(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5108155号
(P5108155)

(45)発行日　平成24年12月26日(2012.12.26)　(24)登録日　平成24年10月12日(2012.10.12)

(51)Int.Cl.		F I		
G06F 21/24	(2006.01)	G06F	21/24	163J
G06F 21/20	(2006.01)	G06F	21/20	131C
G06F 12/00	(2006.01)	G06F	12/00	537A

請求項の数 6　外国語出願　(全 19 頁)

(21)出願番号	特願2012-15556(P2012-15556)
(22)出願日	平成24年1月27日(2012.1.27)
(62)分割の表示	特願2008-515373(P2008-515373)の分割
原出願日	平成18年5月21日(2006.5.21)
(65)公開番号	特開2012-108934(P2012-108934A)
(43)公開日	平成24年6月7日(2012.6.7)
審査請求日	平成24年2月27日(2012.2.27)
(31)優先権主張番号	60/688,486
(32)優先日	平成17年6月7日(2005.6.7)
(33)優先権主張国	米国(US)
(31)優先権主張番号	11/258,256
(32)優先日	平成17年10月25日(2005.10.25)
(33)優先権主張国	米国(US)

(73)特許権者　508242768
バロニス　システムズ，インコーポレイティド
アメリカ合衆国，ニューヨーク　１００１８，ニューヨーク，セブンス　アベニュ　４９９
(74)代理人　100099759
弁理士　青木　篤
(74)代理人　100092624
弁理士　鶴田　準一
(74)代理人　100108383
弁理士　下道　晶久
(74)代理人　100141162
弁理士　森　啓

最終頁に続く

(54)【発明の名称】データ記憶アクセスの制御方法

(57)【特許請求の範囲】

【請求項１】

記憶要素を備えたファイルシステムの複数のユーザを有する組織におけるデータ記憶アクセスの制御方法であって、

プローブエンジンが、前記記憶要素に対する前記ユーザのアクセスを記録し、該記録されたアクセスから各アクセスプロファイルを導出するステップと、

解析エンジンが、前記ユーザ及び前記記憶要素をバイクラスタしてユーザクラスタ及びデータクラスタを規定するステップと、

該バイクラスタステップに応答して、前記解析エンジンが、自動的かつ人を介さずに前記ユーザによる前記記憶要素へのアクセスの制御ポリシを規定するステップと、

前記プローブエンジンが、前記ポリシを用いて前記ユーザによる前記記憶要素へのアクセスを制御するステップと、

を具備し、

前記ユーザクラスタにおける前記ユーザの前記アクセスプロファイルが互いに相似しており、前記データクラスタにおける前記記憶要素が、前記複数のユーザの中で互いに相似した前記アクセスプロファイルを有するユーザによってのみアクセスされ、

前記制御ポリシを規定するステップは、

前記解析エンジンが、前記規定されたポリシを制御ポリシの暫定版として提案するステップと、

コミットモジュールが、前記ユーザによる前記記憶要素の後続アクセスを監視するステ

ップと、
前記コミットモジュールが、前記後続アクセスが前記制御ポリシの前記暫定版に従っていることを判別するステップと、
前記判別ステップに応答して、前記コミットモジュールが、前記暫定版を前記制御ポリシの確定版として認定するステップと、
を有することを特徴とするデータ記憶アクセスの制御方法。
【請求項２】
さらに、
コミットモジュールが、前記ユーザの少なくとも１つのユーザ集合及び前記記憶要素の少なくとも１つのデータ集合を備えるアクセス制御リストを参照するステップと、
前記コミットモジュールが、各前記ユーザクラスタのメンバによる各前記データクラスタのメンバに対するアクセスの不存在を検出するステップと、
該検出ステップに応答して、前記コミットモジュールが、前記ユーザ集合から少なくとも前記ユーザの一部を削除し、かつ前記データ集合から少なくとも前記記憶要素の一部を削除するステップと、
を具備し、
前記ユーザ集合の前記ユーザは前記ユーザクラスタのそれぞれに含まれ、前記データ集合の前記記憶要素は前記データクラスタのそれぞれに含まれている、請求項１に記載のデータ記憶アクセスの制御方法。
【請求項３】
コンピュータプログラムが格納され、該コンピュータプログラムはコンピュータによって読込まれて該コンピュータに複数のユーザを有する組織における記憶要素を有するファイルシステムのデータ記憶アクセスを制御するための方法を実行させるコンピュータ読出可能記憶媒体であって、前記方法は、
プローブエンジンが、前記記憶要素に対する前記ユーザのアクセスを記録し、該記録されたアクセスから各アクセスプロファイルを導出するステップと、
解析エンジンが、前記ユーザ及び前記記憶要素をバイクラスタしてユーザクラスタ及びデータクラスタを規定するステップと、
該バイクラスタステップに応答して、前記解析エンジンが、自動的かつ人を介さずに前記ユーザによる前記記憶要素へのアクセスの制御ポリシを規定するステップと、
前記プローブエンジンが、前記ポリシを用いて前記ユーザによる前記記憶要素へのアクセスを制御するステップと、
を有し、
前記ユーザクラスタにおける前記ユーザの前記アクセスプロファイルが互いに相似しており、前記データクラスタにおける前記記憶要素が、前記複数のユーザの中で互いに相似した前記アクセスプロファイルを有するユーザによってのみアクセスされ、
前記制御ポリシを規定するステップは、
前記解析エンジンが、前記規定されたポリシを制御ポリシの暫定版として提案するステップと、
コミットモジュールが、前記ユーザによる前記記憶要素の後続アクセスを監視するステップと、
前記コミットモジュールが、前記後続アクセスが前記制御ポリシの前記暫定版に従っていることを判別するステップと、
前記判別ステップに応答して、前記コミットモジュールが、前記暫定版を前記制御ポリシの確定版として認定するステップと、
を有する、コンピュータ読出可能記憶媒体。
【請求項４】
前記方法は、さらに、
コミットモジュールが、前記ユーザの少なくとも１つのユーザ集合及び前記記憶要素の少なくとも１つのデータ集合を備えるアクセス制御リストを参照するステップと、

