

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6844788号
(P6844788)

(45) 発行日 令和3年3月17日 (2021.3.17)

(24) 登録日 令和3年3月1日 (2021.3.1)

(51) Int. Cl.	F I
HO 4 M 11/00 (2006.01)	HO 4 M 11/00 3 O 1
HO 4 M 1/00 (2006.01)	HO 4 M 1/00 U
HO 4 L 9/32 (2006.01)	HO 4 L 9/00 6 7 3 A
	HO 4 L 9/00 6 7 5 B

請求項の数 7 (全 41 頁)

(21) 出願番号	特願2019-39047 (P2019-39047)	(73) 特許権者	313004654
(22) 出願日	平成31年3月4日 (2019.3.4)		株式会社ブラットフィールド
(62) 分割の表示	特願2015-173684 (P2015-173684)		兵庫県宝塚市安倉北2丁目18番27号
原出願日	平成27年9月3日 (2015.9.3)	(74) 代理人	100106013
(65) 公開番号	特開2019-118130 (P2019-118130A)		弁理士 田川 幸一
(43) 公開日	令和1年7月18日 (2019.7.18)	(72) 発明者	水田 猛
審査請求日	平成31年4月1日 (2019.4.1)		兵庫県宝塚市安倉北2丁目18番27号
		審査官	白川 瑞樹

最終頁に続く

(54) 【発明の名称】 情報通信システム

(57) 【特許請求の範囲】

【請求項 1】

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムにおいて、

前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行うシステムであって、

前記認証用機器は、当該認証用機器側の秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵とを生成して、当該認証側秘密鍵を記憶するとともに、当該認証側公開鍵を前記サービス用機器に送信する認証側登録部、を備えた認証側制御部を備え、

前記サービス用機器は、前記認証用機器から前記認証側公開鍵を受信すると、前記認証側公開鍵を前記特定のサービスに係る前記認証用機器の識別標識である内部ユーザIDに対応付けて記憶するとともに、当該内部ユーザIDを前記認証用機器に送信するサービス側登録部、を備えたサービス側制御部を備え、

前記サービス側制御部は、前記認証用機器から内部ユーザIDを指定した認証を求める情報を受信すると、当該サービス用機器において用意した任意のデータであるサービス側元データを前記サービス側登録部に記憶されている前記内部ユーザIDに対応する認証側公開鍵を用いて暗号化したデータであるサービス側暗号化データを前記認証用機器に送信するサービス側暗号部、を備え、

10

20

前記認証側制御部は、前記サービス用機器から受信したサービス側暗号化データを当該認証側登録部に記憶されている前記認証側秘密鍵を用いて復号化したデータであるサービス側復号化データに所定の演算を施して得られるサービス側演算化データを前記サービス用機器に送信する認証側復号部、を備え、

前記サービス側制御部は、前記認証用機器から受信したサービス側演算化データが、前記サービス側元データに当該所定の演算を施して得られるデータと一致する場合は、前記内部ユーザIDが真正であると判定する内部ユーザID真正判定部、を備え、

当該情報通信システムは、

複数の特定のサービスについて、それぞれの特定のサービスに係る内部ユーザIDの認証を行うための認証側公開鍵を当該内部ユーザIDと関連付けて当該特定のサービスを提供するサービス用機器に記憶させるとともに、当該認証側公開鍵に対応する認証側秘密鍵を前記認証用機器に記憶させておき、一の前記認証用機器を用いて、それぞれの特定のサービスについて内部ユーザIDの認証を実行することができるよう構成したこと、

を特徴とする、情報通信システム。

【請求項2】

請求項1の情報通信システムにおいて、

前記サービス側登録部は、さらに、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービスIDとともに、前記認証用機器に送信し、

前記認証側登録部は、さらに、前記サービス用機器から前記サービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービスIDと関連付けて記憶し、

前記認証側制御部は、前記サービス用機器からサービスIDを指定した認証を求める情報を受信すると、当該認証用機器において用意した任意のデータである認証側元データを前記認証側登録部に記憶されている前記サービスIDに対応する前記サービス側公開鍵を用いて暗号化したデータである認証側暗号化データを前記サービス用機器に送信する認証側暗号部、を備え、

前記サービス側制御部は、前記認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データを前記認証用機器に送信するサービス側復号部、を備え、

前記認証側制御部は、前記サービス用機器から受信した認証側演算化データが、前記認証側元データに当該所定の演算を施して得られるデータと一致する場合は、前記サービスIDが真正であると判定するサービスID真正判定部、を備え、

当該情報通信システムは、

複数の特定のサービスについて、それぞれの特定のサービスに係るサービスIDの認証を行うためのサービス側公開鍵を当該サービスIDと関連付けて前記認証用機器に記憶させるとともに、当該サービス側公開鍵に対応するサービス側秘密鍵をそれぞれの特定のサービスを提供する前記サービス用機器に記憶させておき、一の前記認証用機器を用いて、それぞれの特定のサービスについてサービスIDの認証を実行することができるよう構成したこと、

を特徴とする、情報通信システム。

【請求項3】

請求項1ないし2のいずれかの情報通信システムに用いられる前記サービス用機器。

【請求項4】

請求項1ないし2のいずれかの情報通信システムに用いられる前記認証用機器。

【請求項5】

コンピュータを、請求項3のサービス用機器のサービス側制御部、または、請求項4の認証用機器の認証側制御部として機能させるためのプログラム。

【請求項 6】

請求項 5 のプログラムを記憶した記録媒体。

【請求項 7】

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムであって、前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行う情報通信システム、を用いて行う情報通信方法であって、

前記認証用機器が、当該認証用機器側の秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵とを生成して、当該認証側秘密鍵を記憶するとともに、当該認証側公開鍵を前記サービス用機器に送信する認証側登録ステップと、

10

前記サービス用機器が、前記認証用機器から前記認証側公開鍵を受信すると、前記認証側公開鍵を前記特定のサービスに係る前記認証用機器の識別標識である内部ユーザ ID に対応付けて記憶するとともに、当該内部ユーザ ID を前記認証用機器に送信するサービス側登録ステップと、

前記サービス用機器が、前記認証用機器から内部ユーザ ID を指定した認証を求める情報を受信すると、当該サービス用機器において用意した任意のデータであるサービス側元データを前記サービス側登録部に記憶されている前記内部ユーザ ID に対応する認証側公開鍵を用いて暗号化したデータであるサービス側暗号化データを前記認証用機器に送信するサービス側暗号化ステップと、

20

前記認証用機器が、前記サービス用機器から受信したサービス側暗号化データを当該認証側登録部に記憶されている前記認証側秘密鍵を用いて復号化したデータであるサービス側復号化データに所定の演算を施して得られるサービス側演算化データを前記サービス用機器に送信する認証側復号ステップと、

前記サービス用機器が、前記認証用機器から受信したサービス側演算化データが、前記サービス側元データに当該所定の演算を施して得られるデータと一致する場合は、前記内部ユーザ ID が真正であると判定する内部ユーザ ID 真正判定ステップと、を備え、

当該情報通信方法は、

複数の特定のサービスについて、それぞれの特定のサービスに係る内部ユーザ ID の認証を行うための認証側公開鍵を当該内部ユーザ ID と関連付けて当該特定のサービスを提供するサービス用機器に記憶させるとともに、当該認証側公開鍵に対応する認証側秘密鍵を前記認証用機器に記憶させておき、一の前記認証用機器を用いて、それぞれの特定のサービスについて内部ユーザ ID の認証を実行することができるよう構成したこと、

30

を特徴とする、情報通信方法。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、情報通信システムに関し、とくに情報通信網に接続される複数の機器間におけるペアリングに関する。

【背景技術】

40

【0002】

たとえば、2つのクライアント端末（スマートフォンなど）が、同一時刻に同一地点に存在する場合、これらのクライアント端末間におけるペアリングを実現する方法として、シェーク処理やQRコード（登録商標、以下同様）処理が知られている（特許文献1の、段落[0211]～[0239]、図19、図20参照）。

【0003】

これらの方法を用いてペアリングを実現することで、事前に電話番号や電子メールアドレス等の個人情報を開示していない特定の相手との間で相互通信が可能となる、という利点がある。また、2つのクライアント端末間におけるペアリングを、インターネットなどの情報通信網を介して実現するので、クライアント端末同士が直接通信するための赤外線

50

通信手段やBluetooth（登録商標、以下同様）通信手段を備えていない場合でも、ペアリングが可能となる。

【0004】

しかし、上述のシェーク処理を実行するためには、双方のクライアント端末が、加速度センサーおよびGPS機能を備えていなければならないし、QRコード処理を実行するためには、少なくとも一方のクライアント端末は画像表示可能な表示装置を備え、他方のクライアント端末はカメラ機能を備えていなければならない。

【0005】

したがって、上述の方法は、どのようなタイプの機器にも適用できるものではないという問題があった。

10

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開2009-44591号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

この発明は、このような従来の問題を解決し、情報通信網に接続されるより多くのタイプの機器間においてペアリングを実現することができる情報通信システム等を提供することを目的とする。

20

【課題を解決するための手段】

【0008】

この発明による情報通信システムは、情報通信網に接続される複数の機器と、情報通信網に接続されるサーバ装置と、を備えた情報通信システムであって、複数の機器のうち第1の機器は、一定時間ごとに桁上げしつつ最下位桁に新たな文字を追加することで一定時間ごとに変化するよう構成された一定桁数の文字列である提供用文字列を当該第1の機器の表示装置に表示するとともに、提供用文字列を含むペアリング提供情報をサーバ装置に送信するペアリング提供処理を実行するペアリング提供処理部、を備えた第1制御部を備え、複数の機器のうち第2の機器は、第1の機器の表示装置に表示された提供用文字列に基づいて当該第2の機器の入力装置から入力された文字列である受諾用文字列を当該第2の機器の表示装置に表示するとともに、表示された受諾用文字列を含むペアリング受諾情報をサーバ装置に送信するペアリング受諾処理を実行するペアリング受諾処理部、を備えた第2制御部を備え、サーバ装置は、第1の機器から受信したペアリング提供情報に含まれる提供用文字列と、第2の機器から受信したペアリング受諾情報に含まれる受諾用文字列とを比較し、これらが一致すると判定したことを条件として、第1の機器と第2の機器との間にペアリングが成立したと判定するペアリング判定処理部、を備えたサーバ側制御部を備え、第2の機器のペアリング受諾処理部は、第1の機器における提供用文字列の変化に対応するために、変化前の提供用文字列に対応する受諾用文字列を桁上げしつつ最下位桁に当該第2の機器の入力装置から入力された新たな文字に対応する文字を追加することで変化後の提供用文字列に対応する受諾用文字列を生成する桁上げ処理部を備えたこと、を特徴とする。

30

40

【0009】

本発明の特徴は、上記のように広く示することができるが、その構成や内容は、目的および特徴とともに、図面を考慮に入れた上で、以下の開示によりさらに明らかになるであろう。

【発明の効果】

【0010】

本願の第1発明による情報通信システムは、情報通信網に接続される複数の機器と、情報通信網に接続されるサーバ装置と、を備えた情報通信システムであって、複数の機器のうち第1の機器は、一定時間ごとに桁上げしつつ最下位桁に新たな文字を追加することで

50

一定時間ごとに変化するよう構成された一定桁数の文字列である提供用文字列を当該第1の機器の表示装置に表示するとともに、提供用文字列を含むペアリング提供情報をサーバ装置に送信するペアリング提供処理を実行するペアリング提供処理部、を備えた第1制御部を備え、複数の機器のうち第2の機器は、第1の機器の表示装置に表示された提供用文字列に基づいて当該第2の機器の入力装置から入力された文字列である受諾用文字列を当該第2の機器の表示装置に表示するとともに、表示された受諾用文字列を含むペアリング受諾情報をサーバ装置に送信するペアリング受諾処理を実行するペアリング受諾処理部、を備えた第2制御部を備え、サーバ装置は、第1の機器から受信したペアリング提供情報に含まれる提供用文字列と、第2の機器から受信したペアリング受諾情報に含まれる受諾用文字列とを比較し、これらが一致すると判定したことを条件として、第1の機器と第2の機器との間にペアリングが成立したと判定するペアリング判定処理部、を備えたサーバ側制御部を備え、第2の機器のペアリング受諾処理部は、第1の機器における提供用文字列の変化に対応するために、変化前の提供用文字列に対応する受諾用文字列を桁上げしつつ最下位桁に当該第2の機器の入力装置から入力された新たな文字に対応する文字を追加することで変化後の提供用文字列に対応する受諾用文字列を生成する桁上げ処理部を備えたこと、を特徴とする。

10

【0011】

したがって、表示装置と入力装置とを備え情報通信網に接続される機器であれば、機器の種類を問わず、相互間でペアリングを成立させることが可能となる。

【0012】

20

そして、当該システムにおいては、第1の機器に表示される提供用文字列が一定時間ごとに変化するよう構成している。このように構成することで、提供用文字列の有効期限を短くすることができるため、偶然の一致や悪意の操作者による予期せぬペアリングの成立を抑制することができる。

【0013】

さらに、当該システムにおいては、第1の機器に表示される一定桁数の提供用文字列を、一定時間ごとに桁上げしつつ最下位桁に新たな文字を追加することで変化させるよう構成するとともに、第2の機器を、変化前の提供用文字列に対応する受諾用文字列を桁上げしつつ最下位桁に当該第2の機器の入力装置から入力された当該新たな文字に対応する文字を追加することで変化後の提供用文字列に対応する受諾用文字列を生成するよう構成している。このように構成することで、第2の機器の入力装置から受諾用文字列を入力している途中で第1の機器に表示される提供用文字列が変化した場合であっても、変化前の提供用文字列に対応する受諾用文字列に続いて当該新たな文字に対応する文字を入力することで、変化後の提供用文字列に対応する受諾用文字列の入力を完了することができる。したがって、第2の機器から受諾用文字列を入力する際、第1の機器における提供用文字列の変化に容易に対応することができる。

30

【0014】

このように、当該システムは、情報通信網に接続される多くのタイプの機器間においてペアリングを成立させることが可能であるうえ、予期せぬペアリングの成立を抑制をすることができ、かつ、第2の機器における受諾用文字列の入力が容易となっている。

40

【0015】

すなわち、当該システムは、情報通信網に接続されるより多くのタイプの機器間において、より実用的にペアリングを実現することができる。

【0016】

本願の第2発明による情報通信システムは、本願の第1発明による情報通信システムにおいて、第2の機器の桁上げ処理部は、第1の機器における提供用文字列の桁上げに同期して受諾用文字列の桁上げを行うよう構成されたこと、を特徴とする。

【0017】

したがって、第2の機器において、第1の機器における提供用文字列が変化したことを速やかに知ることができる。このため、変化後の提供用文字列に対応する受諾用文字列の

50

入力を速やかに行うことが可能となる。

【0018】

本願の第3発明による情報通信システムは、本願の第1ないし第2のいずれかの発明による情報通信システムにおいて、サーバ装置のペアリング判定処理部は、第2の機器から受信したペアリング受諾情報に含まれる受諾用文字列と一致する提供用文字列に対応する第1の機器が複数存在する場合は、当該複数の第1の機器に対して、再度、ペアリング提供処理を実行するよう促すとともに、当該第2の機器に対して、再度、ペアリング受諾処理を実行するよう指示する再ペアリング実行指示処理部、を備えたこと、を特徴とする。

【0019】

したがって、偶然の一致による予期せぬペアリングの成立を防止し、速やかに所望の第1の機器に対するペアリングを成立させることができる。

10

【0020】

本願の第4発明による情報通信システムは、本願の第1ないし第3のいずれかの発明による情報通信システムにおいて、第2の機器のペアリング受諾処理部は、サーバ装置のペアリング判定処理部において提供用文字列と受諾用文字列とが一致すると判定されたことを条件として、当該第2の機器の表示装置に確認用文字列を表示する確認用文字列表示処理部、を備え、第1の機器のペアリング提供処理部は、第2の機器の表示装置に表示された確認用文字列に基づいて第1の機器の入力装置から入力された文字列である応答用文字列を取得する応答用文字列取得処理部、を備え、サーバ装置のペアリング判定処理部は、第2の機器の表示装置に表示された確認用文字列と第1の機器によって取得された応答用文字列とが一致したことを条件として、第1の機器と第2の機器とのペアリングが成立したと判定するよう構成されたこと、を特徴とする。

