(19)日本国特許庁(JP)

再 公 表 特 許(A1)

(11)国際公開番号
WO2013/145517

発行日　平成27年12月10日(2015.12.10)

(43)国際公開日　平成25年10月3日(2013.10.3)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/41	(2013.01)	G06F	21/20	141

審査請求 有　予備審査請求 未請求　（全 27 頁）

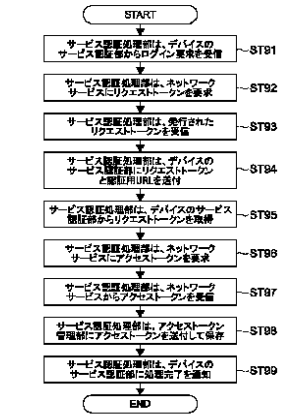
出願番号	特願2014-507353 (P2014-507353)
(21)国際出願番号	PCT/JP2013/000390
(22)国際出願日	平成25年1月25日 (2013.1.25)
(31)優先権主張番号	特願2012-73374 (P2012-73374)
(32)優先日	平成24年3月28日 (2012.3.28)
(33)優先権主張国	日本国(JP)

(71)出願人　000002185
ソニー株式会社
東京都港区港南１丁目７番１号
(74)代理人　100104215
弁理士　大森　純一
(74)代理人　100117330
弁理士　折居　章
(74)代理人　100168181
弁理士　中村　哲平
(74)代理人　100170346
弁理士　吉田　望
(74)代理人　100168745
弁理士　金子　彩子
(74)代理人　100176131
弁理士　金山　慎太郎

最終頁に続く

(54)【発明の名称】情報処理装置、情報処理システム、情報処理方法及びプログラム

(57)【要約】
【課題】複数のデバイスやネットワークサービスの連携に必要な認証処理の手間を削減すること。
【解決手段】情報処理装置は、通信部と、記憶部と、制御部とを有する。通信部は、第１の機器と、第２の機器と、第１の機器のユーザに関するリソースを有するネットワーク上のサービスと通信する。制御部は、第１の機器からの、上記リソースへのアクセス権の取得要求と、当該アクセス権の取得に対する上記ユーザの承認を示す承認情報とに基づいて、サービスへアクセス権を示すアクセストークンの発行要求を送信し、サービスから発行されたアクセストークンを受信するように通信部を制御する。また制御部は、受信されたアクセストークンを安全に記憶するように記憶部を制御し、ユーザと関連付けられた第２の機器からの要求に応じて、記憶されたアクセストークンを用いてリソースへアクセスするように通信部を制御する。
【選択図】図９



ST91 Service authentication processing unit receives login request from service authentication unit of device
ST92 Service authentication processing unit requests request token from network service
ST93 Service authentication processing unit receives issued request token
ST94 Service authentication processing unit transmits request token and authentication URL to service authentication unit of device
ST95 Service authentication processing unit acquires request token from service authentication unit of device
ST96 Service authentication processing unit requests access token from network service
ST97 Service authentication processing unit receives access token from network service
ST98 Service authentication processing unit transmits access token to access token management unit and saves access token
ST99 Service authentication processing unit notifies service authentication unit of device regarding process completion

【特許請求の範囲】
【請求項１】
第１の機器と、第２の機器と、前記第１の機器のユーザに関するリソースを有するネットワーク上のサービスと通信可能な通信部と、
記憶部と、
前記第１の機器からの、前記リソースへのアクセス権の取得要求と、当該アクセス権の取得に対する前記ユーザの承認を示す承認情報とに基づいて、前記サービスへ、前記アクセス権を示すアクセストークンの発行要求を送信し、前記サービスから、当該サービスによって発行されたアクセストークンを受信するように前記通信部を制御し、
前記受信されたアクセストークンを安全に記憶するように前記記憶部を制御することが可能な制御部と
を具備する情報処理装置。
【請求項２】
請求項１に記載の情報処理装置であって、
前記制御部は、前記ユーザと関連付けられた第２の機器からの要求に応じて、前記記憶されたアクセストークンを用いて前記リソースへアクセスするように前記通信部を制御する
情報処理装置。
【請求項３】
請求項１に記載の情報処理装置であって、
前記制御部は、安全な通信路を介して前記第１の機器または前記第２の機器へ前記記憶されたアクセストークンを送信するように前記通信部を制御する
情報処理装置。
【請求項４】
請求項１に記載の情報処理装置であって、
前記第１の機器は、前記ユーザが前記承認の意思を前記サービスへ通知するために必要な操作が入力される入力装置と、当該入力のための画面を出力する出力装置とを有し、
前記第２の機器は前記入力装置及び前記出力装置を有さない
情報処理装置。
【請求項５】
請求項２に記載の情報処理装置であって、
前記制御部は、前記第１の機器から、前記ユーザと、前記第１の機器と、前記第２の機器との関連付けを示す関連付け情報を受信するように前記通信部を制御し、前記受信された前記関連付け情報を記憶するように前記記憶部を制御する
情報処理装置。
【請求項６】
サーバ装置と情報処理装置とを具備する情報処理システムであって、
前記サーバ装置は、
ユーザ機器と、当該ユーザ機器のユーザに関するリソースを有するネットワーク上のサービスと通信可能な第１の通信部と、
記憶部と、
前記ユーザ機器からの、前記リソースへのアクセス権の取得要求と、当該アクセス権の取得に対する前記ユーザの承認を示す承認情報とに基づいて、前記サービスへ、前記アクセス権を示すアクセストークンの発行要求を送信し、前記サービスから、当該サービスによって発行されたアクセストークンを受信するように前記第１の通信部を制御し、
前記受信されたアクセストークンを安全に記憶するように前記記憶部を制御することが可能な第１の制御部と
を有し、
前記情報処理装置は、
前記サーバ装置及び前記サービスと通信可能な第２の通信部と、

前記サーバ装置から、前記記憶されたアクセストークンを安全な通信路を介して受信し、前記受信されたアクセストークンを用いて、前記リソースへアクセスするように前記第２の通信部を制御可能な第２の制御部と
を有する
情報処理システム。
【請求項７】
第１の機器から、ネットワーク上のサービスが有する当該第１の機器のユーザに関するリソースへのアクセス権の取得要求と、当該アクセス権の取得に対する前記ユーザの承認を示す承認情報とを受信し、
前記サービスへ、前記アクセス権を示すアクセストークンの発行要求を送信し、
前記サービスから、当該サービスによって発行されたアクセストークンを受信し、
前記受信されたアクセストークンを安全に記憶する
情報処理方法。
【請求項８】
情報処理装置に、
第１の機器から、ネットワーク上のサービスが有する当該第１の機器のユーザに関するリソースへのアクセス権の取得要求と、当該アクセス権の取得に対する前記ユーザの承認を示す承認情報とを受信するステップと、
前記サービスへ、前記アクセス権を示すアクセストークンの発行要求を送信するステップと、
前記サービスから、当該サービスによって発行されたアクセストークンを受信するステップと、
前記受信されたアクセストークンを安全に記憶するステップと
を実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本技術は、ネットワークを介して他の情報処理装置と通信可能な情報処理装置、当該情報処理装置を含む情報処理システム、当該情報処理装置における情報処理方法及びプログラムに関する。
【背景技術】
【０００２】
従来、ネットワークを介して複数のデバイスや各種のネットワークサービスが連携して動作する場合、そのためのユーザ認証に関しては、以下のような扱いがなされてきた。
（１）ユーザの概念が廃され、どのデバイス/サービスも自由に連携する（例えばＤＬＮＡ（Digital Living Network Alliance））。
（２）ユーザの手元にある、制御される側のデバイス／サービスを、制御する側のデバイスがユーザ認証し、制御される側のデバイス／サービスはユーザ認証しない（ＴＶ番組録画機器へのリモート予約）。
（３）ユーザ認証処理は他のデバイスを経由して実行されるが、デバイス／サービス連携機能が利用されるたびに、それぞれのデバイス／サービス毎にユーザＩＤ／パスワードが入力される（例えば、ＰＣ上でのネットワークファイル共有）。
（４）上記（３）で、一度入力された他のデバイス／サービス用のＩＤ／パスワードが、ユーザの手元のデバイスで記憶され、次回以降自動的にそれが用いられる。
【０００３】
しかしながら、上記（１）、（２）のような方法では、制御対象となるデバイス／サービス上にユーザのデータが存在する場合には、セキュリティ上の問題が生じてしまう。また（３）のような方法では、ユーザは、制御対象デバイス毎に毎回ＩＤ／パスワードを入力しなければならないため利便性が損なわれ、また扱うデバイスが多数存在する場合には現実的ではなくなってしまう。さらに、（４）のような方法では、ユーザのパスワードの

ような重要な情報が個々のデバイス上に保存されることになってしまい、セキュリティ上問題がある。仮に当該情報が暗号化されるとしても、それは必ず元の形に復号できる形で保存されるため、それが解読された場合には同様の問題が生じる。

【０００４】

また従来、ネットワークサービス間のマッシュアップなどを容易にするために、あるサービスが、他のサービスの機能を、そこで管理されているユーザのＩＤ／パスワードを直接与えられることなく利用できるようにするための様々なプロトコルが提案されてきた。そのための代表的なプロトコルとしてＯａｕｔｈ等があり、例えば、Facebook（登録商標）等のサービスで用いられてきた。Ｏａｕｔｈでは、ユーザのＩＤ／パスワードを管理するサービスプロバイダが、それが有する機能を利用する側のサービス（コンシューマ）に対して、ＩＤやパスワードを提供することなく、サービスプロバイダへのアクセス権を委譲する（例えば、特許文献１参照）。

