(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2007-48080
(P2007-48080A)
(43)公開日　平成19年2月22日(2007.2.22)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330D	5B021
G06Q 10/00	(2006.01)	G06F	17/60	174	5B076
G06F 21/22	(2006.01)	G06F	17/60	512	5B276
G06F 3/12	(2006.01)	G06F	9/06	660E	5B285
H04N 1/00	(2006.01)	G06F	3/12	K	5C062

審査請求 未請求　請求項の数 19　ＯＬ　（全 18 頁）　最終頁に続く

(21)出願番号　特願2005-232357 (P2005-232357)
(22)出願日　平成17年8月10日 (2005.8.10)

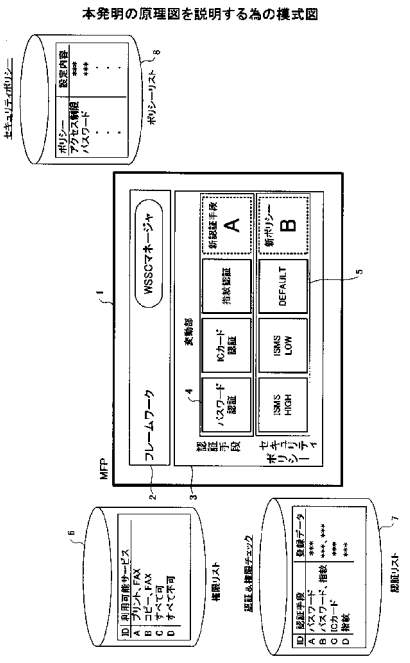
(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　藤本　綾子
東京都大田区中馬込１丁目３番６号　株式会社リコー内

Ｆターム(参考)　5B021 AA01
5B076 FB05
5B276 FB05
5B285 AA04 BA04 CA06
5C062 AA05 AB11 AB42 AC22 AC58
AF12 AF14

(54)【発明の名称】サービス提供装置，サービス提供方法及びサービス提供プログラム

(57)【要約】
【課題】　利用者の要望に応じたセキュリティ情報を柔軟に設定可能なサービス提供装置，サービス提供方法及びサービス提供プログラムを提供することを目的とする。
【解決手段】　利用者にサービスを提供する為の１つ以上の機能を有し、その機能を用いてサービスを提供するサービス提供装置１であって、セキュリティに関する１つ以上のセキュリティ情報５と、利用者の認証を行なう１つ以上の認証手段４と、利用可能なサービス，認証に利用する認証手段４およびセキュリティ情報が利用者毎に関連付けられた情報を取得し、利用者に関連付けられているセキュリティ情報に対応した認証レベルの認証手段４を用いた認証結果が正常終了したときに、利用者に関連付けられているサービスを機能に提供させるサービス提供手段２とを備えたことにより上記課題を解決する。
【選択図】　図１

本発明の原理図を説明する為の模式図



【特許請求の範囲】
【請求項１】
利用者にサービスを提供する為の１つ以上の機能を有し、その機能を用いてサービスを提供するサービス提供装置であって、
セキュリティに関する１つ以上のセキュリティ情報と、
利用者の認証を行なう１つ以上の認証手段と、
利用可能なサービス，認証に利用する認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を取得し、利用者に関連付けられている前記セキュリティ情報に対応した認証レベルの前記認証手段を用いた認証結果が正常終了したときに、利用者に関連付けられている前記利用可能なサービスを前記機能に提供させるサービス提供手段と
を備えたサービス提供装置。
【請求項２】
前記セキュリティ情報は、データ通信可能な外部装置からのダウンロードまたはデータの読み出しが可能な記録媒体からのインストールにより追加されることを特徴とする請求項１記載のサービス提供装置。
【請求項３】
前記セキュリティ情報のダウンロード元となる外部装置、又は前記セキュリティ情報のインストール元となる記録媒体を一つ以上表示し、前記外部装置又は記録媒体の何れか一つを選択させる表示手段を更に備えた請求項２記載のサービス提供装置。
【請求項４】
前記セキュリティ情報に対応した認証レベルの前記認証手段を用いた認証結果が正常終了したときに、利用者に関連付けられている前記利用可能なサービスを一つ以上表示する表示手段を更に備えた請求項１記載のサービス提供装置。
【請求項５】
前記サービス提供手段は、利用者ＩＤを取得し、前記利用者ＩＤに関連付けられている前記セキュリティ情報を検索することを特徴とする請求項１記載のサービス提供装置。
【請求項６】
前記サービス提供手段は、検索された前記セキュリティ情報に対応した認証レベルの前記認証手段を用いて利用者の認証を行い、前記認証手段を用いた認証結果が正常終了したときに、前記利用者ＩＤに関連付けられている前記利用可能なサービスをチェックすることを特徴とする請求項５記載のサービス提供装置。
【請求項７】
前記認証手段は、パスワード認証，ＩＣカード認証又は指紋認証を行なうことを特徴とする請求項１乃至６何れか一項記載のサービス提供装置。
【請求項８】
前記サービス提供装置は、印刷部又は撮像部を有し、画像形成にかかるアプリケーションを複数搭載可能とした画像処理装置であって、
オペレーティングシステムと、
前記オペレーティングシステム上で動作し、複数の前記アプリケーションからアクセスされ、複数の前記アプリケーションで共通的に利用される前記画像形成処理の制御を行なうプログラムとを備え、
前記セキュリティ情報，認証手段およびサービス提供手段は、前記アプリケーションに含まれることを特徴とする請求項１乃至７何れか一項記載のサービス提供装置。
【請求項９】
利用可能なサービス，認証に利用する認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を、データ通信可能な外部装置から取得することを特徴とする請求項１乃至８何れか一項記載のサービス提供装置。
【請求項１０】
利用者にサービスを提供する為の１つ以上の機能を有し、その機能を用いてサービスを提供するサービス提供装置のサービス提供方法であって、

前記サービス提供装置は、セキュリティに関する１つ以上のセキュリティ情報と、
利用者の認証を行なう１つ以上の認証手段とを備え、
利用可能なサービス，認証に利用する認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を取得するステップと、
利用者に関連付けられている前記セキュリティ情報に対応した認証レベルの前記認証手段を用いた認証結果が正常終了したときに、利用者に関連付けられている前記利用可能なサービスを前記機能に提供させるステップと
を有するサービス提供方法。

【請求項１１】
前記セキュリティ情報が、データ通信可能な外部装置からのダウンロードまたはデータの読み出しが可能な記録媒体からのインストールにより追加されるステップを更に有することを特徴とする請求項１０記載のサービス提供方法。

【請求項１２】
前記セキュリティ情報のダウンロード元となる外部装置、又は前記セキュリティ情報のインストール元となる記録媒体を一つ以上表示し、前記外部装置又は記録媒体の何れか一つを選択させるステップを更に有することを特徴とする請求項１１記載のサービス提供方法。

【請求項１３】
前記セキュリティ情報に対応した認証レベルの前記認証手段を用いた認証結果が正常終了したときに、利用者に関連付けられている前記利用可能なサービスを一つ以上表示するステップを更に有することを特徴とする請求項１０記載のサービス提供方法。

【請求項１４】
利用者ＩＤを取得し、前記利用者ＩＤに関連付けられている前記セキュリティ情報を検索するステップを更に有することを特徴とする請求項１０記載のサービス提供方法。

【請求項１５】
検索された前記セキュリティ情報に対応した認証レベルの前記認証手段を用いて利用者の認証を行うステップと、
前記認証手段を用いた認証結果が正常終了したときに、前記利用者ＩＤに関連付けられている前記利用可能なサービスをチェックするステップとを更に有することを特徴とする請求項１４記載のサービス提供方法。

【請求項１６】
前記認証手段が、パスワード認証，ＩＣカード認証又は指紋認証を行なうことを特徴とする請求項１０乃至１５何れか一項記載のサービス提供方法。

【請求項１７】
前記サービス提供装置は、印刷部又は撮像部を有し、画像形成にかかるアプリケーションを複数搭載可能とした画像処理装置のサービス提供方法であって、
前記画像処理装置は、オペレーティングシステムと、
前記オペレーティングシステム上で動作し、複数の前記アプリケーションからアクセスされ、複数の前記アプリケーションで共通的に利用される前記画像形成処理の制御を行なうプログラムとを備え、
前記セキュリティ情報および認証手段は、前記アプリケーションに含まれることを特徴とする請求項１０乃至１６何れか一項記載のサービス提供方法。

