企業システムにおけるアイデンティティー管理に関する一考察

A Study of Identity Control in Corporate Systems

システムの分散化、Web化の波の中、多くの企業内では複数の認証システムが混在し、運用コストの増加が指摘されている。また、退職者IDの悪用による情報漏えいの報告、個人情報保護法への対応から、セキュリティー・ポリシーをベースとしたアイデンティティー管理の必要性を痛感されているお客様は多い。当論文では、企業システムにおける利用者情報であるアイデンティティー管理のあり方について、セキュリティー基盤強化の観点から論じる。アイデンティティー管理は、情報資産の活用方針・経営戦略・雇用方針からの要件が重要であり、すべてのお客様で共通の解を出すことは困難である。しかしながら、検討のポイント・経緯・考察においては、いまだ事例が少ないことからも、今後同様のシステムを構築するIT技術者の方々の参考となることを確信する。

Amidst the decentralization of systems and the ongoing advance of Web applications, many companies are making use of several authentication systems and reference is frequently being made to the increase in application costs. Having received reports on how information has been leaked and has resulted in the misuse of the identities of retired personnel and through concern over how to respond to the Personal Data Protection Law, there are many customers who have come to feel acutely the need to control their identities on the basis of a security policy. In this paper I take a look at how it is possible to control identity, which is a form of information on users in corporate systems, from the standpoint of strengthening the foundations of security. In the case of identity control, requirements are important from the standpoints of policy involving the use of information resources, management strategy and employment policy, and it is difficult to come up with an identical response which is likely to be applicable to all customers. However, due to the fact that there are still few examples relating to the main points involved in studies, their history and the nature of the studies involved, I feel confident that the ideas that I have ventured to bring forward in this paper will be of interest to IT engineers who wish to construct similar systems in the future.

日本アイ・ビー・エム株式会社 ソフトウェア事業
ソフトウェア・テクニカル・セールス
主任ITアーキテクト
Advisory IT Architect
Software Technical Sales, Software,
IBM Japan, Ltd.

丹羽 奈津子 Natsuko Niwa

[プロフィール]
1990年、日本アイ・ビー・エム入社。分散システムの構築サービス、技術支援をへて、システム管理／セキュリティー分野の技術支援を行う。現在はソフトウェアITアーキテクトとして製造／保険のお客様を担当。

1. はじめに

ホスト集中から分散システムへの変革、Web化の流れの中、企業システムにおいては複数の認証システムが混在する環境が多く見られるようになった。日本アイ・ビー・エムも例外ではない。全社Webアプリケーションについてはインターネット・メール・アドレスにほぼ統一されたが、営業系社員においても、それ以外にWindows® ID、Notes® ID、VTS IDと複数のIDを管理している。さらには、開発部門からの情報提供サイト、事業部サーバーなど、部門管理サーバーの中には、別系統のID付与を行っているケースもある。

また多くのお客様では、事業部再編成、法人統廃合、M&A（Mergers and Acquisitions：企業合併／買収）など、組織構造のダイナミックな変革が進められ、情報資産へのアクセスもこれらの変革に合わせた柔軟な対応が求められている。

一方では、出向・転籍・契約社員など、雇用形態の多様化も進められている。あるお客様では、総務部門を別法人として独立させ、一部社員は新会社へ転籍することになったが、業務内容は従来通りのため、本社社員同様のアクセス権を与えることになった。またあるお客様では、情報子会社へ出向中の本社社員が参加したプロジェクトで、他社からの契約社員がプロジェクト・マネジャーとしてアサインされ、チーム内での情報共有の範囲をどう定義するか、ガイドに苦慮されることとなった。この状況を「戸籍と座席」と表現されたお客様がいる。ここでいう「戸籍」とは正社員・契約社員・出向社員などの雇用種別を、「座席」は業務内容を指す。従来型の雇用形態では、アクセス権は「戸籍」によってコントロールされていた。しかし、先の2例に見られるように、現在は必ずしも「座席」が要求する情報資産と「戸籍」が許可するアクセス権が一定ではない。

このように、認証システムが複雑化し、利用者情報、アクセス制御が多様化していく一方で、セキュリティー要件はシビアになっている。一部マスコミでも報道された退職者IDを悪用した情報漏えい、個人情報保護法への対応など、社内ユーザーに関しては性善説を取っていたお客様も、企業責任としてセキュリティー対策を打たざるを得ない状況となった。とはいえ、現在の複雑化したシステムで認証情報のメンテナンスを行うには、多くの運用コストが発生する。

