前記乱数情報および前記ワンタイムパスワードの復号化処理を行う復号化手段を有し、
前記乱数情報出力手段は、予め規定された暗号化キーを用いて前記暗号化手段により暗号化された乱数情報を前記認証判断装置に出力し、
前記ワンタイムパスワード出力手段は、前記乱数情報を暗号化キーとして用いて前記暗号化手段により暗号化されたワンタイムパスワードを前記認証判断装置に出力し、
前記復号化手段では、前記情報受信手段により受信された前記乱数情報を予め規定された暗号化キーを用いて復号化すると共に、前記情報受信手段により受信された前記ワンタイムパスワードを、前記乱数情報を暗号化キーとして用いて復号化すること
を特徴とする請求項１または請求項２に記載のワンタイムパスワード認証システム。
【請求項４】
前記時刻検出手段および前記受信時刻検出手段は、
時刻管理機能を備える内部時計手段と、
時刻情報を含む標準電波を受信する電波受信手段と、
前記電波受信手段により受信された標準電波に基づいて前記内部時計手段における時刻情報の補正を行う時刻補正手段と
を有することを特徴とする請求項１乃至請求項３のいずれか１項に記載のワンタイムパスワード認証システム。
【請求項５】
情報通信装置より出力されたワンタイムパスワードを、認証判断装置において受信して認証判断処理を行うためのワンタイムパスワード認証方法であって、
前記情報通信装置の乱数生成手段が乱数情報を生成する乱数生成ステップと、
前記情報通信装置の時刻検出手段が時刻検出を行う時刻検出ステップと、
前記乱数生成ステップにおいて生成された乱数情報と、前記時刻検出ステップにおいて検出された時刻情報とに基づいて、前記情報通信装置のワンタイムパスワード生成手段が前記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ステップと、
前記時刻検出ステップにおいて前記時刻情報を検出した時に、前記乱数生成ステップにおいて生成された乱数情報を、前記情報通信装置の乱数情報出力手段が、前記情報通信装置から前記認証判断装置に出力する乱数情報出力ステップと、
前記ワンタイムパスワード生成ステップにおいて生成されたワンタイムパスワードを、前記情報通信装置のワンタイムパスワード出力手段が、前記情報通信装置から前記認証判断装置に出力するワンタイムパスワード出力ステップと、
前記認証判断装置の情報受信手段が、前記乱数情報および前記ワンタイムパスワードを受信する情報受信ステップと、
前記情報受信ステップにおいて前記乱数情報を受信した時の時刻検出を、前記認証判断装置の受信時刻検出手段が行う受信時刻検出ステップと、
該受信時刻検出ステップにより検出された時刻情報と前記情報受信ステップにより受信

された乱数情報とに基づいて、前記認証判断装置の認証用ワンタイムパスワード生成手段が認証用ワンタイムパスワードを生成する認証用ワンタイムパスワード生成ステップと、
該認証用ワンタイムパスワード生成ステップにおいて生成された認証用ワンタイムパスワードと、前記情報受信ステップにおいて受信されたワンタイムパスワードとを比較して、前記認証判断装置の認証判断手段が、前記情報通信装置に対する認証判断を行う認証判断ステップと
を有することを特徴とするワンタイムパスワード認証方法。
【請求項６】
前記乱数生成ステップにおいて生成される乱数情報は、物理的現象を利用して乱数情報を生成する物理乱数生成装置を乱数生成手段として用いることにより生成されること
を特徴とする請求項５に記載のワンタイムパスワード認証方法。
【請求項７】
前記情報通信装置の暗号化手段が、予め規定された暗号化キーを用いて、前記乱数情報の暗号化を行う乱数情報暗号化ステップと、
前記暗号化手段が、前記乱数情報を暗号化キーとして用いて、前記ワンタイムパスワードの暗号化を行うワンタイムパスワード暗号化ステップと、
前記認証判断装置の復号化手段が、予め規定された暗号化キーを用いて、暗号化された前記乱数情報の復号化を行う乱数情報復号化ステップと、
前記復号化手段が前記乱数情報を暗号化キーとして用いて、前記ワンタイムパスワードの復号化を行うワンタイムパスワード復号化ステップと
を有し、
前記乱数情報出力ステップでは、前記乱数情報暗号化ステップにおいて暗号化された乱数情報を、前記情報通信装置の乱数情報出力手段が、前記情報通信装置から前記認証判断装置に出力し、
前記ワンタイムパスワード出力ステップでは、前記ワンタイムパスワード暗号化ステップにおいて暗号化されたワンタイムパスワードを、前記情報通信装置のワンタイムパスワード出力手段が、前記情報通信装置から前記認証判断装置に出力し、
前記乱数情報復号化ステップでは、前記復号化手段が、前記情報受信ステップにおいて受信された乱数情報の復号化処理を行い、
前記ワンタイムパスワード復号化ステップでは、前記復号化手段が、前記情報受信ステップにおいて受信されたワンタイムパスワードの復号化処理を行うこと
を特徴とする請求項５または請求項６に記載のワンタイムパスワード認証方法。
【請求項８】
認証判断処理を行うためのワンタイムパスワードを情報通信装置で生成して認証判断装置に出力するためのワンタイムパスワード生成プログラムであって、
前記情報通信装置のコンピュータに、
乱数情報を生成させる乱数生成機能と、
時刻検出を行う時刻検出機能と、
前記乱数生成機能により生成された乱数情報と、前記時刻検出機能により検出された時刻情報とに基づいて、前記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機能と、
前記時刻検出機能により前記時刻情報を検出した時に、前記乱数生成機能により生成された乱数情報を、前記情報通信装置から前記認証判断装置に出力する乱数情報出力機能と、
前記ワンタイムパスワード生成機能により生成されたワンタイムパスワードを、前記情報通信装置から前記認証判断装置に出力するワンタイムパスワード出力機能と
を実現させるためのワンタイムパスワード生成プログラム。
【請求項９】
前記乱数生成機能により生成される乱数情報は、物理的現象を利用して生成される乱数情報であることを特徴とする請求項８に記載のワンタイムパスワード生成プログラム。

【請求項１０】
前記情報通信装置のコンピュータに、
前記乱数情報を予め規定された暗号化キーを用いて暗号化する乱数情報暗号化機能と、
前記乱数情報を暗号化キーとして用いて前記ワンタイムパスワードの暗号化を行うワンタイムパスワード暗号化機能とを実現させ、
前記乱数情報出力機能において、前記乱数情報暗号化機能により暗号化された乱数情報を前記情報通信装置から前記認証判断装置に出力させ、
前記ワンタイムパスワード出力機能において、前記ワンタイムパスワード暗号化機能により暗号化されたワンタイムパスワードを、前記情報通信装置から前記認証判断装置に出力させる
ための請求項８または請求項９に記載のワンタイムパスワード生成プログラム。
【請求項１１】
情報通信装置より出力されたワンタイムパスワードを認証判断装置において受信して認証判断するためのワンタイムパスワード認証プログラムであって、
前記認証判断装置のコンピュータに、
前記情報通信装置より出力された乱数情報およびワンタイムパスワードを受信する情報受信機能と、
該情報受信機能により前記乱数情報を受信した時の時刻検出を行う受信時刻検出機能と、
該受信時刻検出機能により検出された時刻情報と前記情報受信機能により受信された乱数情報とに基づいて、認証用ワンタイムパスワードを生成する認証用ワンタイムパスワード生成機能と、
該認証用ワンタイムパスワード生成機能により生成された認証用ワンタイムパスワードと、前記情報受信機能により受信されたワンタイムパスワードとを比較して、前記情報通信装置に対する認証判断を行う認証判断機能と
を実現させるためのワンタイムパスワード認証プログラム。
【請求項１２】
前記認証判断装置のコンピュータに、
前記情報受信機能により受信された乱数情報が暗号化されていた場合に、暗号化された乱数情報を予め規定された暗号化キーを用いて復号化する乱数情報復号化機能と、
前記情報受信機能により受信されたワンタイムパスワードが暗号化されていた場合に、前記乱数情報を暗号化キーとして用いて前記ワンタイムパスワードの復号化を行うワンタイムパスワード復号化機能と
を実現させることを特徴とする請求項１１に記載のワンタイムパスワード認証プログラム。
【請求項１３】
認証判断装置において認証判断を行うための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装置であって、
乱数情報を生成する乱数生成手段と、
時刻検出を行う時刻検出手段と、
前記乱数生成手段により生成された乱数情報と、前記時刻検出手段により検出された時刻情報とに基づいて、前記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手段と、
前記時刻検出手段により前記時刻情報を検出した時に、前記乱数生成手段により生成された乱数情報を、前記認証判断装置に出力する乱数情報出力手段と、
前記ワンタイムパスワード生成手段により生成されたワンタイムパスワードを、前記認証判断装置に出力するワンタイムパスワード出力手段と
を有することを特徴とするワンタイムパスワード生成装置。

