(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2005-259140
(P2005-259140A)
(43)公開日　平成17年9月22日(2005.9.22)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06F 12/14	G06F	12/14　560B	5B017

審査請求 未請求　請求項の数 30　ＯＬ　（全 43 頁）

(21)出願番号　特願2005-64244(P2005-64244)
(22)出願日　平成17年3月8日(2005.3.8)
(31)優先権主張番号　10/796932
(32)優先日　平成16年3月9日(2004.3.9)
(33)優先権主張国　米国(US)

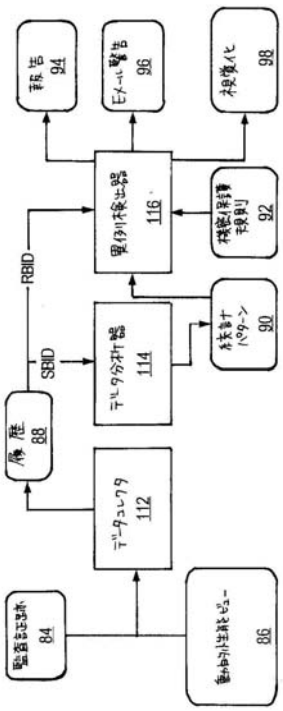
（特許庁注：以下のものは登録商標）
１．リナックス
２．Ｌｉｎｕｘ

(71)出願人　504317879
アイピーロックス・インコーポレイテッド
アメリカ合衆国、９５１３１　カリフォルニア州、サン・ノゼ、ウェスト・トリンブル・ロード、４４１・エイ
(74)代理人　100064746
弁理士　深見　久郎
(74)代理人　100085132
弁理士　森田　俊雄
(74)代理人　100083703
弁理士　仲村　義平
(74)代理人　100096781
弁理士　堀井　豊
(74)代理人　100098316
弁理士　野田　久登

最終頁に続く

(54)【発明の名称】データベースを監視するための方法、命令の１つ以上のシーケンスを保持するコンピュータ読み取り可能な媒体、および装置

(57)【要約】
【課題】　異例のアクティビティについてデータベースシステムを監視するための手法を提供する。
【解決手段】　監視中の対象データベースに関するユーザ挙動情報は、異例のアクティビティを検出するために、自動的に収集され、分析され、１つ以上の方針と比較される。実施例は、対象データベースに関するユーザ挙動データを、監査証跡および動的ビューを含むさまざまなソースから、データベースのデータベース管理システムと連携して収集する。実施例は、異例のデータベースアクティビティを検出するために、統計ベースの侵入検出（ＳＢＩＤ）および規則ベースの侵入検出（ＲＢＩＤ）のうちの１つ以上を採用する。正規の使用パターンから逸脱する不審なデータベースアクセスが検出されると、責任を有する機密保護担当者への警告、報告生成、ｅメール警告などの目標とされる動作が行なわれる。
【選択図】　図２



【特許請求の範囲】
【請求項１】
データベースを監視するための方法であって、
１人以上のユーザが前記データベースをどのように使用するかを示すユーザ挙動データを収集するステップと、
前記データを履歴データとして処理し、記憶するステップと、
挙動パターンを決定するために前記履歴データを分析するステップと、
１人以上のユーザが前記データベースをどのように使用したかを示す新しい１組のデータを受信するステップと、
前記新しい１組のデータと前記挙動パターンとの比較を行なうステップと、
前記比較に基づき、前記新しい１組のデータが１組の基準を満たすかどうかを判断するステップと、
前記新しい１組のデータが前記１組の基準を満たす場合、前記新しい１組のデータは異例の活動を表わしていると判断するステップと、
目標とされる動作を行なうことによって前記判断に応じるステップとを含む、データベース監視するための方法。
【請求項２】
前記新しい１組のデータが規則ベースの方針に違反しているかどうかを判断するステップと、
前記新しい１組のデータが前記規則ベースの方針に違反している場合、前記新しい１組のデータは異例の活動を表わしていると判断するステップとをさらに含む、請求項１に記載の方法。
【請求項３】
ユーザ挙動データを収集するステップは、データベースマネージャの監査証跡または動的性能ビューから情報を読出すステップをさらに含む、請求項２に記載の方法。
【請求項４】
ユーザ挙動データを収集するステップは、監視レベルで、
１つ以上の選択されたデータベースオブジェクトについてのデータベースアクセスに関する情報、
１人以上の選択されたデータベースユーザについてのデータベースアクセスに関する情報、および、
１つ以上の選択されたデータベースユーザセッションについてのデータベースアクセスに関する情報のうちの少なくとも１つから選択される情報を収集するステップをさらに含む、請求項３に記載の方法。
【請求項５】
ユーザ挙動データを収集するステップは、
監視されるべき情報の種類を受信するステップと、
前記情報の種類から監視レベルを決定するステップと、
決定された前記監視レベルに基づいて前記データベースマネージャの監視オプションを起動するステップとをさらに含む、請求項３に記載の方法。
【請求項６】
挙動パターンを決定するために前記履歴データを分析するステップは、前記履歴データから統計的モデルを決定するステップをさらに含む、請求項２に記載の方法。
【請求項７】
前記履歴データから統計的モデルを決定するステップは、
前記履歴データからデータベースアクセスの頻度を決定するステップと、
データベースアクセスの頻度についての確率関数を決定するステップと、
前記確率関数から累積確率関数を決定するステップとをさらに含む、請求項６に記載の方法。
【請求項８】

前記新しい１組のデータと前記挙動パターンとの比較を行なうステップは、前記統計的モデルに対して前記新しい１組のデータを用いて仮説を検証するステップをさらに含む、請求項７に記載の方法。

【請求項９】

前記統計的モデルに対して前記新しい１組のデータを用いて仮説を検証するステップは、

前記新しい１組のデータについてのデータベースアクセスの頻度を決定するステップと、

防護基準および確率関数パラメータからしきい値を決定するステップとをさらに含む、請求項８に記載の方法。

【請求項１０】

前記統計的モデルパターンに対して前記新しい１組のデータを用いて仮説を検証するステップは、前記新しい１組のデータについてのデータベースアクセスの頻度を前記しきい値と比較するステップをさらに含む、請求項９に記載の方法。

【請求項１１】

履歴情報は１つ以上の選択されたデータベースオブジェクトについてのデータベースアクセスに関するものであり、前記履歴データからデータベースアクセスの頻度を決定するステップは、

１日の時間別のオブジェクトアクセス頻度、１日の時間およびオペレーティングシステムユーザ別のオブジェクトアクセス頻度、１日の時間およびデータベースユーザ別のオブジェクトアクセス頻度、１日の時間および場所別のオブジェクトアクセス頻度、１日の時間およびオペレーティングシステムユーザ、データベースユーザならびに場所のうちの少なくとも２つの組合せ別のオブジェクトアクセス頻度のうちの少なくとも１つの頻度を決定するステップをさらに含む、請求項７に記載の方法。

【請求項１２】

履歴情報は１つ以上の選択されたデータベースユーザについてのデータベースアクセスに関するものであり、前記履歴データからデータベースアクセスの頻度を決定するステップは、

１日の時間別のユーザアクセス頻度、１日の時間およびオペレーティングシステムユーザ別のユーザアクセス頻度、１日の時間およびデータベースユーザ別のユーザアクセス頻度、１日の時間および場所別のユーザアクセス頻度、１日の時間およびオペレーティングシステムユーザ、データベースユーザならびに場所のうちの少なくとも２つの組合せ別のユーザアクセス頻度のうちの少なくとも１つの頻度を決定するステップをさらに含む、請求項７に記載の方法。

【請求項１３】

履歴情報は１つ以上の選択されたデータベースユーザセッションについてのデータベースアクセスに関するものであり、前記履歴データからデータベースアクセスの頻度を決定するステップは、

セッションごとのページ読出の数、セッションごとのアクセス期間、時間単位ごとのページ読出の数のうちの少なくとも１つの頻度を決定するステップをさらに含む、請求項７に記載の方法。

【請求項１４】

目標とされる動作を行なうステップは、警告を発するステップ、ｅメールを送信するステップ、報告を生成するステップ、視覚化を行なうステップのうちの少なくとも１つを含む、請求項１に記載の方法。

【請求項１５】

装置の障害に応じて回復設定へ戻るための命令の１つ以上のシーケンスを保持するコンピュータ読み取り可能な媒体であって、前記命令は、１つ以上のプロセッサによって実行される際、前記１つ以上のプロセッサに、

１人以上のユーザがデータベースをどのように使用するかを示すユーザ挙動データを収

集するステップと、
前記データを履歴データとして処理し、記憶するステップと、
挙動パターンを決定するために前記履歴データを分析するステップと、
１人以上のユーザが前記データベースをどのように使用したかを示す新しい１組のデータを受信するステップと、
前記新しい１組のデータと前記挙動パターンとの比較を行なうステップと、
前記比較に基づき、前記新しい１組のデータが１組の基準を満たすかどうかを判断するステップと、
前記新しい１組のデータが前記１組の基準を満たす場合、前記新しい１組のデータは異例の活動を表わしていると判断するステップと、
目標とされる動作を行なうことによって前記判断に応じるステップとを実行させる、命令の１つ以上のシーケンスを保持するコンピュータ読み取り可能な媒体。
【請求項１６】
前記１つ以上のプロセッサによって実行される際、前記１つ以上のプロセッサに、
前記新しい１組のデータが規則ベースの方針に違反しているかどうかを判断するステップと、
前記新しい１組のデータが前記規則ベースの方針に違反している場合、前記新しい１組のデータは異例の活動を表わしていると判断するステップとを実行させる命令をさらに含む、請求項１５に記載のコンピュータ読み取り可能な媒体。
【請求項１７】
ユーザ挙動データを収集するステップを実行するための命令は、データベースマネージャの監査証跡から情報を読出すステップを実行するための命令をさらに含む、請求項１６に記載のコンピュータ読み取り可能な媒体。
【請求項１８】
ユーザ挙動データを収集するステップを実行するための命令は、
１つ以上の選択されたデータベースオブジェクトについてのデータベースアクセスに関する情報、
１人以上の選択されたデータベースユーザについてのデータベースアクセスに関する情報、および、
１つ以上の選択されたデータベースユーザセッションについてのデータベースアクセスに関する情報のうちの少なくとも１つから選択される情報を監視レベルで収集するステップを実行するための命令をさらに含む、請求項１７に記載のコンピュータ読み取り可能な媒体。
【請求項１９】
ユーザ挙動データを収集するステップを実行するための命令は、
監視されるべき情報の種類を受信するステップと、
前記情報の種類から監視レベルを決定するステップと、
決定された前記監視レベルに基づいて前記データベースマネージャの監視オプションを起動するステップとを実行するための命令をさらに含む、請求項１７に記載のコンピュータ読み取り可能な媒体。
【請求項２０】
挙動パターンを決定するために前記履歴データを分析するステップを実行するための命令は、前記履歴データから統計的モデルを決定するステップを実行するための命令をさらに含む、請求項１６に記載のコンピュータ読み取り可能な媒体。
【請求項２１】
前記履歴データから統計的モデルを決定するステップを実行するための命令は、
前記履歴データからデータベースアクセスの頻度を決定するステップと、
データベースアクセスの頻度についての確率関数を決定するステップと、
前記確率関数から累積確率関数を決定するステップとを実行するための命令をさらに含む、請求項２０に記載のコンピュータ読み取り可能な媒体。

【請求項２２】
前記新しい１組のデータと前記挙動パターンとの比較を行なうステップを実行するための命令は、前記統計的モデルに対して前記新しい１組のデータを用いて仮説を検証するステップを実行するための命令をさらに含む、請求項２１に記載のコンピュータ読み取り可能な媒体。
【請求項２３】
前記統計的モデルに対して前記新しい１組のデータを用いて仮説を検証するステップを実行するための命令は、
前記新しい１組のデータについてのデータベースアクセスの頻度を決定するステップと、
防護基準および確率関数パラメータからしきい値を決定するステップとを実行するための命令をさらに含む、請求項２２に記載のコンピュータ読み取り可能な媒体。
【請求項２４】
前記統計的モデルに対して前記新しい１組のデータを用いて仮説を検証するステップを実行するための命令は、前記新しい１組のデータについてのデータベースアクセスの頻度を前記しきい値と比較するステップを実行するための命令をさらに含む、請求項２３に記載のコンピュータ読み取り可能な媒体。
【請求項２５】
履歴情報は１つ以上の選択されたデータベースオブジェクトについてのデータベースアクセスに関するものであり、前記履歴データからデータベースアクセスの頻度を決定するステップを実行するための命令は、
１日の時間別のオブジェクトアクセス頻度、１日の時間およびオペレーティングシステムユーザ別のオブジェクトアクセス頻度、１日の時間およびデータベースユーザ別のオブジェクトアクセス頻度、１日の時間および場所別のオブジェクトアクセス頻度、１日の時間およびオペレーティングシステムユーザ、データベースユーザならびに場所のうちの少なくとも２つの組合せ別のオブジェクトアクセス頻度のうちの少なくとも１つの頻度を決定するステップを実行するための命令をさらに含む、請求項２１に記載のコンピュータ読み取り可能な媒体。
【請求項２６】
履歴情報は１つ以上の選択されたデータベースユーザについてのデータベースアクセスに関するものであり、前記履歴データからデータベースアクセスの頻度を決定するステップを実行するための命令は、
１日の時間別のユーザアクセス頻度、１日の時間およびオペレーティングシステムユーザ別のユーザアクセス頻度、１日の時間およびデータベースユーザ別のユーザアクセス頻度、１日の時間および場所別のユーザアクセス頻度、１日の時間およびオペレーティングシステムユーザ、データベースユーザならびに場所のうちの少なくとも２つの組合せ別のユーザアクセス頻度のうちの少なくとも１つの頻度を決定するステップを実行するための命令をさらに含む、請求項２１に記載のコンピュータ読み取り可能な媒体。
【請求項２７】
履歴情報は１つ以上の選択されたデータベースユーザセッションについてのデータベースアクセスに関するものであり、前記履歴データからデータベースアクセスの頻度を決定するステップを実行するための命令は、
セッションごとのページ読出の数、セッションごとのアクセス期間、時間単位ごとのページ読出の数のうちの少なくとも１つの頻度を決定するステップを実行するための命令をさらに含む、請求項２１に記載のコンピュータ読み取り可能な媒体。
【請求項２８】
目標とされる動作を行なうステップを実行するための命令は、警告を発するステップ、ｅメールを送信するステップ、報告を生成するステップ、視覚化を行なうステップのうちの少なくとも１つを実行するための命令を含む、請求項１５に記載のコンピュータ読み取り可能な媒体。

【請求項２９】
１人以上のユーザがデータベースをどのように使用するかを示すユーザ挙動データを収集するための手段と、
前記データを履歴データとして処理し、記憶するための手段と、
挙動パターンを決定するために前記履歴データを分析するための手段と、
１人以上のユーザが前記データベースをどのように使用したかを示す新しい１組のデータを受信するための手段と、
前記新しい１組のデータと前記挙動パターンとの比較を行なうための手段と、
前記比較に基づき、前記新しい１組のデータが１組の基準を満たすかどうかを判断するための手段と、
前記新しい１組のデータが前記１組の基準を満たす場合、前記新しい１組のデータは異例の活動を表わしていると判断するための手段と、
目標とされる動作を行なうことによって前記判断に応じるための手段とを含む、装置。
【請求項３０】
１人以上のユーザがデータベースをどのように使用するかを示すユーザ挙動データを収集し、前記データを履歴データとして処理して記憶し、１人以上のユーザが前記データベースをどのように使用したかを示す新しい１組のデータを受信するためのデータコレクタと、
挙動パターンを決定するために前記履歴データを分析するためのデータ分析器と、
前記新しい１組のデータと前記挙動パターンとの比較を行ない、前記比較に基づき、前記新しい１組のデータが１組の基準を満たすかどうかを判断し、前記新しい１組のデータが前記１組の基準を満たす場合、前記新しい１組のデータは異例の活動を表わしていると判断し、目標とされる動作を行なうことによって前記判断に応じるための異例分析器とを含む、装置。
【発明の詳細な説明】
【技術分野】
【０００１】
発明の分野
この発明はデータベースシステムを管理することに関する。特に、この発明はデータベースシステムを監視するための方法および装置に関する。
【背景技術】
【０００２】
背景
ネットワーク化されたシステムにおいてデータを保護することは重大である。ネットワークシステムが発展するにつれ、貴重なデータの機密保護を脅かすおそれがある状況の種類は数多く、かつ増加している。機密保護違反が起こった場合、それを検出できることが重要である。さもなければ、よくあることだが、データは将来における同様の種類の事象に無防備なままとなる。
【０００３】
ネットワーク管理者が貴重なデータを保護する際に直面する問題の種類は、たとえば、不正侵入攻撃、無断使用、インサイダー詐欺または誤用、および知的情報窃盗を含む。
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ネットワーク化されたシステムが遭遇する共通の問題のいくつかについて、異なるアプローチが開発されてきた。たとえば、ファイヤウォールおよび仮想プライベートネットワークは、ネットワーク化されたシステムを外部サイトからの無断アクセスから防護する。パスワードの使用または特権の指定を介するアクセス制御は、あるレベルの保護を提供する。しかしながら、ファイヤウォールおよび仮想プライベートネットワークは、データをインサイダー窃盗から保護することはできない。なぜなら、パスワードが盗まれるおそれ

があるためである。特権は管理が難しく、ユーザはしばしば自分の仕事の範囲外のデータにアクセス可能であり、機密保護は容易に破られ得る。

【０００５】

このセクションで説明するアプローチは、遂行可能なアプローチであるが、必ずしも、以前に考えられたかまたは遂行されたアプローチではない。したがって、他に指示がない限り、このセクションで説明するどのアプローチも、単にこのセクションに含まれるという理由で先行技術として適格であると仮定されるべきではない。

【課題を解決するための手段】

【０００６】

概要

この発明の実施例は、異例のアクティビティについてデータベースシステムを監視するための手法を提供する。監視中の対象データベースに関するユーザ挙動情報は、異例のアクティビティを検出するために、自動的に収集され、分析され、統計的に得られた標準および／または１つ以上の方針と比較され得る。実施例は、対象データベースに関するユーザ挙動データを、監査証跡および動的ビューを含むさまざまなソースから、データベースのデータベース管理システムと連携して収集する。実施例は、統計ベースの侵入検出（ＳＢＩＤ）および規則ベースの侵入検出（ＲＢＩＤ）の１つ以上を採用して、異例のデータベースアクティビティを検出する。統計ベースの侵入検出では、収集された情報は正規使用プロファイルを決定するために統計的プロファイリングを用いて分析される。規則ベースの侵入検出では、収集されたデータは明示的な機密保護規則と比較される。正規使用パターンから逸脱している不審なデータベースアクセスが検出された場合、責任を有する機密保護担当者に警告する、報告、ｅメール警告などを生成するといった、目標とされる動作が行なわれる。