20

【0021】

このように、第1の機器に表示された提供用文字列と、これを見て第2の機器から入力された受諾用文字列との一致に加え、これを前提として、第2の機器に表示された確認用文字列と、これを見て第1の機器から入力された応答用文字列とが一致したことを条件としてペアリングを成立させることで、悪意の操作者による予期せぬペアリングの成立を防止し、所望の第2の機器に対するペアリングを成立させることができる。

【0022】

本願の第5発明による情報通信システムは、本願の第1ないし第3のいずれかの発明による情報通信システムにおいて、当該情報通信システムは、複数の第2の機器を備え、1の第1の機器と複数の第2の機器とのペアリングを成立させるよう構成されたこと、を特徴とする。

30

【0023】

したがって、第1の機器の表示装置を目視できる範囲に第2の機器が複数存在する場合は、第1の機器とこれら複数の第2の機器との間でペアリングを成立させることができる。このため、たとえば、特定のグループ内で相互通信可能な状態を作り出すことができる。なお、グループの構成員数が多い場合は、第1の機器の表示装置として、スクリーン等の大画面を有する表示装置を用いることで対処することができる。また、第1の機器から地理的に遠い場所に存する構成員に対しては、第1の機器の表示装置として、中継表示可能な表示装置を用いることで対処することができる。

40

【0024】

本願の第6発明による情報通信システムは、本願の第1ないし第4のいずれかの発明による情報通信システムにおいて、第1および第2の機器の一方を、特定のサービスを提供する機器であるサービス用機器とし、他方を、当該特定のサービスを利用する際の認証を行う機器である認証用機器とし、サービス用機器と認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行うシステムであって、認証用機器は、当該認証用機器側の秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵とを生成して、当該認証側秘密鍵を記憶するとともに、当該認証側公開鍵をサービス用機器に送信する認証側登録部、を備えた認証側制御部を備

50

え、サービス用機器は、認証用機器から認証側公開鍵を受信すると、特定のサービスに係る認証用機器の識別標識である内部ユーザIDを生成し、認証側公開鍵を当該内部ユーザIDに対応付けて記憶するとともに、当該内部ユーザIDを認証用機器に送信するサービス側登録部、を備えたサービス側制御部を備え、サービス側制御部は、認証用機器から内部ユーザIDを指定した認証を求める情報を受信すると、当該サービス用機器において用意した任意のデータであるサービス側元データをサービス側登録部に記憶されている内部ユーザIDに対応する認証側公開鍵を用いて暗号化したデータであるサービス側暗号化データを認証用機器に送信するサービス側暗号部、を備え、認証側制御部は、サービス用機器から受信したサービス側暗号化データを当該認証側登録部に記憶されている認証側秘密鍵を用いて復号化したデータであるサービス側復号化データに所定の演算を施して得られるサービス側演算化データをサービス用機器に送信する認証側復号部、を備え、サービス側制御部は、認証用機器から受信したサービス側演算化データが、サービス側元データに当該所定の演算を施して得られるデータと一致する場合は、内部ユーザIDが真正であると判定する内部ユーザID真正判定部、を備えたこと、を特徴とする。

10

【0025】

したがって、サービス用機器と認証用機器とのペアリング成立による相互通信可能な状態を利用して、認証側公開鍵をサービス用機器に送信して記憶させることで、認証側公開鍵のサービス用機器への送信及び登録を、安全かつ容易に行うことができる。また、ペアリング成立による相互通信可能な状態を利用して、サービス用機器と認証用機器との間で認証側公開鍵及び認証側秘密鍵の対応性を確認することで、サービス用機器による内部ユーザIDの認証を安全かつ容易に行うことができる。このように、サービス用機器と認証用機器との間のペアリング成立を利用することで、内部ユーザIDの認証に関して、安全性の高い公開鍵認証方式を容易に実現することができる。このため、サービス利用者のなりすましを容易に防止することができる。

20

【0026】

ところで、従来行われている共通鍵認証方式では、特定のサービス（たとえば特定のソフトウェア）を利用する場合、ユーザIDを用いて利用者を特定するとともに、パスワードを用いて利用者の認証を行うのが一般的であるため、利用するサービスの種類が増加するにしたがって、ユーザIDとパスワードが増加し、これらの管理が煩雑となる。

【0027】

一方、この発明によると、利用者を特定するための内部ユーザIDは、サービス用機器において生成され認証用機器に送信されている。また、利用者の認証を行うための認証側公開鍵は内部ユーザIDと関連付けてサービス用機器に記憶され、この認証側公開鍵に対応する認証側秘密鍵は認証用機器に記憶されている。このため、複数のサービスについて、上記各情報を認証用機器および各サービス機器に記憶させておけば、サービス用機器と認証用機器との間のペアリングが成立すれば、あとは自動的に内部ユーザIDの認証を実行することが可能となる。したがって、サービスの利用者は、自己の認証用機器をユニバーサルキー（汎用鍵）として用いることで、それぞれのサービスについて内部ユーザIDの認証を実行することができ、従来のようにサービスごとにユーザIDおよびパスワードを記憶しておく必要はない。

30

40

【0028】

本願の第7発明による情報通信システムは、本願の第6発明による情報通信システムにおいて、サービス側登録部は、さらに、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービスIDとともに、認証用機器に送信し、認証側登録部は、さらに、サービス用機器からサービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービスIDと関連付けて記憶し、認証側制御部は、サービス用機器からサービスIDを指定した認証を求める情報を受信すると、当該認証用機器において用意した任意のデータである認証側元データを認証側登録部に記憶されているサービスID

50

に対応するサービス側公開鍵を用いて暗号化したデータである認証側暗号化データをサービス用機器に送信する認証側暗号部、を備え、サービス側制御部は、認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データを認証用機器に送信するサービス側復号部、を備え、認証側制御部は、サービス用機器から受信した認証側演算化データが、認証側元データに当該所定の演算を施して得られるデータと一致する場合は、サービスIDが真正であると判定するサービスID真正判定部、を備えたこと、を特徴とする。

【0029】

したがって、サービス用機器と認証用機器とのペアリング成立による相互通信可能な状態を利用して、サービス側公開鍵を認証用機器に送信して記憶させることで、サービス側公開鍵の認証用機器への送信及び登録を、安全かつ容易に行うことができる。また、ペアリング成立による相互通信可能な状態を利用して、サービス用機器と認証用機器との間でサービス側公開鍵及びサービス側秘密鍵の対応性を確認することで、認証用機器によるサービスIDの認証を安全かつ容易に行うことができる。このように、サービス用機器と認証用機器との間のペアリング成立を利用することで、サービスIDの認証に関して、安全性の高い公開鍵認証方式を容易に実現することができる。このため、サービス提供側のなりすましを容易に防止することができる。

【0030】

さらに、この発明によると、サービスIDの認証を行うためのサービス側公開鍵はサービスIDと関連付けて認証用機器に記憶され、このサービス側公開鍵に対応するサービス側秘密鍵はサービス用機器に記憶されている。このため、複数のサービスについて、上記各情報を認証用機器および各サービス機器に記憶させておけば、サービス用機器と認証用機器との間のペアリングが成立すれば、あとは自動的にサービスIDの認証を実行することが可能となる。したがって、サービスの利用者は、自己の認証用機器をユニバーサルキー（汎用鍵）として用いることで、それぞれのサービスについてサービスIDの認証を実行することができ、安全かつ容易に各サービスを利用することができる。

【0031】

また、内部ユーザIDの認証に加え、サービスIDの認証をも公開鍵認証方式を用いて行うことで、サービス用機器により提供されるサービスの利用を、より安全なものとする

【0032】

本願の第8発明による情報通信システムは、本願の第1ないし第4のいずれかの発明による情報通信システムにおいて、第1および第2の機器の一方を、特定のサービスを提供する機器であるサービス用機器とし、他方を、当該特定のサービスを利用する際の認証を行う機器である認証用機器とし、サービス用機器と認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行うシステムであって、サービス用機器は、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービスIDとともに、認証用機器に送信するサービス側登録部、を備えたサービス側制御部を備え、認証用機器は、サービス用機器からサービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービスIDと関連付けて記憶する認証側登録部、を備えた認証側制御部を備え、認証側制御部は、サービス用機器からサービスIDを指定した認証を求める情報を受信すると、当該認証用機器において用意した任意のデータである認証側元データを前記認証側登録部に記憶されているサービスIDに対応するサービス側公開鍵を用いて暗号化したデータである認証側暗号化データをサービス用機器に送信する認証側暗号部、を備え、サービス側制御部は、認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データ

を認証用機器に送信するサービス側復号部、を備え、認証側制御部は、サービス用機器から受信した認証側演算化データが、認証側元データに当該所定の演算を施して得られるデータと一致する場合は、サービスIDが真正であると判定するサービスID真正判定部、を備えたこと、を特徴とする。

【0033】

したがって、サービス用機器と認証用機器とのペアリング成立による相互通信可能な状態を利用して、サービス側公開鍵を認証用機器に送信して記憶させることで、サービス側公開鍵の認証用機器への送信及び登録を、安全かつ容易に行うことができる。また、ペアリング成立による相互通信可能な状態を利用して、サービス用機器と認証用機器との間でサービス側公開鍵及びサービス側秘密鍵の対応性を確認することで、認証用機器によるサービスIDの認証を安全かつ容易に行うことができる。このように、サービス用機器と認証用機器との間のペアリング成立を利用することで、サービスIDの認証に関して、安全性の高い公開鍵認証方式を容易に実現することができる。このため、サービス提供側のなりすましを容易に防止することができる。

10

【0034】

さらに、この発明によると、サービスIDの認証を行うためのサービス側公開鍵はサービスIDと関連付けて認証用機器に記憶され、このサービス側公開鍵に対応するサービス側秘密鍵はサービス用機器に記憶されている。このため、複数のサービスについて、上記各情報を認証用機器および各サービス機器に記憶させておけば、サービス用機器と認証用機器との間のペアリングが成立すれば、あとは自動的にサービスIDの認証を実行することが可能となる。したがって、サービスの利用者は、自己の認証用機器をユニバーサルキー（汎用鍵）として用いることで、それぞれのサービスについてサービスIDの認証を実行することができ、安全かつ容易に各サービスを利用することができる。

20

【0035】

このように、サービス用機器と認証用機器とのペアリング成立による相互通信可能な状態を利用することで、従来、一般的なユーザでは困難であったサービスIDの認証を実行することができ、サービス提供側のなりすましを容易に防止することができる。

【0036】

本願の第9発明によるサーバ装置は、本願の第1ないし第8のいずれかの発明による情報通信システムに用いられるサーバ装置である。

30

【0037】

したがって、これらのサーバ装置を情報通信システムに用いることで、上記第1ないし第8のいずれかの発明と同様の効果を奏する。

【0038】

本願の第10発明による第1の機器は、本願の第1ないし第8のいずれかの発明による情報通信システムに用いられる第1の機器である。

【0039】

したがって、この第1の機器を情報通信システムに用いることで、上記第1ないし第8のいずれかの発明と同様の効果を奏する。

【0040】

本願の第11発明による第2の機器は、本願の第1ないし第8のいずれかの発明による情報通信システムに用いられる第2の機器である。

40

【0041】

したがって、この第2の機器を情報通信システムに用いることで、上記第1ないし第8のいずれかの発明と同様の効果を奏する。

【0042】

本願の第12発明によるサービス用機器は、本願の第6ないし第8のいずれかの発明による情報通信システムに用いられるサービス用機器である。

【0043】

したがって、このサービス用機器を情報通信システムに用いることで、上記第6ないし

50

第 8 のいずれかの発明と同様の効果を奏する。

【0044】

本願の第 13 発明による認証用機器は、本願の第 6 ないし第 8 のいずれかの発明による情報通信システムに用いられる認証用機器である。

【0045】

したがって、この認証用機器を情報通信システムに用いることで、上記第 6 ないし第 8 のいずれかの発明と同様の効果を奏する。

【0046】

本願の第 14 発明によるプログラムは、コンピュータを、本願の第 9 発明によるサーバ装置のサーバ側制御部、第 10 発明による第 1 の機器の第 1 制御部、第 11 発明による第 2 の機器の第 2 制御部、第 12 発明によるサービス用機器のサービス側制御部、または、第 13 発明による認証用機器の認証側制御部として機能させるためのプログラムである。

【0047】

したがって、当該プログラムをコンピュータに実行させることで、上記第 9 ないし第 13 のいずれかの発明と同様の効果を奏する。

【0048】

本願の第 15 発明による記録媒体は、本願の第 14 発明によるプログラムを記憶した記録媒体である。

【0049】

したがって、これらの記録媒体に記憶されたプログラムをコンピュータに実行させることで、上記第 14 発明と同様の効果を奏する。

【0050】

また、本願の第 16 発明による情報通信方法は、情報通信網に接続される複数の機器と、情報通信網に接続されるサーバ装置と、を備えた情報通信システムを用いて行う情報通信方法であって、複数の機器のうち第 1 の機器が、一定時間ごとに桁上げしつつ最下位桁に新たな文字を追加することで一定時間ごとに変化するよう構成された一定桁数の文字列である提供用文字列を当該第 1 の機器の表示装置に表示するとともに、提供用文字列を含むペアリング提供情報をサーバ装置に送信するペアリング提供処理を実行するペアリング提供処理ステップと、複数の機器のうち第 2 の機器が、第 1 の機器の表示装置に表示された提供用文字列に基づいて当該第 2 の機器の入力装置から入力された文字列である受諾用文字列を当該第 2 の機器の表示装置に表示するとともに、表示された受諾用文字列を含むペアリング受諾情報をサーバ装置に送信するペアリング受諾処理を実行するペアリング受諾処理ステップと、サーバ装置が、第 1 の機器から受信したペアリング提供情報に含まれる提供用文字列と、第 2 の機器から受信したペアリング受諾情報に含まれる受諾用文字列とを比較し、これらが一致すると判定したことを条件として、第 1 の機器と第 2 の機器との間にペアリングが成立したと判定するペアリング判定処理ステップと、を備え、ペアリング受諾処理ステップは、第 1 の機器における提供用文字列の変化に対応するために、第 2 の機器が、変化前の提供用文字列に対応する受諾用文字列を桁上げしつつ最下位桁に当該第 2 の機器の入力装置から入力された新たな文字に対応する文字を追加することで変化後の提供用文字列に対応する受諾用文字列を生成する桁上げ処理ステップを備えたこと、を特徴とする。

【0051】

したがって、サーバ装置、第 1 の機器および第 2 の機器を用いて当該方法を使用することで、上記第 1 発明と同様の効果を奏する。

【0052】

なお、上記各発明における「ペアリング」とは、2 つの機器間で相手を特定して情報通信網を介する通信を確立することをいう。

【図面の簡単な説明】

【0053】

【図 1】図 1 は、この発明の一実施形態による情報通信システム 2 の構成を示すブロック

10

20

30

40

50

図である。

【図 2】図 2 は、第 1 の機器 6、第 2 の機器 7 およびサーバ装置 4 の構成を例示するブロック図である。

【図 3】図 3 は、応用例としての情報通信システム 2 を構成する、サービス用機器 40 および認証用機器 30 の構成を例示するブロック図である。

【図 4】図 4 は、図 2 または図 3 に示すサーバ装置 4、第 1 の機器 6 および第 2 の機器 7（第 1 の機器 6 または第 2 の機器 7 でもある認証用機器 30 またはサービス用機器 40 を含む。）のハードウェア構成の一例を示すブロック図である。

【図 5】図 5 は、本願におけるペアリング処理の流れの一例を示すフローチャートである。

10

【図 6】図 6 は、本願におけるペアリング処理の流れの一例を示すフローチャートである。

【図 7】図 7 は、本願におけるペアリング処理の流れの一例を示すフローチャートである。

【図 8】図 8 は、本願におけるペアリング処理の流れの一例を示すフローチャートである。

【図 9】図 9 は、本願におけるペアリング処理の流れの一例を示すフローチャートである。

【図 10】図 10 は、本願におけるペアリング処理の流れの一例を示すフローチャートである。

20

【図 11】図 11 A、図 11 B、図 11 C、図 11 D は、ペアリング処理におけるプロバイダ 6 の表示画面の一例を示す図面である。

【図 12】図 12 A、図 12 B、図 12 C、図 12 D は、ペアリング処理におけるレジスタ 7 の表示画面の一例を示す図面である。

【図 13】図 13 A、図 13 B は、ペアリング処理におけるレジスタ 7 の表示画面の一例を示す図面である。

【図 14】図 14 は、ペアリング処理におけるプロバイダ 6 およびレジスタ 7 a、レジスタ 7 b、レジスタ 7 c の表示画面の一例を示す図面である。

【図 15】図 15 A は、ペアリング処理におけるレジスタ 7 の表示画面の一例を示す図面である。図 15 B は、ペアリング処理におけるプロバイダ 6 の表示画面の一例を示す図面である。

