(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6066751号
(P6066751)
(45)発行日　平成29年1月25日(2017.1.25)　(24)登録日　平成29年1月6日(2017.1.6)

(51)Int.Cl.　F I
G06F 21/60 (2013.01)　G06F 21/60

請求項の数 14　(全 35 頁)

(21)出願番号　特願2013-16866(P2013-16866)
(22)出願日　平成25年1月31日(2013.1.31)
(65)公開番号　特開2014-149595(P2014-149595A)
(43)公開日　平成26年8月21日(2014.8.21)
審査請求日　平成28年2月1日(2016.2.1)

(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　100125254
弁理士　別役　重尚
(72)発明者　土樋　直基
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
(72)発明者　安川　朱里
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
(72)発明者　清水　将太
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

最終頁に続く

(54)【発明の名称】情報処理システム及びその制御方法、並びにプログラム

(57)【特許請求の範囲】
【請求項１】
画像処理装置と情報処理装置とがネットワークを介して接続された情報処理システムにおいて、
前記情報処理装置は、
情報セキュリティポリシーが記述されたセキュリティポリシーデータを生成する生成手段と、
前記生成されたセキュリティポリシーデータを送信する送信手段とを備え、
前記画像処理装置は、
前記セキュリティポリシーデータを受信する受信手段と、
前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理手段と、
前記管理手段で管理された拡張アプリケーションが前記セキュリティポリシーデータに記述された情報セキュリティポリシーを遵守することができないアプリケーションである場合で、かつ当該セキュリティポリシーデータから抽出された、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子と、前記管理手段で管理されている拡張アプリケーションの識別子とが一致しない場合は、当該拡張アプリケーションに対して前記情報セキュリティポリシーの再設定が必要であることを管理者に通知する変更通知手段とを備えることを特徴とする情報処理システム。
【請求項２】

画像処理装置と情報処理装置とがネットワークを介して接続された情報処理システムにおいて、
前記情報処理装置は、
情報セキュリティポリシーが記述されたセキュリティポリシーデータを生成する生成手段と、
前記生成されたセキュリティポリシーデータを送信する送信手段とを備え、
前記画像処理装置は、
前記セキュリティポリシーデータを受信する受信手段と、
前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理手段と、
前記受信手段で受信したセキュリティポリシーデータから、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子を抽出し、前記管理手段で管理されている拡張アプリケーションの識別子と比較して一致するものがなかった場合は、当該拡張アプリケーションの動作を停止させる変更通知手段とを備えることを特徴とする情報処理システム。
【請求項３】
前記管理手段で管理されている拡張アプリケーションの情報セキュリティポリシーにポリシーバージョンが設定されているか否かを判定する判定手段をさらに備え、
前記変更通知手段は、前記判定手段により前記ポリシーバージョンが設定されていると判定された場合に前記動作を実行することを特徴とする請求項１または２に記載の情報処理システム。
【請求項４】
前記変更通知手段は、
前記管理手段で管理されている拡張アプリケーションの情報セキュリティポリシーのバージョンと前記画像処理装置の情報セキュリティポリシーのバージョンとが異なる場合には、前記拡張アプリケーションの情報セキュリティポリシーと前記画像処理装置の情報セキュリティポリシーの差分となる項目を表示手段に表示させることを特徴とする請求項１乃至３のいずれか１項に記載の情報処理システム。
【請求項５】
画像処理装置と情報処理装置とがネットワークを介して接続された情報処理システムの制御方法において、
前記情報処理装置の生成手段が、情報セキュリティポリシーが記述されたセキュリティポリシーデータを生成する生成工程と、
前記情報処理装置の送信手段が、前記生成されたセキュリティポリシーデータを送信する送信工程と、
前記画像処理装置の受信手段が、前記セキュリティポリシーデータを受信する受信工程と、
前記画像処理装置の管理手段が、前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理工程と、
前記画像処理装置の変更通知手段が、前記管理工程で管理された拡張アプリケーションが前記セキュリティポリシーデータに記述された情報セキュリティポリシーを遵守することができないアプリケーションである場合で、かつ当該セキュリティポリシーデータから抽出された、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子と、前記管理工程で管理されている拡張アプリケーションの識別子とが一致しない場合は、当該拡張アプリケーションに対して前記情報セキュリティポリシーの再設定が必要であることを管理者に通知する変更通知工程とを備えることを特徴とする制御方法。
【請求項６】
画像処理装置と情報処理装置とがネットワークを介して接続された情報処理システムの制御方法において、
前記情報処理装置の生成手段が、情報セキュリティポリシーが記述されたセキュリティ

ポリシーデータを生成する生成工程と、
前記情報処理装置の送信手段が、前記生成されたセキュリティポリシーデータを送信する送信工程と、
前記画像処理装置の受信手段が、前記セキュリティポリシーデータを受信する受信工程と、
前記画像処理装置の管理手段が、前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理工程と、
前記画像処理装置の変更通知手段が、前記受信工程で受信したセキュリティポリシーデータから、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子を抽出し、前記管理工程で管理されている拡張アプリケーションの識別子と比較して一致するものがなかった場合は、当該拡張アプリケーションの動作を停止させる変更通知工程とを備えることを特徴とする制御方法。
【請求項７】
請求項５または６に記載の制御方法を情報処理装置及び／又は画像処理装置に実行させるためのコンピュータに読み取り可能なプログラム。
【請求項８】
ネットワークに接続された画像処理装置において、
情報セキュリティポリシーが記述されたセキュリティポリシーデータを受信する受信手段と、
前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理手段と、
前記管理手段で管理された拡張アプリケーションが前記セキュリティポリシーデータに記述された情報セキュリティポリシーを遵守することができないアプリケーションである場合で、かつ当該セキュリティポリシーデータから抽出された、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子と、前記管理手段で管理されている拡張アプリケーションの識別子とが一致しない場合は、当該拡張アプリケーションに対して前記情報セキュリティポリシーの再設定が必要であることを管理者に通知する変更通知手段とを備えることを特徴とする画像処理装置。
【請求項９】
ネットワークに接続された画像処理装置において、
情報セキュリティポリシーが記述されたセキュリティポリシーデータを受信する受信手段と、
前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理手段と、
前記受信手段で受信したセキュリティポリシーデータから、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子を抽出し、前記管理手段で管理されている拡張アプリケーションの識別子と比較して一致するものがなかった場合は、当該拡張アプリケーションの動作を停止させる変更通知手段とを備えることを特徴とする画像処理装置。
【請求項１０】
前記管理手段で管理されている拡張アプリケーションの情報セキュリティポリシーにポリシーバージョンが設定されているか否かを判定する判定手段をさらに備え、
前記変更通知手段は、前記判定手段により前記ポリシーバージョンが設定されていると判定された場合に前記動作を実行することを特徴とする請求項８または９に記載の画像処理装置。
【請求項１１】
前記変更通知手段は、
前記管理手段で管理されている拡張アプリケーションの情報セキュリティポリシーのバージョンと前記画像処理装置の情報セキュリティポリシーのバージョンとが異なる場合には、前記拡張アプリケーションの情報セキュリティポリシーと前記画像処理装置の情報セ

キュリティポリシーの差分となる項目を表示手段に表示させることを特徴とする請求項８乃至１０のいずれか１項に記載の画像処理装置。

【請求項１２】

ネットワークに接続された画像処理装置の制御方法において、

前記画像処理装置の受信手段が、情報セキュリティポリシーが記述されたセキュリティポリシーデータを受信する受信工程と、

前記画像処理装置の管理手段が、前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理工程と、

前記画像処理装置の変更通知手段が、前記管理工程で管理された拡張アプリケーションが前記セキュリティポリシーデータに記述された情報セキュリティポリシーを遵守することができないアプリケーションである場合で、かつ当該セキュリティポリシーデータから抽出された、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子と、前記管理工程で管理されている拡張アプリケーションの識別子とが一致しない場合は、当該拡張アプリケーションに対して前記情報セキュリティポリシーの再設定が必要であることを管理者に通知する変更通知工程とを備えることを特徴とする制御方法。

【請求項１３】

ネットワークに接続された画像処理装置の制御方法において、

前記画像処理装置の受信手段が、情報セキュリティポリシーが記述されたセキュリティポリシーデータを受信する受信工程と、

前記画像処理装置の管理手段が、前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理工程と、

前記画像処理装置の変更通知手段が、前記受信工程で受信したセキュリティポリシーデータから、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子を抽出し、前記管理工程で管理されている拡張アプリケーションの識別子と比較して一致するものがなかった場合は、当該拡張アプリケーションの動作を停止させる変更通知工程とを備えることを特徴とする制御方法。

【請求項１４】

請求項１２または１３に記載の制御方法を画像処理装置に実行させるためのコンピュータに読み取り可能なプログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、情報処理システム及びその制御方法、並びにプログラムに関し、特に、ネットワーク環境における機器間の情報セキュリティポリシー技術に関する。

【背景技術】

【０００２】

オフィス等のネットワークに接続するパーソナルコンピュータ（ＰＣ）やサーバ機器（ファイルサーバや認証サーバ等）は、オフィス毎に決められた情報セキュリティポリシーに従って運用されることが望ましい。情報セキュリティポリシーとは、企業全体の情報セキュリティに関する基本方針であり、情報の利用や外部からの侵入、情報漏えいを防止するための方針をまとめたものである。

【０００３】

オフィスのネットワークに接続する機器としては、ＰＣやサーバ機器以外に、複合機やプリンタといった周辺装置がある。近年の複合機においては、単純に画像を印刷や送信するだけではなく、画像データを記憶し、ＰＣに対してファイルサービス機能を提供し、ネットワーク上に存在するその他のサーバ機器と同様の役割を果たすようになってきている。

【０００４】

安全・安心なオフィス環境を維持するためには、ＰＣやサーバ機器と同様に、複合機においても、情報セキュリティポリシーに従うことが求められることになる。ここでいう情

報セキュリティポリシーに従うとは、複合機を操作する際にユーザー認証を必須とすることや通信経路の暗号化を必須とするなど、オフィス内の複合機の不正使用や情報漏えいを防ぐためにセキュリティ上の運用に制約を設けることを示している。

【０００５】

情報セキュリティポリシーに従わせるために、ＰＣやサーバ機器においてはＯＳに依存する設定値を配信する方法が取られている。例えば、通信経路の暗号化に関するＯＳに依存する設定値としては、「非ＳＳＬ接続を許可する」などがあり、どのベンダーのＰＣであっても統一的に情報セキュリティポリシーに従うよう管理されている。

【０００６】

一方で複合機はベンダーによって設定可能な項目が異なるので、管理者は複合機毎に数多くの動作設定（以下、「ユーザーモード」と呼ぶ）を熟知した上で、１台ずつ情報セキュリティポリシーに従った状態にする必要がある。例えば、通信経路の暗号化を行うユーザーモードの設定値が、Ａ社の複合機は「ＳＳＬを使用する」であったり、Ｂ社の複合機は「ＨＴＴＰ通信を暗号化する」であったりする。そのため、ＰＣやサーバ機器のように設定値を配信することで、統一的に情報セキュリティポリシーに従わせる方法を取ることができず、管理者に多大な労力がかかる。また、正しい設定がなされないと、情報セキュリティポリシーに従わない運用を事実上許容することになり、オフィスのセキュリティを脅かす可能性がある。

【０００７】

昨今の複合機の一部のモデルでは、開発環境とＡＰＩ（アプリケーション・プログラム・インターフェイス）が公開されている。これによって複合機を設計・生産するベンダー以外のいわゆるサードパーティベンダーでも、複合機の内部で動作する機能を拡張アプリケーションとして追加する仕組みを用意している。例えば、顧客毎にユーザー認証の仕組みが異なるような場合でも、顧客の要望に合致する拡張アプリケーションをサードパーティベンダーが作成することにより、顧客毎の細やかな要求にも受け応えることが可能となっている。このような拡張アプリケーションでもセキュリティに関する設定値を持っているものがあり、情報セキュリティポリシーに従った状態での動作が望まれている。

【０００８】

そこで、管理者が情報セキュリティポリシーに従った入力をすることで、複数の複合機のユーザーモードを生成、配信するシステムが提案されている（例えば特許文献１参照）。このシステムでは、管理者がＰＣに表示される設定画面上の質問に対して、情報セキュリティポリシーに従った回答を行う。回答を受けたＰＣは、回答に基づいて複合機に依存しない設定（以下、「セキュリティポリシーデータ」と呼ぶ）を生成し、生成したセキュリティポリシーデータから配信先の複合機に依存したユーザーモードに変換する。そして、ＰＣから各複合機にユーザーモードを配信することで、ユーザーモードが異なる複合機であっても、複合機に対する知識なしに情報セキュリティポリシーに従った状態にすることができる。

【０００９】

また、拡張アプリケーションに対するポリシーの反映については、パーソナルコンピュータのＯＳで情報セキュリティポリシー変更を通知する仕組みが提案されている（例えば、特許文献２参照）。これによれば、システムは情報セキュリティポリシーの受信時に、情報セキュリティポリシーを管理するモジュールが各セキュリティエンジン（例えばファイヤウォールやウィルス検知ソフト）に対して情報セキュリティポリシーを配信する。セキュリティエンジンは、情報セキュリティポリシーが配信された状態で、他のセキュリティエンジンに対してＡＰＩ（アプリケーション・プログラム・インターフェイス）を用いて情報収集を行う。各セキュリティエンジンは、他のセキュリティエンジンの設定状態に基づいて動作を決定していくものである。