【請求項１８】
利用可能なサービス，認証に利用する認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を、データ通信可能な外部装置から取得するステップを更に有することを特徴とする請求項１０乃至１７何れか一項記載のサービス提供方法。

【請求項１９】
利用者にサービスを提供する為の１つ以上の機能を有し、その機能を用いてサービスを提供するサービス提供装置を、
セキュリティに関する１つ以上のセキュリティ情報を格納する格納手段と、

利用者の認証を行なう１つ以上の認証手段と、
利用可能なサービス，認証に利用する認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を取得し、利用者に関連付けられている前記セキュリティ情報に対応した認証レベルの前記認証手段を用いた認証結果が正常終了したときに、利用者に関連付けられている前記利用可能なサービスを前記機能に提供させるサービス提供手段と
して機能させるためのサービス提供プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、サービス提供装置，サービス提供方法及びサービス提供プログラムに係り、特に利用者にサービスを提供するサービス提供装置，サービス提供方法及びサービス提供プログラムに関する。
【背景技術】
【０００２】
近年、プリンタ，コピー，ファクシミリおよびスキャナなどの各装置の機能を１つの筐体内に収納した情報処理装置の一例としての画像処理装置（以下、複合機という）が知られるようになった。この複合機は、１つの筐体内に表示部，印刷部および撮像部などを設けると共に、プリンタ，コピー，ファクシミリおよびスキャナにそれぞれ対応する４種類のソフトウェアを設け、そのソフトウェアを切り替えることより、プリンタ，コピー，ファクシミリおよびスキャナとして動作させるものである。特許文献１には、上記のような複合機の一例が記載されている。
【０００３】
このような複合機では、プリンタ，コピー，ファクシミリ又はスキャナとして動作するときに、利用者がプリンタ，コピー，ファクシミリ又はスキャナを利用する権限を有しているかを認証手段を利用して認証していた。なお、複合機ではセキュリティに関する決まりごとやルールをセキュリティポリシーとして体系化している。
【０００４】
特許文献２には、カードリーダにカードがセットされているときに利用者が利用可能な画像処理システムの一例が記載されている。
【特許文献１】特開２００２－８４３８３号公報
【特許文献２】特開２００２－２８８７３７号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】
従来の複合機は、利用する可能性のある認証手段を複合機単位で予め設定している。しかしながら、利用者や管理者が複合機に求めるセキュリティレベルは様々であるため、複合機に搭載される認証手段の組み合わせも様々である。また、認証手段のセキュリティレベルは新しい方式または新しいバージョンほど高くなることが多い。
【０００６】
従って、従来の複合機では搭載されている認証手段に応じたセキュリティポリシーを複合機単位で予め設定しておく必要があった。つまり、従来の複合機は、利用する可能性のあるセキュリティポリシーを複合機単位で予め設定しておく必要があった。なお、利用者や管理者が複合機に求めるセキュリティレベル、言い換えればセキュリティポリシーは様々である。
【０００７】
従来の複合機は、セキュリティポリシーを追加，変更，削除するためにプログラムの修正が必要であり、セキュリティポリシーを容易に追加，変更，削除できない。この為、従来の複合機では利用者の要望に応じたセキュリティポリシーを、柔軟に設定できないという問題があった。
【０００８】

本発明は、上記の点に鑑みなされたもので、利用者の要望に応じたセキュリティ情報を柔軟に設定可能なサービス提供装置，サービス提供方法及びサービス提供プログラム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】

【０００９】

そこで、上記課題を解決するため、本発明は、利用者にサービスを提供する為の１つ以上の機能を有し、その機能を用いてサービスを提供するサービス提供装置であって、セキュリティに関する１つ以上のセキュリティ情報と、利用者の認証を行なう１つ以上の認証手段と、利用可能なサービス，認証に利用する認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を取得し、利用者に関連付けられている前記セキュリティ情報に対応した認証レベルの前記認証手段を用いた認証結果が正常終了したときに、利用者に関連付けられている前記利用可能なサービスを前記機能に提供させるサービス提供手段とを備えたことを特徴とする。

【００１０】

また、本発明は、利用者にサービスを提供する為の１つ以上の機能を有し、その機能を用いてサービスを提供するサービス提供装置のサービス提供方法であって、前記サービス提供装置は、セキュリティに関する１つ以上のセキュリティ情報と、利用者の認証を行なう１つ以上の認証手段とを備え、利用可能なサービス，認証に利用する認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を取得するステップと、利用者に関連付けられている前記セキュリティ情報に対応した認証レベルの前記認証手段を用いた認証結果が正常終了したときに、利用者に関連付けられている前記利用可能なサービスを前記機能に提供させるステップとを有することを特徴とする。

【００１１】

また、本発明は、利用者にサービスを提供する為の１つ以上の機能を有し、その機能を用いてサービスを提供するサービス提供装置を、セキュリティに関する１つ以上のセキュリティ情報を格納する格納手段と、利用者の認証を行なう１つ以上の認証手段と、利用可能なサービス，認証に利用する認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を取得し、利用者に関連付けられている前記セキュリティ情報に対応した認証レベルの前記認証手段を用いた認証結果が正常終了したときに、利用者に関連付けられている前記利用可能なサービスを前記機能に提供させるサービス提供手段として機能させるためのサービス提供プログラムであることを特徴とする。

【００１２】

本発明では、セキュリティ情報を追加可能である。本発明では、サービス，認証手段およびセキュリティ情報が利用者毎に関連付けられた情報を取得して、利用者に関連付けられているセキュリティ情報に対応した認証レベルの認証手段を用いることにより、使用者毎に異なるセキュリティ情報に対応した認証レベルの認証手段を柔軟に設定できる。本発明では、使用者毎に異なるセキュリティ情報に対応した認証レベルの認証手段により行った認証結果が正常終了したときに、利用者に関連付けられているサービスを機能に提供させることができる。

【発明の効果】

【００１３】

本発明によれば、利用者の要望に応じたセキュリティ情報を柔軟に設定可能なサービス提供装置，サービス提供方法及びサービス提供プログラムを提供できる。

【発明を実施するための最良の形態】

【００１４】

次に、本発明を実施するための最良の形態を、以下の実施例に基づき図面を参照しつつ説明していく。なお、本実施例では、サービス提供装置の一例としての複合機を例に説明するが、使用者にサービスを提供する如何なるサービス提供装置であってもよい。

【００１５】

図１は、本発明の原理図を説明する為の模式図である。複合機（ＭＦＰ）１は、固定部

としてのフレームワーク２，変動部３を含む構成である。変動部３は、１つ以上の認証手段から成る認証変動部４，１つ以上のセキュリティポリシーから成るポリシー変動部５を含む構成である。図１の認証変動部４は、認証手段としてのパスワード認証，ＩＣカード認証，指紋認証から成る。また、図１のポリシー変動部５はセキュリティポリシーＩＳＭＳ　ＨＩＧＨ，ＩＳＭＳ　ＬＯＷ，ＤＥＦＡＵＬＴから成る。ここで言う、セキュリティポリシーとは、セキュリティに関する情報であって、セキュリティ対策を規定するものである。

【００１６】

フレームワーク２は、サービス利用権限チェック，認証，権限サーバや認証サーバの検索などを行なう。例えばフレームワーク２は権限サーバを検索し、権限サーバが格納している権限リスト６を取得して、サービス利用権限チェックを行なう。権限リスト６は、利用者ＩＤと、その利用者ＩＤにより識別される利用者の利用可能サービスとを関連付けた情報である。また、フレームワーク２は認証サーバを検索し、認証サーバが格納している認証リスト７を取得して、認証を行なう。認証リスト７は、利用者ＩＤと、その利用者ＩＤにより識別される利用者の認証に利用する認証手段と、パスワード等の登録データとを関連付けた情報である。

