(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2005-242988
(P2005-242988A)
(43)公開日　平成17年9月8日(2005.9.8)

| (51)Int.Cl.[7] | F I | | テーマコード（参考） |
|---|---|---|---|
| G06F 11/30 | G06F 11/30 | 305C | 5B042 |
| G06F 11/34 | G06F 11/34 | C | |

審査請求 未請求　請求項の数 15　ＯＬ　（全 23 頁）

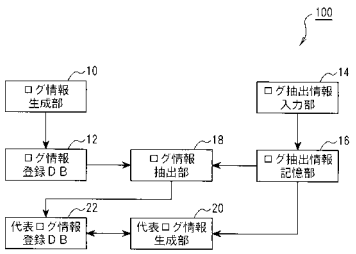
(21)出願番号　特願2004-344175 (P2004-344175)
(22)出願日　平成16年11月29日 (2004.11.29)
(31)優先権主張番号　特願2004-18378 (P2004-18378)
(32)優先日　平成16年1月27日 (2004.1.27)
(33)優先権主張国　日本国(JP)

(71)出願人　000002369
セイコーエプソン株式会社
東京都新宿区西新宿２丁目４番１号
(74)代理人　100066980
弁理士　森　哲也
(74)代理人　100075579
弁理士　内藤　嘉昭
(74)代理人　100103850
弁理士　崔　秀▲てつ▼
(72)発明者　深尾　明人
長野県諏訪市大和３丁目３番５号　セイコーエプソン株式会社内

Ｆターム(参考)　5B042 GA10 GA12 GB01 GC10 GC17 JJ02 JJ03 JJ17 LA17 MA14 MB05 MC15 MC35 MC37 MC40

(54)【発明の名称】ログ情報管理システム、サービス提供システム、ログ情報管理プログラムおよびサービス提供プログラム、並びにログ情報管理方法およびサービス提供方法

(57)【要約】　（修正有）
【課題】複雑な状態を検出するのに好適なログ情報管理システムを提供する。
【解決手段】複数の条件を組み合わせて設定可能なログ抽出条件を含むログ抽出情報を入力１４し、入力したログ抽出情報１６に基づいて、ログ抽出条件を満たすログ情報をログ情報登録ＤＢ１２のなかから抽出し、抽出したログ情報を代表する代表ログ情報２２を生成する。
【選択図】図１



【特許請求の範囲】
【請求項１】
システムのイベントをログ情報として管理するログ情報管理システムであって、
前記ログ情報を記憶するログ情報記憶手段と、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定手段と、前記ログ抽出条件設定手段で設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出手段と、前記ログ情報抽出手段で抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成手段とを備えることを特徴とするログ情報管理システム。
【請求項２】
請求項１において、
前記代表ログ情報生成手段は、前記ログ情報抽出手段で抽出したログ情報を参照可能なログ参照情報を含む代表ログ情報を生成するようになっていることを特徴とするログ情報管理システム。
【請求項３】
請求項１および２のいずれか１項において、
前記代表ログ情報を記憶する代表ログ情報記憶手段を備え、
前記代表ログ情報生成手段は、生成した代表ログ情報を前記代表ログ情報記憶手段に記憶するようになっていることを特徴とするログ情報管理システム。
【請求項４】
請求項１ないし３のいずれか１項において、
前記ログ抽出条件設定手段は、各ユーザごとに前記ログ抽出条件を設定するようになっていることを特徴とするログ情報管理システム。
【請求項５】
請求項１ないし４のいずれか１項において、
前記ログ抽出条件は、異常と想定される状態を規定した条件であることを特徴とするログ情報管理システム。
【請求項６】
請求項５において、
前記ログ抽出条件は、前記ログ情報の発生条件を規定したログ発生条件、前記ログ情報の発生日時の範囲を規定したログ発生期間、および前記ログ発生期間において前記ログ情報の発生回数を規定したログ発生回数を含むことを特徴とするログ情報管理システム。
【請求項７】
ネットワークデバイスのログ情報を管理するログ情報管理システムであって、
ログ情報記憶手段と、前記ネットワークデバイスからのログ情報を受信するログ情報受信手段と、前記ログ情報受信手段で受信したログ情報を前記ログ情報記憶手段に保存するログ情報保存手段と、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定手段と、前記ログ抽出条件設定手段で設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出手段と、前記ログ情報抽出手段で抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成手段とを備えることを特徴とするログ情報管理システム。
【請求項８】
ネットワークを介してサービスを提供するサービス提供システムであって、
ログ情報記憶手段と、前記ネットワークからのアクセスに応じてサービスを提供するサービス処理手段と、前記サービス処理手段で発生したイベントに基づいてログ情報を生成するログ情報生成手段と、前記ログ情報生成手段で生成したログ情報を前記ログ情報記憶手段に保存するログ情報保存手段と、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定手段と、前記ログ抽出条件設定手段で設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出手段と、前記ログ情報抽出手段で抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成手段とを備えることを特徴とするサービス提供システム。

【請求項９】
システムのイベントをログ情報として管理するログ情報管理プログラムであって、
前記ログ情報を記憶するログ情報記憶手段を利用可能なコンピュータに対して、
複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとからなる処理を実行させるためのプログラムであることを特徴とするログ情報管理プログラム。
【請求項１０】
ネットワークデバイスのログ情報を管理するログ情報管理プログラムであって、
前記ネットワークデバイスからのログ情報を受信するログ情報受信ステップと、前記ログ情報受信ステップで受信したログ情報をログ情報記憶手段に保存するログ情報保存ステップと、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとからなる処理をコンピュータに実行させるためのプログラムを含むことを特徴とするログ情報管理プログラム。
【請求項１１】
ネットワークを介してサービスを提供するサービス提供プログラムであって、
前記ネットワークからのアクセスに応じてサービスを提供するサービス処理ステップと、前記サービス処理ステップで発生したイベントに基づいてログ情報を生成するログ情報生成ステップと、前記ログ情報生成ステップで生成したログ情報をログ情報記憶手段に保存するログ情報保存ステップと、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとからなる処理をコンピュータに実行させるためのプログラムを含むことを特徴とするサービス提供プログラム。
【請求項１２】
システムのイベントをログ情報として管理するログ情報管理方法であって、
複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、
前記ログ情報を記憶したログ情報記憶手段から、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を抽出するログ情報抽出ステップと、
前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとを含むことを特徴とするログ情報管理方法。
【請求項１３】
システムのイベントをログ情報として管理するログ情報管理方法であって、
入力手段が、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、
演算手段が、前記ログ情報を記憶したログ情報記憶手段から、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を抽出するログ情報抽出ステップと、
前記演算手段が、前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとを含むことを特徴とするログ情報管理方法。
【請求項１４】
ネットワークデバイスのログ情報を管理するログ情報管理方法であって、
前記ネットワークデバイスからのログ情報を受信するログ情報受信ステップと、
前記ログ情報受信ステップで受信したログ情報をログ情報記憶手段に保存するログ情報保存ステップと、

複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、
前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、
前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとを含むことを特徴とするログ情報管理方法。
【請求項１５】
ネットワークを介してサービスを提供するサービス提供方法であって、
前記ネットワークからのアクセスに応じてサービスを提供するサービス処理ステップと、
前記サービス処理ステップで発生したイベントに基づいてログ情報を生成するログ情報生成ステップと、
前記ログ情報生成ステップで生成したログ情報をログ情報記憶手段に保存するログ情報保存ステップと、
複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、
前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、
前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとを含むことを特徴とするサービス提供方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、システムのイベントをログ情報として管理するシステムおよびプログラム、並びに方法に係り、特に、複雑な状態を検出するのに好適なログ情報管理システム、サービス提供システム、ログ情報管理プログラムおよびサービス提供プログラム、並びにログ情報管理方法およびサービス提供方法に関する。
【背景技術】
【０００２】
コンピュータシステムでは、システムの動作に起因して発生するイベントを各イベントごとにログ情報としてデータベースに記憶している。ログ情報は、発生日時、操作内容および情報レベル（情報、注意、警告等）といった形式でデータベースに保存されており、システムのデバッグ時などには、情報レベル等により必要なログ情報を識別しやすいように作られている。
【０００３】
従来、ログ情報を管理する技術としては、例えば、特許文献１に開示されている通信ログの処理方法があった。
特許文献１記載の発明は、保存されるログリストの各行に対して所定の不正アクセスパターンを適用することで不正アクセスの有無を検出し、検出したログ情報を他の記憶媒体に保存する。
【特許文献１】特開２００３－９９２９５号公報
【発明の開示】
【発明が解決しようとする課題】
【０００４】
システムの異常には、１つのログ情報から把握することができる単純な異常もあれば、複数のログ情報を組み合わせて初めて把握することができる複雑な異常もある。後者の場合、例えば、パスワードの入力ミスを立て続けに数回行うような不正アクセス（異常）は、同一ユーザＩＤについてログインエラーとなるログ情報が所定時間内に所定回出現している箇所をデータベースのなかから見つけ出して初めて把握することができる。
【０００５】

