

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第6257085号
(P6257085)

(45) 発行日 平成30年1月10日 (2018. 1. 10)

(24) 登録日 平成29年12月15日 (2017. 12. 15)

(51) Int. Cl. F 1
G 0 6 F 21/31 (2013.01) G 0 6 F 21/31

請求項の数 6 (全 14 頁)

(21) 出願番号	特願2014-96001 (P2014-96001)	(73) 特許権者	599115217
(22) 出願日	平成26年5月7日 (2014. 5. 7)		株式会社 ディー・エヌ・エー
(62) 分割の表示	特願2013-263744 (P2013-263744) の分割		東京都渋谷区渋谷二丁目2 1 番 1 号
原出願日	平成25年12月20日 (2013. 12. 20)	(74) 代理人	100126572
(65) 公開番号	特開2015-122049 (P2015-122049A)		弁理士 村越 智史
(43) 公開日	平成27年7月2日 (2015. 7. 2)	(74) 代理人	100125195
審査請求日	平成28年12月19日 (2016. 12. 19)		弁理士 尾畑 雄一
		(72) 発明者	川上 裕幸
			東京都渋谷区渋谷二丁目2 1 番 1 号 株式
			会社ディー・エヌ・エー内
		(72) 発明者	水島 壮太
			東京都渋谷区渋谷二丁目2 1 番 1 号 株式
			会社ディー・エヌ・エー内

最終頁に続く

(54) 【発明の名称】 所定のサーバに対してログインを要求するログイン要求装置及び方法、並びにこれらに用いられるプログラム

(57) 【特許請求の範囲】

【請求項 1】

所定のサーバへログイン可能な複数のアプリケーションプログラムを実行可能な情報処理装置であって、前記複数のアプリケーションプログラムの中の1のアプリケーションプログラムを起動する起動部と、前記複数のアプリケーションプログラムの前記所定のサーバへのログイン情報をログイン履歴として所定数記憶するログイン履歴部と、前記ログイン履歴に含まれる他のアプリケーションプログラムに対応する記憶領域から前記所定のサーバへのログインの認証用情報を取得する第1の取得部と、取得したログインの認証用情報を用いて前記所定のサーバにログインを要求するログイン要求部と、要求したログインが該所定のサーバに許可された場合に前記所定のサーバにより発行される認証用情報を取得する第2の取得部と、発行された認証用情報を前記1のアプリケーションプログラムに対応する記憶領域に記憶する記憶部と、を備え、前記ログイン履歴部は、新たにログインした前記1のアプリケーションプログラムのログイン情報を追加し、最も古いログイン情報を削除する、情報処理装置。

【請求項 2】

前記第1の取得部は、前記ログイン履歴に含まれる各ログイン情報の中からログイン日

10

20

時が新しいほど優先される傾向で１のログイン情報を特定し、当該特定された１のログイン情報に用いられたアプリケーションプログラムに対して前記認証用情報を要求する請求項１記載の情報処理装置。

【請求項３】

前記第１の取得部は、前記ログイン履歴に含まれるログイン情報の中からログインに用いられたアプリケーションプログラムが前記コンピュータからアンインストールされていないログインのうちログイン日時が最も新しいログイン情報を前記１のログイン情報として特定する請求項２記載の情報処理装置。

【請求項４】

前記他のアプリケーションプログラムのそれぞれに対応する記憶領域は、対応するアプリケーションプログラムを介したアクセスのみが許容される記憶領域である請求項１から請求項３のいずれかに記載の情報処理装置。

【請求項５】

情報処理装置で実行可能な複数のアプリケーションプログラムが所定のサーバに対してログインを要求する方法であって、

前記複数のアプリケーションプログラムの中の１のアプリケーションプログラムを起動するステップと、

前記複数のアプリケーションプログラムの前記所定のサーバへのログイン情報で構成されるログイン履歴に含まれる他のアプリケーションプログラムに対応する記憶領域から前記所定のサーバへのログインの認証用情報を取得するステップと、

取得したログインの認証用情報を用いて前記所定のサーバにログインを要求するステップと、

要求したログインが該所定のサーバに許可された場合に前記所定のサーバにより発行される認証用情報を取得するステップと、

発行された認証用情報を前記１のアプリケーションプログラムに対応する記憶領域に記憶するステップと、

前記１のアプリケーションプログラムのログイン情報を前記ログイン履歴に追加し、最も古いログイン情報を前記ログイン履歴から削除するステップと、を備える、方法。

【請求項６】

情報処理装置で実行可能な複数のアプリケーションプログラムが所定のサーバに対してログインを要求するためのプログラムであって、

前記情報処理装置で実行されることに応じて、前記情報処理装置に、

前記複数のアプリケーションプログラムの中の１のアプリケーションプログラムを起動するステップと、

前記複数のアプリケーションプログラムの前記所定のサーバへのログイン情報で構成されるログイン履歴に含まれる他のアプリケーションプログラムに対応する記憶領域から前記所定のサーバへのログインの認証用情報を取得するステップと、

取得したログインの認証用情報を用いて前記所定のサーバにログインを要求するステップと、

要求したログインが該所定のサーバに許可された場合に前記所定のサーバにより発行される認証用情報を取得するステップと、

発行された認証用情報を前記１のアプリケーションプログラムに対応する記憶領域に記憶するステップと、

前記１のアプリケーションプログラムのログイン情報を前記ログイン履歴に追加し、最も古いログイン情報を前記ログイン履歴から削除するステップと、を実行させる、プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

