明　細　書

発明の名称 ：

ログ分析装置、不正アクセス監査システム、ログ分析プログラム及びログ分析方法

技術分野

[0001] 本発明は情報システムにおいて、業務サーバへのアクセスログを分析し、監査する技術に関する。

背景技術

[0002] ログを用いた監査方式では、アクセスログと本人の権限を対比し、本人の権限を越えたリソースへのアクセスや操作がないかを点検する方式が主流であった。しかし、本人の権限内の操作であっても、不適切なタイミングでの操作（例．修正モジュール等の更新がないのに、モジュールを変更する）が可能であった。このため悪意を持った犯行や、誤操作などを点検時に検出することが困難であるという課題があった。

[0003] この課題に対して、以下の特許文献１では、利用申請ワークフローとアクセスログを用いて、ログの分析および監査を実施する仕組みが開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特開２００９－７５９４０号公報

発明の概要

発明が解決しようとする課題

[0005] 従来の監査方式では、利用申請ログとアクセスログにより監査を行うため、利用申請ログに情報の残らない業務サーバ間のアクセスや、申請された利用時間内の外部犯行者によるアクセスを検出できない。このため、不適切なアクセスを正しく点検できないという課題があった。

[0006] この発明は、業務サーバに対する不正アクセスを適切に検出する装置の提供を目的とする。

課題を解決するための手段

[0007] この発明のログ分析装置は、

アクセス先サーバ装置へのアクセスを申請する複数の申請レコードが記録された申請ログを保有する申請ログ保有装置から前記申請ログを収集し、

前記申請ログ保有装置から通知された前記複数の申請レコードを保有し、前記アクセス先サーバ装置へアクセスするログインをアクセス装置から受け付け、前記ログインに対応する前記申請レコードが存在するか判定し、前記申請レコードが存在する場合には前記アクセス装置から前記アクセス先サーバ装置へアクセスを中継すると共に前記アクセス装置による前記アクセス先サーバ装置へのアクセス状態を操作レコードとして操作ログに記録するアクセス中継装置から前記操作ログを収集し、

アクセスされたアクセス状態をアクセスレコードとしてアクセスログに記録する前記アクセス先サーバ装置から前記アクセスログを収集するログ収集部と、

前記ログ収集部が収集した前記申請ログと、前記操作ログと、前記アクセスログとに基づいて、前記アクセスレコードとして記録されたアクセス状態が正規のアクセスかどうかを判定する判定部と

を備えたことを特徴とする。

発明の効果

[0008] この発明により、業務サーバに対する不正アクセスを適切に検出する装置を提供できる。

図面の簡単な説明

[0009] [図1]実施の形態１の図で、不正アクセス監査システム１００１の構成図。

[図2]実施の形態１の図で、ＷＦサーバ２００等の構成図。

[図3]実施の形態１の図で、運用者Ｙの業務サーバ６００に対する変更操作の流れを示すフローチャート。

[図4]図３をシーケンスとして表した図。

[図5]実施の形態１の図で、申請情報４０１の内容を示す図。

[図6]実施の形態１の図で、申請情報４０１の具体例を示す図。

[図7]実施の形態１の図で、申請ログ２１１の内容を示す図。

[図8]実施の形態１の図で、申請ログ２１１の具体例を示す図。

[図9]実施の形態１の図で、操作ログ５１１の内容を示す図。

[図10]実施の形態１の図で、操作ログ５１１の具体例を示す図。

[図11]実施の形態１の図で、アクセスログ６１１の内容を示す図。

[図12]実施の形態１の図で、アクセスログ６１１の具体例を示す図。

[図13]実施の形態１の図で、点検作業のフローを示す図。

[図14]図１３をシーケンス化した前半の図。

[図15]図１３をシーケンス化した後半の図。

[図16]実施の形態１の図で、アクセスの種類とログとの対応を示す図。

[図17]実施の形態２の図で、不正アクセス監査システム１００２の構成図。

[図18]実施の形態２の図で、図４に対応するシーケンス図。

[図19]実施の形態２の図で、アクセスの種類とログとの対応を示す図。

[図20]実施の形態３の図で、自動延長時の判定方法を示す図。

[図21]実施の形態４の図で、ログ分析サーバ１００の外観の一例を示す図。

[図22]実施の形態４の図で、ログ分析サーバ１００のハードウェア構成の一例を示す図。

発明を実施するための形態

[0010] 実施の形態１.

図１～図１６を参照して、実施の形態１の不正アクセス監査システム１００１を説明する。

図１は、特権ＩＤを用いた不適切なアクセスを監査する、不正アクセス監査システム１００１の構成を示す。

[0011] 不正アクセス監査システム１００１は、ログ分析サーバ１００（ログ分析装置）、作業申請ワークフローサーバ２００（申請ログ保有装置）、管理者

端末装置３００、運用者端末装置４００（アクセス装置）、ＩＤ利用制御部５００（アクセス中継装置）、業務サーバ装置６００（アクセス先サーバ装置）、利用者端末装置７００を備える。なお、ＩＤ利用制御部５００は作業申請ワークフローサーバ２００に組み込まれても構わない。

[0012] 以下では、作業申請ワークフローサーバ２００はＷＦサーバ２００と記し、管理者端末装置３００は管理者端末３００と記し、運用者端末装置４００は運用者端末４００と記し、ＩＤ利用制御部５００はＩＤ制御部５００と記し、業務サーバ装置６００は業務サーバ６００と記し、利用者端末装置７００は利用者端末７００と記す。

[0013] 不正アクセス監査システム１００１では、ログ分析サーバ１００、ＷＦサーバ２００、管理者端末３００、運用者端末４００及びＩＤ制御部５００は業務ネットワーク８００に接続している。業務サーバ６００は管理ネットワーク８１０を介してＩＤ制御部５００に接続している。利用者端末７００はサービスネットワーク８２０を介して業務サーバ６００に接続している。利用者は利用者端末７００からサービスネットワーク８２０を経由して、業務サーバ６００の業務アプリケーションに対してリクエストを送信する。

