

(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2010-33191

(P2010-33191A)

(43) 公開日 平成22年2月12日(2010.2.12)

(51) Int.Cl.	F I	テーマコード (参考)
G06F 21/20 (2006.01)	G06F 15/00 330G	5B017
G06K 17/00 (2006.01)	G06K 17/00 F	5B058
H04L 9/32 (2006.01)	G06K 17/00 T	5B285
	H04L 9/00 673E	5J104

審査請求 有 請求項の数 5 O L (全 14 頁)

(21) 出願番号	特願2008-192678 (P2008-192678)	(71) 出願人	507369969 株式会社蝶理コム
(22) 出願日	平成20年7月25日 (2008. 7. 25)		大阪府大阪市中央区淡路町 1 丁目 7 番 3 号
(11) 特許番号	特許第4190023号 (P4190023)	(74) 代理人	100103872 弁理士 柏川 敏夫
(45) 特許公報発行日	平成20年12月3日 (2008. 12. 3)	(72) 発明者	川勝 敏郎 大阪府大阪市中央区瓦町 2 丁目 4 番 7 号 株式会社蝶理コム内
		(72) 発明者	山崎 正義 大阪府大阪市中央区瓦町 2 丁目 4 番 7 号株 式会社蝶理コム内
		(72) 発明者	青木 克仁 東京都中央区日本橋堀留町 2 丁目 4 番 3 号 株式会社蝶理コム内
		F ターム (参考)	5B017 AA04 BB09

最終頁に続く

(54) 【発明の名称】 認証装置、方法及びコンピュータプログラム

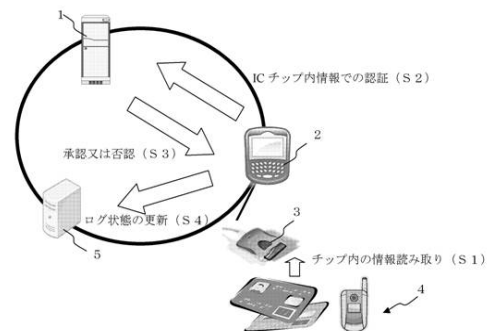
(57) 【要約】

【課題】 ネットワーク認証をActive

Directoryと各種デバイスで読み取ったICチップ内の情報との認証とそれらの自動整合処理モジュールと仕組みを提供する。

【解決手段】 リーダーライター経由でICチップ内の情報を読み込んだネットワーク端末は、ネットワーク経由でActive Directoryサーバを見て同一情報が存在していれば認証し、存在していなければ否認する。また、キーのみ一致する場合はICチップ内の情報をActive Directoryサーバに更新して自動的に整合性を保つ仕組みにより、ネットワーク内認証の認証テーブルの一元化、及び、ICチップ搭載デバイスの紛失等による認証テーブル修正工数の軽減を図る。

【選択図】 図 1



【特許請求の範囲】**【請求項 1】**

ＩＣチップを識別する製造番号と、ユーザーを識別するユーザーＩＤとを記憶するＩＣチップと、

上記ＩＣチップに記憶されているデータを読み取る読取手段と、

上記読み取ったＩＣチップのデータをサーバに対して送信することで認証要求を行い、認証が正しい場合に所定の動作を行うネットワーク端末とを有し、上記ネットワーク端末に通信を介して接続可能に構成されたサーバであって、

ユーザーＩＤに関連付けて、少なくとも最新のＩＣチップの製造番号及び上記ＩＣチップが再発行された際に過去に関連付けられていた上記ＩＣチップの製造番号と、当該ユーザーＩＤがアカウントとして有効又は無効を表すアカウント属性情報を関連付けて記憶する記憶手段と、

上記ネットワーク端末が、上記ＩＣチップから読み取り、送信したＩＣチップの製造番号及びユーザーＩＤを含む認証要求を受信する受信手段と、

上記記憶手段を参照して、上記受信したユーザーＩＤと一致するユーザーＩＤが記憶されているか否か判別する第１処理手段と、

判別の結果、一致するユーザーＩＤが存在する場合に、上記記憶手段を参照して当該ユーザーＩＤに関連付けて記憶されている上記最新の製造番号が上記受信した製造番号と一致するか否か判別する第２処理手段と、

上記判別の結果、製造番号が一致しない場合に、上記ユーザーＩＤに関連付けられた製造番号が未登録か否かを判別する第３処理手段と、

上記判別の結果、製造番号が未登録であると判別された場合に、上記受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶することで新規登録処理を行い、また上記判別の結果、製造番号が未登録ではないと判別され、かつ、上記記憶手段に記憶されている過去の製造番号と一致しない場合には、上記ネットワーク端末から受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶するとともにアカウント属性情報を有効に変更する更新処理を行う第４の処理手段、

を有することを特徴とする認証装置。

【請求項 2】

上記ネットワーク端末は、所定の動作を行うための組織単位情報を記憶しており、上記サーバから通知された組織単位情報が上記予め記憶されている組織単位情報に一致する場合に所定の動作を行うようになっており、

上記記憶手段には、組織単位情報がさらに記憶されており、

上記第２の処理手段により製造番号が一致すると判別された場合、又は上記第４の手段により新規登録処理又は更新処理が行われた場合に、上記記憶手段に記憶されている当該ＩＣチップのアカウント属性情報を上記ネットワーク端末に送信して上記ネットワーク端末に対して所定の処理を実行させる第５処理手段と、を有する、

