(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5452374号
(P5452374)
(45)発行日　平成26年3月26日(2014.3.26)　(24)登録日　平成26年1月10日(2014.1.10)

(51)Int.Cl.　F I
G06F 21/31 (2013.01)　G06F 21/20 131A

請求項の数 7 (全 18 頁)

(21)出願番号　特願2010-126489(P2010-126489)
(22)出願日　平成22年6月2日(2010.6.2)
(65)公開番号　特開2011-253342(P2011-253342A)
(43)公開日　平成23年12月15日(2011.12.15)
審査請求日　平成24年11月19日(2012.11.19)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100151220
弁理士　八巻　満隆
(72)発明者　白木　宏明
東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　平井　誠

最終頁に続く

(54)【発明の名称】認証装置、認証方法及び認証プログラム

(57)【特許請求の範囲】
【請求項１】
第１認証方式でユーザに対して認証処理を処理装置により実行する第１認証部と、
前記第１認証部が実行した認証処理が成功した場合、複数の第２認証方式から前記ユーザの属性に応じた第２認証方式を処理装置により選択する認証方式選択部と、
前記認証方式選択部が選択した第２認証方式で、前記ユーザに対して認証処理を処理装置により実行する第２認証部と、
前記第１認証部が実行した認証処理が成功した場合、前記ユーザの属性に応じて、処理装置により前記ユーザに対して所定のポイントを設定するとともに、前記第２認証部が実行した認証処理が成功した場合、前記第２認証部が実行した認証処理がどの第２認証方式であったかに応じて、処理装置により前記ユーザに対して所定のポイントを設定するポイント設定部と、
前記ポイント設定部が設定したポイントに応じて、処理装置により所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定するアクセス制御部と
を備えることを特徴とする認証装置。
【請求項２】
第１認証方式でユーザに対して認証処理を処理装置により実行する第１認証部と、
前記第１認証部が実行した認証処理が成功した場合、複数の第２認証方式から前記ユーザの属性に応じた第２認証方式を処理装置により選択する認証方式選択部と、
前記認証方式選択部が選択した第２認証方式で、前記ユーザに対して認証処理を処理装

置により実行する第２認証部と、
前記第２認証部が実行した認証処理が成功した場合、前記第２認証部が実行した認証処理がどの第２認証方式であったかに応じて、処理装置により前記ユーザに対して所定のポイントを設定するポイント設定部と、
前記ポイント設定部が設定したポイントに応じて、処理装置により所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定するアクセス制御部と
を備え、
前記ポイント設定部は、前記第２認証部が認証処理を実行してから経過した時間に応じて、設定したポイントを徐々に減らし、
前記アクセス制御部は、前記ユーザが再び前記所定の情報へアクセスする場合、その時点で設定されたポイントに応じて、前記所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定する
ことを特徴とする認証装置。
【請求項３】
前記認証方式選択部は、前記ユーザが再び前記所定の情報へアクセスする場合において、アクセスしようとする情報へのアクセスが前記アクセス制御部によって許可されなかった場合、その情報へのアクセスが許可されるために不足しているポイント数に応じて、複数の第２認証方式から第２認証方式を選択し、
前記第２認証部は、前記認証方式選択部が不足しているポイント数に応じて選択した第２認証方式で、前記ユーザに対して再び認証処理を実行し、
前記ポイント設定部は、前記第２認証部が再び実行した認証処理が成功した場合、前記第２認証部が実行した認証処理がどの第２認証方式であったかに応じて、前記ユーザに対して所定のポイントを加算し、
前記アクセス制御部は、前記ポイント設定部が加算した後のポイントに応じて、前記所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定する
ことを特徴とする請求項２に記載の認証装置。
【請求項４】
処理装置が、第１認証方式でユーザに対して認証処理を実行する第１認証ステップと、
処理装置が、前記第１認証ステップで実行した認証処理が成功した場合、複数の第２認証方式から前記ユーザの属性に応じた第２認証方式を選択する認証方式選択ステップと、
処理装置が、前記認証方式選択ステップで選択した第２認証方式で、前記ユーザに対して認証処理を実行する第２認証ステップと、
処理装置が、前記第１認証ステップで実行した認証処理が成功した場合、前記ユーザの属性に応じて、前記ユーザに対して所定のポイントを設定するとともに、前記第２認証ステップで実行した認証処理が成功した場合、前記第２認証ステップで実行した認証処理がどの第２認証方式であったかに応じて、前記ユーザに対して所定のポイントを設定するポイント設定ステップと、
処理装置が、前記ポイント設定ステップで設定したポイントに応じて、所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定するアクセス制御ステップと
を備えることを特徴とする認証方法。
【請求項５】
処理装置が、第１認証方式でユーザに対して認証処理を実行する第１認証ステップと、
処理装置が、前記第１認証ステップで実行した認証処理が成功した場合、複数の第２認証方式から前記ユーザの属性に応じた第２認証方式を選択する認証方式選択ステップと、
処理装置が、前記認証方式選択ステップで選択した第２認証方式で、前記ユーザに対して認証処理を実行する第２認証ステップと、
処理装置が、前記第２認証ステップで実行した認証処理が成功した場合、前記第２認証ステップで実行した認証処理がどの第２認証方式であったかに応じて、前記ユーザに対して所定のポイントを設定するポイント設定ステップと、
処理装置が、前記ポイント設定ステップで設定したポイントに応じて、所定の情報のう

ちどの情報へのアクセスを前記ユーザに許可するかを決定するアクセス制御ステップと
を備え、
前記ポイント設定ステップでは、前記第２認証ステップで認証処理を実行してから経過した時間に応じて、設定したポイントを徐々に減らし、
前記アクセス制御ステップでは、前記ユーザが再び前記所定の情報へアクセスする場合、その時点で設定されたポイントに応じて、前記所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定する
を備えることを特徴とする認証方法。
【請求項６】
第１認証方式でユーザに対して認証処理を実行する第１認証処理と、
前記第１認証処理で実行した認証処理が成功した場合、複数の第２認証方式から前記ユーザの属性に応じた第２認証方式を選択する認証方式選択処理と、
前記認証方式選択処理で選択した第２認証方式で、前記ユーザに対して認証処理を実行する第２認証処理と、
前記第１認証処理で実行した認証処理が成功した場合、前記ユーザの属性に応じて、前記ユーザに対して所定のポイントを設定するとともに、前記第２認証処理で実行した認証処理が成功した場合、前記第２認証処理で実行した認証処理がどの第２認証方式であったかに応じて、前記ユーザに対して所定のポイントを設定するポイント設定処理と、
前記ポイント設定処理で設定したポイントに応じて、所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定するアクセス制御処理と
をコンピュータに実行させることを特徴とする認証プログラム。
【請求項７】
第１認証方式でユーザに対して認証処理を実行する第１認証処理と、
前記第１認証処理で実行した認証処理が成功した場合、複数の第２認証方式から前記ユーザの属性に応じた第２認証方式を選択する認証方式選択処理と、
前記認証方式選択処理で選択した第２認証方式で、前記ユーザに対して認証処理を実行する第２認証処理と、
前記第２認証処理で実行した認証処理が成功した場合、前記第２認証処理で実行した認証処理がどの第２認証方式であったかに応じて、前記ユーザに対して所定のポイントを設定するポイント設定処理と、
前記ポイント設定処理で設定したポイントに応じて、所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定するアクセス制御処理と
をコンピュータに実行させ、
前記ポイント設定処理では、前記第２認証処理で認証処理を実行してから経過した時間に応じて、設定したポイントを徐々に減らし、
前記アクセス制御処理では、前記ユーザが再び前記所定の情報へアクセスする場合、その時点で設定されたポイントに応じて、前記所定の情報のうちどの情報へのアクセスを前記ユーザに許可するかを決定する
ことを特徴とする認証プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
この発明は、２種類以上の認証方式で認証処理を行う二要素認証方式に関する。
【背景技術】
【０００２】
二要素認証方式を用いた二要素認証システムとしては、例えば、パスワード認証と指紋認証とを組み合わせたもの等がある。また、銀行のＡＴＭ等で利用されている、キャッシュカードを有しているか否かによる認証とパスワード認証とを組み合わせたものも二要素認証システムである。
いずれの認証方式を用いたものであっても、従来の二要素認証システムは、全てのユー

