

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号
特開2000-10927
(P2000-10927A)

(43)公開日 平成12年1月14日(2000.1.14)

(51)Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 8 5
H 0 4 Q 7/38		H 0 4 M 1/66	B 5 J 1 0 4
H 0 4 L 9/32		11/00	3 0 3 5 K 0 2 7
12/28		H 0 4 B 7/26	1 0 9 S 5 K 0 3 3
H 0 4 M 1/66		H 0 4 L 9/00	6 7 3 A 5 K 0 6 7

審査請求 有 請求項の数 6 O L (全 7 頁) 最終頁に続く

(21)出願番号 特願平10-178410

(22)出願日 平成10年6月25日(1998.6.25)

(71)出願人 000240617

米沢日本電気株式会社
山形県米沢市下花沢2丁目6番80号

(72)発明者 花等 勝

山形県米沢市下花沢2丁目6番80号 米沢
日本電気株式会社内

(74)代理人 100085235

弁理士 松浦 兼行

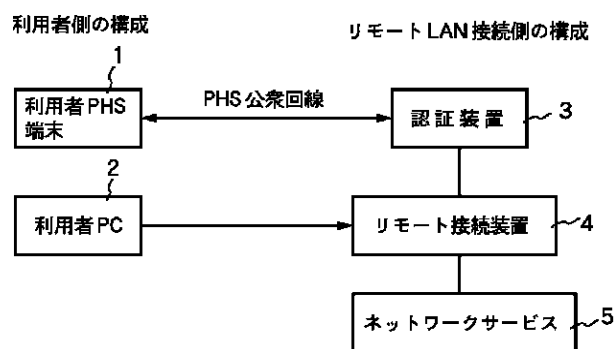
最終頁に続く

(54)【発明の名称】 認証システム及び認証装置

(57)【要約】

【課題】 従来の認証システムでは、変化するパスワードを作成／管理する装置（ワンタイムパスワード生成カード及び認証装置）が非常に高価であるため、大規模な普及には至っていない。

【解決手段】 認証装置3は、利用者における「利用者パスワード要求／通知機能」の管理と、利用者からの接続要求に対し「一時的なパスワード」の発行と、「一時的なパスワード」を利用者PHS端末1とリモート接続装置4への通知とを実行する。リモート接続装置4は、「一時的なパスワード」を基に利用者PC2からの接続要求を受け付け、認証装置3に対して正規ユーザか問い合わせ利用者のリモート接続を行う。利用者PC2は、「一時的なパスワード」に基づいて、リモート接続装置4に対して接続を行う。ネットワークサービス5は各利用者がサービスを受けるネットワークの資源である。



【特許請求の範囲】

【請求項1】 利用者の正当性を確認してから当該利用者のパーソナルコンピュータからネットワークサービスの資源の利用を許可する認証システムにおいて、前記利用者の簡易型携帯電話端末と、前記簡易型携帯電話端末の電話番号とパスワードとリモート接続IDを予め登録し、前記パスワードとリモート接続IDを前記利用者に通知し、前記利用者の簡易型携帯電話端末からの電話番号とパスワードを受け、予め登録してある前記電話番号とパスワードと比較して一致するときは、一時的なパスワードを前記利用者の簡易型携帯電話端末に発行する認証装置と、前記簡易型携帯電話端末への前記一時的なパスワードの通知により前記利用者が前記パーソナルコンピュータを用いて行う接続要求を受け、前記認証装置に対し前記パスワードと前記リモート接続IDが正しいか問い合わせ、前記認証装置より正しいと通知された時のみ前記パーソナルコンピュータと前記ネットワークサービスを接続させるリモート接続装置とを有することを特徴とする認証システム。

【請求項2】 前記利用者は、前記パーソナルコンピュータを使用して、前記認証装置から通知された前記リモート接続IDと前記一時的なパスワードとを使用して前記リモート接続装置に接続要求を行うことを特徴とする請求項1記載の認証システム。

【請求項3】 前記認証装置は前記リモート接続装置からの問い合わせに対して、前記利用者に発行した情報と前記リモート接続装置からの情報とが一致するか判断し、その判断結果を前記リモート接続装置に通知することを特徴とする請求項1記載の認証システム。