【請求項１４】

前記乱数生成手段は、物理的現象を利用して真性乱数情報を生成する物理乱数生成装置により構成されることを特徴とする請求項１３に記載のワンタイムパスワード生成装置。
【請求項１５】
前記時刻検出手段は、
時刻管理機能を備える内部時計手段と、
時刻情報を含む標準電波を受信する電波受信手段と、
前記電波受信手段により受信された標準電波に基づいて前記内部時計手段における時刻情報の補正を行う時刻補正手段と
を有することを特徴とする請求項１３または請求項１４に記載のワンタイムパスワード生成装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置に関し、より詳細には、情報通信装置により出力されたワンタイムパスワードを認証判断装置で受信して認証判断処理を行うワンタイムパスワード認証システム、ワンタイムパスワード認証方法等に関する。
【背景技術】
【０００２】
通信環境が発達した今日では、インターネットなどのオープンなネットワックを介して情報通信装置（クライアント装置）から所定のサーバ装置にアクセスすることによってネットショッピングを行ったり、所定の情報を取得したりすることが多くなっている。情報通信装置からサーバ装置にアクセスする場合、アクセスしたユーザ（情報通信装置）の認証を行うことによって、許諾を得ていないユーザ（情報通信装置）からのアクセスを制限することにより、セキュリティの確保を実現する方法が多く採用されている。
【０００３】
具体的には、ユーザを特定するためのＩＤ情報とパスワード情報とを予め設定し、情報通信装置からサーバ装置に対してＩＤ情報とパスワード情報とを送信することによって、ユーザが正当なアクセス権限を有するか否かの判断を行っている。
【０００４】
しかしながら、ＩＤ情報とパスワード情報を、インターネットなどのオープンなネットワークを介して送信すると、悪意を有する第三者にＩＤ情報およびパスワード情報が知られ得る可能性が生ずる。悪意を有する第三者にＩＤ情報およびパスワード情報が知られてしまった場合、第三者は取得したＩＤ情報およびパスワード情報を用いることによって正規ユーザのふりをしてサーバ装置にアクセスすることが可能となってしまい（いわゆる、なりすまし）、重要な情報を第三者に盗まれてしまうおそれがあった。
【０００５】
このため、パスワード情報を一定期間毎に変更することによって、同一のパスワード情報を用いてアクセス可能な期間を制限し、セキュリティの確保を図る方法も用いられている。しかしながら、頻繁にパスワード情報を変更すると、ユーザにおいてパスワード情報を管理するための負担が増大してしまうおそれが生ずるという問題があった。
【０００６】
このため、今日では、時刻情報（時間情報）とＩＤ情報とに基づいて一定期間（例えば１分間）だけ有効となるワンタイムパスワードを情報通信装置において生成し、ワンタイムパスワードに基づいてサーバ装置側で認証処理を行うシステム（いわゆるワンタイムパスワード認証システム）が考案されている（例えば、特許文献１参照）。
【０００７】
このワンタイムパスワード認証システムでは、情報通信装置とサーバ装置とに、時刻情報とＩＤ情報とに基づいてワンタイムパスワードを生成するための共通するアルゴリズム

が記録されている。このため、情報通信装置では、ＩＤ情報とサーバ装置から取得した時刻情報とに基づいてワンタイムパスワードを生成して、サーバ側にＩＤ情報とワンタイムパスワードとを送信する。一方で、サーバ装置では、時刻情報と情報通信装置のＩＤ情報とに基づいて、共通するアルゴリズムを用いて認証用のワンタイムパスワードを生成する。そして、サーバ装置では、生成された認証用のワンタイムパスワードと、情報通信装置より受信したワンタイムパスワードとを比較し、両方のパスワードが同じである場合には情報通信装置のアクセスを許可し、両方のパスワードが異なる場合には情報通信装置のアクセスを制限する判断を行う。

【０００８】

このように、ワンタイムパスワードは時刻情報に基づいて生成されるパスワードであるため、時刻情報が異なることによって全く異なったワンタイムパスワードが生成される。従って、従来のパスワードのように常に同じパスワードがオープンなネットワークを介して送信されることがなくなる。さらに、ワンタイムパスワードは一定期間（例えば、１分間）だけ有効なパスワードとして認証されるため、もし、悪意を有する第三者にワンタイムパスワードが盗まれた場合であっても、第三者がワンタイムパスワードを用いて不正に認証を得ようとする場合には、通常、パスワードの有効期限が過ぎて無効なパスワードとなってサーバ装置で認証されないため、セキュリティを高く確保することが可能となる。

【特許文献１】特開２００５－５０２９２号公報

【発明の開示】

【発明が解決しようとする課題】

【０００９】

しかしながら、時刻情報およびユーザＩＤは、ネットワークを介して情報通信装置およびサーバ装置の間に送受信される情報であるため、悪意を有する第三者知られてしまうおそれがある。また、ワンタイムパスワードも同様にネットワークを介して送受信される情報であるため、第三者に知られてしまうおそれがある。このため、情報通信装置およびサーバ装置においてワンタイムパスワードを生成するアルゴリズムが知られていない場合であっても、生成されたワンタイムパスワードの情報と、このワンタイムパスワードの情報を生成するための種となる時刻情報およびＩＤ情報とが知られてしまうと、アルゴリズムが解析されてしまうおそれがあった。

【００１０】

本発明は上記問題に鑑みてなされたものであり、時刻情報を送信することなくワンタイムパスワードの認証処理を行うことによりセキュリティの向上を図ることが可能なワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置を提供することを課題とする。

【課題を解決するための手段】

【００１１】

上記課題を解決するために、本発明に係るワンタイムパスワード認証システムは、ワンタイムパスワードを出力する情報通信装置と、該情報通信装置より前記ワンタイムパスワードを受信して前記情報通信装置の認証判断を行う認証判断装置とを備えるワンタイムパスワード認証システムであって、前記情報通信装置は、乱数情報を生成する乱数生成手段と、時刻検出を行うための時刻検出手段と、前記乱数生成手段により生成された乱数情報と、前記時刻検出手段により検出された時刻情報とに基づいて前記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手段と、前記時刻検出手段による前記時刻情報の検出時に、前記乱数生成手段により生成された乱数情報を前記認証判断装置に出力する乱数情報出力手段と、前記ワンタイムパスワード生成手段により生成されたワンタイムパスワードを前記認証判断装置に出力するワンタイムパスワード出力手段とを有し、前記認証判断装置は、前記乱数情報および前記ワンタイムパスワードを受信する情報受信手段と、前記情報受信手段により前記乱数情報を受信した時の時刻検出を行う受信時刻検出手段と、該受信時刻検出手段により検出された時刻情報と前記情報受信手段により受信された乱数

情報とに基づいて認証用ワンタイムパスワードを生成する認証用ワンタイムパスワード生成手段と、該認証用ワンタイムパスワード生成手段により生成された認証用ワンタイムパスワードと、前記情報受信手段により受信されたワンタイムパスワードとを比較して前記情報通信装置に対する認証判断を行う認証判断手段とを有することを特徴とする。

