(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2011-128662
(P2011-128662A)
(43)公開日　平成23年6月30日(2011.6.30)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	560B	5B017
		G06F	12/14	520B	

審査請求 未請求　請求項の数 11　ＯＬ　（全 12 頁）

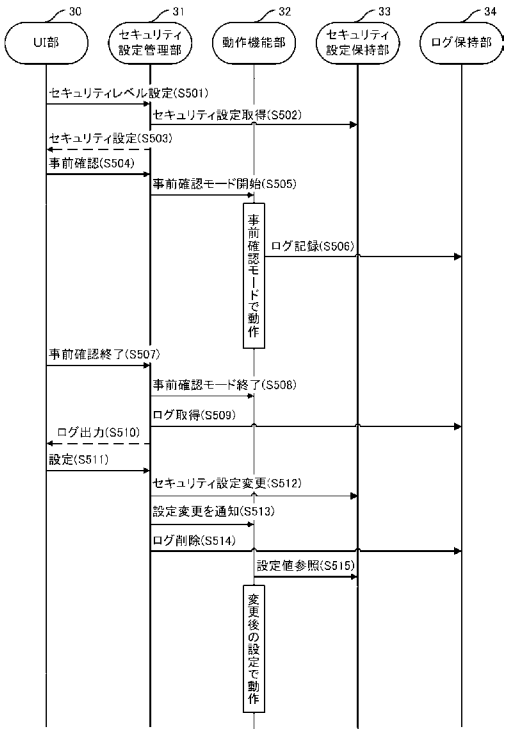
(21)出願番号　特願2009-282225 (P2009-282225)
(22)出願日　平成21年12月11日 (2009.12.11)
(31)優先権主張番号　特願2009-263346 (P2009-263346)
(32)優先日　平成21年11月18日 (2009.11.18)
(33)優先権主張国　日本国 (JP)

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

最終頁に続く

(54)【発明の名称】情報処理装置及びそのセキュリティ設定方法

(57)【要約】
【課題】セキュリティ設定の変更に起因する影響をユーザが事前に認識した上で変更を行うか否かを選択可能である情報処理装置及びそのセキュリティ設定方法を提供する。
【解決手段】ユーザからの指示を受け付ける受付手段と、受付手段が受け付けたユーザからの指示に基づいて、情報処理装置のセキュリティに関する設定を行う設定手段と、受付手段がセキュリティに関する設定を変更する指示を受け付けたことに従って設定手段がセキュリティに関する設定を変更する前に、情報処理装置で発生する事象のうちセキュリティに関する設定の変更を行う場合と行わない場合とで内容が異なる事象を記録する記録手段と、記録手段が記録した事象をユーザへ通知する通知手段と、を備える。
【選択図】図５



【特許請求の範囲】
【請求項１】
情報処理装置であって、
ユーザからの指示を受け付ける受付手段と、
前記受付手段が受け付けたユーザからの指示に基づいて、前記情報処理装置のセキュリティに関する設定を行う設定手段と、
前記受付手段が前記セキュリティに関する設定を変更する指示を受け付けたことに従って前記設定手段が前記セキュリティに関する設定を変更する前に、前記情報処理装置で発生する事象のうち前記セキュリティに関する設定の変更を行う場合と行わない場合とで内容が異なる事象を記録する記録手段と、
前記記録手段が記録した事象を前記ユーザへ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装置。
【請求項２】
前記設定手段は前記通知手段が前記記録した事象を前記ユーザへ通知した後、ユーザからの指示に従って前記セキュリティに関する設定を変更することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記設定手段は複数段階のセキュリティレベルの１つを選択することが可能であり、前記セキュリティレベルを変更することで前記セキュリティに関する設定の変更を行うことを特徴とする請求項１または２に記載の情報処理装置。
【請求項４】
前記記録手段が前記セキュリティに関する設定の変更を行う場合と行わない場合とで内容が異なる事象を記録しなかった場合、前記設定手段は前記受付手段が受け付けた指示に従って前記セキュリティに関する設定を変更することを特徴とする請求項１に記載の情報処理装置。
【請求項５】
前記受付手段が受け付けた前記セキュリティに関する設定を変更する指示は、前記情報処理装置のネットワークポートを閉じている状態から開いた状態に変更する指示であり、
前記記録手段は前記ネットワークポートが閉じている状態において前記ネットワークポートに対するアクセスを記録することを特徴とする請求項１に記載の情報処理装置。
【請求項６】
前記設定手段は、前記記録手段が記録した前記アクセスを前記ユーザへ通知した後、前記ユーザからの指示に従って前記ネットワークポートを開くよう設定することを特徴とする請求項５に記載の情報処理装置。
【請求項７】
前記受付手段が受け付けた前記セキュリティに関する設定を変更する指示は、前記情報処理装置のネットワークポートを開いている状態から閉じた状態に変更する指示であり、
前記記録手段は前記ネットワークポートが開いている状態において前記ネットワークポートに対するアクセスを記録することを特徴とする請求項１に記載の情報処理装置。
【請求項８】
前記設定手段は、前記記録手段が記録した前記アクセスを前記ユーザへ通知した後、前記ユーザからの指示に従って前記ネットワークポートを閉じるよう設定することを特徴とする請求項７に記載の情報処理装置。
【請求項９】
前記受付手段はパスワードの入力を受け付けることが可能であり、
前記受付手段が受け付けた前記セキュリティに関する設定を変更する指示は、前記受付手段が入力を受け付けるパスワードに必要な文字数を変更する指示であり、
前記記録手段は前記必要な文字数が変更されることによって前記受付手段が受付不可となるようなパスワードの入力があったことを、前記必要な文字数を変更する前に記録することを特徴とする請求項１に記載の情報処理装置。

