6D-03

ITSMS 監査における不正特権 ID アクセス検出方式

砂田 英之†

三菱電機株式会社　情報技術総合研究所†

1．はじめに

近年、IT が企業活動の中核を担うにつれて、IT に対する監査要求が厳しくなってきている。また、トラブルの事後対応による作業負荷を軽減するため、PDCA サイクルを軸とした予防的な取り組みとして IT サービス管理(ITSMS)の考え方が重要性を増している[1]。

ITSMS 監査において、特権 ID による不正アクセスがないかを把握するためにアクセス履歴の調査を実施するが、作業が繁雑であることや、本人の権限を越えたアクセスしか検出できないという問題があった。

この問題に対し、申請ワークフロー（以下、WF と略す）と連携し、申請記録とアクセス履歴を照合して点検する方式[2]が提起されているが、業務サーバ間のアクセスに対して点検の例外処理が必要なことや、申請された利用時間と重複した不正アクセスが検知できないといった課題が残っていた。

本論文では、これらの課題を解決するために、アクセス履歴、申請記録、操作ログの照合により点検作業を自動化する方式について提案する。

2．従来技術

(1)申請記録とアクセス記録による照合

文献[2]では、申請 WF に登録された申請記録（業務の種類および作業予定時刻を含む）と、監査対象サーバのアクセス履歴を照合することで、不正アクセスの有無を点検する仕組みが開示されている。

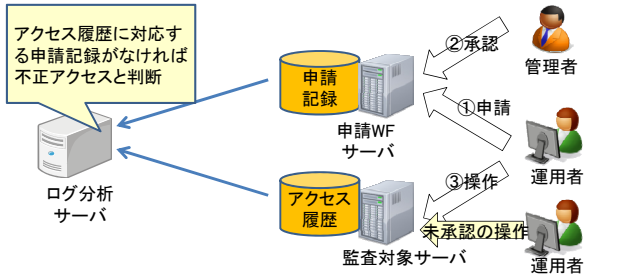


図1　システム構成（従来技術）

Unauthorized Access Detection Method for ITSMS
†Hideyuki SUNADA
Information Technology R&D Center, Mitsubishi Electric Corporation

これにより、運用者本人の権限内であっても、不適切なタイミングでの操作を容易に検知することが可能となった。

(2)課題

特権 ID によるアクセスには、業務サーバ間のアクセスのように、利用時間が不定のため利用期間を限定できないものがあり、これらを適切に判断するためには例外処理が必要で自動化することが困難であった。

また、申請記録があっても作業予定時刻と外部犯行者による攻撃が偶然同じタイミングで行われた場合には、従来の方式では、これらを適切に判断することが困難であった。

3．解決策

(1)操作ログとの照合による点検方式

監査対象サーバへは ID 利用制御部を経由してアクセスし、ID 利用制御部にて申請記録に基づきサーバへのアクセス制御を行うとともに、操作ログを残す構成とする。

担当者は事前に利用申請を行い、監査対象サーバにアクセスする。

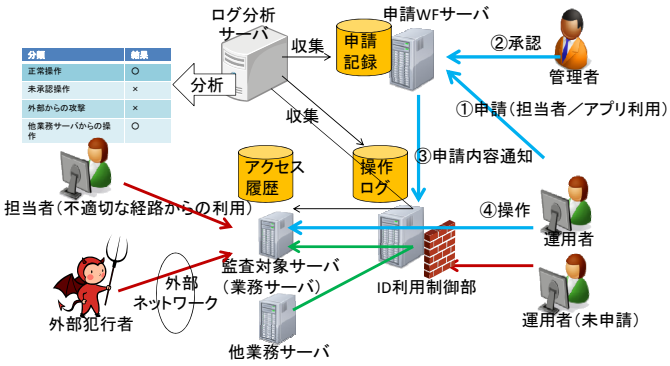


図2　システム構成（解決策）

また、他の業務サーバ（アプリケーション）から監査対象サーバへのアクセスも同様に、ID 利用制御部を経由して監査対象サーバにアクセスする構成とする。利用申請は業務サーバ管理者が事前に実施する。

点検時には、ID 利用制御部を経由したアクセスを正当なアクセスとして扱う。

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.