【００１２】

また、本発明に係るワンタイムパスワード認証方法は、情報通信装置より出力されたワンタイムパスワードを、認証判断装置において受信して認証判断処理を行うためのワンタイムパスワード認証方法であって、前記情報通信装置の乱数生成手段が乱数情報を生成する乱数生成ステップと、前記情報通信装置の時刻検出手段が時刻検出を行う時刻検出ステップと、前記乱数生成ステップにおいて生成された乱数情報と、前記時刻検出ステップにおいて検出された時刻情報とに基づいて、前記情報通信装置のワンタイムパスワード生成手段が前記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ステップと、前記時刻検出ステップにおいて前記時刻情報を検出した時に、前記乱数生成ステップにおいて生成された乱数情報を、前記情報通信装置の乱数情報出力手段が、前記情報通信装置から前記認証判断装置に出力する乱数情報出力ステップと、前記ワンタイムパスワード生成ステップにおいて生成されたワンタイムパスワードを、前記情報通信装置のワンタイムパスワード出力手段が、前記情報通信装置から前記認証判断装置に出力するワンタイムパスワード出力ステップと、前記認証判断装置の情報受信手段が、前記乱数情報および前記ワンタイムパスワードを受信する情報受信ステップと、前記情報受信ステップにおいて前記乱数情報を受信した時の時刻検出を、前記認証判断装置の受信時刻検出手段が行う受信時刻検出ステップと、該受信時刻検出ステップにより検出された時刻情報と前記情報受信ステップにより受信された乱数情報とに基づいて、前記認証判断装置の認証用ワンタイムパスワード生成手段が認証用ワンタイムパスワードを生成する認証用ワンタイムパスワード生成ステップと、該認証用ワンタイムパスワード生成ステップにおいて生成された認証用ワンタイムパスワードと、前記情報受信ステップにおいて受信されたワンタイムパスワードとを比較して、前記認証判断装置の認証判断手段が、前記情報通信装置に対する認証判断を行う認証判断ステップとを有することを特徴とする。

【００１３】

さらに、本発明に係るワンタイムパスワード生成プログラムは、認証判断処理を行うためのワンタイムパスワードを情報通信装置で生成して認証判断装置に出力するためのワンタイムパスワード生成プログラムであって、前記情報通信装置のコンピュータに、時刻検出を行う時刻検出機能と、前記乱数生成手段により生成された乱数情報と、前記時刻検出機能により検出された時刻情報とに基づいて、前記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機能と、前記時刻検出機能により前記時刻情報を検出した時に、前記乱数生成手段により生成された乱数情報を前記情報通信装置から前記認証判断装置に出力する乱数情報出力機能と、前記ワンタイムパスワード生成機能により生成されたワンタイムパスワードを、前記情報通信装置から前記認証判断装置に出力するワンタイムパスワード出力機能とを実現させるためのプログラムであることを特徴とする。

【００１４】

また、本発明に係るワンタイムパスワード認証プログラムは、情報通信装置より出力されたワンタイムパスワードを認証判断装置において受信して認証判断するためのワンタイムパスワード認証プログラムであって、前記認証判断装置のコンピュータに、前記情報通信装置より出力された乱数情報およびワンタイムパスワードを受信する情報受信機能と、該情報受信機能により前記乱数情報を受信した時の時刻検出を行う受信時刻検出機能と、該受信時刻検出機能により検出された時刻情報と前記情報受信機能により受信された乱数情報とに基づいて、認証用ワンタイムパスワードを生成する認証用ワンタイムパスワード生成機能と、該認証用ワンタイムパスワード生成機能により生成された認証用ワンタイムパスワードと、前記情報受信機能により受信されたワンタイムパスワードとを比較して、前記情報通信装置に対する認証判断を行う認証判断機能とを実現させるためのプログラムであることを特徴とする。

【００１５】
さらに、本発明に係るワンタイムパスワード生成装置は、認証判断装置において認証判断を行うための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装置であって、乱数情報を生成する乱数生成手段と、時刻検出を行うための時刻検出手段と、前記乱数生成手段により生成された乱数情報と、前記時刻検出手段により検出された時刻情報とに基づいて前記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手段とを有することを特徴とする。
【００１６】
このように、本発明に係るワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置では、認証処理に用いられるワンタイムパスワードが、毎回異なる値となる乱数情報と、常に変化する時刻情報とに基づいて生成される。このため、従来のように一定の情報（例えば、ＩＤ情報）と時刻情報とによりワンタイムパスワードを生成する場合よりも、ワンタイムパスワードの生成パターンが増大し、ワンタイムパスワードの解析がより難しくなり、安全性の向上を図ることが可能となる。
【００１７】
また、本発明に係るワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置では、ワンタイムパスワードの生成に必要とされる時刻情報がネットワークを介して送受信されることがない。このため、悪意のある第三者は、時刻情報を取得することが困難となり、容易にワンタイムパスワードを生成・解析することができなくなる。
【００１８】
さらに、上述した乱数生成手段は、物理的現象を利用して乱数情報を生成する物理乱数生成装置により構成されるものであってもよい。従って、乱数生成手段を物理的現象を利用して乱数情報を生成する物理乱数生成装置により構成することにより、生成される乱数情報は、物理的現象を利用して生成される真性の乱数情報となる。
【００１９】
このようにして本発明に係るワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラムおよびワンタイムパスワード生成装置において、物理的現象を利用して生成された乱数情報が用いられる場合には、プログラムなどに基づいて生成される乱数情報のように乱数情報の生成アルゴリズムが解析されてしまうおそれや、プログラムの不具合により不適切な乱数情報が生成されてしまうおそれがなくなるという利点がある。また、物理的現象を利用して生成される乱数であるため、乱数生成のアルゴリズムを解析することが困難となる。このように全くランダムに生成される乱数情報を用いてワンタイムパスワードが生成されるため、ワンタイムパスワードの偽造等を行うことが困難となり、結果として、ワンタイムパスワード認証システムの認証精度を向上させることが可能となる。
【００２０】
また、上述したワンタイムパスワード認証システムは、前記情報通信装置が、前記乱数情報および前記ワンタイムパスワードの暗号化処理を行う暗号化手段を有し、前記認証判断装置は、前記暗号化手段により暗号化された前記乱数情報および前記ワンタイムパスワードの復号化処理を行う復号化手段を有し、前記乱数情報出力手段は、予め規定された暗号化キーを用いて前記暗号化手段により暗号化された乱数情報を前記認証判断装置に出力し、前記ワンタイムパスワード出力手段は、前記乱数情報を暗号化キーとして用いて前記暗号化手段により暗号化されたワンタイムパスワードを前記認証判断装置に出力し、前記復号化手段では、前記情報受信手段により受信された前記乱数情報を予め規定された暗号化キーを用いて復号化すると共に、前記情報受信手段により受信された前記ワンタイムパスワードを、前記乱数情報を暗号化キーとして用いて復号化するものであってもよい。
【００２１】

また、上述したワンタイムパスワード認証方法は、前記情報通信装置の暗号化手段が、予め規定された暗号化キーを用いて、前記乱数情報の暗号化を行う乱数情報暗号化ステップと、前記暗号化手段が、前記乱数情報を暗号化キーとして用いて、前記ワンタイムパスワードの暗号化を行うワンタイムパスワード暗号化ステップと、前記認証判断装置の復号化手段が、予め規定された暗号化キーを用いて、暗号化された前記乱数情報の復号化を行う乱数情報復号化ステップと、前記復号化手段が前記乱数情報を暗号化キーとして用いて、前記ワンタイムパスワードの復号化を行うワンタイムパスワード復号化ステップとを有し、前記乱数情報出力ステップでは、前記乱数情報暗号化ステップにおいて暗号化された乱数情報を、前記情報通信装置の乱数情報出力手段が前記情報通信装置から前記認証判断装置に出力し、前記ワンタイムパスワード出力ステップでは、前記ワンタイムパスワード暗号化ステップにおいて暗号化されたワンタイムパスワードを、前記情報通信装置のワンタイムパスワード出力手段が、前記情報通信装置から前記認証判断装置に出力し、前記乱数情報復号化ステップでは、前記復号化手段が前記情報受信ステップにおいて受信された乱数情報の復号化処理を行い、前記ワンタイムパスワード復号化ステップでは、前記復号化手段が前記情報受信ステップにおいて受信されたワンタイムパスワードの復号化処理を行うものであってもよい。