【０００５】

またこのようなプロトコルは、ユーザＩＤ／パスワードの記録を必要としないことから、デバイスからネットワーク上のサービスを利用する際にも有用であり、ＰＣやスマートフォンなどのアプリケーションも多く利用している。

【先行技術文献】

【特許文献】

【０００６】

【特許文献１】特開２０１１－１５５５４５号公報

【発明の概要】

【発明が解決しようとする課題】

【０００７】

しかし、当該プロトコルでは、ユーザ認証の際に、そのＵＸ（User Experience）を担うディスプレイやキーボード等の入出力機能が必要となるため、これらを持たないデバイスからは利用できないという制約があった。

【０００８】

また、ユーザが複数のデバイスを持つ場合、同じサービスを利用するための認証手続きを、全てのデバイスごとに行わなければならず、上記（３）の手法と同様、非常に手間がかかり実用的ではなかった。さらに、通常、認証により得たアクセス権には有効期限があるため、有効期限が切れた場合には再度認証が必要になり、頻繁に認証手続きを繰り返す必要があった。

【０００９】

以上のような事情に鑑み、本技術の目的は、複数のデバイスやネットワークサービスの連携に必要な認証処理の手間を削減することが可能な情報処理装置、情報処理システム、情報処理方法及びプログラムを提供することにある。

【課題を解決するための手段】

【００１０】

上述の課題を解決するため、本技術の一形態に係る情報処理装置は、通信部と、記憶部と、制御部とを有する。上記通信部は、第１の機器と、第２の機器と、上記第１の機器のユーザに関するリソースを有するネットワーク上のサービスと通信可能である。上記制御部は、上記第１の機器からの、上記リソースへのアクセス権の取得要求と、当該アクセス権の取得に対する上記ユーザの承認を示す承認情報とに基づいて、上記サービスへ、上記アクセス権を示すアクセストークンの発行要求を送信し、上記サービスから、当該サービスによって発行されたアクセストークンを受信するように上記通信部を制御可能である。また制御部は、上記受信されたアクセストークンを安全に記憶するように上記記憶部を制御可能である。

【００１１】

この構成により情報処理装置は、ユーザのリソースへのアクセストークンを、複数の機器に共有させることができるため、複数の機器及びネットワークサービスの連携に必要な

認証処理の手間を削減することができる。

【００１２】

上記制御部は、上記ユーザと関連付けられた第２の機器からの要求に応じて、上記記憶されたアクセストークンを用いて上記リソースへアクセスするように上記通信部を制御してもよい。

【００１３】

これにより第２の機器は、みずからサービスとの間で認証処理を経ずとも、第１の機器及び情報処理装置の処理により取得されたアクセストークンを用いてネットワークサービスへアクセスすることができる。

【００１４】

上記制御部は、安全な通信路を介して上記第１の機器または上記第２の機器へ上記記憶されたアクセストークンを送信するように上記通信部を制御してもよい。

【００１５】

これにより、第１の機器または第２の機器は、受信したアクセストークンを用いて、情報処理装置を介さずにサービスへ直接アクセスすることができるようになるため、情報処理装置の負荷が軽減する。

【００１６】

上記第１の機器は、上記ユーザが上記承認の意思を上記サービスへ通知するために必要な操作が入力される入力装置と、当該入力のための画面を出力する出力装置とを有し、

上記第２の機器は上記入力装置及び上記出力装置を有さない

情報処理装置。

【００１７】

これにより、ユーザ認証及びアクセス権取得の承認のためのＵＸの表示や当該ＵＸに対する操作の受付が不可能な機器であっても、アクセストークンを利用してサービスにアクセスすることが可能となる。

【００１８】

上記制御部は、上記第１の機器から、上記ユーザと、上記第１の機器と、上記第２の機器との関連付けを示す関連付け情報を受信するように上記通信部を制御し、上記受信された上記関連付け情報を記憶するように上記記憶部を制御してもよい。

【００１９】

これにより第１の機器と第２の機器が、信頼できる同じユーザによって関連付けられていることが保証されるため、第２の機器からの要求に応じてアクセストークンを送信する際の安全性が担保される。

【００２０】

本技術の他の形態に係る情報処理システムは、サーバ装置と情報処理装置とを有する。

上記サーバ装置は、第１の通信部と、記憶部と、第１の制御部とを有する。第１の通信部は、ユーザ機器と、当該ユーザ機器のユーザに関するリソースを有するネットワーク上のサービスと通信可能である。上記制御部は、上記ユーザ機器からの、上記リソースへのアクセス権の取得要求と、当該アクセス権の取得に対する上記ユーザの承認を示す承認情報とに基づいて、上記サービスへ、上記アクセス権を示すアクセストークンの発行要求を送信し、上記サービスから、当該サービスによって発行されたアクセストークンを受信するように上記第１の通信部を制御可能である。また第１の制御部は、記受信されたアクセストークンを安全に記憶するように上記記憶部を制御可能である。

上記情報処理装置は、第２の通信部と、第２の制御部とを有する。上記第２の通信部は、上記サーバ装置及び上記サービスと通信可能である。上記第２の制御部は、上記サーバ装置から、上記記憶されたアクセストークンを安全な通信路を介して受信し、上記受信されたアクセストークンを用いて、上記リソースへアクセスするように上記第２の通信部を制御可能である。

【００２１】

本技術のまた別の形態に係る情報処理方法は、第１の機器から、ネットワーク上のサー

ビスが有する当該第１の機器のユーザに関するリソースへのアクセス権の取得要求と、当該アクセス権の取得に対する上記ユーザの承認を示す承認情報とを受信することを含む。上記サービスへは、上記アクセス権を示すアクセストークンの発行要求が送信される。上記サービスからは、当該サービスによって発行されたアクセストークンが受信される。上記受信されたアクセストークンは安全に記憶される。

【００２２】

本技術のまた別の形態に係るプログラムは、情報処理装置に、第１の受信ステップと、第１の送信ステップと、第２の受信ステップと、記憶ステップとを実行させる。上記第１の受信ステップでは、第１の機器から、ネットワーク上のサービスが有する当該第１の機器のユーザに関するリソースへのアクセス権の取得要求と、当該アクセス権の取得に対する上記ユーザの承認を示す承認情報とが受信される。上記第１の送信ステップでは、上記サービスへ、上記アクセス権を示すアクセストークンの発行要求が送信される。上記第２の受信ステップでは、上記サービスから、当該サービスによって発行されたアクセストークンが受信される。上記記憶ステップでは、上記受信されたアクセストークンが安全に記憶される。

