

(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2008-9850

(P2008-9850A)

(43) 公開日 平成20年1月17日(2008.1.17)

(51) Int. Cl.

G06F 11/34 (2006.01)

F I

G06F 11/34

C

テーマコード (参考)

5B042

審査請求 未請求 請求項の数 20 O L (全 86 頁)

(21) 出願番号 特願2006-181415 (P2006-181415)

(22) 出願日 平成18年6月30日 (2006.6.30)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目7番3号

(74) 代理人 100099461

弁理士 溝井 章司

(72) 発明者 鶴川 達也

東京都千代田区丸の内二丁目7番3号 三

菱電機株式会社内

Fターム(参考) 5B042 MA08 MA10 MA11 MA14 MC35

MC37 MC39 MC40

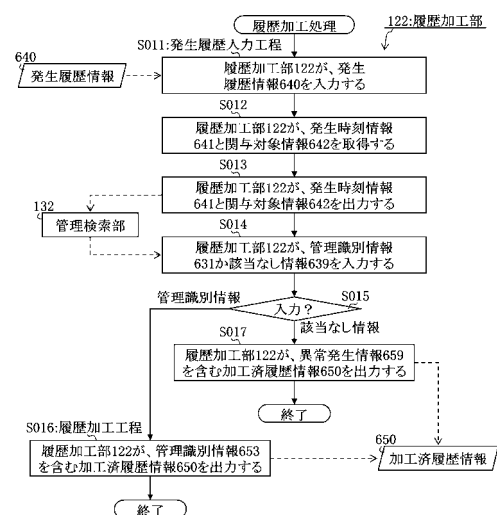
(54) 【発明の名称】 履歴管理装置及び履歴管理方法及び履歴管理プログラム

(57) 【要約】

【課題】形式などが異なる膨大な量のログのなかから、目的とするログを迅速・容易に発見することができるように、ログを管理する。

【解決手段】履歴加工部122は、発生履歴情報640（ログ）を入力し、発生履歴情報640に含まれる発生時刻情報641と関与対象情報642とに基づいて、関与対象情報642が示す対象を一意に識別する管理識別情報653を取得する。履歴加工部122は、取得した管理識別情報653を発生履歴情報640に付加して、加工済履歴情報650を生成し、出力する。

【選択図】図7



【特許請求の範囲】

【請求項 1】

情報を処理する処理装置と、
情報を記憶する記憶装置と、

上記処理装置を用いて、対象を識別する情報である管理識別情報と、期間を示す情報である期間情報と、上記期間情報によって示される期間において上記対象を示す情報である対象識別情報とを含む情報である管理情報を上記記憶装置に記憶する管理記憶部と、

上記処理装置を用いて、時刻を示す情報である時刻情報と、対象を示す情報である対象情報とを入力し、上記処理装置を用いて、上記管理記憶部が記憶した管理情報のなかから、入力した上記対象情報と、上記管理情報に含まれる対象識別情報とが一致し、かつ、入力した上記時刻情報によって示される時刻が上記管理情報に含まれる期間情報によって示される期間内である管理情報を抽出し、上記処理装置を用いて、抽出した上記管理情報に含まれる管理識別情報を出力する管理検索部と、

上記処理装置を用いて、事象が発生した時刻である発生時刻を示す情報である発生時刻情報と、上記事象の発生に関与した対象である関与対象を示す情報である関与対象情報とを含む情報である発生履歴情報を入力し、上記処理装置を用いて、入力した上記発生履歴情報に含まれる発生時刻情報によって示される発生時刻を示す情報を、上記管理検索部が入力する時刻情報として出力し、入力した上記発生履歴情報に含まれる関与対象情報を上記管理検索部が入力する対象情報として出力し、上記処理装置を用いて、上記管理検索部が出力した管理識別情報を入力し、上記処理装置を用いて、入力した上記発生履歴情報に含まれる情報と、入力した上記管理識別情報とを含む情報である加工済履歴情報を出力する履歴加工部と、
を有することを特徴とする履歴管理装置。

【請求項 2】

上記管理検索部は、

上記処理装置を用いて、開始時刻を示す情報である開始時刻情報と、終了時刻を示す情報である終了時刻情報とを、上記時刻情報として入力し、

上記処理装置を用いて、上記管理記憶部が記憶した管理情報のなかから、入力した上記対象情報と、上記管理情報に含まれる対象識別情報とが一致し、かつ、入力した上記開始時刻情報によって示される開始時刻から入力した上記終了時刻情報によって示される終了時刻までの期間と、上記管理情報に含まれる期間情報によって示される期間との間に重複する期間がある管理情報を抽出し、

上記処理装置を用いて、抽出した上記管理情報に含まれる管理識別情報と、抽出した上記管理情報に含まれる期間情報とを含む情報である期間付管理識別情報を出力し、

上記履歴加工部は、

上記処理装置を用いて、上記発生履歴情報を複数入力し、

上記処理装置を用いて、入力した上記発生履歴情報に含まれる関与対象情報が互いに一致する発生履歴情報が複数あるか否かを判断し、

上記処理装置を用いて、上記関与対象情報が互いに一致する発生履歴情報が複数あると判断した場合に、上記関与対象情報が互いに一致すると判断した複数の発生履歴情報に含まれる発生時刻情報によって示される発生時刻のうち、最も早い発生時刻を示す情報を、上記管理検索部が入力する開始時刻情報として出力し、上記関与対象情報が互いに一致すると判断した複数の発生履歴情報に含まれる発生時刻情報によって示される発生時刻のうち、最も遅い発生時刻を示す情報を上記管理検索部が入力する終了時刻情報として出力し、

上記処理装置を用いて、上記管理検索部が出力した期間付管理識別情報を入力し、

上記処理装置を用いて、入力した上記発生履歴情報に含まれる情報と、入力した上記期間付管理識別情報のうち、上記発生履歴情報に含まれる発生時刻情報によって示される発生時刻が上記期間付管理識別情報に含まれる期間情報によって示される期間内である期間付管理識別情報に含まれる管理識別情報とを含む加工済履歴情報を出力する

10

20

30

40

50

ことを特徴とする請求項 1 に記載の履歴管理装置。

【請求項 3】

上記履歴管理装置は、更に、

上記処理装置を用いて、上記履歴加工部が出力した加工済履歴情報を入力し、上記処理装置を用いて、入力した加工済履歴情報を上記記憶装置に記憶する履歴蓄積部と、

上記処理装置を用いて、上記加工済履歴情報に含まれる情報についての検索条件を示す情報である履歴検索条件情報を入力し、上記処理装置を用いて、上記履歴蓄積部が記憶した加工済履歴情報のなかから、入力した上記履歴検索条件情報によって示される検索条件に合致する加工済履歴情報を抽出し、上記処理装置を用いて、抽出した上記加工済履歴情報に含まれる情報を出力する履歴検索部と、

を有することを特徴とする請求項 1 に記載の履歴管理装置。

【請求項 4】

上記履歴蓄積部は、

上記記憶装置を用いて、上記履歴加工部が入力した上記発生履歴情報に含まれる情報と、上記管理識別情報とのみを含む加工済履歴情報を記憶し、上記管理識別情報によって識別される対象の属性を示す情報を記憶しない

ことを特徴とする請求項 3 に記載の履歴管理装置。

【請求項 5】

上記履歴管理装置は、更に、

情報を入力する入力装置と、

情報を出力する出力装置と、

上記処理装置を用いて、上記管理識別情報と、上記管理識別情報によって識別される対象の属性を示す情報である属性情報とを含む情報である管理属性情報を上記記憶装置に記憶する属性記憶部と、

上記処理装置を用いて、上記管理識別情報を入力し、上記処理装置を用いて、上記属性記憶部が記憶した管理属性情報のなかから、入力した上記管理識別情報と、上記管理属性情報に含まれる管理識別情報とが一致する管理属性情報を抽出し、上記処理装置を用いて、抽出した上記管理属性情報に含まれる情報を出力する属性検索部と、

上記処理装置を用いて、検索条件を示す情報である検索条件情報を、上記入力装置から入力し、上記処理装置を用いて、入力した上記検索条件情報によって示される検索条件を示す情報を、上記履歴検索部が入力する履歴検索条件情報として出力し、上記処理装置を用いて、上記履歴検索部が出力した加工済履歴情報に含まれる情報を入力し、上記処理装置を用いて、入力した上記加工済履歴情報に含まれる管理識別情報を、上記属性検索部が入力する管理識別情報として出力し、上記処理装置を用いて、上記属性検索部が出力した管理属性情報に含まれる情報を入力し、上記処理装置を用いて、入力した上記加工済履歴情報に含まれる情報と、入力した上記管理属性情報に含まれる情報とを上記出力装置に出力する履歴照会部と、

を有することを特徴とする請求項 3 に記載の履歴管理装置。

【請求項 6】

上記属性記憶部は、

上記処理装置を用いて、上記管理識別情報によって識別される対象が上記属性情報によって示される属性を有する期間を示す情報である属性期間情報を更に含む管理属性情報を上記記憶装置に記憶し、

上記属性検索部は、

上記処理装置を用いて、時刻を示す情報である時刻情報と、上記管理識別情報とを入力し、

上記処理装置を用いて、上記属性記憶部が記憶した管理属性情報のなかから、入力した上記管理識別情報と、上記管理属性情報に含まれる管理識別情報とが一致し、かつ、入力した上記時刻情報によって示される時刻が、上記管理属性情報に含まれる属性期間情報によって示される期間内である管理属性情報を抽出し、

10

20

30

40

50

上記処理装置を用いて、抽出した上記管理属性情報に含まれる情報を出力し、
上記履歴照会部は、

上記処理装置を用いて、入力した上記加工済履歴情報に含まれる発生時刻情報によって示される発生時刻を示す情報を、上記属性検索部が入力する時刻情報として出力することを特徴とする請求項 5 に記載の履歴管理装置。

【請求項 7】

上記履歴照会部は、更に、

上記処理装置を用いて、現在時刻を示す情報を、上記属性検索部が入力する時刻情報として出力することを特徴とする請求項 6 に記載の履歴管理装置。

10

【請求項 8】

上記管理検索部は、更に、

上記処理装置を用いて、上記管理記憶部が記憶した管理情報のなかから、抽出できる管理情報が存在しない場合に、該当する管理情報がないことを示す情報である該当なし情報を出力し、

上記履歴加工部は、

上記処理装置を用いて、上記管理検索部が該当なし情報を出力した場合に、異常発生を示す情報である異常発生情報を更に含む加工済履歴情報を出力することを特徴とする請求項 1 に記載の履歴管理装置。

【請求項 9】

20

上記管理記憶部は、

上記処理装置を用いて、利用者を識別する情報である利用者識別情報を、上記管理識別情報として含む管理情報を上記記憶装置に記憶し、

上記履歴加工部は、

上記処理装置を用いて、機器を操作した時刻である操作時刻を示す情報である操作時刻情報と、上記機器を操作した利用者を示す情報である操作者情報とを含む情報である操作履歴情報を、上記発生履歴情報として入力し、

上記処理装置を用いて、入力した上記操作履歴情報に含まれる操作時刻情報によって示される操作時刻を示す情報を、上記管理検索部が入力する時刻情報として出力し、入力した上記操作履歴情報に含まれる操作者情報を上記管理検索部が入力する対象情報として出力し、

30

上記処理装置を用いて、上記管理検索部が出力した利用者識別情報を入力し、

上記処理装置を用いて、入力した上記操作履歴情報に含まれる情報と、入力した上記利用者識別情報とを含む加工済履歴情報を出力することを特徴とする請求項 1 に記載の履歴管理装置。

【請求項 10】

上記管理記憶部は、

上記処理装置を用いて、従業員を識別する従業員コードを、上記管理識別情報として含む管理情報を、上記記憶装置に記憶し、

上記管理検索部は、

40

上記処理装置を用いて、抽出した上記管理情報に含まれる従業員コードによって識別される従業員が上記機器の操作を許可された従業員であるか否かを判断し、

上記処理装置を用いて、上記従業員コードによって識別される従業員が上記機器の操作を許可された従業員でないと判断した場合に、異常発生を示す情報である異常発生情報を出力する

ことを特徴とする請求項 9 に記載の履歴管理装置。

【請求項 11】

上記管理記憶部は、

上記処理装置を用いて、機器を識別する情報である機器識別情報を、上記管理識別情報として含む管理情報を上記記憶装置に記憶し、

50

上記履歴加工部は、

上記処理装置を用いて、機器を操作した時刻である操作時刻を示す情報である操作時刻情報と、上記操作時刻に操作された機器を示す情報である操作機器情報とを含む情報である操作履歴情報を、上記発生履歴情報として入力し、

上記処理装置を用いて、入力した上記操作履歴情報に含まれる操作時刻情報によって示される操作時刻を示す情報を、上記管理検索部が入力する時刻情報として出力し、入力した上記操作履歴情報に含まれる操作機器情報を上記管理検索部が入力する対象情報として出力し、

上記処理装置を用いて、上記管理検索部が出力した機器識別情報を入力し、

上記処理装置を用いて、入力した上記操作履歴情報に含まれる情報と、入力した上記機器識別情報とを含む加工済履歴情報を出力することを特徴とする請求項 1 に記載の履歴管理装置。 10

【請求項 1 2】

上記管理記憶部は、

上記処理装置を用いて、機器を識別する資産管理コードを、上記管理識別情報として含む管理情報を、上記記憶装置に記憶することを特徴とする請求項 1 1 に記載の履歴管理装置。

【請求項 1 3】

上記管理検索部は、更に、

上記処理装置を用いて、データを移動した時刻である移動時刻を示す情報である移動時刻情報を上記時刻情報として入力し、上記データを移動した移動元を示す情報である移動元情報と、上記データを移動した移動先を示す情報である移動先情報とを上記対象情報として入力し、 20

上記処理装置を用いて、入力した上記移動元情報に基づいて、上記移動元の種別を判別し、入力した上記移動先情報に基づいて、上記移動先の種別を判別し、判別した上記移動元の種別と判別した上記移動先の種別とに基づいて、上記データの移動方向を判別し、

上記処理装置を用いて、判別した上記データの移動方向を示す情報である移動方向情報を出力し、

上記履歴加工部は、更に、

上記処理装置を用いて、上記移動時刻情報と上記移動元情報と上記移動先情報とを含むデータ移動履歴情報を、上記発生履歴情報として入力し、 30

上記処理装置を用いて、入力した上記データ移動履歴情報に含まれる上記移動時刻情報と上記移動元情報と上記移動先情報とを、上記管理検索部に対して出力し、

上記処理装置を用いて、上記管理検索部が出力した移動方向情報を入力し、

上記処理装置を用いて、入力した移動方向情報を更に含む加工済履歴情報を出力することを特徴とする請求項 1 に記載の履歴管理装置。

【請求項 1 4】

上記管理記憶部は、

上記処理装置を用いて、利用者を識別する情報である利用者識別情報を、上記管理識別情報として含み、上記利用者が所有する電子メールアドレスを、上記対象識別情報として含む管理情報を上記記憶装置に記憶し、 40

上記履歴加工部は、

上記処理装置を用いて、電子メールを送信した時刻である送信時刻を示す情報である送信時刻情報と、上記電子メールの送信元を示す電子メールアドレスである送信元メールアドレスと、上記電子メールの送信先を示す電子メールアドレスである送信先メールアドレスとを含む情報であるメール送信履歴情報を、上記データ移動履歴情報として入力し、

上記処理装置を用いて、入力した上記メール送信履歴情報に含まれる上記送信時刻情報を上記管理検索部が入力する移動時刻情報として出力し、入力した上記メール送信履歴情報に含まれる送信元メールアドレスを上記管理検索部が入力する移動元情報として出力し、入力した上記メール送信冷機情報に含まれる送信先メールアドレスを上記管理検索部が 50

入力する移動先情報として出力し、

上記管理検索部は、

上記処理装置を用いて、入力した上記送信元メールアドレスに基づいて、上記送信元の種別を判別し、入力した上記送信先メールアドレスに基づいて、上記送信先の種別を判別し、判別した上記送信元の種別と判別した上記送信先の種別とに基づいて、上記電子メールの送受信方向を判別し、

上記処理装置を用いて、判別した上記電子メールの送受信方向を示す情報であるメール送受信方向情報を上記移動方向情報として出力することを特徴とする請求項 13 に記載の履歴管理装置。

【請求項 15】

10

上記管理検索部は、更に、

上記処理装置を用いて、判別した上記送信先の種別に基づいて、上記電子メールが不審メールであるか否かを判断し、

上記処理装置を用いて、上記電子メールが不審メールであると判断した場合に、異常発生を示す情報である異常発生情報を出力することを特徴とする請求項 14 に記載の履歴管理装置。

【請求項 16】

上記管理記憶部は、

上記処理装置を用いて、ファイルを記憶するファイル記憶装置を識別する情報であるファイル記憶装置識別情報を、上記管理識別情報として含む管理情報を上記記憶装置に記憶し、

20

上記履歴加工部は、

上記処理装置を用いて、ファイル記憶装置が記憶したファイルを他のファイル記憶装置に複製した時刻を示す複製時刻情報と、上記ファイルを記憶していたファイル記憶装置を示す情報である複製元情報と、上記ファイルを複製した他のファイル記憶装置を示す情報である複製先情報とを含む情報である複製履歴情報を、上記データ移動履歴情報として入力し、

上記処理装置を用いて、入力した上記複製履歴情報に含まれる複製時刻情報を上記管理検索部が入力する移動時刻情報として出力し、入力した上記複製履歴情報に含まれる複製元情報を上記管理検索部が入力する移動元情報として出力し、入力した上記複製履歴情報 30

30

上記管理検索部は、

上記処理装置を用いて、入力した上記複製元情報に対応するファイル記憶装置識別情報に基づいて、上記ファイル記憶装置の種別を判別し、入力した上記複製先情報に対応するファイル記憶装置識別情報に基づいて、上記他のファイル記憶装置の種別を判別し、判別した上記ファイル記憶装置の種別と判別した上記他のファイル記憶装置の種別とに基づいて、上記ファイルの移動方向を判別し、

上記処理装置を用いて、判別した上記ファイルの移動方向を示す情報であるファイル移動方向情報を出力する

ことを特徴とする請求項 13 に記載の履歴管理装置。

40

【請求項 17】

上記管理検索部は、更に、

上記処理装置を用いて、判別した上記ファイルの移動方向に基づいて、不審な複製であるか否かを判断し、

上記処理装置を用いて、不審な複製であると判断した場合に、異常発生を示す情報である異常発生情報を出力する

ことを特徴とする請求項 16 に記載の履歴管理装置。

【請求項 18】

上記履歴管理装置は、更に、

情報を出力する出力装置と、

50

上記処理装置を用いて、上記管理検索部が上記異常発生情報を出力した場合に、異常発生を示す警告を上記出力装置に出力する警告出力部と、
を有することを特徴とする請求項 10 及び請求項 15 及び請求項 17 のいずれかに記載の履歴管理装置。

【請求項 19】

情報を処理する処理装置と、情報を記憶する記憶装置とを有する履歴管理装置が履歴情報を管理する履歴管理方法において、

上記処理装置が、対象を識別する情報である管理識別情報と、期間を示す情報である期間情報と、上記期間情報によって示される期間において上記対象を示す情報である対象識別情報とを含む情報である管理情報を上記記憶装置に記憶する管理記憶工程と、

10

上記処理装置が、事象が発生した時刻である発生時刻を示す情報である発生時刻情報と、上記事象の発生に関与した対象である関与対象を示す情報である関与対象情報とを含む情報である発生履歴情報を入力する発生履歴入力工程と、

上記処理装置が、上記発生履歴入力工程で入力した上記発生履歴情報に含まれる発生時刻情報によって示される発生時刻を示す情報を、時刻情報とし、上記発生履歴入力工程で入力した上記発生履歴情報に含まれる関与対象情報を、対象情報として、上記管理記憶工程で記憶した管理情報のなかから、上記対象情報と、上記管理情報に含まれる対象識別情報とが一致し、かつ、上記時刻情報によって示される時刻が上記管理情報に含まれる期間情報によって示される期間内である管理情報を抽出する管理情報抽出工程と、

上記処理装置が、上記発生履歴入力工程で入力した上記発生履歴情報に含まれる情報と、上記管理情報抽出工程で抽出した上記管理情報に含まれる管理識別情報とを含む情報である加工済履歴情報を出力する履歴加工工程と、
を有することを特徴とする履歴管理方法。

20

【請求項 20】

情報を処理する処理装置と、情報を記憶する記憶装置とを有するコンピュータを、請求項 1 に記載の履歴管理装置として機能させることを特徴とする履歴管理プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

この発明は、膨大な量のログなどを収集管理する履歴管理装置に関する。

30

【背景技術】

【0002】

企業情報システムにおいて、システムを構成する様々な機器が出力するログの収集・保存が行われている。

収集保存されたログは、例えば、情報漏洩などのセキュリティに関する問題が発生した場合に、その原因を究明するために利用される。あるいは、システムが正しく運用されていることを客観的に示すためにも利用される。

【特許文献 1】特開 2002-7399 号公報

【非特許文献 1】小林雅一「プライバシー・ゼロ 社員監視時代」、光文社、2005 年 6 月 30 日、122～123 ページ

40

【発明の開示】

【発明が解決しようとする課題】

【0003】

収集保存されるログは、その量が膨大であり、情報漏洩などの問題が発生したことが発覚するには時間がかかることから、長期間にわたるログを保存しておく必要がある。

また、ログは、出力した機器により形式が異なり、これらを一括して管理することを難しくしている。

【0004】

この発明は、例えば、上記のような課題を解決するためになされたものであり、過去何年・何十年にもわたる膨大な量のログのなかから、必要なログを迅速・容易に見つける

50

ようにすることを目的とする。

【課題を解決するための手段】

【0005】

この発明にかかる履歴管理装置は、
情報を処理する処理装置と、
情報を記憶する記憶装置と、

上記処理装置を用いて、対象を識別する情報である管理識別情報と、期間を示す情報である期間情報と、上記期間情報によって示される期間において上記対象を示す情報である対象識別情報とを含む情報である管理情報を上記記憶装置に記憶する管理記憶部と、

上記処理装置を用いて、時刻を示す情報である時刻情報と、対象を示す情報である対象情報とを入力し、上記処理装置を用いて、上記管理記憶部が記憶した管理情報のなかから、入力した上記対象情報と、上記管理情報に含まれる対象識別情報とが一致し、かつ、入力した上記時刻情報によって示される時刻が上記管理情報に含まれる期間情報によって示される期間内である管理情報を抽出し、上記処理装置を用いて、抽出した上記管理情報に含まれる管理識別情報を出力する管理検索部と、

上記処理装置を用いて、事象が発生した時刻である発生時刻を示す情報である発生時刻情報と、上記事象の発生に関与した対象である関与対象を示す情報である関与対象情報とを含む情報である発生履歴情報を入力し、上記処理装置を用いて、入力した上記発生履歴情報に含まれる発生時刻情報によって示される発生時刻を示す情報を、上記管理検索部が入力する時刻情報として出力し、入力した上記発生履歴情報に含まれる関与対象情報を上記管理検索部が入力する対象情報として出力し、上記処理装置を用いて、上記管理検索部が出力した管理識別情報を入力し、上記処理装置を用いて、入力した上記発生履歴情報に含まれる情報と、入力した上記管理識別情報とを含む情報である加工済履歴情報を出力する履歴加工部と、
を有することを特徴とする。

【発明の効果】

【0006】

この発明にかかる履歴管理装置によれば、履歴加工部122が、発生履歴情報640に含まれる関与対象情報642が示す対象を識別する管理識別情報631を含む加工済履歴情報650を出力するので、出力された加工済履歴情報650を蓄積しておけば、あとで検索する必要が生じた場合に、膨大な加工済履歴情報650のなかから、目的とする加工済履歴情報650を素早く発見することができるという効果を奏する。

【発明を実施するための最良の形態】

【0007】

実施の形態1.

実施の形態1を、図1～図7を用いて説明する。

【0008】

図1は、この実施の形態における履歴管理装置100の外観の一例を示す図である。

図1において、履歴管理装置100は、システムユニット910、CRT（Cathode・Ray・Tube）やLCD（液晶）の表示画面を有する表示装置901、キーボード902（Key・Board：K/B）、マウス903、FDD904（Flexible・Disk・Drive）、コンパクトディスク装置905（CDD）、プリンタ装置906、スキャナ装置907などのハードウェア資源を備え、これらはケーブルや信号線で接続されている。

システムユニット910は、コンピュータであり、ファクシミリ機932、電話器931とケーブルで接続され、また、ローカルエリアネットワーク942（LAN）、ゲートウェイ941を介してインターネット940に接続されている。

【0009】

図2は、この実施の形態における履歴管理装置100のハードウェア資源の一例を示す図である。

図2において、履歴管理装置100は、プログラムを実行するCPU911(Central・Processing・Unit、中央処理装置、処理装置、演算装置、マイクロプロセッサ、マイクロコンピュータ、プロセッサともいう)を備えている。CPU911は、バス912を介してROM913、RAM914、通信ボード915、表示装置901、キーボード902、マウス903、FDD904、CDD905、プリンタ装置906、スキャナ装置907、磁気ディスク装置920と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置920の代わりに、光ディスク装置、メモリカード読み書き装置などの記憶装置でもよい。

RAM914は、揮発性メモリの一例である。ROM913、FDD904、CDD905、磁気ディスク装置920の記憶媒体は、不揮発性メモリの一例である。これらは、10
記憶装置あるいは記憶部の一例である。

通信ボード915、キーボード902、スキャナ装置907、FDD904などは、入力部、入力装置の一例である。

また、通信ボード915、表示装置901、プリンタ装置906などは、出力部、出力装置の一例である。

【0010】

通信ボード915は、ファクシミリ機932、電話器931、LAN942等に接続されている。通信ボード915は、LAN942に限らず、インターネット940、ISDN等のWAN(ワイドエリアネットワーク)などに接続されていても構わない。インターネット940或いはISDN等のWANに接続されている場合、ゲートウェイ941は不
20
用となる。

磁気ディスク装置920には、オペレーティングシステム921(OS)、ウィンドウシステム922、プログラム群923、ファイル群924が記憶されている。プログラム群923のプログラムは、CPU911、オペレーティングシステム921、ウィンドウシステム922により実行される。

【0011】

上記プログラム群923には、以下に述べる実施の形態の説明において「～部」、「～手段」として説明する機能を実行するプログラムが記憶されている。プログラムは、CPU911により読み出され実行される。

ファイル群924には、以下に述べる実施の形態の説明において、「～の判定結果」、30
「～の計算結果」、「～の処理結果」として説明する情報やデータや信号値や変数値やパラメータが、「～ファイル」や「～データベース」の各項目として記憶されている。「～ファイル」や「～データベース」は、ディスクやメモリなどの記録媒体に記憶される。ディスクやメモリなどの記憶媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してCPU911によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのCPUの動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示のCPUの動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

また、以下に述べる実施の形態の説明において説明するフローチャートの矢印の部分は40
主としてデータや信号の入出力を示し、データや信号値は、RAM914のメモリ、FDD904のフレキシブルディスク、CDD905のコンパクトディスク、磁気ディスク装置920の磁気ディスク、その他光ディスク、ミニディスク、DVD(Digital・Versatile・Disc)等の記録媒体に記録される。また、データや信号は、バス912や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

【0012】

また、以下に述べる実施の形態の説明において「～部」、「～手段」として説明するのは、「～回路」、「～装置」、「～機器」であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」、「～手段」として説明するものは、ROM913に記憶されたファームウェアで実現されていても構わない。或いは50

、ソフトウェアのみ、或いは、素子・デバイス・基板・配線などのハードウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ミニディスク、DVD等の記録媒体に記憶される。プログラムはCPU911により読み出され、CPU911により実行される。すなわち、プログラムは、以下に述べる「～部」、「～手段」としてコンピュータを機能させるものである。あるいは、以下に述べる「～部」、「～手段」の手順や方法をコンピュータに実行させるものである。

【0013】

図3は、この実施の形態における履歴管理装置100の機能ブロックの構成の一例を示すブロック構成図である。 10

履歴管理装置100は、ログ管理装置120、ID(Identifier)管理装置130、管理端末装置140を有する。

履歴管理装置100は、監視対象機器500から発生履歴情報を収集し、加工して蓄積し、入力した検索条件に合致するものを表示する。

【0014】

ログ管理装置120は、監視対象機器500から発生履歴情報を収集し、加工して蓄積する。

ID管理装置130は、ログ管理装置120が発生履歴情報を加工するために必要な識別情報を管理する。 20

管理端末装置140は、検索条件を入力し、ログ管理装置120が検索した結果を表示する。なお、管理端末装置140は、履歴管理装置100の一部でなくてもよい。

【0015】

ログ管理装置120は、履歴収集部121、履歴加工部122、履歴蓄積部123、履歴検索部124を有する。

履歴収集部121は、CPU911などの処理装置を用いて、監視対象機器500から通知される発生履歴情報を収集する。

ここで、発生履歴情報とは、監視対象機器500において発生した事象を記録した情報である。例えば、監視対象機器500が出力したログファイルに含まれるログ情報などであり、監視対象機器500を操作した場合、監視対象機器500が何かを検出した場合、監視対象機器500の状態が変化した場合など、様々な事象が発生した場合に発生履歴情報が生成される。 30

監視対象機器500は、発生履歴情報を生成する都度、履歴収集部121に通知してもよいし、生成した発生履歴情報を蓄積しておき、履歴収集部121から発生履歴情報の通知を要求する履歴通知要求を通知された場合に、まとめて履歴収集部121に通知することとしてもよい。

【0016】

履歴加工部122は、CPU911などの処理装置を用いて、履歴収集部121が収集した発生履歴情報を分析し、検索しやすいように加工して、加工済履歴情報を生成する。

履歴蓄積部123は、CPU911などの処理装置を用いて、履歴加工部122が加工した加工済履歴情報を、磁気ディスク装置920などの記憶装置に記憶する。 40

履歴検索部124は、CPU911などの処理装置を用いて、管理端末装置140から通知された検索条件に基づいて、履歴蓄積部123が記憶した加工済履歴情報を検索し、検索結果を管理端末装置140に通知する。

【0017】

ID管理装置130は、管理記憶部131、管理検索部132を有する。

管理記憶部131は、CPU911などの処理装置を用いて、管理情報を磁気ディスク装置920などの記憶装置に記憶する。

ここで、管理情報とは、発生履歴情報に含まれる識別情報の対応関係などを示す情報である。管理情報は、履歴加工部122が発生履歴情報を加工する際に利用される。 50

【0018】

管理検索部132は、CPU911などの処理装置を用いて、管理記憶部131が記憶した管理情報のなかから、履歴加工部122から通知された条件に合致する管理情報を検索し、検索結果を履歴加工部122に通知する。

管理検索部132は、また、CPU911などの処理装置を用いて、管理端末装置140から通知された検索条件に基づいて、管理記憶部131が記憶した管理情報を検索し、検索結果を管理端末装置140に通知する。

【0019】

管理端末装置140は、検索条件入力部141、検索結果表示部142を有する。

検索条件入力部141は、CPU911などの処理装置を用いて、検索条件をキーボード902などの入力装置から入力し、入力した検索条件を示す情報を、履歴検索部124や管理検索部132に通知する。 10

検索結果表示部142は、CPU911などの処理装置を用いて、履歴検索部124や管理検索部132が通知する検索結果を取得し、CRTなどの表示装置901やその他の出力装置に表示し、あるいは出力する。

管理端末装置140は、履歴照会部の一例である。

【0020】

次に、履歴管理装置100のうち、ID管理装置130について詳しく説明する。

図4は、この実施の形態におけるID管理装置130の詳細の一例を示す詳細ブロック図である。 20

管理記憶部131が記憶した管理情報610は、管理識別情報611、期間情報612、対象識別情報613などを含む情報である。

管理識別情報611は、対象を一意に識別する情報である。ここで、「一意に」とは、対象と一対一に対応した識別情報であることを意味する。すなわち、対象を指定すれば、対応する管理識別情報611が1つに定まり、逆に管理識別情報611を指定すれば、対応する対象が1つに定まる。また、時間が経過しても、対象と管理識別情報611との間の対応関係が変化することはない。

対象識別情報613は、対象を示す情報である。対象識別情報613は、管理識別情報611と同様、対象を識別することができる識別情報であるが、管理識別情報611と異なり、対象と一対一の対応関係にはない。したがって、1つの対象について、複数の対象識別情報613が存在してもよい。また、時間の経過により、対象と対象識別情報613との間の対応関係が変化することがあり、同じ対象識別情報613であっても、異なる対象を示す場合がある。 30

【0021】

例えば、コンピュータにログオンするためのユーザ名は、そのユーザを示す対象識別情報613である。しかし、同一のユーザが、別のコンピュータにログオンするため、異なるユーザ名を有している場合もあるので、管理識別情報611ではない。

また、電子メールを送受信するためのメールアドレスも、その利用者を示す対象識別情報613である。

また、ネットワークに接続したコンピュータのマシン名あるいはIP(Internet Protocol)アドレスは、そのコンピュータを示す対象識別情報613である。しかし、ネットワークの構成を変更した場合、マシン名やIPアドレスを付け替える可能性があるため、管理識別情報611ではない。 40

【0022】

従業員を管理するために付与する従業員コードや、会社の資産を管理するために付与する資産管理コードも、対象識別情報613である。なお、従業員コードや資産管理コードは、対象と一対一に対応しており、一度付与したら通常は変更しないので、管理識別情報611として用いることができる。

【0023】

期間情報612は、対象識別情報613が示す対象が、管理識別情報611によって識 50

別される対象と同一である期間を示す情報である。

期間情報 6 1 2 は、例えば、その期間の開始時刻を示す期間開始時刻情報と、その期間の終了時刻を示す期間終了時刻情報とを有し、期間開始時刻情報によって示される開始時刻から期間終了時刻情報によって示される終了時刻までの期間を示す。なお、ここで「開始時刻」「終了時刻」には、1 日のなかのいわゆる「時刻」だけでなく、日付も含まれるものとする。

例えば、コンピュータの IP アドレスが対象識別情報 6 1 3 である場合、そのコンピュータをネットワークに接続するなどして、その IP アドレスで運用することを開始した時刻から、例えばネットワークの構成を変更するなどして、そのコンピュータをその IP アドレスで運用することを終了した時刻までの期間を示す情報を、期間情報 6 1 2 とする。

10

なお、現在もその IP アドレスで運用中であれば、期間終了時刻情報を空欄とするなどして、その期間の終了時刻を指定しなくてもよい。

【0024】

管理記憶部 1 3 1 は、管理情報 6 1 0 を複数記憶する。1 つの管理情報 6 1 0 に含まれる管理識別情報 6 1 1、期間情報 6 1 2、対象識別情報 6 1 3 は、互いに対応づけられ、1 つの管理情報 6 1 0 は、期間情報 6 1 2 が示す期間内において、対象識別情報 6 1 3 が示す対象が、管理識別情報 6 1 1 によって識別される対象と同一であることを示す。

1 つの対象は複数の対象識別情報 6 1 3 を有する場合があるので、同じ管理識別情報 6 1 1 を含み、対象識別情報 6 1 3 が異なる管理情報 6 1 0 が複数ある場合がある。この場合、期間情報 6 1 2 が示す期間は、互いに重複していてもよいし、重複していなくてもよい。

20

また、時間の経過により、対象識別情報 6 1 3 が示す対象が変更される場合があるので、同じ対象識別情報 6 1 3 を含み、管理識別情報 6 1 1 が異なる管理情報 6 1 0 が複数ある場合もある。ただし、この場合は、期間情報 6 1 2 が示す期間が重複しないものとする。ある時刻において対象識別情報 6 1 3 が示す対象は、1 つに定まる必要があるからである。

【0025】

管理検索部 1 3 2 は、CPU 9 1 1 などの処理装置を用いて、時刻情報 6 2 1 と対象情報 6 2 2 とを入力し、管理記憶部 1 3 1 が記憶した管理情報 6 1 0 を検索して、入力した時刻情報 6 2 1 と対象情報 6 2 2 とに対応する管理識別情報 6 3 1 を出力する。

30

ここで、時刻情報 6 2 1 とは、時刻を示す情報であり、対象情報 6 2 2 とは、ユーザやコンピュータなどの対象を示す情報である。

管理検索部 1 3 2 は、時刻情報 6 2 1 が示す時刻において、対象情報 6 2 2 が示す対象を識別する管理識別情報 6 3 1 を出力する。

【0026】

図 5 は、この実施の形態における管理検索部 1 3 2 が管理情報 6 1 0 を検索する管理検索処理の流れの一例を示すフローチャート図である。

管理検索処理は、管理情報抽出工程の一例である。

なお、管理記憶部 1 3 1 が管理情報 6 1 0 を記憶する管理記憶工程は、管理検索処理の開始前に行われ、管理記憶部 1 3 1 が管理情報 6 1 0 を記憶しているものとする。

40

【0027】

S 0 0 1 において、管理検索部 1 3 2 は、CPU 9 1 1 などの処理装置を用いて、時刻情報 6 2 1 と対象情報 6 2 2 とを入力する。

S 0 0 2 において、管理検索部 1 3 2 は、CPU 9 1 1 などの処理装置を用いて、管理記憶部 1 3 1 が記憶した管理情報 6 1 0 を、順番に一つずつ取得する。

S 0 0 3 において、管理検索部 1 3 2 は、CPU 9 1 1 などの処理装置を用いて、S 0 0 2 で管理情報 6 1 0 を取得できたか否かを判断する。

管理情報 6 1 0 を取得できた場合には、S 0 0 4 へ進む。

管理記憶部 1 3 1 が記憶した管理情報 6 1 0 をすべて取得してしまい、これ以上取得できる管理情報 6 1 0 がいない場合には、S 0 0 9 へ進む。

