

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号
特許第6070102号
(P6070102)

(45) 発行日 平成29年2月1日 (2017.2.1)

(24) 登録日 平成29年1月13日 (2017.1.13)

(51) Int. Cl.

F I

G O 6 F 11/30 (2006.01)

G O 6 F 11/30 1 5 8

G O 6 F 1/14 (2006.01)

G O 6 F 11/30 1 8 9

G O 6 F 13/00 (2006.01)

G O 6 F 1/14 5 1 2

G O 6 F 13/00 3 5 1 C

請求項の数 9 (全 25 頁)

(21) 出願番号	特願2012-254717 (P2012-254717)	(73) 特許権者	000005223
(22) 出願日	平成24年11月20日 (2012.11.20)		富士通株式会社
(65) 公開番号	特開2014-102706 (P2014-102706A)		神奈川県川崎市中原区上小田中4丁目1番1号
(43) 公開日	平成26年6月5日 (2014.6.5)	(74) 代理人	100104190
審査請求日	平成27年7月6日 (2015.7.6)		弁理士 酒井 昭徳
		(72) 発明者	岩本 良平
			福岡県福岡市早良区百道浜二丁目2番1号
			株式会社富士通九州システムズ内
		(72) 発明者	坂部 信
			福岡県福岡市早良区百道浜二丁目2番1号
			株式会社富士通九州システムズ内
		(72) 発明者	今別府 晋哉
			福岡県福岡市早良区百道浜二丁目2番1号
			株式会社富士通九州システムズ内
			最終頁に続く

(54) 【発明の名称】 ずれ算出プログラム、プログラム、情報処理装置および情報処理方法

(57) 【特許請求の範囲】

【請求項 1】

第 1 の装置と第 2 の装置間とで重複する時間範囲のログをそれぞれの装置から取得し、
類似文字とログ時刻とに基づいて、前記第 1 の装置から取得したログのうち第 1 のログ
群と、前記第 2 の装置から取得したログのうち第 2 のログ群とを抽出し、

抽出した前記第 1 のログ群および前記第 2 のログ群のうち、送信と受信との対応関係で
あるログの組のそれぞれのログ時刻に基づいて、前記第 1 の装置と前記第 2 の装置との時
刻のずれを算出する、

処理をコンピュータに実行させることを特徴とする ずれ算出プログラム。

【請求項 2】

第 1 内部時刻によってログを記憶する第 1 装置と、第 2 内部時刻によってログを記憶す
る第 2 装置と、のログに関する処理を行う情報処理装置であって、

前記第 1 装置が第 1 信号を送信した前記第 1 内部時刻に基づく第 1 送信時刻と、前記第
1 信号を前記第 2 装置が受信した前記第 2 内部時刻に基づく第 1 受信時刻と、前記第 2 装
置が第 2 信号を送信した前記第 2 内部時刻に基づく第 2 送信時刻と、前記第 2 信号を前記
第 1 装置が受信した前記第 1 内部時刻に基づく第 2 受信時刻と、を取得する取得部と、

前記取得部によって取得された前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時
刻および前記第 2 受信時刻に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出
する算出部と、

を備え、前記取得部は、

前記第 1 装置によって記憶された所定期間内の第 1 ログと、前記第 2 装置によって記憶された前記所定期間内の第 2 ログと、を取得し、

取得した前記第 1 ログに含まれる前記第 1 信号の第 1 通信記録から前記第 1 送信時刻を取得し、

取得した前記第 2 ログの中から、取得した前記第 1 送信時刻との時間差が閾値以下の第 2 通信記録を抽出することにより前記第 1 受信時刻を取得し、

取得した前記第 2 ログの中から、取得した前記第 1 受信時刻との時間差が閾値以下の第 3 通信記録を抽出することにより前記第 2 送信時刻を取得し、

取得した前記第 1 ログの中から、取得した前記第 2 送信時刻との時間差が閾値以下の第 4 通信記録を抽出することにより前記第 2 受信時刻を取得する、

ことを特徴とする情報処理装置。

【請求項 3】

前記算出部は、

前記第 1 受信時刻および前記第 1 送信時刻の差と、前記第 2 受信時刻および前記第 2 送信時刻の差と、の差の半分と、

前記第 1 受信時刻および前記第 1 送信時刻の差または前記第 2 受信時刻および前記第 2 送信時刻の差と、

の差を示す値を算出することによって前記第 1 内部時刻と前記第 2 内部時刻との差を算出することを特徴とする請求項 2 に記載の情報処理装置。

【請求項 4】

前記取得部は、

取得した前記第 1 ログの中から互いに類似する類似文字を抽出し、前記第 1 ログの中から抽出した類似文字ごとに、前記類似文字に該当するキーワードの前記第 1 ログにおける出現数を算出し、

取得した前記第 2 ログの中から互いに類似する類似文字を抽出し、前記第 2 ログの中から抽出した類似文字ごとに、前記類似文字に該当するキーワードの前記第 2 ログにおける出現数を算出し、

前記第 1 ログの中から抽出した類似文字から、算出した前記出現数に基づいて第 1 類似文字を選択し、選択した前記第 1 類似文字のキーワードを含む前記第 1 通信記録を前記第 1 ログから抽出することにより前記第 1 送信時刻を取得し、

前記第 2 ログの中から抽出した類似文字のうちの算出した前記出現数が前記第 1 類似文字と同じである第 2 類似文字のキーワードを含む前記第 2 通信記録を前記第 2 ログから抽出することにより前記第 1 受信時刻を取得し、

前記第 2 ログの中から抽出した類似文字のうちの算出した前記出現数が前記第 2 類似文字と同じである第 3 類似文字のキーワードを含む前記第 3 通信記録を前記第 2 ログから抽出することにより前記第 2 送信時刻を取得し、

前記第 1 ログの中から抽出した類似文字のうちの算出した前記出現数が前記第 3 類似文字と同じである第 4 類似文字のキーワードを含む前記第 4 通信記録を前記第 1 ログから抽出することにより前記第 2 受信時刻を取得する、

ことを特徴とする請求項 2 または 3 に記載の情報処理装置。

【請求項 5】

前記取得部は、前記第 1 ログの中から抽出した類似文字ごとに、前記類似文字に含まれる各キーワードの類似度を算出し、算出した前記出現数および前記類似度に基づいて前記第 1 類似文字を選択することを特徴とする請求項 4 に記載の情報処理装置。

【請求項 6】

前記第 1 装置によって記憶された所定期間内のログと、前記第 2 装置によって記憶された前記所定期間内のログと、前記算出部によって算出された差と、に基づいて、前記第 1 装置および前記第 2 装置の間で行われた通信の履歴を示すシーケンスログを作成する作成部を備えることを特徴とする請求項 2 ～ 5 のいずれか一つに記載の情報処理装置。

【請求項 7】

前記取得部は、前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻の組を複数取得し、

前記算出部は、前記組ごとに、前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻に基づく前記第 1 内部時刻と前記第 2 内部時刻との差を算出し、前記組ごとの算出結果に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出することを特徴とする請求項 2 ～ 6 のいずれか一つに記載の情報処理装置。

【請求項 8】

第 1 内部時刻によってログを記憶する第 1 装置と、第 2 内部時刻によってログを記憶する第 2 装置と、のログに関する処理を行う情報処理装置に、

前記第 1 装置が第 1 信号を送信した前記第 1 内部時刻に基づく第 1 送信時刻と、前記第 1 信号を前記第 2 装置が受信した前記第 2 内部時刻に基づく第 1 受信時刻と、前記第 2 装置が第 2 信号を送信した前記第 2 内部時刻に基づく第 2 送信時刻と、前記第 2 信号を前記第 1 装置が受信した前記第 1 内部時刻に基づく第 2 受信時刻と、を取得し、

取得した前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出する、

処理を実行させ、

前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻を取得する処理は、

前記第 1 装置によって記憶された所定期間内の第 1 ログと、前記第 2 装置によって記憶された前記所定期間内の第 2 ログと、を取得し、

取得した前記第 1 ログに含まれる前記第 1 信号の第 1 通信記録から前記第 1 送信時刻を取得し、

取得した前記第 2 ログの中から、取得した前記第 1 送信時刻との時間差が閾値以下の第 2 通信記録を抽出することにより前記第 1 受信時刻を取得し、

取得した前記第 2 ログの中から、取得した前記第 1 受信時刻との時間差が閾値以下の第 3 通信記録を抽出することにより前記第 2 送信時刻を取得し、

取得した前記第 1 ログの中から、取得した前記第 2 送信時刻との時間差が閾値以下の第 4 通信記録を抽出することにより前記第 2 受信時刻を取得する、

処理を含む、

ことを特徴とするプログラム。

【請求項 9】

第 1 内部時刻によってログを記憶する第 1 装置と、第 2 内部時刻によってログを記憶する第 2 装置と、のログに関する処理を行う情報処理装置により、

前記第 1 装置が第 1 信号を送信した前記第 1 内部時刻に基づく第 1 送信時刻と、前記第 1 信号を前記第 2 装置が受信した前記第 2 内部時刻に基づく第 1 受信時刻と、前記第 2 装置が第 2 信号を送信した前記第 2 内部時刻に基づく第 2 送信時刻と、前記第 2 信号を前記第 1 装置が受信した前記第 1 内部時刻に基づく第 2 受信時刻と、を取得し、

取得した前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出し、

前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻を取得する際に、

前記第 1 装置によって記憶された所定期間内の第 1 ログと、前記第 2 装置によって記憶された前記所定期間内の第 2 ログと、を取得し、

取得した前記第 1 ログに含まれる前記第 1 信号の第 1 通信記録から前記第 1 送信時刻を取得し、

取得した前記第 2 ログの中から、取得した前記第 1 送信時刻との時間差が閾値以下の第 2 通信記録を抽出することにより前記第 1 受信時刻を取得し、

取得した前記第 2 ログの中から、取得した前記第 1 受信時刻との時間差が閾値以下の第 3 通信記録を抽出することにより前記第 2 送信時刻を取得し、

取得した前記第 1 ログの中から、取得した前記第 2 送信時刻との時間差が閾値以下の第

10

20

30

40

50

4 通信記録を抽出することにより前記第 2 受信時刻を取得する、
ことを特徴とする情報処理方法。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、プログラム、情報処理装置および情報処理方法に関する。

【背景技術】

【0002】

従来、複数の装置の間でやり取りされる処理のシーケンスログを生成する技術が知られている。たとえば、複数の装置のそれぞれのログを収集して合成することによってシーケンスログが作成される。

10

【0003】

また、複数パケットがプロトコルシーケンスの特定状況にあるか否かを判断し、特定状況にある場合に当該複数パケットを圧縮可能と判定し、圧縮可能な複数パケットのやり取りをまとめて出力する技術が知られている（たとえば、下記特許文献 1 参照。）。

【0004】

また、監視装置において被監視装置の装置情報をログとして記録・表示するログ管理方式において、被監視装置での発生順にログを格納する技術が知られている（たとえば、下記特許文献 2 参照。）。

