

(19) 日本国特許庁(JP)

(12) 特許公報(B2)

(11) 特許番号

特許第5274114号
(P5274114)

(45) 発行日 平成25年8月28日(2013.8.28)

(24) 登録日 平成25年5月24日(2013.5.24)

(51) Int.Cl.

G06F 21/62 (2013.01)
G06F 17/21 (2006.01)

F 1

G06F 21/24 163D
G06F 17/21 570M

請求項の数 18 (全 25 頁)

(21) 出願番号 特願2008-149364 (P2008-149364)
 (22) 出願日 平成20年6月6日 (2008.6.6)
 (65) 公開番号 特開2009-295009 (P2009-295009A)
 (43) 公開日 平成21年12月17日 (2009.12.17)
 審査請求日 平成23年6月6日 (2011.6.6)

(73) 特許権者 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 100126240
 弁理士 阿部 琢磨
 (74) 代理人 100124442
 弁理士 黒岩 創吾
 (72) 発明者 猪瀬 康二
 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

審査官 宮司 卓佳

最終頁に続く

(54) 【発明の名称】ドキュメント管理装置およびドキュメント管理方法並びにドキュメント管理システム

(57) 【特許請求の範囲】

【請求項 1】

ドキュメント管理装置と、ドキュメントに対してアクセス権であるポリシーを発行するポリシーサーバからなるドキュメント管理システムにおけるドキュメント管理装置であり、

前記ドキュメントに入力されたデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権記述を照合し、該照合の結果より、前記データが入力されたドキュメントに対するアクセス権記述を決定するアクセス権記述決定手段、

該アクセス権記述決定手段にて決定されたアクセス権記述を用いてポリシーの発行を前記ポリシーサーバに依頼する依頼手段、

前記ポリシーサーバから発行されたポリシーを前記データが入力されたドキュメントに適用させる適用手段、

を有することを特徴とするドキュメント管理装置。

【請求項 2】

前記アクセス権記述とは、予め前記ドキュメント管理装置に入力されるデータ及び該データが入力されるドキュメントを構成するテンプレート識別子とフィールド識別子に関するデータに対応して定義され、前記ドキュメントに対する権限内容が表記されていることを特徴とする請求項1に記載のドキュメント管理装置。

【請求項 3】

ドキュメント管理装置と、ドキュメントに対してアクセス権であるポリシーを発行する

10

20

ポリシーサーバからなるドキュメント管理システムにおけるポリシーサーバであり、前記ドキュメント管理装置から前記ドキュメントに入力されたデータ及び該データが入力されたドキュメントを構成するテンプレート識別子とフィールド識別子に関するデータを受信する受信手段、

該受信手段によって受信したデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権記述を照合し、該照合の結果より、前記データが入力されたドキュメントに対するアクセス権記述を決定するアクセス権記述決定手段、

該アクセス権記述決定手段にて決定されたアクセス権記述を用いてポリシーを前記ドキュメント管理装置へ発行する発行手段を有することを特徴とするポリシーサーバ。

【請求項 4】

前記入力されたデータが変更された際、

前記変更されたデータ及び該データを入力されたドキュメントに関するデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権の内容を照合し、

該照合の結果より前記データが変更されたドキュメントに対するアクセス権記述を変更するアクセス権記述変更手段、

前記アクセス権記述変更手段にて変更されたアクセス権記述を用いたポリシーの再発行を前記ポリシーサーバに依頼する再依頼手段、

前記再依頼手段によって依頼して取得したポリシーを、前記入力されたデータが変更されたドキュメントに対して用いるか否かを決定する決定手段を有することを特徴とする請求項 1 に記載のドキュメント管理装置。

【請求項 5】

さらに、

前記変更される前のデータを用いたアクセス権限記述と、前記アクセス権記述変更手段により変更されたアクセス権限記述に差があるか判断をする判断手段を有し、

該判断手段により差があると判断された場合に、前記アクセス権記述変更手段にて変更されたアクセス権記述を用いたポリシーの再発行を前記ポリシーサーバに依頼することを特徴とする請求項 4 に記載のドキュメント管理装置。

【請求項 6】

前記入力されたデータを用いて、前記ポリシーサーバにポリシーの発行が依頼できない場合、ユーザに再び入力の指示をするための表示を行う、またはポリシーの発行依頼を終了することを特徴とする請求項 1 に記載のドキュメント管理装置。

【請求項 7】

前記アクセス権記述を決める際に参照するフィールドの種類を、選択するフィールド選択手段、を有することを特徴とする請求項 1 に記載のドキュメント管理装置。

【請求項 8】

アクセス権記述決定手段を用いるか否かをユーザに決定させるための表示を行うことを特徴とする請求項 1 に記載のドキュメント管理装置。

【請求項 9】

ドキュメント管理装置と、ドキュメントに対してアクセス権であるポリシーを発行するポリシーサーバからなるドキュメント管理システムにおけるドキュメント管理装置を制御する方法であり、

アクセス権記述決定手段が、前記ドキュメントに入力されたデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権記述を照合し、該照合の結果より、前記データが入力されたドキュメントに対するアクセス権記述を決定するアクセス権記述決定ステップ、

依頼手段が、前記アクセス権記述決定ステップにて決定されたアクセス権記述を用いてポリシーの発行を前記ポリシーサーバに依頼する依頼ステップ、

適用手段が、前記ポリシーサーバから発行されたポリシーを前記データが入力されたドキュメントに適用させる適用ステップ、

を有することを特徴とするドキュメント管理装置を制御する方法。

10

20

30

40

50

【請求項 10】

前記アクセス権記述とは、予め前記ドキュメント管理装置に入力されるデータ及び該データが入力されるドキュメントを構成するテンプレート識別子とフィールド識別子に関するデータに対応して定義され、前記ドキュメントに対する権限内容が表記されていることを特徴とする請求項 9 に記載のドキュメント管理装置を制御する方法。

【請求項 11】

ドキュメント管理装置と、ドキュメントに対してアクセス権であるポリシーを発行するポリシーサーバからなるドキュメント管理システムにおけるポリシーサーバを制御する方法であり、

前記ドキュメント管理装置から前記ドキュメントに入力されるデータ及び該データが入力されるドキュメントを構成するテンプレート識別子とフィールド識別子に関するデータを受信する受信ステップ、

該受信ステップによって受信したデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権記述を照合し、該照合の結果より、前記データが入力されたドキュメントに対するアクセス権記述を決定するアクセス権記述決定ステップ、

該アクセス権記述決定ステップにて決定されたアクセス権記述を用いてポリシーを前記ドキュメント管理装置へ発行する発行ステップ

を有することを特徴とするポリシーサーバを制御する方法。

【請求項 12】

前記入力されたデータが変更された際、

アクセス権記述変更手段が、前記変更されたデータ及び該データを入力されたドキュメントに関するデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権の内容を照合し、該照合の結果より前記データが変更されたドキュメントに対するアクセス権記述を変更するアクセス権記述変更ステップ、