【発明の効果】

【００２３】

以上のように、本技術によれば、複数のデバイスやネットワークサービスの連携に必要な認証処理の手間を削減することができる。

【図面の簡単な説明】

【００２４】

【図１】本技術の第１の実施形態におけるシステムのネットワーク構成を示した図である。

【図２】第１の実施形態におけるサーバのハードウェア構成を示したブロック図である。

【図３】第１の実施形態におけるデバイスのハードウェア構成を示したブロック図である。

【図４】第１の実施形態におけるサーバのソフトウェアモジュール構成を示したブロック図である。

【図５】第１の実施形態におけるデバイスのソフトウェアモジュール構成を示したブロック図である。

【図６】第１の実施形態におけるネットワークサービス認証の概要を示した図である。

【図７】第１の実施形態におけるネットワークサービス認証の流れを示したシーケンス図である。

【図８】第１の実施形態におけるデバイスによるネットワークサービス認証処理の流れを示したフローチャートである。

【図９】第１の実施形態におけるサーバによるネットワークサービス認証処理の流れを示したフローチャートである。

【図１０】第１の実施形態におけるデバイスによるネットワークサービスへのアクセス処理の流れを示したフローチャートである。

【図１１】第１の実施形態におけるサーバによるネットワークサービスへのアクセス処理の流れを示したフローチャートである。

【図１２】第２の実施形態におけるサーバのソフトウェアモジュール構成を示したブロック図である。

【図１３】第２の実施形態におけるデバイスのソフトウェアモジュール構成を示したブロック図である。

【図１４】第２の実施形態におけるデバイスによるネットワークサービスへのアクセス処理の流れを示したフローチャートである。

【図１５】第２の実施形態におけるサーバによるネットワークサービスへのアクセス処理の流れを示したフローチャートである。

【発明を実施するための形態】

【００２５】
以下、本技術に係る実施形態を、図面を参照しながら説明する。
【００２６】
＜第１の実施形態＞
まず、本技術の第１の実施形態を説明する。
【００２７】
［システムのネットワーク構成］
図１は、本実施形態に係るシステムのネットワーク構成を示した図である。
【００２８】
同図に示すように、このシステムは、クラウド上のサーバ１００と、ネットワークサービス２００と、デバイス３００とを有する。これらはそれぞれＷＡＮ５０により通信可能とされている。ネットワークサービス２００及びデバイス３００は複数存在し得る。
【００２９】
サーバ１００は、複数のデバイス３００間の通信を仲介するとともに、デバイス３００のユーザが有するネットワークサービス２００へのアクセス権（アクセストークン）の委譲を受け、当該アクセストークンを管理する機能を有する。
【００３０】
サーバ１００にはユーザ認証サーバ１５０が接続されている。ユーザ認証サーバ１５０は、後述する各デバイス３００とユーザとの関連付け処理において、サーバ１００からの要求により、ユーザＩＤ及びパスワードによるユーザ認証処理を行う。
【００３１】
ネットワークサービス２００は、他の機器(サーバ１００、デバイス３００等)にネットワークサービスを提供する。またネットワークサービス２００は、サービス提供のためのサービス認証機構を提供し、要求されたアクセス内容をデバイス３００経由でユーザに提示し、ユーザから承認を得ることで、サービス認証処理を行う。同図では、ネットワークサービス２００Ａ～２００Ｃの３つのみが示されているが、ネットワークサービス２００の数は４つ以上であっても構わない。
【００３２】
デバイス３００は、例えばスマートフォン、携帯電話機、タブレットＰＣ（Personal Computer）、デスクトップＰＣ、ノートブックＰＣ、ＰＤＡ（Personal Digital Assistant）、携帯型ＡＶプレイヤー、電子ブック、デジタルスチルカメラ、カムコーダ、テレビジョン装置、ＰＶＲ（Personal Video Recorder）、ゲーム機器、プロジェクター、カーナビゲーションシステム、デジタルフォトフレーム、ＨＤＤ（Hard Disk Drive）装置、ヘルスケア機器、家庭用電気製品等、あらゆる情報処理装置であり得る。同図では、デバイス３００Ａ～３００Ｃの３台のみが示されているが、デバイス３００の数は４台以上であっても構わない。
【００３３】
［サーバのハードウェア構成］
図２は、上記サーバ１００のハードウェア構成を示した図である。同図に示すように、サーバ１００は、ＣＰＵ（Central Processing Unit）１１、ＲＯＭ（Read Only Memory）１２、ＲＡＭ（Random Access Memory）１３、入出力インタフェース１５、及び、これらを互いに接続するバス１４を備える。
【００３４】
ＣＰＵ１１は、必要に応じてＲＡＭ１３等に適宜アクセスし、上記アクセストークンの取得処理等において、各種演算処理を行いながらサーバ１００の各ブロック全体を統括的に制御する。ＲＯＭ１２は、ＣＰＵ１１に実行させるＯＳ、プログラムや各種パラメータなどのファームウェアが固定的に記憶されている不揮発性のメモリである。ＲＡＭ１３は、ＣＰＵ１１の作業用領域等として用いられ、ＯＳ、実行中の各種アプリケーション、処理中の各種データを一時的に保持する。
【００３５】

入出力インタフェース１５には、表示部１６、操作受付部１７、記憶部１８、通信部１９等が接続される。

【００３６】

表示部１６は、例えばＬＣＤ（Liquid Crystal Display）、ＯＥＬＤ（Organic ElectroLuminescence Display）、ＣＲＴ（Cathode Ray Tube）等を用いた出力装置である。

【００３７】

操作受付部１７は、例えばマウス等のポインティングデバイス、キーボード、タッチパネル、その他の入力装置である。操作受付部１７がタッチパネルである場合、そのタッチパネルは表示部１６と一体となり得る。

【００３８】

記憶部１８は、例えばＨＤＤや、ＳＳＤ（Solid State Drive）等のフラッシュメモリを用いた不揮発性メモリ等である。当該記憶部１８には、上記ＯＳや各種アプリケーション、各種データが記憶される。特に本実施形態において、記憶部１８には、後述する複数のソフトウェアモジュール等のプログラムや、ネットワークサービス２００から取得したアクセストークンが記憶される。これらのプログラムは、サーバ１００に、ＷＡＮ５０を介して提供されてもよいし、サーバ１００で読み取り可能な記録媒体として提供されてもよい。

【００３９】

通信部１９は、ＷＡＮ５０に接続するためのＮＩＣ等であり、デバイス３００との間の通信処理を担う。

【００４０】

［デバイスのハードウェア構成］

図３は、上記デバイス３００のハードウェア構成を示した図である。同図に示すように、デバイス３００のハードウェア構成も、上記サーバ１００のハードウェア構成と基本的に同様である。すなわち、デバイス３００は、ＣＰＵ３１、ＲＯＭ３２、ＲＡＭ３３、入出力インタフェース３５、及び、これらを互いに接続するバス３４、表示部３６、操作受付部３７、記憶部３８、通信部３９を備える。ここで表示部３６は、デバイス３００に内蔵されていてもよいし、デバイス３００に外部接続されていてもよい。

【００４１】

ＣＰＵ３１は、記憶部３８や通信部３９等の各ブロックを制御して、サーバ１００やネットワークサービス２００との通信処理や、各種データ処理を実行する。

【００４２】

記憶部３８には、後述する複数のソフトウェアモジュール等のプログラムや、各種データベースが記憶される。これらのプログラムは、デバイス３００に、ＷＡＮ５０を介して提供されてもよいし、デバイス３００で読み取り可能な記録媒体として提供されてもよい。

【００４３】

デバイス３００がスマートフォン等のモバイル機器の場合、通信部３９は、無線ＬＡＮ等の無線通信用のモジュールであり得る。

【００４４】

デバイス３００が、例えばデジタルフォトフレームやヘルスケア機器（例えば体温計、体重計、血圧計、脈拍計等）である場合、操作受付部３７は、ボタンやスイッチのみで構成され、キーボードやタッチパネルのような文字入力機能を有さない場合もある。また同様に表示部３６は、写真のスライドショーや計測値の表示は可能であっても、ブラウザ等のアプリケーションのＵＩを出力する機能を有さない場合もある。

【００４５】

［サーバのモジュール構成］

図４は、上記サーバ１００が有するソフトウェアモジュールの構成を示した図である。同図に示すように、サーバ１００は、データベースマネージャ１１０、セキュリティマネージャ１２０及びコミュニケーションマネージャ１３０の各モジュールマネージャを有す

る。

【００４６】

データベースマネージャ１１０は、サーバ１００が有するデータベースをまとめて管理する。データベースマネージャ１１０は、ユーザ／デバイス管理部１１１及びアクセストークン管理部１１２の各ソフトウェアモジュールを有する。

【００４７】

ユーザ／デバイス管理部１１１は、デバイス３００のユーザを一意に識別するユーザＩＤ毎に、デバイス３００のリストを管理する。

【００４８】

アクセストークン管理部１１２は、上記ユーザＩＤ毎及び、ネットワークサービス２００を一意に識別するサービスＩＤ毎に、各種ネットワークサービス２００から取得した、当該ネットワークサービス２００のリソースへアクセスするためのアクセストークンを管理する。

【００４９】

セキュリティマネージャ１２０は、サーバ１００と、デバイス３００及びネットワークサービス２００間の通信におけるセキュリティに関連する処理をまとめて取り扱う。セキュリティマネージャ１２０は、ユーザ認証処理部１２１、簡単設定処理部１２２、サービス認証処理部１２３、サービスアクセス処理部１２４、デバイス認証部１２５及び暗号処理部１２６の各ソフトウェアモジュールを有する。

【００５０】

ユーザ認証処理部１２１は、デバイスベースのセキュリティ機構上で、デバイス３００のユーザ認証処理（詳細は後述）を行う。

【００５１】

ここで、デバイスベースのセキュリティ機構とは、デバイス３００間及びデバイス３００とサーバ１００間で機器レベルの相互認証が行われ、ユーザの介在なく、安全な通信を行うための通信路が構築される機構をいう。この機構により、デバイス３００間及びデバイス３００とサーバ１００間のセキュリティ関連処理部が安全な通信路で結ばれ、１つのセキュリティシステムとして機能することとなる。

【００５２】

具体的には、デバイスベースセキュリティ機構は、予めデバイス３００とサーバ１００に鍵／証明書を埋め込んでおき、これらに基づいてデバイス３００及びサーバ１００が正規のものであることを確認する認証処理と、以後の通信で利用する鍵を生成するための鍵交換処理とを行う。

【００５３】

上記認証処理及び鍵交換処理は、実際の接続形態に関わらず、End To Endで行われる。例えば、デバイス３００Ａとデバイス３００Ｂがサーバ１００を介して接続されている場合、実際にはデバイス３００Ａと３００Ｂとは直接接続されていないが、認証処理及び鍵交換処理は、デバイスＡ及びＢで行われ、サーバ１００は単にそれらの処理を通信部１９で中継する。

【００５４】

簡単設定処理部１２２は、上記デバイスベースセキュリティ機構上で、ユーザ認証済のデバイス３００を利用して、他のデバイス３００にユーザ情報を設定し、それを認証済（関連付け設定済）デバイスとする。

【００５５】

上記デバイスベースセキュリティ機構により、例えばデバイス３００Ａとデバイス３００Ｂで認証を行うと、機器および通信経路の安全性が確保される。したがってサーバ１００は、デバイス３００Ａのユーザ情報を信頼してデバイスＢにユーザ情報を設定することができ、これによりユーザ認証を行ったものとみなすことができる。

【００５６】

このユーザ情報の設定処理のためのユーザインタフェースには、どのような形態のもの

が用いられてもよい。本実施形態では、例えば、設定元のデバイス３００Ａの表示部３６には、デバイス検索処理によって検索された他のデバイス３００の画像またはアイコンの一覧が表示される。デバイス３００Ａのユーザが、当該画像またはアイコンをクリック、タッチ、囲う等の操作により選択すると、デバイス３００Ａから当該選択された他のデバイスへ設定要求メッセージがサーバ１００を介して送信される。当該他のデバイスにおいて、当該設定要求に同意する意思を示す操作（例えばＯＫボタンの押下）が入力されると、その旨の応答情報がサーバ１００を介して設定元のデバイス３００Ａへ送信される。そして、デバイス３００Ａの表示部３６では、上記応答情報が受信されると、上記一覧において、設定済となったデバイスの画像またはアイコンの表示態様が変化する。例えば当該画像またはアイコンが枠で囲まれたり、それらの色が変更されたりする。これによりユーザは設定が完了したことを知ることができる。