20

【先行技術文献】

【特許文献】

【0005】

【特許文献 1】特開 2003 - 264609 号公報

【特許文献 2】特開平 10 - 327217 号公報

【発明の概要】

【発明が解決しようとする課題】

【0006】

しかしながら、上述した従来技術では、複数の装置の内部時刻が合致していない場合があり、この場合は正確なシーケンスログを作成することが困難という問題がある。

【0007】

30

本発明は、上述した従来技術による問題点を解消するため、より正確なシーケンスログの作成を図ることができるプログラム、情報処理装置および情報処理方法を提供することを目的とする。

【課題を解決するための手段】

【0008】

上述した課題を解決し、目的を達成するため、本発明の一側面によれば、装置間で重複する時間範囲のログをそれぞれの装置から取得し、取得したそれぞれのログから、一方の装置から送信され他方の装置が受信した第 1 の一対のログおよび該他方の装置から送信して該一方の装置が受信した第 2 の一対のログを抽出し、抽出した前記第 1 および前記第 2 の一対のログから前記一方の装置および前記他方の装置の時刻のずれを算出するプログラム、情報処理装置および情報処理方法が提案される。

40

【0009】

また、本発明の別の側面によれば、第 1 内部時刻によってログを記憶する第 1 装置と、第 2 内部時刻によってログを記憶する第 2 装置と、のログに関する処理を行う場合に、前記第 1 装置が第 1 信号を送信した前記第 1 内部時刻に基づく第 1 送信時刻と、前記第 1 信号を前記第 2 装置が受信した前記第 2 内部時刻に基づく第 1 受信時刻と、前記第 2 装置が第 2 信号を送信した前記第 2 内部時刻に基づく第 2 送信時刻と、前記第 2 信号を前記第 1 装置が受信した前記第 1 内部時刻に基づく第 2 受信時刻と、を取得し、取得した前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出するプログラム、情報処理装置および情報

50

処理方法が提案される。

【発明の効果】

【0010】

本発明の一側面によれば、より正確なシーケンスログの作成を図ることができるという効果を奏する。

【図面の簡単な説明】

【0011】

【図1】図1は、実施の形態にかかる情報処理装置によって取得される各時刻の一例を示す図である。

【図2】図2は、実施の形態にかかる情報処理装置の構成の一例を示す図である。

10

【図3】図3は、実施の形態にかかる情報処理装置のハードウェア構成の一例を示す図である。

【図4】図4は、ログの処理対象の通信システムの一例を示す図である。

【図5】図5は、自動マージの処理の一例を示すフローチャートである。

【図6】図6は、自動時刻補正の処理の一例を示すフローチャートである。

【図7-1】図7-1は、装置Aによって記憶されたログの一例を示す図である。

【図7-2】図7-2は、装置Bによって記憶されたログの一例を示す図である。

【図7-3】図7-3は、装置Cによって記憶されたログの一例を示す図である。

【図7-4】図7-4は、装置Dによって記憶されたログの一例を示す図である。

【図8】図8は、ログ形式のパターンファイルの一例を示す図である。

20

【図9-1】図9-1は、装置Aのログに基づく類似度の算出結果の一例を示す図である。

【図9-2】図9-2は、装置Bのログに基づく類似度の算出結果の一例を示す図である。

【図10-1】図10-1は、キーワードの抽出結果の一例を示す図（その1）である。

【図10-2】図10-2は、キーワードの抽出結果の一例を示す図（その2）である。

【図10-3】図10-3は、キーワードの抽出結果の一例を示す図（その3）である。

【図10-4】図10-4は、キーワードの抽出結果の一例を示す図（その4）である。

【図11-1】図11-1は、ログの処理時間の算出結果の一例を示す図（その1）である。

30

【図11-2】図11-2は、ログの処理時間の算出結果の一例を示す図（その2）である。

【図12】図12は、装置Bのログの補正結果の一例を示す図である。

【図13】図13は、シーケンスログの一例を示す図である。

【発明を実施するための形態】

【0012】

以下に添付図面を参照して、本発明にかかるプログラム、情報処理装置および情報処理方法の実施の形態を詳細に説明する。

【0013】

（実施の形態）

40

（実施の形態にかかる情報処理装置によって取得される各時刻）

図1は、実施の形態にかかる情報処理装置によって取得される各時刻の一例を示す図である。実施の形態にかかる情報処理装置は、たとえば図1に示す第1装置110および第2装置120のログに関する処理を行う。第1装置110および第2装置120は、互いに通信可能な通信装置である。

【0014】

第1装置110は、第1内部時刻に基づいて第1装置110の通信動作等のログを記憶する。第2装置120は、第2内部時刻に基づいて第2装置120の通信動作等のログを記憶する。第1内部時刻および第2内部時刻は、それぞれ第1装置110および第2装置120の内部時計に基づく時刻である。したがって、第1内部時刻および第2内部時刻の

50

間にはずれが存在する場合がある。

【 0 0 1 5 】

図 1 に示すように、たとえば、第 1 装置 1 1 0 が第 2 装置 1 2 0 へ第 1 信号 1 0 1 を送信したとする。また、第 2 装置 1 2 0 が第 1 装置 1 1 0 へ第 2 信号 1 0 2 を送信したとする。たとえば、第 1 信号 1 0 1 は第 1 装置 1 1 0 から第 2 装置 1 2 0 への要求信号であり、第 2 信号 1 0 2 は第 2 装置 1 2 0 から第 1 装置 1 1 0 への応答信号である。ただし、第 1 信号 1 0 1 と第 2 信号 1 0 2 との間の関係はこれに限らない。たとえば、第 1 信号 1 0 1 は第 2 信号 1 0 2 よりも後に送信された信号であってもよい。

【 0 0 1 6 】

第 1 送信時刻 1 1 1 は、第 1 装置 1 1 0 によって記憶された、第 1 装置 1 1 0 による第 1 信号 1 0 1 の送信時刻である。第 1 受信時刻 1 2 1 は、第 2 装置 1 2 0 によって記憶された、第 2 装置 1 2 0 による第 1 信号 1 0 1 の受信時刻である。

10

【 0 0 1 7 】

第 2 送信時刻 1 2 2 は、第 2 装置 1 2 0 によって記憶された、第 2 装置 1 2 0 による第 2 信号 1 0 2 の送信時刻である。第 2 受信時刻 1 1 2 は、第 1 装置 1 1 0 によって記憶された、第 1 装置 1 1 0 による第 2 信号 1 0 2 の受信時刻である。

【 0 0 1 8 】

したがって、第 1 送信時刻 1 1 1 および第 2 受信時刻 1 1 2 は、第 1 装置 1 1 0 の第 1 内部時刻に基づく時刻である。また、第 1 受信時刻 1 2 1 および第 2 送信時刻 1 2 2 は、第 2 装置 1 2 0 の第 2 内部時刻に基づく時刻である。

20

【 0 0 1 9 】

実施の形態にかかる情報処理装置は、第 1 送信時刻 1 1 1、第 2 受信時刻 1 1 2、第 1 受信時刻 1 2 1 および第 2 送信時刻 1 2 2 を取得する。

【 0 0 2 0 】

(実施の形態にかかる情報処理装置の構成)

図 2 は、実施の形態にかかる情報処理装置の構成の一例を示す図である。実施の形態にかかる情報処理装置 2 0 0 は、たとえば、図 2 に示すように、取得部 2 1 0 と、算出部 2 2 0 と、を備えている。

【 0 0 2 1 】

取得部 2 1 0 は、図 1 に示した第 1 送信時刻 1 1 1、第 2 受信時刻 1 1 2、第 1 受信時刻 1 2 1 および第 2 送信時刻 1 2 2 を取得する。たとえば、取得部 2 1 0 は、第 1 装置 1 1 0 および第 2 装置 1 2 0 によって記憶された各ログの中から第 1 送信時刻 1 1 1、第 2 受信時刻 1 1 2、第 1 受信時刻 1 2 1 および第 2 送信時刻 1 2 2 を取得する。

30

【 0 0 2 2 】

または、取得部 2 1 0 は、第 1 送信時刻 1 1 1、第 2 受信時刻 1 1 2、第 1 受信時刻 1 2 1 および第 2 送信時刻 1 2 2 をユーザ入力等によって直接取得してもよい。取得部 2 1 0 は、取得した第 1 送信時刻 1 1 1、第 2 受信時刻 1 1 2、第 1 受信時刻 1 2 1 および第 2 送信時刻 1 2 2 を算出部 2 2 0 へ出力する。

【 0 0 2 3 】

算出部 2 2 0 は、取得部 2 1 0 から出力された第 1 送信時刻 1 1 1、第 2 受信時刻 1 1 2、第 1 受信時刻 1 2 1 および第 2 送信時刻 1 2 2 に基づいて、第 1 装置 1 1 0 の第 1 内部時刻と第 2 装置 1 2 0 の第 2 内部時刻との差 (ずれ) を算出する。算出部 2 2 0 は、算出した差を示す情報を出力する。

40

【 0 0 2 4 】

たとえば、算出部 2 2 0 は、算出した差を示す情報をユーザへ出力する。これにより、ユーザは、第 1 装置 1 1 0 および第 2 装置 1 2 0 によって記憶された各ログの時刻を、算出部 2 2 0 によって出力された情報が示すずれに基づいて補正し、第 1 装置 1 1 0 と第 2 装置 1 2 0 との間の正確なシーケンスログを作成することが可能になる。

【 0 0 2 5 】

または、情報処理装置 2 0 0 が、第 1 装置 1 1 0 と第 2 装置 1 2 0 との間の正確なシー

50

ケンスログを作成する作成部を有していてもよい。この場合は、算出部 220 は、算出した差を示す情報を作成部へ出力する。これにより、作成部において、第 1 装置 110 および第 2 装置 120 によって記憶された各ログの時刻を、算出部 220 によって出力された情報が示すずれに基づいて補正し、第 1 装置 110 と第 2 装置 120 との間の正確なシーケンスログを作成することができる。作成部は、作成したシーケンスログを出力する。

【0026】

< 第 1 内部時刻と第 2 内部時刻との差の算出 >

算出部 220 による第 1 内部時刻と第 2 内部時刻との差の算出について説明する。たとえば、所定の基準時刻に対して、第 1 装置 110 の第 1 内部時刻は D1 だけずれており、第 2 装置 120 の第 2 内部時刻は D2 だけずれているとする。なお、基準時刻は第 1 内部時刻（すなわち D1 = 0）または第 2 内部時刻（すなわち D2 = 0）であってもよい。

10

【0027】

取得部 210 によって取得される第 1 送信時刻 111、第 1 受信時刻 121、第 2 送信時刻 122 および第 2 受信時刻 112 は、それぞれたとえば下記（1）～（4）式によって示すことができる。

【0028】

第 1 送信時刻 = 基準時刻に基づく第 1 信号の送信時刻 + D1 ... (1)

第 1 受信時刻 = 基準時刻に基づく第 1 信号の受信時刻 + D2 ... (2)

第 2 送信時刻 = 基準時刻に基づく第 2 信号の送信時刻 + D2 ... (3)

第 2 受信時刻 = 基準時刻に基づく第 2 信号の受信時刻 + D1 ... (4)

