

(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2009-122995

(P2009-122995A)

(43) 公開日 平成21年6月4日(2009.6.4)

(51) Int.Cl.
G06F 12/00 (2006.01)F I
G06F 12/00 520Eテーマコード (参考)
5B082

審査請求 未請求 請求項の数 13 O L (全 19 頁)

(21) 出願番号 特願2007-296781 (P2007-296781)
(22) 出願日 平成19年11月15日 (2007.11.15)(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 110000350
ポレール特許業務法人
(72) 発明者 伊藤 信治
神奈川県川崎市麻生区王禅寺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 本多 義則
神奈川県川崎市麻生区王禅寺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

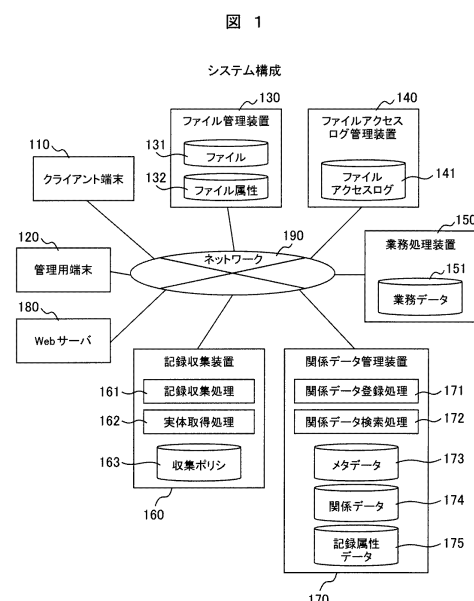
(54) 【発明の名称】 関連処理記録の管理システム及び管理方法

(57) 【要約】

【課題】 異種のシステムを跨いだ電子ファイルやログなどの記録を関連付け、関連する記録の検索を効率化する。

【解決手段】 本発明の関連処理記録の管理システム及びその方法は、各々異なる種別の処理記録を管理する複数の記録管理装置と、その複数の記録管理装置と接続し、予め設定した収集条件に基づいて複数の記録管理装置で管理される、異なる種別の処理記録を示すデータを取得する記録収集装置と、記録収集装置に接続し、取得されたデータから異なる種別の処理記録間の関係を示す関係データを生成し、生成した関係データを管理する関係データ管理装置とを有する。

【選択図】 図1



【特許請求の範囲】

【請求項 1】

各々異なる種別の処理記録を管理する複数の記録管理装置と、
前記複数の記録管理装置と接続し、予め設定した収集条件に基づいて前記複数の記録管理装置で管理される前記異なる種別の処理記録を示すデータを取得する記録収集装置と、
前記記録収集装置に接続し、前記取得されたデータから前記異なる種別の処理記録間の関係を示す関係データを生成し、前記生成した関係データを管理する関係データ管理装置とを有することを特徴とする関連処理記録の管理システム。

【請求項 2】

前記異なる種別の処理記録を示すデータは、少なくとも前記複数の記録管理装置の個々を特定する第 1 の識別子と前記異なる種別の処理記録の個々を特定する識別情報とを含むことを特徴とする請求項 1 記載の関連処理記録の管理システム。

10

【請求項 3】

前記予め設定した収集条件には、少なくとも個々の収集条件を特定する第 2 の識別子に対応して、前記第 1 の識別子、前記第 1 の識別子により特定される前記記録管理装置に管理される処理記録を検索するための検索条件、及び前記第 2 の識別子で特定される収集条件に関連する他の収集条件を特定する第 3 の識別子を含むことを特徴とする請求項 2 記載の関連処理記録の管理システム。

【請求項 4】

前記記録収集装置は、前記第 2 の識別子で特定される収集条件に基づいて前記第 1 の識別子により特定される前記記録管理装置に管理される処理記録を検索した後に、前記第 3 の識別子で特定される収集条件に基づく検索を実行し、前記関係データ管理装置は、前記第 3 の識別子で特定される収集条件に基づく第 1 の検索結果を登録した後に、前記第 2 の識別子で特定される収集条件に基づく第 2 の検索結果と、前記第 1 の検索結果と前記第 2 の検索結果とに基づいて生成した前記関係データとを登録することを特徴とする請求項 3 記載の関連処理記録の管理システム。

20

【請求項 5】

前記第 1 の検索結果と前記第 2 の検索結果との各々に識別子を付して、該各々に識別子の対応関係が前記関係データであることを特徴とする請求項 4 記載の関連処理記録の管理システム。

30

【請求項 6】

前記関係データ管理装置は、前記記録管理装置内の前記異なる種別の処理記録の個々を特定する識別情報と、前記関係データに含まれる前記第 1 の検索結果と前記第 2 の検索結果とに付された識別子の少なく一方とを含んだ検索要求に応答して、前記検索要求に含まれる前記第 1 の検索結果と前記第 2 の検索結果とに付された識別子を前記関係データの中で辿り、前記辿った識別子に対応する前記第 1 の検索結果と前記第 2 の検索結果との中から、前記識別情報で特定される処理記録を検索することを特徴とする請求項 5 記載の関連処理記録の管理システム。

【請求項 7】

前記複数の記録管理装置、前記記録収集装置、及び前記関係データ管理装置は、少なくとも 1 台のコンピュータ上にソフトウェアで実装されることを特徴とする請求項 2 記載の関連処理記録の管理システム。

40

【請求項 8】

複数の記録管理装置が各々異なる種別の処理記録を管理し、
前記複数の記録管理装置と接続する記録収集装置が、予め設定した収集条件に基づいて前記複数の記録管理装置で管理される前記異なる種別の処理記録を示すデータを取得し、
前記記録収集装置に接続する関係データ管理装置が、前記取得されたデータから前記異なる種別の処理記録間の関係を示す関係データを生成し、前記生成した関係データを管理することを特徴とする関連処理記録の管理方法。

【請求項 9】

50

前記異なる種別の処理記録を示すデータは、少なくとも前記複数の記録管理装置の個々を特定する第1の識別子と前記異なる種別の処理記録の個々を特定する識別情報とを含むことを特徴とする請求項8記載の関連処理記録の管理方法。

【請求項10】

前記予め設定した収集条件には、少なくとも個々の収集条件を特定する第2の識別子に対応して、前記第1の識別子、前記第1の識別子により特定される前記記録管理装置に管理される処理記録を検索するための検索条件、及び前記第2の識別子で特定される収集条件に関連する他の収集条件を特定する第3の識別子を含むことを特徴とする請求項9記載の関連処理記録の管理方法。

【請求項11】

10

前記記録収集装置は、前記第2の識別子で特定される収集条件に基づいて前記第1の識別子により特定される前記記録管理装置に管理される処理記録を検索し、前記第3の識別子で特定される収集条件に基づく検索を実行し、前記関係データ管理装置は、前記第3の識別子で特定される収集条件に基づく第1の検索結果を登録し、前記第2の識別子で特定される収集条件に基づく第2の検索結果と、前記第1の検索結果と前記第2の検索結果とに基づいて生成した前記関係データとを登録することを特徴とする請求項10記載の関連処理記録の管理方法。

