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

特許第6124531号
(P6124531)

(45)発行日　平成29年5月10日(2017.5.10)　(24)登録日　平成29年4月14日(2017.4.14)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| G06F 21/62 | (2013.01) | G06F | 21/62 | |
| B41J 29/00 | (2006.01) | B41J | 29/00 | Z |
| G06F 3/12 | (2006.01) | G06F | 3/12 | 338 |

請求項の数 12　(全 27 頁)

(21)出願番号　特願2012-173941(P2012-173941)
(22)出願日　平成24年8月6日(2012.8.6)
(65)公開番号　特開2014-32595(P2014-32595A)
(43)公開日　平成26年2月20日(2014.2.20)
審査請求日　平成27年8月5日(2015.8.5)

(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　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

審査官　児玉　崇晶

最終頁に続く

(54)【発明の名称】情報処理システム、画像処理装置及びその制御方法、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、
１又は複数の画像処理装置の運用方針を示す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ポリシー生成手段と、
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ポリシー送信手段とを備え、
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ポリシー受信手段と、
前記情報セキュリティポリシーと前記画像処理装置の動作に関する設定との対応関係を定義した情報を記憶する記憶手段と、
前記記憶手段に記憶された前記情報に基づいて、前記ポリシー受信手段で受信したセキュリティポリシーデータに記述された前記情報セキュリティポリシーを、前記情報セキュリティポリシーに対応する前記画像処理装置の動作に関する設定に変換するポリシー変換手段と、
前記ポリシー変換手段によって変換された設定と当該画像処理装置の現在の設定とを比較する比較手段と、
前記比較手段による比較結果に基づいて、前記画像処理装置の現在の設定を変更するように通知する通知手段と、

を備えることを特徴とする情報処理システム。
【請求項２】
画像処理装置であって、
１又は複数の画像処理装置の運用方針を示す情報セキュリティポリシーを示すセキュリティポリシーデータであって、一の設定項目に対応し尚且つ前記情報セキュリティポリシーに従う複数の設定候補に対応するセキュリティポリシーデータをネットワークを介して外部装置から受信する受信手段と、
１又は複数の画像処理装置の運用方針を示す情報セキュリティポリシーと前記画像処理装置の動作に関する設定との対応関係を定義した情報を記憶する第１の記憶手段と、
前記第１の記憶手段に記憶された前記情報と前記受信手段が受信したセキュリティポリシーデータに基づいて、前記受信手段で受信したセキュリティポリシーデータが示す前記情報セキュリティポリシーに対応する設定を、前記複数の設定候補の範囲内で設定する設定手段と、
前記設定手段により設定した設定を記憶する第２の記憶手段と、
を備えることを特徴とする画像処理装置。
【請求項３】
前記設定手段により設定した設定を前記画像処理装置に設定する設定手段、
を更に備えることを特徴とする請求項２に記載の画像処理装置。
【請求項４】
前記第１の記憶手段は、１つの種類の情報セキュリティポリシーに対して、前記画像処理装置の動作に関する設定を複数対応付けて記憶することが可能であり、
前記設定手段は、前記受信手段で受信したセキュリティポリシーデータに記述された１つの種類の情報セキュリティポリシーに基づいて、前記画像処理装置の動作に関する複数の設定に変換可能であることを特徴とする請求項２又は３に記載の画像処理装置。
【請求項５】
前記画像処理装置の動作に関する設定の変更を受け付ける受付手段と、
前記受付手段によって、前記情報セキュリティポリシーに対応する設定が前記情報セキュリティポリシーを満たさない状態に変更されることを制限する制限手段と、
を更に備えることを特徴とする請求項２乃至４のいずれか１項に記載の画像処理装置。
【請求項６】
前記受信手段で受信したセキュリティポリシーデータに記述された前記情報セキュリティポリシーの種類が通信経路のセキュリティに関連する情報セキュリティポリシーである場合、前記設定手段は、前記第１の記憶手段に記憶された前記情報に基づいて、前記画像処理装置の通信経路の暗号化に関する設定を設定することを特徴とする請求項２乃至５のいずれか１項に記載の画像処理装置。
【請求項７】
前記セキュリティポリシーデータに含まれる前記情報セキュリティポリシーは、前記情報セキュリティポリシーの種類と当該情報セキュリティーポリシーの設定値を含み、
前記設定手段は、前記情報セキュリティポリシーの種類と前記第１の記憶手段に記憶された前記情報に基づいて、前記情報セキュリティポリシーに対応する前記画像処理装置の動作に関する設定項目を設定し、且つ、当該情報セキュリティポリシーの設定値と前記第１の記憶手段に記憶された前記情報に基づいて、前記設定した設定項目に対応する設定値を設定することを特徴とする請求項２乃至６のいずれか１項に記載の画像処理装置。
【請求項８】
前記セキュリティポリシーデータに含まれる少なくとも１つの情報セキュリティポリシーの種類は、ファイルの改ざん検知であり、前記ファイルの改ざん検知に対応する前記画像処理装置の動作に関する設定は、強制デジタル署名付きＰＤＦの設定、及び、強制ハッシュ付きＰＤＦの設定であることを特徴とする請求項７に記載の画像処理装置。
【請求項９】
前記セキュリティポリシーデータに含まれる少なくとも１つの情報セキュリティポリシ

ーの種類は、ファイルの送受信方式であり、前記ファイルの送受信方式に対応する前記画像処理装置の動作に関する設定は、ＦＴＰの設定、及び、ＳＦＴＰの設定であることを特徴とする請求項７又は８に記載の画像処理装置。
【請求項１０】
請求項２乃至７のいずれか１項に記載の画像処理装置と、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ポリシー生成手段と、
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、
を備えることを特徴とする情報処理システム。
【請求項１１】
１又は複数の画像処理装置の運用方針を示す情報セキュリティポリシーと前記画像処理装置の動作に関する設定との対応関係を定義した情報を記憶する第１の記憶部を有する画像処理装置の制御方法であって、
外部装置から、前記情報セキュリティポリシーを示すセキュリティポリシーデータであって、一の設定項目に対応し尚且つ前記情報セキュリティポリシーに従う複数の設定候補に対応するセキュリティポリシーデータを受信する受信工程と、
前記第１の記憶部に記憶された前記情報と前記受信手段が受信したセキュリティポリシーデータに基づいて、前記受信工程で受信したセキュリティポリシーデータが示す前記情報セキュリティポリシーに対応する設定を、前記複数の設定候補の範囲内で設定する設定工程と、
前記設定工程で設定した設定を第２の記憶部に記憶する記憶工程と、
を備えることを特徴とする画像処理装置の制御方法。
【請求項１２】
請求項１１に記載の画像処理装置の制御方法をコンピュータに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、情報処理システム、画像処理装置及びその制御方法、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、画像データを格納し、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布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ない。そのため、管理者は複合機毎に数多くの動作設定（以下、「ユーザモード」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ことから、管理者に多大な労力がかかる。例えば、通信経路の暗号化を行うユーザモードの設定値としては、Ａ社の複合機では「ＳＳＬを使用する」となり、Ｂ社の複合機では「ＨＴＴＰ通信を暗号化する」となっている。そのため、従来は統一的な情報セキュリティポリシーに従わせることができず、管理者が各社の複合機のユーザモード設定を熟知した上で１台ずつ情報セキュリティポリシーに従った状態に設定する作業を行っている。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】
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）。管理者がＰＣ上の設定画面にて表示される質問に対して、情報セキュリティポリシーに従った回答を行う。回答を受けたシステムは、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布先の複合機に依存したユーザモードに変換する。このユーザモードを配信することで、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システムである。
【先行技術文献】
【特許文献】
【０００８】
【特許文献１】特開２００８－２１９４１９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００９】
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という情報セキュリティポリシーがあったときに、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とする。このとき、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布すると、ユーザは「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、ユーザが管理者に情報セキュリティポリシーに従ったユーザモードの再配信を要請する必要があり、利便性に欠ける。
【００１０】
本発明は、上記問題に鑑みて成されたものであり、情報セキュリティポリシーに従った状態を維持しつつ、ユーザモードの変更が可能となる情報処理システム、画像処理装置及びその制御方法、並びに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】
【００１１】
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