[0014]（ログ分析サーバ１００）

ログ分析サーバ１００は、ログ収集部１１０、ログ情報管理部１２０、ログ解析部１３０（判定部）を備える。

（１）ログ収集部１１０は、ＷＦサーバ２００、ＩＤ制御部５００、業務サーバ６００のそれぞれから、利用申請ログ２１１（以下、申請ログ２１１と記す）、操作ログ５１１、アクセスログ６１１を収集する。

（２）ログ情報管理部１２０は、ログ収集部１１０によって収集された申請ログ２１１等のログ情報を保管する。

（３）ログ解析部１３０は、ログ情報管理部１２０によって保管されているログ情報を入力とし、各ログに記録されているレコード（後述する）の対応関係を解析する。ログ解析部１３０はこの解析によって、業務サーバ６００へのアクセスが、不適切なアクセスかどうかを判定し、判定結果を出力する

。

[0015] 図２の（ａ）～（ｆ）は、ＷＦサーバ２００、管理者端末３００、運用者端末４００，ＩＤ制御部５００、業務サーバ６００、利用者端末７００の構成を示す。ＷＦサーバ２００等は、記憶部、通信を行う通信部、情報処理を行う処理部を備える。

[0016] 以下に、不正アクセス監査システム１００１において、運用者Ｙに関連する作業の流れを説明する。

図３は、運用者Ｙの業務サーバ６００に対する変更操作の流れを示すフローチャートである。

図４は、図３をシーケンス化した図である。

[0017] 運用者Ｙは、ベンダから業務サーバ６００の修正モジュールが公開された場合や、業務サーバ６００を利用する顧客の要望がある場合に、特権ＩＤ（Ａｄｍｉｎｉｓｔｒａｔｏｒ権限を持つＩＤ）にて業務サーバ６００にログインし、モジュール更新や設定変更などの変更操作を行う。このような場合、不適切なタイミングのアクセス（業務サーバ６００における不要な変更操作などの誤操作）を防ぐために、運用者Ｙは、ＷＦサーバ２００に対して利用申請を行うものとする。

[0018]（Ｓ１０１）

運用者Ｙは、業務サーバ６００を利用するための利用申請である申請情報４０１を、運用者端末４００（通信部４２０）からＷＦサーバ２００に送信する（Ｓ１０１）。申請情報４０１の送信は、以下の様である。運用者端末４００（通信部４２０）はＷＦサーバ２００（通信部２２０）との通信により、ＷＦサーバ２００から作業申請ワークフロー２０１（以下、申請ＷＦ２０１と記す）を呼び出す。運用者端末４００の処理部４３０は、運用者端末４００の画面に申請ＷＦ２０１を表示する。運用者Ｙは画面に表示された申請ＷＦ２０１に申請情報４０１を記入（処理部４３０が記入処理を実施）する。

通信部４２０は申請情報４０１が記入された申請ＷＦ２０１をＷＦサーバ

２００に送信する。

[0019] 図５は申請情報４０１の内容を示す図である。

図６は、申請情報４０１の具体例を示す。図５のように、申請情報４０１は、以下の（１）～（５）の情報を含む。

（１）特権ＩＤ１１

特権ＩＤ１１は、業務サーバ６００に対してログインするアカウントである。パスワード情報は、ＩＤ制御部５００にて管理しておき、中継する際にパスワード情報を付与する形態が望ましいが（後述のＳ１０５で説明する、ＩＤ制御部５００によるログインのＩＤ、パスワード及び特権ＩＤの保有）、特権ＩＤ１１は申請情報４０１の中に含めても良い。

（２）利用者情報１２

利用者情報１２は、運用者Ｙを識別するための情報であり、例えば運用者Ｙの識別子（ＩＤ）である。

（３）業務サーバ識別子１３

業務サーバ識別子１３は、ログインする業務サーバ６００のホスト名などの識別子である。

（４）利用期間１４

利用期間１４（アクセス予定期間情報）は、申請情報４０１の申請内容に従った操作を、いつからいつまでの予定で実施するかを示す期間である。

（５）利用予定のコマンド／プロトコル１５

利用予定のコマンド／プロトコル１５は、業務サーバ６００に対して、どのようなプロトコルでアクセスするか、また、どのような作業（コマンド）を実行するかを示すコマンドあるいはプロトコルである。

[0020]（Ｓ１０２）

ＷＦサーバ２００（通信部２２０）は申請情報４０１を受信する。処理部２３０が申請情報４０１の起票を行うとともに、通信部２２０が管理者Ｘの管理者端末３００に電子メール等で、申請情報４０１に対する承認依頼の通知を行う（Ｓ１０２）。

[0021]（Ｓ１０３）

管理者Ｘは管理者端末３００（通信部３２０）によるＷＦサーバ２００との通信により申請ＷＦ２０１を管理者端末３００の画面に表示する。申請ＷＦ２０１の表示は処理部３３０が行う。管理者Ｘは、申請ＷＦ２０１で申請情報４０１の内容を確認し、問題がなければ承認する（Ｓ１０３）。承認状況は処理部３３０によって申請ＷＦ２０１に記載され、管理者端末３００（通信部３２０）からＷＦサーバ２００に送信される。

[0022]（Ｓ１０４）

ＷＦサーバ２００の処理部２３０は、申請情報４０１が承認済みであることを申請ログ２１１に記録する。また、通信部２２０は申請情報４０１をＩＤ制御部５００に通知する（Ｓ１０４）。

