再発見セッション：エンタープライズ・アイデンティティー ～これまで・これから～

デロイト トーマツ サイバー合同会社 シニアマネジャー 大森 潤

SailPoint Japan シニアセールスエンジニア, CISSP, CISA,CISM　佐藤公理

目次

- IT環境の変化、アイデンティティ管理の必要性
- アイデンティティ管理　今昔
- ロール管理　今昔
- 特権ID管理　今昔
- まとめ

自己紹介　佐藤公理　SailPoint シニアSE

CISSP（公認情報システムセキュリティプロフェッショナル）
CISA（公認情報システム監査人）、CISM（公認情報セキュリティマネージャ）

2001年より現在までサン・マイクロシステムズ、ノベル、マカフィー、エントラスト、SailPoint においてセキュリティ・デジタルアイデンティティ分野のコンサルタント、プリセールスエンジニアとして活動。幅広いセキュリティ分野の知識・経験と、コンサルタント、プリセールス・エンジニアとしての現場感を大切に、製品・サービスとITの現場をつないで、安心・安全な情報システムを少しでも増やすことを目標に日々精進中。

＜主な活動＞
2020年: JNSAデジタルアイデンティティWG：「クレデンシャルの歴史」執筆者
https://www.jnsa.org/result/digitalidentity/index.html

2016年: JNSAデジタルアイデンティティWG：エンタープライズにおける特権ID管理解説書（第１版）主要執筆者
https://www.jnsa.org/result/2016/idm_pum/index.html

Eight

LinkedIn

自己紹介　大森潤　Deloitte Tohmatsu Cyber

大森　潤

デロイト トーマツ サイバー合同会社

シニアマネジャー
情報処理安全確保支援士

略歴

2005年より現在まで日本オラクルおよびデロイトにおいて、サイバーセキュリティおよびデジタルアイデンティティ分野のコンサルタント、プリセールスエンジニアとして活動。ゼロトラストセキュリティ、アイデンティティ・アクセス管理（IAM）を中心としたセキュリティ基盤構想・戦略の策定とともに、IAM各種（クラウド認証基盤、アイデンティティガバナンス、特権アクセス管理、カスタマーID管理基盤等）、端末管理、SWG/CASB（クラウド利用のセキュリティー対策）などの個別施策の推進、技術的な助言業務などに従事。

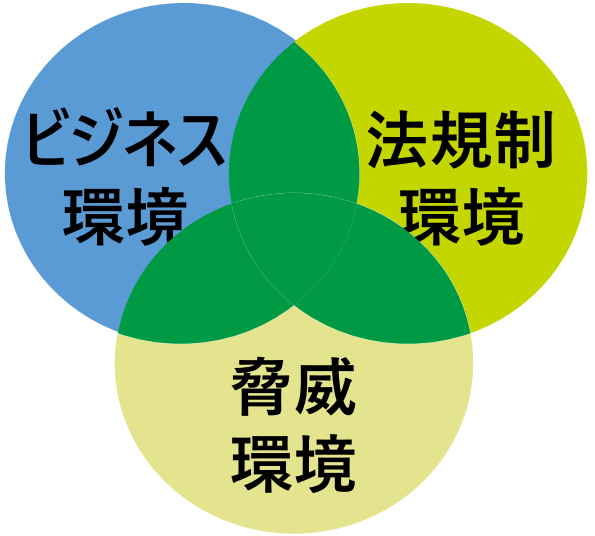
＜主な活動＞
2011年: JNSAデジタルアイデンティティWG：「クラウド環境におけるアイデンティティ管理ガイドライン」執筆者
https://www.jnsa.org/result/digitalidentity/index.html

IT環境の変化

サイバーに注目が集まる様々な要因

デジタル化・働き方の変化

✓デジタル変革の加速的進展
✓グローバル化・事業再編の波
✓New Normalによる環境変化
✓・・・



国内外における
法規制・ガイドラインの制定・改正

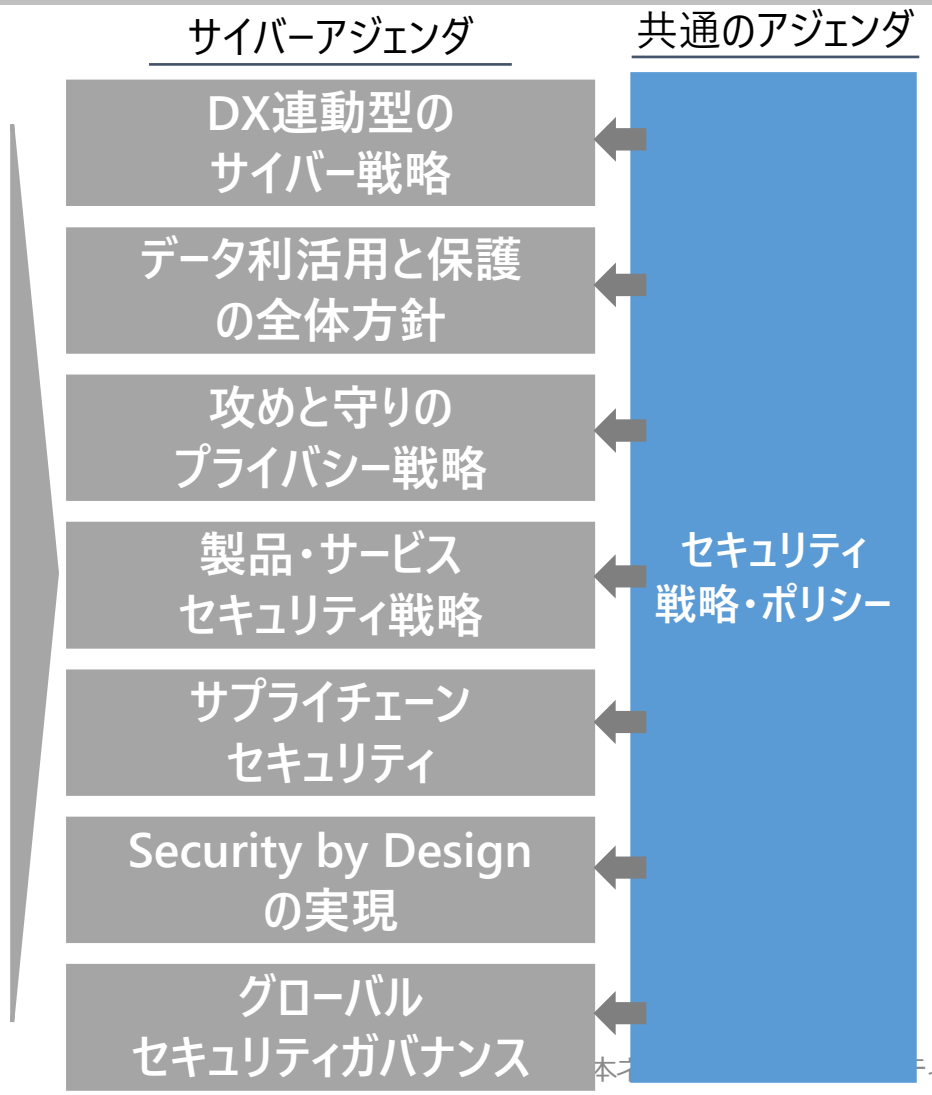
✓ サイバーリスクに関する法規制・業界ルールの強化
✓サプライチェーンリスクへの対応要請
✓企業間の機密情報管理の厳格化
✓・・・

サイバー攻撃の被害深刻化

✓国家規模のサイバー攻撃
✓ランサムウェアによる二重恐喝、世界同時多発的被害の発生
✓制御系にまで波及するサイバー攻撃
✓IoTシステム・サービスへのサイバー攻撃深刻化
✓攻撃による経済的損出の増大化
✓・・・

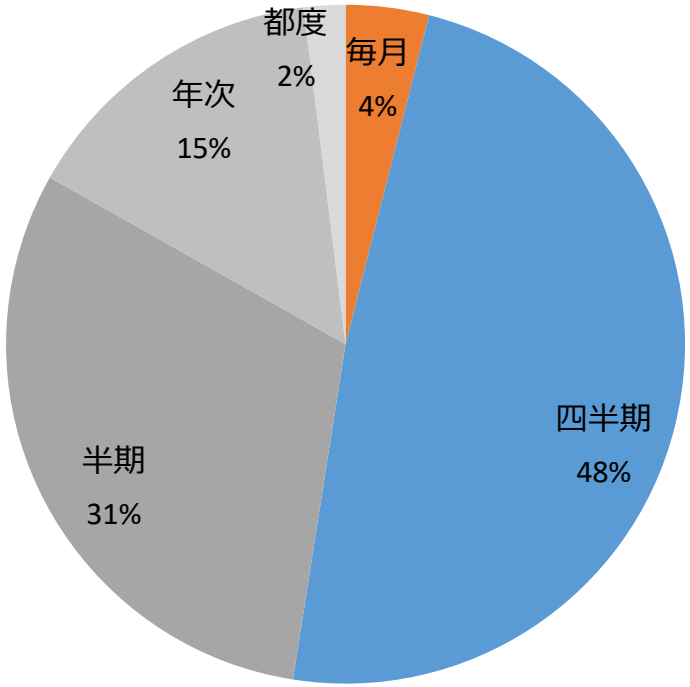
主流は攻めと守りのサイバー対策

目的	企業の動向
DX推進のための投資	■dXは事業変革において最も重要なドライバーとして捉えられており、日系企業の76%がdXに着手済み、または着手予定 ■dX推進において「サイバーセキュリティ」は「投資コスト」、「人材不足」とともに3大課題の一つとCxOには認識されている
製品・サービス品質の向上	■dXにおいては、フィジカル空間、サイバー空間をより一層融合させ、製品・サービスの付加価値を向上させることが重要 ■サイバーセキュリティ対策を製品・サービス品質の重要な要素、研究・開発投資の一部と捉え、サイバーセキュリティ対策を促進
既存ビジネスの差別化	■サイバーセキュリティ対策を調達基準に入れる政府機関・企業が増えている ■ISO、NIST等の標準化団体、業界団体からは、サプライチェーンセキュリティに対する要請が高まっており、法規制化の動きもみられる