再依頼手段が、前記アクセス権記述変更ステップにて変更されたアクセス権記述に用いたポリシーの再発行を前記ポリシーサーバに依頼する再依頼ステップ、

決定手段が、前記再依頼ステップによって依頼して取得したポリシーを、前記入力されたデータが変更されたドキュメントに対して用いるか否かを決定する決定ステップを有することを特徴とする請求項 9 に記載のドキュメント管理装置を制御する方法。

【請求項 13】

さらに、判断手段が、前記変更される前のデータを用いたアクセス権限記述と、前記アクセス権記述変更ステップにより変更されたアクセス権限記述に差があるか判断をする判断ステップを有し、該判断ステップにより差があると判断された場合に、前記アクセス権記述変更ステップにて変更されたアクセス権記述を用いたポリシーの再発行を前記ポリシーサーバに依頼することを特徴とする請求項 12 に記載のドキュメント管理装置を制御する方法。

【請求項 14】

前記入力されたデータを用いて、前記ポリシーサーバにポリシーの発行が依頼できない場合、ユーザに再び入力の指示をするための表示を行う、またはポリシーの発行依頼を終了することを特徴とする請求項 9 に記載のドキュメント管理装置を制御する方法。

【請求項 15】

フィールド選択手段が、前記アクセス権記述を決める際に参照するフィールドの種類を選択するフィールド選択ステップ、を有することを特徴とする請求項 9 に記載のドキュメント管理装置を制御する方法。

【請求項 16】

前記アクセス権記述決定ステップを実行する否かをユーザに決定させるための表示を行うことを特徴とする請求項 9 に記載のドキュメント管理装置を制御する方法。

【請求項 17】

コンピュータに請求項 9 に記載の方法を実行させるためのプログラム。

【請求項 18】

10

20

30

40

50

コンピュータに請求項 1 1 に記載の方法を実行させるためのプログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は帳票などを作成する際にテンプレートにデータを入力し、そのデータに応じてドキュメント生成を行う、ドキュメント管理装置およびドキュメント管理方法並びにドキュメント管理システムに関するものである。

【背景技術】

【0002】

近年、ドキュメントの情報漏洩を防止するために、ドキュメントに対してアクセス権（10 閲覧権、編集権、印刷権など）を設定するアクセス権管理サーバが開発されている。

【0003】

このサーバでは、ドキュメントに対して有効期限も設定することができる。設定された有効期限を過ぎると、いかなるアクセス権が設定されていようとも、そのアクセス権が無効になる。

【0004】

ドキュメントに対するアクセス権管理サーバの一つとして、A d o b e 社のポリシーサーバ（LiveCycle E S R i g h t s M a n a g e m e n t（登録商標））が知られている。

【0005】

20

このポリシーサーバは、ドキュメントの一種である P D F（P o r t a b l e D o c u m e n t F o r m a t）ファイルのためのポリシーを発行し、適用させることで、上記のアクセス権設定、有効期限の設定を可能としている。

【0006】

ところで、企業内システムはサーバレス、分散処理型に移行しつつある。

【0007】

こうした状況下、多機能デバイスや P C を代表とする操作端末が、基幹業務に必要なドキュメント管理の多くを担うよう設計されたシステムも少なくない。

【0008】

基幹業務におけるドキュメント管理といえば、請求書や見積書、伝票など帳票の生成などはその代表である。

30

【0009】

帳票生成に必要なテンプレートの一種として例えば、ユーザが直接データ入力可能なフィールドを有する A d o b e 社の P D F フォームがある。

【0010】

操作端末上でそれを表示しフィールド入力、例えば見積書に顧客氏名や担当者名を入力し、専用サーバ等で帳票を生成することなく操作端末上でオンデマンドで帳票を作成し、ユーザへ送信する状況が容易に想定される。

【0011】

生成される帳票は、一般にその内容が特定のユーザに向けたものであることが多く、したがって適切にアクセス制限する必要がある。

40

【0012】

操作端末上に適切なポリシーが存在すればそれを適用すればよいのだが、操作端末上にあるポリシーはテンプレートが有するポリシーのみである。

【0013】

一般的に、オンデマンドで記載内容が変更されるテンプレートの性質からテンプレートに付与されるポリシーは任意のユーザが編集できる制限の小さいポリシーまたは、ポリシー自体が付与されていない。

【0014】

したがって、テンプレートに付与されたポリシーをそのまま帳票に適用することは適切

50

でない。

【0015】

この課題を解決することを目的とした技術として、例えば特許文献1に示されるように、ドキュメントを変更すると、変更箇所を暗号化することにより、閲覧可能なユーザと閲覧範囲を制御する技術がある。

【0016】

また、例えば特許文献2に示されるように、テンプレート上の特定のフィールドにデータを入力すると、そのデータの内容に応じて、テンプレートを元に生成される帳票へアクセス可能な端末を制御する技術がある。

【特許文献1】特開2003-6028号公報

10

【特許文献2】特開2004-178334号公報

【発明の開示】

【発明が解決しようとする課題】

【0017】

たとえば特許文献1に記載の技術を用いても、操作端末に保存されたドキュメントが多数ある場合、この多数のドキュメントに対して逐一システム管理者がアクセス制限をかけ（ポリシーを付与し）なければならない。これは、システム管理者にとって手間である。

【0018】

また、たとえば特許文献2に記載の技術を用いると、フィールドに入力したデータに応じて操作端末上のドキュメントのアクセス権を制御する（ポリシーを付与する）のでシステム管理者の手間はない。

20

【0019】

しかし、制御の対象は生成したドキュメントを閲覧や印刷することが可能な端末であり、任意の端末で閲覧、印刷することが想定される帳票などのドキュメントの制御には適さない。

【課題を解決するための手段】

【0020】

上述した課題を解決するために、本発明におけるドキュメント管理装置は、ドキュメント管理装置と、ドキュメントに対してアクセス権であるポリシーを発行するポリシーサーバからなるドキュメント管理システムにおけるドキュメント管理装置であり、

30

前記ドキュメントに入力されたデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権記述を照合し、該照合の結果より、前記データが入力されたドキュメントに対するアクセス権記述を決定するアクセス権記述決定手段、

該アクセス権記述決定手段にて決定されたアクセス権記述を用いてポリシーの発行を前記ポリシーサーバに依頼する依頼手段、前記ポリシーサーバから発行されたポリシーを前記データが入力されたドキュメントに適用させる適用手段を有することを特徴とする。

【0021】

また、本発明におけるポリシーサーバは、ドキュメント管理装置と、ドキュメントに対してアクセス権であるポリシーを発行するポリシーサーバからなるドキュメント管理システムにおけるポリシーサーバであり、前記ドキュメント管理装置から前記ドキュメントに入力されたデータ及び該データが入力されたドキュメントを構成するテンプレート識別子とフィールド識別子に関するデータを受信する受信手段、該受信手段によって受信したデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権記述を照合し、該照合の結果より、前記データが入力されたドキュメントに対するアクセス権記述を決定するアクセス権記述決定手段、該アクセス権記述決定手段にて決定されたアクセス権記述を用いてポリシーを前記ドキュメント管理装置へ発行する発行手段を有することを特徴とする。