【請求項4】 前記携帯電話端末は、前記認証装置からの前記一時的なパスワード通知前に電源をオフすることを特徴とする請求項1記載の認証システム。

【請求項5】 利用者の正当性を確認してから当該利用者のパーソナルコンピュータからネットワークサービスの資源の利用を許可する認証システムに用いる認証装置において、前記利用者の簡易型携帯電話端末の電話番号とパスワードとリモート接続IDを予め登録し、前記パスワードとリモート接続IDを前記利用者に通知し、前記利用者の簡易型携帯電話端末からの電話番号とパスワードを受け、予め登録してある前記電話番号とパスワードと比較して一致するときは、一時的なパスワードを前記利用者の簡易型携帯電話端末に発行し、リモート接続装置からの問い合わせに対して正しいと判断した時は、前記リモート接続装置により前記パーソナルコンピュータと前記ネットワークサービスを接続させることを特徴とする認証装置。

【請求項6】 前記リモート接続装置からの問い合わせに対して、前記利用者に発行した情報と前記リモート接

続装置からの情報とが一致するか判断し、その判断結果を前記リモート接続装置に通知することを特徴とする請求項5記載の認証装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は認証システム及び認証装置に係り、特にローカルエリアネットワーク（LAN）サービスの提供を正規の利用者に対してのみ許可する認証システム及び認証装置に関する。

【0002】

【従来の技術】LANにおける相互の計算機のサービスを利用するネットワークサービス機能として、一般に送信されてくるログイン計算機の利用者識別子（ID、パスワード）を用いて、リモート資源の利用権を検査する認証機能がある。ネットワーク接続計算機システムでは、利用者識別子は計算機利用開始時にネットワーク計算機システムを構成する各計算機上の利用者登録リストを用いて、各計算機上のシステムソフトウェアにより与えられている。また、パーソナルハンディホンシステム（PHS）端末を利用した国際電話利用システムにおいて、ID番号とパスワードを用いてシステムを呼び出し、正当性確認後はシステム側からのコールバック機能を利用するシステムも知られている（特開平9-135295号公報）。

【0003】しかし、この方法では利用者のIDやパスワードが第三者に盗まれると、許可されていない第三者がネットワークサービスに侵入できる危険性を持っている。そこで、近年は一定時間毎に変化するパスワードを利用した認証システムが提案され、既に実用化されている。この従来の認証システムでは、パスワードが一定時間毎に変化するので、第三者によるパスワードの盗用を困難にできる。

【0004】

【発明が解決しようとする課題】しかるに、上記の従来の認証システムでは、変化するパスワードを作成／管理する装置（ワンタイムパスワード生成カード及び認証装置）が非常に高価であるため、大規模な普及には至っていないという問題がある。

【0005】本発明は以上の点に鑑みなされたもので、高速で高信頼性な認証システム及び安価な認証装置を提供することを目的とする。

【0006】また、本発明の他の目的は、生産性や保守性、資源の再利用性が可能な認証システム及び認証装置を提供することにある。

【0007】更に、本発明の他の目的は、小型で軽量な認証装置を提供することにある。

【0008】

【課題を解決するための手段】上記の目的を達成するため、本発明の認証システムは、利用者の正当性を確認してから当該利用者のパーソナルコンピュータからネット

ワークサービスの資源の利用を許可する認証システムにおいて、利用者の簡易型携帯電話端末と、簡易型携帯電話端末の電話番号とパスワードとリモート接続IDを予め登録し、パスワードとリモート接続IDを利用者に通知し、利用者の簡易型携帯電話端末からの電話番号とパスワードを受け、予め登録してある電話番号とパスワードと比較して一致するときは、一時的なパスワードを利用者の簡易型携帯電話端末に発行する認証装置と、簡易型携帯電話端末への一時的なパスワードの通知により利用者がパーソナルコンピュータを用いて行う接続要求を受け、認証装置に対しパスワードとリモート接続IDが正しいか問い合わせ、認証装置より正しいと通知された時のみ前記パーソナルコンピュータとネットワークサービスを接続させるリモート接続装置とを有することを特徴とする。

【0009】また、本発明の認証システムは、上記の目的を達成するため、利用者の正当性を確認してから当該利用者のパーソナルコンピュータからネットワークサービスの資源の利用を許可する認証システムに用いる認証装置において、利用者の簡易型携帯電話端末の電話番号とパスワードとリモート接続IDを予め登録し、パスワードとリモート接続IDを利用者に通知し、利用者の簡易型携帯電話端末からの電話番号とパスワードを受け、予め登録してある電話番号とパスワードと比較して一致するときは、一時的なパスワードを利用者の簡易型携帯電話端末に発行し、リモート接続装置からの問い合わせに対して正しいと判断した時は、リモート接続装置によりパーソナルコンピュータとネットワークサービスを接続させる構成としたものである。