【００１７】

変動部３の認証変動部４は、データ通信可能な外部装置からのダウンロード又はデータの読み出しが可能な記録媒体からのインストールにより認証手段が追加される。本実施例で言う認証手段は、認証の為の処理を行う認証アプリケーションである。また、変動部３のポリシー変動部５はフレームワーク２のポリシーリスト８により表される。ポリシーリスト８は、ポリシーと、そのポリシーの設定内容とを関連付けた情報である。

【００１８】

複合機１は、利用者に合わせた認証変動部４及びポリシー変動部５を変動部３として開発及び提供される。つまり、複合機１は変動部３を開発及び提供されることで、利用者の要望に応じた認証手段およびセキュリティポリシーの追加，変更，削除などの設定を柔軟に行なうことができる。

【００１９】

図２は、本発明による複合機の一実施例の構成図を示す。図２の複合機１は、ハードウェア資源１０と，ソフトウェア群１１とを有するように構成されている。ハードウェア資源１０は、プロッタ２１と，スキャナ２２と，ＩＣカードリーダ２３，ＳＤカードリーダ２４などのその他のハードウェアリソースとを有する。ソフトウェア群１１は、ＵＮＩＸ（登録商標）などのオペレーティングシステム（以下、ＯＳという）２５上で実行されているアプリケーションとプラットフォームとを有する。

【００２０】

アプリケーションは、コピーアプリ２７，ファックスアプリ２８，スキャナアプリ２９及びＷＳＳＣ（Ｗｅｂサービスサーバコンポーネント）３０などを有している。プラットフォームは、コントロールサービス２６を有する。

【００２１】

コントロールサービス２６は、ＳＣＳ（システムコントロールサービス），ＥＣＳ（エンジンコントロールサービス），ＭＣＳ（メモリコントロールサービス），ＯＣＳ（オペレーションパネルコントロールサービス），ＦＣＳ（ファックスコントロールサービス），ＮＣＳ（ネットワークコントロールサービス）など、一つ以上のサービスモジュールを有するように構成されている。なお、プラットフォームはＡＰＩ（アプリケーションプログラムインターフェース）を有するように構成されている。

【００２２】

ＷＳＳＣ３０は、図１に示したフレームワーク２と、認証変動部４及びポリシー変動部５から成る変動部とを有するように構成されている。図２のフレームワーク２はＷＳＳＣマネージャ３１を有しており、そのＷＳＳＣマネージャ３１を共通のインタフェースとしてコントロールサービス２６に接続される。フレームワーク２は、複合機１に認証手段，

セキュリティポリシーを追加、又は複合機１から認証手段，セキュリティポリシーを変更または削除する為のものである。認証手段は、フレームワーク２のＷＳＳＣマネージャ３１を介してコントロールサービス２６に接続される。なお、図２に示した複合機１のコントロールサービス２６等の詳細は、例えば特開２００２－８４３８３号公報などに記載されている。以下、複合機１により実現されるサービス提供方法について、図面を参照しつつ説明していく。

（セキュリティポリシーの設定）

複合機１の利用者又はサードベンダー等は、予め希望のセキュリティポリシーを複数設定しておく。セキュリティポリシーの設定は、ＭＦＰアプリ作成用ソフトを実行可能なＰＣ等で行なう。ここで言うＭＦＰアプリは、認証手段およびセキュリティポリシーを含むものとする。

【００２３】

図３は、セキュリティポリシーの設定処理を表すイメージ図である。セキュリティポリシーの設定は、ＰＣの表示装置に表示されるＧＵＩ３５により行われる。ＧＵＩ３５はポリシー毎に設定内容を変更可能である。また、ＧＵＩ３５のユーザ追加ボタン３６が押下されると、ユーザリスト３７が表示される。利用者又はサードベンダー等はユーザリスト３７からポリシー適用対象ユーザを選択できる。

【００２４】

ＧＵＩ３５のＯＫボタン又は適用ボタンが押下されると、例えばＭＦＰアプリ作成用ソフトがＧＵＩ３５の設定内容からセキュリティポリシー３８を自動生成又はハードコーディングする。図３では、セキュリティポリシーＩＳＭＳ　ＬＯＷを設定している。図４はセキュリティポリシーの設定処理を表す他の例のイメージ図である。図４ではセキュリティポリシーＩＳＭＳ　ＭＩＤを設定するときのイメージ図を表している。

（ＭＦＰアプリの作成及びインストール）

図５は、ＭＦＰアプリの作成及びインストールを表すイメージ図である。ＭＦＰアプリの作成は、ＭＦＰアプリ作成用ソフトを実行可能なＰＣ５１で行なう。ＰＣ５１は、作成した１つ以上のＭＦＰアプリをメディアの一例としてのＳＤカード５２に記録する。ＳＤカード５２は、データの記録及び読み出しが可能な記録媒体の一例である。

【００２５】

ＭＦＰアプリが記録されたＳＤカード５２は、例えばＭＦＰ５３のＳＤカードスロットに挿入される。ＭＦＰ５３は、ＳＤカードスロットに挿入されたＳＤカード５２からＭＦＰアプリの読み出しが可能となる。ＭＦＰ５３は、ＳＤカード５２に記録されたＭＦＰアプリをインストールすることで、認証手段およびセキュリティポリシーを追加することができる。

【００２６】

また、ＰＣ５１は作成した１つ以上のＭＦＰアプリをＭＦＰアプリ配布サーバ５４に記録するようにしてもよい。ＭＦＰアプリ配布サーバ５４は、データ通信可能な外部装置の一例である。ＭＦＰ５６は、ＭＦＰアプリのインストールをＭＦＰアプリ配布サーバ５４に申請し、ＭＦＰアプリ配布サーバ５４からＭＦＰアプリをダウンロードすることで、認証手段およびセキュリティポリシーを追加することができる。

【００２７】

図６は、メディアに記録された認証手段（認証アプリ）をインストールする処理を表した一例のシーケンス図である。なお、メディアに記録されたセキュリティーポリシーをインストールする処理も図６のシーケンス図と同様である。

【００２８】

ステップＳ１に進み、利用者であるユーザがメディアを所定のスロットに挿入する。ステップＳ２に進み、ＭＦＰのＷＳＳＣマネージャはメディア内のファイル（認証手段）のチェックを行なう。

【００２９】

ステップＳ３に進み、ＷＳＳＣマネージャはメディア内のファイル（認証手段）を検出

する。ステップＳ４に進み、コントロールサービスに含まれるＯＣＳはステップＳ３で検出したメディア内のファイル（認証手段）をオペレーションパネルの画面に表示する。

【００３０】

ステップＳ５に進み、ユーザはオペレーションパネルの画面に表示されたファイル（認証手段）の中からインストールを所望するファイル（認証手段）を選択する。ステップＳ６に進み、ＯＣＳはオペレーションパネルの画面上で選択されたファイル（認証手段）を判定する。ステップＳ７に進み、ＷＳＳＣマネージャはオペレーションパネルの画面上で選択されたファイル（認証手段）をＯＣＳから通知される。

【００３１】

ステップＳ８に進み、ＷＳＳＣマネージャはオペレーションパネルの画面上で選択されたファイル（認証手段）をメディアからダウンロードする。ステップＳ９に進み、ＷＳＳＣマネージャは、ダウンロードしたファイル（認証手段）を認証変動部４にインストールする。ＷＳＳＣマネージャはオペレーションパネルの画面にインストール完了表示を行ったあと、処理を終了する。

【００３２】

図７は、メディア又はＰＣを指定して認証手段をインストールする時、オペレーションパネルに表示される画面の遷移図である。まず、ユーザは画面７１に利用者ＩＤを入力してＯＫボタンを押下する。続いて、ユーザは画面７２にパスワードを入力してＯＫボタンを押下する。

【００３３】

画面７１及び画面７２に入力された利用者ＩＤ及びパスワードによる認証が正常に終了すると、オペレーションパネルには画面７３が表示される。ユーザが画面７３においてメンテナンスモードを選択すると、オペレーションパネルには画面７４が表示される。画面７４では、新規に認証手段を追加する為の新規認証追加設定が選択できる。

【００３４】

画面７４で新規認証追加設定が選択されると、オペレーションパネルには画面７５が表示される。画面７５では、認証手段のダウンロード元となるメディア又はＰＣを選択することができる。画面７５は、ＳＤカードが選択された例を表している。ＳＤカードが選択されると、オペレーションパネルには画面７６が表示される。

