基盤技術

内部統制時代の統合ID管理

田中 伸佳・桑田 雅彦

要　旨

企業は情報システムごとに利用者情報の管理を実装してきた結果、直面している問題を解決するために、また、社会的にも法規制としても求められている内部統制強化のために、情報システムや企業秘密情報への厳密なアクセス管理の基になるID情報の管理を統合し厳密化する必要があります。NECは、社内外での豊富な統合ID管理システムの導入経験で苦労したことを生かしたコンサルティングと、自社製品のSECUREMASTERを提供し、統合ID管理システムの整備を効率的に進めることに寄与します。また将来的には、企業がそれぞれの価値を組み合わせて新しい価値を生み出したり、多様な組合せの統合サービスを実現したりできるような統合ID管理基盤をめざします。

キーワード

●内部統制　●統合 ID (アイデンティティ) 管理　● ID 情報のプロビジョニング　●個人認証　●シングルサインオン　●アクセス管理　●アクセス制御　●アクセスログ　●証跡

1. まえがき

企業は業務の効率化や情報の活用のために、様々な業務の情報システム化を次から次へと進めてきました。そのなかでそれぞれのシステムを個別に建て増し的に導入してきた結果、システムごとに利用者情報の管理が実装されており、そのために以下のような問題に企業は直面しています。

① 利用者情報のメンテナンスを多くのシステムすべてに対して繰り返し行わなければならない。

② 1人の利用者に対してシステムごとに異なるIDやパスワードが設定され、利用者の混乱や忘失を招く。その結果、IDとパスワードの管理がずさんになる。

これらの問題を解決するために、システム共通の基盤として、利用者情報の管理を一元化することが必要です。

一方で社会的な背景として、情報漏えい対策、コンプライアンスの徹底、増加する派遣社員/契約社員の統制など、企業の内部統制強化が強く求められています。情報システムの利用を安全にする内部統制強化としては、不正な利用を排除し、情報システムおよび企業秘密情報へのアクセス管理を厳密に行うことが重要です。それには、厳密な利用者の個人認証とアクセス管理の基になる、利用者個人の権限を表すアイデンティティ(以下､IDと略す)情報の管理が基本となります。

法規制としても､2008年4月1日以後に開始する事業年度からの日本版SOX法の適用が近づいています。これは米国SOX法を参考にIT部分の統制を加えて制定されたものですが、米国の監査では多くの企業でID管理やアクセス管理の不備が指摘されました。これら企業は徹底的な改善を余儀なくされ、多くのコストが後で発生しました。日本版SOX法に基づく監査で同じ問題を繰り返さないために､ID管理やアクセス管理の基盤を最初に整備することが重要なのです。

2. 内部統制のコアになる統合ID管理

企業で内部統制強化のために厳密な個人認証とID管理を実現するには、従来のID管理における以下のような問題を解決しなければなりません。

1) 共用IDを利用しているため本人を特定できない。

2) システムごとに利用者を管理しており、1人の利用者がシステムごとに複数のIDとパスワードを持っている。その結果、利用者はIDやパスワードを覚えきれず、紙に書き留めて端末に貼り付けたり、覚えやすい(他人が推測しやすい)パスワードを設定したりしている。

3) システムごとに利用者の属性情報(所属、役職、雇用区分といった権限の基になる情報など)を管理しており、同じ利用者属性情報のシステム間での不整合(たとえば、人事異動の際に、あるシステムでの所属情報の修正漏れが

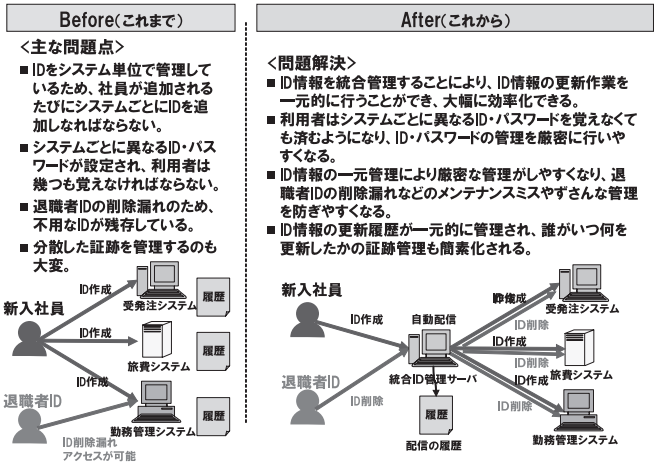

図1　統合ID管理の導入による問題解決

発生する等)が起こる。その結果、利用者のシステム利用権限が正しく設定されず、不正利用を招く。

4) 退職者のIDを即座に削除/無効化できない。

これらの問題を解決するためには、**図1**に示すとおり、システムごとに管理している利用者のID情報(ID・パスワード等の認証情報や属性情報)を一元管理し、どのシステムを利用するときでも、一元管理された個人IDを用いて利用者認証を行わなければなりません。また、IDの生成から削除に至るまでのライフサイクルに沿ってID情報を厳密に管理し、この間の利用者個人に対する権限の付与は必要最小限に絞らなければなりません。なぜなら、必要以上の権限があると、悪用や操作ミスを犯すリスクが高くなるためです。

