特権IDの取扱い

「特権IDの取り扱いの現状と見直し」
と
「クラウド環境における特権ID管理」

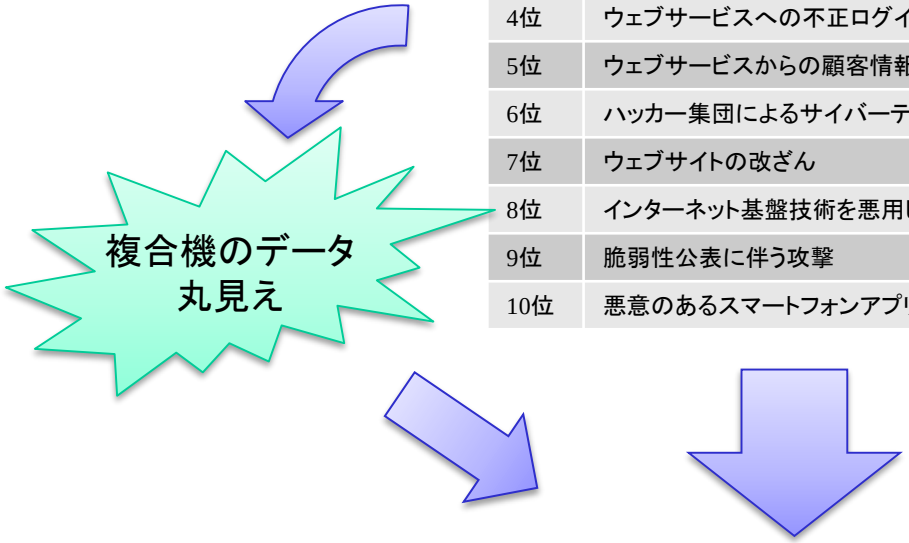
情報セキュリティの現状

■ 最近もいろいろNEWSになっています。

順位	情報セキュリティ10大脅威 2015
1位	インターネットバンキングやクレジットカード情報の不正
2位	内部不正による情報漏洩
3位	標的型攻撃による諜報活動
4位	ウェブサービスへの不正ログイン
5位	ウェブサービスからの顧客情報の窃取
6位	ハッカー集団によるサイバーテロ
7位	ウェブサイトの改ざん
8位	インターネット基盤技術を悪用した攻撃
9位	脆弱性公表に伴う攻撃
10位	悪意のあるスマートフォンアプリ

IPA：情報セキュリティ 10大脅威2015から

順位	情報セキュリティ10大脅威 2015
6位	ウイルスを使った詐欺・恐喝
7位	サービス妨害
8位	無線LANの無断使用・盗聴
9位	ネット上の誹謗・中傷・いじめ
10位	悪意のあるアプリを使った遠隔操作
16位	利用者情報の不適切な取り扱いによる信用失墜
17位	不適切な情報公開
18位	不正請求詐欺
19位	過失や災害による情報漏えいやサービス停止



色々と高度な対策製品が出ています！　　…でも。

おさらい：特権ID管理とは。

rootやAdministrator, adminなどのOSやミドルウェアに予め組み込まれたユーザーアカウント、sysやsystem, saなどDBMS（データベースマネジメントシステム）に用意されているDBA（データベースアドミニストレータ）など

特権ID：
システムの維持・管理のために利用するIDであり、システムの利用目的（業務目的）以外で利用するすべてのID

「業務目的で利用されるIDに対して付与される権限の高さ、大きさ」の管理 ⇒**ロールマネジメントへ**

おさらい：一般IDと特権IDの違い

一般IDと比べた場合の特権ID特徴	影響
権限範囲が広い	不正アクセスや誤操作等が発生した場合、一般IDに比べ、大きな被害になりやすい
デフォルトでIDが用意されいてる	IDが広く知られているため、パスワード攻撃を受けやすい
運用上、共有IDになりやすい	利用者の識別が難しいため、監査ができない。パスワードが変更しにくい
IDのライフサイクルが異なる	一般IDのライフサイクルは人に紐づくことに対して、システムの寿命に紐づく

