(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2006-251932
(P2006-251932A)
(43)公開日　平成18年9月21日(2006.9.21)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	520B	5B017
		G06F	12/14	530B	
		G06F	12/14	530D	
		G06F	12/14	560B	

審査請求 未請求　請求項の数 18　ＯＬ　（全 27 頁）

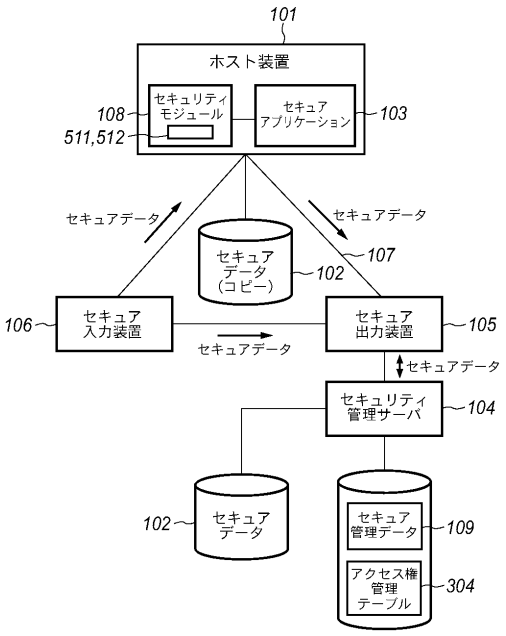
(21)出願番号　特願2005-64560 (P2005-64560)
(22)出願日　平成17年3月8日 (2005.3.8)

(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
(72)発明者　小澤　修司
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 AA03　BA06　BB10　CA16

(54)【発明の名称】セキュリティ管理方法、装置およびセキュリティ管理用プログラム

(57)【要約】
【目的】ネットワークでセキュリティ管理サーバと接続されていない環境においてもセキュリティを維持しながらセキュアデータへのアクセスを許可し利便性を損なわない。
【構成】PC１０１、出力装置１０５、入力装置１０６等のセキュリティモジュール１０８は、自身の設置状態に応じて動的にセキュリティレベル５１１を決定する機能と、認証履歴を保存する機能とを備えている。セキュアアプリケーション１０３等は、セキュリティレベル５１１に応じてセキュアデータに対する処理内容を制限する。これにより、ネットワークでセキュリティ管理サーバ１０４と接続されていない装置であっても、認証履歴によりユーザは認証を受けるとともに、セキュリティレベルを動的に変更することで処理宣言を変更し、セキュリティを維持しながらユーザにセキュアデータへの処理を許可する。【選択図】図１



【特許請求の範囲】
【請求項１】
装置のセキュリティレベルと利用者のアクセス権とに応じて前記処理対象データへのアクセスを制御するセキュリティ管理用プログラムであって、
認証サーバにアクセス不可能な場合、保存されたユーザ認証履歴を参照して当該ユーザのアクセス権を設定するユーザ認証工程と、
前記装置のセキュリティレベルを当該装置の状態に応じて決定し、決定されたセキュリティレベルを保存するセキュリティレベル設定工程と
を備えることを特徴とするセキュリティ管理用プログラム。
【請求項２】
前記ユーザ認証工程は、さらに、ユーザ認証の際に、認証サーバにアクセス可能であれば、認証サーバにより当該ユーザに対して与えられたアクセス権を当該ユーザのアクセス権として設定するとともに、ユーザ識別子と設定したアクセス権とをユーザ認証履歴としてメモリに保存することを特徴とする請求項１に記載のプログラム。
【請求項３】
前記セキュリティレベル決定工程は、前記ユーザ認証工程において、前記認証サーバにアクセス不可能な場合、または、当該ユーザにアクセス権が設定できなかった場合、または、ユーザに与えられたアクセス権限が所定ランク以下の場合、または、前記装置が所定の範囲内に存在していない場合には、それぞれに該当しない場合に対して、前記セキュリティレベルを引き下げることを特徴とする請求項１または２に記載のプログラム。
【請求項４】
前記認証サーバにより、あらかじめセキュリティレベルの引き下げの対象とならないケースの認証を受けて、当該ケースを特定する情報を保存する事前認証工程をさらに備え、
前記セキュリティレベル決定工程においては、前記セキュリティレベルが引き下げられる場合であっても、前記事前認証工程において認証を受けたケースに該当する場合には、セキュリティレベルの引き下げは行わないことを特徴とする請求項３に記載のプログラム。
【請求項５】
前記データを処理するデータ処理工程を更に備え、
前記データ処理工程では、前記処理対象データごとに、前記セキュリティレベルと前記利用者のアクセス権とに応じてあらかじめ定められた処理制限に応じて前記処理対象データを処理可能であって、
前記処理制限は、閲覧処理および編集処理および印刷処理の少なくともいずれかについて定められていることを特徴とする請求項１乃至４のいずれか１項に記載のプログラム。
【請求項６】
前記処理制限は、前記閲覧処理または印刷処理については、セキュリティレベルに応じて、（１）処理対象データ全体を対象として処理が可能であるか、（２）ウォーターマークが付加されるか、（３）個人情報や詳細情報がマスク処理が行われるか、（４）目次やトピックを対象として処理が可能であるか、（５）サムネイル表示あるいは印刷が可能であるか、（６）処理は不可能であるかの少なくともいずれかが定められていることを特徴とする請求項５に記載のプログラム。
【請求項７】
前記処理制限は、編集処理については、セキュリティレベルに応じて処理が可能であるかあるいは不可能であるかが定められていることを特徴とする請求項５または６に記載のプログラム。
【請求項８】
前記データ処理工程では、前記セキュリティレベルと前記利用者のアクセス権とに応じてあらかじめ定められた処理制限を、前記セキュリティ管理プログラムによる処理対象データに共通に適用することを特徴とする請求項１乃至４のいずれか１項に記載のプログラム。

【請求項９】
装置のセキュリティレベルと利用者のアクセス権とに応じて前記処理対象データへのアクセスを制御するセキュリティ管理装置であって、
認証サーバにアクセス不可能な場合、保存されたユーザ認証履歴を参照して当該ユーザのアクセス権を設定するユーザ認証手段と、
前記装置のセキュリティレベルを当該装置の状態に応じて決定し、決定されたセキュリティレベルを保存するセキュリティレベル設定手段と
を備えることを特徴とするセキュリティ管理装置。
【請求項１０】
装置のセキュリティレベルと利用者のアクセス権とに応じて前記処理対象データへのアクセスを制御するセキュリティ管理方法であって、
認証サーバにアクセス不可能な場合、保存されたユーザ認証履歴を参照して当該ユーザのアクセス権を設定するユーザ認証工程と、
前記装置のセキュリティレベルを当該装置の状態に応じて決定し、決定されたセキュリティレベルを保存するセキュリティレベル設定工程と
を備えることを特徴とするセキュリティ管理方法。
【請求項１１】
装置のセキュリティレベルを当該装置の状態に応じて決定し、決定されたセキュリティレベルを保存するセキュリティレベル設定工程と、
前記セキュリティレベルと利用者のアクセス権とに応じて前記処理対象データへのアクセスを制御する制御工程と
を備えることを特徴とするセキュリティ管理用プログラム。
【請求項１２】
装置のセキュリティレベルを当該装置の状態に応じて決定し、決定されたセキュリティレベルを保存するセキュリティレベル設定手段と、
前記セキュリティレベルと利用者のアクセス権とに応じて前記処理対象データへのアクセスを制御する制御手段と
を備えることを特徴とするセキュリティ管理装置。
【請求項１３】
装置のセキュリティレベルを当該装置の状態に応じて決定し、決定されたセキュリティレベルを保存するセキュリティレベル設定工程と、
前記セキュリティレベルと利用者のアクセス権とに応じて前記処理対象データへのアクセスを制御する制御工程と
を備えることを特徴とするセキュリティ管理方法。
【請求項１４】
前記装置はコンピュータまたはプリンタまたは画像スキャナであることを特徴とする請求項１乃至８または１１に記載のプログラム。
【請求項１５】
請求項９または請求項１２に記載のセキュリティ管理装置を有するホストコンピュータと、請求項９または請求項１２に記載のセキュリティ管理装置を有するプリンタとを具備するセキュア印刷システムであって、
前記ホストコンピュータのセキュリティレベルと、前記プリンタのセキュリティレベルの、いずれか低い方のセキュリティレベルに従って、データの印刷が行われることを特徴とするセキュアドキュメントシステム。
【請求項１６】
セキュリティ管理サーバにアクセスできるか否かを判別する判別手段と、
前記判別手段によりセキュリティ管理サーバにアクセスできると判別された場合、アクセス管理サーバからのアクセス権情報に基づきセキュアデータの編集を行う編集手段と、
前記判別手段によりセキュリティ管理サーバにアクセスできないと判別された場合、装置の状態に応じてセキュアデータの出力を行う出力手段とを有することを特徴とするセキ

ュリティ管理装置。
【請求項１７】
セキュリティ管理サーバにアクセスできるか否かを判別する判別ステップと、
前記判別ステップによりセキュリティ管理サーバにアクセスできると判別された場合、アクセス管理サーバからのアクセス権情報に基づきセキュアデータの編集を行う編集ステップと、
前記判別ステップによりセキュリティ管理サーバにアクセスできないと判別された場合、装置の状態に応じてセキュアデータの出力を行う出力ステップとを有することを特徴とするセキュリティ管理方法。
【請求項１８】
セキュリティ管理サーバにアクセスできるか否かを判別する判別ステップと、
前記判別ステップによりセキュリティ管理サーバにアクセスできると判別された場合、アクセス管理サーバからのアクセス権情報に基づきセキュアデータの編集を行う編集ステップと、
前記判別ステップによりセキュリティ管理サーバにアクセスできないと判別された場合、装置の状態に応じてセキュアデータの出力を行う出力ステップと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】
本発明はたとえば文書管理システムに係わり、特にネットワークを介して接続されたパーソナルコンピュータ、サーバ、出力装置、入力装置で扱われる文書への統合的なセキュリティ管理を行なうセキュアドキュメントシステム、すなわちセキュリティ管理方法、装置およびセキュリティ管理用プログラムに関するものである。
【背景技術】
【０００２】
コンピュータネットワークからの機密情報の漏洩を防止するための対策として、セキュアドキュメントシステムがある。セキュアドキュメントシステムでは、ネットワークに接続されたＰＣ、入出力装置およびそこで取り扱われるセキュアデータを、セキュリティ管理サーバにて一元管理する。セキュアドキュメントシステムはアクセス権管理を行なうセキュリティ管理サーバを有し、ネットワークに接続されたＰＣや入出力装置が暗号化されたセキュアデータにアクセスする際には、アクセスする主体、たとえばセキュアアプリケーションやセキュアプリンタ等が適時セキュリティ管理サーバから認証を得なければならない。
【０００３】
このため、暗号化されたセキュアデータへアクセスするには、アクセスの主体がセキュリティ管理サーバにアクセス可能である必要がある。仮にセキュアデータをセキュアドキュメントシステムの外に持ち出してもサーバによる認証が得られないため、セキュアデータに対する一切のアクセスは行なえない。また、セキュアデータにアクセスするＰＣおよびアプリケーション、入出力装置のアクセス状況やアクセス履歴を全てセキュリティ管理サーバによって一元的に管理することが出来る。
【０００４】
しかしながら、セキュアデータをセキュアドキュメントシステムの外部へと持ち出して利用したい場合も多い。その解決方法として、例えば、外出先からセキュリティ管理サーバに電話回線を介してアクセスし、認証を取得するリモートアクセスという方法がある（特許文献１参照）。
【特許文献１】特開２００２－３６６３１４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００５】

しかしながら、リモートアクセスを用いてセキュアドキュメントシステムにアクセスする場合、セキュリティ管理サーバがたとえば電話回線等、外部からのアクセスを許可している必要がある。これは、コンピュータウィルスや侵入などに対する防御という観点からセキュリティ上望ましく無いという問題がある。

【０００６】

さらに、セキュアドキュメントシステムについては、たとえば企業における管理者等や管理機器、管理プログラム等により高度な管理が期待できるが、セキュリティ管理サーバにリモートアクセスしようとするパーソナルコンピュータ等の装置は、セキュアドキュメントシステムから切り離されてセキュリティ管理水準が低い状態にある。そのため、セキュアドキュメントシステムに属する装置と同水準のアクセス権限あるいは処理権限を与えてしまうと、機密情報の漏洩などが生じ、セキュリティが失われるおそれがあるといった問題点がある。

【０００７】

すなわち、セキュリティを高めれば操作性、利便性が低下し、操作性、利便性を高めればセキュリティが低下し、これら２つの相反する要求を満たすことが困難であった。

【０００８】

本発明は上記従来例に鑑みてなされたもので、保護すべきセキュアデータを扱う装置の状況に応じて当該セキュアデータに対する処理の制限を変更することで、セキュリティの程度に応じた利便性を提供できる。このため、機密が保持しやすい状況においてキュリティ維持のために利便性を過度に損ねたり、機密が漏洩しやすい状況においてセキュリティを損ねて利便性を高めることなどを防止できるセキュリティ管理方法、装置およびセキュリティ管理用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】

