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

2011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

2012年 6 月 8日

WG活動報告内容

１．グローバル環境におけるID管理

２．企業におけるロール管理

３．今年度のテーマについて

４．2011年度ＷＧメンバー紹介

１．グローバル環境におけるID管理

1-1. グローバルID管理検討の背景

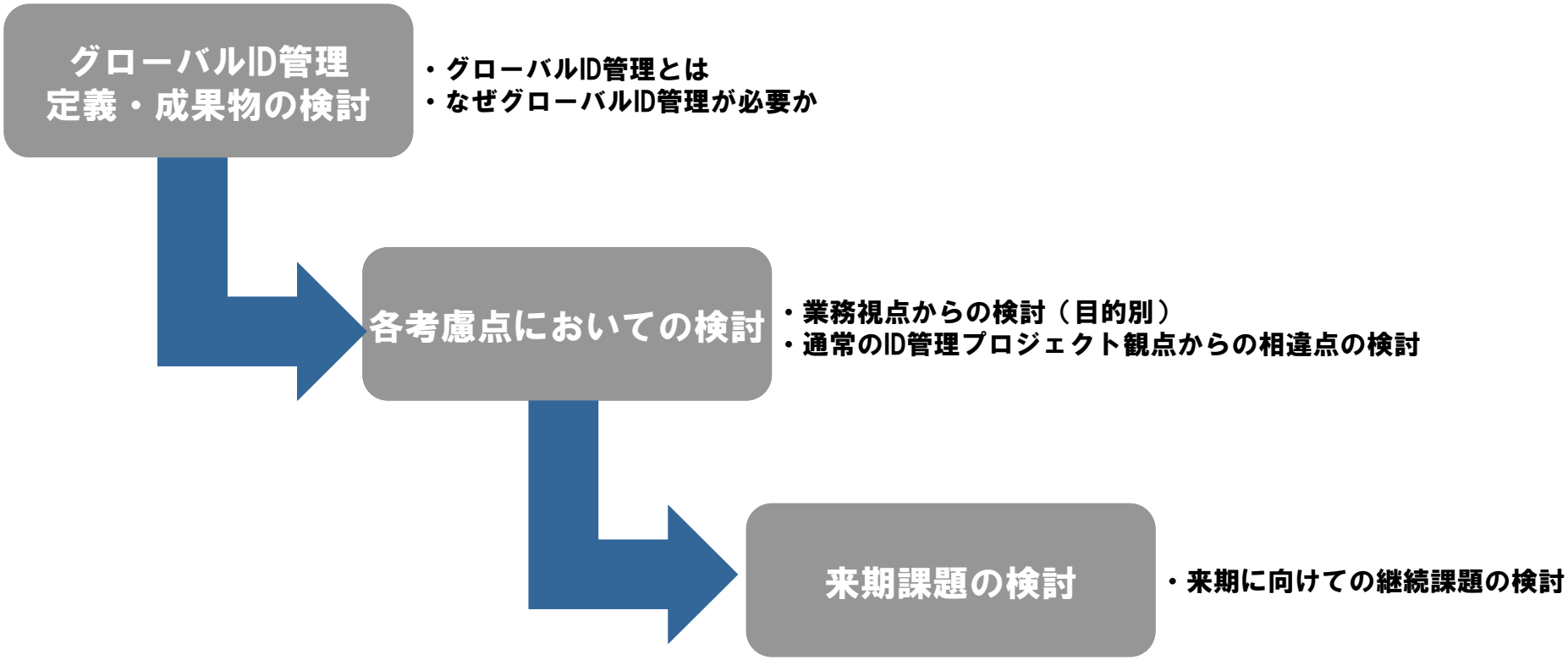
昨年度出版した「クラウド環境におけるアイデンティティ管理ガイドライン」（第2章 ID管理基盤導入における課題と解決 ⑧、⑦）でも触れた下記に挙げるような昨今のビジネス情勢を踏まえグローバルIDについてのある一定の指針を示す必要性からWGでの検討を行った。なお、本検討はID管理の考え方をベースにグローバルID管理に関して追加検討が必要と考えられる箇所について言及している。

- 業務のボーダーレス化に伴い、グローバル展開、グループ企業間や、JOC※、国外工場、海外の企業と提携する場合など、日本国内の社員だけではなく国外に存在するユーザーに対して、情報管理・情報共有を行ったり、システムの利用をさせるケースが増加傾向にある。
- 国外に存在するバックグラウンドの異なるユーザーの情報を統合して管理するに当たっては、既存の国内のID管理の考え方に加え、国外の法対応や独特の人事・組織体系に基づいた管理の考え方を加える必要がある

※JOC：Joint Operations Command

1-2. WGでの検討プロセス

今期のID管理WGでは「グローバルID管理」を検討するにあたり、以下のプロセスを経て成果物を作成した。



1-3. グローバルID管理の利用場面

企業の財産である「人」「物」「金」「情報」を組織横断で活用することに寄って、企業活動においては、生産性の向上、コスト削減等の大きなメリットが生まれる。これらをグローバル規模で実践するにあたって、共通システムを整備し、そのシステムの管理を行う必要性が生まれる。

それぞれの財産に紐付く主なシステム例は以下のとおり

What	Why （課題）	Where （検討者）	Who （対象範囲）	システム例
人	人材管理 グローバルディレクトリ	人事、経営者	社員全員	人事給与システム
物	Supply Chain	業務部門	業務部門	物流・在庫管理システム（SCM、etc） 生産管理システム
金	連結決算	財務部門	営業部門 財務部門	財務会計システム 管理会計システム 販売管理システム
情報	コミュニケーション基盤 Knowledge Mgmt	一般ユーザー	社員全員	メール、グループウェア ファイルサーバ ナレッジマネジメントシステム

1-4. グローバルID管理の定義

本WGにおける「グローバルID管理」の定義

企業のグローバル展開による海外拠点や現地法人、グループ企業、JOC、海外の提携企業等との組織、会社間において、ユーザーに対して共通のシステムを利用させる、またはサービスを提供するための統合的なユーザー情報（アカウント）管理