【００２２】

さらに、上述したワンタイムパスワード生成プログラムは、前記情報通信装置のコンピュータに、前記乱数情報を予め規定された暗号化キーを用いて暗号化する乱数情報暗号化機能と、前記乱数情報を暗号化キーとして用いて前記ワンタイムパスワードの暗号化を行うワンタイムパスワード暗号化機能と実現させ、前記乱数情報出力機能において、前記乱数情報暗号化機能により暗号化された乱数情報を、前記情報通信装置から前記認証判断装置に出力させ、前記ワンタイムパスワード出力機能において、前記ワンタイムパスワード暗号化機能により暗号化されたワンタイムパスワードを、前記情報通信装置から前記認証判断装置に出力させるためのプログラムであってもよい。

【００２３】

また、上述したワンタイムパスワード認証プログラムは、前記認証判断装置のコンピュータに、前記情報受信機能により受信された乱数情報が暗号化されていた場合に、暗号化された乱数情報を予め規定された暗号化キーを用いて復号化する乱数情報復号化機能と、前記情報受信機能により受信されたワンタイムパスワードが暗号化されていた場合に、前記乱数情報を暗号化キーとして用いて前記ワンタイムパスワードの復号化を行うワンタイムパスワード復号化機能とを実現させるためのプログラムであってもよい。

【００２４】

このように、本発明に係るワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラムおよびワンタイムパスワード認証プログラムでは、情報通信装置とサーバ装置との間で送受信される乱数情報およびワンタイムパスワードの暗号化処理が行われるので、第三者がこれらの情報を受信しても、容易に中身を判断することができない。このため、情報通信装置とサーバ装置との認証処理に必要な情報が第三者に容易に知られてしまうことを防止することができ、高いセキュリティを確保することが可能となる。

【００２５】

特に、ワンタイムパスワードは、乱数情報を暗号化キーとして用いて暗号化される。このため、ワンタイムパスワードの暗号化を行う度に、暗号化キーの内容が変更されることになり、安全の確保を図ることが容易となる。

【００２６】

さらに、暗号化キーとして用いられる乱数情報は物理的現象を利用して生成される乱数情報を用いることが可能である。このように物理的現象を利用して生成された乱数情報を暗号化キーに用いることによって、プログラムなどに基づいて生成される乱数情報のように、乱数情報の生成アルゴリズムが解析されてしまうおそれや、プログラムの不具合により不適切な乱数情報が生成されてしまうおそれがない。このため、暗号化キー自体のセキ

ュリティを高めることができ、容易にワンタイムパスワードの復号化が行われてしまうことを防止することができる。

【００２７】

また、本発明に係るワンタイムパスワード認証システムでは、前記時刻検出手段および前記受信時刻検出手段が、時刻管理機能を備える内部時計手段と、時刻情報を含む標準電波を受信する電波受信手段と、前記電波受信手段により受信された標準電波に基づいて前記内部時計手段における時刻情報の補正を行う時刻補正手段とを有するものであってもよい。

【００２８】

また、本発明に係るワンタイムパスワード生成装置では、前記時刻検出手段が、時刻管理機能を備える内部時計手段と、時刻情報を含む標準電波を受信する電波受信手段と、前記電波受信手段により受信された標準電波に基づいて前記内部時計手段における時刻情報の補正を行う時刻補正手段とを有するものであってもよい。

【００２９】

このように、本発明に係るワンタイムパスワード認証システムおよびワンタイムパスワード生成装置では、内部時計手段と電波受信手段とが設けられており、電波受信手段において受信された標準電波に基づいて内部時計手段の時刻が修正されるため、情報通信装置およびサーバ装置の内部時計手段が、常に正確な時刻を示すことになる。このため、時刻情報を情報通信装置とサーバ装置との間で送受信しなくても、情報通信装置とサーバ装置との時刻を同期させることが可能なり、ワンタイムパスワードおよび認証用ワンタイムパスワードの生成に不可欠な時刻情報のズレを低減させることが可能となる。

【発明の効果】

【００３０】

本発明に係るワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置では、認証処理に用いられるワンタイムパスワードが、毎回異なる値となる乱数情報と、常に変化する時刻情報とに基づいて生成される。このため、従来のように一定の情報（一度決められると変わらない情報）と時刻情報とによりワンタイムパスワードを生成する場合よりも、ワンタイムパスワードの生成パターンが増大し、ワンタイムパスワードの解析がより難しくなり、安全性の向上を図ることが可能となる。

【００３１】

また、本発明に係るワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置では、ワンタイムパスワードの生成に必要とされる時刻情報がネットワークを介して送受信されることがないため、悪意のある第三者は、時刻情報を取得することが困難となり、容易にワンタイムパスワードを生成・解析することができなくなる。

【発明を実施するための最良の形態】

【００３２】

以下、本発明に係るワンタイムパスワード認証システムについて、図面を用いて詳細に説明する。図１は、本発明に係るワンタイムパスワード認証システムを示した概略構成を示した図ある。

【００３３】

ワンタイムパスワード認証システム１は、サーバ装置（認証判断装置）２と情報通信装置３とを有している。サーバ装置２および情報通信装置３は、ネットワーク４を介して接続されている。このネットワーク４は、例えばインターネットなどの広く公に公開されネットワークであってもよく、また、ＬＡＮ（Local Area Network）のように限定されたエリア内において構築される閉ざされたネットワークであってもよい。なお、図１には、便宜上、サーバ装置２と情報通信装置３とが１台ずつしか示していないが、サーバ装置２および情報通信装置３の設置数は図１に示される１台ずつに限定されるものではなく、それ

ぞれ２台以上で構成されるものであってもよい。

【００３４】

ワンタイムパスワード認証システム１は、サーバ装置２において情報通信装置３のアクセスの認否を判断するための認証処理を行うシステムである。サーバ装置２では、情報通信装置３のＩＤ情報、乱数情報およびワンタイムパスワードを取得することによって、アクセスを希望する情報通信装置３が正当な権限を有しているか否かを判断し、正当な権限を有していると判断した場合には、情報通信装置３からのアクセスを許可する。一方で、正当な権限を有していないと判断した場合には、情報通信装置３からのアクセスを禁止（拒否）する。

【００３５】

図２は、情報通信装置３の概略構成を示している。

【００３６】

情報通信装置３は、通信部（乱数情報出力手段、ワンタイムパスワード出力手段）６とパスワード生成部７とにより概略構成されている。なお、本実施の形態に示す情報通信装置３では、通信部６とパスワード生成部７とが一体に形成される場合について説明を行うが、通信部６とパスワード生成部７とは必ずしも一体に形成されている必要はなく、別体に形成されているものであってもよい。

【００３７】

通信部６は、ユーザのＩＤ情報、次述する物理乱数生成部１２により生成された乱数情報、パスワード生成部７により生成されたワンタイムパスワードを、サーバ装置２に出力（送信）する機能を有している。通信部６は、例えば、ネットワークカード（ＮＩＣ：Network Interface Card）等が該当し、情報通信装置３をネットワーク４に接続させる役割を有している。なお、図２では、便宜上、情報通信装置３に内蔵されるネットワークカードを通信部６として記載しているが、通信部６より延設されるネットワークケーブルに対してモデムやメディアコンバータ等が接続される場合には、通信部６にモデム等が含まれることになる。

【００３８】

また、通信部６がパスワード生成部７と別体に形成されている場合には、通信部６としてネットワーク４に接続することが可能な装置、例えば、携帯電話端末（通信機能を有するＰＤＡ（Personal Digital Assistant）などを含む）などを用いることが可能となる。この場合には、パスワード生成部７と携帯電話端末とを専用のケーブルで接続することによって、ＩＤ情報、乱数情報、ワンタイムパスワードを、携帯電話端末を介してサーバ装置２に出力することが可能になる。