【０００９】

上記目的を達成するために本発明は以下の構成を備える。

【００１０】

装置のセキュリティレベルと利用者のアクセス権とに応じて前記処理対象データへのアクセスを制御するセキュリティ管理用プログラムであって、

認証サーバにアクセス不可能な場合、保存されたユーザ認証履歴を参照して当該ユーザのアクセス権を設定するユーザ認証工程と、

前記装置のセキュリティレベルを当該装置の状態に応じて決定し、決定されたセキュリティレベルを保存するセキュリティレベル設定工程とを備える。

【００１１】

あるいは、セキュリティ管理用プログラムであって、装置のセキュリティレベルを当該装置の状態に応じて決定し、決定されたセキュリティレベルを保存するセキュリティレベル設定工程と、

前記セキュリティレベルと利用者のアクセス権とに応じて前記処理対象データへのアクセスを制御する制御工程とを備える。

【００１２】

あるいは、セキュリティ管理サーバにアクセスできるか否かを判別する判別手段と、

前記判別手段によりセキュリティ管理サーバにアクセスできると判別された場合、アクセス管理サーバからのアクセス権情報に基づきセキュアデータの編集を行う編集手段と、

前記判別手段によりセキュリティ管理サーバにアクセスできないと判別された場合、装置の状態に応じてセキュアデータの出力を行う出力手段とを有することを特徴とするセキュリティ管理装置。

【発明の効果】

【００１３】

本発明によれば、保護すべきセキュアデータを扱う装置の状況に応じて当該セキュアデータに対する処理の制限を変更することで、セキュリティの程度に応じた利便性を提供できる。このため、機密が保持しやすい状況においてキュリティ維持のために利便性を過度

に損ねたり、機密が漏洩しやすい状況においてセキュリティを損ねて利便性を高めることなどを防止できる。

【発明を実施するための最良の形態】

【００１４】

［定義］

実施形態を説明する前にまずいくつかの用語についてその定義をしておく。セキュアデータとは暗号化されて保護されたデータをいう。セキュアアプリケーションとは、セキュアデータを処理するための暗号化機能および復号機能を有するアプリケーションプログラムをいう。セキュア出力装置とは、セキュアデータを復号するための復号機能を有するプリンタ等の出力装置をいう。セキュア入力装置とは、入力データをセキュアデータ化するための暗号化機能を有するスキャナ等の入力装置をいう。セキュリティモジュールとは本実施形態で説明するユーザ認証要求機能やセキュリティレベル設定機能を有するプログラムモジュールである。セキュリティモジュールは、コンピュータにおいてはセキュアアプリケーション等により使用される。セキュア入出力装置において使用される場合もある。セキュリティ管理サーバとは、ユーザのアクセス権やセキュアデータの管理、それらに伴う処理等を行うサーバ装置である。セキュアドキュメントシステムとは、セキュアアプリケーションがインストールされたコンピュータやセキュア入力装置、セキュア出力装置、セキュリティ管理サーバ等を含み、ドキュメントデータをセキュアデータとして流通させ、その編集や印刷等の処理を行う文書処理システムを言う。

【００１５】

［第１実施形態］

以下、添付図面に従って本発明に係わる実施形態を詳細に説明する。図１から図４は本発明であるセキュリティレベルに応じてセキュアデータに対する処理内容を制限する処理を実現するセキュアドキュメントシステムの構成の一例を示す。

【００１６】

＜セキュアドキュメントシステムの構成＞

図１は、本発明が適用されるセキュアドキュメントシステムの構成範囲を示したものである。本システムは、ネットワーク１０７に接続されセキュアデータ１０２にアクセスすることが出来るセキュア出力装置１０５、ホスト装置１０１に搭載されたセキュアアプリケーション１０３およびセキュリティモジュール１０８、あるいはセキュア入力装置１０６の少なくとも一つと、それら装置１０３、１０５、１０６に接続されたセキュリティ管理サーバ１０４により構成される。なお図１は接続関係は模式的な例であり、物理的なネットワークはバスアーキテクチャやスターアーキテクチャといった構造を有している。また、セキュリティ管理サーバ１０４はセキュア出力装置１０５に限らず、セキュア入力装置１０６やホストコンピュータ１０１によりアクセス可能である。またセキュリティ管理サーバ１０４は、セキュア入力装置１０６やホスト装置１０１に接続されていても本発明が適用されるセキュアドキュメントシステムの構成範囲としては同様である。セキュアアプリケーション１０３およびセキュリティモジュール１０８は必ずしもホスト装置１０１に搭載されている必要はなく、セキュア出力装置１０５やセキュア入力装置１０６に搭載されていてもよい。セキュアアプリケーション１０３およびセキュリティモジュール１０８、セキュア出力装置１０５、セキュア入力装置１０６とは、暗号化されたセキュアデータ１０３にアクセス出来、セキュリティ管理サーバ１０４により認証を受けることが出来る。

【００１７】

セキュリティ管理サーバ１０４は、登録されたセキュアデータ１０２を保存して管理するほか、セキュア管理データ１０９およびアクセス権管理テーブル３０４を保存管理する。セキュアデータ１０２は、セキュアドキュメントシステム上の装置により読み出される。たとえば図１では、ホスト装置１０１がセキュアデータ１０２の複製を読み出してそのストレージ等に保存している。セキュリティモジュール１０８はそれがインストールされた装置のセキュリティレベルの監視、および、セキュリティ管理サーバ１０４への作業指

示を実行する。セキュアアプリケーション１０３を利用してユーザは閲覧、編集、印刷等の操作や処理を行なうこと可能である。その操作や処理はセキュリティアプリケーション１０３がセキュリティモジュール１０８より取得したセキュリティレベルによって制限される。

【００１８】

セキュアアプリケーション１０３やセキュア出力装置１０５は、セキュアデータ１０２を解読する機能を備えている。解読は復号鍵を用いて行われ、その復号鍵はたとえばセキュリティ管理サーバ１０４や、その他の鍵サーバ等により提供されたり、あるいはホスト装置１０１自身が保存管理していても良い。これは暗号化鍵についても同様である。

【００１９】

＜セキュアデータ＞

図２は、本発明が適用されるセキュアドキュメントシステムのセキュアデータ１０２の内部構造の一例を示したものである。セキュアデータ１０２は暗号化されており、少なくともデータＩＤ部２０１と実データ部２０２の２種類の領域を持つ。このデータＩＤ部２０１はセキュリティ管理サーバ１０４で管理される単位でデータＩＤ部２０１が割り当てられ、必ずしもセキュアデータ１０２のファイル名と１対１対応する必要はなく、ファイル名が同じであっても異なるデータＩＤが割り当てうる。実データ部２０２の内容は、文書、画像、映像等で有り得る。セキュアデータ１０２自体が暗号化されているため、セキュアアプリケーション１０３およびセキュリティモジュール１０８、セキュア出力装置１０５、セキュア入力装置１０６、セキュリティ管理サーバ１０４以外の装置やアプリケーションでは実データ部２０２にアクセスすることは出来ない。なお、セキュアデータ１０２をデータＩＤ２０１で特定するために、データＩＤ２０１については平文のままとしてもよい。本実施形態においては、セキュアデータ１０２にはさらにセキュリティレベル別処理テーブル２０３が含まれる。セキュリティレベル別処理テーブル２０３は、各装置のセキュリティレベルに応じた処理内容（あるいは処理の制限や制約）が記載されたテーブルである。セキュリティレベル別処理テーブル２０３には、編集用テーブル２０４、閲覧用テーブル２０５、印刷用テーブル２０６を含む。それぞれ編集処理における制約、閲覧処理における制約、印刷処理における制約を示すデータが、１～５のセキュリティレベル毎に登録されている。本実施形態ではセキュリティレベル「１」を、当該装置のセキュリティレベルが低い状態、セキュリティレベル「５」を当該装置のセキュリティレベルが高い状態としている。なおセキュリティレベルは、後述の図２１あるいは図２９の手順で与えられる。編集用テーブル２０４、閲覧用テーブル２０５、印刷用テーブル２０６において、各装置では、そのセキュリティレベルに対応して登録されている処理の制約を受ける。閲覧用テーブル２０５を例にすれば、装置のセキュリティレベルが現在「５」であるとすると、たとえばその装置にインストールされたセキュアアプリケーションによって、セキュアデータを復号してそのまま閲覧できる。装置のセキュリティレベルが現在「４」であるとすると、閲覧時には必ず「社外秘」のウォーターマークが付加される。装置のセキュリティレベルが現在「３」であるとすると、閲覧時には個人情報や詳細情報はマスクされて表示されない。装置のセキュリティレベルが現在「２」であるとすると、閲覧時には必ずサムネール化される。装置のセキュリティレベルが現在「１」であるとすると、閲覧が許されない。このように、装置のセキュリティレベルが「４」以下であれば、通常表示である復号された元データに何も手を加えていない状態での閲覧は出来ない。印刷の場合にも同じ要領で制約を受けるが、制約の内容は異なる設定が可能である。図２の例では、セキュリティレベルが２であれば、目次及びトピックに限って印刷が許可される。なお、閲覧や印刷において、データの一部が表示あるいは印刷されないという制約は、たとえば制約の内容毎に制約の対象となる部分をあらかじめ定義しておけばよい。たとえば「個人情報」の領域や、「詳細情報」の領域、「目次」や「トピック」の領域等を、平文化したセキュアデータにおいて定義しておけばよい。

【００２０】

＜セキュア管理データ＞

図３は、本発明が適用されるセキュアドキュメントシステムのセキュリティ管理サーバ１０４に格納されたセキュア管理データ１０９およびユーザ管理データ３０４の一例を示したものである。セキュリティ管理サーバ１０４には、セキュアデータ１０２に１対１で対応づけられたセキュア管理データ１０９が格納されている。セキュア管理データ１０９は、データＩＤ部３０１、アクセスログ格納部３０２と基本的には２種類の領域を持つ。よってセキュア管理データは、セキュアドキュメントシステム内に存在するデータＩＤが割り当てられた全てのセキュアデータ１０２と同じ数だけ存在する。データＩＤ部３０１はセキュアデータ１０２のデータＩＤ部２０１に対応しており、関連づけられたセキュアデータ１０２とは同一のデータＩＤを有する。アクセスログ格納部３０３にはセキュアアプリケーション１０３およびセキュリティモジュール１０８、セキュア出力装置１０４、セキュア入力装置１０５のセキュアデータ１０２に対するアクセス状況がログデータとして格納されている。

【００２１】

ユーザ管理データ３０４には、ユーザＩＤに対するアクセス権を示すデータが関連づけられている。このユーザ管理データ３０４にはユーザＩＤ３０５毎のアクセス権の種別を示すデータ（アクセス権種別）３０６が登録されている。ユーザのアクセス権はこのユーザ管理データ３０４の情報を元に定められる。なお、アクセス許可種別３０６とは、許可された処理内容を示す情報である。具体的には、たとえばセキュアデータ１０２の編集やコピー（例えばＰＣに接続された記憶装置へのセキュアデータ（電子ファイル）の保存）のための「編集」権限、表示処理のための「閲覧」権限、新たなセキュアデータの登録や編集後の保存を承認するための「承認」権限、管理のための「管理」権限が含まれる。これら権限は排他的であっても良いが、本実施形態では包含関係にある。アクセス許可種別３０６には、たとえばこれら処理の区分に応じたコードが格納されている。そして、たとえば「編集」権限を有するユーザが取得したセキュアデータを出力あるいは加工する場合には、そのセキュアデータに関連づけられたセキュリティレベル別処理テーブル２０３が参照される。そして、当該ユーザに対して許される具体的な処理が決定され、そのユーザには許された処理のみ操作を許す。

【００２２】

なお、ユーザ認証がパスワード認証の場合には、ユーザＩＤに対応付けたパスワードが保存され、認証時におけるパスワードの照合に使用される。

【００２３】

＜認証手順例の概略＞

図４Ａ，４Ｂは、本発明が適用されるセキュアドキュメントシステムのセキュリティ管理サーバ１０４とセキュアアプリケーション１０３およびセキュリティモジュール１０８やセキュア入出力装置との認証の仕組みを示したものである。図４Ａはセキュリティ管理サーバにアクセス可能な場合と、図４Ｂはセキュリティ管理サーバにアクセスできない場合の手順である。

【００２４】

ユーザが編集や印刷等、暗号化されたセキュアデータ１０２に対して作業を行いたい場合、セキュアアプリケーション１０３やセキュア出力装置１０５、セキュア入力装置１０６、あるいはセキュリティモジュール１０８の提供するユーザインターフェース（ＵＩ）に行いたい作業に対する作業指示４０１を入力する。このとき作業内容４０２、該当セキュアデータ１０２を指示すると共に、ユーザを特定するユーザＩＤ４０３も合わせて指定する。ユーザの認証や処理の選択など、セキュアデータを扱う上で、個々のデータの属性等やそれを扱うアプリケーション、装置から独立した事項に関しては、後述する図７，８等に示すようにセキュリティモジュール１０８が提供するユーザインターフェースを介して入力される。また、編集操作や印刷設定、入力設定等、個々のデータの属性等やそれを扱う装置やアプリケーションに従属する事項に関しては、セキュアアプリケーション１０８やセキュア入力装置１０６、セキュア出力装置１０５により提供されるユーザインターフェースを介して入力される。なお図４ではセキュアアプリケーション１０３を代表とし

て説明しているが、これをセキュア入力装置１０６、あるいはセキュア出力装置１０５に置き換えても以下の説明は同様である。また、図４では、記録媒体等に記録されたセキュアデータがユーザによりセキュアドキュメントシステムに入力された場合、あるいは、セキュアアプリケーションにより新たに作成された場合を説明する。セキュリティ管理サーバ１０４により管理されている既存のセキュアデータを利用する場合には、セキュアデータ１０２はセキュリティ管理サーバ１０４に保存されているため、ユーザから入力されることはない。

