(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6249006号
(P6249006)
(45)発行日　平成29年12月20日(2017.12.20)　(24)登録日　平成29年12月1日(2017.12.1)

(51)Int.Cl.　　F I
G06F 21/31 (2013.01)　　G06F 21/31
G06F 3/12 (2006.01)　　G06F 3/12 322
G06F 3/12 338

請求項の数 26　(全 32 頁)

(21)出願番号　特願2015-203776(P2015-203776)
(22)出願日　平成27年10月15日(2015.10.15)
(65)公開番号　特開2017-76277(P2017-76277A)
(43)公開日　平成29年4月20日(2017.4.20)
審査請求日　平成28年10月20日(2016.10.20)

早期審査対象出願

(73)特許権者　000001270
コニカミノルタ株式会社
東京都千代田区丸の内二丁目７番２号
(74)代理人　100108523
弁理士　中川　雅博
(72)発明者　白石　潤
東京都千代田区丸の内二丁目７番２号　コニカミノルタ株式会社内
(72)発明者　正崎　敏哉
東京都千代田区丸の内二丁目７番２号　コニカミノルタ株式会社内
(72)発明者　西村　亮佑
東京都千代田区丸の内二丁目７番２号　コニカミノルタ株式会社内

最終頁に続く

(54)【発明の名称】セキュリティ情報更新システム、情報処理装置、セキュリティ情報更新方法およびセキュリティ情報更新プログラム

(57)【特許請求の範囲】
【請求項１】
サービス提供サーバーと、複数の情報処理装置と、を含むセキュリティ情報更新システムであって、
前記サービス提供サーバーは、更新日時に更新されるセキュリティ情報と、前記セキュリティ情報の種類を識別するための識別情報との組を記憶する認証情報記憶手段と、
前記複数の情報処理装置のいずれかから受信される識別情報とセキュリティ情報との組と同一の組が前記認証情報記憶手段に記憶されていることを条件に、前記情報処理装置にサービスを提供するサービス提供手段と、を備え、
前記複数の情報処理装置それぞれは、
前記サービス提供サーバーに記憶された前記識別情報と更新日時とを定めたセキュリティポリシーを取得するポリシー取得手段と、
前記サービス提供サーバーに記憶された前記識別情報と同一の識別情報に関連付けてセキュリティ情報を記憶するセキュリティ情報記憶手段と、
前記サービス提供サーバーにより提供されるサービスを受ける処理を実行する場合、前記サービス提供サーバーに記憶された前記識別情報と同一の識別情報と、その識別情報と関連付けて記憶されているセキュリティ情報との組を、前記サービス提供サーバーに送信し、前記サービス提供サーバーによるサービスの提供を受ける処理実行手段と、
前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報を取得する認証情報取得手段と、

前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時以降に、前記セキュリティ情報記憶手段に前記サービス提供サーバーに記憶された前記識別情報と関連付けて記憶されたセキュリティ情報を前記取得されたセキュリティ情報で更新する更新手段と、

前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時以降、前記更新手段により前記取得されたセキュリティ情報で更新されるまで、前記処理実行手段による前記サービス提供サーバーによるサービスの提供を受ける処理の実行を禁止する禁止手段と、を備えた、セキュリティ情報更新システム。

【請求項２】

前記処理実行手段は、前記更新日時が経過した後に前記更新手段により前記セキュリティ情報記憶手段に記憶されたセキュリティ情報が更新されることに応じて、前記禁止手段により実行が禁止されていた処理を実行する、請求項１に記載のセキュリティ情報更新システム。

【請求項３】

前記複数の情報処理装置それぞれは、さらに、前記処理実行手段による前記サービス提供サーバーによるサービスの提供を受ける処理の実行が前記禁止手段により禁止されている間、セキュリティ情報が更新されていないことをユーザーに通知する通知手段を備えた、請求項１または２に記載のセキュリティ情報更新システム。

【請求項４】

前記複数の情報処理装置それぞれは、さらに、前記サービス提供サーバーとの間の通信状態を検出する通信状態検出手段を備え、

前記通知手段は、前記処理実行手段による前記サービス提供サーバーによるサービスの提供を受ける処理の実行が前記禁止手段により禁止されている間に、前記通信状態検出手段により前記サービス提供サーバーとの間の通信ができないことが検出される場合、前記サービス提供サーバーと通信できないことを通知する、請求項３に記載のセキュリティ情報更新システム。

【請求項５】

前記サービス提供サーバーに記憶されたセキュリティ情報を管理する管理サーバーを、さらに備え、

前記管理サーバーは、前記セキュリティポリシーを記憶するポリシー記憶手段を、備え、

前記ポリシー取得手段は、前記管理サーバーから前記管理サーバーに記憶されたセキュリティポリシーを取得する、請求項１～４のいずれかに記載のセキュリティ情報更新システム。

【請求項６】

前記管理サーバーは、さらに、前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時を基準に定まる日時に、前記複数の情報処理装置それぞれに前記識別情報と、前記サービス提供サーバーにおいて更新された後の新たなセキュリティ情報を含む更新指示を送信する更新指示送信手段を備え、

前記認証情報取得手段は、前記管理サーバーから前記更新指示を受信することに応じて、前記更新指示に含まれる前記新たなセキュリティ情報を、前記更新指示に含まれる前記識別情報を記憶する前記サービス提供サーバーにおいて更新された後のセキュリティ情報として取得する、請求項５に記載のセキュリティ情報更新システム。

【請求項７】

前記認証情報取得手段は、前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時を基準に定まる日時以降に、前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報を取得する、請求項５に記載のセキュリティ情

報更新システム。
【請求項８】
前記管理サーバーは、前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後の新たなセキュリティ情報を記憶しており、
前記認証情報取得手段は、前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報を前記管理サーバーから取得する、請求項７に記載のセキュリティ情報更新システム。
【請求項９】
前記複数の情報処理装置それぞれは、さらに、
ユーザーによる操作を受け付ける操作受付手段を備え、
前記認証情報取得手段は、前記操作受付手段により受け付けられる新たなセキュリティ情報を、前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報として取得する、請求項７に記載のセキュリティ情報更新システム。
【請求項１０】
前記複数の情報処理装置それぞれは、１以上のグループのいずれかに分類され、
前記識別情報は、前記１以上のグループのいずれかを識別するためのグループ識別情報である、請求項１～９のいずれかに記載のセキュリティ情報更新システム。
【請求項１１】
前記複数の情報処理装置それぞれは、１以上のグループのいずれかに分類され、
前記セキュリティ情報の取得に応じて、前記複数の情報処理装置のうち同一グループ内の他の情報処理装置に前記セキュリティ情報を送信する、請求項１～１０のいずれかに記載のセキュリティ情報更新システム。
【請求項１２】
前記複数の情報処理装置それぞれは、１以上のグループのいずれかに分類され、
前記セキュリティ情報を更新後、前記管理サーバーに前記複数の情報処理装置のうち同一グループの他の情報処理装置の装置識別情報と前記セキュリティ情報を送信する、請求項１～１０のいずれかに記載のセキュリティ情報更新システム。
【請求項１３】
予め記憶された識別情報とセキュリティ情報の組と同じ組が受信されることを条件にサービスを提供するサービス提供サーバーと通信可能な情報処理装置であって、
前記サービス提供サーバーに記憶された前記識別情報と更新日時とを定めたセキュリティポリシーを取得するポリシー取得手段と、
前記サービス提供サーバーに記憶された前記識別情報と同一の識別情報に関連付けてセキュリティ情報を記憶するセキュリティ情報記憶手段と、
前記サービス提供サーバーにより提供されるサービスを受ける処理を実行する場合、前記サービス提供サーバーに記憶された前記識別情報と同一の識別情報と、その識別情報と関連付けて記憶されているセキュリティ情報との組を、前記サービス提供サーバーに送信し、前記サービス提供サーバーによるサービスの提供を受ける処理実行手段と、
前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報を取得する認証情報取得手段と、
前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時以降に、前記セキュリティ情報記憶手段に前記サービス提供サーバーに記憶された前記識別情報と関連付けて記憶されたセキュリティ情報を前記取得されたセキュリティ情報で更新する更新手段と、
前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時以降、前記更新手段により前記取得されたセキュリティ情報で更新されるまで、前記処理実行手段による前記サービス提供サーバーによるサービスの提供を受ける処理の実行を禁止する禁止手段と、を備えた情報処理装置。

【請求項１４】
予め記憶された識別情報とセキュリティ情報の組と同じ組が受信されることを条件にサービスを提供するサービス提供サーバーと通信可能な情報処理装置で実行されるセキュリティ情報更新方法であって、
前記情報処理装置は、前記サービス提供サーバーに記憶された前記識別情報と同一の識別情報に関連付けてセキュリティ情報を記憶するセキュリティ情報記憶手段を備えており、
前記サービス提供サーバーに記憶された前記識別情報と更新日時とを定めたセキュリティポリシーを取得するポリシー取得ステップと、
前記サービス提供サーバーにより提供されるサービスを受ける処理を実行する場合、前記サービス提供サーバーに記憶された前記識別情報と同一の識別情報と、その識別情報と関連付けて記憶されているセキュリティ情報との組を、前記サービス提供サーバーに送信し、前記サービス提供サーバーによるサービスの提供を受ける処理実行ステップと、
前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報を取得する認証情報取得ステップと、
前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時以降に、前記セキュリティ情報記憶手段に前記サービス提供サーバーに記憶された前記識別情報と関連付けて記憶されたセキュリティ情報を前記取得されたセキュリティ情報で更新する更新ステップと、
前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時以降、前記更新ステップにおいて前記取得されたセキュリティ情報で更新されるまで、前記処理実行ステップにおける前記サービス提供サーバーによるサービスの提供を受ける処理の実行を禁止する禁止ステップと、を含む、セキュリティ情報更新方法。
【請求項１５】
予め記憶された識別情報とセキュリティ情報の組と同じ組が受信されることを条件にサービスを提供するサービス提供サーバーと通信可能な情報処理装置を制御するコンピューターで実行されるセキュリティ情報更新プログラム方法であって、
前記情報処理装置は、前記サービス提供サーバーに記憶された前記識別情報と同一の識別情報に関連付けてセキュリティ情報を記憶するセキュリティ情報記憶手段を備えており、
前記サービス提供サーバーに記憶された前記識別情報と更新日時とを定めたセキュリティポリシーを取得するポリシー取得ステップと、
前記サービス提供サーバーにより提供されるサービスを受ける処理を実行する場合、前記サービス提供サーバーに記憶された前記識別情報と同一の識別情報と、その識別情報と関連付けて記憶されているセキュリティ情報との組を、前記サービス提供サーバーに送信し、前記サービス提供サーバーによるサービスの提供を受ける処理実行ステップと、
前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報を取得する認証情報取得ステップと、
前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時以降に、前記セキュリティ情報記憶手段に前記サービス提供サーバーに記憶された前記識別情報と関連付けて記憶されたセキュリティ情報を前記取得されたセキュリティ情報で更新する更新ステップと、
前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時以降、前記更新ステップにおいて前記取得されたセキュリティ情報で更新されるまで、前記処理実行ステップにおける前記サービス提供サーバーによるサービスの提供を受ける処理の実行を禁止する禁止ステップと、を前記コンピューターに実行させるセキュリティ情報更新プログラム。
【請求項１６】
前記処理実行ステップは、前記更新日時が経過した後に前記更新ステップにおいて前記セ

キュリティ情報記憶手段に記憶されたセキュリティ情報が更新されることに応じて、前記禁止ステップにおいて実行が禁止されていた処理を実行するステップを含む、請求項１５に記載のセキュリティ情報更新プログラム。

【請求項１７】

前記処理実行ステップにおいて、前記サービス提供サーバーによるサービスの提供を受ける処理の実行が前記禁止ステップにおいて禁止されている間、セキュリティ情報が更新されていないことをユーザーに通知する通知ステップを、さらに前記コンピューターに実行させる、請求項１５または１６に記載のセキュリティ情報更新プログラム。

【請求項１８】

前記サービス提供サーバーとの間の通信状態を検出する通信状態検出ステップを、さらに、前記コンピューターに実行させ、

前記通知ステップは、前記処理実行ステップにおいて前記サービス提供サーバーによるサービスの提供を受ける処理の実行が前記禁止ステップにおいて禁止されている間に、前記通信状態検出ステップにおいて前記サービス提供サーバーとの間の通信ができないことが検出される場合、前記サービス提供サーバーと通信できないことを通知するステップを含む、請求項１７に記載のセキュリティ情報更新プログラム。

【請求項１９】

前記ポリシー取得ステップは、前記サービス提供サーバーに記憶されたセキュリティ情報を管理する管理サーバーから前記管理サーバーに記憶されたセキュリティポリシーを取得するステップを含む、請求項１５～１８のいずれかに記載のセキュリティ情報更新プログラム。

【請求項２０】

前記管理サーバーは、前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時を基準に定まる日時に、前記情報処理装置に前記識別情報と、前記サービス提供サーバーにおいて更新された後の新たなセキュリティ情報を含む更新指示を送信し、

前記認証情報取得ステップは、前記管理サーバーから前記更新指示を受信することに応じて、前記更新指示に含まれる前記新たなセキュリティ情報を、前記更新指示に含まれる前記識別情報を記憶する前記サービス提供サーバーにおいて更新された後のセキュリティ情報として取得するステップを含む、請求項１９に記載のセキュリティ情報更新プログラム。