【0010】本発明では、認証装置に登録した携帯電話端末だけが持つセキュリティと、利用者が携帯型電話端末に他するパスワードを管理することのセキュリティと、認証装置が一時的なパスワードを決められた利用者の携帯電話端末に送ることのセキュリティを組み合わせたセキュリティをもつことができる。

【0011】また、本発明ではPHS端末のような一般市販の簡易型携帯電話端末を使用して認証許可を得ることができる。

【0012】

【発明の実施の形態】次に、本発明の実施の形態について図面と共に説明する。図1は本発明になる認証システムの一実施の形態のブロック図を示す。同図において、利用者のパーソナルハンディホンシステム（PHS）端末1と、利用者のパーソナルコンピュータ（PC）2と、PHS端末1とPHS公衆回線を介して接続される認証装置3と、利用者PC2と認証装置3に接続されたリモート接続装置4と、リモート接続装置4が提供するネットワークサービス5とからなる。リモートLAN接続側の構成は、認証装置3、リモート接続装置4及びネットワーク5からなる。

【0013】認証装置3は利用者の正当性を確認する装置であり、利用者における「利用者パスワード要求／通知機能」の管理と、利用者からの接続要求に対し「一時的なパスワード」の発行と、「一時的なパスワード」を利用者パスワード要求／通知機能を持つ利用者PHS端末1と、リモート接続機能を持つリモート接続装置4への通知とを実行する。

【0014】リモート接続装置4は、認証装置3から発行された「一時的なパスワード」を基に、利用者接続用計算機システムである利用者PC2からの接続要求を受け付け、認証装置3に対して正規ユーザか問い合わせ利用者のリモート接続を行う。利用者PHS端末1は、利用者パスワード要求／通知機能を有する一般市販の簡易型携帯電話機であり、利用者が認証装置3に対して「一時的なパスワード」を要求し、正しく認証されれば、認証装置から「一時的なパスワード」が通知される。「一時的なパスワード」は予め定められた特定のものではなく、要求の都度適宜設定されるパスワードである。

【0015】利用者接続用計算機システムである利用者PC2は、認証装置から利用者PHS端末1に通知された「一時的なパスワード」に基づいて、リモート接続装置4に対して接続を行う。ネットワークサービス5は各利用者がサービスを受けるネットワークの資源である。

【0016】次に、この実施の形態の動作について図2のフローチャートを併せ参照して説明する。まず、認証装置3に利用者のPHS端末1のPHS番号、認証装置パスワード及びリモート接続IDを登録する（ステップ11）。続いて、認証装置パスワード及びリモート接続IDをあらかじめ利用者に通知する（ステップ12）。続いて、利用者は利用者PHS端末1から認証装置3に対して電話（TEL）をかける（ステップ13）。電話をかける方法は、例えば「認証装置電話番号#認証装置パスワード」の数字列である。例えば0238211234#ABCDである。

【0017】次に、認証装置3は利用者PHS端末1からの電話を受け、利用者PHS番号と認証装置パスワードを確認し（ステップ14）、それらの値がステップ11での登録情報と一致しているかどうか判断し、一致していれば利用者PHS端末1に対し、「これからパスワードを発行します。電源を切ってお待ち下さい。」等の音声メッセージで答える（ステップ15）。なお、音声メッセージ以外の文字メッセージその他の方法も可能である。

【0018】次に、利用者は上記の音声メッセージに従い、利用者PHS端末1の電源をオフにする（ステップ16）。続いて、認証装置3は、利用者PHS端末1に対し、「一時的なパスワード」を発行し、利用者PHS端末1に文字メッセージで通知する（ステップ17）。この場合、きやらめーる等のサービスを利用する。一時的なパスワードは、例えばVWXYZとする。

【0019】上記の一時的なパスワード「VWXYZ」が利用者のPHS端末1に通知されると（ステップ18）、利用者はリモート接続装置4に対してネットワーク接続要求を行う（ステップ19）。すなわち、利用者PC2を使用してリモート接続装置4に対してダイヤルアップを行う。この場合、IDはステップ11で入手したID、パスワードはステップ18で入手した「一時的なパスワード」を使用する。例えば、IDは「SUZUKI」であり、一時的なパスワードは「VWXYZ」である。

