(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第6465542号
(P6465542)

(45)発行日　平成31年2月6日(2019.2.6)　(24)登録日　平成31年1月18日(2019.1.18)

(51)Int.Cl.		F I		
G06F 21/46	(2013.01)	G06F	21/46	
G06F 21/31	(2013.01)	G06F	21/31	
H04L 9/32	(2006.01)	H04L	9/00	673A
B41J 29/00	(2006.01)	B41J	29/00	Z
B41J 29/38	(2006.01)	B41J	29/38	Z

請求項の数 9　(全 17 頁)

(21)出願番号　特願2013-181564(P2013-181564)
(22)出願日　平成25年9月2日(2013.9.2)
(65)公開番号　特開2015-49755(P2015-49755A)
(43)公開日　平成27年3月16日(2015.3.16)
審査請求日　平成28年9月2日(2016.9.2)

前置審査

(73)特許権者　000001007
キヤノン株式会社
東京都大田区下丸子３丁目３０番２号
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治
(74)代理人　100134175
弁理士　永川　行光

最終頁に続く

(54)【発明の名称】情報処理装置、その制御方法及びプログラム

(57)【特許請求の範囲】
【請求項１】
情報処理装置であって、
前記情報処理装置に含まれる第１のサーバに対応付けられた第１の認証処理方法と、前記情報処理装置に含まれる第２のサーバに対応付けられた第２の認証処理方法とを記憶する記憶手段と、
前記第１のサーバ及び前記第２のサーバから認証情報を受け付ける認証制御手段と、を有し、
前記認証制御手段は、前記第１のサーバから第１認証情報を受け付けた場合には、当該第１認証情報に含まれる第１パラメータのユーザ名に対応する第１パスワードを取得し、当該第１パスワードが所定のパスワードポリシーを満たしているかを判定する判定処理を実行し、かつ、前記認証制御手段による照合処理の結果を前記第１のサーバに応答する前記第１の認証処理方法を実行し、前記第２のサーバから第２認証情報を受け付けた場合には、当該第２認証情報に含まれる第２パラメータのユーザ名に対応する第２パスワードを取得し、当該第２パスワードが前記所定のパスワードポリシーを満たしているかを判定する判定処理を実行し、かつ、前記第２のサーバが認証処理を実行するために用いる認証データを前記第２のサーバに送信する前記第２の認証処理方法を実行することを特徴とする情報処理装置。
【請求項２】
前記第１のサーバは、第１の通信プロトコルを用いて第１のアプリケーションと通信し

、前記第２のサーバは、前記第１の通信プロトコルと異なる第２の通信プロトコルを用いて第２のアプリケーションと通信することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記所定のパスワードポリシーは、前記第１パスワード或いは前記第２パスワードの有効期限、又は、前記第１パスワード或いは前記第２パスワードが所定の複雑さを満たしているか否かについての条件を含むことを特徴とする請求項１に記載の情報処理装置。
【請求項４】
前記ユーザ名に関連付けられた認証情報を蓄積する蓄積手段を、更に有し、
前記認証制御手段は、前記第１のサーバから前記第１認証情報を受信した場合には、前記第１のサーバから受信した前記第１認証情報と前記蓄積手段に蓄積されている認証情報とを照合した結果を前記認証処理の結果として前記第１のサーバに応答することを特徴とする請求項１から３のうち何れか１項に記載の情報処理装置。
【請求項５】
前記認証制御手段は、前記第２のサーバから前記第２認証情報を受信した場合には、前記第２のサーバから受信した前記第２認証情報に基づいて所定の計算を行った結果を前記認証データとして前記第２のサーバに応答することを特徴とする請求項１から４のうち何れか１項に記載の情報処理装置。
【請求項６】
前記第１のサーバは、ＨＴＴＰサーバであることを特徴とする請求項１から５のうち何れか１項に記載の情報処理装置。
【請求項７】
前記第２のサーバは、ＳＭＢ/ＣＩＦＳサーバ又はＳＮＭＰサーバであることを特徴とする請求項１から６のうち何れか１項に記載の情報処理装置。
【請求項８】
第１のサーバと第２のサーバを含み、前記第１のサーバに対応付けられた第１の認証処理方法と、前記第２のサーバに対応付けられた第２の認証処理方法とを記憶する記憶手段と、前記第１のサーバ及び前記第２のサーバから認証情報を受け付ける認証制御手段と、を有する情報処理装置の制御方法であって、
前記認証制御手段が、前記第１のサーバから第１認証情報を受け付けた場合には、当該第１認証情報に含まれる第１パラメータのユーザ名に対応する第１パスワードを取得し、当該第１パスワードが所定のパスワードポリシーを満たしているかを判定する判定処理を実行し、かつ、前記認証制御手段による照合処理の結果を前記第１のサーバに応答する前記第１の認証処理方法を実行し、前記第２のサーバから第２認証情報を受け付けた場合には、当該第２認証情報に含まれる第２パラメータのユーザ名に対応する第２パスワードを取得し、当該第２パスワードが前記所定のパスワードポリシーを満たしているかを判定する判定処理を実行し、かつ、前記第２のサーバが認証処理を実行するために用いる認証データを前記第２のサーバに送信する前記第２の認証処理方法を実行する認証制御ステップを有することを特徴とする制御方法。
【請求項９】
第１のサーバと第２のサーバを含み、前記第１のサーバに対応付けられた第１の認証処理方法と、前記第２のサーバに対応付けられた第２の認証処理方法とを記憶する記憶手段と、前記第１のサーバ及び前記第２のサーバから認証情報を受け付ける認証制御手段と、を有するコンピュータに、
前記認証制御手段が前記第１のサーバから第１認証情報を受け付けた場合には、前記認証制御手段が、前記第１認証情報に含まれる第１パラメータのユーザ名に対応する第１パスワードを取得し、当該第１パスワードが所定のパスワードポリシーを満たしているかを判定する判定処理を実行し、かつ、前記認証制御手段による照合処理の結果を前記第１のサーバに応答する前記第１の認証処理方法を実行する第１の認証処理手順と、
前記認証制御手段が前記第２のサーバから第２認証情報を受け付けた場合には、前記認証制御手段が、当該第２認証情報に含まれる第２パラメータのユーザ名に対応する第２パ

スワードを取得し、当該第２パスワードが前記所定のパスワードポリシーを満たしているかを判定する判定処理を実行し、かつ、前記第２のサーバが認証処理を実行するために用いる認証データを前記第２のサーバに送信する前記第２の認証処理方法を実行する第２の認証処理手順と、
を実行させるためのプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報処理装置、その制御方法及びプログラムに関する。
【背景技術】
【０００２】
スキャナ、プリンタ、通信等の機能を備える複合機（ＭＦＰ：Ｍｕｌｔｉ Ｆｕｎｃｔｉｏｎ Ｐｅｒｉｐｈｅｒａｌ）が知られている。ＭＦＰは本体に操作パネルを備えており、ユーザはその操作パネルを操作してＭＦＰのコピー機能やスキャン機能等を利用することができる。また近年のＭＦＰは、ファイル共有サーバやウェブサーバの機能を備えており、ネットワーク上の端末は、ＳＭＢ（Ｓｅｒｖｅｒ Ｍｅｓｓａｇｅ Ｂｌｏｃｋ）や、ＨＴＴＰ等の通信プロトコルを用いてＭＦＰのサーバ機能にアクセスできる。またＭＦＰは、ＭＩＢ（Ｍａｎａｇｅｍｅｎｔ ｉｎｆｏｒｍａｔｉｏｎ ｂａｓｅ）を備えており、ネットワーク上の端末は、ネットワーク機器の管理プロトコルとして知られるＳＮＭＰｖ３（非特許文献１）を用いてＭＦＰのＭＩＢにアクセスできる。
【０００３】
更に近年のＭＦＰは、そのＭＦＰを利用するユーザを特定するためのユーザ認証機構を備える。一般に１つのＭＦＰが複数の機能や通信プロトコルを備える場合、各機能や通信プロトコルに応じた複数のユーザ認証機構を備える。例えば、操作パネル用、ウェブサーバ用、ファイル共有サーバ用、ＳＮＭＰｖ３用のユーザ認証機構はそれぞれ異なることがある。
【０００４】
このように一つのＭＦＰの中に複数のユーザ認証機構が備わっている場合に、これらを連携させるための手段としては以下のものがある。主に操作パネル用の認証に使用するユーザ情報と、ＳＮＭＰｖ３のＵＳＭ（Ｕｓｅｒ－ｂａｓｅｄ Ｓｅｃｕｒｉｔｙ Ｍｏｄｅｌ）で管理されるユーザ情報とを関連付けて同期する方法が知られている（例えば特許文献１）。
【０００５】
また近年、ＭＦＰはパーソナルコンピュータ等のネットワーク端末と同様のセキュリティが必要と考えられている。このため、パスワードポリシー（パスワードの有効期限、パスワードの複雑さ、ロックアウトの設定・制御）や認証ログ（認証成功／失敗ログの記録）に対応したユーザ認証機構を備えるＭＦＰも出現している。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００６－１９５７５５号公報
【非特許文献】
【０００７】
【非特許文献１】RFC3414 (User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3))
【発明の概要】
【発明が解決しようとする課題】
【０００８】
一つの機器の中に複数のユーザ認証機構が存在する場合、以下のような課題がある。
・それぞれのユーザ認証機構に対して同じユーザのアカウントを登録する場合があり、ユ