10

20

30

40

50

本発明は、所定のサーバに対してログインを要求するログイン要求装置及び方法、並びにこれらに用いられるプログラムに関する。

【背景技術】

【0002】

従来より、インターネット等のネットワークを介して提供されるサービスをユーザが利用するには、ユーザID及びパスワード等の情報をユーザが入力し、入力された情報に基づくログイン認証が行われている。また、ユーザID及びパスワード等の情報を入力する手間を軽減するために、初回のログイン時にサーバが認証トークンを発行してユーザの端末装置に送信し、2回目以降のログイン時にはこの認証トークンをサーバに送信することによってログイン認証を行う技術が提案されている（例えば、特許文献1参照）。一方、近年、スマートフォン等の端末装置にアプリケーションプログラムをインストールし、このアプリケーションプログラムを用いて上述したサービスを利用する形態が増えている。このようにアプリケーションプログラムを用いてサービスを利用する形態においては、例えば、利用するサービスの運営者が同一である場合等には、複数のアプリケーションプログラムにおいて同一のユーザID及びパスワード等の情報を用いてログインすることが可能となることがある。従って、上述した認証トークンを複数のアプリケーションプログラム間で共有することによって、ユーザID及びパスワード等の情報を入力する手間をより一層軽減することができるように考えると考えられる。

10

【先行技術文献】

【特許文献】

20

【0003】

【特許文献1】特開2012-191270号公報

【発明の概要】

【発明が解決しようとする課題】

【0004】

しかしながら、複数のアプリケーションプログラム間で上述した認証トークンを共有する場合、機密性が高い認証トークンのセキュリティを確保する必要が生じる。このように機密性が高い情報を管理するための特別な仕組み（例えば、暗号化処理のなされたセキュアな記憶領域を用いてユーザID及びパスワード等の情報を管理する仕組み等）が実装されているオペレーティングシステムも存在するものの、こうした仕組みは全てのオペレーティングシステムにおいて実装されているとは限らない。例えば、暗号化処理のなされていない非セキュアな記憶領域に認証トークンを記憶して複数のアプリケーションプログラム間で共有してしまうと、悪意のある第三者によるアプリケーションプログラムによって認証トークンが不正に利用され、不正なログインを許容してしまう恐れがある。従って、セキュリティを確保しつつ複数のアプリケーションプログラム間で認証トークンを共有するより簡易な仕組みの実現が望まれる。

30

【0005】

本発明の実施形態は、ログインに必要な情報をセキュリティを確保しつつ複数のアプリケーションプログラム間で共有するより簡易な仕組みを提供することを目的の一つとする。本発明の他の目的は、本明細書全体を参照することにより明らかとなる。

40

【課題を解決するための手段】

【0006】

本発明の一実施形態に係る第1のプログラムは、複数のプログラムモジュールによって構成され、コンピュータに、当該プログラムモジュールに対応する機能を実現させる第1のプログラムであって、前記複数のプログラムモジュールは、前記コンピュータ上で実行可能な所定のプログラムを用いた所定のサーバへのログインの履歴であって当該コンピュータによってアクセス可能な所定の記憶領域に記憶されているログイン履歴を参照し、当該ログイン履歴に含まれるログインに用いられた第2のプログラムに対して当該所定のサーバへのログインに用いる認証用情報を要求する認証用情報要求モジュールと、前記第2のプログラムから取得した前記認証用情報を用いて前記所定のサーバに対してログインを

50

要求するログイン要求モジュールと、を含む。

【 0 0 0 7 】

上述した一実施形態に係る第 1 のプログラムにおいて、前記複数のプログラムモジュールは、前記所定のサーバへのログインに応じて当該所定のサーバから新たに認証用情報を取得し、当該取得した認証用情報を前記第 1 のプログラムによって管理され前記コンピュータによってアクセス可能な第 1 のプログラム用記憶領域に記憶させる認証用情報記憶モジュールと、第 3 のプログラムからの要求に応答し、前記第 1 のプログラム用記憶領域に記憶されている前記認証用情報を当該第 3 のプログラムに対して提供する認証用情報提供モジュールと、を更に含む態様としたり、前記複数のプログラムモジュールは、前記所定のサーバへのログインに応じて前記第 1 のプログラムを用いた前記所定のサーバへのログインを前記ログイン履歴に記録するログイン履歴記録モジュールを更に含む態様とすることもできる。

10

【 0 0 0 8 】

本発明の一実施形態に係る方法は、コンピュータが、所定のサーバに対してログインを要求する方法であって、第 2 のプログラムによって、当該第 2 のプログラムを用いた前記所定のサーバへのログインに応じて当該所定のサーバから当該所定のサーバへのログインに用いる認証用情報を取得し、当該取得した認証用情報を当該第 2 のプログラムによって管理され前記コンピュータによってアクセス可能な第 2 のプログラム用記憶領域に記憶させ、前記第 2 のプログラムによって、当該第 2 のプログラムを用いた前記所定のサーバへのログインに応じて当該第 2 のプログラムを用いた当該所定のサーバへのログインを、前記コンピュータ上で実行可能な所定のプログラムを用いた当該所定のサーバへのログインの履歴であって当該コンピュータによってアクセス可能な所定の記憶領域に記憶されているログイン履歴に記録し、第 1 のプログラムによって、前記ログイン履歴を参照し、当該ログイン履歴に含まれるログインに用いられた前記第 2 のプログラムに対して前記認証用情報を要求し、前記第 2 のプログラムによって、前記第 1 のプログラムからの要求に応答し、前記第 2 のプログラム用記憶領域に記憶されている前記認証用情報を当該第 1 のプログラムに対して提供し、前記第 1 のプログラムによって、前記第 2 のプログラムから取得した前記認証用情報を用いて前記所定のサーバに対してログインを要求する。