前記コミットモジュールが、各前記ユーザクラスタのメンバによる各前記データクラスタのメンバに対するアクセスの不存在を検出するステップと、
該検出ステップに応答して、前記コミットモジュールが、前記ユーザ集合から少なくとも前記ユーザの一部を削除し、かつ前記データ集合から少なくとも前記記憶要素の一部を削除するステップと、
を有し、
前記ユーザ集合の前記ユーザは前記ユーザクラスタのそれぞれに含まれ、前記データ集合の前記記憶要素は前記データクラスタのそれぞれに含まれている、請求項３に記載のコンピュータ読出可能記憶媒体。
【請求項５】
複数のユーザを有する組織における記憶要素を有するファイルシステムのデータ記憶アクセスの制御装置であって、該装置は以下のステップを実行できるコンピュータシステムを有し、該コンピュータシステムは、
プローブエンジンが、前記記憶要素に対する前記ユーザのアクセスを記録し、該記録されたアクセスから各アクセスプロファイルを導出するステップと、
解析エンジンが、前記ユーザ及び前記記憶要素をバイクラスタしてユーザクラスタ及びデータクラスタを規定するステップと、
該バイクラスタステップに応答して、前記解析エンジンが、自動的かつ人を介さずに前記ユーザによる前記記憶要素へのアクセスの制御ポリシを規定するステップと、
前記プローブエンジンが、前記ポリシを用いて前記ユーザによる前記記憶要素へのアクセスを制御するステップと、
を実行するように動作し、
前記ユーザクラスタにおける前記ユーザの前記アクセスプロファイルが互いに相似しており、前記データクラスタにおける前記記憶要素が、前記複数のユーザの中で互いに相似した前記アクセスプロファイルを有するユーザによってのみアクセスされ、
前記制御ポリシを規定するステップは、
前記解析エンジンが、前記規定されたポリシを制御ポリシの暫定版として提案するステップと、
コミットモジュールが、前記ユーザによる前記記憶要素の後続アクセスを監視するステップと、
前記コミットモジュールが、前記後続アクセスが前記制御ポリシの前記暫定版に従っていることを判別するステップと、
前記判別ステップに応答して、前記コミットモジュールが、前記暫定版を前記制御ポリシの確定版として認定するステップと、
を有する、データ記憶アクセスの制御装置。
【請求項６】
前記コンピュータシステムは、さらに、
コミットモジュールが、前記ユーザの少なくとも１つのユーザ集合及び前記記憶要素の少なくとも１つのデータ集合を備えるアクセス制御リストを参照するステップと、
前記コミットモジュールが、各前記ユーザクラスタのメンバによる各前記データクラスタのメンバに対するアクセスの不存在を検出するステップと、
該検出ステップに応答して、前記コミットモジュールが、前記ユーザ集合から少なくとも前記ユーザの一部を削除し、かつ前記データ集合から少なくとも前記記憶要素の一部を削除するステップと、
を実行するように動作し、
前記ユーザ集合の前記ユーザは前記ユーザクラスタのそれぞれに含まれ、前記データ集合の前記記憶要素は前記データクラスタのそれぞれに含まれている、請求項５に記載のデータ記憶アクセスの制御装置。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明はコンピュータセキュリティに関する。特に、本発明は多様なファイルアクセス制御モデルを有する組織におけるセキュリティポリシの自動生成及び管理に関する。
【背景技術】
【０００２】
データセキュリティポリシは、典型的には、蓄積された組織のデータに様々なコンピュータシステム上で誰がアクセスしたかを究明する。これらのポリシは固定的ではありえない。組織内部のユーザ、例えば、従業員、パートナ、請負業者は、組織外部からの脅威と同じくらいシビアな脅威を与えることがあり得る。従って、組織の構造及び人員構成が変る際に、セキュリティポリシはそのときに応じて調整されなければならない。しかしながら、組織の極秘データを保護する一方で、情報技術（IT）部門は、ユーザアクセス権を管理し、必要とされる情報が都合よく得られることを確実に行なう有効な手段に欠けている。
【０００３】
ＩＴ部門に利用可能な最新技術は、ユーザネーム、パスワード、バイオメトリクス、暗号化及びシングルサインオンへのアクセス制限を含むような技術の拡張の管理と共に、アクセス制御リストの点検及びメンテナンスを含む。そのような技術は、効率的でなく、しばしば不正確であり、構成及び人員が絶えず変化する大規模かつ複雑な組織においては、実用的ではない。
【０００４】
特別なオペレーティングシステム及び操作環境を利用することで、企業はセキュリティ支援手段を入手することができる。これらは、しばしば役割ベースのアクセス制御を基礎としており、政府組織により過去数年間、相当の興味を持たれ、つい最近営利事業に受け入れられた技術を基礎としている。マルチユーザQSLデータベースにおける役割ベースのアクセス制御に対する代表的な提案は、非特許文献１に示される。
【先行技術文献】
【非特許文献】
【０００５】
【非特許文献１】Sahadeb De et al., “Secure Access Control in a Multi-user Geodatabase”, URL “http://www10.giscafe.con”
【発明の概要】
【発明が解決しようとする課題】
【０００６】
それにもかかわらず、アクセス制御技術は、多様なアクセス制御モデルを利用する企業において、最適に実施されてはいなかった。今日の最新技術の状態は、そのような環境下でシステム管理者が、誰が何にアクセスしているのかを簡単に知ることができないことにある。その結果、多くの組織において、受け入れ難いほど高い比率のユーザが、不正なアクセス権を有している。冗長なアクセス権及び組織を去った人員の持ち主のいないアカウントに関連する問題も完全には解決されていない。従って、データ機密保護を改善し、不正行為を防止し、会社の生産性を改善するために、ユーザファイルの承認を自動的に制御する方法が求められている。
【課題を解決するための手段】
【０００７】
本発明の開示された実施例によれば、多様なアクセス制御モデル及びファイルサーバプロトコルを有するネットワーク化された組織において、データセキュリティポリシを自動的に作成し管理するための方法及びシステムが得られる。組織を構成するネットワーク内の記憶素子へのアクセスは、データアクセスの分類とユーザの分類とを同時に決定するために、継続的にモニタされ、解析される。実際の組織的構成は、これらのグループ分けから学び、ダイナミック・データ・アクセス制御ポリシの基礎となり、これは組織の経時的な変化に常に適合している。ファイルアクセス制御の対話型管理のための決定援助インタ

ーフェイスが提供される。また、異常なユーザの行動を検出及び追跡する施設が提供される。このように、組織はこれらのデータ及びアプリケーションをよりよくアクセス制御できる。

【０００８】

いくつかの実施形態において、ユーザグルーピング、データアクセスグルーピング及び通常のアクセス制御リストを協調させて、これらのアクセス制御リストを変更させることによりファイルアクセス制御を半自動的に管理することによって技法を拡張する。

【０００９】

本発明の教示を適用することによって展開するアクセスポリシは補助的利益、たとえば、サービス否認（denial-of-service）攻撃が生じた場合にリソース使用を制限する補助的利益を有する。

【００１０】

本発明によれば、複数のユーザを有する組織における記憶要素を有するファイルシステムのデータ記憶アクセスを制御するための方法であって、前記記憶要素に対する前記ユーザのアクセスを記録し該記録されたアクセスから各アクセスプロファイルを導くステップと、前記ユーザ及び前記記憶要素をバイクラスタ（bicluster）してユーザクラスタ及びデータクラスタを規定するステップと、該バイクラスタステップに応答して前記ユーザによるアクセスの制御ポリシを規定するステップとを具備し、前記ユーザクラスタにおける前記ユーザの前記アクセス特性（profiles）が互いに相似しており、前記データクラスタにおける前記記憶要素が、互いに相似した前記アクセス特性を有する、前記複数ユーザの中のユーザによってのみアクセスされる方法が提供される。

【００１１】

上記方法の一局面によれば、前記１つのデータクラスタにおける前記記憶要素の少なくとも１つの記憶要素が前記ユーザの１つのユーザによってアクセスされているときのみ、前記制御ポリシは、前記１つのユーザによる前記１つのデータクラスタの前記記憶要素のアクセスを可能とする。

【００１２】

また、上記方法の一局面によれば、前記１つのデータクラスタにおける前記記憶要素の少なくとも１つの記憶要素が前記ユーザクラスタの少なくとも１つのユーザによってアクセスされているときのみ、前記制御ポリシは、前記ユーザクラスタのユーザによる前記１つのデータクラスタの前記記憶要素のアクセスを可能とする。

【００１３】

さらに、上記方法の一局面によれば、前記バイクラスタステップに応答して前記ファイルシステムの構造を導くステップを具備する。

【００１４】

さらに、上述の方法の一局面は、前記バイクラスタステップに応答して前記ファイルシステムの使用パターンを導くステップを具備する。

【００１５】

上述の方法の一局面は、前記使用パターンの異常パターンを検出するステップを具備する。

【００１６】

さらに、上述の方法の一局面において、前記バイクラスタステップは繰返して実行され、前記アクセス特性は該繰返し毎に再決定され、前記制御ポリシは前記各繰返し後に更新される。

【００１７】

さらに、上述の方法の一局面において、前記制御ポリシを規定するステップは、前記制御ポリシの仮改訂を要求するステップと、前記ユーザによる前記記憶要素の後続アクセスを監視するステップと、前記後続アクセスが前記制御ポリシの前記仮改訂に従っていることを判別するステップと、前記判別ステップに応答して前記仮改訂を前記制御ポリシの確定版として認定するステップとを具備する。