ザに対して同一の認証方式を２つ以上組み合わせて用いている。したがって、全てのユーザが、そのシステムで用いられる認証方式を実行可能であることが必要である。

【０００３】

なお、特許文献１には、使用する回線を認証の１方式として扱うことについての記載がある。特許文献１では、使用する回線による認証と、パスワード認証のような低セキュリティの認証とを組み合わせて、高いセキュリティの認証方式を実現しようとしている。

また、特許文献２には、認証方式毎にレベルを割り当てておき、実行した認証方式の組み合わせにより、一定のレベルを達成すれば認証成立とすることについての記載がある。

【先行技術文献】

【特許文献】

【０００４】

【特許文献１】特開２００９－０４３０４２号公報

【特許文献２】特開２００３－１３２０２３号公報

【発明の概要】

【発明が解決しようとする課題】

【０００５】

上述したように、従来の二要素認証システムでは、全てのユーザに対して認証方式の組み合わせが固定的である。

この発明は、高いセキュリティを持ちつつ、柔軟に設計可能な二要素認証方式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】

【０００６】

この発明に係る認証装置は、

第１認証方式でユーザに対して認証処理を処理装置により実行する第１認証部と、

前記第１認証部が実行した認証処理が成功した場合、複数の第２認証方式から前記ユーザの属性に応じた第２認証方式を処理装置により選択する認証方式選択部と、

前記認証方式選択部が選択した第２認証方式で、前記ユーザに対して認証処理を処理装置により実行する第２認証部と、

前記第２認証部が実行した認証処理が成功した場合、処理装置により所定の情報へのアクセスを前記ユーザに許可するアクセス制御部と

を備えることを特徴とする。

【発明の効果】

【０００７】

この発明に係る認証装置は、ユーザの属性に応じて異なる認証方式を用いる。したがって、例えば、社員等の信頼度の高いユーザには、セキュリティレベルの低い認証方式を用い、外部の業者等の信頼度の低いユーザには、セキュリティレベルの高い認証方式を用いる等とすることができる。これにより、高いセキュリティを持ちつつ、柔軟に設計が可能である。

【図面の簡単な説明】

【０００８】

【図１】実施の形態１に係る認証システム１の構成図。

【図２】実施の形態１に係るユーザ情報テーブル１５１を示す図。

【図３】実施の形態１に係る認証方式テーブル１５２を示す図。

【図４】実施の形態１に係る認証ポリシーテーブル１５３を示す図。

【図５】実施の形態１に係るアクセス制御定義テーブル１５４を示す図。

【図６】実施の形態１に係るセッション管理テーブル１５５を示す図。

【図７】実施の形態１に係る認証サーバ１００による認証処理の流れを示すフローチャート。

【図８】実施の形態１に係る認証サーバ１００による認可処理の流れを示すフローチャート。

【図９】実施の形態２に係る認証システム１の構成図。
【図１０】実施の形態２に係る認証方式テーブル１５２を示す図。
【図１１】実施の形態２に係るアクセス制御定義テーブル１５４を示す図。
【図１２】実施の形態２に係るセッション管理テーブル１５５を示す図。
【図１３】実施の形態２に係る認証サーバ１００による認証処理の流れを示すフローチャート。
【図１４】実施の形態２に係る認証サーバ１００による認可処理の流れを示すフローチャート。
【図１５】実施の形態３に係る認証システム１の構成図。
【図１６】実施の形態３に係るアクセス制御定義テーブル１５４を示す図。
【図１７】実施の形態３に係る役職情報テーブル１５６を示す図。
【図１８】実施の形態３に係る認証サーバ１００による認証処理の流れを示すフローチャート。
【図１９】実施の形態４に係る認証サーバ１００による認可処理の流れを示すフローチャート。
【図２０】認証サーバ１００のハードウェア構成の一例を示す図。
【発明を実施するための形態】
【０００９】
以下、図に基づき、発明の実施の形態を説明する。
以下の説明において、処理装置は後述するＣＰＵ９１１等である。記憶装置は後述するＲＯＭ９１３、ＲＡＭ９１４、磁気ディスク９２０等の記憶装置である。入力装置はキーボード９０２、マウス９０３等である。つまり、処理装置、記憶装置、入力装置はハードウェアである。
【００１０】
実施の形態１.
図１は、実施の形態１に係る認証システム１の構成図である。
認証システム１は、複数のクライアント１０と、複数のＷｅｂアプリケーション２０（ここでは、ＷｅｂアプリケーションＡとＷｅｂアプリケーションＢ）と、認証サーバ１００（認証装置）とを備える。各クライアント１０と認証サーバ１００とはネットワークを介して接続されており、認証サーバ１００と各Ｗｅｂアプリケーション２０ともネットワークを介して接続されている。
認証サーバ１００は、認証処理を実行する装置である。各クライアント１０は、いずれかのＷｅｂアプリケーション２０へアクセスする場合、認証サーバ１００によって認証処理が実行される。認証サーバ１００によってアクセスが許可された場合に、クライアント１０はＷｅｂアプリケーション２０へアクセスすることができる。
【００１１】
認証サーバ１００は、セッション情報チェック部１１０、認証方式選択部１２０、認証部１３０、アクセス権限判定部１４０（アクセス制御部）、認証用リポジトリ１５０を備える。認証サーバ１００が備える各機能部の動作については、全体の処理の流れとともに後で説明する。
なお、認証部１３０は、処理装置により、複数の方式の認証処理を実行する。認証部１３０は、パスワード認証を実行するパスワード認証部１３１、背景配列の移動量に基づく認証を実行する背景移動認証部１３２、ワンタイムパスワードによる認証を実行するＯＴＰ認証部１３３、指紋認証を実行する指紋認証部１３４、公開鍵暗号を用いた認証を実行するＰＫＩ認証部１３５を備える。
また、認証用リポジトリ１５０は、各種情報を記憶した記憶装置である。認証用リポジトリ１５０は、ユーザ情報テーブル１５１、認証方式テーブル１５２、認証ポリシーテーブル１５３、アクセス制御定義テーブル１５４、セッション管理テーブル１５５を備える。
【００１２】

図２は、実施の形態１に係るユーザ情報テーブル１５１を示す図である。
ユーザ情報テーブル１５１は、ユーザ毎に、そのユーザの属性を示す属性情報が格納されるテーブルである。ユーザ情報テーブル１５１は、ユーザＩＤ、名前、部、課、役職、パスワード、証明書、指紋の項目を有する。
ユーザＩＤは、ユーザを識別可能なＩＤ（ＩＤｅｎｔｉｆｉｅｒ）が格納される。名前、部、課、役職は、そのユーザの名前、そのユーザが所属する部及び課、そのユーザの役職が格納される。パスワードには、予め設定されたパスワードが格納される。証明書には、ＰＫＩ認証部１３５が使用する証明書データが格納される。指紋には、そのユーザの指紋情報が格納される。

【００１３】

図３は、実施の形態１に係る認証方式テーブル１５２を示す図である。
認証方式テーブル１５２は、認証部１３０が実行する認証方式についての情報が格納されるテーブルである。認証方式テーブル１５２は、認証方式ＩＤ、認証方式の項目を有する。
認証方式ＩＤは、認証方式を識別可能なＩＤが格納される。認証方式は、その認証方式の名称が格納される。

【００１４】

図４は、実施の形態１に係る認証ポリシーテーブル１５３を示す図である。
認証ポリシーテーブル１５３は、認証ポリシーを示す情報が格納されるテーブルである。認証ポリシーテーブル１５３は、認証ポリシーＩＤ、条件、認証方式１、認証方式２の項目を有する。
認証ポリシーＩＤは、認証ポリシーを識別可能なＩＤが格納される。条件は、その認証ポリシーを適用する条件が格納される。ここでは、条件には、ユーザがどの役職であるかが設定されている。認証方式１は、第１段階の認証に用いられる認証方式（第１認証方式）のＩＤが格納される。認証方式２は、第２段階の認証に用いられる認証方式（第２認証方式）のＩＤが格納される。