20

【 0 0 0 9 】

本発明の一実施形態に係るログイン要求装置は、所定のサーバに対してログインを要求するログイン要求装置であって、第 2 のプログラムによって、当該第 2 のプログラムを用いた前記所定のサーバへのログインに応じて当該所定のサーバから当該所定のサーバへのログインに用いる認証用情報を取得し、当該取得した認証用情報を当該第 2 のプログラムによって管理され前記コンピュータによってアクセス可能な第 2 のプログラム用記憶領域に記憶させる認証用情報記憶部と、前記第 2 のプログラムによって、当該第 2 のプログラムを用いた前記所定のサーバへのログインに応じて当該第 2 のプログラムを用いた当該所定のサーバへのログインを、前記コンピュータ上で実行可能な所定のプログラムを用いた当該所定のサーバへのログインの履歴であって当該コンピュータによってアクセス可能な所定の記憶領域に記憶されているログイン履歴に記録するログイン履歴記録部と、第 1 のプログラムによって、前記ログイン履歴を参照し、当該ログイン履歴に含まれるログインに用いられた前記第 2 のプログラムに対して前記認証用情報を要求する認証用情報要求部と、前記第 2 のプログラムによって、前記第 1 のプログラムからの要求に応答し、前記第 2 のプログラム用記憶領域に記憶されている前記認証用情報を当該第 1 のプログラムに対して提供する認証用情報提供部と、前記第 1 のプログラムによって、前記第 2 のプログラムから取得した前記認証用情報を用いて前記所定のサーバに対してログインを要求するログイン要求部と、を備える。

30

40

【発明の効果】

【 0 0 1 0 】

本発明の様々な実施形態によって、ログインに必要な情報をセキュリティを確保しつつ複数のアプリケーションプログラム間で共有するより簡易な仕組みを提供することができ

50

る。

【図面の簡単な説明】

【 0 0 1 1 】

【図 1】本発明の一実施形態に係る端末装置 30 を含むシステム 1 のネットワーク構成を概略的に示すブロック図。

【図 2】本発明の一実施形態に係るプログラム 50 のモジュール構成を概略的に示すブロック図。

【図 3】一実施形態におけるログイン履歴によって管理される情報の具体例を示す図。

【図 4】一実施形態におけるログイン処理の一例を示すフロー図。

【発明を実施するための形態】

10

【 0 0 1 2 】

図 1 は、本発明の一実施形態に係る端末装置 30 を含むシステム 1 のネットワーク構成を概略的に示すブロック図である。図 1 に示すように、一実施形態における端末装置 30 は、一般的なコンピュータとして構成されるサーバ 10 とインターネット等の通信網 20 を介して通信可能に接続されており、端末装置 30 のユーザは、サーバ 10 が提供する様々なインターネットサービスを利用することができる。ここで、サーバ 10 が提供するインターネットサービスとしては、例えば、ゲーム等のデジタルコンテンツを提供するサービス、及び、それぞれ端末装置 30 を操作する複数のユーザ間の様々なコミュニケーション（チャット（ミニメール）、サークル、アバター、日記、伝言板、挨拶、通話等）を実現するプラットフォームサービス（SNS サービス）等を例示することができるが、これらに限定されない。また、後述するように、端末装置 30 は、サーバ 10 に対してログインを要求する本発明の一実施形態に係るログイン要求装置としても機能する。

20

【 0 0 1 3 】

サーバ 10 は、図示のとおり、CPU（コンピュータプロセッサ）11 と、メインメモリ 12 と、ユーザ I / F 13 と、通信 I / F 14 と、ストレージ 15 と、ディスクドライブ 16 とを含み、これらの各構成要素がバス 17 を介して互いに電氣的に接続されている。CPU 11 は、ストレージ 15 から様々なプログラムをメインメモリ 12 にロードし、ロードしたプログラムに含まれる命令を実行する。メインメモリ 12 は、CPU 11 が実行するプログラムを格納するために用いられ、例えば、DRAM によって構成される。

【 0 0 1 4 】

30

ユーザ I / F 13 は、例えば、オペレータの入力を受け付けるキーボードやマウス等の情報入力装置と、CPU 11 の演算結果を出力する液晶ディスプレイ等の情報出力装置とを含む。通信 I / F 14 は、ハードウェア、ファームウェア、又は TCP / IP ドライバや PPP ドライバ等の通信用ソフトウェア又はこれらの組み合わせとして実装され、通信網 20 を介して端末装置 30 と通信可能に構成される。

【 0 0 1 5 】

ストレージ 15 は、例えば磁気ディスクドライブで構成され、サーバ 10 によって提供される各種サービスの進行を制御するための制御用プログラム等の様々なプログラムが記憶される。また、ストレージ 15 には、各種サービスにおいて用いられる各種データも記憶され得る。ストレージ 15 に記憶され得る各種データは、サーバ 10 と通信可能に接続されるサーバ 10 とは物理的に別体のデータベースサーバ等に格納されてもよい。ディスクドライブ 16 は、CD - ROM、DVD - ROM、DVD - R 等の各種の記憶メディアに格納されたデータを読み込み、又は、これらの記憶メディアにデータを書き込む。

40

【 0 0 1 6 】

一実施形態において、サーバ 10 は、階層構造の複数のウェブページから成るウェブサイトを管理するウェブサーバとしても機能し、端末装置 30 に対してこのウェブサイトを介して各種サービスを提供することができる。端末装置 30 は、ウェブページを表示するための HTML データをサーバ 10 から取得し、取得した HTML データを解析して、当該ウェブページを端末装置 30 のユーザに提示することができる。例えば、このようなウェブページを介して提供されるゲームは、ブラウザゲームと称されることがある。ストレ

50

ージ 15 には、このウェブページを表示するための HTML データも記憶される。HTML データは、HTML 等のマークアップ言語で記述された HTML 文書から成り、この HTML 文書には、様々な画像が関連付けられる。また、HTML 文書には、各種スクリプト言語等で記述されたプログラムが埋め込まれ得る。