【００１８】
さらに、上述の方法の一局面は、前記制御ポリシを対話的に修正するステップを具備する。
【００１９】
さらに、上述の方法の一局面において、前記制御ポリシを規定するステップは自動的かつ実質的に人を介さずに実行される。
【００２０】
さらに、上述の方法の一局面は、前記ユーザの少なくとも１つのユーザ集合及び前記記憶要素の少なくとも１つのデータ集合を備えるアクセス制御リストを参照するステップと、前記各ユーザクラスタのメンバによる前記各データクラスタのメンバに対するアクセスの不存在を検出するステップと、該検出ステップに応答して前記ユーザ集合から少なくとも前記ユーザの一部を削除しかつ前記データ集合から少なくとも前記記憶要素の一部を削除するステップとを具備し、前記ユーザ集合の前記ユーザは前記ユーザクラスタのそれぞれに含まれ、前記データ集合の前記記憶要素は前記データクラスタのそれぞれに含まれている。
【００２１】
本発明によれば、コンピュータプログラムが格納されたコンピュータ読出可能媒体を含有し、該コンピュータプログラムはコンピュータによって読込まれて該コンピュータに複数のユーザを有する組織における記憶要素を有するファイルシステムのデータ記憶アクセスを制御するための方法を実行させるコンピュータソフトウェア製品にあって、前記方法は、前記記憶要素に対する前記ユーザのアクセスを記録し該記録されたアクセスから各アクセスプロファイルを導くステップと、前記ユーザ及び前記記憶要素をバイクラスタ（bicluster）してユーザクラスタ及びデータクラスタを規定するステップと、該バイクラスタステップに応答して前記ユーザによるアクセスの制御ポリシを規定するステップとを具備し、前記ユーザクラスタにおける前記ユーザの前記アクセス特性（profiles）が互いに相似しており、前記データクラスタにおける前記記憶要素が、互いに相似した前記アクセス特性を有する、前記複数ユーザの中のユーザによってのみアクセスされるコンピュータソフトウェア製品が提供される。
【００２２】
本発明によれば、複数のユーザを有する組織における記憶要素を有するファイルシステムのデータ記憶アクセスを制御するための装置であって、該装置は以下のステップを実行できるコンピュータシステムを具備し、該コンピュータシステムは、前記記憶要素に対する前記ユーザのアクセスを記録し該記録されたアクセスから各アクセスプロファイルを導くステップと、前記ユーザ及び前記記憶要素をバイクラスタ（bicluster）してユーザクラスタ及びデータクラスタを規定するステップと、該バイクラスタステップに応答して前記ユーザによるアクセスの制御ポリシを規定するステップとを実行するように動作し、前記ユーザクラスタにおける前記ユーザの前記アクセス特性（profiles）が互いに相似しており、前記データクラスタにおける前記記憶要素が、互いに相似した前記アクセス特性を有する、前記複数ユーザの中のユーザによってのみアクセスされる装置が提供される。
【図面の簡単な説明】
【００２３】
【図１】本発明の開示された実施の形態に係るデータアクセス制御ポリシが自動的に規定され管理されるデータ処理システムを示すブロック図である。
【図２】本発明の開示された実施の形態に係る図１のシステムのプローブエンジンを示すブロック図である。
【図３】本発明の開示された実施の形態に係る図１のシステムのプローブエンジンの変更例を示すブロック図である。
【図４】本発明の開示された実施の形態に係るユーザクラスタリング方法を示すフローチャートである。
【図５】本発明の開示された実施の形態に係る記憶要素クラスタリング方法を示すフロー

チャートである。
【図６Ａ】本発明の開示された実施の形態に係る半自動ファイルアクセス制御方法を示すフローチャートである。
【図６Ｂ】本発明の開示された実施の形態に係る半自動ファイルアクセス制御方法を示すフローチャートである。
【発明を実施するための形態】
【００２４】
以下の説明においては、種々の具体的な詳細について説明して本発明の完全な理解を提供する。しかしながら、当業者にとっては、これらの具体的な詳細な説明なしでも本発明は実行できることが明らかである。他の例においては、周知の回路、制御論理、及び通常のアルゴリズム及び処理に対するコンピュータプログラム命令の詳細は本発明を不必要に曖昧にしないために示していない。
【００２５】
本発明を具体化するソフトウェアプログラムコードは、たとえばコンピュータ読込可能媒体のような永久的記憶媒体に保持される。クライアントサーバ環境においては、このようなソフトウェアプログラムコードはクライアントもしくはサーバに格納される。ソフトウェアプログラムコードはデータ処理システムについて使用される種々の公知の媒体において具体化される。この媒体としては、ディスクドライブ、磁気テープ、コンパクトディスク（ＣＤ）、デジタルビデオディスク（ＤＶＤ）のような磁気的及び光学的記憶装置があるが、これに限定されるものではない。コンピュータ命令信号は伝送媒体にこれらの信号が変調されている搬送波と共にもしくは搬送波なしで具体化されている。たとえば、伝送媒体としては、インターネットのような通信ネットワークを含むことができる。また、本発明はコンピュータソフトウェアにより具体化できるが、本発明を実行するのに必要な機能の一部もしくは全体は特定用途向集積回路もしくは他のハードウェアのようなハードウェア部品、もしくはハードウェア部品及びソフトウェアの組合せにより具体化することができる。
【００２６】
［システム全体］
まず、図１はデータ処理システム１０のブロック図である。図１を参照すると、データアクセスポリシは本発明の開示された実施の形態に従って自動的に規定され管理される。システム１０は汎用コンピュータとしてあるいは１つのネットワークたとえばインターネットに接続された複数のコンピュータとして構成される。
【００２７】
システム１０によってアクセスできる組織全体のデータ記憶は組織ファイルシステム１２によって表される。組織ファイルシステム１２は１つもしくは複数の同一場所（colocated）の記憶ユニットを備えており、あるいは、当業者に周知のごとく、地理的に分散したデータ記憶システムでもよい。組織ファイルシステム１２の個々の記憶ユニットは同一の能力を有している要件を必要としない。
【００２８】
組織ファイルシステム１２はグラフィックユーザインターフェイス（ＧＵＩ）アプリケーション１６を用いて複数のユーザ１４によってアクセスできる。ＧＵＩアプリケーション１６は応用プログラムインターフェイス（ＡＰＵ）１８を介するシステム１０以外の要素である。ユーザ１４はたとえば組織のメンバであるが、顧客のような外部のメンバを含むことができる。グラフィックユーザインターフェイスアプリケーション１６は管理システムのインターフェイスであり、これを介してユーザ１４は解析エンジン２０が決定した実際の使用解析の結果を受信できる。ある実施の形態においては、十分に権限が与えられたユーザたとえば管理部員は現在の状況を考慮することができ、また、システムによって勧告された変更を考慮することができる。このようなユーザは勧告された変更を受理もしくは拒絶する権限を有することができる。勧告された変更を選択する前に、権限を与えられたユーザはシステム上における勧告された変更の効果を考慮する能力を有する。次に、

