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

JNSA 2015年度活動報告会

2015年度 アイデンティティ管理WG 成果報告

宮川　晃一
（日本ビジネスシステムズ株式会社）

2016 年　6月　17日（金） ベルサール神田

WG活動報告内容

1. 2015年度の活動内容

2. IDの融合と分離

3. エンタープライズにおける特権ID管理

4. エンタープライズロール管理

5. 今年度の活動テーマ

１．2015年度の活動内容について

2015年度活動内容について

2015年度は以下のテーマで議論をいたしました。

1. IDの融合と分離
2. エンタープライズにおける特権ID管理
3. エンタープライズロール管理

4. 書籍改定作業
5. IDと個人情報保護法（勉強会）
6. WGメンバー紹介HP作成（普及）

7. 10周年記念セミナー
8. ID&IT 2015　協賛

２．IDの融合と分離

個人アイデンティティの結合・融合・分離とは

- 個人はコンテキストに応じた各種アイデンティティを保有しているが、全体として一個人
- コンテキストに応じて使い分けるのは不便だが、別コンテキストのアイデンティティとは分離したい場合がある
  - ✓パブリック（範囲限定を含む）とプライベート
  - ✓ビジネス／ソーシャルとパーソナル
- 用語の定義
  - ✓結合：異種のアイデンティティを同一個人として結び付ける
  - ✓融合：異種のアイデンティティを一つにまとめる
  - ✓分離：異種のアイデンティティを結合も融合もさせない

検討テーマ

- 各種の個人アイデンティティの結合・融合・分離にかかわるメリット／デメリットの明確化、課題の整理と解決方法の考案
  - ✓職業人
  - ✓公民（国民、自治体民）
  - ✓コミュニティ人
  - ✓消費者

検討内容、スケジュール

月	検討内容
2014年度	各種個人アイデンティティの洗い出し、 それぞれの特徴、位置付け、関係の整理、 各種個人属性の性質の整理、 アイデンティティ結合・融合・分離にかかわるメリット／デメリットの洗い出し、課題の整理
2015年 8月	アイデンティティ結合・融合・分離にかかわる課題整理の精査・深堀
10月	アイデンティティ結合・融合・分離にかかわる課題整理の精査・深堀
2016年 2月	アイデンティティ結合・融合・分離にかかわる課題解決方法の 検討・考案
3月	アイデンティティ結合・融合・分離にかかわる課題解決方法の 検討・考案、2015年度のまとめ
2016年度	2014～15年度の検討内容の精査・深堀、 課題解決方法(詳細)の検討・考案

各種個人アイデンティティの洗い出し(1/2)

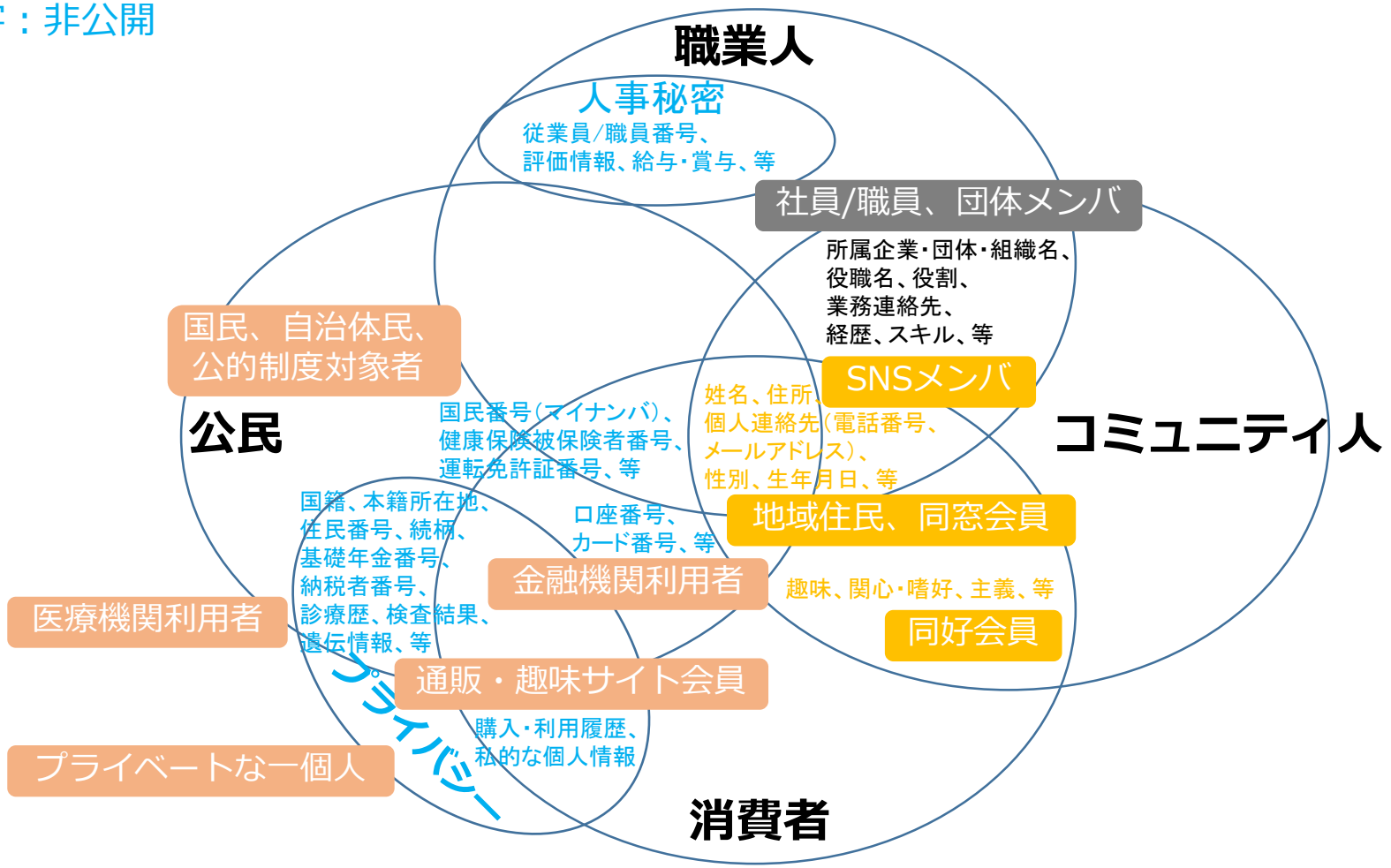
分類	アイデンティティ（例）	属性（例）　青字：非公開	特徴、位置付け・関係
職業人	企業社員、 公務員、 団体職員、 学校職員 等	所属企業・組織名、 従業員/職員番号、姓名、 役職名、役割、 業務連絡先（電話番号、メールアドレス、勤務地 等）、 経歴、スキル、 評価情報、給与・賞与、	• 所属企業・組織から付与された属性が大半を占める • 組織としての正式な個人属性 • 所属企業・組織から秘密指定された一部の属性や、本人が知られたくない属性を除き、公開属性が基本
	業務関連団体 メンバ	所属団体名、役割、	• 組織としての正式な個人属性 • 一部の非公開団体を除き、公開属性
公民	国民	国民番号（マイナンバ）、姓名、 国籍、本籍所在地、住所、性別、 生年月日、	• 国としての正式な個人属性 • 本人以外には非公開属性が基本
	自治体民	住民番号、姓名、住所、性別、 生年月日、続柄、	• 自治体としての正式な個人属性 • 本人および家族以外には非公開属性が基本
	公的制度対象者	健康保険被保険者番号、 基礎年金番号、 納税者番号、 運転免許証番号、	• 公的機関から付与された属性 • 公的制度としての正式な個人属性 • 本人および制度上認められた機関・目的以外には非公開属性が基本
	金融機関利用者	口座番号、カード番号、姓名、 住所、電話番号、性別、生年月日、	• 金融機関としての正式な個人属性 • 本人以外には非公開属性が基本
	医療機関利用者	健康保険被保険者番号、姓名、 住所、電話番号、性別、生年月日、 診療歴、検査結果、遺伝情報、	• 医療機関としての正式な個人属性 • 本人以外には非公開属性が基本

