(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第4843546号
(P4843546)
(45)発行日　平成23年12月21日(2011.12.21)　(24)登録日　平成23年10月14日(2011.10.14)

(51)Int.Cl.　F I
G06F 21/24 (2006.01)　G06F 12/14　560B

請求項の数 5　(全 21 頁)

(21)出願番号　特願2007-91729(P2007-91729)
(22)出願日　平成19年3月30日(2007.3.30)
(65)公開番号　特開2008-250728(P2008-250728A)
(43)公開日　平成20年10月16日(2008.10.16)
審査請求日　平成21年3月31日(2009.3.31)

(73)特許権者　500257300
ヤフー株式会社
東京都港区赤坂９丁目７番１号
(74)代理人　110000637
特許業務法人樹之下知的財産事務所
(74)代理人　100079083
弁理士　木下　實三
(74)代理人　100094075
弁理士　中山　寛二
(74)代理人　100106390
弁理士　石崎　剛
(72)発明者　津留　雅文
東京都港区六本木六丁目１０番１号　ヤフー株式会社内

最終頁に続く

(54)【発明の名称】情報漏洩監視システムおよび情報漏洩監視方法

(57)【特許請求の範囲】
【請求項１】
秘密情報を蓄積するデータベースの情報漏洩を抑止する情報漏洩監視システムであって、
前記データベースに対する特定のユーザに関するアクセス計画情報の登録要求を受けて登録済アクセス計画情報を生成するアクセス計画登録手段と、
前記登録済アクセス計画情報の承認要求を受けて承認済アクセス計画情報を生成するアクセス計画承認手段と、
前記承認済アクセス計画情報から前記データベースのセキュリティポリシー情報を生成するセキュリティポリシー生成手段と、
前記データベースに対する実アクセス情報を監査ログデータベースに蓄積記憶する手段と、
前記セキュリティポリシー情報を参照して、前記監査ログデータベースに記憶された実アクセス情報から異常アクセスを検出する異常アクセス検出手段と
を備え、
前記アクセス計画承認手段は、前記アクセス計画情報に関するアクセスリスク許容値の入力を受け付けるアクセスリスク許容値入力手段を有し、
前記セキュリティポリシー情報には前記アクセスリスク許容値が含まれ、
前記異常アクセス検出手段は、前記実アクセス情報からアクセスリスク値を算出し、このアクセスリスク値が前記アクセスリスク許容値を超えた際に異常アクセスとして検出す

る
ことを特徴とする情報漏洩監視システム。
【請求項２】
請求項１に記載した情報漏洩監視システムにおいて、
更に、前記異常アクセスを検出した際に予め指定された関係者へ通知する異常アクセス通知手段
を備えたことを特徴とする情報漏洩監視システム。
【請求項３】
請求項１または請求項２に記載した情報漏洩監視システムにおいて、
前記セキュリティポリシー情報は前記アクセスリスク許容値のみで構成される
ことを特徴とする情報漏洩監視システム。
【請求項４】
請求項１から請求項３のいずれかに記載した情報漏洩監視システムにおいて、
前記異常アクセス検出手段は、前記アクセスリスク値の計算にあたって、ＳＱＬ文のステートメント、コマンドの種類、アクセス対象のオブジェクトの少なくとも何れかを含む情報に対して機密性の度合いをリスク指数として重み付けたリスクテーブルを利用する
ことを特徴とする情報漏洩監視システム。
【請求項５】
秘密情報を蓄積するデータベースの情報漏洩を抑止する情報漏洩監視方法であって、
情報漏洩監視システムが、
前記データベースに対するアクセス計画情報の登録要求を受けて登録済アクセス計画情報を生成するアクセス計画登録ステップと、
前記登録済アクセス計画情報の承認要求を受けて承認済アクセス計画情報を生成するアクセス計画承認ステップと、
前記承認済アクセス計画情報から前記データベースのセキュリティポリシー情報を生成するセキュリティポリシー生成ステップと、
前記データベースに対する実アクセス情報を監査ログデータベースに蓄積記憶する記憶ステップと、
前記セキュリティポリシー情報を参照して、前記監査ログデータベースに記憶された実アクセス情報から異常アクセスを検出する異常アクセス検出ステップと、
を実施し、
前記アクセス計画承認ステップは、前記アクセス計画情報に関するアクセスリスク許容値の入力を受け付け、
前記セキュリティポリシー情報には前記アクセスリスク許容値が含まれ、
前記異常アクセス検出ステップは、前記実アクセス情報からアクセスリスク値を算出し、このアクセスリスク値が前記アクセスリスク許容値を超えた際に異常アクセスとして検出する
ことを特徴とする情報漏洩監視方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、情報漏洩監視システムおよび情報漏洩監視方法に関し、ネットワーク上のデータベースに蓄積される個人情報等の秘密情報の漏洩防止に関する。
【背景技術】
【０００２】
近年、インターネット上の仮想商店など、ネットワークを利用した電子商取引等のサービスが普及している。これらのサービスにおいては、個人情報等の顧客情報をデータベースシステムに蓄積することが一般的である。例えば、ＩＴ機器をベースとしたインターネットのサービスにおいては、サービス運用のため、顧客情報、クレジット番号等の個人情報を取り扱う必要性があり、これらの情報は、データベースシステムに蓄積される。

これらの顧客情報は秘密情報であり、情報漏洩が生じないように厳重に管理することが求められている。

【０００３】

一方、サービス提供者がシステムに蓄積する顧客情報は、利用者の急増に伴って増加の一途をたどっている。これに伴い、これらの情報が漏洩することによるサービス提供者のリスク及び管理コストも増加している。これらの情報は、いったんインターネット上で漏洩すると、大規模なネットワークの特性上、漏洩先の全てを辿って完全に漏洩情報を削除することは困難である。

【０００４】

ところで、ネットワーク上の情報漏洩に関して、インターネットの発展過程においては、外部からのネットワークへの侵入による当該情報アクセスに対する対策が主流であった。これに対し、最近は内部犯罪による脅威が増加している。

従来型の外部侵入に関しては、既に様々な対策技術が開発されている。例えば、社外からの不正アクセスに対して蓄積情報を保護する方法としては、ファイヤウォール、アクセス制御機能等多様な手法が利用されている。さらに、暗号化手法の改善、ハードウェア機器の処理速度の向上等によって、外部侵入に対する堅牢性は更に向上している。

その結果、ネットワークの内部は外部から厳重に保護されるようになっており、外部からの不正アクセスによって非合法的に当該情報が参照、取得される等による情報漏洩の脅威は少なくなっている。

【０００５】

しかし、近年の情報漏洩事件に代表される諸問題の多くは、システム開発者、システム運用者、メンテナンスなどの受託者など、ネットワーク内部の人物による不正アクセスである。

このような、保護されたネットワークの内部での不正アクセスは、前述した既存の対策技術で防止することが難しい。

すなわち、ネットワーク内部の正当なアクセス権限を持った人物のアクセスは、例え情報の引き抜きや複製などの不正アクセスであっても、表面的には正常なシステムの利用状態と何ら変わらない。このため、前述したファイヤウォールや暗号化等の社外を想定した対策技術では、内部不正アクセスの識別が困難である。そして、近年ではこのような内部不正アクセスによる情報漏洩が問題となってきている。

これらは、企業の信頼喪失、ひいては、インターネットを利用した将来のビジネスの発展を阻害しかねない。

【０００６】

このような内部不正アクセスに対して、最近では、保護すべき情報を蓄積するデータベースそのものへのアクセスの履歴（ログ）により、ポアソン分布等の統計的手法を取り入れ、定常的なアクセスパターンを逸脱するアクセスを検出することによって、本来の正常アクセス以外の意図的な行動を検出し、管理者へ通知する技術が開発されている（特許文献１参照）。

また、システム運用者の犯罪を防止する技術として、従来システム運用者へはシステムに対する特権つまり広範なアクセス権限を付与するのが一般的であるが、運用者自体のリスクを低減するために、通常は必要最小限のアクセス権限のみを付与しておき、メンテナンス等の際など必要な場合に限って特権を付与するとした技術が開発されている（特許文献２参照）。

【０００７】

【特許文献１】特開２００５－２５９１４０号公報

【特許文献２】特許第３７９３９４４号公報

【発明の開示】

【発明が解決しようとする課題】

【０００８】

しかしながら、前述した統計処理による不正検出は、データベースシステムを利用する

アプリケーションの仕様の変更や、突発的なメンテナンス等によるデータベースアクセスが発生した場合、誤動作することが発生し得る。また、定常のアクセスパターンであることを認識することに難点がある。そのため、統計情報を概観する人的な介入が余儀なくされ、判断に対する個人差によって画一的な監視が難しい。そして、解析内容を人的な手段にて精査する必要があり、実務的な観点から管理コストの増加、監視品質のばらつきを招く。