[0023] 図７は申請ログ２１１に含まれる情報の内容を示す図である。申請ログ２１１は、業務サーバ６００へのアクセスを申請する複数の申請レコードが記録されている。一つの申請が、一つの申請レコード（１レコード）である。図４の申請情報４０１（Ｓ１０１）は申請ログ２１１に記録される一つの申請レコードである。また、図７の申請ログ２１１は、一つの申請レコードを示している。

一つの申請レコードは、特権ＩＤ１１が対応付けられており、また利用期間１４（アクセス期間予定情報）を含む。また一つの申請レコードは、利用予定のコマンド／プロトコル１５（予定コマンド情報）を持つ。図７の特権ＩＤ１１～利用予定コマンド／プロトコル１５は、図５の特権ＩＤ１１～利用予定コマンド／プロトコル１５である。承認状況１６は管理者端末３００による承認結果である。

図８は申請ログ２１１の具体例である。図８における利用予定コマンド／プロトコル１５の項目の内容に関しては、例えばＴｅｌｎｅｔのコマンドについては、ホワイトリスト、ブラックリストなどグループ化して、どのホワイトリスト（またはブラックリスト以外）を指定するかといった情報を記録しても良い。

[0024]（Ｓ１０５）

運用者Ｙは、運用者端末４００により、（申請ＷＦ２０１に登録された）予定の日時になった場合、Ｔｅｌｎｅｔやリモートデスクトッププロトコル（ＲＤＰ）を用いて、ＩＤ制御部５００に対して変更操作のためのログイン操作を行う（Ｓ１０５）。運用者端末４００におけるログイン処理は、処理部４３０が行う。このログインにはＩＤとパスワードとを用いるが、ＩＤおよびパスワードの組は、運用者Ｙを識別するために予めＩＤ制御部５００に登録されているものを用いる。例えば、ＩＤは図５の利用者情報１２の運用者ＹのＩＤ、パスワードは社内システムの利用のために運用者Ｙに与えられているパスワードである。ＩＤ制御部５００には、これらのＩＤとパスワードの組が登録されている。

[0025]（Ｓ１０６）

ＩＤ制御部５００は、運用者Ｙの利用しているＩＤおよびプロトコルから、対応する申請情報４０１が存在すること、また、申請された利用期間内のアクセスであることを確認して、利用の可否を判断する（Ｓ１０６）。ＩＤ制御部５００は、Ｓ１０４で申請情報４０１を受信済みである。よって、ＩＤ制御部５００は、Ｓ１０５のログインにおけるＩＤ及び使用するプロトコルと、申請情報４０１（図５）における利用者情報１２及び利用予定コマンド／プロトコル１５との比較により、Ｓ１０５のログインに対応する申請情報４０１が存在するか確認できる。申請情報４０１が存在する場合、ＩＤ制御部５００は、Ｓ１０５のログインが申請情報４０１の利用期間１４内であるか判断する。

[0026]（Ｓ１０７、Ｓ１０８）

申請情報４０１が存在しないまたは利用期間内ではない場合は利用不可である。この場合は、ＩＤ制御部５００が運用者Ｙ（運用者端末４００）からのリクエストを破棄する。利用可（申請情報４０１が存在し、かつ、利用期間内）である場合は、ＩＤ制御部５００は、運用者端末４００（処理部４３０）による変更操作の内容を、業務サーバ６００に対して中継する（Ｓ１０

７）。この中継に際しては、ＩＤ制御部５００は、通知された申請情報４０１に記載された特権ＩＤで業務サーバ６００にログインし、変更操作の内容を中継する。また、中継する変更操作の内容を、ＩＤ制御部５００は操作ログ５１１に記録する（Ｓ１０８）。なお、図５の特権ＩＤ１１の項目の説明で述べたように、申請情報４０１に特権ＩＤ１１が記載されていない場合は、Ｓ１０５のログインで使用されるＩＤ及びパスワードの組と対応付けられた特権ＩＤを、ＩＤ制御部５００が予め保有する構成でも構わない。

[0027] 図９は、ＩＤ制御部５００によって記録される操作ログ５１１の内容（アクセス状態）を示す。

図１０は、操作ログ５１１の具体例を示す。図９における特権ＩＤ１１－５、利用者情報１２－５、利用期間１４－５（アクセス期間情報）は、図５の特権ＩＤ１１、利用者情報１２、利用期間１４に対応する。また、操作内容１７－５は、図５の申請情報４０１における利用予定コマンド／プロトコル１５に対応する。操作ログ５１１は、複数の操作レコードが記録されている。中継する一つの操作が、一つの操作レコードとなる。図９、図１０は一つの操作レコードを示している。特権ＩＤ１１－５は、Ｓ１０７のログインに使用したＩＤである。一つの操作レコードは特権ＩＤ１１－５が対応付けられている。利用者情報１２－５は、存在が確認された申請情報４０１に記載の利用者情報１２である。利用期間１４－５（アクセス期間情報）は、中継期間である。操作内容１７－５（中継コマンド情報）は、中継した変更操作における利用予定コマンドやプロトコルである。

[0028] （Ｓ１０９）

業務サーバ６００（処理部６３０）は、ＯＳのセキュリティログなどの機能によって、ＩＤ制御部５００によって中継された変更操作の内容をアクセスログ６１１に記録する。

[0029] 図１１は、業務サーバ６００によって記録されるアクセスログ６１１の内容（アクセス状態）を示す。

図１２は、アクセスログ６１１の具体例を示す。アクセスログ６１１は、

複数のアクセスレコードが記録されている。業務サーバ６００への一つの操作（１アクセス）が、一のアクセスレコードとなる。図１１、図１２は一つのアクセスレコードを示している。図１１において、利用者ＩＤ１１－６は特権ＩＤであり、図９の特権ＩＤ１１－５に対応し、Ｓ１０７のログイン（図４）で使用されたＩＤである。一つのアクセスレコードには特権ＩＤが対応付けられている。操作内容１７－６は、図９の操作内容１７－５に対応し、業務サーバ６００に対する操作やコマンドの情報である。利用期間１４－６（アクセス期間情報）は、利用期間１４－５に対応し、他の装置から業務サーバ６００に対して変更操作が実行された期間である。