しかしながら、特許文献１記載の発明にあっては、１つのログ情報に基づいて不正アクセスの有無を検出するだけの構成であるため、複数のログ情報を組み合わせて把握することができる複雑な異常を検出することは困難であった。

また、例えば、ユーザに対してサービスを提供しているにもかかわらず、ユーザがそのサービスを一度も利用してない場合は、そのサービスの提供を停止するか、より適切な他のサービスを提供することが望ましい。しかしながら、特許文献１記載の発明にあっては、不正アクセスの有無を検出するだけの構成であるため、そのような状態を調査するには、ログ情報を１つ１つ手作業で解析しなければならない。

【０００６】

そこで、本発明は、このような従来の技術の有する未解決の課題に着目してなされたものであって、複雑な状態を検出するのに好適なログ情報管理システム、サービス提供システム、ログ情報管理プログラムおよびサービス提供プログラム、並びにログ情報管理方法およびサービス提供方法を提供することを目的としている。

【課題を解決するための手段】

【０００７】

〔発明１〕　上記目的を達成するために、発明１のログ情報管理システムは、

システムのイベントをログ情報として管理するログ情報管理システムであって、

前記ログ情報を記憶するログ情報記憶手段と、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定手段と、前記ログ抽出条件設定手段で設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出手段と、前記ログ情報抽出手段で抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成手段とを備えることを特徴とする。

【０００８】

このような構成であれば、システム管理者は、ログ抽出条件設定手段により、複数の条件を組み合わせてログ抽出条件を設定する。そして、ログ抽出条件に適合するログ情報がログ情報記憶手段に記憶されると、ログ情報抽出手段により、ログ抽出条件に適合するログ情報がログ情報記憶手段から抽出され、代表ログ情報生成手段により、抽出されたログ情報を代表する代表ログ情報が生成される。

【０００９】

これにより、システム管理者は、代表ログ情報を参照すれば、複数のログ情報を組み合わせて把握することができる複雑な状態を把握することができるので、従来に比して、複雑な状態を比較的容易に検出することができるという効果が得られる。

ここで、ログ情報抽出手段は、ログ抽出条件に適合するログ情報を抽出するようになっていればどのような構成であってもよく、例えば、ログ抽出条件を満たすログ情報（完全一致）を抽出するようになっていてもよいし、ログ抽出条件の一部を満たすログ情報（部分一致）を抽出するようになっていてもよい。以下、発明７のログ情報管理システム、および発明８のサービス提供システムにおいて同じである。

【００１０】

また、システムのイベントとは、システムを使用しているユーザや、システムを構成するプログラムが起こした操作や処理をいう。以下、発明７のログ情報管理システム、発明８のサービス提供システム、発明９および１５のログ情報管理プログラム、発明１６のサービス提供プログラム、発明１７、１８および２４のログ情報管理方法、並びに発明２５のサービス提供方法において同じである。

【００１１】

また、ログ情報とは、システム上で起こった操作や処理を記録したものをいう。ログ情報には、例えば、操作や処理が行われた日時、および行われた操作や処理の内容が含まれる。以下、発明７のログ情報管理システム、発明８のサービス提供システム、発明９および１５のログ情報管理プログラム、発明１６のサービス提供プログラム、発明１７、１８および２４のログ情報管理方法、並びに発明２５のサービス提供方法において同じである。

【００１２】
　また、ログ情報記憶手段は、ログ情報をあらゆる手段でかつあらゆる時期に記憶するものであり、ログ情報をあらかじめ記憶してあるものであってもよいし、ログ情報をあらかじめ記憶することなく、本システムの動作時に外部からの入力等によってログ情報を記憶するようになっていてもよい。以下、発明７のログ情報管理システム、および発明８のサービス提供システムにおいて同じである。
【００１３】
　また、本システムは、単一の装置、端末その他の機器として実現するようにしてもよいし、複数の装置、端末その他の機器を通信可能に接続したネットワークシステムとして実現するようにしてもよい。後者の場合、各構成要素は、それぞれ通信可能に接続されていれば、複数の機器等のうちいずれに属していてもよい。以下、発明７のログ情報管理システム、および発明８のサービス提供システムにおいて同じである。
【００１４】
　〔発明２〕　さらに、発明２のログ情報管理システムは、発明１のログ情報管理システムにおいて、
　前記代表ログ情報生成手段は、前記ログ情報抽出手段で抽出したログ情報を参照可能なログ参照情報を含む代表ログ情報を生成するようになっていることを特徴とする。
　このような構成であれば、代表ログ情報生成手段により、抽出されたログ情報を参照可能なログ参照情報を含む代表ログ情報が生成される。
【００１５】
　これにより、システム管理者は、代表ログ情報を参照すれば、その代表ログ情報の生成の原因となったログ情報を参照することができるので、状態発生の原因を分析しやすくなるという効果が得られる。
　ここで、参照情報は、ログ情報を参照可能な情報であればどのようなものであってもよく、例えば、ログ情報を識別する識別情報であってもよいし、ログ情報の参照先を示すリンク情報であってもよいし、ログ情報と同一の内容からなる複製ログ情報であってもよい。以下、発明１０のログ情報管理プログラム、および発明１９のログ情報管理方法において同じである。
【００１６】
　〔発明３〕　さらに、発明３のログ情報管理システムは、発明１および２のいずれか１のログ情報管理システムにおいて、
　前記代表ログ情報を記憶する代表ログ情報記憶手段を備え、
　前記代表ログ情報生成手段は、生成した代表ログ情報を前記代表ログ情報記憶手段に記憶するようになっていることを特徴とする。
【００１７】
　このような構成であれば、代表ログ情報生成手段により、生成された代表ログ情報が代表ログ情報記憶手段に記憶される。
　これにより、代表ログ情報は、代表ログ情報記憶手段に他のログ情報とは別に記憶されるので、システム管理者は、代表ログ情報を参照しやすくなる。したがって、複雑な状態をさらに容易に検出することができるという効果が得られる。
【００１８】
　ここで、代表ログ情報記憶手段は、代表ログ情報をあらゆる手段でかつあらゆる時期に記憶するものであり、代表ログ情報をあらかじめ記憶してあるものであってもよいし、代表ログ情報をあらかじめ記憶することなく、本システムの動作時に外部からの入力等によって代表ログ情報を記憶するようになっていてもよい。
【００１９】
　〔発明４〕　さらに、発明４のログ情報管理システムは、発明１ないし３のいずれか１のログ情報管理システムにおいて、
　前記ログ抽出条件設定手段は、各ユーザごとに前記ログ抽出条件を設定するようになっていることを特徴とする。

【００２０】
このような構成であれば、同一のシステムに対して複数のシステム管理者が存在する場合は、ログ抽出条件設定手段により、各システム管理者ごとにログ抽出条件を設定することができる。
これにより、各システム管理者ごとに、そのシステム管理者が注目する複雑な状態を検出することができるので、システムの利便性を向上することができるという効果が得られる。
【００２１】
〔発明５〕　さらに、発明５のログ情報管理システムは、発明１ないし４のいずれか１のログ情報管理システムにおいて、
前記ログ抽出条件は、異常と想定される状態を規定した条件であることを特徴とする。
このような構成であれば、ログ情報抽出手段により、異常と想定される状態を規定したログ抽出条件に適合するログ情報がログ情報記憶手段から抽出される。
【００２２】
これにより、システム管理者は、代表ログ情報を参照すれば、複数のログ情報を組み合わせて把握することができる複雑な異常を把握することができるので、複雑な異常を比較的容易に検出することができるという効果が得られる。
【００２３】
〔発明６〕　さらに、発明６のログ情報管理システムは、発明５のログ情報管理システムにおいて、
前記ログ抽出条件は、前記ログ情報の発生条件を規定したログ発生条件、前記ログ情報の発生日時の範囲を規定したログ発生期間、および前記ログ発生期間において前記ログ情報の発生回数を規定したログ発生回数を含むことを特徴とする。
このような構成であれば、ログ発生期間において、ログ発生条件に適合しかつログ発生回数だけ発生したログ情報がログ情報記憶手段から抽出される。
これにより、複雑な異常をさらに容易に検出することができるという効果が得られる。
【００２４】
〔発明７〕　さらに、発明７のログ情報管理システムは、
ネットワークデバイスのログ情報を管理するログ情報管理システムであって、
ログ情報記憶手段と、前記ネットワークデバイスからのログ情報を受信するログ情報受信手段と、前記ログ情報受信手段で受信したログ情報を前記ログ情報記憶手段に保存するログ情報保存手段と、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定手段と、前記ログ抽出条件設定手段で設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出手段と、前記ログ情報抽出手段で抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成手段とを備えることを特徴とする。
【００２５】
このような構成であれば、システム管理者は、ログ抽出条件設定手段により、複数の条件を組み合わせてログ抽出条件を設定する。次いで、ログ情報受信手段によりネットワークデバイスからログ情報を受信すると、ログ情報保存手段により、受信したログ情報がログ情報記憶手段に保存される。そして、ログ情報抽出手段により、ログ抽出条件に適合するログ情報がログ情報記憶手段から抽出され、代表ログ情報生成手段により、抽出されたログ情報を代表する代表ログ情報が生成される。
【００２６】
これにより、システム管理者は、代表ログ情報を参照すれば、複数のログ情報を組み合わせて把握することができる複雑な異常を把握することができるので、従来に比して、ネットワークデバイスで発生した複雑な異常を比較的容易に検出することができるという効果が得られる。
【００２７】
〔発明８〕　一方、上記目的を達成するために、発明８のサービス提供システムは、

