(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7629151号
(P7629151)

(45)発行日　令和7年2月13日(2025.2.13)

(24)登録日　令和7年2月4日(2025.2.4)

(51)国際特許分類

Ｈ０４Ｌ	*61/00*	*(2022.01)*	Ｈ０４Ｌ	61/00
Ｇ０６Ｆ	*21/33*	*(2013.01)*	Ｇ０６Ｆ	21/33

ＦＩ

請求項の数　18　（全17頁）

(21)出願番号　特願2018-232482(P2018-232482)
(22)出願日　平成30年12月12日(2018.12.12)
(65)公開番号　特開2020-96275(P2020-96275A)
(43)公開日　令和2年6月18日(2020.6.18)
審査請求日　令和3年12月3日(2021.12.3)
審判番号　不服2023-11136(P2023-11136/J1)
審判請求日　令和5年7月4日(2023.7.4)

(73)特許権者　521314127
帝都 久利寿
京都府京都市下京区四条烏丸西入ル函谷鉾町８３番地 コネクトフリー株式会社内
(73)特許権者　514318600
コネクトフリー株式会社
京都府京都市下京区四条烏丸西入ル函谷鉾町８３番地
(74)代理人　110001195
弁理士法人深見特許事務所
(72)発明者　帝都 久利寿
京都府京都市下京区四条烏丸西入ル函谷鉾町８３番地 コネクトフリー株式会社内
(72)発明者　岡本 光弘
京都府京都市下京区四条烏丸西入ル函谷
最終頁に続く

(54)【発明の名称】　情報通信方法及び情報通信システム

(57)【特許請求の範囲】

【請求項１】

ユーザに関連付けられた第１のデバイスに向けられた第１のネットワークアドレスを生成するステップと、

第２のデバイスに向けられた第２のネットワークアドレスを生成するステップと、

前記第１及び第２のネットワークアドレスに対して、認証局で認証を行った後に、前記第１のネットワークアドレス及び前記第２のネットワークアドレスをそれぞれ前記第１のデバイス及び前記第２のデバイスに設定するステップと、

前記第１のネットワークアドレスと前記ユーザの個人情報を含むユーザ情報とを関連付けるステップと、

前記第１のデバイスと第２のデバイスとが通信するステップと、

前記第２のデバイスが前記第１のネットワークアドレスに関連付けられた前記ユーザ情報を参照するステップとを含む、情報通信方法。

【請求項２】

前記参照するステップの後に、前記第２のデバイスは前記ユーザ情報に基づいて、前記第１のデバイスを所有するユーザの前記ユーザ情報を取得することなくサービスを提供する、請求項１に記載の情報通信方法。

【請求項３】

前記ユーザ情報の関連付けは前記ユーザによる承認によって行われる、請求項１または２に記載の情報通信方法。

【請求項４】
前記ユーザ情報の関連付けは前記第２のデバイスの要求によって行われる、請求項１から３のうちいずれか一項に記載の情報通信方法。
【請求項５】
前記第１のデバイスはポータブル端末であって、該ポータブル端末は回線契約時のユーザ情報を前記第１のネットワークアドレスと関連付ける、請求項１から４のうちいずれか一項に記載の情報通信方法。
【請求項６】
第１のネットワークアドレスをユーザに関連付けられた第１のデバイスに予め固有に設定するステップを備え、前記第１のネットワークアドレスは、暗号学的に決定されたものであり、
前記第１のネットワークアドレスと前記ユーザの個人情報を含むユーザ情報とを関連付けるステップと、
前記第１のデバイスと第２のデバイスとが通信するステップと、
前記第２のデバイスが前記第１のネットワークアドレスに関連付けられた前記ユーザ情報を参照するステップと、
前記第２のデバイスが前記ユーザ情報に基づき、前記ユーザがサービス利用アカウントを有しているかどうかを判定するステップとを含む、情報通信方法。
【請求項７】
前記第１のデバイスに前記第１のネットワークアドレスを生成するステップと、
前記第２のデバイスに第２のネットワークアドレスを生成するステップと、
前記第１及び第２のネットワークアドレスに対して、認証局で認証を行った後に、前記第１のネットワークアドレス及び前記第２のネットワークアドレスをそれぞれ前記第１のデバイス及び前記第２のデバイスに設定するステップとをさらに含む、請求項６に記載の情報通信方法。
【請求項８】
前記判定するステップにて前記ユーザが前記サービス利用アカウントを有していないと判定された場合、前記第２のデバイスは前記第１のデバイスに前記サービス利用アカウントを生成することを求めることを特徴とする、請求項６又は７に記載の情報通信方法。
【請求項９】
前記第１のデバイスにて前記サービス利用アカウントを生成することが認められた場合、前記第２のデバイスは前記サービス利用アカウントの情報を保存する、請求項８に記載の情報通信方法。
【請求項１０】
前記判定するステップにて前記ユーザが前記サービス利用アカウントを有していると判定された場合、前記第２のデバイスは前記第１のデバイスに対してサービスの利用を許可する、請求項６又は７に記載の情報通信方法。
【請求項１１】
前記第１のデバイスはポータブル端末であって、該ポータブル端末は回線契約時のユーザ情報を前記第１のネットワークアドレスと関連付ける、請求項６から１０のうちいずれか一項に記載の情報通信方法。
【請求項１２】
請求項１から１１のうちいずれか一項に記載の情報通信方法をコンピュータに実行させるためのプログラム。
【請求項１３】
情報通信システムであって、
第１のネットワークアドレスを有する端末装置と、
第２のネットワークアドレスを有するサーバと、
第３のネットワークアドレスを有するデータベースとを備え、
前記第１、第２及び第３の認証済みネットワークアドレスの各々は、暗号学的に決定され

