JNSA

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

2010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

＜標準化部会＞
日本ビジネスシステムズ株式会社
宮川　晃一

2011年 6 月 8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。

2010年度の活動内容

JNSA

1．WGの開催（全9回実施）

テーマ1：「クラウド環境におけるアイデンティティ管理ガイドライン」執筆

・インプレスR＆Dより発売中

http://www.jnsa.org/result/2010/idm_guideline.html

テーマ2： ID管理におけるロールマネジメントとは（中間報告）

1） ロール管理とは何か
2） ID管理におけるロール管理の重要性
3） ロール管理定義における課題
4） ロール定義の検討の進め方

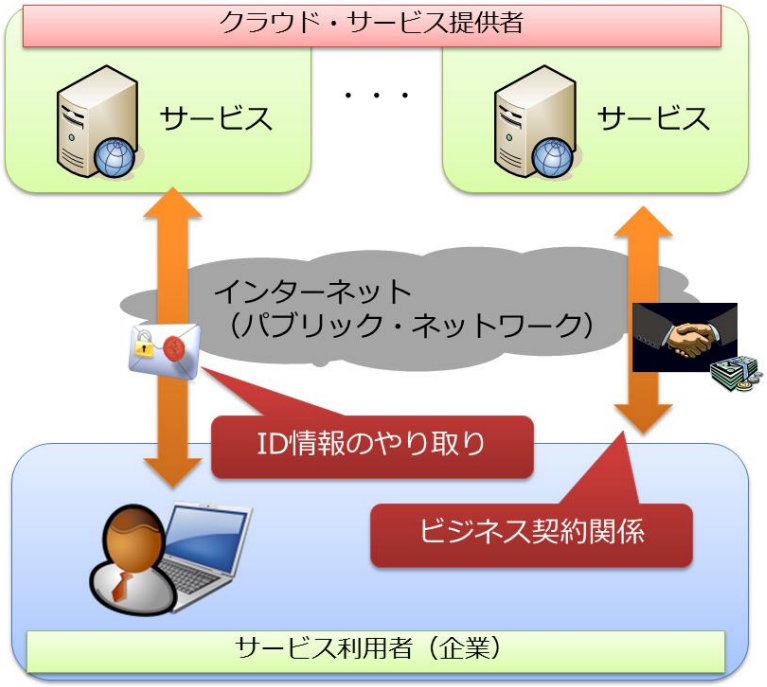
クラウド環境における
アイデンティティ管理ガイドライン
内容紹介

「クラウド環境におけるアイデンティティ管理ガイドライン」

＜目次＞

「クラウド環境におけるアイデンティティ管理ガイドライン」（4章）

- クラウド環境におけるアイデンティティ管理の必要性と課題



クラウド環境の特長

- パブリックなネットワークを介してID情報をやり取りする必要がある
- サービス利用者・提供者との関係にビジネス的な契約関係がある

利用者側の考慮点

- サービス利用時にID情報を安全にやり取りすることができるか？
- 不特定多数からの脅威に対するセキュリティの考慮
- サービス移行などを考慮した汎用的技術の利用
- サービス提供者の信頼性

提供者側の考慮点

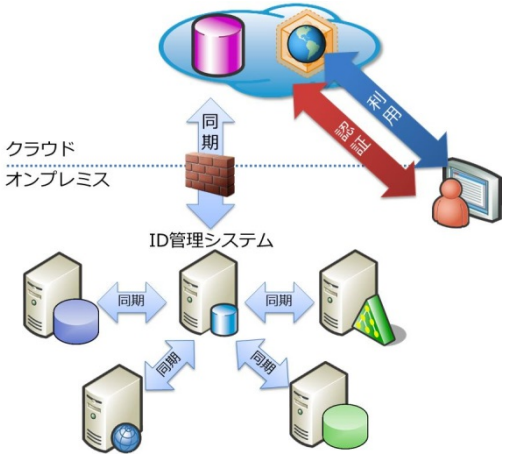
- 主にSaaS型サービスにおいて、他のクラウド・サービスとの間でIDの相互運用性を確保したサービス基盤を保持することができるか？
- ID情報の安全性を利用者にどのように証明することができるか？
- 利用者に割り当てるIDに対してどのような権限を付与するのか？
- サービスの不正利用をどのように検知するのか？または、防ぐか？

「クラウド環境におけるアイデンティティ管理ガイドライン」（4章）

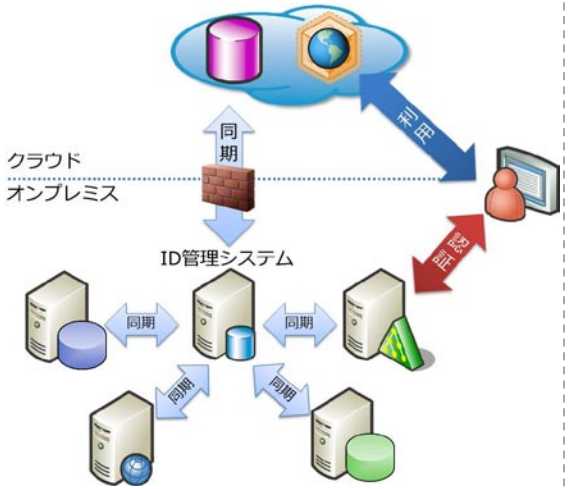
- クラウド環境におけるセキュリティ・ガイドライン
  - CSAガイドラインにおけるアイデンティティ管理の位置づけと推奨事項
    - アイデンティティ・プロビジョニングに関する推奨事項
    - 認証に関する推奨事項
    - ID連携に関する推奨事項
    - 認可とユーザプロファイル管理に関する推奨事項
  - ENISAガイドラインにおけるアイデンティティ管理の位置づけと推奨事項
    - 権限付与、IDの割当、個人データの管理、鍵管理、暗号化、認証、クレデンシャルの危殆化または盗難、クラウド利用者に提供されるID管理およびアクセス管理システム
  - 各ガイドラインにおけるアイデンティティ管理についての考察
    - 「標準仕様への対応」が強調
    - ID連携（フェデレーション）への着目
    - 国内外の標準化推進団体（GICTF etc）

