

(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2010-15542

(P2010-15542A)

(43) 公開日 平成22年1月21日(2010.1.21)

(51) Int.Cl.	F I	テーマコード (参考)
G 0 6 F 21/24 (2006.01)	G 0 6 F 12/14 5 6 0 B	3 E 0 3 8
G 0 6 F 12/00 (2006.01)	G 0 6 F 12/14 5 2 0 F	5 B 0 1 7
G 0 6 F 17/30 (2006.01)	G 0 6 F 12/14 5 2 0 A	5 B 0 7 5
G 0 7 C 9/00 (2006.01)	G 0 6 F 12/14 5 4 0 A	5 B 0 8 2
	G 0 6 F 12/00 5 3 7 A	
審査請求 未請求 請求項の数 18 O L (全 46 頁) 最終頁に続く		

(21) 出願番号 特願2009-93323 (P2009-93323)
 (22) 出願日 平成21年4月7日 (2009.4.7)
 (31) 優先権主張番号 特願2008-145265 (P2008-145265)
 (32) 優先日 平成20年6月3日 (2008.6.3)
 (33) 優先権主張国 日本国 (JP)

(特許庁注：以下のものは登録商標)

1. B l u e t o o t h

(71) 出願人 000005108
 株式会社日立製作所
 東京都千代田区丸の内一丁目6番6号
 (74) 代理人 110000176
 一色国際特許業務法人
 (72) 発明者 橋本 宏美
 神奈川県横浜市麻生区王禅寺1099番地
 株式会社日立製作所システム開発研究所
 内
 (72) 発明者 荒井 正人
 神奈川県横浜市麻生区王禅寺1099番地
 株式会社日立製作所システム開発研究所
 内

最終頁に続く

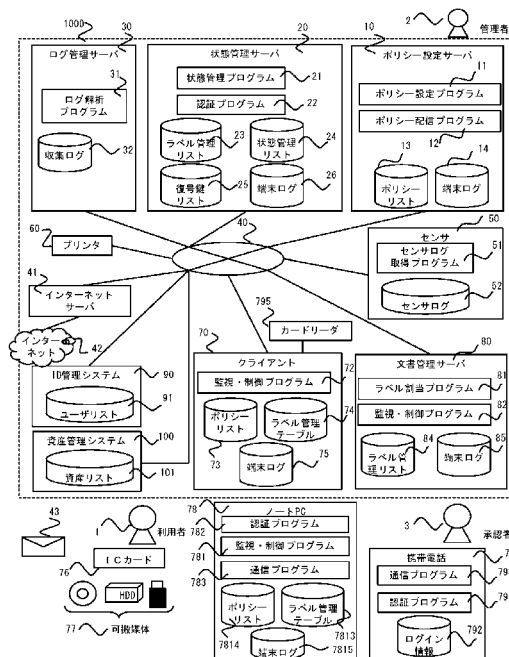
(54) 【発明の名称】 ファイル管理システム

(57) 【要約】

【課題】情報を格納する記憶媒体や人の所在の変化を特定し、漏洩につながる操作を未然に防止する。

【解決手段】上記目的を達成するために、情報のカテゴリとレベルの組合せをラベルとして、ラベルごとに情報の共有範囲を越える可能性が高い操作を実行する条件をポリシーリストとして定義し、ファイルにラベルを割り当てる。さらに、利用者がICカードをセンサにかざして入退室を行うことにより、利用者の所在情報を取得する。これにより、利用者がファイルを操作した場合に、利用者の属性情報や所在情報、ファイルの格納媒体などがポリシーリストに適合していない場合には操作を防止することにより、情報漏洩につながる操作を未然防止できる。さらに、ラベル割り当ておよびファイルの組織外持ち出し時の承認操作ごとに、承認結果を情報識別のためのDBに反映させることにより、承認者や管理者が登録しなくても情報識別精度の向上を図ることができる。

【選択図】 図1



【特許請求の範囲】**【請求項 1】**

ファイルにラベルを割り当て、情報漏洩につながる操作を制限するファイル管理システムにおいて、

少なくともポリシーを設定するポリシー設定手段と、

前記ポリシーを監視・制御手段を備えるクライアントに配信するポリシー配信手段と、

利用者の通過時に利用者を識別するセンサと、

前記センサから取得した情報を一元管理して利用者の所在を特定する状態管理手段と、

ファイルにラベルを割り当てることにより前記ポリシーを対応付けするラベル割当手段と、を備え、

前記監視・制御手段は、利用者のファイル操作時にファイルに割り当てたラベルを特定し、利用者の所在および利用者の属性およびファイルの格納場所を元にラベルとポリシーとを照合し、操作の実行を許可する、

ことを特徴とするファイル管理システム。

10

【請求項 2】

請求項 1 に記載のファイル管理システムにおいて、

前記ポリシーには、情報のカテゴリとレベルの組合せをラベルとし、ラベル単位で操作ごとの実行条件と共有先とを設定することを特徴とするファイル管理システム。

【請求項 3】

請求項 2 に記載のポリシーにおいて、

20

前記ポリシーには、少なくともファイルの利用者と、格納場所と、利用場所と、を前記実行条件として指定することを特徴とするファイル管理システム。

【請求項 4】

請求項 1 に記載のファイル管理システムにおいて、

前記ポリシー設定手段は、

前記ポリシーを設定するときに、操作を実行するための条件一覧を表形式で表示し、設定者が指定したい条件のみを押下させることにより条件を設定することを特徴とするファイル管理システム。

【請求項 5】

請求項 1 に記載のファイル管理システムにおいて、

30

前記ラベル割当手段は、

利用者がファイルに割り当てたラベルに設定されたポリシーをファイルに適用することを特徴とするファイル管理システム。

【請求項 6】

請求項 5 に記載のファイル管理システムにおいて、

前記ラベル割り当て手段は、

利用者がファイルにラベルを割り当てるときに、前記利用者が操作を実行できないラベルを非表示とすることを特徴とするファイル管理システム。

【請求項 7】

請求項 5 に記載のファイル管理システムにおいて、

40

前記ラベル割り当て手段は、

承認者が利用者の割り当てたラベルを承認するときに、類似するラベルを表示することにより、ラベルが適切かどうかを判断しやすくすることを特徴とするファイル管理システム。

【請求項 8】

請求項 1 に記載のファイル管理システムにおいて、

前記クライアントの前記監視・制御手段は、

ポリシーに一意に特定可能な共有先の条件を指定しておき、条件を満たす場合に操作を実行させることで、情報漏洩あるいは過失や故意のファイル転送を防止することを特徴とするファイル管理システム。

50

【請求項 9】

請求項 1 に記載のファイル管理システムにおいて、
前記クライアントの前記監視・制御手段は、
ラベルが未設定のファイルを社外秘扱いとするポリシーを設定し、ラベルを割り当てていないファイルの持ち出しを制御することを特徴とするファイル管理システム。

【請求項 10】

請求項 9 に記載のファイル管理システムにおいて、
前記クライアントの前記監視・制御手段は、
ポリシー配信手段ならびに状態管理手段とネットワーク通信できない場合には、ラベルが割り当てられたファイルに対してもラベル未設定のポリシーを適用することを特徴とするファイル管理システム。

10

【請求項 11】

請求項 1 に記載のファイル管理システムにおいて、
前記クライアントの前記監視・制御手段は、
ファイル操作を行う位置情報を操作の実行条件とし、利用者の入退室情報と連携することにより、適切でない利用環境からのファイル操作を制御することを特徴とするファイル管理システム。

【請求項 12】

請求項 11 に記載のファイル管理システムにおいて、
前記クライアントの前記監視・制御手段は、
利用者がファイルを持ち出す場合に、承認者から承認を得た後に暗号化する状態管理手段と、前記利用者の位置情報を計測し、状態管理手段と通信可能な通信手段を備え、状態管理手段と通信して位置情報が適切であった場合には復号条件を取得し、ファイルを格納した可搬媒体と通信して復号条件を送信する携帯電話と、復号条件を用いて持ち出したファイルでも特定の利用環境で操作可能とすることを特徴とするファイル管理システム。

20

【請求項 13】

請求項 11 に記載のファイル管理システムにおいて、
前記状態管理手段は、
ファイルを持ち出す前に持ち出し期限を設定させ、情報を削除するまで持ち出し期限を保持し、持ち出し期限を過ぎた情報を検知することを特徴とするファイル管理システム。

30

【請求項 14】

請求項 1 に記載のファイル管理システムにおいて、
前記クライアントの前記監視・制御手段は、
ラベルが未設定のファイルを職制上同じ役職あるいは上位の役職宛であれば共有するポリシーを設定し、ラベルを割り当てていないファイルの持ち出しを制御することを特徴とするファイル管理システム。

【請求項 15】

情報の種類を示すカテゴリと機密レベルの組合せデータであるラベルをファイルに割り当て、情報漏洩につながる操作を制限するファイル管理システムであって、

オブジェクトの属性情報および取り扱い情報を格納するオブジェクト登録データベースを記憶する記憶手段と、

ラベルの申請受付時ないしファイルの持出し申請受付時において、申請を受け付けたファイルにおける利用禁止オブジェクトの有無を、前記オブジェクト登録データベースにおける前記取り扱い情報に基づき特定するファイル識別手段と、

前記ラベルの申請ないしファイルの持出し申請に対する承認結果を他端末ないし入力手段から得て、前記オブジェクト登録データベースにおける該当オブジェクトに関する取り扱い情報を更新する DB 管理手段と、

を備えることを特徴とするファイル管理システム。

40

【請求項 16】

請求項 15 に記載のファイル管理システムにおいて、

50

前記DB管理手段は、承認結果を受信したときに前記オブジェクト登録データベースを更新することを特徴とするファイル管理システム。

【請求項17】

請求項15に記載のファイル管理システムにおいて、

前記オブジェクト登録データベースは、ラベルごとにファイルのオブジェクトを登録したデータベースと、ファイルを持出した履歴のある相手先ごとにオブジェクトを登録したデータベースと、ファイルおよびラベルを問わないオブジェクトを登録したデータベースとを含む、ことを特徴とするファイル管理システム。

【請求項18】

請求項15に記載のファイル管理システムにおいて、

前記ファイル識別手段は、前記申請を受け付けたファイルについて、ページ構成と該当ページにおけるテキストの位置とオブジェクトの位置とを特定し、ここで前記ファイルについて特定した事項に関して類似する他ファイルを、前記オブジェクト登録データベースの属性情報に基づき特定し、前記ファイルと他ファイルとの差分を取得して、前記取得した差分において前記オブジェクト登録データベースに登録されたオブジェクトの有無を検出し出力手段ないし他端末に出力する、ことを特徴とするファイル管理システム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報漏洩の未然防止と情報の活用を両立するファイル管理システムに関するものである。

【背景技術】

【0002】

近年、情報の電子化は進む一方であり、個人情報や技術情報、営業情報など様々な情報が組織内で電子化され、組織内あるいは社外の取引先など様々な範囲で活用されている。しかし、その一方で情報の漏洩や紛失も多発しており、組織にとって情報漏洩防止は非常に関心が高く、早急に取り組むべき項目である。

【0003】

情報漏洩を防止する製品も様々なものが提供されているが、情報漏洩事故は未だなくならず、一度漏洩が発生すると、たとえ従業員の過失であろうと組織に及ぶ被害は多大であり、事故対策費用やその後の予防対策費用までかかってしまう。

【0004】

情報は利用目的によって共有範囲が異なるため、情報漏洩を防止するためには、情報によって異なる共有範囲を越えないよう制限すればよい。しかしながら、以下の要因により共有範囲を越えて情報の漏洩につながる可能性のある経路が多様化している。

【0005】

(1) 情報の種類の多様化

組織で扱う情報は多岐に渡る。文書、設計図、個人情報、従業員情報、製品の流通履歴を示すものまで、組織が行うサービスや組織が効率よく活動を推進するために、幅広い情報が扱われている。これらの情報は利用目的によって共有範囲が異なることから、情報の取り扱い側からすると同じ操作でも、情報によっては共有範囲を越える行為になる可能性がある。

【0006】

(2) 情報を格納する媒体の多様化、小型化

近年、情報を格納する媒体の小型化、多様化が進んでいる。従来の情報の格納庫としては固定されたデスクトップPCに備え付けられていたHDDが主であったが、現在は情報を容易に持ち出し可能なUSBメモリやCD-Rなどの可搬媒体が容易に入手可能である。また、可搬媒体は小型であることから、勝手な持ち出しなどを確認することが困難となった。

【0007】

10

20

30

40

50

(3) 雇用形態やワークスタイルの多様化

組織における雇用形態やワークスタイルの変化も情報の共有範囲を越える原因となる可能性がある。組織内には、社員だけではなく、契約社員などが勤務する場合があります、このときに本来従業員のみ参照すべき情報を見られてしまう可能性がある。また、在宅勤務制度などの採用により、今後組織内だけではなく、自宅などでも作業ができるようになる可能性がある。組織にとって機密性の高い情報は社外での閲覧は防止すべきであるが、組織側で社員の属性や社員の所在の変化によって共有範囲を越える可能性がある行為を防止することは困難である。

【0008】

上記述べたような多様な経路で発生する可能性がある情報漏洩を防止するためには、情報の識別、情報の取り扱いポリシーの設定、ポリシーに基づくコントロール、コントロールの記録・監査、を行うことが必要である。

【0009】

例えば情報の識別に関しては、社外に文書を持出す場合には、持出す文書が何であるかを上長が見て確認することが考えられる。特許文献1では、承認を得ないと文書を登録できない文書管理サーバにおいて、その文書に機密情報、個人情報または誤記が含まれていないかどうかを基準に従ってチェックし、機密情報や個人情報が含まれている場合には承認画面に表示することにより、承認者の情報の識別作業を支援する技術が示されている。

【0010】

また、情報の取り扱いポリシーの設定に関しては、例えば可搬媒体を経由した機密情報の漏洩を防止するために、可搬媒体を一律持ち出し禁止にするなどの厳しいルールを制定することが考えられる。

【0011】

また、ポリシーに基づくコントロールに関しては、非特許文献1によるロールベースアクセス制御技術がある。これは情報の利用者に対して直接操作の実行許可を与えるのではなく、ロールに操作の実行許可を与え、利用者とロールとの対応付けを行うことで、情報ごとに「Read」や「Write」の操作を行う利用者を制限する技術である。

【先行技術文献】

【特許文献】

【0012】

【特許文献1】特開2007-299093号公報

【非特許文献】

【0013】

【非特許文献1】David Ferraiolo他、「Role Based Access Control」、15th National Computer Security Conference、1992.

【発明の概要】

【発明が解決しようとする課題】

【0014】

しかしながら、従来技術を用いて情報漏洩を防止しようとする場合、以下の問題がある。

情報の識別に関して、特許文献1では予め設定した機密情報を特定するためのキーワードと申請した情報のテキストとのマッチングをとっているが、組織で取り扱う情報は様々であるため、情報に合わせた質の良いキーワードを事前に設定するのは困難である。さらに、キーワードを更新しない限り検出精度は変わらないため、本来検出すべきキーワードに漏れが生じてしまうことや、不要なキーワードがいつまでも検出されてしまうことが考えられる。

【0015】

情報の取り扱いポリシーとコントロールに関しては、まず、可搬媒体を一律持ち出し禁止にするような極端な対策を行うと、営業などの社外で業務を行うことが多い社員の負担

10

20

30

40

50

が大きくなるなど業務に支障がでることが予想される。

【0016】

また、非特許文献1についても、前述したように情報の漏洩経路は幅広いため、利用者とロールとの対応付けだけで情報漏洩を防止することは困難である。例えば、非特許文献1の技術では、組織内では閲覧を許可させ、組織外からは閲覧させたくないファイルでも、操作を許可するロールに割り当てられた利用者であれば、利用者の所在の変化によらず操作を実行できてしまうため、組織外でファイルを閲覧し、第三者にファイルの中身を見られてしまう可能性がある。組織の情報を管理する場合には、情報の利用環境や記憶媒体の動的な変化に合わせて漏洩を未然に防止することが必要である。

【0017】

さらに、上記従来技術では、情報によって異なる共有範囲について、動的に変化する情報の格納先や利用者の状態・状況から、リアルタイムで共有範囲を越えないように操作を制御するようなポリシーを情報一つ一つに設定することは手間がかかる。

【課題を解決するための手段】

【0018】

本発明では、情報の活用を阻害することなく、情報の格納先や利用者の状態・状況が動的に変化しても漏洩につながる操作を未然に防止するファイル管理システムを提供する。

【0019】

すなわち、本発明は、組織の管理下に散在するファイルなどの情報に対して、情報の価値に応じて共有範囲を設定し、共有範囲をこえて情報漏洩につながる可能性の高い操作を防止するファイル管理システムを提供する。

【0020】

本発明に係るファイル管理方法は、情報の種類を示すカテゴリと機密レベルの組合せをラベルとして設定し、ラベル単位で情報漏洩につながる可能性の高い操作ごとの実行条件を設定し、さらに予めわかっている共有先も設定したポリシーリストを備え、ファイルに直接ポリシーを割り当てるのではなく、ファイルにラベルを割り当てることによってファイルの共有範囲を設定する。

【0021】

ラベルには操作ごとに実行条件を設定しているため、ラベルを割り当てたファイルに対してきめ細かい設定および制御を行うことができる。また、実行条件を設定する操作は情報漏洩につながる可能性の高い操作を対象としているため、「Read」や「Write」に留まらず幅広い範囲の操作の実行条件を一元管理することができる。さらに、実行条件として、例えば利用者の役職などの属性、および利用環境および情報を格納する媒体などを指定することにより、従来技術では成しえなかった動的変化による権限設定を行うことができる。

【0022】

上記ポリシーのファイルへの割り当てについては、利用者が情報のカテゴリおよび機密レベルを見て該当するラベルを選択するだけで、ファイルとラベルとをラベル付けし、ファイルにポリシーを適用するよう設定することができる。

【0023】

上記ラベルを設定したファイルの利用環境は、環境を構築および管理する管理者と、承認者と、一般ユーザである利用者とはからなり、管理者は予め各ラベルに対するアクセス権をポリシーとして設定し、利用者に割り当てられたクライアントにポリシーを配布するようにする。

【0024】

ファイルを取り扱う利用者は、ファイルにラベルを割り当てることで、配布されたポリシーに設定されたコントロールが適用される。なお、ファイルにラベルを割り当てる場合、まずファイルの所有者が情報のカテゴリおよび機密レベルを元にラベルを設定し、その後承認者が、利用者が割り当てたラベルが適切かどうかを判断し、ラベルを変更または承認することで、情報にラベルが割り当てられる。これにより、最初にラベル割り当てを行

10

20

30

40

50

う利用者が、過失または故意により適切でないラベルを付与したとしても、承認者が確認することにより、信頼性をもたせることができる。

【0025】

なお、ラベルの割り当てられていないファイルについては、一律社外秘情報とみなし、社外へのメール送信や可搬媒体の持ち出しなどの操作を一切禁止する。これにより、ラベルを割り当てていなくてもファイルを社外に持ち出す操作を防止することができる。

【0026】

さらに、上記ファイル管理システムは、漏洩リスクを判断するために機密性の高いオブジェクト（記述や画像、ロゴなどの特徴）を登録したデータベースを備えており、あるファイルにラベルが付与され承認者に承認依頼がなされた場合、あるいはファイルの持出し時にラベルが割り当てられておらず承認者に承認依頼がなされた場合に、データベースとファイルとを照合し、申請されたファイルに機密性の高いオブジェクトが含まれるかを特定して承認画面に表示する。これにより、承認者は申請されたファイルの価値を迅速に把握することができる。さらに、上記ファイル管理システムは承認結果を元にデータベースを更新するため、承認者や管理者がデータベースを更新しなくても、漏洩リスクの未然防止に有効な本来登録されるべきオブジェクトの追加や本来不要なオブジェクトの削除などを行うことができる。

【0027】

さらに、上記ファイル管理システムは、利用者の操作をポリシーに基づいて制御する監視・制御プログラムを備えるクライアントおよび文書管理サーバと、登録されている利用者の移動を検出し、例えば利用者が現在社内のどのエリアにいるのかを把握することができるセンサを備えており、センサから得た利用者の所在情報とクライアントで行われる操作の情報からポリシーを参照して操作の実行許可／不許可と、実行許可した場合には、ラベルの継承を行う。これにより、ラベルを割り当てた情報がクライアントから別な媒体に移動した場合でもラベルを損なうことなく制御を行うことができる。あるいは利用者の所在が適切な場合にのみ操作を実行することができる。

【0028】

さらに、利用者は組織外にファイルを持ち出す場合に、承認者から承認を得た後に暗号化したファイルをノートPCに格納する。利用者が組織外にて暗号化したファイルを利用する場合には、携帯電話を用いて利用者の所在情報が適切であると確認できた場合にのみ復号鍵を携帯電話に送信する。利用者は携帯電話とノートPCを通信することによって復号鍵を受け渡し、組織外においても適切な場所でのみファイルを利用することができる。

【0029】

上記態様によって、以下のような効果を得ることが出来る。

- ・情報の取り扱い条件について、組織内外の利用環境、および社員の役職などの属性からきめ細かい条件を指定することができるため、共有範囲を越えて漏洩につながる操作を防止し、情報の活用と漏洩防止を両立できる。

