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

特許第6207340号
(P6207340)

(45)発行日　平成29年10月4日(2017.10.4)　(24)登録日　平成29年9月15日(2017.9.15)

(51)Int.Cl.		F I		
G06F 21/45	(2013.01)	G06F	21/45	
G06F 21/60	(2013.01)	G06F	21/60	340
G06F 3/12	(2006.01)	G06F	3/12	302
B41J 29/38	(2006.01)	B41J	29/38	Z
B41J 29/00	(2006.01)	B41J	29/00	Z

請求項の数 9　(全 17 頁)　最終頁に続く

(21)出願番号　特願2013-217689(P2013-217689)
(22)出願日　平成25年10月18日(2013.10.18)
(65)公開番号　特開2015-79451(P2015-79451A)
(43)公開日　平成27年4月23日(2015.4.23)
審査請求日　平成28年10月17日(2016.10.17)

(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　武田　匡平
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　平井　誠

最終頁に続く

(54)【発明の名称】画像形成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】
外部からアクセス要求を受信する受信手段と、
前記受信手段で受信したアクセス要求を解析する第１の解析手段と、
前記第１の解析手段により、前記アクセス要求が、再設定ができなくなるセキュリティポリシーの変更確定要求であると判断された場合、前記受信手段が現在使用している第１のポートとは異なる第２のポートを開く制御手段とを備えることを特徴とする画像形成装置。
【請求項２】
前記再設定ができなくなるセキュリティポリシーは、少なくともＨＴＴＰアクセスを禁止するポリシーが含まれることを特徴とする請求項１に記載の画像形成装置。
【請求項３】
前記受信手段が前記第２のポートを使用して、再設定が可能になるセキュリティポリシーを受信したときは、前記制御手段は、前記再設定ができなくなったセキュリティポリシーを、前記再設定が可能になるセキュリティポリシーに変更することを特徴とする請求項１または２に記載の画像形成装置。
【請求項４】
外部からアクセス要求を受信する受信手段と、
前記受信手段で受信したアクセス要求を解析する第１の解析手段と、
前記第１の解析手段により、前記アクセス要求が、再設定ができなくなるセキュリティ

ポリシーの変更確定要求であると判断された場合、再設定が可能になるセキュリティポリシーを外部から取得する制御手段とを備えることを特徴とする画像形成装置。
【請求項５】
前記制御手段は、前記再設定が可能になるセキュリティポリシーが格納されたサーバーから定期的に取得して、前記再設定ができなくなったセキュリティポリシーを、前記再設定が可能になるセキュリティポリシーに変更することを特徴とする請求項４に記載の画像形成装置。
【請求項６】
前記第１の解析手段により、前記アクセス要求がセキュリティポリシーの変更要求であると判断された場合、変更されるセキュリティポリシーを解析する第２の解析手段と、
前記第２の解析手段により、前記変更されるセキュリティポリシーが、前記再設定ができなくなるセキュリティポリシーであると判断された場合、前記アクセス要求の要求元に対して警告を行う警告手段とをさらに備えることを特徴とする請求項１乃至５のいずれか１項に記載の画像形成装置。
【請求項７】
外部からアクセス要求を受信する受信工程と、
前記受信工程で受信したアクセス要求を解析する解析工程と、
前記解析工程にて、前記アクセス要求が、再設定ができなくなるセキュリティポリシーの変更確定要求であると判断された場合、前記受信工程で現在使用しているポートとは異なるポートを開く制御工程とを備えることを特徴とする画像形成装置の制御方法。
【請求項８】
外部からアクセス要求を受信する受信工程と、
前記受信工程で受信したアクセス要求を解析する解析工程と、
前記解析工程にて、前記アクセス要求が、再設定ができなくなるセキュリティポリシーの変更確定要求であると判断された場合、再設定が可能になるセキュリティポリシーを外部から取得する制御工程とを備えることを特徴とする画像形成装置の制御方法。
【請求項９】
請求項７または８に記載の制御方法を画像形成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、画像形成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セキュリティポリシーの配信技術に関する。
【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）やサーバー機器（ファイルサーバーや認証サーバー等）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って、セキュリティを扱う管理者が策定するものである。
【０００３】
オフィスのネットワークに接続する機器としては、ＰＣやサーバー機器以外に、複合機などの周辺装置がある。近年の複合機は、単純に画像を印刷や送信するだけではなく、複合機内に画像データを格納し、ＰＣに対してファイルサービスを提供する機能を有するものがあり、ネットワーク上に存在するその他のサーバー機器と同様の役割を果たすようになってきている。また、近年、複合機に搭載するアプリケーションの開発環境が公開されており、ＰＣなどと同様に、第三者によって開発されたアプリケーションが利用されている。

【０００４】
安全安心なオフィス環境を維持するためには、ＰＣやサーバー機器と同様に、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など、オフィス内の複合機の正規でない使用や情報漏えいを防ぐために運用に制約を設けることを意味する。
【０００５】
情報セキュリティポリシーに従わせるために、ＰＣやサーバー機器においては、ＯＳに依存する設定値（以下、「セキュリティポリシー」と呼ぶ）を配信サーバーで一括して設定し、設定されたセキュリティポリシーを各ＰＣやサーバー機器に配信する方法がある。例えば、通信経路の暗号化に関するＯＳ依存の設定値としては、「非ＳＳＬ接続を許可する」などがあり、どのベンダーのＰＣであっても情報セキュリティポリシーに従うよう統一的管理がされている。
【０００６】
複合機においては、複合機毎にセキュリティに関して設定可能な項目が異なるため、ＰＣやサーバー機器のようにＯＳに依存する設定値をそのままセキュリティポリシーとして配信することはできない。そのため、機器毎に設けられたルールに基づき機器にセキュリティポリシーに従ったセキュリティ設定を行うシステムが提案されている（例えば、特許文献１参照）。また、配信サーバーから一括して配信する以外にもＰＣのブラウザに表示された画面から複合機にアクセスして個別にセキュリティポリシーを設定することも可能である。
【先行技術文献】
【特許文献】
【０００７】
【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】
【０００８】
上記従来技術では、セキュリティポリシーを設定する際の通信プロトコルとして主にＨＴＴＰが使用されている。そのため、例えば「ＨＴＴＰ接続を禁止する」というポリシーが設定された場合、セキュリティポリシーを配信サーバーから配信することも、個別にブラウザから設定することもできなくなってしまう。そこで、複写機の表示パネルからセキュリティポリシーを変更する機能を設けることで対応することも可能である。
【０００９】
しかしながら、セキュリティ管理者がオフィス外のネットワークから複数の機器を管理しているケースも想定され、それら全ての機器に対して個別に再設定するのは困難である。そのため、遠隔地からでもネットワーク経由で再設定する機能が求められる。
【００１０】
本発明は、上記問題に鑑みて成されたものであり、再設定ができなくなるセキュリティポリシーが設定された場合であっても、ネットワーク経由でセキュリティポリシーの再設定が可能となるセキュリティポリシーの配信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】
【００１１】
上記目的を達成するために、本発明の画像形成装置は、外部からセキュリティポリシーを受信する受信手段と、前記受信手段で受信したセキュリティポリシーを解析する解析手段と、前記解析手段による解析結果から前記受信したセキュリティポリシーが、再設定ができなくなるセキュリティポリシーであると判断した場合に緊急用のポートをオープンする制御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、セキュリティポリシーが再設定できなくなった場合でも、予め設定された緊急用のポートを使用してアクセスを行う。これにより、再設定ができなくなるセキュリティポリシーが設定された場合であっても、ネットワーク経由でセキュリティポリシーの再設定が可能となる。