【0017】

ストレージ 15 には、端末装置 30 においてブラウザソフトウェア以外の実行環境上で実行されるアプリケーションも格納され得る。このアプリケーションには、各種処理を実行するためのプログラムや当該プログラム実行時に参照される画像データ等の各種データを含めることができる。プログラムは、例えば、Objective-C、Java（登録商標）等のオブジェクト指向プログラミング言語で作成される。ストレージ 15 に記憶されたアプリケーションは、配信要求に応じて端末装置 30 に配信され得る。サーバ 10 から配信されたアプリケーションは、端末装置 30 において、CPU 31 の制御に従って通信 I/F 34 を介して受信され、受信されたアプリケーションがストレージ 35 に送信され記憶される。このアプリケーションは、ユーザによる端末装置 30 の操作に応じて起動され、端末装置 30 に実装された NgCore（商標）や Android（商標）等の実行環境上で実行される。サーバ 10 は、端末装置 30 で実行されているアプリケーションに対して必要な各種データを提供し得る。また、サーバ 10 は、端末装置 30 から送信される各種データをユーザ毎に記憶することで、ユーザ毎にゲームの進行等の各種サービスの状況を管理することができる。

【0018】

このように、サーバ 10 は、各種サービスを提供するウェブサイト进行管理し、当該ウェブサイトを作成するウェブページを端末装置 30 からの要求に応じて配信することにより、各種サービスを提供することができる。また、サーバ 10 は、このようなブラウザベースのサービスとは代替的に、又は、ブラウザベースのサービスに加えて、端末装置 30 で実行されるアプリケーションとの通信に基づいて各種サービスを提供させることができる。詳細な説明は省略するが、サーバ 10 は、各種サービスの提供開始時におけるユーザの認証処理や各種サービスの提供に応じて発生する課金処理を行う機能等を有することもできる。

【0019】

端末装置 30 は、一実施形態において、サーバ 10 から取得したウェブサイトのウェブページをウェブブラウザ上で表示すると共にアプリケーションを実行するためのアプリケーション実行環境を実装した任意の情報処理装置であり、パーソナルコンピュータ、スマートフォン、タブレット端末、及びゲーム専用端末等が含まれ得る。

【0020】

端末装置 30 は、図示のとおり、CPU（コンピュータプロセッサ）31 と、メインメモリ 32 と、ユーザ I/F 33 と、通信 I/F 34 と、ストレージ 35 と、を含み、これらの各構成要素がバス 36 を介して互いに電氣的に接続されている。

【0021】

CPU 31 は、ストレージ 35 から様々なプログラムをメインメモリ 32 にロードし、ロードしたプログラムに含まれる命令を実行する。メインメモリ 32 は、CPU 31 が実行するプログラムを格納するために用いられ、例えば、DRAM によって構成される。

【0022】

ユーザ I/F 33 は、ユーザの入力を受け付ける情報入力装置と、CPU 31 の演算結果を出力する情報出力装置であり、タッチパネルを備える液晶ディスプレイなどの表示装置を含む。

【0023】

通信 I/F 34 は、ハードウェア、ファームウェア、又は、TCP/IP ドライバや PPP ドライバ等の通信用ソフトウェア又はこれらの組み合わせとして実装され、通信網 20 を介してサーバ 10 と通信可能に構成される。

【0024】

10

20

30

40

50

ストレージ３５は、例えば磁気ディスクドライブやフラッシュメモリ等により構成され、オペレーティングシステム及びアプリケーションプログラム等の様々なプログラム、並びにこれらのプログラムによって扱われる様々なデータを記憶し得る。ここで、ストレージ３５は、内蔵ストレージ及び取り外し可能なリムーバブルストレージの両方が含まれる。リムーバブルストレージとしては、例えば、フラッシュメモリが内蔵されたＳＤメモリカード等が含まれる。

【００２５】

このようなアーキテクチャを有する端末装置３０は、例えば、ＨＴＭＬデータを解釈して画面表示するためのブラウザソフトウェアを備えており、このブラウザソフトウェアの機能によりサーバ１０から取得したＨＴＭＬデータを解釈して、受信したＨＴＭＬデータ
10
に対応するウェブページを表示することができる。また、端末装置３０は、ブラウザソフトウェアに組み込まれるプラグインソフトを備えており、ＨＴＭＬデータに埋め込まれたＳＷＦ形式等のファイルをサーバ１０又は他のサーバ等から取得し、当該ＳＷＦ形式のファイルをブラウザソフトウェア及びプラグインソフトを用いて実行することもできる。

【００２６】

端末装置３０においてブラウザソフトウェア又はアプリケーションプログラムが実行されると、例えば、プログラムにより指示されたアニメーションや操作用アイコンが端末装置
20
３０の画面に表示される。ユーザは、端末装置３０のユーザＩ／Ｆ３３を用いて各種指示を入力することができる。ユーザから入力された指示は、端末装置３０のブラウザやＮｇＣｏｒｅ（商標）等の実行環境の機能を通じてサーバ１０に伝達される。

【００２７】

次に、本発明の一実施形態に係るアプリケーションプログラム５０について説明する。一実施形態におけるアプリケーションプログラム５０は、サーバ１０によって提供される各種サービスを利用するためのアプリケーションプログラムであって、端末装置３０等のコンピュータ上で実行されることによって、このコンピュータを、サーバ１０に対してログインを要求するログイン要求装置として機能させる。また、端末装置３０を操作するユーザがサーバ１０によって提供される各種サービスをアプリケーションプログラム５０を用いて利用しようとする場合には、サーバ１０又は他のサーバ（例えば、アプリケーションプログラム、映画、音楽、書籍等の配信サービスを提供するサーバ等）から利用するサービスに対応するアプリケーションプログラム５０をダウンロードして端末装置３０にイン
30
ストールする。インストールされたアプリケーションプログラム５０はストレージ３５に記憶される。こうしたアプリケーションプログラム５０のインストール及びアンインストールは、主に、端末装置３０のオペレーティングシステムの機能によって実現される。なお、端末装置３０には、サーバ１０が提供する複数のサービスにそれぞれ対応する複数のアプリケーションプログラム５０がインストールされ、又、アプリケーションプログラム５０以外の複数のアプリケーションプログラム（例えば、サーバ１０以外のサーバが提供するサービス（サーバ１０の運営者以外の運営者によって提供されるサービス）を利用するためのアプリケーションプログラム等）がインストールされ得る。

