アイデンティティ管理
Identity Management System

永島秀雄
カスタム・テクノロジー株式会社

要旨
企業や大学等の大組織では、多くの業務 IT アプリケーションを使用している。企業では、正社員、契約社員、協力会社社員、関連会社社員、パートタイマー、アルバイト等の多岐に亘る雇用形態が常用になっている。このような様々な方々が業務アプリケーションを活用して企業活動を支えているのが現状である。反面、セキュリティ管理が煩雑になりがちになるので、アイデンティティ管理は情報漏洩防止や内部統制（SOX 法）の面から必須となる。システム面及び法制面から考察する。

1. アイデンティティ管理の重要性

過去数十年間、Information Technology (IT)は、組織の生産性を高め、また、個人の活動にも利便性を与え、社会の隅々まで浸透してきた。大組織（大企業、大学、政府機関等）は、電子メール、文書管理システム、顧客管理システム、生産管理システム、グループウェア等々の数多くの業務 IT アプリケーションを使用している。今後も、益々業務 IT アプリケーションは増加していくのは間違いない。業務 IT アプリケーションを使うために、ユーザは ID やパスワード等のアイデンティティを登録して使う必要がある。

システム管理者はアイデンティティの整合性やセキュリティを保つために、煩雑な作業を強いられている。業務 IT アプリケーションの増加により、システム管理者の負担は益々増加している。更に、正社員のみならず、契約社員、協力会社社員、派遣社員、アルバイト、パートタイマーなど雇用形態が多岐に亘ってきており、システム毎のアイデンティティ運用管理は益々複雑になってきている。大学においても多量の入学・卒業だけでなく、留年・退学・休学・復学・編入などの処理や、一般社会人に対するオープンカレッジの開放、地域住民への業務 IT アプリケーションの開放（図書館システムなど）と、企業同様の処理に追われているのが事実である。現状、大多数の組織は、「人手」に頼り、アプリケーションの増加に四苦八苦している。その結果、「人手」に頼ったアイデンティティの管理は、作業コストの増大、アイデンティティの不整合といった問題を起こしている。

また、このような状況下、システム・セキュリティの問題は看過できないレベルに達している。多岐に亘り、且つ複雑な雇用形態や高い労働流動性の下、組織への出入りが頻繁であるので、正確で迅速なアイデンティティ管理を実施しないと、情報漏洩、情報喪失、情報書き換え、アクセス制限不十分等のセキュリティ問題が起きてしまう。

さらに、企業は新会社法や日本版 SOX 法を遵守する必要があり、早急に対策を実行しなければならない。特に、日本版 SOX 法対応について、下記に詳細する。

2. 求められる機能

アイデンティティ管理には以下の機能が必須である。

(a) **アイデンティティの一元管理機能**

これまで各システムで行っていたアイデンティティ情報のメンテナンス作業（登録、変更、削除）を一箇所で管理する。分散されたアイデンティティ管理はコスト増大になるだけではなく、ゴースト・アカウントを生み出す要因になる。一元管理することで、大幅な管理コスト削減と、退職した社員など本来削除すべきアイデンティティの削除漏れを防ぎ、不正アクセスによる悪用を防止し、セキュリティ・リスク低減を実現する。さらに、システム管理者の負担軽減を実現する。

(b) **承認ワークフロー機能**

アイデンティティの申請、承認/却下、決済を組織のルールに則って実現できる機能である。本承認ワークフロー機能により、システマティックな承認プロセス、煩雑な承認作業の簡略化、アイデンティティの一元管理のフロント・プロセスを実現できる。

(c) **プロビジョニング機能**

アイデンティティにアクセス権（パーミッション）と役割（ロール）を割り当てるポリシー管理機能を提供する。本プロビジョニング機能により、人事異動などで属性情報の変更が生じたアイデンティティに関して、特定の業務 IT アプリケーションに対するアクセス権を自動的に付与または削除することができる。大組織または複雑な組織ほど、本機能は威力を発揮する。

(d) **様々なシステムとの連携（マッピング・ファンクション）**

組織では様々な業務 IT アプリケーション、ミドルウェア、ソフトウェア・プラットフォームを活用しているので、それらとの連携が必要である。アイデンティティ管理プログラムを中心として、入力データ（アイデンティティ属性値）を出力アプリケーションの属性値に変換する。この変換をダイナミックに行うのがマッピング・ファンクションである。このダイナミック・マッピング・ファンクションは一度設定すると、以後は定められたルールでデータ・マッピングするため、システム管理者の負担を大幅に軽減する。下記は典型的出力先アプリケーション例である。