請求項１記載の認証装置。

【請求項 3】

上記ＩＣチップには、暗号化キーを使用するか否かを表すシステムコードがさらに記憶されており、

上記ネットワーク端末は、上記暗号化キーを読み取り、暗号化キーを使用するか否かを判別する手段と、

判別した結果、暗号化キーを使用しない場合には、上記第２処理手段が、上記記憶手段に記憶されている最新の製造番号が、上記受信した製造番号と一致するか否か判別することで認証処理を行う、

請求項１又は２記載の認証装置。

【請求項 4】

ＩＣチップを識別する製造番号と、ユーザーを識別するユーザーＩＤとを記憶するＩＣチップと、

10

20

30

40

50

上記ＩＣチップに記憶されているデータを読み取る読取手段と、

上記読み取ったＩＣチップのデータをサーバに対して送信することで認証要求を行い、認証が正しい場合に所定の動作を行うネットワーク端末とを有し、上記ネットワーク端末に通信を介して接続可能に構成され、ユーザーＩＤに関連付けて、少なくとも最新のＩＣチップの製造番号及び上記ＩＣチップが再発行された際に過去に関連付けられていた上記ＩＣチップの製造番号と、ユーザーＩＤと、当該ユーザーアカウントの有効又は無効を表すアカウント属性情報を関連付けて記憶する記憶手段を有するコンピュータにより実行される方法であって、

上記ネットワーク端末が上記ＩＣチップから読み取り送信したＩＣチップの製造番号及びユーザーＩＤを含む認証要求を受信する処理と、

上記記憶手段を参照して、上記受信したユーザーＩＤと一致するユーザーＩＤが記憶されているか否か判別する処理と、

判別の結果、一致するユーザーＩＤが存在する場合に、上記記憶手段を参照して当該ユーザーＩＤに関連付けて記憶されている上記最新の製造番号が上記受信した製造番号と一致するか否か判別する処理と、

上記判別の結果、製造番号が一致しない場合に、上記ユーザーＩＤに関連付けられた製造番号が未登録か否かを判別する処理と、

上記判別の結果、製造番号が未登録であると判別された場合に、上記受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶することで新規登録処理を行い、また上記判別の結果、製造番号が未登録ではないと判別され、かつ、上記記憶手段に記憶されている過去の製造番号と一致しない場合には、上記ネットワーク端末から受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶するとともにアカウント属性情報を有効に変更する更新処理を行う処理と、

を行うことを特徴とする認証方法。

【請求項５】

ＩＣチップを識別する製造番号と、ユーザーを識別するユーザーＩＤとを記憶するＩＣチップと、

上記ＩＣチップに記憶されているデータを読み取る読取手段と、

上記読み取ったＩＣチップのデータをサーバに対して送信することで認証要求を行い、認証が正しい場合に所定の動作を行うネットワーク端末とを有し、上記ネットワーク端末に通信を介して接続可能に構成され、ユーザーＩＤに関連付けて、少なくとも、最新の上記ＩＣチップの製造番号及び上記ＩＣチップが再発行された際に過去に関連付けられていた上記ＩＣチップの製造番号と、当該ユーザーＩＤがアカウントとして有効又は無効を表すアカウント属性情報を関連付けて記憶する記憶手段を有するコンピュータを、認証装置として機能させるためのコンピュータプログラムであって、

上記コンピュータに対して、

上記ネットワーク端末が、上記ＩＣチップから読み取り、送信したＩＣチップの製造番号及びユーザーＩＤを含む認証要求を受信する処理と、

上記記憶手段を参照して、上記受信したユーザーＩＤと一致するユーザーＩＤが記憶されているか否か判別する処理と、

判別の結果、一致するユーザーＩＤが存在する場合に、上記記憶手段を参照して当該ユーザーＩＤに関連付けて記憶されている上記最新の製造番号が上記受信した製造番号と一致するか否か判別する処理と、

上記判別の結果、製造番号が一致しない場合に、上記ユーザーＩＤに関連付けられた製造番号が未登録か否かを判別する処理と、

上記判別の結果、製造番号が未登録であると判別された場合に、上記受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶することで新規登録処理を行い、また上記判別の結果、製造番号が未登録ではないと判別され、かつ、上記記憶手段に記憶されている過去の製造番号と一致しない場合には、上記ネットワーク端末から受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶するとともにアカウント属性情

10

20

30

40

50

報を有効に変更する更新処理を行う処理と、
を行わせるコンピュータプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ネットワーク内での個体認証を行う仕組みに関するものであり、特に、Windows（登録商標）ネットワーク内での個体認証を行う際に、ＩＣカードや携帯電話といったＩＣチップ搭載機器の製造番号とユーザーの識別番号とをActive Directoryに自動的に登録、更新等する仕組みに好適な技術に関する。 10

【背景技術】

【0002】

最近、様々なシステムの認証やデバイス認証を統合する統合認証システムを導入する企業が増えている。これは、複数のシステム開発によって乱立したユーザー認証データベースを統合することにより、その管理を一元化することを目的としている。

【0003】

また、様々なシステムの認証やデバイス認証を行う上でシングルサインオン認証という仕組みも存在する。これは、一つのユーザーアカウントで様々なシステムやデバイスの認証を行うのでユーザー認証テーブルは一つになり、その乱立を防ぐことを目的としている。 20

