統合的なID管理に関する考察
－成功するID管理、失敗するID管理－

コンサルティング推進部
コンサルタント・プロフェッショナル

月岡　鉄三

Tetsuzo　Tukioka
tetsuzo-tsukioka@exa-corp.co.jp

企業における内部統制の活動をきっかけに、ここ2、3年で、ID管理の導入が活発化してきた。しかしながら、まだID管理に関する事例や導入関連の情報が少ないこと、およびパッケージ製品の情報が先行していることにより、企業が求めるID管理の姿と、実際に作られるID管理システムに大きな乖離が生じるケースが多い。その結果、ID管理システムの構築において、難航、または暗礁に乗り上げる事例が増えている。

今回、技術的な視点、および業務的な視点で、さまざまな構成要素を整理し、ID管理の構成を多角的に体系化するとともに、多くの事例を通して得られた成功のポイントをベストプラクティスとしてまとめ、考察する。

1. はじめに

Windowsから大型ホスト計算機までさまざまなシステムのユーザIDを一元管理する仕組みは、Identity Management（以下、ID管理と略す）と呼ばれ、ここ2、3年で導入が活発化してきた。

ユーザが、さまざまなシステムにログオンし利用するためのユーザIDを、中央で一元管理するという考え方自体は、以前から存在し、全社的なディレクトリサーバやRDBによるデータ管理システムなどのような形で実現されてきた。これまでのID管理で重視されてきたのは、中央で保持されるID関連のデータ（ユーザID、パスワード、名前、所属など）、およびその管理方式であった。

ID管理は、これまでもアクセス制御の重要な基本構成要素と考えられていたが、内部統制対応の動きをきっかけに、その重要性は、広く一般に認識されるようになった。

さらに異動や退社時における不適切なID改廃がもたらしたさまざまなセキュリティ事故がマスコミ、メディアを賑わすに至り、世の中のID管理に対する認識や期待は大きく変わってきた。この変化の要因は、企業などが求めるID管理が従来のようにユーザデータに焦点を合わせた単なるID関連のデータの一元管理から、ID管理の業務の一元化と、アクセス制御に関わるデータの一元管理に変わったことである。

しかしながらID管理の検討や導入が活発化するにつれ、ID管理の導入の難しさも徐々に世の中に知られるようになってきた。ID管理の難しさは、導入段階だけでなく、その検討段階から生じている。その理由として、ID管理での達成目標の曖昧さ、多くのシステムの中からID管理の対象システムを絞り込む難しさ、および導入時に解決すべき業務課題や運用課題を明確にすることの難しさなどが挙げられる。また、ID管理の導入段階まで進んだとしても、計画時の想定以上に大きな費用や期間を要する事例や、期待どおりの効果を得られなかったという事例が増えてきている。

当社では、難航するID管理プロジェクトの火消し作業を多数経験してきた。それらを整理し、その問題点と原因を表１に示す。

表１に示す事例やJNSAのID管理に関する解説書[1)]など

表１　ID管理の難航事例における問題と原因

No	導入企業の業種	問題発覚フェーズ	現象	主要原因
1	製造	基本設計	作業が進むほどに、不足事項が発生し、決定事項の不整合が多発し、作業が進まなくなった。	ユーザ情報のソース源（人事データなど）から、対象システムまでの一連の ID 作成、改廃の業務プロセスに不備や不足があった。
2	金融	総合試験	総合試験段階で、テストケースの半分が失敗した。	本来、要件定義や設計で決定すべき事項が決定されないまま業務プロセスが部分的に作られており、一貫した形では業務や運用が成立していなかった。
3	製造	導入後	対象システムの追加が行えなかった。	ID 管理システムが、ある特定システムの管理に特化しており、汎用性や拡張性がなかった。
4	サービス	導入後	ID 管理システムの導入後、ユーザ部門の業務負荷が増えた。	業務イベント（入社、退社など）に連動した一連の業務や運用フローの検討が不足し、大量の異動などの生じる季節変動要素などが盛り込まれていなかった。
5	通信	導入後	ID 管理システムの導入後、運用部門の業務負荷が増えた。	ID 作成後の後続処理の自動化が不足し、手動運用を余儀なくされた。

から、現在、ID管理の導入において、次のような問題が生じていることが分かる。

(1) ID管理導入時、その上流工程（要件定義、基本設計）で、特に問題が生じやすい。

(2) ID管理システムを導入しても、期待どおりの効果が得られない､あるいは逆に業務負荷が上がってしまう。

(3) ID管理の導入作業が難航、かつ予算や期間の大きな変動が生じやすい。

即ち、現在、ID管理の導入において、期待と現実の大きな乖離が生じている。

これらの問題を解決するため、本論文では、技術的視点だけではなく、業務的な視点も入れて、「仕組みとしてのID管理」を考察した。

当社では、既に６年以上にわたり、さまざまな業種の企業にID管理の導入を行い、ID管理におけるアワード受賞など国内有数の実績を積み重ねてきた。その知見を元に、第２章では、ID管理の目的を整理した後、ID管理を定義し、その現状と課題をまとめる。第３章では、多くの事例を通して、ID管理の構成要素を整理し、ID管理の実現におけるベストプラクティスを考察する。そして、第４章では、本論文のまとめとして、最近の動向を踏まえ、ID管理の将来像を述べる。

2. ID管理の現状と課題

ID管理の現状と課題を明確にするため、まずID管理とは何かを整理する。

2.1. ID管理とは

ID管理には、次節以降で述べる共通的な目的と、普遍的な概念、イメージが存在する。

2.1.1. ID管理の目的

ID管理は、表２に示す３つの目的で導入される。

表２に示す１番目の目的である業務効率化は、さらに分解すると「管理者の負荷軽減」、および「ユーザの業務効率化」の２つに分けられる。

ID管理では、管理者の負荷軽減は主要な目的として認知されており、大きくスポットライトが当たるため、ユーザの業務効率化の検討が浅くなる傾向がある。ユーザの業務効率化は、IDが発行されるまでの待ち時間の短縮や、初期パスワードの通知やパスワードのリセット対応などのパスワード管理に関する非効率な業務や運用の解消を図るものである。ユーザの業務効率化は、生産性向上に繋がるため、昨今の投資対効果に対する厳しい状況の中では、特に重要視されるケースが増えてきている。