30

【図 16】図 16 は、待受けテーブル 26 のデータ構成の一例を示す図面である。

【図 17】図 17 A、図 17 B は、ペアリング処理における一部の処理を説明するための図面である。

【図 18】図 18 は、本願のペアリング処理を利用した認証処理の流れの一例を示すフローチャートである。

【図 19】図 19 は、本願のペアリング処理を利用した認証処理の流れの一例を示すフローチャートである。

【図 20】図 20 は、本願のペアリング処理を利用した認証処理の流れの一例を示すフローチャートである。

40

【図 21】図 21 は、本願のペアリング処理を利用した認証処理の流れの一例を示すフローチャートである。

【図 22】図 22 は、本願のペアリング処理を利用した認証処理の流れの一例を示すフローチャートである。

【図 23】図 23 は、認証処理における認証用機器 30 およびサービス用機器 40 の表示画面の推移の一例を示す図面である。

【図 24】図 24 は、認証処理における認証用機器 30 およびサービス用機器 40 の表示画面の推移の一例を示す図面である。

【図 25】図 25 は、認証側テーブル 36 のデータ構成の一例を示す図面である。

【図 26】図 26 は、サービス側テーブル 46 のデータ構成の一例を示す図面である。

50

【発明を実施するための形態】

【0054】

図1は、この発明の一実施形態による情報通信システム2の構成を示すブロック図である。情報通信システム2は、情報通信網8に接続される複数の機器としての第1の機器6および第2の機器7と、情報通信網8に接続されるサーバ装置4と、を備えている。

【0055】

なお、図1は、1の第1の機器6と1の第2の機器7とのペアリングを成立させる場合の例であるが、1の第1の機器6と複数の第2の機器7とのペアリングを成立させるよう構成することもできる（後述）。

【0056】

つぎに、図2は、第1の機器6、第2の機器7およびサーバ装置4の構成を例示するブロック図である。

【0057】

図2に示すように、第1の機器6は第1制御部10を備えている。第1制御部10はペアリング提供処理部11を備えている。

【0058】

ペアリング提供処理部11はペアリング提供処理を実行する。ペアリング提供処理において、提供用文字列が第1の機器6の表示装置に表示される。提供用文字列は、一定時間ごとに桁上げしつつ最下位桁に新たな文字を追加することで一定時間ごとに変化するよう構成された一定桁数の文字列である。また、ペアリング提供処理において、提供用文字列を含むペアリング提供情報がサーバ装置4に送信される。

【0059】

第2の機器7は、第2制御部15を備えている。第2制御部15はペアリング受諾処理部16を備えている。

【0060】

ペアリング受諾処理部16はペアリング受諾処理を実行する。ペアリング受諾処理において、受諾用文字列が第2の機器7の表示装置に表示される。受諾用文字列は、第1の機器6の表示装置に表示された提供用文字列に基づいて第2の機器7の入力装置から入力された文字列である。また、ペアリング受諾処理において、受諾用文字列を含むペアリング受諾情報がサーバ装置4に送信される。

【0061】

ペアリング受諾処理部16は桁上げ処理部17を備えている。桁上げ処理部17は、第1の機器6における提供用文字列の変化に対応するために、変化前の提供用文字列に対応する受諾用文字列を桁上げしつつ最下位桁に第2の機器7の入力装置から入力された新たな文字に対応する文字を追加することで、変化後の提供用文字列に対応する受諾用文字列を生成する。

【0062】

桁上げ処理部17は、さらに、第1の機器6における提供用文字列の桁上げに同期して受諾用文字列の桁上げを行うよう構成されている。

【0063】

サーバ装置4はサーバ側制御部20を備えている。サーバ側制御部20はペアリング判定処理部21を備えている。

【0064】

ペアリング判定処理部21は、第1の機器6から受信したペアリング提供情報に含まれる提供用文字列と、第2の機器7から受信したペアリング受諾情報に含まれる受諾用文字列とを比較し、これらが一致すると判定したことを条件として、第1の機器6と第2の機器7との間にペアリングが成立したと判定する。

【0065】

ペアリング判定処理部21は、さらに、再ペアリング実行指示処理部22を備えている。

10

20

30

40

50

【0066】

再ペアリング実行指示処理部22は、第2の機器7から受信したペアリング受諾情報に含まれる受諾用文字列と一致する提供用文字列に対応する第1の機器6が複数存在する場合は、複数の第1の機器6に対して、再度、ペアリング提供処理を実行するよう促すとともに、第2の機器7に対して、再度、ペアリング受諾処理を実行するよう指示する。

【0067】

第2の機器7のペアリング受諾処理部16は、さらに、確認用文字列表示処理部18を備えている。

【0068】

確認用文字列表示処理部18は、サーバ装置4のペアリング判定処理部21において提供用文字列と受諾用文字列とが一致すると判定されたことを条件として、第2の機器7の表示装置に確認用文字列を表示する。

10

【0069】

第1の機器6のペアリング提供処理部11は、さらに、応答用文字列取得処理部12を備えている。

【0070】

応答用文字列取得処理部12は応答用文字列を取得する。応答用文字列は、第2の機器7の表示装置に表示された確認用文字列に基づいて第1の機器6の入力装置から入力された文字列である。

【0071】

20

サーバ装置4のペアリング判定処理部21は、さらに、第2の機器7の表示装置に表示された確認用文字列と第1の機器6によって取得された応答用文字列とが一致したことを条件として、第1の機器6と第2の機器7とのペアリングが成立したと判定するよう構成されている。

【0072】

サーバ装置4はデータベース25を備えている。データベース25は待受けテーブル26を備えている。待受けテーブル26については後述する。

【0073】

つぎに、図3は、応用例としての情報通信システム2を構成する、サービス用機器40および認証用機器30の構成を例示するブロック図である。

30

【0074】

サービス用機器40は特定のサービスを提供する機器である。認証用機器30は特定のサービスを利用する際の認証を行う機器である。

【0075】

図3に示す情報通信システム2は、第1の機器6および第2の機器7の一方を、サービス用機器40とし、他方を認証用機器30として、サービス用機器40と認証用機器30とのペアリングが成立したことを前提に、特定のサービスを利用可能とするための認証を行うシステムである。

【0076】

図3に示すように、認証用機器30は認証側制御部31を備えている。認証側制御部31は認証側登録部32を備えている。

40

【0077】

認証側登録部32は、認証用機器30側の秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵とを生成して、当該認証側秘密鍵を記憶するとともに、当該認証側公開鍵をサービス用機器40に送信する。

【0078】

サービス用機器40はサービス側制御部41を備えている。サービス側制御部41はサービス側登録部42を備えている。

【0079】

サービス側登録部42は、認証用機器30から認証側公開鍵を受信すると、特定のサー

50

ビスに係る認証用機器 30 の識別標識である内部ユーザ I D を生成し、認証側公開鍵を当該内部ユーザ I D に対応付けて記憶するとともに、当該内部ユーザ I D を認証用機器 30 に送信する。

【0080】

サービス用機器 40 のサービス側制御部 41 は、サービス側暗号部 43 を備えている。

【0081】

サービス側暗号部 43 は、認証用機器 30 から内部ユーザ I D を指定した認証を求める情報を受信すると、サービス側暗号化データを生成し、認証用機器 30 に送信する。サービス側暗号化データは、当該サービス用機器 40 において用意した任意のデータであるサービス側元データを、サービス側登録部 42 に記憶されている内部ユーザ I D に対応する
10

認証側公開鍵を用いて暗号化したデータである。

【0082】

認証用機器 30 の認証側制御部 31 は、認証側復号部 34 を備えている。

【0083】

認証側復号部 34 は、サービス側復号化データに所定の演算を施して得られるサービス側演算化データをサービス用機器 40 に送信する。サービス側復号化データは、サービス用機器 40 から受信したサービス側暗号化データを、当該認証側登録部 32 に記憶されている認証側秘密鍵を用いて復号化したデータである。

【0084】

サービス用機器 40 のサービス側制御部 41 は内部ユーザ I D 真正判定部 45 を備えて
20

いる。

【0085】

内部ユーザ I D 真正判定部 45 は、認証用機器 30 から受信したサービス側演算化データが、サービス側元データに当該所定の演算を施して得られるデータと一致する場合は、内部ユーザ I D が真正であると判定する。

【0086】

サービス側登録部 42 は、さらに、当該サービス用機器 40 側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器 40 に係る特定のサービスの識別標識であるサービス I D とともに、認証用機器 30
30

に送信する。

【0087】

認証側登録部 32 は、さらに、サービス用機器 40 からサービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービス I D と関連付けて記憶する。

【0088】

認証用機器 30 の認証側制御部 31 は、認証側暗号部 33 を備えている。

【0089】

認証側暗号部 33 は、サービス用機器 40 からサービス I D を指定した認証を求める情報を受信すると、認証側暗号化データを生成し、サービス用機器 40 に送信する。認証側暗号化データは、当該認証用機器 30 において用意した任意のデータである認証側元データを、認証側登録部 32 に記憶されているサービス I D に対応するサービス側公開鍵を用いて暗号化したデータである。
40

【0090】

サービス用機器 40 のサービス側制御部 41 は、サービス側復号部 44 を備えている。

【0091】

サービス側復号部 44 は、認証側復号化データに所定の演算を施して得られる認証側演算化データを認証用機器 30 に送信する。認証側復号化データは、認証用機器 30 から受信した認証側暗号化データを、当該サービス側登録部 42 に記憶されているサービス側秘密鍵を用いて復号化したデータである。

【0092】

認証用機器 30 の認証側制御部 31 は、サービス ID 真正判定部 35 を備えている。

【0093】

サービス ID 真正判定部 35 は、サービス用機器 40 から受信した認証側演算化データが、認証側元データに当該所定の演算を施して得られるデータと一致する場合は、サービス ID が真正であると判定する。

【0094】

認証用機器 30 は認証側テーブル 36 を備えている。サービス用機器 40 はサービス側テーブル 46 を備えている。これらのテーブル 36、46 については後述する。

【0095】

つぎに、図 4 は、図 2 または図 3 に示すサーバ装置 4、第 1 の機器 6 および第 2 の機器 7（第 1 の機器 6 または第 2 の機器 7 でもある認証用機器 30 またはサービス用機器 40 を含む。以下同様。）のハードウェア構成の一例を示すブロック図である。

10

【0096】

サーバ装置 4 は、とくに限定されるものではないが、この例では、一般的なサーバコンピュータと同様の構成である。

【0097】

サーバ装置 4 は、情報通信システム 2 のサーバ装置 4 側のプログラムを記憶した記録媒体であり、データベース 25 の記憶媒体でもあるハードディスクを備えた HDD（ハードディスクドライブ）等の補助記憶装置 55、補助記憶装置 55 に記憶されたプログラムがロードされる主記憶装置 54、主記憶装置 54 にロードされたプログラムを実行するサーバ側制御部 20 に対応する CPU 51、LCD（液晶表示装置）等の表示装置 52、キーボード、マウス、トラックパッド等の入力装置 53、および、情報通信網 8 を介して第 1 の機器 6 または第 2 の機器 7 と通信するための通信インタフェース 56 を備えている。

20

【0098】

第 1 の機器 6 は、とくに限定されるものではなく、たとえばパーソナルコンピュータであってもよいし、タブレット型コンピュータであってもよいし、携帯情報端末装置であってもよいし、いわゆるスマートフォンに代表される携帯電話機であってもよい。さらに、家庭用電気機器、生産用機器、自動車などの運輸用機器であってもよい。第 2 の機器 7 についても同様である。要は、情報通信網 8 に接続される機器であれば、第 1 の機器 6 または第 2 の機器 7 として、本願発明を適用することができる。

30

【0099】

図 4 は、第 1 の機器 6 および第 2 の機器 7 が、いずれもスマートフォンである場合のハードウェア構成を例示したものである。

【0100】

第 1 の機器 6 は、情報通信システム 2 の第 1 の機器 6 側のプログラムを記憶した記録媒体であるフラッシュメモリを搭載した SSD（ソリッドステートドライブ）等の補助記憶装置 65、補助記憶装置 65 に記憶されたプログラムがロードされる主記憶装置 64、主記憶装置 64 にロードされたプログラムを実行する第 1 制御部 10 に対応する CPU 61、LCD（液晶表示装置）等の表示装置 62、入力キー、タッチパネル等の入力装置 63、および、情報通信網 8 を介してサーバ装置 4 および第 2 の機器 7 と通信するための通信インタフェース 66、を備えている。

40

【0101】

第 2 の機器 7 も、第 1 の機器 6 と同様のハードウェア構成である。

【0102】

情報通信網 8 は、情報を伝達するための通信ネットワークであって、有線、無線の別を問わない。情報通信網 8 として、インターネットに代表される WAN（Wide Area Network）、LAN（Local Area Network）等のコンピュータネットワーク、電話回線（携帯電話回線を含む。以下同様。）あるいはこれらを組合わせたものが例示される。

【0103】

50

つぎに、図5～図10は、本願におけるペアリングを実行する処理（以下、「ペアリング処理」ということがある。）の流れの一例を示すフローチャートである。以下、サーバ装置4をサーバ4、第1の機器6をプロバイダ6、第2の機器7をレジスタ7ということがある。また、情報通信網8として、インターネット、または、インターネットと電話回線とを組み合わせたものを例に説明する。

【0104】

図11A～図15Bは、ペアリング処理における、プロバイダ6またはレジスタ7の表示画面の一例を示す図面である。図16は、待受けテーブル26のデータ構成の一例を示す図面である。図17A、図17Bは、ペアリング処理における一部の処理を説明するための図面である。

10

【0105】

図5～図17Bを参照しつつ、ペアリング処理について説明する。

【0106】

図5に示すように、プロバイダ6のCPU61（以下、単に「プロバイダ6」ということがある。）は、提供用文字列の表示指示の有無を監視している（ステップS1）。

【0107】

ステップS1において、プロバイダ6の入力装置63（以下、単に「プロバイダ6」ということがある。）から、提供用文字列の表示指示が入力されると、ストリームシードを生成し、生成したストリームシードとタイムヘッダとの組み合わせであるストリームシードデータを、プロバイダ6の記憶装置、すなわち、主記憶装置64または補助記憶装置65（以下、単に「プロバイダ6」ということがある。）に記憶するとともに、サーバ4に送信する。（ステップS2）。

20

【0108】

ストリームシードとは、提供用文字列の素となる文字列であって、提供用文字列の桁数より大きい桁数の文字列である。ストリームシードの構成はとくに限定されるものではないが、たとえば、乱数により構成することができる。

【0109】

なお、提供用文字列の文字種および文字数は、とくに限定されるものではないが、この実施形態においては、提供用文字列が4桁の数字である場合を例に説明することとする。そして、ストリームシードを183桁の数字としている。この理由については後述する。

30

【0110】

タイムヘッダは、ストリームシードから提供用文字列を抽出するタイミングの基準となる時刻である。タイムヘッダの決定方法については、後述する。

【0111】

サーバ4のCPU51（以下、単に「サーバ4」ということがある。）は、ストリームシードデータを受信すると、待受けテーブル26を検索し、受信したストリームシードデータに一致する既登録のストリームシードデータが存在するか否かをチェックする（ステップS3、ステップS4）。

【0112】

受信したストリームシードデータに一致する既登録のストリームシードデータが存在する場合は、プロバイダ6に対し、ストリームシードデータ再生の要求を送信し、要求を受けたプロバイダ6は、ステップS2に制御を戻す（ステップS5）。

40

【0113】

一方、ステップS4において、受信したストリームシードデータに一致する既登録のストリームシードデータが存在しない場合、サーバ4は、当該ペアリング（セッション）を特定する識別標識としてプロバイダIDを生成し、プロバイダIDと受信したストリームシードデータとを対応付けたレコードを、新たに待受けテーブル26に登録する（ステップS6）。