各種個人アイデンティティの洗い出し(2/2)

分類	アイデンティティ（例）	属性（例）　青字：非公開	特徴、位置付け・関係
コミュニティ人	地域住民	姓名、住所、同居家族構成、	• 地域住民としての公開属性 • 公開している姓名は実名とは限らない
	SNSメンバ	SNSアカウント名、表示名、 個人連絡先（電話番号、メールアドレス等）、顔写真、性別、 生年月日、経歴、スキル、 関心・嗜好、主義 、	• SNS上の公開/非公開属性 • SNSサービスによるが、本人が自らの裁量で登録した個人属性 • 本人が自ら知られたい（観られたい）属性を公開
	同窓会員	姓名、性別、出身学校、入学・卒業年、	• 同窓会としての正式な個人属性 • 同窓会内の公開属性
	同好会員	趣味、主義、	• 同好会内の公開属性 • 公開している表示名は実名とは限らない
消費者	通販サイト会員	通販サイトアカウント名、購入履歴、姓名、住所、性別、生年月日、電話番号、支払口座/カード番号、	• 通販サイト上の非公開属性 • 通販サービスを利用するために必要な/要求される個人属性
	趣味サイト会員	趣味サイトアカウント名、趣味、性別、生年月日、関心・嗜好、	• 趣味サイト上の非公開属性 • 趣味サービスを利用するために必要な/要求される個人属性
	プライベートな一個人	私的な個人情報、位置情報、	• 他人に知られたくない非公開属性

各種個人アイデンティティの位置付け・関係

黒字：公開
橙字：コンテキストにより公開/限定公開/非公開
青字：非公開



各種個人属性の性質の分類

パブリック／プライベートによる分類
- パブリック属性
- 限定パブリック属性
- プライベート

ビジネス/ソーシャル/パーソナルによる分類
- ビジネス属性
- ソーシャル属性
- パーソナル属性

獲得方法による分類
- 先天的属性
- 自発的後天的属性
- 強制的後天属性

付与主体による分類
- 企業組織属性
- 公的機関属性
- コミュニティ属性
- 消費者属性
- 個人獲得属性

存続期間による分類
- 不変属性
- 期間更新属性
- 期間限定属性
- 連続不定属性
- 非連続不定属性
- 一時属性

可変性による分類
- 不変属性
- 随時可変属性
- 指定時可変属性
- 個人設定可変属性
- 付与主体可変属性

識別性による分類
- 個人識別特定属性
- 個人識別非特定属性
- 個人識別不可属性

表意性による分類
- 表意属性
- 非表意属性

用途要件による分類
- 個人識別用属性
- 個人認証用属性
- 認可用属性
- 制御用属性
- 表示用属性
- 消費嗜好属性

個人アイデンティティの結合・融合・分離にかかわる課題の洗い出し(1)立場別-1

＜立場別に課題を整理＞

立場	結合・融合の課題	分離の課題
本人	•アイデンティティのコンテキストを明確に区別し切り替えるのが難しい •アイデンティティの種別ごとに同一の個人属性の見せ方を変えるのが難しい •公開/非公開の区分を用途ごとに切り替えるのが難しい •ある種別のアイデンティティ（属性）から別の種別のアイデンティティ（属性）を辿られ結び付けられる可能性が高い	•アイデンティティの使い分けが必要 •アイデンティティの種別ごとに個人属性の登録・更新を繰り返す必要がある •アイデンティティの種別間における個人属性の不整合が生じる •個人情報の保護・アクセスコントロールを分散・重複的に行う必要がある

個人アイデンティティの結合・融合・分離にかかわる課題の洗い出し(1)立場別-2

立場	結合・融合の課題	分離の課題
所属企業/団体	•本人にアイデンティティのコンテキストを明確に区別させ切り替えさせるのが難しい •所属企業/団体が知る必要のない個人属性まで知ること（ができるよう）になってしまう可能性がある	•所属企業/団体が付与した個人属性とそれ以外の個人属性とを分離して（取扱いを分けて）管理する必要がある •所属企業/団体が知る必要のある個人の公民としての属性を、所属企業/団体が個別に保持する必要がある •所属企業/団体が付与したもの以外の個人属性の更新漏れが生じる
公的機関	•公的機関が把握する必要のない個人属性まで知ること（ができるよう）になってしまう可能性がある	•公的機関が付与した個人属性とそれ以外の個人属性とを分離して（取扱いを分けて）管理する必要がある •公的機関が知る必要のある個人の公民/職業人/消費者としての属性を、公的機関が個別に保持する必要がある •公的機関が付与したもの以外の個人属性の更新漏れが生じる •公的機関が把握する必要のある個人の職業人/消費者としての属性を、把握するのが難しい

個人アイデンティティの結合・融合・分離にかかわる課題の洗い出し(1)立場別-3

立場	結合・融合の課題	分離の課題
コミュニティ及びコミュニティメンバ	•コミュニティ及びコミュニティメンバが知る必要のない個人属性まで知ること（ができるよう）になってしまう可能性がある	•コミュニティが付与した個人属性とそれ以外の個人属性とを分離して（取扱いを分けて）管理する必要がある •コミュニティ及びコミュニティメンバが知る必要のある個人の職業人/公民/消費者としての属性を、コミュニティが個別に保持する必要がある •コミュニティが付与したもの以外の個人属性の更新漏れが生じる
消費者向け事業者	•消費者向け事業者が知る必要のない個人属性まで知ること（ができるよう）になってしまう可能性がある	•消費者向け事業者が付与した個人属性とそれ以外の個人属性とを分離して（取扱いを分けて）管理する必要がある •消費者向け事業者が知る必要のある個人の公民/職業人/コミュニティ人としての属性を、消費者向け事業者が個別に保持する必要がある •消費者向け事業者が付与したもの以外の個人属性の更新漏れが生じる