[0030] 図１３～図１５を参照して、不正アクセス監査時における点検作業の流れを説明する。

図１３は、点検作業のフローを示す。

図１４、図１５は図１３をシーケンス化した図であり、図１４の「Ａ」は図１５の「Ａ」と同一である。図１４はログ収集のシーケンスであり、図１５はログ収集後の、不正アクセスの監査のシーケンスである。

[0031] （Ｓ２０１）

監査者（例えば管理者Ｘ）は管理者端末３００（監査者が管理者の場合）を用いることにより、ＷＦサーバ２００、ＩＤ制御部５００及び業務サーバ６００のそれぞれから、申請ログ２１１、操作ログ５１１、アクセスログ６１１を収集するスケジュール（例えば、毎日夜間に実施）を、予め申請ＷＦ２０１に登録することで利用申請する（Ｓ２０１）。スケジュールの登録作業は、ログ分析サーバ１００が、ＩＤ制御部５００の中継を介して（後述のＳ２０３）業務サーバ６００のアクセスログ６１１を収集するために実施する。また、管理者端末３００の処理部３３０によって、申請ＷＦ２０１には、ログ収集のスケジュールと共に、後述のＳ２０３－１（図１４）のログインで用いる「ＩＤ、パスワード」、及びＳ２０３－２（図１４）のログインで用いる特権ＩＤが登録される。これらが記載された申請ＷＦ２０１の情報は、管理者端末３００（監査者の端末）の通信部３２０によって、ログ分析

サーバ１００に送信される。なお、Ｓ２０１では申請ＷＦ２０１にスケジュール等を登録したが、スケジュールやＩＤ等は、ログ分析サーバ１００に、端末から直接設定しても構わない。

[0032]（Ｓ２０２）

予定時刻になった場合、ログ収集部１１０は、ＯＳのスケジュール機能などを利用して起動される。起動された後、ログ収集部１１０は、ＦＴＰなどのプロトコルで、申請ログ２１１、操作ログ５１１を収集し、ログ情報管理部１２０に格納する（Ｓ２０２）。

[0033]（Ｓ２０３）

また、ログ収集部１１０は、ＩＤ制御部５００を経由し、リモートデスクトップ等の機能を用いて業務サーバ６００に接続し、ログイン操作を実施する（Ｓ２０３）。ログイン操作の自動化は、リモートデスクトッププロトコル（ＲＤＰ）の制御によって実施するか、リモートデスクトップ機能に対するキー操作の再生機能などを用いて実現する。ログ分析サーバ１００によるＩＤ制御部５００へのログイン（図１４のＳ２０３－１）には、Ｓ２０１で登録された「ＩＤ、パスワード」の組が使用される。ＩＤ制御部５００による業務サーバ６００へのログイン（図１４のＳ２０３－２）には、Ｓ２０１で登録された特権ＩＤが使用される。

[0034]（Ｓ２０４、Ｓ２０５）

業務サーバ６００の処理部６３０は、監査対象期間のアクセスログ６１１を出力する（Ｓ２０４）。ログ収集部１１０は、処理部６３０が出力したファイル（アクセスログ６１１）を、ファイルコピーや、その他のプロトコルを用いることにより、ＩＤ制御部５００を介して収集し、ログ情報管理部１２０に格納する（Ｓ２０５）。

[0035]（Ｓ２０６、Ｓ２０７）

次に、図１５を参照して説明する。ログ収集後の監査時には、ログ解析部１３０が、ログ情報管理部１２０から、監査期間に該当するアクセスログ６１１から、期間の最も早い（古い）一つのアクセスレコードを抽出する（Ｓ

２０６）。アクセスログ６１１は図１１の内容を有するが、アクセスログ６１１の一つのアクセスレコードは、上記のように、業務サーバ６００への１操作を単位とする。つまり一つのアクセスレコードは１操作である。ログ解析部１３０は、抽出したアクセスレコードから、操作日時（操作日時１４－６）、操作の実施者（利用者ＩＤ（特権ＩＤ）１１－６））、操作内容（操作内容１７－６）を抽出する（Ｓ２０７）。なお、アクセスレコードの内容によっては、特権ＩＤとの対応が一つのアクセスレコードに記録されていない場合がある。つまり、一つの特権ＩＤに複数の操作が対応して記録される場合がある。このような場合、ログ解析部１３０は、ログイン操作のレコードまで遡って検索し、利用した特権ＩＤを判別する。

[0036]（Ｓ２０８）

Ｓ２０８はアクセスレコードと申請ログ２１１との比較である。ログ解析部１３０は、申請ログ２１１の中に、アクセスレコードの特権ＩＤ１１－６と特権ＩＤ１１が一致し、かつ、アクセスレコードの操作日時１４－６（アクセス期間情報）が利用期間１４（アクセス予定期間情報）に含まれる申請レコードがないか検索する（Ｓ２０８）。対応する申請レコードがない場合には、ログ解析部１３０は不適切なアクセス（未申請での操作）があったと判定し、アクセスレコードの属性として記録する（Ｓ２１３）。

[0037]（Ｓ２０９）

Ｓ２０９は申請レコードと操作ログ５１１との比較である。対応する申請レコードがＳ２０８でヒットした場合、ログ解析部１３０は、この申請レコードに含まれる特権ＩＤ１１（または利用者ＩＤ）及び利用期間１４をキーとして、申請レコードに対応する操作ログ５１１の操作レコードが存在するか検索する（Ｓ２０９）。検索条件は以下である。上記したように、ヒットした申請レコードに対して、特権ＩＤ（または利用者ＩＤ）が一致し、かつ、操作ログ５１１に記載された情報の開始日時、終了日時が、申請レコードの利用期間１４に含まれることである。ヒットした申請レコードに対応する操作レコードがない場合には、ログ解析部１３０は不適切なアクセス（不適