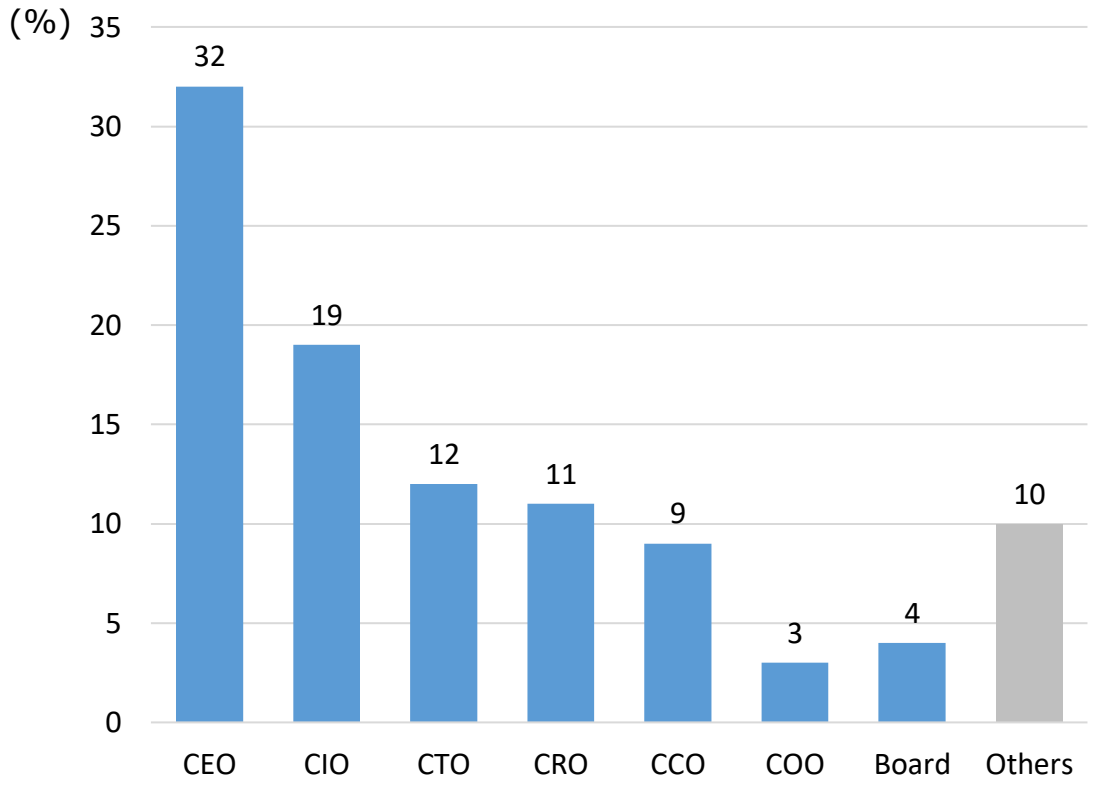


経営課題としてのサイバー対策

■**50%以上の企業では4半期より高頻度でサイバーセキュリティに関する報告が経営層になされている**



■**約90%の企業でサイバーセキュリティに関しては日常的にCxOにレポートされている**

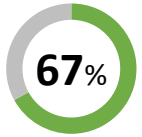


出所: The future of cyber survey 2019 | Cyber everywhere. Succeed anywhere. Deloitte Development LLC. See www2.deloitte.com/us/cyber

IT環境における変化

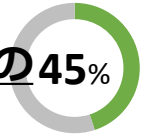
働き方の多様化

社外ユーザーの増加



大企業のうち67%は今後も**契約社員や外部委託者等の契約が増える**と予想。また人外労働力の導入も進んでいる。

外部NWからのアクセスの増加



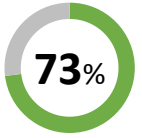
モバイルや外部ネットワークからのアクセスが増加。45%の企業はセキュリティを懸念している。**COVID19によるリモートワークの増加**もあり、この懸念は増大している。

ジョブ型働き方

ジョブ型の働き方が増え、またベンチャー企業連携や産学連携など、社外コラボレーションも活発化している。

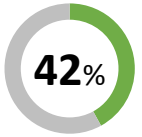
クラウドシフト

クラウド利用



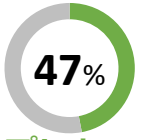
73%の企業がすでに何らかの**クラウドプラットフォームを利用**している

複数のクラウド利用



42%の企業では**複数のクラウド**プラットフォームを利用している

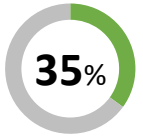
企業システム内のクラウド利用割合



クラウド導入している企業では**オンプレとのハイブリッドの状態**であり、平均して47%のシステムがクラウドとなる

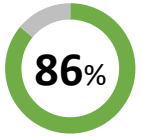
DX*の促進

ビジネスモデルの転換



大企業の35%がビジネスモデルの転換を検討しており、そのうち半分が**業務の「デジタル化」**を検討をしている。

新しい技術の活用



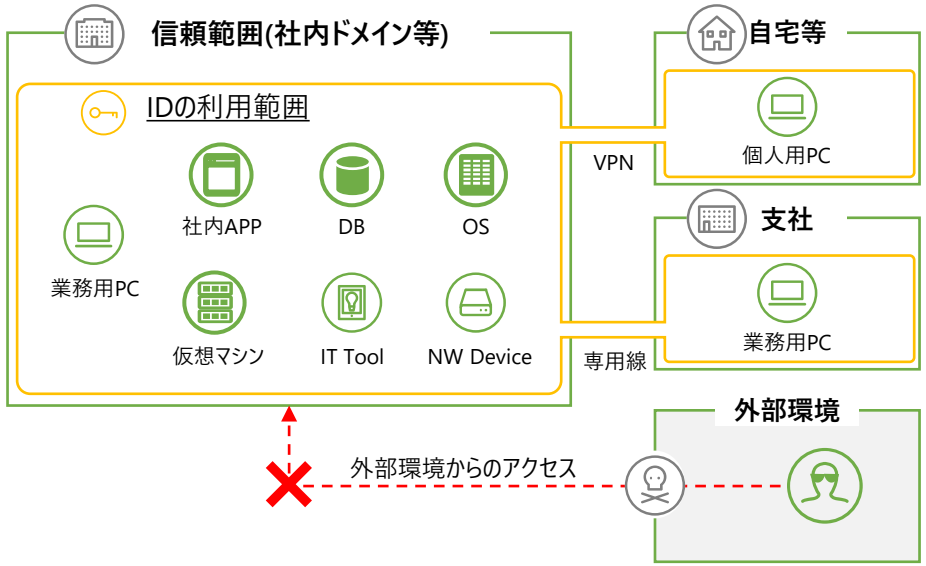
業務のデジタル化を検討している企業の86%がアプリ開発などの必要に迫られており、**RPA、BlockchainやAI**の活用などに乗り出している

出所:Okta The Digital Enterprise report 2019

複雑化するIT環境

いままでのIT環境

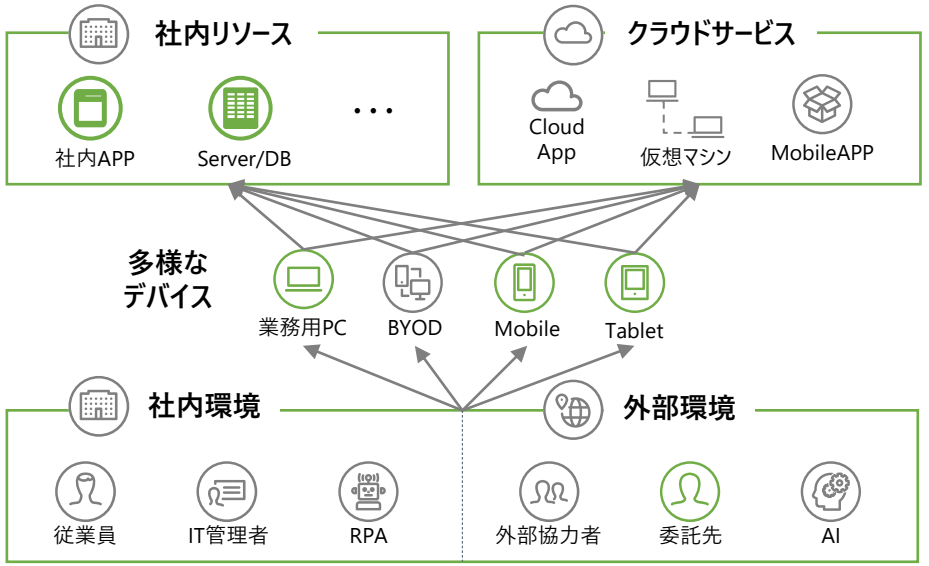
ネットワークを軸として「信頼」したゾーンのみアクセスを許容する



- ITリソースのアクセス境界は**IPセグメントやFWが主**となる
- 社外からのITリソースへのアクセスはVPNや専用線を用いて行い、それ**以外のアクセスは基本的に不可**
- 定められた範囲のITリソースを守る形でセキュリティ境界を敷く事で、一定程度のセキュリティを担保した

