

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号
特許第6366457号
(P6366457)

(45) 発行日 平成30年8月1日 (2018. 8. 1)

(24) 登録日 平成30年7月13日 (2018. 7. 13)

(51) Int. Cl.

F I

G O 6 F 21/60 (2013. 01)

G O 6 F 13/00 (2006. 01)

G O 6 F 21/60 3 4 O

G O 6 F 13/00 5 6 O A

請求項の数 14 (全 29 頁)

(21) 出願番号	特願2014-210897 (P2014-210897)	(73) 特許権者	000005108
(22) 出願日	平成26年10月15日 (2014. 10. 15)		株式会社日立製作所
(65) 公開番号	特開2016-81243 (P2016-81243A)		東京都千代田区丸の内一丁目6番6号
(43) 公開日	平成28年5月16日 (2016. 5. 16)	(74) 代理人	110001678
審査請求日	平成29年3月16日 (2017. 3. 16)		特許業務法人藤央特許事務所
		(72) 発明者	谷川 嘉伸
			東京都千代田区丸の内一丁目6番6号 株
			式会社日立製作所内
		(72) 発明者	井手口 恒太
			東京都千代田区丸の内一丁目6番6号 株
			式会社日立製作所内
		(72) 発明者	川口 信隆
			東京都千代田区丸の内一丁目6番6号 株
			式会社日立製作所内

最終頁に続く

(54) 【発明の名称】 情報共有装置、及び、情報共有方法

(57) 【特許請求の範囲】

【請求項 1】

情報共有装置であって、
プロセッサ及びメモリを有し、
第1のシステムと、第2のシステムとに接続され、
情報へのアクセスの許可又は不許可を判定するために前記第1のシステムにおいて用いられる、第1アクセス要求元の属性を取得し、
情報へのアクセスの許可又は不許可を判定するために前記第2のシステムにおいて用いられる、第2アクセス要求元の属性を取得し、
前記第1アクセス要求元の属性と前記第2アクセス要求元の属性とを対応させて、前記メモリが有する対応記憶領域に格納し、
前記第1アクセス要求元の属性を含むアクセスルールと、当該アクセスルールが適用される情報とを、前記第1のシステムから受信した場合、前記アクセスルールに含まれる第1アクセス要求元の属性を前記対応記憶領域を参照して、前記第2アクセス要求元の属性に変換し、
前記受信した情報と前記変換後のアクセスルールとを含む提供情報を、前記第2のシステムに送信するために生成することを特徴とする情報共有装置。

【請求項 2】

請求項 1 に記載の情報共有装置であって、
入力インタフェースを有し、

情報へのアクセスの許可又は不許可を判定するためのセキュリティレベルが割り当てられた基準属性を、前記メモリに格納し、

前記基準属性に対応する前記第1アクセス要求元の属性を、前記入力インタフェースを介して取得し、

前記基準属性に対応する前記第2アクセス要求元の属性を、前記入力インタフェースを介して取得した場合、前記基準属性を用いて、前記取得した第1アクセス要求元の属性と前記取得した第2アクセス要求元の属性とを対応させて前記対応記憶領域に格納することを特徴とする情報共有装置。

【請求項3】

請求項1に記載の情報共有装置であって、

10

前記第2のシステムが前記受信した情報と前記第2アクセス要求元の属性とを格納する方法を、管理情報として前記メモリが有する方法記憶領域に格納し、

前記第1アクセス要求元の属性を含むアクセスルールと、当該アクセスルールが適用される情報と、前記第1アクセス要求元の属性とを、前記第1アクセス要求元から受信した場合、

前記受信した第1アクセス要求元の属性を、前記対応記憶領域に基づいて前記第2アクセス要求元の属性に変換し、

前記方法記憶領域が示す方法によって前記第2のシステムが、前記受信した情報と前記変換後のアクセス第2要求元の属性とを格納するように、前記受信した情報と前記変換後の第2アクセス要求元の属性と前記変換後のアクセスルールとを含む前記提供情報を生成し、

20

前記生成した提供情報を前記第2のシステムに送信することを特徴とする情報共有装置。

【請求項4】

請求項1に記載の情報共有装置であって、

前記第1アクセス要求元の属性を含むアクセスルールと、当該アクセスルールが適用される情報とを、前記第1のシステムから受信した場合、前記アクセスルールに含まれる第1アクセス要求元の属性に対応する前記第2アクセス要求元の属性が前記対応記憶領域に格納されているか否かを判定し、

前記アクセスルールに含まれる第1アクセス要求元の属性に対応する前記第2アクセス要求元の属性が前記対応記憶領域に格納されている場合、前記第2のシステムに前記受信した情報を送信することを決定することを特徴とする情報共有装置。

30

【請求項5】

請求項2に記載の情報共有装置であって、

出力インタフェースを有し、

前記基準属性と前記セキュリティレベルとを示す画面を表示するための画面データを、前記出力インタフェースを介して出力し、

前記入力インタフェースを介して入力された、前記基準属性に対応する第1アクセス要求元の属性、及び、前記基準属性に対応する第2アクセス要求元の属性を取得することを特徴とする情報共有装置。

40

【請求項6】

請求項5に記載の情報共有装置であって、

前記出力インタフェースを介して、前記第2アクセス要求元の属性を入力する指示を示す画像を出力することを特徴とする情報共有装置。

【請求項7】

請求項1に記載の情報共有装置であって、

前記属性は、前記情報へのアクセスを要求するユーザを識別するための属性、及び、前記アクセスが要求される情報を識別するための属性の少なくとも一つであることを特徴とする情報共有装置。

【請求項8】

50

情報共有装置による情報共有方法であって、
前記情報共有装置は、
プロセッサ及びメモリを有し、
第１のシステムと、第２のシステムとに接続され、
前記方法は、

前記プロセッサが、情報へのアクセスの許可又は不許可を判定するために前記第１のシステムにおいて用いられる、第１アクセス要求元の属性を取得する手順と、

前記プロセッサが、情報へのアクセスの許可又は不許可を判定するために前記第２のシステムにおいて用いられる、第２アクセス要求元の属性を取得する手順と、

前記プロセッサが、前記第１アクセス要求元の属性と前記第２アクセス要求元の属性とを対応させて、前記メモリが有する対応記憶領域に格納する手順と、

10

前記プロセッサが、前記第１アクセス要求元の属性を含むアクセスルールと、当該アクセスルールが適用される情報とを、前記第１のシステムから受信した場合、前記アクセスルールに含まれる第１アクセス要求元の属性を前記対応記憶領域を参照して、前記第２アクセス要求元の属性に変換する手順と、

前記プロセッサが、前記受信した情報と前記変換後のアクセスルールとを含む提供情報を、前記第２のシステムに送信するために生成する手順とを含むことを特徴とする情報共有方法。

【請求項 9】

請求項 8 に記載の情報共有方法であって、

20

前記情報共有装置は、入力インタフェースを有し、

前記方法は、

前記プロセッサが、情報へのアクセスの許可又は不許可を判定するためのセキュリティレベルが割り当てられた基準属性を、前記メモリに格納する手順と、

前記プロセッサが、前記基準属性に対応する前記第１アクセス要求元の属性を、前記入力インタフェースを介して取得する手順と、

前記プロセッサが、前記基準属性に対応する前記第２アクセス要求元の属性を、前記入力インタフェースを介して取得した場合、前記基準属性を用いて、前記取得した第１アクセス要求元の属性と前記取得した第２アクセス要求元の属性とを対応させて前記対応記憶領域に格納する手順とを含むことを特徴とする情報共有方法。

30

【請求項 10】

請求項 8 に記載の情報共有方法であって、

前記プロセッサが、前記第２のシステムが前記受信した情報と前記第２アクセス要求元の属性とを格納する方法を、管理情報として前記メモリが有する方法記憶領域に格納する手順と、

前記プロセッサが、前記第１アクセス要求元の属性を含むアクセスルールと、当該アクセスルールが適用される情報と、前記第１アクセス要求元の属性とを、前記第１アクセス要求元から受信した場合、

前記プロセッサが、前記受信した第１アクセス要求元の属性を、前記対応記憶領域に基づいて前記第２アクセス要求元の属性に変換する手順と、

40

前記プロセッサが、前記方法記憶領域が示す方法によって前記第２のシステムが、前記受信した情報と前記変換後のアクセス第２要求元の属性とを格納するように、前記受信した情報と前記変換後の第２アクセス要求元の属性と前記変換後のアクセスルールとを含む前記提供情報を生成する手順と、

前記プロセッサが、前記生成した提供情報を前記第２のシステムに送信する手順とを含むことを特徴とする情報共有方法。

【請求項 11】

請求項 8 に記載の情報共有方法であって、

前記プロセッサが、前記第１アクセス要求元の属性を含むアクセスルールと、当該アクセスルールが適用される情報とを、前記第１のシステムから受信した場合、前記アクセス

50

ルールに含まれる第1アクセス要求元の属性に対応する前記第2アクセス要求元の属性が前記対応記憶領域に格納されているか否かを判定する手順と、

前記プロセッサが、前記アクセスルールに含まれる第1アクセス要求元の属性に対応する前記第2アクセス要求元の属性が前記対応記憶領域に格納されている場合、前記第2のシステムに前記受信した情報を送信することを決定する手順とを含むことを特徴とする情報共有方法。

【請求項12】

請求項9に記載の情報共有方法であって、

前記情報共有装置は、出力インタフェースを有し、

前記方法は、

前記プロセッサが、前記基準属性と前記セキュリティレベルとを示す画面を表示するための画面データを、前記出力インタフェースを介して出力する手順と、

前記プロセッサが、前記入力インタフェースを介して入力された、前記基準属性に対応する第1アクセス要求元の属性、及び、前記基準属性に対応する第2アクセス要求元の属性を取得する手順とを含むことを特徴とする情報共有方法。

【請求項13】

請求項12に記載の情報共有方法であって、

前記プロセッサが、前記出力インタフェースを介して、前記第2アクセス要求元の属性を入力する指示を示す画像を出力する手順を含むことを特徴とする情報共有方法。

【請求項14】

請求項8に記載の情報共有方法であって、

前記属性は、前記情報へのアクセスを要求するユーザを識別するための属性、及び、前記アクセスが要求される情報を識別するための属性の少なくとも一つであることを特徴とする情報共有方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、情報共有装置に関する。

【背景技術】

【0002】

企業、又は、官公庁若しくは自治体では、パソコンなどを使ったIT環境が普及し、電子的な文書を扱う業務が一般的になっている。さらに、電子的な情報が、複数の企業間、又は、企業と官公庁又は自治体との間など、複数の組織間において通信ネットワークを介して交換されており、これによって、複数の組織が、協調しながら業務を進めている。