一方、前述した状況によりアクセス権を切り替える手法においては、運用目的で一旦アクセス権が付与された状態では、その権限の範囲内で特定のデータへアクセス可能であり、悪意があればこの段階で情報を取得することが可能となってしまうという問題がある。

【０００９】

本発明の目的は、前述した従来の手法の問題を回避できる情報漏洩監視システムおよび情報漏洩監視方法を提供することである。

【課題を解決するための手段】

【００１０】

本発明の情報漏洩監視システムは、秘密情報を蓄積するデータベースの情報漏洩を抑止する情報漏洩監視システムであって、前記データベースに対する特定のユーザに関するアクセス計画情報の登録要求を受けて登録済アクセス計画情報を生成するアクセス計画登録手段と、前記登録済アクセス計画情報の承認要求を受けて承認済アクセス計画情報を生成するアクセス計画承認手段と、前記承認済アクセス計画情報から前記データベースのセキュリティポリシー情報を生成するセキュリティポリシー生成手段と、前記データベースに対する実アクセス情報を監査ログデータベースに蓄積記憶する手段と、前記セキュリティポリシー情報を参照して、前記監査ログデータベースに記憶された実アクセス情報から異常アクセスを検出する異常アクセス検出手段とを備え、前記アクセス計画承認手段は、前記アクセス計画情報に関するアクセスリスク許容値の入力を受け付けるアクセスリスク許容値入力手段を有し、前記セキュリティポリシー情報には前記アクセスリスク許容値が含まれ、前記異常アクセス検出手段は、前記実アクセス情報からアクセスリスク値を算出し、このアクセスリスク値が前記アクセスリスク許容値を超えた際に異常アクセスとして検出することを特徴とする。

【００１１】

このような本発明では、特定のユーザ（前記データベースにアクセスする内部のアクセス者）は、予め自らのアクセス計画を登録し、これを承認者が承認する。承認されたアクセス計画は、システムから参照可能なポリシーに変換され、実際のアクセスの監視に利用される。そして、実アクセスのうち、予め登録ないし承認されたアクセス計画に沿ったアクセスは異常と判定されないが、アクセス計画に沿わないアクセスは異常と判定される。このため、アクセス権限を有する内部のアクセス者であっても、アクセス計画にない不正なアクセスを行うとこれが検出されることになり、内部不正アクセスの防止に利用できる。なお、アクセス計画の登録は主にアクセス者が自ら行うが、申請に基づいて他者が代行してもよい。

【００１２】

本発明の情報漏洩監視システムにおいて、更に、前記異常アクセスを検出した際に予め指定された関係者へ通知する異常アクセス通知手段を備えることが望ましい。

このような本発明では、異常アクセスが検出された際に関係者への通知を行うことで、通知を受けた関係者が適宜対応することができ、内部の不正アクセスであっても防止することができる。

【００１３】

本発明の情報漏洩監視システムにおいて、前記アクセス計画承認手段は、前記アクセス計画情報に関するアクセスリスク許容値の入力を受け付けるアクセスリスク許容値入力手段を有し、前記セキュリティポリシー情報には前記アクセスリスク許容値が含まれ、前記異常アクセス検出手段は、前記実アクセス情報からアクセスリスク値を算出し、このアクセスリスク値が前記アクセスリスク許容値を超えた際に異常アクセスとして検出すること

が望ましい。
　このような本発明では、承認者がアクセス者に関するアクセスリスク許容値を設定し、実アクセスにおけるアクセスリスクの評価により異常検出を行うことで、処理負荷の軽減を図りながら確実な検出を行うことができる。
【００１４】
　本発明の情報漏洩監視システムにおいて、前記セキュリティポリシー情報は前記アクセスリスク許容値のみで構成されることが望ましい。
　このような本発明では、異常検出をアクセス者のアクセスリスクに絞ることで、処理負荷を軽減でき、かつ十分な検出制度を確保することができる。
【００１５】
　本発明の情報漏洩監視システムにおいて、前記異常アクセス検出手段は、前記アクセスリスク値の計算にあたって、ＳＱＬ文のステートメント、コマンドの種類、アクセス対象のオブジェクトの少なくとも何れかを含む情報に対して機密性の度合いをリスク指数として重み付けたリスクテーブルを利用することが望ましい。
　このような本発明では、情報に応じてリスクテーブルを参照することでアクセスリスクの計算を簡単かつ確実に行える。
【００１６】
　本発明の情報漏洩監視システムは、秘密情報を蓄積するデータベースの情報漏洩を抑止する情報漏洩監視システムであって、
　前記データベースに対するアプリケーションソフトウェアのアクセスシーケンスおよびアクセスタイミングをアプリケーション認証情報として登録するアプリケーション認証情報登録手段と、
　前記アプリケーション認証情報から前記データベースのセキュリティポリシー情報を生成するセキュリティポリシー生成手段と、
　前記データベースに対する実アクセス情報を監査ログデータベースに蓄積記憶する手段と、
　前記セキュリティポリシー情報を参照して、前記監査ログデータベースに記憶された前記アプリケーションソフトウェアの実アクセス情報に基づくアクセスパターン情報と比較することにより異常アクセスを検出する異常アクセス検出手段と
　を備えたことを特徴とする。
【００１７】
　このような本発明では、アクセス者による異常アクセスとは別に、データベースを利用するアプリケーションソフトウェアの改ざん等による不正アクセスを検出することができる。
　すなわち、アプリケーションソフトウェアが正常に動作している状態では、そのアクセス挙動は一定のパターンを示す。これに対し、不正アクセス等を実行するようにアプリケーションソフトウェアに改ざん等が行われると、そのアクセス挙動は正常時とは異なったものとなる。このため、アプリケーションソフトウェアの正常時のアクセス挙動（アクセスシーケンスおよびアクセスタイミング）をアプリケーション認証情報として記録しておき、これを参照して実際のアクセス挙動を検査することで、アプリケーションソフトの改ざんあるいは不正アクセスを検出することができる。
【００１８】
　本発明の情報漏洩監視システムにおいて、前記アプリケーションソフトウェアに関する前記セキュリティポリシー情報は前記アプリケーションソフトウェアのアクセスシーケンスのみで構成されることが望ましい。
　このような本発明では、異常検出をアプリケーションソフトウェアのアクセスシーケンスのみに絞ることで、処理負荷を軽減でき、かつ十分な検出制度を確保することができる。
【００１９】
　本発明の情報漏洩監視方法は、秘密情報を蓄積するデータベースの情報漏洩を抑止する

情報漏洩監視方法であって、情報漏洩監視システムが、前記データベースに対するアクセス計画情報の登録要求を受けて登録済アクセス計画情報を生成するアクセス計画登録ステップと、前記登録済アクセス計画情報の承認要求を受けて承認済アクセス計画情報を生成するアクセス計画承認ステップと、前記承認済アクセス計画情報から前記データベースのセキュリティポリシー情報を生成するセキュリティポリシー生成ステップと、前記データベースに対する実アクセス情報を監査ログデータベースに蓄積記憶する記憶ステップと、前記セキュリティポリシー情報を参照して、前記監査ログデータベースに記憶された実アクセス情報から異常アクセスを検出する異常アクセス検出ステップと、を実施し、前記アクセス計画承認ステップは、前記アクセス計画情報に関するアクセスリスク許容値の入力を受け付け、前記セキュリティポリシー情報には前記アクセスリスク許容値が含まれ、前記異常アクセス検出ステップは、前記実アクセス情報からアクセスリスク値を算出し、このアクセスリスク値が前記アクセスリスク許容値を超えた際に異常アクセスとして検出することを特徴とする。

【００２０】

本発明の情報漏洩監視方法は、秘密情報を蓄積するデータベースの情報漏洩を抑止する情報漏洩監視方法であって、情報漏洩監視システムが、前記データベースに対するアプリケーションソフトウェアのアクセスシーケンスおよびアクセスタイミングをアプリケーション認証情報として登録し、前記アプリケーション認証情報から前記データベースのセキュリティポリシー情報を生成し、前記データベースに対する実アクセス情報を監査ログデータベースに蓄積記憶し、前記セキュリティポリシー情報を参照して、前記監査ログデータベースに記憶された前記アプリケーションソフトウェアの実アクセス情報に基づくアクセスパターン情報と比較することにより異常アクセスを検出することを特徴とする。

【００２１】

これらの本発明の情報漏洩監視方法では、前述した本発明の情報漏洩監視システムで説明したように、予め設定された承認済アクセス計画情報あるいはアプリケーション認証情報を参照して実際のデータベースアクセスを検査することで、アクセス者の不正アクセスあるいは改ざん等によるアプリケーションソフトウェアによる不正アクセスを検出することができる。