システム管理者は最も適切である許可セットを選択もしくは確認することができる。
【００２９】
プローブエンジン２２は組織ファイルシステム１２からアクセス情報を前進方法（ongoing manner）で収集し、二重もしくは冗長情報単位をフィルタ（filter）し、その結果の情報ストリームをデータベース２４に格納する。また、プローブエンジン２２を用いて、組織の現在のファイルセキュリティポリシ、組織ファイルシステム１２の現在の構造及びユーザ１４についての情報を収集する。プローブエンジン２２は種々の環境及びアーキテクチャにおいて実行できる。
【００３０】
解析エンジン２０は記憶アクセスを制御するシステム能力の心臓部に存在する専用モジュールである。解析エンジン２０は組織セキュリティポリシを自動的に提案して改訂する。解析エンジン２０の前縁にはデータコレクタ２６があり、このデータコレクタ２６は記憶アクセス動作をデータベース２４に効率よく記録する。さらに解析エンジン２０の出力は対話型管理インターフェイス２８を用いて操作でき、この対話型管理インターフェイス２８はシステム管理者に対して収集されたデータについて質問させるようにする。管理インターフェイス２８を用いて管理者は必要であれば自動的に要求されたセキュリティポリシを修正でき、また、最終的に新しいもしくは改定されたポリシを活性化する。
【００３１】
解析エンジン２０に関係しているコミットモジュール３０はその実行前に収集されたデータを用いて要求されたセキュリティポリシを検証する。コミットモジュール３０はアクセス制御リスト（ＡＣＬ）３２を参照する。コミットモジュール３０の動作を以下に詳述する。
【００３２】
［プローブエンジン］
プローブエンジンは特別のオペレーティングシステム及び環境に合うように作られる。以下にその例を説明するが、これに限定されるものではない。
【００３３】
［ウィン－プローブアーキテクチャ］
次に、本発明の開示された実施の形態に係るプローブエンジン２２（図１）の一実施の形態を示すブロック図である図２を参照する。この実施の形態での用語ウィン－プローブ（Win-Probe）モジュールはマイクロソフトウィンドウズ（登録商標）プラットフォームのプローブとして作用する。このプローブの責務は、組織ファイルシステム１２（図１）の部品であるローカルファイルシステムをオペレーティングシステムレベルで監視することである。たとえば、組織におけるすべてのウィンドウズ（登録商標）コンピュータを操作するウィン－プローブモジュールがある。このウィン－プローブモジュールは他のオペレーティングシステムに適合するプローブエンジンと並列に動作する。あるいは、複雑な組織は効果的な動作を確保するために複数のウィン－プローブモジュールを必要とすることができる。ウィン－プローブモジュールはファイルシステムフィルタ（ＳＩＤＦＩＬＥ）３４を有し、ファイルシステムフィルタ３４はカーネルモードフィルタドライバ３６を用いてローカルファイルシステム３８の動作を傍受し（intercept）傍受した動作に関するセキュリティ情報のログをとる。サービス（ＳＩＤＦＩＬＥ　ＳＥＲＶＩＣＥ）４０はフィルタドライバ３６と相互作用し新しいログエントリに登録する。ログエントリはサービス４０によってフィルタされる。サービス４０はフィルタされたログエントリから統計を編する責任を有し、さらなる処理のために生のログエントリ及びこれらの統計の両方をデータベース２４（図１）に送る。フィルタ３４はオペレーティングシステムに対して無処理（transparent）であり、そのオーバヘッドは入出力（Ｉ／Ｏ）動作及びログ当りのセキュリティ属性の抽出に制限される。フィルタドライバ３６とサービス４０との間の通信は装置Ｉ／Ｏ制御のようなオペレーティングシステム機構及び予め定義された制御コードたとえば収集統計（collect statistics）を用いて達成される。
【００３４】

［ネットワーク付記憶プローブアーキテクチャ］
次に、図１のプローブエンジン２２の他の実施の形態を示すブロック図である図３を参照すると、本発明に開示された実施の形態に従ってネットワーク装置に適用されている。ネットワーク付記憶（ＮＡＳ）プローブ４２はＮＡＳ装置４４からアクセスデータを収集する責任を有する。ある実施の形態においては、１つのＮＡＳプローブは組織全体に貢献する。あるいは、複数のＮＡＳプローブも備えることができる。プローブ４２は専用たとえばベンダ特定のプロトコルを用いてＮＡＳ装置４４に相互作用する。このプロトコルはＮＡＳ装置４４に対してユーザ４８から発生した要求ファイルアクセス動作上の通知をプローブ４２に送る。プローブ４２は現在支配するポリシに従って要求をＮＡＳ装置４４によって満足させるかＮＡＳ装置４４へのアクセスを拒絶する。ログエントリ５０はプローブ４２によってなされ、イネーブル要求を書類化し、このイネーブル要求はＮＡＳ装置４４に送られ、そのオペレーティングシステムに従って通常の処理に供される。ある実施の形態においては、拒否された要求は単に廃棄される。あるいは、拒否された要求は異常なユーザ行為を追跡するのを助けるためにログに登録できる。いずれの場合も、ユーザ４８はその要求に対する応答５２を、アクセス拒否の形式もしくはＮＡＳ装置４４によって要求された結果の指示の形式で、その要求に対する応答５２を受信する。いずれの場合も、最小の性能の効果（impact）がある。ＮＡＳ装置４４はそれ自身所有のオペレーティングシステムを有するので、すべてのドライバ関連の問題たとえばシステム識別子（ＳＩＤ）、ユーザ識別子（ＵＩＤ）、及び要求ファイルアクセスの型の抽出はＮＡＳ装置４４側で取扱われ、プローブ４２によって単にログに登録されるだけである。

【００３５】
［解析エンジン］
上述したように、解析エンジン２０（図１）はシステム１０の心臓部にある。プローブエンジン２２によって報告された組織ファイルシステム１２における各データ記憶要素に対応する組織の各メンバを含むユーザ１４の実際のアクセスの統計を用いてユーザ及びデータ記憶要素の同時かつ自動のクラスタリングを実行する。バイクラスタリングは以下のように行われる。つまり、同一ユーザクラスタのメンバであるユーザが相似のデータアクセス特性を共有するように、また、同一データクラスタのメンバであるデータ記憶要素（ファイルもしくはディレクトリ）が大部分相似のアクセス特性を有するユーザによってアクセスされるように行われる。クラスタは組織構造のグローバル像を提供する。また、解析エンジン２０はクラスタリングの結果からユーザにおける相似性の局所的尺度及び同一クラスタに属するデータ要素における相似性の局所的尺度を展開することができる。さらに、クラスタリングプロセスは組織メンバによる将来のデータ記憶アクセスを予測する。ユーザ１４の１人があるファイルもしくは記憶要素をアクセスしておらず、かつ相似のユーザが相似のファイルをアクセスしていなければ、あるユーザは近い将来における対応記憶要素に対するアクセス権を必要としないことが、高い信頼性で確証できる。このように、解析エンジン２０はＩＴ管理者に情報利用パターンの明瞭なグローバル像を提供し、また、セキュリティポリシの最適化のための詳細な勧告を提供できる。同時に、管理者は異常なユーザの行為に警戒する。また、解析エンジン２０はいかなる不審な活動の完全な裁判上の手がかりをも自動的に作成できる。この結果は劇的な能力であり、アクセス及びプライバシポリシに対するコンプライアンスを確保し、また、付加的な管理負担をＩＴ人員に課すことなく適切な情報使用を確保する。

【００３６】
［バイクラスタリングアルゴリズム］
以下のクラスタリングアルゴリズムを現在の環境に用いる。しかしながら、本発明は以下に説明する特定のアルゴリズムに限定されるものではない。当業者にとっては、他のクラスタリングアルゴリズムをプローブエンジン２２（図１）によって得られたデータに適用して同等の結果を得ることができるのは明らかである。