こうした背景の中で、企業システムにおいては、セキュリティー・

ポリシーにのっとったアイデンティティー管理の実装が望まれている。当論文では、ある製造業のお客様において検討が進められているセキュリティー基盤強化プロジェクトを基に、企業システムにおけるアイデンティティー管理のあり方について考察する。今回のケースでは、管理対象ユーザーはイントラネット利用者すべてと定義され、ユーザー数約2万、アクセス先のアプリケーションとしては、Webアプリケーション、SAP R/3、Lotus Notes®など11が対象となった。

2. セキュリティー基盤強化のためのID管理

ここでいうアイデンティティー（ID）は、システムへの認証・認可のためのものを指す。最近では、デジタル証明書・バイオ認証など、ユーザーID／パスワード以外の方式も一部採用されているが、当論文では、ユーザーID／パスワードを前提とし考察を進める。

IDは認証（Authentication）のためのパスワード、認可（Authorization）のための属性情報とともに、LDAP（Lightweight Directory Access Protocol）に代表されるユーザー・レジストリーに登録されている。セキュリティー基盤強化において、アイデンティティー管理実施の要件を以下に3点示す。

（1）退職者／休眠IDの的確な削除

削除されていない退職者ID、あるいは休眠IDは、ハッカーの活動基点となることも少なくない。しかし、部門単位、アプリケーション単位でメンテナンスされているユーザー・レジストリーにおいて、全社的なID管理を徹底することは困難である。全社利用者マスターを整備することで、ID情報の的確な削除が期待される。

（2）セキュリティー・ポリシーにのっとったアクセス管理の徹底

情報資産のアクセス権設定は多様化しており、従来通り、部門コード・雇用形態などで自動的にアクセス権を設定できるアプリケーションだけではない。Need to Knowの原則（情報は必要とする人のみアクセス可能とすべきという情報セキュリティーの原則）に従い、契約社員・出向者が業務上の必要に応じアクセス権を個別申請するケースも特別なことではなくなっている。個別申請によるアクセス権付与・属性情報の変更に応じ、セキュリティー・ポリシーへのチェック機能が働く仕組みが期待される。

（3）利便性向上によるセキュリティー向上

エンド・ユーザーは今や平均五つのIDを持っているといわれている。ID数の増加により、セキュリティー意識の低いユーザーがID／パスワードを机の前に張っていることも少なくない。認証システムでいくらアクセス制限をかけたとしても、これでは意味がない。ID情報をできる限り統一することでユーザーの利便性を向上し、この問題を解決することも、アイデンティティー管理の効果となる。

これらの要件に対し、既存システムを前提に手作業で対応するとなると、莫大（ばくだい）な運用コストが予想される。実現に向けては全社的な基盤検討が必須と考える。

3. アイデンティティー管理検討の実践

3.1. 検討の進め方

アイデンティティー管理基盤の構築に当たっては、以下の四つの要素について検討を進める必要がある。

（1）アイデンティティー情報

利用者マスターに相当する部分を指す。対象となる情報資産、あるいは情報資産活用方針からユーザーを洗い出し、利用者種別を整理することとなる。従来は人事マスターが利用者マスターとなるケースが多かったが、雇用形態の変革、企業間システム共有により、契約社員情報、別法人の人事マスターからの情報ソースの確保が必要となる。複数の情報ソースから利用者種別を整理し、標準的な属性リスト・登録インターフェース・運用ルールを決定する。

（2）認可情報

近年SAML（Security Assertion Markup Language）に代表される標準言語も整備されつつあるが、アクセス権種別についてはアプリケーションによりパターンが大きく異なるため、認可情報の統合は困難である。またアクセス権設定が多様化していることからも、マスター情報としては標準的な属性情報のみ保持し、実際のアクセス権設定・グループ定義はアプリケーション単位で生成する方式が現実的と考える。また個別申請によるアクセス権付与を想定し、認可申請ワークフローを合わせて検討する必要がある。

（3）情報資産

セキュリティー・ポリシーにのっとったアクセス管理を実現するには、情報資産の機密区分、アクセス・ポリシーを定義する必要がある。この基準を基に、利用者マスター上での属性情報変更により、アクセス権を変更・確認することになる。機密区分は全情報資産で共有する基準となるため、詳細なアクセス権はアプリケーション単位で設定すると割り切り、あくまでセキュリティー・ポリシーを実現するためのシンプルな区分が望ましい。表1に検討プロジェクト内で決定された機密区分の例を示す。

