(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2010-525424
(P2010-525424A)
(43)公表日　平成22年7月22日(2010.7.22)

| (51)Int.Cl. | F I | テーマコード（参考） |
|---|---|---|
| G06Q 10/00 (2006.01) | G06F 17/60 174 | |

審査請求 未請求　予備審査請求 未請求　（全 24 頁）

| | |
|---|---|
| (21)出願番号 | 特願2009-554678 (P2009-554678) |
| (86)(22)出願日 | 平成20年3月17日 (2008.3.17) |
| (85)翻訳文提出日 | 平成21年11月10日 (2009.11.10) |
| (86)国際出願番号 | PCT/US2008/057220 |
| (87)国際公開番号 | WO2008/115864 |
| (87)国際公開日 | 平成20年9月25日 (2008.9.25) |
| (31)優先権主張番号 | 11/687,864 |
| (32)優先日 | 平成19年3月19日 (2007.3.19) |
| (33)優先権主張国 | 米国 (US) |

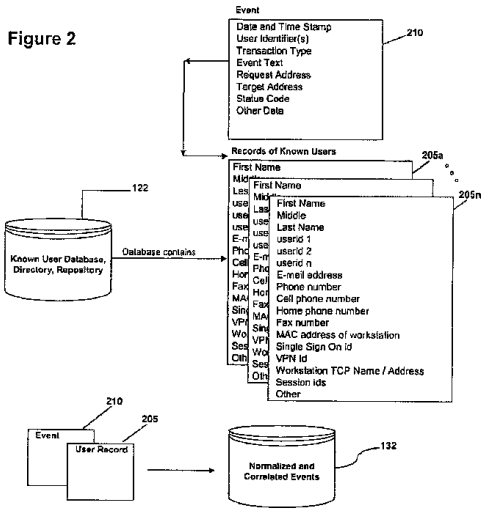
(71)出願人　509263124
ロング・クルト・ジェームス
アメリカ合衆国、フロリダ州　３３７０３、セント・ピーターズバーグ、カロライナ・アベニュー・エヌイー、１９４５
(74)代理人　100069556
弁理士　江崎　光史
(74)代理人　100111486
弁理士　鍛冶澤　實
(74)代理人　100157440
弁理士　今村　良太
(74)代理人　100153419
弁理士　清田　栄章

最終頁に続く

(54)【発明の名称】悪用及び乱用を検出するシステム及び方法

(57)【要約】
データと関連する少なくとも一つのトランザクション及びアクティビティを監視するための規則を生成することによって、コンピュータ環境でのデータの悪用及び／又は乱用を検知するシステムと方法を提示するものである。この規則は、データの悪用又は乱用を示す、少なくとも一つのトランザクション及びアクティビティに関する少なくとも一つの判断基準にもとづき生成することができる。当該の少なくとも一つの判断基準が満たされた時にイベントが発生し、そのイベントが起こったか否かを決定するために、当該の少なくとも一つのトランザクション及びアクティビティに規則を適用する。イベントが起こった場合に一つのヒットを保存し、イベントが起こった場合に通報を発出することができる。規則に関するヒットの集合体を提供することができる。

Figure 2



【特許請求の範囲】
【請求項１】
コンピュータ環境でのデータの悪用又は乱用を検知する方法であって、
データと関連する少なくとも一つのトランザクション及びアクティビティを監視するための規則を生成して、その規則が、データの悪用及び乱用を示す少なくとも一つのトランザクション及びアクティビティに関する少なくとも一つの判断基準を含むようにする工程と、
当該の少なくとも一つの判断基準を満たした時にイベントが発生し、そのイベントが起こったか否かを決定するために、当該の少なくとも一つのトランザクション及びアクティビティに規則を適用する工程と、
イベントが起こった場合に一つのヒットを保存する工程と、
イベントが起こった場合に通報を発出する工程と、
規則に関するヒットの集合体を提供する工程と、
を有する方法。
【請求項２】
当該の少なくとも一つのトランザクション及びアクティビティに規則を適用するスケジュールを立てる工程を更に有する請求項１に記載の方法。
【請求項３】
当該の少なくとも一つのトランザクション及びアクティビティに規則をリアルタイムで適用するか否かを決定する工程と、
規則をリアルタイムで適用しない場合、当該の少なくとも一つのトランザクション及びアクティビティに規則を適用するスケジュールを立てる工程と、
を更に有する請求項１に記載の方法。
【請求項４】
当該の通報の受信者を指定する工程と、
当該の通報で送信するメッセージを生成する工程と、
を更に有する請求項１に記載の方法。
【請求項５】
時間パラメータ、数量パラメータ及びユーザパラメータの中の少なくとも一つにもとづき、当該の規則に関する少なくとも一つの判断基準の少なくとも一部を選定する工程を更に有する請求項１に記載の方法。
【請求項６】
複数のデータベースのデータと関連する少なくとも一つのトランザクション及びアクティビティに規則を適用する工程を更に有する請求項１に記載の方法。
【請求項７】
時間パラメータと数量パラメータにもとづき、当該の規則に関する少なくとも一つの判断基準の少なくとも一部を選定する工程を更に有する請求項１に記載の方法。
【請求項８】
少なくとも一つの判断基準を選定するための規則管理ページを提示する工程と、
選定した少なくとも一つの判断基準にもとづき規則の少なくとも一部を生成する工程と、
を更に有する請求項１に記載の方法。
【請求項９】
当該の少なくとも一つのトランザクション及びアクティビティに規則を適用するスケジュールを選定するための規則スケジュールページを提示する工程と、
当該のイベントが起こったか否かを決定するために、当該のスケジュールにもとづき当該の少なくとも一つのトランザクション及びアクティビティに規則を適用する工程と、
を更に有する請求項８に記載の方法。
【請求項１０】
当該の規則をリアルタイムで適用するスケジュールを立てる工程を更に有する請求項１

に記載の方法。
【請求項１１】
当該の通報の受信者の電子メールアドレスを指定する工程を更に有する請求項１に記載の方法。
【請求項１２】
コンピュータ環境でのデータの悪用又は乱用を検知するシステムであって、このシステムが、
データと関連する少なくとも一つのトランザクション及びアクティビティに関する、そのデータの悪用及び乱用を示す少なくとも一つの判断基準を選定するとともに、当該の少なくとも一つのトランザクション及びアクティビティを監視するための規則を適用するスケジュールを選定するためのユーザインタフェースと、
そのユーザインタフェースと通信して、データと関連するトランザクション及びアクティビティにアクセスするマイクロプロセッサと、
を備えており、
このマイクロプロセッサが、選定された少なくとも一つの判断基準にもとづき規則の少なくとも一部を生成するとともに、当該の少なくとも一つの判断基準が満たされた時にイベントが発生し、そのイベントが起こったか否かを決定するために、選定したスケジュールにもとづき当該の少なくとも一つのトランザクション及びアクティビティに規則を適用し、
イベントが起こった場合に、このマイクロプロセッサが一つのヒットを保存し、
イベントが起こった場合に、このマイクロプロセッサが通報を発出し、
このマイクロプロセッサが規則に関するヒットの集合体を生成する、
システム。
【請求項１３】
マイクロプロセッサが、当該の少なくとも一つのトランザクション及びアクティビティに規則をリアルタイムで適用するか否かを決定する請求項１２に記載のシステム。
【請求項１４】
マイクロプロセッサが、通報で送信するメッセージを生成する請求項１２に記載のシステム。
【請求項１５】
マイクロプロセッサが、時間パラメータ、数量パラメータ及びユーザパラメータの中の少なくとも一つにもとづき規則の少なくとも一部を生成する請求項１２に記載のシステム。
【請求項１６】
マイクロプロセッサが、複数のデータベースのデータと関連する少なくとも一つのトランザクション及びアクティビティに規則を適用する請求項１２に記載のシステム。
【請求項１７】
コンピュータ環境でのデータの悪用又は乱用を検知するためのコンピュータで読み取り可能なプログラム命令を有する、製品内に組み込まれたコンピュータで読み取り可能なプログラムであって、そのプログラムが、
データと関連する少なくとも一つのトランザクション及びアクティビティに関する、データの悪用及び乱用を示す少なくとも一つの判断基準の選定をコンピュータに実行させるプログラム命令と、
少なくとも一つの判断基準にもとづき、当該の少なくとも一つのトランザクション及びアクティビティを監視するための規則の少なくとも一部を生成することをコンピュータに実行させるプログラム命令と、
当該の少なくとも一つのトランザクション及びアクティビティに規則を適用するスケジュールの選定をコンピュータに実行させるプログラム命令と、
当該の少なくとも一つの判断基準が満たされた時にイベントが発生し、そのイベントが起こったか否かを決定するために、選定したスケジュールにもとづき当該の少なくとも一