1-5. グローバルID管理システムの構成要素と視点

ID管理システムの構成要素を踏まえ、グローバルID管理を行う際の検討が必要な視点について整理を行った。

ID管理システムの構成要素

構成要素	役割
IDサービス	ライフサイクルに係るプロセスの管理 ・源泉からのデータ取り込み ・ワークフロー、セルフサービスなどでの保守
プロビジョニング	他システムへのアイデンティティの伝搬 ・連携先のアカウント保守（作成、変更、削除）
リポジトリ	アイデンティティ情報ストア ・属性 ・プロビジョニング先との紐付け

グローバルID管理のシステム化を行う際の視点

視点	概要
法令・文化	遵守すべき法令、業界標準、社内ルール、国/地域/企業文化
組織・人事	採用～退職までのライフサイクル、雇用区分
システム	連携するシステム間での属性マッピング、インターフェース

1-6. 視点別グローバルID管理の考慮点

グローバルID管理を考える際に、通常のID管理と下記の点で考慮する点が異なる。これらの考慮点をもとに、企業や組織のグローバルID管理を考えていく。

	構成要素	法的規制・文化	組織・人事	システム
IDサービス	ワークフロー パスワード管理 セルフサービス 委任管理 他システムとの同期 ユーザ/グループ管理	・データ受け渡しに係る規制 ・会社のポリシー ・機密情報を扱う社員の教育	・採用プロセス（リポジトリへの投入基準） ・本人確認プロセス ・組織の体系 ・申請・承認権限	・多言語対応 ・時差対応
プロビジョニング	アカウント作成 アカウント保守 アカウント終了	・データ受け渡しに係る規制 ・会社のポリシー	・組織改編のサイクル ・引き継ぎバッファ ・兼務	・時差対応 ・ネットワーク
リポジトリ	属性管理 データモデル	・保持できる属性 ・本名に関する考え方 ・データの保管場所に係る規制 ・会社として保持（管理）しなければならない情報の整理 ・人の情報のトレースに係る規制	・共通項目の洗い出し ・項目の有無 ・ID体系 ・IDライフサイクルの洗い出し ・組織の体系 ・兼務	・多言語対応 ・システム管理方法 ・情報管理方法

1-7.「法令・文化」視点からの考慮点

検討ポイント	解説
データ受け渡しに係る規制 IDサービス プロビジョニング	・各国間でのデータ移送（データ受け渡し）に関わる法規制→EU指令などでデータを移転できる国が限られている場合がある（個人属性の移送の可否） ・利用者の同意→データ受け渡しの許諾に関して、Opt In、Opt Outの申請承認が可能なこと、など定めている国があるため、データの受け渡しに係る各国の規制を把握する必要がある
会社のポリシー IDサービス プロビジョニング	・人事情報の改廃に関わる会社のポリシー ・機密情報の扱いに関するポリシー ・パスワードポリシー ・データの暗号化ポリシー
機密情報を扱う社員の教育 IDサービス	・情報の扱いにおいて人為的な流出を避けるためにも社員教育を徹底させる必要がある
保持できる属性 リポジトリ	・プライバシ情報保持にかかわる各国の法規制
本名に関する考え方 リポジトリ	・国によって名前の考え方が異なる（姓、名、ミドルネームだけでは整理できない）
データの保管場所に係る規制 リポジトリ	・クラウドサービスの場合などどこに情報が保管されるかをきちんと把握する必要がある。場合によってはデータセンターの差し押さえによってサービスへのアクセスが不可能になるケースもある
会社として保持（管理）しなければならない情報の整理 リポジトリ	・事業に適用される法規制（銀行法、医療系法規等） ・Social Security Number（SSN）、年金番号、健康保険関連情報など
人の情報のトレースに係る規制 リポジトリ	・社員の職歴に関するトレーサビリティの確保

1-8.「組織・人事」視点からの考慮点

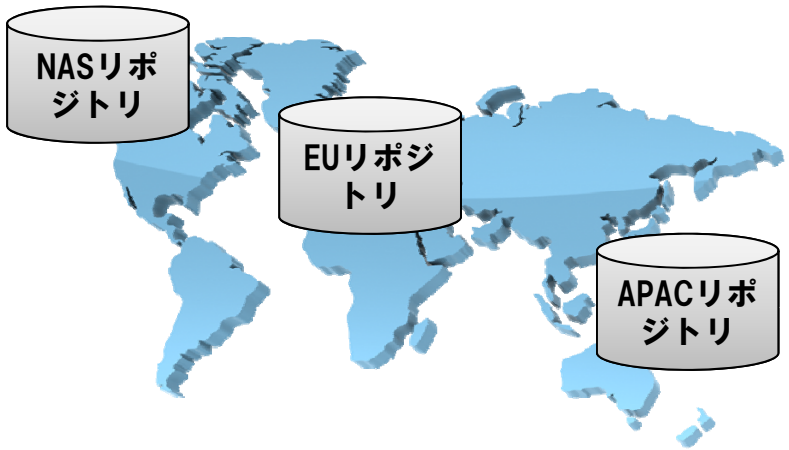
検討ポイント		解説
採用プロセス	IDサービス	・リポジトリへの投入基準
本人確認プロセス	IDサービス	・遠隔地での本人確認の手段
申請・承認権限	IDサービス	・承認権限の付与方法（例：役職による、完全にオンデマンドなど） ・承認フローの有無
組織の体系（役職や役割の統一）	IDサービス リポジトリ	・役職やReport Toなどの扱いは各国で異なるか否かの検討。それにより権限付与方法やユーザー管理の範囲等に影響がある→例として、本社では課長級だが、グループ会社では部長級として扱われる場合、権限はどう与えるべきか、などが挙げられる。
組織改編のサイクル	プロビジョニング	・人事イベントの規模と頻度 ・出向、転籍などの扱い ・グループをまたいで活動する
引き継ぎバッファ	プロビジョニング	・組織改編、人事異動時の引き継ぎ時に伴う一時的な権限（兼務）の取り扱い
兼務	プロビジョニング リポジトリ	・組織の重なりによる新規の組織の発生など権限付与やデータの体系に影響する
共通項目の洗い出し	リポジトリ	・各会社間で共通項目として扱える項目はあるか否か
項目の有無	リポジトリ	・目的により必須項目は変化するが、必要項目がそろっているか否かの検討が必要
ID体系（識別子の付番体系）	リポジトリ	・ID体系をどうそろえるかの検討
IDライフサイクルの洗い出し	リポジトリ	・利用者のIDの改廃のルールに基づいて検討する必要がある。後述の情報の管理方法によって各国で異なるライフサイクル管理を行う必要があり、それらに対応するシステムが必要となる。

