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

JNSA　2014年度活動報告会

「 2014年度 アイデンティティ管理WG 成果報告 」

富士榮　尚寛
（伊藤忠テクノソリューションズ）

2015 年　6月　9日（火）　ベルサール神田

WG活動報告内容

１．２０１４年度の活動内容

２．IDの融合と分離

３．特権ID管理

４．今年度の活動テーマ

１．２０１４年度の活動内容について

２０１４年度活動内容について

２０１３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．特権ID管理

３．ロール管理

４．IDとプライバシー（勉強会）

５．普及活動および資格制度検討

２０１４年度活動内容について

また、各種セミナー協力、他団体連携を行いました。

１． ID & IT Management Conference 2014 (9/17,9/19)　**協力**

・OpenID EIWG については一旦協力終了
・ID連携トラストフレームワークについては動きがあれば協力する

（今後）
・CSA-J (Cloud Security Alliance Japan ）の協力を模索中

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

検討状況

- 各種の個人アイデンティティを洗い出し、以下を整理
  - ✓個人アイデンティティの特徴
  - ✓個人属性の性質
  - ✓個人アイデンティティの位置付け・関係
  - ✓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、課題

- 2015年度は、2014年度の検討内容の精査・深堀、および課題の解決方法を検討する予定

検討内容、スケジュール

月	検討内容
8月	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、 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
11月	各種個人アイデンティティの位置付け、関係の整理、 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
12月	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
1月	各種個人属性の性質の整理
3月	アイデンティティ結合・融合・分離にかかわる課題の整理、 2014年度のまとめ
2015年度	2014年度の検討内容の精査・深堀、 アイデンティティ結合・融合・分離にかかわる課題の解決方法の考案・検討 （モバイル（スマートフォン）活用における個人アイデンティティの位置づけと課題の整理）

以降、2014年度の検討成果

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

各種個人属性の性質(1/6)

分類	性質	属性(例)
パブリック/プライベートによる分類		
・パブリック(公開)属性	相手を限定せずに公開している属性	所属企業・組織名、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)、
・パブリック(限定公開)属性	限定した一部の人へ公開している属性	個人連絡先(電話番号、メールアドレス等)、顔写真、生年月日、経歴、関心・嗜好、主義、
・プライベート(非公開)属性	他人へ公開していない属性	国民番号(マイナンバ)、本籍所在地、口座番号、カード番号、診療歴、検査結果、遺伝情報、
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	ビジネス用途の(組織としての)正式な属性	所属企業・組織名、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)、
・ソーシャル属性	ソーシャル(社会交流)用途で公開している属性	表示名、個人連絡先(電話番号、メールアドレス等)、顔写真、経歴、スキル、関心・嗜好、主義、
・パーソナル属性	個人用途の属性	口座番号、カード番号、購入履歴、

各種個人属性の性質(2/6)

分類	性質	属性(例)
獲得方法による分類		
・先天的属性	先天的に保有している属性	生体情報、遺伝情報、
・後天的属性(自発獲得)	後天的に自ら獲得・選定した属性	スキル、趣味、関心・嗜好、主義、
・後天的属性(社会付与)	社会的に付与された属性	役職、権限属性、資格、評価情報、
付与主体による分類		
・企業・組織属性	所属企業・組織から付与された属性	所属企業・組織名、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)、
・公的機関属性	公的機関から付与された属性	国民番号(マイナンバ)、住民番号、健康保険被保険者番号、運転免許証番号、口座番号、
・コミュニティ属性	所属コミュニティから付与された属性	役割、権限属性、評判・評価情報、
・消費者属性	消費者として関係のある事業者から付与された属性	通販サイトアカウント、信用情報、アクセス履歴、購入・利用履歴、
・個人獲得属性	個人が自ら獲得した属性	スキル、趣味、関心・嗜好、主義、

各種個人属性の性質(3/6)

分類	性質	属性(例)
存続期間による分類		
・不変属性	一生不変な属性	生体情報、遺伝情報、生年月日、
・期間更新属性	ある長さの期間ごとに変更される属性	パスワード、秘密鍵・公開鍵、
・期間限定属性	ある長さの期間のみ存続する属性	所属企業・組織名、役職名、権限属性、
・連続不定属性	その時々により変更し存続する属性(連続性あり)	位置情報、
・非連続不定属性	その時々により変更し存続する属性(連続性なし)	アクセス履歴、購入・利用履歴、
・一時属性	一時的に存在する属性	キャッシュ情報、cookie情報、状態属性、