たものであり、
前記データベースは、前記端末装置の前記第１のネットワークアドレスに関連付けて、前記端末装置のユーザのユーザ情報を有しており、前記ユーザ情報は前記ユーザの個人情報を含み、
前記サーバは、前記データベースに、前記端末装置の前記第１のネットワークアドレスに基づく問い合わせを行い、
前記サーバは、前記データベースからの前記第１のネットワークアドレスに関連付けられた前記ユーザ情報を参照する、情報通信システム。
【請求項１４】
前記第１、第２及び第３の認証済みネットワークアドレスは、認証局によって認証を得た後に前記端末装置、前記サーバ、および前記データベースにそれぞれ設定される、請求項１３に記載の情報通信システム。
【請求項１５】
前記ユーザ情報は、クレジットカード情報を含む、請求項１３または１４に記載の情報通信システム。
【請求項１６】
ユーザに関連付けられた第１のデバイスと、
第２のデバイスと、
前記第１のデバイスに予め固有に設定された第１のネットワークアドレスとを含み、前記第１のネットワークアドレスは、暗号学的に決定されたものであり、
前記第１のネットワークアドレスは前記第１のデバイスにおいて前記ユーザの個人情報を含むユーザ情報と関連付けられており、
前記第２のデバイスは前記第１のデバイスとの通信時に前記第１のネットワークアドレスに関連付けられた前記ユーザ情報を参照する、情報通信システム。
【請求項１７】
所定のサイトを提供するサーバによって実行される方法であって、
ユーザに関連付けられた端末装置から前記端末装置に予め設定された固有のネットワークアドレスと、前記固有のネットワークアドレスに関連付けられると共に、前記ユーザの個人情報及び属性情報を含む電子証明書とを受信するステップと、
前記電子証明書に含まれる前記ユーザの属性情報に基づいて、前記所定のサイトに対する前記ユーザのログインを許可するステップとを含む、方法。
【請求項１８】
前記ログインを許可するステップは、
前記ユーザの属性情報が前記所定のサイトのログインに必要なユーザログイン情報を含んでいるかどうかを判定するステップと、
前記ユーザの属性情報が前記ユーザログイン情報を含んでいる場合に、前記所定のサイトに対する前記ユーザのログインを許可するステップとを含む、請求項１７に記載の方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、情報通信方法及び情報通信システムに関する。
【背景技術】
【０００２】
近年の情報通信技術の発展は目覚ましく、インターネットなどのネットワークに接続されるデバイスは、従来のパーソナルコンピュータやスマートフォンといったユーザが利用する情報処理装置に限らず、例えばサーバや工業用計測器のような様々なモノ（things）に広がっている。このような技術トレンドは、「ＩｏＴ（Internet of Things；モノのインターネット）」と称され、様々な技術およびサービスが提案および実用化されつつある（特許文献１を参照）。
【０００３】

例えば、特許文献１では、プロバイダから測定器に対してＩＰアドレスが割り当てられており、各測定器からクラウドサーバへ通信を行うためにはＩｏＴ中継機器によってプロトコル変換を行う必要がある。さらに、従来の方式では、ローカルエリアネットワーク（ＬＡＮ）と他のローカルエリアネットワーク（ＬＡＮ）との間の通信を行う場合、一般に、通信相手を決定するためにグローバルＩＰアドレスを固定し、セキュリティを保つためにＩＰパケットを暗号化して通信を行う。

【０００４】

また通常、ネットワーク上では、各デバイスに静的または動的に割り当てられたネットワークアドレスを用いて、デバイス間のデータ通信が実現される。このようなネットワークアドレスとしては、典型的には、ＩＰ（Internet Protocol）アドレスが用いられる。

【０００５】

一般的に、ＩＰアドレスは、グローバルアドレスのように、インターネット上で一意に定められるものと、プライベートアドレスのように、プライベートネットワーク上において重複なく割り当てられるものとがある。また、ＤＨＣＰ（Dynamic Host Configuration Protocol）などを用いて、ＩＰアドレスを動的に割り当てるような仕組みも存在する。

【０００６】

このように、ＩＰアドレスの設定は、データ通信のために、同一ネットワーク上において重複なく割り当てられることのみが考慮される。つまり、ＩＰアドレスは、対象のネットワークに応じて、任意に設定されるネットワークアドレスである。

【先行技術文献】

【特許文献】

【０００７】

【文献】特開２０１８－１４２２４７号公報

【発明の概要】

【発明が解決しようとする課題】

【０００８】

従来のネットワークアドレスは、通信先を特定するための識別情報としてプロバイダから割り当てられるものである。しかしながら、そのアドレス自体には何の信頼性も付与されていない。そのため、ＩＰアドレスを用いてデバイス間でデータ通信する際の認証処理は、より上位の層（例えば、アプリケーション層など）で実現される。

【０００９】

例えば、ＳＮＳサービス運営会社、インターネットショッピングの提供会社、又は会員制サイト運営会社（以下、サービス提供会社ということがある）はサービスを提供するにあたってユーザの情報を取得して利用する必要がある。ユーザの情報とは、氏名、生年月日、性別、住所、電話番号、各種口座情報などである。サービス提供会社はユーザ情報に基づいてサービス利用アカウントを生成しユーザに対して割り当てる。サービス提供会社は社内のサーバ又は外部のサーバにてユーザ情報としてのサービス利用アカウントを管理する。

【００１０】

しかしながら、昨今のセキュリティ事情を鑑みるとサービス提供会社にとってはユーザ情報を管理すること自体がサービス運営上のリスクとなりうる。サービス提供会社において、サーバからユーザ情報を漏洩させないようにするためには、例えばアプリケーション層にて高額なセキュリティ対策を実施する必要がある。ただし、現在のインターネットの仕組みではアプリケーション層でのセキュリティ強化だけでは不十分である場合がある。また、ユーザ側の努力では十分でない場合もある。