２番目の目的のセキュリティ強化では、休眠IDや幽霊IDと呼ばれる不要なIDの発生防止やパスワードに関連するさまざまな問題の解決を図るとともに、ID管理の業務の標準化を図り、セキュリティレベルの均一化を図る。ID管理の導入目的や検討のきっかけとして、セキュリティ強化が最も多い。

３番目の目的のコンプライアンスでは、属人化を回避し、全社的な方針やルールに則り、ID管理業務が遂行されるこ

表２　ID管理の目的

No	目的	概要
1	業務効率化	システム毎の個別の ID 管理業務を中央で一元管理することで、ID 管理に関わる業務や運用負荷を軽減する。
2	セキュリティ強化	システム毎にばらばら、あるいは各システムの運用担当者に属人化している ID 管理業務やパスワード関連のポリシーなどを標準化し、セキュリティを向上させる。
3	コンプライアンス	ID の発行申請や承認の記録、ID 発行や削除等の操作の記録、および ID の棚卸しなどを行い、ID 管理業務の正当性を外部に説明できるようにする。

とを目指す。このため、個別システムの視点ではなく、全社的な視点で、ID管理の方針、ルール、およびフローなどを検討し、明確化していく。

2.1.2. ID管理の定義

ID管理とは、企業活動に参加し、離脱するまでのIDのライフサイクルを管理することである。この概念図を図１に示す。

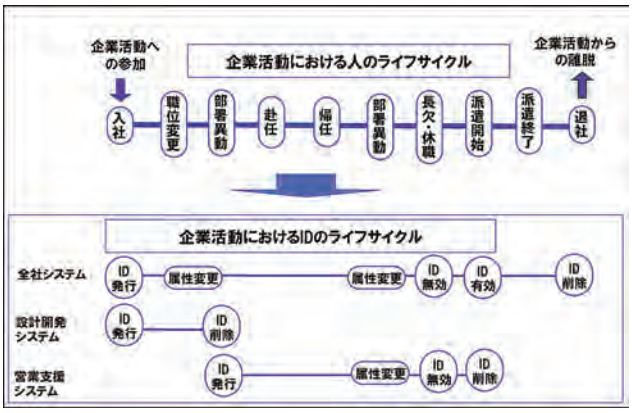

図１　IDのライフサイクルの概念

企業などに入社し、退社するまでの人のライフサイクルは、入社や退社などの業務イベントに連動して、人事システムなどにより一元的に管理されている。同様にIDも、これらの業務イベントと連動し、適切に、そのライフサイクルが管理される必要がある。即ち、ID管理では、業務イベントと連動して、IDの発行や削除、IDの有効化や無効化、および属性情報の変更が行われることが重要である。

図１に示すように、全社員に利用が認められているシステムにおいては、入社という業務イベントが生じれば、自動的に、そのシステムを利用するためのIDが発行され、職位変更や異動などが生じれば、業務上必要なシステムのIDが発行される。そして、最終的には、退社すれば、その人のIDが全システムから削除される。このような仕組みがID管理で実現できなければならない。

2.1.3. ID管理システムのイメージ

ID管理の概念を、入力、処理、出力というIPO（Input/Process/Output）で考えると、入力はユーザ情報を取り込む部分であり、処理は取り込んだユーザ情報を管理し、業務イベントに連動させてID情報を管理する部分であり、出力は対象システムにID情報を配信する部分である。

このID管理のシステム的な概念図を、図２に示す。

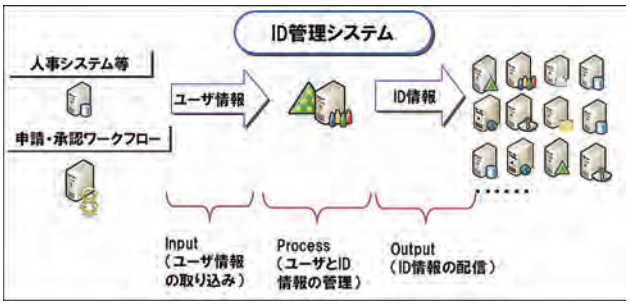

図２　ID管理のシステム概念図

図２に示すInput部分では、通常、多様なユーザ、即ち、社員、派遣社員、グループ会社社員、協力会社社員、アルバイト、パートなどのユーザ情報を対象としている。社員のユーザ情報は、人事システムで管理されているのが一般的である。社員以外のユーザ情報は、通常、人事システム以外のシステム、または申請書などの紙台帳などで管理され、そのIDの発行や削除などは、申請・承認の手続きを経て行われる。したがって、ID管理システムは、人事システムなどの外部システムや、ワークフローシステムと連携しなければならない。

図２に示すProcess部分では、一元管理のために、ユーザ情報とそのユーザのID情報を保持、管理する。ID管理システムとしては、特に、業務イベントと連動して、IDの発行や削除を行うため、保持するユーザ情報内のデータの変化（所属や職位の変化など）を抽出し、必要なIDの発行や削除を行えるような機能を持たなければならない。

図２に示すOutput部分では、ID管理の対象システムに対し、ID情報の配信、即ちIDの発行や削除、およびIDに付随する属性情報（名前、所属、職位など）の作成や変更を行う。