- ・利用者は情報のレベルやカテゴリを選択するだけで、きめ細かいポリシーが設定できる。

- ・ポリシーを一元管理し、クライアントに配布するシステム構成のため、ポリシーの修正を行えば、各ファイルの設定を更新しなくてもクライアントに反映できる。

- ・ラベル割当をしていないファイルについてもポリシーを設定することにより、ラベル割当をしていないファイルであっても漏洩の可能性の高い操作を防止することができる。これにより、過失や故意を問わず情報の組織外持ち出しを防ぐことができる。

- ・識別に用いるデータベースを承認判断時に更新することにより、管理者が更新を行うことなく情報の識別精度を向上させることができる。

- ・例えば、情報漏洩の未然防止に備えて、情報システムおよびその周辺環境に散在するファイルの管理において、セキュリティ部門の管理者などによるファイル管理を支援するツールに使用できる。

【0030】

10

20

30

40

50

上述した本発明のファイル管理システムは、ファイルにラベルを割り当て、情報漏洩につながる操作を制限するシステムであり、少なくともポリシーを設定するポリシー設定手段と、前記ポリシーを監視・制御手段を備えるクライアントに配信するポリシー配信手段と、利用者の通過時に利用者を識別するセンサと、前記センサから取得した情報を一元管理して利用者の所在を特定する状態管理手段と、ファイルにラベルを割り当てることにより前記ポリシーを対応付けするラベル割当手段と、を備え、前記監視・制御手段は、利用者のファイル操作時にファイルに割り当てたラベルを特定し、利用者の所在および利用者の属性およびファイルの格納場所を元にラベルとポリシーとを照合し、操作の実行を許可する、ことを特徴とする。

【0031】

また、本発明のファイル管理システムは、情報の種類を示すカテゴリと機密レベルの組合せデータであるラベルをファイルに割り当て、情報漏洩につながる操作を制限するファイル管理システムであって、オブジェクトの属性情報および取り扱い情報を格納するオブジェクト登録データベースを記憶する記憶手段と、ラベルの申請受付時ないしファイルの持出し申請受付時において、申請を受け付けたファイルにおける利用禁止オブジェクトの有無を、前記オブジェクト登録データベースにおける前記取り扱い情報に基づき特定するファイル識別手段と、前記ラベルの申請ないしファイルの持出し申請に対する承認結果を他端末ないし入力手段から得て、前記オブジェクト登録データベースにおける該当オブジェクトに関する取り扱い情報を更新するDB管理手段と、を備えることを特徴とする。

【0032】

なお、前記ファイル管理システムにおいて、前記DB管理手段は、承認結果を受信したときに前記オブジェクト登録データベースを更新するとしてもよい。

【0033】

また、前記ファイル管理システムにおいて、前記オブジェクト登録データベースは、ラベルごとにファイルのオブジェクトを登録したデータベースと、ファイルを持出した履歴のある相手先ごとにオブジェクトを登録したデータベースと、ファイルおよびラベルを問わないオブジェクトを登録したデータベースとを含む、としてもよい。

【0034】

また、ファイル管理システムにおいて、前記ファイル識別手段は、前記申請を受け付けたファイルについて、ページ構成と該当ページにおけるテキストの位置とオブジェクトの位置とを特定し、ここで前記ファイルについて特定した事項に関して類似する他ファイルを、前記オブジェクト登録データベースの属性情報に基づき特定し、前記ファイルと他ファイルとの差分を取得して、前記取得した差分において前記オブジェクト登録データベースに登録されたオブジェクトの有無を検出し出力装置ないし他端末に出力する、としてもよい。

【発明の効果】

【0035】

本発明により、情報の活用を阻害することなく、情報漏洩につながる操作を未然に防止することが可能になる。

【図面の簡単な説明】

【0036】

【図1】第1実施例に係るファイル管理システムの構成図である。

【図2】クライアントのハードウェア構成を例示するブロック図である。

【図3】ポリシーリストのデータ構造を例示する図である。

【図4】ポリシーリストのデータ構造を例示する図である。

【図5】ポリシーリストの設定画面を例示する図である。

【図6】ポリシー配信処理の流れを例示する図である。

【図7】ラベル割り当て処理の流れを例示する図である。

【図8】ラベルの割り当て申請画面を例示する図である。

【図9】ラベル割り当ての承認画面を例示する図である。

10

20

30

40

50

【図 1 0】ラベルリストおよび状態管理リストのデータ構造を例示する図である。
【図 1 1】利用者の所在を特定する処理を例示する図である。
【図 1 2】監視・制御プログラムの動作を例示するフローチャートである。
【図 1 3】ファイルの持ち出し操作に係る処理を例示する図である。
【図 1 4】組織外におけるファイル操作に係る処理を例示する図である。
【図 1 5】ファイル持ち出し後の組織内での処理を例示する図である。
【図 1 6】持ち出し操作に係る申請および承認画面を例示する図である。
【図 1 7】第 2 実施例におけるラベル割り当て処理を例示する図である。
【図 1 8】第 2 実施例における監視・制御プログラムの動作を例示するフローチャートである。

10

【図 1 9】第 3 実施例に係るファイル管理システムの構成図である。
【図 2 0】第 3 実施例における取引先リストを例示する図である。
【図 2 1】第 3 実施例における承認管理 DB を例示する図である。
【図 2 2】第 3 実施例における照合用 DB を例示する図である。
【図 2 3】第 3 実施例における持ち出しルール DB を例示する図である。
【図 2 4】第 3 実施例におけるファイルの持ち出し申請画面を例示する図である。
【図 2 5】第 3 実施例におけるファイルの持ち出し承認画面を例示する図である。
【図 2 6】第 3 実施例におけるファイルの持ち出し申請操作に係る処理を例示する図である。

【図 2 7】第 3 実施例におけるファイルの持ち出し承認操作に係る処理を例示するフローチャートである。

20

【図 2 8】第 3 実施例におけるファイル識別プログラムの動作を例示するフローチャートである。

【図 2 9】第 3 実施例における DB 管理プログラムの動作を例示するフローチャートである。

【発明を実施するための形態】

【0037】

――実施例 1――

以下、図面を適宜参照しつつ、実施例について説明する。図 1 は第 1 実施例に係るファイル管理システムの構成図である。ファイル管理システム 1000 は、ポリシー設定サーバ 10、状態管理サーバ 20、ログ管理サーバ 30、インターネットサーバ 41、1 台以上のセンサ 50、1 台以上のプリンタ 60、1 台以上のクライアント 70、文書管理サーバ 80、ID 管理システム 90、資産管理システム 100、が有線あるいは無線でネットワーク 40 に接続された構成をとる。

30

【0038】

利用者 1 は例えば自身のユーザ ID が耐タンパ領域に格納された IC カード 76 を用いて組織への入退室を行う。なお、組織とは建屋あるいは執務室などの居室を分ける部分にセンサが設置されており、最も外側に配置されたセンサの内側を指す。利用者 1 はさらに、クライアント 70 あるいは可搬媒体 77 あるいはノート PC 78 を使って種々の作業を行う。利用者 1 は一意に特定可能なユーザ情報を耐タンパ領域に格納した携帯電話 79 を持ち、組織内外に携帯電話 79 を持ち歩く。また、クライアント 70 では、カードリーダー 795 を接続し、IC カード 76 を読み込ませてクライアント 70 と通信することにより、IC カードに記録された ID を読み込むこともできる。管理者 2 はポリシー設定サーバ 10 を使って種々の作業を行う。承認者 3 は文書管理サーバ 80 を使って種々の作業を行う。

40

【0039】

センサ 50 は組織の建屋や執務室を分ける入口などに設置してあり、例えば支店のよう、同じ組織で物理的な建屋が離れている場合にも、センサ 50 が設置してあれば、利用者 1 が IC カード 76 をかざすことにより、センサが IC カードの ID を読み取り、認証を行って入退室が可能である。

50

【0040】

インターネットサーバ41とは、ネットワーク40内あるいはインターネットでやりとりされる電子メール43の送受信を中継し、送受信した電子メールを保存する電子メールサーバあるいは、インターネット42とのWeb通信を中継するProxyサーバなどである。

【0041】

さらにクライアント70は、CD-R/DVD-RやUSBフラッシュメモリ、ポータブルHDD、マルチメディアコンテンツを格納するSDカードなどの可搬媒体77が接続可能であり、クライアント70は可搬媒体77とファイル交換をすることができる。

【0042】

ここで、クライアント70は利用者1ごとに割り当てられていることを原則とする。なお、クライアント70が2人以上の利用者に割り当てられていてもよく、その場合にはクライアント70が利用者を識別および認証することにより、どの利用者がクライアント70を利用したのかを区別できるようにすればよい。さらに、クライアント70で複数人が共通のアカウントを用いてクライアントを使用する場合、ID管理システム90でアカウント管理を行うことにより、誰がどのアカウントと紐付いているかを把握しておく。

【0043】

さらに図1を使って、ポリシー設定サーバ10、状態管理サーバ20、ログ管理サーバ30、センサ50、クライアント70、文書管理サーバ80、ノートPC78におけるソフトウェア構成を説明する。

【0044】

ポリシー設定サーバ10では、ファイルに適用するポリシーを格納したポリシーリスト13を設定するポリシー設定プログラム11と、ポリシー設定プログラム11で設定したポリシーリスト13をクライアント70に配信するポリシー配信プログラム12を備える。さらに、ポリシー設定プログラム11およびポリシー配信プログラム12では、作業したログを端末ログ14に格納する。ポリシー設定プログラム11は、管理者2が直接ポリシー設定サーバ10にアクセスするか、管理者用の端末からネットワーク40を介してアクセスしてもよい。

【0045】

状態管理サーバ20では、ラベル管理リスト23と状態管理リスト24、復号鍵リスト25、端末ログ26を備えており、ログ管理サーバ30のログ解析プログラム31から受信したセンサログと、ID管理システム90のユーザの属性情報を格納するユーザリスト91をつき合わせ、ユーザリスト91に登録したユーザの所在を状態管理リスト24に書き込む状態管理プログラム21が動作する。さらに状態管理プログラム21は、クライアント間をファイルが移動する場合に、ファイルの格納先情報を管理するラベル管理リスト23の更新も行う。また、状態管理サーバは、利用者1が持ち歩く携帯電話79の認証を行う認証プログラム22と、認証が成功した携帯電話に配信する復号鍵リスト25を備える。これにより、利用者が組織外にいる場合でも、本実施例で説明するファイルの制御を行うことが可能となる。

【0046】

ログ管理サーバ30では、クライアント70、文書管理サーバ80、ポリシー設定サーバ10でそれぞれ取得した端末ログと、センサ50で取得したセンサログ52を収集し、収集した端末ログを解析してログを整形して収集ログ32に格納し、収集ログのうちセンサから取得したセンサログを状態管理サーバ20に送信するログ解析プログラム31が動作する。

【0047】

クライアント70では、利用者1の操作を詳細に監視し、操作発生時には、対象となるファイルのラベル情報を格納したラベル管理テーブル74と、ポリシー設定サーバ10から受信したポリシーリスト73を参照し、ポリシーに従って操作を許可あるいは防止し、制御した結果をログとして端末ログ75に格納する監視・制御プログラム72が動作する

10

20

30

40

50

。

【0048】

文書管理サーバ80では、ファイルにラベルを割り当てるラベル割当プログラム81と、クライアント70に備えた監視・制御プログラム72と同じ機能を備える監視・制御プログラム82が動作する。ラベル割当プログラム81は、クライアント70で利用者1が申請したファイルのラベル情報を受け付け、承認者による承認あるいは変更要求を受け付け、ラベル管理リスト84を更新する。ラベル割当プログラム81で割り当てたファイルとラベルとの対応関係情報は、ラベル管理リスト84に格納する。文書管理サーバ80のラベル割当プログラム81および監視・制御プログラム82で実行した操作のログは端末ログ85に格納される。なお、文書管理サーバ80に格納したファイルは、組織内で審査済みのファイルとし、上書き禁止として取り扱いを行う。

10

【0049】

なお、本特許で述べるファイルとは、システムファイルなどではなく、組織内で生成あるいは外部から入手した、組織内で価値のある情報資産全てを対象とする。

【0050】

図2は、ファイル管理システム1000におけるクライアント70のハードウェア構成を示すブロック図である。クライアント70は、端末ログ75ならびにポリシーリスト73、ラベル管理テーブル74を保存する外部記憶媒体702、監視・制御プログラム72を実行するCPU701、メモリ703、入出力画面を表示する表示部704、入出力を制御する操作部705、可搬媒体77に格納されたデータなどを読み書きするための可搬媒体接続部706、RAM707、有線あるいは無線でネットワーク40と通信を行う通信部708、これらの各装置等を相互接続するバス709から構成される。

20

【0051】

また、文書管理サーバ80、ポリシー設定サーバ10、状態管理サーバ20、ログ管理サーバ30も、図2に示したクライアント70のブロック図と同様のハードウェア構成をとる。ただし、文書管理サーバ80、ポリシー設定サーバ10、状態管理サーバ20、ログ管理サーバ30に可搬媒体接続部706は必ずしもなくてよい。

【0052】

各装置では、CPUが外部記憶媒体702に格納されたプログラムを実行することにより、以下に説明する処理、機能が実現される。ただし、各実施形態の説明では、便宜上、各プログラムを実行主体としている。

30

【0053】

また、各プログラムは、あらかじめ、上記各装置の外部記憶媒体702やメモリ703に格納されていても良いし、必要なときに、可搬媒体接続部706や通信部708と、各装置が利用可能な媒体と、を介して、他の装置から導入されてもよい。媒体とは、たとえば、着脱可能な可搬媒体77、または通信媒体（すなわちネットワーク40またはネットワーク40を伝搬する搬送波やデジタル信号）を指す。

【0054】

図3にポリシーリスト13のデータ構造の一例を示す。ポリシーリスト13は、クライアント70、文書管理サーバ80、可搬媒体77、ノートPC78のいずれかに格納しているファイルに対して操作が発生した場合に操作を実行する条件を記録したものであり、ポリシー設定サーバ10上およびクライアント70上の記憶装置に格納したものである。

40

【0055】

ポリシーリスト13は0個以上のエントリから構成される表データであり、情報のカテゴリとレベルの組合せについて設定したラベル281、情報のカテゴリ282、情報の機密性の度合いを示すレベル283、制御対象とする操作284、284の操作を実行するための条件を示すアクセス主体285、ID管理システム90のユーザリスト91に登録されていないユーザあるいはインターネット42を介してアクセス可能なWebサイトなどにおいてファイルを共有可能な共有先286、からなる。

【0056】

50

以下、ポリシーリスト 13 の構成について詳細に説明する。

まず、ラベル 281 は、列 282 に示すカテゴリと、列 283 に示すレベルとの組合せで設定する。なお、ラベル名は列 281 に示すようにアルファベットでもよいし、ラベルが一意に特定できる名称であればその他の名称でもよい。

【0057】

ラベルをカテゴリとレベルの組合せで設定するのは、現在情報の種類は多様化しており、レベルやカテゴリによって共有範囲などの取り扱い規則が異なるためである。例えば、情報の共有範囲を大きく以下の 4 つに分類した場合、それぞれの取り扱い規則は異なるため、それぞれの共有範囲を越えないようなコントロールが必要である。

(1) 一般に公開可能なもの

組織内で審査済みのものや、外部から入手した公開情報など。

(2) 組織内だけで共有したいもの

ドラフト版や分類不能なものも含めて、大多数の情報が該当する。

(3) 組織内でもさらに共有範囲を制限したいもの

機密レベルや種類に応じて分類可能。

(4) 特定の組織（組織外）と共有したいもの

取引先や委託先ごとに分類可能。

【0058】

さらに、各クライアント 70 に格納しているファイルは、作成途中のドラフト版のものや、完成した文書なども混在する。これらのファイルについて、それぞれ異なる共有範囲を越えないようにするためには、ファイルを取り扱う人だけではなく、ファイルを格納する場所や利用場所を操作ごとに制限すべきである。ポリシーリスト 13 は、共有範囲の異なる単位をカテゴリとレベルからラベルとして設定し、さらに、ラベルごとに操作に対するアクセス主体および共有先を指定した上で、ラベルをファイルに割り当てることで、情報の種類にあわせたきめ細かいポリシーを適用することができる。

【0059】

なお、ラベル 281 は、ラベルが未設定のファイルに割り当てるポリシーとして、ラベルなし 2811 というラベルを設定し、操作に対する条件の設定を行う。本実施例では、ファイルに対して利用者 1 がラベルを割り当てると、例えばクライアント 70 の監視・制御プログラム 72 がラベルに紐付くポリシーを適用するが、クライアントが格納するファイル全てについてラベルを割り当てるのは手間がかかる。さらに、ラベル付けされないファイルについて制御対象から外れ、漏洩してしまう可能性も考えられる。そこで、ラベルが割り当てられていないファイルについては、少なくとも社外秘として扱い、組織外に情報が持ち出されるような操作は制御すべきと考え、ラベルなしのポリシーも設定し、適用することとする。

【0060】

次にカテゴリ 282 は、組織の情報の種類に基づいて設定する値であり、例えば「人事情報」「財務情報」「技術情報」などの情報の種類を定義してもよいし、「取引先 A」などのように顧客情報としてもよい。これらの値は、管理者 2 がポリシー設定プログラム 11 を用いて追加あるいは修正可能である。

【0061】

レベル 283 は、情報の価値に基づいて設定する値であり、例えば「極秘」「秘」「公開」「未設定」を定義する。これらの定義は、ラベルの割り当てを行う利用者 1 およびラベルの承認を行う承認者 3 が設定しやすいような分類とする。

【0062】

操作 284 は、従来のアクセス制御技術でアクセス権を指定した操作である「閲覧」「編集」に加えて、情報の共有範囲を越えて漏洩につながる可能性の高い操作まで定義したものであり、例えば「閲覧」「編集（ファイルの削除、ファイル名の変更なども含む）」「コピー（電子、紙、スキャンなど）」「印刷」「ネットワーク送信（以下、NW送信とする）（メール、Webアップロードなど）」「持ち出し」などを定義する。

【0063】

アクセス主体285は、操作284を実行可能な条件を定義したものであり、具体的にはアクセス主体条件一覧301を元に設定する。アクセス主体285は、少なくとも0個以上の論理式から構成されるデータであり、アクセス主体条件一覧301から選択した条件を一意に識別可能な式を定義する。なお、論理式は、該操作を実行可能な条件、または許可しない条件を書く。さらに、論理式は記号「 $\wedge$ 」でAND演算子を示し、記号「 $\vee$ 」でOR演算子を示す。AND演算子で接続された条件式が情報の取り扱い条件を示す。

アクセス主体285の定義方法についてはアクセス主体条件一覧301のデータ構造を説明した後述べる。

【0064】

アクセス主体条件一覧301は、少なくとも1個以上のエントリから構成される表データであり、条件として設定する候補となるカテゴリ番号302、カテゴリ番号302について組織が選択し得る属性情報を示すカテゴリの概要303、カテゴリ303で組織が選択し得るデータ(304~308)、からなる。

カテゴリ303は、例えば「雇用区分」「役職」「組織名」など利用者の属性情報や、ファイルを取り扱う利用者の場所、ファイルを格納する媒体の種類、組織外で利用するための条件、などを定義する。

【0065】

カテゴリごとに設定するデータ(列304~列308)は、例えばアクセス主体条件一覧301のC1に記載した「雇用区分」では、「パート」「契約」「社員」など、組織で選択し得る属性情報を定義する。なお、より細かく定義したいカテゴリや属性情報があれば管理者2が追加してもよい。これらのデータに関して、利用者や資産の管理は、別途ユーザリスト91および資産リスト101を用いて行う。ユーザリスト91は、ID管理システム90で管理され、例えば「氏名」「雇用区分」「役職」などの属性情報を、利用者を一意に特定可能なユーザID単位で管理するものである。また、資産リスト101は、資産管理システム100で管理され、例えば「資産ID」や記憶媒体の種類を示す「種類」「所有部署」「媒体識別ID」などを資産単位で管理するものである。これらユーザリスト91および資産リスト101は、利用者および資産の追加に伴う登録、あるいは利用者の移動や退職、資産の所有部署の変更や滅却に伴う項目の削除について、ID管理システム90および資産管理システム100の一般的な機能を用いて行われることとする。

【0066】

さて、ポリシーリスト13におけるアクセス主体285の定義方法について説明する。「閲覧」操作を実行する条件2861では、「 $C1 = 3 \wedge C2 > 3 \wedge C3 = 3 \wedge C4 > 2$ 」を記述している。これらの式で左辺に記述する項目は、アクセス主体条件一覧301のカテゴリ番号302を示し、右辺に記述する項目は列304~列308に示したデータの番号を示す。この例では、「C1が示す雇用区分が3(すなわち社員)」、かつ「C2が示す役職が3より大きい役職(すなわち課長以上)」、かつ「C3が示す組織名が3(すなわち研究部門)」、かつ「C4が示す場所が2より大きい(すなわち執務室、サーバ室、実験室のいずれか)」という条件を全て満たす場合、閲覧操作を実行可能であることを示す。このように、情報のカテゴリとレベルの組合せで定義するラベルについて、共有範囲を越える可能性のある操作ごとにアクセス主体を設定しておくことにより、きめ細かい条件設定を行うことが可能となる。