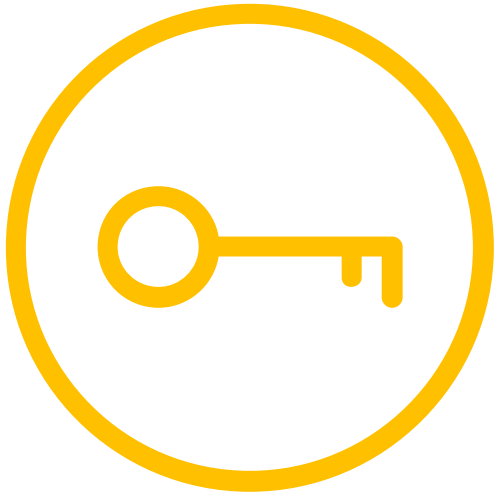
複雑化したIT環境

ITリソースへのアクセス境界が曖昧となっている



- 複雑化したIT環境ではクラウド等、**社内の外側**にもITリソースが存在する
- そのため、**アクセス境界が曖昧となり**、使用者、場所、時間およびデバイスに関わらず**柔軟なアクセス**が求められる
- **どこからでも、どのデバイスからでも**ITリソースへのアクセスが求められるため、セキュリティレベルの維持が困難

再注目されるデジタル・アイデンティティ



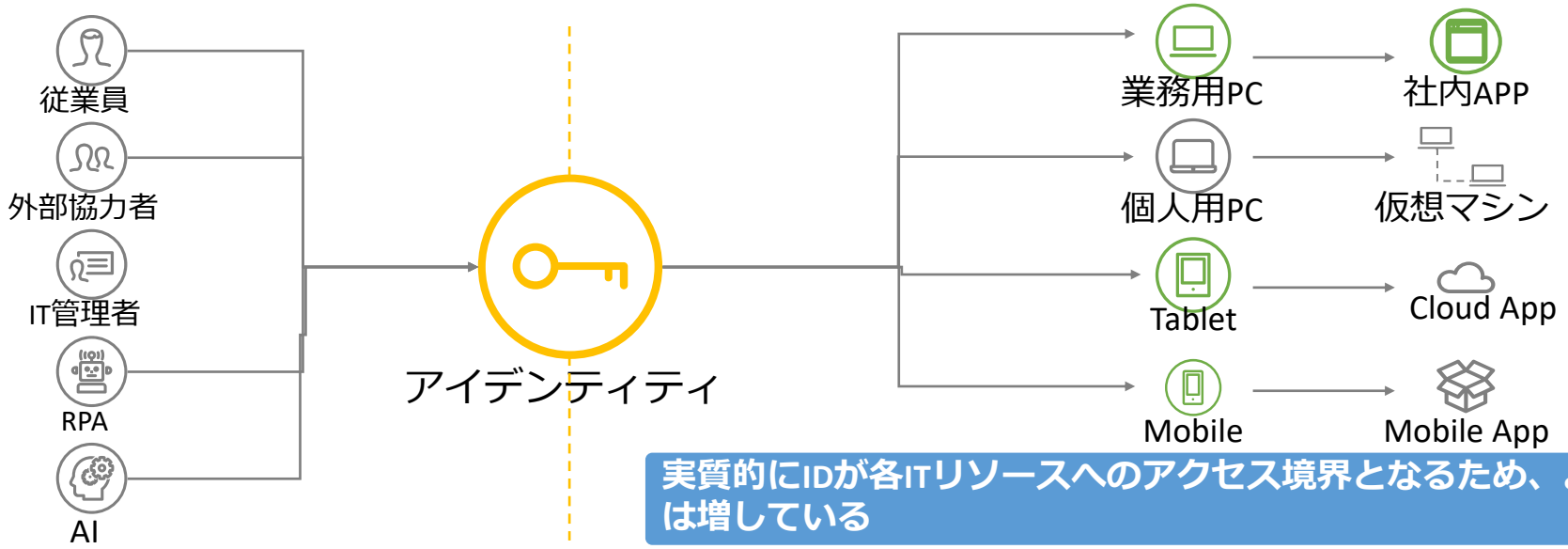
デジタル・アイデンティティ

デジタル空間での自分を表すもの。

アイデンティティ中心の世界

アイデンティティを境界としたIT環境

アイデンティティにアクセス権を付与し厳密な管理の元でITリソースを利用させる



実質的にIDが各ITリソースへのアクセス境界となるため、より重要度は増している

- 曖昧となったアクセス境界は実質的に**アイデンティティが各ITリソースへのアクセス境界**となる。そうすることで、誰が、どういうデバイスでどこからアクセスしようと、セキュリティポリシー（アクセス制御だけでなく、個人情報保護等のプライバシー対応）の適用が一律に行うことができる。また新規のITリソースを追加する際にもそのアイデンティティの管理ができていることで、新しい働き方への対応や、NW等の追加投資なしに使い始めることができる
- 従業員、外部協力者等の人だけではなく、**RPA、AI等の人間外のアイデンティティも管理対象**となる。
- その反面、アイデンティティ単位でセキュリティを管理するため真正性や鮮度など**厳密な管理**が求められる