【0004】

このように、統合認証システムやシングルサインオン認証という仕組みで様々なシステムやデバイスの認証を行うことにより、ユーザー認証テーブルの複雑な管理を簡素化するということを目的とした製品が世の中に広がっている。

【0005】

ユーザー管理の仕組みとしては、サーバが、発生させた乱数と共通鍵をクライアントに送信し、クライアントから受信した機器識別子を共通鍵で復号し、機器識別子に対応する公開鍵で受信した乱数を復号し、復号された乱数と発生させた乱数とを比較照合して機器認証を行い、クライアントが、サーバからの乱数と共通鍵をＩＣカードに出力し、ＩＣカードからの乱数と暗号化された機器識別子をサーバに送信し、ＩＣカードが、クライアントからの乱数を秘密鍵で暗号化し、機器識別子を共通鍵で暗号化し、暗号化された乱数及び機器識別子をクライアントに出力し、クライアントからの更新データを秘密鍵で復号して、更新データでＩＣカード内の書き替えを行うデータ更新システムがある（特許文献１）。 30

【0006】

【特許文献１】特開２００６－０２４２３７

【発明の開示】

【発明が解決しようとする課題】

【0007】 40

しかし、Windows（登録商標）ネットワークを組んでいる多くの企業ではActive Directoryによってネットワーク認証を行っており、統合認証やシングルサインオン認証の仕組みを構築する場合にはActive Directoryの他にもユーザーアカウント管理をする必要があった。

【0008】

さらに、ＩＣカードによる入退室管理システムや複合機能プリンタの出力制御なども各製品毎にそのアカウント管理を行う仕組みの構築が必要になり、Windows（登録商標）ネットワーク管理者の作業負荷を高めてしまうという問題があった。

【0009】

ＩＣカードによる認証の場合、ＩＣカードの紛失や破損の度に、管理者がユーザー（ユー 50

ザＩＤなど）とＩＣカード（ＩＣカードの製造番号など）を紐付ける情報を修正しなければならず、大変手間がかかり効率的ではないという問題があった。

【００１０】

また、複数のユーザーアカウントデータベースを管理するということは、ユーザーアカウント登録等の作業を担当者が行う必要があるため、情報漏洩の可能性が高まってしまい、企業の情報漏洩防止の観点からも好ましくないという問題もあった。

【００１１】

本発明は、上述の問題及び課題を解決するためになされた発明であって、ネットワーク上のデバイス認証データベースを集約することで管理の煩雑さを軽減するとともに、ユーザーとＩＣカード等のＩＣチップの関連付け情報を自動的に登録・修正するための仕組みを提供することを目的とする。

10

【課題を解決するための手段】

【００１２】

本発明の一の観点にかかる認証装置は、ＩＣチップを識別する製造番号と、ユーザーを識別するユーザーＩＤとを記憶するＩＣチップと、上記ＩＣチップに記憶されているデータを読み取る読取手段と、上記読み取ったＩＣチップのデータをサーバに対して送信することで認証要求を行い、認証が正しい場合に所定の動作を行うネットワーク端末とを有し、上記ネットワーク端末に通信を介して接続可能に構成されたサーバであって、ユーザーＩＤに関連付けて、少なくとも、最新のＩＣチップの製造番号及び上記ＩＣチップが再発行された際に過去に関連付けられていた上記ＩＣチップの製造番号と、ユーザーＩＤと、当該ユーザーアカウントの有効又は無効を表すアカウント属性情報を関連付けて記憶する記憶手段と、上記ネットワーク端末が、上記ＩＣチップから読み取り、送信したＩＣチップの製造番号及びユーザーＩＤを含む認証要求を受信する受信手段と、上記記憶手段を参照して、上記受信したユーザーＩＤと一致するユーザーＩＤが記憶されているか否か判別する第１処理手段と、判別の結果、一致するユーザーＩＤが存在する場合に、上記記憶手段を参照して当該ユーザーＩＤに関連付けて記憶されている上記最新の製造番号が上記受信した製造番号と一致するか否か判別する第２処理手段と、上記判別の結果、製造番号が一致しない場合に、上記ユーザーＩＤに関連付けてられた製造番号が未登録か否かを判別する第３処理手段と、上記判別の結果、製造番号が未登録であると判別された場合に、上記受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶することで新規登録処理を行い、また上記判別の結果、製造番号が未登録ではないと判別され、かつ、上記記憶手段に記憶されている過去の製造番号と一致しない場合には、上記ネットワーク端末から受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶するとともにアカウント属性情報を有効に変更する更新処理を行う第４の処理手段を有することを特徴とする認証装置。

20

30

【００１３】

上記ネットワーク端末は、所定の動作を行うための組織単位情報を記憶しており、上記サーバから通知された組織単位情報が上記予め記憶されている組織単位情報に一致する場合に所定の動作を行うようになっており、上記記憶手段には、組織単位情報がさらに記憶されており、上記第２の処理手段により製造番号が一致すると判別された場合、又は上記第４の手段により新規登録処理又は更新処理が行われた場合に、上記記憶手段に記憶されている当該ＩＣチップのアカウント属性情報を上記ネットワーク端末に送信して上記ネットワーク端末に対して所定の処理を実行させる第５処理手段とを有してもよい。