つのトランザクション及びアクティビティに規則を適用することをコンピュータに実行させるプログラム命令と、
イベントが起こった場合に一つのヒットを保存することをコンピュータに実行させるプログラム命令と、
イベントが起こった場合に通報を発出することをコンピュータに実行させるプログラム命令と、
規則に関するヒットの集合体を提供することをコンピュータに実行させるプログラム命令と、
を有するコンピュータで読み取り可能なプログラム
【請求項１８】
複数のデータベースのデータと関連する少なくとも一つのトランザクション及びアクティビティに規則を適用することをコンピュータに実行させるプログラム命令を更に有する請求項１７に記載のプログラム。
【請求項１９】
当該の少なくとも一つのトランザクション及びアクティビティに規則をリアルタイムで適用することをコンピュータに実行させるプログラム命令を更に有する請求項１７に記載のプログラム。
【請求項２０】
時間パラメータ、数量パラメータ及びユーザパラメータの中の少なくとも一つにもとづき、規則の少なくとも一部を生成することをコンピュータに実行させるプログラム命令を更に有する請求項１７に記載のプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ユーザ識別データを含む、ログファイルやそれ以外の同様のレコード内などのデータの分析にもとづき、コンピュータ環境での悪用及び／又は乱用を検出するシステム及び方法に関する。より詳しくは、本発明は、ユーザ識別データを含む、ログファイル内などのアプリケーションレイヤのデータの分析にもとづき、コンピュータ環境での悪用及び／又は乱用を検出するシステム及び方法に関する。
【背景技術】
【０００２】
ユーザによる悪用又は乱用を検出する従来システムは、少なくとも従来システムの能力がログファイルのフォーマットを認識して、ログファイルにアクセスすることに限られているという理由において不十分である。そのことは、システムが異なるアプリケーションによって生成されたログファイルにアクセスする場合、各アプリケーションが異なる形式のログファイルを生成する可能性が有るので、特に難しい。
【０００３】
従来システムでの別の問題は、ユーザが会社（又はその他の同様の組織）のシステムにアクセスするのに幾つかの異なる方法が有ることである。例えば、多くの実例において、ユーザが組織の異なるアプリケーション又は保存データにアクセスするために、幾つかの異なるユーザＩＤとパスワードを使用する可能性が有る。そのような悪用又は乱用検知システムは、様々なアプリケーションに渡るユーザのアクティビティを関連付ける方法を持っていない。同様に、幾つかの実例において、一つのアプリケーションにもとづきユーザの挙動を評価しても、会社のシステム又は情報の悪用又は乱用を示す挙動パターンを識別するのに十分な情報を提供することはできない。
【０００４】
システムの悪用又は乱用の検知に関する従来システムの幾つかが、特許文献１～４に記載されている。そのようなシステム及びその他の周知のシステムには、別の様々な欠点が有る。
【先行技術文献】

【特許文献】
【０００５】
【特許文献１】米国特許第５，５５７，７４２号明細書（Method and System for Detecting Intrusion Into and Misuse of a Data Processing System ）
【特許文献２】米国特許第６，３４７，３７４号明細書（Event Detection ）
【特許文献３】米国特許第６，４０５，３１８号明細書（Intrusion Detection System）
【特許文献４】米国特許第６，５４９，２０８号明細書（Information Security Analysis System）
【発明の概要】
【発明が解決しようとする課題】
【０００６】
本発明の様々な特徴は、既存システムの前記及びその他の欠点の中の少なくとも幾つかを克服するものである。
【課題を解決するための手段】
【０００７】
一つの実施形態において、ユーザがアクセスする様々なアプリケーションのアプリケーションレイヤのログを通してユーザを追跡するためのシステム及び方法を提供する。
【０００８】
一つの実施形態において、監視システムが、イベントログファイルにアクセスして、そのようなイベントログファイルを既知のユーザ又はシステムが識別子を取り出すことが可能なユーザと関連付ける。イベントログは、アプリケーション及びアクセスレイヤ機器によって記録されたトランザクション及び／又はアクティビティの記録の集合体とすることができる。抽出されたイベントは、分析、保存及び／又は報告に適したレコードに正規化することができる。正規化されたイベントは、所与の環境に対して定義された悪用シナリオに関して分析することができる。一つの実施形態において、イベントがシステムのユーザと関連付けられ、イベントレコードが既知のユーザと関連する識別子を含むことができる。
【０００９】
一つの実施形態において、正規化され、関連付けられたイベントは、ユーザ固有の識別子又は職務／組織との関係にもとづきモデル化されたユーザ特有の悪用監視シナリオに関して分析することができる。
【００１０】
一つの実施形態において、コンピュータ環境内でのデータの悪用又は乱用を検知する方法を規定する。その方法は、データと関連する少なくとも一つのトランザクション及びアクティビティを監視するための規則を生成し、その規則が、データの悪用又は乱用を示す、当該の少なくとも一つのトランザクション及びアクティビティに関する少なくとも一つの判断基準を含むようにする工程と、当該の少なくとも一つの判断基準が満たされた時にイベントが発生し、そのようなイベントが発生したか否かを決定するために、当該の少なくとも一つのトランザクション及びアクティビティに規則を適用する工程と、イベントが発生した場合に一つのヒットを保存する工程と、イベントが発生した場合に通報を発出する工程と、当該の規則に関するヒットの集合体を提供する工程とを有する。
【００１１】
一つの実施形態において、コンピュータ環境内でのデータの悪用又は乱用を検知するシステムを規定する。そのシステムは、データの悪用又は乱用を示す、データと関連した少なくとも一つのトランザクション及びアクティビティに関する少なくとも一つの判断基準を選定するとともに、当該の少なくとも一つのトランザクション及びアクティビティを監視するための規則を適用するスケジュールを選定するためのユーザインタフェースと、そのユーザインタフェースと通信して、データと関連するトランザクション及びアクティビティにアクセスするマイクロプロセッサとを有する。このマイクロプロセッサは、選定された少なくとも一つの判断基準にもとづき規則の少なくとも一部を生成して、イベントが

発生したか否かを決定するために、選定されたスケジュールにもとづき当該の少なくとも一つのトランザクション及びアクティビティに規則を適用する。当該の少なくとも一つの判断基準が満たされた時に、イベントが発生する。マイクロプロセッサは、イベントが発生した場合に一つのヒットを保存するとともに、イベントが発生した場合に通報を発出する。マイクロプロセッサは、規則に関するヒットの集合体を生成する。

【００１２】

一つの実施形態において、コンピュータ環境内でのデータの悪用又は乱用を検知するためのコンピュータで読み取り可能なプログラム命令を有する、製品に組み込まれたコンピュータで読み取り可能なプログラムを規定する。このプログラムは、データの悪用又は乱用を示す、データと関連する少なくとも一つのトランザクション及びアクティビティに関する少なくとも一つの判断基準の選定をコンピュータに実行させるプログラム命令と、少なくとも一つの判断基準にもとづき、当該の少なくとも一つのトランザクション及びアクティビティを監視するための規則の少なくとも一部を生成することをコンピュータに実行させるプログラム命令と、当該の少なくとも一つのトランザクション及びアクティビティに規則を適用するスケジュールの選定をコンピュータに実行させるプログラム命令と、少なくとも一つの判断基準が満たされた場合にイベントが発生し、イベントが発生したか否かを決定するために、選定したスケジュールにもとづき当該の少なくとも一つのトランザクション及びアクティビティに規則を適用することをコンピュータに実行させるプログラム命令と、イベントが発生した場合に一つのヒットを保存することをコンピュータに実行させるプログラム命令と、イベントが発生した場合に通報を発出することをコンピュータに実行させるプログラム命令と、当該の規則に関するヒットの集合体を提供することをコンピュータに実行させるプログラム命令とを有する。

【００１３】

本発明は、多くの利点を有するとともに、従来システムの多くの欠点を克服するものである。本発明の前記及びその他の対象物、特徴及び利点は、実施形態の詳細な記述及びそれに付属する図面から明らかとなる。また、以上の全体的な記述と以下の詳細な記述の両方は例であって、本発明の範囲を制限するものではないことを理解されたい。ここで、本発明のその他の多くの対象物、特徴及び利点は、添付図面と関連して以下の詳細な記述を読めば明らかとなる。

【図面の簡単な説明】

【００１４】

【図１Ａ】本発明の一つの実施形態にもとづくプロセスフローのフローチャート

【図１Ｂ】本発明の一つの実施形態にもとづくプロセスフローのフローチャート

【図２】本発明の一つの実施形態にもとづくイベントを既知のユーザと関連付けるプロセス

【図３】本発明の一つの実施形態にもとづくイベント構文解析のために使用されるＸＭＬ定義例

【図４】本発明の一つの実施形態にもとづく悪用検知のフローチャート

【図５】監視システムの一つ以上の特徴を実現するために使用される、ネットワークと接続された汎用コンピュータシステム

【図６】本発明の別の実施形態にもとづく悪用又は乱用検知プロセスのフローチャート

【図７】図６のプロセスを利用するシステムのユーザインタフェース

【図８】本発明の別の実施形態におけるログ監査にもとづき様々な悪用又は乱用シナリオを検知するためのフローチャート

【図９】本発明の別の実施形態におけるログ監査と患者データの選定にもとづく様々な悪用又は乱用シナリオを検知するためのフローチャート

【図１０】本発明の別の実施形態におけるログ監査とユーザデータの選定にもとづく様々な悪用又は乱用シナリオを検知するためのフローチャート

【発明を実施するための形態】

【００１５】

図１Ａと１Ｂは、共に本発明の一つの実施形態にもとづく幾つかのプロセスを示すフローチャートを図示している。ステップ１００では、本発明が規定する監視システムが、イベントログファイル（以降、イベントログと呼ぶ）にアクセスしている。一つの実施形態において、イベントログは、既知のユーザと関連する、イベントを含む記録データであり、本システムを介してネットワーク上のサーバ及び機器からアクセスされる。本発明の代替実施形態において、一時記憶装置がイベントログを保持することができる。別の実施形態において、プロトコル及びメッセージセットを介して監視システムにイベントログを送ることができる。監視システムは、サーバからのアクセス又はメッセージを介した受信によって、既知のユーザ又はシステムが識別子を取り出すことが可能なユーザと関連するイベントログにアクセスする。

【００１６】

一つの実施形態において、イベントログは、アプリケーション及びアクセスレイヤ機器によって記録されたトランザクション及び／又はアクティビティの記録の集合体である。一つの実施形態において、それらには、ＶＰＮ機器、サードパーティのアプリケーション、インハウスのアプリケーション、Ｗｅｂサーバ、シングルサインオンサーバ、データベース、電子メールサーバ、プリンタサーバ、ファックスサーバ、電話サーバ、並びに既知のユーザによる組織の情報システムの使用又は対話にもとづくイベント情報を含む、或いは生成するその他の機器又はサーバなどのサーバ及びアプリケーションが含まれる。監視システムは、周期的に実施するか、或いはイベントの発生に合わせてリアルタイムに実行するように、イベントログからデータを収集するスケジュールを立てる。