【００１５】

図５は、実施の形態１に係るアクセス制御定義テーブル１５４を示す図である。
アクセス制御定義テーブル１５４は、各情報に対するアクセス条件が格納されるテーブルである。アクセス制御定義テーブル１５４は、ＵＲＬ（Ｕｎｉｆｏｒｍ　Ｒｅｓｏｕｒｃｅ　Ｌｏｃａｔｏｒ）、アクセス条件の項目を有する。
ＵＲＬは、ＷｅｂページのＵＲＬが格納される。アクセス条件は、ＵＲＬが示すＷｅｂページへのアクセスを許可するために満たす必要がある条件が格納される。ここでは、アクセス条件には、ユーザがどの役職であるかが設定されている。

【００１６】

図６は、実施の形態１に係るセッション管理テーブル１５５を示す図である。
セッション管理テーブル１５５は、セッション情報が格納されるテーブルである。セッション管理テーブル１５５は、セッションＩＤ、ユーザＩＤ、認証時刻、セッション期限の項目を有する。
セッションＩＤは、セッションを識別可能なＩＤが格納される。ユーザＩＤは、そのセッションが割り当てられたユーザのＩＤが格納される。認証時刻は、そのセッションが割り当てられたユーザが認証された日時が格納される。セッション期限は、そのセッションの有効期限が格納され、セッション期限を過ぎるとそのセッションは無効になる。なお、ここでは、セッションが有効である残り時間が格納され、残り時間が０となった時点で無効になる。

【００１７】

図７は、実施の形態１に係る認証サーバ１００による認証処理の流れを示すフローチャートである。
（Ｓ１０１）では、ユーザがあるクライアント１０からＷｅｂアプリケーション２０へ、認証サーバ１００経由のＵＲＬのＨＴＴＰ（ＨｙｐｅｒＴｅｘｔ　Ｔｒａｎｓｆｅｒ

Ｐｒｏｔｏｃｏｌ）リクエストを送信する。なお、クライアント１０がセッションＩＤを有している場合には、ＨＴＴＰリクエストとともに、セッションＩＤも送信される。

（Ｓ１０２）では、認証サーバ１００がＨＴＴＰリクエストを受信する。すると、セッション情報チェック部１１０が、ＨＴＴＰリクエストとともに送信されたセッションＩＤに基づき、セッション管理テーブル１５５をチェックして、セッションが有効であるか無効であるかを処理装置により判定する。これにより、ユーザについて既に認証済であるか否かを判定する。セッションが有効である場合（Ｓ１０２で済）、認証済であると判定し処理を認可処理へ進める。一方、セッションが無効である場合（Ｓ１０２で未）、認証済でないと判定し処理を（Ｓ１０３）へ進める。なお、セッションＩＤが送信されていない場合、セッションは無効であると判定される。

【００１８】

（Ｓ１０３）から（Ｓ１０７）までで、第１段階の認証処理が実行される。なお、ここでは、図４に示すように、認証ポリシーテーブル１５３の認証方式１には、いずれもパスワード認証を示す認証方式のＩＤが格納されており、第１段階の認証に用いられる認証方式はいずれもパスワード認証である。そこで、パスワード認証が実行される。なお、第１段階の認証処理を実行する機能部を第１認証部と呼ぶ。したがって、ここでは、パスワード認証部１３１が第１認証部である。

（Ｓ１０３）では、認証部１３０のパスワード認証部１３１が、パスワード認証用のログイン画面をクライアント１０の表示装置に表示させる。

（Ｓ１０４）では、ユーザが表示されたログイン画面に、ユーザＩＤとパスワードとを入力して、認証サーバ１００へ送信する。

（Ｓ１０５）では、パスワード認証部１３１が、ユーザ情報テーブル１５１に格納されている情報に基づき、送信されたユーザＩＤとパスワードとの組み合わせが正しいか否かを処理装置により判定する。正しくない場合、第１段階での認証処理は失敗となり（Ｓ１０５で失敗）、処理を（Ｓ１０６）へ進める。一方、正しい場合、第１段階での認証処理は成功となり（Ｓ１０５で成功）、処理を（Ｓ１０７）へ進める。

（Ｓ１０６）では、パスワード認証部１３１が第１段階での認証処理の失敗回数が所定回数以下であるか否かを処理装置により判定する。所定回数以下である場合（Ｓ１０６で所定回数以下）、処理を（Ｓ１０３）へ戻して再びユーザＩＤとパスワードとを入力させる。一方、所定回数より多い場合（Ｓ１０６で所定回数より多い）、処理を（Ｓ１１５）へ進め、認証エラー画面をクライアント１０の表示装置に表示させ、処理を終了する。

（Ｓ１０７）では、第１段階の認証処理が成功したため、パスワード認証部１３１が、セッション管理テーブル１５５に新たなセッションＩＤでレコードを作成して、ユーザＩＤに認証したユーザのＩＤを、認証時刻に第１段階の認証処理を実行した日時を、セッション期限に所定の時間を格納する。

【００１９】

（Ｓ１０８）では、認証方式選択部１２０が、ユーザ情報テーブル１５１の認証したユーザのレコードにおける役職に格納された情報（役職情報）を取得する。

（Ｓ１０９）では、認証方式選択部１２０が、処理装置により、（Ｓ１０８）で取得した役職情報で、認証ポリシーテーブル１５３の条件を検索して、該当するレコードの認証方式２に格納された情報を取得する。さらに、認証方式選択部１２０は、取得した情報で認証方式テーブル１５２を検索して、第２段階の認証処理に用いる認証方式を特定する。

【００２０】

（Ｓ１１０）から（Ｓ１１４）までで、第２段階の認証処理が実行される。なお、第２段階の認証処理を実行する機能部を第２認証部と呼ぶ。

（Ｓ１１０）では、（Ｓ１０９）で選択された認証方式による認証要求を、認証部１３０の対応する機能部（第２認証部）がクライアント１０へ送信する。

（Ｓ１１１）では、ユーザが、要求に応じた認証情報（ＰＫＩ認証ならば電子証明書、指紋認証ならば指紋情報、背景移動型認証ならば背景画像を動かして生成されるパスワード）を入力し、認証サーバ１００へ送信する。

（Ｓ１１２）では、第２認証部が送信された認証情報をチェックして、認証処理が成功か失敗かを処理装置により判定する。認証処理が失敗した場合（Ｓ１１２で失敗）、処理を（Ｓ１１３）へ進める。認証処理が成功した場合（Ｓ１１２で成功）、処理を（Ｓ１１４）へ進める。

（Ｓ１１３）では、第２認証部が、第２段階での認証処理の失敗回数が所定回数以下であるか否かを処理装置により判定する。所定回数以下である場合（Ｓ１１３で所定回数以下）、処理を（Ｓ１１０）へ戻して再び認証情報を入力させる。一方、所定回数より多い場合（Ｓ１１３で所定回数より多い）、処理を（Ｓ１１５）へ進め、認証エラー画面をクライアント１０の表示装置に表示させ、処理を終了する。

（Ｓ１１４）では、第２段階の認証処理が成功したため、第２認証部が、セッション管理テーブル１５５の（Ｓ１０７）で追加したレコードの認証時刻を、第２段階の認証処理を実行した日時に更新する。そして、処理を認可処理へ進める。

【００２１】

図８は、実施の形態１に係る認証サーバ１００による認可処理の流れを示すフローチャートである。

（Ｓ２０１）では、アクセス権限判定部１４０が、ユーザ情報テーブル１５１から認証処理で認証されたユーザの役職情報を取得する。

（Ｓ２０２）では、アクセス権限判定部１４０が、アクセス制御定義テーブル１５４において、（Ｓ１０１）で送信されたＨＴＴＰリクエストでアクセスを要求するＵＲＬのアクセス条件に格納された条件を、（Ｓ２０１）で取得した役職情報が満たすか否かを処理装置により判定する。満たしていない場合（Ｓ２０２でＮＧ）、アクセス権を有していないため、処理を（Ｓ２０３）へ進め、アクセスエラー画面をクライアント１０の表示装置に表示させ、処理を終了する。一方、満たしている場合（Ｓ２０２でＯＫ）、アクセス権を有しているため、処理を（Ｓ２０４）へ進める。