【発明を実施するための最良の形態】

【００２２】

以下、本発明の実施形態を図面に基づいて説明する。

図１には、本発明が適用された電子商取引サービスシステム１が示されている。

電子商取引サービスシステム１は、ネットワークを経由して接続される多数の顧客（サービスユーザ）３１に対してデータベースシステム２により電子商取引サービスを提供するものである。

【００２３】

データベースシステム２は、データベースサーバ１０およびアプリケーションサーバ２０を備え、データベースサーバ１０に各種サービスに必要な情報を記憶するとともに、アプリケーションサーバ２０に格納されたアプリケーションソフトウェア２１により各種サービスを提供する。

【００２４】

ここで、データベースサーバ１０は顧客情報等の秘密情報を含むものであり、これらの秘密情報の漏洩を防止するために、電子商取引サービスシステム１には本発明に基づく情報漏洩監視システム４０が設置されている。

以下、システム各部について詳細に説明する。

なお、以下の説明において、サービスユーザ３１等の語はシステムに関与する人のことを指すが、システムに直接関与するのはコンピュータ端末等であるため、図面上では端末機器の絵柄で表示している。

また、データベースサーバ１０には複数のデータベースが構築されていてもよく、その

うち少なくとも一つが情報漏洩監視システムの監視対象であればデータベースシステム２は監視対象とされる。データベースサーバ１０における複数のデータベースの識別は既存のデータベース名称等で適宜識別される。

【００２５】

［１］サービスユーザの接続

図２に示すように、電子商取引サービスシステム１にはＤＭＺ（非武装地帯）３を介してインターネット等の外部ネットワーク４が接続されている。電子商取引サービスシステム１の電子商取引サービス（以下Ｗｅｂサービスとも呼ぶ）を利用するサービスユーザ３１は、外部ネットワーク４においてルータ２５およびファイヤウォール２４を経由してウェブサーバ２３に接続される。

ウェブサーバ２３は、サービスユーザ３１と電子商取引サービスシステム１のインターフェースを提供するもので、Ｗｅｂサービスに必要なサービスユーザ３１からの情報入力や物品購入等の指示を行うための画面表示や入出力機能等をサービスユーザ３１の端末に提供する。サービスユーザ３１により入力される顧客情報は、ファイヤウォール２２を経由してアプリケーションサーバ２０へ引き渡され、データベースサーバ１０に記録される。

従って、データベースサーバ１０には秘密情報として厳重に管理すべき顧客情報等が蓄積される。

【００２６】

［２］データベースサーバに対するアクセス

電子商取引サービスシステム１において、データベースサーバ１０へのアクセスとしては、前述したアプリケーションサーバ２０に格納されてＷｅｂサービスを提供するアプリケーションソフトウェア２１によるものがあるほか、システムの保守管理のためのアクセスがある。

図３に示すように、データベースシステム２において、データベースサーバ１０およびアプリケーションサーバ２０には、その開発から運用にあたってシステム開発者を含むシステム保守担当者３２の関与が必要である。また、アプリケーションソフトウェア２１の設定ないし保守のために、データベースサーバ１０およびアプリケーションサーバ２０にはデータ保守担当者を含むアプリケーション運用担当者３３の関与が必要である。更に、アプリケーションソフトウェア２１の設定あるいは更新などのために、アプリケーション開発者あるいはアプリケーション保守担当者３４の関与が必要となる。

【００２７】

これらのシステム保守担当者３２、アプリケーション運用担当者３３、アプリケーション保守担当者３４によるデータベースシステム２へのアクセスについては、通常、各々の担当業務で必要となる必要最低限のアクセス権限が付与される。

ここで、データベースシステム２の内部で発生する問題の多くは、これら付与された権限の範囲内で実施可能なアクセスによって漏洩する可能性があり、従来のセキュリティ技術で防止することは非常に難しい。

そこで、本実施形態の電子商取引サービスシステム１には、データベースシステム２を監視対象とする情報漏洩監視システム４０が設置されている。

【００２８】

［３］情報漏洩監視システム４０の概要

図１に戻って、本実施形態の情報漏洩監視システム４０は、前述したアプリケーション運用担当者３３、アプリケーション保守担当者３４等の内部のアクセス者からの不正アクセスを監視する機能を有するとともに、前述したアプリケーションソフトウェア２１の改ざんによる不正アクセスを監視する機能を有する。

【００２９】

内部のアクセス者からの不正アクセスを監視する機能として、アクセス者（３２～３４）がデータベースサーバ１０内のデータベースへのアクセス計画情報５１の登録要求を受けて登録済アクセス計画情報５２を生成し、登録済アクセス計画情報５２の承認要求を受

けて承認済アクセス計画情報５３を生成し、承認済アクセス計画情報５３からデータベースサーバ１０のセキュリティポリシー情報５９を生成し、セキュリティポリシー情報５９を参照してデータベースサーバ１０の実際のアクセス記録情報（アクセスログ１２）から異常アクセスを検出する、という各手順を実行する。

【００３０】

アプリケーションソフトウェア２１の改ざんによる不正アクセスを監視する機能として、データベースサーバ１０内のデータベースに対するアプリケーションソフトウェア２１のアクセスシーケンスおよびアクセスタイミングをアプリケーション認証情報５４として登録し、アプリケーション認証情報５４からデータベースサーバ１０のセキュリティポリシー情報５９を生成し、セキュリティポリシー情報５９を参照してデータベースサーバ１０に対するアプリケーションソフトウェア２１の実際のアクセス記録から異常アクセスを検出する、という各手順を実行する。

【００３１】

このような各手順を実行するために、監視対象であるデータベースシステム２にはエージェント１１が設置されており、情報漏洩監視システム４０にはワークフローサーバ４１、ポリシーデータベース４２、ログ監視サーバ４３が設置されている。

【００３２】

［４］情報漏洩監視システム４０の詳細

（ワークフローサーバ）

ワークフローサーバ４１は、本発明の情報漏洩監視方法に基づいて、アクセス計画の登録、承認、セキュリティポリシーの生成までを行うものである。

本発明に基づく情報漏洩監視方法のうち、アクセス計画の登録、承認、セキュリティポリシーの生成までを行うものである。

【００３３】

図４に示すように、ワークフローサーバ４１は、アクセス計画登録手段であるアクセス計画登録機能４１１、アクセス計画承認手段であるアクセス計画承認機能４１２、セキュリティポリシー生成手段であるセキュリティポリシー生成機能４１３、アプリケーション認証情報登録機能４１５を備えるとともに、Ｗｅｂサーバシステム管理機能４１７、Ｗｅｂサーバ監視機能４１８、対策実施確認機能４１９を備えている。なお、本発明における異常アクセス検出手段であるポリシー判定機能４３２はログ監視サーバ４３に配置されている。

図５には、前述したアクセス計画登録機能４１１により登録されるアクセス計画情報５１および登録済アクセス計画情報５２、アクセス計画承認機能４１２で生成される承認済アクセス計画情報５３、アプリケーション認証情報登録機能４１５で生成されるアプリケーション認証情報５４の詳細が示されている。

【００３４】

アクセス計画登録機能４１１は、アクセス者（システム保守担当者３２、アプリケーション運用担当者３３、アプリケーション保守担当者３４）によるデータベースサーバ１０内のデータベースへのアクセス計画情報５１を登録することで登録済アクセス計画情報５２を生成する処理を行う。

アクセス計画情報５１は、監視対象であるデータベースシステム２へアクセスする必要があるアクセス者が、当該システムにアクセスする前に、「誰が、何時、どのような目的でアクセスを実施するか」等を計画情報として設定するものであり、通常は本人がアクセス計画登録機能４１１から登録要求することで登録済アクセス計画情報５２となる。

登録済アクセス計画情報５２はアクセス計画情報５１と同じ内容である。

【００３５】

図５において、登録済アクセス計画情報５２（アクセス計画情報５１も同じ）は、アクセス者（３２～３４）がデータベースシステム２へのアクセスに先立ってそのアクセスに関する計画情報を入力するものであり、アクセス目的の「作業名」、アクセス者の「作業担当者名」と「所属」、アクセスする「作業日／時間帯」と「アクセス先ＤＢ名」と「ア

クセス先ホスト名」、「ＤＢユーザ名」、「ＩＰアドレス」、アクセスを行う「端末名」と「ＯＳユーザ名」、「アクション」、「対象オブジェクト」、「担当者メールアドレス」、「ポリシー有効期限」を備えている。

【００３６】

図４において、アクセス計画承認機能４１２は、登録済アクセス計画情報５２を承認者３９が承認することで承認済アクセス計画情報５３を生成する処理を行う。

承認者３９は、アクセス者（３２～３４）等の作業者の管理責任者であり、作業者によって登録された登録済アクセス計画情報５２を確認し、承認要求および必要な情報の追加入力を行う。

図５において、承認済アクセス計画情報５３は、前述した登録済アクセス計画情報５２の内容に、「承認者名」、「承認者メールアドレス」、承認者が入力した「アクセスリスク許容値」の情報を追加したものである。