【００３５】

画面７６では、ＳＤカードに記録されている１つ以上の認証手段が表示される。画面７６では、インストールする認証手段を選択できる。画面７６で認証手段が選択されてインストールボタンが押下されると、前述したように認証手段が認証変動部４にインストールされる。認証手段のインストールが完了すると、オペレーションパネルにはインストール完了表示である画面７７が表示される。なお、メディア又はＰＣを指定してセキュリティポリシーをインストールする時、オペレーションパネルに表示される画面は、図７と同様に遷移する。

【００３６】

図８は、セキュリティポリシーを追加する前後のセキュリティポリシーのヘッダファイルの変化を表した模式図である。セキュリティポリシーを追加する前のセキュリティポリシーのヘッダファイル８１は、セキュリティポリシーＩＳＭＳ　ＨＩＧＨ，ＩＳＭＳ　ＬＯＷ，ＤＥＦＡＵＬＴの構造体から成る。

【００３７】

その後、セキュリティポリシーＩＳＭＳ　ＭＩＤを複合機に追加すると、セキュリティポリシーのヘッダファイル８２にはセキュリティポリシーＩＳＭＳ　ＭＩＤの構造体が追加される。

【００３８】

図９は、セキュリティポリシーを追加する前後で、オペレーションパネルに表示される画面の変化を表した遷移図である。画面９１は、セキュリティポリシーＩＳＭＳ　ＭＩＤを複合機に追加する前の画面イメージであり、セキュリティポリシーのヘッダファイル８

１に基づいてオペレーションパネルに表示される。

【００３９】

また、画面９２は、セキュリティポリシーＩＳＭＳ　ＭＩＤを複合機に追加した後の画面イメージであり、セキュリティポリシーのヘッダファイル８２に基づいてオペレーションパネルに表示される。

【００４０】

複合機１に搭載されているセキュリティポリシーは、画面９１又は画面９２に示すようにオペレーションパネルから選択可能である。複合機１の起動時、複合機１はユーザにより選択されたセキュリティポリシーに対応するポリシークラスを生成し、ユーザの希望するセキュリティポリシーを用いて認証が行われる。

【００４１】

図１０は、複合機のＷＳＳＣを表した一例のクラス図である。ＷＳＳＣは、図１０に表した内部構造のクラスと、クラス間の関係とで表される。ＷＳＳＣは、サービスクラス１０１，サービス利用可能者リストクラス１０２，利用権クラス１０３，利用者クラス１０４，照合データクラス１０５，ポリシーリストクラス１０６，ポリシークラス１０７，認証手段クラス１０８，利用ポリシークラス１０９，利用認証手段クラス１１０，登録データクラス１１１，登録場所クラス１１２で構成される。

【００４２】

なお、サービスクラス１０１，サービス利用可能者リストクラス１０２，利用権クラス１０３，利用者クラス１０４，照合データクラス１０５，ポリシーリストクラス１０６，登録データクラス１１１，登録場所クラス１１２は、フレームワーク２を構成する。ポリシークラス１０７，認証手段クラス１０８，利用ポリシークラス１０９，利用認証手段クラス１１０は、変動部３を構成する。

【００４３】

外部の権限サーバは権限リスト６を格納している。サービス利用可能者リストクラス１０２は権限サーバの権限リスト６を利用してサービス利用権限審査を行なう。外部の認証サーバは認証リスト７を格納している。登録場所クラス１１２は認証サーバの認証リスト７を利用して認証手段検索を行なう。なお、照合データクラス１０５はユーザの入力したパスワード等の入力データを表す。登録データクラス１１１は、認証リスト７から読み出したパスワード等の登録データを表す。

【００４４】

以下、図１０の各クラスについて、パスワード認証時とＩＣカード認証時とに分けて説明していく。まず、パスワード認証時について説明する。

【００４５】

図１１は、認証手段およびセキュリティポリシー検索処理の手順を表す一例のシーケンス図である。ステップＳ２１では、オペレーションパネルの表示装置にログイン画面が表示される。ステップＳ２２では、ユーザがログイン画面に利用者ＩＤ（以下、単にＩＤと言う）を入力することで、利用者クラス１０４に認証手段検索依頼を行なう。

【００４６】

ステップＳ２３に進み、利用者クラス１０４は登録場所クラス１１２に認証手段検索依頼を行なう。登録場所クラス１１２は認証サーバの認証リスト７を利用して認証手段検索を行い、ＩＤに関連付けられている認証手段を検索する。ステップＳ２４に進み、登録場所クラス１１２は検索された認証手段の認証手段クラス１０８を生成する。さらに、ステップＳ２５に進み、登録場所クラス１１２はＩＤに関連付けられている登録データを認証リスト７から検索し、検索された登録データの登録データクラス１１１を生成する。ステップＳ２６に進み、登録場所クラス１１２はＩＤに関連付けられている認証手段を利用者クラス１０４に通知する。

【００４７】

さらに、ステップＳ２７に進み、利用者クラス１０４はポリシーリストクラス１０６にポリシー検索依頼を行なう。ステップＳ２８に進み、ポリシーリストクラス１０６はポリ

シークラス１０７にポリシー検索を依頼する。ポリシークラス１０７は、利用ポリシークラス１０９を参照し、ＩＤに関連付けられているセキュリティポリシーを検索する。ステップＳ２９に進み、ポリシーリストクラス１０６はＩＤに関連付けられているセキュリティポリシーを利用者クラス１０４に通知する。

【００４８】

図１２は、認証およびサービス利用権限チェック処理の手順を表す一例のシーケンス図である。ステップＳ３１では、オペレーションパネルの表示装置にパスワード入力画面が表示される。ステップＳ３２では、ユーザがパスワード入力画面にパスワードを入力することで、利用者クラス１０４に認証依頼を行なう。

【００４９】

ステップＳ３３に進み、利用者クラス１０４は認証手段クラス１０８に照合データ入力依頼を行なう。ステップＳ３４に進み、認証手段クラス１０８は、ユーザにより入力されたパスワードに応じた照合データクラス１０５を生成する。ステップＳ３５に進み、認証手段クラス１０８は、ポリシークラス１０７にセキュリティポリシーの参照を依頼してセキュリティポリシーを参照する。認証手段クラス１０８は、セキュリティポリシーに対応したセキュリティレベルの認証方法を確認する。

【００５０】

ステップＳ３６に進み、認証手段クラス１０８は、照合データクラス１０５および登録データクラス１１１を利用して照合データと登録データとが一致するか確認する。ステップＳ３７に進み、認証手段クラス１０８は利用者クラス１０４に認証結果を通知する。

【００５１】

ステップＳ３８に進み、利用者クラス１０４は利用権クラス１０３に権限チェック依頼を行なう。ステップＳ３９に進み、利用権クラス１０３はサービス利用可能者リストクラス１０２にサービス利用権限審査依頼を行なう。サービス利用可能者リストクラス１０２は権限サーバの権限リスト６を利用して利用権限チェックを行い、ＩＤに関連付けられている利用可能サービスを検索する。ステップＳ４０に進み、サービス利用可能者リストクラス１０２は検索された利用可能サービスのサービスクラス１０１を生成する。

【００５２】

ステップＳ４１に進み、サービス利用可能者リストクラス１０２は生成したサービスクラス１０１に応じて利用権の発行依頼を利用権クラス１０３に行なう。ステップＳ４２に進み、利用権クラス１０３は利用権を発行したサービスを通知する為の利用権取得結果通知を利用者クラス１０４に対して行なう。そして、ステップＳ４３に進み、利用者クラス１０４はオペレーションパネルの表示装置に認証結果画面を表示する。

【００５３】

図１３は、パスワード認証時にオペレーションパネルに表示される一部画面の遷移図である。画面１３０１はログイン画面の一例である。画面１３０２はパスワード入力画面の一例である。画面１３０３は認証が異常終了したときの認証結果画面の一例である。画面１３０４は認証が正常終了したときの認証結果画面の一例である。認証が正常終了したときの認証結果画面には、利用可能なサービスが表示される。