20

【0029】

第 2 送信時刻 122 から第 1 受信時刻 121 を減算すると、上記（3）、（2）式により下記（5）式のようなになる。また、第 2 受信時刻 112 から第 1 送信時刻 111 を減算すると、上記（1）、（4）式により下記（6）式のようなになる。

【0030】

(3) - (2) = 基準時刻に基づく第 2 信号の送信時刻
- 基準時刻に基づく第 1 信号の受信時刻 ... (5)

【0031】

(4) - (1) = 基準時刻に基づく第 2 信号の受信時刻
- 基準時刻に基づく第 1 信号の送信時刻 ... (6)

30

【0032】

上記（6）式から上記（5）式を減算すると下記（7）式のようなになる。

【0033】

(6) - (5) = 基準時刻に基づく第 1 信号の受信時刻
- 基準時刻に基づく第 1 信号の送信時刻
+ 基準時刻に基づく第 2 信号の受信時刻
- 基準時刻に基づく第 2 信号の送信時刻
= 第 1 信号の送信時刻から受信時刻までの時間
+ 第 2 信号の送信時刻から受信時刻までの時間 ... (7)

40

【0034】

ここで、第 1 装置 110 から第 2 装置 120 への通信にかかる時間と、第 2 装置 120 から第 1 装置 110 への通信にかかる時間と、が同じであると仮定する。この場合は、上記（7）式を半分にすると、下記（8）式のように、第 1 装置 110 と第 2 装置 120 との間の片道の通信にかかる時間を算出することができる。

【0035】

(7) ÷ 2 = 通信にかかる時間 ... (8)

【0036】

また、上記（2）式から上記（1）式を減算すると、下記（9）式のようなになる。

【0037】

(2) - (1) = 基準時刻に基づく第 1 信号の受信時刻 + D2

50

$$\begin{aligned}
 & - \text{基準時刻に基づく第1信号の送信時刻} - D1 \\
 & = \text{通信にかかる時間} + D2 - D1 \quad \dots (9)
 \end{aligned}$$

【0038】

したがって、上記(9)式から上記(8)式を減算すると、下記(10)式のように、第1内部時刻の基準時刻からのずれD1と、第2内部時刻の基準時刻からのずれD2と、の差を算出することができる。

【0039】

$$(9) - (8) = D2 - D1 \quad \dots (10)$$

【0040】

または、上記(4)式から上記(3)式を減算すると、下記(11)式のようになる。

10

【0041】

$$\begin{aligned}
 (4) - (3) & = \text{基準時刻に基づく第2信号の受信時刻} + D1 \\
 & - \text{基準時刻に基づく第2信号の送信時刻} - D2 \\
 & = \text{通信にかかる時間} + D1 - D2 \quad \dots (11)
 \end{aligned}$$

【0042】

したがって、上記(11)式から上記(8)式を減算すると、下記(12)式のように第1内部時刻の基準時刻からのずれD1と、第2内部時刻の基準時刻からのずれD2と、の差を算出することができる。

【0043】

$$(11) - (8) = D1 - D2 \quad \dots (12)$$

20

【0044】

このように、第1送信時刻111、第2受信時刻112、第1受信時刻121および第2送信時刻122に基づいて、第1装置110と第2装置120との間の通信にかかる時間を算出することができる。そして、算出した通信にかかる時間に基づいて、第1内部時刻と第2内部時刻との差を算出することができる。

【0045】

ただし、第1内部時刻と第2内部時刻との差を算出する手順は、上記の各式の手順に限らず、たとえば上記(10)式または上記(12)式の結果と同等の値を算出すればよい。たとえば、算出部220は、下記(13)式または下記(14)式によって第1内部時刻と第2内部時刻との差を算出することができる。

30

【0046】

$$\begin{aligned}
 (2) - (1) - ((2) - (1) + (3) - (4)) \div 2 & \quad \dots (13) \\
 (4) - (3) - ((2) - (1) + (3) - (4)) \div 2 & \quad \dots (14)
 \end{aligned}$$

【0047】

すなわち、たとえば算出部220は、第1受信時刻121および第1送信時刻111の差と、第2受信時刻112および第2送信時刻122の差と、の差の半分と、第1受信時刻121および第1送信時刻111の差と、の差を示す値を算出すればよい。または、算出部220は、第1受信時刻121および第1送信時刻111の差と、第2受信時刻112および第2送信時刻122の差と、の差の半分と、第2受信時刻112および第2送信時刻122の差と、の差を示す値を算出すればよい。

40

【0048】

また、情報処理装置200は、第1装置110および第2装置120との間で送受信された上記の第1信号101および第2信号102とは異なる信号の送受信時刻を取得してもよい。そして、情報処理装置200は、第1送信時刻111、第2受信時刻112、第1受信時刻121および第2送信時刻122の組を複数取得し、取得した組ごとに第1装置110および第2装置120の内部時刻のずれを算出してもよい。

【0049】

また、情報処理装置200は、取得した組ごとに算出したずれに基づいて、第1装置110および第2装置120の内部時刻のずれを算出してもよい。たとえば、情報処理装置200は、取得した組ごとに算出したずれを平均することによって第1装置110および

50

第2装置120の内部時刻のずれを算出する。これにより、たとえば突発的な通信の遅延等の影響を小さくし、第1装置110および第2装置120の内部時刻のずれをより正確に算出することができる。

【0050】

(情報処理装置のハードウェア構成)

図3は、実施の形態にかかる情報処理装置のハードウェア構成の一例を示す図である。図2に示した情報処理装置200は、たとえば図3に示す情報処理装置300によって実現することができる。情報処理装置300は、CPU301と、メモリ302と、ユーザインタフェース303と、通信インタフェース304と、を備えている。CPU301、メモリ302、ユーザインタフェース303および通信インタフェース304は、バス309によって接続されている。

10

【0051】

CPU301(Central Processing Unit)は、情報処理装置300の全体の制御を司る。メモリ302には、たとえばメインメモリおよび補助メモリが含まれる。メインメモリは、たとえばRAM(Random Access Memory)である。メインメモリは、CPU301のワークエリアとして使用される。補助メモリは、たとえば磁気ディスク、光ディスク、フラッシュメモリなどの不揮発メモリである。補助メモリには、情報処理装置300を動作させる各種のプログラムが記憶されている。補助メモリに記憶されたプログラムは、メインメモリにロードされてCPU301によって実行される。

20

【0052】

ユーザインタフェース303は、たとえば、ユーザからの操作入力を受け付ける入力デバイスや、ユーザへ情報を出力する出力デバイスなどを含む。入力デバイスは、たとえばキー(たとえばキーボード)やリモコンなどによって実現することができる。出力デバイスは、たとえばディスプレイやスピーカなどによって実現することができる。また、タッチパネルなどによって入力デバイスおよび出力デバイスを実現してもよい。ユーザインタフェース303は、CPU301によって制御される。

【0053】

通信インタフェース304は、たとえば、無線や有線によって情報処理装置300の外部(たとえば第1装置110や第2装置120)との間で通信を行う通信インタフェースである。通信インタフェース304は、CPU301によって制御される。たとえば、通信インタフェース304は、第1装置110および第2装置120のログを、通信インタフェース304を介して取得する。

30

【0054】

図2に示した取得部210は、たとえばCPU301、ユーザインタフェース303、通信インタフェース304などによって実現することができる。図2に示した算出部220は、たとえばCPU301などによって実現することができる。上記の作成部は、たとえばCPU301などによって実現することができる。

【0055】

(ログの処理対象の通信システム)

40

図4は、ログの処理対象の通信システムの一例を示す図である。図4に示す通信システムは、装置A~Dを含む。装置Aは、装置Bと接続されており、装置Bとの間で通信可能である。装置Cは、装置Bと接続されており、装置Bとの間で通信可能である。装置Dは、装置Bと接続されており、装置Bとの間で通信可能である。

【0056】

図4に示す例では、装置Aの内部時刻を基準時刻とする。そして、装置Bの内部時刻は、基準時刻に対して500[ms]遅れている(+500[ms])とする。また、装置Cの内部時刻は、基準時刻に対して500[ms]進んでいる(-500[ms])とする。また、装置Dの内部時刻は、基準時刻と一致している(+0[ms])とする。

【0057】

50

実施の形態にかかる情報処理装置 200 は、たとえば、装置 A ～ D がそれぞれの内部時刻に基づいて作成したログ 401 ～ 404 を取得する。そして、情報処理装置 200 は、取得したログに基づいて、装置 A ～ D のうちの少なくとも 2 つの装置の各内部時刻の間のずれを算出する。たとえば、情報処理装置 200 は、装置 A , B の各内部時刻の間のずれ（図 4 に示す例では + 500 [ms]）を算出する。これにより、装置 A , B の間の正確なシーケンスログを作成することが可能になる。

【0058】

この場合に、たとえば装置 A は上記の第 1 装置 110 に対応する構成であり、装置 B は上記の第 2 装置 120 に対応する構成である。以下、情報処理装置 200 が装置 A , B の各内部時刻の間のずれを算出し、算出したずれに基づいて装置 A , B の間のシーケンスログを作成する場合について説明する。

10

【0059】

また、以下の説明において、第 1 送信時刻 111、第 1 受信時刻 121、第 2 送信時刻 122 および第 2 受信時刻 112 に対応する各通信記録のキーワードをそれぞれ起句キーワード、承句キーワード、転句キーワードおよび結句キーワードと称する。

【0060】

（自動マージの処理）

図 5 は、自動マージの処理の一例を示すフローチャートである。情報処理装置 200 は、自動マージの処理として、たとえば以下の各ステップを実行する。まず、取得部 210 が、装置 A および装置 B の重複する時間範囲のログを取得する（ステップ S501）。

20

【0061】

つぎに、取得部 210 が、ステップ S501 によって取得した装置 A のログから類似文字を抽出する（ステップ S502）。類似文字は、互いに類似するキーワード群を示す文字である。つぎに、取得部 210 が、ステップ S502 によって抽出した類似文字ごとに、装置 A のログでの出現数および類似度を算出する（ステップ S503）。装置 A のログからの類似文字の抽出や出現数および類似度の算出については後述する（たとえば図 9 - 1 参照）。

【0062】

つぎに、取得部 210 が、ステップ S502 によって抽出した類似文字の中から、ステップ S503 によって算出した類似度が高く、ステップ S503 によって算出した出現数が多い類似文字を特定する。類似度が高く出現数が多い類似文字とは、たとえば、類似度および出現数が閾値以上である類似文字の中から選択された類似文字などである。そして、取得部 210 が、特定した類似文字に該当するキーワードを装置 A のログの中から起句キーワードとして抽出する（ステップ S504）。起句キーワードの抽出については後述する（たとえば図 10 - 1 参照）。

30

【0063】

つぎに、取得部 210 が、ステップ S501 によって取得した装置 B のログから類似文字を抽出する（ステップ S505）。つぎに、取得部 210 が、ステップ S505 によって抽出した類似文字ごとに、装置 B のログ B での出現数を算出する（ステップ S506）。装置 B のログからの類似文字の抽出や出現数の算出については後述する（たとえば図 9 - 2 参照）。

