

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2016-66132
(P2016-66132A)

(43) 公開日 平成28年4月28日(2016.4.28)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/31 (2013.01)	G06F 21/31	5 J 1 0 4
G09C 1/00 (2006.01)	G09C 1/00 6 4 0 E	
	G06F 21/31 3 6 0	

審査請求 未請求 請求項の数 12 O L (全 14 頁)

(21) 出願番号	特願2014-193242 (P2014-193242)	(71) 出願人	000233055 株式会社日立ソリューションズ 東京都品川区東品川四丁目12番7号
(22) 出願日	平成26年9月24日 (2014.9.24)	(74) 代理人	100091096 弁理士 平木 祐輔
		(74) 代理人	100102576 弁理士 渡辺 敏章
		(74) 代理人	100162330 弁理士 広瀬 幹規
		(72) 発明者	伊藤 博康 東京都品川区東品川四丁目12番7号 株 株式会社日立ソリューションズ内 Fターム(参考) 5J104 AA07 AA37 KA01 PA07

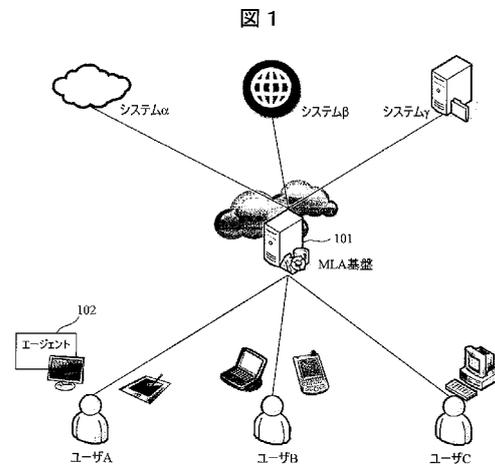
(54) 【発明の名称】 マルチレベル認証装置及びマルチレベル認証方法

(57) 【要約】

【課題】本発明は、統一した認証基準でシステムのセキュリティレベルに応じた認証を適切かつ簡単に運用でき、セキュリティと運用利便性を向上させることができる技術を提供する。

【解決手段】本発明は、複数のユーザの中のあるユーザの端末から複数のシステム中の選択されたシステムへの認証を管理するマルチレベル認証装置である。当該マルチレベル認証装置は、選択された認証方式に対応する認証レベルと、選択されたシステムのシステム認証レベルとを比較することにより、選択されたシステムへの認証を行う。

【選択図】 図 1



【特許請求の範囲】**【請求項 1】**

複数のユーザの中のあるユーザの端末から複数のシステム中の選択されたシステムへの認証を管理するマルチレベル認証装置であって、

記憶部と、
認証処理部と、

を備え、

前記記憶部は、

複数の認証方式と各認証方式に対応する認証情報と各認証方式に対応する認証レベルとが前記ユーザ毎に設定されている認証管理情報と、

10

前記システム毎のシステム認証レベルが設定されているシステム情報と、

を少なくとも格納しており、

前記認証処理部は、

前記複数の認証方式の中の選択された認証方式に対応する前記記憶部の前記認証情報と、前記端末から受信した認証情報とを比較することにより、認証処理を実行し、

前記認証処理が成功した場合、前記選択された認証方式に対応する前記認証レベルと、前記選択されたシステムの前記システム認証レベルとを比較することにより、前記選択されたシステムへの認証を行うことを特徴とするマルチレベル認証装置。

【請求項 2】

請求項 1 に記載のマルチレベル認証装置において、

20

前記認証処理部は、前記選択された認証方式に対応する前記認証レベルを加算していき、当該加算した結果が前記選択されたシステムの前記システム認証レベルに到達したかを判定することにより、前記選択されたシステムへの認証を行うことを特徴とするマルチレベル認証装置。

【請求項 3】

請求項 2 に記載のマルチレベル認証装置において、

前記認証処理部は、前記加算した結果が前記選択されたシステムの前記システム認証レベルに到達していない場合、前記端末に追加の認証を行うことを通知することを特徴とするマルチレベル認証装置。

【請求項 4】

30

請求項 1 ~ 3 のいずれか一項に記載のマルチレベル認証装置において、

前記記憶部は、前記ユーザ毎の行動特性情報をさらに格納しており、

前記端末から受信した行動特性情報と、前記記憶部の前記行動特性情報とを比較することにより、前記選択されたシステムの利用を制御する行動特性判定部をさらに備えることを特徴とするマルチレベル認証装置。

【請求項 5】

請求項 4 に記載のマルチレベル認証装置において、

前記行動特性判定部は、前記端末から受信した行動特性情報と、前記記憶部の前記行動特性情報とが一致する場合、前記選択されたシステムの利用を継続させることを特徴とするマルチレベル認証装置。

40

【請求項 6】

請求項 4 または 5 に記載のマルチレベル認証装置において、

前記行動特性判定部は、前記端末から受信した行動特性情報と、前記記憶部の前記行動特性情報とが一致しない場合、前記端末に追加の認証を通知することを特徴とするマルチレベル認証装置。

【請求項 7】

複数のユーザの中のあるユーザの端末から複数のシステム中の選択されたシステムへの認証を管理するマルチレベル認証装置によるマルチレベル認証方法であって、前記マルチレベル認証装置が、複数の認証方式と各認証方式に対応する認証レベルとが前記ユーザ毎に設定されている認証情報と、前記システム毎のシステム認証レベルが設定されているシ