切な経路によるアクセス）があったと判定し、ヒットした申請レコードに対応するアクセスレコードの属性として記録する（Ｓ２１３）。

[0038]（Ｓ２１０）

Ｓ２１０は、Ｓ２０８でヒットした申請レコードと、Ｓ２０９でヒットした操作レコードとの比較である。ログ解析部１３０は、操作レコードがＳ２０９でヒットした場合には、ヒットした操作レコードの操作内容１７－５（中継コマンド情報）に含まれる利用コマンドが、Ｓ２０８でヒットした申請レコードの利用予定コマンド／プロトコル１５と合致するかをチェックする（Ｓ２１０）。この場合、ログ解析部１３０は、ヒットした操作レコード操作内容１７－５の利用コマンドが、申請レコードに記載されたコマンドであること、またはホワイトリストの範囲内、ブラックリストの範囲外であることを確認する。コマンドのチェックは、許可するコマンド、禁止するコマンドを、正規表現の文字列で定義し、正規表現とのマッチングによる判定などによって実施する。

なお、利用するプロトコルによっては、コマンドレベルの情報をＩＤ制御部５００でログに出力することが困難な場合があるため、この場合は操作レコードの有無のみで判定してもよい。

[0039] ログ解析部１３０は、操作レコードの利用コマンドが申請レコードの範囲外のものであれば、不適切なアクセス（未許可のコマンド実行）があったと判定し、レコードの属性として記録する（Ｓ２１３）。

[0040]（Ｓ２１１）

ログ解析部１３０は、利用コマンドが申請レコードの範囲内（承認されたコマンド）であれば、アクセスレコードの属性として適切なアクセスであったこと（不適切なアクセスがなかったこと）を記録する（Ｓ２１１）。

[0041]（Ｓ２１２）

ログ解析部１３０は、Ｓ２０６からＳ２１２までの処理を、監査対象期間のアクセスログ６１１の最後のアクセスレコード（もっとも新しいアクセスレコード）まで繰り返し実行する（Ｓ２１２）。

[0042] 以上から、ログ解析部１３０は、以下の（１）～（３）の条件を満たしているアクセスレコードを適切なアクセス、満たしていないアクセスレコードを、不適切なアクセスと判断することができる。

（１）関連する申請ログ２１１、操作ログ５１１、アクセスログ６１１が揃っている。

つまり関連する申請レコード、操作レコード及びアクセスレコードがそろっていることである。これは、Ｓ２０８でＹＥＳ、Ｓ２０９でＹＥＳの場合である。

（２）操作ログ５１１に記録された操作レコードが、申請ログ２１１に記録された申請レコードの利用期間内にある。これは、Ｓ２０９でＹＥＳの場合である。

（３）アクセスログ６１１に記録されたアクセスレコードのコマンドが申請レコードの範囲内にある。

これは、Ｓ２１０でＹＥＳの場合である。

[0043] 図１６は、アクセスの種類とログとの対応を示す図である。「〇」はログに記載（レコード）がある事を示し、「×」はログに記載（レコード）がない事を示す。例えば、「適切」は申請ログ２１１、操作ログ５１１、アクセスログ６１１のすべてに対応する情報（レコード）が記載されている場合であり、「不適切（未申請）」は申請ログ２１１、操作ログ５１１、アクセスログ６１１のどれにも情報が記載されていない場合である。図１６の「△」の「※」は以下の意味である。外部犯行者の操作は偶然に利用申請期間内に入ることがある（〇の場合がある）ので、申請ログ２１１と操作ログ５１１とを比較することで、正規なアクセスかが判別ができる。

[0044] 実施の形態２.

図１７～図１９を参照して、実施の形態２の不正アクセス監査システム１００２を説明する。実施の形態２は、業務サーバ間で特権ＩＤを用いた呼び出し関係がある場合に、以下のように、不正アクセスの有無を点検するシステムである。

[0045] 図１７は、業務サーバ間で呼び出しがある場合の不正アクセス監査システム１００２の構成図である。不正アクセス監査システム１００２は不正アクセス監査システム１００１に対して、管理ネットワーク８１０に、プロバイダである業務サーバ６００と、リクエスタである業務サーバ９００（アクセス装置）とが接続している点が異なる。このように業務サーバには、呼び出される側の業務サーバ６００（プロバイダ）と、呼び出す側の業務サーバ９００（リクエスタ）が存在する。業務サーバ上のアプリケーションの構成によっては、プロバイダ、リクエスタを兼ねる場合もある。

[0046] ネットワーク設定（および業務アプリケーション設定）は、業務サーバ９００（リクエスタ）からの呼び出しが、管理ネットワーク８１０に接続されたＩＤ制御部５００を介して、業務サーバ６００（プロバイダ）に接続するように行う。

[0047] 図１８は、図４に対応する図である。図１８は図運用者端末４００が業務サーバ担当者であり、また図４では運用者端末４００がＩＤ制御部５００にログイン（Ｓ１０５）するのに対して、図１８では業務サーバ９００がログインし、業務サーバ６００にアクセスする。申請ログ２１１、操作ログ５１１、アクセスログ６１１に記録される情報は図４の場合と同様である。なお操作ログ５１１、アクセスログ６１１に記録される情報は、業務サーバ９００によるアクセス内容である。

[0048] 業務サーバ９００の不正アクセスの監査では、図１３（図１４）の「点検作業の流れ」における利用申請（Ｓ２０１）において、利用期間、利用する特権ＩＤ等の情報を入力する。以降の処理は、実施の形態１の図１３（図１４及び図１５）と同様になる。

[0049] 図１９はアクセスの種類とログとの対応を示す図であり、実施の形態１の図１６と同様の図である。図１９の内容は図１６と同一である。

[0050] 実施の形態２により、業務サーバ間のアクセスや、申請された利用時間内に外部の犯行者からのアクセスなどを検出することができるので、不適切なアクセスを正しく点検することができる。

[0051] 実施の形態２により、業務サーバ間のアクセスも正しく点検できるので、監査時の例外処置が不要になり、監査作業の効率化、自動化が可能となる。また、判定しきれていなかった外部犯行者のアクセスに対して不適切であると判定することが可能になる。

[0052] 実施の形態３.