【００５７】

簡単設定によるユーザ情報の設定には、ユーザ認証（ＩＤ及びキーワードの入力）のためのユーザインタフェースが必要とないことから、たとえば、表示デバイスやキーボードを持たない小型デバイスであっても設定対象となり得る。これにより、ユーザは、いずれか１台のデバイスだけでユーザＩＤ及びパスワードによるユーザ認証を行い、他のデバイスを上記簡単設定で設定することにより、面倒な操作をすることなく、様々なデバイスを自身に関連付けることができる。

【００５８】

サービス認証処理部１２３は、デバイス３００からの要求により、ネットワークサービス２００と通信してサービス認証処理を行い、アクセストークンを取得する。サービス認証処理の詳細については後述する。

【００５９】

サービスアクセス処理部１２４は、デバイス３００からの要求により取得済みのアクセストークンを利用してネットワークサービス２００にアクセスする。

【００６０】

デバイス認証部１２５は、上述したデバイスベースセキュリティ機構としてデバイス３００の認証処理を行う。

【００６１】

暗号処理部１２６は、デバイスベースセキュリティ機構として暗号処理を行う。すなわち、セキュリティマネージャ１２０と、その他のモジュールとのやり取りは、デバイスベースセキュリティ機構に基づいて暗号化される。また、セキュリティマネージャ１２０は、各デバイス３００及びサーバ１００上で、例えばソフトウェア耐タンパ処理等によって強固に保護される。

【００６２】

これにより、強固に保護された複数のデバイス３００及びサーバ１００上のセキュリティマネージャ１２０が、デバイスベースセキュリティ機構に基づいて、暗号化された通信によって接続されていることになる。したがってこれら全体が、１つのシステムと見なされることになる。

【００６３】

コミュニケーションマネージャ１３０は、ソフトウェアモジュールとしての通信部１３１を有する。通信部１３１は、セキュリティマネージャ１２０とデバイス３００との通信処理を行う。

【００６４】

［デバイスのモジュール構成］

図５は、上記デバイス３００が有するソフトウェアモジュールの構成を示した図である。同図に示すように、デバイス３００は、コミュニケーションマネージャ３１０、セキュリティマネージャ３２０、ユーザ／デバイスＵＩマネージャ３３０及びサービスＵＩマネージャ３４０の各モジュールマネージャを有する。

【００６５】

コミュニケーションマネージャ３１０は、ソフトウェアモジュールとしての通信部３１１を有する。通信部３１１は、セキュリティマネージャ３２０とサーバ１００との通信処理を行う。

【００６６】

セキュリティマネージャ３２０は、デバイス認証部３２１、暗号処理部３２２、ユーザ認証部３２３、簡単設定部３２４、ユーザ情報管理部３２５及びサービス認証部３２６の各ソフトウェアモジュールを有する。

【００６７】

デバイス認証部３２１は、上記デバイスベースセキュリティ機構としてデバイス認証を行う。

【００６８】

暗号処理部３２２は、上記デバイスベースセキュリティ機構として暗号処理を行う。

【００６９】

ユーザ認証部３２３は、上記デバイスベースセキュリティ機構上で、サーバ１００（のユーザ認証処理部１２１）との間でユーザ認証処理を行う。

【００７０】

簡単設定部３２４は、上記デバイスベースセキュリティ機構上で、サーバ１００（の簡単設定処理部１２２）との間で上述した簡単設定処理を行う。

【００７１】

ユーザ情報管理部３２５は、上記簡単設定処理によってデバイス３００と関連付けられたユーザＩＤを管理する。

【００７２】

サービス認証部３２６は、デバイスベースセキュリティ機構上で、サーバ１００との間でネットワークサービス認証に関する処理を行う。

【００７３】

サービスアクセス要求部３２７は、デバイスベースセキュリティ機構上で、サーバ１００との間でネットワークサービスへのアクセスに関する処理を行う。

【００７４】

ユーザ／デバイスＵＩマネージャ３３０は、ソフトウェアモジュールとして、簡単設定ＵＩ部３３１と、ユーザ認証ＵＩ部３４１とを有する。

【００７５】

簡単設定ＵＩ部３３１は、上記簡単設定処理のために表示部３６に表示されるＵＩを生成及び制御する。

【００７６】

ユーザ認証ＵＩ部３３２は、上記ユーザ認証のために表示部３６に表示されるＵＩを生成及び制御する。

【００７７】

サービスＵＩマネージャ３４０は、ソフトウェアモジュールとしてサービスＵＩ部３４１を有する。サービスＵＩ部３４は、ネットワークサービス２００の認証およびアクセスのために表示部３６に表示されるＵＩを生成及び制御する。

【００７８】

ここで、上記ユーザ認証処理について説明する。上記サーバ１００とデバイス３００間でのユーザ認証処理は次のように行われる。

【００７９】

まず、ユーザ認証ＵＩ部３３２が、ユーザからユーザＩＤ及びパスワードを受け付け、ユーザ認証部３２３に送付する。

【００８０】

ユーザ認証部３２３は、当該ユーザＩＤ及びパスワードを、デバイスベースセキュリティ機構を経由してサーバ１００のユーザ認証処理部１２１に送付する。

【００８１】

ユーザ認証処理部１２１は、ユーザ認証サーバ１５０に認証を依頼する。当該認証が成功した場合、ユーザ認証処理部１２１は、ユーザＩＤ及びデバイスＩＤをユーザ／デバイス管理部１１１に送付するとともに、デバイス３００に認証結果を送付する。

【００８２】

ユーザ／デバイス管理部１１１は、ユーザデータベース上のデバイスリストに、ユーザ認証処理部１２１から受け取ったデバイスＩＤを追加する。

【００８３】

上記認証結果を受け取ったデバイス３００のユーザ認証部３２３は、ユーザ情報管理部３２５にユーザＩＤを送付し、記録させる。

【００８４】

［システムの動作］

次に、以上のように構成されたシステムにおけるサーバ１００及びデバイス３００の動作について説明する。本実施形態及び他の実施形態において、サーバ１００及びデバイス３００における動作は、ＣＰＵと、その制御下において実行される上記各ソフトウェアモジュールとで協働して行われる。

【００８５】

（ネットワークサービス認証処理）

まず、上記ネットワークサービス認証処理について説明する。図６は、本実施形態におけるネットワークサービス認証の概要を示した図である。

【００８６】

本実施形態におけるネットワークサービスの認証処理としては、様々な方式を用いることができるが、例えば、ＯＡｕｔｈに相当する方式が用いられる。

【００８７】

ＯＡｕｔｈでは、ネットワークサービスへのアクセス権が、アクセストークンで表される。サービス認証処理では、ユーザがネットワークサービス上の自分のリソース（アカウント）へのアクセスを承認することで、ネットワークサービスからアクセストークンの発行を受ける。

【００８８】

ＯＡｕｔｈでは、サービスの認証を受ける機器をConsumer、ネットワークサービス側で認証処理を行い、アクセストークンを発行する側をService Providerと呼ぶ。本実施形態では、サーバ１００がConsumer、ネットワークサービス２００がService Providerに該当する。

【００８９】

図６に示すように、まず、デバイス３００からConsumerであるサーバ１００に対して、Service Providerであるネットワークサービス２００上のリソースを利用するように（アクセス権を取得するように）要求する（同図（１））。

【００９０】

サーバ１００は、当該要求を受けて、ネットワークサービス２００へ認証を要求する（同図（２））。

【００９１】

上記サーバ１００からの認証要求を受けて、ネットワークサービス２００は、デバイス３００のユーザに対して、上記認証（アクセス権の取得）を承認するか否かを確認する（同図（３））。

【００９２】

ユーザがデバイス３００を介してネットワークサービス２００に対して承認を通知すると（同図（４））、ネットワークサービス２００は、サーバ１００に対してアクセストークンを発行する（同図（５））。