【００５４】

次に、ＩＣカード認証時について説明する。図１４は認証手段およびセキュリティポリシー検索処理の手順を表す一例のシーケンス図である。ステップＳ５１では、オペレーションパネルの表示装置にログイン画面が表示される。ステップＳ５２では、ユーザがＩＣカードリーダにＩＣカードを通す。なお、ここで言うＩＣカードをＩＣカードリーダに通すとは、ＩＣカードからデータの読み出しが可能な状態にする行為の一例であって、他の行為であってもよい。ステップＳ５３では、ＩＣカードリーダがＩＣカードからＩＤを読み出し、利用者クラス１０４に認証手段検索依頼を行なう。

【００５５】

ステップＳ５４に進み、利用者クラス１０４は登録場所クラス１１２に認証手段検索依頼を行なう。登録場所クラス１１２は認証サーバの認証リスト７を利用して認証手段検索

を行い、ＩＤに関連付けられている認証手段を検索する。ステップＳ５５に進み、登録場所クラス１１２は検索された認証手段の認証手段クラス１０８を生成する。さらに、ステップＳ５６に進み、登録場所クラス１１２はＩＤに関連付けられている登録データを認証リスト７から検索し、検索された登録データの登録データクラス１１１を生成する。ステップＳ５７に進み、登録場所クラス１１２はＩＤに関連付けられている認証手段を利用者クラス１０４に通知する。

【００５６】

さらに、ステップＳ５８に進み、利用者クラス１０４はポリシーリストクラス１０６にポリシー検索依頼を行なう。ステップＳ５９に進み、ポリシーリストクラス１０６はポリシークラス１０７にポリシー検索を依頼する。ポリシークラス１０７は、利用ポリシークラス１０９を参照し、ＩＤに関連付けられているセキュリティポリシーを検索する。ステップＳ６０に進み、ポリシーリストクラス１０６はＩＤに関連付けられているセキュリティポリシーを利用者クラス１０４に通知する。

【００５７】

図１５は、認証およびサービス利用権限チェック処理の手順を表す一例のシーケンス図である。ステップＳ６１では、オペレーションパネルの表示装置上に、ＩＣカードをＩＣカードリーダに通す旨のメッセージを含むパスワード入力画面が表示される。ステップＳ６２では、ユーザがＩＣカードをＩＣカードリーダに通すことで、利用者クラス１０４に認証依頼を行なう。

【００５８】

ステップＳ６２に進み、利用者クラス１０４は認証手段クラス１０８に照合データ入力依頼を行なう。ステップＳ６３に進み、認証手段クラス１０８は、ＩＣカードから読み出したパスワードに応じて照合データクラス１０５を生成する。ステップＳ６４に進み、認証手段クラス１０８は、ポリシークラス１０７にセキュリティポリシーの参照を依頼してセキュリティポリシーを参照する。認証手段クラス１０８は、セキュリティポリシーに対応したセキュリティレベルの認証方法を確認する。

【００５９】

ステップＳ６５に進み、認証手段クラス１０８は、照合データクラス１０５および登録データクラス１１１を利用して照合データと登録データとが一致するか確認する。ステップＳ６６に進み、認証手段クラス１０８は利用者クラス１０４に認証結果を通知する。

【００６０】

ステップＳ６７に進み、利用者クラス１０４は利用権クラス１０３に権限チェック依頼を行なう。ステップＳ６８に進み、利用権クラス１０３はサービス利用可能者リストクラス１０２にサービス利用権限審査依頼を行なう。サービス利用可能者リストクラス１０２は権限サーバの権限リスト６を利用して利用権限チェックを行い、ＩＤに関連付けられている利用可能サービスを検索する。ステップＳ６９に進み、サービス利用可能者リストクラス１０２は検索された利用可能サービスのサービスクラス１０１を生成する。

【００６１】

ステップＳ７０に進み、サービス利用可能者リストクラス１０２は生成したサービスクラス１０１に応じて利用権の発行依頼を利用権クラス１０３に行なう。ステップＳ７１に進み、利用権クラス１０３は利用権を発行したサービスを通知する為の利用権取得結果通知を利用者クラス１０４に対して行なう。そして、ステップＳ７２に進み、利用者クラス１０４はオペレーションパネルの表示装置に認証結果画面を表示する。

【００６２】

図１６は、ＩＣカード認証時にオペレーションパネルに表示される一部画面の遷移図である。画面１６０１はログイン画面の一例である。画面１６０２はパスワード入力画面の一例である。画面１６０３はＩＣカードからＩＤやパスワードを読み出しているときの画面の一例である。また、画面１６０４は認証が正常終了したときの認証結果画面の一例であって、利用可能なサービスが表示される。

【００６３】

図１７及び図１８は、複合機のＷＳＳＣを表した一例のオブジェクト図である。図１７は、認証手段Ｃが追加される前のオブジェクト図である。また、図１８は認証手段Ｃが追加された後のオブジェクト図である。

【００６４】

本発明は、具体的に開示された実施例に限定されるものではなく、特許請求の範囲から逸脱することなく、種々の変形や変更が可能である。

【図面の簡単な説明】

【００６５】

【図１】本発明の原理図を説明する為の模式図である。

【図２】本発明による複合機の一実施例の構成図を示す。

【図３】セキュリティポリシーの設定処理を表すイメージ図である。

【図４】セキュリティポリシーの設定処理を表す他の例のイメージ図である。

【図５】ＭＦＰアプリの作成及びインストールを表すイメージ図である。

【図６】メディアに記録された認証手段（認証アプリ）をインストールする処理を表した一例のシーケンス図である。

【図７】メディア又はＰＣを指定して認証手段をインストールする時、オペレーションパネルに表示される画面の遷移図である。

【図８】セキュリティポリシーを追加する前後のセキュリティポリシーのヘッダファイルの変化を表した模式図である。

【図９】セキュリティポリシーを追加する前後で、オペレーションパネルに表示される画面の変化を表した遷移図である。

【図１０】複合機のＷＳＳＣを表した一例のクラス図である。

【図１１】認証手段およびセキュリティポリシー検索処理の手順を表す一例のシーケンス図である。

【図１２】認証およびサービス利用権限チェック処理の手順を表す一例のシーケンス図である。

【図１３】パスワード認証時にオペレーションパネルに表示される一部画面の遷移図である。

【図１４】認証手段およびセキュリティポリシー検索処理の手順を表す一例のシーケンス図である。

【図１５】認証およびサービス利用権限チェック処理の手順を表す一例のシーケンス図である。

【図１６】ＩＣカード認証時にオペレーションパネルに表示される一部画面の遷移図である。

【図１７】複合機のＷＳＳＣを表した一例のオブジェクト図である。

【図１８】複合機のＷＳＳＣを表した一例のオブジェクト図である。

【符号の説明】

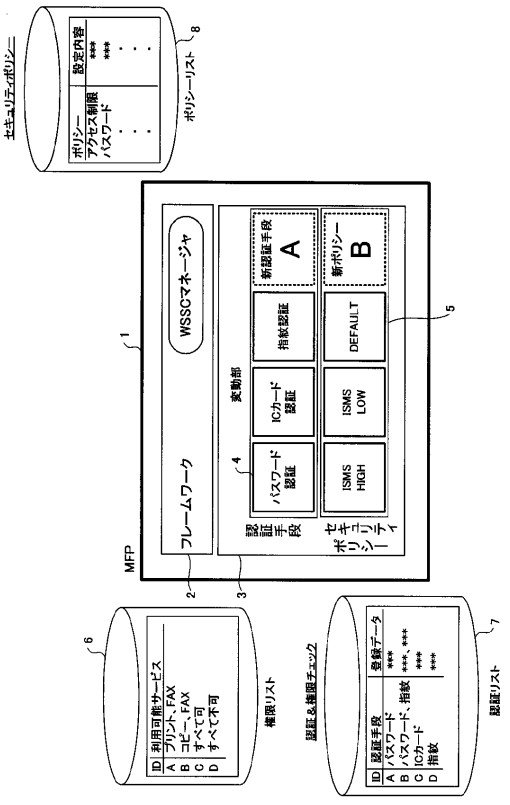
【００６６】

１　複合機（ＭＦＰ）
２　フレームワーク
３　変動部
４　認証変動部
５　ポリシー変動部
６　権限リスト
７　認証リスト
８　ポリシーリスト
１０　ハードウェア資源
１１　ソフトウェア群
２１　プロッタ
２２　スキャナ

