【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成23年10月20日(2011.10.20)

【公表番号】特表2009-500697(P2009-500697A)
【公表日】平成21年1月8日(2009.1.8)
【年通号数】公開・登録公報2009-001
【出願番号】特願2008-515373(P2008-515373)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｇ０６Ｆ　21/20　　(2006.01)
Ｇ０９Ｃ　 1/00　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５２０Ｃ
Ｇ０６Ｆ　15/00　　３３０Ｄ
Ｇ０９Ｃ　 1/00　　６６０Ｄ

【誤訳訂正書】
【提出日】平成23年8月30日(2011.8.30)
【誤訳訂正１】
【訂正対象書類名】特許請求の範囲
【訂正対象項目名】全文
【訂正方法】変更
【訂正の内容】
【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】
１つの前記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複数のユーザのうちの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、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】
１つの前記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１つの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１つの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

前記記憶要素へのアクセスを可能とする、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４】
さらに、
前記バイクラスタステップに応答して、前記解析エンジンが、前記ファイルシステムの構造を導出するステップを具備する、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５】
さらに、
前記バイクラスタステップに応答して、前記解析エンジンが、前記複数のユーザによる前記ファイルシステムの使用パターンを導出するステップを具備する、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６】
さらに、
コミットモジュールが、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、請求項５に記載のデータ記憶アクセスの制御方法。
【請求項７】
前記バイクラスタステップは繰返して実行され、前記アクセスプロファイル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、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８】
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、前記制御ポリシの暫定版を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、
を具備する、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９】
さらに、
管理インターフェイスが、前記制御ポリシを対話形式で修正するステップを具備する、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１０】
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乃至９のいずれか一項に記載のデータ記憶アクセスの制御方法。
【請求項１１】
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る、コンピュータソフトウェア製品。
【請求項１２】
１つの前記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複数のユーザのうちの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、請求項１１に記載のコンピュータソフトウェア製品。
【請求項１３】
１つの前記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１つの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１つの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へのアクセスを可能とする、請求項１１に記載のコンピュータソフトウェア製品。
【請求項１４】
前記バイクラスタステップは繰返して実行され、前記アクセスプロファイル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、請求項１１に記載のコンピュータソフトウェア製品。
【請求項１５】
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、前記制御ポリシの暫定版を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、請求項１１に記載のコンピュータソフトウェア製品。
【請求項１６】
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１１乃至１５のいずれか一項に記載のコンピュータソフトウェア製品。
【請求項１７】
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る、データ記憶アクセスの制御装置。
【請求項１８】
１つの前記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複数のユーザのうちの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、請求項１７に記載のデータ記憶アクセスの制御装置。
【請求項１９】
１つの前記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１つの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１つの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へのアクセスを可能とする、請求項１７に記載のデータ記憶アクセスの制御装置。
【請求項２０】
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、前記制御ポリシの暫定版を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、請求項１７に記載のデータ記憶アクセスの制御装置。
【請求項２１】
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１７乃至２０のいずれか一項に記載のデータ記憶アクセスの制御装置。

【誤訳訂正２】
【訂正対象書類名】明細書
【訂正対象項目名】００２８
【訂正方法】変更
【訂正の内容】
【００２８】
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。
【誤訳訂正３】
【訂正対象書類名】明細書
【訂正対象項目名】００３１
【訂正方法】変更
【訂正の内容】
【００３１】
［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。
【誤訳訂正４】
【訂正対象書類名】明細書
【訂正対象項目名】００３３
【訂正方法】変更
【訂正の内容】

【００３３】
［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。
【誤訳訂正５】
【訂正対象書類名】明細書
【訂正対象項目名】００３５
【訂正方法】変更
【訂正の内容】
【００３５】
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。
【誤訳訂正６】
【訂正対象書類名】明細書
【訂正対象項目名】００３８
【訂正方法】変更
【訂正の内容】
【００３８】
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。
【誤訳訂正７】
【訂正対象書類名】明細書
【訂正対象項目名】００４２
【訂正方法】変更
【訂正の内容】
【００４２】
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。
【誤訳訂正８】
【訂正対象書類名】明細書
【訂正対象項目名】００４７
【訂正方法】変更
【訂正の内容】
【００４７】
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。
【誤訳訂正９】
【訂正対象書類名】明細書
【訂正対象項目名】００４８
【訂正方法】変更
【訂正の内容】
【００４８】
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。
【誤訳訂正１０】
【訂正対象書類名】明細書
【訂正対象項目名】００５７
【訂正方法】変更
【訂正の内容】
【００５７】
［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。

【誤訳訂正１１】
【訂正対象書類名】明細書
【訂正対象項目名】００５８
【訂正方法】変更
【訂正の内容】
【００５８】
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。

【誤訳訂正１２】
【訂正対象書類名】明細書
【訂正対象項目名】００６１
【訂正方法】変更
【訂正の内容】
【００６１】
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。

【誤訳訂正１３】
【訂正対象書類名】明細書
【訂正対象項目名】００６２
【訂正方法】変更
【訂正の内容】
【００６２】
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。

【誤訳訂正１４】
【訂正対象書類名】明細書
【訂正対象項目名】００６３
【訂正方法】変更
【訂正の内容】
【００６３】
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。