【０００７】

一実施例では、データベースアクティビティについての履歴情報から正規使用パターンを決定するメカニズムが提供される。正規使用パターンから統計的に著しく逸脱しているデータベースアクセスは検出され、警告される。使用パターンの一例は、１日の時間別のデータベースアクセス頻度を含む。

【０００８】

一実施例では、ユーザが明示的な機密保護規則を特定できるようにするメカニズムが提供される。規則に違反しているデータベースアクセスは検出され、警告される。機密保護規則のいくつかの例は、不審なＯＳユーザまたは場所を含む。

【０００９】

一実施例では、データベースアクセス情報は、対象データベースを制御するデータベース管理システムによって提供される機能を用いて収集される。たとえば、データベース管理システムは監査証跡を提供してもよく、それはデータベースアクセスについての情報を含んでいる。データベース管理システムはまた、現在のユーザセッションおよびリソース利用といった現在のデータベース使用に関する情報を提供する動的性能ビューも提供する。この情報は、監査証跡から得られた情報とともに使用可能である。

【００１０】

実施例は、データベースオブジェクトレベル監視、データベースユーザレベル監視、およびデータベースセッションレベル監視を含む１つ以上のレベルでの監視を可能にする。データベースオブジェクトレベル監視は、ある特定のデータベースオブジェクトに焦点を合せる。データベースユーザレベル監視は、あるデータベースユーザに焦点を合せる。データベースセッションレベル監視は、あるデータベースログインセッションに焦点を合せる。実施例は、さまざまな侵入検出アプローチに基づいて、各監視レベルのためのさまざまな機密保護方針をサポート可能である。

【発明を実施するための最良の形態】

【００１１】

この発明を、添付図面の図において、限定のためではなく例示のために図示する。図中

、同様の参照符号は同様の要素を指す。

【００１２】

実施例の詳細な説明

概要

データベースを監視するための方法および装置を記載する。以下の記載では、説明のために、多数の特定の詳細が、この発明の完全な理解を提供するために述べられる。しかしながら、この発明がこれらの特定の詳細なしで実践されてもよいことは明らかである。他の点では、この発明を不必要に不明瞭にしないよう、周知の構造および装置はブロック図の形で示される。

【００１３】

図３Ａを参照すると、それは、この発明の一実施例に従った、データベースを監視するための方法を示している。図３Ａに示す方法は、１人以上のユーザがデータベースをどのように使用するかを示すユーザ挙動データを収集するステップ（ブロック３１０）を含む。図示された方法はさらに、データを履歴データとして処理し、記憶するステップ（ブロック３２０）を含む。挙動パターンを決定するために履歴データを分析するステップ（ブロック３３０）も、図示された方法の一部である。図示された方法はさらに、１人以上のユーザがデータベースをどのように使用したかを示す新しい１組のデータを受信するステップ（ブロック３４０）を含む。図示された方法はまた、新しい１組のデータと挙動パターンとの比較を行なうステップ（ブロック３５０）も含む。比較に基づき、新しい１組のデータが１組の基準を満たすかどうかを判断するステップ（ブロック３６０）も、図示された方法の一部である。図示された方法はまた、新しい１組のデータが１組の基準を満たす場合に、新しい１組のデータが異例のアクティビティを表わしていると判断するステップ（ブロック３７０）も含む。目標とされる動作を行なうことによって判断に応じるステップ（ブロック３８０）も、図示された方法に含まれていてもよい。

【００１４】

一実施例では、ユーザ挙動データを収集するステップは、データベースマネージャの監査証跡から情報を読出すステップをさらに含む。一実施例では、ユーザ挙動データを収集するステップはさらに、（１）１つ以上の選択されたデータベースオブジェクトについてのデータベースアクセスに関する情報、（２）１人以上の選択されたデータベースユーザについてのデータベースアクセスに関する情報、および（３）１つ以上の選択されたデータベースユーザセッションについてのデータベースアクセスに関する情報から選択された監視レベルで情報を収集するステップを含む。一実施例では、ユーザ挙動データを収集するステップはさらに、監視されるべき情報の種類を受信するステップと、情報の種類から監視レベルを決定するステップと、決定された監視レベルに基づいてデータベースマネージャ監査オプションを起動するステップとを含む。

【００１５】

一実施例では、挙動パターンを決定するために履歴データを分析するステップはさらに、履歴データから統計的モデルを決定するステップを含む。一実施例では、履歴データから統計的モデルを決定するステップはさらに、履歴データからデータベースアクセスの頻度を決定するステップと、データベースアクセスの頻度についての確率関数を決定するステップと、確率関数から累積確率関数を決定するステップとを含む。一実施例では、確率関数は、ポアソン確率分布、正規確率分布などであってもよい。

【００１６】

一実施例では、新しい１組のデータと挙動パターンとの比較を行なうステップはさらに、統計的モデルに対して新しい１組のデータを用いて仮説を検証するステップを含む。一実施例では、統計的モデルに対して新しい１組のデータを用いて仮説を検証するステップはさらに、新しい１組のデータについてのデータベースアクセスの頻度を決定するステップと、防護基準および確率関数パラメータからしきい値を決定するステップとを含む。一実施例では、統計的モデルパターンに対して新しい１組のデータを用いて仮説を検証するステップはさらに、新しい１組のデータについてのデータベースアクセスの頻度をしきい

値と比較するステップを含む。

【００１７】

履歴情報は、１つ以上の選択されたデータベースオブジェクトについてのデータベースアクセスに関する情報を含んでいてもよい。さまざまな実施例において、履歴データからデータベースアクセスの頻度を決定するステップは、１日の時間別のオブジェクトアクセス頻度、１日の時間およびオペレーティングシステムユーザ別のオブジェクトアクセス頻度、１日の時間およびデータベースユーザ別のオブジェクトアクセス頻度、１日の時間および場所別のオブジェクトアクセス頻度、１日の時間またはオペレーティングシステムユーザ、データベースユーザおよび場所のうちの少なくとも２つの組合せ別のオブジェクトアクセス頻度のうちの１つ以上の頻度を決定するステップのうちの１つ以上を含む。

【００１８】

履歴情報は、１つ以上の選択されたデータベースユーザについてのデータベースアクセスに関する情報を含んでいてもよい。さまざまな実施例において、履歴データからデータベースアクセスの頻度を決定するステップは、１日の時間別のユーザアクセス頻度、１日の時間およびオペレーティングシステムユーザ別のユーザアクセス頻度、１日の時間およびデータベースユーザ別のユーザアクセス頻度、１日の時間および場所別のユーザアクセス頻度、１日の時間またはオペレーティングシステムユーザ、データベースユーザおよび場所のうちの少なくとも２つの組合せ別のユーザアクセス頻度のうちの１つ以上の頻度を決定するステップのうちの１つ以上を含む。

【００１９】

履歴情報は、１つ以上の選択されたデータベースユーザセッションについてのデータベースアクセスに関する情報を含んでいてもよい。さまざまな実施例において、履歴データからデータベースアクセスの頻度を決定するステップは、セッションごとのページ読出の数、セッションごとのアクセス期間、または単位時間ごとのページ読出の数のうちの１つ以上の頻度を決定するステップのうちの１つ以上を含む。

【００２０】

さまざまな実施例において、目標とされる動作を行なうステップは、警告を発するステップ、ｅメールを送信するステップ、報告を作成するステップ、および視覚化を行なうステップのうちの１つ以上を含む。

【００２１】

一実施例では、新しい１組のデータが規則ベースの方針に違反しているかどうかを判断するステップが行なわれる。新しい１組のデータが規則ベースの方針に違反している場合、新しい１組のデータは異例のアクティビティを表わしていると判断される。一実施例では、異例のアクティビティは不審なアクティビティを含む。

【００２２】

他の点では、この発明の実施例は、前述のプロセスを実行するよう設定された装置およびコンピュータ読み取り可能な媒体を包含する。

【００２３】

用語

「データベース」は、ある編成に従ってデータを記憶するための使用される任意のデータ構造を含む。データベースは、リレーショナルデータベース、オブジェクトデータベース、階層型データベース、ネットワークデータベース、多次元データベースなどを含む。

【００２４】

「データベーストリガ」は、データベースオブジェクトに関与するある特定のイベントに応じて、たとえばテーブルまたはビューが選択または修正される場合にはいつでも、自動的に呼出される記憶されたデータベースプロシージャを指す。

【００２５】

「データベースセッション」は、ユーザプロセスを介した、ユーザのデータベースへの特定の接続を指す。セッションは、ユーザがデータベースアプリケーションに接続した時点から、ユーザがデータベースアプリケーションとの接続を排除するかまたはデータベー

スアプリケーションから出る時点まで続く。

【００２６】

「Java（登録商標）データベースコネクティビティ（ＪＤＢＣ）ＡＰＩ」は、ユーザがJava（登録商標）プログラミング言語からどのデータソースにもアクセスできるようにする、標準ＳＱＬデータベースアクセスインターフェイスである。

【００２７】

「ポアソン分布」は、イベント間の待機時間が指数的に分布している場合の間隔におけるイベントの数の確率分布である。

【００２８】

「監査証跡」は、コンピュータイベントの一連の記録である。それは、システムアクティビティを監視する監査システムによって生成される。記録は、コンピュータファイル、またはデータベーステーブルを含むもののこれらに限定されないさまざまな形で記憶されてもよい。

【００２９】

「特権」は、ネットワークまたはデータベースのユーザが実行を許可された１組のアクションまたは動作を指す。また、これに代えて、特権は、認可または１組の認可として言及されてもよい。

【００３０】

システム説明

図１は、一実施例においてデータベースを監視するための手法が実現され得るネットワークコンピューティングシステムの高レベル概要を示すブロック図である。図１に示す一実施例によれば、データベース監査エンジン１１０は、ユーザおよび／またはプロセスによるデータベース１３２へのアクセスの監視を提供するために、データベースサーバ１３０およびデータベース１３２から構成されるデータベースシステムにネットワーク１０６によって結合されている。一実施例では、ネットワーク１０６は、ファイヤウォール１２４およびルータ１２２を介してインターネット１０８に接続されている。ファイヤウォール１２４は、ネットワーク１０６および関連する構成要素を、インターネット１０８を越えて送信される有害なプログラムから保護するよう設定されている。ルータ１２２は、インターネット１０８とネットワーク１０６との間のネットワークトラフィックを管理し、制御する。

【００３１】

データベースサーバ１３０は、データベース１３２内のデータを保持する。データベース１３２内のデータの中には、ネットワーク１０６上の１人以上のユーザにとって重大なものもあるかもしれない。重大なデータは、監査記録、顧客口座情報および従業員給与情報を、例として、かつこれらに限定されずに含んでいてもよい。実施例によっては、データベース１３２はデータベース１３０の不可欠な部分であるかもしれない。アドミニストレータステーション１４４は、アドミニストレータがネットワーク１０６上で管理機能を行なうことができるようにする。管理機能は、ユーザのアクティビティを含め、ネットワーク１０６の機密保護を監視することを含んでいてもよい。実施例によっては、ネットワーク１０６に他の要素および構成要素（図１には図示せず）が接続されていてもよい。

【００３２】

一実施例では、データベース監査エンジン１１０は、データコレクタ１１２、データ分析器１１４および異例検出器１１６を含む。データコレクタ１１２は、データベース１３２にアクセスすることに関するユーザ挙動についてのデータを、データベースサーバ１３０から、指定された間隔で、または指定された条件（手動コマンドなど）の発生時に読出し、データを履歴データとして記憶するよう設定されている。データベース分析器１１４は、データコレクタ１１２によって記憶された履歴データに対して分析動作を行ない、データベース１３２にアクセスすることに関する挙動パターンを決定する。新規データが受信されると、異例検出器１１６は、新規データと履歴データから決定された挙動パターンとの比較に基づき、新規データが異例のアクティビティを表わしているかどうかを判断す

る。実施例の中には、データベース監査エンジン１１０が、データベースサーバ１３０の性能に顕著な影響を与えることなく、警告を収集し、分析し、信号で送る能力を提供するものもある。データコレクタ１１２、データ分析器１１４および異例検出器１１６によって行なわれる処理の一例のより詳細な説明を、図３Ａ～図３Ｅを参照して、以下に述べる。

【００３３】

図２は、一実施例における例示的なデータベース監査エンジンでの処理の高レベル概要を示すブロック図である。

【００３４】

一実施例では、データベース監査エンジン１１０は、データベースサーバとの干渉を低減するために、データベースサーバ１３０の外部で作動する。一実施例では、データコレクタ１１２は、たとえばデータベースサーバ１３０上でエージェントを実行する必要なく作動する。そのような実施例では、データコレクタ１１２は、ユーザ挙動に関する情報を、データベースサーバ１３０によって保持される監査証跡８４から収集し、および／または、データベース１３２への「読出専用」アクセスを採用してデータを収集する。一実施例では、データコレクタ１１２は、監視されるべき情報の種類に基づいて監視レベルを決定し、この監視レベルに基づいてデータベースマネージャ１３０の監査オプションを起動する。次に、データコレクタ１１２は、設定された監査オプションのためにデータベースサーバによって作成され保持された監査証跡を読出す。いくつかの実施例では、データコレクタは、ユーザセッション、および、データベース管理システム（ＤＢＭＳ）によって保持されているリソース利用といった、データベース使用についての情報を含む動的性能ビュー８６も含む。データコレクタ１１２は、監査証跡８４および動的性能ビュー８６から得たユーザ挙動データを、履歴データ８８として記憶する。ユーザ挙動データを収集し、それを履歴データとして記憶するための処理の一例のより詳細な説明を、図３Ｂを参照して以下に述べる。

【００３５】

データ分析器１１４は、データコレクタ１１２によって記憶された履歴データ８８に対して１つ以上の分析プロセスを実行する。一実施例では、データ分析器１１４は、履歴データ８８の分析を含む一連の動作を実行して挙動パターン９０を決定する。一実施例では、データ分析器１１４は、データベースアクセスの頻度を履歴データ８８から決定する。データベースアクセスの頻度は、１日の時間などの時間単位について計算されてもよい。次に、データ分析器１１４は、データベースアクセスの頻度についての確率関数を決定する。挙動パターンを決定するために履歴データを分析するための処理の一例のより詳細な説明を、図３Ｃを参照して以下に述べる。

【００３６】

新しい１組のデータがデータベースサーバ１３０から受信されると、異例検出器１１６は、この新しい１組のデータを、履歴データから決定された挙動パターンと比較する。異例検出器１１６は、新規データと履歴データ８８から決定された挙動パターンとの比較に基づき、新規データが異例のアクティビティを表わしているかどうかを判断する。一実施例では、異例検出器１１６は、規則ベースの侵入検出を行なうために、新規データを機密保護規則９２とも比較する。分析動作の１つ以上は、機密保護規則９２または他の規則と、データベースサーバ１３０のアドミニストレータまたはオペレータによって指定される条件との使用を必要とするかもしれない。機密保護規則９２は、機密保護違反が起こったかどうかを異例検出器１１６が判断できるようにするためのメカニズムを提供する。アドミニストレータステーション１４４は、機密保護規則９２の管理を可能にする。異例なデータが一旦識別されると、異例検出器１１６は目標とされる動作を行なう。たとえば、異例検出器１１６はｅメール警告９６を送信して、アドミニストレータステーション１４４に侵入を信号で知らせてもよい。異例検出器１１６はまた、または加えて、報告９４を提供するか、もしくは視覚化９８を作成してもよい。

【００３７】

一実施例では、データベース監査エンジン１１０は、あるイベントがいつ、データベースサーバ１３０によって保持されるデータに悪影響を与えるかを検出する。たとえば、データベース監査エンジン１１０は、インターネット１０８を越えてネットワーク１０６にアクセスする身元不明のユーザからの、データベースサーバにより保持されるデータの無断アクセスおよび／または操作を検出してもよい。データベース監査エンジン１１０はまた、ネットワーク１０６のユーザがいつ、データベースサーバ１３０によって記憶されたデータを故意にまたは意図せずに損なうかも判断してもよい。データベース監査エンジン１１０は、ネットワークを通って渡された「有害ソフト」の存在を、その有害ソフトがデータベースサーバ１３０により保持されるデータに影響を与える際に検出してもよい。データベースサーバ１３０に影響を与え、データベース監査エンジン１１０によって検出可能なイベントの他の例は、盗まれたパスワードを用いた無断アクセス、インサイダー詐欺、誤用、または特権濫用を含むもののこれらに限定されない。インサイダー詐欺の一例は、銀行の出納係による貴重な顧客口座情報の複製である。特権濫用の一例は、データベースアドミニストレータ（ＤＢＡ）による従業員給与情報へのアクセスである。

【００３８】

図３Ａは、一実施例におけるデータ収集、分析および異例検出処理の高レベル概要を示すフローチャートである。ブロック３１０で、ユーザ挙動データを含むデータセットがデータベースサーバから収集される。ブロック３２０で、ユーザ挙動データは履歴データとして記憶される。ブロック３３０で、履歴データは、挙動パターンを決定するために分析される。ブロック３４０で、データベースサーバから新しい１組のデータが受信される。ブロック３５０で、新しい１組のデータは挙動パターンと比較される。ブロック３６０で、比較に基づき、新しいデータセットが１組の基準を満たすかどうか、判断が下される。ブロック３７０で、新規データが異例のアクティビティを表わしているかどうか、判断が下される。ブロック３８０で、ブロック３７０によって異例のアクティビティが検出された場合には、目標とされる動作が行なわれる。目標とされる動作は、さまざまな実施例において、ｅメール警告を送信するステップ、報告を作成するステップ、視覚化を行なうステップなどのうちの１つ以上を含んでいてもよい。

【００３９】

データ収集

この発明の実施例は、データベースアクセスに関する情報を収集し、情報を内部データベースに履歴データとして記憶するためのさまざまな手法のうちの１つ以上を用いる。データベースアクセスに関する情報をデータベース管理システムから収集するさまざまな方法は、データベーストリガ、データベーストランザクション変更ログ、データベース監査機能、およびデータベース動的システムビューを含むもののこれらに限定されない。

【００４０】

監査機能は、さまざまな市販のデータベース管理システムによって提供されてもよい。この監査機能はさまざまなイベントを監査するよう設定可能である。監査機能は、データベースアクセス情報を含む監査証跡を生成する。通常、監査機能によって追跡されるデータベースアクセス情報はデータベース管理システムに依存するが、多くのデータベース管理システムは、ユーザ名、オブジェクト名、アクション、端末、タイムスタンプなどの監査情報の追跡を提供する。

