(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2010-9621
(P2010-9621A)
(43)公開日　平成22年1月14日(2010.1.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/24	(2006.01)	G06F	12/14	520A	5B017
G06F 12/00	(2006.01)	G06F	12/14	540A	5B082
G06F 3/12	(2006.01)	G06F	12/00	537A	5J104
H04L 9/08	(2006.01)	G06F	3/12	K	
		H04L	9/00	601B	

審査請求 有　請求項の数 4　OL　（全 21 頁）　最終頁に続く

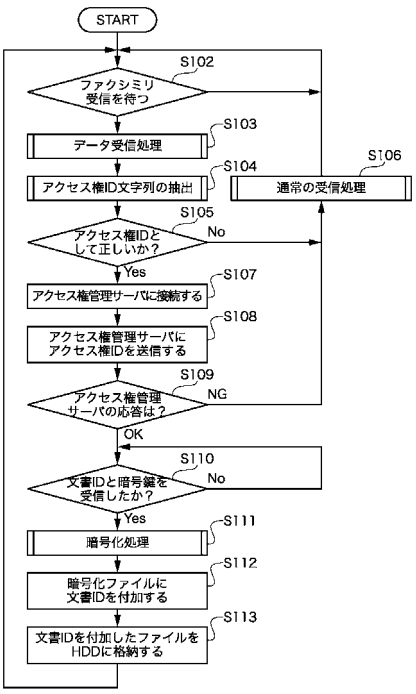
(21)出願番号　特願2009-232853 (P2009-232853)
(22)出願日　平成21年10月6日 (2009.10.6)
(62)分割の表示　特願2005-296961 (P2005-296961)の分割
原出願日　平成17年10月11日 (2005.10.11)

(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】情報処理方法およびその装置

(57)【要約】
【課題】　アクセス権管理システムは、アクセス権が設定可能なアプリケーションが限定され、ユーザが使用する情報機器に特定のアプリケーションが搭載されていなければ、所望するアクセス権を電子文書に設定することができない。
【解決手段】　外部からデータを受信し(S103)、受信したデータの所定位置からアクセス権IDを抽出し(S104)、アクセス権IDをアクセス権管理サーバに送信し(S108)、アクセス権管理サーバから文書IDおよび暗号鍵を取得する(S110)。そして、その暗号鍵を用いて受信したデータを暗号化し(S111)、暗号化したデータに文書IDを付加してメモリに格納する(S112、S113)。
【選択図】　図4



【特許請求の範囲】
【請求項１】
データに対する操作の権限を示すアクセス権を特定するアクセス権IDと、前記データを特定する文書IDとを関連付けて管理し、文書IDに基づいて当該文書IDで特定されるデータに対するアクセス権を特定することが可能なアクセス権管理サーバとネットワークを介して接続し、前記ネットワークまたは公衆回線を介して前記アクセス権管理サーバとは異なる情報機器と接続が可能な情報処理装置における情報処理方法であって、
前記情報処理装置の受信手段は、前記情報機器からデータを受信し、前記受信したデータを特定する文書IDを前記アクセス権管理サーバから受信し、
前記情報処理装置の送信手段は、前記受信したデータの中の予め定めた情報と一致する、前記情報処理装置が保持するテーブルに設定されたルールを探索し、前記一致するルールに設定されたアクセス権IDを前記アクセス権管理サーバへ送信し、
前記受信手段は、前記アクセス権IDを送信したことに基づき前記アクセス権管理サーバから送信される暗号鍵を受信し、
前記情報処理装置の暗号化手段は、前記受信した暗号鍵を用いて前記受信したデータを暗号化し、
前記情報処理装置の格納手段は、前記暗号化したデータに前記文書IDを付加してメモリに格納することを特徴とする情報処理方法。
【請求項２】
さらに、前記情報処理装置の変換手段は、前記受信データが予め定めたフォーマットではない場合、前記暗号化の前に当該受信データを前記予め定めたフォーマットに変換することを特徴とする請求項1に記載された情報処理方法。
【請求項３】
データに対する操作の権限を示すアクセス権を特定するアクセス権IDと、前記データを特定する文書IDとを関連付けて管理し、文書IDに基づいて当該文書IDで特定されるデータに対するアクセス権を特定することが可能なアクセス権管理サーバとネットワークを介して接続し、前記ネットワークまたは公衆回線を介して前記アクセス権管理サーバとは異なる情報機器と接続が可能な情報処理装置であって、
前記情報機器からデータを受信する一の受信手段と、
前記一の受信手段が受信したデータを特定する文書IDを前記アクセス権管理サーバから受信する二の受信手段と、
前記一の受信手段が受信したデータの中の予め定めた情報と一致する、前記情報処理装置が保持するテーブルに設定されたルールを探索する探索手段と、
前記探索手段が検出した前記一致するルールに設定されたアクセス権IDを前記アクセス権管理サーバへ送信する送信手段と、
前記送信手段が前記アクセス権IDを送信したことに基づき前記アクセス権管理サーバから送信される暗号鍵を受信する三の受信手段と、
前記三の受信手段が受信した暗号鍵を用いて前記一の受信手段が受信したデータを暗号化する暗号化手段と、
前記暗号化手段が暗号化したデータに、前記二の受信手段が受信した文書IDを付加してメモリに格納する格納手段とを有することを特徴とする情報処理装置。
【請求項４】
情報処理装置を制御して、請求項1または請求項2に記載された情報処理を実行することを特徴とするプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、電子データのアクセス権を制御する情報処理に関する。
【背景技術】
【０００２】

近年、情報漏洩を防ぐため、特定のユーザにだけ電子文書へのアクセス（閲覧、編集、印刷など）を許可する。あるいは、電子文書に有効期限を設定し、有効期限を過ぎると電子文書へのアクセスを禁止する機能をもつ電子文書のアクセス権管理システムが開発されている。このようなアクセス権管理システムにおいては、電子文書の作成時に、その文書に適用するポリシによってアクセス権を制御する。

【０００３】

このようなアクセス権管理サーバとして既に発表されているものに、例えばAdobe（登録商標）社のPolicy Server（非特許文献1）がある。Policy Serverは、PDF (Portable Document Format)ファイルに対して上記のアクセス権制御が可能である。しかし、Policy Serverによってアクセス権を設定可能なアプリケーションは、同社のAcrobat（登録商標）だけである。

【０００４】

またMicrosoft（登録商標）社が発表したInformation Rights Management (IRM)（非特許文献2）は、上記のアクセス権制御が可能である。しかし、アクセス権を設定可能なアプリケーションは、やはり同社のオフィスアプリケーションだけである。

【０００５】

つまり、従来のアクセス権管理システムは、アクセス権が設定可能なアプリケーションが限定され、ユーザが使用する情報機器に特定のアプリケーションが搭載されていなければ、所望するアクセス権を電子文書に設定することができない。

【０００６】

また、データに関するアクセス権制御の評価方法として、条件付きアクセス許可方法が知られている（特許文献1）。また、どのような制御を実施するかを記述したポリシの配布方法も知られている（特許文献2）。

【０００７】

一方、公衆網やネットワークに接続される複合機は、外部の情報機器から様々な経路を介して電子文書を受信する機能を有する。そして、受信した様々なデータフォーマットの電子文書を自己のボックスと呼ばれる記憶装置の領域へ蓄積したり、他の情報機器に転送する機能を有する。つまり、複合機が受信した電子文書は、ネットワーク環境を流通する。従って、オフィスなどの環境にアクセス権管理システムを導入する場合、受信した電子文書をボックスに蓄積したり、ネットワーク環境に送出する複合機がセキュリティホールになりかねない。

【先行技術文献】

【特許文献】

【０００８】

【特許文献１】特開2001-184264公報

【特許文献２】特開2004-166241公報

【非特許文献】

【０００９】

【非特許文献１】http://www.adobe.co.jp/products/server/policy/main.html

【非特許文献２】http://office.microsoft.com/ja-jp/assistance/HA010397891041.aspx

【発明の概要】

【発明が解決しようとする課題】

【００１０】

本発明は、発信元情報や受信方法に応じて、受信したデータのアクセス権制御を行うことを目的とする。

【課題を解決するための手段】

【００１１】

本発明は、前記の目的を達成する一手段として、以下の構成を備える。

【００１２】

本発明にかかる情報処理は、データに対する操作の権限を示すアクセス権を特定するア

クセス権IDと、前記データを特定する文書IDとを関連付けて管理し、文書IDに基づいて当該文書IDで特定されるデータに対するアクセス権を特定することが可能なアクセス権管理サーバとネットワークを介して接続し、前記ネットワークまたは公衆回線を介して前記アクセス権管理サーバとは異なる情報機器と接続が可能な情報処理装置における情報処理であって、前記情報機器からデータを受信し、前記受信したデータを特定する文書IDを前記アクセス権管理サーバから受信し、前記受信したデータの中の予め定めた情報と一致する、前記情報処理装置が保持するテーブルに設定されたルールを探索し、前記一致するルールに設定されたアクセス権IDを前記アクセス権管理サーバへ送信し、前記アクセス権IDを送信したことに基づき前記アクセス権管理サーバから送信される暗号鍵を受信し、前記受信した暗号鍵を用いて前記受信したデータを暗号化し、前記暗号化したデータに前記文書IDを付加してメモリに格納することを特徴とする。