40

【００１４】

上記ＩＣチップには、暗号化キーを使用するか否かを表すシステムコードがさらに記憶されており、上記ネットワーク端末は、上記暗号化キーを読み取り、暗号化キーを使用するか否かを判別する手段と、判別した結果、暗号化キーを使用しない場合には、上記第２処理手段が、上記記憶手段に記憶されている最新の製造番号が、上記受信した製造番号と一致するか否か判別することで認証処理を行うようにしてもよい。

【００１５】

50

本発明の一の観点にかかる認証方法は、ＩＣチップを識別する製造番号と、ユーザーを識別するユーザーＩＤとを記憶するＩＣチップと、上記ＩＣチップに記憶されているデータを読み取る読取手段と、上記読み取ったＩＣチップのデータをサーバに対して送信することで認証要求を行い、認証が正しい場合に所定の動作を行うネットワーク端末とを有し、上記ネットワーク端末に通信を介して接続可能に構成され、ユーザＩＤに関連付けて、少なくとも、最新のＩＣチップの製造番号及び上記ＩＣチップが再発行された際に過去に関連付けられていた上記ＩＣチップの製造番号と、ユーザーＩＤと、当該ユーザーアカウントの有効又は無効を表すアカウント属性情報を関連付けて記憶する記憶手段を有するコンピュータにより実行される方法であって、上記ネットワーク端末が上記ＩＣチップから読み取り送信したＩＣチップの製造番号及びユーザーＩＤを含む認証要求を受信する処理と、上記記憶手段を参照して、上記受信したユーザーＩＤと一致するユーザーＩＤが記憶されているか否か判別する処理と、判別の結果、一致するユーザーＩＤが存在する場合に、上記記憶手段を参照して当該ユーザーＩＤに関連付けて記憶されている上記最新の製造番号が上記受信した製造番号と一致するか否か判別する処理と、上記判別の結果、製造番号が一致しない場合に、上記ユーザーＩＤに関連付けてられた製造番号が未登録か否かを判別する処理と、上記判別の結果、製造番号が未登録であると判別され、かつ、上記記憶手段に記憶されている過去の製造番号と一致しない場合に、上記受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶することで新規登録処理を行い、また上記判別の結果、製造番号が未登録ではないと判別された場合には、上記ネットワーク端末から受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶するとともにアカウント属性情報を有効に変更する更新処理を行う処理とを行うことを特徴とする。

10

20

【００１６】

ＩＣチップを識別する製造番号と、ユーザーを識別するユーザーＩＤとを記憶するＩＣチップと、上記ＩＣチップに記憶されているデータを読み取る読取手段と、上記読み取ったＩＣチップのデータをサーバに対して送信することで認証要求を行い、認証が正しい場合に所定の動作を行うネットワーク端末とを有し、上記ネットワーク端末に通信を介して接続可能に構成され、ユーザーＩＤに関連付けて、少なくとも、最新の上記ＩＣチップの製造番号及び上記ＩＣチップが再発行された際に過去に関連付けられていた上記ＩＣチップの製造番号と、当該ユーザーＩＤがアカウントとして有効又は無効を表すアカウント属性情報を関連付けて記憶する記憶手段を有するコンピュータを、認証装置として機能させるためのコンピュータプログラムであって、上記コンピュータに対して、上記ネットワーク端末が、上記ＩＣチップから読み取り、送信したＩＣチップの製造番号及びユーザーＩＤを含む認証要求を受信する処理と、上記記憶手段を参照して、上記受信したユーザーＩＤと一致するユーザーＩＤが記憶されているか否か判別する処理と、判別の結果、一致するユーザーＩＤが存在する場合に、上記記憶手段を参照して当該ユーザーＩＤに関連付けて記憶されている上記最新の製造番号が上記受信した製造番号と一致するか否か判別する処理と、上記判別の結果、製造番号が一致しない場合に、上記ユーザーＩＤに関連付けられた製造番号が未登録か否かを判別する処理と、上記判別の結果、製造番号が未登録であると判別された場合に、上記受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶することで新規登録処理を行い、また上記判別の結果、製造番号が未登録ではないと判別された場合には、上記ネットワーク端末から受信した製造番号を上記ユーザーＩＤと関連付けて上記記憶手段に記憶するとともにアカウント属性情報を有効に変更する更新処理を行う処理とを行わせるコンピュータプログラム。

30

40

【発明の効果】

【００１７】

本発明によれば、ネットワーク上でのＩＣカードや携帯電話などのＩＣチップ搭載デバイスのネットワーク認証を一元管理することができる。

また、ＩＣカードや携帯電話などのＩＣチップ搭載デバイスを紛失・破損した場合なども、ネットワーク管理者がその紐付け情報を修正することなく、新しいＩＣチップ搭載デバイスをリーダーにかざすだけでユーザー情報とＩＣチップ情報の関連付けを自動的に行

50

うことが可能となる。

【発明を実施するための最良の形態】

【0018】

以下、本発明の実施形態に係る実施形態について図面を参照して説明する。

図1は本発明に係る一の実施形態の全体概要を示した模式図である。

図1において、本発明では、Active Directoryサーバ1と、Active Directoryサーバ1と通信を介して接続可能に構成されたネットワーク端末2、ネットワーク端末2に接続されたICチップリーダーライター3、ICチップ搭載デバイス4、入退室の履歴を更新管理するデータベースサーバ5を有している。