【００９３】

そしてサーバ１００は、当該発行されたアクセストークンを用いて、ネットワークサービス２００上のリソース（ＡＰＩ）を呼び出す（同図８（６））。

【００９４】
上記ユーザによる承認は、ネットワークサービス２００側で用意する認証用のＷｅｂページを用いるため、デバイス３００側ではＵＩモジュールとしてブラウザが利用される。実際にサービス認証を行う際には、ユーザデバイス上にブラウザが搭載されていることが前提であることから、必ずしも全てのデバイスで認証が行えるわけではない。
【００９５】
上記サービス認証処理をさらに詳細に説明する。図７は、当該ネットワークサービス認証の流れを示したシーケンス図である。また図８は、デバイス３００におけるネットワークサービス認証処理の流れを示したフローチャートである。また図９は、サーバ１００におけるネットワークサービス認証処理の流れを示したフローチャートである。
【００９６】
これらの処理にあたっては、サーバ１００とデバイス３００間では、上述したデバイスベースのセキュリティ機構により、安全な通信路が確立されているものとする。
【００９７】
まず、デバイス３００のサービス認証部３２６は、上記デバイスベースセキュリティ機構を用いて、サーバ１００のサービス認証処理部１２３に対して、ネットワークサービス２００へのログイン要求を送信する（図７のステップ７１、図８のステップ８１）。
【００９８】
サーバ１００のサービス認証処理部１２３は、当該ログイン要求を受信すると（図９のステップ９１）、ネットワークサービス２００へ、リクエストトークンを要求する（図７のステップ７２、図９のステップ９２）。
【００９９】
上記リクエストトークンの要求を受けたネットワークサービス２００は、サーバ１００のサービス認証処理部１２３へリクエストトークン（未承認）を発行する（図７のステップ７３）。
【０１００】
サーバ１００のサービス認証処理部１２３は、上記発行されたリクエストトークンを受信すると（図９のステップ９３）、デバイス３００のサービス認証部３２６へ、当該リクエストトークンと、サービス認証用ページへのＵＲＬを送信する（デバイス３００を当該ＵＲＬへリダイレクトさせる）（図７のステップ７４、図９のステップ９４）。
【０１０１】
デバイス３００のサービス認証部３２６は、上記リクエストトークン及び認証用ＵＲＬを受信し、それらをサービスＵＩ部３４１へ送信する（図８のステップ８２）。
【０１０２】
サービスＵＩ部３４１は、当該認証用ＵＲＬによりネットワークサービス２００へアクセスし（図７のステップ７４）、ブラウザにより、サービス認証の承認のための確認画面を表示部３６に表示する（図７のステップ７５、図８のステップ８３）。
【０１０３】
当該認証用ＵＲＬへのアクセスの際、ユーザは、ネットワークサービス２００から、ユーザＩＤ及びパスワードの入力を要求される。ユーザがブラウザを介してユーザＩＤ及びパスワードを入力し、ユーザ認証に成功すると、上記確認画面が表示される。
【０１０４】
すなわち、ネットワークサービス認証処理では、ユーザＩＤ及びパスワードのやり取りは、デバイス３００とネットワークサービス２００との間で直接行われる。したがって、サーバ１００がユーザのＩＤ／パスワードを取得してそれを不正に保存及び利用することが防止される。
【０１０５】
サービスＵＩ部３４１は、当該確認画面上でユーザから承認可否を選択する操作を受け付けると、その結果をネットワークサービス２００へ送信する（図７のステップ７６、図８のステップ８４）。

【０１０６】
上記確認画面上でユーザが承認した場合（図８のステップ８５のＹｅｓ）、サービスＵＩ部３４１は、ネットワークサービス２００から、承認済を示すリクエストトークンを受信し、サービス認証部３２６へ送信する（図８のステップ８６）。
【０１０７】
サービス認証部３２６は、当該受信したリクエストトークンを、サーバ１００のサービス認証処理部１２３へ送信する（図８のステップ８７）。
【０１０８】
サーバ１００のサービス認証処理部１２３は、デバイス３００のサービス認証部３２６から上記リクエストトークンを受信すると（図９のステップ９５）、それに基づいて、ネットワークサービス２００へアクセストークンを要求する（図７のステップ７７、図９のステップ９６）。
【０１０９】
ネットワークサービス２００は、上記アクセストークンの要求に対して、サーバ１００のサービス認証処理部１２３へアクセストークンを発行し（図７のステップ７８）、サービス認証処理部１２３は当該発行されたアクセストークンを受信する（図９のステップ９７）。
【０１１０】
アクセストークンを受信したサービス認証処理部１２３は、当該アクセストークンをアクセストークン管理部１１２へ送付して、ユーザＩＤ及びサービスＩＤと関連付けて記憶部１８に保存させる（図９のステップ９８）。
【０１１１】
そして、サービス認証処理部１２３は、デバイス３００のサービス認証部３２６へ、サービス認証処理（アクセストークン取得処理）の完了を通知する（図９のステップ９９）。
【０１１２】
デバイス３００のサービス認証部３２６は、上記処理完了通知を受信する（図８のステップ８８）。
【０１１３】
（ネットワークサービスへのアクセス処理）
次に、上記ネットワークサービス認証により取得されたアクセストークンを利用した、ネットワークサービス２００へのアクセス処理について説明する。
【０１１４】
図１０は、デバイス３００によるネットワークサービスへのアクセス処理の流れを示したフローチャートである。また図１１は、サーバ１００によるネットワークサービスへのアクセス処理の流れを示したフローチャートである。
【０１１５】
この場合のデバイス３００は、上記ネットワークサービス認証処理に携わったデバイスでもよいし、認証処理に携わっておらず、認証処理に携わったデバイスと上記デバイスベースセキュリティ機構で接続された他のデバイスであってもよい。またデバイス３００は、上記サービス認証処理に必要なブラウザ用の表示部３６や操作受付部３７を有していてもよいし（例えばＰＣ、スマートフォン等）、有していなくてもよい（例えばデジタルフォトフレームやヘルスケア機器）。
【０１１６】
まずデバイス３００のサービスＵＩ部３４１は、ネットワークサービスへのアクセス要求をユーザから受け付け、それをサービスアクセス要求部３２７へ送信する（図１０のステップ１０１）。
【０１１７】
上記アクセス要求を受けたサービスアクセス要求部３２７は、サーバ１００のサービスアクセス処理部１２４へ、ネットワークサービス２００へのアクセス要求をユーザＩＤと

ともに送信する（図１０のステップ１０２）。
【０１１８】
サーバ１００のサービスアクセス処理部１２４は、上記アクセス要求を受信すると（図１１のステップ１１１）、アクセストークン管理部１１２から、記憶部１８に記憶された、上記ユーザＩＤに対応するアクセストークンを取得する（図１１のステップ１１２）。
【０１１９】
続いてサービスアクセス処理部１２４は、当該取得したアクセストークンを用いて、ネットワークサービス２００へアクセスする（図１１のステップ１１３）。
【０１２０】
そしてサービスアクセス処理部１２４は、ネットワークサービス２００へのアクセス結果（例えばＡＰＩ）をデバイス３００のサービスアクセス要求部３２７へ送信する（図１１のステップ１１４）。
【０１２１】
デバイス３００のサービスアクセス要求部３２７は、上記アクセス結果を受信し、サービスＵＩ部３４１へ送信する（図１０のステップ１０３）。
【０１２２】
そしてサービスＵＩ部３４１は、上記アクセス結果を、表示部３６を介してユーザに提示する（図１０のステップ１０４）。
【０１２３】
［まとめ］
以上説明したように、本実施形態では、サーバ１００は、デバイス３００からの要求によりネットワークサービス２００から取得したアクセストークンをサーバ１００上に安全に記憶する。
【０１２４】
そして、サーバ１００とデバイス３００間及び複数のデバイス３００間のセキュリティは、上記デバイスベースセキュリティ機構により、ユーザＩＤ／パスワードの組の入力によらずに守られており、ユーザとデバイス３００との関連付けは、デバイス３００でのユーザ認証処理によらずに行われる。
【０１２５】
したがって、上記ネットワークサービス認証処理により、ネットワークサービス２００のユーザ認証をいずれか１つのデバイス３００上で行えば、サーバ１００により取得されて記憶されたアクセストークンを、デバイスベースセキュリティ機構上で関連付けられた他のデバイス３００が利用することができる。
【０１２６】
これは、ユーザがネットワークサービス２００のＩＤ／パスワードを、利用するデバイス３００毎に何度も入力することなく、自由にサービスを利用できるようになることを意味する。
【０１２７】
また、ネットワークサービス２００のユーザ認証においては、アクセストークンの取得を承認するに際してＩＤ／パスワードの入力や承認意思を通知するための入力（例えばＯＫボタンの押下）を行うためのＵＩ機能がデバイス３００上に必要である。しかし本実施形態では、いずれか１つのデバイス３００でのみユーザ認証を行えばよい。したがって、ＩＤ／パスワード入力やボタン押下を行うためのＵＩ機能（文字や操作の入力装置及びＵＩの出力装置）を持たないデバイス３００でも、ネットワークサービス２００が利用できるようになる。
【０１２８】
＜第２の実施形態＞
次に、本技術の第２の実施形態を説明する。本実施形態においては、特に説明しない箇所は、上記第１の実施形態と同様の構成である。また本実施形態において、上記第１の実施形態と同様の機能及び構成を有する箇所には同一の符号を付し、その説明を省略または

簡略化する。

【０１２９】

上記第１の実施形態では、サーバ１００によって取得されたアクセストークンを利用したネットワークサービス２００へのアクセスは、必ずサーバ１００を経由することになる。しかし、一般に、ネットワークサービス２００へのアクセスは、ネットワークサービス２００が提供するいくつかのサービスＡＰＩを連続してアクセスする傾向があるため、この度にサーバ１００を経由するのは効率がよくない。

【０１３０】

一方、上記デバイスベースセキュリティ機構により、複数のデバイス３００及びサーバ１００のセキュリティマネージャは、暗号通信により連携した１つのシステムとみなせる。そこで、本実施形態では、サーバ１００側で管理しているアクセストークンを、デバイス３００が一時的に取得し、これを用いて直接ネットワークサービス２００へアクセスすることとしている。

【０１３１】

［サーバ及びデバイスのモジュール構成］

図１２は、本実施形態におけるサーバ１００のソフトウェアモジュール構成を示したブロック図である。また図１３は、本実施形態におけるデバイス３００のソフトウェアモジュール構成を示したブロック図である。

【０１３２】

図１２に示すように、上記デバイス３００からネットワークサービス２００への直接アクセスを実現するため、本実施形態では、サーバ１００は、第１実施形態におけるサービスアクセス処理部１２４に代えて、アクセストークン転送処理部１２７を有する。

【０１３３】

一方、図１３に示すように、本実施形態では、デバイス３００は、第１実施形態におけるサービスアクセス要求部３２７に代えて、サービスアクセス部３２８を有する。

【０１３４】

サーバ１００のアクセストークン転送処理部１２７は、デバイス３００からの要求に従い、アクセストークン管理部１１２からアクセストークンを取得してデバイス３００へ転送する。