【0003】

電子的な情報の中には、経営計画資料、研究開発資料、住民情報が記載された資料、及び、申請書など機密性の確保が必要な内容が含まれている。情報の機密性を確保するためには、電子的な情報の開示範囲及び取扱制限のポリシーを決めて、そのポリシーを、人又はシステムが実行することが重要である。このような機密性確保を実現するために、アクセス制御技術が使われてきた。

【0004】

特許文献1は、企業等の組織における複数部門の間で機密文書を共有する時のアクセス制御方法を開示している。ここでは、開示範囲として、相手部門の主体名を事前に全てを明確に決め難いことに注目し、直接アクセス権限判定手段と間接アクセス権限判定手段の組合せを提案している。

【0005】

直接アクセス権限判定手段では、特定の主体名を指定する。次に、間接アクセス権限判定手段では、組織構造や座席レイアウト等の主体の関係性を指定する。この間接アクセス権限判定手段により、具体的な主体名を指定することなく、ある特定の主体の上司や同じ座席の島にいる者、などの別の主体名を開示範囲として追加することが可能になる。

【先行技術文献】

【特許文献】

【0006】

【特許文献1】特開2006-323535号公報

【発明の概要】

【発明が解決しようとする課題】

【0007】

組織毎に設置される情報システムには、異なるアクセス制御モデルが適用される。そして、複数の組織が電子的な情報を共有する場合、このような情報システムが相互に連携する状況が考えられる。

10

【0008】

アクセス制御モデルを適用するためには、ユーザ属性（情報にアクセスする側の属性）又は情報属性（アクセスされる情報の属性）などの定義及びアクセスルールが必要である。そして、同じアクセス制御モデルを複数の情報システムに適用した場合も、定義及びアクセスルールを表現する名前又は番号等の識別子、及び、関係性を示す言葉等が、組織毎に異なる可能性がある。

【0009】

一般的に、複数の組織間で情報を共有する場合、組織毎に適用されるアクセス制御方法の違いを解消することが重要である。従来技術は、同一のアクセス制御モデルが適用される複数の組織間での情報共有を前提としている。そのため、特許文献1の技術を使った場合、情報を提供する者は、情報共有する相手（情報が提供される者）の情報システムが定義する属性の定義及びアクセスルールを知ることが出来ない。このため、情報を提供する物が、情報が提供される者にとって適切なアクセスルールを、情報に設定することは困難である。

20

【0010】

本発明は、上記のような問題点を解決するためのものである。すなわち、複数の情報システムに異なる表現によるアクセス制御モデルが適用されている場合においても、複数の情報システム間の情報共有を可能にするシステムの提供を目的とする。

【課題を解決するための手段】

【0011】

上記課題を解決するために、本発明は、情報共有装置であって、プロセッサ及びメモリを有し、第1のシステムと、第2のシステムとに接続され、情報へのアクセスの許可又は不許可を判定するために前記第1のシステムにおいて用いられる、第1アクセス要求元の属性を取得し、情報へのアクセスの許可又は不許可を判定するために前記第2のシステムにおいて用いられる、第2アクセス要求元の属性を取得し、前記第1アクセス要求元の属性と前記第2アクセス要求元の属性とを対応させて、前記メモリが有する対応記憶領域に格納し、前記第1アクセス要求元の属性を含むアクセスルールと、当該アクセスルールが適用される情報とを、前記第1のシステムから受信した場合、前記アクセスルールに含まれる第1アクセス要求元の属性を前記対応記憶領域を参照して、前記第2アクセス要求元の属性に変換し、前記受信した情報と前記変換後のアクセスルールとを含む提供情報を、前記第2のシステムに送信するために生成する。

30

40

【発明の効果】

【0012】

本発明によれば、複数の異なるシステムがアクセス制御モデルを維持しつつ情報を共有できる。

【0013】

上記した以外の課題、構成及び効果は、以下の実施形態の説明により明らかにされる。

【図面の簡単な説明】

【0014】

【図1】本実施例の情報共有システムの構成を示すブロック図である。

50

【図 2】本実施例の計算機のハードウェア構成を示すブロック図である。

【図 3】本実施例のユーザ属性、情報属性、属性管理方法、及び、アクセスルールの表現をマッピングする概念を示す説明図である。

【図 4】本実施例の情報共有サーバの処理を示すフローチャートである。

【図 5】本実施例の接続システム情報を示す説明図である。

【図 6】本実施例の属性辞書を示す説明図である。

【図 7】本実施例の属性マッピングエディタのユーザインタフェースを示す説明図である。

【図 8】本実施例のマッピング情報を示す説明図である。

【図 9】本実施例のユーザインタフェースに表示される警告ダイアログを示す説明図である。

10

【図 10】本実施例のユーザインタフェースを示す説明図である。

【図 11】本実施例のアクセスルールを示す説明図である。

【図 12】本実施例の情報管理サーバから情報共有サーバに共有情報を送信する処理を示すシーケンス図である。

【図 13】本実施例の第 1 の共有情報パッケージを示す説明図である。

【図 14】本実施例の共有情報を示す説明図である。

【図 15】本実施例の情報管理サーバが、情報共有サーバから共有情報を取得する処理を示すシーケンス図である。

【図 16】本実施例の第 2 の共有情報パッケージを示す説明図である。

20

【発明を実施するための形態】

【0015】

以下、本発明の実施形態を、図面を用いて説明する。

【0016】

本実施例の情報共有システムは、複数の組織がそれぞれ運用する複数の情報管理システムにおいて生成された文書ファイルなどの情報を、他の情報管理システムと横断的に共有するための機能を提供する。

【0017】

組織の運用管理者は、ユーザ及び情報等の属性を用いて定義されたアクセスルールを事前に生成し、情報管理システムに登録する。情報共有システムによって共有される情報が情報管理システムにおいて生成された場合、登録されたアクセスルールに基づいてその情報の取り扱いが制限される。

30

【0018】

本実施例のアクセスルールは、情報へのアクセスの許可又は不許可を判定するためのルールを示し、属性によって定義される。また、本実施例のアクセスルールは、アクセスの具体的な行為である、情報への閲覧又は更新等を示す。

【0019】

本実施例の属性は、ユーザ属性、情報属性、及びその他属性を含む。本実施例のユーザとは、情報管理システム及び情報共有システムを利用する者であり、情報にアクセスする意思を持つ者である。ユーザ属性は、情報にアクセスする者を識別するための属性である。

40

【0020】

情報属性は、アクセスされる文書ファイル及び画像ファイル等の情報を識別するための属性である。その他属性には、情報にアクセスする環境（時間、季節、及び場所等）が含まれる。

【0021】

図 1 は、本実施例の情報共有システムの構成を示すブロック図である。

【0022】

本実施例の情報共有システムは、少なくとも二つ以上の情報管理システム 100（100-1、100-N）と、通信ネットワーク 190 と、情報共有サーバ 160 とから構成

50

される。情報管理システム１００及び情報共有サーバ１６０は、通信ネットワーク１９０を介して相互に接続される。

【００２３】

情報管理システム１００は、複数の端末１０２と、通信ネットワーク１２０と、情報管理サーバ＃１（１０４）とから構成される。情報管理システム１００は、利用者が端末１０２を介して情報にアクセスする場合、属性によって定義されるアクセス制御モデルを適用する。

【００２４】

また、端末１０２及び情報管理サーバ＃１（１０４）は、通信ネットワーク１２０を介して相互に接続される。端末１０２及び情報管理サーバ＃１（１０４）は、通信ネットワーク１２０及び通信ネットワーク１９０を介して情報共有サーバ１６０と接続する。

10

【００２５】

端末１０２は、運用管理システム＃１（１００－１）の運用又は管理を行う者（以下、運用管理者）からの指示を受け付ける入力装置であり、また、運用管理者に処理結果を出力する出力装置である。端末１０２は、情報１１６、及び、情報共有サーバ１６０が持つ共有情報１７８へアクセスする要求を受け付ける。

【００２６】

情報管理サーバ＃１（１０４）は、演算装置及び記憶装置を有する計算機である。情報管理サーバ＃１（１０４）は、運用管理インタフェース１１０、情報管理部１０６、及び連携部１０８を機能部として有し、ユーザ属性１１２、情報属性１１４、情報１１６、及びアクセスルール１１８を記憶部として有する。

20

【００２７】

運用管理インタフェース１１０は、端末１０２が受け付けた情報１１６へアクセスする要求を受信する。情報管理部１０６は、アクセスルール１１８等を参照し、情報１１６へのアクセスを制限する。連携部１０８は、他の情報管理システム１００及び情報共有サーバ１６０と接続する機能を提供する。

【００２８】

ユーザ属性１１２は、情報管理システム＃１（１００－１）において用いられるユーザ属性を格納する。情報属性１１４は、情報管理システム＃１（１００－１）において用いられる情報属性を格納する。情報１１６は、情報共有システム内で共有する情報を、少なくとも格納する。アクセスルール１１８は、属性を用いて定義されたアクセスルールを格納する。

30

【００２９】

情報管理システム＃１（１００－１）と情報管理システム＃Ｎ（１００－Ｎ）とは、同様の機能を有する。情報管理システム＃Ｎ（１００－Ｎ）は、複数の端末１３２と、通信ネットワーク１５０と、情報管理サーバ＃Ｎ（１３４）とから構成される。

【００３０】

端末１３２は、端末１０２と同じ機能を有し、通信ネットワーク１５０は、通信ネットワーク１２０と同じ機能を有する。

【００３１】

40

情報管理サーバ＃Ｎ（１３４）は、演算装置及び記憶装置を有する計算機である。情報管理サーバ＃Ｎ（１３４）は、運用管理インタフェース１４０、及び、情報管理部１３６、連携部１３８を機能部として有し、ユーザ属性１４２、情報１４４及びアクセスルール１４６を記憶部として有する。

【００３２】

運用管理インタフェース１４０は、運用管理インタフェース１１０と同じ機能を有し、情報管理部１３６は、情報管理部１０６と同じ機能を有し、連携部１３８は、連携部１０８と同じ機能を有する。

【００３３】

ユーザ属性１４２は、情報管理システム＃Ｎ（１００－Ｎ）において用いられるユーザ

50

属性を格納する。情報144は、情報共有システム内で共有する情報を格納する。アクセスルール146は、アクセスルールを格納する。

【0034】

情報管理システム#1(100-1)と情報管理システム#N(100-N)との違いは、情報と情報属性とを自らに格納する方法(以下、属性管理方法)の違いである。情報管理システム100-1は、情報属性を情報から独立させ、複数のアクセスルールにおいて用いられる情報属性を一元的に格納する方法を用いる(以下、独立型管理方法と記載)。独立型管理方法は、例えば、ファイルシステムで規定された代替データストリームとして情報属性を格納する方法である。