承認者３９は、登録済アクセス計画情報５２に記載された業務の内容に応じて、このアクセス計画のアクセスリスク許容値を設定する。

【００３７】

図４において、アプリケーション認証情報登録機能４１５は、アプリケーションソフトウェア２１の改ざんによる不正アクセスを監視する機能として、データベースサーバ１０に対するアプリケーションソフトウェア２１のアクセスシーケンスおよびアクセスタイミングを調査し、これをアプリケーション認証情報５４として登録する処理を行う。

図５において、アクセスパターン情報（Ｍ１，Ｍ２等）と、そのアプリケーションが動作する時間帯を示すアクセス時間（１，２等）の情報によって構成される。

アプリケーション認証は、Ｗｅｂサービスを行うシステム開発やアプリケーション開発の完了後、試験運用を実施する段階で、監視対象データベースをアクセスするアプリケーションのアクセスパターンを分析し、その特徴情報を利用して正規のアプリケーションとして認証するものであり、アプリケーション自体の改ざん、SQL文改ざん等によるデータベースへの異常アクセスを検出することができる。

アプリケーション認証に関する詳細に関しては、後述する。

【００３８】

図４において、セキュリティポリシー生成機能４１３は、承認済アクセス計画情報５３からデータベースサーバ１０のセキュリティポリシー情報５９を生成するとともに、アプリケーション認証情報５４からデータベースサーバ１０のセキュリティポリシー情報５９を生成する処理を行う。

【００３９】

（ポリシーデータベース）

ポリシーデータベース４２は、本発明の情報漏洩監視方法に基づいて生成されたセキュリティポリシーを記録し、必要に応じてこの情報を提供するものである。

図５に示すように、ポリシーデータベース４２には、登録済アクセス計画情報５２、承認済アクセス計画情報５３が登録されるとともに、予め登録されたアプリケーション認証情報５４か格納されている。更に、データベースサーバ１０に格納された個々のデータベース毎に予め作成されたアクセスリスクテーブル５５が登録されている。

【００４０】

アクセスリスクテーブル５５は、データベースサーバ１０に構築された「データベース名」、各データベースに対する「アクション名」、ＳＱＬ文および対象オブジェクトを示す「オブジェクト」の組み合わせ毎に、想定されるアクセスリスクを示す「リスク指数」を記録したものである。

リスク指数は、監視対象データベースに蓄積される情報の機密性の度合いにより管理者によって設定され、大きな数値ほど機密性が高く、漏洩リスクも高いことを表している。

このアクセスリスクテーブル５５を参照することで、任意のアクセス計画のリスク指数を調査することができる。

【００４１】

（エージェント）
エージェント１１は、情報漏洩監視システム４０が本発明の情報漏洩監視方法に基づいて異常アクセス検出を行う対象であるデータベースサーバ１０の実アクセス情報を提供するものである。
図４に示すように、エージェント１１は、監視対象であるデータベースシステム２上に設置され、データベースサーバ１０にアクセスが行われる毎にアクセスログを生成するものであり、監査ログ設定機能１１１、監査ログ収集機能１１２、監査ログ送信機能１１３、コマンド処理機能１１４を備えている。
【００４２】
監査ログ設定機能１１１はデータベースシステム２に対して初期設定を実施するものであり、コマンド処理機能１１４は監視マネージャであるログ監視サーバ４３からの監査ログ要求１２２等のコマンドを処理するものである。監査ログ収集機能１１２はログ監視サーバ４３からの監査ログ要求１２２に基づいてデータベースシステム２を調べて必要な監査ログを収集するものであり、監査ログ送信機能１１３は収集された監査ログ１２１をログ監視サーバ４３へ送信するものである。
【００４３】
図６に示すように、エージェント１１においては、監視対象であるデータベースシステム２の起動時に、プロセスの初期化（Ｓ６１）を行った後、データベースシステム２に対して監査ログ生成を行うための初期設定を実施する（Ｓ６２）。その後、ログ監視サーバ４３からのコマンドを待機し（Ｓ６３）、受信したコマンド解析を行い（Ｓ６４）、受信したコマンドが監査ログ要求１２２であれば（Ｓ６５）、データベースシステム２から必要な監査ログ１２１を取得し（Ｓ６６）、フォーマット変換を行ってログ監視サーバ４３へ監査ログを送信する（Ｓ６７）。
なお、データベースサーバ１０に複数のデータベースがある場合、エージェント１１も各データベースに対応して複数設けてもよい。
【００４４】
（ログ監視サーバ）
ログ監視サーバ４３は、本発明の情報漏洩監視方法に基づいて、エージェント１１から送られるデータベースサーバ１０の実アクセス情報とポリシーデータベース４２から得られるセキュリティポリシー情報５９とを参照し、異常アクセスの判定を行うものである。
図４に示すように、ログ監視サーバ４３は、監査ログコレクタ機能４３１、ポリシー判定機能４３２、アラート機能４３３、監査ログデータベース４３９を備えている。
【００４５】
監査ログコレクタ機能４３１はエージェント１１によって収集された監査ログ１２１を受信して監査ログデータベース４３９に蓄積するものである。
ポリシー判定機能４３２は、本発明における異常アクセス検出手段であり、ポリシーデータベース４２に蓄積されたセキュリティポリシー情報５９を参照して、監査ログデータベース４３９に記録された監査ログ１２１を分析し、予定外の異常アクセスを検出するものである。
アラート機能４３３はポリシー判定機能４３２から異常アクセス情報５８が出力された際に、アラート情報５７を生成し、メールサーバ４４等を介して監視者３８に通知するものである。
【００４６】
このようなログ監視サーバ４３において、監査ログコレクタ機能４３１は、インターバルタイマーによって定期的に起動され、予め設定された時間が経過するとデータ受信処理を行う。
図７に示すように、監査ログコレクタ機能４３１におけるデータ受信処理は、予め設定された監視対象のデータベースシステム２の情報を取得し（Ｓ７１）、エージェント１１に接続（Ｓ７２）して監査ログ要求１２２を送信し（Ｓ７３）、エラーチェック（Ｓ７４）ののち、エージェント１１から監査ログ１２１を取得し（Ｓ７５）、受信した監査ログ１

２１を監査ログデータベース４３９に格納する（Ｓ７６）。
【００４７】
ポリシー判定機能４３２は、監査ログコレクタ機能４３１におけるデータ受信処理に続いて起動される。
図７に示すように、ポリシー判定機能４３２は、監視対象のデータベースシステム２に関する監査ログ１２１を読み込み（Ｓ８１）、このデータベースシステム２における監査対象データベース名に該当するセキュリティポリシー情報５９をポリシーデータベース４２から読み込む（Ｓ８２）。次に、ポリシー判定を行うための前処理として、セキュリティポリシー情報５９の構文を解析して判定しやすい情報に分解する（Ｓ８３）。ポリシー判定（Ｓ８４）では、アクセス計画情報５１に基づく監査ログ１２１の判定、アプリケーション認証情報５４に基づくアプリケーションのアクセス判定、リスク検知等の判定を行う。これらの何れかの判定で問題が発生した場合（Ｓ８５）、アラートフラグをセットする（Ｓ８６）。収集されている全てのログの判定を実施したら本処理を終える。ここでアラートフラグがセットされた場合、当該DBに関連するポリシー違反情報を監査ログDBに蓄積し、関係者へ対応を即すため、アラート情報５７としてメール等で即座に通知する。
【００４８】
前述したポリシー判定機能４３２によるポリシー判定（図８のＳ８４）においては、アクセス計画情報５１に基づく監査ログ１２１の判定、アプリケーション認証情報５４に基づくアプリケーションのアクセス判定、アクセスリスク値を用いたアクセスリスク判定による異常アクセス検出を行う。
以下に各判定処理の詳細を説明する。
【００４９】
（アクセス計画判定）
ポリシー判定機能４３２によるポリシー判定の一つとしてアクセス計画判定機能がある。
図９に示すように、アクセス計画判定機能は、データベースユーザのアクセス権限を監視するＡＬＣポリシー、アクセス対象を監視するオブジェクトポリシー、アクセス時間帯を監視するタイムポリシー、アクセスする際に利用するデータベースコマンドを監視するアクションポリシーなどの各ポリシー判定により構成される。
各々のポリシー判定は、ログ監視サーバ４３で収集される監査ログ１２１と、ポリシーデータベース４２から読み込まれたセキュリティポリシー情報５９とを比較することによって行う。また、何れのポリシー判定を利用するかは、ポリシーデータベース４２から読み込まれたセキュリティポリシー情報５９により決定される。
図９に示すように、セキュリティポリシー情報５９で指定された検査対象データベースの判定指定を調べ（Ｓ９１）、対応した判定（Ｓ９２～Ｓ９６）を実施し、ポリシー違反情報を監査ログDBに蓄積する（Ｓ９７）。
【００５０】
（条件リスト）
アクセス計画判定機能における各ポリシー判定では、セキュリティポリシー情報５９に基づく下記の条件判定を利用する。
（ａ）　監査ログ１２１のＯＳユーザ名が承認済アクセス計画情報５３のＯＳユーザ名と一致する。
（ｂ）　監査ログ１２１のＤＢユーザ名が承認済アクセス計画情報５３のＤＢユーザ名と一致する。
（ｃ）　監査ログ１２１の対象データベース名が承認済アクセス計画情報５３のアクセス先ＤＢ名と一致する。
（ｄ）　監査ログ１２１のアクションが承認済アクセス計画情報５３のアクションと一致する。
（ｅ）　監査ログ１２１に含まれるホストＩＰアドレスが承認済アクセス計画情報５３の端末ＩＰアドレスと一致する。