【００２２】

（Ｓ２０４）では、認証サーバ１００が、（Ｓ１０１）で送信されたＨＴＴＰリクエストをＷｅｂアプリケーション２０へ転送する。（Ｓ２０５）では、ＨＴＴＰリクエストを受信したＷｅｂアプリケーション２０が、ＨＴＴＰリクエストに応じた画面を処理装置により生成する。（Ｓ２０６）では、Ｗｅｂアプリケーション２０が、（Ｓ２０５）で生成した画面を結果画面として、認証サーバ１００へ送信する。（Ｓ２０７）では、認証サーバ１００が、受け取った結果画面をクライアント１０へ転送する。（Ｓ２０８）では、クライアント１０が結果画面を表示装置に表示する。これにより、処理が終了する。

【００２３】

以上のように、実施の形態１に係る認証サーバ１００は、ユーザの属性に応じて第２段階の認証方式を自動選択する。これにより、同じＷｅｂアプリケーション２０を操作する場合であっても、信頼できるユーザ（例えば社員やより上の役職）には低レベルの認証方式でもアクセス可能とするが、信頼の度合いの低いユーザにはより高レベルの認証方式を要求することができる。したがって、安全性を高めつつ、信頼できるユーザには利便性を向上させるという柔軟な設計が可能である。

【００２４】

なお、上記説明では、ユーザ情報テーブル１５１に各ユーザの認証情報（パスワード、証明書、指紋など）を格納しておくこととした。しかし、このテーブルを正規化して各認証情報を管理してもよい。

また、上記説明では、２つの認証方式を用いて認証する場合について説明した。しかし、図７の（Ｓ１１０）から（Ｓ１１４）までの処理を繰り返すことで、３つ以上の認証方式を用いて認証することも可能である。

【００２５】

実施の形態２．

実施の形態１では、要求された全て認証方式の認証処理に成功しなければアクセス権が与えられなかった。実施の形態２では、認証処理に成功した際にセキュリティポイントを

与え、与えられたセキュリティポイントに応じてアクセス権を与える方法について説明する。

なお、実施の形態２では、実施の形態１と異なる点のみ説明する。

【００２６】

図９は、実施の形態２に係る認証システム１の構成図である。

図９に示す認証システム１は、認証サーバ１００がポイント設定部１６０を備える点で、図１に示す認証システム１と異なる。

【００２７】

図１０は、実施の形態２に係る認証方式テーブル１５２を示す図である。

図１０に示す認証方式テーブル１５２は、セキュリティポイントの項目を有する点で、図３に示す認証方式テーブル１５２と異なる。セキュリティポイントは、その認証方式の認証処理で成功した場合に与えられるセキュリティポイントの値が格納される。

【００２８】

図１１は、実施の形態２に係るアクセス制御定義テーブル１５４を示す図である。

図１１に示すアクセス制御定義テーブル１５４は、図５に示すアクセス制御定義テーブル１５４と同一の構成である。但し、アクセス条件として、ユーザがどの役職であるか、又は、セキュリティポイントがいくつ以上であるかが設定されている点が異なる。

【００２９】

図１２は、実施の形態２に係るセッション管理テーブル１５５を示す図である。

図１２に示すセッション管理テーブル１５５は、セキュリティポイントの項目を有する点で、図６に示すセッション管理テーブル１５５と異なる。セキュリティポイントは、そのユーザに与えられたセキュリティポイントの値が格納される。

【００３０】

図１３は、実施の形態２に係る認証サーバ１００による認証処理の流れを示すフローチャートである。

（Ｓ３０１）から（Ｓ３０６）までは、図７に示す（Ｓ１０１）から（Ｓ１０６）までと同様である。

（Ｓ３０７）では、第１段階の認証処理が成功したため、（Ｓ１０７）と同様に、パスワード認証部１３１が、セッション管理テーブル１５５に新たなレコードに、ユーザＩＤ、認証時刻、セッション期限に情報を格納する。さらに、ポイント設定部１６０が、前記新たなレコードのセキュリティポイントに、認証方式テーブル１５２においてパスワード認証に割り当てられたセキュリティポイント（ここでは、“１”）を格納する。

【００３１】

（Ｓ３０８）から（Ｓ３１２）までは、図７に示す（Ｓ１０８）から（Ｓ１１２）までと同様である。

（Ｓ３１４）では、第２段階の認証処理が成功したため、（Ｓ１１４）と同様に、第２認証部が、セッション管理テーブル１５５の（Ｓ３０７）で追加したレコードの認証時刻を、第２段階の認証処理を実行した日時に更新する。さらに、ポイント設定部１６０が、認証方式テーブル１５２において、第２段階の認証処理として選択された認証方式に割り当てられたセキュリティポイントを、セッション管理テーブル１５５のそのレコードのセキュリティポイントに格納された値に加算する。例えば、第２段階の認証処理として選択された認証方式が指紋認証であった場合には、“５”をセキュリティポイントに格納された値“１”に加算した値“６”が、セキュリティポイントに格納される。

【００３２】

また、（Ｓ３１３）では、認証失敗回数が所定回数より多くなったとしても、処理を（Ｓ３１５）へ進めず、認可処理へ進める。

【００３３】

図１４は、実施の形態２に係る認証サーバ１００による認可処理の流れを示すフローチャートである。

（Ｓ４０１）では、アクセス権限判定部１４０が、ユーザ情報テーブル１５１から認証

処理で認証されたユーザの役職情報を取得するとともに、セッション管理テーブル１５５のセキュリティポイントから値を取得する。
（Ｓ４０２）では、アクセス条件に格納された条件を、（Ｓ４０１）で取得した役職情報、又は、セキュリティポイントの値が満たすか否かを判定する。
（Ｓ４０３）から（Ｓ４０８）までの処理は、図８に示す（Ｓ２０３）から（Ｓ２０８）までの処理と同様である。
【００３４】
以上のように、実施の形態２に係る認証サーバ１００は、ユーザの属性だけではなく、成功した認証方式によって付与されるセキュリティポイントによってアクセス権を与える。そのため、要求されたセキュリティレベルによってＷｅｂページを保護することも可能となる。
また、実施の形態２に係る認証サーバ１００は、第２段階の認証処理で失敗となっても、認可処理へ進め、セキュリティポイントに応じてアクセス権を与える。つまり、第２段階の認証処理で失敗となっても、一部のＷｅｂページへのアクセスは許可される。クライアント１０が一部の認証方式を実行する環境を有していない場合（例えば、パスワード認証はできるが、指紋認証、ＩＣカードによる認証はできない場合）も考えられる。このような場合であっても、パスワード認証だけでセキュリティレベルの低いＷｅｂページへのアクセスが許可される。
【００３５】
実施の形態３．
実施の形態２では、アクセス制御定義テーブル１５４のアクセス条件に、ユーザの役職と、セキュリティポイントとの両方を設定した。これにより、高い役職（例えば、部長）は、低レベルの認証方式で認証処理を実行して少ないセキュリティポイントだけが付与される場合であっても、セキュリティレベルの高いＷｅｂページへのアクセスを許可できる設定となっていた。実施の形態３では、ユーザの役職に応じてセキュリティポイントを付与することで、実施の形態２と同様のアクセス条件設定を、セキュリティポイントのみの設定で可能とする方法について説明する。
なお、実施の形態２では、実施の形態１と異なる点のみ説明する。
【００３６】
図１５は、実施の形態３に係る認証システム１の構成図である。
図１５に示す認証システム１は、認証サーバ１００の認証用リポジトリ１５０が役職情報テーブル１５６を備える点で、図９に示す認証システム１と異なる。
【００３７】
図１６は、実施の形態３に係るアクセス制御定義テーブル１５４を示す図である。
図１６に示すアクセス制御定義テーブル１５４は、図１１に示すアクセス制御定義テーブル１５４と同一の構成である。但し、アクセス条件として、セキュリティポイントがいくつ以上であるかのみが設定されている点が異なる。
【００３８】
図１７は、実施の形態３に係る役職情報テーブル１５６を示す図である。
役職情報テーブル１５６は、役職毎に付与されるセキュリティポイントが格納されるテーブルである。役職情報テーブル１５６は、役職、セキュリティポイントの項目を有する。
役職は、ユーザに割り振られる各役職が格納される。セキュリティポイントは、その役職に与えられるセキュリティポイントの値が格納される。
【００３９】
図１８は、実施の形態３に係る認証サーバ１００による認証処理の流れを示すフローチャートである。
（Ｓ５０１）から（Ｓ５０６）までは、図１３に示す（Ｓ３０１）から（Ｓ３０６）までと同様である。
（Ｓ５０７）では、認証方式選択部１２０が、ユーザ情報テーブル１５１の認証したユ