「クラウド環境におけるアイデンティティ管理ガイドライン」（4章）

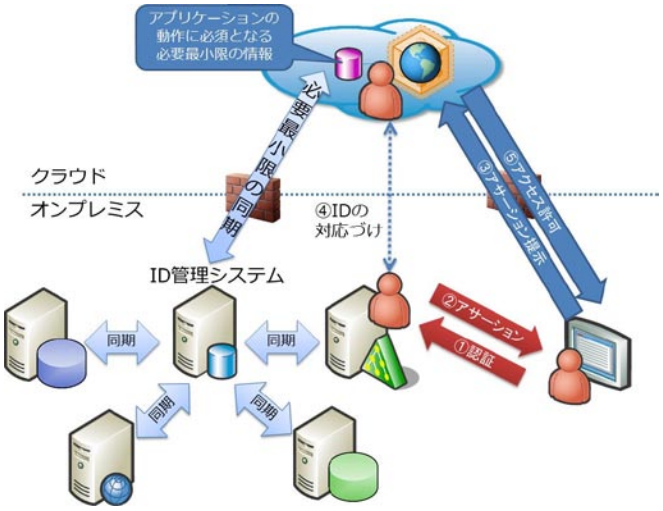
- クラウド環境におけるアイデンティティ管理システム
  - 考えられる実装パターンと利用者側の考慮点への対応