【請求項２１】

前記認証情報取得ステップは、前記サービス提供サーバーに記憶された前記識別情報に対して前記セキュリティポリシーにより定められる前記更新日時を基準に定まる日時以降に、前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報を取得するステップを含む、請求項１９に記載のセキュリティ情報更新プログラム。

【請求項２２】

前記管理サーバーは、前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後の新たなセキュリティ情報を記憶しており、

前記認証情報取得ステップは、前記サービス提供サーバーに記憶された前記識別情報に対して前記サービス提供サーバーにおいて更新された後のセキュリティ情報を前記管理サーバーから取得するステップを含む、請求項２１に記載のセキュリティ情報更新プログラム。

【請求項２３】

ユーザーによる操作を受け付ける操作受付ステップを、前記コンピューターにさらに実行させ、

前記認証情報取得ステップは、前記操作受付ステップにおいて受け付けられる新たなセキュリティ情報を、前記サービス提供サーバーに記憶された前記識別情報に対して前記サ

ービス提供サーバーにおいて更新された後のセキュリティ情報として取得するステップを含む、請求項２１に記載のセキュリティ情報更新プログラム。

【請求項２４】

前記情報処理装置は、１以上のグループのいずれかに分類され、

前記識別情報は、前記１以上のグループのいずれかを識別するためのグループ識別情報である、請求項１５～２３のいずれかに記載のセキュリティ情報更新プログラム。

【請求項２５】

前記情報処理装置は、１以上のグループのいずれかに分類され、

前記セキュリティ情報の取得に応じて、同一グループ内の他の情報処理装置に前記セキュリティ情報を送信する、請求項１５～２４のいずれかに記載のセキュリティ情報更新プログラム。

【請求項２６】

前記情報処理装置は、１以上のグループのいずれかに分類され、

前記セキュリティ情報を更新後、前記管理サーバーに同一グループの他の情報処理装置の装置識別情報と前記セキュリティ情報を送信する、請求項１５～２４のいずれかに記載のセキュリティ情報更新プログラム。

【発明の詳細な説明】

【技術分野】

【０００１】

この発明は、セキュリティ情報更新システム、情報処理装置、セキュリティ情報更新方法およびセキュリティ情報更新プログラムに関し、複数の情報処理装置それぞれに記憶されたセキュリティ情報を更新するセキュリティ情報更新システム、その情報処理装置、セキュリティ情報更新システムおよび情報処理装置で実行されるセキュリティ情報更新方法およびセキュリティ情報更新プログラムに関する。

【背景技術】

【０００２】

複合機（以下「ＭＦＰ」という）で代表される画像処理装置は、外部の装置と通信して、互いに連携した処理を実行する場合がある。この場合に、通信する２以上の装置間で互いに通信相手の装置を確認するために、２以上の装置間で予め定められたパスワードが用いられる。さらに、このパスワードは機密性が要求されるため、画像形成装置を管理する管理者により管理されており、定期的または不定期に変更されるのが好ましい。しかしながら、パスワードを変更する場合は、そのパスワードを記憶する複数の画像形成装置のすべてで、それぞれパスワードを変更する必要がある。

【０００３】

このパスワードの変更に関する技術として、特開２０１２－２５２６２４号公報には、利用者情報に基づき、機器利用者を管理する管理サーバと接続され、利用者情報に基づき、利用者の機器利用を制御する情報処理装置は、利用者認証の要求を受け付ける受付手段と、利用者要求を受け付けると、自機が保持している、認証要求した利用者の内部利用者情報の有効期間が超過しているか否かを判定する判定手段と、有効期間を超過していると判定された場合に、管理サーバから、認証要求した利用者の外部利用者情報を取得する取得手段と、取得された外部利用者情報に基づき内部利用者情報を更新する更新手段と、更新された内部利用者情報に基づき、認証要求した利用者に対して機器利用を許可するか否かを制御する制御手段と、を有する情報処理装置が記載されている。

しかしながら、特開２０１２－２５２６２４号公報においては、情報処理装置を使用する利用者は、有効期間が超過する前後で、更新前の利用者情報と、更新後の利用者情報とを使い分けねばならない。この利用者情報の使い分けを誤る場合、具体的には、有効期限が超過する前に更新後の利用者情報を用いる場合、または、有効期限が超過した後に更新前の利用者情報を用いる場合、利用者情報が一致しないことにより情報処理装置により機器利用が許可されない事象（認証失敗）が発生するといった問題がある。さらに、利用者情報の使い分けを誤って機器利用が許可されない事象が所定回数連続する場合には、利用

者情報がロックされて、ロックが解除されるまで機器を利用することができなくなってしまう、といった問題がある。

【特許文献１】特開２０１２－２５２６２４号公報

【発明の概要】

【発明が解決しようとする課題】

【０００４】

この発明は上述した問題点を解決するためになされたもので、この発明の目的の一つは、サービス提供サーバーにおいて認証に失敗する事象が発生するのを防止したセキュリティ情報更新システムを提供することである。

【０００５】

この発明の他の目的は、サービス提供サーバーにおいて認証に失敗する事象が発生するのを防止した情報処理装置を提供することである。

【０００６】

この発明のさらに他の目的は、サービス提供サーバーにおいて認証に失敗する事象が発生するのを防止したセキュリティ情報更新方法を提供することである。

【０００７】

この発明のさらに他の目的は、サービス提供サーバーにおいて認証に失敗する事象が発生するのを防止したセキュリティ情報更新プログラムを提供することである。

【課題を解決するための手段】

【０００８】

上述した目的を達成するためにこの発明のある局面によれば、セキュリティ情報更新システムは、サービス提供サーバーと、複数の情報処理装置と、を含むセキュリティ情報更新システムであって、サービス提供サーバーは、更新日時に更新されるセキュリティ情報と、セキュリティ情報の種類を識別するための識別情報との組を記憶する認証情報記憶手段と、複数の情報処理装置のいずれかから受信される識別情報とセキュリティ情報との組と同一の組が認証情報記憶手段に記憶されていることを条件に、情報処理装置にサービスを提供するサービス提供手段と、を備え、複数の情報処理装置それぞれは、サービス提供サーバーに記憶された識別情報と更新日時とを定めたセキュリティポリシーを取得するポリシー取得手段と、サービス提供サーバーに記憶された識別情報と同一の識別情報に関連付けてセキュリティ情報を記憶するセキュリティ情報記憶手段と、サービス提供サーバーにより提供されるサービスを受ける処理を実行する場合、サービス提供サーバーに記憶された識別情報と同一の識別情報と、その識別情報と関連付けて記憶されているセキュリティ情報との組を、サービス提供サーバーに送信し、サービス提供サーバーによるサービスの提供を受ける処理実行手段と、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報を取得する認証情報取得手段と、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降に、セキュリティ情報記憶手段にサービス提供サーバーに記憶された識別情報と関連付けて記憶されたセキュリティ情報を取得されたセキュリティ情報で更新する更新手段と、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降、更新手段により取得されたセキュリティ情報で更新されるまで、処理実行手段によるサービス提供サーバーによるサービスの提供を受ける処理の実行を禁止する禁止手段と、を備える。

【０００９】

この局面に従えば、複数の情報処理装置それぞれは、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降、サービス提供サーバーに記憶された識別情報と関連付けて記憶されたセキュリティ情報が取得されたセキュリティ情報によって更新されるまで、サービス提供サーバーによるサービスの提供を受ける処理の実行を禁止するので、サービス提供サーバーにおいて認証に失敗する事象が発生するのを防止したセキュリティ情報更新システムを提供することができる。

【００１０】

好ましくは、処理実行手段は、更新日時が経過した後に更新手段によりセキュリティ情報記憶手段に記憶されたセキュリティ情報が更新されることに応じて、禁止手段により実行が禁止されていた処理を実行する。

【００１１】

この局面に従えば、更新日時が経過した後に実行が禁止されていた処理を、セキュリティ情報が更新された後に実行するので、実行を禁止した処理を再度実行させる操作をする必要がない。

【００１２】

好ましくは、複数の情報処理装置それぞれは、さらに、処理実行手段によるサービス提供サーバーによるサービスの提供を受ける処理の実行が禁止手段により禁止されている間、セキュリティ情報が更新されていないことをユーザーに通知する通知手段を備える。

【００１３】

この局面に従えば、サービス提供サーバーによるサービスの提供を受ける処理の実行が禁止されている間、セキュリティ情報が更新されていないことをユーザーに通知するので、ユーザーに、サービスの提供を受ける処理が実行されない原因を通知することができる。

【００１４】

好ましくは、複数の情報処理装置それぞれは、さらに、サービス提供サーバーとの間の通信状態を検出する通信状態検出手段を備え、通知手段は、処理実行手段によるサービス提供サーバーによるサービスの提供を受ける処理の実行が禁止手段により禁止されている間に、通信状態検出手段によりサービス提供サーバーとの間の通信ができないことが検出される場合、サービス提供サーバーと通信できないことを通知する。

【００１５】

この局面に従えば、ユーザーに、サービスの提供を受ける処理が実行されない原因が通信不良であることを通知することができる。

【００１６】

好ましくは、サービス提供サーバーに記憶されたセキュリティ情報を管理する管理サーバーを、さらに備え、管理サーバーは、セキュリティポリシーを記憶するポリシー記憶手段を、備え、ポリシー取得手段は、管理サーバーから管理サーバーに記憶されたセキュリティポリシーを取得する。

【００１７】

この局面に従えば、情報処理装置それぞれが、管理サーバーに記憶されたセキュリティポリシーを取得するので、管理サーバーにおいてセキュリティ情報の更新日時を管理すればよく、セキュリティ情報の管理が容易となる。

【００１８】

好ましくは、管理サーバーは、さらに、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時を基準に定まる日時に、複数の情報処理装置それぞれに識別情報と、サービス提供サーバーにおいて更新された後の新たなセキュリティ情報を含む更新指示を送信する更新指示送信手段を備え、認証情報取得手段は、管理サーバーから更新指示を受信することに応じて、更新指示に含まれる新たなセキュリティ情報を、更新指示に含まれる識別情報を記憶するサービス提供サーバーにおいて更新された後のセキュリティ情報として取得する。

【００１９】

この局面に従えば、複数の情報処理装置それぞれは、管理サーバーから更新指示を受信することに応じて、更新指示に含まれる新たなセキュリティ情報で、更新指示に含まれる識別情報の種類で特定されるセキュリティ情報を更新するので、複数の情報処理装置それぞれでセキュリティ情報を更新するタイミングのずれを短くすることができる。

【００２０】

好ましくは、認証情報取得手段は、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時を基準に定まる日時以降に、サービス

提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報を取得する。

【００２１】

この局面に従えば、更新日時を基準に定まる日時以降に更新された後のセキュリティ情報を取得するので、更新日時より後に更新された後のセキュリティ情報を取得する場合には、取得後直ちにセキュリティ情報を更新することができ、更新日時より前に更新された後のセキュリティ情報を取得する場合には、更新日時にセキュリティ情報を更新することができる。

【００２２】

好ましくは、管理サーバーは、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後の新たなセキュリティ情報を記憶しており、認証情報取得手段は、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報を管理サーバーから取得する。

【００２３】

この局面に従えば、管理サーバーから更新された後のセキュリティ情報を取得するので、更新された後のセキュリティ情報の取得が容易である。

【００２４】

好ましくは、複数の情報処理装置それぞれは、さらに、ユーザーによる操作を受け付ける操作受付手段を備え、認証情報取得手段は、操作受付手段により受け付けられる新たなセキュリティ情報を、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報として取得する。

【００２５】

この局面に従えば、ユーザーが入力するセキュリティ情報を更新された後のセキュリティ情報として取得するので、セキュリティ情報を送信しないようにして、機密性を向上させることができる。

【００２６】

好ましくは、複数の情報処理装置それぞれは、１以上のグループのいずれかに分類され、識別情報は、１以上のグループのいずれかを識別するためのグループ識別情報である。

【００２７】

この局面に従えば、１以上のグループごとに、セキュリティ情報を更新することができる。

好ましくは、複数の情報処理装置それぞれは、１以上のグループのいずれかに分類され、セキュリティ情報の取得に応じて、複数の情報処理装置のうち同一グループ内の他の情報処理装置にセキュリティ情報を送信する。

好ましくは、複数の情報処理装置それぞれは、１以上のグループのいずれかに分類され、セキュリティ情報を更新後、管理サーバーに複数の情報処理装置のうち同一グループの他の情報処理装置の装置識別情報とセキュリティ情報を送信する。

【００２８】

この発明の他の局面によれば、情報処理装置は、予め記憶された識別情報とセキュリティ情報の組と同じ組が受信されることを条件にサービスを提供するサービス提供サーバーと通信可能な情報処理装置であって、サービス提供サーバーに記憶された識別情報と更新日時とを定めたセキュリティポリシーを取得するポリシー取得手段と、サービス提供サーバーに記憶された識別情報と同一の識別情報に関連付けてセキュリティ情報を記憶するセキュリティ情報記憶手段と、サービス提供サーバーにより提供されるサービスを受ける処理を実行する場合、サービス提供サーバーに記憶された識別情報と同一の識別情報と、その識別情報と関連付けて記憶されているセキュリティ情報との組を、サービス提供サーバーに送信し、サービス提供サーバーによるサービスの提供を受ける処理実行手段と、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報を取得する認証情報取得手段と、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降に、セキュリ