【００２５】

図４Ａにおいて、ユーザから、ユーザＩＤ４０３、セキュアデータ１０２と共に作業内容の指示（以下単に作業内容と呼ぶ。）４０２を受けたセキュアアプリケーション１０３およびセキュリティモジュール１０８は、セキュアデータ１０２のデータＩＤ部２０１からデータＩＤを抽出し（４０４）、セキュリティ管理サーバ１０４に作業認証依頼４０５を行う。このときユーザＩＤ４０２、パスワードあるいはパスワードから派生したデータ４０３がセキュリティ管理サーバ１０４に渡される。セキュリティ管理サーバ１０４ではそれらの情報から、ユーザ管理テーブル３０４を参照して、該当するユーザＩＤが登録されているか否かを判定し、登録されていればそのユーザのアクセス権を読み取る（４０７）。ユーザＩＤが登録されており、パスワード認証が成功すれば、認証は成功である。その場合、読み取られたアクセス権（アクセス権を示す情報）とともにアクセス許可４０８をセキュリティモジュール１０８に返す（４０９）。認証が受けられたセキュアアプリケーション１０３およびセキュリティモジュール１０８、セキュア出力装置１０５、セキュア入力装置１０６は、該当セキュアデータに対しユーザからの指示４１５に従って作業を行い（４１０）、作業完了通知を行う（４１１）。この作業完了通知４１１はユーザとセキュリティ管理サーバ１０４の両方に対して行われる。セキュリティ管理サーバ１０４へはユーザＩＤ４０３、データＩＤ４０６、作業完了通知４０７を発行することで、セキュリティ管理サーバ１０４に格納されたセキュア管理データ１０９のアクセスログ格納部３０２のアクセスログが更新される（４１３）。ユーザに対しては作業管理通知４１２と共に、作業を施したセキュアデータ１０２を発行することで、ユーザが指示した作業が完了する（４１４）。

【００２６】

一方、セキュリティ管理サーバ１０４にアクセスできない場合には、図４Ｂの手順となる。ユーザＩＤ４０２およびパスワード４０３が入力されたセキュリティモジュール１０８は、ユーザ認証を、あらかじめ記憶しておいた認証履歴情報を参照して行う（４２１）。認証履歴情報には少なくともユーザＩＤとそのアクセス権情報とが対で保存されている。アクセス権情報を獲得すれば、後は図４Ａと同様である。

【００２７】

図２８に認証履歴情報２８００の一例を示す。認証履歴情報には、ユーザＩＤ２８０１、付与されたアクセス権２８０２、認証日時２８０３が含まれる。パスワード認証が行われる場合にはパスワードを含める。

【００２８】

＜セキュリティレベル＞

図５を用いて各装置のセキュリティレベル決定の様子を説明する。セキュリティレベルは、本実施形態では固定的に与えられず、装置の置かれた状態（すなわち装置に入力される、状態を示す情報）に応じてセキュリティモジュール１０８により決定される。装置の状態を示す情報の例としては以下に示すものがある。

（１）各装置に常駐するセキュリティモジュール１０８がセキュリティ管理サーバ１０４へのアクセスが可能であるか否か（５０１）。

（２）ユーザ認証におけるアクセス権の種類（５０２）

（３）装置が備えているＧＰＳ５０３、スケジューラソフトやデータベース５０４、出退社記録５０５から得られる装置の現在位置情報。

（４）装置にウィルスチェックソフト５０６が導入されているか否か。

（５）ＲＦＩＤ認証５０９。ただしこれは第５の実施形態において詳述する。

【００２９】

以上のような情報をセキュリティレベルの判断要素とする。セキュリティ管理サーバ１０８へのアクセスが出来ない状態では、ユーザ認証が実行出来ないため、過去の認証情報５１０をもってユーザ認証とする。本実施形態においてはセキュリティ管理サーバでの認証か、過去の認証情報（認証履歴情報と同じ。）による認証の何れも行なえ無い場合はセキュアデータへのアクセスは不可能となっている。認証出来ないことによってセキュリティレベルを低下させるような動作にすることにより、認証が出来ない場合にもセキュリティレベルを利用し、セキュリティを保ちながらセキュアデータへのアクセスを実現できる。

【００３０】

セキュリティモジュール１０８は、減点・加点内容表５１２（図５（Ｂ））を保持する。減点・加点内容表５１２には、セキュリティレベルの各判断要素５０１～５１０の状態により、どのようにセキュリティレベルを上下させるかが記載されており、セキュリティモジュール１０８は各判断要素５０１～５１０より得られた状態を減点、加点内容表５１２に照らし合わせてセキュリティレベルの上下を行なう。またユーザに与えられたアクセス権毎に減点・加点内容表５１２を複数を保持しておき、減点・加点内容表をアクセス権に応じて切り替えることも可能である。また、アクセス権に応じて一定点数減点するようにしてもよい。本実施形態では後者の処理が行われる。

【００３１】

図６は本発明を適応するのに好適なセキュアドキュメントワークフローの一例を示している。なお本発明では承認のアクセス権をもつユーザは承認、登録、セキュアデータ取得、印刷の処理が可能、編集のアクセス権を持つユーザは登録、セキュアデータ取得、印刷の処理が可能、閲覧のアクセス権を持つユーザはセキュアデータ取得、印刷のみ可能となっている。また、セキュリティ管理サーバ１０４の管理を行なう管理のアクセス権が別途存在する。

【００３２】

編集または承認のアクセス権をもったユーザ６０１により、装置６１１においてセキュアデータ１０２が作成される。作成されたセキュアデータ１０２は編集または承認のアクセス権をもったユーザ６０１によって装置６１２において登録処理が行われ、承認のアクセス権をもったユーザ６０２によって承認処理されることにより、初めてセキュリティ管理サーバ１０４によって管理されるようになる。セキュリティ管理サーバ１０４に管理されたセキュアデータ１０２は閲覧、編集、承認の何れのアクセス権をもったユーザ６０３でも装置６１３においてファイル取得処理を行うことにより、閲覧および印刷が可能となる。もちろん装置６１１，６１２，６１３は同一の装置であっても良い。編集あるいは承認のアクセス権をもったユーザ６０１によって取得され編集されたセキュアデータ１０２は、承認者６０２によって再度承認処理されなければならない。

【００３３】

図２１に本実施形態におけるセキュリティモジュール１０８５によるセキュリティレベルの決定手順の例を示す。図２１の手順は、セキュリティレベルを変更させるようなイベントを割り込み等で入力しておき、その割り込みによって実行されても良いし、定期的に実行されても良い。要は、最新の状態に合わせてセキュリティレベルが維持されていることが必要である。

【００３４】

セキュリティレベルは、セキュリティモジュールが実行される装置の持つ記憶部の所定位置に記憶される。まずその記憶位置に、セキュリティレベルとして「５」を記憶する（Ｓ２１０１）。次に、現在セキュリティ管理サーバ１０４にアクセス可能であるか判定する（Ｓ２１０２）。可能でなければ、セキュリティレベルから一定の値（例えば３）を減ずる（Ｓ２１０３）。次に、ユーザ認証フラグを参照して、ユーザ認証が成功したか判定する（Ｓ２１０４）。ユーザ認証フラグは、後述する図２２等の手順でセキュリティ管理

サーバ１０４によるユーザ認証が成功した場合にその旨セットされるフラグである。認証が成功した場合には、認証の種類、すなわち得られたアクセス権に応じてセキュリティレベルを下げる。たとえばアクセス権が「閲覧」であれば、セキュリティレベルから一定点数たとえば１減ずる（Ｓ２１０５）。さらに、スケジューラやＧＰＳ、出退社記録で現在の位置を求め（Ｓ２１０６）、その位置が一定の範囲（たとえば会社内など）にあるか判定する（Ｓ２１０７）。一定範囲内になければ、それに応じて一定点数たとえば１をセキュリティレベルから減ずる（Ｓ２１０８）。一方、認証フラグを参照して、認証されていないと判定されれば、セキュリティレベルとして最低の値を与える（Ｓ２１０９）。

【００３５】

なお、装置の現在位置は、たとえばＧＰＳが装着されていれば、ＧＰＳにより測定された位置で与えられる。またスケジューラがインストールされていれば、そのスケジュールに記載された移動先等の記載から、一定の範囲内にあるか否かが判定できる。また、出退社記録とは第５実施形態のようにＲＦＩＤタグを用いた方法で記録できる。

【００３６】

＜ユーザ認証処理手順＞

図７から図１３のセキュリティモジュール１０８が表示するユーザインターフェース図を用いて、ユーザが図６に記載のセキュアドキュメントワークフロー中での操作の様子と、セキュアデータにセキュリティレベル別処理テーブル２０３を付加する様子について説明する。図７はセキュリティ管理サーバ１０４に認証を受けるためにセキュリティモジュール１０８が表示するユーザインターフェースである。これはたとえばセキュアアプリケーション１０３などを起動すると、それにより呼び出されたセキュアモジュール１０８により表示される。

【００３７】

ユーザは、認証ＵＩ７０１にユーザＩＤ７０２とパスワード７０３を入力し、認証ボタン７０４を押下する。それにより、セキュリティモジュール１０８はセキュリティ管理サーバ１０４との通信を行い認証操作を行なう。またセキュリティモジュール１０８は認証結果を過去の認証履歴情報として、ユーザＩＤ７０２、パスワード７０３、セキュリティ管理サーバ１０４から付与された当該ユーザのアクセス権の保存を実行する。セキュリティ管理サーバ１０４に接続できない場合は、過去の認証履歴情報にしたがって認証を行なう。その場合には、セキュリティレベルは低下する。認証を中止したい場合はキャンセルボタン７０５を押下すれば良い。

【００３８】

セキュリティ管理サーバ１０４により認証が済むと処理選択画面７０６が表示される。処理選択画面からはファイル取得７０７、登録７０８、承認７０９、終了７１０の処理が選択可能である。編集や閲覧のアクセス権のユーザは操作が制限される。そのため、実行出来ない処理ボタンはグレーアウトされて表示される。編集のアクセス権限のユーザであれば承認処理は実行不可能なので、承認を選択するボタンがグレーアウトされる（７１１）。閲覧のアクセス権限のユーザであれば登録処理、承認処理の２つが実行不可能であるのでグレーアウトされる（７１２）。終了ボタン７１０はセキュリティ管理サーバ１０４へ認証の終了を通知し、画面上は処理選択ＵＩ７０６を消去する。

【００３９】

図２２にコンピュータにインストールされたセキュリティモジュール１０８によるユーザ認証手順の一例を示す。ユーザインターフェースにおいてユーザによりそのユーザＩＤをパスワードとが入力されると（Ｓ２２０１）、セキュリティモジュール１０８はセキュリティ管理サーバ１０４にアクセス可能であるか判定する（Ｓ２２０２）。たとえば、セキュリティ管理サーバ１０４に対するユーザ認証要求の発行を試みて、応答がなければアクセスできないと判断し、応答があればアクセス可能と判断できる。そしてアクセス可能な場合、セキュリティ管理サーバ１０４からユーザＩＤに応じたアクセス権レベル（アクセス権情報）を受信する（Ｓ２２０３）。そして、そのアクセス権情報を当該ユーザのアクセス権として保存するとともに、ユーザＩＤ、パスワード、アクセス権情報、認証日時

を認証履歴情報５１２に付加して、その装置のローカルな記憶装置、たとえばフラッシュメモリなどのリムーバブル記憶媒体に保存する（Ｓ２２０４）。そしてたとえばユーザ認証フラグなどによりユーザ認証があったことを記録する（Ｓ２２０５）。最後に獲得したアクセス権に対応したユーザインターフェースを、図７に示すように表示する（Ｓ２２０６）。一方、セキュリティ管理サーバ１０４にアクセスできない場合には、過去のアクセス権テーブルすなわち認証履歴情報５１２を参照する（Ｓ２２０７）。そして入力されたユーザＩＤおよびパスワードにより、ユーザ認証が過去の一定期間以内たとえば１週間以内にされたか否か判定する（Ｓ２２０８）。されていれば該当するアクセス権を認証履歴情報５１２から読み取ってそれを当該ユーザのアクセス権として保存する（Ｓ２２０９）。ユーザのアクセス権を参照する場合には、ステップＳ２２０３またはステップＳ２２０９で保存されたアクセス権情報が参照される。一方、ステップＳ２２０８で該当する認証が行われていないと判定された場合には、前述したユーザ認証フラグなどに、ユーザ認証が失敗した旨を記録しておく（Ｓ２２１０）。

【００４０】

＜ファイル登録手順の例＞

図８は図７の登録処理ボタン７０８を押下されたときにセキュリティモジュール１０８が表示するファイル登録ＵＩ画面８０１である。ユーザは作成したセキュアデータをファイル名欄８０２に記載し、送信先８０３に承認のアクセス件をもったユーザを指定する。送信先に電子メールを送信する場合には、ファイル登録ＵＩ画面８０１のチェックボックス８０４にチェックを入れる。コメント８０５には特記事項等を記載する。特に無い場合は記載する必要は無い。登録ボタン８０６を押下することにより承認のアクセス権を持つユーザに承認処理が任される。このときセキュアデータはセキュリティ管理サーバ１０４に仮保存されている。登録を中止したければキャンセルボタン８０７を押下すれば良い。電子メールを送信するチェックボックス８０４にチェックした場合、電子メール例８０８が送信先８０３で指定した承認のアクセス権をもったユーザに送信される。電子メール内にはファイル名８０２、コメント８０５等が記載されている。

