(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2007-220120
(P2007-220120A)
(43)公開日　平成19年8月30日(2007.8.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06K 17/00	(2006.01)	G06K	17/00	T	5B058
H04L 9/32	(2006.01)	H04L	9/00	673E	5J104

審査請求 未請求　請求項の数 17　ＯＬ　（全 17 頁）

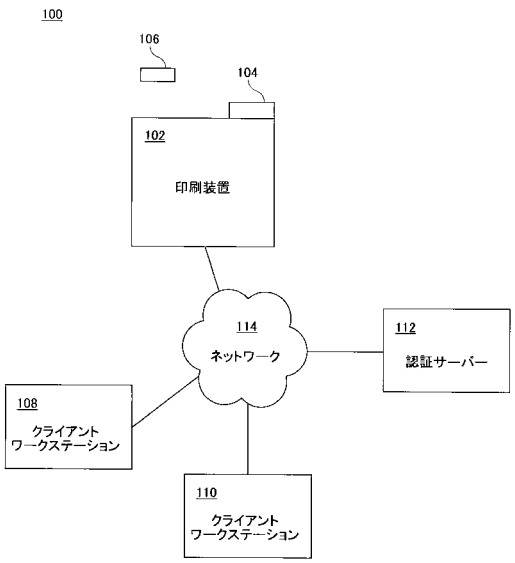
(21)出願番号　特願2007-33985(P2007-33985)
(22)出願日　平成19年2月14日(2007.2.14)
(31)優先権主張番号　11/355,113
(32)優先日　平成18年2月14日(2006.2.14)
(33)優先権主張国　米国(US)

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　ジアン　ホォン
アメリカ合衆国，カリフォルニア州　９５０１４－５９２４，クパチーノ　リザルツ　ウェイ　４　リコー　コーポレイション内
(72)発明者　サム　ワン
アメリカ合衆国，カリフォルニア州　９５０１４－５９２４，クパチーノ　リザルツ　ウェイ　４　リコー　コーポレイション内

最終頁に続く

(54)【発明の名称】スマートカードを認証するための装置、方法及びコンピュータ読み取り可能な媒体

(57)【要約】
【課題】スマートカード及びデータモデルのような認証要素に対して認証システムが変更を加える柔軟性を拡大すること。
【解決手段】スマートカード認証用に用意される手法は、動的に変更可能なデータを利用し、スマートカードを認証し、デフォルト環境ではサポートされていないバックエンドシステムと通信する。新たなスマートカードタイプ、カードについての新たなデータモデル、又は新たなリモート認証手段のような認証環境の変化を反映するように、データはユーザにより動的に再設定可能である。
【選択図】図１



【特許請求の範囲】
【請求項１】
スマートカードを認証するよう構築されたスマートカード認証プロセスを実行するスマートカード認証装置であって、当該スマートカード認証装置は、
スマートカードを識別し、
前記スマートカードが当該スマートカード認証装置のデフォルトコンフィギュレーションによってサポートされているか否かを確認し、
前記スマートカードがデフォルトコンフィギュレーションによってサポートされていた場合には、前記デフォルトコンフィギュレーションで用意されている命令を用いて前記スマートカードから認証に関連するデータを読み取り、
前記スマートカードがデフォルトコンフィギュレーションによってサポートされていなかった場合には、別のコンフィギュレーションデータからデータを読み取り、前記スマートカードが、前記別のコンフィギュレーションデータから読み取ったデータによってサポートされているか否かを確認し、
前記スマートカードが前記別のコンフィギュレーションデータによってサポートされていた場合には、前記別のコンフィギュレーションデータから読み取った前記データを用いて、前記スマートカードから認証に関連するデータを読み取り、
前記スマートカード認証プロセス及び前記スマートカードから読み取った認証に関連する前記データを用いて、前記スマートカードを認証しようとする
ように構成されることを特徴とするスマートカード認証装置。
【請求項２】
前記別のコンフィギュレーションデータが、当該スマートカード認証装置にローカルに格納されている
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項３】
前記別のコンフィギュレーションデータが、XMLフォーマットのデータを有する
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項４】
前記別のコンフィギュレーションデータが、テキストファイルを有する
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項５】
前記別のコンフィギュレーションデータが、ローカルユーザ認証に関連するデータを含む
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項６】
前記別のコンフィギュレーションデータが、サーバーベース認証に関連するデータを含む
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項７】
前記別のコンフィギュレーションデータが、ローカルユーザ認証及びサーバーベース認証の双方に関連するデータを含む
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項８】
前記別のコンフィギュレーションデータが、編集可能である
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項９】
前記別のコンフィギュレーションデータが、暗号化される
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項１０】
当該スマートカード認証装置が、

前記スマートカードが成功裏に認証されなかった場合に、前記スマートカード認証プロセスを実行する装置に通信可能に結合される印刷装置の複数の機能に対するアクセスを制限するよう構成される
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項１１】
当該スマートカード認証装置が、前記別のコンフィギュレーションデータを表示及び編集するためのウェブベースインターフェースを用意するよう構成される
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項１２】
前記スマートカードから読み取った認証に関する前記データが、ディジタル署名を有する
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項１３】
前記スマートカードから読み取った認証に関する前記データが、LDAPデータを有する
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項１４】
当該スマートカード認証装置が、前記スマートカードからの認証に関連するデータへのアクセス前に、セキュリティコードの入力を要求するよう構成される
ことを特徴とする請求項１記載のスマートカード認証装置。
【請求項１５】
前記セキュリティコードが、PIN番号である
ことを特徴とする請求項１４記載のスマートカード認証装置。
【請求項１６】
認証データが格納され、スマートカード読取装置に挿入されるスマートカードを識別するステップと（前記スマートカード読取装置は、スマートカード認証用命令を実行する装置に通信可能に結合される）、
前記スマートカードからデータを読み取るようにデフォルト命令を実行するステップと、
前記スマートカードに格納されている前記認証データが前記デフォルト命令で読み取り可能であるか否かを確認し、可能であれば、前記スマートカードから前記認証データを読み取るステップと、
前記スマートカードに格納されている前記認証データが前記デフォルト命令で読み取り可能でなかった場合に、前記スマートカードに格納されている前記認証データを読み取るための命令を有する、前記デフォルト命令とは別のコンフィギュレーションデータを読み取るステップと、
前記スマートカードを認証するステップと、
を有することを特徴とするスマートカード認証方法。
【請求項１７】
スマートカード認証用の１以上の命令シーケンスを運ぶコンピュータ読み取り可能な媒体であって、前記１以上の命令シーケンスは、
認証データが格納され、スマートカード読取装置に挿入されるスマートカードを識別するステップと（前記スマートカード読取装置は、スマートカード認証用命令を実行する装置に通信可能に結合される）、
前記スマートカードからデータを読み取るようにデフォルト命令を実行するステップと、
前記スマートカードに格納されている前記認証データが前記デフォルト命令で読み取り可能であるか否かを確認し、可能であれば、前記スマートカードから前記認証データを読み取るステップと、
前記スマートカードに格納されている前記認証データが前記デフォルト命令で読み取り可能でなかった場合に、前記スマートカードに格納されている前記認証データを読み取る