【００１７】

一つの実施形態において、監視システムは、オペレーション１０５で、例えば、構文解析エンジンを用いて、イベントログに含まれるイベントを抽出することができる。一つの実施形態において、構文解析エンジンは、例えば、ＸＭＬテンプレートを用いて、コンフィギュレーション可能なアプリケーションである。一つの実施形態において、構文解析エンジンは、（既知のイベントに関する標準フォーマットの例としての）既知のイベントログ及びイベントのＸＭＬテンプレートを有する。ＸＭＬテンプレートは、イベントとイベントログ間の関係を識別する情報を含むこともでき、更に、次の分析、保存及び報告のためにイベントから抽出すべき情報を含むことができる。例えば、ＸＭＬテンプレートは、イベントログに含まれるデータのフォーマットを有し、そのためＸＭＬテンプレート情報にもとづきイベントログのデータを既知のフィールドと容易に関連付けることが可能である。当業者は、ＸＭＬテンプレートがそのようなテンプレートの一つの実施形態であることを分かっており、当業者が認識する通り、それ以外の同様のテンプレート又はマッピング技法を使用することも可能である。従来遭遇しなかったイベントデータフォーマットに関して、構文解析エンジンは、デフォルトのＸＭＬテンプレートを手動で定義及び操作して、それに適したＸＭＬテンプレートを生成するように構成するか、或いはグラフィカルユーザインタフェースによるツールを用いて、当業者が理解できる形でイベントフォーマットを定義するように構成することができる。

【００１８】

一つの実施形態において、オペレーション１１０で、抽出したイベントを（例えば、前述したテンプレートを用いて）分析、保存及び報告に適したレコードに正規化する。正規化プロセスの一部として、イベントソース識別子（又はイベントログ識別子）、日時、ソースネットワークアドレス、デスティネーションネットワークアドレス、イベントと関連するテキスト及びトランザクションコードをレコードに配置することができる。ソース識別子にもとづき、正規化された標準レコードの一部とならないレコードに追加情報を保存することができる。例えば、そのようなレコードは、イベントをイベントソース識別子と関連付ける情報を含むことができる。当業者は、ここに列挙したフィールドが単なる例であることを分かっており、当業者は、様々な代替及び変化形態が有り、それらの全てが本発明の一部と考えられることを分かっている。

【００１９】

一つの実施形態において、オペレーション１１５で、正規化したイベントを所与の組織環境に対して定義された悪用シナリオに関して分析する。そのような分析の例には、保健医療、財務会計サービス又はモーゲージ環境に特有の形式のレコードへのアクセスの監視、或いは所定の時間期間に渡ってのトランザクション量の監視が含まれる。システムは、警報及びオフライン報告を発出することができる。この段階の分析は、速く検出することが有利なシナリオを分析することを特徴とする。悪用シナリオの分析は、以下において詳しく考察する。

【００２０】

一つの実施形態において、オペレーション１２０で、イベントを組織のシステムのユーザと関連付ける。一つの実施形態において、イベントレコードには、既知のユーザと関連する識別子が含まれる。以下において詳しく考察する通り、ユーザを識別するための識別子のリストは、データリポジトリ１２２に保存されているか、或いはアクセス可能である。そのような（イベントレコード内に見られる）相関識別子には、電子メールアドレス、ユーザＩＤ、データベースＩＤ、電話番号、セッションＩＤ、ＴＣＰ／ＩＰアドレス、ＭＡＣアドレス、シングルサインオンＩＤ又は所与の組織環境内のユーザとユニークに関連するその他のＩＤ（識別子）が含まれる。一つの実施形態において、そのような識別子を正規化したデータに置き換えて、正規化したデータを既知のユーザと関連付けることができる。監視システムは、識別子を用いて、正規化されたイベントを既知のユーザのデータベース、ディレクトリ又は共通のリポジトリ１２２と関連付けることができる。一つの実施形態において、既知のユーザに関して一致しない（例えば、リポジトリ１２２内の既知のユーザにもとづき識別することができないユーザの）イベントを別個のレコードリストに保持することができる。別の実施形態において、そのようなレコードを既知のユーザと照合する試みは、オフラインプロセスで実施することとして、時間的に後で行うか、或いは監視システムが未知のレコードの照合を開始するためのメッセージを送信することによって、ほぼリアルタイムで開始することができる。一つの実施形態において、監視システムは、それ自身のユーザリポジトリ１２２を保持することができる。別の実施形態において、監視システムは、識別子管理リポジトリ、シングルサインオンリポジトリ、人事リポジトリ、ＥＲＰ又は既知のユーザのその他のリポジトリと連携することが可能である。それに代わって、監視システムは、組織内のユーザ情報の別のリポジトリと連携する前に、先ずは自身のリポジトリ１２２をチェックする組み合わせたアプローチを採用することもできる。

【００２１】

一つの実施形態において、オペレーション１２５で、正規化され、関連付けられたイベントは、例えば、規則、アルゴリズム、データベースクエリ又はその他の手法を用いて、ユーザ固有の識別子又は職務／組織との関係にもとづきモデル化されたユーザ固有の悪用シナリオに関して分析される。一つの実施形態において、悪用シナリオをモデル化して、ＸＭＬテンプレートに保存することができる。例えば、監視システムは、悪用又は乱用シナリオが発生したか否かを決定するために照合するテンプレートを有する。悪用又は乱用シナリオの例は、更に詳しく考察する。

【００２２】

一つの実施形態において、オペレーション１３２で、正規化され、関連付けられたイベントは、次の分析及び報告のためにデータベース１３２に保存される。一つの実施形態において、ユーザと関連付けられないイベントは、別個のレコードリストに保持され、そのようなレコードを既知のユーザと照合する試みをオフラインプロセスで実施することができる。

【００２３】

一つの実施形態において、オペレーション１３５で、監視システムは、正規化され、関連付けられたイベントのオフラインデータベース１３２を、データ、時間又は性能の限界のためにリアルタイムで検出することができない悪用シナリオに関して分析する。そのようなオフライン分析が悪用シナリオを暴いた場合、監視システムは警報１３７を発出する

ことができる。そのような警報は、責任者に悪用又は乱用シナリオを捜査するように注意喚起する報告又はメッセージの形とすることができる。別の実施形態において、監視システムは、例えば、警報を発出させたアクティビティを起こした既知のユーザのアクセスを保留することによって、防止行動を開始することができる。別の実施形態において、オペレーション１４０で、本システムは、認証されたユーザによるトランザクション及びアクセスにもとづき、一般化されたセキュリティ報告を生成することができる。そのような報告は、組織のシステムのセキュリティを追跡するために使用するか、或いは悪用又は乱用シナリオが曝露された場合にそれに続く捜査のために使用することができる。

【００２４】

以下の記載は、前述したオペレーションの中の幾つかの特別な実施形態を記述している。本発明の特別な実施形態をここで考察し、添付した図面に図示するが、本発明は、ここで述べ、図示した特別な実体よりも広い範囲をカバーするものである。当業者が理解する通り、ここで述べた実施形態は、本発明の広い範囲の幾つかの例を提供するだけである。ここで述べた実施形態だけに本発明の範囲を限定する意図は無い。

１．イベントへのアクセス

一つの実施形態において、監視システムは、イベントを読み出す能力において柔軟である。一つの実施形態において、ネットワーク機器間での管理情報の交換を容易にするために、シンプルネットワークマネジメントプロトコロ（ＳＮＭＰ）などのアプリケーションレイヤプロトコルを使用することができる。監視システムは、ログファイルなどの所与のイベントソースへのプログラムによる入力（読み出し）アクセスを必要とするだけである。ログファイルの場合、ログファイルは、ローカルなハードディスクドライブ、ネットワーク上のハードディスクドライブを介してアクセス可能であるか、ｆｔｐなどのファイル転送プロトコルによりローカル上に転送するか、或いはその両方を行うことができる。一つの実施形態において、監視システムは、関連するイベントにアクセスするために、ＯＤＢＣなどのプロトコルを介してローカル又はリモートのデータベースからの読み出しに関しても十分に柔軟である。それに代わって、一つ以上のデータベースから系統的な抽出によりログファイルを生成した後、生成したログファイルをｆｔｐにより監視システムのローカルドライブに転送することができる。別の実施形態において、監視システムは、シンプルオブジェクトアクセスプロトコル（ＳＯＡＰ）などのメッセージプロトコルを用いて、イベントを受信するためのＷｅｂサービスインタフェースを備えることができる。前述した通り、監視システムは、全体として柔軟であり、イベントソースへのプログラムによるアクセス（読み出し）を採用している。

２．イベント内容及びフォーマット

一つの実施形態において、監視システムは、如何なるイベントログも処理することができる一方、（例えば、組織に知られた）既知のユーザによって直接的又は間接的に生成されたイベントを処理した後、それらのイベントを既知のユーザと関連付ける能力を有する。ユーザと関連するイベントに関して、追跡すべきイベントの一つの一般的なフォーマットを以下で略述する。当然のことながら、そのようなフォーマットは単なる例であると解釈すべきあり、当業者は、様々な代替及び変化形態が有り、それらの全てが本発明の一部として考えられると理解している。一つの一般的なフォーマットには、［日時スタンプ］、［ユーザ識別子］、［トランザクションタイプ］、「イベントテキスト」、［リクエストアドレス］、［ターゲットアドレス］、［ステータスコード］、［その他のデータ］が含まれる。これら以外のフォーマットも考えられる。