40

【発明の効果】

【0022】

本発明により、任意の端末で閲覧や印刷をすることが想定されるテンプレートにデータ

50

が入力されることにより生成されるドキュメントに対して適切なポリシーを適用することが可能となる。そのため、ポリシーが発行されたドキュメントを速やかに得ることができ、セキュリティ上の問題を発生させない。

【0023】

また、テンプレートのフィールドに入力されるデータがユーザにより異なるようなオンデマンドで生成されるドキュメントに対して動的に、適切なポリシーに手間を掛けずに適用することが可能となる。

【0024】

この際、テンプレートのあるフィールドと、別のフィールドに入力されるデータの組合せが何パターンもあることが想定できるが、様々なパターンの組合せがドキュメントに入力された場合でも、適切なポリシーを発行することができる。

10

【0025】

したがって、システム管理者が個々のドキュメント内容を確認し、ポリシーを適用するといった手間を回避できる。

【発明を実施するための最良の形態】

【0026】

(実施例1)

以下では、本実施例において使用する言葉の定義を行う。

【0027】

(1) アクセスする

20

「ドキュメントにアクセスする」とは、

- ・ユーザからの表示指示に応じてクライアントコンピュータがドキュメントを表示する、
- ・ユーザからの編集指示に応じてクライアントコンピュータがドキュメントを編集する、
- ・ユーザからの印刷指示に応じてクライアントコンピュータがドキュメントの印刷命令を印刷機に送る

ことを含む。

この表示指示、編集指示、印刷指示のことをアクセス指示という。

【0028】

(2) アクセス権

「ドキュメントに対するアクセス権」とは、アクセス指示に応じた処理（ドキュメントに対する処理）をクライアントコンピュータに実行させるための権限である。

30

特定のユーザ又は任意のユーザからのアクセス指示に応じた処理（ドキュメントに対する処理）の実行がクライアントコンピュータに許可されている状態を、そのユーザは、そのドキュメントに対してアクセス権がある、という。

また、特定のユーザ又は任意のユーザのアクセス指示に応じた処理（ドキュメントに対する処理）の実行がクライアントコンピュータに禁止されている状態を、そのユーザは、そのドキュメントに対してアクセス権がない、という。

このアクセス権には、閲覧権と編集権と印刷権とが含まれる。

【0029】

(3) アクセス権を設定する

40

「アクセス権を設定する」とは、

概念的には、特定のユーザ又はその任意のユーザに対して、特定のドキュメントに対してアクセス権を与えることを示す。

処理的には、アクセス権とユーザ情報（ユーザ、または任意のユーザを指定する情報）とを関連付けるファイルを作成して保存すると共に、そのファイルを特定のドキュメントに対して適用することを言う。

【0030】

(4) ポリシー

「ポリシー」とは、

上記関連付けを示すファイルのこと。

50

従って、「ポリシーを作成して保存する」ということと、「そのポリシーをドキュメントに対して適用する」ということを合わせて「ドキュメントに対してアクセス権を設定する」ということを示す。

【0031】

(5) ポリシーサーバ

「ポリシーサーバ」とは、

ポリシーを作成して保存するサーバ装置。あるドキュメントに対するポリシーを作成して保存することを、(あるドキュメントのための)ポリシーを発行するともいう。

【0032】

(構成)

10

図1は、本発明を説明するのに最も適当な構成図である。

【0033】

ネットワーク101、クライアントコンピュータ102、ポリシーサーバ103、アクセス権決定サーバ104を示す。

【0034】

これらによってドキュメント管理システムが構成される。

【0035】

このネットワーク101は、上述の各装置間での情報のやり取りのための通信回線として働く。例えば、TCP/IPプロトコルなどをサポートする通信回線網であり、有線、無線と回線を問わない。

20

【0036】

クライアントコンピュータ102は、アクセス権制御部1021、ポリシー制御部1022、入力制御部1023、表示制御部1024からなるドキュメント管理装置である。

【0037】

アクセス権制御部1021は、アクセス権決定サーバ104に対して、ユーザが特定したデータなどから具体的なアクセス権記述、例えはどのユーザがどのような操作が可能か、などの情報を問い合わせる。

【0038】

ポリシー制御部1022は、例えはAdobe社のAcrobat(登録商標)などであり、アクセス権制御部1021にて取得したアクセス権記述をポリシーサーバ103に送信し、ポリシーの識別子を受信、ドキュメントに適用する。

30

【0039】

入力制御部1023はユーザによるデータ入力やダイアログ操作により指示された処理を行う。表示制御部1024はデータ入力用のインターフェース、メッセージ、ダイアログなどを表示する。

【0040】

アクセス権決定サーバ104はアクセス権決定部1041を有し、クライアントコンピュータ102から送信される情報に基づき具体的なアクセス権記述を決定し、クライアントコンピュータ102に送信する。

【0041】

40

なお、アクセス権決定部1041の配置はクライアントコンピュータ102上でもよい。

【0042】

その場合、クライアントコンピュータ102内でアクセス権制御部1021と協調しアクセス権記述を決定する。

【0043】

また、アクセス権決定部1041の配置はポリシーサーバ103上でもよい。その場合、ポリシーサーバ103内でアクセス権記述に基づきポリシーを生成、同識別子をクライアントコンピュータ102に送信する。

【0044】

50

しかしながら、本発明をわかりやすく説明するために以降では、図1に示す構成を前提とする。

【0045】

(アクセス権記述を決定する処理)

図6、図7、図8、図9、図11、図12を用いて、クライアントコンピュータ102がポリシーサーバ103に対してポリシーの発行を依頼する際に必要な、アクセス権記述を決定する処理を説明する。