（4）認証システム

Webアプリケーションについては、TAM（Tivoli® Access

表1. 情報資産の機密区分例

機密区分	デフォルトのアクセス権設定	個別申請可否
設定なし	利用者全員	個別申請・定期確認対象外
社外秘	社員のみ（含む出向者）	申請ベースで契約社員・転籍者もアクセス可
機密情報	社員かつ管理職以上	申請ベースで一般社員・契約社員・転籍者もアクセス可。定期的な在籍確認・業務内容確認要。
超機密情報	社員かつ上級管理職以上	申請ベースで社員のみアクセス可。定期的な在籍／業務内容確認要。

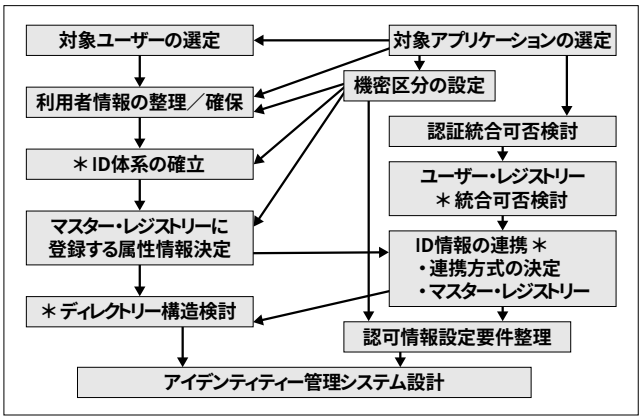

図1. アイデンティティー管理の検討プロセス

Manager for e-business）に代表される統合認証サーバーを使用することも考えられるが、クライアント/サーバー型アプリケーションについては、標準的な統合認証の仕組みは現時点で存在しない。また、TAMによる認証統合においても、パッケージ・ソフトウェアの中には接続不可のケースもあり、現実的には、複数の認証システムを運用せざるを得ない。検討の段階では、認証システムと参照先レジストリーを整理し、認証情報の同期範囲についてアセスする必要がある。

図1に検討プロセスを示す。当論文では、ID管理を主体とするため、＊を付記した四つのステップにつき、次節より論じる。

3.2. ID体系の確立

アイデンティティー管理の大前提として、全社利用者マスターに登録されるID体系の確立が挙げられる。

ID体系の方針を大別すると、米国におけるソーシャル・セキュリティー・ナンバーのように、利用者登録から削除まで一意のIDを使用し続ける方式と、出向・転籍など、所属法人／雇用種別が変更になる都度、異なるIDを付与する方式に分けられる。前者の場合は、所属法人／雇用種別は、IDにひも付けられた属性情報として管理され、後者の場合は、IDの中に所属法人／雇用種別を示す文字を入れることが可能である。いずれを選択するかは、お客様での情報資産利用ポリシー・人事施策によって決定される。

今回のプロジェクトでは、後者を選択することとなった。さらに出向社員には、本来の「戸籍」でのIDと出向先IDの二つを付与し、アクセス先／目的によりユーザー自身に選択させる運用方針を採用した。この方針を選択した理由は、お客様での情報資産の機密区分が所属法人によって異なることにある。出向先の立場で参照可能な情報と元の所属の立場でアクセス可能な情報を、ユーザー自身に分かる形で示すことによって、情報リテラシーを向上させることも目的の一つとなった。検討に当たり、一部の担当者からは、出向・転籍によりIDが変更されるのは労務管理上好ましくないという意見も出された。しかし、プロジェクトの目的がセキュリティー基盤強化であり、複数の立場で業務に携わる可能性がある以上、情報資産へのアクセス範囲をあいまいにするべきではないと判断した。

3.3. ユーザー・レジストリー統合可否

ところLDAPという言葉が過大に期待され、社内のユーザー・レジストリーはLDAP化さえすれば統合できるかのような期待をされたお客様も少なくなかったが、実際にはそのようなことはない。LDAPはその名が示す通り単なるプロトコルにすぎず、複数のアプリケーションが単一のユーザー・レジストリーを参照するためには、参照先レジストリーとしてサポートされるソフトウェアのバージョン含め共通であること、それぞれが参照する情報が競合しないスキーマ設計が可能であることなどの考慮点が存在する。

