特集論文

IT全般統制における特権ID管理システムの導入

砂田英之*
長田康志**

Implementation of Unrestricted Privilege ID Management System under IT General Control

Hideyuki Sunada, Yasushi Nagata

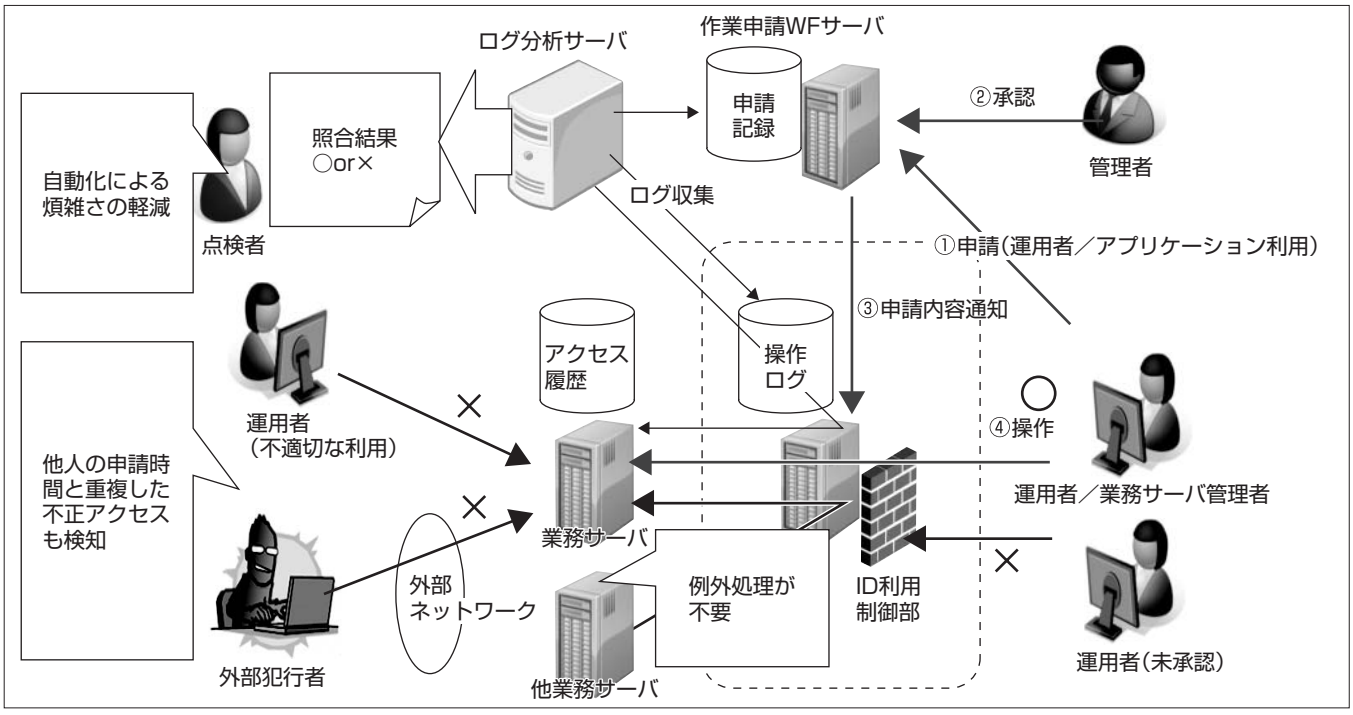
要　旨

近年，IT（Information Technology）が企業活動の中核を担うにつれ，財務統制の一環として実施されるIT全般統制で，その監査要求が年々厳しくなってきている。一部上場企業における個人情報の不正入手等を防止するため，IT運営管理基準を設ける対策が肝要である。さらに監査要件としての証憑（しょうひょう）取得や障害時の事後対応作業負荷の軽減，作業ミスの撲滅を図るため，PDCA（Plan-Do-Check-Action）サイクルを軸とした予防的な取組みとして，国際規格の１つであるITサービス管理システム（ISO（International Organization for Standardization）/IEC（International Electrotechnical Commission）20000-1/ITSMS（IT Service Management Standard））の重要性が増している(1)。