【先行技術文献】

【特許文献】

【００１０】

【特許文献１】特開２００８－２１９４１９号公報
【特許文献２】特許第４６７６７４４号
【発明の概要】
【発明が解決しようとする課題】
【００１１】
上記従来技術に対して、情報セキュリティポリシーに従った状態を維持しつつ、ユーザーモードの変更を行えるシステムが望ましい場合がある。例えば、通信経路の暗号化を必須とする情報セキュリティポリシーにおいて、複合機が「ＳＳＬを使用する」、「ＩＰＳＥＣを使用する」に対応しており、そのいずれかを有効にすれば情報セキュリティポリシーに従った状態にできるものとする。
【００１２】
従来のシステムでは、「ＩＰＳＥＣを使用する」を有効にする設定値を配信すると、ユーザーは「ＳＳＬを使用する」を有効にしたいとしても、変更することができない。変更を行うためには、ユーザーが管理者に情報セキュリティポリシーに従ったユーザーモードの再配信を依頼する必要があり、利便性に欠けるという課題がある。
【００１３】
また、従来のシステムにおいては、拡張アプリケーションに情報セキュリティポリシーを配信した後に、システムに対する明示的な指示（例えばセッション断、当該ユーザーのログアウト、システムの再起動など）を行う仕組みを用意していない。そのため、配信後は常に再起動を行うといった手続きを強制されるようになっている。例えば、一般のＰＣの場合には、システムの再起動でもそのＰＣを利用しているユーザーだけが影響を受けていたが、複合機は複数のユーザーで共有して同時に複数のジョブを処理しているため、機器が利用できない時間（いわゆるダウンタイム）が発生する。このようなダウンタイムを最小化するためにも、再起動をできるだけ行いたくないという課題がある。
【００１４】
そこで、本発明は、上記課題に鑑み、外部から画像処理装置に導入された拡張アプリケーションに対しても情報セキュリティポリシーの管理が容易になる制御技術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】
【００１５】
上記目的を達成するために、本発明の情報処理システムは、画像処理装置と情報処理装置とがネットワークを介して接続された情報処理システムにおいて、前記情報処理装置は、情報セキュリティポリシーが記述されたセキュリティポリシーデータを生成する生成手段と、前記生成されたセキュリティポリシーデータを送信する送信手段とを備え、前記画像処理装置は、前記セキュリティポリシーデータを受信する受信手段と、前記画像処理装置で動作させるために追加または削除することが可能な拡張アプリケーションを管理する管理手段と、前記管理手段で管理された拡張アプリケーションが前記セキュリティポリシーデータに記述された情報セキュリティポリシーを遵守することができないアプリケーションである場合で、かつ当該セキュリティポリシーデータから抽出された、前記情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子と、前記管理手段で管理されている拡張アプリケーションの識別子とが一致しない場合は、当該拡張アプリケーションに対して前記情報セキュリティポリシーの再設定が必要であることを管理者に通知する変更通知手段とを備えることを特徴とする。
【発明の効果】
【００１６】
本発明によれば、外部から画像処理装置に導入された拡張アプリケーションに対しても情報セキュリティポリシーの管理が容易になる。
【図面の簡単な説明】
【００１７】
【図１】本発明の第１の実施形態に係る情報処理システムを構成する機器のハードウェア

構成の概略を示すブロック図である。
【図２】（ａ）図１の複合機における情報セキュリティポリシーの制御に関連する機能の概略構成を示すブロック図、（ｂ）図１のＰＣにおける情報セキュリティポリシーの制御に関連する機能の概略構成を示すブロック図である。
【図３】ＰＣの操作表示部に表示されるポリシー設定画面の一例を示す図である。
【図４】（ａ）ＰＣに記憶されたセキュリティポリシーデータの一例を示す図、（ｂ）複合機に記憶された変換ルールファイルの一例を示す図、（ｃ）複合機に記憶される中間情報の一例を示す図である。
【図５】複合機にて実行される情報セキュリティポリシー変換処理の流れを示すフローチャートである。
【図６】複合機にて実行される情報セキュリティポリシー適用処理の流れを示すフローチャートである。
【図７】（ａ）複合機のユーザーモード格納部に格納されるユーザーモードの名称と値の一例を示す図、（ｂ）複合機に記憶される画面制御情報の一例を示す図である。
【図８】（ａ）ＰＣが管理者に通知を行うための表示画面の一例を示す図、（ｂ）エラー画面の一例を示す図である。
【図９】複合機にて画面制御部により実行されるエラー画面表示処理の流れを示すフローチャートである。
【図１０】拡張アプリケーションの構成例を示す模式図である。
【図１１】複合機と拡張アプリケーション間で情報のやり取りや指示を行うＡＰＩを説明するための図である。
【図１２】拡張アプリケーション管理部の動作を説明するためのフローチャートである。
【図１３】拡張アプリケーション管理テーブルの一例を示す図である。
【図１４】ポリシー変更通知部の動作を説明するためのフローチャートである。
【図１５】（ａ）拡張アプリケーションにおける情報セキュリティポリシーと設定値との関係の一例を示す図、（ｂ）拡張アプリケーションの設定値の変更に対して再起動が必要かどうかを判定するためのテーブル情報の一例を示す図である。
【図１６】ポリシー強制処理部の動作を説明するためのフローチャートである。
【図１７】ＸＭＬ形式で表されたセキュリティポリシーデータの一例を示す図である。
【図１８】ＸＭＬ形式で表された変換ルールファイルの一例を示す図である。
【図１９】情報セキュリティポリシーを認識しない拡張アプリケーションの構成例を示す模式図である。
【図２０】第２の実施形態におけるポリシー変更通知部の動作を説明するためのフローチャートである。
【図２１】図２０の処理にてＵＩ操作部に表示される注意メッセージの一例を示す図である。
【図２２】（ａ）ポリシーバージョンがＶ１．００の場合の情報セキュリティポリシー項目の一覧を示す図、（ｂ）ポリシーバージョンがＶ１．０１の場合の情報セキュリティポリシー項目の一覧を示す図である。
【図２３】第３の実施形態におけるポリシー変更通知部の動作を説明するためのフローチャートである。
【図２４】図２３の処理にてＵＩ操作部に表示される注意メッセージの一例を示す図である。
【図２５】第４の実施形態におけるセキュリティポリシーデータの一例を示す図である。
【図２６】第４実施形態におけるポリシー変更通知部の動作を説明するためのフローチャートである。
【図２７】拡張アプリケーションの情報がＵＩ操作部１０３に表示されたＵＩ画面の一例を示す図である。
【図２８】第５の実施形態におけるＡＰＩの動作を説明するための図である。
【図２９】第５の実施形態における改良された情報セキュリティポリシー変更部の動作を

説明するためのフローチャートである。
【発明を実施するための形態】
【００１８】
以下、本発明の実施の形態を図面を参照して詳細に説明する。
【００１９】
［第１の実施形態］
図１は、本発明の第１の実施形態に係る情報処理システムを構成する機器のハードウェア構成の概略を示すブロック図である。
【００２０】
図１において、本発明の第１の実施形態に係る情報処理システムは、画像処理装置の一例である複合機１０１と、情報処理装置の一例であるパーソナルコンピュータ（ＰＣ）２０１と、これらを互いに接続するネットワーク１２６とを備える。なお、本発明の情報処理システムを構成する機器は、図示例に限定されるものではなく、図示の機器以外に複数の機器がネットワーク１２６に接続されていてもよい。また、画像処理装置が複合機以外の機器（例えば、プリンタ、スキャナ、携帯端末等）であってもよい。
【００２１】
まず、複合機１０１について説明する。
【００２２】
１０２はネットワーク１２６を介して外部機器（例えばＰＣ２０１）と通信を行うためのネットワーク通信部である。１０３は複合機１０１に対する設定を受け付けたり、複合機１０１の状態を表示したり、ユーザーからの操作を可能とするＵＩ操作部である。１０４はプリントデータの画像処理や各種制御を実行するＣＰＵである。１０６はＣＰＵ１０４が実行するプログラムコードや、画像データなどの情報を一時的に記憶するＲＡＭである。１０７はプログラムコードや画像データ等を記憶する記憶装置である。１０８は画像データを実際の用紙媒体に印刷するために、電子写真技術やインクジェット技術などの既知の技術を用いた印刷エンジンである。１１４は用紙媒体に印刷された画像を光学的に読み取るスキャナエンジンである。
【００２３】
上記構成において、複合機１０１におけるコピー機能は次のように実現される。すなわち、ＵＩ操作部１０３の操作を起点として、ＣＰＵ１０４がＲＡＭ１０５に記憶されたプログラムコードに従ってスキャナエンジン１０８から画像データを読み込む。読み込んだ画像データは記憶装置１０６に取り込まれ、必要な画像処理を加えて印刷エンジン１０７によって出力される。
【００２４】
また、ＰＤＦ送信機能は次のように実現される。すなわち、ＵＩ操作部１０３の操作を起点として、ＣＰＵ１０４はＲＡＭ１０５に記憶されたプログラムコードに従ってスキャナエンジン１０８から画像データを読み込む。読み込んだ画像データは記憶装置２０５に取り込まれ、所定のフォーマット変換が行われた後に、指定された宛先に対して、ネットワーク通信部１０２から送信される。
【００２５】
次に、ＰＣ２０１について説明する。
【００２６】
２０２はネットワーク１２６を介して外部機器と通信を行うためのネットワーク通信部である。２０３は各種制御を実行するＣＰＵである。２０４はＣＰＵ１０４が実行するプログラムコードなどの情報を一時的に記憶するＲＡＭである。２０５はプログラムコードやデータを記憶する記憶装置である。２０６は管理者によるＰＣ２０１への入力を受け付ける操作表示部である。操作表示部２０６は、操作手段及び表示手段として機能する。
【００２７】
図２（ａ）は、図１の複合機１０１における情報セキュリティポリシーの制御に関連する機能の概略構成を示すブロック図である。図２（ｂ）は、図１のＰＣ２０１における情

報セキュリティポリシーの制御に関連する機能の概略構成を示すブロック図である。なお、本実施形態では、図示の機能がソフトウェアで構成されているものとして説明するが、ハードウェアで構成されていてもよい。

【００２８】

図２（ａ）において、１１４は、ＵＩ操作部１０３によって設定された、複合機１０１の動作に関わる設定項目（以下、「ユーザーモード」と呼ぶ）の名称と値を格納するユーザーモード格納部である。なお、ユーザーモードの名称と値等は、実際は記憶装置１０６等に記憶される。

【００２９】

ユーザーモード設定項目には、例えば、「強制デジタル署名付きＰＤＦ」や「強制ハッシュ付きＰＤＦ」がある。

【００３０】

「強制デジタル署名付きＰＤＦ」とは、次のことである。すなわち、複合機１０１がＰＤＦファイル生成時に強制的にＰＤＦファイルからハッシュ値を計算する。そして、そのハッシュ値をファイル作成者の秘密鍵で暗号化することで得られた電子署名をファイルに付加することでファイル作成者が本人であることを検証する機能の設定項目である。なお、「強制デジタル署名付きＰＤＦ」のユーザーモード設定項目を有効にした場合は作成したファイルの改ざんを検知することもできる。

【００３１】

「強制ハッシュ付きＰＤＦ」は、ＰＤＦファイル生成時に強制的にＰＤＦファイルからハッシュ値を計算し、そのハッシュ値をファイルに付加することでファイルの改ざんを検知可能とする機能の設定項目である。

【００３２】

また、「ＦＴＰ」や「ＳＦＴＰ」などもユーザーモード設定項目の一例である。ＦＴＰとはＦｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌの略称であり、ネットワークでファイル転送を行うための通信プロトコルである。ＳＦＴＰはＳＳＨ　Ｆｉｌｅ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌの略称であり、ネットワークで暗号通信を用いてファイル転送を行うための通信プロトコルである。「ＦＴＰ」や「ＳＦＴＰ」のユーザーモード設定項目を有効にした場合、記憶装置１０６に記憶されたファイルをＦＴＰで送信するといった機能を利用することができる。

【００３３】

１１０は、ネットワーク通信部１０２を介して外部から送られてきたセキュリティポリシーデータを記憶装置１０６等に格納するポリシー格納部である。１１１は、セキュリティポリシーデータと複合機１０１の現在のユーザーモードの値とを比較するために必要な情報が書かれた変換ルールファイルを記憶装置１０６等に格納する変換ルール格納部である。変換ルールファイルの詳細については後述する。

【００３４】

１１２はポリシー変換手段であるポリシー変換部であり、変換ルール格納部１１１に格納された変換ルールファイルに基づいて、セキュリティポリシーデータをユーザーモードの値と比較するための中間情報を生成する。１１５は不揮発記憶装置によって構成され、ポリシー変換部１１２によって生成された中間情報を格納する中間情報格納部である。

【００３５】

１０９はポリシー判定手段であるポリシー検証部であり、中間情報格納部１１５に格納された中間情報とユーザーモード格納部１１４に格納されたユーザーモードの値とを比較し、変換ルールファイルに書かれた条件によって判定を行う。この判定を行った結果、条件を満たさない場合、ポリシー検証部１０９は画面制御を行うための画面制御情報を生成する。

【００３６】

１１６は、ポリシー検証部１０９によって生成された画面制御情報を格納する画面制御情報格納部である。画面制御情報は、記憶装置１０６等に記憶される。

【００３７】
ポリシー検証部１０９は、上記に加えて、複合機１０１の各種アプリケーションの動作制御をも行う。複合機１０１には、図示されていないが、複合機１０１の送信機能・プリント機能・ファイルサーバ機能等を提供するための各種アプリケーションを有している。ポリシー検証部１０９は、これら各種アプリケーションが情報セキュリティポリシーに応じて限定的に動作されるように制御したり、あるいは情報セキュリティポリシーを遵守しないアプリケーションの起動を禁止したりする。
【００３８】
複合機１０１は、不図示であるが、スキャナエンジン１０８を制御し、原稿を光学的に読み取って得られた画像データを電子ファイル化して指定の宛先に送信するＳｅｎｄモジュールを有している。
【００３９】
また、複合機１０１は、ＰＣ２０１や他のデバイスからネットワークを介して受信したＰＤＬコードを解釈して印刷を実行するモジュールなどを有している。また、複合機１０１は、画像データを記憶装置１０６に蓄積するＢＯＸモジュールを有している。さらに、ＨＴＴＰ又はＨＴＴＰＳプロトコルによりインターネットまたはイントラネット上の各種Ｗｅｂサイト（ホームページ）の情報を読み込んで表示を行うためのＷｅｂブラウザモジュールなども有している。これらアプリケーションは、ポリシー検証部１０９によって情報セキュリティポリシーを遵守しているか否かの判定がなされる。そして、情報セキュリティポリシーを遵守していないアプリケーションであると判定されると、画面制御情報が生成されたり、当該アプリケーションの起動が制限される。
【００４０】
ポリシー検証部１０９によって制御されるアプリケーションは、複合機１０１に動的に追加・削除されるアプリケーションも含まれる。例えば、複合機１０１にＪａｖａ（登録商標）の実行環境を組み込むことにより、組み込みアプリケーションを動的に追加・削除できるＭＥＡＰ（登録商標）が製品化されている。（ＭＥＡＰ：Ｍｕｌｔｉ－ｆｕｎｃｔｉｏｎａｌ　Ｅｍｂｅｄｄｅｄ　Ａｐｐｌｉｃａｔｉｏｎ　Ｐｌａｔｆｏｒｍ）
また、ＭＥＡＰのＡＰＩ（アプリケーション・プラットホーム・インターフェイス）を自社以外に公開することにより、サードパーティがアプリケーションを作成することが可能となる。以降、このようなアプリケーションを拡張アプリケーションと呼称する。
【００４１】
１１８は、拡張アプリケーション管理手段である拡張アプリケーション管理部であり、複合機１０１の複数の拡張アプリケーションを管理、動作させる。
【００４２】
１１９は、情報セキュリティポリシーの変更を検知した場合に、拡張アプリケーション管理部１１８により管理されている拡張アプリケーションに対して変更通知を行う。
【００４３】
１２０は、ポリシー問い合わせ手段であるポリシー問い合わせ部であり、拡張アプリケーションからの情報セキュリティポリシーの設定値の問い合わせを受け付ける。
【００４４】
１２１は、システム動作指示手段であるシステム動作指示部であり、拡張アプリケーションから複合機１０１の再起動の指示を受け付ける。
【００４５】
１１７はポリシー受信手段であるポリシー受信部であり、ネットワーク通信部１０２に受信したセキュリティポリシーデータをポリシー格納部１１０に格納する。１１３は画面制御手段である画面制御部であり、画面制御情報格納部１１６に格納された画面制御情報を利用して画面制御を行う。
【００４６】
図２（ｂ）において、２０７はポリシー生成手段であるポリシー生成部であり、管理者の入力に従って、セキュリティポリシーデータの生成を行う。２０８はポリシー送信手段