【図面の簡単な説明】

【００１３】

【図１】本発明の第１の実施形態に係る画像形成装置が配置されたネットワーク環境の一例を示す図である。

【図２】図１における画像形成装置のハードウェア構成の一例を示すブロック図である。

【図３】図１における画像形成装置のソフトウェア構成の一例を示すブロック図である。

【図４】セキュリティポリシーの設定変更時のクライアントＰＣと画像形成装置間のアクセス動作を示すシーケンス図である。

【図５】ＨＴＴＰアクセス制御部の動作処理の流れを示すフローチャートである。

【図６】セキュリティポリシー制御部の動作処理の流れを示すフローチャートである。

【図７】クライアントＰＣのブラウザに表示される画像形成装置へのログイン画面の一例を示す図である。

【図８】クライアントＰＣのブラウザに表示される設定登録画面の一例を示す図である。

【図９】クライアントＰＣのブラウザに表示されるセキュリティポリシー設定画面の一例を示す図である。

【図１０】画像形成装置内のＨＤＤに格納されているポリシーデータベースの一例を示す図である。

【図１１】クライアントＰＣのブラウザに表示されるアクセス不可警告画面の一例を示す図である。

【図１２】セキュリティポリシーの再設定ができない状況でアクセスしたときのクライアントＰＣと画像形成装置間のアクセス動作を示すシーケンス図である。

【図１３】クライアントＰＣのブラウザに表示されるアクセス不可画面の一例を示す図である。

【図１４】セキュリティポリシーの再設定ができず、緊急用のポートを使用してアクセスするときのクライアントＰＣと画像形成装置間のアクセス動作を示すシーケンス図である。

【図１５】クライアントＰＣのブラウザに表示されるセキュリティポリシー設定用ログイン画面の一例を示す図である。

【図１６】本発明の第２の実施形態におけるセキュリティポリシー制御部の動作処理の流れを示すフローチャートである。

【図１７】サーバーから取得するモードにおけるセキュリティポリシー設定時のクライアントＰＣ、画像形成装置、ポリシーサーバー間のアクセス動作を示すシーケンス図である。

【図１８】クライアントＰＣのブラウザに表示される確認画面の一例を示す図である。

【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の実施形態に係る画像形成装置が配置されたネットワーク環境の一例を示す図である。

【００１６】

画像形成装置１０１，１０４、クライアントＰＣ１０２、及びポリシーサーバー１０３がＬＡＮ等のネットワーク１０５に接続されており、通信可能な状態となっている。

【００１７】

図示のネットワーク環境では、クライアントＰＣ１０２のブラウザに表示された画面か

ら、画像形成装置１０１または画像形成装置１０４のＵＲＬを入力し、ブラウザに表示されたセキュリティポリシー設定画面からセキュリティポリシー設定を行うことができる。また、ポリシーサーバー１０３を利用して画像形成装置１０１，１０４の複数の装置に同時にセキュリティポリシーを配信することも可能である。さらに、画像形成装置１０１または画像形成装置１０４がポリシーサーバー１０３に対してセキュリティポリシーを取得することも可能である。

【００１８】

図２は、図１における画像形成装置１０１のハードウェア構成の一例を示すブロック図である。なお、画像形成装置１０４も画像形成装置１０１と略同一の構成を有するものとする。

【００１９】

ＣＰＵ２０１は、ソフトウェアプログラムを実行し、装置全体の制御を行う。ＲＯＭ２０２は、リードオンリーメモリであり、装置のブートプログラムや固定パラメータ等が格納されている。ＲＡＭ２０３は、ランダムアクセスメモリであり、ＣＰＵ２０１が装置を制御する際に、一時的なデータの格納などに使用する。

【００２０】

ＨＤＤ２０４は、ハードディスクドライブであり、印刷データなどの様々なデータが格納される。ネットワークＩ／Ｆ制御部２０５は、ネットワーク１０５とのデータの送受信を制御する。

【００２１】

スキャナＩ／Ｆ制御部２０６は、スキャナ２１１を制御するためのインターフェースである。プリンタＩ／Ｆ制御部２０７は、プリンタ２１０を制御するためのインターフェースである。

【００２２】

パネル制御部２０８は、オペレーションパネル２１２を制御し、各種情報の表示、使用者からの指示入力を行う。

【００２３】

ＣＰＵ２０１、ＲＯＭ２０２、ＲＡＭ２０３、ＨＤＤ２０４、ネットワークＩ／Ｆ制御部２０５、スキャナＩ／Ｆ制御部２０６、プリンタＩ／Ｆ制御部２０７、及びパネル制御部２０８は、バス２０９を介して互いに接続されている。バス２０９は、ＣＰＵ２０１からの制御信号や各装置間のデータ信号が送受信されるシステムバスである。

【００２４】

図３は、図１における画像形成装置１０１のソフトウェア構成の一例を示すブロック図である。図示例では、セキュリティポリシーに関連するソフトウェアについてのみ記載されている。

【００２５】

ＨＴＴＰアクセス制御部３０１は、ＨＴＴＰアクセスを制御するためのソフトウェアプログラムであり、以下の各機能を備える。

【００２６】

アクセス受信機能３１１は、ネットワークＩ／Ｆ制御部２０５を経由してネットワーク上の端末からのＨＴＴＰアクセスを受けたときにＨＴＴＰデータを受信する。アクセス解析機能３１２は、受信したＨＴＴＰデータを解析する。

【００２７】

ポリシー制御機能３１３は、アクセス解析機能３１２によりＨＴＴＰデータを解析した結果からポリシー変更の要求があったと判断した場合に、セキュリティポリシー制御部３０２に対して変更要求を行う。ポート制御機能３１４は、アクセス解析機能３１２によりＨＴＴＰデータを解析した結果からポート変更要求が有ったと判断した場合にポート変更を行う。