ネットワークを介してサービスを提供するサービス提供システムであって、
ログ情報記憶手段と、前記ネットワークからのアクセスに応じてサービスを提供するサービス処理手段と、前記サービス処理手段で発生したイベントに基づいてログ情報を生成するログ情報生成手段と、前記ログ情報生成手段で生成したログ情報を前記ログ情報記憶手段に保存するログ情報保存手段と、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定手段と、前記ログ抽出条件設定手段で設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出手段と、前記ログ情報抽出手段で抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成手段とを備えることを特徴とする。

【００２８】

このような構成であれば、システム管理者は、ログ抽出条件設定手段により、複数の条件を組み合わせてログ抽出条件を設定する。次いで、ネットワークからアクセスを受けると、サービス処理手段により、アクセスに応じてサービスが提供される。その結果、サービス処理手段でイベントが発生すると、ログ情報生成手段により、発生したイベントに基づいてログ情報が生成され、ログ情報保存手段により、生成されたログ情報がログ情報記憶手段に保存される。そして、ログ情報抽出手段により、ログ抽出条件に適合するログ情報がログ情報記憶手段から抽出され、代表ログ情報生成手段により、抽出されたログ情報を代表する代表ログ情報が生成される。

【００２９】

これにより、システム管理者は、代表ログ情報を参照すれば、複数のログ情報を組み合わせて把握することができる複雑な状態を把握することができるので、従来に比して、ネットワークからのアクセスにより発生した複雑な状態を比較的容易に検出することができるという効果が得られる。

【００３０】

〔発明９〕　一方、上記目的を達成するために、発明９のログ情報管理プログラムは、
システムのイベントをログ情報として管理するログ情報管理プログラムであって、
前記ログ情報を記憶するログ情報記憶手段を利用可能なコンピュータに対して、
複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとからなる処理を実行させるためのプログラムであることを特徴とする。

【００３１】

このような構成であれば、コンピュータによってプログラムが読み取られ、読み取られたプログラムに従ってコンピュータが処理を実行すると、発明１のログ情報管理システムと同等の作用および効果が得られる。
ここで、ログ情報抽出ステップは、ログ抽出条件に適合するログ情報を抽出すればどのような形態であってもよく、例えば、ログ抽出条件を満たすログ情報（完全一致）を抽出してもよいし、ログ抽出条件の一部を満たすログ情報（部分一致）を抽出してもよい。以下、発明１５のログ情報管理プログラム、発明１６のサービス提供プログラム、発明１７、１８および２４のログ情報管理方法、並びに発明２５のサービス提供方法において同じである。

【００３２】

〔発明１０〕　さらに、発明１０のログ情報管理プログラムは、発明９のログ情報管理プログラムにおいて、
前記代表ログ情報生成ステップは、前記ログ情報抽出ステップで抽出したログ情報を参照可能なログ参照情報を含む代表ログ情報を生成することを特徴とする。
このような構成であれば、コンピュータによってプログラムが読み取られ、読み取られたプログラムに従ってコンピュータが処理を実行すると、発明２のログ情報管理システムと同等の作用および効果が得られる。

【００３３】
〔発明１１〕　さらに、発明１１のログ情報管理プログラムは、発明９および１０のいずれか１のログ情報管理プログラムにおいて、
前記コンピュータは、前記代表ログ情報を記憶する代表ログ情報記憶手段を利用可能となっており、
前記代表ログ情報生成ステップは、生成した代表ログ情報を前記代表ログ情報記憶手段に記憶することを特徴とする。
このような構成であれば、コンピュータによってプログラムが読み取られ、読み取られたプログラムに従ってコンピュータが処理を実行すると、発明３のログ情報管理システムと同等の作用および効果が得られる。
【００３４】
〔発明１２〕　さらに、発明１２のログ情報管理プログラムは、発明９ないし１１のいずれか１のログ情報管理プログラムにおいて、
前記ログ抽出条件設定ステップは、各ユーザごとに前記ログ抽出条件を設定することを特徴とする。
このような構成であれば、コンピュータによってプログラムが読み取られ、読み取られたプログラムに従ってコンピュータが処理を実行すると、発明４のログ情報管理システムと同等の作用および効果が得られる。
【００３５】
〔発明１３〕　さらに、発明１３のログ情報管理プログラムは、発明９ないし１２のいずれか１のログ情報管理プログラムにおいて、
前記ログ抽出条件は、異常と想定される状態を規定した条件であることを特徴とする。
このような構成であれば、コンピュータによってプログラムが読み取られ、読み取られたプログラムに従ってコンピュータが処理を実行すると、発明５のログ情報管理システムと同等の作用および効果が得られる。
【００３６】
〔発明１４〕　さらに、発明１４のログ情報管理プログラムは、発明１３のログ情報管理プログラムにおいて、
前記ログ抽出条件は、前記ログ情報の発生条件を規定したログ発生条件、前記ログ情報の発生日時の範囲を規定したログ発生期間、および前記ログ発生期間において前記ログ情報の発生回数を規定したログ発生回数を含むことを特徴とする。
このような構成であれば、コンピュータによってプログラムが読み取られ、読み取られたプログラムに従ってコンピュータが処理を実行すると、発明６のログ情報管理システムと同等の作用および効果が得られる。
【００３７】
〔発明１５〕　さらに、発明１５のログ情報管理プログラムは、
ネットワークデバイスのログ情報を管理するログ情報管理プログラムであって、
前記ネットワークデバイスからのログ情報を受信するログ情報受信ステップと、前記ログ情報受信ステップで受信したログ情報をログ情報記憶手段に保存するログ情報保存ステップと、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとからなる処理をコンピュータに実行させるためのプログラムを含むことを特徴とする。
このような構成であれば、コンピュータによってプログラムが読み取られ、読み取られたプログラムに従ってコンピュータが処理を実行すると、発明７のログ情報管理システムと同等の作用および効果が得られる。
【００３８】
〔発明１６〕　一方、上記目的を達成するために、発明１６のサービス提供プログラムは、

ネットワークを介してサービスを提供するサービス提供プログラムであって、
前記ネットワークからのアクセスに応じてサービスを提供するサービス処理ステップと、前記サービス処理ステップで発生したイベントに基づいてログ情報を生成するログ情報生成ステップと、前記ログ情報生成ステップで生成したログ情報をログ情報記憶手段に保存するログ情報保存ステップと、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとからなる処理をコンピュータに実行させるためのプログラムを含むことを特徴とする。
このような構成であれば、コンピュータによってプログラムが読み取られ、読み取られたプログラムに従ってコンピュータが処理を実行すると、発明８のサービス提供システムと同等の作用および効果が得られる。

【００３９】

〔発明１７〕　一方、上記目的を達成するために、発明１７のログ情報管理方法は、
システムのイベントをログ情報として管理するログ情報管理方法であって、
複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、
前記ログ情報を記憶したログ情報記憶手段から、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を抽出するログ情報抽出ステップと、
前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとを含むことを特徴とする。
これにより、発明１のログ情報管理システムと同等の効果が得られる。

【００４０】

〔発明１８〕　さらに、発明１８のログ情報管理方法は、
システムのイベントをログ情報として管理するログ情報管理方法であって、
入力手段が、複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、
演算手段が、前記ログ情報を記憶したログ情報記憶手段から、前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を抽出するログ情報抽出ステップと、
前記演算手段が、前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとを含むことを特徴とする。
これにより、発明１のログ情報管理システムと同等の効果が得られる。

【００４１】

〔発明１９〕　さらに、発明１９のログ情報管理方法は、発明１７および１８のいずれか１のログ情報管理方法において、
前記代表ログ情報生成ステップは、前記ログ情報抽出ステップで抽出したログ情報を参照可能なログ参照情報を含む代表ログ情報を生成することを特徴とする。
これにより、発明２のログ情報管理システムと同等の効果が得られる。

【００４２】

〔発明２０〕　さらに、発明２０のログ情報管理方法は、発明１７ないし１９のいずれか１のログ情報管理方法において、
前記代表ログ情報生成ステップは、生成した代表ログ情報を、前記ログ情報記憶手段とは異なる代表ログ情報記憶手段に記憶することを特徴とする。
これにより、発明３のログ情報管理システムと同等の効果が得られる。

【００４３】

〔発明２１〕　さらに、発明２１のログ情報管理方法は、発明１７ないし２０のいずれか１のログ情報管理方法において、
前記ログ抽出条件設定ステップは、各ユーザごとに前記ログ抽出条件を設定することを特徴とする。