【請求項１０】
情報処理装置のセキュリティ設定方法であって、
ユーザからの指示を受け付ける受付工程と、
前記受付工程で受け付けたユーザからの指示に基づいて、セキュリティに関する設定を行う設定工程と、
前記受付工程で前記セキュリティに関する設定を変更する指示を受け付けたことに従って前記設定工程で前記セキュリティに関する設定を変更する前に、前記情報処理装置で発生する事象のうち前記セキュリティに関する設定の変更を行う場合と行わない場合とで内容が異なる事象を記録する記録工程と、
前記記録工程で記録した事象を前記ユーザへ通知する通知工程と、
を備えることを特徴とする情報処理装置のセキュリティ設定方法。
【請求項１１】
コンピュータを請求項１乃至９のいずれか１項に記載の情報処理装置の各手段として機能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、ユーザが複数段階のセキュリティレベルのうちの１つを選択可能である情報処理装置及びそのセキュリティ設定方法に関する。
【背景技術】
【０００２】
情報処理装置（例えば、ＭＦＰ等に組み込まれる）では、情報漏洩、外部からの不正アクセス防止等の各種セキュリティ対策のために、セキュリティに関する各種設定項目を設け、この設定に従って動作を切り替える技術がある。また、セキュリティレベルを設定するだけで、複数のセキュリティ関連の設定項目を一括して設定可能な技術がある（例えば、特許文献１）。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２００７－１２８２３４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかしながら、セキュリティ関連の設定項目の中には、設定変更によりどのような影響が出るかを判断することが困難な項目もある。例えば、ネットワークポートのＯＮ／ＯＦＦ設定等は、事前に各ポートの使用状況を把握しておかないと影響が判断できない。また、セキュリティレベルを設定するだけで、複数のセキュリティ設定項目を一括して設定可能とした装置では、個々の設定の内容を良く確認せずに一括設定されてしまう可能性がある。この場合、設定変更してしまった後で、利用していたホストやホスト・アプリケーションが使用不可能となる等のように、予期しない事態を招きかねない。
【０００５】
本発明は、上記問題点に鑑みてなされたものであり、セキュリティ設定の変更に起因する影響をユーザが事前に認識した上で変更を行うか否かを選択可能である情報処理装置及びそのセキュリティ設定方法を提供するものである。
【課題を解決するための手段】
【０００６】
上記課題を解決するため、本発明に係る情報処理装置は、ユーザからの指示を受け付ける受付手段と、前記受付手段が受け付けたユーザからの指示に基づいて、前記情報処理装置のセキュリティに関する設定を行う設定手段と、前記受付手段が前記セキュリティに関する設定を変更する指示を受け付けたことに従って前記設定手段が前記セキュリティに関

する設定を変更する前に、前記情報処理装置で発生する事象のうち前記セキュリティに関する設定の変更を行う場合と行わない場合とで内容が異なる事象を記録する記録手段と、前記記録手段が記録した事象を前記ユーザへ通知する通知手段と、を備える。

【発明の効果】

【０００７】

本発明によれば、セキュリティ設定の変更に起因する影響をユーザが事前に認識した上で変更を行うか否かを選択可能にすることができる。

【図面の簡単な説明】

【０００８】

【図１】本発明の一実施形態に係る情報処理システムを示す図である。

【図２】情報処理装置１のハードウェア構成を示す図である。

【図３】情報処理装置１のソフトウェア構成を示す図である。

【図４】セキュリティ設定保持部３３が保持する設定値の一例を示す図である。

【図５】情報処理装置１の処理手順を示す図である。

【図６】セキュリティ設定動作時の操作画面の遷移例を示す図である。

【図７】セキュリティ設定管理部３１の詳細な処理手順を示す図である。

【図８】動作機能部３２の詳細な処理手順を示す図である。

【図９】動作機能部３２の事前確認モード時の処理手順を示す図である。

【図１０】差分情報及びログの一例を示す図である。

【発明を実施するための形態】

【０００９】

以下、図面を参照して本発明の実施形態を詳細に説明する。なお、以下の実施形態は特許請求の範囲を限定するものでなく、また、実施形態で説明される特徴の組み合わせの全てが発明の解決手段に必須のものとは限らない。

