

(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2009-230482

(P2009-230482A)

(43) 公開日 平成21年10月8日(2009.10.8)

(51) Int.Cl.		F I			テーマコード (参考)
<b>G06F 21/20</b>	<b>(2006.01)</b>	G06F 15/00	330B		5B285
<b>H04L 9/32</b>	<b>(2006.01)</b>	H04L 9/00	673D		5J104

審査請求 未請求 請求項の数 15 O L (全 21 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)

(71) 出願人 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  
 (71) 出願人 508088214  
 株式会社福島県中央計算センター  
 福島県福島市新町7番22号  
 (71) 出願人 508088225  
 株式会社福島情報処理センター  
 福島県郡山市桑野三丁目18番24号  
 (71) 出願人 508088236  
 株式会社FSK  
 福島県いわき市内郷御厩町3丁目168  
 (74) 代理人 100118094  
 弁理士 殿元 基城

最終頁に続く

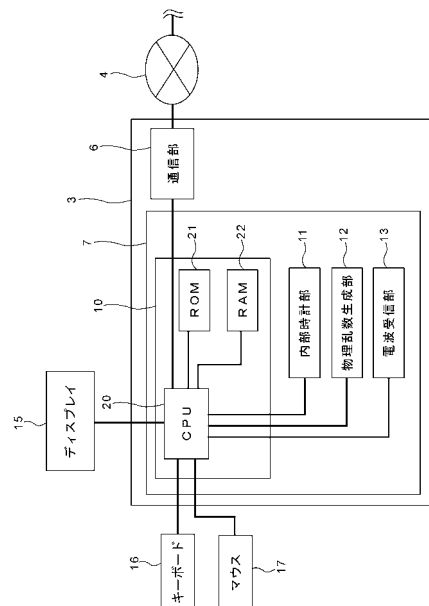
(54) 【発明の名称】 ワンタイムパスワード認証システム、ワンタイムパスワード認証方法、ワンタイムパスワード生成プログラム、ワンタイムパスワード認証プログラムおよびワンタイムパスワード生成装置。

(57) 【要約】

【課題】 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。

【解決手段】 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3と、該情報通信装置3よりワンタイムパスワードを受信して情報通信装置3の認証判断を行う認証判断装置とを備えている。情報通信装置3は、乱数生成手段12により生成された乱数情報と、時刻検出手段11により検出された時刻情報とに基づい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手段10と、時刻検出手段11による時刻情報の検出時に、生成された乱数情報を認証判断装置に出力する乱数情報出力手段6と、生成されたワンタイムパスワードを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6とを有している。

【選択図】 図2



**【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

10

20

30

40

50

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情報受信手段が行う情報受信時刻検出ステップと、

該情報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

10

20

30

40

50

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、

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、

10

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】

前記乱数生成手段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】

20

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。

30

【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、

40

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、

50

前記乱数情報を暗号化キーとして用いて前記ワнтаイムパスワードの復号化を行うワнта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 1 1 に記載のワнтаイムパスワード認証プログラム。

【請求項 1 3】

認証判断装置において認証判断を行うためのワнтаイムパスワードを生成するワнта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нтаイムパスワードを生成するワнтаイムパスワード生成手段と

を有することを特徴とするワнтаイムパスワード生成装置。

【請求項 1 4】

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 1 3 に記載のワнтаイムパスワード生成装置。

【請求項 1 5】

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 1 3 または請求項 1 4 に記載のワнта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нтаイムパスワード認証システム、ワнтаイムパスワード認証方法、ワнтаイムパスワード生成プログラム、ワнтаイムパスワード認証プログラムおよびワнта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нта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нтаイムパスワード認証システム、ワнта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ー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う（いわゆる、

10

20

30

40

50

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、頻り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)。

10

【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。

20

【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つ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。

30

【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。

40

【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】

50

## 【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。

10

## 【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。

20

30

40

## 【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

50

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。

10

【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。

20

【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】

30

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。

40

【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いという利点がある。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

50



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。

10

【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。

20

30

【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プログラムであってもよい。

40

【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

50

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。

10

【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。

20

【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。

30

【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。

40

【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な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

50

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である。

【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た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。

10

【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。

20

【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。

30

【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。

40

【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

50

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нта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нта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нта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нта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нтаイムパスワードを生成するためのワнта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нта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нта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нта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