これにより、発明４のログ情報管理システムと同等の効果が得られる。

【００４４】

〔発明２２〕　さらに、発明２２のログ情報管理方法は、発明１７ないし２１のいずれか１のログ情報管理方法において、

前記ログ抽出条件は、異常と想定される状態を規定した条件であることを特徴とする。

これにより、発明５のログ情報管理システムと同等の効果が得られる。

【００４５】

〔発明２３〕　さらに、発明２３のログ情報管理方法は、発明２２のログ情報管理方法において、

前記ログ抽出条件は、前記ログ情報の発生条件を規定したログ発生条件、前記ログ情報の発生日時の範囲を規定したログ発生期間、および前記ログ発生期間において前記ログ情報の発生回数を規定したログ発生回数を含むことを特徴とする。

これにより、発明６のログ情報管理システムと同等の効果が得られる。

【００４６】

〔発明２４〕　さらに、発明２４のログ情報管理方法は、

ネットワークデバイスのログ情報を管理するログ情報管理方法であって、

前記ネットワークデバイスからのログ情報を受信するログ情報受信ステップと、

前記ログ情報受信ステップで受信したログ情報をログ情報記憶手段に保存するログ情報保存ステップと、

複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、

前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、

前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとを含むことを特徴とする。

これにより、発明７のログ情報管理システムと同等の効果が得られる。

【００４７】

〔発明２５〕　一方、上記目的を達成するために、発明２５のサービス提供方法は、

ネットワークを介してサービスを提供するサービス提供方法であって、

前記ネットワークからのアクセスに応じてサービスを提供するサービス処理ステップと、

前記サービス処理ステップで発生したイベントに基づいてログ情報を生成するログ情報生成ステップと、

前記ログ情報生成ステップで生成したログ情報をログ情報記憶手段に保存するログ情報保存ステップと、

複数の条件を組み合わせて設定可能なログ抽出条件を設定するログ抽出条件設定ステップと、

前記ログ抽出条件設定ステップで設定したログ抽出条件に適合するログ情報を前記ログ情報記憶手段から抽出するログ情報抽出ステップと、

前記ログ情報抽出ステップで抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成ステップとを含むことを特徴とする。

これにより、発明８のサービス提供システムと同等の効果が得られる。

【発明を実施するための最良の形態】

【００４８】

以下、本発明の実施の形態を図面を参照しながら説明する。図１ないし図１３は、本発明に係るログ情報管理システム、サービス提供システム、ログ情報管理プログラムおよびサービス提供プログラム、並びにログ情報管理方法およびサービス提供方法の実施の形態を示す図である。

本実施の形態は、本発明に係るログ情報管理システム、サービス提供システム、ログ情報管理プログラムおよびサービス提供プログラム、並びにログ情報管理方法およびサービ

ス提供方法を、図１に示すように、システムの異常を検出する場合について適用したものである。

【００４９】

まず、本発明を適用するログ情報管理装置１００の機能概要を図１を参照しながら説明する。

図１は、ログ情報管理装置１００の機能概要を示す機能ブロック図である。

ログ情報管理装置１００は、図１に示すように、ログ情報を生成するログ情報生成部１０と、ログ情報生成部１０で生成したログ情報を登録するログ情報登録データベース（以下、データベースのことを単にＤＢと略記する。）１２と、複数の条件を組み合わせて設定可能なログ抽出条件を含むログ抽出情報を入力するログ抽出情報入力部１４と、ログ抽出情報入力部１４で入力したログ抽出情報を記憶するログ抽出情報記憶部１６とを有して構成されている。

【００５０】

ログ情報生成部１０は、システムの動作に起因してイベントが発生したときは、発生したイベントのログ情報を生成し、生成したログ情報をログ情報登録ＤＢ１２に登録する。

ログ情報管理装置１００は、さらに、ログ抽出情報記憶部１６のログ抽出情報に基づいてログ情報登録ＤＢ１２のなかからログ情報を抽出するログ情報抽出部１８と、ログ情報抽出部１８で抽出したログ情報を代表する代表ログ情報を生成する代表ログ情報生成部２０と、代表ログ情報生成部２０で生成した代表ログ情報を登録する代表ログ情報登録ＤＢ２２とを有して構成されている。

【００５１】

ログ情報抽出部１８は、ログ抽出情報記憶部１６のログ抽出情報に基づいて、ログ抽出条件を満たすログ情報をログ情報登録ＤＢ１２のなかから抽出し、抽出したログ情報を代表ログ情報登録ＤＢ２２に登録する。

代表ログ情報生成部２０は、ログ抽出情報記憶部１６のログ抽出情報に基づいて、ログ抽出条件を満たすログ情報を代表ログ情報登録ＤＢ２２のなかから抽出し、抽出したログ情報を代表する代表ログ情報を生成し、生成した代表ログ情報を代表ログ情報登録ＤＢ２２に登録する。

【００５２】

次に、ログ情報管理装置１００の構成を図２ないし図７を参照しながら詳細に説明する。

図２は、ログ情報管理装置１００のハードウェア構成を示すブロック図である。

ログ情報管理装置１００は、図２に示すように、制御プログラムに基づいて演算およびシステム全体を制御するＣＰＵ３０と、所定領域にあらかじめＣＰＵ３０の制御プログラム等を格納しているＲＯＭ３２と、ＲＯＭ３２等から読み出したデータやＣＰＵ３０の演算過程で必要な演算結果を格納するためのＲＡＭ３４と、外部装置に対してデータの入出力を媒介するＩ／Ｆ３８とで構成されており、これらは、データを転送するための信号線であるバス３９で相互にかつデータ授受可能に接続されている。

【００５３】

Ｉ／Ｆ３８には、外部装置として、ヒューマンインターフェースとしてデータの入力が可能なキーボードやマウス等からなる入力装置４０と、ログ情報登録ＤＢ１２と、代表ログ情報登録ＤＢ２２と、データやテーブル等をファイルとして格納する記憶装置４２と、画像信号に基づいて画面を表示する表示装置４４とが接続されている。

図３は、ログ情報登録ＤＢ１２のデータ構造を示す図である。

【００５４】

ログ情報登録ＤＢ１２には、各イベントごとに１つのレコードが登録される。各レコードは、図３に示すように、ログ情報を一意に識別するログＩＤを登録するフィールド４００と、ログ情報の発生元（例えば、ユーザまたはデバイス）を一意に識別するログ発生元ＩＤを登録するフィールド４０２と、ログ情報が生成された日時（ログ発生日時）を登録するフィールド４０４と、ログ情報の種別（ログ種別）を登録するフィールド４０６と、

ログ情報の通知レベル（ログレベル）を登録するフィールド４０８と、ログ情報に関する説明（ログ説明）を登録するフィールド４１０とを含んで構成されている。

【００５５】

フィールド４０６には、ログ種別として、例えば、イベントが印刷であれば「print」が、イベントがログインであれば「Login」が登録される。

フィールド４０８には、ログレベルとして、例えば、通知の重要度が低いイベントの順に「INFORMATION」、「CAUTION」、「WARNING」および「ERROR」が登録される。

図４は、代表ログ情報登録ＤＢ２２のデータ構造を示す図である。

【００５６】

代表ログ情報登録ＤＢ２２には、ログ抽出条件を満たすログ情報を抽出するたびに１つのレコードが登録される。各レコードは、図４に示すように、代表ログ情報を一意に識別するログＩＤを登録するフィールド４２０と、代表ログ情報の発生元を一意に識別するログ発生元ＩＤを登録するフィールド４２２と、代表ログ情報が生成された日時（ログ発生日時）を登録するフィールド４２４と、代表ログ情報の種別（ログ種別）を登録するフィールド４２６と、代表ログ情報の通知レベル（ログレベル）を登録するフィールド４２８と、代表ログ情報に関する説明（ログ説明）を登録するフィールド４３０と、代表ログ情報の生成の原因となったログ情報のログＩＤ（ログリスト）を登録するフィールド４３２とを含んで構成されている。

【００５７】

記憶装置４２は、ログ抽出情報記憶部１６として構成され、システム管理者により入力されたログ抽出情報を記憶する。ログ抽出情報は、例えば、入力装置４０を利用して入力する。

図５は、ログ抽出情報のデータ構造を示す図である。

ログ抽出情報は、図５に示すように、ログ抽出情報の基本情報を格納するヘッダ部４４０を１つ、ログ抽出条件を格納するボディ部４６０を１または複数含んで構成されている。

【００５８】

ヘッダ部４４０は、ログ抽出情報を一意に識別するログ抽出情報ＩＤを格納するデータ領域４４２と、ログ抽出情報に関する説明を格納するデータ領域４４４と、複数のログ抽出条件を組み合わせて設定する場合に各ログ抽出条件の論理演算式を格納するデータ領域４４６とを含んで構成されている。

ボディ部４６０は、ログ抽出条件を一意に識別するログ抽出条件ＩＤを格納するデータ領域４６２と、抽出対象とするログ情報の発生条件をログ発生条件として格納するデータ領域４６４と、抽出対象とするログ情報の発生日時の範囲をログ発生期間として格納するデータ領域４６６と、ログ発生期間において抽出対象となるログ情報の発生回数をログ発生回数として格納するデータ領域４６８とを含んで構成されている。

