(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2007-316952
(P2007-316952A)
(43)公開日　平成19年12月6日(2007.12.6)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/00	(2006.01)	G06F	15/00	330Z	5B017
H04N 1/21	(2006.01)	H04N	1/21		5B285
H04N 1/44	(2006.01)	H04N	1/44		5C073
G06F 21/24	(2006.01)	G06F	12/14	560B	5C075
		G06F	12/14	520C	

審査請求 未請求　請求項の数 9　ＯＬ　（全 15 頁）

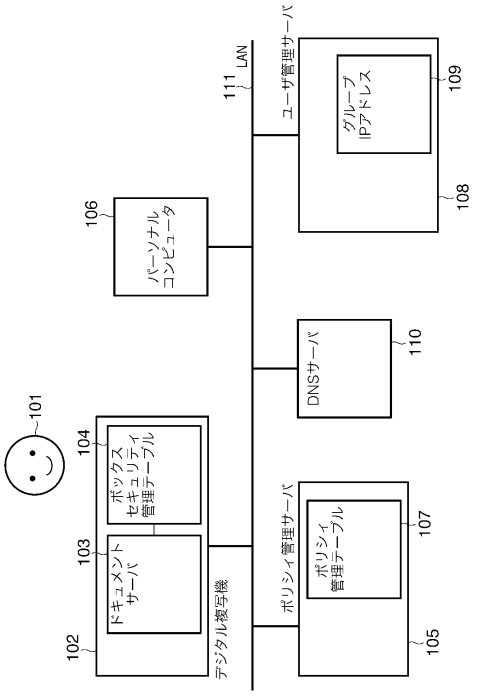
(21)出願番号　特願2006-145883 (P2006-145883)
(22)出願日　平成18年5月25日 (2006.5.25)

(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　宝木　洋一
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

最終頁に続く

(54)【発明の名称】情報処理装置及びその装置におけるデータ管理方法

(57)【要約】
【課題】　特定のグループでの運用ポリシィを変更した場合、外部に送出したファイルのAdobe Policy Server等の管理下にある個別ファイルのセキュリティポリシィも同様に変更したい。
【解決手段】　メモリエリアを複数のボックスに分割し、各ボックスに記憶したデータを管理する情報処理装置において、各ボックスごとに設定された、少なくとも編集条件及び出力条件を含むセキュリティ情報を記憶し（１０４）、ボックスに記憶されているデータを外部機器に転送する際、当該ボックスに設定されたセキュリティ情報に応じて、転送対象のデータに対するセキュリティ情報を設定し、そのボックスに設定されたセキュリティ情報が変更されると、そのボックスに記憶されたデータに設定されたセキュリティ情報を、その変更に応じて変更する（１０５）。
【選択図】　図１



【特許請求の範囲】
【請求項１】
複数の記憶領域を有するデータ記憶手段を備え、各記憶領域に記憶したデータを管理する情報処理装置であって、
前記各記憶領域ごとに設定された、少なくとも前記データに対する操作権限を示す情報を含むセキュリティ情報を記憶するセキュリティ記憶手段と、
前記記憶領域に記憶されているデータを外部機器に送信する際、前記セキュリティ記憶手段に記憶された当該記憶領域に設定された前記セキュリティ情報に応じて、送信対象のデータに対するセキュリティ情報を設定する設定手段と、
前記記憶領域に設定された前記セキュリティ情報が変更されると、前記記憶領域に記憶された前記データに設定された前記セキュリティ情報を、その変更に応じて変更する変更手段と、
を有することを特徴とする情報処理装置。
【請求項２】
前記設定手段は、前記セキュリティ記憶手段に記憶されている前記外部機器へ送信するデータに関するセキュリティ情報の内容を、前記情報処理装置が管理しないデータのセキュリティ情報を管理することが可能なセキュリティ管理サーバに設定することで前記送信対象のデータに対するセキュリティ情報を設定し、
前記変更手段は、前記セキュリティ情報が変更されたことに基づいて、前記セキュリティ管理サーバに設定されたセキュリティ情報を変更することによって前記データに設定されたセキュリティ情報を変更することを特徴とする請求項１に記載の情報処理装置。
【請求項３】
前記記憶領域に記憶されているデータの送信先のメールアドレスをＩＰアドレスに変更する手段を更に有することを特徴とする請求項１又は２に記載の情報処理装置。
【請求項４】
前記セキュリティ情報は、データの変更、消去、送信、カラー印刷の可否、及びデータの有効期限を示す情報を含むことを特徴とする請求項１乃至３のいずれか１項に記載の情報処理装置。
【請求項５】
複数の記憶領域を有するデータ記憶手段を備え、各記憶領域に記憶したデータを管理する情報処理装置におけるデータ管理方法であって、
前記各記憶領域ごとに設定された、少なくとも前記データに対する操作権限を示す情報を含むセキュリティ情報を記憶するセキュリティ記憶工程と、
前記記憶領域に記憶されているデータを外部機器に送信する際、前記セキュリティ記憶工程で記憶された当該記憶領域に設定された前記セキュリティ情報に応じて、送信対象のデータに対するセキュリティ情報を設定する設定工程と、
前記記憶領域に設定された前記セキュリティ情報が変更されると、前記記憶領域に記憶された前記データに設定された前記セキュリティ情報を、その変更に応じて変更する変更工程と、
を有することを特徴とするデータ管理方法。
【請求項６】
前記設定工程は、前記セキュリティ記憶工程で記憶した前記外部機器へ送信するデータに関するセキュリティ情報の内容を、前記情報処理装置が管理しないデータのセキュリティ情報を管理することが可能なセキュリティ管理サーバに設定することで前記送信対象のデータに対するセキュリティ情報を設定し、
前記変更工程は、前記セキュリティ情報が変更されたことに基づいて、前記セキュリティ管理サーバに設定されたセキュリティ情報を変更することによって前記データに設定されたセキュリティ情報を変更することを特徴とする請求項５に記載の情報処理装置。
【請求項７】
前記記憶領域に記憶されているデータの送信先のメールアドレスをＩＰアドレスに変更