2008年から始まった三菱電機㈱のIT全般統制の監査では，システム構築・運用時に使われる一切の制限がない特権ID（Identification）による不正アクセスがないかを，Windows(注1)，データベース，ミドルウェアであるERP（Enterprise Resource Planning）システムのアクセス履歴を証憑として監査する。しかし，年々その基準が厳格になり，証憑を取得する作業が煩雑でかつ時間がかかることや，職務権限内で持ち出し許可されていない情報へのアクセスは点検できないという問題があった。この課題に対し，従来は申請ワークフロー（以下“WF”という。）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で対応していた。この仕組みを用いても，業務サーバ間のアクセス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は検知ができないといった課題が残る。

本稿では，これらの課題を解決するため，アクセス履歴，申請記録，操作ログの照合を毎月行い，複数の本番サーバ上のアクセスログ点検作業を自動化して事象発生後に特権IDによる不正アクセスを効率的に“発見”する方式と，それが運用上問題ないことを検証するために行う負荷試験について述べる。

（注１）　Windowsは，Microsoft Corp. の登録商標である。



特権ID管理システムのシステム構成と作業フロー

作業フローは，①運用者が特権IDの利用を管理者へ申請，②管理者が作業日時，作業内容，作業対象サーバを確認して承認，③ID利用制御部へ自動的に申請内容を通知，④運用者が作業を開始し，申請時間内に作業を終了の4ステップからなる。この一連の作業は監査ログとして各業務サーバに蓄積され，ID利用制御部で蓄積された操作ログを点検することで，“不正アクセスの有無”を検知する。

*三菱電機㈱ 情報技術総合研究所
**三菱電機インフォメーションネットワーク㈱

1. まえがき

2008年から始まった三菱電機㈱のIT全般統制では，特権ID管理の監査対象がWindowsからデータベース，ミドルウェアのERPシステムへと範囲が広がり，開発者が本番機にアクセスできない規定も新たにできた。そのため，アウトソーシングサービス提供元である三菱電機インフォメーションネットワーク㈱(MIND)が本番機のメンテナンス作業を行い，特権ID管理における“承認”とその“申請書及び監査ログ収集”及び“月次での不正アクセスの点検”が必須の通常業務となった。手作業では数台のサーバしか対応できないため，今後MINDのクラウド事業の拡大によってその数が急速に増加する場合，システムの変更管理の煩雑化を防ぎ人為ミスを防ぐ運営手段の構築が急務となった。

2013年から今回の特権ID管理システムの開発に着手し，200台のサーバに適用するというシステム要件の下，システムの信頼性を担保するための負荷試験の方式を考案し，実施した。

本稿では，この開発に採用したアクセスログ点検方式及びその運用実証の一環としての負荷試験について述べる。

2. 従来技術

2.1 アクセスログ点検方式

⑴ 申請記録とアクセス履歴による照合

申請WFによって登録された申請記録(業務の種類と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し，不正アクセスの有無を点検する仕組みで対応していた(**図1**)。これによって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できる。

⑵ 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同様，利用期間を限定できないものがあり，これらを“アクセス許可”“アクセス不許可”と適切に判断するためには例外処理が必要であり，自動化することが困難であった。さらに，申請記録があっても作業予定時刻と外部犯行者による不正アクセスが偶然同じタイミングで行われた場合には，従来方式では適切に区別できない。

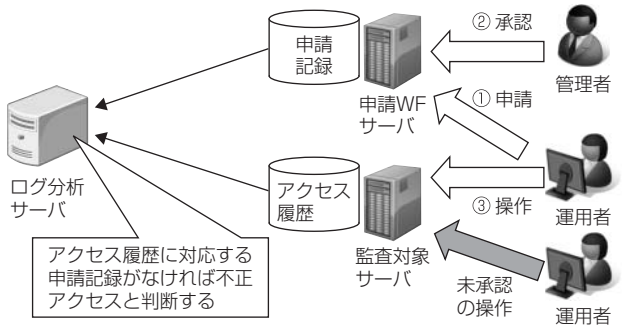


図1．システム構成(従来技術)