10

20

30

40

50

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 1 1 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 1 3 を介して正確な時間を取得して内部時計部 1 1 の時刻補正を行っている。

#### 【 0 0 4 9 】

電波受信部 1 3 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。CPU 2 0 では、送信局から送られてくる標準電波を電波受信部 1 3 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 1 1 の時刻の修正を行っている。このため、内部時計部 1 1 では、電波受信部 1 3 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 1 0 の CPU 2 0 が、電波受信部 1 3 において受信された標準電波に基づいて内部時計部 1 1 の時刻を補正するので、制御部 1 0 は、時刻補正手段としての機能を有している。

#### 【 0 0 5 0 】

物理乱数生成部 1 2 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。

#### 【 0 0 5 1 】

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。

#### 【 0 0 5 2 】

物理乱数生成部 1 2 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 1 2 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 F I S P 1 4 0 - 2 相当の乱数品位を確保することが可能となる。

#### 【 0 0 5 3 】

次にサーバ装置 2 の構成について説明する。

#### 【 0 0 5 4 】

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）3 0 と、データ記録部 3 1 と、情報通信部（情報受信手段）3 3 と、内部時計部（受信時刻検出手段、内部時計手段）3 4 と、電波受信部（受信時刻検出手段、電波受信手段）3 5 とを有している。

#### 【 0 0 5 5 】

サーバ制御部 3 0 は、サーバ用の CPU 3 8 と、サーバ用の ROM 3 9 と、サーバ用の RAM 4 0 とを有している。

#### 【 0 0 5 6 】

CPU 3 8 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

10

20

30

40

50

刻を内部時計部 3 4 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、CPU 3 8 (サーバ制御部 3 0) 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】

ROM 3 9 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。

10

【0058】

なお、ROM 3 9 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 2 1 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 ROM 2 1 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】

RAM 4 0 は、CPU 3 8 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。

20

【0060】

データ記録部 3 1 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 3 0 の CPU 3 8 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 3 1 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 3 1 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】

30

情報通信部 3 3 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 3 3 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 3 3 として記載しているが、情報通信部 3 3 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 3 3 にモデム等が含まれることになる。

40

【0063】

内部時計部 3 4 と電波受信部 3 5 とは、上述した情報通信装置 3 に設けられる内部時計部 1 1 と電波受信部 1 3 と同一の機能を備えている。内部時計部 3 4 は、情報通信装置 3 の内部時計部 1 1 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 3 5 は、情報通信装置 3 の電波受信部 1 3 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 3 0 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 3 4 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。

50

## 【 0 0 6 5 】

まず、情報通信装置 3 の CPU 2 0 は、キーボード 1 6 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 1 2 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、ROM 2 1 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 CPU 2 0 は、内部時計部 1 1 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 ）。

## 【 0 0 6 6 】

CPU 2 0 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、短時間に行う。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。CPU 2 0 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。

10

## 【 0 0 6 7 】

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 1 1 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 1 3 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 1 1 の時刻修正が行われているので、CPU 2 0 では、正確な時刻情報を取得することができる。

20

## 【 0 0 6 8 】

そして、情報通信装置 3 の CPU 2 0 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、CPU 2 0 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 ）。

## 【 0 0 6 9 】

ステップ S . 5 において、CPU 2 0 は、ROM 2 1 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 ROM 3 9 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。

30

## 【 0 0 7 0 】

サーバ装置 2 の CPU 3 8 は、情報通信部 3 3 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 . 2 1 ）、乱数情報の受信時刻（時刻情報）を、内部時計部 3 4 より取得する（ステップ S . 2 2 ）。

## 【 0 0 7 1 】

なお、ステップ S . 2 2 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 3 4 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 3 5 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 3 4 の時刻修正が行われているので、CPU 3 8 では、正確な時刻情報を取得することができる。

40

## 【 0 0 7 2 】

次に、サーバ装置 2 の CPU 3 8 は、受信した乱数情報を、ROM 3 9 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 . 2 3 ）。次に、サーバ装置 2 の CPU 3 8 は、情報通信部 3 3 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 . 2 4 ）、ステップ S . 2 3 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 . 2 5 ）。