であるポリシー送信部であり、ポリシー生成部２０７によって生成されたセキュリティポリシーデータをネットワーク通信部２０２からネットワーク１２６を介して送信する。

【００４７】

次に、本発明の情報セキュリティポリシー制御方法における３つの段階について説明する。

【００４８】

まず、管理者がＰＣ２０１を用いて、複合機１０１を情報セキュリティポリシー（以下、単に「情報セキュリティポリシー」とも呼ぶ）に従った状態にするためのセキュリティポリシーデータを生成する段階である。

【００４９】

次に、生成したセキュリティポリシーデータをＰＣ２０１から複合機１０１に送信、適用することで、複合機１０１が情報セキュリティポリシーに従った状態にあるか判定し、管理者に通知する段階である。

【００５０】

最後に、ユーザーがセキュリティポリシーデータを適用した複合機１０１を情報セキュリティポリシーに違反しない状態で利用する段階である。

【００５１】

まず、管理者がＰＣ２０１を用いて、複合機１０１を情報セキュリティポリシーに従った状態にするためのセキュリティポリシーデータを生成する段階の処理について説明する。

【００５２】

図３は、ＰＣ２０１の操作表示部２０６に表示される、セキュリティポリシーデータを生成するためのポリシー設定画面の一例を示す図である。なお、本実施形態では、説明を簡単にするために、ファイルの改ざん検知、ファイル共有、ＨＤＤ残存データ削除の３つの情報セキュリティポリシーを設定する場合のみを説明するが、実際にはより多くの情報セキュリティポリシーが存在してもよい。また、各情報セキュリティポリシーの値がラジオボタンによって選択される場合のみを説明するが、テキストフィールドによる入力やチェックボックスによって複数の選択肢から選択が可能な形式であってもよい。

【００５３】

図３において、ポリシー設定画面３０１は、「ファイルの改ざん検知」３０２、「ファイルの送信方式」３０３、「ＨＤＤ残存データ削除」３０４という３つの情報セキュリティポリシーを設定するための設定画面である。

【００５４】

「ファイルの改ざん検知」３０２は、生成したファイルに改ざん検知が必要か否かを示す情報セキュリティポリシーである。本実施形態では、「もっともセキュリティレベルの高い手段を使う」、「どれか一つを使う」、「情報セキュリティポリシーなし」の３つから情報セキュリティポリシーを選択できる。図示例では、「どれか一つが有効」が選択されている状態を示す。

【００５５】

「ファイルの送信方式」３０３は、ファイルの送受信を行うときに、暗号化通信を使う必要があるか否かを示す情報セキュリティポリシーである。本実施形態では、「暗号化通信ならＯＫ」、「情報セキュリティポリシーなし」の２つから情報セキュリティポリシーを選択できる。図示例では、「情報セキュリティポリシーなし」が選択されている状態を示す。

【００５６】

「ＨＤＤ残存データ削除」３０４は、複合機１０１におけるコピー処理等で不揮発記憶装置（不図示）を一時データ記憶領域として使用した場合に、処理完了後に残存するデータを削除するか否かを示す情報セキュリティポリシーである。図示例では、「削除」が選択されている状態を示す。

【００５７】

管理者は、ポリシー設定画面３０１を使って各情報セキュリティポリシーの設定を行う。ポリシー設定画面３０１において、「ＯＫ」ボタン３０５の押下を操作表示部２０６が受け付けると、ポリシー生成部２０７は、ポリシー設定画面３０１上で設定された内容に応じたセキュリティポリシーデータを生成し、記憶装置２０５に記憶する。記憶装置２０５に記憶されたセキュリティポリシーデータを表形式で表した一例を図４（ａ）に示す。なお、本実施形態では、説明を簡単にするために、表形式のセキュリティポリシーデータについて説明するが、ＸＭＬ等のデータ形式であってもよい。図４（ａ）に示すセキュリティポリシーデータをＸＭＬ形式で表したセキュリティポリシーデータを図１７に示す。

【００５８】

セキュリティポリシーデータ４０１では、１列目が、ポリシー設定画面３０１上で管理者により設定された情報セキュリティポリシーの名称（ルール）４０２である。２列目が、ポリシー設定画面３０１上で管理者によって選択された各情報セキュリティポリシーの値（条件）４０３となっている。

【００５９】

次に、生成したセキュリティポリシーデータをＰＣ２０１から複合機１０１に送信、適用することで、複合機１０１が情報セキュリティポリシーに従った状態にあるか判定し、管理者に通知する段階の処理について説明する。

【００６０】

管理者によるセキュリティポリシーデータ送信の指示を受け付けた操作表示部２０６は、ポリシー送信部２０８に送信を指示する。指示を受けたポリシー送信部２０８は、記憶装置２０５に記憶されたセキュリティポリシーデータをネットワーク通信部２０２からネットワーク１２６を介して、複合機１０１のネットワーク通信部１０２に送信する。なお、セキュリティポリシーデータは、ＰＣ２０１から自動配信されるように構成してもよい。また、管理者や特定のコンピュータから送られたことを認証する方法が望ましいが、本実施形態ではそれらの説明を省略する。

【００６１】

図５は、複合機１０１にセキュリティポリシーデータを適用する際に実行される情報セキュリティポリシー変換処理の流れを示すフローチャートである。なお、本処理は、特に断りがない限り、記憶装置１０６からＲＡＭ１０５に読み込んだプログラムコードによって、ＣＰＵ１０４が実行するものとする。

【００６２】

図５において、ステップＳ４０１では、ネットワーク通信部１０２がセキュリティポリシーデータをＰＣ２０１から受信すると、ポリシー受信部１１７が該セキュリティポリシーデータをポリシー格納部１１０に格納する。

【００６３】

次に、ステップＳ４０２では、ポリシー変換部１１２は、ポリシー格納部１１０に格納されたセキュリティポリシーデータから１行目の情報セキュリティポリシーを取得する。そして、情報セキュリティポリシーの名称と値を抽出してＲＡＭ１０５に記憶する。

【００６４】

次に、ステップＳ４０３では、ポリシー変換部１１２は、変換ルール格納部１１１に格納されている変換ルールファイル５０１（図４（ｂ））を取得する。そして、取得した変換ルールファイルのルール部５０２に書かれた情報セキュリティポリシーの名称と、ＲＡＭ１０５に記憶された情報セキュリティポリシーの名称とを比較する。そして、その比較結果から一致する名称があるか判定する。つまり、ステップＳ４０２で抽出した情報セキュリティポリシーの名称が、図４（ｂ）に示す変換ルールファイル５０１の情報セキュリティポリシーの名称群に含まれるか否かを判定する。変換ルール格納部１１１に格納されている変換ルールファイルを表形式で表した一例を図４（ｂ）に示す。なお、本実施形態では、表形式の変換ルールファイルについて説明するが、セキュリティポリシーデータと同様に、必ずしも表形式である必要はない。

【００６５】

図４（ｂ）において、変換ルールファイル５０１は、ルール部５０２と条件部５０３から構成されている。

【００６６】

ルール部５０２の２列目には、セキュリティポリシーデータに記述可能な情報セキュリティポリシーの名称がそれぞれ記述されている。ルール部５０２の３列目には、情報セキュリティポリシーの名称に対応したユーザーモードの名称がそれぞれ記述されている。

【００６７】

条件部５０３の２列目には、セキュリティポリシーデータに記述可能な情報セキュリティポリシーの名称がそれぞれ記述されている。条件部５０３の３列目には、セキュリティポリシーデータに設定可能な情報セキュリティポリシーの値がそれぞれ記述されている。条件部５０３の最後の列には、ユーザーモードの設定が情報セキュリティポリシーに従っているか判定するための条件がそれぞれ記述されている。

【００６８】

本実施形態では、変換ルールファイル５０１は、予め変換ルール格納部１１１に格納されているものとして説明するが、セキュリティポリシーデータと同様に、ネットワーク通信部１０２で外部（例えばＰＣ２０１）から受信する形態であってもよい。また、変換ルールファイル５０１は、セキュリティポリシーデータを作成する情報システム部門の管理者とは別の管理者、例えば機器管理者によってネットワーク通信部１０２に配信され、変換ルール格納部１１１に格納されるというものであってもよい。

【００６９】

図４（ｂ）において、ルール部５０２の２列目の「ファイルの改ざん検知」は、複合機１０１のユーザーモードの中でも、「強制デジタル署名付きＰＤＦ」、「強制ハッシュ付きＰＤＦ」に対応していることを示している。これは、複合機１０１がＰＤＦファイル生成時に強制的にＰＤＦファイルのハッシュ値（「強制デジタル署名付きＰＤＦ」の場合はハッシュ値を暗号化して得られたデジタル署名）を付加する機能を有している。これらの値によって、「ファイルの改ざん検知」の情報セキュリティポリシーに従っているか否かが決まることを意味している。

【００７０】

また、ルール部５０２の２列目における「ファイル送信の送受信方式」は、複合機１０１のユーザーモードの中でも、「ＦＴＰ」、「ＳＦＴＰ」に対応していることを示している。これらは複合機１０１が利用できる通信プロトコルとして、ＦＴＰやＳＦＴＰの利用の可否を選択する機能を有しており、これらの値によって、「ファイル送信の送受信方式」の情報セキュリティポリシーに従っているか否かが決まることを意味している。なお、図４（ｂ）の変換ルールファイル５０１をＸＭＬ形式で表したものを図１８に示す。

【００７１】

図５に戻り、ステップＳ４０３にて一致する名称があると判定した場合、ステップＳ４０４へ進む。ステップＳ４０４では、ポリシー変換部１１２は、ステップＳ４０２にてＲＡＭ１０５に記憶された情報セキュリティポリシーの名称を変換ルールファイル５０１のルール部５０２に記述されたユーザーモードの名称に変換する。そして、ポリシー変換部１１２は、管理者によって選択された情報セキュリティポリシーの値と対応付けてＲＡＭ１０５に中間情報として記憶する。例えば、図４（ａ）のセキュリティポリシーデータ４０１における「ファイルの改ざん検知」は、図４（ｂ）の変換ルールファイル５０１におけるルール部５０２の「ファイルの改ざん検知」と一致する。

【００７２】

そこで、ポリシー変換部１１２は、情報セキュリティポリシーの名称「ファイルの改ざん検知」をユーザーモードの名称「強制デジタル署名付きＰＤＦ」、「強制ハッシュ付きＰＤＦ」に変換する。そして、これらと情報セキュリティポリシーの値「どれか一つ有効」と対応付けて中間情報としてＲＡＭ１０５に記憶する。

【００７３】

一方、ステップＳ４０３の判定結果から一致する名称がないと判定した場合、ポリシー

変換部１１２は、ステップＳ４０２にＲＡＭ１０５に記憶された情報セキュリティポリシーの名称をエラー情報としてＲＡＭ１０５に記憶する（ステップＳ４０５）。

【００７４】

ステップＳ４０３でＮＯと判定される場合は例えば次のような場合である。セキュリティポリシーデータ４０１から取得した名称４０２が「ＨＤＤの残存データ削除」で且つ変換ルールファイルのルール部５０２に記述されている情報セキュリティポリシーの名称群に「ＨＤＤの残存データ削除」の項目が含まれていない場合である。

【００７５】

次に、ステップＳ４０６では、ポリシー変換部１１２は、セキュリティポリシーデータの次の行の情報セキュリティポリシーがあるか判定する。次の行の情報セキュリティポリシーがあると判定した場合、ステップＳ４０７へ進む。

【００７６】

ステップＳ４０７では、ポリシー変換部１１２は、セキュリティポリシーデータの次の行を取得し、情報セキュリティポリシーの名称と値を抽出してＲＡＭ１０５に記憶し、ステップＳ４０３に戻る。ステップＳ４０３～Ｓ４０７の処理は、セキュリティポリシーデータに含まれるすべての情報セキュリティポリシーを読み取るまで行われる。図４（ａ）に示すセキュリティポリシーデータをすべて読み取った後に、ＲＡＭ１０５に記憶された中間情報を表形式で表した一例を図４（ｃ）に示す。

【００７７】

図４（ｃ）に示す中間情報６０１では、ユーザーモードの名称「強制デジタル署名付きＰＤＦ」と「強制ハッシュ付きＰＤＦ」が、情報セキュリティポリシーの値「どれか一つ有効」に対応することを示している。また、ユーザーモードの名称「ＦＴＰ」と「ＳＦＴＰ」が、情報セキュリティポリシーの値「情報セキュリティポリシーなし」に対応することを示している。なお、セキュリティポリシーデータ４０１における「ＨＤＤ残存データ削除」は、変換ルールファイル５０１に名称が存在しないため、ステップＳ４０５にてエラー情報としてＲＡＭ１０５（エラー情報格納手段）に記憶される。

【００７８】

図５に戻り、ステップＳ４０８において、ポリシー変換部１１２は、セキュリティポリシーデータをすべて読み取ると、ＲＡＭ１０５に記憶された中間情報を中間情報格納部１１５に格納する。

【００７９】

図６は、複合機１０１にセキュリティポリシーデータを適用する際に実行される情報セキュリティポリシー適用処理の流れを示すフローチャートである。なお、本処理は、特に断りがない限り、記憶装置１０６からＲＡＭ１０５に読み込んだプログラムコードによって、ＣＰＵ１０４が実行するものとする。

