JNSA

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

内部統制におけるアイデンティティ管理WG

宮川　晃一
グローバルセキュリティエキスパート株式会社

2007 年 6 月6日

WGの目的

J-SOX法における「内部統制」の必要性が叫ばれている中で、ITの全般統制として、ITセキュリティに関する対応の必然性が求められています。

その中でも、ID管理（アイデンティティマネージメント）分野については、セキュリティポリシーを実装する上での共通基盤として注目されている分野です。内部統制とアイデンティティ・マネジメントの関連をWG討議の中で紐解き、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を狙って行きたいと考えています。

重点整理テーマとしては、以下の3つを掲げました。

- アイデンティティ・マネジメントの意義
- IT内部統制におけるアイデンティティ・マネジメントの位置づけ
- アイデンティティ・マネジメント導入にかかる導入方針

2006年度の活動

1. ワークショップの開催（4回）

ID管理の定義、SSOとの違いから始まり、現状国内の取り組み状況を意見交換した。
また、メーカー製品に依存しない形で議論をすることとした。

2. WGの開催（3回）

トーマツ監査法人の丸山氏に、ID管理と内部統制の関係を、監査の立場から
説明していただいた。
また、成果物のイメージをまとめた。

3. 分科会の開催

2章分科会　「アイデンティティ管理の意義」

4章分科会　「アイデンティティ管理システム導入指針」

2006年度の活動

トーマツ監査法人の丸山氏のコメント

- 手作業は確実性がないので、ITを活用すればよい。
- コントロールを集約し、ITを利用した統制で確実に、効率的に内部統制の評価ができるように
  - 自動化された”変更コントロール”関連システムの導入も一案
  - “アイデンティティ・マネジメント”関連システムの導入も一案
  - 思い切って委員会報告18号の報告書が入手できる外部委託先にシステムの運用等を委託するのも一案