2.2. ID管理の現状と課題

ID管理には、様々な実現方式が存在する。その実現方式の変遷を整理した上で、現状と課題を述べる。

2.2.1. ID管理の現状

ID管理の方式の変遷を図３に示す。

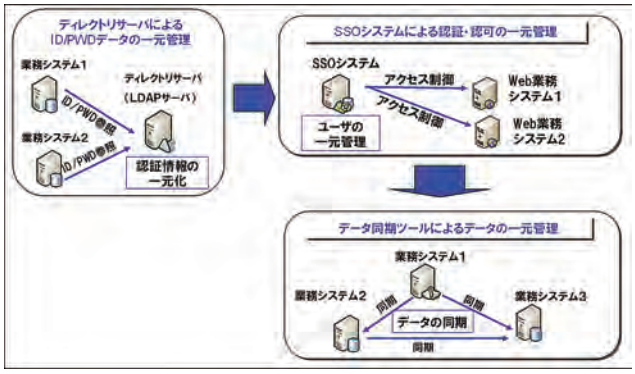

図３　ID管理の方式の変遷

ID管理は、1990年代後半から2000年代初めにかけては、IDとパスワードを中心とした認証情報を、ディレクトリサーバ（LDAPサーバ）上で一元管理する方式が一般的であった。即ち、各業務システムでは、IDとパスワードを保持せず、ディレクトリサーバを参照する形態であった。この方式は、今でも、UNIX/LinuxなどのOSアカウントの一元管理では利用されているが、さまざまな業務システムの多様なID情報まで管理しようとするとディレクトリサーバの肥大化、およびディレクトリサーバの障害が与えるリスクが大きいという問題がある。

2002～2007年において、一時期、Webアプリケーション用のシングルサインオン(SSO)システムを、統合認証基盤と呼び、一元的なユーザ管理基盤であると位置付ける企業も現れた。この場合、SSOシステムをID管理基盤として位置付けていた。ただし、この方式には、対象システムがWebアプリケーションに限定されるという問題があった。

2000年代半ばには、ID、パスワード、および属性情報を、データ同期ツールを用いて、システム間で同期する方式が流行した。しかしながら、この方式は、マスターデータが複数のシステムに分散する傾向があり、障害発生時において分散したデータの復旧が難しく、その利用は広がらなかった。

現在では、図４に示すような機能を持つID管理のパッケージ製品を用いて、ID管理の仕組みを実現することが一般的になった。

その理由は、ID管理のパッケージ製品が、図２のIPOで想定した機能だけでなく、IDの棚卸しなどの豊富な機能を

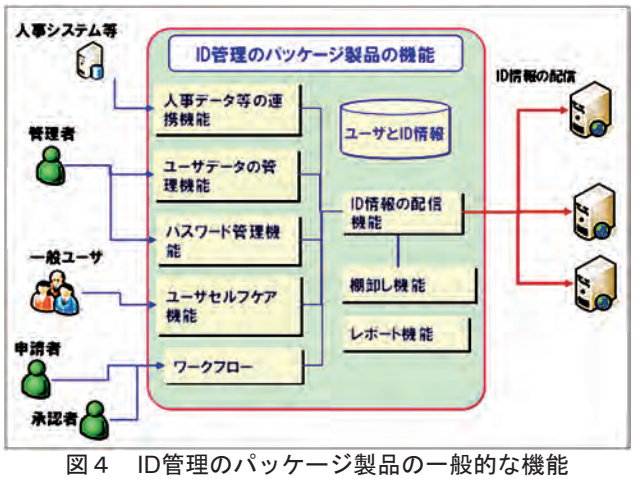

図４　ID管理のパッケージ製品の一般的な機能

有しており、業務効率化の達成などが比較的容易に実現できるためである。

また、ID管理のパッケージ製品は、ID情報の送信を基本アーキテクチャにしているため、ID管理の対象システム側でもID情報を保持することになり、ID管理のシステム側が障害などで停止しても、対象システムには影響を与えないという利点がある。

特に、ID管理のパッケージ製品が脚光を浴びた理由として、さまざまなシステムとオンラインで直接接続するコネクター/アダプターと呼ばれる接続モジュールが豊富に提供されていることが挙げられる。Windowsサーバから大型ホスト計算機までの多様なシステムとの接続モジュールを開発し、対象システムの変更やバージョンアップの都度、開発したモジュールを修正するのは現実的でなく、これら接続モジュールの存在がID管理のパッケージ製品の導入が活発化した大きな要因になっている。

2.2.2. 現状の課題

ID管理における現状の課題は、ID管理用のパッケージ製品が存在するにも関わらず、事例などからも分かるようにID管理の仕組みを作るのが難しいということにある。その理由を分析するにあたり、ID管理の事例を整理しID管理で取り組んだ主要な課題解決事項の一部を下記に列挙する。

・誰に、どういう条件でIDを発行するかの全社的なルールを作る。
・IDの発行、削除、変更に関する標準化されたルールやフローを作る。

・IDの発行、改廃に関する記録を取る。
・多様なユーザの利用を分類、定義し、IDの発行、改廃を制御する。
・誰が利用しているか分からない共有IDの問題を解決する。
・IDの棚卸しを行い、必要以上にIDを発行しないようにする。
・IDの発行、削除、変更に関する申請・承認プロセスの運用が適切に回るようにする。

上記の主要なテーマを見渡して浮かび上がるのは、これらのテーマの解決には、業務視点に立ち、ID管理の業務プロセス（業務方針、業務ルール、業務フローなど）を作ることが必要ということである。

ID管理のパッケージ製品は、IDのライフサイクル管理や対象システムへのID情報配信など、さまざまな機能を提供する。しかしながら、必要な業務プロセス自体は、パッケージ製品では提供されない。

ID管理の仕組み作りが難航するのは、この業務プロセス作りの視点が薄くなり、ID管理のパッケージ製品を導入し、設定すれば、ID管理の仕組みができるという期待が大きいためである。実際には、ID管理の業務プロセスを定義し、その中に、ID管理のパッケージ製品を１つの構成要素として組み込み、かつ定義した業務ロジックをパッケージ製品の中に実装することが必要である。

3. ID管理のフレームワーク

ID管理の構成要素を技術的構成要素と業務的構成要素に分けて整理し、フレームワークとして体系化する。

3.1. ID管理の技術的構成要素

ID管理の技術的構成要素を機能と非機能で体系化し、表３「ID管理の技術的構成要素（機能的視点）」と表４「ID管理の技術的構成要素（非機能的視点）」に示す。また、事例から得られた知見を元に、各構成要素の課題を考察する。