特権IDを取り巻く現状

デフォルトの特権IDが用意されている

複数の担当者で特権IDを共有している

バッチファイルで特権IDを利用している

デフォルトの特権IDを利用している

同じパスワードを長期間利用している

一時的に外部に利用させる場合がある

何かあったら特権IDでログインする

常に特権IDでログインしている

何が問題か

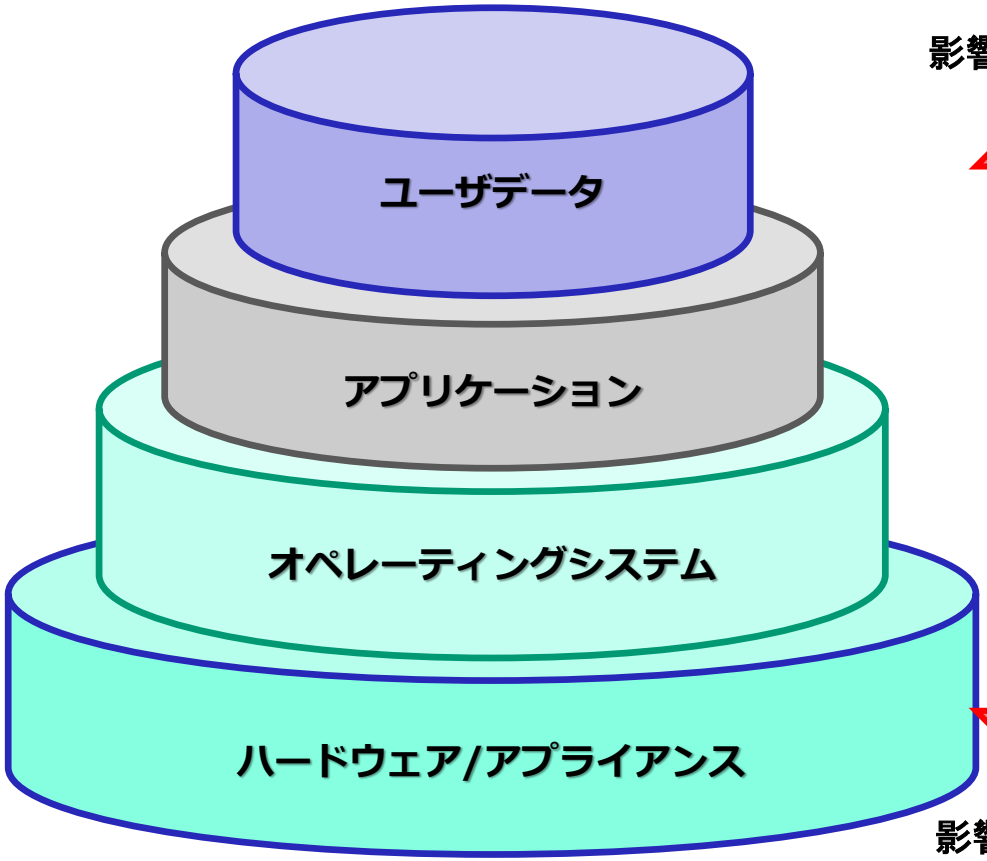
誤用 操作ミスによる障害発生

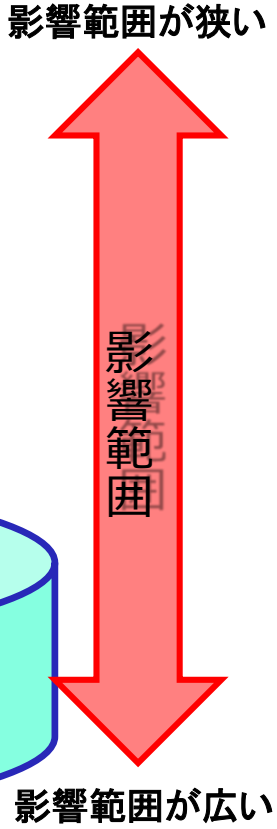
乱用 過度な操作

故意 悪意を持った操作

監査 誰がいつ、操作したか不明

特権IDの影響度（レイヤ）





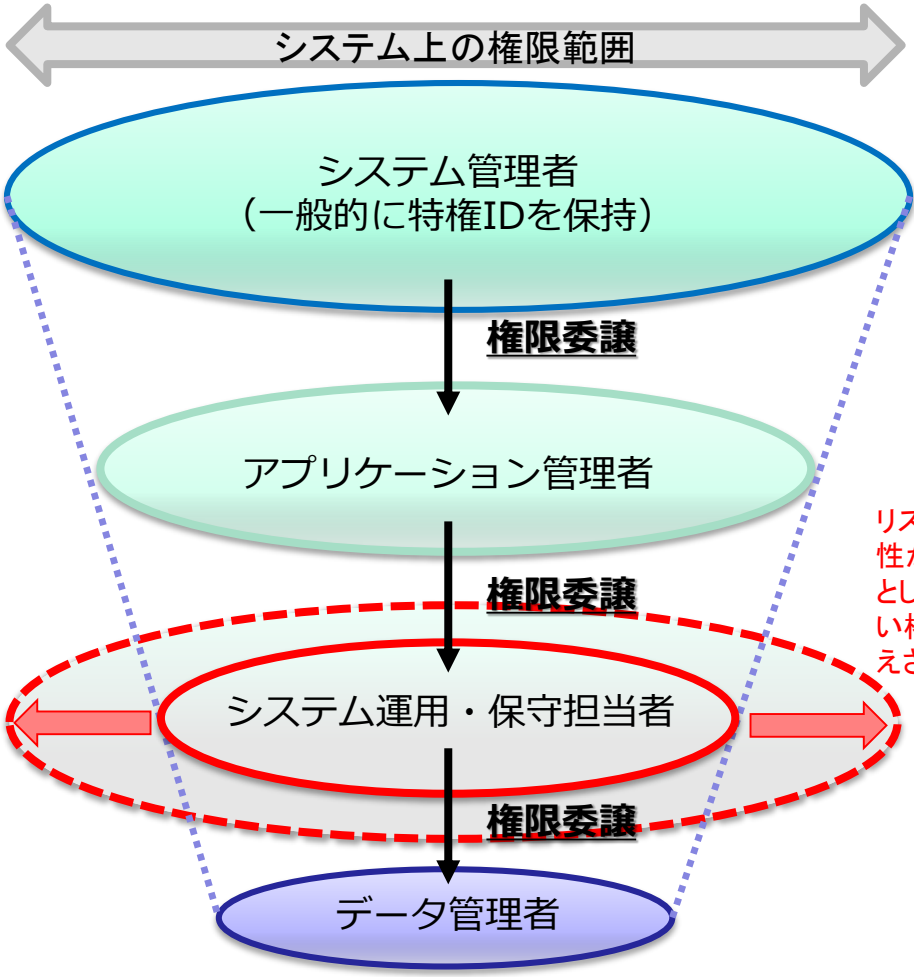
特権IDが奪取された場合の影響

奪取された特権IDがどのレイヤで利用されているものかによって、システムに与える影響度が大きく異なる。

下位レイヤが上位レイヤに与える影響

一般的により下位レイヤー（ハードウェア基盤に近い層）のIDが奪取された場合には、それよりも上位のレイヤーへの制御・改竄・破壊などが可能となるため、システムへの影響は相対的に大きい。

特権IDの影響度（利用用途）



リストアなどの必要性から、業務ロールとしては与えたくない権限レベルを与えざるを得ない。

権限の拡大

保守要員など運用上の権限範囲が本来は狭いメンバーに対して、ハードウェアやOS障害時を想定した場合に、特権IDまたはそれに相当する権限を保持するIDを割り振らざるを得ない状況が発生する。