【0046】

図6は、ユーザがクライアントコンピュータ102上にて、テンプレート中のフィールドにデータ入力操作を行う前のデータ入力画面である。

10

【0047】

図7は、ユーザがクライアントコンピュータ102上にて、テンプレート中のフィールドにデータ入力操作を行った後のデータ入力画面である。

【0048】

このようにして、テンプレート中のフィールドにデータが入力されることによって生成されたものをドキュメントと呼ぶ。

【0049】

図8は、アクセス権記述を決定するための情報が登録されているテーブルである。

このテーブルは、アクセス権決定部1041に存在する。

【0050】

また、このテーブルはシステムの管理者によって管理されるものであり、予めアクセス権決定部1041に保存されている。

20

【0051】

801はテンプレートの種類、802はフィールド名、803はフィールドに入力されるデータについて記載されている。

これらのデータによって定義されているのがアクセス権記述804である。

【0052】

この記述によって、あるテンプレートのフィールドにあるデータが入力された際のアクセス権の種類が定義つけられる。

【0053】

つまり、あるテンプレートのフィールドにあるデータが入力された際のユーザの権限内容が表記されている。

30

【0054】

例えば、見積書のフィールドである顧客名欄にnmX1、担当者欄にnmY1が入力されるとする。

【0055】

すると、この入力されたデータと、予めドキュメントに入力されるデータに対応して定義されているアクセス権記述を照合する。

【0056】

この照合結果より、

40

nmX1に対応する人物は閲覧可、nmY1に対応する人物は印刷可といった具体的なアクセス権の種類が定義付けがされていることがわかる。

【0057】

図9は、フィールドにデータ入力が完了し最終的にポリシーが適用され、生成されたドキュメントである。

【0058】

図11は、アクセス権制御部1021が主体となってアクセス権決定サーバ104に、具体的なアクセス権記述の決定を依頼する処理について説明するフローチャートである。

【0059】

図12は、アクセス権決定部1041にてアクセス権記述決定を行う処理について説明

50

するフローチャートである。

【0060】

図11を用いて、アクセス権記述の決定を依頼する処理を説明する。

【0061】

まず、S1101で処理を開始する。

【0062】

次に、S1102では、表示制御部1024が図6に示すような表示を行い、ユーザからのデータ入力を待機する。

【0063】

図6の601はユーザがデータを入力する画面を、602は生成するドキュメントのテンプレートをそれぞれ示す。 10

【0064】

603および604はユーザによるデータの入力が可能であるフィールドであり、データが未確定な状態を表す。

【0065】

図7は具体的に入力したデータが確定した状態を示した入力画面であり、701は601と同等、702は602と同等である。 20

【0066】

また、703、704はそれぞれ603、604に対して具体的なデータが確定した状態を表し、データが確定するとS1103に移行する。 20

【0067】

S1103では、データ入力用のインターフェースからユーザが入力したデータを、入力制御部1023が記録する。

【0068】

S1104にて、ユーザが入力したデータ、602のテンプレートを特定するテンプレート識別子、データを入力したフィールドを特定するフィールド識別子を入力制御部1023が受信する。そして、これらの情報をアクセス権決定サーバ104に送信する。 20

【0069】

アクセス権決定サーバ104にてアクセス権の内容を具体的に記述する、「アクセス権記述」を決定する処理は、図12にて後述する(S1201～S1205)として、S1105にてアクセス権の具体的な記述を受信する。 30

【0070】

S1106にて、アクセス権制御部1021が受信したアクセス権記述をポリシー制御部1022に引き渡し、処理を終了する。

【0071】

図12を用いて、アクセス権決定サーバ104にてアクセス権記述を決定する処理について説明する。

【0072】

まず、S1201で処理を開始する。

次に、S1202でユーザからのデータ入力を待機する。 40

S1203にて、クライアントコンピュータ102から、ユーザが入力したデータ、ドキュメントのテンプレートを特定するテンプレート識別子、データを入力したフィールドを特定するフィールド識別子を受信する。

S1204では、アクセス権決定部1041が、S1203にて受信した情報と、保存しているテーブルである図8の801、802、803を照合する。

保存するテーブルに合致する全てのデータと関連付いた804のアクセス権限記述に記載された定義が存在する場合、S1205でその定義をクライアントコンピュータ102に送信する。

【0073】

例えば、テンプレートを特定する識別子として702に例示した“見積書”を受信し 8

50

01と照合する。

【0074】

そして、データとして703に例示した“nmX1”およびフィールド識別子として“顧客名”を受信し、802および803と照合する。

【0075】

ならびにデータとして704に例示した“nmY1”およびフィールド識別子として“担当者”を受信し、802および803と照合する。

【0076】

すると、801、802、803全てと合致するデータと関連付いた、804に示すアクセス権記述が存在する。すなわち『“顧客名”としてフィールドに内に入力された名前のユーザ“nmX1”は閲覧可能、“担当者”としてフィールド内に入力された名前のユーザ“nmY1”は印刷可能』という定義が存在する。

【0077】

これを基に『“顧客名”である“nmX1”氏は閲覧可能、“担当者”である“nmY1”氏は印刷可能』あるいはこれと同等の意味の情報をクライアントコンピュータ102に送信する。

【0078】

受信したクライアントコンピュータ102のアクセス権制御部1021は前述した通り、受信した情報をポリシー制御部1022に引き渡す。

【0079】

つまり、テンプレートである見積書のフィールド部分の顧客名欄に“nmX1”担当者欄に“nmY1”と入力されることによって生成されたドキュメントに対して、適切なアクセス権記述を定義することが可能である。

【0080】

この場合、テンプレートのフィールド部分の種類と、フィールドに入力されるデータの組合せは何通りもある。

【0081】

この何通りもある組合せが入力されるドキュメントに対して、それぞれ詳細にアクセス権限記述を定義することによって、どんな組合せの入力があっても、それに適切に対応したポリシーの発行依頼が可能になる。

【0082】

なお、アクセス権決定部1041を構成する、図8に示すアクセス権記述を決定するための情報は、テンプレートが保持してもよい。

【0083】

その場合、クライアントコンピュータ102がアクセス権記述を決定する。

【0084】

また、アクセス権決定部1041が、ポリシーサーバ103中にある場合、クライアントコンピュータにて入力されたデータをポリシーサーバ中のアクセス権決定部へ送信する。

【0085】

そして、アクセス権決定部で決定されたアクセス権記述の定義に基づいてポリシーサーバがポリシーを発行する。

【0086】

(アクセス権記述に基づきポリシーを発行する処理)

以上のようにして決定されたアクセス権に基づきポリシーを発行する処理について、説明する。

【0087】

図2は、ポリシーサーバ103がポリシーを発行する際のフローチャート、図3はクライアントコンピュータ102がドキュメント(例えば、PDFファイル)に対して、そのポリシーを適用する際のフローチャートである。

10

20

30

40

50

【 0 0 8 8 】

ユーザからのポリシー作成指示を受けると、クライアントコンピュータ102は、その旨をポリシーサーバ103に送信する。

【 0 0 8 9 】

なお、このポリシー作成指示には、「ポリシーを作成して下さい」という指示と、「その作成して欲しいポリシーとはどのようなポリシーです」というのを示す指示とが含まれる。

【 0 0 9 0 】

この「作成して欲しいポリシーは、どのようなポリシーです」を示す指示とは、言い換えると「各ユーザに対してどのようなアクセス権を設定すべきか」を示し、上述したアクセス権記述のことである。