各種個人属性の性質(4/6)

分類	性質	属性(例)
可変性による分類		
・不変属性	変更不可能な属性	生体情報、遺伝情報、生年月日、
・可変属性(随時)	随時変更可能な属性	パスワード、連絡先、
・可変属性(指定時)	指定時に変更可能な属性	サービス特典属性、
・可変属性(個人設定)	個人自ら変更可能な属性	趣味、関心・嗜好、
・可変属性(付与主体設定)	付与主体が変更可能な属性	権限情報、信用情報、

各種個人属性の性質(5/6)

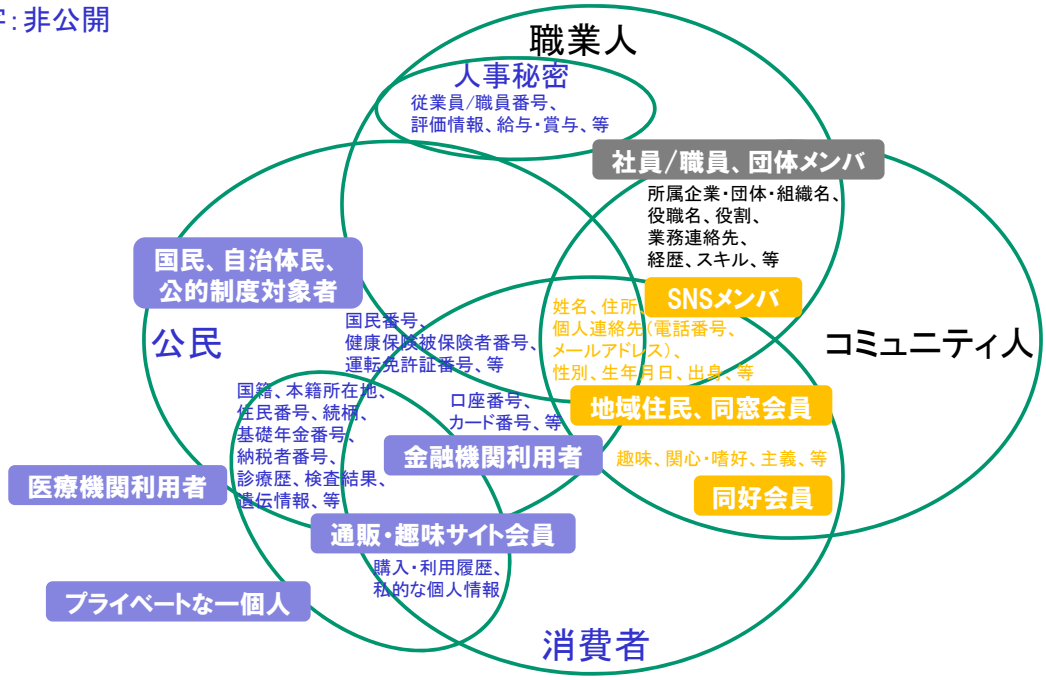
分類	性質	属性(例)
識別性による分類		
・個人識別・特定属性	個人を識別可能かつ特定可能な属性	国民番号(マイナンバ)、姓名、住所、電話番号、アカウント名、生体情報、
・個人識別・非特定属性	個人を識別可能だが、特定は不可能な属性	購入・利用履歴、
・個人識別不可属性	個人を識別不可能な属性	性別、生年月日、
表意性による分類		
・表意属性	属性値そのものが表意的な属性	スキル、趣味、関心・嗜好、主義、住所、役割、
・非表意属性	属性値そのものは意味不明な属性	各種番号、

各種個人属性の性質(6/6)

分類	性質	属性(例)
用途要件による分類		
・個人識別用属性	個人を識別するための属性	社員番号、アカウント名、生体情報、
・個人認証用属性	個人を認証するための属性	パスワード、生体情報、秘密鍵、
・認可用属性	認可の可否を判断する基になる属性	権限属性、資格、
・制御用属性	処理を制御する基になる属性	関心・嗜好、アクセス履歴、
・表示用属性	画面や印刷物に表示するための属性	アカウント名、姓名、
・消費性向属性	消費者としての個人の性向を表す属性	アクセス履歴、購入・利用履歴、趣味、関心・嗜好、主義、