ーザ情報の管理が煩わしい。ユーザの手を煩わせることなく、複数のユーザ認証機構に対して同じアカウントを利用可能にするためには、特許文献１のようにユーザの認証を行う機構間での連携が必要になる。
・一つの機器に、パスワードポリシーや認証ログに対応しているユーザ認証機構と、それらに対応していないユーザ認証機構が混在するのはセキュリティの点からも好ましくない。このため機器を製造するベンダーは、複数あるユーザ認証機構に対して、同等のセキュリティ機能を提供するために開発コストをかける必要があるという課題がある。
【０００９】
一つの機器に複数のユーザ認証機構が存在する場合は上記のような課題があるため、通信プロトコルや機能が異なる場合も、単一のユーザ認証機構を共通で使用する構成が望ましい。しかしながら、各種通信プロトコルのユーザ認証方法には仕様の差異があり、単一のユーザ認証機構で全ての通信プロトコルのユーザ認証に関わる処理をサポートするのは困難であった。例えば、ＳＮＭＰｖ３のＵＳＭで規定される方式は、ユーザのパスワードを使用して、ユーザの認証のみならず、パスワードを基に生成した鍵により暗号処理や署名・改ざん検知処理を行っているため、その処理は複雑である。
【００１０】
また、ＲＦＣで規定された一般に良く知られるプロトコルは、そのプロトコルを実装したソフトウェアモジュールやソースコードが一般に公開されている。このため、サーバを実装するベンダーは、これらの既存のソフトウェアモジュールやソースコードを利用することができる。しかし、機器を製造するベンダーがプロトコル毎に異なる既存のソフトウェアモジュールやソースコードからユーザ認証に関わる全ての部分を機器共通のユーザ認証機構に置き換えるのには非常に手間と工数がかかる。また、パスワードポリシーのチェックや、パスワードの変更、認証ログの記録に関する仕様がプロトコルに規定されていない場合、公開された既存のソフトウェアモジュールやソースコードもその機能を持たない。従って、機器を製造するベンダーが、既存のソフトウェアモジュールやソースコードに、パスワードポリシーのチェックや、パスワードの変更、認証ログの記録等の機能を追加・実装しなければならず、それには非常に手間と工数がかかるという問題がある。
【００１１】
本発明の目的は、上記従来技術の問題点を解決することにある。
【００１２】
本発明の特徴は、ユーザの認証に関わる管理を統合できる技術を提供することにある。
【課題を解決するための手段】
【００１３】
上記目的を達成するために本発明の一態様に係る情報処理装置は以下のような構成を備える。即ち、
情報処理装置であって、
前記情報処理装置に含まれる第１のサーバに対応付けられた第１の認証処理方法と、前記情報処理装置に含まれる第２のサーバに対応付けられた第２の認証処理方法とを記憶する記憶手段と、
前記第１のサーバ及び前記第２のサーバから認証情報を受け付ける認証制御手段と、を有し、
前記認証制御手段は、前記第１のサーバから第１認証情報を受け付けた場合には、当該第１認証情報に含まれる第１パラメータのユーザ名に対応する第１パスワードを取得し、当該第１パスワードが所定のパスワードポリシーを満たしているかを判定する判定処理を実行し、かつ、前記認証制御手段による照合処理の結果を前記第１のサーバに応答する前記第１の認証処理方法を実行し、前記第２のサーバから第２認証情報を受け付けた場合には、当該第２認証情報に含まれる第２パラメータのユーザ名に対応する第２パスワードを取得し、当該第２パスワードが前記所定のパスワードポリシーを満たしているかを判定する判定処理を実行し、かつ、前記第２のサーバが認証処理を実行するために用いる認証データを前記第２のサーバに送信する前記第２の認証処理方法を実行することを特徴とする

。
【発明の効果】
【００１４】
本発明によれば、複数のソフトウェアモジュールが、共通のユーザ認証機能を利用してユーザの認証を行うことができる。
【図面の簡単な説明】
【００１５】
【図１】本発明の実施形態１に係るネットワーク構成を示す簡略図。
【図２】実施形態１に係るＭＦＰのハードウェア構成を示すブロック図。
【図３】実施形態１に係るＭＦＰとＰＣのソフトウェア及びソフトウェアが管理するデータの構成を説明するブロック図。
【図４】実施形態１に係るローカルＵＩが操作部に表示するユーザインターフェースの例を示す図。
【図５】設定ＵＩのユーザインターフェースを説明する図。
【図６】実施形態１に係るユーザＤＢのデータ構成例を示す図。
【図７】実施形態１に係るユーザ認証システムが備えるＡＰＩの例を示す図。
【図８】実施形態１に係る認証処理テーブルの内容例を示す図。
【図９】実施形態１に係るＭＦＰにおいて、図７（Ａ）のＡＰＩが呼び出された際のユーザ認証システムの動作を説明するフローチャート。
【図１０】実施形態１に係るＭＦＰがユーザ認証を実施する際のソフトウェアモジュールとの関係をデータの流れと共に示す図。
【図１１】本発明の実施形態２に係るユーザ認証システムを認証サーバとして構成したシステム構成の例を示す図。
【図１２】実施形態に２に係るＭＦＰと認証サーバのソフトウェア構成を示すブロック図。
【発明を実施するための形態】
【００１６】
以下、添付図面を参照して本発明の実施形態を詳しく説明する。尚、以下の実施形態は特許請求の範囲に係る本発明を限定するものでなく、また本実施形態で説明されている特徴の組み合わせの全てが本発明の解決手段に必須のものとは限らない。
【００１７】
図１は、本発明の実施形態１に係るネットワーク構成を示す簡略図である。
【００１８】
ネットワーク（ＬＡＮ）１００には、本発明に係る情報処理装置の一例であるＭＦＰ１０１とパーソナルコンピュータ（ＰＣ）１０２とが接続されている。ＭＦＰ１０１とＰＣ１０２は、ＬＡＮ１００を介して相互に通信を行うことができる。ここでＭＦＰ１０１は、スキャナ、プリンタ、通信等の複数の機能を備える複合機である。
【００１９】
図２は、実施形態１に係るＭＦＰ１０１のハードウェア構成を示すブロック図である。
【００２０】
ＣＰＵ２０１を含む制御部２００は、ＭＦＰ１０１全体の動作を制御する。ＣＰＵ２０１は、ＲＯＭ２０２に記憶されたブートプログラムに従ってＨＤＤ２０４にインストールされているＯＳや制御プログラムをＲＡＭ２０３に展開し、ＣＰＵ２０１がそのプログラムを実行することによりＭＦＰ１０１が動作する。ＲＡＭ２０３は、ＣＰＵ２０１の主メモリ、ワークエリア等の一時記憶領域として用いられる。ＨＤＤ２０４は、画像データや各種プログラムを記憶する。操作部Ｉ／Ｆ２０５は、操作部２０９と制御部２００とを接続する。操作部２０９は、タッチパネルとして動作する表示部を備える。プリンタＩ／Ｆ２０６は、プリンタ２１０と制御部２００とを接続する。プリンタ１２０で印刷すべき画像データは、プリンタＩ／Ｆ２０６を介して制御部２００からプリンタ２１０に転送され、プリンタ２１０によりシート等の記録媒体に印刷される。スキャナＩ／Ｆ２０７は、ス