【００１１】

本開示は、セキュアにユーザ情報を利用することができる情報通信方法及び情報通信システムを提供することを目的とする。

【課題を解決するための手段】

【００１２】
本開示の一態様にかかる情報通信方法は、認証局で認証された第１のネットワークアドレスをユーザに関連付けられた端末装置に予め固有に設けるステップと、
前記認証局で認証された第２のネットワークアドレスをサーバに予め固有に設けるステップと、
前記第１のネットワークアドレスと前記ユーザのユーザ情報とを関連付けるステップと、
前記端末装置と前記サーバとを通信接続するステップと、
前記サーバが前記ユーザ情報を参照するステップと、を含む。
【００１３】
上記情報通信方法によれば、サービス提供会社にてユーザ情報の管理を行う必要がない。
【００１４】
また、前記情報通信方法は、前記端末装置に前記第１のネットワークアドレスを生成するステップと、
前記サーバに前記第２のネットワークアドレスを生成するステップと、
前記第１及び第２のネットワークアドレスに対して、前記認証局で認証を行った後に、前記第１のネットワークアドレス及び前記第２のネットワークアドレスをそれぞれ前記端末装置及び前記サーバに設定するステップと、をさらに含んでもよい。
【００１５】
上記情報通信方法によれば、デバイスにネットワークアドレスが設定される前に認証が行われている。この認証情報に基づいて通信可否の判断が可能であるため、なりすましを好適に防止しうる。
【００１６】
また、前記情報通信方法において、前記参照の後に、前記サーバは前記ユーザ情報に基づいて、前記端末装置を所有するユーザの前記ユーザ情報を取得することなくサービスを提供してもよい。
【００１７】
上記情報通信方法によれば、ユーザに対してユーザ情報の入力をさせなくてもよいので、ユーザがサービスに対してストレスを感じなくて済む。
【００１８】
また、前記情報通信方法において、前記ユーザ情報の関連付けは前記ユーザによる承認によって行われてもよい。
【００１９】
上記情報通信方法によれば、ユーザはユーザ情報の関連付け処理が行われることを把握できる。
【００２０】
また、前記情報通信方法において、前記ユーザ情報の関連付けは前記サーバの要求によって行われてもよい。
【００２１】
上記情報通信方法によれば、必要に応じてユーザ情報の関連付けが行われるので、予めユーザが関連付け操作をしておくという手間を省くことができる。
【００２２】
また、前記情報通信方法において、前記端末装置はポータブル端末であって、該ポータブル端末は回線契約時のユーザ情報を前記第１のネットワークアドレスと関連付けられてもよい。
【００２３】
上記情報通信方法によれば、ポータブル端末の回線契約時のデータがそのままユーザ情報として利用できる。
【００２４】
本開示の一態様にかかる情報通信方法は、認証局で認証された第１のネットワークアドレスをユーザに関連付けられた端末装置に予め固有に設けるステップと、

前記認証局で認証された第２のネットワークアドレスをサーバに予め固有に設けるステップと、
前記第１のネットワークアドレスと前記ユーザのユーザ情報とを関連付けるステップと、
前記端末装置と前記サーバとを通信接続するステップと、
前記サーバが前記ユーザ情報を参照するステップと、
前記サーバが前記ユーザ情報に基づき、前記ユーザがサービス利用アカウントを有しているかどうかを判定するステップと、を含む。

【００２５】

上記情報通信方法によれば、サービス提供会社が行うサービスの販促を効率的に行うことができる。

【００２６】

また、前記情報通信方法は、前記端末装置に前記第１のネットワークアドレスを生成するステップと、
前記サーバに前記第２のネットワークアドレスを生成するステップと、
前記第１及び第２のネットワークアドレスに対して、前記認証局で認証を行った後に、前記第１のネットワークアドレス及び前記第２のネットワークアドレスをそれぞれ前記端末装置及び前記サーバに設定するステップと、をさらに含んでもよい。

【００２７】

上記情報通信方法によれば、デバイスにネットワークアドレスが設定される前に認証が行われている。この認証情報に基づいて通信可否の判断が可能であるため、なりすましを好適に防止しうる。

【００２８】

また、前記情報通信方法において、前記判定ステップにて前記ユーザが前記サービス利用アカウントを有していないと判定された場合、前記サーバは前記端末装置に前記サービス利用アカウントを生成することを求めてもよい。

【００２９】

上記情報通信方法によれば、サービス提供会社はユーザがゲストなのかサービス利用アカウントを有しているのを判断できるから、ゲストユーザだけにサービス利用の提案を行うことができる。

【００３０】

また、前記情報通信方法において、前記端末装置にて前記サービス利用アカウントを生成することが認められた場合、前記サーバは前記サービス利用アカウント情報を保存してもよい。

【００３１】

上記情報通信方法によれば、サービス利用アカウントがあるかないかだけを保持すればよく、その他の機密情報を保持する必要がない。

【００３２】

また、前期情報通信方法において、前記判定ステップにて前記ユーザが前記サービス利用アカウントを有していると判定された場合、前記サーバは前記端末装置に対してサービスの利用を許可してもよい。

【００３３】

上記情報通信方法によれば、既にサービスを利用しているユーザに対してストレスを与えずに済む。

【００３４】

また、前期情報通信方法において、前記端末装置はポータブル端末であって、該ポータブル端末は回線契約時のユーザ情報を前記第１のネットワークアドレスと関連付けてもよい。

【００３５】

上記情報通信方法によれば、ポータブル端末の回線契約時のデータがそのままユーザ情報として利用できる。

【００３６】
本開示の一態様にかかる情報通信方法は、認証局で認証された第１のネットワークアドレスと、
前記認証局で認証された第２のネットワークアドレスと、
前記認証局で認証された第３のネットワークアドレスと、を有する情報通信方法であって、
前記第３のネットワークアドレスによって前記第１のネットワークアドレスを認証するステップと、
前記第２のネットワークアドレスと前記第３のネットワークアドレスとを関連付けて認証するステップと、を有し、
前記第２のネットワークアドレスによって前記前記第３のネットワークアドレスに認証された前記第１のネットワークアドレスを認証するステップと、を含む。
【００３７】
上記情報通信方法によれば、データ発行体がユーザに対して認証を与えるため、サービス提供会社はデータ発行体のデータベースにアクセスして認証確認をする必要がない。
【００３８】
また、前記情報通信方法において、前記第１、第２及び第３のネットワークアドレスは、認証局によって認証を得た後にデバイスに設定されてもよい。
【００３９】
上記情報通信方法によれば、デバイスにネットワークアドレスが設定される前に認証が行われている。この認証情報に基づいて通信可否の判断が可能であるため、なりすましを好適に防止しうる。
【００４０】
また、前記情報通信方法において、前記第１のネットワークアドレスは端末装置に設定され、前記第２のネットワークアドレスは第１のサーバに設定され、前記第３のネットワークアドレスは第２のサーバに設定されてもよい。
【００４１】
上記情報通信方法によれば、ユーザは所定の端末装置における所定のサービス利用時にデータ発行体の情報を意識せずに利用することができる。また、サービス提供会社等においては、データの真正を確認する手間を省略できる。
【００４２】
本開示の一態様にかかる情報通信システムは、端末装置と、
サーバと、
認証サーバと、
前記認証サーバから認証を得ることで前記端末装置に予め固有に設けられた第１のネットワークアドレスと、
前記認証サーバから認証を得ることで前記サーバに予め固有に設けられた第２のネットワークアドレスと、を有し、
前記第１のネットワークアドレスは前記端末装置においてユーザ情報と関連付けられており、
前記サーバは前記端末装置との通信時に前記ユーザ情報を参照する、ことを含む。
【００４３】
上記情報通信システムによれば、サービス提供会社にてユーザ情報の管理を行う必要がない。
【発明の効果】
【００４４】
本開示によれば、セキュアにユーザ情報を利用することができる情報通信方法及び情報通信システムを提供することができる。
【図面の簡単な説明】
【００４５】