【0035】

一方、情報管理システム#N(100-N)は、情報144の中に情報属性を格納する管理方法を用いる(以下、一体型管理方法と記載)。一体型管理方法は、例えば、ワードプロセッサのファイルフォーマットで規定されたアプリケーションメタデータとして、情報属性を情報144の中に格納する方法である。アプリケーションメタデータには、例えば、情報を含む文書ファイルのプロパティとして文書ファイルに情報属性を含める方法がある。

【0036】

このように情報共有システムには、情報属性を情報の外部に保持する方法を採用する情報管理システム100と、情報属性を情報の内部で管理する方法とを採用する情報管理が混在している。これは、情報管理サーバが有するアプリケーションが、情報を識別するための情報属性を取得する方法が、アプリケーションによって相違するためである。

【0037】

情報共有サーバ160は、演算装置及び記憶装置を有する計算機である。情報共有サーバ160は、運用管理インタフェース172、共有制御部162、接続システム管理部164、共有情報管理部166、アクセスルール管理部168及びマッピング管理部170を管理部として有し、接続システム情報174、共有情報178、アクセスルール180、マッピング情報182、及び属性辞書184を記憶部として有する。

【0038】

運用管理インタフェース172は、端末102及び端末132から入力された要求を受け付ける。共有制御部162は、情報管理システム100との接続機能を提供する。接続システム管理部164は、接続システム情報174を管理する。

【0039】

共有情報管理部166は、共有情報178を管理する。アクセスルール管理部168は、アクセスルール180を管理する。マッピング管理部170は、マッピング情報182及び属性辞書184を管理する。

【0040】

接続システム情報174は、情報管理システム100に関する情報を有する。共有情報178は、情報管理システム100間で共有する情報を含む。共有情報178は、属性情報176を有する。属性情報176は、ユーザ属性及び情報属性を有する。

【0041】

アクセスルール180は、情報管理システム100から送られたアクセスルールを有する。マッピング情報182は、ユーザ属性及び情報属性等、情報管理システム100において用いられるユーザ属性及び情報属性等に対応させて格納する対応記憶領域である。属性辞書184は、ユーザ属性及び情報属性等を識別するための基準となる基準属性を有する。

【0042】

なお、通信ネットワーク120、通信ネットワーク150及び通信ネットワーク190は、公衆網、インターネット、ISDN、専用線若しくはLANなどの有線網、又は、移動通信用基地局若しくは通信用人工衛星を利用した無線網などの通信ネットワークであってもよい。

10

20

30

40

50

【0043】

また、情報共有システムが有する装置は、予め設定された通信相手となる他の装置のアドレスを用いて、他の装置と通信する。また、一つの装置が、ブロードキャスト通信又はマルチキャスト通信などを使って、複数の装置と同報的に通信してもよい。さらに、情報共有システムが有する装置は、パブリッシュ／サブスクライブ型の通信のように、位置透過的に通信してもよい。

【0044】

図2は、本実施例の計算機のハードウェア構成を示すブロック図である。

【0045】

端末102、端末132、情報管理サーバ104、情報管理サーバ134、及び情報共有サーバ160は、例えば、図2に示す計算機200と同じ装置を有する。計算機200は、中央演算装置（CPU）202、入力装置210、外部記憶装置206、半導体メモリ（RAM）204、出力装置212、記憶媒体216、外部メディアインタフェース214、通信インタフェース208、及び内部通信線250を有する。

10

【0046】

CPU202は、演算装置及び制御装置であり、プロセッサであってもよい。端末102、端末132、情報管理サーバ104、情報管理サーバ134、及び情報共有サーバ160は、CPU202がプログラムを実行することによって、各々の機能を実現する。

【0047】

入力装置210は、キーボード及びマウスなどの装置であり、運用管理者が指示を入力するための装置である。出力装置212は、CRTディスプレイ、液晶ディスプレイ及びプリンタなどの装置であり、運用管理者等に処理結果を提供するための装置である。

20

【0048】

外部記憶装置206は、ハードディスク又はフラッシュメモリ（SSD）等の大容量かつ不揮発性の記憶装置である。外部記憶装置206は、CPU202が実行するプログラム及びプログラムの実行時に使用されるデータを格納してもよい。すなわち、CPU202は、外部記憶装置206からプログラムを読み出し、RAM204にプログラムをロードした後、プログラムを実行する。

【0049】

半導体メモリ（RAM）204は、高速かつ揮発性の記憶素子であり、外部記憶装置206に格納されたプログラム及びプログラムの実行時に使用されるデータを一時的に格納する。例えば、情報共有サーバ160の半導体メモリ（RAM）204は、共有制御部162、接続システム管理部164、共有情報管理部166、アクセスルール管理部168、マッピング管理部170及び運用管理インタフェース172を実装するためのプログラムを格納する。

30

【0050】

外部メディアインタフェース214は、光磁気メディアなどの記憶媒体216を読み書きするためのインタフェースである。記憶媒体216は、着脱可能であり、例えば、CD-ROM又はフラッシュメモリなどのリムーバブルメディアである。

【0051】

CPU202が実行するプログラムは、記憶媒体216、又は、通信ネットワーク（120、150、190）を伝搬する搬送波又はデジタル信号を介して計算機200に提供され、非一時的記憶媒体である外部記憶装置206に格納されてもよい。このため、計算機200は、外部メディアインタフェース214を介して、データを取得する。

40

【0052】

通信インタフェース208は、通信ネットワーク190等と所定のプロトコルによって通信するためのインタフェースである。内部通信線250は、例えばバスであり、計算機200に備わる装置を相互に接続する。

【0053】

計算機200は、物理的に一つの計算機であってもよく、又は、論理的又は物理的に複

50

数の計算機によって構成される計算機システムであってもよい。また、計算機 200 が有するプログラムは、一つの計算機 200 において複数のスレッドによって実行されてもよく、また、複数の物理的計算機の資源上に構築された仮想計算機において実行されてもよい。

【0054】

また、計算機 200 は、図 2 に示すすべての装置を有する必要はない。例えば、端末 102 及び端末 132 は、外部メディアインタフェース 214 を有さなくてもよい。

【0055】

図 3 は、本実施例のユーザ属性、情報属性、属性管理方法、及び、アクセスルールの表現をマッピングする概念を示す説明図である。

10

【0056】

情報管理システム 100 に適用されるユーザ属性、情報属性、属性管理方法、及び、アクセスルール等は、情報管理システム 100 間で表現が異なる。表現 302、表現 304 及び表現 306 は、情報管理システム #1 (100-1)、情報管理システム #2 (100-2) 及び情報管理システム #N (100-N) に適用されるユーザ属性、情報属性、情報属性管理方法及びアクセスルールの表現である。

【0057】

そして、表現 302、表現 304 及び表現 306 は、用いられるセキュリティレベルごとに、情報共有サーバ 160 が有する表現 300 にマッピングされる。このため、情報管理システム 100 が新たに追加された場合、既存の複数の情報管理システム 100 の表現と、新たな情報管理システム 100 の表現とを直接複数回対応づける必要がない。

20

【0058】

そして、情報共有サーバ 160 の表現 300 と、新たな情報管理システム 100 とを 1 回のみマッピングすれば、本実施例の情報共有システムは、新たな情報管理システム 100 の表現と、既存の複数の情報管理システム 100 の表現とを対応づけることができる。

【0059】

表現 300 は、情報共有サーバ 160 のマッピング情報 182 及び接続システム情報 174 に格納される。以降において、この概念を具現化した処理手順及びデータ構造を説明する。

【0060】

図 4 は、本実施例の情報共有サーバ 160 の処理を示すフローチャートである。

30

【0061】

情報共有サーバ 160 の共有制御部 162 は、情報共有サーバ 160 の起動後、又は、所定の期間ごとに図 4 に示す開始する (400)。また、共有制御部 162 は、運用管理者等の指示により、図 4 に示す処理を開始してもよい。

【0062】

共有制御部 162 は、端末 102 又は端末 132 から運用管理処理を開始する指示を受け付けたか否かを判定する (402)。共有制御部 162 は、運用管理処理を開始する指示を受け付けた場合、指示された運用管理処理を、マッピング管理部 170 又はアクセスルール管理部 168 に実行させる (404)。

40

【0063】

本実施例の運用管理処理は、後述する属性マッピング処理、及び、アクセスルール生成処理を含む。運用管理処理を開始する指示には、開始する運用管理処理を示す情報が含まれる。

【0064】

共有制御部 162 は、運用管理処理を開始する指示を受け付けていないと判定した場合、共有情報を受信したか、又は、共有情報を送信する必要があるかを判定する (406)。共有情報とは、情報管理システム 100 から情報共有サーバ 160 に送信された情報であり、本実施例の情報共有システムにおいて共有する情報である。

【0065】

50

共有制御部 162 は、情報管理システム 100 から共有情報を受信したか否かを判定する。また、共有制御部 162 は、情報管理システム 100 から共有情報が要求された場合、共有情報を送信する必要があると判定してもよい。

【0066】

なお、共有制御部 162 は、接続システム情報 174 を参照し、情報管理システム 100 に未送信の共有情報があると判定した場合、ステップ 406 において共有情報を送信する必要があると判定してもよい。

【0067】

図 5 は、本実施例の接続システム情報 174 を示す説明図である。

【0068】

接続システム情報 174 は、認証情報 500 及び送受信情報 520 を格納する。認証情報 500 は、複数の領域（502、504、506、508、510 及び 512）を有する。認証情報 500 は、情報共有システムの管理者によってあらかじめ設定される。

【0069】

領域 502 は、情報管理システム 100 を識別するための識別子を含む。領域 504 は、システムクレデンシャルを示し、情報管理システム 100 と情報共有サーバ 160 とが相互に通信する際、用いられる認証方法を示す。

【0070】

領域 506 は、領域 502 が示す情報管理システム 100 が、情報と情報属性とを格納する方法（属性管理方法）を示す記憶領域である。領域 506 は、領域 506 が示す独立型管理方法を適用するために、情報に含まれていた情報属性を情報から抽出する具体的な方法を含んでもよいし、また、領域 506 が示す一体型管理方法を適用するために、情報と分割されていた情報属性を情報に含める具体的な方法を含んでもよい。

【0071】

共有情報管理部 166 は、領域 506 を参照することによって、情報管理システム 100 に送る情報を、情報管理システム 100 の属性管理方法に従った状態に変更することができる。