アイデンティティ管理　今昔

アイデンティティ管理　今昔

JNSA

昔

オンプレ

ウォータフォール、発注

パッケージ

社員、たまに派遣

コンプライアンス
（監査レポート）

今

オンプレ＋クラウド

アジャイル、内製化

SaaS、PaaS、IaaS

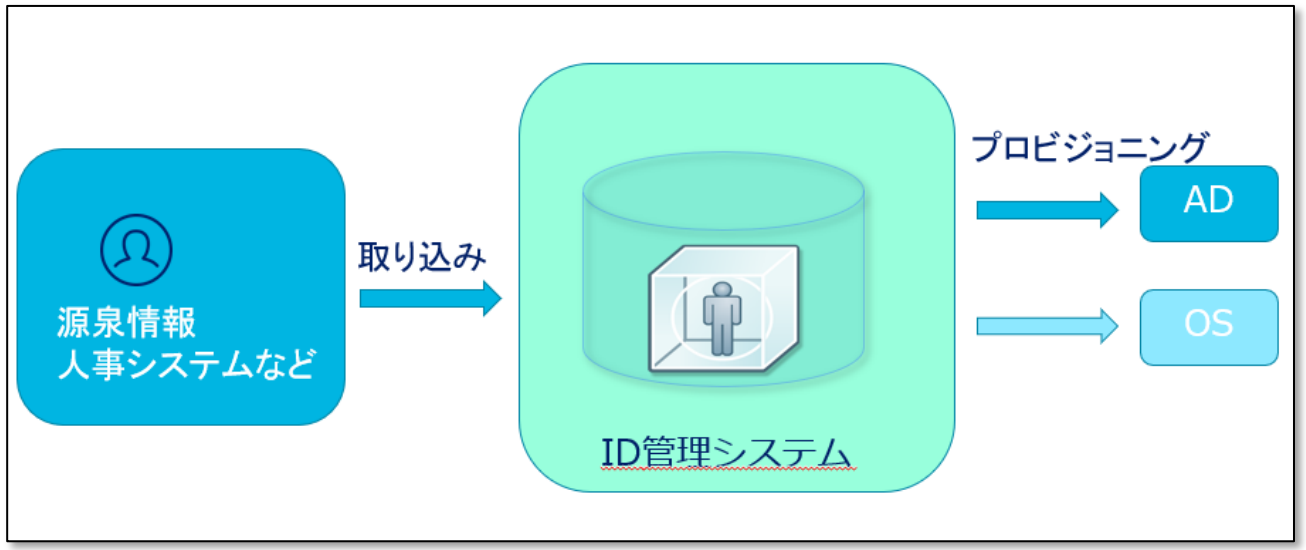
社員、派遣、委託先、パートナー

ガバナンス
（棚卸・アクセスレビュー）

大きく変わったのは？

アイデンティティ管理とは？（昔）

ライフサイクルに応じて対象システムに対してユーザアカウントの作成・変更・削除等を行うこと。（プロビジョニング）



大きく変わったのは？

User Administration & Provisioning
（ユーザ管理&プロビジョニング）

大きく変わったのは？

User Administration & Provisioning
（ユーザ管理＆プロビジョニング）

+

Identity & Access Governance
（アイデンティティ＆アクセスガバナンス）

大きく変わったのは？

Identity Governance and Administration
アイデンティティガバナンス＆管理

=

User Administration & Provisioning
（ユーザ管理＆プロビジョニング）

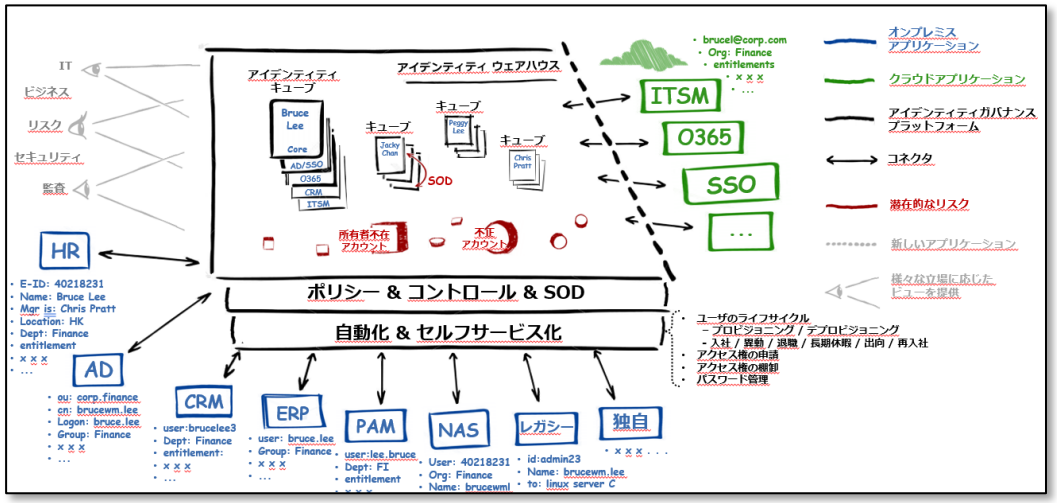
+

Identity & Access Governance
（アイデンティティ＆アクセスガバナンス）

大きく変わったのは？

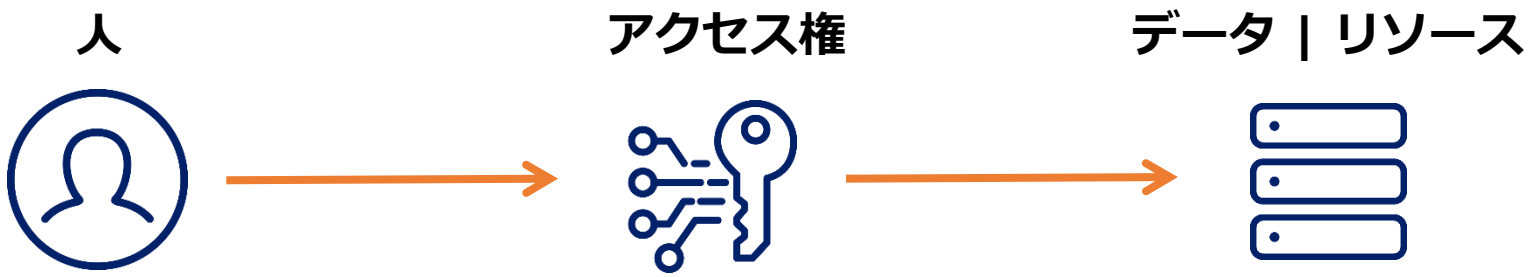
アイデンティティ管理とは？（今）

ライフサイクルに応じて対象システムに対してユーザアカウントの作成・変更・削除等を行い（プロビジョニング）、**適切に実施されているかを確認・レビューすること（ガバナンス）**



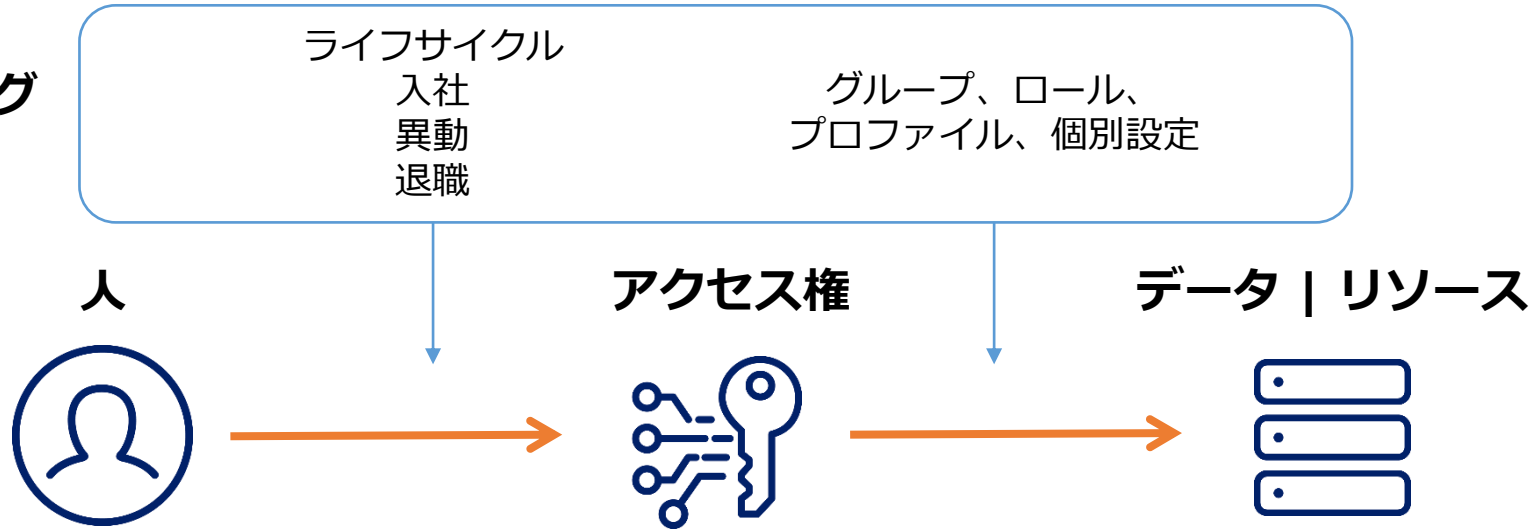
プロビジョニングとガバナンス

リソースへのアクセス権



プロビジョニングとガバナンス

プロビジョニング
Administration



プロビジョニングとガバナンス

プロビジョニング
Administration

ライフサイクル
入社
異動
退職

グループ、ロール、
プロファイル、個別設定

人

アクセス権

データ | リソース

ガバナンス
Governance

誰が申請したか
誰が承認したか
いつ付与されたか
今も必要か
最後に利用されたのは
最後に認定されたのは
利益相反関係はないか

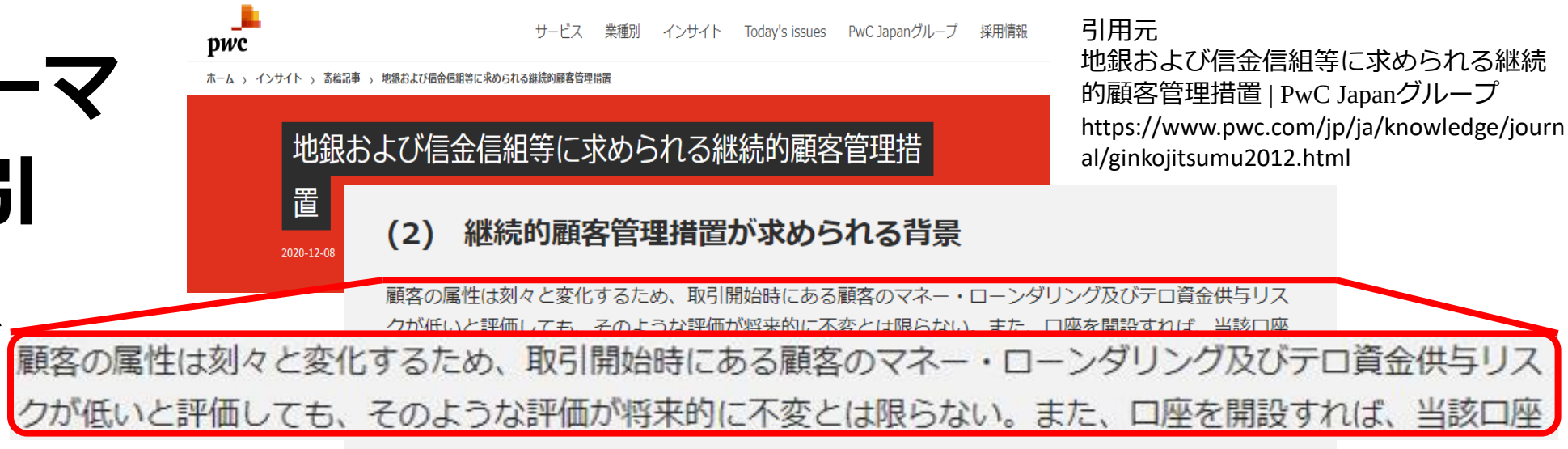
誰がオーナーか
特権アクセスか
構成は正確か
最後に確認されたのは

なぜ、常に確認・レビューが必要？

サイバーセキュリティの視点

ゼロトラスト
＝Never Trust , Always Verify
信頼するな、常に検証せよ

コンシューマ金融取引の視点



引用元
地銀および信金信組等に求められる継続的顧客管理措置 | PwC Japanグループ
https://www.pwc.com/jp/ja/knowledge/journal/ginkojitsumu2012.html