(ア) ActiveDirectory や LDAP との連携

ActiveDirectory や LDAP はそれぞれ Windows、UNIX 系 OS においてディレクトリ・サービスや認証サービスを提供する。ディレクトリ・サービスとは、コンピュータ・ネットワーク上にあるユーザ情報や機器情報などの資源を記憶し、検索しやすくするサービスである。他方、認証サービスとは VPN やメールサーバなど様々なアプリケーションのログイン（認証）に使用される。アイデンティティ管理との連携により、全社的管理の実現の第一歩を踏み出す。

(イ) SSO との連携

シングル・サイン・オン（SSO）とは、ユーザが一度認証を受けるだけで、許可されている全ての業務 IT アプリケーションなどを利用できるようになり、何度も ID とパスワードを入力する手間を省くシステムである。しかし、SSO を使うためには、業務 IT アプリケーションへのアイデンティティをあらかじめ登録しておく必要がある。アイデンティティ管理と連携させることで、ユーザアカウント登録や変更を一元化し、利便性を高めることができる。アイデンティティ管理のプロビジョニング機能を利用することで、SSO の機能が飛躍的に有効になる。

(ウ) RDB との連携

リレーショナル・データベースは様々な業務 IT アプリケーションで使用されている最も一般的なリポジトリである、よって RDB との連携はアイデンティティ管理上、必須である。

(エ) UNIX/Linux アクセス管理ソリューションとの連携

本連携は「誰に対して、何月何日何時何分から何月何日何時何分まで **UNIX/Linux 上の**どの資源にアクセス権を与えるか」を承認するアクセス制限管理を実現する。SOX 法対策に必要な機能である。

(オ) メール・サーバとの連携

PC メール及び携帯電話メール・システムと連携させ、一元的アイデンティティ管理を実現させる。

(カ) その他システムとの連携

多くのアイデンティティ管理ソリューションはグループウェア、人事システム、ERP、CRM、SCM 等との連携（コネクタ）を可能にしている。PKI 認証局と連携させ、新規ユーザアカウント登録時に証明書を発行することも可能である。また、入退出管理システム、社員・職員証発行システム、図書館利用の仮アカウント発行システム、ネットワークの一時利用システム、デー

タセンターでの作業アカウント承認発行システムなどの連携で活用されている。

(e) **パスワード・ポータル**

システムの業務アプリケーションが増加すると、利用するためのパスワードも増加する。パスワードを忘れるユーザも多く出現するのが現実で、パスワードを変更しなければならないケースが増える。アイデンティティ管理のパスワードと各アプリケーションのユーザアカウントのパスワードを一括変更することで、社内システムの円滑な運用を実現する。この機能により、システム管理者の負担を大幅に軽減できる。

(f) **パスワード管理機能**

組織のポリシーにより、システム管理者がパスワード管理をすることも、またユーザ自らにもパスワード管理権限を付与させることもできる。

(g) **バリデーション機能**

各入力項目に対して設定し、ユーザが入力する値が正しいかどうかをチェックする。例えば、半角の数字の入力だけを許可している場合、漢字やアルファベットを入力すると、バリデーション・エラーになり、画面上にエラー内容を出す。チェックする入力値は多岐に亘る。

(h) **ログ機能**

アイデンティティ発行業務がポリシー通りに実施されたかを確認し、保証する。別の言い方をすれば、誰がいつどんなアイデンティティを登録したのか及び誰がいつ誰を承認したのかを把握する。本機能は内部監査のために必須な機能である。

(i) **アイデンティティ情報のレビュー**

アイデンティティの管理は利用者増加や人事異動などの変化に合わせて行われるので、定期的なレビューを実施し、不整合の確認をする機能が必要である。こうすることで、利便性が増し、セキュリティ・リスクも低減できる。