する工程を更に有することを特徴とする請求項５又は６に記載のデータ管理方法。
【請求項８】
前記セキュリティ情報は、データの変更、消去、送信、カラー印刷の可否、及びデータの有効期限を示す情報を含むことを特徴とする請求項５乃至７のいずれか１項に記載のデータ管理方法。
【請求項９】
請求項５乃至８のいずれか１項に記載のデータ管理方法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】
本願発明は、複数の記憶領域のそれぞれに記憶しているデータのセキュリティポリシィを管理する情報処理装置及びその装置におけるデータ管理方法に関する。
【背景技術】
【０００２】
複写機、スキャナ、ファクシミリ装置などの機能を備えるデジタル複合機は、文書ファイルを格納するためにハードディスク等で構成される大容量の記憶装置を有している。このような記憶装置はボックス（ＢＯＸ）と呼ばれる複数の記憶領域を有している。そして、各ボックスに対してセキュリティ（個々のユーザに対する読み出し、書き込み、編集、印刷等の操作権限やアクセス権の設定）を設定することにより、ボックス内の文書に対するセキュリティを確保することが行われている（特許文献１参照）。このようなセキュリティの設定をセキュリティポリシィと呼ぶ。
【０００３】
一方、文書ファイルに対するアクセス権を管理する別の方法として、Adobe PolicyServer等の、セキュリティポリシィをサーバで一元管理するシステムの運用が始まっている。
【特許文献１】特開２００５－３４６３６６号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
しかしながら上記従来例では、大量の文書ファイルの全てのセキュリティポリシィをサーバが管理しなければならないため、文書ファイルへの操作要求が発生するたびにサーバへのアクセスが発生し、サーバへの負荷が大きくなる。また特定のグループ内の閉じられた環境でのみ運用している場合は、そのグループの運用ポリシィで簡便にセキュリティポリシィの管理を実施したい場合がある。更に、特定のグループから、そのグループ外の機器にデータを送出する場合には、Adobe PolicyServer 等の個別ファイルのセキュリティポリシィを管理できるサーバの管理下で、確実にセキュリティを管理したい。この場合の更なる課題として、特定のグループでの運用ポリシィを変更した場合、外部に送出したファイルのAdobe PolicyServer 等の管理下にある個別ファイルのセキュリティポリシィも同様に変更したいという要望が発生する。
【０００５】
本発明の目的は、上記従来技術の問題点を解決することにある。
【０００６】
本願発明の特徴は、
【課題を解決するための手段】
【０００７】
上記目的を達成するために本発明の一態様に係る情報処理装置は以下のような構成を備える。即ち、
複数の記憶領域を有するデータ記憶手段を備え、各記憶領域に記憶したデータを管理する情報処理装置であって、
前記各記憶領域ごとに設定された、少なくとも前記データに対する操作権限を示す情報

を含むセキュリティ情報を記憶するセキュリティ記憶手段と、
前記記憶領域に記憶されているデータを外部機器に送信する際、前記セキュリティ記憶手段に記憶された当該記憶領域に設定された前記セキュリティ情報に応じて、送信対象のデータに対するセキュリティ情報を設定する設定手段と、
前記記憶領域に設定された前記セキュリティ情報が変更されると、前記記憶領域に記憶された前記データに設定された前記セキュリティ情報を、その変更に応じて変更する変更手段とを有することを特徴とする。

【０００８】

上記目的を達成するために本発明の一態様に係る情報処理装置におけるデータ管理方法は以下のような工程を備える。即ち、
複数の記憶領域を有するデータ記憶手段を備え、各記憶領域に記憶したデータを管理する情報処理装置におけるデータ管理方法であって、
前記各記憶領域ごとに設定された、少なくとも前記データに対する操作権限を示す情報を含むセキュリティ情報を記憶するセキュリティ記憶工程と、
前記記憶領域に記憶されているデータを外部機器に送信する際、前記セキュリティ記憶工程で記憶された当該記憶領域に設定された前記セキュリティ情報に応じて、送信対象のデータに対するセキュリティ情報を設定する設定工程と、
前記記憶領域に設定された前記セキュリティ情報が変更されると、前記記憶領域に記憶された前記データに設定された前記セキュリティ情報を、その変更に応じて変更する変更工程と、を有することを特徴とする。

【０００９】

尚、この課題を解決するための手段は、本願発明の特徴の全てを列挙しているものではなく、特許請求の範囲に記載された他の請求項及びそれら特徴群の組み合わせも発明になり得る。

【発明の効果】

【００１０】

本発明によれば、特定の記憶領域のデータを、特定セキュリティポリシィで管理することにより、記憶領域内のデータを、外部のセキュリティポリシィサーバを用いずに統一したセキュリティポリシィで簡便かつ確実に管理できる。

【００１１】

又、各記憶領域から外部機器にデータ送出する場合に、その送出するデータ単位でセキュリティの管理及び設定ができるようにすることにより、外部機器へ送出したデータのセキュリティ管理が確実に行える。

【００１２】

又、各記憶領域のセキュリティポリシィを変更した場合、対応するポリシィサーバ側の情報をも同様に変更する。これにより、管理しているセキュリティポリシィを変更した場合に、既に外部機器に転送したデータのセキュリティポリシィの運用をも確実に変更できる。

【発明を実施するための最良の形態】

【００１３】

以下、添付図面を参照して本発明の好適な実施の形態を詳しく説明する。尚、以下の実施の形態は特許請求の範囲に係る本発明を限定するものでなく、また本実施の形態で説明されている特徴の組み合わせの全てが本発明の解決手段に必須のものとは限らない。

【００１４】

図１は、本発明の実施の形態に係る情報処理装置としてのデジタル複写機とサーバとを含むシステムの概略構成を示す図である。尚、このデジタル複写機は、スキャナ、プリンタ、ファクシミリ装置としても機能する多機能装置である。