個人アイデンティティの結合・融合・分離にかかわる課題の洗い出し(2)用途別-1

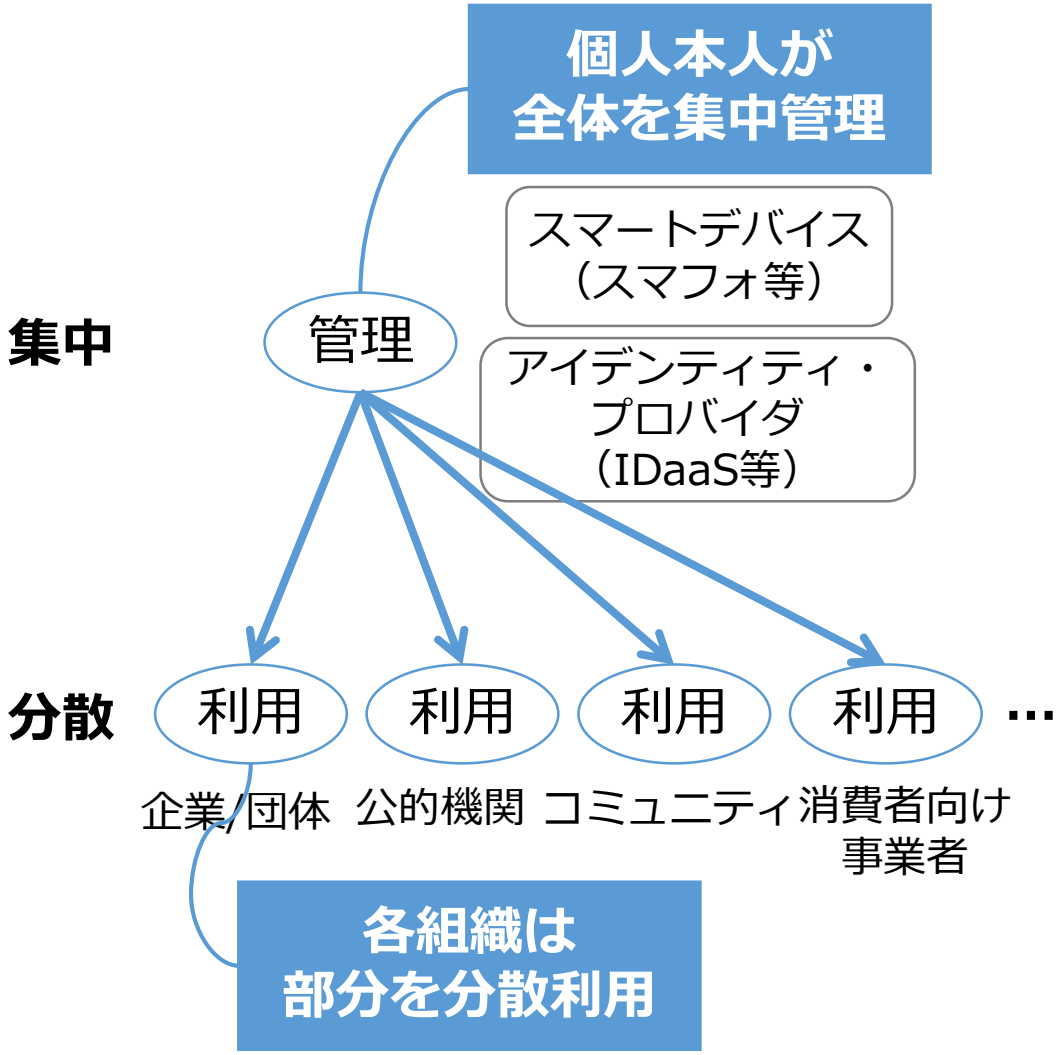
＜用途別に課題の整理＞

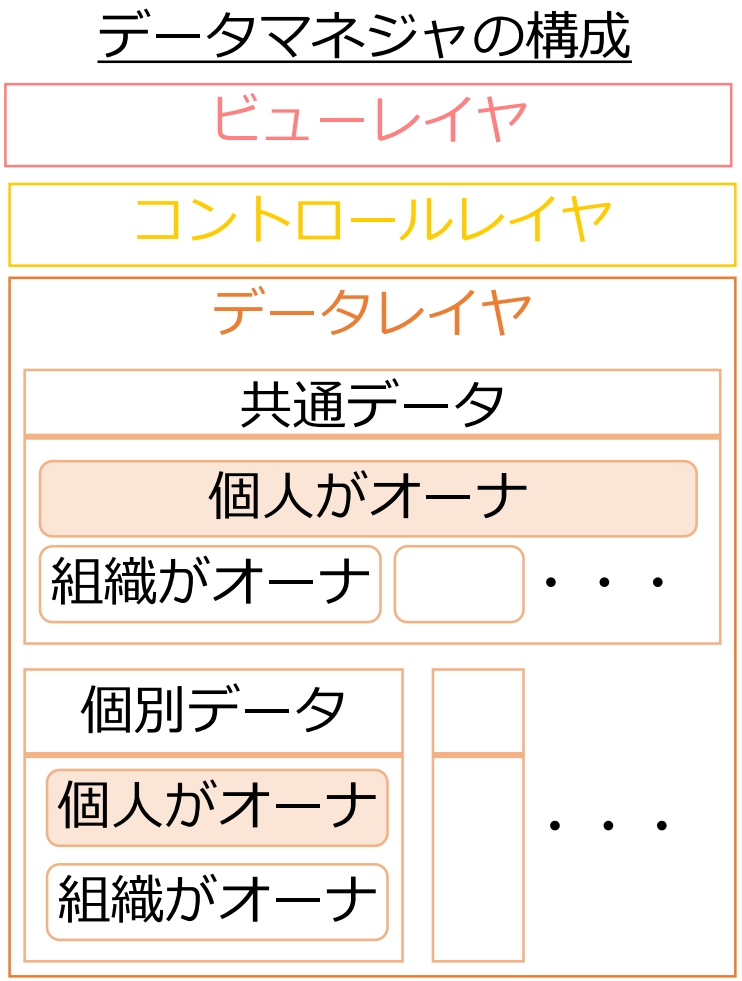
個人アイデンティティの用途		結合・融合の課題	分離の課題
個人認証	識別用属性と認証用属性に基づき、アクセス者が当該個人本人であることを確認する。	• 識別用属性と認証用属性の一つの値で、どのアイデンティティに関しても対応付けて本人確認が取れてしまう。	• アクセス者がアイデンティティを正しく使い分ける必要がある。 • アイデンティティごとに識別用属性と認証用属性を登録・管理しなければならない。
アクセス制御	認可用属性の値に基づき、アクセス対象に対する当該個人のアクセス可否を判断する。	• 認可用属性（ロール属性等）の値がアイデンティティの種別に応じて異なる場合、どの値に基づきアクセス可否を判断するのか、属性値にコンテキストの付与が必要。	• アクセス者がアイデンティティを正しく使い分ける必要がある。 • アイデンティティ間で共通の属性値をアイデンティティごとに登録・管理しなければならない。

個人アイデンティティの結合・融合・分離にかかわる課題の洗い出し(2)用途別-2

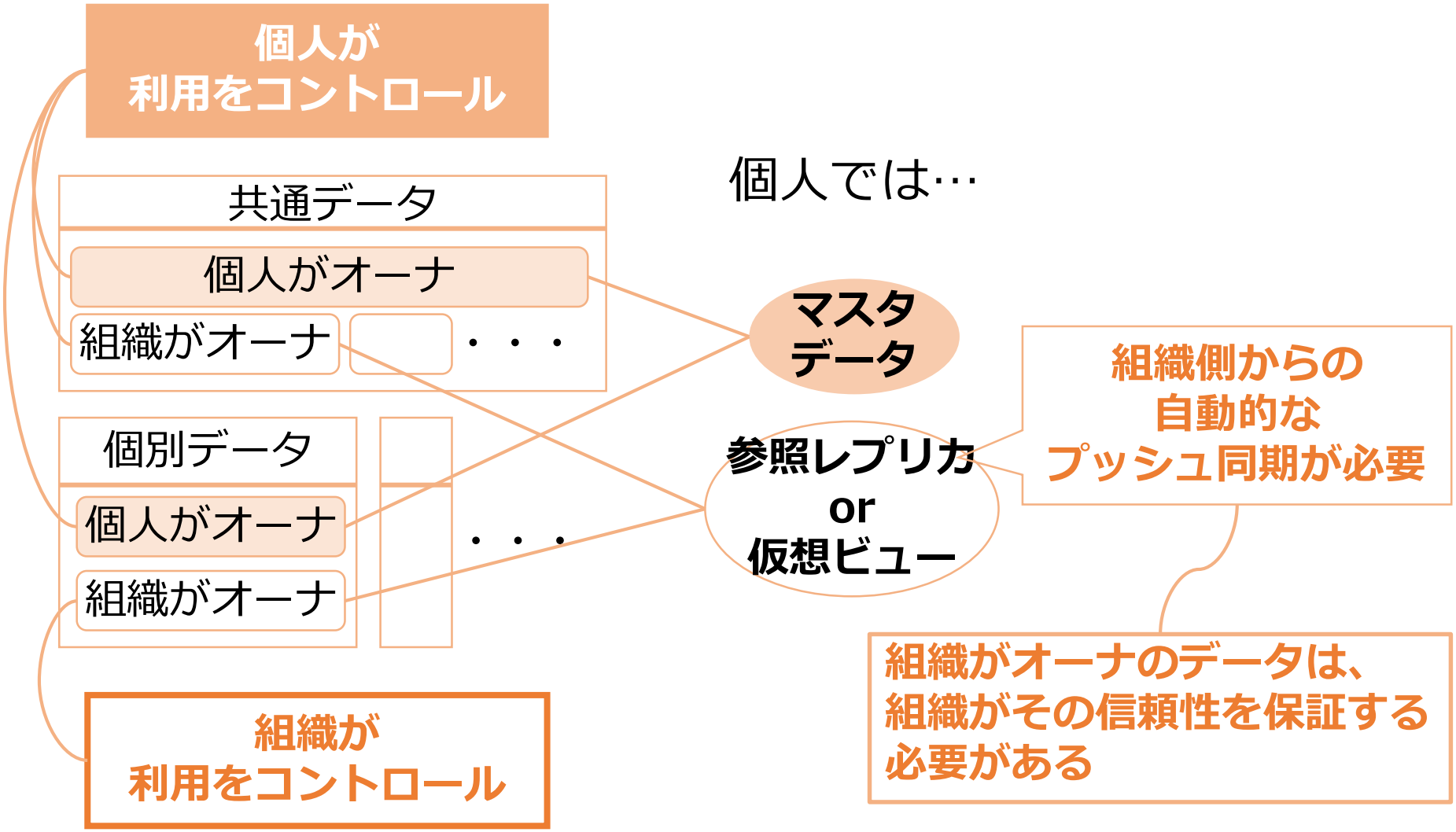
個人アイデンティティの用途		結合・融合の課題	分離の課題
パーソナライズ	制御用属性や表示用属性の値に基づき、処理の制御や画面の表示をアクセス者個人向け専用のものに調整する。	• 制御用属性や表示用属性の値がアイデンティティの種別に応じて異なる場合、どの値に基づき処理の制御や画面の表示を調整するのか、属性値にコンテキストの付与が必要。	• アクセス者がアイデンティティを正しく使い分ける必要がある。 • アイデンティティ間で共通の属性値をアイデンティティごとに登録・管理しなければならない。
ビッグデータ（統計データ）	大量の個人の各種アイデンティティ属性の値（データ）を収集し、統計的に処理・分析することで、属性値（データ）間の相関関係や全体の傾向を見出す。	• プライバシー保護の観点から、データ収集・処理者が知る必要のない個人属性まで知ること（ができるよう）になってしまう可能性がある。	• データ収集・処理の対象範囲がアイデンティティごと区切られ、それを跨る相関関係や全体傾向が見出せなくなる。