【0019】

Active Directoryサーバ1は、Windows（登録商標）ネットワーク内のネットワーク認証を行うサーバである。このActive Directoryサーバ1は、そのActive Directoryデータベースに図2に示すように、ユーザーを識別するためのユーザーIDに関連付けて、少なくとも、パスワード、ICチップ製造番号が関連付けて記憶できるようになっており、さらにこれらに加えてこの例ではユーザーが属する組織単位情報（OU：Organizational Unit）、アカウント属性の有効又は無効が記憶できるようになっている。また、開錠条件として、ネットワーク端末2の識別情報に対応付けて、当該ネットワーク端末2が設置されている電子錠を開錠できる組織単位情報が記憶されている。

ICチップの製造番号は、現在ユーザーにより使用されている最新のICチップの製造番号（本例では3333333333）と、過去にこのユーザーIDに対して、ICチップが再発行されていた場合には、当該過去のICチップの製造番号（本例では、0000000000と1111111111）が関連付けて記憶できるようになっている。

このActive Directoryサーバ1のユーザーIDとICチップ製造番号が、Windows（登録商標）ネットワークへの認証を許可されたユーザーとICチップ搭載デバイスを紐付けることとなる。

【0020】

ネットワーク端末2は、Windows（登録商標）ネットワーク回線を介してActive Directoryサーバ1に接続可能に構成されている。

このネットワーク端末2としては、例えば、いわゆるパーソナルコンピュータ、PDA（Personal Data Assistance）などで構成することができる。このICチップ搭載デバイス4としては、例えば、いわゆるICカード、携帯電話、RFID（Radio Frequency Identification）などで構成することができる。

このネットワーク端末2は、ICチップリーダーライター3を制御して、ICチップ搭載デバイス4のメモリに記憶されているデータを読み取り、認証する処理を行う。

【0021】

また、ネットワーク端末2は、LANやWANなどを介して通信処理を行う通信制御部を有しており、この通信制御部により、Active Directoryサーバ1やデータベースサーバ5との間で所定のデータの送受信処理を行うことができる。

ネットワーク端末2は、ICチップリーダーライター3により読み取ったデータをActive Directoryサーバ1に対して送信して照合を要求することで、ICチップ搭載デバイス4の認証をする認証処理部を有している。

本例では、ネットワーク端末2は、そのメモリやハードディスクドライブなどの記憶部に、予め開錠条件として、開錠することができる組織単位情報（OU）が記憶されている。これにより、Active Directoryサーバ1による認証が完了し、送信されたユーザーの組織単位情報が、予め記憶部に記憶されている組織単位情報に一致するか否か判別し、判別の結果、一致する場合には開錠を行うように構成されている。

また、ネットワーク端末2は、認証結果のログをデータベースサーバ5へ送信して、履歴情報を更新する履歴更新処理部も有している。

また、取得したデータとActive Directoryを照合して見つかった不整合箇所を修正する修正処理部を有している。

10

20

30

40

50

なお、このネットワーク端末 2 は、本例では、ＩＣカードリーダーライター 3 と接続可能なネットワーク高機能端末により構成することができる。

【 0 0 2 2 】

ＩＣチップリーダーライター 3 は、ネットワーク端末 2 と接続して、ネットワーク端末 2 からの要求により、ＩＣチップ搭載デバイス 4 のＩＣチップ内のデータを読み書きする装置である。

なお、本例では、ＩＣチップリーダーライター 3 とネットワーク端末 2 とは別装置として構成した例について説明したが、ＩＣチップリーダーライター 3 とネットワーク端末 2 が一体化された装置としてもよい。

【 0 0 2 3 】

ＩＣチップ搭載デバイス 4 は、入退室者が保持するデバイスである。具体的には、ＩＣチップ搭載デバイス 4 は、例えば、ＩＣカード、携帯電話、ＲＦＩＤチップなどにより構成することができる。

このＩＣチップ搭載デバイス 4 はメモリを有しており、このメモリに入退室者を識別するためのユーザーＩＤと、ＩＣチップ搭載デバイス 4 に割り当てられた固有のデバイス製造番号が記憶できるようになっている。

また、その他、ＩＣチップ搭載デバイス 4 には、入退室者の氏名などの個人情報や、パスワードを記憶してもよい。

【 0 0 2 4 】

データベースサーバ 5 は、ネットワーク内でのネットワーク認証の履歴ログデータを保存・管理する装置である。

このデータベースサーバ 5 は、ネットワークに接続されており、該ネットワーク回線を通じて認証履歴ログ情報を受信することで、履歴データベースを更新する。

【 0 0 2 5 】

次に、上述の実施形態による処理の方法について説明する。

まず全体の概略について図 1 を参照して説明する。

図 1 に示した例は、入退室者が保持するＩＣチップ搭載デバイス 4 を使って、ネットワーク端末 2 が制御している電子錠を開錠して入退室を行う場合の例である。

まず、入退室者が保持しているＩＣチップ搭載デバイス 4 をＩＣチップリーダーライター 3 の端子に接続又はかざすことで、ＩＣチップリーダーライター 3 がＩＣチップ内のデータを読み取る（Ｓ１）。