50

【0028】

S004において、管理検索部132は、CPU911などの処理装置を用いて、S002で取得した管理情報610に含まれる対象識別情報613と、S001で入力した対象情報622とを比較する。

S005において、管理検索部132は、CPU911などの処理装置を用いて、S004で比較した結果、対象識別情報613と対象情報622とが一致すると判断した場合には、S006へ進む。

対象識別情報613と対象情報622とが一致しないと判断した場合には、S002に戻る。

【0029】

S006において、管理検索部132は、CPU911などの処理装置を用いて、S001で取得した時刻情報621が示す時刻と、S002で取得した管理情報610に含まれる期間情報612が示す期間とを比較する。

S007において、管理検索部132は、CPU911などの処理装置を用いて、S006で比較した結果、時刻情報621が示す時刻が期間情報612が示す期間内であると判断した場合には、S008へ進む。

期間内であると判断した場合には、S002に戻る。

【0030】

S008において、管理検索部132は、CPU911などの処理装置を用いて、S002で取得した管理情報610に含まれる管理識別情報611を、管理識別情報631として出力する。その後、管理検索処理を終了する。

【0031】

S009において、管理検索部132は、CPU911などの処理装置を用いて、該当なし情報639を出力する。その後、管理検索処理を終了する。

ここで、該当なし情報639とは、管理記憶部131が記憶した管理情報610のなかに、S001で入力した時刻情報621が示す時刻において、S001で入力した対象情報622が示す対象を識別する管理識別情報611を含む管理情報610が存在しないことを示す情報である。例えば、管理識別情報611として使用しないデータ（例えば「0」）を出力して、通常の出力である管理識別情報631と区別できるようにした情報である。

【0032】

なお、ここでの説明では、リニア検索方式により管理検索処理を行っているが、二分木方式やハッシュ方式など、他の検索方式を用いてもよい。

【0033】

次に、履歴管理装置100のうち、履歴加工部122について詳しく説明する。

図6は、この実施の形態における履歴加工部122の詳細の一例を示す詳細ブロック図である。

【0034】

履歴加工部122は、CPU911などの処理装置を用いて、発生履歴情報640を入力し、入力した発生履歴情報640を加工して、加工済履歴情報650を生成し、生成した加工済履歴情報650を出力する。

履歴加工部122が入力する発生履歴情報640には、発生時刻情報641と関与対象情報642とが含まれている。

発生時刻情報641は、発生履歴情報640が示す事象の発生した時刻を示す情報である。

関与対象情報642は、発生履歴情報640が示す事象に関与した対象を示す情報である。

【0035】

例えば、ある時刻に、あるユーザが、監視対象機器500であるコンピュータにログオンしたとする。ログオンされたコンピュータは、これを事象の発生と認識し、発生履歴情

10

20

30

40

50

報 6 4 0 を生成する。なお、ログオンされたコンピュータではなく、ログオンされたコンピュータの動作を監視している他のコンピュータが、発生履歴情報 6 4 0 を生成してもよい。

この場合、生成された発生履歴情報 6 4 0 には、そのユーザがコンピュータにログオンした時刻を示す発生時刻情報 6 4 1 が含まれる。

また、関与対象情報 6 4 2 として、そのユーザを示すユーザ名などの情報や、そのコンピュータを示すマシン名などの情報が含まれる。

【0036】

あるいは、ある時刻に、ある従業員が、監視対象機器 5 0 0 である入退室管理装置に I D カードを挿入し、部屋の扉を開けたとする。入退室管理装置は、これを事象の発生と認識し、発生履歴情報 6 4 0 を生成する。 10

この場合、生成された発生履歴情報 6 4 0 には、その従業員が入退室管理装置に I D カードを挿入した時刻を示す発生時刻情報 6 4 1 が含まれる。

また、関与対象情報 6 4 2 として、その従業員を示す I D カード番号などの情報や、開けられた扉を示す扉番号などの情報が含まれる。

【0037】

生成された発生履歴情報 6 4 0 は、履歴収集部 1 2 1 が収集し、履歴加工部 1 2 2 に入力される。

【0038】

関与対象情報 6 4 2 は、管理記憶部 1 3 1 が記憶した管理情報 6 1 0 に含まれる対象識別情報 6 1 3 と同一の情報であり、ユーザやコンピュータなどの対象を示す情報である。 20

関与対象情報 6 4 2 は、その事象が発生した時点においてその対象を示す情報であり、時間の経過によって、同一の関与対象情報 6 4 2 が示す対象が変化する場合がある。

また、一人の利用者が I D カードを使って部屋に入り、部屋のなかのコンピュータにログオンした場合、同じ利用者が関与した事象であるにもかかわらず、一方では I D カード番号を、他方ではユーザ名を関与対象情報 6 4 2 として含む発生履歴情報 6 4 0 が生成される。

このように、発生履歴情報 6 4 0 に含まれる関与対象情報 6 4 2 は、その事象が発生した時刻や、その発生履歴情報 6 4 0 を生成した監視対象機器 5 0 0 によって異なり、統一されていない。 30

履歴加工部 1 2 2 は、このようにバラバラの関与対象情報 6 4 2 を含む発生履歴情報 6 4 0 を加工して、統一された管理識別情報 6 5 3 を含む加工済履歴情報 6 5 0 を生成する。

これにより、なにか問題が発生して、履歴蓄積部 1 2 3 が記憶した加工済履歴情報 6 5 0 を検索する必要がある場合、膨大な履歴情報のなかから、目的とする履歴情報を素早く発見することができる。

【0039】

そのため、履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、入力した発生履歴情報 6 4 0 に含まれる発生時刻情報 6 4 1 と関与対象情報 6 4 2 とを取得し、管理検索部 1 3 2 が入力する時刻情報 6 2 1 と対象情報 6 2 2 として、管理検索部 1 3 2 に対して出力する。管理検索部 1 3 2 は、C P U 9 1 1 などの処理装置を用いて、図 5 で説明した管理検索処理を行い、入力した発生時刻情報 6 4 1 と関与対象情報 6 4 2 とから、対応する管理識別情報 6 3 1 を求めて出力する。履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、管理検索部 1 3 2 が出力した管理識別情報 6 3 1 を取得し、発生履歴情報 6 4 0 に含まれる発生時刻情報 6 4 1 や関与対象情報 6 4 2 などの情報と合わせて、加工済履歴情報 6 5 0 を生成し、出力する。 40

【0040】

図 7 は、この実施の形態における履歴加工部 1 2 2 が履歴情報を加工する履歴加工処理の流れの一例を示すフローチャート図である。

【0041】

S 0 1 1（発生履歴入力工程）において、履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、発生履歴情報 6 4 0 を入力する。なお、この例では、履歴収集部 1 2 1 が監視対象機器 5 0 0 から収集した発生履歴情報 6 4 0 を出力し、履歴収集部 1 2 1 が出力した発生履歴情報 6 4 0 を入力する構成としているが、監視対象機器 5 0 0 が出力した発生履歴情報 6 4 0 を、履歴加工部 1 2 2 が直接入力する構成としてもよい。

【0 0 4 2】

S 0 1 2 において、履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 1 1 で入力した発生履歴情報 6 4 0 を解析し、入力した発生履歴情報 6 4 0 に含まれる発生時刻情報 6 4 1 と関与対象情報 6 4 2 とを取得する。

【0 0 4 3】

S 0 1 3 において、履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 1 2 で取得した発生時刻情報 6 4 1 と関与対象情報 6 4 2 とを、管理検索部 1 3 2 が入力する時刻情報 6 2 1 と対象情報 6 2 2 として、管理検索部 1 3 2 に対して出力する。

なお、発生履歴情報 6 4 0 に含まれる発生時刻情報 6 4 1 は、グリニッジ標準時で時刻を示す情報であったり、ローカル時で時刻を示す情報であったり、時分までの情報であったり、ミリ秒単位の情報であったり、生成した監視対象機器 5 0 0 によって異なる形式の発生時刻情報 6 4 1 である可能性がある。履歴加工部 1 2 2 は、これら異なる形式の発生時刻情報 6 4 1 である場合には、その発生時刻情報 6 4 1 によって示される時刻を示す、統一された形式の時刻情報 6 2 1 を生成し、管理検索部 1 3 2 に対して出力する。

なお、最初から形式の統一された発生時刻情報 6 4 1 を含む発生履歴情報 6 4 0 を履歴収集部 1 2 1 が収集する場合や、履歴収集部 1 2 1 が形式を統一する場合には、履歴加工部 1 2 2 は、入力した発生時刻情報 6 4 1 をそのまま管理検索部 1 3 2 に対して出力してもよい。

【0 0 4 4】

S 0 1 4 において、履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 1 3 での出力した情報を入力した管理検索部 1 3 2 が管理検索処理をした結果を入力する。履歴加工部 1 2 2 が入力する管理検索処理の結果は、管理識別情報 6 3 1 または該当なし情報 6 3 9 である。

【0 0 4 5】

S 0 1 5 において、履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 1 4 で入力した情報が管理識別情報 6 3 1 であるか該当なし情報 6 3 9 であるかを判断する。

管理識別情報 6 3 1 であると判断した場合には、S 0 1 6 へ進む。

該当なし情報 6 3 9 であると判断した場合には、S 0 1 7 へ進む。

【0 0 4 6】

S 0 1 6（履歴加工工程）において、履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 1 4 で入力した管理識別情報 6 3 1 を、管理識別情報 6 5 3 として含む加工済履歴情報 6 5 0 を生成し、出力する。

履歴加工部 1 2 2 が出力する加工済履歴情報 6 5 0 は、S 0 1 1 で入力した発生履歴情報 6 4 0 に含まれるすべての情報を含み、更に管理識別情報 6 5 3 を含む情報であってもよい。あるいは、S 0 1 1 で入力した発生履歴情報 6 4 0 に含まれる関与対象情報 6 4 2 を、管理識別情報 6 5 3 で置き換えた情報であってもよい。

【0 0 4 7】

S 0 1 7 において、履歴加工部 1 2 2 は、C P U 9 1 1 などの処理装置を用いて、異常発生情報 6 5 9 を含む加工済履歴情報 6 5 0 を生成し、出力する。

異常発生情報 6 5 9 とは、異常発生を示す情報である。

【0 0 4 8】

例えば、従業員が退職して、その従業員が使用していたユーザ I D が抹消された場合、管理記憶部 1 3 1 が記憶する管理情報 6 1 0 に含まれる期間情報 6 1 2 は、そのユーザ I D が抹消された時刻を終了時刻とする情報に書き換えられている。

10

20

30

40

50

しかし、一部の監視対象機器 500 において、そのユーザ ID を抹消するのを忘れてしまうと、抹消されたはずのユーザ ID で、その監視対象機器 500 を操作することができる。

その場合、そのユーザ ID でその監視対象機器 500 を操作すると、監視対象機器 500 は、そのユーザ ID を関与対象情報 642 として含む発生履歴情報 640 を生成する。

履歴加工部 122 がそのようにして生成された発生履歴情報 640 を加工しようとする、その監視対象機器 500 が操作された時刻は、そのユーザ ID についての管理情報 610 に含まれる期間情報 612 が示す期間外の時刻であるから、管理検索部 132 は、該当なし情報 639 を出力する。

これにより、ユーザ ID の抹消忘れという異常事態が発生していることがわかる。そこで、履歴加工部 122 は、異常発生を示す異常発生情報 659 を含む加工済履歴情報 650 を出力する。 10

【0049】

あるいは、利用者が勝手にユーザ ID を生成して監視対象機器 500 を使用した場合も、そのユーザ ID は管理記憶部 131 が記憶した管理情報 610 に反映されていないので、管理検索部 132 は、該当なし情報 639 を出力する。これにより、不正使用という異常事態が発生していることがわかるので、履歴加工部 122 は、異常発生を示す異常発生情報 659 を含む加工済履歴情報 650 を出力する。

【0050】

のちになんらかの問題が発生し、履歴蓄積部 123 が記憶した加工済履歴情報 650 を調べる必要が生じた場合、異常発生情報 659 を含む加工済履歴情報 650 を検索すれば、問題発生の原因を突き止めることができる。 20

なお、異常発生情報 659 を含む加工済履歴情報 650 を出力するにとどめ、なんらかの問題が発生しない限りは放置する構成としてもよい。あるいは、CPU 911 などの処理装置を用いて、異常発生を示す警告を CRT などの表示装置 901 やその他の出力装置に出力する警告出力部を設け、履歴加工部 122 が出力した加工済履歴情報 650 を警告出力部が入力して、入力した加工済履歴情報 650 に異常発生情報 659 が含まれているか否かを判断し、異常発生情報 659 が含まれていると判断した場合には、警告出力部が警告を出力する構成としてもよい。そうすれば、問題が発生する前に異常事態を把握し、なんらかの対処をすることができるので、好ましい。 30

【0051】

この実施の形態における履歴管理装置 100 は、情報を処理する CPU 911 などの処理装置と、情報を記憶する磁気ディスク装置 920 などの記憶装置と、CPU 911 などの処理装置を用いて、対象を識別する情報である管理識別情報 611 と、期間を示す情報である期間情報 612 と、期間情報 612 によって示される期間において対象を示す情報である対象識別情報 613 とを含む情報である管理情報 610 を磁気ディスク装置 920 などの記憶装置に記憶する管理記憶部 131 と、CPU 911 などの処理装置を用いて、時刻を示す情報である時刻情報 621 と、対象を示す情報である対象情報 622 とを入力し、CPU 911 などの処理装置を用いて、管理記憶部 131 が記憶した管理情報のなかから、入力した対象情報 622 と、管理情報 610 に含まれる対象識別情報 613 とが一致し、かつ、入力した時刻情報 621 によって示される時刻が管理情報 610 に含まれる期間情報 612 によって示される期間内である管理情報 610 を抽出し、CPU 911 などの処理装置を用いて、抽出した管理情報 610 に含まれる管理識別情報 611 を出力する管理検索部 132 と、CPU 911 などの処理装置を用いて、事象が発生した時刻である発生時刻を示す情報である発生時刻情報 641 と、上記事象の発生に関与した対象である関与対象を示す情報である関与対象情報 642 とを含む情報である発生履歴情報 640 を入力し、CPU 911 などの処理装置を用いて、入力した発生履歴情報 640 に含まれる発生時刻情報 641 によって示される発生時刻を示す情報を、管理検索部 132 が入力する時刻情報 621 として出力し、入力した発生履歴情報 640 に含まれる関与対象情報 642 を管理検索部 132 が入力する対象情報 622 として出力し、CPU 911 などの 40 50

処理装置を用いて、管理検索部 1 3 2 が出力した管理識別情報 6 3 1 を入力し、CPU 9 1 1 などの処理装置を用いて、入力した発生履歴情報 6 4 0 に含まれる情報と、入力した管理識別情報 6 3 1 とを含む情報である加工済履歴情報 6 5 0 を出力する履歴加工部 1 2 2 とを有することを特徴とする。

【0052】

この実施の形態における履歴管理装置 1 0 0 によれば、履歴加工部 1 2 2 が、発生履歴情報 6 4 0 に含まれる関与対象情報 6 4 2 が示す対象を識別する管理識別情報 6 3 1 を含む加工済履歴情報 6 5 0 を出力するので、出力された加工済履歴情報 6 5 0 を蓄積しておけば、あとで検索する必要がある場合に、膨大な加工済履歴情報 6 5 0 のなかから、目的とする加工済履歴情報 6 5 0 を素早く発見することができるという効果を奏する。

10

【0053】

この実施の形態における履歴管理装置 1 0 0 は、更に、CPU 9 1 1 などの処理装置を用いて、履歴加工部 1 2 2 が出力した加工済履歴情報 6 5 0 を入力し、CPU 9 1 1 などの処理装置を用いて、入力した加工済履歴情報 6 5 0 を磁気ディスク装置 9 2 0 などの記憶装置に記憶する履歴蓄積部 1 2 3 と、CPU 9 1 1 などの処理装置を用いて、加工済履歴情報 6 5 0 に含まれる情報についての検索条件を示す情報である履歴検索条件情報を入力し、CPU 9 1 1 などの処理装置を用いて、履歴蓄積部 1 2 3 が記憶した加工済履歴情報 6 5 0 のなかから、入力した履歴検索条件情報によって示される検索条件に合致する加工済履歴情報 6 5 0 を抽出し、CPU 9 1 1 などの処理装置を用いて、抽出した加工済履歴情報 6 5 0 に含まれる情報を出力することを特徴とする。

20

【0054】

この実施の形態における履歴管理装置 1 0 0 によれば、履歴蓄積部 1 2 3 が加工済履歴情報 6 5 0 を記憶しておき、あとで必要になった場合に、履歴検索部 1 2 4 が加工済履歴情報 6 5 0 を検索して必要な加工済履歴情報 6 5 0 を抽出するので、のちに問題が発生した場合などに、速やかにその原因を解明することができるという効果を奏する。

【0055】

この実施の形態における履歴管理装置 1 0 0 は、履歴蓄積部 1 2 3 が、磁気ディスク装置 9 2 0 などの記憶装置を用いて、履歴加工部 1 2 2 が入力した発生履歴情報と、管理識別情報とのみを含む加工済履歴情報を記憶し、管理識別情報によって識別される対象の属性を示す情報を記憶しないことを特徴とする。

30

【0056】

この実施の形態における履歴管理装置 1 0 0 によれば、履歴蓄積部 1 2 3 は、履歴検索に必要な情報のみを記憶するので、履歴蓄積部 1 2 3 が記憶する加工済履歴情報の情報量を抑えることができ、履歴を保存するために必要な記憶装置の記憶容量が小さくて済み、履歴検索も速いという効果を奏する。

また、履歴検索結果を表示する際には、対象の属性を示す情報を付加して表示等するので、利用者が理解しやすいという効果を奏する。

【0057】

この実施の形態における履歴管理装置 1 0 0 は、管理検索部 1 3 2 が、更に、CPU 9 1 1 などの処理装置を用いて、管理記憶部 1 3 1 が記憶した管理情報 6 1 0 のなかから、抽出できる管理情報が存在しない場合に、該当する管理情報 6 1 0 がないことを示す情報である該当なし情報 6 3 9 を出力し、履歴加工部 1 2 2 が、CPU 9 1 1 などの処理装置を用いて、管理検索部 1 3 2 が該当なし情報 6 3 9 を出力した場合に、異常発生を示す異常発生情報 6 5 9 を更に含む加工済履歴情報 6 5 0 を出力することを特徴とする。

40

【0058】

この実施の形態の履歴管理装置 1 0 0 によれば、履歴加工部 1 2 2 が、入力した発生履歴情報 6 4 0 に含まれる関与対象情報 6 4 2 に該当する管理情報 6 1 0 がない場合に、異常発生情報 6 5 9 を含む加工済履歴情報 6 5 0 を出力するので、のちになんらかの問題が発生して加工済履歴情報 6 5 0 を検索する必要がある場合に、異常発生情報 6 5 9 を含む加工済履歴情報 6 5 0 を検索することで、問題発生の原因を突き止めることができると

50

いう効果を奏する。

【0059】

この実施の形態における履歴管理装置100は、更に、情報を入力するCRTなどの表示装置901やその他の出力装置と、CPU911などの処理装置を用いて、履歴加工部122が異常発生情報659を含む加工済履歴情報650を出力した場合に、異常発生を示す警告をCRTなどの表示装置901やその他の出力装置に出力する警告出力部とを有することを特徴とする。

【0060】

この実施の形態の履歴管理装置100によれば、履歴加工部122が異常発生情報659を含む加工済履歴情報650を出力した場合に、警告出力部が警告を出力するので、問題が発生する前に異常事態に対処することができ、その異常に基づく問題の発生を未然に防ぐことができるという効果を奏する。 10

【0061】

なお、警告出力部がない構成であっても、不正行為をのちに見つけようと思ったら見つけられるというだけで、不正行為を抑止する効果を期待することができる。そのほうが、常に監視されているというプレッシャーを従業員に与えなくて済むので、好ましい場合もある。

【0062】

この実施の形態における履歴管理装置100が履歴情報を管理する履歴管理方法は、CPU911などの処理装置が、対象を識別する情報である管理識別情報611と、期間を示す情報である期間情報612と、期間情報612によって示される期間においてその対象を示す情報である対象識別情報613とを含む情報である管理情報610を磁気ディスク装置920などの記憶装置に記憶する管理記憶工程と、CPU911などの処理装置が、事象が発生した時刻である発生時刻を示す情報である発生時刻情報641と、上記事象の発生に関与した対象である関与対象を示す情報である関与対象情報642とを含む情報である発生履歴情報640を入力する発生履歴入力工程と、CPU911などの処理装置が、発生履歴入力工程で入力した発生履歴情報640に含まれる発生時刻情報641によって示される発生時刻を、時刻情報とし、発生履歴入力工程で入力した発生履歴情報640に含まれる関与対象情報642を、対象情報として、管理記憶工程で記憶した管理情報610のなかから、対象情報と、管理情報610に含まれる対象識別情報613とが一致し、かつ、時刻情報によって示される時刻が管理情報610に含まれる期間情報612によって示される期間内である管理情報610を抽出する管理情報抽出工程と、CPU911などの処理装置が、発生履歴入力工程で入力した発生履歴情報640に含まれる情報と、管理情報抽出工程で抽出した管理情報610に含まれる管理識別情報611とを含む情報である加工済履歴情報650を出力する履歴加工工程とを有することを特徴とする。 20 30

【0063】

この実施の形態における履歴管理装置100が履歴情報を管理する履歴管理方法によれば、発生履歴入力工程で入力した発生履歴情報640に含まれる対象識別情報613に対応する管理情報610を管理情報抽出工程で抽出し、抽出した管理情報610に含まれる管理識別情報611を含む加工済履歴情報650を出力するので、加工済履歴情報650を蓄積しておけば、あとで検索する必要が生じた場合に、膨大な加工済履歴情報650のなかから、目的とする加工済履歴情報650を素早く見つけることができるという効果を奏する。 40

【0064】

この実施の形態における履歴管理装置100は、情報を処理するCPU911などの処理装置と、情報を記憶する磁気ディスク装置920などの記憶装置とを有するコンピュータを上述した履歴管理装置100として機能させる履歴管理プログラムを、コンピュータに実行させることにより実現することができる。

【0065】

この実施の形態における履歴管理プログラムによれば、履歴加工部122が、発生履歴 50

情報 6 4 0 に含まれる関与対象情報 6 4 2 が示す対象を識別する管理識別情報 6 3 1 を含む加工済履歴情報 6 5 0 を出力する履歴管理装置 1 0 0 としてコンピュータを機能させるので、出力された加工済履歴情報 6 5 0 を蓄積しておけば、あとで検索する必要が生じた場合に、膨大な加工済履歴情報 6 5 0 のなかから、目的とする加工済履歴情報 6 5 0 を素早く発見することができるという効果を奏する。

【0066】

この実施の形態における履歴管理装置 1 0 0 は、例えばログなどの履歴情報を加工するものであり、ログ加工装置とも呼ばれる。

この実施の形態におけるログ加工装置は、ログごとに異なる、個人や機器を特定する個別 ID（ログオンアカウントやマシン名など）（対象識別情報 6 1 3）を、ログに依存せず個人や機器を一意に特定する統合 ID（管理識別情報 6 1 1）を導入し、それと紐付けて管理し、さらにログに含まれる、ログごとの個別 ID を、統合 ID で置き換えることを特徴とする。 10

この実施の形態におけるログ加工装置は、個別 ID を、現在使われている ID のみならず過去に使われていた ID についても、その有効期間とともに管理し、個別 ID から統合 ID を照会する際に、時刻もキーに照会することを特徴とする。

【0067】

実施の形態 2 .

実施の形態 2 について、図 8 ～図 1 1 を用いて説明する。

この実施の形態における履歴管理装置 1 0 0 の外観、ハードウェア資源、ブロック構成は、実施の形態 1 において説明した履歴管理装置 1 0 0 と同様なので、ここでは説明を省略する。 20

【0068】

この実施の形態における履歴管理装置 1 0 0 は、監視対象機器 5 0 0 が生成した発生履歴情報 6 4 0 がある程度溜まってから、履歴収集部 1 2 1 が収集し、履歴加工部 1 2 2 が、複数の発生履歴情報 6 4 0 をまとめて加工するものである。

例えば、1 日の業務が終了したあとの深夜など負荷の少ない時間帯を利用して、その日 1 日に発生した発生履歴情報 6 4 0 をまとめて処理する場合である。

【0069】

このように、複数の発生履歴情報 6 4 0 をまとめて処理する場合には、加工すべき発生履歴情報 6 4 0 のなかに、同一の関与対象情報 6 4 2 を含む発生履歴情報 6 4 0 が複数存在する場合がある。この実施の形態における履歴管理装置 1 0 0 は、そのような場合に、管理検索部 1 3 2 が重複した管理検索処理をしないようにすることにより、処理を少なくし、膨大な発生履歴情報 6 4 0 を速く加工できるようにするものである。 30

【0070】

図 8 は、この実施の形態における履歴加工部 1 2 2 のブロック構成の一例を示す詳細ブロック図である。

【0071】

履歴加工部 1 2 2 は、CPU 9 1 1 などの処理装置を用いて、複数の発生履歴情報 6 4 0 を入力し、入力した複数の発生履歴情報 6 4 0 を加工して複数の加工済履歴情報 6 5 0 を生成し、生成した複数の加工済履歴情報 6 5 0 を出力する。 40

履歴加工部 1 2 2 は、発生履歴情報 6 4 0 の加工に際し、発生履歴情報 6 4 0 に含まれる関与対象情報 6 4 2 が示す対象を識別する管理識別情報 6 3 1 を取得するため、管理検索部 1 3 2 に対して、関与対象情報 6 6 1、開始時刻情報 6 6 2、終了時刻情報 6 6 3 を通知し、管理検索部 1 3 2 が出力した期間付管理識別情報 6 3 0 を取得する。

【0072】

管理検索部 1 3 2 は、CPU 9 1 1 などの処理装置を用いて、履歴加工部 1 2 2 が通知した関与対象情報 6 6 1 を対象情報 6 2 2 として入力する。また、管理検索部 1 3 2 は、CPU 9 1 1 などの処理装置を用いて、履歴加工部 1 2 2 が通知した開始時刻情報 6 6 2 及び終了時刻情報 6 6 3 を時刻情報 6 2 1 として入力する。 50

【0073】

この実施の形態における管理検索部132は、入力した開始時刻情報662が示す開始時刻から、入力した終了時刻情報663が示す終了時刻までの期間において、入力した関与対象情報661が示す対象を識別する管理識別情報631を検索し、出力する。

【0074】

実施の形態1で説明したように、関与対象情報661と関与対象情報661が示す対象との対応関係は、時間の経過により変化する可能性がある。

例えば、関与対象情報661がコンピュータのIPアドレスである場合、ネットワークの構成を変更することにより、IPアドレスが変化する場合がある。このとき、変更前は他のコンピュータに割り当てられていたIPアドレスが、変更後には別のコンピュータに割り当てられる場合があり、同じ関与対象情報661でも、異なる対象を示す場合がある。

10

したがって、一定の幅がある期間を指定して、関与対象情報661が示す対象を識別する管理識別情報631を検索すると、その期間内に、関与対象情報661と対象との対応関係が変化した結果、複数の管理識別情報631が抽出される場合がある。

この実施の形態の管理検索部132は、期間付管理識別情報630として、期間情報632を管理識別情報631とともに出力する。

期間情報632は、入力した関与対象情報661が、出力した管理識別情報631によって識別される対象を示す期間を示す情報である。

【0075】

20

図9は、この実施の形態における管理検索部132が管理情報610を検索する管理検索処理の流れの一例を示すフローチャート図である。

管理検索処理は、管理情報抽出工程の一例である。

【0076】

S021において、管理検索部132は、CPU911などの処理装置を用いて、開始時刻情報662と、終了時刻情報663と、関与対象情報661とを入力する。

管理検索部132は、開始時刻情報662と終了時刻情報663とを、時刻情報として入力する。開始時刻情報662は、開始時刻を示す情報である。終了時刻情報663は、終了時刻を示す情報である。

管理検索部132は、関与対象情報661を、対象情報として入力する。

30

【0077】

S022において、管理検索部132は、CPU911などの処理装置を用いて、管理記憶部131が記憶した管理情報610を、順番に一つずつ取得する。

S023において、管理検索部132は、CPU911などの処理装置を用いて、S022で管理情報610を取得できたか否かを判断する。

管理情報610を取得できた場合には、S024へ進む。

管理記憶部131が記憶した管理情報610をすべて取得してしまい、これ以上取得できる管理情報610がない場合には、S031へ進む。

【0078】

S024において、管理検索部132は、CPU911などの処理装置を用いて、S022で取得した管理情報610に含まれる対象識別情報613と、S021で入力した関与対象情報661とを比較する。

40

S025において、管理検索部132は、CPU911などの処理装置を用いて、S024で比較した結果、対象識別情報613と関与対象情報661とが一致すると判断した場合には、S026へ進む。

対象識別情報613と関与対象情報661とが一致しないと判断した場合には、S022に戻る。

【0079】

S026において、管理検索部132は、CPU911などの処理装置を用いて、S022で取得した管理情報610に含まれる期間情報612が示す期間の終了時刻と、S0

50

21で入力した開始時刻情報662が示す開始時刻とを比較する。

S027において、管理検索部132は、CPU911などの処理装置を用いて、S026で比較した結果、開始時刻情報662が示す開始時刻が、期間情報612が示す期間の終了時刻より後であると判断した場合には、S022に戻る。

開始時刻情報662が示す開始時刻が、期間情報612が示す期間の終了時刻以前であると判断した場合には、S028へ進む。

【0080】

S028において、管理検索部132は、CPU911などの処理装置を用いて、S022で取得した管理情報610に含まれる期間情報612が示す期間の開始時刻と、S021で入力した終了時刻情報663が示す終了時刻とを比較する。

S029において、管理検索部132は、CPU911などの処理装置を用いて、S028で判断した結果、終了時刻情報663が示す終了時刻が、期間情報612が示す期間の開始時刻よりも前であると判断した場合には、S022に戻る。

終了時刻情報663が示す終了時刻が、期間情報612が示す期間の開始時刻以後であると判断した場合には、S030へ進む。

【0081】

S030において、管理検索部132は、CPU911などの処理装置を用いて、期間付管理識別情報630を出力する。期間付管理識別情報630は、管理識別情報631と期間情報632とを含む。

期間付管理識別情報630に含まれる管理識別情報631は、S022で取得した管理情報610に含まれる管理識別情報611である。

期間付管理識別情報630に含まれる期間情報632は、S022で取得した管理情報610に含まれる期間情報612である。

あるいは、期間付管理識別情報630に含まれる期間情報632は、S022で取得した管理情報610に含まれる期間情報612が示す期間から、S021で取得した開始時刻情報662及び終了時刻情報663によって示される開始時刻から終了時刻までの期間以外の期間を除いた期間を示す情報であってもよい。

すなわち、管理情報610に含まれる期間情報612が示す期間の開始時刻が、S021で入力した開始時刻情報662が示す開始時刻より前の場合には、管理検索部132は、管理情報610に含まれる期間情報612を、S021で入力した開始時刻情報662が示す開始時刻が、期間の開始時刻となるよう修正して、期間情報632としてもよい。

同様に、管理情報610に含まれる期間情報612が示す期間の終了時刻が、S021で入力した終了時刻情報663が示す終了時刻より後の場合には、管理検索部132は、管理情報610に含まれる期間情報612を、S021で入力した終了時刻情報663が示す終了時刻が、期間の終了時刻となるよう修正して、期間情報632としてもよい。

【0082】

S031において、管理検索部132は、CPU911などの処理装置を用いて、検索終了情報638を出力し、管理検索処理を終了する。

検索終了情報638は、管理検索処理が終了したことを示す情報である。

【0083】

なお、実施の形態1で説明したのと同様、リニア検索方式ではなく、他の検索方式により管理検索処理をしてもよい。

【0084】

これにより、管理検索部132は、入力した対象情報と、管理情報610に含まれる対象識別情報613とが一致し、かつ、入力した開始時刻情報662によって示される開始時刻から入力した終了時刻情報663によって示される終了時刻までの期間と、管理情報610に含まれる期間情報612によって示される時間との間に重複する期間がある管理情報610を、管理記憶部131が記憶した管理情報610のなかから抽出し、抽出した管理情報610に対応する期間付管理識別情報630を出力する。

【0085】

この実施の形態における管理検索部 1 3 2 は、入力した条件に合致する管理情報 6 1 0 が複数ある場合には、条件に合致する管理情報 6 1 0 に対応する期間付管理識別情報 6 3 0 を複数出力する。

【0086】

この例では、条件に合致する管理情報 6 1 0 が見つかる都度、管理検索部 1 3 2 が期間付管理識別情報 6 3 0 を出力しているが、期間付管理識別情報 6 3 0 を一時的に記憶しておき、管理記憶部 1 3 1 が記憶した管理情報 6 1 0 の検索がすべて終了した後に、それまでに見つけた期間付管理識別情報 6 3 0 をまとめて出力することとしてもよい。

その場合には、検索終了情報 6 3 8 を出力せず、例えば、条件に合致した管理情報 6 1 0 の数を示す情報を出力することとしてもよい。

10

【0087】

図 8 に戻り、履歴加工部 1 2 2 の説明を続ける。

【0088】

履歴加工部 1 2 2 は、発生履歴記憶部 2 2 1、発生期間判断部 2 2 2、発生期間記憶部 2 2 3、発生期間通知部 2 2 4、対応期間取得部 2 2 5、対応期間記憶部 2 2 6、対応判断部 2 2 7 を有する。

【0089】

発生履歴記憶部 2 2 1 は、CPU 9 1 1 などの処理装置を用いて、複数の発生履歴情報 6 4 0 を入力する。発生履歴記憶部 2 2 1 は、CPU 9 1 1 などの処理装置を用いて、入力した複数の発生履歴情報 6 4 0 を磁気ディスク装置 9 2 0 などの記憶装置に記憶する。

20

【0090】

発生期間判断部 2 2 2 は、CPU 9 1 1 などの処理装置を用いて、発生履歴記憶部 2 2 1 が記憶した発生履歴情報 6 4 0 を取得する。発生期間判断部 2 2 2 は、CPU 9 1 1 などの処理装置を用いて、取得した発生履歴情報 6 4 0 に含まれる発生時刻情報 6 4 1 と関与対象情報 6 4 2 とを取得する。

発生期間判断部 2 2 2 は、取得した発生時刻情報 6 4 1 及び関与対象情報 6 4 2 に基づいて、発生期間記憶部 2 2 3 が記憶した発生期間情報 6 6 0 を更新する。

【0091】

発生期間記憶部 2 2 3 は、CPU 9 1 1 などの処理装置を用いて、発生期間情報 6 6 0 を磁気ディスク装置 9 2 0 などの記憶装置に記憶する。

30

発生期間情報 6 6 0 は、発生履歴情報 6 4 0 に含まれる関与対象情報 6 4 2 が、出現した時刻の範囲を示す情報である。発生期間情報 6 6 0 は、関与対象情報 6 6 1、開始時刻情報 6 6 2、終了時刻情報 6 6 3 を含む。

発生期間情報 6 6 0 に含まれる関与対象情報 6 6 1 は、発生履歴記憶部 2 2 1 が入力した発生履歴情報 6 4 0 のなかに出現した関与対象情報 6 4 2 である。

発生期間情報 6 6 0 に含まれる開始時刻情報 6 6 2 は、発生履歴記憶部 2 2 1 が入力した発生履歴情報 6 4 0 のなかで、関与対象情報 6 6 1 と同一の関与対象情報 6 4 2 を含む発生履歴情報 6 4 0 に含まれる発生時刻情報 6 4 1 が示す発生時刻のうち、最も早い時刻を示す情報である。

発生期間情報 6 6 0 に含まれる終了時刻情報 6 6 3 は、発生履歴記憶部 2 2 1 が入力した発生履歴情報 6 4 0 のなかで、関与対象情報 6 6 1 と同一の関与対象情報 6 4 2 を含む発生履歴情報 6 4 0 に含まれる発生時刻情報 6 4 1 が示す発生時刻のうち、最も遅い時刻を示す情報である。

40

すなわち、発生履歴記憶部 2 2 1 が入力した発生履歴情報 6 4 0 のうち、開始時刻情報 6 6 2 が示す時刻から終了時刻情報 6 6 3 が示す時刻までの期間に発生した事象を記録した発生履歴情報 6 4 0 のなかに、関与対象情報 6 6 1 が含まれていることを示している。

【0092】

発生期間判断部 2 2 2 は、CPU 9 1 1 などの処理装置を用いて、取得した発生履歴情報 6 4 0 に含まれる関与対象情報 6 4 2 についての発生期間情報 6 6 0 を、発生期間記憶部 2 2 3 が記憶しているか否かを判断する。記憶していない場合には、発生期間記憶部 2

50

23が、CPU911などの処理装置を用いて、新たに発生期間情報660を記憶する。

記憶している場合には、発生期間判断部222が、CPU911などの処理装置を用いて、発生履歴情報640に含まれる発生時刻情報641が示す時刻が、発生期間情報660に含まれる開始時刻情報662と終了時刻情報663とが示す開始時刻から終了時刻までの間に入るか否かを判断する。入らない場合には、発生期間記憶部223が、CPU911などの処理装置を用いて、発生期間情報660を更新する。

【0093】

発生期間通知部224は、CPU911などの処理装置を用いて、発生期間記憶部223が記憶した発生期間情報660を取得する。発生期間通知部224は、CPU911などの処理装置を用いて、取得した発生期間情報660に含まれる関与対象情報661、開始時刻情報662、終了時刻情報663を、管理検索部132が入力する対象情報及び時刻情報として出力する。 10

【0094】

対応期間取得部225は、CPU911などの処理装置を用いて、発生期間通知部224が出力した関与対象情報661・開始時刻情報662・終了時刻情報663に対する応答として、管理検索部132が出力した期間付管理識別情報630を入力する。