【００１５】

図において、ドキュメントサーバ１０３は、デジタル複写機１０２のボックス（ＢＯＸ）にデータを格納するサーバシステムである。「ボックス」は複写機１０２のハードディ

スク（ＨＤＤ）内に構築される、データの格納領域であり、後に詳述する。このドキュメントサーバ１０３は、ボックスセキュリティ管理テーブル１０４（図４）を保持している。このボックスセキュリティ管理テーブル１０４は、対応するボックスに格納されたファイルデータのセキュリティに関する情報を記憶している。各ボックスに格納された全てのデータは一律に、このボックスセキュリティ管理テーブル１０４の内容に従って運用される。なお、ドキュメントサーバ１０３およびボックスセキュリティ管理テーブル１０４はデジタル複写機１０２に内蔵されていても良いし、デジタル複写機１０２の外部にあっても良い。

【００１６】

図４は、本実施の形態に係るボックスセキュリティ管理テーブル１０４の一例を示す図である。

【００１７】

４０１は、デジタル複写機１０２のボックスを特定するボックスＩＤ（識別子）である。４０２は、このボックスのデータが転送可能かどうか、４０３はこのボックスのデータを変更可能かどうか、また４０４はこのボックスのデータを消去可能かどうかを、それぞれ示すデータを記憶する。４０５は、このボックスのデータをカラーで印刷可能かどうか、４０６は、このボックスのデータを白黒で印刷可能かどうかを、それぞれ示すデータを記憶する。これら４０２～４０６において、「ＯＫ」は可能を示し、そうでないときは「ＮＧ」がセットされている。４０７は、このボックスのデータの格納期限を記憶している。

【００１８】

このように各ボックスに記憶されたデータは、このボックスセキュリティ管理テーブル１０４の内容に従って、そのセキュリティが管理される。例えば図４の例では、ＩＤが「００１」であるボックスのデータは格納期限が「無期限」で、そのデータの転送、変更及び白黒印刷が可能であるが、そのデータの消去及びカラーでの印刷は禁止されている。

【００１９】

ユーザ管理サーバ１０８は、ボックスセキュリティ管理テーブル１０４の運用対象であるグループに含まれる機器（コンピュータやデジタル複写機）を規定するグループＩＰアドレス１０９（図５）を保持している。このグループＩＰアドレスに対応して、図８で示すデジタル複写機１０２の操作部２１３（図２）のユーザ認証画面で、ユーザ認証を行うためのユーザ名及びパスワードを保持している。

【００２０】

図８は、本実施の形態に係るデジタル複写機１０２の操作部２１３（図２で詳述する）の表示部に表示された認証画面の一例を示す図である。

【００２１】

ここで、ユーザ１０１は、予め定められているユーザ名及びパスワードを入力し、「ＯＫ」ボタンを指示することにより、このデジタル複写機１０２の操作が可能になる。尚、「キャンセル」ボタンは、このユーザ認証処理をキャンセルするのに使用される。

【００２２】

ポリシィ管理サーバ１０５は、各ボックスのデータ毎のセキュリティを管理するポリシィ管理テーブル１０７を保持している。このポリシィ管理テーブル１０７の一例を図７に示す。いまデジタル複写機１０２から、共通のグループに含まれる機器以外のパーソナルコンピュータ１０６にファイルを送出する際に、ボックスセキュリティ管理テーブル１０４の内容に従って、そのファイルのセキュリティに関する使用制限が設定され、それがポリシィ管理テーブル１０７に格納される。

【００２３】

図７は、本実施の形態に係るポリシィ管理テーブル１０７の一例を示す図である。

【００２４】

７０１は、電子データのファイルを特定するファイルＩＤを示す。７０２～７０６のそれぞれは、前述の図４に示すボックスのセキュリティ管理テーブル１０４の４０２～４０

６に対応している。即ち、このファイルが格納されているボックスのセキュリティ管理テーブル１０４の４０２～４０６と同じ値がセットされる。７０７はＩＰアドレスで、このファイルが含まれるボックスの運用対象であるグループに含まれる機器を規定するグループＩＰアドレスを記憶している。７０８は、ボックスＩＤで、このファイルを格納しているボックスを特定する。７０９は、このファイルの格納期間が有効期間内であるか否かを格納している。

【００２５】

図７の例では、ボックスＩＤが「００２」のファイルＩＤが「０１２．．」であるファイルのセキュリティ情報がセットされている。この図７において、７０２～７０６の値は、図４の対応する（ＢＯＸ　ＩＤが００２の行）４０２～４０６の値にそれぞれ等しい。

【００２６】

ＤＮＳサーバ１１０は、デジタル複写機１０２のボックスから他の機器にファイルを送信する際、その送信先のメールアドレス（E-mail Address）やホスト名などから、該当するＩＰアドレスを決定し、その決定したＩＰアドレスをデジタル複写機１０２に伝える。不図示のＳＭＴＰ（Simple Mail Transfer Protocol）サーバなどがＤＮＳサーバの代わりにメールアドレスから機器のＩＰアドレスを決定する役割を果たしても良い。

【００２７】

図６は、本実施の形態に係るデジタル複写機１０２の操作部２１３の表示部に表示されたファイル送信を指示する画面の一例を示す図である。

【００２８】

図において、６０１はボックスＩＤの入力欄を示す。６０２は、送信するファイルを指定する欄で、ここには、入力欄６０１で特定されたボックス（この例ではボックスＩＤ：００１）に格納されているファイルの一覧が表示される。ここでユーザ１０１は、カーソル（不図示）等により、送信したいファイルを選択する。選択されたファイル名は反転表示するなどして識別可能にしても良い。６０３は送信先を特定するメールアドレス等を入力する欄である。ここに入力されたメールアドレスやホスト名に基づいて、ＤＮＳサーバ１１０により、対応するＩＰアドレスが決定される。

【００２９】

デジタル複写機１０２、ポリシィ管理サーバ１０５、パーソナルコンピュータ１０６、ユーザ管理サーバ１０８、ＤＮＳサーバ１１０は例えば、イーサネット（登録商標）等で構成されるＬＡＮ（Local Area Network）に接続されている。