50

システム情報とを格納しており、

前記マルチレベル認証装置が、前記端末によって選択された認証方式に対応する前記マルチレベル認証装置における前記認証情報と、前記端末から受信した認証情報とを比較することにより、認証処理を実行する第1ステップと、

前記第1ステップにおける前記認証処理が成功した場合、前記マルチレベル認証装置が、前記選択された認証方式に対応する前記認証レベルと、前記選択されたシステムの前記システム認証レベルとを比較することにより、前記選択されたシステムへの認証を行う第2ステップと

を含むことを特徴とするマルチレベル認証方法。

【請求項8】

10

請求項7に記載のマルチレベル認証方法において、

前記第2ステップは、前記選択された認証方式に対応する前記認証レベルを加算していき、当該加算した結果が前記選択されたシステムの前記システム認証レベルに到達したかを判定することにより、前記選択されたシステムへの認証を行うことを含むことを特徴とするマルチレベル認証方法。

【請求項9】

請求項8に記載のマルチレベル認証方法において、

前記第2ステップは、前記加算した結果が前記選択されたシステムの前記システム認証レベルに到達していない場合、前記端末に追加の認証を行うことを通知することを含むことを特徴とするマルチレベル認証方法。

20

【請求項10】

請求項7～9のいずれか一項に記載のマルチレベル認証方法において、

前記マルチレベル認証装置は、前記ユーザ毎の行動特性情報をさらに格納しており、当該方法は、

前記端末から受信した行動特性情報と、前記マルチレベル認証装置における前記行動特性情報とを比較することにより、前記選択されたシステムの利用を制御する第3ステップをさらに含むことを特徴とするマルチレベル認証方法。

【請求項11】

請求項10に記載のマルチレベル認証方法において、

前記第3ステップは、前記端末から受信した行動特性情報と、前記マルチレベル認証装置における前記行動特性情報が一致する場合、前記選択されたシステムの利用を継続させることを含むことを特徴とするマルチレベル認証方法。

30

【請求項12】

請求項10または11に記載のマルチレベル認証方法において、

前記第3ステップは、前記端末から受信した行動特性情報と、前記マルチレベル認証装置における前記行動特性情報が一致しない場合、前記端末に追加の認証を通知することを含むことを特徴とするマルチレベル認証方法。

【発明の詳細な説明】

【技術分野】

40

【0001】

本発明は、基盤サービスとして提供されるマルチレベル認証装置及びマルチレベル認証方法に関する。

【背景技術】

【0002】

クラウドの利用は年々増加傾向にあり、SaaS (Software as a Service) 型のサービスを提供するソフトウェアも増加している。このように、基盤としてサービスを提供するという運用も広がっている。

【0003】

スマートフォンなどに代表されるスマートデバイスは、ほぼ社会に浸透している状況に

50

ある。従来のPCを利用したシステムでは、ID/PW（ユーザID及びパスワード）のような認証を多用していたが、スマートデバイスではその特性上、ID/PW以外の認証（たとえば、PIN（Personal Identification Number）認証やジェスチャー認証など）が多く利用されている。

【0004】

シングルサインオンを利用したシステムも市場には多くある。これらの多くは、特定の認証情報を用いて、複数のシステムの認証を統一に行うというシステムであり、ユーザの運用負荷軽減を主目的として利用されている。

【0005】

本人認証の方法として、行動特性を用いた認証方法がある。これは、キーボードのキーストロークやマウスのクリック速度、ファイルアクセスの方法など端末を利用するユーザの行動を解析して本人かを推定するという方法である。これら行動特性の認証を組み合わせることでID/PWよりも正確な本人認証が可能となる。従来の技術としては特許文献1がある。

10

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開2009-175984号公報

【発明の概要】

【発明が解決しようとする課題】

20

【0007】

現在は、さまざまなシステムやサービスを利用するシーンが多く、システムごとに認証情報を扱っているため、統一した基準での認証レベルというものを規定できない。また、さまざまなシステムやサービスごとに利用者は認証処理を行う必要があり、利用者の認証処理に伴う負担も大きい。

【0008】

一方、一度の認証処理によって複数のシステムやサービスが利用可能になるシングルサインオンの技術も存在する。しかし、シングルサインオンを利用した認証では、攻撃者によって一度でも認証を突破された場合、その後の運用でさまざまなシステムやサービスが利用されてしまう恐れがある。

30

【0009】

また、認証後に利用するシステムやサービスはその重要度によって求められるセキュリティレベルが異なる。たとえば、クレジットカードや個人情報を入力するようなシステムはセキュリティレベルを高くしなければならないが、無記名のアンケートなどセキュリティレベルは低くても問題とならない。しかし、現状の認証では、システムのセキュリティレベルに応じた適切な認証を行えていない。

【0010】

また、PW認証や生体認証以外に、画像のタッチによる画像認証や、タッチでの軌跡による認証など新しい認証方式が登場しているが、その認証による本人推定確率はバラバラである。これを考慮すれば、例えば、本人推定確率が低い認証方式は、セキュリティレベルの高いシステムの認証には利用することができない。したがって、システムごとに異なる認証方式で認証することが必要となり、運用利便性が低くなる。