3.1.1. 機能的構成要素

ID管理は、IDのライフサイクルを管理するという特性から、表３に示すように９個の機能で構成される。

表３　ID管理の技術的構成要素（機能的視点）

No	構成要素（機能）	概要
1	ユーザ管理	・ユーザ情報(人情報)と、ID 情報（ID と ID の属性情報）を管理する機能
2	ライフサイクル管理	・人事・業務イベント（入社、退社など）と連携して、ID の発行（作成)、修正、削除を行う機能
3	パスワード管理	・パスワードの同期、逆同期、リセットなどを行う機能
4	ユーザセルフケア	・パスワード忘れ時のユーザ自身によるリセットなど、ユーザ自身で自分の情報を変更する機能
5	データ取り込み（人事データ連携)	・ユーザ情報を外部システム（人事システム等）から取り込むための機能
6	ワークフロー	・ID の発行、削除等に関する申請・承認を行う機能
7	ID 情報配信	・対象システム上での ID、および ID の属性情報(パスワードなど)の発行、変更、削除を行う機能
8	リポジトリ	・ユーザ情報や ID 情報を保持する機能
9	点検・棚卸し	・リポジトリ内の ID 情報と、対象システム上の ID 情報の照合を行う機能

(1)ユーザ管理

ユーザ管理機能としては、ユーザ情報と、対象システムのID情報を紐付けて管理することが基本になる。ID情報には、名前などの基本情報の他に、パスワードや権限に関する情報も含まれる。ただし、対象システムごとにID情報は異なるので、システムごとに異なる多様なID情報を管理しなければならない。

多くの事例を見ると、ユーザ管理では、ID体系が主要な検討テーマになり、対象システムのID体系を統一するという目標を置く場合がある。しかしながら、対象システムが稼働中の場合も多く、対象システムのID体系の変更が難しいという現実がある。したがって、ID体系の検討では、対象システムを新規と既存に分けて検討し、ID体系の統一を図ろうとする場合、新規システムに対してのみ、新しい体系を適用することがポイントである。

このためユーザ管理機能は、稼働中の対象システムに対しては、既存のID体系に沿ってID情報を管理し、新規の対象システムに対しては、統一的なID体系でID情報を管理することが必要になる。

(2)ライフサイクル管理

ライフサイクル管理は、ユーザ情報の変更を検知して、IDの発行、改廃に関する必要なアクションを行う機能である。このためライフサイクル管理では、業務イベントごとのID発行と改廃操作に関する業務ルールを定義し、そのルールを実装することが求められる。例えば、ユーザ情報の所属という属性の値が「開発部」から「営業部」に変われば、その変更を抽出し、必要なアクションとして「開発部」の業務システムのIDを削除し、代わりに「営業部」の業務システムのIDを発行するなどを行う。

企業における業務イベントの個数は、正社員などのイベントの多いユーザの場合、平均して20～40個程度である（入社、退社、異動、出向、転籍など）。社員以外のユーザ（派遣社員など）の場合は、業務イベントの数が少なく、10個程度である（契約開始、契約完了など）。

入社、退社などの業務イベント自体の名称、種類、内容には、企業間で共通性が見られるが、IDの発行、改廃に関連している業務イベント、およびその業務イベントが生じたときのID発行、改廃の業務ルールは、企業や対象システムで差異が見られる。ID管理のパッケージ製品は、企業や対象システムで異なるさまざまな業務ルールを実装できるように、業務ルールの実装を、パラメータの設定ではなく、プログラミングで行えるようになっている。

(3)パスワード管理

ID管理では、対象システム上のユーザのパスワードを管理する。ID管理システムが対象システム上のパスワードを管理するためのパスワードの送信は、パスワード同期と呼ばれ、図５に示す２つの方式がある。

① パスワード同期方式
ユーザが対象システムのパスワード変更をID管理システム上で行う場合であり、ID管理システムから対象システム側へパスワードを送信する（パスワード同期）。

② パスワード逆同期方式
ユーザが対象システム上でパスワード変更を行う場合であり、対象システム上でのパスワード変更が検知され、対象システム側からID管理システム側へパスワードが送信される（パスワード逆同期）。

図５　パスワードの２つの同期方式

パスワードは、対象システム上で暗号化（ハッシュ化も含む）されていることが多いので、パスワード同期の上記の方式には、次の２つの注意点がある。

① パスワード同期方式の場合
ID管理システムと対象システムをオンラインで接続する場合、対象システム上でのパスワードの保存形式に合わせて送信する。

② パスワード逆同期方式の場合
対象システム上でのパスワード変更を捉え、ID管理システムに送信する必要がある。しかしながら、対象システム上の暗号化方式によってはパスワードの復号が困難なため、パスワード変更を捉えるタイミ

ングは、暗号化されて対象システムのリポジトリに保存される前でなければならない。

(4)ユーザセルフケア

ユーザ数が多い場合、パスワードに関連した問題の１つに、パスワード忘れ対応の管理者負荷が高いことが挙げられる。これは、一般に、ユーザが利用しているシステムの数が多いことと、昨今のセキュリティ強化で、各システムのパスワードポリシーが強化され、パスワード変更の頻度が増えたためである。

この問題を解決するためには、ID管理として、ユーザセルフケア機能、即ちユーザ自身で自分のパスワードをリセットするという機能を実現することが考えられる。ユーザ自身によるパスワードリセットという考え方は、管理者負荷軽減だけでなく、管理者によりパスワードが新たに設定されるまで、対象システムにユーザがログオンできず、ユーザの業務遂行が止まるという事態も避けられ、ユーザの業務効率化に大きく貢献する。

(5)データ取り込み(人事データ連携)

社員のユーザ情報は、人事システム上に存在するのが一般的である。そのためID管理の仕組みとしては、人事データを取り込むことが必要になる。人事情報の取り込みにおいては、人事DBに接続し、直接データを取得することも可能であるが、個人情報保護の観点から、昨今では、人事DBへの接続は許されず、必要な情報のみをCSVファイルで、日次などでもらう方式が一般的である。また、長期の視点に立ち、将来の人事システムなどのリプレースなども視野に入れると、環境変化に強いID管理の仕組みとするためには、人事DBとID管理システムは直結せず、CSVファイルなどによる疎結合接続が最適の方式である。