この際読み取る情報としては、少なくともＩＣチップ搭載デバイス 4 のＩＣチップ内に記憶されているユーザーＩＤとＩＣチップの製造番号が含まれており、さらに入退室者の氏名などの個人情報やパスワードなどのデータが含まれてもよい。

【 0 0 2 6 】

ＩＣチップ内のデータが読み取られると、ネットワーク端末 2 が、Active Directoryサーバ 1 に対して読み取ったデータを送信して、ＩＣチップ内のデータの認証要求を行う（Ｓ２）。

【 0 0 2 7 】

Active Directoryサーバ 1 は、受信したデータに基づいて認証処理を行い、承認又は否認の結果をネットワーク端末 2 に送信する（Ｓ３）。

また、この際、Active Directoryサーバ 1 は、必要に応じて、Active Directoryデータベースを参照して、後述するＩＣチップ搭載デバイス 4 のデータの登録、更新処理を行う。

【 0 0 2 8 】

Active Directoryサーバ 1 から承認又は否認の通知があると、ネットワーク端末 2 は承認の際は開錠するなどの所定の処理を行うとともに、当該ログデータをデータベースサーバ 5 に送信する（Ｓ４）。なお、否認の場合は、ネットワーク端末 2 は、エラーメッセージを表示するなどして、当該ログデータをデータベースサーバ 5 に送信する。

これにより、データベースサーバ 5 は、送信されたログデータを履歴データベースに記

10

20

30

40

50

憶して、一連の処理を終了する。

【 0 0 2 9 】

次に、上述の認証又は否認処理（ S 3 ）におけるActive Directoryサーバ 1 の詳細な処理について、図 3 を参照して説明する。

図 3 において、ネットワーク端末 2 は、 I C チップのSystem Codeを読み取り（ S 1 0 1 ）、システムコードが暗号化キーを使用する設定となっているかどうかを判別する（ S 1 0 2 ）。

判別の結果、暗号化キーを使用する場合には、後述するモード 2 の処理が開始される。

【 0 0 3 0 】

判別の結果使用しない場合には、モード 1 の処理として、ネットワーク端末 2 は、 I C チップの製造番号を読み取り、これをActive Directoryサーバ 1 に送信する（ S 1 0 3 ）。

10

【 0 0 3 1 】

Active Directoryサーバ 1 は、Active Directoryデータベースを検索して、最新の製造番号を照合し（ S 1 0 4 ）、該当する製造番号が存在するか否かを判別する（ S 1 0 5 ）。

この判別の結果、存在しない場合には、後述するエラー処理が行われる。

【 0 0 3 2 】

また、判別の結果、製造番号がActive Directoryデータベースに存在する場合には、Active Directoryサーバ 1 は、Active Directoryデータベースに記憶されている当該製造番号のアカウント属性及び、組織単位情報（ O U : Organizational Unit ）を取得する（ S 1 0 6 ）。

20

【 0 0 3 3 】

Active Directoryサーバ 1 は、アカウント属性情報が有効か無効かの照合を行い（ S 1 0 7 、 S 1 0 8 ）、無効の場合には、後述するエラー処理を行う。

また、判別の結果、アカウント属性情報が有効な場合には、Active Directoryサーバ 1 は、組織単位情報（ O U ）の照合を行い開錠条件に合致する組織単位情報が否かを判別する（ S 1 0 9 、 S 1 1 0 ）。

判別の結果、開錠条件に合致しない場合には、後述するエラー処理を行う。

【 0 0 3 4 】

また、判別の結果、開錠条件に合致する場合には、Active Directoryサーバ 1 は、電子錠開錠指示データと組織単位情報をネットワーク端末 2 に送信し、ネットワーク端末 2 は受信した組織単位情報が予め記憶部に記憶されている開錠できる組織単位情報に一致するか判別して、該当する場合には電子錠を開錠する処理を行う（ S 1 1 1 ）。

30

【 0 0 3 5 】

また、ネットワーク端末 2 は、開錠を行ったログデータをデータベースサーバ 5 に送信することで、データベースサーバ 5 はログ情報をデータベースに記憶して（ S 1 1 2 ）、処理を終了する。

【 0 0 3 6 】

また、上述の S 1 0 2 の処理で暗号化キーを使用すると判別された場合（モード 2 ）の処理について、図 4 を参照して説明する。

40

図 4 において、ネットワーク端末 2 は、 I C チップの製造番号と、 I C チップに記憶されているユーザー I D を読み取り、Active Directoryサーバ 1 に送信する（ S 2 0 1 ）。

【 0 0 3 7 】

Active Directoryサーバ 1 は、Active Directoryデータベースを参照してユーザー I D の照合を行い、受信したユーザー I D に一致するユーザー I D が存在するか否かを判別する（ S 2 0 2 、 S 2 0 3 ）。

判別の結果、一致するユーザー I D が存在しない場合は、不正なユーザー I D として後述するエラー処理を行う。

【 0 0 3 8 】

また、判別の結果、一致するユーザー I D が存在する場合には、Active Directoryサー

50

サーバ1は、Active Directoryデータベースを参照して、ICチップの製造番号が、S203の処理で特定されたユーザーIDに関連付けられて記憶されている最新の製造番号と一致するか否かを判別する(S204、S205)。