【００２５】

当業者が理解する通り、イベント当りの行数、フィールドの順序、デリミタ、フィールドフォーマット等は、アプリケーション、アクセスサーバ、データベース等毎に変化する。監視システムは、様々なイベントの取り扱いに関して十分にコンフィギュレーション可能である。「ユーザ識別子」フィールドは、ユーザＩＤ、電子メールアドレス、電話番号、データベースＩＤ、シングルサインオンＩＤ、ＴＣＰ／ＩＰアドレス、ＭＡＣアドレス、セッションＩＤ又はイベントを既知のユーザと関連付けるその他の識別子とすることが

できる。識別子が適用可能であるかは、ユーザＩＤポリシー、アプリケーション環境、ネットワーク配置等を含む組織の環境に依存する。監視システムは、そのような変数に関してイベントを既知のユーザと関連付けることができることに関して十分にコンフィギュレーション可能である。

３．イベントの定義

一つの実施形態において、監視システムは、前述したイベントを処理する能力に関して柔軟である。一つの実施形態において、本システムは、フィールド、フィールドの順序、フィールドのデリミタ、イベント当りの行数、文字数、フィールドタイプ、話し言葉タイプなどの所与のイベントタイプの変数を規定するために使用するＸＭＬベースの記述言語を有する。同様に、（ログファイルなどの）所与のイベントソース内に複数のイベントタイプを記述することもできる。一つの実施形態において、（ディレクトリ内に定義が有る）所与のイベントタイプを処理する際に何時でも使用することができるように、イベントタイプの定義を監視システムの既知のディレクトリに保持することができる。

４．システムデータベーススキーム

一つの実施形態において、監視システムは、処理するイベントタイプに対応する一連のスキームを有する。そのようなスキームは、データベーステーブルを生成するために使用することができる。例えば、「ｈｔｔｐ共通ログフォーマット」は、監視システムが保持し、「ｈｔｔｐ共通ログフォーマット」タイプのイベントを処理する際に何時でも共通して再利用することができる予め定義されたスキームを有する。別の実施形態において、監視システムは、特定のイベントタイプにユニークなフィールドをイベントの保存フォーマットと関連付けるためのスキームを使用する能力を備えている。言い換えると、本システムは、前述した標準フォーマットの一部ではないイベントフィールドの取り扱いに関して十分にコンフィギュレーション可能である。例えば、キーワード又は或る英数字列にもとづくプログラム論理をイベントデータレコード内のフィールドを識別するために使用して、正規化されたレコードの標準保存フォーマットと関連付けることができる。

【００２６】

一つの実施形態において、監視システムは、前述した通り多くの使用可能なフィールドをここで定義したスキームとテーブルにマッピングすることと、イベント特有のフィールドをイベントタイプ特有のスキームで記述されたテーブルとフィールドにマッピングすることとによって、イベントを正規化する。別の実施形態において、監視システムは、処理してシステムのデータベースに保存するイベント毎にユニークな識別子を生成して、次の索引付け、相関及び報告のために使用することができる。一つの実施形態において、好適に索引付けされたフィールドは、保存データへのアクセス、報告の生成及びイベントの処理の際に効率を向上させることが可能なスキーム定義の一部である。正規化されたイベントは、一般的にイベントレコードに含まれるデータと同じデータを含むが、データベース用にフォーマット及び索引付けすることができる。

【００２７】

一つの実施形態において、監視システムは、（データベース１３２内に）組織の既知のユーザ及び関連する識別子に対応するテーブルを保持する。一つの実施形態において、監視システムは、ユーザ及び識別子の保持のために既存の識別子管理システムを発展させることに関して十分に柔軟である。そのようなシステムには、コンピュータアソシエイツ、ＢＭＣ、サン、ＩＢＭ、ノーベルなどのベンダーによるアクティブディレクトリ又は識別子管理システムなどのディレクトリが含まれる。一般的に、本システムは、如何なる種類の既存の識別子ソースの発展及びリポジトリ内での識別子自体の保持に関して十分に柔軟である。

５．既知のユーザとの関連付け

一つの実施形態において、監視システムは、イベントを処理する際に、システムの処理環境及びアプリケーションに依存して、イベントを既知のユーザとリアルタイムで関連付けることに関して柔軟である。別の実施形態において、本システムは、オフラインプロセスの間にイベントを既知のユーザと関連付けることができる。両方の場合の結果において

、本システムが処理するイベントは、組織の既知のユーザと関連付けられて、ここで考察している通り、セキュリティ報告、悪用検知、監視等のために使用される。

【００２８】

本発明の一つの実施形態において、図２は、イベント２１０を既知のユーザのレコード２０５と関連付けるプロセスの図面を図示している。監視システムは、前に略述した一般的なプロセスによって、正規化されたイベント２１０を生成している。一つの実施形態において、正規化されたイベント２１０は、一つ以上のユーザ識別子を含むことができ、その例として、電子メールアドレス、ユーザＩＤ、データベースＩＤ、電話番号、ＴＣＰ／ＩＰアドレス、ＭＡＣアドレス、シングルサインオンＩＤ、セッションＩＤ又は組織環境を与えられたユーザとユニークに関連付けることが可能なその他のＩＤが含まれる。

【００２９】

一つの実施形態において、本システムは、ユーザ及び既知のユーザのレコード２０５に例が図示されている関連する識別子のディレクトリ、データベース又はその他のリポジトリ１２２にアクセスする。そのため、図２に図示されている通り、特別なユーザを広範囲の識別子と関連付けることができる。そのような識別子の中の幾つかは持続的に保持される一方、セッションＩＤなどのその他の識別子は、ユーザ特有のセッションが存在するか、或いは直前に生成されていた間の短期間しか保持されない。同様に、例えば、ユーザが複数の電子メールアドレス又は複数の電話番号を持っている場合に、特定のタイプの識別子の異なる変化形態を保持して、それらの全てをユーザリポジトリ１２２内に保存することもできる。

【００３０】

本発明の一つの実施形態において、監視システムは、一致した識別子にもとづきイベント２１０を既知のユーザのレコード２０５と関連付ける。本発明の一つの実施形態において、イベント２１０とユーザレコード２０５は、正規化され、関連付けられたイベントを含むリポジトリ１３２内で互いに連携させることができる。セッションＩＤ及び同様の一時的な識別子は、イベントレコードから収集して、たとえイベント２１０がイベント２１０を既知のユーザのレコード２０５と直接連携させるための識別子を持っていなくとも、イベント２１０が既知のユーザのレコード２０５と関連付けられているように保持することができる。そのような一時的な識別子は、ユーザリポジトリ１２２又はユーザリポジトリ１２２内の既知のユーザのレコードと逆向きに連携させることが可能なその他のリポジトリ内のレコードとして保持することができる。このフローの或る時点において、（一時的なＩＤの例としての）セッションＩＤを或るログイベントのユーザと連携させるべきである。例えば、ＶＰＮは、典型的には、ユーザログインイベントと関連してセッションＩＤを生成し、それに続いてそのユーザと関連するイベントにセッションＩＤの「ログを取る」だけである。しかし、監視システムは、初期のユーザログインイベントにもとづきセッションＩＤを追跡して、イベントログのセッションＩＤのみによって識別されるユーザのアクティビティをその特定の既知のユーザに関連付けて追跡することができる。

【００３１】

本発明の別の実施形態において、ユーザレコードと関連付けられないイベントは、報告と追加処理を可能とする特別なテーブルの下でデータベースに保存することができる。

【００３２】

本発明の一つの実施形態において、図３は、イベント構文解析に使用されるＸＭＬ定義３０１の例を図示している。

【００３３】

本発明の一つの実施形態において、悪用及び／又は乱用の検知は、関連付けられなかったイベントの分析により実施することができる。幾つかの悪用及び乱用シナリオは、イベントとユーザとの関連付けの前に検知することができる。それによって、監視システムが、組織のリソースを監視して、特定のユーザが怪しいと特定される前に、高いリスクと考えられる挙動を一般的に検知することが可能となる。例えば、監視システムは、次の手法の幾つかを用いて、警報及び警報レコードを発出することができる。

・或るユーザ又は特定のカテゴリのユーザが、所定の時間間隔に渡って或る量のトランザクション又はアクティビティを実施する場合、
・或るユーザ又は特定のカテゴリのユーザが、予め定義された順番のトランザクション又はアクティビティを実施する場合、
・或るユーザ又は特定のカテゴリのユーザが、一日の中の予め定義された時間外にリソースにアクセスする場合、
・或るユーザ又は特定のカテゴリのユーザが、データベースフィールド、ファイル、アプリケーションフィールドなどの予め定められたリソースを変更、或いはそのようなリソースにアクセスする場合、
・或るユーザ又は特定のカテゴリのユーザが、病院に登録された有名人と関連するレコードや特定の顧客又はパートナーに対応するレコードなどの予め定められたエンティティと関連するリソースを変更、或いはそのようなリソースにアクセスする場合。

【００３４】

本発明の別の実施形態において、悪用及び／又は乱用の検知は、関連付けられたイベントの分析により実施される。幾つかの悪用及び乱用シナリオは、イベントがユーザと関連付けられた場合に検知することができる。例えば、監視システムは、次の手法の幾つかを用いて、警報及び警報レコードを発出することができる。
・或るユーザが、その組織との関係（職能、サプライヤとの関係、顧客との関係など）の予め定義された特性外のアクティビティ又はトランザクションを実行する場合、
・或るユーザが、そのユーザの行ってきた挙動の履歴（又はそのユーザが属するユーザカテゴリ）と整合しないアクティビティ又はトランザクションを実行する場合、
・予め定められたユーザが予め定義されたアクティビティ、トランザクションを実施するか、或いはシステムにアクセスする場合、
・或るユーザが過去のアクセスと整合しないアドレス（ＴＣＰ／ＩＰ、ＭＡＣ、ドメイン等）からリソースにアクセスする場合、
・或るユーザが、そのユーザを前に怪しいと判断されたユーザと関連付けるアクティビティ又はトランザクションを実施する場合。

