

2009年度 セキュリティにおけるアイデンティティ管理 WG成果報告

グローバルセキュリティエキスパート株式会社

宮川 晃一

標準化部会

2010 年 6 月11日

本WGの目的

セキュリティにおけるアイデンティティ管理WGの目的

ID管理(アイデンティティマネージメント)分野は、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非常に注目されている分野です。
また、最近のクラウド環境利用においても益々重要な要素になっています。

本WGでは、アイデンティティ管理における、様々な課題をWG討議の中で検討し、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を目的に活動しています。

2009年度の活動内容

1. WGの開催(全9回実施)

- 1) 内部統制監査1年目の状況について(トーマツ監査法人 丸山様)
- 2) ロールマネジメント製品のご説明(オラクル様、サンマイクロシステムズ様)
- 3) マイクロソフトクラウドIDソリューション(Geneva)のご説明(マイクロソフト様)
- 4) カンターラ・イニシアチブの活動の紹介(NTT情報流通プラットフォーム研究所様)

2. 「内部統制におけるアイデンティティ管理解説書」(第3版)執筆

以下の3テーマを分科会形式でディスカッションした。

Aチーム: 解説書FAQ作成

Bチーム: アンチパターン(失敗事例)作成

Cチーム: ID管理システムの開発標準作成

＊ ＊ 第3版は6月中に発行予定

Aチーム:FAQ作成の背景・目的と実施方針

以下の背景・目的と実施方針によりFAQを作成

背景

アイデンティティ管理導入促進

目的

①

アイデンティティ管理の導入促進のためのFAQ作成

②

既存の解説書の更なる有効活用

③

幅広く一般的なIDMを意識した情報提供

実現方針

背景・目的・対象者などを明確にし、基本的にユーザ視点での資料を意識する

単なるFAQではなく、IDM導入促進のための資料作成とする

既存の解説書を利用するだけでなく、FAQ内で完結しその補助として解説書を利用する

Aチーム：作成したFAQの例

質問	回答案
内部統制においてアイデンティティ管理の役割りはどのようなものですか？また、どのような機能が必要ですか？	アイデンティティ管理は職務分掌の確立や、個人情報管理ポリシーの適用、経済犯罪や情報漏洩の防止の仕組みの基盤となるものです。 “誰”がどのような処理を行う権限をもつべきか、“誰”が実際に処理を行ったかを個人に結びつけることができ初めて統制は意味を持つからであります。
アイデンティティ管理において、ワークフローは必要でしょうか？	アイデンティティ管理のシステム全体の要求事項により、アイデンティティ管理のワークフローの必要性は異なります。 たとえば、人事データなど一元管理されている情報を元にアイデンティティ管理を導入される場合では、ワークフローを導入する必要はありません。 ワークフローの導入については、場合によっては運用フローが増大し、管理が大変になることもございますので、十分な検討を行ったうえの導入が必要です。
アイデンティティ管理は社内(組織)のすべてのシステムを対象とする必要がありますか。	基本的には、すべてのシステムに対してID管理が必要です。費用対効果やセキュリティのリスクを検討した上でプライオリティ付けを行い、実装のロードマップを策定していくことが必要です。
アイデンティティ管理システムの導入に先立って、調査・準備しておくべき項目は何ですか？	管理する対象となるユーザやシステム、運用管理プロセスに関して、一般的に下記のような項目を調査いただきます。 ・対象ユーザ どの範囲まで管理対象とするか(社員のみ/契約含むなど) 組織体制や職務権限は明確か ソースとなる情報は存在するか ・対象システム どの範囲まで管理対象とするか(基幹系のみ/監査対象システムなど) 各システムとの連携は技術的に可能か ネーミングポリシーやパスワードポリシーは明確か ・運用管理プロセス どのようなオペレーションを想定しているか 承認フローは明確か 監査対応やレポートニングはどうするか

Bチーム: アンチパターンの分類フレーム

アンチパターン記載事項

- ①症状
- ②原因
- ③解決策または
予防策

アンチパターンのパターン分析と構成

パターンの構成(レイアウト)においてMECEを意識して5W1Hで分析。
Whoの視点では大別して発注者側と受注者側の視点単位でそれぞれのアンチパターン进行分类し考察していくこととする

What (何に対して: ID管理基盤構築に対して)

Why (なぜ: 原因) 【アンチパターン】

Who (だれが: どういった立場の人が)

When (いつ: どの工程で)

Where (どこで: どのような業態/業種において)

Why (なぜ: 原因)