50

## 【 0 0 7 3 】

そして、サーバ装置 2 の CPU 3 8 は、復号化した ID 情報を、データ記録部 3 1 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 . 2 6 ）。

## 【 0 0 7 4 】

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 . 2 6 において N o の場合）、CPU 3 8 は、情報通信部 3 3 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 . 2 9 ）、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 . 3 0 ）、処理を終了する。

## 【 0 0 7 5 】

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 . 2 6 において Y e s の場合）、CPU 3 8 は、ステップ S . 2 2 において取得された時刻情報と、ステップ S . 2 3 において復号化した乱数情報とを用い、ROM 3 9 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 . 2 7 ）。

## 【 0 0 7 6 】

このとき、CPU 3 8 は、ステップ S . 3 において情報通信装置 3 の CPU 2 0 により取得された時刻情報と、ステップ S . 2 2 においてサーバ装置 2 の CPU 3 8 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 . 2 2 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。

## 【 0 0 7 7 】

次に、サーバ装置 2 の CPU 3 8 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、CPU 3 8 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 . 2 8 ）。

## 【 0 0 7 8 】

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 . 2 8 において N o の場合）、CPU 3 8 は、情報通信部 3 3 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 . 2 9 ）、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 . 3 0 ）、処理を終了する。

## 【 0 0 7 9 】

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 . 2 8 において Y e s の場合）、CPU 3 8 は、情報通信部 3 3 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 . 3 1 ）、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 . 3 2 ）、処理を終了する。

## 【 0 0 8 0 】

情報通信装置 3 の CPU 2 0 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 1 5 に表示して（ステップ S . 9 ）処理を終了する。

## 【 0 0 8 1 】

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。

10

20

30

40

50



## 【 0 0 8 2 】

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。

## 【 0 0 8 3 】

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。

10

## 【 0 0 8 4 】

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。

## 【 0 0 8 5 】

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。

20

## 【 0 0 8 6 】

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。

30

## 【 0 0 8 7 】

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。

40

## 【 0 0 8 8 】

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 】

## 【 0 0 8 9 】

【 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

50

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。

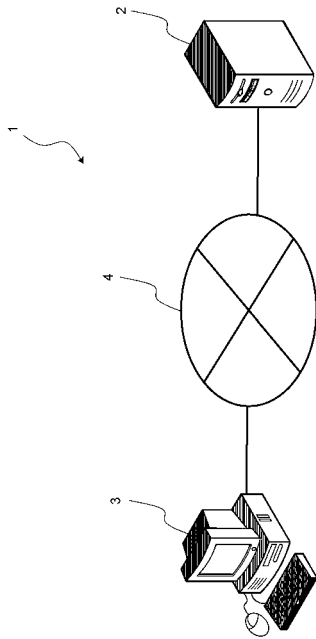
【図5】本実施の形態に係るワンタイムパスワード認証システムの認証処理の後半を示したフローチャートである。

【符号の説明】

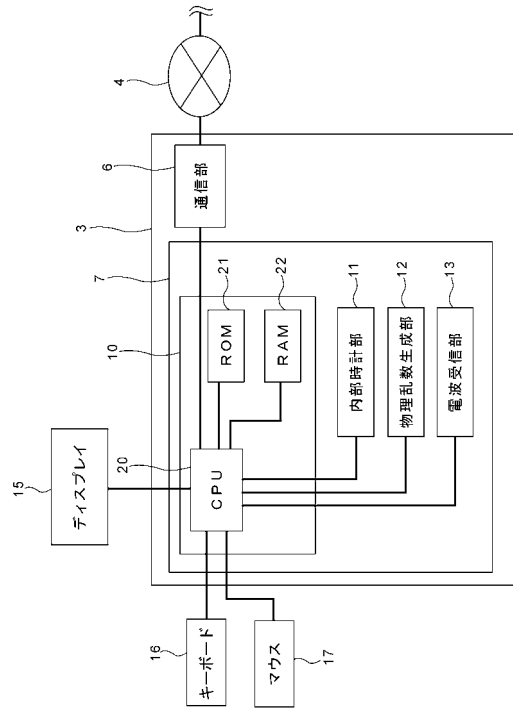
【0090】

- |    |   |    |
|----|---|----|
| 1  | ...ワンタイムパスワード認証システム   | 10 |
| 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)                                     | 20 |
| 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   | 30 |
| 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  |    |