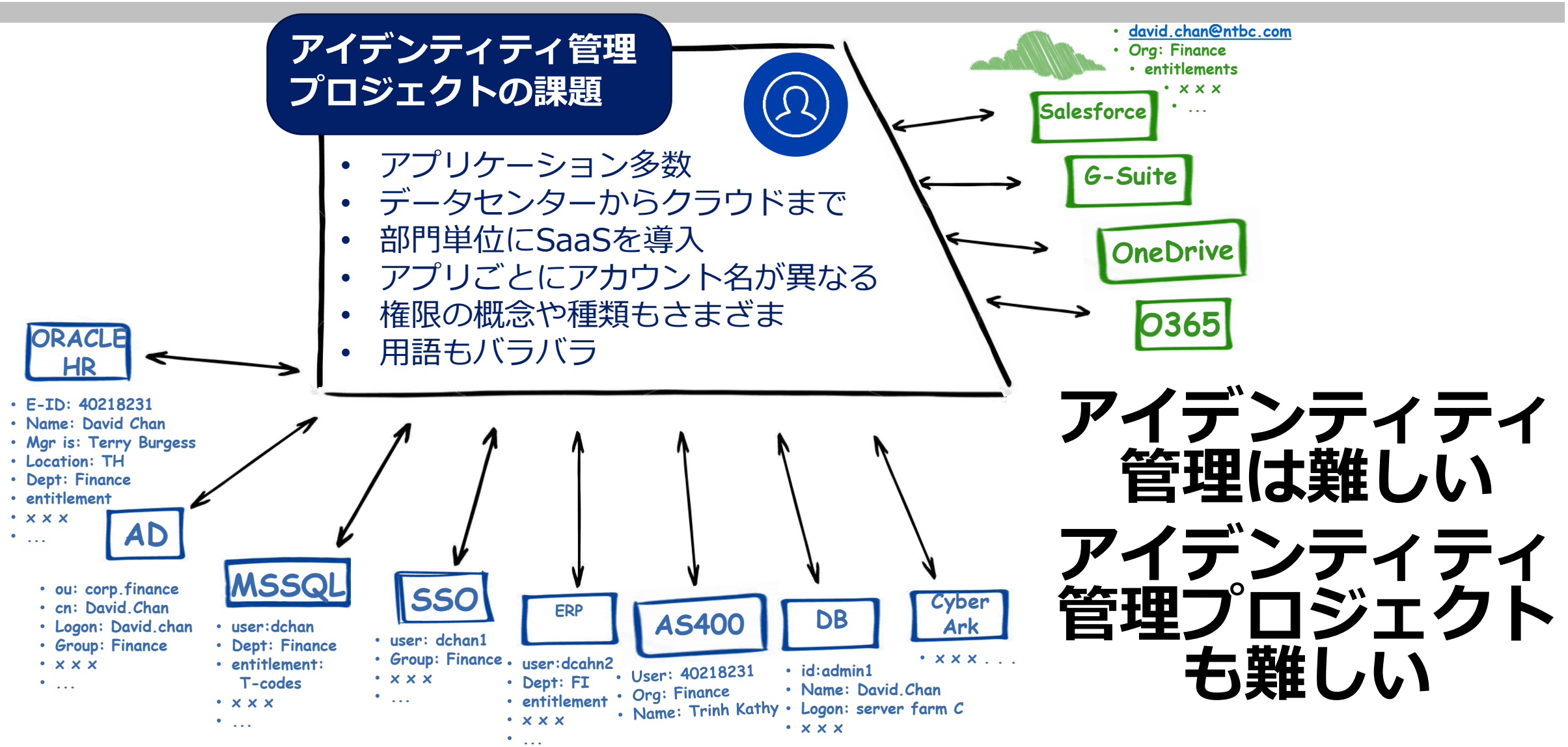
なぜ、常に確認・レビューが必要？

ある時点（入社、異動時等）にアカウント情報・アクセス権限が正当・確かであったとしても

将来的に・あるいは“今”正当・確かであるとは限らない。

継続的に、アイデンティティ情報を確認・レビューし、最小権限の原則を維持することが必要

昔から変わらないのは？



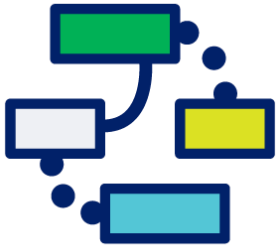
アイデンティティ管理は難しい

アイデンティティ管理プロジェクトも難しい

昔から変わらないのは？
アイデンティティ管理アンチパターン

JNSA

「絵に描いた餅」「業務知らず」



“社内の関係者（業務部門や運用担当）を巻き込まずに企画・要件定義”
“アイデンティティ管理の業務フローを把握せず、現場からの反発”

▼

全社プロジェクト化
アイデンティティ管理
業務・システムの把握

「製品そっちのけ」

“製品・サービスを想定せず、あるべき論での企画・要件定義・設計。追加開発続出！”

▼

製品サービスの理解
（ドキュメント・トレーニング・簡易検証）

「ブラックボックスプロビジョニング」「つながるだろう症候群」

“連携先の仕様調査不足・アイデンティティ管理サービス・製品の仕様への過信。想定通りに連携できない・追加工数発生！”

▼

連携システム毎の
連携方式・連携内容の調査

引用元：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 | JNSA アイデンティティ管理WG https://www.amazon.co.jp/dp/4844395866
を参考に資料作成

ロール管理　今昔

そもそもロール管理がなぜ必要なのか？

- 前提
  - 情報システムを利用するには、**ユーザが利用するアカウント**が当該情報システムに対する**アクセス権**を有している必要がある。

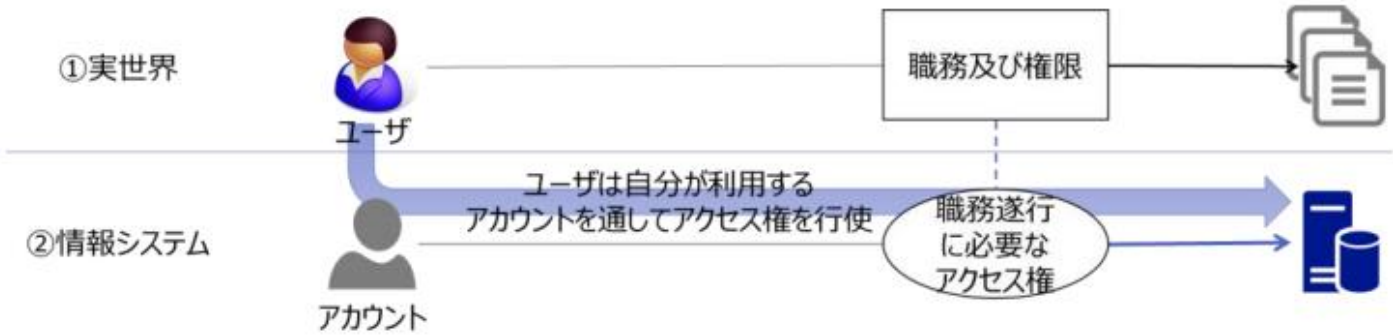


図 1.1　ユーザ・職務の関係とアカウント・アクセス権の関係

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ロール管理が必要な背景①
  - ユーザとアクセス権を1対1で管理している場合。ユーザの数×利用するアクセス権分の管理が必要。

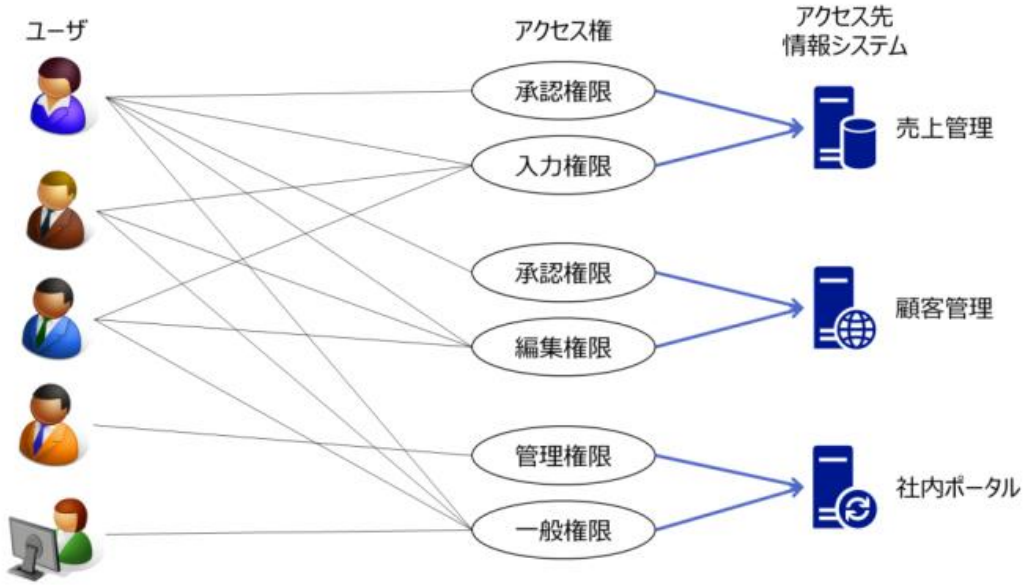


図 1.2　ユーザ（とそのユーザが利用するアカウント）とアクセス権を 1 対 1 で管理している状態

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ロール管理が必要な背景②
  - ユーザとアクセス権の関係は変化する。

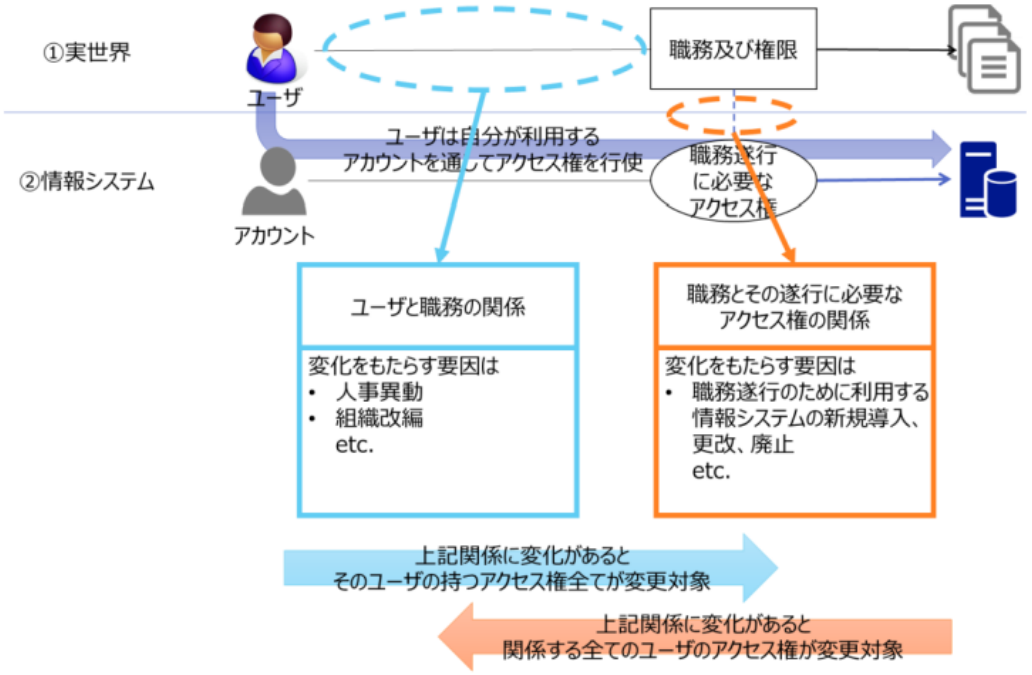


図 1.3　ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係（ロールを介さない場合）

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ロール管理がないと困る！
  - ユーザとアクセス権の関係が変化すると。。。
  - **実現不可能なほど複雑で手間のかかる作業**が発生する。