システム的な制限だけではなく、「社内規定」、「運用手順書」、「承認フローの遵守」など運用ルールの確率、さらにログ管理によるトレーサビリティの確保により、想定外の作業事故や故意の不正アクセスなどを抑制する努力も必要となる。

特権IDの取扱い

特権IDの取り扱いの現状と見直し

「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。

例）ツール

環境	ツール	利用イメージ
UNIX/Linux	su コマンド	一般ユーザでログイン → su コマンドにより特権IDへ移行
	sudo コマンド	一般ユーザでログイン → sudo コマンドにより特権でコマンド実行
Windows	ranas コマンド	一般ユーザでサインイン →ranas コマンドにより特権でコマンド実行
ネットワーク機器	enable コマンド	ユーザモードでログイン →enable コマンドにより特権モードへ移行
	administrator コマンド	ユーザモードでログイン →administrator コマンドにより特権モードへ移行
DBMS	connect コマンド	一般ユーザでログイン → connect コマンドによる特権IDで接続

環境	ツール
Windows クライアント端末	LAPS（Local Administrator Password Solution

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

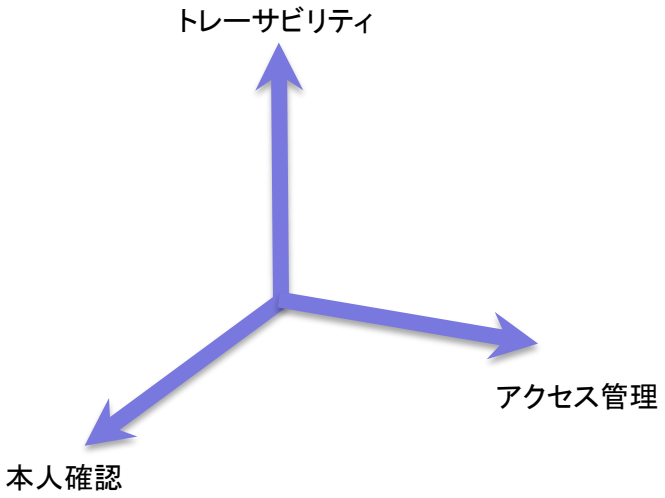
理由/背景:
特権IDに複雑なパスワードを設定すると忘れてしまいそう！
システムの仕様でパスワードに設定可能な文字種や文字数の制限がある。