多くの事例を分析すると、人事データは全件データのケースが多い。したがって、ID管理の仕組みとしては、全件データに関して前回分と今回分の差分処理を行い、差分データを作成する機能がデータ取り込み機能には必要である。

(6)ワークフロー

社員以外のユーザに対するIDの発行については、一般的に人の判断が不可欠である。そのため、社員以外のユーザに対するIDの発行、改廃は、申請・承認のワークフローを経由して行われることが多い。したがって、ID管理の仕組みとしては、IDの発行、改廃のワークフロー機能を有するか、または外部のワークフローの結果を取り込む機能が必要になる。

ID管理に必要なワークフローは、その目的がIDの発行、改廃であるため、一般的なワークフローに比べてシンプルであり、IDの発行対象者のユーザ情報、理由、および発行対象システムに関する情報などを申請する際に取り込めればよい。

(7)ID情報配信

対象システムへのID情報の配信には、次の２つの方式がある。

① 密結合方式
ID管理システムと対象システムをオンラインで接続してID情報を配信する場合を密結合方式と呼ぶ。ID管理システムは、ID情報の作成、削除、および修正を、直接、対象システムのユーザリポジトリ（RDBなどのデータ格納の器）に対して行う。

② 疎結合方式
ID管理システムと対象システムをオンラインで接続せず、ID管理システムから対象システムへのID情報配信をCSVファイルなどで行う場合を疎結合方式と呼ぶ。対象システム上でのID情報の作成、削除、および修正は、ID管理システムから渡されたCSVファイルなどを元に、対象システムによって行われる。

対象システム上のIDの発行、改廃は、どちらの方式でも実現可能だが、密結合方式の場合、対象システム上のID情報を吸い上げることも可能になる。一方、疎結合方式では、対象システムと厳密には接続されていないため、対象システム上のID情報を吸い上げることはできない。

また密結合方式では、ID情報を対象システム側のリポジトリに直接送信するため、対象システムのリポジトリとの接続モジュールが必須になるが、対象システム側ではID情報の受信のための開発作業は一般的に不要である。一方、疎結合方式では、ID情報の受信のために対象システム側ではCSVを読み込む機能の開発が必要になる。

(8)リポジトリ

ユーザ情報やID情報を保持する器(リポジトリ)は、ユーザ情報とID情報を長期的に保持し、さまざまな対象システ

ムのID情報のマスターデータになるため、そのリポジトリは信頼性が高く、可用性やバックアップ・リストアの容易なRDBなどが適している。また、ユーザ情報やID情報は、重要な個人情報を含むケースが多く、高いセキュリティレベルも求められるので、リポジトリとしては、セキュリティ上安全に保持できることも重要である。

(9)点検・棚卸し

ID情報の配信方式が密結合方式の場合、対象システムのID情報を吸い上げることが可能なので、中央のID管理側で保持しているID情報との照合がリアルタイムに可能になる。これは、広くIDの点検、棚卸しとして認識されている。疎結合方式の場合は対象システムのID情報を吸い上げることができないので、ID情報の照合は行えない。

ただし、業務視点で見ると、点検、棚卸しに密結合方式が必須なわけではない。業務プロセスとして、ID情報を中央で管理し、配信する形が取れて、対象システム側でローカルにIDを作成するという運用を排除できれば、中央で管理しているID情報を定期的に点検することで、棚卸しという運用を実現できる。このため、疎結合の形態を採る事例は多い。

ID管理の技術的構成要素を体系化したが、ID管理としては、表３に示す機能的な構成要素を必ずしも全て実現する必要はない。自社のID管理の業務プロセスに合わせて、必要な機能を選択し、実現していくことが重要である。

またID管理のパッケージ製品のみで、これらの機能を全て実現する必要もなく、既存の仕組みやシステムと組み合わせて、ID管理の仕組みを構成することが現実的である。実際の事例を見ても、ワークフローなどは、既存のシステムを利用していることが多い。

3.1.2. 非機能的構成要素

ID管理が仕組みとして企業内で利用されていくためには、表４に示す７個の非機能的な構成要素が重要である。

(1)可用性

ID管理システムの可用性は、ID情報配信の視点では不要な場合が多い。その理由は、次の２点である。

① 対象システム上でID情報が保持されること
ID情報は、ID管理システムから対象システムに配信され、対象システム上で保持される。ID管理システムに障害が生じ、ID情報の配信が行えない場合、対象システムは自システムで保持しているID情報を用いて動作可能である。

② 対象システム上でID情報の作成、改廃が可能なこと
ID管理システムに障害が生じ、ID情報を配信できない状況において、対象システム上で緊急のID発行が必要な場合、定義された例外処理手続きに則り、対象システム上で、直接、ID情報の発行を行うことができる。

表４　ID管理の技術的構成要素（非機能的視点）

No	構成要素（非機能）	概要
1	可用性	対象システムへのID情報の配信やパスワード変更が必要な時に実行できる。
2	拡張性	ユーザの増加や対象システムの追加などの状況の変化に対応できる。
3	堅牢性	ユーザ情報をセキュリティ的に安全に保持できる。
4	保守性	運用管理が容易で、障害時の復旧手段も確立しており、脆弱性が見つかればセキュリティパッチなどで対応可能である。
5	柔軟性	要件の変動に合わせて、機能の追加や修正が可能であり、さらにハードウエアやOSなどの環境の変化にも対応できる。
6	オープン性	製品仕様の開示に懸念がないこと、およびID管理システム自体の寿命やバージョンアップなどを考慮し、稼動プラットフォームの選択肢が多い。
7	多様性	Windowsサーバから大型ホスト計算機までの多種多様なシステムとの接続が可能である。

ID管理システムの可用性は、ID情報の配信ではなく、ユーザの利用形態に依存して、必要性が決まる。例えば、ユーザが、対象システム上ではなく中央のID管理システムでパスワード変更を行う場合、パスワード変更処理の停止は一般に許されないため、ID管理システムには可用性が必要になる。