、１又は複数の画像処理装置の運用方針を示す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ポリシー生成手段と、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ポリシー送信手段とを備え、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ポリシー受信手段と、前記情報セキュリティポリシーと前記画像処理装置の動作に関する設定との対応関係を定義した情報を記憶する記憶手段と、前記記憶手段に記憶された前記情報に基づいて、前記ポリシー受信手段で受信したセキュリティポリシーデータに記述された前記情報セキュリティポリシーを、前記情報セキュリティポリシーに対応する前記画像処理装置の動作に関する設定に変換するポリシー変換手段と、前記ポリシー変換手段によって変換された設定と当該画像処理装置の現在の設定とを比較する比較手段と、前記比較手段による比較結果に基づいて、前記画像処理装置の現在の設定を変更するように通知する通知手段と、を備えることを特徴とする。

【発明の効果】

【００１２】

本発明によれば、情報セキュリティポリシーに従うように画像処理装置の設定変更を行うことができ、情報セキュリティポリシーに従った状態を維持しながらユーザモードの変更が可能となる。

【図面の簡単な説明】

【００１３】

【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の入力部に表示されたポリシー設定画面の一例を示す図である。

【図４】（ａ）ＰＣの記憶装置に保存されたセキュリティポリシーデータの一例を示す図、（ｂ）複合機の変換ルール格納部に格納される変換ルールファイルの一例を示す図、（ｃ）複合機のＲＡＭに記憶された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）複合機のユーザモード格納部に格納されるユーザモードの名称と値の一例を示す図、（ｂ）複合機のＲＡＭに記憶された画面制御情報の一例を示す図である。

【図８】（ａ）ＰＣ１２５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）画面制御部１１３が表示する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処理の流れを示すフローチャートである。

【図１０】第２の実施形態における、ユーザモード設定時の情報セキュリティポリシー違反防止処理の流れを示すフローチャートである。

【図１１】（ａ）複合機のＵＩ操作部に表示されたユーザモードの設定画面の一例を示す図、（ｂ）情報セキュリティポリシーに違反する項目を設定変更できないようにしたユーザモードの設定画面の一例を示す図である。

【図１２】（ａ）図１１（ｂ）に示す画面上で「強制ハッシュ付きＰＤＦ」が「ＯＮ」にされた画面、（ｂ）生成したユーザモードの設定画面の一例を示す図である。

【図１３】第３の実施形態における画像処理装置のハードウェア構成の概略を示す図である。

【図１４】図１３の複合機１４５０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１５】（ａ）図１３の複合機１４０１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）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１６】ＰＣの変換ルール格納部に格納される複合機種別と変換ルールファイルの組の一例を示す図である。
【図１７】ＰＣのユーザモード生成部により実行される処理の流れを示すフローチャートである。
【図１８】第４の実施形態における画像処理装置の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１９】複合機のポリシー適用判定部により実行されるセキュリティポリシー判定処理の流れを示すフローチャートである。
【図２０】図４（ａ）のセキュリティポリシーデータのＸＭＬ記述例を示す図である。
【図２１】図４（ｂ）のポリシー変換ファイルのＸＭＬ記述例を示す図である。
【発明を実施するための形態】
【００１４】
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。
【００１５】
［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。
【００１６】
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）１０２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。
【００１７】
まず、複合機１０１について説明する。
【００１８】
１０２はネットワーク１２６を介して外部機器（例えばＰＣ１２５）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、ユーザからの操作を可能とするＵＩ操作部である。１０５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ＣＰＵ１０５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保存するＲＡＭである。１０７はプログラムコードや画像データ等を保存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。
【００１９】
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、ＣＰＵ１０５がＲＡＭ１０６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１１４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１２２に取り込まれ、必要な画像処理を加えて印刷エンジン１０８によって出力される。
【００２０】
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、ＣＰＵ１０５はＲＡＭ１０６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１１４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１２２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。
【００２１】

次に、ＰＣ１２５について説明する。

【００２２】

１１８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。１１９は各種制御を実行するＣＰＵである。１２０はＣＰＵ１０５が実行するプログラムコードなどの情報を一時的に保存するＲＡＭである。１２２はプログラムコードやデータを保存する記憶装置である。１２３は管理者によるＰＣ１２５への入力を受け付ける入力部である。入力部１２３は、操作手段及び表示手段として機能する。

【００２３】

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ＰＣ１２５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。

【００２４】

図２（ａ）において、１０４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、「ユーザモード」と呼ぶ）の名称と値を格納するユーザモード格納部である。例えば「強制デジタル署名付きＰＤＦ」や「強制ハッシュ付きＰＤＦ」がユーザモード設定項目の一例である。

【００２５】

「強制デジタル署名付きＰＤＦ」とは、次の通りである。すなわち、複合機が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し、そのハッシュ値をファイル作成者の秘密鍵で暗号化して得られた電子署名をファイルに付加して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。

【００２６】

なお、「強制デジタル署名付きＰＤＦ」のユーザ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。また「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。

【００２７】

また、「ｆｔｐ」や「ＳＦＴＰ」などもユーザ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。また、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」のユーザモード設定項目を有効にした場合、記憶装置１０７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。

【００２８】

なお、ユーザモードの名称と値等は記憶装置１０７等に格納される。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１０７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１０７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。

【００２９】

１１２はポリシー変換手段であるところの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。

【００３０】
１０９はポリシー判定手段であるところの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モード格納部１０４に格納されたユーザ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。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。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１０７等に格納される。
【００３１】
さらに、ポリシー検証部１０９は、上記の検証に加えて、複合機１０１の各アプリケーションの動作制御をも行う。複合機１０１には、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（機能実行部１５０）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（機能実行部１５０）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。
【００３２】
なお、図２には図示していないが、複合機１０１は、スキャナエンジン１１４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。更に、複合機１０１は、ＰＣ１２５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、画像データを記憶装置１０７に蓄積するＢＯＸモジュールや、ＨＴＴＰ又はＨＴＴＰＳプロトコルによりインターネット又はイントラネット上の各種Ｗｅｂサイト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によってセキュリティポリシーを遵守しているか否かの確認がなされる。そして、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、画面制御情報を生成したり、当該アプリケーションの起動を制限したりする。
【００３３】
なお、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。例えばキヤノンは複合機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（Ｍｕｌｔｉ－ｆｕｎｃｔｉｏｎａｌ　Ｅｍｂｅｄｄｅｄ　Ａｐｐｌｉｃａｔｉｏｎ　Ｐｌａｔｆｏｒｍ）（登録商標）を製品化している。このようなＪａｖａ（登録商標）の実行環境で動作するＭＥＡＰのアプリケーションも、機能実行部１５０による動作制限対象となる。
【００３４】
１１７はポリシー受信手段であるところの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ところの画面制御部であり、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。
【００３５】
図２（ｂ）において、１２１はポリシー生成手段であるところの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。１２４はポリシー送信手段であるところのポリシー送信部であり、ポリシー生成部１２１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１１８からネットワーク１２６を介して送信する。
【００３６】
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。
【００３７】
まず、管理者がＰＣ１２５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「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。

【００３８】

次に、生成したセキュリティポリシーデータをＰＣ１２５から複合機１０１に送信、適用することで、複合機１０１が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。

【００３９】

最後に、ユーザがセキュリティポリシーデータを適用した複合機１０１を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。

【００４０】

まず、管理者がＰＣ１２５を用いて、複合機１０１を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。

【００４１】

図３は、ＰＣ１２５の入力部１２３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。

【００４２】

図３において、ポリシー設定画面２０１は、「ファイルの改ざん検知」２０２、「ファイルの送信方式」２０３、「ＨＤＤ残存データ削除」２０４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。

【００４３】

「ファイルの改ざん検知」２０２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」、「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。

【００４４】

「ファイルの送信方式」２０３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」、「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、「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。