【００１０】

情報処理システムは、図１で示すように、ネットワーク４に接続する情報処理装置１（例えば、ＭＦＰ等）と、ネットワーク４に接続するホスト２、３（例えば、パーソナルコンピュータ）とを備える。情報処理装置１は、ネットワーク４を介して、ホスト２、３との間でデータの送受信を行い、その結果に基づいて種々の処理（例えば、画像形成処理）を行う。なお、情報処理装置１は、ＭＦＰ全体の構成を備えることは必須ではなく、ＭＦＰに組み込まれる制御装置として機能するものであっても構わない。

【００１１】

［情報処理装置１のハードウェア構成（図２）］

情報処理装置１は、装置全体を制御する制御部１０（コントローラ）、原稿画像を読み取るスキャナ１３、印刷を行うプリンタ１２、及びユーザからの指示入力を受け付け、また、表示出力を行うためのパネル１１（提示手段）を備える。

【００１２】

制御部１０は、パネルＩ／Ｆ１０３、ＦＡＸモデム１０４、画像処理部１０５、ＨＤＤ１０６、プリンタＩ／Ｆ１０７、スキャナＩ／Ｆ１０８、ネットワークＩ／Ｆ１０９、ＣＰＵ１０１、ＲＯＭ１１０、ＲＡＭ１１１を備える。

【００１３】

パネルＩ／Ｆ１０３は、パネル１１に接続し、パネル１１より入力されたユーザの指示をＣＰＵ１０１に通知したり、ＣＰＵ１０１からの指示を受けて、画面情報をパネル１１に出力する。

【００１４】

ＦＡＸモデム１０４は、公衆回線に接続する他のファクシミリとの間で、ＦＡＸの送受信を行う。スキャナＩ／Ｆ１０８は、スキャナ１３に接続し、スキャナ１３で読み取った画像データをＨＤＤ１０６に格納する。

【００１５】

プリンタＩ／Ｆ１０７は、プリンタ１２に接続し、ＨＤＤ１０６に格納されている画像

データをプリンタ１２に出力する。ネットワークＩ／Ｆ１０９は、ネットワーク４に接続する他の装置との間で、データの送受信を行う。

【００１６】

ＨＤＤ１０６は、システムソフトウェア、画像データ、後述のセキュリティ設定保持部３３及び後述のログ保持部３４を格納する。画像処理部１０５は、ＣＰＵ１０１の指示に基づいて、画像入出力の際に、該画像に対して種々の画像処理を行う。

【００１７】

ＣＰＵ１０１は、ＨＤＤ１０６に格納されたシステムソフトウェアに従って、制御部１０の各部を制御する。ＲＯＭ１１０は、ブートＲＯＭとして構成され、システムのブートプログラムを格納する。ＲＡＭ１１１は、ＣＰＵ１０１が動作するためのシステムワークメモリであり、画像データを一時的に格納するための画像メモリでもある。

【００１８】

［情報処理装置１のソフトウェア構成（図３の上段図）］

情報処理装置１は、ユーザ・インターフェース部３０（以下、ＵＩ部と略す）、セキュリティ設定管理部３１、動作機能部３２（ネットワーク機能部）、セキュリティ設定保持部３３及びログ保持部３４を備える。

【００１９】

ＵＩ部３０は、パネル１１を介してユーザからの要求を受け付け、また、操作画面をパネル１１に表示する。セキュリティ設定保持部３３は、セキュリティに関する各種設定を保持する。動作機能部３２は、セキュリティ設定保持部３３に保持されたセキュリティ設定に基づいて動作する所定の機能部である。動作機能部３２は、本実施例では、ネットワーク４に接続する他の機器（ホスト２、３）との間で通信を行うネットワーク機能部として機能する。

【００２０】

ログ保持部３４は、動作機能部３２が後述の事前確認モード（第２のモード）で動作した場合に発生した事象をログとして保持する。事前確認モードとは、変更後の設定で動作していたらどのような影響が発生するかを、事前に確認できるようにした動作モードである。これに対して、事前確認を省略し、即座に設定変更を反映するモードを通常モード（第１のモード）とする。セキュリティ設定管理部３１は、ＵＩ部３０及び動作機能部３２との間で情報の送受信を行うことにより、セキュリティ設定動作全体を管理する。

【００２１】

セキュリティ設定保持部３３は、複数段階のセキュリティレベルに応じた制限情報を、アクセスが想定されるアドレス毎に予め記憶している。例えば、セキュリティ設定保持部３３は、図４で示す通り、ネットワークポート５０１～５０３毎に、該ネットワークポートの現在の設定値（ＯＮ：開いた状態／ＯＦＦ：閉じた状態）と、複数段階のセキュリティレベル１～３に対応する既定値とを保持している。

【００２２】

なお、ＵＩ部３０、セキュリティ設定管理部３１及び動作機能部３２の処理は、ＨＤＤ１０６に格納されているシステムソフトウェアに基づいて、ＣＰＵ１０１によって実行される。また、セキュリティ設定保持部３３及びログ保持部３４は、ＨＤＤ１０６に格納される。