また、LDAP対応していれば、複数種のサーバーの情報同期が容易に実現できるかといえばそうでもなく、IDS（IBM Directory Server）、Sun ONE Directoryなど、LDAP対応といわれるDirectory同士であっても、情報の同期には、LDIF（LDAP Data Interchange Format）などのファイル経由あるいはIBM Tivoli Directory Integratorなどの同期ツールが必要となる。

複数のアプリケーションが参照するユーザー・レジストリーが共有可能な条件を満たしていた場合、共有すべきだろうか。筆者自身の経験からは共有すべきではないと考える。理由は、構築時点で共有可能であっても、共有構成がその後のアップグレードの阻害要因となりかねないことにある。分散系のアプリケーションでは、サポート・プラットフォーム同様、対応ユーザー・レジストリーのバージョンの幅も狭い。また、アップグレード／パッチ適用によって、スキーマ構造が大きく変更されることもある。実際にTAMとWPS（WebSphere® Portal Server）で共有構成を採ったお客様でも、追加要件によりWPS側のアップグレードが計画された時点で、レジストリーを分割・再設計せざるを得なくなったケースもある。

企業システムにおいては、アプリケーションの継続的な追

加・変更は当然のことであり、各アプリケーションが必要に応じて更改可能であるべきなのは、ビジネス要件からも明らかである。複数のユーザー・レジストリーが存在することを前提に、ID情報の連携による緩やかな結合を目指すのが妥当といえる。

3.4. ID情報の連携

複数のユーザー・レジストリーがある環境で全社ID管理を行うには、ID情報の連携が必要となる。ここでの主な検討項目は以下4点になる。

- レジストリー構成の検討
- マスター・レジストリーの選択
- 連携方式の検討
- 情報同期の範囲

各項目での検討ポイントについて以降に記す。

(1) レジストリー構成の検討

ID情報の連携を検討する際に、レジストリーの構成を考慮する必要がある。図2にあるように、マスター・レジストリーを配し他レジストリーに片方向で認証情報を配信する構成と、各レジストリー間で双方向に情報同期を取る構成の二つが考えられる。情報の一元管理を目的とするのであれば、万一の障害時のロールバックを想定し、マスターからの片方向同期が現実的である。

今回の検討では、ID情報を一元管理することが目的なので、全社利用者マスターをマスター・レジストリーとし、片方向で他レジストリーに情報配信する方式を採用した。

(2) マスター・レジストリー選択基準

マスター・レジストリーは、人事データベースなど情報ソースから情報を取り込み、ID・パスワード・共通属性を保持し、ほかのレジストリーに対しデータを配信するものである。このことから、マスター・レジストリーに求められる機能要件は以下の5点となる。

① 標準的なデータ・インポートのインターフェースを有すること。
② 他レジストリーへのデータ配信のインターフェースを有すること。
③ データ配信の際に使用される通信は暗号化可能であること。
④ レジストリー内に保持される情報が暗号化可能であり、かつ復号方法が提供されていること。
⑤スキーマ構造が柔軟に変更可能であること。

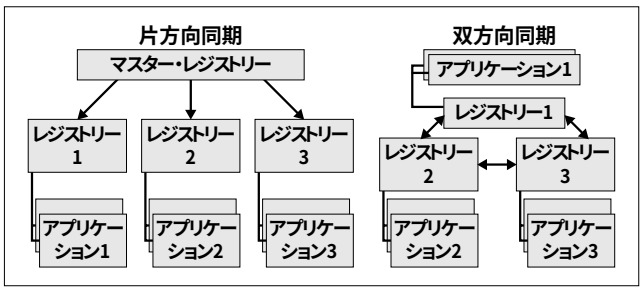

図2. レジストリーの配置

④の観点から不適切なものとして、Active Directory、Lotus Domino®レジストリーなどがある。これらのレジストリーでは、パスワード情報の復号方式が公開されておらず、汎用的なツールでは同種のレジストリー以外でのパスワード情報同期が取れない。そのため製品選定の柔軟性に欠ける点からマスター・レジストリーとしては不適切と考えた。