２３　ＩＣカードリーダ
２４　ＳＤカードリーダ
２５　ＯＳ
２６　コントロールサービス
２７　コピーアプリ
２８　ファックスアプリ
２９　スキャナアプリ
３０　Ｗｅｂサービスサーバコンポーネント（ＷＳＳＣ）
３１　ＷＳＳＣマネージャ

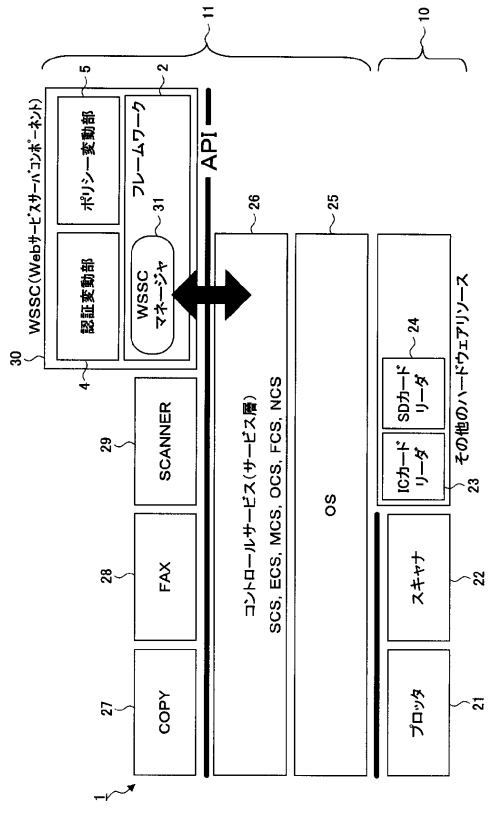
【図１】

本発明の原理図を説明する為の模式図



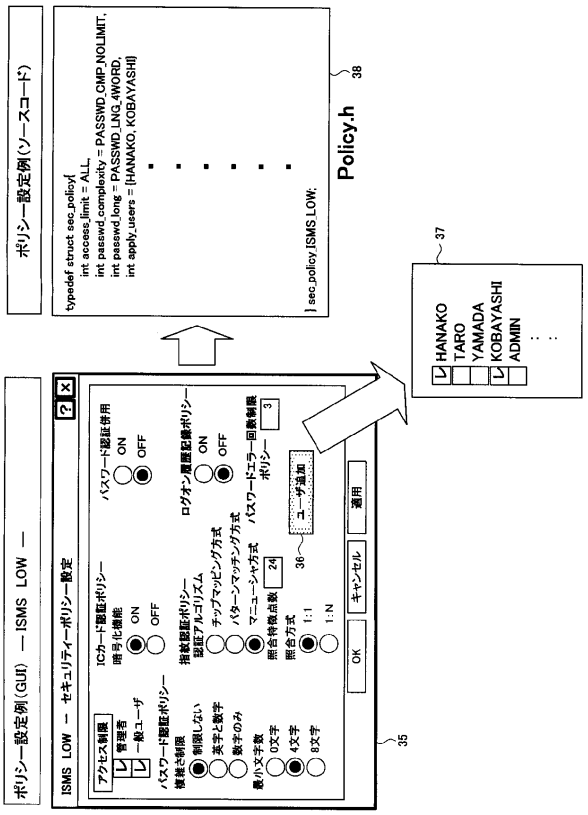
【図２】

本発明による複合機の一実施例の構成図



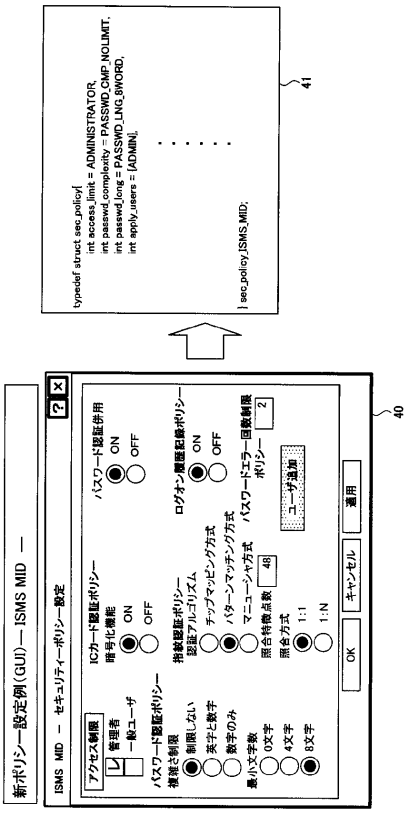
【図３】

セキュリティポリシーの設定処理を表すイメージ図



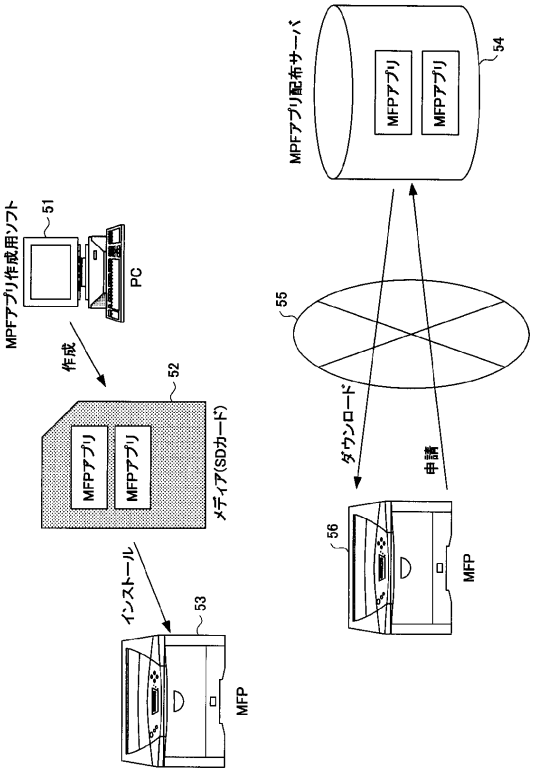
【図４】

セキュリティポリシーの設定処理を表す他の例のイメージ図



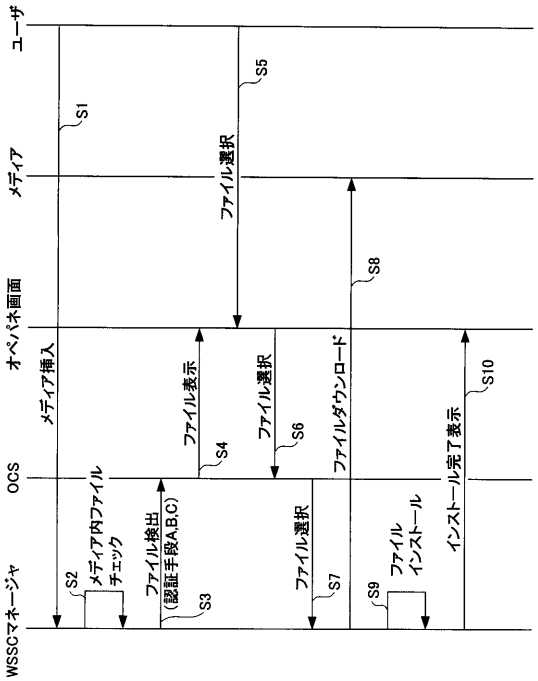
【図５】

MFPアプリの作成及びインストールを表すイメージ図



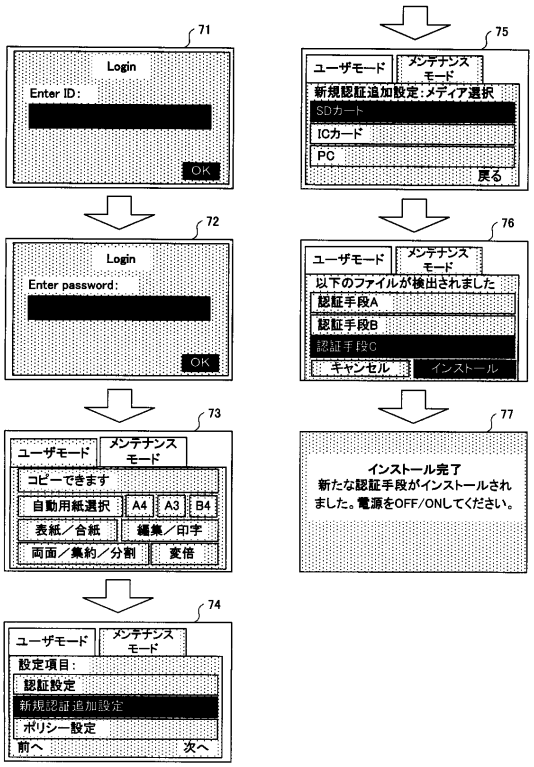
【図６】

メディアに記録された認証手段(認証アプリ)を