【図１】ネットワークアドレス生成の一例を示すフローチャートである。
【図２】端末装置と他の装置との通信接続の一例を示す模式図である。
【図３】端末装置のハードウェア構成とサーバのハードウェア構成の一例を示す模式図である。
【図４】端末装置とサーバとの通信接続の一例を示す模式図である。
【図５】電子証明書と電子証明書に付随する認証情報の構成の一例を示す模式図である。
【図６】端末装置とサーバ間での認証処理手順の一例を示すフローチャートである。
【図７】端末装置でインターネットサービスを利用する場合に端末装置に表示される画面の一例を示す図である。
【図８】端末装置でインターネットサービスを利用する場合に端末装置に表示される画面の一例を示す図である。
【図９】端末装置とサーバ間での別の認証処理手順の一例を示すフローチャートである。
【図１０】端末装置、サーバ、及びデータベース間の認証を示す模式図である。
【発明を実施するための形態】
【００４６】
以下、本実施形態について、図面を参照しながら詳細に説明する。なお、図中の同一または相当部分については、同一符号を付してその説明は繰返さない。また、複数の実施形態が存在する場合、共通する符号は援用して用いるものとしてその説明は繰り返さない。
【００４７】
まず、図１においてネットワークアドレスの生成方法の一例を説明する。（Ｓ１）まず、デバイスが有する静的な秘密鍵に対して所定の暗号学的アルゴリズム関数をかけることで公開鍵を生成する。（Ｓ２）その文字列の先頭または任意の部分が１２８ビットのＩＰｖ６空間であってユニークローカルアドレスの文字列となるまで計算を繰り返す。なお、ユニークローカルアドレスとはｆｃ又はｆｄから始まるアドレス空間を意味する。（Ｓ３）ＩＰｖ６のユニークローカルアドレスに対応する文字列が生成された場合、その公開鍵に対して暗号学的ハッシュ関数をかけることで所定の値を生成し、当該所定の値をネットワークアドレスとして設定するとともに、認証局によって公開鍵に対して正式ライセンスを付与する。（Ｓ４）上記一連のプロセスによってデバイスの公開鍵と紐付けて発行された認証済みネットワークアドレスが生成される。認証局としては例えば認証サーバが用いられるが、サーバ装置に限定されない。
【００４８】
なお、（Ｓ１）の公開鍵の生成ステップの前に乱数発生器等による秘密鍵の生成ステップを含んでもよい。乱数発生器はデバイスのシリアルナンバー等に基づき秘密鍵を生成しうる。さらに、上述のステップ（Ｓ１）から（Ｓ４）の処理はデバイス自身が実行するものであってもよいし、デバイスに対して他の装置が実行するものであってもよい。
【００４９】
上述のようにして得られたデバイスに固有のネットワークアドレスはＥＶＥＲ／ＩＰ（登録商標）と呼ばれることがある。ＥＶＥＲ／ＩＰ（登録商標）は従来のようにインターネットサービスプロバイダ（ＩＳＰ）から割り当てられるネットワークアドレスとは異なり、デバイス自身がＩＳＰの役目の一部を果たしている。また、ＥＶＥＲ／ＩＰ（登録商標）と公開鍵は対応関係にあり、同じ意味として用いられることがある。以下では、特に断りのない場合、ＥＶＥＲ／ＩＰ（登録商標）のことをＥｖｅｒＩＰという。
【００５０】
図２において、本実施形態における典型的な通信接続を説明する。端末装置１０、１１、１２、映像機器１３及びサーバ１４は通信インターフェースを有するデバイスである。本実施形態の通信ネットワーク２０は、ＯＳＩ参照モデルにおける物理層またはデータリンク層を考慮すればよい。ＥｖｅｒＩＰを有する２つの装置は物理層上のあらゆる通信経路を介して接続可能である。なお、各デバイスの初回セッション時には互いに暗号学的ハッシュ関数を計算することによって所定のハンドシェイクを完了する。
【００５１】

このような物理層上のＥｖｅｒＩＰ間の通信接続網を以下では「ＥＶＥＲネットワーク」という。なお、端末装置１０、１１、１２がそれぞれ近距離の無線通信によって通信が可能であれば、ＥＶＥＲネットワークはメッシュネットワークを構築することもできる。言い換えると、ＥＶＥＲネットワークは既存のネットワーク上に重ねて張り巡らされた第２のインターネットということができる。

【００５２】

ネットワークアドレスの典型例としてＩＰアドレスが採用される場合には、バージョンによって、規定されるビット数が異なっている。現在制定されているＩＰｖ４（Internet Protocol Version 4）においては、３２ビットのアドレス区間が規定されている。一方、現在制定されているＩＰｖ６（Internet Protocol Version 6）においては、１２８ビットのアドレス区間が規定されている。本実施形態においては、ネットワークアドレスの一例として、ＩＰｖ６に従うＩＰアドレスについて言及する。

【００５３】

本明細書において、「デバイス」という場合、通信ネットワーク２０を介してデータ通信が可能な任意のモノを包含する。典型的には、デバイスは、通信装置単体として構成されることもあるし、何らかのモノの一部として、あるいは、何らかのモノに組み込まれて構成されることもある。