（ｆ）　監査ログ１２１に含まれるアクセス日及び時間が承認済アクセス計画情報５３のポリシー有効期限内である。
（ｇ）　監査ログ１２１に含まれるアクセス日時が承認済アクセス計画情報５３のアクセス日及び時間帯の範囲内である。
（ｈ）　監査ログ１２１に含まれるオブジェクト名が承認済アクセス計画情報５３の対象オブジェクトと一致する。
（ｉ）　監査ログ１２１に含まれるオブジェクトオーナが承認済アクセス計画情報５３のＤＢユーザ名と一致する。

【００５１】

（ＡＬＣポリシー判定）

ＡＬＣポリシー判定（Ｓ９２）では、前述した条件リストの条件（ｂ）を必須とし、その他の条件を含めるかどうかはセキュリティポリシー生成機能４１３の設定に従う。

（アクションポリシー判定）

アクションポリシー判定（Ｓ９３）では、前述した条件リストの条件（ｄ）を必須とし、その他の条件を含めるかどうかはセキュリティポリシー生成機能４１３の設定に従う。

（タイムポリシー判定）

タイムポリシー判定（Ｓ９４）では、前述した条件リストの条件（ｇ）を必須とし、その他の条件を含めるかどうかはセキュリティポリシー生成機能４１３の設定に従う。

（オブジェクトポリシー判定）

オブジェクトポリシー判定（Ｓ９５）では、前述した条件リストの条件（ｈ）及び条件（ｉ）を必須とし、その他の条件を含めるかどうかはセキュリティポリシー生成機能４１３の設定に従う。

（カスタムポリシー判定）

カスタムポリシー判定（Ｓ９５）では、前述した条件リストの何れかをセキュリティポリシー生成機能４１３で設定する。

【００５２】

（アプリケーション認証）

ポリシー判定機能４３２によるポリシー判定の一つとしてアプリケーション認証機能が行われる。

アプリケーション認証機能では判定にあたってアプリケーション認証情報５４（図１参照）を利用する。アプリケーション認証情報５４は、データベースサーバ１０にアクセスするアプリケーションソフトウェア２１のアクセスシーケンスおよびアクセスタイミングを記述したものであり、予めワークフローサーバ４１のアプリケーション認証情報登録機能４１５によって登録される。

これらのアクセスシーケンスおよびアクセスタイミング（以下認証パターンという）は、アプリケーションソフトウェア２１の通常動作におけるデータベースアクセスの結果から生成される。具体的には通常動作におけるデータベースアクセスを行った際に得られるアクセスログ１２（監査ログ１２１）を参照する。

【００５３】

図１０において、監査ログ１２１から、認証登録を実施するアプリケーションソフトウェア２１のＤＢユーザ名と同じＤＢユーザ名を有する監査ログを抽出する（Ｓ１０１）。次に、セッション毎のアクセスパターンを解析するため、ＤＢユーザ名が同じ監査ログから更にセッション情報が同一のログ情報を抽出する（Ｓ１０２）。

こうして抽出されたログ情報から、データベースアクセスの開始を示すマーカを検索し、一連のアクセスブロックの先頭を検出する（Ｓ１０３）。そこで検出されたマーカログより、ＤＢユーザ名、ＩＰアドレスを記録する（Ｓ１０４）。以降の抽出ログから順にＳＱＬ文を検出し（Ｓ１０５）、検出したＳＱＬ文の情報を記録し（Ｓ１０６）、実行時間の差を記録し（Ｓ１０７）してゆく。これらの処理Ｓ１０５～Ｓ１０７は終了マーカの検出（Ｓ１０８）まで繰り返す。

終了マーカが検出されたら、全マーカが検出されたかを調べ（Ｓ１０９）、未処理のマ

ーカが残っていれば、次のマーカログのＤＢユーザ名およびＩＰアドレスの記録（Ｓ１０４）から繰り返す。
全マーカが検出し終わったなら、全セッションが検出されたかを調べ（Ｓ１０１０）、未処理のセッションが残っていれば、次のセッション情報と同一のログ情報の抽出（Ｓ１０２）から繰り返す。
全セッションが検出し終わったなら処理を終了する（Ｓ１０１１）。その結果、図１２に示すＤＢユーザ毎のアクセスパターン情報５４Ａが得られる。
【００５４】
図１１において、アクセスパターン情報５４Ａは、ＤＢユーザ名５４１、ＩＰアドレス５４２を有するとともに、複数のアクセスパターンリスト５４３を備えている。
アクセスパターンリスト５４３は、一連のＳＱＬ文情報５４４と、各々の時間間隔情報５４５とを備えている。
これらにより、ＤＢユーザ名５４１、ＩＰアドレス５４２で特定されるアプリケーションソフトウェア２１がデータベースサーバ１０内のデータベースに対して、ある時はアクセスパターン１に記述されたＳＱＬ文の発信パターンでアクセスを行い、別の時にはアクセスパターン２に記述されたパターンの動作を行うことが正常である、ということが識別できる。
このようなアクセスパターン情報５４Ａは、セキュリティポリシー情報５９の一部としてポリシーデータベース４２に記録される。そして、ポリシー判定機能４３２におけるアプリケーション認証機能の際に参照される。
【００５５】
図１２において、アプリケーション認証によるポリシー判定では、先ず監査ログ１２１の読み込みを行い（Ｓ１２１）、ポリシーデータベース４２よりアプリケーション認証情報５４を読み込む（Ｓ１２２）。次に、判定対象のアプリケーションＤＢユーザアカウントのみを抽出し（Ｓ１２３）、さらにセッション毎に分類する（Ｓ１２４）。
分類されたセッション毎の特定ログから開始マーカを検出する（Ｓ１２５）。開始マーカ以降のＳＱＬ文の実行順序と時間間隔を比較し（Ｓ１２６）、その類似性によって、認証されたアプリケーションからのアクセスか否かを判定する（Ｓ１２７）。
類似性が確認できなかった場合、アプリケーションの改ざんがあったと判断し、該当データベース名、マーカ名等、当該アプリケーションを特定する情報を監査ログに蓄積し（Ｓ１２８）、アプリケーション異常フラグをセットする（Ｓ１２９）。
この後、全マーカが検出されたかを調べ（Ｓ１２１０）、未処理のマーカが残っていれば、次のマーカについて処理Ｓ１２５から処理Ｓ１２１０を繰り返す。
全マーカが検出し終わったなら、全セッションが検出されたかを調べ（Ｓ１２１１）、未処理のセッションが残っていれば、処理Ｓ１２５から処理Ｓ１２１１を繰り返す。
全セッションが検出し終わったなら処理を終了する。
【００５６】
（アクセスリスク判定）
ポリシー判定機能４３２によるポリシー判定の一つとしてアクセスリスク判定が行われる。
アクセスリスク判定ではアクセスリスクテーブル５５（図５参照）および承認者により設定されて承認済アクセス計画情報５３に記述されるアクセスリスク許容値を利用する。
図１３にアクセスリスク判定によるアクセス危険度判定機能の動作フローを示す。
アクセスリスク判定では、先ず監査ログ１２１を読み込み（Ｓ１３１）、アクセス者（３２～３４）によるアクセスの危険度を算出するため、ポリシーデータベース４２に記録されたアクセスリスクテーブル５５を読み込む（Ｓ１３２）。次に、分析対象のユーザアカウントに関連した監査ログを抽出し（Ｓ１３３）、その抽出されたログをさらにセッション毎に分類する（Ｓ１３４）。そして、アクセスリスクテーブル５５に記述されたリスク指数をもとに、ＳＱＬ文毎のリスク指数を積算し、単位時間毎の積算値の推移を記録してゆく（Ｓ１３５）。同様、特定ユーザアカウントの全てのセッションに関して、処理を

実行する（Ｓ１３６）。全セッションの終了後、単位時間当たりのリスク積算値と閾値であるアクセスリスク許容値とを比較し（Ｓ１３７）、このアクセスリスク許容値を上回った場合にはリスク異常インシデントを監査ログＤＢに格納し（Ｓ１３８）、リスク異常フラグをセットする（Ｓ１３９）。

