

アイデンティティ管理システム構築ビジネスの課題とITスキル Issues and IT skills for identity management system's development business

駒井 忍

Shinobu Komai

株式会社ネットマークス コンサルティング部
Consulting Dev., Netmarks Inc.

要旨

本事例研究では、アイデンティティ（ID）管理システムの構築プロジェクトをとおして得られた ID 管理システム構築ビジネスにおける課題とそこで活動する IT 要員の要素や水準（スキルレベル）を明確にする。

また、本プロジェクトのために米国より招聘したインド人 IT アーキテクトの助言により明確になったプロジェクト体制を紹介し、プロジェクト要員の中核となる IT アーキテクトに関してセキュリティの視点を含めた考察を図るとともに、プロジェクトの実施過程で見えてきた ID 管理システム構築ビジネスに対する課題を考察した。

1. はじめに

2000 年以降、セキュリティや個人情報保護法の施行、内部統制などの観点から企業内に乱立したシステムのアクセス権に対する管理の必要性が求められるようになった。

一方で、1990 年代後半から 2000 年にかけて主要 OS にディレクトリサービスが標準機能として実装されたことにより、オープン系のシステムで開発されてきたアプリケーションや情報共有（ファイル）サーバに対してもユーザ認証の統合管理が容易に実装可能となった。

しかしながら、企業内にはレガシーシステムと呼ばれる汎用機や独自に開発されたクライアント / サーバ（C/S）型のシステムが第一線で稼働している。これらを含めて認証を統合するにはシステムの改修が必要になるなどの課題があり困難であることが多い。そこで、様々なシステムに存在する ID の整合性を保ち ID のライフサイクルを管理することにより、セキュリティの担保や監査に耐えうるような運用マネジメントを実現する ID 管理システムの構築が求められるようになった。

ID 管理システムに求められる機能は、ID の一元管理機能、承認ワークフロー機能、プロビジョニング機能や様々なシステムとの連携（マッピング・ファンクション）機能などが考えられる。[1]

しかしながら、私が参加した ID 管理システム構築のプロジェクトにおいて、プロジェクトの体制やそこで活動する IT 要員のスキルが明確でなかったために、要件定義が遅延し、その品質レベルが満たせない状況に陥ったことから、そのプロジェクトの支援のために米国から ID 管理システムに精通した IT アーキテクトを招聘してプロジェクトを終息させた。

本事例では、それらの経験を通して習得した ID 管理システム構築に必要なプロジェクト体制や要員のスキルを紹介し、現状の要員のスキルレベルを分析した上で、今後の ID 管理システム構築ビジネスに対する課題を検討した。

2. ID 管理システム構築ビジネスに必要な要員スキルとプロジェクト体制

本事例では、ID 管理システム構築における企画、現状分析・要件定義、基本・詳細設計、開発・テスト、運用・保守のライフサイクルから、特に顧客の課題やビジネス要求に応えるための企画～現状分析・要件定義フェーズにフォーカスして必要となる要員のスキルを以下のように定義した。なお、要員のスキルの可視化のために、情報処理推進機構（IPA）の IT スキル標準 Ver.2（ITSS）を利用した。[2]

2.1. 企画フェーズ

企画フェーズでは顧客の課題からビジネス要求事項を整理することになる。ここでは、ITSS の職種「コンサルタント」における“提言等を通して顧客のビジネス戦略やビジョンの実現、課題解決に貢献すること”に該当する「コンサルタント」のスキルが要求される。このフェーズにおいては、顧客から RFP（提案要求書）がベンダーに提示され、弊社のようなベンダーからの提案書を比較検討した結果、ベンダー選定が行われ、選定されたベンダーにより現状分析・要件定義以降の作業が実施されることになる。

2.2. 現状調査と要件定義フェーズ

現状調査と要件定義フェーズではまず、既存システムの主管部署における担当者にチェックシートを使用して、ネットワークやプラットフォームの内容とその運用状況、および ID やパスワードの付与ルール等を確認する。次に ID の申請ルールや承認ルートなどの運用を含む現状業務フローを確認しながら要件定義を実施する。要件定義では、ユーザの要求とシステムで実現できることの差を明確にし、双方が納得して“落とし所”を見出す事が重要である。ここでは主に、ITSS の職種「IT アーキテクト」と「IT スペシャリスト」における以下のようなスキルが要求される。

「IT アーキテクト」のスキル

- ・ ビジネス及び IT 上の課題を分析し、ソリューションを構成する情報システム化要件として再構成する。
- ・ ハードウェア、ソフトウェア関連技術を活用し、顧客のビジネス戦略を実現するために情報システム全体の品質を保った IT アーキテクチャを設計する。

「IT スペシャリスト」のスキル

- ・ ハードウェア、ソフトウェア関連の専門技術を活用し、顧客の環境に最適なシステム基盤の設計、構築、導入を実施する。
- ・ 構築したシステム基盤の非機能要件（性能、回復性、可用性など）に責任を持つ。