【００４１】

商業的に入手可能なさまざまなデータベース管理システムはまた、動的システムビューも提供する。動的システムビューは、現在のユーザセッションおよびリソース利用に関する情報を提供する。たとえば、ある人気のあるデータベース管理システムは、機密保護に関連するいくつかの動的性能ビューを提供し、Ｖ＿＄ＳＥＳＳＩＯＮは各々の現在のユーザセッションについての情報を列挙し、Ｖ＿＄ＳＥＳＳ＿ＩＯは各ユーザセッションについてのＩ／Ｏ統計を列挙し、Ｖ＿＄ＳＥＳＳＴＡＴはユーザセッション統計を列挙し、Ｖ＿＄ＡＣＣＥＳＳは、現在ロックされているオブジェクトとそれらにアクセス中のセッションとを示し、Ｖ＿＄ＳＱＬは、ＳＱＬプールにおけるＳＱＬコマンドテキストを示して

いる。

【００４２】

通常は常駐記録である監査証跡と比較して、データベース動的ビューは通常、非常駐データを含む。データベース動的ビューは、データベースの定期的サンプリングをとることによって監視可能である。定期的サンプリングを用いるアプローチが監視間隔間で発生する或る不審なデータベースアクセスを検出し損なう、ということは起こり得る。この可能性を最小限に抑えるため、サンプリング間隔はかなり短くなるよう設定されてもよい。これに対し、監査アプローチは、監査される全イベントを、パージされるまで監査証跡に出現するよう提供する。また、動的ビューは、データベースアクセスに関する一般的な情報を比較的粗めの細分性で提供するが、一方、監査証跡は、比較的より詳細で特定の情報をデータベースオブジェクトレベルの細分性で提供する。一実施例では、動的ビューは、監査証跡が利用できない場合、たとえばデータベース監査機能がアクティブでない場合などに、補助情報として、または情報の代替的な源として使用可能である。

【００４３】

データベーストリガは、監視中のデータベースから情報を収集するための別の手法であり、それは、リアルタイム監視がデータベースのユーザによって侵入的すぎると考えられていないアプリケーションにおいて有用であり得る。データベーストランザクション再実行ログは、読出専用アクセスに関する情報が必要とされないアプリケーションにおいて有用であり得る、データ変更に関する情報を収集するためのさらに別の手法である。

【００４４】

図３Ｂは、一実施例におけるデータ収集処理の高レベル概要を示すフローチャートである。ブロック３１１で、監視されるべき情報の種類が受信される。ブロック３１２で、監視されるべき情報の種類に基づいて監視レベルが決定される。ブロック３１３で、監視レベルに基づいてデータベースマネージャの監査オプションが起動される。ブロック３１４で、データセットが監査証跡から読出される。ブロック３１５で、データセットは処理される。ブロック３１６で、読出すべきデータが他にないかどうかを判断するために検証が行なわれる。読出すべきデータが他にある場合、制御はブロック３１４に戻って続く。その他の場合、制御は呼出元に戻る。

【００４５】

データコレクタは、監査証跡または動的性能ビューからユーザ挙動データを収集し、情報を処理し、そのデータを履歴データとして記憶する。履歴データはたとえば内部データベースに保存可能である。一実施例では、対象となっている各アクションについて、さまざまな属性が履歴データに記憶される。たとえば、ＳＥＬＥＣＴまたはＬＯＧＩＮアクションは、（１）オペレーティングシステムユーザ識別子（ＯＳＵＳＥＲ）、（２）アクションを行なうユーザのデータベースユーザ識別子（ＤＢＵＳＥＲ）、（３）対象スキーマオブジェクト識別子（ＯＢＪＥＣＴ）、（４）オブジェクトのオーナー（ＯＷＮＥＲ）、（５）クライアントシステム識別子（ＬＯＣＡＴＩＯＮ）、（６）アクション識別子（ＡＣＴＩＯＮ）、（７）アクションの時点（ＴＩＭＥＳＴＡＭＰ）、（８）セッション用論理読出の数（ＲＥＡＤ）、（９）セッション用論理書込の数（ＷＲＩＴＥ）、および（１０）成功または失敗理由コード（ＲＥＴＵＲＮＣＯＤＥ）などの属性を含むものの、これらに限定されない。

【００４６】

データベースユーザ挙動監視は、たとえばデータベースオブジェクトレベル、データベースユーザレベル、およびデータベースセッションレベルを含む異なる焦点を各々有する異なる観点から実行可能である。

【００４７】

たとえば、一実施例では、データベースオブジェクトレベル監視は、選択された重大な、または敏感なデータベースオブジェクトについてデータベースアクセスを監視することを含む。データベースオブジェクトは、データベーステーブル、データベースビュー、または、データベースに記憶されたプロシージャであり得る。データベース監視は、このオ

ブジェクトがだれに、いつ、どこで、およびどのぐらいの頻度で任意のユーザによってアクセスされるかを追跡する。重大なデータベースオブジェクトの一例は、企業の「従業員」テーブルであり、それは従業員の給与情報を含んでいる。

【００４８】

別の例では、一実施例において、データベースユーザレベル監視は、選択されたデータベースユーザによるデータベースオブジェクトアクセスを監視することを含む。データベース監視は、このユーザが何に、いつ、どこで、およびどのくらいの頻度で任意のオブジェクトにアクセスするかを追跡する。選択されたデータベースユーザの一例は、データベースから情報を盗んだ疑いがかけられている、不満をもつ従業員であり得る。

【００４９】

さらに別の例では、一実施例において、データベースセッションレベル監視は、選択されたデータベースユーザによるデータベース接続またはログインセッションを監視することを含む。データベース監視は、このユーザによるログイン期間、ログイン失敗、およびリソース利用を追跡する。

【００５０】

一実施例では、データベースにおける１つ以上の異なる監査オプションが、データベース監査エンジンによって実行されるべき監視のレベルに基づいて自動的にイネーブルにされる。イネーブルにされた監査オプションは、対象データベースのデータベース管理システムに依存している。たとえば、一実施例では、データベースオブジェクトレベル監視をサポートするには、データベース監視システムは、ある特定のオブジェクトについてのオブジェクト監査を自動的にイネーブルにする。データベースユーザレベルまたはセッションレベル監視をサポートするには、このシステムは、ある特定のユーザについてのステートメント監査を自動的にイネーブルにする。

【００５１】

データ分析

この発明の実施例は、侵入検出データ分析への１つ以上のアプローチを実現してもよい。一実施例では、異例のデータベースアクセスを検出するために、統計ベースの侵入検出（ＳＢＩＤ）および規則ベースの侵入検出（ＲＢＩＤ）がともに用いられてもよい。統計ベースの侵入検出を用いる実施例では、ユーザ挙動情報の履歴の統計的分析が、ユーザ挙動パターンを生成するために行なわれる。これらのパターンから著しく逸脱するその後のどのデータベースアクセスも、異例のアクティビティを表わしていると判断される。規則ベースの侵入検出を用いる実施例は、方針としても知られる機密保護規則または制約から構成される知識ベースを維持する。方針に違反しているデータベースアクセスは、異例のアクティビティを表わしていると判断されてもよい。

【００５２】

図３Ｃは、一実施例において統計ベースの侵入検出を実現するデータ分析処理の高レベル概要を示すフローチャートである。ブロック３３１で、データベースアクセスの頻度が履歴データから決定される。履歴データに基づき、統計的モデルが構築され、異例なアクティビティの検出において使用するために妥当性を検証されてもよい。履歴データの統計的分析は、正規のデータベースアクセスレートを決定可能である。

【００５３】

ブロック３３２で、ブロック３３１で決定されたデータベースアクセスの頻度から、データベースアクセスの頻度についての確率関数が決定される。データベースアクセスの頻度は確率分布に適合可能である。特定の実施例では、正規確率分布またはポアソン確率分布などを含むもののこれらに限定されないさまざまな確率分布が使用されてもよい。

【００５４】

一例では、ユーザは昼間または夜間、一定のレートでランダムにデータベースにアクセスする。データベースアクセスのレートは、昼間と夜間とでは異なる場合がある。この１組の基準の下で、ポアソン分布を用いて、イベント間の時間が指数分布に従うデータベースアクセス頻度を記述してもよい。Ｘは間隔ごとのランダム発生の数、ｍは間隔ごとのラ

ンダム発生の平均数、Ｐは間隔内でｎ回発生するＸの確率とすると、以下のようになる。

【００５５】

【数１】

$$P(X=n)=e^{-m}\left[\frac{m^n}{n!}\right] \qquad (1)$$

【００５６】

ブロック３３３で、累積分布関数（ＣＤＦ：Cumulative Distribution Function）が決定可能である。ポアソン分布を用いる実施例では、累積分布関数は、式（２）に示すように、ｎよりも小さいかまたは等しい値を有するＸの確率を与える。

【００５７】

【数２】

$$F(n)=P(X<=n)=\sum_{i=0}^{n}e^{-m}\left[\frac{m^i}{i!}\right] \qquad (2)$$

【００５８】

データ分析器は、確率分布関数のパラメータ値を決定する。ポアソン分布の場合、それは、履歴データのための間隔ごとのランダム発生の平均数ｍの値である。

【００５９】

たとえば、発生はデータベースに対して発行されるＳＥＬＥＣＴコマンドの数として定義されてもよく、間隔は１日の１時間として定義されてもよい。他の実現化例では、発生は他の種類のコマンドまたはイベントとして定義されてもよく、間隔は他の時間周期として定義されてもよい。次に続く処理では、異例検出器が確率関数に基づいて新しいデータポイントを履歴データと比較する。

【００６０】

さまざまな実施例において、データ分析器は、ＯＳユーザ、データベースユーザ、場所、およびオブジェクトを含むもののこれらに限定されない多数の次元の属性に基づいて、履歴データを分析する。アクセス頻度は、各ＯＳユーザ、データベースユーザ、場所、オブジェクト、または多数の属性の組合せについて計算可能である。さまざまな次元に基づく測定値が定量的な比較のために使用されてもよい。

【００６１】

たとえば、一実施例では、オブジェクトレベル監視は、１日の時間別のオブジェクトアクセス頻度、１日の時間およびＯＳユーザ別のオブジェクトアクセス頻度、１日の時間およびデータベースユーザ別のオブジェクトアクセス頻度、１日の時間および場所別のオブジェクトアクセス頻度、１日の時間および属性（ＯＳユーザ、データベースユーザ、ならびに場所）の組合せ別のオブジェクトアクセス頻度を含む多次元のオブジェクトアクセス頻度規則、といった測定値のうちの１つ以上を含んでいてもよいが、それらに限定されない。

【００６２】

別の例では、一実施例において、ユーザレベル監視は、１日の時間別のユーザアクセス頻度、１日の時間およびＯＳユーザ別のユーザアクセス頻度、１日の時間およびデータベースユーザ別のユーザアクセス頻度、１日の時間および場所別のユーザアクセス頻度、１日の時間および属性（ＯＳユーザ、データベースユーザ、ならびに場所）の組合せ別のユーザアクセス頻度を含む多次元のオブジェクトアクセス頻度規則、といった測定値のうちの１つ以上を含んでいてもよいが、それらに限定されない。

【００６３】

オブジェクトまたはユーザアクセス頻度に加え、さまざまな実施例において他の測定値がセッションレベル監視のために使用可能であり、たとえば、セッションごとのページ読

出の数によって測定されるセッション別アクセス頻度、セッションごとの時間数によって測定されるセッション別アクセス期間、および毎分あたりのページ読出の数によって測定されるアクセス比率を含むものの、それらに限定されない。

【００６４】

異例検出

図３Ｄは、一実施例における異例検出処理の高レベル概要を示すフローチャートである。ブロック３５１で、データベースアクセスの頻度が、新しい１組のデータから決定される。

【００６５】

ブロック３５２で、しきい値頻度が、防護基準および確率関数パラメータから決定される。一実施例では、確率関数パラメータは、前にブロック３３１でデータ分析器によって決定された履歴データのアクセス頻度である。一実施例では、アクセス頻度は、１日の時間別のＳＥＬＥＣＴ動作の平均数である。

【００６６】

たとえば、午前２時についての平均アクセス頻度が１．５であるとデータ分析器が履歴データから判断し、午前２時についての現在のアクセス頻度が７であることを示す新規データが受信された場合、その新規データは異常であろうか？答えは防護基準による。一実施例では、防護基準は確率百分位として表わされてもよい。異例検出器は、しきい値アクセス頻度値を、防護基準確率百分位および確率関数パラメータ、つまりブロック３３１でデータ分析器によって計算された履歴アクセス頻度から決定する。しきい値を越える頻度値はどれも検証に合格せず、異例であると考えられる。防護百分位が低くなるにつれて、イベントが異例であるとして分類されることがより難しくなり、失敗警告の発生がより少なくなる。

【００６７】

たとえば、防護確率基準が０．１％として特定される場合、異例検出器はしきい値ｎを、式（３）に示すように、ｎを越える値を有する確率が０．１％よりも小さくなるように計算する。

【００６８】

【数３】

$$P(X > n) = 1 - P(X <= n) < 0.1\% \qquad (3)$$

【００６９】

これは、式（４）に示すように、ｎより小さいかまたは等しい値を有する確率が９９．９％よりも大きくなるようにしきい値ｎを決めることと同等である。

【００７０】

【数４】

$$F(n) = P(X <= n) > 99.9\% \qquad (4)$$

【００７１】

式（２）の累積分布関数に代えて、式（４）からのＦ（ｎ）＞９９．９％、および値が１．５のｍ（確率関数パラメータ、履歴データの平均アクセス頻度）を用いることは、ｎのためのしきい値が６という結果をもたらす。

【００７２】

新規データセットのアクセス頻度は７で、アクセス頻度しきい値６を上回っているため、異例が検出される。

【００７３】

ブロック３５３で、（ブロック３５１からの）現在のアクセス頻度の値が、（ブロック

３５２からの）しきい値アクセス頻度と比較される。

【００７４】

一実施例では、異例検出器は、動的な統計パターンおよび／または静的な不規則ベースの方針のいずれかに基づいて、履歴データにおける不審なデータベースアクセスを検出し、ｅメール警告を生成する。報告またはグラフも生成可能である。

【００７５】

機密保護方針を用いてデータベースユーザ挙動を監視することが可能である。たとえば、一実施例では、機密保護方針の２つの異なるカテゴリ、つまり（１）アクセス頻度方針と（２）アクセス違反方針とがある。アクセス頻度方針は、データベース監査エンジンがさまざまな次元に基づいて１日の時間別のアクセス数を防護できるようにする。そのような侵入検出は、前に述べたように統計ベースであってもよく、および／または規則ベースであってもよい。一実施例では、防護しきい値は、１日の時間別のアクセス数などの点で絶対値として特定可能である。アクセス違反方針は、データベース監査エンジンが明示的な機密保護規則を用いて各個々のデータベースアクセスを防護できるようにする。表１は、一実施例においてデータベースユーザ挙動を監視するために使用可能なさまざまな機密保護方針を示す。

【００７６】

【表１】

表 1: 不機密保護方針

監視レベル	分類	不機密保護方針	侵入検出方法
オブジェクトレベル監視	アクセス頻度	1日の時間別のオブジェクトアクセス頻度	統計ベースまたは規則ベース
		1日の時間およびOSユーザ別のオブジェクトアクセス頻度	統計ベースまたは規則ベース
		1日の時間およびデータベースユーザ別のオブジェクトアクセス頻度	統計ベースまたは規則ベース
		1日の時間および場所別のオブジェクトアクセス頻度	統計ベースまたは規則ベース
		多次元オブジェクトアクセス頻度規則	統計ベースまたは規則ベース
	アクセス違反	オブジェクトアクセス不機密保護違反	規則ベース
		不審なOSユーザによるオブジェクトアクセス	規則ベース
		不審なデータベースユーザによるオブジェクトアクセス	規則ベース
		不審な場所からのオブジェクトアクセス	規則ベース
		多次元オブジェクトアクセス違反規則	規則ベース
ユーザレベル監視	アクセス頻度	1日の時間別のユーザアクセス頻度	統計ベースまたは規則ベース
		1日の時間およびOSユーザ別のユーザアクセス頻度	統計ベースまたは規則ベース
		1日の時間およびデータベースユーザ別のユーザアクセス頻度	統計ベースまたは規則ベース
		1日の時間および場所別のユーザアクセス頻度	統計ベースまたは規則ベース
		多次元ユーザアクセス頻度規則	統計ベースまたは規則ベース
	アクセス違反	ユーザアクセス不機密保護違反	規則ベース
		不審なOSユーザによるユーザアクセス	規則ベース
		不審なデータベースユーザによるユーザアクセス	規則ベース
		不審な場所からのユーザアクセス	規則ベース
		多次元ユーザアクセス違反規則	規則ベース
セッションレベル監視	アクセス頻度	高い読出率（ページ/分）	統計ベースまたは規則ベース
		過度の読出アクティビティ	統計ベースまたは規則ベース
		極端に長いログインセッション	統計ベースまたは規則ベース
	アクセス違反	ログイン失敗	規則ベース
		不審な時間枠でのログイン	規則ベース
		不審なOSユーザによるログイン	規則ベース
		不審な場所からのログイン	規則ベース
		多次元セッション規則	規則ベース

【００７７】

たとえば、さまざまな実施例において、以下のアクセス違反規則がオブジェクトレベル監視に対して特定可能である。（１）オブジェクトアクセス機密保護違反：適正な許可なく特定のオブジェクトを読出そうとして失敗した試みはどれも警告される。（２）不審な

ＯＳユーザによるオブジェクトアクセス：無効なＯＳユーザによる特定のオブジェクトのうまくいった読出はどれも警告される。一実施例では、有効なＯＳユーザのリストが定義可能であり、リストにないＯＳユーザによるアクセスはどれも警告される。別の実施例では、無効なＯＳユーザのリストが定義可能であり、リストにあるＯＳユーザによるアクセスはどれも警告される。（３）不審なデータベースユーザによるオブジェクトアクセス：無効なデータベースユーザによる特定のオブジェクトのうまくいった読出はどれも警告される。一実施例では、有効な、および／または無効なデータベースユーザのリストが定義可能である。（４）不審な場所からのオブジェクトアクセス：無効なクライアントシステムからの特定のオブジェクトのうまくいった読出はどれも警告される。一実施例では、有効な、および／または無効な場所のリストが定義可能である。（５）多次元オブジェクトアクセス規則：属性（ＯＳユーザ、データベースユーザ、および場所）の無効な組合せでの特定のオブジェクトのうまくいった読出はどれも警告される。