【0072】

領域 508 は、情報管理システム 100 の運用管理者の識別子を示す。領域 510 は、情報管理システム 100 の運用管理者が情報共有サーバ 160 にアクセスするための認証方法を示す。

【0073】

領域 512 は、送受信情報 520 と認証情報 500 とを関連づけるための識別子を示す。具体的には、送受信情報 520 の識別子を示す。図 5 において、一つの情報管理システム 100 は、認証情報 500 の中の一つのエントリに対応し、一つの送受信情報 520 に対応する。

【0074】

接続システム管理部 164 は、情報管理システム 100 と情報共有サーバ 160 との間で、共有情報が送受信された場合に送受信情報 520 を更新する。送受信情報 520 は、通信ログとして、複数の領域（522、524、526、528）を含む。

【0075】

領域 522 は、情報管理システム 100 を識別するための識別子を含み、領域 502 に対応する。領域 524 は、共有情報を送信又は受信した日時を示す。

【0076】

領域 526 は、領域 522 が示す情報管理システム 100 から情報共有サーバ 160 が共有情報を受信した場合「受信」を示し、領域 522 が示す情報管理システム 100 に情報共有サーバ 160 が共有情報を送信した場合「送信」を示す。領域 528 は、送受信した共有情報を識別するための識別子を示す。

【0077】

共有制御部 162 は、領域 526 が「受信」を示し共有情報の中から、かつ、領域 52

10

20

30

40

50

6が「受信」を示す情報管理システム100以外の情報管理システム100のすべてに送信されていない共有情報がある場合、ステップ406において共有情報を送信する必要があると判定してよい。

【0078】

ステップ406において、共有情報を受信したか、又は、共有情報を送信する必要があると判定した場合、共有情報管理部166は、後述する処理によって共有情報を受信、又は、送信する(408)。ステップ406において、共有情報を受信しておらず、かつ、共有情報を送信する必要はないと判定した場合、シャットダウンの指示を受け付けたか否かを判定する(410)。

【0079】

シャットダウンの指示を受け付けたと判定した場合、共有制御部162は、終了する(412)。シャットダウンの指示を受け付けていないと判定した場合、共有制御部162は、ステップ402に戻る。

【0080】

ステップ404における運用管理処理の一つである属性マッピング処理を以下に示す。まず、情報管理システム#1(100-1)の運用管理者がマッピング処理を行う手順を説明する。

【0081】

情報共有サーバ160のマッピング管理部170は、ステップ404において、運用管理インタフェース172を介して端末102に、図7に示すユーザインタフェース700を出力するためのデータを送信する。これによってマッピング管理部170は、端末102に、属性マッピングエディタの機能を提供する。

【0082】

なお、マッピング管理部170は、ユーザインタフェース700を端末102のディスプレイ等から出力させるために、接続システム情報174のフィールド(504、506、508及び510)の内容を用いて出力させる。

【0083】

ステップ404の運用管理処理において属性マッピング処理が開始した場合、マッピング管理部170は、情報管理サーバ104に格納されたユーザ属性112からユーザ属性をインポートし、情報共有サーバ160に格納された属性辞書184のユーザ属性をインポートする。また、マッピング管理部170は、情報管理サーバ104に格納された情報属性114をインポートし、情報共有サーバ160に格納された属性辞書184の情報属性をインポートする。

【0084】

また、マッピング管理部170は、その他属性が情報管理サーバ104に格納される場合、その他属性を情報管理サーバ104からインポートし、属性辞書184からその他属性をインポートしてもよい。

【0085】

ここで、情報管理サーバ104からインポートするユーザ属性、情報属性、及び、その他属性は、端末102を介して運用管理者等から指示されたユーザ属性、情報属性、及び、その他属性であってよい。また、ユーザ属性112及び情報属性114等がマッピング済みか否かを示す場合、マッピング管理部170は、属性辞書184が有する基準とマッピングされていない属性を特定し、特定した属性を情報管理サーバ104からインポートしてもよい。

【0086】

ユーザ属性112は、情報管理システム#1(100-1)において情報にアクセスするユーザを、識別するための属性を含む。また、ユーザ属性112は、情報管理システム#1(100-1)において用いられる表現302によって固有に定義されたユーザ属性を含む。ユーザ属性112は、ユーザの各々を識別するための識別子を含む。識別子は、例えば、英数字から構成されるユーザIDでもよい。

10

20

30

40

50

【0087】

また、ユーザ属性112は、情報116にアクセスできるユーザを特定するために用いられる属性であればいかなる属性を含んでもよい。ユーザ属性112は、例えば、所属部署、職務、役職、資格、メールアドレス、及び、国籍などの具体的な名称又は識別子を含む。

【0088】

また、ユーザ属性112は、ユーザにあらかじめ割り当てられる秘密取り扱い区分を含んでもよい。さらに、ユーザ属性112は、役職及び資格など、割り当てられる権限に上位及び下位がある属性についての階層構造を、情報として含んでもよい。

【0089】

情報属性114は、情報管理システム#1(100-1)の情報116に格納された情報を識別するための属性を含む。情報属性114は、情報管理システム#1(100-1)において用いられる表現302によって固有に定義された情報属性を含む。情報属性114は、情報116の情報を識別するための識別子を含む。例えば、情報属性114は、ファイル名及び格納場所を示す情報を含む。

【0090】

情報属性114は、情報116に格納される情報の属性であればいかなる属性を含んでもよい。情報属性114は、例えば、作成部署、分類、機密レベル、名称、作成者、管理部署及び運用管理者などの具体的な識別子を含む。

【0091】

また、情報属性114は、情報116に格納される情報にあらかじめ割り当てられる秘密取り扱い区分も含む。さらに、ユーザ属性112は、機密レベルなど、割り当てられる権限に上位及び下位がある属性についての階層構造を、情報として含んでもよい。

【0092】

なお、端末102を介して運用管理者から、ユーザ属性112及び情報属性114以外のその他属性(後述)を指定された場合、マッピング管理部170は、情報管理サーバ104のメモリに格納されたその他属性と、属性辞書184に格納されたその他属性とをインポートしてもよい。

【0093】

その他属性は、情報にアクセスできる、環境及び条件等を示す。その他属性は、例えば、時間帯、気温、非常警戒レベル及び場所等を示す。

【0094】

一方、属性辞書184は、情報共有サーバ160の運用者又は管理者等によってあらかじめ設定された基準のユーザ属性及び情報属性を含み、情報管理システム100のユーザ属性及び情報属性とマッピングされるユーザ属性及び情報属性を含む。属性辞書184は、図3に示す表現300によって定義されたユーザ属性及び情報属性を含む。

【0095】

図6は、本実施例の属性辞書184を示す説明図である。

【0096】

属性辞書184は、基準の属性の表現を示し、複数の領域(600、602、604、606)を含む。領域600は、属性の分類を示す。本実施例の領域600は、ユーザ属性、情報属性、その他属性の少なくとも一つを示す。

【0097】

領域602は、属性の項目を表現する識別子を含む。領域604は、属性の項目の具体的な値を表現する識別子を含む。例えば、領域602が「役職」を示す場合、領域604は、「課長」又は「リーダー」等を示す。領域602及び領域604は、表現300によって定義される属性を示す。

【0098】

領域606は、属性マッピング処理において、情報管理システム100の運用管理者に出力する説明文(使用ガイドライン)を格納する。領域604が「-」を示す場合、領域

10

20

30

40

50

606は、領域602が示す項目の説明を示す。また、領域606の説明文は、領域602及び領域604が示す属性の定義のセキュリティレベルを示す。

【0099】

なお、属性辞書184は、割り当てられる権限に上位及び下位がある属性についての階層構造を、情報として含んでもよい。例えば、領域602が「役職」である場合、領域604の値である「部長」には、機密レベルAを閲覧できる権限が割り当てられ、領域604の値である「課長」には、機密レベルAを閲覧できない権限が割り当てられる場合、属性辞書184は、「部長」には上位の権限が割り当てられ、「課長」には下位の権限が割り当てられることを示す階層構造を含んでもよい。

【0100】

マッピング管理部170は、ユーザ属性、情報属性及びその他属性の少なくとも1種類を情報管理サーバ104からインポートした後、インポートした情報に基づいて、属性マッピングエディタを表示するためのデータを生成する。そして、マッピング管理部170は、属性マッピング処理を指示した端末102に、生成したデータを送る。端末102の出力プログラム及び出力装置212は、受信したデータに基づいて属性マッピングエディタのユーザインタフェース700を表示する。

【0101】

図7は、本実施例の属性マッピングエディタのユーザインタフェース700を示す説明図である。

【0102】

図7に示すユーザインタフェース700は、属性マッピングエディタの例であり、情報管理システム100から取得した属性と、情報共有サーバ160が有する基準の属性とを、情報管理システム100の運用管理者がマッピングするインタフェースであれば、いかなるインタフェースでもよい。

【0103】

図7に示すユーザインタフェース700は、三つの表示領域(702、704、710)から構成される。表示領域702は、処理のタイトルを表示する領域である。

【0104】

表示領域704は、機能ボタンを表示する領域である。表示領域710は、属性をマッピングする領域である。

【0105】

表示領域710は、複数のボタン(720、722、724、706、760)、及び、領域(730、740、750)を表示する。ボタン720は、情報属性をマッピングする際に操作するボタンである。ボタン722は、ユーザ属性をマッピングする際に操作するボタンである。ボタン724は、その他属性をマッピングする際に操作するボタンである。

【0106】

マッピング管理部170は、ボタン720、ボタン722及びボタン724の少なくとも一つが操作されたことを検知した場合、マッピングする属性が選択されたことを可視的に表示するため、例えば、操作されたボタンを他のボタンと違う色に着色して表示してもよい。

【0107】

表示領域730は、情報管理システム100からインポートした属性を表示する。マッピング管理部170は、情報管理システム100から属性の階層構造が取得できる場合、階層構造を示すツリー構造を表示領域730に表示してもよい。

【0108】

表示領域740は、属性辞書184からインポートした属性の項目及び値の識別子を表示する。属性辞書184が属性の階層構造を保持する場合、マッピング管理部170は、階層構造を示すツリー構造を表示領域740に表示してもよい。

【0109】

10

20

30

40

50

また、マッピング管理部 170 は、属性の識別子を示す表示領域に所定の操作がされた場合、操作された表示領域に対応する属性の説明文を、属性辞書 184 の表示領域 706 から取得し、表示領域 742 に表示してもよい。

【0110】

運用管理者は、表示領域 742 に表示された説明文を参照することで、情報管理システム 100 における属性のセキュリティレベルと、基準の属性のセキュリティレベルとの対応関係を識別することができる。そして、これによって、異なる情報管理システム 100 において各々用いられている属性を対応づけることができる。