【００２８】

セキュリティポリシー制御部３０２は、セキュリティポリシーを制御するためのソフト

ウェアプログラムであり、以下の各機能を備える。

【００２９】

ポリシー受信機能３２１は、ＨＴＴＰアクセス制御部３０１を含む他のプログラムからセキュリティポリシーを受信する。ポリシー解析機能３２２は、受信したセキュリティポリシーを解析する。ポリシー設定機能３２３は、受信したセキュリティポリシーを適用するための機能である。

【００３０】

ＨＴＴＰアクセス制御部３０１及びセキュリティポリシー制御部３０２は、ＲＯＭ２０２に格納され、ＣＰＵ２０１により装置を制御する際にＲＡＭ２０３に展開され実行される。また、ＨＤＤ２０４には、ポリシーデータベース３３１が格納されている。ポリシーデータベース３３１には、画像形成装置１０１が保持するセキュリティポリシーの情報が格納されている。

【００３１】

図４は、セキュリティポリシーの設定変更時のクライアントＰＣ１０２と画像形成装置１０１間のアクセス動作を示すシーケンス図である。なお、画像形成装置１０１では、ＨＴＴＰアクセス制御部３０１とセキュリティポリシー制御部３０２間のアクセス動作を示す。

【００３２】

クライアントＰＣ１０２からブラウザを起動して表示された画面上のＵＲＬ欄に画像形成装置１０１のＵＲＬを入力すると、クライアントＰＣ１０２から画像形成装置１０１に対してＨＴＴＰアクセス要求が行われる（Ｓ４００１）。Ｓ４００１のＨＴＴＰアクセス要求は画面表示の要求であり、ＨＴＴＰアクセス制御部３０１は、ＨＴＴＰアクセス要求を解析してレスポンスとしてレスポンス画面を返す（Ｓ４００２）。これにより、クライアントＰＣ１０２のブラウザに図７に示すログイン画面７００が表示される。

【００３３】

ログイン画面７００上でユーザＩＤとパスワードが入力され、ログインボタンが押下されると、図８に示す設定登録画面８００に遷移する。設定登録画面８００上で「セキュリティポリシー設定」が選択されると、図９に示すセキュリティポリシー設定画面９００に遷移する。なお、図４には記載されていないが、画面遷移の度にＳ４００１とＳ４００２のやり取りが繰り返し行われる。

【００３４】

セキュリティポリシー設定画面上で各種セキュリティポリシーの設定変更が可能であるが、本実施形態では、ＨＴＴＰアクセス禁止のケースについて説明する。セキュリティポリシー設定画面９００上で「ＨＴＴＰアクセスを禁止」９０１の有効にしてＯＫボタン９０２が押下されると、クライアントＰＣ１０２から画像形成装置１０１にポリシー設定変更要求が行われる（Ｓ４００３）。

【００３５】

ＨＴＴＰアクセス制御部３０１は、クライアントＰＣ１０２からのＨＴＴＰアクセス要求を解析し、ポリシー設定変更要求のアクセスであると判断した場合は、セキュリティポリシー制御部３０２にポリシー変更通知を行う（Ｓ４００４）。画像形成装置１０１では、図１０に示すようなポリシーデータベース３３１によりセキュリティポリシーが管理されている。

【００３６】

図１０において、ポリシーデータベース３３１は、ＩＤ１００１、ポリシー名称１００２、再設定不可フラグ１００３、及び有効無効フラグ１００４の情報を有する。例えば、ＩＤ「０１」には、ポリシー名称「ＨＴＴＰアクセスを禁止」、再設定不可フラグ「不可能」、有効無効フラグ「有効」のポリシー情報１００５が登録されている。

【００３７】

ＩＤ１００１はセキュリティポリシーを識別するための識別子、ポリシー名称１００２はセキュリティポリシーの名前を表す。再設定不可フラグ１００３は、そのセキュリティ

ポリシーを有効にすると、ネットワーク経由でのポリシーの再設定ができなくなることを表している。この情報はユーザが設定する情報ではなく、セキュリティポリシー制御部３０２が予め決定し、ポリシーデータベース３３１に登録しておく情報である。有効無効フラグ１００４は、ポリシー設定機能３２３によりセキュリティポリシーが設定されたときに、ポリシーを有効化または無効化されるものであり、有効化時に当該ポリシーが適用される。

【００３８】

図４に戻り、Ｓ４００４でポリシーの変更が通知されると、セキュリティポリシー制御部３０２は、ポリシーを解析して当該ポリシーが再設定不可となるポリシーであるかどうかを判断する。その結果、再設定が不可能と判断された場合は利用者に再設定ができなくなるが、このまま変更を反映していいかどうかを確認するために、ＨＴＴＰアクセス制御部３０１にアクセス不可警告画面の表示要求を行う（Ｓ４００５）。

【００３９】

ＨＴＴＰアクセス制御部３０１は、セキュリティポリシー制御部３０２からアクセス不可警告画面の表示要求を受けると、Ｓ４００３のＨＴＴＰリクエストのレスポンスとしてアクセス不可警告画面を要求元に返す（Ｓ４００６）。これにより、クライアントＰＣ１０２のブラウザに図１１に示すアクセス不可警告画面１１００が表示される。このように、セキュリティポリシーを設定すると再設定ができなくなる旨の警告表示を行い、ＯＫボタンが押下されると、クライアントＰＣ１０２からＨＴＴＰアクセス制御部３０１にポリシー変更確定要求が行われる（Ｓ４００７）。

【００４０】

ＨＴＴＰアクセス制御部３０１は、クライアントＰＣ１０２からポリシー変更確定要求が通知されると、現在使用しているポートを閉じて、緊急用のポートを開く。ここでポートの変更を行う理由は、例えばＨＴＴＰアクセスを禁止するセキュリティポリシーの再設定ができなくなるようなポリシーが反映された場合に、特別なアクセス方法によって再設定ができるようにするためである。通常、ＨＴＴＰでは、８０番ポートが使用されるが、ＨＴＴＰアクセスが禁止されることにより、８０番ポートが閉じられる。本実施形態では、緊急用に特別なポート番号を開くことでセキュリティポリシー設定のみを継続させることができる。緊急用のポートについては、予め管理者が知っている前提で固定したポートを開くようにしてもよいし、登録されている管理者のメールアドレスに対してポート番号を通知するような構成でもよい。本実施形態では、前者の固定したポートを開く構成で説明を行う。その後、ＨＴＴＰアクセス制御部３０１は、セキュリティポリシー制御部３０２にポリシー変更確定通知を行う（Ｓ４００８）。Ｓ４００８でポリシーの変更確定が通知されると、セキュリティポリシー制御部３０２では当該ポリシーの適用を行う。