【0114】

図16に示すように、待受けテーブル26のレコードは、プロバイダIDおよびストリ

50

ームシードデータの2つのフィールドにより構成され、ストリームシードデータは、タイムヘッダおよびストリームシードの2つのサブフィールドにより構成されている。

【0115】

つぎに、サーバ4は、プロバイダ6に対し、プロバイダID（この例では、図16に示す待受けテーブル26の最上行のレコードに対応する「123456」）を含むペアリングの待受け開始要求を送信する（ステップS7）。

【0116】

この要求を受信したプロバイダ6は、プロバイダIDを記憶するとともに、提供用文字列の表示画面を初期化し（ステップS8）、提供用文字列を表示する（ステップS9）。

【0117】

図11Aに示すように、プロバイダ6の初期化された表示画面80の提供用文字列表示部81には、提供用文字列「3517」が表示されている。これは、ステップS2においてプロバイダ6に記憶されたストリームシードの先頭桁から連続する4桁の数字を抽出したものである。当然のことながら、この数字は、図16に示す待受けテーブル26におけるプロバイダID「123456」に対応するストリームシードの先頭から連続する4桁の数字に一致している。

【0118】

つぎに、プロバイダ6は、提供用文字列の桁上げタイミングが到来したか否かを監視しており（ステップS10）、桁上げタイミングが到来すると、提供用文字列の桁上げ処理を行い、制御をステップS9に戻す（ステップS11）。

【0119】

提供用文字列の桁上げタイミングはとくに限定されるものではないが、この実施形態においては、当該ストリームシードに対応するタイムヘッダの示す時刻から10秒経過ごとに桁上げ処理を実行するよう構成している。

【0120】

なお、タイムヘッダは、当該ストリームシードの生成時刻および提供用文字列の桁上げの時間間隔に基づいて決定される。内部時計の基準時、たとえば、午前0時からストリームシードの生成時刻までの経過時間を提供用文字列の桁上げの時間間隔で除した値の整数部分と提供用文字列の桁上げの時間間隔との積に相当する時刻とすることができる。

【0121】

この例では、提供用文字列の桁上げの時間間隔が10秒であるから、当該ストリームシードの生成時刻から10秒未満の端数を減じた時刻がタイムヘッダの示す時刻となっている。

【0122】

図11Bに示すように、桁上げ処理が実行された後の表示画面80の提供用文字列表示部81には、提供用文字列「5179」が表示されている。これは、ステップS2においてプロバイダ6に記憶されたストリームシードの第2桁から連続する4桁の数字を抽出したものである。当然のことながら、この数字は、図16に示す待受けテーブル26におけるプロバイダID「123456」に対応するストリームシードの第2桁から連続する4桁の数字に一致している。

【0123】

以下、同様に、桁上げ処理が実行されるたびに、提供用文字列は、「1797」（図11C参照）、「7973」（図11D参照）へと変化する。

【0124】

一般的な表現を用いれば、この実施形態においては、提供用文字列の桁数を n 桁とし、ストリームシードを構成する文字列の文字数を m （ $m > n$ ）桁としたとき、ストリームシードを構成する文字列の先頭から連続する n 桁の文字列を抽出して提供用文字列を構成するとともに、一定時間経過ごとに抽出する文字列を1桁下位にずらせることで、提供用文字列を一定時間ごとに変化するよう構成している。

【0125】

上述のように、この例では、ストリームシードを183桁の数字としている。これは、提供用文字列を4桁の数字とし、10秒経過ごとに提供用文字列の桁上げ処理を行うとして、最大30分間の待受けを可能とするためである。もちろん、ストリームシードの桁数は、これに限定されるものではない。

【0126】

つぎに、図6に示すように、レジスタ7のCPU61（以下、単に「レジスタ7」ということがある。）は、受諾用文字列の入力画面の起動指示の有無を監視している（ステップS12）。

【0127】

ステップS12において、レジスタ7の入力装置63（以下、単に「レジスタ7」ということがある。）から、受諾用文字列の入力画面の起動指示が入力されると、レジスタ7は、初期パラメータの設定を行うとともに、対象プロバイダ値に「ALL」をセットする（ステップS13）。

【0128】

初期パラメータの設定には、内部時計の校正が含まれる。内部時計の校正は、たとえば、インターネット上の特定のタイムサーバとの間で時刻を同期することにより行われる。なお、内部時計の校正は、プロバイダ6においても同様の方法で適時実行されており、その結果、両者の間で内部時計の同期がとれている。

【0129】

対象プロバイダ値については、後述する。

【0130】

つづいて、レジスタ7は、受諾用文字列を入力するための画面を初期化して表示する（ステップS14）。

【0131】

図12Aに示すように、レジスタ7の初期化された表示画面70には、入力用キーボタン73が表示され、数字入力が可能となっている。残時間表示部74には、後述の受諾用文字列の桁上げまでの残時間がグラフ（この例では棒グラフ）表示されている。この例では、残時間が少なくなるほど棒グラフの長さが短くなるよう構成されている。受諾用文字列表示部71には、まだ何も表示されていない。ペアリングボタン72は、受諾用文字列表示部71に4桁の数字が表示されたとき以外は操作できないよう構成されている。

【0132】

図11Aに示すプロバイダ6の表示画面80の提供用文字列表示部81に表示された提供用文字列「3517」を見たレジスタ7の操作者により、レジスタ7への受諾用文字列の入力が行われると（ステップS15）、レジスタ7は、ペアリングボタン72が操作されたか否かを判断する（ステップS16）。

【0133】

レジスタ7への受諾用文字列の入力が行われた状態の表示画面70を図12Bに示す。なお、この状態では、ペアリングボタン72は操作可能となっている。

【0134】

ステップS16においてペアリングボタン72が操作されないときは、レジスタ7は、受諾用文字列の桁上げタイミングが到来したか否かを監視し（ステップS17）、桁上げタイミングが到来すると、受諾用文字列の桁上げ処理を行い、制御をステップS15に戻す（ステップS18）。

【0135】

受諾用文字列の桁上げはプロバイダ6における提供用文字列の桁上げと同期して行われるよう構成されている。すなわち、受諾用文字列の桁上げのタイミングは、提供用文字列の桁上げのタイミングと同様の方法で決定される。この例では、レジスタ7の内部時計の正10秒毎に受諾用文字列の桁上げを行えば、プロバイダ6における提供用文字列の桁上げと同期することになる。

【0136】

10

20

30

40

50

図12Cに示すように、桁上げ処理が実行された後の表示画面70の受諾用文字列表示部71には、新たな受諾用文字列の上3桁「517」が表示され、受諾用文字列の最下位桁が空白となっている。この状態においては、ペアリングボタン72は操作不能となっている。

【0137】

この状態から、図11Bに示すプロバイダ6の表示画面80の提供用文字列表示部81に表示された提供用文字列「5179」を見たレジスタ7の操作者により、受諾用文字列の最下位桁に1桁の数字（この場合は「9」）が入力されると、図12Dに示すように、表示画面70の受諾用文字列表示部71には、完全な受諾用文字列「5179」が表示され、ペアリングボタン72は操作可能となる。

10

【0138】

しかし、何らかの理由でペアリングボタン72を操作するのが遅れ、その間に、プロバイダ6の表示画面80に表示された提供用文字列が、「1797」（図11C参照）、「7973」（図11D参照）と変化してしまった場合でも、レジスタ7の操作者により、既入力を受諾用文字列の最下位桁に「7」、「3」を追加入力することで、レジスタ7の表示画面70の受諾用文字列表示部71には、現時点における完全な受諾用文字列「7973」が表示され、ペアリングボタン72は操作可能となる。

【0139】

ここで、ペアリングボタン72が操作されると、レジスタ7は、入力された受諾用文字列、タイムスタンプ、および、対象プロバイダ値（ステップS13において設定された値、または、後述のステップS25において設定された値）をサーバ4に送信する（ステップS19）。

20

【0140】

タイムスタンプは、当該ペアリングボタン72の操作時刻および提供用文字列の桁上げの時間間隔に基づいて、上記タイムヘッダの決定方法と同様の方法で決定される。

【0141】

つぎに、図7に示すように、サーバ4は、受信した受諾用文字列、タイムスタンプ、および、対象プロバイダ値に基づいて待受けテーブル26を検索し（ステップS20）、該当するプロバイダ6の有無を判断する（ステップS21）。

【0142】

ステップS20、ステップS21について詳述する。

30

【0143】

対象プロバイダ値とは、上記ステップS20における待受けテーブル26の検索の対象となるレコードを特定するための情報であり、対象プロバイダ値として設定されたプロバイダIDを持つレコードが検索の対象となる。対象プロバイダ値が「ALL」の場合は、待受けテーブル26の全レコードが検索対象となる。

【0144】

ステップS20において受信した受諾用文字列、タイムスタンプ、および、対象プロバイダ値を図17Aに例示する。この場合、対象プロバイダ値が「ALL」であるから、待受けテーブル26の全レコードが検索対象となる。

40

【0145】

タイムスタンプの時刻と待受けテーブル26の検索対象となるレコードのタイムヘッダの時刻との差を、提供用文字列の桁上げの時間間隔（この例では10秒）で除した値sを算出する。

【0146】

提供用文字列の桁数をn桁（この例では4桁）とした場合、当該レコードのストリームシードを構成する文字列の先頭桁からs桁下位にずれた位置にある文字を先頭とする連続するn桁の文字列を抽出し、この抽出した文字列と受信した受諾用文字列とを比較する。

【0147】

両者が一致すれば、ステップS21において、該当するプロバイダ6が存在すると判断

50

される。

【0148】

たとえば、図17Aに示す受信情報と、図17Bに示す待受けテーブル26のプロバイダID「123456」であらわされるレコードとを比較すれば、上記s=3となる。これに基づいて当該レコードのストリームシードを構成する文字列から抽出した4桁の文字列は「7973」となり、これは、図17Aに示す受諾用文字列「7973」に一致する。したがって、この場合、ステップS21において、該当するプロバイダ6が存在すると判断されることになる。

【0149】

検索対象となっているレコードすべてについて、上記判断が行われる。

10

【0150】

この結果、ステップS21において該当するプロバイダ6が存在しないと判断されると、その旨の情報が、サーバ4からレジスタ7に送信され、図13Aに示すように、レジスタ7の表示画面70に「無効なPINです」との表示がなされる（ステップS22）。この表示は、当該レジスタ7から入力されサーバ6に送信された受諾用文字列が無効であることを示す表示である。

【0151】

ステップS22の表示後、レジスタ7は、制御をステップS13（図6参照）に戻す。

【0152】

一方、ステップS21において該当するプロバイダ6が存在すると判断されると、サーバ4は、該当するプロバイダの数が1つか複数かを判断する（ステップS23）。

20

【0153】

ステップS23において、該当するプロバイダの数が複数であると判断すると、サーバ4は、該当するすべてのプロバイダ6に対し、その旨の情報を送信し、この情報を受信したプロバイダ6は、制御をステップS2（図5参照）に戻し、再度、ストリームシードの生成・送信から始める。

【0154】

ステップS23において、該当するプロバイダ6の数が複数となるのは、ペアリングの待受けをしている複数のプロバイダ6間で、ある時点での提供用文字列が偶然に一致したためであると考えられる。そこで、当該プロバイダ6に対して、再度、ストリームシードの生成・送信からやり直しをさせ、偶然の一致を解消して、所望の相手とのペアリングを実現させるのである。

30

【0155】

なお、ステップS23において、該当するプロバイダの数が複数であると判断された場合、制御を、ステップS2ではなくステップS9（図5参照）に戻し、該当する各プロバイダに、提供用文字列の表示を継続させるよう構成することもできる。提供用文字列の桁上げの時間間隔（この例では10秒）が経過すると提供用文字列が自動的に変化するため、変化後の提供用文字列が、該当する複数のプロバイダ間で再び一致する可能性は、極めて低いと考えられるからである。

【0156】

なお、ステップS23において、該当するプロバイダの数が複数であると判断すると、サーバ4は、レジスタ7に対して、その旨および該当する複数のプロバイダIDを含む情報を送信する（ステップS24）。

40

【0157】

この情報を受信したレジスタ7は、上記ステップS13（図6参照）と同様の処理を行う（ステップS25）。ただし、ステップS13と異なり、ステップS25においては、対象プロバイダ値として、サーバ4から受信した複数のプロバイダIDのリストが設定される。

【0158】

つづいて、図13Bに示すように、レジスタ7の表示画面70に「追加の認証を求めら

50

れています」との表示がなされる（ステップS 2 6）。この表示は、当該レジスタ7から入力されサーバ6に送信された受諾用文字列によっては、ペアリングが成立しなかったことを示すエラー表示である。

【0 1 5 9】

当該表示画面7 0に表示された「続ける」ボタン7 5が操作されると、レジスタ7は、制御をステップS 1 4（図6参照）に戻し、再度、受諾用文字列の入力画面の初期化からやり直す。

【0 1 6 0】

一方、ステップS 2 3において該当するプロバイダ6の数が1つであると判断されると、サーバ4は、その旨の情報を当該プロバイダ6に送信し、図8に示すように、この情報を受信したプロバイダ6において、当該情報に係るペアリングのモードがマルチプルペアリングモードであるか否かが判断される（ステップS 2 7）。

10

【0 1 6 1】

図1 4に示すように、マルチプルペアリングモードとは、1のプロバイダ6と複数のレジスタ7 a、7 b、7 cとの間のペアリング（マルチプルペアリング）を許容するモードである。これは、1のプロバイダ6と1のレジスタ7 a、1のプロバイダ6と1のレジスタ7 b、1のプロバイダ6と1のレジスタ7 cからなる3つのシングルペアリング（1対1のペアリング）を1回のペアリング処理で実現するモードと見ることができる。

【0 1 6 2】

なお、当該ペアリングのモードがマルチプルペアリングモードであるかシングルペアリングモード（1回のペアリング処理で1つのシングルペアリングのみを許容するモード）であるかは、前もって（たとえば図5に示すステップS 1において）設定されて、プロバイダ6に記憶されている。

20

【0 1 6 3】

ステップS 2 7において、マルチプルペアリングモードであると判断されると、当該レジスタ（たとえば、図1 4に示すレジスタ7 a）に、その旨およびプロバイダIDを含む情報が送信され、当該レジスタ7 aの表示画面7 0に、ペアリングが成功した旨の表示（図示せず）がなされ（ステップS 3 2）、ペアリング処理は続行される。

【0 1 6 4】

この場合、プロバイダ6の操作者が、残りのレジスタ（たとえば、図1 4に示すレジスタ7 b、レジスタ7 c）との間のペアリングが成功したと判断した場合や、ペアリング処理を中止すると判断した場合の処理については、後述する。

30

【0 1 6 5】

一方、ステップS 2 7において、マルチプルペアリングモードでないと判断されると、つぎに、プロバイダ6において、当該情報に係るペアリングのモードがセーフペアリングモードであるか否かが判断される（ステップS 2 8）。

【0 1 6 6】

セーフペアリングモードとは、より安全にペアリングを行うためのモードである。当該ペアリングのモードがセーフペアリングモードであるか通常のペアリングモード（セーフペアリングモードでないモード）であるかは、前もって（たとえば図5に示すステップS 1において）設定されて、プロバイダ6に記憶されている。

40

【0 1 6 7】

ステップS 2 8において、セーフペアリングモードでないと判断されると、プロバイダ6はサーバ4に、プロバイダIDを含むペアリング待受け終了コマンドを送信する（ステップS 2 9）。

【0 1 6 8】

サーバ4は、ペアリング待受け終了コマンドを受信すると、待受けテーブル2 6のレコードのうち、当該プロバイダIDに対応するレコードを無効化する（ステップS 3 1）。当該プロバイダIDに対応するペアリングが成立したため、当該レコードを維持する必要がなくなったからである。レコードの無効化は、たとえば、当該レコードの削除や、当該

50

レコードに無効フラグをたてる等の方法により行うことができる。

【0169】

これと同時に、当該プロバイダ6の表示画面80に、ペアリングが成功した旨の表示（図示せず）がなされる（ステップS30）。また、ペアリングの相手となるレジスタ7に、その旨およびプロバイダIDを含む情報が送信され、当該レジスタ7の表示画面70に、ペアリングが成功した旨の表示（図示せず）がなされ（ステップS32）、ペアリング処理は終了する。