【００３５】

業務情報システムの悪用の例

業務情報システムの悪用は、多くの形態を取り、異なる複雑な関係者及び技法と関連する。一つの実施形態において、監視システムは、特定の形態の悪用に適用するか、或いは複雑な形態の悪用に対する一般的なプラットフォームとして使用することができる。一つの実施形態において、監視システムは、組織の既知のユーザ（又はユーザ識別子）と関連して実施される悪用に関する監視、報告、事故調査を実施することができる。そのような悪用シナリオは、最新の形式のファイヤウォール、侵入検知及び防止、認証／許可技法を用いても検出することができない場合が有る。そのようなシナリオは単なる例であり、当業者は様々な代替及び変化形態が有ることを認識しており、それらの全ては本発明の一部と考えられることに留意されたい。

１．顧客レコードの販売

多くの産業において、顧客情報は金になる情報である。長期保健医療、モーゲージ、高額財務サービスは、何れも従業員、パートナー、サプライヤ及びその他の既知のエンティティが既知のユーザＩＤを用いてアプリケーション、データベース等にアクセスする産業の例である。悪意のユーザは、そのような情報を競争相手又はその他の業者に売り渡す場合が有る。本発明の一つの実施形態において、監視システムは、乱用状況が起こっているのかを、例えば、営業マンがその得意先の何れとも関連しない情報にアクセスしているのかを事前に決定するために、如何なるユーザが如何なる顧客データにアクセスしているのかを追跡することができる。

２．保護されている健康情報の許可されない開示

保健医療分野において、保護されている健康情報（ＰＨＩ）へのアクセスは、法律によって保護されている。一般的にシステムにアクセスする人は、ＰＨＩにアクセスして、第

三者と協力して、犠牲者を恐喝する、或いは法律で保護されている機密情報を見るために、隣人、関係者、仕事仲間、有名人又は責任者に関するＰＨＩを取得することができる。医療での悪用も一般的な行為となっており、嘘の、或いは大げさな要求を共謀して出してくる共犯者一味を巻き込んでいる場合が有る。そのようなスキームでは、既知のユーザ／信頼されたユーザに医療提供者内のシステムを騙すように要求して来る。本発明の一つの実施形態において、監視システムは、如何なるユーザが有名な患者に関するデータにアクセスしているのかを精密に追跡するか、或いはユーザグループが一人以上の患者に関するデータにアクセスして、アクセスしたデータを組み合わせて乱用する可能性が有るのかを追跡することができる。

３．注文の宛先住所の変更

電子的に注文を処理する組織では、従業員などの既存のユーザが「宛先」住所を変更する場合が有る。その場合、従業員は、従業員が注文品を横取りして注文品を公開市場で売りさばくための宛先に住所を変更する可能性が有る。典型的には、そのような悪用行為は、本来の購入者が請求に対する支払いを拒否するか、或いは注文が届かなかったと苦情を言って来るまで検知されない。一つの実施形態において、監視システムは、如何なるユーザが宛先住所を変更しているのか、或いはユーザが通常通り宛先住所を変更しているのかを追跡することができる。従来技術を用いてイベントをトランザクションと関連付けるには、多くの時間がかかる。

４．退社する従業員による顧客データベースの略取

退社する営業マンが顧客データベース及び有望な販売ルートの電子コピー又は印刷したコピーを取得することが良く知られている。彼らは、そのようなデータを競争会社と関係する新しい職場で使用する可能性が有る。本発明の一つの実施形態において、システムは、報告及び一般的な検知能力を提供し、アプリケーション及びデータベースアクティビティを調査対象のユーザと関連付けることができる。本発明の一つの実施形態において、監視システムは、営業マンが比較的大量の営業レコードにアクセスしているか否か、或いは営業マンがその営業マンと関係のない顧客のレコードにアクセスしているか否かを追跡することができる。

５．会社のエクストラネット又はＶＰＮを介した認証の弱点の乱用

会社のエクストラネット又はＶＰＮは、最も一般的にはユーザＩＤとパスワードにより認証されている。会社のパートナーとして、既知のユーザが価格表、在庫状況、商品保管庫の住所、販売促進策等の機密情報にアクセスする場合が有る。ユーザが「パートナー」会社から退社して、競争会社に転職した場合、そのユーザは、依然として同じユーザＩＤとパスワードを使用して、機密情報に自由にアクセスすることができる。本発明の一つの実施形態において、監視システムは、ユーザＩＤを特定のＩＰアドレス（又はドメイン）と関連付けて、そのＩＰアドレス又はドメインが競争相手又はパートナー会社でないエンティティのものである場合に警報を発出することができる。

６．債券トレーダーの否認防止

債券トレーダーは、多くの場合マーケットの動きを期待して思惑で有価証券を購入する。マーケットが期待しなかった動きをする事象では、債券トレーダーは電子的な注文の指標を否認する場合が有る。本発明の一つの実施形態において、電子的なトランザクションの指標及びステージを既知のユーザ（トレーダー）と関連付けて、そのようなトレーダーによる悪意の要求を拒否することができる。

７．金融インサイダー取引団

インサイダー取引団は、アプリケーション、電子メール、電話、ファックスを含む様々な電子システムを利用する多くの協力者から構成される。本発明の一つの実施形態において、監視システムは、怪しい挙動を検知するために使用するか、或いは全ての共謀者を特定するための事件の捜査に使用することができる。典型的なシナリオは、一人の構成員が何らかの電子的な手段により外部ソースから「内部情報」を受信することである。次に、第一の情報源が、別の構成員と協力して、不正に取得した情報にもとづき不法な利得を生み出す取引を行う。本発明の一つの実施形態において、監視システムは、従来のインサイ

ダー取引検知方法を用いて実現可能であった段階よりも大幅に早い段階でそのようなアクティビティを検知することができる。

８．Ｗｅｂサービス

業務情報システムは、多くの場合Ｗｅｂサービスとして公開されている。認証及び許可標準が確立している一方、従来システムを悩ましている同じ悪意のユーザが多くの場合公開されているＷｅｂサービスを利用する。本発明の一つの実施形態において、システムは、報告及び一般的な検知能力を備えており、アプリケーション及びデータベースアクティビティを調査対象のユーザと関連付けることができる。

【００３６】

本発明の一つの実施形態において、図４は、退社する従業員のアクティビティにもとづき乱用を検知するために監視システムを使用する際のオペレーションを図示している。一つのシナリオ例において、組織の従業員である営業マンが競争会社の同様の地位を受けていたとする。その従業員は、組織に退社する意志を通報せず、通常通り働き続けている。その従業員は、次の職場で新たなビジネスの助けになる出来るだけ多くの情報源を集めることを決心している。

１．顧客及び見込み客のレコードへのアクセス

従業員は、その職務の一部として、組織の顧客及び見込み客に関する詳細な情報にアクセスする。顧客及び見込み客のレコードは、組織のＶＰＮ及びエクストラネットを介して利用可能なＣＲＭ（カスタマ・リレーションシップ・マネッジメント）アプリケーションに保持されている。ＣＲＭアプリケーションは、レコードへのアクセスを「レコードの所有者」のみに制限するための特権管理システムを有する。しかし、営業及び支援プロセスの協力し合う特性のために、そのような特徴はめったに使われず、全ての従業員が全てのレコードにアクセスしている。

２．リモートによるデータ略取

組織と活発に関係している顧客及び見込み客に関する詳細を知ることは、次の職場での時間の節約と新たなビジネスを作り出す際に有益である。従業員は、オペレーション４０５で会社のＶＰＮを介してＣＲＭアプリケーションにアクセスし、オペレーション４１０で組織の顧客及び見込み客のデータを略取することを決心する。従業員の職場は、組織の本社から離れた遠隔の職場に有り、そのため従業員は、楽に午前中全部を使ってＣＲＭシステムにアクセスし、１２５以上の顧客及び見込み客レコードを電子的に略取することができる。次に、電子的に略取された顧客及び見込み客レコードは、個人的な「ホットメイル」の電子メールアカウントに転送される。従業員は、後で更に２００のレコードにアクセスするつもりでいた。

３．検知

本発明の一つの実施形態において、監視システムは、ＣＲＭ、ＶＰＮ及びインターネットプロキシログへのアクセスを監視するように構成されている。監視システムは、特定の時間期間（例えば、４時間）に５０以上の顧客及び見込み客レコードがアクセスされたイベントにおいて、セキュリティチームに警報を発出するように構成することができる。そのようにして、退社する従業員のアクティビティがオペレーション４１５でセキュリティ警報を発出させることとなる。

４．捜査

本発明の一つの実施形態において、監視システムは、オペレーション４２０と４２５で、警報が発出されると同時に科学的捜査を進める。セキュリティチームは、潜在的な事件の警報を受けると、過去３０日以降のＶＰＮ、ＣＲＭ及びインターネットプロキシのイベントを収集した報告を監視システムから取得する。一つの実施形態において、セキュリティチームは、そのような報告から、従業員が会社のＶＰＮを介してリモートで１２５の顧客及び見込み客レコードにアクセスしたことと、従業員が同じ期間中にホットメイルアカウントに一連の電子メールも送信していたこととを確認することができる。一つの実施形態において、そのような分析は、悪用／乱用状況が検知されたことを確認するために、自動的な規則を用いて実施することができる。