How (どうして: どのような仮定で)

「絵にかいたモチ」

「業務知らず」

「製品村八部」

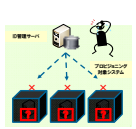
「ブラックボックスプロビジョニング」

「繋がるだろう症候群」

発注者

受注者

Bチーム: アンチパターン紹介

アンチパターン名	アンチパターン概説	ガイドライン参照ポイント
絵にかいたモチ 	IT部門が業務システムの状況を把握することなく、自分(IT部門)本位、かつ、こうあるべきだの理想論でID管理システム導入を進めようとしたため、時間をかけて作り上げたID管理システム構想企画／整備計画は社内合意が得られず、実行に至らなかった。	4.2 企画フェーズ
業務知らず 	IDM施策主管が現場のID管理業務フローを把握しておらず想定で設計したフローをIDサービス実装段階で現場説明を実施するも受け入れられず、結果としてプロビジョニング先システム数が当初想定数より大幅に少なくなった。	4.2 企画フェーズ 4.4 設計フェーズ
製品村八分 	選定済みのIDM製品があるにもかかわらず、IDM製品の仕様を意識した要件定義や概要設計を行わなかったため、ギャップを埋めるための追加作業が発生してしまう現象。	4.5 IDサービス定義 4.6 IDサービス設計(外部設計) 4.7 IDサービス設計(詳細設計)
ブラックボックス プロビジョニング 	事前の調査不足により、プロビジョニング先がブラックボックス化。自動でのプロビジョニングに困難が伴うプロビジョニング先が多発する現象。プロジェクトの大幅遅延や導入効果が出ないなどのトラブルを招く。	4.9.1 プロビジョニング定義 4.10. プロビジョニング設計
繋がるだろう症候群 	IDM製品への過信から、プロビジョニング先のインターフェイス設計/連携方式設計が不十分なまま構築に突入。IDM製品でつながるだろうと思っていた連携が不可であることが判明する現象。工数の増大に直結する。	4.10. プロビジョニング設計

Bチーム：アンチパターンアウトプット

アンチパターン名 「業務知らず」	
アンチパターン概説 IDM施策主管が現場のID管理業務フローを把握しておらず想定で設計したフローをIDサービス実装段階で現場説明を実施するも受け入れられず、結果としてプロビジョニング先システム数が当初想定数より大幅に少なくなった。	
症状例 工程：全体計画策定、IDサービス設計 A社IT部門は全国に拠点を持つ企業であり、SOX法対応としてIDMプロジェクトを立ち上げた。早期にプロジェクトをスタートしたかったこと、現場との壁があったことから十分な調査を実施することなく設計をはじめた。 ID管理業務フローに関しては現場のフローの現状を誰も理解していないこともあって、理想的かつすべてのプロビジョニング先が統一的なフローに従ってID管理を行うような設計とし、現場説明時に業務フロー変更を依頼することとした。 現場説明当日、プロジェクトメンバは淡々と目的、スケジュール、システムの概要等を説明していった。業務フロー変更の説明を始めるやいなや、説明会参加メンバから「急に言われても変えられない」「現場は楽になるのか」「現在のフローのどこが問題でどう変えることによって何が改善されるのか」等の厳しい質問が続いた。現状の分析をしていなかったためにプロジェクトメンバは十分な回答ができず、再度現場の業務フローの現状分析から始めることとなり大幅にプロジェクトが遅延した。	
原因  事前調査不足 ・現場の業務フローを理解 ・各種規定類の事前確認 体制構築およびコミュニケーション不足 ・現場も巻き込んだ体制作り ・プロビジョニング先への協力依頼	
予防策/回避策 関連部署との協力体制を構築し、業務フロー分析・整理は必ず行うこと ID管理業務フローはあるルールに基づいて初期は作られることが多いですがシステムが介在していなければ時間が経過するにつれてフローは変化していき現場独自の運用ルールができてきます。よって本来決められたルールは何か？ それに従ったフローはどうなっているべきか？ 現状の運用とのGAPはあるか？ そのGAPは解消できるものなのか？ 等の観点で分析をするのがよいでしょう。またプロビジョニング先システム毎にフロー統一されているか否かもここで分析し、フローの統一可否に関しても確認します。 このアンチパターンは泥臭い現場の分析を怠ったことによる問題です。とかくIT部門は現場の利用状況を把握しないままプロジェクトを進めてしまいがちです。組織・人に対する調整は労力がかかる仕事ですがIDMは特にさけてはいけないポイントとなります。	
備考/その他 業務分析をスムーズに行うためにも現場を巻き込んだ体制の構築と各種協力依頼を行う必要があります。 ガイドライン参照ポイント 4.2 企画フェーズ 4.2.1 現状分析 4.4 設計フェーズ 4.4.1 IDサービス設計	