2.2 負荷試験

⑴ 仮想化基盤を活用した負荷試験

多重接続の負荷試験を実施する場合，必要台数分の物理マシンを準備することは非効率であり，仮想マシンで実現するケースが増えてきている。一時的に仮想マシンを複製して試験環境を構築することで，試験に係る費用を抑制できるほか，設置場所の問題や管理コンソールによる一括操作によって試験の効率化を図ることができる。

⑵ 課題

大量の仮想マシンを試験環境に用意する場合，テンプレートとなる仮想マシンを用意し，それを複製する方法を採用していた。しかし，この方法では複製時にホスト名を指定できるが，インストールされているソフトウェアによってはホスト名(又はIPアドレス)が変更された場合に再設定／再インストールが必要になるという問題があった。これに対して，プロビジョニングスクリプトの実行等，仮想マシンの作成時に初期設定を行う方法が仮想環境で準備されているが，バックグラウンドで実行されるため，画面がアクティブにならず，画面インタフェースを持つ操作の自動化が困難であるという課題があった。また，運用者の操作の自動化も本試験の効率化のために必要であったが，これも同様に課題となっていた。

3. 解決策

3.1 アクセスログ点検方式

3.1.1 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利用制御部では申請記録に基づき，サーバへのアクセス制御を行い，操作ログを残す構成とする。運用者は事前に利用申請して，監査対象サーバへアクセスする。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。なお，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取り扱う(**図2**)。

3.1.2 実現方式

⑴ 特権IDの利用申請と申請記録

監査対象サーバの運用者は，作業を実施する前に申請WFで利用申請を行う。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，管理者の承認手続きによって，申請記録(**表1**)を保存する。

⑵ ID利用制御部を経由した対象サーバへのアクセス

ID利用制御部では，運用者の認証及び各種利用プロトコルの中継を制御する機構を持つ。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場合は，アクセスをブ