ティ情報記憶手段にサービス提供サーバーに記憶された識別情報と関連付けて記憶されたセキュリティ情報を取得されたセキュリティ情報で更新する更新手段と、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降、更新手段により取得されたセキュリティ情報で更新されるまで、処理実行手段によるサービス提供サーバーによるサービスの提供を受ける処理の実行を禁止する禁止手段と、を備える。

【００２９】

この局面に従えば、サービス提供サーバーにおいて認証に失敗する事象が発生するのを防止した情報処理装置を提供することができる。

【００３０】

この発明のさらに他の局面によれば、セキュリティ情報更新方法は、予め記憶された識別情報とセキュリティ情報の組と同じ組が受信されることを条件にサービスを提供するサービス提供サーバーと通信可能な情報処理装置で実行されるセキュリティ情報更新方法であって、情報処理装置は、サービス提供サーバーに記憶された識別情報と同一の識別情報に関連付けてセキュリティ情報を記憶するセキュリティ情報記憶手段を備えており、サービス提供サーバーに記憶された識別情報と更新日時とを定めたセキュリティポリシーを取得するポリシー取得ステップと、サービス提供サーバーにより提供されるサービスを受ける処理を実行する場合、サービス提供サーバーに記憶された識別情報と同一の識別情報と、その識別情報と関連付けて記憶されているセキュリティ情報との組を、サービス提供サーバーに送信し、サービス提供サーバーによるサービスの提供を受ける処理実行ステップと、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報を取得する認証情報取得ステップと、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降に、セキュリティ情報記憶手段にサービス提供サーバーに記憶された識別情報と関連付けて記憶されたセキュリティ情報を取得されたセキュリティ情報で更新する更新ステップと、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降、更新ステップにおいて取得されたセキュリティ情報で更新されるまで、処理実行ステップにおけるサービス提供サーバーによるサービスの提供を受ける処理の実行を禁止する禁止ステップと、を含む。

【００３１】

この局面に従えば、サービス提供サーバーにおいて認証に失敗する事象が発生するのを防止したセキュリティ情報更新方法を提供することができる。

【００３２】

この発明のさらに他の局面によれば、セキュリティ情報更新プログラムは、予め記憶された識別情報とセキュリティ情報の組と同じ組が受信されることを条件にサービスを提供するサービス提供サーバーと通信可能な情報処理装置を制御するコンピューターで実行されるセキュリティ情報更新プログラム方法であって、情報処理装置は、サービス提供サーバーに記憶された識別情報と同一の識別情報に関連付けてセキュリティ情報を記憶するセキュリティ情報記憶手段を備えており、サービス提供サーバーに記憶された識別情報と更新日時とを定めたセキュリティポリシーを取得するポリシー取得ステップと、サービス提供サーバーにより提供されるサービスを受ける処理を実行する場合、サービス提供サーバーに記憶された識別情報と同一の識別情報と、その識別情報と関連付けて記憶されているセキュリティ情報との組を、サービス提供サーバーに送信し、サービス提供サーバーによるサービスの提供を受ける処理実行ステップと、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報を取得する認証情報取得ステップと、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降に、セキュリティ情報記憶手段にサービス提供サーバーに記憶された識別情報と関連付けて記憶されたセキュリティ情報を取得されたセキュリティ情報で更新する更新ステップと、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時以降、更新ステップにおいて

取得されたセキュリティ情報で更新されるまで、処理実行ステップにおけるサービス提供サーバーによるサービスの提供を受ける処理の実行を禁止する禁止ステップと、をコンピューターに実行させる。

【００３３】

この局面に従えば、サービス提供サーバーにおいて認証に失敗する事象が発生するのを防止したセキュリティ情報更新プログラムを提供することができる。

好ましくは、処理実行ステップは、更新日時が経過した後に更新ステップにおいてセキュリティ情報記憶手段に記憶されたセキュリティ情報が更新されることに応じて、禁止ステップにおいて実行が禁止されていた処理を実行するステップを含む。

好ましくは、処理実行ステップにおいて、サービス提供サーバーによるサービスの提供を受ける処理の実行が禁止ステップにおいて禁止されている間、セキュリティ情報が更新されていないことをユーザーに通知する通知ステップを、さらにコンピューターに実行させる。

好ましくは、サービス提供サーバーとの間の通信状態を検出する通信状態検出ステップを、さらに、コンピューターに実行させ、通知ステップは、処理実行ステップにおいてサービス提供サーバーによるサービスの提供を受ける処理の実行が禁止ステップにおいて禁止されている間に、通信状態検出ステップにおいてサービス提供サーバーとの間の通信ができないことが検出される場合、サービス提供サーバーと通信できないことを通知するステップを含む。

好ましくは、ポリシー取得ステップは、サービス提供サーバーに記憶されたセキュリティ情報を管理する管理サーバーから管理サーバーに記憶されたセキュリティポリシーを取得するステップを含む。

好ましくは、管理サーバーは、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時を基準に定まる日時に、情報処理装置に識別情報と、サービス提供サーバーにおいて更新された後の新たなセキュリティ情報を含む更新指示を送信し、認証情報取得ステップは、管理サーバーから更新指示を受信することに応じて、更新指示に含まれる新たなセキュリティ情報を、更新指示に含まれる識別情報を記憶するサービス提供サーバーにおいて更新された後のセキュリティ情報として取得するステップを含む。

好ましくは、認証情報取得ステップは、サービス提供サーバーに記憶された識別情報に対してセキュリティポリシーにより定められる更新日時を基準に定まる日時以降に、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報を取得するステップを含む。

好ましくは、管理サーバーは、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後の新たなセキュリティ情報を記憶しており、認証情報取得ステップは、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報を管理サーバーから取得するステップを含む。

好ましくは、ユーザーによる操作を受け付ける操作受付ステップを、コンピューターにさらに実行させ、認証情報取得ステップは、操作受付ステップにおいて受け付けられる新たなセキュリティ情報を、サービス提供サーバーに記憶された識別情報に対してサービス提供サーバーにおいて更新された後のセキュリティ情報として取得するステップを含む。

好ましくは、情報処理装置は、１以上のグループのいずれかに分類され、識別情報は、１以上のグループのいずれかを識別するためのグループ識別情報である。

好ましくは、情報処理装置は、１以上のグループのいずれかに分類され、セキュリティ情報の取得に応じて、同一グループ内の他の情報処理装置にセキュリティ情報を送信する。

好ましくは、情報処理装置は、１以上のグループのいずれかに分類され、セキュリティ情報を更新後、管理サーバーに同一グループの他の情報処理装置の装置識別情報とセキュリティ情報を送信する。

【図面の簡単な説明】
【００３４】
【図１】本実施の形態におけるセキュリティ情報更新システムの全体概要の一例を示す図である。
【図２】本実施の形態におけるＭＦＰのハードウェア構成の概要の一例を示すブロック図である。
【図３】本実施の形態における管理サーバーのハードウェア構成の概要の一例を示すブロック図である。
【図４】本実施の形態における管理サーバーが備えるＣＰＵの機能の一例をＨＤＤに記憶される情報とともに示すブロック図である。
【図５】ポリシーテーブルの一例を示す図である。
【図６】本実施の形態におけるＭＦＰが備えるＣＰＵの機能の一例をＨＤＤに記憶される情報とともに示すブロック図である。
【図７】管理処理の流れの一例を示すフローチャートである。
【図８】セキュリティ情報更新処理の流れの一例を示すフローチャートである。
【図９】実行制御処理の流れの一例を示すフローチャートである。
【図１０】第２の変形例における管理サーバーが備えるＣＰＵの機能の一例をＨＤＤに記憶される情報とともに示すブロック図である。
【図１１】第２の変形例におけるＭＦＰが備えるＣＰＵの機能の一例をＨＤＤに記憶される情報とともに示すブロック図である。
【図１２】第２の変形例における管理処理の流れの一例を示すフローチャートである。
【図１３】第２の変形例におけるセキュリティ情報更新処理の流れの一例を示すフローチャートである。
【発明を実施するための形態】
【００３５】
以下、本発明の実施の形態について図面を参照して説明する。以下の説明では同一の部品には同一の符号を付してある。それらの名称および機能も同じである。したがってそれらについての詳細な説明は繰返さない。
【００３６】
図１は、本実施の形態におけるセキュリティ情報更新システムの全体概要の一例を示す図である。図１を参照して、セキュリティ情報更新システム１は、管理サーバー２００と、サービス提供サーバー３００，３００Ａと、複合機であるＭＦＰ（Ｍｕｌｔｉ　Ｆｕｎｃｔｉｏｎ　Ｐｅｒｉｐｈｅｒａｌ）１００，１００Ａ～１００Ｄと、を含む。管理サーバー２００、サービス提供サーバー３００，３００ＡおよびＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、ネットワーク３と接続されている。ネットワーク３は、例えば、ローカルエリアネットワーク（ＬＡＮ）である。このため、管理サーバー２００、サービス提供サーバー３００，３００ＡおよびＭＦＰ１００，１００Ａ～１００Ｄは、互いに通信可能である。ＭＦＰ１００，１００Ａ～１００Ｄおよびサービス提供サーバー３００，３００Ａは、情報処理装置の一例である。ＭＦＰ１００，１００Ａ～１００Ｄそれぞれのハードウェア構成および機能は同じである。したがって、ここでは特に言及しない限りＭＦＰ１００を例に説明する。
【００３７】
なお、ここでは、ネットワーク３をＬＡＮとしたが、ＬＡＮに限らず、インターネット、ワイドエリアネットワーク（ＷＡＮ）、公衆交換電話網を用いたネットワーク等であってもよい。
【００３８】
サービス提供サーバー３００，３００Ａそれぞれは、所定のサービスを提供するコンピューターである。ここでは、サービス提供サーバー３００が、電子メールを送受信するサービスを提供する電子メールサーバーとして機能し、サービス提供サーバー３００Ａがデータベースを提供するデータベースサーバー（以下「ＤＢサーバー」という）として機能

する。なお、サービス提供サーバー３００，３００Ａそれぞれが提供するサービスは、これらに限定するものではなく、他のサービスであってもよい。

【００３９】

サービス提供サーバー３００，３００Ａそれぞれは、セキュリティを強化するために、それにアクセスしてくる装置またはユーザーの認証に成功することを条件にサービスを提供する。具体的には、サービス提供サーバー３００，３００Ａそれぞれは、識別情報とセキュリティ情報との組を予め登録しており、登録された識別情報とセキュリティ情報との組を送信してきた装置にサービスを提供する。サービス提供サーバー３００，３００Ａそれぞれに記憶される識別情報は、例えば、それにアクセスしてくる装置またはユーザーを識別するためのアカウントであり、セキュリティ情報は、パスワードである。ここでは、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、サービス提供サーバー３００，３００Ａごとに登録された識別情報とセキュリティ情報との組を記憶している。換言すれば、ＭＦＰ１００，１００Ａ～１００Ｄは、サービス提供サーバー３００に登録された識別情報とセキュリティ情報との組と、サービス提供サーバー３００Ａに登録された識別情報とセキュリティ情報との組と、を記憶する。このため、サービス提供サーバー３００に対応し、ＭＦＰ１００，１００Ａ～１００Ｄからなる第１のグループと、サービス提供サーバー３００Ａに対応し、ＭＦＰ１００，１００Ａ～１００Ｄからなる第２のグループとに、分類される。第１のグループに分類されるＭＦＰ１００，１００Ａ～１００Ｄそれぞれには、サービス提供サーバー３００において登録された識別情報とセキュリティ情報との組が記憶され、第２のグループに分類されるＭＦＰ１００，１００Ａ～１００Ｄそれぞれには、サービス提供サーバー３００Ａにおいて登録された識別情報とセキュリティ情報との組が記憶される。第１のグループに対応する識別情報と、第２のグループに対応する識別情報とは異なる。換言すれば、第１のグループに対応する識別情報は第１のグループを識別するためのグループ識別情報であり、第２のグループに対応する識別情報は、第２のグループを識別するためのグループ識別情報である。

【００４０】

例えば、ＭＦＰ１００が、第１のグループに属するサービス提供サーバー３００によるサービスの提供を受ける際には、サービス提供サーバー３００において登録された識別情報とセキュリティ情報の組を、サービス提供サーバー３００に送信する。サービス提供サーバー３００においては、ＭＦＰ１００から受信される識別情報とセキュリティ情報との組が登録されていれば認証し、認証に成功することを条件にＭＦＰ１００にサービスを提供する。また、ＭＦＰ１００が、第２のグループに属するサービス提供サーバー３００Ａによるサービスの提供を受ける際には、サービス提供サーバー３００Ａにおいて登録された識別情報とセキュリティ情報の組を、サービス提供サーバー３００Ａに送信する。サービス提供サーバー３００Ａにおいては、ＭＦＰ１００から受信される識別情報とセキュリティ情報との組が登録されていれば認証し、認証に成功することを条件にＭＦＰ１００にサービスを提供する。

【００４１】

第１グループおよび第２グループそれぞれを、複数のグループに分割するようにしてもよい。例えば、第１グループに属するＭＦＰ１００，１００Ａ～１００Ｄを、ＭＦＰ１００，１００Ａとからなる第３グループと、ＭＦＰ１００Ｂ～１００Ｄからなる第４グループと、に分割してもよい。この場合における識別情報は、第３グループと第４グループとで異なる。

