IT全般統制における特権IDのアクセス管理

金融商品取引法にいう内部統制が2008年４月から本格適用され、財務データの改ざんリスクが高いシステム管理者などの特権IDに対するアクセス管理が急務の課題となっている。本稿では、特権IDのアクセス管理に関わる問題点について述べ、NRIセキュアテクノロジーズが提供するアクセス管理ソリューション「SecureCube/Access Check」による解決策を紹介する。

高まるアクセス管理の重要性

内部統制の柱のひとつであるIT全般統制で求められる「内外からのアクセス管理」は、同じくIT全般統制の要素である「ITの開発、保守に係る管理」「システムの運用、管理」などと比べて対応への遅れが目立っていた。しかし内部統制整備の本格適用を受けて、その重要性への認識が高まってきている。

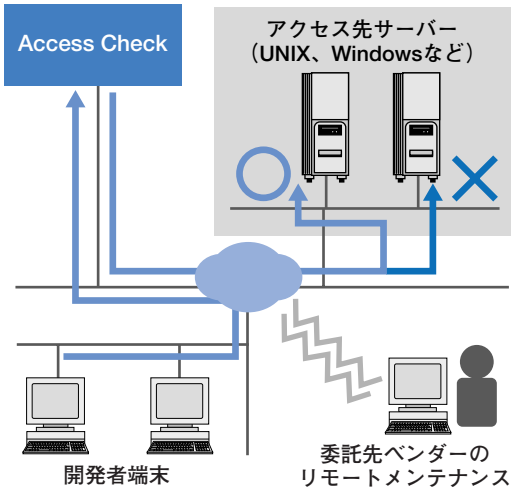
財務データを管理するシステムに対してアクセス権をもつ者のなかでも、システム管理者やシステム開発担当者のようないわゆる特権IDの保持者は、システムに対して大きな権限をもつと同時に、本番環境で稼動しているプログラムやデータの破壊・改ざんが立場上可能であることから、財務データの粉飾につながる大きなリスク要因でもある。そのため、特権IDに対しては高いレベルの統制が求められる。

特権IDのアクセス管理における課題

IT全般統制のアクセス管理では、本番サーバーごとにアクセス可能な人を限定し、適切なアクセス権を与え、本番サーバー上で誰が作業したかという証跡を残すことが重要である。しかし、システム開発・運用の現場では、通常よりもリスクが高い特権IDがメンバー間で共有され、リスクが放置されているケースが多いのが実情である。

この問題を解決するための一般的な方法には、各サーバー上に個人を識別するためのアカウントを作成したり、アクセス管理用のプログラムを導入したりすることなどが考えられる。しかし、サーバーの台数が多ければ多いほど、対応するための期間やコストがより大きくなる。そのため、特権IDのアクセス管理の必要性を認識しながらも、対応が遅れているという企業も多いのではないだろうか。

図１「Access Check」を介したサーバーアクセス



NRIセキュアテクノロジーズ
ソリューション事業部
上級セキュリティコンサルタント
池浦規之（いけうらのりゆき）
専門は情報セキュリティシステム

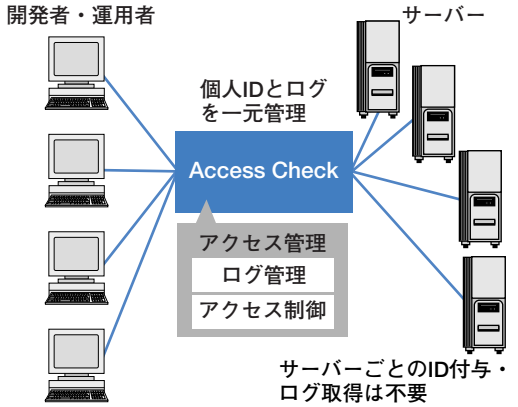
導入が容易なアクセス管理ソリューション

NRIセキュアテクノロジーズでは、導入コストおよび導入負荷を低減したアクセス管理ソリューション「SecureCube/Access Check」（以下、「Access Check」）を提供している（http://www.nri-secure.co.jp/service/cube/accesscheck.html）。

「Access Check」は、本番サーバーではなく、開発者端末と本番サーバーとの間に入るプロキシ（代理）サーバー上でアクセス管理を行う（図1参照）。こうすることで、24時間365日の稼動が必要なシステムでも、本番サーバーに影響を与えずにアクセス管理が行える。

本番サーバーにアクセスするユーザーのアカウントを「Access Check」に登録しておけば、ユーザーごとにアクセス対象のサーバーを制限することが可能となる。また、許可された本番サーバーへのアクセスは「Access Check」経由で行われるため、誰がどの本番サーバー上で作業を行ったのかというログ（やり取りの記録）を「Access Check」サーバー上で一元管理することができる（図2参照）。さらに、ほかに類のない「アクセス申請・承認機能」により、本番サーバーへアクセスした記録だけでなく、アクセスの目的や時間など、アクセス申請内容や承認者もログとして残し、「Access Check」上で突き合わせを行う。このため、従来は紙ベースで行っていた本番サーバーへのアクセス申請に関わる業務フローを「Access Check」上で実現でき、より厳格なアクセス統制を構築することができる。

図2 「Access Check」上で個人を識別



限られた時間での対応に向けて

従来、「Access Check」は高いセキュリティを求められる金融機関を中心に多くの導入実績があった。いまではIT全般統制への対応の必要から、製造業や流通業などへの導入も増えてきている。

内部統制の構築を義務づけられた企業は、自社が抱えるリスクや統制目的を判断しながら、対応すべき統制内容を決めていく必要がある。しかし最終的には監査人の判断に左右されるところもあり、必ずしも解が1つではないのが難しいところである。監査人からのさまざまな指摘事項への対応に迫られるなか、「Access Check」は、報告までの限られた時間のなかで現実的かつ効果的なアクセス管理を実現するための有力な選択肢となろう。■