【００３０】

図２は、本実施の形態に係るデジタル複写機１０２の構成を説明するブロック図である。

【００３１】

図２において、スキャナ２０１は、原稿を光学的に読み取って、それを電気信号に変換して原稿画像データを生成する。このスキャナ２０１は、１画素を、それぞれが８ビットの輝度情報を有するＲＧＢ（赤（Ｒｅｄ），緑（Ｇｒｅｅｎ），青（Ｂｌｕｅ））のデジタルデータを生成する。本実施形態において、このスキャナ２０１の読み取り解像度は、主走査方向及び副走査方向ともに４００ｄｐｉとする。画像処理部２０２は、スキャナ２０１から入力した画像データに対して、入力マスキングやＲＧＢからシアン（Ｃ）マゼンタ（Ｍ）イエロー（Ｙ）黒（Ｋ）へのログ変換、出力マスキング等の処理を実行する。プリンタ２０３は、画像処理部２０２で処理された面順次のＣＭＹＫデータを入力し、例えば電子写真方式等によりカラー画像を印刷する。

【００３２】

フレームバッファ２０４は、例えば１３９ＭＢのメモリ容量を有するシンクロナスＤＲＡＭである。このフレームバッファ２０４は、スキャナ２０１から取り込んだラスタ画像データを記憶したり、ネットワークから受信した画像データをＣＰＵ２０６の制御の下に記憶する。ＣＰＵ２０６は、ＲＯＭ２０８あるいはＨＤＤ２１１及びＲＡＭ２０９に記憶されているプログラムを実行して、このデジタル複写機１０２を制御している。Ｉ／Ｏポ

ート２１２は、ＣＰＵバス２０５に接続されており、ＣＰＵ２０６からの制御信号をスキャナ２０１やプリンタ２０３に出力して制御したり、センサ等から信号を入力する。ＲＯＭ２０８は、このシステムのブート時に実行されるブートプログラムを記憶している。ＲＡＭ２０９は、例えば１１７ＭＢのシンクロナスＤＲＡＭである。このＲＡＭ２０９は、フレームバッファ２０４と合わせて２５６ＭＢのシンクロナスＤＲＡＭのメモリモジュールで構成され、ＣＰＵバス２０５に接続されていてもよい。ＣＰＵ２０６により実行されるプログラムはＨＤＤ２１１にインストールされており、この複写機の電源オン時に、ＲＯＭ２０８のブートプログラムに従ってＲＡＭ２０９にロードされて、ＣＰＵ２０６の制御の下に実行される。

【００３３】

ＳＣＳＩのコントローラ２１０は、ＣＰＵバス２０５に接続している。ＨＤＤ２１１は、ＳＣＳＩコントローラ２１０に接続された、ハードディスクドライブである。ネットワークＩ／Ｆ２０７はＣＰＵバス２０５に接続されており、外部の１０ＢａｓｅＴ又は１００ＢａｓｅＴのＥｔｈｅｒｎｅｔ（登録商標）ネットワークと接続されデータのやりとりを行う。このネットワークＩ／Ｆ２０７を介して図１に示すパーソナルコンピュータ１０６、ＤＮＳサーバ１１０が接続されている。操作部２１３は、ＬＣＤ等の表示部とタッチパネル、各種操作用ボタン等を含んでいる。

【００３４】

デジタル複写機１０２のＨＤＤ２１１には、「ボックス」と呼ばれる複数のデータ格納領域が設けられている。これら複数の格納領域全体をボックスと称する場合もあるし、複数の格納領域のうち、ある格納領域を指してボックスと称する場合もある。ドキュメントサーバ１０３はボックス全体を管理している。ボックスの複数の格納領域は、ＢＯＸ ＩＤによって特定することが出来る。各ボックスに対する操作権限やボックス内のデータの格納期限は図４のボックスセキュリティ管理テーブル１０４で管理されている。

【００３５】

ボックスに格納されるデータとしては、デジタル複写機１０２のスキャナ２０１が読み取った原稿画像の画像データや、パーソナルコンピュータ１０６から受信した印刷データをイメージに展開した画像データが含まれる。また、パーソナルコンピュータで作成した文書データなどが格納されても良い。

【００３６】

図９は、本実施の形態に係るデジタル複写機１０２のスキャナ２０１で読み取った原稿データを、ドキュメントサーバ１０３のボックスに格納するまでの一連の動作を説明する図である。

【００３７】

９０１において、操作部２１３の表示部に表示されたユーザ認証画面（図８）で、ユーザ１０１は操作部２１３から、そのユーザ名及びパスワードを入力する。デジタル複写機１０２は、ユーザ認証画面で入力されたユーザ名とパスワードをユーザ管理サーバ１０８へ問い合わせて、入力されたユーザ名とパスワードが正当であるかをチェックする。正当である場合、ユーザ管理サーバ１０８から肯定応答を受理し、これによりユーザ１０１が、そのデジタル複写機１０２にログインできる。ユーザ管理サーバから否定応答があった場合、デジタル複写機１０２はユーザ１０１からのログイン要求を受け付けないようにすればよい。９０２では、スキャナ２０１で読み取った画像データを格納するボックスを選択する。

【００３８】

図３は、画像データを格納するボックスを選択する際の操作部２１３の表示部に表示されるボックス選択画面の一例を示す図である。

【００３９】

図３では、ドキュメントサーバ１０３のボックスの一覧が表示されており、ユーザ１０１は、この一覧の中から、カーソル（不図示）等を用いて、その画像データを格納したいボックスを選択する。３００はファイル名の入力欄で、その画像データのファイル名を入

力するのに使用される。

【００４０】

９０２では、この操作部２１３に表示されたボックス選択画面で、格納したいボックスを指定し、そのボックスに格納するデータファイルの名称を入力する。これにより９０４で、ドキュメントサーバ１０３は、その選択されたボックスと、そのファイル名を記憶する。

【００４１】

次に９０３で、デジタル複写機１０２は、スキャナ２０１で読み取った原稿のデータファイルをドキュメントサーバ１０３に送出する。これにより９０５で、ドキュメントサーバ１０３は、デジタル複写機１０２から送られてくる画像データを、９０４で記憶したボックス名に該当する記憶領域に格納する。

【００４２】

図１０は、本実施の形態に係るデジタル複写機１０２のドキュメントサーバ１０３のデータを外部機器（ここではパーソナルコンピュータ１０６）に送信する一連の動作を説明する図である。