【請求項12】

前記第1の検索結果と前記第2の検索結果との各々に識別子を付して、該各々に識別子の対応関係が前記関係データであることを特徴とする請求項11記載の関連処理記録の管理方法。

20

【請求項13】

前記関係データ管理装置は、前記記録管理装置内の前記異なる種別の処理記録の個々を特定する識別情報と、前記関係データに含まれる前記第1の検索結果と前記第2の検索結果とに付された識別子の少なくとも一方とを含んだ検索要求に応答して、前記検索要求に含まれる前記第1の検索結果と前記第2の検索結果とに付された識別子を前記関係データの中で辿り、前記辿った識別子に対応する前記第1の検索結果と前記第2の検索結果との中から、前記識別情報で特定される処理記録を検索することを特徴とする請求項12記載の関連処理記録の管理方法。

【発明の詳細な説明】

30

【技術分野】

【0001】

本発明は、各種業務で発生した電子ファイル、操作ログなどの記録を一元的に管理する関連処理記録の管理システム及びその管理方法に関する。

【背景技術】

【0002】

近年、各種法整備に伴い、企業は業務で発生した記録を適切に管理し、監査など必要に応じて、記録を閲覧可能にする、又は提示する必要がある。

【0003】

40

記録としては、例えば、紙で受け取った書類、電子メール、PC（パーソナル・コンピュータ）上で作成した電子ファイル、ファイルアクセスログ、アプリケーションプログラムの操作ログ、業務システムで管理されている業務データ（例、日付、品名、金額など）などが挙げられる。これらの記録を個別に収集し、管理するシステムは多数ある。しかし、各記録は、個々のシステムで独立して管理されているため、記録間の関係を追跡する必要がある場合には、人手でその関係を追う必要があり、非常に手間がかかる。

【0004】

このような課題に対して、特許文献1では、異なる業務システムで管理されている業務データを抽出し、共通のフォーマットに変換して管理することで、業務データの分析を効率化している。

【0005】

50

特許文献2では、業務システム、データベースサーバ等で個別に管理されているログを分析し、アクセスしたユーザを追跡する方法が開示されている。

【0006】

【特許文献1】US2006/0143231A1

【特許文献2】特開2007-48266号公報

【発明の開示】

【発明が解決しようとする課題】

【0007】

特許文献1で開示されている技術では、既存の業務システムで管理されているデータを共通のフォーマットに変換して、変換したデータを別途保管する必要がある。そのため、既存の業務システムとほぼ同容量の記憶領域が新たに必要となる。また、特許文献1で扱うデータは業務データが対象であり、異種の電子ファイルやログなどを対象として扱えない。

【0008】

特許文献2で開示されている技術では、ログを対象としたものであり、電子ファイルや業務データを扱えない。

【0009】

本発明は、以上の従来技術の問題点を考慮し、異種のシステムに亘る電子ファイルやログなどの異なる種類の処理記録であるが、互いに関連する処理記録を関連付け、関連する記録の検索を効率化するシステムを提供する。

【課題を解決するための手段】

【0010】

本発明の関連処理記録の管理システム及びその方法の態様は、各々異なる種別の処理記録を管理する複数の記録管理装置と、その複数の記録管理装置と接続し、予め設定した収集条件に基づいて複数の記録管理装置で管理される、異なる種別の処理記録を示すデータを取得する記録収集装置と、記録収集装置に接続し、取得されたデータから異なる種別の処理記録間の関係を示す関係データを生成し、生成した関係データを管理する関係データ管理装置とを有する。

【0011】

なお、上記各装置は、少なくとも1台のコンピュータ上にソフトウェアで実装されてもよい。

【発明の効果】

【0012】

本発明によれば、異種のシステムに亘る電子ファイルやログなどの異なる種類の処理記録であるが、互いに関連する処理記録を関連付けすることができるので、結果として関連する記録の検索を効率化できる。

【発明を実施するための最良の形態】

【0013】

本発明を実施するための最良の形態を説明する。

【0014】

図1は、本発明の実施形態に係るシステム構成の例を示した図である。図1に示すように、本システムは、クライアント端末110、管理用端末120、ファイル管理装置130、ファイルアクセスログ管理装置140、業務処理装置150、記録収集装置160、関係データ管理装置170、及びWebサーバ180を含み、これらの装置はネットワーク190を介して相互に接続されて構成される。ネットワーク190に接続する各装置は、少なくともCPU（Central Processing Unit）と記憶装置とを備えたコンピュータであり、その機能に応じて端末、サーバなどと呼ぶ。以下、これら各装置およびその装置の構成および動作について説明する。

【0015】

なお、以下では、ファイル管理装置130、ファイルアクセスログ管理装置140、及

び業務処理装置 150 の各装置又はそれらを総称して記録管理装置と呼ぶ場合がある。

【0016】

図 1 において、ユーザは、クライアント端末 110 の Web ブラウザや専用のプログラム等(図示せず)を使用して、見積や受注などの業務を遂行する。クライアント端末 110 は、クライアント端末 110 で作成したファイル、他の装置から受け取ったファイル、紙の書類をスキャナ等で電子化したファイル、ファイルに対するアクセスログ、Web ブラウザや専用プログラムに入力したデータなどを、ファイル管理装置 130、ファイルアクセスログ管理装置 140、業務処理装置 150 などの記録管理装置に登録する。具体的には、クライアント端末 110 がファイルやデータなどを記録管理装置に送ることにより、記録管理装置はそれらを処理記録として格納し、管理する。クライアント端末 110 は、各記録管理装置に送信する記録(ファイルやデータなど)間の関連性を示すデータを関係データ管理装置 170 に送信しても良い。

10

【0017】

ユーザは、管理用端末 120 の Web ブラウザや専用のプログラム等(図示せず)を使用して、各装置へのアクセス権の設定やバックアップの設定等の、各装置やその運用の全般を管理する。また、管理用端末 120 は、各装置に対して、検索クエリを発行し、検索結果を表示する。

【0018】

ファイル管理装置 130 は、クライアント端末 110 が登録(送信)したファイル 131 およびファイル属性 132 を記憶装置に格納する。

20

【0019】

ファイルアクセスログ管理装置 140 は、クライアント端末 110 で収集したファイルアクセスログ 141 を記憶装置に格納する。

【0020】

業務処理装置 150 は、クライアント端末 110 を用いてユーザが入力したデータや承認データなどの業務データ 151 を記憶装置に格納する。業務処理装置 150 によるシステムは、例えば、受注管理システム、ワークフローシステムなどである。