【００２３】

［情報処理装置１の処理手順（図５）］

情報処理装置１は、セキュリティ設定動作時に各機能部間で次のような処理を行う。まず、ＵＩ部３０が、セキュリティ設定管理部３１に、セキュリティレベル設定動作の開始を通知する（Ｓ５０１）。セキュリティ設定管理部３１は、セキュリティ設定保持部３３が保持する設定値を取得し（Ｓ５０２）、取得した設定値をＵＩ部３０に送信する（Ｓ５０３）。

【００２４】

ＵＩ部３０は、セキュリティ設定の初期画面６１（図６参照）をパネル１１に表示する

。初期画面６１でユーザにより「事前確認する」ボタンが押下されると、ＵＩ部３０は、その旨の信号をセキュリティ設定管理部３１に送信する（Ｓ５０４）。そして、セキュリティ設定管理部３１は、動作機能部３２に事前確認モードの開始を通知する（Ｓ５０５）。

【００２５】

動作機能部３２は、事前確認モードでの動作を開始し、この間所定の事象が発生した場合、その内容をログとしてログ保持部３４に記録する（Ｓ５０６）。そして、事前確認モード中の画面６３（図６参照）で、ユーザにより「事前確認終了」ボタンが押下されると、ＵＩ部３０は、その旨の信号をセキュリティ設定管理部３１に送信する（Ｓ５０７）。そして、セキュリティ設定管理部３１は、動作機能部３２に事前確認モード終了を通知する（Ｓ５０８）。動作機能部３２は、事前確認モードの動作を終了し、次の指示を待機する。

【００２６】

セキュリティ設定管理部３１は、ログ保持部３４が保持するログを取得して（Ｓ５０９）、ＵＩ部３０に出力する（Ｓ５１０）。ＵＩ部３０は、事前確認モードの事前確認結果画面６４（図６参照）をパネル１１に表示する。

【００２７】

事前確認結果画面６４で、ユーザにより「設定する」ボタンが押下されると、ＵＩ部３０は、その旨の信号をセキュリティ設定管理部３１に送信する（Ｓ５１１）。そして、セキュリティ設定管理部３１は、セキュリティ設定保持部３３が保持する設定値を変更し（Ｓ５１２）、設定変更したことを動作機能部３２に通知する（Ｓ５１３）。

【００２８】

最後に、セキュリティ設定管理部３１は、ログ保持部３４が保持するログを削除して（Ｓ５１４）、セキュリティ設定動作を終了する。動作機能部３２は、変更されたセキュリティ設定保持部３３が保持する設定値を参照し（Ｓ５１５）、変更後の設定で動作を開始する。

【００２９】

（セキュリティ設定管理部３１の詳細な処理手順（図７））

セキュリティ設定管理部３１は、ＵＩ部３０からセキュリティレベル設定処理の開始を示す信号を受信すると（Ｓ５０１）、次のような処理を開始する。まず、セキュリティ設定管理部３１は、セキュリティ設定保持部３３からセキュリティ設定値を取得し、取得した設定値をＵＩ部３０に送信し（Ｓ７０１、Ｓ５０３）、ＵＩ部３０からの通知を待つ。

【００３０】

そして、セキュリティ設定管理部３１は、ＵＩ部３０からの通知を受けると、その通知が事前確認モードを示すか否かを判定する（Ｓ７０２）。ＵＩ部３０からの通知が事前確認モードでなく、通常モードを示す場合には、セキュリティ設定管理部３１は、セキュリティ設定保持部３３が保持する各項目の「現在の設定値」を、変更後のセキュリティレベルの既定値に更新する（Ｓ７０３）。続いて、セキュリティ設定管理部３１は、動作機能部３２に設定変更したことを通知して（Ｓ７０４）、処理を終了する。

【００３１】

一方、ＵＩ部３０からの通知が事前確認モードを示す場合には、セキュリティ設定管理部３１は、セキュリティ設定保持部３３の「現在の設定値」と、変更後のセキュリティレベルの既定値との差分情報を抽出する（Ｓ７０５）。例えば、セキュリティ設定保持部３３が、図４で示すようなセキュリティレベルの設定値を「現在の設定値」として保持している場合を想定する。この場合、変更後のセキュリティレベルが２に指定されると、実際にアクセスがあったアドレス（ポート番号５０１）及び変更後のセキュリティレベル２に対応する制限情報（ＯＮ又はＯＦＦ）を参照することにより、図１０の上段図に示すような差分情報が抽出される。

【００３２】

なお、本実施例では、セキュリティレベルの変更に連動して、各設定項目が変更される

例を想定するが、各設定項目を個別に変更した場合も、同様に差分情報を抽出して所望の処理を行うことができる。

【００３３】

セキュリティ設定管理部３１は、動作機能部３２にこの差分情報を送信すると共に、事前確認モードが開始された旨を通知する（Ｓ７０６、Ｓ５０５）。そして、セキュリティ設定管理部３１は、ＵＩ部３０から事前確認モードが終了した旨の通知を受信したか否かを判定する（Ｓ７０７）。通知を受信していない場合には、セキュリティ設定管理部３１は、待機を継続する。通知を受信した場合（Ｓ５０７）には、セキュリティ設定管理部３１は、動作機能部３２に事前確認モードが終了した旨を通知する（Ｓ７０８、Ｓ５０８）。