【０１３５】

デバイス３００のサービスアクセス部３２８は、サーバ１００側で管理しているアクセストークンを取得し、これを用いて直接ネットワークサービス２００へアクセスする。

【０１３６】

［システムの動作］

次に、本実施形態におけるサーバ１００及びデバイスの動作について説明する。ネットワークサービス認証処理については、上記第１の実施形態と同様である。

【０１３７】

（ネットワークサービスへのアクセス処理）

図１４は、本実施形態におけるデバイス３００によるネットワークサービスへのアクセス処理の流れを示したフローチャートである。また図１５は、本実施形態におけるサーバ１００によるネットワークサービスへのアクセス処理の流れを示したフローチャートである。

【０１３８】

まず、デバイス３００のサービスＵＩ部３４１は、ユーザからのネットワークサービスへのアクセス要求を受け付け、それをサービスアクセス部３２８へ送信する（図１４のステップ１４１）。

【０１３９】

当該アクセス要求を受けたサービスアクセス部３２８は、サーバ１００のアクセストークン転送処理部１２７へ、アクセストークンの転送要求をユーザＩＤ及びサービスＩＤとともに送信する（図１４のステップ１４２）。

【０１４０】
サーバ１００のアクセストークン転送処理部１２７は、当該転送要求を受信すると（図１５のステップ１５１）、アクセストークン管理部１１２から、ユーザＩＤ及びサービスＩＤに対応するネットワークサービス２００へのアクセストークンを取得する（図１５のステップ１５２）。
【０１４１】
そしてアクセストークン転送処理部１２７は、当該取得したアクセストークンを、転送要求元のデバイス３００のサービスアクセス部３２８へ送信する（図１５のステップ１５３）。
【０１４２】
デバイス３００のサービスアクセス部３２８は、サーバ１００からアクセストークンを受信すると、それを用いてネットワークサービス２００へアクセスし、そのアクセス結果をサービスＵＩ部３４１へ送信する（図１４のステップ１４３）。
【０１４３】
そしてサービスＵＩ部３４１は、上記ネットワークサービス２００へのアクセス結果を、表示部３６を介してユーザに提示する（図１４のステップ１４４）。
【０１４４】
［まとめ］
以上説明したように、本実施形態によれば、サーバ１００側で管理しているアクセストークンを、デバイス３００が一時的に取得し、これを用いて直接ネットワークサービス２００へアクセスすることができる。これによりネットワークサービス２００へのアクセス効率が向上するとともに、サーバ１００の負荷が軽減する。
【０１４５】
［変形例］
本技術は上述の実施形態にのみ限定されるものではなく、本技術の要旨を逸脱しない範囲内において種々変更され得る。
【０１４６】
上述の第１及び第２の実施形態において、サーバ１００が取得したアクセストークンの記憶場所は、サーバ１００内部の記憶部１８（アクセストークン管理部１１２）とされている。しかし、アクセストークンは、セキュリティが確保されていれば、サーバ１００とは物理的に離れた、クラウド上の他の記憶装置に記憶されてもよい。
【０１４７】
上述の第２の実施形態では、デバイス３００は、ネットワークサービス２００へのアクセスの度にアクセストークンをサーバ１００から取得している。しかし、デバイス３００は、一旦サーバ１００から取得したアクセストークンをＲＡＭ３３や記憶部３８に一定時間保持しておいてもよい。そしてデバイス３００は、保持したものと同じアクセストークンを必要とするネットワークサービスアクセス要求がユーザからあった場合には、それを再度利用してもよい。
【０１４８】
上述の第１及び第２の実施形態においては、デバイス３００間及びデバイス３００とサーバ１００との通信には、デバイスベースのセキュリティ機構が用いられた。しかし、他の手段によりセキュリティが確保される場合においては、デバイスベースのセキュリティ機構が用いられなくてもよい。
【０１４９】
上述した第１及び第２の実施形態における各技術は、それぞれ独立して実施可能であるとともに、互いに矛盾しない限り、如何様にも組み合わされて実施されうる。
【０１５０】
［その他］
本技術は以下のような構成も採ることができる。
（１）

第１の機器と、第２の機器と、前記第１の機器のユーザに関するリソースを有するネットワーク上のサービスと通信可能な通信部と、
記憶部と、
前記第１の機器からの、前記リソースへのアクセス権の取得要求と、当該アクセス権の取得に対する前記ユーザの承認を示す承認情報とに基づいて、前記サービスへ、前記アクセス権を示すアクセストークンの発行要求を送信し、前記サービスから、当該サービスによって発行されたアクセストークンを受信するように前記通信部を制御し、
前記受信されたアクセストークンを安全に記憶するように前記記憶部を制御する
ことが可能な制御部と
を具備する情報処理装置。

（２）
上記（１）に記載の情報処理装置であって、
前記制御部は、前記ユーザと関連付けられた第２の機器からの要求に応じて、前記記憶されたアクセストークンを用いて前記リソースへアクセスするように前記通信部を制御する
情報処理装置。

（３）
上記（１）または（２）に記載の情報処理装置であって、
前記制御部は、安全な通信路を介して前記第１の機器または前記第２の機器へ前記記憶されたアクセストークンを送信するように前記通信部を制御する
情報処理装置。

（４）
上記（１）～（３）に記載の情報処理装置であって、
前記第１の機器は、前記ユーザが前記承認の意思を前記サービスへ通知するために必要な操作が入力される入力装置と、当該入力のための画面を出力する出力装置とを有し、
前記第２の機器は前記入力装置及び前記出力装置を有さない
情報処理装置。

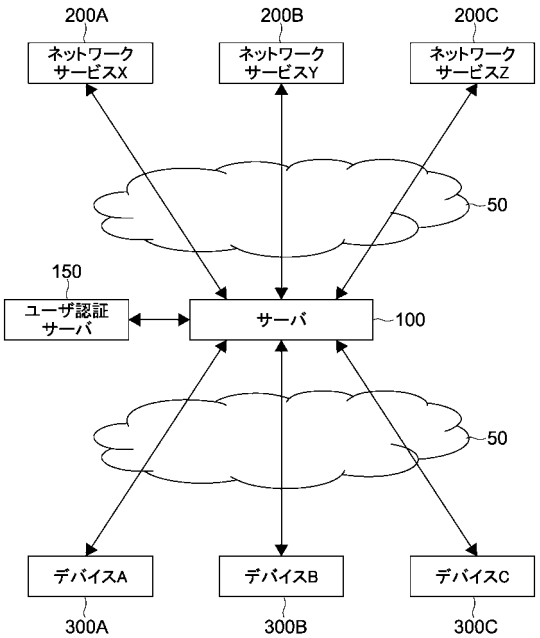
（５）
上記（１）～（４）のいずれかに記載の情報処理装置であって、
前記制御部は、前記第１の機器から、前記ユーザと、前記第１の機器と、前記第２の機器との関連付けを示す関連付け情報を受信するように前記通信部を制御し、前記受信された前記関連付け情報を記憶するように前記記憶部を制御する
情報処理装置。

【符号の説明】

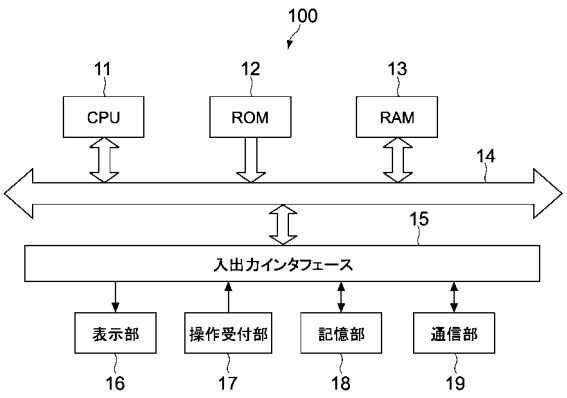
【０１５１】
１１、３１…ＣＰＵ
１３、３３…ＲＡＭ
１８、３８…記憶部
１９、３９…通信部
３６…表示部
３７…操作受付部
５０…ＷＡＮ
１００…サーバ
１１２…アクセストークン管理部
１２３…サービス認証処理部
１２４…サービスアクセス処理部
１２７…アクセストークン転送処理部
１３１…通信部
１５０…ユーザ認証サーバ
２００（２００Ａ、２００Ｂ、２００Ｃ）…ネットワークサービス

３００（３００Ａ、３００Ｂ、３００Ｃ）…デバイス
３１１…通信部
３２６…サービス認証部
３２７…サービスアクセス要求部
３２８…サービスアクセス部
３４１…サービスＵＩ部