【0111】

情報管理システム 100 の運用管理者が表示領域 706 を押下した場合、マッピング管理部 170 は、表示領域 710 における描画ツールを起動する。

10

【0112】

運用管理者は、起動した描画ツールを使って、情報管理システム 100 の属性と、属性辞書 184 の属性とを、例えば矢印の図形オブジェクトによって視覚的に接続することにより、マッピングする。マッピング管理部 170 は、表示領域 710 においてマッピングができれば、いかなるツールを起動してもよい。

【0113】

表示領域 750 は、情報管理システム 100 の属性管理方法を示す。マッピング管理部 170 は、属性マッピング処理の指示の送信元である情報管理システム 100 の属性管理方法を接続システム情報 174 の領域 506 から取得し、取得した値を表示領域 750 に表示する。

20

【0114】

ボタン 760 は、マッピング結果を情報共有サーバ 160 に登録するためのボタンである。表示領域 730 及び表示領域 740 間のマッピングが終了した後、マッピング結果を情報共有サーバ 160 に反映する場合、運用管理者は、ボタン 760 を操作する。

【0115】

運用管理者が、ボタン 760 を押下した場合、表示領域 710 においてマッピングされた情報は、図 8 に示すデータ構造で情報共有サーバ 160 に格納される。

【0116】

図 8 は、本実施例のマッピング情報 182 を示す説明図である。

30

【0117】

マッピング情報 182 は、複数の領域（800、802、804、806、808、810、812～816）を含む。マッピング情報 182 は、ユーザ属性、情報属性、及び、その他属性を有する。図 8 に示すマッピング情報 182 は、機密性に関する情報属性のマッピング情報と、ユーザの所属に関するユーザ属性のマッピング情報とを含む。

【0118】

領域 800 は、情報管理システム 100 の各々と情報共有サーバ 160 とを特定するための識別子を示す。図 8 に示す "Sys_global" は、情報共有サーバ 160 を示す。"Sys_no1" と "Sys_no2" とは、それぞれ情報管理システム 100-1 と情報管理システム 100-2 とを示す。

40

【0119】

マッピング情報 182 は、システムごとに複数のエントリ（817～822）を有する。エントリ 817 及び 820 は、情報共有サーバ 160 が有する基準の属性の定義（すなわち表現）を含む。エントリ（818、819、821 及び 822）は、情報管理システム 100 において用いられる属性の定義（すなわち表現）を含む。

【0120】

領域 802 及び領域 813 は、領域 800 が示す情報管理システム 100 において用いられる、属性の項目を定義する識別子を示す。領域（804、806、808、810 及び 812）は、領域 800 が示す情報管理システム 100 において用いられる、情報属性の値を定義する識別子を示す。また、領域（814～816）は、領域 800 が示す情報

50

管理システム 100 において用いられる、ユーザ属性の値を定義する識別子を示す。

【0121】

マッピング情報 182 には、属性の項目を定義する識別子を示す領域と、属性の値を定義する識別子を示す領域とが、あらかじめ設定される。

【0122】

領域 (802、804、806、808、810、812～816) は、図 8 において、単語によって表現される識別子を含むが、属性を識別できればいかなる文字列又は数列を含んでもよい。

【0123】

情報共有サーバ 160 のマッピング管理部 170 等は、マッピング情報 182 を参照することによって、属性辞書 184 において定義された基準の属性と、情報管理システム 100 の各々で用いられる属性との対応関係を取得する。そして、これにより、後述するアクセスルール生成処理において用いられる属性の変換処理を実行することができる。

10

【0124】

また、属性辞書 184 が基準の属性を保持することにより、新たな情報管理システム 100 が追加した場合にも、マッピング管理部 170 は、基準の属性と新たな情報管理システム 100 において用いられる属性とを対応させることができるため、属性を容易に追加できる。

【0125】

図 7 の例では、情報に対する属性名のマッピングとして、秘密区分と機密性取扱区分が対応付けられている。また、属性の値のマッピングとして、極秘と機密度 5、秘と機密度 4、注意と機密度 3、区分無と機密度 1 が対応付けられている。

20

【0126】

なお、マッピング管理部 170 は、ユーザインタフェース 700 を表示している間、マッピング処理において発生する警告を、警告ダイアログ 900 として表示してもよい。

【0127】

図 9 は、本実施例のユーザインタフェース 700 に表示される警告ダイアログ 900 を示す説明図である。

【0128】

マッピング管理部 170 は、ボタン 760 が押下されたことを検知した場合、属性をインポートした情報管理システム 100 に対応するマッピング情報 182 のエントリを特定し、値が格納されていない領域を検索する。検索の結果、値が格納されていない領域が特定された場合、マッピング管理部 170 は、図 9 に示す警告ダイアログ 900 を表示してもよい。

30

【0129】

警告ダイアログ 900 は、他の情報管理システム 100 からインポートされた属性がマッピングされた基準の属性に、ユーザインタフェース 700 に表示された情報管理システム 100 において用いられる属性がマッピングされていないことを警告し、属性の入力を指示する表示である。

【0130】

警告ダイアログ 900 を表示することにより、他の情報管理システム 100 において必要な属性への、マッピング忘れを防ぐことが可能になり、情報の共有を阻害する要因を取り除くことができる。

40

【0131】

運用管理処理 404 の他の例は、アクセスルール生成処理である。情報管理システム #1 (100-1) の運用管理者がアクセスルール生成処理を行う手順を、例として以下に記載する。

【0132】

共有制御部 162 がステップ 402 において、アクセスルール生成処理の運用管理処理を開始する指示を受け付けたと判定した場合、アクセスルール管理部 168 は、ステップ

50

404において、アクセスルール生成処理を開始する。

【0133】

アクセスルール生成処理を開始後、アクセスルール管理部168は、情報管理サーバ104に格納されたアクセスルール118からアクセスルールをインポートする。アクセスルール118は、複数のレコードから構成される。アクセスルール118の1レコードには、ユーザ属性の条件、情報属性の条件、その他属性の条件、及び、許可される権限が定義される。

【0134】

そして、アクセスルール管理部168は、情報共有サーバ160が有するマッピング情報182を参照する。そして、アクセスルール管理部168は、運用管理インタフェース172を介して、運用管理者の操作を受け付けた端末102に、図10に示すユーザインタフェース1000を持つアクセスルールエディタの機能を提供する。

10

【0135】

図10は、本実施例のユーザインタフェース1000を示す説明図である。

【0136】

図10で示すアクセスルールエディタのユーザインタフェース1000は、三つの表示領域(1002、1004、1010)から構成される。表示領域1002は、タイトルを表示する領域である。表示領域1004は、機能ボタンを表示する領域である。表示領域1010は、アクセスルールを生成する領域である。

20

【0137】

表示領域1004は、情報管理システム100からインポートしたアクセスルールの定義を、選択するための機能ボタンを表示する。表示領域1004は、前ボタン1006及び次ボタン1008を含む。前ボタン1006は、表示領域1010に表示中のアクセスルールより、前のアクセスルールのレコードを表示するための領域であり、次ボタン1008は、次のアクセスルールのレコードを表示するための領域である。

【0138】

表示領域1010は、情報管理システム100において用いられる表現による属性の名称及び条件を表示する。また、表示領域1010には、インポートされたアクセスルールがデフォルトで表示される。表示領域1010には、条件1020、条件1030、条件1040及び認可アクション1050を含む。

30

【0139】

条件1020は、情報属性の値の条件を入力する領域である。条件1030は、ユーザ属性の値の条件を入力する領域である。条件1040は、その他属性の値の条件を入力する領域である。認可アクション1050は、条件1020、条件1030及び条件1040において定義された属性に、許可される共有情報への操作内容を示す。

【0140】

条件1020、条件1030、及び条件1040は、属性1072、演算子1074、値1076、及び選択肢1078を各々含む。また、認可アクション1050は、値1076及び選択肢1078を含む。

【0141】

属性1072は、情報管理システム100において用いられる属性の項目名を示す。属性1072は、マッピング情報182において、領域802又は領域813に相当する値を表示する。

40

【0142】

演算子1074は、情報管理システム100において用いられる属性の条件を示す。図10において演算子1074は、等号不等号等の論理演算子又は比較演算子によって示されるが、属性の条件を示せば、いかなる表現を含んでもよい。

【0143】

また、本実施例において、演算子1074に表示される値は、複数の情報管理システム100間において共通の方法によって表現される論理演算子等である。しかし、演算子1

50

074に表示される値が複数の情報管理システム100間において異なる場合、マッピング管理部は、ユーザ属性及び情報属性と同じく、ユーザインタフェース700を用いて基準の演算子と各情報管理システム100の演算子とをマッピングしてもよい。

【0144】

値1076に入力される値は、属性の値を示す。値1076は、マッピング情報182において、領域(804、806、808、810、812、及び、814～816)に相当する値を表示する。

【0145】

選択肢1078は、アクセスルールとして採用するか否かを運用管理者に選択させる領域である。また、運用管理者は、認可アクション1050における値1076及び選択肢1078を操作することによって、権限を追加及び修正することが可能である。

10

【0146】

アクセスルール管理部168は、インポートされたアクセスルールに含まれない属性も、表示領域1010に表示してもよい。具体的には、アクセスルール管理部168は、マッピング情報182に定義されている基準の属性(エントリ817、820)の中から、情報管理システム100からインポートしたアクセスルールには含まれない属性の項目を抽出してもよい。そして、アクセスルール管理部168は、抽出した項目を表示領域1010に表示してもよい。

【0147】

図10に示す条件1040の属性1072において、アクセスルール管理部168は、情報管理システム100からインポートしたアクセスルールには含まれない属性の項目である、「場所」と「時間」とを表示する。これによって、アクセスルール管理部168は、情報共有サーバ160が持っている属性情報を用いて、運用管理者による入力漏れを抑制することができる。

20

【0148】

情報管理システム100の運用管理者は、表示領域1010に表示されたアクセスルールを変更、削除及び追加することによって、情報共有サーバ160に登録するアクセスルールを生成する。そして、後述の処理によって共有情報にアクセスルールを割り当てることによって、複数の情報管理システム100間で同じアクセスルールを用いることができる。

30

【0149】

表示領域1010は、ルール登録ボタン1060を含む。アクセスルール管理部168は、ルール登録ボタン1060が操作された場合、表示領域1010において生成されたアクセスルールをアクセスルール180に格納する。