【0170】

一方、ステップS28において、セーフペアリングモードであると判断されると、図9に示すように、プロバイダ6はレジスタ7に、確認用文字列発行要求およびプロバイダIDを含む情報を送信する（ステップS33）。 10

【0171】

確認用文字列発行要求を受信したレジスタ7は、確認用文字列を発行し（ステップS34）、発行した確認用文字列を表示する（ステップS35）。

【0172】

図15Aに示すように、レジスタ7の表示画面70の確認用文字列表示部76には、確認用文字列「8451」が表示されている。確認用文字列の生成方法はとくに限定されるものではないが、たとえば、レジスタ7の乱数生成機能を利用して生成することができる。確認用文字列の文字種、文字数はとくに限定されるものではないが、ここでは、4桁の数字を例示する。 20

【0173】

一方、図15Bに示すように、プロバイダ6の表示画面80には、入力用キーボタン83が表示され、数字入力が可能となっている。確認ボタン85は、応答用文字列が入力されて応答用文字列表示部84に4桁の数字が表示されたとき以外は操作できないよう構成されている。

【0174】

図15Aに示すレジスタ7の表示画面70の確認用文字列表示部76に表示された確認用文字列「8451」を見たプロバイダ6の操作者により、プロバイダ6への応答用文字列の入力が行われ、確認ボタン85が操作されると（ステップS36）、プロバイダ6は、入力された応答用文字列をレジスタ7に送信する（ステップS37）。 30

【0175】

レジスタ7は、受信した応答用文字列と確認用文字列とを比較し（ステップS38）、一致しない場合は、当該ペアリングが失敗した旨の表示（図示せず）を行う（ステップS40）。

【0176】

一方、ステップS38において、応答用文字列と確認用文字列とが一致した場合は、当該レジスタ7の表示画面70に、ペアリングが成功した旨の表示（図示せず）がなされるとともに（ステップS39）、上記ステップS29（図8参照）に制御を移す。

【0177】

さて、図10に示すように、プロバイダ6は、待受け終了指示を監視している（ステップS41）。 40

【0178】

図14に示すマルチプルペアリングモードにおいて、プロバイダ6の操作者が、残りのレジスタ（たとえば、図14に示すレジスタ7b、レジスタ7c）との間のペアリングが成功したと判断した場合や、ペアリング処理を中止すると判断した場合、待受け終了ボタン82を操作することで、ペアリング処理を中止することができる。シングルペアリングモードにおいて、ペアリング成立前にペアリング処理を中止する場合も、同様である。

【0179】

待受け終了ボタン82が操作されると、プロバイダ6はサーバ4に、プロバイダIDを含むペアリング待受け終了コマンドを送信し、上記ステップS31（図8参照）に制御が 50

移される（ステップS42）。

【0180】

これと同時に、当該プロバイダ6の表示画面80に、待受けが終了した旨の表示（図示せず）がなされ（ステップS43）、ペアリング処理が終了する。

【0181】

なお、上述の実施形態においては、提供用文字列の桁数を n 桁とし、予め作成したストリームシードを構成する文字列の文字数を m （ $m > n$ ）桁としたとき、ストリームシードを構成する文字列の先頭から連続する n 桁の文字列を抽出して提供用文字列を構成するとともに、一定時間経過ごとに抽出する文字列を1桁下位にずらせることで、提供用文字列を一定時間ごとに変化するように構成した場合の例について説明したが、この発明はこれに

10

【0182】

たとえば、最初に任意の n 桁の文字列のみを生成して提供用文字列とし、一定時間ごとにこれを繰り返して最上位桁の文字を削除するとともに、任意の新たな文字をその都度生成して最下位桁に追加するように構成することもできる。

【0183】

また、上述の実施形態においては、受諾用文字列の桁上げを、提供用文字列の桁上げと同期して行うよう構成した場合の例について説明したが、受諾用文字列の桁上げタイミングを、提供用文字列の桁上げタイミングと無関係に行うよう構成することもできる。

【0184】

20

たとえば、受諾用文字列の桁数を n 桁としたとき、既入力を受諾用文字列（ n 桁）が表示された状態において新たな文字が第2の機器の入力装置から入力されたタイミングで、受諾用文字列の桁上げを行うよう構成することもできる。

【0185】

つぎに、図18～図22は、本願のペアリング処理を利用したエンティティ認証処理（以下、単に「認証処理」ということがある。）の流れの一例を示すフローチャートである。認証処理におけるペアリング処理では、プロバイダ6の操作者とレジスタ7の操作者が同一である点で、上述のペアリング処理と異なる。

【0186】

図23～図24は、認証処理における、認証用機器30およびサービス用機器40の表示画面の推移の一例を示す図面である。図25、図26は、それぞれ認証側テーブル36およびサービス側テーブル46のデータ構成の一例を示す図面である。

30

【0187】

図18～図26を参照しつつ、認証処理について説明する。

【0188】

認証処理のうち、最初に、認証登録処理について説明する。認証登録処理は、サービス用機器40によって提供される特定のサービス（以下、「サービスA」ということがある。）を利用する際の認証キーとして、認証用機器30を登録する処理である。

【0189】

図18に示すように、認証登録処理においては、まず、認証用機器30とサービス用機器40との間でペアリング処理が実行される（ステップS49）。

40

【0190】

認証登録処理におけるペアリング処理においては、とくに限定されるものではないが、たとえば、認証用機器30をプロバイダ6とし、サービス用機器40をレジスタ7として、上記ペアリング処理と同様の処理が実行される。ただし、ステップS49のペアリング処理においては、その性質上、原則として、マルチプルペアリングモード（図8、ステップS27参照）は想定されておらず待受け終了処理（図10参照）も想定されていない。また、認証用機器30、サービス用機器40における表示内容も、上記実施形態におけるプロバイダ6、レジスタ7の表示内容と一部異なる。

【0191】

50

図23の(a)に示すように、認証登録処理においては、まず、サービス用機器40の表示画面210に新規サービス利用登録画面が表示される。この画面から、ユーザ名その他登録に必要な情報が入力される。ここで認証キー登録ボタン215が操作されるとともに、認証用機器30の表示画面110の認証キー追加ボタン(図示せず)が操作されると、ペアリング処理が開始される。

【0192】

ペアリング処理が開始されると、図23の(b)に示すように、認証用機器30の表示画面110の提供用文字列表示部111に、提供用文字列が表示される。

【0193】

操作者はこれを見て、図23の(c)に示すサービス用機器40の表示画面210に表示された入力用キーボタン213を操作して受諾用文字列を入力する。受諾用文字列表示部212に受諾用文字列が表示された状況で登録ボタン214(図12A等のペアリングボタン72に相当する。)が操作されると、ペアリング処理が実行される。

【0194】

その結果、認証用機器30とサービス用機器40との間でペアリングが成立すると、図18に示すように、ペアリング成立による相互通信可能な状態を利用して、サービス用機器40と認証用機器30との間で公開鍵送信処理が自動的に実行される(ステップS50)。

【0195】

図19は、公開鍵送信処理(ステップS50)の詳細な流れの一例を示すフローチャートである。公開鍵送信処理において、サービス用機器40は、サービス側鍵ペア、すなわち、サービスAに係る秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵、を生成して、サービス側テーブル46に記憶する(ステップS54)。

【0196】

図26に示すサービス側テーブル46において、内部ユーザIDフィールドが「N/A(該当なし)」となっているレコードであって、鍵グループIDフィールドが同一値(たとえば「0」)となっている一対のレコードがサービス側鍵ペアに対応する。この一対のレコードのうち種別フィールドが「秘密鍵」となっているレコードの鍵フィールドがサービス側秘密鍵を表し、種別フィールドが「公開鍵」となっているレコードの鍵フィールドがサービス側公開鍵を表す。サービス側テーブル46には、2対のサービス側鍵ペアが記憶されている。

【0197】

一方、認証用機器30は、認証側鍵ペア、すなわち、認証用機器30に係る秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵、を生成して、認証側テーブル36に記憶するとともに(ステップS51)、生成した認証側公開鍵をサービス用機器40に送信する(ステップS52)。

【0198】

図25に示す認証側テーブル36において、サービスIDフィールド、サービス名フィールドおよび内部ユーザIDフィールドがいずれも「N/A(該当なし)」となっているレコードであって、鍵グループIDフィールドが同一値(たとえば「0」)となっている一対のレコードが認証側鍵ペアに対応する。この一対のレコードのうち種別フィールドが「秘密鍵」となっているレコードの鍵フィールドが認証側秘密鍵を表し、種別フィールドが「公開鍵」となっているレコードの鍵フィールドが認証側公開鍵を表す。認証側テーブル36には、2対の認証側鍵ペアが記憶されている。

【0199】

サービス用機器40は、認証側公開鍵を受信すると、サービスAに係る認証用機器30の識別標識である内部ユーザIDを生成し、受信した認証側公開鍵を当該内部ユーザIDに対応付けて、サービス側テーブル46に記憶する(ステップS55)。

【0200】

10

20

30

40

50

図26に示すサービス側テーブル46において、内部ユーザIDフィールドが「N/A（該当なし）」以外の値（たとえば「BBB」）となっているレコードの鍵フィールドが、当該内部ユーザIDに対応する認証側公開鍵を表す。

【0201】

サービス側テーブル46に3つの認証側公開鍵が記憶されている。これらの認証側公開鍵に対応するレコードのうち、鍵グループIDフィールドが同一値（たとえば「0」）となっているレコードは同一グループとして管理され、後述のように、認証実行処理において、当該内部ユーザIDに対応する認証側公開鍵とともに、同一の鍵グループIDフィールドを持つサービス側秘密鍵を用いて、正当性検証処理が行われる。

【0202】

サービス用機器40は、さらに、ステップS54において生成したサービス側公開鍵を、サービスAの識別標識であるサービスID、当該サービスIDに対応するサービス名、および上記内部ユーザIDとともに、認証用機器30に送信する（ステップS56）。

【0203】

認証用機器30は、サービス用機器40からサービス側公開鍵、サービスID、サービス名、内部ユーザIDを受信すると、これらを関連付けて認証側テーブル36に記憶する（ステップS53）。

【0204】

図25に示す認証側テーブル36において、サービスIDフィールド、サービス名フィールドおよび内部ユーザIDフィールドがいずれも「N/A（該当なし）」以外の値（たとえば「AAA」、「サービスA」、「BBB」）となっているレコードの鍵フィールドが、当該サービスIDに対応するサービス側公開鍵を表す。

【0205】

認証側テーブル36に3つのサービス側公開鍵が記憶されている。これらのサービス側公開鍵に対応するレコードのうち、鍵グループIDフィールドが同一値（たとえば「0」）となっているレコードは同一グループとして管理され、後述のように、認証実行処理において、当該サービスIDに対応するサービス側公開鍵とともに、同一の鍵グループIDフィールドを持つ認証側秘密鍵を用いて、正当性検証処理が行われる。

【0206】

図18に示す処理が完了すると、図23の（d）および（e）に示すように、サービス用機器40の表示画面210および認証用機器30の表示画面110に、それぞれ、認証登録処理が完了した旨の表示がなされ、認証登録処理（図18参照）が終了する。

【0207】

なお、図18に示す処理において、複数のサービス側鍵ペアを生成し、サービス側鍵ペアおよびこれに対応する1または2以上の認証側公開鍵を同一グループとして管理するよう構成したが、この発明はこれに限定されるものではない。たとえば、サービス側鍵ペアを、異なる認証用機器30に対し別個に生成・記憶するようにしてもよいし、異なる認証用機器30に対し全て共通のサービス側鍵ペアを用いることもできる。後者の場合、ステップS54の処理は、一度実行しておけば、認証登録処理ごとに実行する必要はない。

【0208】

また、図18に示す処理において、複数の認証側鍵ペアを生成し、認証側鍵ペアおよびこれに対応する1または2以上のサービス側公開鍵を同一グループとして管理するよう構成したが、この発明はこれに限定されるものではない。たとえば、認証側鍵ペアを、異なるサービス用機器40に対し別個に生成・記憶するようにしてもよいし、異なるサービス用機器40に対し全て共通の認証側鍵ペアを用いることもできる。後者の場合、ステップS51の処理は、一度実行しておけば、認証登録処理ごとに実行する必要はない。

【0209】

つぎに、認証実行処理について説明する。認証実行処理は、認証登録処理によって認証キーとして登録された認証用機器30を用いて、サービス用機器40によって提供されるサービスAを利用するための認証を行う処理である。

10

20

30

40

50

【0210】

図20に示すように、認証実行処理においては、まず、認証用機器30とサービス用機器40との間でペアリング処理が実行される（ステップS49）。

【0211】

認証実行処理におけるペアリング処理においては、とくに限定されるものではないが、たとえば、サービス用機器40をプロバイダ6とし、認証用機器30をレジスタ7として、認証登録処理におけるペアリング処理と同様の処理が実行される。

【0212】

図24の（a）に示すように、認証実行処理においては、まず、サービス用機器40の表示画面210に認証開始画面が表示される。この画面からキー認証ボタン216が操作されると、ペアリング処理が開始される。

10

【0213】

なお、この例では、上記認証開始画面から、ログインIDおよびパスワードを入力することによっても、認証用機器30を用いることなく、認証が可能となるよう構成されている。

【0214】

さて、キー認証ボタン216の操作によりペアリング処理が開始されると、図24の（b）に示すように、サービス用機器40の表示画面210の提供用文字列表示部211に、提供用文字列が表示される。

【0215】

20

操作者はこれを見て、図24の（c）に示す認証用機器30の表示画面110に表示された入力用キーボタン113を操作して受諾用文字列を入力する。受諾用文字列表示部112に受諾用文字列が表示された状態で認証ボタン114（図12A等のペアリングボタン72に相当する。）が操作されると、ペアリング処理が実行される。

【0216】

その結果、認証用機器30とサービス用機器40との間でペアリングが成立すると、図20に示すように、ペアリング成立による相互通信可能な状態を利用して、サービス用機器40と認証用機器30との間で正当性検証処理が自動的に実行される（ステップS60）。

【0217】

30

図21および図22は、正当性検証処理（ステップS60）の詳細な流れの一例を示すフローチャートである。正当性検証処理において、サービス用機器40は、サービスAに係るサービスIDの指定を含む認証を求める情報を認証用機器30に送信する（ステップS61）。

【0218】

認証用機器30は、当該認証を求める情報を受信すると、認証側元データとして乱数を生成する（ステップS62）。この乱数を認証側乱数とよぶ。もちろん、認証側元データは乱数に限定されるものではなく、認証用機器30において用意した任意のデータであればよい。

【0219】

40

認証用機器30は、受信したサービスIDに対応するサービス側公開鍵および内部ユーザIDを、認証用機器30の認証側テーブル36（以下、単に「認証用機器30」ということがある。）から読み出し、読み出したサービス側公開鍵を用いて、認証側乱数を暗号化する（ステップS63）。この暗号化された認証側乱数が、認証側暗号化データである。

【0220】

認証用機器30は、上記認証側暗号化データと読み出した内部ユーザIDとを、サービス用機器40に送信する（ステップS64）。

【0221】

サービス用機器40は、認証側暗号化データと内部ユーザIDとを受信すると、受信し

50

た認証側暗号化データを、サービス側テーブル46に記憶されているサービス側秘密鍵を用いて復号化する(ステップS65)。サービス側テーブル46に記憶されている複数のサービス側秘密鍵のうち、復号化に用いられるサービス側秘密鍵は、受信した内部ユーザIDに対応する認証側公開鍵と同一の鍵グループIDフィールドを持つサービス側秘密鍵である。この復号化された認証側暗号化データが、認証側復号化データである。

【0222】

サービス用機器40は、認証側復号化データに所定の演算を施して認証側演算化データを得る(ステップS66)。この例では、所定の演算として、不可逆的な一方向性関数を含む関数、たとえば、特定のハッシュ関数を用いた演算を行うよう構成している。したがって、ステップS66において、認証側復号化データに特定のハッシュ関数を用いた演算

10

【0223】

もちろん、所定の演算は、ハッシュ関数を用いた演算に限定されるものではない。たとえば、認証側演算化データを認証側復号化データと同一の値とすることもできる。この場合、所定の演算は「1」を乗ずる演算、とみることができる。