このようなアクセスリスク判定では、アクセス者に関するアクセスリスク許容値を設定し、実アクセスにおけるアクセスリスクの評価により異常検出を行うことで、処理負荷の軽減を図りながら確実な検出を行うことができる。

【００５７】

図４において、Ｗｅｂサーバシステム管理機能４１７は、データベースシステム２の管理を行うために必要な既存の機能を提供する。

また、Ｗｅｂサーバ監視機能４１８および対策実施確認機能４１９は以下の監視機能を提供する。

【００５８】

（監視機能）

Ｗｅｂサーバ監視機能４１８は、前述した各判定による異常発生など、データベース毎に発生したインシデントをリアルタイムに表示、対処する機能を備える。ポリシー判定機能４３２によるポリシー判定の結果は、監査ログデータベース４３９にその都度蓄積され、迅速な対処を要求するため、その旨をメール等によるアラート情報５７として送信する。

アラート情報５７を受けた現場の監視者３８は、アラートを発生させた監視対象データベースのアクセス者（３２～３４）を特定し、実施確認を行ない、承認者３９へその旨報告する。

Ｗｅｂサーバ監視機能４１８は、定期的に監査ログデータベース４３９をモニターしており、新規のインシデントが発生した場合、関連情報を監査ログデータベース４３９より取得し、監視端末に表示する。監査報告を受けた監視者３８は、実施者報告に問題があった場合は、緊急対応と判断し、アラート発生の要因を作ったアクセス者（３２～３４）の端末からの接続を遮断し、監視機能を利用して以降のアクセスを拒否する設定を実施する。

対策実施確認機能４１９は、Ｗｅｂサーバ監視機能４１８をモニタし、予め定められた時間内に前述した実施確認が取れない場合は、自動的に先述の遮断処理を実施する。

【００５９】

本発明を利用することにより、従来技術であるファイヤウォールや、ネットワークセキュリティにより防止することが難しかった内部犯罪による情報漏洩を防止することができる。また、ＩＴ犯罪の被害の多くは、社外からのアタックではなく、内部者によるケースが増えてきており、問題が発生した場合の会社の信用失墜によるダメージは膨大なものとなっている。従来のネットワークセキュリティでは、アクセス権付与による限定アクセスが一般的であるが、一度付与された権限の範疇で当該情報へのアクセスを行うことによる情報の漏洩の可能性に関しては抑制することができなかった問題に対しても、抑止効果が得られる。また、データベースへのアクセスは、Ｗｅｂサービスを利用する一般ユーザ数増加に伴いより多くのアクセスが発生し、生成される監査ログも膨大なものとなる。これら膨大なログ情報から異常アクセスを見つけ出す監視者のコスト低減や、精度向上が期待できる。さらに、内部統制等の法律遵守のためのツールとしても有効である。

【００６０】

なお、本発明は前述した実施形態に限定されるものではなく、本発明の目的を達成できる範囲内での変形等は本発明に含まれるものである。

前記実施形態におけるネットワーク構成あるいはシステム構成は適宜変更することができる。

例えば、前記実施形態では、承認者３９とは別に監視者３８を設定してアラート情報７５が送られるようにしたが、アラート情報５７は承認者３９にも送ってもよく、あるいは承認者３９が兼ねる場合は監視者３８を省略してもよい。

前記実施形態における処理の詳細、手順あるいはその順序の詳細は適宜変更することができる。各処理の具体的な手法としてはその機能に応じて既存のソフトウェア技術を適宜採用することができる。

【産業上の利用可能性】

【００６１】

本発明は、情報漏洩監視システムおよび情報漏洩監視方法に利用でき、ネットワーク上のデータベースに蓄積される個人情報等の秘密情報の漏洩防止に利用できる。

【図面の簡単な説明】

【００６２】

【図１】本発明の一実施形態の全体構成を示すブロック図。

【図２】前記実施形態における外部の顧客ユーザのアクセスを示す模式図。

【図３】前記実施形態における内部のアクセス者のアクセスを示す模式図。

【図４】前記実施形態における情報漏洩監視システムの概要を示すブロック図。

【図５】前記実施形態におけるデータの関連を示すブロック図。

【図６】前記実施形態におけるエージェントのアクセスログ収集動作を示すフローチャート。

【図７】前記実施形態におけるログ監視サーバのアクセスログデータ受信処理を示すフローチャート。

【図８】前記実施形態におけるポリシー判定処理の概略を示すフローチャート。

【図９】前記実施形態におけるアクセス計画判定によるポリシー判定処理を示すフローチャート。

【図１０】前記実施形態におけるアプリケーション認証情報の登録処理を示すフローチャート。

【図１１】前記実施形態におけるアプリケーション認証情報を示す模式図。

【図１２】前記実施形態におけるアプリケーション認証判定処理を示すフローチャート。

【図１３】前記実施形態におけるアクセスリスク判定処理を示すフローチャート。

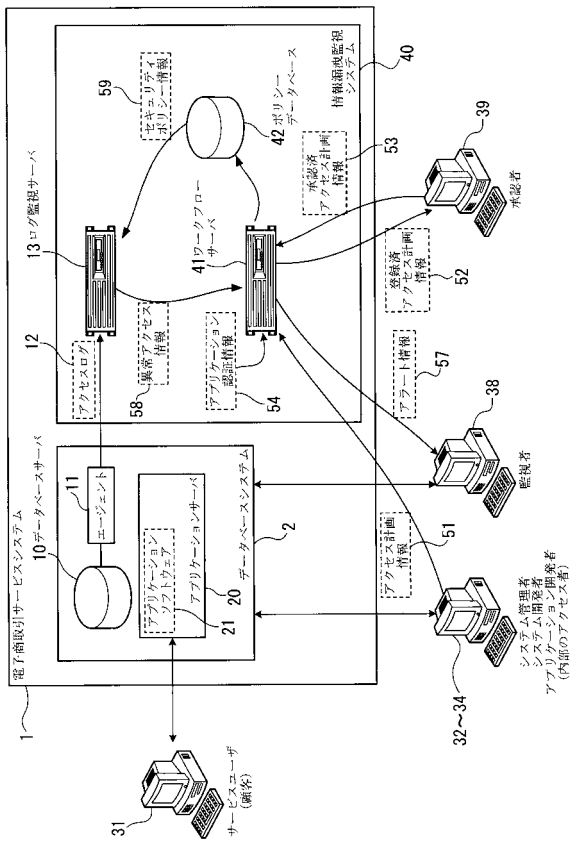
【符号の説明】

【００６３】

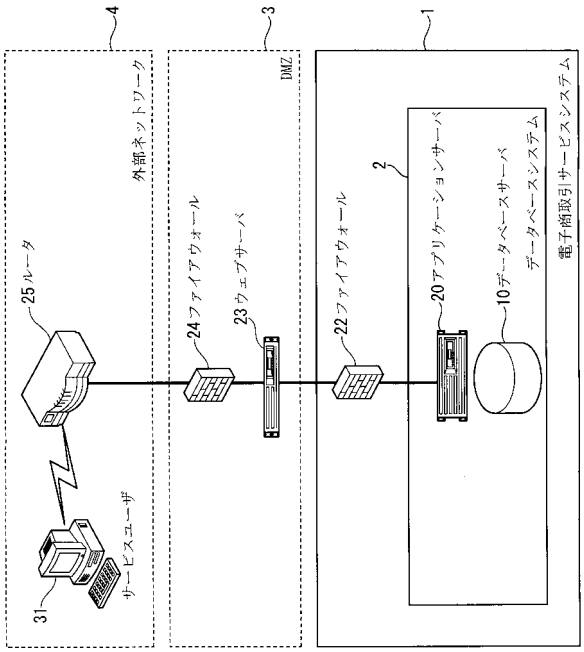
１　電子商取引サービスシステム
２　データベースシステム
４　外部ネットワーク
１０　データベースサーバ
１１　エージェント
１２　アクセスログ（アクセス記録情報）
２０　アプリケーションサーバ
２１　アプリケーションソフトウェア
２２　ファイヤウォール
２３　ウェブサーバ
２４　ファイヤウォール
２５　ルータ
３１　サービスユーザ
３２　システム保守担当者
３３　アプリケーション運用担当者
３４　アプリケーション保守担当者
３８　監視者
３９　承認者
４０　情報漏洩監視システム
４１　ワークフローサーバ
４２　ポリシーデータベース
４３　ログ監視サーバ