【００４１】

次に、図４におけるＨＴＴＰアクセス制御部３０１の詳細な動作処理について図５を参照して説明する。

【００４２】

図５は、ＨＴＴＰアクセス制御部３０１の動作処理の流れを示すフローチャートである。

【００４３】

ＨＴＴＰアクセス制御部３０１では、アクセス受信機能３１１がＨＴＴＰアクセス要求を受信し（ステップＳ５０１）、アクセス解析機能３１２がＨＴＴＰアクセスの解析を行う（ステップＳ５０２）。アクセス解析機能３１２は解析結果から処理を判断し（ステップＳ５０３）、画面表示のアクセス要求と判断したときは、レスポンス画面を生成してリクエスト元に返す（ステップＳ５０４）。ステップＳ５０３での判定結果がポリシー変更要求の場合は、ポリシー制御機能３１３がセキュリティポリシー制御部３０２に変更要求を実施する（ステップＳ５０５）。ステップＳ５０３での判定結果がポリシー変更確定要求の場合は、ポート制御機能３１４が現在使用しているポートを閉じて、緊急用のポートを開く（ステップＳ５０６）。その後、ポリシー制御機能３１３がセキュリティポリシー

制御部３０２にポリシー変更確定通知を実施する（ステップＳ５０７）。

【００４４】

次に、図４におけるセキュリティポリシー制御部３０２の詳細な動作処理について図６を参照して説明する。

【００４５】

図６は、セキュリティポリシー制御部３０２の動作処理の流れを示すフローチャートである。

【００４６】

セキュリティポリシー制御部３０２は、ポリシー受信機能３２１がポリシー変更要求を受信し（ステップＳ６０１）し、ポリシー解析機能３２２が受信したポリシーの解析を行う（ステップＳ６０２）。ポリシー解析機能３２２は解析結果から処理を判断し（ステップＳ６０３）、ポリシー変更通知と判断したときは、受信したポリシーのポリシーデータベース３３１に登録されている再設定不可フラグ１００３を確認する処理を行う（ステップＳ６０４）。その結果、再設定不可フラグ１００３が「可能」となっている場合は、セキュリティポリシー制御部３０２は、上述した警告表示を行わずにステップＳ６０７のポリシー設定の変更を反映する。一方、再設定不可フラグ１００３が「不可能」となっている場合は、利用者に再設定ができなくなるがこのまま変更を反映していいかどうかを確認するためにＨＴＴＰアクセス制御部３０１に警告表示を要求する（ステップＳ６０５）。このとき、図５には図示していないが、ＨＴＴＰアクセス制御部３０１では、ポリシー制御機能３１３が要求を受け、Ｓ４００３のＨＴＴＰリクエストのレスポンスとしてアクセス不可警告画面を生成して返している。

【００４７】

ステップＳ６０３の判定結果がポリシー変更確定通知の場合、ポリシー設定機能３２３が図１０に示すポリシーデータベース３３１における有効無効フラグ１００４を有効に変更して、ポリシー設定の変更を反映する（ステップＳ６０７）。

【００４８】

次に、上述したセキュリティポリシーの設定変更によりＨＴＴＰアクセスの禁止が設定されたときにクライアントＰＣ１０２と画像形成装置１０１間のアクセス動作について説明する。

【００４９】

図１２は、セキュリティポリシーの再設定ができない状況でアクセスしたときのクライアントＰＣ１０２と画像形成装置１０１間のアクセス動作を示すシーケンス図である。

【００５０】

クライアントＰＣ１０２からブラウザを起動してＵＲＬ欄に画像形成装置１０１のＩＰアドレスを入力すると、クライアントＰＣ１０２から画像形成装置１０１に対してＨＴＴＰアクセス要求が行われる（Ｓ４００１）。通常、ブラウザからＩＰアドレスを入力してアクセスする場合、８０番ポートを使用してアクセスが行われる。ＨＴＴＰアクセスが禁止されている場合、８０番ポートが閉じているため、ＨＴＴＰアクセス制御部３０１は、この要求を受信することができない。そのため、ブラウザがタイムアウトして、図１３に示すように、アクセスできない旨のアクセス不可画面１３００が表示される（Ｓ１２００１）。

【００５１】

図１４は、セキュリティポリシーの再設定ができず、緊急用のポートを使用してアクセスするときのクライアントＰＣ１０２と画像形成装置１０１間の動作を示すシーケンス図である。

【００５２】

クライアントＰＣ１０２からブラウザを起動してＵＲＬ欄に画像形成装置１０１のＩＰアドレスと緊急用のポート番号を入力すると、クライアントＰＣ１０２から画像形成装置１０１に対してＨＴＴＰアクセス要求が行われる（Ｓ１４００１）。例えば、ここで画像形成装置１０１のＩＰアドレスが１９２．１６８．０．１１、緊急用のポート番号が１２

３４番ポートであれば、ｈｔｔｐ：／／１９２．１６８．０．１：１２３４のようにポート番号を直接指定してアクセスを行う。このとき、表示される画面は、通常時は図７に示すログイン画面７００を表示するが、緊急用のポートへのアクセス時はセキュリティポリシーの再設定のみを行わせるために、図１５に示すセキュリティポリシーの設定用のログイン画面１５００を表示する。ここで正しいパスワードが入力されると、図９に示すセキュリティポリシー設定画面９００に遷移する。

【００５３】

セキュリティポリシーの再設定不可の状態を解除するためには、「ＨＴＴＰアクセスを禁止」９０１を「無効」にしてＯＫボタン９０２を押下する。その結果、クライアントＰＣ１０２から画像形成装置１０１にポリシー設定変更要求が行われる。このときのＨＴＴＰアクセス制御部３０１、セキュリティポリシー制御部３０２の処理に関しては通常時と同様であり、Ｓ４００３のポリシー設定要求、Ｓ４００４のポリシー変更通知も同様に行われる。

【００５４】

以上説明したように、本実施形態によれば、セキュリティポリシーの再設定ができなくなった場合であっても、予め設定された緊急用のポートへアクセスすることで、ネットワーク経由でのセキュリティポリシーの再設定が可能となる。

【００５５】

［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。

【００５６】

本第２の実施形態では、セキュリティポリシーの再設定ができなくなった場合に、外部のサーバーからセキュリティポリシーを取得するモードに自動的に切り替える点が上記第１の実施形態と異なる。セキュリティポリシーの設定変更時の処理は、上記第１の実施形態で説明した図４のＳ４００１～Ｓ４００８と同じである。しかしながら、その際のＨＴＴＰアクセス制御部３０１とセキュリティポリシー制御部３０２の内部の動作に差異があるため、その点について説明を行う。