【0067】

なお、アクセス主体285について、どのような条件でも操作を許可しないカテゴリについては何も記述しなければよい。例えば、「持ち出し」操作を実行する条件2864には何も記述していない。これは、どのような条件であってもファイルの持ち出しは許可しないことを意味する。

【0068】

さらに、制限が不要なカテゴリについても式に含めなければよい。例えば、「編集」操

10

20

30

40

50

作を実行する条件 2862 に「C5 > 3」を記述する。この場合は、C5 の条件を示す格納媒体の条件を満たせば、その他のカテゴリのデータが何であれ操作を許可することを意味する。

【0069】

一方、どのような条件でも操作を許可する場合には「*」を記述する。例えば、「NW 送信」操作を実行する条件 2863 は「*」と記述してあるため、どのような条件であっても NW 送信を実行できることを意味する。

【0070】

ポリシーリスト 13 における共有先 286 では、組織外における情報の共有先を指定する。主に操作 284 の NW 送信において、取引先の担当者などが決まっている場合や、ファイルを上ロードする Web サイトの URL がわかっている場合、予め担当者のメールアドレスや URL を登録しておくことによって、登録した担当者や URL には組織外であってもファイルを共有可能として設定できる。また、これらの情報を登録しておくことにより、メールアドレスの入力間違いによる誤送信や、送信するファイルを間違えて送信してしまうことを防止することが可能となる。共有先（列 286）として登録していない場合についても、承認者 3 に共有先情報と目的などを申請し、承認を得ることでこれらの操作を実行することが可能である。

【0071】

以上述べた構造のポリシーリスト 13 を備えることにより、従来技術のようなユーザの閲覧および編集だけを監視・制御するのではなく、漏洩につながる可能性の高い幅広い操作に対する実施条件を設定することができる。

【0072】

さらに、本ポリシーはポリシー設定サーバ 10 に格納したポリシーリスト 13 で一元管理し、管理者 2 がポリシー設定プログラム 11 を用いて予め設定する。管理者 2 は定期的な見直しの都度、あるいは利用者からの申請に応じてポリシーを変更してもよい。本実施形態では、ファイル 300 に対してラベル 281 を割り当てているため、一度ラベルをファイルに割り当てた後に、ラベルを定義するカテゴリやレベル、および各操作に対するアクセス主体の変更を行っても、既に割り当てたファイルには影響しない。また、ポリシーリスト 13 はポリシー配信プログラム 12 によってクライアント 70 にも配信され、クライアント 70 の監視・制御プログラム 72 で参照されるため、ファイルのコピーなどによりクライアントが変わった場合でも、ラベルがわかれば同じポリシーを適用することができる。より具体的なポリシーの設定例と実現可能な制御については図 4 で述べる。

【0073】

図 4 に、図 3 で説明したポリシーの具体的な例を示し、情報の種類ごとにきめ細かい制御ができることを示す。図 4 では、4 種類のラベルを定義した例として、ラベル「A」の定義を 4001、ラベル「B」の定義を 4002、ラベル「C」の定義を 4003、ラベル「なし」の定義を 4004 に示す。

【0074】

ラベル A 4001 は、レベルが極秘の人事情報に割り当てたラベルであり、組織内でもさらに共有範囲を制限したいものである。このような情報は、社外に持ち出す用途はなく、組織内でも公開期限になるまで共有を制限すべきである。そのため、ラベル A 4001 が割り当てられたファイルの制御として、持ち出しは許可せずに、閲覧操作から NW 送信までの操作を、課長以上の社員が執務室のデスクトップ PC でのみ実行できる条件を設定する。これにより、例えば、課長以上の社員がラベル A 4001 のファイルをデスクトップ PC から可搬媒体へコピーしようとしても、コピー操作ができる装置としてデスクトップ PC を設定しているため、条件を満たすことができず、実行できない。また、NW 送信についても、共有範囲が課長以上のため、課長が誤って部下にファイルを転送するような操作も防止することができる。万が一、部下がファイルを入手したとしても、閲覧条件が一致しないため、見られることはない。

【0075】

ラベル B 4 0 0 2 は、公開可能なカタログ情報に割り当てたラベルである。用途としては、社内での閲覧から社外の特定顧客への説明など持ち出す行為まで想定される。そのため、ラベル B 4 0 0 2 が割り当てられたファイルの制御として、閲覧および NW 送信は「＊（条件なしで可能）」とし、それ以外の操作の条件を設定する。例えば、既に公開されているため、上書きを禁止するために、「編集」操作を許可しないなどがある。一方、持ち出し操作は社員が R F I D 貼り付け紙以外の媒体を利用すれば、共有先を選ばずに組織外に持ち出すことができる。

【 0 0 7 6 】

ラベル C 4 0 0 3 は、レベルが秘の取引先 A に割り当てたラベルである。本情報は、組織内でも取引先 A と関係のあるユーザのみ、また、組織外では取引先 A の利用者のみと情報を共有すべきである。そのため、ラベル C 4 0 0 3 が割り当てられたファイルの制御として、社内では、研究または営業部門の契約社員以上の利用者が、執務室以上の場所で閲覧や編集操作を行うように定義する。また、NW 送信の共有先として、取引先 A の担当者のメールアドレスを登録し、持ち出し先として、取引先 A の東京オフィスを登録する。これにより、利用者が取引先 A に作成したファイルをメールなどで送信あるいは持ち出す場合は、登録したアドレスまたは宛先以外には承認がないと実行できない。また、承認を得ずに持ち出した場合、あるいは利用先として登録してある取引先 A の東京オフィス以外においても操作できない。なお、ファイルの持ち出し処理の詳細については図 1 3 から図 1 5 で説明する。

【 0 0 7 7 】

ラベル未設定 4 0 0 4 は、ラベルが割り当てられていないファイルに割り当てるラベルである。ラベルが未設定のファイルは、本来極秘で扱うべき情報から、公開する情報までが混在するため、社外秘と同じ共有範囲にすることや、最も狭い範囲となるよう共有範囲を設定し、制御すべきである。そのため、例えば、印刷や NW 送信、持ち出しの操作は禁止し、閲覧や編集、コピーを利用者自身のクライアントでのみ（「ID」部分）行わせる。なお、誰かと共同でファイルを作成する場合や情報共有する場合など、利用者自身以外とファイルを共有する必要がある場合には、「未設定」以外の該当するラベルを割り当てればよい。

【 0 0 7 8 】

なお、ラベル未設定のポリシーは組織における業務などに応じて変更してもよく、例えば ID システムと連携して、ファイルの利用者の職制情報や所属が同じである利用者間、あるいは利用者の役職以上のユーザとの間では閲覧、編集、印刷、NW 送信を許可するポリシーとすることも考えられる。

【 0 0 7 9 】

また、ラベル割り当ての手間を削減する方法の一つの例として、予めテンプレートが決まっているファイルについては、ラベルを割り当てたテンプレートを文書管理サーバ 8 0 に格納し、利用者がダウンロードして利用する。

【 0 0 8 0 】

以上説明したように、ポリシーリスト 1 3 を定義することにより、情報の種類によって操作を行う利用者の属性や場所、情報を格納する媒体を制限することができる。以下に、漏洩につながる可能性の高い操作と、操作を防止するためのポリシーの一例を示す。

【 0 0 8 1 】

（１）情報の持ち出し制御

例えば、ラベル A のように高い機密性が要求されるファイルへのコピー操作に対して、コピー先をデスクトップ PC に限定することにより、価値が高い情報を漏洩につながる可搬媒体に書き出す行為を禁止することができる。また、ラベル B 4 0 0 2 の公開可能なファイルに対しては、可搬媒体へのコピーや持ち出しも可能とし、ラベル C では持ち出しにあたり、持ち出しの承認が必要とすることにより、情報の種類に応じて持ち出しの制御ができる。

【 0 0 8 2 】

(2) 持ち出したファイルのアクセス制御

例えば、ラベル A 4 0 0 1 の閲覧操作に対して、場所における条件を社内のみとすることにより、ノート P C を社外で利用する場合など、不適切な場所での閲覧を防止できる。なお、これは人の所在を特定することが必要であるため、上記センサ 5 0 での入退室情報と連携して制御を行う。具体的な処理については、図 1 4 で説明する。

【0083】

(3) 印刷の制御

例えば、ラベル A 4 0 0 1 のように印刷する場所を制限するポリシーやラベル B 4 0 0 2 のように誰でも印刷可能とするポリシーを設定できる。情報の価値に応じて印刷を制限することにより、機密性の高い情報について閲覧はできても印刷はできないように制御することが可能となる。

【0084】

(4) ネットワーク送信の制御

例えば、ラベル A 4 0 0 1 の機密性の高い情報については、ネットワーク送信を社内に限定することにより、組織外への不正な送信や宛先間違い、送信するファイルの間違いを防止することが可能である。

【0085】

さらに、ラベル C 4 0 0 3 のように社外の取引先と共有するファイルについては、共有先として取引相手や委託先企業のメールアドレスや W e b アップロード先の U R L を事前に指定してあるため、指定している相手には申請をすることにより、承認者の承認を待たずに操作を行うことができる。また、相手先へ不正に電子メールを送信することや、誤送信の防止、正規の宛先に情報を正しく送信することが可能となる。

【0086】

(5) 社外から社内の機密情報へのアクセス制御

例えば、ラベル A 4 0 0 1 の閲覧操作では、閲覧可能な場所を社内にするのを条件として設定する。利用者が退室して社外に出る際に I C カードをセンサに近づけて I D を読み取らせることにより、利用者の所在が社外として状態管理リスト 2 4 に記録されるため、リモートアクセス機能を利用してラベル A 4 0 0 1 のファイルにアクセスしようとしてもアクセスできない。これにより、社外でのノート P C 利用が認められている社員が社外でノート P C を操作する場合でも、機密性の高い情報の閲覧は防止できるため、第三者にファイルを見られてしまうことによる漏洩を防ぐことができる。

【0087】

なお、入退室管理とクライアントへのログインとを連携させ、I C カードをかざして入室し、入室した記録がないとクライアントにログインできないようにすることも可能である。また、退室した記録がないと社外ネットワークからリモートアクセスできないようにすることも可能である。これにより、退室時に I C カードをかざさずに、社内にいると成りすましてリモートアクセスする行為を防止することができる。なお、上記説明した制御は一例であり、その他の制御も可能である。

【0088】

図 5 にポリシーリスト 1 3 の設定画面の一例を示す。

ポリシー設定サーバ 1 0 に格納するポリシーリスト 1 3 は、管理者 2 がポリシー設定サーバ 1 0 の操作部 7 0 5 を介してポリシー設定プログラム 1 1 に直接アクセスする、あるいは、別な端末からネットワーク 4 0 を介してポリシー設定プログラム 1 1 にアクセスすることで設定する。管理者 2 がポリシー設定プログラム 1 1 にアクセスすると、表示部 7 0 4 が図 5 に示したポリシー設定画面 5 0 1 を表示する。

【0089】

ポリシー設定画面 5 0 1 では、新規ポリシーの設定、あるいは登録済みポリシーの設定確認や修正を行う。ポリシー設定画面 5 0 1 は、登録済みポリシーのラベル一覧を表す登録済みラベル一覧 5 1 0 と、新規ポリシーを設定する新規追加ボタン 5 1 1 から構成される。

10

20

30

40

50

【0090】

登録済みラベル一覧テーブル510は0個以上のエントリから構成される表データであり、登録済みポリシーのラベル名5011、ファイルのカテゴリ5012、機密性の度合いを表すレベル5013、ラベル5011に設定済みのポリシーを表示する設定表示ボタン5014、ラベル5011に設定済みのポリシーを修正する画面を表示する修正ボタン5015、ラベル5011に設定済みのポリシーを再利用して新規ポリシーを追加するために設定済みポリシーを複製したポリシー設定画面を表示する再利用ボタン5016、ラベル5011が割り当てられているファイルの登録数5017、からなる。

【0091】

管理者2が実行したいボタンを押下すると、以下のようにそれぞれ画面が表示される。例えば、設定済みポリシーを参照する場合は列5014のボタンを押下し、設定済みポリシーを修正する場合は列5015のボタンを押下し、設定済みポリシーを複製して新規ラベルを登録する場合は列5016のボタンを押下し、新規ポリシーを追加する場合は新規追加ボタン511を押下する。

管理者2から上記ボタンのいずれかが押下されると、ポリシー設定プログラム11はポリシー設定画面502を表示する。

【0092】

ポリシー設定画面502は、新規登録するラベル名にカテゴリとレベルを割り当てるラベル設定フォーム520、共有先のURLやメールアドレスを入力する入力フォーム5214、共有先のURLやメールアドレスをID管理システムなどから特定する参照ボタン5215、新規追加するラベルについて、操作ごとに実行する権限を設定する操作権限設定画面522、設定したデータをポリシーリスト13に登録するための登録ボタン523から構成される。なお、ボタン5014が押下された場合には、操作権限設定画面522に設定済みのポリシーを表示し、ボタン5015が押下された場合には、操作権限設定画面522に設定済みのポリシーを表示し、さらに表示した権限を変更することができる。さらに、ボタン5016が押下された場合には、操作権限設定画面522に設定済みのポリシーを表示し、新規追加するようラベル520を修正することができる。

【0093】

ラベル設定フォーム520では、ラベル名5211を入力し、カテゴリ5212とレベル5213から管理者2が設定したい値をプルダウンから選択する。また、設定したいカテゴリがない場合には、管理者2が新規入力フォーム521に適切なカテゴリ名を入力してもよい。

社外共有先入力フォーム5214では、社外でファイルを共有する相手が予めわかっている場合に、URLあるいはメールアドレスなど相手を一意に識別できる情報を入力する。

【0094】

操作権限設定画面522は、操作ごとに異なるタブ5221で権限設定画面を切り替えることができるため、管理者2はタブ5221を押下して操作を切り替え、全ての操作の権限を設定する。操作権限設定画面522は、操作権限を設定する表5223と、設定したデータのうち表示している表についてのみ入力を全て無効として初期表示に戻すリセットボタン5222、からなる。

【0095】

操作権限設定表5223は、図3で説明した情報漏洩につながる可能性の高い操作全てについて権限を設定する表であり、新規追加ボタン511を押下した場合など何も入力されていない場合は背景が白く(5224)表示される。管理者2が操作権限を設定する場合は、操作権限設定表5223のうち、条件に該当させない項目を押下すると、押下した項目の背景を例えば黒に反転する(5225)。このように、操作権限設定表5223で押下した項目の色を変えることにより、操作権限を設定することができる。

【0096】

管理者が全ての権限を設定して登録ボタン523を押下すると、ポリシー設定プログラ

10

20

30

40

50

ム 1 1 は、操作権限設定画面 5 2 2 を閉じ、操作権限設定表 5 2 2 3 に入力されたデータから図 3 のアクセス主体 2 8 5 に示した論理式を生成し、入力されたデータ全てをポリシーリスト 1 3 に登録する。そして、ポリシーリスト 1 3 へのデータ登録が終了すると、登録済みラベル一覧テーブル 5 1 0 の最後の行を新規追加し、設定したラベル情報を表示する。

【0097】

以上説明したように管理者 2 がポリシーリスト 1 3 を生成し、ポリシー配信プログラム 1 2 が更新したポリシーリスト 1 3 をクライアント 7 0 に配信することにより、クライアント 7 0 のポリシーリスト 7 3 が更新される。ポリシーリスト 1 3 のクライアント 7 0 への配信については、図 6 を用いて説明する。

10

【0098】

図 6 にポリシー配信処理の流れを示す。

クライアント 7 0 の監視・制御プログラム 7 2 は、プログラムを起動した後（ステップ 6 0 1）、ポリシー設定サーバ 1 0 のポリシー配信プログラム 1 2 にアクセスし、クライアント 7 0 のユーザ ID を送信し、ポリシーテーブルの取得を申請する（ステップ 6 0 2）。

【0099】

ポリシー配信プログラム 1 2 は、ポリシーテーブル取得申請を受信後、ID 管理システム 9 0 のユーザリスト 9 1 を参照し（ステップ 6 0 3）、ユーザリスト 9 1 に受信したユーザ ID が登録されているかを判断する（ステップ 6 0 4）。ユーザ ID が登録されてい

20

ればポリシーリスト 1 3 をクライアント 7 0 に配信し（ステップ 6 0 7）、登録されていない場合はクライアント 7 0 の監視・制御プログラム 7 2 にエラーを返し（ステップ 6 0 5）、ポリシー設定サーバ 1 0 の表示部 7 0 4 にエラーとユーザ ID を表示する（ステップ 6 0 6）。

【0100】

本動作フローにより、クライアント 7 0 が起動するたびにポリシーリスト 7 3 は最新の状態に更新される。なお、クライアント 7 0 に監視・制御プログラム 7 2 を新規インストールした場合には、少なくともラベル「なし」のファイルに対するポリシーを格納したポリシーリストが同時にインストールされる。これにより、監視・制御プログラム 7 2 をインストールした直後にファイルにラベルを割り当てていない場合でも、ラベルに基づいた制御を実行することができる。また、クライアント 7 0 がネットワーク接続しない場合、またはポリシー設定サーバ 1 0 と通信できない場合、またはカードリーダー 7 9 5 で IC カードとクライアントを通信して組織内にいることが確認できない場合には、ラベル「なし」のポリシーを全てのファイルに適用する。

30

【0101】

図 7 にラベル割り当て処理の流れを示す。

ファイルへのラベル割り当て処理は、ファイルの利用者 1 がファイルの共有範囲を利用者以外に設定したい場合に実施する。なお、ファイルの作成者が利用者 1 でない場合でも、ファイルをクライアント 7 0 に格納した場合には、利用者 1 がラベルを割り当てるまではラベル「なし」のポリシーが適用される。

40

【0102】

まず、クライアント 7 0 の利用者 1 がファイルを新規作成あるいはクライアント外から NW 送信やインターネット 4 0 を通じて入手して保存したファイルについて、自発的にラベルを割り当てる場合、利用者が文書管理サーバ 8 0 のラベル割当プログラム 8 1 にアクセスし、ログインする。このとき、クライアントの監視・制御プログラム 7 2 は、クライアントのユーザ ID を送信する。また、ラベルが未設定のファイルを操作しようとして制御された場合、監視・制御プログラム 7 2 が文書管理サーバにアクセスし、ユーザ ID を

50

送信する（7001）。

【0103】

すると、文書管理サーバ80のラベル割当プログラム81はサーバ認証を行い（7002）、ポリシー設定サーバ10のポリシーリスト13を参照して（7003）、ユーザIDがアクセス主体の条件を満たすラベルを特定し（7004）、クライアントの画面上にラベル割当画面を表示させる（7005）。

【0104】

利用者1は、表示されたラベル割当画面でファイルのラベルを割り当て（7006）、さらにラベルを割り当てるファイルを指定し（7007）、ラベル割当プログラム81に送信する（7008）。なお、ラベル割当画面の詳細については、図8で説明する。監視・制御プログラム72は、ラベル管理テーブル74を更新し、申請したファイルの状態を承認待ちとする（7009）。

【0105】

ラベル割当プログラム81は、クライアント70から受信したユーザIDおよびラベル情報とポリシーリスト13を照合し、承認が必要かを判断し（7010）、承認が必要なラベルの場合は承認者に申請内容を送信する。なお、承認を必要としないラベルは設定してもよいし、しなくてもよい。このとき、ラベル割当プログラム81は、ラベル管理リスト84を参照し、ラベル管理リスト84に登録されたラベル割り当て済みファイルの一覧から、利用者が選択したラベルと同じラベルを割り当てられているファイル、あるいは同じカテゴリを割り当てられているファイルなどを少なくとも1以上抽出して送信する（7011）。なお、抽出する条件として、利用者と同一部署のユーザが所有するファイルのラベルとしてもよい。

【0106】

承認者3は、申請されたファイルとラベルが適切であるか確認し、必要であればラベルの変更を要求する（7012）。このときの編集画面の詳細については、図8で説明する。

承認者3がラベルを確認あるいは変更要求を実行した後、ラベル割当プログラム81では、ラベルを割り当てたファイルが完成文書である場合には（7013）文書管理サーバ10にファイルを格納し（7014）、ラベル管理リスト84を更新する（7015）。なお、完成文書でない場合には、ファイルは格納せずにラベル管理リスト84を更新する（7015）。

【0107】

次に、ラベル割当プログラム81は、申請内容に共有先の指定もあるかを確認し（7016）、共有先の指定が必要な場合にはポリシーリスト13を参照し、共有先を追加するようポリシー設定プログラム11に共有先情報を送信する（7017）。また、共有先情報の指定が必要でない場合には操作を行わない。

【0108】

ラベル割当プログラム81が登録を完了し、登録完了通知を監視・制御プログラム72に送信すると（7018）、クライアント70の監視・制御プログラム72はラベル管理テーブル74を更新し、申請したファイルの状態を承認済みとする（7019）。これにより、ファイルにはラベルが割り当てられ、以降ファイルにはラベルに設定されたポリシーが適用される。