４４　メールサーバ
５１　アクセス計画情報
５２　登録済アクセス計画情報
５３　承認済アクセス計画情報
５４Ａ　アクセスパターン情報
５４　アプリケーション認証情報
５５　アクセスリスクテーブル
５７　アラート情報
５８　異常アクセス情報
５９　セキュリティポリシー情報
１１１　監査ログ設定機能
１１２　監査ログ収集機能
１１３　監査ログ送信機能
１１４　コマンド処理機能
１２１　監査ログ
１２２　監査ログ要求
４１１　アクセス計画登録機能（アクセス計画登録手段）
４１２　アクセス計画承認機能（アクセス計画承認手段）
４１３　セキュリティポリシー生成機能（セキュリティポリシー生成手段）
４１５　アプリケーション認証情報登録機能（アプリケーション認証情報登録手段）
４１７　サーバシステム管理機能
４１８　サーバ監視機能
４１９　対策実施確認機能
４３１　監査ログコレクタ機能
４３２　ポリシー判定機能（異常アクセス検出手段）
４３３　アラート機能
４３９　監査ログデータベース
５４１　ユーザ名
５４２　アドレス
５４３　アクセスパターンリスト
５４４　文情報
５４５　時間間隔情報

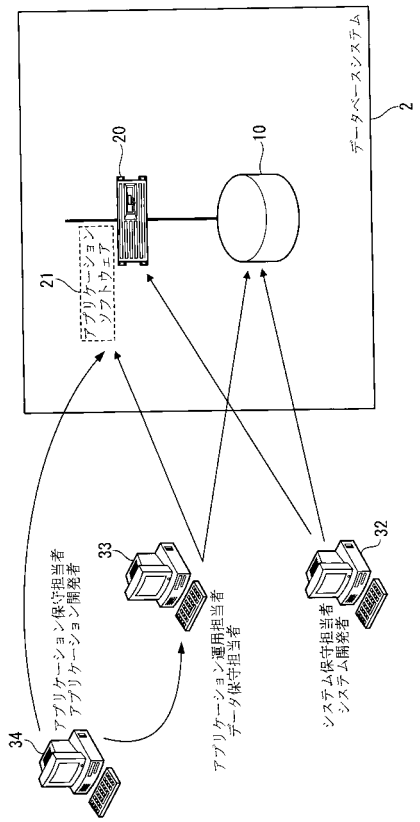
【図１】


電子商取引サービスシステム
データベースサーバ
10
11
エージェント
アプリケーション
ソフトウェア
21
アプリケーションサーバ
20
データベースシステム
2
ログ監視サーバ
13
アクセスログ
12
異常アクセス情報
58
アプリケーション認証情報
54
ワークフローサーバ
41
セキュリティポリシー情報
59
ポリシーデータベース
42
承認済アクセス計画情報
53
情報漏洩監視システム
40
登録済アクセス計画情報
52
アラート情報
57
アクセス計画情報
51
1
31
サービスユーザ（顧客）
32～34
システム管理者
システム開発者
アプリケーション開発者
（内部のアクセス者）
監視者
38
承認者
39

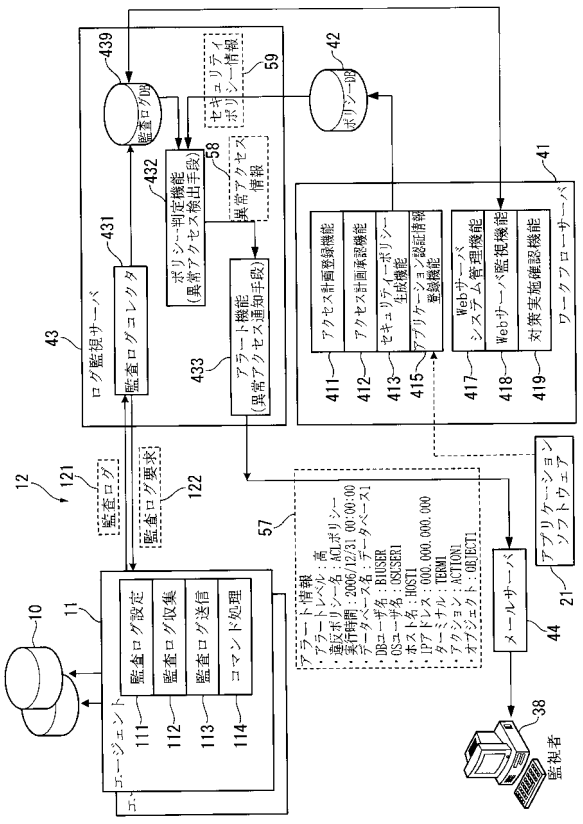
【図２】


4
外部ネットワーク
3
DMZ
1
2
25ルータ
24ファイアウォール
23ウェブサーバ
22ファイアウォール
20アプリケーションサーバ
10データベースサーバ
データベースシステム
電子商取引サービスシステム
31
サービスユーザ

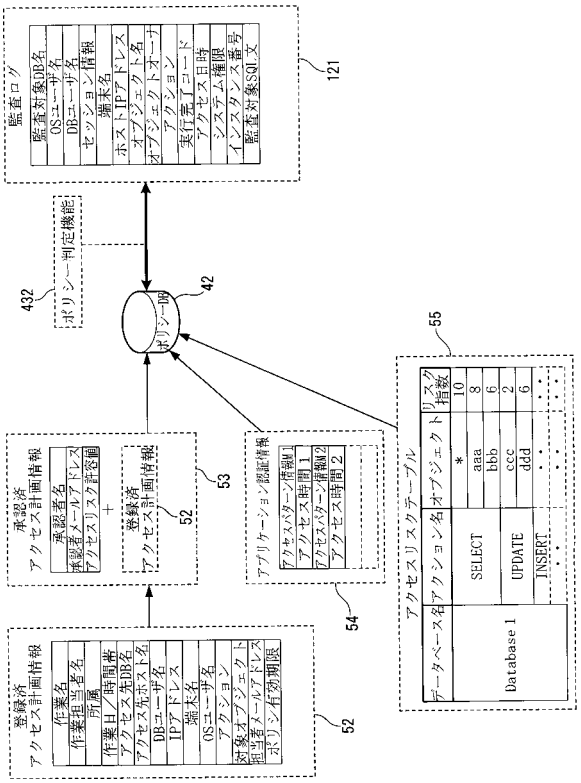
【図３】


データベースシステム
2
20
10
21
アプリケーション
ソフトウェア
34
アプリケーション保守担当者
アプリケーション開発者
33
アプリケーション運用担当者
データ保守担当者
32
システム保守担当者
システム開発者

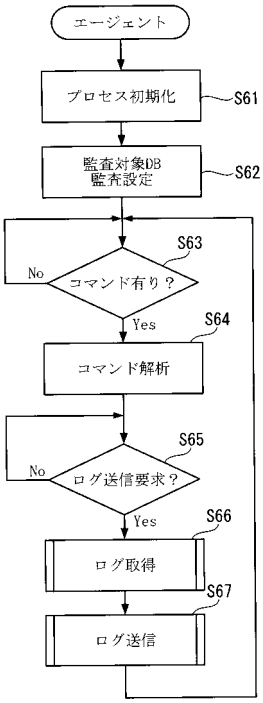
【図４】


ログ監視サーバ
43
監査ログコレクタ
431
監査ログ
121
監査ログ要求
122
12
439
監査ログDB
42
ポリシーDB
59
セキュリティポリシー情報
異常アクセス情報
58
ポリシー判定機能
（異常アクセス検出手段）
432
アラート機能
（異常アクセス通知手段）
433
ワークフローサーバ
41
アクセス計画登録機能
411
アクセス計画承認機能
412
セキュリティポリシー生成機能
413
アプリケーション認証情報登録機能
415
Webサーバシステム管理機能
417
Webサーバ監視機能
418
対策実施確認機能
419
アプリケーションソフトウェア
21
メールサーバ
44
エージェント
11
監査ログ設定
111
監査ログ収集
112
監査ログ送信
113
コマンド処理
114
10
アラート情報
・アラートレベル：高
・違反ポリシー名：ACLポリシー
・実行時間：2006/12/31 00:00:00
・データベース名：データベース1
・DBユーザ名：BIUSER
・OSユーザ名：OSUSER1
・ホスト名：HOST1
・IPアドレス：000.000.000.000
・ターミナル：TERM1
・アクション：ACTION1
・オブジェクト：OBJECT1
57
38
監視者