キャナ２１１と制御部２００とを接続する。スキャナ２１１は、原稿上の画像を読み取って画像データを生成し、スキャナＩ／Ｆ２０７を介して制御部２００に入力する。ネットワークＩ／Ｆ２０８は、制御部２００（ＭＦＰ１０１）をＬＡＮ１００に接続する。ネットワークＩ／Ｆ２０８は、ＬＡＮ１００に接続された外部装置（例えば、Ｗｅｂサーバ等）に画像データや情報を送信したり、ＬＡＮ１００上の外部装置から各種情報を受信したりする。

【００２１】

尚、ＰＣ１０２は、一般に知られている汎用コンピュータのハードウェア構成で構成されるため、その説明を省略する。

【００２２】

図３は、実施形態１に係るＭＦＰ１０１とＰＣ１０２のソフトウェア及びソフトウェアが管理するデータの構成を説明するブロック図である。尚、図３の矢印は、主なユースケースにおける機能の呼び出し元と呼び出し先を示す。ソフトウェアの機能とソフトウェアが管理するデータについて、以下に説明する。

【００２３】

ＭＦＰ１０１のソフトウェアは、ＭＦＰ１０１のＨＤＤ２０４にプログラムとして記憶されており、そのプログラムをＲＡＭ２０３に展開してＣＰＵ２０１が実行することにより以下に説明する機能を実現する。

【００２４】

ローカルＵＩ（ユーザインターフェース）３０１は、ユーザが操作可能なユーザインターフェースを操作部２０９に表示して、ＭＦＰ１０１が持つ機能をユーザに提供する。

【００２５】

図４（Ａ）～（Ｄ）は、実施形態１に係るローカルＵＩ３０１が操作部２０９に表示するユーザインターフェースの例を示す図である。

【００２６】

例えば、図４（Ａ）は、操作部２０９を利用するユーザを認証するためのユーザ認証画面の一例を示す図である。図４（Ｂ）は、図４（Ａ）のユーザ認証画面で認証したユーザにパスワードの変更を求めるためのパスワード変更画面の一例を示す。図４（Ｃ）は、操作部２０９を利用するユーザに提供する機能一覧を示すメニュー画面の一例である。図４（Ｄ）は、ＭＦＰ１０１のボックス機能を利用するためのユーザインターフェース画面の一例を示す。例えば、ユーザは、図４（Ｄ）のユーザインターフェース画面を利用して、スキャナ２１１から取得した画像データを、電子ドキュメントとしてＨＤＤ２０４へ保存することができる。またＨＤＤ２０４から取得した電子ドキュメントをプリンタ２１０を使用してプリントすることができる。

【００２７】

ＰＣ１０２は、ウェブブラウザ３１７、ファイル管理ツール３１９、ＭＦＰ管理ツール３２１等のソフトウェアを備える。

【００２８】

ウェブブラウザ３１７は、ＭＦＰ１０１のＨＴＴＰサーバ３０２と通信するためのＨＴＴＰクライアント３１８としての機能を備える。ＨＴＴＰサーバ３０２は、ウェブブラウザ３１７から要求を受けて、リモートＵＩ３０３を呼び出す。リモートＵＩ３０３は、ウェブブラウザ３１７を操作するユーザに対して、ＨＴＭＬで記載されたユーザインターフェースを提供する。ＨＴＴＰサーバ３０２は、ウェブブラウザ３１７からの要求の応答として、リモートＵＩ３０３から取得したＨＴＭＬデータをウェブブラウザ３１７に返却する。

【００２９】

ファイル管理ツール３１９は、ＭＦＰ１０１のＳＭＢ／ＣＩＦＳサーバ３０４と通信するためのＳＭＢ／ＣＩＦＳクライアント３２０としての機能を備える。ＳＭＢ／ＣＩＦＳサーバ３０４は、ＮＴＬＭ（ＮＴ ＬＡＮ Ｍａｎａｇｅｒ）認証プロトコルを処理するＮＴＬＭ認証処理部３０５を備える。ＳＭＢ／ＣＩＦＳサーバ３０４は、ファイル管理ツー

ル３１９からファイルの閲覧やファイル保存等の要求を受けとると、文書管理サービス３０６を呼び出す。文書管理サービス３０６は、ＨＤＤ２０４に保存された電子ドキュメント（ＰＤＦ，ＪＰＥＧ，ＰＮＧ，ＤＯＣ等の拡張子を持つファイル）の閲覧、更新、新規ファイルの保存等を行う機能を備える。

【００３０】

ＭＦＰ管理ツール３２１は、ＭＦＰ１０１のＳＮＭＰサーバ３０７にアクセスして、ＭＦＰ１０１が備えるＭＩＢ３０９にアクセスするためのＳＮＭＰクライアント３２２としての機能を備える。ＳＮＭＰサーバ３０７は、ＳＮＭＰ ｖｅｒｓｉｏｎ３ のＵＳＭで規定されているユーザ認証プロトコルを処理するＵＳＭ認証処理部３０８を備える。ＳＮＭＰサーバ３０７は、ＰＣ１０２のＭＦＰ管理ツール３２１からのアクセス要求を受けると、ＭＩＢ３０９に保存されたデータの参照や設定を行う。

【００３１】

ユーザ認証システム３１０は、ＭＦＰ１０１を利用するユーザを認証するための機構を備える。このユーザ認証システム３１０が持つ機能の詳細を以下に説明する。

【００３２】

ユーザ認証システム３１０は、ＭＦＰ１０１を管理するユーザが、ＭＦＰ１０１のユーザ認証に関わる設定を行うための設定ＵＩ３１１を備える。設定ＵＩ３１１は、リモートＵＩ３０３と同様に、ＰＣ１０２のウェブブラウザ３１７から利用可能なＨＴＭＬで記載されたユーザインターフェースとして構成することができる。

【００３３】

図５（Ａ）～（Ｆ）は、設定ＵＩ３１１のユーザインターフェースを説明する図である。

【００３４】

図５（Ａ）はメニュー画面例を示す。図５（Ａ）の画面で、５０２～５０５で示す項目のいずれかが指示されると、その指示された機能の画面に遷移する。ユーザ認証設定５０２は、ＭＦＰ１０１のユーザ認証機能のＯＮ／ＯＦＦを設定するユーザインターフェースである。図５（Ａ）の画面でユーザ認証設定５０２が指示されると図５（Ｂ）の画面に遷移する。図５（Ｂ）の画面では、ユーザ認証のＯＮ／ＯＦＦを設定することができ、ここで設定された内容は、ユーザ認証システム３１０がＨＤＤ２０４に認証設定３１２として格納する。各ソフトウェアモジュールは、この認証設定３１２にアクセスしてユーザ認証のＯＮ／ＯＦＦ設定を参照することができる。図５（Ｂ）の例では、ユーザ認証がＯＮに設定されている。

【００３５】

図５（Ｃ）の画面は、図５（Ａ）の画面で、ユーザアカウント管理５０３が指示されることにより表示される。図５（Ｃ）の画面では、ユーザ名と、そのユーザの権限を登録したり編集することができる。図５（Ｄ）の画面は、図５（Ｃ）の画面で、登録或いは編集が指示されたときに表示される画面例を示す。ユーザは、図５（Ｃ）と図５（Ｄ）に示すユーザインターフェース画面を表示して、ユーザアカウントの登録や編集を行うことができる。図５（Ｄ）の画面を用いて登録されたユーザのアカウントに関わる情報は、ユーザ認証システム３１０がＨＤＤ２０４のユーザＤＢ３１３に格納して管理する。図５（Ｄ）の画面では、ユーザ名「Ａｌｉｃｅ」が管理者で登録され、それとともにそのユーザ名に対応するパスワードが登録される。