【００５９】

ログ抽出式は、ログ抽出条件ＩＤを所定の演算子で結合することにより記述する。例えば、ログ抽出条件を２つ設定し、そのＩＤがそれぞれＡ，Ｂである場合、両方のログ抽出条件を満たすログ情報を抽出すべきことを設定するには、演算子「AND」を利用して「Ａ AND Ｂ」と記述する。また、いずれか一方のログ抽出条件を満たすログ情報を抽出すべきことを設定するには、演算子「OR」を利用して「Ａ OR Ｂ」と記述する。

【００６０】

ログ抽出条件は、ログ情報の項目とその値を所定の演算子で結合することにより記述する。例えば、ログ種別が「Login」となるログ情報を抽出すべきことを設定するには、「ログ種別=Login」と記述する。また、複数の条件を組み合わせて設定することもでき、その場合は、ログ抽出式の演算子で各条件を結合することにより記述する。例えば、ログ種別が「Login」でかつログレベルが「ERROR」となるログ情報を抽出すべきことを設定するには、演算子「AND」を利用して「ログ種別=Login AND ログレベル=ERROR」と記述する。

【００６１】

図２に戻り、ＣＰＵ３０は、マイクロプロセッシングユニット（ＭＰＵ）等からなり、ＲＯＭ３２の所定領域に格納されている所定のプログラムを起動させ、そのプログラムに従って、図６および図７のフローチャートに示すログ情報抽出処理および代表ログ情報生成処理をそれぞれ時分割で実行するようになっている。

初めに、ログ情報抽出処理を図６を参照しながら詳細に説明する。

【００６２】

図６は、ログ情報抽出処理を示すフローチャートである。

ログ情報抽出処理は、ログ情報生成部１０およびログ情報抽出部１８として実現される処理であって、ＣＰＵ３０において実行されると、図６に示すように、まず、ステップＳ１００に移行するようになっている。

ステップＳ１００では、ログ情報の生成対象となるイベントが発生したか否かを判定し、イベントが発生したと判定したとき(Yes)は、ステップＳ１０２に移行するが、そうでないと判定したとき(No)は、イベントが発生するまでステップＳ１００で待機する。

【００６３】

ステップＳ１０２では、発生したイベントのログ情報を生成し、ステップＳ１０４に移行して、生成したログ情報をログ情報登録ＤＢ１２に登録し、ステップＳ１０６に移行する。

ステップＳ１０６では、先頭のログ抽出情報を記憶装置４２から読み出し、ステップＳ１０８に移行して、読み出したログ抽出情報に基づいて、ログ抽出条件を満たすログ情報をログ情報登録ＤＢ１２のなかから検索し、ステップＳ１１０に移行する。

【００６４】

ステップＳ１１０では、該当のログ情報を索出したか否かを判定し、該当のログ情報を索出したと判定したとき(Yes)は、ステップＳ１１２に移行して、索出したログ情報を代表ログ情報登録ＤＢ２２に登録し、ステップＳ１１４に移行する。

ステップＳ１１４では、記憶装置４２のすべてのログ抽出情報についてステップＳ１０８～Ｓ１１２の処理が終了したか否かを判定し、すべてのログ抽出情報について処理が終了したと判定したとき(Yes)は、一連の処理を終了して元の処理に復帰させる。

【００６５】

一方、ステップＳ１１４で、記憶装置４２のすべてのログ抽出情報についてステップＳ１０８～Ｓ１１２の処理が終了していないと判定したとき(No)は、ステップＳ１１６に移行して、次のログ抽出情報を記憶装置４２から読み出し、ステップＳ１０８に移行する。

一方、ステップＳ１１０で、該当のログ情報を索出しないと判定したとき(No)は、ステップＳ１１４に移行する。

【００６６】

次に、代表ログ情報生成処理を図７を参照しながら詳細に説明する。

図７は、代表ログ情報生成処理を示すフローチャートである。

代表ログ情報生成処理は、代表ログ情報生成部２０として実現される処理であって、ＣＰＵ３０において実行されると、図７に示すように、まず、ステップＳ２００に移行するようになっている。

【００６７】

ステップＳ２００では、前回の実行時から所定時間（例えば、１０分）が経過したか否かを判定し、所定時間が経過したと判定したとき(Yes)は、ステップＳ２０２に移行するが、そうでないと判定したとき(No)は、所定時間が経過するまでステップＳ２００で待機する。

ステップＳ２０２では、先頭のログ抽出情報を記憶装置４２から読み出し、ステップＳ２０４に移行して、読み出したログ抽出情報に基づいて、ログ抽出条件を満たすログ情報を代表ログ情報登録ＤＢ２２のなかから検索し、ステップＳ２０６に移行する。

【００６８】

ステップＳ２０６では、該当のログ情報を索出したか否かを判定し、該当のログ情報を索出したと判定したとき(Yes)は、ステップＳ２０８に移行して、代表ログ情報を生成し

、ステップＳ２１０に移行して、生成した代表ログ情報を代表ログ情報登録ＤＢ２２に登録し、ステップＳ２１２に移行する。

ステップＳ２１２では、記憶装置４２のすべてのログ抽出情報についてステップＳ２０４～Ｓ２１０の処理が終了したか否かを判定し、すべてのログ抽出情報について処理が終了したと判定したとき(Yes)は、一連の処理を終了して元の処理に復帰させる。

【００６９】

一方、ステップＳ２１２で、記憶装置４２のすべてのログ抽出情報についてステップＳ２０４～Ｓ２１０の処理が終了していないと判定したとき(No)は、ステップＳ２１４に移行して、次のログ抽出情報を記憶装置４２から読み出し、ステップＳ２０４に移行する。

一方、ステップＳ２０６で、該当のログ情報を索出しないと判定したとき(No)は、ステップＳ２１２に移行する。

【００７０】

次に、本実施の形態の動作を図８ないし図１３を参照しながら説明する。

初めに、パスワードの入力ミスが立て続けに数回行われた異常を検出する場合を説明する。

図８は、ログ抽出情報の設定内容を示す図である。

この場合、ログインエラーとなるログ情報が所定時間内に所定回出現している箇所を見つけ出せばよいので、ログ抽出情報は、例えば、図８に示すように、ログ発生条件として「ログ種別=Login AND ログレベル=ERROR」を、ログ発生期間として「１分間」を、ログ発生回数として「３回」をそれぞれ設定する。これは、ログ種別が「Login」でかつログレベルが「ERROR」となるログ情報であって、１分間に少なくとも３回出現するものが抽出可能となる。システム管理者は、このように設定したログ抽出情報を記憶装置４２に記憶しておく。

【００７１】

ログ情報管理装置１００では、ログ情報の生成対象となるイベントが発生すると、ステップＳ１０２，Ｓ１０４を経て、発生したイベントのログ情報が生成され、生成されたログ情報がログ情報登録ＤＢ１２に登録される。

図９は、ログ情報登録ＤＢ１２の登録内容を示す図である。

いま、ログ情報登録ＤＢ１２には、例えば、図９に示すように、５つのログ情報が登録され、ログＩＤとしてそれぞれ「１」～「５」が割り当てられているとする。ログ情報１（ログＩＤ「１」のログ情報をいう。以下、同様に略記する。）およびログ情報３，４はいずれも、ユーザＩＤ「userA」でログインを行った結果、パスワードエラーが発生したことを示し、最初の発生日時から最後の発生日時まで２０秒となっている。

【００７２】

したがって、ログ情報４が登録されると、ステップＳ１０６，Ｓ１０８を経て、ログ抽出情報が読み出され、読み出されたログ抽出情報に基づいて、ログ抽出条件を満たすログ情報がログ情報登録ＤＢ１２のなかから検索される。その結果、ログ情報１，３，４がログ抽出条件を満たすので、ログ情報１，３，４が索出され、ステップＳ１１２を経て、索出されたログ情報１，３，４が代表ログ情報登録ＤＢ２２に登録される。

【００７３】

さらに、ログ情報管理装置１００では、所定時間が経過すると、ステップＳ２０２，Ｓ２０４を経て、ログ抽出情報が読み出され、読み出されたログ抽出情報に基づいて、ログ抽出条件を満たすログ情報が代表ログ情報登録ＤＢ２２のなかから検索される。その結果、ログ情報１，３，４がログ抽出条件を満たすので、ログ情報１，３，４が索出され、ステップＳ２０８を経て、索出されたログ情報１，３，４を代表する代表ログ情報が生成される。

【００７４】

図１０は、代表ログ情報の内容を示す図である。

代表ログ情報は、例えば、図１０に示すように、ログ発生元ＩＤとして「0001」が、発生日時として「2003/12/08 01:10:00」が、ログ種別として「0111」が、ログレベルとし

て「NOTICE」が、ログ説明として「ログインチェック」がそれぞれ設定される。さらに、代表ログ情報の生成の原因となったログ情報１，３，４のログＩＤのリストが設定される。