【発明の効果】

【００１３】

本発明によれば、発信元情報や受信方法に応じて、受信したデータのアクセス権制御を行うことができる。

【図面の簡単な説明】

【００１４】

【図１】情報処理システムの構成例を示す図、

【図２】文書の暗号化し、暗号化文書への文書IDの付加を説明する図、

【図３】図1に示すアクセス権管理サーバやクライアント、複合機、ファクシミリ装置などの情報機器の構成例を示すブロック図、

【図４】複合機によるファクシミリ受信時の処理を説明するフローチャート、

【図５】データ受信処理の詳細を示すフローチャート、

【図６】アクセス権IDの抽出処理を示すフローチャート、

【図７】暗号化処理を示すフローチャート、

【図８】アクセス権IDの抽出処理を示すフローチャート、

【図９】実施例2の複合機による電子メール受信時の処理を説明するフローチャート、

【図１０】データ受信処理の詳細を示すフローチャート、

【図１１】アクセス権IDの抽出処理を示すフローチャート、

【図１２】暗号化処理を示すフローチャート、

【図１３】アクセス権IDの抽出処理を示すフローチャート、

【図１４】データ受信処理の詳細を示すフローチャート、

【図１５】暗号化処理の詳細を示すフローチャート、

【図１６】実施例4におけるシステムの構成例を示す図、

【図１７】複合機の構成例を示すブロック図、

【図１８】コントローラのソフトウェアモジュールの構成例を示すブロック図、

【図１９】アクセス権管理サーバが管理するポリシデータの一例を示す図、

【図２０】アクセス権管理サーバが管理する電子文書リストの一例を示す図、

【図２１】電子文書フォーマットの一例を示す図、

【図２２】図18に示す受信ルールが保持するデータの一例を示す図、

【図２３】受信ルールを登録する際に表示されるルール登録画面の一例を示す図、

【図２４】受信した電子文書にポリシを設定する処理例を示すフローチャート、

【図２５】実施例5の受信ルールが保持するデータの一例を示す図、

【図２６】受信ルールを登録する際に表示されるルール登録画面の一例を示す図、

【図２７】受信した電子文書にポリシを設定する処理例を示すフローチャート、

【図２８】受信した電子文書のポリシ設定履歴を含む受信履歴画面の一例を示す図である。

【発明を実施するための形態】

【００１５】

以下、本発明にかかる実施例の情報処理を図面を参照して詳細に説明する。なお、以下

では、人が読み取り、解釈可能な文章や画像が記録された電子文書をアクセス権制御、管理の対象として説明する。しかし、コンピュータが読み取り、解釈可能な例えばデータベースデータのようなデータが記録された電子ファイルもアクセス権制御、管理の対象になることは言うまでもない。

【実施例１】

【００１６】

［システムの構成］

図1は情報処理システムの構成例を示す図である。

【００１７】

アクセス権管理サーバ1007は、個々のファイルに対するユーザ個々の様々なアクセス権（例えば閲覧、有効期限、コピー、印刷、変更等）を制御する機能を提供する。

【００１８】

例えば、ユーザは、クライアントコンピュータ（以下「クライアント」と呼ぶ）1005を操作して文書を作成し、ネットワーク1008を介して、アクセス権管理サーバ1007から作成文書の文書IDを取得する。そして、予めアクセス権管理サーバ1007に登録した、作成者が設定したアクセス制御方法（ポリシ）のアクセス制御ID（ポリシID）を、文書IDとともに指定する。アクセス権管理サーバ1007は、文書IDとアクセス制御ID、および、復号鍵を自身の記憶領域に登録する。そして、ネットワーク1008を介して、クライアント1005に暗号鍵を送信する。クライアント1005は、受信した暗号鍵で作成文書（図2(a)）を暗号化し、そして、暗号化文書（図2(b)）に文書IDと、アクセス権管理サーバ1007を特定する情報（ホスト名やIPアドレスなど）を付加する（図2(c)）。暗号化が完了した後は受信した暗号鍵は削除して構わない。

【００１９】

文書の参照を希望するユーザは、クライアント1006を操作して、ネットワーク1008を介して、当該文書の文書IDと文書参照に関する諸条件（ユーザID、閲覧、印刷、コピー、配信等）をアクセス権管理サーバ1007に送信する。アクセス権管理サーバ1007は、受信した文書IDに対応するアクセス制御IDが示すアクセス制御方法と、受信した諸条件を比較して、当該文書の参照を認めるか否かを判定する。認める場合は、ネットワーク1008を介して、受信した文書IDに対応する復号鍵をクライアント1006に送信する。クライアント1006は、当該文書のファイルから文書IDを削除し、受信した復号鍵で暗号化文書を復号する。

【００２０】

上記のアクセス権制御は、クライアント間に限らず、複合機1001とクライアント間でも成り立つ。

【００２１】

［情報機器の構成］

図3は、図1に示すアクセス権管理サーバやクライアント、複合機、ファクシミリ装置などの情報機器の構成例を示すブロック図である。

【００２２】

CPU 11は、RAM 12をワークエリアとして、ROM 13やハードディスクドライブ(HDD) 14に格納されたオペレーティングシステム(OS)や様々なプログラムなどを実行し、システムバス18を介して後述する各構成を制御する。アクセス権管理サーバ1007やクライアント1005、1006の場合、HDD 14に格納され、CPU 13が実行するプログラムには、先述した文書作成プログラムやアクセス権を管理するアプリケーションプログラムや、後述する処理のプログラムが含まれる。

【００２３】

キーボードインタフェイス(KB I/F) 15には、キーボードやマウスなどの入力デバイスが接続される。ビデオカード19には、LCDなどのモニタが接続される。CPU 11は、モニタにユーザインタフェイスを表示する。ユーザは、ユーザインタフェイスに基づき、キーボードやマウスを操作して、コマンドやデータをCPU 11に入力する。なお、複合機1001やファクシミリ装置1003の場合、キーボードに代わるテンキーや様々な操作キーと、モニタが

操作パネルに配置される。

【００２４】

MODEM 16は公衆回線網とのインタフェイス、NIC 17はローカルエリアネットワーク(LAN)などのネットワーク1008とのインタフェイスである。なお、ファクシミリ装置1003はNIC 17を搭載しない場合もある。

【００２５】

［ファクシミリ受信文書のアクセス権管理］

図1に示すシステム構成の場合、上述したように、クライアント間に限らず、複合機1001とクライアント間でも上記のアクセス権制御が成り立つ。しかし、ネットワーク1008に接続せず、アクセス権管理サーバ1007と通信ができないファクシミリ装置1003がファクシミリ送信し、複合機1001やクライアントがファクシミリ受信した文書にはアクセス権制御が成り立たない。

【００２６】

以下では、複合機1001がファクシミリ装置1003から公衆回線を介してファクシミリ受信した文書のアクセス権を設定する処理を説明する。なお、ファクシミリ送信は、ファクシミリ装置1003に限らず、公衆回線に接続されたクライアントや複合機でもよい。また、ファクシミリ受信は、複合機1001に限らず、ネットワーク1008を介してアクセス権管理サーバ1007にアクセス可能な情報機器（例えばクライアント1005や1006）であればよい。

【００２７】

ファクシミリ装置1003は、ユーザが指示するアクセス権ID（例えば所定の文字列）を送信するファクシミリ文書のヘッダに埋め込み、ユーザが指定する電話番号にファクシミリ文書を送信する。