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



個人アイデンティティの結合・融合にかかわるメリット／デメリットの洗い出し（１）

立場	結合・融合のメリット	結合・融合のデメリット	備考
本人	• アイデンティティの使い分けが不要になる • アイデンティティの種別ごとに個人属性を登録・更新しなおす必要がなくなる	• アイデンティティの種別ごとに個人属性の見せ方を変えるのが難しくなる • 公開/非公開の区分をすべての用途から考慮する必要が生じる • 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くなる	
所属企業/団体	• 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）管理する必要がなくなる • 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/団体が個別に管理する必要がなくなる（国民番号のみを管理すればよくなる等）	• 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	
公的機関	• 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）管理する必要がなくなる • 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、把握しやすくなる	• 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	

個人アイデンティティの結合・融合にかかわるメリット／デメリットの洗い出し（２）

立場	結合・融合のメリット	結合・融合のデメリット	備考
コミュニティ及びコミュニティメンバ	• 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）管理する必要がなくなる • 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管理する必要がなくなる（国民番号のみを管理すればよくなる等）	• 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	
消費者向け事業者	• 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）管理する必要がなくなる • 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管理する必要がなくなる（国民番号のみを管理すればよくなる等）	• 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	

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）

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）

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。

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・深堀
  - 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を検討・考案
  （～2015年度末を目標に）