ための命令を有する、前記デフォルト命令とは別のコンフィギュレーションデータを読み取るステップと、
前記スマートカードを認証するステップと、
を１以上のプロセッサに実行させることを特徴とするコンピュータ読み取り可能な媒体。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は一般に認証システムに関連し、特に複数のカード及びサービスをサポートするスマートカード認証システムのための手法に関する。

【背景技術】
【０００２】
この（背景技術の）セクションで説明される手法は探求可能な手法であるかもしれないが、必ずしも過去に想定又は探求された手法であるとは限らない。従って特に示されていない限り、このセクションで説明される手法は本願の特許請求の範囲に対する従来技術でないかもしれないし、このセクションに含まれることをもって出願人が従来技術であると認めているわけではない。
【０００３】
企業は日々の業務で印刷装置を頼りにしている。１つの建物又は部署の中でしばしば多くの印刷装置が利用可能であり、その各々はいくつもの機能を備えている可能性がある。企業は、これらの装置を監視したり、アクセスを制御したり、使用度を追跡することを望む。これを行う１つの手法は「スマートカード」システムを利用することである。これらのシステムは、情報（通常的にはマイクロチップに組み込まれた情報）を格納することができる物理的なカードを利用する。スマートカードはユーザを個人的に識別するデータを含むかもしれない。このデータは或るスキーマ(schema)又はデータモデルにしばしば従う。この情報にアクセスできるカードリーダは、印刷装置に接続され、印刷装置と通信を行う。
【０００４】
例えば印刷装置を利用したいと思うユーザは、印刷装置に接続されたスマートカードリーダにスマートカードを挿入する。スマートカードリーダは、ユーザ名及びパスワード等のような認証データをカードから抽出し、そのデータを印刷装置に又は（しばしば遠隔している）バックエンドシステムに認証用に記憶されているデータと比較する。ユーザが認証されると、そのユーザの信用証明書に基づいて情報が印刷装置に伝送される。この情報はスマートカードのデータから又は別のソースから来てもよい。
【０００５】
例えば、あるユーザは印刷装置のカラー印刷機能にアクセスできないかもしれないし、別のユーザは装置のスキャナ機能を利用することしか認められていないかもしれない。
【０００６】
この認証手法の欠点は、認証システムを調整して様々なカードタイプ及び認証システムを利用できるようにする柔軟性に欠けることである。１つの例は、上述のシステムのユーザが新たなカードタイプ又はモデルを利用することを望む場合である。別の例は、上述のシステムのユーザがスマートカードのデータモデルを変更することを望む場合である。別の例は、上述のシステムのユーザが、サーバー、プロトコルタイプ又は他のシステム形態の変更によって、異なるバックエンドシステムを利用することを望む場合である。別の例は、認証を制限するアプリケーションが開発され、コンパイルされ、リリースされた後に、上述のシステムのユーザが別の環境で新たな顧客をサポートすることを望む場合である。
【０００７】
この問題に対する１つの手法は、新たなスマートカードタイプ、データモデル、バックエンド認証システム又は新たな環境をサポートするための認証アプリケーションを書き直

してコンパイルし直すことである。この手法には多くの欠点がある。１つは、新たなアプリケーションを書き直してコンパイルし直すのに多くの時間と労力を費やすかもしれないことである。例えばその変更が些細なものであり、新たなサーバーアドレスをバックエンド認証システムに追加するような場合でも、その労力は変更量に対してかなり釣り合っていない（多い）。２つ目は、新たな顧客及び新たなカード又はデータモデルをサポートするためにレギュラーベースで認証アプリケーションを更新することはユーザにとって法外に高価になるかもしれないことである。従って、スマートカード及びデータモデルのような認証要素に対して認証システムが変更を加える柔軟性を拡大する要請がある。

【発明の開示】

【発明が解決しようとする課題】

【０００８】

本発明の課題は、スマートカード及びデータモデルのような認証要素に対して認証システムが変更を加える柔軟性を拡大することである。

【課題を解決するための手段】

【０００９】

スマートカード認証用に用意される手法は、動的に変更可能なデータを利用し、スマートカードを認証し、デフォルト環境ではサポートされていないバックエンドシステムと通信する。新たなスマートカードタイプ、カードについての新たなデータモデル、又は新たなリモート認証手段のような認証環境の変化を反映するように、データはユーザにより動的に再設定可能である。

【００１０】

本手法は、所望の変更全てについて（マイナーであることは問題でなく）認証アプリケーションを書き直してコンパイルし直すのではなくユーザの設定可能なデータを定義することで、新たな追加的なスマートカード、データモデル及び／又はバックエンド認証システムをユーザがサポートできるようにする。本手法を用いることで、スマートカード認証システムは、新たなカスタマ、新たなスマートカード、新たなデータモデル、新たなバックエンド認証手段その他の変更をサポートするように迅速且つ効率的に再構築される。

【発明を実施するための最良の形態】

【００１１】

添付図面では同様な参照番号は同様な要素に関連する。

【００１２】

以下の説明では、説明の目的で、本発明の十分な理解をもたらすように多くの具体的詳細が述べられる。しかしながらこれらの具体的詳細によらず本発明は実施されてもよいことは当業者にとって明白であろう。場合によっては、本発明を曖昧にすることを避けるために、周知の構造及び装置がブロック図形式で描かれる。本発明の様々な形態は以下のセクションで説明される。

【００１３】

I. 概要

II. アーキテクチャ及び認証の詳細

III. ローカルユーザ信用証明認証

IV. サーバーベースのユーザ信用証明認証

V. ウェブベースインターフェース

VI. 実現手段

【実施例１】

【００１４】

I. 概要

スマートカード認証用に用意される手法は、動的に変更可能なデータを利用し、承認されていないスマートカードを認証し、デフォルト環境ではサポートされていないバックエンドシステムと通信する。新たなスマートカードタイプ、カードについての新たなデータモデル又は新たなリモート認証手段のような認証環境の変化を反映するように、データは

ユーザにより動的に再設定されてよい。

【００１５】

本発明の一実施例によれば、スマートカード認証モジュールは認証データを抽出するためにスマートカードリーダと通信する。スマートカード認証モジュールは１以上のデフォルトのスマートカードタイプ及びデータモデルについてのサポート機能を含む。サポートされていないカードタイプ又はデータモデルをユーザが利用したい場合には、スマートカード認証モジュールを制御するソフトウエアを書き直すのではなく、スマートカード認証モジュールによりアクセス可能な別個のデータが、新たなカードタイプ及び／又はデータモデルを認識するために動的に再構築され、新たなユーザ信用証明情報を取り出す命令を用意する。一実施例では、これは、デフォルトの所定のカードタイプ及び／又はデータモデルがユーザを認証するには不十分であった場合に、アクセスされたスマートカード認証モジュールによってアクセス可能なユーザの決めたコンフィギュレーションファイルを作成及び格納することで達成される。