【００４３】

１００１では、図９の９０１と同様に、ユーザ１０１が操作部２１３の認証画面（図８）を操作してデジタル複写機１０２にログインする。次に１００２で、操作部２１３のファイル選択画面（図６）を操作して、ボックスＩＤを選択し、送信したいファイルを特定する。更に、その送信先を特定するメールアドレス、あるいはホスト名などの情報を入力欄６０３に入力して、送信宛先を決定する。そしてこの入力されたメールアドレス等の情報がＤＮＳサーバ１１０に送られる。１００９では、ＤＮＳサーバ１１０は、そのメールアドレス等の情報に対応するＩＰアドレスを応答する。これによりデジタル複写機１０２は、そのファイルを転送する転送先のＩＰアドレスを特定できる。

【００４４】

こうしてＩＰアドレスが特定されると１００３で、そのデータの転送先の機器のＩＰアドレスが、特定のグループのＩＰアドレスであるか否かを、ユーザ管理サーバ１０８に問い合わせる。これによりユーザ管理サーバ１０８は、１００４で、グループＩＰアドレス１０９を参照して、そのＩＰアドレスが、特定のグループに属しているか否かを判定する。ここで転送先の機器が、この特定のグループ以外であれば１００５～１００６で示す処理を実行する。一方、転送先の機器が、この特定のグループに含まれていれば１００７に進み、その転送するデータを取得し、１００８でＩＰアドレスに従ってパーソナルコンピュータ１０６に送信する。なお、特定のグループ内の機器のメールアドレスを予め送信側のデジタル複写機１０２に登録しておく様にしても良い。その場合、１００４で送信先のメールアドレスがグループ内であるか否かをＤＮＳサーバに問い合わせることなく判断できる。

【００４５】

１００５では、デジタル複写機１０２は、その転送したファイルが格納されているボックスに対応する、ボックスセキュリティ管理テーブル１０４（図４）の情報をポリシィ管理サーバ１０５に送出する。これにより、ポリシィ管理サーバ１０５が管理しているポリシィ管理テーブル１０７（図７）の「転送」「変更」「削除」「カラー印刷」「白黒印刷」「ＩＰアドレス」「ボックスＩＤ」「有効／無効」のそれぞれの項目の値が設定される（１０１０）。即ち、ポリシィ管理サーバ１０５は、そのファイルのファイルＩＤを決定し、デジタル複写機１０２から送られてきたボックスのボックスセキュリティ管理テーブル１０４（図４）の内容を、そのファイルに対応するポリシィ管理テーブル１０７（図７）に反映させる。

【００４６】

図１１は、本実施の形態に係るデジタル複写機１０２からポリシィ管理サーバ１０５に登録した内容を記憶している登録履歴テーブルを説明する図である。この登録履歴テーブルは、ドキュメントサーバ１０３で管理されている。

【００４７】
ここでは、指定されたボックス内のデータに対応するファイル名と、そのファイルを特定するファイルＩＤ、そのファイルが格納されているボックスを特定するボックスＩＤ，そしてこのファイル情報を送信する送信先であるポリシィ管理サーバ１０５のＩＰアドレスが設けられている。
【００４８】
１００６でデジタル複写機１０２は、ポリシィ管理サーバ１０５から送られてきたファイルＩＤをドキュメントサーバ１０３に転送する。これによりドキュメントサーバ１０３は、１０１１で、図１１に示す登録履歴テーブルを更新し、その指定されたファイルのセキュリティ情報をデジタル複写機１０２に送出する。
【００４９】
これにより１００７でデジタル複写機１０２は、前述の１００２で指定したファイルをドキュメントサーバ１０３からを受け取る。次に１００８で、デジタル複写機１０２は、１００２で取得したＩＰアドレスに基づいて、宛先であるパーソナルコンピュータ１０６にそのファイルを送信する。
【００５０】
なお、１００５、１０１０、１００６、１０１１を経て１００７で送信されるファイルには、ポリシィ管理サーバ１０５バで生成され、デジタル複写機１０２へ通知されたファイルＩＤが属性情報として付加されている。更に、送信されるファイルの属性情報として、ポリシィ管理サーバ１０５のＩＰアドレスも付加される。このように、ファイルに対してポリシィ管理サーバ１０５で生成したファイルＩＤとポリシィ管理サーバ１０５のＩＰアドレスの情報を属性情報として付加することを、ファイルに対して「ポリシィを付与する」という。
【００５１】
ポリシィを付与されたファイルを受信したパーソナルコンピュータ１０６は、当該ファイルに対する操作（アプリケーションでファイルを開く、など）を実行する場合、以下のような手順を実行する。すなわち、パーソナルコンピュータ１０６は、ポリシィが付与されたファイルの属性情報を参照し、ポリシィ管理サーバ１０５のＩＰアドレスとファイルＩＤとを取得する。そして、当該ＩＰアドレスに対して、ファイルＩＤと、パーソナルコンピュータ１０６のＩＰアドレスとを送信する。ポリシィ管理サーバ１０５は受信したファイルＩＤを元に図７のポリシィ管理テーブルを参照してパーソナルコンピュータ１０６のＩＰアドレスが図７のＩＰアドレス７０７に含まれていることを確認する。そして、当該ファイルＩＤに対して定義されている各種操作権限（転送、変更、消去、、など）のＯＫ／ＮＧの情報をパーソナルコンピュータ１０６に対して返送する。なお、パーソナルコンピュータ１０６のＩＰアドレスが図７の当該ファイルＩＤに対するＩＰアドレス７０７の欄にない場合、ポリシィ管理サーバ１０５はパーソナルコンピュータ１０６に対して当該ファイルに対する操作権限がない旨を通知する。
【００５２】
ポリシィ管理サーバ１０５から操作権限に関する情報を受信したパーソナルコンピュータ１０６は、受信した操作権限情報に従って、ファイルに対する各種操作のＯＫ／ＮＧを制御する。
【００５３】
このようにして、ドキュメントサーバ１０３内でアクセス権が管理されていたファイルがドキュメントサーバ１０３の外部へ送信された場合においても、ポリシィ管理サーバ１０５を用いることによって、ドキュメントサーバ内と同様のアクセス権管理を実現することが可能になる。
【００５４】
図１２は、本実施の形態に係るデジタル複写機１０２のボックスのセキュリティ管理情報を変更する際の処理シーケンスを説明する図である。
【００５５】