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。

特権ID管理で

- システム組み込みまたはオプション機能によるアクセス管理強化（権限最小化）
- 本人確認の強化
- トレーサビリティの確保



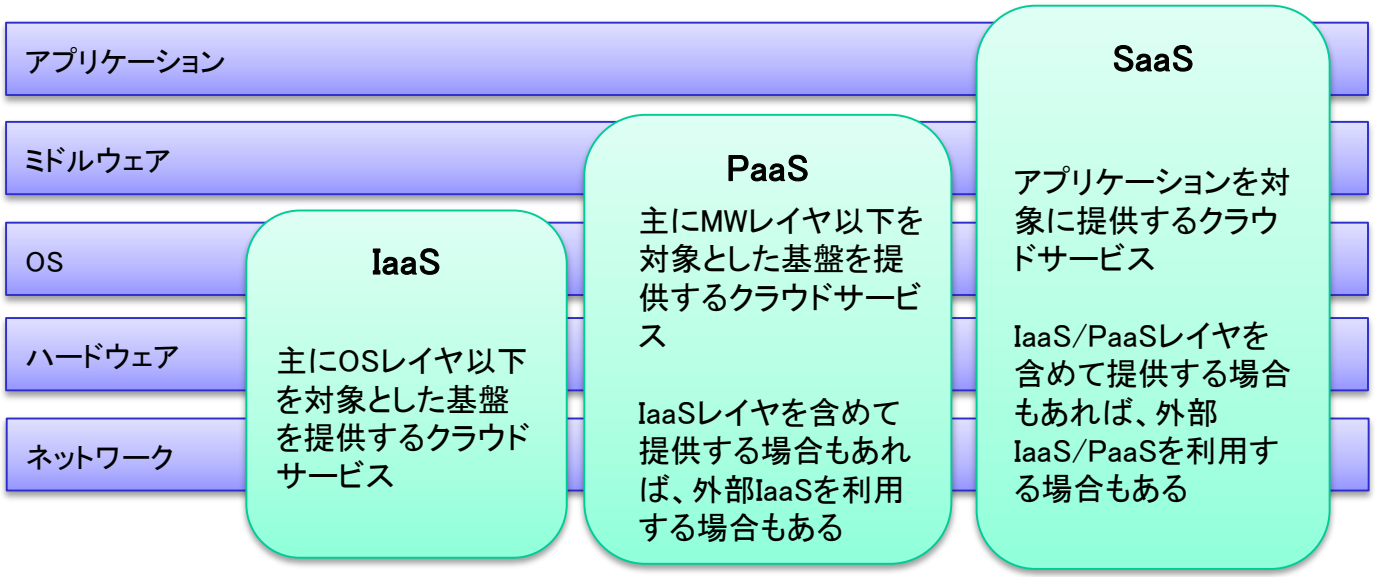
特権IDの取扱い

クラウド環境における特権ID管理

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

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（開発者も含む）がおり、登場人物が多数いる
3. マルチテナントが前提