【0020】続いて、リモート接続装置4は利用者PC2から接続要求を受けると（ステップ20）、認証装置3に対してユーザID及びパスワードが正しいかどうか問い合わせる（ステップ21）。すると、認証装置3はリモート接続装置4からの問い合わせに対して利用者に発行した情報と一致するか判断する（ステップ22）。上記のステップ22で認証装置3が一致しているとの判断をした場合、その判断結果をリモート接続装置4に通知し、これによりリモート接続装置4はネットワークサービス5の利用を利用者に対して許可し、利用者PC2とネットワークサービス5との接続を行う（ステップ23）。

【0021】これにより、利用者PC2からネットワークサービス5の資源が利用可能となる（ステップ24）。なお、認証装置3がステップ22で不一致の判断結果を得た場合、リモート接続装置4はその判断結果を受け、利用者に対するネットワークサービス5の提供を拒否する。

【0022】このように、この実施の形態では、PHS端末1が自分のPHS番号を通知する機能があることを利用して、利用者が認証装置3に登録したPHS端末1だけを認証することで、他のPHS端末ではなりすましができにくいというセキュリティと、利用者のPHS端末1が例え盗難に遭っても、パスワードを知らないで認証装置3に接続できないため、利用者がPHS端末1に対するパスワードを管理することのセキュリティと、正しいPHS端末1に認証装置3が一時的なパスワードを発行することのセキュリティの組み合わせにより、非常に強固なセキュリティを持つため、第三者が不正にネットワークサービス5を利用することは極めて困難にできる。

【0023】また、利用者PHS端末1は市販のPHS

端末であり、小型、軽量、低消費電力の端末を利用できると共に、操作性が簡単であり、またこの実施の形態では、PHS公衆回線のインフラストラクチャを使用するので、高速・伝送効率の向上・高信頼性のデータ転送ができ、更にシステム全体の費用の削減も出切る。また、PHSの高速通信機能（PIAFS）を利用したサービスも可能となる。更に、この実施の形態では市販のPHS端末を利用することにより、量産効果のため価格が低く設定されており、生産性、保守性も高く、未使用PHS端末を使用することによる資源の再利用も可能である。

【0024】

【発明の効果】以上説明したように、本発明によれば、認証装置に登録した携帯電話端末だけが持つセキュリティと、利用者が携帯型電話端末に他するパスワードを管理することのセキュリティと、認証装置が一時的なパスワードを決められた利用者の携帯電話端末に送ることのセキュリティを組み合わせたセキュリティをもつようにしたため、従来に比べて非常に強固なセキュリティを向上できる。

【0025】また、本発明によれば、PHS端末のような一般市販の簡易型携帯電話端末を使用して認証許可を得るようにしているため、PHS公衆回線のインフラストラクチャを使用でき、よって高速・伝送効率向上・高信頼性のデータ転送ができる。更に、本発明によれば、PHS端末のような一般市販の簡易型携帯電話端末を使用しているため、端末として小型・軽量・低消費電力の端末や、生産性、保守性が高く、操作性も簡単な端末を使用でき、未使用PHS端末を使用することによる資源の再利用もでき、ひいてはシステム全体の費用を削減でき、高速通信機能を利用したサービスも受けることができる。