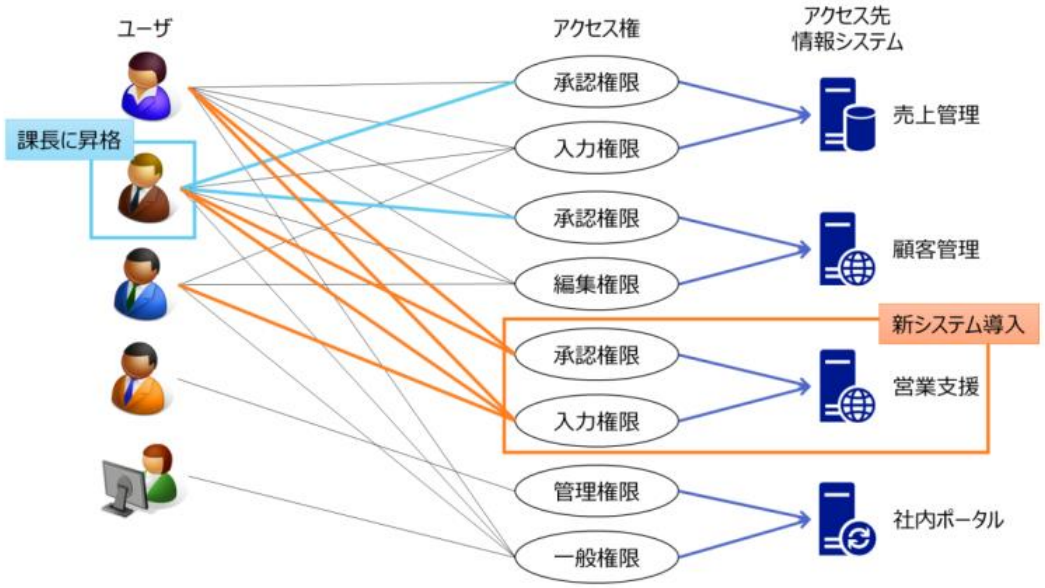


図 1.4　関係に変化が生じた場合のユーザと割り当てるアクセス権の変更箇所

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ロール登場！
  - ロールとは！**職務遂行に必要な各種情報システムに対するアクセス権の組み合わせ**
  - **管理の煩雑さを抑制し、適切な管理を実現！**