■アンチパターン名
アンチパターンが連想できるキャッチーな名前

■アンチパターン概説
アンチパターンの概要

■症状例
アンチパターンが発生している症状を生々しく(読み物的に興味
が引かれるように)

■原因
アンチパターンに陥った原因

■予防策/回避策
アンチパターンに陥らない処方箋

■備考/その他
アンチパターンに間接的に影響を与える事項に関するアドバイス
ガイドラインの参照ポイント

Cチーム：目標と作業コンセプト

目標

解説書の4章（開発標準）をさらに使い易く、効果的な文書にする

作業コンセプト

章立ての再編

開発工程の流れで読んでいけるように章立てを再編する

論点の集約

ID管理に特化した内容のみを記載することとし、一般的なシステム開発でも言える内容は記載しない

テンプレートの追加

コンサル、プレセールス、システム開発などの場面で、使えるテンプレートを追加する

【その他】用語の統一、段落の使い方補正、体裁の整理

Cチーム:全体像、章立ての見直し

工程に合わせて章立てを見直しました。

工程名	章	工程名	章
4.2 企画フェーズ		4.5 実装・テストフェーズ	
プロジェクトの目的	4.2.0	IDサービス実装・テスト	4.5.1
現状分析	4.2.1	プロビジョニング実装・テスト	4.5.2
ID管理システム計画案作成	4.2.2	リポジトリ実装・テスト	4.5.3
ID体系の決定	4.2.3	移行リハーサル	4.5.4
ID管理運用体制・手順作成	4.2.4	4.6 移行	
4.3 要件定義フェーズ		サービスイン	4.6
IDサービス定義	4.3.1	4.7 教育・トレーニング	
プロビジョニング定義	4.3.2	教育・トレーニング	4.7
リポジトリ定義	4.3.3	4.8 評価	
移行の要件定義	4.3.4	評価	4.8
4.4 設計フェーズ			
IDサービス設計	4.4.1		
プロビジョニング設計	4.4.2		
リポジトリ設計	4.4.3		
移行計画の詳細化	4.4.4		

効果1

システム開発に沿った流れにしたことで、読み易くなりました。

効果2

先行タスクと後続タスクの関係性が読み取り易くなりました。

効果3

章内の構成も標準化し、レベルを合わせました。

Cチーム:ID管理に特化した内容に集約

ID管理に特化した内容のみに集約しました

4.2.3 ID 体系の決定

本フェーズでは、ID 体系を決める。これは ID 管理システムによって扱う ID 情報を正規化（標準化）するための作業である。

(1) 目的

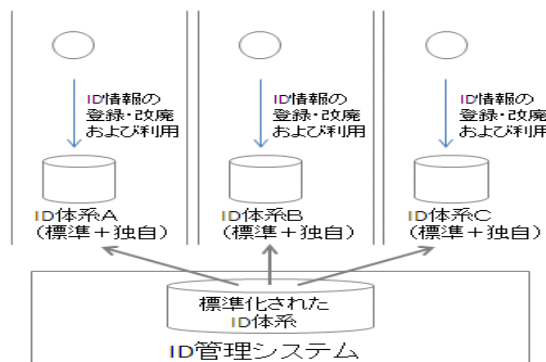
ID 管理システムは、人とシステムを ID によって結びつける仕組みである。そのため、本システムで取り扱う ID の種類と内容を精査して、企業にとって最適な ID の持ち方を定義する必要がある。