【００８０】

ステップＳ４０９にて、ポリシー検証部１０９は、中間情報格納部１１５に格納された中間情報をすべて読み取ったか判定する。すべて読み取っていないと判定した場合、ステップＳ４１０にてポリシー検証部１０９は、中間情報から、取得していない情報セキュリティポリシーの値を１つと、それに対応するユーザーモードの名称を取得し、ＲＡＭ１０５に記憶する。図４（ｃ）に示す中間情報６０１の場合、「どれか一つ有効」と「強制デジタル署名付きＰＤＦ」、「強制ハッシュ付きＰＤＦ」がＲＡＭ１０５に記憶される。

【００８１】

次に、ステップＳ４１１にて、ポリシー検証部１０９は、ＲＡＭ１０５に記憶されたユーザーモードの名称を用いて、ユーザーモード格納部１１４から複合機１０１に設定された現在のユーザーモードの値を取得する。複合機１０１のユーザーモード格納部１１４に格納されているユーザーモードの名称と値を表形式で表したものを図７（ａ）に示す。なお、表中の「ＯＮ」はユーザーモードの名称によって示される機能が有効であることを示し、「ＯＦＦ」は無効であることを示す。例えば、ステップＳ４１１では、「強制デジタル署名付きＰＤＦ」の値として「ＯＦＦ」、「強制ハッシュ付きＰＤＦ」の値として「Ｏ

ＦＦ」を取得し、ＲＡＭ１０５に記憶する。

【００８２】

ステップＳ４１２にて、ポリシー検証部１０９は、読み取った情報セキュリティポリシーの値を用いて、変換ルール格納部１１１に格納された変換ルールファイルの条件部５０３から、対応する条件を取得する。そして、ＲＡＭ１０５に記憶された現在のユーザーモードが条件を満たすか判定する。

【００８３】

図４（ｂ）に示す条件部５０３の「もっともセキュリティレベルの高い手段を使う」は、現在のユーザーモードの「強制デジタル署名付きＰＤＦ」の値が「ＯＮ」である場合に、ステップＳ４１２で条件を満たすと判定されることを示している。

【００８４】

「どれか一つ有効」は、現在のユーザーモードの「強制デジタル署名付きＰＤＦ」が「ＯＮ」もしくは「強制ハッシュ付きＰＤＦ」が「ＯＮ」である場合に、ステップＳ４１２で条件を満たすと判定されることを示している。

【００８５】

「情報セキュリティポリシーなし」は現在のユーザーモードの値に関わらず、ステップＳ４１２で条件を満たすと判定されることを示している。「暗号化通信ならＯＫ」は現在のユーザーモードの「ＦＴＰ」が「ＯＦＦ」、「ＳＦＴＰ」が「ＯＮ」である場合に条件を満たすと判定することを示している。

【００８６】

ステップＳ４１２の判定結果から条件を満たすと判定した場合、ステップＳ４０９に戻る。一方、条件を満たさないと判定した場合、ポリシー検証部１０９は、ステップＳ４１０でＲＡＭ１０５に記憶された情報とステップＳ４１２にて変換ルールから取得した条件の組を画面制御情報としてＲＡＭ１０５に一時的に記憶する（ステップＳ４１３）。そして、ステップＳ４０９に戻る。

【００８７】

更に、本実施形態では、ステップＳ４１２にて、ポリシー検証部１０９は、ユーザーモードの値の確認だけでなく、複合機１０１の各アプリケーションが情報セキュリティポリシーを遵守しているかの確認も行う。具体的には、まずポリシー検証部１０９は、複合機１０１にインストールされている各アプリケーションが情報セキュリティポリシーに関係するアプリケーションであるかを判定する。例えば、「ファイルの改ざん検知」という情報セキュリティポリシーを適用する場合、複合機１０１にインストールされているアプリケーションが、「ファイルの改ざん検知」の情報セキュリティポリシーを遵守することができるアプリケーションであるか判定する。そして、遵守することができるアプリケーションである場合はアプリケーションのファイル改ざん検知機能を強制的にＯＮにしたり、ファイルの改ざん検知を必須とする旨を当該アプリケーションに通知したりする。

【００８８】

また、ステップＳ４１２の判定の結果、ファイル改ざん検知の情報セキュリティポリシーを遵守することができないアプリケーションであると判定された場合には、ステップＳ４１３にてそのアプリケーションを示す画面制御情報をＲＡＭ１０５に記憶する。また、情報セキュリティポリシーを遵守しないアプリケーションの起動を制限したりしてもよい。

【００８９】

ステップＳ４０９からステップＳ４１３の処理は中間情報をすべて読み取るまで行われる。中間情報をすべて読み取ると、ステップＳ４１４へ進む。

【００９０】

ステップＳ４１４では、ポリシー検証部１０９は、ＲＡＭ１０５に記憶された画面制御情報を画面制御情報格納部１１６に格納する。ステップＳ４１４を実行する時点でＲＡＭ１０５に記憶された画面制御情報を表形式で表したものを図７（ｂ）に示す。

【００９１】

図７（ｂ）において、複合機１０１の現在の「強制デジタル署名付きＰＤＦ」と「強制ハッシュ付きＰＤＦ」の両方の値がＯＦＦであるため、「どれか一つ有効」の条件を満たさず、画面制御情報が記憶される。一方、「ＦＴＰ」、「ＳＦＴＰ」の条件は「情報セキュリティポリシーなし」であるため、画面制御情報は記憶されない。

【００９２】

図６のステップＳ４１５では、ポリシー検証部１０９は、図５のステップＳ４０５でエラーとしてＲＡＭ１０５に記憶された情報セキュリティポリシーの名称若しくはステップＳ４１４にて画面制御情報格納部１１６に格納された画面制御情報があるか判定する。情報セキュリティポリシーの名称若しくは画面制御情報があると判定された場合、ステップＳ４１６に進む。ステップＳ４１６では、ポリシー検証部１０９は、これらの情報をネットワーク通信部１０２からネットワーク１２６を介してＰＣ２０１に送信する。

【００９３】

ＰＣ２０１は、情報セキュリティポリシーの名称をネットワーク通信部２０２で受け取ると、複合機１０１に適用できない情報セキュリティポリシーがあった旨を管理者に通知する。また、ＰＣ２０１は、複合機１０１から画面制御情報を受け取った場合、ＰＣ２０１のディスプレイに図８（ａ）のような表示画面を表示し、複合機１０１が情報セキュリティポリシーに反した状態であることを管理者に通知する。

【００９４】

図８（ａ）では、「＜エラー！＞」の項目に、ステップＳ４０５でエラーとしてＲＡＭ１０５に記憶された「ＨＤＤ残存データ削除」を、「注意！」の項目に、画面制御情報から抽出した「強制デジタル署名付きＰＤＦ」、「強制ハッシュ付きＰＤＦ」を表示する。なお、管理者に通知する方法として、ＰＣ２０１が画面を表示するとしたが、メールで情報を送信する等の方法であってもよい。

【００９５】

以上により、ＰＣ２０１で作成されたセキュリティポリシーデータを複合機１０１に好適に適用させることができる。特に、ＰＣ２０１で情報セキュリティポリシーを作成する情報システム部門の管理者は、複合機１０１の機能やユーザーモードの設定値などを意識せずに上記情報セキュリティポリシーを作成することができる。

【００９６】

次に、セキュリティポリシーデータが適用された複合機１０１におけるエラー画面表示処理について説明する。

【００９７】

図９は、複合機１０１の画面制御部１１３により実行されるエラー画面表示処理の流れを示すフローチャートである。なお、本処理は、特に断りがない限り、記憶装置１０６からＲＡＭ１０５に読み込んだプログラムコードによって、ＣＰＵ１０４が実行するものとする。なお図９の処理は、図６のフローチャートが実行された後に実行される。

【００９８】

ステップＳ１００１にて、画面制御部１１３は、画面制御情報格納部１１６に格納された画面制御情報が存在するか判定する。画面制御情報が存在すると判定した場合、ステップＳ１００２にて画面制御部１１３はエラー画面を表示する。画面制御部１１３が表示するエラー画面の一例を図８（ｂ）に示す。

【００９９】

図８（ｂ）に示すエラー画面では、画面制御部１１３が図７（ｂ）に示す画面制御情報から、ユーザーモードの名称を抽出し、「強制デジタル署名付きＰＤＦ」と「強制ハッシュ付きＰＤＦ」の設定変更が必要な旨が表示されている。なお、図８（ａ）に示すエラー画面と同様に「＜エラー！＞」の項目として「ＨＤＤ残存データ削除」の情報セキュリティポリシーが適用されていない旨が表示されてもよい。そして、「ＨＤＤ残存データ削除」の情報セキュリティポリシーを遵守するために必要な機能を複合機１０１に追加する旨が表示されてもよい。

【０１００】

本実施形態では、エラー画面が表示された状態で、ユーザーが複合機１０１で利用可能な機能が、ＵＩ操作部１０３を用いたユーザーモードの設定のみとして説明する。なお、情報セキュリティポリシーに違反したユーザーモードに関連しない機能は利用できるように画面制御を行ってもよい。

【０１０１】

図９に戻り、ステップＳ１００３にて、画面制御部１１３は、ユーザーによるＵＩ操作部１０３の操作によってユーザーモード格納部１１４に格納されたユーザーモードの値が変更されたか否かを判定する。設定が変更されないと判定した場合、ステップＳ１００２に戻り、図８（ｂ）に示すエラー画面を表示する。一方、設定が変更された場合、図６に示すセキュリティポリシーの適用処理を行い、ステップＳ１００１に戻る。

【０１０２】

ステップＳ１００１にて画面制御情報が存在しないと判定した場合、画面制御部１１３は、ステップＳ１００３と同様の判定をする（ステップＳ１００５）。ステップＳ１００５にてユーザーモードの値が変更されたと判定した場合、ステップＳ１００４に進む。一方、ステップＳ１００５にてユーザーモードの値が変更されていないと判定した場合、本処理を終了して再度図９の処理を開始する。

【０１０３】

なお、本実施形態では、管理者がＰＣ２０１のポリシー生成部２０７を用いてセキュリティポリシーデータを生成する形態について説明した。しかし、ポリシー生成部２０７が複合機１０１内部にあり、管理者がＵＩ操作部１０３もしくはＰＣ２０１を用いて複合機１０１にアクセスし、セキュリティポリシーデータの設定を行う構成であってもよい。

【０１０４】

次に、外部から追加された拡張アプリケーションに対して情報セキュリティポリシーを適用させる方法について説明する。

【０１０５】

図１０は、拡張アプリケーションの構成例を示す模式図である。

【０１０６】

拡張アプリケーションは、複合機１０１とは異なる形態（ＣＤ－ＲＯＭやネットワーク配信など）で図１０に示す形式で提供され、複合機１０１に取り込まれると構成要素が分解されて複合機１０１に格納される。

【０１０７】

図１０において、１００１は拡張アプリケーションの全体を包含したパッケージ、１００２は拡張アプリケーションの本体を示しており、例えばＪａｖａ（登録商標）コードで構成される。また、アプリケーションの本体は、実際に機能を実現する機能実行部１００４と、ポリシー強制処理部１００５の両方を持つ。

【０１０８】

１００３は拡張アプリケーションそのものの情報を示すアプリケーション属性情報であり、マニフェストファイルとも呼ばれる。アプリケーション属性情報は例えばテキスト形式で記載されており、拡張アプリケーションの特徴を示す情報が記載されている。図示例では、拡張アプリケーションのアプリケーション名は「スキャン送信アプリケーション」、アプリケーションのバージョンはＶ１．００、アプリケーション識別子は１６進数表記で０ｘ１２３４、ポリシーバージョンはｖ１．００であることを示す。

【０１０９】

複合機１０１は、拡張アプリケーション管理部１１８によって複数の拡張アプリケーションを管理、動作させることが可能である。また、ＡＰＩ（アプリケーション・プログラム・インターフェイス）によって、複合機１０１のスキャン動作結果の受け渡しや、拡張アプリケーションによって作られた画像データの出力も可能である。さらに、ユーザー認証によって得られた認証情報の受け渡しや、機器のシャットダウンのようなソフトウェアの制御も可能となっている。

【０１１０】

また、情報セキュリティポリシーに対応する拡張アプリケーションの場合、情報セキュリティポリシーの変更を拡張アプリケーションに通知し、関係する設定値を変更する。これにより、当該拡張アプリケーションの動作を情報セキュリティポリシーの範囲内に強制することが可能である。

【０１１１】

図１１は、複合機１０１と拡張アプリケーション間で情報のやり取りや指示を行うＡＰＩを説明するための図である。

【０１１２】

図１１において、１６０１は複合機１０１を示し、１６０２は拡張アプリケーションを示す。両者の間にインターフェイスとしてＡＰＩが取りきめられ、所定の呼び出しによってお互いの情報のやり取りや指示を行う。

【０１１３】

１６０３は、拡張アプリケーション１６０２が動作中に、情報セキュリティポリシーの変更が行われたときに、変更を通知するためのイベント通知方法を登録するＡＰＩである。このＡＰＩは拡張アプリケーション１６０２から複合機１０１内の拡張アプリケーション管理部１１８に通知を行う。

【０１１４】

複合機１０１は予め登録される拡張アプリケーションを把握していないため、個々の拡張アプリケーションが起動したときにイベント通知方法を登録する。イベント通知方法には、一般的なＩＰＣ（プロセス間通信）であるメッセージ通知を用いられるが、プロセス間の通信方法であれば他の方法を用いてもよい。

【０１１５】

１６０４は実際に情報セキュリティポリシーの変更が発生した場合に、ポリシー変更通知部１１９が個々の拡張アプリケーションに通知を行うＡＰＩである。これは１６０３のＡＰＩ呼び出しで登録されたメッセージを呼び出すことによって実現する。

【０１１６】

１６０５は拡張アプリケーション１６０２がポリシー問い合わせ部１２０に対して情報セキュリティポリシーの設定値を問い合わせるためのＡＰＩである。このＡＰＩが呼び出されるのは、拡張アプリケーション１６０２が起動を始めた場合と、１６０４のＡＰＩによって情報セキュリティポリシーの変更を通知された場合である。この問い合わせ結果に応じて、拡張アプリケーション１６０２は自身が持つ設定値を情報セキュリティポリシーに合うように強制する。

【０１１７】

１６０６は拡張アプリケーション１６０２からシステム動作指示部１２１に対して複合機１０１の再起動の指示を行うためのＡＰＩである。このＡＰＩによって再起動の指示が行われると、複合機１０１は全ての情報セキュリティポリシーの変更に係わる処理が完了した時点で再起動を行う。