【００２８】

図4は複合機1001によるファクシミリ受信時の処理を説明するフローチャートである。

【００２９】

複合機1001は、ファクシミリを受信するまで待機する(S102)。そして、ファクシミリを受信すると、データ受信処理を行う(S103)。

【００３０】

図5はデータ受信処理の詳細を示すフローチャートである。まず、MODEM 16によって受信したデータをHDD 14の所定領域に格納する(S201)。そして、受信データの画像部分を伸長し、その画像（以下「受信画像」と呼ぶ）をファイル化し(S202)、当該ファイルをHDD 14の所定領域に格納する(S203)。

【００３１】

次に、図4において、受信データから送信者が指定するアクセス権IDを抽出する(S104)。

【００３２】

図6はアクセス権IDの抽出処理を示すフローチャートである。受信したデータのヘッダの所定部分から文字列を抽出する(S204)。ヘッダの所定部分としては、例えば発信者番号欄などが考えられる。

【００３３】

次に、図4において、抽出した文字列がアクセス権IDとして正しいか否かを判定し(S105)、正しくなければ通常の受信処理を行い(S106)、処理をステップS102に戻す。

【００３４】

また、抽出した文字列がアクセス権IDとして正しければ、アクセス権管理サーバ1007に接続する(S107)。そして、当該アクセス権IDをアクセス権管理サーバ1007に送信し(S108)、アクセス権管理サーバ1007の応答を待つ(S109)。アクセス権管理サーバ1007の応答が「アクセス権ID未登録(NG)」の旨を示す場合は通常の受信処理を行い(S106)、処理をステップS102に戻す。

【００３５】

また、アクセス権管理サーバ1007の応答が「アクセス権ID既登録(OK)」の旨を示せば、

アクセス権管理サーバ1007から文書IDと暗号鍵を受信するのを待つ(S110)。そして、文書IDと暗号鍵を受信すると暗号化処理を行う(S111)。

【００３６】

図7は暗号化処理を示すフローチャートである。受信した暗号鍵でHDD 14に格納した受信画像のファイルを暗号化する(S205)。なお、暗号化前のファイルや、暗号化処理が完了した後の暗号鍵は、暗号化ファイルや乱数で所定回数上書きする、削除するなど、HDD 14から削除する。

【００３７】

次に、図4において、ステップS111で暗号化したファイルに文書IDを付加し(S112)、文書IDを付加した暗号化ファイルをHDD 14の所定領域に格納し(S113)、処理をステップS102に戻す。

【００３８】

［変形例］

上記では、アクセス権IDをファクシミリプロトコルで定められたヘッダに埋め込む例を説明した。しかし、ファクシミリベンダが自由に使える領域、G3ならNSX、G4ならNSCといった非標準の手順信号を利用することも考えられる。この場合、アクセス権IDをG3ならNSXに、G4ならNSCに書き込む。

【００３９】

この場合、受信動作は、図4に示すステップS104の詳細（図6）が異なる。図8はアクセス権IDの抽出処理を示すフローチャートである。つまり、受信したデータのベンダが自由に使用可能な領域から文字列を抽出する(S204')。

【００４０】

このように、ユーザの近傍にある情報機器が、アクセス権の設定が可能な特定のアプリケーションを搭載しない場合や、アクセス権管理サーバ1007にアクセスできない場合でも、ファクシミリ送信する文書にアクセス権を設定することができる。なお、上記の情報機器は、例えば図1に示すシステム構成の場合は、ファクシミリ装置1003やネットワーク1008に未接続のクライアントや複合機（不図示）などである。

【実施例２】

【００４１】

以下、本発明にかかる実施例2の情報処理を説明する。なお、実施例2において、実施例1と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００４２】

［電子メール添付文書のアクセス権管理］

図1に示すネットワーク1008がインターネットなどの広域ネットワーク(WAN)に接続されている場合、クライアント1005、1006や複合機1001は、WANを経由する電子メールに添付された文書を受信することができる。しかし、その電子メールを発信した情報機器がアクセス権管理サーバ1007にアクセスできない場合、上記のアクセス権制御は成り立たない。

【００４３】

実施例2では、複合機1001がWANを介して受信した電子メールに添付された文書のアクセス権を設定する処理を説明する。なお、電子メールの受信は、複合機1001に限らず、ネットワーク1008を介してアクセス権管理サーバ1007にアクセス可能な情報機器（例えばクライアント1005や1006）であればよい。また、なお、複合機1001がインターネットファクス機能をもつ場合のインターネットファクス受信においても、実施例2で説明する電子メール受信時の処理が適用可能である。

【００４４】

図9は複合機1001による電子メール受信時の処理を説明するフローチャートである。

【００４５】

複合機1001は、電子メールを受信するまで待機する(S302)。そして、電子メールを受信すると、データ受信処理を行う(S303)。

【００４６】

図10はデータ受信処理の詳細を示すフローチャートである。まず、受信した電子メールデータをHDD 14の所定領域に格納する(S401)。そして、電子メールの本文をファイル化し(S402)、本文ファイルをHDD 14の所定領域に格納する(S403)。そして、添付ファイルがあるか否かを判定し(S404)、あれば添付ファイルをHDD 14の所定領域に格納する(S405)。

【００４７】

次に、図9において、受信データから送信者が指定するアクセス権IDを抽出する(S304)。

【００４８】

図11はアクセス権IDの抽出処理を示すフローチャートである。受信データのヘッダ内の件名（Subjectフィールド）に続く文字列をアクセス権IDとして抽出する(S411)。

【００４９】

次に、図9において、抽出した文字列がアクセス権IDとして正しいか否かを判定する(S305)。正しくなければ通常の受信処理を行い(S306)、処理をステップS302に戻す。

【００５０】

また、抽出した文字列がアクセス権IDとして正しければ、アクセス権管理サーバ1007に接続する(S307)。そして、当該アクセス権IDをアクセス権管理サーバ1007に送信し(S308)、アクセス権管理サーバ1007の応答を待つ(S309)。アクセス権管理サーバ1007の応答が「アクセス権ID未登録(NG)」の旨を示す場合は通常の受信処理を行い(S306)、処理をステップS302に戻す。

【００５１】

また、アクセス権管理サーバ1007の応答が「アクセス権ID既登録(OK)」の旨を示せば、アクセス権管理サーバ1007から文書IDと暗号鍵を受信するのを待つ(S310)。そして、文書IDと暗号鍵を受信すると暗号化処理を行う(S311)。

【００５２】

図12は暗号化処理を示すフローチャートである。受信した暗号鍵でHDD 14に格納した本文ファイルを暗号化する(S421)。そして、添付ファイルがあるか否かを判定し(S422)、あれば、受信した暗号鍵でHDD 14に格納した添付ファイルを暗号化する(S423)。なお、暗号化前のファイルは、暗号化ファイルで上書きする、削除するなど、HDD 14から削除する。

【００５３】

次に、図9において、ステップS311で暗号化したファイルに文書IDを付加し(S312)、文書IDを付加した暗号化ファイルをHDD 14の所定領域に格納し(S313)、処理をステップS302に戻す。なお、図4に示すフローチャートにおいて、ステップS311の暗号化処理の中で添付ファイルがあるか否かを判定するが、例えば、ステップS303のデータ受信処理中に添付ファイルの有無を判定してもよい。この場合、ステップS303で添付ファイルがあると判定した電子メールに対してのみ、ステップS304のアクセス権ID文字列の抽出処理を行う。一方、添付ファイルがないと判定した電子メールに対しては通常の受信処理(S306)を実行すればよい。

【００５４】

［変形例］

上記の実施例では、アクセス権IDを電子メールの件名欄（Subjectフィールド）に指定する例を説明したが、電子メールの他のヘッダ要素を用いても構わない。また、電子メールの本文にアクセス権IDを記載する方法も考えられる。

【００５５】

この場合、受信動作は、図9に示すステップS304の詳細（図11）が異なる。図13はアクセス権IDの抽出処理を示すフローチャートである。まず、電子メールの本文から所定のアクセス権IDの識別子を検索する(S511)。当該識別子を検出した場合、その識別子によって指示される文字列をアクセス権IDとして抽出する(S512)。なお、抽出する文字列は、例えば識別子の直後から改行コードや所定のコードの直前までの文字列や、識別子の後ろの所定長の文字列である。

【００５６】

また、上記の実施例では、抽出したアクセス権IDに対応するアクセス制御を、電子メールの本文および添付ファイルに適用する例を説明した。しかし、複合機1001がメール転送機能、印刷機能、閲覧機能などを有する場合は、受信した電子メールデータ全体をアクセス制御することが望ましい。