パターンA）
クラウド・サービス側でID情報をすべて格納し管理する



パターンB）
オンプレミスの認証機能を利用する



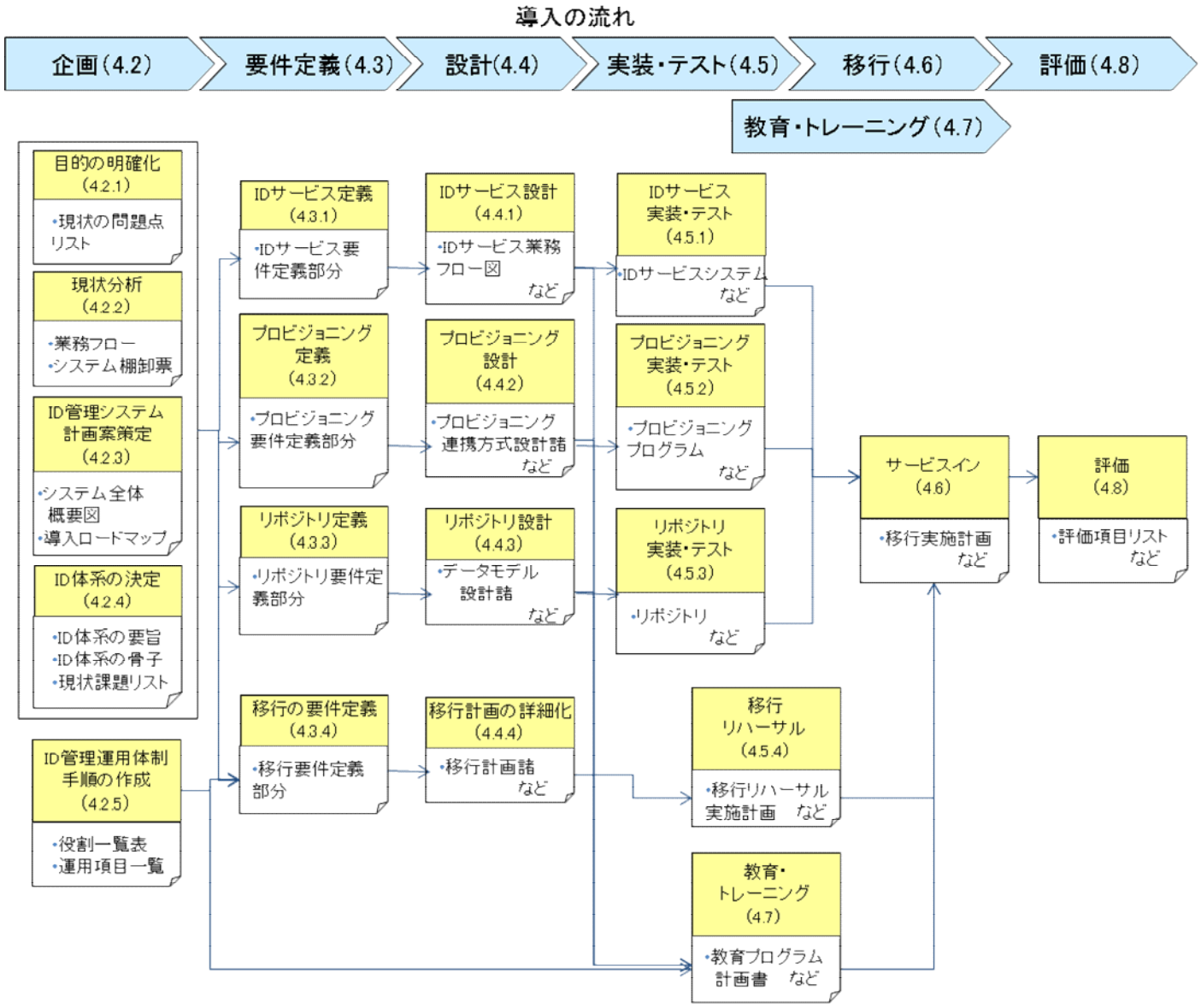
パターンC）
オンプレミスで大部分のID情報を管理する

「クラウド環境におけるアイデンティティ管理ガイドライン」（4章）

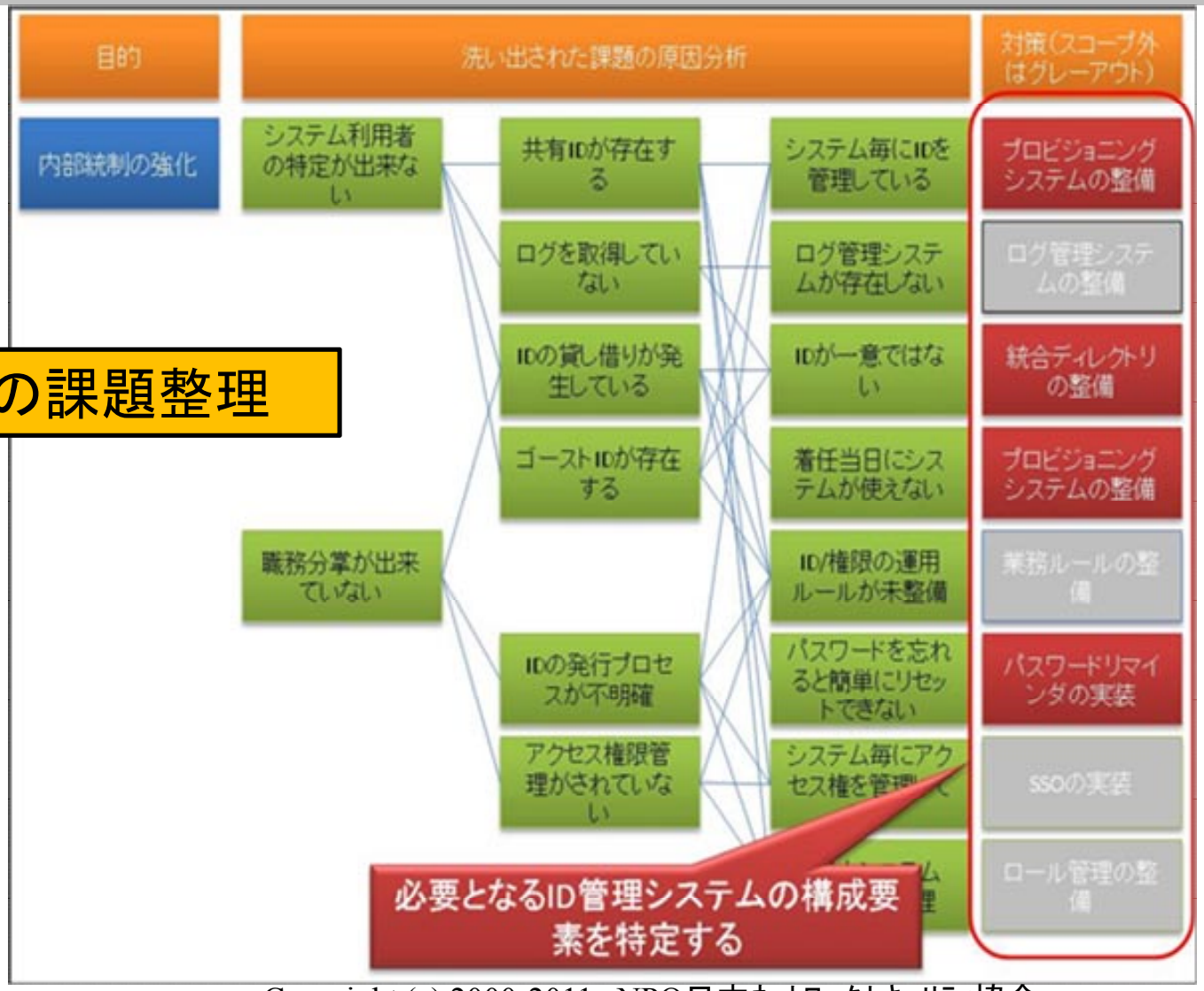
- クラウド環境におけるアイデンティティ管理システム
  - 各実装パターンのメリットとデメリット

実装パターン	メリット	デメリット
1 クラウドークラウド	クラウド・サービスのビルトインの機能をそのまま使うことができるため、オンプレミス側に特別なインフラの構築を含めた改変が少ない	パブリック・ネットワークをクレデンシャル情報が流れる クラウド・サービスが攻撃された場合にID情報の盗難・不正利用が発生しやすい クラウド・サービスの認証機能やユーザリポジトリを利用するのでサービス提供者側の信頼性について十分考慮する必要がある
2 オンプレミスークラウド	認証がオンプレミス側で実行されるため、クレデンシャル情報がパブリック・ネットワークを流れない 認証機能がオンプレミス側にあるため、クラウド・サービスが攻撃を受けた際にもなりすまし等の不正利用が発生しにくい	クラウド・サービスのユーザリポジトリを利用するのでサービス提供者側の信頼性について十分考慮する必要がある オンプレミス側にもID連携用のインフラを構築する必要がある
3 オンプレミスーオンプレミス	認証がオンプレミス側で実行されるため、クレデンシャル情報がパブリック・ネットワークを流れない 認証機能がオンプレミス側にあるため、クラウド・サービスが攻撃を受けた際にもなりすまし等の不正利用が発生しにくい クラウド・サービスのユーザリポジトリをには最低限の情報しか置かないので不正利用時の影響が少ない	アプリケーションの大幅改修が必要になる可能性が高い オンプレミス側にもID連携用のインフラを構築する必要がある