【０１１８】

図１２は、拡張アプリケーション管理部１１８の動作を説明するためのフローチャートである。

【０１１９】

拡張アプリケーション管理部１１８は、複合機１０１の動作開始と共に起動し、以降電源遮断まで動作を継続する。

【０１２０】

図１２において、ステップＳ１１０１では、拡張アプリケーション管理部１１８は、拡張アプリケーションの登録が指示されたかどうかを判定する。拡張アプリケーション管理部１１８は、不図示のＷｅｂサービスインターフェイスを持ち、ＰＣ２０１の不図示のウェブ・ブラウザソフトウェアを用いることによって、拡張アプリケーションのパッケージ１００１をネットワーク１２６を介して転送する。

【０１２１】

次に、ステップＳ１１０２では、拡張アプリケーション管理部１１８は、転送されたパッケージ１００１からアプリケーション属性情報１００３を抽出して取得し、書き込まれた情報を調査する。

【０１２２】

ステップＳ１１０３では、拡張アプリケーション管理部１１８は、ポリシーバージョンが記載されているかを判定する。ポリシーバージョンが記載されていると判定した場合、拡張アプリケーション管理テーブル１２００にポリシーバージョンを記載する（ステップＳ１１０４）。

【０１２３】

次に、拡張アプリケーション管理部１１８は、拡張アプリケーションにポリシー変更通知を行うためのポリシー変更イベントを登録する（ＡＰＩ１６０３）（ステップＳ１１０５）。これは、上述したポリシー強制処理部１００５に通知を行うイベントであり、Ｊａｖａ(登録商標)コードのメッセージを想定しているが、他のプロセス間通信を使っても実現可能である。

【０１２４】

ステップＳ１１０６では、拡張アプリケーション管理部１１８は、情報セキュリティポリシー以外のその他のアプリケーション属性を記憶装置１０６に記憶する。

【０１２５】

次に、ステップＳ１１０７では、拡張アプリケーション管理部１１８は、アプリケーション本体１００２を記憶装置１０６に記憶して、ステップＳ１１０１に戻り、次の拡張アプリケーションの登録を待つ。

【０１２６】

図１３は、拡張アプリケーション管理テーブル１２００の一例を示す図である。

【０１２７】

拡張アプリケーション管理テーブル１２００は、拡張アプリケーション管理部１１８により管理及び保持され、図１２のステップＳ１１０４及びステップＳ１１０６にてエントリが作成される。

【０１２８】

図１３において、１２０１～１２０３は、登録された拡張アプリケーションの一例であり、複合機１０１に登録される拡張アプリケーションの数だけエントリを持つ。１２０４～１２０７は拡張アプリケーション固有の情報であって、アプリケーション属性情報１００３に記載された情報と同一の情報である。

【０１２９】

１２０３で登録されている拡張アプリケーション「パーソナルセキュアプリント」のポリシーバージョンが「－（ハイフン）」になっている。これは当該拡張アプリケーションがポリシーバージョンを持っていないこと、すなわち情報セキュリティポリシーによって設定を強制する機能を持っていないことを示す。情報セキュリティポリシーによって設定を強制する機能を持っていないとは、例えば拡張アプリケーションが情報セキュリティポリシーに対応する前の古い拡張アプリケーション（レガシーアプリケーション）である場合である。または、そもそも情報セキュリティポリシーによって制限させる設定値がない場合である。これらの場合の扱いについては第２の実施形態で説明する。

【０１３０】

次に、複合機１０１の情報セキュリティポリシーが変更になった場合の動作を説明する。

【０１３１】

図１４は、ポリシー変更通知部１１９の動作を説明するためのフローチャートである。

【０１３２】

ポリシー変更通知部１１９は複合機１０１の動作開始と共に起動し、以降電源遮断まで動作を継続する。

【０１３３】

図１４において、ステップＳ１３０１では、ポリシー変更通知部１１９は、情報セキュリティポリシーの変更を検知した場合、拡張アプリケーション管理テーブル１２００から拡張アプリケーションの情報を１つ取得する（ステップＳ１３０２）。これは、図６で説明したセキュリティポリシーの適用処理のステップＳ４１４を通過することによって検知したと判定する。

【０１３４】

次に、ポリシー変更通知部１１９は、取得した拡張アプリケーションのポリシーバージョンを調査し（ステップＳ１３０３）、当該拡張アプリケーションのポリシーバージョンが設定されているかを判定する（ステップＳ１３０４）。ポリシーバージョンが設定されている場合、当該拡張アプリケーションが情報セキュリティポリシーに対応可能であるため、ポリシー変更通知部１１９は、当該拡張アプリケーションに情報セキュリティポリシー変更イベントを通知する（ステップＳ１３０５）。これは図１２のステップＳ１１０５で登録した拡張アプリケーションのＡＰＩ１６０４を用いており、拡張アプリケーションは情報セキュリティポリシーの変更を検知して、情報セキュリティポリシーの問い合わせを行うきっかけとなる。

【０１３５】

ステップＳ１３０６では、ポリシー変更通知部１１９は、拡張アプリケーション管理テーブル１２００のすべての拡張アプリケーションへの問い合わせが完了したかを判定する。完了していない場合はステップＳ１３０２から次の拡張アプリケーションへの問い合わせを開始する。一方、すべての拡張アプリケーションへの問い合わせが完了した場合にはステップＳ１３０１に戻り、次の情報セキュリティポリシーの変更を待つ。

【０１３６】

次に、個々の拡張アプリケーションにおける情報セキュリティポリシーの変更方法について説明する。

【０１３７】

図１５（ａ）は、拡張アプリケーションにおける情報セキュリティポリシーと設定値との関係の一例を示す図である。実際には、図示のような対応付けをデータ構造としてもよいし、あるいはＪａｖａ(登録商標)コードとして実現されていてもよい。

【０１３８】

１４０１は、「ファイルの改ざん検知」という情報セキュリティポリシーに対して、関連する設定値がないことを示している。１４０２は、「ファイルの送信方式＝暗号化通信のみ」という情報セキュリティポリシーにおいて、ＦＴＰ通信をＯＦＦとし、ＳＳＬ通信をＯＮにする必要があることを示している。ここでいうＦＴＰでは、通信時に認証情報が平文で流れるため、暗号化通信のみ許可されている場合にはプロトコルそのものを使用することができない。また、ＳＳＬ通信はセキュアソケット層（Ｓｅｃｕｒｅ　Ｓｏｃｋｅｔ　Ｌａｙｅｒ）を構成しているものであり、この経路上にながれる情報はすべて暗号化されるため、上記情報セキュリティポリシーを満たすことが可能である。

【０１３９】

図１６は、ポリシー強制処理部１００５の動作を説明するためのフローチャートである。

【０１４０】

ポリシー強制処理部１００５は、拡張アプリケーションの動作開始と共に起動し、ポリシー変更に伴う拡張アプリケーションの設定変更を行う。

【０１４１】

図１６において、ステップＳ１５０１では、ポリシー強制処理部１００５は、ポリシー変更イベントが届いたかどうかを判定する。届いたと判定した場合、ポリシー強制処理部１００５は、拡張アプリケーションに関係する情報セキュリティポリシーを１つ取得して調査を行う（ステップＳ１５０２）。図１５（ａ）に示す例では、設定値が影響を受ける情報セキュリティポリシーは「ファイルの送信方式＝暗号通信ならＯＫ」のみであるので、ステップＳ１５０２ではこの情報セキュリティポリシーに注目する。

【０１４２】
次に、ステップＳ１５０３では、ポリシー強制処理部１００５は、関連する設定値を１つ取得して調査する。図１５（ａ）に示す例では、設定値は２つあり、最初に「ＦＴＰ通信」という設定に注目する。
【０１４３】
ステップＳ１５０４では、ポリシー強制処理部１００５は、設定値が情報セキュリティポリシーを守っているかどうかを判定する。図１５（ａ）に示す例では、「ファイルの送信方式＝暗号通信ならＯＫ」の情報セキュリティポリシーは「ＦＴＰ通信」という設定値が「ＯＦＦ」であることを要求している。もしＦＴＰ通信がＯＮになっている場合は、ポリシー強制処理部１００５は、ポリシーに合わせるために設定値を強制的にＯＦＦに変更する（ステップＳ１５０５）。
【０１４４】
ステップＳ１５０６では、ポリシー強制処理部１００５は、情報セキュリティポリシーの設定値変更に伴い、再起動が必要かどうかを判定する。例えばネットワークでサービスを行っている場合、リアルタイムで設定を反映させることができない。その場合は複合機１０１全体の再起動を必要とする。そこで、ポリシー強制処理部１００５は、図１５（ｂ）に示すテーブル情報を利用して、拡張アプリケーションの設定値の変更に伴い、再起動が必要かどうかを判定する。
【０１４５】
図１５（ｂ）において、行１４１１では、設定値「ＦＴＰ通信」は、再起動が必要と判定される。一方、行１４１２では、設定値「ＳＳＬ通信」は、再起動が不要と判定される。
【０１４６】
ステップＳ１５０６で再起動が必要と判定されると、ステップＳ１５０７において再起動フラグがセットされる。
【０１４７】
ステップＳ１５０８では、ポリシー強制処理部１００５は、全ての設定値について調査したかを判定する。ここでは「ＳＳＬ通信」についても確認が必要となり、同様の判定が行われる。すべての設定値の確認が終わると、ポリシー強制処理部１００５は、すべての情報セキュリティポリシーを調査したかを判定する（ステップＳ１５０９）。
【０１４８】
すべての情報セキュリティポリシーを調査していない場合には、ステップＳ１５０２に移動し、ポリシー強制処理部１００５は、次の情報セキュリティポリシーに関連する設定値の調査を同様に行う。
【０１４９】
すべての情報セキュリティポリシーに関する調査が完了した場合、ポリシー強制処理部１００５は、再起動フラグがセットされているかどうかを判定する（ステップＳ１５１０）。セットされている場合には、ステップＳ１５１１においてシステムに再起動が必要であることを、ＡＰＩ１６０６を呼び出すことによって通知する。すべての処理が終わるとステップＳ１５０１に戻り、次のポリシー変更イベントを待つ。
【０１５０】
上記第１の実施形態によれば、複合機に外部から導入される拡張アプリケーションに対しても、情報セキュリティポリシーの変更が発生したことを通知し、それに伴う設定値を強制する仕組みを提供する。これによって拡張アプリケーションに対しても情報セキュリティポリシーに従った状態の維持を図ることができる。また、拡張アプリケーションの設定を強制的に変更した場合に、必要な場合にだけ再起動を指示することが可能となり、ダウンタイムの縮小を行うことが可能となる。
【０１５１】
さらに、セキュリティポリシーデータを複合機の設定が満たすべき条件に変換し、変換された条件を、現在の複合機の設定が満たしているか否か判定する。そして、複合機の設

定が、変換された条件を満たしていないと判定された場合には、複合機の利用を制限して複合機の設定を見直すように通知する。これにより、情報セキュリティポリシーに従うようにユーザーモードの設定変更を促し、複合機の情報セキュリティポリシーに従った状態の維持を図ることができる。

【０１５２】

［第２の実施形態］

上記第１の実施形態では、情報セキュリティポリシーを扱うことができる拡張アプリケーションの場合の説明のみを行った。この場合、情報セキュリティポリシーを認識しない拡張アプリケーションが複合機１０１に導入されている場合、情報セキュリティポリシーを変更しても当該拡張アプリケーションに設定値の変更を行わせることができない。

【０１５３】

また、管理者は、このような拡張アプリケーションの設定値の見直しをする必要性に気付かず、情報セキュリティポリシーに合致しない状態での複合機１０１の運用を行ってしまうことで、セキュリティの脅威にさらされてしまうというリスクがある。

【０１５４】

そこで本実施形態では、管理者に対して拡張アプリケーションを適切な設定値に変更する必要があることを通知する方法について説明する。

【０１５５】

図１９は、情報セキュリティポリシーを認識しない拡張アプリケーションの構成例を示す模式図である。図示の拡張アプリケーションは、図１０に示す拡張アプリケーションから、ポリシー強制処理部１００５とアプリケーション属性情報１００３のポリシーバージョンが省かれている。

【０１５６】

図示の拡張アプリケーションは、ポリシー強制処理部１００５を有しないために、情報セキュリティポリシーが変更されても当該拡張アプリケーションの設定を情報セキュリティポリシーに合致させるように変更することができない。このような拡張アプリケーションを使用する場合は、情報セキュリティポリシーの変更による自動的な設定値の強制ができないため、複合機１０１の管理者に対して、手動による設定値の変更を促す。

【０１５７】

図２０は、本実施形態におけるポリシー変更通知部１１９の動作を説明するためのフローチャートである。図２０のフローチャートは図１２に示すフローチャートに対してステップＳ１７０７が追加されたものであり、この異なる点のみ説明する。

【０１５８】

ステップＳ１７０４において、ポリシー変更通知部１１９は、調査中の拡張アプリケーションのポリシーバージョンを調査する。ポリシーバージョンが設定されていない場合（図１９の場合が該当）、管理者に対して当該アプリケーションは手動による再設定が必要であるとの注意メッセージをＵＩ操作部１０３に表示する（ステップＳ１７０７）。ＵＩ操作部１０３に表示される注意メッセージの一例を図２１に示す。本実施形態では、拡張アプリケーションを識別するために、アプリケーション属性情報１８０３からアプリケーション名とバージョン名の情報を抽出して表示をおこなっている。

【０１５９】

このように、拡張アプリケーションが情報セキュリティポリシーを扱うことができる場合には、上記第１の実施形態のように設定値を情報セキュリティポリシーに合致するように自動的に適用し、扱えない場合には注意メッセージを表示する。これによって管理者に対して最小限の設定見直しを提示することが可能となり、管理者の設定負荷を最小限に抑えることが可能となる。

【０１６０】

［第３の実施形態］

情報セキュリティポリシーの項目は、一般的に一度決めたら不変というわけではなく、複合機の機能の追加やセキュリティ対策等に応じて、項目が追加される可能性がある。ど

の項目に対応しているかは情報セキュリティポリシーのポリシーバージョンで識別される。

【０１６１】

図２２（ａ）はポリシーバージョンがＶ１．００の場合の情報セキュリティポリシー項目の一覧を示す図であり、図２２（ｂ）はポリシーバージョンがＶ１．０１の場合の情報セキュリティポリシー項目の一覧を示す図である。

【０１６２】

図示例では、ポリシーバージョンがＶ１．０１に上がることにより、新たに「パスワードの文字数は８文字以上を使う」という情報セキュリティポリシー項目が増加している。この情報セキュリティポリシーは、文字数の短いパスワードが使用可能であると、容易に他人にわかってしまい、なりすましが可能であるという脅威に対抗することを目的とする項目である。

