

情報システムアカウントの統合管理を実現する 大規模企業向け ID 管理ソリューション

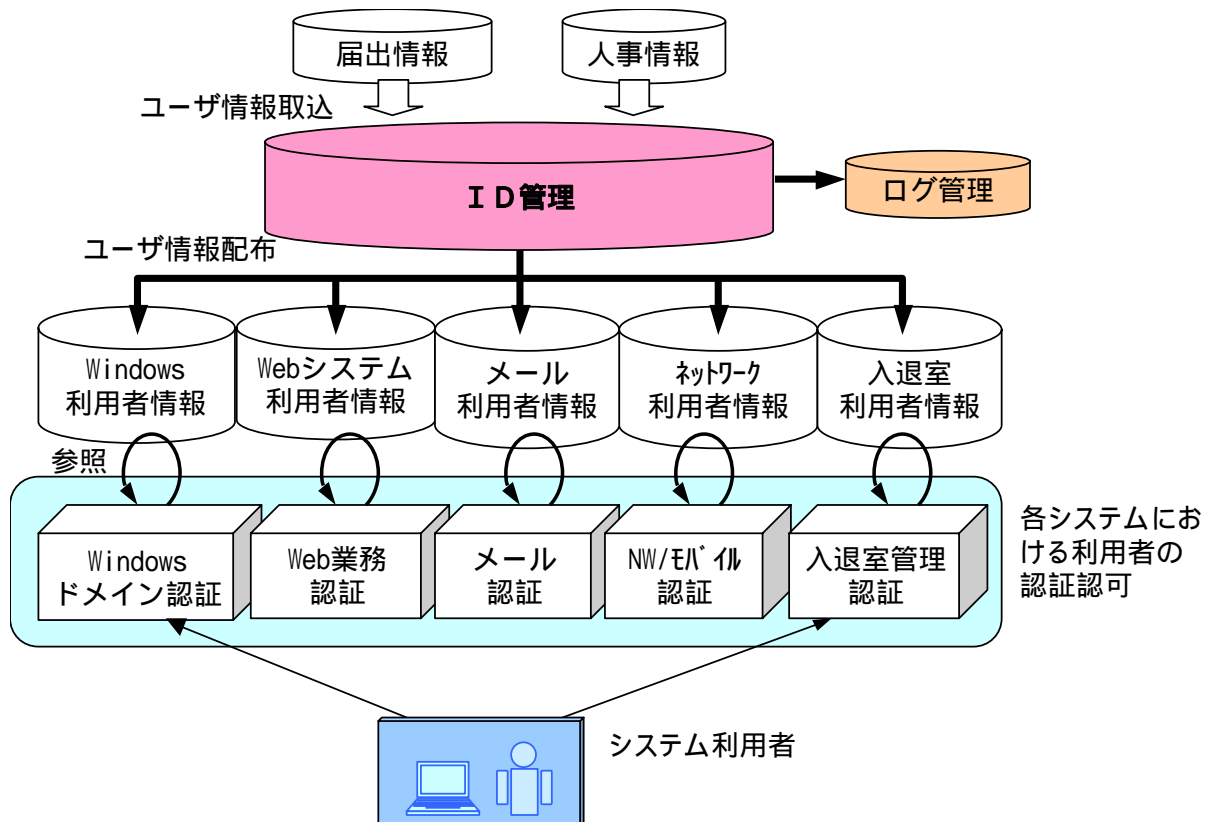
玉田 純*
白木 宏明**

要 旨

企業の情報システムセキュリティは、個人情報保護法や金融商品取引法等、法令面での要求もあり、必要性は高まる一方である。情報システムにおけるセキュリティ対策の基本は、システム利用者の特定（認証）及び利用権限管理（認可）を正確に行うことである。これを実現するためには、システム利用者の情報を正確に管理する事が必要であるが、大規模企業においては利用者、所属組織数、業務システム数などが膨大な数になるため、これを各システムや組織毎に管理していると組織改編などの際に多くの労力が必要となるのみでなく、これらの情報そのものに対するセキュリティを担保するうえでも問題が多い。