【００２８】

一実施形態におけるアプリケーションプログラム５０は、複数のプログラムモジュールによって構成され、端末装置３０等のコンピュータに、このプログラムモジュールに対応する機能を実現させる。具体的には、アプリケーションプログラム５０が端末装置３０のＣＰＵ３１（コンピュータプロセッサ）によって実行されると、このアプリケーションプログラム５０を構成する複数のプログラムモジュールに対応する機能が端末装置３０によって実現される。図２は、アプリケーションプログラム５０を構成する複数のプログラムモジュールの一例を示すブロック図である。一実施形態におけるアプリケーションプログラム５０は、図示するように、端末装置３０上で実行可能なアプリケーションプログラムを用いたサーバ１０へのログインの履歴であって、この端末装置３０によってアクセス可能なストレージ３５等の記憶領域（所定の記憶領域）に記憶されているログイン履歴を参照し、このログイン履歴に含まれるログインに用いられた他のアプリケーションプログラ
40
50

ム 5 0 (第 2 のプログラム) に対してサーバ 1 0 へのログインに用いる認証トークン (認証用情報) を要求する認証用情報要求モジュール 5 1 と、この他のアプリケーションプログラムから取得した認証トークンを用いてサーバ 1 0 に対してログインを要求するログイン要求モジュール 5 2 と、サーバ 1 0 へのログインに応じてこのサーバ 1 0 から認証トークンを取得し、この取得した認証トークンをアプリケーションプログラム 5 0 によって管理され端末装置 3 0 によってアクセス可能なアプリケーションプログラム 5 0 用記憶領域に記憶させる認証用情報記憶モジュール 5 3 と、サーバ 1 0 へのログインに応じてアプリケーションプログラム 5 0 を用いたサーバ 1 0 へのログインを上記したログイン履歴に記録するログイン履歴記録モジュール 5 4 と、他のアプリケーションプログラム 5 0 (第 3 のプログラム) からの要求に応答し、上記したアプリケーションプログラム 5 0 用記憶領域に記憶されている認証トークンをこの他のアプリケーションプログラムに対して提供する認証用情報提供モジュール 5 5 と、を含む複数のプログラムモジュールによって構成される。上記したように、一実施形態におけるアプリケーションプログラム 5 0 を C P U 3 1 に実行させることによって、一実施形態における端末装置 3 0 は、アプリケーションプログラム 5 0 を構成する各プログラムモジュールの機能に対応する手段又はユニットとして機能し、例えば、サーバ 1 0 に対してログインを要求するログイン要求装置として機能する。ここで、上記したプログラムモジュール 5 1 - 5 5 は、主に、サーバ 1 0 に対してログインを要求する機能に関連するプログラムモジュールであり、アプリケーションプログラム 5 0 を構成する複数のプログラムモジュールは、プログラムモジュール 5 1 - 5 5 以外の他の機能に対応するプログラムモジュールを含み得る。例えば、アプリケーションプログラム 5 0 は、サーバ 1 0 が提供する様々なサービスのうち、このアプリケーションプログラム 5 0 を用いて利用するサービスに対応する機能 (例えば、特定のゲームをプレイするための機能) に対応する他のプログラムモジュールを含み得る。なお、プログラムモジュール 5 1 - 5 5 を備えたアドオンソフトウェア (S D K 等) をアプリケーションプログラムの開発者に公開することにより、開発者によって提供される様々なアプリケーションプログラムを、一実施形態におけるアプリケーションプログラム 5 0 として機能させることができる。

【 0 0 2 9 】

図 3 は、一実施形態における端末装置 3 0 のストレージ 3 5 等の記憶領域に記憶されるログイン履歴によって管理される情報の具体例を示す図である。ログイン履歴は、一実施形態では、図示するように、ログインが行われた日時を示すログイン日時と、このログインに用いられたアプリケーションプログラムを特定可能なアプリケーション特定情報 (例えば、アプリケーション名又はパッケージ名等) との組合せによって 1 つのログインに関する情報を構成し、例えば、最新の所定数 (例えば、1 つ又は 5 つ等) のログインに関する情報を管理する。ログイン履歴が記憶される記憶領域は、例えば、端末装置 3 0 に着脱可能な S D メモリカードに内蔵されるフラッシュメモリ等とすることができる。ここで、ログイン履歴は、ログインに用いる認証トークン等の情報と比較して機密性が高い情報ではないから、暗号化処理がなされていない非セキュアな領域である S D メモリカード等に記憶することができる。後述するように、このログイン履歴は、一実施形態におけるアプリケーションプログラム 5 0 のログイン履歴記録モジュール 5 4 の機能によって記録される情報であり、端末装置 3 0 にインストールされているアプリケーションプログラム 5 0 以外の他のアプリケーションプログラムを用いたログインに関する情報は含まれない。

【 0 0 3 0 】

次に、こうして構成された一実施形態におけるアプリケーションプログラム 5 0 を実行することによって端末装置 3 0 において実現される動作について説明する。図 4 は、一実施形態における端末装置 3 0 によって実行されるログイン処理の一例を示すフロー図である。このログイン処理は、一実施形態におけるアプリケーションプログラム 5 0 が起動されたときに実行される。以下、説明の都合上、ログイン処理の実行の契機として起動されたアプリケーションプログラム 5 0 をアプリケーションプログラム 5 0 - 1 (第 1 のプログラム) と呼ぶ。ログイン処理では、まず、図示するように、上記したログイン履歴を参