判別の結果、一致しない場合には、後述するモード3の新規登録又は再発行処理に移る。

【0039】

また判別の結果、製造番号が一致する場合には、Active Directoryサーバ1は、Active Directoryデータベースを参照して属性情報及びActive Directoryデータベースに記憶されているユーザーIDのアカウント属性情報及び、組織単位情報(OU: Organizational Unit)を取得する(S206)。

10

【0040】

Active Directoryサーバ1は、アカウント属性情報が有効か無効かの照合を行い(S207、S208)、無効の場合には、後述するエラー処理を行う。

また、判別の結果、属性情報が有効な場合には、Active Directoryサーバ1は、Active Directoryデータベースを参照して、組織単位情報の照合を行い開錠条件に合致する組織単位情報が否かを判別する(S209、S210)。

判別の結果、開錠条件に合致しない場合には、後述するエラー処理を行う。

【0041】

また、判別の結果、開錠条件に合致する場合には、Active Directoryサーバ1は、電子錠開錠指示データと組織単位情報をネットワーク端末2に送信し、ネットワーク端末2は受信した組織単位情報が予め記憶部に記憶されている開錠できる組織単位情報に一致するか判別して、該当する場合には電子錠を開錠する処理を行う(S211)。

20

【0042】

また、ネットワーク端末2は、開錠を行ったログデータをデータベースサーバ5に送信することで、データベースサーバ5はログ情報を履歴データベースに記憶して(S212)、処理を終了する。

【0043】

次に、S205の処理で、製造番号が登録されておらず無効と判別された場合の場合(新規登録又は再発行処理)の処理について図5を参照して説明する。

図5において、前述のS205の処理で、製造番号が一致しないと判別された場合、Active Directoryサーバ1は、製造番号更新処理を開始し、Active Directoryサーバ1は、Active Directoryデータベースを参照して、製造番号が登録されていない状態か否かを判別する(S301)。

30

【0044】

判別の結果、製造番号が登録されていない場合、即ち、ユーザーIDは登録されているがICチップの製造番号が登録されていない場合には、新規登録としてネットワーク端末2から送信された製造番号を、既に登録されているユーザーIDと関連付けて登録し(S302)、番号更新処理を終了して、前述のS206以下の処理を行う。

【0045】

また、S301の処理で製造番号が一致しないと判別された場合には、Active Directoryサーバ1は、取得したICチップの製造番号が、Active Directoryデータベースに記憶されている過去のICチップの製造番号に一致しないか否かを判別する(S303)。

40

判別の結果、過去のICチップの製造番号と一致する場合には、紛失したカードを誰かが使用している場合であるとして、後述するエラー処理を行う。

また、判別の結果、過去のICチップの製造番号とは一致しないと判別された場合には、Active Directoryサーバ1は、Active Directoryデータベースを参照して、アカウント属性情報及び、組織単位情報(OU: Organizational Unit)を取得する(S304)。

【0046】

Active Directoryサーバ1は、アカウント属性情報が無効となっているか否かを照合を行う(S305、S306)。

50

すなわち、ＩＣチップ搭載デバイス４を紛失した場合には、ユーザーが紛失を届け出ており、システム管理者によってアカウント属性情報が無効となっているため、システム属性が無効となっているか否か判別することで、紛失したＩＣチップ搭載デバイス４が再発行されたか否か判別する。

【００４７】

判別の結果、アカウント属性が無効でなく、有効となっている場合には、不正なＩＣチップ搭載デバイスとして、後述するエラー処理を行う。

【００４８】

また、判別の結果、アカウント属性情報が無効となっている場合には、Active Directoryサーバ１は、当該ユーザーＩＤに関連付けられているActive Directoryデータベースの製造番号を、ＩＣチップ搭載デバイス４から読み取った製造番号に更新し（Ｓ３０７）、当該製造番号のステータスを有効に変更して再発行処理を行い（Ｓ３０８）、前述のＳ２０６以下の処理を行う。

【００４９】

次に、図６を参照してエラー処理の流れについて説明する。

図６において、エラー処理通知されると、Active Directoryサーバ１はエラー処理を開始し、不正侵入警告を発する（Ｓ４０１）。これにより、システム管理者などに対してアラームを通知するなどの処理を行う。

そして、Active Directoryサーバ１は、エラー処理をデータベースサーバ５に通知することで、データベースサーバ５はエラー処理のログを記憶して（Ｓ４０２）、エラー処理を終了する。

【００５０】

このように、上述の実施形態によれば、Windows（登録商標）ネットワーク上でのＩＣカードや携帯電話などのＩＣチップ搭載デバイス４のネットワーク認証を、Active Directoryサーバ１で一元管理できる。

また、ＩＣカードや携帯電話などのＩＣチップ搭載デバイス４を紛失・破損した場合なども、ネットワーク管理者がその紐付け情報を修正することなく、上述の更新処理で新しいＩＣチップ搭載デバイス４をＩＣチップリーダーライター３にかざすだけでユーザー情報とＩＣチップ情報の関連付けを自動的に行うことができ、人手による登録の場合のミスがなくなり、効率的にかつ正確に登録・更新処理を行うことができる。

【符号の説明】

【００５１】

- １ Active Directoryサーバ
- ２ ネットワーク端末
- ３ ＩＣチップリーダーライター
- ４ ＩＣチップ搭載デバイス
- ５ データベースサーバ