【００１６】

本発明の一実施例によれば、ユーザの決めたコンフィギュレーションファイルが、デフォルト環境でサポートされていない新たなバックエンド認証システムをサポートするために使用される。新たなプロトコルに対してバックエンド認証サーバーをユーザが変更すると又は切り替えると、例えば、ユーザの決めたコンフィギュレーションファイルはスマートカード認証モジュールによって使用され、バックエンドサーバーと通信し、認証システムアプリケーション全体を書き直さずにユーザを認証する。一実施例では、スマートカード認証モジュールはローカル対リモートの認証目的で別々のモジュールに分割されてもよい。

【００１７】

一実施例の手法はウェブベースのインターフェースを含み、スマートカード認証モジュールで使用されるユーザの決めたコンフィギュレーションファイルをユーザが容易に変更できるようにする。

【００１８】

ここで説明される手法は、ユーザの設定可能なデータを定義することで新たな追加的なスマートカード、データモデル及びバックエンド認証システムをユーザがサポートすることを可能にし、所望の変更全てについて（変更が小さいことは問題でなく）認証アプリケーションを書き直してコンパイルし直す時間及び費用をかけずに済む。ここで説明される手法を利用することで、スマートカード認証システムは新たなカスタマ、新たなスマートカード、新たなデータモデル及び新たなバックエンド認証手段をサポートするように迅速且つ効率的に再構築される。

【００１９】

II. アーキテクチャ及び認証の詳細

図１は本発明の一実施例によるスマートカード認証システム構成１００を示すブロック図である。システム１００は、ユーザ認証機能に関連するデータを格納、処理及びアクセスすることができる少なくとも１つの印刷装置１０２を含む。印刷装置１０２の具体例は限定ではないが複写機、プリンタ　スキャナ及び複合装置(MFP)を含む。本発明の一実施例では、印刷装置はメモリ中の及び電子ストレージ中の認証モジュールを実行することができる。例えば、印刷装置１０２は認証ソフトウエアを実行し、スマートカードからのデータの読み込みを制御し、印刷装置１０２にローカルに又は遠隔的に格納されたデータベースに対してそのデータを問い合わせる。ユーザの認証に成功すると、印刷装置は、認証処理結果に基づいてそのユーザに利用可能な機能を確認し、それに従って印刷装置の機能へのユーザのアクセスを制限する。

【００２０】

印刷装置１０２は１以上のスマートカード１０６に格納されたデータを受信して読み取ることの可能なカードリーダ１０４に通信可能に結合される。カードリーダ１０４はディスプレイを利用することでユーザに情報を伝えることができる。更にカードリーダ１０４

は印刷装置に情報を送信すること及びそこから情報を受信することができる。スマートカード１０６は例えばカードに組み込まれたマイクロチップにデータを格納することができる。本発明の一実施例では、カードリーダ１０４はマイクロチップからデータを読み取る。スマートカード１０６に格納されているデータは或るモデル又はスキームに従い；例えばカードはユーザ名、社会保障番号、従業員ID及び誕生日を格納してもよい。別のカードは名前、住所、眼色及び社員番号のような様々なデータモデルを利用してもよい。

【００２１】

印刷装置１０２及びカードリーダ１０４はネットワーク１１４を介して１以上のクライアントワークステーション１０８，１１０及び／又はバックエンドサーバー１１２に通信可能に結合される。印刷装置１０２及びクライアントワークステーション１０８，１１０及び／又はバックエンドサーバー１１２の間でデータ交換機能をもたらす如何なる媒体又は手段でネットワーク１１４が実現されてもよい。ネットワーク１１４の具体例は、限定ではないが、ローカルエリアネットワーク(LAN)、広域ネットワーク(WAN)、イーサーネット又は１以上の地上、衛星若しくは無線リンクのようなネットワークを含む。特定の実施状況に依存して、ネットワーク１１４の一部分が有線接続であり、他の部分が無線接続でもよい。例えば、印刷装置１０２及び或るワークステーション１０８間の接続が有線接続であり、バックエンド認証サーバー１１２及び印刷装置１０２間の接続が無線接続でもよい。

【００２２】

ワークステーション１０８－１１０の構成要素（複数）はいっせいに又は別々に印刷装置１０２とデータを通信するよう機能する。例えばワークステーション１０８のユーザは印刷ジョブを記述するデータがワークステーション１０８から印刷装置１０２へ伝送されるようにしてもよい。一実施例によれば、本願で説明される手法を用いてユーザが認証されるまで、印刷ジョブは完了しない。

【００２３】

バックエンド認証サーバー１１２は、ここで説明される認証プロセスの一部として使用される。一実施例によれば、バックエンド認証サーバー１１２は印刷装置１０２と通信することができる。ユーザの信用証明は、スマートカードから読み取られ、印刷装置１０２で動作する認証ソフトウエアによってバックエンド認証サーバー１１２に通知される。バックエンド認証サーバー１１２はその信用証明を認証し、認証結果を反映するデータを印刷装置１０２に返す。認証処理結果に基づいて、このデータは、ユーザが認証されたか否か、如何なる機能がそのユーザに利用可能であるかを含んでよい。一実施例によれば、確認方式の認証処理、LDAPエンティティ及び他の手法のような様々なタイプの認証手法に基づいて、バックエンド認証サーバー１１２はユーザを認証することができる。

【００２４】

III. ローカルユーザ信用証明認証

図２は、本発明の一実施例によるローカルスマートカードベースの認証手法を示すフローチャート２００である。ステップ２０２では、印刷装置に通信可能に結合されたカードリーダにスマートカードをユーザが挿入する。本発明の一実施例によれば、カードリーダは、スマートカードから格納済みデータを読み取り、そのスマートカード及びタイプを判別するのに十分なデータを印刷装置で実行するプロセスに通知する。カードリーダは、そのカードに格納済みの全てのデータを読み取って伝送してもよいし、或いは認証用に限定した情報だけを先ず印刷装置に提供してもよい。例えばカードリーダはスマートカードのタイプ及びモデルに関連する情報だけを抽出及び通知してもよい。

【００２５】

ステップ２０４では、印刷装置上で又は印刷装置と通信可能な装置上で動作するスマートカード認証モジュールは、ステップ２０２からのデータを利用して、そのカードがサポートされているタイプ及びモデルであるか否かを確認する。上述したように、スマートカード認証システムは、デフォルト設定でサポートされているスマートカードタイプ及びデータモデルに関するデフォルトソフトウエア及びデータと共に供給され分配されているこ