【００５４】

図３に示すように、本実施形態に係る端末装置１０は、少なくともプロセッサとしてのＣＰＵ１０Ａと、ストレージ１０Ｂおよびメモリ１０Ｃを有している。サーバ１４は少なくともプロセッサとしてのＣＰＵ１４Ａと、ストレージ１４Ｂおよびメモリ１４Ｃを有している。また、端末装置１０やサーバ１４はそれぞれ図示しない通信インターフェース、電源、操作部等を適宜有している。メモリは、コンピュータ可読命令（例えば、情報処理プログラム）を記憶するように構成されている。例えば、メモリは、各種プログラム等が格納されたＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）及びプロセッサにより実行される各種プログラム等が格納される複数のワークエリアを有するＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）等から構成されてもよい。また、メモリは、フラッシュメモリ等によって構成されてもよい。尚、プロセッサは、ＣＰＵの代わりに、ＭＰＵ（Ｍｉｃｒｏ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）及びＧＰＵ（Ｇｒａｐｈｉｃｓ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）であってもよい。ＣＰＵは、複数のＣＰＵコアによって構成されてもよい。ＧＰＵは、複数のＧＰＵコアによって構成されてもよい。プロセッサは、ストレージ１０Ｂ、１４Ｂ又はＲＯＭに組み込まれた各種プログラムから指定されたプログラムをＲＡＭ上に展開し、ＲＡＭとの協働で各種処理を実行するように構成されてもよい。特に、プロセッサがメモリに記憶された情報処理プログラムを実行することで、端末装置１０は本実施形態に係る情報処理方法を実行するように構成される。

【００５５】

端末装置１０は、例えば、パーソナルコンピュータ、スマートフォン、タブレット、ユーザの身体（例えば、腕や頭等）に装着されるウェアラブルデバイス（例えば、スマートウォッチやＡＲグラス等）であってもよい。また、端末装置１０は、スマート家電、コネクティッド自動車、工場等に設置された制御機器であってもよい。このように、端末装置１０の種類は、ＩＰアドレスを用いてインターネット等の通信ネットワークに接続されると共に、プロセッサとメモリを備える全てのモノが対象となる。

【００５６】

ストレージ１０Ｂ、１４Ｂは、例えば、ＨＤＤ（Ｈａｒｄ Ｄｉｓｋ Ｄｒｉｖｅ）、ＳＳＤ（Ｓｏｌｉｄ Ｓｔａｔｅ Ｄｒｉｖｅ）、フラッシュメモリ等の記憶装置であって、プログラムや各種データを格納するように構成されている。ストレージ１０Ｂ、１４Ｂには、インターネット上のサーバから送信された本実施形態に係る情報処理プログラムが保存されてもよい。

【００５７】

本実施形態における通信インターフェースは、通信ネットワーク２０を介してサーバ等

の外部装置と通信するための各種有線接続端子を含んでもよい。また、通信インターフェースは、無線ルータ若しくは無線基地局と通信するための各種処理回路及びアンテナ等を含んでもよい。無線通信の規格は、例えば、Ｗｉ－Ｆｉ（登録商標）、Ｂｌｕｅｔｏｏｔｈ（登録商標）、ＺｉｇＢｅｅ（登録商標）、ＬＰＷＡ又は第５世代移動通信システム（５Ｇ）である。また、通信ネットワークは、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、無線アクセスネットワーク（ＲＡＮ）及びインターネットのうちの少なくとも一つを含む。

【００５８】

図４は、本実施形態の典型的な端末装置１０とサーバ１４との通信接続を示す。図４に示すように、端末装置１０は公開鍵としてのＥｖｅｒＩＰ２３に基づき例えばＴＣＰ／ＩＰプロトコルにてパケットをサーバ１４に送信する。このとき、端末装置１０は第１のネットワークアドレスとしてのＥｖｅｒＩＰ２３とともにＥｖｅｒＩＰ２３発行時に認証局にて認証された電子証明書２５Ａを同時にサーバ１４に送信する。一方で、サーバ１４は第２のネットワークアドレスとしてのＥｖｅｒＩＰ２４とともにＥｖｅｒＩＰ２４発行時に認証局にて認証された電子証明書２６Ａを同時に端末装置１０に送信する。端末装置１０とサーバ１４との間には通信ネットワーク２０を介してもよい。

【００５９】

認証局においては、電子証明書が正式なものであることを証明している。ＥｖｅｒＩＰ発行時に紐づけられる電子証明書は基本認証としての属性を有する。言い換えれば、ＥｖｅｒＩＰには必ず基本認証という属性が付与されている。端末装置１０とサーバ１４との通信が成立する条件として基本認証という属性を必須としている。基本認証がない場合、通信は確立されない。

【００６０】

また、本実施形態における端末装置１０はユーザ２１が有し、ユーザ２１が操作可能な携帯端末である。一方、サーバ１４は典型には企業２２により管理されており、ユーザ２１に対して各種インターネットサービスを提供するものである。インターネットサービスとしては、インターネット通販、出前サービス、オンラインバンキング、宿泊予約サイト、オンライン証券サービス、ＳＮＳサービスなどがある。

【００６１】

また、端末装置１０やサーバ１４は、複数の組織の認証局からＥｖｅｒＩＰ２３に関連付けられた複数の電子証明書を取得してもよい。ここで、図５を用いて端末装置１０の電子証明書の例を説明する。前述のとおり端末装置１０の電子証明書２５Ａには基本認証が備わっているが、端末装置１０のＥｖｅｒＩＰ２３には追加の電子証明書２５Ｂがさらに関連づけられてもよい。また、電子証明書２５Ａに対してさらなる属性Ａを付加することも可能である。すなわち、ＥｖｅｒＩＰ２３には少なくとも基本認証の属性を備える電子証明書２５Ａが関連づけられているが、複数の電子証明書を有してもよいし、各電子証明書内に複数の更なる認証属性を有していてもよい。また、２つ目以降の電子証明書にも基本認証を必ず備えることとしてもよい。つまり、属性Ｂが別の発行体によって認証された基本認証という属性であってもよい。

【００６２】

なお、本実施形態において、属性は電子証明書に付与されるものとしたが、ソフトウェア上で管理するものであってもよいし、アプリケーションとして管理するようにしてもよい。