【0150】

図11は、本実施例のアクセスルール180を示す説明図である。

【0151】

アクセスルール180は、複数の領域(1102、1104、1106、1108、1110及び1112)を含む。

【0152】

40

領域1102は、情報管理システム100の各々と情報共有サーバ160とを特定するための識別子を示す。領域1104は、アクセスルールを識別するための識別子を示す。

【0153】

領域1106は、条件1030において設定されたユーザ属性の条件を示す。領域1108は、条件1020において設定された情報属性の条件を示す。領域1110は、条件1040において設定されたその他属性の条件を示す。領域1112は、認可アクション1050において設定された権限を示す。

【0154】

図11に示す領域1106、領域1108及び領域1112が示す条件は、論理演算子又は比較演算子等を用いて表現される。領域1112は、許可される共有情報への操作内

50

容を示す。

【0155】

例えば、図11に示す領域1106には、ユーザ属性の条件として、「秘密区分≧秘 and 所属部署=A部署」が格納される。また、図11に示す領域1108には、情報属性の条件として、「秘密区分=秘 and 分類=統計資料」が格納される。図11に示す領域1110には、その他属性の条件として、「時間=9:00-17:00」が格納される。図11に示す領域1112には、権限として「閲覧」が格納される。

【0156】

アクセスルール180における各エントリは、領域1102が示す情報管理システム100において用いられた属性の定義によって表現される。

10

【0157】

図12は、本実施例の情報管理サーバ#1(104)から情報共有サーバ160に共有情報を送信する処理を示すシーケンス図である。

【0158】

情報116が更新された場合、又は、運用管理者から情報116を共有する指示を受け付けた場合、情報管理サーバ#1(104)の情報管理部106は、共有する共有情報を含む第1の共有情報パッケージを生成する(1210)。第1の共有情報パッケージは、情報116に含まれる共有する情報(共有情報)を含む。

【0159】

シーケンス1210の後、情報管理部106は、第1の共有情報パッケージを情報共有サーバ160に送信する(1212)。情報共有サーバ160が第1の共有情報パッケージを受信した場合(1220)、共有情報管理部166は、受信した第1の共有情報パッケージの共有情報に、情報共有サーバ160において一意な識別子を割り当てる。

20

【0160】

図13は、本実施例の情報共有サーバ160が受け付けた第1の共有情報パッケージを示す説明図である。

【0161】

第1の共有情報パッケージは、複数の領域(1304、1306、1308、1310、1312、及び1314)を含む。また、共有情報管理部166は、第1の共有情報パッケージに領域1302を付加する。

30

【0162】

領域1302は、第1の共有情報パッケージに含まれる共有情報を一意に示す識別子である。領域1302が示す識別子は、例えば、共有情報が含まれるファイルの識別子と、情報管理システム#1(100-1)の識別子とを結合した識別子である。

【0163】

領域1304は、領域1302が示す共有情報のバイナリデータを格納する。領域1306は、領域1304に格納された共有情報の、情報属性を示す。

【0164】

なお、図13に示す第1の共有情報パッケージは、情報管理システム#1(100-1)が独立型管理方法によって情報116の情報属性を管理する場合に生成されたパッケージである。情報管理システム#1(100-1)が一体型管理方法によって情報116の情報属性を管理する場合、領域1306は、例えばnull値を含み、領域1304が情報属性を含む。

40

【0165】

領域1308は、領域1304に格納された共有情報に、領域1314が示す操作を行うことが可能なユーザのユーザ属性を示す。領域1310は、領域1314が示す操作を行うことが可能な共有情報の、情報属性を示す。このため、領域1306は、領域1310が示す情報属性を少なくとも含む。

【0166】

その他属性の条件1312は、領域1304に格納された共有情報に、領域1314が

50

示す操作を行うことが可能な状況等の属性を示す。領域1314は、領域1304に格納された共有情報に許可される操作を示す。領域(1308、1310、1312、及び1314)は、領域1304が示す共有情報へのアクセスルールを示す。

【0167】

図13に示す領域(1308、1310、1312、及び1314)は、null値を格納する。本実施例の情報管理部106は、第1の共有情報パッケージの領域(1308、1310、1312、及び1314)に、アクセスルールを格納しなくてもよい。そして、この場合、情報共有サーバ160が、後述する処理により共有情報にアクセスルールを割り当ててもよい。

【0168】

シーケンス1220の後、共有情報管理部166は、受信した第1の共有情報パッケージから、領域(1304、1306、1308、1310、1312及び1314)に格納された共有情報、情報属性、及びアクセスルールを抽出する(1222)。

【0169】

また、第1の共有情報パッケージの領域(1308、1310、1312、及び1314)がnull値である場合、共有情報管理部166は、シーケンス1222において、情報共有サーバ160に事前に登録されていたアクセスルール180から、領域(1308、1310、1312、及び1314)に対応するアクセスルールを抽出する。そして、共有情報管理部166は、抽出したアクセスルールを第1の共有情報パッケージに含まれる共有情報に割り当てる。

【0170】

具体的には、共有情報管理部166は、領域1102が第1の共有情報パッケージを送信した情報管理システム100を示し、かつ、領域1108が領域1306の情報属性を少なくとも含むアクセスルール180のエントリを特定する。そして、共有情報管理部166は、特定したエントリの領域(1106、1108、1110及び1112)の値を、第1の共有情報パッケージに含まれる共有情報のアクセスルールとして抽出する。

【0171】

これにより、情報管理システム100は、第1の共有情報パッケージを送信する毎に、共有情報に適用するアクセスルールを情報共有サーバ160に送信する必要がない。また、情報共有サーバ160に登録済みのアクセスルールを共有情報に割り当てることによって、複数の情報管理システム100が同じアクセスルールを割り当てられた共有情報を受信した場合、同じアクセスルールを用いることができる。

【0172】

なお、第1の共有情報パッケージは、情報を送信する情報管理システム100の固有な表現による属性を含む。

【0173】

シーケンス1222の後、共有情報管理部166は、マッピング情報182を参照する。そして、共有情報管理部166は、抽出した領域(1304、1306、1308、1310、1312及び1314)に含まれる属性の表現を、マッピング情報182に基づいて、基準の属性の表現に変換する(1224)。

【0174】

ここで、第1の共有情報パッケージを送信した情報管理システム100が、一体型管理方法によって情報属性を管理する場合(すなわち、接続システム情報174の領域506が「代替データストリーム」を示す場合)、領域1304から抽出した共有情報に含まれる情報属性の表現を、基準の情報属性の表現に変換する。

【0175】

シーケンス1224の後、共有情報管理部166は、含んでいる属性を基準の属性に変換された領域(1304、1306、1308、1310、1312及び1314)を、基準の属性によって定義された共有情報パッケージとして、共有情報178に格納する(1226)。また、共有情報管理部166は、シーケンス1220において割り当てられ

10

20

30

40

50

た共有情報の識別子を、共有情報１７８に格納する。

【０１７６】

図１４は、本実施例の共有情報１７８を示す説明図である。

【０１７７】

共有情報１７８は、複数の領域（１４０２、１４０４、１４０６、１４０８、１４１０、１４１２及び１４１４）を含む。共有情報１７８のエントリは、第１の共有情報パッケージの内容を含む。このため、領域（１４０２、１４０４、１４０６、１４０８、１４１０、１４１２及び１４１４）は、領域（１３０２、１３０４、１３０６、１３０８、１３１０、１３１２、及び１３１４）に対応する。

【０１７８】

共有情報１７８の領域（１４０６、１４０８、１４１０、１４１２及び１４１４）の属性は、属性辞書１８４で定義される基準の属性によって表現される。図１４に示す共有情報１７８は、エントリ１４１６を含む。エントリ１４１６は、図１３に示す第１の共有情報パッケージに対応する。

【０１７９】

なお、シーケンス１２２６において、接続システム管理部１６４は、共有情報を受信したことを記録するため、受信した第１の共有情報パッケージに基づいて接続システム情報１７４を更新する。具体的には、接続システム管理部１６４は、第１の共有情報パッケージを送信した情報管理システム１００を示す識別子を、領域５２２に格納し、第１の共有情報パッケージを受信した日時を領域５２４に格納する。

【０１８０】

また、接続システム管理部１６４は、受信を示す文字列又は識別子を領域５２６に格納し、第１の共有情報パッケージが格納された共有情報１７８の領域１４０２の値を領域５２８に格納する。

【０１８１】

これにより、共有情報管理部１６６は、接続システム情報１７４を参照することによって、新たな共有情報を受け付けたか否かを判定できる。

【０１８２】

また、共有情報管理部１６６は、シーケンス１２２６において、領域（１４０６、１４０８、１４１０、１４１２及び１４１４）に含まれる属性を属性情報１７６に格納してもよい。

【０１８３】

図１５は、本実施例の情報管理サーバ＃Ｎ（１３４）が、情報共有サーバ１６０から共有情報１７８を取得する処理を示すシーケンス図である。

【０１８４】

情報管理サーバ＃Ｎ（１３４）の情報管理部１３６は、あらかじめ設定された一定時間毎、又は、運用管理者若しくは利用者が指示した際、共有情報へのアクセスを要求する。具体的には、情報管理部１３６は、新規登録された共有情報１７８、又は、更新された共有情報１７８を、情報共有サーバ１６０に要求する（１５１０）。

【０１８５】

図１５において、情報管理サーバ＃Ｎ（１３４）の情報管理部１３６が共有情報へのアクセスを要求したが、本実施例において情報管理サーバ＃１（１０４）の情報管理部１３６が共有情報へのアクセスを要求してもよい。

【０１８６】

情報管理サーバ＃Ｎ（１３４）から要求を受け付けた場合（１５１２）、情報共有サーバ１６０の共有情報管理部１６６は、接続システム情報１７４に含まれる領域（５２２、５２４、５２６及び５２８）を参照し、情報管理サーバ＃Ｎ（１３４）に未送信の共有情報を特定する。

【０１８７】

具体的には、共有情報管理部１６６は、領域５２６が「受信」を示すエントリの領域５

10

20

30

40

50

28の共有情報識別子を特定する。そして、共有情報管理部166は、特定した共有情報識別子を領域528に格納し、領域526が「送信」を示し、かつ、領域522が情報管理システム#N(100-N)を示すエントリ(以下、エントリAと記載)があるか否かを判定する。エントリAがない場合、共有情報管理部166は、特定した共有情報識別子の共有情報を、情報管理システム#N(100-N)に未送信の共有情報であると特定する(1514)。

【0188】

シーケンス1514の後、共有情報管理部166は、未送信の共有情報を含む共有情報178のエントリ(以下、エントリBと記載)を抽出する。そして、抽出したエントリBの領域(1406、1408、1410及び1412)に含まれる属性の表現(基準の属性の表現)を、マッピング情報182を用いて、情報管理システム#N(100-N)において用いられる属性の表現に変換する(1516)。