ーザのレコードにおける役職に格納された情報（役職情報）を取得する。
（Ｓ５０８）では、ポイント設定部１６０が、（Ｓ５０７）で取得した役職情報に割り当てられたセキュリティポイントを役職情報テーブル１５６から取得する。
（Ｓ５０９）では、（Ｓ３０７）と同様に、パスワード認証部１３１が、セッション管理テーブル１５５に新たなレコードに、ユーザＩＤ、認証時刻、セッション期限に情報を格納する。さらに、ポイント設定部１６０が、前記新たなレコードのセキュリティポイントに、（Ｓ５０８）で取得したセキュリティポイントと、認証方式テーブル１５２においてパスワード認証に割り当てられたセキュリティポイント（ここでは、“１”）とを合算した値を格納する。
（Ｓ５１０）から（Ｓ５１６）までの処理は、図１３に示す（Ｓ３０９）から（Ｓ３１５）までの処理と同様である。
【００４０】
実施の形態３に係る認可処理の流れは、図１４に示す実施の形態２に係る認可処理の流れと同様である。但し、図１４の（Ｓ４０１）では、役職情報を取得する必要はなく、（Ｓ４０２）では、セキュリティポイントがアクセス条件を満たすか否か判定すればよく、役職情報を用いる必要はない。
【００４１】
以上のように役職情報など設定値にレベルがあるものに対してセキュリティポイントを対応させることで、セキュリティポイントという１つの指標でセキュリティレベルを制御することが可能となる。したがって、アクセス条件の設定が単純になり、設定の誤りを防ぐことができる。
【００４２】
実施の形態４.
以上の実施の形態では、セッションの有効期限が切れた瞬間にセッションが無効となり、認証処理を一から実行し直す必要があった。実施の形態４では、認証処理が実行された後、時間の経過とともに、セッション管理テーブル１５５のセキュリティポイントに設定したセキュリティポイントを徐々に減らし、アクセスするＷｅｂページで要求するセキュリティポイントに対して不足が発生した時点で再度認証処理を実行する方法について説明する。
なお、実施の形態４では、実施の形態３と異なる部分のみ説明する。
【００４３】
図１９は、実施の形態４に係る認証サーバ１００による認可処理の流れを示すフローチャートである。
（Ｓ６０１）では、ポイント設定部１６０が、セッション管理テーブル１５５の認証時刻に格納された日時と、セキュリティポイントに格納された値とを取得する。
（Ｓ６０２）では、ポイント設定部１６０が、セキュリティポイントから取得した値と、認証時刻から取得した日時と、現在の日時とから、現在のセキュリティポイントの値を処理装置により計算する。つまり、ポイント設定部１６０は、認証処理が実行された日時から時間が経過することによるセキュリティポイントの減少を加味して、現在のセキュリティポイントの値を算出する。
（Ｓ６０３）では、アクセス条件に格納された条件を、（Ｓ６０２）で計算された、現在のセキュリティポイントの値が満たすか否かを判定する。
【００４４】
（Ｓ６０４）から（Ｓ６０８）までは、図１４の（Ｓ４０４）から（Ｓ４０８）までの処理と同様である。なお、（Ｓ６０３）では、実施の形態３と同様に、セキュリティポイントがアクセス条件を満たすか否か判定すればよく、役職情報を用いる必要はない。
【００４５】
（Ｓ６０９）では、認証方式選択部１２０が、認証方式テーブル１５２からセキュリティポイント不足分を満たす認証方式を処理装置により検索する。
（Ｓ６１０）では、（Ｓ６０９）で検索された認証方式による認証要求を、第２認証部

がクライアント１０へ送信する。
（Ｓ６１１）では、ユーザが、要求に応じた認証情報を入力し、認証サーバ１００へ送信する。
（Ｓ６１２）では、第２認証部が送信された認証情報をチェックして、認証処理が成功か失敗かを処理装置により判定する。認証処理が失敗した場合（Ｓ６１２で失敗）、処理を（Ｓ６１３）へ進める。認証処理が成功した場合（Ｓ６１２で成功）、処理を（Ｓ６１４）へ進める。
（Ｓ６１３）では、第２認証部が、ここでの認証処理の失敗回数が所定回数以下であるか否かを処理装置により判定する。所定回数以下である場合（Ｓ６１３で所定回数以下）、処理を（Ｓ６１０）へ戻して再び認証情報を入力させる。一方、所定回数より多い場合（Ｓ６１３で所定回数より多い）、処理を（Ｓ６１５）へ進め、アクセスエラー画面をクライアント１０の表示装置に表示させ、処理を終了する。
（Ｓ６１４）では、認証処理が成功したため、認証部１３０の対応する機能部が、セッション管理テーブル１５５のセッションＩＤを新しいＩＤに更新する。さらに、ポイント設定部１６０が、認証方式テーブル１５２において、第２段階の認証処理として選択された認証方式に割り当てられたセキュリティポイントを、セッション管理テーブル１５５のセキュリティポイントに格納された値に加算する。そして、処理を（Ｓ６０４）へ進め、Ｗｅｂアプリケーション２０へアクセスさせる。
【００４６】
なお、（Ｓ６０９）で複数の認証方式が検索された場合、ユーザにどの認証方式を用いるか選択させてもよいし、所定の方法により認証方式を選択してしまってもよい。
【００４７】
以上のように、実施の形態４に係る認証サーバ１００は、セッションの有効期限が切れた瞬間にすべての認証を一からやり直すのではなく、セキュリティポイントを時間経過とともに減らす。そして、アクセス先のセキュリティレベルから不足した分のみ再認証を行う。そのため、ユーザ利便性を高くすることができる。
また、同一のセッションを長期間利用可能とすると、なりすまし等の不正アクセスをされる危険性が高くなる。しかし、（Ｓ６１４）では、再認証された場合、セッションＩＤを更新しているため、不正アクセスされる危険性が高くなることを防止している。
【００４８】
次に、実施の形態における認証サーバ１００のハードウェア構成について説明する。
図２０は、認証サーバ１００のハードウェア構成の一例を示す図である。
図２０に示すように、認証サーバ１００は、プログラムを実行するＣＰＵ９１１（Ｃｅｎｔｒａｌ・Ｐｒｏｃｅｓｓｉｎｇ・Ｕｎｉｔ、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう）を備えている。ＣＰＵ９１１は、バス９１２を介してＲＯＭ９１３、ＲＡＭ９１４、ＬＣＤ９０１（Ｌｉｑｕｉｄ Ｃｒｙｓｔａｌ Ｄｉｓｐｌａｙ）、キーボード９０２（Ｋ／Ｂ）、通信ボード９１５、磁気ディスク装置９２０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９２０（固定ディスク装置）の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。磁気ディスク装置９２０は、所定の固定ディスクインタフェースを介して接続される。
【００４９】
ＲＯＭ９１３、磁気ディスク装置９２０は、不揮発性メモリの一例である。ＲＡＭ９１４は、揮発性メモリの一例である。ＲＯＭ９１３とＲＡＭ９１４と磁気ディスク装置９２０とは、記憶装置（メモリ）の一例である。また、キーボード９０２、通信ボード９１５は、入力装置の一例である。また、通信ボード９１５は、通信装置（ネットワークインタフェース）の一例である。さらに、ＬＣＤ９０１は、表示装置の一例である。
【００５０】
磁気ディスク装置９２０又はＲＯＭ９１３などには、オペレーティングシステム９２１（ＯＳ）、ウィンドウシステム９２２、プログラム群９２３、ファイル群９２４が記憶さ