【０１６３】

このような前提において、追加される可能性のある情報セキュリティポリシーの仕様が予めわからないため、必ずしも拡張アプリケーションが情報セキュリティポリシーのバージョンアップに追随できるわけではない。そのため、複合機１０１が扱う情報セキュリティポリシーのポリシーバージョンと、拡張アプリケーションの扱うことができる情報セキュリティポリシーのポリシーバージョンが異なる場合がある。このとき、新しく追加された情報セキュリティポリシー項目に対して、導入済みの拡張アプリケーションが設定値を強制できないことがある。管理者は、このような拡張アプリケーションの設定値の見直しをする必要性に気付かず、情報セキュリティポリシーに合致しない状態での複合機１０１の運用を行ってしまうおそれがある。本実施形態では、このような場合に、管理者に対して適切な設定値に変更する必要があることを通知する方法について説明する。

【０１６４】

本実施形態では、複合機１０１に図１０に示す拡張アプリケーションを導入しているときに、複合機１０１全体の情報セキュリティポリシーのポリシーバージョンをＶ１．０１に更新するものとする。

【０１６５】

ポリシーバージョンを更新するとともに、当該バージョンに対する情報セキュリティポリシーの設定が行われると、ポリシー変更通知部１１９が呼び出される。

【０１６６】

図２３は、第３の実施形態におけるポリシー変更通知部１１９の動作を説明するためのフローチャートである。図２３のフローチャートは図２０に示すフローチャートに対してステップＳ２３０８，Ｓ２３０９が追加されたものであり、これら異なる点のみ説明する。

【０１６７】

ステップＳ２３０８において、ポリシー変更通知部１１９は、拡張アプリケーションのポリシーバージョン（例えば図１０のＶ１．００）と、複合機１０１のポリシーバージョン（Ｖ１．０１）とを比較する。複合機１０１のバージョンが大きいので、ステップＳ２３０９に進み、複合機１０１のバージョンが大きいので、ステップＳ２３０９に進み、図２４に示す注意メッセージが表示される。

【０１６８】

図２４において、２４０１は拡張アプリケーションの名称を表示し、２４０２は差分となる情報セキュリティポリシー項目を表示している。

【０１６９】

一方、拡張アプリケーションの情報セキュリティポリシーのバージョンと、複合機の情報セキュリティポリシーのバージョンが一致する場合、上記第１の実施形態のように、設定値を情報セキュリティポリシーに合致するように自動的に変更することが可能である。

【０１７０】

両者の情報セキュリティポリシーが一致しない場合には、注意メッセージを表示するよ

うに構成してもよい。これによって管理者に対して最小限の設定見直しを提示することが可能となり、管理者の設定負荷を最小限に抑えることが可能となる。

【０１７１】

［第４の実施形態］

上記実施形態では、拡張アプリケーションが保持しているアプリケーション属性情報にポリシーバージョンが付与されている場合には、当該拡張アプリケーションの情報セキュリティポリシーの対応状況がシステム上で識別できる。

【０１７２】

しかしながら、実際の運用としてアプリケーション属性情報にポリシーバージョンが付与できない場合がある。例えば拡張アプリケーションがすでに市場に広く出回っており、アプリケーション属性情報にポリシーバージョンを保持しない場合である。このような拡張アプリケーションを実際に使用したいという要求がある一方、機器の情報セキュリティポリシーに反するため、無条件には許可することはできない。

【０１７３】

ここで、拡張アプリケーションが機器の情報セキュリティポリシーに対応せずに問題となる場合について説明する。

【０１７４】

アプリケーションＡは、ＦＴＰで印刷ジョブを受けつける独自のサーバ機能を持ち、受信した印刷ジョブを機器において印刷する機能を有するものとする。ＡによるＦＴＰポートは、図７（ａ）のユーザーモード設定と無関係に動作する場合、第１の実施形態で説明した情報セキュリティポリシー（ファイルの送信方式＝暗号化通信ならＯＫ）による設定変更を行っても、Ａの動作には影響せず、ＦＴＰ動作を続ける。本来、このような場合、アプリケーションＡは情報セキュリティポリシーの変更を検知して、それに従うようにＦＴＰポートを閉じる必要がある。

【０１７５】

しかしながら、アプリケーションＡが情報セキュリティポリシーに対応していないため、機器全体ではアプリケーションＡによるＦＴＰポートが空いた状態が継続する。一般的にネットワーク機器に対しては、ポートスキャンという解析手法を用いることにより、当該機器で空いているポート番号が明確に判断できる。この手法により、当該機器は、情報セキュリティポリシー（ファイルの送信方式＝暗号化通信ならＯＫ）に反してＦＴＰ動作を許可していることを解析可能であり、運用上の問題が露呈する。

【０１７６】

次に、拡張アプリケーションが機器の情報セキュリティポリシーに対応しなくても問題がない場合について説明する。

【０１７７】

アプリケーションＢは、機器にたまった印刷データを印刷指示する機能を持つものとする。このアプリケーションＢは、ネットワークを使った受信処理には関与せず、セキュリティポリシー（ファイルの送信方式＝暗号化通信ならＯＫ）には影響を受けない。アプリケーションＢの場合は、セキュリティポリシーがどのような設定になっていたとしても動作には影響せず、かつセキュリティポリシーを外れないことが分かる。

【０１７８】

機器はアプリケーションＡ，Ｂについて、アプリケーション属性情報１００３に情報セキュリティポリシーに関する情報がないため、どのアプリケーションを動作させていいかの判断がシステム上できない。そのため、第１の実施形態では、図２３のステップＳ２３０７において手動による再設定が必要であることを警告表示している。

【０１７９】

本実施形態では、上述したアプリケーションの特徴を管理者が判断し、組織で使用してもセキュリティポリシーとして問題ないアプリケーションＢの警告表示を行わないようにさせる方法について説明する。

【０１８０】

図２５は、第４の実施形態におけるセキュリティポリシーデータの一例を示す図である。

【０１８１】

図２５に示すセキュリティポリシーデータは、図１７に示すセキュリティポリシーデータに対して、２６０１の枠内に記載された部分が追加されたものである。＜ポリシー除外アプリＩＤ＞というタグの中には、除外すべきアプリケーション識別子のリストが記載されている。図示例では、「ａｂｃ１２３４５６７」と「ｘｙｚ２３４５６８」という２つのアプリケーション識別子を除外としている。このように、情報セキュリティポリシーの適用有無にかかわらず動作が可能な拡張アプリケーションの識別子のリストをホワイトリストと呼ぶ。ポリシー変更通知部１１９は、セキュリティポリシーデータから、このホワイトリストを抽出して格納する。

【０１８２】

セキュリティポリシーデータは、当該組織の情報セキュリティポリシーを決める権限が持つ人が記述するものであり、その権限において使用を許可するアプリケーションを事前にホワイトリストに指定することが可能である。

【０１８３】

次に、セキュリティポリシーデータに、除外するアプリケーション識別子が記載されている場合のポリシー変更通知部の動作について説明する。

【０１８４】

図２６は、第４の実施形態におけるポリシー変更通知部１１９の動作を説明するためのフローチャートである。図２６のフローチャートは図２３のフローチャートに対してステップＳ２５１０，Ｓ２５１１が追加されたものであり、これら異なる点のみ説明する。

【０１８５】

ステップＳ２５１０では、ポリシー変更通知部１１９は、拡張アプリケーションがホワイトリストに登録されているか調査する。つづいて、ホワイトリストに登録されている場合には、特に警告表示等を行わずにステップＳ２５０６に進む。一方、ホワイトリストに登録されていない場合にはステップＳ２５０７に進み、拡張アプリケーションの手動による再設定が必要である旨の警告表示が行われる。このような処理を設けることによって、管理者がホワイトリストに予め登録した拡張アプリケーションに関しては、特に警告を表示することなく利用することが可能である。

【０１８６】

さらに拡張アプリケーションが情報セキュリティポリシーに応じて、動作可能かを利用者に知らせるためのＧＵＩを設けてもよい。

【０１８７】

図２７は、拡張アプリケーションの情報がＵＩ操作部１０３に表示されたＵＩ画面の一例を示す図である。

【０１８８】

拡張アプリケーションの情報は、ポリシー変更通知部１１９が、登録された各拡張アプリケーションの確認をする過程において、拡張アプリケーション管理部１１８に保存される。

【０１８９】

図２７において、２７０１は画面全体を示し、２７０２はアプリケーションに関する情報である。ここでは「アプリケーション名」は「印刷アプリケーション」であり、「製品バージョン」が「１．０．１」であることを示す。これらの情報は、図１０に示したアプリケーション属性情報１００３に記載されたアプリケーション名とバージョンに記載された情報である。

【０１９０】

２７０３は情報セキュリティポリシー対応に関する情報である。「ポリシー対応」の項目は、図２６のステップＳ２５０４の判定結果から「なし」であることを示す。「ホワイトリスト対応」の項目は、図２６のステップＳ２５１０で調査した結果であり、「あり」

が表示されている。

【０１９１】

「ポリシーによる制限」は、図２６のステップＳ２５０７において拡張アプリケーションがセキュリティポリシーによる制限（警告が表示される）と判定された場合には「あり」となり、そうでない場合は「なし」となる。図２７ではホワイトリストに記載されているため、制限が「なし」と判定される。このように拡張アプリケーションの情報セキュリティポリシーに関する情報を表示することによって、利用者にとって当該拡張アプリケーションが利用可能かどうかを判断することが可能となる。

【０１９２】

第４の実施形態によれば、複合機１０１では、外部のＰＣ２０１から配信されたセキュリティポリシーデータから、情報セキュリティポリシーの適用が除外される拡張アプリケーションの識別子を抽出する。そして、複合機１０１内の拡張アプリケーションの識別子に、上記抽出した拡張アプリケーションの識別子と一致するものがなく、且つ複合機１０１内の拡張アプリケーションが、セキュリティポリシーデータに記述された情報セキュリティポリシーを満たさない場合は、拡張アプリケーションの情報セキュリティポリシーの再設定が必要であることを管理者に通知する。これにより、機器内の拡張アプリケーションの情報セキュリティポリシーが機器のセキュリティポリシーに対応していなくとも、管理者が判断して当該拡張アプリケーションの利用が可能となり、機器における情報セキュリティポリシーの管理が容易になる。

【０１９３】

［第５の実施形態］

上記第２～第４の実施形態では、拡張アプリケーションが情報セキュリティポリシーに違反する可能性がある場合、当該アプリケーションは手動による再設定が必要である旨のメッセージを表示する構成である（ステップＳ１７０７，Ｓ２５０７）。そこで、より情報セキュリティポリシーによる強制力を増すために、設定の見直しではなく、動作を停止するようにしてもよい。

【０１９４】

図２８は、第５の実施形態における複合機１０１と拡張アプリケーション間で情報のやり取りや指示を行うＡＰＩの動作を説明するための図である。なお、図２８は、図１１に対して、ＡＰＩである２８０７が追加されたものであり、他の構成については説明を省略する。

【０１９５】

図２８において、２８０７は拡張アプリケーションが情報セキュリティポリシーを守れないと判断されたときに、当該拡張アプリケーションに対して停止を指示するＡＰＩである。このＡＰＩ２８０７は、拡張アプリケーションが動作時あるいは複合機１０１が起動するタイミングで拡張アプリケーションに通知を行う。その結果、当該拡張アプリケーションは停止処理を行い、以降当該拡張アプリケーションが提供するサービスを停止する。

【０１９６】

図２９は、第５の実施形態におけるポリシー変更通知部１１９の動作を説明するためのフローチャートである。図２９のフローチャートは図２６のフローチャートに対してステップＳ２９０７が異なるのみである。

【０１９７】

図２６のステップＳ２５０７では、管理者に拡張アプリケーションの設定を見直すよう促す表示が行われていたが、図２９のステップＳ２９０７では、拡張アプリケーションに対する停止指示として、ステップＳ２８０７に相当するＡＰＩをコールする。

【０１９８】

このように、情報セキュリティポリシーに応じて拡張アプリケーションの動作を停止させることにより、厳格に情報セキュリティポリシーを維持することも可能である。

【０１９９】

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

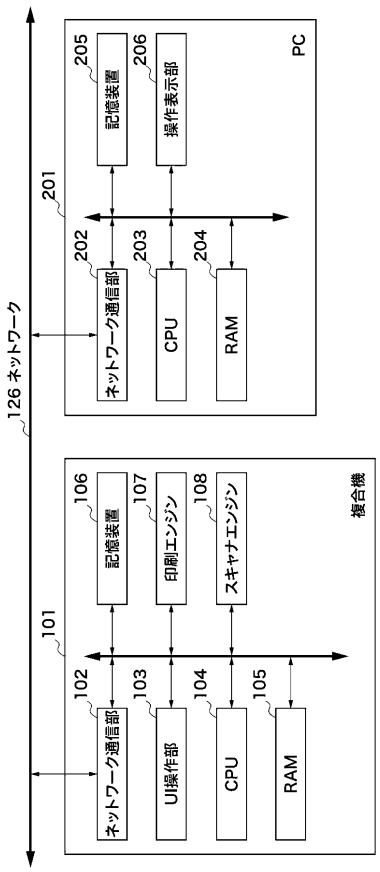
の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

【符号の説明】

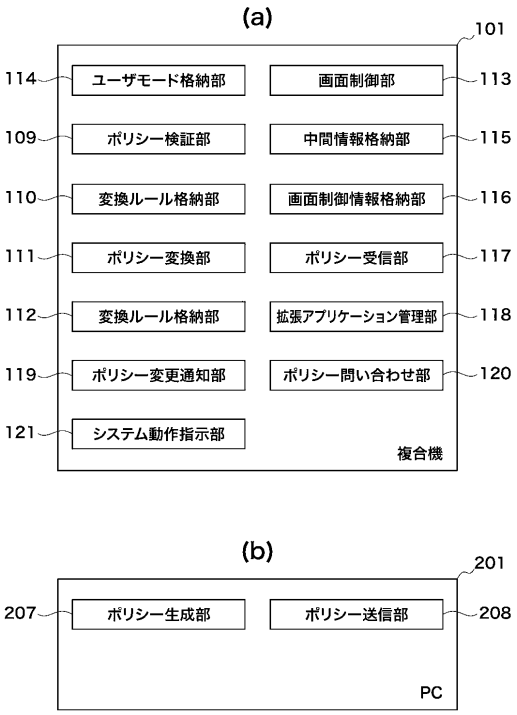
【０２００】

１０１　複合機
１０９　ポリシー検証部
１１２　ポリシー変換部
１１３　画面制御部
１１７　ポリシー受信部
１２１　ポリシー生成部
１２４　ポリシー送信部
２０１　ＰＣ