【0095】

対応期間記憶部226は、CPU911などの処理装置を用いて、対応期間取得部225が入力した期間付管理識別情報630に含まれる管理識別情報631及び期間情報632と、発生期間通知部224が出力した関与対象情報661とを対応づけて、対応期間情報670として記憶する。 20

対応期間記憶部226が記憶する対応期間情報670は、関与対象情報671、期間情報672、管理識別情報673を含む。

対応期間情報670に含まれる関与対象情報671は、発生期間通知部224が出力した関与対象情報661である。

対応期間情報670に含まれる期間情報672は、発生期間通知部224が出力した関与対象情報661他に対する応答として管理検索部132が出力した期間付管理識別情報630に含まれる期間情報632である。

対応期間情報670に含まれる管理識別情報673は、発生期間通知部224が出力した関与対象情報661他に対する応答として管理検索部132が出力した期間付管理識別情報630に含まれる管理識別情報631である。 30

すなわち、対応期間情報670は、関与対象情報671が、期間情報672が示す期間において、管理識別情報673によって識別される対象を示すことを示す情報である。

対応期間情報670は、管理記憶部131が記憶した管理情報610のなかから、発生履歴記憶部221が入力した発生履歴情報640を加工するのに必要な情報を抜き出したものである。

【0096】

対応判断部227は、CPU911などの処理装置を用いて、発生履歴記憶部221が記憶した発生履歴情報640を取得する。対応判断部227は、CPU911などの処理装置を用いて、対応期間記憶部226が記憶した対応期間情報670に基づいて、発生履歴情報640を加工し、加工済履歴情報650を生成する。対応判断部227は、生成した加工済履歴情報650を出力する。 40

【0097】

図10及び図11は、この実施の形態における履歴加工部122が履歴情報を加工する履歴加工処理の流れの一例を示すフローチャート図である。

【0098】

なお、履歴加工処理の開始前に、初期化処理として、発生履歴記憶部221は、CPU911などの処理装置を用いて、磁気ディスク装置920などの記憶装置に記憶した発生履歴情報640を消去し、発生期間記憶部223は、CPU911などの処理装置を用いて、磁気ディスク装置920などの記憶装置に記憶した発生期間情報660を消去してい 50

るものとする。

初期化処理は、履歴加工処理の開始前ではなく、履歴加工処理の終了後に行い、次の履歴加工処理に備えることとしてもよい。

【0099】

S041（発生履歴入力工程）において、発生履歴記憶部221は、CPU911などの処理装置を用いて、発生履歴情報640を、1つずつ入力する。

S042において、発生履歴記憶部221は、CPU911などの処理装置を用いて、S041で発生履歴情報640を入力したか否かを判断する。

発生履歴情報640を入力したと判断した場合には、S043へ進む。

今回の履歴加工処理で処理すべき発生履歴情報640をすべて入力し終わり、発生履歴情報640を入力しなかった場合には、S055へ進む。 10

【0100】

S043において、発生履歴記憶部221は、CPU911などの処理装置を用いて、S041で入力した発生履歴情報640を、磁気ディスク装置920などの記憶装置に記憶する。

【0101】

S044において、発生期間判断部222は、CPU911などの処理装置を用いて、S043で発生履歴記憶部221が記憶した発生履歴情報640を取得する。発生期間判断部222は、CPU911などの処理装置を用いて、取得した発生履歴情報640から、発生時刻情報641と関与対象情報642とを取得する。 20

【0102】

S045において、発生期間判断部222は、CPU911などの処理装置を用いて、発生期間記憶部223が記憶した発生期間情報660のなかから、S044で取得した発生時刻情報641と同一の関与対象情報661を含む発生期間情報660を取得する。

【0103】

S046において、発生期間判断部222は、CPU911などの処理装置を用いて、S045で発生期間情報660を取得できたか否かを判断する。

S044で取得した発生時刻情報641と同一の関与対象情報661を含む発生期間情報660を発生期間記憶部223が既に記憶していて、S045で発生期間情報660を取得できた場合には、S047へ進む。 30

S044で取得した発生時刻情報641と同一の関与対象情報661を含む発生期間情報660を発生期間記憶部223がまだ記憶しておらず、S045で発生期間情報660を取得できなかった場合には、S051へ進む。

【0104】

S047において、発生期間判断部222は、CPU911などの処理装置を用いて、S045で取得した発生期間情報660に含まれる終了時刻情報663が示す終了時刻と、

S043で取得した発生履歴情報640に含まれる発生時刻情報641が示す発生時刻とを比較して、発生時刻が終了時刻よりも遅いか否かを判断する。

【0105】

S048において、発生期間判断部222は、CPU911などの処理装置を用いて、S047で判断した結果、発生時刻が終了時刻よりも遅いと判断した場合には、S053へ進む。 40

発生時刻が終了時刻以前であると判断した場合には、S049へ進む。

【0106】

S049において、発生期間判断部222は、CPU911などの処理装置を用いて、S045で取得した発生期間情報660に含まれる開始時刻情報662が示す開始時刻と、S043で取得した発生履歴情報640に含まれる発生時刻情報641が示す発生時刻とを比較して、発生時刻が開始時刻よりも早いか否かを判断する。

【0107】

S050において、発生期間判断部222は、CPU911などの処理装置を用いて、 50

S 0 4 9で判断した結果、発生時刻が開始時刻よりも早いと判断したばあいには、S 0 5 4へ進む。

発生時刻が開始時刻以後であると判断した場合には、S 0 4 1に戻る。

【0 1 0 8】

なお、発生履歴記憶部 2 2 1が入力する発生履歴情報 6 4 0が発生時刻の早い順に並んでいる場合には、発生時刻情報 6 4 1が示す発生時刻が、既に発生期間記憶部 2 2 3が記憶している発生期間情報 6 6 0に含まれる開始時刻情報 6 6 2が示す開始時刻よりも早いことはあり得ないので、S 0 4 9及びS 0 5 0の処理は必要ない。

【0 1 0 9】

S 0 5 1において、発生期間記憶部 2 2 3は、C P U 9 1 1などの処理装置を用いて、
S 0 4 3で発生期間判断部 2 2 2が取得した発生履歴情報 6 4 0に含まれる関与対象情報 6 4 2を取得する。発生期間記憶部 2 2 3は、C P U 9 1 1などの処理装置を用いて、取得した関与対象情報 6 4 2を、新たな発生期間情報 6 6 0として、磁気ディスク装置 9 2 0などの記憶装置に記憶する。 10

【0 1 1 0】

S 0 5 2において、発生期間記憶部 2 2 3は、C P U 9 1 1などの処理装置を用いて、
S 0 4 3で発生期間判断部 2 2 2が取得した発生履歴情報 6 4 0に含まれる発生時刻情報 6 4 1を取得する。発生期間記憶部 2 2 3は、C P U 9 1 1などの処理装置を用いて、取得した発生時刻情報 6 4 1が示す時刻を示す情報を、S 0 5 1で記憶した発生期間情報 6 6 0の開始時刻情報 6 6 2として、磁気ディスク装置 9 2 0などの記憶装置に記憶する。 20

【0 1 1 1】

S 0 5 3において、発生期間記憶部 2 2 3は、C P U 9 1 1などの処理装置を用いて、
S 0 4 3で発生期間判断部 2 2 2が取得した発生履歴情報 6 4 0に含まれる発生時刻情報 6 4 1を取得する。発生期間記憶部 2 2 3は、C P U 9 1 1などの処理装置を用いて、取得した発生時刻情報 6 4 1が示す時刻を示す情報を、S 0 5 1で記憶した発生期間情報 6 6 0またはS 0 4 5で取得した発生期間情報 6 6 0の終了時刻情報 6 6 3として、磁気ディスク装置 9 2 0などの記憶装置に記憶する。

その後、S 0 4 1に戻る。

【0 1 1 2】

S 0 5 4において、発生期間記憶部 2 2 3は、C P U 9 1 1などの処理装置を用いて、
S 0 4 3で発生期間判断部 2 2 2が取得した発生履歴情報 6 4 0に含まれる発生時刻情報 6 4 1を取得する。発生期間記憶部 2 2 3は、C P U 9 1 1などの処理装置を用いて、取得した発生時刻情報 6 4 1が示す時刻を示す情報を、S 0 4 5で取得した発生期間情報 6 6 0の開始時刻情報 6 6 2として、磁気ディスク装置 9 2 0などの記憶装置に記憶する。 30

その後、S 0 4 1に戻る。

【0 1 1 3】

図 1 1に移って、履歴加工処理の説明を続ける。

S 0 5 5において、発生期間通知部 2 2 4は、C P U 9 1 1などの処理装置を用いて、発生期間記憶部 2 2 3が記憶した発生期間情報 6 6 0を、1つずつ取得する。

【0 1 1 4】

S 0 5 6において、発生期間通知部 2 2 4は、C P U 9 1 1などの処理装置を用いて、S 0 5 5で発生期間情報 6 6 0を取得できたか否かを判断する。 40

発生期間情報 6 6 0を取得できたと判断した場合には、S 0 5 7へ進む。

発生期間記憶部 2 2 3が記憶した発生期間情報 6 6 0をすべて取得してしまい、これ以上取得できる発生期間情報 6 6 0がないため、発生期間情報 6 6 0を取得できなかった場合には、S 0 6 0へ進む。

【0 1 1 5】

S 0 5 7において、発生期間通知部 2 2 4は、C P U 9 1 1などの処理装置を用いて、S 0 5 6で取得した発生期間情報 6 6 0から、関与対象情報 6 6 1と、開始時刻情報 6 6 2と、終了時刻情報 6 6 3とを取得する。発生期間通知部 2 2 4は、C P U 9 1 1などの 50

処理装置を用いて、取得した関与対象情報 6 6 1、開始時刻情報 6 6 2、終了時刻情報 6 6 3を、管理検索部 1 3 2が入力する対象情報及び時刻情報として、出力する。

【0 1 1 6】

管理検索部 1 3 2はこれを入力して、図 9で説明した管理検索処理をし、期間付管理識別情報 6 3 0を出力する。

【0 1 1 7】

S 0 5 8において、対応期間取得部 2 2 5は、C P U 9 1 1などの処理装置を用いて、管理検索部 1 3 2が出力した期間付管理識別情報 6 3 0を入力する。

【0 1 1 8】

S 0 5 9において、対応期間記憶部 2 2 6は、C P U 9 1 1などの処理装置を用いて、S 0 5 7で発生期間通知部 2 2 4が出力した関与対象情報 6 6 1と、S 0 5 8で対応期間取得部 2 2 5が入力した期間付管理識別情報 6 3 0に含まれる管理識別情報 6 3 1及び期間情報 6 3 2とを対応づけて、対応期間情報 6 7 0を生成し、生成した対応期間情報 6 7 0を磁気ディスク装置 9 2 0などの記憶装置に記憶する。 10

その後、S 0 5 5に戻る。

【0 1 1 9】

S 0 6 0において、対応判断部 2 2 7は、C P U 9 1 1などの処理装置を用いて、S 0 4 1で発生履歴記憶部 2 2 1が記憶した発生履歴情報 6 4 0を、最初から1つつ取得する。

【0 1 2 0】

S 0 6 1において、対応判断部 2 2 7は、C P U 9 1 1などの処理装置を用いて、S 0 6 0で発生履歴情報 6 4 0を取得できたか否かを判断する。 20

発生履歴情報 6 4 0を取得できた場合には、S 0 6 2へ進む。

発生履歴記憶部 2 2 1が記憶した発生履歴情報 6 4 0をすべて取得してしまい、これ以上取得できる発生履歴情報 6 4 0がない場合には、履歴加工処理を終了する。

【0 1 2 1】

S 0 6 2において、対応判断部 2 2 7は、C P U 9 1 1などの処理装置を用いて、S 0 5 9で対応期間記憶部 2 2 6が記憶した対応期間情報 6 7 0のなかから、S 0 6 0で取得した発生履歴情報 6 4 0に対応する対応期間情報 6 7 0を取得する。

すなわち、対応判断部 2 2 7は、C P U 9 1 1などの処理装置を用いて、発生履歴情報 6 4 0に含まれる関与対象情報 6 4 2と、対応期間情報 6 7 0に含まれる関与対象情報 6 7 1とが一致し、かつ、発生履歴情報 6 4 0に含まれる発生時刻情報 6 4 1が示す時刻が、対応期間情報 6 7 0に含まれる期間情報 6 7 2が示す期間内にある対応期間情報 6 7 0を探し、対応期間記憶部 2 2 6から取得する。 30

【0 1 2 2】

S 0 6 3（履歴加工工程）において、対応判断部 2 2 7は、C P U 9 1 1などの処理装置を用いて、S 0 6 1で取得した発生履歴情報 6 4 0に含まれる情報と、S 0 6 2で取得した対応期間情報 6 7 0に含まれる関与対象情報 6 7 1とを含む加工済履歴情報 6 5 0を生成する。対応判断部 2 2 7は、C P U 9 1 1などの処理装置を用いて、生成した加工済履歴情報 6 5 0を出力する。 40

その後、S 0 6 0に戻る。

【0 1 2 3】

なお、S 0 6 2で対応する対応期間情報 6 7 0を取得できなかった場合には、S 0 6 3で対応判断部 2 2 7が、関与対象情報 6 7 1を含む加工済履歴情報 6 5 0の代わりに異常発生情報 6 5 9を含む加工済履歴情報 6 5 0を出力することとしてもよい。その場合、実施の形態 1と同様、警告出力部が、C R Tなどの表示装置 9 0 1やその他の出力装置に異常発生を示す情報を出力する構成としてもよい。

【0 1 2 4】

このように、複数の発生履歴情報 6 4 0がある場合に、そのなかで重複する関与対象情報 6 4 2があるか否かを発生期間判断部 2 2 2が判断し、重複する関与対象情報 6 4 2が 50

ある場合には、それを1つにまとめてから、管理検索部132に対する検索要求を出す。

これにより、管理検索部132が、同一の対象情報について重複する管理検索処理をしないので、処理の量が減り、膨大な発生履歴情報640を速く加工できるようになる。

【0125】

また、ログ管理装置120とID管理装置130とが離れている場合には、ログ管理装置120がID管理装置130に対して管理検索処理を要求し、ID管理装置130がログ管理装置120に対して検索の結果を返す通信にかかる通信コストも無視できない。

このように、重複する関与対象情報642を1つにまとめて検索することにより、ログ管理装置120とID管理装置130との間の通信にかかるコストを削減することができる。

【0126】

この実施の形態における履歴管理装置100は、管理検索部132が、CPU911などの処理装置を用いて、開始時刻を示す情報である開始時刻情報662と、終了時刻を示す情報である終了時刻情報663とを、時刻情報として入力し、CPU911などの処理装置を用いて、管理記憶部131が記憶した管理情報610のなかから、入力した対象情報と、管理情報610に含まれる対象識別情報613とが一致し、かつ、入力した開始時刻情報662によって示される開始時刻から入力した終了時刻情報663によって示される終了時刻までの期間と、管理情報610に含まれる期間情報612によって示される時間との間に重複する期間がある管理情報610を抽出し、CPU911などの処理装置を用いて、抽出した管理情報610に含まれる管理識別情報611と、抽出した管理情報610に含まれる期間情報612とを含む情報である期間付管理識別情報630を出力し、履歴加工部122の発生履歴記憶部221が、CPU911などの処理装置を用いて、発生履歴情報640を複数入力し、履歴加工部122の発生期間判断部222が、CPU911などの処理装置を用いて、入力した発生履歴情報640に含まれる関与対象情報642が互いに一致する発生履歴情報640が複数あるか否かを判断し、履歴加工部122の発生期間通知部224が、CPU911などの処理装置を用いて、関与対象情報642が互いに一致する発生履歴情報640が複数あると判断した場合に、関与対象情報642が互いに一致すると判断した複数の発生履歴情報640に含まれる発生時刻情報641によって示される発生時刻のうち、最も早い発生時刻を示す情報を、管理検索部132が入力する開始時刻情報662として出力し、関与対象情報642が互いに一致すると判断した複数の発生履歴情報640に含まれる発生時刻情報641によって示される発生時刻のうち、最も遅い発生時刻を示す情報を、管理検索部132が入力する終了時刻情報663として出力し、履歴加工部122の対応期間取得部225が、CPU911などの処理装置を用いて、管理検索部132が出力した期間付管理識別情報630を入力し、履歴加工部122の対応判断部227が、CPU911などの処理装置を用いて、入力した発生履歴情報640に含まれる情報と、入力した期間付管理識別情報630のうち、発生履歴情報640に含まれる発生時刻情報641によって示される発生時刻が期間付管理識別情報630に含まれる期間情報によって示される期間内である期間付管理識別情報630に含まれる管理識別情報631とを含む加工済履歴情報650を出力することを特徴とする。

【0127】

この実施の形態における履歴管理装置100によれば、履歴加工部122が、入力した発生履歴情報640に含まれる関与対象情報642が互いに一致する発生履歴情報640が複数ある場合に、それを一つにまとめて、管理検索部132に対して検索要求をするので、管理検索部132に対する検索要求の回数が少なくて済む。これにより、管理検索部132の処理によるCPU911などの処理装置の計算量が少なくなるという効果を奏する。

【0128】

また、管理検索部132と履歴加工部122との間の通信量が減るので、通信コストを抑えることができるという効果を奏する。例えば、本社にID管理装置130を設置して、管理情報610を集中管理し、各地にある支社にログ管理装置120を設置して、履歴

10

20

30

40

50

情報を管理する（履歴情報はその量が膨大なので、本社で集中管理するよりも各支社で管理するほうが通信コストが抑えられる）場合などに、通信コストを抑えることができるという効果を奏する。

【0129】

上述したように、履歴管理装置100は、物理的に一つの装置である必要はなく、一または複数の機能ブロックを実現する装置がインターネットや専用回線などにより接続して互いに情報をやり取りすることにより、全体が履歴管理装置100として機能するように構成してもよい。

【0130】

また、管理検索部132の処理量が減るので、1つのID管理装置130に対して、ログ管理装置120が多数存在する場合には、処理の分散が図れる。これにより、全体としての処理速度が速くなるという効果を奏する。例えば、上述したような本社にID管理装置130を設置して、各地の支社にログ管理装置120を設置する場合などに、効果を奏する。

【0131】

この実施の形態におけるログ加工装置（履歴管理装置100）は、統合ID照会時に、ログレコード（発生履歴情報640）ごとに照会するのではなく、複数のログレコードの固まりを一つの照会単位とし、個別IDと、そのログ内で個別IDが現れる時間範囲で照会することの特徴とする。

【0132】

実施の形態3.

実施の形態3について、図12～図21を用いて説明する。

この実施の形態では、上述した履歴管理装置100の具体的な応用例について説明する。

【0133】

図12は、この実施の形態におけるログ加工装置110の構成の一例を示すブロック図である。

図12において、ログ加工装置110は、ログ管理装置120、及びID管理装置130を有する。

また、管理端末装置140は、ログ加工装置110からは独立した装置である。管理端末装置140は、主にログの検索表示を行うための装置である。

なお、ログ管理装置120、ID管理装置130、管理端末装置140の外観及びハードウェア資源の構成は、実施の形態1で説明したものと同様なので、ここでは説明を省略する。

【0134】

ログ管理装置120は、ログ収集部321、統合ID照会部322、ログ蓄積部323、ログ検索部324、及びログデータベース記憶装置325（以下「ログDB」という）を有する。

ログ収集部321は、CPU911などの処理装置を用いて、ログ管理装置120とLAN942などのネットワークを介して接続された各種端末装置、機器などからログを収集する。ログ収集部321は、履歴収集部の一例である。

ログとは、機器の操作・動作などを記録した情報である。ログは、機器あるいは機器の動作等を監視する監視装置などが生成する。ログは、機器の1つの動作等を記録したログレコードの集合である。ログは、動作等が発生するたびにログレコードが追加されていくので、ログレコードは発生時刻順に並んでいる。ログレコードには、発生時刻、機器の識別子、操作者の識別子などの情報が記録されている。ログレコードは、発生履歴情報の一例である。

【0135】

例えば、利用者が機器を操作した場合に、機器を操作した利用者や操作された機器を識別する情報、機器を操作した時刻を示す情報、操作内容や操作結果を示す情報などを含む

情報がログレコードとして、ログに追加される。

【0136】

統合ID照会部322は、CPU911などの処理装置を用いて、ログ収集部321が収集したログの各ログレコードから、個別ユーザID及び個別機器IDを抽出する。

統合ID照会部322は、CPU911などの処理装置を用いて、ID管理装置130と連携し、各々統合ユーザID、統合機器IDを照会して、照会結果をログレコードに反映する。

【0137】

個別ユーザIDとは、その操作を行った利用者を示す識別子である。例えば、コンピュータにログオンするためのユーザ名、電子メールを送信するためのメールアドレスなどである。個別ユーザIDは、対象識別情報の一例である。また、ログレコードに含まれる個別ユーザIDは、事象の発生に関与した対象を示す関与対象情報の一例であり、機器を操作した利用者を示す操作者情報の一例である。 10

個別機器IDとは、その操作の対象である機器を示す識別子である。例えば、コンピュータをネットワーク上で識別するためのマシン名、IPアドレスなどである。個別機器IDは、対象識別情報の一例である。また、ログレコードに含まれる個別機器IDは、事象の発生に関与した対象を示す関与対象情報の一例であり、操作された機器を示す情報である操作機器情報の一例である。

【0138】

図13は、この実施の形態におけるログ収集部321が収集するログ704の一例を示す図である。 20

ログ704は、複数のログレコード740を有する。この例では、ログ704は、テキスト形式の情報であり、ログ704の1行が、1つのログレコード740である。

ログレコード740には、ログレコードが記録された日付時刻741（この例では“2006/03/28 10:01:47”）、ログに固有の個別ユーザID742（この例では“yamada”）、ログに固有の個別機器ID743（この例では“host001”）が記録されている。

【0139】

日付時刻741は、ログレコードが記録された時刻を示す情報である。日付時刻741は、発生時刻情報の一例である。また、ログレコードが機器の操作を記録したものである場合、日付時刻741は操作時刻情報の一例である。 30

ログ704において、ログレコード740は発生順に追加されていくので、日付時刻741が示す時刻が早い順に並んでいる。

なお、ログ704は、この例のようなCSV（Comma Separated Values）形式のテキストデータである必要はなく、他の形式で表わされた情報であってもよい。

【0140】

図14は、この実施の形態における統合ID照会部322が加工して、統合IDを反映した加工済ログ705の一例を示す図である。

加工済ログ705は、統合ID（統合ユーザID、統合機器IDなど）を反映したログである。 40

統合ID照会部322は、CPU911などの処理装置を用いて、ログ704を加工し、加工済ログ705を生成する。

加工済ログ705には、ログ704のログレコード740に対応するログレコード750が記録される。ログレコード750は、加工済履歴情報の一例である。

【0141】

ログレコード750は、日付時刻751、個別ユーザID752、個別機器ID753、統合ユーザID754、統合機器ID755を含む。

日付時刻751、個別ユーザID752、個別機器ID753は、ログ704のログレコード740に含まれていた日付時刻741、個別ユーザID742、個別機器ID74 50

3 と同一の情報である。

【0142】

統合ユーザ I D 7 5 4 (この例では“ U S E R 1 2 3 4 5 6 ”) は、ユーザを一意に特定する識別子である。

個別ユーザ I D 7 5 2 は、ログ 7 0 4 を生成した機器などにより、異なる個別ユーザ I D 7 5 2 が、同一のユーザを示す場合がある。例えば、あるログ 7 0 4 には、個別ユーザ I D 7 5 2 としてユーザ名が記録され、別のログ 7 0 4 には、個別ユーザ I D 7 5 2 としてメールアドレスが記録されている。

これに対して、統合ユーザ I D 7 5 4 は、一人のユーザに対して 1 つしかない。したがって、統合ユーザ I D 7 5 4 が異なればユーザが異なり、ユーザが異なれば統合ユーザ I D 7 5 4 も異なる。 10

【0143】

また、個別ユーザ I D 7 5 2 は、メールアドレスの変更などにより変わる可能性があるが、統合ユーザ I D 7 5 4 は、一度設定したら変更しない。したがって、例えば、過去何年にも渡るログを検索するような場合、同じ個別ユーザ I D 7 5 2 が異なるユーザを示している可能性もあるが、統合ユーザ I D 7 5 4 が同じなら、それは必ず同一人物を示している。

【0144】

統合機器 I D 7 5 5 (この例では“ A S S E T 9 8 7 6 5 4 ”) は、機器を一意に特定する識別子である。個別機器 I D 7 5 3 と異なり、統合機器 I D 7 5 5 が同一なら必ず同じ機器を示し、統合機器 I D 7 5 5 が異なれば必ず異なる機器を示す。 20

【0145】

このように、統合ユーザ I D 7 5 4 や統合機器 I D 7 5 5 などの統合 I D は、対象を一意に特定する。したがって、過去何年にも渡る膨大な量のログを解析しなければならない場合であっても、統合 I D を使えば、比較的楽に検索することができる。

【0146】

統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、このように、ログ 7 0 4 に、統合 I D を付加して、加工済ログ 7 0 5 を生成する。

【0147】

統合 I D 照会部 3 2 2 は、以上のようなログの加工を行った後、生成した加工済ログ 7 0 5 を出力する。 30

ログ蓄積部 3 2 3 は、C P U 9 1 1 などの処理装置を用いて、統合 I D 照会部 3 2 2 が出力した加工後の加工済ログ 7 0 5 を、ログ D B 3 2 5 に蓄積する。ログ蓄積部 3 2 3 は、履歴蓄積部の一例である。

ログ D B 3 2 5 は、磁気ディスク装置 9 2 0 などの記憶装置である。ログ D B 3 2 5 は、例えば、一般の R D B (リレーショナル・データベース) などのデータ構造を有するデータとして、加工済ログ 7 0 5 を記憶する。

ログ検索部 3 2 4 は、C P U 9 1 1 などの処理装置を用いて、管理端末装置 1 4 0 からのログ検索要求を入力し、ログの検索を行う。ログ検索部 3 2 4 は、例えば、S Q L 文などによるログ検索要求にしたがって、データの検索取り出しを行う。ログ検索部 3 2 4 は 40

、C P U 9 1 1 などの処理装置を用いて、検索の結果を管理端末装置 1 4 0 に返す。ログ検索部 3 2 4 は、履歴検索部の一例である。

【0148】

I D 管理装置 1 3 0 は、統合 I D 取得部 3 3 1、統合 I D 属性情報取得部 3 3 2、I D 管理データベース記憶装置 3 3 3 (以下「I D 管理 D B」という) を有する。

統合 I D 取得部 3 3 1 は、C P U 9 1 1 などの処理装置を用いて、ログ管理装置 1 2 0 の統合 I D 照会部 3 2 2 からの要求を入力する。統合 I D 取得部 3 3 1 は、C P U 9 1 1 などの処理装置を用いて、入力した要求に応じて、I D 管理 D B 3 3 3 を検索し、ユーザを一意に特定する統合ユーザ I D 7 5 4 または機器を一意に特定する統合機器 I D 7 5 5 50

などの統合IDを取得する。統合ID取得部331は、CPU911などの処理装置を用いて、取得した統合IDを、ログ管理装置120の統合ID照会部322に返す。

【0149】

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、管理端末装置140からの要求を入力する。統合ID属性情報取得部332は、CPU911などの処理装置を用いて、入力した要求に応じて、ID管理DB333を検索し、統合IDに付随する属性情報を取得する。

属性情報は、例えば、統合ユーザIDに付随する属性情報であれば、氏名、所属名、役職などを示す情報である。あるいは、統合機器IDに付随する属性情報であれば、機器種別、設置場所名、管理者名などを示す情報である。

統合ID属性情報取得部332は、ID管理DB333から取得した属性情報を、管理端末装置140に返す。

【0150】

管理端末装置140は、統合ID属性情報照会部341、ログ検索表示部342を有する。

統合ID属性情報照会部341は、CPU911などの処理装置を用いて、キーボード902などの入力装置から入力した統合IDをキーにして、統合IDに付随する属性情報を照会する要求を生成し、ID管理装置130に発行する。検索条件入力部141は、CPU911などの処理装置を用いて、ID管理装置130が返した属性情報を取得する。

ログ検索表示部342は、CPU911などの処理装置を用いて、キーボード902などの入力装置から入力した検索条件に基づいて、ログDB325が記憶した加工済ログ705を検索するログ検索条件を生成し、ログ管理装置120のログ検索部324に発行する。ログ検索表示部342は、CPU911などの処理装置を用いて、ログ検索部324が返した検索結果を受信する。

ログ検索表示部342は、また、CPU911などの処理装置を用いて、ログ検索部324から入力した加工済ログ705に含まれる統合IDを取得する。ログ検索表示部342は、CPU911などの処理装置を用いて、取得した統合IDを、統合ID属性情報照会部341に通知する。統合ID属性情報照会部341が通知された統合IDに基づいて、統合ID属性情報取得部332にID管理DB333の検索を要求し、統合ID属性情報取得部332が返した属性情報を、統合ID属性情報照会部341から取得する。

ログ検索表示部342は、ログ検索部324が返した検索結果や、統合ID属性情報照会部341から取得した属性情報を、CRTなどの表示装置901やその他の出力装置に表示・出力する。

【0151】

次に、ID管理DB333が記憶する情報のデータ構造について説明する。

ID管理DB333は、磁気ディスク装置920などの記憶装置である。ID管理DB333は、個別ユーザID・個別機器IDなどの個別ID、統合ユーザID・統合機器IDなどの統合ID、及び統合IDに付随する属性情報を、時間情報とともに保持するデータベースを記憶する。

【0152】

ID管理DB333は、個別IDデータベース701及び属性データベース702を記憶する。

【0153】

個別IDデータベース701は、統合IDと個別IDとの間の関係を示す管理情報710を登録したデータベースである。

属性データベース702は、統合IDと属性との間の関係を示す管理属性情報720を登録したデータベースである。

【0154】

図15は、この実施の形態におけるID管理DB333が記憶する属性データベース702の内容の一例を示す図である。

10

20

30

40

50

属性データベース702は、例えば、種別721、属性722、統合ID723、開始時刻724、終了時刻725などのフィールドを有する。管理属性情報720は、属性データベース702の1つのレコードであり、属性データベース702は複数の管理属性情報720の集合である。

種別721は、属性の種類を示す情報である。属性722は、属性の内容を示す情報である。統合ID723は、その属性を有する対象の統合IDを示す情報である。開始時刻724は、その対象がその属性を有する期間の開始時刻を示す情報である。終了時刻725は、その対象がその属性を有する期間の終了時刻を示す情報である。

この例において、終了時刻725が「9999/12/31 23:59:59」となっているのは、現在もその期間が終了していないことを示している。なお、その期間が終了する時刻があらかじめわかっている場合には、未来の時刻を終了時刻725として記憶しておいてもよい。

10

【0155】

この例では、統合ID（統合機器ID）「ASSET987654」を付与された機器は、PCサーバであり、1997年4月1日に購入されている。このPCサーバは、1棟6階に設置され、管理者は佐藤一郎である。

2003年4月1日に、このPCサーバは、2棟8階に移動している。同時に、管理者が田中二郎に変更されている。

また、統合ID（統合ユーザID）「USER123456」を付与された従業員は、「山口花子」さんであり、1998年4月1日に入社している。人事部に配属され、役職は担当である。

20

2003年6月16日に人事異動があり、山口花子さんは経理部に移ったが、役職は担当のままである。

また、2004年10月16日に山口花子さんは結婚して、苗字が「鈴木」になっている。

【0156】

なお、この例では、管理属性情報720が開始時刻724の順に並んでいるが、統合ID723ごとに並んでいてもよい。また、統合ユーザIDについての管理属性情報720と、統合機器IDについての管理属性情報720とを別のファイルにするなど分離して管理してもよい。あるいは、属性の種類ごとに別のファイルにするなど分離して管理してもよい。

30

また、氏名、所属、役職はユーザの属性の一例であり、管理者、設置場所、機器種別は機器の属性の一例であって、メールアドレス、電話番号、内線番号、資格、従業者タイプ、機器説明、機器接続ネットワーク（イントラネット、非武装地帯（Demilitarized Zone。以下「DMZ」という）などの区別）など、他の属性でもよい。

【0157】

図16は、この実施の形態におけるID管理DB333が記憶する個別IDデータベース701の内容の一例を示す図である。

個別IDデータベース701は、例えば、種別711、個別ID712、統合ID713、開始時刻714、終了時刻715などのフィールドを有する。管理情報710は、個別IDデータベース701の1つのレコードであり、個別IDデータベース701は複数の管理情報710の集合である。

40

種別711は、個別IDの種類を示す情報である。個別ID712は、個別IDの値を示す情報である。統合ID713は、その個別IDが示す対象の統合IDを示す情報である。開始時刻714は、その個別IDがその対象を示す期間の開始時刻を示す情報である。終了時刻715は、その個別IDがその対象を示す期間の終了時刻を示す情報である。

この例において、終了時刻715が「9999/12/31 23:59:59」となっているのは、現在もその期間が終了していないことを示している。すなわち、その個別IDが現在有効であることを示している。なお、その期間が終了する時刻があらかじめわかっている場合には、未来の時刻を終了時刻715として記憶しておいてもよい。

50

【0158】

この例では、統合ID「ASSET987654」のPCサーバは、1997年4月1日の導入時には、マシン名が「shogun」、IPアドレスが「192.168.1.100」となっている。

2003年4月1日に、このPCサーバを移動したことに伴い、マシン名が「posideon」に、IPアドレスが「192.168.1.105」に変更されている。

また、2005年4月16日には、社内LANの再構築があり、IPアドレスが「192.168.1.120」に変更されている。

また、統合ID「USER123456」の鈴木（旧姓山口）花子さんは、1998年4月1日の入社時に、OSログオンID「yamaguchi」、アプリケーションAのユーザIDとして「0006」、電子メールアドレスをユーザIDとするアプリケーションB（例えば、電子メールソフトなど）のユーザID（すなわち、電子メールアドレス）として「hanako@domain.co.jp」をもらっている。

2000年10月16日に、アプリケーションAのユーザIDが「0106」に変更されている。また、2004年10月16日に苗字が変わったので、OSログオンIDも「suzuki」に変更されている。

2005年3月16日には、全社的なメールアドレス体系の変更があり、電子メールアドレスが「Suzuki.Hanako@domain.co.jp」になっている。また、2005年4月16日には、再びアプリケーションAのユーザIDが変更され、「10000106」になっている。

【0159】

なお、この例では、管理情報710が開始時刻714の順に並んでいるが、統合ID713ごとに並んでいてもよい。また、統合ユーザIDについての管理情報710と、統合機器IDについての管理情報710とを別のファイルにするなど分離して管理してもよい。あるいは、個別IDの種類ごとに別のファイルにするなど分離して管理してもよい。

また、OSログオンID、アプリケーションAユーザID、アプリケーションBユーザIDは個別ユーザIDの一例であり、マシン名、IPアドレスは個別機器IDの一例であって、他の個別IDでもよい。

【0160】

図17は、この実施の形態におけるID管理DB333が記憶した個別IDデータベース701及び属性データベース702によって示される統合IDと個別ID、属性との間の関係を視覚的に表現した概念図である。

【0161】

このように、OSログオンID、アプリケーションAユーザID、アプリケーションBユーザIDなどの個別IDと、氏名、所属、役職などの属性とが、1つの統合ユーザID「USER123456」によって紐付けされ、これらすべての情報が一人の従業員のものであることを示している。

同様に、マシン名、IPアドレスなどの個別IDと、管理者、設置場所、機器種別などの属性とが、1つの統合機器ID「ASSET987654」によって紐付けされ、これらすべての情報が一台の機器のものであることを示している。

【0162】

また、個別IDや属性は変更される場合があるが、統合IDは変更しないので、過去のログを検索する場合、統合IDを利用すれば、探したい従業員や機器についてのログを素早く見つけることができる。

【0163】

次に、動作の詳細について説明する。

図18は、この実施の形態におけるログ加工装置110がログ704を加工するログ加工処理の流れの一例を示すフローチャート図である。

【0164】

S071において、ログ収集部321は、CPU911などの処理装置を用いて、ログ

10

20

30

40

50

704を収集する。

ログ収集部321は、CPU911などの処理装置を用いて、収集したログ704を出力する。

【0165】

S072（発生履歴入力工程）において、統合ID照会部322は、CPU911などの処理装置を用いて、S071でログ収集部321が出力したログ704を入力する。

統合ID照会部322は、CPU911などの処理装置を用いて、入力したログ704に基づいて、統合ID照会データ706を生成する。

統合ID照会部322は、CPU911などの処理装置を用いて、生成した統合ID照会データ706を出力する。

10

【0166】

S073（管理情報抽出工程）において、統合ID取得部331は、CPU911などの処理装置を用いて、S072で統合ID照会部322が出力した統合ID照会データ706を入力する。

統合ID取得部331は、CPU911などの処理装置を用いて、入力した統合ID照会データ706に基づいて、ID管理DB333を検索する。

統合ID取得部331は、CPU911などの処理装置を用いて、ID管理DB333を検索した結果に基づいて、統合ID照会結果707を生成する。

統合ID取得部331は、CPU911などの処理装置を用いて、生成した統合ID照会結果707を出力する。

20

【0167】

S074（履歴加工工程）において、統合ID照会部322は、CPU911などの処理装置を用いて、S073で統合ID取得部331が出力した統合ID照会結果707を入力する。