【００４５】

「ＨＤＤ残存データ削除」２０４は、複合機１０１におけるコピー処理等で不揮発記憶装置を一時データ保存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。

【００４６】

管理者は、ポリシー設定画面２０１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２０１において、「ＯＫ」ボタン２０５の押下を入力部１２３が受け付けると、ポリシー生成部１２１は、ポリシー設定画面２０１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１２２に保存する。記憶装置１２２に保存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。なお、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２０に示す。

【００４７】
セキュリティポリシーデータ３０１では、１列目が、ポリシー設定画面２０１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）３０２である。２列目が、ポリシー設定画面２０１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）３０３となっている。
【００４８】
次に、生成したセキュリティポリシーデータをＰＣ１２５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。
【００４９】
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入力部１２３は、ポリシー送信部１２４に送信を指示する。指示を受けたポリシー送信部１２４は、記憶装置１２２に保存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１１８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、ＰＣ１２５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。
【００５０】
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１０７からＲＡＭ１０６に読み込んだプログラムコードによって、ＣＰＵ１０５が実行するものとする。
【００５１】
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ＰＣ１２５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。
【００５２】
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情報セキュリティポリシーの値を抽出してＲＡＭ１０６に記憶する。
【００５３】
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（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、ＲＡＭ１０６に記憶した情報セキュリティポリシーの名称とを比較する。さらに、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）の変換ルールファイル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。
【００５４】
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。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モードの名称が記述されている。条件部５０３３列目には、ユーザ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５

０３の最後の列には、ユーザ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記述されている。

【００５５】

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ＰＣ１２５）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。

【００５６】

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おり、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。

【００５７】

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のユーザモードの中でも、「ｆｔｐ」、「ＳＦＴＰ」に対応していることを示している。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。また、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。これは複合機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２１に示す。

【００５８】

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ＲＡＭ１０６に記憶し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ＲＡＭ１０６に中間情報として記憶する。

【００５９】

例えば、図４（ａ）のセキュリティポリシーデータ３０１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。

【００６０】

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ＲＡＭ１０６に記憶する。

【００６１】

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ＲＡＭ１０６に記憶し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ＲＡＭ１０６に記憶する（ステップＳ４０５）。

【００６２】

ステップＳ４０３でＮＯと判定される場合は例えば以下のような場合である。すなわち

、セキュリティポリシーデータ３０１から取得した名称３０２が「ＨＤＤの残存データ削除」である場合で、かつ、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、ステップＳ４０３でＮＯと判定される。

【００６３】

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。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ＲＡＭ１０６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、ＲＡＭ１０６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。

【００６４】

図４（ｃ）に示す中間情報６０１では、ユーザモードの名称「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、ユーザモードの名称「ｆｔｐ」と「ＳＦＴＰ」が、情報セキュリティポリシーの値「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３０１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ＲＡＭ１０６（エラー情報格納手段）に記憶される。

【００６５】

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、ＲＡＭ１０６に記憶した中間情報を中間情報格納部１１５に格納する。

【００６６】

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１０７からＲＡＭ１０６に読み込んだプログラムコードによって、ＣＰＵ１０５が実行するものとする。

【００６７】

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モードの名称を取得し、ＲＡＭ１０６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ＲＡＭ１０６に記憶される。

【００６８】

次に、ステップＳ４１１にて、ポリシー検証部１０９は、ＲＡＭ１０６に記憶したユーザモードの名称を用いて、ユーザモード格納部１０４から複合機１０１に設定された現在のユーザモードの値を取得する。複合機１０１のユーザモード格納部１０４に格納されているユーザ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「ＯＦＦ」を取得し、ＲＡＭ１０６に記憶する。

【００６９】

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５０

３から、対応する条件を取得する。そして、ＲＡＭ１０６に記憶した現在のユーザモードの値が条件を満たすか判定する。

【００７０】

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。「どれか一つ有効」は、現在のユーザモードの「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。「セキュリティポリシーなし」は現在のユーザ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。

【００７１】

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Ｓ４１７に進む。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ＲＡＭ１０６に記憶した情報とステップ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ＲＡＭ１０６に一時的に記憶する（ステップＳ４１３）。そして、ステップＳ４１７に進む。

【００７２】

ステップＳ４１７にて、ポリシー検証部１０９は、ユーザ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（機能実行部４１８）がセキュリティポリシーを遵守しているかの確認も行う。ステップＳ４１７でセキュリティポリシーを遵守していると判定した場合（ステップＳ４１７でＹＥＳ）、ステップＳ４０９に戻る。一方、ステップＳ４１７でセキュリティポリシーを遵守していないと判定した場合（ステップＳ４１７でＮＯ）、ステップＳ４１８に進む。ステップＳ４１８で、ポリシー検証部１０９は、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（機能実行部４１８）の動作の停止を行う。

【００７３】

ステップＳ４１７とステップＳ４１８の処理の具体例を説明する。

【００７４】

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（機能実行部４１８）が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」というセキュリティポリシーを適用しようとする場合、複合機にインストールされているアプリケーション（機能実行部４１８）が、ファイルを扱うアプリケーションであるかを判断する。そして、もし「ファイルの改ざん検知」に関連するアプリケーションである場合には、ポリシー検証部１０９は、そのアプリケーションが「ファイルの改ざん検知」の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を判定する。

【００７５】

一方、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に設定したり、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してもよい。

【００７６】

また、ステップＳ４１２の判定の結果、ファイル改ざん検知の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、ポリシー検証部１０９は、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動作を停止する。アプリケーションの動作の停止とは、例えばアプリケーションの起動の停止を意味する。

【００７７】

なお、複合機１０１にインストールされているアプリケーション（機能実行部４１８）が複数ある場合には、当該複数のアプリケーションのうちセキュリティポリシーを遵守し

ないアプリケーションを特定し、特定したアプリケーションの動作を停止する。
【００７８】
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。
【００７９】
ステップＳ４１４では、ポリシー検証部１０９は、ＲＡＭ１０６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ＲＡＭ１０６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。
【００８０】
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「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。
【００８１】
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ＲＡＭ１０６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。
【００８２】
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ＰＣ１２５に送信する。
【００８３】
ＰＣ１２５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１１８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、ＰＣ１２５は、複合機１０１から画面制御情報を受け取った場合、ＰＣ１２５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。
【００８４】
図８（ａ）では、「＜エラー！＞」の項目に、ステップＳ４０５でエラーとしてＲＡＭ１０６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、ＰＣ１２５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。
【００８５】
以上より、本実施形態によれば、ＰＣ１２５で作成した情報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、ＰＣ１２５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。
【００８６】
次に、ユーザ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の処理について説明する。
【００８７】
図９は、複合機１０１の画面制御部１１３により実行される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１０７からＲＡＭ１０６に読み込んだプログラムコードによって、ＣＰＵ１０５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。
【００８８】
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。本実施形態では、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を表示している。ただし、図８（ａ）の画面と同様に「＜エラー！＞」の項目として「ＨＤＤ残存データ削除」のセキュリティポリシーが適用されていない旨を表示してもよい。そして、「ＨＤＤ残存データ削除」の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に追加する旨を表示してもよい。

【００８９】

また、本実施形態では、エラー画面が表示された状態で、ユーザが複合機１０１で利用可能な機能は、ＵＩ操作部１０３を持用いたユーザ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。

【００９０】

図９に戻り、ステップＳ１００３にて、画面制御部１１３は、ユーザによるＵＩ操作部１０３の操作によってユーザモード格納部１０４に格納されたユーザ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）のエラー画面を表示する。一方、設定が変更された場合、ステップＳ１００４にて中間情報格納部１１５に格納された中間情報を利用して、セキュリティポリシーデータの適用を行い、ステップＳ１００１に戻る。なお、ステップＳ１００４の処理は図５のステップＳ４０９からステップＳ４１６までの処理と同様であるため、それらの説明を省略する。

【００９１】

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にてユーザモードの値が変更されていないと判定した場合、画面制御部１１３は本処理を終了し、再度、図９の処理を開始する。