インストールする処理を表した一例のシーケンス図



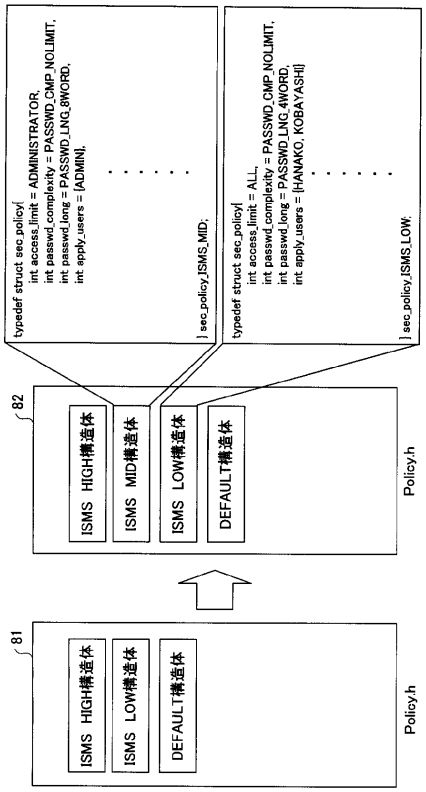
【図７】

メディア又はPCを指定して認証手段をインストールする時、
オペレーションパネルに表示される画面の遷移図



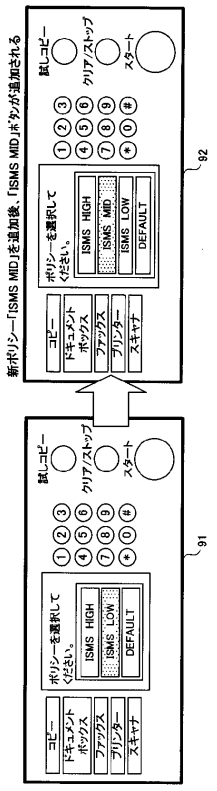
【図８】

セキュリティポリシーを追加する前後の
セキュリティポリシーのヘッダファイルの変化を表した模式図



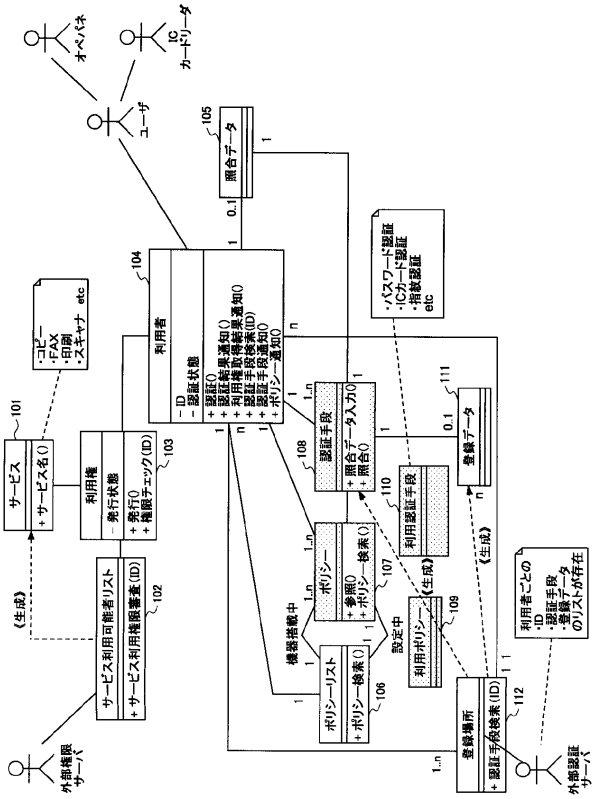
【図９】

セキュリティポリシーを追加する前後で、
オペレーションパネルに表示される画面の変化を表した遷移図



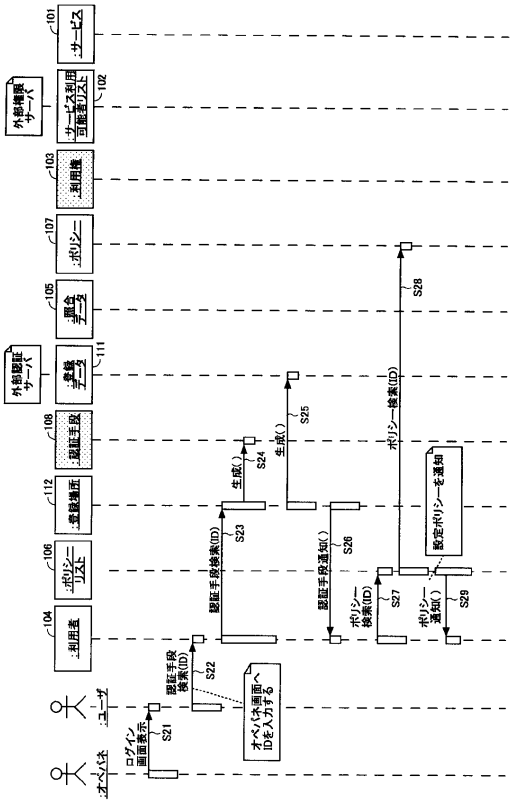
【図１０】

複合機のWSSC2を表した一例のクラス図



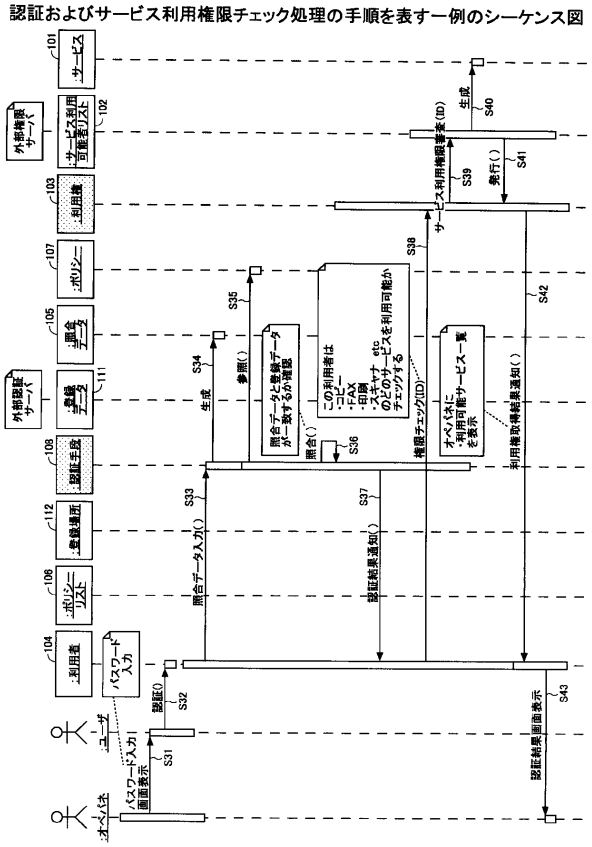
【図１１】

認証手段およびセキュリティポリシー検索処理の手順を表す一例のシーケンス図



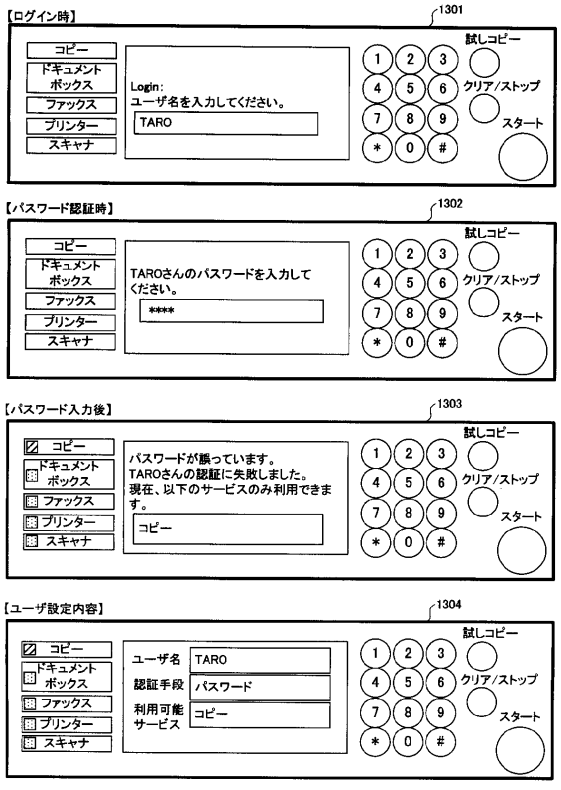
【図１２】