40

【0011】

本発明は、このような状況に鑑みてなされたものであり、統一した認証基準でシステムのセキュリティレベルに応じた認証を適切かつ簡単に運用でき、セキュリティと運用利便性を向上させることができる技術を提供する。

【課題を解決するための手段】

【0012】

上記課題を解決するために、例えば特許請求の範囲に記載の構成を採用する。本願は上記課題を解決する手段を複数含んでいるが、その一例を挙げるならば、複数のユーザの中

50

のあるユーザの端末から複数のシステム中の選択されたシステムへの認証を管理するマルチレベル認証装置が提供される。当該マルチレベル認証装置は、記憶部と、認証処理部と、を備える。前記記憶部は、複数の認証方式と各認証方式に対応する認証情報と各認証方式に対応する認証レベルとが前記ユーザ毎に設定されている認証管理情報と、前記システム毎のシステム認証レベルが設定されているシステム情報と、を少なくとも格納している。前記認証処理部は、前記複数の認証方式の中の選択された認証方式に対応する前記記憶部の前記認証情報と、前記端末から受信した認証情報とを比較することにより、認証処理を実行し、前記認証処理が成功した場合、前記選択された認証方式に対応する前記認証レベルと、前記選択されたシステムの前記システム認証レベルとを比較することにより、前記選択されたシステムへの認証を行う。

10

【0013】

また、他の例によれば、複数のユーザの中のあるユーザの端末から複数のシステム中の選択されたシステムへの認証を管理するマルチレベル認証装置によるマルチレベル認証方法が提供される。前記マルチレベル認証装置が、複数の認証方式と各認証方式に対応する認証レベルとが前記ユーザ毎に設定されている認証情報と、前記システム毎のシステム認証レベルが設定されているシステム情報とを格納している。当該マルチレベル認証方法は、前記マルチレベル認証装置が、前記端末によって選択された認証方式に対応する前記マルチレベル認証装置における前記認証情報と、前記端末から受信した認証情報とを比較することにより、認証処理を実行する第1ステップと、前記第1ステップにおける前記認証処理が成功した場合、前記マルチレベル認証装置が、前記選択された認証方式に対応する前記認証レベルと、前記選択されたシステムの前記システム認証レベルとを比較することにより、前記選択されたシステムへの認証を行う第2ステップとを含む。

20

【発明の効果】**【0014】**

本発明によれば、統一した認証基準でシステムのセキュリティレベルに応じた認証を適切かつ簡単に運用でき、セキュリティと運用利便性を向上させることができる。

【0015】

本発明に関連する更なる特徴は、本明細書の記述、添付図面から明らかになるものである。また、上記した以外の、課題、構成及び効果は、以下の実施例の説明により明らかにされる。

30

【図面の簡単な説明】**【0016】**

【図1】本発明の実施例におけるマルチレベル認証装置を含むシステム全体図である。

【図2A】本発明の実施例におけるマルチレベル認証装置の機能ブロック図である。

【図2B】本発明の実施例におけるエージェントの機能ブロック図である。

【図3】本発明の実施例におけるユーザ情報の一例である。

【図4】本発明の実施例における認証管理情報の一例である。

【図5】本発明の実施例における行動特性情報の一例である。

【図6】本発明の実施例における端末情報の一例である。

【図7】本発明の実施例におけるシステム情報の一例である。

40

【図8】本発明の実施例における認証処理のフローチャートである。

【図9】本発明の実施例における行動特性判定処理のフローチャートである。

【発明を実施するための形態】**【0017】**

以下、添付図面を参照して本発明の実施例について説明する。なお、添付図面は本発明の原理に則った具体的な実施例を示しているが、これらは本発明の理解のためのものであり、決して本発明を限定的に解釈するために用いられるものではない。

【0018】

課題の解決に当たり、統一的な認証情報および認証を管理するための基盤サービス（以下、MLA（Multi Level Authentication）基盤）を設ける。また、さまざまな端末からの

50

認証情報を管理するためにクラウドを利用する。

【0019】

本実施例では、基盤サービスとして、SaaS型のマルチレベル認証装置を提供する。図1は、基盤サービスとしてのマルチレベル認証装置を含むシステム全体図である。MLA基盤（マルチレベル認証装置101）は、複数のユーザの複数の端末からの複数のシステムへの認証を管理するものである。図1の運用例では、MLA基盤（マルチレベル認証装置101）と、3種類のシステム、と、複数のユーザA、B、Cの端末とが示されている。

【0020】

マルチレベル認証装置101は、クラウド上にある装置であり、ネットワークを介して複数のシステム、と接続されている。マルチレベル認証装置101は、プログラム（以下、エージェント）102を介して複数のユーザA、B、Cが所有する複数の端末から接続される。ユーザA、B、Cは、その端末の種類や端末の所持数が異なり、端末の例としては、PC（Personal Computer）、タブレット端末、スマートフォンなどの情報処理端末である。

10

【0021】

マルチレベル認証装置101は、統一的な認証情報を管理しており、ユーザA、B、Cの端末からエージェント102を介して接続されたときに、各ユーザの認証を行う。マルチレベル認証装置101は、認証処理が終了すると、選択されたシステム、への接続を許可する。その後、ユーザA、B、Cは、エージェント102を介して、選択したシステム、を利用することができる。また、エージェント102は、ユーザA、B、Cの行動特性を収集してマルチレベル認証装置101へ送信し、マルチレベル認証装置101は、その行動特性の情報からユーザA、B、Cの認証を行う。