40

【0064】

つぎに、取得部 210 が、ステップ S505 によって抽出した類似文字の中から、ステップ S504 によって抽出した起句キーワードと、時刻が近く、ステップ S506 によって算出した出現数が同じ類似文字を特定する。時刻が近い類似文字とは、たとえば、対応時刻の差が閾値以下の類似文字などである。そして、取得部 210 が、特定した類似文字に該当するキーワードを装置 B のログの中から承句キーワードとして抽出する（ステップ S507）。承句キーワードの抽出については後述する（たとえば図 10 - 2 参照）。

【0065】

つぎに、取得部 210 が、ステップ S505 によって抽出した類似文字の中から、ステ

50

ップS507によって抽出した承句キーワードと、時刻が近く、ステップS506によって算出した出現数が同じ類似文字を特定する。そして、取得部210が、特定した類似文字に該当するキーワードを装置Bのログの中から転句キーワードとして抽出する(ステップS508)。転句キーワードの抽出については後述する(たとえば図10-3参照)。
【0066】

つぎに、取得部210が、ステップS502によって抽出した類似文字の中から、ステップS508によって抽出した転句キーワードと、時刻が近く、ステップS503によって算出した出現数が同じ類似文字を特定する。そして、取得部210が、特定した類似文字に該当するキーワードを装置Aのログの中から結句キーワードとして抽出する(ステップS509)。結句キーワードの抽出については後述する(たとえば図10-4参照)。
【0067】

そして、取得部210は、ステップS504によって抽出した起句キーワードに対応する装置Aのログの通信記録の時刻をたとえば上記の第1送信時刻111として取得する。また、取得部210は、ステップS507によって抽出した承句キーワードに対応する装置Bのログの通信記録の時刻をたとえば上記の第1受信時刻121として取得する。
【0068】

また、取得部210は、ステップS508によって抽出した転句キーワードに対応する装置Bのログの通信記録の時刻をたとえば上記の第2送信時刻122として取得する。また、取得部210は、ステップS509によって抽出した結句キーワードに対応する装置Aのログの通信記録の時刻をたとえば上記の第2受信時刻112として取得する。
【0069】

このように、取得部210は、装置Aおよび装置Bの各ログから類似文字を自動抽出し、出現数の多いキーワードを起句キーワード、承句キーワード、転句キーワードおよび結句キーワードとして自動マージすることができる。これにより、装置Aおよび装置Bの各ログから第1送信時刻111、第1受信時刻121、第2送信時刻122および第2受信時刻112を取得することができる。
【0070】

【0070】

なお、たとえばステップS504、S507、S508、S509において、抽出対象のキーワードに複数の候補が存在する場合は、ユーザに複数の候補を提示し、ユーザによって抽出するキーワードを選択させるようにしてもよい。これにより、より高精度なキーワードの抽出が可能になる。

【0071】

(自動時刻補正の処理)

図6は、自動時刻補正の処理の一例を示すフローチャートである。情報処理装置200は、自動時刻補正の処理として、たとえば以下の各ステップを実行する。まず、算出部220が、図5に示す各ステップによって取得部210によって取得された、起句キーワードに対応する装置Aのログの通信記録の時刻と、結句キーワードに対応する装置Aのログの通信記録の時刻と、の差を算出する(ステップS601)。これにより、装置Aのログの処理時間を算出することができる。
【0072】

【0072】

つぎに、算出部220が、図5に示す各ステップによって取得部210によって取得された、承句キーワードに対応する装置Bのログの通信記録の時刻と、転句キーワードに対応する装置Bのログの通信記録の時刻と、の差を算出する(ステップS602)。これにより、装置Bのログの処理時間を算出することができる。
【0073】

【0073】

つぎに、算出部220が、ステップS601によって算出した差と、ステップS602によって算出した差と、の差から装置Aと装置Bとの間の通信にかかる時間を算出する(ステップS603)。たとえば、装置Aから装置Bへの通信にかかる時間と、装置Bから装置Aへの通信にかかる時間と、が同じであると仮定する。この場合は、ステップS601、S602によって算出された各差の間の差を半分にすることによって装置Aと装置B

10

20

30

40

50

との間の通信にかかる時間を算出することができる。

【 0 0 7 4 】

つぎに、算出部 2 2 0 が、起句キーワードに対応する装置 A のログの通信記録の時刻に、ステップ S 6 0 3 によって算出された時間を加算した時刻と、承句キーワードに対応する装置 B のログの通信記録の時刻と、の差を算出する（ステップ S 6 0 4）。なお、ステップ S 6 0 4 において、算出部 2 2 0 が、転句キーワードに対応する装置 B のログの通信記録の時刻に、ステップ S 6 0 3 によって算出された時間を加算した時刻と、結句キーワードに対応する装置 A のログの通信記録の時刻と、の差を算出してもよい。

【 0 0 7 5 】

つぎに、算出部 2 2 0 が、ステップ S 6 0 4 によって算出した差を装置 A と装置 B との間の内部時刻のずれとして出力し（ステップ S 6 0 5）、一連の処理を終了する。これにより、第 1 送信時刻 1 1 1、第 1 受信時刻 1 2 1、第 2 送信時刻 1 2 2 および第 2 受信時刻 1 1 2 に基づく装置 A、B の内部時刻のずれを得ることができる。

【 0 0 7 6 】

（装置 A ～ D によって記憶されたログ）

図 7 - 1 は、装置 A によって記憶されたログの一例を示す図である。図 7 - 2 は、装置 B によって記憶されたログの一例を示す図である。図 7 - 3 は、装置 C によって記憶されたログの一例を示す図である。図 7 - 4 は、装置 D によって記憶されたログの一例を示す図である。図 7 - 1 ～ 図 7 - 4 に示すログ 4 0 1 ～ 4 0 4 は、それぞれ装置 A ～ D によって記憶されたログである（たとえば図 4 参照）。ログ 4 0 1 ～ 4 0 4 のそれぞれには、項目として「日付」、「時刻」、「ホスト名」、「ユーザ名」、「種類」、「通信方向」、「通信相手」および「ログメッセージ」が含まれている。

【 0 0 7 7 】

項目「日付」および項目「時刻」は、内部時刻に基づく、対象通信が行われた時刻である。項目「ホスト名」および項目「ユーザ名」は、対象通信における自装置のホスト名およびユーザ名である。装置 A ～ D のホスト名はそれぞれ「h o s t A」～「h o s t D」となっている。項目「種類」は、対象通信の種類である。項目「種類」の値「I N F O」はたとえば情報通信を示している。項目「種類」の値「E R R O R」はたとえばエラー通知を示している。

【 0 0 7 8 】

項目「通信方向」は、対象通信の方向を示している。項目「通信方向」の値「S E N D」は、対象通信が自装置からの送信であることを示している。項目「通信方向」の値「R E C V」は、対象通信が自装置による受信であることを示している。項目「通信相手」は、対象通信の相手の装置を示している。項目「通信相手」の値は、装置 A ～ D のうちの自装置に接続された装置のホスト名となる。項目「ログメッセージ」は、たとえば、対象通信によって伝送された情報のうちのログとして記憶されたメッセージや、対象通信のその他の情報を示している。

【 0 0 7 9 】

また、ログ 4 0 1 ～ 4 0 4 とともに図示した「I N」および「O U T」は、各装置間の通信の対応関係を示している。たとえば、図 7 - 1 の「O U T」の「A - 1」に対応する装置 A からの送信にかかる通信（ログ 4 0 1 の一行目の通信）は、図 7 - 2 の「I N」の「A - 1」に対応する装置 B による受信にかかる通信（ログ 4 0 2 の一行目の通信）と対応している。

【 0 0 8 0 】

（ログ形式のパターンファイル）

図 8 は、ログ形式のパターンファイルの一例を示す図である。図 7 - 1 ～ 図 7 - 4 に示したログ 4 0 1 ～ 4 0 4 は、たとえば装置 A ～ 装置 B に記憶されたパターンファイル 8 0 0 の定義にしたがって作成される。パターンファイル 8 0 0 においては、「データ項目」として「項目 1」～「項目 8」が定義されている。「項目 1」～「項目 8」はそれぞれ図 7 - 1 ～ 図 7 - 4 に示した項目「日付」、「時刻」、「ホスト名」、「ユーザ名」、「種

10

20

30

40

50

類」、「通信方向」、「通信相手」および「ログメッセージ」に対応する。

【0081】

また、パターンファイル800においては、「項目1」～「項目8」のそれぞれについて「データ型」、「データ形式」および「入力情報」が定義されている。「入力情報」においては、時刻補正する項目として「日付」および「時刻」が指定されている。また、「入力情報」においては、類似度を算出する「キーワード」が指定されている。

【0082】

(ログに基づく類似度の算出結果)

図9-1は、装置Aのログに基づく類似度の算出結果の一例を示す図である。図9-1に示す類似度算出テーブル901は、装置Aのログ401に基づく類似度の算出結果の一例を示す図である。情報処理装置200は、装置Aのログ401について、「通信相手」別に、ログメッセージに含まれるキーワードから類似文字を抽出する。なお、キーワード中の「x」や「y」は任意の文字とする。

【0083】

類似度の抽出は、たとえば、図8に示したパターンファイル800の「キーワード」を対象に文字列を抽出することによって行うことができる。たとえば、情報処理装置200は、通信相手別に「キーワード」に対して類似文字数を減らしながらフィルタリングを行い、出現数の変化のあった類似文字で、類似文字数、出現数および類似度を算出する。

【0084】

たとえば、情報処理装置200は、ログ401のログメッセージの中から複数回出現するキーワードを「類似文字」として抽出する。そして、情報処理装置200は、抽出した「類似文字」ごとに、「類似文字」の文字数を示す「類似文字数」および「出現数」を導出し、導出した「類似文字数」および「出現数」に基づいて「類似度」を算出する。「類似度」は、たとえば(類似文字数) $\times \log$ (出現数)によって算出することができる。

【0085】

たとえば、情報処理装置200は、ログ401で2回出現しているキーワード「SEARCH xxx01 yyy01」を類似文字として抽出する。類似文字「SEARCH xxx01 yyy01」の文字数は18文字であるため「類似文字数」は18となる。また、類似文字「SEARCH xxx01 yyy01」の出現数は2回であるため「出現数」は2となる。そして、「類似文字数」 $\times \log$ (出現数) $= 18 \times \log(2)$ によって「類似度」は約5.418539922と算出される。

【0086】

図9-2は、装置Bのログに基づく類似度の算出結果の一例を示す図である。図9-2に示す類似度算出テーブル902は、装置Bのログ402に基づく類似度の算出結果の一例を示す図である。情報処理装置200は、装置Bのログ402についても同様に、「通信相手」別に、ログメッセージに含まれるキーワードから類似文字を抽出する。そして、情報処理装置200は、抽出した「類似文字」ごとに、「類似文字」の文字数を示す「類似文字数」および「出現数」を導出し、導出した「類似文字数」および「出現数」に基づいて「類似度」を算出する。

【0087】

たとえば、情報処理装置200は、ログ402で2回出現しているキーワード「SEARCH xxx01 yyy01」を類似文字として抽出する。類似文字「SEARCH xxx01 yyy01」の文字数は18文字であるため「類似文字数」は18となる。また、類似文字「SEARCH xxx01 yyy01」の出現数は2回であるため「出現数」は2となる。そして、「類似文字数」 $\times \log$ (出現数) $= 18 \times \log(2)$ によって「類似度」は約5.418539922と算出される。