10

【 0 0 9 1 】

このポリシー作成指示をポリシーサーバ103が受信すると、S201の処理が開始する。

【 0 0 9 2 】

S201では、ポリシーサーバ103は指定されたドキュメントのために、上記ポリシー作成指示に基づくポリシーを作成して保存する。

【 0 0 9 3 】

なお、このポリシーはどのユーザIDを持つユーザにどのようなアクセス権が設定されるかを示すファイルとなっている。

20

【 0 0 9 4 】

言い換えると、ユーザ情報とアクセス権との関連付けを示すファイルとなっている。

【 0 0 9 5 】

S202では、ポリシーサーバ103は、ポリシーサーバ識別情報（ポリシーサーバを一意に識別するための情報。例えばIPアドレス）と、ポリシー識別情報（ポリシーサーバに保存されるポリシーを識別するための情報。例えばID）とを含むドキュメントライセンスを作成する。

【 0 0 9 6 】

S203では、ポリシーサーバ103はドキュメントライセンスに電子署名を行い、データの整合性を確保する。

30

【 0 0 9 7 】

さらに、ポリシーサーバ103は、ドキュメントを暗号化するために後に使用するドキュメントキー（一種の暗号キー）を作成する。

【 0 0 9 8 】

このドキュメントキーは、ポリシーを適用するドキュメント毎に作成されるものであり、本実施例では、指定されたドキュメントのための唯一無二のドキュメントキーということになる。

【 0 0 9 9 】

S204では、ポリシーサーバ103は、S201で作成されたポリシーを暗号化する。

40

【 0 1 0 0 】

S205では、ポリシーサーバ103は、ドキュメントライセンス、ドキュメントキー、暗号化されたポリシーの夫々を関連付けてクライアントコンピュータ102に送信する。さらに、このS205では、クライアントコンピュータ102に送信した暗号化されたポリシーと、ポリシー識別情報と、ドキュメントキーとを、関連付けた上でポリシーサーバ103の内部に保存する。

【 0 1 0 1 】

S301では、クライアントコンピュータ102は、ポリシーサーバ103から、夫々関連付けられているドキュメントライセンス、ドキュメントキー、暗号化されたポリシーを受信する。すると、Adobe社のAcrobat（登録商標）のインストールされて

50

いるクライアントコンピュータ 102 内のポリシー制御部 1022 は、受信したポリシーを上記指定されたドキュメントに対して適用する。

【0102】

この適用の処理を S302、S303、S304 に示す。

【0103】

まず、S302 では、クライアントコンピュータ 102 内のポリシー制御部 1022 は、受信したドキュメントキーを使用してドキュメントを暗号化する。この暗号化が終了すると、S303 に移行する。

【0104】

S303 では、クライアントコンピュータ 102 内のポリシー制御部 1022 は、暗号化の終了によりドキュメントキーが不要になったと判断し、ドキュメントキーを破棄する。

【0105】

S304 では、クライアントコンピュータ 102 内のポリシー制御部 1022 は、暗号化されたドキュメントに対してドキュメントライセンスと、暗号化されたポリシーとを埋め込む。これにより、ドキュメントに対するポリシーの適用の処理が終了する。

【0106】

このようにして、テンプレートの種類と入力データによって定義されたアクセス権記述に基づいて発行されたポリシーが、テンプレートから生成されたドキュメントに対して適用される。

10

20

【0107】

(オンライン環境で使用するドキュメントへのアクセス)

オンライン環境で使用するドキュメントへのアクセスは本発明に直接関係しないが、上述した「アクセス権記述を決定する処理」の裏づけとなるため、説明する。

【0108】

図 4 はオンライン環境での使用を必要とするポリシーが適用されたドキュメントにアクセスする際のフローチャートである。

【0109】

なお、本実施例では、ドキュメントにアクセスする装置（即ち、図 4 の処理の主体）が、ポリシーをドキュメントに適用した装置（即ち、図 3 の処理の主体）と、たまたま同じものであるとして説明を行う。即ち、図 4 の処理の主体が、クライアントコンピュータ 102 であるものとして説明を行う。ただし、図 3 の処理の主体と図 4 の処理の主体とが異なっていたとしても、図 3 で説明された処理も図 4 で説明する処理も、何ら変わることはない。

30

【0110】

ユーザから、ポリシーが適用されているドキュメントを開くための指示がポリシー制御部 1022 に指示されると、以下の処理が行われる。

【0111】

S401 では、ポリシーが適用されているドキュメントにアクセスする為に、ポリシー制御部 1022 が、ネットワーク 101 を介してポリシーサーバに接続を行う。

40

【0112】

なお、ポリシー制御部 1022 は、そのドキュメントに適用されているポリシーを保存するポリシーサーバとそのポリシーを、そのドキュメントに埋め込まれたドキュメントライセンスに従って見つけ出すものとする。ここで、ドキュメントライセンスとは、ポリシーサーバ識別情報、ポリシー情報情報を含む。

【0113】

なお、今回の例では、そのポリシーサーバ識別情報によって識別されるポリシーサーバは、ポリシーサーバ 103 であるものとする。また、そのポリシー識別情報によって識別されるポリシーは、S205 でポリシーサーバ 103 の内部にポリシー識別情報と関連付けて保存されたポリシーである。

50

【0114】

さらに、この接続に際して、クライアントコンピュータ102内のポリシー制御部102が、ユーザから受けたユーザIDとパスワードとをポリシーサーバ103に送信するものとする。

【0115】

S402では、ポリシーサーバ103は、クライアントコンピュータ102内のポリシー制御部102から送られてきたユーザIDでの認証を行う。

【0116】

この認証が成功すると、ポリシーサーバ103は上記ポリシー識別情報により識別（特定）されるポリシーの内容を確認して、図5にて後述する証明書ファイルをポリシー制御部102に送信する。
10

【0117】

このS402の処理の詳細を、S501、S502、S503、S504に示す。図5はポリシーサーバ103で行われるポリシーの認証処理を示したフローチャートである。

【0118】

S501では、ポリシーサーバ103は、クライアントコンピュータ102から受信したユーザIDでの認証（正しいパスワードが入力されているかの確認）を行う。

【0119】

この上で、そのユーザIDに対応付けられて（ポリシーサーバ103に）保存されているユーザ情報を取得する。
20

【0120】

S502では、ポリシーサーバ103は、見つけ出されたポリシーと、S501で取得したユーザ情報を照合し、上記ユーザIDを有するユーザの上記ドキュメントに対するアクセス権（上記ユーザ情報のユーザのアクセス権）を確認する。また、ポリシーサーバ103は、S205で保存されたドキュメントキー（上記ポリシーと関連付けられているドキュメントキー）を保存場所から読み出す。

【0121】

S503では、ポリシーサーバ103は、上記ドキュメントキーと上記ユーザ情報により特定されるユーザのアクセス権とを含む証明書ファイルを作成する。

【0122】

S504では、ポリシーサーバ103は、クライアントコンピュータ102に、S503で作成した証明書ファイルを送信する。
30

【0123】

S403では、クライアントコンピュータ102うちのポリシー制御部102は、ポリシーサーバ103から送信された証明書ファイルを受信し、ドキュメントへのアクセスを開始する。

【0124】

S404では、ポリシー制御部102は、証明書ファイルに含まれるドキュメントキーを使用し、その証明書ファイルに対応する上記ドキュメントの複合化を行う。この複合化が終了すると、S405に移行する。
40