【0109】

なお、ファイルに対するラベルの割り当ては、本実施例で説明したテーブルを用いてラベルを管理する方式だけではなく、ファイルのヘッダ領域やコンテンツにラベルを埋め込む方法や、DRM技術を用いてラベルとファイル本体をカプセル化してもよい。

【0110】

図8にラベルの割り当て申請画面の一例を示す。

ファイルへのラベル割り当ては、図7で説明したように、ファイルを格納しているクライアント70の利用者1がまずラベルを割り当てし、割り当てたラベルが適切であるかを

10

20

30

40

50

承認者 3 が確認して承認するとファイルにラベルが割り当てられ、ラベルに基づく制御を行う。

【0111】

ラベル割当申請画面 801 は、ラベルを新規で割り当てるか、あるいは一度割り当てたラベルを変更するかを選択するボタン 8011 と、ラベル割り当てを申請する利用者のユーザ ID 8012 と、ラベルを割り当てるファイルパス 8013 と、ラベルを割り当てるファイルを参照して選択するボタン 8014 と、文書管理サーバに登録するかどうかなを選択し、登録する場合には登録先のフォルダを指定する登録先フォルダ 8015 と、登録先フォルダ 8015 を文書管理サーバから参照して選択するボタン 8016 と、ラベルの選択方法を選択するための履歴利用タブ 8017 またはプルダウン選択タブ 8018 と、履歴利用タブを選択した場合の選択肢を表示したラベル選択表 8019 と、入力内容を申請する申請ボタン 8020、からなる。なお、履歴利用タブ 8017 の選択肢として表示するラベルは、利用者 1 が操作を実行する条件を満たすラベルである。

10

【0112】

利用者 1 は、例えば 8010 に示したように該当するラベルを選択することで、割り当てたラベルを選択することができる。

また、利用者 1 がプルダウンによるラベルの選択を希望し、プルダウン選択タブ 8018 を押下すると、ラベル割当申請画面 802 が表示される。

【0113】

ラベル割当申請画面 802 では、基本的な構成はラベル割当申請画面 801 と同じであり、ラベル選択表 8019 の部分をプルダウンで選択するプルダウン選択表 8021 を表示する。プルダウン選択表 8021 は、カテゴリ 8022 を選択するプルダウンと、レベル 8023 を選択するプルダウンが表示されるため、利用者 1 は該当するカテゴリとレベルを選択し、選択が終わったら決定ボタン 8014 を押下することで、割り当てたラベルを申請することができる。

20

【0114】

図 9 にラベル割り当ての承認画面の一例を示し、承認者 3 のラベル承認方法を説明する。

承認者 3 が文書管理サーバ 80 のラベル割当プログラム 81 にアクセスすると、ラベル承認画面 901 が表示される。ラベル承認画面 901 は、申請者のユーザ ID 9011 と、利用者 1 がラベルを割り当てたファイルパス 9012 と、文書管理サーバ 80 に登録する場合には登録先フォルダ 9013 と、利用者 1 が割り当てたラベル 9014 と、ファイルを表示する表示ボタン 9015 と、ラベルを変更する場合に選択するラベルの候補リスト 9016 と、類似するファイルのラベル一覧 9018 と、承認ボタン 9019、からなる。

30

【0115】

承認者 3 は、ラベル承認画面 901 を見てファイルとラベルが適しているかを判断する。もし、ファイルの中身を確認する場合は、表示ボタン 9015 を押下すると、文書管理サーバ 10 にアップロードされたファイルが開くため、承認者 3 はファイルの中身を見てラベルを承認することもできる。承認者 3 は、申請されたファイルについて、ラベルの変更が必要ないと判断した場合は、承認ボタン 9019 を押下し、ラベルの変更が必要と判断した場合は、別なラベルを選択し（9017）、承認ボタン 9019 を押下する。これにより、もし利用者 1 が適切でないラベルをファイルに割り当てていた場合でも、承認者 3 が変更することにより、適切なラベル割り当てがなされる。

40

なお、ラベル承認画面 901 には、類似するファイルのラベル一覧を表示しているため、承認者 3 は利用者 1 が設定したラベルが適切かどうかを判断するための目安とすることができる。

【0116】

図 10 にラベル管理リスト 23 および状態管理リスト 24 のデータ構造の一例を示す。

50

ラベル管理リスト 23 は、ラベルが割り当てられたファイルに関するデータを格納している。ラベル管理リスト 23 は、少なくとも 0 個以上のエントリからなるデータであり、一意に情報の格納場所を識別可能なファイルパス 1011、ファイルを格納する媒体識別 ID 1012、ファイルに割り当てたラベル 1013、ラベルを最後に割り当てた最終ラベル割当者 ID 1014、ラベルの登録日時 1015、ラベルの承認状態 1016、その他状態 1017、からなる。

【0117】

その他状態 1017 で管理するデータは、例えば「ラベル承認中」「持ち出し申請中」「持ち出し中」などのファイルの状態を表示する。ラベル管理リスト 23 により、どのクライアントにどのラベルをもつ情報が格納されているか、また、ラベルが割り当てられている情報の承認状態などを迅速に把握することができる。また、クライアント 70 は同じ形式を持つラベル管理テーブル 74 を備えており、文書管理サーバ 80 は同じ形式を持つラベル管理リスト 84 を備えている。ラベル管理テーブル 74 およびラベル管理リスト 84 では、クライアント 70 あるいは文書管理サーバ 80 に格納しているファイルについて同じ形式で状態を管理している。

【0118】

次に、状態管理リスト 24 について説明する。

状態管理リスト 24 はセンサ 50 を利用者が通過したログを元に、ID 管理システム 90 のユーザリスト 91 に登録した利用者の所在を管理するものである。

状態管理リスト 24 は少なくとも 0 個以上のエントリからなるデータであり、ユーザ ID 1031、利用者の現在地を示す所在 1032、からなる。

【0119】

例えば、ユーザ ID 1031 が 001 の利用者は執務室にすることを示す。これは、組織外から組織内の建屋、建屋から執務室に利用者が通過する際に IC カードをセンサ 50 に近づけて ID を読み取らせることにより、入室したデータが状態管理リスト 24 に反映されていることを意味する。状態管理リスト 24 は、利用者 1 が IC カードをセンサ 50 を近づけて ID を読み取らせるなど正当な方法で通過した場合に更新されるため、例えば状態管理リスト 24 で建屋内にいないことをクライアント 70 のログイン条件にしておくことにより、なりすましや共連れにより入室してクライアント 70 を操作し、ファイルにアクセスしようとしても、状態管理リスト 24 に入室した記録がない場合には、ログインすることができないよう制御することができる。

なお、利用者の所在を確認する手段として、センサ 50 だけではなく、利用者が操作するクライアント 70 が接続する IP アドレスなどを取得することによって、社内のどこに利用者がいるかを判断してもよい。

【0120】

図 11 に利用者の所在を特定する処理の流れを示す。

利用者 1 がセンサ 50 に IC カード 76 あるいは ID 情報を格納した携帯電話 79 をかざしてセンサが設置してあるエリアに入退室すると (1101)、センサ 50 のセンサログ取得プログラム 51 で取得したセンサログをログ管理サーバ 30 のログ解析プログラム 31 に送信する (1102)。ログ解析プログラム 31 は、センサログを受信すると (1103)、ユーザリスト 91 を参照し (1104)、入退室した利用者のユーザ ID を特定する (1105)。さらに、ログ解析プログラム 31 は、特定したユーザ ID とセンサの識別情報を状態管理サーバ 20 の状態管理プログラム 21 に送信する (1106)。状態管理プログラム 21 は、ユーザ ID とセンサの識別情報を受信すると (1107)、状態管理リスト 24 を参照し (1108)、受信したユーザ ID の所在情報を更新する (1109)。

【0121】

以上、図 11 で説明したように、組織内に設置されたセンサ 50 を利用者が通過した情報を状態管理サーバ 20 の状態管理リスト 24 で管理することにより、利用者の所在の変化を把握することができる。

10

20

30

40

50

【0122】

図12でクライアント70、文書管理サーバ80、ノートPC78で動作する監視・制御プログラム72の動作フローについて説明する。

監視・制御プログラム72が起動すると（ステップ1201）、クライアント70における利用者の操作を監視する（ステップ1202）。利用者がファイルに対して操作を行うと（ステップ1203）、発生した操作の状態を識別する（ステップ1204）。このとき監視・制御プログラム72は、発生した操作と、Webアップロードなどネットワーク送信の操作である場合には宛先であるメールアドレスあるいはURLなどの社外共有先情報、クライアントのユーザID、ファイルパス、なども識別する。

【0123】

次に、クライアント70に格納したラベル管理テーブル74を参照し（ステップ1205）、操作対象であるファイルのファイルパスをキーとしてファイルに割り当てたラベルを特定する（ステップ1206）。

ラベルが「なし」以外に設定されている場合には（ステップ1207）、状態管理サーバ20にアクセスして状態管理リスト24を参照し（ステップ1209）、ユーザIDをキーとして利用者の所在を特定する（ステップ1210）。

【0124】

ステップ1207においてラベルが未設定の場合、またはステップ1209で状態管理サーバ20にアクセスできなかった場合は、ラベル未設定用のポリシーを参照する（ステップ1208）。なお、ステップ1209で状態管理リスト24にアクセスできない場合もラベル未設定として扱うのは、状態管理サーバ20とアクセスできない場合はクライアントがオフラインの場合と考えられ、オフラインの場合は利用者の所在が特定できないためである。また、クライアントがオフラインの場合は、ポリシー設定サーバ10に格納しているポリシーリスト13とクライアント70に格納しているポリシーテーブル73とが異なってしまう可能性があるため、適用すべき制御が異なってしまうことを防ぐためである。

【0125】

次に、ステップ1208でラベルが「なし」のポリシーを参照した場合、ステップ1204で識別した状態がラベル「なし」のポリシーと一致するかを判定し（ステップ1214）、一致する場合には操作を実施し（ステップ1215）、一致しない場合には操作を防止する（ステップ1216）。ステップ1216で操作を防止した場合には、利用者にアラートを表示し（ステップ1217）、さらにラベル割当操作を行うか利用者に入力させる画面を表示し、ラベル割り当て操作を利用者が行うと入力を受け付けた場合には（ステップ1218）、ラベル割当画面を表示する（ステップ1219）。ラベルの割り当てを行わない場合、あるいはラベル割当画面を表示した（ステップ1219）後は、ログを取得する（ステップ1220）。

【0126】

一方、ステップ1210において利用者の所在を特定した場合は、操作がNW送信あるいはクライアント以外の記憶媒体へのファイルのコピー、印刷などいずれかのクライアント以外の格納先への操作であるかを判定し、出力操作である場合には（1211）、資産リスト101を参照してファイル格納先の資産情報を取得し（ステップ1212）、ポリシーリスト73のラベルに設定しているポリシーを参照する（ステップ1213）。また、ステップ1211で操作が出力操作でない場には、ステップ1213を実行する。

【0127】

ステップ1213でポリシーを参照し、ステップ1204で識別した状態がポリシーの条件と一致するかを判定した結果、一致する場合には（ステップ1221）、操作を実施する（ステップ1222）。さらに、例えばコピーや名前変更、あるいは削除などのように操作を実行することによりファイルパスが変更になる操作であれば（ステップ1223）、ラベル管理テーブル74を更新し（ステップ1224）、ログを取得する（ステップ1220）。ファイルパスが変更にならない場合はステップ1220を実行する。

10

20

30

40

50

【0128】

ステップ1221でポリシーの条件を満たさなかった操作の場合は、操作を防止し（ステップ1225）、アラートを利用者に表示し（ステップ1226）、ログを取得する（ステップ1220）。なお、ステップ1220では、少なくとも操作の発生時刻と、ユーザIDと、操作の実行有無と、ファイルのラベルをログとして記録する。

【0129】

ステップ1220の後、プログラム終了命令がされない限り（ステップ1227）、ステップ1202に戻って監視を行い、プログラム終了命令がなされた場合は、プログラムを終了する（ステップ1228）。

【0130】

本実施例では、状態管理サーバ20で管理している状態管理リスト24を参照し、利用者の操作環境も取得して制御することにより、単なる人物からファイルへのアクセス権の制御だけではなく、ファイルを利用する利用者の環境によってもファイルの操作を制御することが可能となる。

【0131】

なお、図12ではクライアント70における監視・制御プログラム72の説明をしたが、文書管理サーバ80の監視・制御プログラム82では、ラベル管理リスト84とポリシー設定サーバ10のポリシーリスト13を参照し、ノートPC78では、クライアント70からコピーしたラベル管理テーブル7813とポリシーリスト7814を参照する。

【0132】

図13にファイルの持ち出し操作に係る処理の流れを示す。

利用者1が状態管理サーバ20の状態管理プログラム21にアクセスすると（1301）、申請画面が表示される（1302）。利用者1が表示された申請画面に従い申請情報を入力し（1303）、申請情報および持ち出すファイルを状態管理サーバ20に送信すると（1304）、状態管理プログラム21はラベル管理リスト23と持ち出すファイルのファイルパスとを照合してファイルのラベルを特定し、特定したラベルのポリシーを参照して持ち出し可能かを識別し（1305）、持ち出し操作の条件を満たしていない場合には条件を不適切のエラーメッセージを表示する（1306）。持ち出し操作の条件を満たしている場合には、申請情報を承認者3に送信する（1307）。承認者3は表示された承認画面で持ち出し申請情報を確認し、申請情報の持ち出し許可あるいは不許可を判断し（1308）、状態管理プログラム21に送信する（1309）。

【0133】

状態管理プログラム21は承認結果を受け付け（1310）、不許可の場合は申請不許可のメッセージを通知し（1311）、許可の場合はラベル管理リスト23の状態を持ち出し承認済に更新し（1312）、少なくとも利用先の所在情報と格納媒体の識別IDを復号条件として含めた暗号鍵を生成し（1313）、ファイルを暗号化する（1314）。

【0134】

状態管理プログラム21が利用者に持ち出し許可通知を送信すると（1315）、利用者1は状態管理サーバ20にアクセスし（1316）、暗号化したファイルをダウンロードし（1317）、持ち出すノートPC78にファイルを格納する（1318）。このとき、クライアント70の監視・制御プログラム71はファイルのダウンロードを検知し、ラベル管理テーブル74に承認結果を反映する（1323）。

【0135】

利用者1は、その後組織内から組織外に出る場合、ICカード76あるいは利用者のID情報を格納した携帯電話79をセンサ50に近づけて近距離無線通信を行わせ、IDを読み取らせる（1319）。すると、センサ50のログ取得プログラム51でユーザ情報を取得し（1320）、状態管理プログラム21に取得した情報を送信する（1321）。状態管理プログラム21では、受信したユーザ情報を元にラベル管理リスト23の状態を持ち出し中に更新する（1322）。

10

20

30

40

50

【0136】

この処理により、組織外に持ち出したファイルは暗号化して持ち出されるため、あらかじめ申請し承認された利用先以外の場所で利用者1がアクセスしても復号化されず、不適切な利用場所での操作を防止することができる。

【0137】

なお、USBメモリなどのCPUを持たない可搬媒体に格納する情報のレベルが高い場合も、強制的にファイル暗号化を行う。暗号化の方法については、例えば「情報漏洩リスク提言のための内部統制と情報資産管理（著：甲斐他、日立評論 2007年9月号、p.p. 51、3.3節）」に開示しているように、持ち出すファイルを自己復号型で暗号化し、規定PCの識別情報（MACアドレスなど）を暗号ファイルに格納することにより、自宅PCや不審なPCでの閲覧・編集を防止することができる。

10

【0138】

図14に組織外におけるファイル操作に係る処理の流れを示す。

利用者1は、携帯電話79に格納された認証プログラム791を用いて状態管理サーバ20の認証プログラム22にアクセスし、ログイン情報792を送信する（1401）。

状態管理サーバ20の認証プログラム22はログイン情報792が正規のものかどうかを判断し（1402）、認証に成功した場合は認証プログラム791に携帯電話79の所在情報送信を要求し（1403）、認証に失敗した場合はエラーメッセージを送信する（1408）。

20

認証プログラム22が利用者2の所在情報としてGPS情報を送信すると（1404）、状態管理プログラム21は状態管理リスト24を参照し（1405）、利用者の所在が承認済みの場所かどうかを照合する（1406）。

状態管理プログラム21は、所在が承認済みでない場合はエラーメッセージを送信し（1407）、承認済みであった場合は復号鍵リスト25を参照して現在の所在地で利用可能なファイルの復号鍵を特定し、送信する（1408）。

【0139】

認証プログラム22は復号鍵を受信し（1409）、通信プログラム793を起動する（1410）。通信プログラム793はノートPC78の認証プログラム782にログイン情報を送信し（1411）、認証が成功した場合には（1412）、通信プログラム793に復号鍵を要求し（1413）、通信プログラム793からBluetoothなどを用いて復号鍵を送信する（1414）。ノートPC78の通信プログラム783では、復号鍵を受信すると、ノートPC78に格納し（1415）、利用者1がファイルにアクセスした場合には（1416）、承認されたファイルのみ、復号鍵により復号化し（1417）、閲覧などの操作を実行できるようになる。

30

【0140】

なお、ノートPC78の通信プログラム783は、携帯電話79の認証プログラム791と一定時間ごとに通信し、通信できなくなった場合はノートPC78の監視・制御プログラム791が操作を防止する。これにより、ノートPC78を開いたまま承認済みの場所から移動した場合に操作を継続させないことができる。

40

【0141】

図15にファイル持ち出し後の組織内での処理の流れを示す。

利用者1がノートPC78を組織外から組織内に持ち帰り（1501）、センサ50に例えばICカード76を近づけIDを読み取らせると（1502）、センサ50のセンサログ取得プログラム51は、ICカード76に格納されたユーザ情報を取得し（1503）、状態管理サーバ20の状態管理プログラム21にデータを送信する（1504）。

【0142】

状態管理プログラム21はラベル管理リスト23を参照し（1505）、持ち出し中のファイルのうち、持ち出し期限の切れたファイルがあるか特定し（1506）、持ち出し期限の切れたファイルがある場合には利用者1のクライアント70にファイル削除のメッ

50

ページを表示させる（１５０７）。利用者１がノートＰＣ７８から持ち出し期限の切れたファイルを削除すると（１５０８）、クライアント７０の監視・制御プログラム７２は、削除したファイルを格納した記憶媒体の識別ＩＤを状態管理プログラム２１に送信し（１５０９）、状態管理プログラム２１は、ラベル管理リスト２３の状態欄に設定した「持ち出し中」データを削除する（１５１０）。これにより、ノートＰＣ７８に格納したファイルを残留させたままにすることを防止することができるため、持ち出しの都度、持ち出しに関係のあるファイルのみを持ち出すことができる。

【０１４３】

図１６に持ち出し操作に係る申請および承認画面の一例を示す。

持ち出し申請画面の一例を１６０に示す。持ち出し申請画面１６０は、ファイルを組織外に持ち出す利用者１が入力を行う画面であり、図１３におけるステップ１３０３で表示する。

持ち出し申請画面１６０には、少なくとも申請者情報１６０１と、持ち出すファイル名１６０２と、持ち出すファイルをクライアント７０から参照して選択するボタン１６０３と、ファイルを格納する媒体の識別ＩＤ１６０４と、格納する媒体を参照して選択するボタン１６０５と、利用先１６０６と、利用先の所在の位置情報を選択するボタン１６０７と、持ち出し期限１６０８と、持ち出し目的１６０９と、申請ボタン１６１と、申請中止ボタン１６２と、を表示する。

利用者１が持ち出し申請画面１６０に入力し、申請ボタン１６１を押下すると、承認者３に持ち出し操作の承認申請と、持ち出すファイル名を選択するボタン１６０３で選択したファイルが送信される。

【０１４４】

次に、持ち出し承認画面の一例を１６３に示す。持ち出し承認画面１６３は、利用者１の申請を承認する承認者３が承認を行う画面であり、図１３におけるステップ１３０８で表示する。

持ち出し承認画面１６３には、少なくとも持ち出し申請画面１６０で利用者１が入力した情報として、申請者情報１６０１と、持ち出すファイル名１６０２と、ファイルを格納する媒体の識別ＩＤ１６０４と、持ち出し期限１６０８と、持ち出し目的１６０９、に加えて、持ち出すファイルを表示するボタン１６１１と、持ち出すファイルのラベル情報１６１２と、利用先情報の位置情報設定状況１６１３と、承認を許可するボタン１６４と、承認を差し戻しするボタン１６５と、を表示する。なお、持ち出すファイルのラベル情報１６１２は、持ち出し承認プログラム８３が、利用者１が入力したファイル名１６０２を受け付けた後、ラベル管理リスト８４を参照してラベルを特定し、表示する。

【０１４５】

以上述べた第１実施例により、情報の活用を阻害することなく、情報漏洩につながる操作を未然に防止することが可能になる。

【０１４６】

——実施例２——

第２実施例では、ファイルのラベル情報をファイルに埋め込む方法を示す。

図１７に第２実施例におけるラベル割り当て処理の流れを示す。第２実施例におけるラベル割り当て処理の大まかな流れは、図７に示した第１実施例におけるラベル割り当て処理と同じだが、第２実施例ではファイルの拡張領域を利用し、拡張領域に少なくともラベル名と、ラベル設定あるいは承認者情報と、を埋め込む。具体的には、ステップ７０１４で完成文書の識別を行う前に、ラベル埋め込み処理を行う（１７０１）。