1-9.「システム」視点からの考慮点

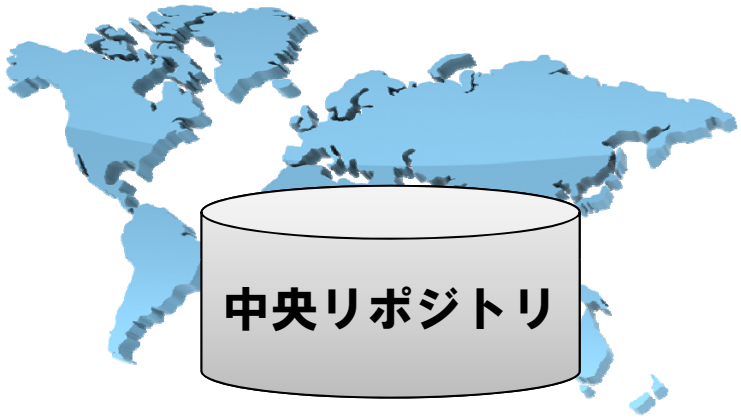
検討ポイント		解説	
多言語対応 IDサービス リポジトリ		・UIの多言語対応（表示される言語） ・利用できる文字コード（属性データの言語依存文字） ・英字名、現地名の扱い→国によって名前の考え方が異なる（姓、名、ミドルネームだけでは整理できない） ・エンドユーザーに対するサポート体制	
時差対応（バッチ処理、サービス停止時間の選択） IDサービス プロビジョニング		・複数のタイムゾーンをまたがり運用する場合、24時間にわたり運用を要求される。その状況において、データのレプリケーション、バックアップ・メンテナンスやバッチ運用をどうするかなどの運用を検討する必要がある	
ネットワーク プロビジョニング		・安全な通信経路の確保 ・通信品質の考慮	
システム管理方法 リポジトリ		・後述の情報の管理方法により、それぞれのシステム配置が異なるため、それに合ったシステム管理方法を検討する必要がある	
情報管理方法 リポジトリ		・分散管理（それぞれのデータを各国リポジトリで管理する方法）と集中管理（統合的なリポジトリを一つ作成する方法）によるメリットデメリットを検討し、構築するシステムに合った管理手法を検討する必要がある	
		メリット	デメリット
	分散管理	・現状のID管理手法の踏襲が可能 ・各国の法規制に沿いやすい ・移行時のNWの問題が起きにくい	・ID体系の検討が困難 ・プロビジョニングを考えたときに情報元と先の検討が必要
	集中管理	・情報の一元管理が実現可能 ・プライバシー情報の一元管理 ・ID体系のトップダウンが行い易い	・ID情報を実際に寄せられるかどうか（金銭面、人工面、法規面など）の検討が必要

1-10. IDの分散管理と集中管理

IDの分散管理と集中管理においては、最終的には集中管理とする方が、管理容易性やコストメリットが得られやすく、またガバナンスの観点からも望ましい。しかし、現状の管理方法や各国の法令などにより実現に際しては困難も多々見られる。下記に分散管理と集中管理方法およびそれぞれの優位点を例示した。



	メリット	デメリット
分散管理	・現状のID管理手法の踏襲が可能 ・各国の法規制に沿いやすい ・移行時のNWの問題が起きにくい	・ID体系の検討が困難 ・プロビジョニングを考えたときに情報元と先の検討が必要



	メリット	デメリット
集中管理	・情報の一元管理が実現可能 ・プライバシー情報の一元管理 ・ID体系のトップダウンが行い易い	・ID情報を実際に寄せられるかどうか（金銭面、人工面、法規面など）の検討が必要

1-11. グローバルID管理まとめ

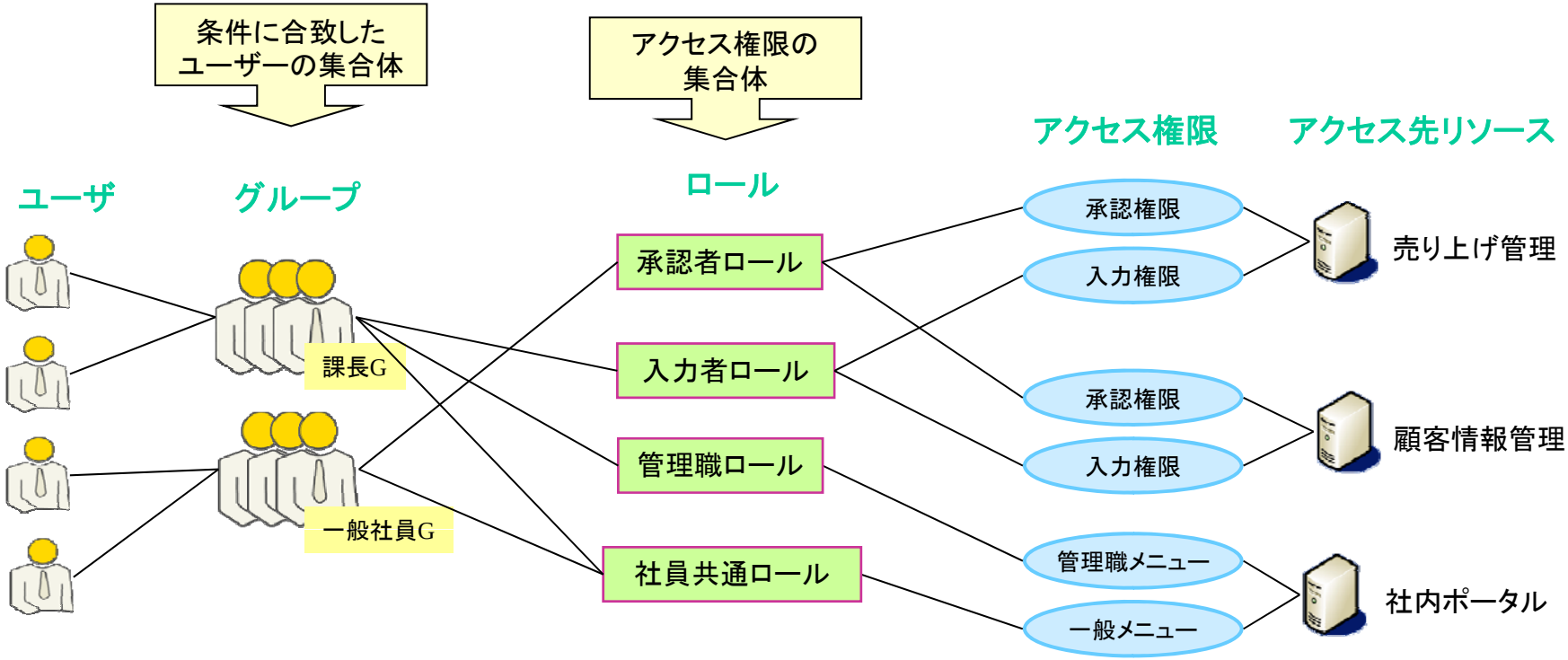
グローバルID管理と言っても、今まで企業内で行われてきた、
ID管理を行うための課題と同じ課題が発生する。