【００３７】
２つの離散的確率変数Ｘ及びＹの結合分布をｐ（ｘ，ｙ）＝ｐ（Ｘ＝ｘ，Ｙ＝ｙ）と表

す。この場合、Ｘは組織におけるユーザ集合を表し、また、Ｙは組織のメンバによってアクセスされたファイルディレクトリ集合を表す。値ｐ（ｘ，ｙ）は１登録フェイズ（enrollment phase）においてユーザｘがデータ記憶要素に接近した正規化された回数を示す。本発明は、ｐ（ｘ，ｙ）の近傍（contiguity）テーブルによって構成され収集されたデータに基づき、２つの集合の基本的に存在する構造及びこれらの相互関係を発見しようとするものである。より正確には、確率変数Ｘ及びＹを相似要素の互いに素な（交わらない）集合にクラスタするものである。確率変数のクラスタリングとはＸの要素をＸ’で表される互いに素な（disjoint）クラスタに区分することであり、同様に、ＹをＹ’による区分で示せる。

【００３８】

クラスタの数を（システム構成パラメータの一部として）予め定義すると、ユーザクラスタとデータクラスタとの間の相互情報量Ｉ（Ｘ’，Ｙ’）が最大となるようにクラスタリングＸ’，Ｙ’を求める。言い換えると、システムは相互情報量基準をコスト関数として用い、種々のクラスタリング構造の品質を評価する。

【００３９】

相互情報量は次のごとく定義される。

【数１】

$$I(X;Y) = -\sum_{x,y} p(X=x,Y=y)\log p(X=x,Y=y) \quad (1).$$

【００４０】

相互情報量は１つの確率変数が出現する不確からしさの程度を他の確率変数が観測されているときにカプセル化する。また、以下に用いる２つの関連する概念を定義する。Ｐ＝（Ｐ（１），…，Ｐ（ｎ）），Ｑ＝（Ｑ（１），…，Ｑ（ｎ））を２つの離散的確率分布とする。確率分布Ｐ，Ｑの相対的エントロピー（カルバック－ライプラのダイバージェンス）は、

【数２】

$$KL(P||Q) = \sum_{i} P(i)\log(P(i)/Q(i)) \quad (2).$$

となる。

【００４１】

混合係数ｃに係る確率分布Ｐ，Ｑ間のジェンロン－シャノンダイバージンスは、

【数３】

$$JS(P,Q)=cKL(P||cP+(1-c)Q)+(1-c)KL(Q||cP+(1-c)Q) \quad (3).$$

となる。

【００４２】

次のステップは相互情報量基準を用いて最適なクラスタリングを発見することである。ユーザ集合Ｘ及びデータ集合Ｙに対して異なる戦略を用いる。ユーザ集合Ｘの場合には、現在の構造は存在せず、従って、これを維持する必要がない。しかしながら、ある実施の

形態において、組織のユーザ構造を保持することは好ましい。これに対し、データファイルシステムは木構造に基づく。木構造は木における近いディレクトリ間の動作上の相似を反映しているので、木構造を維持したい。従って、記憶要素クラスタリングは基本的に木を剪定することによって達成される。以下このプロセスをさらに詳細に説明する。

【００４３】

［ユーザクラスタリング］

本発明の開示された実施の形態に係るユーザクラスタリング方法を示すフローチャートである。この方法はランダム解で開始し、次に、単調方法で結果を逐次改良していく。

【００４４】

初期ステップ５４において、開始点としてユーザのリストの所定数のクラスタへのランダム区分を選択する。この区分は以下に説明する現在のサイクル集合において用いられる。各ユーザｘに対して、確率分布ｐ（ｙ／ｘ）はユーザｘのデータアクセス活動を表し、つまり、ｐ（ｙ／ｘ）はユーザｘがデータ要素ｙにアクセスした回数であって、登録期間（enrollment period）におけるｘによって実行された全データ活動回数によって正規化されたものである。各ランダムに形成されたクラスタＣに対してｐ（ｙ｜Ｃ）をクラスタＣのメンバであるユーザに関連した条件付確率分布ｐ（ｙ｜ｘ）の平均として定義する。

【００４５】

次に、ステップ５６において、初期ステップ５４において確立したクラスタのうち１つをランダムに選択する。

【００４６】

次に、ステップ５８において、ユーザのうちの１つを選択する。ステップ５８は繰返し実行され、また、ユーザは周期的に評価される。しかしながら、１周期における評価順序は重要でない。

【００４７】

次に、ステップ６０において、現在のユーザｘを現在のクラスタからステップ５６において選択されたクラスタへ仮に移動させ、ユーザの仮の新規クラスタリングを形成する。

【００４８】

制御は決定ステップ６２に進み、新規クラスタリングのグローバル相互情報量Ｉ（Ｘ；Ｙ）が現在クラスタリングのそれより大きいか否かを判別する。ユーザｘとｃユーザからなるクラスタＣとの距離は次のごとく定義する。

【数４】

$$d(x,C) \cdots = (c+1)JS(p(y|x),p(y|C)) \cdots$$
$$= KL(p(y|x)\,||\,(p(y|x)+c\,p(y|C))/(c+1))+$$
$$c*KL(p(y|c)\,||\,(p(y|x)+c\,p(y|C))/(c+1))) \quad (4).$$

【００４９】

各ユーザｘは、距離ｄ（ｘ，Ｃ）を最小化するクラスタＣにマージされる。条件付アクセス確率ｐ（ｙ｜Ｃ）は新しいメンバｘの統計に従って修正される。距離ｄ（ｘ，Ｃ）の最小化はクラスタとデータ活動との相互情報量の最大化と等価である。

【００５０】

決定ステップ６２の判定が肯定的である場合、制御はステップ６４に進む。現在ユーザｘはステップ５６において選択されたクラスタに滞り、また、ステップ６０において確立した仮新規クラスタリングが承認される。

【００５１】

決定ステップ６２の判定が否定的である場合、制御はステップ６６に進む。現在ユーザｘを選択先のクラスタに戻し、また、ステップ６０において確立した仮新規クラスタリングを拒絶する。

【００５２】
いずれの場合でも、次に、制御はステップ６８に進み、現在サイクルにおいて評価すべきユーザが残っているか否かを判別する。決定ステップ６８における判定が肯定的である場合、制御はステップ５８に戻る。
【００５３】
決定ステップ６８における判定が否定的である場合、制御は決定ステップ７０に進み、最後のサイクルが相互情報量において何らかの改良をもたらしたか否かを判別する。
【００５４】
決定ステップ７０の判定が肯定的である場合、最適クラスタリングがまだ達成されていないことになる。ステップ７２にて、ユーザリストはリセットされて現在サイクル集合の他のサイクルを開始する。制御はステップ５６に戻り、また、初期ステップ５４において確立した同一のランダム区分を用いて新クラスタを選択することによって新サイクルを開始する。
【００５５】
決定ステップ７０の判定が否定的である場合、制御はステップ７４に進む。現在のサイクル集合において達成された最良のクラスタリングが記憶される。
【００５６】
次に、制御は決定ステップ７６に進み、終了基準に合致したか否かを判別する。終了基準は初期ステップ５４の所定の繰返回数の完了とすることができる。あるいは、性能インジケータを終了基準とすることができる。
【００５７】
決定ステップ７６の判定が否定的である場合、制御は初期ステップ５４に戻り、この方法が繰返されて新しい開始点を選択する。
【００５８】
決定ステップ７６の判定が肯定的である場合、制御は最終ステップ７８に進む。ステップ７４の繰返において記憶されたクラスタリングにおいて得られた最良の結果がユーザクラスタとデータクラスタとの相互情報量を最大とする最終クラスタリングとして報告される。
【００５９】
［データ要素クラスタリング］
次に、本発明の実施の形態に従って記憶要素をクラスタリングする方法を示すフローチャートである図５を参照する。これはデータファイル木における兄弟要素によって表されるクラスタのマージに基づく集積的（agglomerative）方法である。図４を参照した上述のユーザクラスタリングが実行されたものと仮定する。初期段階で、ユーザアクセス事象として区別できない兄弟ディレクトリあるいは親－子孫ディレクトリ間でマージする。この段階で扱いやすい（tractable）要素数に剪定された（pruned）ディレクトリ木となる。次の段階で、現在剪定された木のすべての葉が観察され（visited）、また、２つの兄弟ディレクトリもしくは両親－子孫ディレクトリ間のマージャが存在し、ユーザクラスタとデータクラスタとの間の相互情報量減少が最小となるようにする。このプロセスは、終了基準を満たすまで、つまり、所定数のクラスタが得られるとき、もしくは現在の相互情報量が所定しきい値より小さくなるときまで繰返される。次に、この方法を詳述する。
【００６０】
初期ステップ８０はファイル木のディレクトリの横断（transversal）を開始する。クラスタリングを選択するに当り、親－子孫ディレクトリ、兄弟ディレクトリ及びこれらのクラスタを考慮し、集合的に隣人（neighbors）と定義する。すべてのデータ要素を観察し、すべての互いの隣人を評価する限り、横断順序は重要でない。多くの未知の木横断アルゴリズムを用いることができる２つの隣人を選択する。
【００６１】
次に、決定ステップ８２に進み、ユーザアクセス事象の見地から本発明の相似の所定基準に従って現在の候補が識別不可能もしくはほとんど識別不可能か否かを判別する。