【0088】

(キーワードの抽出結果)

図10-1～図10-4は、キーワードの抽出結果の一例を示す図である。情報処理装置200は、図9-1の類似度算出テーブル901および図9-2の類似度算出テーブル

10

20

30

40

50

902に基づいて、装置Aのログ401および装置Bのログ402から、起句キーワード、承句キーワード、転句キーワードおよび結句キーワードを抽出する。

【0089】

具体的には、情報処理装置200は、装置Aのログ401から、出現数および類似度が高い類似文字を起句キーワードとして抽出する。たとえば、情報処理装置200は、図10-1に示すように、ログ401の通信履歴1001の類似文字「SEARCH xxx01 yyy01」を起句キーワードとして抽出したとする。

【0090】

つぎに、情報処理装置200は、装置Bのログ402から、起句キーワードとして抽出した類似文字「SEARCH xxx01 yyy01」と出現数が同じであり、通信履歴1001との時刻差が小さい類似文字を承句キーワードとして抽出する。たとえば、情報処理装置200は、図10-2に示すように、ログ402の通信履歴1002の類似文字「SEARCH xxx01 yyy01」を承句キーワードとして抽出したとする。

【0091】

つぎに、情報処理装置200は、装置Bのログ402から、承句キーワードとして抽出した類似文字「SEARCH xxx01 yyy01」と出現数が同じであり、通信履歴1002との時刻差が小さい類似文字を転句キーワードとして抽出する。たとえば、情報処理装置200は、図10-3に示すように、ログ402の通信履歴1003の類似文字「SEARCH xxx01 yyy01」を転句キーワードとして抽出したとする。

【0092】

つぎに、情報処理装置200は、装置Aのログ401から、転句キーワードとして抽出した類似文字「SEARCH xxx01 yyy01」と出現数が同じであり、通信履歴1003との時刻差が小さい類似文字を結句キーワードとして抽出する。たとえば、情報処理装置200は、図10-4に示すように、ログ401の通信履歴1004の類似文字「SEARCH xxx01 yyy01」を結句キーワードとして抽出したとする。

【0093】

これにより、たとえば上記の第1送信時刻111として、通信履歴1001の時刻「10:54:10.000」を取得することができる。また、たとえば上記の第1受信時刻121として、通信履歴1002の時刻「10:54:10.505」を取得することができる。また、たとえば上記の第2送信時刻122として、通信履歴1003の時刻「10:54:10.695」を取得することができる。また、たとえば上記の第2受信時刻112として、通信履歴1004の時刻「10:54:10.200」を取得することができる。

【0094】

(ログの処理時間の算出結果)

図11-1および図11-2は、ログの処理時間の算出結果の一例を示す図である。情報処理装置200は、図11-1に示すように、装置Aのログ401の通信履歴1001の時刻「10:54:10.000」(起句キーワード)と、通信履歴1004の時刻「10:54:10.200」(結句キーワード)と、の差を算出する。これにより、装置Aのログの処理時間として200[m s]を算出することができる。

【0095】

また、情報処理装置200は、図11-2に示すように、装置Bのログ402の通信履歴1002の時刻「10:54:10.505」(承句キーワード)と、通信履歴1003の時刻「10:54:10.695」(転句キーワード)と、の差を算出する。これにより、装置Bのログの処理時間として190[m s]を算出することができる。

【0096】

そして、情報処理装置200は、装置Aの処理時間である200[m s]と、装置Bの処理時間である190[m s]と、の差の半分を算出する。これにより、装置Aと装置Bとの間の通信にかかる時間として $(200 - 190) \div 2 = 5$ [m s]を算出することができる。

10

20

30

40

50

【 0 0 9 7 】

つぎに、情報処理装置 2 0 0 は、装置 A のログ 4 0 1 の通信履歴 1 0 0 1 の時刻「 1 0 : 5 4 : 1 0 . 0 0 0 」(起句キーワード)に、装置 A と装置 B との間の通信にかかる時間である 5 [m s] を加算する。そして、加算結果と、装置 B のログ 4 0 2 の通信履歴 1 0 0 2 の時刻「 1 0 : 5 4 : 1 0 . 5 0 5 」(承句キーワード)と、の差を算出する。これにより、装置 A の内部時刻と、装置 B の内部時刻と、のずれとして 5 0 0 [m s] を算出することができる。

【 0 0 9 8 】

(ログの補正結果)

図 1 2 は、装置 B のログの補正結果の一例を示す図である。情報処理装置 2 0 0 は、たとえば、図 7 - 2 に示した装置 B のログ 4 0 2 の「時刻」を、装置 A , B の内部時刻のずれとして算出した 5 0 0 [m s] によって補正する。具体的には、情報処理装置 2 0 0 は、ログ 4 0 2 の「時刻」の各値から 5 0 0 [m s] を減算することによりログ 4 0 2 の「時刻」を補正する。

10

【 0 0 9 9 】

ただし、装置 A , B の内部時刻のずれの算出結果によるログの補正はこれに限らない。たとえば、情報処理装置 2 0 0 は、装置 A のログ 4 0 1 の「時刻」の各値に 5 0 0 [m s] を加算することによりログ 4 0 1 の「時刻」を補正してもよい。

【 0 1 0 0 】

(シーケンスログ)

図 1 3 は、シーケンスログの一例を示す図である。たとえば図 1 2 に示した補正後の装置 B のログ 4 0 2 と、図 4 - 1 に示した装置 A のログ 4 0 1 と、を用いることにより、ログ 4 0 1 , 4 0 2 においてそれぞれ基準となっている時刻のずれが解消した状態でシーケンスログ 1 3 0 0 を作成することが可能になる。このため、装置 A と装置 B との間の通信動作の履歴を示す正確なシーケンスログ 1 3 0 0 を作成することが可能になる。

20

【 0 1 0 1 】

シーケンスログ 1 3 0 0 は、たとえば、装置 A と装置 B との間で行われた各通信を時刻とともに視覚的に示す情報である。シーケンスログ 1 3 0 0 は、情報処理装置 2 0 0 によって算出された内部時刻のずれに基づいてユーザによって作成される。また、シーケンスログ 1 3 0 0 は、上記の情報処理装置 2 0 0 の作成部によって作成されてもよい。このとき、たとえばユーザ入力によって、通信履歴 1 0 0 1 によって算出された内部時刻のずれを微調整できるようにしてもよい。

30

【 0 1 0 2 】

また、情報処理装置 2 0 0 が装置 A および装置 B の各ログから第 1 送信時刻 1 1 1、第 1 受信時刻 1 2 1、第 2 送信時刻 1 2 2 および第 2 受信時刻 1 1 2 を自動的に(または半自動的に)に取得する場合について説明したが、このような構成に限らない。たとえば、図 7 - 1 に示した装置 A のログ 4 0 1 と、図 7 - 2 に示した装置 B のログ 4 0 2 と、をユーザに表示し、上記の通信履歴 1 0 0 1 ~ 1 0 0 4 をユーザ操作によって選択させるようにしてもよい。

【 0 1 0 3 】

このとき、たとえばログ 4 0 1 とログ 4 0 2 の間で時刻の近い通信記録同士を対応付けて(たとえば高さを合わせる等)表示することによって、上記の通信履歴 1 0 0 1 ~ 1 0 0 4 をユーザが容易に選択することができる。上記の通信履歴 1 0 0 1 ~ 1 0 0 4 をユーザが選択することにより、選択された通信履歴 1 0 0 1 ~ 1 0 0 4 に基づいて情報処理装置 2 0 0 が第 1 送信時刻 1 1 1、第 1 受信時刻 1 2 1、第 2 送信時刻 1 2 2 および第 2 受信時刻 1 1 2 を取得することができる。

40

【 0 1 0 4 】

また、ここでは装置 A および装置 B の間のシーケンスログを作成する場合について説明したが、装置 C や装置 D も含めたシーケンスログを作成することも可能である。たとえば、情報処理装置 2 0 0 は、装置 C や装置 D における内部時刻の基準時刻からのずれについ

50

ても算出する。これにより、算出結果に基づいて装置 A ~ D のログ 4 0 1 ~ 4 0 4 の時刻を補正し、装置 A ~ D の間のシーケンスログを作成することが可能になる。

【 0 1 0 5 】

以上説明したように、プログラム、情報処理装置および情報処理方法によれば、装置間の双方向の各通信について各装置で記憶された送受信時刻から各装置の内部時刻のずれを求めることができる。これにより、装置間の正確なシーケンスログを作成することが可能になる。

【 0 1 0 6 】

また、各通信装置における同一期間（所定期間）のログを取得し、取得した各ログから装置間の双方向の各通信について各装置で記憶された送受信時刻を自動的に抽出することができる。また、各ログから、互いに時間差の小さい通信記録を抽出することにより、装置間の双方向の各通信について各装置で記憶された送受信時刻を精度よく抽出することができる。また、抽出した送受信時刻にかかる各通信の条件（たとえば通信にかかる時間）が近くなりやすくなり、送受信時刻に基づく内部時刻のずれの算出精度の向上を図ることができる。また、類似文字の類似度を用いて各通信記録を抽出することにより、抽出した送受信時刻にかかる各通信の条件（たとえば通信にかかる時間）が近くなりやすくなり、装置間の双方向の各通信について各装置で記憶された送受信時刻を精度よく抽出することができる。

【 0 1 0 7 】

なお、本実施の形態で説明した情報処理方法は、予め用意されたプログラムをパーソナル・コンピュータやワークステーション等のコンピュータで実行することにより実現することができる。このプログラムは、ハードディスク、フレキシブルディスク、CD-ROM、MO、DVD等のコンピュータで読み取り可能な記録媒体に記録され、コンピュータによって記録媒体から読み出されることによって実行される。またこのプログラムは、インターネット等のネットワークを介して配布することが可能な伝送媒体であってもよい。

【 0 1 0 8 】

上述した実施の形態に関し、さらに以下の付記を開示する。

【 0 1 0 9 】

（付記 1）装置間で重複する時間範囲のログをそれぞれの装置から取得し、

取得したそれぞれのログから、一方の装置から送信され他方の装置が受信した第 1 の一対のログおよび該他方の装置から送信して該一方の装置が受信した第 2 の一対のログを抽出し、

抽出した前記第 1 および前記第 2 の一対のログから前記一方の装置および前記他方の装置の時刻のずれを算出する

処理をコンピュータに実行させることを特徴とするプログラム。

【 0 1 1 0 】

（付記 2）第 1 内部時刻によってログを記憶する第 1 装置と、第 2 内部時刻によってログを記憶する第 2 装置と、のログに関する処理を行う情報処理装置であって、

前記第 1 装置が第 1 信号を送信した前記第 1 内部時刻に基づく第 1 送信時刻と、前記第 1 信号を前記第 2 装置が受信した前記第 2 内部時刻に基づく第 1 受信時刻と、前記第 2 装置が第 2 信号を送信した前記第 2 内部時刻に基づく第 2 送信時刻と、前記第 2 信号を前記第 1 装置が受信した前記第 1 内部時刻に基づく第 2 受信時刻と、を取得する取得部と、