3．特権ID管理

特権ID管理の検討課題

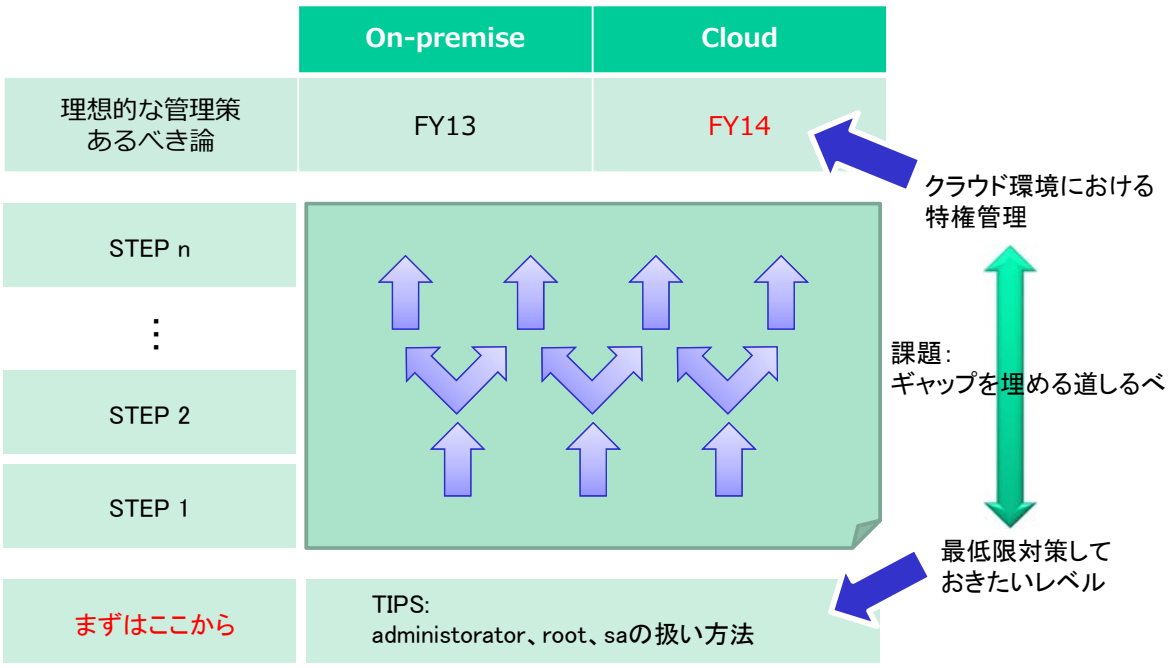
特権IDの現状の深掘りと管理策

✓ 特権ID利用の現状に対する管理策

クラウド環境における特権ID管理

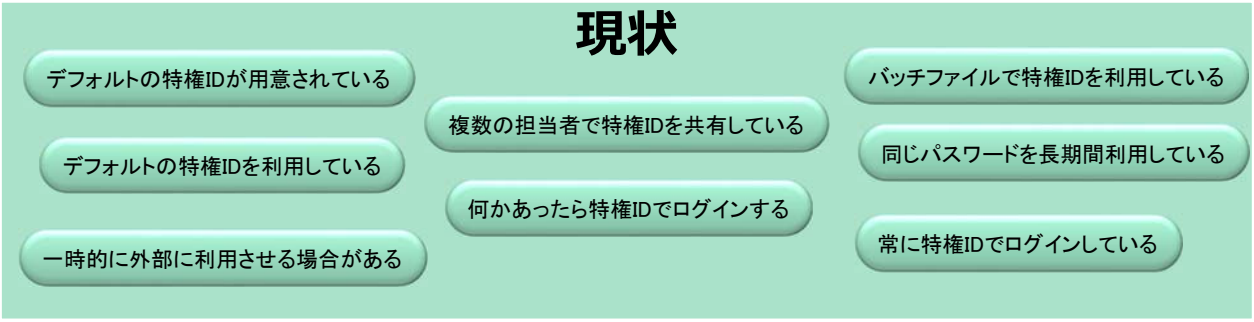
✓ IaaS, PaaS等各種サービス形態における特権ID管理

特権ID管理　まとめ方全体マップ



特権IDの現状の深堀と管理策

特権ID管理のあるべき論は、昨年度検討してきた。



現状のままの運用していた場合の問題点についても整理を行った。
今年度は、現状の深堀として

・なぜそうしてしまっているのか
・現実的な落としどころ →管理策

を検討し、できることから始められる管理策を整理する。

「特権ID」こんな使い方してませんか？

特権IDは、与えられた権限が大きいため（強いため）便利に使えます。
特に製品の出荷状態から設定されている特権IDは、初期設定作業のためにすべての権限を付与されている場合もあります。そして、初期設定が終わってからもそのまま使い続けてしまいがちです。

製品にビルドインされた特権IDを構築作業時にベンダーが設定したパスワードのまま、複数名のIT担当者が共有で常時利用している。

ついつい、このような使い方をしてしまっていませんか？

- 製品にビルトインされているアカウントを使っている。
- 構築作業時にベンダーが設定したパスワードがそのままになっている。
- 不特定多数のユーザが使っている。
- 何でもできる便利なアカウントとして常用している。
- 連携用として複数のシステムで共有している。
- 長期間同じパスワードで利用してる。
- 同じパスワードを複数のシステムで使いまわしている。
- 類推しやすいパスワードを設定している。

特権IDの現状と対策　①

製品にビルトインされているアカウント（特権ID）を使っている

パスワードも出荷状態のままだったり

理由/背景：
あらたに設定することが面倒！
設定しても、特権IDの利用頻度が低いから、忘れそうなのでそのまま製品上設定できない

脅威：
製品にビルトインされている特権を持ったIDは、初期パスワードを含めインターネット上に情報として公開されてしまっているケースがほとんどです。IDと初期パスワードが一般に知られてしまっている状況ですので、パスワードの秘匿だけが保護の手段となります。

対策：
パスワードは初期値から必ず変更（空白の場合は設定）することを強くお勧めします。
また、システム上可能な場合は無効化することも有効です。
パスワードの持ち主を決めて、変更後のパスワードがわからなくならないようにしましょう。

特権IDの現状と対策　②

構築作業時にベンダーが設定したパスワードがそのままになっている。

理由/背景：
変更することが面倒だ、変更することを忘れていた！
いざというときにベンダーに調査を依頼したいのでそのままにしておきたい。
パスワードの管理はベンダーに任せている。
ID/パスワードを払い出す仕組みがない。

脅威：
パスワードを知っているベンダー側のエンジニアが誰かを把握することが困難です。そのためパスワードがどのように伝播するかコントロールできなくなります。別の作業時に勝手にアクセスされても把握しにくい状況に陥ります。

対策：
作業毎にIDを払い出し、作業後はベンダーに払い出したIDを無効/削除する、もしくはパスワードを変更するなどを行い、意図しないところでアクセスされないようにしましょう。

特権IDの現状と対策　③

不特定多数のユーザが使っている。

理由/背景：
管理者個別にIDを発行することが面倒だ！
特権を持ったIDを多く発行することに抵抗がある！

脅威：
IDを共有してしまうと、実際に誰が利用したか把握ができなくなります。万が一不正アクセスがあった場合に利用者の特定が困難です。

対策：
一般ユーザとしてログインしたあと、特権を付与する機能（sudoやrunas）を活用しましょう。

→不特定多数って何人？
貸し出しの管理台帳で管理。

特権IDの現状と対策　④

何でもできる便利なアカウントとして常用している。

理由/背景：
オペレーションごとにIDを使い分けることが面倒だ！
アプリケーション・プログラムも特権IDアカウントを利用しているため、あまり意識をしていない。
IDを分けるにしても、アプリケーションごとにどういった権限を与えればよいのかわからない。