【0021】

記録収集装置 160 は、記録収集処理 161、実体取得処理 162 などの処理を実行する。これらの処理は CPU によって実行されるソフトウェアで実装される。記録収集処理 161 は、記憶装置に格納されている収集ポリシ 163 に基づき、記録管理装置にアクセスし、データを収集し、関係データ管理装置 170 に収集したデータを送信する処理である。実体取得処理 162 は、管理用端末 120 または Web サーバ 180 からの実体取得要求に基づき、ファイル管理装置 130、ファイルアクセスログ管理装置 140、業務処理装置 150 などの記録管理装置にアクセスして、実体データ(ファイルやデータの実体)、または実体データへのリファレンスを返す処理である。

30

【0022】

関係データ管理装置 170 は、関係データ登録処理 171、関係データ検索処理 172 などの処理を実行する。これらの処理は CPU によって実行されるソフトウェアで実装される。関係データ登録処理 171 は、クライアント端末 110 または記録収集装置 160 が送信したデータからメタデータ 173 および関係データ 174 を生成し、これらのデータを記憶装置に格納する処理である。関係データ検索処理 172 は、管理用端末 120 又は Web サーバ 180 からの検索要求に基づき、メタデータ 173 と関係データ 174 とから検索要求に対応したデータを抽出する処理である。

40

【0023】

Web サーバ 180 は、記録収集装置 160、関係データ管理装置 170、ファイル管理装置 130、ファイルアクセスログ管理装置 140、及び業務処理装置 150 にアクセスして、管理用端末 120 からの要求に基づく処理を実行し、処理結果を管理用端末 120 に送信する。

【0024】

50

ここでは、ファイル管理装置 130、ファイルアクセスログ管理装置 140、及び業務処理装置 150 を記録管理装置として説明するが、メールを格納するメールアーカイブ装置、ユーザのアプリケーションプログラムの操作ログを管理するアプリケーション操作ログ管理装置、ユーザの Web アクセスのログを管理する Web アクセルログ管理装置、印刷ログを管理する印刷ログ管理装置などを備えても良い。

【0025】

ファイル管理装置 130、ファイルアクセスログ管理装置 140、業務処理装置 150 などの記録管理装置は、いずれか 1 つ以上の装置があれば良く、各記録管理装置は 2 つ以上あっても良い。

【0026】

ファイル管理装置 130、ファイルアクセスログ管理装置 140、業務処理装置 150 などの記録管理装置、および、記録収集装置 160、関係データ管理装置 170、Web サーバ 180 のうち 2 つ以上の装置を組み合わせ、1 つの装置としても良い。図 1 では、説明を分かり易くするために各装置を独立したコンピュータで構成するようにしているが、コンピュータへの機能分担は適宜最適に設計される。小規模システムであれば、端末装置としてのクライアントコンピュータと所定の処理を実行するサーバコンピュータとで構成しても良い。

【0027】

図 2 を参照して、本実施形態に係る各装置を実現するコンピュータの構成例について説明する。図 2 に示すように、コンピュータ 201 は、CPU 202、主記憶装置 203、補助記憶装置 204、ネットワークインターフェース 205、I/O インターフェース 206 などが内部バス 207 によって相互に接続されて構成される。なお、本明細書では、主記憶装置 203 と補助記憶装置 204 とを総称する場合には、単に記憶装置という。図 3 を参照して、本実施形態に係る各記録管理装置で管理するファイル属性 132、ファイルアクセスログ 141、及び業務データ 151 の例について説明する。

【0028】

図 3 (a) はファイル属性 132 の例を示している。図 3 (a) に示す通り、ファイル属性 132 には、ファイル ID、ファイルハッシュ値、ファイル名、書類種別、登録者、登録日時、IP アドレス、及び案件番号がある。ファイル ID は、ファイル 131 の識別情報であり、ファイル管理装置 130 が割当てする。書類種別は、ファイル 131 の書類名であり、例えば、見積書、注文書、請求書、領収書などの種別を示す識別情報である。案件番号は、申請や注文などの案件を特定する識別情報であり、業務処理装置 150 が割当てする。ファイル属性 132 には、その他任意のデータを追加しても良い。業務ごとに又は書類種別ごとに、ファイル属性 132 に含むデータの種別を変更しても良い。

【0029】

図 3 (b) を参照して、ファイルアクセスログ 141 の例を示す。図 3 (b) に示す通り、ファイルアクセスログ 141 には、ファイル名、ユーザ名、アクセス日時、IP アドレス、MAC アドレス、アプリケーション名、及び操作がある。操作とは、ファイルに対する操作を示す情報であって、例えば、ファイルの新規作成、参照、削除、更新、ファイル名変更などの情報である。

【0030】

図 3 (c) を参照して、業務データ 151 の例を示す。図 3 (c) に示す通り、業務データ 151 には、案件番号、取引先名、取引日、品名、数量、金額、及び担当者名がある。案件番号は、申請や注文などの案件を特定する識別情報であり、業務処理装置 150 が割当てする。図 3 (c) は、業務データ 151 の一例であり、業務により、業務データ 151 に含まれるデータは異なる。

【0031】

各記録管理装置で管理するデータは、ファイル他データなどの記録を一意に特定可能なデータを含んでいれば、管理するデータに含まれるデータやデータ名が異なっても良い。記録を一意に特定するデータとしては、例えば、ファイル ID や案件番号などの識別

10

20

30

40

50

情報や、ファイル名とユーザ名とアクセス日時のようなデータを組み合わせた情報でも良い。

【0032】

図4を参照して、本実施形態に係る記録収集装置160における記録収集処理161について説明する。記録収集処理161は、管理者による操作、定期的なバッチ処理などにより実行が開始される。

【0033】

図4において、記録収集装置160は、収集ポリシー(収集条件)163を読み込む(S401)。収集ポリシー163が複数ある場合には、未処理の収集ポリシーを1つ読み込む。収集ポリシー(収集条件)163の詳細については、後述する。

10

【0034】

記録収集装置160は、収集ポリシー163に含まれる装置ID(記録管理装置を特定する識別子)に対応する記録管理装置から、収集ポリシー163に含まれる検索条件に一致した、デフォルトとしての取得データ(図5を用いて後述する)、及び収集ポリシー163で取得データとして指定されたデータを取得する(S402)。装置IDに対応する記録管理装置にアクセスするための情報は、記録収集装置160が管理している。管理している情報としては、例えば、装置ID、URL(Uniform Resource Locator)、モジュール名を管理する。モジュール名は、装置IDで識別される記録管理装置からデータを取得するプログラム(データ収集のためのエージェントプログラム)の識別情報である。HTTP(HyperText Transfer Protocol)でデータを取得できる場合、POST/GETの種別、クエリのパターンを管理するようにしても良い。

20

【0035】

S402で取得するデフォルトとしての取得データは、「データ(処理記録)識別情報」、「ユーザ名」、「マシン識別情報」、「日時」、および「収集ポリシーに記載の取得データ」である。「データ識別情報」、「ユーザ名」、「マシン識別情報」及び「日時」は、記録管理装置により、その内容が異なる。実際には、図5に示す属性名の対応関係を参照して、データを取得する。