とが間々ある。一実施例によれば、或るカードタイプ及びモデルを読み取ること、カードに格納済みの或るデータモデルを認識して読み取ること、及び或るバックエンド認証サーバーやプロトコルを利用することができるソフトウエア又はモジュールをスマートカード認証システムは実行する。挿入されたカードタイプ又はモジュールが例えばデフォルトソフトウエアでサポートされていなかった場合、本発明手法以前では、デフォルトのソフトウエアは認識されていないカードタイプ又はモデルをサポートするために各印刷装置で書き直されてコンパイルされ直す必要があった。

【００２６】

ステップ２０６では、カードタイプ及びモデルがサポートされているか否かを確認するための検査がなされる。その結果がYes(はい)であったならば、カードは認証ソフトウエアにとって既知のカードであり、その旨がカードリーダに通知されることに加えて、所定のデータモデルに従って特定のユーザ信用証明書をカードリーダが取り出すように指示するデータも通知する。ステップ２０８では、カードリーダは、所定のデータモデルに従ってカードデータにアクセスし、カードからユーザ信用証明書を読み取り、印刷装置で動作する認証モジュールにその信用証明書を通知する。このステップ又は別のステップの一部として、PINコード又は同様なデータが、スマートカードにアクセスする前に入力されるよう要求されてもよい。

【００２７】

例えば、デフォルト認証ソフトウエアは、或るカードタイプ及びモデルを認識し、スマートカードに記憶されているユーザ名及びパスワードである、そのカードタイプ及びモデルに必要なユーザ信用証明書を確認する。ユーザ名及びパスワードはこの特定の認証についてのデータモデルである。上述したようにデータモデルを構成するデータ量又はタイプは如何なるものでもよい。一実施例では、カードリーダに通知されるデータは、カードタイプ及び／又はモデルに関連するデータモデルを記述するデータを含み、このデータはカードリーダがその特定のデータモデルにどのようにアクセスするかを指示する。一実施例では、カードから取り出されるデータは、その認証がローカルに完了するか又はリモート装置でもなされる必要があるかを示す。

【００２８】

ステップ２０６の結果が、カードタイプ及び／又はモデルがデフォルトコンフィギュレーションでサポートされていないことを示す場合には、ステップ２１０で、認証モジュールはユーザの決めたコンフィギュレーションファイルを特定及び受信し、そのカードタイプ及び／又はモデルをサポートするユーザの決めたコンフィギュレーションファイル中にデータが存在するか否かを確認する。一実施例によれば、ユーザの決めたコンフィギュレーションファイルは、フィールドセパレータ（例えば、コンマ－デリミタファイル）を備えたプレインテキストファイル、XMLファイルのようなフォーマット済みテキストファイル又は他のフォーマット済みデータであってよい。コンフィギュレーションファイルは、１より多くのカードモデル及び／又はタイプをサポートするために複数のエントリを有し、編集及び消去されてもよい。コンフィギュレーションファイルは、スマートカードリーダで理解可能なコマンド(命令)を含み、そのコマンドはユーザを認証するのに必要な必要情報をどのように取り出すかを認証システムに指示する。一実施例によれば、コンフィギュレーションファイルはコマンドを含み、認証モジュールが、デフォルトの認証モジュールではサポートされていないタイプ又はデータモデルを含むカードから必要情報を取り出すのに使用する。コンフィギュレーションファイルは、認証モジュールで使用可能なユーザの決めたデータモデルを含んでもよい。一実施例によれば、暗号化技術及び他の方法が、ユーザの決めたコンフィギュレーションファイルへのアクセスを制限するのに使用されてもよい。

【００２９】

一実施例によれば、ユーザの決めた別々のコンフィギュレーションファイルが印刷装置に常駐し、スマートカード認証モジュールによりアクセス可能である。或るコンフィギュレーションファイルは、スマートカードモデル／タイプ、データモデル、パスワードオプ

ション及びローカル認証（別の又は離れている認証サーバーにアクセスすることを要しない認証）用のユーザ信用証明書取得コマンドを決定する。別のコンフィギュレーションファイルが、リモート認証処理に関連するサーバーアドレス、プロトコルタイプ及びデータフォーマットを決定してもよい。使用する適切なコンフィギュレーションファイルがカードモデル及び／又はタイプに基づいていてもよい。

【００３０】

ステップ２１２では、スマートカードリーダは、ユーザの決めたコンフィギュレーションファイルからのデータ及び命令に従って、そのスマートカードのユーザ信用証明データにアクセスする。ユーザ信用証明データは、デフォルトソフトウエアでサポートされているように、又はコンフィギュレーションファイルを用いて決定されるカスタマのように、予め決定されていてもよい。そのデータは、ユーザID及びパスワード、LDAPエントリ、PKI認証物の形式をとってもよいし、その他の識別形式をとってもよい。本ステップ及び別ステップの一部として、PINコード又は同様なデータが、スマートカードにアクセスする前に入力されるよう要求されてもよい。

【００３１】

ステップ２１４では、有効な応答が受信されたか否かを確認する検査がなされる。有効でなければ、エラーメッセージ又は同様なフィードバックがユーザに与えられ、カードが出てくる。

【００３２】

ステップ２１６では、認証ソフトウエアが、印刷装置にローカルなデータベースと共に、取得した信用証明書を比較する。別の実施例では、信用証明書は、データベースフォーマットでは格納されていないデータと比較され、遠隔して格納されたデータを比較されてもよい。

【００３３】

ステップ２１８では、データの比較結果が認証の成功に至ったか否かを確認する検査がなされる。認証が成功していなければ、エラーメッセージ又は同様なフィードバックがユーザに与えられ、カードが出てくる２２０。

【００３４】

認証が成功していると、ステップ２２２でアクセスが許可され、ユーザの認証された機能にユーザが相応しいように認められる。例えば、印刷装置は、ユーザ情報を利用してローカル機能制御データベースにアクセスし、ユーザが使用してよい装置機能を決定してもよい。これは、カラー印刷の許可やスキャントゥ電子メールの許可等のような様々な機能に適用されてもよい。経理システムのような機能やアプリケーションを制御する他のリソースが、スマートカード認証システムに加えて用意されてもよい。

【００３５】

IV. サーバーベースのユーザ信用証明認証

図３は、本発明の別の実施例によるサーバーベースのスマートカード認証手法を示すフローチャート３００である。ステップ３０２では、印刷装置に通信可能に結合されたカードリーダにユーザがスマートカードを挿入する。本発明の一実施例では、カードリーダはスマートカードから記憶済みのデータを読み取り、スマートカード及びタイプを識別するのに十分なデータを、印刷装置で実行するプロセスに通知する。リーダは、カードに記憶済みのデータ全てを読み取って通知してもよいし、或いは認証目的用に限定された情報だけを先ず印刷装置に与えてもよい。例えば、カードリーダはスマートカードタイプ及び／又はモデルに関連する情報だけを取得して通知してもよい。

【００３６】

ステップ３０４では、印刷装置上で又は印刷装置と通信可能な装置上で動作するスマートカード認証モジュールは、ステップ３０２からのデータを利用して、そのカードがサポートされているタイプ及びモデルであるか否かを確認する。上述したように、スマートカード認証システムは、デフォルト設定でサポートされているスマートカードタイプ及びデータモデルに関するデフォルトソフトウエア及びデータと共に供給され分配されているこ