追加内容

BEFORE



AFTER



効果1

必要な項目の網羅性が増しました。

効果2

ページ数が減り、とっつき易くなりました。

効果3

論点が絞られ、分かり易くなりました。

削減内容

4.6 サービスイン

本フェーズでは、サービスインを行う作業を行う。

ただし、アイデンティティ管理に特化した内容はないため、通常のシステム開発におけるサービスインと同様に検討することができる。

Cチーム：現場で使えるテンプレートを追加

現場で使えるテンプレートを追加しました。

テンプレート例：状況可視化シート

			システムA			システムB			システムC			調査目的	記述例
利用 者	本 体	正社員											
		嘱託											
		派遣											
		出向者 出向してきた人											
	関 係 会 社	正社員											
		嘱託											
		派遣											
		出向してきた人 本体へ出向した人											
ID命名規約										・移行の可否の判断 ・移行時の影響度合い	・固有のIDを使用 ・社員番号を使用		
ユ ー ザ ID	管 理 フ ロ ー		新規	変更	削除	新規	変更	削除	新規	変更	削除	・IDの管理(追加、変更、削除)を行う際に発生する手順	[トリガー] 申請ベース [作業:新規] 情報システム部 [作業:変更] 自身 [タイミング:変更] 夜間バッチ [タイミング:削除] 退社1週間後
		トリガー											
		作業											
		タイミング											
	認証・管理DB											・ユーザーを認証・管理する際に参照するDB	・独自データベース ・ActiveDirectory ・LDAP
パスワードの管理方法			新規	変更		新規	変更		新規	変更		・新規構築のツールに準拠可能かどうか	[トリガー] 申請ベース [作業:新規] 情報システム部 [作業:変更] 自身 [タイミング:変更] 夜間バッチ
		トリガー											
		作業											
		タイミング											
使用している部門の範囲												・HRから取得する際に絞込みの要不要	・経理部のみ使用
必要項目属性												・HRと連携する属性を判断する	・組織、メール情報が必要
物理的ロケーション												・現在の設置場所に伴い制約が発生するか否か?	・本社に設置
新システムへの融合に伴う調整(システム更改)の可否												・新システムへユーザー管理を移行する際に、システム側で作りこみが発生する可能性がある	・可能 ・不可能
今後のシステム改変の予定												・システムの改変と移行のタイミングを合わせる事の可否	
特記事項												・システム独自ルールなど特記する事項があれば記入	

効果1

活用できるものになりました。

効果2

工数の削減、品質の標準化に繋がります。

効果3

スケジュールの短縮、先行タスクの気づきに繋がります。

2010年度の活動予定

1. 活動テーマ

- 1) ロールマネジメント(アクセス権限管理)をどう考えるか
- 2) 解説書の書籍化検討
- 3) 英文化(ISFとの連携模索)
- 4) カンターラ・イニシアチブの連携(カンターラ講演セミナーなどでの講演など)

2. 活動計画

- | | |
|-------|---------------|
| 6月 | メンバー改編(新規、継続) |
| 7月－3月 | 月1回の定期WGの開催 |
| 随時 | 執筆活動など |

合宿も企画中……

討議風景



謝 辞



本WGにご協力していただいた皆様へ
ご協力いただき、大変ありがとうございました。

No.	会員名称	会社名称
1	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(WGリーダー)
2	柿崎 司	株式会社アクシオ
3	富士榮 尚寛	伊藤忠テクノソリューションズ株式会社
4	中島 浩光	株式会社インフォセック
5	山口 雅史	NRIセキュアテクノロジーズ(Aチームリーダー)
6	駒沢 健	NTTコムウェア(Bチームリーダー)
7	前園 暁子	NTTコムウェア
8	永井 克則	グローバルセキュリティエキスパート株式会社
9	篠原 信之	株式会社シグマクス
10	島 泰三	大日本印刷株式会社
11	西山 まゆみ	TIS株式会社
12	小林 智恵子	東芝ソリューション株式会社
13	丹羽 奈津子	日本IBM株式会社
14	酒井 美香	日本アイ・ビー・エム システムズ・エンジニアリング株式会社
15	北野 晴人	日本オラクル株式会社(特別顧問)
16	澤井 真二	日本オラクル株式会社

順不同
敬称略



謝 辞

No.	会員名称	会社名称
17	大森 潤	日本オラクル株式会社
18	小坂 嘉誉	日本CA株式会社
19	兼岡 禎朗	日本CA株式会社
20	桑田 雅彦	日本電気株式会社
21	外山 英尚	日本電気株式会社
22	竹下 勉	日本電気株式会社
23	中村 有一	日本電気株式会社
24	高木 経夫	株式会社ネットマークス
25	岩竹 智之	株式会社ネットマークス
26	大竹 章裕	株式会社ネットマークス
27	佳山 こうせつ	富士通株式会社(Cチームリーダー)
28	岩田 洋一	富士通株式会社(Cチームリーダー)
29	今堀 秀史	富士通関西中部ネットテック株式会社
30	恵美 玲央奈	株式会社富士通ソーシャルサイエンスラボトリ
31	安納 順一	マイクロソフト株式会社
32	原田 篤史	三菱電機株式会社 情報技術総合研究所

順不同
敬称略