れている。プログラム群９２３のプログラムは、ＣＰＵ９１１、オペレーティングシステム９２１、ウィンドウシステム９２２により実行される。

【００５１】

プログラム群９２３には、上記の説明において「セッション情報チェック部１１０」、「認証方式選択部１２０」、「認証部１３０」、「アクセス権限判定部１４０」等として説明した機能を実行するソフトウェアやプログラムやその他のプログラムが記憶されている。プログラムは、ＣＰＵ９１１により読み出され実行される。

ファイル群９２４には、上記の説明において「認証用リポジトリ１５０」に格納される情報やデータや信号値や変数値やパラメータが、「ファイル」や「データベース」の各項目として記憶される。「ファイル」や「データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９１１によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵ９１１の動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のＣＰＵ９１１の動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

【００５２】

また、上記の説明におけるフローチャートの矢印の部分は主としてデータや信号の入出力を示し、データや信号値は、ＲＡＭ９１４のメモリ、その他光ディスク等の記録媒体やＩＣチップに記録される。また、データや信号は、バス９１２や信号線やケーブルその他の伝送媒体や電波によりオンライン伝送される。

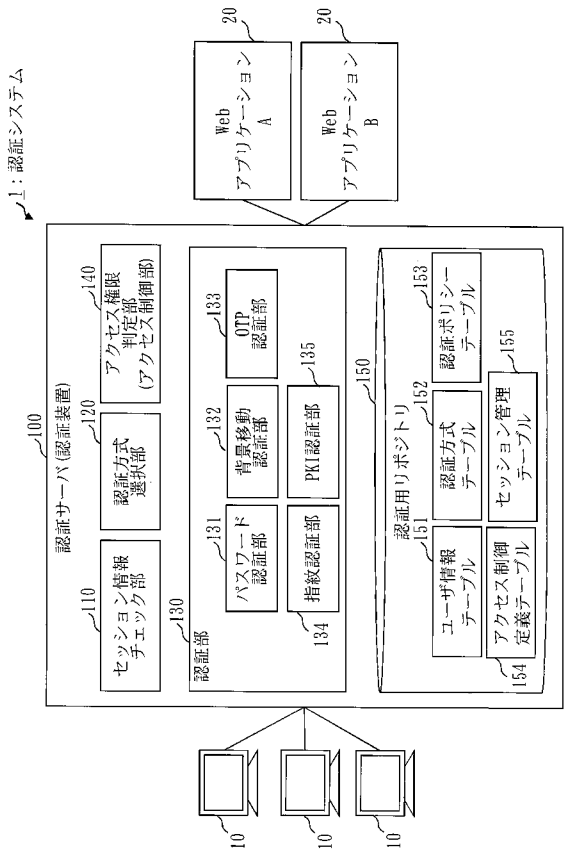
また、上記の説明において「～部」として説明するものは、「～回路」、「～装置」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。また、「～装置」として説明するものは、「～回路」、「～機器」、「～手段」、「～機能」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。さらに、「～処理」として説明するものは「～ステップ」であっても構わない。すなわち、「～部」として説明するものは、ＲＯＭ９１３に記憶されたファームウェアで実現されていても構わない。或いは、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、ＲＯＭ９１３等の記録媒体に記憶される。プログラムはＣＰＵ９１１により読み出され、ＣＰＵ９１１により実行される。すなわち、プログラムは、上記で述べた「～部」としてコンピュータ等を機能させるものである。あるいは、上記で述べた「～部」の手順や方法をコンピュータ等に実行させるものである。

【符号の説明】

【００５３】

１　認証システム、１０　クライアント、２０　Ｗｅｂアプリケーション、１００　認証サーバ、１１０　セッション情報チェック部、１２０　認証方式選択部、１３０　認証部、１３１　パスワード認証部、１３２　背景移動認証部、１３３　ＯＴＰ認証部、１３４　指紋認証部、１３５　ＰＫＩ認証部、１４０　アクセス権限判定部、１５０　認証用リポジトリ、１５１　ユーザ情報テーブル、１５２　認証方式テーブル、１５３　認証ポリシーテーブル、１５４　アクセス制御定義テーブル、１５５　セッション管理テーブル、１５６　役職情報テーブル、１６０　ポイント設定部。

【図１】



【図２】

151:ユーザ情報テーブル

ユーザID	名前	部	課	役職	パスワード	証明書	指紋
User-A	ユーザA	部1		部長	*******	&#($)A	&A($)&
User-B	ユーザB	部1	課1－1	課長	*******	&#($)B	&B($)&
User-C	ユーザC	部1	課1－1	一般	*******	&#($)C	&C($)&
User-D	ユーザD	部2		部長	*******	&#($)D	&D($)&
User-E	ユーザE	部2	課2－1	課長	*******	&#($)E	&E($)&

【図３】

152:認証方式テーブル

認証方式ID	認証方式
Auth01	パスワード
Auth02	背景移動
Auth03	OTP
Auth04	PKI
Auth05	指紋

【図４】

153:認証ポリシーテーブル

認証ポリシーID	条件	認証方式１	認証方式２
Policy-1	役職=部長	Auth01	Auth02
Policy-2	役職=課長	Auth01	Auth03
Policy-3	役職=一般	Auth01	Auth04

【図５】

154:アクセス制御定義テーブル

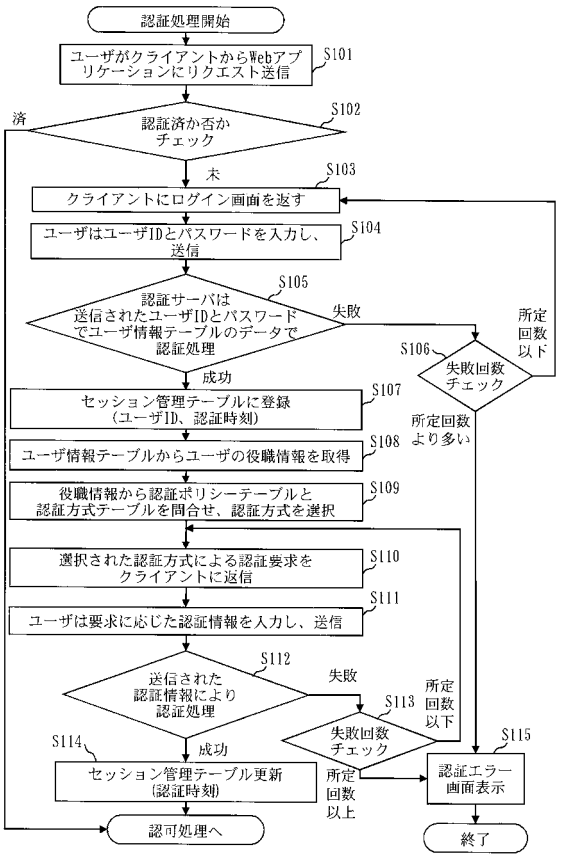
URL	アクセス条件
http://認証サーバ/Webアプリケーション1/top.html	役職>=一般
http://認証サーバ/Webアプリケーション1/work1/	役職>=部長
http://認証サーバ/Webアプリケーション1/work2/	役職>=部長
http://認証サーバ/Webアプリケーション2/top.html	役職>=課長
http://認証サーバ/Webアプリケーション2/work3/	役職>=課長