(2)拡張性

ID管理システムは、一般的に、導入後に対象ユーザや対象システムの追加が生じる“成長していくシステム”である。その特徴を考えると、将来の拡張を念頭に置いて、ID管理システムを構築することが重要である。そのためには、将来のID情報の追加を考慮した設計や、業務プロセスを汎用的に策定していくことが必要である。ID管理の導入において拡張性の視点が欠け、対象システムの追加の際に問題が生じる事例は多い。

(3)堅牢性

ID管理では、ユーザ情報とID情報を、セキュリティ上、安全で強固な形で保護し、保持する必要がある。そのためには、これらの情報が保持されるリポジトリ内のユーザ情報などへのアクセス制御やデータの暗号化などを実施しなければならない。

(4)保守性

ID管理は、企業の根幹を成すIT基盤であり、一度、構築され、利用され始めると、極めて長期に利用される。そのため、保守のしやすさ、長期利用で生じるプラットフォームの変更への対応、およびセキュリティ上の脆弱性が発見された場合のセキュリティパッチ適用の容易さなどが保守の視点で重要になる。

(5)柔軟性

企業活動が、今後もダイナミックに変化していくことは容易に予測できる。したがって、ID管理は、組織構造の変化や雇用形態の変化などに柔軟に対応していかなければならない。そのために必要な機能を追加したり、変更したり、あるいはID管理システム自体もOSやハードウエアを必要に応じて変更可能なことが必要である。

(6)オープン性

ID管理の対象は、多種多様なシステムであるため、接続対象システムに制限があってはならない。またID管理が長期利用される際、稼働プラットフォームの寿命などを考えると、プラットフォームの選択肢が多く、時代に合わせた最適の稼働環境を選択できることが重要である。

(7)多様性

ID管理では、Windowsサーバから大型ホスト計算機まで幅広いシステムが対象になることを考えると、これらの多様なシステムとの接続のしやすさは特に重要である。ID管理のパッケージ製品では、対象システムとの接続用にコネクター/アダプターと呼ばれる接続モジュールが用意されているが、その種類の豊富さや実績などが多様性を確保する上で有効である。

多くの事例から、機能的な視点よりも、非機能的視点が不足し、問題が生じたケースが多い。表１で紹介した難航事例のNo.3などは、拡張性と多様性を欠いた典型的な事例である。

3.2. ID管理の業務的構成要素

ID管理のシステム化で難航する事例の多くでは、上流工程で機能的な視点に重点を置き、要件を決めている。即ち、ID管理のパッケージ製品を採用し、そのパッケージ製品で提供されている機能を、どのように利用するか、そのためにどのような設定を行うかという進め方である。したがって、表４に示したような機能をリストアップし、その機能を利用するユースケースを記述し、パラメータを決めていくというアプローチが多い。

一方、当社が構築し、成功した多くのID管理のシステム化プロジェクトを見ると、業務的な視点に重点を置き、要件を決めている。ID管理における仕組み作りの成功のポイントは、表５に示す業務的構成要素を上流工程で決めることである。この業務的な視点を分類、整理し、体系化したものを表５にID管理の業務的構成要素として示す。これら業務的構成要素を決めるということは、業務プロセスを決めることに他ならない。

多くの事例を元に、表５に示す業務的構成要素の中から、重要な事項を整理し、ID管理のベストプラクティスとして、次に述べる。

表５　ID管理の構成要素（業務的視点）

No	構成要素	概要
1	管理原則	正当性、一意性、一貫性という３つのキーワードを満たす方針やルールを作る。
2	体制と役割	全社的なID管理の業務の体制や役割、責任を明確にする。
3	ライフサイクル管理	人が企業活動に参画し離脱するまでの様々な業務イベント（入社、退社、異動など）に対応したID発行、改廃のプロセスを作る。
4	ユーザ管理	ユーザを分類、定義し、それら多様なユーザのID体系を対象システムと紐付けて管理する。
5	ID情報管理	中央で管理すべきデータと、対象システムで管理すべきデータを明確にし、対象システム毎にIDの属性情報(名前、所属、職位など)を管理する。
6	パスワード管理	ID管理システム、および管理対象システム上でのパスワードを一元的に管理、または同期する。
7	記録・点検・監査	IDの発行、改廃に関する操作記録、およびID発行に関する申請・承認の記録を取り、さらに、中央で管理しているID情報と、管理対象システム上のID情報の照合を行う。
8	利用者の役割・責任	ID情報に関する利用者の役割や責任を明確にする。
9	不測事態対応	ID情報に関する不測事態時（パスワード漏洩など）の対応方針を明確にする。
10	特殊なIDの運用	共有ID、および兼務時などのIDの扱いに関する方針やルールを明確にする。

3.2.1. ID管理の３原則

ID管理の成功は、「正当性」、「一意性」、および「一貫性」の３つが確保できたかで判断できる。「正当性」とは、IDの発行、改廃対象のユーザが、正式、かつ適切に認められた人であることを担保することである。「一意性」とは、全社方針に基づくユーザ分類とID体系の基で、ユーザと、そのユーザが各システムで利用するID情報が一意に対応付けられていることなどを指す。「一貫性」は、さまざまな対象システムに対し、同じ方針、同じルールでIDの発行、改廃が行われることを指す。

3.2.2. ID管理の効率的な実現方法

ID管理の対象システムは、一般的に非常に多い。限られた予算の中で、最初にビックバン的に全てのシステムをID管理の対象にすることは現実的ではない。ID管理では、３原則（正当性、一意性、一貫性）を意識して、全社的な視点でさまざまな方針、ルール、およびフローを作る必要がある。そのため、ID管理を効率的に実現するには、最初は、ID管理のルールやフローが汎用的、標準的になるように整備することに注力し、中核となるID管理システムを作るようにすることが重要である。

最初に、汎用的、標準的な中核となるID管理システムを構築できれば、次に、最初に決めた方針やルール、フローに準拠し、ID管理の対象システムを加えていくというアプローチが取れる。最初に作ったルールやフローなどに汎用性がなければ、ID管理の対象システムを追加するたびに、最初のルールやフローと合わず、ルールやフローの見直しが生じ、ID管理の実現が非効率的になる。