【００５７】

第１の実施形態では、図４のＳ４００７でクライアントＰＣ１０２から画像形成装置１０１にポリシー変更確定要求が送信されると、ＨＴＴＰアクセス制御部３０１は、図５のステップＳ５０６で現在使用中のポートを閉じて、緊急用のポートを開いていた。第２の実施形態では、この処理は行わない。

【００５８】

図１６は、本発明の第２の実施形態におけるセキュリティポリシー制御部３０２の動作処理の流れを示すフローチャートである。なお、図示の処理では、図６と同一のステップにはついては同じ符号を付して、それらの説明を省略する。

【００５９】

セキュリティポリシー制御部３０２は、図４のＳ４００８でポリシー変更確定通知が行われたときに、サーバーから取得するモードに切り替える処理を行う（ステップＳ１６０１）。サーバーから取得するモードとは、上述したクライアントＰＣのブラウザ等から設定変更を受け付けるモードと異なり、ポリシーサーバー１０３に対して定期的にセキュリティポリシーの更新を要求するモードである。

【００６０】

ＨＴＴＰアクセスを禁止する設定変更によりセキュリティポリシーが再設定できなくなる課題に対して、本実施形態では、ポリシーサーバー１０３に予めＨＴＴＰアクセス禁止を無効にしたセキュリティポリシーを保存しておく。そして、画像形成装置１０１からポリシーサーバー１０３への定期的なアクセスにより画像形成装置１０１のセキュリティポリシーが更新される。これにより、セキュリティポリシーの再設定が可能となる。なお、画像形成装置１０１からポリシーサーバー１０３へのアクセスは、予め設定された時間（時刻）に定期的に行われるようにすることが好ましいが、これに限定されるものではない

。
【００６１】
ところで、画像形成装置１０１からポリシーサーバー１０３にアクセスしたときにポリシーサーバー１０３が稼働していない場合は、図１８に示すセキュリティポリシー設定確認画面１８００が表示される。セキュリティポリシー設定確認画面１８００では、サーバーから取得するモードに切り替えてもポリシーサーバー１０３との通信が確認できない場合は処理を継続していいかどうかをユーザに問い合わせる内容になっている。これらの再警告処理は、図４のＳ４００５～Ｓ４００７の処理と同じである。
【００６２】
また、オペレーションパネル２１２からセキュリティポリシーの設定を変更することも可能である。例えば、図１０に示すポリシーデータベース３３１のように、再設定不可フラグ１００３がＨＴＴＰアクセス禁止のみである場合に、ＨＴＴＰアクセス禁止を無効にすることで再設定可能にすることができる。このとき、動作モードはサーバーから取得するモードではなく、外部から設定の変更を受け付けるモードに切り替わる。
【００６３】
図１７は、サーバーから取得するモードにおけるセキュリティポリシー設定時のクライアントＰＣ１０２、画像形成装置１０１、ポリシーサーバー１０３間のアクセス動作を示すシーケンス図である。
【００６４】
ポリシーの再設定ができなくなった場合に、クライアントＰＣ１０２からポリシーサーバー１０３に対して再設定したいポリシーファイルが送信される（Ｓ１７０００）。ポリシーファイルとは、セキュリティポリシーの設定をファイルにしたものでポリシーデータベース３３１の構成である図１０と同等の設定値を持つ。ポリシーファイルの設定値であるＩＤ１００１、ポリシー名称１００２、再設定不可フラグ１００３の値は予め決められており変更することはできない。変更可能な設定値は、有効無効フラグ１００４の値である。例えば、ポリシー情報１００５の「ＨＴＴＰアクセスを禁止」が有効で再設定が不可能となっている場合は、「ＨＴＴＰアクセスを禁止」を無効にしたポリシーファイルをポリシーサーバー１０３に送信しておくことで再設定不可能な状態を解除することができる。
【００６５】
ポリシーファイルには、サーバーから取得する時間等を設定することが可能である。画像形成装置１０１がポリシーサーバー１０３からポリシーファイルを取得する時間を、例えば深夜０時とポリシーファイルに設定しておくと、このポリシーファイルを取得した画像形成装置１０１がポリシーサーバー１０３へのアクセス時間を変更する。
【００６６】
セキュリティポリシー制御部３０２は、予め決められた時間になると、セキュリティポリシーを更新するために、ポリシー設定変更要求をＨＴＴＰアクセス制御部３０１に送信する（Ｓ１７００１）。
【００６７】
ＨＴＴＰアクセス制御部３０１は、ポリシー設定変更要求を受信すると、ポリシーサーバー１０３に対してポリシー取得要求を行う（Ｓ１７００２）。
【００６８】
ポリシーサーバー１０３は、ＨＴＴＰアクセス制御部３０１からポリシー取得要求を受けると、画像形成装置１０１に該当するポリシーファイルを探索し、該当するポリシーファイルを配信する（Ｓ１７００３）。
【００６９】
ＨＴＴＰアクセス制御部３０１は、ポリシーサーバー１０３からポリシーファイルを受け取ると、セキュリティポリシー制御部３０２にポリシー設定要求を行う（Ｓ１７００４）。
【００７０】

セキュリティポリシー制御部３０２は、ＨＴＴＰアクセス制御部３０１から設定要求を受けると、当該ポリシーファイルの設定に従ってセキュリティポリシーの変更を反映する。

【００７１】

以上説明したように、本実施形態によれば、ポリシーサーバー１０３にセキュリティポリシーの再設定が可能なセキュリティポリシーのポリシーファイルを予め保存しておく。そして、画像形成装置１０１のセキュリティポリシーの再設定ができなくなった場合にはサーバーから取得するモードに切り替える。そして、ポリシーサーバー１０３から取得した、再設定が可能なセキュリティポリシーにより画像形成装置１０１のセキュリティポリシーを更新する。これにより、ネットワーク経由でのセキュリティポリシーの再設定が可能となる。

【００７２】

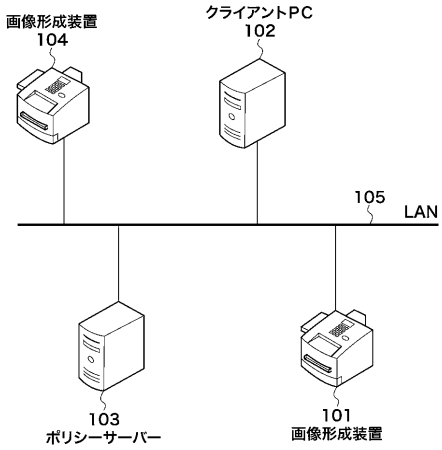
また、本発明は、以下の処理を実行することによっても実現される。即ち、上述した実施形態の機能を実現するソフトウェア（プログラム）を、ネットワークまたは各種記憶媒体を介してシステム或いは装置に供給し、そのシステム或いは装置のコンピュータ（またはＣＰＵやＭＰＵ等）がプログラムを読み出して実行する処理である。