三菱電機インフォメーションシステムズ(株) (MDIS) では、これらの課題を解消するためのソリューションを“ID

管理ソリューション”として提供している。このID管理ソリューションは、MDISのトータルセキュリティソリューションの中核に位置するものであり、5つの階層（データソース、マスターデータ、ID管理サービス、管理対象、業務アプリ）から構成され、人事データベース等と連携してユーザ情報を最新に維持するほか、この情報に基づいて各業務システムの利用者情報を更新し、対象システムに対して配布・反映するための機能を有している。組織変更や人事異動などによる変更を自動的・一元的に各業務システムの利用権限に反映できるため、企業全体のセキュリティシステムを維持・管理するうえでの必要性は高く、今後は更にニーズが高まるものと予測している。



セキュリティシステムにおける ID 管理の位置付け

ID管理は企業全体のセキュリティシステムの中核にあつて、各種業務システムにおける利用者（ユーザ）のID（識別情報）や利用権限情報などを一元的に管理する仕組みである。人事情報や各種届出等の変更と連動して各業務システムの利用者情報や利用権限情報を最新の状態に維持・更新し、所定のタイミングでこれらの情報を該当するシステムに配布・反映する。また、これらの変更履歴は、後日の内部統制監査などのために情報更新の証跡として保管しておく。

1. ま え が き

個人情報保護法や金融商品取引法におけるIT統制等、法令面での要求もあり、企業の情報システムセキュリティについてはその必要性は高まる一方である。情報システムにおけるセキュリティ対策の基本は、当該システムの利用者を特定（認証）し、その利用者が有している権限に基づいた利用制限を行う（認可）ことである。そのためには個々の利用者に関する情報（アカウント名、認証に必要となるデータ、利用権限、その他付帯情報）を管理する必要があるが、大規模企業においては人事組織が複雑なことや情報システムが多数に渡ることから、これらの利用者情報を各システムで個々に管理することは、効率及び網羅性の点で多くの労力が必要となる。また、情報セキュリティの根幹となる利用者情報が、各システムに散在してそれぞれのシステム管理者に管理を委ねられることから、セキュリティ面でも脆弱になる。

ID管理ソリューションは、これらの問題を解決し、全社的な情報システムセキュリティを構築するうえでの基盤を提供するものである。

2. トータルセキュリティとID管理

2.1 トータルセキュリティモデル

図1に我々が提唱しているトータルセキュリティモデルを示す。本モデルは、企業内の情報を保護する事を目的に、“物理セキュリティ”と“情報セキュリティ”の両面からの施策を組合せた構成となっている。

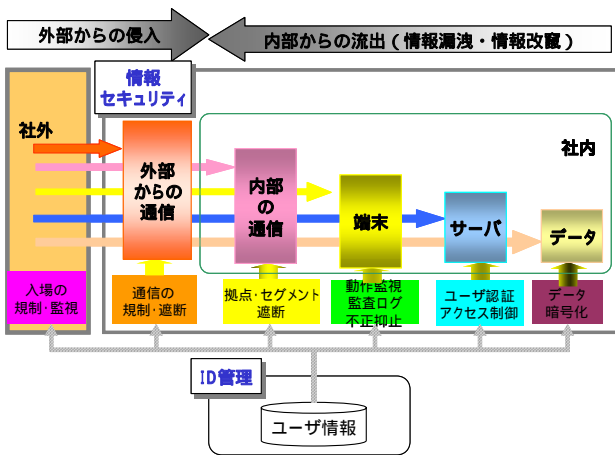


図1 . トータルセキュリティモデル

“物理セキュリティ”は、物理的な不正アクセス防止を実現するための施策であり、具体的には、入退室管理システムなどが該当する。また、“情報セキュリティ”は、システム内に保有している電子的な情報へのアクセス制御を実現するための施策であり、以下の5つのセキュリティ施策を複合的に組合せることで実現する。