個人アイデンティティの結合・融合・分離にかかわる課題の解決方法の考案(1)

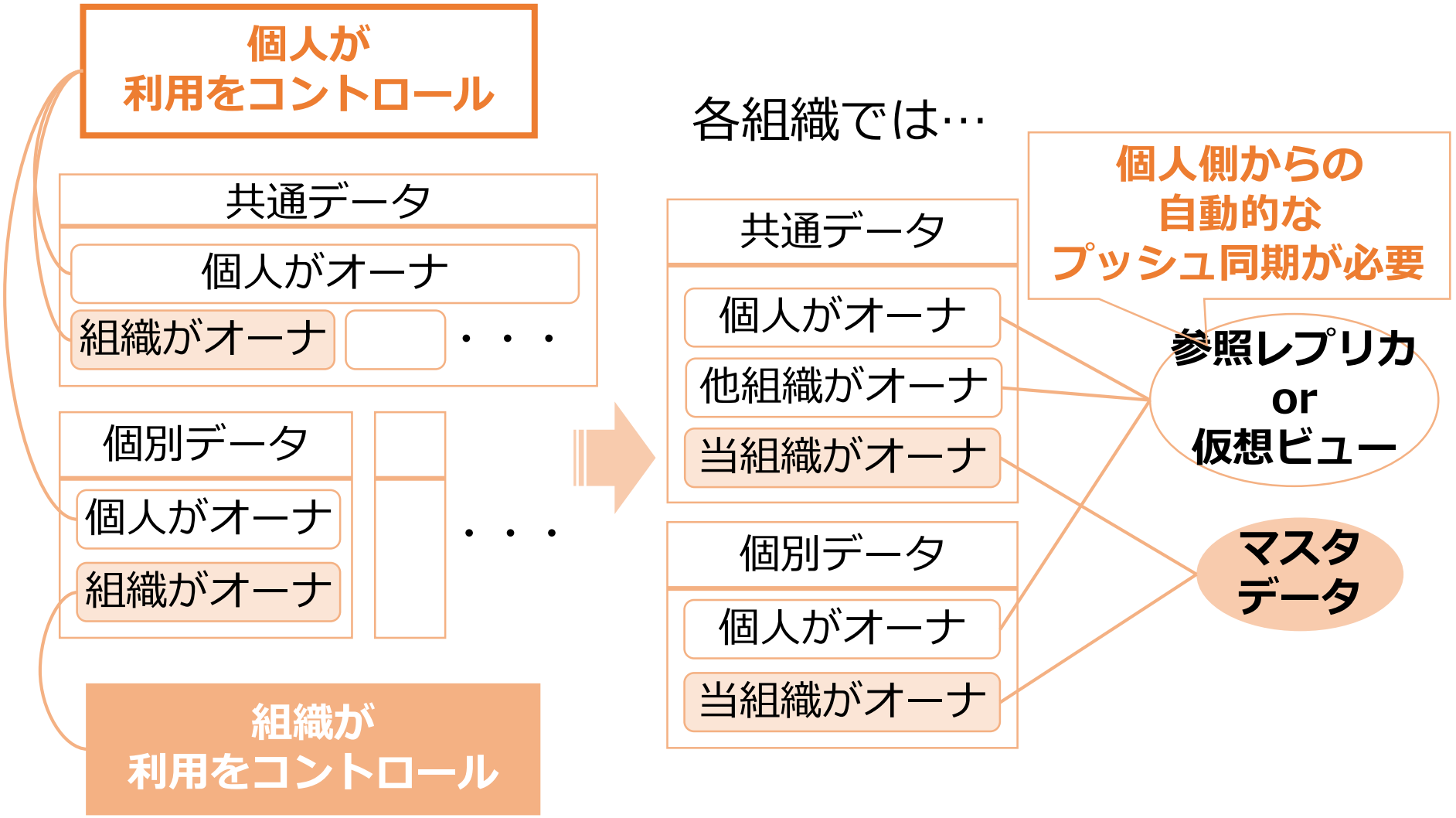




個人アイデンティティの結合・融合・分離にかかわる課題の解決方法の考案(2)



個人アイデンティティの結合・融合・分離にかかわる課題の解決方法の考案(3)



個人オーナの共通データの属性（例）

属性	コントロール者	付与(割当)者	保証者	確認方法
姓名	個人	個人	国、自治体	戸籍謄本、住民票、運転免許証、健康保険証、マイナンバカード 等
住所	個人	自治体	自治体	住民票、運転免許証、マイナンバカード、実際の郵便連絡 等
電話番号	個人	電話事業者	電話事業者	実際の電話連絡
メールアドレス	個人	メールプロバイダ	メールプロバイダ	実際のメール連絡
性別	個人	医師	国、自治体	戸籍謄本、住民票、健康保険証、マイナンバカード 等
生年月日	個人	医師、助産師 等	国、自治体	戸籍謄本、住民票、運転免許証、健康保険証、マイナンバカード 等

個人オーナの個別データの属性（例）

属性	コントロール者	付与(割当)者	保証者	確認方法
住民番号	個人	自治体	自治体	住民票
基礎年金番号	個人	日本年金機構	日本年金機構	年金手帳、基礎年金番号通知書、年金証書
納税者番号	個人	国、税務署	国、税務署	e-Taxシステム、税務署

組織オーナの共通データの属性（例）

属性	コントロール者	付与(割当)者	保証者	確認方法
所属企業・団体・組織名	個人	所属企業・団体・組織	所属企業・団体・組織	所属企業・団体・組織への照会、電子証明書
役職名	個人	所属企業・団体・組織	所属企業・団体・組織	所属企業・団体・組織への照会
役割	個人	所属企業・団体・組織	所属企業・団体・組織	所属企業・団体・組織への照会
業務連絡先	個人	所属企業・団体・組織	所属企業・団体・組織	実際の連絡