【0224】

サービス用機器40は、算出されたハッシュ値を認証用機器30に送信する(ステップS67)。

【0225】

認証用機器30は、ハッシュ値を受信する一方(ステップS69)、ステップS62において生成した認証側乱数に、ステップS66において用いられるハッシュ関数と同一のハッシュ関数を用いた演算を行って得られるハッシュ値を算出し(ステップS68)、この2つのハッシュ値が一致するか否かを判断する(ステップS70)。

20

【0226】

2つのハッシュ値が一致しない場合は、サービスIDの認証は失敗した(サービスIDが真正でない)と判断し、認証実行処理を終了する(ステップS71)。

【0227】

一方、ステップS70において、2つのハッシュ値が一致する場合は、サービスIDの認証は成功した(サービスIDが真正である)と判断され、つぎの認証を求める情報がサービス用機器40に送信され、制御は、図22に示すステップS72に移される。

30

【0228】

ステップS72～ステップS81の処理は、認証用機器30とサービス用機器40の役割が逆転しているが、上記ステップS62～ステップS71の処理と略同様の処理である。

【0229】

すなわち、ステップS72において、サービス用機器40は、サービス側元データとして乱数を生成する(ステップS72)。この乱数をサービス側乱数とよぶ。もちろん、サービス側元データは乱数に限定されるものではなく、サービス用機器40において用意した任意のデータであればよい。

【0230】

サービス用機器40は、ステップS65において認証用機器30から受信した内部ユーザIDに対応する認証側公開鍵を、サービス用機器40のサービス側テーブル46(以下、単に「サービス用機器40」ということがある。)から読み出し、読み出した認証側公開鍵を用いて、サービス側乱数を暗号化する(ステップS73)。この暗号化されたサービス側乱数が、サービス側暗号化データである。

40

【0231】

サービス用機器40は、上記サービス側暗号化データを、認証用機器30に送信する(ステップS74)。

【0232】

認証用機器30は、受信したサービス側暗号化データを、認証側テーブル36に記憶さ

50

れている認証側秘密鍵を用いて復号化する（ステップS75）。認証側テーブル36に記憶されている複数の認証側秘密鍵のうち、復号化に用いられる認証側秘密鍵は、ステップS62において受信したサービスIDに対応するサービス側公開鍵と同一の鍵グループIDフィールドを持つ認証側秘密鍵である。この復号化されたサービス側暗号化データが、サービス側復号化データである。

【0233】

認証用機器30は、サービス側復号化データに所定の演算を施してサービス側演算化データを得る（ステップS76）。この例では、所定の演算として、不可逆的な一方向性関数を含む関数、たとえば、特定のハッシュ関数を用いた演算を行うよう構成している。したがって、ステップS76において、サービス側復号化データに特定のハッシュ関数を用いた演算を行い、サービス側演算化データであるハッシュ値を算出する。

10

【0234】

もちろん、所定の演算は、ハッシュ関数を用いた演算に限定されるものではない。たとえば、サービス側演算化データをサービス側復号化データと同一の値とすることもできる。この場合、所定の演算は「1」を乗ずる演算、とみることができる。

【0235】

認証用機器30は、算出されたハッシュ値をサービス用機器40に送信する（ステップS77）。

【0236】

サービス用機器40は、ハッシュ値を受信する一方（ステップS79）、ステップS72において生成したサービス側乱数に、ステップS76において用いられるハッシュ関数と同一のハッシュ関数を用いた演算を行って得られるハッシュ値を算出し（ステップS78）、この2つのハッシュ値が一致するか否かを判断する（ステップS80）。

20

【0237】

2つのハッシュ値が一致しない場合は、内部ユーザIDの認証は失敗した（内部ユーザIDが真正でない）と判断し、認証実行処理を終了する（ステップS81）。

【0238】

一方、ステップS80において、2つのハッシュ値が一致する場合は、内部ユーザIDの認証は成功した（内部ユーザIDが真正である）と判断され、図20に示す認証実行処理が成功したと判断される（ステップS82）。

30

【0239】

認証実行処理が成功すると、図24の（d）に示すように、サービス用機器40の表示画面210に、認証が成功した旨の表示がなされ、認証実行処理（図20参照）が終了する。

【0240】

この後、利用者（操作者）は、サービス用機器40によって提供されるサービスAを利用することが可能となる。

【0241】

なお、上述の実施形態においては、正当性検証処理（図20、ステップS60）として、サービスIDの正当性検証処理（図21、ステップS61～ステップS71）および内部ユーザIDの正当性検証処理（図22、ステップS72～ステップS82）の双方の正当性検証処理を行うよう構成したが、この発明はこれに限定されるものではない。

40

【0242】

提供されるサービスの種類・性質・利用態様などに応じ、正当性検証処理（図20、ステップS60）として、サービスIDの正当性検証処理（図21、ステップS61～ステップS71）および内部ユーザIDの正当性検証処理（図22、ステップS72～ステップS82）のいずれか一方のみを実行するよう構成することもできる。

【0243】

また、本発明による認証の態様はとくに限定されるものではない。たとえば、ソフトウェアの利用認証、ウェブサイトへのログイン認証、ウェブショッピング等における決済サ

50

ービス認証（リダイレクトによる決済サービスへの移行を含む）など、あらゆる認証に本発明を適用することができる。

【0244】

さらに、本発明による認証実行処理（図20参照）済みのサービスの利用中に、当該サービスの一部について、さらに認証実行処理を行うよう構成することもできる。

【0245】

たとえば、ウェブサイトへの本発明によるログイン認証を済ませた上でサービス用機器40を用いて当該ウェブサイトを利用しているときに、利用者から当該ウェブサイトにおける特定の重要なサービス（たとえば、物品の売買）の提供が求められると、当該特定の重要なサービス提供の諾否の確認を認証用機器30に表示し、認証用機器30から承諾をする旨の入力があった場合に、重ねて本発明による認証実行処理を行うよう構成するのである。

10

【0246】

この場合、先の認証実行処理（図20参照）によるペアリング処理（ステップS49参照）が完了し、サービス用機器40と認証用機器30との間の通信は確立していることから、後の認証実行処理においては、あらためてペアリング処理を行う必要はなく、正当性検証処理（ステップS60参照）と同様の処理のみを実行すれば足りる。

【0247】

なお、上述の認証処理においては、認証用機器30を実機として実現した場合を例に説明したが、この発明はこれに限定されるものではない。認証用機器30を仮想マシンとして実現することもできる。この場合、サービス用機器40と認証用機器30とを同一の物理マシン上に並存させることもできる。

20

【0248】

なお、上述の認証処理においては、本願の第1ないし第4のいずれかの発明による情報通信システムにおいて、第1および第2の機器の一方を、特定のサービスを提供する機器であるサービス用機器とし、他方を、当該特定のサービスを利用する際の認証を行う機器である認証用機器とし、サービス用機器と認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行う場合を例に説明したが、認証処理は、これに限定されるものではない。

【0249】

何らかの手段を用いてサービス用機器と認証用機器との間で相手を特定して通信が確立されたこと（広義のペアリングの成立）を前提に、当該特定のサービスを利用可能とするための認証を行うよう構成することもできる。

30

【0250】

この場合、サービス用機器と認証用機器との間のペアリングは、インターネット等の情報通信網を介して行うようにしてもよいが、より一般的に、情報通信手段を介して行うよう構成することができる。

【0251】

ここで、情報通信手段とは、電気信号、光信号等に変換された情報を伝達するための通信手段であって、有線、無線の別を問わない。情報通信手段として、インターネットに代表されるWAN（Wide Area Network）、LAN（Local Area Network）等のコンピュータネットワーク、電話回線（携帯電話回線を含む。）、専用回線等の通信回線、Bluetoothその他の近距離無線通信、赤外線等による通信、通信ケーブルによる通信、機器相互の接触による通信、または、これらを組み合わせたものが例示される。

40

【0252】

すなわち、何らかの手段を用いてペアリング処理（図18および図20、ステップS49）に相当する処理（サービス用機器と認証用機器との間で相手を特定して通信を確立する処理）を行い、続いて、公開鍵送信処理（図18、ステップS50）または正当性検証処理（図20、ステップS60）を実行することで、認証登録処理（図18）または認証

50

実行処理（図 20）と同等の処理を行うことができる。

【0253】

この場合、この発明は、次のように把握することができる。

【0254】

[発明 A]

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムにおいて、

前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行うシステムであって、

前記認証用機器は、当該認証用機器側の秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵とを生成して、当該認証側秘密鍵を記憶するとともに、当該認証側公開鍵を前記サービス用機器に送信する認証側登録部、を備えた認証側制御部を備え、

前記サービス用機器は、前記認証用機器から前記認証側公開鍵を受信すると、前記特定のサービスに係る前記認証用機器の識別標識である内部ユーザ ID を生成し、前記認証側公開鍵を当該内部ユーザ ID に対応付けて記憶するとともに、当該内部ユーザ ID を前記認証用機器に送信するサービス側登録部、を備えたサービス側制御部を備え、

前記サービス側制御部は、前記認証用機器から内部ユーザ ID を指定した認証を求める情報を受信すると、当該サービス用機器において用意した任意のデータであるサービス側元データを前記サービス側登録部に記憶されている前記内部ユーザ ID に対応する認証側公開鍵を用いて暗号化したデータであるサービス側暗号化データを前記認証用機器に送信するサービス側暗号部、を備え、

前記認証側制御部は、前記サービス用機器から受信したサービス側暗号化データを当該認証側登録部に記憶されている前記認証側秘密鍵を用いて復号化したデータであるサービス側復号化データに所定の演算を施して得られるサービス側演算化データを前記サービス用機器に送信する認証側復号部、を備え、

前記サービス側制御部は、前記認証用機器から受信したサービス側演算化データが、前記サービス側元データに当該所定の演算を施して得られるデータと一致する場合は、前記内部ユーザ ID が真正であると判定する内部ユーザ ID 真正判定部、を備えたこと、

を特徴とする、情報通信システム。

【0255】

[発明 B]

発明 A の情報通信システムにおいて、

前記サービス側登録部は、さらに、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービス ID とともに、前記認証用機器に送信し、

前記認証側登録部は、さらに、前記サービス用機器から前記サービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービス ID と関連付けて記憶し、

前記認証側制御部は、前記サービス用機器からサービス ID を指定した認証を求める情報を受信すると、当該認証用機器において用意した任意のデータである認証側元データを前記認証側登録部に記憶されている前記サービス ID に対応する前記サービス側公開鍵を用いて暗号化したデータである認証側暗号化データを前記サービス用機器に送信する認証側暗号部、を備え、

前記サービス側制御部は、前記認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データを前記認証用機器に送信するサービス側復号部、を備え、

前記認証側制御部は、前記サービス用機器から受信した認証側演算化データが、前記認証側元データに当該所定の演算を施して得られるデータと一致する場合は、前記サービスIDが真正であると判定するサービスID真正判定部、を備えたこと、
を特徴とする、情報通信システム。

【0256】

[発明C]

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムにおいて、

前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行うシステムであって、

前記サービス用機器は、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービスIDとともに、前記認証用機器に送信するサービス側登録部、を備えたサービス側制御部を備え、

前記認証用機器は、前記サービス用機器から前記サービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービスIDと関連付けて記憶する認証側登録部、を備えた認証側制御部を備え、

前記認証側制御部は、前記サービス用機器からサービスIDを指定した認証を求める情報を受信すると、当該認証用機器において用意した任意のデータである認証側元データを前記認証側登録部に記憶されている前記サービスIDに対応する前記サービス側公開鍵を用いて暗号化したデータである認証側暗号化データを前記サービス用機器に送信する認証側暗号部、を備え、

前記サービス側制御部は、前記認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データを前記認証用機器に送信するサービス側復号部、を備え、

前記認証側制御部は、前記サービス用機器から受信した認証側演算化データが、前記認証側元データに当該所定の演算を施して得られるデータと一致する場合は、前記サービスIDが真正であると判定するサービスID真正判定部、を備えたこと、
を特徴とする、情報通信システム。

【0257】

[発明D]

発明AないしCのいずれかの情報通信システムに用いられる前記サービス用機器。

【0258】

[発明E]

発明AないしCのいずれかの情報通信システムに用いられる前記認証用機器。

【0259】

[発明F]

コンピュータを、発明Dのサービス用機器のサービス側制御部、または、発明Eの認証用機器の認証側制御部として機能させるためのプログラム。

【0260】

[発明G]

発明Fのプログラムを記憶した記録媒体。

【0261】

[発明H]

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムであって、前記サービス用機器と前記

10

20

30

40

50

認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行う情報通信システム、を用いて行う情報通信方法であって、

前記認証用機器が、当該認証用機器側の秘密鍵である認証側秘密鍵と当該認証側秘密鍵に対応する公開鍵である認証側公開鍵とを生成して、当該認証側秘密鍵を記憶するとともに、当該認証側公開鍵を前記サービス用機器に送信する認証側登録ステップと、

前記サービス用機器が、前記認証用機器から前記認証側公開鍵を受信すると、前記特定のサービスに係る前記認証用機器の識別標識である内部ユーザIDを生成し、前記認証側公開鍵を当該内部ユーザIDに対応付けて記憶するとともに、当該内部ユーザIDを前記認証用機器に送信するサービス側登録ステップと、

前記サービス用機器が、前記認証用機器から内部ユーザIDを指定した認証を求める情報を受信すると、当該サービス用機器において用意した任意のデータであるサービス側元データを前記サービス側登録部に記憶されている前記内部ユーザIDに対応する認証側公開鍵を用いて暗号化したデータであるサービス側暗号化データを前記認証用機器に送信するサービス側暗号ステップと、

前記認証用機器が、前記サービス用機器から受信したサービス側暗号化データを当該認証側登録部に記憶されている前記認証側秘密鍵を用いて復号化したデータであるサービス側復号化データに所定の演算を施して得られるサービス側演算化データを前記サービス用機器に送信する認証側復号ステップと、

前記サービス用機器が、前記認証用機器から受信したサービス側演算化データが、前記サービス側元データに当該所定の演算を施して得られるデータと一致する場合は、前記内部ユーザIDが真正であると判定する内部ユーザID真正判定ステップと、

を備えたこと、

を特徴とする、情報通信方法。

【0262】

〔発明I〕

特定のサービスを提供する機器であるサービス用機器と、当該特定のサービスを利用する際の認証を行う機器であって情報通信手段を介して前記サービス用機器と通信可能な機器である認証用機器と、を備えた情報通信システムであって、前記サービス用機器と前記認証用機器とのペアリングが成立したことを前提に、当該特定のサービスを利用可能とするための認証を行う情報通信システム、を用いて行う情報通信方法であって、

前記サービス用機器が、当該サービス用機器側の秘密鍵であるサービス側秘密鍵と当該サービス側秘密鍵に対応する公開鍵であるサービス側公開鍵とを生成して、当該サービス側秘密鍵を記憶するとともに、当該サービス側公開鍵を、当該サービス用機器に係る特定のサービスの識別標識であるサービスIDとともに、前記認証用機器に送信するサービス側登録ステップと、

前記認証用機器が、前記サービス用機器から前記サービス側公開鍵を受信すると、当該サービス側公開鍵を当該サービスIDと関連付けて記憶する認証側登録ステップと、

前記認証用機器が、前記サービス用機器からサービスIDを指定した認証を求める情報を受信すると、当該認証用機器において用意した任意のデータである認証側元データを前記認証側登録部に記憶されている前記サービスIDに対応する前記サービス側公開鍵を用いて暗号化したデータである認証側暗号化データを前記サービス用機器に送信する認証側暗号ステップと、

前記サービス用機器が、前記認証用機器から受信した認証側暗号化データを当該サービス側登録部に記憶されているサービス側秘密鍵を用いて復号化したデータである認証側復号化データに所定の演算を施して得られる認証側演算化データを前記認証用機器に送信するサービス側復号ステップと、

前記認証用機器が、前記サービス用機器から受信した認証側演算化データが、前記認証側元データに当該所定の演算を施して得られるデータと一致する場合は、前記サービスIDが真正であると判定するサービスID真正判定ステップと、

を備えたこと、

を特徴とする、情報通信方法。

【0263】

なお、図5に示すステップS1～ステップS2、ステップS8～ステップS11、図8に示すステップS27～ステップS30、図9に示すステップS33、ステップS36～ステップS37および図10に示すステップS41～ステップS43が、図2の第1の機器6の第1制御部10に対応する。