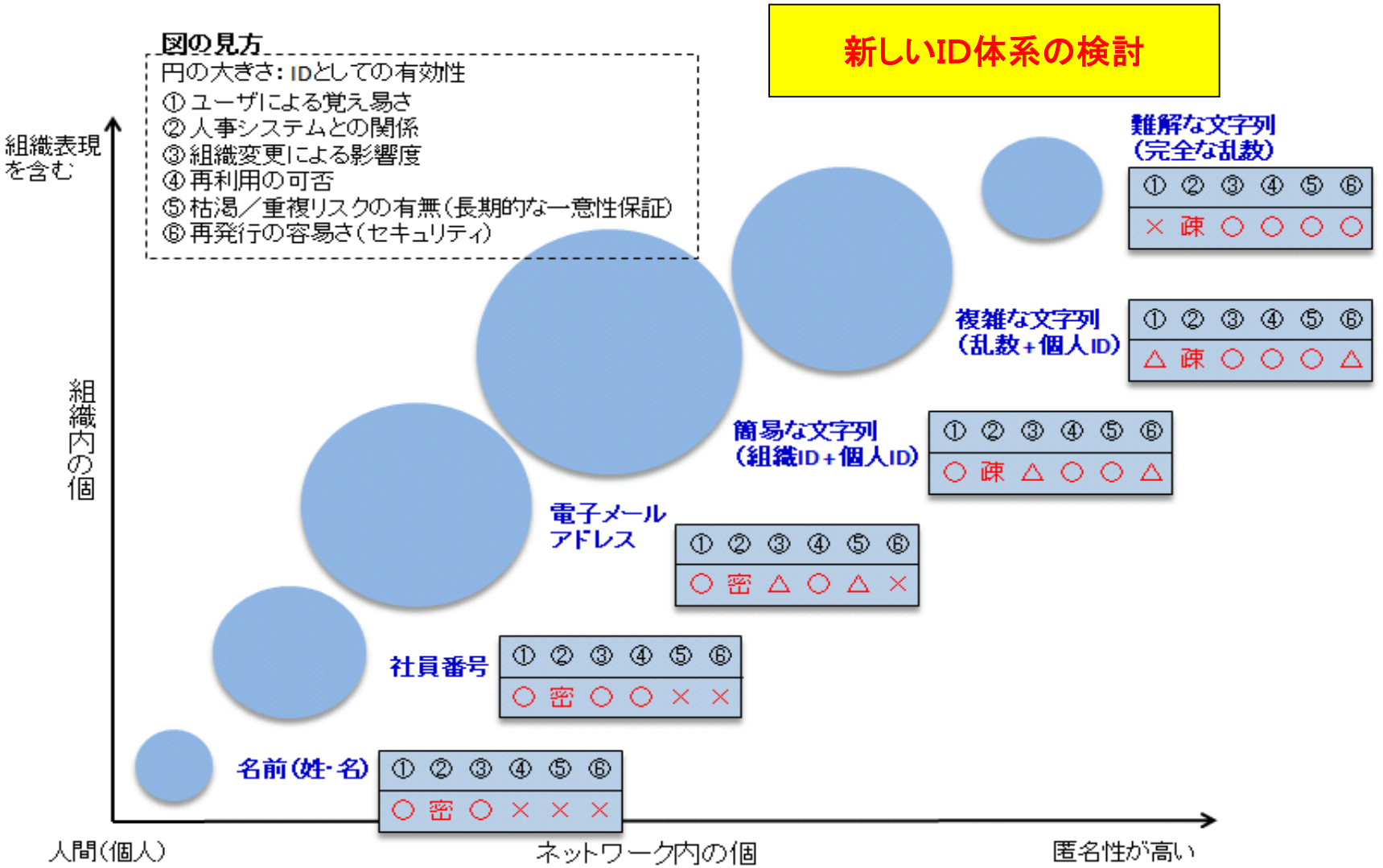
「クラウド環境におけるアイデンティティ管理ガイドライン」（5章）



現状の課題整理



「クラウド環境におけるアイデンティティ管理ガイドライン」（5章）



「クラウド環境におけるアイデンティティ管理ガイドライン」（5章）

- 実装方法の検討プロセス
  （1）サービス提供者の提供する機能の調査
  アイデンティティ・プロビジョニング、ID連携、ユーザプロファイル管理の各側面でチェックリストを作成
  （2）組織内のアイデンティティ管理基盤が提供する機能の調査
  アイデンティティ・プロビジョニング、ID連携の各側面でチェックリストを作成
  （3）実装パターンの検討／選択
  4章で紹介した実装パターンと調査結果で適合度を判定

クラウドへの実装方法検討

機能領域	チェック項目		適合するパターン		
			1	2	3
アイデンティティ・プロビジョニング／デプロビジョニング	インターフェイス	適合したものを持っている	○	○	○
		適合しない（カスタムも不可）	×	×	△
	通信経路	セキュアである	○	○	○
		セキュアでない	×	△	○
	必要なID情報	持っている	○	○	○
		持っていない	×	×	×
	クラウドへ展開不可な属性	あり	×	○	○
		なし	○	○	○
ID連携	外部認証のサポート	あり	－	○	○
		なし	－	×	×
	インターフェイス	適合したものを持っている	－	○	○
		適合しない（カスタムも不可）	－	×	×
ユーザプロファイル管理	独自管理インターフェイス	あり（無効化不可）	○	△	△
		なし	○	○	○
	リアルタイム属性交換のサポート	あり	－	－	○
		なし	－	－	×

「クラウド環境におけるアイデンティティ管理ガイドライン」（5章）

JNSA

			システム									調査目的	記述例
			システムA			システムB			システムC				
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 [作業者:新規] 情報システム部 [作業者: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											
		作業者											
		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 [作業者:新規] 情報システム部 [作業者:変更] 自身 [タイミング:変更] 夜間バッチ
		トリガー											
		作業者											
		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為	・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	