【0125】

S405では、ポリシー制御部102は、上記ドキュメントの複合化が終了したドキュメントキーを破棄する。

【0126】

S406では、ポリシー制御部102は、証明書ファイルに含まれるアクセス権に応じて、ドキュメントへのアクセスを制御する。

即ち、アクセス権で許可されている処理のみ、ポリシー制御部102は実行することが出来る。

【0127】

また、クライアントコンピュータ102は、ドキュメントへのアクセスが終了した時点
50

で証明書ファイルを破棄する。

【0128】

以上のようにして、オンライン環境で使用するドキュメントへのアクセスの制御が行われる。

【0129】

(実施例2)

実施例1では、ポリシーが発行されていなかったテンプレートに対して、フィールドにデータが入力された際、そのデータに応じてアクセス権の内容を決定し、それに基づいてドキュメントにポリシーを発行することを可能にした。

【0130】

本実施例2では、ドキュメントにて入力データが変更された場合について述べる。この場合、変更されたデータに適したアクセス権記述が、データ変更前のアクセス権限と異なることがあるため、ドキュメントに対して、データ変更後のアクセス権記述に従ったポリシーを付与することを可能にする。

10

【0131】

図13～図17を用いて、ドキュメントにポリシーを適用する前に、ユーザが入力するデータによって、アクセス権決定サーバ104から得られるアクセス権記述が異なる場合について述べる。

【0132】

この場合、アクセス権の差異に応じてユーザインターフェースを変化させ、ユーザが実施可能な指示を制御し、ユーザの指示に応じた制御を行う。

20

【0133】

この一連の処理について説明する。

【0134】

図13、図14はユーザがデータ入力操作を行った後のドキュメントを示した入力画面である。

【0135】

ただし、これらはポリシーを確定させる前のデータ入力画面である。

【0136】

図15は、入力したデータにより決まるポリシーをドキュメントに適用する処理まで進むか、それとも確認に留めるかの選択を表示するユーザインターフェースを示す。これにより、ユーザによる選択指示を受信することが可能である。

30

【0137】

図16はポリシーに差異が生じる旨を表示し、ユーザによる確認指示が可能なユーザインターフェースを示す。

【0138】

図17は一連の処理を説明するフローチャートを示す。

図17を用いて、一連の処理を説明する。

【0139】

先ず、S1701で処理を開始する。

40

次にS1702では、表示制御部1024が図13に示すような表示をし、ユーザからのデータ入力を待機する。

【0140】

図13の1301はユーザがデータを入力する画面を、1302は生成するドキュメントのテンプレートをそれぞれ表す。

【0141】

1303と1304はユーザによるデータの入力が可能であるフィールドであり、それぞれデータが確定した状態を表す。データが確定するとS1703に移行する。

【0142】

S1703では、ユーザがデータ入力用のインターフェースから入力したデータを入力

50

制御部 1023 が記録する。

【0143】

S1711 では、表示制御部 1024 が図 15 の 1501 に示すメッセージを表示し、S1712 ではユーザからの指示を待機する。

【0144】

ユーザが 1502 の受信予定のアクセス権記述でポリシーを適用するという指示、あるいは 1503 のポリシーの適用までは行わずアクセス権記述の確認のみという指示のいずれを行っても S1704 へ進む。

【0145】

S1704 では、実施例 1 にて述べたようにユーザが入力したデータ、1302 を特定するテンプレート識別子、データを入力したフィールドの識別子をアクセス権決定サーバ 104 に送信する。

【0146】

そして、アクセス権決定サーバ 104 から具体的なアクセス権記述を取得する。

【0147】

S1705 では、S1712 でのユーザ指示がアクセス権記述の確認のみかアクセス権記述に基づきドキュメントにポリシーを適用するか、いずれかの判断を行う。

【0148】

つまり、ユーザから 1502 の「ポリシーの適応」の指示を受信していた場合、新たなアクセス権記述に基づきドキュメントに対して新たにポリシーを発行する。

【0149】

一方、ユーザから 1503 の「ポリシーの確認」の指示を受信していた場合、新たにポリシーは発行しないで、確認に留める。

【0150】

アクセス権記述の確認のみと判断された場合、S1706 で受信したアクセス権記述を記録する。

【0151】

S1707 では直前に記録したアクセス権記述の有無を確認する。

【0152】

直前に記録したアクセス権記述があれば、S1708 にてアクセス権記述の内容を比較する。

【0153】

つまり、一度アクセス権記述が適用されていたものであれば、新たなアクセス権記述の内容と以前のアクセス権記述の内容を比較する。

【0154】

上記 2 つのアクセス権記述に差異があればポリシーが変更されるので、S1709 にて、差異に応じたユーザインターフェースを作成する。

【0155】

図 16 がその 1 例であり、1601 が、アクセス権記述の差異に起因して、結果としてドキュメントに適用するによるポリシーに差異が生じる旨のメッセージである。

【0156】

また、1602 がユーザによる確認指示のためのボタンである。

【0157】

S1710 ではユーザの指示に応じた処理を行う。

【0158】

つまり、S1705 で「確認のみ」が選択されていればポリシーの変更は行わず、「適応」がされていればポリシーの変更が行われる。

【0159】

なお、S1707、S1708 にてアクセス権記述の内容を比較したが、これを行わず、フィールドに新たなデータが入力されデータが変更されるごとに、変更されたデータに

10

20

30

40

50

対応したアクセス権限記述を受信してもよい。

【0160】

図13と図14を用いて、S1707の処理をより詳細に説明する。

【0161】

1401は1301と同等のテンプレート入力画面を示す。1402は1302と同等のテンプレートを示す。1403は1303と同等、1404は1404と同等のフィールドを示す。ただし、1303への入力データと1403への入力データは異なる。

【0162】

図13に示すデータ入力に基づきアクセス権決定サーバ104から取得するアクセス権の記述を前記“直前に記録したアクセス権記述”とし、図14に示すデータ入力に基づきアクセス権決定サーバ104から得られるアクセス権記述と比較とする。(S1708)

10

この場合1303のデータと1403のデータが異なっているがゆえに、両アクセス権記述に際が生じる。この際にS1709に移行することになる。

【0163】

以上のように、一度ポリシーを発行してもテンプレート中の入力データが変更されると、それに対応してアクセス権記述変更が行われる。

【0164】

その新たなアクセス権記述に基づいて、クライアントコンピュータ102は、ポリシーサーバ103に新たなポリシーを再依頼することができる。この再依頼を受けたポリシーサーバは、入力データが変更されたドキュメントに対して新たなポリシーを再発行することができる。

20

【0165】

したがって、オンデマンドで生成されるドキュメントに対して動的に適切なポリシーを適用することができる。

【0166】

(実施例3)