【００３６】

図６は、実施形態１に係るユーザＤＢ３１３のデータ構成例を示す図である。

【００３７】

ここには、図５（Ｃ）と図５（Ｄ）に示すユーザインターフェース画面を介して登録されたユーザ名６０１、パスワード６０２、権限６０３等が登録されている。パスワード最終更新日時６０４は、図５（Ｄ）の画面を介してパスワードが登録、或いは更新された日時を示す。

【００３８】

図５（Ｅ）の画面は、図５（Ａ）の画面で、パスワードポリシー設定５０４が指示されることにより表示される。図５（Ｅ）は、パスワードに関わるポリシーを設定するためのユーザインターフェース画面例を示す。例えば、パスワードの有効期限として、「有効期限なし」、「３０日」、「９０日」を選択できる。また、パスワードの複雑さの設定として、「３文字以上」（３文字以上のパスワードを強制する設定）や、「記号を含める」（パスワードに記号を含めることを強制する設定）等の有効／無効を選択できる。図５（Ｅ）の画面を介して設定された事項は、ユーザ認証システム３１０が、ＨＤＤ２０４にパスワードポリシー設定３１４として格納する。

【００３９】

図５（Ｆ）の画面は、図５（Ａ）の画面で、認証ログ管理５０５が指示されることにより表示される。図５（Ｆ）は、認証結果のログ記録を管理するユーザインターフェース画面である。図５（Ｆ）では、ユーザ認証システム３１０がＨＤＤ２０４に記録した認証ログ３１６を閲覧することができる。この画面には、認証ログ３１６に登録されている、ユーザ名と、その認証方式、更にはその認証を行った日時とその認証結果（ＯＫ又はＮＧ）が表示される。

【００４０】

図７（Ａ）～（Ｃ）は、実施形態１に係るユーザ認証システム３１０が備えるＡＰＩ（Application Programming Interface）の例を示す図である。

【００４１】

他のソフトウェアモジュールが図７（Ａ）のＡＰＩ７０１をコールすることで、ユーザ認証システム３１０に、ユーザの認証を要求する認証要求を発行することができる。ユーザ認証システム３１０は、呼び出し元の情報７０２を基に認証処理テーブル３１５を参照して、ＡＰＩ７０１の動作を決定する。

【００４２】

図８は、実施形態１に係る認証処理テーブル３１５の内容例を示す図である。

【００４３】

認証処理テーブル３１５は、呼び出し元の情報８０１、呼び出し元のパスワード変更機能有無８０２、計算方法８０３、認証処理タイプ８０４等の組み合わせを記憶する。呼び出し元の情報８０１には、認証要求の発行元である呼び出し元の通信プロトコルが登録されている。呼び出し元パスワードの変更機能有無８０２は、呼び出し元のソフトウェアモジュールが、パスワードの変更機能を有するか否かを示す。例えば、ユーザとのインタフェースを制御するローカルＵＩ３０１は、呼び出し元パスワードの変更機能有無８０２が「有」であるため、図４（Ｂ）のパスワード変更画面を操作画面に表示する機能を有する。

【００４４】

一方、ＨＴＴＰ，ＳＭＢ／ＣＩＦＳ，ＳＮＭＰｖ３等の通信プロトコルは、パスワードを変更するためのプロトコルが規定されていない。このためＨＴＴＰサーバ３０２，ＳＭＢ／ＣＩＦＳサーバ３０４，ＳＮＭＰｖ３サーバ３０７は、パスワード変更を要求する機能が無い。計算方法８０３は、ＡＰＩ７０１がパスワードから別の値に変換するために使用する計算アルゴリズムを示す。「ＲＡＷ」は、パスワードを加工せずにそのまま使用することを示す。「ＭＤ４」は、パスワードからＭＤ４（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ａｌｇｏｒｉｔｈｍ ４）のダイジェストを算出することを示す。「ＭＤ５」は、パスワードからのＭＤ５（Ｍｅｓｓａｇｅ Ｄｉｇｅｓｔ Ａｌｇｏｒｉｔｈｍ ５）のダイジェストを算出することを示す。計算方法８０３は、これら「ＭＤ４」や「ＭＤ５」に限定するものではなく、ユーザ認証システム３１０が実装している既知の計算方法であればどのような計算方法であっても良い。例えば、ＨＭＡＣ（Ｋｅｙｅｄ－Ｈａｓｈｉｎｇ ｆｏｒ Ｍｅｓｓａｇｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ｃｏｄｅ）（ＲＦＣ２１０４）や、ＳＨＡ（Ｓｅｃｕｒｅ Ｈａｓｈ Ａｌｇｏｒｉｔｈｍ）など計算アルゴリズムが一般によく知られる。ユーザ認証システム３１０は、ＮＴＬＭや、ＳＮＭＰ ｖｅｒｓｉｏｎ３ のＵＳＭの計算アルゴリズムを計算方法として備えるようにしても良い。認証処理タイプ８０４

は、ＡＰＩ７０１の動作を「照合」と「算出値返却」のいずれかに分類する。「照合」は、ＡＰＩ７０１が、パスワードから算出した値と、呼び出し元から受信した認証データ７０４とを照合して照合結果を返却する動作を行うことを示す。「算出値返却」は、ＡＰＩ７０１が、パスワードを「計算方法」８０３で示すアルゴリズムで、パスワードと異なる値を算出し、その算出した値を返却する（図７（Ａ）の７０５）動作を行うことを示す。

【００４５】

次に、ＡＰＩ７０１が返却する戻り値７０６の意味を以下に説明する。

・ＳＵＣＣＥＳＳ

ＡＰＩ７０１の処理が成功したことを示す。認証処理タイプ８０４が「照合」の場合は、ユーザの認証処理が成功したことを示す。認証処理タイプ８０４が「算出値返却」の場合は、パスワードから算出した値をアウトプットデータ７０５に格納して返却する。

・ＳＵＣＣＥＳＳ＿ＮＥＥＤ＿ＰＷＤ＿ＣＨＡＮＧＥ

ＡＰＩ７０１の処理は成功したが、パスワードがパスワードポリシーを満たしていないため、ユーザがパスワードの変更を行う必要があることを示す。呼び出し元がパスワードの変更機能を有する場合にこの値を返却する。

・ＥＲＲＯＲ

ＡＰＩ７０１が処理を中断したことを示す。認証処理タイプ８０４が「照合」の場合は、ユーザの認証処理が失敗したことを示す。認証処理タイプ８０４が「算出値返却」の場合は、パスワードから算出した値を返却しない。

・ＥＲＲＯＲ＿ＮＥＥＤ＿ＰＷＤ＿ＣＨＡＮＧＥ

パスワードがパスワードポリシーを満たしていないため、ＡＰＩ７０１処理を中断したことを示す。呼び出し元にパスワードの変更機能が無い場合に、この値を返却する。

【００４６】

以上説明したＡＰＩ７０１の仕様は、あくまでも一例であり本発明を限定するものではない。例えば、図８に示す認証処理テーブル３１５の情報の一部もしくは全てをＡＰＩの呼び出し元から取得するように構成しても良い。一部の情報だけを呼び出し元から取得する場合は、ＡＰＩの動作を決定するのに足りない情報のみを認証処理テーブルから取得するように構成する。こうして認証処理テーブルを外部から編集可能に構成することにより、ＡＰＩを使用するソフトウェアモジュールの変更や追加に柔軟に対応することが可能となる。