【００４２】

管理サーバー２００は、サービス提供サーバー３００，３００ＡおよびＭＦＰ１００，１００Ａ～１００Ｄそれぞれに記憶されたセキュリティ情報を管理する。具体的には、管理サーバー２００は、セキュリティ情報の種類ごとに更新する日時を定めたセキュリティポリシーを定める。セキュリティポリシーは、セキュリティ情報の種類ごとに更新日時を定める。管理サーバーを２００操作するユーザーが管理サーバー２００にセキュリティ情報の種類ごとの更新日時を入力することによって、セキュリティ情報の種類ごとの更新日

時を定めたポリシーテーブルが管理サーバー２００に記憶される。

【００４３】

図２は、本実施の形態におけるＭＦＰのハードウェア構成の概要の一例を示すブロック図である。図２を参照して、ＭＦＰ１００は、メイン回路１１０と、原稿を読み取るための原稿読取部１３０と、原稿を原稿読取部１３０に搬送するための自動原稿搬送装置１２０と、原稿読取部１３０が原稿を読み取って出力する画像データに基づいて用紙等に画像を形成するための画像形成部１４０と、画像形成部１４０に用紙を供給するための給紙部１５０と、画像が形成された用紙を処理する後処理部１５５と、ユーザーインターフェースとしての操作パネル１６０とを含む。

【００４４】

後処理部１５５は、画像形成部１４０により画像が形成された１以上の用紙を並び替えて排紙するソート処理、パンチ穴加工するパンチ処理、ステープル針を打ち込むステープル処理を実行する。

【００４５】

メイン回路１１０は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１１１と、通信インターフェース（Ｉ／Ｆ）部１１２と、ＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）１１３と、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）１１４と、大容量記憶装置としてのハードディスクドライブ（ＨＤＤ）１１５と、ファクシミリ部１１６と、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ　Ｄｉｓｋ　ＲＯＭ）１１８が装着される外部記憶装置１１７と、を含む。ＣＰＵ１１１は、自動原稿搬送装置１２０、原稿読取部１３０、画像形成部１４０、給紙部１５０、後処理部１５５および操作パネル１６０と接続され、ＭＦＰ１００の全体を制御する。

【００４６】

ＲＯＭ１１３は、ＣＰＵ１１１が実行するプログラム、またはそのプログラムを実行するために必要なデータを記憶する。ＲＡＭ１１４は、ＣＰＵ１１１がプログラムを実行する際の作業領域として用いられる。また、ＲＡＭ１１４は、原稿読取部１３０から連続的に送られてくる読取データ（画像データ）を一時的に記憶する。

【００４７】

操作パネル１６０は、ＭＦＰ１００の上面に設けられ、表示部１６１と操作部１６３とを含む。表示部１６１は、液晶表示装置（ＬＣＤ）、有機ＥＬＤ（Ｅｌｅｃｔｒｏ－Ｌｕｍｉｎｅｓｃｅｎｃｅ　Ｄｉｓｐｌａｙ）等の表示装置であり、ユーザーに対する指示メニューや取得した画像データに関する情報等を表示する。操作部１６３は、複数のキーからなるハードキー部１６７を備え、キーに対応するユーザーの操作による各種の指示、文字、数字などのデータの入力を受け付ける。操作部１６３は、表示部１６１上に設けられたタッチパネル１６５をさらに含む。

【００４８】

ファクシミリ部１１６は、公衆交換電話網（ＰＳＴＮ）に接続され、ファクシミリの通信手順に従ってファクシミリデータを送受信する。

【００４９】

通信Ｉ／Ｆ部１１２は、ＭＦＰ１００をネットワーク３に接続するためのインターフェースである。ここでは、通信Ｉ／Ｆ部１１２が、ＴＣＰ（Ｔｒａｎｓｍｉｓｓｉｏｎ　Ｃｏｎｔｒｏｌ　Ｐｒｏｔｏｃｏｌ）の通信手順でデータを送受信する場合について説明する。なお、ここでは、通信手順の一例としてＴＣＰを例に説明するが、通信Ｉ／Ｆ部１１２を介してデータを送受信する通信手順は、ＴＣＰに限らず、例えば、ＵＤＰ（Ｕｓｅｒ　Ｄａｔａｇｒａｍ　Ｐｒｏｔｏｃｏｌ）であってもよい。ＣＰＵ１１１は、通信Ｉ／Ｆ部１１２を介して、ネットワーク３に接続された装置との間で通信し、データを送受信する。さらに、通信Ｉ／Ｆ部１１２は、ネットワーク３がインターネットに接続されている場合には、インターネットに接続されたコンピューターと通信が可能である。

【００５０】

ＨＤＤ１１５は、複数の記憶領域を有する。複数の記憶領域のうち少なくとも１つは、

共有設定されており、パスワードが設定されている。他のＭＦＰ１００Ａ～１００Ｄ、管理サーバー２００、サービス提供サーバー３００，３００Ａそれぞれは、ＨＤＤ１１５に設定されたパスワードをＭＦＰ１００に送信することにより、ＨＤＤ１１５の共有設定された記憶領域にアクセス可能である。

【００５１】

外部記憶装置１１７は、ＣＤ－ＲＯＭ１１８が装着される。ＣＰＵ１１１は、外部記憶装置１１７を介してＣＤ－ＲＯＭ１１８にアクセス可能である。ＣＰＵ１１１は、外部記憶装置１１７に装着されたＣＤ－ＲＯＭ１１８に記録されたプログラムをＲＡＭ１１４にロードして実行する。なお、ＣＰＵ１１１が実行するプログラムを記憶する媒体としては、ＣＤ－ＲＯＭ１１８に限られず、光ディスク（ＭＯ（Ｍａｇｎｅｔｉｃ Ｏｐｔｉｃａｌ Ｄｉｓｃ）／ＭＤ（Ｍｉｎｉ Ｄｉｓｃ）／ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ））、ＩＣカード、光カード、マスクＲＯＭ、ＥＰＲＯＭ（Ｅｒａｓａｂｌｅ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）、ＥＥＰＲＯＭ（Ｅｌｅｃｔｒｉｃａｌｌｙ ＥＰＲＯＭ）などの半導体メモリであってもよい。

【００５２】

また、ＣＰＵ１１１は、ＨＤＤ１１５に記憶されたプログラムをＲＡＭ１１４にロードして実行するようにしてもよい。この場合、ネットワーク３またはインターネットに接続された他のコンピューターが、ＭＦＰ１００のＨＤＤ１１５に記憶されたプログラムを書換える、または、新たなプログラムを追加して書き込むようにしてもよい。さらに、ＭＦＰ１００が、ネットワーク３またはインターネットに接続された他のコンピューターからプログラムをダウンロードして、そのプログラムをＨＤＤ１１５に記憶するようにしてもよい。ここでいうプログラムは、ＣＰＵ１１１が直接実行可能なプログラムだけでなく、ソースプログラム、圧縮処理されたプログラム、暗号化されたプログラム等を含む。

【００５３】

図３は、本実施の形態における管理サーバーのハードウェア構成の概要の一例を示すブロック図である。図３を参照して、管理サーバー２００は、管理サーバー２００の全体を制御するためのＣＰＵ２０１と、ＣＰＵ２０１が実行するためのプログラムを記憶するＲＯＭ２０２と、ＣＰＵ２０１の作業領域として使用されるＲＡＭ２０３と、データを不揮発的に記憶するＨＤＤ２０４と、ＣＰＵ２０１をネットワーク３に接続する通信部２０５と、情報を表示する表示部２０６と、ユーザーの操作の入力を受け付ける操作部２０７と、外部記憶装置２０９と、を含む。

【００５４】

外部記憶装置２０９は、ＣＤ－ＲＯＭ２０９Ａが装着される。ＣＰＵ２０１は、外部記憶装置２０９を介してＣＤ－ＲＯＭ２０９Ａにアクセス可能である。ＣＰＵ２０１は、外部記憶装置２０９に装着されたＣＤ－ＲＯＭ２０９Ａに記録されたプログラムをＲＡＭ２０３にロードして実行する。なお、ＣＰＵ２０１が実行するプログラムを記憶する媒体としては、ＣＤ－ＲＯＭ２０９Ａに限られず、光ディスク、ＩＣカード、光カード、マスクＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭなどの半導体メモリであってもよい。

【００５５】

また、ＣＰＵ２０１が実行するプログラムは、ＣＤ－ＲＯＭ２０９Ａに記録されたプログラムに限られず、ＨＤＤ２０４に記憶されたプログラムをＲＡＭ２０３にロードして実行するようにしてもよい。この場合、ネットワーク３に接続された他のコンピューターが、管理サーバー２００のＨＤＤ２０４に記憶されたプログラムを書換える、または、新たなプログラムを追加して書き込むようにしてもよい。さらに、管理サーバー２００が、ネットワーク３またはインターネットに接続された他のコンピューターからプログラムをダウンロードして、そのプログラムをＨＤＤ２０４に記憶するようにしてもよい。ここでいうプログラムは、ＣＰＵ２０１が直接実行可能なプログラムだけでなく、ソースプログラム、圧縮処理されたプログラム、暗号化されたプログラム等を含む。

【００５６】

図４は、本実施の形態における管理サーバーが備えるＣＰＵの機能の一例をＨＤＤに記

憶される情報とともに示すブロック図である。図４に示す機能は、管理サーバー２００が備えるＣＰＵ２０１が、ＲＯＭ２０２、ＨＤＤ２０４またはＣＤ－ＲＯＭ２０９Ａに記憶された管理プログラムを実行することにより、ＣＰＵ２０１に形成される機能である。図５を参照して、管理サーバー２００が備えるＣＰＵ２０１は、ポリシー送信部２５１と、更新指示部２５３と、を含む。ＨＤＤ１１５には、ポリシーテーブル２９１が記憶される。

【００５７】

図５は、ポリシーテーブルの一例を示す図である。図５を参照して、ポリシーテーブルは、２つのセキュリティレコードを含む。セキュリティレコードは、種類の項目と更新日時の項目と、グループ装置の項目を含む。種類の項目は、セキュリティ情報の種類を識別するための識別情報が設定され、更新日時の項目は、セキュリティ情報を更新する日時が設定され、グループ装置の項目は、セキュリティ情報を記憶する装置の装置識別情報が設定される。第１行目のセキュリティレコードは、種類の項目に、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」が設定され、更新日時の項目に「毎月１日　００：００」が設定され、グループ装置の項目に、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれの装置識別情報が設定される。識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」は、電子メールサーバーであるサービス提供サーバー３００に登録されるアカウントである。ここでは、ＭＦＰ１００，１００Ａ～１００Ｄの装置識別情報を、それぞれ「ＭＦＰ－１」、「ＭＦＰ－２」、「ＭＦＰ－３」、「ＭＦＰ－４」、「ＭＦＰ－５」としている。

【００５８】

第２行目のセキュリティレコードは、種類の項目に、識別情報「ＤＢ－ａｃｃｏｕｎｔ－Ｂ」が設定され、更新日時の項目に「毎月１０日　００：００」が設定され、グループ装置の項目に、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれの装置識別情報が設定される。識別情報「ＤＢ－ａｃｃｏｕｎｔ－Ｂ」は、ＤＢサーバーであるサービス提供サーバー３００Ａに登録されるアカウントである。

【００５９】

図４に戻って、ポリシー送信部２５１は、ＭＦＰ１００，１００Ａ～１００Ｄのいずれかからセキュリティポリシーが要求されると、ＨＤＤ２０４に記憶されたポリシーテーブル２９１を、要求してきた装置に送信する。

【００６０】

更新指示部２５３は、更新日時を基準に予め定められた日時を経過したセキュリティ情報を記憶する装置に更新指示を送信する。具体的には、更新指示部２５３は、ポリシーテーブル２９１を参照して、現在日時が更新日時を基準に定まる日時を経過したポリシーレコードを抽出する。更新日時を基準に定まる日時は、例えば、更新日時よりも予め定められた期間だけ後の日時である。サービス提供サーバー３００，３００Ａそれぞれにおいて、更新日時にセキュリティ情報が更新されるので、更新指示部２５３は、サービス提供サーバー３００に対応するセキュリティ情報の更新日時が経過すると、サービス提供サーバー３００から更新後の新たなセキュリティ情報を取得し、サービス提供サーバー３００Ａに対応するセキュリティ情報の更新日時が経過すると、サービス提供サーバー３００Ａから更新後の新たなセキュリティ情報を取得する。更新指示部２５３は、抽出されたポリシーレコードの種類の項目に設定された識別情報と、新たなセキュリティ情報と、を含む更新指示を、グループ装置の項目に設定された装置識別情報で特定される装置の全てに送信する。

【００６１】

例えば、更新指示部２５３は、ポリシーテーブル２９１の第１行目のセキュリティレコードを抽出する場合、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれに、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」と、サービス提供サーバー３００から取得された新たなセキュリティ情報との組を含む更新指示を送信する。また、更新指示部２５３は、ポリシーテーブル２９１の第２行目のセキュリティレコードを抽出する場合、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれに、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」と、サービス提供サ

ーバー３００Ａから取得された新たなセキュリティ情報との組を含む更新指示を送信する。

【００６２】

図６は、本実施の形態におけるＭＦＰが備えるＣＰＵの機能の一例をＨＤＤに記憶される情報とともに示すブロック図である。図６に示す機能は、ＭＦＰ１００が備えるＣＰＵ１１１が、ＲＯＭ１１３、ＨＤＤ１１５またはＣＤ－ＲＯＭ１１８に記憶されたセキュリティ情報更新プログラムを実行することにより、ＣＰＵ１１１に形成される機能である。図６を参照して、ＭＦＰ１００が備えるＣＰＵ１１１は、ポリシー取得部５１と、更新指示受信部５３と、更新部５５と、処理実行部５７と、禁止部５９と、通知部６１と、通信状態検出部６３と、を含む。