【００７８】

別の例では、さまざまな実施例において、以下のアクセス違反規則がユーザレベル監視に対して特定可能である。（１）ユーザアクセス機密保護違反：特定のデータベースユーザが適正な許可なく読出そうとして失敗した試みはどれも警告される。（２）不審なＯＳユーザによるユーザアクセス：無効なＯＳユーザからの特定のデータベースユーザによるうまくいった読出はどれも警告される。一実施例では、有効な、および／または無効なＯＳユーザのリストが定義可能である。（３）不審なデータベースオブジェクトのユーザアクセス：特定のデータベースユーザによる無効なデータベースオブジェクトへのうまくいった読出はどれも警告される。一実施例では、有効な、および／または無効なオブジェクトのリストが定義可能である。（４）不審な場所からのユーザアクセス：無効なクライアントシステムからの特定のデータベースユーザによるうまくいった読出はどれも警告される。一実施例では、有効な、および／または無効な場所のリストが定義可能である。（５）多次元ユーザアクセス規則：属性（ＯＳユーザ、データベースオブジェクト、および場所）の無効な組合せでの特定のデータベースユーザによるうまくいった読出はどれも警告される。

【００７９】

さらに別の例では、さまざまな実施例において、以下のアクセス違反規則がセッションレベル監視に対して特定可能であり、以下のアクセス違反規則は次のように特定可能である。（１）ログイン失敗：無効のパスワードによるログインの失敗は警告される。（２）不審な時間枠でのログイン：特定された正規の時間外のログイン時間は警告される。（３）不審なＯＳユーザによるログイン：特定のデータベースユーザおよび無効なＯＳユーザによるうまくいったログインはどれも警告される。一実施例では、有効な、および／または無効なＯＳユーザのリストが定義可能である。（４）不審な場所からのログイン：無効のクライアントシステムからの特定のデータベースユーザによるうまくいったログインはどれも警告される。一実施例では、有効な、および／または無効な場所のリストが定義可能である。（５）多次元セッション規則：属性（ＯＳユーザおよび場所）の無効な組合せでのうまくいったログインはどれも警告される。

【００８０】

監視例

一実施例におけるデータベース監視の動作を、図３Ｅのフローチャートおよび図６Ａ～図６Ｍで示すスクリーンショットを参照して述べられるデータベース用監視動作を設定し、使用する一例を用いて示す。一実施例では、監視動作の設定は、グラフィカルユーザインターフェイスがウェブブラウザを用いて実現された状態で行なわれる。図６Ａ～図６Ｍで示す例示的なユーザインターフェイススクリーンでは、ユーザは前の／次の誘導矢印に従って、監視動作を設定するプロセスをたどって１ステップずつ実行できる。また、これに代えて、ユーザはパネル上部のメニューバーから項目を選択してもよく、または、パネル左側の階層型ツリービューからリンクをクリックしてもよい。

【００８１】

ユーザは、図３Ｅ、ブロック４１０に示すように、監視されるべきデータベースを開くことによってプロセスを開始してもよい。一実施例では、データベースを開くステップは、図６Ａに示すように、ホスト名、データベース名、ユーザ名およびパスワードを特定することによってデータベース接続を定義するステップを含む。ユーザは、図６Ｂに示すように、特定されたデータベースに接続する。

【００８２】

ブロック４２０で、ユーザは、特定されたデータベースのための監視スケジュールを設定する。監視スケジュールを設定するプロセスの間、ユーザは、図６Ｃに示すように、データ分析器がどれぐらいの頻度でユーザ挙動データを「学習」し、統計的モデルを再構築するかを特定する。ユーザはまた、図６Ｃに示すスクリーンを再度用いて、異例検出器がどれぐらいの頻度で異例データに対して「防護」し、警告を送信するかを特定する。

【００８３】

ブロック４３０で、ユーザはｅメール受信者を設定する。ユーザは、例示的な一実施例において、図６Ｄに示すスクリーンを用いて、異例が生じた際に誰に警告ｅメールを送信するかを特定する。

【００８４】

ブロック４４０で、ユーザは監視方針を設定する。図６Ｅ～図６Ｆに示すスクリーンは、例示的な一実施例における監視方針の設定を示している。ユーザは、図６Ｅに示すように、監視する「重大な」オブジェクトを選択する。ユーザは、図６Ｆに示すように、このオブジェクトのために起動するアクセス違反方針を選択する。ユーザは、誰がこのオブジェクトにアクセスすることを許可されるかを特定する。多次元オブジェクト規則については、それは属性の組合せとして定義可能である。たとえば、図６Ｇに示すように、データベースユーザＷＡＮＩは、自分がＯＳユーザＩＰＬＯＣＫＳ／ＷＴＡＮＧとして、クライアントシステムＷＬＩＮＵＸからログインされる場合に限り、このオブジェクトにアクセス可能である。このユーザはまた、図６Ｈに示すように、このオブジェクトを監視するために起動するアクセス頻度方針も特定する。

【００８５】

ブロック４５０で、ユーザは監視を開始する。一実施例では、監視は、図６Ｉに示すようなステータススクリーンのチェックボックスをクリックすることによって開始される。

【００８６】

ブロック４６０で、ユーザは警告および／またはグラフを見る。階層型の一例では、データベースユーザＷＡＮＩに属するデータベースパスワードが盗まれ、不法行為者が盗まれたパスワードを用いて、そのパスワードが使用を割当てられたもの以外のマシンからデータベースオブジェクトにアクセスしようとする。不法行為者が使用を試みると、図６Ｊに示すような多次元オブジェクト規則のアクセス違反を引起こす。たとえば、設定された多次元オブジェクト規則は、（図６Ｇに示すように）データベースユーザＷＡＮＩが、ＯＳユーザＩＰＬＯＣＫＳ／ＷＡＮＩによって、かつ場所ＷＬＩＮＵＸからしか、オブジェクトＨＲ．ＥＭＰにアクセスできないことを示している。不法行為者は、データベースユーザＷＡＮＩとして、異なるＯＳユーザＩＰＬＯＣＫＳ／ＣＫＣＨＯＵによって、かつ異なる場所ＣＫＤＥＳＫＴＯＰから、オブジェクトにアクセスしようとすると、それはアクセス違反を引起こす。目標とされる動作がトリガされてもよい。図６Ｊに示す例では、図６Ｄに示すスクリーンを用いて定義されたｅメール受信者に、ｅメール警告が送信される。ユーザは、図６Ｋに示すように、グラフィックユーザインターフェイスを介して警告を見る。ユーザはまた、図６Ｌに示すような、任意のユーザによる任意のオブジェクトについてのアクセスパターンを見る。ユーザがアクセス頻度しきい値または百分位に違反している場合、警告が同様に送信される。

【００８７】

ブロック４７０で、ユーザは報告を生成する。ユーザは警告についての概要報告を生成し、それは、図６Ｍに示すように問題の分析を支援できる。図３Ｅおよび図６Ａ～図６Ｍを参照して上に説明したプロセスは単に、一実施例を用いた一例である。他の実施例は、

簡略のためここでは述べられなかった他のプロセスおよびスクリーンを含み、および／または、説明された処理および／またはスクリーンのいくつかを省略してもよい。

【００８８】

図４は、一実施例におけるデータベースへのアクセスの例示的な確率分布を示すグラフである。図４は、２４時間の期間中での或る特定のユーザによるデータベースアクセスアクティビティの一例を示している。図４では、各棒は、このユーザによる１時間当たりのオブジェクトアクセスの数を表わしている。図４に示す例示的な確率分布では、ユーザがデータベースにアクセスする確率は２つのピークを有し、一方のピークは午前の中頃の時間に起る可能性があり、別のピークは午後の中頃の時間に起る可能性がある。これらの時間枠外の過度のデータベースアクセスアクティビティは疑わしい可能性がある。

【００８９】

図５は、一実施例におけるデータベース監視システムの高レベル概要を示すブロック図である。図５に示すように、データベース監視システムは３層アーキテクチャを含む。第１の層では、データベース監視システムは、データベース監視機能性へのアクセスを提供するためのウェブブラウザを含む。一実施例では、Java（登録商標）サーバページ（ＪＳＰ）がユーザインターフェイスを提供する。

【００９０】

第２の層では、データベース監視システムは、一実施例ではアパッチトムキャット（Apache Tomcat）を用いて実現されているウェブサーバと、一実施例ではポストグレ（Postgre）ＳＱＬ（登録商標）データベースを用いて実現されている履歴データの記憶用の内部データベースとを用いる。この発明の実施例は、安全なリナックス（Linux）オペレーティングシステムとともに実行されるペンティアム（Pentium）（登録商標）または同等の機能性のハードウェアプラットフォームを含むもののこれらに限定されない任意のコンピューティングプラットフォーム上にあり得る。データベース監視システムの構成要素は、データコレクタ、データ分析器、および異例検出器を含む。支持構成要素は、（１）ユーザがスケジュール設定および方針設定といった実現化に特有の必要性に従ってデータベース監視システムをカスタマイズできるようにするコンフィギュレータ、（２）指定された機密保護担当者に警告メッセージを送信するＥメール警告、（３）診断報告を生成する報告マネージャ、（４）データベースユーザ挙動パターンのグラフィック表現を生成するビジュアライザのうちの１つ以上を含む。

【００９１】

第３の層では、データベース監視システムはJava（登録商標）データベースコネクティビティ（ＪＤＢＣ）ＡＰＩを用いてターゲットデータベースにアクセスする。

【００９２】

ハードウェア概要

一実施例では、図１に示すコンピューティング環境１００のさまざまな構成要素は、１つ以上のプロセッサによって実行可能な命令の組として実現可能である。図７は、これらの構成要素を実行させるために使用され得るコンピュータシステム７００のブロック図を示す。コンピュータシステム７００は、情報を通信するためのバス７０２または他の通信メカニズムと、情報を処理するためにバス７０２と結合されたプロセッサ７０４とを含む。コンピュータシステム７００はまた、プロセッサ７０４により実行されるべき命令および情報を記憶するためにバス７０２に結合された、ランダムアクセスメモリ（ＲＡＭ）または他のダイナミック記憶装置といったメインメモリ７０６も含む。メインメモリ７０６は、プロセッサ７０４により実行されるべき命令の実行中に一時的な変数または他の中間情報を記憶するためにも使用されてもよい。コンピュータシステム７００はさらに、プロセッサ７０４用の命令およびスタティック情報を記憶するためにバス７０２に結合された読出専用メモリ（ＲＯＭ）７０８または他のスタティック記憶装置を含む。磁気ディスクまたは光ディスクといった記憶装置７１０が、情報および命令を記憶するために提供され、バス７０２に結合されている。

【００９３】

コンピュータシステム７００は、情報をコンピュータユーザに表示するためのブラウン管（ＣＲＴ）などのディスプレイ７１２に、バス７０２を介して結合されていてもよい。英数字キーおよび他のキーを含む入力装置７１４が、情報およびコマンド選択をプロセッサ７０４に通信するためにバス７０２に結合されている。ユーザ入力装置の別の種類は、方向情報およびコマンド選択をプロセッサ７０４に通信し、ディスプレイ７１２上のカーソルの動きを制御するための、マウス、トラックボール、またはカーソル方向キーといったカーソル制御７１６である。この入力装置は通常、２つの軸、つまり第１の軸（たとえばｘ）および第２の軸（たとえばｙ）において２つの自由度を有しており、それによりこの装置は平面における場所を特定することができる。

【００９４】

一実施例によれば、この発明の機能性は、プロセッサ７０４がメインメモリ７０６に含まれる１つ以上の命令の１つ以上のシーケンスを実行するのに応じて、コンピュータシステム７００によって提供される。そのような命令は、記憶装置７１０などの別のコンピュータ読み取り可能な媒体からメインメモリ７０６に読込まれてもよい。メインメモリ７０６に含まれる命令のシーケンスの実行により、プロセッサ７０４は、ここに説明されたプロセスステップを行なうようになる。代替的な実施例では、この発明を実現するために、ソフトウェア命令の代わりに、またはソフトウェア命令と組合わせて、配線接続回路が使用されてもよい。このため、この発明の実施例は、配線接続回路とソフトウェアとのどの特定の組合せにも限定されない。

【００９５】

ここで用いられるような用語「コンピュータ読み取り可能な媒体」とは、プロセッサ７０４に命令を実行用に提供することに関与するあらゆる媒体を指す。そのような媒体は、不揮発性媒体、揮発性媒体、および通信媒体を含むもののそれらに限定されない多くの形態を取り得る。不揮発性媒体はたとえば、記憶装置７１０などの光ディスクまたは磁気ディスクを含む。揮発性媒体は、メインメモリ７０６などのダイナミックメモリを含む。通信媒体は、バス７０２を構成する配線を含む、同軸ケーブル、銅線および光ファイバを含む。通信媒体はまた、無線周波数および赤外線データ通信中に発生するものといった音波または光波の形も取り得る。

【００９６】

コンピュータ読み取り可能な媒体の一般的な形態は、たとえば、フロッピー（登録商標）ディスク、フレキシブルディスク、ハードディスク、磁気テープ、または任意の他の磁気媒体、ＣＤ－ＲＯＭ、任意の他の光媒体、パンチカード、紙テープ、孔のパターンを有する任意の他の物理的媒体、ＲＡＭ、ＰＲＯＭ、ＥＰＲＯＭ、ＦＬＡＳＨ－ＥＰＲＯＭ、任意の他のメモリチップまたはカートリッジ、以下に説明するような搬送波、または、コンピュータがそこから読み取り可能な任意の他の媒体を含む。

【００９７】

コンピュータ読み取り可能な媒体のさまざまな形態は、プロセッサ７０４に１つ以上の命令の１つ以上のシーケンスを実行用に保持することに関与していてもよい。たとえば、命令はまず、遠隔コンピュータの磁気ディスク上に保持されてもよい。遠隔コンピュータは命令をそのダイナミックメモリにロードし、電話回線を通してモデムを用いて命令を送信することができる。コンピュータシステム７００にとってローカルなモデムは、電話回線上のデータを受信し、赤外線送信機を用いてデータを赤外線信号に変換することができる。赤外線検出器は赤外線信号で搬送されたデータを受信でき、適切な回路がデータをバス７０２上に配置することができる。バス７０２はデータをメインメモリ７０６に搬送し、そこからプロセッサ７０４が命令を検索して実行する。メインメモリ７０６によって受信された命令は、プロセッサ７０４による実行の前または後のいずれかで、記憶装置７１０上に随意に記憶されてもよい。

【００９８】

コンピュータシステム７００はまた、バス７０２に結合された通信インターフェイス７１８も含む。通信インターフェイス７１８は、ローカルネットワーク７２２に接続された

ネットワークリンク７２０に双方向データ通信結合を提供する。たとえば、通信インターフェイス７１８は、データ通信接続を対応する種類の電話回線に提供するデジタル相互サービス網（ＩＳＤＮ）カード、またはモデムであってもよい。別の例として、通信インターフェイス７１８は、データ通信接続を互換性があるＬＡＭに提供するローカルエリアネットワーク（ＬＡＮ）カードであってもよい。無線リンクも実現され得る。任意のそのような実現化例では、通信インターフェイス７１８は、さまざまな種類の情報を表わすデジタルデータストリームを搬送する電気信号、電磁信号、または光信号を送信および受信する。

【００９９】

ネットワークリンク７２０は通常、１つ以上のネットワークを介して、他のデータ装置にデータ通信を提供する。たとえば、ネットワークリンク７２０は、ローカルネットワーク７２２を介して、ホストコンピュータ７２４に、またはインターネットサービスプロバイダ（ＩＳＰ）７２６により運営されるデータ装置に、接続を提供してもよい。ＩＳＰ７２６は次に、現在一般に「インターネット」７２８と呼ばれている全世界的パケットデータ通信ネットワークを介して、データ通信サービスを提供する。ローカルネットワーク７２２およびインターネット７２８は双方とも、デジタルデータストリームを搬送する電気信号、電磁信号または光信号を使用する。コンピュータシステム７００へ、またはコンピュータシステム７００からデジタルデータを搬送する、さまざまなネットワークを通る信号、ネットワークリンク７２０上の信号、および通信インターフェイス７１８を通る信号は、情報を運ぶ搬送波の例示的な形態である。

【０１００】

コンピュータシステム７００は、ネットワーク、ネットワークリンク７２０および通信インターフェイス７１８を介して、メッセージを送信し、プログラムコードを含むデータを受信する。インターネットの例では、サーバ７３０は、アプリケーションプログラム用の要求されたコードを、インターネット７２８、ＩＳＰ７２６、ローカルネットワーク７２２、および通信インターフェイス７１８を介して送信してもよい。受信されたコードは、受信された際にプロセッサ７０４によって実行されてもよく、および／または、後の実行用に記憶装置７１０または他の不揮発性記憶装置に記憶されてもよい。このように、コンピュータシステム７００は、搬送波の形をしたアプリケーションコードを取得し得る。

【０１０１】

前述の明細書においてこの発明を特定の実施例を参照して説明してきたが、それがそのように限定されると解釈されるべきではないことに留意するべきである。さまざまな修正が当業者により、この開示の恩恵を用いて、この発明の精神から逸脱することなく行なわれてもよい。このため、この発明は、それを例示するために用いられた特定の実施例によって限定されるべきではなく、発行された特許請求の範囲のみによって限定されるべきである。したがって、明細書および図面は、限定的というよりはむしろ例示的であると考えられるべきである。

【図面の簡単な説明】

【０１０２】

【図１】データベースを監視するための手法が一実施例において実現され得るネットワークコンピューティングシステムの高レベル概要を示すブロック図である。

【図２】一実施例における例示的なデータベース監査エンジンでのプロセスの高レベル概要を示すブロック図である。

【図３Ａ】一実施例におけるデータ収集、分析および異例検出処理の高レベル概要を示すブロックフローチャートである。

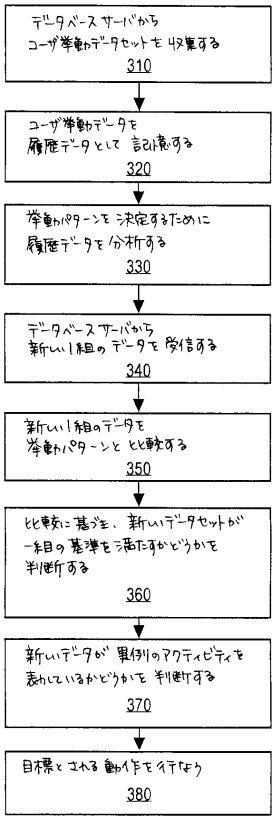
【図３Ｂ】一実施例におけるデータ収集、分析および異例検出処理の高レベル概要を示すブロックフローチャートである。