【００３４】

次に、セキュリティ設定管理部３１は、ログ保持部３４が保持するログを取得してＵＩ部３０に出力し（Ｓ７０９、Ｓ５１０）、ＵＩ部３０からの指示を待つ。そして、ＵＩ部３０からの指示を受信した場合には、セキュリティ設定管理部３１は、当該指示が設定する旨を示すか否かを判定する（Ｓ７１０）。すなわち、ユーザが事前確認結果画面６４（図６参照）に表示された情報に基づいて、「設定する」ボタンを押下したか否かが判定される。

【００３５】

当該通知が設定する旨を示す場合には、セキュリティ設定管理部３１は、Ｓ７０３及びＳ７０４と同様に、セキュリティ設定保持部３３が保持する設定値を更新し（Ｓ７１１、Ｓ５１２）、動作機能部３２に設定変更したことを通知する（Ｓ７１２、Ｓ５１３）。最後に、セキュリティ設定管理部３１は、ログ保持部３４が保持するログを削除して（Ｓ７１３、Ｓ５１４）、一連の処理を終了する。

【００３６】

（動作機能部３２の詳細な処理手順（図８））

動作機能部３２は、セキュリティ設定管理部３１から動作機能部３２に指示が入力されると、次のような処理を開始する。まず、動作機能部３２は、セキュリティ設定管理部３１から通知された指示が、事前確認モードでの処理を開始すべき旨の指示であるか否かを判定する（Ｓ８０１）。事前確認モードでなく、通常モードでの処理を開始すべき旨の指示である場合には、動作機能部３２は、セキュリティ設定保持部３３から「現在の設定値」を読み込み、その設定で動作を開始する（Ｓ８０２）。

【００３７】

一方、事前確認モードでの処理を開始すべき旨の指示である場合には、動作機能部３２は、セキュリティ設定管理部３１から受信した差分情報に基づいて、事前確認モードで動作を開始する（Ｓ８０３）。動作機能部３２は、事前確認モードで処理を実行中に、仮に変更後の設定で動作した場合には挙動が異なる事象が発生するか否かを判定し、発生すると判定した場合には、これをログ保持部３４に記録する。なお、このログ記録処理については、図９を用いて後述する。

【００３８】

その後、動作機能部３２は、セキュリティ設定管理部３１から事前確認モードが終了した旨が通知されたか否かを判定する（Ｓ８０４）。事前確認モードが終了した旨が通知されていない場合には、通知されるまで待機する。一方、事前確認モードが終了した旨が通知されると、動作機能部３２は、事前確認モードを終了し、通常モードで動作を開始する（Ｓ８０５）。

【００３９】

次に、動作機能部３２の事前確認モードでのログ記録処理を図９を用いて詳細に説明する。動作機能部３２は、ネットワーク４に接続する他の機器（ホスト２、３）からアクセスされると、次のような処理を開始する。

【００４０】

動作機能部３２は、Ｓ８０３でセキュリティ設定管理部３１から受信した差分情報に基

づいて、アクセスされたポートが、セキュリティ設定を変更することによりＯＮからＯＦＦになるポートであるか否かを判定する（Ｓ９１１）。すなわち、動作機能部３２は、アクセスされたポートがセキュリティレベルの変更後にアクセス制限を受けるか否かを判定する。ＯＮからＯＦＦになるポートである場合には、動作機能部３２は、そのアクセスを受け付けるが、設定変更後には受付不可能となるアクセスとして、ログ保持部３４にアクセスを行ったホスト情報をログとして記録する。ここでは、例えば、アクセス元であるホスト２、３のネットワーク上のＩＰアドレス等と関連づけて、設定変更後にアクセス制限を受ける旨を記録する。

【００４１】

一方、ＯＮからＯＦＦになるポートではない場合には、動作機能部３２は、ＯＦＦからＯＮになるポートであるか否かを判定する（Ｓ９１２）。ＯＦＦからＯＮになるポートではない場合には、ポートのＯＮ／ＯＦＦに変更が生じない（設定差分の無いポートである）ため、動作機能部３２は、ログを記録することなく、処理を終了する。一方、動作機能部３２は、ＯＦＦからＯＮになるポートである場合には、動作機能部３２は、アクセスは受け付けないが、設定変更後には受付可能なアクセスとして、ログ保持部３４にそのホスト情報をログとして記録する（Ｓ９１４）。

【００４２】

例えば、図１０の上段図の差分情報で示す差分がある場合、動作機能部３２は、Ｓ９１３において、ポート番号５０１に対してアクセスしてきたホスト情報をログ保持部３４に記録する。また、セキュリティ設定管理部３１がログ保持部３４に保持されたログを取得し、取得したログをＵＩ部３０に出力することにより、ＵＩ部３０が事前確認モードの事前確認結果画面６４を表示することができる（図５のＳ５０９、Ｓ５１０参照）。