【００４７】

その他のＡＰＩの例を図７（Ｂ）に示す。図７（Ｂ）のＡＰＩは、パラメータ７０８を用いて、図８に示す認証処理テーブル３１５の全ての情報を呼び出し元から取得可能にしている。このように全ての情報を呼び出し元から取得するように構成した場合は、ユーザ認証システム３１０は、認証処理テーブル３１５を参照する必要が無い。また、認証処理用のＡＰＩは１つに限定する必要はなく、予め想定される処理の組み合わせ毎に複数のＡＰＩを用意しても良い。これ以降の説明では認証処理用のＡＰＩとして、図７（Ａ）に示すＡＰＩ７０１を使用するものとして説明する。

【００４８】

図７（Ｃ）のＡＰＩは、ソフトウェアモジュールが実施したユーザ認証の結果を取得して、認証ログ３１６にログを記録するものである。

【００４９】

図９は、実施形態１に係るＭＦＰ１０１において、ソフトウェアモジュールが図７（Ａ）のＡＰＩ７０１を呼び出した際のユーザ認証システム３１０の動作を説明するフローチャートである。尚、この処理を実行するプログラムは、実行時にはＲＡＭ２０３に展開されており、ＣＰＵ２０１の制御の下に実行される。

【００５０】

この処理は、図７（Ａ）のＡＰＩ７０１がコールされて、ユーザ認証システム３１０がユーザ認証に関わる処理の要求を受信することにより開始される。まずＳ９０１でユーザ認証システム３１０は、ＡＰＩ７０１のパラメータから呼び出し元の情報７０２とユーザ

名７０３（ユーザ識別子）を取得する。次にＳ９０２に進みユーザ認証システム３１０は、呼び出し元の情報７０２を基に認証処理テーブル３１５を参照し、認証方式（パスワード変更機能の有無、計算方法、認証処理タイプ）を取得する。次にＳ９０３に進みユーザ認証システム３１０は、Ｓ９０１で取得したユーザ名がユーザＤＢ３１３（図６）に登録されているか否かを判定する。そのユーザ名が登録されている場合は、そのユーザ名と関連付けて登録されたパスワード６０２、パスワード最終更新日時６０４を取得する。一方、Ｓ９０３でユーザ名がユーザＤＢ３１３に登録されておらずパスワードが取得できなかった場合は、Ｓ９０４でユーザ認証システム３１０はパスワードが取得できないため認証失敗と判断してＳ９１４に進む。Ｓ９１４でユーザ認証システム３１０は認証失敗ログを記録する。そしてＳ９１５に進みユーザ認証システム３１０は、ＡＰＩ７０１の呼び出し元にエラー（ＥＲＲＯＲ）を返却して、この処理を終了する。

【００５１】

一方、Ｓ９０４でパスワードの取得に成功した場合はＳ９０５に進みユーザ認証システム３１０は、パスワードポリシー設定３１４を参照し、その取得したパスワードが有効期限や複雑さの設定を満たしているか否かを判定する。ここでパスワードの有効期限が切れているか、或いは複雑さを満たしていない場合はＳ９０６に進みユーザ認証システム３１０は、更に呼び出し元のパスワード変更機能の有無を判定する。ここでパスワード変更機能が有の場合はＳ９０７に進んで、処理を継続する。しかしＳ９０６でパスワード変更機能が無しと判定した場合はＳ９１４に進み、認証失敗ログを記録し、Ｓ９１５でＡＰＩ７０１の呼び出し元にエラー（ＥＲＲＯＲ＿ＮＥＥＤ＿ＰＷＤ＿ＣＨＡＮＧＥ）を返却して、この処理を終了する。

【００５２】

Ｓ９０５でユーザ認証システム３１０が、取得したパスワードが有効期限や複雑さの設定を満たしていると判定した場合、或いはＳ９０６で呼び出し元がパスワード変更機能を有すると判定した場合はＳ９０７に進む。Ｓ９０７でユーザ認証システム３１０は、認証処理テーブル３１５を参照して、その呼出し元に設定されている計算方法８０３を確認する。ここで計算方法が「ＲＡＷ」ではない場合（例えば、「ＭＤ４」や「ＭＤ５」の場合）はＳ９０８に進み、その計算方法に従って、取得したパスワードを基に計算処理を行う。ここでは例えば、ＭＤ４やＭＤ５等のアルゴリズムに従い、ＭＤ４ダイジェストやＭＤ５ダイジェストを算出する。そしてＳ９０９に進みユーザ認証システム３１０は、認証処理テーブル３１５を参照して、その呼出し元に設定されている認証処理タイプ８０４を確認する。ここで認証処理タイプ８０４が「算出値返却」の場合はＳ９１０に進みユーザ認証システム３１０は、算出した値をアウトプットデータ７０５に格納して、処理成功（ＳＵＣＣＥＳＳ）を返却して、この処理を終了する。また、このときＳ９０５のパスワードポリシーのチェックでＮＧになっている場合は、その旨（ＳＵＣＣＥＳＳ＿ＮＥＥＤ＿ＰＷＤ＿ＣＨＡＮＧＥ）を返却する。

【００５３】

一方、Ｓ９０９でユーザ認証システム３１０が認証処理タイプ８０４が「照合」であると判定した場合はＳ９１１に進みユーザ認証システム３１０は、認証データ７０４と、Ｓ９０８で算出した値とを照合する。この照合の結果、認証データ７０４と算出した値とが一致した場合はＳ９１２に進みユーザ認証システム３１０は、認証成功のログを記録してＳ９１３に進み、ＡＰＩの呼び出し元に処理成功（ＳＵＣＣＥＳＳ）を返却して、この処理を終了する。この場合、Ｓ９０５のパスワードポリシーのチェックでＮＧになっている場合は、その旨（ＳＵＣＣＥＳＳ＿ＮＥＥＤ＿ＰＷＤ＿ＣＨＡＮＧＥ）を返却する。

【００５４】

一方、Ｓ９１１の照合の結果、認証データ７０４と算出した値とが一致しないと判定した場合は認証失敗と判断してＳ９１４に進み、ユーザ認証システム３１０は認証失敗ログを記録する。そしてＳ９１５でＡＰＩの呼び出し元にエラー（ＥＲＲＯＲ）を返却して、この処理を終了する。

【００５５】

次に、ＭＦＰ１０１のユーザ認証がＯＮに設定されており、各種ソフトウェアモジュールが、ユーザ認証システム３１０を利用してユーザ認証を実施する際の動作例を説明する。ここではソフトウェアモジュールが、ローカルＵＩ３０１，ＨＴＴＰサーバ３０２，ＳＭＢ／ＣＩＦＳサーバ３０４，ＳＮＭＰサーバ３０７である場合で説明する。

【００５６】

図１０（Ａ）～（Ｄ）は、実施形態１に係るＭＦＰ１０１がユーザ認証を実施する際のソフトウェアモジュールとの関係をデータの流れと共に示す図である。

【００５７】

図１０（Ａ）はローカルＵＩ３０１がユーザ認証システム３１０を利用してユーザ認証を実施する場合を説明する図である。図１０（Ａ）において、ユーザ認証画面を操作画面に表示して、ＭＦＰ１０１を利用するユーザにユーザ認証を要求する。ローカルＵＩ３０１はＳ１００１で、ユーザが図４（Ａ）のユーザ認証画面に入力したユーザ名及びパスワードを取得する。またＳ１００２でローカルＵＩ３０１は、図７（Ａ）のＡＰＩ７０１を介して、それらユーザ名とパスワードをユーザ認証システム３１０に渡して認証処理を要求する。これによりユーザ認証システム３１０は認証処理テーブル３１５を参照して、パスワードポリシーチェック、パスワードの照合、認証ログの記録を行い、Ｓ１００３で、その処理結果をローカルＵＩ３０１に応答する。

【００５８】

ここでローカルＵＩ３０１は、結果が成功（ＳＵＣＣＥＳＳ）であった場合は、例えば図４（Ｃ）のメニュー画面を表示して、ユーザにＭＦＰ１０１の機能の利用を許可する。一方、認証結果がＮＧ（ＳＵＣＣＥＳＳ＿ＮＥＥＤ＿ＰＷＤ＿ＣＨＡＮＧＥ）であった場合は、パスワードポリシーのチェックがＮＧであったため操作画面に、図４（Ｂ）のパスワード変更画面を表示して、ユーザにパスワードの変更を求める。また認証結果が、エラー（ＥＲＲＯＲ）であった場合は図４（Ａ）のユーザ認証画面を表示し、ユーザに認証情報の再入力を求める。