討議内容と課題

「章立て」

第1章　アイデンティティ管理とは

第2章　アイデンティティ管理の意義

第3章　IT内部統制におけるアイデンティティ管理の位置づけ

第4章　アイデンティティ管理システム導入指針

討議内容と課題

第1章　アイデンティティ管理とは

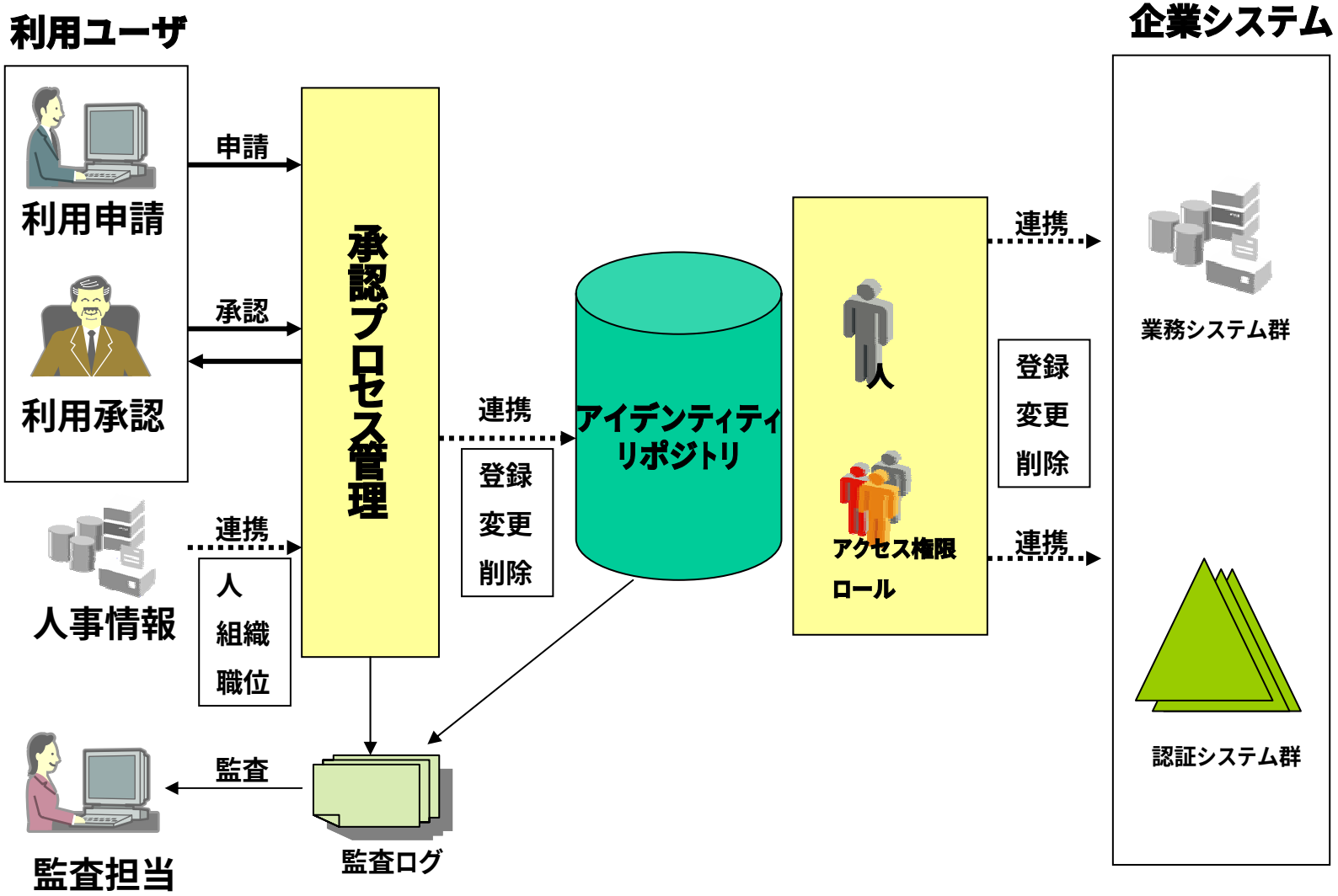
＜討議のポイント＞

- **ーアイデンティティ管理の定義は何か**
- **ーシングルサインオンとの違い**
- **ー認証と認可との関連**
- **ーアイデンティティ管理の発展の歴史**

＜今後の課題＞

- **ー最新動向**
- **ー用語集**

討議内容と課題



討議内容と課題

第2章　アイデンティティ管理の意義

＜討議のポイント＞

- ー事件・事故の事例
- ーアイデンティティ管理の不備によるリスクの洗い出し
- ー業種別によるアイデンティティ管理の必要性のまとめ
  （通信・製造・小売・金融・B2C・公官庁）

＜今後の課題＞

- ー米国SOX法においてのIDM取り組み状況

討議内容と課題

企業に所属するユーザ

協力会社社員 | 出向社員 | 転籍社員 | 他社からの出向社員 | 契約社員 | 正社員

企業経営に関与する組織

取引先 | 関係会社 | 50%以上出資会社 | 100%出資会社 | グループ企業 | 本社

業務プロセス・取引のクラス

B2C	B2B	グループ共有	社内公開	社内機密	運用管理
製品情報 サービス 問い合わせ	発注・購買 生産管理 物流管理	発注・購買 生産管理 物流管理	経費精算 電子メール	財務システム 人事システム 研究開発関連情報	バックアップ・リカバリ パフォーマンス監視 構成管理

討議内容と課題

第3章　IT内部統制におけるアイデンティティ管理の位置づけ

＜討議のポイント＞

- **COBIT4.0J との関連解説 （COBIT for SOX)**
- **ISMS（ISO27001） との関連**

＜今後の課題＞

- **経済産業省のシステム管理基準（追補版）との関連**

討議内容と課題

IT統制目標の対象範囲とCOBIT4．0

主にDS5の対応について解説

IT統制目標の対象領域		COBIT4.0
1.	アプリケーション・ソフトウエアの調達と保守	AI2
2.	技術インフラの調達と保守	AI3
3.	ITプロセス、組織およびその関係性の構築	PO4
4.	ソリューションおよび変更の導入と検収	AI7
5.	変更管理	AI6
6.	サービスレベルの設定と定義	DS1
7.	外注管理	DS2
8.	システム・セキュリティの保証	DS5
9.	構成管理	DS9
10.	障害管理	DS8、DS10
11.	データ管理	DS11
12.	物理環境および運用管理	DS12、DS13

※IT Control Objectives for Sarbanes －Oxley(第2版)から一部修正して転載した

討議内容と課題

第4章　アイデンティティ管理システム導入指針

＜討議のポイント＞

- ープロジェクトの進め方
- ー現状調査項目としてあるもの
- ー問題点分析のポイント
- ー想定効果分析
- ー導入モデルケース
- ーツール選定のポイント
- ー導入にあたっての留意点

＜今後の課題＞

- ー米国での事例や適用状況（特にアクセス権の考え方とログ管理）

討議内容と課題

導入想定効果

導入目的 想定効果	運用コストの低減	セキュリティ レベル向上	認証システムの 標準化	内部統制、監査のための 基盤構築
個別ID管理にかかる運用コストの低減	○			
ヘルプデスク運用コストの低減	○			
エンドユーザの個別IDを運用コスト低減	○			
退職者ID残留による不正アクセスリスクの軽減		○		
ID／PWDメモによる不正アクセスリスクの軽減		○		
パスワードポリシーが非統一による パスワード未変更に関するリスクの軽減		○		
容易かつ適正な認証基盤導入の基礎			○	
認証基盤利用による新規システム 開発コストの低減			○	
内部統制の適正な実施の基礎				○
監査・ロギングの適正に実施の基礎				○
ID申請ルートの明確化によるガバナンスの強化				○

今期の計画

＜2007年度計画（案）＞

6月	：	今年度の活動方針の詳細を決定
6月－　8月	：	成果物レポートの作成
9月	：	成果物のまとめ　（第1版の発行）
10月	：	セミナーの開催
10月－12月	：	第2版に発行の向けてのWG討議
1月－　3月	：	第2版成果物レポート作成