現場で使えるテンプレート

テンプレート例：状況可視化シート

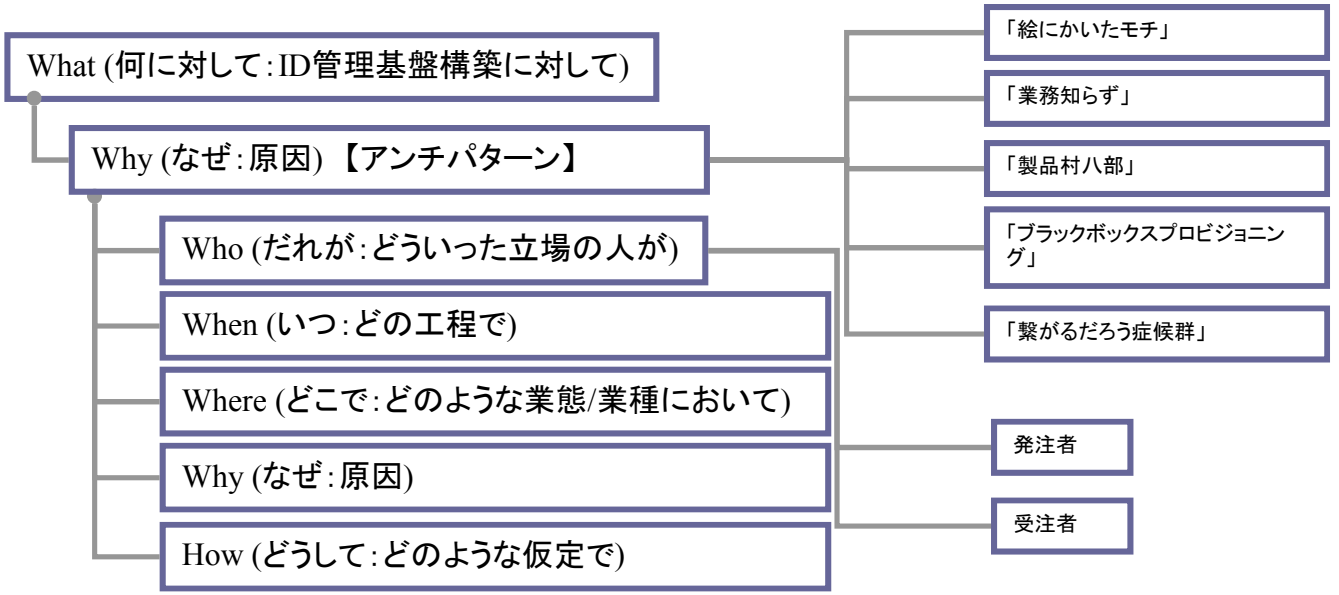
アンチパターンの分類フレーム

アンチパターン記載事項

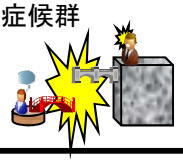
①症状
②原因
③解決策または
予防策

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を分類し考察していくこととする



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。	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。	企画フェーズ 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。	IDサービス定義 IDサービス設計(外部設計) 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。	プロビジョニング定義 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。	プロビジョニング設計

「クラウド環境におけるアイデンティティ管理ガイドライン」(7章)

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いる仕事ですが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