【００９２】

なお、本実施形態では、管理者がＰＣ１２５のポリシー生成部１２１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１２１が複合機１０１内部にあり、管理者がＵＩ操作部１０３もしくはＰＣ１２５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。

【００９３】

上記第１の実施形態によれば、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。

【００９４】

［第２の実施形態］

次に、本発明の第２の実施形態について説明する。第２の実施形態では、複合機１０１にてユーザが誤って情報セキュリティポリシーを従った状態から違反した状態に変えてしまうことを防ぐ方法について述べる。なお、ユーザがＵＩ操作部１０３を用いてユーザモード設定画面を開いたときの処理を除いては、上記第１の実施形態と同様であり、同様の部分については、同一の符号を用いてその説明を省略する。以下に、上記第１の実施の形態と異なる点のみを説明する。

【００９５】

本実施形態では、第１の実施形態と同じセキュリティポリシーデータが適用された状態の複合機１０１を使って説明する。

【００９６】
図１０は、ユーザモード設定時の情報セキュリティポリシー違反防止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１０７からＲＡＭ１０６に読み込んだプログラムコードによって、ＣＰＵ１０５が実行するものとする。
【００９７】
ステップＳ１２１１にて、画面制御部１１３は、ＵＩ操作部１０３にてユーザからの操作を受け付け、ユーザモード設定画面を表示する。
【００９８】
次に、ステップＳ１２１２にて、画面制御部１１３は、中間情報格納部１１５からユーザモードの名称を取得し、表示された画面が情報セキュリティポリシーに関するユーザモードの設定画面か判定する。この判定結果から情報セキュリティポリシーに関するユーザモードの設定画面ではないと判定した場合、本処理を終了する。一方、情報セキュリティポリシーに関するユーザモードの設定画面であると判定した場合、ステップＳ１２１３に進む。
【００９９】
ステップＳ１２１３では、画面制御部１１３は、ユーザモードの設定画面で現在の設定から変更すると、情報セキュリティポリシーに違反する項目があるか判定する。例えば、ＵＩ操作部１０３に表示されたユーザモードの設定画面の一例を図１１（ａ）に示す。図示例では、「強制デジタル署名付きＰＤＦ」１１０１は「ＯＮ」、「強制ハッシュ付きＰＤＦ」１１０２は「ＯＦＦ」に設定されている。なお、「設定反映」ボタン１１０３は、画面中の選択を複合機１０１のユーザモード格納部１０４に格納されているユーザモードの値に反映させるためのボタンである。
【０１００】
図１１（ａ）の場合、情報セキュリティポリシーに違反する項目の有無を判定するために、まず、「強制デジタル署名付きＰＤＦ」１１０１がＯＦＦになったと仮定した上で、図６のステップＳ４０９～Ｓ４１３の処理を行う。複合機１０１では、「強制デジタル署名付きＰＤＦ」と「強制ハッシュ付きＰＤＦ」のいずれかがＯＮでなければ、情報セキュリティポリシーに違反した状態になってしまう。そのため、「強制デジタル署名付きＰＤＦ」１１０１の「ＯＦＦ」は、変更すると情報セキュリティポリシーに違反する項目と判定される。同様の処理によって、「強制ハッシュ付きＰＤＦ」１１０２の「ＯＮ」は、違反しない項目と判定される。
【０１０１】
ステップＳ１２１４にて、画面制御部１１３は、違反する項目については、ユーザ操作により設定変更できないように画面制御する。例えば、図１１（ａ）に示す画面が図１１（ｂ）に示す画面に変更される。図示例では、「強制デジタル署名付きＰＤＦ」１１０１の「ＯＦＦ」ボタン１１０４は、設定変更できないように変更（斜線部）されている。すなわち、「強制ハッシュ付きＰＤＦ」１１０２は「ＯＮ」にできるが、「強制デジタル署名付きＰＤＦ」１１０１は「ＯＦＦ」にできなくなっている。
【０１０２】
ステップＳ１２１５にて、画面制御部１１３は、変更可能な項目が変更されたか判定する。変更可能な項目が変更された場合はステップＳ１２１６に進む。例えば、図１２（ａ）に示す画面は、図１１（ｂ）に示す画面上で「強制ハッシュ付きＰＤＦ」１１０２が「ＯＮ」にされた画面である。
【０１０３】
ステップＳ１２１６では、画面制御部１１３は、ＵＩ操作部１０３にユーザによる設定完了の入力がされたか判定する。入力されなかった場合はステップＳ１２１５に戻る一方、入力された場合は、ステップＳ１２１７に進む。ステップＳ１２１７では、画面制御部１１３はＵＩ操作部１０３によって入力された値に基づいて、ユーザモード格納部１０４の値を更新して本処理を終了する。
【０１０４】

本実施形態によれば、情報セキュリティポリシーに反する設定をユーザが入力できなくなるため、誤ったユーザモード設定によって、複合機が情報セキュリティポリシー違反になることを防ぐことができる。

【０１０５】

［第３の実施形態］

上記第１の実施形態で説明した機能を有する複合機と当該機能がない複合機が混在するオフィスでは、後者の複合機に対して、手動で情報セキュリティポリシーに従う設定をする必要がある。そこで、本実施形態では、第１の実施形態で説明した機能がない複合機に対しても同一の情報セキュリティポリシーに従う設定を行う方法について述べる。なお、上記第１の実施形態と同様の部分については、同一の符号を用いてその説明を省略する。以下に、上記第１の実施の形態と異なる点のみを説明する。

【０１０６】

図１３は、本発明の第３の実施形態における画像処理装置のハードウェア構成の概略を示す図である。

【０１０７】

図１３において、１４０１は上記第１の実施形態で説明した機能がない複合機である。１４５０は上記第１の実施形態で説明した機能を有する複合機である。１４１４は管理者がセキュリティポリシーデータの生成、配信や情報セキュリティポリシーに従ったユーザモードの設定の生成・配信を行うＰＣである。

【０１０８】

複合機１４５０は、複合機１０１と同様に、ネットワーク通信部１０２、ＵＩ操作部１０３、ＣＰＵ１０５、ＲＡＭ１０６、記憶装置１０７、印刷エンジン１０８、スキャナエンジン１１４を備える。複合機１４０１は、ネットワーク通信部１４０２、ＵＩ操作部１４０３、ＣＰＵ１４０５、ＲＡＭ１４０６、記憶装置１４０７、印刷エンジン１４０９、スキャナエンジン１４０８を備える。複合機１４０１を構成する部分には、便宜上、複合機１０１と異なる符号が付されているが、ハードウェア構成は略同一である。

【０１０９】

ＰＣ１４１４は、ネットワーク通信部１４１５、ＣＰＵ１４１６、ＲＡＭ１４１７、記憶装置１４２２、入力部１４３０を備える。ＰＣ１４１４を構成する部分には、便宜上、ＰＣ１２５と異なる符号が付されているが、ハードウェア構成は略同一である。

【０１１０】

図１４は、複合機１４５０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。

【０１１１】

複合機１４５０は、図２（ａ）に示す複合機１０１に対して、性能応答部１４３３が追加されたものである。性能応答部１４３３は、外部の機器からネットワーク１２６を介してネットワーク通信部１４４０にセキュリティポリシーデータを受信する機能を有する確認する要求を受け取ると、応答を行う。

【０１１２】

図１５（ａ）は、複合機１４０１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り、図１５（ｂ）は、ＰＣ１４１４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。

【０１１３】

図１５（ａ）において、１４１０はネットワーク１２６を介して配信されたユーザモードファイルを読み取り、ユーザモード格納部１４０４に格納されたユーザモードの値の更新を行うユーザモード反映部である。１４１１はネットワーク１２６を介してネットワーク通信部１４０２にユーザモードの設定を取得する要求を受信すると、ユーザモード格納部１４０４に格納されたユーザモードの名称と値を取得し、要求元に返信するユーザモード応答部である。１４１２は複合機の種別を示す情報が書かれた複合機種別ファイルを格納する複合機種別格納部である。１４１３はネットワーク１２６を介してネットワーク通