前述の要件を満たすものとしては、IDSなど、いわゆるLDAPサーバーか、あるいはRDBMS(Relational Database Management System:リレーショナル・データベース管理システム)が挙げられる。ユーザー・レジストリーといえばLDAPサーバーを選択するケースが多いが、筆者は必ずしもLDAPである必要はないと考える。理由は、マスター・レジストリーにおいては、自身のユーザー管理アプリケーション以外に認証で用いられることはないため参照系のパフォーマンス要件は必ずしも高くないこと、また人事異動などの大量データ更新が予想されるため更新系のパフォーマンスが要求されることが挙げられる。一般に、LDAPは更新系の処理に弱く、RDBMS並みの更新パフォーマンス・排他制御機能が備わっていないケースが多い。IDSについても同様であるが、IDSの場合内部的にDB2®を使用していることから、更新処理については、DB2を直接更新することも可能である。今回のケースでは、更新系はDB2のインターフェースを前提とし、ユーザー管理アプリケーションの認証においては、IDSのLDAP機能を使用する方向で検討を進めた。

(3) 連携方式の検討

次に連携方式であるが、技術動向からは以下二つが挙げられる。これらの方式はベンダーによる定義が分かれるところではあるが、当論文では以下の定義とする。

① メタディレクトリー方式

あらかじめマッピングされたロジックを基に、マスター・レジストリーの情報から、他レジストリーに対し情報の同期、あるいは複数のスキーマ情報から属性の生成・変換を行う。IBM Tivoli Directory Integratorに代表される方式。

② プロビジョニング方式

あらかじめ登録されたポリシーに従い、属性情報の変更に従って、必要なリソースの割り振り、アクセス権の付与/削除を行う。また、ID管理アプリケーションとして、アクセス権の申請、在籍確認などのワークフローを組み込むことも可能。Tivoli Identity Managerに代表される方式。

実装の容易性からは①がシンプルではあるが、ポリシーに

従ったメンテナンスを想定すると②の実装が望まれる。今回のケースでは、ユーザー管理ワークフローの構築が要件の一つであったため、②の方式をお勧めすることになった。

(4) 情報同期の範囲

ユーザーの立場でID情報の同期に期待するのは、認証処理を1回で済ませるシングル・サインオン、あるいは認証情報(ID／パスワード)の同期である。とはいえ、アプリケーションによっては、いずれも困難なケースもある。シングル・サインオンについては、3.3節で述べたように、Webアプリケーション以外を対象とするには認証システムを独自開発しない限り困難である。認証情報、特にパスワード同期についても同様で、最も困難な例として、Lotus Notesクライアントを使用したDomino／Notesサーバーを以下に説明する。

Notesクライアントでは、パスワード情報は各クライアント上のIDファイルに格納される。そのためDomino R.5以前では、サーバー上にはパスワード情報が保持されることはなかった。R.6の新機能で、各クライアントのIDファイル内のパスワードをサーバー上のNotesレジストリーにあるインターネット・パスワードとして保持する機能が提供された。しかし、この場合もあくまでマスター情報はIDファイルであり、この機能を使用するためには、インターネット・パスワードはIDファイル以外からは変更できないよう設定する必要がある。では、Dominoレジストリー上のパスワード情報を抽出しマスター・レジストリーにインポートすることは可能だろうか。残念ながらこれも不可である。R.6では、IDファイルから抽出されたパスワード情報はNotesレジストリーに格納される段階で暗号化される。それを復号する方法が公開されていないため、マスター情報としての抽出、他レジストリーへのインポートは不可能となる。

Domino／Notesはある意味特殊例ではあるが、パスワード同期が技術的に不可能であれば、ID情報の連携は無意味だろうか。筆者はそうは考えない。2章で述べたように、セキュリティー基盤強化を目的としたアイデンティティー管理の目的は、以下の3点である。

① 退職者／休眠IDの的確な削除。
② セキュリティー・ポリシーにのっとったリソース・アクセスの徹底。
③ 利便性向上によるセキュリティー向上。

確かに、パスワード同期が不可能なケースでは③の目的は達せられない。しかし、ユーザー・レジストリーへのID追加／削除、属性情報の更新が可能であれば、①、②の要件は十分満たすことができる。このことから、アプリケーションの属性上、パスワードを含めた認証情報の同期ができないケースであっても、ID情報の連携をもってセキュリティー基盤強化といえると判断した。

3.5. ディレクトリー構造の検討

利用者マスターへのデータを登録の前に、ディレクトリー構造を決定する必要がある。

従来のX.500関連のガイドでは、ディレクトリーに組織構造を反映したツリー型が主流であった。しかし、今後の企業動向から考えると、定期的な組織変更・法人統廃合・人事異動のたびにディレクトリー構造を再設計する構造は運用困難であろう。そのため、今回は法人以下には組織階層を作成しないフラットな構造を採用した。図3にディレクトリー構造の比較を示す。