【００４３】

以上述べた通り、本実施例によれば、セキュリティ設定の変更に起因する影響をユーザが事前に認識した上で変更を行うか否かを選択可能である情報処理装置及びその制御方法を提供することができる。

【００４４】

なお、上記実施例では、セキュリティ設定として、ネットワークポートのＯＮ／ＯＦＦ設定を例に説明したが、設定変更により動作が異なる設定であれば、同様に適用することができる。例えば、設定変更により、パスワード長が所定の文字数（例えば、５文字）に満たない場合には、アクセス不可能となることとする。この場合、同様に情報処理装置１を事前確認モードで動作させれば、パスワード長が５文字に満たなくてもアクセス可能であるが、設定変更後は受付不可能となるアクセスとしてログ保持部３４に記録される。なお、ここでは、パスワードは、例えば情報処理装置１にログインするための認証情報として用いられるものとする。これにより、ユーザは、設定変更後に受付不可能となるアクセスを事前に把握し、そのようなアクセスを行っているユーザに注意喚起や改善要求を行う等の必要な対策を取ることができる。

【００４５】

また、上記実施例では、事前確認モードが、ユーザからの終了指示を待って終了するものとしたが、予め定めた時間が経過した後に自動的に終了するようにしてもよい。この場合、セキュリティ設定管理部３１は、図７のＳ７０７で、ＵＩ部３０からの「事前確認終了」通知を待つのではなく、予め定めた時間が経過するのを待つようにすればよい。

【００４６】

また、上記実施例では、事前確認モードの動作結果をパネル１１に表示するものとしたが、メールで管理者に通知するようにしてもよい。この場合、図３の上段図に示す情報処理装置１のソフトウェア構成にメール通知機能部３５を追加し（図３の下段図参照）、図５のＳ５１０で、ログをセキュリティ設定管理部３１からメール通知機能部３５に出力するようにすればよい。

【００４７】

また、上記実施例では、事前確認が終了した後、取得したログをＵＩ部３０に出力し、

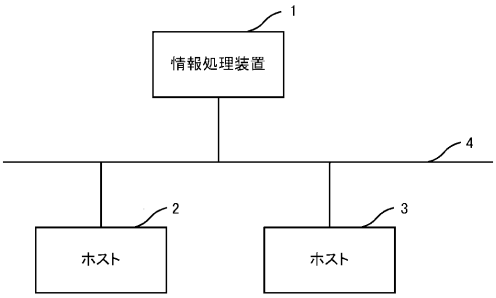
ユーザからのセキュリティ設定の変更を行うか否かの指示に従ってセキュリティ設定の変更を行った。しかし、事前確認の結果ログが記録されなかった場合、ユーザからの指示を待たずにセキュリティ設定の変更を行っても良い。