【図面の簡単な説明】

【００５２】

【図１】本発明の実施形態にかかるシステムの全体構成を表す概略図。

【図２】本実施形態のActive Directoryデータベースのデータ項目を示した図。

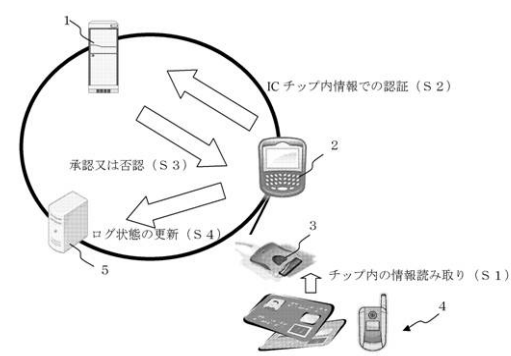
【図３】本実施形態にかかる処理フローを示した図。

【図４】本実施形態にかかるモード２の処理フローを示した図。

【図５】本実施形態にかかるモード３の処理フローを示した図。

【図６】本実施形態にかかるモード４の処理フローを示した図。

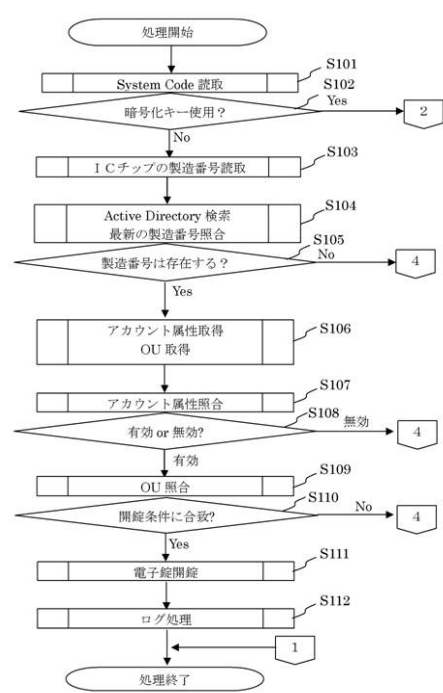
【 図 1 】



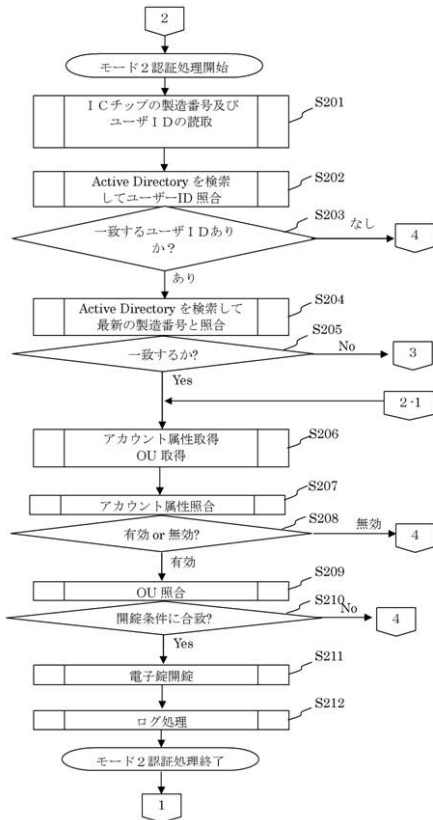
【 図 2 】

ユーザーID	パスワード	最新の製造番号	過去の製造番号	OU	アカウント属性
ABC01	***ab1	2222222222	0000000000 1111111111	KK	有効
ABC02	***ab2	3333333333	-	KB	無効

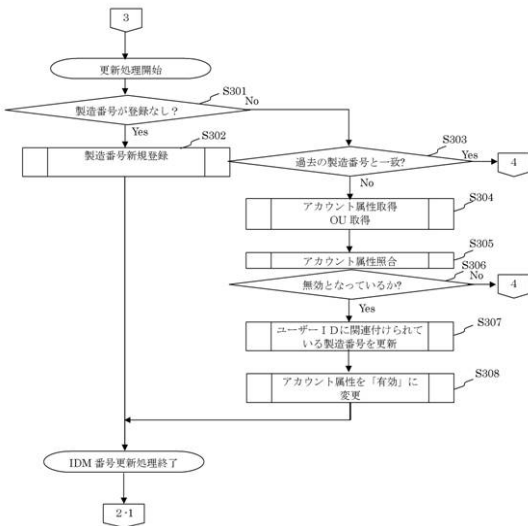
【 図 3 】



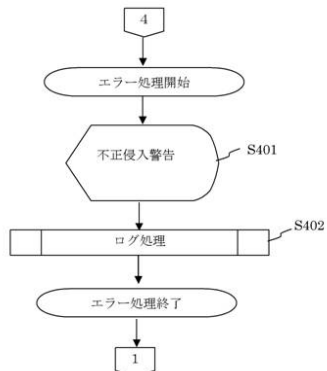
【図 4】



【図 5】



【図 6】



フロントページの続き

F ターム(参考) 5B058 CA17 KA31
5B285 AA01 BA00 BA03 CA41 CB02 CB07 CB42 CB44 CB53 CB62
CB64 CB72
5J104 AA07 AA16 EA03 EA15 EA16 EA22 KA02 KA04 NA05 NA35
NA38 PA07