これを実現するのが統合ID管理システムです。統合ID管理システムを導入し、①すべての利用者個人を漏れなく厳密に管理した上で、②個人IDによる厳密な本人確認と、③必要最小限の情報/システムへのアクセスのみを許可する制御を実施し、④誰が情報/システムのどの部分へいつアクセスしたのかを記録し分析します。それが、企業秘密情報の適正な利用を証明し、監査を受けるために必要です。

3. 導入効果の高い統合ID管理システムに求められる要件

良い統合ID管理システムは、以下の要件を満たします。

a) 利用者個人のID情報を一元管理しやすくするデータベースとデータ参照/更新用GUI

b) 利用者の入社(ID生成)から退職(ID削除)までのライフサイクルに沿った、IDおよびシステム利用権限の登録、変更、削除、停止、再開

c) 利用者個人のIDおよびシステム利用権限を申請・承認するワークフロー処理の効率化

d) 利用者個人のID情報の各システムへのプロビジョニング(各システムの利用者のID情報を、統合ID管理システムで集中管理し、そこから各システムへID情報を配信し同期を取ること)

e) 利用権限に応じた各システムへのシングルサインオン(以下、SSOと略す)およびアクセス制御

f) アクセスログの記録、収集、閲覧、検索、分析、監査

これらの要件を満たす統合ID管理システムを導入することにより、以下の効果が得られます。

①従来システムごとに繰り返し必要だった同じID情報のメンテナンスを一元化でき、管理コストを削減できます。また、メンテナンスミスやずさんな管理を防ぎ、ID情報の精度を高められます。

②利用者の覚えなければならないIDとパスワードが一対に限定され、利用者自身が厳密に保管できます。

③各システムで共通する個人IDの管理やアクセス管理を容易にする基盤を提供することで、IDを統合化するためのシステム開発コストを削減できます。

④利用者および利用権限を登録するとき、管理責任者による確認・承認を確実に実施することが可能となり、管理の厳密化を図れます。

⑤各利用者のシステム利用範囲を管理責任者が承認した必要最小限に制限する管理がしやすくなります。

⑥利用者個人のシステム利用証跡を確実に記録することが可能となり、監査も容易になります。

4. NECが提供する統合ID管理ソリューション

NECでは、グループ従業員15万人を対象に、2000年から他社に先駆け統合ID管理システムの導入・強化を進めてきました。また、50社を超えるお客様の統合ID管理システムの導入実績があります。NECは、これらの豊富な経験から得たノウハウをお客様に提供しています。

また、統合ID管理領域の専門家が、お客様の環境に合った統合ID管理システム導入のコンサルティング、企画、システム提案から、要件定義、設計、構築、運用までをトータルにサポートします。

以下に、NECが提供する統合ID管理ソリューションのうちNECの特徴であるコンサルティングと製品、並びに物理(入退)セキュリティとの連携について紹介します。

4.1 コンサルティング

統合ID管理システムを導入するとき、上流工程である企画、要件定義、基本設計における検討の深さが、システムの導入を成功させられるか否かに大きく影響します。

NECが初めて統合ID管理システムを社内導入したときは、試行錯誤が多く、何度も難しい課題に直面しました。後から分析した結果、上流工程での検討不足が大きな原因だと分かりました。逆に、要件定義と基本設計を入念に行うと、システムの見直しは起こりません。ID管理の統合は、既存システム環境の分析を十分に行い、これを要件定義と基本設計に結び付けなければなりません。豊富な経験が重要な領域です。

