特権ID管理の落とし穴
特権ID管理を成功させる３つの視点

基盤第２ソリューション部　第５ソリューション室
シニアITスペシャリスト　須永　義隆

1. はじめに

ID管理は、アプリケーションを利用する一般ユーザのIDを管理する一般ユーザID管理と、システムやアプリケーション運用者のIDを管理する特権ID管理に分類できる。

一般ユーザID管理は、2008年のJ-SOX法施行を機会にシステム化が進んできた。それに対し、特権IDは、一般ユーザと比較しID利用者が少ないため、システム化が進んでおらず、手作業で管理している場合が多い。

特権IDは、一般ユーザと異なる特徴を持っており（表１）、特権ID独自の視点での管理が必要である。

表１　特権IDと一般ユーザIDの特徴

	特権ID	一般ユーザID
ID例	root、Administratorなど	一般ユーザ個別のID
利用目的	システムやアプリケーションの運用および動作	システムやアプリケーションの利用
権限範囲	権限が広い（重要な情報にアクセス可能）	権限が狭い（許可された限定的なアクセスのみ可能）
利用者	人およびプログラム・アプリケーションが使用し、複数人が使う共用ID	人だけが使用し、個人に割り当てられたID

2. なぜ今、特権ID管理なのか

今、企業は、セキュリティの向上、内部統制、およびコンプライアンスなどの実現のために、特権IDを適切に管理することが求められている。特に、セキュリティ面では、情報漏洩の原因の80%が内部犯行と言われており、情報システム部門の責任者は、特権ID管理に特に不安を抱いている。また、監査等で、一般ユーザID管理から特権ID管理に監査視点が移ってきている。これらの理由により、特権ID管理のシステム化に取り組む企業が増えている。

3. 特権ID管理とは

3.1. 特権ID管理の課題

特権ID管理は、利便性・セキュリティ・コンプライアンスの３つの視点で、様々な課題がある。代表的な課題には、次の３つがある。

1. 特権IDは人に割り当てられたIDでないため、複数人が使用し、誰が使用したかの特定が困難
2. 特権IDの持つ権限は、広く、かつ強力であるため、担当業務以外の作業が実施可能
3. プログラム・アプリケーションが特権IDを使用していることが多く、パスワード変更で動作しなくなる可能性があるため、パスワード変更が困難

3.2. ３つの落とし穴

特権ID管理を考える場合、注意しなければならない３つの落とし穴がある。

第一の落とし穴は、rootやAdministratorだけが特権IDでないことである。OS、ミドルウェア、およびアプリケーションをインストールした時に作られるID、および設定の変更用にインストール後に作るIDなど、システム管理に用いる全てのIDを特権IDと考える必要がある。

第二の落とし穴は、企業の特権ID管理に対する要求事項が、IDの作成、変更、削除といったライフサイクル管理だけではないことである。担当業務以外の作業ができないようにするための権限管理も特権ID管理に求められている。

第三の落とし穴は、特権ID管理の一般化、共通化された概念が存在しないことである。そのため、特権ID管理の導入では、特権IDの種類、範囲、および管理業務を定義し、明確にすることが重要である。

3.3. 特権ID管理のシステムイメージ

特権ID管理に期待される課題解決やお客様要望を考慮すると、特権ID管理システム（図１）は、３つの機能から構成される。

1. IDの一元管理を実現する、ID管理機能
2. 権限制御を実現する、アクセス権管理機能
3. ログの一元管理を実現する、ログ管理機能

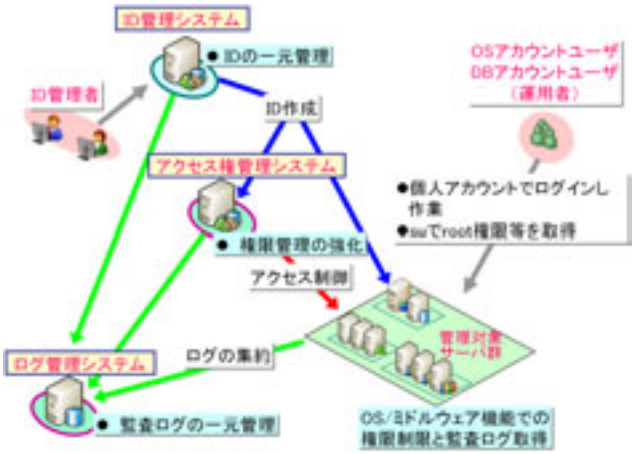

図１　特権ID管理全体イメージ

4. 特権ID管理を考える３つの視点

特権ID管理に必要な３つの機能を述べたが、これら３つの機能を全て高いレベルで実現する必要はない。特権ID管理は、３つの機能の三位一体で実現するものである。そのため、以下の３つの視点で、それぞれの機能をどの様に配置し、どのくらいの機能レベルで実装するかを考え、システム要件を決めていく。

1. 目的は、利便性・セキュリティ・コンプライアンスのどれか
2. 必須の要件は何か
3. 専用の製品を導入するのか、既存システムが持つ機能を利用するのか

ID管理の目的と対策例をまとめた結果（表２）、例えば、権限管理は、セキュリティを重視した場合に、優先度が高い機能となる。この場合、専用の製品を導入するか、既存のOSやミドルウェアの機能を使うかは、権限管理への要求レベルによって判断する。

表２　特権ID管理の目的と対策例

目的	機能	対策例	優先度
利便性を重視した場合	ID管理	・ID管理システムで、各人用のOSアカウント作成、修正、削除、およびパスワード変更の一元化	高
	権限管理	・OS機能で特権IDへのスイッチの制限を実施	中
	ログ管理	・各システム（サーバ）で、最低限のログ（認証ログ、suログ等）を取得	低
セキュリティを重視した場合	ID管理	・ID管理システムで、各人用のOSアカウントおよびDBアカウント作成、修正、削除、およびパスワード変更の一元化 ・共有IDの廃止 ・不要なアカウントの有無を管理 ・定期的なパスワード変更の実施	高
	権限管理	・root等を使わないように、必要な権限を付与したアカウントの作成 ・アクセス管理製品で、権限の制限を実施	高
	ログ管理	・各システムで認証ログ、suログ、および特権IDでの操作ログを取得 ・ログファイルを改竄されないように保護	中
コンプライアンスを重視した場合	ID管理	・特権ID管理のルール化 ・共有IDの廃止 ・特権IDを台帳で手動管理	高
	権限管理	・OS機能で特権IDへのスイッチの制限を実施	中
	ログ管理	・各システムで認証ログ、suログ、および特権IDでの操作ログを取得し、ログ管理システムで、ログを集約	高

5. まとめ

特権IDの適切な管理は、情報システム部門が早急に取り組むべき重要な課題である。この課題を、３つの視点を織り込んで特権ID管理システムとしてシステム化すれば、お客様が満足できる形で解決できると確信している。