20

【0022】

本実施例において、エージェント102は、ユーザA、B、Cの端末にあらかじめインストールされている。なお、ユーザA、B、Cの端末がマルチレベル認証装置101に接続したときに、マルチレベル認証装置101からエージェント102がダウンロードされるようにしてもよい。

【0023】

次に、マルチレベル認証装置101及びエージェント102について説明する。マルチレベル認証装置101は、中央演算処理部（CPU：Central Processing Unit）などのプロセッサと、メモリと、ハードディスクなどの記憶装置とを少なくとも備える情報処理装置で構成されている。なお、図1では、マルチレベル認証装置101を1つの情報処理装置として示しているが、これに限定されない。マルチレベル認証装置101の構成要素をネットワーク上の複数の情報処理装置に分散して構成してもよい。

30

【0024】

また、以降で説明する各種情報（図3～図7の情報）は、マルチレベル認証装置101の記憶装置に格納される。なお、これらの情報は、マルチレベル認証装置101とは別の情報処理装置あるいはネットワーク上の記憶装置に格納されてもよい。

【0025】

図2Aは、マルチレベル認証装置101の機能ブロック図を示す。マルチレベル認証装置101は、認証処理部201と、行動特性判定部202と、記憶部203とを備える。認証処理部201は、エージェント102を介して受け取った認証情報を、記憶部203にあらかじめ登録された認証情報と比較することにより認証処理を実行する。行動特性判定部202は、エージェント102を介して受け取った行動特性情報を、記憶部203にあらかじめ登録された行動特性情報と比較することにより、システムの利用を制御する。記憶部203は、上述のハードディスクなどの記憶装置であり、認証処理に必要な認証情報を格納するものである。

40

【0026】

図2Bは、エージェント102の機能ブロック図を示す。エージェント102は、認証

50

情報送受信部 2 1 1 と、行動特性収集部 2 1 2 とを備える。認証情報送受信部 2 1 1 は、ユーザが選択したシステムの情報、ユーザの端末の情報、及び、ユーザの入力した認証情報などをマルチレベル認証装置 1 0 1 へ送信する。また、認証情報送受信部 2 1 1 は、マルチレベル認証装置 1 0 1 での認証処理の結果の通知を受け取る。なお、認証情報送受信部 2 1 1 とマルチレベル認証装置 1 0 1 との間で送受信する情報については暗号化 / 復号化することにより安全性を確保する。また、行動特性収集部 2 1 2 は、ユーザの端末上での行動特性の情報を収集し、その収集した行動特性情報をマルチレベル認証装置 1 0 1 へ送信する。

【 0 0 2 7 】

次に、マルチレベル認証装置 1 0 1 において管理する情報について説明する。本実施例におけるマルチレベル認証装置 1 0 1 では、認証処理に必要な様々な情報を管理する。これらの情報は、あらかじめマルチレベル認証装置 1 0 1 の記憶部 2 0 3 に格納されている。表 1 は、マルチレベル認証装置 1 0 1 上で管理する情報を説明する表である。

【 0 0 2 8 】

【表 1】

#	管理項目	内容
1	ユーザ情報	ユーザの情報を管理する。ユーザを特定するため、ユーザ ID、役職、及び、認証ポイントなどの情報を管理する。
2	認証方式	認証方式を管理する。ここでは、ID/PW 認証や PIN 認証、生体認証などの利用できる認証方式が列挙されている。
3	認証情報	認証方式ごとに認証情報を管理する。ID/PW 認証では PW 情報を管理し、PIN 認証では PIN コードの情報を管理する。また、生体情報の場合は、生体情報のパターンなどを管理する。
4	行動特性情報	行動特性で利用する情報を管理する。行動特性で利用する項目と、本人推定のための情報(キーストローク速度など)と、前回の統計データなどを管理する。
5	端末情報	ユーザの利用する端末の情報を管理する。
6	システム情報	MLA 基盤 (マルチレベル認証装置 1 0 1) を利用するシステムの情報を管理する。あに、システム側で求めるシステム認証レベルを規定する。

【 0 0 2 9 】

次に、表 1 で説明した情報の詳細な例を図 3 ~ 図 7 を用いて説明する。各種情報について、以後の説明では「テーブル」構造を用いて説明するが、必ずしもテーブルによるデータ構造で表現されていなくても良く、他のデータ構造で表現されていても良い。

【 0 0 3 0 】

図 3 は、ユーザ情報の一例である。ユーザ情報は、項番 3 0 1 と、ユーザ ID 3 0 2 と、ユーザ名 3 0 3 と、役職 3 0 4 と、認証ポイント 3 0 5 とから構成される。本実施例のユーザ情報では、役職 3 0 4 ごとに認証ポイント 3 0 5 を管理する。例えば、会社内での役職や職務権限などによりアクセスできるシステムへの権限などが異なる場合がある。例えば、役職 3 0 4 がより高いユーザに対して高い認証ポイント 3 0 5 を付与し、以後に説明する認証処理において認証ポイント 3 0 5 の高いユーザに対しては 1 回の認証に対する認証レベルのポイントが高くなるように重み付けなどの操作を行ってもよい。このような処理を行うことにより、役職に応じてシステムへのアクセスを管理することも可能となる。