【００５７】

この場合、受信動作は、図9に示すステップS303の詳細（図10）と、暗号化処理S111の詳細（図12）が異なる。図14はデータ受信処理の詳細を示すフローチャートで、受信した電子メールデータの全体をファイルとしてHDD 14の所定領域に格納する(S501)。また、図15は暗号化処理の詳細を示すフローチャートで、受信した暗号鍵により電子メールデータ全体のファイルを暗号化する(S431)。

【００５８】

このように、ユーザの近傍にある情報機器が、アクセス権の設定が可能な特定のアプリケーションを搭載しない場合や、アクセス権管理サーバ1007にアクセスできない場合でも、電子メールの本文や添付文書にアクセス権を設定することができる。なお、上記の情報機器は、例えば図1に示すシステム構成の場合は、ネットワーク1008に未接続のクライアントや複合機（不図示）などである。

【実施例３】

【００５９】

以下、本発明にかかる実施例3の情報処理を説明する。なお、実施例3において、実施例1、2と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００６０】

上記の各実施例では、インターネットファクスを含むファクシミリ通信においてファクシミリヘッダにアクセス権IDを設定する方法、あるいは、電子メールの件名欄または本文にアクセス権IDを設定する方法を説明した。しかし、送信側ではアプリケーションによってファクシミリ送信する文書や電子メールに添付するファイルにアクセス権IDを付加してもよい。この場合、受信側では受信した電子メールに添付されたファイルからアクセス権IDを抽出して、アクセス制御すればよい。

【実施例４】

【００６１】

以下、本発明にかかる実施例4の情報処理を説明する。なお、実施例4において、実施例1～3と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【００６２】

［システムの構成］

図16は実施例4におけるシステムの構成例を示す図である。

【００６３】

LANなどのネットワーク1008には、複合機1001、1002、アプリケーションサーバ1004、クライアント1005、アクセス権管理サーバ1007、プリンタ1009などが接続されている。

【００６４】

複合機1001は、公衆網を介して、ファクシミリ装置1003とファクシミリ通信が可能である。

【００６５】

アプリケーションサーバ1004上では、複合機1001や1002が原稿から読み取った画像を格納するデータベース(DB)サーバと、WANを介して電子メールの送受信を行うメールサーバが動作する。クライアント1005は、アプリケーションサーバ1004に接続して、当該サーバが格納する画像などのデータをダウンロードしてモニタに表示する。また、クライアント1005は、画像などを含むページ記述言語形式のデータ（PDLデータ）を生成し、プリンタ1009、複合機1001、1002を利用して印刷を行うことができる。

【００６６】

［複合機の構成］

図17は複合機1001、1002の構成例を示すブロック図である。

【００６７】
コントローラ100は、スキャナ200およびプリンタ300に接続して、それらを制御するとともに、ネットワーク1008や公衆網と接続し、画像データやデバイス情報の入出力を行う。
【００６８】
CPU 103は、RAM 107をワークメモリとして、ROM 108やハードディスクドライブ(HDD) 109に格納された制御プログラムや画像処理プログラムを実行し、システムバス101およびイメージバス102を介して後述する各構成を制御する。また、RAM 107およびHDD 109は、画像データを一時記憶する画像メモリとしても利用される。
【００６９】
操作部インタフェイス(I/F) 104は、操作部400とのインタフェイスで、操作部400を操作するユーザの入力（指示）をCPU 103に伝えるとともに、操作部400のLCDに表示する画像データを操作部400に出力する。
【００７０】
ネットワークインタフェイスカード(NIC) 105は、ネットワーク1008とのインタフェイスで、ネットワーク1008との間でデータや情報の入出力を行う。MODEM 106は、公衆網とのインタフェイスで、公衆網を介したファクシミリ通信などを行う。
【００７１】
以上の構成はシステムバス101上に配置される。バスブリッジ110は、システムバス101と画像データを高速で転送するイメージバス102間のインタフェイスで、データ構造を変換することで、システムバス101とイメージバス102間のデータの流れをブリッジする。なお、イメージバス102は、PCI (Peripheral Component Interconnect)バスまたはIEEE1394などの高速バスで構成する。
【００７２】
次に、イメージバス102上に配置される構成を説明する。レンダリング部111は、PDLデータをビットマップイメージにレンダリング(RIP)するとともに、PDLデータに付属する情報をコントローラ100内で使用可能な後述する属性フラグデータに変換する。
【００７３】
デバイスI/F 112は、画像入出力デバイス（スキャナ200およびプリンタ300など）との間のインタフェイスで、画像データ転送の同期/非同期を変換する。なお、デバイスI/F 112と画像入出力デバイスの間は、USB (Universal Serial Bus)やIEEE1394などのシリアルバスで接続する。
【００７４】
入力画像処理部113は、スキャナ200から入力される画像データや、NIC 105を介して外部から受信した画像データに、後のプリントまたは画像送信を考慮した補正、加工、編集処理を施す。中間画像処理部114は、データ圧縮伸長処理および画像の変倍（拡大縮小）処理を行う。出力画像処理部115は、プリントすべき画像データに対して、プリンタ300に応じた補正、解像度変換などを施す。なお、中間画像処理部114は、多値画像データをJPEG符号化し、二値画像データをJBIG、MMRまたはMH符号化する。
【００７５】
なお、レンダリング部111のレンダリング結果である画像データおよび属性フラグデータは、入力画像処理部113を通さずに、中間画像処理部114に入力する場合もある。また、後述するように、外部から受信した画像データを処理する場合、その画像データおよび操作部400からの設定に従い割り当てた属性フラグデータは、入力画像処理部113を通さずに、中間画像処理部114に入力する場合もある。
【００７６】
また、ICカードスロット117にICカードメディアを挿入した後、操作部400に適切なPIN (Personal Identifier Number)コードを入力することで、暗号化、復号に用いる鍵情報の入出力が可能になる。暗号/復号部116は、ICカードメディアの鍵情報を用いて、データの暗号化、復号を行うハードウェアアクセラレータカードである。

【００７７】
図18はコントローラ100のソフトウェアモジュールの構成例を示すブロック図である。なお、コントローラ100のCPU 103が実行するソフトウェアは、所謂ファームウェアとして実装される。
【００７８】
OS 3001は、リアルタイムオペレーティングシステムで、組込システムの制御に最適化された各種資源管理のサービスと枠組みを、OS 3001上で動作するソフトウェアに提供する。OS 3001が提供する各種資源管理のサービスと枠組みには、例えば、次のものがある。
【００７９】
CPU 103による処理の実行コンテクストを複数管理することにより、複数の処理を実質的に並行動作させるマルチタスク管理（スレッド管理）。タスク間の同期やデータ交換を実現するタスク間通信。メモリ管理。割り込み管理。各種のデバイスドライバ、ローカルインタフェイスやネットワークや通信などの各種プロトコルの処理を実装したプロトコルスタックなど。
【００８０】
コントローラプラットフォーム3002は、ファイルシステム3003やジョブデバイス制御3004から構成される。ファイルシステム3003は、HDD 109やRAM 107などに構築された、データを格納するための機構で、コントローラ100が扱うジョブのスプール、各種データの保存に利用される。ジョブデバイス制御3004は、複合機のハードウェアを制御し、また、複合機の主にハードウェアが提供する基本機能（プリント、スキャン、通信、画像変換など）を利用するジョブを制御する。
【００８１】
アプリケーション3006は、OS 3001やコントローラプラットフォーム3002によって提供される機構を利用して、ネットワーク1008や公衆網を介して画像やテキストデータを入出力する組込アプリケーションである。アプリケーション3006の主な機構として、送信ジョブを統合管理する送信管理3007と、受信ジョブを統合管理する受信管理3008がある。
【００８２】
送信管理3007は、インターネットファックス(I-FAX)送信3009、FAX送信3010、FTP送信3011、Email送信3012を備え、送信ジョブを制御する。受信管理3008は、I-FAX受信3013、FAX受信3014、FTP受信3015、Email受信3016を備え、受信ジョブを制御する。これら送受信を補助する機構として、送信宛先のメールアドレスやURI (Uniform Resource Identifier)を管理するアドレス帳3017がある。また、受信時の処理ルールを管理する受信ルール3018、送受信履歴を管理する履歴管理3019、各種設定情報を管理する設定管理3020などがある。
【００８３】
［ポリシデータ］
図19はアクセス権管理サーバ1007が管理するポリシデータの一例を示す図である。
【００８４】
ポリシデータには、ポリシを識別するポリシID、ユーザがポリシを識別するための文字列であるポリシ名4002、ポリシを適用するユーザIDやグループIDを記録するUID/GID、各UIDやGIDに許可された権限を示すフィールドが備わる。権限フィールドには、データの読み取り、編集、印刷の許可不許可を示すビットがある。このポリシデータにより、ユーザやグループに対して、どのようなデータ操作を許可するかを、ポリシ単位に設定することができる。なお、実施例1のアクセス制御方法とアクセス制御IDはそれぞれポリシとポリシIDに相当する。
【００８５】
［電子文書リスト］
図20はアクセス権管理サーバ1007が管理する電子文書リストの一例を示す図である。
【００８６】