脅威：
何のためにそのIDでアクセスしてきたのかを特定することが困難です。
アプリケーション・プログラムがアクセスするIDと同様のIDで管理者がアクセスをした場合に、アクセスの要因をトレースすることが困難です。
オペレーション上不必要な権限を持つIDの利用による人的ミスによる障害を誘発する可能性があります。

対策：
特権を持つIDを付与するユーザは必要最低限としましょう。また、複数名でのIDの使いまわしはやめましょう。
予め想定できるオペレーション権限を策定し、適切な管理者に対してのみ最低限の権限を付与するようにしましょう。

特権IDの現状と対策　⑤

連携用として複数のシステムで共有している。

理由/背景：
他システム側が、処理に必要な権限が何かを把握しておらず、特権IDでとりあえず何とかしたい
連携用IDに求められる権限がわかっていたとしても、専用のIDを一々準備できない
連携用のIDの利用ルールを事前に定めておらず、それぞれ勝手にパスワードまでプログラムに書き込んでしまった！

脅威：
IDとパスワードが連携対象のシステム側に渡るため、そこからパスワードがもれる可能性があります。
複数のシステムで共有しているため、パスワードの変更に対応できない使い方をするシステムがひとつでもあると、パスワードの変更そのものが困難になり、漏えいのリスクが高まります。

対策：
パスワードを使う場合は定期変更が可能な実装をする、あるいは、証明書認証を使い証明書の更新プロセスを決めておくなど連携用IDの利用ルールを事前に決めておきましょう。
パスワードを保管する場合は、暗号化やファイルへのアクセス制御などを行うようにしましょう。

特権IDの現状と対策　⑥

長期間同じパスワードで利用してる

理由/背景：
一度設定したパスワードを変更すると周知が面倒
変更した際のシステムへの影響が不明なため、変更できない。

脅威：
異動や退職により、管理者の任が解かれた人がアクセスできる手段を知っていることになります。トラブルによる退職者の逆恨みによる不正アクセスの事件などが実際に起きています。

対策：
パスワード自体を解読される可能性を減らすため、または解読されたり、知られてしまったため進入を許すなどの被害を最小限に抑えるという点で、パスワードを利用後に変更（使い捨て）することが有効です。
連続したアクセス試行に回数制限を設定するなどの方策も有効です。

特権IDの現状と対策 ⑦

複数のシステムの特権IDに同じパスワードを設定している。

理由/背景：
それぞれのシステムで個別に特権IDのパスワードを設定すると管理が面倒！

脅威：
一つのシステムの特権IDのパスワードが漏れてしまうと、複数のシステムの特権が奪われることになります。

対策：
各システムで個別のパスワードを設定しましょう。被害を最小限に食い止めることができます。
パスワードの一部にホスト名の頭文字を付けるなど、使いまわしを防止しながらも管理しやすい生成ルールを考える方法などがあります。

特権IDの現状と対策 ⑧

特権IDに簡単な（類推しやすい脆弱な）パスワードを設定している

理由/背景：
特権IDに複雑なパスワードを設定すると忘れてしまいそう！
システムの仕様でパスワードに設定可能な文字種や文字数の制限がある。

脅威：
インターネット上には、パスワード解析のためのツールや辞書が出回っており、脆弱なパスワードではすぐに解読されてしまう可能性が高く、不正アクセスを防ぐ効果が下がります。

対策：
類推しにくいパスワードを設定しましょう（SplashData社 “Worst Passwords” List等にランクインしているパスワードは設定しない）。複雑さを維持しながら管理しやすいパスワード生成方法などを利用して、パスワードを設定しましょう。システム仕様上での制限がある場合は、ネットワークや物理的（サーバールームへの入退出）な制限を組み合わせて管理しましょう。

ユースケース

【組織プロファイル】
IT部門メンバー数：10名（派遣社員6名）
システム数（サーバー数）：100

【現状】
複数のシステムに対し、製品にビルドインされた特権IDを構築作業時にベンダーが設定したシステム共通パスワードのまま、複数名のIT担当者が共有で常時利用している。

【このままでは！】
ビルドインされた特権IDは、普段の運用管理のオペレーションに必要な権限に対して、必要以上に権限を持っていることが多いです。そのため、常時利用が故の人的ミスによる障害を誘発する恐れがあります。
ベンダーが設定したままのパスワード、また特権IDの共有は、社内にも社外にも複数名システムへアクセスできる人が存在することになり、万が一の不正アクセスされた場合に、特権ID利用者の把握ができなくなります。