(1) 外部ネットワーク施策

企業のネットワークにおいて、外部ネットワークとの通信境界で実施する。具体的には、FW(Firewall)やIDS(Intrusion Detection System)などが該当する。

(2) 内部ネットワーク施策

イントラネットのアクセス点にて実施する。具体的には、メールフィルタリングやネットワーク認証などが該当する。

(3) 端末における施策

端末上での不正操作対策であり、操作監視、操作抑止、監査ログ収集などが該当する。

(4) サーバにおける施策

業務アプリケーションを実行するサーバにおける施策であり、業務処理の実行に対するユーザ認証のほか、データベースアクセスへのアクセス権限の管理などが該当する。

(5) データに対する施策

データ自体に対する保護で、コンテンツ管理や暗号化などが該当する。

2.2 ID管理の役割

図1のモデルで示した各セキュリティ施策では、“正当な利用者による正当な行為”が否かについて判断する必要がある。“ID管理”の役割は、この判断に必要となる個々の利用者に関する情報を一元的に管理した上で各施策に提供する事であり、本稿で紹介する“ID管理ソリューション”はこれを実現するための具体的手段である。

3. ID管理ソリューション

3.1 概略アーキテクチャ

ID管理ソリューションにおける“ID管理”と、それに関連した基本的な処理構造を図2に示す。

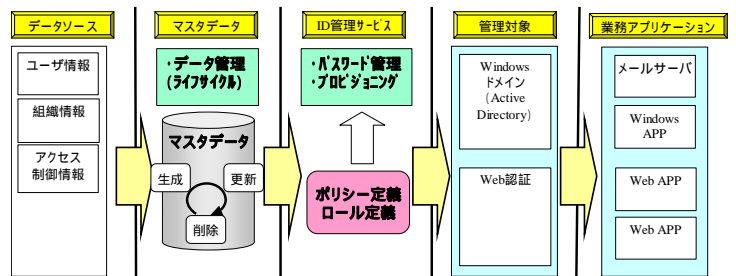


図2 . ID管理アーキテクチャ

図からも解るように、外部から“データソース”を取り込んで、“マスターデータ”としての利用者情報の生成・更新・削除を行い、“ID管理サービス”としてポリシー定義やロール定義に基づいたID管理を支援する。また、所定のタイミングや手動操作によって、“管理対象”別

の利用権限情報を配布し、各システムの“業務アプリケーション”では、配布された利用権限情報に基づいて認証や認可を実行する。以下に、から の各構成要素について補足説明する。

(1) データソース

ID管理のための入力情報となる情報源であり、ID管理ソリューションの外部に位置する。それぞれの業務システムを利用する利用者の情報（氏名、システム上のアカウント名とパスワード、職制情報等）のほか、人事組織情報などからなる。データソースは、一つにまとまっている必要は無く、複数のソースに分散していても構わない。

(2) マスタデータ

利用者情報など、ID管理を実現するうえでの基本となるデータであり、複数のデータソースから収集したデータを所定のアルゴリズムによって加工整形する事で作成される。マスタデータには、個々の利用者の人事情報やその利用者が使用する業務システムの利用権限管理に必要な情報のほか、後述する“ライフサイクル管理”を含めたID管理を実現するための内部処理に必要なデータ（例えば入社、異動及び退社日付や各ユーザの業務システム利用履歴、業務システム毎の使用可否等）が格納されている。

(3) ID管理サービス

予め設定されているシステム利用権限管理ルール（ポリシー定義、ロール定義）に従い、マスタデータに登録されている個々の利用者の利用権限情報を更新し、利用者情報と共に“管理対象”に提供する。なお、利用権限情報の更新及び管理対象への配布は、人事情報・組織情報の変動（人事異動や組織変更等）、業務システム利用権限管理ルールの変更、業務システムの変更（新規構築等）などのほか、パスワードの有効期限切れなどの時限発生的なタイミングでも行われるようになっている。