【００４８】

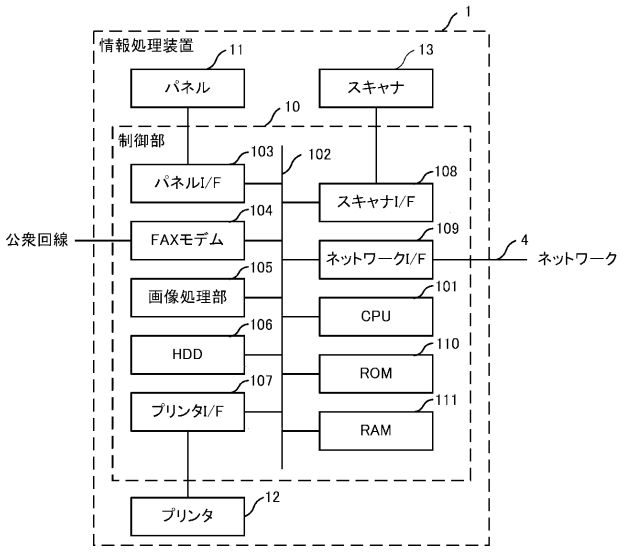
＜他の実施形態＞

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。

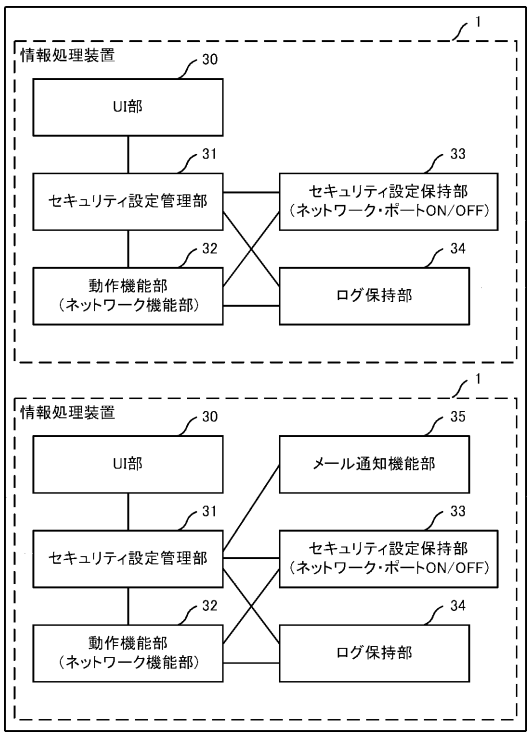
【図１】



【図２】



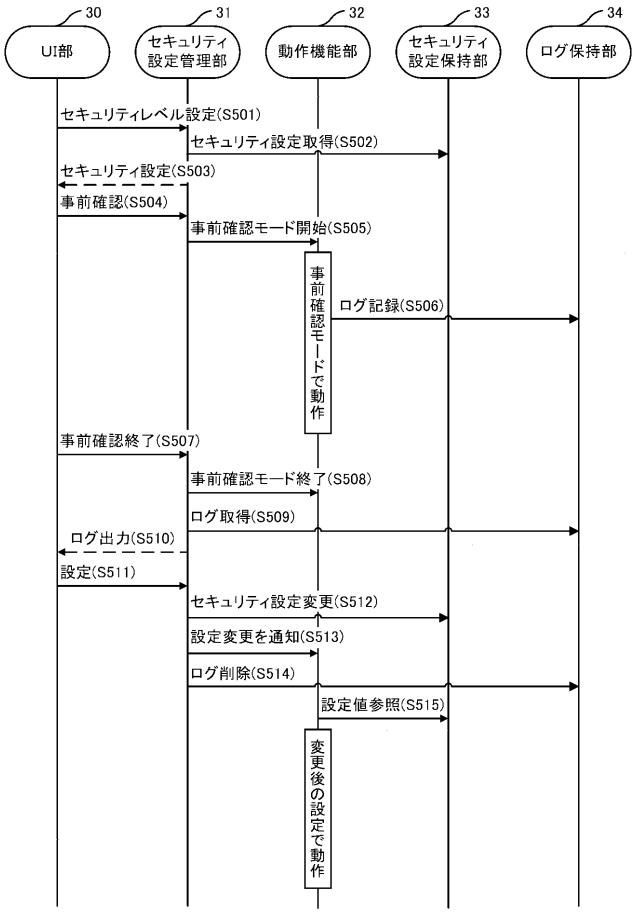
【図３】



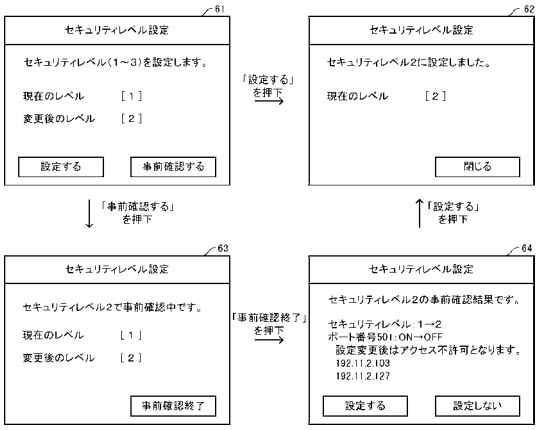
【図４】

ポート番号	現在の設定値	セキュリティレベル		
		レベル1	レベル2	レベル3
501	ON	ON	OFF	OFF
502	ON	ON	ON	OFF
503	ON	ON	ON	ON