【００６３】

複数の電子証明書を有する場合、又は複数の属性を有する場合、それら属性や電子証明書の有無に応じて通信の可否を判定できる。さらに、属性としてユーザ２１の情報を含むことができる。ユーザ２１の情報とは、氏名、生年月日、性別、住所、電話番号、各種口座情報などである。例えば、ユーザ２１が端末装置１０の通信契約をする際に提出した情報を属性として電子証明書内に含むこともできるため、実質的にユーザ２１が端末装置１０に対して自己の情報を入力することを省略しうる。ユーザ２１は自らの意思によって特

定のユーザ情報を変更してもよい。

【００６４】

（実施例１）

本実施形態における実施例１について図６を用いて説明する。ステップＳ１０において、ユーザ２１は企業２２の提供するサービスを利用するために、端末装置１０からサーバ１４にアクセスする。企業２２はサーバ１４を用いて各種インターネットサービスを提供している。まず、サーバ１４がＥｖｅｒＩＰ２４を有していない場合、通常のＩＰｖ４での通信と同じようにサービス提供画面が表示される。もしくは通信は確立しない態様としてもよい。

【００６５】

また、ステップＳ２０において、サーバ１４が基本認証を有しているか否か判定する。ステップＳ２０でＹＥＳの場合、ステップＳ３０に進み、サーバ１４は端末装置１０の電子証明書２５Ａの属性を読み取る。サーバ１４がＥｖｅｒＩＰ２４を有していても、電子証明書２５Ａが基本認証を含まない場合（ステップＳ２０でＮＯの場合）、ＥｖｅｒＩＰ２４が正式な発行手続きを経て生成されたものではないと判断し通信を確立しない。もしくは、通常のＩＰｖ４での通信接続としてサービス提供画面が表示されるようにしてもよい。ステップＳ３０では、電子証明書２５Ａに基本認証以外の属性情報（認証情報）が存在するかどうかを判定し、存在する場合にはどんな属性情報が存在しているかを一通り参照し、ステップＳ４０に進む。

【００６６】

ステップＳ４０において、サーバ１４が端末装置１０及びそのＥｖｅｒＩＰ２３に関連する電子証明書２５Ａにサービス利用アカウントの属性情報が含まれているかどうかを判定する。

【００６７】

ステップＳ４０にて、サービス利用アカウントの属性があると判断された場合、ステップＳ５０に進む。すなわち、サーバ１４はユーザ２１の端末装置１０に対してログインユーザとしてのサービス利用を許可する。このとき、ユーザ２１は「ログインする」という操作を行う必要がない。図７に示すように、ステップＳ５０における更なるユーザ体験としては、例えば、企業２２が提供するインターネット通販において端末装置１０の回線契約時に提出したユーザ情報が利用されることにより、入力画面なく「購入」ボタンを操作するだけで決済が完了する。代金の支払いは回線利用料金に追加して請求可能である。企業２２側のメリットとしては、端末装置１０とサーバ１４とが接続されているときだけ端末装置１０に関連したユーザ情報を参照できるため、ユーザ２１の情報をサーバ１４に保持する必要がない。つまり、企業２２における情報流出の危険性がなく、さらにはユーザ２１に各種情報を入力させる手間を省略できるためユーザフレンドリーなサービス環境を提供することができ集客効果を期待できる。

【００６８】

ステップＳ４０にて、サービス利用アカウントの属性がないと判断された場合、ステップＳ６０に進む。すなわち、サーバ１４はユーザ２１の端末装置１０に対してゲストとしてのサービス利用を許可する。この場合、図８に示すようにＩＰｖ４で接続したときと同様に「ログインする」という操作が必要となる。またはゲストユーザとして所定の情報を入力することによってサービスの利用を完了することができる。企業２２の視点でいえば、ユーザ２１「ログインする」ことを許可するためにはサーバ１４内にユーザ情報を保持しておかなければならない。

【００６９】

（実施例２）

本実施形態における実施例１について図９を用いて説明する。ステップＳ１１０において、ユーザ２１は企業２２の提供するサービスを利用するために、端末装置１０からサーバ１４にアクセスする。企業２２はサーバ１４を用いて各種インターネットサービスを提供している。まず、サーバ１４がＥｖｅｒＩＰ２４を有していない場合、通常のＩＰｖ４

での通信と同じようにサービス提供画面が表示される。もしくは通信は確立しない態様としてもよい。

【００７０】

また、ステップＳ１２０において、サーバ１４が基本認証を有しているか否か判定する。ステップＳ１２０でＹＥＳの場合、ステップＳ１３０に進み、サーバ１４は端末装置１０の電子証明書２５Ａの属性を読み取る。サーバ１４がＥｖｅｒＩＰ２４を有していても、電子証明書２５Ａが基本認証を含まない場合（ステップＳ１２０でＮＯの場合）、ＥｖｅｒＩＰ２４が正式な発行手続きを経て生成されたものではないと判断し通信を確立しない。もしくは、通常のＩＰｖ４での通信接続としてサービス提供画面が表示されるようにしてもよい。ステップＳ１３０では、電子証明書２５Ａに基本認証以外の属性情報（認証情報）が存在するかどうかを判定し、存在する場合にはどんな属性情報が存在しているかを一通り参照し、ステップＳ１４０に進む。

【００７１】

ステップＳ１４０において、サーバ１４が端末装置１０及びそのＥｖｅｒＩＰ２３に関連する電子証明書２５Ａにサービス利用アカウントの属性情報が含まれているかどうかを判定する。

【００７２】

ステップＳ１４０にて、サービス利用アカウントの属性があると判断された場合、ステップＳ１５０に進む。すなわち、企業２２は端末装置１０を利用しているユーザ２１がログインユーザであるとしてログインユーザ向けのサービスを提供することができる。