信部１４０２に複合機の種別を取得する要求を受信すると、複合機種別格納部１４１２に格納された複合機種別ファイルを要求元に返信する複合機種別応答部である。

【０１１４】

図１５（ｂ）の１４２３は特定の複合機の変換ルールではなく、ネットワーク１２６に接続されたすべての複合機の変換ルールが、複合機の種別と組になって格納されている点を除き、第１の実施形態の変換ルール格納部１１１と同等の変換ルール格納部である。

【０１１５】

１４２７は情報セキュリティポリシーに従ったユーザモードの値を生成するユーザモード生成部である。１４２８はネットワーク１２６を介してネットワーク通信部１４１５から他の機器と通信を行い、他の機器がセキュリティポリシーデータを受信する機能を有するか確認を行う複合機性能確認部である。

【０１１６】

１４２９はユーザモード生成部によって生成された値とそれに対応するユーザモードの名称を格納するユーザモード格納部である。１４３１はユーザモード格納部１４２９に格納されたユーザモードの名称と値を送信するユーザモード送信部である。

【０１１７】

なお、ポリシー生成部１４１８、ポリシー格納部１４１９、ポリシー変換部１４２０、ポリシー生成部１４２１、画面制御部１４２４、画面制御情報格納部１４２５、中間情報格納部１４２６、ポリシー送信部１４３２は図２（ａ）と略同一で説明を省略する。また、本実施形態における管理者によるセキュリティポリシーデータの生成は、上記第１の実施形態と同じであるため、それらの説明を省略する。

【０１１８】

次に、本実施形態における情報セキュリティポリシー配信時の各装置の動作について説明する。

【０１１９】

まず、ＰＣ１４１４では、複合機性能確認部１４２８が、セキュリティポリシーデータを配信するネットワーク上の複合機に対して、セキュリティポリシーデータの受信が可能か問い合わせを行う。例えば、複合機１４５０に問い合わせた場合、性能応答部１４３３がネットワーク通信部１０２からネットワーク１２６を介して、ネットワーク通信部１４１５に可能であると応答する。複合機性能確認部１４２８は、ネットワーク通信部１４１５に応答を受けると、複合機１４５０がセキュリティポリシーデータの受信が可能であると判定する。

【０１２０】

一方、複合機１４０１に問い合わせた場合、性能応答部が存在しないため、ネットワーク通信部１４１５に応答を受信しない。よって、複合機性能確認部１４２８は、複合機１４０１がセキュリティポリシーデータの受信が不可能であると判定する。

【０１２１】

複合機１４５０がセキュリティポリシーデータの受信が可能であると判定した場合、ＰＣ１４１４は、セキュリティポリシーデータの配信を行う。複合機１４５０は、受信したセキュリティポリシーデータの適用を行う。この適用処理について、第１の実施形態で説明した図５、図６に示す処理と同じであるため、それらの説明を省略する。

【０１２２】

複合機１４０１がセキュリティポリシーデータの受信が不可能であると判定した場合、ＰＣ１４１４のユーザモード生成部１４２７は、複合機１４０１にネットワーク通信部１４１５からネットワーク１２６を介して、現在のユーザモードの値を要求する。

【０１２３】

現在のユーザモードの値の要求をネットワーク通信部１４０２が受信すると、ユーザモード応答部１４１１は、ユーザモード格納部１４０４に格納されたユーザモードの名称と値を取得する。ユーザモード応答部１４１１は、取得したユーザモードの名称と値をネットワーク通信部１４０２からネットワーク１２６を介して、ＰＣ１４１４のネットワーク

通信部１４１５に送信する。
【０１２４】
ユーザモードの名称と値をネットワーク通信部１４１５が受信すると、ユーザモード生成部１４２７は、受信したユーザモードの名称と値をＲＡＭ１４１７に記憶する。複合機１４０１のユーザモード格納部１４０４に格納されたユーザモードの名称と値が、図７（ａ）に示すように、「強制デジタル署名付きＰＤＦ」と「強制ハッシュ付きＰＤＦ」が「ＯＦＦ」、「ｆｔｐ」と「ＳＦＴＰ」が「ＯＮ」であるものとして説明する。
【０１２５】
ＰＣ１４１４のユーザモード生成部１４２７は、ネットワーク通信部１４１５からネットワーク１２６を介して、複合機１４０１のネットワーク通信部１４０２に複合機の種別を要求する。
【０１２６】
複合機の種別の要求をネットワーク通信部１４０２が受けると、複合機種別応答部１４１３は、複合機種別格納部１４１２に格納された複合機種別ファイルを、ネットワーク通信部１４０２からネットワーク１２６を介して、ネットワーク通信部１４１５に送信する。
【０１２７】
複合機種別ファイルをネットワーク通信部１４１５が受信すると、ＰＣ１４１４のユーザモード生成部１４２７は、複合機種別ファイルから複合機の種別を取得し、ＲＡＭ１４１７に記憶する。本実施形態では、複合機種別格納部１４１２に格納された複合機を示す情報が「ａａａ」であるものとして説明する。よって、ＲＡＭ１４１７には「ａａａ」が記憶される。
【０１２８】
図１６は、ＰＣ１４１４の変換ルール格納部１４２３に格納されている複合機種別と変換ルールファイルの組の一例を表形式で表した図である。なお、図示例のように、必ずしも表形式である必要はなく、ＸＭＬ形式などでもよい。図示例では、ａａａという機種の複合機の変換ルールファイルと、ｂｂｂという機種の複合機の変換ルールファイルが変換ルール格納部１４２３に格納されている。
【０１２９】
ＰＣ１４１４のユーザモード生成部１４２７は、ＲＡＭ１４１７に記憶した複合機種別に対応する変換ルールファイルを変換ルール格納部１４２３から取得し、ＲＡＭ１４１７に記憶する。次に、複合機１４０１では、セキュリティポリシーデータの適用を行う。なお、ＰＣ１４１４で実行され、変換ルールと現在のユーザモードの設定の格納場所がＲＡＭ１４１７である点を除いては、図５のステップＳ４０２～図６のステップＳ４１６の処理と同等であるため、それらの説明は省略する。
【０１３０】
本実施形態では、セキュリティポリシーデータの適用後、図７（ｂ）に示す画面制御情報が画面制御情報格納部１４２５に格納される。
【０１３１】
次に、セキュリティポリシーデータの適用後に実行されるユーザモード生成部１４２７の処理を図１７を参照して説明する。
【０１３２】
図１７は、ユーザモード生成部１４２７により実行される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１４２２からＲＡＭ１４１７に読み込んだプログラムコードによって、ＣＰＵ１４１６が実行するものとする。
【０１３３】
ステップＳ１５０１にて、ユーザモード生成部１４２７は、複合機１４０１が情報セキュリティポリシーに従っているか否かを画面制御情報格納部１４２５に画面制御情報が格納されているか否かで判定する。画面制御情報が格納されていないと判定した場合、ユーザモード生成部１４２７は、複合機１４０１が情報セキュリティポリシーに従っていると

判定して本処理を終了する。一方、画面制御情報が格納されていると判定した場合、複合機１４０１は、情報セキュリティポリシーに従っていないため、ユーザモードの設定を変更する必要がある。そこで、ステップＳ１５０２にて、ユーザモード生成部１４２７は、画面制御情報格納部１４２５から画面制御情報を取得する。そして、該画面制御情報からユーザモードの名称を抽出し、ＲＡＭ１４１７から取得した名称を用いて、ユーザモードの値を取得し、ユーザモード格納部１４２９に格納する。さらに、ユーザモード生成部１４２７は、ユーザモード格納部１４２９に格納したユーザモードの名称と値に基づいて、ユーザモードの設定画面を生成する（ステップＳ１５０２）。生成したユーザモードの設定画面の一例を図１２（ｂ）に示す。