【対策】
システムそれぞれのビルドインされた特権IDに対して、ベンダーが設定したパスワードから個別の複雑性の高いパスワードを設定しましょう。
システムの仕様によっては、ビルドインされた特権IDを無効にできるので必要以外のときは無効化にしておきましょう。
複数人のシステム管理者で運用を行う場合は、個別にユーザアカウントを必要最小限の権限付与で作成しましょう。

クラウド環境は従来と何が異なるのか

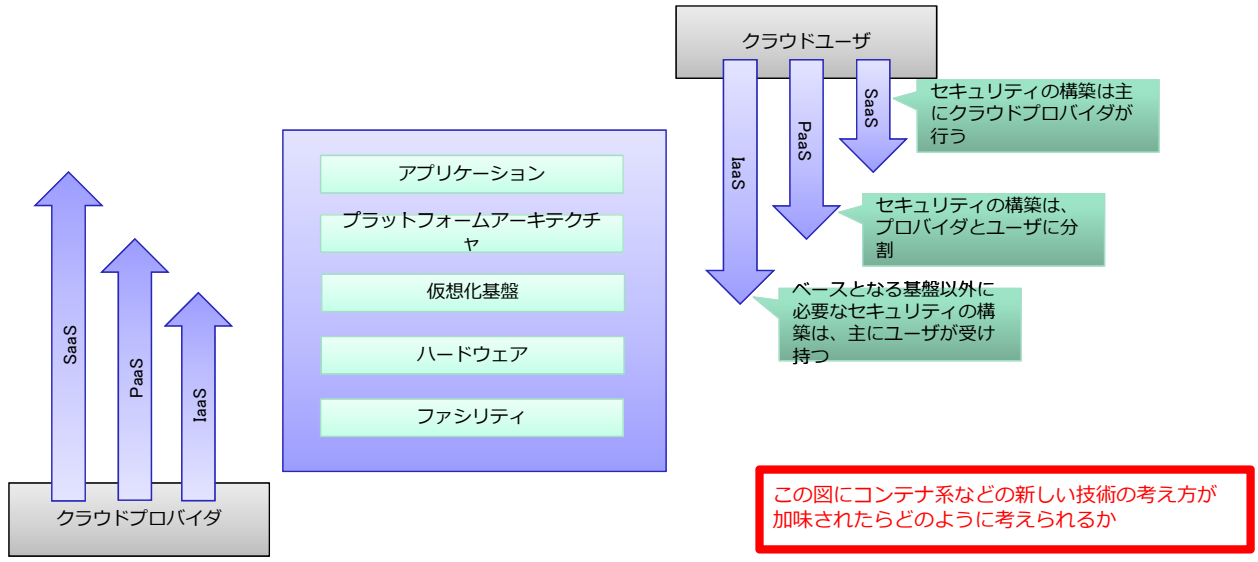
オンプレミス環境との違い

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

サーバ仮想化からさらなる発展

- サーバ仮想化ではハイパーバイザ上での管理が主流となる。（例：クラウド上のリソースをセルフポータルで管理など。）
- コンテナ型対応はユーザ空間が複数なのでリソースを制限し、複数コンテナの管理が求められる。（例：マルチテナント型のアプリを提供する場合、そのアプリに必要なプロセスだけを含む複数コンテナを起動するなど。）