【００６３】

ＨＤＤ１１５には、パスワードテーブル９１が記憶される。パスワードテーブル９１は、識別情報とセキュリティ情報との組を含む。具体的には、サービス提供サーバー３００に登録された識別情報とセキュリティ情報との組、サービス提供サーバー３００Ａに登録された識別情報とセキュリティ情報との組、を、含む。

【００６４】

ポリシー取得部５１は、管理サーバー２００からセキュリティポリシーを取得する。ＨＤＤ１１５に管理サーバー２００のネットワークアドレスを記憶しておき、管理サーバー２００にセキュリティポリシーを要求する。ポリシー取得部５１は、セキュリティポリシーの要求に応じて管理サーバー２００が送信するポリシーテーブル２９１を取得する。ポリシー取得部５１は、取得されたポリシーテーブル２９１を更新部５５および禁止部５９に出力する。ポリシー取得部５１は、予め定められた時にポリシーテーブル２９１を取得するようにすればよい。予め定められた時は、限定するものではないが、例えば、ＭＦＰ１００に電源が投入された時、または毎日予め定められた時刻等である。

【００６５】

更新指示受信部５３は、通信Ｉ／Ｆ部１１２を制御して、管理サーバー２００から更新指示を受信する。更新指示は、セキュリティ情報の識別情報と新たなセキュリティ情報との組を含む。更新指示受信部５３は、更新指示を受信することに応じて、受信された更新指示を更新部５５に出力する。

【００６６】

更新部５５は、ポリシー取得部５１からポリシーテーブル２９１が入力され、更新指示受信部５３から更新指示が入力される。更新指示は、セキュリティ情報の識別情報と新たなセキュリティ情報との組を含む。更新部５５は、現在日時がセキュリティ情報に対する更新日時より後であることを条件に、セキュリティ情報を更新する。具体的には、更新部５５は、更新指示が入力されることに応じて、ポリシーテーブル２９１を参照して、更新指示に含まれる識別情報が種類の項目に設定されたポリシーレコードを抽出する。そして、更新部５５は、現在日時が、抽出されたポリシーレコードの更新日時の項目に設定された更新日時より後であるならば、更新指示に含まれる識別情報で特定される種類のセキュリティ情報を、更新指示に含まれるセキュリティ情報で更新する。更新部５５は、ＨＤＤ１１５に記憶されたパスワードテーブル９１に記憶されている識別情報とセキュリティ情報との組のうちから、更新指示に含まれる識別情報と同じ識別情報を含む組を特定し、特定した組のセキュリティ情報を、更新指示に含まれる新たなセキュリティ情報で更新する。更新部５５は、セキュリティ情報を更新することに応じて、そのセキュリティ情報の識別情報と更新した日時とを含む履歴情報を禁止部５９に出力する。

【００６７】

処理実行部５７は、ユーザーが操作部１６３に入力する操作に従って、処理を実行する。また、処理実行部５７は、ＭＦＰ１００がパーソナルコンピュータまたはスマートフォン等の携帯情報装置によって遠隔操作される場合には、パーソナルコンピュータまたは携帯情報装置から受信される遠隔操作に従って、処理を実行する。処理実行部５７が実行する処理は、パスワードテーブル９１に含まれるセキュリティ情報を用いて処理を含む。セ

キュリティ情報を用いて実行する処理は、サービス提供サーバー３００によるサービスの提供を受けるためにサービス提供サーバー３００に処理の実行を依頼する処理、サービス提供サーバー３００Ａによるサービスの提供を受けるためにサービス提供サーバー３００Ａに処理の実行を依頼する処理を含む。

【００６８】

処理実行部５７は、サービス提供サーバー３００に処理の実行を依頼する場合、パスワードテーブル９１を参照して、サービス提供サーバー３００に対応する識別情報のセキュリティ情報を取得する。サービス提供サーバー３００は、電子メールサーバーなので、サービス提供サーバー３００に対応する識別情報としてアカウント「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」、それと組になるセキュリティ情報とを取得する。処理実行部５７は、取得されたアカウントとセキュリティ情報とを用いて、サービス提供サーバー３００に認証を依頼し、サービス提供サーバー３００による認証が成功すると、サービス提供サーバー３００に電子メールの送受信を依頼する。

【００６９】

サービス提供サーバー３００に依頼する処理の一例は、サービス提供サーバー３００に蓄積された電子メールを所定時間間隔で受信する処理、ジョブを実行中にエラーが発生した場合、予め定められた宛先に不具合を通知するための電子メールを送信する処理、ファクシミリの送信件数または受信件数が所定件数に達した場合に予め定められた宛先にファクシミリの送信件数または受信件数が所定件数に達したことを通知するための電子メールを送信する処理、を含む。

【００７０】

また、処理実行部５７は、サービス提供サーバー３００Ａに処理の実行を依頼する場合、パスワードテーブル９１を参照して、サービス提供サーバー３００Ａに対応する識別情報のセキュリティ情報を取得する。サービス提供サーバー３００Ａは、ＤＢサーバーなので、サービス提供サーバー３００Ａに対応する識別情報としてアカウント「ＤＢ－ａｃｃｏｕｎｔ－Ｂ」とパスワードとの組を取得する。処理実行部５７は、取得されたアカウントとパスワードとを用いて、サービス提供サーバー３００Ａに認証を依頼し、サービス提供サーバー３００Ａによる認証が成功すると、サービス提供サーバー３００Ａにデータベースにアクセスする処理の実行を依頼する。

【００７１】

サービス提供サーバー３００Ａに依頼する処理の一例は、画像形成するプリント処理または原稿を読み取るスキャン処理を実行した結果を示すログデータをデータベースに登録する処理、プリント処理した画像のログをデータベースに登録する処理、を含む。

【００７２】

禁止部５９は、ポリシー取得部５１からポリシーテーブル２９１が入力され、更新部５５から履歴情報が入力される。禁止部５９は、処理実行部５７で実行される処理がセキュリティ情報を用いる場合に、そのセキュリティ情報の更新日時を経過してからそのセキュリティ情報が更新されるまでの間、処理実行部５７によるセキュリティ情報を用いる処理の実行を禁止する。

【００７３】

具体的には、禁止部５９は、処理実行部５７によりセキュリティ情報を用いる処理が実行される前に、処理実行部５７からその処理に用いるセキュリティ情報の種類を示す識別情報を取得する。禁止部５９は、ポリシーテーブル２９１を参照して、取得された識別情報に対応する更新日時を特定する。具体的には、禁止部５９は、処理実行部５７から取得された識別情報が種類の項目に設定されたポリシーレコードを抽出し、抽出されたポリシーレコードの更新日時の項目に設定された更新日時を取得する。禁止部５９は、現在日時が更新日時よりも後の場合に、処理実行部５７から取得された識別情報を含み、かつ、更新日時よりの後の日時を含む履歴情報が更新部５５から入力されていれば、その識別情報で特定される種類のセキュリティ情報が更新されたと判断する。禁止部５９は、現在日時が更新日時よりも後の場合に、処理実行部５７から取得された識別情報を含み、かつ、更

新日時よりの後の日時を含む履歴情報が更新部５５から入力されていなければ、その識別情報で特定される種類のセキュリティ情報が更新されたと判断する。

【００７４】

禁止部５９は、処理実行部５７から識別情報を取得した時点で、取得された識別情報で特定される種類のセキュリティ情報が更新されていないと判断する場合、処理実行部５７による処理の実行を禁止する。禁止部５９は、処理実行部５７による処理の実行を禁止した後に、取得された識別情報と更新日時よりの後の日時を含む履歴情報が更新部５５から入力されることに応じて、処理実行部５７による処理の実行を許可する。禁止部５９は、処理実行部５７から識別情報を取得した時点で、取得された識別情報で特定される種類のセキュリティ情報が更新されていると判断する場合、処理実行部５７による処理の実行を許可する。禁止部５９は、処理実行部５７による処理の実行を禁止している間、禁止した処理が用いるセキュリティ情報の種類を示す識別情報を含む禁止信号を通知部６１および通信状態検出部６３に出力する。

【００７５】

処理実行部５７は、禁止部５９によって処理の実行が禁止される場合、その処理を一時的に保留し、その後、禁止部５９により処理の実行が許可されることに応じて、一時保留された処理を実行する。

【００７６】

通信状態検出部６３は、禁止部５９から禁止信号が入力されている間、通信Ｉ／Ｆ部１１２を制御して、ネットワーク３の通信状態を検出する。具体的には、禁止信号に含まれる識別情報で特定される種類のセキュリティ情報を登録する装置を特定し、特定された装置との通信状態を確認する。例えば、禁止信号に含まれる識別情報が、サービス提供サーバー３００に登録されたセキュリティ情報の種類を示す場合、サービス提供サーバー３００に対するＰＩＮＧコマンドを実行し、サービス提供サーバー３００からの応答がある場合にサービス提供サーバー３００と通信可能と判断し、応答がない場合にはサービス提供サーバー３００と通信不可能と判断する。通信状態検出部６３は、サービス提供サーバー３００の通信状態を通知部６１に出力する。

【００７７】

通知部６１は、禁止部５９から禁止信号が入力されている間、処理を実行することができないことをユーザーに通知する。例えば、表示部１６１に、セキュリティ情報が更新されておらず、処理が保留中であることを示すエラーメッセージを表示する。通知部６１は、禁止信号に含まれる識別情報で特定される種類のセキュリティ情報を登録する装置を特定することによって、実行が禁止される処理を特定する。例えば、禁止信号に含まれる識別情報が、サービス提供サーバー３００に登録されたセキュリティ情報の種類を示す場合、通知部６１は、サービス提供サーバー３００が提供するサービスを受ける処理として、電子メールの送受信処理を特定する。通知部６１は、通信状態検出部６３から入力されるサービス提供サーバー３００の通信状態が通信可能であることを示す場合は、サービス提供サーバー３００に対応するセキュリティ情報が更新されておらず、特定された電子メールの送受信処理を実行できないことを示すメッセージを、表示部１６１に表示する。

【００７８】

また、通知部６１は、禁止部５９によって実行が禁止される処理が電子メールの送受信処理を特定する場合であって、通信状態検出部６３から入力されるサービス提供サーバー３００の通信状態が通信不可能であることを示す場合、サービス提供サーバー３００と通信不可能であることを示すメッセージを、表示部１６１に表示する。サービス提供サーバー３００と通信できない場合には、ネットワーク３の障害等の原因で管理サーバー２００から更新指示を受信できない場合があり、更新部５５によるセキュリティ情報の更新ができない場合があるからである。

【００７９】

図７は、管理処理の流れの一例を示すフローチャートである。管理処理は、管理サーバー２００が備えるＣＰＵ２０１が、ＲＯＭ２０２、ＨＤＤ２０４またはＣＤ－ＲＯＭ２０

９Ａに記憶された管理プログラムを実行することにより、ＣＰＵ２０１により実行される処理である。図７を参照して、管理サーバー２００が備えるＣＰＵ２０１は、セキュリティポリシーの要求があったか否かを判断する（ステップＳ０１）。情報処理装置として機能するＭＦＰ１００，１００Ａ～１００Ｄのいずれかからセキュリティポリシーの要求を受信したならば処理をステップＳ０２に進めるが、そうでなければ処理をステップＳ０３に進める。ステップＳ０２においては、ＭＦＰ１００，１００Ａ～１００Ｄのうちセキュリティポリシーを要求してきた装置に、ＨＤＤ２０４に記憶されたポリシーテーブル２９１を送信し、処理をステップＳ０３に進める。

【００８０】

ステップＳ０３においては、更新日時を経過したセキュリティ情報が存在するか否かを判断する。具体的には、ＣＰＵ２０１は、ＨＤＤ２０４に記憶されたポリシーテーブル２９１を参照して、現在日時が更新日時を経過したポリシーレコードを抽出する。次のステップＳ０４においては、更新指示を送信済か否かを判断する。後述するステップＳ０８において記憶される送信履歴を用いて、更新指示を送信済か否かを判断する。送信履歴は、更新指示を送信した場合に記憶され、更新指示を送信した日時と、その更新指示に含まれる識別情報と、を含む。同一の識別情報を含む更新指示と、送信履歴とが対応し、送信履歴に含まれる更新指示が送信された日時が、更新日時より後ならば更新指示を送信済と判断する。更新指示を送信済でなければ処理をステップＳ０５に進め、送信済ならば処理をステップＳ０１に戻す。

【００８１】

ステップＳ０５においては、セキュリティ情報を取得する。ここでは、ポリシーレコードの種類の項目に設定された識別情報で特定される種類のセキュリティ情報を登録する装置からセキュリティ情報を取得する。例えば、ポリシーレコードの種類の項目に設定された識別情報で特定される種類のセキュリティ情報を登録する装置が、サービス提供サーバー３００ならばサービス提供サーバー３００から更新後の新たなセキュリティ情報を取得し、サービス提供サーバー３００Ａならばサービス提供サーバー３００Ａから更新後の新たなセキュリティ情報を取得する。

【００８２】

次のステップＳ０６においては、グループの装置を特定する。ステップＳ０３において抽出されたポリシーレコードのグループ装置の項目に設定された複数の装置識別情報でそれぞれ特定される複数の装置を、グループに属する装置として特定する。そして、グループに属する装置それぞれに、更新指示を送信する（ステップＳ０７）。更新指示は、ステップＳ０１において抽出されたポリシーレコードの種類の項目に設定された識別情報と、ステップＳ０５において取得されたセキュリティ情報と、を含む。