【図３Ｃ】一実施例におけるデータ収集、分析および異例検出処理の高レベル概要を示すブロックフローチャートである。

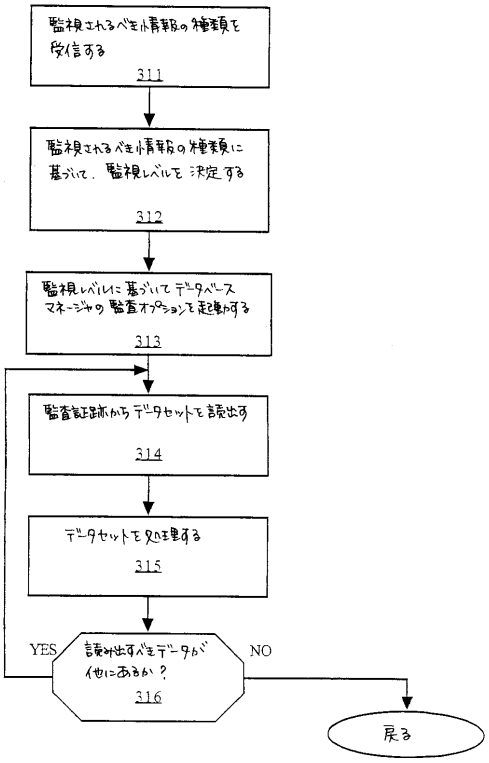
【図３Ｄ】一実施例におけるデータ収集、分析および異例検出処理の高レベル概要を示す

ブロックフローチャートである。
【図３Ｅ】一実施例におけるデータ収集、分析および異例検出処理の高レベル概要を示すブロックフローチャートである。
【図４】一実施例におけるデータベースへのアクセスの例示的な確率分布を示すグラフである。
【図５】一実施例におけるデータベース監視システムの高レベル概要を示すブロック図である。
【図６Ａ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｂ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｃ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｄ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｅ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｆ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｇ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｈ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｉ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｊ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｋ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｌ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図６Ｍ】一実施例において監視動作を設定する一例を示すスクリーンショットである。
【図７】一実施例の１つ以上の構成要素を具体化するために使用され得る代表的なコンピュータシステムを示すハードウェアブロック図である。
【符号の説明】
【０１０３】
８４　監査証跡、８６　動的性能ビュー、８８　履歴データ、９０　挙動パターン、９２　機密保護規則、９４　報告、９６　Ｅメール警告、９８　視覚化、１００　コンピューティング環境、１０６　ネットワーク、１０８　インターネット、１１０　データベース監査エンジン、１１２　データコレクタ、１１４　データ分析器、１１６　異例検出器、１２２　ルータ、１２４　ファイヤウォール、１３０　データベースサーバ、１３２　データベース、１４４　アドミニストレータ。

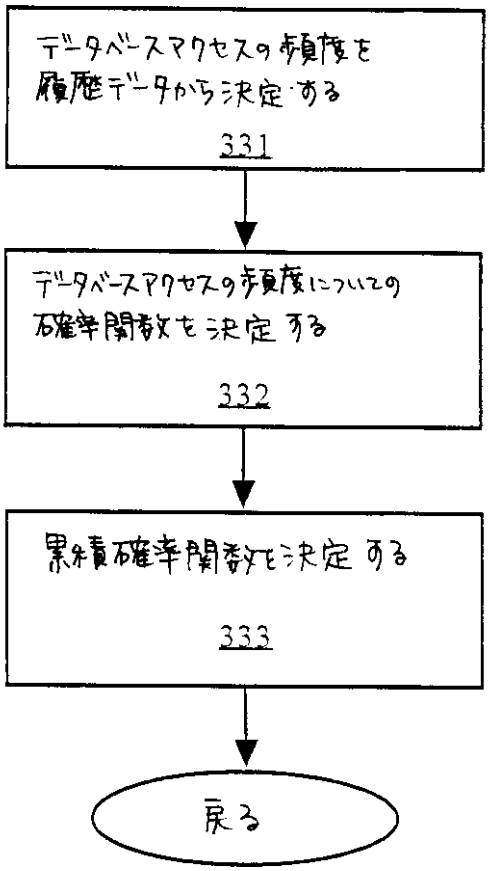
【図３Ａ】



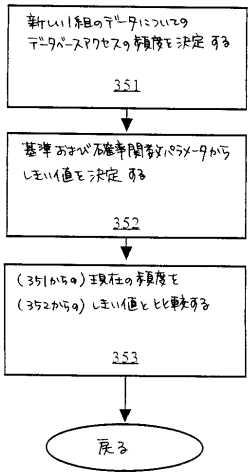
【図３Ｂ】



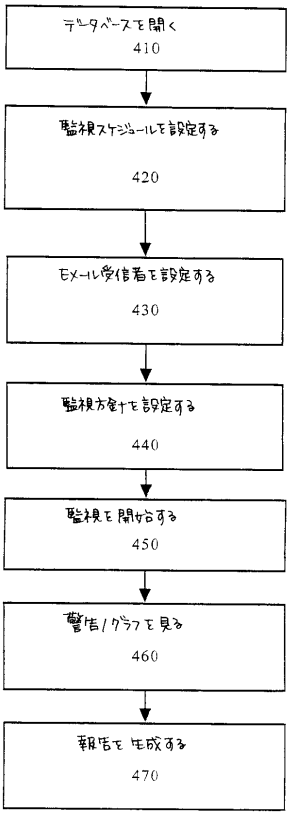
【図３Ｃ】



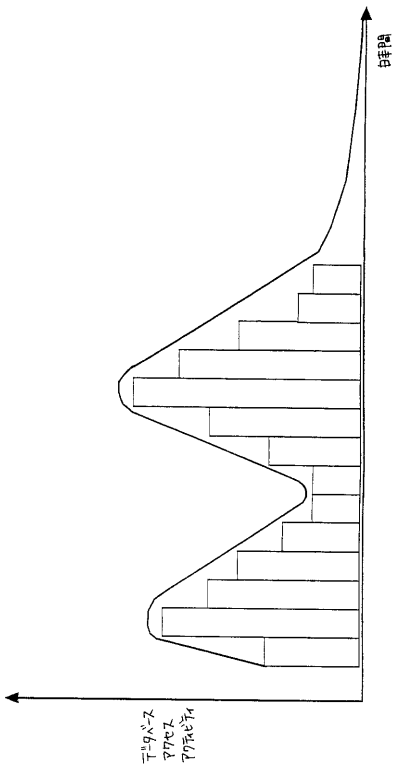
【図３Ｄ】



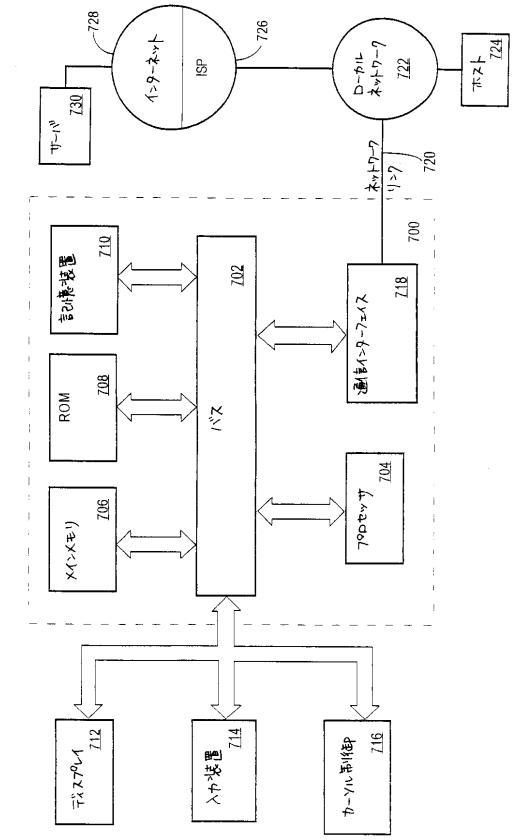
【図３Ｅ】


データベースを開く
410
監視スケジュールを設定する
420
Eメール受信者を設定する
430
監視方針を設定する
440
監視を開始する
450
警告/グラフを見る
460
報告を生成する
470

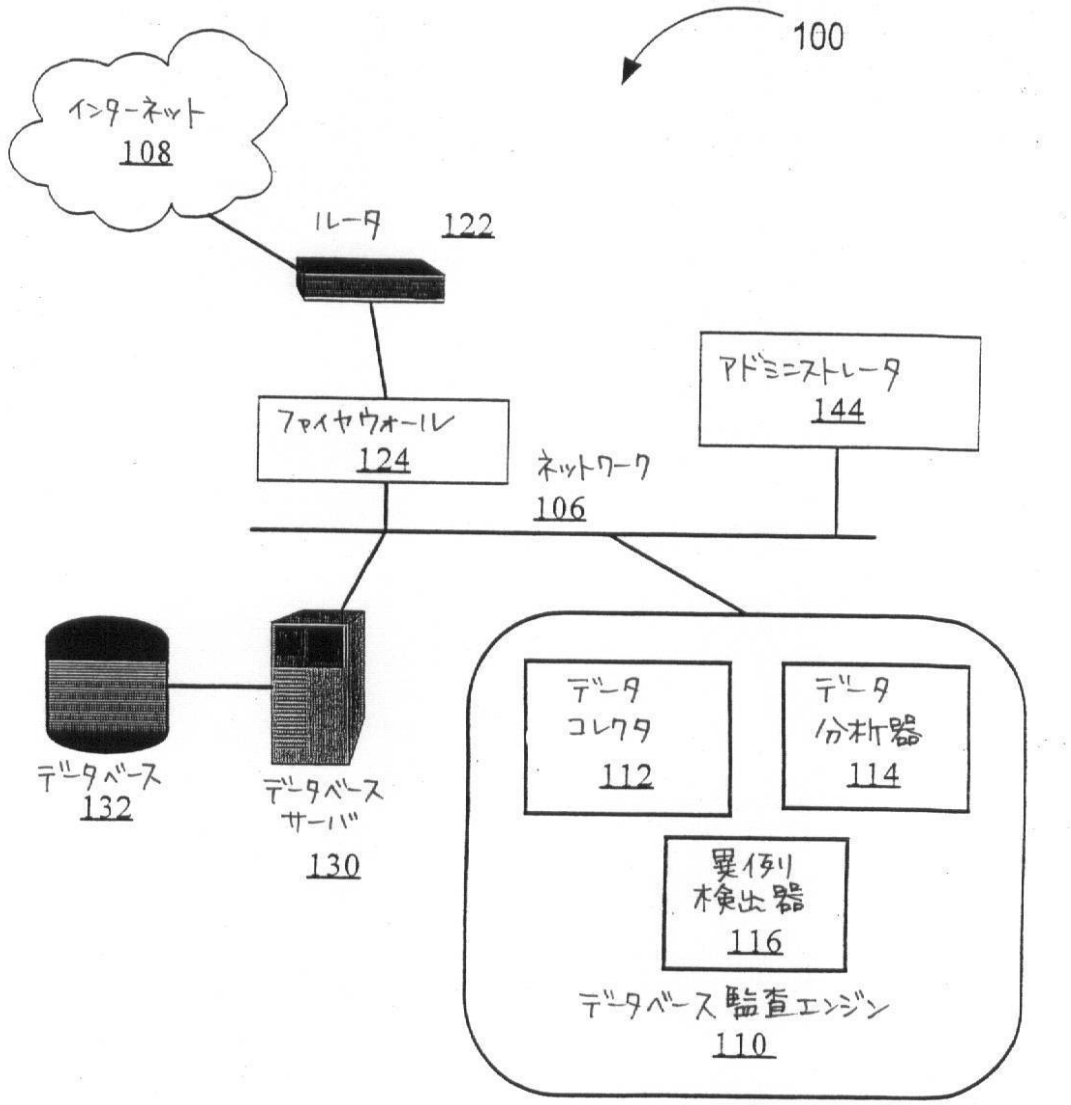
【図４】


時間
データベース
アクセス
アクティビティ

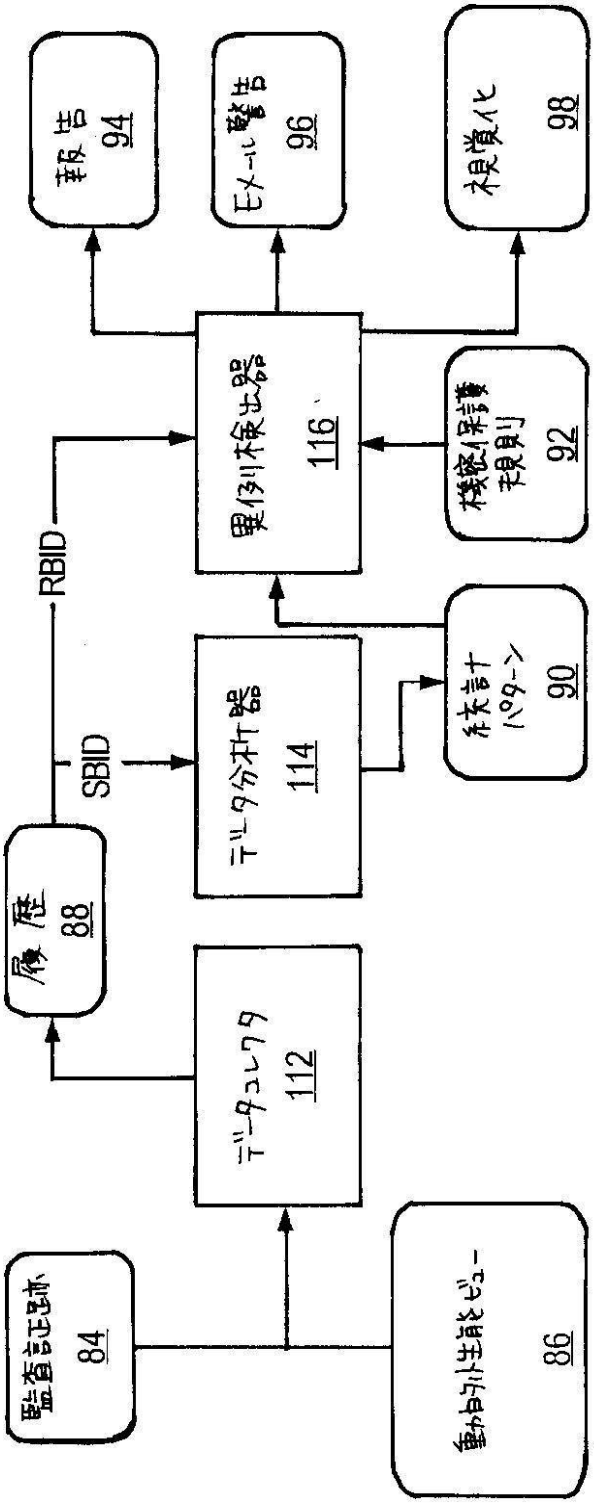
【図７】


インターネット
ISP
728
726
ローカル
ネットワーク
722
ホスト
724
サーバ
730
ネットワーク
リンク
720
700
記憶装置
710
ROM
708
メインメモリ
706
バス
702
通信インターフェイス
718
プロセッサ
704
ディスプレイ
712
入力装置
714
カーソル制御
716

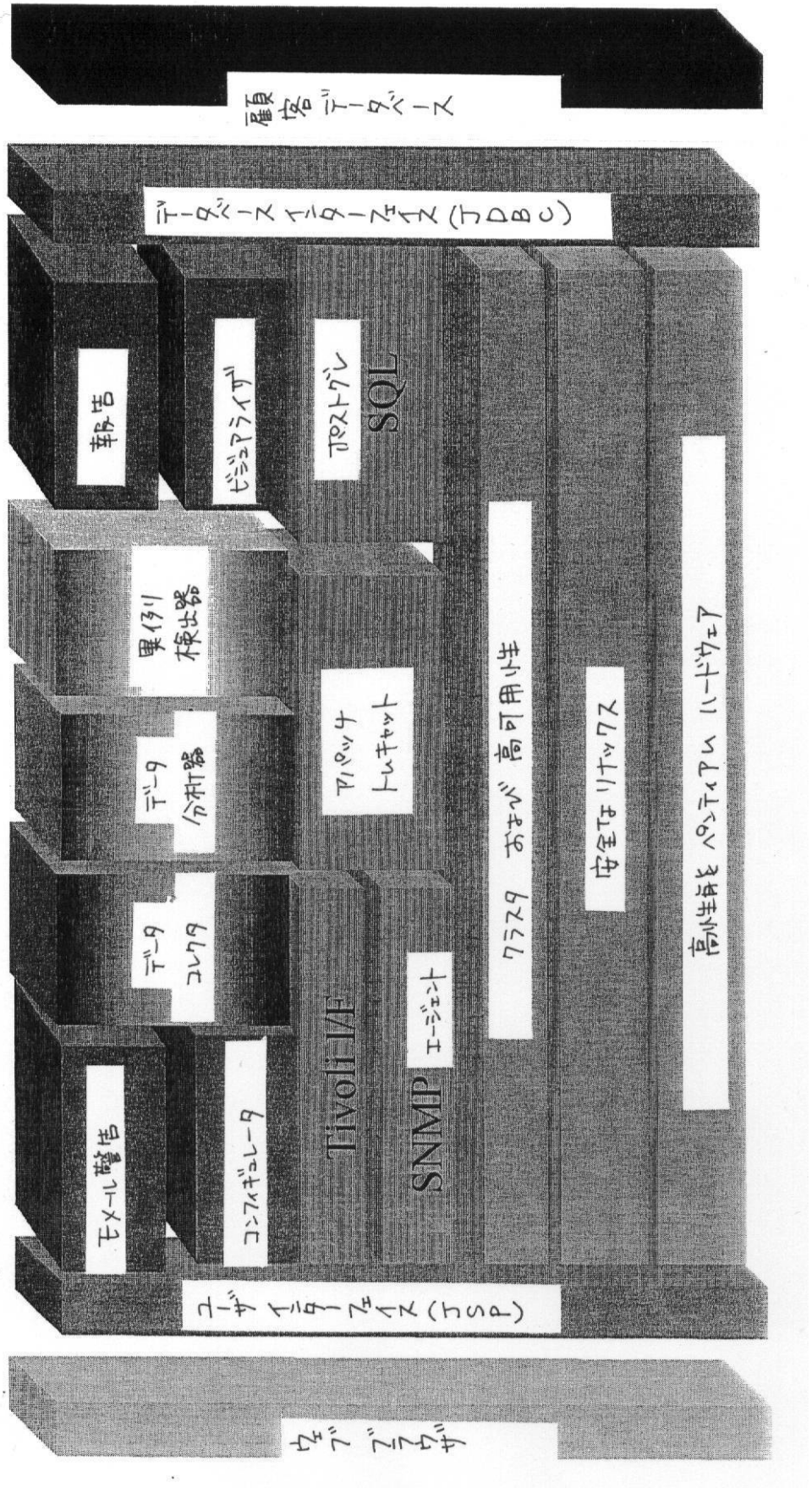
【図１】


100
インターネット
108
ルータ 122
ファイヤウォール
124
ネットワーク
106
アドミニストレータ
144
データベース
132
データベース
サーバ
130
データ
コレクタ
112
データ
分析器
114
異例
検出器
116
データベース監査エンジン
110