【図６】

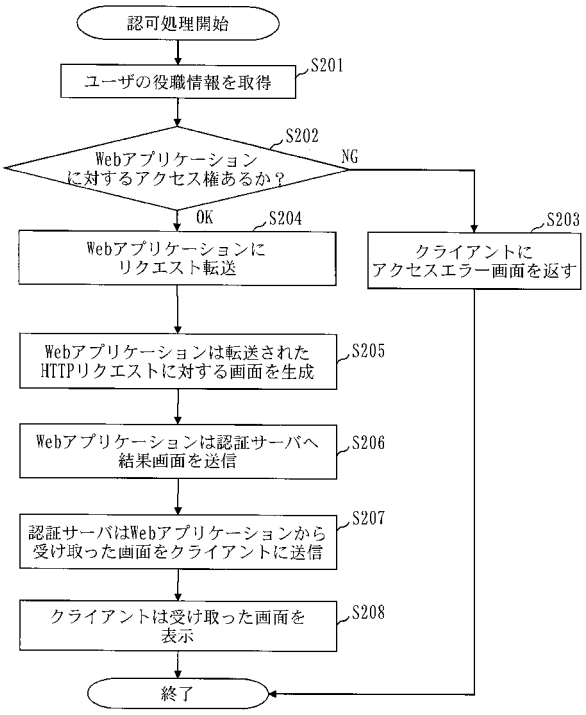
155:セッション管理テーブル

セッションID	ユーザID	認証時刻	セッション期限
0000001	User-A	20100301 10:00:05	90分
0000002	User-B	20100301 10:05:35	95分
0000003	User-C	20100301 10:30:26	120分

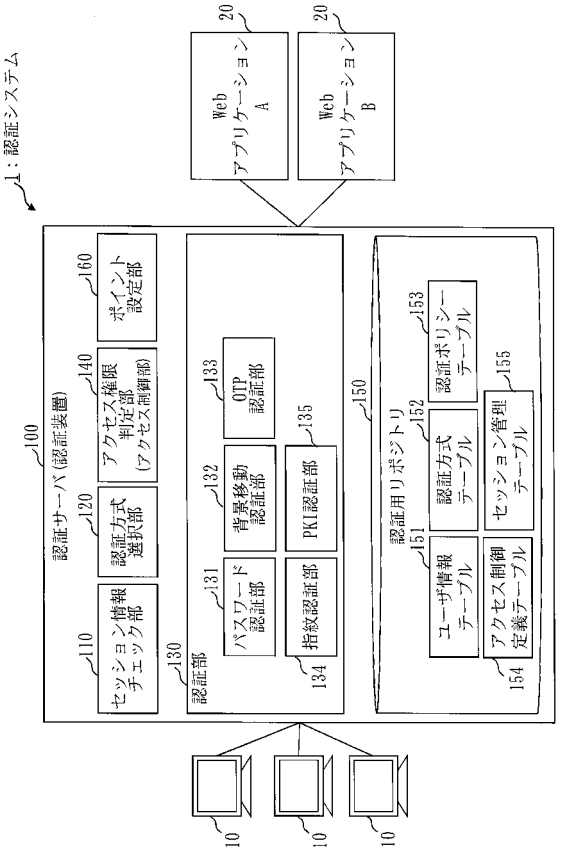
【図７】



【図８】



【図９】



【図１０】

152:認証方式テーブル

認証方式ID	認証方式	セキュリティポイント
Auth01	パスワード	1
Auth02	背景移動	3
Auth03	OTP	4
Auth04	PKI	5
Auth05	指紋	5

【図１１】

154:アクセス制御定義テーブル

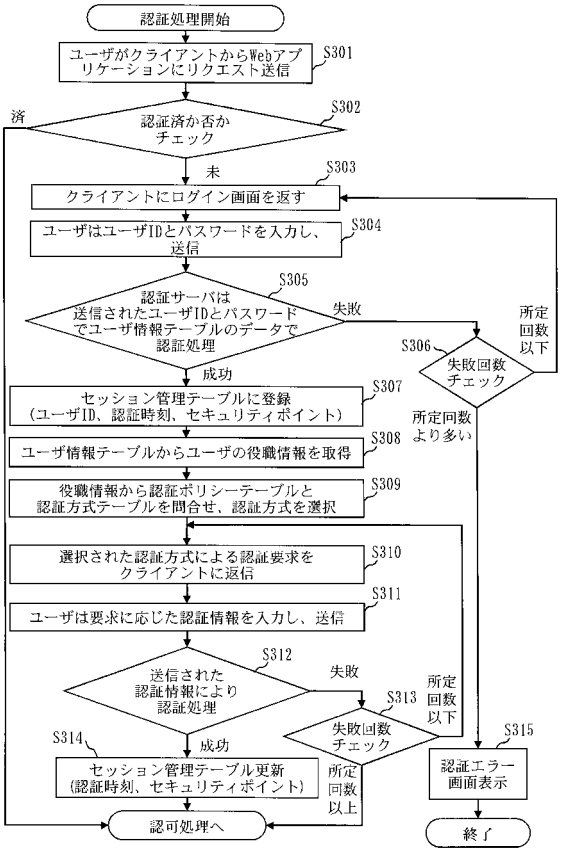
URL	アクセス条件
http://認証サーバ/Webアプリケーション1/top.html	(セキュリティポイント)>= 1)
http://認証サーバ/Webアプリケーション1/work1/	(セキュリティポイント)>= 4) or (役職)>=部長)
http://認証サーバ/Webアプリケーション1/work2/	(セキュリティポイント)>= 6) or (役職)>=部長)
http://認証サーバ/Webアプリケーション2/top.html	(セキュリティポイント)>= 3)
http://認証サーバ/Webアプリケーション2/work3/	(セキュリティポイント)>= 5) or (役職)>=課長)

【図１２】

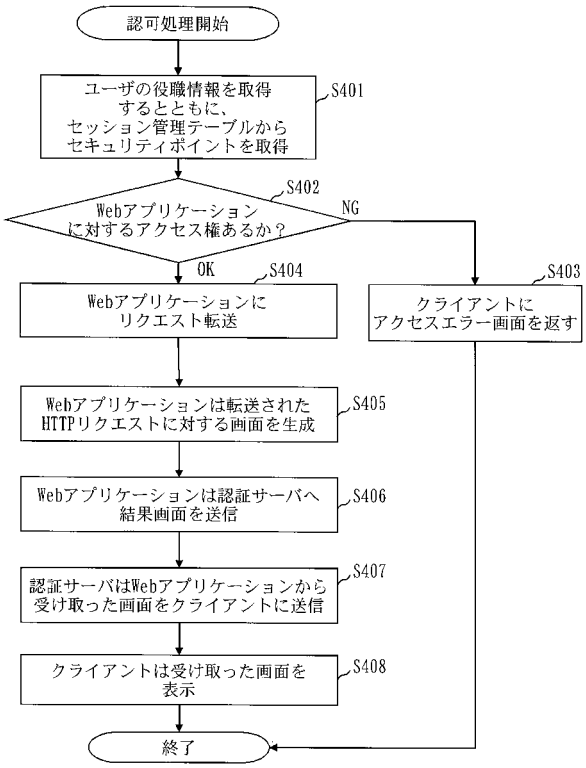
155:セッション管理テーブル

セッションID	ユーザID	認証時刻	セキュリティポイント	セッション期限
0000001	User-A	20100301 10:00:05	5	90分
0000002	User-B	20100301 10:05:35	6	95分
0000003	User-C	20100301 10:30:26	4	120分