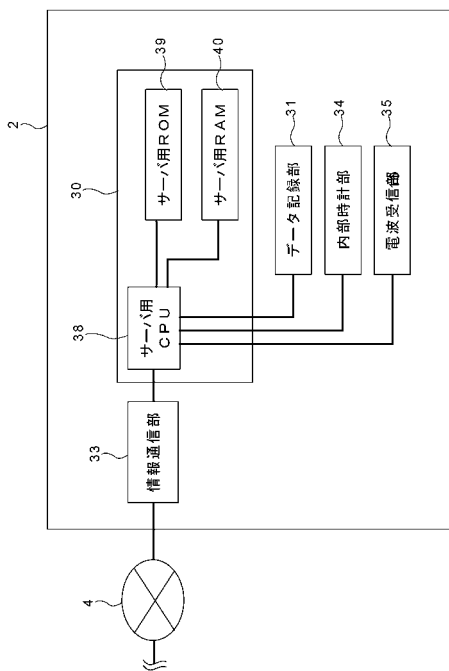
【図1】



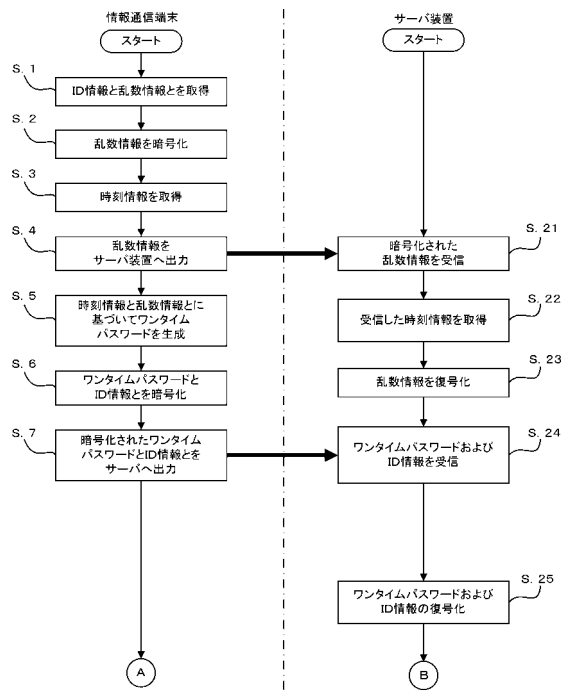
【図2】



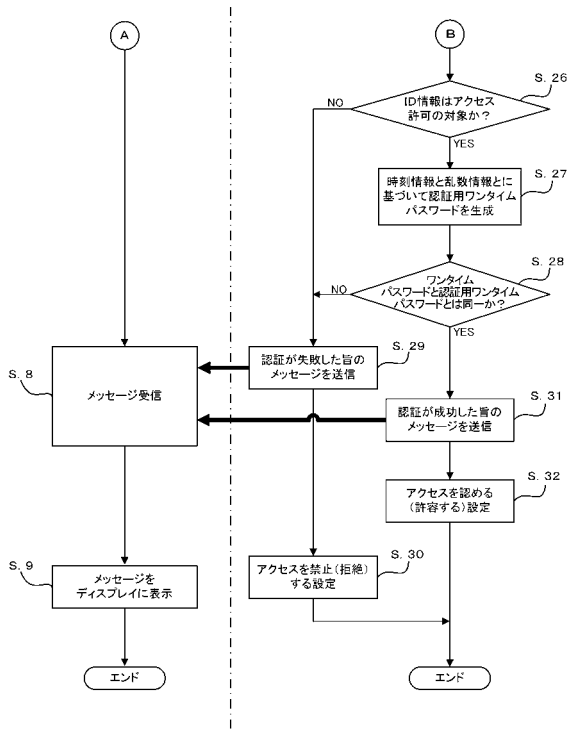
【図3】



【図4】



【 図 5 】



---

フロントページの続き

(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

Fターム(参考) 5B285 AA01 BA03 CA47 CB02 CB53 CB58 CB59 CB62 CB72 CB95  
5J104 AA07 AA11 AA16 EA03 EA04 EA08 EA16 EA17 GA05 KA02  
KA21 NA02 NA05 NA36 NA37 PA07