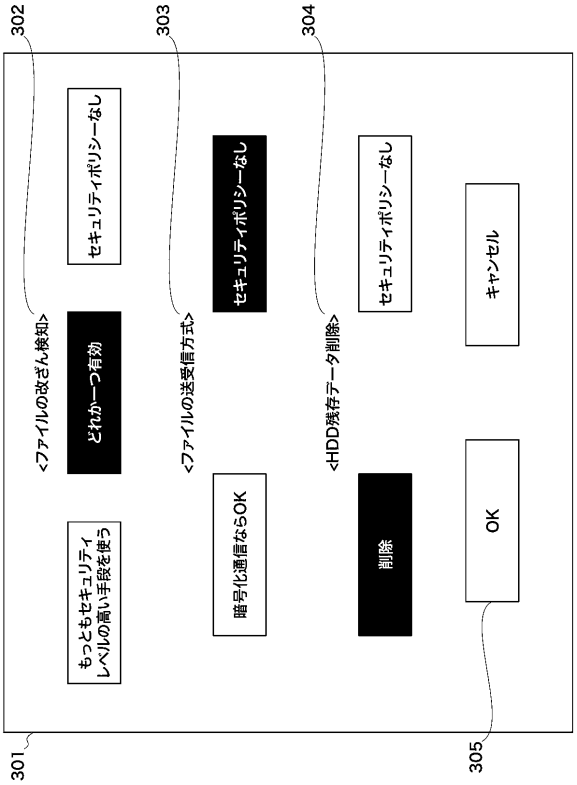
【図１】



【図２】



【図３】



【図４】

(a)

情報セキュリティポリシーの名称 (402)	情報セキュリティポリシーの値 (403)
ファイルの改ざん検知	どれか一つ有効
ファイルの送受信方式	セキュリティポリシーなし
HDDの残存データ削除	削除

(401)

(b)

(501)

	情報セキュリティポリシーの名称	対応するユーザモードの名称
ルール部 (502)	ファイルの改ざん検知	強制デジタル署名付きPDF
		強制ハッシュ付きPDF
	ファイルの送受信方式	FTP
		SFTP

(501)

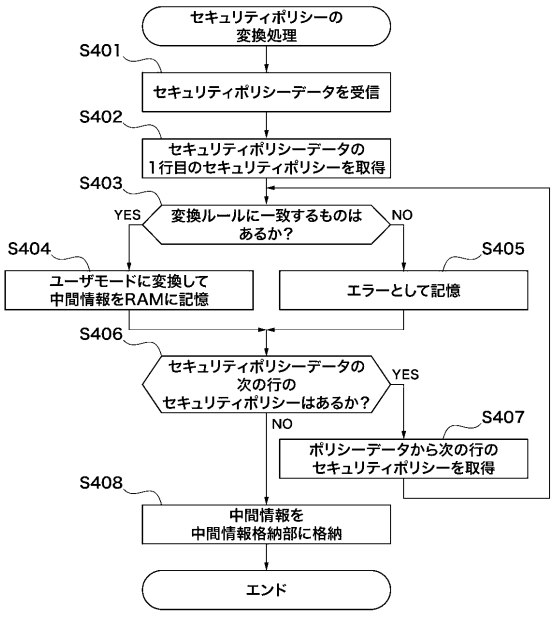
	情報セキュリティポリシーの名称	設定可能なセキュリティポリシーの値	情報セキュリティポリシーに従っているか判定するための条件
条件部 (503)	ファイルの改ざん検知	もっともセキュリティレベルの高い手段を使う	強制デジタル署名付きPDF:ON
		どれか一つ有効	強制デジタル署名付きPDF:ON もしくは 強制ハッシュ付きPDF:ON
		セキュリティポリシーなし	なし
	ファイルの送受信方式	暗号化通信ならOK	FTP:OFF かつ SFTP:ON
		セキュリティポリシーなし	なし

(c)

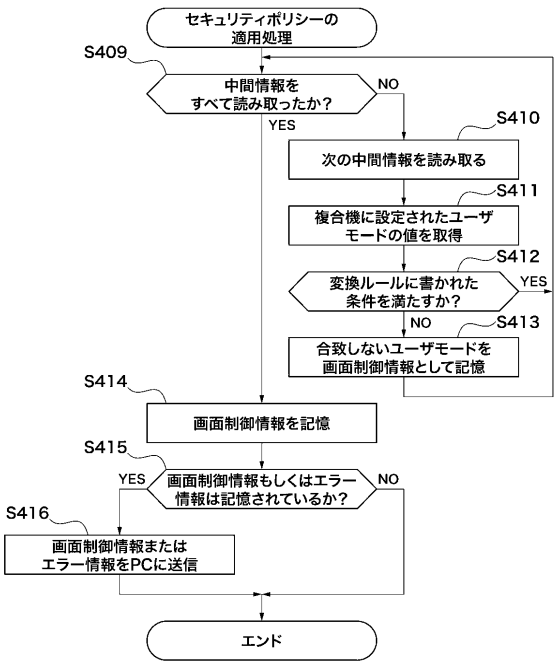
(601)

強制デジタル署名付きPDF	どれか一つ有効
強制ハッシュ付きPDF	
FTP	セキュリティポリシーなし
SFTP	

【図５】



【図６】



【図７】

(a)

701

強制デジタル署名付きPDF	OFF
強制ハッシュ付きPDF	OFF
FTP	ON
SFTP	ON

(b)

801

強制デジタル署名付きPDF	どれか一つ有効	強制デジタル署名付きPDF:ON もしくは 強制ハッシュ付きPDF:ON
強制ハッシュ付きPDF		

【図８】

(a)

<エラー!>
以下のセキュリティポリシーは
設定できませんでした。
・HDD残存データ削除

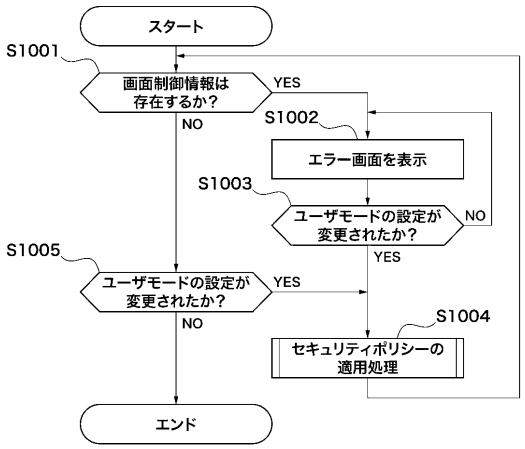
<注意!>
セキュリティポリシーに違反しています。
以下の設定を見直してください。
・強制デジタル署名付きPDF
・強制ハッシュ付きPDF

(b)

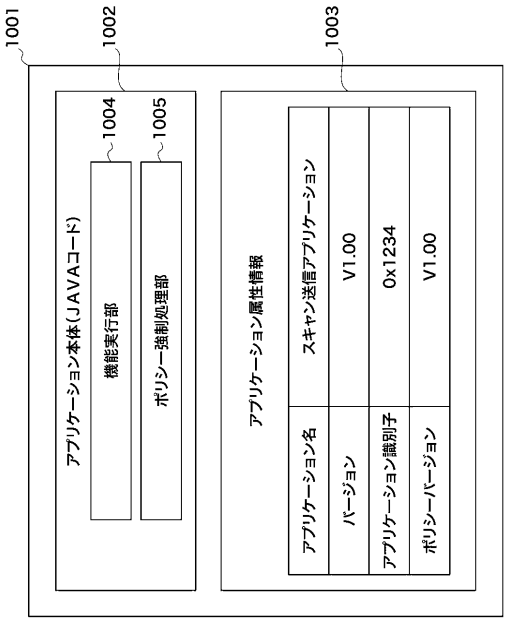
<注意!>
セキュリティポリシーに違反しているため、
デバイスを利用できません。

以下の設定を見直してください。
・強制デジタル署名付きPDF
・強制ハッシュ付きPDF

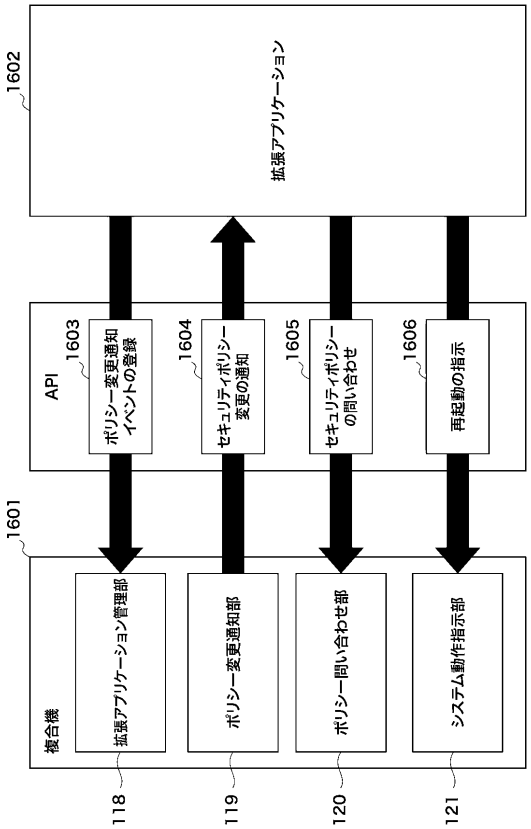
【図９】



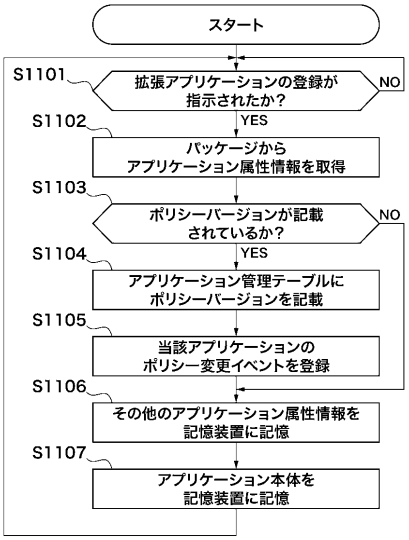
【図１０】



【図１１】



【図１２】

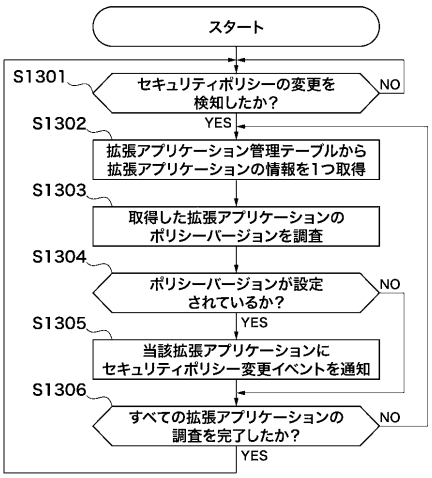


【図１３】

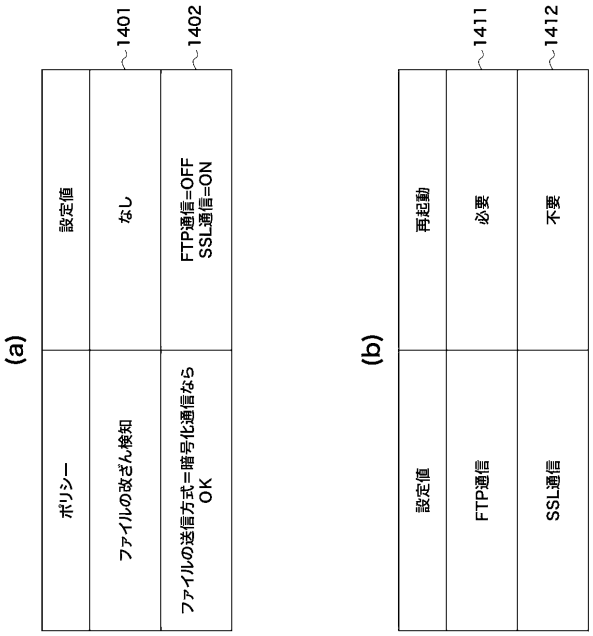
1200

1204 アプリケーション名	1205 バージョン	1206 アプリケーション識別子	1207 ポリシーバージョン
	1201	1202	1203
スキャン送信アプリケーション	V1.00	0x1234	V1.00
ICカード認証アプリケーション	V1.05	0x1256	V2.00
パーソナルセキュアプリント	V1.00	0x1278	-

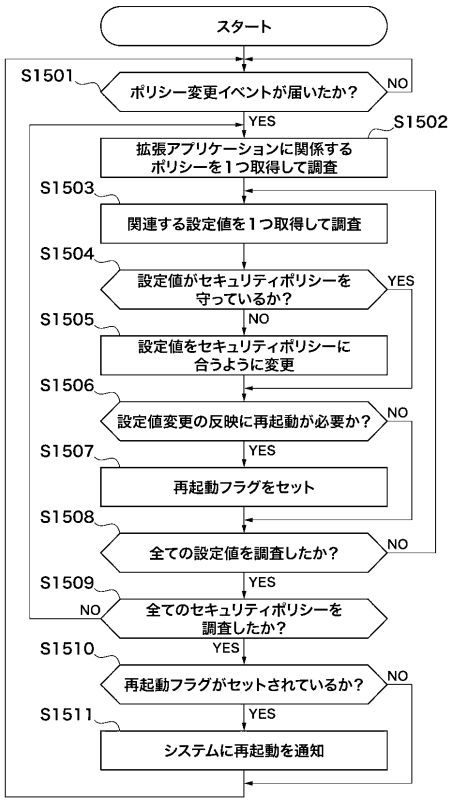
【図１４】



【図１５】



【図１６】



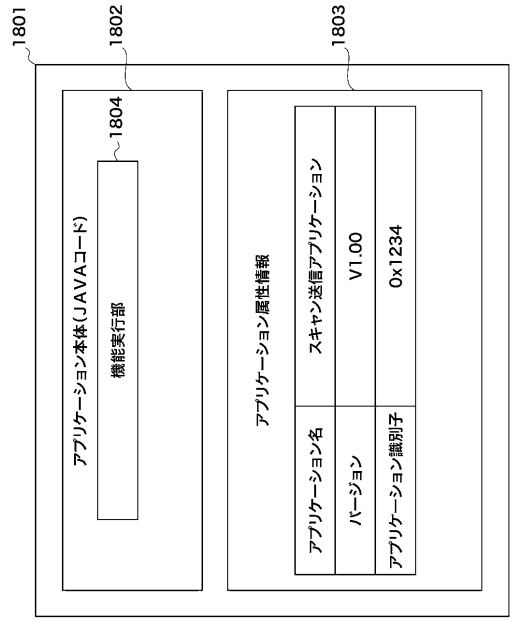
【図１７】

```
<?xml version="1.0" encoding="UTF-8"?>
- <セキュリティポリシー>
    <ファイルの改ざん検知 value="どれか一つ有効"/>
    <ファイルの送受信方式 value="セキュリティポリシーなし"/>
    <HDD残存データ削除 value="削除"/>
  </セキュリティポリシー>
```