(4) 管理対象

ID管理サービスから配布される利用者情報及びその利用者に付与された利用権限情報を受取る業務システム側の機構であり、その業務システムが提供するサービスへのアクセス制御に当該情報を使用する。業務システム毎に必要なとなる利用権限情報の内容は異なるため、ID管理サービスでは、管理対象毎に配布する情報のテンプレートを所有しており、情報配布の際にはこのテンプレートを通して必要な種類の情報のみを選別して配布する。

(5) 業務アプリケーション

管理対象から利用者情報及び利用権限情報を受けとり、必要に応じて業務アプリケーション単位での利用制限管理を実現する。

3.2 基本機能と実現アルゴリズム

ID管理ソリューションでは、3.1 で説明したアーキテクチャの下で、効率的且つ一元的なID管理を実現している。この機能を実現するための基本的な仕組みについて、以下に記す。

(1) マスタデータの定義

マスタデータには、各業務システムを利用する全ユーザの情報が保持されている。これらの情報には、各業務システムに共通するもの（氏名、所属組織、役職等）のほか、業務システム毎に固有のもの（システム利用アカウント、パスワード、システム個別届出情報等）があり、データソースや業務アプリケーション側の情報との対応付けを含めて事前にデータ項目の内容を定義しておく必要がある。

(2) 利用者関連情報の収集及び保存

複数のデータソースから必要な情報を収集し、上記の定義に基づいてマスタデータに収集・保存する。データソースの収集方法には、バッチ系とオンライン系の2種類があり、バッチ系は主に人事情報や組織情報などの定期更新を反映する時に使用し、オンライン系は各種届出やワークフローからの利用者情報の収集や各業務システムのパスワード変更等を反映する時に使用する。

(3) 利用権限と配布情報の管理

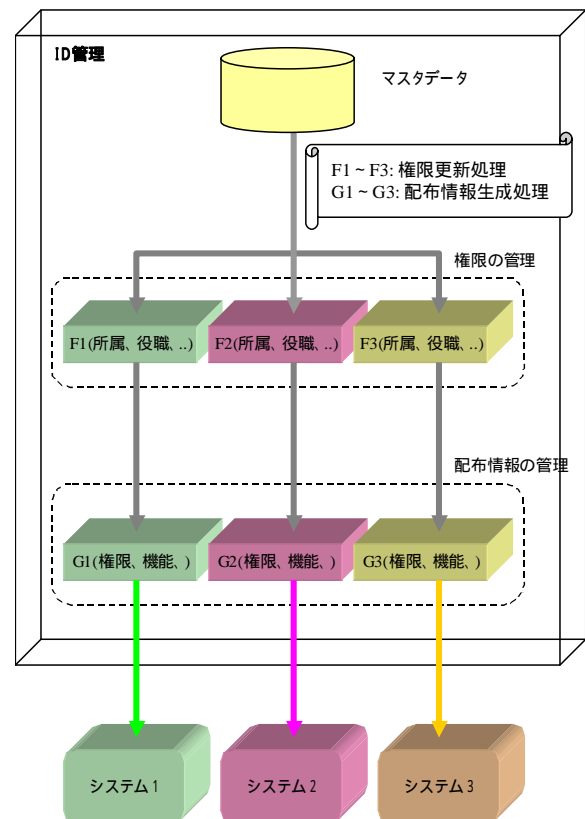


図3 . 利用権限と配布情報の管理

(a) 利用権限の管理

マスタデータ上の各種情報に基づいて、管理対象毎に個々の利用者の利用権限情報を更新する。この更新処理は、既述のように予め設定されているシステム利用権限管理ルールに基づいて、個々の利用者の属性情報である所属組織、役職等を利用することで実現している。

(b) 配布情報の管理

更新された利用権限情報は、該当する利用者情報と合わせて管理対象としたシステムに配布するが、対象システムにおける各種プラットフォーム（OS及びミドルウェア）や業務アプリケーションによって内容やデータ形式が異なるため、それぞれの管理対象適した形に変換したうえで配布している。

(4) 利用者情報のライフサイクル管理

企業における組織変更や人事異動などによる変更をマスタデータに適宜反映し、管理対象の利用者情報・利用権限情報を最新に維持する機能である。更新タイミングには定期と即時の2通りが存在し、前述の“権限の管理”と“配布情報の管理”のアルゴリズムに基づいて関連情報を自動更新することで、利用者情報のライフサイクル管理を一元的に行うことができる。