2.3. セキュリティのスキル

ID 管理システム構築において忘れてはならない大切なポイントがセキュリティである。なぜならば、ユーザからの ID 認証は一般的にはクライアント PC、ネットワーク、対象サーバあるいはアプリケーションへと順次実行され、対象となるデータや情報へのアクセスが許可されることによって可能になる。

そのため、システム全体のセキュリティをバランスよく保つための業務への深い洞察力とセキュリティの実装を前提としたノウハウが重要になる。ここでは、ITSS の職種「IT スペシャリスト」の専門分野「セキュリティ」における“企業内、企業間で必要とされるセキュリティ機能、セキュリティのためのコンポーネントなどの設計、構築及び導入を行う”スキルが要求される。

2.4. プロジェクト体制

本プロジェクトを参考に、標準的な ID 管理システム構築（工数が 30～40 人月規模）における開発体制を想定し、必要な要員のスキルレベルと要員数を当てはめると、図 1 のようになる。なお、プロジェクト体制図におけるコンサルタントやアーキテクトの位置づけは、米国から招聘した IT アーキテクトの支援を受けた結果として導き出したものである。

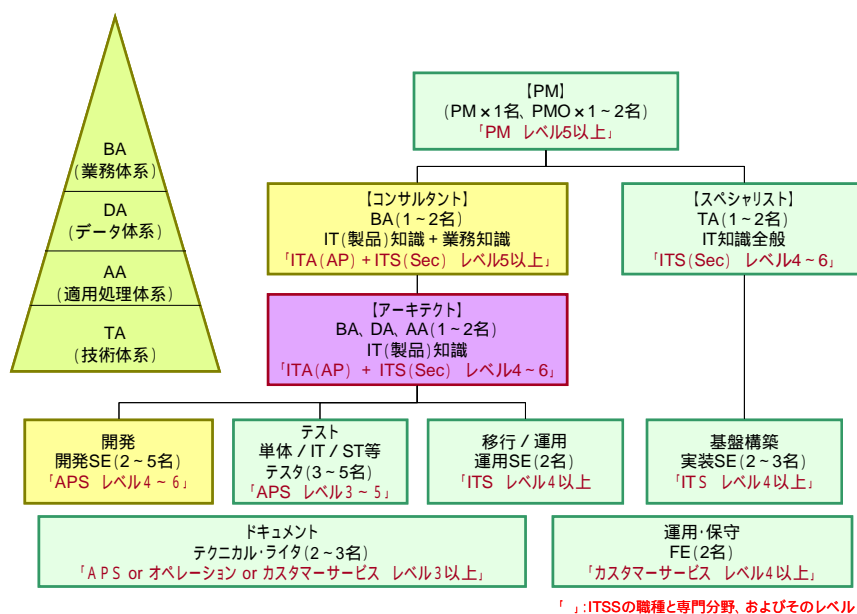


図 1 ID 管理システム構築に必要な体制

3. 要員スキルの測定

要員のスキルの可視化のために、本プロジェクトに関与したメンバーに対して、技術レベル、経験などのヒアリングを行い、ITSS による測定を行った。[2]

ヒアリングではレベルの特定だけではなく、本人の職務経験や取得資格についても経験的観測による話し合いと本人との合意をもってレベルを特定した。

なぜならば、ITSS のキャリア編における達成度指標は、ビジネス貢献の責任性としてプロジェクトのサイズや実施回数といった定量的な項目とプロジェクトの複雑性に関する定性的な項目があるものの、本人がどのような立場で、どのような規模のプロジェクトを、どのように担当したか、といった過去の経験(コンテキスト)を客観的に把握しながら合意形成によるレベル付けを行う必要があると判断した。

また、本事例において米国より招聘したインド人 IT アーキテクトが製品特有の知識(ノウハウ)を保持していることがプロジェクトの成功要因となったこともあり、そのアーキテクトの 1 人にも上記のような IT スキルのヒアリングを実施した。

4. 要員スキルの分析と ID 管理システム構築ビジネスの課題

プロジェクトに係わったエンジニアの IT スキルレベルをまとめると以下の表になる。

表1 エンジニアリング要員別 IT スキル一覧表

職種		ITアーキテクト			プロジェクト マネジメント		ITスペシャリスト					備考
専門分野		アーキテクチャ アプリケーション	アーキテクチャ レイション	アーキテクチャ ストラクチャー	システム 開発	ネット ワーク サービス	プラ ット フォ ーム	シ ス テ ム 管 理	ネ ット ワ ー ク	デ ー タ ベ ー ス	セ キ ユ リ テ ィ	
ハイ レベル	レベル7											
	レベル6	1	1	2	1		2	2	1		1	□ :インド人ITアーキテクトの スキルレベル
	レベル5	1		1		2	2	1	1	1	5	
ミドル レベル	レベル4	1	2	1								
	レベル3											注記)レベル3以上を記載