統合ID照会部322は、CPU911などの処理装置を用いて、入力した統合ID照会結果707に基づいて、ログ704を加工し、加工済ログ705を生成する。

統合ID照会部322は、CPU911などの処理装置を用いて、生成した加工済ログ705を出力する。

【0168】

S075において、ログ蓄積部323は、CPU911などの処理装置を用いて、S074で統合ID照会部322が出力した加工済ログ705を入力する。

30

ログ蓄積部323は、CPU911などの処理装置を用いて、入力した加工済ログ705を、ログDB325に蓄積する。

【0169】

図19は、この実施の形態におけるログ管理装置120の各機能ブロックの間でやり取りする情報の一例を示す図である。

【0170】

ログ704は、ログ収集部321が収集し、統合ID照会部322に通知する。

ログ704は、図13を用いて説明したように、例えば、日付時刻741、個別機器ID743などを有するログレコード740の集合である。

40

図19に一例として示したログ704には、2003年3月31日11時24分32秒に記録されたログレコード740に個別機器ID743として「shogun」が記録されている。また、2003年3月31日12時12分47秒に記録されたログレコード740には、個別機器ID743として「poseidon」が記録されている。

【0171】

統合ID照会データ706は、統合ID照会部322がログ704に基づいて生成し、統合ID取得部331に送信する。

統合ID照会データ706は、照会条件の集合であり、それぞれの照会条件は、個別ID761、開始時刻762、終了時刻763を有する。

個別ID761は、個別ユーザIDや個別機器IDなどの個別IDを示す情報であり、

50

照会の対象である個別IDを示す。個別ID 761は、対象情報の一例である。

開始時刻762と終了時刻763とは、個別ID 761を照会する期間を示す情報である。開始時刻762と終了時刻763とは、時刻情報の一例である。

開始時刻762は、個別ID 761を照会する期間の開始時刻を示す情報である。

終了時刻763は、個別ID 761を照会する期間の終了時刻を示す情報である。

【0172】

図19に一例として示した統合ID照会データ706は、個別ID「shogun」について2003年3月31日11時24分32秒から2003年4月1日13時52分23秒までの期間で照会する照会条件と、個別ID「poseidon」について2003年3月31日12時12分47秒から2003年4月1日8時6分11秒までの期間で照会する照会条件との2つの照会条件を含んでいる。 10

【0173】

統合ID照会結果707は、統合ID取得部331が統合ID照会データ706に基づいてID管理DB333を検索した結果に基づいて生成し、統合ID照会部322に送信するものである。

統合ID照会結果707は、照会結果の集合であり、それぞれの照会結果は、個別ID 771、開始時刻772、終了時刻773、統合ID 774を有する。

個別ID 771は、個別ユーザID 742や個別機器ID 743などの個別IDを示す情報であり、統合ID照会データ706によって照会された個別IDを示す。

開始時刻772と終了時刻773とは、照会された個別ID 771が、統合ID 774によって識別される対象を示す期間を示す情報である。開始時刻772と終了時刻773とは、期間情報の一例である。 20

統合ID 774は、統合ユーザIDや統合機器IDなどの統合IDを示す情報であり、照会された個別ID 771が示す対象を識別する統合IDを示す。統合ID 774は、管理識別情報の一例である。

【0174】

図19に一例として示した統合ID照会結果707は、個別ID「shogun」が2003年3月31日11時24分32秒から2003年3月31日23時59分59秒までの期間において示す対象は、統合ID「ASSET987654」によって識別される対象であるという照会結果と、個別ID「poseidon」が2003年3月31日12時12分47秒から2003年3月31日23時59分59秒までの期間において示す対象は、統合ID「ASSET123456」によって識別される対象であるという照会結果と、個別ID「poseidon」が2003年4月1日0時0分0秒から2003年4月1日8時6分11秒までの期間において示す対象は、統合ID「ASSET987654」によって識別される対象であるという照会結果との3つの照会結果を含んでいる。 30

この照会結果は、統合機器ID「ASSET987654」によって識別されるPCサーバが、2003年3月31日までは「shogun」と呼ばれていたが、2003年4月1日から「poseidon」と呼ばれるようになったことを示している。

また、2003年3月31日まで「poseidon」と呼ばれていた機器は別にあり、その機器の統合機器IDは「ASSET123456」である。 40

また、「shogun」についての照会期間が2003年4月1日13時52分23秒までなのに、「shogun」についての照会結果が2003年3月31日23時59分59秒までしかないので、2003年4月1日以降は「shogun」と呼ばれる機器が存在しないことがわかる。

【0175】

加工済ログ705は、統合ID照会部322がログ704と統合ID照会結果707とに基づいて生成し、ログ蓄積部323に通知するものである。

加工済ログ705は、図14を用いて説明したように、例えば、日付時刻751、個別機器ID 753、統合機器ID 755などを有するログレコード750の集合である。 50

図 19 に一例として示した加工済ログ 705 は、ログ収集部 321 が収集したログ 704 に、統合機器 ID 755 や異常発生情報 759 などを追加した内容となっている。

【0176】

次に、図 18 の S072 における統合 ID 照会部 322 の動作について、更に詳しく説明する。

図 20 は、この実施の形態における統合 ID 照会部 322 が統合 ID 照会データ 706 を生成する統合 ID 照会データ生成処理の流れの一例を示すフローチャート図である。

【0177】

S081 において、統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、複数のログレコード 740 を含むログ 704 を入力する。

10

統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、入力したログ 704 を磁気ディスク装置 920 などの記憶装置に記憶する。

【0178】

S082 において、統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、S081 で入力したログ 704 の先頭から、ログレコード 740 を 1 行ずつ読み込む。

ログレコード 740 は、発生時刻順に並んでいるので、統合 ID 照会部 322 は、ログレコード 740 を古いものから順に読み込む。

【0179】

S083a において、統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、S082 で読み込んだログレコード 740 を解析し、個別ユーザ ID 742 と日付時刻 741 とを取得する。

20

統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、取得した個別ユーザ ID 742 と日付時刻 741 とを RAM 914 などの記憶装置に一時記憶する。

【0180】

S084a において、統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、既に生成した統合 ID 照会データ 706 の照会条件のなかに、S083a で取得した個別ユーザ ID 742 が記録されているか否かを判断する。

記録されていないと判断した場合には、S085a へ進む。

記録されていると判断した場合には、S086a へ進む。

【0181】

30

S085a において、統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、統合 ID 照会データ 706 に照会条件を追加し、個別 ID 761 として、S083a で取得した個別ユーザ ID 742 を記録する。

統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、追加した照会条件の開始時刻 762 として、S083a で取得した日付時刻 741 を設定する。

【0182】

S086a において、統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、統合 ID 照会データ 706 に記録された照会条件の終了時刻 763 として、S083a で取得した日付時刻 741 を設定する。

【0183】

40

S083b において、統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、S082 で読み込んだログレコード 740 を解析し、個別機器 ID 743 を取得する。

統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、取得した個別機器 ID 743 を RAM 914 などの記憶装置に一時記憶する。

【0184】

S084b において、統合 ID 照会部 322 は、CPU 911 などの処理装置を用いて、既に生成した統合 ID 照会データ 706 の照会条件のなかに、S083b で取得した個別機器 ID 743 が記録されているか否かを判断する。

記録されていないと判断した場合には、S085b へ進む。

記録されていると判断した場合には、S086b へ進む。

50

【0185】

S085bにおいて、統合ID照会部322は、CPU911などの処理装置を用いて、統合ID照会データ706に照会条件を追加し、個別ID761として、S083bで取得した個別機器ID743を記録する。

統合ID照会部322は、CPU911などの処理装置を用いて、追加した照会条件の開始時刻762として、S083aで取得した日付時刻741を設定する。

【0186】

S086bにおいて、統合ID照会部322は、CPU911などの処理装置を用いて、統合ID照会データ706に記録された照会条件の終了時刻763として、S083aで取得した日付時刻741を設定する。

10

【0187】

このように、S083b～S086bの処理は、S083a～S086aの処理とほとんど同じであり、処理の対象となる個別IDが、個別ユーザIDではなく、個別機器IDである点が異なる。

個別ユーザID、個別機器ID以外の個別IDがある場合には、同様に、それぞれの個別IDに対する処理をする。

あるいは、個別IDの種類を区別せず、1回の処理で、1つのログレコード740に含まれるすべての個別IDについて処理してもよい。

【0188】

S087において、統合ID照会部322は、S081で入力したログ704のなかに、S082でまだ取得していないログレコード740があるか否かを判断する。

20

取得していないログレコード740があると判断した場合には、S082に戻る。

すべてのログレコード740を取得したと判断した場合には、統合ID照会データ生成処理を終了する。

【0189】

このようにして生成した統合ID照会データ706は、統合ID照会部322が送信し、統合ID取得部331が受信する。統合ID照会部322は、受信した統合ID照会データ706に基づいてID管理DB333を検索し、検索結果から統合ID照会結果707を生成する。統合ID照会結果707は、統合ID取得部331が送信し、統合ID照会部322が受信する。

30

【0190】

これにより、統合ID照会部322と統合ID取得部331との間でやり取りされる通信が1回の往復で済むので、通信コストが抑えられる。

【0191】

次に、図18のS074における統合ID照会部322の動作について、更に詳しく説明する。

図21は、この実施の形態における統合ID照会部322が統合ID照会結果707に基づいてログ704を加工し、加工済ログ705を生成する統合ID照会結果反映処理の流れの一例を示すフローチャート図である。

【0192】

40

S091において、統合ID照会部322は、CPU911などの処理装置を用いて、複数のログレコード740を含むログ704を入力する。

統合ID照会部322は、CPU911などの処理装置を用いて、入力したログ704を磁気ディスク装置920などの記憶装置に記憶する。

なお、S091で統合ID照会部322が入力するログ704は、図20のS081で入力したログ704と同じものである。したがって、S081で入力したログ704を再利用する場合には、S091の処理はなくてもよい。

【0193】

S092において、統合ID照会部322は、CPU911などの処理装置を用いて、統合ID取得部331が出力した統合ID照会結果707を入力する。

50

【0194】

S093において、統合ID照会部322は、CPU911などの処理装置を用いて、S091で入力したログ704の先頭から、ログレコード740を1行ずつ読み込む。

統合ID照会部322は、CPU911などの処理装置を用いて、読み込んだログレコード740を解析して、日付時刻741と個別ユーザID742と個別機器ID743とを取得する。

統合ID照会部322は、CPU911などの処理装置を用いて、取得した日付時刻741と個別ユーザID742と個別機器ID743とを、RAM914などの記憶装置に記憶する。

【0195】

10

S094aにおいて、統合ID照会部322は、CPU911などの処理装置を用いて、S093で取得した個別ユーザID742についての照会結果を、S092で入力した統合ID照会結果707から取得する。

個別ユーザID742についての照会結果を取得できた場合には、S095aへ進む。

個別ユーザID742についての照会結果を取得できなかった場合には、S097aへ進む。

【0196】

S095aにおいて、統合ID照会部322は、CPU911などの処理装置を用いて、S094aで取得した照会結果を解析して、開始時刻772と終了時刻773とを取得する。

20

統合ID照会部322は、CPU911などの処理装置を用いて、S093で取得した日付時刻741が、取得した開始時刻772から終了時刻773までの期間内であるか否かを判断する。

日付時刻741が開始時刻772から終了時刻773の期間内であると判断した場合には、S096aへ進む。

日付時刻741が開始時刻772から終了時刻773の期間外であると判断した場合には、S094aに戻り、他の照会結果を取得する。

【0197】

S096aにおいて、統合ID照会部322は、CPU911などの処理装置を用いて、S094aで取得した照会結果を解析して、統合ID774を取得する。

30

統合ID照会部322は、CPU911などの処理装置を用いて、S093で取得したログレコード740に、取得した統合ID774を追加して、ログレコード750を生成する。

統合ID照会部322は、CPU911などの処理装置を用いて、生成したログレコード750を、磁気ディスク装置920などの記憶装置に記憶する。

その後、S094bへ進む。

【0198】

S097aにおいて、統合ID照会部322は、CPU911などの処理装置を用いて、S093で取得したログレコード740に、異常発生情報759を追加して、ログレコード750を生成する。

40

統合ID照会部322は、CPU911などの処理装置を用いて、生成したログレコード750を、磁気ディスク装置920などの記憶装置に記憶する。

【0199】

S094bにおいて、統合ID照会部322は、CPU911などの処理装置を用いて、S093で取得した個別機器ID743についての照会結果を、S092で入力した統合ID照会結果707から取得する。

個別機器ID743についての照会結果を取得できた場合には、S095bへ進む。

個別機器ID743についての照会結果を取得できなかった場合には、S097bへ進む。

【0200】

50

S 0 9 5 bにおいて、統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 9 4 b で取得した照会結果を解析して、開始時刻 7 7 2 と終了時刻 7 7 3 とを取得する。

統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 9 3 で取得した日付時刻 7 4 1 が、取得した開始時刻 7 7 2 から終了時刻 7 7 3 の期間内であるか否かを判断する。

日付時刻 7 4 1 が開始時刻 7 7 2 から終了時刻 7 7 3 の期間内であると判断した場合には、S 0 9 6 b へ進む。

日付時刻 7 4 1 が開始時刻 7 7 2 から終了時刻 7 7 3 の期間外であると判断した場合には、S 0 9 4 b へ戻り、他の照会結果を取得する。

10

【0 2 0 1】

S 0 9 6 b において、統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 9 4 b で取得した照会結果を解析して、統合 I D 7 7 4 を取得する。

統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 9 6 a または S 0 9 7 a で生成したログレコード 7 5 0 に、取得した統合 I D 7 7 4 を追加して、新たなログレコード 7 5 0 を生成する。

統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、生成したログレコード 7 5 0 を出力する。

その後、S 0 9 8 へ進む。

【0 2 0 2】

20

S 0 9 7 b において、統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 9 6 a または S 0 9 7 a で生成したログレコード 7 5 0 に、異常発生情報 7 5 9 を追加して、新たなログレコード 7 5 0 を生成する。

統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、生成したログレコード 7 5 0 を出力する。

【0 2 0 3】

S 0 9 8 において、統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、S 0 9 3 で読み込むべきログレコード 7 4 0 がまだあるか否かを判断する。

次のログレコード 7 4 0 があると判断した場合には、S 0 9 3 に戻る。

最後のログレコード 7 4 0 まで処理が終わり、次のログレコード 7 4 0 がないと判断した場合には、統合 I D 照会結果反映処理を終了する。

30

【0 2 0 4】

なお、S 0 9 4 a 及び S 0 9 4 b において、統合 I D 照会部 3 2 2 が、個別ユーザ I D 7 4 2 または個別機器 I D 7 4 3 についての照会結果をすべて、統合 I D 照会結果 7 0 7 から取得し、取得した照会結果が 1 つしかない場合は、期間内であるか否かの判断をせず、S 0 9 6 a または S 0 9 6 b の処理をすることとしてもよい。

取得した照会結果が複数ある場合には、統合 I D 照会部 3 2 2 が、日付時刻 7 4 1 に基づいて、どの照会結果に該当するか判断し、S 0 9 6 a または S 0 9 6 b の処理へ進む。

【0 2 0 5】

その場合、統合 I D 取得部 3 3 1 は、照会された個別 I D 7 6 1 に対応する統合 I D 7 7 4 がない期間があれば、その期間について、対応する統合 I D 7 7 4 がないことを示す照会結果を返す構成とする。そうすれば、対応する統合 I D 7 7 4 がない場合にも間違っ

40

て統合 I D 7 7 4 と対応づけてしまう可能性がなく、好ましい。

【0 2 0 6】

このようにして、統合 I D 照会部 3 2 2 は、統合 I D が反映されたログレコード 7 5 0 を出力する。

ログ蓄積部 3 2 3 は、統合 I D 照会部 3 2 2 が出力した複数のログレコード 7 5 0 を入力し、加工済ログ 7 0 5 として 1 つにまとめて、ログ D B 3 2 5 に記憶する。

【0 2 0 7】

ログ管理装置 1 2 0 のログ収集部 3 2 1 が収集するログ 7 0 4 は、一般に複数のログレ

50

コード 740 を含んだ、一定期間（ログ収集間隔）に発生したログレコード 740 の集合である。各ログレコード 740 は、一般にそのレコードの生成に関与したユーザや機器の個別 ID（個別ユーザ ID 742 や個別機器 ID 743）が記録されている。

【0208】

統合 ID 照会部 322 は、各レコードから個別ユーザ ID 742、個別機器 ID 743 を抽出し、ID 管理装置 130 に各々該当する統合ユーザ ID、統合機器 ID を照会する。

統合 ID 属性情報取得部 332 は、照会にあたり、個別 ID のみならず、そのログレコードが記録された日付時刻 741 も ID 管理装置 130 に送る。個別 ID が示す対象は、日付時刻 741 によって変化している可能性があるからである。

10

【0209】

例えば、機器のマシン名（個別機器 ID の一例）は、その機器がネットワーク上で果たしている役割に基づいて名づけられる場合がある。例えば、共用ファイルサーバとして運用している機器に「file server」というマシン名をつける場合などである。そうすれば、他の機器は、ネットワーク上で「file server」というマシン名の機器を探すことにより、必要とする機能の提供を受けることができ、その機器が実際にどれであるかを意識しなくて済むからである。

【0210】

この場合、サーバのリプレースにより機器の実体が変わっても、マシン名は「file server」のままである。したがって、置き換え前と置き換え後とでは、同じマシン名であっても、異なる機器を示している。

20

【0211】

このように、同一の個別機器 ID に対して時間軸により異なる機器が割り付けられている場合であっても、日付時刻 741 を指定して照会すれば、正しい統合機器 ID を照会することができる。

【0212】

また、統合 ID 照会部 322 は、ログ収集部 321 が収集したログ 704 から個別 ID とそれが出現する時間範囲を各個別 ID ごとにあらかじめ抽出し、個別 ID と時間範囲の組を複数まとめて ID 管理装置に照会する。これにより、処理の効率が高くなる。

【0213】

以上説明した処理により、具体的にログ 704 がどのように加工されるかを示すため、図 19 に示した例を用いて説明する。

30

【0214】

図 20 の統合 ID 照会データ生成処理の開始時において、統合 ID 照会データ 706 は新規に作成され、内容は空である。

統合 ID 属性情報取得部 332 は、ログ 704 からログレコード 740 を 1 行ずつ読み込み（図 20 の S082）、処理を行う（図 20 の S083a～S086b）。

【0215】

2003 年 3 月 31 日 11 時 24 分 32 秒のログレコード 740 についての処理において、個別機器 ID 743「shogun」がまだ統合 ID 照会データ 706 に記録されていないので（図 20 の S084b）、統合 ID 照会部 322 は、新たな照会条件を生成し、統合 ID 照会データ 706 に追加する（図 20 の S085b）。このとき、個別 ID 761 は「shogun」、開始時刻 762 は「2003/03/31 11:24:32」に設定する。また、終了時刻 763 も「2003/03/31 11:24:32」に設定する（図 20 の S086b）。

40

【0216】

次のログレコード 740（2003 年 3 月 31 日 12 時 12 分 47 秒）の処理に移り、個別機器 ID 743「poseidon」もまだ統合 ID 照会データ 706 に記録されていないので（図 20 の S084b）、統合 ID 照会部 322 は、新たな照会条件を生成し、統合 ID 照会データ 706 に追加する（図 20 の S085b）。このとき、個別 ID 7

50

61は「poseidon」、開始時刻762は「2003/03/31 12:12:47」に設定する。また、終了時刻763も「2003/03/31 12:12:47」に設定する（図20のS086b）。

【0217】

次のログレコード740（2003年3月31日14時8分19秒）の処理に移り、個別機器ID743「shogun」は統合ID照会データ706に既に記録されている（図20のS084b）。そこで、「shogun」についての照会条件の終了時刻763を、「2003/03/31 14:08:19」に更新する（図20のS086b）。

【0218】

統合ID照会部322は、このようにして、図19に示した統合ID照会データ706 10
を生成する。

統合ID取得部331は、この統合ID照会データ706を入力し、ID管理DB333を検索した結果から、図19に示した統合ID照会結果707を生成し、出力する。

【0219】

統合ID照会部322は、この統合ID照会結果707を入力し、入力した統合ID照会結果707に基づいて、ログ704を加工して、加工済ログ705を生成する。

統合ID属性情報取得部332は、ログ704からログレコード740を1行ずつ読み込み（図21のS093）、処理を行う（図21のS094a～S097b）。

統合ID照会部322は、処理の結果生成したログレコード750を1行ずつ出力し、これが全体として、加工済ログ705となる。 20

【0220】

2003年3月31日11時24分32秒のログレコード740についての処理において、統合ID照会部322は、個別機器ID743「shogun」についての照会結果を、統合ID照会結果707から取得する（図21のS094b）。「shogun」についての照会結果は1つしかなく、日付時刻741「2003/03/31 11:24:32」が、開始時刻772「2003/03/31 11:24:32」から終了時刻773「2003/03/31 23:59:59」の期間内なので（図21のS095b）、統合ID属性情報取得部332は、統合ID774「ASSET987654」を、ログレコード740に追加してログレコード750を生成する（図21のS096b）。 30

【0221】

次のログレコード740（2003年3月31日12時12分47秒）の処理に移り、統合ID照会部322は、個別機器ID743「poseidon」についての照会結果を、統合ID照会結果707から取得する（図21のS094b）。「poseidon」についての照会結果は2つあるが、日付時刻741「2003/03/31 12:12:47」は、開始時刻772「2003/03/31 12:12:47」から終了時刻773「2003/03/31 23:59:59」の期間内なので、上の紹介結果を採用し（図21のS095b）、統合ID属性情報取得部332は、統合ID774「ASSET123456」を、ログレコード740に追加してログレコード750を生成する（図21のS096b）。 40

【0222】

間を省略して、2003年4月1日13時52分23秒のログレコード740についての処理を説明する。

統合ID照会部322は、個別機器ID743「shogun」についての照会結果を、統合ID照会結果707から取得する（図21のS094b）。「shogun」についての照会結果は1つしかないが、日付時刻741「2003/04/01 13:52:23」は、開始時刻772「2003/03/31 11:24:32」から終了時刻773「2003/03/31 23:59:59」の期間外なので採用せず（図21のS095b）、統合ID照会部322は、異常発生情報759「ErrUnknown」を、ログレコード740に追加してログレコード750を生成する。 50

なお、異常発生情報 759 は、まったく存在しない個別 ID と、かつて存在したが期限切れの個別 ID とを区別して（例えば「Err Expired」など）、統合 ID 照会部 322 がログレコード 750 を生成する構成としてもよい。

【0223】

統合 ID 照会部 322 は、このようにして、図 19 に示した加工済ログ 705 を生成する。

【0224】

以上のようにして、ログ 704 に統合 ID を反映して生成された加工済ログ 705 をログ蓄積部 323 がログ DB 325 に蓄積するので、統合 ID が示すオブジェクト（具体的な人や機器）に関連する、各ログに分散したイベントを、統合ユーザ ID や統合機器 ID をキーに一括して検索できる。

10

【0225】

また、統合 ID 照会時に個別 ID のみならず時刻も照会データに含めるため、個別 ID が、複数の統合 ID で繰り返し利用されていても、そのログレコードが記録された時の統合 ID を照会することができる。

【0226】

さらに、統合 ID 照会時に個々のログレコードごとに照会するのではなく、個別 ID とそれがログに出現する時間範囲で照会を行うので、統合 ID 照会の性能を向上させることができる。

【0227】

20

ここで、統合 ID について補足する。

統合 ID は、ユーザや機器などの対象を一意に識別する情報である。

統合 ID は、新たに付与して管理してもよいし、対象を一意に識別できるという条件のもと、既に管理されている情報を用いてもよい。統合 ID として、既に管理されている情報を用いれば、導入が容易であり、好ましい。

【0228】

例えば、ある企業のなかでその企業の備品である機器を操作したユーザを対象として統合 ID による管理を行う場合であれば、識別の対象であるユーザはその企業の従業員であるから、従業員コードを統合 ID として用いることができる。

なお、従業員を一意に識別できるという条件を満たすのであれば、従業員コード以外の人事情報を統合 ID として用いてもよい。

30

【0229】

また、ある企業のなかでその企業の備品である機器を対象として統合 ID による管理を行う場合であれば、識別の対象である機器はその企業の備品であるから、資産管理コードを統合 ID として用いることができる。

なお、機器を一意に識別できるという条件を満たすのであれば、資産管理コード以外の資産管理情報を統合 ID として用いてもよい。

【0230】

このように、既に管理されている情報を統合 ID として用いれば、管理端末装置 140 に条件を入力して加工済ログ 705 を検索する利用者にとって、その統合 ID によって識別される対象が、具体的に誰であるのか、物理的にどの機器であるのかを特定することが容易となり、ログの解析性が向上するので、好ましい。

40

【0231】

次に、ログ管理装置 120 からの照会に対して、ID 管理装置 130 が個別 ID に対応する統合 ID を発見できなかった場合について、補足する。

照会された個別ユーザ ID に該当する統合ユーザ ID がない場合、物理的な人物にたどり着かない ID が使われていることになる。例えば、マシン上にローカルに生成した不正なアカウントが使用されているなどの不正が行われている可能性がある。あるいは、退社した人物のアカウントを消去し忘れるなどして、有効期限の切れたアカウントが残っていて、不正に利用されている可能性がある。

50

【0232】

この実施の形態におけるログ加工装置110によれば、ログ704をそのまま蓄積するのではなく、加工済ログ705に加工してから蓄積するので、加工の際に統合IDにたどり着けない個別IDが使われていることを検知することができる。

そのような個別IDを検知した場合、ログ加工装置110は、異常発生情報759を含むログレコード750を生成するので、あとで検索する際、不正の可能性の高い動作を記録したログレコード750を容易に発見することができる。

【0233】

あるいは、そのような個別IDを検知した場合、警告出力部が、CPU911などの処理装置を用いて、CRTなどの表示装置901やその他の出力装置に、異常発生を示す警告を出力する構成としてもよい。

例えば、退社した人物の統合ユーザIDを一定期間保持し、それに対する照会がなされた場合はID管理装置が失効IDであることをログ管理装置に返すように構成してもよい。そうすれば、退職者のID無効化の運用忘れを防止することができる。

【0234】

同様に、ログ704の解析過程において、統合機器IDに該当する統合機器IDがない場合には、個人ノートPCの社内持込使用など、不正な機器の使用である可能性を検知することができる。

【0235】

退職や人事異動によって、以前は有効だった個別ユーザIDが無効になる場合がある。しかし、管理ミスなどにより、個別ユーザIDを無効化する処理をしないでいると、不正なアクセスを許すことになる。

【0236】

このように管理ミスなどによる不正アクセスを他の不正アクセスと区別するため、統合ID取得部331は、その日付時刻741において個別ユーザID742に対応する統合ユーザID754を、ID管理DB333が記憶した個別IDデータベース701のなかから発見できなかった場合には、期間外であってもその個別ユーザID742に対応する統合ユーザID754があれば、それを含む統合ID照会結果707を出力する構成としてもよい。

【0237】

その場合、統合ID取得部331は、CPU911などの処理装置を用いて、期限切れの個別ユーザID742が使われているという異常発生を示す異常発生情報759を統合ID照会結果707に含めて一緒に出力する。通常の場合と区別するためである。

統合ID照会部322は、CPU911などの処理装置を用いて、統合ID照会結果707を入力し、入力した統合ID照会結果707に含まれる異常発生情報759もログレコード740に追加して、異常発生情報759を含むログレコード750を生成し、出力する。

【0238】

これにより、異常発生を検知できるだけでなく、その操作者が誰であるかを推測することができる。

【0239】

この実施の形態におけるログ加工装置110（履歴管理装置）は、ID管理DB333（管理記憶部）が、CPU911などの処理装置を用いて、利用者を識別する情報である統合ユーザID（利用者識別情報）を、管理識別情報として含む管理情報710を磁気ディスク装置920などの記憶装置に記憶し、統合ID照会部322（履歴加工部）が、CPU911などの処理装置を用いて、機器を操作した時刻である操作時刻を示す情報である日付時刻741（操作時刻情報）と、機器を操作した利用者を示す情報である個別ユーザID742（操作者情報）とを含む情報であるログレコード740（操作履歴情報）を、発生履歴情報として入力し、CPU911などの処理装置を用いて、入力したログレコード740に含まれる日付時刻741によって示される操作時刻を示す情報を、統合ID

10

20

30

40

50

取得部 3 3 1 (管理検索部) が入力する時刻情報として出力し、入力したログレコード 7 4 0 に含まれる個別ユーザ ID 7 4 2 を、統合 ID 取得部 3 3 1 が入力する個別 ID 7 6 1 (対象情報) として出力し、CPU 9 1 1 などの処理装置を用いて、統合 ID 取得部 3 3 1 が出力した統合ユーザ ID を含む統合 ID 照会結果 7 0 7 を入力し、CPU 9 1 1 などの処理装置を用いて、入力したログレコード 7 4 0 に含まれる情報と、入力した統合ユーザ ID とを含むログレコード 7 5 0 (加工済履歴情報) を出力することを特徴とする。

【0 2 4 0】

この実施の形態におけるログ加工装置 1 1 0 によれば、ログ 7 0 4 のログレコード 7 4 0 に含まれる個別ユーザ ID 7 4 2 から、対応する統合ユーザ ID 7 5 4 を求め、統合ユーザ ID 7 5 4 を含むログレコード 7 5 0 を出力するので、利用者の統合ユーザ ID 7 5 4 を検索条件とすれば、特定の利用者が機器を操作したことに關するログを容易に発見することができるという効果を奏する。 10

【0 2 4 1】

この実施の形態におけるログ加工装置 1 1 0 は、ID 管理 DB 3 3 3 (管理記憶部) が、CPU 9 1 1 などの処理装置を用いて、従業員を識別する従業員コードを、統合ユーザ ID (管理識別情報) として含む管理情報 7 1 0 を磁気ディスク装置 9 2 0 などの記憶装置に記憶し、統合 ID 取得部 3 3 1 (管理検索部) が、CPU 9 1 1 などの処理装置を用いて、抽出した管理情報 7 1 0 に含まれる従業員コードによって識別される従業員がその機器の操作を許可された従業員であるか否かを判断し、CPU 9 1 1 などの処理装置を用いて、その従業員コードによって識別される従業員がその機器の操作を許可された従業員でないと判断した場合に、異常発生を示す情報である異常発生情報 7 5 9 を出力することを特徴とする。 20

【0 2 4 2】

この実施の形態におけるログ加工装置 1 1 0 によれば、期限切れのアカウントを削除し忘れるなどの管理ミスにより発生した不正アクセスを容易に発見でき、更に、その不正アクセスに關与したと思われる従業員を推定することができるという効果を奏する。

【0 2 4 3】

この実施の形態におけるログ加工装置 1 1 0 は、ID 管理 DB 3 3 3 (管理記憶部) が、CPU 9 1 1 などの処理装置を用いて、機器を識別する情報である統合機器 ID (機器識別情報) を、管理識別情報として含む管理情報 7 1 0 を磁気ディスク装置 9 2 0 などの記憶装置に記憶し、統合 ID 照会部 3 2 2 が、CPU 9 1 1 などの処理装置を用いて、機器を操作した時刻である操作時刻を示す情報である日付時刻 7 4 1 (操作時刻情報) と、その操作時刻に操作された機器を示す情報である個別機器 ID 7 4 3 (操作機器情報) とを含む情報であるログレコード 7 4 0 (操作履歴情報) を、発生履歴情報として入力し、CPU 9 1 1 などの処理装置を用いて、入力したログレコード 7 4 0 に含まれる日付時刻 7 4 1 によって示される操作時刻を示す情報を、統合 ID 取得部 3 3 1 が入力する時刻情報として出力し、入力したログレコード 7 4 0 に含まれる個別機器 ID 7 4 3 を統合 ID 取得部 3 3 1 が入力する個別 ID 7 6 1 (対象情報) として出力し、CPU 9 1 1 などの処理装置を用いて、統合 ID 取得部 3 3 1 が出力した統合機器 ID を含む統合 ID 照会結果 7 0 7 を入力し、CPU 9 1 1 などの処理装置を用いて、入力したログレコード 7 4 0 に含まれる情報と、入力した統合機器 ID とを含むログレコード 7 5 0 (加工済履歴情報) を出力することを特徴とする。 30 40

【0 2 4 4】

この実施の形態におけるログ加工装置 1 1 0 によれば、マシン名や IP アドレスなどの個別機器 ID が再利用され、時刻によって異なる機器を示す場合であっても、正しく対応する統合機器 ID を取得して、取得した統合機器 ID を含むログレコード 7 5 0 を出力するので、特定の機器に關するログを容易に発見することができるという効果を奏する。

【0 2 4 5】

例えば、あるサーバが保有している機密情報が流出した場合、そのサーバに対するアクセスを容易に抽出することができるので、情報流出の原因を突き止める助けとなる。 50

【0246】

この実施の形態におけるログ加工装置110は、ID管理DB333が、CPU911などの処理装置を用いて、機器を識別する資産管理コードを、統合機器ID（管理識別情報）として含む管理情報710を、磁気ディスク装置920などの記憶装置に記憶することを特徴とする。

【0247】

この実施の形態におけるログ加工装置110によれば、統合機器IDとして資産管理コードを用いるので、導入が容易であり、ログの解析性が向上するという効果を奏する。

【0248】

この実施の形態におけるログ加工装置110（履歴管理装置）は、更に、情報を出力するCRTなどの表示装置901やその他の出力装置と、CPU911などの処理装置を用いて、統合ID取得部331が異常発生情報759を出力した場合に、異常発生を示す警告をCRTなどの表示装置901やその他の出力装置に出力する警告出力部とを有することを特徴とする。 10

【0249】

この実施の形態のログ加工装置110によれば、統合ID取得部331が異常発生情報759を出力した場合に、警告出力部が警告を出力するので、問題が発生する前に異常事態に対処することができ、その異常に基づく問題の発生を未然に防ぐことができるという効果を奏する。

【0250】

この実施の形態におけるログ加工装置110は、統合ユーザIDとして、人事情報に割り付けられたIDを用いることを特徴とする。 20

【0251】

この実施の形態におけるログ加工装置110は、照会した統合ユーザIDが失効IDである場合、統合ユーザID照会時に、照会エラーのみならず、失効IDであることを返答することを特徴とする。

【0252】

この実施の形態におけるログ加工装置110は、統合機器IDとして、資産管理情報に割り付けられたIDを用いることを特徴とする。

【0253】

実施の形態4.