【 0 0 3 1 】

図 4 は、認証管理情報の一例である。認証管理情報では、複数の認証方式と各認証方式に対応する認証情報と各認証方式に対応する認証レベルとがユーザ毎に設定されている。認証管理情報は、項番 4 0 1 と、ユーザ ID 4 0 2 と、認証方式 4 0 3 と、認証情報 4 0 4 と、認証 ID 4 0 5 と、認証方式認証レベル 4 0 6 とから構成される。

【 0 0 3 2 】

認証方式 4 0 3 としては、PW認証、PIN認証、生体認証（例えば、指紋認証）、画像認証、軌跡認証など、各ユーザに対して任意の複数の方式を登録できる。ここで、画像認証とは、複数の画像から特定の画像をユーザがあらかじめ選択しておく認証であり、例えば、認証情報 4 0 4 には画像情報が登録される。生体認証なども同様に、認証情報 4 0 4 として生体情報のパターンなどの画像情報が登録される。軌跡認証は、例えばスマートフォンやタブレット端末上の画面の指の軌跡パターンを用いた認証であり、認証情報 4 0 4 としては、指の軌跡パターンの情報が登録される。

10

【 0 0 3 3 】

認証方式認証レベル 4 0 6 には、各認証方式で認証が成功した場合に得られる認証レベルが登録されている。例えば、ユーザ「U 0 0 1」が「PW認証」を成功したときには、認証レベルのポイント「5」を得ることができる。本実施例では、この認証方式認証レベル 4 0 6 のポイントと、以降で説明するシステム認証レベルとを比較することにより、選択されたシステムへの認証を行う。認証方式認証レベル 4 0 6 のポイントがシステム認証レベルに到達していない場合でも、複数の認証方式を実行して認証方式認証レベル 4 0 6 のポイントを加算させていくことにより、最終的にシステム側が求める認証レベルまで到達するかを判定する。最終的にシステム側が求める認証レベルまで到達すると、選択されたシステムへのアクセスが許可される。

20

【 0 0 3 4 】

図 5 は、行動特性情報の一例である。行動特性情報は、項番 5 0 1 と、ユーザ ID 5 0 2 と、行動特性項目 5 0 3 と、行動特性 5 0 4 と、前回統計データ 5 0 5 とから構成される。

【 0 0 3 5 】

本人の行動特性に起因する情報は、本人の行動データの統計データを利用する。統計データとして一定期間の情報が集約されて、ユーザの行動特性があらかじめ分析される。この期間は「行動特性収集期間」とし、統計分析に必要なデータを収集できるまでとする。この期間は収集するデータによって確度が異なる（マウスクリック速度であれば、10クリックで一定の確度が保たれるが、キーストロークは100文字入力までの期間が必要など）ため、それぞれ必要なデータが収集できるまでは行動特性を収集し続ける。このように収集された行動特性の情報が、行動特性 5 0 4 としてあらかじめ登録されている。行動特性 5 0 4 としては、キーストローク、マウスクリック、特定ファイルへのアクセスなど、各ユーザに対して任意の複数の行動特性を登録できる。

30

【 0 0 3 6 】

また、行動特性 5 0 4 とは別に、前回統計データ 5 0 5 を管理してもよい。これは、ユーザの行動特性が徐々に変化する場合に有益である。例えば、ユーザの行動特性が徐々に変化している場合、取得された行動特性の情報が行動特性 5 0 4 と一致しない場合でも、前回統計データ 5 0 5 と一致すれば本人であると推定することも可能である。より直近の統計データを用いることで、一定の本人推定の確度を得ることも可能となる。

40

【 0 0 3 7 】

図 6 は、端末情報の一例である。端末情報は、項番 6 0 1 と、ユーザ ID 6 0 2 と、端末 ID 6 0 3 と、端末種別 6 0 4 と、端末名 6 0 5 とから構成される。端末情報は、例えば、認証方式の選択の際に利用することが可能である。利用する端末によって可能な認証方式は異なる。例えば、ユーザの端末がタブレットやスマートフォンであるときは、マルチレベル認証装置 1 0 1 は、認証方式として軌跡認証を選択できることをエージェント 1 0 2 を介して通知することができる。

50

【 0 0 3 8 】

図 7 は、システム情報の一例である。システム情報には、システム毎のシステム認証レベルが設定されている。システム情報は、項番 7 0 1 と、システム ID 7 0 2 と、システム名 7 0 3 と、システム認証レベル 7 0 4 と、システム情報 7 0 5 とから構成される。システム側で求める認証レベルはシステムごとに異なるため、システム毎にシステム認証レベル 7 0 4 をあらかじめ規定する。

【 0 0 3 9 】

ユーザは、システム利用時に MLA 基盤 (マルチレベル認証装置 1 0 1) に対して認証を行うが、1 つの認証方式だけではなく複数の認証方式を組み合わせることが可能である。ユーザは選択した認証方式で認証処理を行うことで、認証管理情報の認証方式認証レベル 4 0 6 のポイントを加算させていき、最終的にシステム側が求めるシステム認証レベル 7 0 4 まで到達すると、そのシステムへのアクセスが許可される。

10

【 0 0 4 0 】

次に、本実施例における認証処理を説明する。図 8 は、認証処理のフローチャートである。なお、以後の説明では、図 2 A 及び図 2 B で示した機能ブロックを主語として説明を行うが、プログラムはプロセッサによって実行されることで定められた処理をメモリ及び通信ポート (通信制御装置) を用いながら行うため、プロセッサを主語とした説明としてもよい。