とが間々ある。一実施例によれば、或るカードタイプ及びモデルを読み取ること、カードに格納済みの或るデータモデルを認識して読み取ること、及び或るバックエンド認証サーバーやプロトコルを利用することができるソフトウエア又はモジュールをスマートカード認証システムは実行する。挿入されたカードタイプ又はモジュールが例えばデフォルトソフトウエアでサポートされていなかった場合、本発明手法以前では、デフォルトのソフトウエアは認識されていないカードタイプ又はモデルをサポートするために各印刷装置で書き直されてコンパイルされ直す必要があった。

【００３７】

ステップ３０６では、カードタイプ及びモデルがサポートされているか否かを確認するための検査がなされる。その結果がYes(はい)であったならば、カードは認証ソフトウエアにとって既知のカードであり、その旨がカードリーダに通知されることに加えて、所定のデータモデルに従って特定のユーザ信用証明書をカードリーダが取り出すように指示するデータも通知する。ステップ３０８では、カードリーダは、所定のデータモデルに従ってカードデータにアクセスし、カードからユーザ信用証明書を読み取り、印刷装置で動作する認証モジュールにその信用証明書を通知する。このステップ又は別のステップの一部として、PINコード又は同様なデータが、スマートカードにアクセスする前に入力されるよう要求されてもよい。

【００３８】

例えば、デフォルト認証ソフトウエアは、或るカードタイプ及びモデルを認識し、スマートカードに記憶されているユーザ名及びパスワードである、そのカードタイプ及びモデルに必要なユーザ信用証明書を確認する。ユーザ名及びパスワードはこの特定の認証についてのデータモデルである。上述したようにデータモデルを構成するデータ量又はタイプは如何なるものでもよい。一実施例では、カードリーダに通知されるデータは、カードタイプ及び／又はモデルに関連するデータモデルを記述するデータを含み、このデータはカードリーダがその特定のデータモデルにどのようにアクセスするかを指示する。一実施例では、カードから取り出されるデータは、その認証がローカルに完了するか又はリモート装置でもなされる必要があるかを示す。

【００３９】

ステップ３０６の結果が、カードタイプ及び／又はモデルがデフォルトコンフィギュレーションでサポートされていないことを示す場合には、ステップ３１０で、認証モジュールはユーザの決めたコンフィギュレーションファイルを特定及び受信し、そのカードタイプ及び／又はモデルをサポートするユーザの決めたコンフィギュレーションファイル中にデータが存在するか否かを確認する。一実施例によれば、ユーザの決めたコンフィギュレーションファイルは、フィールドセパレータ（例えば、コンマ－デリミタファイル）を備えたプレインテキストファイル、XMLファイルのようなフォーマット済みテキストファイル又は他のフォーマット済みデータであってよい。コンフィギュレーションファイルは、１より多くのカードモデル及び／又はタイプをサポートするために複数のエントリを有し、編集及び消去されてもよい。コンフィギュレーションファイルは、スマートカードリーダで理解可能なコマンド(命令)を含み、そのコマンドはユーザを認証するのに必要な必要情報をどのように取り出すかを認証システムに指示する。一実施例によれば、コンフィギュレーションファイルはコマンドを含み、認証モジュールが、デフォルトの認証モジュールではサポートされていないタイプ又はデータモデルを含むカードから必要情報を取り出すのに使用する。コンフィギュレーションファイルは、認証モジュールで使用可能なユーザの決めたデータモデルを含んでもよい。

【００４０】

一実施例によれば、ユーザの決めた別々のコンフィギュレーションファイルが印刷装置に常駐し、スマートカード認証モジュールによりアクセス可能である。或るコンフィギュレーションファイルは、スマートカードモデル／タイプ、データモデル、パスワードオプション及びローカル認証（別の又は離れている認証サーバーにアクセスすることを要しない認証）用のユーザ信用証明書取得コマンドを決定する。別のコンフィギュレーションフ

ァイルが、リモート認証処理に関連するサーバーアドレス、プロトコルタイプ及びデータフォーマットを決定してもよい。使用する適切なコンフィギュレーションファイルがカードモデル及び／又はタイプに基づいていてもよい。

【００４１】

ステップ３１２では、スマートカードリーダは、ユーザの決めたコンフィギュレーションファイルからのデータ及び命令に従って、そのスマートカードのユーザ信用証明データにアクセスする。ユーザ信用証明データは、デフォルトソフトウエアでサポートされているように、又はコンフィギュレーションファイルを用いて決定されるカスタマのように、予め決定されていてもよい。そのデータは、ユーザID及びパスワード、LDAPエントリ、PKI認証物の形式をとってもよいし、その他の識別形式をとってもよい。本ステップ及び別ステップの一部として、PINコード又は同様なデータが、スマートカードにアクセスする前に入力されるよう要求されてもよい。

【００４２】

ステップ３１４では、有効な応答が受信されたか否かを確認する検査がなされる。有効でなければ、エラーメッセージ又は同様なフィードバックがユーザに与えられ、カードが出てくる。

【００４３】

ステップ３１６では、リモート認証処理に関するデータが読み取られる。例えば、認証サーバーアドレス、プロトコルタイプ、データフォーマット及び／又は他の情報がユーザの決めたコンフィギュレーションファイルから読み取られ、それにより、デフォルトソフトウエアでサポートされていないサーバーとの認証を可能にする。例えば、新たなサーバーアドレス又はプロトコルが認証システムに加えられる場合に、本発明手法以前の従来方式では、その変更を認識するために認証モジュール全てが書き直されてコンパイルされ直す必要があったであろう。ユーザの決めたコンフィギュレーションファイルを利用することで、その変更は動的に加えられてサポートされる。

【００４４】

ステップ３１８では、認証ソフトウエアは取得した信用証明書を適切なプロトコルと共に適切なサーバーに通知する。上述したように、信用証明書はユーザ名／パスワードの対、LDAPエントリ、又はサーバーベースの確認認証データで構成されてもよい。

【００４５】

ステップ３２０では、データの比較結果が認証の成功に至ったか否かを確認する検査がなされる。認証が成功していなければ、エラーメッセージ又は同様なフィードバックがユーザに与えられ、カードが出てくる３２２。

【００４６】

認証が成功していると、ステップ３２４でアクセスが許可され、ユーザの認証された機能にユーザが相応しいように認められる。例えば、印刷装置は、ユーザ情報を利用してローカル機能制御データベースにアクセスし、ユーザが使用してよい装置機能を決定してもよい。これは、カラー印刷の許可やスキャントゥ電子メールの許可等のような様々な機能に適用されてもよい。経理システムのような機能やアプリケーションを制御する他のリソースが、スマートカード認証システムに加えて用意されてもよい。