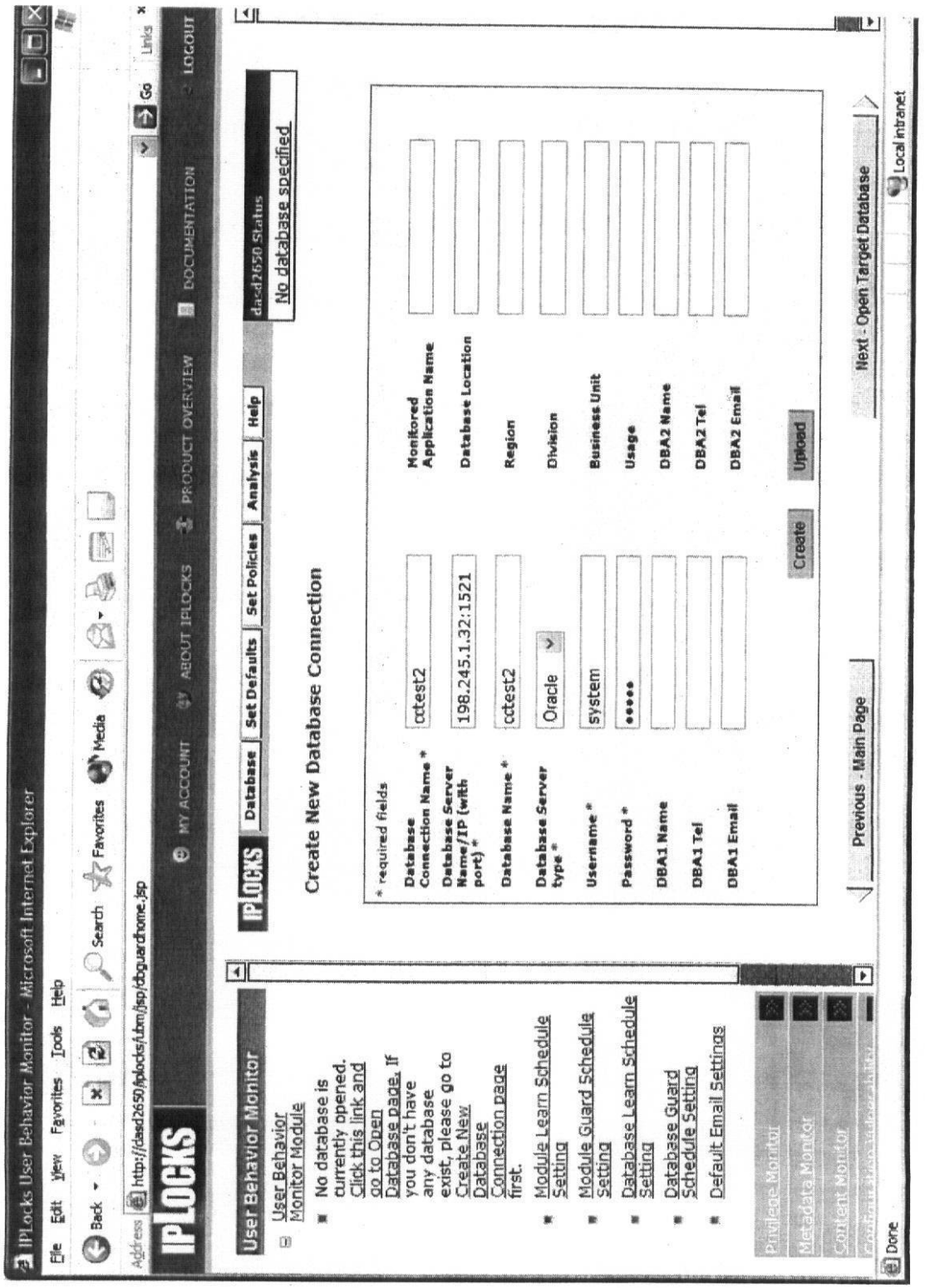
【図２】


監査証跡
84
自動外注能ビュー
86
データコレクタ
112
履歴
88
RBID
SBID
データ分析器
114
異例検出器
116
統計パターン
90
機密保護規則
92
報告
94
Eメール警告
96
視覚化
98

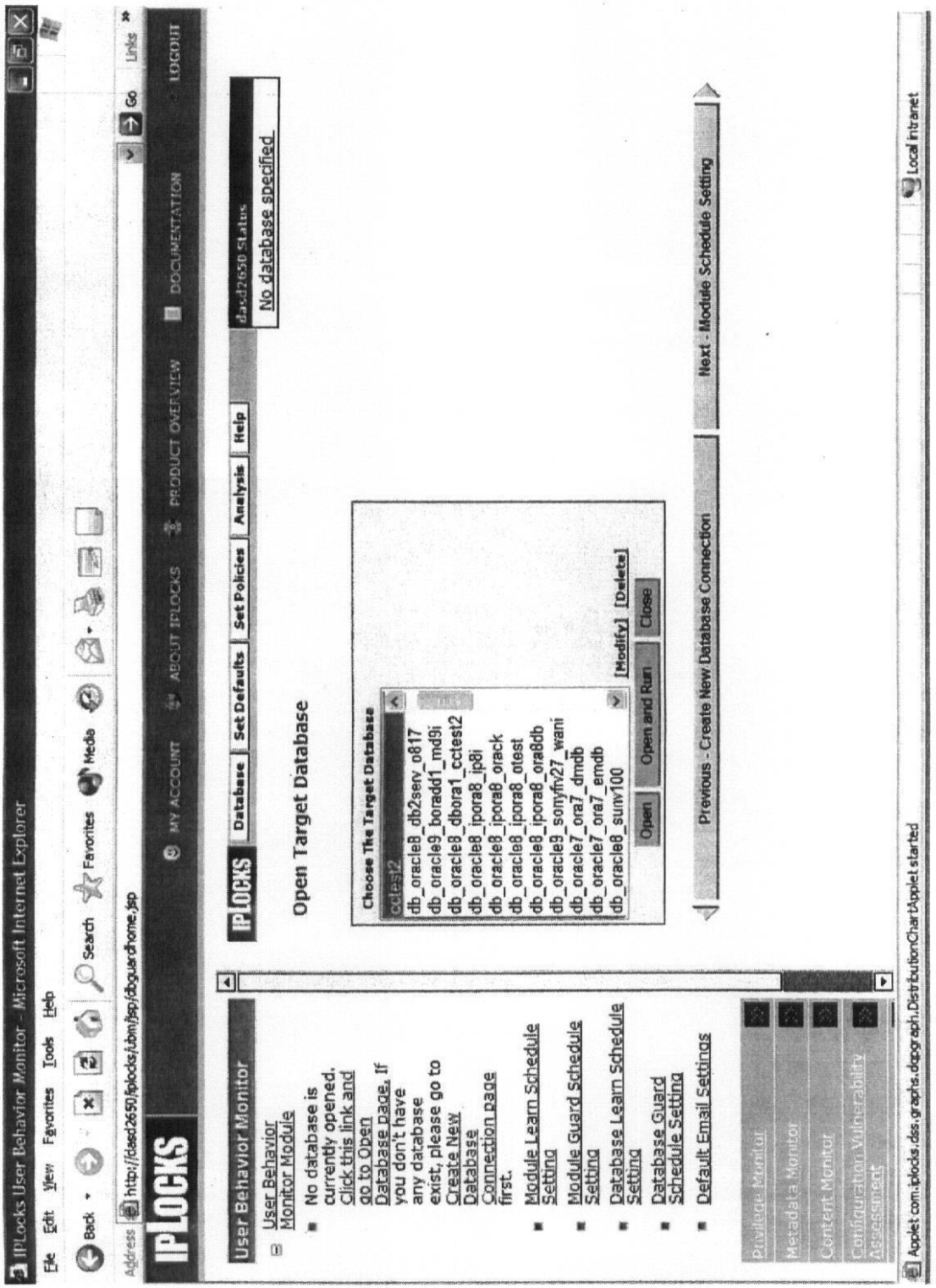
【図５】


履歴データベース
データベースインターフェイス（JDBC）
報告
ビジュアライザ
ポストグレ
SQL
異常検出器
データ分析器
アラート トレンド
データコレクタ
TivoliI/F
SNMP エージェント
クラスタ おまかせ高可用性
ユーザインターフェイス（JSP）
モバイル
コンフィギュレータ
ハードウェア
ウェブブラウザ

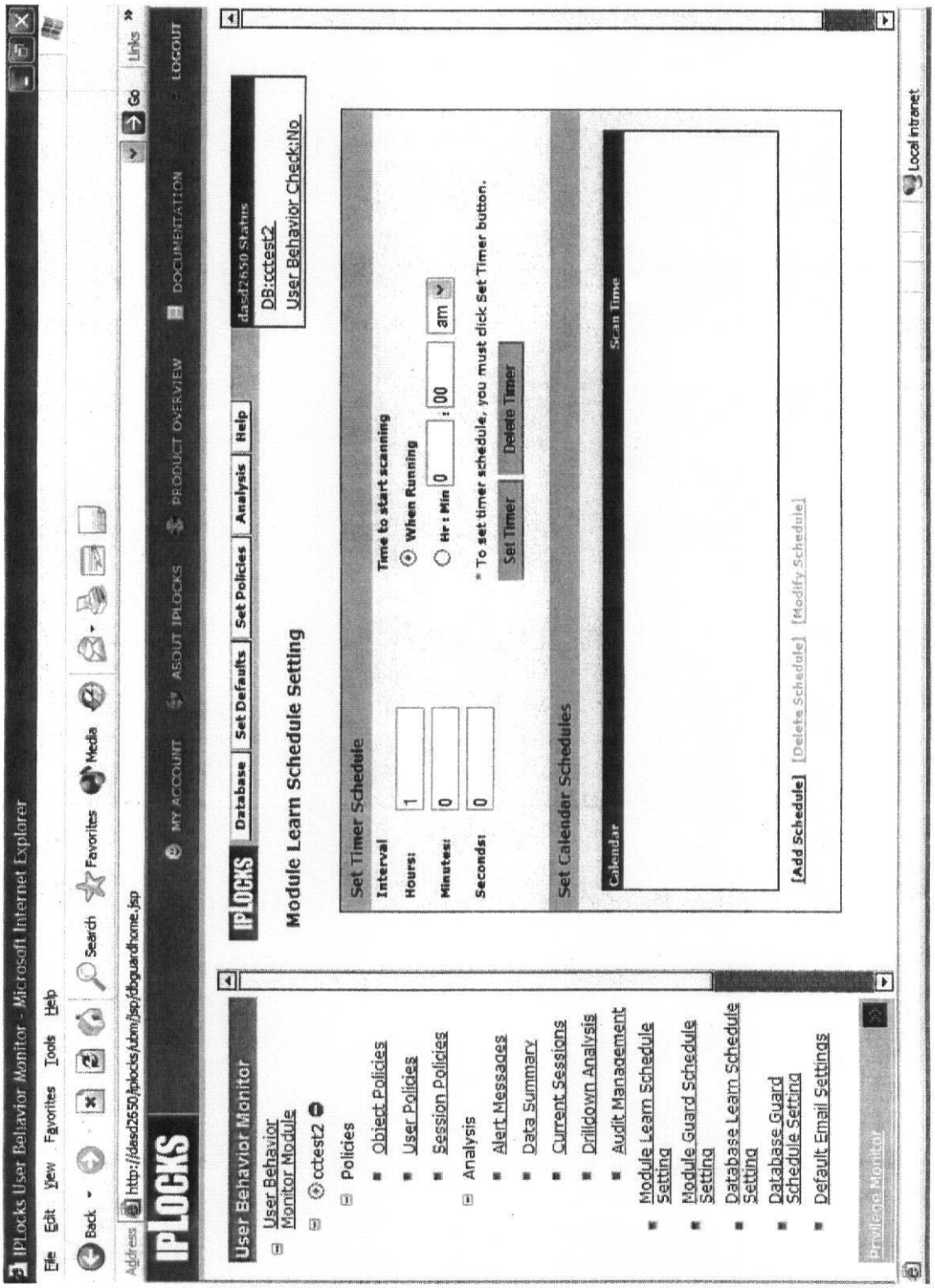
【図６Ａ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/Ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
No database is currently opened. Click this link and go to Open Database page. If you don't have any database exist, please go to Create New Database Connection page first.
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Metadata Monitor
Content Monitor
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
No database specified
Create New Database Connection
* required fields
Database Connection Name *
cctest2
Database Server Name/IP (with port) *
198.245.1.32:1521
Database Name *
cctest2
Database Server type *
Oracle
Username *
system
Password *
DBA1 Name
DBA1 Tel
DBA1 Email
Monitored Application Name
Database Location
Region
Division
Business Unit
Usage
DBA2 Name
DBA2 Tel
DBA2 Email
Create
Upload
Previous - Main Page
Next - Open Target Database
Done
Local intranet

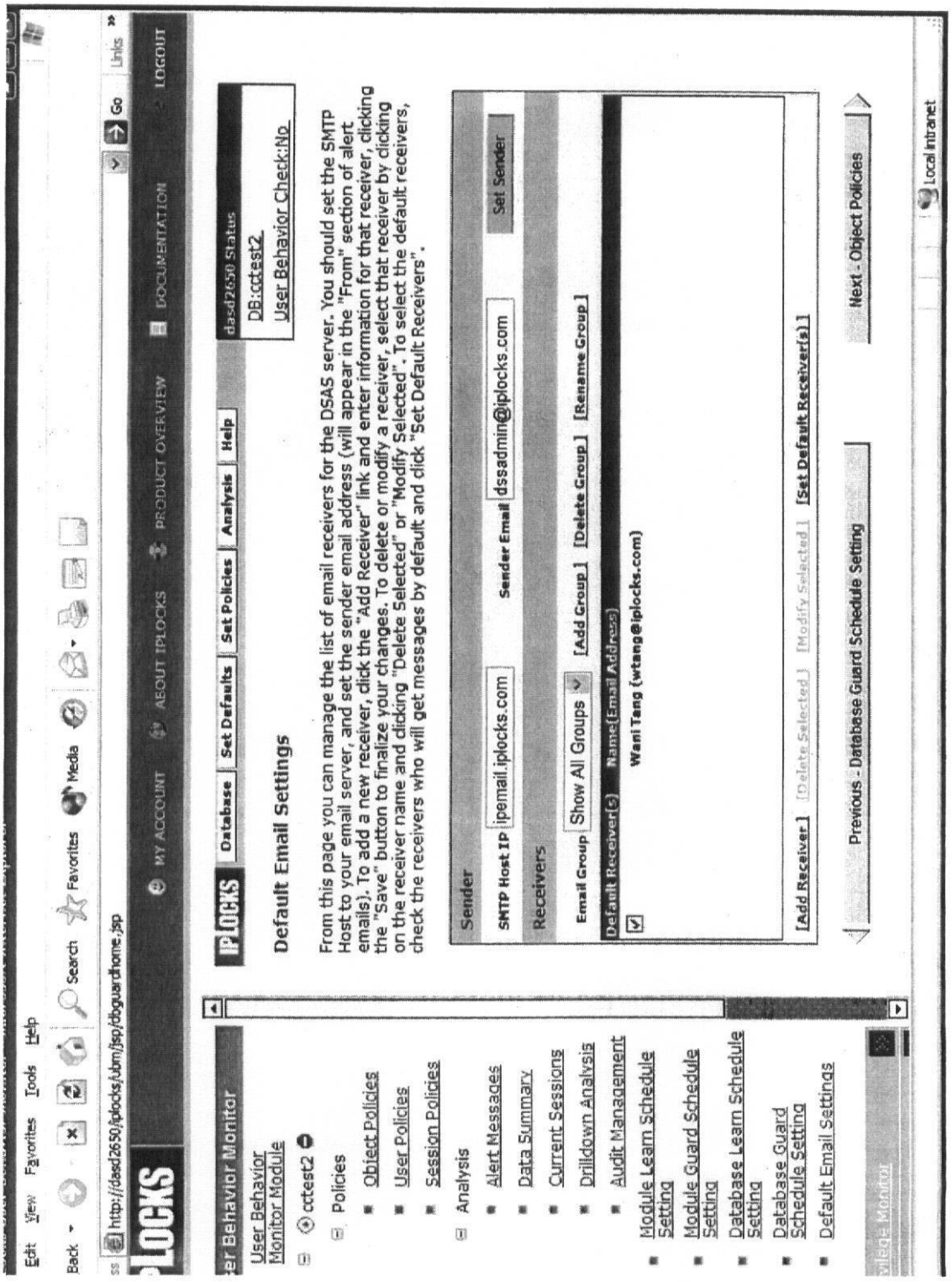
【図６Ｂ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/jsm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
No database is currently opened. Click this link and go to Open Database page. If you don't have any database exist, please go to Create New Database Connection page first.
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Metadata Monitor
Content Monitor
Configuration Vulnerability Assessment
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
No database specified
Open Target Database
Choose The Target Database
cctest2
db_oracle8_db2serv_o817
db_oracle9_boradd1_md9i
db_oracle8_dbora1_cctest2
db_oracle8_ipora8_ip8i
db_oracle8_ipora8_orack
db_oracle8_ipora8_otest
db_oracle8_ipora8_ora8db
db_oracle9_somyfh27_wani
db_oracle7_ora7_dmdb
db_oracle7_ora7_emdb
db_oracle8_sunv100
[Modify] [Delete]
Open
Open and Run
Close
Previous - Create New Database Connection
Next - Module Schedule Setting
Applet com.iplocks.dss.graphs.dopgraph.DistributionChartApplet started
Local intranet