前記取得部によって取得された前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出する算出部と、

を備えることを特徴とする情報処理装置。

【 0 1 1 1 】

（付記 3）前記算出部は、

前記第 1 受信時刻および前記第 1 送信時刻の差と、前記第 2 受信時刻および前記第 2 送信時刻の差と、の差の半分と、

10

20

30

40

50

前記第 1 受信時刻および前記第 1 送信時刻の差または前記第 2 受信時刻および前記第 2 送信時刻の差と、

の差を示す値を算出することによって前記第 1 内部時刻と前記第 2 内部時刻との差を算出することを特徴とする付記 2 に記載の情報処理装置。

【0112】

(付記 4) 前記算出部は、前記第 1 装置と前記第 2 装置との間の通信にかかる時間を算出し、算出した前記通信にかかる時間に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出することを特徴とする付記 2 または 3 に記載の情報処理装置。

【0113】

(付記 5) 前記算出部は、前記第 1 受信時刻および前記第 2 受信時刻との和と、前記第 1 送信時刻および前記第 2 送信時刻との和と、の差に基づいて前記通信にかかる時間を算出することを特徴とする付記 4 に記載の情報処理装置。

【0114】

(付記 6) 前記算出部は、前記通信にかかる時間と、前記第 1 送信時刻および前記第 1 受信時刻の差または前記第 2 送信時刻および前記第 2 受信時刻の差と、の差に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出することを特徴とする付記 4 または 5 に記載の情報処理装置。

【0115】

(付記 7) 前記取得部は、

前記第 1 装置によって記憶された所定期間内の第 1 ログと、前記第 2 装置によって記憶された前記所定期間内の第 2 ログと、を取得し、

取得した前記第 1 ログに含まれる前記第 1 信号の第 1 通信記録から前記第 1 送信時刻を取得し、

取得した前記第 2 ログの中から、取得した前記第 1 送信時刻との時間差が閾値以下の第 2 通信記録を抽出することにより前記第 1 受信時刻を取得し、

取得した前記第 2 ログの中から、取得した前記第 1 受信時刻との時間差が閾値以下の第 3 通信記録を抽出することにより前記第 2 送信時刻を取得し、

取得した前記第 1 ログの中から、取得した前記第 2 送信時刻との時間差が閾値以下の第 4 通信記録を抽出することにより前記第 2 受信時刻を取得することを特徴とする付記 2 ~ 6 のいずれか一つに記載の情報処理装置。

【0116】

(付記 8) 前記取得部は、

取得した前記第 1 ログの中から互いに類似する類似文字を抽出し、前記第 1 ログの中から抽出した類似文字ごとに、前記類似文字に該当するキーワードの前記第 1 ログにおける出現数を算出し、

取得した前記第 2 ログの中から互いに類似する類似文字を抽出し、前記第 2 ログの中から抽出した類似文字ごとに、前記類似文字に該当するキーワードの前記第 2 ログにおける出現数を算出し、

前記第 1 ログの中から抽出した類似文字から、算出した前記出現数に基づいて第 1 類似文字を選択し、選択した前記第 1 類似文字のキーワードを含む前記第 1 通信記録を前記第 1 ログから抽出することにより前記第 1 送信時刻を取得し、

前記第 2 ログの中から抽出した類似文字のうちの算出した前記出現数が前記第 1 類似文字と同じである第 2 類似文字のキーワードを含む前記第 2 通信記録を前記第 2 ログから抽出することにより前記第 1 受信時刻を取得し、

前記第 2 ログの中から抽出した類似文字のうちの算出した前記出現数が前記第 2 類似文字と同じである第 3 類似文字のキーワードを含む前記第 3 通信記録を前記第 2 ログから抽出することにより前記第 2 送信時刻を取得し、

前記第 1 ログの中から抽出した類似文字のうちの算出した前記出現数が前記第 3 類似文字と同じである第 4 類似文字のキーワードを含む前記第 4 通信記録を前記第 1 ログから抽出することにより前記第 2 受信時刻を取得する、

10

20

30

40

50

ことを特徴とする付記 7 に記載の情報処理装置。

【0117】

(付記 9) 前記取得部は、前記第 1 ログの中から抽出した類似文字ごとに、前記類似文字に含まれる各キーワードの類似度を算出し、算出した前記出現数および前記類似度に基づいて前記第 1 類似文字を選択することを特徴とする付記 8 に記載の情報処理装置。

【0118】

(付記 10) 前記類似度は、前記類似文字の文字数に基づいて算出されることを特徴とする付記 9 に記載の情報処理装置。

【0119】

(付記 11) 前記第 1 装置によって記憶された所定期間内のログと、前記第 2 装置によって記憶された前記所定期間内のログと、前記算出部によって算出された差と、に基づいて、前記第 1 装置および前記第 2 装置の間で行われた通信の履歴を示すシーケンスログを作成する作成部を備えることを特徴とする付記 2 ~ 10 のいずれか一つに記載の情報処理装置。

10

【0120】

(付記 12) 前記取得部は、前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻の組を複数取得し、

前記算出部は、前記組ごとに、前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻に基づく前記第 1 内部時刻と前記第 2 内部時刻との差を算出し、前記組ごとの算出結果に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出することを特徴とする付記 2 ~ 11 のいずれか一つに記載の情報処理装置。

20

【0121】

(付記 13) 第 1 内部時刻によってログを記憶する第 1 装置と、第 2 内部時刻によってログを記憶する第 2 装置と、のログに関する処理を行う情報処理装置に、

前記第 1 装置が第 1 信号を送信した前記第 1 内部時刻に基づく第 1 送信時刻と、前記第 1 信号を前記第 2 装置が受信した前記第 2 内部時刻に基づく第 1 受信時刻と、前記第 2 装置が第 2 信号を送信した前記第 2 内部時刻に基づく第 2 送信時刻と、前記第 2 信号を前記第 1 装置が受信した前記第 1 内部時刻に基づく第 2 受信時刻と、を取得し、

取得した前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出する、

30

処理を実行させることを特徴とするプログラム。

【0122】

(付記 14) 第 1 内部時刻によってログを記憶する第 1 装置と、第 2 内部時刻によってログを記憶する第 2 装置と、のログに関する処理を行う情報処理装置により、

前記第 1 装置が第 1 信号を送信した前記第 1 内部時刻に基づく第 1 送信時刻と、前記第 1 信号を前記第 2 装置が受信した前記第 2 内部時刻に基づく第 1 受信時刻と、前記第 2 装置が第 2 信号を送信した前記第 2 内部時刻に基づく第 2 送信時刻と、前記第 2 信号を前記第 1 装置が受信した前記第 1 内部時刻に基づく第 2 受信時刻と、を取得し、

取得した前記第 1 送信時刻、前記第 1 受信時刻、前記第 2 送信時刻および前記第 2 受信時刻に基づいて前記第 1 内部時刻と前記第 2 内部時刻との差を算出する、

40

ことを特徴とする情報処理方法。

【符号の説明】

【0123】

- 101 第 1 信号
- 102 第 2 信号
- 110 第 1 装置
- 111 第 1 送信時刻
- 112 第 2 受信時刻
- 120 第 2 装置
- 121 第 1 受信時刻

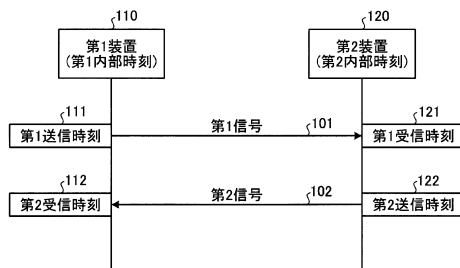
50

1 2 2 第 2 送信時刻
 2 0 0 , 3 0 0 情報処理装置
 2 1 0 取得部
 2 2 0 算出部
 3 0 1 C P U
 3 0 2 メモリ
 3 0 3 ユーザインタフェース
 3 0 4 通信インタフェース
 3 0 9 バス
 4 0 1 ~ 4 0 4 ログ
 8 0 0 パターンファイル
 9 0 1 , 9 0 2 類似度算出テーブル
 1 0 0 1 ~ 1 0 0 4 通信履歴
 1 3 0 0 シーケンスログ