システム導入の上流工程での重要な検討事項としては、以下に挙げるようなものがあります。

要件定義として

1)統合ID管理システムの位置づけ・役目の定義

2)ID情報として管理対象とするデータ項目の決定

3)データの利用目的の明確化と利用アプリケーション(業務システム)の想定

4)承認権限と申請・承認フロー

基本設計として

5)個人ID、所属コード、役職コード等の共通コード体系の標準化

6)データの精度を維持するためのデータソース決定とデータ更新業務運用

7)人事システムや人事部門との連携

8)アプリケーション(業務システム)との連携方法

9)セキュリティの確保

このような事項についてお客様の事情や特性に応じた解の検討を効率的に進めます。

4.2 統合ID管理製品

NECは、統合ID管理の導入時に直面する課題をトータルにカバーする統合ID管理製品SECUREMASTERを提供しています。

海外ベンダー製品が多い中で、SECUREMASTERは国産の統合ID管理製品であり、日本企業独特の兼務や階層の深い組織構造を管理できる製品となっています。また、国内の技術サポート部隊が充実しており、タイムリーで柔軟な対応が可能です。

以下に、SECUREMASTERについて紹介します。本製品の構成は**図2**に示すとおりとなっています。

SECUREMASTERは、第3章で挙げた統合ID管理システムの各要件を図2に示した対応関係で実現します。

(1)Enterprise Identity Manager

ID情報管理・プロビジョニング製品です。提供する機能を**図3**に示します。

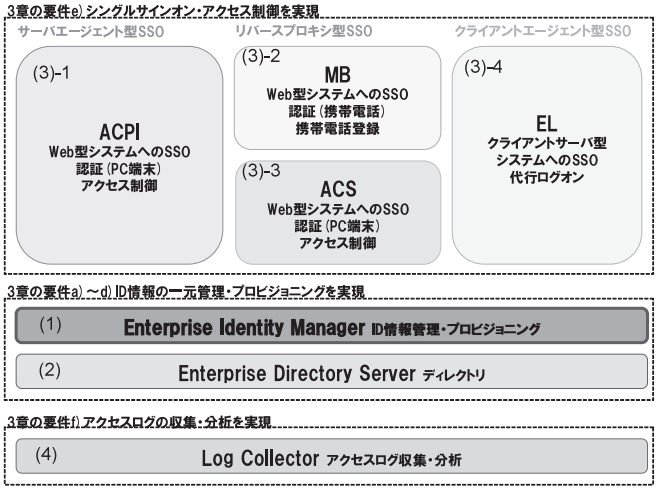

図2　統合ID管理製品SECUREMASTERの構成

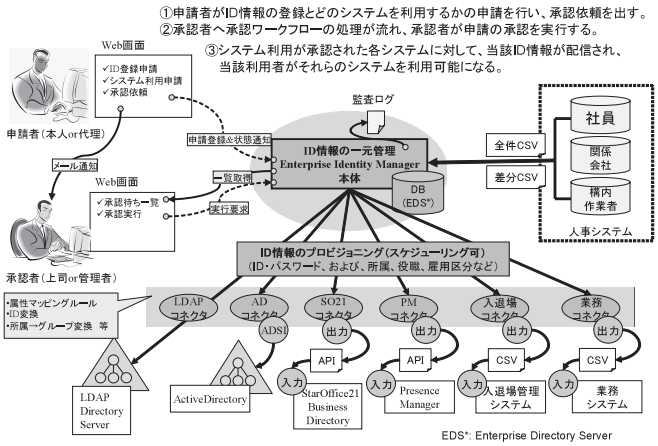

図3　Enterprise Identity Manager 機能概要図

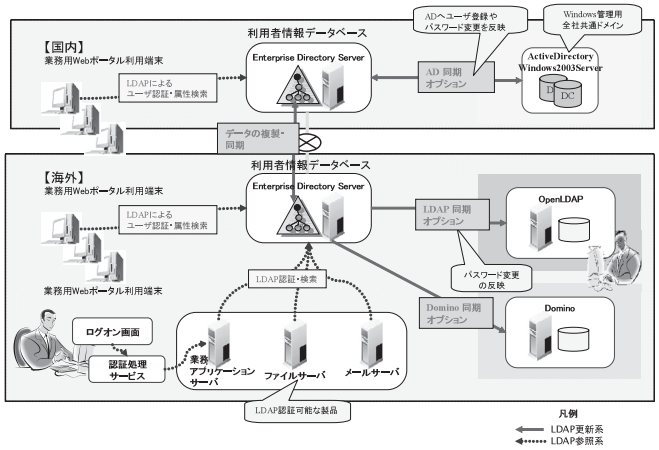

図4　Enterprise Directory Server 機能概要図

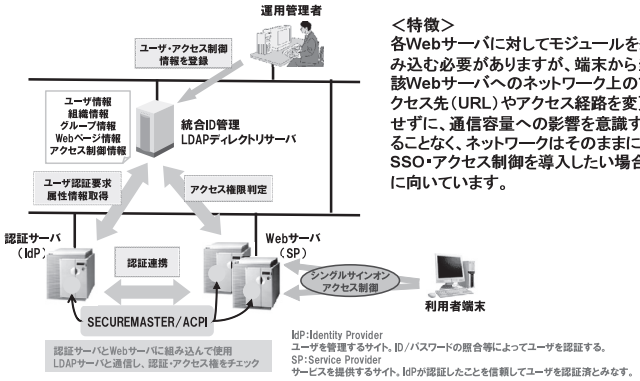

図5　SECUREMASTER/ACPI機能概要図

＜特徴＞
各Webサーバに対してモジュールを組み込む必要がありますが、端末から当該Webサーバへのネットワーク上のアクセス先（URL）やアクセス経路を変更せずに、通信容量への影響を意識することなく、ネットワークはそのままにSSO・アクセス制御を導入したい場合に向いています。