【００４７】

V. ウェブベースインターフェース

図４はここで説明されるようなスマートカード認証システムで使用されるユーザの決めたコンフィギュレーションファイルをウェブベースのインターフェースを用いて構成する方法を示すフローチャート４００である。一実施例によれば、ウェブベースインターフェースは視覚的なユーティリティを用意し、ユーザ決定コンフィギュレーションファイルをユーザが構築するのを支援する。一実施例によれば、コンフィギュレーションファイルの変更及び追加は、印刷装置と通信しながら動作するスマートカード認証モジュールによる使用に備えて、印刷装置のローカルストレージに保存される。

【００４８】

インターフェースは、如何なるウェブブラウザを介して起動されてもよく、所定のディレクトリ及び／又はページを宛先システムで引用してよい。ステップ４０２ではユーザは閲覧するコンフィギュレーションファイルを選択し、エントリを追加する又は変更する。一実施例によれば、別個のコンフィギュレーションファイルが、サーバー認証手法用に及びローカル認証手法用に存在する。一実施例では、双方の機能に関する１つのファイルのみが使用されてもよい。ステップ４０４ではユーザはローカルユーザコンフィギュレーションファイルを選択する。これは、サーバーベースの認証用に対してローカルに別個のコンフィギュレーションファイルがある場合である。ローカルユーザコンフィギュレーションファイルが選択されると、ファイルが開かれ、ユーザは様々なタスクを実行してよい（タスクは例えばコンフィギュレーションを変更すること４０６、現在のコンフィギュレーションを表示すること４０８及び／又はコンフィギュレーションファイルに新規エントリを定義すること４１０等である。）。新規エントリを定義する場合、ユーザはスマートカードタイプ、データモデル、パスワードオプション及び発行するユーザ信用証明の取得コマンドに関連する情報をカードリーダに加える。様々な実施例で他の情報も想定されている。ユーザがその動作を終了すると、ローカルユーザコンフィギュレーションファイル４１２が保存される又はアクセスされる。

【００４９】

或いは、別個のコンフィギュレーションファイルの場合、ステップ４１４でユーザはサーバーベースのコンフィギュレーションファイルを選択する。これは、サーバーベースの認証に対してローカルの別個のコンフィギュレーションファイルがある場合である。サーバーベースのコンフィギュレーションファイルが選択されると、そのファイルは開かれ、ユーザは様々なタスクを実行してよい（タスクは例えばコンフィギュレーションを変更すること４１６、現在のコンフィギュレーションを表示すること４１８及び／又はコンフィギュレーションファイルに新規エントリを定義すること４２０等である。）。新規エントリを定義する場合、ユーザはサーバーアドレス、プロトコルタイプ及びデータフォーマットに加えてもよい。様々な実施例で他の情報も想定されている。ユーザがその動作を終了すると、サーバーベースのコンフィギュレーションファイル４２２が保存される又はアクセスされる。

【００５０】

VI. 実現手段

印刷装置へのアクセスを制限するスマートカード認証システムに関連して主に説明がなされてきたが、本手法は如何なるタイプのスマートカード認証手法にも適用可能である。ここで説明される手法及び様々な要素はハードウエアで、コンピュータソフトウエアで又はハードウエア及びコンピュータソフトウエアの如何なる組み合わせで如何なるコンピュータプラットフォームででも実現されてよい。図５は本発明を利用可能なコンピュータシステム例５００を示すブロック図である。コンピュータシステム５００は、情報を通信するためのバス５０２又は他の通信手段、及びバス５０２に結合され、情報を処理するプロセッサ５０４を含む。コンピュータシステム５００は、プロセッサ５０４により実行される命令及び情報を格納するために、バス５０２に結合された、ランダムアクセスメモリ(RAM)又は他のダイナミック記憶装置のようなメインメモリ５０６も含む。メインメモリ５０６は、プロセッサ５０４により実行される命令の実行中に、一時的な変数や他の中間的な情報を格納するために使用されてもよい。コンピュータシステム５００は、プロセッサ５０４のための命令及び静的な情報を記憶するために、バス５０２に結合されたリードオンリメモリ(ROM)５０８又は他のスタティック記憶装置を更に含む。情報及び命令を格納するために磁気ディスク又は光ディスクのような記憶装置５１０が用意され、バス５０２に結合される。

【００５１】

コンピュータシステム５００はバス５０２を介して液晶ディスプレイ(LCD)のようなディスプレイ５１２に結合され、ユーザに情報を表示してもよい。英数字その他のキーを含む入力装置５１４は、情報及び命令選択内容をプロセッサ５０４に通知するためのバス５

０２に結合される。他のタイプのユーザ入力装置はカーソル制御部５１６であり、マウス、トラックボール、スタイラス又はカーソル方向キーのようなものであり、方向情報及び命令選択内容をプロセッサに通知し、ディスプレイ５１２におけるカーソルの動きを制御する。この入力装置は一般的には２軸－第１軸(例えば、ｘ)及び第２軸(例えば、ｙ)－による二次元の自由度を有し、装置が平面内で位置を指定できるようにする。

【００５２】

本発明は無線通信アーキテクチャにおける通信システム５００の用途に関連する。本発明の一実施例によれば、メインメモリ５０６に含まれる１以上の命令の１以上のシーケンスを実行するプロセッサ５０４に応じて、コンピュータシステム５００により無線通信がなされる。そのような命令は記憶装置５１０のような他のコンピュータ読み取り可能な媒体からメインメモリ５０６に読み込まれてもよい。メインメモリ５０６に含まれる命令シーケンスを実行すると、プロセッサ５０４は上述のプロセスステップを実行するようになる。代替実施例では、本発明を実現するソフトウエア命令を組み合わせる代わりに、ハードワイヤード回路が使用されてもよい。かくて本発明の実施例はハードウエア回路及びソフトウエアの如何なる特定の組み合わせにも限定されない。

【００５３】

ここで使用されるような「マシン読み取り可能な媒体」は、特定の形式でマシン（コンピュータ）に動作を引き起こすデータを用意することに関与する如何なる媒体にも関連する。コンピュータシステム５００を利用して実現される例では、様々なマシン読み取り可能な媒体はプロセッサ５０４に命令を実行用に提供することを含む。そのような媒体は様々な形態をとってよく、不揮発性媒体、揮発性媒体及び伝送媒体を含むがそれらに限定されない。不揮発性媒体は、例えば、記憶装置５１０のような光学的又は磁気的なディスクを含む。揮発性媒体はメインメモリ５０６のようなダイナミックメモリを含む。伝送媒体は、同軸ケーブル、導線及び光ファイバを含み、バス５０２を構成するワイヤを含む。伝送媒体は、無線波及び赤外線データ通信で生成されるような音響的な又は光学的な波の形態をとってもよい。

【００５４】

コンピュータ読み取り可能な媒体の一般的な形態は、例えば、フロッピディスク、フレキシブルディスク、ハードディスク、磁気テープその他の何らかの磁気媒体、CD-ROMその他の光媒体、パンチカード、紙テープその他の穿孔パターンによる物理的媒体、RAM、RPOM、EPROM、フラッシュメモリその他の何らかのメモリチップ若しくはカートリッジ、後述の搬送波又は他のコンピュータが読み取り可能な何らかの媒体を含む。