10

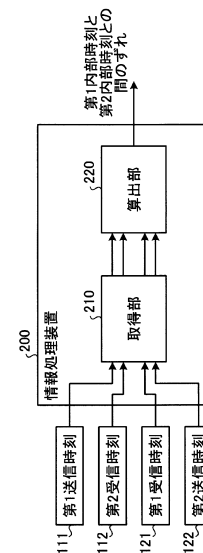
【図 1】

実施の形態にかかる情報処理装置によって取得される各時刻の一例を示す図



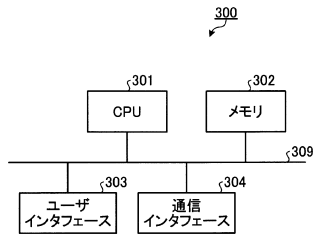
【図 2】

実施の形態にかかる情報処理装置の構成の一例を示す図



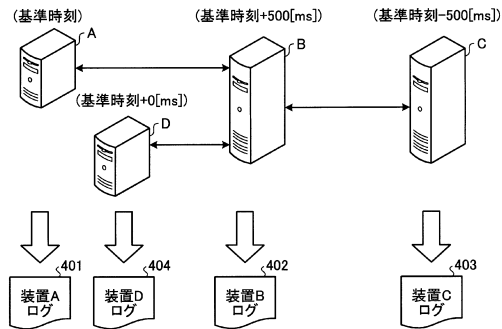
【 図 3 】

実施の形態にかかる情報処理装置のハードウェア構成の一例を示す図



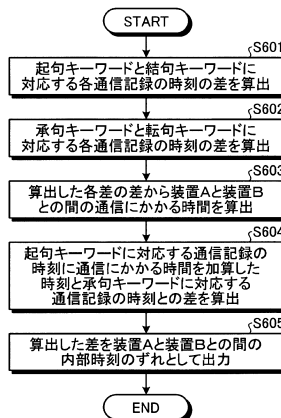
【 図 4 】

ログの処理対象の通信システムの一例を示す図



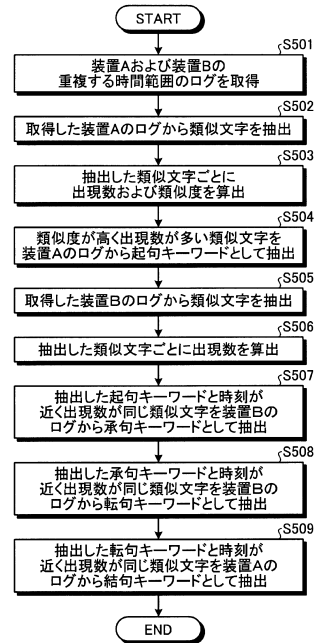
【 図 6 】

自動時刻補正の処理の一例を示すフローチャート



【 図 5 】

自動マージの処理の一例を示すフローチャート



【圖 7 - 1】

装置Aによって記憶されたログの一例を示す図

装置A ログ	時刻		ユーザ名	種類	通信相手		ログメッセージ	OUT
	日付	時刻			SEND	RECV		
	2011/08/05	10:54:00.000	hostA user01	INFO	SEND	hostB	LOGIN xxx01	A-1
	2011/08/05	10:54:00.000	hostA user01	INFO	RECV	hostB	LOGIN xxx01	A-2
	2011/08/05	10:54:01.000	hostA user01	INFO	INFO	hostB	TOP xxx01	A-3
	2011/08/05	10:54:01.000	hostA user01	INFO	INFO	hostB	TOP xxx01	A-4
	2011/08/05	10:54:01.200	hostA user01	INFO	RECV	hostB	TOP xxx01	A-5
	2011/08/05	10:54:05.000	hostA user01	INFO	SEND	hostB	MENU 1 xxx01	A-6
	2011/08/05	10:54:05.200	hostA user01	INFO	RECV	hostB	MENU 1 xxx01	A-7
	2011/08/05	10:54:10.000	hostA user01	INFO	SEND	hostB	SEARCH xxx01 yyy01	A-8
	2011/08/05	10:54:10.200	hostA user01	INFO	RECV	hostB	SEARCH xxx01 yyy01	A-9
	2011/08/05	10:54:40.000	hostA user01	INFO	SEND	hostB	UPDATE xxx01 yyy01	A-10
	2011/08/05	10:54:40.200	hostA user01	ERROR	RECV	hostB	UPDATE xxx01 yyy01	A-11
	2011/08/05	10:54:50.000	hostA user01	INFO	SEND	hostB	MENU 2 zzz01	A-12
	2011/08/05	10:55:00.000	hostA user01	INFO	RECV	hostB	MENU 2 zzz01	A-13
	2011/08/05	10:55:00.200	hostA user01	INFO	SEND	hostB	LOGOUT xxx01	A-14
	2011/08/05	10:55:00.200	hostA user01	INFO	RECV	hostB	LOGOUT xxx01	A-14

装置Bによって記憶されたログの一例を示す図

装置B ログ					
IN	日付	時刻	ユーザ名	種類	通信相手
A-1	2011/08/05	10:54:00.505	hostB	INFO	hostA
D-1	2011/08/05	10:54:00.510	user01	INFO	hostA
B-1	2011/08/05	10:54:00.515	hostB	INFO	hostA
	2011/08/05	10:54:00.520	user01	INFO	hostA
	2011/08/05	10:54:00.525	hostB	INFO	hostA
	2011/08/05	10:54:00.530	user01	INFO	hostA
B-2	2011/08/05	10:54:00.535	hostB	INFO	hostA
	2011/08/05	10:54:00.540	user01	INFO	hostA
	2011/08/05	10:54:00.545	hostB	INFO	hostA
	2011/08/05	10:54:00.550	user01	INFO	hostA
B-3	2011/08/05	10:54:00.555	hostB	INFO	hostA
	2011/08/05	10:54:00.560	user01	INFO	hostA
	2011/08/05	10:54:00.565	hostB	INFO	hostA
	2011/08/05	10:54:00.570	user01	INFO	hostA
B-4	2011/08/05	10:54:00.575	hostB	INFO	hostA
	2011/08/05	10:54:00.580	user01	INFO	hostA
	2011/08/05	10:54:00.585	hostB	INFO	hostA
	2011/08/05	10:54:00.590	user01	INFO	hostA
A-2	2011/08/05	10:54:00.595	hostB	INFO	hostA
	2011/08/05	10:54:00.600	user01	INFO	hostA
	2011/08/05	10:54:00.605	hostB	INFO	hostA
	2011/08/05	10:54:00.610	user01	INFO	hostA
D-2	2011/08/05	10:54:00.615	hostB	INFO	hostA
	2011/08/05	10:54:00.620	user01	INFO	hostA
	2011/08/05	10:54:00.625	hostB	INFO	hostA
	2011/08/05	10:54:00.630	user01	INFO	hostA
A-3	2011/08/05	10:54:00.635	hostB	INFO	hostA
	2011/08/05	10:54:00.640	user01	INFO	hostA
	2011/08/05	10:54:00.645	hostB	INFO	hostA
	2011/08/05	10:54:00.650	user01	INFO	hostA
D-3	2011/08/05	10:54:00.655	hostB	INFO	hostA
	2011/08/05	10:54:00.660	user01	INFO	hostA
	2011/08/05	10:54:00.665	hostB	INFO	hostA
	2011/08/05	10:54:00.670	user01	INFO	hostA
D-4	2011/08/05	10:54:00.675	hostB	INFO	hostA
	2011/08/05	10:54:00.680	user01	INFO	hostA
	2011/08/05	10:54:00.685	hostB	INFO	hostA
	2011/08/05	10:54:00.690	user01	INFO	hostA
A-5	2011/08/05	10:54:00.695	hostB	INFO	hostA
	2011/08/05	10:54:00.700	user01	INFO	hostA
	2011/08/05	10:54:00.705	hostB	INFO	hostA
	2011/08/05	10:54:00.710	user01	INFO	hostA
A-6	2011/08/05	10:54:00.715	hostB	INFO	hostA
	2011/08/05	10:54:00.720	user01	INFO	hostA
	2011/08/05	10:54:00.725	hostB	INFO	hostA
	2011/08/05	10:54:00.730	user01	INFO	hostA
A-7	2011/08/05	10:54:00.735	hostB	INFO	hostA
	2011/08/05	10:54:00.740	user01	INFO	hostA
	2011/08/05	10:54:00.745	hostB	INFO	hostA
	2011/08/05	10:54:00.750	user01	INFO	hostA
A-8	2011/08/05	10:54:00.755	hostB	INFO	hostA
	2011/08/05	10:54:00.760	user01	INFO	hostA
	2011/08/05	10:54:00.765	hostB	INFO	hostA
	2011/08/05	10:54:00.770	user01	INFO	hostA
A-9	2011/08/05	10:54:00.775	hostB	INFO	hostA
	2011/08/05	10:54:00.780	user01	INFO	hostA
	2011/08/05	10:54:00.785	hostB	INFO	hostA
	2011/08/05	10:54:00.790	user01	INFO	hostA
A-10	2011/08/05	10:54:00.795	hostB	INFO	hostA
	2011/08/05	10:54:00.800	user01	INFO	hostA
	2011/08/05	10:54:00.805	hostB	INFO	hostA
	2011/08/05	10:54:00.810	user01	INFO	hostA
A-11	2011/08/05	10:54:00.815	hostB	INFO	hostA
	2011/08/05	10:54:00.820	user01	INFO	hostA
	2011/08/05	10:54:00.825	hostB	INFO	hostA
	2011/08/05	10:54:00.830	user01	INFO	hostA
A-12	2011/08/05	10:54:00.835	hostB	INFO	hostA
	2011/08/05	10:54:00.840	user01	INFO	hostA
	2011/08/05	10:54:00.845	hostB	INFO	hostA
	2011/08/05	10:54:00.850	user01	INFO	hostA
A-13	2011/08/05	10:54:00.855	hostB	INFO	hostA
	2011/08/05	10:54:00.860	user01	INFO	hostA
	2011/08/05	10:54:00.865	hostB	INFO	hostA
	2011/08/05	10:54:00.870	user01	INFO	hostA
A-14	2011/08/05	10:54:00.875	hostB	INFO	hostA
	2011/08/05	10:54:00.880	user01	INFO	hostA
	2011/08/05	10:54:00.885	hostB	INFO	hostA
	2011/08/05	10:54:00.890	user01	INFO	hostA
D-5	2011/08/05	10:54:00.895	hostB	INFO	hostA
	2011/08/05	10:54:00.900	user01	INFO	hostA
	2011/08/05	10:54:00.905	hostB	INFO	hostA
	2011/08/05	10:54:00.910	user01	INFO	hostA
D-6	2011/08/05	10:54:00.915	hostB	INFO	hostA
	2011/08/05	10:54:00.920	user01	INFO	hostA
	2011/08/05	10:54:00.925	hostB	INFO	hostA
	2011/08/05	10:54:00.930	user01	INFO	hostA

装置Dによって記憶されたログの一例を示す図

装置D ログ					
OUT	日付	時刻	ユーザ名	種類	通信相手
D-1	2011/08/05	10:54:00.005	hostD	INFO	hostB
D-2	2011/08/05	10:54:00.265	user02	INFO	hostB
D-3	2011/08/05	10:54:02.005	hostD	INFO	hostB
D-4	2011/08/05	10:54:02.205	user02	INFO	hostB
D-5	2011/08/05	10:55:30.005	hostD	INFO	hostB
D-6	2011/08/05	10:55:30.205	user02	INFO	hostB

装置Cによって記憶されたログの一例を示す図

装置C ログ					
IN	日付	時刻	ユーザ名	種類	通信相手
B-1	2011/08/05	10:53:59.520	hostC	INFO	hostB
B-2	2011/08/05	10:53:59.680	user01	INFO	hostB
B-3	2011/08/05	10:53:59.690	hostC	INFO	hostB
B-4	2011/08/05	10:53:59.740	user02	INFO	hostB
B-5	2011/08/05	10:54:59.520	hostC	INFO	hostB
B-6	2011/08/05	10:54:59.680	user01	INFO	hostB
B-7	2011/08/05	10:55:29.525	hostC	INFO	hostB
B-8	2011/08/05	10:55:29.685	user02	INFO	hostB

ログ形式のパターンファイルの一例を示す図

データ項目	名称	データ型	データ形式	入力情報
項目1	日付	日付	YYYY/MM/DD	日付
項目2	時刻	時刻	hh:mm:ss.999	時刻
項目3	ホスト名	文字列	任意	
項目4	ユーザ名	文字列	任意	
項目5	種類	文字列	任意	
項目6	通信方向	文字列	任意	
項目7	通信相手	文字列	任意	
項目8	ログメッセージ	文字列	任意	キーワード

装置Aのログに基づく類似度の算出結果の一例を示す図

類似度算出テーブル				
通信相手	類似文字	類似文字数	出現数	類似度
hostB	SEARCH xxx01 yyy01	18	2	5.418539922
hostB	UPDATE xxx01 yyy01	18	2	5.418539922
hostB	MENU 1 xxx01	12	2	3.612359948
hostB	MENU 2 zzz01	12	2	3.612359948
hostB	LOGOUT xxx01	12	2	3.612359948
hostB	LOGIN xxx01	11	2	3.311329952
hostB	TOP xxx01	9	2	2.709269961

【 図 9 - 2 】

装置Bのログに基づく類似度の算出結果の一例を示す図

類似度算出テーブル		902		
通信相手	類似文字	類似文字数	出現数	類似度
hostA	SEARCH xxx01 yyy01	18	2	5.418539922
hostA	UPDATE xxx01 yyy01	18	2	5.418539922
hostA	LOGOUT xxx01	12	2	3.612359948
hostA	MENU 1 xxx01	12	2	3.612359948
hostA	MENU 2 zzz01	12	2	3.612359948
hostA	LOGIN xxx01	11	2	3.311329952
hostA	MENU	5	4	3.010299957
hostA	TOP xxx01	9	2	2.709269961
hostC	LOGOUT xxx0	11	4	6.622659905
hostC	LOGIN xxx0	10	4	6.020599913
hostC	LOGOUT xxx01	12	2	3.612359948
hostC	LOGOUT xxx02	12	2	3.612359948
hostC	LOGIN xxx01	11	2	3.311329952
hostC	LOGIN xxx02	11	2	3.311329952
hostD	LOGOUT xxx02	12	2	3.612359948
hostD	LOGIN xxx02	11	2	3.311329952
hostD	TOP xxx02	9	2	2.709269961