【００３９】

パスワード生成部７は、制御部（時刻検出手段、時刻補正手段、ワンタイムパスワード生成手段、暗号化手段）１０と、内部時計部（時刻検出手段、内部時計手段）１１と、物理乱数生成部（乱数生成手段）１２と、電波受信部（時刻検出手段、電波受信手段）１３とを有している。また、パスワード生成部７の制御部１０には、ディスプレイ１５とキーボード１６とマウス１７とが接続されている。

【００４０】

制御部１０は、パスワード生成部７の制御部１０における一連の処理、具体的には、乱数情報取得処理、時刻情報取得処理、内部時計修正処理、ワンタイムパスワード生成処理、暗号化処理などの処理を行う役割を有している。また、キーボード１６およびマウス１７により入力された情報を取得すると共に、必要な情報をディスプレイ１５に出力する機能を有している。

【００４１】

制御部１０は、ＣＰＵ（Central Processing Unit）２０と、ＲＯＭ（Read Only Memory）２１と、ＲＡＭ（Random Access Memory）２２とを有している。

【００４２】

ＣＰＵ２０は、上述した処理における様々な演算・制御処理を実行する役割を有してい

る。ＲＯＭ２１は、上述した処理を行うためのプログラムや必要な情報、例えば、後述するワンタイムパスワードを生成するためのアルゴリズムプログラム、後述する乱数情報やワンタイムパスワードなどを暗号化するための暗号化プログラムおよび予め規定される暗号化キーなどが記録されている。

【００４３】

ＣＰＵ２０（制御部１０）は、ＲＯＭ２１に記録されるこれらのプログラムに従って乱数情報取得処理を行い、時刻情報取得処理を行い、内部時計修正処理を行い、ワンタイムパスワード生成処理を行い、暗号化処理を行う。このため、ＣＰＵ２０は、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手段としての機能を備えており、また、乱数情報、ＩＤ情報およびワンタイムパスワードの暗号化を行うための暗号化手段としての機能を備えている。

【００４４】

なお、後述するサーバ装置２のＲＯＭ３９（図３参照）にも、ＲＯＭ２１に記録される予め規定された暗号化キーと同一の暗号化キーが記録されている。このため、情報通信装置３において予め規定された暗号化キーを用いて暗号化された情報は、同一の暗号化キーを用いることにより、サーバ装置２で復号化することが可能となっている。

【００４５】

また、ＲＯＭ２１に記録されるアルゴリズムプログラムは、サーバ装置２において認証用ワンタイムパスワードを生成するためのアルゴリズムプログラムと共通するアルゴリズムによって構築されている。このため、後述するように、ＣＰＵ２０が、乱数情報および時刻情報に基づいて生成したワンタイムパスワードと一致するパスワードを、サーバ装置２のＣＰＵ３８において生成することが可能となっている。

【００４６】

ＲＡＭ２２は、ＣＰＵ２０において行われる処理のワークエリア等として用いられる記録手段である。

【００４７】

なお、ディスプレイ１５は、一般的な液晶ディスプレイやＣＲＴディスプレイ（ブラウン管ディスプレイ）が該当し、処理の内容等をユーザに視認可能に表示させる機能を有している。また、キーボード１６およびマウス１７は、ユーザが情報通信装置３の処理に必要な操作を行うための入力手段であり、マウス１７によってディスプレイ１５に表示されるカーソル等を操作し、キーボード１６によって文字等の入力を行うことが可能となっている。ユーザがサーバ装置２に対するアクセス認証を試みる場合、ユーザは、キーボード１６を介してユーザのＩＤ情報を入力する必要が生ずる。

【００４８】

内部時計部１１は、水晶振動子により構成されており、この水晶振動子の振動に基づいて情報通信装置３における時間管理が行われる。ここで、内部時計部１１における時刻精度はこの水晶振動子により維持されることとなるが、水晶振動子は温度変化などにより振動周期にズレが生じるおそれがある。このため、内部時計部１１における時刻精度を確保するため、一定期間毎に電波受信部１３を介して正確な時間を取得して内部時計部１１の時刻補正を行っている。

【００４９】

電波受信部１３は、標準電波を受信する機能を有している。ここで標準電波とは、標準周波数報時電波とも呼ばれ、時刻と周波数の国家標準または国際標準として、政府や国際機関が放送している電波のことを意味している。ＣＰＵ２０では、送信局から送られてくる標準電波を電波受信部１３で一定時間ごとに読み取り、読み取られた標準電波に基づいて内部時計部１１の時刻の修正を行っている。このため、内部時計部１１では、電波受信部１３において電波が正常に受信できる環境であれば、ユーザが時刻合わせなどを手動で行うことなく、秒単位で正確な時刻を維持することができる。このように、制御部１０のＣＰＵ２０が、電波受信部１３において受信された標準電波に基づいて内部時計部１１の時刻を補正するので、制御部１０は、時刻補正手段としての機能を有している。

【００５０】
物理乱数生成部１２は、プログラムなどに基づくアルゴリズムではなく、物理的現象に基づいて、乱数情報となる乱数値を生成させる機能を有している。
【００５１】
今日では、ソフトウェアプログラムにより乱数を生成させるためのアルゴリズムを構築し、ソフトウェア処理により乱数値を生成させる方法が多く用いられている。しかしながら、ソフトウェア処理による乱数値の生成では、アルゴリズムの解読により乱数値の生成パターンを解読されたり、プログラム構築に伴う処理の不具合などが発生するおそれがある。本実施の形態に係るパスワード生成部７では、このようなソフトウェア処理による乱数値の生成ではなく、物理的な装置を用いて真性乱数値の生成を行う。
【００５２】
物理乱数生成部１２は、自然界の不規則性を利用することによって、自然界のランダムな現象に基づいた真性乱数値を生成させる装置である。自然界のランダムな現象に基づく乱数値の生成方法としては、例えば、半導体素子内部の熱電子のランダムな信号を用いる方法や、白色雑音（周波数に依存せず、全周波数成分を均等な強さで含んでいる雑音）を乱数源に用いる方法などが一般的である。このような自然界のランダムな現象に基づく物理的な乱数値の生成により、第三者に乱数値の生成パターンが解読されてしまう危険性を回避することができ、高いセキュリティを確保することが可能となる。このような物理乱数生成装置を物理乱数生成部１２に用いることにより、アメリカ政府機関における暗号モジュールの標準規格であるＦＩＳＰ１４０－２相当の乱数品位を確保することが可能となる。
【００５３】
次にサーバ装置２の構成について説明する。
【００５４】
図３は、サーバ装置の概略構成を示している。サーバ装置２は、情報通信装置３より受信した乱数情報、ワンタイムパスワード、ＩＤ情報に基づいて、情報通信装置３によるアクセスを許可するか否かの認証を行う装置である。サーバ装置２は、サーバ制御部（受信時刻検出手段、時刻補正手段、認証用ワンタイムパスワード生成手段、認証判断手段、復号化手段）３０と、データ記録部３１と、情報通信部（情報受信手段）３３と、内部時計部（受信時刻検出手段、内部時計手段）３４と、電波受信部（受信時刻検出手段、電波受信手段）３５とを有している。
【００５５】
サーバ制御部３０は、サーバ用のＣＰＵ３８と、サーバ用のＲＯＭ３９と、サーバ用のＲＡＭ４０とを有している。
【００５６】
ＣＰＵ３８は、サーバ装置２における一連の処理、具体的には、乱数情報を受信した時刻を内部時計部３４に基づいて検出取得する受信時刻検出処理や、受信した乱数情報に基づいて認証用ワンタイムパスワードを生成する認証用ワンタイムパスワード生成処理や、生成された認証用ワンタイムパスワードと情報通信装置３より受信したワンタイムパスワードとに基づいてアクセスの認証判断を行う認証判断処理や、暗号化されたワンタイムパスワードなどの復号化処理などを行う役割を有している。このため、ＣＰＵ３８（サーバ制御部３０）は、本発明に係る受信時刻検出手段、認証用ワンタイムパスワード生成手段、認証判断手段、復号化手段としての機能を有している。
【００５７】
ＲＯＭ３９は、上述した一連の処理を行うためのプログラムや必要な情報、例えば、認証用ワンタイムパスワードを生成するためのアルゴリズムプログラムや、暗号化された乱数情報やワンタイムパスワードなどを復号化するための復号化プログラムおよび予め規定される暗号化キー（復号化に用いられるキー情報）が記録されている。
【００５８】
なお、ＲＯＭ３９に記録される予め規定された暗号化キーは、情報通信装置３のＲＯＭ