10

20

30

40

50

照して最新のログインを特定する（ステップ S 1 0 0）。この処理は、認証用情報要求モジュール 5 1 の機能に対応する処理であり、具体的には、ストレージ 3 5 等の記憶領域に記憶されているログイン履歴を参照し、このログイン履歴に含まれるログインの中から最新のログイン（ログイン日時が最も新しいログイン）を特定する処理である。

【 0 0 3 1 】

そして、特定した最新のログインに用いられたアプリケーションプログラム 5 0 がアンインストールされているか否かを判定し（ステップ S 1 0 5）、アンインストールされている場合には、再度ログイン履歴を参照し、次に新しいログインを特定する。この処理は、認証用情報要求モジュール 5 1 の機能に対応する処理であり、具体的には、オペレーティングシステム等によって管理されているインストールされているアプリケーションプログラムに関する情報に基づいて、ステップ S 1 0 0 で特定したログインに用いられたアプリケーションプログラムがアンインストールされているか否かを判定する処理である。このように、一実施形態では、ログイン履歴に含まれる複数のログインの中から、ログインに用いられたアプリケーションプログラムがアンインストールされていないログインのうちログイン日時が最も新しいログインを特定する。

【 0 0 3 2 】

続いて、アプリケーションプログラム 5 0 - 1 の発行者と、特定したログインに用いられたアプリケーションプログラム 5 0 の発行者とが対応するか否かを判定し（ステップ S 1 1 0）、対応しない場合には、所定のエラー処理を行って、このログイン処理を終了する。この処理は、認証用情報要求モジュール 5 1 の機能に対応する処理であり、具体的には、例えば、アプリケーションプログラム 5 0 - 1 のデジタル署名と、特定したログインに用いられたアプリケーションプログラム 5 0 のデジタル署名とを比較し、デジタル署名によって特定される発行者が同一である場合には発行者が対応すると判定し、同一でない場合には発行者が対応しないと判定する処理である。こうしたアプリケーションプログラムのデジタル署名を比較する機能は、端末装置 3 0 のオペレーティングシステムに組み込まれ得る。

【 0 0 3 3 】

そして、アプリケーションプログラム 5 0 - 1 の発行者と、特定したログインに用いられたアプリケーションプログラム 5 0 の発行者とが対応する場合には、このアプリケーションプログラム 5 0 に対して認証トークンを要求する（ステップ S 1 2 0）。以下、説明の都合上、認証トークンを要求された（認証トークンの要求先となる）アプリケーションプログラム 5 0 をアプリケーションプログラム 5 0 - 2（第 2 のプログラム）と呼ぶ。この処理は、認証用情報要求モジュール 5 1 の機能に対応する処理である。ここで、認証トークンとは、端末装置 3 0 がサーバ 1 0 に対してログインしたときに、次のログインにおいてユーザ ID 及びパスワード等を入力することなくログインできるようにするためにサーバ 1 0 から発行される認証用情報である。

【 0 0 3 4 】

認証トークンを要求されたアプリケーションプログラム 5 0 - 2 は、端末装置 3 0 のアプリケーションプログラム 5 0 - 2 用記憶領域に記憶されている認証トークンをアプリケーションプログラム 5 0 - 1 に提供する（ステップ S 1 2 5）。この処理は、アプリケーションプログラム 5 0 - 2 の認証用情報提供モジュール 5 5 の機能に対応する処理である。ここで、アプリケーションプログラム 5 0 - 2 用記憶領域に記憶されている認証トークンは、アプリケーションプログラム 5 0 - 2 の実行を契機とするログイン処理が実行されたときに、サーバ 1 0 に対するログインに応じてサーバ 1 0 から取得して記憶されたものである。認証トークンをサーバ 1 0 から取得して記憶する動作については後述する。こうしたアプリケーションプログラム 5 0 - 1 及び 5 0 - 2 間の通信は、例えば、オペレーティングシステムが有するアプリケーションプログラム間の通信を制御するプログラム間通信制御機能（例えば、オペレーティングシステム「Android」における「Binder」等）を用いて、バックグラウンドでの処理として実現することができる。こうしたプログラム間通信（プロセス間通信（IPC））に関する処理は、当業者にとって一般的

10

20

30

40

50

な処理であるから、これ以上の詳細な説明は省略する。

【 0 0 3 5 】

そして、アプリケーションプログラム 5 0 - 1 がアプリケーションプログラム 5 0 - 2 から認証トークンを取得すると、次に、取得した認証トークンを用いてサーバ 1 0 に対してログインを要求する（ステップ S 1 3 0）。この処理は、ログイン要求モジュール 5 2 の機能に対応する処理であり、具体的には、取得した認証トークンをサーバ 1 0 に対して送信する処理である。認証トークンを受信したサーバ 1 0 では、認証トークンの内容に基づいてログインの許否を判定する。例えば、受信した認証トークンの有効期間が切れていたり、又は、この認証トークンが発行された以降にパスワードが変更されている場合には、無効な認証トークンと判断され、ログインを拒否すると判定される。こうした認証トークンを用いたログインの許否の判定（ログイン認証）に関する処理は、当業者にとって一般的な処理であるから、これ以上の詳細な説明は省略する。

10

【 0 0 3 6 】

そして、サーバ 1 0 によってログインが許可されると、サーバ 1 0 が認証トークンを発行し、端末装置 3 0 では、認証トークンをサーバ 1 0 から取得すると共に取得した認証トークンをアプリケーションプログラム 5 0 - 1 用記憶領域に記憶する（ステップ S 1 4 0）。この処理は、認証用情報記憶モジュール 5 3 の機能に対応する処理である。一実施形態において、アプリケーションプログラム 5 0 - 1 用記憶領域は、ストレージ 3 5 内の任意の領域に構成されるアプリケーションプログラム 5 0 - 1 によって管理される領域である。より具体的には、このアプリケーションプログラム 5 0 - 1 用記憶領域に記憶されている情報は、アプリケーションプログラム 5 0 - 1 を介したアクセスのみが許容され、他のアプリケーションプログラム 5 0 及び一実施形態におけるアプリケーションプログラム 5 0 以外の他のアプリケーションプログラムからのアクセスは許容されない。