【符号の説明】

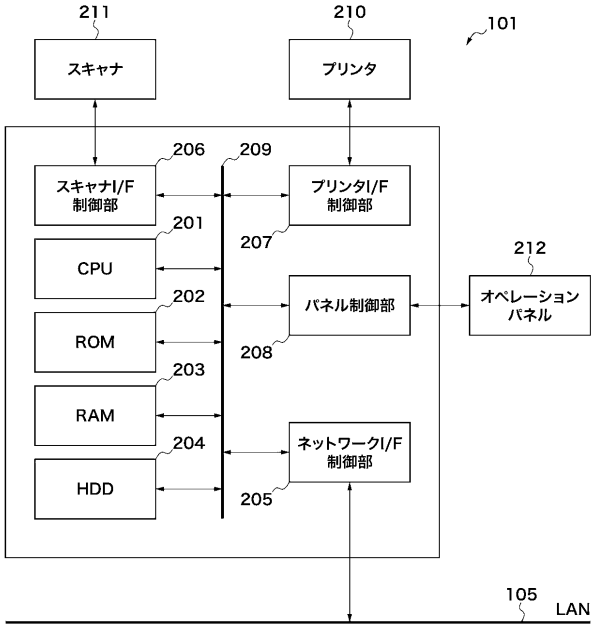
【００７３】

１０１　画像形成装置
１０２　クライアントＰＣ
１０３　ポリシーサーバー
２０１　ＣＰＵ
３０１　ＨＴＴＰアクセス制御部
３０２　セキュリティポリシー制御部
３３１　アクセス受信機能
３１３　ポリシー制御機能
３１４　ポート制御機能
３３１　ポリシーデータベース

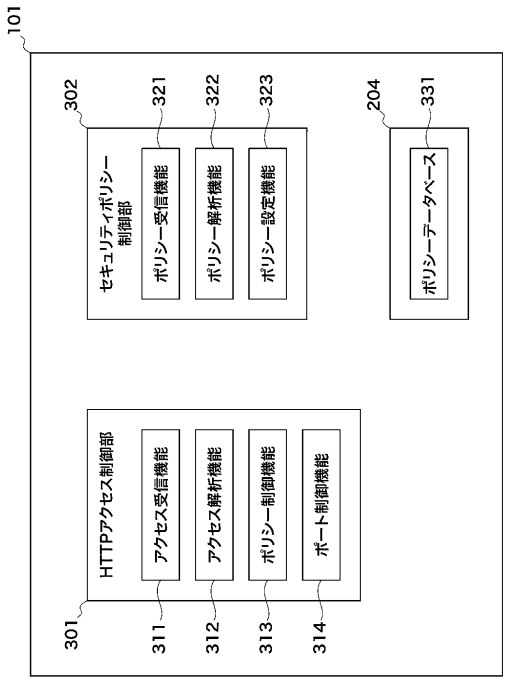
【図１】


画像形成装置
104
クライアントPC
102
105
LAN
103
ポリシーサーバー
101
画像形成装置

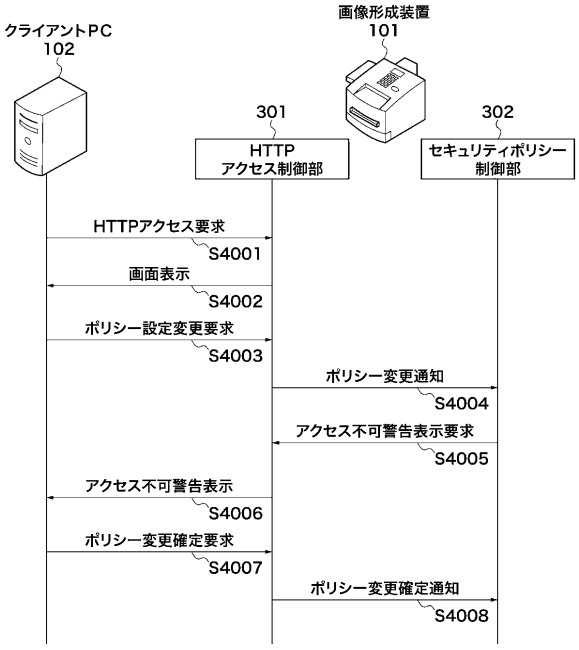
【図２】


211
210
101
スキャナ
プリンタ
206
209
スキャナI/F
制御部
プリンタI/F
制御部
201
207
CPU
212
202
パネル制御部
オペレーション
パネル
ROM
208
203
RAM
204
ネットワークI/F
制御部
HDD
205
105
LAN

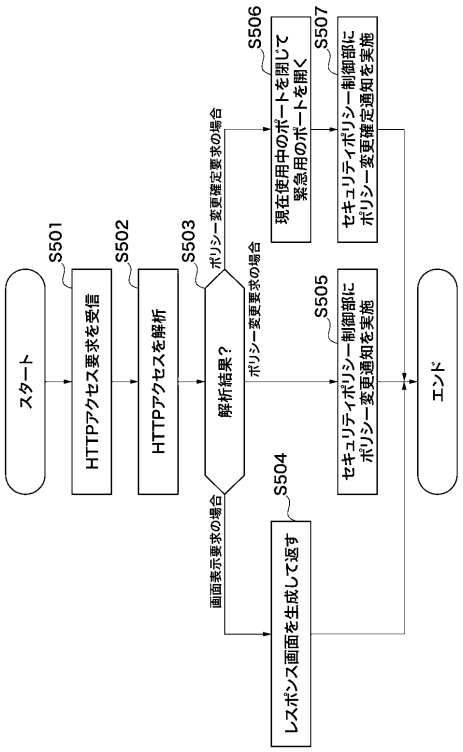
【図３】


101
302
321
322
323
204
331
セキュリティポリシー
制御部
ポリシー受信機能
ポリシー解析機能
ポリシー設定機能
ポリシーデータベース
HTTPアクセス制御部
アクセス受信機能
アクセス解析機能
ポリシー制御機能
ポート制御機能
301
311
312
313
314