クラウドサービスのレイヤ表現

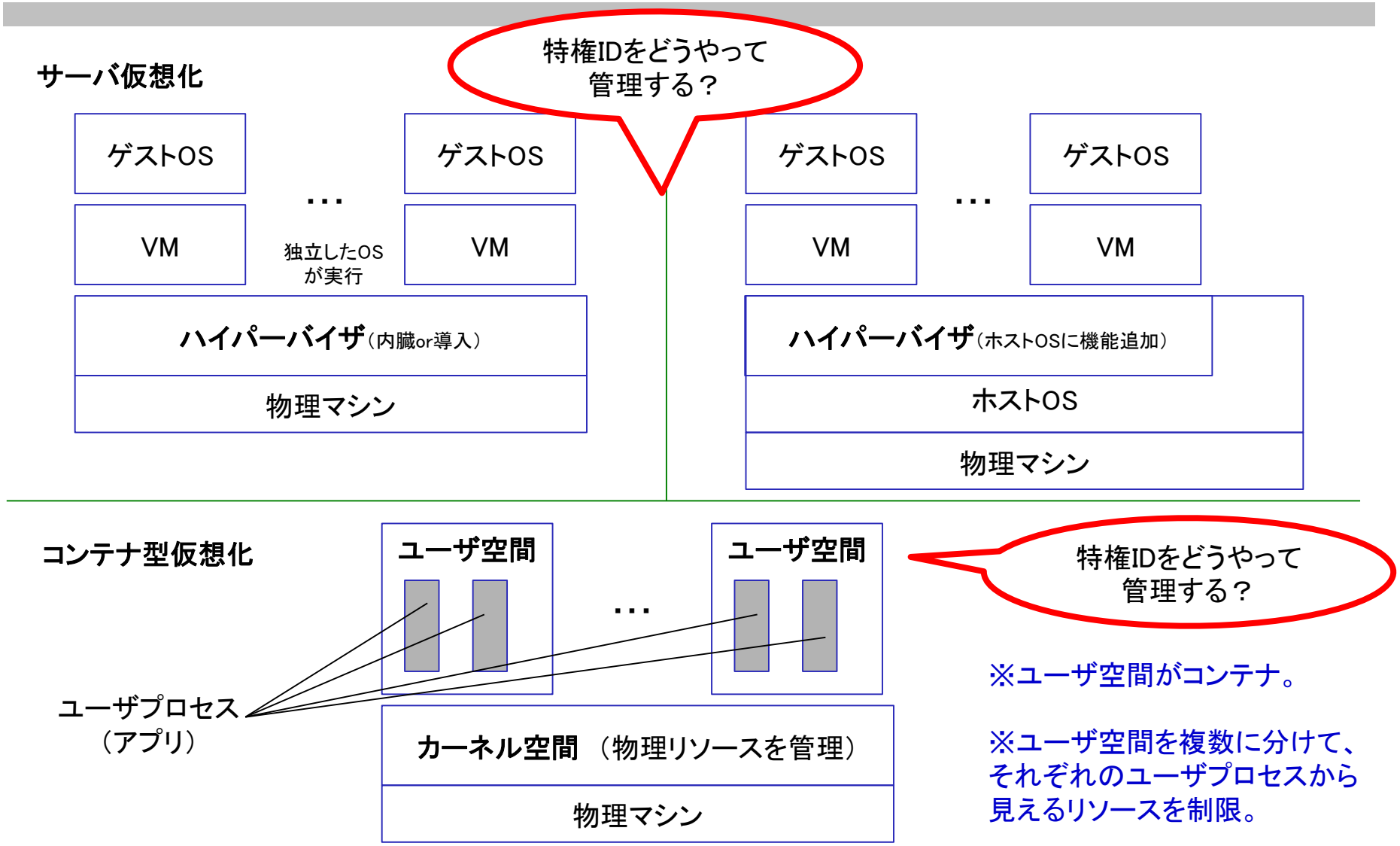
クラウド環境は従来と何が異なるのか

サーバ仮想化からさらなる発展

1. 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。）

2. 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。）

サーバ仮想化 と コンテナ型仮想化（イメージ）



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