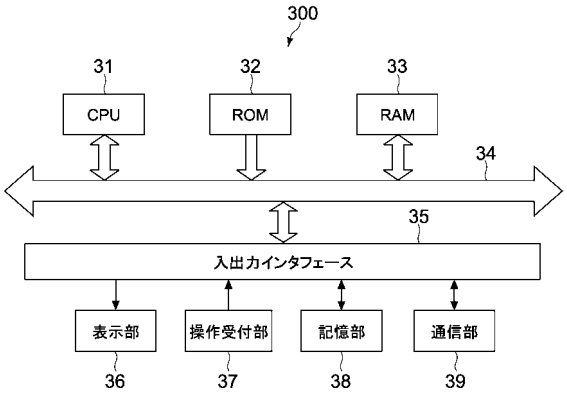
【図１】



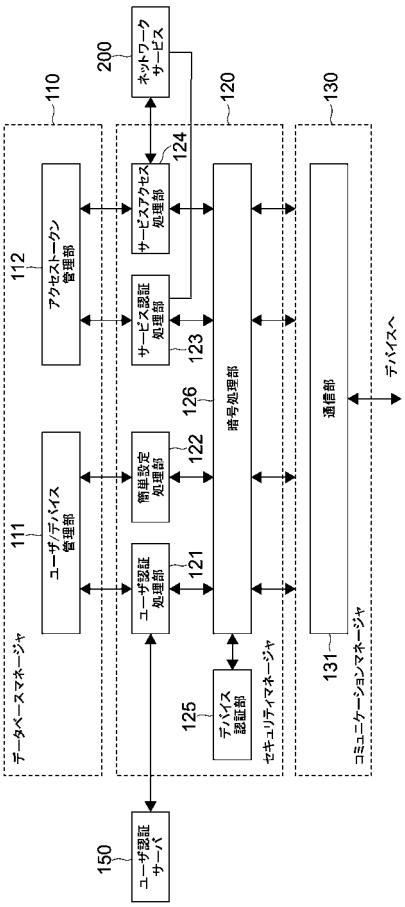
【図２】



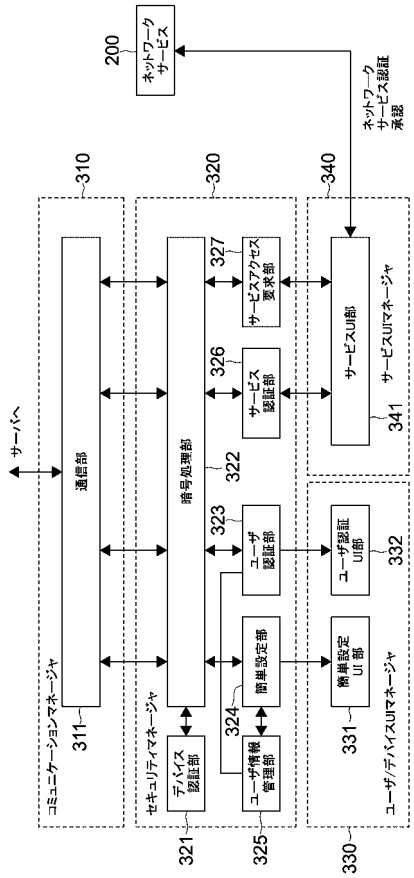
【図３】



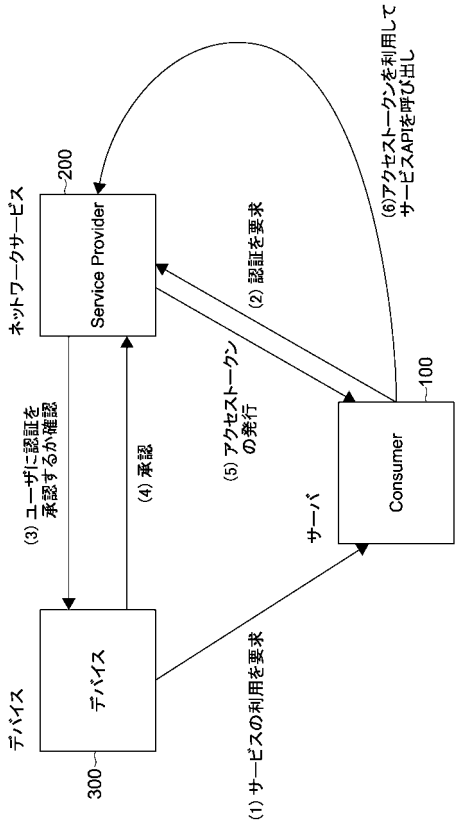
【図４】


データベースマネージャ
ユーザ/デバイス管理部
アクセストークン管理部
ユーザ認証処理部
簡単設定処理部
サービス認証処理部
サービスアクセス処理部
暗号処理部
デバイス認証部
セキュリティマネージャ
通信部
コミュニケーションマネージャ
デバイスへ
ネットワークサービス
ユーザ認証サーバ
110
111
112
120
121
122
123
124
125
126
130
131
150
200

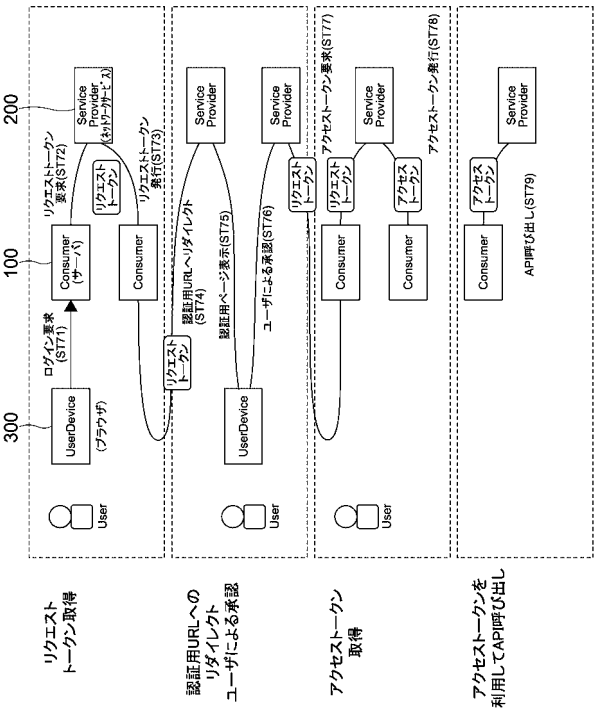
【図５】


サーバへ
通信部
コミュニケーションマネージャ
暗号処理部
セキュリティマネージャ
デバイス認証部
ユーザ認証部
サービス認証部
サービスアクセス要求部
サービスUI部
サービスUIマネージャ
簡単設定UI部
ユーザ認証UI部
ユーザ/デバイスUIマネージャ
ユーザ情報管理部
ネットワークサービス
ネットワークサービス認証承認
200
310
311
320
321
322
323
324
325
326
327
330
331
332
340
341

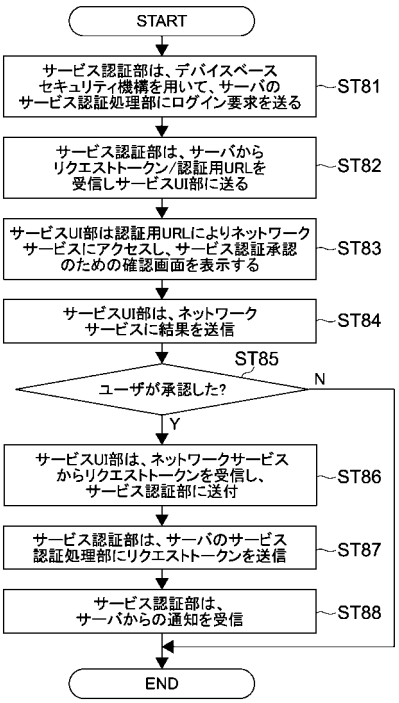
【図６】


ネットワークサービス
Service Provider
デバイス
Consumer
サーバ
(1) サービスの利用を要求
(2) 認証を要求
(3) ユーザに認証を承認するか確認
(4) 承認
(5) アクセストークンの発行
(6)アクセストークンを利用してサービスAPIを呼び出し
200
300
100

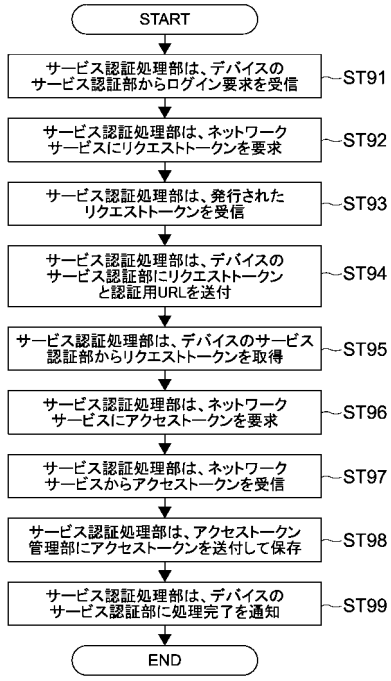
【図７】


200
100
300
Service Provider
Consumer
UserDevice
User
ログイン要求(ST71)
リクエストトークン要求(ST72)
リクエストトークン発行(ST73)
認証用URLへリダイレクト(ST74)
認証用ページ表示(ST75)
ユーザによる承認(ST76)
アクセストークン要求(ST77)
アクセストークン発行(ST78)
API呼び出し(ST79)
リクエストトークン
アクセストークン
リクエストトークン取得
認証用URLへのリダイレクトユーザによる承認
アクセストークン取得
アクセストークンを利用してAPI呼び出し

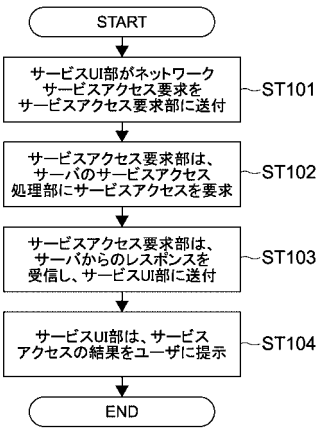
【図８】


START
サービス認証部は、デバイスベース セキュリティ機構を用いて、サーバの サービス認証処理部にログイン要求を送る
ST81
サービス認証部は、サーバから リクエストトークン/認証用URLを 受信しサービスUI部に送る
ST82
サービスUI部は認証用URLによりネットワーク サービスにアクセスし、サービス認証承認 のための確認画面を表示する
ST83
サービスUI部は、ネットワーク サービスに結果を送信
ST84
ST85
ユーザが承認した?
N
Y
サービスUI部は、ネットワークサービス からリクエストトークンを受信し、 サービス認証部に送付
ST86
サービス認証部は、サーバのサービス 認証処理部にリクエストトークンを送信
ST87
サービス認証部は、 サーバからの通知を受信
ST88
END