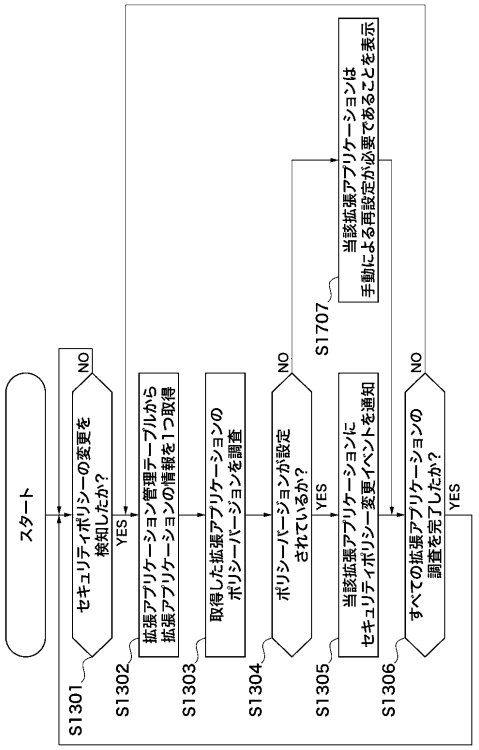
【図１８】

```
<?xml version="1.0"?>
- <ポリシー変換ルール>
  - <ファイルの改ざん検知>
    - <対応ユーザモード>
        <強制デジタル署名付きPDF/>
        <強制ハッシュ付きPDF/>
      </対応ユーザモード>
    - <ルール>
      - <もっともセキュリティレベルの高い手段を使う>
          <条件>強制デジタル署名==ON</条件>
        </もっともセキュリティレベルの高い手段を使う>
      - <どれか一つ有効>
          <条件>(強制デジタル署名==ON)||(強制ハッシュ付きPDF==ON)</条件>
        </どれか一つ有効>
      - <セキュリティポリシーなし>
          <条件/>
        <セキュリティポリシーなし>
      </ルール>
    </ファイルの改ざん検知>
  - <ファイルの送受信方式>
    - <対応ユーザモード>
        <ftp/>
        <SFTP/>
      </対応ユーザモード>
    - <ルール>
      - <暗号化通信ならOK>
          <条件>(ftp==OFF)&&(STFP==ON)</条件>
        </暗号化通信ならOK>
      - <セキュリティポリシーなし>
          <条件/>
        <セキュリティポリシーなし>
      </ルール>
    </ファイルの送受信方式>
  <ポリシー変換ルール>
```

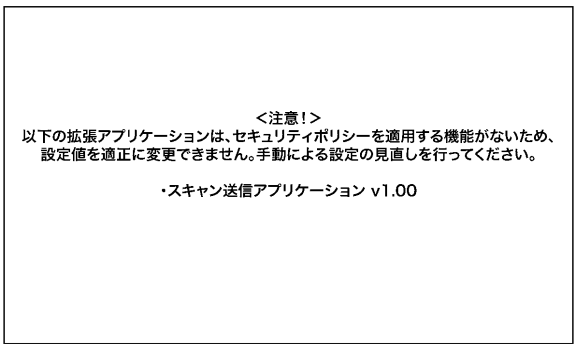
【図１９】



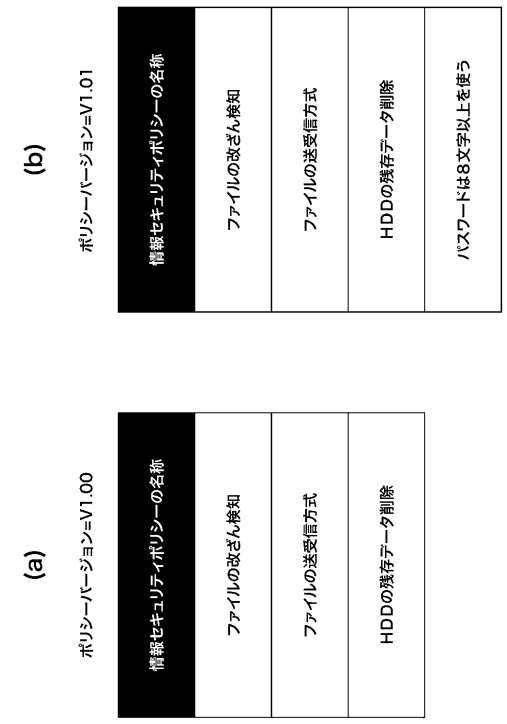
【図２０】



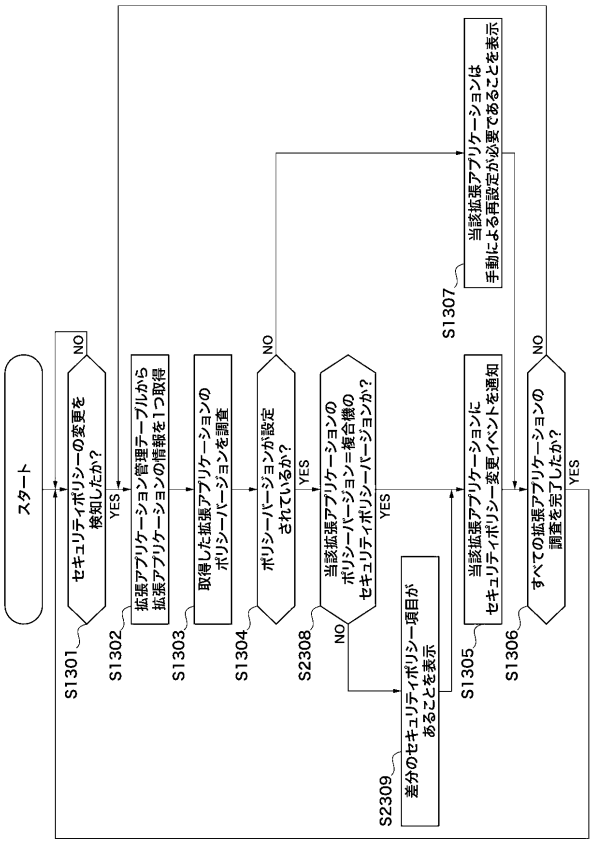
【図２１】



【図２２】



【図２３】



【図２４】

<注意!>
以下の拡張アプリケーションは、セキュリティポリシーのバージョンが異なるため、
一部のセキュリティポリシーの設定が反映されていない可能性があります。
手動による設定の見直しを行ってください。

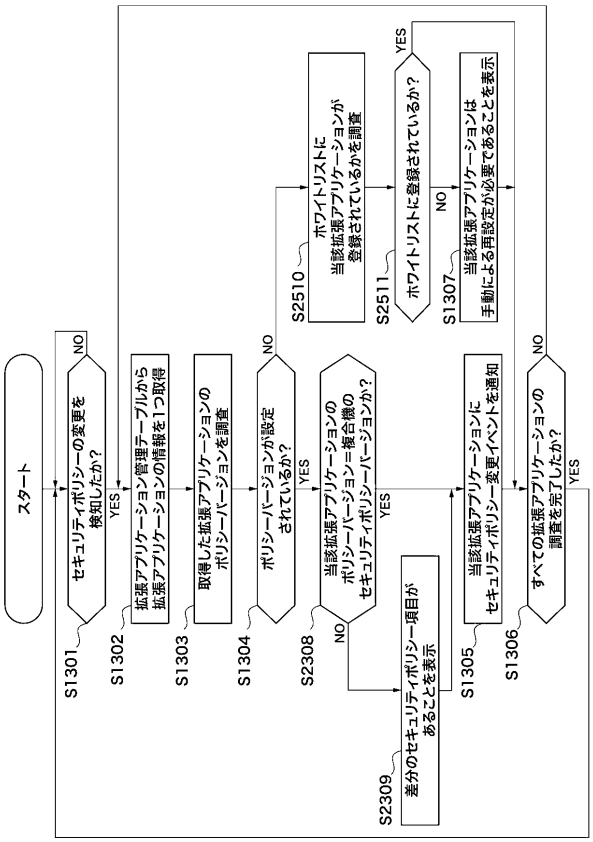
・スキャン送信アプリケーション v1.00 2401

セキュリティポリシー項目
「パスワードの文字数に8文字以上を使う」 2402

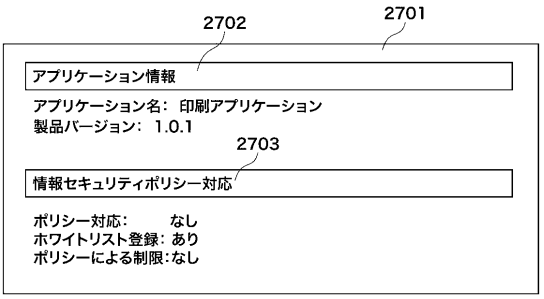
【図２５】

```
<?xml version="1.0" encoding="UTF-8"?>
- <セキュリティポリシー>
    <ファイルの改ざん検知 value="どれか一つ有効"/>
    <ファイルの送受信方式 value="暗号化通信のみ許可"/>
    <HDD残存データ削除 value="削除"/>
    <ポリシー除外アプリID>
      abc1234567,
      xyz2345678,
    </ポリシー除外アプリID>          2601
  </セキュリティポリシー>
```

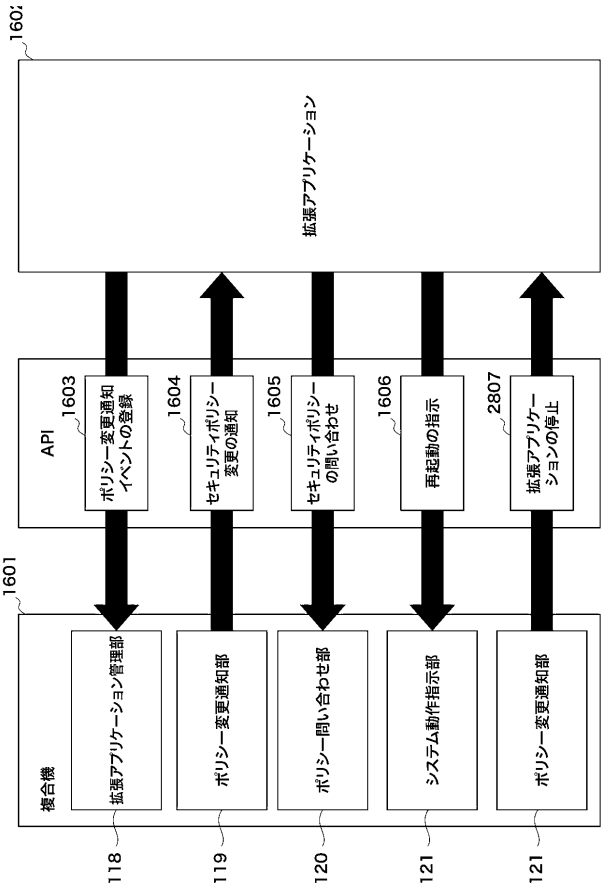
【図２６】



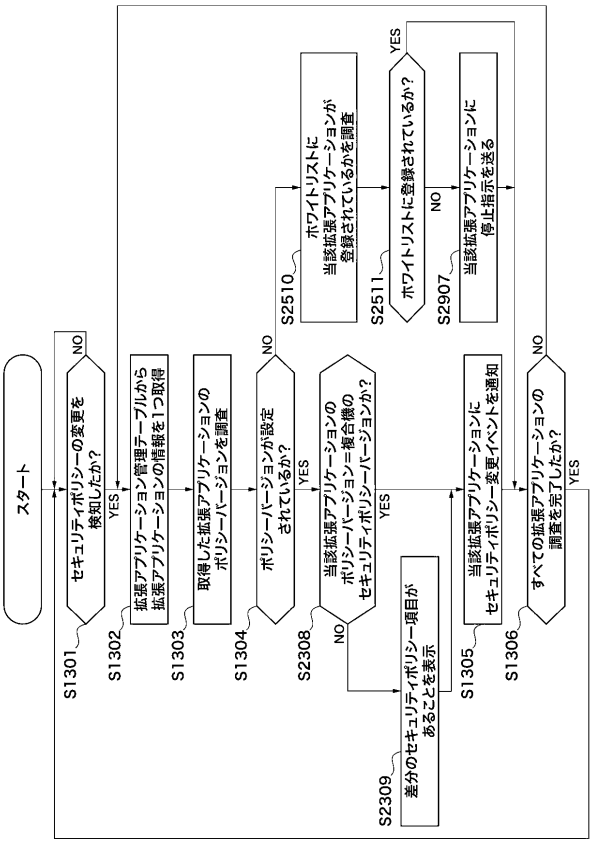
【図２７】



【図２８】


1602
拡張アプリケーション
API
1603
ポリシー変更通知イベントの登録
1604
セキュリティポリシー変更の通知
1605
セキュリティポリシーの問い合わせ
1606
再起動の指示
2807
拡張アプリケーションの停止
1601
複合機
拡張アプリケーション管理部
ポリシー変更通知部
ポリシー問い合わせ部
システム動作指示部
ポリシー変更通知部
118
119
120
121
121

【図２９】


スタート
セキュリティポリシーの変更を検知したか？
NO
YES
S1301
拡張アプリケーション管理テーブルから拡張アプリケーションの情報を1つ取得
S1302
取得した拡張アプリケーションのポリシーバージョンを調査
S1303
ポリシーバージョンが設定されているか？
NO
YES
S1304
当該拡張アプリケーションのポリシーバージョン＝複合機のセキュリティポリシーバージョンか？
NO
YES
S2308
差分のセキュリティポリシー項目があることを表示
S2309
当該拡張アプリケーションにセキュリティポリシー変更イベントを通知
S1305
すべての拡張アプリケーションの調査を完了したか？
NO
YES
S1306
ホワイトリストに当該拡張アプリケーションが登録されているかを調査
S2510
ホワイトリストに登録されているか？
YES
NO
S2511
当該拡張アプリケーションに停止指示を送る
S2907

フロントページの続き

審査官　岸野　徹

(56)参考文献　特開２０１１－１２３８４１（ＪＰ，Ａ）
特開２００９－０１５５８５（ＪＰ，Ａ）
特開２００７－３２８７７０（ＪＰ，Ａ）
特開２００７－０４８０７９（ＪＰ，Ａ）
特開２０１０－２８２４７９（ＪＰ，Ａ）
特開２０１０－１０８２６０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／６０