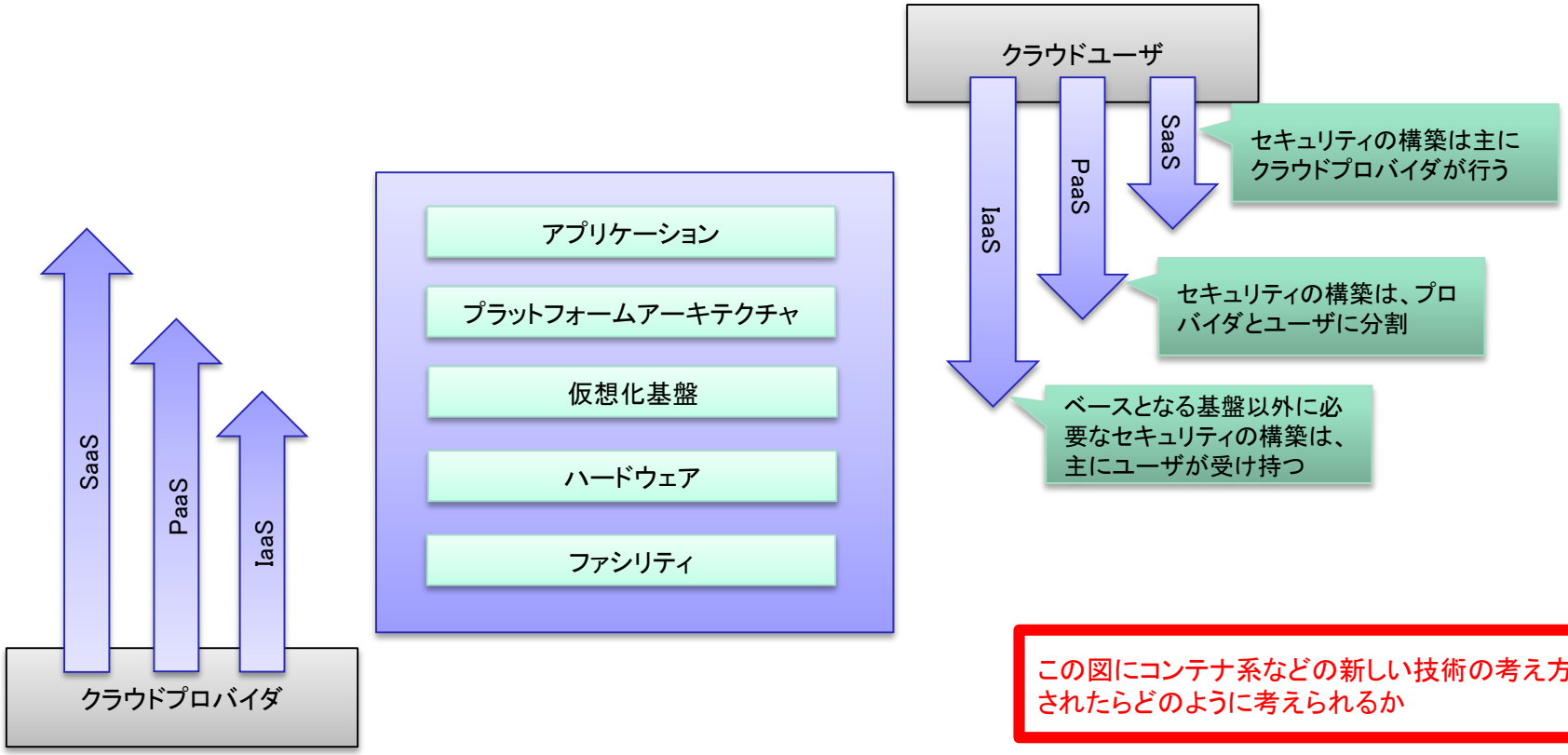
契約や運用面の変化

- 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

（参考）クラウドサービスモデル



この図にコンテナ系などの新しい技術の考え方が加味されたらどのように考えられるか

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

どのような特権ID管理があるか

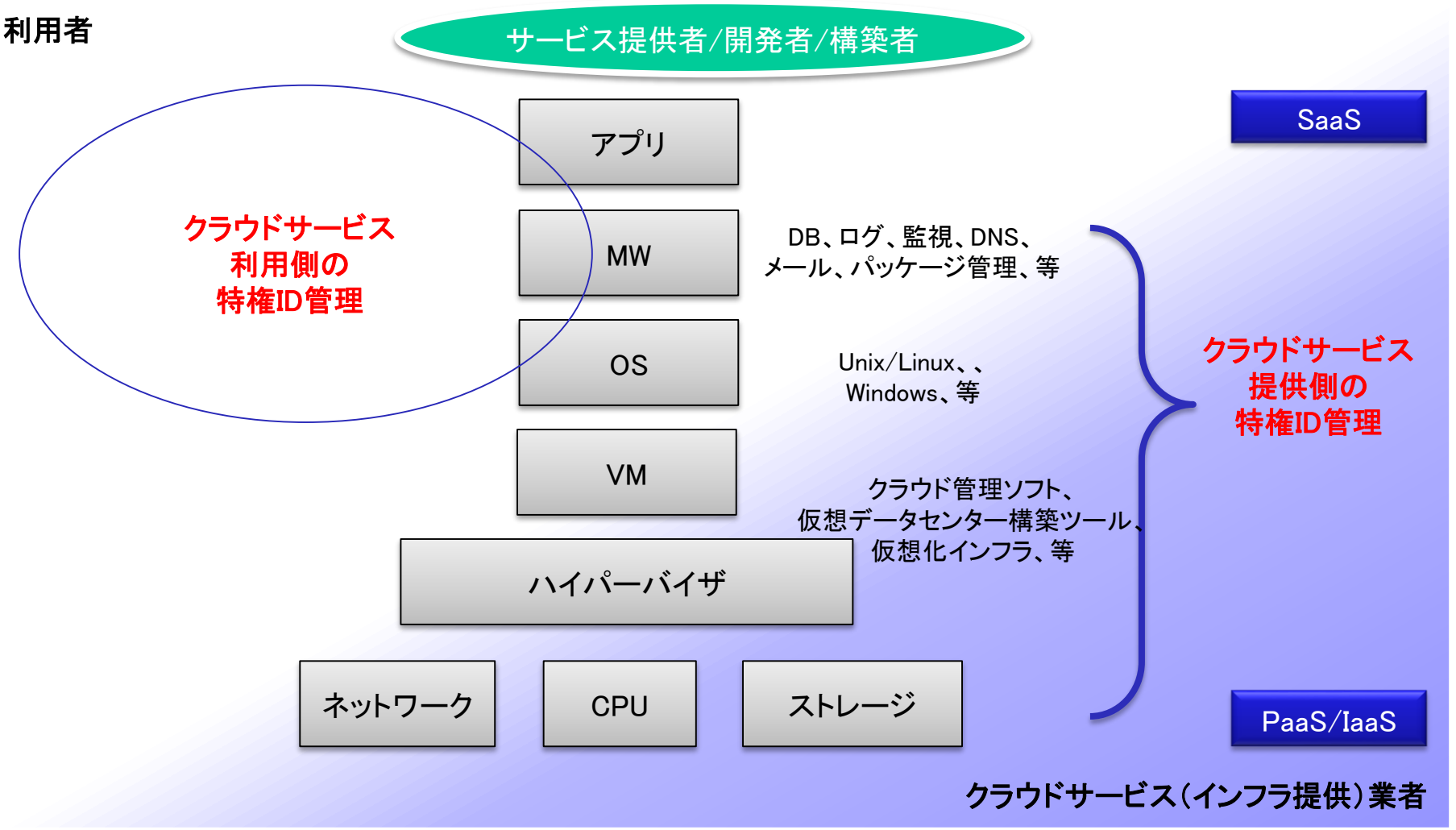