この表の職種・専門分野における各レベルにある数字“1”、“2”、“5”は該当レベルを満たす数値であり、1名のエンジニアが複数の該当レベルに配置されている。全体的にみてレベル5、6にエンジニアがいることから、かなり高いレベルのエンジニアがこのプロジェクトに参加していたことが伺える。

ただし、IT アーキテクトにおけるレベル6と、IT スペシャリストのセキュリティにおけるレベル6はインド人 IT アーキテクトである。彼は NIT (National Institute of Technology) の出身で大学を卒業後渡米し、ドイツ銀行などのセキュリティ構築プロジェクトを複数案件経験し、その後、本プロジェクトで使用した ID 管理製品パッケージに関連したプロジェクトを経験していることがインタビューで確認できた。

本プロジェクトでは、ID 管理製品の適用を基本にシステム要件定義、開発等を実施したが、顧客との要件のすり合わせのためにプロトタイプを作成しながら要件を固めていく必要があった。

このすり合わせの作業では、製品のソースコードを含むアーキテクチャを理解していない限り、顧客

のビジネス要求に対する“可否判断”ができない状況となった。

図1にある“アーキテクト”とは製品に関して2-3年の開発経験を有するエンジニア（プログラミングを含む）を意味し、支援を受けたITアーキテクトは“テクニカルリード”と表現したが、彼は本製品の開発経験とプログラマー“Java certified programmer”の資格も保有していたことから、そのようなスキルが重要なポイントであることが分かった。

本プロジェクトの開始時点において開発案件であるという認識がなく、そのようなプロジェクト体制を取らなかった（取れなかった）ことがトラブルの主な原因と考えられる。

一般的には、ID管理ビジネスは上場企業における2008年3月までのSOX対応の追い風もあり、IT業界で賄える要員が絶対的に不足している。米国では、SOX対応が一段落したこともあり本プロジェクトの支援に来日したインド人ITアーキテクトのような経験豊富な人材がいることは心強い。

また、米国では設計～開発の1サイクルはID管理システムに精通したベンダーがユーザ（情報システムも含む）と共同で要件定義から開発を行い、それらの過程においてユーザ側にスキルをトランスファーした成功事例があるとのこと。そのユーザは2サイクル目からはユーザ自身の要員で構築し、彼らは支援に回るとのことである。米国におけるユーザ側のプログラミングを含むITアーキテクトに関するスキルの高さは日本とはだいぶ違うようだ。

5. まとめ

本事例のようなID管理製品（パッケージ）の導入においては、製品の生い立ちを見極める必要がある。当該プロジェクトのリサーチのために米国にエンジニアを派遣し、米国での製品導入の状況を把握してからプロジェクトに取り組んだが、製品のアーキテクチャまでを熟知して開発にあたるという準備がなかった。

このような原因で本プロジェクトの要件定義が遅延する中で、製品の供給ベンダーと開発側に多大なリソースを要求するだけで、ユーザ側のビジネス要求がなかなか決まらなかった。支援してくれたITアーキテクトによれば、このようなことは米国ではありえない状況であるとのコメントがあった。

経営課題のためにIT製品を導入する場合、ユーザ側の体制においてビジネス要件に対するオーナーシップが重要であるということに他ならない。

よかった点として、ID管理業務の現状から次期システムを検討する際に業務のプロセスを可視化する必要があったので、経済産業省のEA（Enterprise Architecture）ポータルにあるEAドキュメントを参考にWFA（Work Flow Analysis）と同等のドキュメントを記述したが、ユーザ要件のすり合せに大変有効であった。プロジェクトの期間に余裕があればDFD（Data Flow Diagram）を作成して業務の機能と情報の関係を整理すべきであった。[3]

また、ITSSにあるITスペシャリストのセキュリティに関するスキル定義においてリスク管理の視点での説明や記述がないことから、セキュリティに関する知見をもっと盛り込むべきであろう。前述の経済産業省におけるEA（業務・システム最適化計画）では、セキュリティの観点から業務・システムを検討することを注意点としてはいるものの、米国のFEA（Federal Enterprise Architecture）が提唱しているようなEAとセキュリティの補完関係を明示したガイドラインが必要であると思われる。[4]

我々としては、このような事例を重ねて日本の市場に合うID管理システムの構築、およびID管理のライフサイクルを意識した顧客支援プログラムの検討を今後も継続していきたい。

最後に、本プロジェクトにおいて3ヶ月という短期間でプロジェクトの建て直しを支援しながら、多忙な中をインタビューに快く応じてくれたインド人ITアーキテクトのVikas Tyagi氏に謝辞を述べたい。

参考文献

- [1] 永島秀雄，“アイデンティティ管理”，情報システム学会，2006年
- [2] 情報処理推進機構，“ITスキル標準 Ver.2”，2006年
- [3] 経済産業省，“EAポータル”，2005年
- [4] FEA，“Security and Privacy Profile Phase-1”，2004年