【００６２】
決定ステップ８２の判定が肯定的である場合、制御はステップ８４に進む。候補はマージされて新規データクラスタを形成する。このデータクラスタは初期ステップ８０の後の繰返において単一記憶要素もしくは隣人として取扱う。
【００６３】
ステップ８４を実行後、もしくは決定ステップ８２の判別が否定的である場合、制御は決定ステップ８６に進み、データファイル木の横断が完了したか否かを判別する。決定ステップ８６の判別が否定的である場合、制御は初期ステップ８０に戻り繰返を開始する。
【００６４】
決定ステップ８６の判別が肯定的である場合、この方法の１段階が終了し、剪定されたディレクトリ木となる。一般に、剪定されたディレクトリ木のディレクトリ及びそのクラスタは扱いやすい（tractable）要素数を構成する。
【００６５】
次に、ステップ８８に進み、この方法のもう１つの段階を開始し、剪定されたディレクトリ木を再び横断し、相互情報量Ｉ（Ｘ；Ｙ）の減少が最小となるように候補をさらにマージする。図４を参照した上述の方法から得られたユーザクラスタと現在剪定された木のデータクラスタとの間の相互情報量Ｉ（Ｘ；Ｙ）を記憶する。
【００６６】
次に、ステップ９０において、２つの候補を選択する。上述のごとく、これらの候補は候補が兄弟、親－子の関係を有する限り、クラスタ、ディレクトリもしくはこれらの組合せとすることができる。
【００６７】
次に、ステップ９２において、現在の候補を仮にマージしてユーザ及びデータ要素の新規クラスタリングを形成する。この仮の構造の相互情報量Ｉ’（Ｘ；Ｙ）を決定する。
【００６８】
次に、制御は決定ステップ９４に進み、仮クラスタリングによって生じた相互情報量Ｉ’（Ｘ；Ｙ）－Ｉ（Ｘ；Ｙ）の減少が最良の前回の仮クラスタリングによって生じた相互情報量の減少より小さいか否かを判別する。決定ステップ９４の最初の繰返では、この判別は常に肯定的である。
【００６９】
決定ステップ９４の判別が肯定的である場合、制御はステップ９６に進む。現在の仮クラスタリングが記憶され、高い水位標（water mark）として設定される。このように、これは利用可能な最高の新規クラスタリングである。
【００７０】
決定ステップ９６を実行後あるいは決定ステップ９４の判別が否定的である場合、制御はステップ９８に進み、木に評価すべき候補が残っているか否かを判別する。決定ステップ９８の判別が肯定的である場合、制御はステップ９０に戻る。
【００７１】
決定ステップ９８の判別が否定的である場合、制御は決定ステップ１００に進み、終了基準に合致したか否かを判別する。この終了基準は所定数の新規クラスタの確立とすることができる。あるいは、相互情報量の現在の最良の減少が所定のしきい値より小さくなったときに終了させることもできる。
【００７２】
決定ステップ１００の判別が否定的である場合、現在の最良クラスタリングの相互情報量を開始点として用いて上述の方法を繰返す。制御はステップ８８に戻り、相互情報量Ｉ（Ｘ，Ｙ）の新しい値を設定する。
【００７３】
決定ステップ１００の判別が肯定的である場合、制御は最終ステップ１０２に進む。ステップ９６にて最後に記憶されたクラスタリングが最適データ要素クラスタリングとして報告される。

【００７４】
クラスタリングアルゴリズムの最後に、ユーザ及びデータ記憶要素の両方は互いに素なクラスタに配置される。階層的木構造はデータ記憶要素に維持され、他方、ユーザは、階層的構造を有することなく、ユーザ空間に配置される。次に、組織のユーザ間におけるロバスト相似測度を抽出することができる。ユーザが同一クラスタに属すれば、ユーザは相似的に行動するといわれ、これはこれら２つのユーザはデータ記憶システムの相似的な部分をアクセスするということを示している。２つのディレクトリもしくは他の記憶要素が同一データクラスタに属していれば、これら２つのディレクトリもしくは記憶要素は相似と考えられる。
【００７５】
［記憶アクセス制御］
図５を参照して上述した方法を用いて得られたクラスタリングを用いて不必要なアクセス許可を自動的に除去できる。たとえば、ユーザｘが要素ｙ（ｙに相似する要素も）を登録期間（enrollment period）にアクセスしていなければ、ユーザｘが記憶要素ｙをアクセスする許可は除去される。予測は組織の相似メンバのアクセス特性に基づく。要素ｙに対する相似アクセス特性を有し、かつユーザｘの同一クラスタに存在するユーザがだれも要素ｙもアクセスせず、また、要素ｙに相似する記憶要素にもアクセスしていなければ、近い将来も、ユーザｘは要素ｙにアクセスしない、ということが確認できる。従って、組織データセキュリティのレベルを上昇させるために、要素ｙに関するユーザｘに対してアクセス許可をキャンセルできる。ユーザの見直しは所定時間毎に繰返され、従って、アクセスポリシも更新される。
【００７６】
［半自動クラスタリング］
上述のセクションでは、組織の実際の構造を反映するアクセス制御ポリシを規定するために、いかにしてユーザデータクラスタリングアプローチを用いるかについて記載した。記録されたデータ活動は、抽出して最適なデータアクセス制御ポリシを規定できる情報源の一つにすぎない。新規つまり更新されたデータアクセスポリシを提案するために、現在のユーザデータグループ構造及び現在のデータセキュリティポリシもまた考慮すべきである。組織について他の主な知識源は現在の（手動にて設定された）アクセス制御リスト３２（図１）である。ＡＣＬは対の集合と見ることができる。ここで、各対は、ユーザグループとこのユーザグループによってアクセスできるデータ要素グループとよりなる。たとえ現在のＡＣＬは多くの誤りを含んでいても、なお所望の制御ポリシと高度に相関していることが合理的に確証できる。以下に説明する手順は上述の非管理のクラスタリング手順を用いて現在のＡＣＬを修正して改良されたポリシを得ることができる。次に、記録されたユーザアクセスデータから学習された組織構造を用いて不必要なデータアクセス許可を除去できる。アルゴリズムは現在のＡＣＬに基づいており、次のごとく各ユーザデータグループに対して別個に動作する。まず、各ユーザに対して対によって定義されたデータ要素の１つに対するアクセスが記録されたか否かをチェックする。記録されていなければ、相似ユーザが登録期間（enrollment period）内にデータ要素をアクセスしたか否かをチェックする。ここで、相似は上述と同一の意味を有する。そのようなユーザがいなければ、特別のユーザが近い将来そのデータ要素にアクセスする必要はないといえる。また、これがデータグループにおいて現れるデータ要素の場合、アクセス制御対からユーザを除去する。以下に説明するごとく、プロセスの第２段階を適用してアクセス制御対からデータ要素を除去する。
【００７７】
次に、本発明の開示された実施の形態に係る部分的に監督されたファイルアクセス制御方法を示すフローチャートである図６を参照する。この方法のステップは明確にするために図６に例示のシーケンスとして示されている。しかしながら、当業者においては、これらのステップが部分的に非同期に実行され、もしくは異なる順序で実行できることは明らかである。