実施例1及び2では、アクセス権記述を決定するために必要な情報が得られるため、そのアクセス権限に従ったポリシーをドキュメントに対して付与することができた。

【0167】

本実施例では、このアクセス権記述を決定するために必要な情報が得られない場合の処理について述べる。

30

【0168】

なお、この本実施例は、実施例1および2と同時に利用することができる。

【0169】

図18、図19を用いて、アクセス権記述を決定するために必要な情報が得られない場合の処理について説明する。

【0170】

図18はアクセス権記述を決定できない旨を表示し、ユーザによる確認指示が可能なユーザインターフェースである。

40

【0171】

図19は本処理を説明するフローチャートを示す。

【0172】

図19を用いて、アクセス権記述を決定するために必要な情報が得られない場合の処理について述べる。

【0173】

まず、S1901で処理を開始する。

次に、S1902では、表示制御部1024が図6に示すような表示を行い、ユーザからのデータ入力を待機する。

【0174】

例えば図6の603、604に示すデータ入力画面にてユーザによってデータが入力さ

50

れ、そのデータが確定すると S 1 9 0 3 に移行する。

【 0 1 7 5 】

S 1 9 0 3 ではユーザによって入力されたデータを記録する。

【 0 1 7 6 】

ユーザ指示により S 1 9 0 4 では、入力したデータ、テンプレートを特定する識別子、およびデータを入力したフィールドの識別子をアクセス権決定サーバ 1 0 4 に送信する。

【 0 1 7 7 】

ここで、アクセス権決定サーバ 1 0 4 にて上述したアクセス権記述を決定する処理を実施し、アクセス権記述を決定できなかった場合、アクセス権記述は空であると判断する。

【 0 1 7 8 】

S 1 9 0 5 ではアクセス権記述を受信し、

S 1 9 0 6 ではアクセス権記述が空であるか否かを判定する。

【 0 1 7 9 】

空である場合は S 1 9 0 7 で、1 8 0 1 に示すメッセージを表示し、1 8 0 2 に示す確認指示のボタンを有するユーザインターフェースを生成する。

【 0 1 8 0 】

S 1 9 0 9 にて、ユーザが確認を指示すると再びデータ入力画面に戻る。

【 0 1 8 1 】

S 1 9 0 6 にてアクセス権記述が空でないと判定された場合は、S 1 9 0 8 にてアクセス権記述をポリシー制御部 1 0 2 2 に引き渡し、処理を終了する。

【 0 1 8 2 】

なお、アクセス権決定サーバ 1 0 4 にてアクセス権記述が見つからなかった場合の、クライアントコンピュータへ送信する情報は必ずしも空でなく、同義のデータであればその形式を問わない。

【 0 1 8 3 】

以上の実施例によって、テンプレートのフィールド内にて適切なデータが入力されなかった場合に、ポリシーを発行させない、またはユーザに適切なデータを入力することを知らせることが可能になる。

【 0 1 8 4 】

(実施例 4)

本実施例では、アクセス権記述を動的に決定する機能を有効にするための設定について説明する。

【 0 1 8 5 】

本実施例は、上述した実施例 1 ~ 3 と同時に利用することが可能である。

【 0 1 8 6 】

図 1 0 を用いてアクセス権決定サーバ 1 0 4 を利用する為の設定について説明する。

【 0 1 8 7 】

2 0 0 1 は設定画面を示している。2 0 0 2 はアクセス権決定サーバ 1 0 4 を利用するか否かを指定するスイッチである。

【 0 1 8 8 】

アクセス権決定サーバ 1 0 4 を有効にした場合、アクセス権決定サーバ 1 0 4 にアクセス権記述を問い合わせる。

【 0 1 8 9 】

一方、アクセス権決定サーバ 1 0 4 を無効にした場合、アクセス権記述の取得を行わず、テンプレートから生成されるドキュメントに対してポリシーを適用しないものとする。

【 0 1 9 0 】

2 0 0 3 はテンプレートを選択するメニューである。2 0 0 4 は 2 0 0 3 で選択したテンプレートが有するフィールドを表示し、ユーザによる選択指示を受付ける。

【 0 1 9 1 】

例えば、2 0 0 3 で選択されたテンプレートの種類が、“見積書”であり、ユーザが図

10

20

30

40

50

6に示すデータ入力画面にて603、604にデータ入力を行うとする。すると、選択されたテンプレートを特定する識別子、およびデータ入力したフィールドのうち2004で選択指示されたフィールドの識別子が、S1104でアクセス権決定サーバ104に送信する情報となる。

【0192】

本実施例によって、管理者がテンプレートから生成されるドキュメントに対して、アクセス権記述を動的に決定する機能を設定するか否かを決めることができる。

【0193】

また、管理者がアクセス権記述を決定するために参照するフィールド識別子の種類を選択できるので、数種類入力されるデータの中で、何をもってアクセス権記述を決定するのかを決めることができる。

10

【0194】

このようにアクセス権限記述を決定するために参照するフィールド選択を行えるので、管理者の意図を反映してよりドキュメントに対する適切なポリシーを発行することができる。

【0195】

(その他の実施例)

前述した実施形態の機能を実現するように前述した実施形態の構成を動作させるプログラムを記憶媒体に記憶させ、該記憶媒体に記憶されたプログラムをコードとして読み出し、コンピュータにおいて実行する処理方法も上述の実施形態の範疇に含まれる。また、前述のプログラムが記憶された記憶媒体はもちろんそのプログラム自体も上述の実施形態に含まれる。

20

【0196】

かかる記憶媒体としてはたとえばフロッピー(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、CD-ROM、磁気テープ、不揮発性メモリカード、ROMを用いることができる。

【0197】

また前述の記憶媒体に記憶されたプログラム単体で処理を実行しているものに限らず、他のソフトウェア、拡張ボードの機能と共同して、OS上で動作し前述の実施形態の動作を実行するものも前述した実施形態の範疇に含まれる。