【0036】

図5において、ファイル管理装置130(装置ID:ID__FILE)から取得する「データ識別情報」、「ユーザ名」、「マシン識別情報」及び「日時」は、それぞれファイル属性132に含まれる「ファイルID」、「登録者」、「IPアドレス」及び「登録日時」に対応する。

30

【0037】

ファイルアクセスログ管理装置140(装置ID:ID__LOG)から取得する「データ識別情報」、「ユーザ名」、「マシン識別情報」及び「日時」は、ファイルアクセスログ141に含まれる「ファイル名+アクセス日時+操作」、「ユーザ名」、「IPアドレス」及び「アクセス日時」に対応する。「データ識別情報」のように「ファイル名+アクセス日時+操作」と複数のデータを組み合わせても良い。

【0038】

業務処理装置150(装置ID:ID__BUSINESS)から取得する「データ識別情報」、「ユーザ名」、「マシン識別情報」及び「日時」は、業務データ151に含まれる「案件番号」、「担当者名」、「(NULL)」及び「取引日」に対応する。ここで、「(NULL)」は、データを取得しないことを意味する。記録管理装置によって、データを管理していない場合があり、そのような場合には、「(NULL)」を指定する。

40

【0039】

なお、記録管理装置から取得したユーザ名を別名に変換する変換辞書を用意しても良い。同一人物であっても、システムによりユーザ名は異なる場合がある。ユーザ名の変換辞書を用い、変換することで、そのような問題を解決できる。具体的には、図5の対応表により、記録管理装置よりユーザ名を取得し、取得したユーザ名を変換辞書により別名に変換する。

50

【0040】

記録収集装置160は、関連ポリシIDの収集ポリシ163に含まれる装置IDに対応する記録管理装置から、収集ポリシ163に含まれる検索条件に一致した、デフォルトとしての取得データ、及び収集ポリシ163で取得データとして指定されたデータ(以下、単にデータと呼ぶことがある。)を取得する(S403)。

【0041】

関連ポリシIDが複数ある場合には、各関連ポリシIDに対応する収集ポリシ163に関してデータを取得する。また、関連ポリシIDに対応する収集ポリシ163に、さらに他の関連ポリシIDが含まれる場合には、含まれる他の関連ポリシに関連する収集ポリシ163に関してデータを取得する。前者の並列的に関連ポリシIDが複数ある場合も、後者の階層的に関連ポリシIDが複数ある場合も、それらの関連ポリシ163について上述の処理を繰り返す。

10

【0042】

記録収集装置160は、取得したデータ(収集ポリシ163に含まれる検索条件に一致した、デフォルトとしての取得データ、及び収集ポリシ163で取得データとして指定されたデータ)を、後述する記録関連データとして関係データ管理装置170に送信する(S404)。記録収集装置160が、データを取得した順序で関係データ管理装置170にデータを送信することが望ましい。具体的には、S402で取得したデータを送信した後で、S403で取得したデータを送信することが望ましい。記録収集装置160が関係データ管理装置170に送信する記録関連データの詳細については後述する。

20

【0043】

記録収集装置160は、未処理の収集ポリシ163があるかを判定する(S405)。未処理の収集ポリシ163がある場合には、S401に戻り、未処理の収集ポリシ163がない場合には、データ収集の処理を終了する。

【0044】

なお、関係データ管理装置170へのデータ送信処理(S404)を、S402の処理の後に追加しても良い。この場合、S402及びS403の処理の後に、それぞれS404の処理を実行する。

【0045】

別の実施形態として、S402とS403でデータの実体を取得するようにしても良い。例えば、ファイル管理装置130から収集する場合、ファイル131を取得するようにしても良い。さらに、記録収集装置160は、取得した実体データに対して、電子署名、タイムスタンプ、ハッシュ値などの改ざん検知情報を作成し、改ざん検知情報を関係データ管理装置170に送信しても良い。記録管理装置に改ざん検知機能がない場合には、記録管理装置に変更を加えることなく、実体データの改ざん検知機能を実現できる。

30

【0046】

さらに別の実施形態として、S403で、条件に一致するデータを取得できない場合、一致するデータ数が指定された数より少ない場合などにアラートを出すようにしても良い。例えば、受注業務であれば、業務処理装置151に受注データが登録されている場合、基本的には注文書が存在するはずである。受注データに関連するデータとして、注文書を検索して見つからなければアラートを出す、というようにである。この場合、アラートを出す条件は、記録収集装置160が管理する。

40

【0047】

さらに別の実施形態として、S403で、条件に一致するデータを取得した後、検索条件としなかった他のデータとの対比により、不整合がある場合などにアラートを出すようにしても良い。例えば、ファイル管理装置130への注文書の登録者と、業務処理装置151への受注データの登録者は同一である必要がある場合に、ファイル属性132の登録者と業務データ151の担当者名を比較し、一致しなければアラートを出す。

【0048】

図6を参照して、本実施形態に係る収集ポリシ(収集条件)163の例について説明する

50

。図 6 に示す通り、収集ポリシー 163 には、ポリシー ID、装置 ID、取得データ、検索条件、関連ポリシー ID、及び送信先がある。以下、種々の識別子を単に ID と呼ぶことがある。

【0049】

ポリシー ID は、収集ポリシー 163 を特定する識別情報である。装置 ID は、記録管理装置を特定する識別情報である。

【0050】

取得データは、図 5 で指定された以外に取得するデータである。取得データに「NULL」を指定した場合には、図 5 で指定したデータのみを取得する。取得データで指定したデータは、関連するデータを検索する際の条件指定として利用できる。

10

【0051】

検索条件は、記録収集装置 160 が記録管理装置から収集するデータを検索するための条件である。記録収集装置 160 は、図 5 で指定したデータに加えて、この検索条件に一致し、取得データとして指定されたデータを取得する。

【0052】

関連ポリシー ID は、関連する別のポリシー ID がある場合に、その別のポリシー ID を示す。関連ポリシー ID を参照して、ある収集ポリシー 163 で検索した記録と関連のある記録を検索する。関連する記録がない場合には、関連ポリシー ID に「NULL」を指定する。

【0053】

送信先は、収集したデータの送信先である関係データ管理装置 170 のアドレス（例、IP アドレス、URL）である。「NULL」を指定した場合には、参照元（当該ポリシー ID を関連ポリシー ID として指定したポリシー ID）の収集ポリシー 163 の値を継承する。送信先の指定により、収集したデータを用途に応じて振り分けることができる。例えば、情報漏洩対策としてファイルのフローを追跡する用途、内部統制の監査対応として取引のフローを追跡する用途などによって振り分けることができる。

20

【0054】

別の実施形態として、収集ポリシー 163 に「用途」を追加しても良い。「用途」には、収集するデータの用途、例えば、情報漏洩対策、内部統制の監査対応などを識別する情報を格納する。さらに、「用途」に関する情報を関係データ管理装置 170 に送信し、関係データ管理装置 170 がメタデータ 173 や記録属性データ 175 で「用途」に関する情報を管理する。これにより、同一の関係データ管理装置 170 で異なる用途で収集されたデータを管理できる。