図２０を参照して実施の形態３の不正アクセス監査システム１００３（図示せず）を説明する。不正アクセス監査システム１００３の構成は、不正アクセス監査システム１００１（図１）あるいは不正アクセス監査システム１００２（図１７）の構成と同じである。実施の形態３は、ＩＤ制御部５００での作業が遅延した場合を考慮して、利用期間に関する許可を自動延長する（または設定により許可する）構成である。該当するセッションが、申請された利用期間を超えても継続している場合などに、延長処理を行う。

[0053] 延長処理を認める設定がある場合には、申請情報４０１に自動延長の許可／不許可の情報が含まれる。このため、ログ収集部１１０によるログ収集時には、自動延長の情報も含めて申請ログ２１１の収集を行う。

図２０は、ログ解析部１３０による自動延長時の判定方法を示す図である。

図２０に示すように、ログ解析部１３０は、

（１）作業時刻が利用期間を過ぎたレコード（アクセスログのレコード）がある。

（２）自動延長が許可となっている。

の両方の条件を満たす場合には、開始時刻のみのチェックで判定を行う。

その他の処理については実施の形態１と同様である。

[0054] 具体的には、申請レコードは、業務サーバ６００へのアクセス予定期間の延長の可否を示す延長情報を含む。ログ解析部１３０は、延長情報の示す可否を参照して、アクセスレコードに対応する申請レコードが申請ログ２１１に記録されているかどうかの判定（Ｓ２０８）と、申請レコードに対応する操作レコードが操作ログ５１１に記録されているかの判定（Ｓ２０９）とを

実行する。これによって、正規のセッションが、ＩＤ制御部５００での作業遅延により、申請された利用期間を超えても継続している場合も、正規なアクセスとして扱うことができる。

[0055] 以上、実施の形態１～３を説明したが、これらの実施の形態のうち、２つ以上を組み合わせて実施しても構わない。あるいは、これらの実施の形態のうち、１つを部分的に実施しても構わない。あるいは、これらの実施の形態のうち、２つ以上を部分的に組み合わせて実施しても構わない。なお、本発明はこれらの実施の形態に限定されるものではなく、必要に応じて種々の変形が可能である。

[0056] 実施の形態４．

図２１、図２２を参照して実施の形態４を説明する。実施の形態４は、コンピュータであるログ分析サーバ１００のハードウェア構成を説明する。なお、ＷＦサーバ２００、管理者端末３００、運用者端末４００、ＩＤ制御部５００、業務サーバ６００、利用者端末７００及び業務サーバ９００もログ分析サーバ１００と同様のコンピュータである。よって以下のログ分析サーバ１００の説明は、ＷＦサーバ２００等にも当てはまる。

[0057] 図２１は、コンピュータであるログ分析サーバ１００の外観の一例を示す図である。

図２２は、ログ分析サーバ１００のハードウェア資源の一例を示す図である。

[0058] 外観を示す図２１おいて、ログ分析サーバ１００は、システムユニット９７０、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）やＬＣＤ（液晶）の表示画面を有する表示装置９５３、キーボード９５４（Ｋｅｙ　Ｂｏａｒｄ：Ｋ／Ｂ）、マウス９５５、コンパクトディスク装置９５７（ＣＤＤ：Ｃｏｍｐａｃｔ　Ｄｉｓｋ　Ｄｒｉｖｅ）などのハードウェア資源を備え、これらはケーブルや信号線で接続されている。システムユニット９７０は業務ネットワーク８００，８１０，８２０に接続している。

[0059] またハードウェア資源を示す図２２において、ログ分析サーバ１００は、

プログラムを実行するＣＰＵ９５０（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）を備えている。ＣＰＵ９５０は、バス９５８を介してＲＯＭ（Ｒｅａｄ　Ｏｎｌｙ　Ｍｅｍｏｒｙ）９５１、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）９５２、表示装置９５３、キーボード９５４、マウス９５５、通信ボード９５６、ＣＤＤ９５７、磁気ディスク装置９６０と接続され、これらのハードウェアデバイスを制御する。磁気ディスク装置９６０の代わりに、光ディスク装置、フラッシュメモリなどの記憶装置でもよい。

[0060] ＲＡＭ９５２は、揮発性メモリの一例である。ＲＯＭ９５１、ＣＤＤ９５７、磁気ディスク装置９６０等の記録媒体は、不揮発性メモリの一例である。これらは、記憶装置あるいは記憶部、格納部、バッファの一例である。通信ボード９５６、キーボード９５４などは、入力部、入力装置の一例である。また、通信ボード９５６、表示装置９５３などは、出力部、出力装置の一例である。通信ボード９５６は、ネットワークに接続されている。

[0061] 磁気ディスク装置９６０には、オペレーティングシステム９６１（ＯＳ）、プログラム群９６２、ファイル群９６３が記憶されている。プログラム群９６２のプログラムは、ＣＰＵ９５０、オペレーティングシステム９６１により実行される。