電子文書リストは、文書IDとポリシIDの対応関係を示し、どの文書にどのポリシを適用するかを参照することが可能である。

【００８７】

［電子文書フォーマット］

図21は電子文書フォーマットの一例を示す図である。

【００８８】

ファイルヘッダ6001は、電子文書フォーマットを識別するための情報（特定の文字列）を示す。バージョン6002は、電子文書フォーマットのバージョンを表す。文書ID6003は、当該電子文書にユニークな識別IDを示し、当該電子文書に適用するポリシを決定するために利用する。データ長6004は、データ部6005に格納されたデータ量を表す。データ部6005は、文書データそのものであるが、アクセス権管理サーバ1007が発行する暗号鍵で暗号化されている。

【００８９】

［受信ルール］

図22は、図18に示す受信ルール3018が保持するデータの一例を示す図である。

【００９０】

ルールIDは、各ルールに対してユニークな識別IDで内部管理用に利用する。ルール名は、ユーザがルールを識別するための任意の文字列である。受信手段は、I-FAX受信3013、FAX受信3014、FTP受信3015、Email受信3016など、複数存在する受信手段のどれを対象にするかを示す。

【００９１】

比較属性は、受信ジョブに含まれる、発信者番号や発信アドレスなど、様々な属性のどれを比較対象にするかを表す。比較値は、比較属性に指定された属性と、受信ジョブを比較するための値を表す。式は、値の比較方法を表し「と等しい」「で終わる」「で始まる」といった比較方法から選択する。

【００９２】

転送先は、受信ジョブが受信手段、比較属性、比較値、式で示される条件に一致した場合に、その電子文書の転送先を表す。ポリシIDは、同様に条件に一致した場合に、その電子文書に設定するポリシIDを表す。ポリシ名は、ユーザがポリシを識別するための文字列である。なお、複合機は、ポリシIDおよびポリシ名を、アクセス権管理サーバ1007と通信して取得する。

【００９３】

また、ユーザ名およびパスワードは、複合機がアクセス権管理サーバ1007と通信する際に利用する認証情報を表す。

【００９４】

図23は受信ルール3018にルールを登録する際に、CPU 103によって操作部400などに表示されるルール登録画面の一例を示す図である。

【００９５】

図23に示すルールは、受信ファクシミリの発信者番号が「123456789」と等しい場合に、ポリシ名「管理職」に対応するポリシを電子文書に設定する。そして、ファイル転送プロトコル(ftp)によりパス名「//server/honsya」へ、ポリシを設定した電子文書を転送する。

【００９６】

［アクセス権制御］

図24は受信した電子文書にポリシを設定する処理例を示すフローチャートで、CPU 103が実行する処理である。

【００９７】

まず、受信ジョブの発生を検知し(S901)、データ受信が完了すると(S902)、受信した電子文書のフォーマットを判定する(S903)。図21に示すフォーマットの電子文書であれば処理をS905へ進めるが、ファクシミリ受信したMMR、MHまたはJBIG符号化が施された文書の

場合はフォーマット変換し、文書IDを生成する(S904)。なお、文書IDは、アクセス権管理サーバ1007などから取得してもよい。また、受信した電子メールに添付されたファイルで、所定のフォーマットではない（ポリシの設定に対応しないフォーマット）場合も同様にステップS904の処理を行う。

【００９８】

次に、受信ルール3018から登録済みルールの数Rを取得し、カウンタnを0に初期化する(S905)。そして、R＞nを判定し(S906)、R≦nであれば受信ルールに一致しなかった場合であり、デフォルトの受信処理を行い(S907)、処理を終了する。なお、デフォルトの受信処理は、設定管理3020に予め設定された、電子文書をプリントする、ファイルシステム3003に格納する、などを行う。

【００９９】

一方、ステップS906においてR＞nであれば、n番目のルールを取得し(S908)、受信ジョブが取得したルールの条件に一致するか否かを判定する(S909)。一致しない場合は、カウンタnをインクリメントし(S910)、処理をステップS906へ戻す。

【０１００】

他方、受信ジョブが取得したルールの条件に一致する場合は、設定管理3020からアクセス権管理サーバ1007の情報を取得して、アクセス権管理サーバ1007に接続を試みる(S911)。そして、接続に失敗した場合は、ファイルシステム3003に予め用意されたエラー発生時の待避フォルダへ電子文書を格納し(S913)、処理を終了する。

【０１０１】

一方、アクセス権管理サーバ1007への接続に成功した場合は、電子文書から文書IDを抽出し(S914)、n番目のルールに設定されたポリシIDやユーザの認証情報を取得する(S915)。そして、文書ID、ポリシID、ユーザ認証情報をアクセス権管理サーバ1007に送信する(S916)。そして、アクセス権管理サーバ1007の応答を判定して(S917)、ポリシの設定に失敗した場合は、ファイルシステム3003に予め用意されたエラー発生時の待避フォルダへ電子文書を格納し(S913)、処理を終了する。

【０１０２】

また、ポリシの設定に成功した場合は、アクセス権管理サーバ1007の応答に含まれる暗号鍵で電子文書を暗号化し(S918)、n番目のルールに設定された転送先に暗号化した電子文書を送信、または、ボックスに保存し(S919)、処理を終了する。

【０１０３】

なお、ポリシの設定の成功失敗は、アクセス権管理サーバ1007の応答を解読することで判定することができるが、応答に暗号鍵が添付されていれば成功、添付されていなければ失敗と判定してもよい。また、暗号化した電子文書を送信した後、暗号化前後の当該電子文書は削除する。

【０１０４】

また、CPU 103は、アクセス権管理サーバ1007への接続、または、ポリシの設定に失敗してエラー退避フォルダに格納した電子文書について、所定時間経過後、再びポリシの設定にチャレンジする。あるいは、システム管理者または複合機の管理者が、定期的にエラー退避フォルダを調べ、格納された電子文書があれば、その時点でポリシの再設定をCPU 103に指示してもよい。勿論、CPU 103が、上記失敗を上記管理者のクライアント端末に通知するようにすることが好ましい。

【０１０５】

電子文書のアクセス権は、その文書の作成者が文書の性質などに応じて設定することが望ましいが、公衆網やネットワークから受信する電子文書にはアクセス権が全く設定されていない場合がある。仮に、一律のアクセス権を電子文書に設定する仕組は、柔軟性に欠け、ユーザが意図するアクセス権を設定することができず、不便である。これに対して、実施例4に従えば、電子文書の受信手段や発信者情報に応じたアクセス権を電子文書に設定する。さらに、電子文書の受信手段や発信者情報に応じた転送先に電子文書を転送、または、複合機のボックス（特定の記憶領域）に保存する配信を実現するので、柔軟性に富

んだシステムにすることができる。

【実施例５】

【０１０６】

以下、本発明にかかる実施例5の情報処理を説明する。なお、実施例5において、実施例1～4と略同様の構成については、同一符号を付して、その詳細説明を省略する。

【０１０７】

［受信ルール］

図25は実施例5の受信ルール3018が保持するデータの一例を示す図で、上書きフィールドが追加されている。上書きフィールドが「する」に設定されている場合、受信ジョブがルールに一致し、かつ、受信ジョブの電子文書にアクセス権が設定されている場合、受信ルールに従って電子文書のアクセス権を上書き（更新）する。

【０１０８】

図26は受信ルール3018にルールを登録する際に、CPU 103によって操作部400などに表示されるルール登録画面の一例を示す図である。

【０１０９】

図26に示すルールは、電子メールの発信者アドレス(From:)が「honsya@aaa.com」と等しい場合に、ポリシ名「管理職」に対応するポリシを電子文書に設定する。そして、ファイル転送プロトコル(ftp)によりパス名「//server/honsya」へ、ポリシを設定した電子文書を転送する。その際、受信した電子文書に既にアクセス権が設定されていた場合は、アクセス権を上書きするルールである。