30

【0055】

図 6（a）（b）（c）を参照して、収集ポリシー（収集条件）163 の具体例を説明する。図 6 では、注文書（ファイル 131）に関連する業務データ 151 とファイルアクセスログ 141 とを関連付ける収集ポリシー 163 の例を示している。記録収集装置 160 は、収集ポリシー 163（a）に基づいて、注文書を検索し、この注文書に関連する業務データ 151 及びファイルアクセスログ 141 を、収集ポリシー 163（b）及び 163（c）の各々に基づいて検索する。

【0056】

収集ポリシー 163（a）に基づいて、記録収集装置 160 は、ファイル管理装置 130 から、書類種別が注文書、かつ、登録日時が、記録収集装置 160 がファイル管理装置 130 からデータを収集した前回の日時以降のファイル属性 132 の取得データで指定される案件番号を取得する。この処理が、図 4 の S402 において、デフォルトとしての取得データの取得に加わる処理である。

40

【0057】

取得した個々のデータ（案件番号）について、記録収集装置 160 は、収集ポリシー 163（a）の関連ポリシー ID が P__002 と P__003 の収集ポリシー 163（b）及び 163（c）に一致するデータを収集する。例えば、収集ポリシー 163（a）に一致するデータが 10 件あった場合には、10 件のデータの 1 件 1 件をチェックして、記録収集装置 16

50

0 は、P__002 と P__003 の収集ポリシ 163 (b) 及び 163 (c) に一致するデータを収集する。この処理が、図 4 の S403 において、デフォルトとしての取得データの取得に加わる処理である。

【0058】

収集ポリシ 163 (b) に基づいて、記録収集装置 160 は業務処理装置 150 から、収集ポリシ 163 (a) で取得したファイル属性 132 の案件番号が、業務処理装置 150 の業務データ 151 の案件番号と等しいデータ (デフォルトとしての取得データ及び収集ポリシ 163 (b) で取得データとして指定されたデータ) を取得する。

【0059】

収集ポリシ 163 (c) に基づいて、記録収集装置 160 はファイルアクセスログ管理装置 140 から、収集ポリシ 163 (a) で取得したファイル属性 132 の IP アドレスとファイルアクセスログ管理装置 140 のファイルアクセスログ 141 の IP アドレスが等しく、かつ、ファイル属性 132 のファイル名とファイルアクセスログ 141 のファイル名が等しく、かつ、ファイルアクセスログ 141 のアクセス日時がファイル属性 132 の登録日時以降のデータ (デフォルトとしての取得データ及び収集ポリシ 163 (c) で取得データとして指定されたデータ) を取得する。

【0060】

図 6 の例では、収集ポリシ 163 (a) が収集ポリシ 163 (b) と収集ポリシ 163 (c) を参照している。このとき、他の収集ポリシを参照している側 (収集ポリシ 163 (a)) を親の収集ポリシ、他の収集ポリシから参照されている側 (収集ポリシ 163 (b)、163 (c)) を子の収集ポリシと呼ぶこととする。また、親の収集ポリシに基づき収集したデータ (デフォルトとしての取得データ及び収集ポリシ 163 (a) で取得データとして指定されたデータ) を親データ、子の収集ポリシに基づき収集したデータを子データと呼ぶこととする。

【0061】

図 6 の例では、条件に一致する全てのデータを取得する指定になっているが、条件に一致する最新の 1 件のみ取得というように、取得する件数を指定してもよい。ファイルアクセスログ 141 などのログは、膨大な量になるため、関連する最新の 1 件のみと関連付けることが望ましい。

【0062】

続いて、図 7 を参照して、本実施形態に係る記録収集装置 160 が関係データ管理装置 170 に送信する記録関係データ 700 の例について説明する。図 7 に示す通り、記録関係データ 700 には、装置 ID、データ識別情報、ユーザ名、マシン識別情報、日時、記録種別、関連装置 ID、及び関連データ識別情報がある。

【0063】

装置 ID、データ識別情報、ユーザ名、マシン識別情報、及び日時は、図 5 に示す対応関係に基づき、記録収集装置 160 が各記録管理装置から取得したデータである。

【0064】

記録種別は、記録の種類に関する識別情報である。記録種別としては、例えば、ファイル、ファイルアクセスログ、Web 操作ログ、業務データ、メールなどがある。別の実施形態として、記録種別に記録のフォーマットを指定しても良い。

【0065】

関連装置 ID と関連データ識別情報とは、親の収集ポリシ 163 で収集したデータの装置 ID とデータ識別情報である。関連装置 ID と関連データ識別情報により、記録間の関係を表す。すなわち、子データに対する記録関係データ 700 の関連装置 ID と関連データ識別情報には、親データの関連装置 ID と関連データ識別情報が指定される。

【0066】

別の実施形態として、任意の属性データを追加して送信しても良い。任意の属性データを追加する場合には、属性を識別する情報 (属性名、型情報など) と属性値とのペアを送信する。例えば、属性を識別する情報として「書類名」、属性値として「注文書」を指定

10

20

30

40

50

することができる。

【0067】

さらに別の実施形態として、ファイル131などの実体データに対する、電子署名、タイムスタンプ、ハッシュ値などの改ざん検知情報を、記録関係データ700に含めても良い。

【0068】

さらに別の実施形態として、クライアント端末110が記録関係データ700を作成し、関係データ管理装置170に送信しても良い。この場合、クライアント端末110は、記録関係データ700を作成し、関係データ管理装置170に記録関係データ700を送信する。例えば、クライアント端末110からファイル管理装置130、ファイルアクセスログ管理装置140、業務処理装置150などの記録管理装置にデータを登録するプログラムと連携、または、そのプログラムへの入力を監視することで、必要なデータを収集し、記録関係データ700を生成する。記録関係データ700の作成に必要な情報を記録管理装置にアクセスして取得しても良い。なお、関連装置ID、関連データ識別情報は、収集ポリシ163をクライアント端末110の記憶装置に読み込み、収集ポリシ163に基づき、記録間を関連付けする。

【0069】

図8を参照して、本実施形態に係る関係データ管理装置170における関係データ登録処理171について説明する。

【0070】

図8において、関係データ管理装置170は、クライアント端末110または記録収集装置160が送信した記録関係データ700を受信する(S801)。記録関係データ700は、1つ1つ受信してもよいし、複数の記録関係データ700をまとめて受信してもよい。複数の記録関係データ700を受信した場合、以降の処理は、記録関係データ700の1つ1つに対して実行される。また、複数の記録関係データ700を受信した場合、関連装置IDおよび関連データ識別情報が記載されていないデータから順番に以降の処理することが望ましい。最良の形態は、記録関係データ700を送信する側で、データを取得した順序に並べ変えて送信することが望ましい。すなわち、図4のS403で取得したデータよりも、S402で取得したデータをS404で先に送信することが望ましい。