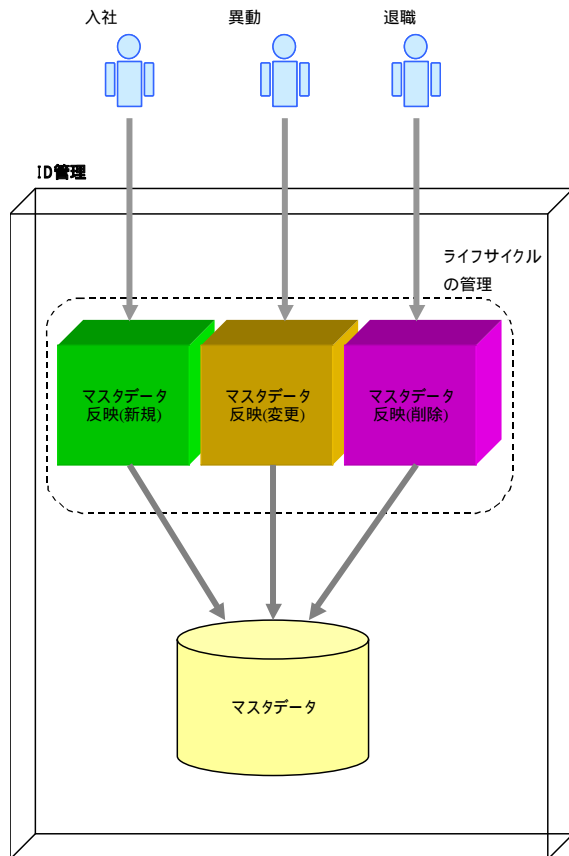


図4. 利用者情報のライフサイクル管理

3.3 セキュリティ強化に向けた応用

ID管理ソリューションは今まで述べてきたように、各種の業務システムにおいて利用者の認証及び利用権限管理を行うための基礎情報を提供するものであるが、それ以外にも下記のような用途への応用が可能である。

(1) 内部統制監査等への証跡提供

システム利用の正当性を確認する際の参考情報として利用権限の変更履歴などを提供する。

(2) ユーザ電子証明の管理

電子検認など個々のユーザが電子証明を発行するようなシステムにおいて、利用者情報のライフサイクル管理機能を電子証明の有効性を担保する仕組みとして利用する。

4. 導入事例

現在導入工事中の、某企業向けシステム構成事例を図5に示す。

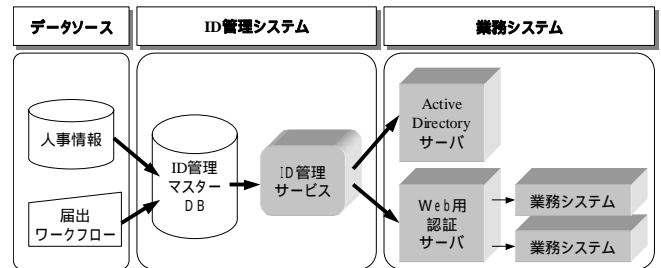


図5. 導入事例構成図

ユーザ数は数万人規模であり、これには社員及び協力会社社員が含まれる。執筆時点では、管理対象としているシステムは、ActiveDirectory^(注1)サーバ（Windows^(注2)ログオンアカウントの管理）とWebベース業務システムの2システムである。

5. む す び

セキュリティシステム構築の核となるID管理ソリューションについて紹介した。今後、企業の情報システムセキュリティに対する取り組みが拡大することは確実であり、現有のシステムを活かしつつ利用者情報等の一元管理が実現できるID管理ソリューションに対する需要は更に高まるものと考えている。

参 考 文 献

- (1) 日経BP内部統制プロジェクト編：ITから見た内部統制実践ガイド、日経BP社、（2006）

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

（注2）WindowsはMicrosoft Corp.の登録商標である。