30

【図面の簡単な説明】

【0198】

【図1】モジュール構成図

【図2】ポリシーサーバの振る舞いを説明するフローチャート

【図3】ポリシーを適用する処理を説明するフローチャート

【図4】ドキュメントへのアクセスを説明するフローチャート

【図5】ドキュメントへのアクセスを説明するフローチャート

【図6】データ入力前のデータ入力用画面

【図7】データ入力後のデータ入力用画面

【図8】アクセス権記述を決定するためのテーブル

40

【図9】帳票の一例

【図10】アクセス権決定サーバの利用を設定するユーザインタフェース

【図11】クライアントコンピュータでアクセス権記述をサーバに問い合わせるフローチャート

【図12】サーバでアクセス権記述決定依頼を処理するフローチャート

【図13】データ入力後のデータ入力用画面

【図14】データ入力後のデータ入力用画面

【図15】アクセス権の確認のみかポリシー決定かを選択するユーザインタフェース

【図16】ポリシーが変更される旨を表示するユーザインタフェース

【図17】アクセス権の確認のみかポリシー決定かを選択する処理を説明するフローチャ

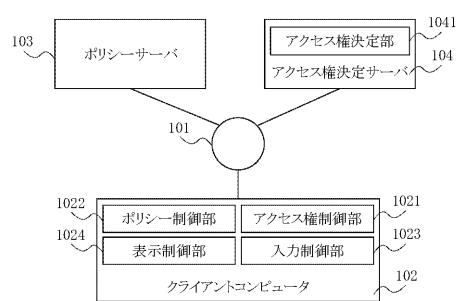
50

一ト

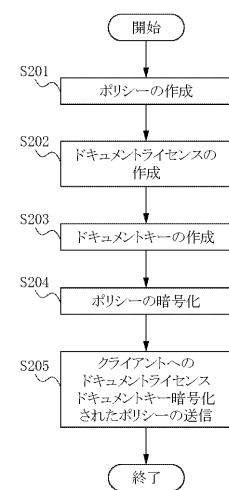
【図18】アクセス権を決定できない旨表示するユーザインターフェース

【図19】アクセス権を決定できない処理を説明するフローチャート

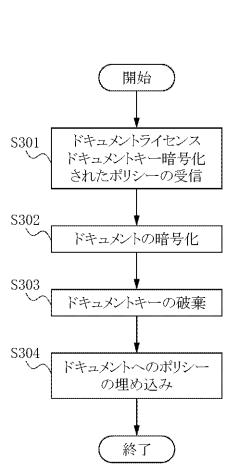
【図1】



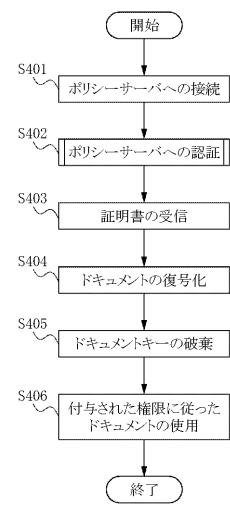
【図2】



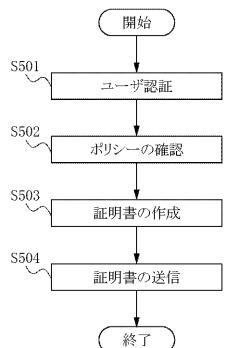
【図3】



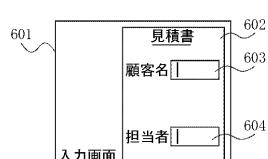
【図4】



【図5】



【図6】



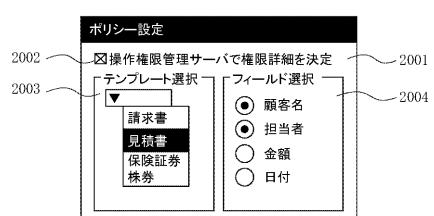
【図7】



801	802	803	804
帳票	フィールド名	値	アクセス権記述
見積書	顧客名	nmX1 nmX2 nmX3	"顧客名"氏は閲覧可 "担当者"氏は印刷可
	担当者	nmY1 nmY2	

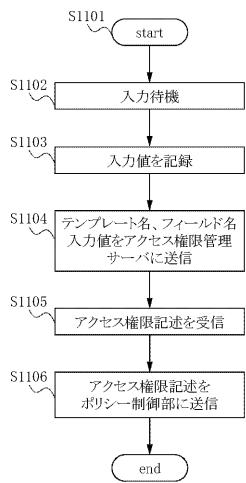
【図8】

【図9】

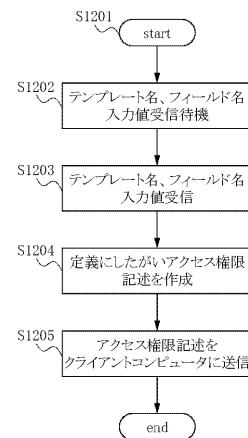


【図10】

【図11】



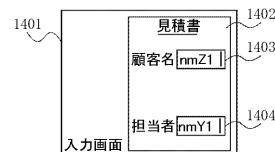
【図12】



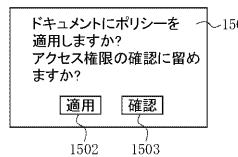
【図13】



【図14】



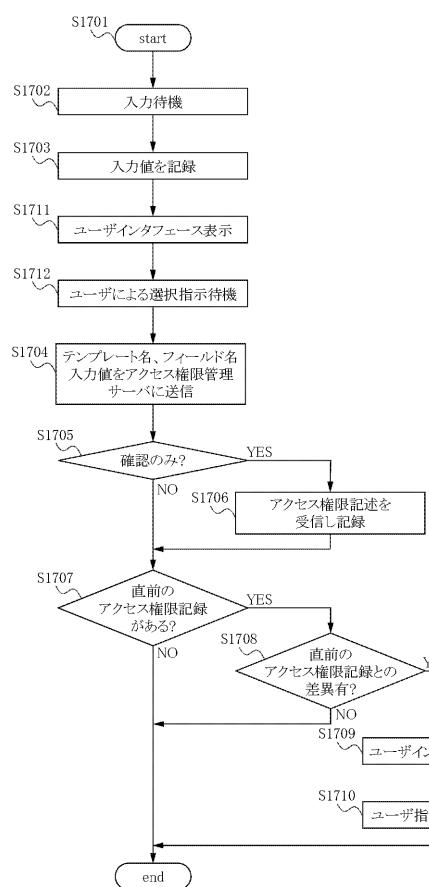
【図15】



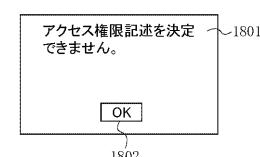
【図16】



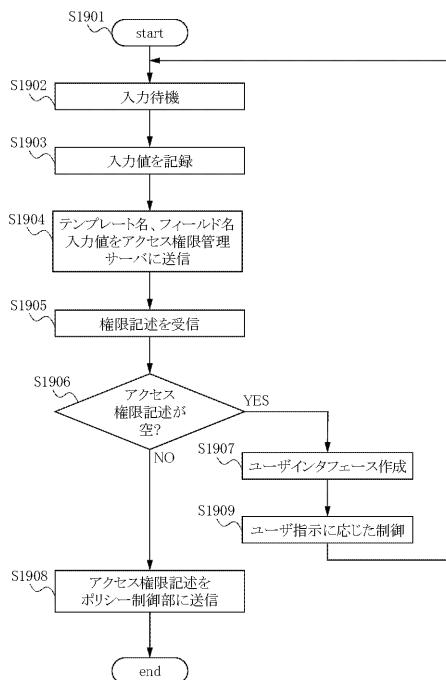
【図17】



【図18】



【図19】



フロントページの続き

(56)参考文献 特開2004-133816(JP,A)
特開2007-199909(JP,A)
特開2004-178334(JP,A)
特開2007-156612(JP,A)
特開平08-339352(JP,A)

(58)調査した分野(Int.Cl., DB名)

G 06 F 21 / 00 - G 06 F 21 / 88
G 06 F 17 / 21