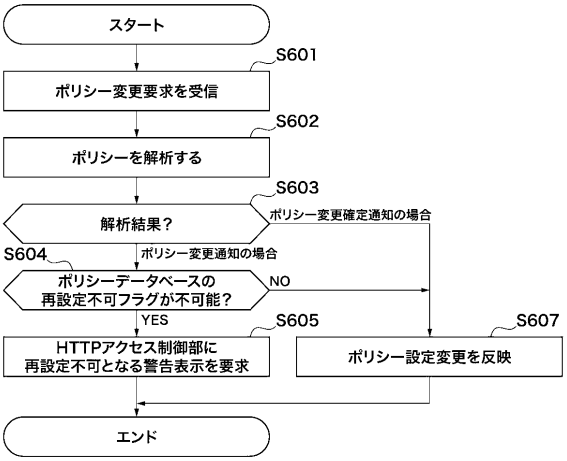
【図４】


クライアントPC
102
画像形成装置
101
301
302
HTTP
アクセス制御部
セキュリティポリシー
制御部
HTTPアクセス要求
S4001
画面表示
S4002
ポリシー設定変更要求
S4003
ポリシー変更通知
S4004
アクセス不可警告表示要求
S4005
アクセス不可警告表示
S4006
ポリシー変更確定要求
S4007
ポリシー変更確定通知
S4008

【図５】


スタート
S501
HTTPアクセス要求を受信
S502
HTTPアクセスを解析
S503
解析結果？
ポリシー変更確定要求の場合
ポリシー変更要求の場合
画面表示要求の場合
S506
現在使用中のポートを閉じて緊急用のポートを開く
S507
セキュリティポリシー制御部にポリシー変更確定通知を実施
S505
セキュリティポリシー制御部にポリシー変更通知を実施
S504
レスポンス画面を生成して返す
エンド

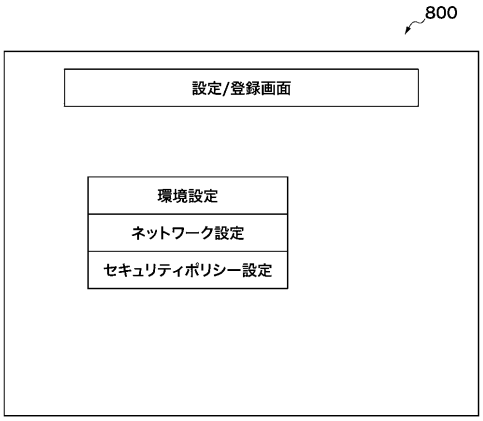
【図６】


スタート
S601
ポリシー変更要求を受信
S602
ポリシーを解析する
S603
解析結果？
ポリシー変更確定通知の場合
ポリシー変更通知の場合
S604
ポリシーデータベースの再設定不可フラグが不可能？
NO
YES
S605
HTTPアクセス制御部に再設定不可となる警告表示を要求
S607
ポリシー設定変更を反映
エンド