【0071】

関係データ管理装置170は、受信した記録関係データ700と同一データが既に登録されていないかを確認する(S802)。同一データであるかどうかは、装置IDとデータ識別情報とが共に一致しているかどうかで判定する。同一データが存在する場合は、次の記録関係データを処理する(図示略)。

【0072】

関係データ管理装置170は、記録関係データ700に関連装置IDと関連データ識別情報が含まれるかを確認する(S803)。含まれる場合には、S804へ進み、含まれない場合には、S805へ進む。含まれる場合とは、親子の2階層の記録関係データ700がある場合、親の記録関係データ700の場合であり、含まれない場合とは子の記録関係データ700の場合である。

【0073】

関係データ管理装置170は、関連装置IDと関連データ識別情報で特定されるメタデータ173(詳細は後述)から記録IDを取得する(S804)。すなわち、処理の対象が子の記録関係データ700であるので、その親の記録関係データ700に対応するメタデータ173から記録IDを取得する。記録IDを取得できない場合(図示略)は、親の記録関係データ700の処理が実行されていないので、処理を中断して先に未処理の記録関係データ700を処理するか、所定の時間を待って、S801から再実行するなどにより、記録関係データ700の処理順序を整える。

【0074】

関係データ管理装置170は、処理対象の記録関係データ700に対して、記録IDを

10

20

30

40

50

割り当てる（S805）。記録IDは、関係データ管理装置170で一意であれば良い。例えば、登録された順序に割り当てる連続番号、記録関係データ700のハッシュ値でも良い。

【0075】

関係データ管理装置170は、S802とS804で取得した記録IDと記録関係データ700とをメタデータ173および関係データ174に登録する（S806）。具体的には、記録IDと記録関係データ700とに基づいて、新たなメタデータ173および関係データ174のレコードを生成して、追加格納する。

【0076】

関係データ管理装置170は、未処理の記録関係データ700があるかを確認する（S807）。未処理の記録関係データ700がある場合にはS802へ進み、ない場合には関係データ登録処理171の処理を終了する。

【0077】

図9を参照して、本実施形態に係る関係データ管理装置170が管理するメタデータ173、関係データ174、及び記録属性データ175の例について説明する。

【0078】

図9（a）はメタデータ173の例を示している。メタデータ173には、記録ID、装置ID、データ識別情報、ユーザ名、マシン識別情報、日時、及び記録種別がある。記録IDは、メタデータ173を一意に特定する識別情報であり、関係データ管理装置170が割り当てる。記録ID以外のデータは、記録関係データ700の該当するデータと同じである。別の実施形態として、ファイル131などの実体データに対する、電子署名、タイムスタンプ、ハッシュ値などの改ざん検知情報を、メタデータ173に含めても良い。

【0079】

図9（b）を参照して、関係データ174の例を説明する。関係データ174には、記録ID（parent）及び記録ID（child）がある。記録ID（parent）は、記録関係データ700の関連装置IDと関連データ識別情報で特定されるメタデータ173の記録IDであり、記録ID（child）は、記録関係データ700の装置IDとデータ識別情報で特定されるメタデータの記録IDである。関係データ174では、記録間の親子関係（階層構造）を管理している。

【0080】

図9（c）を参照して、記録属性データ175の例を説明する。記録属性データ175は、記録関係データ700に属性データを含める場合に利用する。記録属性データ175には、記録ID、属性識別ID、及び属性値がある。属性識別IDは、属性の識別情報であり、例えば、属性名や型情報である。

【0081】

図8におけるS806では、記録関係データ700をメタデータ173にマッピングし、S805で割り当てた記録IDをメタデータ173の記録IDに指定する。関係データ174は、記録関係データ700に関連装置IDと関連データ識別情報が含まれる場合に生成される。記録関係データ700に関連装置IDと関連データ識別情報が含まれる場合、すなわち子の記録関係データ700がある場合であり、記録ID（child）には、S804で取得した記録IDを指定し、記録ID（parent）には、S805で発行した記録IDを指定する。

【0082】

図10を参照して、本実施形態に係る検索要求データ1000の例について説明する。検索要求データ1000は、管理用端末120またはWebサーバ180が、ある記録に関連するデータを検索する際に、関係データ管理装置170に送信するデータである。

【0083】

図10に示す通り、検索要求データ1000には、装置ID、データ識別情報、検索フィールド、検索階層、及び検索条件がある。

10

20

30

40

50

【0084】

検索フィールドは、関連するデータを検索する際の検索フィールド名を識別する情報である。関連するデータを検索する際には、関係データ174を参照する。検索フィールドには、関係データ174の記録ID (parent) 及び記録ID (child) の少なくとも一方を指定する。例えば、検索フィールドに「記録ID (parent)」を指定した場合、親方向に関連するデータを検索する。具体的には、記録ID (child) で関係データ174を検索し、検索結果の記録ID (parent) を取得する。次に、取得した記録ID (parent) を記録ID (child) として、関係データ174を検索する。子を検索キーとして親を検索し、さらにその親の親を検索する。

【0085】

検索階層は、検索する階層数である。関係データ管理装置170では、関係データ174により、記録間の関係を階層構造で管理している。例えば、検索フィールドに「記録ID (parent)、検索階層に「2」を指定した場合には、親方向に関連するデータを2つ辿ることになる。なお、検索階層に「0」を指定した場合には、階層構造の始点、または、終点まで階層構造を辿る。

【0086】

検索条件は、検索結果をフィルタリングする条件である。メタデータ173及び記録属性データ175に関する条件を指定する。例えば、「ユーザ名=user A」と指定した場合には、メタデータ173のユーザ名が「user A」であるデータを、検索要求データ1000の送信元に返す。条件は、複数指定しても良く、検索結果として返す数を指定しても良い。

【0087】

図11を参照して、本実施形態に係る関係データ管理装置170における関係データ検索処理172について説明する。

【0088】

関係データ検索処理172は、管理用端末120又はWebサーバ180が送信した検索要求データ1000に基づき、メタデータ173と関係データ174とから要求されたデータを抽出する。

【0089】

図11において、関係データ管理装置170は、検索要求データ1000を受信し (S1101)、検索要求データ1000に含まれる装置IDとデータ識別情報で特定されるメタデータ173の記録IDを取得する (S1102)。

【0090】

関係データ管理装置170は、「N=検索要求データ1000の検索階層」及び「i=0」を設定する (S1103)。

【0091】

関係データ管理装置170は、検索要求データ1000の検索フィールドの設定に基づき、関係データ174から記録ID (parent / child) を抽出する (S1104)。検索フィールドに記録ID (parent) が指定されている場合には、関係データ管理装置170は、S1104で取得した記録IDと記録ID (child) が等しい記録ID (parent) を関係データ174から抽出する。また、検索フィールドに記録ID (child) が指定されている場合には、関係データ管理装置170は、S1104で取得した記録IDと記録ID (parent) が等しい記録ID (child) を関係データ174から抽出する。