２１に記録される暗号化キーと共通する暗号化キーである。また、認証用ワンタイムパスワードを生成するためのアルゴリズムプログラムのアルゴリズムは、情報通信装置３のＲＯＭ２１に記録されるプログラムのアルゴリズムに共通するアルゴリズムによって構築されている。

【００５９】

ＲＡＭ４０は、ＣＰＵ３８において行われる処理のワークエリア等として用いられる記録手段である。

【００６０】

データ記録部３１は、認証処理に必要な様々な情報が記録されている。具体的にはアクセスの認証判断に用いるＩＤ情報が記録されている。サーバ装置２では、サーバ制御部３０のＣＰＵ３８が、情報通信装置３より受信したＩＤ情報に基づいて、データ記録部３１に記録されたＩＤ情報と照合を行い、アクセス許可の判断対象となるＩＤ情報であるか否かの判断を行う。受信したＩＤ情報がデータ記録部３１に記録されるＩＤ情報と一致しない場合には、ワンタイムパスワードに基づく認証を行うことなく、情報通信装置３のアクセスを拒絶（拒否）する旨の決定が行われる。

【００６１】

情報通信部３３は、情報通信装置３によって出力された乱数情報、ＩＤ情報、ワンタイムパスワードを受信する役割を有しており、また、後述するメッセージを情報通信装置３に対して出力する役割を有している。情報通信部３３は、情報通信装置３の通信部６と同様に、例えば、ネットワークカード（ＮＩＣ：Network Interface Card）等が該当し、サーバ装置２をネットワーク４に接続させる役割を有している。

【００６２】

なお、図３では、情報通信装置３の通信部６と同様に、便宜的にサーバ装置２に内蔵されるネットワークカードを情報通信部３３として記載しているが、情報通信部３３より延設されるネットワークケーブルに対してモデムやメディアコンバータ等が接続される場合には、情報通信部３３にモデム等が含まれることになる。

【００６３】

内部時計部３４と電波受信部３５とは、上述した情報通信装置３に設けられる内部時計部１１と電波受信部１３と同一の機能を備えている。内部時計部３４は、情報通信装置３の内部時計部１１と同様に水晶振動子によって構成されており、この水晶振動子の振動に基づいてサーバ装置２における時間管理が行われる。電波受信部３５は、情報通信装置３の電波受信部１３と同様に、標準電波を受信する機能を有しており、サーバ制御部３０よって、標準電波が一定時間ごとに読み取られて内部時計部３４の時刻の修正が行われる。

【００６４】

次に、図４および図５に示すフローチャートに基づいて、情報通信装置３とサーバ装置２との認証判断処理を説明する。

【００６５】

まず。情報通信装置３のＣＰＵ２０は、キーボード１６を介して入力されたＩＤ情報を取得すると共に、物理乱数生成部１２より乱数情報（乱数値）を取得する（ステップＳ．１）。そして、取得した乱数情報を、ＲＯＭ２１に記録される予め規定された暗号化キーを用いて暗号化する（ステップＳ．２）。その後、情報通信装置３のＣＰＵ２０は、内部時計部１１より時刻情報を取得（ステップＳ．３）し、時刻情報を取得した後直ぐに、暗号化された乱数情報を、通信部６を介してサーバ装置２へと出力する（ステップＳ．４）。

【００６６】

ＣＰＵ２０は、ステップＳ．３において時刻情報を取得してから、ステップＳ．４において暗号化された乱数情報をサーバ装置２へ出力するまでの処理を、短時間に実行する。この処理を短時間で実行することにより、取得した時刻情報の時刻とほぼ同じ時間、具体的には、時分まで同じ時間内に、暗号化された乱数情報をサーバ装置２で受信することが可能となる。ＣＰＵ２０では、サーバ装置２における乱数情報の受信時刻と、ステップＳ

．３の時刻情報取得処理により取得される時刻との対応を考慮して、時分まで（秒は含まない）の時刻を時刻情報として取得する。

【００６７】

なお、ステップＳ．３において取得される時刻情報は、上述したように内部時計部１１において管理される時刻情報であるが、既に説明したように、電波受信部１３において一定時間毎に標準電波が受信されて内部時計部１１の時刻修正が行われているので、ＣＰＵ２０では、正確な時刻情報を取得することができる。

【００６８】

そして、情報通信装置３のＣＰＵ２０は、取得した時刻情報とステップＳ．１において取得した乱数情報とに基づいてワンタイムパスワードを生成する（ステップＳ．５）。そして、ＣＰＵ２０は、生成したワンタイムパスワードとＩＤ情報とを、取得した乱数情報を暗号化キーに用いて暗号化し（ステップＳ．６）、暗号化されたワンタイムパスワードおよびＩＤ情報を、通信部６を介してサーバ装置２へと出力する（ステップＳ．７）。

【００６９】

ステップＳ．５において、ＣＰＵ２０は、ＲＯＭ２１に記録されるアルゴリズムプログラムのアルゴリズムに基づいて、時刻情報と乱数情報とを用いてワンタイムパスワードを生成する。このアルゴリズムは、上述したようにサーバ装置２のＲＯＭ３９に記録されるアルゴリズムプログラムのアルゴリズムと同一であるため、サーバ装置２では、同一の時刻情報と同一の乱数情報とに基づいて同一のワンタイムパスワードを生成することが可能となっている。

【００７０】

サーバ装置２のＣＰＵ３８は、情報通信部３３を介して情報通信装置３より暗号化された乱数情報を受信し（ステップＳ．２１）、乱数情報の受信時刻（時刻情報）を、内部時計部３４より取得する（ステップＳ．２２）。

【００７１】

なお、ステップＳ．２２において取得される時刻情報も、上述したように内部時計部３４において管理される時刻情報であるが、既に説明したように、電波受信部３５において一定時間毎に標準電波が受信されて内部時計部３４の時刻修正が行われているので、ＣＰＵ３８では、正確な時刻情報を取得することができる。

【００７２】

次に、サーバ装置２のＣＰＵ３８は、受信した乱数情報を、ＲＯＭ３９に記録される暗号化キーを用いて暗号化された乱数情報を復号化する（ステップＳ．２３）。次に、サーバ装置２のＣＰＵ３８は、情報通信部３３を介して情報通信装置３より暗号化されたワンタイムパスワードおよびＩＤ情報を受信し（ステップＳ．２４）、ステップＳ．２３において復号化した乱数情報を用いて、受信したワンタイムパスワードおよびＩＤ情報の復号化を行う（ステップＳ．２５）。

【００７３】

そして、サーバ装置２のＣＰＵ３８は、復号化したＩＤ情報を、データ記録部３１に記録されるアクセスの許可対象となるＩＤ情報群と比較し、情報通信装置３のＩＤ情報がアクセス許可の対象となるＩＤ情報であるか否かを判断する（ステップＳ．２６）。

【００７４】

アクセス許可の対象とならないＩＤ情報である場合（ステップＳ．２６においてＮｏの場合）、ＣＰＵ３８は、情報通信部３３を介して、情報通信装置３に対して認証が失敗した旨のメッセージを送信し（ステップＳ．２９）、情報通信装置３からのアクセスを禁止（拒絶）する設定を行い（ステップＳ．３０）、処理を終了する。