【００３７】
本発明の一つの実施形態において、次に、セキュリティチームは、そのような情報又は自動警報を組織の人事部に転送することができる。次に、オペレーション４３０において、組織は、そのような事実を従業員に突きつけて、将来的な損害を限定するとともに、組織が説明した上で従業員の分離を行うことが可能である。それに代わって、監視システムは、従業員による組織のシステムへのアクセスを自動的に無効化又は保留して、従業員による状況を更に評価する前に更なる損害を防止することができる。
【００３８】
本発明の一つの実施形態において、図５は、コンピュータ網などの汎用電子ネットワーク１０を介して接続されたコンピュータシステムのコンポーネントを図示している。コンピュータ網１０は、インターネットなどのバーチャルプライベートネットワーク又は公衆網である。図５に図示されている通り、コンピュータシステム１２は、システムメモリ１８と接続された中央処理装置（ＣＰＵ）１４を有する。システムメモリ１８には、オペレーティングシステム１６、ＢＩＯＳドライバ２２、アプリケーションプログラム２０が保存されている。更に、コンピュータシステム１２、マウス、キーボード３２などの入力機器２４と、プリンタ３０、ディスプレイモニタ２８などの出力機器と、データベース２１などのパーマネントデータ記憶装置を有する。コンピュータシステム１２は、電子ネットワーク１０と通信するために、イーサネットカードなどの通信インタフェース２６を有する。別のコンピュータシステム１３と１３Ａも、ワイドエリアネットワーク（ＷＡＮ）又はインターネットなどの相互接続網として実現することが可能な電子ネットワーク１０と接続することができる。
【００３９】
一つの実施形態において、コンピュータシステム１２は、図１～４と関連して、ここで考察しているロジック及びモジュールを実装したプログラムコードを含む、監視システム又はここで考察している構成部分を実装した監視サーバ５０を有する。当業者は、そのようなコンピュータシステムが、図１～４と関連して、ここで考察しているプロセスを実施するように論理的に構成、プログラミングすることが可能であることを理解している。その他の多くの同様の構成が当業者の考え得る範囲内に有り、そのような如何なる構成も本発明による方法及びシステムにおいて使用可能であると考えられることを理解されたい。更に、ここで考察している本発明による方法の或る実施形態の工程を実施するように、ネットワーク化されたコンピュータシステムをプログラミング、構成することは、当業者の考え得る範囲内に有ると理解されたい。
【００４０】
一つの実施形態において、監視サーバ５０は、コンピュータユーザに対応するデータを提供するユーザ識別子モジュール５１と、悪用検知情報及び乱用検知情報を提供するモデル化データ提供モジュール５２と、アプリケーションレイヤデータとコンピュータユーザと関連するトランザクション及びアクティビティに対応するデータを提供するデータ捕捉モジュール５３と、アプリケーションレイヤデータとコンピュータユーザと関連するトランザクション及びアクティビティに対応するデータを抽出する構文解析エンジン５４と、構文解析エンジンによって抽出されたデータを正規化する正規化エンジン５５と、正規化されたデータを関連付ける相関モジュール５６と、関連付けた情報とモデル化データを分析する分析モジュール５７と、関連付けた情報が悪用検知情報と乱用検知情報の中の少なくとも一つに対応するか否かを決定する決定モジュール５８と、コンピュータユーザ識別子、各コンピュータユーザと関連する予め定義された職務及びコンピュータユーザに対して規定された予め定義された関係の中の一つ以上にもとづきユーザ特有の悪用検知情報に関して関連付けた情報を分析するユーザ別分析モジュール５９と、警報を発出する警報発生モジュール６０とを有する。より多い数又はより少ない数のモジュールも使用可能であることが容易に分かる。当業者は、本発明が個々のモジュール、二つ以上の前述した別個のモジュールの特徴を統合した単一のモジュール、個々のソフトウェアプログラム及び単一のソフトウェアプログラムの中の一つ以上を用いて実現可能であることを容易に理解し

ている。

【００４１】

本発明の一つの実施形態において、図６は、医療保険の相互運用性と説明責任に関する法律（ＨＩＰＡＡ）の違反、識別子の窃盗、保険証番号の窃盗などのデータの悪用又は乱用に関する事件の自動的な検知を可能とする規則エンジン又はプロセス６００を図示している。そのような規則は、当該データと関連するトランザクション及び／又はアクティビティ、例えば、データを保存しているシステムのユーザ又は非ユーザによるデータへのアクセスを監視することができる。プロセス６００は、当該データを有する一つ以上のデータベースを含むコンピュータ環境でのデータと関連するトランザクション及び／又はアクティビティから起こる事象を捕捉、構文解析、相関、正規化、分析及び決定するための様々なモジュールを有する、システム１２と関連して前述したコンポーネントの中の一つ以上を利用することができる。規則エンジン６００は、特定のタイプのコンピュータ環境又はデータ、或いは特定のタイプのデータの悪用又は乱用に限定することを意図するものではない。しかし、データタイプ及びデータの悪用又は乱用タイプの少なくとも一部は、データ又はコンピュータ環境と関連するトランザクション及び／又はアクティビティを監視するための規則の一つ以上の判断基準のベースとすることができる。

【００４２】

ステップ６０５において、規則は、ユーザ及び／又は特定のタイプのデータの悪用又は乱用に関する特別な知識を有するコンサルタントなどの第三者によって生成される。そのような規則は、悪用事件及び乱用事件の定義及び／又は検知のためのアルゴリズム、データベースクエリ及びデータ分析方法の中の一つ以上を含むことができる。そのような規則の生成又は制定のために様々な判断基準を使用することができる。そのような判断基準は、データの悪用又は乱用を示すトランザクション及び／又はアクティビティと関連付けることができる。例えば、プロセス６００は、次のパラメータの中の一つ以上にもとづき規則を制定又は生成することができる。

・データ範囲や使い易い時間設定、例えば、昨日、先月、前の四半期などのタイムフレーム判断基準を利用することができる。

・発見したイベント数にもとづく数量閾値判断基準を利用することができる。数量閾値判断基準は、タイムフレーム判断基準と関連して使用することができる。

・ユーザにイベントソースの選定を可能とし、次に、ユーザに一つのフィールドとそのフィールド値の選定を可能とするフィールド値照合判断基準を利用することができる。

・ユーザにカテゴリと照合パターンの選択を可能とする分類別フィールド値照合判断基準を利用することができる。

・ユーザに全ての利用可能なアプリケーションを通じて検索するための共通ユーザ名の選定を可能とする共通ユーザ名照合判断基準を利用することができる。共通ユーザ名照合判断基準は、各アプリケーション用のユーザデータが取り込まれる場所に実装することができる。

【００４３】

また、ステップ６０５では、ユーザは、規則が起動された際に使用することができる通報又は警報に関する判断基準を指定することが可能である。一つの実施形態において、規則が起動されとことを通報すべきエンティティの電子メールアドレスを指定することができる。プロセス６００は、警報に関する初期値として、規則制定者の電子メールアドレスを使用することができる。一つの実施形態において、ユーザが如何なる規則が起動されたのかが分かるように電子メールで送信すべきテキストや提供可能な特定の情報などの通報の形式を指定することができる。

【００４４】

本規則の範囲には、単一システム内での一致の発見などの単一のイベントソースを含めることができる。例えば、単一イベントソースの規則は、タイムフレーム及び／又は数量閾値判断基準によるパターン照合を許容するものである。別の例として、規則は、所定の時間間隔に渡っての所定の数の医療レコードへのアクセスが行われた時点を決定すること

ができる。そのような挙動は、保険証番号の窃盗を示す場合が有る。本規則の範囲には、複数のシステムに渡る一致の発見などの複数のイベントソース規則を含めることができる。例えば、複数のイベントソースの規則は、共通ユーザ名又は特定のデータカテゴリへのアクセスを監視することができる。

【００４５】

ステップ６１０において、プロセス６００がリアルタイムによる事件の検知を実施するのか否かを決定することができる。リアルタイムによる事件の検知は、各イベントが読み出される毎に、かつデータベースに挿入される前に、規則を処理するものである。プロセス６００は、リアルタイムによる事件の検知をステップ６００で制定された規則の中の幾つか、ほとんど又は全部に適用することができる。

【００４６】

ステップ６１５において、リアルタイムによる事件の検知に依存しない規則に対して、プロセススケジュールを立てることができる。そのようなスケジュールは、時間で区切るか、システムアクティビティなどのスケジュールを決定するためのその他の要因を利用するか、或いはその両方とすることができる。特定のスケジュールを規則の判断基準と関連付けることができる。例えば、所定の時間間隔に渡って所定の量の医療レコードへのアクセスを監視するための規則のスケジュールを所定の時間周期で処理されるように立てることができる。そのような規則のスケジューリングに使用することができるアプリケーションの例は、クオーツである。

【００４７】

本開示は、規則の調整可能又は動的なスケジューリングも考慮している。ユーザは、規則のスケジューリングのために、一つ以上の判断基準を指定することができ、スケジュールを立てて、後で一つ以上の判断基準にもとづき自動的に調整することができる。例えば、システムアクティビティやアクセス可能なデータ量などの要因にもとづき、同じ規則の処理間の時間間隔を調整することができる。

【００４８】

ステップ６２０において、規則を実行又は処理することができる。一つ以上の一致を発見するための規則は、図５と関連して前述したシステム１２のデータベースなどにおいて、規則のヒット又は起動を表すデータベースエントリを生成することができる。そのようなヒットによって、ステップ６２５での通り、通報又は警報を発出して、指定された受信者に送信することができる。

【００４９】

警報又は通報の受信にもとづき、ユーザは、ステップ６３０での通り、起動された規則又は複数の規則に付随する追加情報のために、システム１２にアクセスすることができる。そのような追加情報は、規則が起動された特定の時間と、規則が起動されたその他の時間の全てを提供することができる。ユーザが、システム１２にアクセスした際にヒットに付随する関連情報に直結できるように、特定のリンクを通報又は警報に配備することができる。