【0092】

関係データ管理装置170は、S1104で抽出した記録IDに一致するメタデータ173と記録属性データ175とを取得し (S1105)、取得したメタデータ173と記録属性データ175とが検索要求データ1000の検索条件に一致するか確認する (S1106)。例えば、検索条件に「ユーザ名=user A」と指定されている場合には、メタデータ173のユーザ名が「user A」であるかを確認する。検索条件に一致する場

10

20

30

40

50

合には、S 1 1 0 7 へ進み、そうでない場合には、S 1 1 0 8 へ進む。

【0093】

関係データ管理装置170は、S 1 1 0 5で取得したメタデータ173に含まれる装置ID及びデータ識別情報を検索結果に追加する(S 1 1 0 7)。なお、S 1 1 0 4で複数の記録IDが抽出された場合には、それぞれの記録IDに対して、S 1 1 0 5からS 1 1 0 7の処理を実行する。

【0094】

関係データ管理装置170は、「 $i = i + 1$ 」の処理を実行しする(S 1 1 0 8)、パラメータ*i*がNと等しいかを確認する(S 1 1 0 9)。等しい場合には、S 1 1 0 4へ進む、等しくない場合には、S 1 1 1 0へ進む。

10

【0095】

関係データ管理装置170は、検索結果を検索要求元に返し(S 1 1 1 0)、処理を終了する。

【0096】

図12を参照して、本実施形態に係るデータの検索処理について説明する。管理用端末120またはWebサーバ180は、検索要求データ1000を生成し、関係データ管理装置170に送信し、検索結果を受信する(S 1 2 0 1)。関係データ管理装置170は、関係データ検索処理172により、検索結果を作成する。検索結果には、装置IDとデータ識別情報とが含まれる。

【0097】

管理用端末120またはWebサーバ180は、記録収集装置160に検索結果を送信し、実体データまたは実体データへのリファレンスを受信する(S 1 2 0 2)。記録収集装置160は、実体取得処理162を実行することにより、検索結果(装置IDとデータ識別情報の集合)を解析し、実体データを記録管理装置から取得、または、実体データへのリファレンスを作成する。実体データとは、例えば、ファイル131、ファイルアクセスログ141、又は業務データ151である。実体データへのリファレンスとは、例えば、実体データにアクセスするためのURLである。

20

【0098】

管理用端末120またはWebサーバ180は、実体データを表示、または、実体データへのリファレンスを用いてアクセスし、アクセスした実体データを表示する(S 1 2 0 3)。

30

【0099】

以上のようにして、種類の異なる複数の記録管理装置に格納されている記録同士を、既存の記録管理装置に変更を加えることなく、関連付けることができ、関連するデータの検索を効率化できる。

【図面の簡単な説明】

【0100】

【図1】実施形態に係るシステム構成の例を示した図である。

【図2】各装置を実現するコンピュータの構成例を示した図である。

【図3】各記録管理装置で管理するファイル属性、ファイルアクセスログ、及び業務データの例を示した図である。

40

【図4】記録収集装置における記録収集処理を示した図である。

【図5】各記録管理装置から取得する情報の対応関係の例を示した図である。

【図6】収集ポリシーの例を示した図である。

【図7】記録収集装置が関係データ管理装置に送信する記録関係データの例を示した図である。

【図8】関係データ管理装置における関係データ登録処理を示した図である。

【図9】関係データ管理装置が管理するメタデータ、関係データ、及び記録属性データの例を示した図である。

【図10】検索要求データの例を示した図である。

50

【図 1 1】 関係データ管理装置における関係データ検索処理を示した図である。

【図 1 2】 データの検索処理を示した図である。

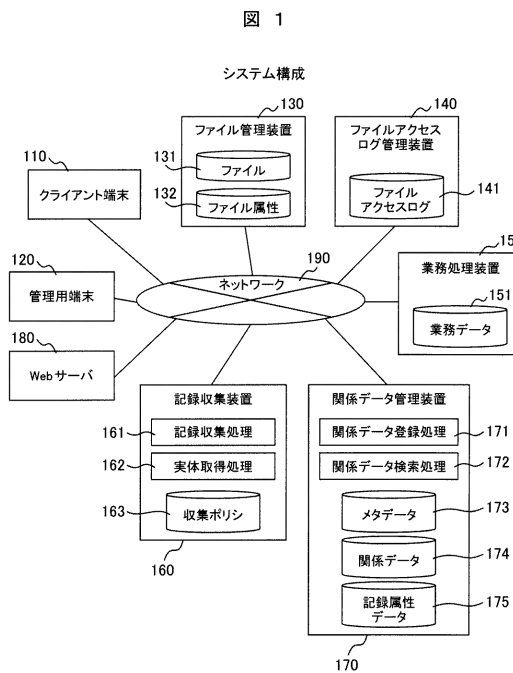
【符号の説明】

【0101】

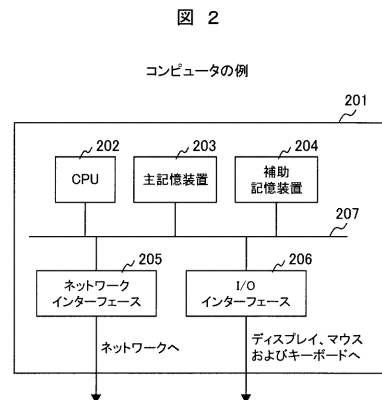
110：クライアント端末、120：管理用端末、130：ファイル管理装置、131：ファイル、132：ファイル属性、140：ファイルアクセスログ管理装置、141：ファイルアクセスログ、150：業務処理装置、151：業務データ、160：記録収集装置、161：記録収集処理、162：実体取得処理、163：収集ポリシー、170：関係データ管理装置、171：関係データ登録処理、172：関係データ検索処理、173：メタデータ、174：関係データ、175：記録属性データ、180：Webサーバ、190：ネットワーク、700：記録関係データ、1000：検索要求データ。