しかしながら、国をまたがることで、法令や時差、利用者の範囲など
が大きく異なるため、その点での考慮は十分必要である。

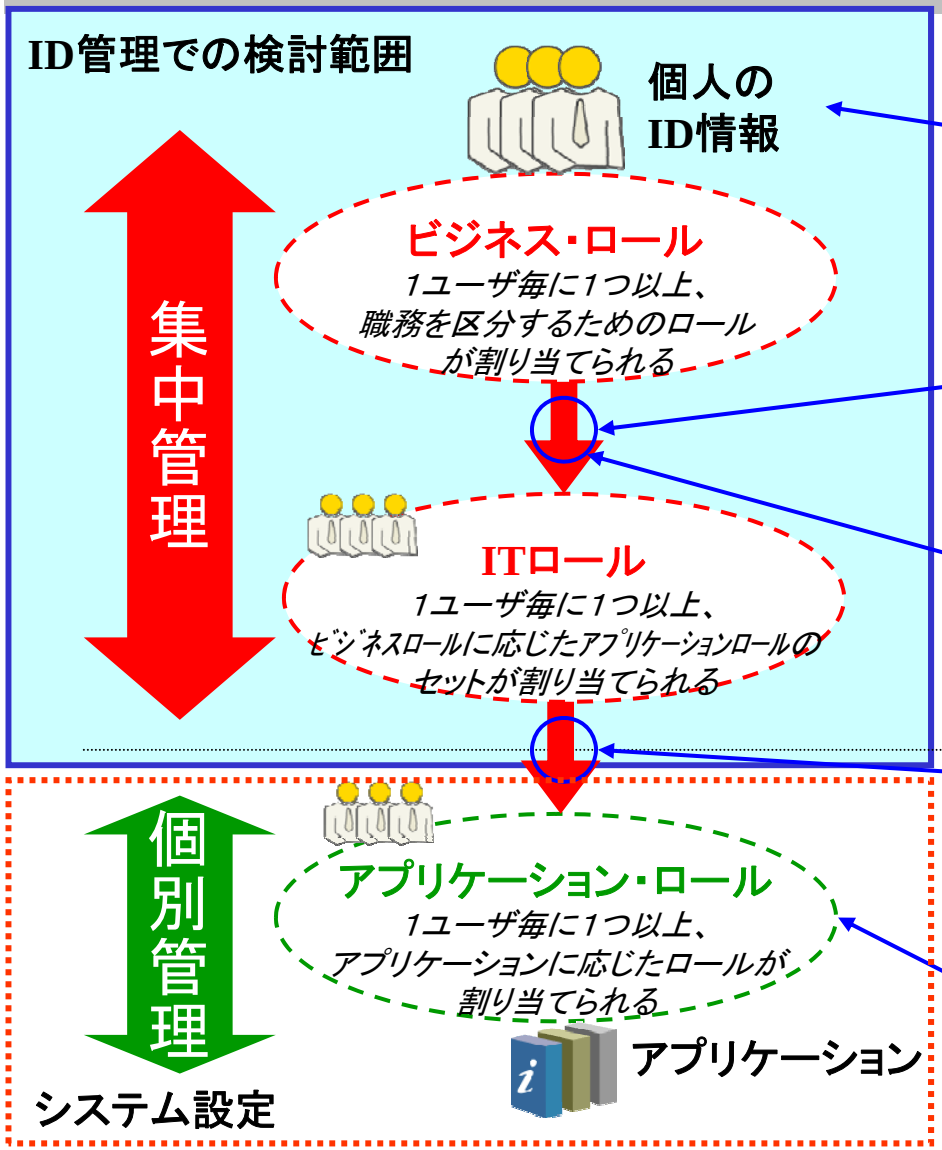
2. 企業におけるロール管理

２－１．ロール管理とは何か？（２０１０年度テーマ）
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。



2－1.ロール管理とは何か？（2010年度テーマ）
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。

２－１．ロール管理とは何か？（２０１０年度テーマ）
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	R001	×	○	○	○	×	×	×	○	○	○	○	○	○	×
		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	R009	×	○	○	×	○	×	×	○	○	○	○	○	×	×
		協力会社社員	R010	×	○	○	×	×	×	×	○	×	×	×	×	×	×
			ACL	ACL001	ACL002		ACL003	ACL004	ACL005	ACL006	ACL007	ACL008	ACL009		ACL010	ACL011	ACL012