【００７５】

一方で、アクセス許可の対象となるＩＤ情報である場合（ステップＳ．２６においてＹｅｓの場合）、ＣＰＵ３８は、ステップＳ．２２において取得された時刻情報と、ステップＳ．２３において復号化した乱数情報とを用い、ＲＯＭ３９に記録されるアルゴリズムプログラムのアルゴリズムに基づいて、認証用のワンタイムパスワードを生成する（ステ

ップＳ．２７）。
【００７６】
このとき、ＣＰＵ３８は、ステップＳ．３において情報通信装置３のＣＰＵ２０により取得された時刻情報と、ステップＳ．２２においてサーバ装置２のＣＰＵ３８により取得された時刻情報との時間差を考慮して、ステップＳ．２２において取得された時刻情報よりも１～２分程度早い時間となる複数の時刻情報を用いて、複数の認証用ワンタイムパスワードを生成する。このように１～２分程度の時間差を考慮した複数の認証用ワンタイムパスワードを生成することにより、ワンタイムパスワードの送信に時間を要した場合などを考慮することが可能となる。
【００７７】
次に、サーバ装置２のＣＰＵ３８は、情報通信装置３より取得し復号化処理したワンタイムパスワードと、ＣＰＵ３８において生成した認証用ワンタイムパスワードとを比較し、同一のパスワードであるか否かを判断する（ステップＳ．２８）。
【００７８】
生成した複数の認証用ワンタイムパスワードと取得したワンタイムパスワードとが一致しない場合（ステップＳ．２８においてＮｏの場合）、ＣＰＵ３８は、情報通信部３３を介して、情報通信装置３に対して認証が失敗した旨のメッセージを送信し（ステップＳ．２９）、情報通信装置３からのアクセスを禁止（拒絶）する設定を行い（ステップＳ．３０）、処理を終了する。
【００７９】
一方で、生成した複数の認証用ワンタイムパスワードと取得したワンタイムパスワードとが一致する場合（ステップＳ．２８においてＹｅｓの場合）、ＣＰＵ３８は、情報通信部３３を介して、情報通信装置３に対して認証が成功した旨のメッセージを送信し（ステップＳ．３１）、情報通信装置３からのアクセスを認める（許容する）設定を行い（ステップＳ．３２）、処理を終了する。
【００８０】
情報通信装置３のＣＰＵ２０は、通信部６を介して、サーバ装置２よりメッセージを受信し（ステップＳ．８）、受信したメッセージをディスプレイ１５に表示して（ステップＳ．９）処理を終了する。
【００８１】
以上説明したように、本実施の形態に係るワンタイムパスワード認証システム１では、ネットワーク４を介して、情報通信装置３とサーバ装置２との間で送受信される乱数情報、ワンタイムパスワード、ＩＤ情報の暗号化処理が行われているので、第三者がこれらの情報を受信しても、容易に中身を判断することができない。このため、情報通信装置３とサーバ装置２との認証処理に必要な情報が第三者に容易に知られてしまうことを防止することができ、高いセキュリティを確保することが可能となる。
【００８２】
特に、ワンタイムパスワードとＩＤ情報とは、乱数情報を暗号化キーとして用いて暗号化されている。このため、ワンタイムパスワードの暗号化を行う度に、暗号化キーの内容が変更されることになり、安全の確保を図ることが容易となる。
【００８３】
さらに、暗号化キーとして用いられる乱数情報は物理乱数生成部１２において物理的現象を利用して生成される乱数情報であるため、プログラムなどに基づいて生成される乱数情報のように、乱数情報の生成アルゴリズムが解析されてしまうおそれや、プログラムの不具合により不適切な乱数情報が生成されてしまうおそれがない。このため、暗号化キー自体のセキュリティを高めることができ、容易にワンタイムパスワードおよびＩＤ情報の復号化が行われてしまうことを防止することができる。
【００８４】
一方で、情報通信装置３の認証処理に用いられるワンタイムパスワードは、毎回異なる値となる乱数情報と、常に変化する時刻情報とに基づいて生成される。このため、従来の

ように一定の情報（例えば、ＩＤ情報）と時刻情報とによりワンタイムパスワードを生成する場合よりも、ワンタイムパスワードの生成パターンが増大し、ワンタイムパスワードの解析がより難しくなり、安全性の向上を図ることが可能となる。

【００８５】

また、本実施の形態に係るワンタイムパスワード認証システム１では、ワンタイムパスワードの生成に必要とされる時刻情報がネットワーク４を介して送受信されることがない。このため、悪意のある第三者は、時刻情報を取得することが困難となり、容易にワンタイムパスワードを生成・解析することができなくなる。

【００８６】

さらに、情報通信装置３およびサーバ装置２には、内部時計部１１，３４と電波受信部１３，３５とが設けられており、電波受信部１３，３５において受信された標準電波に基づいて内部時計部１１，３４の時刻が修正されるため、情報通信装置３およびサーバ装置２の内部時計部１１，３４は、常に正確な時刻を示すことになる。このため、時刻情報を情報通信装置３とサーバ装置２との間で送受信しなくても、情報通信装置３とサーバ装置２との時刻を同期させることが可能なり、ワンタイムパスワードおよび認証用ワンタイムパスワードの生成に不可欠な時刻情報のズレを低減させることが可能となる。

【００８７】

また、本実施の形態に係るワンタイムパスワード認証システム１では、ワンタイムパスワードの生成に、物理乱数生成部１２で生成された乱数情報が用いられる。この乱数情報は、上述したように、物理的現象を利用して生成される乱数情報であるため、プログラムなどに基づいて生成される乱数情報のように、乱数情報の生成アルゴリズムが解析されてしまうおそれや、プログラムの不具合により不適切な乱数情報が生成されてしまうおそれがない。また、物理的現象を利用して生成される乱数であるため、乱数生成のアルゴリズムを解析することが困難である。このような全くランダムに生成される乱数情報を用いてワンタイムパスワードが生成されるため、ワンタイムパスワードの偽造等を行うことが困難となり、結果として、ワンタイムパスワード認証システムの認証精度を向上させることが可能となる。

【００８８】

以上、本発明に係るワンタイムパスワード認証システムを、図面を用いて詳細に説明したが、本発明に係るワンタイムパスワード認証システムは上述した本実施の形態に記載した内容に限定されるものではない。いわゆる当業者であれば、特許請求の範囲に記載された範疇内において、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。

【図面の簡単な説明】

【００８９】

【図１】本実施の形態に係るワンタイムパスワード認証システムを示した概略構成図である。

【図２】本実施の形態に係る情報通信装置の概略構成を示したブロック図である。

【図３】本実施の形態に係るサーバ装置の概略構成を示したブロック図である。

【図４】本実施の形態に係るワンタイムパスワード認証システムの認証処理の前半を示したフローチャートである。

【図５】本実施の形態に係るワンタイムパスワード認証システムの認証処理の後半を示したフローチャートである。

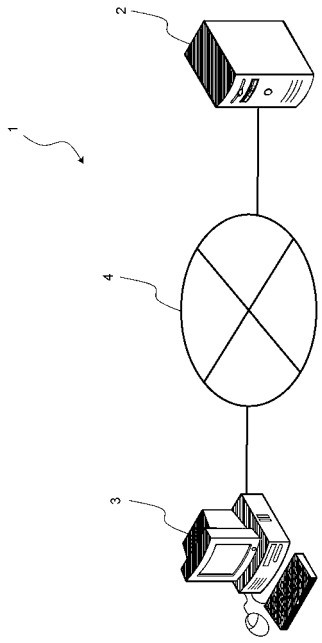
【符号の説明】

【００９０】

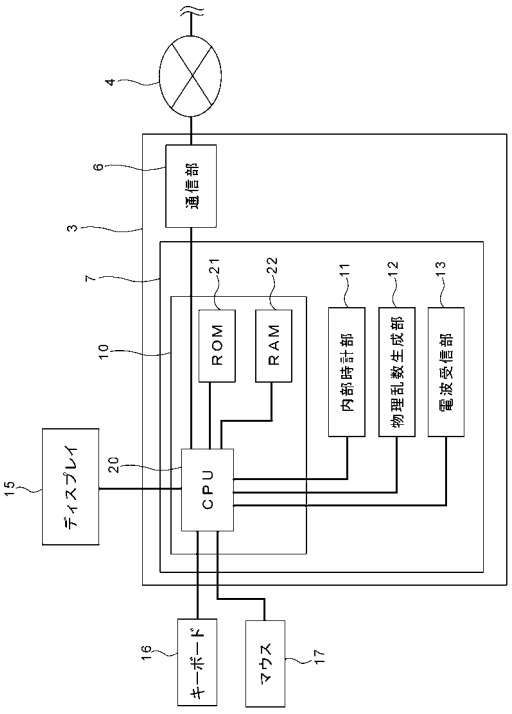
１　…ワンタイムパスワード認証システム
２　…サーバ装置（認証判断装置）
３　…情報通信装置
４　…ネットワーク
６　…（情報通信装置の）通信部（乱数情報出力手段、ワンタイムパスワード出力手