（参考）クラウドサービスモデル



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

特権ID管理が複雑化

クラウドになり、対応が難しくなった

- 所有と利用の混在　→　分離が必要
- ハイブリッドクラウド環境への対応
  - （例）自社IaaSを外部IaaSに切り替え

契約や運用面の変化

- サービス利用者と提供者（開発者も含む）の役割
- 法人をまたいだ管理者

技術面の変化

- 各レイヤ（IaaS/PaaS/SaaS）での管理の必要性
- 縦方向と横方向
- コンテナ系などの新しい考え方

どのような特権ID管理があるか

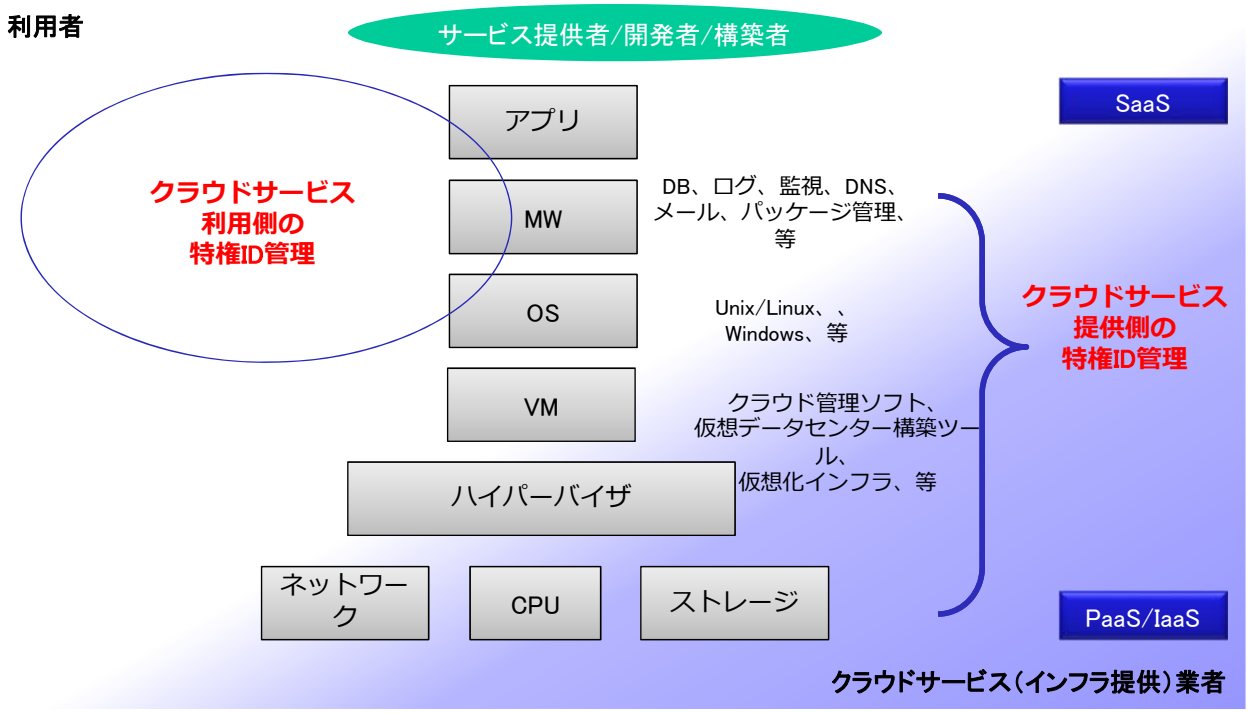
SaaSアプリを中心とした特権ID管理

- 払い出された仮想環境の運用
- テナント単位のID管理
  - SaaSアプリ利用者
  - SaaSアプリ開発者
  - SaaSアプリ運用／仮想環境運用者