２－２．ID管理におけるロール管理の重要性
（２０１０年度テーマ）

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。

２－２．ID管理におけるロール管理の重要性
（２０１０年度テーマ）

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

２－３．２０１１年度のテーマは？

１．各タイプのロールについて整理

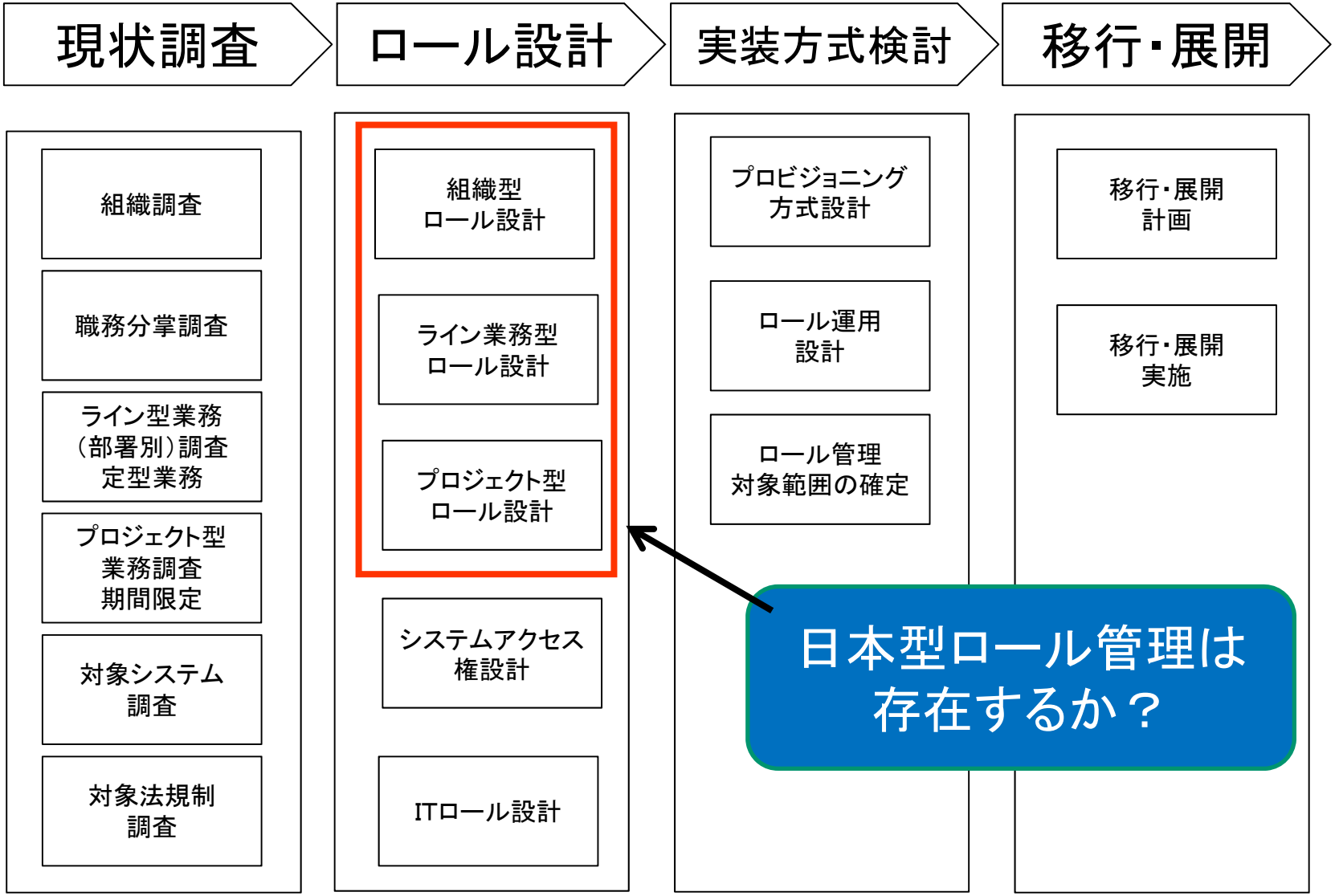
- 組織型ロール
- ライン業務型ロール
- プロジェクト型ロール
- 具体的な利用イメージの共有（サンプルアプリ）

２．ロールの検討・設計手法

- トップダウン型／ボトムアップ型
- ロール・マイニング

など

2－4．ロール定義　検討の進め方
①タスクチャート



２－５．各種ロールについての整理

組織型ロール、ライン業務型ロール、プロジェクト型ロール
について下記観点で整理

- **ロールの用途と特徴の整理**
  - **それぞれ何のために使うロールか**
- **具体的な利用イメージ**
  - **各ロールが必要になるアプリケーション例**
  - **サンプルアプリケーション**
- **各種ロールタイプの考慮点**