(2)実現方式

監査対象サーバの担当者は、作業を実施する前に申請 WF にて利用申請を行う。申請 WF では、管理者に対して利用申請があったことを通知し、管理者による承認の手続きにより、申請記録を承認状態に変更し、申請記録として保存する。

表１　申請記録（承認状態）

項目	内容
特権 ID	作業時に利用する特権 ID
運用者 ID	運用者の識別情報
対象サーバ情報	サーバのホスト名など
目的	作業の目的
利用期間	作業の開始～終了予定日時
作業内容	利用プロトコルなど

ID 利用制御部では、運用者の認証および各種利用プロトコルを中継する機構を持ち、運用者の認証後、申請記録と適合するアクセスであれば、指定された特権 ID で対象サーバとの認証を行い、アクセスを中継する。利用時間やプロトコルが異なるなど、不適合なアクセスの場合にはアクセスをブロックする。

アクセスを中継した場合には、ID 利用制御部にて、以下の操作ログを記録する。

表２　操作ログ

項目	内容
特権 ID	サーバへの認証に使った ID
運用者情報	運用者の識別情報
アクセス日時	アクセスを中継した日時
操作内容	利用プロトコルなど

監査対象サーバでは、OS のセキュリティログなどの機能により、運用者の操作の内容がアクセス履歴として記録される。

表３　アクセス履歴

項目	内容
利用 ID	認証したアカウント情報
操作内容	「ログイン」など操作内容
日時	操作の実施日時

ID 利用制御部を経由した場合には、申請記録と適合したアクセスのみが許可され、アクセス履歴に記録されたレコードの日時に対応する申請記録／操作ログが整った状態で保存される。

また、内部／外部犯行者による不正アクセスで、ID 利用制御部を経由しない場合には、操作ログが残らない状態となる。

表４　アクセス状態と各種記録の対応

アクセス状態		申請記録	操作ログ	アクセス履歴
運用者	正当	○	○	○
	不正 *未申請*	×	×	× アクセス不可
	不正 *経路不正*	×	×	○
業務サーバ	正当	○	○	○
外部犯行者	不正	?	×	○

以上により、ITSMS 監査における不正アクセスの点検作業としては、アクセス履歴に対応する申請記録および操作ログが揃っているかどうかで正当／不正を判断でき、例外処置もないため処理が自動化できるようになる。

４．評価

不正アクセス検出において、作業の繁雑さや本人の権限以上のアクセスしか検出できないことが課題となっていた。

従来技術では、申請 WF と連携することで、本人の権限内であっても不正なタイミング／操作によるアクセスを検出が可能になったが、業務サーバ間のアクセスや、他人の申請記録（利用時間）と重複した不正アクセスを検出できない課題が残っていた。

本方式を用いることで、アクセス履歴、申請記録、操作ログの対応関係を照合するだけで前述の不正アクセスの検出が可能になる。また、例外処置がないため処理の自動化ができ、作業を効率化することが可能となった。

５．今後の課題

本論文にて、業務サーバ間のアクセスや他人の申請記録と重複した時間帯でアクセスも含めた不正アクセスの検出方式を示した。

今後は、ログ自体の改ざんへの対策も含め、検討を進める予定である。

参考文献

[1]ITC プロセスにおける情報システムの信頼性向上へのアプローチ,（経済産業省 企業内 ITC・IT ガバナンス研究会、2008 年 6 月）

[2] ログ分析装置およびプログラム（株式会社ラック、特開 2009-75940）

Copyright ©2015 Information Processing Society of Japan.
All Rights Reserved.