【 0 0 4 1 】

ここでは、ユーザ A がシステム を利用する場合の例で説明する。まず、エージェント 1 0 2 の認証情報送受信部 2 1 1 は、マルチレベル認証装置 1 0 1 からシステム情報を取得し、ユーザ A の端末上に表示する。ユーザ A は、端末上に表示されたシステムの一覧からシステム を選択する (8 0 1)。その際、認証情報送受信部 2 1 1 は、選択したシステムの情報と、ユーザ A の端末の情報をマルチレベル認証装置 1 0 1 に送信する。

20

【 0 0 4 2 】

次に、認証情報送受信部 2 1 1 は、マルチレベル認証装置 1 0 1 からその端末で可能な認証方式の情報を取得する。例えば、ユーザ A の端末がパソコンであった場合、図 4 の例では PW 認証及び画像認証が可能となる。ユーザ A の端末上に表示された 2 つの認証方式が表示され、ユーザ A は、端末上に表示された認証方式の一覧から、例えば PW 認証を選択する (8 0 2)。

30

【 0 0 4 3 】

次に、ユーザ A は端末上で認証情報を入力する (8 0 3)。このとき、認証情報送受信部 2 1 1 は、入力された認証情報をマルチレベル認証装置 1 0 1 へ送信する。

【 0 0 4 4 】

次に、マルチレベル認証装置 1 0 1 の認証処理部 2 0 1 は、複数の認証方式の中の選択された認証方式 (PW 認証) に対応する認証情報と、ユーザ A の端末から受信した認証情報とを比較することにより、認証処理を実行する (8 0 4)。ユーザ A の端末から受信した認証情報が、図 4 の認証情報 4 0 4 と一致した場合、ステップ 8 0 5 へ進み、一致しない場合はステップ 8 0 3 へ戻る。

【 0 0 4 5 】

認証情報が一致した場合、認証処理部 2 0 1 は、図 4 の認証情報から、PW 認証に対応する認証レベルのポイント「 5 」を取得する (8 0 5)。次に、認証処理部 2 0 1 は、PW 認証に対応する認証レベルのポイント「 5 」と、選択されたシステムのシステム認証レベル「 1 0 」とを比較し、システムのシステム認証レベル 7 0 4 に到達したかを判定する (8 0 6)。この場合、ユーザ A が獲得した認証レベルのポイント「 5 」は、システムが求めるシステム認証レベル「 1 0 」には到達していないため、ステップ 8 0 2 へ戻って追加の認証を行うことになる。このとき、認証処理部 2 0 1 は、エージェント 1 0 2 へ追加の認証が必要なことを通知する。

40

【 0 0 4 6 】

次に、ステップ 8 0 2 で画像認証を選択し、ステップ 8 0 2 ~ 8 0 4 の処理を実行した

50

とする。ステップ 804 の後、認証処理部 201 は、図 4 の認証情報から、画像認証に対応する認証レベル「8」を取得し、現在の認証レベルのポイントに加算する(805)。これにより、2つの認証方式によって得られた認証レベルのポイントは「13」となる。

【0047】

次に、認証処理部 201 は、認証レベルのポイントの加算結果が、システム のシステム認証レベル 704 に到達したかを判定する(806)。この場合、ユーザ A が獲得した認証レベルのポイントは「13」であり、システム のシステム認証レベル「10」を超えたため、ステップ 807 へ進む。その後、認証処理部 201 は、エージェント 102 の認証情報送受信部 211 を介して、ユーザ A の端末にシステム への接続の許可を通知する。これにより、ユーザ A の端末は、システム への接続が許可され、システム を利用

10

【0048】

なお、ユーザ A がシステム や を利用する場合も、システム と同様の処理を行い、認証をさせる。なお、上述の例では、複数の認証方式を組み合わせることでシステムへの認証を行ったが、ユーザが本人推定確率の高い認証方式(例えば、指紋認証)を最初に選択すれば、1回の認証方式でシステムへ接続することも可能である。ユーザ自身が任意の認証方式を選択することで、選択したシステムへの接続が可能である。

【0049】

また、ユーザ B や C がシステム を利用する場合も、ユーザ A と同様の処理で認証を行う。ただし、ユーザごとに権限が異なる(ユーザ情報の役職及び認証ポイント 305 が異なる)ため、同じ端末であったとしても必要な認証レベルは異なる。マルチレベル認証装置 101 (MLA基盤)は、ユーザの権限(認証ポイント 305)に応じて、認証処理によって得られる認証方式認証レベル 406 のポイントを変化させてもよく、必要な認証レベルを各ユーザへ要求することになる。

20

【0050】

以上説明したように、本実施例によれば、さまざまな認証方式を組み合わせ、それらの認証方式ごとの認証レベルのポイントを加算していくことによって、システムが利用できるようになる。したがって、さまざまなシステムを利用する複数のユーザに関して、ユーザがそれぞれのシステムに対して適切な認証レベルで認証を行うことができる。また、本実施例では、さまざまな認証情報をクラウド上で管理し、それらの認証情報を基盤として提供することができる。各システムが求める認証レベルは、マルチレベル認証装置 101 (MLA基盤)で管理しているため、各システムは認証にかかるポイントなど、認証処理に必要な情報を意識する必要はなく、システムの運用利便性も向上する。