実施の形態4について、図22を用いて説明する。

この実施の形態におけるログ管理システム300は、ログ加工装置110、管理端末装置140を有する。

ログ加工装置110及び管理端末装置140は、実施の形態3で説明したものと同様なので、ここでは説明を省略する。

ログ管理システム300は、履歴管理装置の一例である。

【0254】

この実施の形態では、ログ蓄積部323がログDB325に蓄積した加工済ログ705の利用例について説明する。 40

【0255】

管理端末装置140のログ検索表示部342は、CPU911などの処理装置を用いて、キーボード902などの入力装置からログ検索条件を入力する。

ログ検索条件とは、ログ蓄積部323がログDB325に蓄積した加工済ログ705を検索するための条件を示す情報である。ログ検索条件は、検索条件情報の一例である。

ログ検索条件は、例えば、統合IDについての条件を示す情報が含んでもよいし、含まなくてもよい。

【0256】

ログ検索表示部342は、CPU911などの処理装置を用いて、入力したログ検索条件を出力する。ログ検索表示部342は、履歴照会部の一例である。 50

【0257】

ログ管理装置120のログ検索部324は、CPU911などの処理装置を用いて、ログ検索表示部342が出力したログ検索条件を入力し、入力したログ検索条件によって示される検索条件に基づいて、ログDB325が記憶した加工済ログ705を検索する。ログ検索部324は、検索結果を示す情報を出力する。ログ検索部324は、履歴検索部の一例である。

ログ検索部324が出力する検索結果を示す情報は、検索条件に合致する加工済ログ705のログレコード750に含まれる情報のすべてを含んでいてもよいし、一部だけを含んでいてもよい。例えば、ログレコード750のなかから抜粋した情報だけを検索結果として出力し、更に詳しい情報の表示を要求された場合に、すべての情報を出力することと10

【0258】

ログ検索表示部342は、入力したログ検索条件に統合IDについての条件が含まれている場合、CPU911などの処理装置を用いて、その統合IDを統合ID属性情報照会部341に対して出力する。

あるいは、ログ検索表示部342は、CPU911などの処理装置を用いて、ログ検索部324から入力した情報によって示される検索結果から統合IDを取得し、取得した統合IDを統合ID属性情報照会部341に対して出力してもよい。

【0259】

統合ID属性情報照会部341は、CPU911などの処理装置を用いて、ログ検索表示部342が出力した統合IDを入力する。統合ID属性情報照会部341は、CPU911などの処理装置を用いて、入力した統合IDについての属性情報の照会を要求する情報を生成し、統合ID属性情報取得部332に対して出力する。20

また、統合ID属性情報照会部341は、CPU911などの処理装置を用いて、ログ検索条件とは別に、キーボード902などの入力装置から統合IDを入力し、入力した統合IDについての属性情報の照会を要求する情報を生成して、統合ID属性情報取得部332に対して出力してもよい。

【0260】

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、統合ID属性情報照会部341が出力した照会要求を入力する。照会要求には、統合ID属性情報照会部341が照会を要求する統合IDが含まれている。30

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、ID管理DB333が記憶した属性データベース702を検索して、入力した統合IDについての管理属性情報720を取得する。統合ID属性情報取得部332は、CPU911などの処理装置を用いて、取得した管理属性情報720を、統合ID属性情報照会部341に対して出力する。統合ID属性情報取得部332は、属性検索部の一例である。

【0261】

統合ID属性情報照会部341は、CPU911などの処理装置を用いて、統合ID属性情報取得部332が出力した管理属性情報720を入力する。統合ID属性情報照会部341は、入力した管理属性情報720を、ログ検索表示部342に対して出力する。40

【0262】

ログ検索表示部342は、CPU911などの処理装置を用いて、統合ID属性情報照会部341が出力した管理属性情報720を入力する。

ログ検索表示部342は、CPU911などの処理装置を用いて、ログ検索部324から入力した検索結果に含まれるログレコード750の情報と、そのログレコード750に含まれる統合IDについて、統合ID属性情報照会部341から入力した管理属性情報720とを合わせて、CRTなどの表示装置901やその他の出力装置に表示・出力する。

【0263】

これにより、ログの解析過程において統合IDが割り出された場合、それに付随する属性情報も参照できるので、実体が把握し易くなり、ログの解析性が向上する。50

【0264】

図17などを用いて説明したとおり、対象の属性は時刻によって変化する可能性があり、ID管理DB333が記憶する属性データベース702に含まれる管理属性情報720には、その統合IDによって識別される対象がその属性を有している期間を示す属性期間情報（例えば、図15の開始時刻724及び終了時刻725）が含まれている。

【0265】

そのため、統合ID属性情報照会部341が生成し、統合ID属性情報取得部332に対して出力する照会要求には、統合IDのほか、照会したい時刻を示す時刻情報が含まれる。

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、統合IDとともに、時刻情報を入力し、時刻情報によって示される時刻における管理属性情報720を検索して、出力する。 10

【0266】

統合ID属性情報照会部341が生成し、統合ID属性情報取得部332に対して出力する照会要求に含まれる時刻情報は、現在時刻を示す情報であってもよい。これにより、その統合IDによって識別される対象の現在の属性を取得することができるので、ログ検索表示部342が出力した情報を見た利用者が、容易に実体を把握することができる。

【0267】

また、時刻情報が示す時刻は、ログ検索表示部342がログ検索部324から入力したログレコード750に含まれる日付時刻751によって示される時刻であってもよい。これにより、その統合IDによって識別される対象の当時の属性を取得することができるので、ログ検索表示部342が出力した情報を見た利用者が、容易に実体を把握することができる。 20

【0268】

ログ検索表示部342が入力するログ検索条件は、対象の属性についての条件を含んでもよい。

例えば、現在「2棟8階」に設置されている「PCサーバ」について検索したい場合や、2001年当時「人事部」にいた「山口花子」さんについて検索したい場合などは、統合ユーザIDや統合機器IDが不明であっても、属性についての条件に基づいて検索をする。このように、日時を指定して属性を検索すれば、例えば「山口花子」さんが結婚して 30
姓が変わったことを知らなくても、検索が可能になる。

【0269】

ログ蓄積部323がログDB325に蓄積した加工済ログ705には、統合ユーザID754や統合機器ID755などの統合IDが含まれているが、その対象の属性についての情報は含まれていない。

そこで、ログ検索表示部342は、CPU911などの処理装置を用いて、統合ID属性情報照会部341を介して、統合ID属性情報取得部332に対して、その属性を有する対象の統合IDを照会する。

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、照会された条件に合致する管理属性情報720を検索し、検索結果を出力する。 40

ログ検索表示部342は、CPU911などの処理装置を用いて、統合ID属性情報取得部332が出力した検索結果を入力する。

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、入力した検索結果から統合IDを取得し、取得した統合IDを含むログ検索条件を生成して、生成したログ検索条件をログ検索部324に対して出力する。

【0270】

次に、動作について説明する。

図22は、この実施の形態における検索結果表示部142がログを照会するログ照会処理の流れの一例を示すフローチャート図である。

【0271】

S 4 0 1において、ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、ログ検索条件 8 0 1をキーボード 9 0 2などの入力装置から入力する。

ログ検索条件 8 0 1は、例えば、S Q L (S t r u c t u r e d Q u e r y L a n g u a g e) 文などにより、加工済ログ 7 0 5を検索する条件を示す情報である。

【 0 2 7 2 】

S 4 0 2において、ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、S 4 0 1で入力したログ検索条件 8 0 1を解析する。

ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、ログ検索条件 8 0 1を解析した結果に基づき、ログ検索条件 8 0 1に統合 I D についての条件が含まれているか否かを判断する。

ログ検索条件 8 0 1に統合 I D についての条件が含まれていると判断した場合には、S 4 0 7へ進む。

ログ検索条件 8 0 1に統合 I D についての条件が含まれていないと判断した場合には、S 4 0 3へ進む。

【 0 2 7 3 】

S 4 0 3において、ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、S 4 0 2でログ検索条件 8 0 1を解析した結果に基づき、ログ検索条件 8 0 1に属性についての条件が含まれているか否かを判断する。

ログ検索条件 8 0 1に属性についての条件が含まれていると判断した場合には、S 4 0 4へ進む。

ログ検索条件 8 0 1に属性についての条件が含まれていないと判断した場合には、S 4 0 7へ進む。

【 0 2 7 4 】

S 4 0 4において、ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、S 4 0 2でログ検索条件 8 0 1を解析した結果得られた属性についての条件に基づき、属性照会データ 8 0 2を生成する。

属性照会データ 8 0 2は、統合 I D 属性情報取得部 3 3 2に対して管理属性情報 7 2 0 (図 1 5 参照) の検索を要求する情報である。この場合、属性照会データ 8 0 2は、種別 7 2 1、属性 7 2 2と、検索する時刻を示す時刻情報とを指定して、条件に合致する管理属性情報 7 2 0 の検索を要求する情報である。

ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、生成した属性照会データ 8 0 2を出力する。

【 0 2 7 5 】

ログ検索表示部 3 4 2が出力した属性照会データ 8 0 2は、統合 I D 属性情報照会部 3 4 1を介して、統合 I D 属性情報取得部 3 3 2が入力する。

統合 I D 属性情報取得部 3 3 2は、C P U 9 1 1などの処理装置を用いて、I D 管理 D B 3 3 3 が記憶した属性データベース 7 0 2を検索し、入力した属性照会データ 8 0 2 が示す条件に合致する管理属性情報 7 2 0 を取得する。

統合 I D 属性情報取得部 3 3 2が、C P U 9 1 1などの処理装置を用いて、取得した管理属性情報 7 2 0 を、属性照会結果 8 0 3 として出力する。

【 0 2 7 6 】

S 4 0 5において、ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、統合 I D 属性情報取得部 3 3 2が出力した属性照会結果 8 0 3 を、統合 I D 属性情報照会部 3 4 1 経由で入力する。

ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、入力した属性照会結果 8 0 3 を解析して、管理属性情報 7 2 0 に含まれる統合 I D を取得する。

【 0 2 7 7 】

S 4 0 6において、ログ検索表示部 3 4 2は、C P U 9 1 1などの処理装置を用いて、S 4 0 5で取得した統合 I D と一致する統合 I D を検索する検索条件を、S 4 0 1で入力したログ検索条件 8 0 1 に追加する。

10

20

30

40

50

【0278】

S407において、ログ検索表示部342は、CPU911などの処理装置を用いて、S401で入力したログ検索条件801またはS406で生成したログ検索条件801を、ログ検索部324に対して出力する。

【0279】

ログ検索部324は、CPU911などの処理装置を用いて、ログ検索表示部342が出力したログ検索条件801を入力し、ログDB325が記憶した加工済ログ705を検索して、条件に合致するログレコード750を取得する。

ログ検索部324は、CPU911などの処理装置を用いて、取得したログレコード750をログ検索結果804として出力する。

10

【0280】

S408において、ログ検索表示部342は、CPU911などの処理装置を用いて、ログ検索部324が出力したログ検索結果804を入力する。

ログ検索表示部342は、CPU911などの処理装置を用いて、入力したログ検索結果804を解析して、ログレコード750に含まれる統合IDと日付時刻751とを取得する。

【0281】

S409において、ログ検索表示部342は、CPU911などの処理装置を用いて、S408で取得した統合IDによって識別される対象の有する属性の検索を要求する属性照会データ805を生成する。

20

この場合、属性照会データ805は、統合ID723と時刻情報とを指定した情報である。

時刻情報が示す時刻は、S408で取得した日付時刻751が示す時刻である。これにより、そのログが記録された当時の属性を知ることができる。

あるいは、時刻情報は、現在時刻を示すものであってもよい。そうすれば、その対象が現在どういう状態にあるかを知ることができる。

ログ検索表示部342は、CPU911などの処理装置を用いて、生成した属性照会データ805を出力する。

【0282】

ログ検索表示部342が出力した属性照会データ805は、統合ID属性情報照会部341を経由して、統合ID属性情報取得部332が入力する。

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、ID管理DB333が記憶した属性データベース702を検索し、入力した属性照会データ805が示す条件に合致する管理属性情報720を取得する。

統合ID属性情報取得部332は、取得した管理属性情報720を、属性照会結果806として出力する。

【0283】

S410において、ログ検索表示部342は、CPU911などの処理装置を用いて、統合ID属性情報取得部332が出力した属性照会結果806を、統合ID属性情報照会部341を介して入力する。

40

【0284】

S411において、ログ検索表示部342は、CPU911などの処理装置を用いて、S408で入力したログ検索結果804を、利用者が見やすい形にして照会結果807とし、CRTなどの表示装置901やその他の出力装置に出力する。

ログ検索表示部342は、ログレコード750に含まれる統合IDについて、ログが記録された当時、または現在において、その統合IDによって識別される対象の有する属性を、S410で入力した属性照会結果806から取得し、わかりやすい形でログレコード750に付加して出力する。

【0285】

これにより、ログの解析過程において統合IDが割り出された場合、それに付随する属

50

性情報も参照できるので、実体が把握し易くなり、解析性が向上する。

【0286】

また、属性情報を照会する際、統合IDのみならず、ログレコードの記録された時刻をキーに照会するので、時間とともに変化する属性情報の中から、ログが記録された時刻における属性情報を照会でき、解析性が向上する。

【0287】

さらに、属性情報を照会する際、上記に加え、現在時刻もキーに照会するので、ログが記録された時刻における属性情報の他に、現在の属性情報も照会でき、現在の連絡先などをすぐに把握することができる。

【0288】

このように、統合IDはログを蓄積する際に照会してログに反映させておき、属性情報はログを検索する際に照会して表示することにより、以下の効果を奏する。

【0289】

蓄積されたログには統合IDが反映されているため、統合IDによる検索が可能となり、複数ログに分散記録された特定ユーザ或いは特定機器に関するログを一括検索することができる。

一方、統合IDに付随する属性情報は、ログ検索・表示時に反映するため、蓄積するログの量を抑えることができる。

【0290】

この実施の形態におけるログ管理システム300（履歴管理装置）は、更に、情報を入力するキーボード902などの入力装置と、情報を入力するCRTなどの表示装置901やその他の出力装置と、CPU911などの処理装置を用いて、統合ID723（管理識別情報）と、統合ID723によって識別される対象の属性を示す情報である属性722（属性情報）とを含む情報である管理属性情報720を磁気ディスク装置920などの記憶装置に記憶するID管理DB333（属性記憶部）と、CPU911などの処理装置を用いて、統合IDを入力し、CPU911などの処理装置を用いて、ID管理DB333が記憶した管理属性情報720のなかから、入力した統合IDと、管理属性情報720に含まれる統合ID723とが一致する管理属性情報720を抽出し、CPU911などの処理装置を用いて、抽出した管理属性情報720に含まれる情報を入力する統合ID属性情報取得部332（属性検索部）と、CPU911などの処理装置を用いて、検索条件を示す情報であるログ検索条件801（検索条件情報）を、キーボード902などの入力装置から入力し、CPU911などの処理装置を用いて、入力したログ検索条件801によって示される検索条件を示す情報を、ログ検索部324（履歴検索部）が入力する履歴検索条件情報として出力し、CPU911などの処理装置を用いて、ログ検索部324が出力した加工済ログ705に含まれる情報を入力し、CPU911などの処理装置を用いて、入力した加工済ログ705に含まれる統合IDを、統合ID属性情報取得部332が入力する統合IDとして出力し、CPU911などの処理装置を用いて、統合ID属性情報取得部332が出力した管理属性情報720に含まれる情報を入力し、CPU911などの処理装置を用いて、入力した加工済ログ705に含まれる情報と、入力した管理属性情報720に含まれる情報とをCRTなどの表示装置901やその他の出力装置に出力するログ検索表示部342（履歴照会部）とを有することを特徴とする。

【0291】

この実施の形態におけるログ管理システム300によれば、加工済ログ705に含まれる統合IDを条件として、ログ検索部324が加工済ログ705のログレコード750を検索し、統合IDによって識別される対象の属性を示す管理属性情報720を、統合ID属性情報取得部332が検索し、ログ検索表示部342が検索した加工済ログ705と管理属性情報720とを合わせて出力するので、膨大なログのなかから必要とするログレコード750を容易に見つけることができるという効果を奏する。

【0292】

この実施の形態におけるログ管理システム300（履歴管理装置）は、ID管理DB3

10

20

30

40

50

33（属性記憶部）が、CPU911などの処理装置を用いて、統合ID（管理識別情報）によって識別される対象が属性722（属性情報）によって示される属性を有する期間を示す情報である開始時刻724及び終了時刻725（属性期間情報）を更に含む管理属性情報720を磁気ディスク装置920などの記憶装置に記憶し、統合ID属性情報取得部332（属性検索部）が、CPU911などの処理装置を用いて、時刻を示す情報である時刻情報と、統合IDとを入力し、CPU911などの処理装置を用いて、ID管理DB333が記憶した管理属性情報720のなかから、入力した統合IDと、管理属性情報720に含まれる統合ID723とが一致し、かつ、入力した時刻情報によって示される時刻が、管理属性情報720に含まれる開始時刻724及び終了時刻725によって示される期間内である管理属性情報720を抽出し、CPU911などの処理装置を用いて、抽出した管理属性情報720を出力し、ログ検索表示部342が、CPU911などの処理装置を用いて、入力した加工済ログ705のログレコード750（加工済履歴情報）に含まれる日付時刻751（発生時刻情報）によって示される発生時刻を示す情報を、統合ID取得部331が入力する時刻情報として出力することを特徴とする。 10

【0293】

この実施の形態におけるログ管理システム300によれば、統合ID属性情報取得部332が、ログが記録された時刻における管理属性情報720を検索するので、ログが記録された時刻における対象の属性を知ることができ、ログの可読性が向上するという効果を奏する。

【0294】

この実施の形態におけるログ管理システム300（履歴管理装置）は、更に、ログ検索表示部342（履歴照会部）が、CPU911などの処理装置を用いて、現在時刻を示す情報を、統合ID属性情報取得部332（属性検索部）が入力する時刻情報として出力することを特徴とする。 20

【0295】

この実施の形態におけるログ管理システム300によれば、統合ID属性情報取得部332が、現在時刻における管理属性情報720を検索するので、判明した対象の現在の属性を知ることができ、ログの可読性が向上するという効果を奏する。

【0296】

この実施の形態におけるログ加工装置110は、統合IDが、実体を識別するために割り当てられたIDであり、実体に付随する属性情報（個人であれば所属名、機器であれば設置場所など）を統合IDに紐付けて管理し、統合IDから属性情報の照会をすることを特徴とする。 30

【0297】

この実施の形態におけるログ加工装置110は、統合IDに付属する属性情報を、それらの有効期間範囲とともに管理し（例えば個人の所属部署は時間とともに変わる）、統合IDから属性情報を照会する時に、統合IDと時刻の両方を引数に照会することを特徴とする。

【0298】

この実施の形態におけるログ加工装置110は、統合ID照会時に現在時刻も引数に追加して照会することを特徴とする。 40

【0299】

この実施の形態におけるログ加工装置110は、ログへの統合IDの反映を、ログ蓄積時に行うことを特徴とする。

【0300】

この実施の形態におけるログ加工装置110は、付随する属性情報（所属部署名、氏名、住所、など）を検索・表示時に反映することを特徴とする。

【0301】

この実施の形態におけるログ加工装置110によれば、ログ蓄積前にログに統合IDを反映するので、統合IDが後のログ解析性に効果を発揮する。 50

【0302】

実施の形態5.

実施の形態5について、図23～図25を用いて説明する。

この実施の形態におけるログ管理システム300、ログ加工装置110、管理端末装置140の構成は、実施の形態4で説明したものと同様なので、ここでは説明を省略する。

【0303】

図23は、この実施の形態におけるログ加工装置110の内部ブロックの詳細な構成の一例を示す詳細ブロック図である。

【0304】

統合ID照会部322は、ログレコード解析部371、統合ID照会データ生成部372、統合ID照会結果解析部373、ログレコード加工部374を有する。 10

【0305】

ログレコード解析部371は、CPU911などの処理装置を用いて、ログ収集部321が出力したログ704から、ログレコード740を1行ずつ読み込む。ログレコード解析部371は、CPU911などの処理装置を用いて、読み込んだログレコード740を解析して、日付時刻741や個別ユーザID742などを取得する。

ログレコード解析部371は、CPU911などの処理装置を用いて、取得した日付時刻741や個別ユーザID742などを出力する。

【0306】

統合ID照会データ生成部372は、CPU911などの処理装置を用いて、ログレコード解析部371が取得した個別ユーザID742や個別機器ID743などの個別ID761、日付時刻741を入力する。統合ID照会データ生成部372は、CPU911などの処理装置を用いて、入力した個別ID761などに基づいて、統合ID照会データ706を生成する。統合ID照会データ生成部372は、生成した統合ID照会データ706を、統合ID取得部331に対して出力する。 20

【0307】

統合ID照会結果解析部373は、CPU911などの処理装置を用いて、統合ID取得部331が統合ID照会データ706に基づいて個別IDデータベース701を検索した検索結果を示す統合ID照会結果707を入力する。統合ID照会結果解析部373は、CPU911などの処理装置を用いて、入力した統合ID照会結果707を解析して、統合ID774及び送受信種別791を取得する。統合ID照会結果解析部373は、CPU911などの処理装置を用いて、取得した統合ID774及び送受信種別791を出力する。 30

【0308】

ログレコード加工部374は、CPU911などの処理装置を用いて、ログ収集部321が出力したログ704を入力する。ログレコード加工部374は、CPU911などの処理装置を用いて、統合ID照会結果解析部373が出力した統合ID774及び送受信種別791を入力する。ログレコード加工部374は、CPU911などの処理装置を用いて、入力したログ704を加工し、入力した統合ID774及び送受信種別791を追加して、加工済ログ705を生成する。ログレコード加工部374は、CPU911などの処理装置を用いて、生成した加工済ログ705を、ログ蓄積部323に対して出力する。 40

【0309】

この実施の形態のログ収集部321が収集するログ704は、利用者が、監視対象機器500であるコンピュータを用いて電子メールの送受信操作を行ったことを記録したログである。ログ収集部321が収集するログ704に含まれるログレコード740は、メール送信履歴情報の一例である。

【0310】

ID管理DB333は、個別ID記憶部361、ドメイン種別記憶部375、送受信種別テーブル記憶部377を有する。

個別 I D 記憶部 3 6 1 は、C P U 9 1 1 などの処理装置を用いて、個別 I D データベース 7 0 1 を、磁気ディスク装置 9 2 0 などの記憶装置に記憶している。

【0 3 1 1】

ドメイン種別記憶部 3 7 5 は、C P U 9 1 1 などの処理装置を用いて、電子メールアドレス 7 8 3 のドメイン名と、そのドメインの種別との対応関係を示すドメイン種別テーブルを、磁気ディスク装置 9 2 0 などの記憶装置に記憶している。

【0 3 1 2】

送受信種別テーブル記憶部 3 7 7 は、C P U 9 1 1 などの処理装置を用いて、送信元種別及び送信先種別と、そのメールの送受信の種別との対応関係を示す送受信種別テーブルを、磁気ディスク装置 9 2 0 などの記憶装置に記憶している。

10

【0 3 1 3】

統合 I D 取得部 3 3 1 は、照会データ取得部 3 5 1、統合 I D 検索部 3 5 2、ドメイン種別判定部 3 7 6、送受信種別判定部 3 7 8、照会結果通知部 3 5 3 を有する。

【0 3 1 4】

照会データ取得部 3 5 1 は、C P U 9 1 1 などの処理装置を用いて、統合 I D 照会データ生成部 3 7 2 が出力した統合 I D 照会データ 7 0 6 を入力する。照会データ取得部 3 5 1 は、C P U 9 1 1 などの処理装置を用いて、入力した統合 I D 照会データ 7 0 6 を、統合 I D 検索部 3 5 2 に対して出力する。照会データ取得部 3 5 1 は、C P U 9 1 1 などの処理装置を用いて、入力した統合 I D 照会データ 7 0 6 に含まれる個別 I D が電子メールアドレスである場合、ドメイン種別判定部 3 7 6 に対して、その電子メールアドレスを出力する。

20

【0 3 1 5】

統合 I D 検索部 3 5 2 は、C P U 9 1 1 などの処理装置を用いて、照会データ取得部 3 5 1 が出力した統合 I D 照会データ 7 0 6 を入力する。統合 I D 検索部 3 5 2 は、C P U 9 1 1 などの処理装置を用いて、入力した統合 I D 照会データ 7 0 6 に基づいて、個別 I D 記憶部 3 6 1 が記憶した個別 I D データベース 7 0 1 を検索し、統合 I D 照会データ 7 0 6 に含まれる個別 I D に対応する統合 I D を取得する。統合 I D 検索部 3 5 2 は、C P U 9 1 1 などの処理装置を用いて、取得した統合 I D を出力する。

【0 3 1 6】

ドメイン種別判定部 3 7 6 は、C P U 9 1 1 などの処理装置を用いて、照会データ取得部 3 5 1 が出力した電子メールアドレス 7 8 3 を入力する。ドメイン種別判定部 3 7 6 は、C P U 9 1 1 などの処理装置を用いて、入力した電子メールアドレス 7 8 3 からドメイン名を取得する。ドメイン種別判定部 3 7 6 は、C P U 9 1 1 などの処理装置を用いて、ドメイン種別記憶部 3 7 5 が記憶したドメイン種別テーブルを検索して、取得したドメイン名を有するドメインの種別を判定する。ドメイン種別判定部 3 7 6 は、C P U 9 1 1 などの処理装置を用いて、判定したドメインの種別を示すドメイン種別 7 8 1 を出力する。なお、ドメイン種別 7 8 1 には、送信元メールアドレスについてのドメイン種別である送信元種別と、送信先メールアドレスについてのドメイン種別である送信先種別との 2 種類があり、ドメイン種別判定部 3 7 6 は、送信元種別と送信先種別との 2 つのドメイン種別 7 8 1 を出力する。

30

40

【0 3 1 7】

送受信種別判定部 3 7 8 は、C P U 9 1 1 などの処理装置を用いて、ドメイン種別判定部 3 7 6 が出力したドメイン種別 7 8 1 を入力する。送受信種別判定部 3 7 8 は、C P U 9 1 1 などの処理装置を用いて、送受信種別テーブル記憶部 3 7 7 が記憶した送受信種別テーブルを検索して、メールの送受信の種別を判定する。送受信種別判定部 3 7 8 は、C P U 9 1 1 などの処理装置を用いて、判定した送受信の種別を示す送受信種別 7 9 1 を出力する。

【0 3 1 8】

照会結果通知部 3 5 3 は、C P U 9 1 1 などの処理装置を用いて、統合 I D 検索部 3 5 2 が出力した統合 I D 7 7 4 と、送受信種別判定部 3 7 8 が出力した送受信種別 7 9 1 と

50

を入力する。照会結果通知部 353 は、CPU911 などの処理装置を用いて、入力した統合 ID774 と送受信種別 791 とに基づいて、統合 ID 照会結果 707 を生成する。照会結果通知部 353 は、CPU911 などの処理装置を用いて、生成した統合 ID 照会結果 707 を出力する。

【0319】

図 24 は、この実施の形態における ID 管理装置 130 の各ブロックの間でやり取りされる情報の一例を示す図である。

【0320】

ログ収集部 321 が収集して出力したログ 704 に含まれる各ログレコード 740 に基づいて、統合 ID 照会データ生成部 372 が生成して出力する統合 ID 照会データ 706 は、日付時刻 741、個別ユーザ ID 742、個別機器 ID 743、送信元メールアドレス 746、送信先メールアドレス 747 などを含む。

日付時刻 741 は、利用者が電子メールを送受信した時刻を示す情報（送信時刻情報）である。

個別ユーザ ID 742 は、電子メールを送受信した利用者を示す識別情報であり、例えば、OS のログオン名である。

個別機器 ID 743 は、利用者が電子メールを送受信した機器を示す識別情報であり、例えば、コンピュータのマシン名である。

送信元メールアドレス 746 は、利用者が電子メールを送信した場合であれば、利用者が送信に用いたメールアドレスを示す情報である。利用者が電子メールを受信した場合であれば、受信したメールの送信者が用いたメールアドレスを示す情報である。

送信先メールアドレス 747 は、利用者が電子メールを送信した場合であれば、送信した電子メールの宛先を示すメールアドレスを示す情報である。利用者が電子メールを受信した場合であれば、受信したメールの宛先である利用者のメールアドレスを示す情報である。

日付時刻 741 は、移動時刻情報の一例である。個別ユーザ ID 742、個別機器 ID 743、送信元メールアドレス 746、送信先メールアドレス 747 は、個別 ID の一例である。送信元メールアドレス 746 は、移動元情報の一例である。送信先メールアドレス 747 は、移動先情報の一例である。

【0321】

ログレコード解析部 371 は、CPU911 などの処理装置を用いて、ログレコード 740 を解析し、日付時刻 741、個別ユーザ ID 742 などの個別 ID を取得して出力する。

統合 ID 照会データ生成部 372 は、CPU911 などの処理装置を用いて、ログレコード解析部 371 が出力した日付時刻 741、個別ユーザ ID 742 などの個別 ID を入力する。統合 ID 照会データ生成部 372 は、CPU911 などの処理装置を用いて、それぞれのログレコード 740 について、そのログレコード 740 の日付時刻 741 と、そのログレコード 740 に含まれる個別 ID のリストとからなる統合 ID 照会データ 706 を生成する。統合 ID 照会データ生成部 372 は、CPU911 などの処理装置を用いて、生成した統合 ID 照会データ 706 を出力する。

【0322】

照会データ取得部 351 は、CPU911 などの処理装置を用いて、統合 ID 照会データ生成部 372 が出力した統合 ID 照会データ 706 を入力し、解析する。照会データ取得部 351 は、CPU911 などの処理装置を用いて、入力した統合 ID 照会データ 706 から、日付時刻 741 と電子メールアドレス 783（送信元メールアドレス 746 と送信先メールアドレス 747）を取得する。照会データ取得部 351 は、CPU911 などの処理装置を用いて、取得した日付時刻 741 と電子メールアドレス 783 とを、ドメイン種別判定部 376 に対して出力する。

【0323】

ドメイン種別記憶部 375 が記憶しているドメイン種別テーブル 780 は、項目として

10

20

30

40

50

、ドメイン名 782、ドメイン種別 781、開始時刻 784、終了時刻 785 を有するテーブル形式の情報である。

ドメイン名 782 は、メールアドレスの「@」より後ろの部分の文字列であり、ドメインを示す情報である。

ドメイン種別 781 は、ドメイン名 782 が示すドメインの種別を示す情報である。例えば、そのドメインが「社内」のドメインであるか、「社外」のドメインであるかを示す。なお、これは一例であってもっと細かな種別を設けて区別してもよい。例えば、「社内」のドメインを更に細かく分類し、「人事部」のドメイン、「営業部」のドメインなどの種別を設けてもよい。また、「社外」のドメインを更に細かく分類し、「取引先」のドメイン、「同業他社」のドメインなどの種別を設けてもよい。

10

【0324】

開始時刻 784 及び終了時刻 785 は、そのドメイン名 782 が示すドメインが、そのドメイン種別 781 が示す種別のドメインである期間を示す情報である。開始時刻 784 はその期間の開始時刻を示す。終了時刻 785 はその期間の終了時刻を示す。

例えば、新たなドメイン名を獲得して使用を始めた場合や、それまで取引関係のなかった相手との取引を始めた結果、「社外」だったドメインが「取引先」になった場合など、ドメイン名 782 とドメイン種別 781 との対応関係も、時刻によって変化する場合がありますので、開始時刻 784 及び終了時刻 785 によって、その対応関係がある期間を特定しておく。

開始時刻 784 及び終了時刻 785 は、管理情報 710 や管理属性情報 720 における開始時刻 714、724 や終了時刻 715、725 と同様なので、更に詳しい説明は省略する。

20

【0325】

ドメイン種別判定部 376 は、メールアドレス文字列を入力とし、「@」以降のドメイン文字列から社内アドレスか社外アドレスかを判定するものである。

ドメイン種別判定部 376 は、CPU 911 などの処理装置を用いて、照会データ取得部 351 が出力した電子メールアドレス 783 を入力し、ドメイン種別記憶部 375 が記憶したドメイン種別テーブル 780 を検索して、ドメイン種別 781 を取得し、取得したドメイン種別 781 を出力する。

【0326】

ドメイン種別判定部 376 は、ドメイン種別記憶部 375 が記憶したドメイン種別テーブル 780 のなかに、入力した電子メールアドレス 783 のドメイン名がない場合には、そのドメインは「社外」のドメインであると判定することとしてもよい。ドメイン名が未知であるということは、少なくとも「社内」のドメインではないと判断できるからである。

30

【0327】

送受信種別テーブル記憶部 377 が記憶している送受信種別テーブル 790 は、項目として、送信元種別 792、送信先種別 793、送受信種別 791 を有するテーブル形式の情報である。

送信元種別 792 は、送信元メールアドレス 746 のドメイン種別 781 を示す情報である。

40

送信先種別 793 は、送信先メールアドレス 747 のドメイン種別 781 を示す情報である。

送受信種別 791 は、メールの送受信の方向を示す情報である。この例では、「社内から社内へ」の場合を「1」、「社内から社外へ」の場合を「2」、「社外から社内へ」の場合を「3」、「社外から社外へ」の場合を「4」と定義している。しかし、送受信種別 791 は数字である必要はない。

【0328】

送受信種別判定部 378 は、送信元アドレス及び送信先アドレスが各々社内か社外かの情報を入力とし、送受信種別テーブル 790 を参照して、入力情報の関係から送受信種別

50

を決定するものである。

送受信種別判定部 378 は、CPU 911 などの処理装置を用いて、ドメイン種別判定部 376 が出力したドメイン種別 781 を入力し、送受信種別テーブル記憶部 377 が記憶した送受信種別テーブル 790 を検索して、送受信種別 791 を取得し、取得した送受信種別 791 を出力する。

【0329】

照会結果通知部 353 は、CPU 911 などの処理装置を用いて、統合 ID 検索部 352 が出力した統合ユーザ ID 754 や統合機器 ID 755 などの統合 ID と、送受信種別判定部 378 が出力した送受信種別 791 とを入力して、統合 ID 照会結果 707 を生成し、生成した統合 ID 照会結果 707 を出力する。

10

【0330】

次に、動作について説明する。

図 25 は、この実施の形態における ID 管理装置 130 が統合 ID を検索する ID 検索処理の流れの一例を示すフローチャート図である。

【0331】

S421 において、照会データ取得部 351 は、CPU 911 などの処理装置を用いて、統合 ID 照会データ生成部 372 が出力した統合 ID 照会データ 706 を入力する。照会データ取得部 351 は、CPU 911 などの処理装置を用いて、統合 ID 検索部 352 に対して、入力した統合 ID 照会データ 706 を出力する。照会データ取得部 351 は CPU 911 などの処理装置を用いて、入力した統合 ID 照会データ 706 を解析して、日付時刻 741、送信元メールアドレス 746、送信先メールアドレス 747 を取得する。照会データ取得部 351 は、CPU 911 などの処理装置を用いて、ドメイン種別判定部 376 に退位して、取得した日付時刻 741、送信元メールアドレス 746、送信先メールアドレス 747 を出力する。

20

【0332】

S422 の処理と、S426 から S427 までの処理とは、並列して実行される。しかし、一方の処理を先に実行し、他方の処理を後に実行してもよい。

【0333】

S422 において、統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、S421 で照会データ取得部 351 が出力した統合 ID 照会データ 706 を入力する。統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、入力した統合 ID 照会データ 706 に含まれる日付時刻 741、個別ユーザ ID 742、個別機器 ID 743、送信元メールアドレス 746、送信先メールアドレス 747 を取得する。統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、個別 ID 記憶部 361 が記憶した個別 ID データベース 701 を検索し、取得した日付時刻 741 が示す時刻において、個別ユーザ ID 742、個別機器 ID 743 などの個別 ID に対応する統合 ID を検索する。また、送信元メールアドレス 746、送信先メールアドレス 747 も個別 ID (個別ユーザ ID) の一種であるから、統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、日付時刻 741 が示す時刻において、送信元メールアドレス 746、送信先メールアドレス 747 に対応する統合 ID も同様に検索する。統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、検索した統合 ID を出力する。

30

40

その後、S424 へ進む。

【0334】

一方、S426 において、ドメイン種別判定部 376 は、CPU 911 などの処理装置を用いて、S421 で照会データ取得部 351 が出力した日付時刻 741、送信元メールアドレス 746、送信先メールアドレス 747 を入力する。ドメイン種別判定部 376 は、CPU 911 などの処理装置を用いて、入力した送信元メールアドレス 746 及び送信先メールアドレス 747 それぞれのドメイン名を取得する。ドメイン種別判定部 376 は、CPU 911 などの処理装置を用いて、ドメイン種別記憶部 375 が記憶したドメイン種別テーブル 780 のなかから、取得した送信元メールアドレス 746 及び送信先メール

50

アドレス 747 のドメイン名を検索し、対応するドメイン種別 781 を取得する。ドメイン種別判定部 376 は、CPU 911 などの処理装置を用いて、送信元メールアドレス 746 に対応するドメイン種別 781 である送信元種別と、送信先メールアドレス 747 に対応するドメイン種別 781 である送信先種別とを出力する。

【0335】

S427 において、送受信種別判定部 378 は、CPU 911 などの処理装置を用いて、S426 でドメイン種別判定部 376 が出力したドメイン種別 781 (送信元種別及び送信先種別) を入力する。送受信種別判定部 378 は、CPU 911 などの処理装置を用いて、送受信種別テーブル記憶部 377 が記憶した送受信種別テーブル 790 のなかから、入力した送信元種別及び送信先種別に対応する送受信種別 791 を取得する。送受信種別判定部 378 は、CPU 911 などの処理装置を用いて、取得した送受信種別 791 を出力する。 10

その後、S424 へ進む。

【0336】

S424 において、照会結果通知部 353 は、CPU 911 などの処理装置を用いて、S422 で統合 ID 検索部 352 が出力した統合 ID 774 を入力する。照会結果通知部 353 は、CPU 911 などの処理装置を用いて、S427 で送受信種別判定部 378 が出力した送受信種別 791 を入力する。照会結果通知部 353 は、CPU 911 などの処理装置を用いて、入力した統合 ID 774 及び入力した送受信種別 791 に基づいて、統合 ID 照会結果 707 を生成する。照会結果通知部 353 は、CPU 911 などの処理装置を用いて、生成した統合 ID 照会結果 707 を出力する。 20

【0337】

図 24 に示した具体例を用いて、動作の流れを説明する。

【0338】

照会データ取得部 351 は、入力した統合 ID 照会データ 706 を解析して、日付時刻 741 「2005/03/28 10:01:47」と送信元メールアドレス 746 「Suzuki.Hanako@domain.co.jp」と送信先メールアドレス 747 「xyz@company.co.jp」とを取得し、ドメイン種別判定部 376 に対して出力する (図 25 の S421)。

【0339】

ドメイン種別判定部 376 は、照会データ取得部 351 が出力した日付時刻 741 「2005/03/28 10:01:47」と送信元メールアドレス 746 「Suzuki.Hanako@domain.co.jp」と送信先メールアドレス 747 「xyz@company.co.jp」とを入力し、解析して、送信元ドメイン名「domain.co.jp」と送信先ドメイン名「company.co.jp」とを取得する。ドメイン種別判定部 376 は、これをドメイン種別記憶部 375 が記憶したドメイン種別テーブル 780 と照合することにより、送信元種別「社内」と送信先種別「社外」とを取得し、出力する (図 25 の S426)。 30

【0340】

送受信種別判定部 378 は、ドメイン種別判定部 376 が出力した送信元種別「社内」と送信先種別「社外」とを入力し、送受信種別テーブル記憶部 377 が記憶した送受信種別テーブル 790 と照合することにより、送受信種別 791 「2」を取得し、出力する (図 25 の S427)。 40

【0341】

照会結果通知部 353 は、統合 ID 検索部 352 が出力した統合 ID と、送受信種別判定部 378 が出力した送受信種別 791 とを入力し、統合 ID 照会結果 707 を生成する。

この例において、照会結果通知部 353 は、統合 ID 照会データ 706 に含まれる個別 ID のリストと同じ順番で統合 ID を並べ、最後に送受信種別 791 を加えたリストを生成して、統合 ID 照会結果 707 としている。すなわち、この例に示した統合 ID 照会結 50

果 7 0 7 は、個別ユーザ I D 7 4 2 「s u z u k i」に対応する統合 I D は統合ユーザ I D 7 5 4 「U S E R 1 2 3 4 5 6」、個別機器 I D 7 4 3 「p c 0 0 1」に対応する統合 I D は統合機器 I D 7 5 5 「A S S E T 1 4 7 2 5 8」、送信元メールアドレス 7 4 6 「S u z u k i . H a n a k o @ d o m a i n . c o . j p」に対応する統合 I D は統合ユーザ I D 7 5 4 「U S E R 1 2 3 4 5 6」、送信先メールアドレス 7 4 7 「x y z @ c o m p a n y . c o . j p」に対応する統合 I D はドメイン種別 7 8 1 「社外」であり、送受信種別 7 9 1 は「2」であることを示している。

なお、送信先メールアドレス 7 4 7 「x y z @ c o m p a n y . c o . j p」は、社外のメールアドレスなので、個別 I D 記憶部 3 6 1 が記憶した個別 I D データベース 7 0 1 には、対応する統合 I D がない。しかし、社外のメールアドレスに対応する統合 I D がな
10
いのは当然なので、照会結果通知部 3 5 3 は、該当なし情報や異常発生情報ではなく、その個別 I D が「社外」のものであることを示すドメイン種別 7 8 1 を、統合 I D の代わりに返す。

【0 3 4 2】

なお、この実施の形態では、電子メールの送受信を記録したログを加工する場合を例に説明したが、データの移動を伴う操作であれば、電子メールの送受信に限らず、様々な操作を記憶したログを加工する構成としてもよい。

【0 3 4 3】

この実施の形態におけるログ管理システム 3 0 0（履歴管理装置）は、統合 I D 取得部 3 3 1（管理検索部）が、C P U 9 1 1 などの処理装置を用いて、データを移動した時刻
20
である移動時刻を示す情報である移動時刻情報を時刻情報として入力し、データを移動した移動元を示す情報である移動元情報と、データを移動した移動先を示す情報である移動先情報とを、対象情報として入力し、C P U 9 1 1 などの処理装置を用いて、入力した移動元情報に基づいて、移動元の種別を判別し、入力した移動先情報に基づいて、移動先の種別を判別し、判別した移動元の種別と判別した移動先の種別とに基づいて、データの移動方向を判別し、C P U 9 1 1 などの処理装置を用いて、判別したデータの移動方向を示す情報である移動方向情報を出力し、統合 I D 照会部 3 2 2（履歴加工部）は、更に、C P U 9 1 1 などの処理装置を用いて、移動時刻情報と移動元情報と移動先情報とを含む情報であるデータ移動履歴情報を、発生履歴情報として入力し、C P U 9 1 1 などの処理装置を用いて、入力したデータ移動履歴情報に含まれる移動時刻情報と移動元情報と移動先
30
情報とを、統合 I D 取得部 3 3 1 に対して出力し、C P U 9 1 1 などの処理装置を用いて、統合 I D 取得部 3 3 1 が出力した移動方向情報を入力し、C P U 9 1 1 などの処理装置を用いて、入力した移動方向情報を更に含む加工済履歴情報を出力することを特徴とする。

【0 3 4 4】

この実施の形態におけるログ管理システム 3 0 0 によれば、統合 I D 取得部 3 3 1 が、データの移動を伴う操作を記録したログについて、データの移動方向を判定し、判定した結果を示す移動方向情報を含む加工済ログを、統合 I D 照会部 3 2 2 が出力するので、例えば、のちに情報漏洩が発生した場合に、その情報漏洩の原因となる方向にデータを移動した操作を迅速に発見することができるという効果を奏する。
40

【0 3 4 5】

この実施の形態におけるログ管理システム 3 0 0（履歴管理装置）は、I D 管理 D B 3 3 3 が、C P U 9 1 1 などの処理装置を用いて、利用者を識別する情報である利用者識別情報を、統合ユーザ I D（管理識別情報）として含み、その利用者が所有する電子メールアドレスを個別ユーザ I D（対象識別情報）として含む管理情報 7 1 0 を磁気ディスク装置 9 2 0 などの記憶装置に記憶し、統合 I D 照会部 3 2 2 が、C P U 9 1 1 などの処理装置を用いて、電子メールを送信した時刻である送信時刻を示す情報である日付時刻 7 4 1（送信時刻情報）と、その電子メールの送信元を示す電子メールアドレスである送信元メールアドレス 7 4 6 と、その電子メールの送信先を示す電子メールアドレスである送信先メールアドレス 7 4 7 とを含む情報であるログレコード 7 4 0（メール送信履歴情報）を
50

、データ移動履歴情報として入力し、CPU911などの処理装置を用いて、入力したログレコード740に含まれる日付時刻741を統合ID取得部331が入力する移動時刻情報として出力し、入力したログレコード740に含まれる送信元メールアドレス746を統合ID取得部331が入力する移動元情報として出力し、入力したログレコード740に含まれる送信先メールアドレス747を統合ID取得部331が入力する移動先情報として出力し、統合ID照会部322が、CPU911などの処理装置を用いて、入力した送信元メールアドレス746に基づいて、送信元のドメイン種別781を判別し、入力した送信先メールアドレス747に基づいて、送信先のドメイン種別781を判別し、判別した送信元のドメイン種別781と判別した送信先のドメイン種別781とに基づいて、その電子メールの送受信方向を判別し、CPU911などの処理装置を用いて、判別したその電子メールの送受信方向を示す情報である送受信種別791（メール送受信方向情報）を移動方向情報として出力することを特徴とする。 10

【0346】

この実施の形態におけるログ管理システム300によれば、統合ID取得部331が、電子メールの送受信方向を示す送受信種別791を含むログについて、メールの送受信方向を判定し、判定した送受信方向を示す送受信種別791を含む加工済ログ705を、統合ID照会部322が出力するので、のちにメール送受信ログを検索する必要性が生じた場合に、探したいログを迅速に発見することができるという効果を奏する。

例えば、情報漏洩が発生した場合、膨大なメール送信記録の中から、社内から社外に送信したメール記録を、上記送受信種別をキーとして検索し、対象ログを絞り込むことができる。 20

【0347】

この実施の形態におけるログ加工装置110は、メール送信ログの送信元アドレスと送信先アドレスを読み取り、各々のドメインから社内、社外を判断し、メール送受信が、社内間、社内→社外、社外→社内、のいずれかを区別する判定手段により、その種別をログに反映し、また、ログはこの送受信種別を記録するためのカラムを持つフォーマットとすることを特徴とする。

【0348】

この実施の形態におけるログ加工装置110によれば、統合ユーザID、統合機器ID以外にメール送信を記録したログレコードに対する「送受信種別」をログに反映するので、ログの解析性が更に向上するという効果がある。 30

【0349】

実施の形態6.