【００４１】

図２３はセキュリティモジュール１０８によるファイル登録手順のフローの一例を示す図である。図７の画面７１２等において登録ボタン７０８が押されると、ユーザのアクセス権がチェックされ、「承認」または「登録」以外ならば権限がないと判定されて処理は終了する（Ｓ２３０１）。なお、図７のように権限がない操作ボタンをグレイアウトしてあればステップＳ２３０１は必ずしも必要ではない。権限があれば図８のＵＩ画面を表示し、ファイル名や送信先、電子メールの送信の有無等の入力を待つ（Ｓ２３０２）。入力されたなら、保存されている入力データを参照して電子メールの送信の有無を判定し（Ｓ２３０３）、送信すると指定されていればメッセージ８０８を指定された送信先へと電子メールで送信する（Ｓ２３０４）。最後に承認待ちのデータをセキュリティ管理サーバ２３０５に渡して仮保存させる（Ｓ２３０５）。なお、登録や承認は、本実施形態ではセキュリティ管理サーバ１０４により行われるものとする。

【００４２】

＜ファイル承認手順の例＞

図９は図７の承認処理ボタン７０９を押下されたときにセキュリティモジュール１０８が表示するファイル承認ＵＩ画面９０１である。図２４はその処理手順のフロー図である。まず承認処理ボタン７０９が押されるとアクセス権が「承認」であるかチェックされる（Ｓ２４０１）。アクセス権限が承認であれば、セキュリティモジュール１０８はセキュリティ管理サーバ１０４と通信を行い、仮登録されたセキュアデータで、かつ承認のアクセス権で認証を受けたユーザが承認処理すべきセキュアデータのリスト９０２をセキュリティ管理サーバ１０４から受け取って（Ｓ２４０２）、それを表示する（Ｓ２４０３）。承認のアクセス権で認証を受けたユーザは、リスト９０２の中から承認したいセキュアデータを選択し、承認ボタン９０３を押下する。承認を中止したければキャンセルボタン９０４を押下する。承認ボタン９０３を押下するとテンプレート選択ＵＩ９０５が表示され

る。閲覧ボタン９０６を押下するとセキュアデータ１０２の内容を見ることが出来る。承認のアクセス権で認証を受けたユーザは、内容を確認しながらテンプレート欄９０７から適当なテンプレートを選択する。テンプレートを選択したら選択ボタン９０８で決定する。テンプレート選択を中止し、ファイル承認ＵＩ９０１に戻りたければキャンセルボタン９０９を押下する。テンプレートはセキュリティ管理サーバ１０４に登録されており、セキュリティモジュール１０８が通信することにより取得できる。

【００４３】

テンプレートとは、あらかじめ定義されたセキュリティレベル別処理テーブル２０３である。ユーザがセキュアデータ１０２ごとにセキュリティレベル別処理テーブル２０３を細かく設定するのは面倒であるので、セキュリティ管理サーバ上にいくつかのセキュリティレベル別処理テーブル２０３の例を保存しておき、セキュリティレベル別処理テーブル２０３を選択することにより細かい設定をすることなくセキュリティレベル別処理テーブル２０３をセキュアデータごとに追加することが出来る。

【００４４】

図１０にテンプレートの例を示す。テンプレート選択ＵＩ９０５でユーザが何れかのテンプレートを選択し、選択ボタン９０８を押す。このように必要な入力が行われて（Ｓ２４０４）。選択ボタンが押されると（Ｓ２４０５－ＹＥＳ）、選択されているテンプレートが読み込まれてセキュリティレベル処理確認ＵＩ１００１が表示される（Ｓ２４０６）。このステップでは、テンプレートに登録されているアクセス権ごと、セキュリティレベルごとの処理制限１００２、１００３、１００４が表示される。本実施形態ではセキュリティレベルごとの処理制限はアクセス権ごとに設定でき、承認のアクセス権で認証を受けた場合の処理制限１００２、編集のアクセス権で承認を受けた場合の処理制限１００３、閲覧のアクセス権で承認を受けた場合の処理制限１００４が記載されている。

【００４５】

表示された処理制限で良い場合は確定ボタン１００６をユーザは押下する。この操作により承認処理が全て終了し、セキュリティレベル処理確認ＵＩ１００１に表示されている処理制限がセキュリティレベル別処理テーブル２０３としてセキュアデータ１０２に追加され、セキュアデータ１０２はセキュリティ管理サーバ１０４により保存される（Ｓ２４０８－Ｓ２４１０）。キャンセルボタン１００１を押下することによりセキュリティレベル別処理テーブルテンプレート選択ＵＩ９０６に戻ることが出来る。

【００４６】

選択したテンプレートで定義されている処理制限の一部を変更したい場合は、ユーザは変更ボタン１００５を押下する。それにより、図１１の処理制限変更ＵＩ１１０１が表示される。それぞれの処理制限の横にあるボタン１１０２を押下することにより候補１１０３が表示されるので、候補１１０３の中より選択を行なう。変更した内容を反映したい場合は変更ボタン１１０３、反映しない場合はキャンセルボタン１１０４を押下することによりセキュリティレベル処理確認ＵＩ１００１に戻る。

【００４７】

さらに、セキュリティ管理サーバ１０４はセキュリティレベル別処理テーブルのテンプレートを登録するための登録機能を持つ。認証ＵＩ７０１において「管理」のアクセス権限で認証を受けると管理処理選択ＵＩ１２０１が表示される。テンプレート登録ボタン１２０２を押下することによりテンプレート登録ＵＩ１２０３が表示される。１２０４でテンプレートを選択し、１２０５で任意に処理制限を変更する。登録ボタン１２０６を押下することによりセキュリティ管理サーバ１０４にテンプレート登録ＵＩ１２０３に表示されている内容がテンプレートとして登録される。登録を止めたい場合はキャンセルボタン１２０７を押下すれば良い。

【００４８】

＜ファイル取得処理＞

図１３は、図７のファイル取得処理ボタン７０７を押下されたときにセキュリティモジュール１０８が表示するファイル取得ＵＩ１３０１である。図２５はセキュリティモジュ

ール１０８によるファイル取得処理手順のフローチャートである。ファイル取得処理ボタン７０７を押下されると、まずアクセス権があるかすなわちユーザ認証がされたかが、たとえばユーザ認証フラグ等を参照して行われる（Ｓ２５０１）。ファイル取得はいずれのアクセス権限でも許されているためである。認証されていればＵＩ画面１３０３にアクセス権が表示される（Ｓ２５０２）。この画面でファイル選択欄１３０３で取得したいセキュアデータ１０２をユーザが選択すると、セキュリティレベルに応じでどのような処理制限がなされるかを、アクセス権１３０２とセキュアデータ内のセキュリティレベル別処理テーブル２０３から判断し表示する。セキュアデータはファイル名で表示されているが、特定は対応するデータＩＤでされる。ユーザが処理制限の確認を行い、選択したファイルで良ければ選択ボタン１３０６を押下する。止めたければキャンセルボタン１３０６を押下する。選択ボタン１３０６を押下すると保存先指定ＵＩ１３０１が表示される。保存先記入欄１３０８に各装置内の保存先がユーザにより記入されて決定ボタン１３０９が押下されると（Ｓ２５０４）、セキュリティ管理サーバ１０４からホスト装置１０１、セキュア入力装置１０６、セキュア出力装置１０６へセキュアデータ１０２がコピーされる（Ｓ２５０５，Ｓ２５０６）。各装置にコピーされたセキュアデータ１０２はセキュアアプリケーション１０３によって閲覧や編集が可能となる。

【００４９】

図１４を用いて印刷処理を例にセキュリティレベルに応じて処理が制限される流れを説明する。ユーザ１４０１は、閲覧中のセキュアデータ１０２の印刷をセキュアアプリケーション１０３に対して指示する。セキュアアプリケーション１０３はセキュリティモジュール１０８により決定されるセキュリティレベル１０９を要求する。セキュリティモジュール１４０３はセキュリティレベルを読んでセキュアアプリケーション１４０２に現在のセキュリティレベルを返す。セキュアアプリケーション１０３はセキュアデータ１０２のセキュリティレベル別処理テーブル２０３を参照し、現在のセキュリティレベルと、現在のユーザのアクセス権とで定められるテーブルエントリを読む。読み出した各エントリには、各処理についての制約を定めた処理制限情報が含まれている。その情報が、現在の処理制限情報として、セキュアアプリケーション１０３が実行されている装置のメモリ等に保存される。

【００５０】

たとえば図１０のセキュリティレベル別処理テーブルを参照すると、権限毎のサブテーブル１００２，１００３，１００４が含まれている。したがってまずアクセス権限でひとつのサブテーブルが特定できる。そして、セキュリティレベルにより、制限情報が特定される。たとえばアクセス権が「編集」であり、セキュリティレベルが「５」であれば、「閲覧」処理については「通常閲覧」という処理制限情報が、「編集」処理については「出来ます」という処理制限情報が、「印刷」処理については「通常印刷」という処理制限情報が登録されている。これらがセキュリティレベル別処理テーブルから読み取られる。

【００５１】

現在の処理制限を特定して保存したら、セキュアデータ１０２より実データ２０２を取得して処理制限にしたがった処理を実行してから印刷装置１４０８に処理後のセキュアデータを転送する。セキュアアプリケーション１０３は処理結果をユーザに通知して処理を終了する。

【００５２】

例えばセキュリティレベルが３であって、印刷処理に関するセキュリティレベル別処理テーブル１４０９が与えられている場合、セキュアアプリケーション１０３は実データの個人・詳細情報が記載された部分にマスク処理を行ってから印刷装置１４０８に送信する。

【００５３】

図２６にセキュアアプリケーション１０３によるセキュアデータの編集処理手順の一例を示す。まず前述の要領でユーザ認証及びセキュアデータファイルの取得が行われる（Ｓ２６０１）。既にセキュアアプリケーションが実行される装置にセキュアデータの複製が

保存されている場合には、セキュリティ管理サーバ１０４から取得する必要はなく、既に取得されているファイルが用いられる。そして、セキュリティレベルをセキュリティモジュールから取得して、そのセキュリティレベル及びアクセス権限に応じたセキュリティレベル別処理テーブルのエントリを特定し、セキュアデータから読み取って保存する（Ｓ２６０２）。そして保存したエントリのうち、閲覧処理に対する処理制限情報を参照して（Ｓ２６０３）、制限が「出来ません」であれば閲覧できない旨出力する（Ｓ２６０７）。制限が「通常閲覧」であれば、セキュアデータを解読して平文で表示する（Ｓ２６０４）。また、制限が「個人詳細情報マスク」であれば、平文化したセキュアデータのうち該当する部分をマスク（たとえばマスクされていることを示すパターンで塗りつぶすなど）して、表示する（Ｓ２６０８）。次に、保存したエントリのうち、編集処理に対する処理制限情報を参照して（Ｓ２６０５）、制限が「出来ません」であれば、処理対象のデータを読み出しモードとする。モードは、たとえば開いているファイルの属性を変更することで変更される。もちろんこのモードの変更はユーザには許さない。制限が「出来ます」であれば、そのまま編集操作に移る。

【００５４】

図２７に閲覧中のあるいは編集中のドキュメント（セキュアデータ）を印刷する手順の例を示す。ユーザがセキュアアプリケーションの操作画面等において「印刷」指示を入力すると、まず図２６のステップＳ２６０２で保存したセキュリティレベル別処理制限テーブルのエントリのうち、印刷処理に対する処理制限情報を参照する（Ｓ２７０１）。制限が「出来ません」であれば閲覧できない旨出力する（Ｓ２７０３）。制限が「通常印刷」であれば、ドキュメントを印刷装置に渡して印刷させる（Ｓ２６０４）。また、制限が「個人詳細情報マスク」であれば、平文化したセキュアデータのうち該当する部分をマスク（たとえばマスクされていることを示すパターンで塗りつぶすなど）して（Ｓ２７０４）、それを印刷装置に渡し印刷させる。

【００５５】

図２７の処理は、たとえばセキュリティ管理サーバ１０４から直接セキュアデータを印刷する場合にも適用される。

【００５６】

以上第１実施形態に記載した内容によってセキュアデータごとにセキュリティレベルに応じた処理制限を指定可能になり、セキュリティモジュールが保持するセキュリティレベルとセキュアデータごとに指定されたセキュリティレベルに応じて様々な状況、特にファイルを持ち出した状況において適切なセキュリティを保ちながらセキュアデータを用いた処理を実現することが出来る。

【００５７】

これにより、セキュアデータに対する処理制限を決定するための一要因であるセキュリティレベルを、セキュアデータの存在する環境にしたがって自動的に変えることができる。このため、状況に応じた適切な処理制限を設定することが可能となり、利便性とセキュリティとの兼ね合いのバランスを動的に変更できる。

【００５８】

［第２実施形態］

本実施形態では、セキュリティモジュールにセキュリティレベル別処理テーブルを保持させる。これによりセキュアデータ１０２ごとにセキュリティレベルに応じた処理を設定する必要がなく、全てのセキュアデータに同じセキュリティレベルに応じた処理を行うことができる。図１５を用いてセキュリティレベル別処理テーブル１５０５をセキュリティモジュール１５０３に持たせた場合の処理の流れを説明する。ユーザ１５０１は閲覧中のセキュアデータ１５０７をセキュアアプリケーション１５０２に印刷要求を行なう。セキュアアプリケーション１５０２はセキュリティモジュール１５０３の処理制限の確認を行なう。セキュリティモジュール１５０３をセキュリティレベル１０９を確認後、セキュリティモジュール１５０３が保持すうセキュリティレベル別処理テーブル１５０５を参照し処理制限を確認し、セキュアアプリケーション１５０２に処理制限を返す。セキュアアプ