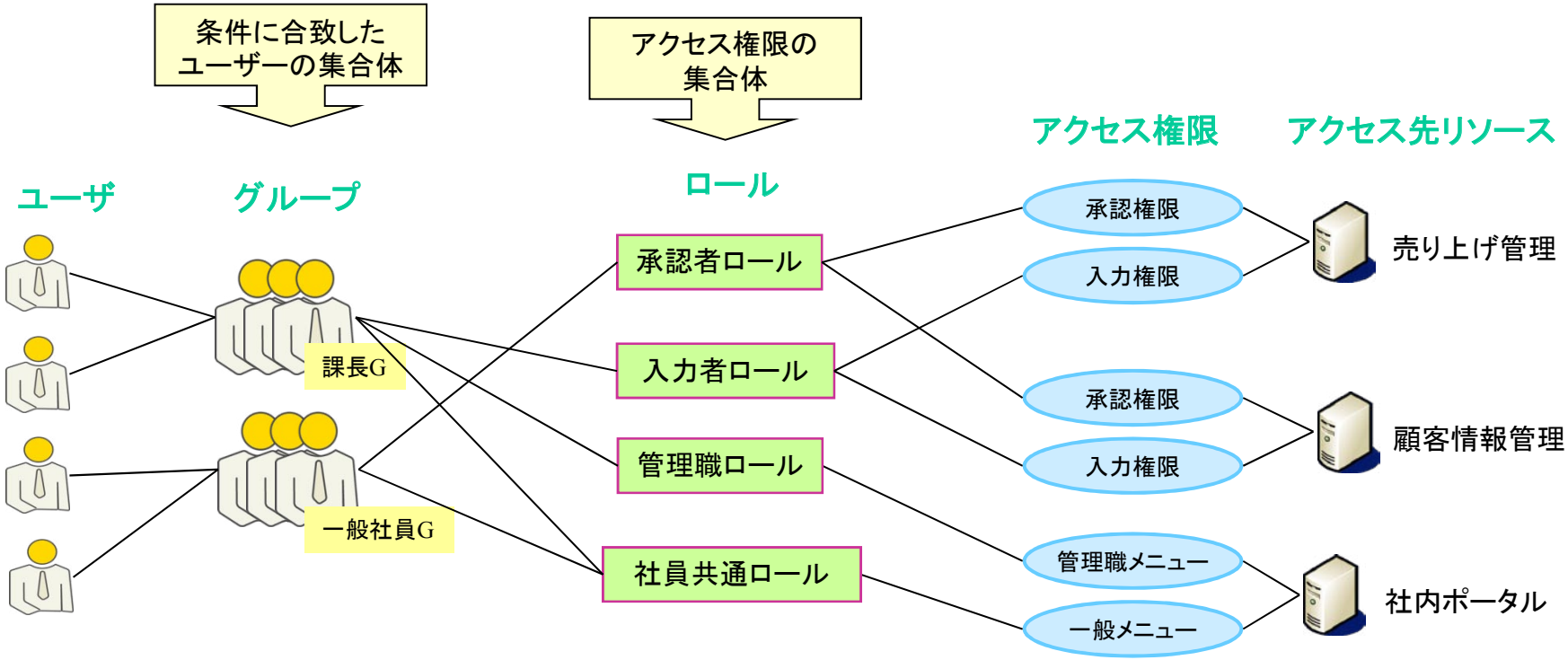
■予防策/回避策
アンチパターンに陥らない処方箋

■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

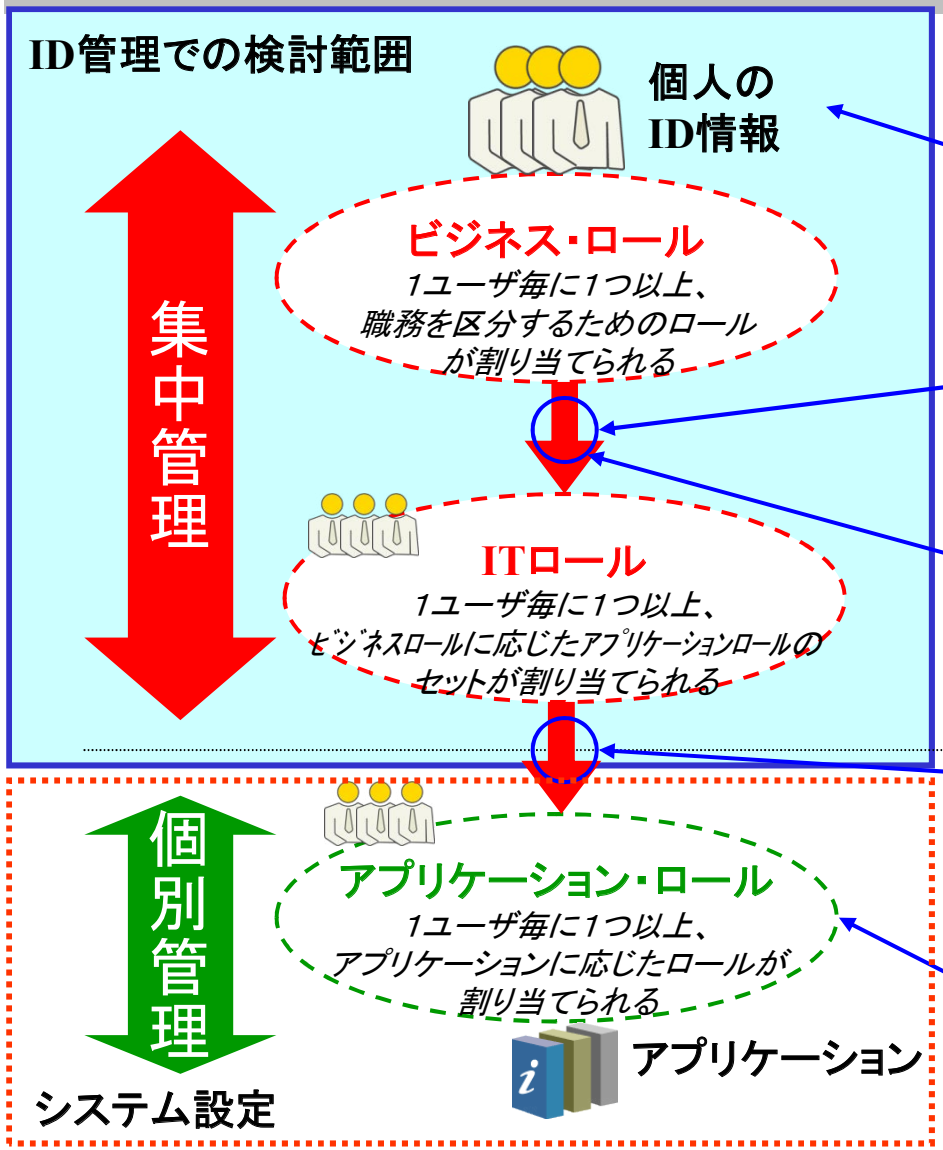
ロールマネジメント　検討結果　中間報告

1．ロール管理とは何か？
①ID管理におけるロールとは

ロールとは職務権限/役割に応じた、リソースへのアクセス権の集合体です。
アクセス権はアクセス先リソース（オブジェクト）とオペレーションから構成され、
ユーザーないしはグループは、ロールの割り当てを経てアクセス権を獲得する。
RBAC (Role-based access control:ロールベース・アクセス制御)は、個々のユーザ/グループ単位での割り当てではなくロールに基いてリソースへのアクセスをコントロールするモデルです。
リソースへのアクセス権をロールで束ねることで、システム横断的なアクセス権管理を実現し、以降の運用を容易することが可能となる。



1.ロール管理とは何か？
②ロールの分類とID管理での検討範囲



ID情報をアプリケーションに対し直接的に割り当てると、管理性や拡張性が失われるため、レイヤーを用いて管理する

ビジネスユーザはビジネス・ロールを持ち、ITロールにマッピングされる。

ビジネスロールは直接的にアプリケーションロールにマッピングすることもできる。

ITユーザはITロールを持ち、ITロールはアプリケーション・ロールにマッピングされる。

アプリケーション管理者はアプリケーション・ロールを定義し、それぞれのシステム権限にマッピングする。

1．ロール管理とは何か？
③ロール定義例

以下にビジネス･ロールからITロールへのマッピングを定義した例を示す。
ここでは所属企業/職制によるビジネス･ロールを定義し、業務単位のアクセス先リソースでの
アプリケーション･ロールからITロールを定義している。
更に業務フローごとの職責ロールなども定義の対象となる。

ビジネス･ロール			ITロール	認証		社内システム												
				認証基盤		ポータル					メール	社内電話帳	会議室予約	スケジュール	各種申請		管理メニュー
所属企業コード	分類	職制		パスワード初期化アカウントロック解除	パスワード変更	トップメニュー	管理職用メニュー	一般職用メニュー	出向者用メニュー	グループ企業用メニュー					申請	承認	
00:本社	一般	役員	R001	×	○	○	○	×	×	×	○	○	○	○	○	○	×
		管理職		×	○	○	○	×	×	×	○	○	○	○	○	○	×
		一般社員	R002	×	○	○	×	○	×	×	○	○	○	○	○	×	×
		出向者	R003	×	○	○	×	×	○	×	×	○	×	×	○	×	×
	システム部	運用管理者	R004	○	○	○	○	○	○	○	○	○	○	○	○	○	○
		ヘルプデスク	R005	○	○	○	○	○	○	○	○	○	○	○	○	○	×
01:グループ企業	スタッフ	管理スタッフ	R006	×	○	○	×	×	×	○	○	○	○	○	○	○	×
		一般スタッフ	R007	×	○	○	×	×	×	○	○	×	×	×	○	×	×
		受入出向者	R008	×	○	○	×	○	×	○	○	○	○	○	○	×	×
02.その他企業	その他	受入出向者	R009	×	○	○	×	○	×	×	○	○	○	○	○	×	×
		契約社員		×	○	○	×	○	×	×	○	○	○	○	○	×	×
		協力会社社員	R010	×	○	○	×	×	×	×	○	×	×	×	×	×	×
			ACL	ACL001	ACL002		ACL003	ACL004	ACL005	ACL006	ACL007	ACL008	ACL009		ACL010	ACL011	ACL012