10

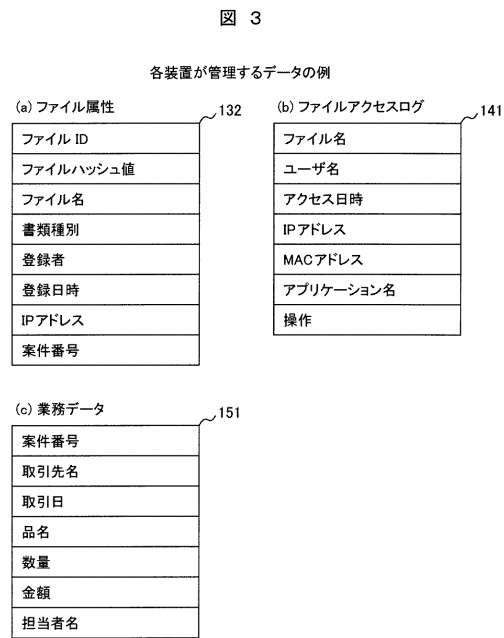
【図 1】



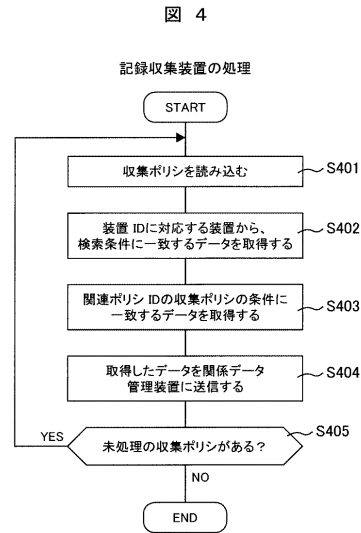
【図 2】



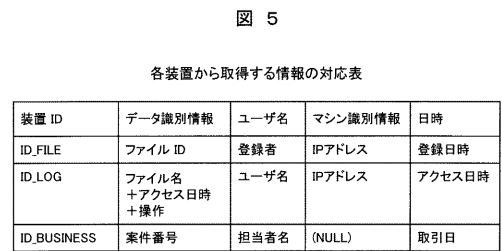
【図 3】



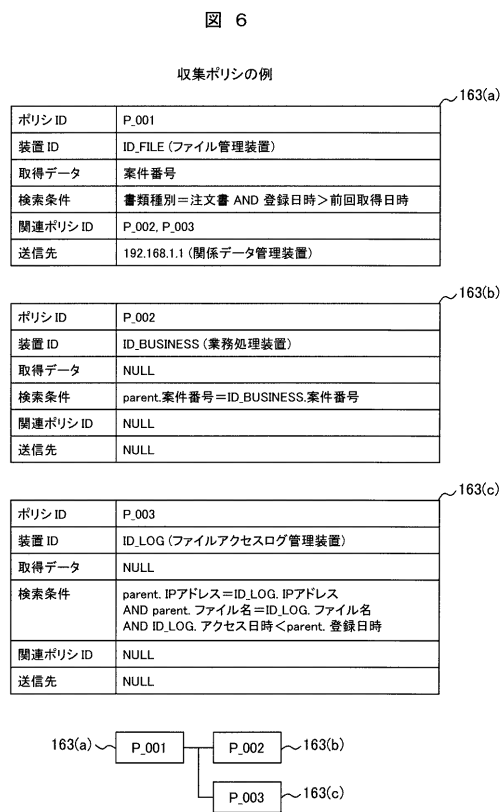
【図 4】



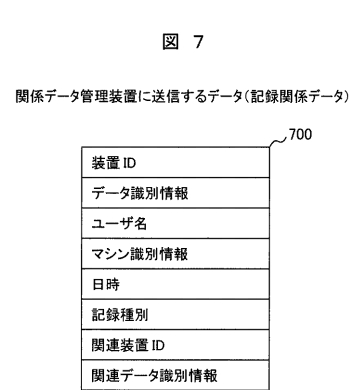
【図 5】



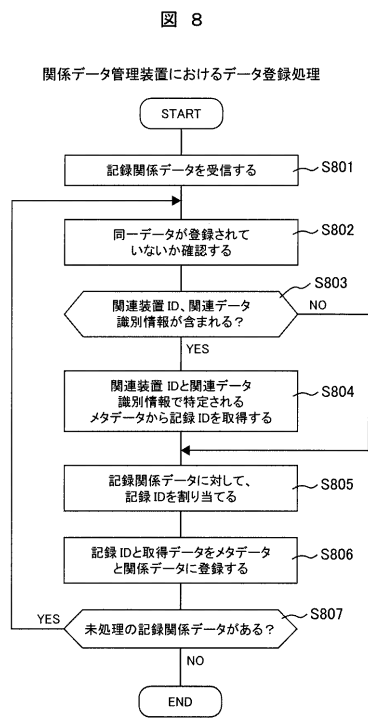
【図 6】



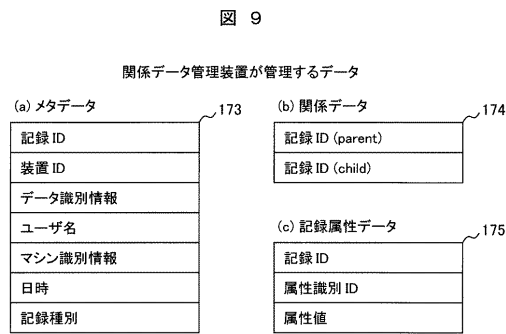
【図 7】



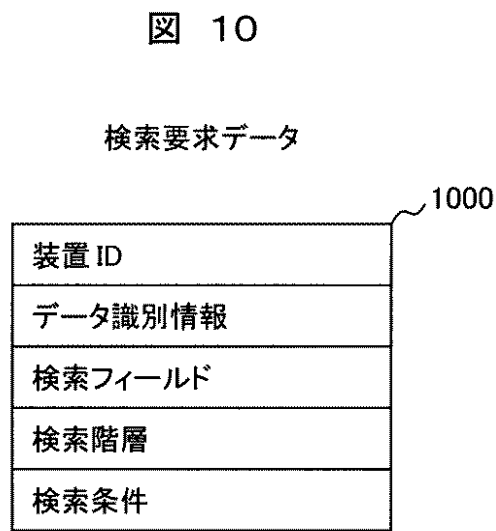
【図 8】



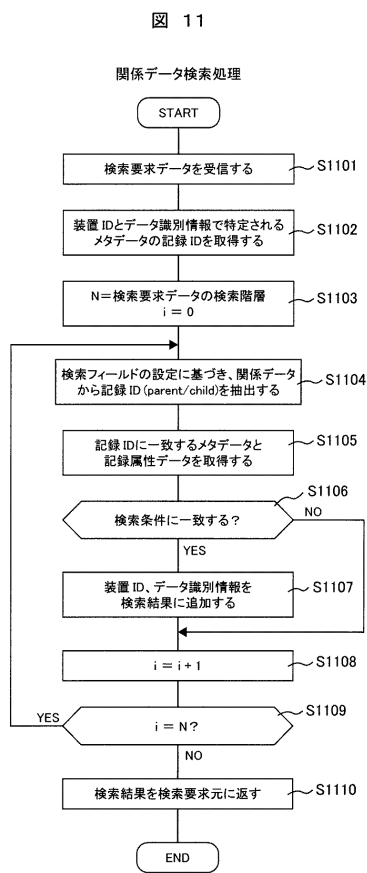
【図 9】



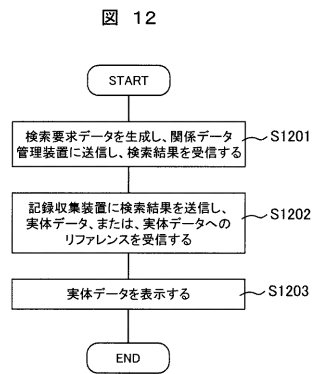
【図 10】



【図 11】



【図 12】



フロントページの続き

(72)発明者 富山 朋哉

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) 5B082 EA07