【００７８】
この方法は初期ステップ１０４にて開始する。図４、図５を参照して上述したバイクラスタリング方法が実行され適用される。
【００７９】
次に、ステップ１０６において、アクセス制御ユニットがＡＣＬから選択される。このユニットはユーザグループ及びディレクトリグループよりなる対である。
【００８０】
次に、ステップ１０８において、現在アクセス制御ユニットのユーザから１つのユーザを選択する。
【００８１】
次に、ステップ１１０において、現在アクセス制御ユニットから１つのデータ要素を選択する。
【００８２】
次に、制御は決定ステップ１１２に進み、現在ユーザは現在データ要素をアクセスしたことがあるか否かを判別する。
【００８３】
決定ステップ１１２の判別が肯定的である場合、ＡＣＬの修正は現在ユーザについては必要ない。制御は以下に説明するステップ１１４に進む。
【００８４】
決定ステップ１１２の判別が否定的である場合、（初期ステップ１０４で実行されたクラスタリング手続において）現在ユーザと相似であると判別されたユーザが評価される。制御はステップ１１６に進む。相似ユーザが選択される。
【００８５】
次に、制御は決定ステップ１１８に進み、現在相似ユーザが現在データ要素をアクセスしたことがあるか否かを判別する。
【００８６】
決定ステップ１１８の判別が肯定的である場合、現在ユーザと現在相似ユーザとのアクセス相似性に基づき、現在ユーザについてＡＣＬの修正はなされない。制御はステップ１１４に進む。
【００８７】
決定ステップ１１８の判別が否定的である場合、決定ステップ１２０においてまだ考慮すべき相似ユーザが存在するか否かを判別する。
【００８８】
決定ステップ１２０の判別が肯定的である場合、制御はステップ１１６に戻る。
【００８９】
決定ステップ１２０の判別が否定的である場合、ステップ１２２において、現在ユーザが現在アクセス制御ユニットから取除かれる。
【００９０】
次に、決定ステップ１２４において、現在アクセス制御ユニットに評価すべきユーザが残っているか否かを判別する。決定ステップ１２４の判別が肯定的である場合、制御はステップ１０８に戻る。
【００９１】
決定ステップ１２４の判別が否定的である場合、評価すべきアクセス制御ユニットが残っているか否かを判別する。決定ステップ１２６の判別が肯定的である場合、制御はステップ１０６に戻り、新しい繰返しを開始する。
【００９２】
決定ステップ１２６の判別が否定的である場合、制御は最終ステップ１２８に進む。次に、記憶アクセス制御は修正されたＡＣＬを導入することができる。
【００９３】
上述のステップ１１４は現在アクセス制御ユニットの現在データ要素の状況に関するア

ルゴリズムの段階を開始する。この段階は現在ユーザも、この相似ユーザも現在データ要素にアクセスしていなかったときのみ実行される。以下のステップの目的は（初期ステップにおいて実行されたクラスタリング手続による）現在データ要素に相似すべきと考えられるデータ要素が現在のアクセス制御ユニットのいずれかのユーザによってアクセスされていたか否かを判別することにある。アクセスされていなければ、現在データ要素は現在アクセス制御ユニットから取除かれる。この動作が一旦達成されると、その後、現在ユーザグループのメンバは現在データ要素にアクセスできない。１つの相似データ要素が初期ステップ１０４において実行されたクラスタリングから選択される。

【００９４】

次に、ステップ１３０において、再び、現在アクセス制御ユニットのユーザから１つのユーザを選択する。これは、現在アクセス制御ユニットのすべてのユーザをステップ１３０の繰返しによって評価対象にするためである。

【００９５】

次に、制御は決定ステップ１３２に進み、現在ユーザは現在相似データ要素をアクセスしたことがあるか否かを判別する。決定ステップ１１２の判別が肯定的である場合、現在データ要素をそのアクセス制御ユニットから取除く必要はない。制御は以下に説明するステップ１２４に進む。

【００９６】

決定ステップ１３２の判別が否定的である場合、決定ステップ１３４において、現在アクセス制御ユニットにユーザが残っているか否かを判別する。決定ステップ１３４の判別が肯定的である場合、制御はステップ１３０に戻る。

【００９７】

決定ステップ１３４の判別が否定的である場合、決定ステップ１３６において、現在アクセス制御ユニットのユーザに対してテストすべき相似データ要素が残っているか否かを判別する。

【００９８】

決定ステップ１３６の判別が肯定的である場合、制御はステップ１１４に戻る。

【００９９】

決定ステップ１３６の判別が否定的である場合、現在アクセス制御ユニットのすべてのユーザが（ステップ１１０の最後の繰返しで選択された）現在データ要素に相似するすべてのデータ要素に対してアクセステストが実行されたか否かを判別する。アクセスは発見できない。ステップ１３７において、現在データ要素が現在アクセス制御ユニットから取除かれる。

【０１００】

次に、制御は決定ステップ１３８に進み、現在アクセス制御ユニットにデータ要素が残っているか否かを判別する。決定ステップ１３８の判別が肯定的である場合、制御はステップ１１０に戻り、現在アクセス制御ユニットから異なるデータ要素を用いて新しい繰返しを開始する。

【０１０１】

決定ステップ１３８の判別が否定的である場合、制御は既に説明した決定ステップ１２４に進む。

【０１０２】

［提案ポリシの検証のための仮想コミット］

図１に戻ると、上述のクラスタリング手順はシステムの登録期間もしくは訓練期間に収集された記憶アクセスに適用される。これらの手順は、時にたとえば、下部組織における買収、合併の後に実行される。提案または仮新規もしくは更新されたアクセス制御ポリシは登録期間の後で発生するユーザ活動の見地から有効であることを保証することが望ましい。登録期間の後に収集されたデータを用いて設定前の仮ポリシの有効性を検証する。この機能はコミットモジュール３０によって実行され、コミットモジュール３０はユーザアクセス活動を記録し、仮ポリシの違反を検出する。ユーザ活動が仮ポリシに違反していな

ければ、仮ポリシは確定的記憶アクセス制御ポリシとして承認される。違反していれば、仮ポリシは拒否もしくは、さらなる評価もしくは改訂のために戻される。このように、コミットモジュール３０は交差有効機構を提供し、提案された記憶アクセス制御ポリシの品質をその実現前にチェックする。

【０１０３】

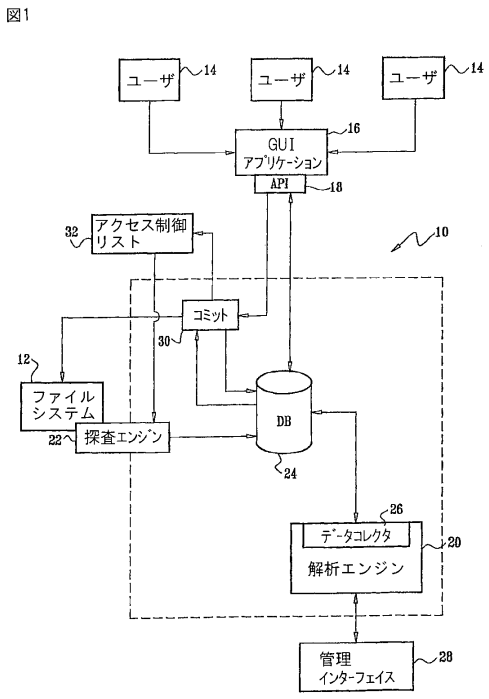
［異常行動の追跡］

記録データに実行されるデータ解析の主な目的は異常行動の検出及び追跡である。コミットユニット３０は記憶アクセス制御実行後に、この機能を実行するのに適している。ユーザが同一ユーザクラスタに属している他のユーザと不一致の行動をした場合に、異常行動が確認できる。