20

【 0 0 3 7 】

続いて、ログイン履歴を更新し（ステップ S 1 5 0）、このログイン処理を終了する。この処理は、ログイン履歴記録モジュール 5 4 の機能に対応する処理であり、具体的には、アプリケーションプログラム 5 0 - 1 を用いたログインとして、ログイン日時及びアプリケーションプログラム 5 0 - 1 のアプリケーション特定情報（アプリケーション名又はパッケージ名等）をログイン履歴に追加する処理である。なお、一実施形態では、ログイン履歴は、最新の所定数のログインに関する情報を管理するから、新たなログインに関する情報の追加に伴って、最も古いログインに関する情報はログイン履歴から削除される。なお、ログイン処理を終了すると、アプリケーションプログラム 5 0 - 1 に対応するサービスの利用を開始することができる（例えば、対応するサービスを利用するための初期画面が端末装置 3 0 に表示される）。

30

【 0 0 3 8 】

ここで、アプリケーションプログラム 5 0 - 1 の起動を契機とするログイン処理を終了した後に、他のアプリケーションプログラム 5 0（第 3 のアプリケーションプログラム。以下、説明の都合上、アプリケーションプログラム 5 0 - 3 と呼ぶ）の起動を契機として新たにログイン処理が実行された場合を考える。この場合、ステップ S 1 0 0 においてアプリケーションプログラム 5 0 - 1 を用いたログインが最新のログインとして特定され、アプリケーションプログラム 5 0 - 3 からアプリケーションプログラム 5 0 - 1 に対して認証トークンが要求される（ステップ S 1 2 0）。認証トークンを要求されたアプリケーションプログラム 5 0 - 1 は、自身が管理するアプリケーションプログラム 5 0 - 1 用記憶領域に記憶されている認証トークンを要求元であるアプリケーションプログラム 5 0 - 3 に提供する（ステップ S 1 2 5）。このように、一実施形態では、サーバ 1 0 に対するログインに応じてログイン履歴が更新され、このログイン履歴に基づいて、最新のログインに用いられたアプリケーションプログラム 5 0 から最新の認証トークンを取得し、取得した最新の認証トークンを用いたログインの要求を、繰り返し行うことができる。

40

【 0 0 3 9 】

ここで、上述したログイン処理において、アプリケーションプログラム 5 0 - 1 が既に

50

認証トークンを保有している（自身のアプリケーションプログラム50-1用記憶領域に認証トークンが記憶されている）場合には、ステップS100-S125の処理をスキップし、既に保有する認証トークンを用いてサーバ10に対してログインを要求するようにしても良い。また、既に保有する認証トークンを用いてログインを要求した後に、既に保有する認証トークンが無効であることを検出した場合（例えば、認証トークンの有効期間が切れ、又は、パスワードが変更されることによって、認証トークンが無効であることをサーバ10から端末装置30に対して通知された場合等）には、ステップS100-S125の処理を実行し、他のアプリケーションプログラム50から認証トークンを取得するようにしても良い。また、ログイン処理のステップS100-S105において、ログイン履歴に含まれる所定数のログインに用いられたアプリケーションプログラム50の全てがアンインストールされている場合には、認証トークンを用いたログインではない他のログイン（例えば、ユーザID及びパスワードを入力する通常のログイン等）をサーバ10に対して要求するようにしても良い。

10

【0040】

以上説明した一実施形態におけるアプリケーションプログラム50では、ログイン履歴を参照し、このログイン履歴に含まれるログインに用いられた他のアプリケーションプログラム50（第2のプログラム）に対してサーバ10へのログインに用いる認証トークン（認証用情報）を要求し、この他のアプリケーションプログラム50から取得した認証トークンを用いてサーバ10に対してログインを要求するように、端末装置30を機能させる。従って、ログイン履歴に基づいて他のアプリケーションプログラム50から取得した認証トークンを用いてログインすることができるから、非セキュアな記憶領域に認証トークンを記憶して複数のアプリケーションプログラム間で共有する場合と比較して、セキュリティが確保された仕組みとすることができる。また、機密性が高い情報を管理するための特別な仕組みが必要とならないから、より簡易な仕組みで複数のアプリケーションプログラム間での認証トークンの共有を実現することができる。即ち、ログインに必要な情報をセキュリティを確保しつつ複数のアプリケーションプログラム間で共有するより簡易な仕組みを提供することができる。

20

【0041】

また、一実施形態におけるアプリケーションプログラム50では、認証トークンの要求先であるアプリケーションプログラム50の発行者が、認証トークンの要求元であるアプリケーションプログラム50の発行者に対応しない場合には、認証トークンの要求、又は、認証トークンの提供が中止されるように、端末装置30を機能させるから、より一層セキュリティが確保された仕組みとすることができる。

30

【0042】

また、一実施形態におけるアプリケーションプログラム50では、サーバ10から取得した認証トークンをアプリケーションプログラム50によって管理されるアプリケーションプログラム50用記憶領域に記憶させるように、端末装置30を機能させるから、より一層セキュリティが確保された仕組みとすることができる。

【0043】

また、一実施形態におけるアプリケーションプログラム50では、ログイン履歴に含まれる複数のログインの中からログインに用いられたアプリケーションプログラム50がアンインストールされていないログインのうちログイン日時が最も新しいログインを特定し（即ち、ログイン日時が新しいほど優先される傾向でログインを特定し）、この特定したログインに用いられたアプリケーションプログラム50を認証トークンの要求先とするから、取得した認証トークンが、有効期間が切れていたり、又は、パスワード変更等によって、無効な認証トークンである可能性を低減することができる。