組織オーナの個別データの属性（例）

属性	コントロール者	付与(割当)者	保証者	確認方法
従業員/職員番号	所属企業・団体・組織	所属企業・団体・組織	所属企業・団体・組織	従業員/職員証
評価情報	所属企業・団体・組織	所属企業・団体・組織	所属企業・団体・組織	人事システム
給与・賞与	所属企業・団体・組織	所属企業・団体・組織	所属企業・団体・組織	人事システム、給与所得の源泉徴収票
診療歴	医療機関	医療機関	医療機関、医師	診療カルテ
医療(臨床)検査結果	医療機関	医療機関	医療機関、医師、臨床検査技師	臨床検査結果報告書

今後の要検討事項

- 個人アイデンティティの結合・融合・分離にかかわる課題整理の精査
  - アクセス制御や個人情報保護の観点
  - 維持管理の観点
  - 活用の観点
    （パーソナライズ、マーケティング、ビッグデータ等）
- 上記課題の解決方法の詳細を検討・考案
  （～2016年度末を目標に）

３．エンタープライズにおける特権ID管理

特権ID管理の検討事項

特権ID管理は製品仕様に依存度が高い特性があるが、
なるべく汎用的な考え方で整理ができないか、検討を開始した。
下記のサブテーマも加味して検討した。

- **「所有から利用へ」のクラウド環境において、それぞれの立場での管理者の関係性が複雑化。**
- **特権ID管理ソリューションを導入することだけが対策なのかという疑問**
- **と言いつつもノーガードは、もってのほか**

なるべく製品仕様に依存せず、特権ID管理ソリューションの紹介にならず、
しかし一般論だけにならないように解説した。

検討過程と成果物

検討過程

- 2013年度 特権ID管理について検討開始
- 2014年度
  - 「クラウド環境での特権ID管理」
  - 「特権ID管理の現状と対策」

  について検討
- 2015年度 執筆
- 2016年1月～5月 最終校正

成果物：6/2～　JNSA　HPにて公開中
「エンタープライズにおける特権ID解説書」（第１版）
http://www.jnsa.org/result/2016/idm_pum/

※ ITRの調査レポート（ITR Market View：アイデンティティ／アクセス管理市場2016）では特権ID管理の市場は伸びており、次年度以降も引き続き拡大するとされている。

エンタープライズにおける特権ID管理目次

目次

クラウド環境における特権管理とは（1）

3.1.1. オンプレミスとの違い

オンプレミスとクラウド環境の違いはいろいろあるが、以下の3点がポイントとなる。

（1）	IaaS、PaaS、SaaSの各レイヤがあり、実現モデルが多岐にわたる。
（2）	サービスの利用者と提供者がおり、登場人物が多数いる。
（3）	マルチテナントが前提。

まず（1）について、クラウドは主にSaaS、PaaS、IaaSといった各レイヤがあるが、ITインフラやITシステムがどのレイヤで運用され、管理されているのかに依存する。下図はIaaS、PaaS、SaaSのクラウドサービスのレイヤを表現したものである。

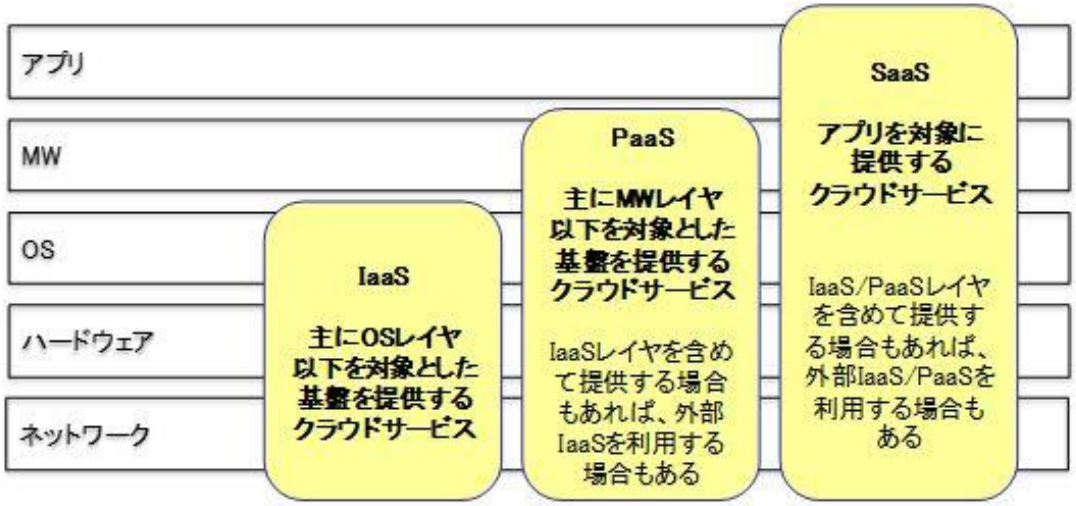
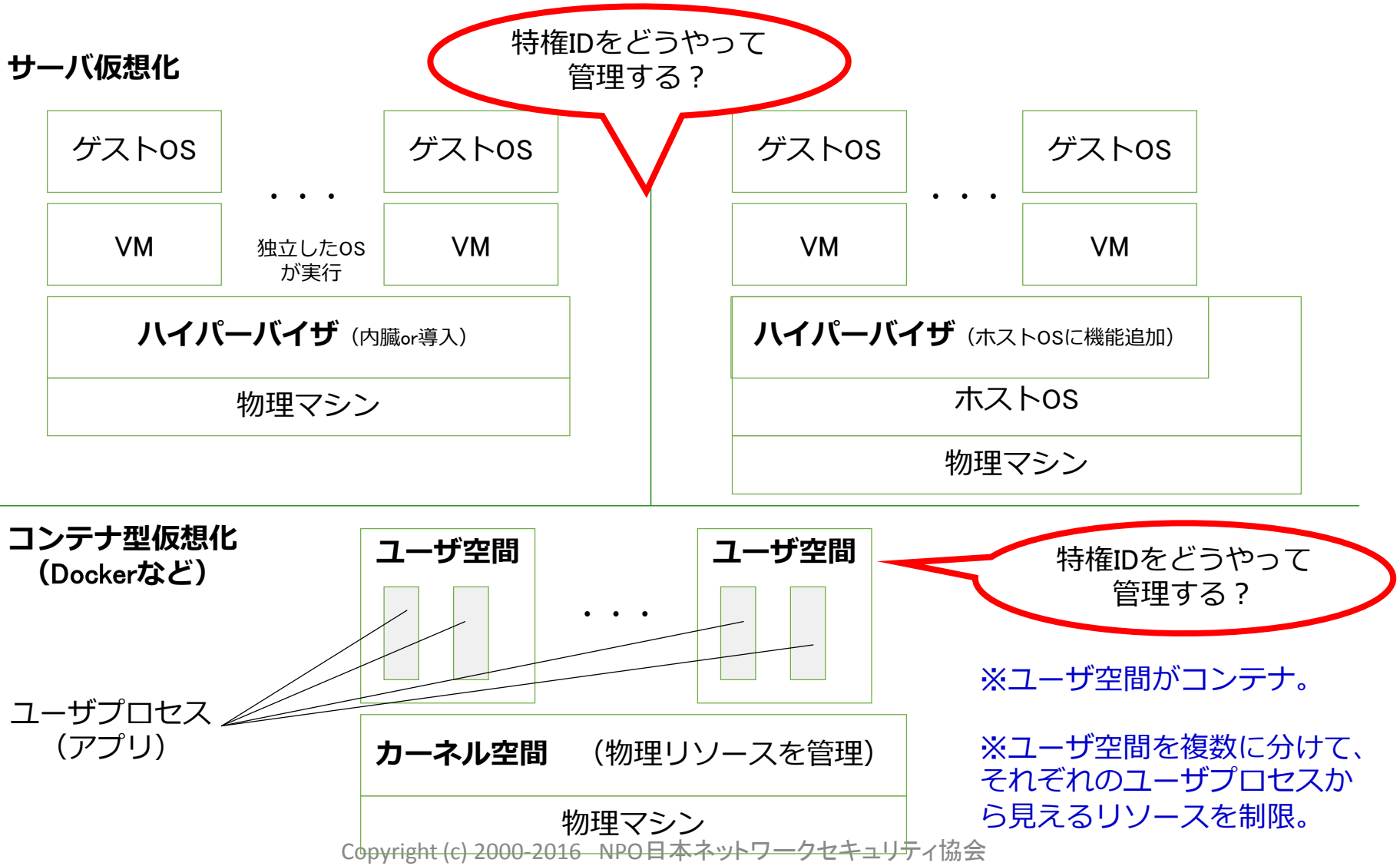
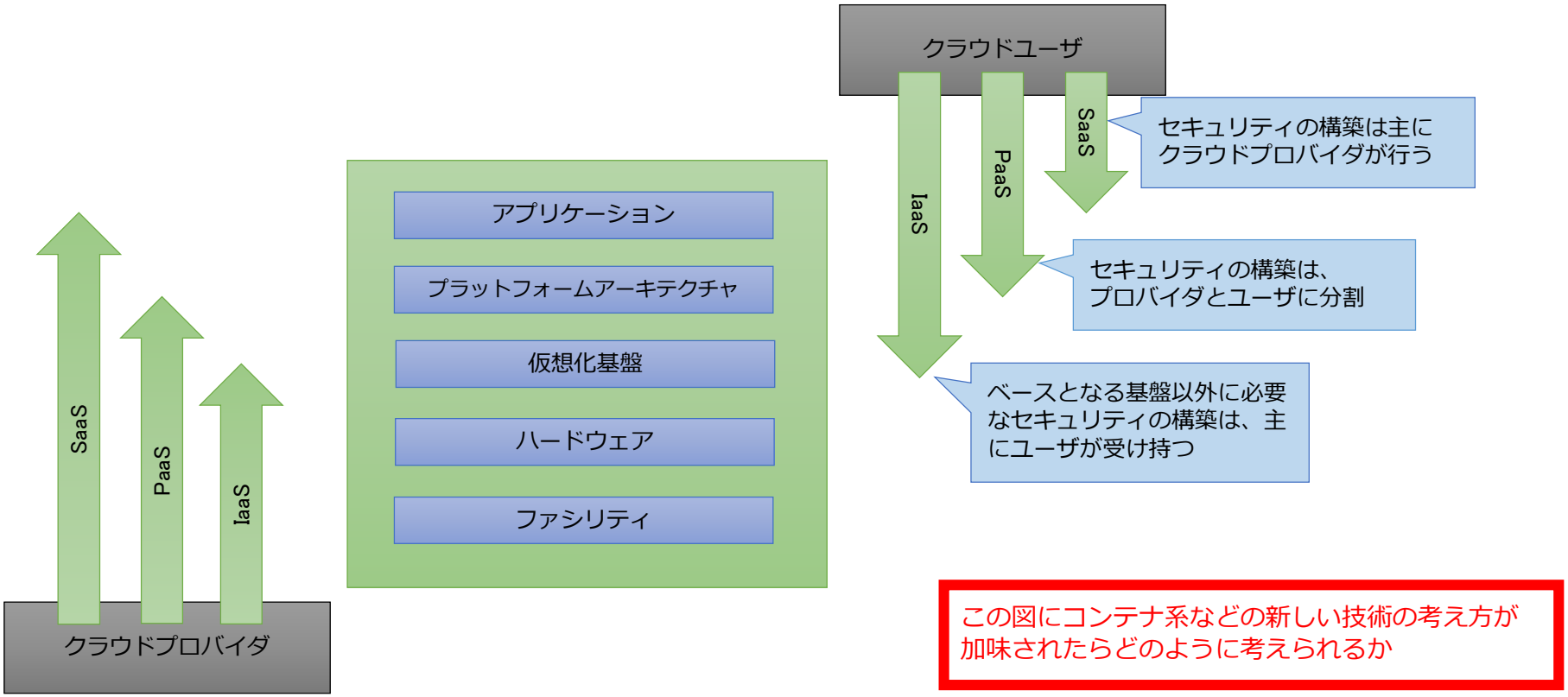