[0062] 上記プログラム群９６２には、以上の実施の形態の説明において「～部」として説明した機能を実行するプログラムが記憶されている。プログラムは、ＣＰＵ９５０により読み出され実行される。

[0063] ファイル群９６３には、以上の実施の形態の説明において、「～の判定結果」、「～の算出結果」、「～の抽出結果」、「～の生成結果」、「～の処理結果」として説明した情報や、データや信号値や変数値やパラメータなどが、「～ファイル」や「～データベース」の各項目として記憶されている。「～ファイル」や「～データベース」は、ディスクやメモリなどの記録媒体に記憶される。また、ディスクやメモリなどの記録媒体に記憶された情報やデータや信号値や変数値やパラメータは、読み書き回路を介してＣＰＵ９５

０によりメインメモリやキャッシュメモリに読み出され、抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵの動作に用いられる。抽出・検索・参照・比較・演算・計算・処理・出力・印刷・表示などのＣＰＵの動作の間、情報やデータや信号値や変数値やパラメータは、メインメモリやキャッシュメモリやバッファメモリに一時的に記憶される。

[0064] また、以上に述べた実施の形態の説明において、データや信号値は、ＲＡＭ９５２のメモリ、ＣＤＤ９５７のコンパクトディスク、磁気ディスク装置９６０の磁気ディスク、その他光ディスク、ミニディスク、ＤＶＤ（Ｄｉｇｉｔａｌ　Ｖｅｒｓａｔｉｌｅ　Ｄｉｓｋ）等の記録媒体に記録される。また、データや信号は、バス９５８や信号線やケーブルその他の伝送媒体によりオンライン伝送される。

[0065] また、以上の実施の形態の説明において、「～部」として説明したものは、「～手段」、であってもよく、また、「～ステップ」、「～手順」、「～処理」であってもよい。すなわち、「～部」として説明したものは、ソフトウェアのみ、或いは、ソフトウェアとハードウェアとの組み合わせ、さらには、ファームウェアとの組み合わせで実施されても構わない。ファームウェアとソフトウェアは、プログラムとして、磁気ディスク、フレキシブルディスク、光ディスク、コンパクトディスク、ミニディスク、ＤＶＤ等の記録媒体に記憶される。プログラムはＣＰＵ９５０により読み出され、ＣＰＵ９５０により実行される。すなわち、プログラムは、以上に述べた「～部」としてコンピュータを機能させるものである。あるいは、以上に述べた「～部」の手順や方法をコンピュータに実行させるものである。

[0066] 以上の実施の形態では、ログ分析サーバ１００を説明したが、ログ分析サーバ１００の動作は、プログラムとしても把握できることは以上の説明から当然である。また、ログ分析サーバ１００の各「～部」の動作は、ログ分析方法としても把握できることは以上の説明により明らかである。

符号の説明

[0067] Ｘ　管理者、Ｙ　運用者、１００　ログ分析サーバ、１１０　ログ収集部

、１２０　ログ情報管理部、１３０　ログ解析部、２００　ＷＦサーバ、２０１　作業申請ＷＦ、２１０　記憶部、２１１　申請ログ、３００　管理者端末、４００　運用者端末、５００　ＩＤ制御部、５１０　記憶部、５１１　操作ログ、６００　業務サーバ、６１０　記憶部、６１１　アクセスログ、７００　利用者端末、８００　業務ネットワーク、８１０　管理ネットワーク、８２０　サービスネットワーク、９００　業務サーバ、１００１，１００２，１００３　不正アクセス監査システム。

請求の範囲

[請求項1] アクセス先サーバ装置へのアクセスを申請する複数の申請レコードが記録された申請ログを保有する申請ログ保有装置から前記申請ログを収集し、

前記申請ログ保有装置から通知された前記複数の申請レコードを保有し、前記アクセス先サーバ装置へアクセスするログインをアクセス装置から受け付け、前記ログインに対応する前記申請レコードが存在するか判定し、前記申請レコードが存在する場合には前記アクセス装置から前記アクセス先サーバ装置へアクセスを中継すると共に前記アクセス装置による前記アクセス先サーバ装置へのアクセス状態を操作レコードとして操作ログに記録するアクセス中継装置から前記操作ログを収集し、

アクセスされたアクセス状態をアクセスレコードとしてアクセスログに記録する前記アクセス先サーバ装置から前記アクセスログを収集するログ収集部と、

前記ログ収集部が収集した前記申請ログと、前記操作ログと、前記アクセスログとに基づいて、前記アクセスレコードとして記録されたアクセス状態が正規のアクセスかどうかを判定する判定部と

を備えたことを特徴とするログ分析装置。

[請求項2] 前記ログ収集部は、

前記アクセス中継装置にログインし、ログインした前記アクセス中継装置を介して、前記アクセス先サーバ装置から、前記アクセスログを収集することを特徴とする請求項１記載のログ分析装置。

[請求項3] 前記アクセス装置は、

前記ログ分析装置が使用される不正アクセス監査システムにおいて前記ログ分析装置と共に使用される、前記不正アクセス監査システムの運用者の端末装置と前記アクセス先サーバ装置をプロバイダとしてアクセスするリクエスタであるリクエスタサーバ装置との、いずれか

であることを特徴とする請求項１または２に記載のログ分析装置。

[請求項4] 前記判定部は、

前記アクセスログと前記申請ログとを比較することにより前記アクセスログに記録された前記アクセスレコードに対応する前記申請レコードが前記申請ログに記録されているかを判定し、前記申請レコードが前記申請ログに記録されている場合には前記申請レコードに対応する前記操作レコードが前記操作ログに記録されているかを判定することにより、前記アクセスレコードとして記録されたアクセス状態が正規のアクセスかどうかを判定することを特徴とする請求項１～３のいずれか１項に記載のログ分析装置。