2. ID管理におけるロール管理の重要性
①ロールの重要性

■権限管理でロールを使う意味

・システムをセキュアに運用するために、権限管理を行う必要があります。

・個別に管理するのではなく、ロールによって集中的に管理したほうが運用の効率化が図れます。

■ロールのメリット

権限をロールで管理することで、以下のメリットが見込めます。

・権限の可視化

権限に名前（ロール）をつけることによって、システムで行なう処理概要を可視化できる。

・管理の単純化

集中管理するため、運用が容易になる。

2. ID管理におけるロール管理の重要性
②ID管理システムでロール管理をおこなう重要性

IT基盤上で稼動しているシステムの従業員のライフサイクルや権限管理を自動化することは「監査」・「運用」面からとても重要です。その実現のためにID管理とロール管理を組み合わせて実装することは以下の点でとても有効と考えられます。

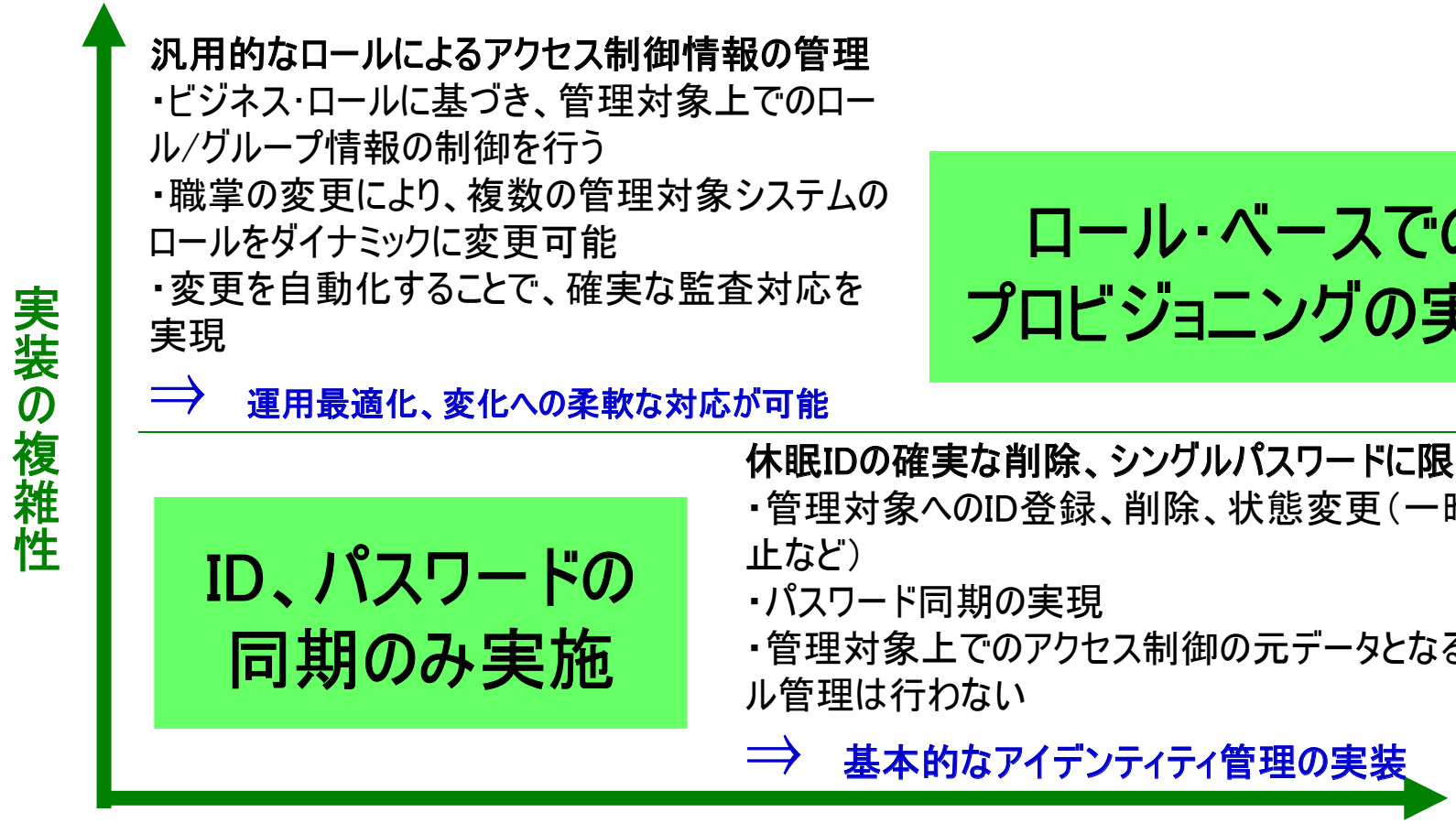
①ID管理とロール管理を一緒に運用することでの運用効率向上
・各アプリケーションに対して、共通で管理する仕組みを提供できるようになる

②ID管理による権限付与の理由明確化
・一元的に管理された情報を利用し、権限を付与することが可能になる。
そのため、権限付与のルール化が実施でき、理由が明確になる