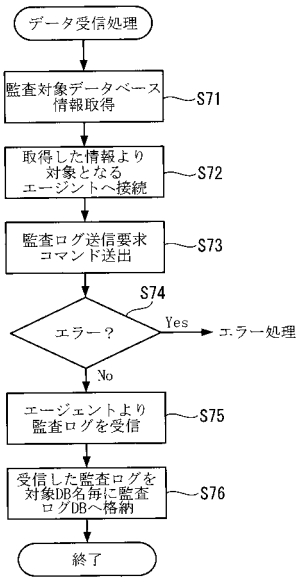
【図５】


監査ログ
監査対象DB名
OSユーザ名
DBユーザ名
セッション情報
端末名
ホストIPアドレス
オブジェクト名
オブジェクトオーナ
アクション
実行完了コード
アクセス日時
システム権限
インスタンス番号
監査対象SQL文
121
ポリシー判定機能
432
ポリシーDB
42
55
データベース名
アクション名
オブジェクト
リスク指数
Database 1
SELECT
UPDATE
INSERT
*
aaa
bbb
ccc
ddd
10
8
6
2
6
54
アプリケーション認証情報
アクセスパターン情報1
アクセス時間1
アクセスパターン情報2
アクセス時間2
53
承認済
アクセス計画情報
承認者名
承認者メールアドレス
アクセスリスク許容値
＋
登録済
アクセス計画情報
52
52
登録済
アクセス計画情報
作業名
作業指示書名
所属
作業日／時間帯
アクセス先DB名
アクセス先ホスト名
DBユーザ名
IPアドレス
端末名
OSユーザ名
アクション
対象オブジェクト
申請者メールアドレス
ポリシー有効期限

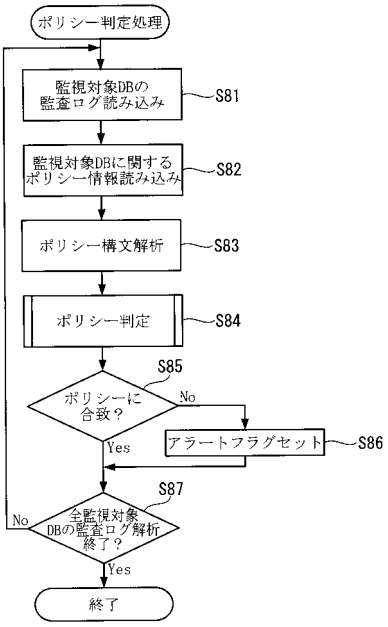
【図６】


エージェント
プロセス初期化
S61
監査対象DB
監査設定
S62
S63
No
コマンド有り？
Yes
S64
コマンド解析
S65
No
ログ送信要求？
Yes
S66
ログ取得
S67
ログ送信

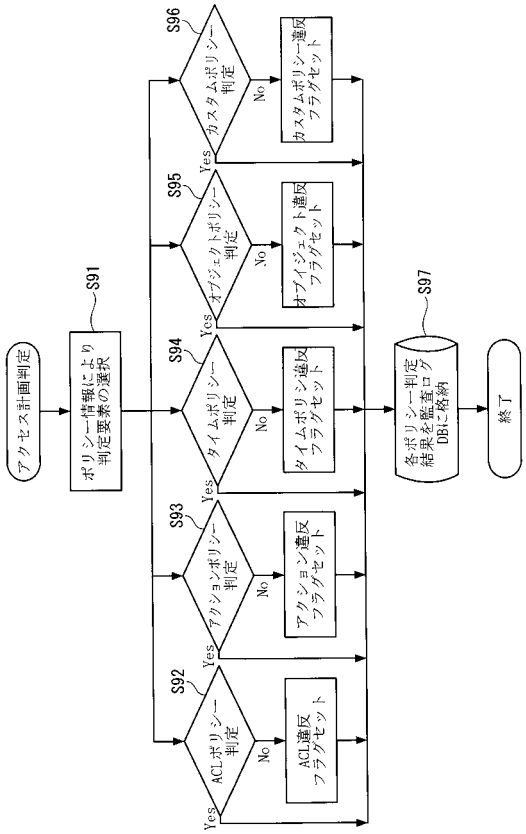
【図７】


データ受信処理
監査対象データベース
情報取得
S71
取得した情報より
対象となる
エージェントへ接続
S72
監査ログ送信要求
コマンド送出
S73
S74
エラー？
Yes
エラー処理
No
エージェントより
監査ログを受信
S75
受信した監査ログを
対象DB名毎に監査
ログDBへ格納
S76
終了

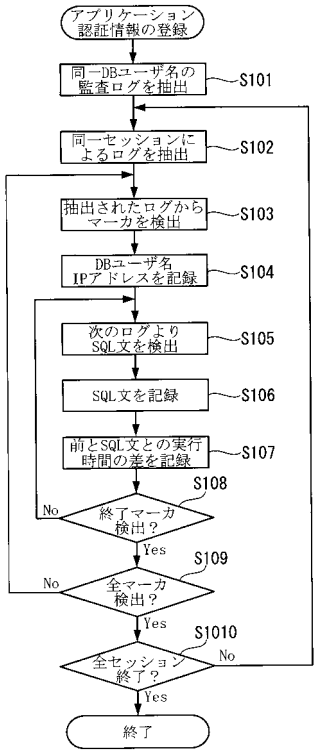
【図８】


ポリシー判定処理
監視対象DBの
監査ログ読み込み
S81
監視対象DBに関する
ポリシー情報読み込み
S82
ポリシー構文解析
S83
ポリシー判定
S84
S85
ポリシーに
合致？
No
Yes
アラートフラグセット
S86
S87
No
全監視対象
DBの監査ログ解析
終了？
Yes
終了

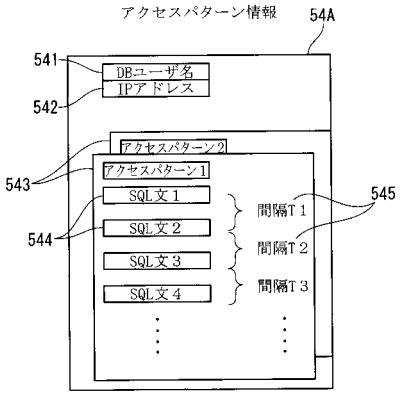
【図９】



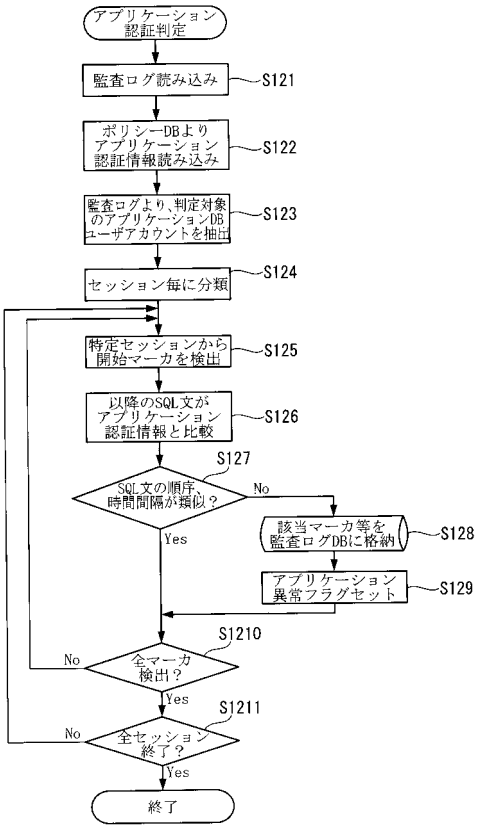
【図１０】



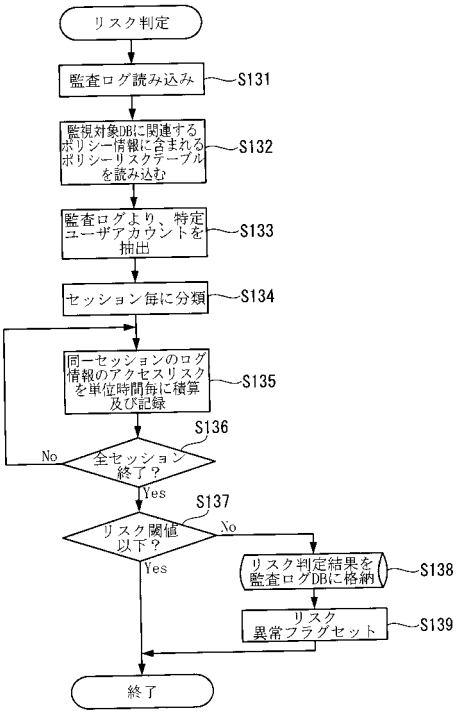
【図１１】



【図１２】



【図１３】


リスク判定
監査ログ読み込み
S131
監視対象DBに関連するポリシー情報に含まれるポリシーリスクテーブルを読み込む
S132
監査ログより、特定ユーザアカウントを抽出
S133
セッション毎に分類
S134
同一セッションのログ情報のアクセスリスクを単位時間毎に積算及び記録
S135
S136
全セッション終了？
No
Yes
S137
リスク閾値以下？
No
Yes
リスク判定結果を監査ログDBに格納
S138
リスク異常フラグセット
S139
終了

フロントページの続き

審査官　後藤　彰

(56)参考文献　特開２００５－２３４７２９（ＪＰ，Ａ）
特開２００６－１５５１２４（ＪＰ，Ａ）
特開２００４－０４６３０７（ＪＰ，Ａ）
特開２００３－２３３５２１（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／２４