【0264】

このうち、ステップS2、ステップS9～ステップS11およびステップS36が、ペアリング提供処理部11に対応する。

【0265】

このうち、ステップS36が応答用文字列取得処理部12に対応する。

【0266】

図6に示すステップS12～ステップS19、図7に示すステップS22、ステップS25～ステップS26、図8に示すステップS32、図9に示すステップS34～ステップS35およびステップS38～ステップS40が、図2の第2の機器7の第2制御部15に対応する。

【0267】

このうち、ステップS15～ステップS19およびステップS35が、ペアリング受諾処理部16に対応する。

【0268】

このうち、ステップS15およびステップS17～ステップS18が桁上げ処理部17に対応し、ステップS35が確認用文字列表示処理部18に対応する。

【0269】

図5に示すステップS3～ステップS7、図7に示すステップS20～ステップS24および図8に示すステップS31が、図2のサーバ装置4のサーバ側制御部20に対応する。

【0270】

このうち、ステップS20～ステップS21、ステップS23～ステップS24およびステップS31が、ペアリング判定処理部21に対応する。

【0271】

このうち、ステップS23～ステップS24が再ペアリング実行指示処理部22に対応する。

【0272】

なお、この実施形態においては、情報通信システム2のサーバ装置4側のプログラムを記憶した記録媒体として、HDDに装着されたハードディスクを例示し、第1の機器6および第2の機器7側のプログラムを記憶した記録媒体として、SSDに装着されたフラッシュメモリを例示しているが、プログラムを記憶した記録媒体はこれらに限定されるものではなく、プログラムを記憶した記録媒体として、たとえば、外部メモリカード、CD-ROM、DVD-ROM、フレキシブルディスク、磁気テープを用いることもできる。さらに、主記憶装置もプログラムを記憶した記録媒体として用いることができる。

【0273】

また、プログラムの配布態様は特に限定されるものではなく、記録媒体にプログラムを記憶した状態で配布するほか、有線や無線の情報通信手段を介して当該プログラムを配布するようにしてもよい。

【0274】

また、プログラムの記録態様は特に限定されるものではない。直接実行できる形で記録媒体に記憶したり配布したりする他、たとえば、解凍して使用するように圧縮された形で記録媒体に記憶したり配布したりすることもできる。

【0275】

なお、上述の各実施形態においては、コンピュータを用いて図2および図3の各機能を

10

20

30

40

50

実現する場合を例に説明したが、これらの機能の一部または全部を、ハードウェアロジックを用いて構成するようにしてもよい。

【0276】

また、上述のブロック図、ハードウェア構成、フローチャート、データベース（テーブル）の構成、表示画面の構成等は、例として挙げたものであり、本願発明は、これらに限定されるものではない。

【0277】

上記においては、本発明を好ましい実施形態として説明したが、各用語は、限定のために用いたのではなく、説明のために用いたものであって、本発明の範囲および精神を逸脱することなく、添付のクレームの範囲において、変更することができるものである。また、上記においては、本発明のいくつかの典型的な実施形態についてのみ詳細に記述したが、当業者であれば、本発明の新規な教示および利点を逸脱することなしに上記典型的な実施形態において多くの変更が可能であることを、容易に認識するであろう。したがって、そのような変更はすべて、本発明の範囲に含まれるものである。