【０１４７】

図１８に第２実施例における監視・制御プログラムの動作フローチャートを示す。第２実施例における監視・制御プログラムの動作フローチャートの大まかな流れは、図１２に示した監視・制御プログラムの動作フローチャートと同じだが、第２実施例では、ラベル管理テーブル７４の参照によるラベル情報の特定処理ではなく、ラベル読み込み処理を行う。また、ラベルをファイルの拡張領域に埋め込むため、ファイルパス変更操作を実行し

10

20

30

40

50

ない。そのため、ステップ1204で状態識別した後は、ラベル読み込み処理を行い（1801）、ラベルの設定状況を確認する（1207）。また、ステップ1222でラベルが設定されているファイルについて操作を実施した後は、ログ取得処理を行う（1220）。

【0148】

以上述べた第2実施例により、第1実施例と同じシステム構成で情報の活用を阻害することなく、情報漏洩につながる操作を未然に防止することが可能になる。

【0149】

――実施例3――

・システム構成について：

第3実施例では、組織外にファイルを持出す場合の承認処理における情報の識別方法を示す。図19に第3実施例のシステム構成図を示す。第3実施例におけるシステム構成では、送受信したメールのログを取得したメールログ1921を備えるメールサーバ192と、承認管理サーバ193を新たに設ける。また、クライアント70は申請管理プログラム1911を備え、ノートPC78は申請管理プログラム7801を備える。

【0150】

前記申請管理プログラム1911と申請管理プログラム7801は、同じ動作を行うものとし、この申請管理プログラムを対象機器にインストールすることにより、承認済みの属性を持つファイルを記憶手段中より特定し、既存のファイル検索プログラム等における表示用インターフェイスにおいて前記承認済みファイルを前記ファイル検索プログラムの既存機能等により強調表示（例：該当ファイルの表示をハイライト化、太字化するなど）することができる。なお、本実施例における承認フローについては図27および図28を用いて後に詳述する。

【0151】

また、前記申請管理プログラム1911は、コンテキストメニューに「持出し申請」を有している。例えば、利用者1がクライアント70あるいはノートPC78を介してファイルを選択し、前記申請管理プログラム1911が提供するコンテキストメニューから「持出し申請」を選択したとする。この場合、前記申請管理プログラム1911は、前記承認管理サーバ193の承認管理プログラム1931と通信して接続し、持出し申請画面を立ち上げるための認証画面を表示する。なお、第1実施例ではファイル持ち出しの承認処理を状態管理サーバで実施しているが、本実施例3におけるシステム構成に示すように、承認管理機能を備えた情報処理装置＝承認管理サーバ193を新たに設け、ラベル割当て処理について役割分担してもよい。

【0152】

前記承認管理サーバ193は、ファイルの持出しを申請する利用者1および持出しの承認判断をする承認者3のクライアント70やノートPC78などに表示する画面の生成や申請案件のステータスやファイルの管理を行う承認管理プログラム1931と、申請されたファイルの識別処理を行うファイル識別プログラム1932（ファイル識別手段）と、組織外の取引先情報を登録した取引先リスト1941およびファイル識別に用いる照合用DB1943（オブジェクト登録データベース）とを管理するDB管理プログラム1934（DB管理手段）と、持出しが承認されたファイルを持出し用のファイル形式に変換するファイル変換プログラム1935と、承認ステータスを格納する承認管理DB1942、ファイルの組織外持ち出しに係る組織のルールを登録した持ち出しルールDB1944、を備える。

【0153】

なお、既に図2にて示したとおり、前記クライアント70のハードウェア構成は、端末ログ75ならびにポリシーリスト73、ラベル管理テーブル74を保存する外部記憶媒体702（記憶手段）、申請管理プログラム1911および監視・制御プログラム72を実行するCPU701、メモリ703、入出力画面を表示する表示部704（出力手段）、入出力を制御する操作部705（入力手段）、可搬媒体77に格納されたデータなどを読

10

20

30

40

50

み書きするための可搬媒体接続部 706、RAM 707、有線あるいは無線でネットワーク 40 と通信を行う通信部 708、これらの各装置等を相互接続するバス 709 から構成される。また、前記ノート PC 78 や、本実施例 3 で新たに登場した承認管理サーバ 193 も、上記クライアント 70 と同様のハードウェア構成をとる。

【0154】

各装置では、CPU が外部記憶媒体に格納されたプログラムを実行することにより、以下に説明する処理、機能が実現される。ただし、各実施形態の説明では、便宜上、各プログラムを実行主体としている。また、各プログラムは、あらかじめ、上記各装置の外部記憶媒体やメモリに格納されていても良いし、必要なときに、可搬媒体接続部や通信部と、各装置が利用可能な媒体と、を介して、他の装置から導入されてもよい。媒体とは、たとえば、着脱可能な可搬媒体、または通信媒体（すなわちネットワーク 40 またはネットワーク 40 を伝搬する搬送波やデジタル信号）を指す。

【0155】

こうした本実施例 3 における前記承認管理サーバ 193 は、情報の種類を示すカテゴリと機密レベルの組合せデータであるラベルをファイルに割り当て、情報漏洩につながる操作を制限するファイル管理システムである。この承認管理サーバ 193 は、ラベルの申請受付時ないしファイルの持出し申請受付時において、申請を受け付けたファイルにおける利用禁止オブジェクトの有無を、前記照合用データベース 1943（オブジェクト登録データベース）における前記取り扱い情報に基づき特定するファイル識別プログラム 1932（ファイル識別手段）を備える。

【0156】

また、前記承認管理サーバ 193 は、前記ラベルの申請ないしファイルの持出し申請に対する承認結果を他端末（クライアント 70 やノート PC 78 など）ないし操作部（入力手段）から得て、前記照合用データベース 1943（オブジェクト登録データベース）における該当オブジェクトに関する取り扱い情報を更新する DB 管理プログラム（DB 管理手段）を備える。なお、前記 DB 管理手段は、承認結果を受信したときに前記オブジェクト登録データベースを更新するとすれば好適である。

【0157】

また、前記ファイル識別プログラム 1932 は、前記申請を受け付けたファイルについて、ページ構成と該当ページにおけるテキストの位置とオブジェクトの位置とを特定し、ここで前記ファイルについて特定した事項に関して類似する他ファイルを、前記照合用 DB 1943（オブジェクト登録データベース）の属性情報に基づき特定し、前記ファイルと他ファイルとの差分を取得して、前記取得した差分において前記照合用 DB 1943（オブジェクト登録データベース）に登録されたオブジェクトの有無を検出し表示部（出力手段）ないし他端末（クライアント 70 やノート PC 78 など）に出力するとしてもよい。

【0158】

・データベース構造等について：

図 20 に取引先リスト 1941 のデータ構造を示す。取引先リスト 1941 は、ファイル管理システム 1000 を導入した組織と業務上取引がある当該組織以外の取引先相手の情報を登録したリストであり、前記 DB 管理プログラム 1934 がメールサーバ 192 に格納されたメールログ 1921 などから作成する。この取引先リスト 1941 は、登録番号 2001、メールアドレス 2002、取引先名 2003、最後にメールを受信した日時である最終受信日時 2004、持ち出し申請が承認された回数を示す承認回数 2005、取引先相手に認識されているユーザ ID から成る。本取引先リストを参照することにより、ファイルの持出しが申請されている持出先がこれまで組織として付き合いのある相手か、あるいは新たに付き合いを始める相手かを判断することができる。

【0159】

なお、上記取引先リスト 1941 は以下の手順で作成される。前記承認管理プログラム 1931 が定期的にメールサーバ 192 に格納しているメールログ 1921 にアクセスす

る。そして前記承認管理プログラム１９３１は、組織のユーザの受信ログを解析し、送信元情報が組織外の相手のメールアドレスを特定する。

【０１６０】

次に、前記承認管理プログラム１９３１は、前記特定した組織外の相手からのメールアドレスに対応する受信元メールアドレスから、組織内のユーザのメールアドレスを特定し、たとえばＩＤ管理システム９０のユーザリスト９１に登録されたメールアドレスと照合してユーザＩＤを特定する。

【０１６１】

そして、前記取引先リストに取引先が登録されている場合、前記承認管理プログラム１９３１は、前記取引先リスト１９４１の該当レコードにて最終受信日時を更新する（前記特定したユーザＩＤが該当取引先に関し未登録のユーザＩＤであった場合、ユーザＩＤ２００６の欄も更新する）。一方、前記取引先リスト１９４１に取引先が登録されていない場合、前記承認管理プログラム１９３１は新規レコードを追加し、取得した情報（取引先の社名やメールアドレス等）を登録する。

【０１６２】

図２１に前記承認管理ＤＢ１９４２のデータ構造を示す。承認管理ＤＢ１９４２は、ユーザＩＤごとに作成した承認案件に関するメタデータと、申請されたファイルのコンテンツに関するメタデータからなる。承認案件に関するメタデータは、ユーザＩＤ２１００、承認案件ごとに作成する承認案件テーブル２１０１、ユーザがメールを受信した相手を日時の新しい順に格納したメール受信テーブル２１０２、とからなる。

【０１６３】

なお、承認案件テーブル２１０１は、承認操作完了時に承認管理プログラム１９３１が更新し、メール受信テーブル２１０２は、図２４で述べる取引先リスト１９４１の更新時にＤＢ管理プログラム１９３４が更新する。前記承認案件テーブル２１０１は、申請されると割り振られる申請ＩＤ２１１１、取引先の登録番号２１１２、持出し方法２１１３、ファイル形式２１１４、持出し理由２１１５、承認者コメント２１１６、承認に係るステータス２１１７、承認日時２１１８、申請されたファイルのＩＤ２１１９、とからなる。

【０１６４】

メール受信テーブル２１０２は、ユーザ２１００の受信したメールのうち、組織外の相手が送信者であるメールの上位件数を登録したものであり、メールアドレス２１２１、受信日時２１２２、とからなる。本件数は管理者がカスタマイズすることもできる。

【０１６５】

また、申請されたファイルのコンテンツに関するメタデータ２１０３は、申請されたファイルのＩＤ２１２３およびファイルそのもの２１２４と、ファイル識別プログラム１９３２で分析した分析データに照合用ＤＢ１９４３で検出したオブジェクトを付与したデータ２１２５と、ファイル比較用のデータ２１２６を格納する。ファイル比較用のデータとしては、ファイル間の類似度を比較可能なものとしてハッシュ値などを格納する。

【０１６６】

また、図２４に照合用ＤＢ１９４３（オブジェクト登録ＤＢ）のデータ構造を示す。前記照合用ＤＢ１９４３は、汎用ＤＢ２１０４と相手先別ＤＢ２１０５からなる。汎用ＤＢ２１０４は、持出し申請やラベル登録などに関する処理に統一的に利用可能なＤＢ（＝ファイルおよびラベルを問わないオブジェクトを登録したデータベース）であり、例えば「社外秘」など無条件で持ち出しが禁止される取り扱い情報（或いはその逆に、インターネット上の公開情報など無条件に持ち出しＯＫの取り扱い情報）が対応付けされた、人名、組織名などの単語、テンプレートなどを示すデータ、図やロゴなど、ファイルに含まれるオブジェクトを登録したものである。また、相手先別ＤＢ２１０５は持出し先ごとに生成し、持出し申請に関する処理に用いるＤＢ（＝ファイルを持出した履歴のある相手先ごとにオブジェクトを登録したデータベース）であり、前記汎用ＤＢ２１０４と同じ形式でオブジェクト情報が登録される。前記照合用ＤＢ１９４３は、更に、ラベルごとにファイルのオブジェクトを登録したラベル別データベース２１０６を備えるとしてもよい。これら各

D Bには、利用禁止オブジェクト 2 1 2 7 と、利用可能オブジェクト 2 1 2 8 がそれぞれ登録されており、承認案件について検出された件数 2 1 2 9 と共に登録されている。

【0 1 6 7】

前記照合用 D B 1 9 4 3 において、前記人名、組織名などの単語、テンプレートなどを示すデータ、図やロゴなどに関するデータが、オブジェクトの属性情報となる。また、これらオブジェクトの属性に対応付けされる「持ち出し禁止」、「持ち出し O K」などの情報が取り扱い情報となる。

【0 1 6 8】

また、図 2 5 に持ち出しルール D B 1 9 4 4 のデータ構造を示す。前記持ち出しルール D B 1 9 4 4 は、ファイル持出し時におけるファイル形式や持出し方法などの組み合わせにおいて許可あるいは不許可のルールが記載されているデータベースである。これは管理者や承認者が事前に D B 管理プログラム 1 9 3 4 を通じて更新するものであり、組織全体や部署などの小規模な単位での設定も可能である。例えば、(1) 取引先リスト 1 9 4 1 に登録されていない持出し先への持ち出しについてはファイルの詳細確認が必要、(2) ファイル形式が D R M 以外の場合は理由の記載が必須、といったルール 2 1 2 9 が定義される。

【0 1 6 9】

・画面表示例について：

図 2 4 に利用者 1 がファイルを組織外に持出し申請をする際の申請画面 2 2 0 の例を示す。本申請画面は、申請者である利用者 1 が承認管理サーバ 1 9 3 にクライアント 7 0 やノート P C 7 8 などアクセスすると、承認管理サーバ 1 9 3 の承認管理プログラム 1 9 3 1 が前記クライアント 7 0 やノート P C 7 8 などに返信して表示させるものである。なお、前記クライアント 7 0 の申請管理プログラム 1 9 1 1 が、そのコンテキストメニューにて利用者 1 から指示を受けて承認管理サーバ 1 9 3 に接続した場合、当該申請管理プログラム 1 9 1 1 は選択されているファイルのファイルパスを承認管理サーバ 1 9 3 に送信する。また、前記承認管理プログラム 1 9 3 1 では、利用者 1 にユーザ認証を行わせ、認証が成立した場合には前記ユーザ認証時における認証情報からユーザ I D を特定し、前記申請画面 2 2 0 に表示させる。

【0 1 7 0】

前記申請画面 2 2 0 では利用者による以下の情報の入力を（クライアント 7 0 やノート P C 7 8 などを介し）受け付ける。申請者名 2 2 1 1、持出し日 2 2 1 2、持出すファイル名 2 2 1 3、持出し先のメールアドレス 2 2 1 4、持出し理由 2 2 1 5、持出し方法 2 2 1 6、持出し時のファイル形式 2 2 1 7、さらにたとえばファイル形式が事前に定義した持ち出し方法以外（本実施例では、D R M (Digital Rights Management) 形式を例示）の場合には、持出し理由を入力させることもできる。このとき、持出すファイル 2 2 1 3 について、利用者 1 は、先ほど述べたようにクライアント 7 0 の申請管理プログラム 1 9 1 1 を利用して入力する以外に、参照ボタン 2 2 2 0 を押下し、ダイアログからファイルを指定することによって入力させてもよい。なお、一度に複数のファイルを持出す場合、前記利用者 1 は「追加」ボタン 2 2 2 1 を押下することで、ファイルを追加登録することができる。

【0 1 7 1】

また、持出し先 2 2 1 4 については、利用者が「履歴から入力」ボタン 2 2 2 3 を押下した際に、承認管理サーバ 1 9 3 が、持出し先候補リスト 2 2 1 をクライアント 7 0 やノート P C 7 8 などに出力し、このリストの中から選択させるとしてもよい。一方、前記持出し先候補リスト 2 2 1 に登録されていない、すなわち新規の持出し先の場合はメールアドレスの入力を受け付けるとしてもよい。なお、前記持出し先候補リスト 2 2 1 は、例えば前記承認管理サーバ 1 9 3 が、前記取引先リスト 1 9 4 1 の格納情報からデータ（メールアドレス 2 0 0 2、取引先名 2 0 0 3 など）を抽出し、メールアドレス 2 2 2 と取引先名 2 2 3 からなるデータベースを構成したものとなる。

【0 1 7 2】

またこの持ち出し先候補リスト 2 2 1 は、これまでの持出し履歴のある取引先 2 2 4 1、持出し申請頻度の高い取引先順 2 2 4 2、メール受信順 2 2 4 3、そして登録された名前順 2 2 4 4、などの条件で前記取引先リスト 1 9 4 1 から抽出したデータがリスト化されており、前記承認管理サーバ 1 9 3 は、該当タブの押下を受けて持ち出し先候補の表示切り替えを行うとすればより好適である。なお、利用者 1 が前記持出し先候補リスト 2 2 1 から持ち出し先の選択を行って持出し先入力を実行した場合、承認管理サーバ 1 9 3 は、入力フォーム 2 2 1 4 の横に、取引先リスト 1 9 4 1 にて既登録の取引先名（図中では“ A 社 A A A ”）も表示させる。これにより、メールアドレスが類似した取引先を間違えて入力していないかを確認することができる。

【0 1 7 3】

また、前記申請画面 2 2 0 において、持出し方法 2 2 1 6 については、例えば D R M、暗号化、平文などを選択可能としている。一方、例えば、組織に応じて前記持出し方法 2 2 1 6 のデフォルト値（例えば“ D R M ”）を予め指定しておくこともできる（例：承認管理サーバ 1 9 3 がクライアント 7 0 やノート P C 7 8 などの指定を受けて当該申請画面 2 2 0 のデータにデフォルト値を設定しておく）。また、承認管理サーバ 1 9 3 は、デフォルト設定されている持出し方法から他の方法に変更する指定を受けた場合、例えば、理由 2 2 1 8 の記入がなされないと申請ボタン 2 2 3 1 が押下されても処理を遷移させないといった判定を実行し、利用者に理由 2 2 1 8 を記入させるとしてもよい。上記申請に係る全ての項目を入力し、利用者が申請ボタン 2 2 3 1 を押下することで、当該申請画面 2 2 0 での入力データはクライアント 7 0 やノート P C 7 8 などから承認管理サーバ 1 9 3 に送信され、申請処理は終了する。承認管理サーバ 1 9 3 では前記申請画面 2 2 0 での入力データを承認管理 D B 1 9 4 2 に格納することとなる。

【0 1 7 4】

図 2 5 に承認者 3 が承認判断をする際の承認画面を示す。承認判断を行うための承認画面は、申請されている情報一覧を示す承認待ち一覧画面 2 3 0 および案件 1 件ずつの詳細画面 2 3 3 からなり、承認者のクライアント 7 0 やノート P C 7 8 などからの指示や前記申請画面 2 2 0 での申請ボタンの押下に応じ、承認管理サーバ 1 9 3 が生成してクライアント 7 0 やノート P C 7 8 などに出力する。承認者 3 は、まず承認待ち一覧画面 2 3 0 で対象となるファイルの承認判断を実施し、詳細な確認が必要なファイルについては、詳細画面 2 3 3 を見て承認判断を行う。以下、画面の詳細について述べる。

【0 1 7 5】

前記承認待ち一覧画面 2 3 0 は、チェックボックス 2 4 1 0 と、申請者名 2 4 1 1、持出し日 2 4 1 2、持出し先 2 4 1 3、要確認項目 2 4 1 4、プレビュー 2 4 1 5、承認判断ボタン 2 4 1 6、を表示する画面であり、承認管理サーバ 1 9 3 が記憶手段において予め該当画面のひな形データを有している。前記承認画面 2 3 0 に示す項目のうち、持出し先 2 4 1 3 については、利用者が入力した持出し先に対し、承認管理サーバ 1 9 3 が取引先リスト 1 9 4 1 を照合し、この取引先リスト 1 9 4 1 に登録済みの持出し先かどうかを特定し、登録済みの場合は登録した顧客名を表示し、登録されていない場合は「未登録」と表示する。また、申請者名 2 4 1 1 や持出し日 2 4 1 2 のデータは、前記承認管理サーバ 1 9 3 が前記申請画面 2 2 0 を通じて受け付けたデータを設定している。

【0 1 7 6】

承認者はメールアドレスだけでは持ち出し先について把握することができないため、承認管理サーバ 1 9 3 は、前記取引先リスト 1 9 4 1 において該当メールアドレスに対応する相手先情報の登録有無と登録名を、前記承認待ち一覧 2 3 0 の持ち出し先 2 4 1 3 の情報として示す。これにより承認者は、取引先の誤入力や不正な取引先の入力を容易に判断することができる。

【0 1 7 7】

また、前記承認待ち一覧画面 2 3 0 における要確認項目 2 4 1 4 では、申請情報を承認判断するにあたり持出しリスクの高い可能性がある項目を示す（後述する図 2 8 のフローにて承認管理サーバ 1 9 3 が実行する処理で特定される）。例えば、図中の案件 2 4 3 1