【 図 1 0 - 1 】

キーワードの抽出結果の一例を示す図(その1)

日付	時刻	ホスト名	ユーザ名	種類	通信方向	通信相手	ログメッセージ
2011/08/05	10:54:00.000	hostA	user01	INFO	SEND	hostB	LOGIN xxx01
2011/08/05	10:54:00.000	hostA	user01	INFO	RECV	hostB	LOGIN xxx01
2011/08/05	10:54:01.000	hostA	user01	INFO	SEND	hostB	TOP xxx01
2011/08/05	10:54:01.200	hostA	user01	INFO	RECV	hostB	TOP xxx01
2011/08/05	10:54:05.000	hostA	user01	INFO	SEND	hostB	MENU 1 xxx01
2011/08/05	10:54:05.000	hostA	user01	INFO	RECV	hostB	MENU 1 xxx01
2011/08/05	10:54:05.200	hostA	user01	INFO	SEND	hostB	SEARCH xxx01 yy01
2011/08/05	10:54:10.000	hostA	user01	INFO	RECV	hostB	SEARCH xxx01 yy01
2011/08/05	10:54:10.200	hostA	user01	INFO	RECV	hostB	SEARCH xxx01 yy01
2011/08/05	10:54:40.000	hostA	user01	INFO	SEND	hostB	UPDATE xxx01 yy01
2011/08/05	10:54:40.200	hostA	user01	ERROR	RECV	hostB	UPDATE xxx01 yy01
2011/08/05	10:54:50.000	hostA	user01	INFO	SEND	hostB	MENU 2 zzz01
2011/08/05	10:54:50.200	hostA	user01	INFO	RECV	hostB	MENU 2 zzz01
2011/08/05	10:55:50.000	hostA	user01	INFO	SEND	hostB	LOGOUT xxx01
2011/08/05	10:55:50.200	hostA	user01	INFO	RECV	hostB	LOGOUT xxx01

1001
 記号キーワード:
 → SEARCH xxx01 yy01

【 図 1 0 - 2 】

キーワードの抽出結果の一例を示す図(その2)

日付	時刻	ホスト名	ユーザ名	種類	通信方向	通信相手	ログメッセージ
2011/08/05	05:54:00.505	hostB	user01	INFO	RECV	hostC	LOGOUT xxa01
2011/08/05	05:54:00.515	hostB	user01	INFO	RECV	hostC	LOGOUT xxa02
2011/08/05	05:54:00.515	hostB	user01	INFO	SEND	hostC	LOGIN xxa01
2011/08/05	05:54:00.520	hostB	user02	INFO	SEND	hostC	LOGIN xxa02
2011/08/05	05:54:00.520	hostB	user01	INFO	SEND	hostC	LOGIN xxa01
2011/08/05	05:54:00.685	hostB	user01	INFO	RECV	hostA	LOGOUT xxa01
2011/08/05	05:54:00.695	hostB	user01	INFO	RECV	hostA	LOGOUT xxa02
2011/08/05	05:54:00.745	hostB	user02	INFO	RECV	hostC	LOGOUT xxa02
2011/08/05	05:54:00.755	hostB	user02	INFO	SEND	hostA	LOGOUT xxa02
2011/08/05	05:54:00.755	hostB	user01	INFO	RECV	hostA	TOP xxa01
2011/08/05	05:54:01.685	hostB	user01	INFO	SEND	hostA	TOP xxa01
2011/08/05	05:54:02.515	hostB	user02	INFO	RECV	hostD	TOP xxa02
2011/08/05	05:54:02.700	hostB	user01	INFO	RECV	hostD	TOP xxa02
2011/08/05	05:54:03.305	hostB	user02	INFO	SEND	hostD	MENU 1 xxa01
2011/08/05	05:54:03.695	hostB	user01	INFO	RECV	hostA	MENU 1 xxa01
2011/08/05	05:54:10.305	hostB	user01	INFO	RECV	hostA	SEARCH xxa01 yyx01
2011/08/05	05:54:10.355	hostB	user01	INFO	RECV	hostA	SEARCH xxa01 yyx01
2011/08/05	05:54:10.355	hostB	user01	INFO	RECV	hostA	SEARCH xxa01 yyx01
2011/08/05	05:54:10.685	hostB	user01	INFO	RECV	hostA	UPDATE xxa01 yyx01
2011/08/05	05:54:00.695	hostB	ERROR	INFO	SEND	hostA	UPDATE xxa01 yyx01
2011/08/05	05:54:05.595	hostB	user01	INFO	RECV	hostA	MENU 2 xxa01
2011/08/05	05:54:06.685	hostB	user01	INFO	SEND	hostA	MENU 2 xxa01
2011/08/05	05:55:00.595	hostB	user01	INFO	RECV	hostA	LOGOUT xxa01
2011/08/05	05:55:00.515	hostB	user01	INFO	SEND	hostC	LOGOUT xxa01
2011/08/05	05:55:00.685	hostB	user01	INFO	RECV	hostC	LOGOUT xxa01
2011/08/05	05:55:00.695	hostB	user01	INFO	SEND	hostA	LOGOUT xxa01
2011/08/05	05:55:30.510	hostB	user02	INFO	RECV	hostC	LOGOUT xxa02
2011/08/05	05:55:30.520	hostB	user02	INFO	SEND	hostC	LOGOUT xxa02
2011/08/05	05:55:30.690	hostB	user02	INFO	RECV	hostC	LOGOUT xxa02
2011/08/05	05:55:30.700	hostB	user02	INFO	SEND	hostD	LOGOUT xxa02

送付キーワード: SEARCH xxa01 yyx01

送付キーワード: SEARCH xxa01 yyx01

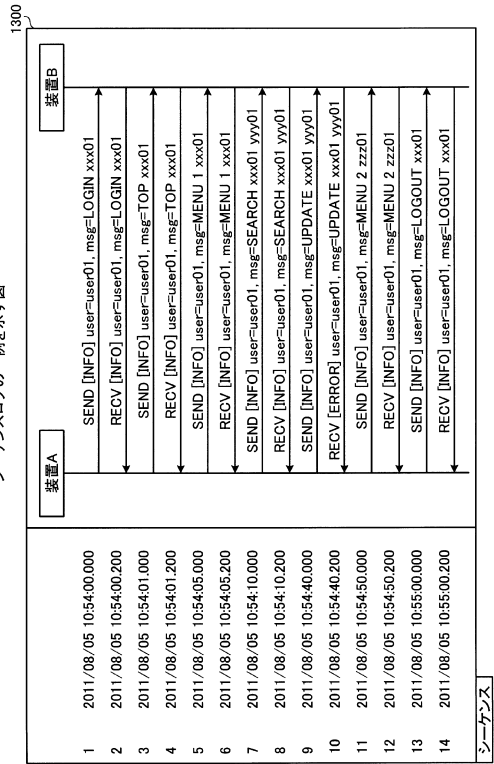
1002

【 図 1 0 - 3 】

キーワードの抽出結果の一例を示す図(その3)

日付	時刻	ホスト名	ユーザ名	種類	通信方向	通信相手	ログメッセージ
2011/08/05	10:40:50.505	hostB	user01	INFO	RECV	hostA	LOGIN xxx01
2011/08/05	10:54:00.515	hostB	user02	INFO	RECV	hostC	LOGIN xxx02
2011/08/05	10:54:00.515	hostB	user01	INFO	SEND	hostC	LOGIN xxx01
2011/08/05	10:54:00.520	hostB	user02	INFO	SEND	hostC	LOGIN xxx02
2011/08/05	10:54:00.685	hostB	user01	INFO	RECV	hostC	LOGIN xxx01
2011/08/05	10:54:00.685	hostB	user02	INFO	SEND	hostA	LOGIN xxx02
2011/08/05	10:54:00.745	hostB	user02	INFO	RECV	hostC	LOGIN xxx02
2011/08/05	10:54:00.755	hostB	user02	INFO	SEND	hostA	TOP xxx01
2011/08/05	10:54:01.505	hostB	user01	INFO	RECV	hostA	TOP xxx01
2011/08/05	10:54:01.665	hostB	user02	INFO	SEND	hostA	TOP xxx02
2011/08/05	10:54:02.510	hostB	user02	INFO	RECV	hostD	TOP xxx02
2011/08/05	10:54:02.700	hostB	user02	INFO	SEND	hostD	TOP xxx02
2011/08/05	10:54:03.505	hostB	user01	INFO	RECV	hostA	MENU 1 xxx01
2011/08/05	10:54:03.685	hostB	user01	INFO	SEND	hostA	MENU 1 xxx01
2011/08/05	10:54:10.035	hostB	user01	INFO	RECV	hostA	SEARCH xxx01
2011/08/05	10:54:10.035	hostB	user01	INFO	SEND	hostA	SEARCH xxx01
2011/08/05	10:54:10.385	hostB	user01	INFO	RECV	hostA	UPDATE xxx01
2011/08/05	10:54:10.385	hostB	user01	INFO	SEND	hostA	UPDATE xxx01
2011/08/05	10:54:50.595	hostB	ERROR	ERROR	SEND	hostA	MENU 2 xxx01
2011/08/05	10:54:50.595	hostB	user01	INFO	RECV	hostA	MENU 2 xxx01
2011/08/05	10:54:50.695	hostB	user01	INFO	SEND	hostA	MENU 2 xxx01
2011/08/05	10:55:00.505	hostB	user01	INFO	RECV	hostC	LOGOUT xxx01
2011/08/05	10:55:00.515	hostB	user01	INFO	SEND	hostC	LOGOUT xxx01
2011/08/05	10:55:00.685	hostB	user01	INFO	RECV	hostC	LOGOUT xxx01
2011/08/05	10:55:30.510	hostB	user01	INFO	SEND	hostA	LOGOUT xxx01
2011/08/05	10:55:30.510	hostB	user02	INFO	RECV	hostC	LOGOUT xxx02
2011/08/05	10:55:30.520	hostB	user02	INFO	SEND	hostC	LOGOUT xxx02
2011/08/05	10:55:30.690	hostB	user02	INFO	RECV	hostC	LOGOUT xxx02
2011/08/05	10:55:30.700	hostB	user02	INFO	SEND	hostD	LOGOUT xxx02

シーケンスログの一例を示す図



フロントページの続き

審査官 多胡 滋

(56)参考文献 特開 2 0 1 1 - 1 5 4 4 8 9 (J P , A)
国際公開第 2 0 1 2 / 1 1 1 1 1 2 (W O , A 1)

(58)調査した分野(Int.Cl. , D B 名)
G 0 6 F 1 1 / 3 0
G 0 6 F 1 / 1 4
G 0 6 F 1 3 / 0 0