２－６．　組織型ロールの用途と特徴・考慮点

組織型ロールの用途と特徴

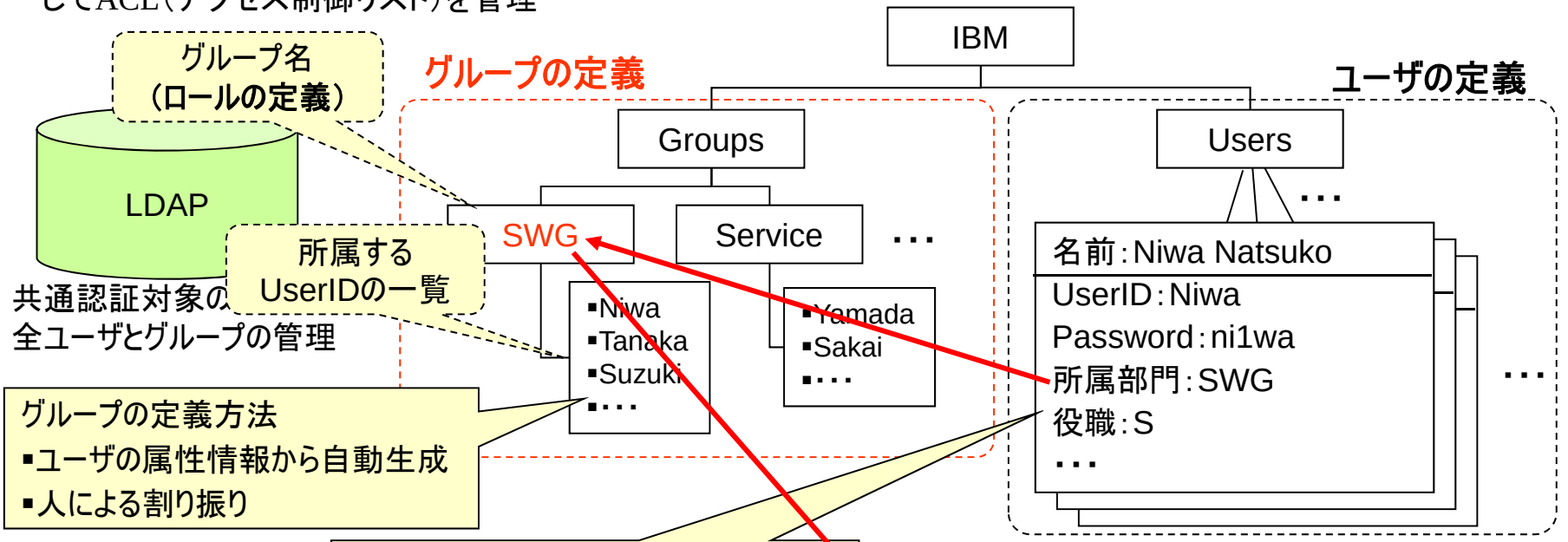
- 組織単位で権限が分けられる業務に利用する
  - 組織ツリーの形でロールが作られる
  - 職位情報をロールに使うことができる
- 人事情報・組織図・名刺情報などからロールを自動生成しやすい
- Top Down　で作成しやすい

組織型ロールの考慮点

- 下位の組織のどこまでロール化が必要か
  - 実装しやすさなども影響
- 組織変更にどう対応するのか？
  - コードであれば比較的メンテナンスは容易
- 権限の継承
  - 入れ子ロールは複雑になる　TOPの権限の継承も考慮
  - 下位ロールの権限　参照権限の範囲を考えておく必要がある
    部門権限　⇔　部長個人権限
    部直属の人（部長）にしか見えない　部に所属している人には見えない　など
- 組織をベースにしていても不適切な権限付与になってしまうことがあるので注意
- 組織そのものの上下・包含関係をどう表現するかも課題

＜組織型ロールの利用例＞　Web認証サーバー

- 統合認証サーバでは、認証情報として利用者情報、認可するための情報としてACL（アクセス制御リスト）を管理



グループ名	リソース	アクセス権限
SWG	URL1	R,W,E
	URL2	R,W,E
	URL3	E
Consulting	URL1	R,W,E
	URL3	R

２－７．　プロジェクト型ロールの用途と特徴・考慮点

プロジェクト型ロールの用途と特徴

- 期限付きの業務（プロジェクト）を行う場合に使用する
- プロジェクト専用のロールを作ることがある
- 組織情報から抽出できない　自由度は高い
- 日常業務上プロジェクトを順次実行していくような部門もある

プロジェクト型ロールの考慮点

- ロールの管理者の設置が必要
  - ロールメンバーの管理
  - ロールのもつ権限管理
  - サブロールの作成・削除
- ロールの管理ルール
  - 管理責任と実作業実施の分離
  - ロールの改廃　基準があるべき
- 増え続ける傾向が強い　強い規制力が必要

２－８．　業務型ロールの用途と特徴・考慮事項

業務型ロールの用途と特徴

- 複数の組織が関わる業務に使用する
- 業務そのものが変わらない限り変更は少ない
- それぞれの組織内でさらに権限が分かれることが多い
- SoD（職務分掌）が求められることが多い
- 組織ロールとプロジェクトロールの両方の特徴を持つ
- 組織・職位とは関係なく決まったパターンがある　○×をする人というロール
  - 入力者ロール　承認者ロール　作業者ロール
- 基幹業務が中心

業務型ロールの考慮点

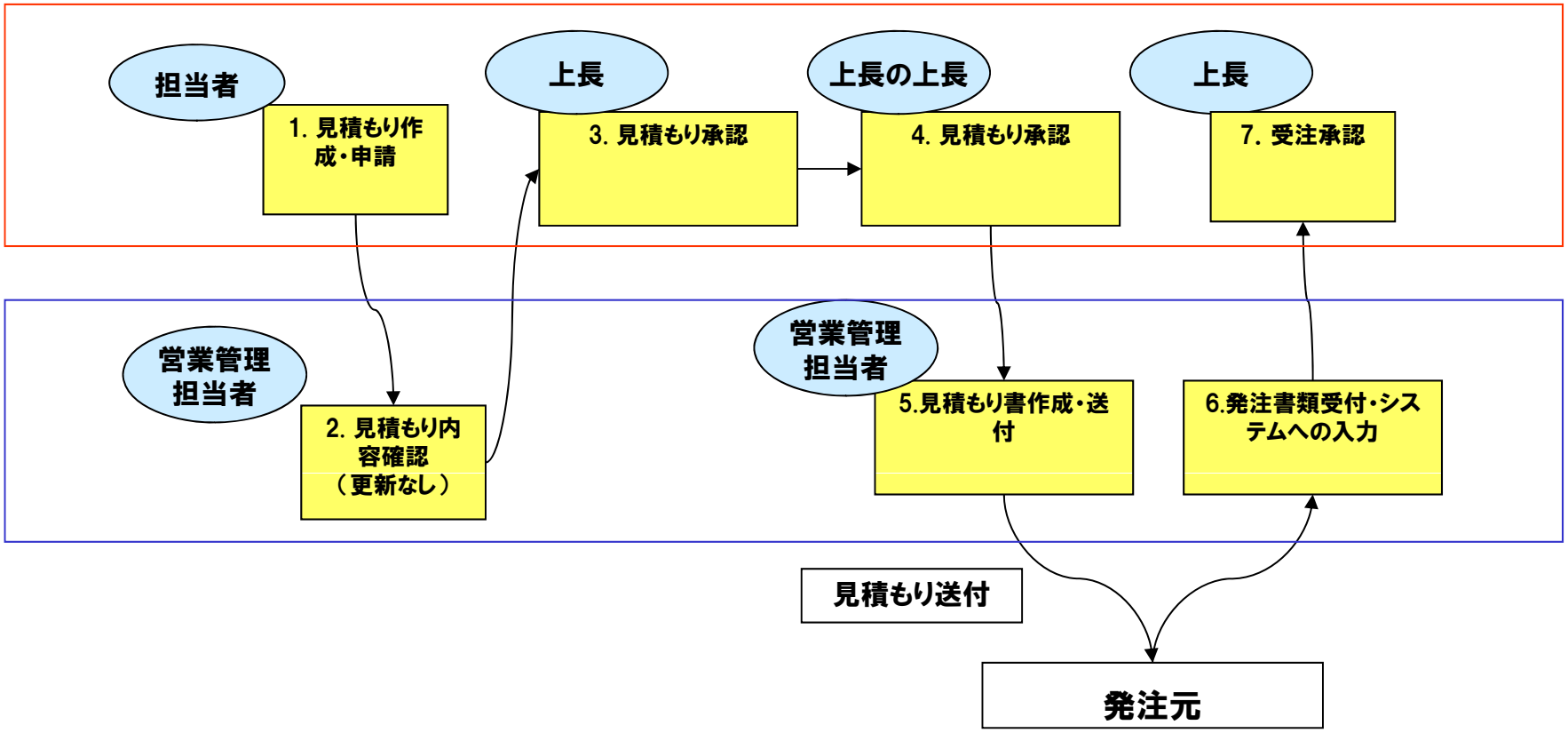
- 業務フローを意識するため、業務分析が不可欠
- 業務全体フロー　＞　システムフロー　システム内でのみロールが必要となる
- ロールと権限が密接に関連している
- ロールと肩書きは対応しない　まず業務上の役割＝ロールありき
  - 部長だからといって承認者でないケースはある
  - 承認者であるためには部長以上というルールはありうる