【０１３４】

ステップＳ１５０３にて、ユーザモード生成部１４２７は、ステップＳ１５０２で生成されたユーザモードの設定画面を入力部１４３０に表示する。

【０１３５】

次に、管理者に情報セキュリティポリシーを満たすようにユーザモードの設定変更を行わせ、ユーザモード格納部１４２９に情報セキュリティポリシーに従ったユーザモードの値が保存される。この処理は、図９のステップＳ１００１～Ｓ１００５の処理に対して、ＵＩ操作部ではなく、入力部１４３０によって行われるほかはすべて略同一であるため、それらの説明は省略する。管理者によって図１１（ａ）に示す入力がされた場合は、「強制デジタル署名付きＰＤＦ」が「ＯＮ」、「強制ハッシュ付きＰＤＦ」が「ＯＦＦ」として、ユーザモード格納部１４２９に格納される。

【０１３６】

次に、ユーザモード送信部１４３１は、ネットワーク通信部１４１５からネットワーク１２６を介して、ネットワーク通信部１４０２に、ユーザモード格納部１４２９に格納されたユーザモードの値とそれに対応する名称を送信する。

【０１３７】

ユーザモードの値と名称をネットワーク通信部１４０２が受信すると、ユーザモード反映部１４１０は、ユーザモード格納部１４０４に格納されたユーザモードの値を、受信したユーザモードの名称と値に更新する。これにより、「強制デジタル署名付きＰＤＦ」が「ＯＦＦ」から「ＯＮ」に更新され、「強制ハッシュ付きＰＤＦ」が「ＯＦＦ」のままとなる。

【０１３８】

本実施形態によれば、セキュリティポリシーデータを受信できない複合機であっても、情報セキュリティポリシーを守る設定を管理者が選択した上で、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。

【０１３９】

［第４の実施形態］

複合機では、ライセンスのインストールやオプションの接続などによって、情報セキュリティポリシーに関わるユーザモードが増減する場合がある。増減した名称や値に関しても、情報セキュリティポリシーに従っているか確認する必要がある。そこで、本実施形態では、ユーザモードの名称や設定できる値の範囲の増減があった場合でも、複合機を情報セキュリティポリシーに従った状態に保つ方法について述べる。なお、上記第１の実施形態と同様の部分については、同一の符号を用いてその説明を省略する。以下に、上記第１の実施の形態と異なる点のみを説明する。

【０１４０】

図１８は、本発明の第４の実施形態における画像処理装置の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。

【０１４１】

複合機１７０１は、図２（ａ）に示す複合機１０１に対して、ポリシー適用判定部１７１７と、ユーザモードバックアップ格納部１７１８が追加されたものである。ポリシー適用判定部１７１７は、ユーザモードの増減を検知し、情報セキュリティポリシーの適用が

必要な状態か判定する。ユーザモードバックアップ格納部１７１８は、情報セキュリティポリシーが適用されたタイミングのユーザモードの名称と値を格納する。なお、情報セキュリティポリシーを適用するまで処理の流れは第１の実施形態と同様であるため、それらの説明を省略する。

【０１４２】

情報セキュリティポリシーが適用されると、ポリシー適用判定部１７１７は、ユーザモードの名称と値をユーザモードバックアップ格納部１７１８に格納する。

【０１４３】

図１９は、ポリシー適用判定部１７１７により実行されるセキュリティポリシー判定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、記憶装置からＲＡＭに読み込んだプログラムコードによって、ＣＰＵが実行するものとする。

【０１４４】

ステップＳ１８０１にて、ポリシー適用判定部１７１７は、複合機１７０１の起動時にユーザモード格納部１０４に保存されたユーザモードの名称と値を、ユーザモードバックアップ格納部１７１８に格納されたユーザモードの名称と値が一致するか判定する。一致すると判定した場合、ユーザモードの増減はなく、情報セキュリティポリシーに従っている状態であるため、本処理を終了する。

【０１４５】

一方、ステップＳ１８０１で一致しないと判定した場合、ステップＳ１８０２にて、情報セキュリティポリシーの適用が行われる。情報セキュリティポリシーの適用処理については、第１の実施形態で説明した通りであるため、それらの説明を省略する。なお、ステップＳ１８０１の処理は、複合機の起動時に行うものとしているが、一定時間ごとに行うものであってもよい。

【０１４６】

本実施形態によれば、ユーザモードの増減が起こったとしても、直ちに情報セキュリティポリシーの適用を行うため、情報セキュリティポリシーに違反した状態で複合機が使われることを防ぐことができる。

【０１４７】

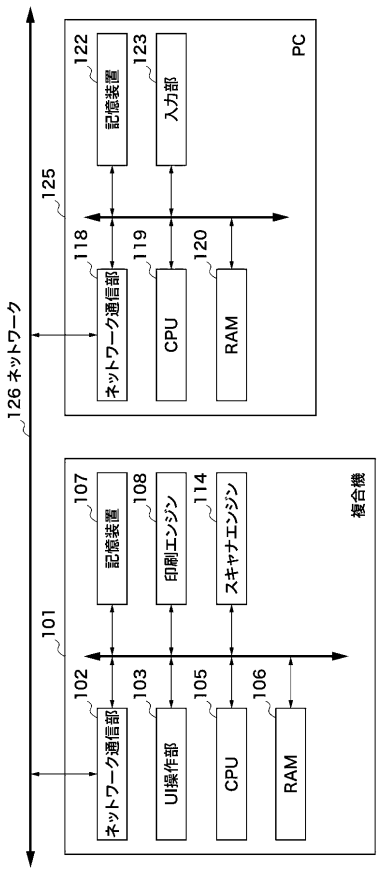
また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワーク又は各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

【符号の説明】

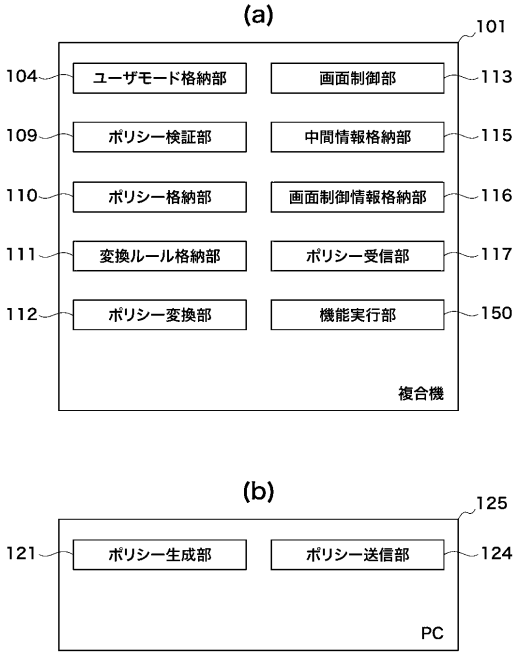
【０１４８】

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
１２５　ＰＣ

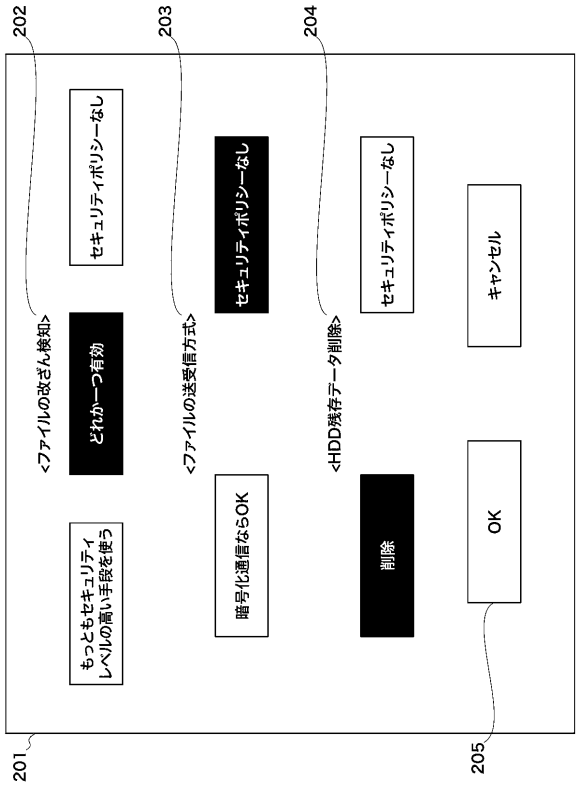
【図１】




【図２】




【図３】




【図４】

(a)