１２０１では、前述の図９の９０１と同様に、ユーザ１０１が操作部２１３の認証画面（図８）を操作してデジタル複写機１０２にログインする。ここでユーザ１０１が、システム管理者としての権限を有する場合のみ１２０２以降の操作が可能となる。１２０２では、デジタル複写機１０２はドキュメントサーバ１０３からボックスセキュリティ管理テーブル１０４（図４）の情報を取得する。次に１２０３において、デジタル複写機１０２のユーザが、ボックスセキュリティ管理情報を変更するように指示する。ここでは例えば、図４でボックスＩＤが「００２」の場合、「カラー印刷」と「白黒印刷」が共に「ＯＫ」に設定されているが、これら設定を「ＮＧ」に変更するように指示されるたものとする。

【００５６】

１２０４において、ドキュメントサーバ１０３は、その変更が指示されたボックスセキュリティ管理情報をボックスセキュリティ管理テーブル１０４に反映する。次に１２０５において、ドキュメントサーバ１０３内部に保持しているポリシィ管理サーバ１０５への登録履歴テーブル（図１１）を検索し、１２０３でボックスセキュリティ管理情報が変更されたボックスに対応する、登録済みのファイルＩＤを特定する。

【００５７】

次に１２０６において、ドキュメントサーバ１０３からポリシィ管理サーバ１０５に対して、１２０５で特定したファイルＩＤ及びその変更したボックスセキュリティ管理情報を通知する。これにより１２０７で、ポリシィ管理サーバ１０５はドキュメントサーバ１０３から通知された内容に従って、ポリシィサーバ１０５内部のポリシィ管理テーブル１０７（図７）を変更する。尚、この実施の形態では、変更したボックスセキュリティ管理情報に応じて、「カラー印刷」と「白黒印刷」がともに「ＮＧ」に設定される。

【００５８】

これにより、ドキュメントサーバ１０３におけるボックスセキュリティ管理テーブル１０４の変更がポリシィ管理サーバ１０５にも反映される。よって、ドキュメントサーバ１０３から外部へ送信したファイルに対してもボックスセキュリティ管理テーブル１０４で変更したセキュリティ管理情報と同じ内容でアクセス権の管理を行うことが出来る。

【００５９】

以上説明したように本実施の形態によれば、デジタル複写機の特定記憶領域（ＢＯＸ）のデータを特定のセキュリティポリシィで管理し、ボックスのデータのセキュリティを統一したセキュリティポリシィで、簡便かつ確実に管理することができる。

【００６０】

またデジタル複写機のボックスから外部機器にファイルデータを送出する場合に、その送出するデータファイルの単位でセキュリティの管理や設定を行うことができる。これにより、デジタル複写機から外部機器へ送信したファイルデータのセキュリティ管理を確実に行うことができる。

【００６１】

またデジタル複写機の特定記憶領域（ＢＯＸ）のセキュリティポリシィを変更した場合に、対応するポリシィサーバ側の情報も同様に変更することができる。これにより、デジタル複写機で管理しているセキュリティポリシィが変更されると、既に外部機器に転送済みのファイルデータであっても、そのセキュリティポリシィの運用に反映させることができる。

【００６２】

（他の実施形態）

以上、本発明の実施形態について詳述したが、本発明は、複数の機器から構成されるシステムに適用しても良いし、また一つの機器からなる装置に適用しても良い。

【００６３】

なお、本発明は、前述した実施形態の機能を実現するソフトウェアのプログラムを、システム或いは装置に直接或いは遠隔から供給し、そのシステム或いは装置のコンピュータが該供給されたプログラムを読み出して実行することによっても達成され得る。その場合

、プログラムの機能を有していれば、形態は、プログラムである必要はない。

【００６４】

従って、本発明の機能処理をコンピュータで実現するために、該コンピュータにインストールされるプログラムコード自体も本発明を実現するものである。つまり、本発明のクレームでは、本発明の機能処理を実現するためのコンピュータプログラム自体も含まれる。その場合、プログラムの機能を有していれば、オブジェクトコード、インタプリタにより実行されるプログラム、ＯＳに供給するスクリプトデータ等、プログラムの形態を問わない。

【００６５】

プログラムを供給するための記録媒体としては、様々なものが使用できる。例えば、フロッピー（登録商標）ディスク、ハードディスク、光ディスク、光磁気ディスク、ＭＯ、ＣＤ－ＲＯＭ、ＣＤ－Ｒ、ＣＤ－ＲＷ、磁気テープ、不揮発性のメモリカード、ＲＯＭ、ＤＶＤ（ＤＶＤ－ＲＯＭ，ＤＶＤ－Ｒ）などである。

【００６６】

その他、プログラムの供給方法としては、クライアントコンピュータのブラウザを用いてインターネットのホームページに接続し、該ホームページからハードディスク等の記録媒体にダウンロードすることによっても供給できる。その場合、ダウンロードされるのは、本発明のコンピュータプログラムそのもの、もしくは圧縮され自動インストール機能を含むファイルであってもよい。また、本発明のプログラムを構成するプログラムコードを複数のファイルに分割し、それぞれのファイルを異なるホームページからダウンロードすることによっても実現可能である。つまり、本発明の機能処理をコンピュータで実現するためのプログラムファイルを複数のユーザに対してダウンロードさせるＷＷＷサーバも、本発明のクレームに含まれるものである。

【００６７】

また、本発明のプログラムを暗号化してＣＤ－ＲＯＭ等の記憶媒体に格納してユーザに配布する形態としても良い。その場合、所定の条件をクリアしたユーザに対し、インターネットを介してホームページから暗号化を解く鍵情報をダウンロードさせ、その鍵情報を使用することにより暗号化されたプログラムが実行可能な形式でコンピュータにインストールされるようにする。