【０１１０】

［アクセス権制御］

図27は、実施例5における受信した電子文書にポリシを設定する処理例を示すフローチャートで、CPU 103が実行する処理である。なお、図24と同じ処理には同一符号を付して、その詳細説明を省略する。

【０１１１】

ステップS912で、アクセス権管理サーバ1007への接続に成功した場合は、電子文書から文書IDを抽出し、アクセス権管理サーバ1007に送信して、ポリシの設定状態を問い合わせる(S921)。そして、ポリシの設定未設定の判定(S922)により、当該文書IDにポリシが未設定であればステップS915以降の処理を実行し、既設定であればn番目のルールの上書きフィールドを参照してポリシを上書きするか否かを判定する(S923)。上書きする場合はステップS915以降の処理を実行し、上書きしない場合は当該電子文書をn番目のルールに設定された転送先に転送する(S919)。

【０１１２】

このように、上書きフィールドによって、電子文書の作成者が設定したアクセス権を優先するか、電子文書を受信した情報機器に設定されたルールを優先するかを設定することができる。

【０１１３】

［受信履歴］

図28は受信した電子文書のポリシ設定履歴を含む受信履歴画面の一例を示す図で、CPU 103によって操作部400に表示される。

【０１１４】

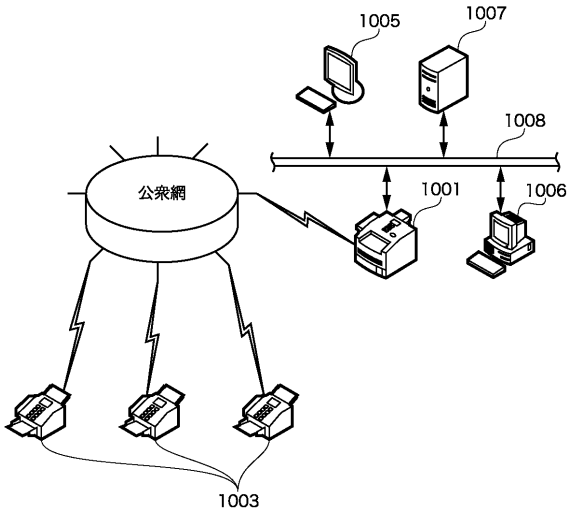
ポリシ付与欄は、電子文書のポリシの設定状況を示し、「ルール優先」は受信ルールに従ってポリシを設定したことを、「オリジナル優先」は既存のポリシを残したことを示す。また、符号1302で示す「－」は受信ルールに一致しなかったことを表し、符号1303で示す「NG」はアクセス権管理サーバ1007への接続、または、ポリシの設定に失敗したことを示す。

【０１１５】

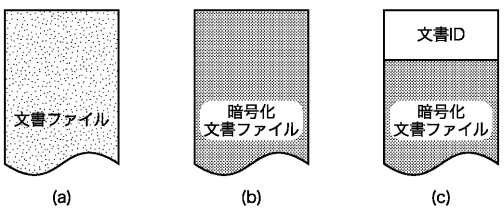
システムまたは情報機器の管理者は、この受信履歴画面を参照して、受信した電子文書にどのようにポリシが設定されたか把握、追跡することができる。

【０１１６】
［他の実施例］
なお、本発明は、複数の機器（例えばホストコンピュータ、インタフェイス機器、リーダ、プリンタなど）から構成されるシステムに適用しても、一つの機器からなる装置（例えば、複写機、ファクシミリ装置など）に適用してもよい。
【０１１７】
また、本発明の目的は、上記実施例の機能を実現するソフトウェアを記録した記憶媒体（記録媒体）をシステムまたは装置に供給し、そのシステムまたは装置のコンピュータ（CPUやMPU）が前記ソフトウェアを実行することでも達成される。この場合、記憶媒体から読み出されたソフトウェア自体が上記実施例の機能を実現することになり、そのソフトウェアを記憶した記憶媒体は本発明を構成する。
【０１１８】
また、前記ソフトウェアの実行により上記機能が実現されるだけでなく、そのソフトウェアの指示により、コンピュータ上で稼働するオペレーティングシステム(OS)などが実際の処理の一部または全部を行い、それによって上記機能が実現される場合も含む。
【０１１９】
また、前記ソフトウェアがコンピュータに接続された機能拡張カードやユニットのメモリに書き込まれ、そのソフトウェアの指示により、前記カードやユニットのCPUなどが実際の処理の一部または全部を行い、それによって上記機能が実現される場合も含む。
【０１２０】
本発明を前記記憶媒体に適用する場合、その記憶媒体には、先に説明したフローチャートに対応するソフトウェアが格納される。