[請求項5] 前記申請レコードと、前記操作レコードと、前記アクセスレコードとは、

前記アクセス先サーバ装置にログインする権限が認められた特権ＩＤが対応付けられており、

前記申請レコードは、

前記アクセス先サーバ装置へのアクセス予定期間情報を含み、

前記操作レコードは、

前記アクセス装置による前記アクセス先サーバ装置へのアクセス期間情報を含み、

前記アクセスレコードは、

アクセスされたアクセス期間情報を含み、

前記判定部は、

前記アクセスレコードに対応する前記特権ＩＤ及び前記アクセスレコードに含まれる前記アクセス期間情報と、前記申請レコードに対応する前記特権ＩＤ及び前記申請レコードに含まれる前記アクセス予定期間情報とに基づいて、前記アクセスレコードに対応する前記申請レコードが前記申請ログに記録されているかを判定し、

前記申請レコードに対応する前記特権ＩＤ及び前記申請レコードに

含まれる前記アクセス予定期間情報と、前記操作レコードに対応する前記特権ＩＤ及び前記操作レコードに含まれる前記アクセス期間情報とに基づいて、前記申請レコードに対応する前記操作レコードが前記操作ログに記録されているかを判定することを特徴とする請求項４記載のログ分析装置。

[請求項6] 前記申請レコードは、

前記アクセス先サーバ装置へのアクセスに用いる予定の予定コマンドを含み、

前記操作レコードは、

中継されたアクセスに用いられた中継コマンドを含み、

前記判定部は、

前記申請レコードに対応する前記操作レコードが前記操作ログに記録されていると判定した場合に、前記申請レコードに含まれる前記予定コマンドと、前記操作レコードに含まれる前記中継コマンドとに基づいて、前記アクセスレコードとして記録されたアクセス状態が正規のアクセスかどうかを判定することを特徴とする請求項５記載のログ分析装置。

[請求項7] 前記申請レコードは、

前記アクセス先サーバ装置へのアクセス予定期間の延長の可否を示す延長情報を含み、

前記判定部は、

前記延長情報の示す可否を参照して、前記アクセスレコードに対応する前記申請レコードが前記申請ログに記録されているかどうかの判定と、前記申請レコードに対応する前記操作レコードが前記操作ログに記録されているかの判定とを実行することを特徴とする請求項５または６のいずれかに記載のログ分析装置。

[請求項8] アクセスされたアクセス状態をアクセスレコードとしてアクセスログに記録するアクセス先サーバ装置と、

前記アクセス先サーバ装置へのアクセスを申請する複数の申請レコードが記録された申請ログを保有する申請ログ保有装置と、

前記申請ログ保有装置から通知された前記複数の申請レコードを保有し、前記アクセス先サーバ装置へアクセスするログインをアクセス装置から受け付け、前記ログインに対応する前記申請レコードが存在するか判定し、前記申請レコードが存在する場合には前記アクセス装置から前記アクセス先サーバ装置へアクセスを中継すると共に前記アクセス装置による前記アクセス先サーバ装置へのアクセス状態を操作レコードとして操作ログに記録するアクセス中継装置と、

前記アクセス先サーバ装置、前記申請ログ保有装置、前記アクセス中継装置から、それぞれ、前記アクセスログ、前記申請ログ、前記操作ログを収集するログ収集部と、前記ログ収集部が収集した前記申請ログと、前記操作ログと、前記アクセスログとに基づいて、前記アクセスレコードとして記録されたアクセス状態が正規のアクセスかどうかを判定する判定部とを有するログ分析装置と

を備えたことを特徴とする不正アクセス監査システム。

[請求項9] コンピュータに、

アクセス先サーバ装置へのアクセスを申請する複数の申請レコードが記録された申請ログを保有する申請ログ保有装置から前記申請ログを収集する処理、

前記申請ログ保有装置から通知された前記複数の申請レコードを保有し、前記アクセス先サーバ装置へアクセスするログインをアクセス装置から受け付け、前記ログインに対応する前記申請レコードが存在するか判定し、前記申請レコードが存在する場合には前記アクセス装置から前記アクセス先サーバ装置へアクセスを中継すると共に前記アクセス装置による前記アクセス先サーバ装置へのアクセス状態を操作レコードとして操作ログに記録するアクセス中継装置から前記操作ログを収集する処理、

アクセスされたアクセス状態をアクセスレコードとしてアクセスログに記録する前記アクセス先サーバ装置から前記アクセスログを収集する処理、

収集した前記申請ログと、前記操作ログと、前記アクセスログとに基づいて、前記アクセスレコードとして記録されたアクセス状態が正規のアクセスかどうかを判定する処理、

を実行させるためのログ分析プログラム。

[請求項10] ログ収集部と、判定部とを備えたログ分析装置が行うログ分析方法であって、

前記ログ収集部が、

アクセス先サーバ装置へのアクセスを申請する複数の申請レコードが記録された申請ログを保有する申請ログ保有装置から前記申請ログを収集し、

前記申請ログ保有装置から通知された前記複数の申請レコードを保有し、前記アクセス先サーバ装置へアクセスするログインをアクセス装置から受け付け、前記ログインに対応する前記申請レコードが存在するか判定し、前記申請レコードが存在する場合には前記アクセス装置から前記アクセス先サーバ装置へアクセスを中継すると共に前記アクセス装置による前記アクセス先サーバ装置へのアクセス状態を操作レコードとして操作ログに記録するアクセス中継装置から前記操作ログを収集し、

アクセスされたアクセス状態をアクセスレコードとしてアクセスログに記録する前記アクセス先サーバ装置から前記アクセスログを収集し、

前記判定部が、

前記ログ収集部が収集した前記申請ログと、前記操作ログと、前記アクセスログとに基づいて、前記アクセスレコードとして記録されたアクセス状態が正規のアクセスかどうかを判定することを特徴とする

ログ分析方法。