段）
７　…（情報通信装置の）パスワード生成部
１０　…（パスワード生成部の）制御部（時刻検出手段、時刻補正手段、ワンタイムパスワード生成手段、暗号化手段）
１１　…（パスワード生成部の）内部時計部（時刻検出手段、内部時計手段）
１２　…（パスワード生成部の）物理乱数生成部（乱数生成手段）
１３　…（パスワード生成部の）電波受信部（時刻検出手段、電波受信手段）
１５　…ディスプレイ
１６　…キーボード
１７　…マウス
２０　…（制御部の）ＣＰＵ
２１　…（制御部の）ＲＯＭ
２２　…（制御部の）ＲＡＭ
３０　…（サーバ装置の）サーバ制御部（受信時刻検出手段、時刻補正手段、認証用ワンタイムパスワード生成手段、認証判断手段、復号化手段）
３１　…（サーバ装置の）データ記録部
３３　…（サーバ装置の）情報通信部（情報受信手段）
３４　…（サーバ装置の）内部時計部（受信時刻検出手段、内部時計手段）
３５　…（サーバ装置の）電波受信部（受信時刻検出手段、電波受信手段）
３８　…（サーバ装置の）ＣＰＵ
３９　…（サーバ装置の）ＲＯＭ
４０　…（サーバ装置の）ＲＡＭ

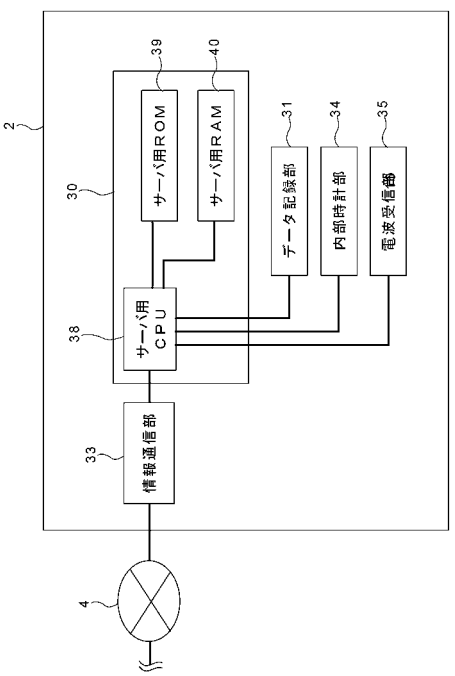
【図１】



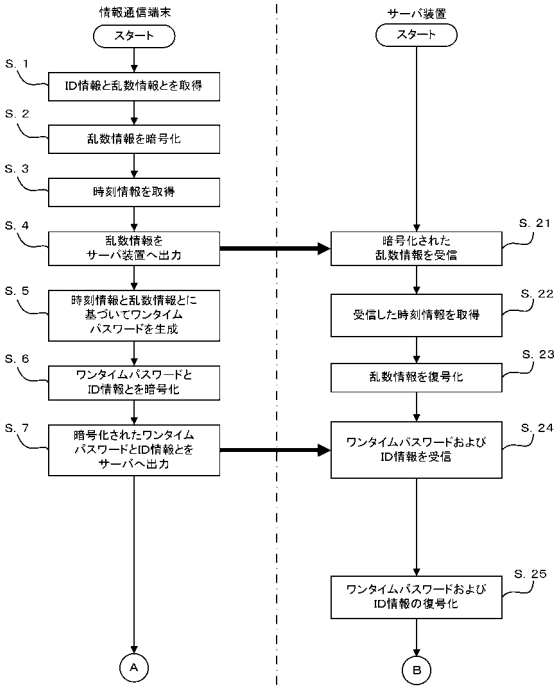
【図２】



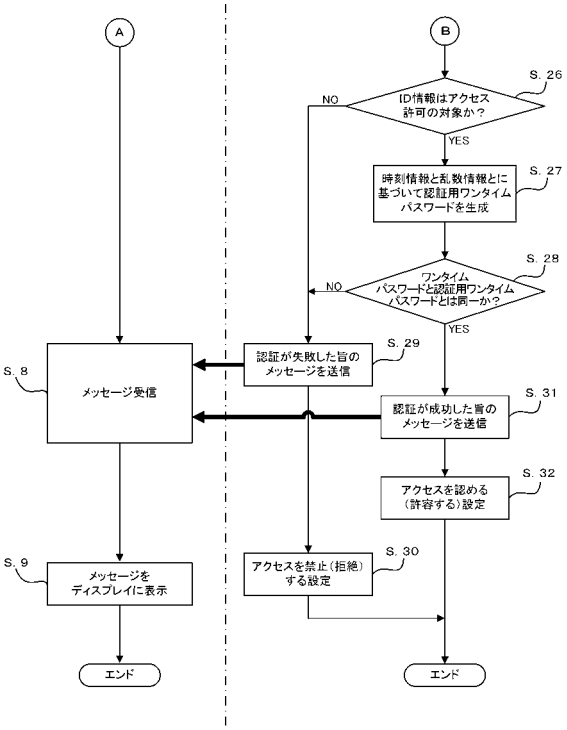
【図３】


2
30
サーバ用ROM
39
サーバ用RAM
40
データ記録部
31
内部時計部
34
電波受信機部
35
38
サーバ用CPU
33
情報通信部
4

【図４】


情報通信端末
スタート
S. 1
ID情報と乱数情報とを取得
S. 2
乱数情報を暗号化
S. 3
時刻情報を取得
S. 4
乱数情報を
サーバ装置へ出力
S. 5
時刻情報と乱数情報とに
基づいてワンタイム
パスワードを生成
S. 6
ワンタイムパスワードと
ID情報とを暗号化
S. 7
暗号化されたワンタイム
パスワードとID情報とを
サーバへ出力
A
サーバ装置
スタート
暗号化された
乱数情報を受信
S. 21
受信した時刻情報を取得
S. 22
乱数情報を復号化
S. 23
ワンタイムパスワードおよび
ID情報を受信
S. 24
ワンタイムパスワードおよび
ID情報の復号化
S. 25
B

【図５】


A
B
S. 26
ID情報はアクセス
許可の対象か？
NO
YES
時刻情報と乱数情報とに
基づいて認証用ワンタイム
パスワードを生成
S. 27
S. 28
ワンタイム
パスワードと認証用ワンタイム
パスワードとは同一か？
NO
YES
S. 8
メッセージ受信
認証が失敗した旨の
メッセージを送信
S. 29
認証が成功した旨の
メッセージを送信
S. 31
アクセスを認める
（許容する）設定
S. 32
S. 9
メッセージを
ディスプレイに表示
アクセスを禁止（拒絶）
する設定
S. 30
エンド
エンド

フロントページの続き

(56)参考文献 特開２００６－２７９４０７（ＪＰ，Ａ）
特開２００８－０２７４２０（ＪＰ，Ａ）
特開２００５－０５０２９２（ＪＰ，Ａ）
特開２００７－３３６５０６（ＪＰ，Ａ）
特表２００２－５２１９６２（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／２０
Ｈ０４Ｌ ９／３２