(2)Enterprise Directory Server

LDAP(Lightweight Directory Access Protocol)*ディレクトリサーバ製品です。提供する主な機能は、図4に示すとおりです。統合ID管理システムではID情報を格納するデータベースの役目を担います。

(3)SECUREMASTER/ACPI, MB, ACS, EL

シングルサインオン(SSO)・アクセス制御製品です。ACPI, MB, ACS, ELのそれぞれが提供する機能と位置付けは、図5、図6、図7に示すとおりです。

これらはお客様の利用環境に応じて使い分けたり組み合わせたりすることができます。それぞれどういう場合に向いているかは各図に示すとおりです。

＊LDAPとは、インターネット標準のディレクトリサーバへアクセスするためのプロトコル（通信手順）のことです。

＜特徴＞
端末から当該Webサーバへのネットワーク上のアクセス先（URL）やアクセス経路はリバースプロキシサーバ経由となり、ネットワークの構成や通信容量への影響を意識する必要がありますが、当該Webサーバ側にモジュールを組み込むことなく、当該Webサーバの動作環境に依存せずに、SSO・アクセス制御を導入したい場合に向いています。

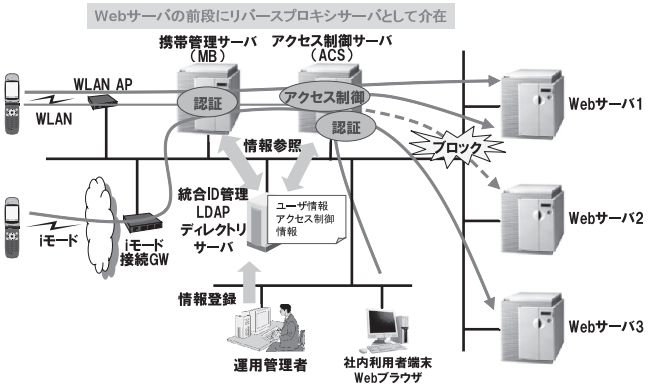

図6　SECUREMASTER/MB,ACS機能概要

＜特徴＞
Web型のSSO・アクセス制御製品のようにURL単位のWebコンテンツへのアクセス制御はできませんが、Web型では対応できないクライアントサーバ型アプリケーション、端末上のスタンドアロン型アプリケーション、メインフレームの端末エミュレータなど、幅広いシステムへのシングルサインオンを導入したい場合に向いています。

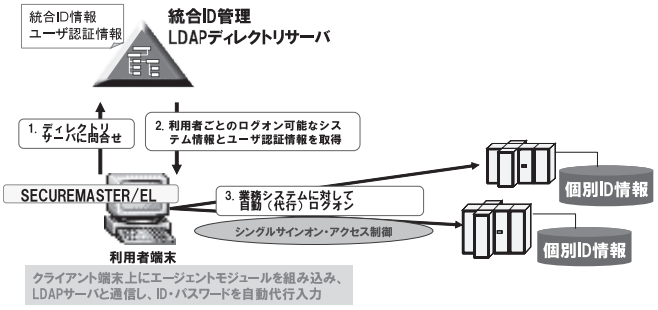

図7　SECUREMASTER/EL機能概要図

(4)LogCollector

ログ収集・分析を支援する製品です。提供する機能は図8に示すとおりです。

統合ID管理システムでは、統合的に管理された個人IDに結び付けられる特定の利用者が、どの情報/システムへのアクセスをいつ行ったのかという、システム利用証跡の記録・監査が重要であり、LogCollectorはそれを容易にします。