【００６８】

また、コンピュータが、読み出したプログラムを実行することによって、前述した実施形態の機能が実現される形態以外の形態でも実現可能である。例えば、そのプログラムの指示に基づき、コンピュータ上で稼動しているＯＳなどが、実際の処理の一部または全部を行ない、その処理によっても前述した実施形態の機能が実現され得る。

【００６９】

更に、記録媒体から読み出されたプログラムが、コンピュータに挿入された機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに書き込まれるようにしてもよい。この場合、その後で、そのプログラムの指示に基づき、その機能拡張ボードや機能拡張ユニットに備わるＣＰＵなどが実際の処理の一部または全部を行ない、その処理によって前述した実施形態の機能が実現される。

【図面の簡単な説明】

【００７０】

【図１】本発明の実施の形態に係るデジタル複写機とサーバとを含むシステムの概略構成を示す図である。

【図２】本実施の形態に係るデジタル複写機の構成を説明するブロック図である。

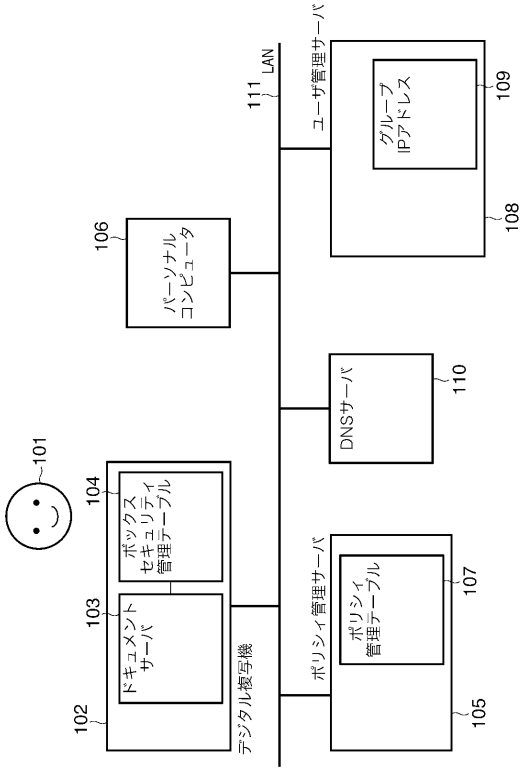
【図３】本実施の形態に係るデジタル複写機において、画像データを格納するボックスを選択する際に操作部に表示されるボックス選択画面の一例を示す図である。

【図４】本実施の形態に係るボックスセキュリティ管理テーブルの一例を示す図である。

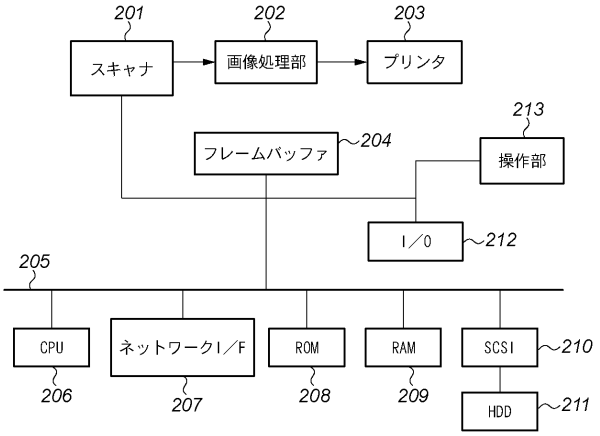
【図５】本実施の形態に係るユーザ管理サーバのグループＩＰアドレステーブルの構成例を示す図である。

【図６】本実施の形態に係るデジタル複写機の操作部の表示部に表示されたファイル転送を指示する画面の一例を示す図である。
【図７】本実施の形態に係るポリシィ管理テーブルの一例を示す図である。
【図８】本実施の形態に係るデジタル複写機の操作部の表示部に表示された認証画面の一例を示す図である。
【図９】本実施の形態に係るデジタル複写機のスキャナで読み取った原稿データを、ドキュメントサーバのボックスに格納するまでの一連の動作を説明する図である。
【図１０】本実施の形態に係るドキュメントサーバのファイルを外部機器に送出する一連の動作を説明する図である。
【図１１】本実施の形態に係るデジタル複写機からポリシィ管理サーバに登録した内容を記憶している登録履歴テーブルを説明する図である。
【図１２】本実施の形態に係るデジタル複写機のボックスセキュリティ管理情報を変更する際の処理シーケンスを説明する図である。