【００５５】

様々な形態のコンピュータ読み取り可能な媒体は、実行に備えて１以上の命令シーケンスをプロセッサ５０４に運ぶことを含んでもよい。例えば、その命令は当初は遠隔的な（リモート）コンピュータの磁気ディスクで携帯されていてもよい。リモートコンピュータはその命令をダイナミックメモリにロードし、その命令をモデムを用いて電話回線で送信してもよい。コンピュータシステム５００にとってローカルなモデムは電話回線でデータを受信し、赤外線送信機を用いてデータを赤外線信号に変換してもよい。バス５０２に結合された赤外線検出器は赤外線信号で搬送されたデータを受信し、バス５０２にデータをのせる。バス５０２はデータをメインメモリ５０６に搬送し、プロセッサ５０４はメインメモリから命令を引き出して実行する。メインメモリ５０６で受信された命令は、プロセッサ５０４による実行の前に又は後に記憶装置５１０に光学的に格納されてもよい。

【００５６】

コンピュータシステム５００はバス５０２に結合された通信インターフェース５１８も含む。通信インターフェース５１８は、ローカルネットワーク５２２に接続されたネットワークリンク５２０に結合する双方向データ通信をもたらす。例えば通信インターフェース５１８は、関連するタイプの電話回線へのデータ通信接続をもたらす統合サービスディジタルネットワーク(ISDN)カード又はモデムでもよい。別の例として、通信インターフェース５１８はコンパチブルLANへのデータ通信接続をもたらすLANカードでもよい。無線リ

ンクが実現されてもよい。そのような如何なる実施例でも、通信インターフェース５１８は電気的な、電磁的な又は光学的な信号を送信及び受信し、その信号は様々なタイプの情報を表現するディジタルデータストリームを搬送する。

【００５７】

ネットワークリンク５２０は典型的には１以上のネットワークを介して他のデータ装置に至るデータ通信をもたらす。例えば、ネットワークリンク５２０は、ローカルネットワーク５２２を介してホストコンピュータ５２４に至る接続を又はインターネットサービスプロバイダ(ISP)５２６により制御されるデータ機器に至る接続をもたらしてもよい。ISP５２６は今日インターネット５２８として一般的に言及されているワールドワイドパケットデータ通信ネットワークを介してデータ通信サービスを提供する。ローカルネットワーク５２２及びインターネット５２８双方はディジタルデータストリームを搬送する電気的な、電磁的な又は光学的な信号を使用する。様々なネットワークを介する信号、コンピュータシステム５００への及びそこからのディジタルデータを搬送する、通信インターフェース５１８を介した及びネットワークリンク５２０における信号は、情報を伝送する搬送波の形態の具体例である。

【００５８】

コンピュータシステム５００は、１つ又は複数のネットワーク、ネットワークリンク５２０及び通信インターフェース５１８を介して、メッセージを送信し、プログラムコードを含むデータを受信することができる。インターネットの例では、サーバー５３０は、インターネット５２８、ISP５２６、ローカルネットワーク５２２及び通信インターフェース５１８を介してアプリケーションプログラムに必要なコードを送信してもよい。

【００５９】

プロセッサ５０４により受信されたコードは、それが受信された際に実行してもよいし、及び／又は以後の実行に備えて記憶装置５１０に又は他の不揮発性記憶装置に格納されてもよい。このようにしてコンピュータシステム５００は搬送波形式でアプリケーションコードを取得してもよい。

【００６０】

以上の説明では、本発明の実施例が実施状況毎に異なってよい多くの具体的詳細に関連して説明されてきた。本願により独占排他的に意図される本発明は、将来の如何なる補正をも含む形式で特許請求の範囲で規定される。従って特許請求の範囲で明示的に言及されていない限定、要素、特性、特徴、効果又は属性は如何なる方法によっても特許請求の範囲を一切限定しない。明細書及び図面は限定な意味ではなく例示的な意味に解釈されるべきである。

【図面の簡単な説明】

【００６１】

【図１】本発明の一実施例によるスマートカード認証ソリューションを示すシステムブロック図である。

【図２】本発明の一実施例によるスマートカード認証手法を示すフローチャートである。

【図３】本発明の別の実施例によるスマートカード認証手法を示すフローチャートである。

【図４】本発明の一実施例によるウェブベースのユーザインターフェースを示すフローチャートである。

【図５】本発明を利用可能なコンピュータシステムのブロック図である。

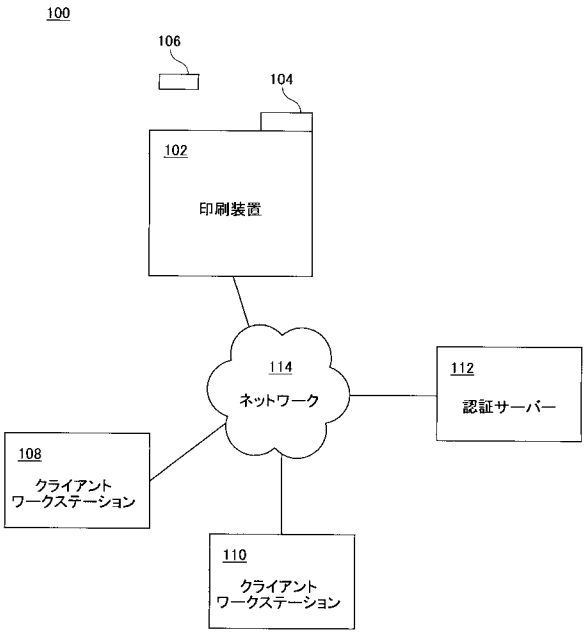
【符号の説明】

【００６２】

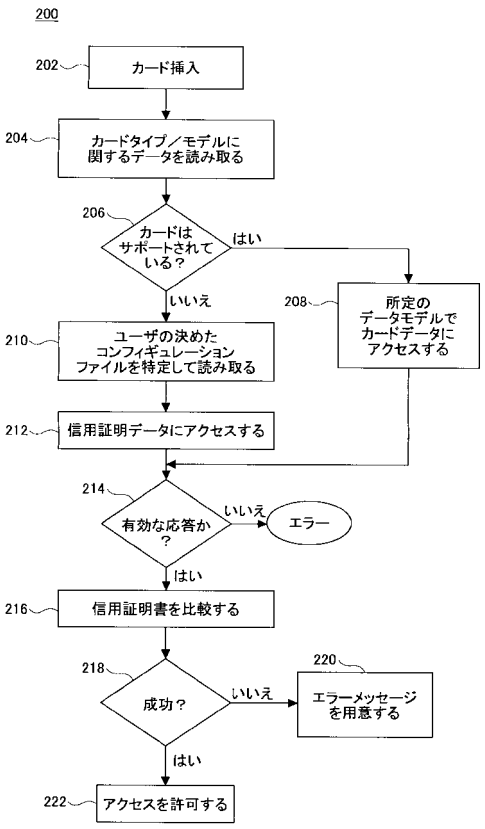
１００　システム
１０２　印刷装置
１０４　カードリーダ
１０６　スマートカード
１０８，１１０　クライアントワークステーション