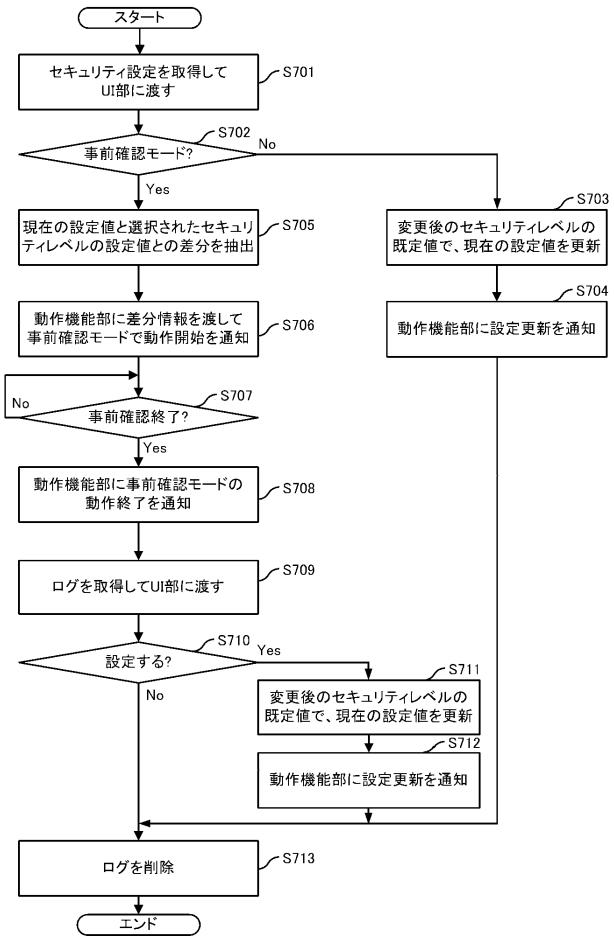
【図５】


30
UI部
31
セキュリティ設定管理部
32
動作機能部
33
セキュリティ設定保持部
34
ログ保持部
セキュリティレベル設定(S501)
セキュリティ設定取得(S502)
セキュリティ設定(S503)
事前確認(S504)
事前確認モード開始(S505)
事前確認モードで動作
ログ記録(S506)
事前確認終了(S507)
事前確認モード終了(S508)
ログ取得(S509)
ログ出力(S510)
設定(S511)
セキュリティ設定変更(S512)
設定変更を通知(S513)
ログ削除(S514)
設定値参照(S515)
変更後の設定で動作

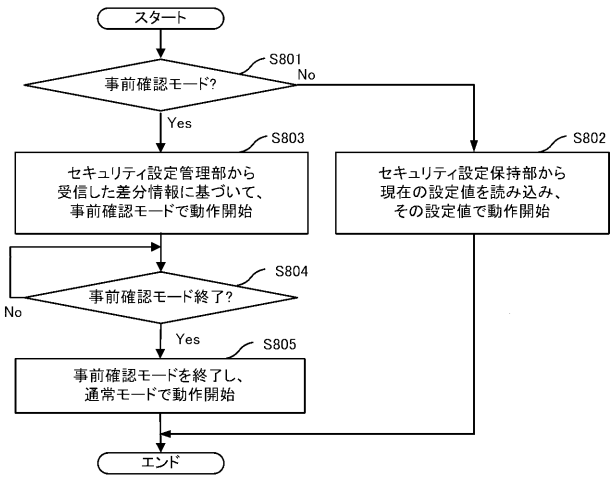
【図６】


61
セキュリティレベル設定
セキュリティレベル(1～3)を設定します。
現在のレベル [1]
変更後のレベル [2]
設定する
事前確認する
「設定する」を押下
62
セキュリティレベル設定
セキュリティレベル2に設定しました。
現在のレベル [2]
閉じる
「事前確認する」を押下
「設定する」を押下
63
セキュリティレベル設定
セキュリティレベル2で事前確認中です。
現在のレベル [1]
変更後のレベル [2]
事前確認終了
「事前確認終了」を押下
64
セキュリティレベル設定
セキュリティレベル2の事前確認結果です。
セキュリティレベル：1→2
ポート番号501：ON→OFF
設定変更後はアクセス不許可となります。
192.11.2.103
192.11.2.127
設定する
設定しない

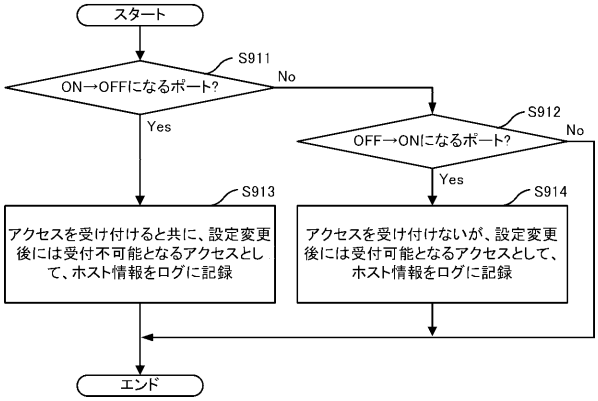
【図７】


スタート
セキュリティ設定を取得して UI部に渡す
S701
事前確認モード?
S702
No
Yes
現在の設定値と選択されたセキュリティレベルの設定値との差分を抽出
S705
動作機能部に差分情報を渡して事前確認モードで動作開始を通知
S706
No
事前確認終了?
S707
Yes
動作機能部に事前確認モードの動作終了を通知
S708
ログを取得してUI部に渡す
S709
設定する?
S710
Yes
No
変更後のセキュリティレベルの既定値で、現在の設定値を更新
S711
動作機能部に設定更新を通知
S712
ログを削除
S713
エンド
変更後のセキュリティレベルの既定値で、現在の設定値を更新
S703
動作機能部に設定更新を通知
S704

【図８】


スタート
事前確認モード?
S801
No
Yes
セキュリティ設定管理部から受信した差分情報に基づいて、事前確認モードで動作開始
S803
セキュリティ設定保持部から現在の設定値を読み込み、その設定値で動作開始
S802
事前確認モード終了?
S804
No
Yes
事前確認モードを終了し、通常モードで動作開始
S805
エンド

【図９】



【図１０】

項目	差分情報
セキュリティレベル	1→2
ポート番号501	ON→OFF

ポート番号	差分情報	アクセス・ホスト情報
501	ON→OFF	192.11.2.103
501	ON→OFF	192.11.2.127

フロントページの続き

(72)発明者　岩舘　政宏
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

Ｆターム(参考) 5B017 AA08　BA06　BB06　CA16