10

【0189】

なお、シーケンス1516において、共有情報管理部166は、接続システム情報174の領域506を参照し、共有情報の送信先の情報管理システム100の属性管理方法に従って、エントリBに含まれる共有情報と情報属性とを更新する。

【0190】

具体的には、情報管理システム#N(100-N)の属性管理方法が一体型管理方法であり(例えば、領域506が「アプリケーションメタデータ」を示す場合)、かつ、共有情報178の領域1406がNull値を格納しない場合、共有情報管理部166は、領域506が示す方法に従って、領域1404の共有情報の中に領域1406の情報属性を含めるように、領域1404に含まれる共有情報を更新する。

20

【0191】

また、シーケンス1516において、情報管理システム#N(100-N)の属性管理方法が独立型管理方法であり(例えば、領域506が「代替データストリーム」を示す場合)、かつ、共有情報178の領域1406がNull値を格納する場合、共有情報管理部166は、領域506が示す方法に従って、領域1404の共有情報の中から情報属性を抽出する。そして、共有情報管理部166は、抽出した情報属性を領域1406に格納する。

【0192】

これにより、エントリBの内容が含まれる後述の第2の共有情報パッケージを受信した場合、情報管理システム100は、受信した共有情報を変更することなく、自システムにおける方法に従って情報属性を利用者に閲覧させることができる。そして、これにより情報管理システム100間において情報を容易に共有できる。

30

【0193】

シーケンス1516の後、共有情報管理部166は、情報管理システム#N(100-N)が未送信の共有情報のアクセスルールを順守可能か否かを、マッピング情報182を用いて判定する(1518)。具体的には、以下の方法により判定する。

【0194】

共有情報管理部166は、エントリBの領域(1408、1410、1412及び1414)が示すアクセスルールに、構成要素として含まれる基準の属性の全てが情報管理システム#N(100-N)の属性に変換できた場合、情報管理システム#N(100-N)が未送信の共有情報のアクセスルールを順守可能であると判定する。

40

【0195】

より具体的には、エントリBの領域(1408、1410、1412及び1414)に含まれる基準の属性に、情報管理システム#N(100-N)において用いられる属性がマッピングされている場合、共有情報管理部166は、順守可能であると判定する。

【0196】

そして、エントリBのアクセスルールに含まれる少なくとも一つの属性が情報管理システム#N(100-N)において用いられる属性にマッピングされていない場合、共有情

50

報管理部 166 は、情報管理システム #N (100-N) が未送信の共有情報のアクセスルールを順守不可能であると判定する。

【0197】

情報管理システム #N (100-N) が未送信の共有情報のアクセスルールを順守不可能であると判定した場合、共有情報管理部 166 は、エントリ B の内容を情報管理システム #N (100-N) に送信しないことを決定し、図 15 に示す処理を終了する (1520)。

【0198】

これは、エントリ B の共有情報に求められるアクセスルールは、情報管理システム #N (100-N) において共有情報に適用できないためである。これにより、情報共有サーバ 160 は、エントリ B の共有情報に求められるセキュリティレベルを維持することができる。

10

【0199】

一方、情報管理システム #N (100-N) が未送信の共有情報のアクセスルールを順守可能であると判定した場合、共有情報管理部 166 は、エントリ B の内容を含む第 2 の共有情報パッケージを生成する (1522)。

【0200】

図 16 は、本実施例の第 2 の共有情報パッケージを示す説明図である。

【0201】

第 2 の共有情報パッケージは、共有情報へのアクセスを要求してきた情報管理システム 100 に、共有情報と、当該共有情報に適用されるアクセスルールとを提供するための提供情報である。

20

【0202】

第 2 の共有情報パッケージは、複数の領域 (1602、1604、1606、1608、1610、1612 及び 1614) を含む。第 2 の共有情報パッケージは、共有情報 178 のエントリの内容を含む。このため、領域 (1602、1604、1606、1608、1610、1612 及び 1614) は、領域 (1402、1404、1406、1408、1410、1412 及び 1414) の値を格納する。

【0203】

図 16 に示す第 2 の共有情報パッケージは、図 14 に示す共有情報 178 のエントリ 1416 に含まれる属性を、情報管理システム #N (100-N) において用いられる属性に変換した結果である。

30

【0204】

また、図 16 に示す第 2 の共有情報パッケージは、情報管理システム #N (100-N) に送信される。その情報管理システム #N (100-N) は、一体型管理方法によって情報属性を管理するため、図 16 に示す第 2 の共有情報パッケージの領域 1606 には情報属性が格納されておらず、領域 1604 の共有情報内に情報属性が格納される。

【0205】

シーケンス 1522 の後、共有情報管理部 166 は、第 2 の共有情報パッケージを情報管理サーバ #N (134) へ送信する (1524)。第 2 の共有情報パッケージを送信した場合、共有情報管理部 166 は、接続システム情報 174 を更新する。具体的には、共有情報管理部 166 は、第 2 の共有情報パッケージの送信先である情報管理システム 100 の識別子を領域 522 に格納し、第 2 の共有情報パッケージを送信した日時を領域 524 に格納し、領域 526 に「送信」を示す値を格納し、第 2 の共有情報パッケージに付加されていた共有情報識別子を領域 528 に格納した新たなエントリを、接続システム情報 174 に追加する。

40

【0206】

シーケンス 1522 の後、情報管理サーバ #N (134) の情報管理部 136 は、情報共有サーバ 160 から第 2 の共有情報パッケージを受信する (1526)。

【0207】

50

なお、共有情報管理部 166 は、送信先の情報管理システム #N (100-N) が領域 1602 の識別子を必要としない場合、シーケンス 1524 において領域 1602 を削除したうえで、第 2 の共有情報パッケージを送信してもよい。

【0208】

シーケンス 1526 の後、情報管理部 136 は、受信した第 2 の共有情報パッケージの内容を、ユーザ属性 142、情報 144 及びアクセスルール 146 に格納する。具体的には、情報管理部 136 は、領域 1604 の内容を情報 144 に格納する。また、情報管理部 136 は、領域 (1608、1610、1612 及び 1614) の内容をアクセスルール 146 に格納する (1528)。

【0209】

なお、情報共有サーバ 160 において新規の共有情報、又は、修正された共有情報が登録された場合、共有情報管理部 166 は、図 15 に示すシーケンス 1514 以降を実行し、情報共有サーバ 160 に接続されている情報管理サーバに共有情報を送信してもよい。

【0210】

本実施例によれば、異なる属性によって定義されたアクセス制御モデルを採用する複数の情報管理システム 100 間の情報共有において、属性情報及びアクセスルールの表現の違いを変換する方法を提供する。これにより、情報管理システム 100 間において情報を共有することができ、かつ、共有された情報へのセキュリティを保つことができる。

【0211】

また、運用管理者が、情報を共有する情報管理システム 100 毎に属性を変換したり、アクセスルールの表現を変換したり、共有情報に付加する情報属性の属性管理方法を変換したりするなどの運用の手間を省略することができる。

【0212】

なお、前述の属性管理方法は、情報属性の管理方法を示したが、ユーザ属性の管理方法を示してもよい。具体的には、ユーザ属性を共有情報に含めるように共有情報を更新してもよいし、ユーザ属性を共有情報から抽出して別のファイルを生成してもよい。

【0213】

本発明は上記した実施例に限定されるものではなく、様々な変形例が含まれる。例えば、上記した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。

【0214】

また、ある実施例の構成の一部を他の実施例の構成に置き換えることが可能であり、また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

【0215】

また、上記の各構成、機能、処理部、処理手順等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、又はファイル等の情報は、メモリ、ハードディスク若しくは SSD (Solid State Drive) 等の記録装置、又は、IC カード、SD カード若しくは DVD 等の記録媒体に置くことができる。

【0216】

また、制御線又は情報線は説明上必要と考えられるものを示しており、製品上必ずしも全ての制御線又は情報線を示しているとは限らない。実際には殆ど全ての構成が相互に接続されている。