【誤訳訂正１５】
【訂正対象書類名】明細書
【訂正対象項目名】００６４

【訂正方法】変更
【訂正の内容】
【００６４】
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。
【誤訳訂正１６】
【訂正対象書類名】明細書
【訂正対象項目名】００７２
【訂正方法】変更
【訂正の内容】
【００７２】
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。
【誤訳訂正１７】
【訂正対象書類名】明細書
【訂正対象項目名】００７４
【訂正方法】変更
【訂正の内容】
【００７４】
［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。
【誤訳訂正１８】
【訂正対象書類名】明細書

【訂正対象項目名】００９０
【訂正方法】変更
【訂正の内容】
【００９０】
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。
【誤訳訂正１９】
【訂正対象書類名】明細書
【訂正対象項目名】０１００
【訂正方法】変更
【訂正の内容】
【０１００】
［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。
【誤訳訂正２０】
【訂正対象書類名】図面
【訂正対象項目名】図６Ａ
【訂正方法】変更
【訂正の内容】

【図６Ａ】

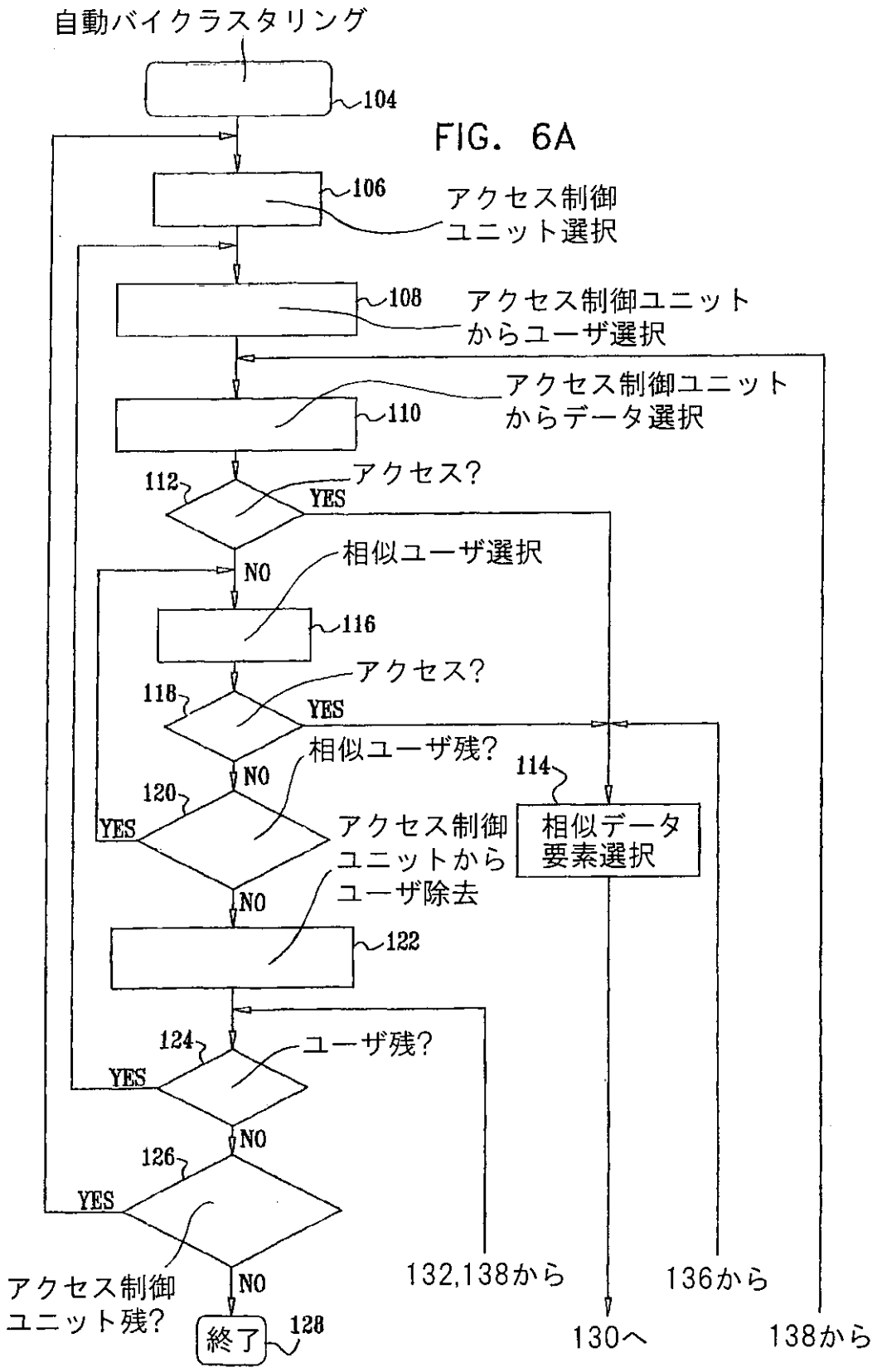
自動バイクラスタリング
104
106
アクセス制御
ユニット選択
108
アクセス制御ユニット
からユーザ選択
110
アクセス制御ユニット
からデータ選択
112
アクセス?
YES
NO
相似ユーザ選択
116
118
アクセス?
YES
NO
相似ユーザ残?
120
YES
NO
アクセス制御
ユニットから
ユーザ除去
122
114
相似データ
要素選択
124
ユーザ残?
YES
NO
126
YES
NO
アクセス制御
ユニット残?
終了
128
132,138から
136から
130へ
138から

FIG. 6A