図 3.1 クラウドサービスのレイヤ

クラウド環境における特権管理とは（2）

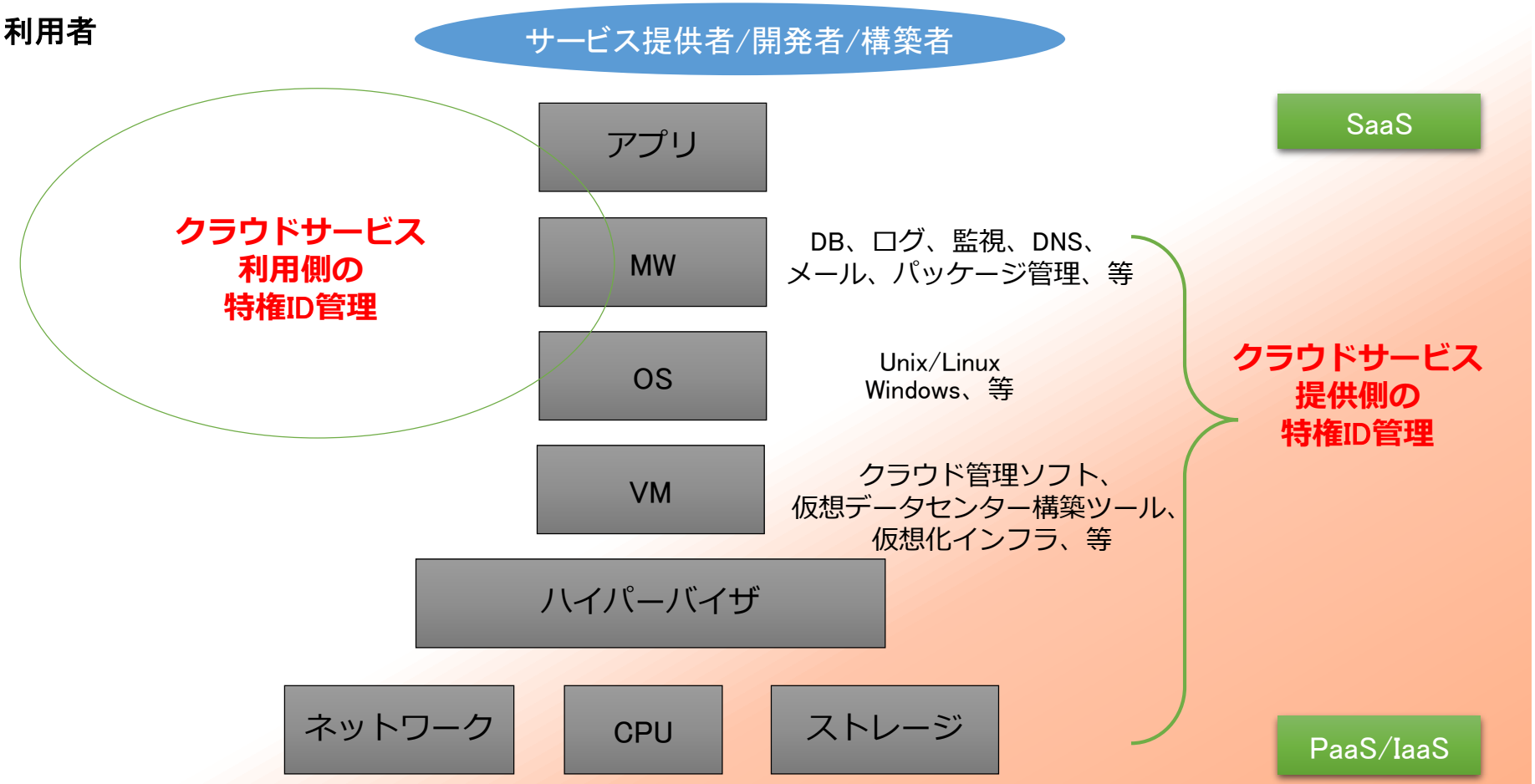


クラウド環境における特権管理とは（3）



出典：NIST パブリッククラウドコンピューティングのセキュリティとプライバシーに関するガイドライン 独立行政法人 情報処理推進機構 訳

クラウド環境における特権管理(4)