では個人情報が発見されており、個人情報を提出しようとしている可能性が高いことを示している。

【0178】

さらに、前記承認管理サーバ193は、前記プレビュー2415において、申請されたファイルの表紙2417と、ファイルの中で最も確認すべき情報が記載されたページ2418、とを表示する（後述する図28のフローにて承認管理サーバ193が実行する処理で特定される）。ファイルの表紙をプレビュー表示させるのは、表紙にはあて先や作成者名、タイトルなどファイルの要約情報を表す情報が記載されていることが多いためである。また、もっとも確認すべき情報が記載されたページ2418のプレビューを表示することにより、承認者が情報の中身を迅速に把握することができる。さらにプレビューを示すことで、承認者がファイルを開かなくても情報を識別することができるという利点もある。たとえばファイルが添付されただけの承認画面の場合、承認者はファイルを開き、記載されているすべてのページを見ないと何に関する情報かすら把握できず、効率的かつ正確に内容を把握することは困難である。これに対し、本プレビュー2415のように、表紙と最も確認すべきページを優先的に表示することによって、承認者におけるファイルを開く手間が削減される。更に、前記承認者が前記画面230における詳細ボタン2432を押下すると、承認管理サーバ193は前記詳細ボタン2432の押下に対応する申請案件に関して記憶手段から情報を抽出し、詳細画面233のデータを生成し返信する。この詳細画面233によれば、例えば前記承認待ち一覧画面230では承認判断しきれなかったファイルの詳細について承認者が確認を行うことができる。

【0179】

なお、承認者が前記画面230にてチェックボックス2431をチェックし、「チェックした申請をすべて承認」232ボタンを押下することにより、承認管理サーバ193は、詳細画面233の表示を行わずに承認判断の結果を受け付けることができる。なお、「チェックした申請をすべて承認」232ボタンは、「チェックした申請をすべて却下」するボタンとしてもよい。ただし、要確認項目2414に記載される数が所定数より多い申請案件については、前記チェックボックス2431にチェックが入っても、前記詳細画面233の出力を実行しないかぎり承認できないよう、承認管理サーバ193が制御するとしてもよい。

【0180】

また、前記詳細画面233の構成について述べる。詳細画面233は、前記承認待ち一覧230の情報では承認者が承認判断をしきれない場合に申請内容の詳細を把握させることを目的としたものである。この詳細画面233は承認管理サーバ193がクライアント70やノートPC78などに出力するものであり、申請日2451、申請者名2452、ファイル2453、持出し日2454、持出し先2455、持出し理由2456、持出し方法2457、要確認項目2458、さらにファイルのプレビュー2461、不適切表現指定ボタン2463、却下理由2464、差し戻し・却下理由などのコメント記述欄2465の各データを含む画面データである。

【0181】

前記要確認項目2458には、リスクの高いオブジェクトの種類だけではなく、過去承認／却下されたファイルのうち最も類似しているファイルが表示される（後述する図28のフローにて承認管理サーバ193が実行する処理で特定し設定する）。また、最も類似したファイルが却下されたファイルであった場合、その却下案件の却下理由（例：承認管理DB1942が却下理由の欄を備え、却下案件についてその却下理由のデータを保持している。承認管理サーバ193はこの承認管理DB1942から却下理由のデータを抽出して前記詳細画面233に設定）まで示すことにより、承認者が承認判断をする参考とすることができる。例えば、図に示した例では、該当申請案件が、過去に却下したファイルに最も類似しており、その却下理由は「個人情報のため」としている。承認者は、類似した案件のファイル持ち出し先と本申請のファイル持ち出し先、また類似した案件との差分を確認することによって、両者に大きな違いがないのであれば類似案件同様却下、ファイ

ル持ち出し先や表現の違いにより承認、などの判断を行うことができる。

【0182】

また、前記承認管理サーバ193は、前記プレビュー2461にて、前記承認待ち一覧画面230で表示したプレビュー画面を該当ファイルにおけるページごとに表示する。さらに、個人情報や企業名などファイルに含まれる情報漏えいリスクの高いオブジェクトをハイライト2462で表示する。これにより、承認者はプレビュー画面2461のどこを注意して確認すればよいか分かる。なお、承認者が「確認必要順」ボタン2459を押下すると、承認管理サーバ193は、確認する優先度の高い順（例：上方漏洩リスクの高いオブジェクトが含まれる数が多い順など）にプレビュー画面の並び替えを行う。また、前記承認者が「ページ順」ボタン2460を押下すると、承認管理サーバ193は、前記プレビュー画面をページ順に表示する。また、承認者が「ファイルを開く」ボタン2466を押下することにより、前記承認管理サーバ193は、申請案件のファイルを記憶手段から読み出してクライアント70やノートPC78などに出力し、承認者におけるファイル内容の確認に供する。

10

【0183】

一方、前記承認者は、承認／却下／差戻のいずれかの判断を選択し、「承認」2471、「却下」2472、「差戻」2473、のいずれかのボタンを押下することによって承認判断を終了する。なお、前記承認判断が「却下」あるいは「差し戻し」の場合、前記承認管理サーバ193は、クライアント70やノートPC78などを介した承認者による理由入力を、コメント2465の欄にて受け付ける。こうした理由入力を受け付けた承認管理サーバ193は、前記理由のデータを利用者のクライアント70やノートPC78などに送信することで、承認者が「差し戻し」や「却下」の判断を行った理由を利用者に通知することができる。

20

【0184】

また、承認者が不適切表現指定ボタン2463を押下して（例えば、範囲指定用のカーソルなどを承認管理サーバ193がクライアント70やノートPC78などに出力する）、プレビュー画面2461上のオブジェクトの範囲を指定した場合、承認管理サーバ193はこの範囲指定を受け付けて、前記承認者が不適切な表現と感じたオブジェクトの情報を取得することができる。承認管理サーバ193は、前記範囲指定の情報を利用者のクライアント70やノートPC78などに送信することで、前記承認者が漏洩リスクが高いと判断した表現がどの部分であったか利用者に教えることができる。

30

【0185】

さらに、却下理由2464では、却下理由として表現に不適切なものがあったのか、あるいは漏洩リスク上、内容上に不適切なものがあったのかを承認者に選択させることができる。例えば、申請された内容が組織内だけで共有すべき機密情報であった場合、承認者は「内容上不適切」にチェックをする。承認管理サーバ193は前記承認者のクライアント70やノートPC78などから前記却下理由2464でのチェック内容を受け付けて、表現の有無に関わらず内容上漏洩リスクが高いと判断し、申請を却下したことを利用者に通知する（としてもよい）。なお、前記承認者が実施するコメントの記入や指摘は「承認結果」であり、前記照合用DB1943の更新に用いられる（次回以降の申請時に反映される）。

40

【0186】

なお、以上述べた各画面の表示項目については、承認者自身で表示する項目をカスタマイズすることも可能である。また、前記承認待ち一覧画面230は承認者が携帯電話を用いて承認操作を行なってもよい。また、ファイルを詳細に確認する必要がある場合には、事前に登録しておいた代理人に承認を依頼することもできる。

【0187】

・処理フローの例：

まず図26にて、利用者によるファイルの持ち出し申請の流れについて説明する。利用者の持ち出し申請の受付処理に係るインタフェースは承認管理サーバ193の前記承認管理プ

50

プログラム 1931 が、利用者のクライアント 70 やノート PC 78 などに提示する（以下、クライアント 70）。

まず、ファイルを組織外に持ち出す利用者がクライアント 70 により承認管理サーバ 193 にアクセスし、ログイン処理を指示したとする。すると前記クライアント 70 はこの指示を受けて前記承認管理サーバ 193 に対するログイン処理を実行する（2501）。

【0188】

一方、前記承認管理サーバ 193 の承認管理プログラム 1931 は、図 24 で例示した申請画面 220 のデータをクライアント 70 に返信する（2502）。なお、図 24 で述べたように、利用者がクライアント 70 の申請管理プログラム 1911 を利用し、クライアント 70 がコンテキストメニューから承認管理プログラム 1931 にアクセスした場合、前記承認管理プログラム 1931 が利用者の ID と選択されているファイルパスを入力した状態の申請画面のデータを返す。

【0189】

次に、利用者が前記申請画面 220 の入力項目のうち「履歴から入力」ボタン 2223 を押下したとする。前記クライアント 70 はこの押下事象を受け付けて（2503：Y）、前記承認管理サーバ 193 に通知を行う。この時、の承認管理プログラム 1931 は、ログインしているユーザ＝前記利用者のユーザ ID をキーとし、前記取引先リスト 1941 および前記承認管理 DB 1942 のメール受信テーブル 2102 を参照し、持出先候補リストを生成する（2504）。そしてこの持出先候補リストのデータを含む持出先候補画面（図 24 参照）のデータを生成してクライアント 70 に送る（2505）。

【0190】

前記利用者が前記申請画面 220 の入力項目を全て入力し、申請ボタン 2231 を押下すると（2506）、クライアント 70 は前記申請画面 220 での入力データを承認管理サーバ 193 に送信する（2507）。他方、前記承認管理サーバ 193 の承認管理プログラム 1931 は前記入力データを受信する。そして、前記入力データを前記持出しルール DB 1944 に照合し、申請内容に不備（例：「社外秘」など無条件で持ち出しが禁止される内容が最初から含まれている等）がないか特定する（2508）。

【0191】

また、前記承認管理プログラム 1931 は、前記ステップ 2508 に続き、前記利用者の申請内容の確認画面を前記クライアント 70 に送信する（2509）。なお、前記ステップ 2508 で申請に不備があることが特定された場合、前記承認管理プログラム 1931 は、前記ステップ 2509 で送信する確認画面において不備がある項目を例えば強調表示する。この場合、前記クライアント 70 は前記確認画面のデータを承認管理サーバ 193 から受信して表示し、該当箇所に関する修正を利用者から受け付ける（2510：Y、2511）。この場合、フローは前記ステップ 2506 に戻る。一方、前記ステップ 2508 で申請に不備が無いと判定された場合（2510：N）、前記クライアント 70 は利用者から申請ボタンの押下を受け付ける（2512）。

【0192】

これにより、申請内容および申請するファイルがクライアント 70 から承認管理サーバ 193 に対し送信される（2513）。前記承認管理サーバ 193 の承認管理プログラム 1931 は、前記クライアント 70 から送信されてくるデータを受信して承認管理 DB 1942 に格納し、該当ファイルに関する組織外持ち出し申請を受け付けることになる（2514）。

【0193】

続いて図 27 に基づき、ファイルの持出し申請に対する承認処理の流れについて説明する。この場合、図 26 のフローに関し述べたように、前記クライアント 70 は、利用者による申請画面 220 での申請ボタン押下を受け付けて（2701）申請内容および申請するファイルを承認管理サーバ 193 に送信する（2702）。前記承認管理サーバ 193 の承認管理プログラム 1931 はこれを受信する。

【0194】

次に、前記承認管理プログラム1931は、申請された持出先について取引先リスト1941を参照し、相手先登録情報を取得する(2703)。そして、相手先用の照合用DB1943の有無を特定する(2704)。なお、新規申請の場合には相手先別の照合用DB1943は存在しないため、前記汎用DB2104のみを用いてファイルの識別を行うこととする。

【0195】

次に、前記承認管理プログラム1931は、前記申請内容(と前記承認管理DB1942の“ステータス”)から保留案件(図26の前記ステップ2510で“不備あり”となって再申請に回された案件)かを特定し(2705)、該案件が保留案件の場合(2705:Y)、保留された前回のファイルをファイル識別プログラム1932に送信する(2706)。そして、申請されたファイルもファイル識別プログラム1932に送信する(2707)。

10

【0196】

一方、前記ファイル識別プログラム1932においてファイル識別処理が行われると(2708)、その識別結果が承認管理プログラム1931に送信される(2709)。なお、ファイル識別プログラム1932の詳細な動作フローについては図28で述べる。

【0197】

前記承認管理プログラム1931がファイル識別プログラム1932から識別結果を受け取ると、前記持出しルールDB1944を参照し、要確認項目を抽出する(2710)。前記持出しルールDB1944には、持出し時におけるファイル形式や持出し方法などの組み合わせにおいて許可あるいは不許可のルールが記載されている。これは管理者や承認者が事前にDB管理プログラム1934を通じて更新するものであり、組織全体や部署などの小規模な単位での設定も可能である。例えば、(1)取引先リスト1941に登録されていない持出しについてはファイルの詳細確認が必要、(2)ファイル形式がDRM以外の場合は理由の記載が必須、といったルールが定義される。

20

【0198】

要確認項目を抽出した前記承認管理プログラム1931は、承認者3のクライアント70等に承認依頼を通知する(2711)。前記承認者のクライアント70は、承認者の指示を受けて承認管理プログラム1931を利用し、承認管理プログラム1931と通信し、前記承認依頼に対応する申請案件の内容を読み出して表示させる(2712、2713)。前記承認者が前記クライアント70にて閲覧する承認待ち一覧画面230については図25で説明したとおりである。

30

【0199】

前記承認者が承認／却下／保留のいずれかの判断を前記クライアント70で入力すると、該クライアント70はこの判断結果を前記承認管理プログラム1931に送信する(2714)。この時、前記承認管理プログラム1931は前記判断結果を受信し、その内容が却下あるいは保留であるか判定する。前記内容が「却下」あるいは「保留」である場合(2715:N)、前記承認管理プログラム1931は、前記利用者のクライアント70に申請が不許可となった通知を送信する(2716)。なお、この通知はメールなどを利用して利用者に通知してもよいし、前記承認管理プログラム1931に前記利用者のクライアント70がアクセスすると承認ステータスを表示させるようにしてもよい。

40

【0200】

他方、前記承認者の判断が「承認」であった場合(2715:Y)、前記承認管理プログラム1931はファイル変換プログラム1935に対して該当ファイルを送信し、承認されたファイル形式に変換させる(2717)。さらに、承認管理プログラム1931は前記DB管理プログラム1934に承認結果を送信して照合用DB1943における該当オブジェクトの取り扱い情報を最新の判断結果に更新させる(2718)。なお、前記ファイル変換プログラム1935ではファイル形式を変換すると共に、承認されたファイルであることを識別可能な属性情報を埋め込む。これにより、クライアント70に当該ファイルがダウンロードされた場合に、申請管理プログラム1911が当該ファイルを識別し

50

色づけして表示するため、クライアント 70 に格納されたファイルのうち、どれが承認されたファイルなのかを一目で把握することができる。

【0201】

前記ファイル変換プログラム 1935 でのファイル変換が完了すると、前記承認管理プログラム 1931 は承認管理 DB 1942（における“ステータス”など）を更新し（2719）、承認結果を利用者のクライアント 70 に通知する（2720）。前記利用者のクライアント 70 が承認管理サーバ 193 にアクセスして（2721）、持出し用の形式に変換されたファイルをダウンロードすると（2722）、利用者は持出しが可能となる。その後の持出しにおけるコントロールの詳細な処理については、実施例 1 に示したとおりである。

10

【0202】

続いて、図 28 に基づきファイル識別プログラム 1932 の処理フローについて説明する。ファイル識別プログラム 1932 は、承認管理プログラム 1931 より、申請対象のファイルを取得し（2811）、申請ファイルの構造を分析する（2812）。この申請ファイルの構造分析では、ファイルにおけるヘッダフッタ情報やテンプレート情報（例：ファイル作成に利用している書式ひな形等）、テキスト情報などをページ単位で取得しメモリ等に格納しておく。さらに、前記申請対象のファイルと類似した他ファイルを特定するために、申請対象のファイルのハッシュ値を取得する。また、ファイル形式などにより構造を分析できなかったファイルについては、前記ステップ 2812 において、前記ファイル識別プログラム 1932 は承認管理プログラム 1931 にエラーを返し、処理を終了する。

20

【0203】

次に、前記ファイル識別プログラム 1932 は、申請が一度承認者に保留された案件である場合（2813：Y）、保留された案件のファイルを記憶手段中から取得し（2814）、保留案件ファイルと今回の申請ファイルとの差分を特定する（2815）。

【0204】

また、新規申請の場合は（2813：N）、前記ファイル識別プログラム 1932 は、同じ持出先に対して持出し申請を行った履歴ファイルや過去却下されたファイルなどを承認管理 DB 1942 から抽出し、ここで抽出したもののうちから前記申請対象のファイルと最も類似するファイルを特定する（2816）。類似の判断基準としては、前記構造分析（ステップ 2812）で得ておいた、ファイルにおけるページ単位のヘッダフッタ情報やテンプレート情報（例：ファイル作成に利用している書式ひな形等）、テキスト情報などであり、前記ファイル識別プログラム 1932 は、これらについて一致するもの（であり、同じ持出先に対して持出し申請を行ったものや過去却下されたものなど）を前記承認管理 DB 1942 で検索する。こうした類似した他ファイルの特定を行ったファイル識別プログラム 1932 は、前記特定した他ファイルと前記申請対象ファイルとの差分を特定する（2817）。この差分特定により、例えば、前記他ファイルにおいても、同じ単語や文章が同じページ位置などに入力されているといった部分を特定しておくことで、過去において既に承認判断がなされたオブジェクト（＝他ファイルにおいて前記申請対象のファイルのオブジェクトと一致するオブジェクト）、に関しては新たな承認判断を省くことが出来る。なお、類似度が高いファイルがなかった場合には、差分取得処理を行わずに次の処理を実行する（2822）。

30

40

【0205】

次に、前記ファイル識別プログラム 1932 は、分析した申請対象のファイルのうち、1 ページのデータを選択し（2818）、照合用 DB 1943 を参照して前記ステップ 2817 で特定した差分部分における利用禁止オブジェクト（例：“極秘”などのテキスト）の有無と、利用禁止オブジェクトが含まれていた場合にはページ内の位置（例：該当ページの〇〇行目〇〇番目）を特定し、前記特定した検出位置をハイライトなどで強調表示する（2819）。なお、前記照合用 DB 1943 は、セキュリティ用語や人名、企業名、相手先個別の DB など複数に分類しておき、DB ごとに照合を行った結果を識別できる

50

ように保持しておくといよい。

【0206】

前記ファイル識別プログラム1932は、前記申請対象のファイルにおける全ページについて前記ステップ2819の処理を行うと(2820:Y)、前記検出した利用禁止オブジェクトの数をページ単位で比較し、利用禁止オブジェクトを含む数の多い順にページをリストアップする。これによって確認必要順を決定し(2821)、承認管理プログラム1931に結果(図25の詳細画面233における、プレビュー2461での確認必要順2459が押下された場合の表示形態)を送信して終了する。

【0207】

以上、ファイル識別プログラム1932では、既に承認(ないし却下)された他ファイルと申請対象のファイルとの差分を特定することにより、これまで持出し許可されたファイルにはない特徴を絞り込みし、さらに利用禁止オブジェクトの有無を検出することで承認者が確認すべきポイントを絞り込みすることができる。さらに、ページ単位でオブジェクトの検出数を比較し、検出数に基づいて確認優先順をつけることにより、承認者が確認すべきページを効率よく提示することができる。さらに、利用禁止オブジェクトの種類ごとに検出位置を特定することにより、ページのどの部分がどのカテゴリでリスクがあるのかを一目でわかるようにすることができる。

【0208】

次に、図29に基づき前記DB管理プログラム1934の処理フローについて説明する。前記DB管理プログラム1934は、承認判断が完了したときに承認結果にもとづいて照合用DB1943の更新を行うプログラムである。この場合、前記承認管理プログラム1931で承認者による承認結果を受信したのち(図27の2718)、DB管理プログラムは承認結果とファイル識別プログラム1932で分析した分析データとを取得する(241)。前記承認結果は、持出先の登録情報と承認/却下/保留のうちいずれかの承認結果を含む。また、前記分析データは、申請対象のファイルの構造データやテキスト情報などに加えて、照合用DB1943での利用禁止オブジェクトなどに該当するとして検出されたオブジェクトとその検出件数を含む。

【0209】

次に、前記DB管理プログラム1934は、前記承認結果から取得した持出先登録情報(例えば、持ち出し先の会社名やそのメールアドレス)より、持出先用の照合用DB1943が存在するか特定する(242)。持出先用の照合用DB1943が存在しない場合(242:N)、前記DB管理プログラム1934は新たに照合用DB1943を作成する(243)。

【0210】

続いて前記DB管理プログラム1934は、前記承認管理プログラム1931から取得した分析データについて、検出されたオブジェクトを検出数順に並び替えてリスト化する(244)。また前記DB管理プログラム1934は、前記承認結果が「承認」だった場合(245:Y)、検出されたオブジェクトを利用可能オブジェクトとして持出先用の照合用DB1943に登録する(246)。

【0211】

他方、前記承認結果が「却下」だった場合(245:N、247)、検出されたオブジェクトを利用不可オブジェクトとして持出先用の照合用DB1943に登録する(248)。このとき登録するデータは、却下理由が「内容上不適切」であった場合とし、前記詳細画面233(図25)において承認者が「不適切」と選択したオブジェクトがある場合は選択した部分のみ登録を行う。これは、句読点や漢字のミスなど表現上の不適切な部分については照合用DB1943へのオブジェクトの登録が不要であるためである。

【0212】

続いて、前記DB管理プログラム1934は、前記ステップ246、248らにおいて、検出された全てのオブジェクトを照合用DB1943に登録すると、現在承認管理サーバ193に登録されている持出先別の照合用DB1943を比較し(249)、あらかじ

10

20

30

40

50

め設定しておいた閾値以上の割合で各照合用DB1943に登録されたオブジェクトがあった場合には(250:Y)、汎用DB2104に登録する(251)。これにより、契約などにより相手先と共有しても問題ないオブジェクト等は相手先別の照合用DB1943で管理しておき、一方、統一的に管理されるべきオブジェクト(ファイル等を跨って共通に取り扱われるべきオブジェクト)については汎用DB2104で管理することができる。そのため、ファイルの持出先に合わせて、検出すべきオブジェクトを設定し、それを洗練させていくことができる。