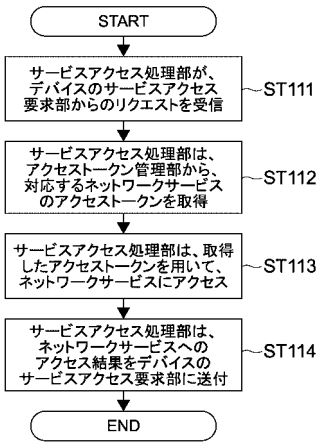
【図９】


START
サービス認証処理部は、デバイスの サービス認証部からログイン要求を受信
ST91
サービス認証処理部は、ネットワーク サービスにリクエストトークンを要求
ST92
サービス認証処理部は、発行された リクエストトークンを受信
ST93
サービス認証処理部は、デバイスの サービス認証部にリクエストトークン と認証用URLを送付
ST94
サービス認証処理部は、デバイスのサービス 認証部からリクエストトークンを取得
ST95
サービス認証処理部は、ネットワーク サービスにアクセストークンを要求
ST96
サービス認証処理部は、ネットワーク サービスからアクセストークンを受信
ST97
サービス認証処理部は、アクセストークン 管理部にアクセストークンを送付して保存
ST98
サービス認証処理部は、デバイスの サービス認証部に処理完了を通知
ST99
END

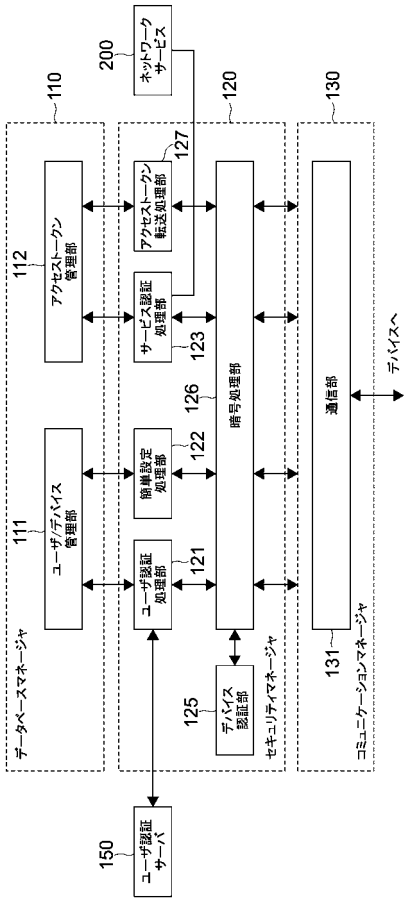
【図１０】


START
サービスUI部がネットワーク サービスアクセス要求を サービスアクセス要求部に送付
ST101
サービスアクセス要求部は、 サーバのサービスアクセス 処理部にサービスアクセスを要求
ST102
サービスアクセス要求部は、 サーバからのレスポンスを 受信し、サービスUI部に送付
ST103
サービスUI部は、サービス アクセスの結果をユーザに提示
ST104
END

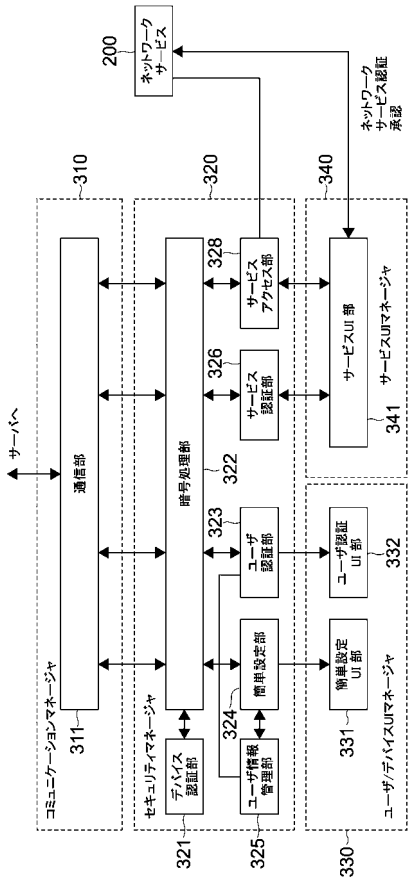
【図１１】


START
サービスアクセス処理部が、 デバイスのサービスアクセス 要求部からのリクエストを受信
ST111
サービスアクセス処理部は、 アクセストークン管理部から、 対応するネットワークサービス のアクセストークンを取得
ST112
サービスアクセス処理部は、取得 したアクセストークンを用いて、 ネットワークサービスにアクセス
ST113
サービスアクセス処理部は、 ネットワークサービスへの アクセス結果をデバイスの サービスアクセス要求部に送付
ST114
END

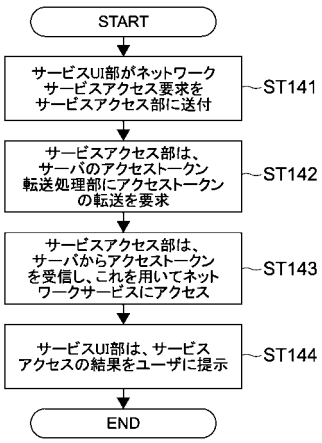
【図１２】



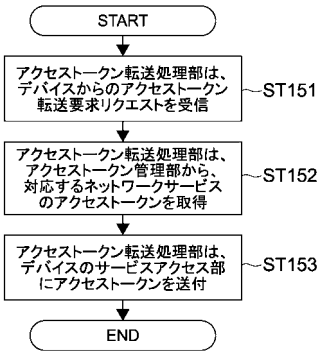
【図１３】



【図１４】



【図１５】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/000390

A. CLASSIFICATION OF SUBJECT MATTER
G06F21/41(2013.01)i, *G06F21/44*(2013.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F21/41, G06F21/44

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2013
Kokai Jitsuyo Shinan Koho 1971-2013 Toroku Jitsuyo Shinan Koho 1994-2013

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Takao OGURA et al., "Proposal of Secure Data/ Service Collaboration Method among Public Clouds", IEICE Technical Report, 14 July 2011 (14.07.2011), vol.111, no.146, pages 69 to 74, IN2011-57 (2011-7)	1-8
A	WO 2011/080874 A1 (NEC Corp.), 07 July 2011 (07.07.2011), paragraphs [0053] to [0076]; fig. 8 to 9 & US 2012/0291109 A1	1-8
A	WO 2012/017561 A1 (Fujitsu Ltd.), 09 February 2012 (09.02.2012), abstract; fig. 4, 5, 7, 9, 13, 14, 17, 18 (Family: none)	1-8

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 March, 2013 (26.03.13)	02 April, 2013 (02.04.13)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2013/000390

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	Ryu WATANABE et al., "An Investigation of the Platform Technology for Mobile Terminals", The Journal of the Institute of Electronics, Information and Communication Engineers, 01 September 2011 (01.09.2011), vol.94, no.9, pages 827 to 843	1-8

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１３／０００３９０

A． 発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl. G06F21/41(2013.01)i, G06F21/44(2013.01)i

B． 調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl. G06F21/41, G06F21/44

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１３年
日本国実用新案登録公報	１９９６－２０１３年
日本国登録実用新案公報	１９９４－２０１３年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C． 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	小倉 孝夫ほか, 他社クラウドを含めた安全なデータ・サービス連携方式の提案, 電子情報通信学会技術研究報告, 2011.07.14, Vol. 111, No. 146, pp. 69-74, IN2011-57 (2011-7)	1-8
A	WO 2011/080874 A1 (日本電気株式会社) 2011.07.07, 段落[0053]-[0076], 図 8-9 & US 2012/0291109 A1	1-8

☑ Ｃ欄の続きにも文献が列挙されている。 ☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日 ２６．０３．２０１３	国際調査報告の発送日 ０２．０４．２０１３
国際調査機関の名称及びあて先 日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員） ５Ｓ ４８７６ 石田 信行 電話番号 ０３－３５８１－１１０１ 内線 ３５４６

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００９年７月）

国際調査報告

国際出願番号 ＰＣＴ／ＪＰ２０１３／０００３９０

C（続き）. 関連すると認められる文献

引用文献のカテゴリー＊	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	WO 2012/017561 A1 (富士通株式会社) 2012.02.09, 要約, 図 4,5,7,9,13,14,17,18 (No Family)	1-8
A	渡辺 龍ほか, 端末プラットホーム技術の研究開発について, 電子情報通信学会誌, 2011.09.01, Vol. 94, No. 9, pp. 827-843	1-8

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LR,LS,MW,MZ,NA,RW,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,RU,TJ,TM),EP(AL,AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MK,MT,NL,NO,PL,PT,RO,RS,SE,SI,SK,SM,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BN,BR,BW,BY,BZ,CA,CH,CL,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PA,PE,PG,PH,PL,PT,QA,RO,RS,RU,RW,SC,SD,SE,SG,SK,SL,SM,ST,SV,SY,TH,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC

（特許庁注：以下のものは登録商標）
１．ＤＬＮＡ

(72)発明者 島川 真人
東京都港区港南１丁目７番１号 ソニー株式会社内

（注）この公表は、国際事務局（ＷＩＰＯ）により国際公開された公報を基に作成したものである。なおこの公表に係る日本語特許出願（日本語実用新案登録出願）の国際公開の効果は、特許法第１８４条の１０第１項(実用新案法第４８条の１３第２項）により生ずるものであり、本掲載とは関係ありません。