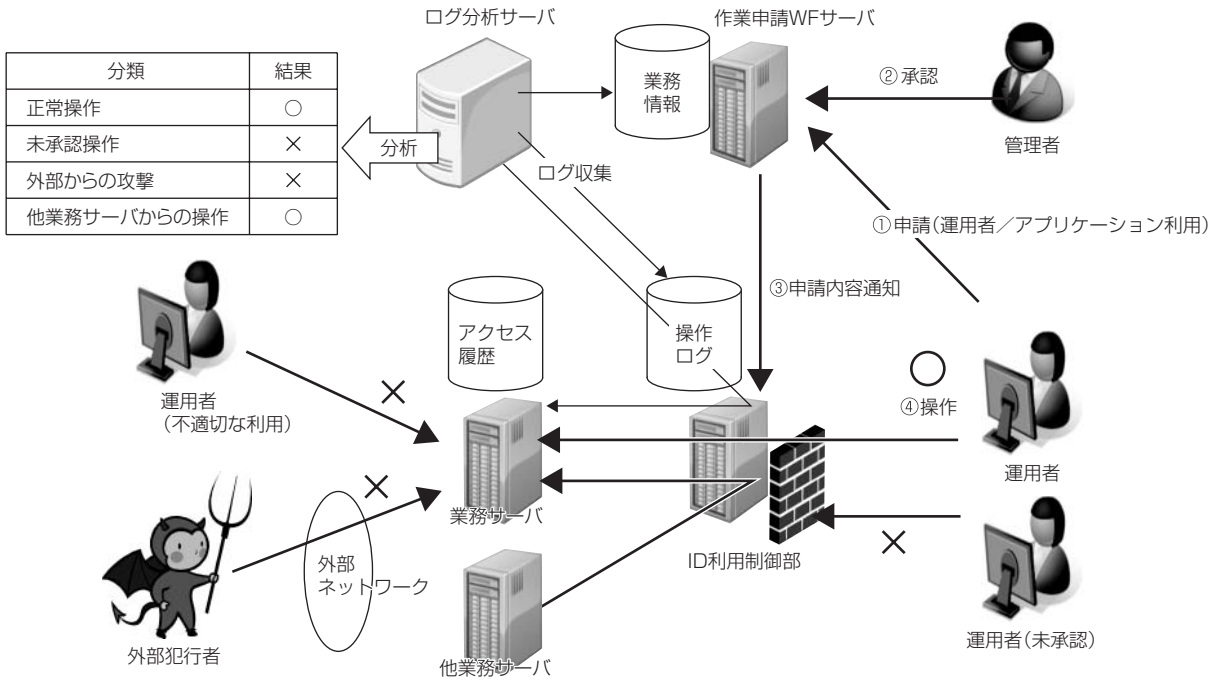


図2．システム構成(解決策)

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	作業開始～終了の予定日時
操作内容	利用プロトコルなど

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など
操作内容	利用プロトコルなど

表3．アクセス履歴

項目	内容
特権ID	サーバへの認証に使ったID
操作内容	“ログイン”などの操作内容
アクセス日時	操作の実施日時

ロックする。**表2**は操作ログの内容である。

(3) アクセス履歴

監査対象サーバ上のOS(Operating System)のセキュリティ監査ログ等の機能によって，運用者の操作内容がアクセス履歴(**表3**)として記録される。

ID利用制御部を経由した場合は，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・操作ログの両方がそろった状態で保存される。一方，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ため，不正なアクセス等であることが判断できる。**表4**は，アクセス状態と各種記録の状況及び，それらに基づく判定結果を整理した一覧である。

表4．アクセス状態と各種記録の対応

アクセス状態		記録			判定	備考
		申請書	アクセス履歴	操作ログ		
ユーザー操作	承認(正常)	あり	あり	あり	○	正当アクセスと判断
	承認(不正)	あり	あり	なし	×	不正アクセスと判断(運用ルール非適合)
	未承認(正常)	なし	－	なし	×	ID利用制御部がブロック
	未承認(不正)	なし	あり	なし	×	不正アクセスと判断
業務サーバ	承認(正常)	あり	あり	あり	○	正当アクセスと判断(点検時例外処理不要)
	承認(不正)	あり	あり	なし	×	不正アクセスと判断(乗っ取り等の可能性あり)
	未承認(正常)	なし	－	なし	×	
	未承認(不正)	なし	あり	なし	×	
外部犯行	承認時間内	あり	あり	なし	×	不正アクセスと判断
	承認時間外	なし	あり	なし	×	不正アクセスと判断

このように，IT全般統制での監査における不正アクセスの点検作業は，アクセス履歴に対応する申請記録及び操作ログがそろっているかどうかで正当・不正を判断でき，例外処理の必要がなく自動処理が可能である。

3.2 負荷試験

(1) 初期設定方式

個別に仮想マシンの初期設定を行うことは煩雑であるため，今回はキー操作可能なスクリプトを採用し，ホスト名をキーとした設定ファイルに実行内容を指定することで対応した。1台の仮想マシンでスクリプトを実行し，スクリプトの処理によってリモートデスクトップで他の仮想マシ

ンのスクリプトを逐次起動し，指数関数的にスクリプトの実行台数が増加するよう設定して，設定に掛かる時間の短縮を図った。

⑵　メンテナンス操作シミュレーション

運用者の操作シミュレーションも初期設定と同様にスクリプトで実現した。環境を共通化するため，各仮想サーバのホスト名の命名ルールを“VMnnn（nnn＝000～150）”と定めて，nnnの仮想マシンはnnn＋１の仮想マシンに対して，メンテナンス操作のシミュレーション（スクリプトによって実施）を行うように設定した。