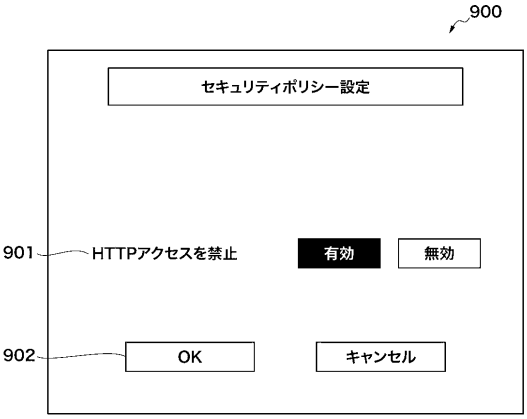
【図７】


700
MFP 01234
ID/パスワードを入力してログインして下さい。
ID
パスワード
ログイン

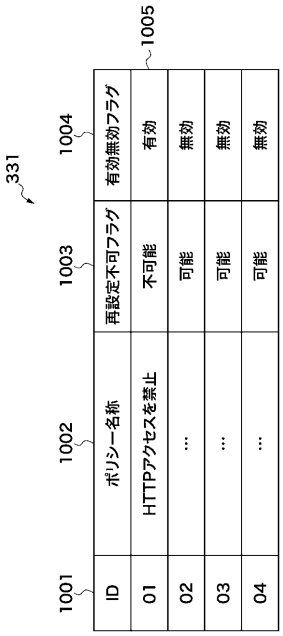
【図８】


800
設定/登録画面
環境設定
ネットワーク設定
セキュリティポリシー設定

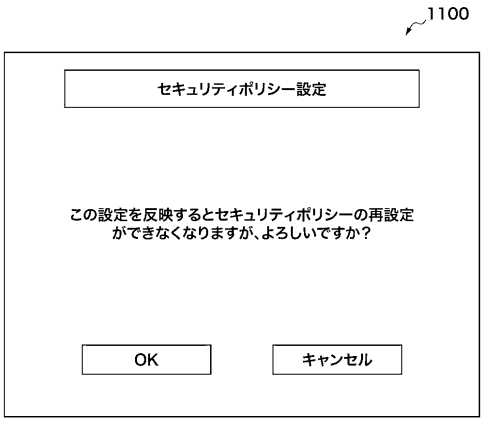
【図９】


900
セキュリティポリシー設定
901
HTTPアクセスを禁止
有効
無効
902
OK
キャンセル

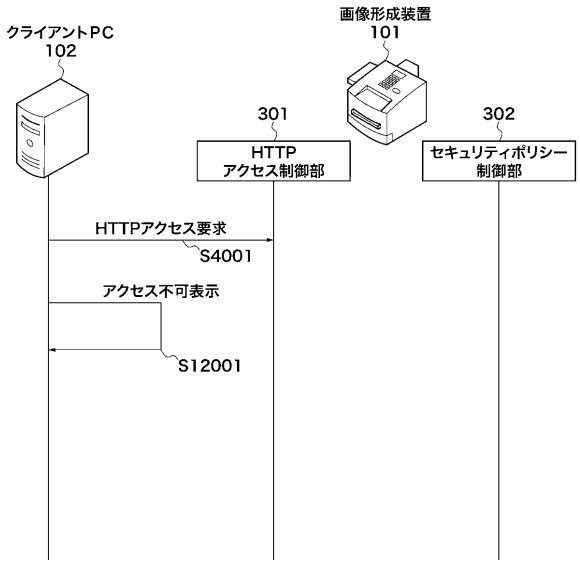
【図１０】



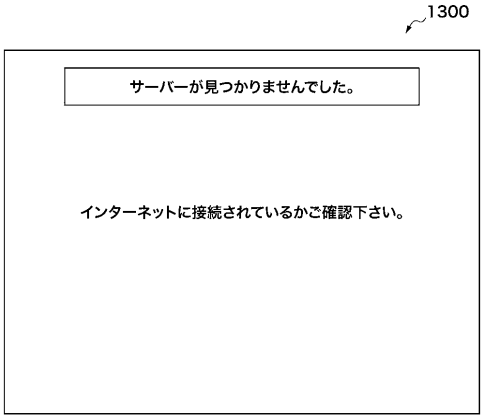
【図１１】



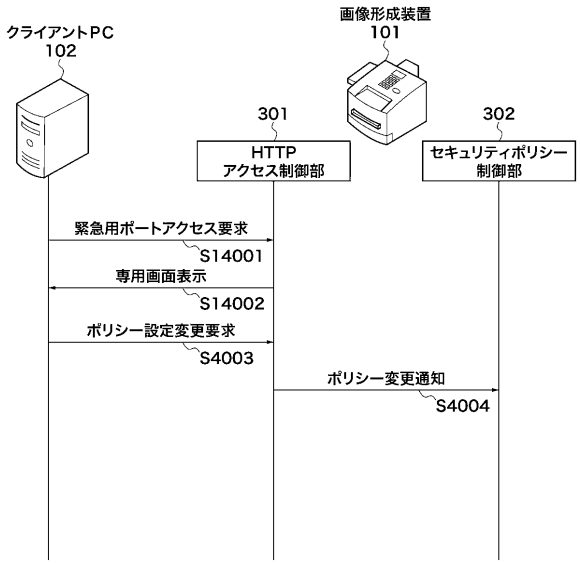
【図１２】



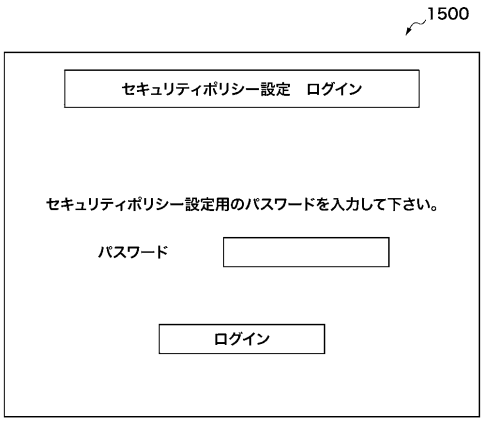
【図１３】



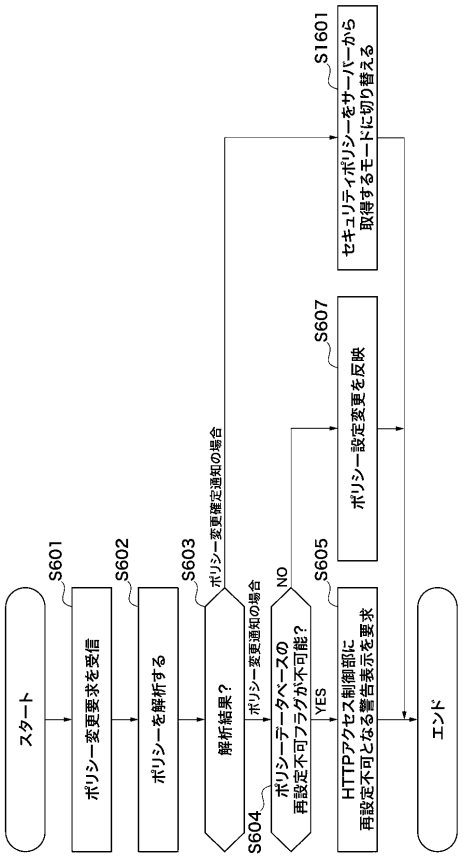
【図１４】



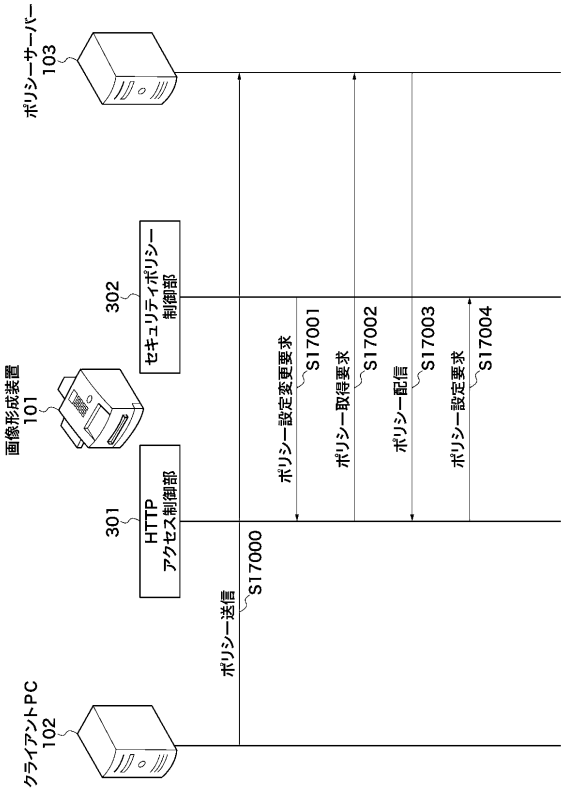
【図１５】



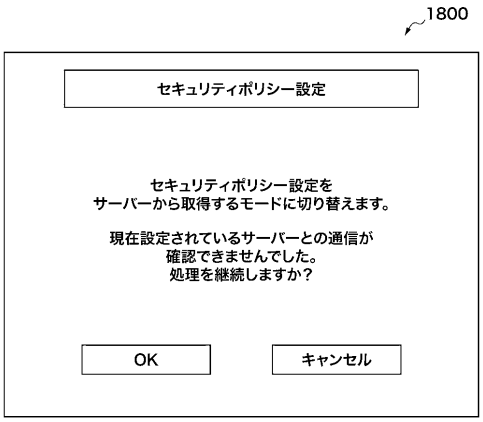
【図１６】



【図１７】



【図１８】


1800
セキュリティポリシー設定
セキュリティポリシー設定を
サーバーから取得するモードに切り替えます。
現在設定されているサーバーとの通信が
確認できませんでした。
処理を継続しますか？
OK
キャンセル

フロントページの続き

(51)Int.Cl. F I
H04N 1/00 (2006.01) H04N 1/00 107Z

(56)参考文献 特開２００５－２５０９６５（ＪＰ，Ａ）
特開２００７－０１１７００（ＪＰ，Ａ）
特開２００９－０３３５４０（ＪＰ，Ａ）
特開２００５－０７２６４４（ＪＰ，Ａ）
特開２０１２－１７３８４１（ＪＰ，Ａ）
特開２０１１－１２８６６２（ＪＰ，Ａ）
特開２０１２－１１８７５７（ＪＰ，Ａ）
特開２０１０－２５３７２４（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ ２１／