【0213】

以上述べた第3実施例により、第1実施例および第2実施例に加えて、承認時に承認者が持出し申請されたファイルを持出してよいか判断しやすくなり、さらに、判断ミスを少なくすることが可能となる。

10

【0214】

以上、3つの実施例について説明したが、上記実施例に限定されるものではなく、その要旨を逸脱しない範囲において種々の変形が可能であるし、各実施例を組み合わせても良い。

【符号の説明】

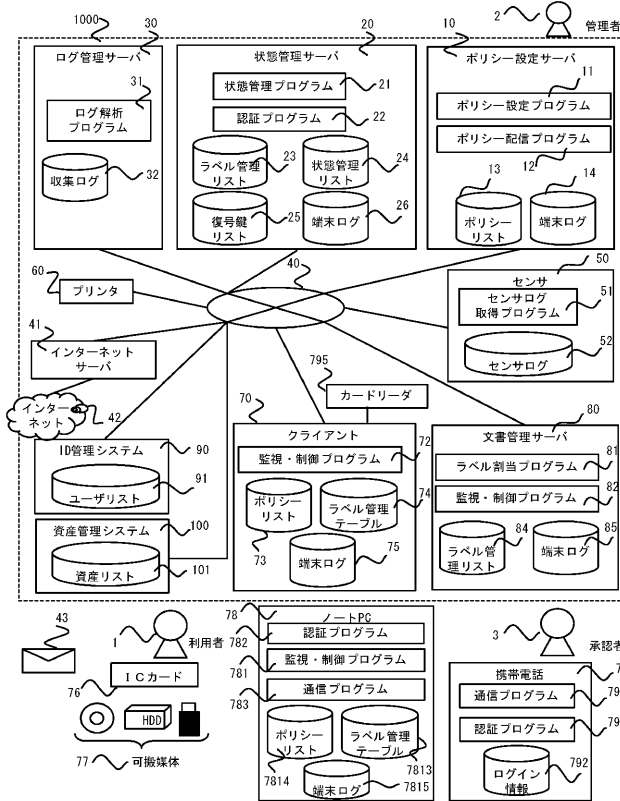
【0215】

1：利用者、2：管理者、3：承認者、10：ポリシー設定サーバ、11：ポリシー設定プログラム、12：ポリシー配信プログラム、13：ポリシーリスト、14：端末ログ、20：状態管理サーバ、21：状態管理プログラム、22：認証プログラム、23：ラベル管理リスト、24：状態管理リスト、25：復号鍵リスト、26：端末ログ、30：ログ管理サーバ、31：ログ解析プログラム、32：収集ログ、40：ネットワーク、41：インターネットサーバ、42：インターネット、43：電子メール、50：センサ、51：センサログ取得プログラム、52：センサログ、60：プリンタ、70：クライアント、72：監視・制御プログラム、73：ポリシーリスト、74：ラベル管理テーブル、75：端末ログ、76：ICカード、77：可搬媒体、78：ノートPC、781：監視・制御プログラム、782：認証プログラム、783：通信プログラム、7813：ラベル管理テーブル、7814：ポリシーリスト、7815：端末ログ、79：携帯電話、791：認証プログラム、792：ログイン情報、793：通信プログラム、80：文書管理サーバ、81：ラベル割当プログラム、82：監視・制御プログラム、84：ラベル管理リスト、85：端末ログ、90：ID管理システム、91：ユーザリスト、100：資産管理システム、101：資産リスト、192：メールサーバ、1921：メールログ、1911：申請管理プログラム、193：承認管理サーバ、1931：承認管理プログラム、1932：ファイル識別プログラム、1934：DB管理プログラム、1935：ファイル変換プログラム、1941：取引先リスト、1942：承認管理DB、1943：照合用DB、1944：持出しルールDB、7801：申請管理プログラム

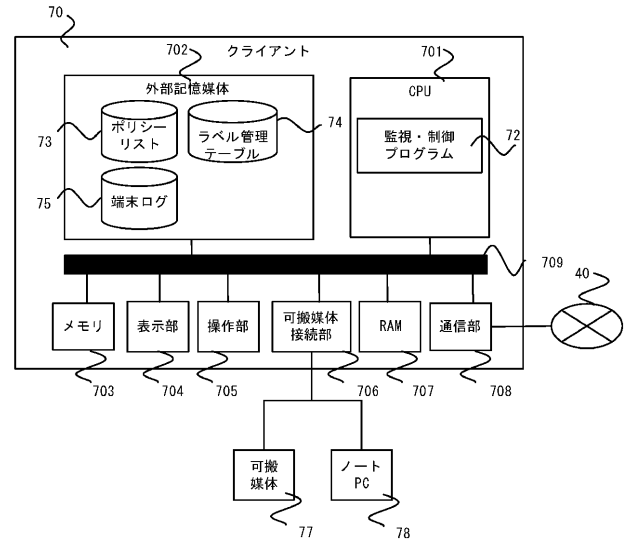
20

30

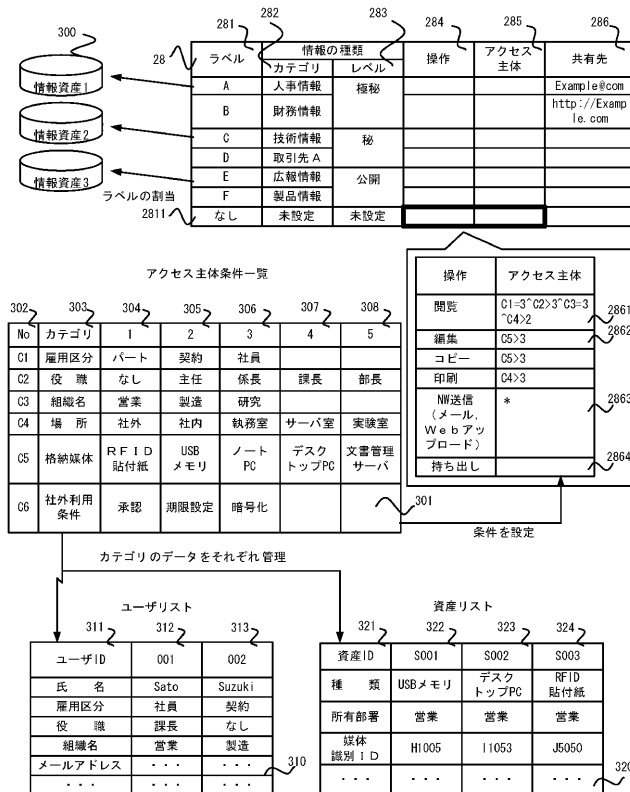
【図 1】



【図 2】



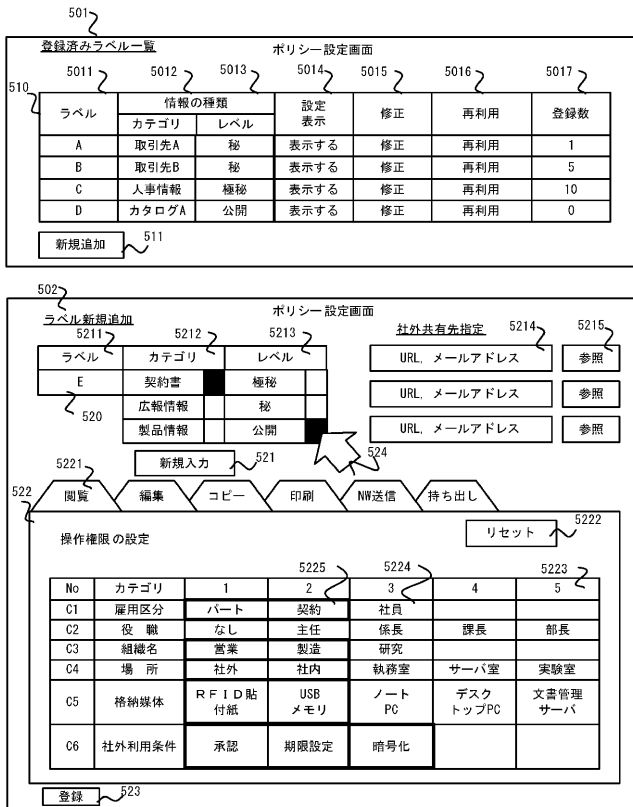
【図 3】



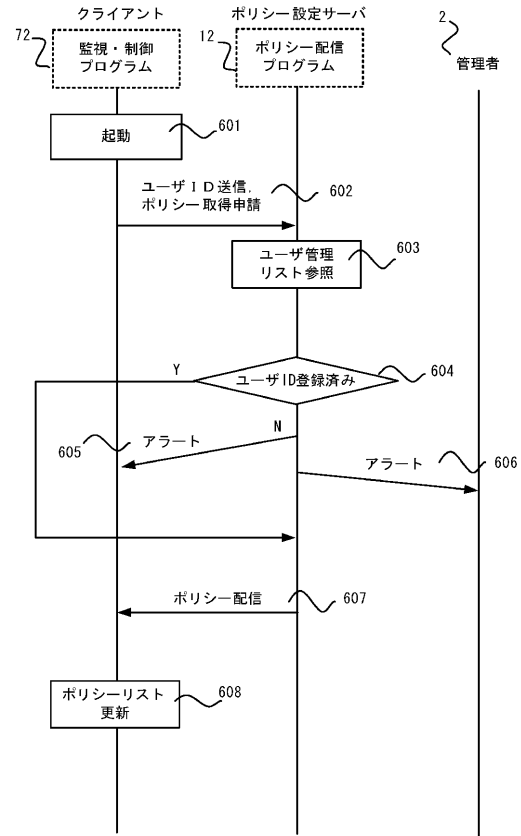
【図 4】

ラベル	情報の種類		操作	実行権限	共有先
	カテゴリ	レベル			
A	人事情報	極秘	閲覧	C1=3^C2≧4^C4=3^C5=4	
			編集	C1=3^C2≧4^C4=3^C5=4	
			コピー	C1=3^C2≧4^C4=3^C5=4	
			印刷	C1=3^C2≧4^C4=3^C5=4	
			NW送信	C1=3^C2≧4^C4=3^C5=4	
			持ち出し	(なし=操作禁止)	
B	カタログ情報	公開	閲覧	*	
			編集	(なし=上書き禁止)	
			コピー	C5=1	
			印刷	C4=2	
			NW送信	*	
C	取引先 A	秘	閲覧	C1≧2^C3=3(C3=1)^C4≧3^C5≧2	
			編集	C1≧2^C3=3(C3=1)^C4≧3^C5≧2	
			コピー	C1≧2^C3=3(C3=1)^C4≧3^C5≧2	
			印刷	C1≧2^C3=3(C3=1)^C4≧3	
			NW送信	C4≧3^C3=C3	Example@com
なし	未設定	未設定	持ち出し	C1=3^C3=3(C3=1)^C5=1^C5=3^C6	A 社東京オフィス
			閲覧	C4≧2^ID	
			編集	C4≧2^ID	
			コピー	C4≧2^C5≧4^ID	
			印刷	(なし=操作禁止)	
			NW送信	(なし=操作禁止)	
			持ち出し	(なし=操作禁止)	