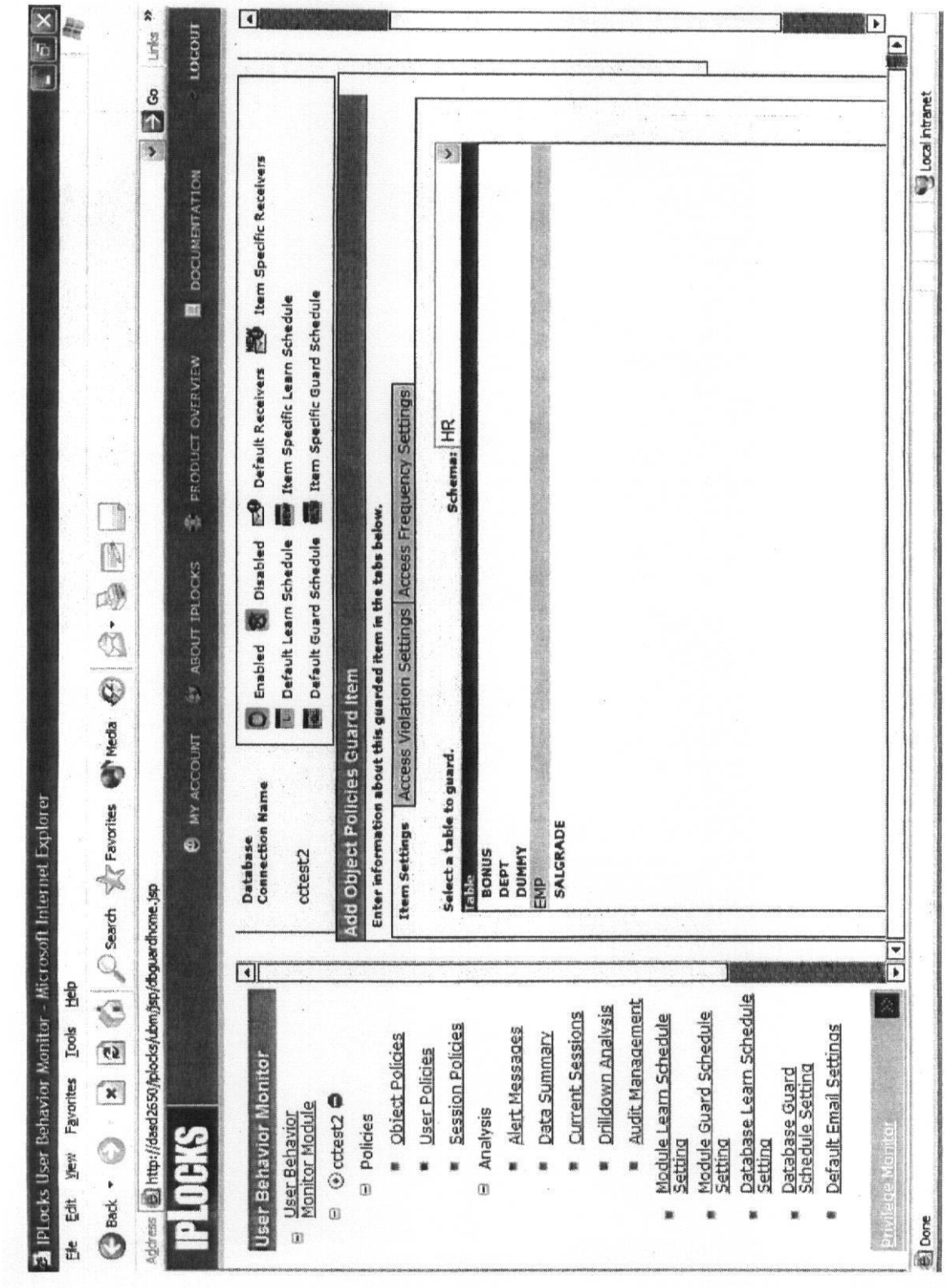
【図６Ｃ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT ABOUT IPLOCKS PRODUCT OVERVIEW DOCUMENTATION LOGOUT
User Behavior Monitor
User Behavior Monitor Module
octest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
IPLOCKS Database Set Defaults Set Policies Analysis Help
dasd2650 Status
DB:octest2
User Behavior Check:No
Module Learn Schedule Setting
Set Timer Schedule
Interval
Hours: 1
Minutes: 0
Seconds: 0
Time to start scanning
When Running
Hr : Min 0 : 00 am
* To set timer schedule, you must click Set Timer button.
Set Timer Delete Timer
Set Calendar Schedules
Calendar
Scan Time
[Add Schedule] [Delete Schedule] [Modify Schedule]
Local intranet

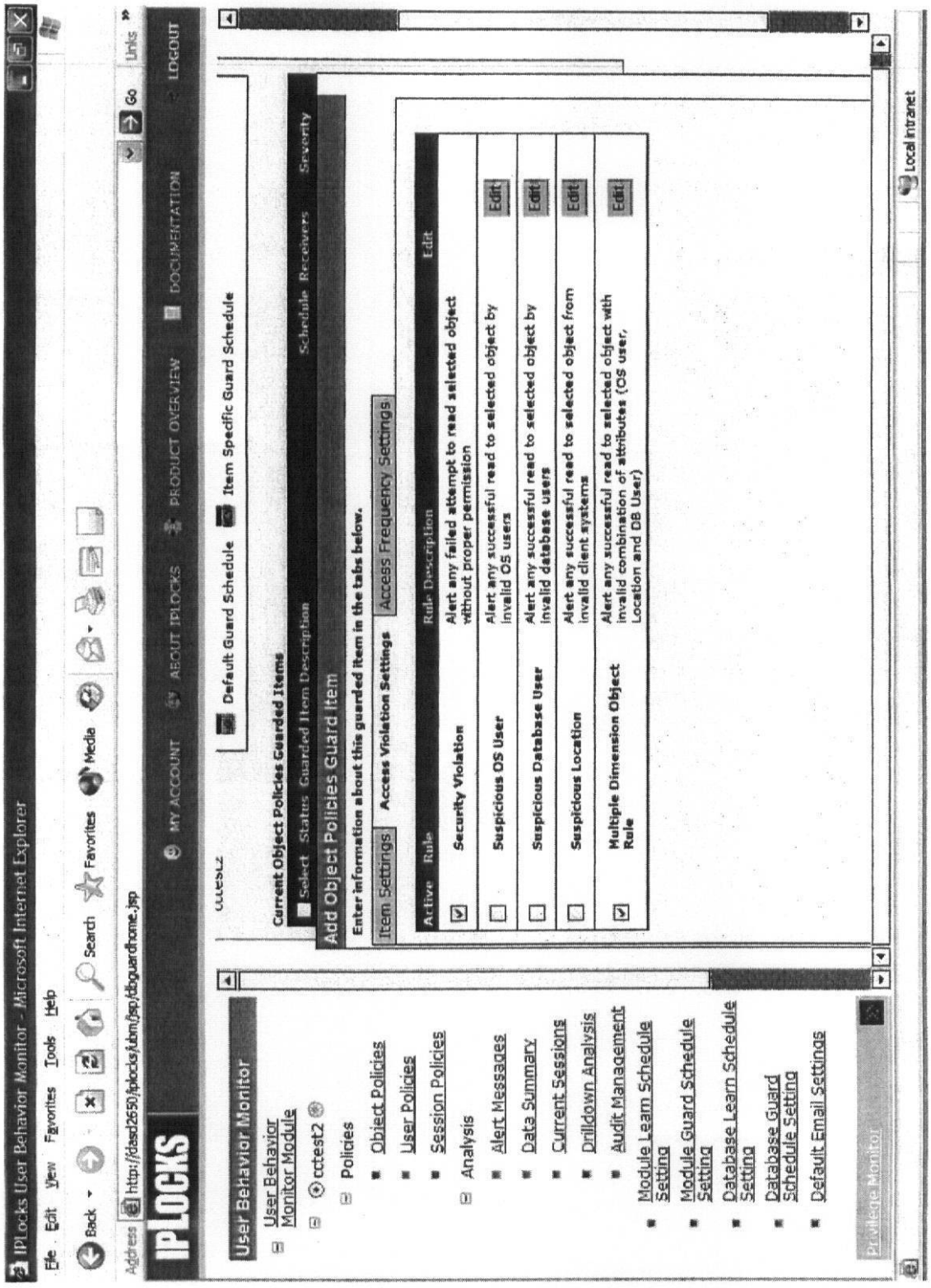
【図６Ｄ】


Edit View Favorites Tools Help
Back Search Favorites Media
http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
octest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
DB:octest2
User Behavior Check:No
Default Email Settings
From this page you can manage the list of email receivers for the DSAS server. You should set the SMTP Host to your email server, and set the sender email address (will appear in the "From" section of alert emails). To add a new receiver, click the "Add Receiver" link and enter information for that receiver, clicking the "Save" button to finalize your changes. To delete or modify a receiver, select that receiver by clicking on the receiver name and clicking "Delete Selected" or "Modify Selected". To select the default receivers, check the receivers who will get messages by default and click "Set Default Receivers".
Sender
SMTP Host IP ipemail.iplocks.com
Sender Email dssadmin@iplocks.com
Set Sender
Receivers
Email Group Show All Groups
[Add Group] [Delete Group] [Rename Group]
Default Receiver(s)
Name(Email Address)
Wani Tang (wtang@iplocks.com)
[Add Receiver] [Delete Selected] [Modify Selected] [Set Default Receiver(s)]
Previous - Database Guard Schedule Setting
Next - Object Policies
Local intranet

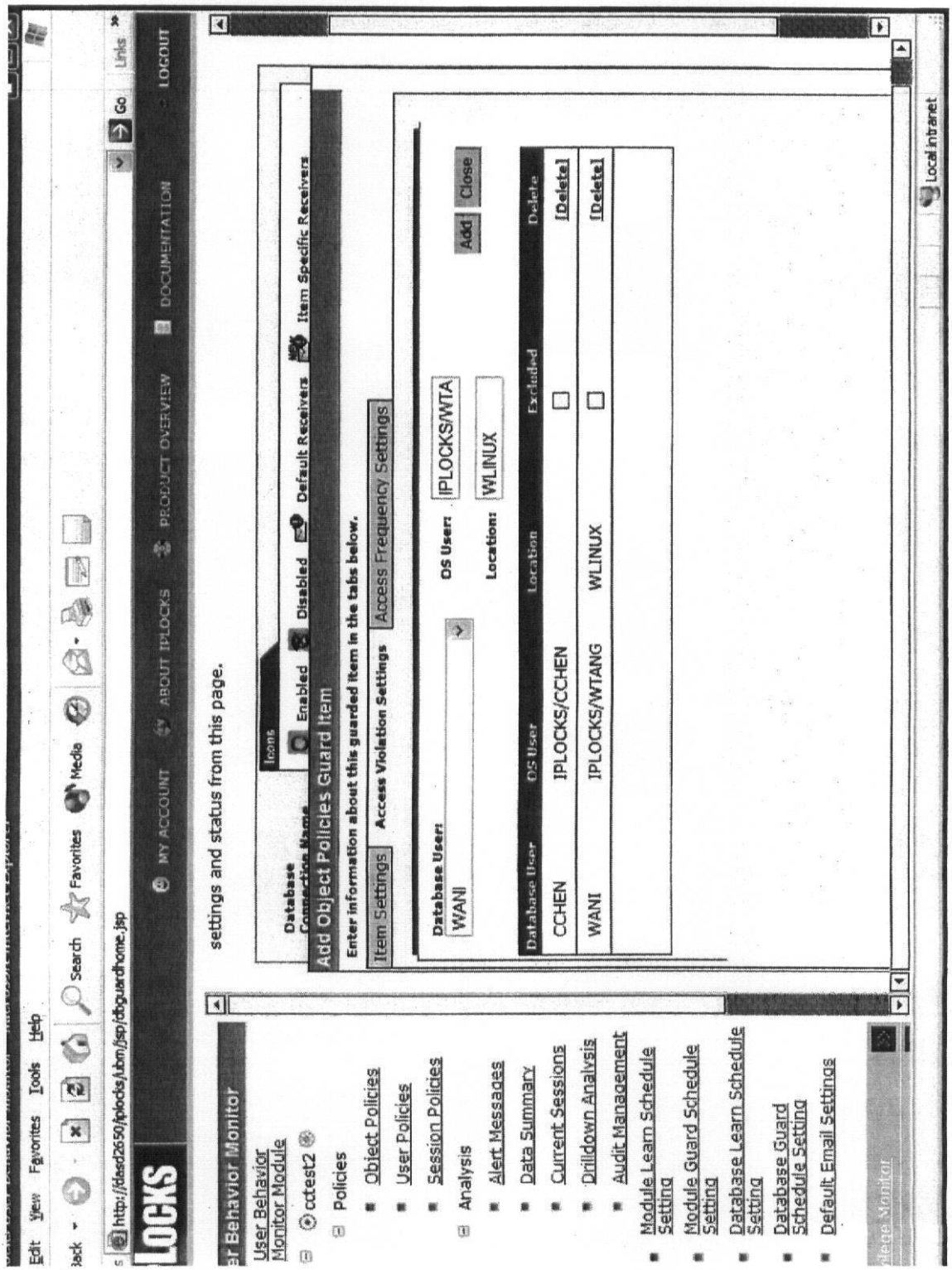
【図６Ｅ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dsed2650/iplocks/tbm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Database Connection Name
cctest2
Enabled
Disabled
Default Receivers
Item Specific Receivers
Default Learn Schedule
Item Specific Learn Schedule
Default Guard Schedule
Item Specific Guard Schedule
Add Object Policies Guard Item
Enter information about this guarded item in the tabs below.
Item Settings
Access Violation Settings
Access Frequency Settings
Select a table to guard.
Schema: HR
Table
BONUS
DEPT
DUMMY
EMP
SALGRADE
Done
Local intranet

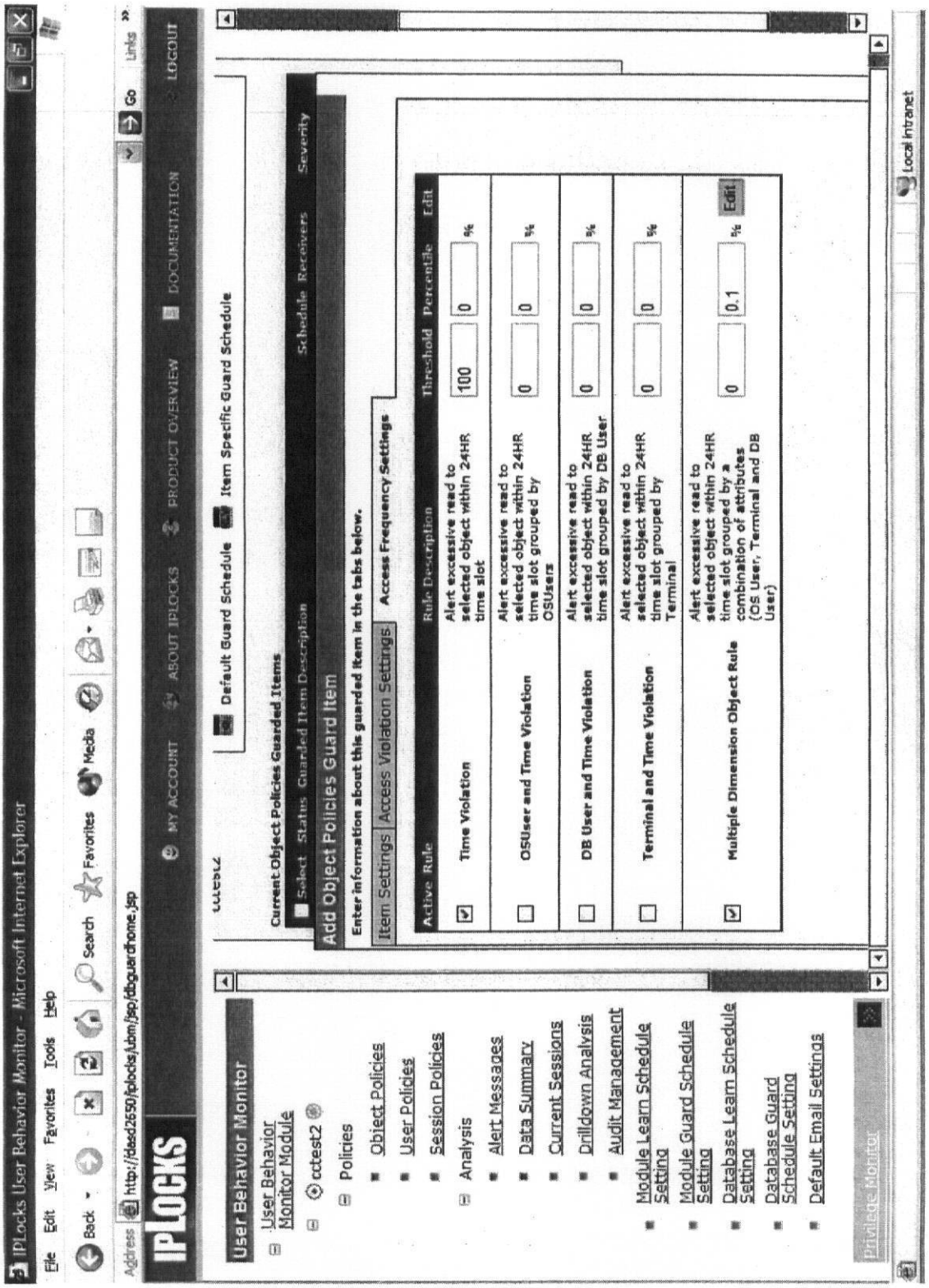
【図６Ｆ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
cctest2
Default Guard Schedule
Item Specific Guard Schedule
Current Object Policies Guarded Items
Select Status Guarded Item Description Schedule Receivers Severity
Add Object Policies Guard Item
Enter information about this guarded item in the tabs below.
Item Settings
Access Violation Settings
Access Frequency Settings
Active Rule Rule Description Edit
Security Violation
Alert any failed attempt to read selected object without proper permission
Suspicious OS User
Alert any successful read to selected object by invalid OS users
Edit
Suspicious Database User
Alert any successful read to selected object by invalid database users
Edit
Suspicious Location
Alert any successful read to selected object from invalid client systems
Edit
Multiple Dimension Object Role
Alert any successful read to selected object with invalid combination of attributes (OS user, Location and DB User)
Edit
Local intranet