実施の形態6について、図26を用いて説明する。

この実施の形態におけるログ管理システム300、ログ加工装置110、管理端末装置140の構成は、実施の形態5で説明したものと同様なので、ここでは説明を省略する。

【0350】

この実施の形態におけるドメイン種別判定部376は、ドメイン種別記憶部375が記憶したドメイン種別テーブル780のなかに、取得したドメイン名と完全に一致するドメイン名が発見できない場合に、ドメイン名の一部を用いてそのドメイン名の種別を推定し、推定したドメイン種別781を出力する。 40

【0351】

図26は、この実施の形態におけるドメイン種別記憶部375が記憶しているドメイン種別テーブル780の一例を示す図である。

【0352】

ドメイン種別テーブル780は、項目として、ドメイン種別781とドメイン名782と開始時刻784と終了時刻785とを有するテーブル形式のデータである。

この実施の形態におけるドメイン種別テーブル780は、一部に「*」を含むドメイン名782を有する。ここで、「*」は任意の文字列と一致するものとみなすことを示す文字の一例である。

また、この実施の形態におけるドメイン種別テーブル780は、ドメイン種別781として「社内」「社外」だけでなく、「取引先」「他社」「個人」などを細かく区別している。

【0353】

この例では、ドメイン名が「domain.co.jp」と完全に一致する場合は「社内」と判断し、ドメイン名が「customer1.co.jp」と完全に一致する場合は「取引先」と判断する。また、ドメイン名の後半が「.customer2.co.jp」と一致する場合も「取引先」と判断する。これにより、この取引先がドメイン名の前半部分が異なる複数のドメイン名を有している場合に、複数のドメイン名をすべて記憶しておく必要がない。

10

また、ドメイン名が一致するものがなく、最後が「.co.jp」で終わる場合には、「他社」と判断する。これは、会社が有するドメイン名が「.co.jp」で終わる場合が多いので、未知のドメイン名であっても「.co.jp」で終わる場合には、会社のドメインであると推定するものである。

同様に、ドメイン名が一致するものがなく、最後が「.ne.jp」で終わる場合には、「個人」と判断する。これは、個人向けのアドレスなどに「.ne.jp」で終わるアドレスがよく使われるので、未知のドメイン名であっても「.ne.jp」で終わる場合には、個人のドメインであると推定するものである。

【0354】

このように、未知のドメイン名である場合に、そのドメインの種別を推定する規則をドメイン種別記憶部375がドメイン種別テーブル780に記憶しておき、ドメイン種別判定部376は、CPU911などの処理装置を用いて、ドメイン種別781を推定する。

20

【0355】

これにより、業務に関するメール送信なのか、私用の可能性の高いメール送信なのかを容易に判別することができる。

例えば、メールの送信先が「個人」あるいは取引関係のない「他社」である場合は、私用メールである可能性が高い。

そこで、送受信種別テーブル記憶部377が記憶した送受信種別テーブル790において、メールの送信先が「個人」あるいは「他社」である場合には、特別な送受信種別791を割り当てておく。

30

【0356】

メールの送信先が「個人」あるいは「他社」である場合、送受信種別判定部378が、送受信種別テーブル790から、特別な送受信種別791を取得し、ログレコード加工部374が加工済ログ705に反映する。

これにより、のちに情報漏洩などの問題が発生してメール送信記録を調べる必要が生じた場合に、その特別な送受信種別791を含むログレコード750を検索すれば、問題発生の原因となった行為を迅速に発見することができる。

【0357】

また、ドメイン種別781が「社内」である場合、ドメイン種別判定部376は、ID管理DB333が記憶した個別IDデータベース701及び属性データベース702とを駆使して、ドメイン種別781を更に細かく判別する。

40

【0358】

統合ID検索部352は、CPU911などの処理装置を用いて、照会データ取得部351が出力した統合ID照会データ706に含まれる個別IDに対応する統合IDを検索し、出力する。

送信元メールアドレス746及び送信先メールアドレス747は、統合ID照会データ706に含まれる個別IDの一種であるから、統合ID検索部352が出力する統合IDのなかには、送信元メールアドレス746及び送信先メールアドレス747に対応する統合IDもある。

【0359】

50

ドメイン種別判定部 376 は、CPU 911 などの処理装置を用いて、統合 ID 検索部 352 が出力した統合 ID のうち、ドメイン種別 781 が「社内」である送信元メールアドレス 746 または送信先メールアドレス 747 に対応する統合 ID を入力する。ドメイン種別判定部 376 は、入力した統合 ID についての管理属性情報 720 の照会を要求する属性照会データ 802 を生成し、統合 ID 属性情報取得部 332 に対して出力する。

ドメイン種別判定部 376 が生成する属性照会データ 802 は、例えば、その統合 ID によって識別される従業員の所属部署の照会を要求するものである。

【0360】

統合 ID 属性情報取得部 332 は、CPU 911 などの処理装置を用いて、ドメイン種別判定部 376 が出力した属性照会データ 802 を入力し、ID 管理 DB 333 が記憶した属性データベース 702 を検索して、属性照会結果 803 を出力する。 10

ドメイン種別判定部 376 は、CPU 911 などの処理装置を用いて、統合 ID 属性情報取得部 332 が出力した属性照会結果 803 を入力する。ドメイン種別判定部 376 は、CPU 911 などの処理装置を用いて、入力した属性照会結果 803 を解析する。

【0361】

ドメイン種別判定部 376 は、属性照会結果 803 に含まれる管理属性情報 720 から、例えば、そのメールアドレスの所有者（従業員）の所属部署（「営業部」「人事部」など）を判別する。

ドメイン種別判定部 376 は、判別した所属部署をドメイン種別 781 として出力する。 20

【0362】

大きな会社であれば、同じ社内であっても互いに業務上なんのつながりもない部署が存在する場合がある。したがって、社内メールであっても、そのような部署間のメールは、私用メールである可能性が高い。

また、取引先とのメールであっても、例えば、資材部と資材納入業者との間のメールであれば正常な業務上のものである可能性が高いが、人事部と資材納入会社との間では通常業務に関するメールをやり取りする必要はないので、私用メールである可能性が高い。

【0363】

そこで、送受信種別テーブル記憶部 377 が記憶した送受信種別テーブル 790 において、このような私用メールである可能性が高い部署が相手である場合には、特別な送受信種別 791 を割り当てておく。 30

特別な送受信種別 791 は、やはり、加工済ログ 705 に反映されるので、のちに検索する際の助けとなる。

【0364】

なお、照会結果通知部 353 は、統合 ID 774 と送受信種別 791 だけでなく、ドメイン種別 781 も追加した統合 ID 照会結果 707 を生成することとしてもよい。その場合、ログレコード加工部 374 は、CPU 911 などの処理装置を用いて、統合 ID 照会結果 707 に含まれるドメイン種別 781 を、加工済ログ 705 に更に追加する。これにより、加工済ログ 705 の解析が更に容易になる。

【0365】

また、照会結果通知部 353 は、CPU 911 などの処理装置を用いて、送受信種別判定部 378 が判定した送受信種別 791 が、私用メールである可能性が高いことなどを示す特別な送受信種別 791 である場合には、更に異常発生情報を追加した統合 ID 照会結果 707 を生成してもよい。その場合、ログレコード加工部 374 は、CPU 911 などの処理装置を用いて、統合 ID 照会結果 707 に含まれる異常発生情報も、加工済ログ 705 に更に追加する。これにより、加工済ログ 705 の解析が更に容易になる。 40

【0366】

また、照会結果通知部 353 は、OS のログオン名などを個別ユーザ ID として取得した統合 ID 774 と、電子メールアドレスを個別ユーザ ID として取得した統合 ID 774 とが不一致の場合にも、統合 ID 照会結果 707 に更に異常発生情報を追加することと 50

してもよい。他人のメールアドレスを不正に使用しているなど、不正な操作が行われている可能性が高いからである。

【0367】

なお、警告出力部が、ログレコード加工部374が出力した加工済ログ705を入力し、異常発生情報が含まれている場合には、異常発生を示す警告をCRTなどの表示装置901やその他の出力装置に表示・出力することとしてもよい。

【0368】

この実施の形態におけるログ加工装置110は、統合ID取得部331（管理検索部）が、更に、CPU911などの処理装置を用いて、判別した送信先の種別に基づいて、その電子メールが不審メールであるか否かを判断し、CPU911などの処理装置を用いて、その電子メールが不審メールであると判断した場合に、異常発生を示す情報である異常発生情報を出力することの特徴とする。 10

【0369】

この実施の形態におけるログ加工装置110によれば、不審メールの可能性が高い電子メールの送受信記録に、統合ID照会部322が異常発生情報を付加して出力するので、のちに検索する必要がある場合に、膨大なログのなかから、不審メールの送受信を容易に見つけることができるという効果を奏する。

【0370】

この実施の形態におけるログ加工装置110は、メール送信が社内から社外であった場合、送信先が会社か個人かをドメイン文字列などにより区別し、その種別をログに反映することを特徴とする。 20

【0371】

この実施の形態におけるログ加工装置110は、社外のメールドメインを、あらかじめ、取引のある会社とそれ以外に分別しておき、メール送信が社内から社外であった場合、取引のある会社か否かを区別し、その種別をログに反映することを特徴とする。

【0372】

この実施の形態におけるログ加工装置110は、メール送受信が、社内間であった場合、所外宛てか、他部宛てか、部内宛てかを区別し、その種別をログに反映することを特徴とする。

【0373】

この実施の形態におけるログ加工装置110は、メール送信アドレス、受信アドレスに該当する統合ユーザIDをログに反映しておくことを特徴とする。 30

【0374】

これにより、業務に関するメール送信か、私用の可能性が高いメール送信かを区別することができる。

【0375】

また、取引のある会社宛てか否かを区別し、その種別もログに反映するように構成することにより、業務に関するメール送信か、不正宛先送信の可能性が高いメール送信かを区別することができる。

【0376】

更に、社内メールであっても、事業所間によるものか、同一事業所内の異なる部門によるものか、同一部門内によるものかを区別し、その種別もログに反映することにより、社内宛てメールの使用状況を把握することができ、業務上あまり関係の無い部門宛ての送信など、不審と思われるメール送信状況を把握することができる。 40

【0377】

また、送信先アドレスが社内宛ての場合、送信元アドレスと送信先アドレスに対応する統合ユーザIDを割り出し、それをそのままログに反映することにより、ある特定の個人間のメール送受信記録を容易に検索することができる。

【0378】

実施の形態7.

実施の形態 7 について、図 27～図 28 を用いて説明する。

【0379】

この実施の形態におけるログ管理システム 300、ログ加工装置 110、管理端末装置 140 の構成は、実施の形態 4 で説明したものと同様なので、ここでは説明を省略する。

【0380】

図 27 は、この実施の形態におけるログ加工装置 110 の内部ブロックの詳細な構成の一例を示す詳細ブロック図である。

なお、実施の形態 5 で説明したブロックと同様のブロックについては、同一の符号を付し、説明を省略する。

【0381】

統合 ID 照会部 322 は、ログレコード解析部 371、統合 ID 照会データ生成部 372、統合 ID 照会結果解析部 373、ログレコード加工部 374 などをも有する。

統合 ID 取得部 331 は、照会データ取得部 351、統合 ID 検索部 352、送受信種別判定部 378、照会結果通知部 353 などをも有する。

ID 管理 DB 333 は、個別 ID 記憶部 361、属性記憶部 362、送受信種別テーブル記憶部 377 などをも有する。

属性記憶部 362 は、CPU 911 などの処理装置を用いて、属性データベース 702 を磁気ディスク装置 920 などの記憶装置に記憶する。

【0382】

統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、個別 ID 記憶部 361 が記憶した個別 ID データベース 701 を検索し、照会データ取得部 351 が出力した統合 ID 照会データ 706 に含まれる個別 ID に対応する統合 ID を取得する。

統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、入力した統合 ID についての管理属性情報 720 を照会する属性照会データ 805 を生成する。

統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、生成した属性照会データ 805 を統合 ID 属性情報取得部 332 に対して出力する。

統合 ID 検索部 352 が生成する属性照会データ 805 は、例えば、その統合 ID によって識別されるコンピュータが接続しているネットワークの種別（機器接続ネットワーク）の照会を要求するものである。

【0383】

統合 ID 属性情報取得部 332 は、CPU 911 などの処理装置を用いて、統合 ID 検索部 352 が出力した属性照会データ 805 を入力する。統合 ID 属性情報取得部 332 は、CPU 911 などの処理装置を用いて、入力した属性照会データ 805 に基づいて、属性記憶部 362 が記憶した属性データベース 702 を検索する。統合 ID 属性情報取得部 332 は、CPU 911 などの処理装置を用いて、検索の結果取得した管理属性情報 720 を含む属性照会結果 806 を出力する。

【0384】

送受信種別判定部 378 は、CPU 911 などの処理装置を用いて、統合 ID 属性情報取得部 332 が出力した属性照会結果 806 を入力する。

送受信種別判定部 378 は、CPU 911 などの処理装置を用いて、入力した属性照会結果 806 を解析して、統合 ID についての管理属性情報 720 を取得する。

【0385】

送受信種別判定部 378 は、CPU 911 などの処理装置を用いて、取得した管理属性情報 720 に基づいて、送受信種別テーブル記憶部 377 が記憶した送受信種別テーブル 790 を検索し、送受信種別 791 を判定する。

送受信種別判定部 378 は、CPU 911 などの処理装置を用いて、判定した送受信種別 791 を出力する。

【0386】

この実施の形態のログ収集部 321 が収集するログ 704 は、利用者が、監視対象機器 500 であるコンピュータを用いて、ファイルのコピー、複製、移動、転送など（以下「

10

20

30

40

50

複製等」という)を行ったことを記録したログである。ログ収集部 321 が収集するログ 704 に含まれるログレコード 740 は、複製履歴情報の一例である。

この実施の形態のログ加工装置 110 は、ファイルの複製等をした場合に、複製元のファイルを記憶していた機器と、複製先のファイルを記憶した機器とから、送受信種別 791 を求めて、ログレコード 750 に追加する。

【0387】

図 28 は、この実施の形態における ID 管理装置 130 の各ブロックの間でやり取りされる情報の一例を示す図である。

【0388】

ログ収集部 321 が収集して出力したログ 704 に含まれる各ログレコード 740 に基づいて、統合 ID 照会データ生成部 372 が生成して出力する統合 ID 照会データ 706 は、日付時刻 741、個別ユーザ ID 742、複製元マシン名 841、複製先マシン名 842 などを含む。 10

日付時刻 741 は、利用者がファイルの複製等を行った時刻を示す情報（複製時刻情報）である。

個別ユーザ ID 742 は、ファイルの複製等を行った利用者を示す個別 ID である。

複製元マシン名 841 は、利用者が複製した元のファイルを記憶していたコンピュータなどの機器（ファイル記憶装置の一例）の個別 ID（複製元情報）である。

複製先マシン名 842 は、利用者が複製した結果できた新しいファイルを記憶したコンピュータなどの機器（ファイル記憶装置の一例）の個別 ID（複製先情報）である。 20

日付時刻 741 は、移動時刻情報の一例である。複製元マシン名 841 は、移動元情報の一例である。複製先マシン名 842 は、移動先情報の一例である。

【0389】

ログレコード解析部 371 は、CPU 911 などの処理装置を用いて、ログ 704 のログレコード 740 を解析し、日付時刻 741、個別ユーザ ID 742 などの個別 ID 761 を取得して出力する。

統合 ID 照会データ生成部 372 は、CPU 911 などの処理装置を用いて、ログレコード解析部 371 が出力した日付時刻 741、個別ユーザ ID 742 などの個別 ID 761 を取得する。統合 ID 照会データ生成部 372 は、CPU 911 などの処理装置を用いて、取得した日付時刻 741、個別ユーザ ID 742 などの個別 ID 761 に基づいて、 30
統合 ID 照会データ 706 を生成する。統合 ID 照会データ生成部 372 は、生成した統合 ID 照会データ 706 を出力する。

【0390】

照会データ取得部 351 は、CPU 911 などの処理装置を用いて、統合 ID 照会データ生成部 372 が出力した統合 ID 照会データ 706 を入力する。照会データ取得部 351 は、CPU 911 などの処理装置を用いて、入力した統合 ID 照会データ 706 を出力する。

【0391】

統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、照会データ取得部 351 が出力した統合 ID 照会データ 706 を入力する。統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、個別 ID 記憶部 361 が記憶した個別 ID データベース 701 を検索し、入力した統合 ID 照会データ 706 に含まれる個別ユーザ ID 742 などの個別 ID に対応する統合 ID を取得する。統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、照会結果通知部 353 に対して、取得した統合 ID を出力する。 40

【0392】

また、統合 ID 検索部 352 は、CPU 911 などの処理装置を用いて、取得した統合 ID 774 のうち、複製元マシン名 841 に対応する統合機器 ID と、複製先マシン名 842 に対応する統合機器 ID と（ファイル記憶装置識別情報の一例）について、その統合機器 ID によって識別される機器の設置種別を示す管理属性情報 720 を照会する属性照会データ 805 を生成する。

統合ID検索部352は、CPU911などの処理装置を用いて、生成した属性照会データ805を、統合ID属性情報取得部332に対して出力する。

【0393】

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、統合ID検索部352が出力した属性照会データ805を入力する。統合ID属性情報取得部332は、CPU911などの処理装置を用いて、属性記憶部362が記憶した属性データベース702を検索し、入力した属性照会データ805に含まれる統合IDについての管理属性情報720を取得する。統合ID属性情報取得部332は、CPU911などの処理装置を用いて、取得した管理属性情報720のうち、種別721が「設置種別」である管理属性情報720の属性722を取得する。統合ID属性情報取得部332は、CPU911などの処理装置を用いて、取得した属性722を含む属性照会結果806を出力する。 10

【0394】

送受信種別判定部378は、CPU911などの処理装置を用いて、統合ID属性情報取得部332が出力した属性照会結果806を入力する。送受信種別判定部378は、CPU911などの処理装置を用いて、入力した属性照会結果806を解析して、機器設置種別786を取得する。

【0395】

機器設置種別786とは、その機器の設置場所の種別を示す情報である。機器設置種別786は、種別721が「設置種別」である管理属性情報720のなかに含まれる属性722として、ID管理DB333の属性記憶部362が記憶している。 20

【0396】

例えば、社内のネットワーク（イントラネット）をインターネットなど社外のネットワークと接続する場合には、社内のネットワークが外部からの攻撃を受けて機密情報が流出することがないように、ファイアウォールなどを設けて、社内のネットワークを外部と隔離する構成とすることが多い。

また、ウェブサーバなど、外部からのアクセスを許す機器は、更にファイアウォールなどにより社内のネットワークと隔離されたDMZなどの領域に配置し、万が一、外部からの攻撃によりウェブサーバが乗っ取られるなどの事態が発生した場合でも、社内のネットワークに被害が及ばないように構成することがある。

【0397】

機器設置種別786とは、ファイアウォールなどにより隔離された各ネットワークの種別を示す情報である。特に、外部からの攻撃に対する安全性を基準に分類した種別であり、例えば、「イントラ」（イントラネット）、「DMZ」などである。 30

【0398】

送受信種別判定部378は、CPU911などの処理装置を用いて、送受信種別テーブル記憶部377が記憶した送受信種別テーブル790を検索し、取得した機器設置種別786に対応する送受信種別791を取得する。

送受信種別791は、ファイル移動方向情報の一例である。

送受信種別判定部378は、CPU911などの処理装置を用いて、取得した送受信種別791を出力する。 40

【0399】

照会結果通知部353は、CPU911などの処理装置を用いて、統合ID検索部352が出力した統合ユーザID754や統合機器ID755などの統合IDと、送受信種別判定部378が出力した送受信種別791とを入力する。照会結果通知部353は、CPU911などの処理装置を用いて、入力した統合ユーザID754や統合機器ID755などの統合IDと送受信種別791とに基づいて、統合ID照会結果707を生成する。統合ID照会結果解析部373は、生成した統合ID照会結果707を出力する。

【0400】

例えば、DMZに接続した機器は、たとえ外部に公開していない機器であっても、社内のネットワークに接続した機器よりも、安全性が低い。したがって、DMZに接続した機 50

器が記憶したファイル内の情報は、情報漏洩の危険が高いといえる。

したがって、一時的にせよ、DMZに接続した機器に複製を置いたファイルの内容が漏洩した場合、その間に受けた攻撃により、ファイルが盗まれた可能性がある。

【0401】

この実施の形態のログ加工装置110は、そのような安全性の低い機器にファイルを複製等した記録であるログレコード750に、送受信種別791をつけて区別することにより、情報漏洩などの原因究明のために加工済ログ705を検索する必要性が生じた場合に、情報漏洩などの原因である可能性の高い行為を絞り込むことを容易にするものである。

【0402】

図28に示した具体例を用いて、動作の流れを説明する。

10

【0403】

照会データ取得部351は、入力した統合ID照会データ706を解析して、日付時刻741「2005/03/29」、個別ユーザID742「tanaka」、複製元マシン名841「pc0013」、複製先マシン名842「webserver1」などの個別IDを取得し、出力する。

【0404】

統合ID検索部352は、照会データ取得部351が出力した日付時刻741、個別IDを入力し、個別ID記憶部361が記憶した個別IDデータベース701を検索して、入力した日付時刻741が示す時刻において、入力した個別IDに対応する統合IDを取得して、出力する。

20

【0405】

また、統合ID検索部352は、取得した統合IDのうち、複製元マシン名841に対応する統合ID774「ASSET963852」（複製元統合ID）と、複製先マシン名842に対応する統合ID774「ASSET183492」（複製先統合ID）とについて、日付時刻741「2005/03/29 14:23:50」が示す時刻における管理属性情報720「設置種別」の照会を要求する属性照会データ805を生成し、出力する。

【0406】

統合ID属性情報取得部332は、統合ID検索部352が出力した属性照会データ805を入力し、属性記憶部362が記憶した属性データベース702を検索して、属性照会結果806を出力する。

30

【0407】

送受信種別判定部378は、統合ID属性情報取得部332が出力した属性照会結果806を入力し、解析して、複製元統合ID「ASSET963852」の機器設置種別786「イントラ」（複製元種別）と、複製先統合ID「ASSET183492」の機器設置種別786「DMZ」（複製先種別）とを取得する。

【0408】

送受信種別判定部378は、取得した機器設置種別786（複製元種別「イントラ」、複製先種別「DMZ」）に基づいて、送受信種別テーブル記憶部377が記憶した送受信種別テーブル790を検索して、送受信種別791「12」を取得し、出力する。

40

【0409】

照会結果通知部353は、統合ID検索部352が出力した統合IDと、送受信種別判定部378が出力した送受信種別791「12」とを入力し、統合ID照会結果707を生成する。

【0410】

この例では、マシン名「pc0013」という個別機器IDで示される機器はイントラネットに接続されており、マシン名「webserver1」という個別機器IDで示される機器はDMZに接続されている。2005年3月29日14時23分50秒に、個別ユーザID「tanaka」で示される利用者が、「pc0013」から「webserver1」へファイルを複製したことが記録されている。

50

【0411】

のちに、そのファイルの内容が漏洩するなどして、加工済ログ705を検索する必要が生じた場合、そのファイルのファイル名を含み、送受信種別791「12」のログレコード750を検索すれば、このログレコード750がすぐに発見でき、その頃に「web server1」が外部から攻撃を受けた痕跡があるか否かを調べれば、迅速な原因究明が可能となる。

【0412】

この実施の形態におけるログ管理システム300（履歴管理装置）は、ID管理DB333（管理記憶部）が、CPU911などの処理装置を用いて、ファイルを記憶する機器（ファイル記憶装置）を識別する情報であるファイル記憶装置識別情報を、統合機器ID（管理識別情報）として含む管理情報710を磁気ディスク装置920などの記憶装置に記憶し、統合ID照会部322（履歴加工部）が、CPU911などの処理装置を用いて、ファイル記憶装置が記憶したファイルを他のファイル記憶装置に複製した時刻を示す日付時刻741（複製時刻情報）と、そのファイルを記憶していたファイル記憶装置を示す情報である複製元マシン名841（複製元情報）と、そのファイルを複製した他のファイル記憶装置を示す情報である複製先マシン名842（複製先情報）とを含む情報であるログレコード740（複製履歴情報）を、データ移動履歴情報として入力し、CPU911などの処理装置を用いて、入力したログレコード740に含まれる日付時刻741を統合ID取得部331が入力する移動時刻情報として入力し、入力したログレコード740に含まれる複製元マシン名841を統合ID取得部331が入力する移動元情報として出力し、入力したログレコード740に含まれる複製先マシン名842を統合ID取得部331が入力する移動先情報として出力し、統合ID取得部331は、CPU911などの処理装置を用いて、入力した複製元マシン名841に対応する統合機器ID（ファイル記憶装置識別情報）に基づいて、複製元種別796（ファイル記憶装置の種別）を判別し、入力した複製先マシン名842に対応する統合機器IDに基づいて、複製先種別797（他のファイル記憶装置の種別）を判別し、判別した複製元種別796と複製先種別797とに基づいて、ファイルの移動方向を判別し、CPU911などの処理装置を用いて、判別したファイルの移動方向を示す情報である送受信種別791（ファイル移動方向情報）を出力することを特徴とする。

【0413】

この実施の形態におけるログ管理システム300によれば、統合ID取得部331が、複製元マシン名841と複製先マシン名842とに基づいて送受信種別791を判別し、判別した送受信種別791を追加した加工済ログ705を、統合ID照会部322が生成して出力するので、加工済ログ705を蓄積しておけば、のちに情報漏洩などの問題が発生した場合に、膨大な加工済ログ705のなかから、問題発生の原因となった行為のログを見つけることが容易になるという効果を奏する。

【0414】

この実施の形態におけるログ加工装置110は、ファイルコピーログのコピー元マシンとコピー先マシンを読み取り、予め、各マシンの属性情報として、設置場所の属性（イントラネットか、DMZか）を統合機器IDに紐付けて管理しておき、イントラ間、イントラ→DMZ、DMZ→イントラ、DMZ間のいずれかを区別する判定手段により、その種別をログに反映することを特徴とする。

【0415】

これにより、例えば情報漏洩が発生した場合、膨大なファイルコピー・転送レコードの中から、イントラネットからDMZに流れたファイルの記録を、上記送受信種別をキーとして検索し、対象ログを絞り込むことができる。

【0416】

なお、送受信種別791（ファイル移動方向情報）は、イントラ・DMZ間の移動を区別するのではなく、例えば、事業所内、事業所間、部署内、部署間などを区別するものとしてもよい。

例えば、複製元マシン名 8 4 1 及び複製先マシン名 8 4 2 に対応する統合 I D について、統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、統合 I D 属性情報取得部 3 3 2 から、その機器の管理者に関する属性情報を取得し、更に、その管理者の所属に関する属性情報を取得する。統合 I D 照会部 3 2 2 は、C P U 9 1 1 などの処理装置を用いて、その機器の管理者の所属からその機器がどの事業所のどの部署で使用されているものであるかを判別し、ファイルの複製等が、事業場所間によるものか、同一事業所内の異なる部間によるものか、同一部内間によるものかを区別し、その種別もログに反映する。

【0 4 1 7】

この実施の形態におけるログ加工装置 1 1 0 は、ファイルコピーが、所外宛てか、他部宛てか、部内宛てかを区別し、その種別をログに反映することを特徴とする。 10

【0 4 1 8】

これにより、ファイルのコピー・転送状況を把握することができ、さらに、業務上あまり関係の無い部門宛てのコピー・転送など、不審と思われるファイルコピー・転送状況を把握することができるという効果を得ることができる。

【0 4 1 9】

なお、不審なファイルの複製等について、特別な送受信種別 7 9 1 を割り当てておき、ログレコード 7 5 0 に追加することとすれば、加工済ログ 7 0 5 を検索する際に、不審なファイルの複製等を容易に見つけることができる。更に、送受信種別判定部 3 7 8 が出力した送受信種別 7 9 1 が、不審なファイルの複製等に割り付けた特別な送受信種別 7 9 1 である場合、照会結果通知部 3 5 3 は、異常発生を示す異常発生情報を含む統合 I D 照会結果 7 0 7 を生成し、ログレコード加工部 3 7 4 は、入力した統合 I D 照会結果 7 0 7 に含まれる異常発生情報をログレコード 7 5 0 に追加しておけば、不審なファイルの複製等を見つけることが更に容易になる。 20

【0 4 2 0】

この実施の形態におけるログ管理システム 3 0 0（履歴管理装置）は、統合 I D 取得部 3 3 1（管理検索部）が、更に、C P U 9 1 1 などの処理装置を用いて、判別したファイルの移動方向に基づいて、不審な複製であるか否かを判断し、C P U 9 1 1 などの処理装置を用いて、不審な複製であると判断した場合に、異常発生を示す情報である異常発生情報を出力することを特徴とする。 30

【0 4 2 1】

この実施の形態におけるログ管理システム 3 0 0 によれば、不審な複製の可能性が高いログにあらかじめ異常発生情報を付加しておくので、のちに膨大なログのなかから、問題発生の原因を究明するために必要なログを発見することが容易になるという効果を奏する。

【0 4 2 2】

実施の形態 8.