30

【0051】

したがって、認証レベルのポイントという統一した認証基準でシステムのセキュリティレベルに応じた認証を適切かつ簡単に運用でき、セキュリティと運用利便性を向上させることができる。

【0052】

次に、図 8 の認証処理が終了し、システムを使用している間の行動特性判定処理について説明する。図 8 の認証処理後、ユーザ A がシステム を利用しているとして説明する。

40

【0053】

本実施例では、認証が成功してユーザ A がシステム へ接続した後、エージェント 102 はユーザ A のさまざまな行動特性を収集する。エージェント 102 は収集した行動特性情報をマルチレベル認証装置 101 (MLA基盤)へ送信する。マルチレベル認証装置 101 は、受け取った行動特性情報と、あらかじめ登録されている行動特性情報とが一致するかを判定し、ユーザ A のシステム の利用を制御する。例えば、行動特性情報が一致した場合には、ユーザ A がシステム を操作しているとしてシステム との接続を維持する。

【0054】

図 9 は、上記の処理の詳細を示す行動特性判定処理のフローチャートである。認証後、ユーザ A がシステム を利用している間、エージェント 102 の行動特性収集部 212 は

50

、所定の期間の間、ユーザ A の端末上での行動データの情報を収集する（901）。

【0055】

その後、行動特性収集部 212 は、収集したデータを解析し、行動特性情報（例えば、キーストロークやマウスクリックなど）をマルチレベル認証装置 101 へ送信する（902）。ここでは、エージェント 102 の行動特性収集部 212 が、解析した結果をマルチレベル認証装置 101 へ送信する例を説明したが、行動特性収集部 212 が端末上での行動データをマルチレベル認証装置 101 へ逐一送信し、マルチレベル認証装置 101 側で行動データを解析して行動特性情報を取得してもよい。

【0056】

次に、マルチレベル認証装置 101 の行動特性判定部 202 は、ユーザ A の端末から受信した行動特性情報と、図 5 の行動特性 504 とが一致するかを判定する（903）。一致した場合は、ステップ 904 へ進む。ここで、ユーザ A の端末から受信した行動特性情報が、図 5 の行動特性 504 と完全に一致する必要はなく、行動特性 504 の値に許容範囲を持たせてもよい。したがって、行動特性判定部 202 は、受信した行動特性情報がその許容範囲内に収まれば、図 5 の行動特性 504 と一致すると判定してもよい。また、図 5 の行動特性 504 と一致しない場合でも、受信した行動特性情報が、前回統計データ 505 と一致する、又は、前回統計データ 505 に対して所定の許容範囲にあれば、ユーザ A がシステム を操作しているとしてステップ 904 へ進んでもよい。

【0057】

行動特性情報が一致した場合は、ユーザ A の端末とシステム との接続が維持される（904）。なお、このとき、行動特性判定部 202 は、今回ユーザ A の端末から受信した行動特性情報を前回統計データ 505 として登録する。

【0058】

一方、行動特性情報が一致しない場合は、ユーザの再認証処理が実施される。この再認証処理として、例えば図 8 のステップ 802 ~ 807 が実施される。なお、このように行動特性判定処理で再認証が必要になったユーザに対しては、システム認証レベル 704 の値を所定の値だけ下げて、認証処理を実行してもよい。すでに一度システム への認証に成功しており、ユーザ A が使用している確率が高いことから、二度目の認証についてはシステム認証レベル 704 を下げることで、ユーザへの負荷を低減することができる。

【0059】

また、別の例として、行動特性情報が一致しない場合に、ユーザ A の端末からのシステム への接続を切断してもよい。この場合、ユーザ A は、再度図 8 の認証処理を実行することになる。再認証処理ではなく、システム を使用できないように制御して、セキュリティを高めてもよい。

【0060】

なお、行動特性情報による認証が有効な期間は 30 分とし、30 分を超えた場合は再度行動特性を収集する。すなわち、ステップ 904 の後、30 分経過後に、再度ステップ 901 へ戻る。なお、この行動特性情報による認証が有効な期間は適宜変更してもよい。

【0061】

以上説明したように、本実施例によれば、システムの認証処理後は利用者の行動特性を端末から収集し、マルチレベル認証装置 101（MLA 基盤）へ通知する。マルチレベル認証装置 101 は、受け取った行動特性情報を、あらかじめ登録されている行動特性情報と比較し、本人認証を行う。マルチレベル認証装置 101 は、本人と推定できない場合は、再認証（あるいはシステム利用不可）などの処理を行い、システムの継続的な利用を行えないようにする。これにより、セキュリティを高めることが可能となる。

【0062】

また、従来では、一度認証を行った後に、一定時間を経過すると認証タイムアウトとしてユーザに再認証を求めるシステムもあったが、再認証をユーザへ要求するため、ユーザにとって煩雑となる。これに対して、本実施例では、行動特性情報により本人であると推定されれば、再認証処理をしないで、システムを利用し続けることが可能である。これに

10

20

30

40

50

よって、システムタイムアウトによって再認証するというような運用負荷は軽減することができる。

【0063】

なお、本発明は上述した実施例に限定されるものではなく、様々な変形例が含まれる。例えば、上述した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施例の構成の一部を他の実施例の構成に置き換えることがあり、また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