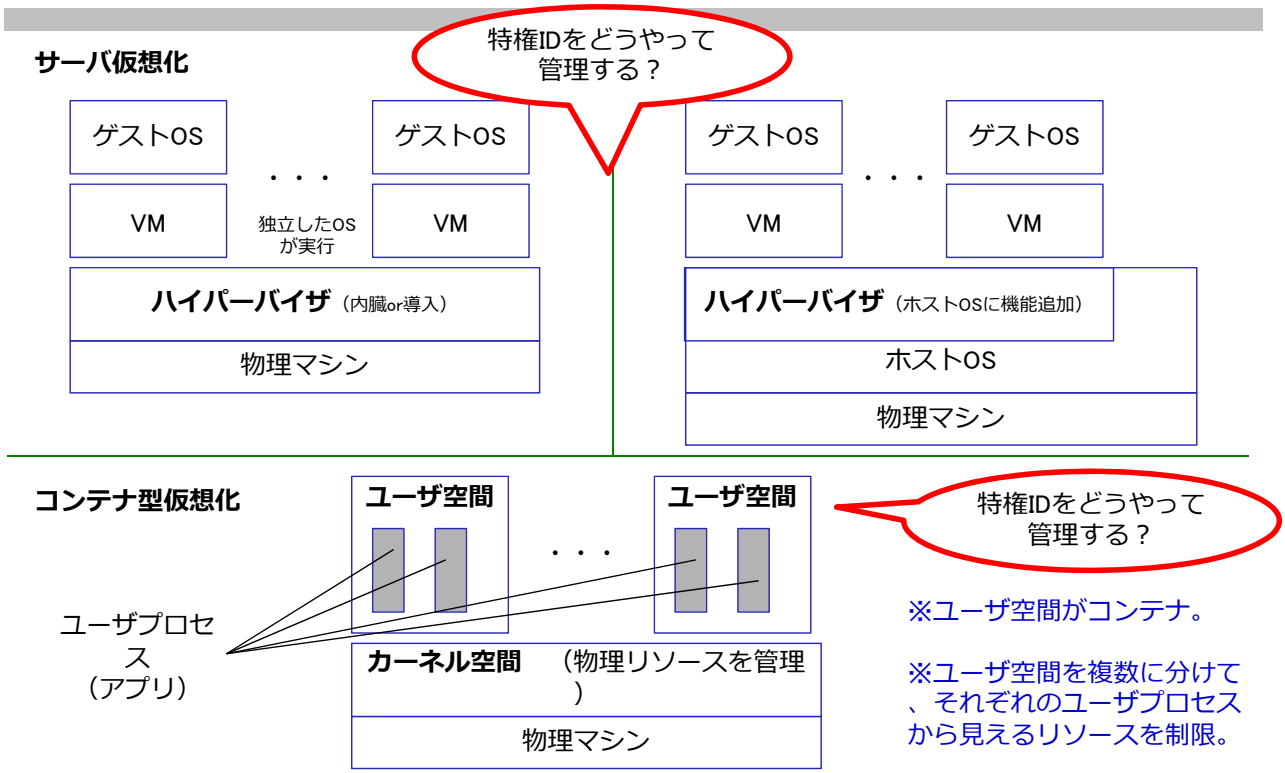
PaaS/IaaSを中心としたクラウド基盤の特権ID管理

- 払い出すための仮想環境の運用
- VMやハイパーバイザでのID管理
- コンテナでのID管理

クラウド環境における特権ID管理（イメージ）



サーバ仮想化 VS コンテナ型仮想化（イメージ）

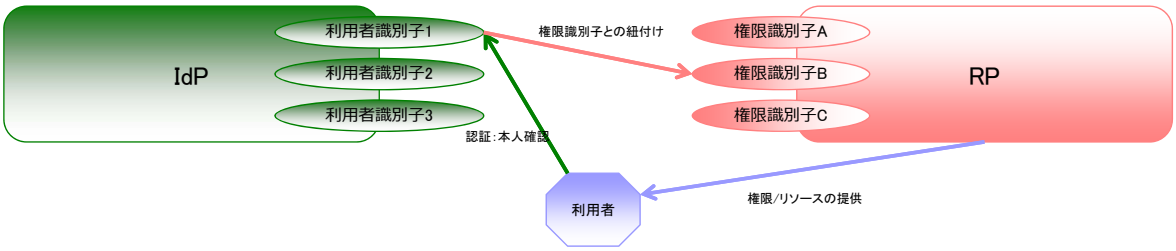


ID連携（IDフェデレーション）の活用

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．今年度のテーマ

今年度のテーマ（案）

１．「クラウド環境におけるアイデンティティ管理」書籍改定
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．エンタープライズロール管理改訂（継続）
４．IDの融合と分離の課題検討（継続）
５．ID管理チェックリスト作成（新規）
６．情報発信活動（資格制度、HP作成）（新規）

（その他）
・WG設立10周年記念パーティー企画

＊現在、新規メンバー募集中！　６／１２（金）１７時まで！

詳細はＪＮＳＡ事務局まで！

WGメンバー紹介

2014年度 アイデンティティ管理WGメンバー

	氏名	所属
1	宮川　晃一	日本ビジネスシステムズ株式会社
2	富士榮　尚寛	伊藤忠テクノソリューションズ株式会社
3	稲吉　英宗	伊藤忠テクノソリューションズ株式会社
4	新嘉喜　康治	伊藤忠テクノソリューションズ株式会社
5	木村　慎吾	インテック
6	駒沢 健	NTTコムウェア
7	杉村 耕司	株式会社NTTデータ
8	南　芳明	株式会社シマンテック
9	貞弘　崇行	サブスクライバ
10	見上 昌成	JBSソリューションズ（日本ビジネスシステムズ）
11	小林 智恵子	東芝ソリューション（株）
12	栃沢 直樹	トレンドマイクロ株式会社
13	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
14	福原 幸一	富士通関西中部ネットテック株式会社
15	塩田　英二	TIS株式会社
16	酒井美香	日本IBMシステムズ・エンジニアリング
17	山端 祐子	日本アイ・ビー・エム株式会社
18	桑田　雅彦	日本電気株式会社
19	後藤 兼太	日本電気株式会社
20	安納 順一	日本マイクロソフト株式会社
21	中島 浩光	株式会社マインド・トゥー・アクション（サブスクライバ）
22	佐藤公理	マカフィー株式会社
23	大竹　章裕	ユニアデックス株式会社
24	後藤厚宏	情報セキュリティ大学院大学（教授）

計24名（順不同）

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