40

【0044】

本明細書で説明された処理及び手順は、実施形態中で明示的に説明されたもの以外にも、ソフトウェア、ハードウェアまたはこれらの任意の組み合わせによって実現される。より具体的には、本明細書で説明される処理及び手順は、集積回路、揮発性メモリ、不揮発

50

性メモリ、磁気ディスク、光ストレージ等の媒体に、当該処理に相当するロジックを実装することによって実現される。また、本明細書で説明される処理及び手順は、それらの処理・手順をコンピュータプログラムとして実装し、各種のコンピュータに実行させることが可能である。

【 0 0 4 5 】

本明細書中で説明される処理及び手順が単一の装置、ソフトウェア、コンポーネント、モジュールによって実行される旨が説明されたとしても、そのような処理または手順は複数の装置、複数のソフトウェア、複数のコンポーネント、及び／又は複数のモジュールによって実行され得る。また、本明細書中で説明されるデータ、テーブル、又はデータベースが単一のメモリに格納される旨説明されたとしても、そのようなデータ、テーブル、又はデータベースは、単一の装置に備えられた複数のメモリまたは複数の装置に分散して配置された複数のメモリに分散して格納され得る。さらに、本明細書において説明されるソフトウェアおよびハードウェアの要素は、それらをより少ない構成要素に統合して、またはより多い構成要素に分解することによって実現することも可能である。

10

【 0 0 4 6 】

本明細書において、発明の構成要素が単数もしくは複数のいずれか一方として説明された場合、又は、単数もしくは複数のいずれとも限定せずに説明された場合であっても、文脈上別に解すべき場合を除き、当該構成要素は単数又は複数のいずれであってもよい。

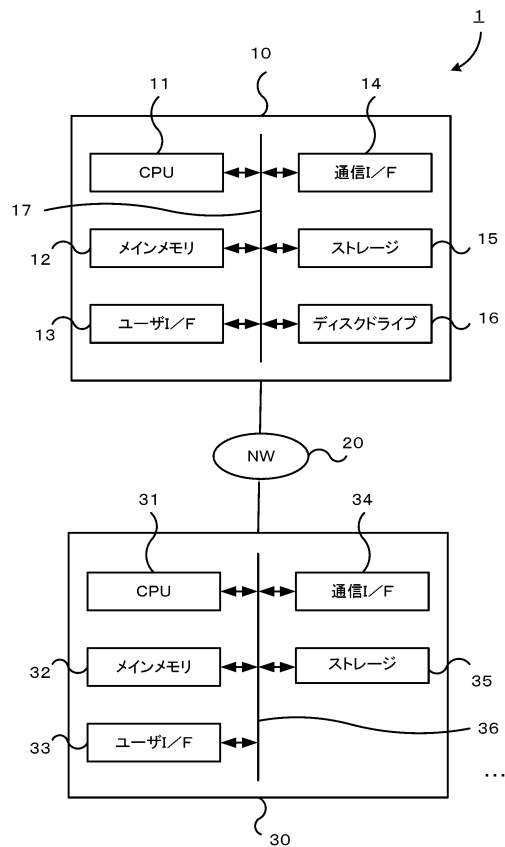
【 符号の説明 】

【 0 0 4 7 】

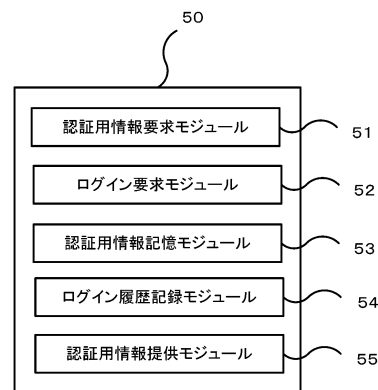
20

- 1 システム
- 1 0 サーバ
- 2 0 通信網
- 3 0 端末装置
- 5 1 認証用情報要求モジュール
- 5 2 ログイン要求モジュール
- 5 3 認証用情報記憶モジュール
- 5 4 ログイン履歴記録モジュール
- 5 5 認証用情報提供モジュール

【図 1】



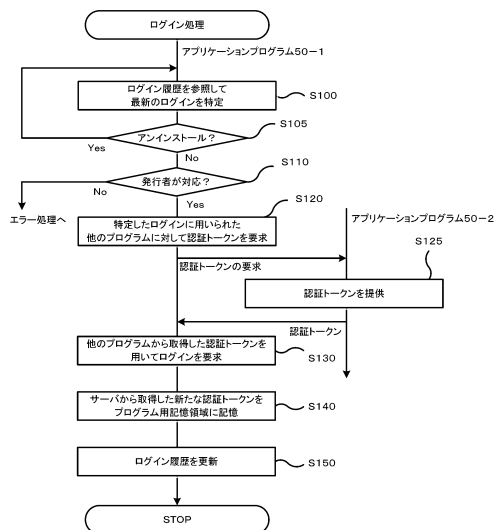
【図 2】



【図 3】

2013/10/12 19:25:01 co.jp.app1
2013/10/12 11:55:25 co.jp.app6
2013/10/12 01:10:28 com.app2
2013/10/11 23:12:31 co.us.app9
2013/10/11 20:05:31 com.app3

【図 4】



フロントページの続き

(72)発明者 平井 貴志

東京都渋谷区渋谷二丁目21番1号 株式会社ディー・エヌ・エー内

審査官 行田 悦資

(56)参考文献 特開2013-105467(JP,A)

米国特許出願公開第2008/0046983(US,A1)

特開2006-221284(JP,A)

特開2003-316743(JP,A)

特開2010-140351(JP,A)

米国特許出願公開第2013/0086669(US,A1)

特開2002-334055(JP,A)

(58)調査した分野(Int.Cl., DB名)

G06F 21/31