【００７５】

代表ログ情報が生成されると、ステップＳ２１０を経て、生成された代表ログ情報が代表ログ情報登録ＤＢ２２に登録される。

なお、ログ抽出条件を満たすログ情報が代表ログ情報登録ＤＢ２２に存在しない場合は、代表ログ情報生成処理が実行されても代表ログ情報が生成されることはない。

次に、ユーザ登録してから所定日数経過しても１度もログインが行われない異常を検出する場合を説明する。

【００７６】

図１１は、ログ抽出情報の設定内容を示す図である。

この場合、ユーザＩＤが登録された時点を基準として所定期間内に一度もログインされていない箇所を見つけ出せばよいので、ログ抽出情報は、例えば、図１１に示すように、２つのログ抽出条件を組み合わせて設定する。第１のログ抽出条件を設定するボディ部Ａでは、ログ発生条件として「ログ種別=Register AND ログレベル=INFORMATION AND ログ説明+userA」を、ログ発生期間として「2003/01/01/00:00:00～2003/03/31/00:00:00」を、ログ発生回数として「１回」をそれぞれ設定する。これは、ログ種別が「Register」でかつログレベルが「INFORMATION」となりかつログ説明に「userA」を含むログ情報であって、２００３年１月１日午前０時０分０秒から２００３年３月３１日午前０時０分０秒までの間に少なくとも１回出現するものが抽出可能となる。

【００７７】

また、第２のログ抽出条件を設定するボディ部Ｂでは、ログ発生条件として「ログ種別=Login AND ログレベル=INFORMATION AND ログ説明+userA」を、ログ発生期間として「現時点から過去３ヶ月間」を、ログ発生回数として「０回」をそれぞれ設定する。これは、ログ種別が「Login」でかつログレベルが「INFORMATION」となりかつログ説明に「userA」を含むログ情報であって、現時点から過去３ヶ月間に１回も出現しないものが抽出可能となる。

【００７８】

したがって、これらログ抽出条件の両方を満たすログ情報を抽出すれば、ユーザＩＤ「userA」を登録してから過去３ヶ月間に１度もログインが行われない異常を検出することができる。そこで、ログ抽出式としては、「Ａ AND Ｂ」を設定する。システム管理者は、このように設定したログ抽出情報を記憶装置４２に記憶しておく。

ログ情報管理装置１００では、ログ情報の生成対象となるイベントが発生すると、ステップＳ１０２，Ｓ１０４を経て、発生したイベントのログ情報が生成され、生成されたログ情報がログ情報登録ＤＢ１２に登録される。

【００７９】

図１２は、ログ情報登録ＤＢ１２の登録内容を示す図である。

いま、ログ情報登録ＤＢ１２には、例えば、図１２に示すように、２００３年１２月現在において３つのログ情報が登録され、ログＩＤとしてそれぞれ「１」～「３」が割り当てられているとする。ログ情報１は、２００３年１月１日においてユーザＩＤ「userA」を登録したことを示している。

【００８０】

この状態で新たなログ情報が登録されると、ステップＳ１０６，Ｓ１０８を経て、ログ抽出情報が読み出され、読み出されたログ抽出情報に基づいて、ログ抽出条件を満たすログ情報がログ情報登録ＤＢ１２のなかから検索される。その結果、ログ情報１がログ抽出条件を満たすので、ログ情報１が索出され、ステップＳ１１２を経て、索出されたログ情報１が代表ログ情報登録ＤＢ２２に登録される。

【００８１】

さらに、ログ情報管理装置１００では、所定時間が経過すると、ステップＳ２０２，Ｓ

２０４を経て、ログ抽出情報が読み出され、読み出されたログ抽出情報に基づいて、ログ抽出条件を満たすログ情報が代表ログ情報登録ＤＢ２２のなかから検索される。その結果、ログ情報１がログ抽出条件を満たすので、ログ情報１が索出され、ステップＳ２０８を経て、索出されたログ情報１を代表する代表ログ情報が生成される。

【００８２】

図１３は、代表ログ情報の内容を示す図である。

代表ログ情報は、例えば、図１３に示すように、ログ発生元ＩＤとして「0001」が、発生日時として「2003/12/08 01:10:00」が、ログ種別として「0010」が、ログレベルとして「NOTICE」が、ログ説明として「システム利用チェック」がそれぞれ設定される。さらに、代表ログ情報の生成の原因となったログ情報１のログＩＤのリストが設定される。

【００８３】

代表ログ情報が生成されると、ステップＳ２１０を経て、生成された代表ログ情報が代表ログ情報登録ＤＢ２２に登録される。

なお、ログ抽出条件を満たすログ情報が代表ログ情報登録ＤＢ２２に存在しない場合は、代表ログ情報生成処理が実行されても代表ログ情報が生成されることはない。

このようにして、本実施の形態では、複数の条件を組み合わせて設定可能なログ抽出条件を含むログ抽出情報を入力し、入力したログ抽出情報に基づいて、ログ抽出条件を満たすログ情報をログ情報登録ＤＢ１２のなかから抽出し、抽出したログ情報を代表する代表ログ情報を生成するようになっている。

【００８４】

これにより、システム管理者は、代表ログ情報を参照すれば、複数のログ情報を組み合わせて把握することができる複雑な異常を把握することができるので、従来に比して、複雑な異常を比較的容易に検出することができる。

さらに、本実施の形態では、抽出したログ情報を参照可能なログリストを含む代表ログ情報を生成するようになっている。

【００８５】

これにより、システム管理者は、代表ログ情報を参照すれば、その代表ログ情報の生成の原因となったログ情報を参照することができるので、異常発生の原因を分析しやすくなる。

さらに、本実施の形態では、生成した代表ログ情報を代表ログ情報登録ＤＢ２２に登録するようになっている。

【００８６】

これにより、代表ログ情報は、代表ログ情報登録ＤＢ２２に他のログ情報とは別に記憶されるので、システム管理者は、代表ログ情報を参照しやすくなる。したがって、複雑な異常をさらに容易に検出することができる。

上記実施の形態において、ログ情報登録ＤＢ１２は、発明１、９、１７、１８または２０のログ情報記憶手段に対応し、代表ログ情報登録ＤＢ２２は、発明３、１１または２０の代表ログ情報記憶手段に対応し、ＣＰＵ３０は、発明１８の演算手段に対応している。また、入力装置４０は、発明１８の入力手段に対応し、ログ抽出情報入力部１４は、発明１のログ抽出条件設定手段に対応し、ログ抽出情報入力部１４による入力は、発明９、１７または１８のログ抽出条件設定ステップに対応し、ログ情報抽出部１８およびステップＳ１０８，Ｓ２０４は、発明１または２のログ情報抽出手段に対応している。

【００８７】

また、上記実施の形態において、ステップＳ１０８，Ｓ２０４は、発明９、１０、１７ないし１９のログ情報抽出ステップに対応し、代表ログ情報生成部２０およびステップＳ２０８は、発明１ないし３の代表ログ情報生成手段に対応し、ステップＳ２０８は、発明９ないし１１、１７ないし２０の代表ログ情報生成ステップに対応している。また、ログリストは、発明２、１０または１９のログ参照情報に対応している。

【００８８】

なお、上記実施の形態においては、１人のシステム管理者がログ抽出条件を設定する場

合について説明したが、ログ情報管理装置１００を複数のシステム管理者が利用する場合は、各システム管理者ごとにログ抽出条件が設定可能となるように構成するのが好ましい。

これにより、各システム管理者ごとに、そのシステム管理者が注目する複雑な異常を検出することができるので、システムの利便性を向上することができる。

【００８９】

この場合において、ログ抽出情報入力部１４は、発明４のログ抽出条件設定手段に対応し、ログ抽出情報入力部１４による入力は、発明１２または２１のログ抽出条件設定ステップに対応している。

また、上記実施の形態において、図６および図７のフローチャートに示す処理を実行するにあたってはいずれも、ＲＯＭ３２にあらかじめ格納されている制御プログラムを実行する場合について説明したが、これに限らず、これらの手順を示したプログラムが記憶された記憶媒体から、そのプログラムをＲＡＭ３４に読み込んで実行するようにしてもよい。

【００９０】

ここで、記憶媒体とは、ＲＡＭ、ＲＯＭ等の半導体記憶媒体、ＦＤ、ＨＤ等の磁気記憶型記憶媒体、ＣＤ、ＣＤＶ、ＬＤ、ＤＶＤ等の光学的読取方式記憶媒体、ＭＯ等の磁気記憶型／光学的読取方式記憶媒体であって、電子的、磁気的、光学的等の読み取り方法のいかんにかかわらず、コンピュータで読み取り可能な記憶媒体であれば、あらゆる記憶媒体を含むものである。

【００９１】

また、上記実施の形態においては、本発明に係るログ情報管理システム、サービス提供システム、ログ情報管理プログラムおよびサービス提供プログラム、並びにログ情報管理方法およびサービス提供方法を、図１に示すように、システムの異常を検出する場合について適用したが、これに限らず、本発明の主旨を逸脱しない範囲で他の場合にも適用可能である。例えば、次の３つの構成を提案することができる。