【符号の説明】

【0278】

4：サーバ装置

6：第1の機器

7：第2の機器

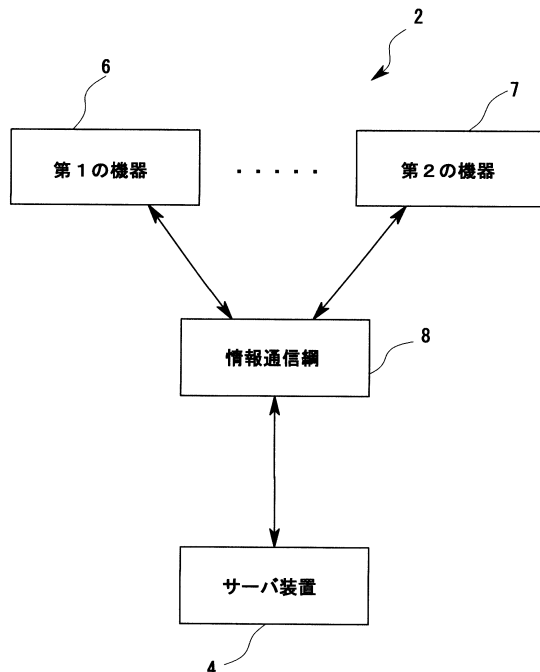
11：ペアリング提供処理部

16：ペアリング受諾処理部

21：ペアリング判定処理部

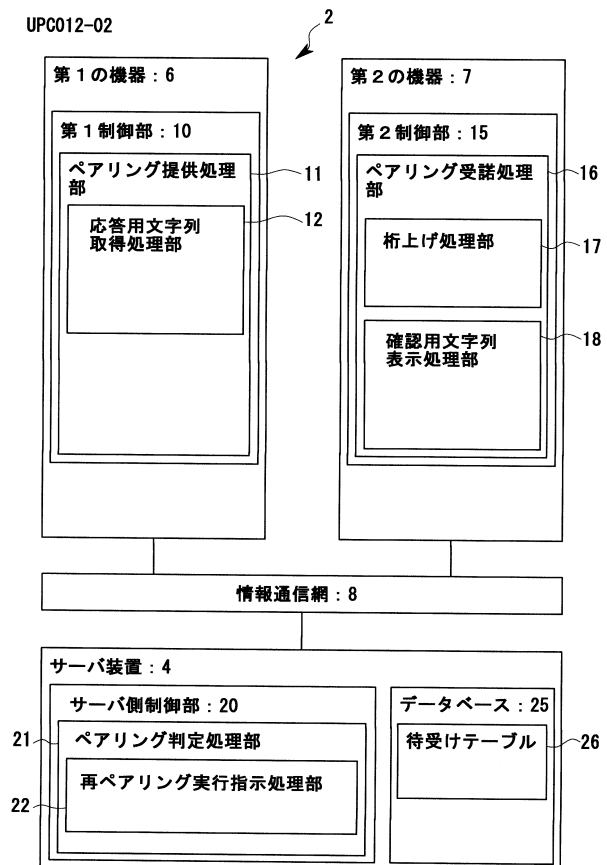
【図1】

UPC012-01



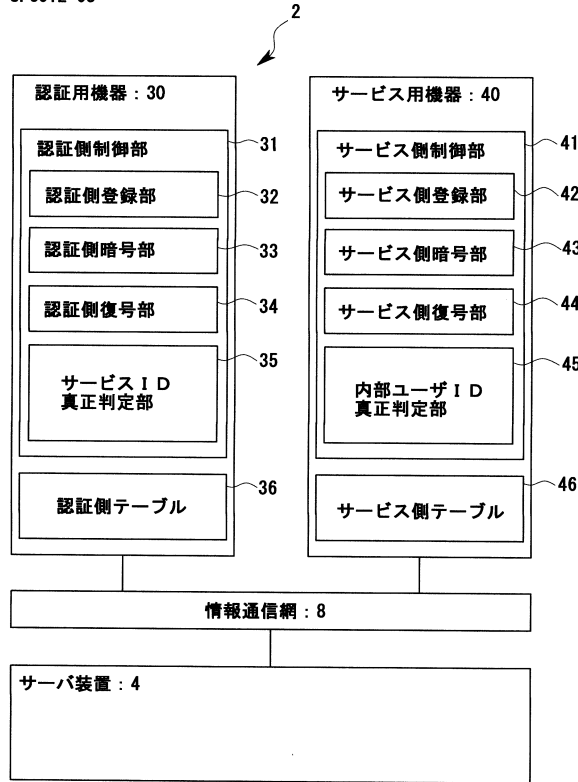
【図2】

UPC012-02



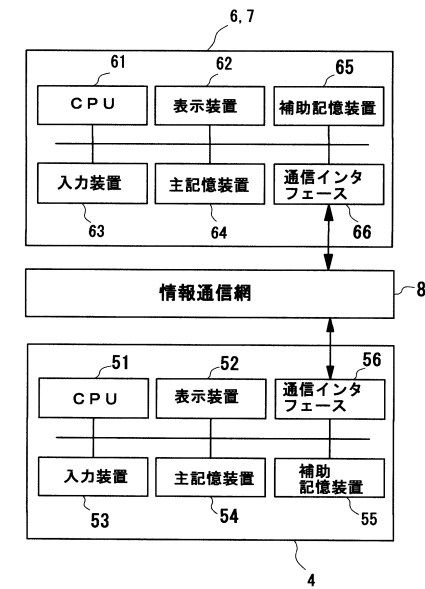
【図 3】

UPC012-03



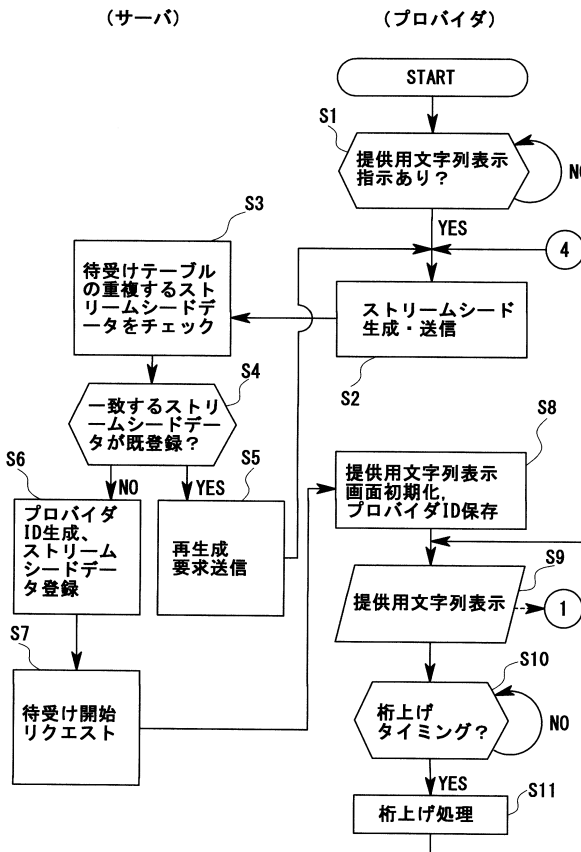
【図 4】

UPC012-04



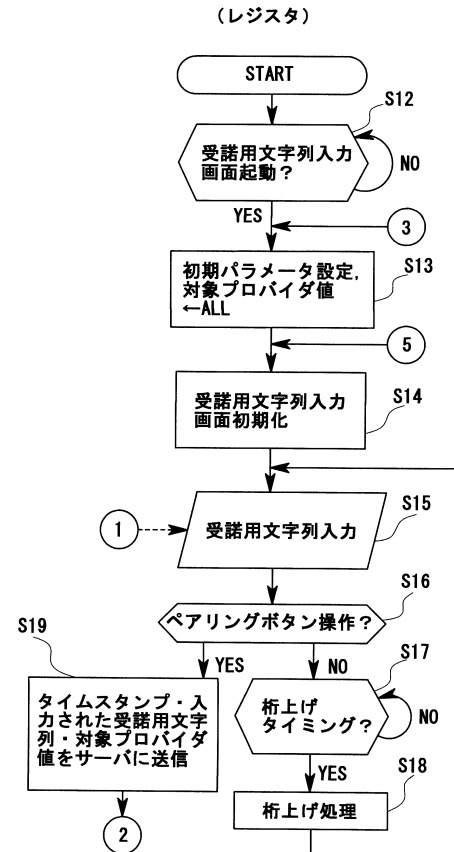
【図 5】

UPC012-05



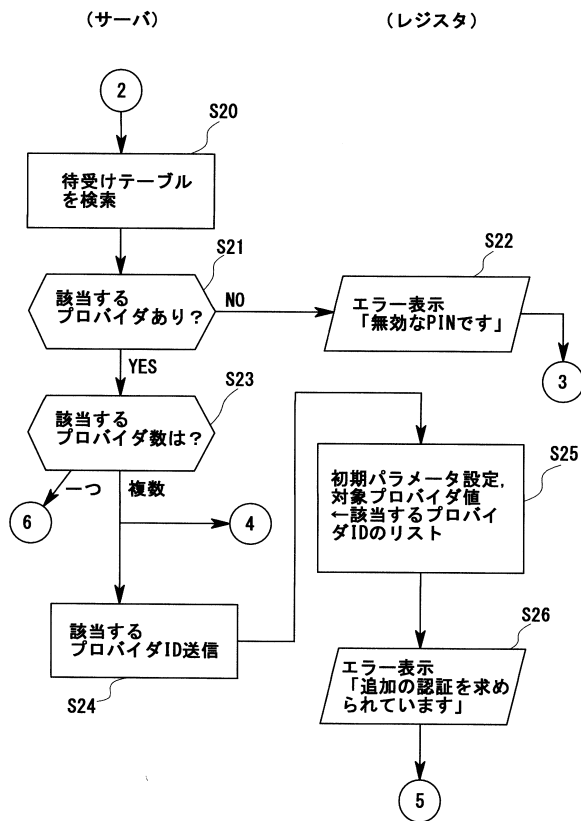
【図 6】

UPC012-06



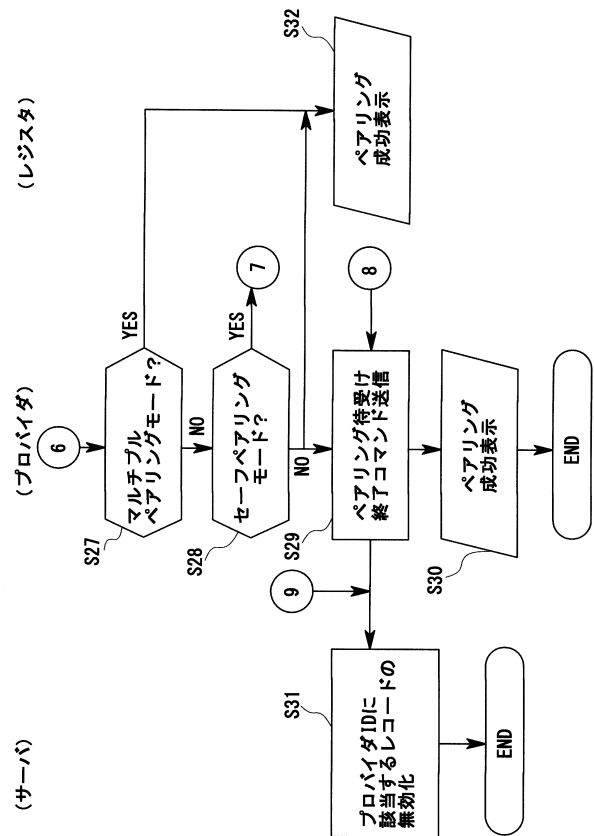
【図 7】

UPC012-07



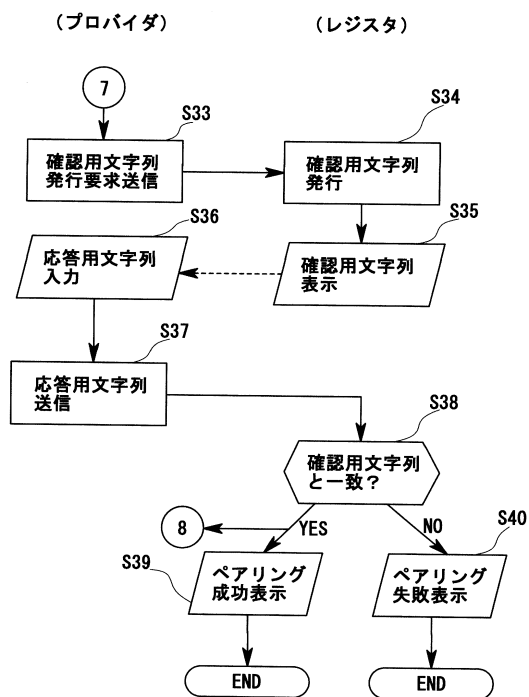
【図 8】

UPC012-08



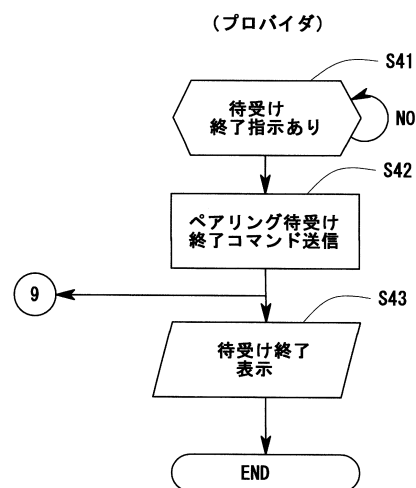
【図 9】

UPC012-09



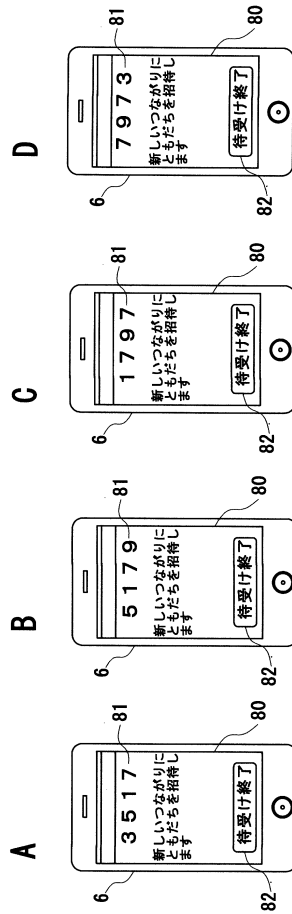
【図 10】

UPC012-10



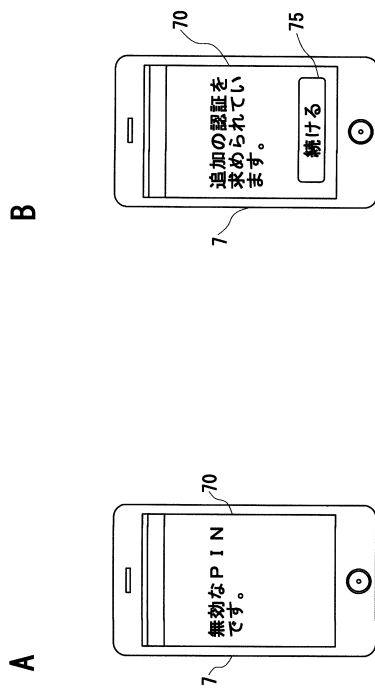
【図 1 1】

UPC012-11



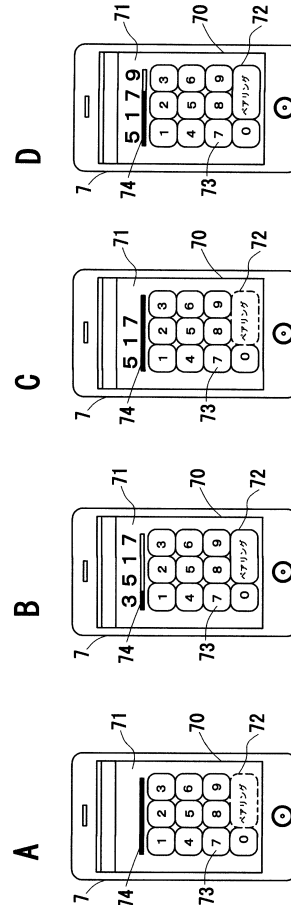
【図 1 3】

UPC012-13



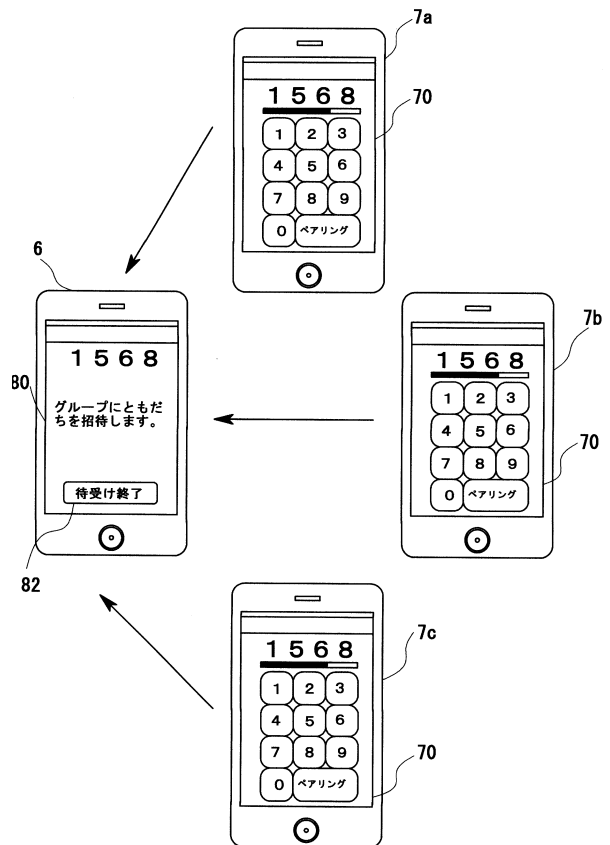
【図 1 2】

UPC012-12

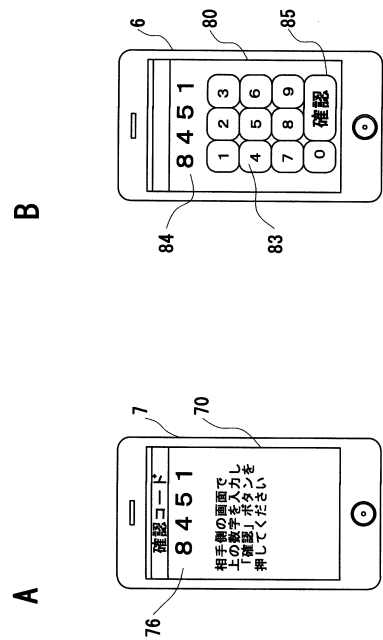


【図 1 4】

UPC012-14



【図 1 5】
UPC012-15



【図 1 6】
UPC012-16

プロバイダID	ストリームシードデータ	
	タイムヘッダ	ストリームシード
123456	2015.6.4 10:45:20	35179734 . . . 02
123455	2015.6.4 10:42:10	23867921 . . . 94
123454	2015.6.4 10:38:50	76134463 . . . 77
.	.	.
.	.	.

【図 1 7】
UPC012-17

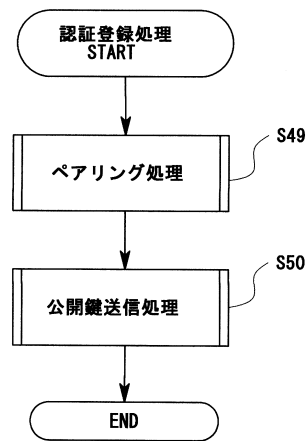
A

受諾用文字列	7973
タイムスタンプ	2015.6.4 10:45:50
対象プロバイダ値	A L L

B

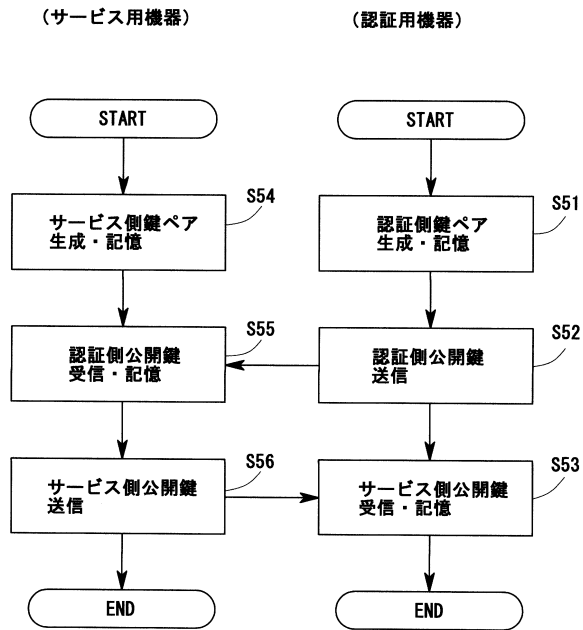
プロバイダID	ストリームシードデータ	
	タイムヘッダ	ストリームシード
123456	2015.6.4 10:45:20	35179734 . . . 02
.	.	.
.	.	.

【図 1 8】
UPC012-18



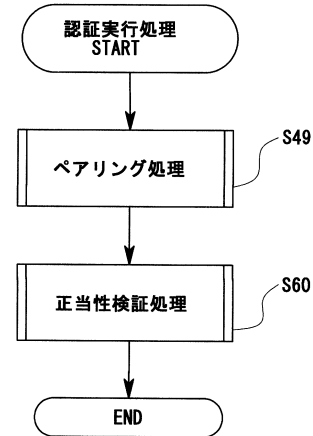
【図 19】

UPC012-19



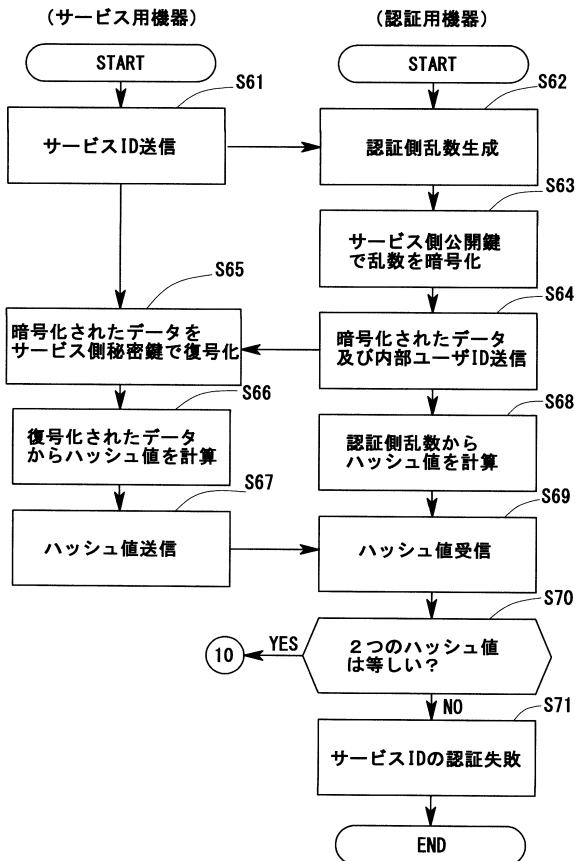
【図 20】

UPC012-20



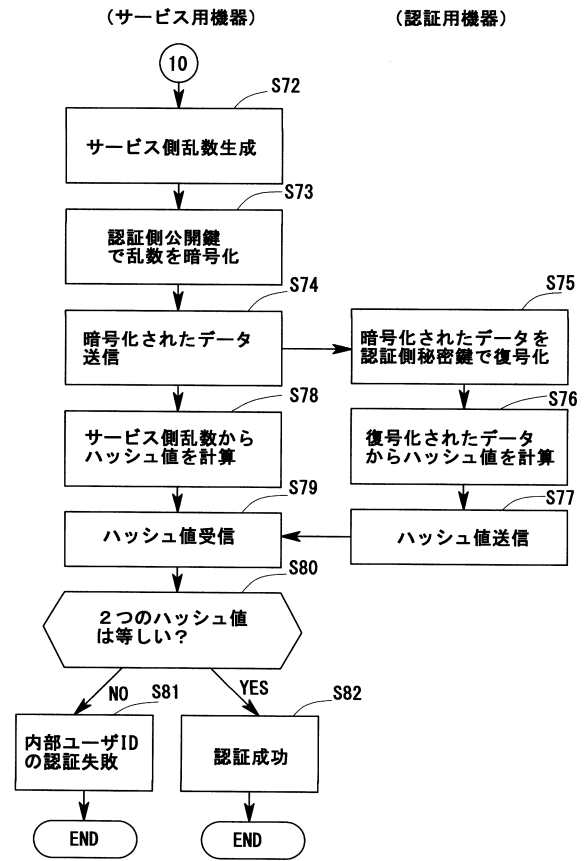
【図 21】

UPC012-21

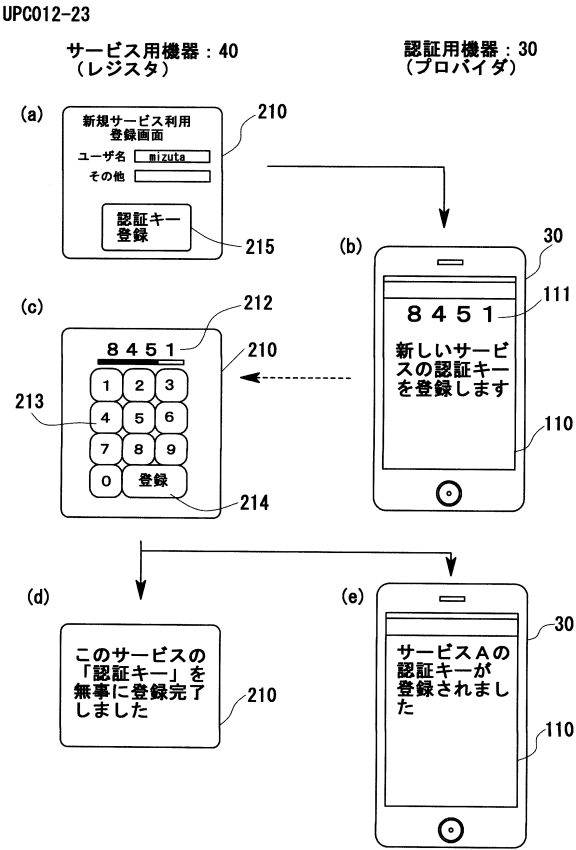


【図 22】

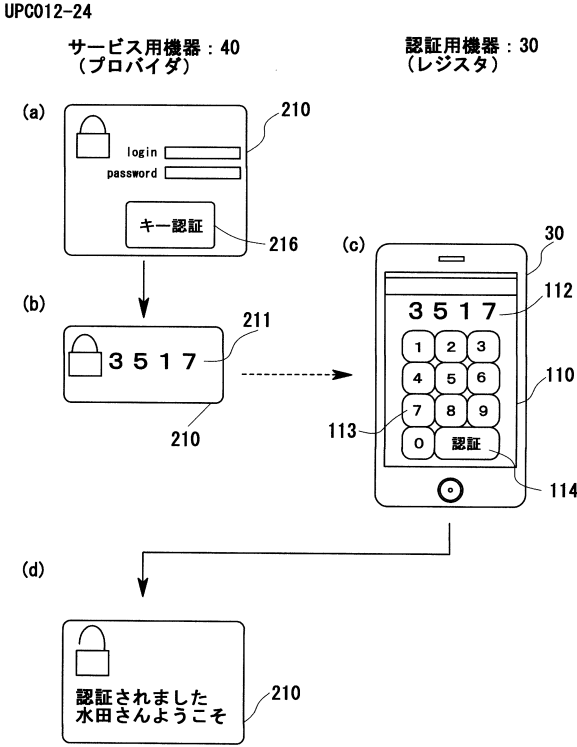
UPC012-22



【図 2 3】



【図 2 4】



【図 2 5】

UPC012-25

サービスID	サービス名	内部ユーザID	鍵グループID	種別	鍵
N/A	N/A	N/A	0	秘密鍵	Afd4indak...
N/A	N/A	N/A	0	公開鍵	d35n4p2q...
AAA	サービスA	BBB	0	公開鍵	4zcdp3iz...
CCC	サービスC	DDD	0	公開鍵	lzp18dbsu9...
N/A	N/A	N/A	1	秘密鍵	M1100jCCAb...
N/A	N/A	N/A	1	公開鍵	CAQAwgYw...
EEE	サービスE	FFF	1	公開鍵	o6J4mbz7...

【図 2 6】

UPC012-26

内部ユーザID	鍵グループID	種別	鍵
N/A	0	秘密鍵	Afd4indak...
N/A	0	公開鍵	4zcdp3iz...
BBB	0	公開鍵	d35n4p2q...
GGG	0	公開鍵	SAH+Vd4p...
N/A	1	秘密鍵	WajblnH22...
N/A	1	公開鍵	sRI9zwWh5...
HHH	1	公開鍵	AMA0GCSq...

フロントページの続き

(56)参考文献 特表2010-506542 (JP, A)
特開2011-101338 (JP, A)
特開2003-124927 (JP, A)
特開2008-046554 (JP, A)
特開2014-238635 (JP, A)

(58)調査した分野(Int.Cl., DB名)

G09C1/00-5/00
H04K1/00-3/00
H04L9/00-9/38
H04M1/00
1/24-3/00
3/16-3/20
3/38-3/58
7/00-7/16
11/00-11/10
99/00