リケーション１５０２はセキュアデータ１５０７より実データ１５０８を所得し処理制限にしたがった処理を実行してから印刷装置１５０８にセキュアデータ１５０７を転送する。セキュアアプリケーション１５０２は処理結果をユーザに通知して処理を終了する。

【００５９】

セキュリティモジュール１５０３に保持するセキュリティ処理テーブルは、図１２の管理処理選択ＵＩ１２０８より管理のアクセス権を持つユーザがセキュリティ管理サーバ１０４に登録する。任意のインストールプログラムによってセキュリティモジュール１５０３を各装置にインストールするときにセキュリティ管理サーバ１０４より取得されセキュリティモジュール１５０３と同時に各装置にインストールされる。

【００６０】

このようにして、セキュアデータから独立したセキュリティレベル別処理テーブルをセキュリティモジュールが管理することで、セキュリティレベル別処理テーブルをセキュアデータから取得する必要がなくなり、より処理が簡素になる。また、セキュアデータとして管理すべきデータ量を減少させることができる。

【００６１】

［第３実施形態］

本実施形態では、セキュア出力装置（たとえばプリンタ）１０５にセキュリテモジュール１０３を導入しておくことにより、ユーザが間違ったセキュア出力装置１０５にセキュアデータを送信し印刷処理してしまったときでもセキュリティを保つ方法について説明する。図１６に示すように、セキュア出力装置１６０２、１６０３、１６０４にはそれぞれセキュリティモジュール１０３をインストールしておく。セキュリティレベルは第１実施形態のように設置状態に応じてセキュリティモジュールが決定しても良いが、本実施形態では、システム管理者等があらかじめ固定的な値を与えておく。したがって、セキュア出力装置１６０２－１６０４では、図２１の処理は行われない。セキュア出力装置のセキュリティレベルは公共性が高い場所に設置されたものほど低い状態にしておく。また、ホスト装置からの印刷要求にも、印刷要求を出したユーザのアクセス権限が付される。これによりユーザがホスト装置１６０１で各セキュア装置１６０２、１６０３、１６０４に印刷処理したときに、例えホスト装置１６０１のセキュリティレベルが高い状態であっても各セキュア出力装置１６０２、１６０３、１６０４によって処理制限を受ける。すなわち、セキュア出力装置のセキュリティモジュールは、セキュアデータを伴う印刷要求を受信すると、それとともに受信したユーザのアクセス権限と、そのセキュア出力装置に与えられたセキュリティレベルとから、処理制限情報を特定する。この場合、処理は「印刷」であるので、アクセス権限と、セキュリティレベルと、処理の内容（印刷）とから、セキュアデータに付随するセキュリティレベル別処理テーブルを参照して、ただひとつのエントリ（処理制限情報）が特定される。その処理制限情報に従って、セキュア出力装置は、要求されている出力に制限を加える。制限を加える処理は、図２７に付した手順と同様である。

【００６２】

例えばセキュアデータ１０２が１６０４に示す印刷処理制限である場合、ホスト装置はセキュリティレベルが高い状態なので通常印刷（加工なし）のセキュアデータ１０２を各セキュア出力装置１６０２、１６０３、１６０４に送信できる。このセキュアデータは、セキュリティレベルの高いセキュア出力装置１６０２では通常印刷され、セキュリティレベルが低いセキュア出力装置１６０４では、処理制限が「出来ません」であるために印刷されない。この結果、公共性が高い場所に設置されているセキュア出力装置にはセキュリティ的に重要なセキュアデータ１０２は印刷されないことになりセキュリティを保つことが出来る。

【００６３】

また、印刷処理のみにセキュリティレベルによる処理制限を行いたい場合にはセキュリティレベルをセキュア出力装置に保持するのも良い。特に処理をせずにセキュア出力装置１６０２、１６０３、１６０４にセキュアデータ１０２を送信しても適当なセキュア出力

装置で適切な処理が行われて印刷される。この場合、セキュリティレベルに係る処理をホスト装置では行わないか、あるいは常にセキュリティレベルが「５」であるとして処理を行う。セキュア出力装置にはセキュリティレベルのみを設定しておき、ホスト装置で印刷先のセキュア出力装置からセキュリティレベルを取得し、ホスト装置で適切な処理を行ってからセキュア出力装置にセキュアデータを送信するような構成でも良い。

【００６４】

この様に構成することで、ユーザがプリンタのセキュリティを意識していなくても、印刷に用いるプリンタのセキュリティレベルに応じて印刷処理が制限される。

【００６５】

［第４実施形態］

図１７、図１８を用いてセキュリティ管理サーバからダイレクトにセキュア出力装置に印刷処理する際に、本発明に係るセキュリティレベルに応じた処理制限を適応する方法について説明する。セキュリティ管理サーバ１７０１とセキュア出力装置１７０２はネットワーク等で接続されている。ユーザはセキュア出力装置上のユーザインターフェースを利用して、セキュリティ管理サーバ１７０１で管理されたセキュアデータをセキュア出力装置１７０２に印刷処理することが出来る。

【００６６】

セキュア出力装置１７０２にインストールされたセキュリティモジュールが表示する認証ＵＩ１７０３によってユーザ認証処理が行われる。認証処理が終了すると処理選択ＵＩ１７０４が表示される。セキュアデータをセキュリティ管理サーバ１７０１からセキュア出力装置１７０２へダイレクトに送信して印刷処理を行いたい場合は、ダイレクト印刷ボタン１７０３をユーザは押下する。処理を止め認証を終了したい場合は終了ボタン１７０４を押下する。ダイレクト印刷ボタン１７０３が押下されるとダイレクト印刷ＵＩ１１７０７が表示される。ダイレクト印刷ＵＩ１７０７にはユーザのアクセス権１７０８、セキュアデータのファイル名を選択欄１７０９、現在のセキュア印刷装置のセキュリティレベル１７１０が表示される。印刷処理したいセキュアデータのファイル名を選択すると、セキュア出力装置内のセキュリティモジュールは、現在のセキュア出力装置のセキュリティレベルと、セキュリティ管理サーバ１７０１から選択されたセキュアデータのセキュリティレベルごとの処理制限が記述されたセキュリティレベル管理テーブルを取得し、コメント１７１１に、処理制限の概要を表示する。

【００６７】

ユーザはコメント１７１１に表示された内容で良ければ印刷実行ボタン１７１３を押下する。セキュア出力装置内のセキュリティモジュールはセキュリティ管理サーバからセキュアデータのファイル名欄１７０９で指定されたファイルを取得し、セキュア出力装置セキュリティレベルとセキュアデータのセキュリティレベル別処理テーブルに従って所定の処理制限を行い印刷処理を実行する。印刷を中止したい場合はキャンセルボタンを押下することにより処理選択ＵＩ１７０４に戻る。

【００６８】

コメント１７１１に表示された処理制限がユーザの要求をみたしてなかった場合は印刷装置検索ボタン１７１２を押下することによりユーザの要求を満たした印刷処理が可能になる印刷装置を検索することが出来る。図１８にその様子を示す。この場合ユーザはセキュア印刷装置１８０２のＵＩ画面を用いて操作を行なうが、セキュアデータはセキュリティ管理サーバ１８０１からユーザが任意に指定し、ユーザが操作していないセキュア出力装置１８０３に転送され印刷処理される。

【００６９】

印刷装置検索ボタン１７１２を押下すると出力先指定ＵＩ１８０４がセキュア出力装置１８０２上のＵＩ画面に表示される。処理指定欄１８０５にユーザが要求する処理を記載する。出力装置１８０２内のセキュリティモジュールはセキュリティデータのセキュリティレベル別処理テーブルを参照することにより、必要とされるセキュリティレベルが判明する。そこで現在そのセキュリティレベルを持ったセキュア出力装置を検索し、検索され

たセキュア出力装置を表示する（１８０５）。ユーザは表示されたセキュア出力装置から任意の装置を選択し、印刷実行ボタン１８０７を押下する。こうすることによりセキュアデータはセキュリティ管理サーバ１８０１からユーザにより任意に指定されて、ユーザが操作していないセキュア出力装置１８０３に転送され印刷処理される。なお、セキュリティモジュールは、互いに通信が行なえ、通信したセキュリティモジュールのセキュリティレベルの情報交換が実行出来る。

【００７０】

このように構成することで、セキュリティ管理サーバでは、印刷しようとするセキュアプリンタのセキュリティレベルに応じた処理制限をあらかじめ知ることが出来る。このため、処理制限に応じて出力先のプリンタを選択することができ、試し印刷を必要としない。

【００７１】

［第５実施形態］

図１９、図２０を用いてＲＦＩＤを利用した現在位置特定方法とＲＦＩＤに一時的な認証を付加しておくとこによるセキュリティレベルの変化について説明する。図１９はＲＦＩＤを利用した現在位置特定方法である。ＲＦＩＤおよびＲＦＩＤ読み取り装置が付属している携帯ホスト装置１９０５にはＲＦＩＤタグが内蔵されている。形態ホスト装置１９０５が、ＲＦＩＤ書き込み装置を有するセキュリティ管理サーバや、ＲＦＩＤ書き込み装置が備えられた会議室や居住スペースの出入り口、ビルや会社の出入り口等にあったり、あるいは通過すると、その事実、もしくは場所を示す情報がそれぞれのＲＦＩＤ書き込み装置１９０１、１９０２、１９０３によって携帯ホスト装置１９０５のＲＦＩＤに記録される。携帯ホスト装置１９０５内にインストールされたセキュリティモジュールは携帯ホスト装置１９０５に付属したＲＦＩＤ読み取り装置１９０４によって上記書き込み情報を取得し、携帯ホスト装置１９０５の現在位置を認識しセキュリティレベルを上下する。すなわち、図２１のステップＳ２１０６で特定される現在位置は、このＲＦＩＤに書き込まれた情報に基づいて特定される。

【００７２】

図２０はＲＦＩＤにセキュリティ管理サーバから所定の認証を受けておくことによりセキュリティレベルの低下を避ける手段の一例を示している。セキュリティモジュールにより表示される処理選択ＵＩには、本実施形態では「ＲＦＩＤ認証」という処理の選択肢が含まれている。これを選択したユーザが、ＲＦＩＤ認証ＵＩ２００２を介してセキュリティレベルを下げる要素の免除を受ける。これによってセキュリティモジュールは免除をうけた事項に関する減点を行なわない。たとえば、社外持ち出し２００３、セキュリティ管理サーバとの通信２００４、ウィルスチェックソフトの導入２００５、アクセス権２００６等が設定できる。免除事項を選択し、認証ボタン２００７を押下すると、携帯ホスト装置２００８のＲＦＩＤに免除情報を示す情報が、セキュリティ管理サーバに付属したＲＦＩＤ書き込み装置２００１によって付加される。認証を中止したい場合キャンセルボタン２００８を押下する。上記認証情報はＲＦＩＤではなく、ＵＳＢメモリ等の外部記憶装置であっても良い。

【００７３】

図２９は本実施形態におけるセキュリティモジュールによるセキュリティレベルの決定手順の例である。本実施形態では、第１実施形態の図２１に代えて図２９が用いられる。なお図２９において図２１と共通のステップには同一の参照番号を付与した。図２９の手順は、セキュリティレベルを変更させるようなイベントを割り込み等で入力しておき、その割り込みによって実行されても良いし、定期的に実行されても良い。要は、最新の状態に合わせてセキュリティレベルが維持されていることが必要である。

【００７４】

セキュリティレベルは、セキュリティモジュールが実行される装置の持つ記憶部の所定位置に記憶される。まずその記憶位置に、セキュリティレベルとして「５」を記憶する（Ｓ２１０１）。次に、現在セキュリティ管理サーバ１０４にアクセス可能であるか判定す

る（Ｓ２１０２）。可能でなければ、アクセス不可能（サーバ不通）な場合の減点の免除について、当該装置がＲＦＩＤ認証を受けているか判定する（Ｓ２９０１）。認証されていなければ、セキュリティレベルから一定の値（例えば３）を減ずる（Ｓ２１０３）。

【００７５】

次に、ユーザ認証フラグを参照して、ユーザ認証が成功したか判定する（Ｓ２１０４）。ユーザ認証フラグは、後述する図２２等の手順でセキュリティ管理サーバ１０４によるユーザ認証が成功した場合にその旨セットされるフラグである。認証が成功した場合には、アクセス権の種類に応じた減点の免除について、当該装置がＲＦＩＤ認証を受けているか判定する（Ｓ２９０２）。認証されていなければ、認証の種類、すなわち得られたアクセス権に応じてセキュリティレベルを下げる。たとえばアクセス権が「閲覧」であれば、セキュリティレベルから一定点数たとえば１減ずる（Ｓ２１０５）。

【００７６】

さらに、ＲＦＩＤに記録された位置情報で現在の位置を求め（Ｓ２１０６）、その位置が一定の範囲（たとえば会社内など）にあるか判定する（Ｓ２１０７）。一定範囲内になければ、一定範囲内（会社内など）に装置が存在しない場合の減点の免除について、当該装置がＲＦＩＤ認証を受けているか判定する（Ｓ２９０３）。認証されていなければ、アクセス権限に応じて一定点数たとえば１をセキュリティレベルから減ずる（Ｓ２１０８）。一方、認証フラグを参照して、認証されていないと判定されれば、セキュリティレベルとして最低の値を与える（Ｓ２１０９）。