セキュリティポリシーデータ　301

| 情報セキュリティポリシーの名称 (302) | 情報セキュリティポリシーの値 (303) |
|---|---|
| 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 |

(b)

変換ルールファイル　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 | 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 |

502

| | 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 | 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 |

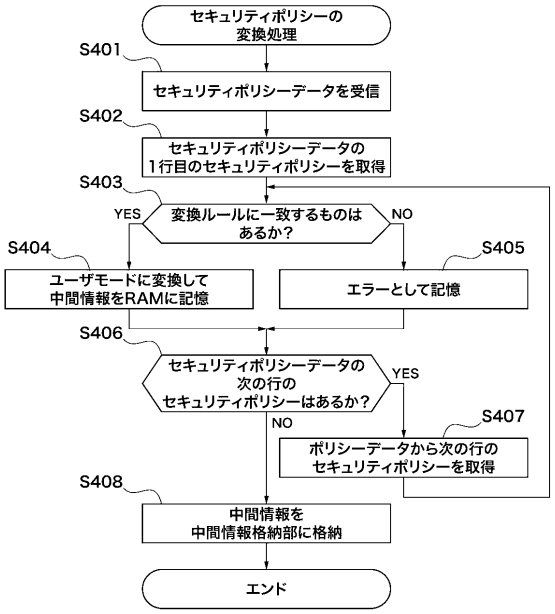
503

(c)

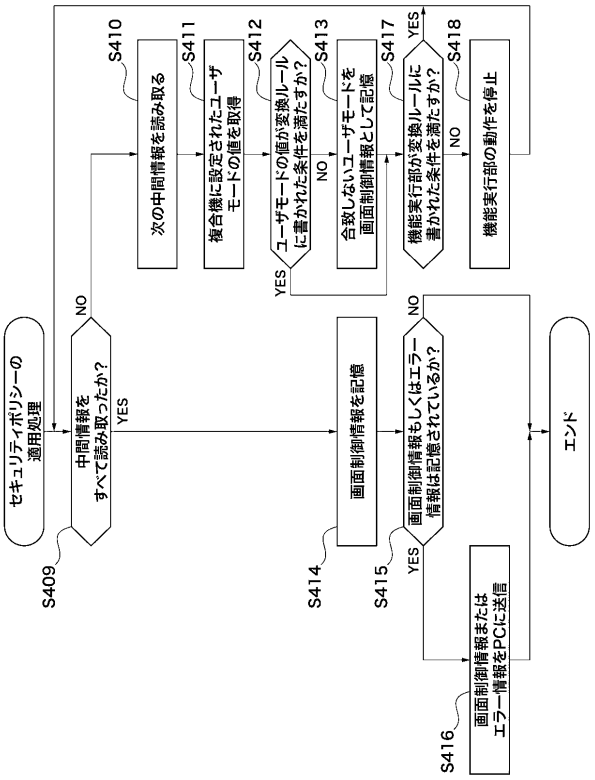
中間情報　601

| | |
|---|---|
| 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<br>もしくは<br>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

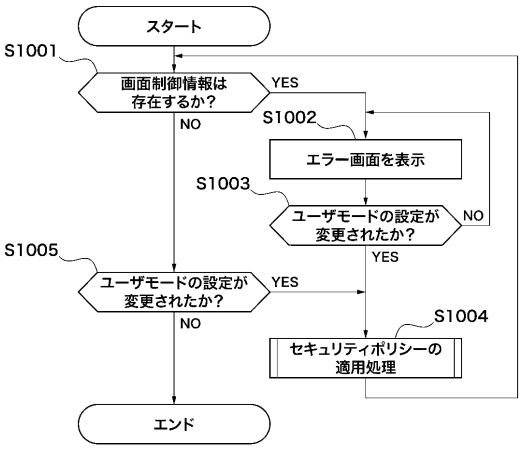
<注意！>
セキュリティポリシーに違反しています。
以下の設定を見直してください。
・強制デジタル署名付きPDF
・強制ハッシュ付きPDF

(b)

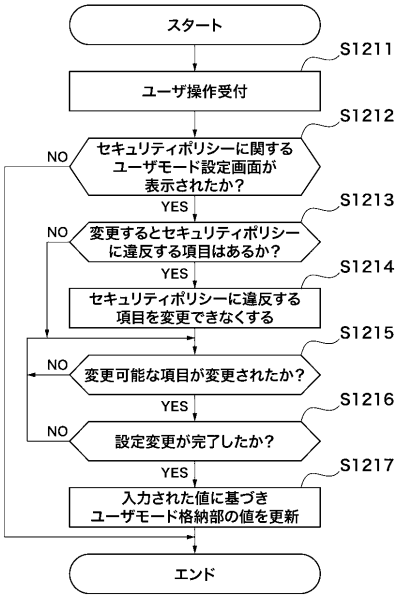
<注意！>
セキュリティポリシーに違反しているため、
デバイスを利用できません。