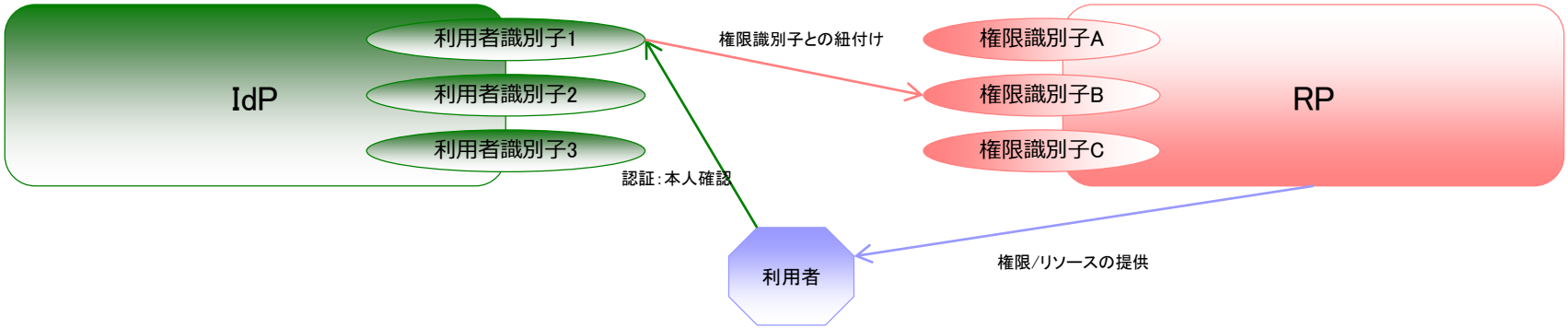


クラウド環境における特権管理(5)

SaaS/PaaS/IaaS/・・・と多層化し複雑化するクラウド環境において、サービス（リソース）を提供する側と提供される側の二面性を持った主体に対する特権の付与を個々のシステムでそれぞれ管理するには限界がある。

提言：ID連携（ID Federation）により解決できるのでは！

RP（リソース側）：リソースに対して権限の識別子
IdP（運用側）：認証後に紐付け



４．エンタープライズロール管理

エンタープライズロール管理解説書改訂

- エンタープライズロール管理解説書
  第2版（2014年7月）の改訂

- 改訂内容の概要
  - 「ロール管理が上手くいっていない状態」の例示
  - ロール管理導入における「落とし穴」の追記
  - ロール管理におけるロールの構造についての検討の実施と追記

検討改訂と成果物

検討経過

- 2015年6月～12月：
  - 第2版へのダメだし。
  - 第3版へ向けた改訂内容の検討
- 2016年1月
  - WG10周年イベントでの、改訂の方向性についての発表
  - 「ロール管理についての「もやもや」」
- 2016年2月～5月
  - 改訂版（第3版）検討、作成
- 成果物：6/2～ JNSA HP 公開中

  「エンタープライズロール管理解説書（第3版）」

  http://www.jnsa.org/result/2016/idm_guideline/

エンタープライズロール管理解説書目次

目次

エンタープライズロール管理解説書見直し事項

成果物:「ロール管理解説書(第3版)」概要

第1章:ロールの定義とロール管理の失敗例(改訂)

- ロールの定義の記述の見直し
- ロール管理の失敗例を加筆

第2章:ロール管理の概要(改訂)

- ロール管理のあるべき姿を分析・検討し、それを実現するための
  ロールの構造のあるべき姿についての加筆
- ロール管理導入における各フェーズの概要を追記

第3章:ロール管理導入指針(第2版の2章)

第4章:ロール管理の運用(第2版の3章)

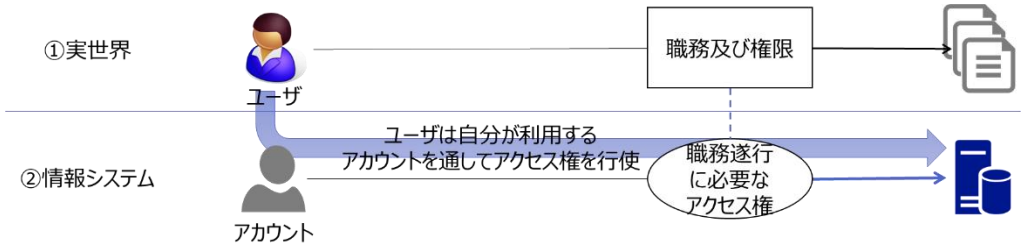
第5章:ロール管理の仮想企業導入事例(第2版の4章)

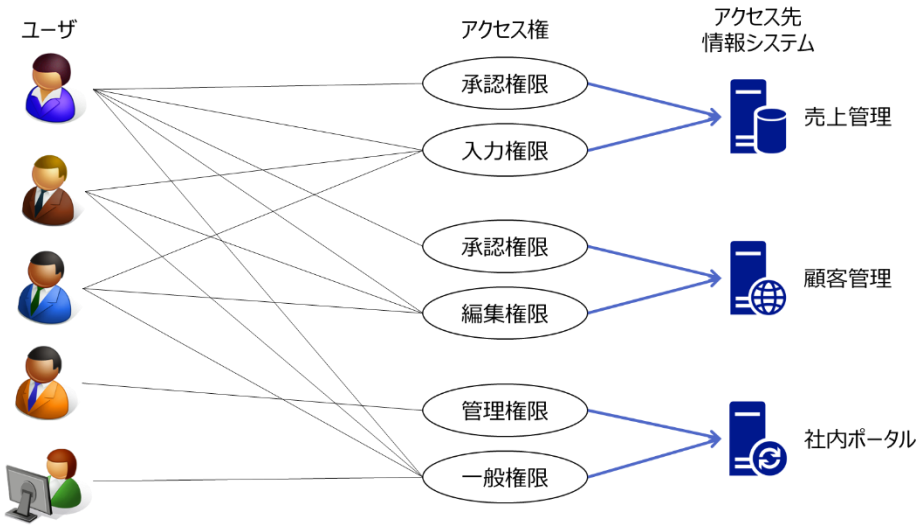
ロール管理の定義と目的(1)