【００７７】

次に、当該装置にウイルスチェックソフトがインストールされているか判定する（Ｓ２９０４）。インストールされていなければ、ウイルスチェックソフトがインストールされていない場合の減点の免除について、当該装置がＲＦＩＤ認証を受けているか判定する（Ｓ２９０５）。認証されていなければ、一定の値をセキュリティレベルから減算する（Ｓ２９０６）。

【００７８】

このようにすることで、セキュリティレベルを引き下げる必要がないと認められる状況については、セキュリティレベルの減点要因から除外することができる。この結果、より適切なセキュリティレベルを装置に対して設定することができ、不要な処理宣言を解除することができる。

【００７９】

［変形例］

第５実施形態では、減点要因毎に減点の免除について認証を受けているが、一括して認証を受けることも出来る。この場合には、図２１の要領でセキュリティレベルを決定した後、ＲＦＩＤ認証を受けていれば一定の点数（たとえば３）をセキュリティレベルに加算する。

【図面の簡単な説明】

【００８０】

【図１】本発明が適用されるセキュアドキュメントシステムの構成例を示す模式図である。

【図２】本発明が適用されるセキュアドキュメントシステムのセキュアデータ内部構造の一例を示す図である。

【図３】本発明が適用されるセキュアドキュメントシステムのセキュリティ管理サーバに格納されたセキュア管理データの一例を示す図である。

【図４Ａ】本発明が適用されるセキュアドキュメントシステムのセキュリテイー管理サーバとセキュリティモジュールとの間のオンライン認証の仕組みを示した図である。

【図４Ｂ】本発明が適用されるセキュアドキュメントシステムのセキュリテイー管理サーバとセキュリティモジュールとの間のオフライン認証の仕組みを示した図である。

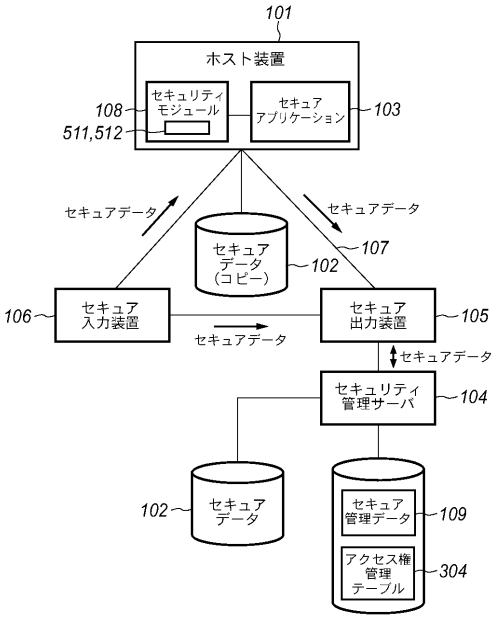
【図５】装置のセキュリティレベルの判定の様子を示した図である

【図６】本実施形態に好適なドキュメントワークフローの一例を示す図である。

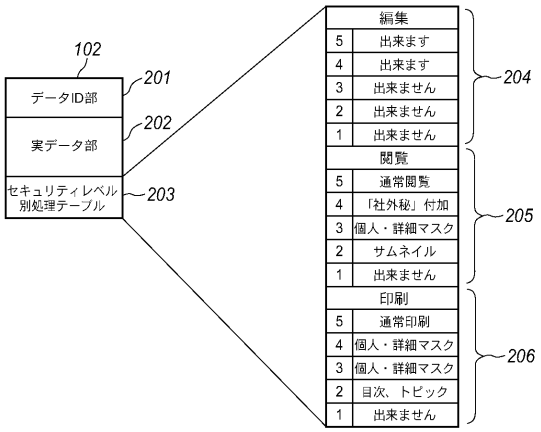
【図７】認証UIと操作選択UIの一例を示す図である。
【図８】ファイル登録UIと承認者への電子メールの一例を示す図である。
【図９】ファイル承認UIおよびセキュリティレベル別処理テーブルテンプレート選択UIの一例を示す図である。
【図１０】テンプレートのセキュリティレベル処理確認UIの一例を示す図である。
【図１１】処理変更UIの一例を示す図である。
【図１２】テンプレート登録UIの一例を示す図である。
【図１３】ファイル取得UIの一例を示す図である。
【図１４】セキュアデータに付属のセキュリティレベル別処理テーブルに基づいた印刷処理における処理制限の様子の一例を示す図である。
【図１５】セキュリティモジュールに付属のセキュリティレベル別処理テーブルに基づいた印刷処理における処理制限の様子の一例を示す図である（変形例）。
【図１６】セキュア出力装置にセキュリティレベルを用いた例を示す図である。
【図１７】ダイレクト印刷の様子の一例を示す図である。
【図１８】操作しているセキュア出力装置以外への出力の一例を示す図である。
【図１９】RFIDによる位置情報認識の一例を示す図である。
【図２０】RFIDによる認証の一例を示す図である。
【図２１】セキュリティモジュールによるセキュリティレベル再設定手順の一例を示す図である。
【図２２】セキュリティモジュールによるユーザ認証手順の一例を示す図である。
【図２３】セキュリティモジュールによるファイル登録手順の一例を示す図である。
【図２４】セキュリティモジュールによるファイル承認手順の一例を示す図である。
【図２５】セキュリティモジュールによるファイル取得手順の一例を示す図である。
【図２６】セキュアアプリケーションによるセキュアデータのオープン処理手順の一例を示す図である。
【図２７】セキュアアプリケーションによるセキュアデータの印刷処理手順の一例を示す図である。
【図２８】セキュリティモジュールが保存・管理するユーザ認証履歴テーブルの一例を示
【図２９】第５実施形態に係るセキュリティレベル決定手順を示すフローチャートである。

【符号の説明】
【００８１】
１００　ホスト装置（PC）
１０２　セキュアデータ
１０３　セキュアアプリケーション
１０４　セキュリティ管理サーバ
１０５　セキュア出力装置
１０６　セキュア入力装置
１０７　ネットワーク
１０８　セキュリティモジュール

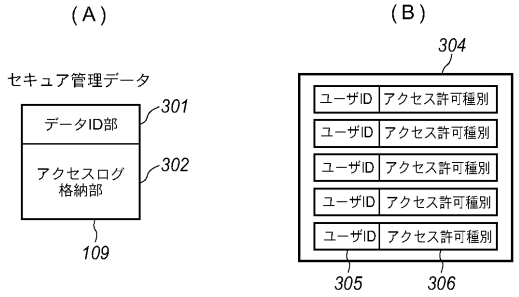
【図１】



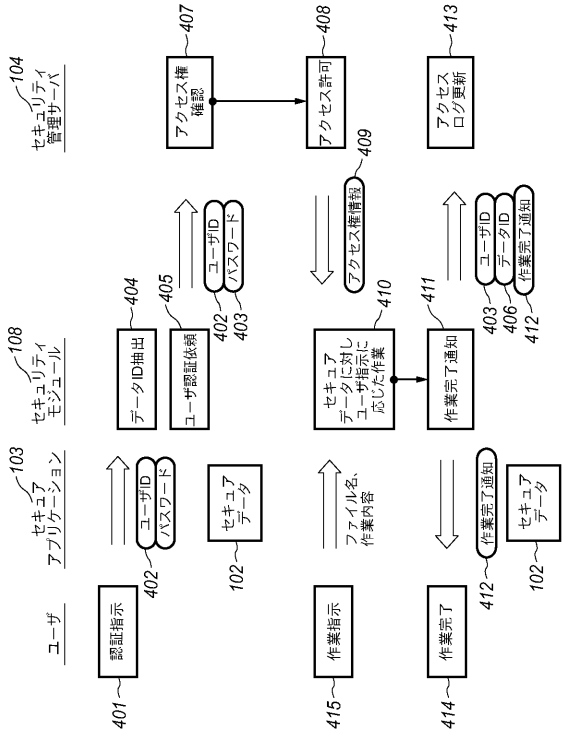
【図２】



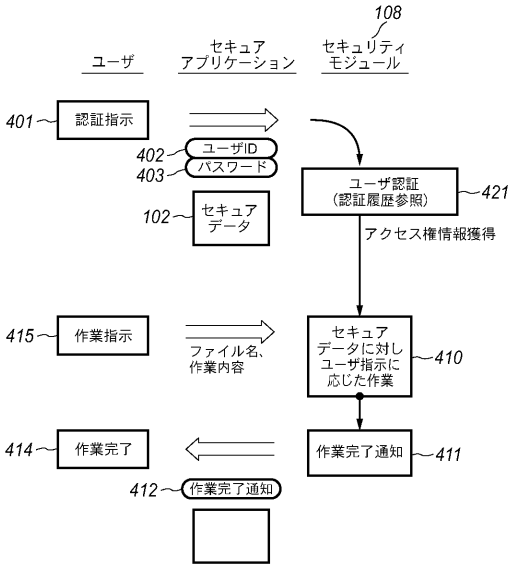
【図３】



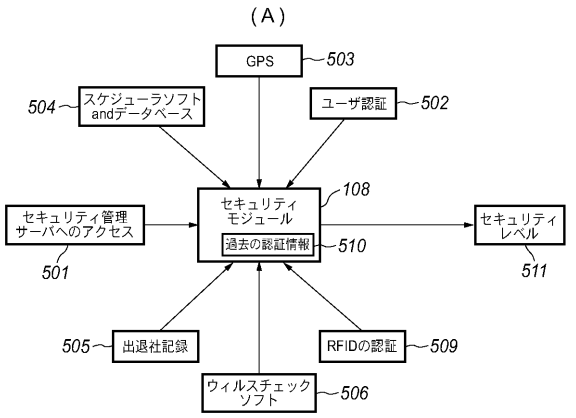
【図４Ａ】



【図４Ｂ】



【図５】



セキュリティレベルの決定

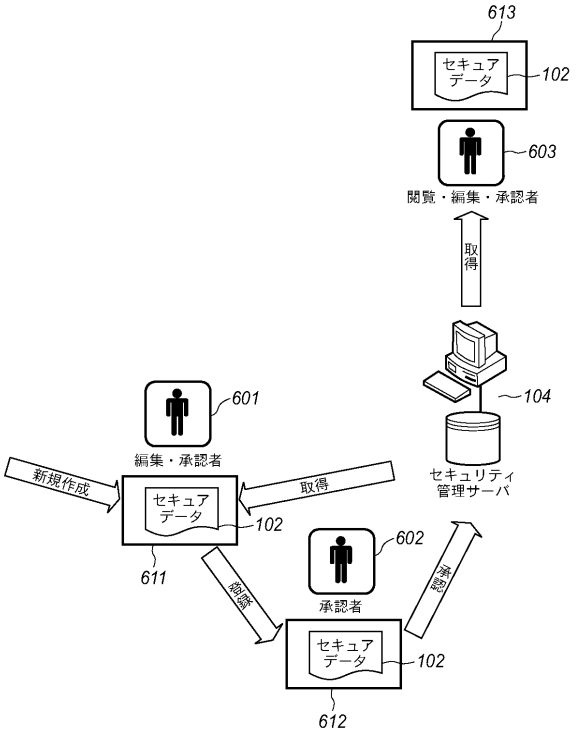
(B)

要素	減点、加点内容		
ユーザ認証	「承認のアクセス権 承認者用のセキュリティ 処理テーブルを使用」	「編集のアクセス権 承認者用のセキュリティ 処理テーブルを使用」	「閲覧のアクセス権 承認者用のセキュリティ 処理テーブルを使用」
セキュリティ管理 サーバへのアクセス	「出来る」場合は減点なし	「出来ない」場合 は減点3(−3)	
GPS	「社内」でかつ 「公共のスペースでない」 は減点なし	「社内」でかつ 「公共のスペース」 は減点2(−2)	「社外」は減点3(−3)
スケジューラソフト andデータベース			
出退社記録			
ウィルスチェック ソフトの導入	「導入されている」場合 は減点なし	「導入されている」場合 は減点1(−1)	
RFIDの認証	「RFID認証」の場合 は加点+3		