実施の形態 8 について、図 2 9～図 3 0 を用いて説明する。

【0 4 2 3】

この実施の形態におけるログ管理システム 3 0 0、ログ加工装置 1 1 0、管理端末装置 1 4 0 の構成は、実施の形態 4 で説明したものと同様なので、ここでは説明を省略する。 40

【0 4 2 4】

図 2 9 は、この実施の形態におけるログ加工装置 1 1 0 の内部ブロックの詳細な構成の一例を示す詳細ブロック図である。

なお、実施の形態 7 で説明したブロックと同様のブロックについては、同一の符号を付し、説明を省略する。

【0 4 2 5】

統合 I D 照会部 3 2 2 は、ログレコード解析部 3 7 1、統合 I D 照会データ生成部 3 7 2、統合 I D 照会結果解析部 3 7 3、送受信種別テーブル記憶部 3 7 7、送受信種別判定部 3 7 8、ログレコード加工部 3 7 4 などを有する。 50

I D 管理 D B 3 3 3 は、個別 I D 記憶部 3 6 1、属性記憶部 3 6 2などを有する。

統合 I D 取得部 3 3 1 は、照会データ取得部 3 5 1、統合 I D 検索部 3 5 2、照会結果通知部 3 5 3などを有する。

【0 4 2 6】

統合 I D 照会データ生成部 3 7 2 は、C P U 9 1 1などの処理装置を用いて、統合 I D 照会データ 7 0 6を生成し、出力する。

【0 4 2 7】

統合 I D 照会データ生成部 3 7 2 が生成する統合 I D 照会データ 7 0 6 は、実施の形態 2 及び実施の形態 3 において説明したのと同様、1つのログ 7 0 4 のなかに同じ個別 I D 7 6 1 が複数回出てくる場合、それらを 1 つにまとめて照会する形式とする。これにより、ログ管理装置 1 2 0 と I D 管理装置 1 3 0 との間の通信量を削減できる。 10

統合 I D 照会データ生成部 3 7 2 がこのような形式の統合 I D 照会データ 7 0 6 を生成する手順については、実施の形態 2 で説明したので、ここでは説明を省略する。

【0 4 2 8】

照会データ取得部 3 5 1 は、C P U 9 1 1などの処理装置を用いて、統合 I D 照会データ生成部 3 7 2 が出力した統合 I D 照会データ 7 0 6 を入力する。照会データ取得部 3 5 1 は、入力した統合 I D 照会データ 7 0 6 を、統合 I D 検索部 3 5 2 に対して出力する。

【0 4 2 9】

統合 I D 検索部 3 5 2 は、C P U 9 1 1などの処理装置を用いて、照会データ取得部 3 5 1 が出力した統合 I D 照会データ 7 0 6 を入力する。統合 I D 検索部 3 5 2 は、C P U 9 1 1などの処理装置を用いて、入力した統合 I D 照会データ 7 0 6 に基づいて、個別 I D 記憶部 3 6 1 が記憶した個別 I D データベース 7 0 1 を検索し、統合 I D 照会データ 7 0 6 に含まれる個別 I D 7 6 1 に対応する統合 I D を取得する。統合 I D 検索部 3 5 2 は、C P U 9 1 1などの処理装置を用いて、取得した統合 I D と、照会された期間のうちその統合 I D と個別 I D とが対応している期間を示す期間情報とを、照会結果通知部 3 5 3 に対して出力する。 20

また、統合 I D 検索部 3 5 2 は、C P U 9 1 1などの処理装置を用いて、取得した統合 I D について、その統合 I D と個別 I D とが対応している期間における属性を照会する属性照会データ 8 0 5 を生成し、統合 I D 属性情報取得部 3 3 2 に対して出力する。

【0 4 3 0】

統合 I D 属性情報取得部 3 3 2 は、C P U 9 1 1などの処理装置を用いて、統合 I D 検索部 3 5 2 が出力した属性照会データ 8 0 5 を入力する。統合 I D 属性情報取得部 3 3 2 は、C P U 9 1 1などの処理装置を用いて、入力した属性照会データ 8 0 5 に基づいて、属性記憶部 3 6 2 が記憶した属性データベース 7 0 2 を検索し、属性照会データ 8 0 5 に含まれる統合 I D についての管理属性情報 7 2 0 を取得する。統合 I D 属性情報取得部 3 3 2 は、C P U 9 1 1などの処理装置を用いて、取得した管理属性情報 7 2 0 に基づいて、属性照会結果 8 0 6 を生成する。統合 I D 属性情報取得部 3 3 2 は、C P U 9 1 1などの処理装置を用いて、生成した属性照会結果 8 0 6 を、照会結果通知部 3 5 3 に対して出力する。 30

【0 4 3 1】

照会結果通知部 3 5 3 は、C P U 9 1 1などの処理装置を用いて、統合 I D 検索部 3 5 2 が出力した統合 I D などと、統合 I D 属性情報取得部 3 3 2 が出力した属性照会結果 8 0 6 とを入力する。照会結果通知部 3 5 3 は、C P U 9 1 1などの処理装置を用いて、入力した統合 I D や属性照会結果 8 0 6 に基づいて、統合 I D 照会結果 7 0 7 を生成する。照会結果通知部 3 5 3 は、C P U 9 1 1などの処理装置を用いて、生成した統合 I D 照会結果 7 0 7 を、統合 I D 照会結果解析部 3 7 3 に対して出力する。 40

【0 4 3 2】

統合 I D 照会結果解析部 3 7 3 は、C P U 9 1 1などの処理装置を用いて、照会結果通知部 3 5 3 が出力した統合 I D 照会結果 7 0 7 を入力する。統合 I D 照会結果解析部 3 7 3 は、C P U 9 1 1などの処理装置を用いて、入力した統合 I D 照会結果 7 0 7 を解析し 50

て、統合 I D や属性などを取得する。統合 I D 照会結果解析部 3 7 3 は、C P U 9 1 1 などの処理装置を用いて、取得した統合 I D や属性などを出力する。

【0 4 3 3】

送受信種別テーブル記憶部 3 7 7 は、C P U 9 1 1 などの処理装置を用いて、送信元種別及び送信先種別と、そのメールの送受信の種別との対応関係を示す送受信種別テーブルを、磁気ディスク装置 9 2 0 などの記憶装置に記憶している。

【0 4 3 4】

送受信種別判定部 3 7 8 は、C P U 9 1 1 などの処理装置を用いて、統合 I D 照会結果解析部 3 7 3 が出力した統合 I D によって識別される対象の属性を入力する。送受信種別判定部 3 7 8 は、C P U 9 1 1 などの処理装置を用いて、入力した属性に基づいて、送受信種別テーブル記憶部 3 7 7 が記憶した送受信種別テーブルを検索し、送受信種別 7 9 1 を判定する。送受信種別判定部 3 7 8 は、C P U 9 1 1 などの処理装置を用いて、判定した送受信種別 7 9 1 を出力する。

10

【0 4 3 5】

ログレコード加工部 3 7 4 は、C P U 9 1 1 などの処理装置を用いて、ログ収集部 3 2 1 が出力したログ 7 0 4 を入力する。ログレコード加工部 3 7 4 は、C P U 9 1 1 などの処理装置を用いて、統合 I D 照会結果解析部 3 7 3 が出力した統合 I D と、送受信種別判定部 3 7 8 が出力した送受信種別 7 9 1 とを入力する。ログレコード加工部 3 7 4 は、入力した統合 I D や送受信種別 7 9 1 を、入力したログ 7 0 4 に追加して、加工済ログ 7 0 5 を生成し、出力する。

20

【0 4 3 6】

この実施の形態におけるログ管理装置 1 2 0 は、統合 I D 照会データ生成部 3 7 2 が個別 I D に対応する統合 I D を照会する際に、統合 I D だけでなく、その統合 I D によって識別される対象の属性についても、同時に照会するものである。これにより、ログ管理装置 1 2 0 と I D 管理装置 1 3 0 との間の通信量を更に削減することができる。

【0 4 3 7】

図 3 0 は、この実施の形態における I D 管理装置 1 3 0 の各ブロックの間でやり取りされる情報の一例を示す図である。

【0 4 3 8】

統合 I D 照会データ生成部 3 7 2 が生成する統合 I D 照会データ 7 0 6 は、個別 I D 7 6 1、開始時刻 7 6 2、終了時刻 7 6 3、照会属性 7 6 8 からなる照会条件のリストである。この例では、統合 I D 照会データ 7 0 6 はテキストデータであり、1 行が 1 つの照会条件を示す。1 つの照会条件は、個別 I D 7 6 1、開始時刻 7 6 2、終了時刻 7 6 3、照会属性 7 6 8 を「，」で区切って並べた C S V 形式のリストである。

30

照会属性 7 6 8 は、統合 I D を照会する際に同時に照会する属性の種別を示す情報である。

【0 4 3 9】

この図の例における統合 I D 照会データ 7 0 6 の 1 行目は、個別 I D 7 6 1 「p c 0 0 1」について、「2 0 0 5 年 3 月 3 1 日 1 1 時 2 4 分 3 2 秒」から「2 0 0 5 年 6 月 1 5 日 1 3 時 5 2 分 2 3 秒」までの期間において対応する統合 I D を照会することを示している。また、その統合 I D によって識別される対象について、同じ期間における属性「設置種別」を同時に照会することを示している。

40

【0 4 4 0】

統合 I D 検索部 3 5 2 が生成する属性照会データ 8 0 5 は、統合 I D 8 5 1、開始時刻 8 5 2、終了時刻 8 5 3、照会属性 8 5 4 からなる属性照会条件のリストである。この例では、属性照会データ 8 0 5 はテキストデータであり、1 行が 1 つの属性照会条件を示す。1 つの属性照会条件は、統合 I D 8 5 1、開始時刻 8 5 2、終了時刻 8 5 3、照会属性 8 5 4 を「，」で区切って並べた C S V 形式のリストである。

【0 4 4 1】

統合 I D 8 5 1 は、照会対象である統合 I D を示す情報である。

50

開始時刻 8 5 2 及び終了時刻 8 5 3 は、属性を照会する期間を示す情報である。開始時刻 8 5 2 は、属性を照会する期間の開始時刻を示す情報である。終了時刻 8 5 3 は、属性を照会する期間の終了時刻を示す情報である。

照会属性 8 5 4 は、照会する属性の種別を示す情報である。

【0 4 4 2】

この図の例における属性照会データ 8 0 5 の 1 行目は、統合 I D 8 5 1 「A S S E T 9 7 3 2 0 1」によって識別される対象について、「2 0 0 5 年 3 月 3 1 日 1 1 時 2 4 分 3 2 秒」から「2 0 0 5 年 3 月 3 1 日 2 3 時 5 9 分 5 9 秒」までの期間における属性「設置種別」を照会することを示している。

【0 4 4 3】

統合 I D 検索部 3 5 2 は、C P U 9 1 1 などの処理装置を用いて、入力した統合 I D 照会データ 7 0 6 に基づいて、個別 I D 記憶部 3 6 1 が記憶した個別 I D データベース 7 0 1 を検索して、個別 I D 7 6 1 に対応する統合 I D と、その統合 I D とその個別 I D 7 6 1 とが対応する期間の開始時刻及び終了時刻とを取得する。

統合 I D 検索部 3 5 2 は、C P U 9 1 1 などの処理装置を用いて、取得した統合 I D と、開始時刻及び終了時刻とに基づいて、属性照会データ 8 0 5 を生成し、出力する。

統合 I D 検索部 3 5 2 が生成する属性照会データ 8 0 5 のうち、統合 I D 8 5 1 は、取得した統合 I D である。

開始時刻 8 5 2 は、取得した開始時刻である。ただし、取得した開始時刻が統合 I D 照会データ 7 0 6 の開始時刻 7 6 2 より前である場合、統合 I D 検索部 3 5 2 は、統合 I D 照会データ 7 0 6 の開始時刻 7 6 2 を、開始時刻 8 5 2 とする。

終了時刻 8 5 3 は、取得した終了時刻である。ただし、取得した終了時刻が統合 I D 照会データ 7 0 6 の終了時刻 7 6 3 より後である場合、統合 I D 検索部 3 5 2 は、統合 I D 照会データ 7 0 6 の終了時刻 7 6 3 を、終了時刻 8 5 3 とする。

照会属性 8 5 4 は、統合 I D 照会データ 7 0 6 の照会属性 7 6 8 である。

【0 4 4 4】

例えば、この図の例に示した統合 I D 照会データ 7 0 6 に基づいて、統合 I D 検索部 3 5 2 が個別 I D データベース 7 0 1 を検索した結果、個別 I D 7 6 1 「p c 0 0 1」は、「2 0 0 5 年 3 月 3 1 日 1 1 時 2 4 分 3 2 秒」から「2 0 0 5 年 3 月 3 1 日 2 3 時 5 9 分 5 9 秒」までの期間において、統合 I D 「A S S E T 9 7 3 2 0 1」に対応し、「2 0 0 5 年 4 月 1 日 0 時 0 分 0 秒」から「2 0 0 5 年 6 月 1 5 日 1 3 時 5 2 分 2 3 秒」までの期間において、統合 I D 「A S S E T 4 2 4 6 1 2」に対応することがわかったとする。同様に、個別 I D 7 6 1 「p c 0 0 2」は、照会された全期間において、統合 I D 「A S S E T 3 5 8 4 6 9」に対応することがわかったとする。

統合 I D 検索部 3 5 2 は、C P U 9 1 1 などの処理装置を用いて、検索の結果取得したこれらの情報に基づいて、この図の例に示した属性照会データ 8 0 5 を生成する。

【0 4 4 5】

統合 I D 属性情報取得部 3 3 2 が生成する属性照会結果 8 0 6 は、統合 I D 8 6 1、開始時刻 8 6 2、終了時刻 8 6 3、属性内容 8 6 4 からなる照会結果のリストである。この例では、属性照会結果 8 0 6 はテキストデータであり、1 行が 1 つの照会結果を示す。1 つの照会結果は、統合 I D 8 6 1、開始時刻 8 6 2、終了時刻 8 6 3、属性内容 8 6 4 を「，」で区切って並べた C S V 形式のリストである。

【0 4 4 6】

統合 I D 8 6 1 は、照会された統合 I D を示す情報である。

開始時刻 8 6 2 及び終了時刻 8 6 3 は、統合 I D 8 6 1 によって識別される対象がその属性を有していた期間を示す情報である。開始時刻 8 6 2 は、その期間の開始時刻を示す情報である。終了時刻 8 6 3 は、その期間の終了時刻を示す情報である。

属性内容 8 6 4 は、統合 I D 8 6 1 によって識別される対象が、開始時刻 8 6 2 及び 8 終了時刻 8 6 3 が示す期間において有する、照会された種別の属性の内容を示す情報である。

10

20

30

40

50

【0447】

この図の例における属性照会結果806の1行目は、統合ID861「ASSET973201」によって識別される対象は、「2005年3月31日11時24分32秒」から「2005年3月31日23時59分59秒」までの期間において、「設置種別」が「イントラ」であったことを示している。

【0448】

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、統合ID検索部352が出力した属性照会データ805を入力する。統合ID属性情報取得部332は、CPU911などの処理装置を用いて、入力した属性照会データ805に持ついて、属性記憶部362が記憶した属性データベース702を検索し、統合ID851によって識別される対象の属性の内容と、その対象がその属性を有する期間の開始時刻及び終了時刻とを取得する。

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、取得した属性の内容と、開始時刻及び終了時刻に基づいて、属性照会結果806を生成し、出力する。

統合ID属性情報取得部332が生成する属性照会結果806のうち、統合ID861は、属性照会データ805の統合ID851である。

開始時刻862は、取得した開始時刻である。ただし、取得した開始時刻が属性照会データ805の開始時刻852より前である場合、統合ID属性情報取得部332は、属性照会データ805の開始時刻852を、開始時刻862とする。

終了時刻863は、取得した終了時刻である。ただし、取得した終了時刻が属性照会データ805の終了時刻853より後である場合、統合ID属性情報取得部332は、属性照会データ805の終了時刻853を、終了時刻863とする。

属性内容864は、取得した属性の内容である。

【0449】

例えば、この図の例に示した属性照会データ805に基づいて、統合ID属性情報取得部332が属性データベース702を検索した結果、統合ID851「ASSET973201」によって識別される対象は、照会された全期間において、「設置種別」が「イントラ」であることがわかったとする。また、統合ID851「ASSET424612」によって識別される対象は、「2005年4月1日0時0分0秒」から「2005年5月31日23時59分59秒」までの期間において、「設置種別」が「イントラ」であり、「2005年6月1日0時0分0秒」から「2005年6月15日13時52分23秒」までの期間において、「設置種別」が「DMZ」であることがわかったとする。また、統合ID851「ASSET358469」によって識別される対象は、「2005年3月30日12時12分47秒」から「2005年4月30日23時59分59秒」までの期間において、「設置種別」が「DMZ」であり、「2005年5月1日0時0分0秒」から「2005年5月20日8時6分11秒」までの期間において、「設置種別」が「イントラ」であることがわかったとする。

統合ID属性情報取得部332は、CPU911などの処理装置を用いて、検索の結果取得したこれらの情報に基づいて、この図の例に示した属性照会結果806を生成する。

【0450】

照会結果通知部353が生成する統合ID照会結果707は、実施の形態3において図19で説明した統合ID照会結果707に、統合ID属性情報取得部332が生成した属性照会結果806を加えたものである。

統合ID照会結果707は、個別ID771、開始時刻772、終了時刻773、統合ID774からなる統合IDの照会結果と、統合ID861、開始時刻862、終了時刻863、属性内容864からなる属性の照会結果とのリストである。この例では、統合ID照会結果707はテキストデータであり、1行が1つの照会結果を示す。

統合IDの照会結果は、個別ID771、開始時刻772、終了時刻773、統合ID774を「，」で区切って並べたCSV形式のリストである。

10

20

30

40

50

属性の照会結果は、統合 I D 8 6 1、開始時刻 8 6 2、終了時刻 8 6 3、属性内容 8 6 4 を「,」で区切って並べた C S V 形式のリストである。属性の照会結果は、属性照会結果 8 0 6 に含まれる照会結果と同じである。

【0 4 5 1】

照会結果通知部 3 5 3 は、C P U 9 1 1 などの処理装置を用いて、統合 I D 検索部 3 5 2 が出力した個別 I D、その個別 I D に対応する統合 I D、その統合 I D と個別 I D とが対応する期間の開始時刻及び終了時刻を入力する。また、照会結果通知部 3 5 3 は、C P U 9 1 1 などの処理装置を用いて、統合 I D 属性情報取得部 3 3 2 が出力した属性照会結果 8 0 6 を入力する。

照会結果通知部 3 5 3 は、C P U 9 1 1 などの処理装置を用いて、入力した個別 I D、統合 I D、開始時刻、終了時刻に基づいて、統合 I D の照会結果を生成する。すなわち、照会結果通知部 3 5 3 は、C P U 9 1 1 などの処理装置を用いて、個別 I D、開始時刻、終了時刻、統合 I D を「,」で区切って並べたテキストデータを生成する。 10

照会結果通知部 3 5 3 は、C P U 9 1 1 などの処理装置を用いて、生成した統合 I D の照会結果の次に、その統合 I D についての属性の照会結果を挿入する。

照会結果通知部 3 5 3 は、このようにして、統合 I D 照会結果 7 0 7 を生成する。

【0 4 5 2】

なお、この例では、統合 I D の照会結果と属性の照会結果とを 1 つに結合して統合 I D 照会結果 7 0 7 として出力する構成としているが、統合 I D 照会結果 7 0 7 は統合 I D の照会結果のみから生成し、それとは別に、属性照会結果 8 0 6 を出力する構成としてもよい。 20

【0 4 5 3】

照会結果通知部 3 5 3 が生成して出力した統合 I D 照会結果 7 0 7 は、統合 I D 照会結果解析部 3 7 3 が C P U 9 1 1 などの処理装置を用いて入力する。統合 I D 照会結果解析部 3 7 3 は、入力した統合 I D 照会結果 7 0 7 を解析して、統合 I D や属性などの情報を取得する。統合 I D 照会結果解析部 3 7 3 が取得した統合 I D などの情報は、ログレコード加工部 3 7 4 がログ 7 0 4 に追加して、加工済ログ 7 0 5 を生成する。

【0 4 5 4】

この例では、統合 I D 照会結果解析部 3 7 3 が取得した属性を、そのままログ 7 0 4 に追加するのではなく、取得した属性に基づいて、送受信種別判定部 3 7 8 が送受信種別を判定し、判定した送受信種別をログレコード加工部 3 7 4 がログ 7 0 4 に追加する構成としている。 30

【0 4 5 5】

送受信種別判定部 3 7 8 が送受信種別を判定する手順については、実施の形態 7 で説明したものと同様なのでここでは説明を省略する。

【0 4 5 6】

このように、ログ管理装置 1 2 0 が I D 管理装置 1 3 0 に対して統合 I D を照会する際、同時にその統合 I D によって識別される対象の属性についても照会することにより、統合 I D によって識別される対象の属性を、ログ 7 0 4 に追加して、加工済ログ 7 0 5 を生成することができる。これにより、加工済ログ 7 0 5 を検索する際に、属性を直接検索することができ、検索の効率が高くなるという効果を奏する。 40

【0 4 5 7】

また、属性の照会を、統合 I D の照会と同時に行うので、ログ管理装置 1 2 0 と I D 管理装置 1 3 0 との間の通信量を少なくすることができるという効果を奏する。

【0 4 5 8】

また、I D 管理装置 1 3 0 が生成して、ログ管理装置 1 2 0 に対して出力する統合 I D 照会結果 7 0 7 は、統合 I D の照会結果のすぐあとにその統合 I D についての属性の照会結果がついているので、個別 I D から対応する属性を容易に見つけることができ、ログレコード加工部 3 7 4 がログ 7 0 4 を加工する処理を速くすることができるという効果を奏する。

【0459】

また、照会した属性をそのままログ704に追加するのではなく、照会した属性に基づいて判別した送受信種別をログ704に追加するので、のちに加工済ログ705を検索する際の検索効率が高くなるという効果を奏する。

【0460】

実施の形態9.

実施の形態9について、図31を用いて説明する。

【0461】

この実施の形態におけるログ管理システム300、ログ加工装置110、管理端末装置140の構成は、実施の形態4で説明したものと同様なので、ここでは説明を省略する。 10

【0462】

図31は、この実施の形態におけるログ加工装置110の内部ブロックの詳細な構成の一例を示す詳細ブロック図である。

なお、実施の形態5で説明したブロックと同様のブロックについては、同一の符号を付し、説明を省略する。

【0463】

統合ID照会部322は、ログレコード解析部371、統合ID照会データ生成部372、統合ID照会結果解析部373、ログレコード加工部374などを有する。

ID管理DB333は、個別ID記憶部361、URL種別記憶部385、送受信種別テーブル記憶部377などを有する。 20

統合ID取得部331は、照会データ取得部351統合ID検索部352、URL種別判定部386、送受信種別判定部378、照会結果通知部353などを有する。

【0464】

この実施の形態におけるログ収集部321が収集するログは、インターネット上のサイトに対するファイルのアップロードやインターネット上のサイトからのファイルのダウンロードを記録したものである。

ログ704のログレコード740は、アップロードあるいはダウンロードしたサイトのURL(Uniform Resource Locator)を示す情報を含んでいる。

【0465】

ログレコード解析部371は、CPU911などの処理装置を用いて、ログ収集部321が出力したログ704のログレコード740を解析して、URL846を取得し、出力する。統合ID照会データ生成部372は、CPU911などの処理装置を用いて、ログレコード解析部371が出力したURL846を含む統合ID照会データ706を生成し、出力する。照会データ取得部351は、CPU911などの処理装置を用いて、統合ID照会データ706に含まれるURL846を取得し、URL種別判定部386に対して出力する。 30

【0466】

URL種別記憶部385は、CPU911などの処理装置を用いて、URLとその種別との対応を示すURL種別テーブルを、磁気ディスク装置920などの記憶装置に記憶している。 40

【0467】

URLの種別とは、例えば、そのURLが示すサイトへのファイルのアップロードやダウンロードを許可するか否かを示す情報である。あるいは、ダウンロードすることが危険なソフトウェア(ウィニーなどセキュリティ上の問題を引き起こす可能性のあるソフトウェアなど)が置かれているサイトであるか否かを示すものであってもよい。

【0468】

URL種別判定部386は、CPU911などの処理装置を用いて、照会データ取得部351が出力したURL846を入力する。

URL種別判定部386は、CPU911などの処理装置を用いて、URL種別記憶部 50

385が記憶したURL種別テーブルを検索し、入力したURL846の種別を取得する。

URL種別判定部386は、CPU911などの処理装置を用いて、取得したURL種別799を出力する。

【0469】

送受信種別判定部378は、CPU911などの処理装置を用いて、URL種別判定部386が出力したURL種別799を入力する。

送受信種別判定部378は、CPU911などの処理装置を用いて、入力したURL種別799と、アップロードかダウンロードかの区別に基づいて、送受信種別テーブル記憶部377を検索し、送受信種別791を取得する。

送受信種別判定部378は、CPU911などの処理装置を用いて、取得した送受信種別791を出力する。

【0470】

照会結果通知部353は、CPU911などの処理装置を用いて、統合ID検索部352が出力した統合IDと、送受信種別判定部378が出力した送受信種別791とを入力する。照会結果通知部353は、CPU911などの処理装置を用いて、入力した統合ID774と送受信種別791とに基づいて、統合ID照会結果707を生成し、出力する。

【0471】

この実施の形態におけるログ加工装置110は、ファイルのウェブアップロード操作において、予めアップロードを許可するURLをリストアップしておき、リストにあるURLか逸脱したURLかを区別する情報をログに反映することを特徴とする。

【0472】

ファイルのウェブアップロード操作において、予めアップロードを許可するURLをリストアップしておき、リストにあるURLか逸脱したURLかを区別する情報をログに反映することにより、許可していない不正なURLへのファイルアップロード操作を把握することができる。

【0473】

この実施の形態におけるログ加工装置110は、ファイルのウェブダウンロード操作において、特定のURLをリストアップしておき、リストにあるURLからのダウンロードか否かを区別する情報をログに反映することを特徴とする。

【0474】

ファイルのウェブダウンロード操作において、特定のURLをリストアップしておき、リストにあるURLからのダウンロードか否かを区別する情報をログに反映することにより、セキュリティ上好ましくないソフトウェアをダウンロードした可能性のあるログを把握することができる。

【0475】

以上説明したログ加工装置は、企業情報システムにおいて、セキュリティ問題が発生した際のインシデント解析などに際に、ログの解析性を向上させることを目的とした用途に有用である。

【0476】

以上説明したログ加工装置は、ネットワークに接続された機器が出力するログを収集し、蓄積する前に、ログレコードの発生に関与したユーザや機器に対し、それらを一意に特定する統合IDを反映したり、情報移動に関するログレコードに対し、情報の送信元と送信先の関係から見出される情報移動の意味を示す送受信種別情報を反映することで、後のログ解析時にログの解析性を向上させることができる。

【0477】

以上説明したログ加工装置は、内部にログ管理装置とID管理装置を備え、

ログ管理装置は、さらにその内部にログを収集するログ収集部と、統合IDをID管理装置に照会し、照会結果をログに反映する統合ID照会部と、統合IDを反映したログを

10

20

30

40

50

ログDBに蓄積するログ蓄積部と、蓄積したログの検索を可能とするログ検索部、及びログDBを備え、

ID管理装置は、さらにその内部にID管理DBから統合IDを取得する統合ID取得部と、同じくID管理DBから、統合IDに付随する属性情報を取得する統合ID属性情報取得部、及びID管理DBを備えている。

【0478】

このように、ログ蓄積時に、後のログ解析に資する情報を予めログに反映しておくことによりログの解析性を向上させることができる。

【0479】

また、統合ID以外にも、後の解析に役立つ各種情報を、蓄積前にログに予め反映しておくことによりログの解析性を高めることができる。 10

【0480】

以上説明したログ加工装置は、ログを収集・蓄積する機能を持つ「ログ管理装置」と、ログに記録される各種ユーザIDや機器IDを、ユーザや機器を一意に特定する統合IDと紐付けて管理する「ID管理装置」から構成されることを特徴とする。

【0481】

ログ管理装置は、ログを蓄積する直前に、ログレコードに含まれるユーザアカウント名やアプリケーションごとのユーザID、マシン名やIPアドレスなど、ユーザや機器に割り付けられたログ固有の個別IDから、ログレコードが記録された時刻とともに、ユーザや機器を一意に特定する統合IDをID管理装置に照会し、統合IDをログレコードに反映することを特徴とする。 20

【0482】

ID管理装置は、ログ固有の個別IDと統合IDの関係、及び、ユーザであれば所属部署名、機器であれば設置場所などを例とした、統合IDに付随する属性情報を、時間情報とともに過去に遡って管理することを特徴とする。

【0483】

ログ管理装置は、統合IDの照会のみならず、更に、ログレコードがメール送信やデータコピーなど、情報の移動を示す場合、情報の送信元と送信先の属性、及びそれらの関係から抽出・分類される情報移動の意味（例えば、社内から社外へのメール送信、イントラネットからDMZへのデータ移動など）をID管理装置に照会し、蓄積前にログに反映することを特徴とする。 30

【0484】

ID管理装置は、個別IDと統合ID及び付随する属性情報の時系列管理のみならず、情報の送信元と送信先の関係から抽出・分類される情報移動の意味を管理することを特徴とするものである。

【0485】

このように、ログ蓄積時に、ログごとに固有のユーザIDや機器IDを、過去に遡って統合IDに変換しログに反映するため、特定のユーザ、特定の機器に関連する、複数のログに分散したログレコードを、統合IDをキーにして一括検索することができる。

【0486】

更に、情報移動の意味（社内から社外へのメール送信や、イントラネットからDMZへのデータ移動、など）をキーにして、それに該当するログレコードを、一括検索することができる。 40

【図面の簡単な説明】

【0487】

【図1】実施の形態1における履歴管理装置100の外観の一例を示す図。

【図2】実施の形態1における履歴管理装置100のハードウェア資源の一例を示す図。

【図3】実施の形態1における履歴管理装置100の機能ブロックの構成の一例を示すブロック構成図。

【図4】実施の形態1におけるID管理装置130の詳細の一例を示す詳細ブロック図。 50

【図 5】実施の形態 1 における管理検索部 1 3 2 が管理情報 6 1 0 を検索する管理検索処理の流れの一例を示すフローチャート図。

【図 6】実施の形態 1 における履歴加工部 1 2 2 の詳細の一例を示す詳細ブロック図。

【図 7】実施の形態 1 における履歴加工部 1 2 2 が履歴情報を加工する履歴加工処理の流れの一例を示すフローチャート図。

【図 8】実施の形態 2 における履歴加工部 1 2 2 のブロック構成の一例を示す詳細ブロック図。

【図 9】実施の形態 2 における管理検索部 1 3 2 が管理情報 6 1 0 を検索する管理検索処理の流れの一例を示すフローチャート図。

【図 10】実施の形態 2 における履歴加工部 1 2 2 が履歴情報を加工する履歴加工処理の流れの一例を示すフローチャート図（1）。 10

【図 11】実施の形態 2 における履歴加工部 1 2 2 が履歴情報を加工する履歴加工処理の流れの一例を示すフローチャート図（2）。

【図 12】実施の形態 3 におけるログ加工装置 1 1 0 の構成の一例を示すブロック図。

【図 13】実施の形態 3 におけるログ収集部 3 2 1 が収集するログ 7 0 4 の一例を示す図。

【図 14】実施の形態 3 における統合 I D 照会部 3 2 2 が加工して、統合 I D を反映した加工済ログ 7 0 5 の一例を示す図。

【図 15】実施の形態 3 における I D 管理 D B 3 3 3 が記憶する属性データベース 7 0 2 の内容の一例を示す図。 20

【図 16】実施の形態 3 における I D 管理 D B 3 3 3 が記憶する個別 I D データベース 7 0 1 の内容の一例を示す図。

【図 17】実施の形態 3 における I D 管理 D B 3 3 3 が記憶した個別 I D データベース 7 0 1 及び属性データベース 7 0 2 によって示される統合 I D と個別 I D、属性との間の関係を視覚的に表現した概念図。

【図 18】実施の形態 3 におけるログ加工装置 1 1 0 がログ 7 0 4 を加工するログ加工処理の流れの一例を示すフローチャート図。

【図 19】実施の形態 3 におけるログ管理装置 1 2 0 の各機能ブロックの間でやり取りする情報の一例を示す図。

【図 20】実施の形態 3 における統合 I D 照会部 3 2 2 が統合 I D 照会データ 7 0 6 を生成する統合 I D 照会データ生成処理の流れの一例を示すフローチャート図。 30

【図 21】実施の形態 3 における統合 I D 照会部 3 2 2 が統合 I D 照会結果 7 0 7 に基づいてログ 7 0 4 を加工し、加工済ログ 7 0 5 を生成する統合 I D 照会結果反映処理の流れの一例を示すフローチャート図。

【図 22】実施の形態 4 における検索結果表示部 1 4 2 がログを照会するログ照会処理の流れの一例を示すフローチャート図。

【図 23】実施の形態 5 におけるログ加工装置 1 1 0 の内部ブロックの詳細な構成の一例を示す詳細ブロック図。

【図 24】実施の形態 5 における I D 管理装置 1 3 0 の各ブロックの間でやり取りされる情報の一例を示す図。 40

【図 25】実施の形態 5 における I D 管理装置 1 3 0 が統合 I D を検索する I D 検索処理の流れの一例を示すフローチャート図。

【図 26】実施の形態 6 におけるドメイン種別記憶部 3 7 5 が記憶しているドメイン種別テーブル 7 8 0 の一例を示す図。

【図 27】実施の形態 7 におけるログ加工装置 1 1 0 の内部ブロックの詳細な構成の一例を示す詳細ブロック図。

【図 28】実施の形態 7 における I D 管理装置 1 3 0 の各ブロックの間でやり取りされる情報の一例を示す図。

【図 29】実施の形態 8 におけるログ加工装置 1 1 0 の内部ブロックの詳細な構成の一例を示す詳細ブロック図。 50

【図 30】実施の形態 8 における I D 管理装置 130 の各ブロック間でやり取りされる情報の一例を示す図。

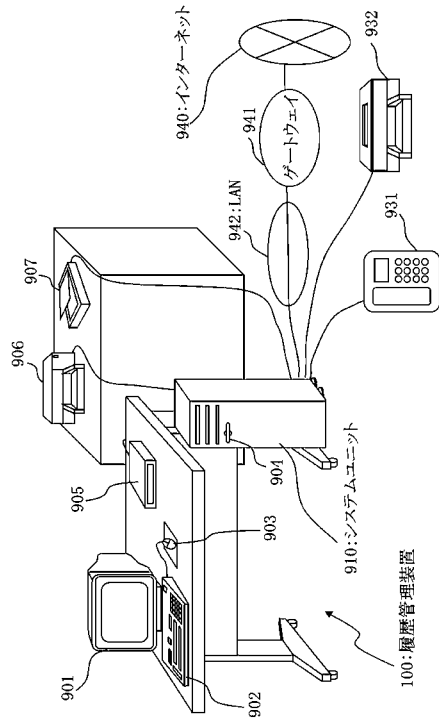
【図 31】実施の形態 9 におけるログ加工装置 110 の内部ブロックの詳細な構成の一例を示す詳細ブロック図。

【符号の説明】

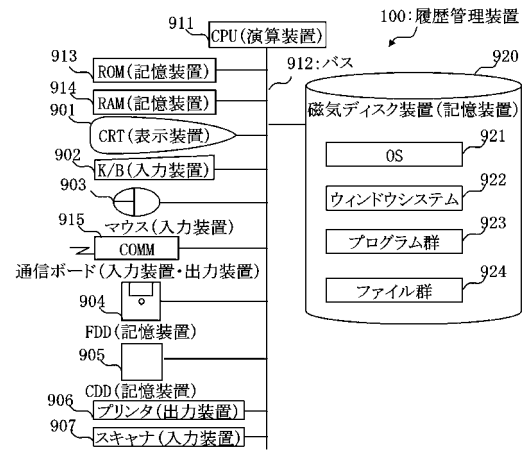
【0488】

100 履歴管理装置、110 ログ加工装置、120 ログ管理装置、121 履歴
 収集部、122 履歴加工部、123 履歴蓄積部、124 履歴検索部、130 I D
 管理装置、131 管理記憶部、132 管理検索部、140 管理端末装置、141
 検索条件入力部、142 検索結果表示部、221 発生履歴記憶部、222 発生期間 10
 判断部、223 発生期間記憶部、224 発生期間通知部、225 対応期間取得部、
 226 対応期間記憶部、227 対応判断部、300 ログ管理システム、321 ロ
 グ収集部、322 統合 I D 照会部、323 ログ蓄積部、324 ログ検索部、325
 ログ D B、331 統合 I D 取得部、332 統合 I D 属性情報取得部、333 I D
 管理 D B、341 統合 I D 属性情報照会部、342 ログ検索表示部、351 照会デ
 ータ取得部、352 統合 I D 検索部、353 照会結果通知部、361 個別 I D 記憶
 部、362 属性記憶部、371 ログレコード解析部、372 統合 I D 照会データ生
 成部、373 統合 I D 照会結果解析部、374 ログレコード加工部、375 ドメイ
 ン種別記憶部、376 ドメイン種別判定部、377 送受信種別テーブル記憶部、37
 8 送受信種別判定部、382 属性照会データ生成部、383 属性照会結果解析部、 20
 385 U R L 種別記憶部、386 U R L 種別判定部、500 監視対象機器、610
 管理情報、611, 631, 653, 673 管理識別情報、612, 632, 672
 期間情報、613 対象識別情報、621 時刻情報、622 対象情報、630 期
 間付管理識別情報、638 検索終了情報、639 該当なし情報、640 発生履歴情
 報、641, 651 発生時刻情報、642, 652, 661, 671 関与対象情報、
 650 加工済履歴情報、659, 759 異常発生情報、660 発生期間情報、66
 2 開始時刻情報、663 終了時刻情報、670 対応期間情報、701 個別 I D デ
 ータベース、702 属性データベース、704 ログ、705 加工済ログ、706
 統合 I D 照会データ、707 統合 I D 照会結果、710 管理情報、711, 721
 種別、712 個別 I D、713, 723 統合 I D、714, 724 開始時刻、71 30
 5, 725 終了時刻、720 管理属性情報、722 属性、740, 750 ログレ
 コード、741, 751 日付時刻、742, 752 個別ユーザ I D、743, 753
 個別機器 I D、746 送信元メールアドレス、747 送信先メールアドレス、74
 8 添付ファイル名、754 統合ユーザ I D、755 統合機器 I D、761, 771
 個別 I D、762, 772, 784 開始時刻、763, 773, 785 終了時刻、
 768 照会属性、774 統合 I D、780 ドメイン種別テーブル、781 ドメイ
 ン種別、782 ドメイン名、783 電子メールアドレス、786 機器設置種別、7
 90 送受信種別テーブル、791 送受信種別、792 送信元種別、793 送信先
 種別、796 複製元種別、797 複製先種別、799 U R L 種別、801 ログ検
 索条件、802, 805 属性照会データ、803, 806 属性照会結果、804 ロ 40
 グ検索結果、807 照会結果、841 複製元マシン名、842 複製先マシン名、8
 43 複製ファイル名、846 U R L、851, 861 統合 I D、852, 862
 開始時刻、853, 863 終了時刻、854 照会属性、864 属性内容、901
 表示装置、902 キーボード、903 マウス、904 F D D、905 C D D、9
 06 プリンタ装置、907 スキャナ装置、910 システムユニット、911 C P
 U、912 バス、913 R O M、914 R A M、915 通信ボード、920 磁
 気ディスク装置、921 O S、922 ウィンドウシステム、923 プログラム群、
 924 ファイル群、931 電話器、932 ファクシミリ機、940 インターネッ
 ト、941 ゲートウェイ、942 L A N。