【図面の簡単な説明】

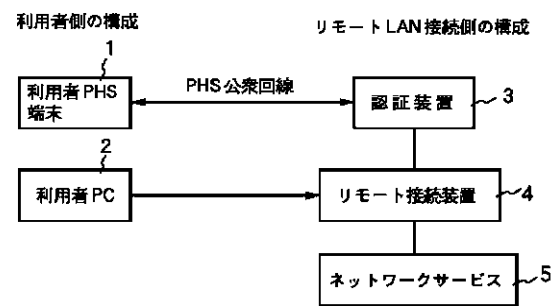
【図1】本発明の一実施の形態のブロック図である。

【図2】本発明の一実施の形態のフローチャートである。

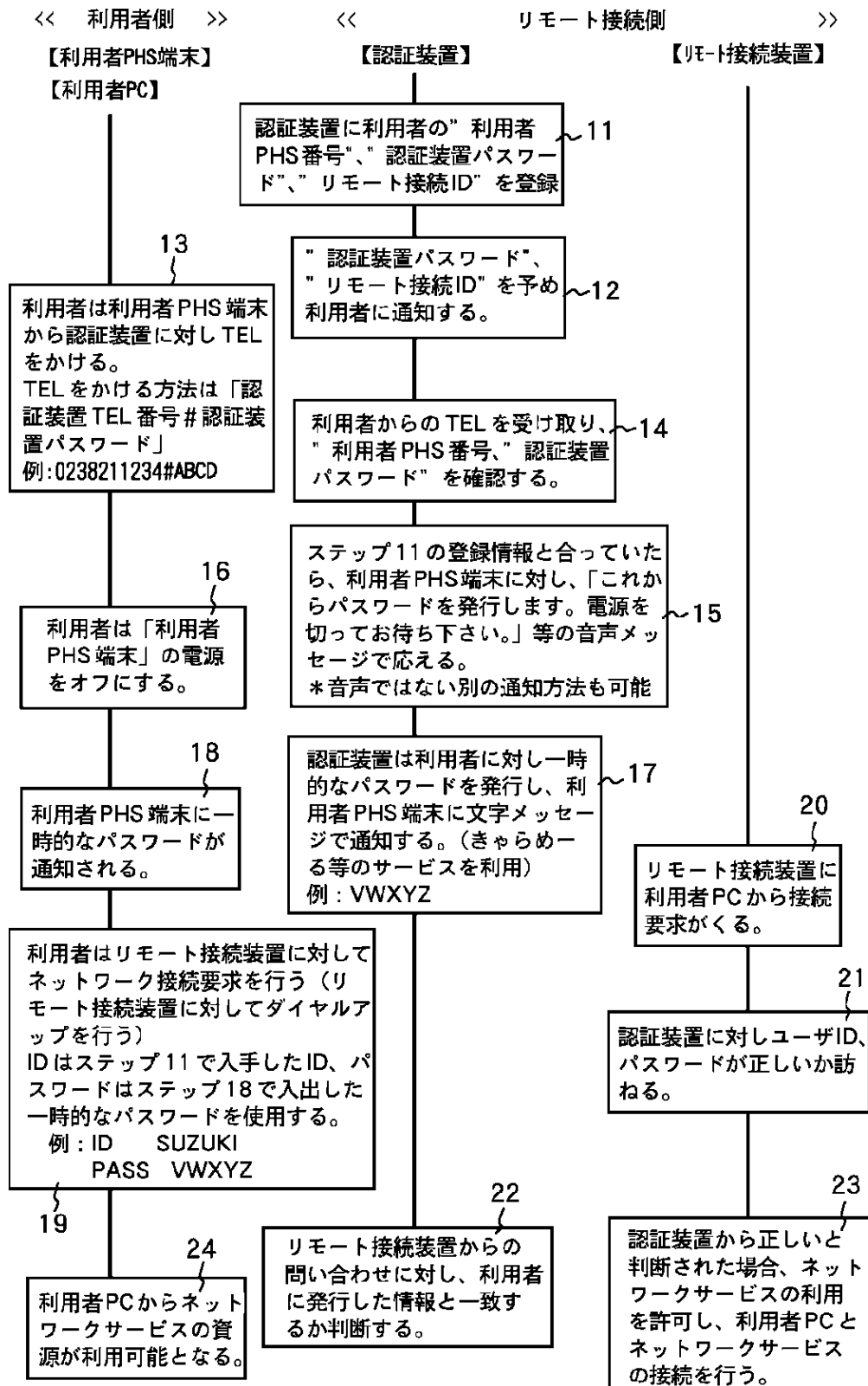
【符号の説明】

- 1 利用者のPHS端末
- 2 利用者のパーソナルコンピュータ（PC）
- 3 認証装置
- 4 リモート接続装置
- 5 ネットワークサービス

【図1】



【図2】



フロントページの続き

(51)Int.Cl. ⁷	識別記号	F I	ターマコード [*] (参考)
H 0 4 M 11/00	3 0 3	H 0 4 L 11/00	3 1 0 Z 5 K 1 0 1

F ターム(参考)	5B085 AA01 AC01 AE01 AE15 AE21 AE23 BG07 CE08 5J104 AA03 AA07 EA01 EA03 EA20 KA01 NA21 PA07 5K027 AA11 BB09 BB14 CC08 5K033 AA08 BA04 CB01 DB12 DB14 DB20 EC03 5K067 AA35 BB32 FF00 KK13 5K101 LL12	10
-----------	---	----