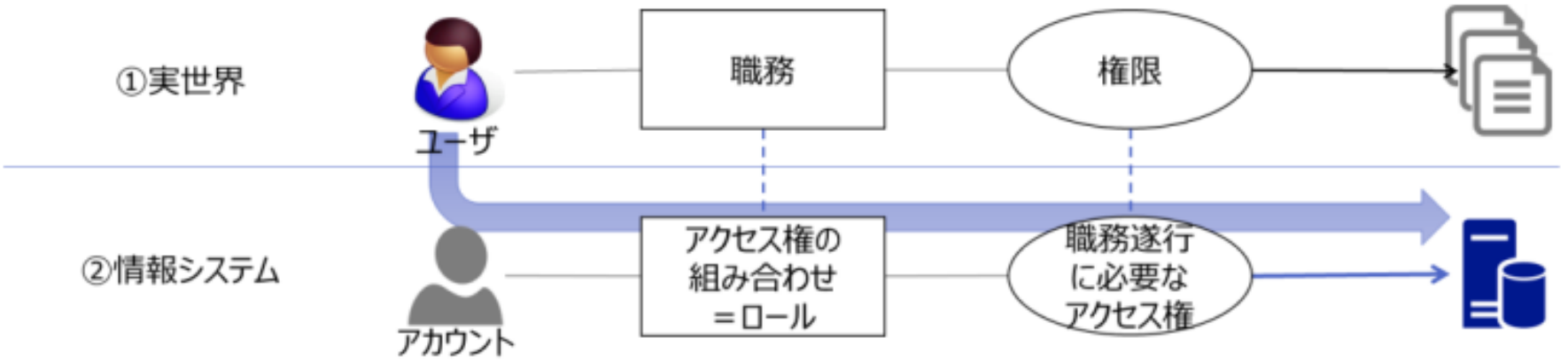


図 1.5　ロールを仲立ちとしたユーザ・職務の関係とアカウント・アクセス権の関係

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ロールを介してアクセス権を割り当てる・管理する。

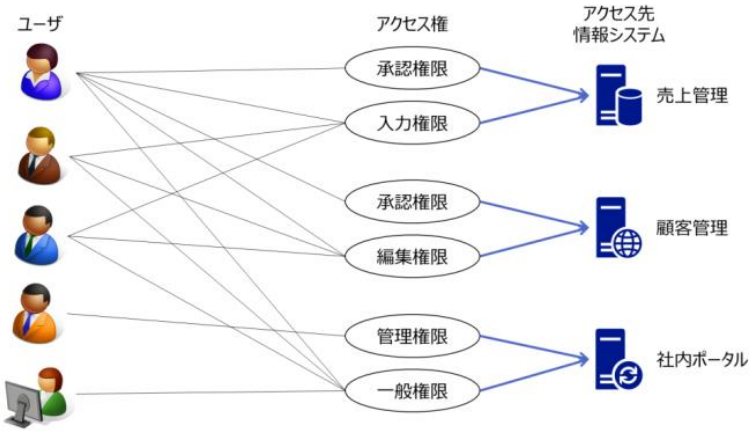


図 1.2　ユーザ（とそのユーザが利用するアカウント）とアクセス権を 1 対 1 で管理している状態

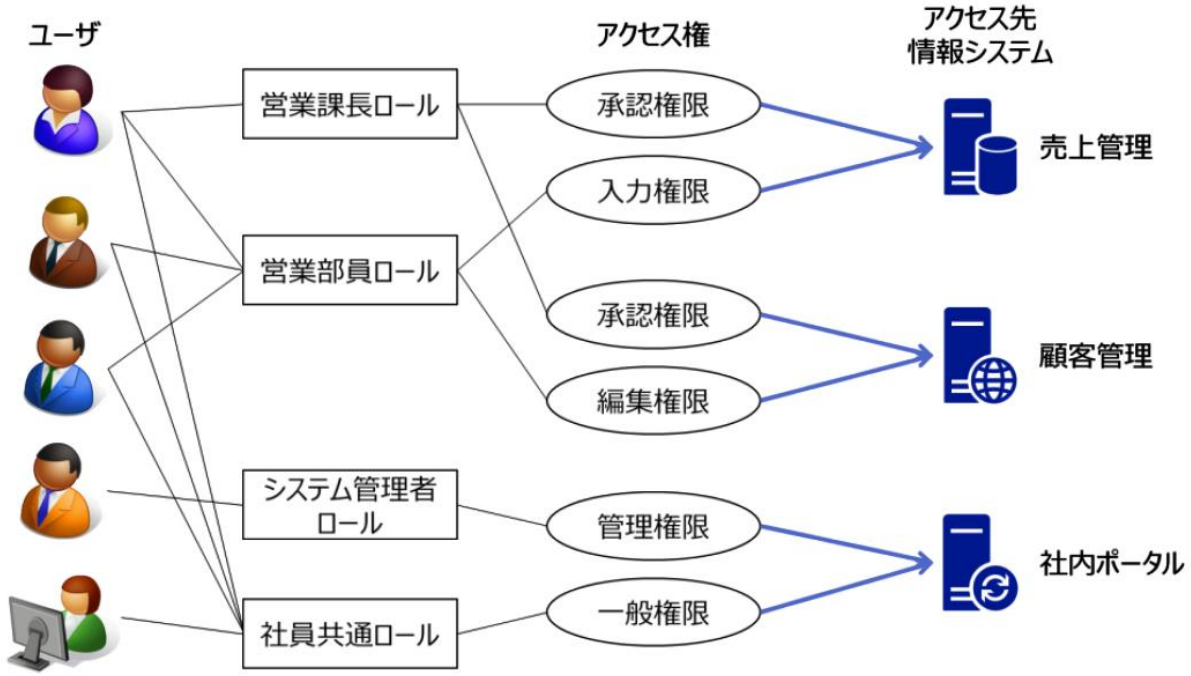


図 1.6　ユーザ（とそのユーザが利用するアカウント）とアクセス権をロール管理している状態

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ロールを介することで**変化の影響範囲が限定される**

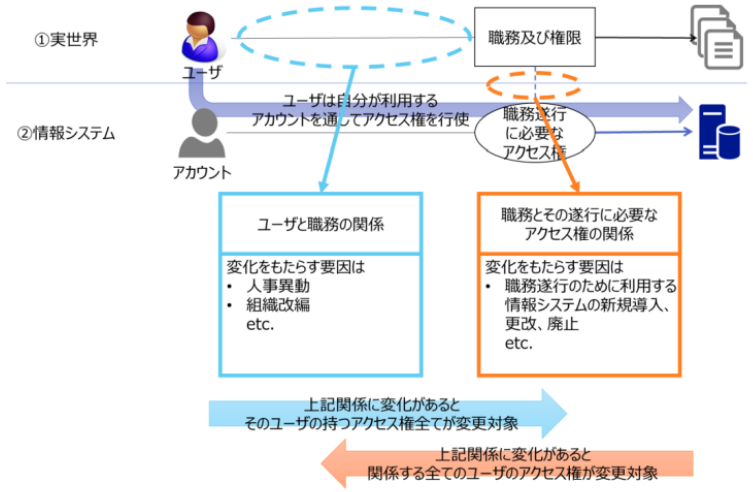


図 1.3　ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係（ロールを介さない場合）

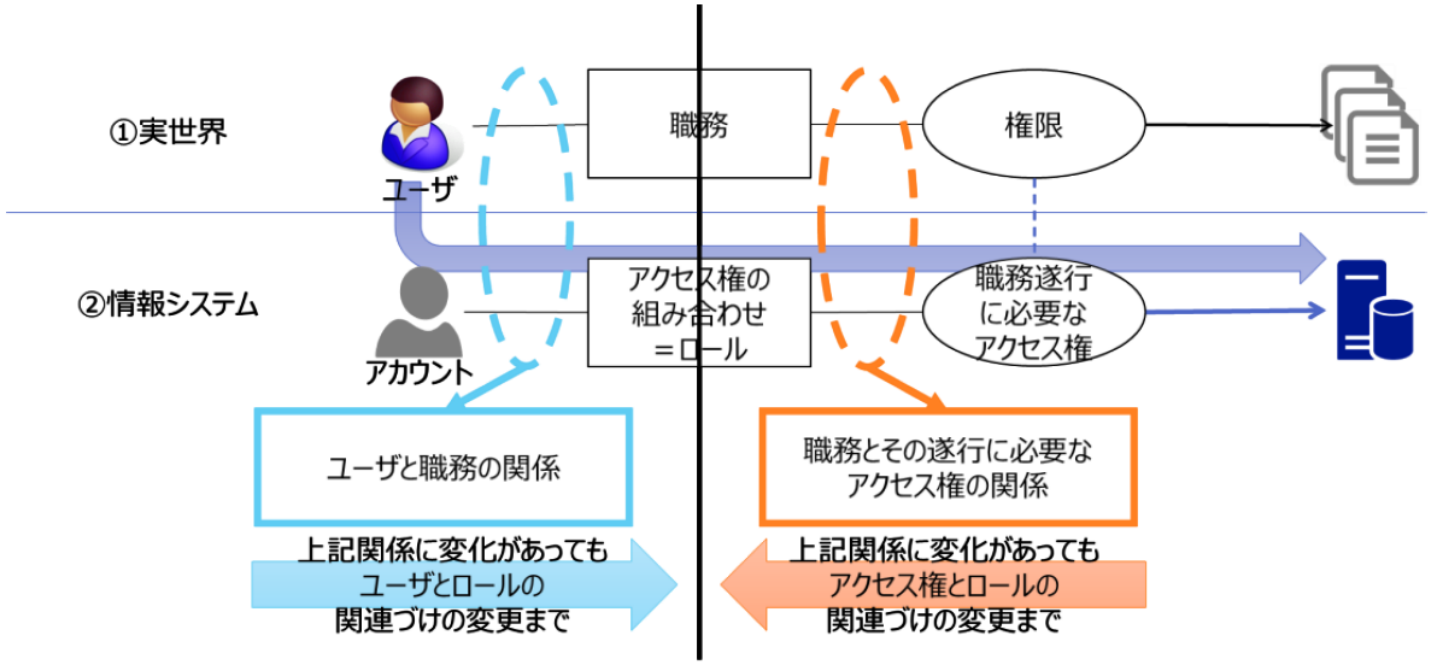


図 1.7　ユーザと職務の関係及び職務とその遂行に必要なアクセス権の関係（ロールを介す場合）

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

- ロールを介することで**変化の影響範囲が限定される！！**

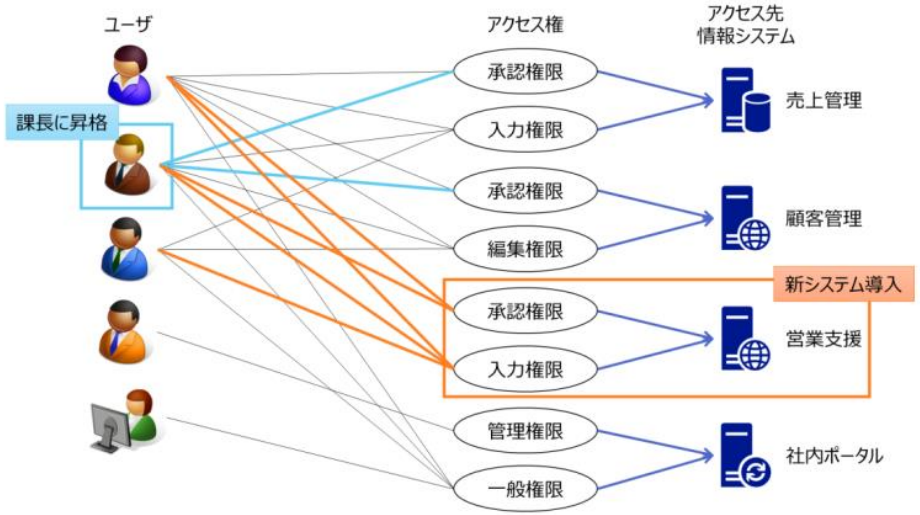


図 1.4　関係に変化が生じた場合のユーザと割り当てるアクセス権の変更箇所

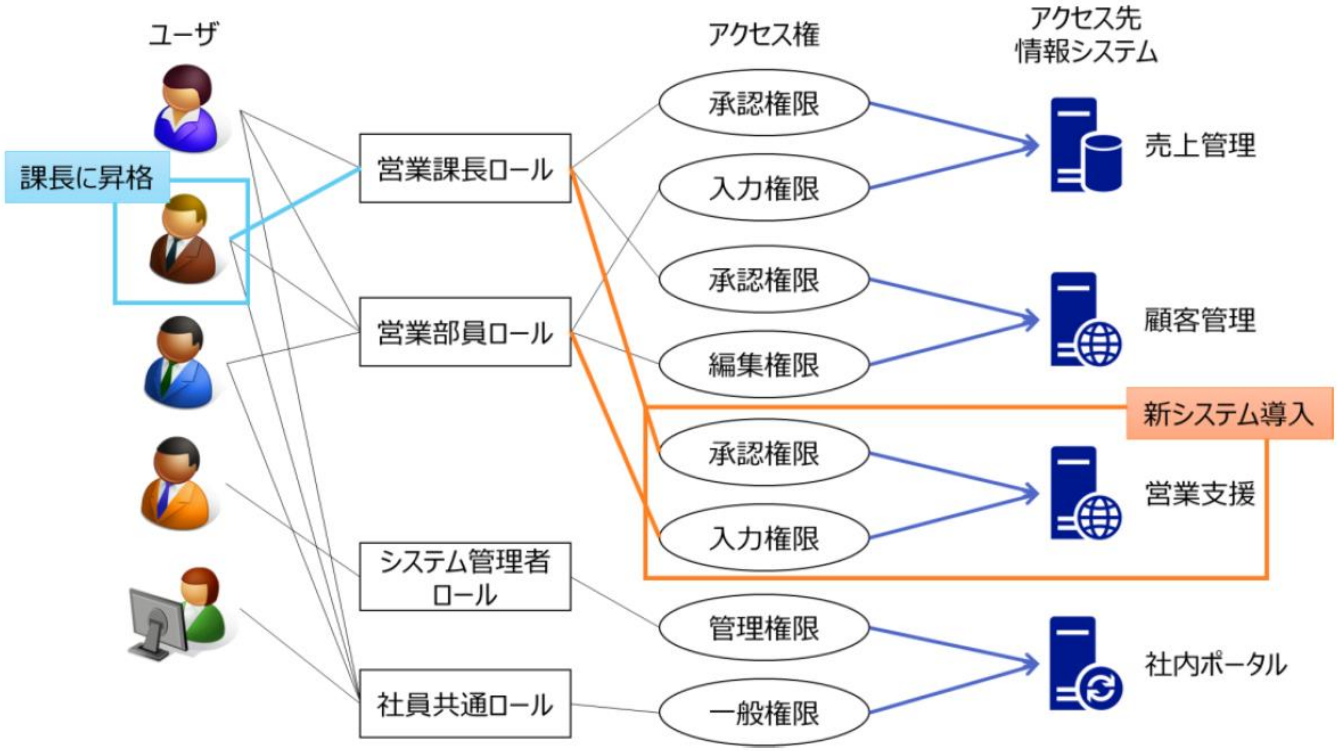
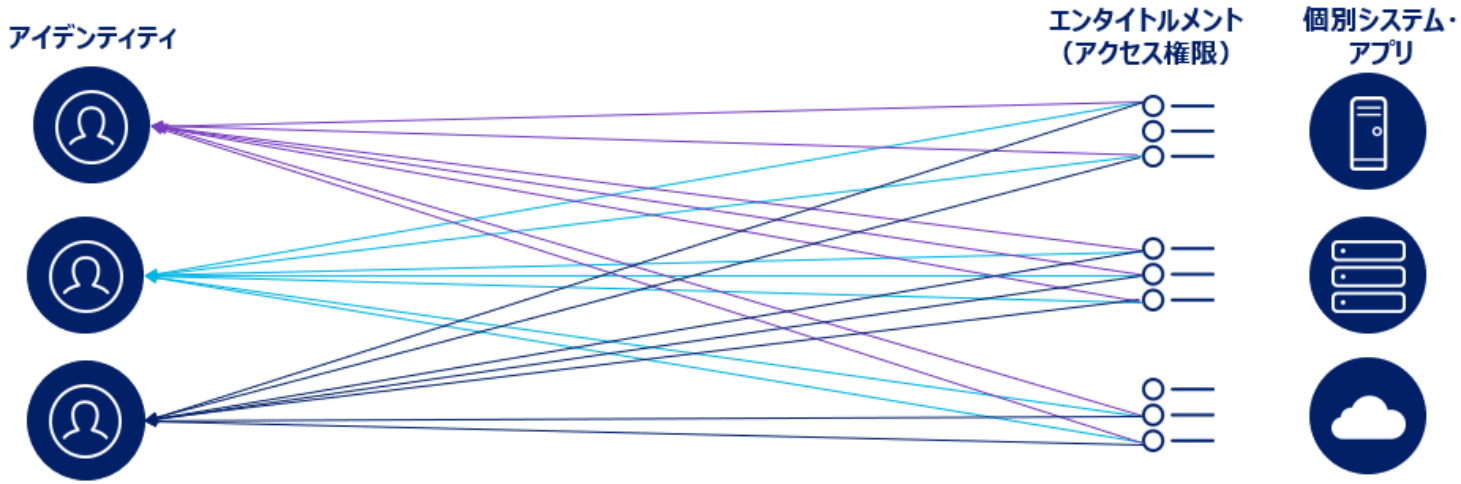