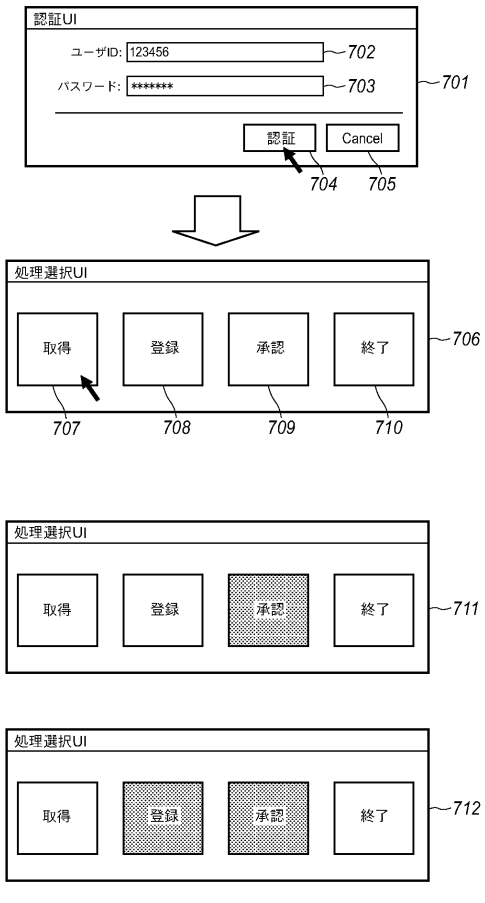
513

512

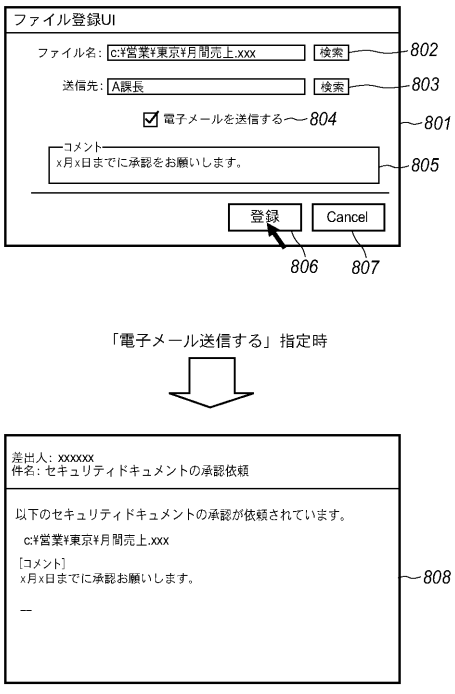
【図６】



【図７】



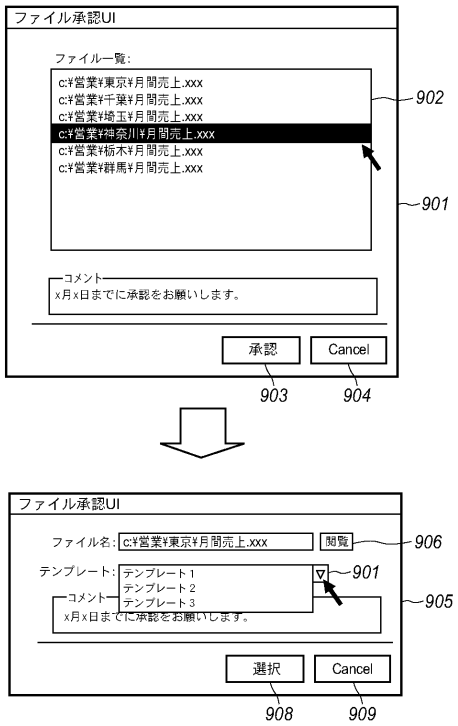
【図８】



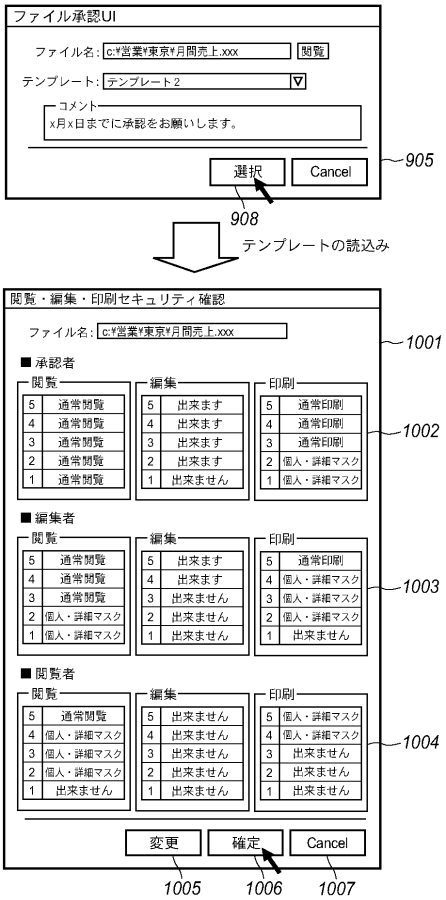
「電子メール送信する」指定時

電子メール例

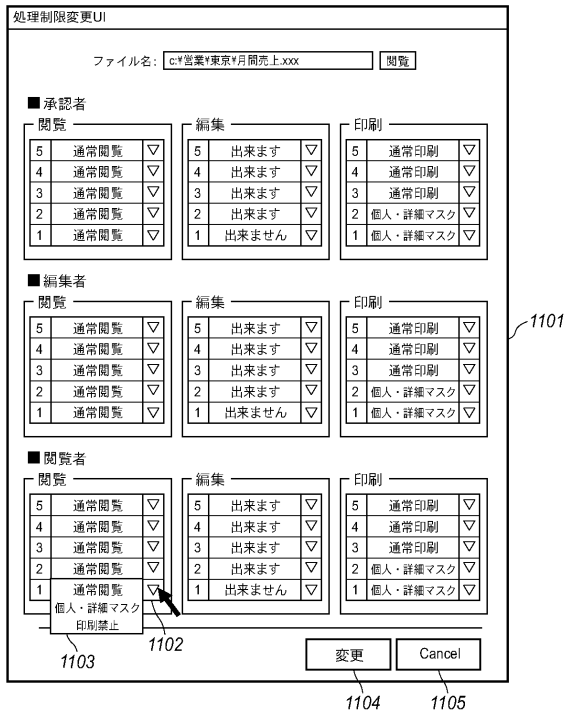
【図９】



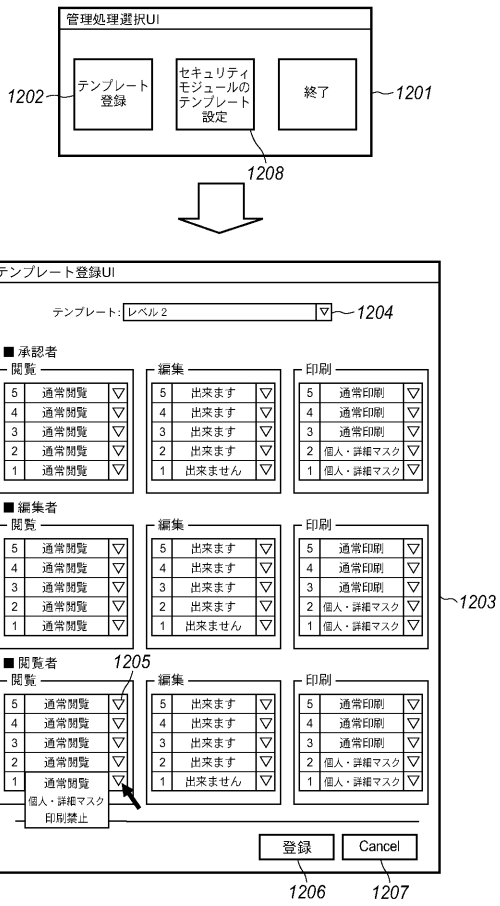
【図１０】



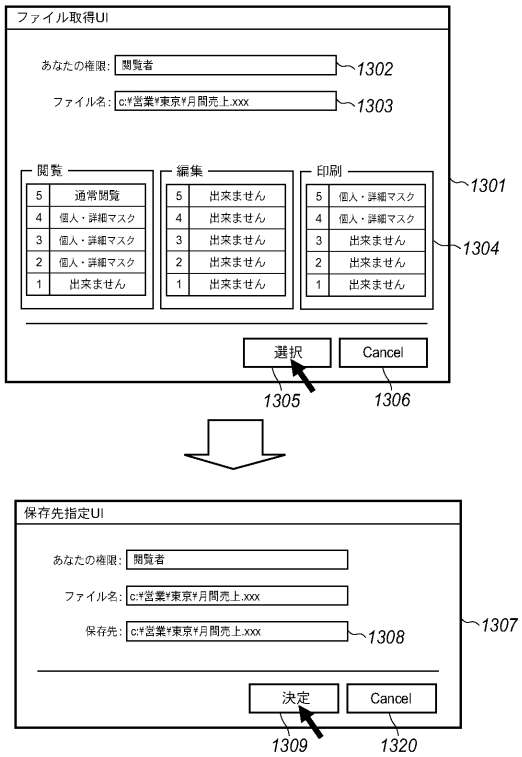
【図１１】



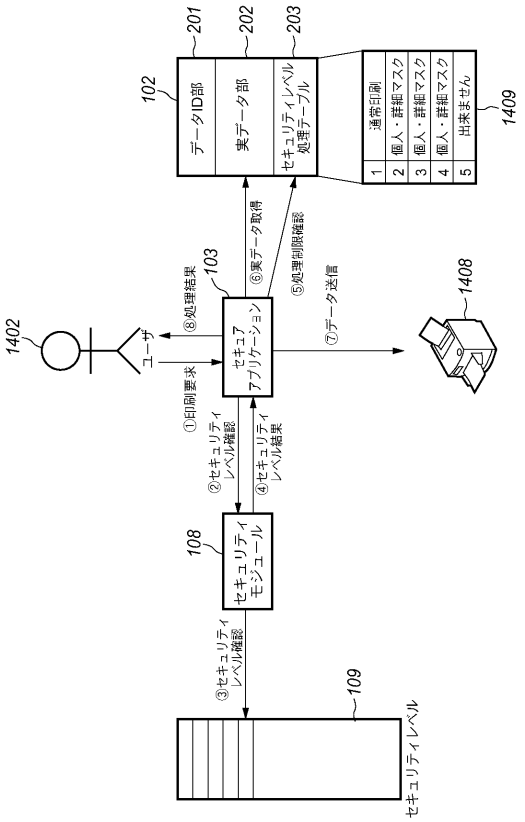
【図１２】



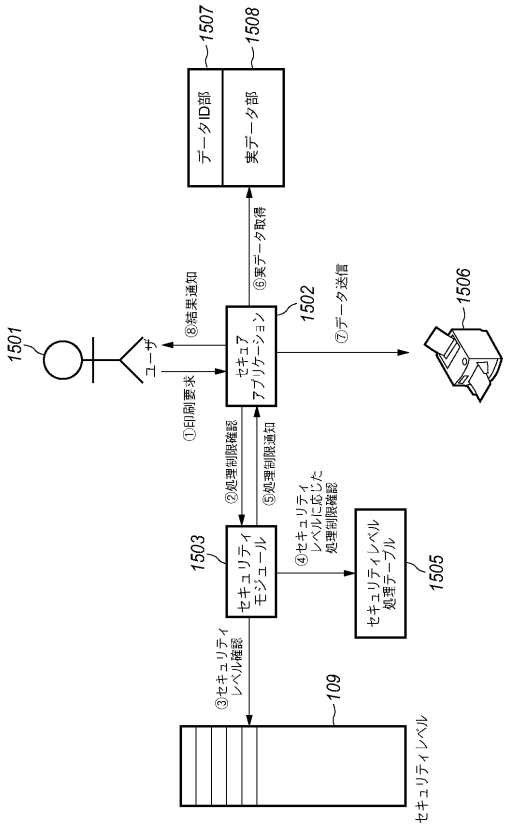
【図１３】



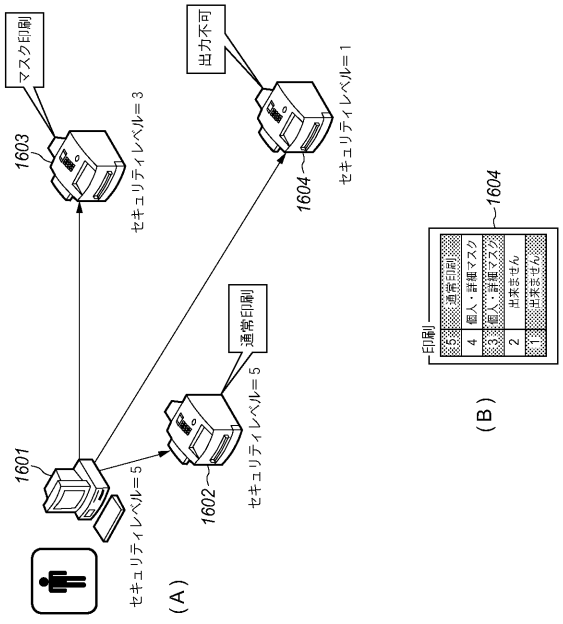
【図１４】



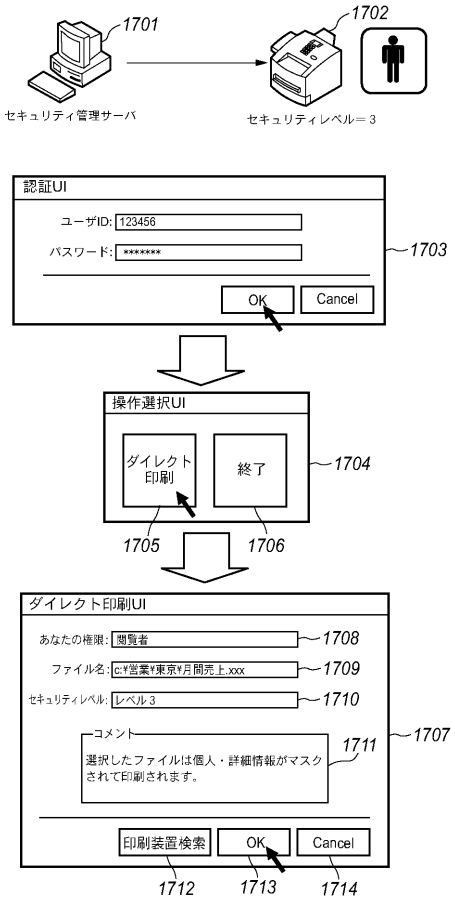
【図１５】



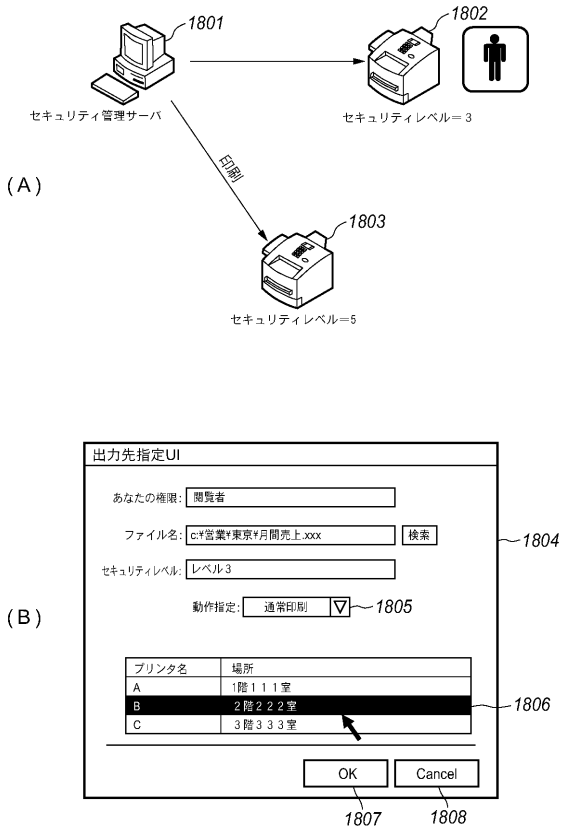
【図１６】