認証およびサービス利用権限チェック処理の手順を表す一例のシーケンス図



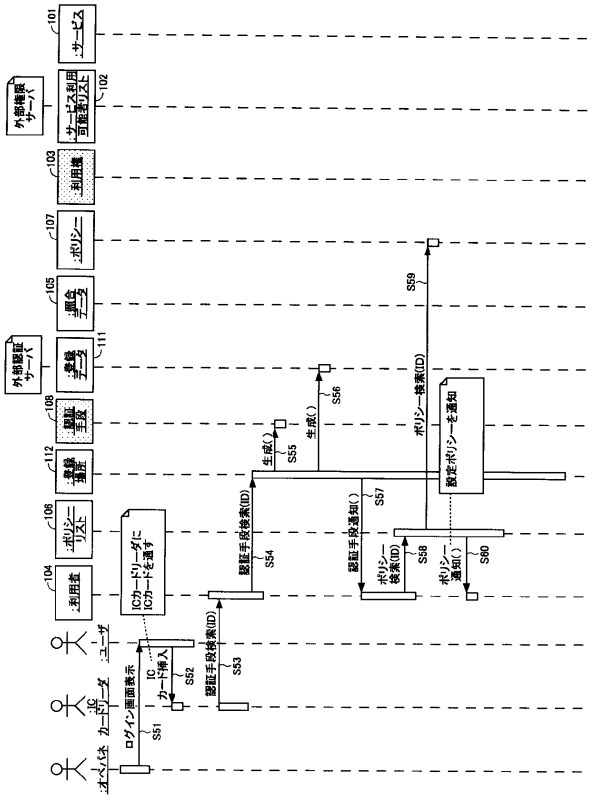
【図１３】

パスワード認証時にオペレーションパネルに表示される一部画面の遷移図



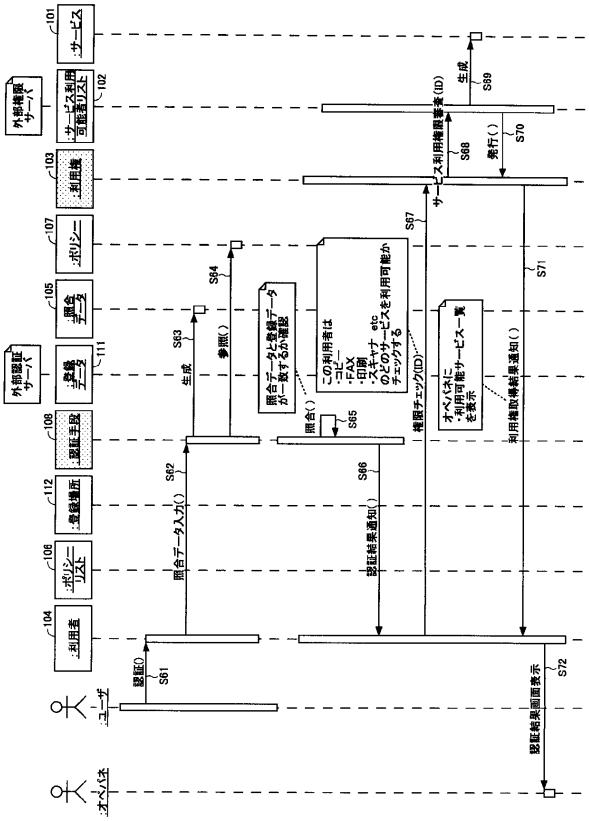
【図１４】

認証手段およびセキュリティポリシー検索処理の手順を表す一例のシーケンス図



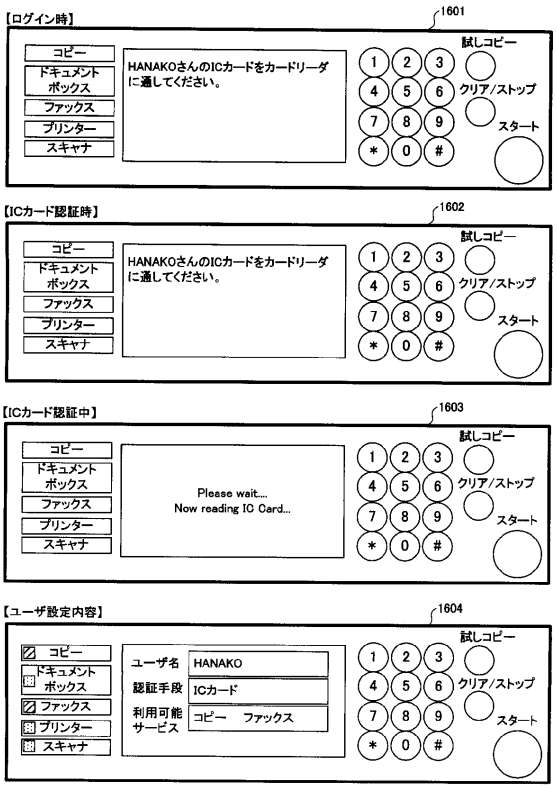
【図１５】

認証およびサービス利用権限チェック処理の手順を表す一例のシーケンス図



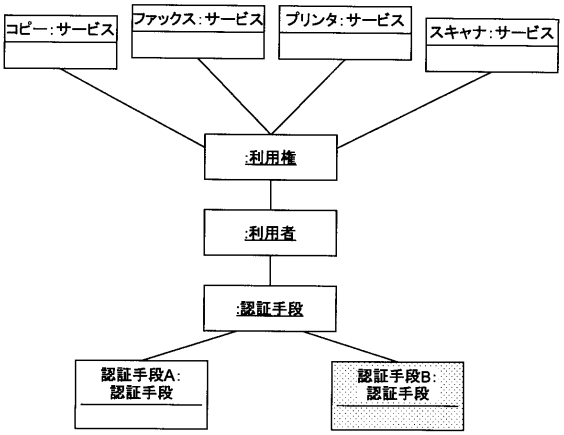
【図１６】

ICカード認証時にオペレーションパネルに表示される一部画面の遷移図



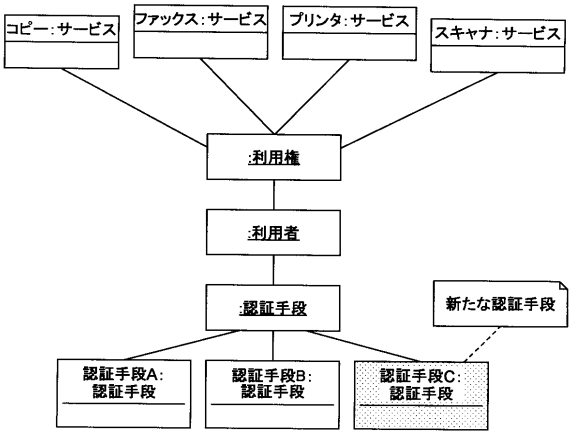
【図１７】

複合機のWSSC2を表した一例のオブジェクト図



【図１８】

複合機のWSSC2を表した一例のオブジェクト図



フロントページの続き

(51)Int.Cl.	FI		テーマコード（参考）
	Ｈ０４Ｎ	1/00	Ｃ