上述した機能の概略図を下記の図１で示す。

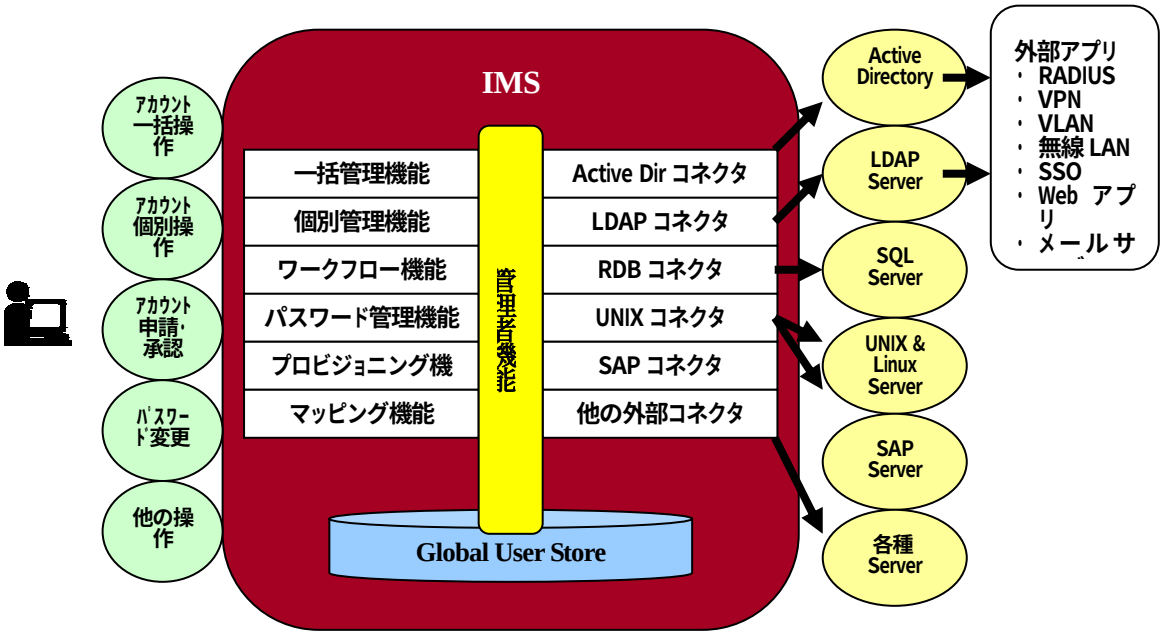

図１　基本システム構成例

3. J-SOX への対応

日本版 SOX 法（金融商品取引法）が 2006 年 6 月 7 日に成立した。日本版 SOX 法は「財務報告に係る内部統制の評価と監査」の制度である。米国では、エンロンやワールドコムによる粉飾決算事件が起こり、上場企業の内部統制が脆弱であると社会が判断し、米国 SOX 法を 2002 年 7 月に成立させた。今まで、日本では監査法人による企業の財務諸表の監査が行われてきたが、決算書の内容結果が正しいかをチェックする監査であった。SOX 法では決算書が作られる過程（プロセス）が適切であるかを企業が証明する必要がある。さらに日本版 SOX 法では、内部統制の基本要素として IT への対応が掲げられている。2008 年 4 月 1 日以降に開始する事業年度から上場企業を中心に内部統制報告書の作成と監査が義務化される。

日本版 SOX 対応の IT 内部統制フレームワーク「COBIT」において、「アイデンティティ管理」も重要なテーマとなっている。COBIT は IT ガバナンスの成熟度を示す。COBIT の中で「DS5：システムセキュリティの保証」で規定されている項目のうち、アイデンティティ管理（アカウント管理）に関連する項目が多数存在する。以下が COBIT におけるアイデンティティ管理関連項目である。IT 業務処理統制において、ユーザの識別、認証、アクセス、そしてアイデンティティの継続管理、アクセス一元管理等が重要になる。申請者が承認者になりすます、未承認でデータベースにアクセスしデータを改ざんしたり、データを盗用したり、退職した者がデータにアクセスしたりすることを不可能にする必要がある。

- **DS5.2 Identification, Authentication, and Access**
  識別、認証、アクセス
- **DS5.4 User account management**
  ユーザアカウント管理
- **DS5.5 Management Review of User Accounts**
  ユーザアカウントの経営監査
- **DS5.9 Central Identification and Access Rights Management**
  ID とアクセス権の中央管理

4. まとめ

上場企業は 2008 年 4 月 1 日には日本版 SOX 法を遵守しなければならない。残された時間は非常に少ない。SOX 法では決算書が作られる過程（プロセス）が適切であるかを問われ、文書化する必要があるので、IT を活用しなければ、高コストになってしまうし、多大な時間を浪費する。IT 活用の中でもアイデンティティ管理は重要である。

但し、アイデンティティ管理は SOX 法があるなしに拘らず、業務アプリケーションを中心とする情報システムの全体的有効活用、低コスト運用、セキュリティ確保等の面で、企業や大学等の組織にとって、必須である。

参考文献

[1] SyncTrust, *http://www.ctech.co.jp/item/synctrust?gad=CP-XzrQBEgieeo9YleAh4hiB2oT-AyDDkLkK*
[2] 日経コンピュータ, 内部統制待ったなし, 2006.3.6, pp40-49
[3] Network Guide, 日本版 SOX 法導入の手引き, 2006,AUTUMN pp.18-27..