【００７３】

ステップＳ１４０にて、サービス利用アカウントの属性がないと判断された場合、ステップＳ１６０に進む。ステップＳ１６０では、サーバ１４はユーザ２１に対してサービス利用アカウントの属性を電子証明書２５Ａに付与することを提案する。すなわち、端末装置１０の電子証明書２５Ａにサービス利用アカウントとしての属性を持つかどうかを選択させる画面を表示するようにしてもよい。この場合、次回の接続からは、ステップＳ１３０～Ｓ１４０における判定時に電子証明書２５Ａにサービス利用アカウントであることを判定できるためステップＳ１５０へと進む。ステップＳ１６０にてユーザ２１が端末装置１０の電子証明書２５Ａにサービス利用アカウントとしての属性を付与しないと判断した場合、次回もユーザ２１に対して同様の提案を行うようにしてもよい。

【００７４】

（実施例３）

次に図１０を参照して複数のデバイス間での認証処理を説明する。データ発行体２８は例えばクレジットカードを発行するクレジットカード会社やマイナンバーカードを発行する行政機関などである。データ発行体２８はデータベース２７を有している。端末装置１０、サーバ１４、及びデータベース２７はそれぞれ固有のＥｖｅｒＩＰを有している。したがって、端末装置１０、サーバ１４、及びデータベース２７はそれぞれの通信がどこから来たものかを認識することができる。データベース２７は好適にはサーバ等に格納されている。

【００７５】

ここで、ユーザ２１が企業２２においてクレジットカード決済をする場合、従来ではクレジットカード情報を所定のフォームに入力する必要があった。企業２２はそのクレジットカード情報がデータ発行体２８が発行したものかどうかデータの真正を確認する必要があった。または、データ発行体２８が行政機関であった場合、ユーザは行政上の書類を取得するために役所に出向く必要があった。役所は、ユーザの個人情報と照らし合わせて行政機関のデータベース２７に保存された情報と比較し、真正が確認された場合に各種証明書（住民票など）を発行している。

【００７６】

本実施例では、ユーザ２１の端末装置１０が有するＥｖｅｒＩＰ２３におけるユーザ情報としてのクレジットカード情報をデータ発行体２８のデータベース２７のＥｖｅｒＩＰ

が認証している。さらに、データ発行体２８のデータベース２７のＥｖｅｒＩＰは端末装置１０のＥｖｅｒＩＰ２３を認証している属性情報を有する。企業２２のサーバ（又は役所のサーバ）はデータ発行体２８のデータベース２７のＥｖｅｒＩＰに対して問い合わせることで、データ発行体２８のデータベース２７のＥｖｅｒＩＰは端末装置１０のＥｖｅｒＩＰ２３を認証していることを知ることができる。

【００７７】

したがって、ユーザ２１が端末装置１０においてクレジットカード決済を行おうとするとき、データ発行体２８のデータベース２７のＥｖｅｒＩＰ、ＥｖｅｒＩＰ２３、及びＥｖｅｒＩＰ２４間で認証情報を確認し合うことができるため、クレジットカード情報を入力する必要がない。ユーザ２１が役所にて各種証明書を発行する場合も、行政機関のデータベース２７のＥｖｅｒＩＰ、ＥｖｅｒＩＰ２３、及びＥｖｅｒＩＰ２４間で認証し合うことができるため、役所における照合作業を行うことなくデータの真正を確認することが可能となる。

【００７８】

上記実施例においては、予め認証されデバイスに設定された固有のネットワークアドレスが存在することから、どのデバイスからの通信であるかを認識することができる。そして、属性情報や認証情報に基づいて当該ネットワークアドレスの真正を確認することができる。さらにデバイスは属性情報や認証情報の有無に基づいて提案やさらなる認証処理を行うことができる。そのため、ユーザ２１、企業２２、データ発行体２８との間でセキュアな通信が確保されるだけでなく、認証情報の真正も同時に担保することが可能となる。また、上記認証処理は例示した実施例に限定されず、あらゆる認証場面で利用することが可能である。