【００８３】

次のステップＳ０８においては、送信履歴を記憶し、処理をステップＳ０１に戻す。送信履歴は、ステップＳ０１において抽出されたポリシーレコードの種類の項目に設定された識別情報と、更新指示が送信された日時とを含む。送信履歴は、ステップＳ０４において、更新指示を送信済か否かを判断する際に用いられ、送信履歴に含まれる更新指示が送信された日時が、更新日時より後ならば更新指示を送信済と判断する。

【００８４】

図８は、セキュリティ情報更新処理の流れの一例を示すフローチャートである。セキュリティ情報更新処理は、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれが備えるＣＰＵ１１１が、ＲＯＭ１１３、ＨＤＤ１１５またはＣＤ－ＲＯＭ１１８に記憶されたセキュリティ情報更新プログラムを実行することにより、ＣＰＵ１１１により実行される処理である。図８を参照して、ＭＦＰ１００が備えるＣＰＵ１１１は、管理サーバー２００からポリシーテーブルを取得する（ステップＳ１１）。具体的には、管理サーバー２００にセキュリティポリシーを要求し、管理サーバー２００がセキュリティポリシーの要求に応じて返信するポリシーテーブル２９１を受信する。

【００８５】

次のステップＳ１２においては、ポリシーテーブル２９１に含まれる１以上のポリシーレコードのうちから処理対象となるポリシーレコードを選択し、処理をステップＳ１３に進める。ステップＳ１３においては、更新日時を経過しているか否かを判断する。現在日時が選択されたポリシーレコードの更新日時の項目に設定された更新日時より後ならば、更新日時を経過していると判断する。更新日時を経過しているならば処理をステップＳ１４に進めるが、そうでなければ処理をステップＳ１５に進める。ステップＳ１４においては、選択されたポリシーレコードの種類の項目に設定された識別情報に対応する更新フラグを「０」に設定し、処理をステップＳ１５に進める。識別情報に対応する更新フラグは、識別情報に対応するセキュリティ情報の種類ごとに更新日時を経過した後にセキュリティ情報が更新されたか否かを示し、更新日時が経過すると「０」に設定され、更新日時が経過した後にセキュリティ情報が更新されると「１」に設定される。

【００８６】

ステップＳ１５においては、処理対象として選択されていないポリシーレコードが存在するか否かを判断する。未選択のポリシーレコードが存在するならば処理をステップＳ１２に戻し、存在しなければ処理をステップＳ１６に進める。

【００８７】

ステップＳ１６においては、管理サーバー２００から更新指示を受信したか否かを判断する。更新指示を受信したならば処理をステップＳ１７に進めるが、そうでなければ処理をステップＳ１２に戻す。ステップＳ１７においては、セキュリティ情報の種類を特定する。更新指示に含まれる識別情報を、セキュリティ情報の種類に特定する。そして、特定された種類と更新指示に含まれるセキュリティ情報とを一時記憶し（ステップＳ１８）、処理をステップＳ１９に進める。

【００８８】

ステップＳ１９においては、更新日時を経過しているか否かを判断する。ステップＳ１１において取得されたポリシーテーブル２９１を参照して、更新指示に含まれる識別情報で特定されるセキュリティ情報の更新日時を取得し、現在日時が更新日時より後ならば更新日時を経過していると判断する。更新日時を経過するまで待機状態となり（ステップＳ１９でＮＯ）、更新日時を経過したならば処理をステップＳ２０に進める。

【００８９】

ステップＳ２０においては、セキュリティ情報を更新し、処理をステップＳ１２に進める。ステップＳ１８において一時記憶されたセキュリティ情報で、ＨＤＤ１１５に記憶されたパスワードテーブル９１を更新する。具体的には、ＨＤＤ１１５に記憶されているパスワードテーブル９１に含まれる識別情報とセキュリティ情報との組のうちから、ステップＳ１８において一時記憶された識別情報と同じ識別情報を含む組を特定し、特定した組のセキュリティ情報を、ステップＳ１８において識別情報とともに一時記憶されたセキュリティ情報で更新する。ステップＳ２１においては、ステップＳ２０において更新されたセキュリティ情報の識別情報に対応する更新フラグを「１」に設定し、処理をステップＳ１２に戻す。

【００９０】

図９は、実行制御処理の流れの一例を示すフローチャートである。実行制御処理は、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれが備えるＣＰＵ１１１が、ＲＯＭ１１３、ＨＤＤ１１５またはＣＤ－ＲＯＭ１１８に記憶された実行制御プログラムを実行することにより、ＣＰＵ１１１により実行される処理である。実行制御プログラムは、セキュリティ情報更新プログラムの一部である。図９を参照して、ＭＦＰ１００が備えるＣＰＵ１１１は、処理実行操作を受け付けたか否かを判断する（ステップＳ３１）。処理実行操作は、処理の実行を指示する操作であり、ユーザーが操作部１６３に入力することにより受け付けられる場合、または、ＭＦＰ１００が外部の装置によって遠隔操作される場合には外部の装置から遠隔操作として受け付けられる場合がある。処理実行操作を受け付けるまで待機状態となり、処理実行操作を受け付けたならば処理をステップＳ３２に進める。

【００９１】

ステップＳ３２においては、処理実行操作で特定される処理がセキュリティ情報を用いる処理か否かを判断する。処理実行操作で特定される処理がセキュリティ情報を用いる処理ならば処理をステップＳ３３に進めるが、そうでなければ処理をステップＳ３５に進める。ステップＳ３５においては、処理実行操作で特定される処理を実行し、処理を終了する。

【００９２】

ステップＳ３３においては、セキュリティ情報の種類を特定する。管理サーバー２００から取得されたポリシーテーブル２９１を参照して、処理実行操作で特定される処理が用いるセキュリティ情報の種類を特定する。例えば、処理実行操作で特定される処理が電子メールを送受信する処理であれば、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」を特定し、処理実行操作で特定される処理がデータベースにアクセスする処理であれば、識別情報「ＤＢ－ａｃｃｏｕｎｔ－Ｂ」を特定する。

【００９３】

次のステップＳ３４においては、ステップＳ３３において特定された種類の識別情報に対応する更新フラグが「１」に設定されているか否かを判断する。更新フラグが「１」に設定されていれば処理をステップＳ３５に進めるが、そうでなければ処理をステップＳ３６に進める。ステップＳ３５においては、ステップＳ３１において受け付けられた処理実行操作で特定される処理を実行し、処理を終了する。

【００９４】

ステップＳ３６においては、処理実行操作で特定される処理を保留し、処理をステップＳ３７に進める。例えば、処理実行操作で特定される処理に対応するジョブを、ＲＡＭ１１４に記憶する。ステップＳ３７においては、通信状態を検出する。処理実行操作で特定される処理が電子メールを送受信する処理であれば、電子メールサーバーであるサービス提供サーバー３００との間の通信状態を検出し、処理実行操作で特定される処理がデータベースにアクセスする処理であれば、ＤＢサーバーであるサービス提供サーバー３００Ａとの間の通信状態を検出する。例えば、通信状態を検出する対象の装置に対してＰＩＧコマンドを実行し、装置からの応答があれば通信可能と判断し、装置からの応答がなければ通信不可能と判断する。

【００９５】

次のステップＳ３８においては、通信状態によって処理を分岐させる。通信状態が通信不可能でならば処理をステップＳ３９に進めるが、そうでなければ処理をステップＳ４０に進める。ステップＳ３９においては、通信エラーを通知し、処理をステップＳ３４に戻す。例えば、通信不可能であることを通知するメッセージを表示部１６１に表示する。ステップＳ３５においては、処理の実行を保留中であることを通知し、処理をステップＳ３４に戻す。セキュリティ情報が更新されていないために処理を実行できないことを通知するメッセージを表示部１６１に表示する。

【００９６】

以上説明したように、本実施の形態におけるセキュリティ情報更新システム１において、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、例えば、サービス提供サーバー３００において更新日時に更新されるセキュリティ情報でセキュリティ情報が更新されるまで、サービス提供サーバー３００によるサービスの提供を受ける処理の実行を禁止するので、サービス提供サーバー３００に更新前のセキュリティ情報を送信しないようにして、サービス提供サーバー３００において認証に失敗する事象が発生するのを防止することができる。特に、ＭＦＰ１００，１００Ａ～１００Ｄが、サービス提供サーバー３００によるサービスの提供を受けるために同一のアカウントとして識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」を用いる場合に有効である。例えば、ＭＦＰ１００，１００Ａ～１００Ｄのうち１つ、例えばＭＦＰ１００において、サービス提供サーバー３００において更新日時に更新されるセキュリティ情報で更新されていない状態で、サービス提供サーバー３００によるサービスの提供を受ける処理の実行を禁止することなく実行する場合、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」と更新前のセキュリティ情報とをサービス提供サーバー３０

０に送信する。この場合には、サービス提供サーバー３００における認証に失敗する。さらに、ＭＦＰ１００において、サービス提供サーバー３００における認証に複数回連続して失敗する場合には、サービス提供３００は、アカウントである識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」をロックする。アカウントである識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」がロックされる場合、他のＭＦＰ１００Ａ～１００Ｄにおいて、セキュリティ情報が更新されている場合であっても、サービス提供サーバー３００における認証に失敗してしまう。本実施の形態におけるＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、例えば、サービス提供サーバー３００において更新日時に更新されるセキュリティ情報でセキュリティ情報が更新されるまで、サービス提供サーバー３００によるサービスの提供を受ける処理の実行を禁止するので、サービス提供サーバー３００においてアカウントがロックされる事象が発生するのを防止することができる。

【００９７】

また、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、サービス提供サーバー３００によるサービスの提供を受ける処理の実行を禁止している間に、セキュリティ情報が更新されることに応じて、実行を禁止していた処理を実行するので、実行を禁止していた処理を再度実行させる操作をする必要がない。

【００９８】

また、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、セキュリティポリシーにより定められる更新日時が経過した後に、更新された後のセキュリティ情報を取得するので、取得後直ちにセキュリティ情報を更新することができる。

【００９９】

また、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、例えば、サービス提供サーバー３００によるサービスの提供を受ける処理の実行が禁止されている間、セキュリティ情報が更新されていないことをユーザーに通知するので、ユーザーに、サービス提供サーバー３００によるサービスの提供を受ける処理が実行されない原因を通知することができる。

【０１００】

また、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、例えば、サービス提供サーバー３００によるサービスの提供を受ける処理の実行が禁止されている間、サービス提供サーバー３００との間の通信ができないことが検出される場合、サービス提供サーバー３００と通信できないことを通知するので、ユーザーに、サービス提供サーバー３００によるサービスの提供を受ける処理が実行されない原因が通信不良であることを通知することができる。

【０１０１】

また、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、管理サーバー２００からポリシーテーブル２９１を取得するので、管理サーバー２００でポリシーテーブル２９１を管理すればよく、セキュリティ情報の更新日時の管理を容易にすることができる。

【０１０２】

また、管理サーバー２００は、例えば、サービス提供サーバー３００に記憶された識別情報に対してセキュリティポリシーにより定められる更新日時を基準に定まる日時に、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれに識別情報と、サービス提供サーバーにおいて更新された後の新たなセキュリティ情報を含む更新指示を送信する。ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、管理サーバー２００から更新指示を受信することに応じて、更新指示に含まれる新たなセキュリティ情報で、更新指示に含まれる識別情報の種類で特定されるサービス提供サーバー３００に対応するセキュリティ情報を更新する。このため、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれでセキュリティ情報を更新するタイミングのずれを短くすることができる。

【０１０３】

また、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、１以上のグループのいずれかに分類され、識別情報を１以上のグループのいずれかを識別するためのグループ識別情報とするので、１つの種類のセキュリティ情報を、複数の情報処理装置のすべてが記憶してい

ない場合であっても、そのセキュリティ情報を更新することができる。例えば、サービス提供サーバーに記憶された識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」を、ＭＦＰ１００，１００Ａで記憶するが、ＭＦＰ１００Ｂ～１００Ｄで記憶しない場合、ＭＦＰ１００，１００Ａが、グループ識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」のグループに分類される。グループ識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」のグループに分類されたＭＦＰ１００，１００Ａで、グループ識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」で特定される種類のセキュリティ情報を更新するが、ＭＦＰ１００Ｂ～１００Ｄでは、グループ識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」で特定される種類のセキュリティ情報を更新しない。

【０１０４】

＜第１の変形例＞

管理サーバー２００が、セキュリティ情報を、更新日時より前に取得する場合には、更新日時を経過する前に、更新指示を送信するようにしてもよい。

【０１０５】

例えば、管理サーバー２００が備えるＣＰＵ２０１が有する更新指示部２５３が、新たなセキュリティ情報を生成するようにしてもよい。この場合には、更新指示部２５３は、サービス提供サーバー３００に登録されたセキュリティ情報に対応する新たなセキュリティ情報を生成して更新指示を送信し、さらに、更新日時になるとサービス提供サーバー３００に、サービス提供サーバー３００に登録されたセキュリティ情報を生成されたセキュリティ情報で更新させる。また、更新指示部２５３は、サービス提供サーバー３００Ａに登録されたセキュリティ情報に対応する新たなセキュリティ情報を生成して更新指示を送信し、さらに、更新日時になるとサービス提供サーバー３００Ａに、サービス提供サーバー３００Ａに登録されたセキュリティ情報を生成されたセキュリティ情報で更新させる。