【００９２】

まず、第１の構成を説明する。第１の構成は、本発明をログ情報管理サーバ３００に適用したものである。

図１４は、本発明をログ情報管理サーバ３００に適用した場合のネットワークシステムの機能概要を示す機能ブロック図である。

ネットワーク１９９には、図１４に示すように、ネットワークプリンタ２００と、ログ情報管理サーバ３００とが接続されている。

【００９３】

ネットワークプリンタ２００は、自己で発生したイベントに基づいてログ情報を生成するログ情報生成部２４と、ログ情報生成部２４で生成したログ情報をログ情報管理サーバ３００に送信するログ情報送信部２５とを有して構成されている。

ログ情報管理サーバ３００は、ログ情報登録ＤＢ１２、ログ抽出情報入力部１４、ログ抽出情報記憶部１６、ログ情報抽出部１８、代表ログ情報生成部２０および代表ログ情報登録ＤＢ２２のほか、ログ情報を受信してログ情報登録ＤＢ１２に登録するログ情報受信部２６を有して構成されている。ここで、ログ情報としては、例えば、ネットワークプリンタ２００で発生した障害（紙詰まり、トナー切れ等）に関する情報を記録する。

【００９４】

これにより、システム管理者は、代表ログ情報を参照すれば、複数のログ情報を組み合わせて把握することができる複雑な異常を把握することができるので、従来に比して、ネットワークプリンタ２００で発生した複雑な異常を比較的容易に検出することができる。

この場合において、ネットワークプリンタ２００は、発明７、１５または２４のネットワークデバイスに対応し、ログ情報受信部２６は、発明７のログ情報受信手段、または発明７のログ情報保存手段に対応している。

【００９５】

なお、図１４の例では、ネットワークプリンタ２００のログ情報を管理する場合について適用したが、これに限らず、ネットワークプリンタ２００に代えて、例えば、プロジェクタ、電子ペーパ、ホームゲートウェイ、パソコン、ＰＤＡ（Personal Digital Assistant）、ネットワークストレージ、オーディオ機器、携帯電話、ＰＨＳ（登録商標）（Personal Handyphone System）、ウォッチ型ＰＤＡ、ＳＴＢ（Set Top Box）、ＰＯＳ（Point Of Sale）端末、ＦＡＸ機、電話（ＩＰ電話等も含む。）、その他のネットワークデバイスに適用することができる。

【００９６】

次に、第２の構成を説明する。第２の構成は、本発明をＷｅｂサーバ３５０に適用したものである。

図１５は、本発明をＷｅｂサーバ３５０に適用した場合のネットワークシステムの機能概要を示す機能ブロック図である。

ネットワーク１９９には、図１５に示すように、ホスト端末２５０と、Ｗｅｂサーバ３５０とが接続されている。

【００９７】

ホスト端末２５０は、Ｗｅｂサーバ３５０にアクセスしてＷｅｂサービスの提供を受けるＷｅｂブラウザ２７を有して構成されている。

Ｗｅｂサーバ３５０は、ログ情報登録ＤＢ１２、ログ抽出情報入力部１４、ログ抽出情報記憶部１６、ログ情報抽出部１８、代表ログ情報生成部２０および代表ログ情報登録ＤＢ２２のほか、ホスト端末２５０からのアクセスに応じてＷｅｂサービスを提供するＷｅｂサービス処理部２８と、Ｗｅｂサービス処理部２８で発生したイベントに基づいてログ情報を生成してログ情報登録ＤＢ１２に登録するログ情報生成部２９とを有して構成されている。ここで、ログ情報としては、例えば、インターネットショッピングでユーザが注文した商品等に関する情報を記録する。

【００９８】

これにより、システム管理者は、代表ログ情報を参照すれば、複数のログ情報を組み合わせて把握することができる複雑な状態を把握することができるので、従来に比して、Ｗｅｂサーバ３５０に対するアクセスにより発生した複雑な状態を比較的容易に検出することができる。

この場合において、Ｗｅｂサービス処理部２８は、発明８のサービス処理手段に対応し、ログ情報生成部２９は、発明８のログ情報生成手段、または発明８のログ情報保存手段に対応している。

【００９９】

次に、第３の構成を説明する。第３の構成は、ユーザに提供したサービスが１度も使用されていない状態を検出する場合について適用したものである。

この場合、上記実施の形態において、ログ発生条件として、検出対象とするサービスのサービス識別子およびサービス利用時に発生するイベントコマンドを、ログ発生期間として、検出対象とする所望の期間を、ログ発生回数として、「０回」を設定すればよい。

【０１００】

これにより、システム管理者は、代表ログ情報を参照すれば、ユーザに提供したサービスが１度も使用されていない状態を把握することができる。

【図面の簡単な説明】

【０１０１】

【図１】ログ情報管理装置１００の機能概要を示す機能ブロック図である。

【図２】ログ情報管理装置１００のハードウェア構成を示すブロック図である。

【図３】ログ情報登録ＤＢ１２のデータ構造を示す図である。

【図４】代表ログ情報登録ＤＢ２２のデータ構造を示す図である。

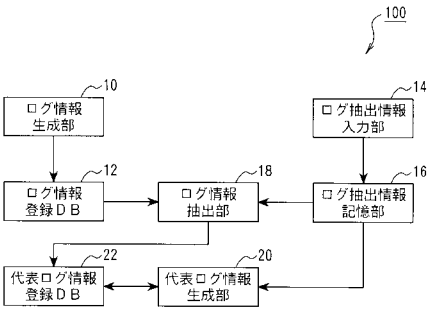
【図５】ログ抽出情報のデータ構造を示す図である。

【図６】ログ情報抽出処理を示すフローチャートである。

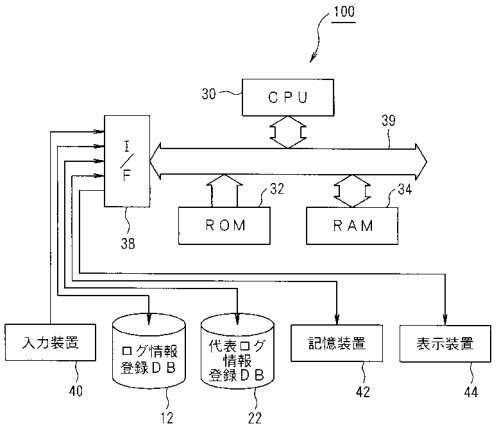
【図７】代表ログ情報生成処理を示すフローチャートである。

【図８】ログ抽出情報の設定内容を示す図である。
【図９】ログ情報登録ＤＢ１２の登録内容を示す図である。
【図１０】代表ログ情報の内容を示す図である。
【図１１】ログ抽出情報の設定内容を示す図である。
【図１２】ログ情報登録ＤＢ１２の登録内容を示す図である。
【図１３】代表ログ情報の内容を示す図である。
【図１４】本発明をログ情報管理サーバ３００に適用した場合のネットワークシステムの機能概要を示す機能ブロック図である。
【図１５】本発明をＷｅｂサーバ３５０に適用した場合のネットワークシステムの機能概要を示す機能ブロック図である。
【符号の説明】
【０１０２】
１００…ログ情報管理装置，　１０，２４，２９…ログ情報生成部，　１２…ログ情報登録ＤＢ，　１４…ログ抽出情報入力部，　１６…ログ抽出情報記憶部，　１８…ログ情報抽出部，　２０…代表ログ情報生成部，　２２…代表ログ情報登録ＤＢ，　２５…ログ情報送信部，　２６…ログ情報受信部，　２７…Ｗｅｂブラウザ，　２８…Ｗｅｂサービス処理部，　３０…ＣＰＵ，　３２…ＲＯＭ，　３４…ＲＡＭ，　３８…Ｉ／Ｆ，　４０…入力装置，　４２…記憶装置，　４４…表示装置，　２００…ネットワークプリンタ，　２５０…ホスト端末，　３００…ログ情報管理サーバ，　３５０…Ｗｅｂサーバ

【図１】




【図２】



【図３】

| | 項目 | 概要 |
|---|---|---|
| 400 | ログＩＤ | このログを一意に識別するＩＤ。 |
| 402 | ログ発生元ＩＤ | このログの作成者を識別するためのＩＤ。<br>ユーザやデバイス、システム等ログを作成した者を識別するなんらかの識別子が設定される。システムとして一意に判別できるように管理されていることが望ましい。 |
| 404 | 発生日時 | このログが生成された時間。 |
| 406 | ログ種別 | このログが発生するのに起因した操作を表す識別子。例えば発生元がプリンタであった場合には、印刷を開始した際のログを意味するログ種別には“print”などといった識別子が入ることが予想される。<br>ユーザであれば、例えばログイン作業を行った際のログであれば“Login”等の識別子が入ることが予想される。システムとして一意に判別できるように管理されていることが望ましい。 |
| 408 | ログレベル | このログ情報のレベルを設定する。例えば、“INFORMATION”、“CAUTION”、“WARNING”、“ERROR”等。 |
| 410 | ログ説明 | このログの詳細な内容が記述される。 |