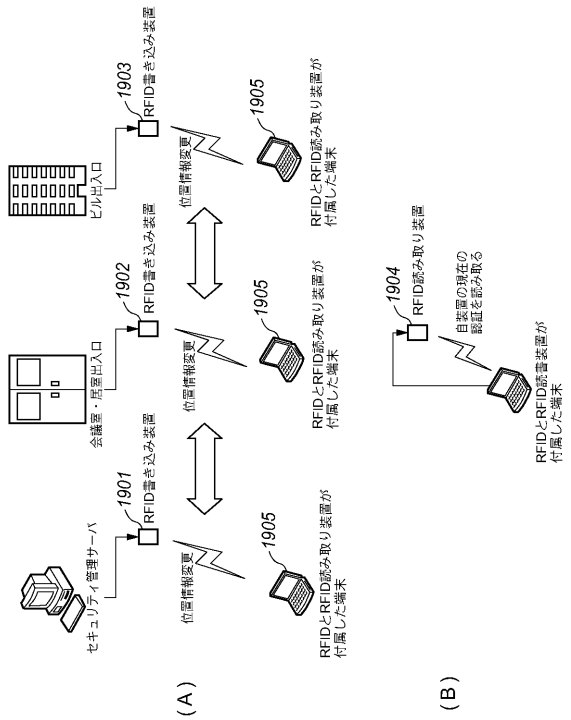
【図１７】



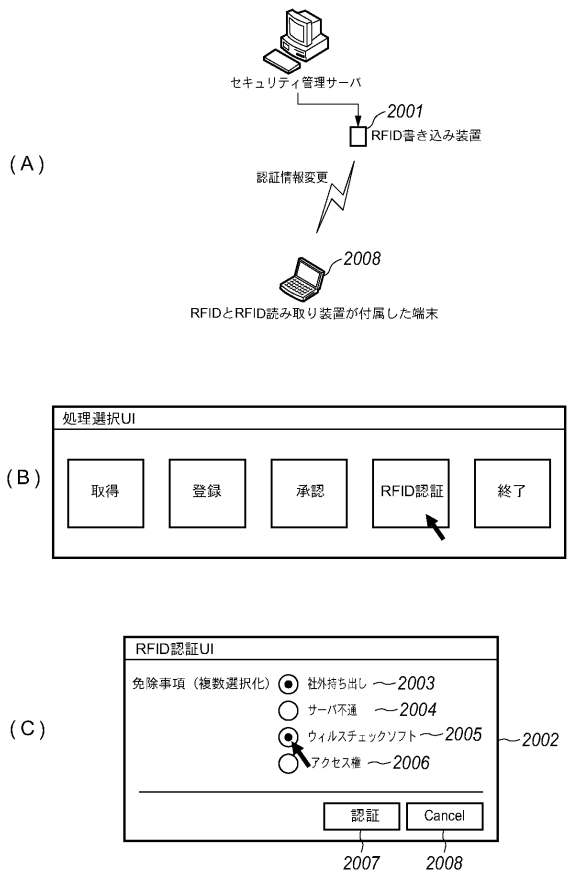
【図１８】



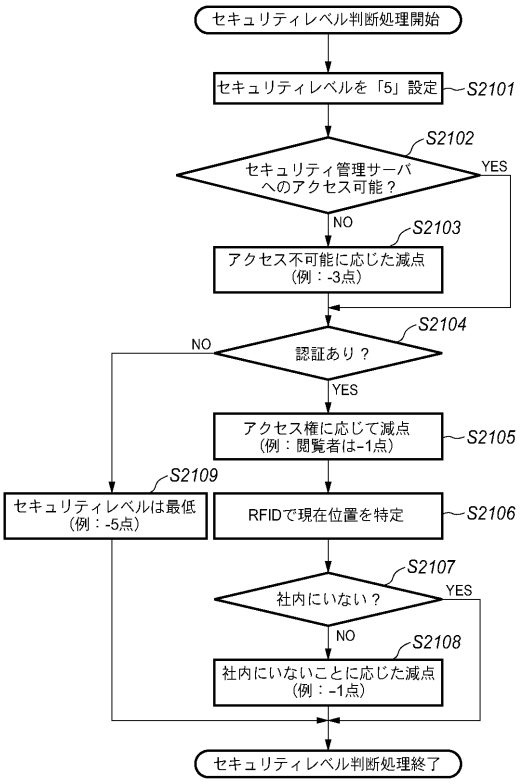
【図１９】



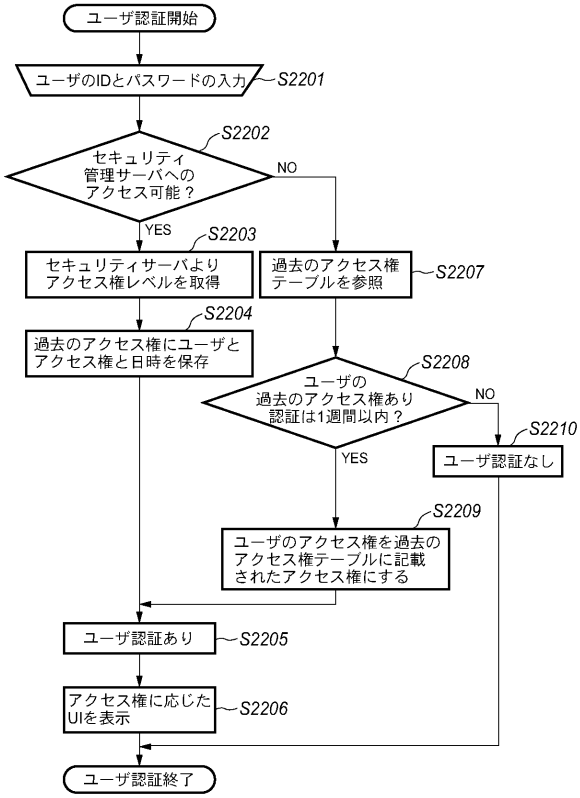
【図２０】



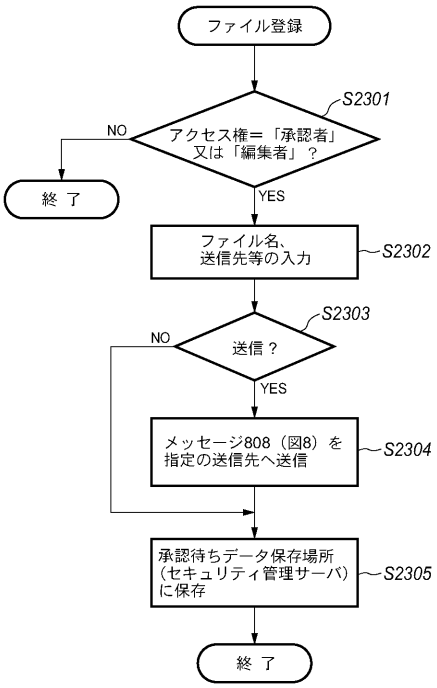
【図２１】



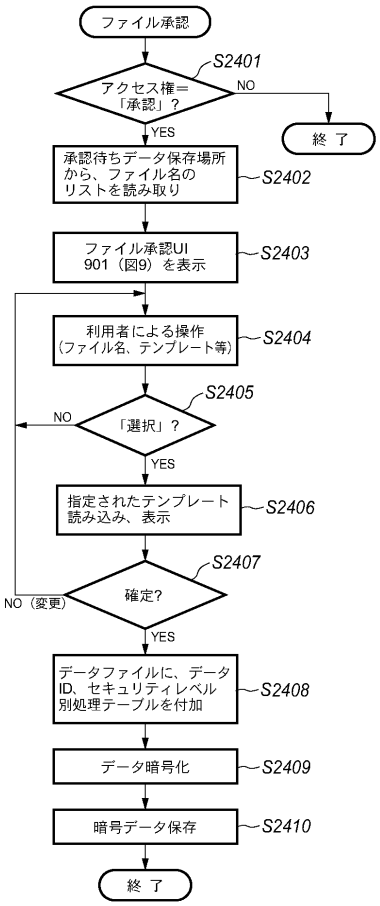
【図２２】



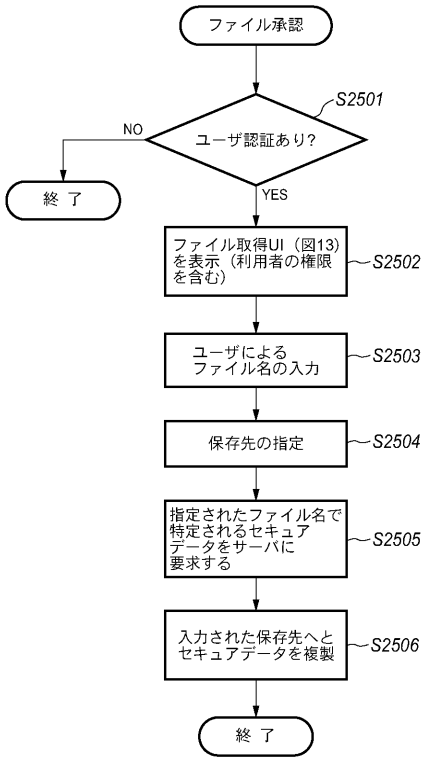
【図２３】



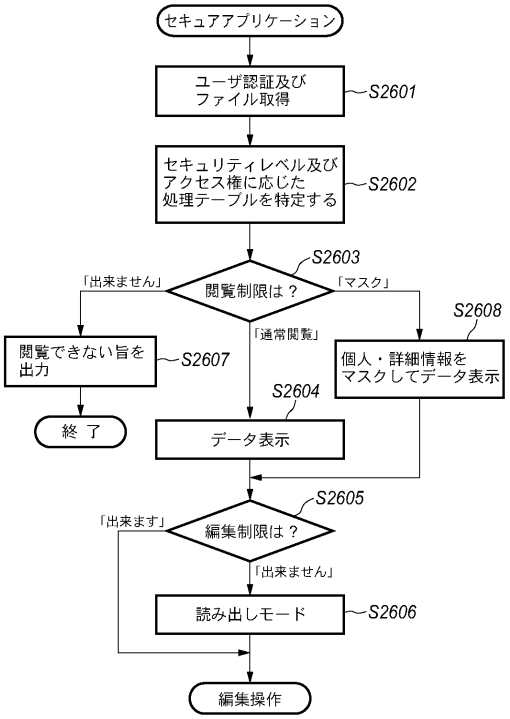
【図２４】



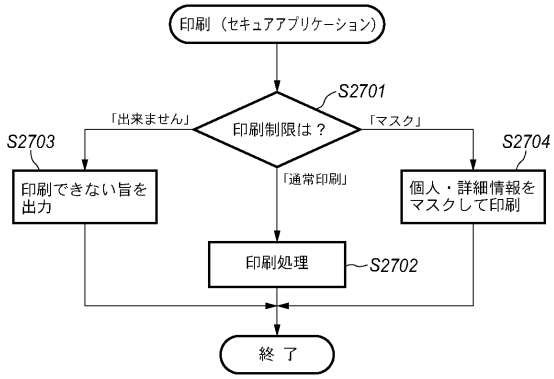
【図２５】



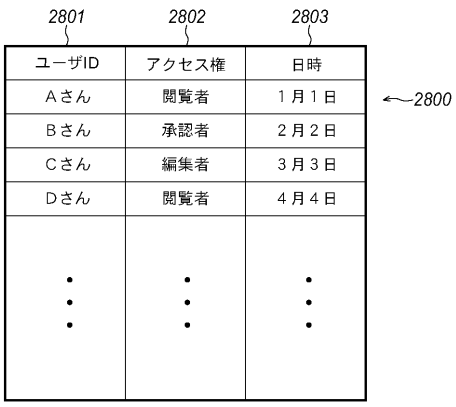
【図２６】



【図２７】



【図２８】



2801 ユーザID	2802 アクセス権	2803 日時
Aさん	閲覧者	1月1日
Bさん	承認者	2月2日
Cさん	編集者	3月3日
Dさん	閲覧者	4月4日
・	・	・
・	・	・
・	・	・

2800

【図２９】