【符号の説明】

【0217】

100 情報管理システム

102、132 端末

10

20

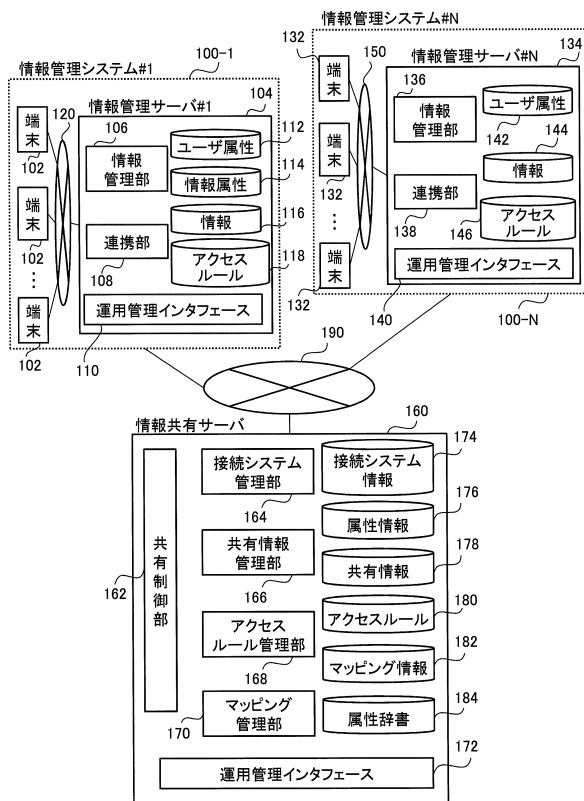
30

40

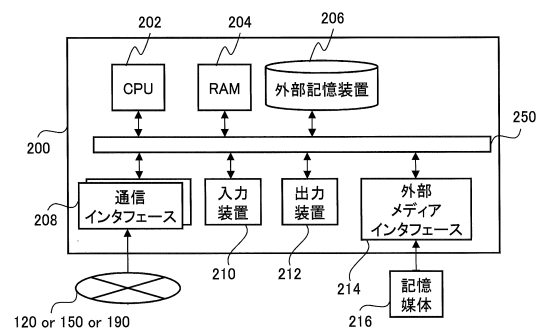
50

104、134 情報管理サーバ
 160 情報共有サーバ
 120、150、190 通信ネットワーク

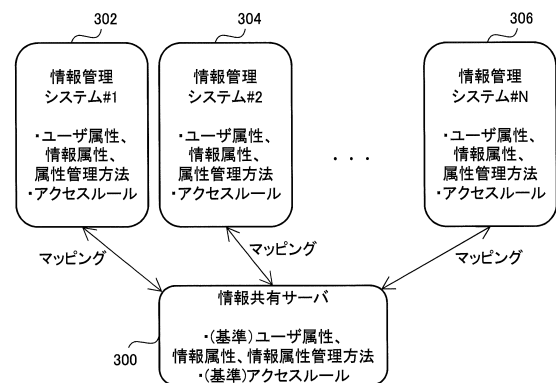
【図 1】



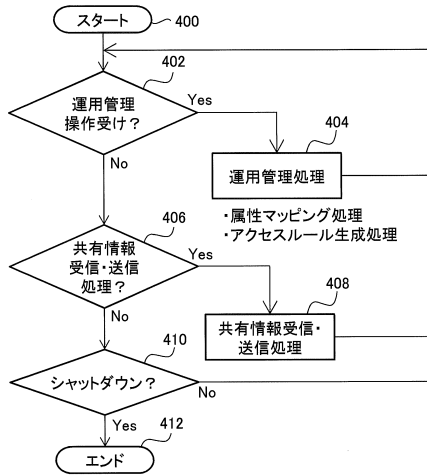
【図 2】



【図 3】



【図 4】



【図 5】

500	502	504	506	508	510	512
システム 識別子	システム クレデンシャル	情報属性 管理方法	管理者 識別子	管理者 クレデンシャル	送受信情報 への参照	
Sys_no1	公開鍵証明書	代替データ ストリーム	admin_m	パスワード	table="aaa"	
Sys_no2	公開鍵証明書	アプリケーション メタデータ	admin_n	公開鍵証明書	table="bbb"	
...	...	...	...	...	...	

522	524	526	528
システム 識別子	日時	送受信タイプ	共有情報識別子
Sys_no1	2014-1-3 13:45	受信	00-12-33-44-55-66
...	...	...	...

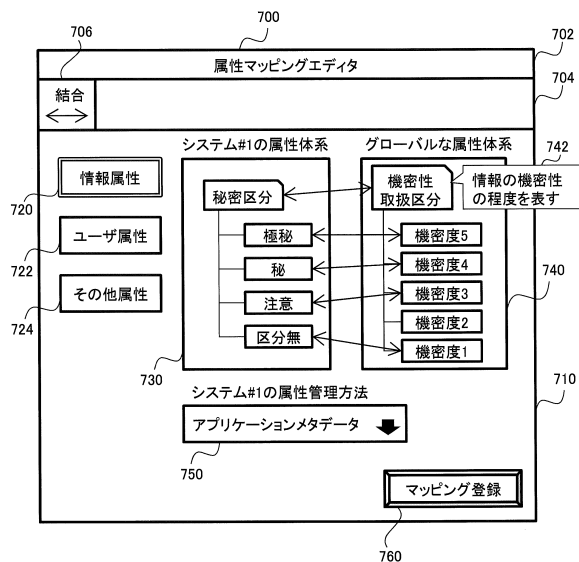
接続システム情報

【図 6】

600	602	604	606	184
分類	属性	値定義	使用ガイドライン	
情報	機密性 取扱区分	-	情報の機密性の程度を表す	
情報	機密性 取扱区分	機密度5	権限の無いユーザに開示された場合、組織及び 関係組織の存続に係る悪影響が発生する	
情報	機密性 取扱区分	機密度4	権限の無いユーザに開示された場合、組織の存 続に係る悪影響が発生する。関係組織には少な い悪影響を与える	
...	...	...	...	
ユーザ	役職	-	組織内の権限を表す	
ユーザ	役職	課長	アクセスを制限する情報にアクセスするため、 必要な権限のうち最も低い権限を有する	
...	...	...	...	

属性辞書

【図 7】



【図 8】

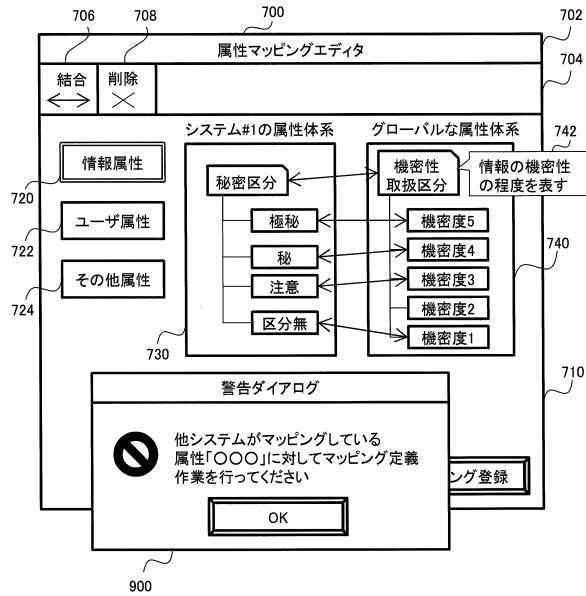
800	802	804	806	808	810	812
Sys_global	機密性 取扱区分	機密度5	機密度4	機密度3	機密度2	機密度1
Sys_no1	秘密区分	極秘	秘	注意	区分無し	
Sys_no2	機密 レベル	機密性5	機密性4	機密性3	機密性2	機密性1
...	...	...	...	...	...	...

マッピング情報(情報属性)

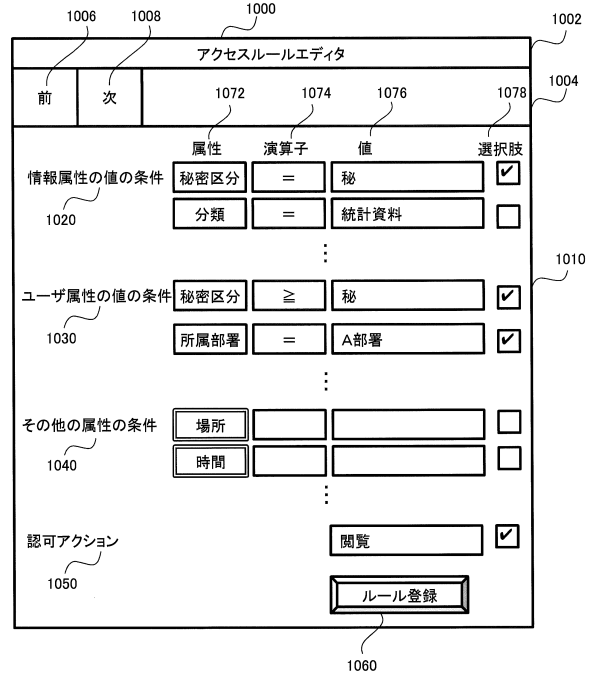
800	813	814	815	816
Sys_global	所属	所属1	所属2	所属3
Sys_no1	所属部署	A部署	B部署	C部署
Sys_no2	チーム	チーム1	チーム2	チーム3
...	...	...	...	...

マッピング情報(ユーザ属性)

【図 9】



【図 10】



【図 11】

システム識別子	アクセスルール識別子	ユーザ属性の条件	情報属性の条件	その他属性の条件	認可アクション
Sys_no1	Acl_001	機密区分 ≥ 秘、...	機密区分 = 秘、...	時間 = 9:00-17:00	閲覧
Sys_no1	Acl_002	...	...	...	...
...	...	...	...	...	...

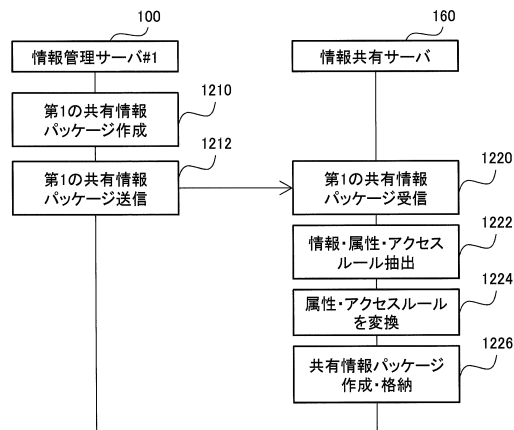
アクセスルール

【図 13】

共有情報識別子	情報データ	情報属性リスト	ユーザ属性の条件	情報属性の条件	その他属性の条件	認可アクション
Sys_no1-00-12-33-44-55-66	0110...	機密区分 = 秘、...	null	null	null	null

第1の共有情報パッケージ

【図 12】

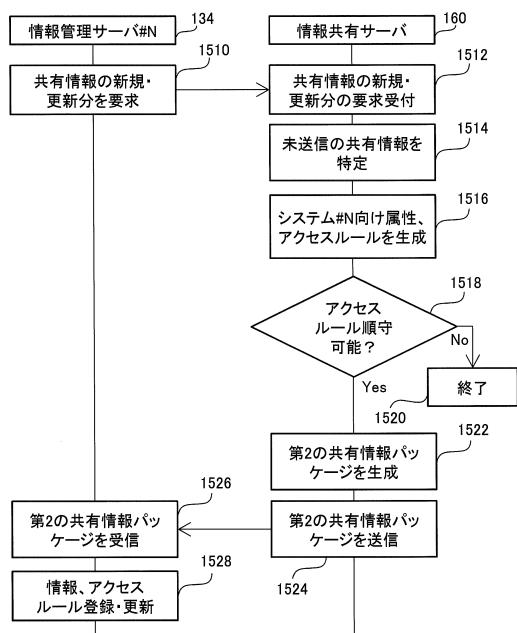


【図 14】

共有情報識別子	情報データ	情報属性リスト	ユーザ属性の条件	情報属性の条件	その他属性の条件	認可アクション
Sys_no1-00-12-33-44-55-66	0110...	機密性取扱区分 = 機密度4、...	秘密レベル ≥ 秘	機密性取扱区分 = 機密度4	時間 = 9:00-17:00	閲覧
...	...	...	...	...	...	...

アクセスルール

【図 15】



【図 16】

共有情報識別子	情報データ	情報属性リスト	ユーザ属性条件	情報属性条件	その他属性条件	認可アクション
Sys_no1-00-12-33-44-55-66	0110...	null	役職 ≥ 課長	機密レベル = 社外秘	時間 = 9:00-17:00	閲覧

第2の共有情報パッケージ

フロントページの続き

審査官 宮司 卓佳

- (56)参考文献 特開平6-250946 (JP, A)
国際公開第2009/113483 (WO, A1)
特開2000-112891 (JP, A)
特開2009-75672 (JP, A)
特表2009-539183 (JP, A)
米国特許出願公開第2008/0066151 (US, A1)
米国特許出願公開第2005/0015674 (US, A1)

- (58)調査した分野(Int.Cl., DB名)
G06F 21/60
G06F 13/00