考慮点としては階層構造を採らないことによる参照系処理の検索パフォーマンスへの影響が挙げられる。もちろんアプリケーションによっては、ユーザー・レジストリー検索時に階層構造を前提にするものもあるだろう。しかし、TAM、Lotus Domino、WebSphereを含めそのような検索方式を採用しているものは少なく、今回のプロジェクトで検討対象となったアプリケーションにおいても皆無であった。これらのことから、フラット型構成による問題はないと判断し採用となった。表2に各構成の比較を示す。

フラット型構成では、組織コード・役職などは属性情報として

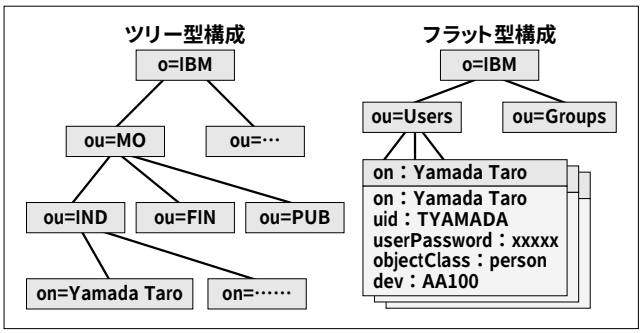

図3. ディレクトリー設計の比較

表2. 情報資産の機密区分例

	ツリー型	フラット型
説　明	X.500のガイドライン通りに、組織構造を反映させた階層を作成し、ディレクトリーを構成する。	法人以下に組織階層を作成せず、全ユーザーをフラットに配置する。組織コード・役職など、必要情報は属性情報として保持する。
長　所	組織構造を反映させているため、組織ベースで参照する際にパフォーマンスが良い。	組織・法人の統廃合時にディレクトリー構造の再設計が不要のため、人事異動・組織変更への対応が容易。
考慮点	大規模な組織異動・法人統廃合があった場合に、ディレクトリー全体の設計変更、大幅なデータ変更が発生する。	アプリケーションから見てキーとなる項目を意識した設計が必須。拡張スキーマの数、キー名を十分に検討する必要がある。
評　価	大学など、大幅な組織変更・属性変更が少ない環境では有効だが、今後の企業動向からは、運用が困難な構成。	大規模な組織変更があり得る環境では、現実的な構成。特に階層化の要件がなければ推奨構成。

保持することになる。今後ツリー型を前提とした検索方式を採用したアプリケーションを使用する際には、これらの情報から、参照用レジストリーを生成することも可能である。

4. おわりに

1～2年前から、お客様より全社ディレクトリーの構築提案のご要望をいただくことが増えてきた。当初はLDAPベースでのディレクトリー設計を期待され、社内に技術者が少ないこともあり試行錯誤を繰り返すばかりだったが、数件のお客様からお話を伺ううちに、これは技術論にはとどまらず、むしろ経営戦略・情報資産活用ポリシーから検討すべき内容ではないかと考え始めた。

当論文で紹介したプロジェクトに参画し、セキュリティー基盤強化のための利用者マスター整備という観点で検討を進めていくと、ベースとなるID情報の整備、情報資産の分類、アクセス権付与ルールなしでは、組織変革、情報資産活用指針の変更に耐える認証／認可基盤の構築はあり得ないことが分かる。そしてこれらのセキュリティー・ポリシーにのっとったID管理の実装は、単純なディレクトリー設計／情報同期ではなく、ポリシー・ベースのプロビジョニングによって実現される。

この分野はまだ立ち上がったばかりで、いずれのベンダーも十分な経験を有しているとは言いがたい。特にID体系の確立、情報資産の整理は、IT技術者よりむしろコンサルタントのスキルが要求される。それだけに、IBMにとっては得意な分野ともいえる。

当論文で示した検討内容は、あくまで一例にすぎず、プロジェクトも今後さまざまな立場の方からのご助言をいただき、実装に向け進めていくことになる。当論文が今後同様の検討に携わる方々の一助となれば幸いである。

[参考文献]
[1] ハリー・B・デマイオ『情報保護マネジメント　管理者のための実践ガイドブック』ダイヤモンド社、ISBN4-478-37137-7、1995年