【００５０】

本発明の一つの実施形態において、図７は、規則プロセス６００に関するユーザインタフェース７００を図示している。規則管理ページ又はウィンドウ７０５は、定義された規則の全てをユーザに提示することができる。ユーザは、規則の制定、修正又は削除のために、規則管理ページ７０５を使用することもできる。新しい規則を定義するための情報を入力するのに、規則定義ページ又はウィンドウ７１０を使用することもできる。規則スケジュール管理ページ又はウィンドウは、規則のスケジュールの全てをユーザに提示することができる。規則スケジュール管理ページ７１５は、新しい規則の制定、既存のスケジュールの修正及びスケジュールの削除の中の一つ以上のために使用することもできる。規則を起動するスケジュールを定義するために、規則スケジュール定義ページ又はウィンドウ７２０を使用することができる。

【００５１】

規則ヒット管理ページ又はウィンドウ７２５は、一致した全ての規則及び規則毎の一致数をユーザに提示することができる。規則ヒット要約スクリーン又はウィンドウ７３０は、特定の規則のヒットに関するデータベースへの全てのエントリをユーザに提示することができる。規則ヒット要約スクリーン７３０は、規則が起動された日と、その規則を起動させた実際のイベントを表示することができる。規則ヒットイベントスクリーン又はウィンドウ７３５は、規則を起動させた一つ以上のイベントをユーザに提示することができる。これらのページ又はウィンドウ間及びそれらのページ又はウィンドウ上の情報間の操作は、プルダウンメニューや新しいウィンドウなどの様々な技法により行うことができる。本開示は、前述した各機能に対して同じウィンドウを使用することも考慮している。

【００５２】

図８と関連して、システム１２又はそのモジュールは、様々な悪用又は乱用シナリオを検知するために、監査ログ１１００と組み合わせて使用することができる。例えば、従業員の自己評価、家族構成員の調査、ＶＩＰの調査、患者である仕事仲間の調査、その他家族全体の調査（隣人等）を検知するために、前述した様々な判断基準にもとづき監査ログ１１００を分析することができる。そのような判断基準に、大量の請求書／連絡先の修正、大量のダウンロード／印刷機能、「非常事態」機能、タイムフレーム内での患者又はユーザに関する高いアクティビティレベル及び尋常でないログインアクティビティの中の一つ以上を含めることができる。当業者は、監査ログにもとづき悪用及び乱用を検知するために、その他の判断基準及びその他の判断基準の組み合わせを使用することができる。

【００５３】

図９と関連して、システム１２又はそのモジュールは、様々な悪用又は乱用シナリオを検知するために、監査ログ１１００と選定した患者データ１２００を組み合わせて使用することができる。例えば、一年以上前又はその他の特定の時間期間に退院した患者或いは通常は年に一度医者の所に来るが、突然年に２５回又はそれ以外の尋常でない回数医者の所に来る患者へのアクセスを含む判断基準にもとづき、監査ログ１１００と選定した患者データ１２００を分析することができる。

【００５４】

図１０と関連して、システム１２又はそのモジュールは、様々な悪用又は乱用シナリオを検知するために、監査ログ１１００と選定したユーザデータ１３００を組み合わせて使用することができる。例えば、遠隔の医師のスタッフがその医師の治療を受けていない患者にアクセスしたり、通常業務範囲外の患者にアクセスしたり、通常の勤務シフト外に患者にアクセスしたり、無給のユーザが給与機能にアクセスするなどを含む判断基準にもとづき、監査ログ１１００と選定したユーザデータ１３００を分析することができる。タイムフレーム内で非常に高いアクティビティレベルの患者、タイムフレーム内で非常に高いアクティビティレベルのユーザ、ログインセッションが異常に長いユーザ、ログイン失敗回数が非常に多いユーザ、血液型の変更などの特殊な機能を含むその他の判断基準を使用することもできる。

【００５５】

前に言及した通り、本発明の範囲内の実施形態には、コンピュータで実行可能な命令又はそこに保存されたデータ構造を持ち運ぶ、或いは保持するためのコンピュータで読み取り可能な媒体を有するプログラム製品が含まれる。そのようなコンピュータで読み取り可能な媒体は、汎用又は専用のコンピュータがアクセスすることができる入手可能な媒体とすることができる。例を挙げると、そのようなコンピュータで読み取り可能な媒体には、ＲＡＭ、ＲＯＭ、ＥＰＲＯＭ、ＥＥＰＲＯＭ、ＣＤ－ＲＯＭ又はその他の光学ディスク記憶装置、磁気ディスク記憶装置又はその他の磁気記憶装置、或いは汎用又は専用のコンピュータがアクセスすることができるコンピュータで実行可能な命令又はデータ構造の形式の所望のプログラムコードを持ち運ぶ、或いは保存するために使用可能なそれ以外の媒体が含まれる。ネットワーク又はその他の通信接続（有線、無線又は有線と無線の組合せのいずれか）を介してコンピュータに情報が伝送又は提供された場合、コンピュータが、そのような接続をコンピュータで読み取り可能な媒体として看做すのが正しい。従って、そ

のような接続をコンピュータで読み取り可能な媒体と呼ぶのが正しい。前記の組合せもコンピュータで読み取り可能な媒体の範囲内に含まれる。コンピュータで実行可能な命令には、例えば、汎用コンピュータ、専用コンピュータ又は専用処理装置に或る機能又は機能グループを実行させるための命令及びデータが含まれる。

【００５６】

一つの実施形態において、ネットワーク化された環境でコンピュータが実行するプログラムコードなどのコンピュータで実行可能な命令を含むプログラム製品によって実現される一般的な意味での操作ステップにより本発明を説明した。一般的に、プログラムコードには、特定のタスクを実行する、或いは特定の抽象データタイプを実装するルーチン、プログラム、オブジェクト、コンポーネント、データ構造等が含まれる。コンピュータで実行可能な命令、関連するデータ構造及びプログラムモジュールは、ここで開示した方法の工程を実行するためのプログラムコードの例を示している。そのような実行可能な命令又は関連するデータ構造の特定のシーケンスは、そのような工程に記述された機能を実現するための相応の操作の例を示すものである。

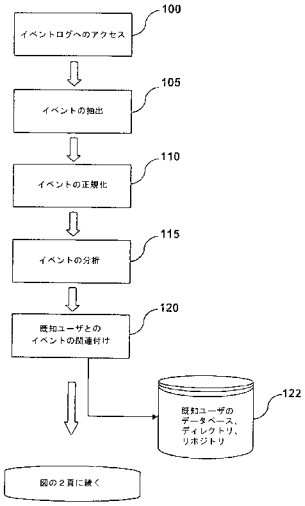
【００５７】

本発明は、幾つかの実施例において、プロセッサを備えた一つ以上のリモートコンピュータとの論理接続を用いるネットワーク化された環境で実施される。論理接続には、ローカルエリアネットワーク（ＬＡＮ）及びワイドエリアネットワーク（ＷＡＮ）が含まれるが、ここでは例示のために挙げており、それらに限定されるものではない。そのようなネットワーク環境は、事務所又は企業に跨がるコンピュータネットワーク、イントラネット及びインターネットにおいて一般的である。当業者は、そのようなネットワークコンピューティング環境が典型的にはパーソナルコンピュータ、ハンドヘルド機器、マルチプロセッサシステム、マイクロプロセッサベース又はプログラマブル家電製品、ネットワークＰＣ、ミニコンピュータ、メインフレームコンピュータ等を含む多くの形式のコンピュータシステム構成を包含するものであることが分かっている。本発明は、通信ネットワーク（有線接続、無線接続、或いは有線接続と無線接続の組合せ）を介して接続されたローカルとリモート処理装置がタスクを実行する分散コンピューティング環境においても実施することができる。分散コンピューティング環境においては、プログラムモジュールをローカルとリモートの両方の記憶装置に配置することができる。

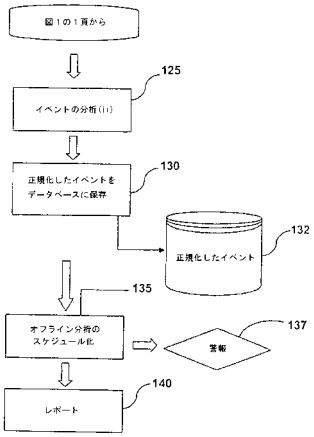
【００５８】

本発明の別の実施形態は、当業者がここに開示した本発明の明細書及び実際の形態を考慮することから明らかとなる。本明細書を例示としてのみ考え、本発明の真の範囲及び技術思想がここで開示した内容及びそれと同等物によって表されることも意図している。