【０１０６】

第１の変形例においては、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、セキュリティポリシーにより定められる更新日時より前の日時に、更新された後のセキュリティ情報を取得するので、更新日時にセキュリティ情報を更新することができる。

【０１０７】

＜第２の変形例＞

上述した実施の形態におけるセキュリティ情報更新システム１においては、管理サーバー２００が、ポリシーテーブル２９１を参照して、ポリシーレコードの更新日時の項目に設定された更新日時を経過する場合に、ポリシーレコードのグループ装置の項目に設定された装置のすべてに更新指示を送信するようにした。第２の変形例におけるセキュリティ情報更新システム１においては、管理サーバー２００が更新指示を送信しないようにしたものである。

【０１０８】

図１０は、第２の変形例における管理サーバーが備えるＣＰＵの機能の一例をＨＤＤに記憶される情報とともに示すブロック図である。図１０に示す機能が、図４に示す機能と異なる点は、更新指示部２５３が削除された点である。その他の機能は、図４に示した機能と同じなのでここでは説明を繰り返さない。

【０１０９】

図１１は、第２の変形例におけるＭＦＰが備えるＣＰＵの機能の一例をＨＤＤに記憶される情報とともに示すブロック図である。図１１に示す機能が図６に示した機能と異なる点は、更新指示受信部５３が認証情報取得部５３Ａに変更された点である。その他の機能は、図６に示した機能と同じなので、ここでは説明を繰り返さない。

【０１１０】

認証情報取得部５３Ａは、ポリシー取得部５１から入力されるポリシーテーブル２９１を参照して、更新日時を経過したセキュリティ情報を抽出する。具体的には、認証情報取得部５３Ａは、ポリシー取得部５１から入力されるポリシーテーブルを参照して、現在日時が更新日時を経過したポリシーレコードを抽出し、抽出されたポリシーレコードの種類

の項目に設定された識別情報で特定される種類の新たなセキュリティ情報を取得する。

【０１１１】

認証情報取得部５３Ａは、管理サーバー２００から識別情報に対応する新たなセキュリティ情報を取得してもよいし、識別情報で特定される種類のセキュリティ情報が登録された装置、ここでは、サービス提供サーバー３００，３００Ａそれぞれから新たなセキュリティ情報を取得するようにしてもよい。また、認証情報取得部５３Ａは、ＭＦＰ１００を操作するユーザーが、操作部１６３に入力するセキュリティ情報を取得するようにしてもよい。

【０１１２】

認証情報取得部５３Ａは、新たなセキュリティ情報を取得することに応じて、識別情報と、取得された新たなセキュリティ情報との組を更新部５５に出力する。

【０１１３】

図１２は、第２の変形例における管理処理の流れの一例を示すフローチャートである。図１２を参照して、図７に示した管理処理と異なる点は、ステップＳ０３～ステップＳ０８が削除された点である。その他の処理は、図７に示した処理と同じなので、ここでは説明を繰り返さない。

【０１１４】

図１３は、第２の変形例におけるセキュリティ情報更新処理の流れの一例を示すフローチャートである。第２の変形例におけるセキュリティ情報更新処理は、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれが備えるＣＰＵ１１１が、ＲＯＭ１１３、ＨＤＤ１１５またはＣＤ－ＲＯＭ１１８に記憶された第２の変形例におけるセキュリティ情報更新プログラムを実行することにより、ＣＰＵ１１１により実行される処理である。図１３を参照して、ステップＳ５１～ステップＳ５３は、図８のステップＳ１１～ステップＳ１３と同じである。すなわち、ＭＦＰ１００が備えるＣＰＵ１１１は、管理サーバー２００からポリシーテーブルを取得し（ステップＳ５１）、ポリシーテーブル２９１に含まれる１以上のポリシーレコードのうちから処理対象となるポリシーレコードを選択し（ステップＳ５２）、更新日時を経過しているか否かを判断する（ステップＳ５３）。現在日時が選択されたポリシーレコードの更新日時の項目に設定された更新日時より後ならば、更新日時を経過していると判断し、処理をステップＳ５４に進めるが、そうでなければ処理をステップＳ６０に進める。

【０１１５】

ステップＳ５４においては、更新履歴が記憶されているか否かを判断する。更新履歴は、後述するステップＳ５９において記憶され、セキュリティ情報の識別情報と、更新した日時とを含む。ステップＳ５２において選択されたポリシーレコードの種類の項目に設定された識別情報と同じ識別情報を含む更新履歴であって、その更新履歴に含まれる日時が更新日時よりも後ならば更新履歴が記憶されていると判断する。更新履歴が記憶されているならば処理をステップＳ６０に進めるが、そうでなければ処理をステップＳ５５に進める。

【０１１６】

ステップＳ５５においては、ステップＳ５２において選択されたポリシーレコードの種類の項目に設定された識別情報に対応する更新フラグを「０」に設定し、処理をステップＳ５６に進める。ステップＳ５６においては、セキュリティ情報を取得したか否かを判断する。ここでは、セキュリティ情報が登録された装置からセキュリティ情報を取得する場合を例に説明する。例えば、ステップＳ５２において選択されたポリシーレコードの種類の項目に設定された識別情報が「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」の場合、その識別情報で特定される種類のセキュリティ情報を登録する装置は、サービス提供サーバー３００なので、サービス提供サーバー３００からサービス提供サーバー３００において更新された後の新たなセキュリティ情報を取得する。また、ステップＳ５２において選択されたポリシーレコードの種類の項目に設定された識別情報が「ＤＢ－ａｃｃｏｕｎｔ－Ｂ」の場合、その識別情報で特定される種類のセキュリティ情報を登録する装置は、サービス提供サ

ーバー３００Ａなので、サービス提供サーバー３００Ａからサービス提供サーバー３００Ａにおいて更新された後の新たなセキュリティ情報を取得する。セキュリティ情報を取得するまで待機状態となり（ステップＳ５６でＮＯ）、セキュリティ情報を取得したならば（ステップＳ５６でＹＥＳ）、処理をステップＳ５７に進める。

【０１１７】

ステップＳ５７においては、セキュリティ情報を更新し、処理をステップＳ５８に進める。ステップＳ５６において取得されたセキュリティ情報で、ＨＤＤ１１５に記憶されたパスワードテーブル９１を更新する。具体的には、ＨＤＤ１１５に記憶されているパスワードテーブル９１に含まれる識別情報とセキュリティ情報との組のうちから、ステップＳ５２において選択されたポリシーレコードの種類の項目に設定された識別情報と同じ識別情報を含む組を特定し、特定した組のセキュリティ情報を、ステップＳ５６において取得されたセキュリティ情報で更新する。ステップＳ５８においては、ステップＳ５８において更新されたセキュリティ情報の識別情報に対応する更新フラグを「１」に設定し、処理をステップＳ５９に進める。

【０１１８】

ステップＳ５９においては、更新履歴を記憶し、処理をステップＳ６０に進める。ここで記憶される更新履歴は、ステップＳ５８において更新されたセキュリティ情報の識別情報と、セキュリティ情報を更新した日時と、を含む。ステップＳ６０においては、次のポリシーレコードを処理対象に設定し、処理をステップＳ５３に戻す。

【０１１９】

第２の変形例においては、ＭＦＰ１００が備えるＣＰＵ１１１は、図９に示した実行制御処理を実行する。

【０１２０】

第２の変形例においては、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、セキュリティポリシーにより定められる更新日時より後の日時に、更新された後のセキュリティ情報を取得する場合は、セキュリティ情報を取得することに応じてセキュリティ情報を更新することができ、セキュリティポリシーにより定められる更新日時より前の日時に更新された後のセキュリティ情報を取得する場合は、更新日時にセキュリティ情報を更新することができる。

【０１２１】

また、管理サーバー２００が更新された後の新たなセキュリティ情報を記憶する場合、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれは、更新された後のセキュリティ情報を管理サーバー２００から取得するので、更新された後のセキュリティ情報の取得が容易である。

【０１２２】

また、ＭＦＰ１００，１００Ａ～１００Ｄにおいて、ユーザーが操作部１６３に入力するセキュリティ情報を更新された後のセキュリティ情報として取得する場合、セキュリティ情報を送受信しないようにして、機密性を向上させることができる。

【０１２３】

＜第３の変形例＞

第２の変形例においては、情報処理装置として機能するＭＦＰ１００，１００Ａ～１００Ｄそれぞれが、管理サーバー２００から取得したポリシーテーブル２９１に基づいて、セキュリティ情報を取得する。第３の変形例におけるセキュリティ情報更新システム１は、情報処理装置として機能するＭＦＰ１００，１００Ａ～１００Ｄのいずれかでセキュリティ情報が取得される事象の発生に連動して、セキュリティ情報が更新された装置と同一のグループに属する他の装置において、セキュリティ情報が更新される点で、第２の変形例におけるセキュリティ情報更新システム１と異なる。

【０１２４】

管理サーバー２００に記憶されたポリシーテーブル２９１によって、セキュリティ情報の種類ごとにグループに属する複数の装置が定められている。なお、同一グループに属す

る複数の装置を、ここでは、ポリシーテーブル２９１によって定めるようにしたが、グループに属する装置は、ポリシーテーブル２９１に限らない。例えば、情報処理装置として機能するＭＦＰ１００，１００Ａ～１００Ｄそれぞれが記憶するようにしてもよい。

【０１２５】

例えば、ＭＦＰ１００，１００Ａ～１００Ｄのいずれか、例えば、ＭＦＰ１００において、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」の種類のセキュリティ情報が更新される事象の発生に連動して、ＭＦＰ１００と同一グループに属するＭＦＰ１００Ａ～１００Ｄそれぞれにおいて、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」の種類のセキュリティ情報が更新される。例えば、セキュリティ情報が取得されたＭＦＰ１００が、同一グループに属する他の装置ＭＦＰ１００Ａ～１００Ｄそれぞれにセキュリティ情報とその種類を示す識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」とを送信し、ＭＦＰ１００Ａ～１００Ｄそれぞれが、ＭＦＰ１００から受信されるセキュリティ情報と識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」とを用いて更新する。また、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」の種類のセキュリティ情報が更新されたＭＦＰ１００が、管理サーバー２００にセキュリティ情報と識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」とを送信し、管理サーバー２００がＭＦＰ１００と同一グループに属する他の装置ＭＦＰ１００Ａ～１００ＤそれぞれにＭＦＰ１００から受信されるセキュリティ情報と識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」とを送信するようにしてもよい。

【０１２６】

第３の変形例におけるセキュリティ情報更新システム１においては、ＭＦＰ１００，１００Ａ～１００Ｄそれぞれが、セキュリティ情報の種類で特定されるグループに分類される。例えば、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」の種類のセキュリティ情報を記憶するＭＦＰ１００，１００Ａ～１００Ｄが同一のグループに分類される。そして、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」に対応するグループに属するＭＦＰ１００，１００Ａ～１００Ｄのいずれか、例えば、ＭＦＰ１００において、識別情報「ｍａｉｌ－ａｃｃｏｕｎｔ－Ａ」の種類のセキュリティ情報が更新される事象の発生に連動して、ＭＦＰ１００と同一グループに属するＭＦＰ１００Ａ～１００Ｄそれぞれにおいて、セキュリティ情報が更新される。このため、同一グループに属するＭＦＰ１００，１００Ａ～１００Ｄのいずれかで、セキュリティ情報を入力すればよく、セキュリティ情報を更新するためのユーザーによる作業を簡略にすることができる。

【０１２７】

今回開示された実施の形態はすべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は上記した説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【０１２８】

＜付記＞

（１）前記サービス提供サーバーにより提供されるサービスは、処理の履歴を記憶するサービスである、

（２）前記サービス提供サーバーにより提供されるサービスは、電子メールを送受信するサービスである、

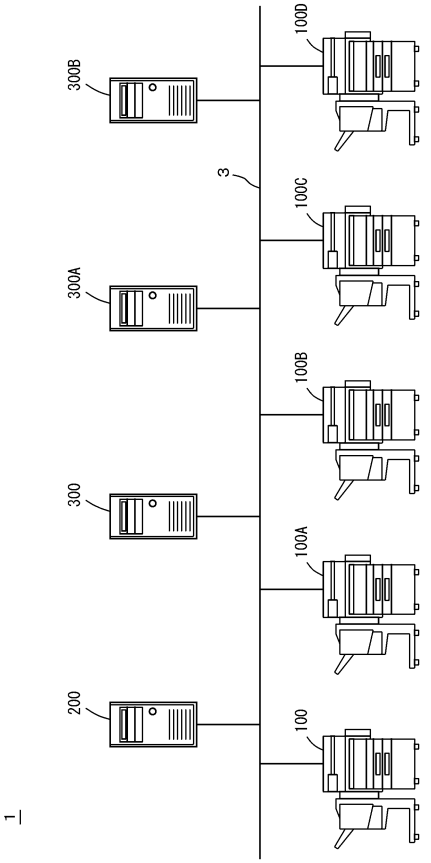
【符号の説明】

【０１２９】

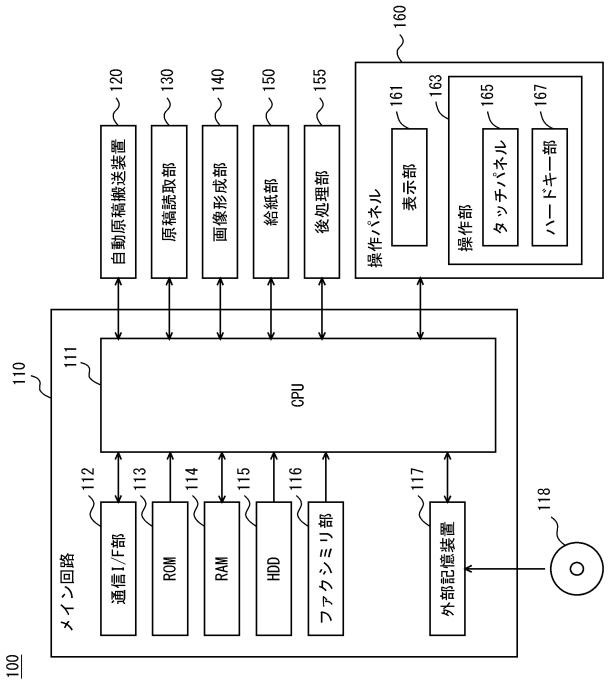
１　セキュリティ情報更新システム、３　ネットワーク、１００，１００Ａ～１００Ｄ　ＭＦＰ、２００　管理サーバー、３００，３００Ａ　サービス提供サーバー、１１０　メイン回路、１１１　ＣＰＵ、１１２　通信Ｉ／Ｆ部、１１３　ＲＯＭ、１１４　ＲＡＭ、１１５　ＨＤＤ、１１６　ファクシミリ部、１１７　外部記憶装置、１１８　ＣＤ－ＲＯＭ、１２０　自動原稿搬送装置、１３０　原稿読取部、１４０　画像形成部、１５０　給紙部、１５５　後処理部、１６０　操作パネル、１６１　表示部、１６３　操作部、１６５　タッチパネル、１６７　ハードキー部、２０１　ＣＰＵ、２０２　ＲＯＭ、２０３