＜ライン業務型ロールの利用例１＞

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

＜ライン業務型ロールの利用例2＞

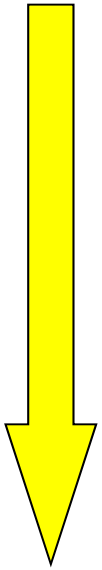
見積もり作成・受注管理システム



２－９. ロール設計手法

- Top down 型モデリング
  - 組織情報、人事情報などからユーザーと属性の組み合わせセットを作り権限セットを作る
- Bottom Up　型　モデリング
  - 実際のアプリケーション上の権限から同じ権限セットを持つユーザーを見つけていく
- ハイブリッド　型
  - Top DownとBottom Upを組み合わせる

２－１０．　ロールデザイン手法とロールタイプ



- 組織ロールはトップダウン、プロジェクトロールはボトムアップが向いているなどそれぞれ適した手法があるか？
  - 定型のないプロジェクトであってもプロジェクトリーダーなどのある程度固定された役割や権限セットがある
  - 組織型であっても定型外ロールは存在する
- ロールのタイプに関わらず、トップダウンとボトムアップの両方のアプローチが必要ではないか？
  - 理想としては、トップダウンで作成したロールですべてカバーできることが望ましい。＝あるべき姿が作れるから
  - トップダウンは資料・情報が整備されていないとできない
    - 何が　どの程度　整備されている必要があるのか
- ボトムアップは実環境情報から　“リバース・エンジニアリング”実施することはできるか？
    - すべてをボトムアップでやろうとすると作業量が大きくなりがち
    - 現状肯定になりがちなので、ロールの数が膨大になり意味を成さない可能性も

２－１１．　ロールデザイン手法とロールタイプ

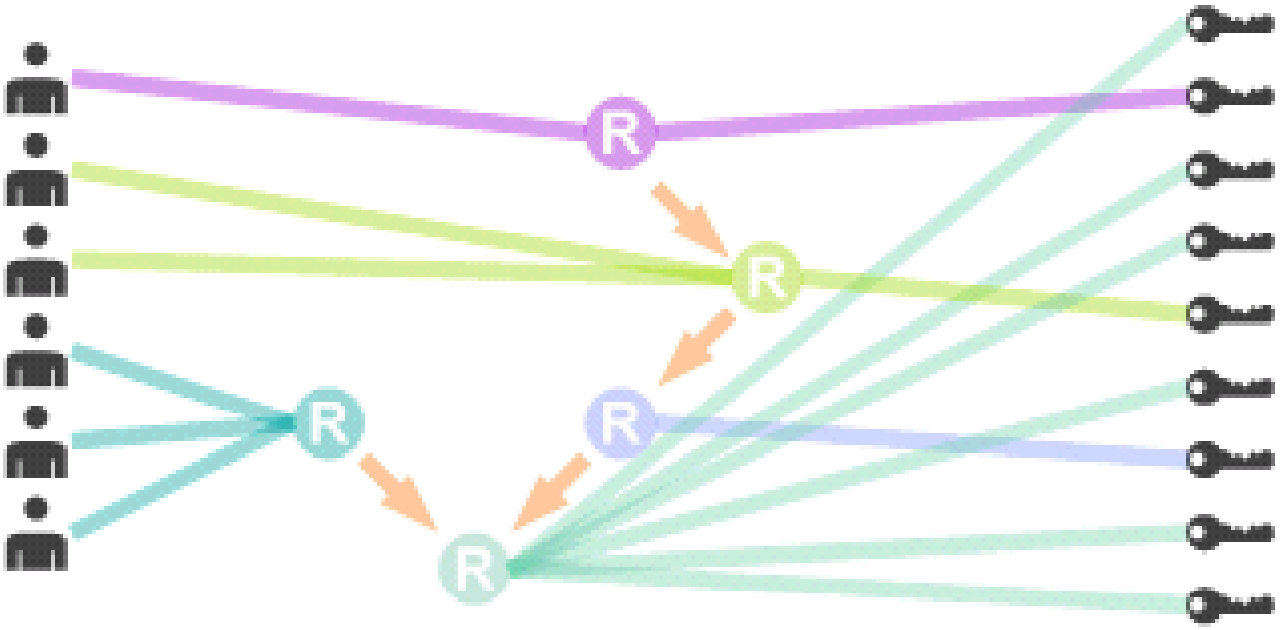
＜デザイン手法に関する結論＞

“ロールのタイプに関わらず、トップダウンとボトムアップの両方のアプローチをすることが望ましい”