一部抜粋

1．1　ロールの定義とロール管理の目的及び前提条件

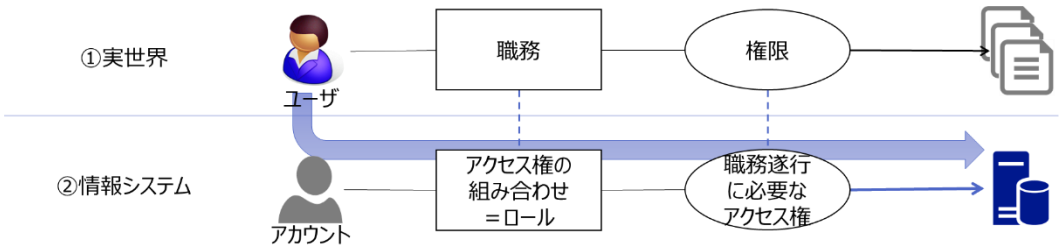
ロールが存在しない場合

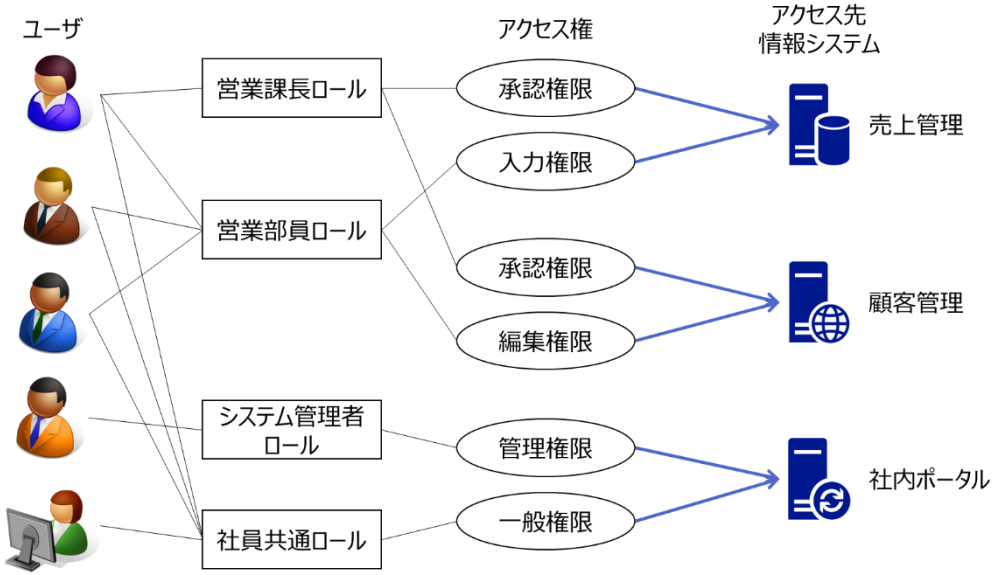




ロール管理の定義と目的(2)

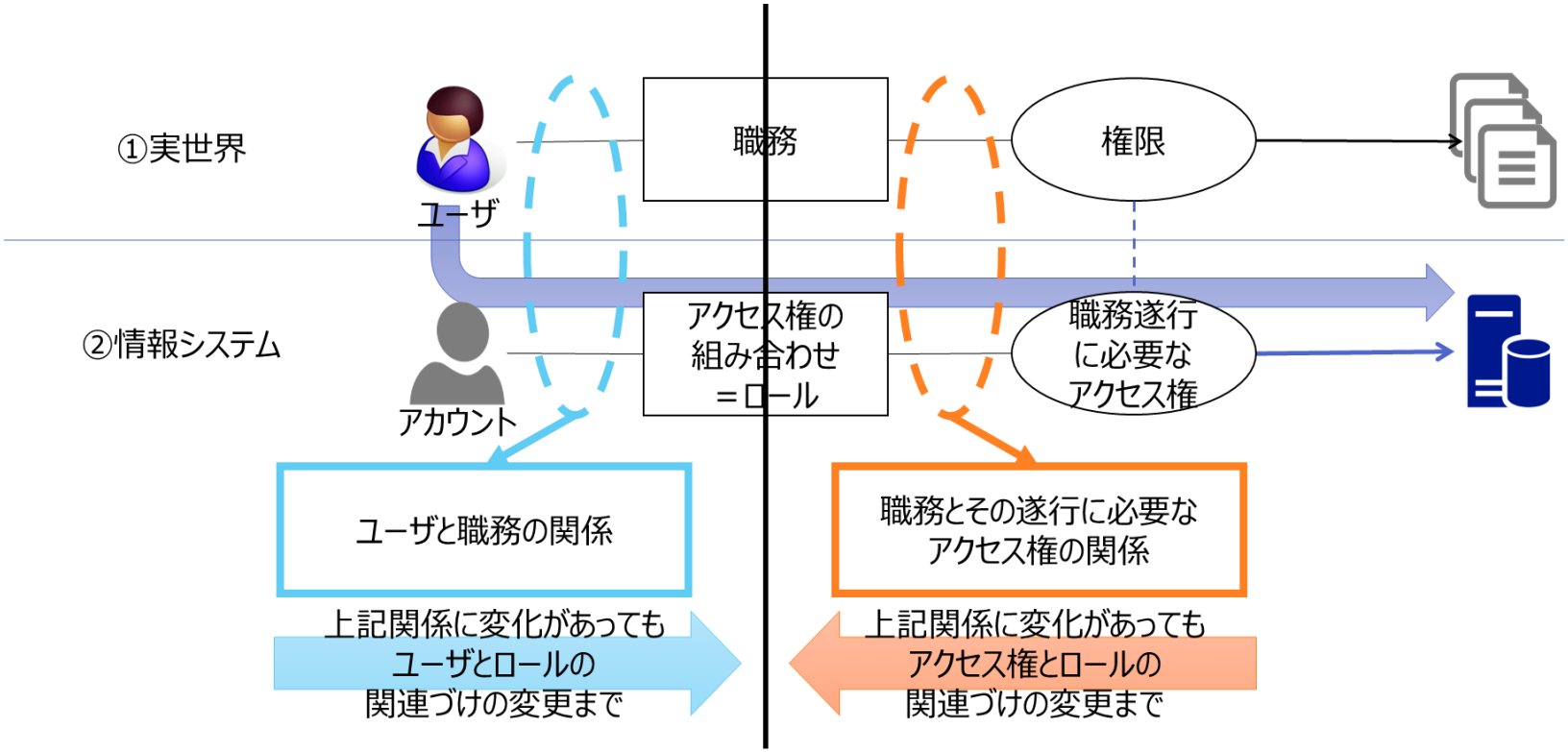
ロールが存在する場合





ロール管理の定義と目的(3)

ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係



５．本年度のテーマ

今年度のテーマ（案）

【テーマ】
1. ID管理チェックリスト作成（CSA Japan協業）
2. アイデンティティとプライバシー勉強会（有識者との懇談）
3. IDの融合と分離の深堀検討（継続）
4. アイデンティティとIoT（IDoT)（新規）
5. ID管理技術勉強会
6. ミニブレスト（即時テーマ）

【その他】
ID&IT2016協賛
その他イベント協賛は随時

WGメンバー紹介

氏 名	所属
宮川　晃一	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
新嘉喜　康治	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	日本電信電話株式会社
山田　達司	株式会社NTTデータ
杉村 耕司	株式会社NTTデータ
篠原　信之	イオンアイビス株式会社
深谷 貴宣	KPMGコンサルティング
齊藤　光司	KPMGコンサルティング
塩田　英二	TIS株式会社
小林 智恵子	東芝ソリューション(株)
栃沢 直樹	トレンドマイクロ株式会社
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
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
酒井美香	日本IBMシステムズ・エンジニアリング
桑田　雅彦	日本電気株式会社
後藤 兼太	日本電気株式会社
内田　健一	NECソリューションイノベータ
工藤達雄	NRIセキュアテクノロジーズ株式会社
深澤　聡	SCSK株式会社
飯塚 昭	日本オラクル株式会社
見上 昌成	日本ビジネスシステムズ株式会社
安納 順一	日本マイクロソフト株式会社
村田　裕昭	日本マイクロソフト株式会社
小野寺 匠	日本マイクロソフト株式会社
佐藤公理	マカフィー株式会社
大竹　章裕	ユニアデックス株式会社
後藤　厚宏	情報セキュリティ大学院大学(教授)
貞弘　崇行	株式会社アイピーキューブ
中島 浩光	サブスクライバ(株式会社マインド・トゥー・アクション)
南　芳明	サブスクライバ(株式会社シマンテック)

計42名
（会社名五十音順）

出版書籍の紹介

書籍名：<改訂新版>
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

出版社：インプレスR&D NextPublishing

形態：電子書籍、Ondemand Print(POD)

販売： Amazon
インプレスR&D libura PRO

http://www.amazon.co.jp/dp/4844395866


JNSA