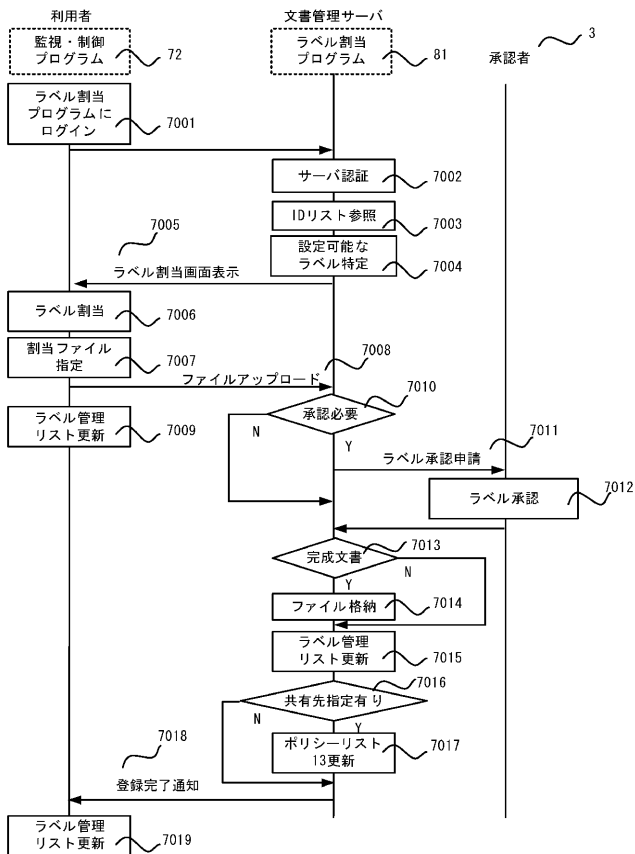
【図 5】



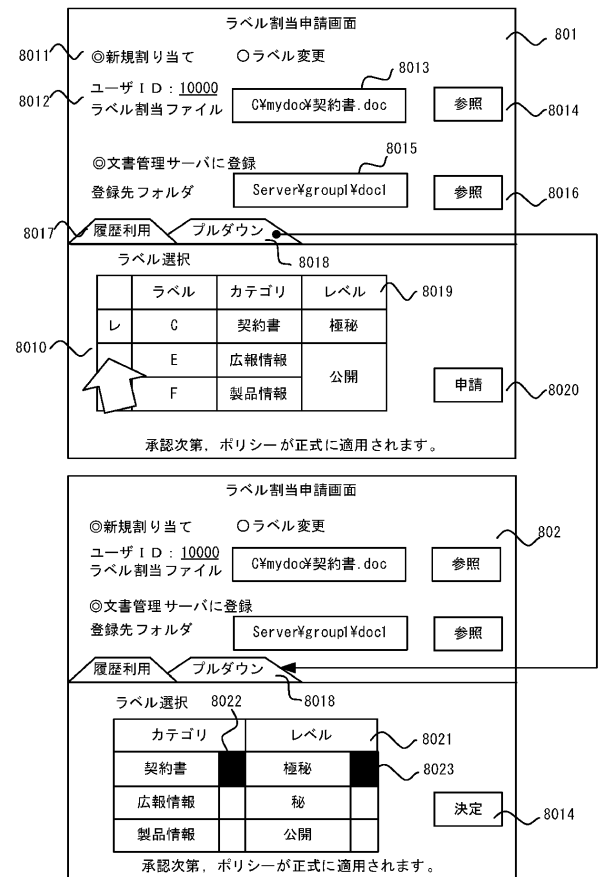
【図 6】



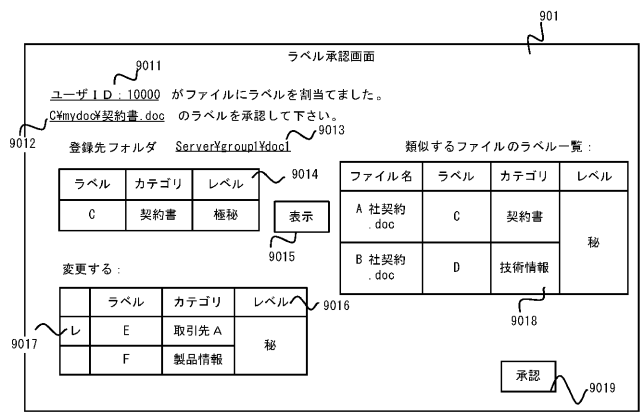
【図 7】



【図 8】



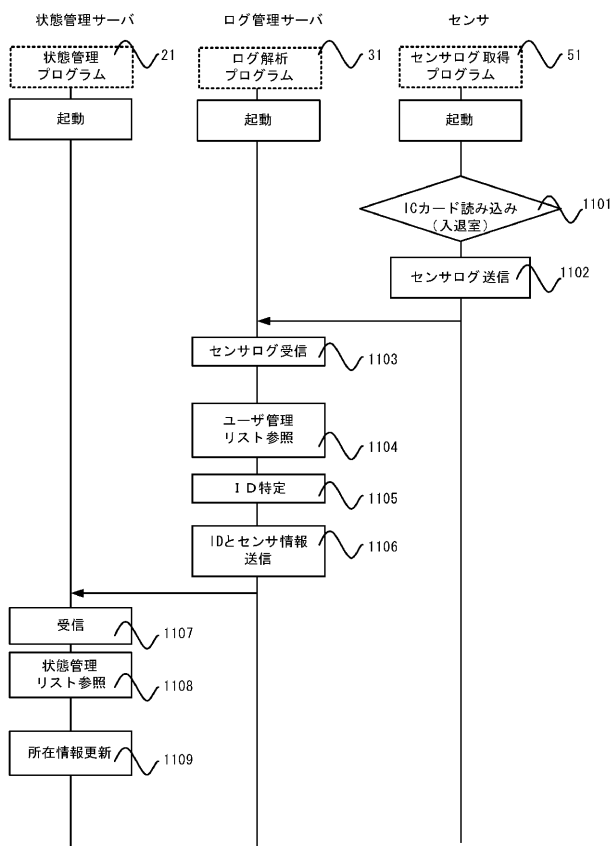
【図 9】



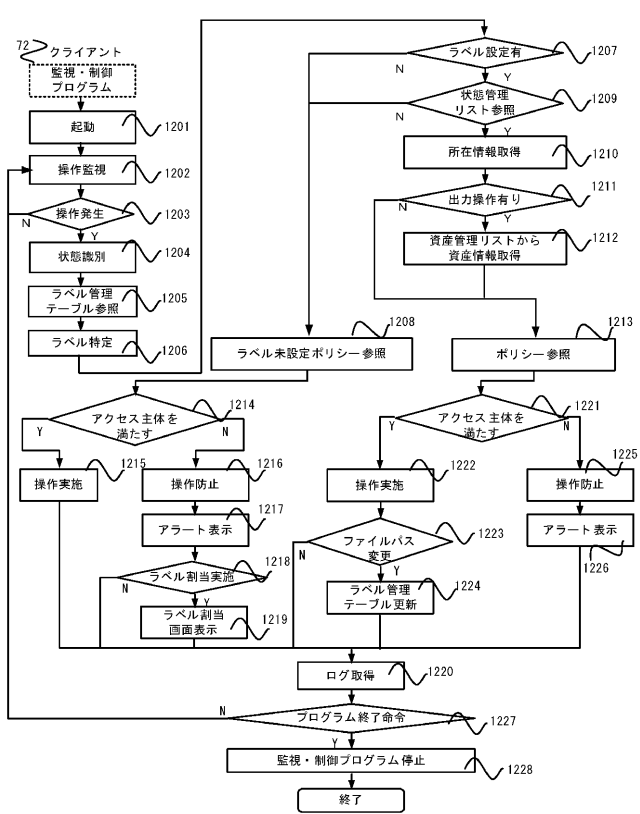
【図 10】



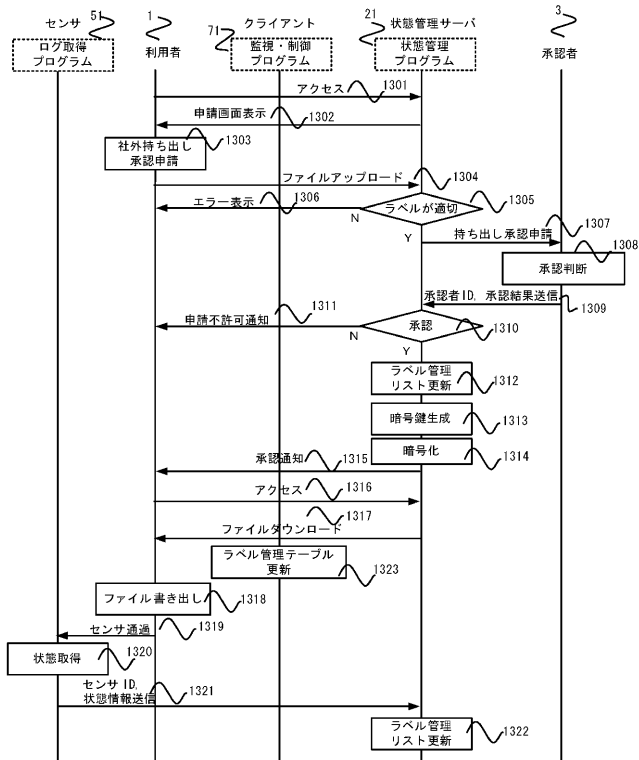
【図 11】



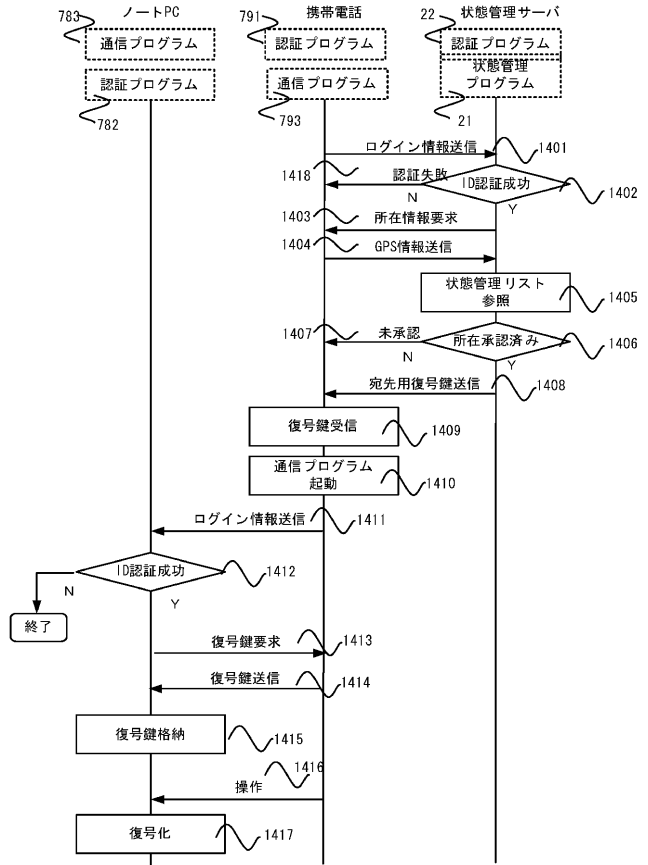
【図 12】



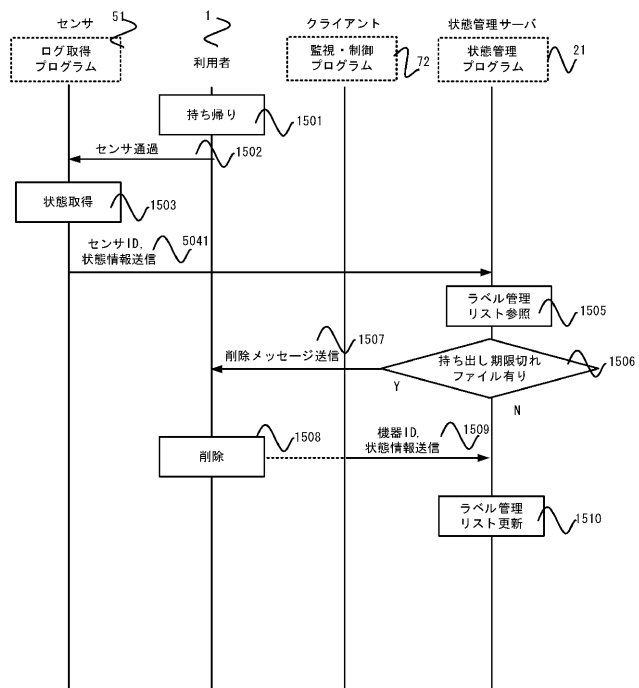
【図 13】



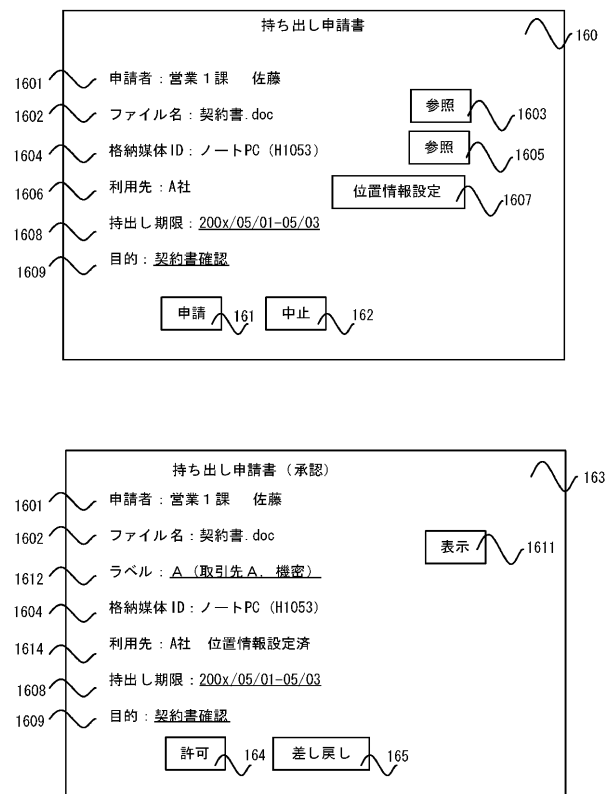
【図 14】



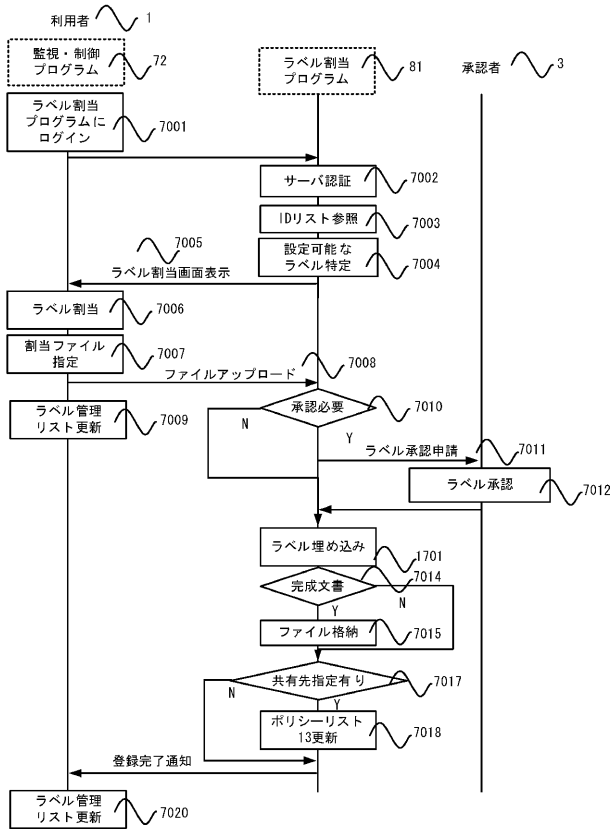
【図 15】



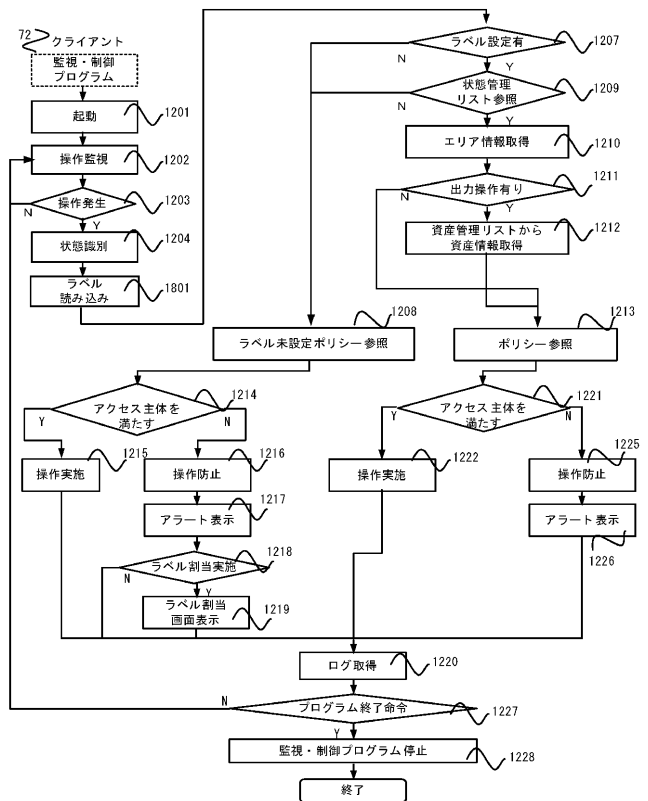
【図 16】



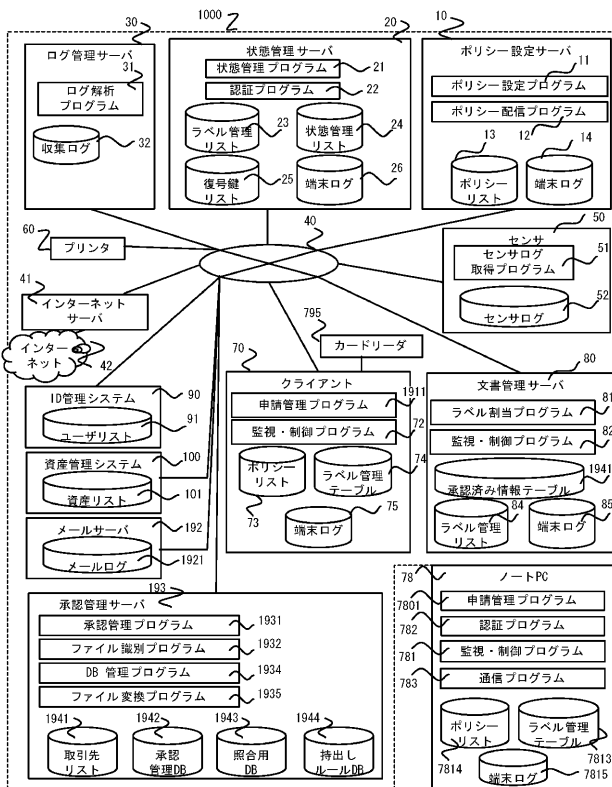
【図 17】



【図 18】



【図 19】

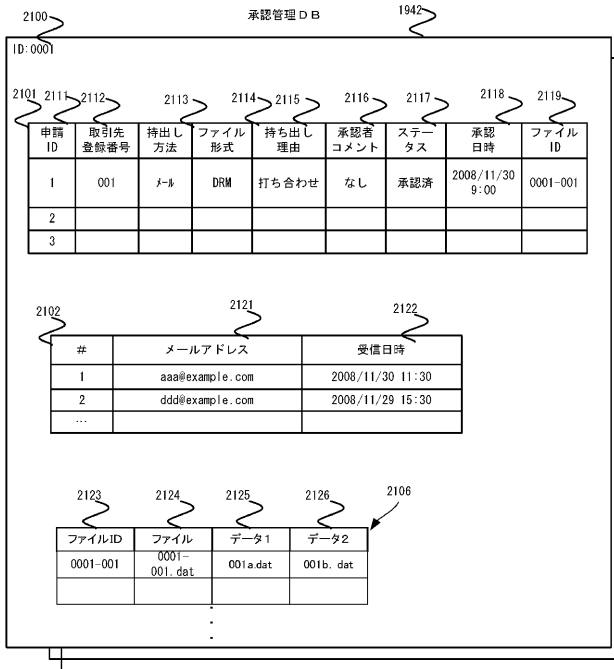


【図 20】

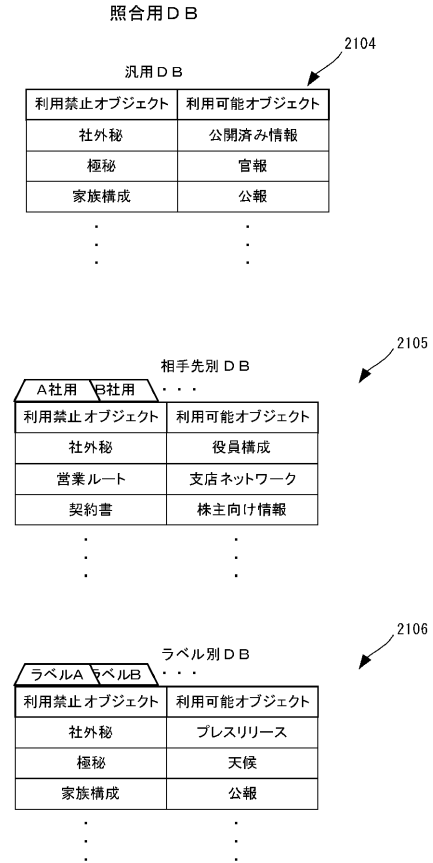
取引先リスト

登録番号	メールアドレス	取引先名	最終受信日時	承認回数	ユーザID
001	aaa@example.com	A社AAA	2008/12/01	0	1011
002	bbb@example.com	B社BBB	2008/11/30	5	2001
003	ccc@example.com	C社CCC	2007/10/01	1	1031
004	ddd@example.com	D社DDD	2008/12/10	0	2000
...					

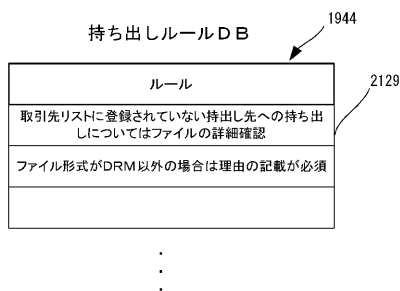
【図 2 1】



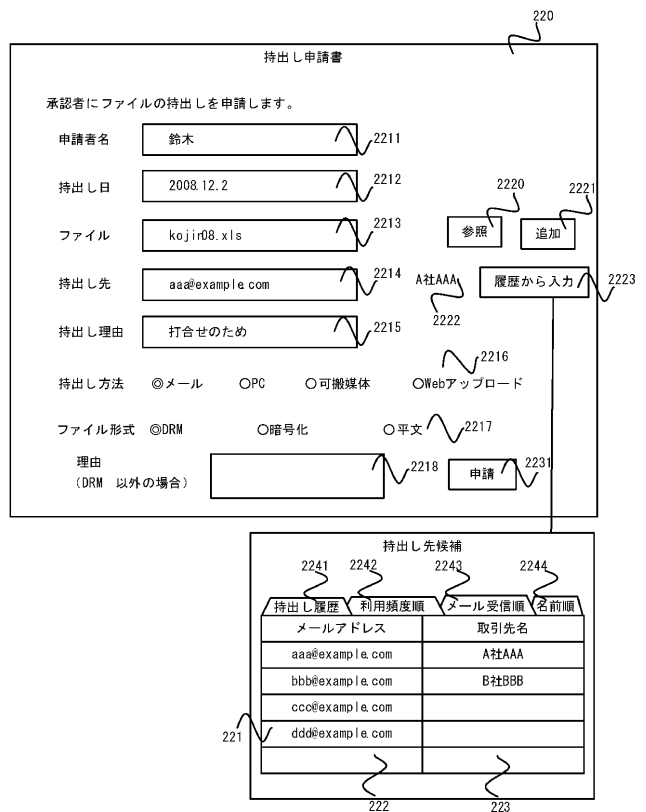
【図 2 2】



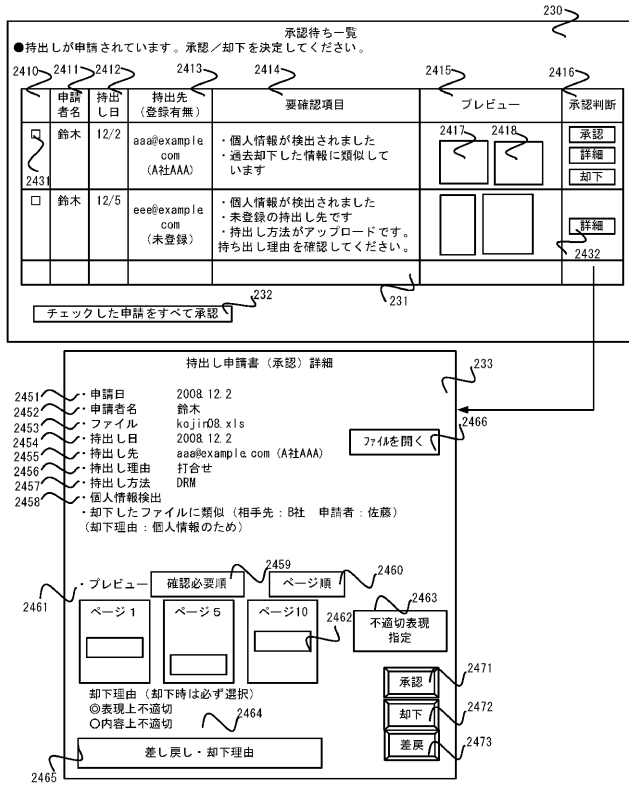
【図 2 3】



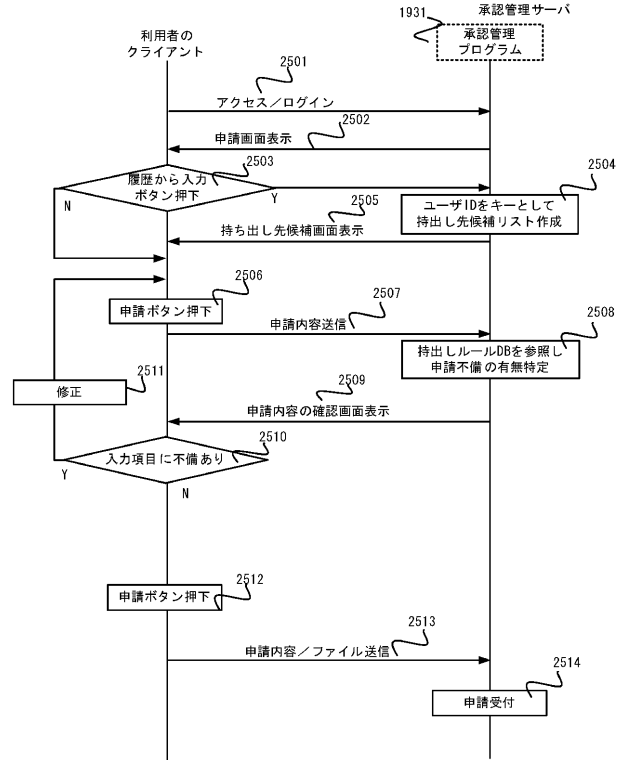
【図 2 4】



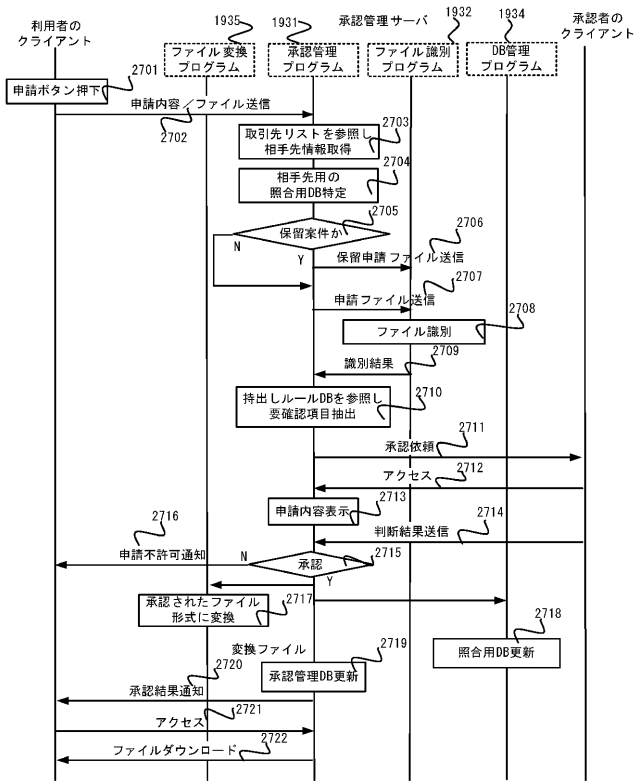
【図 25】



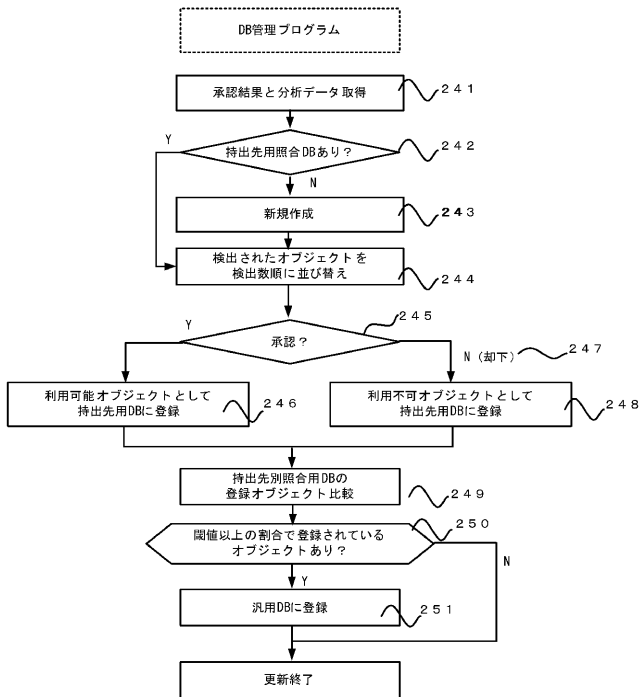
【図 26】



【図 27】



【図 29】



フロントページの続き

(51)Int.Cl.	F I	テーマコード (参考)
	G 0 6 F 17/30	1 2 0 A
	G 0 6 F 17/30	1 9 0
	G 0 7 C 9/00	Z

(72)発明者 笈川 光浩
神奈川県横浜市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所システム開発研究所内

(72)発明者 楠 拓也
神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所セキュリティ・トレーサビリティ事業
部内

(72)発明者 山口 演己
神奈川県川崎市幸区鹿島田 8 9 0 番地 株式会社日立製作所セキュリティ・トレーサビリティ事業
部内

F ターム(参考) 3E038 AA01 GA02 HA07
5B017 AA01 AA03 BA06 BA07 BB10 CA16
5B075 KK54 MM51
5B082 FA11 GA13