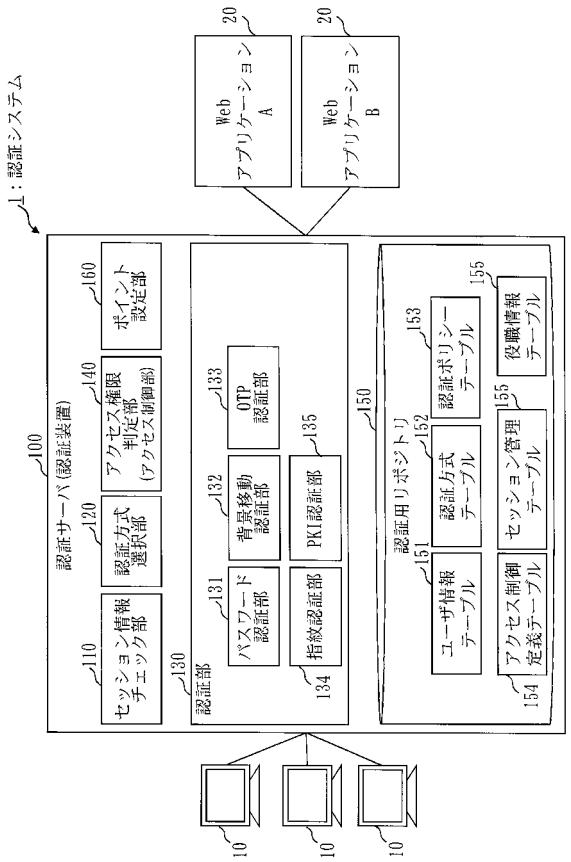
【図１３】



【図１４】



【図１５】



【図１６】

154：アクセス制御定義テーブル

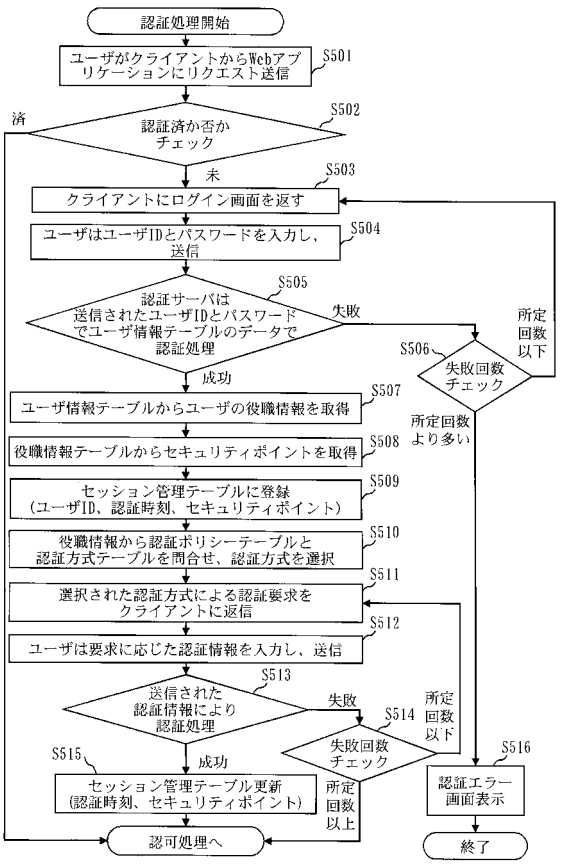
URL	アクセス条件
http://認証サーバ/Webアプリケーション1/top.html	(セキュリティポイント)= 1)
http://認証サーバ/Webアプリケーション1/work1/	(セキュリティポイント)= 4)
http://認証サーバ/Webアプリケーション1/work2/	(セキュリティポイント)= 6)
http://認証サーバ/Webアプリケーション2/top.html	(セキュリティポイント)= 3)
http://認証サーバ/Webアプリケーション2/work3/	(セキュリティポイント)= 5)

【図１７】

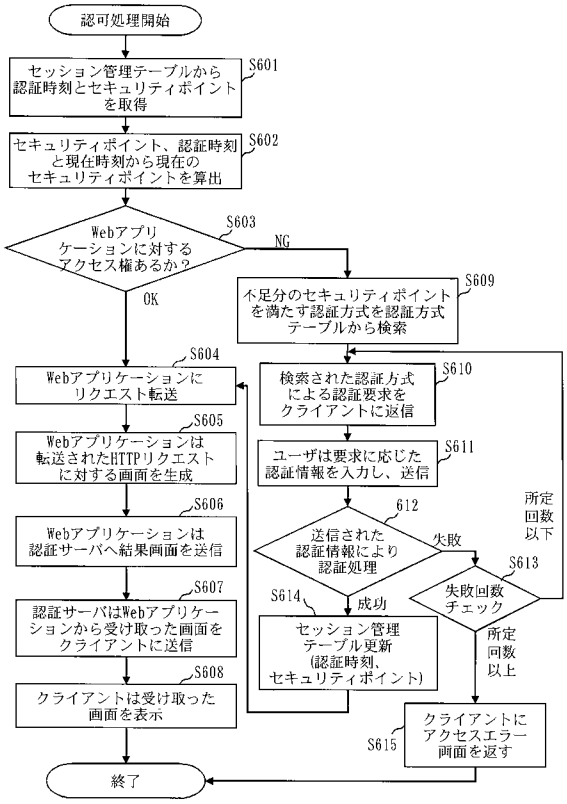
156：役職情報テーブル

役職	セキュリティポイント
部長	4
課長	3
一般	1

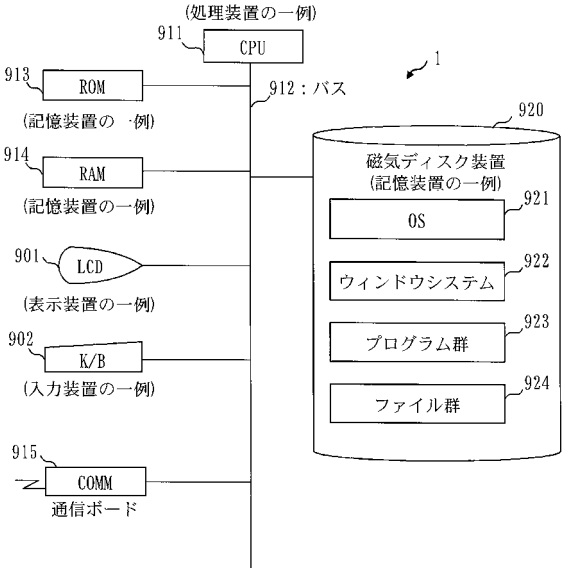
【図１８】



【図１９】


認可処理開始
セッション管理テーブルから認証時刻とセキュリティポイントを取得
S601
セキュリティポイント、認証時刻と現在時刻から現在のセキュリティポイントを算出
S602
Webアプリケーションに対するアクセス権あるか？
S603
NG
OK
不足分のセキュリティポイントを満たす認証方式を認証方式テーブルから検索
S609
Webアプリケーションにリクエスト転送
S604
検索された認証方式による認証要求をクライアントに返信
S610
Webアプリケーションは転送されたHTTPリクエストに対する画面を生成
S605
ユーザは要求に応じた認証情報を入力し、送信
S611
Webアプリケーションは認証サーバへ結果画面を送信
S606
612
送信された認証情報により認証処理
失敗
成功
所定回数以下
S613
失敗回数チェック
S614
セッション管理テーブル更新(認証時刻、セキュリティポイント)
認証サーバはWebアプリケーションから受け取った画面をクライアントに送信
S607
所定回数以上
クライアントは受け取った画面を表示
S608
クライアントにアクセスエラー画面を返す
S615
終了

【図２０】


(処理装置の一例)
911
CPU
1
913
ROM
(記憶装置の一例)
912：バス
920
914
RAM
(記憶装置の一例)
磁気ディスク装置
(記憶装置の一例)
921
OS
922
ウィンドウシステム
901
LCD
(表示装置の一例)
923
プログラム群
902
K/B
(入力装置の一例)
924
ファイル群
915
COMM
通信ボード

フロントページの続き

(56)参考文献 特開２００７－１０２２７８（ＪＰ，Ａ）
特開２００５－１７３８０５（ＪＰ，Ａ）
特開２００４－０８６４９０（ＪＰ，Ａ）
特開２０１０－０６７１２４（ＪＰ，Ａ）
特開２０１０－０９７４６７（ＪＰ，Ａ）
特開２００７－１５７００２（ＪＰ，Ａ）
特開２００９－１１９６２５（ＪＰ，Ａ）
特開２００５－０９２６８３（ＪＰ，Ａ）
特開２００５－０１０８５６（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１