これによって各環境の共通化が図れるとともに，１台目の仮想マシンでスクリプトを実行するだけで，設定及びメンテナンス操作の自動化が可能となる。

4. 評　　価

4.1　新点検方式による効果

不正アクセスの検出で，作業の煩雑さや本人の権限がないアクセスしか検出できないことが課題になっていた。従来技術でも，申請WFと連携することによって，本人の権限内であっても不正なタイミングや操作によるアクセス検出が可能であったが，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。この方式を用いることで，申請記録，操作ログ，アクセス履歴の対応関係を照合して，先に述べた不正アクセスの検出が可能となる。また例外処理がないため，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。

4.2　負荷試験とその効率化

特権ID点検（ログ収集）の実現に当たり，対象サーバ（顧客の本番機）を想定し，監査ログを特権ID点検システムで収集するためのエージェントを開発した。

通常運用の試験23項目，異常試験５項目に加え，200台規模での動作を検証するための負荷試験を実施した。負荷試験では，最大150台のWindowsサーバを構築して，エージェント導入，ログ収集，サーバ削除をクラウド環境で構築することで，負荷試験のための準備を数時間以内にすることができ，試験の効率化を図ることができた。

今回，これらの試験環境の構築方法を活用し，ログ収集対象サーバの台数を最大150台まで段階的に増やして負荷試験を行った。**表５**に試験のシステム要件をまとめた。

この負荷試験は，クラウド環境で監査ログ収集対象Windowsサーバを構築して，サーバ起動時にログ収集エージェントを導入し，さらに運用者の操作シミュレーション（ログイン，ログオフ操作の繰り返し）を自動化するスクリプトを作成することで実施した。

表５．システム要件

分類		内容	
機能要件	特権ID管理	WF機能	WFによる監査サーバ利用の申請及び承認
		アクセス制御機能	利用申請に基づく監査サーバへのアクセス許可／不許可
	特権ID点検	ログ収集機能	監査対象サーバ及び特権ID管理システムからのログ収集
		点検機能	監査ログから不正アクセス抽出と結果の出力
		保管／削除機能	指定期間を経過したファイルの削除
非機能要件	規模	監査対象サーバ数	200台規模
	性能	ログ確認	前日のログを確認可能
		点検時間	数時間以内に完了

その結果，ログ収集エージェントによる操作シミュレーションに対応するログが全て収集されたことを確認できた。さらに，試験手順をスクリプトで自動化し，作業の効率化，試験時間の短縮と試験にかかるコストの最小化が可能となり，150台接続時に次の内容で試験を実施することができた。

＜負荷試験の実績＞

⑴　構築（150台）：3.0時間

⑵　操作シミュレーション・ログ確認：2.0時間

⑶　消去（150台）：0.5時間

⑷　作業時間：合計5.5時間

⑸　利用料金：約５万円

5. む　す　び

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のアクセスも含めた不正アクセスの検出方式について述べた。この技術は監査上“発見的統制”と呼ばれ，事象発生後，特権IDによる不正アクセスを効率的に“発見”するためのものである。今後，ログ自体の改ざん対策，Windows以外のOSの監査ログ収集とその点検方式の開発，仮想化環境での監査ログの点検，特権IDでの不正アクセスのリアルタイム検知技術も含め，検討を進めていく。

負荷試験では，クラウド環境の操作は標準のポータル画面から実施したが，一度に構築・削除可能なサーバ台数に制約があり，構築・削除に数時間を要してしまった。今後は，クラウドのAPI（Application Programming Interface）を活用し，一度の操作で大量のサーバの構築・削除を実現し，より短時間で負荷試験の環境を準備する方式について検討していく。

参 考 文 献

⑴　経済産業省 企業内ITC・ITガバナンス研究会：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（2008）
http://www.itc.or.jp/foritc/itccommunity/search/dlfiles/S07002_syousai.pdf