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

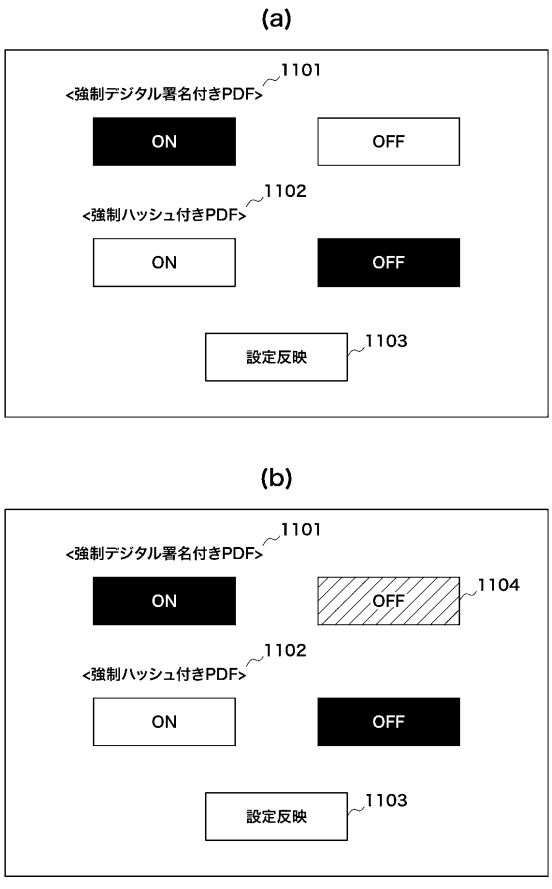
【図９】



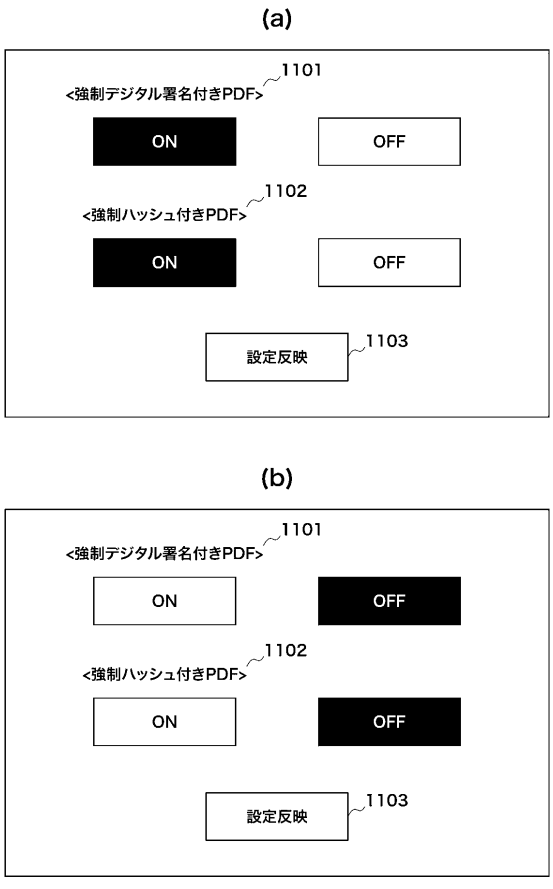

【図１０】



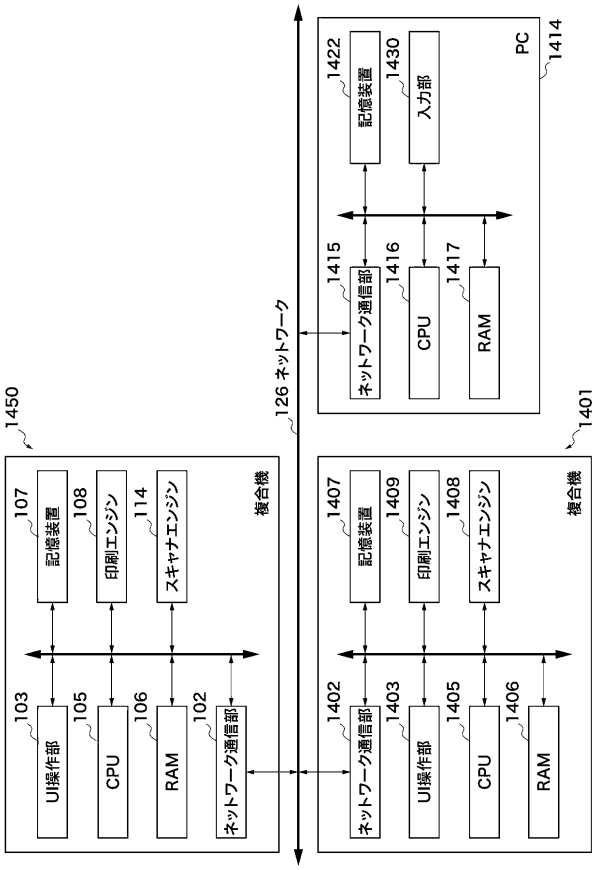

【図１１】



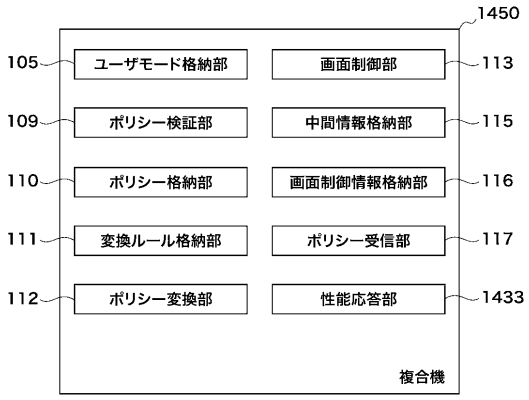

【図１２】



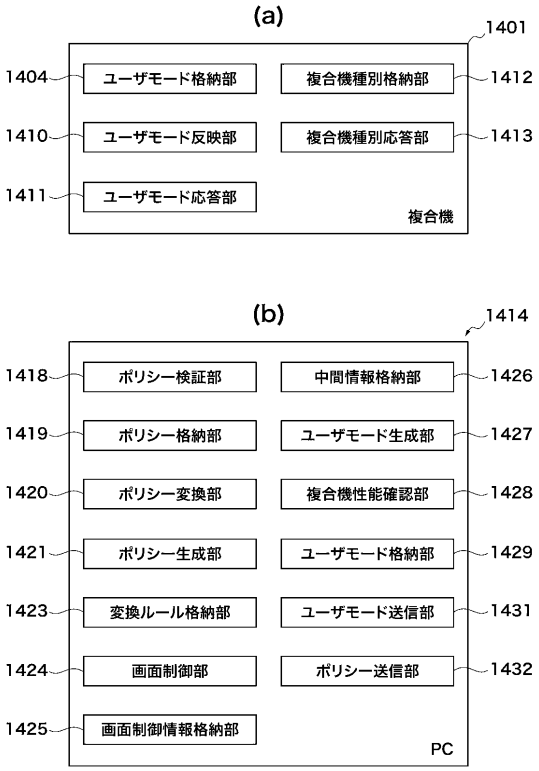
【図１３】




【図１４】




【図１５】




【図１６】

変換ルールファイル 1601

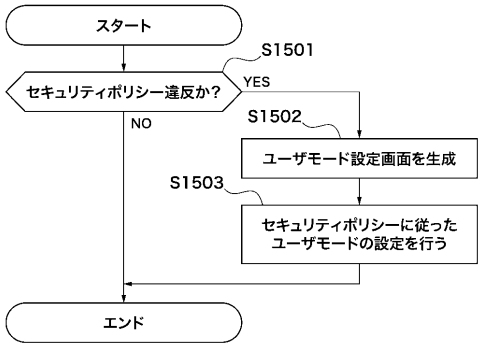
| | 情報セキュリティポリシーの名称 | 対応するユーザモードの名称 |
|---|---|---|
| ルール部 | ファイルの改ざん検知 | 強制デジタル署名付きPDF |
| | | 強制ハッシュ付きPDF |
| | ファイルの送受信方式 | FTP |
| | | SFTP |

| | 情報セキュリティポリシーの名称 | 設定可能な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に従っているか判定するための条件 |
|---|---|---|---|
| 条件部 | 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 |

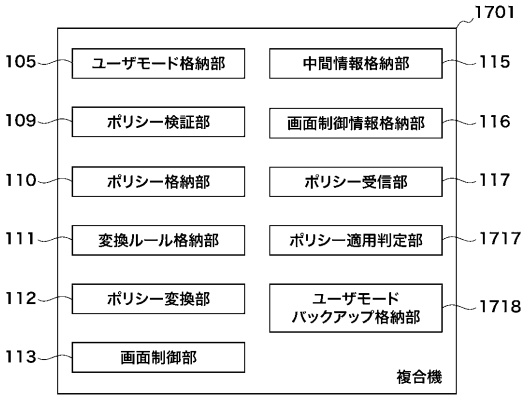
| | 情報セキュリティポリシーの名称 | 対応するユーザモードの名称 |
|---|---|---|
| ルール部 | ファイルの改ざん検知 | 強制デジタル署名付きPDF |
| | | 強制ハッシュ付きPDF |
| | ファイルの送受信方式 | FTP |
| | | SFTP |
| | HDD残存データ削除 | HDD完全消去 |

| | 情報セキュリティポリシーの名称 | 設定可能な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に従っているか判定するための条件 |
|---|---|---|---|
| 条件部 | 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 WebDAV:OFF |
| | | セキュリティポリシーなし | なし |
| | HDD残存データ削除 | 削除 | HDD完全消去:ON |
| | | セキュリティポリシーなし | なし |

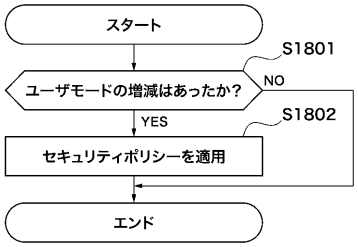
【図１７】




【図１８】




【図１９】




【図２０】

```
<?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２１】

```
<?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>
```

フロントページの続き

(56)参考文献 特開２０１１－１０１２５２（ＪＰ，Ａ）
特開２００７－１２８２３４（ＪＰ，Ａ）
特開２００９－１５９４８５（ＪＰ，Ａ）
特開２００８－１０２８７１（ＪＰ，Ａ）
特開２００１－２７３３８８（ＪＰ，Ａ）
特開２０１１－１２３８４１（ＪＰ，Ａ）
特開２００９－０１５５８５（ＪＰ，Ａ）
特開２００８－２０５８５０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／６２
Ｂ４１Ｊ ２９／００
Ｇ０６Ｆ ３／１２