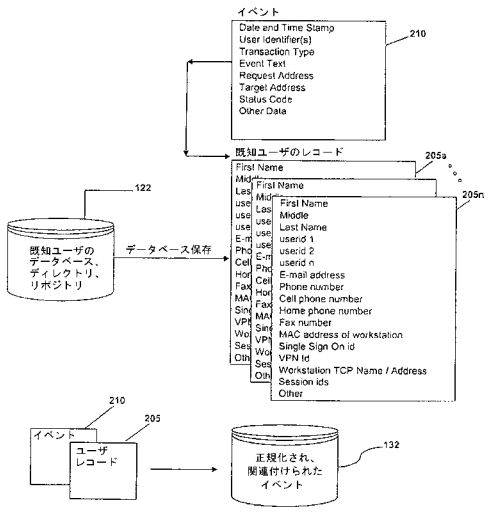
【図１Ａ】




【図１Ｂ】




【図２】



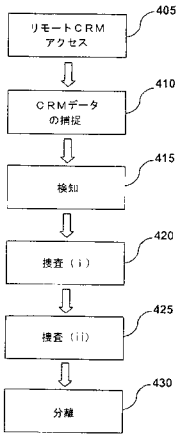

【図３】

Figure 3

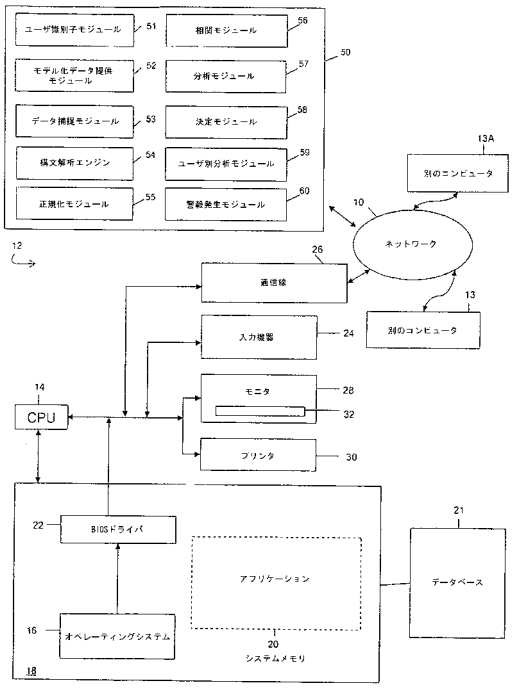
```
- <?xml version="1.0" encoding="UTF-8" ?>
- <LogFormatDefinition definitionName="SharePoint" compatibleWith="web">
- <event numLines="1">
- <timeStampFields>
  <numTSFields>2</numTSFields>
  <concatWith />
  <formatString>yyyy-mm-ddHH:mm:ss</formatString>
  <tsField>date</tsField>
  <tsField>time</tsField>
  </timeStampFields>
- <parseRules>
- <!-- rules for parsing whole lines of data like ignore rules -->
- <rule ruleType="ignore" constrain="startsWith">
- <!-- constraint values: startsWith, endsWith, contains -->
  <searchString text="comment line">#</searchString>
- <!-- ignore lines that start with # because they are comment lines -->
  </rule>
  </parseRules>
- <field fieldName="date" parseType="delimited">
- <!-- parseType values: delimited, bounded, indexed -->
  <delimiter />
  <delimitedIndex>0</delimitedIndex>
  </field>
- <field fieldName="time" parseType="delimited">
  <delimiter />
  <delimitedIndex>1</delimitedIndex>
  </field>
- <field fieldName="serverip" parseType="delimited">
  <delimiter />
  <delimitedIndex>2</delimitedIndex>
  </field>
- <field fieldName="method" parseType="delimited">
  <delimiter />
  <delimitedIndex>3</delimitedIndex>
  </field>
- <field fieldName="uri" parseType="delimited">
  <delimiter />
  <delimitedIndex>4</delimitedIndex>
  </field>
- <field fieldName="query" parseType="delimited">
  <delimiter />
  <delimitedIndex>5</delimitedIndex>
  </field>
- <field fieldName="username" parseType="delimited">
  <delimiter />
  <delimitedIndex>7</delimitedIndex>
  </field>
- <field fieldName="clientip" parseType="delimited">
  <delimiter />
  <delimitedIndex>8</delimitedIndex>
  </field>
- <field fieldName="httpstatus" parseType="delimited">
  <delimiter />
  <delimitedIndex>10</delimitedIndex>
  </field>
- <field fieldName="s-port" parseType="delimited">
  <delimiter />
  <delimitedIndex>5</delimitedIndex>
  </field>
- <field fieldName="cs(User-Agent)" parseType="delimited">
  <delimiter />
  <delimitedIndex>9</delimitedIndex>
  </field>
  </event>
  </LogFormatDefinition>
```

301

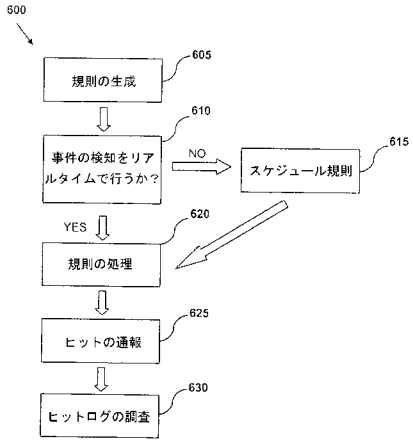
【図４】


リモートCRMアクセス
405
CRMデータの捕捉
410
検知
415
捜査（ｉ）
420
捜査（ｉｉ）
425
分離
430

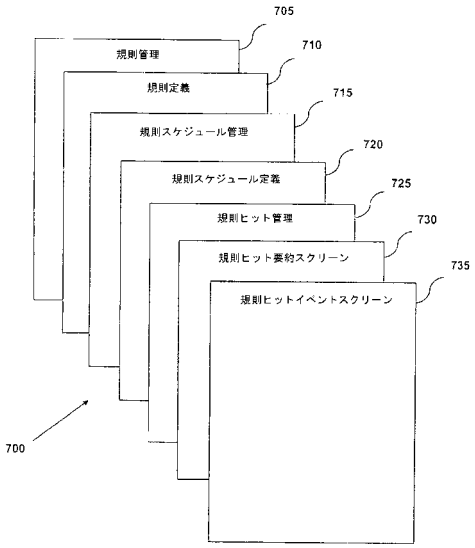
【図５】


ユーザ識別子モジュール
51
相関モジュール
56
モデル化データ提供モジュール
52
分析モジュール
57
データ捕捉モジュール
53
決定モジュール
58
構文解析エンジン
54
ユーザ別分析モジュール
59
正規化モジュール
55
警報発生モジュール
60
50
別のコンピュータ
13A
10
ネットワーク
12
26
通信線
13
別のコンピュータ
入力機器
24
モニタ
28
32
14
CPU
プリンタ
30
21
22
BIOSドライバ
アプリケーション
データベース
16
オペレーティングシステム
20
システムメモリ
18

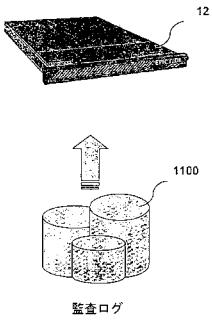
【図６】


600
規則の生成
605
事件の検知をリアルタイムで行うか？
610
NO
スケジュール規則
615
YES
規則の処理
620
ヒットの通報
625
ヒットログの調査
630

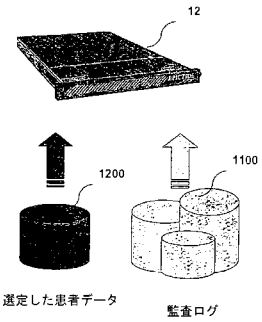
【図７】


705
規則管理
710
規則定義
715
規則スケジュール管理
720
規則スケジュール定義
725
規則ヒット管理
730
規則ヒット要約スクリーン
735
規則ヒットイベントスクリーン
700

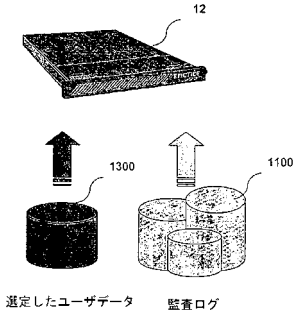
【図８】


12
1100
監査ログ

【図９】


12
1200
1100
選定した患者データ
監査ログ

【図１０】


12
1300
1100
選定したユーザデータ
監査ログ

【国際調査報告】

## INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 08/57220

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - G06F 11/30; G21C 17/00 (2008.04)
USPC - 702/185
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC:702/185

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC:702/185

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
pubWEST(PGPB,USPT), Google patent, Google Scholar
Text search terms: generate rule, monitor, transactions, activities, apply rule, criteria, compile hits, real time, statistics, receive, recipient, user parameter, volume parameter, time parameter, fraud detection, database, misuse, event occur, data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category* | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 2006/0282660 A1 (VARGHESE et al.) 14 December 2006 (14.12.2006) entire document, especially; Fig 13B, Abstract, para [0018], [0025], [0026], [0032], [0067], [0109], [0113], [0125], [0175]. | 1 - 20 |
| A | US 2007/0039049 A1 (KUPFERMAN et al.) 15 February 2007 (15.02.2007) entire document. | 1 - 20 |

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 15 July 2008 (15.07.2008) | 22 JUL 2008 |
| Name and mailing address of the ISA/US<br>Mail Stop PCT, Attn: ISA/US, Commissioner for Patents<br>P.O. Box 1450, Alexandria, Virginia 22313-1450<br>Facsimile No. 571-273-3201 | Authorized officer:<br>Lee W. Young<br>PCT Helpdesk: 571-272-4300<br>PCT OSP: 571-272-7774 |

Form PCT/ISA/210 (second sheet) (April 2007)

フロントページの続き

(81)指定国 AP(BW,GH,GM,KE,LS,MW,MZ,NA,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HR,HU,IE,IS,IT,LT,LU,LV,MC,MT,NL,NO,PL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AO,AT,AU,AZ,BA,BB,BG,BH,BR,BW,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DO,DZ,EC,EE,EG,ES,FI,GB,GD,GE,GH,GM,GT,HN,HR,HU,ID,IL,IN,IS,JP,KE,KG,KM,KN,KP,KR,KZ,LA,LC,LK,LR,LS,LT,LU,LY,MA,MD,ME,MG,MK,MN,MW,MX,MY,MZ,NA,NG,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RS,RU,SC,SD,SE,SG,SK,SL,SM,SV,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,US,UZ,VC,VN,ZA,ZM,ZW

（特許庁注：以下のものは登録商標）
１．イーサネット

(72)発明者 ロング・クルト・ジェームス
アメリカ合衆国、フロリダ州 ３３７０３、セント・ピーターズバーグ、カロライナ・アベニュー・エヌイー、１９４５