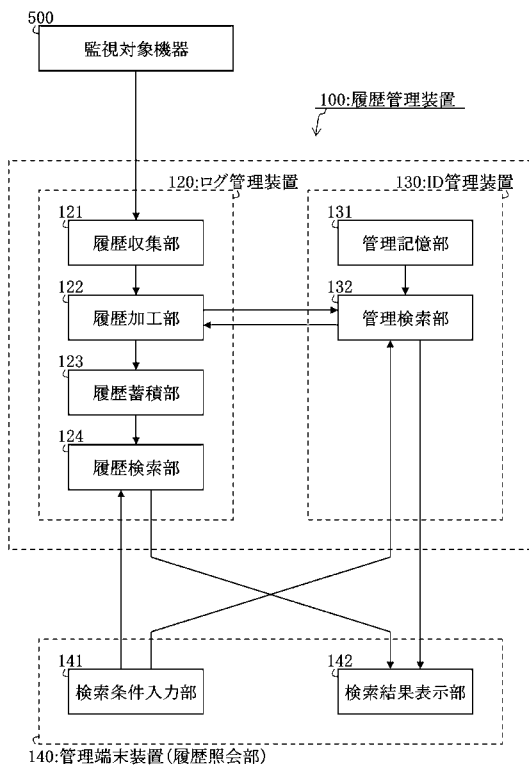
【図 1】



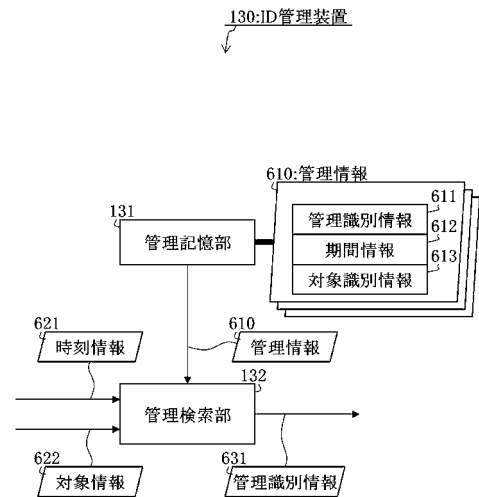
【図 2】



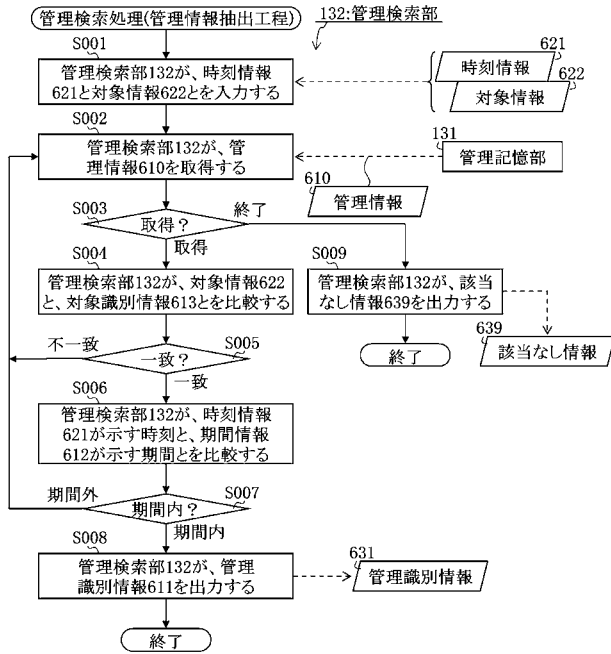
【図 3】



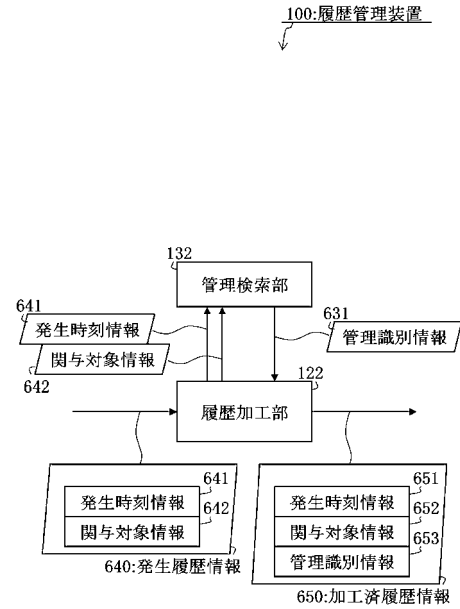
【図 4】



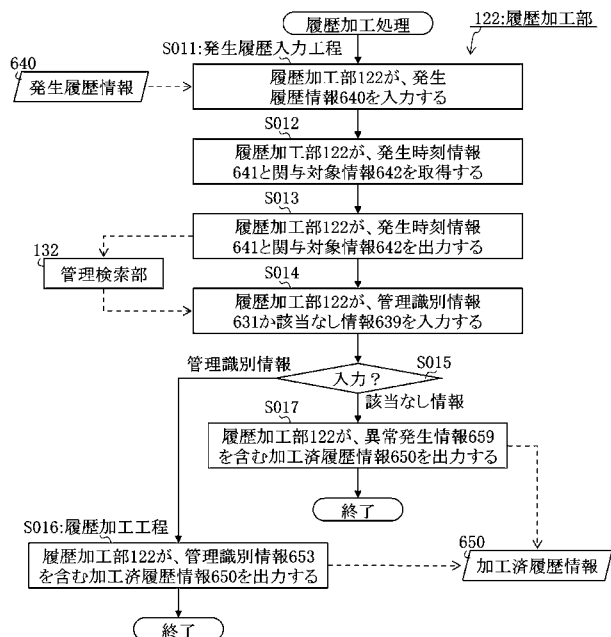
【図 5】



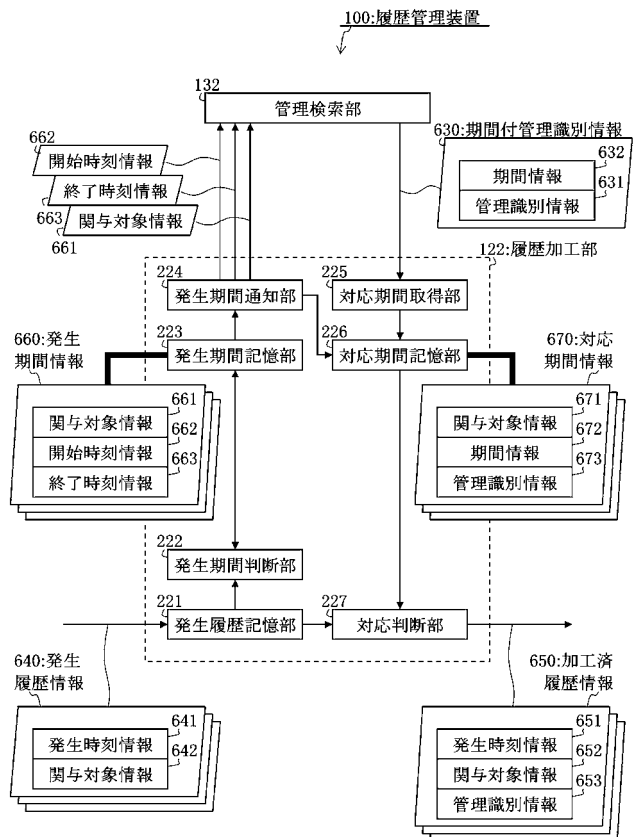
【図 6】



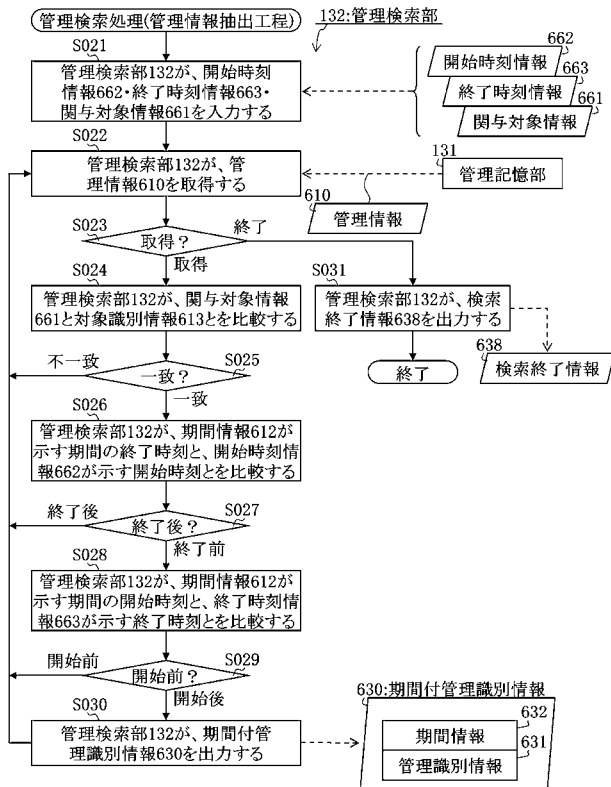
【図 7】



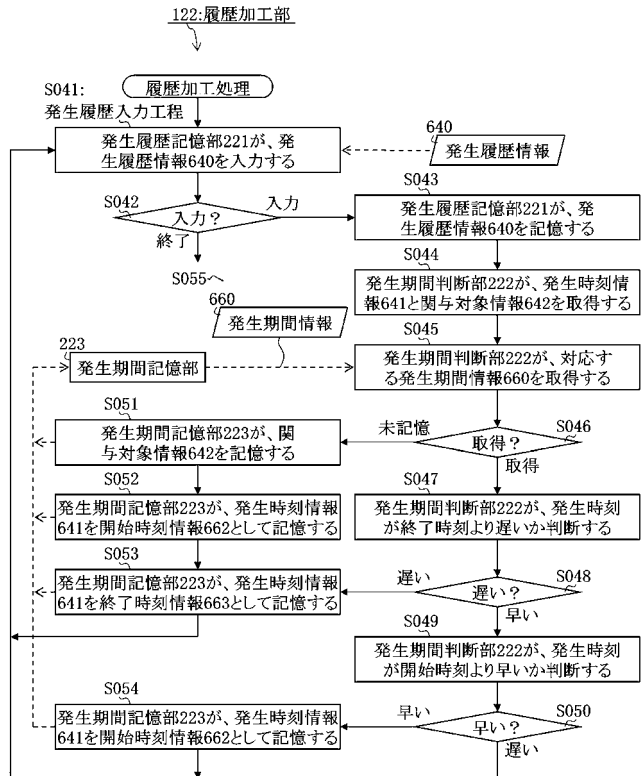
【図 8】



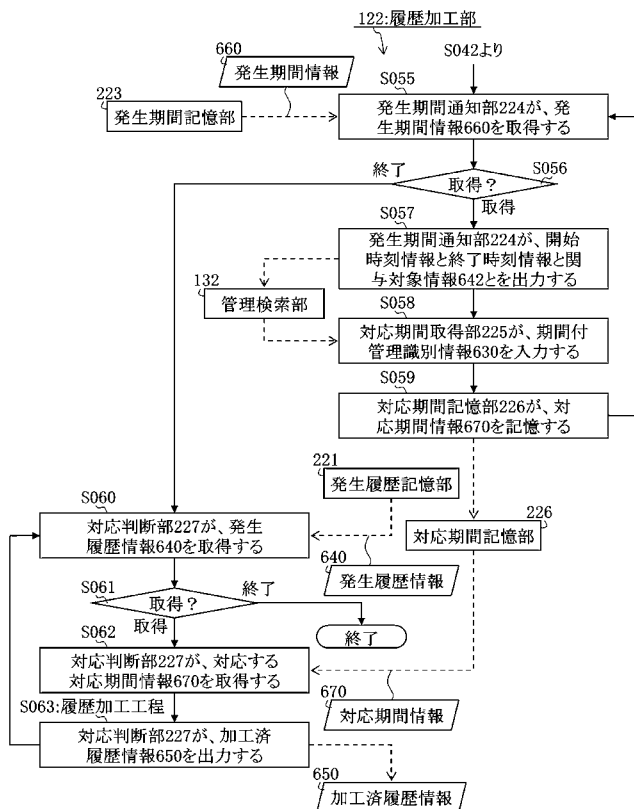
【図 9】



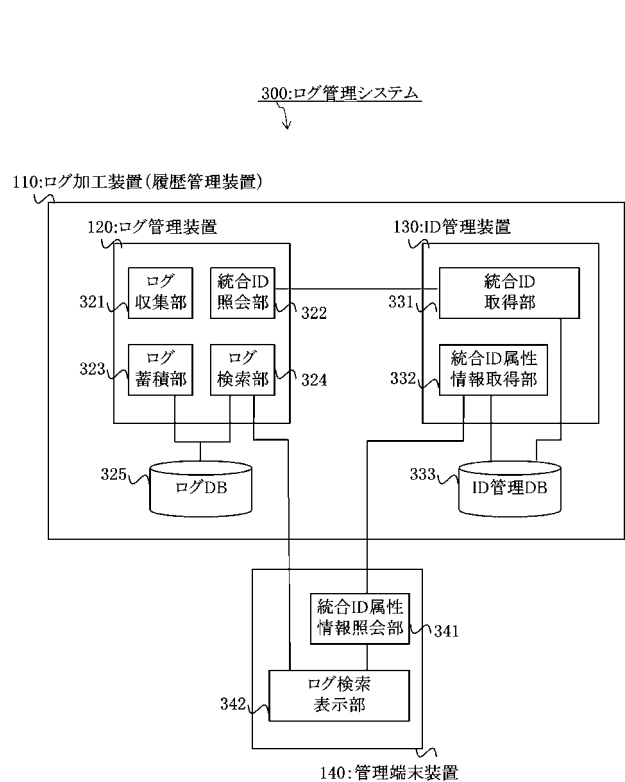
【図 10】



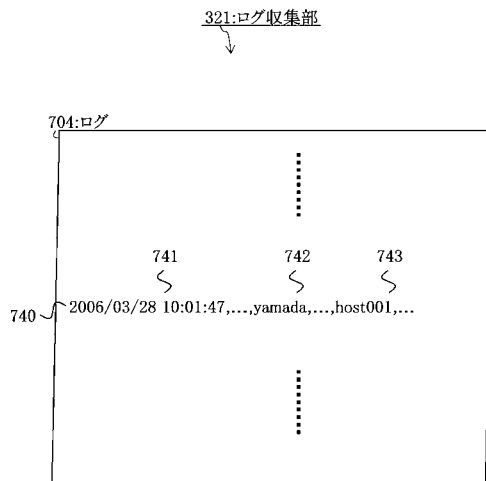
【図 11】



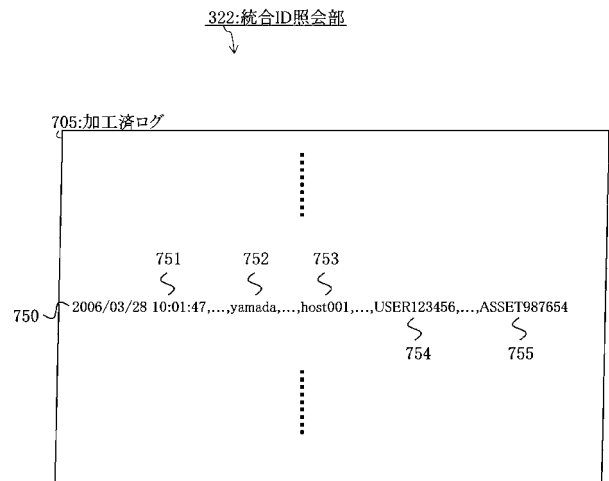
【図 12】



【図 1 3】



【図 1 4】



【図 1 5】

333:ID管理DB

720:管理属性情報

721:種別 722:属性 723:統合ID 724:開始時刻 725:終了時刻

702:属性データベース

種別	属性	統合ID	開始時刻	終了時刻
...	...	...	...	...
機器種別	PCサーバ	ASSET987654	1997/04/01 00:00:00	9999/12/31 23:59:59
設置場所	1棟6階	ASSET987654	1997/04/01 00:00:00	2003/03/31 23:59:59
管理者	佐藤 一郎	ASSET987654	1997/04/01 00:00:00	2003/03/31 23:59:59
氏名	山口 花子	USER123456	1998/04/01 08:00:00	2004/10/15 23:59:59
所属	人事部	USER123456	1998/04/01 08:00:00	2003/06/15 23:59:59
役職	担当	USER123456	1998/04/01 08:00:00	9999/12/31 23:59:59
設置場所	2棟8階	ASSET987654	2003/04/01 00:00:00	9999/12/31 23:59:59
管理者	田中 二郎	ASSET987654	2003/04/01 00:00:00	9999/12/31 23:59:59
所属	経理部	USER123456	2003/06/16 00:00:00	9999/12/31 23:59:59
氏名	鈴木 花子	USER123456	2004/10/16 00:00:00	9999/12/31 23:59:59
...	...	...	...	...

【図 1 6】

333:ID管理DB

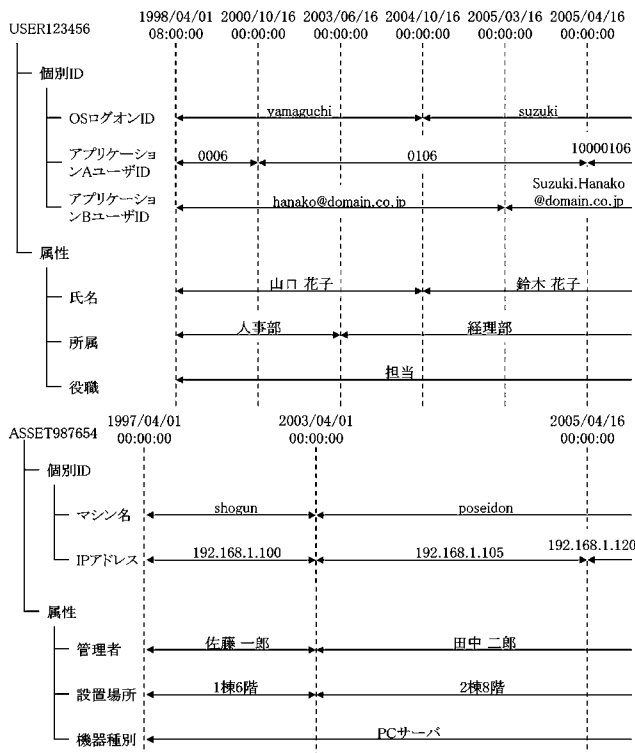
710:管理情報

711:種別 712:個別ID 713:統合ID 714:開始時刻 715:終了時刻

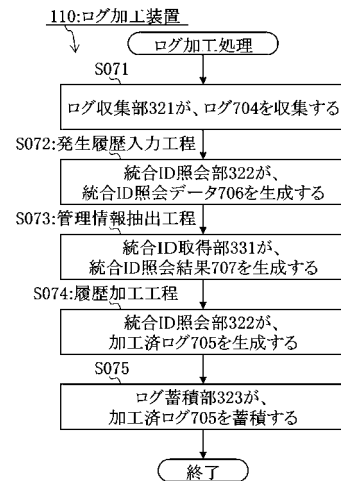
701:個別IDデータベース

種別	個別ID	統合ID	開始時刻	終了時刻
...	...	...	...	...
マシン名	shogun	ASSET987654	1997/04/01 00:00:00	2003/03/31 23:59:59
IPアドレス	192.168.1.100	ASSET987654	1997/04/01 00:00:00	2003/03/31 23:59:59
OSログインID	yamaguchi	USER123456	1998/04/01 08:00:00	2004/10/15 23:59:59
アプリケーションAユーザID	0006	USER123456	1998/04/01 08:00:00	2000/10/15 23:59:59
アプリケーションBユーザID	hanako@domain.co.jp	USER123456	1998/04/01 08:00:00	2005/03/15 23:59:59
アプリケーションAユーザID	0106	USER123456	2000/10/16 00:00:00	2005/04/15 23:59:59
マシン名	poseidon	ASSET987654	2003/04/01 00:00:00	9999/12/31 23:59:59
IPアドレス	192.168.1.105	ASSET987654	2003/04/01 00:00:00	2005/04/15 23:59:59
OSログインID	suzuki	USER123456	2004/10/16 00:00:00	9999/12/31 23:59:59
アプリケーションBユーザID	Suzuki.Hanako@domain.co.jp	USER123456	2005/03/16 00:00:00	9999/12/31 23:59:59
アプリケーションAユーザID	10000106	USER123456	2005/04/16 00:00:00	9999/12/31 23:59:59
IPアドレス	192.168.1.120	ASSET987654	2005/04/16 00:00:00	9999/12/31 23:59:59
...	...	...	...	...

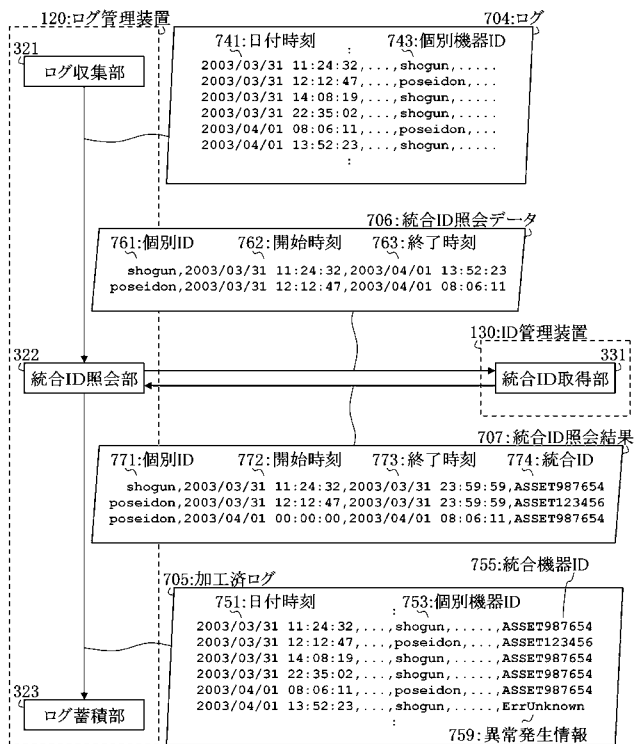
【図 17】



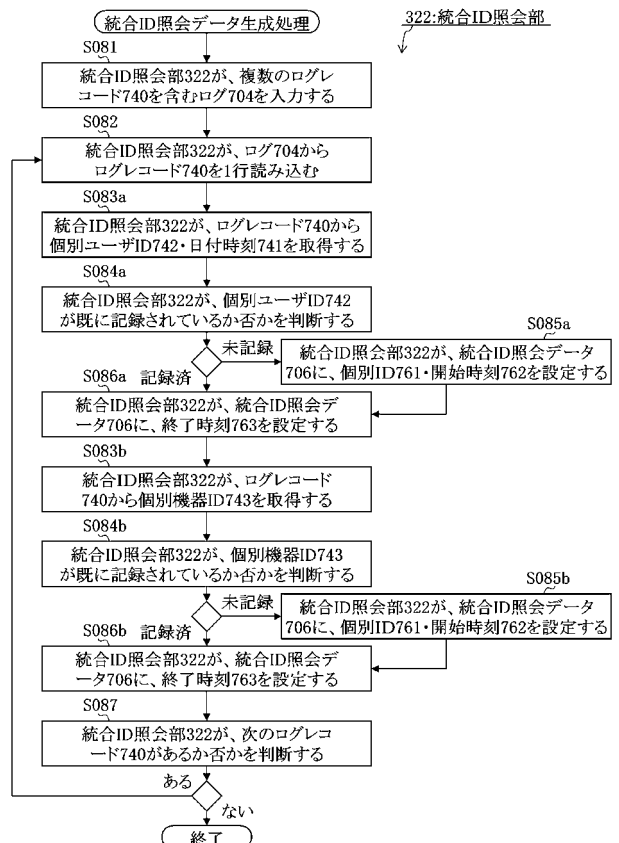
【図 18】



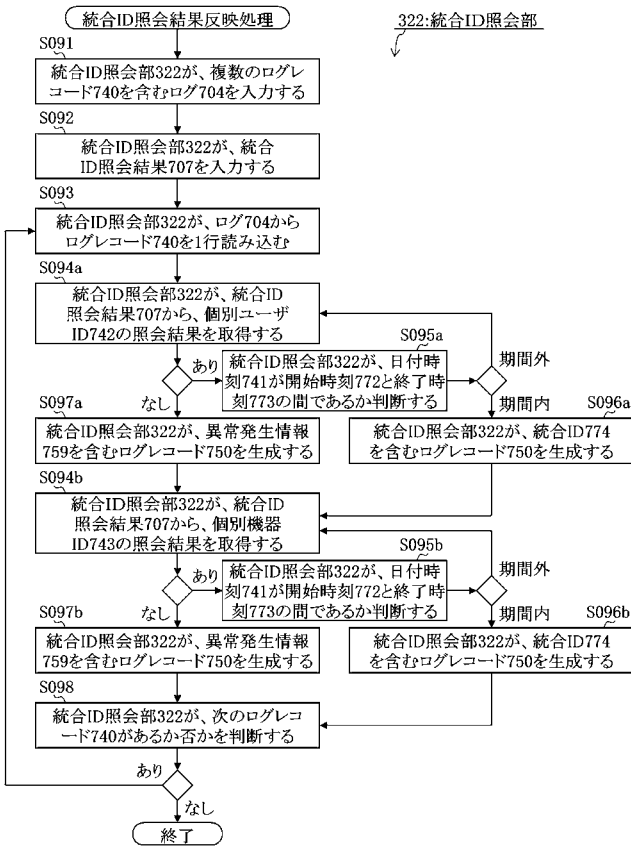
【図 19】



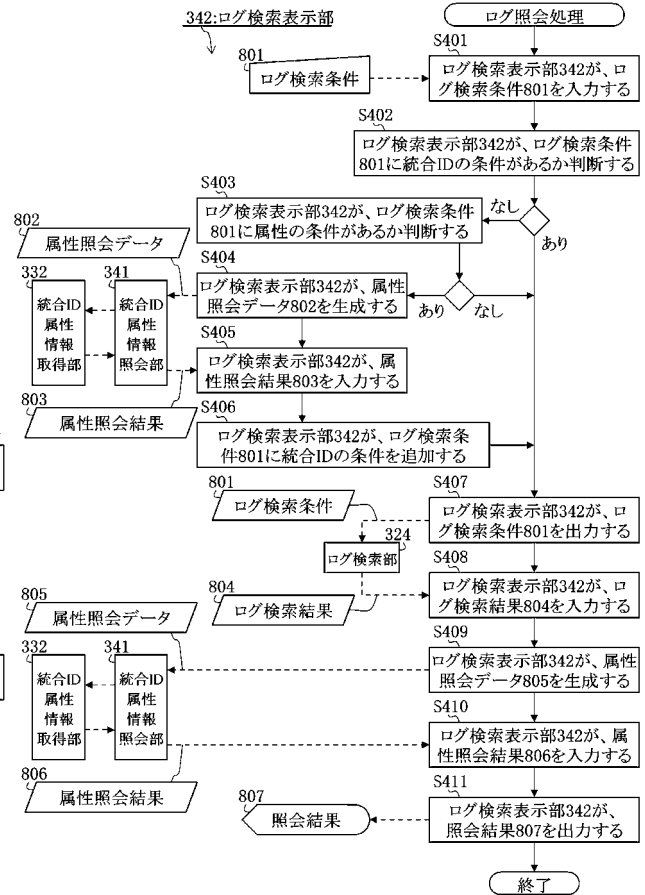
【図 20】



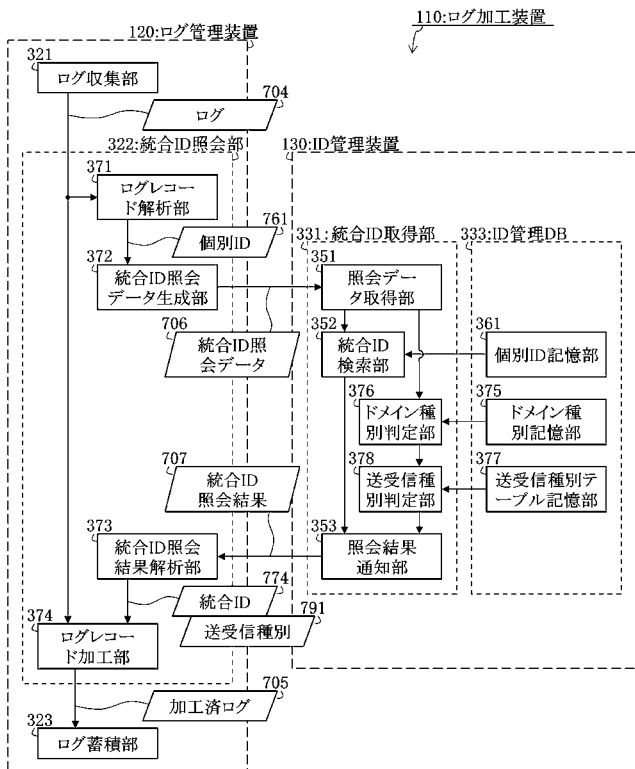
【図 2 1】



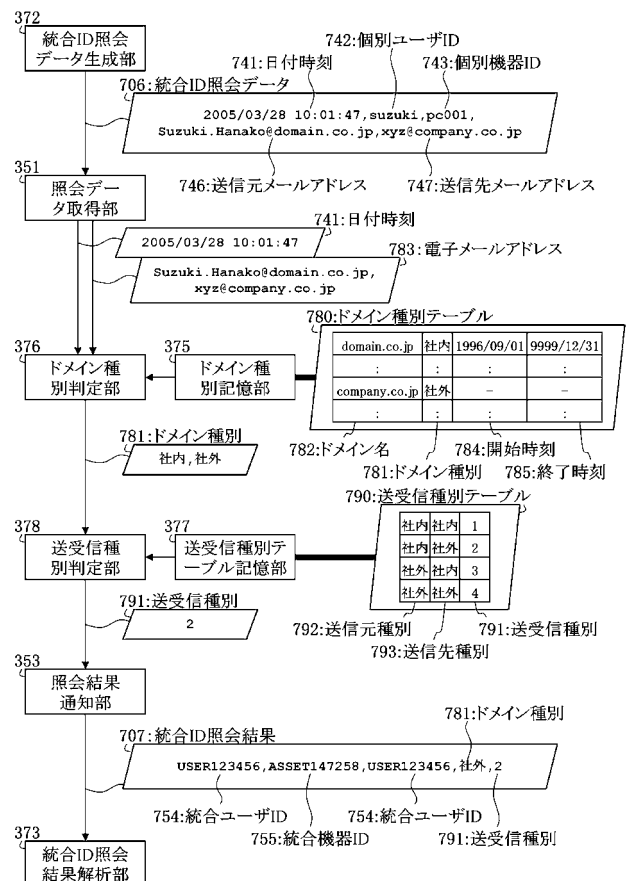
【図 2 2】



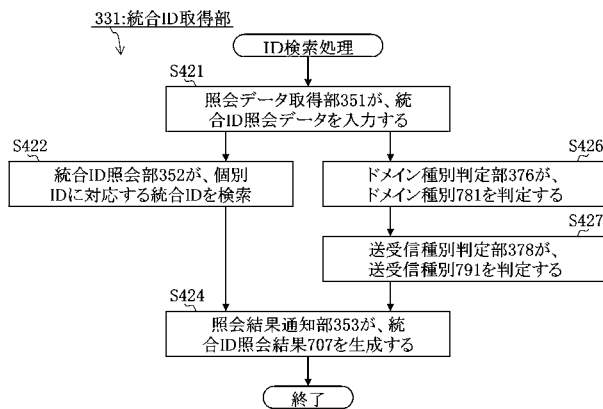
【図 2 3】



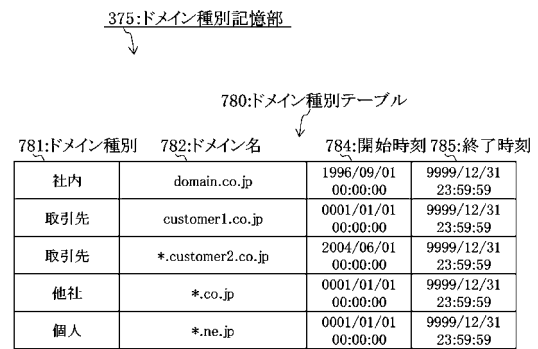
【図 2 4】



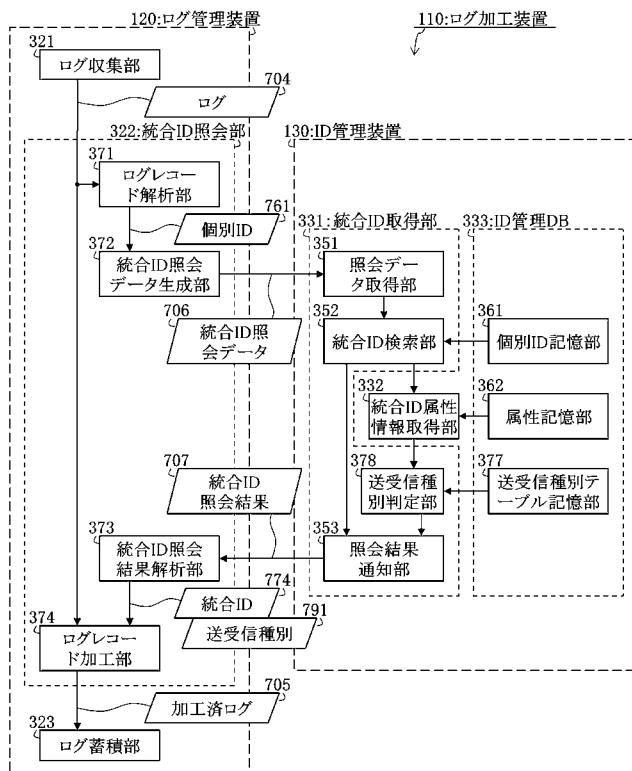
【図 2 5】



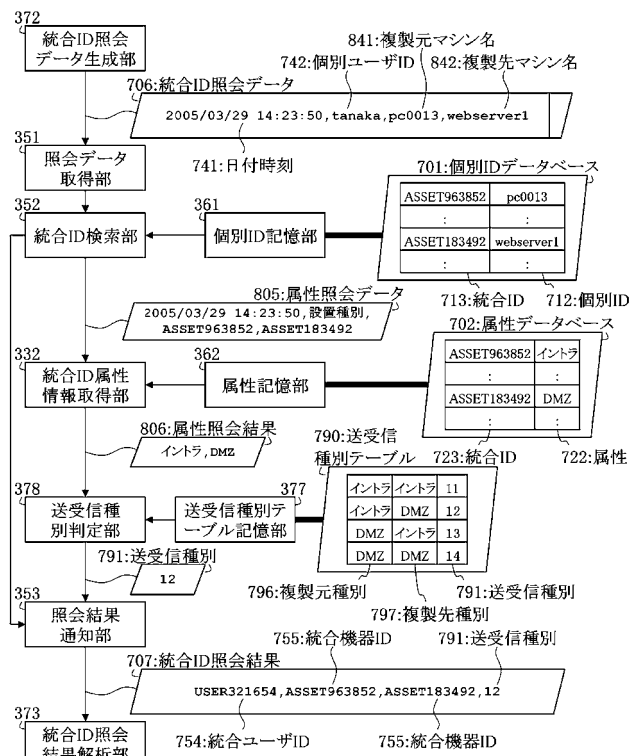
【図 2 6】



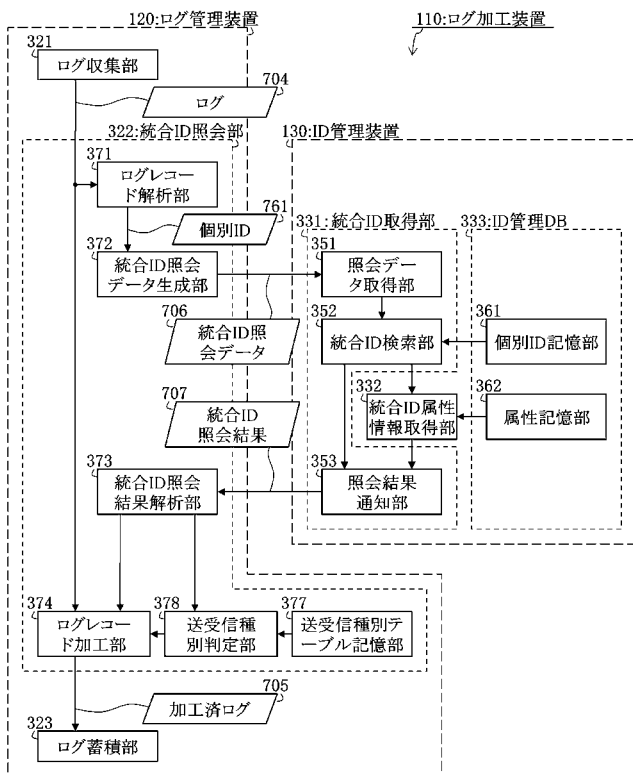
【図 2 7】



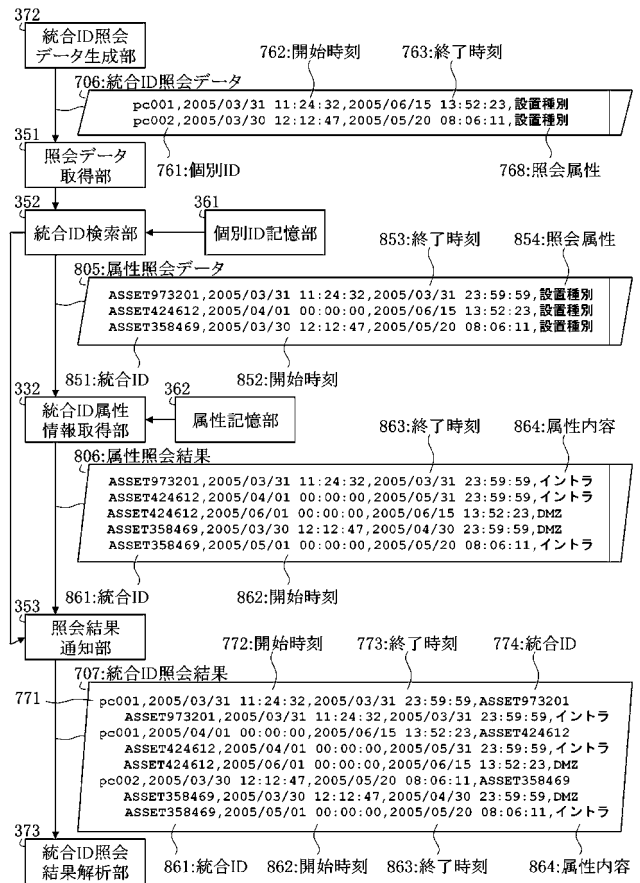
【図 2 8】



【図 29】



【図 30】



【図 31】