SaaSアプリを中心とした特権ID管理

- 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）

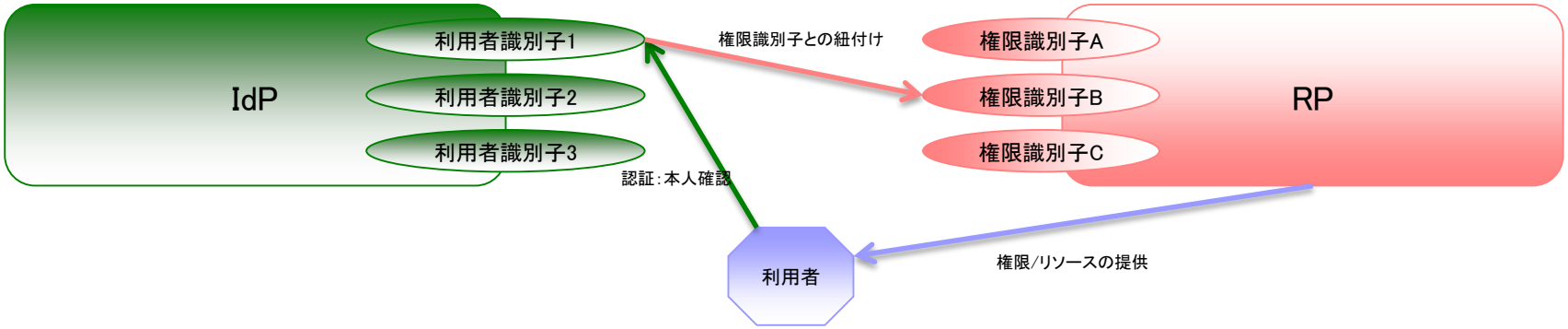


ID連携（IDフェデレーション）の活用

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



まとめ

- 特権IDの取り扱いの見直し
  - もういちど、足元から見直してみましょう。
- クラウド環境での特権ID管理
  - まだ、発展途上です。