ＲＡＭ、２０４　ＨＤＤ、２０５　通信部、２０６　表示部、２０７　操作部、２０９　外部記憶装置、２０９Ａ　ＣＤ－ＲＯＭ、５１　ポリシー取得部、５３　更新指示受信部、５３Ａ　認証情報取得部、５５　更新部、５７　処理実行部、５９　禁止部、６１　通知部、６３　通信状態検出部、９１　パスワードテーブル、２５１　ポリシー送信部、２５３　更新指示部、２９１　ポリシーテーブル。

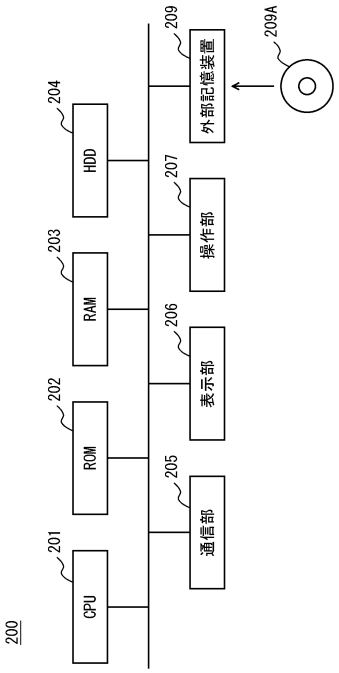
【図１】



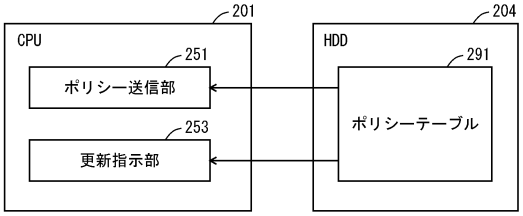
【図２】



【図３】



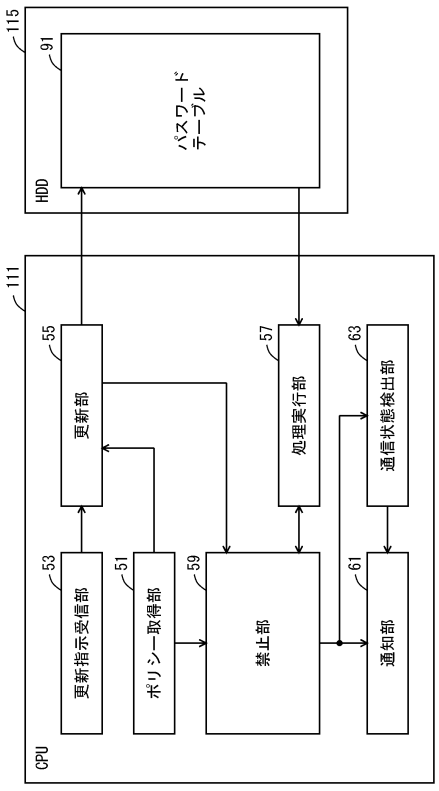
【図４】



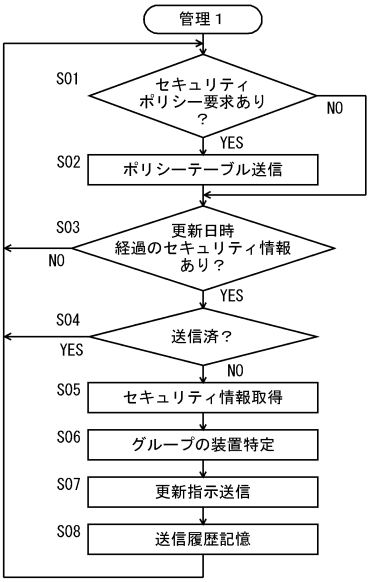
【図５】

種類	更新日時	グループ装置
mail-account-A	毎月1日 00:00	MFP-0,MFP-1,MFP-2,MFP-3,MFP-5
DB-account-B	毎月10日 00:00	MFP-0,MFP-1,MFP-2,MFP-3,MFP-5

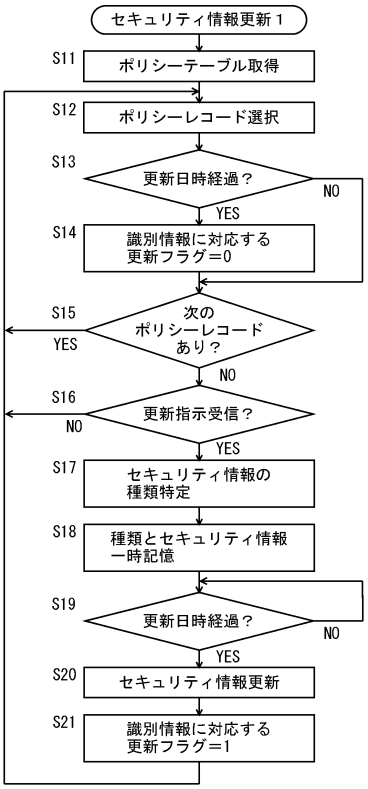
【図６】



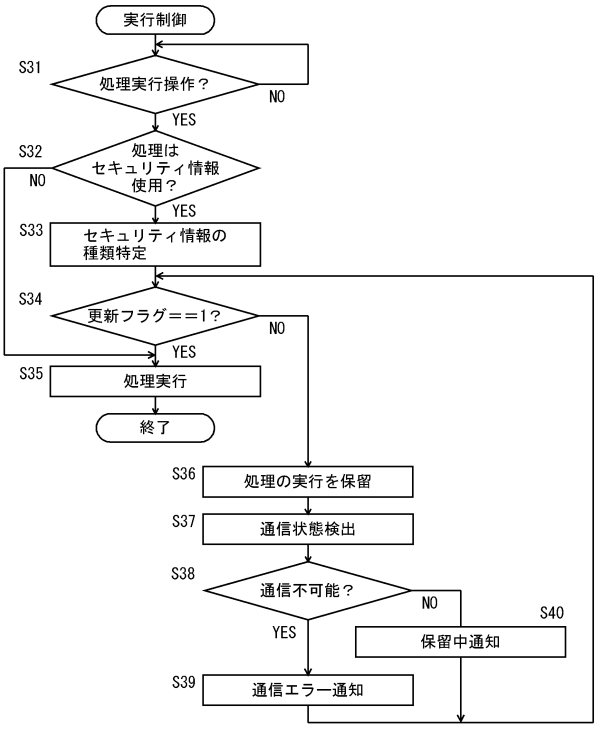
【図７】


管理１
S01
セキュリティ
ポリシー要求あり
？
NO
YES
S02
ポリシーテーブル送信
S03
更新日時
経過のセキュリティ情報
あり？
NO
YES
S04
送信済？
YES
NO
S05
セキュリティ情報取得
S06
グループの装置特定
S07
更新指示送信
S08
送信履歴記憶

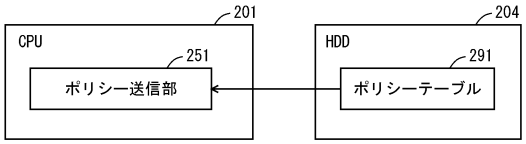
【図８】


セキュリティ情報更新１
S11
ポリシーテーブル取得
S12
ポリシーレコード選択
S13
更新日時経過？
NO
YES
S14
識別情報に対応する
更新フラグ＝0
S15
次の
ポリシーレコード
あり？
YES
NO
S16
更新指示受信？
NO
YES
S17
セキュリティ情報の
種類特定
S18
種類とセキュリティ情報
一時記憶
S19
更新日時経過？
NO
YES
S20
セキュリティ情報更新
S21
識別情報に対応する
更新フラグ＝1

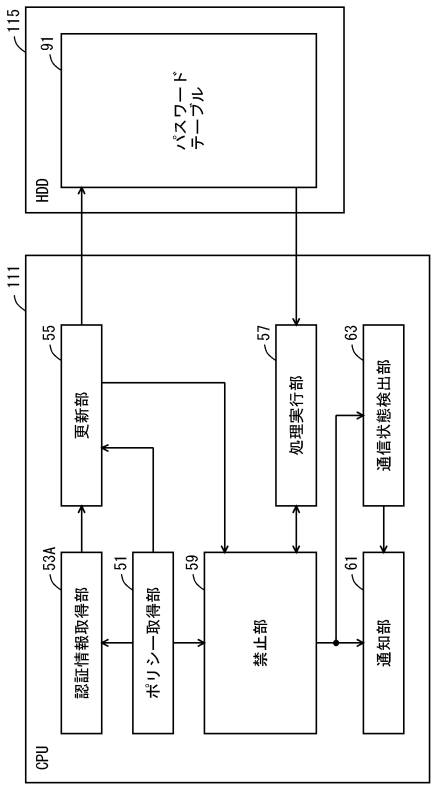
【図９】


実行制御
S31
処理実行操作？
NO
YES
S32
処理は
セキュリティ情報
使用？
NO
YES
S33
セキュリティ情報の
種類特定
S34
更新フラグ＝＝1？
NO
YES
S35
処理実行
終了
S36
処理の実行を保留
S37
通信状態検出
S38
通信不可能？
NO
YES
S40
保留中通知
S39
通信エラー通知

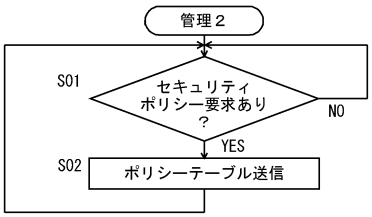
【図１０】


201
CPU
251
ポリシー送信部
204
HDD
291
ポリシーテーブル

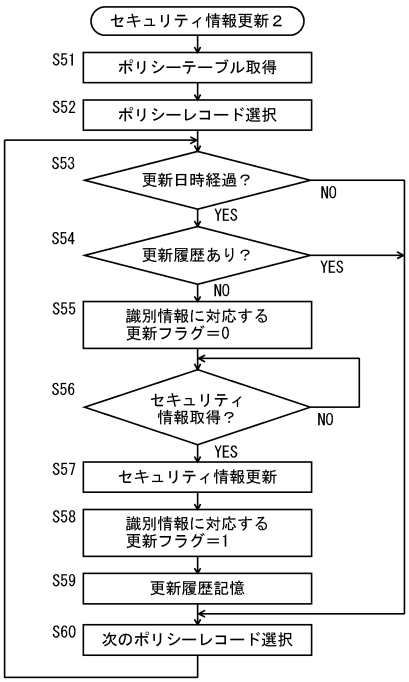
【図１１】


115
91
パスワードテーブル
HDD
111
55
更新部
57
処理実行部
63
通信状態検出部
53A
認証情報取得部
51
ポリシー取得部
59
禁止部
61
通知部
CPU

【図１２】


管理２
S01
セキュリティポリシー要求あり？
NO
YES
S02
ポリシーテーブル送信

【図１３】


セキュリティ情報更新２
S51
ポリシーテーブル取得
S52
ポリシーレコード選択
S53
更新日時経過？
NO
YES
S54
更新履歴あり？
YES
NO
S55
識別情報に対応する更新フラグ＝0
S56
セキュリティ情報取得？
NO
YES
S57
セキュリティ情報更新
S58
識別情報に対応する更新フラグ＝1
S59
更新履歴記憶
S60
次のポリシーレコード選択

フロントページの続き

(72)発明者　丸山　倫子
東京都千代田区丸の内二丁目７番２号　コニカミノルタ株式会社内
(72)発明者　羽場　笑子
東京都千代田区丸の内二丁目７番２号　コニカミノルタ株式会社内

審査官　岸野　徹

(56)参考文献　特開２０１３－０３３４３７（ＪＰ，Ａ）
特開２０１４－１３４９７８（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／３１
Ｇ０６Ｆ　３／１２