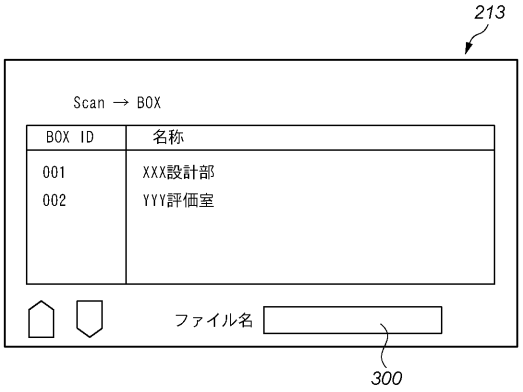
【図１】



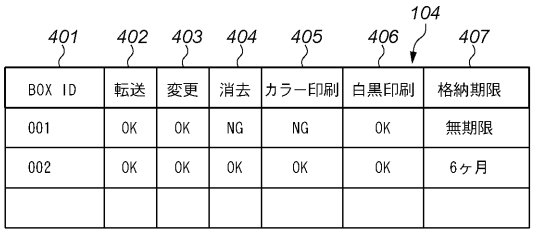
【図２】



【図３】

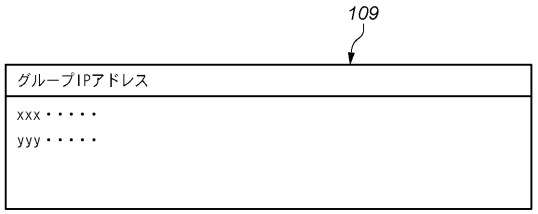


【図４】

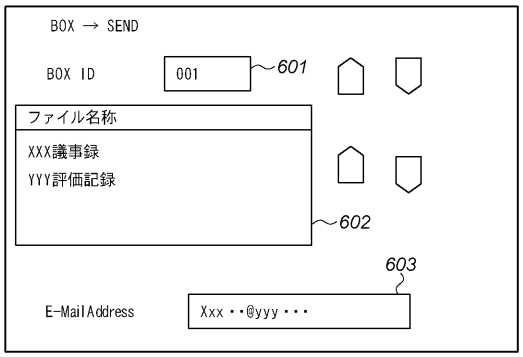


BOX ID	転送	変更	消去	カラー印刷	白黒印刷	格納期限
001	OK	OK	NG	NG	OK	無期限
002	OK	OK	OK	OK	OK	6ヶ月

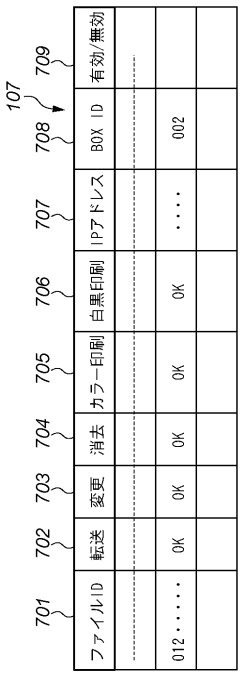
【図５】



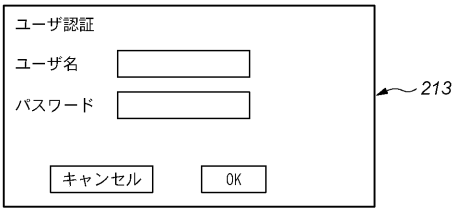
【図６】



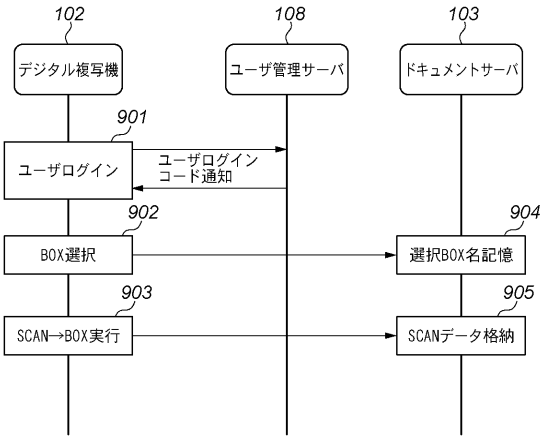
【図７】



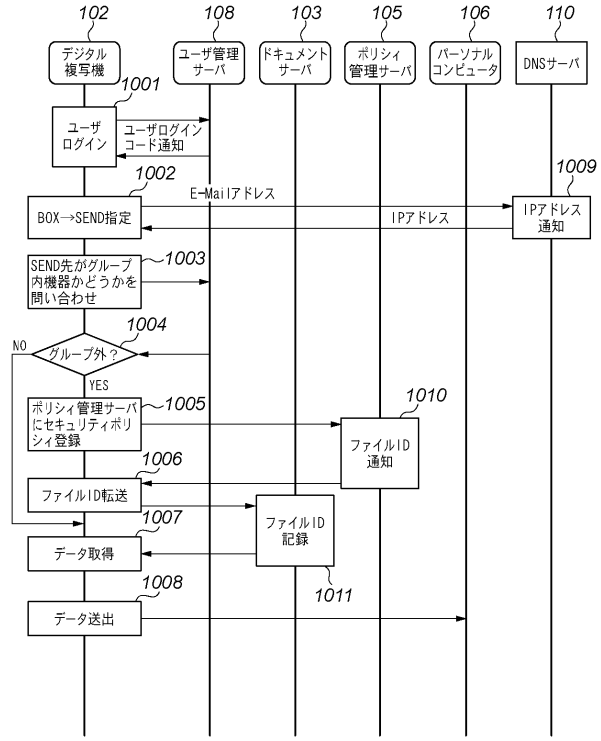
【図８】



【図９】



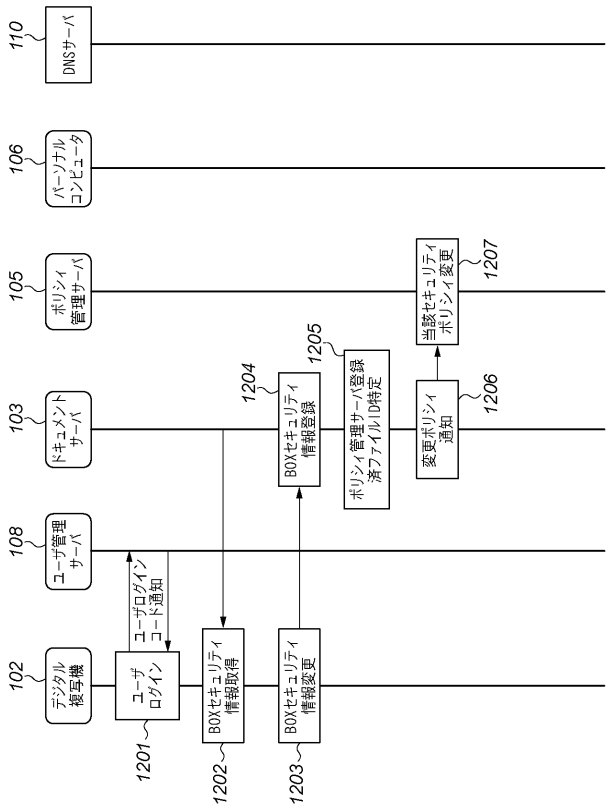
【図１０】



【図１１】

ファイル名	ファイルID	BOX ID	ポリシィ管理サーバIPアドレス
----------	----------	----------	----------
評価報告_20051224	012・・・・・	002	・・・・

【図１２】



フロントページの続き

(72)発明者　村山　努
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　深田　慎一
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　高野　潤一
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　吉原　邦男
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 AA01　BA06　BB06　CA16
5B285 AA04　BA07　CA06　CB43　CB58　CB62　DA04
5C073 CD23
5C075 AB90　BA08　EE90