【0064】

また、上記実施例で示された各機能、処理部等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現しても良い。各機能等を実現するプログラム、テーブル、ファイル等の情報は、メモリやハードディスク、SSD (Solid State Drive) 等の記録或いは記憶装置、またはICカード、SDカード、DVD等の記録或いは記憶媒体に格納することができる。

【0065】

さらに、上述の実施例において、制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線や情報線を示しているとは限らない。全ての構成が相互に接続されていても良い。

【符号の説明】

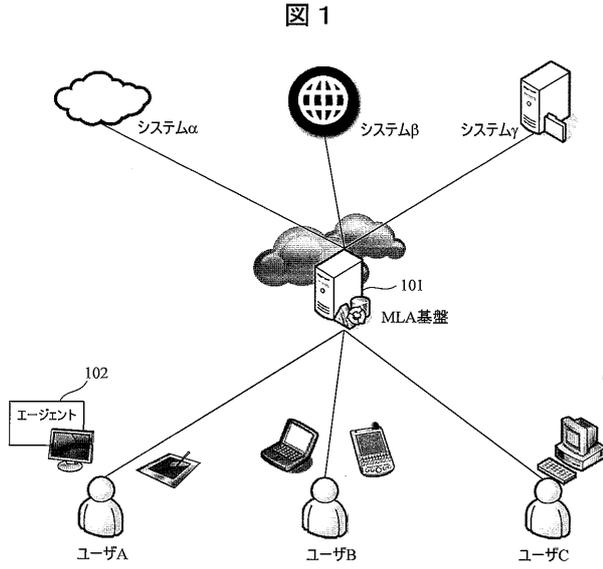
【0066】

- 101 : マルチレベル認証装置
- 102 : プログラム (エージェント)
- 201 : 認証処理部
- 202 : 行動特性判定部
- 203 : 記憶部
- 211 : 認証情報送受信部
- 212 : 行動特性収集部

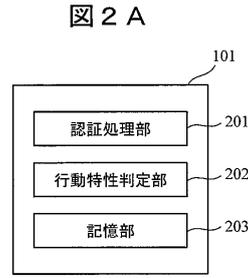
10

20

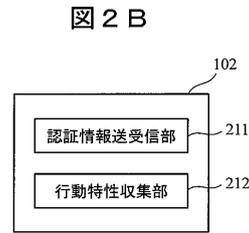
【 図 1 】



【 図 2 A 】



【 図 2 B 】



【 図 3 】

図 3

#	ユーザーID	ユーザー名	役職	認証ポイント
1	U001	ユーザーA	社長	3
2	U002	ユーザーB	課長	2
3	U003	ユーザーC	担当	1

【 図 5 】

図 5

#	ユーザーID	行動特性項目	行動特性	前回統計データ
1	U001	キーストローク	5Key/Sec	5.3Key/Sec
2		マウスクリック	0.1Sec/Click	0.2Sec/Click
3	U002	キーストローク	7Key/Sec	7.8Key/Sec
4		マウスクリック	0.05Sec/Click	0.08Sec/Click
5	U003	キーストローク	10Key/Sec	11.1Key/Sec
6		マウスクリック	0.03Sec/Click	0.02Sec/Click

【 図 4 】

図 4

#	ユーザーID	認証方式	認証情報	認証ID	認証方式認証レベル
1	U001	PW認証	XXXXXX	A001	5
2		PIN認証	XXXX	A002	3
3		画像認証	XXXXXXXX	A003	8
4	U002	PW認証	XXXXXX	A001	5
5		PIN認証	XXXX	A002	3
6		軌跡認証	XXXXXXXXXX	A004	4
7		指紋認証	XXXXXXXXXX	A005	10
8	U003	PW認証	XXX	A001	5
9		指紋認証	XXXXXXXXXX	A005	10

【 図 6 】

図 6

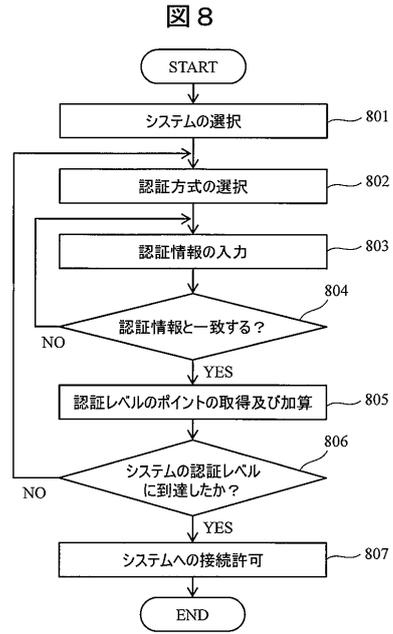
#	ユーザーID	端末ID	端末種別	端末名
1	U001	T001	PC	ユーザーA_PC
2		T002	タブレット	ユーザーA_TAB
3	U002	T003	NPC	ユーザーB_NPC
4		T004	スマートフォン	ユーザーB_PHN
5	U003	T005	PC	ユーザーC_PC

【 図 7 】

図 7

#	システムID	システム名	システム認証レベル	システム情報
1	S001	システムα	10	クラウド
2	S002	システムβ	7	Web
3	S003	システムγ	3	ファイルサーバ

【 図 8 】



【 図 9 】