【００５９】

次に、ＭＦＰ１０１のＨＴＴＰサーバ３０２の動作を図１０（Ｂ）を参照して説明する。図１０（Ｂ）は、ＨＴＴＰサーバ３０２がユーザ認証システム３１０を利用してユーザ認証を実施する場合を説明する図である。

【００６０】

ＨＴＴＰサーバ３０２はＳ１００４で、ウェブブラウザ３１７からＨＴＴＰのＤｉｇｅｓｔ認証（ＲＦＣ ２６１７）を含むＨＴＭＬ取得要求を受信する。これによりＨＴＴＰサーバ３０２は、ユーザ名とＭＤ５ダイジェストをパケットから取得し、Ｓ１００５で、ＡＰＩ７０１を介してユーザ認証システム３１０に認証処理を要求する。これによりユーザ認証システム３１０は、認証処理テーブル３１５を参照して、パスワードポリシーチェック、ＭＤ５ダイジェストの算出と照合処理を実行し、その認証ログの記録を行い、Ｓ１００６で、その認証結果を応答する。ＨＴＴＰサーバ３０２は、その認証結果が成功（ＳＵＣＣＥＳＳ）であった場合は、Ｓ１００７でＨＴＭＬの取得要求をリモートＵＩ３０３に伝える。これによりリモートＵＩ３０３は、認証したユーザの情報をＨＴＴＰサーバ３０２から取得し、そのユーザに応じたＨＴＭＬの提供やアクセス制御を行う。一方、結果が失敗（ＥＲＲＯＲ・ＥＲＲＯＲ＿ＮＥＥＤ＿ＰＷＤ＿ＣＨＡＮＧＥ）であった場合は、ＨＴＴＰサーバ３０２はウェブブラウザ３１７にエラーを通知する。

【００６１】

次に、ＭＦＰ１０１のＳＭＢ／ＣＩＦＳサーバ３０４の動作を図１０（Ｃ）を参照して説明する。図１０（Ｃ）は、ＳＭＢ／ＣＩＦＳサーバ３０４がユーザ認証システム３１０を利用してユーザ認証を実施する場合を説明する図である。

【００６２】

ＳＭＢ／ＣＩＦＳサーバ３０４は、Ｓ１００８でＰＣ１０２のファイル管理ツール３１９からＮＴＬＭデータフォーマットの認証データを含むパケットを受信する。これによりＳＭＢ／ＣＩＦＳサーバ３０４は、ユーザ名をパケットから取得し、Ｓ１００９で、ＡＰ

Ｉ７０１を介して、ユーザ認証システム３１０に認証処理を要求する。これによりユーザ認証システム３１０は、認証処理テーブル３１５を参照して、パスワードポリシーチェック、ＭＤ４ダイジェストの算出を行い、Ｓ１０１０で、その処理結果と共に、ＭＤ４ダイジェストを返却する。これによりＳＭＢ／ＣＩＦＳサーバ３０４は、ＮＴＬＭ認証処理部３０５において、ユーザ認証システム３１０から取得したＭＤ４ダイジェストとパケットから取得したＮＴＬＭの認証データを用いてＮＴＬＭの認証処理を行う。そしてＳＭＢ／ＣＩＦＳサーバ３０４は、ＮＴＬＭ認証処理部３０５による認証結果を取得し、Ｓ１０１１で、図７（Ｃ）のＡＰＩを介してユーザ名と認証結果をユーザ認証システム３１０に通知する。

【００６３】

ここでユーザの認証に成功した場合は、ＳＭＢ／ＣＩＦＳサーバ３０４は、その後のＰＣ１０２のファイル管理ツール３１９から文書管理サービス３０６へのアクセスを許可する。文書管理サービス３０６は、Ｓ１０１２でＳＭＢ／ＣＩＦＳサーバ３０４からユーザ情報を取得し、そのユーザに応じたサービス提供やアクセス制御を行う。一方、ユーザの認証が失敗した場合、ＳＭＢ／ＣＩＦＳサーバ３０４は、ＰＣ１０２のファイル管理ツール３１９にエラーを通知する。

【００６４】

次に、ＭＦＰ１０１のＳＮＭＰサーバ３０７の動作を図１０（Ｄ）を参照して説明する。図１０（Ｄ）は、ＳＮＭＰサーバ３０７がユーザ認証システム３１０を利用してユーザ認証を実施する場合を説明する図である。

【００６５】

ＳＮＭＰサーバ３０７は、Ｓ１０１３で、ＰＣ１０２のＭＦＰ管理ツール３２１からＳＮＭＰｖ３のＵＳＭ（ＲＦＣ３４１４）に従った認証データを含むパケットを受信する。そしてＳＮＭＰサーバ３０７は、そのパケットからユーザ名を取得し、Ｓ１０１４で、ＡＰＩ７０１を介してユーザ認証システム３１０に認証処理を要求する。これによりユーザ認証システム３１０は、認証処理テーブル３１５を参照して、パスワードポリシーチェック、ＭＤ５ダイジェストの算出を行い、Ｓ１０１５で、その処理結果と共に、ＭＤ５ダイジェストを返却する。これによりＳＮＭＰサーバ３０７は、ＵＳＭ認証処理部３０８において、ユーザ認証システム３１０から取得したＭＤ４ダイジェストとパケットから取得したＮＴＬＭの認証データを用いてＮＴＬＭの認証処理を行う。そしてＳＮＭＰサーバ３０７は、ＵＳＭ認証処理部３０８の認証結果を取得し、Ｓ１０１６で、図７（Ｃ）のＡＰＩを介してユーザ名と認証結果をユーザ認証システム３１０に通知する。ここでユーザ認証が成功した場合は、ＳＮＭＰサーバ３０７は、Ｓ１０１７で、ＭＦＰ管理ツール３２１が要求するＭＩＢ３０９へのアクセスを実施する。ＳＮＭＰサーバ３０７は、ユーザに応じたＭＩＢ３０９へのアクセス制御を行う。一方、ユーザの認証が失敗した場合、ＳＮＭＰサーバ３０７は、ＰＣ１０２のＭＦＰ管理ツール３２１にエラーを通知する。

【００６６】

以上説明したように本実施形態１によれば、ＭＦＰ１０１のユーザ認証機構を単一のユーザ認証システム３１０で実現しているため、ユーザ認証に関わる設定の管理やユーザアカウントの管理の煩わしさを軽減できる。

【００６７】

また本実施形態１によれば、全てのアクセス経路に対して、パスワードセキュリティポリシー、認証ログの記録機能を提供するため、全てのアクセス経路に同等のセキュリティ機能を適用できる。

【００６８】

またＭＦＰのユーザ認証システム３１０を利用するソフトウェアモジュールは、パスワードセキュリティポリシー、認証ログの記録に必ずしも対応している必要は無く、既存のソフトウェアモジュールやソースコードの改造コストがかからないという利点がある。

【００６９】

更に本実施形態１によれば、ユーザ認証システム３１０とユーザ認証システムを利用す

るソフトウェアモジュールとがユーザ認証に関わる処理を分散処理できる。このため、既存のソフトウェアモジュールやソースコードを最大限利用しつつ、ユーザ認証に関わる管理が統合された機器を構成できるという効果がある。

【００７０】

［実施形態２］

前述のユーザ認証システム３１０は、必ずしもＭＦＰ１０１の内部にある必要はなく、ネットワーク上の別のノードで構成しても良い。

【００７１】

図１１は、本発明の実施形態２に係るユーザ認証システムを認証サーバとして構成したシステム構成の例を示す図である。

【００７２】

ここでは、ＭＦＰ１１０１とＰＣ１１０２、認証サーバ１１０３がＬＡＮ１１００を介して接続されている。尚、ＭＦＰ１１０１とＰＣ１０２のハードウェア構成は前述の実施形態１に係るＭＦＰ１０１とＰＣ１０２のハードウェア構成と同じであるため、その説明を省略する。