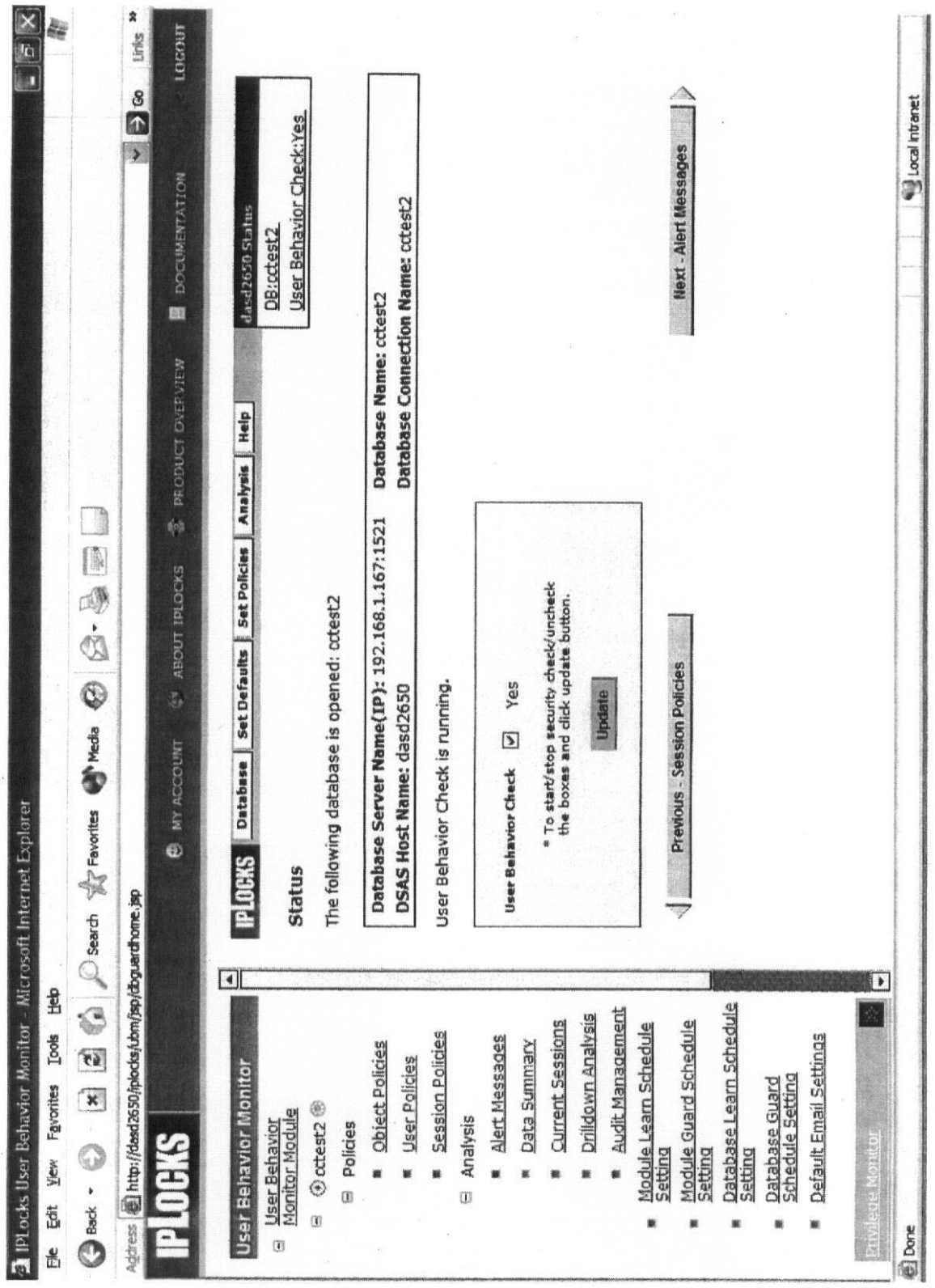
【図６Ｇ】


Edit View Favorites Tools Help
Search Favorites Media
http://dasd2650/iplocks/Jbm/jsp/dbguardhome.jsp
Go Links
LOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
settings and status from this page.
Add Object Policies Guard Item
Enter information about this guarded item in the tabs below.
Item Settings
Access Violation Settings
Access Frequency Settings
Database User:
WANI
OS User:
IPLOCKS/WTA
Location:
WLINUX
Add
Close
Database User
OS User
Location
Excluded
Delete
CCHEN
IPLOCKS/CCHEN
[Delete]
WANI
IPLOCKS/WTANG
WLINUX
[Delete]
Database Connection Name
Icons
Enabled
Disabled
Default Receivers
Item Specific Receivers
Local intranet

【図６Ｈ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dead2650/iplocks/ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
Default Guard Schedule
Item Specific Guard Schedule
Current Object Policies Guarded Items
Select
Status
Guarded Item Description
Schedule
Receivers
Severity
Add Object Policies Guard Item
Enter information about this guarded item in the tabs below.
Item Settings
Access Violation Settings
Access Frequency Settings
Active
Rule
Rule Description
Threshold
Percentile
Edit
Time Violation
Alert excessive read to selected object within 24HR time slot
100
0
%
OSUser and Time Violation
Alert excessive read to selected object within 24HR time slot grouped by OSUsers
0
0
%
DB User and Time Violation
Alert excessive read to selected object within 24HR time slot grouped by DB User
0
0
%
Terminal and Time Violation
Alert excessive read to selected object within 24HR time slot grouped by Terminal
0
0
%
Multiple Dimension Object Rule
Alert excessive read to selected object within 24HR time slot grouped by a combination of attributes (OS User, Terminal and DB User)
0
0.1
%
Edit
Local intranet

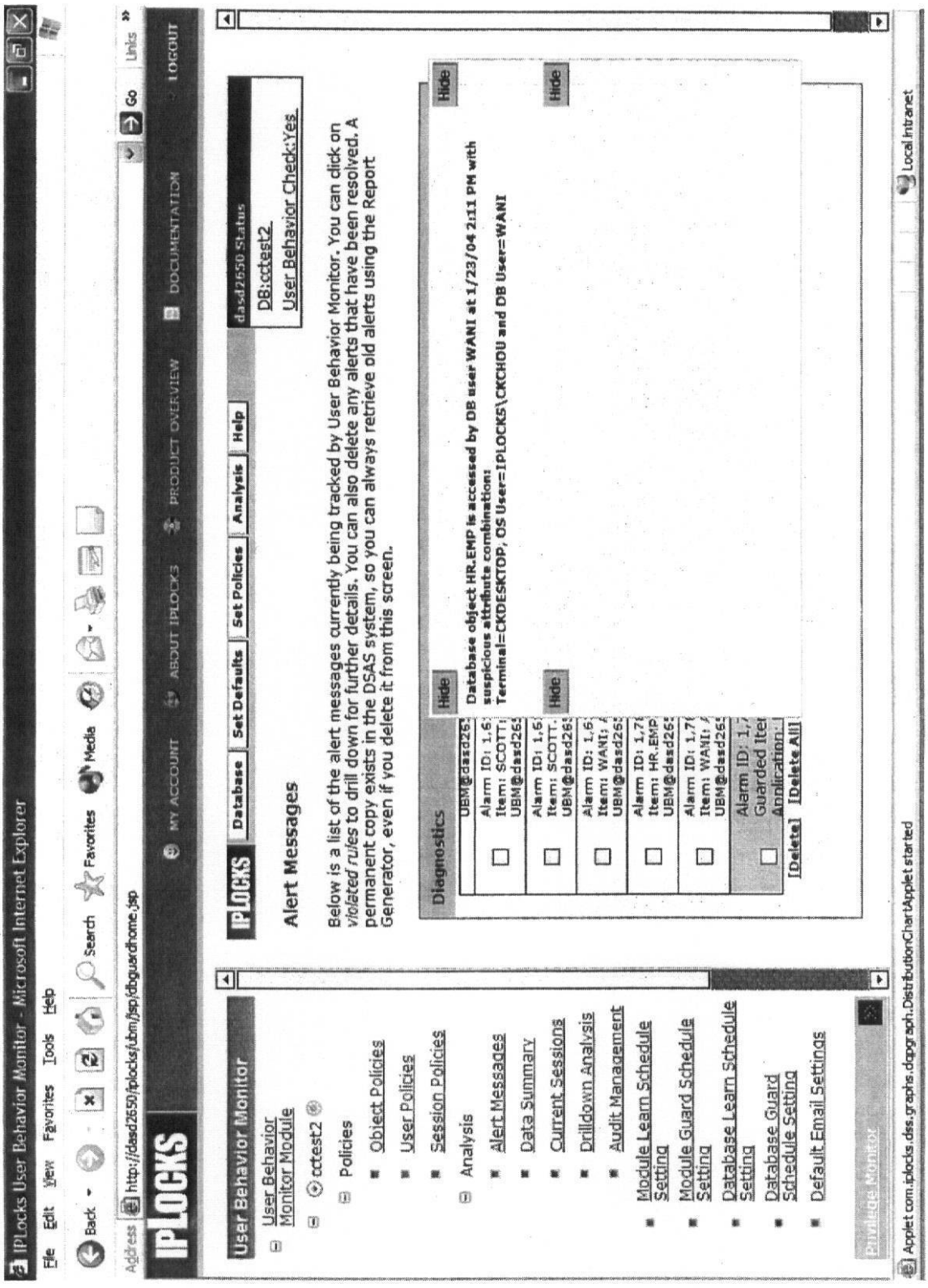
【図６Ｉ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
Links
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
DB:cctest2
User Behavior Check:Yes
Status
The following database is opened: cctest2
Database Server Name(IP): 192.168.1.167:1521
DSAS Host Name: dasd2650
Database Name: cctest2
Database Connection Name: cctest2
User Behavior Check is running.
User Behavior Check
Yes
* To start/stop security check/uncheck the boxes and click update button.
Update
Previous - Session Policies
Next - Alert Messages
Done
Local intranet

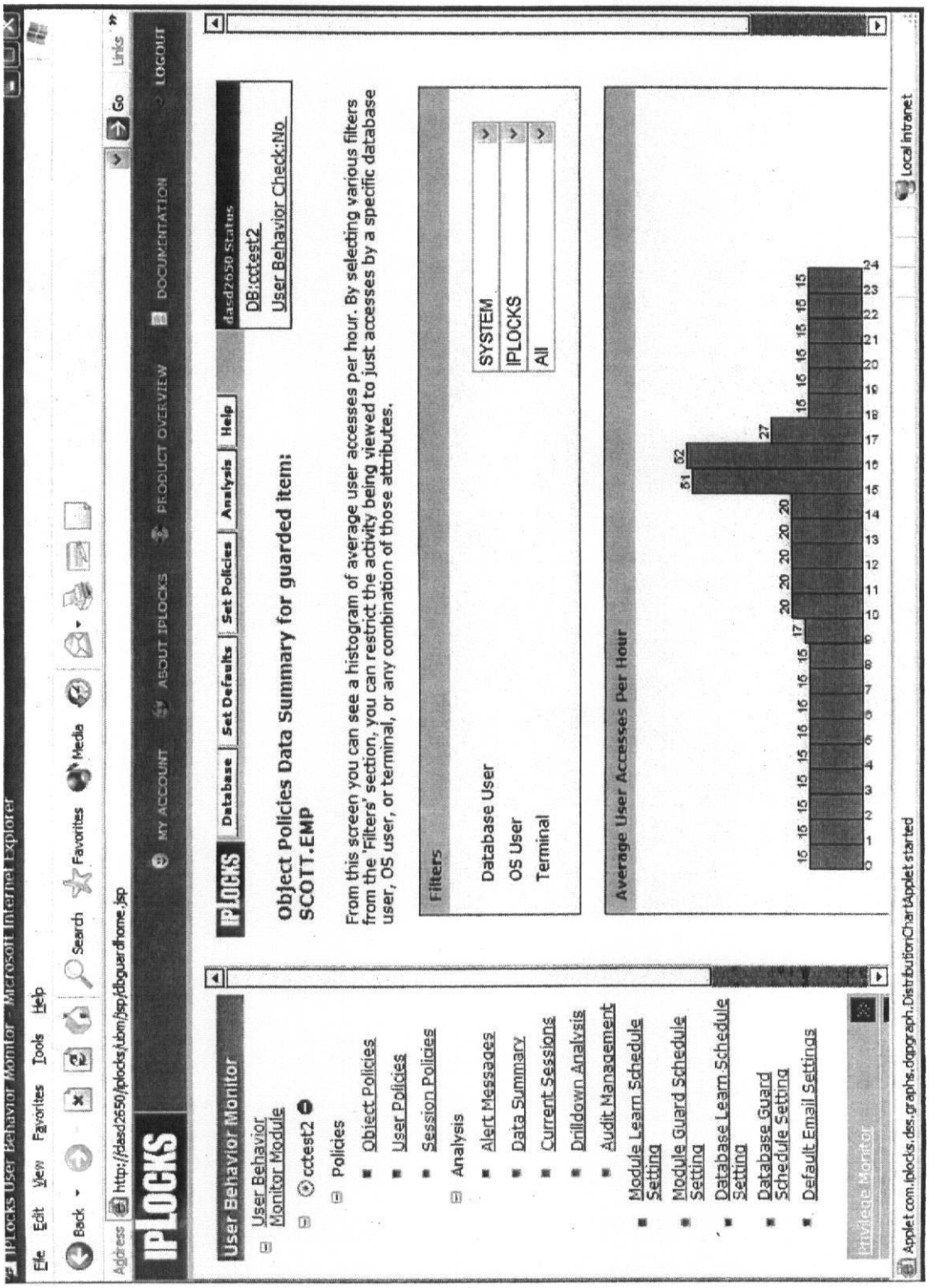
【図６Ｊ】

cautionary UBM alert raised from cctest2 (Object Policies:HR.EMP) - Message (HTML) - Unicode (UTF-8)
File Edit View Insert Format Tools Actions Help
Reply Reply to All Forward
From: dssadmin@iplocks.com
Sent: Fri 1/23/2004 2:11 PM
To: Wani Tang
Cc:
Subject: cautionary UBM alert raised from cctest2 (Object Policies:HR.EMP)
Brief Description:
Alarm ID: 1,782
Severity: cautionary
Violated Policy: Object Policies
Guarded Item: HR.EMP
Alarm Generated Time: 2004-01-23 14:24:22
Application: UBM@dasd2650:80
Database: CCTEST2@192.168.1.166:1521
Detailed Description:
Database object HR.EMP is accessed by DB user WANI at 1/23/04 2:11 PM with suspicious attribute combination:
Terminal=CKDESKTOP, OS User=IPLOCKS\CKCHOU and DB User=WANI
To update alarm status use the link:Update Status

【図６Ｋ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/ubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
DB:cctest2
User Behavior Check:Yes
Alert Messages
Below is a list of the alert messages currently being tracked by User Behavior Monitor. You can click on violated rules to drill down for further details. You can also delete any alerts that have been resolved. A permanent copy exists in the DSAS system, so you can always retrieve old alerts using the Report Generator, even if you delete it from this screen.
Diagnostics
Hide
Database object HR.EMP is accessed by DB user WANI at 1/23/04 2:11 PM with suspicious attribute combination:
Terminal=CKDESKTOP, OS User=IPLOCKS\CKCHOU and DB User=WANI
[Delete]
[Delete All]
Applet com.iplocks.dss.graphs.dggraph.DistributionChartApplet started
Local Intranet

【図６Ｌ】


IPLocks User Behavior Monitor - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/jubm/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
User Behavior Monitor
User Behavior Monitor Module
cctest2
Policies
Object Policies
User Policies
Session Policies
Analysis
Alert Messages
Data Summary
Current Sessions
Drilldown Analysis
Audit Management
Module Learn Schedule Setting
Module Guard Schedule Setting
Database Learn Schedule Setting
Database Guard Schedule Setting
Default Email Settings
Privilege Monitor
IPLOCKS
Database
Set Defaults
Set Policies
Analysis
Help
dasd2650 Status
DB:cctest2
User Behavior Check:No
Object Policies Data Summary for guarded item:
SCOTT.EMP
From this screen you can see a histogram of average user accesses per hour. By selecting various filters from the 'Filters' section, you can restrict the activity being viewed to just accesses by a specific database user, OS user, or terminal, or any combination of those attributes.
Filters
Database User
OS User
Terminal
SYSTEM
IPLOCKS
All
Average User Accesses Per Hour
Applet com.iplocks.dss.graphs.dspgraph.DistributionChartApplet started
Local intranet

【図６Ｍ】

IPLocks Alarm Report Manager - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://dasd2650/iplocks/dse/reports/jsp/dbguardhome.jsp
IPLOCKS
MY ACCOUNT
ABOUT IPLOCKS
PRODUCT OVERVIEW
DOCUMENTATION
LOGOUT
Alarm Report Manager
Alarm Report Manager
Current Reports
Schedule Setting
Default Email Settings
Privilege Monitor
Metadata Monitor
Content Monitor
User Behavior Monitor
Configuration Vulnerability Assessment
Rule Chaining
Policy Management
IPLOCKS
Set Defaults
Reports
Help
dasd2650 Status
Report Running:No
Preview Report Setting
Report Information
Report Name: ubm-cctest2
Date Generated: 2004-01-16 14:17:10
Applications: UBM
Database: cctest2
Number of Alarms Meeting Criteria: 5
* To sort column click on header.
ID
App
Database
Policy
Guarded Item
Severity
Status
Time
1156 UBM cctest2 User Policies CCHEN cautionary Error_Corrected 2003/12/19 11:32
1157 UBM cctest2 Session Policies SCOTT cautionary Not Handled 2003/12/19 11:33
1616 UBM cctest2 Session Policies SCOTT cautionary Not Handled 2004/01/16 13:36
1618 UBM cctest2 Object Policies SCOTT.EMP cautionary Not Handled 2004/01/16 13:54
1619 UBM cctest2 Session Policies WANI cautionary Acknowledged 2004/01/16 14:11
Informational 0 Cautionary 5 Minor 0 Major 0 Critical
Export to Excel Tab Delimited Comma Delimited
Previous - Current Reports
Next - Status
Done
Local intranet

フロントページの続き

(74)代理人 100109162
弁理士 酒井 將行
(72)発明者 坂本 昭夫
アメリカ合衆国、９５０１４ カリフォルニア州、キューパーティーノ、メテオール・プレイス、１０５６４
(72)発明者 チュン－クアン・チョウ
アメリカ合衆国、９４０８６ カリフォルニア州、サニィベイル、フクシア・ドライブ、１０８７
(72)発明者 ワニ・ジィ・タン
アメリカ合衆国、９５０７０ カリフォルニア州、サラトガ、キャニオン・ビュー・ドライブ、２０８５１
(72)発明者 ジアングオ・フ
アメリカ合衆国、９５０５４ カリフォルニア州、サンタ・クララ、マンション・コート、５１０、ナンバー・２０１

Ｆターム(参考) 5B017 AA07 BA09 BB02 CA16