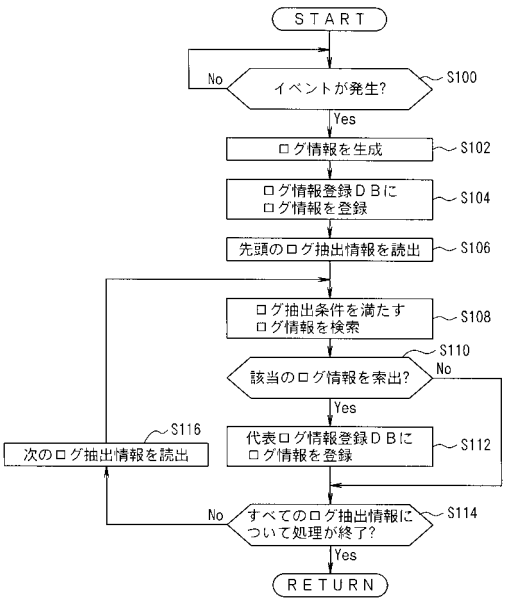
【図４】

| | 項目 | 概要 |
|---|---|---|
| 420 | ログＩＤ | このログを一意に識別するＩＤ。 |
| 422 | ログ発生元ＩＤ | このログの作成者を識別するためのＩＤ。<br>ユーザやデバイス、システム等ログを作成した者を識別するなんらかの識別子が設定される。システムとして一意に判別できるように管理されていることが望ましい。 |
| 424 | 発生日時 | この代表ログ情報が生成された時間。 |
| 426 | ログ種別 | この代表ログ情報が当てはまったログ抽出情報のログ抽出情報ＩＤ。 |
| 428 | ログレベル | このログ情報が代表ログ情報であることを設定する。例えば、NOTICE等。 |
| 430 | ログ説明 | この代表ログ情報の説明。基本的にログ抽出情報のログ抽出説明が入る。 |
| 432 | ログリスト | 代表ログ情報の生成の原因となったログ情報のログＩＤのリスト。 |

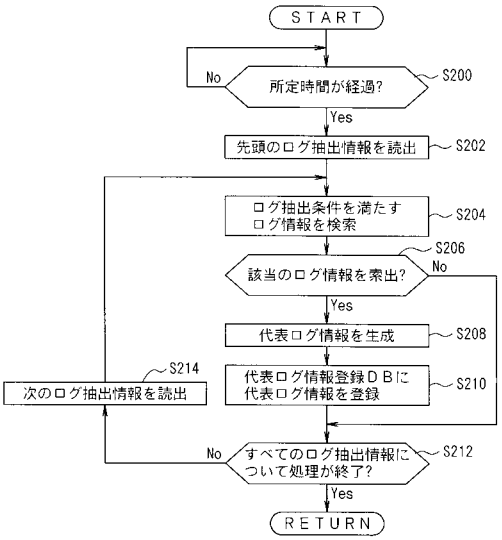
【図５】

| | 項目 | | 概要 |
|---|---|---|---|
| 440 | ヘッダ部 | | ログ抽出情報の基本情報を設定する。<br>以下の3項目から構成される。 |
| 442 | | ログ抽出情報ＩＤ | このログ抽出情報を一意に識別するための識別子。 |
| 444 | | ログ抽出説明 | このログ抽出情報の説明。 |
| 446 | | ログ抽出式 | 各ログ抽出条件を使用した検索式を指定する。複数指定可。<br>例(Ａ/Ｂはログ抽出条件ＩＤとする)<br>Ａ：Ａを満たす<br>!Ａ：Ａを満たさない<br>+Ａ：Ａを含む<br>-Ａ：Ａを含まない<br>Ａ AND Ｂ：ＡとＢを両方満たす<br>Ａ OR Ｂ：ＡかＢを満たす |
| 460 | ボディ部 | | ログ情報を抽出するための各種条件を指定する。以下の4項目から構成される。<br>複数指定可。 |
| 462 | | ログ抽出条件ＩＤ | このログ抽出条件を識別するためのＩＤ。 |
| 464 | | ログ発生条件 | ログ情報の項目のうち、注目する項目についての抽出条件を指定する。指定方法は、ログ抽出式と同一方式とする。 |
| 466 | | ログ発生期間 | 抽出対象とするログの有効期間を指定する。<br>指定方法<br>・開始時刻～終了時刻<br>・現時点からの過去経過時刻<br>・ある時点からの経過時間<br>例1<br>2003/12/01 00:00:00～<br>2003/12/31 00:00:00<br>例2<br>現在時刻から過去1分間の間 |
| 468 | | ログ発生回数 | 注目するべきログの、指定したログ発生期間中での発生回数を指定する。 |

【図６】



【図７】




【図８】

| | | |
|---|---|---|
| | ログ抽出情報 | |
| 440 | ヘッダ部 | |
| 442 | ログ抽出情報ＩＤ | 0111 |
| 444 | ログ抽出説明 | ログインチェック |
| 446 | ログ抽出式 | A |
| 460 | ボディ部 | |
| 462 | ログ抽出条件ＩＤ | A |
| 464 | ログ発生条件 | ログ種別=Login AND<br>ログレベル=ERROR |
| 466 | ログ発生期間 | 1分間 |
| 468 | ログ発生回数 | 3回 |

【図９】

| 400 | 402 | 404 | 406 | 408 | 410 |
|---|---|---|---|---|---|
| ログＩＤ | ログ発生元ＩＤ | 発生日時 | ログ種別 | ログレベル | ログ説明 |
| 1 | 001 | 2003/12/08/<br>01:01:10 | Login | ERROR | id=userA<br>password=userA |
| 2 | 001 | 2003/12/08/<br>01:01:15 | Start | INFO | start |
| 3 | 001 | 2003/12/08/<br>01:01:20 | Login | ERROR | id=userA<br>password=hoge? |
| 4 | 001 | 2003/12/08/<br>01:01:30 | Login | ERROR | id=userA<br>password=hero? |
| 5 | 001 | 2003/12/08/<br>01:01:35 | Continue | INFO | continue |

【図１０】

| | | |
|---|---|---|
| 420 | ログ発生元ＩＤ | 0001 |
| 424 | 発生日時 | 2003/12/08 01:10:00 |
| 426 | ログ種別 | 0111 |
| 428 | ログレベル | NOTICE |
| 430 | ログ説明 | ログインチェック |
| 432 | ログリスト | 1,3,4 |

【図１１】

| | | |
|---|---|---|
| | ログ抽出情報 | |
| 440 | ヘッダ部 | |
| 442 | ログ抽出情報ＩＤ | 0010 |
| 444 | ログ抽出説明 | システム利用チェック |
| 446 | ログ抽出式 | A AND B |
| 460 | ボディ部A | |
| 462 | ログ抽出条件ＩＤ | A |
| 464 | ログ発生条件 | ログ種別=Register<br>AND<br>ログレベル=INFORMATION<br>AND<br>ログ説明+userA |
| 466 | ログ発生期間 | 2003/01/01/00:00:00<br>～<br>2003/03/31/00:00:00 |
| 468 | ログ発生回数 | 1回 |
| 460 | ボディ部B | |
| 462 | ログ抽出条件ＩＤ | B |
| 464 | ログ発生条件 | ログ種別=Login<br>AND<br>ログレベル=INFORMATION<br>AND<br>ログ説明+userA |
| 466 | ログ発生期間 | 現時点から過去3ヶ月間 |
| 468 | ログ発生回数 | 0回 |

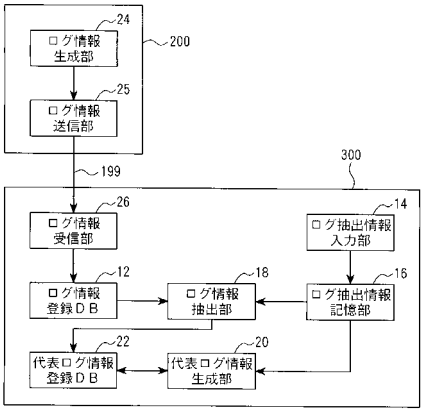
【図１２】

| 400 ログＩＤ | 402 ログ発生元ＩＤ | 404 発生日時 | 406 ログ種別 | 408 ログレベル | 410 ログ説明 |
|---|---|---|---|---|---|
| 1 | 001 | 2003/01/01/ 01:01:01 | Register | INFO | id=userA password=test |
| 2 | 001 | 2003/01/10/ 10:10:10 | Start | INFO | start |
| 3 | 001 | 2003/02/02/ 02:02:02 | Login | ERROR | id=userA password=userA |

【図１３】

| | | |
|---|---|---|
| 420 | ログ発生元ＩＤ | 0001 |
| 424 | 発生日時 | 2003/12/08 01:10:00 |
| 426 | ログ種別 | 0010 |
| 428 | ログレベル | NOTICE |
| 430 | ログ説明 | システム利用チェック |
| 432 | ログリスト | 1 |

【図１４】




【図１５】