【００７３】

図１２は、実施形態に２に係るＭＦＰ１１０１と認証サーバ１１０３のソフトウェア構成を示すブロック図である。ＰＣ１１０２の構成は、前述の実施形態１のＰＣ１０２と同じ構成であるため、その説明を省略する。尚、前述の図３と共通する部分は同じ記号で示し、それらの説明を省略する。またユーザ認証サーバ１１０３の１２１１～１２１６で示す構成は、前述の図３の３１１～３１６で示す構成と同じ機能を有するため、その説明を省略する。

【００７４】

ＭＦＰ１１０１は、認証サーバ１１０３と通信するためのエージェント１２０１を備える。認証サーバ１１０３は、ユーザ認証システム１２０２を備える。ＭＦＰ１１０１と認証サーバ１１０３は、事前に通信に使用する秘密の暗号鍵を交換することにより信頼関係を構築することができる。ＰＫＩ技術を用いたクライアント証明書やサーバ証明書など第三者が発行した証明書を交換しても良い。

【００７５】

エージェント１２０１は、ユーザ認証システム１２０２が持つＡＰＩと同等のＡＰＩ（図７（Ａ）の７０１，図７（Ｃ）など）を備える。エージェント１２０１は、他のソフトウェアモジュールからＡＰＩをコールされると、ネットワークの通信を介してユーザ認証システム１２０２のＡＰＩをコールして処理結果を取得する。このときネットワーク上に流す情報は秘匿する必要があるため、事前に交換した鍵を利用して暗号化を行う。このようにユーザ認証システム１２０２をネットワーク上の独立したノード（認証サーバ）で構成することにより、複数のＭＦＰから利用可能なユーザ認証システムを提供することができる。

【００７６】

以上説明したように本実施形態によれば、以下の様な効果が得られる。

・ユーザ認証機構を単一のユーザ認証システムで実現可能にしたことにより、ユーザ認証に関わる設定の管理やユーザアカウントの管理の煩わしさを軽減できる。

・ユーザ認証システムを利用した機器に対する全てのアクセス経路に、同じユーザ認証機構を適用することができる。

・既存のソフトウェアモジュールやソースコードを流用することができ、比較的少ない手間と工数で、ユーザの認証を行うことができる機器を構成することができる。

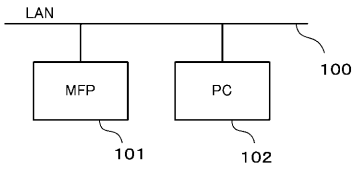
【００７７】

（その他の実施形態）

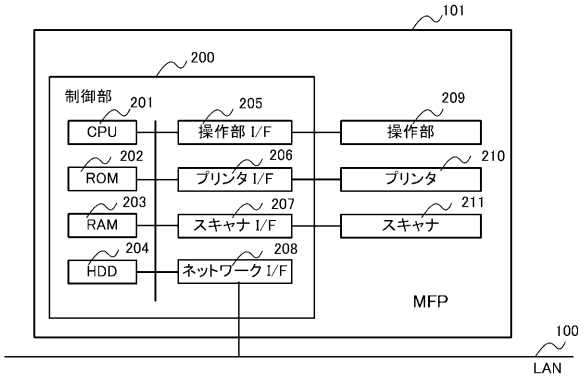
また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（又はＣ

ＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

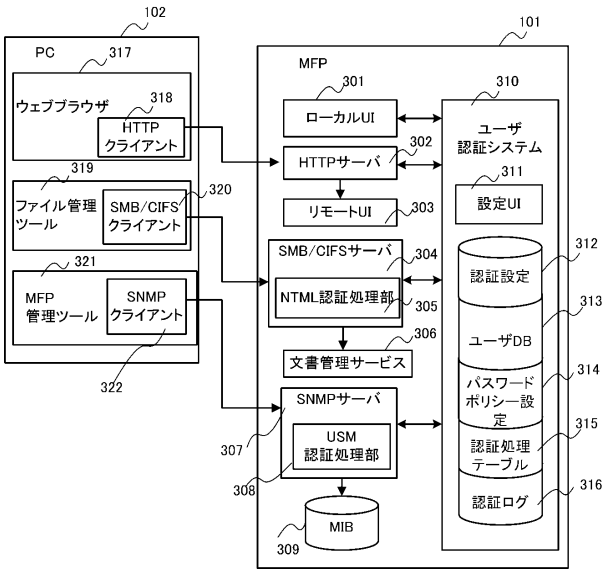
【図１】



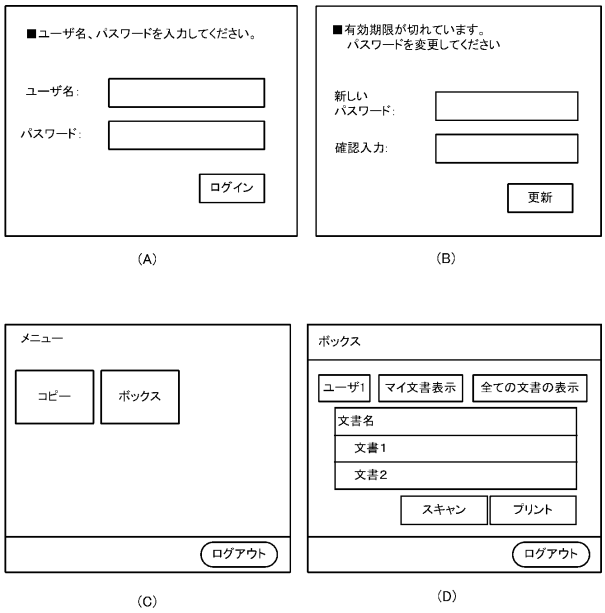
【図２】



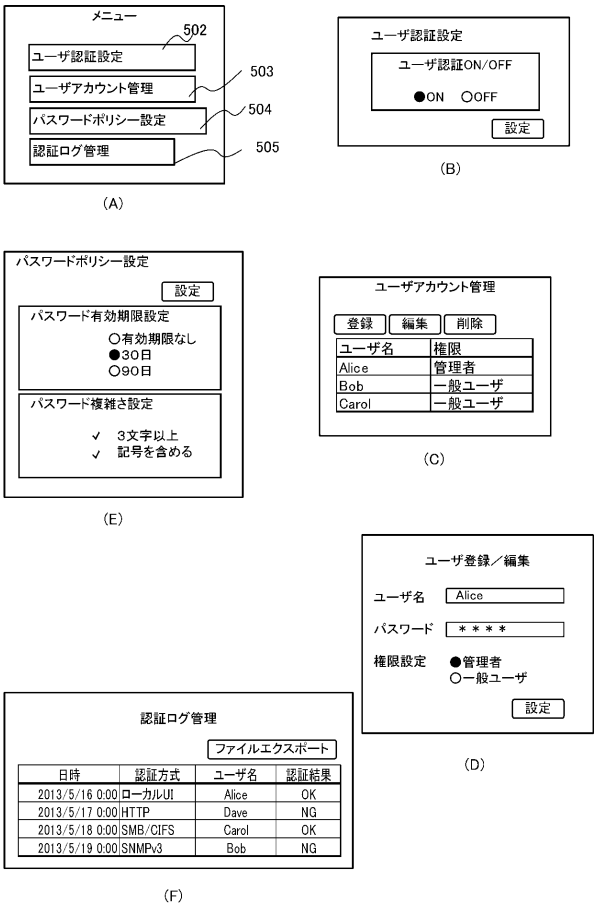
【図３】



【図４】



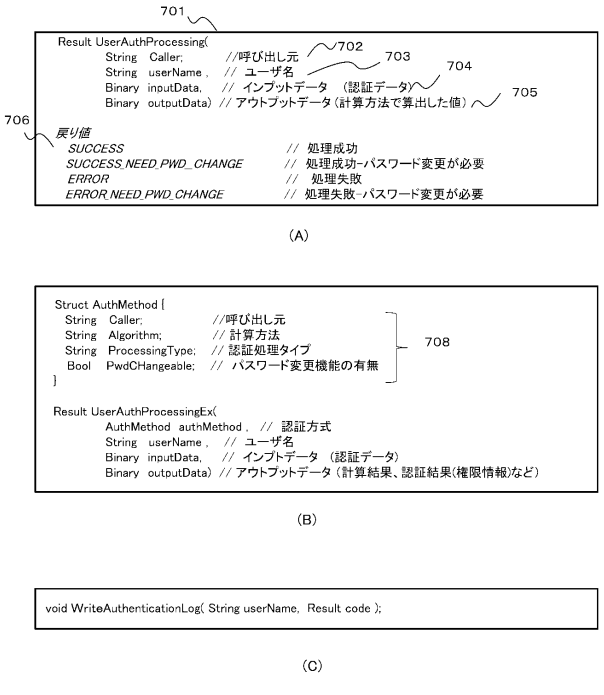
【図５】



【図６】

601 ユーザ名	602 パスワード	603 権限	604 パスワード最終更新日時
Alice	****	管理者	2013/2/1 10:00
Bob	****	一般ユーザ	2013/2/2 10:00
Carol	****	一般ユーザ	2013/2/3 10:00

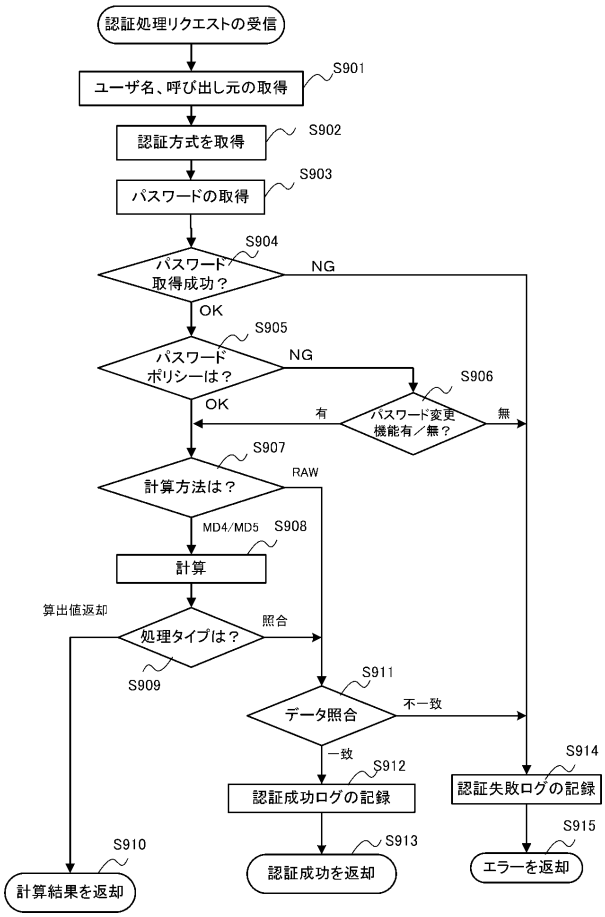
【図７】



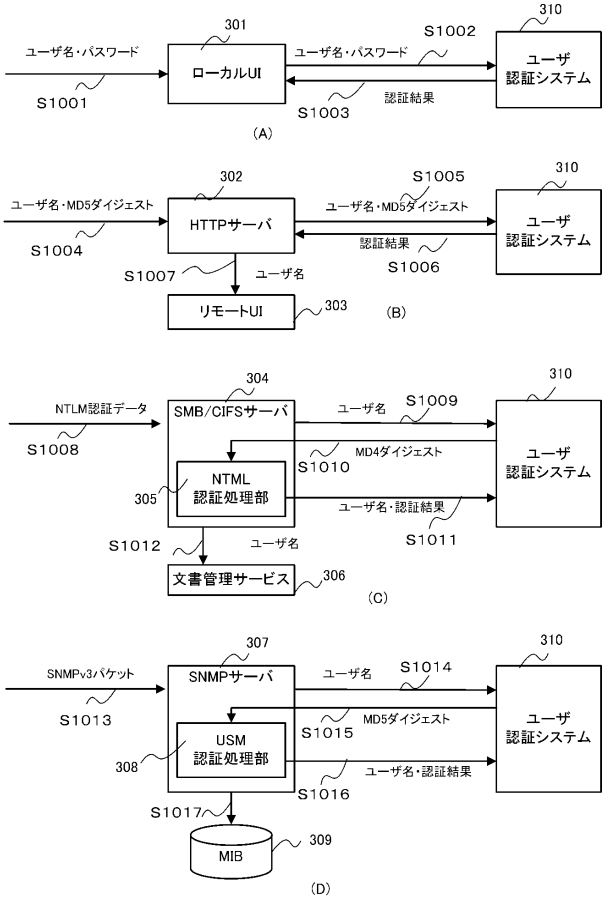
【図８】

801 呼出し元	802 呼出し元のパスワード変更機能有無	803 計算方法	804 認証処理タイプ
ローカルUI	有	RAW	照合
HTTP	無	MD5	照合
SMB／CIFS	無	MD4	算出値返却
SNMPv3	無	MD5	算出値返却

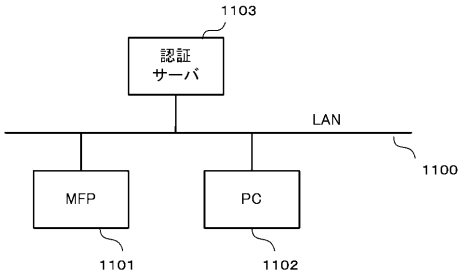
【図９】



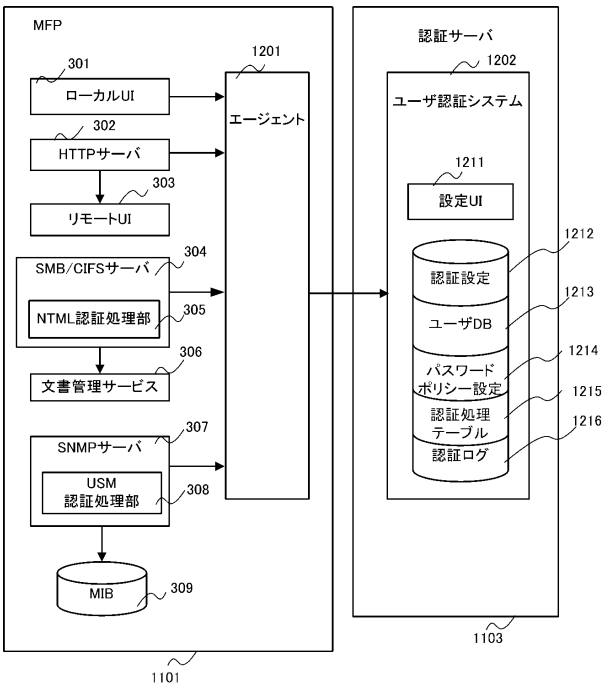
【図１０】



【図１１】



【図１２】



フロントページの続き

(72)発明者　細田　泰弘
東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内

審査官　行田　悦資

(56)参考文献　特開２００４－０７８６２２（ＪＰ，Ａ）
特開２００２－２０２９５５（ＪＰ，Ａ）
特開２００７－２９９２９５（ＪＰ，Ａ）
特開２００９－２４５１１９（ＪＰ，Ａ）
特開２００７－１８８２０９（ＪＰ，Ａ）
米国特許出願公開第２０１３／０１１１５７３（ＵＳ，Ａ１）
特開２００３－１５７２３４（ＪＰ，Ａ）
特開２０１３－０４１５１４（ＪＰ，Ａ）
特開２００５－００４７６９（ＪＰ，Ａ）
特表２００６－５２６８４３（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／４６
Ｂ４１Ｊ　２９／００
Ｂ４１Ｊ　２９／３８
Ｇ０６Ｆ　２１／３１
Ｈ０４Ｌ　９／３２