１１２　認証サーバー
１１４　ネットワーク
５００　コンピュータシステム
５０２　バス
５０４　プロセッサ
５０６　メインメモリ
５０８　ＲＯＭ
５１０　記憶装置
５１２　ディスプレイ
５１４　入力装置
５１６　カーソル制御部
５１８　通信インターフェース
５２０　ネットワークリンク
５２２　ローカルネットワーク
５２４　ホスト
５２６　インターネットサービスプロバイダ
５２８　インターネット
５３０　サーバー

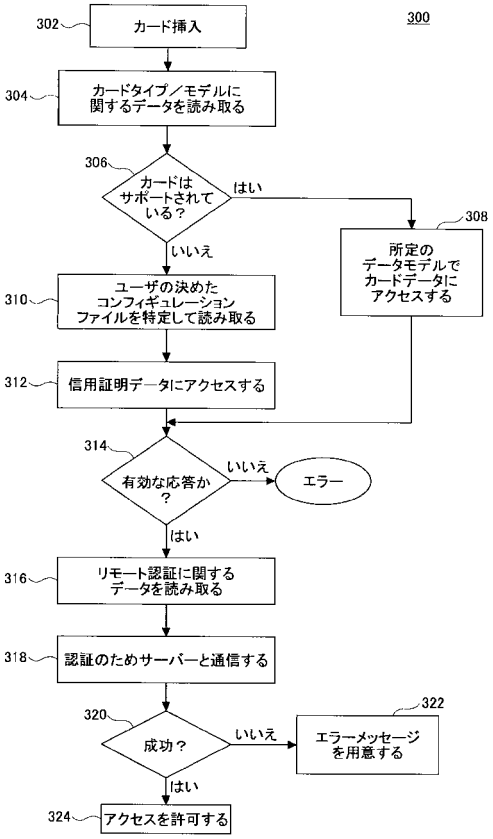
【図１】



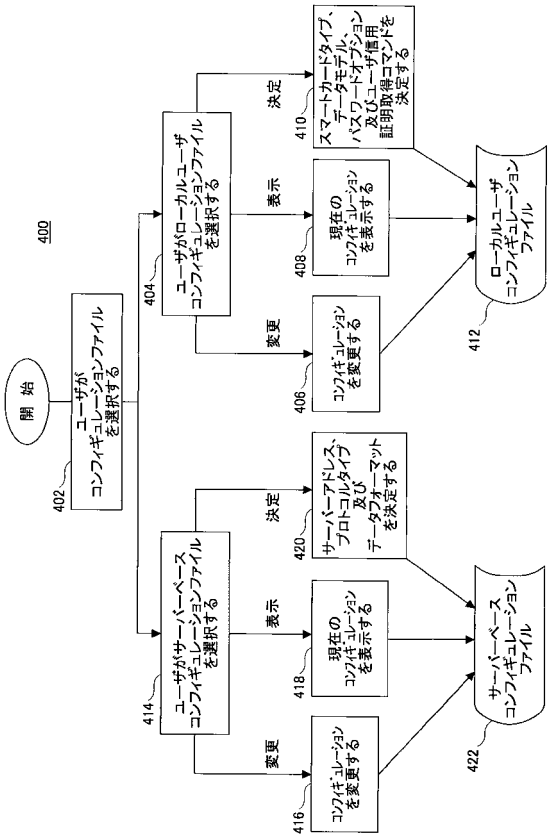
【図２】



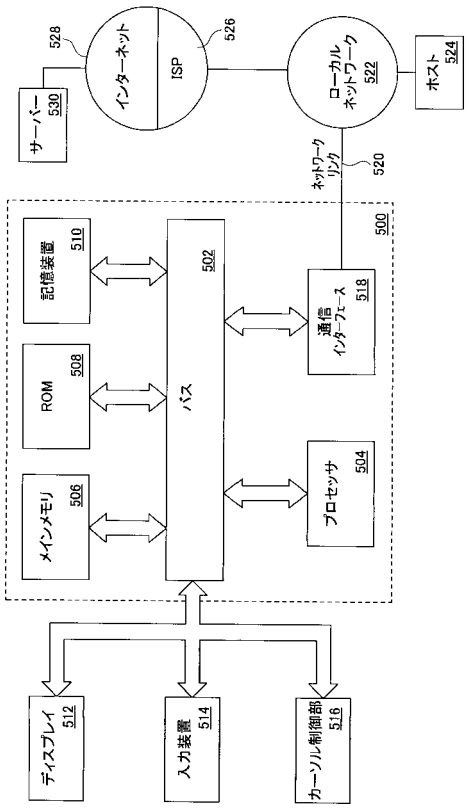
【図３】


300
302
カード挿入
304
カードタイプ／モデルに関するデータを読み取る
306
カードはサポートされている？
はい
いいえ
308
所定のデータモデルでカードデータにアクセスする
310
ユーザの決めたコンフィギュレーションファイルを特定して読み取る
312
信用証明データにアクセスする
314
有効な応答か？
いいえ
エラー
はい
316
リモート認証に関するデータを読み取る
318
認証のためサーバーと通信する
320
成功？
いいえ
322
エラーメッセージを用意する
はい
324
アクセスを許可する

【図４】


400
開始
402
ユーザがコンフィギュレーションファイルを選択する
404
ユーザがローカルユーザコンフィギュレーションファイルを選択する
406
コンフィギュレーションを変更する
408
現在のコンフィギュレーションを表示する
410
スマートカードタイプ、データモデル、パスワードオプション及びユーザ信用証明取得コマンドを決定する
412
ローカルユーザコンフィギュレーションファイル
414
ユーザがサーバーベースコンフィギュレーションファイルを選択する
416
コンフィギュレーションを変更する
418
現在のコンフィギュレーションを表示する
420
サーバーアドレス、プロトコルタイプ及びデータフォーマットを決定する
422
サーバーベースコンフィギュレーションファイル
決定
表示
変更

【図５】


528
インターネット
ISP
526
ローカルネットワーク
522
ホスト
524
サーバー
530
ネットワークリンク
520
500
記憶装置
510
ROM
508
メインメモリ
506
502
バス
通信インターフェース
518
プロセッサ
504
ディスプレイ
512
入力装置
514
カーソル制御部
516

フロントページの続き

(72)発明者　ケ　ウェイ
アメリカ合衆国，カリフォルニア州　９５０１４－５９２４，クパチーノ　リザルツウェイ　４
リコー　コーポレイション内

Ｆターム(参考) 5B058 CA27　KA33
5J104 AA07　AA16　EA22　KA02　KA04　NA35