4.3　物理(入退)セキュリティとの連携

NECでは、統合ID管理・アクセス管理システムを、オフィスへの入退場管理システムと連携させたソリューションを提供しています。

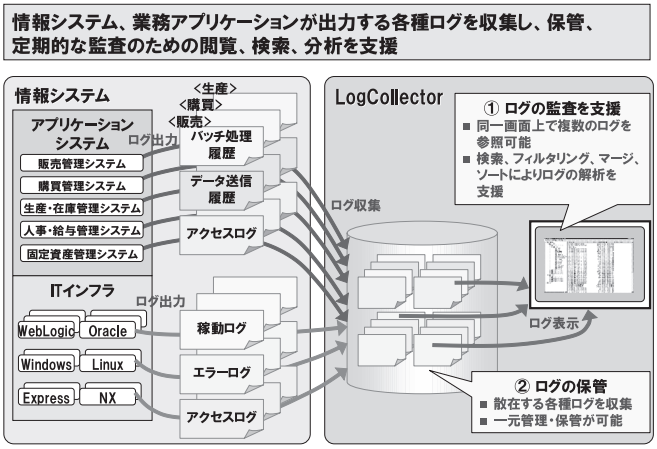

図8　LogCollector機能概要図

両システムを連携させることで、①統合ID管理システムで管理している従業員の社員証（ICカード）による入退場管理システムでの個人認証を実施したり、②従業員の所属、役職、担当業務などにより入退場可能なエリアを制限したり、③入退場管理システムでの認証を通過した従業員でなければ、オフィスのPCの利用やネットワークへの接続ができないように制御したりすることが可能となります。

5. 将来の統合ID管理基盤の活用

統合ID管理基盤の整備は、内部統制強化のために今すぐにも必要ですが、NECはお客様の継続的な事業発展へとつながる統合ID管理基盤の活用を以下のように考えています。

グローバルな厳しい競争の時代を勝ち抜くためには、企業間/サービスプロバイダ間でそれぞれのコアコンピタンスをダイナミックに組み合わせ統合し、総合力のコンピタンスを生み出すことが重要です。

たとえば、ある地方の特産物のインターネットを介した販売が盛り上がりを見せ、それに目を付けた旅行会社がその特産物の販売会社との協業を取り付けたとします。両社はお互いのインターネットサービスである「その地方への旅行プランを提案・販売するサービス」と「特産物を販売するサービス」とを即座に連携させ、利用者(消費者)向けにシングルIDでシングルサインオンによる1つの統合サービスとして提供することができれば、利用者が旅行プランと特産物の組合せに魅力をより大きく感じて両方を併せて購入してくれるチャンスが増えます。つまり、それぞれの市場を統合し、より大きな新しい統合市場へと発展させることを狙えるわけです。

このような企業間/サービスプロバイダ間の情報システム/サービスの連携は、急激に変化するニーズに柔軟に対応し、その時々でダイナミックに相手を変えてタイムリーかつスピーディーに連携できることが重要です。それによって、多様な企業やサービスが柔軟に連携し、それぞれの価値を組み合わせて新しい価値を生み出したり、多様な組合せの統合サービスを実現したりできるからです。

そのためには企業/サービスプロバイダの情報システム/サービスが、不特定の複数の相手と柔軟に連携できるような標準の連携インタフェースを備えるように整備を進めなければなりません。その利用者管理の基盤となっている統合ID管理の整備についても、将来的には、このダイナミックな連携に対応可能なID管理・アクセス管理の実現をめざすことを想定して進めるべきと考えます。

6. むすび

本稿では、統合ID管理システムが果たす役目と具体的な製品SECUREMASTERを紹介し、企業に統合ID管理環境を導入することが、今後求められるITの内部統制強化に役立つことを示しました。また､ID管理を統合するには、要件定義や基本設計の工程が重要と指摘しました。

NECは社内外での豊富な統合ID管理システムの導入で苦労したことを生かして、要件定義や基本設計での深い検討を効率的に進めます。また、自社製品を持つことを生かし、日本企業に合う統合ID管理ソリューションを強化していきます。そして将来的には、多様な企業やサービスがダイナミックに相手を変えて連携し、それぞれの価値を組み合わせて新しい価値を生み出したり、多様な組合せの統合サービスを実現したりできるような統合ID管理基盤をめざしていきます。

NECは、お客様の継続的な事業発展へとつながる統合ID基盤の整備に寄与するために、製品強化やコンサルティングの提供に努めてまいります。

執筆者プロフィール

田中 伸佳
システムソフトウェア事業本部
第一システムソフトウェア事業部
シニアマネージャー

桑田 雅彦
システムソフトウェア事業本部
第一システムソフトウェア事業部
エンジニアリングマネージャー