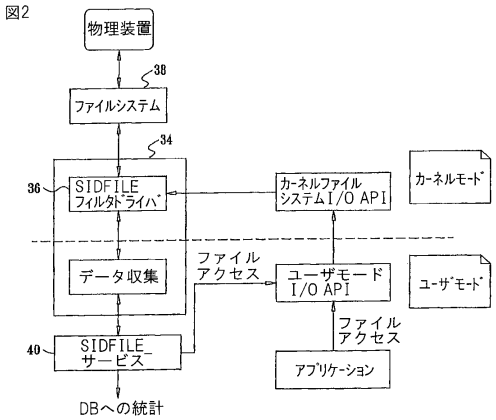
【０１０４】

当業者において、本発明は上述の特別なものに限定されるものではない。また、本発明の範囲は上述の特徴のコンビネーション及びサブコンビネーションを含むと共に、従来にないこれらの変更、修正は上述の説明を読んだ当業者に可能である。

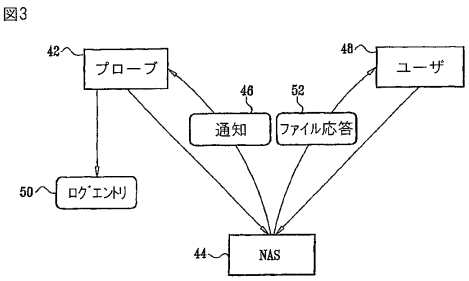
【図１】



【図２】

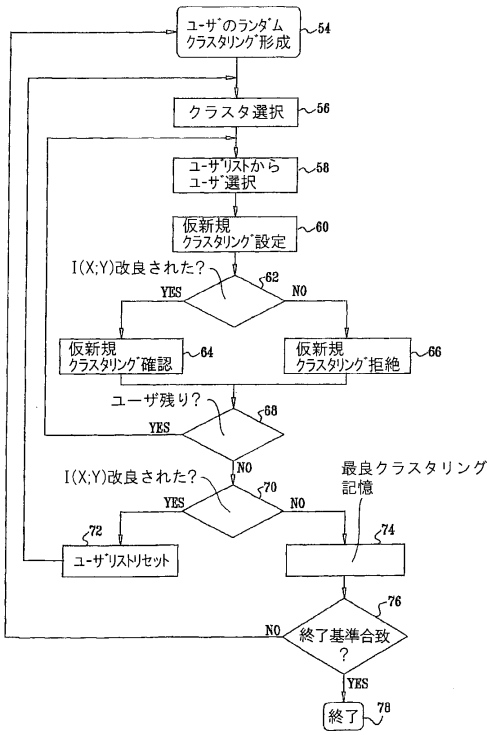


【図３】



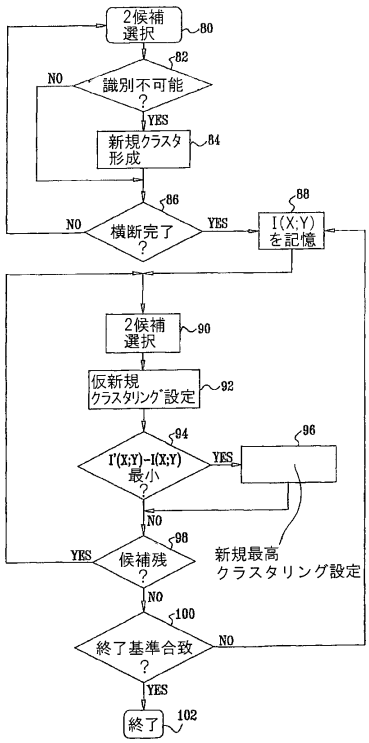
【図４】

図4



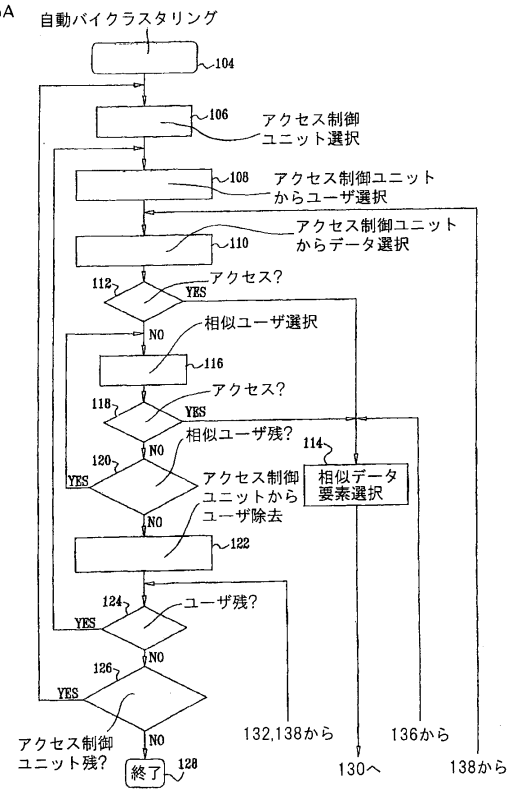
【図５】

図5



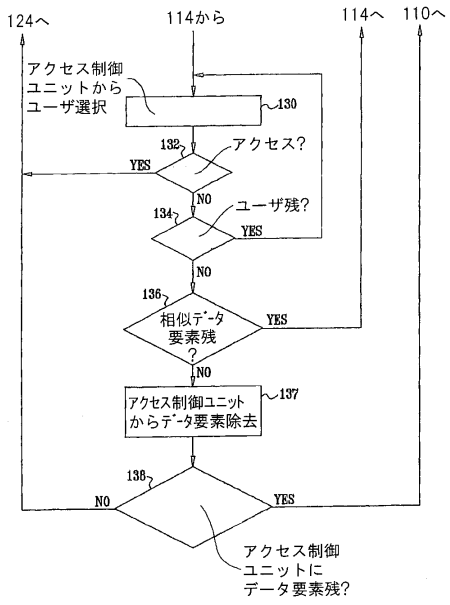
【図６Ａ】

図6A



【図６Ｂ】

図6B



フロントページの続き

(72)発明者　フェイテルソン，ヤコブ
イスラエル国，４４８１４　エルカナ，ミショル　ハサピル　ストリート　３
(72)発明者　ゴールドバーガー，ヤコブ
イスラエル国，６２２６６　テルーアビブ，シュロムジオン　ストリート　４０／９
(72)発明者　コルクス，オハド
イスラエル国，６４９２２　テルーアビブ，アルロゾロブ　ストリート　１５５／８

審査官　和田　財太

(56)参考文献　国際公開第２００４／０２７７０５（WO，Ａ１）
内部情報漏えい対策ツール８製品　データベースのデータの変化やアクセスを監視　ＩＰＬｏｃｋｓ－ＤＳＡＳ，Ｎ＋Ｉ　ＮＥＴＷＯＲＫ，日本，ソフトバンクパブリッシング株式会社，２００３年１１月　１日，第３巻，第１０号，ｐ．１２２

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２０－２１／２４
Ｇ０６Ｆ　１２／００
Ｇ０９Ｃ　１／００