【符号の説明】

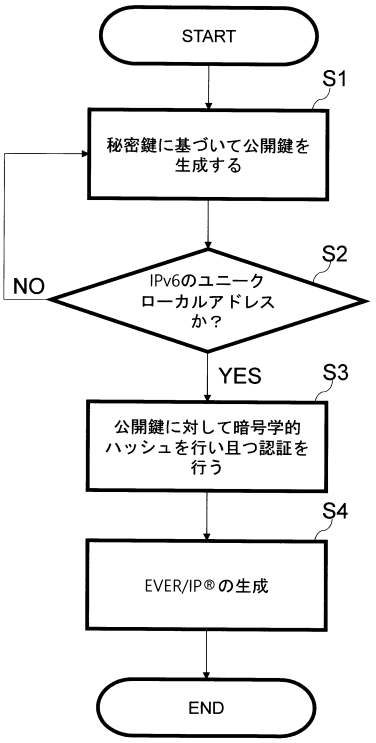
【００７９】

１０　端末装置、１４　サーバ、２３，２４　ＥｖｅｒＩＰ、２５Ａ，２６Ａ　電子証明書、２５Ｂ　追加の電子証明書、２７　データベース、２８　データ発行体。

【図面】

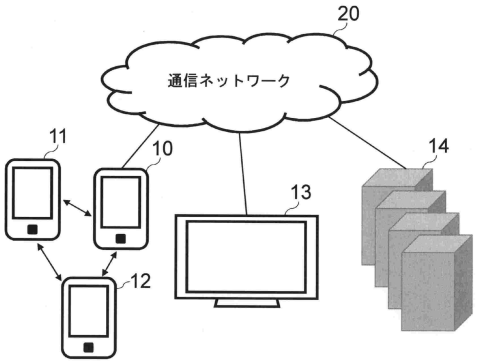
【図１】

FIG. 1



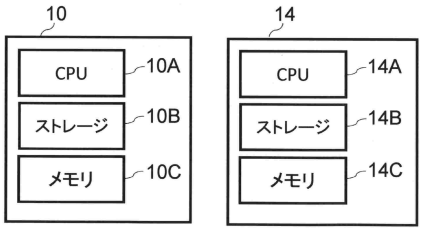
【図２】

FIG. 2



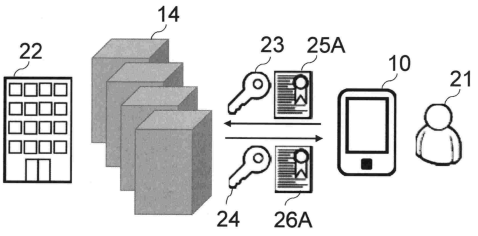
【図３】

FIG. 3



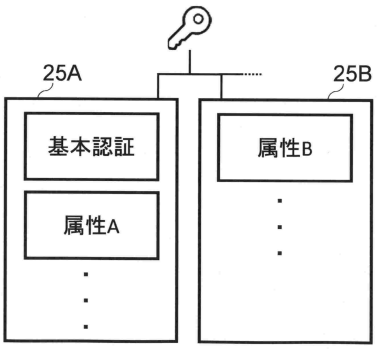
【図４】

FIG. 4



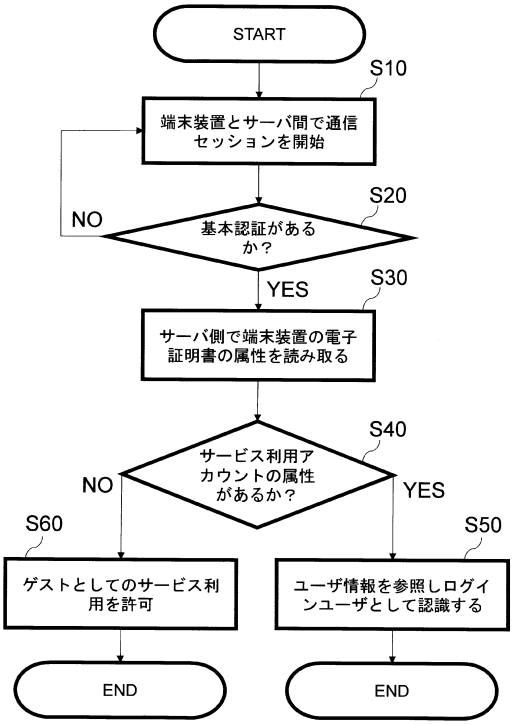
【図５】

FIG. 5



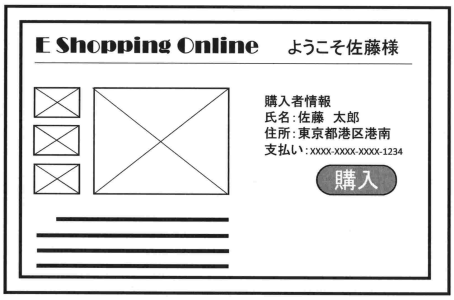
【図６】

FIG. 6



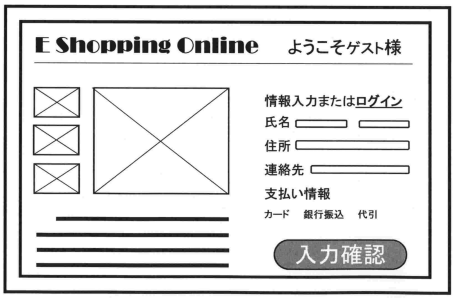
【図７】

FIG. 7



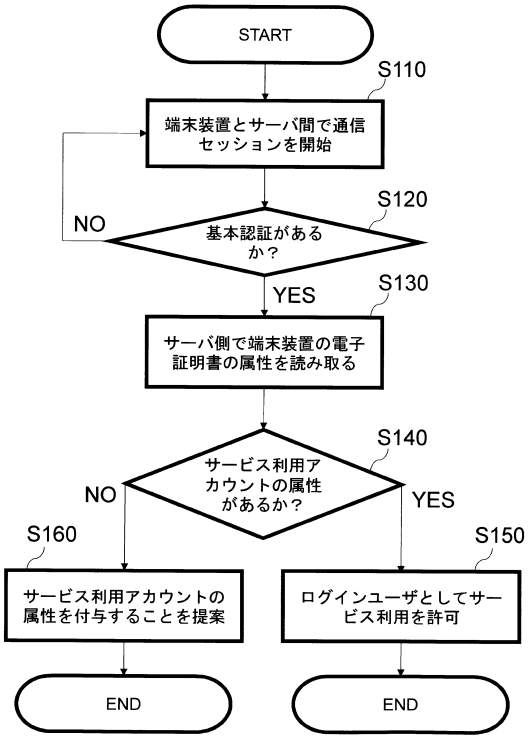
【図８】

FIG. 8



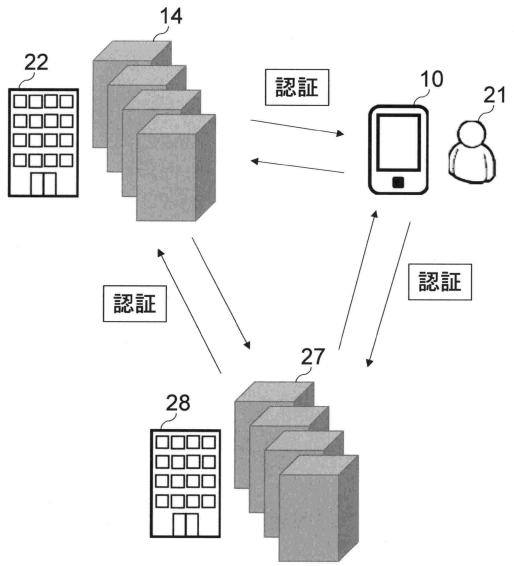
【図９】

FIG. 9



【図１０】

FIG. 10



フロントページの続き

鉾町８３番地 コネクトフリー株式会社内

合議体

審判長　山澤 宏

審判官　篠塚 隆

審判官　村松 貴士

(56)参考文献　米国特許出願公開第２００９／００８９３５７（ＵＳ，Ａ１）
特開２００２－２０７９２９（ＪＰ，Ａ）
国際公開第２００５／０１１１９２（WO，Ａ１）
特開２０１８－０６１２２７（ＪＰ，Ａ）
特開２０１８－１０４０８５（ＪＰ，Ａ）
特開２０１１－１６６３７５（ＪＰ，Ａ）
特表２０１４－５３５２１６（ＪＰ，Ａ）

(58)調査した分野　(Int.Cl.，ＤＢ名)

H04L12/00-13/18
H04L41/00-49/9057
H04L51/00-51/58
H04L61/00-65/80
H04L67/00-67/75
H04L69/00-69/40
G06F21/00
G06F21/30-21/46