3.2.3. ID管理の対象システムの選択方法

ID管理の事例を見ても、最初の対象システムの選定は難しい。その理由は、ID管理を効率的に実現するための明確な対象システムの選定基準がなく、膨大な対象システムのみが目の前にあるためである。最初に選ぶべき対象システムは、前述したID管理の効率的実現方法を考慮すると、下記の視点で２～３個程度が最もよい。

a. 業務課題の多いシステム
b. ユーザの種類の多いシステム
c. ID管理における業務課題、または運用課題が明確な

システム

a.の「業務課題の多いシステム」を選ぶと、網羅性の高い、汎用的な業務プロセスを確立しやすくなる。将来、ID管理の対象システムを追加する際に、確立済みの業務プロセスに準拠する形を取りやすい。

b.の「ユーザの種類の多いシステム」を選ぶと、IDのライフサイクルを管理する上で、入社、退社、異動などの業務イベントの網羅性が高いID管理の仕組みを構築できる。さらには、ユーザ情報のソース源（人事情報システム、申請・承認システムなど）との連携が広範囲に確立しやすくなる。将来、ID管理の対象システムを追加する際に、新たな業務イベントの追加、および新たなユーザ情報のソース源の整備などが不要または最小限化できる。

c.の「ID管理における業務課題、または運用課題が明確なシステム」は、a.の「業務課題の多いシステム」に含まれるケースも多いが、長年の課題を解決することで、ID管理の導入の効果を周囲に目に見える形にし、ID管理の仕組み作りで、プロジェクトの周辺関係者の協力やプロジェクトそのものを促進しやすくなる。

3.2.4. IDのライフサイクル管理

IDのライフサイクル管理とは、具体的には、図６に示すように、ユーザの種類を定義し、入社、退社、異動などのさまざまな業務イベントと、その発生源を明確にし、ID管理システム上でのID情報の状態、および対象システム上でのID情報の作成、変更、削除を関連付けることである。

対象ユーザの種類として、正社員、派遣社員、グループ企業社員、協力会社社員、パート、アルバイトなどを整理し、それらユーザの種類ごとの業務イベントを整理する。そして、各業務イベントが発生した際、対象システム上でのID情報の状態（作成、修正、削除、有効、無効など）を明確にする。

図６に示すIDのライフサイクルの表を作成する上での重要なポイントは、ユーザの種類ごとに、そのユーザ情報と業務イベントの発生源を明確にすること、および業務イベントに関連した対象システム上でのID作成、改廃操作をパターン化することである。

しかしながら、ID管理のシステム化の現場では、パターン化まで実施しているケースは少ない。なぜなら、パターン化は将来の対象システム追加の際に有効なため、最初のシステム化の際には省略することが可能なこと、およびパターン化の重要性が、まだ広く認識されていないためである。

最初にパターン化しておくことで、将来、対象システムを追加する際、そのシステムが、どのパターンに当てはまるかを判別し、そのパターン用の業務ルールやフローを適用することが可能になり、効率的にシステムを拡張することができるため、パターン化は特に重要である。

3.2.5. ユーザ管理

ユーザ管理では、ID体系の見直しを解決すべき大きな問題として取り上げる場合が多い。ID体系は、多様なユーザ

業務イベントと、その情報の供給源							ID管理	対象システム上のIDの状態		
ユーザ種別		イベント	ユーザ情報の発生源				ID管理システム	ID管理の対象システム		
			人事DB	グループ企業人事DB	非人事系システム	その他		分類1 Aシステム、Bシステム	分類2 Xシステム	分類3 Pシステム、Aシステム
社員	1	入社					新規登録、ID発行	ID作成	ID作成	ID作成
	2	異動					属性変更	属性変更		属性変更
	3	職位変更	職位情報				属性変更			
	4	勤務地変更	事業所情報				属性変更			
	5	出向	出向情報				属性変更、ID無効	ID無効化		ID削除
	6	出向受入					新規登録、ID発行	ID作成		ID作成
	7	出向戻り	出向情報				属性変更、ID有効	ID有効化		ID作成
	8	休職	休職情報				ID無効	ID無効化		ID削除
	9	復職	休職情報				ID有効	ID有効化		ID作成
	10	組織改正	所属情報				属性変更			
	11	改姓	名前情報				属性変更		ID再発行	
	12	業務上理由発生					ID発行	ID作成		ID作成
	13	業務上理由消滅					ID削除	ID削除		ID削除
	14	転籍	退職情報				ユーザ削除	ID削除	ID削除	ID削除
	15	退社	退職情報				ユーザ削除	ID削除	ID削除	ID削除
派遣社員	16	契約開始				契約情報	新規登録、ID発行		ID作成	ID作成
	17	契約終了				契約情報	ユーザ削除		ID削除	ID削除
	18	契約更新				契約情報	属性変更			
	19	派遣部署変更				所属情報	属性変更			

図６　IDのライフサイクル管理（業務イベントとID発行、改廃の関連付け）

と、各対象システムのIDを紐付けて管理するためのルールであり、本質的には定義の問題である。したがって、多くの事例で最終的にはあまり問題になっていない。

むしろユーザ管理における問題は別にある。それはユーザの分類が曖昧な点、およびユーザの種類の変更を考慮できていない点などである。

ユーザの分類として、例えば、社員のID体系を考えた場合、ID管理における社員の範囲が定義しきれていないことが多い。即ち、社員扱いでのID発行の定義が曖昧なことが多い。この原因としては、分社化促進などによる最近の組織形態の多様化があり、以前からのID体系では、そこまで考慮した体系になっていないためである。

また、定年退社後の再雇用、あるいは一旦は関係会社の社員として採用し、試用期間経過後に本社採用にする場合などの雇用方法など、企業の多様化する雇用形態の現状に即してID体系を整理することが重要である。