- **その他の考慮点**
  - **例外の扱いはロール設計とは別に考える必要がある**
    - **ロール設計の対象外とし例外権限を付与するプロセスを別途確立する。（例外としての証跡を残す）など**
  - **プロジェクト型ロールの扱いはさらにディスカッションの余地がある**
    - **組織的に期限付きで行われる業務**
    - **専門家のチーム**
    - **定型のないプロジェクト**

（参考）ロール・デザインの基本的な考え方

1. ユーザーと各種リソースへのアクセス権限のマッピングを洗い出す
2. 同じ権限セットを持つユーザーを見つけ、ロールとして定義する
3. 組み合わせ（ロール）が多い場合は、階層化・継承により単純化を検討する



２－１２. トップダウンロール設計に必要な情報

1. 情報の種類 ： 組織・人事情報
   - 情報ソース例
     - 全社ディレクトリー・人事データベース・電話帳 など
   - 属性の例

例１） 全社ディレクトリ(ユーザー属性）
- 所属組織
  事業部・センター・部・グループ
  組織コード
- Managerか、社員か 部下がいるかどうかフラグ
- （決裁権限フラグ ＞ 業務？）
- 社員か協力会社社員か ＞雇用形態
- 職務＝職種 営業とかSEとか
- 職位 ＞ 階級 肩書き 役職
- ワークロケーションコード
- 資格・免許情報 （医師 薬剤師 外務員免許 ・・・）
- 国籍 市民権を持っている国
- 勤務事業所
- 座席位置(何階のどこ）
- 事業所の住所
- 電話番号
- メールアドレス
- 所属長
- 部下
- Managerの場合は管理対象の組織
- 所属プロジェクト・タスク・チーム

例２） 組織構成図 あるだけ必要

２－１２. トップダウンロール設計に必要な情報

2.　情報の種類　：　業務についての情報

- 情報ソース例
  - 業務フロー（J-SOXで整備済みのものなど）
  - 規制、業界ガイドライン
  - 社内の業務情報の取り扱い基準　権限情報
  - 職務分掌一覧
  - プロジェクト体制のテンプレート
  - 業務システムのオペレーションマニュアル・研修資料

- 属性の例
  - 業務上登場する役割
  - フロー上に定義された役割（ロール）
  - 規制・ガイドラインで定められた　SoD定義情報
  - 決済権限情報　承認してよい人の条件規定

２－１３．ボトムアップロール設計に必要な情報

- **情報ソース例**
  - ファイルサーバーのACL
  - 情報共有ツールの　Forumなどのアクセス権限リスト
  - 各種アプリケーションのアクセス制御情報
  - 文書管理システム　ACL
  - ワークフローシステム
  - ID管理システム（LDAPとか）

- **属性の例**　実環境から抽出する

例１）ファイルサーバー

ACL

ユーザー・グループとフォルダーへのアクセス権（Read Write Delete など）

例２）グループウエア

アクセス権設定

ユーザー・グループ と　管理者　作成者　読者　編集者などの権限（すでにロール化？）

例３）ワークフローシステム

承認階層情報　　承認経路情報　決済権限情報

例４）実ディレクトリデータ

２－１４．　属性の特徴によるロールタイプの作りやすさ

- ロールからResouce　の関係が固定
  （変更が少ない・元になる属性が管理されている）
  ＝TopDownで適切なロールを作りやすい
  　　例　：　組織　業務

- ロールからResouce　の関係が流動的
  （基になる属性が管理されていない管理できない）
  ＝BottomUpした方が作りやすい
  　　例　：　タスク　ワーキング

２－１５．　今後の検討テーマ

１．実際のケーススタディーを作成してみる

２．これまでの検討結果を体系的にまとめる

３．実装するときの問題点や運用の視点でも検討してみる

３．今年度のテーマ

３－１．今年度のテーマ

１．ロールマネジメントの検討（継続テーマ）
　　ケーススタディーの実施

２．書籍「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」改訂作業
　　情報の最新化

３．アイデンティティとプライバシー勉強会
　　有識者の方との懇談を予定

４．エンタープライズ市場におけるトラストフレームワーク勉強会
　　ークラウド利用時のID管理におけるセキュリティ/統制課題ー

＊現在、新規メンバー募集中！　６／１５（金）まで！
＊書籍の割引購入券配布中　２０％OFF

４．2011年度WGメンバー紹介

４－１．WGメンバー紹介

氏名	所属
宮川 晃一	WGリーダ　日本ビジネスシステムズ株式会社
富士榮　尚寛	伊藤忠テクノソリューションズ株式会社
木村 慎吾	インテック
駒沢 健	NTT　コムウェア
前園　暁子	NTT　コムウェア
松岡　浩平	NTT　コムウェア
山田　達司	株式会社　NTTデータ
篠原　信之	株式会社　シグマクシス
小林 智恵子	東芝ソリューション株式会社
丹羽　奈津子	日本IBM株式会社
中本 雅寛	日本アイ・ビー・エム株式会社
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
讃井 崇喜	日本アイ・ビー・エム システムズ・エンジニアリング
大森潤	日本オラクル株式会社
貞弘　崇行	JBSソリューションズ

氏名	所属
川田　晋嗣	セコムトラストシステムズ株式会社
酒井　寛	セコムトラストシステムズ株式会社
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
半澤　敦	日本電気株式会社
高木 経夫	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
南　芳明	日本ベリサイン株式会社
岩田　洋一	富士通株式会社
今堀　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
安納　順一	マイクロソフト株式会社
原田　篤史	三菱電機（株）情報技術総合研究所
中島　浩光	株式会社マインド・トゥー・アクション

計33名