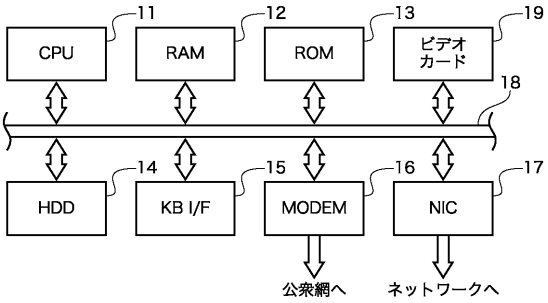
【図１】



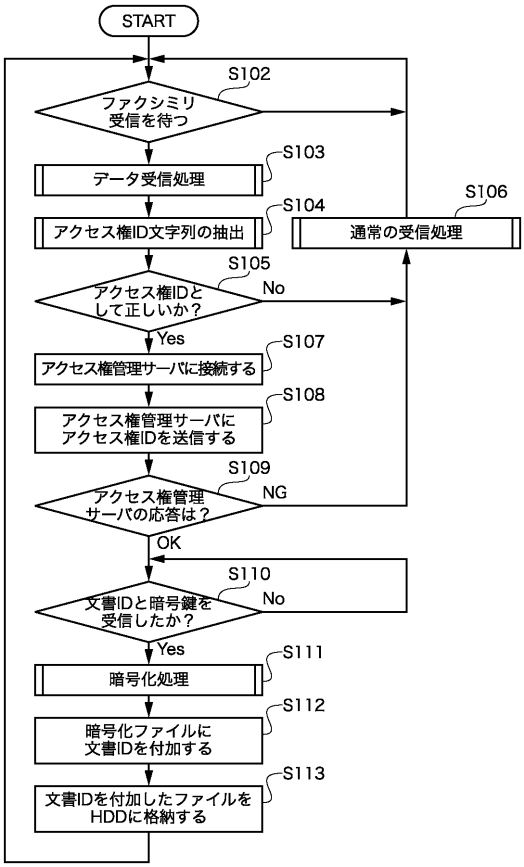
【図２】



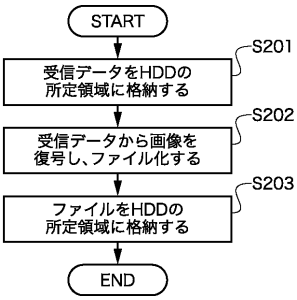
【図３】



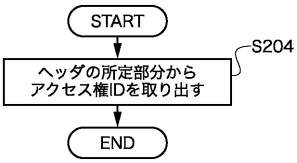
【図４】



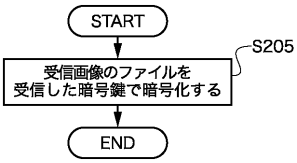
【図５】



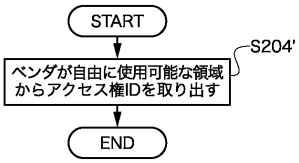
【図６】



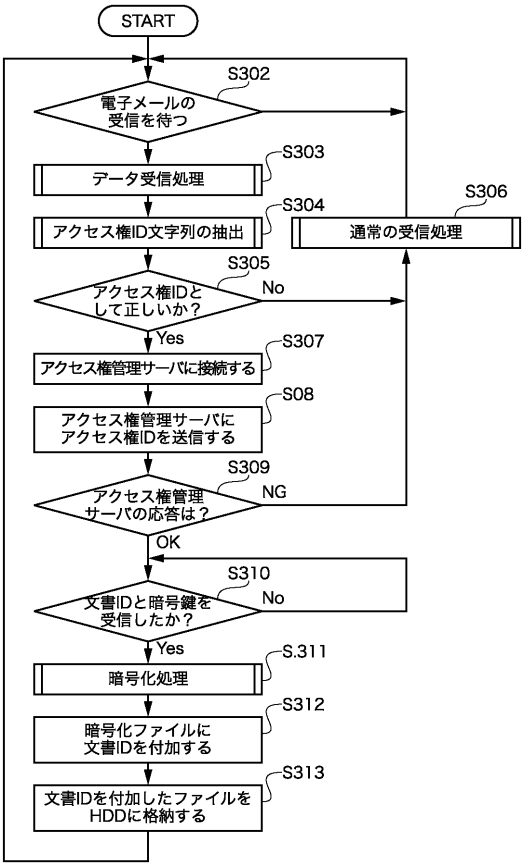
【図７】



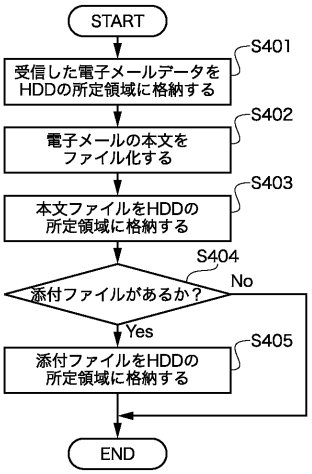
【図８】



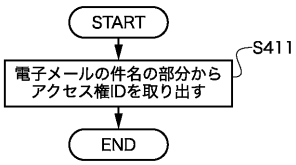
【図９】



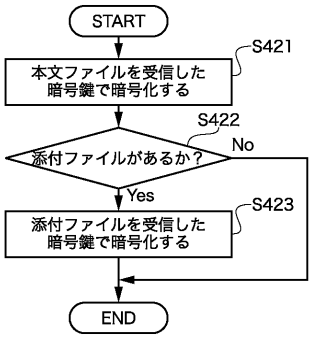
【図１０】



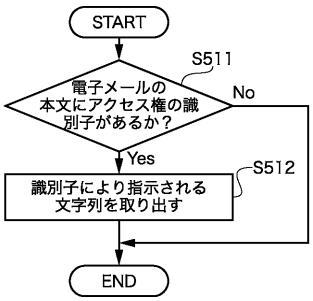
【図１１】



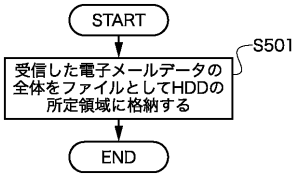
【図１２】



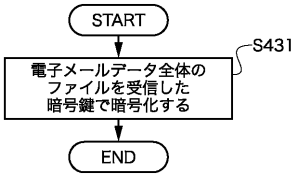
【図１３】



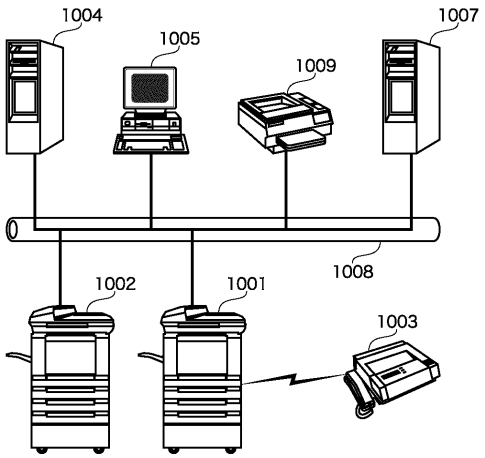
【図１４】



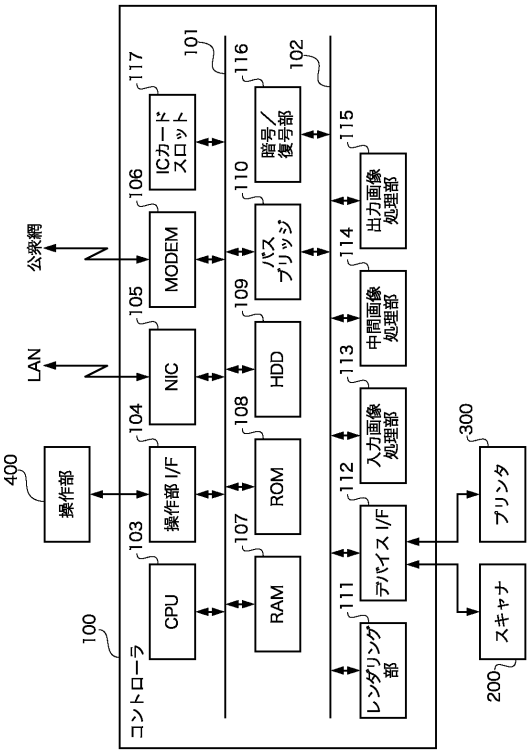
【図１５】



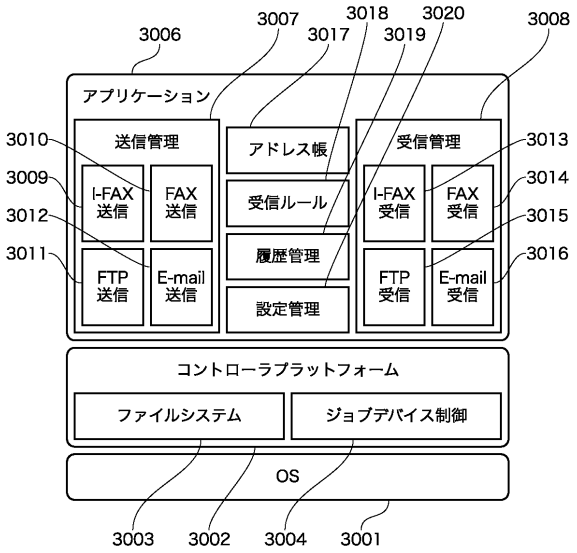
【図１６】



【図１７】



【図１８】



【図１９】

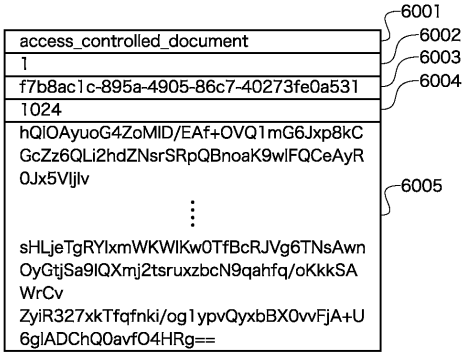
ポリシID	ポリシ名
P1	本社Fax
P2	本社Mail
P3	顧客1
P4	顧客2
P5	支店1
P6	支店2
P7	個人ボックス

ポリシID	UID/GID	権限 読み取り	権限 編集	権限 印刷
P1	UID0001	○	×	○
	GID1000	○	×	○
	GID1001	○	×	○
P2	UID0002	○	×	○
	GID2000	○	×	○
	GID2001	○	×	○
P3	UID0003	○	×	○
	GID3000	○	×	×
……	……	……	……	……
P7	UID0007	○	○	○

【図２０】

文書ID	ポリシID
f7b8ac1c-895a-4905-86c7-40273fe0a531	P1
f7b8ac1c-895a-4905-86c7-40273fe0a532	P2
……	……
f7b8ac1c-895a-4905-86c7-40273fe0a537	P2