多くの事例を通して、ID体系の根幹であるユーザ分類のベストプラクティスは、「ユーザの所属組織」と「雇用形態」の２つの軸でユーザを整理することである。

「ユーザの所属組織」とは、本社、グループ会社などを指し、「雇用形態」とは、正社員、派遣社員、他社からの出向社員などを指す。

3.2.6. ID情報管理

ID管理では、通常、ID管理システム上で管理すべき対象システムのデータ（ID情報）を検討するが、これは、各対象システム上で管理するID情報と、中央で管理すべきID情報の境界線を明確にするという問題に言い換えられる。この問題において、多くの事例を見ると、ID情報に含まれる権限データの検討で難航している。

ID管理システムでは、権限を属性情報として管理できる。しかしながら、中央で対象システムの権限を詳細に管理することは、現実的には、対象システム主管部署との権限管理業務の境界を考えると運用的に難しい。また、仮に全ての権限を中央で管理すると決めた場合、実行段階になり、対象システムの権限を全て棚卸しし、ルール化し、中央で管理できるように業務を各システムの主管部署から移行することは、現実の作業としては非常に難しい。

したがって、表６に示すように権限情報をまず分類、整理し、中央で管理する権限を明確にすることが重要になる。

ID情報管理のベストプラクティスは、表６における「共通的属性情報」までを中央で管理することである。即ち、ユーザに関する基本情報と、そのユーザの権限の根拠になる共通的属性情報までを中央で管理し、各システムでの固有の権限となる個別属性情報は、各システムで管理する。

表６　属性情報の分類

No	属性情報の分類	概要
1	基本的属性情報	氏名、ユーザ種別、所属企業活動への参加日、離脱日/離脱予定日などのライフサイクル情報
2	共通的属性情報	アクセス権限に関する共通情報であり、役職、所属、少し細かなレベルの所属組織情報や職位、拠点など
3	個別的属性情報	個別アプリケーションや個別業務のアクセス権限に直結した属性情報

3.2.7. パスワード管理

ID管理においては、下記の４項目をパスワード管理で扱う。

① ID管理システムから、対象システムのパスワードを変更する（パスワード同期）。
② 対象システム上のパスワードを、ID管理システムに反映させる（パスワード逆同期）。
③ ID管理システムから、対象システムの初期パスワードを設定する。
④ ID管理システムで対象システムのパスワードポリシーを管理する。

上記の内、①は一般的にID管理システムの導入において広く実現されており、管理者やユーザが、ID管理システム上でパスワードを変更すれば、対象システムのパスワードが変わる。

②では、ID管理システムが、対象システム上でのパスワード変更を検知し、吸い上げ、他の対象システム上に反映させる。このとき、ID管理製品によっては、④のように、中央で管理しているパスワードポリシーとの整合性をチェックすることも可能である。②を実現することで、例えば、対象システムがWindowsのドメインサーバ（Active Directory）の場合、ユーザには、PC上でのパスワード変更が即座に対象システム全てに反映されるように見える。

①、②、および④がシステム的な検討の色合いが濃いのに対し、③はシステム的な検討だけでは解決できない。その理由は、初期パスワードには、ユーザへの通知が必須であり、通知は業務プロセスとの関係が極めて深いためである。

ID管理の事例では、初期パスワードの通知の仕組み作りで難航するケースが多い。それは、個別システムごとに初期パスワードの通知の仕組みは存在していても、統合された全社的な初期パスワードの通知の仕組みは存在せず、新たに作る必要があるためである。

初期パスワードに関しては、通常、その通知手段が大きな問題になる。多様なユーザに対しての初期パスワードの通知手段としては、メールでの通知や職制を通じての通知など、さまざまな手段が考えられる。

しかしながら、この問題が難しいのは、さまざまな状況や例外を考慮しなければならないためである。例えば、メールシステムのID管理を対象にしている場合、IDが発行されていないのでメールで初期パスワードを通知することができない。社員以外のユーザには、メールのIDが発行されていない場合もある。そして職制を通じての通知も、その職制が病気や出張などで不在の場合など、整理しなければならないさまざまな事象や例外が存在する。

初期パスワード通知のベストプラクティスは、個別に通知しなくてもよい方法を確立することである。その方法としては、例えば、初期パスワードの値そのものではなく、初期パスワードの設定ルールを周知するという方法がある。

3.3. ID管理のフレームワークのまとめ

ID管理は、前述した技術的構成要素と業務的構成要素によって、その仕組みを作ることになる。ID管理のパッケージ製品は、この内、技術的構成要素の中の機能的な部分を提供する。ID管理の仕組み作りが難航するのは、技術的構成要素の中の非機能的な部分と、業務的構成要素が不足するためである。

特に業務的構成要素を不足することなく適切に構成することが、ID管理における成功の最大のポイントである。

4. おわりに

今、導入が活発化しているID管理は、従来のようなID情報の一元管理ではなく、統合的なIDのライフサイクル管理の実現を目指している。

ライフサイクル管理が重視されるようになったのは、内部統制をきっかけに、現実の世界では人のライフサイクル、ITの世界ではIDのライフサイクルを管理することの重要性が広く認識されたためである。

しかしながら、これまでID管理では個別システムごと、即ち個別最適化で業務が作られて来たため、これを全社的、統合的な視点で組立て直すことは容易ではない。そのため、本論文では、技術的視点と業務的視点で多面的に取り組むことの必要性を述べた。

ID管理は、今後も、世の中の動きに合わせて進化していくものと思われる。実際に、ID管理と、認証基盤（SSOシステムなど）は、仕組みとしては一体化されて導入されるケースが増えてきた。また、権限情報にフォーカスし、多数のシステムの権限情報を中央で一元管理する製品も市場で出てきており、ID管理のパッケージ製品との連携や、製品同士が統合される動きも出てきている。

ID管理は、今後、ますます企業活動を支える重要なIT基盤として発展すると考えられる。ID管理の仕組み作りにおいては、本論文で述べたさまざまな体系化した構成要素やベストプラクティスの下で進めることで、企業における現実的で実りの多いIT基盤を効率よく構築できると確信している。

参考文献

1) 日本ネットワークセキュリティ協会,”内部統制におけるアイデンティティ管理解説書（第2版）”,2009
2) 丹羽奈津子、“企業システムにおけるアイデンティティ管理における一考察”、IBM PROVISION No.40, P76-81(2004)