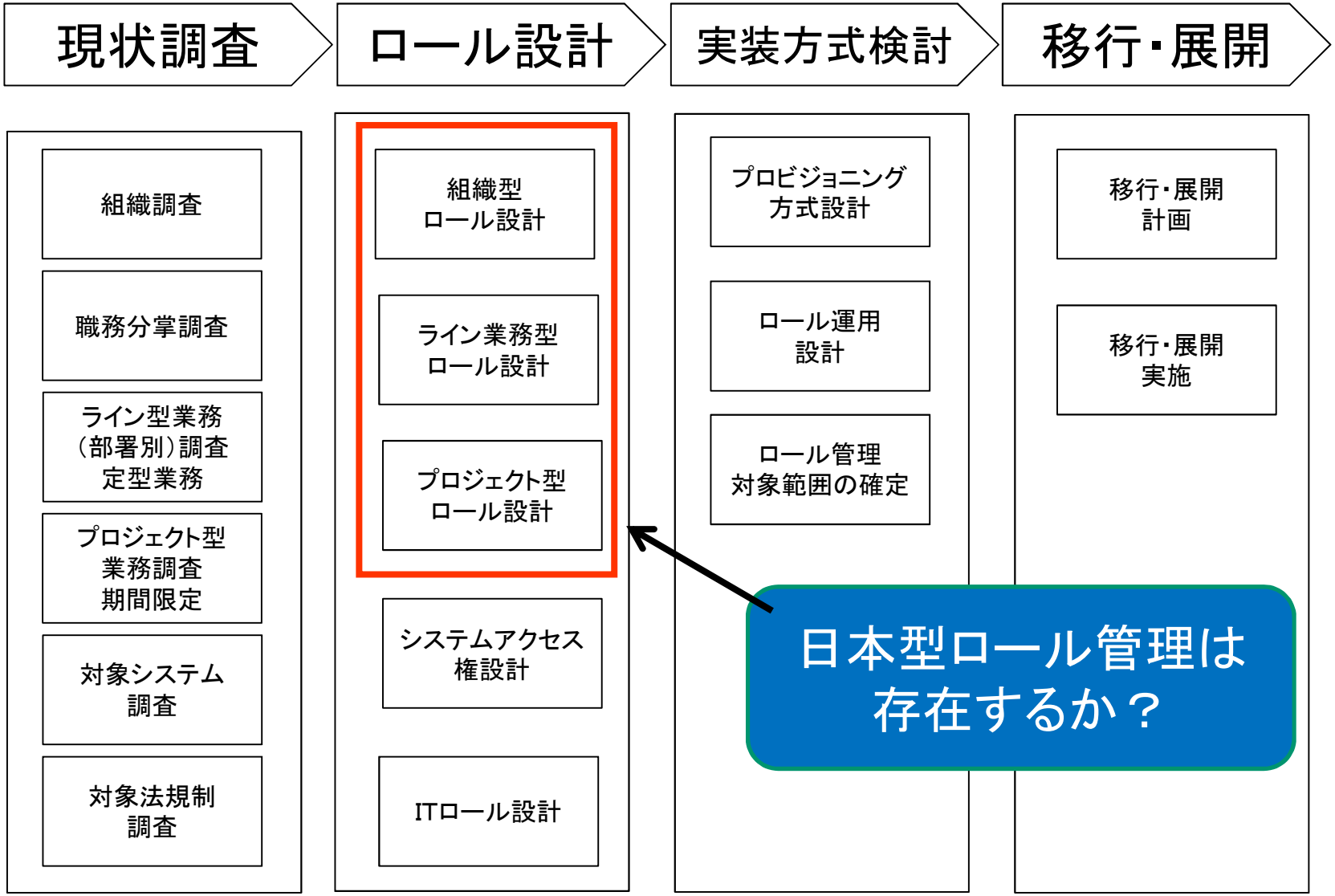
③ID管理とロール管理を一緒に運用することでロールの自動メンテナンスの実現
・ID管理のプロビジョニング処理と連動してロールの割り当てなどを
自動化することで、属人的運用、人為ミスを最小化することができる

2．ID管理におけるロール管理の重要性
③ロール管理検討のスコープ

- ID管理システムを導入されている企業においても、ビジネス･ロールに基づいた制御まで実装しているケースはまだ多くはありません。検討においては、実装のスコープを明確化することが重要です。



3．ロール定義　検討の進め方
①タスクチャート



2011年度の活動予定

1. 活動テーマ

　1）プライバシと番号制度（ID管理部分）について

　2）ロールマネジメント（続き）

　3）グローバル環境やハイブリット環境におけるあるべき論

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

書籍販売

本日、書籍注文販売をしています。
サンプルがありますので、
お手に取って御覧ください。

本WGにご協力していただいた皆様

ご協力いただき、大変ありがとうございました。

「主要執筆者」

宮川 晃一	日本ビジネスシステムズ株式会社（WGリーダ）
富士琴 尚寛	伊藤忠テクノソリューションズ株式会社
山口 雅史	NRIセキュアテクノロジーズ株式会社
駒沢 健	NTTコムウェア株式会社
前園 暁子	NTTコムウェア株式会社
小林 智恵子	東芝ソリューション株式会社
丹羽 宗津子	日本アイ・ビー・エム株式会社
酒井 美香	日本IBMシステムズ・エンジニアリング株式会社
岩田 洋一	富士通株式会社
中島 浩光	株式会社マインド・トゥー・アクション

（会社名　五十音順）

「ワーキングメンバー」

木村 慎吾	株式会社インテック
松岡 浩平	NTTコムウェア株式会社
篠原 信之	株式会社シグマクシス
中本 雅寛	日本アイ・ビー・エム株式会社
大森 潤	日本オラクル株式会社
桑田 雅彦	日本電気株式会社
竹下 勉	日本電気株式会社
中村 有一	日本電気株式会社
安納 順一	日本マイクロソフト株式会社
畠木 絋ま	株式会社ネットマークス
大竹 章裕	株式会社ネットマークス
栃沢 直樹	株式会社ネットマークス
佳山 こうせつ	富士通株式会社
寺嶋 秀史	富士通関西中部ネットテック株式会社
福原 幸一	富士通関西中部ネットテック株式会社
恵美 玲央奈	株式会社富士通ソーシアルサイエンスラボラトリ
原田 篤史	三菱電機株式会社 情報技術総合研究所

（会社名　五十音順）