IT全般統制における企業内ID管理のポイント

OpenIDなどを用いたユーザー向けのID連携サービスを提供するには、まず企業内システムのID管理を徹底させる必要がある。企業内でのID管理はIT全般統制における重要な課題であり、高いレベルの統制が求められる。しかし、実際に内部統制評価を行うと、十分な統制を確立できていないケースは多い。本稿では、企業内システムの開発を中心にID管理のポイントを示す。

内部統制評価で発見されるID管理の不備

内部統制においてID管理が重要だということを認識していても、十分な統制を確立できていない企業は多い。IT全般統制の評価で発見される企業内のID管理の不備は、以下のようなケースが典型的である。

まず、①開発担当者が本番環境にアクセスできるケースがある。この場合、実行プログラムを不正に書き換えられるリスクがある。また、②ユーザーに必要以上に特権IDを与えているケースや、退職者や異動者のIDが残っているケースがある。不要なIDやアクセス権が残っていると、非権限者によりIDが不正利用されるリスクがある。③特権IDが、申請による貸し出しという形で運用され、恒常的には使用されていないものの、貸し出された特権IDとパスワードが固定化され、パスワードの変更が実施されていないケースもある。この場合、特権IDは実質的に申請なしに継続的に利用でき、不正に利用されるリスクがある。

このほか、④実行プログラムまたはデータに対する不正アクセスの有無をモニタリングしていないケースもある。予防的統制がある場合でも、承認された作業の範囲を超えて、不正に実行プログラムまたはデータを書き換えられるリスクがある。

ID管理不備の背景にある根本課題

ID管理に不備がある場合、以下のような状況が問題の真因となっていることが多い。

1つ目は、データや実行プログラムへのアクセスに関する明確なルールが定められていないことである。そのため、セキュリティポリシーのような方針はあっても、アクセスの実務的な手続きが定められていないこと、手続きがあってもシステムごとに異なり、全社的に整合性がとれていないことがある。さらに、ルールは存在してもそれに基づくシステム設定がなされていないケースもある。

2つ目は、開発担当者や運用担当者がシステム稼働率の維持に主眼を置き過ぎることである。リリース作業において受け付けからリリースまでの時間を最小にしようとするあまり、統制活動を二の次にしてしまうケースがある。この場合、必要以上に権限を付与したり、共有IDや未使用IDを発生させやすい。

3つ目は、ID管理の作業負荷に見合った要員が割り当てられていないことである。これまで、現場に対してはつねに運用管理コスト

野村総合研究所
システムコンサルティング事業本部
ERMプロジェクト部
副主任システムコンサルタント
森　哲也（もりてつや）
専門は内部統制評価、システム監査など

の圧縮という要請があった。そのようななかで内部統制強化という新たな要請が出現したために、運用担当者が過負荷状態になっていることがある。特にID管理については、IDの貸し出し管理・払い出し管理、IDの棚卸し、不正アクセスの有無のモニタリングに関して高いレベルの統制が求められ、運用担当者の負担が大きくなっている。

適切なID管理を行うための３つのポイント

ID管理の不備については、目の前の不備の改善に走る前に、先に述べたような根本課題を解決することが、結果として高いレベルの統制の確立および内部統制コストの削減につながる。それには３つのポイントがある。

１つ目のポイントは、漠然としているアクセスに関する要件をルールとして体系化し、それを社内で共有することである。アクセス管理を行うための具体的な施策（IDと参照・更新できる情報との関連づけ、不正アクセスの有無を監視する範囲の決定など）が明確になるとともに、全社視点で整合のとれたアクセス管理を実現することができるようになる。

２つ目のポイントは、内部統制の重要性についての教育・啓蒙活動をさまざまな機会を通じて継続的に実施することである。ID管理に限ったことではないが、監査部門やリスク管理部門の指示によって職務分掌や相互けん制の統制を導入しても、内部統制の本来の趣旨を理解していなければ、十分な統制が確立できているとは言えない。

３つ目のポイントは、統制活動の負荷を考え、必要な数の運用担当者を配置することである。それが難しい場合は、内部統制支援ツールを活用することで、手作業の負荷を軽減し、作業ミスを排除することもできるようになる。また外部委託も有効である。外部委託にあたっては、たとえば日本公認会計士協会の「監査基準委員会報告書18号（監査報告18号）」に記された「委託業務に係る内部統制の有効性の評価報告書」を入手できる委託先を選定することも有効である。

PDCAサイクルを通じ恒常的な取り組みを

内部統制報告制度（いわゆるJ-SOX）の初年度は、システムレベルの特権IDの扱いが注目される傾向にあったが、今後はデータ更新を伴うアプリケーションレベルのIDについても、同様に高いレベルの統制が求められることが予想される。また、リスクは外部環境、内部環境によって変化し、ID管理のリスクは技術革新による影響を受けやすい。今後、企業内・企業間システムでもOpenIDのような技術を利用したID連携が進んでいくと思われるが、技術進歩に合わせて定期的にリスク評価を行うことも、ID管理の重要なポイントとなる。

内部統制は一過性の取り組みではなく、恒常的に有効であることが求められる。内部統制のPDCAサイクルを通じて、組織としてID管理を行うことが必要である。 ■