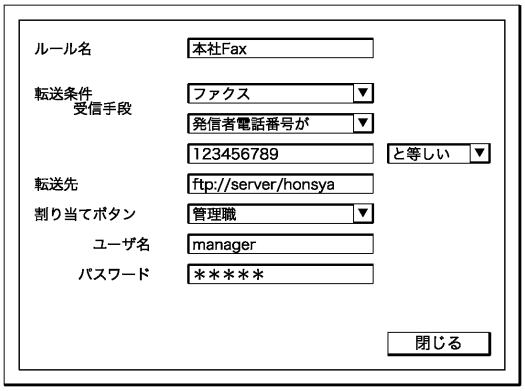
【図２１】



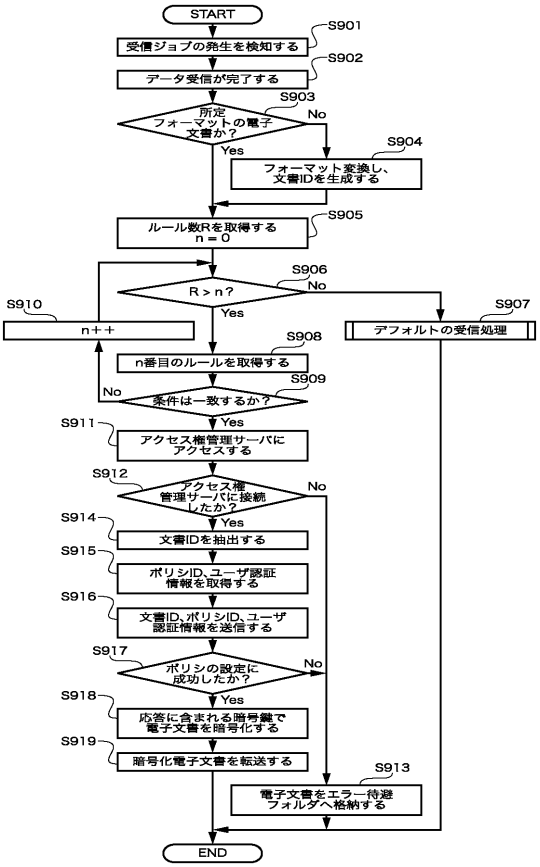
【図２２】

ルールID	ルール名	受信手段	比較属性	比較値	式	転送先	ポリシID	ポリシ名	ユーザ名	パスワード
1	本社Fax	ファクス	発信者電話番号	123456789	と等しい	ftp://server/honsya	P1	管理職	manager	******
2	本社Mail	メール	発信者アドレス	honsya@aaa.com	と等しい	ftp://server/honsya	P2	管理職	manager	******
3	顧客1	メール	発信者アドレス	user@yyy.com	と等しい	eigyo@aaa.com	P3	顧客1担当	sales	******
4	顧客2	メール	発信者アドレス	user@zzz.com	と等しい	eigyo@aaa.com	P4	顧客2担当	sales	******
5	支店1	I-ファクス	発信者アドレス	@aaa.com	で終わる	ftp://server/shiten	P5	支店担当	internal	******
6	支店2	I-ファクス	発信者アドレス	@aa.com	で終わる	ftp://server/shiten	P6	支店担当	internal	******
7	個人BoxF	ファクス	サブアドレス	10	と等しい	localBox00	P7	ユーザA	user_A	******
8	個人BoxM	メール	発信者アドレス	my@aaa.com	と等しい	localBox00	P7	ユーザA	user_A	******

【図２３】



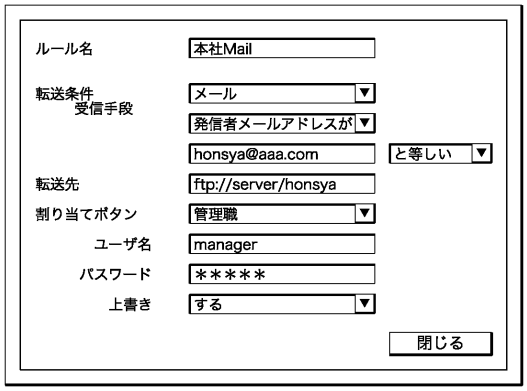
【図２４】



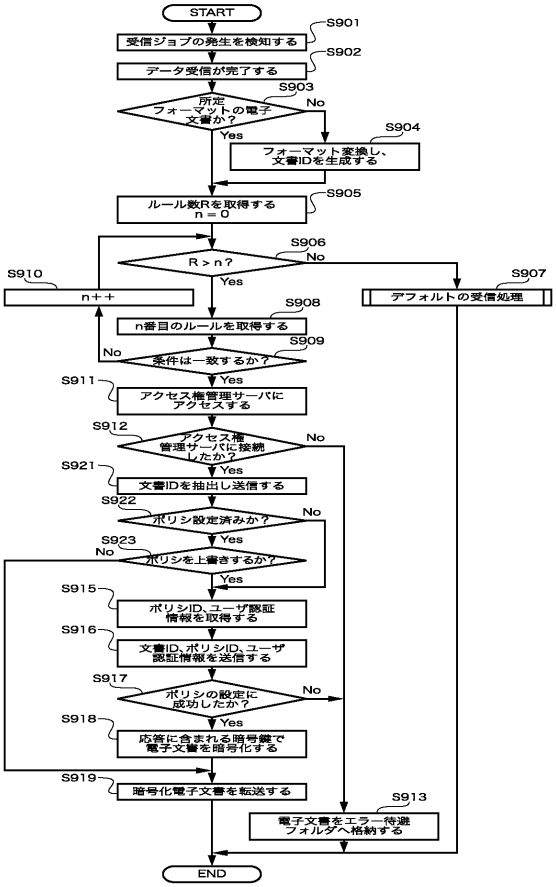
【図２５】

ルールID	ルール名	受信手段	比較属性	比較値	式	転送先	ポリシID	ポリシ名	ユーザ名	パスワード	上書き
1	本社Fax	ファクス	発信者電話番号	123456789	と等しい	ftp://server/honsya	P1	管理職	manager	＊＊＊＊＊	する
2	本社Mail	メール	発信者アドレス	honsya@aaa.com	と等しい	ftp://server/honsya	P2	管理職	manager	＊＊＊＊＊	する
3	顧客1	メール	発信者アドレス	user@yyy.com	と等しい	eigyo@aaa.com	P3	顧客1担当	sales	＊＊＊＊＊	しない
4	顧客2	メール	発信者アドレス	user@zzz.com	と等しい	eigyo@aaa.com	P4	顧客2担当	sales	＊＊＊＊＊	しない
5	支店1	I-ファクス	発信者アドレス	@aaa.com	で終わる	ftp://server/shiten	P5	支店担当	internal	＊＊＊＊＊	する
6	支店2	I-ファクス	発信者アドレス	@aa.com	で終わる	ftp://server/shiten	P6	支店担当	internal	＊＊＊＊＊	する
7	個人BoxF	ファクス	サブアドレス	10	と等しい	localBox00	P7	ユーザA	user_A	＊＊＊＊＊	する
8	個人BoxM	メール	発信者アドレス	my@aaa.com	と等しい	localBox00	P7	ユーザA	user_A	＊＊＊＊＊	する

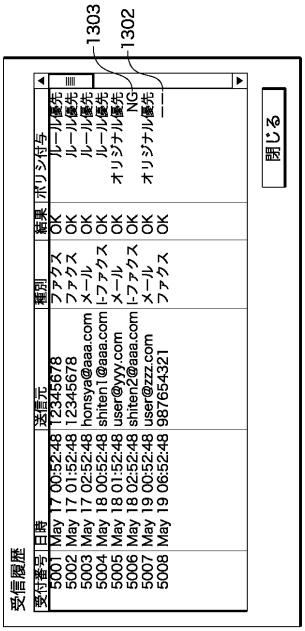
【図２６】



【図２７】


START
S901
受信ジョブの発生を検知する
S902
データ受信が完了する
S903
所定フォーマットの電子文書か？
No
Yes
S904
フォーマット変換し、文書IDを生成する
S905
ルール数Rを取得する n＝0
S906
R＞n？
No
Yes
S907
デフォルトの受信処理
S908
n番目のルールを取得する
S909
条件は一致するか？
No
Yes
S910
n++
S911
アクセス権管理サーバにアクセスする
S912
アクセス権管理サーバに接続したか？
No
Yes
S921
文書IDを抽出し送信する
S922
ポリシ設定済みか？
No
Yes
S923
ポリシを上書きするか？
No
Yes
S915
ポリシID、ユーザ認証情報を取得する
S916
文書ID、ポリシID、ユーザ認証情報を送信する
S917
ポリシの設定に成功したか？
No
Yes
S918
応答に含まれる暗号鍵で電子文書を暗号化する
S919
暗号化電子文書を転送する
S913
電子文書をエラー待避フォルダへ格納する
END

【図２８】


1303
1302
受信履歴
受付番号 日時 送信元 種別 結果 ポリシ付与
5001 May 17 00:52:48 12345678 ファクス OK ルール優先
5002 May 17 01:52:48 12345678 ファクス OK ルール優先
5003 May 17 02:52:48 honsya@aaa.com メール OK ルール優先
5004 May 18 00:52:48 shiten1@aaa.com i-ファクス OK オリジナル優先
5005 May 18 01:52:48 user@yyy.com メール OK オリジナル優先
5006 May 18 02:52:48 shiten2@aaa.com i-ファクス OK オリジナル優先
5007 May 19 00:52:48 user@zzz.com メール NG
5008 May 19 06:52:48 987654321 ファクス OK
閉じる

フロントページの続き

(51)Int.Cl.	F I	テーマコード（参考）
	Ｈ０４Ｌ　9/00　６０１Ｅ	

(72)発明者　内川　宙志
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
(72)発明者　礒田　隆司
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 AA02 AA03 BA06 BA07 CA16
5B082 EA11 GA11
5J104 AA16 EA01 EA04 EA15 EA16 JA03 MA05 NA02 NA37 PA14