図 1.8　関係に変化が生じた場合のロールに生じる変更箇所

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

そもそもロール管理がなぜ必要なのか？

ロール管理なしのアクセス権割当



個々のエンタイトルメントを申請（リクエスト）、承認、棚卸・レビューにより
- 工数増加・コスト増加
- 間違いのリスク
- 意思決定（判断）疲れと「承認・決済の形骸化（Rubber Stamping）」

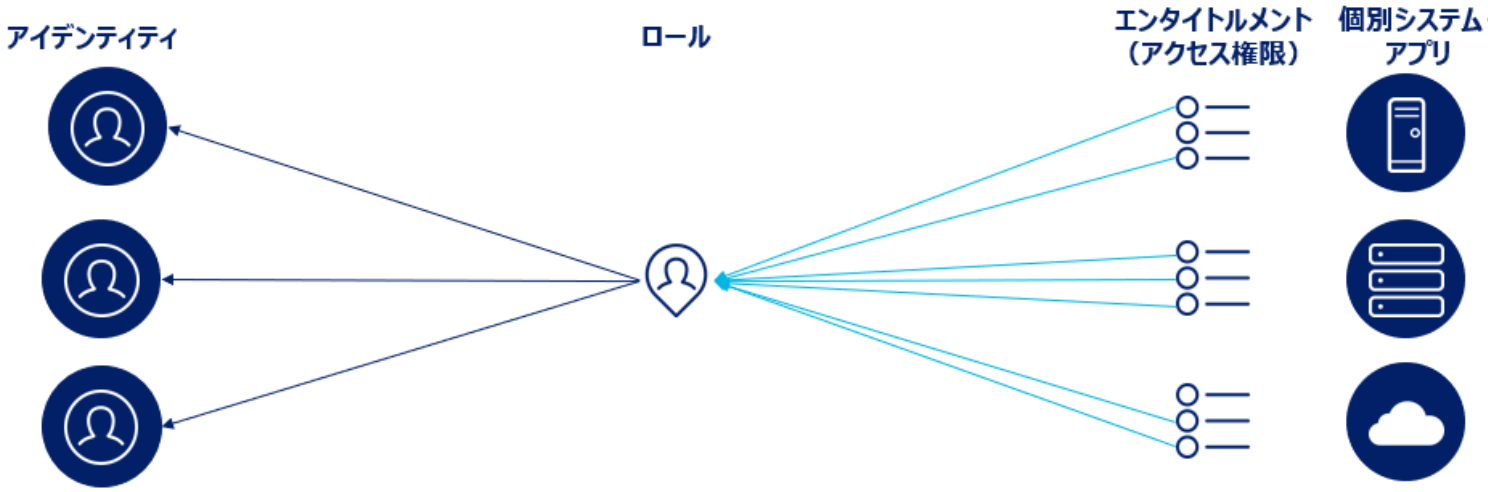
の発生

SailPoint

SaillPoint Japanプレゼン資料より抜粋

そもそもロール管理がなぜ必要なのか？

ロール管理の利点



ロール管理により
- アクセス権限の自動的な割当
- 10～50のエンタイトルメント（アクセス権限）を申請する代わりにロールを1つ申請
- 承認処理数の削減
- 棚卸・レビュー対象数の削減

を実現。アクセス権管理の効率が大幅に向上

SailPoint

SaillPoint Japanプレゼン資料より抜粋

そもそもロール管理がなぜ必要なのか？

**アクセス権を効果的・効率的に管理するために
ロール管理が必要**

**ロール管理なしでは、アクセス権の管理は実質的
に不可能**

ロール管理　今昔

JNSA

昔

オンプレ
グループマスタ、ロールマスタ、
職務マスタ（社内システム用）

事前に設計。各システムで共有

運用でカバー

ロール定義で自動割当

ADのグループ

今

オンプレ＋クラウド
社内システム用
＋SaaS、PaaS、IaaS

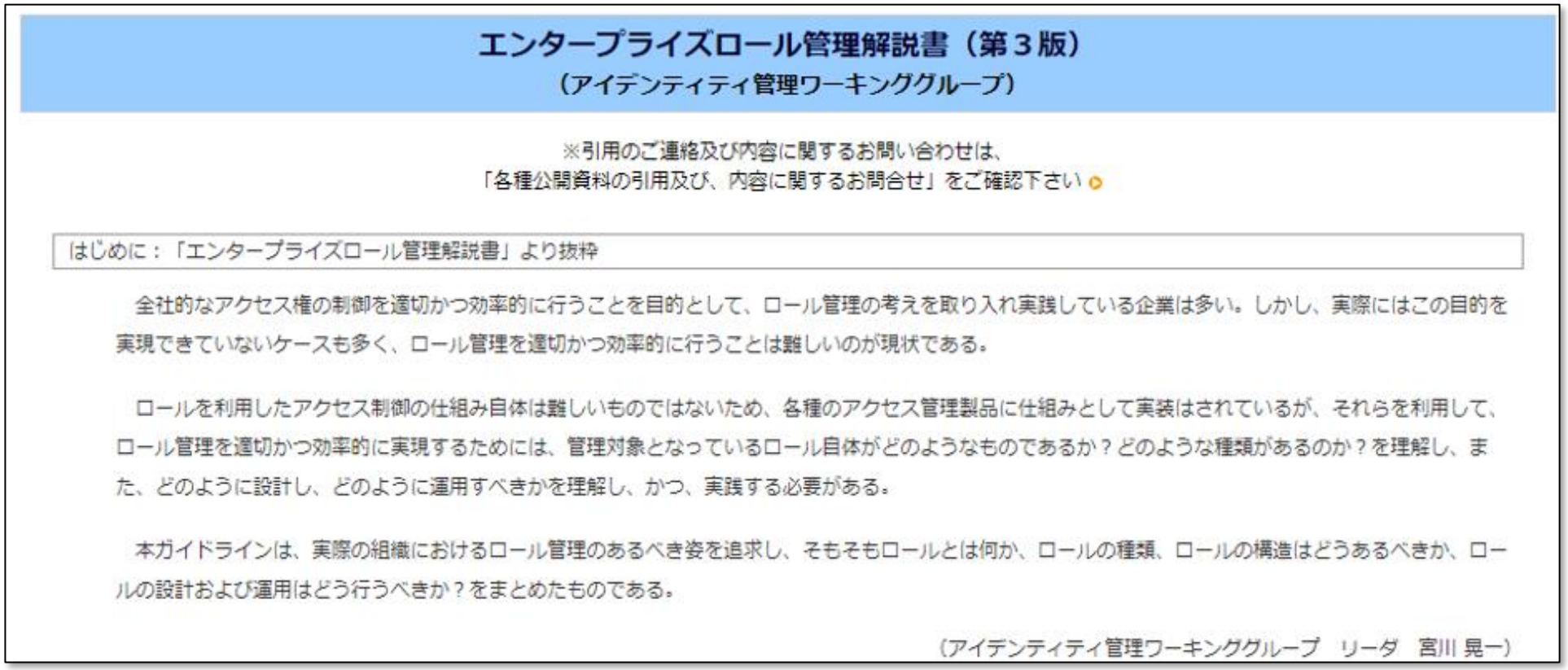
システムに合わせて柔軟に変更、
レビュー

もう運用でカバーできない

自動割当＋アクセス権申請

モデリング、ディスカバリ
アクセス権棚卸

ロール管理　昔から変わらないのは？



エンタープライズロール管理解説書（第３版）
（アイデンティティ管理ワーキンググループ）

※引用のご連絡及び内容に関するお問い合わせは、
「各種公開資料の引用及び、内容に関するお問合せ」をご確認下さい

はじめに：「エンタープライズロール管理解説書」より抜粋

全社的なアクセス権の制御を適切かつ効率的に行うことを目的として、ロール管理の考えを取り入れ実践している企業は多い。しかし、実際にはこの目的を実現できていないケースも多く、ロール管理を適切かつ効率的に行うことは難しいのが現状である。

ロールを利用したアクセス制御の仕組み自体は難しいものではないため、各種のアクセス管理製品に仕組みとして実装はされているが、それらを利用して、ロール管理を適切かつ効率的に実現するためには、管理対象となっているロール自体がどのようなものであるか？どのような種類があるのか？を理解し、また、どのように設計し、どのように運用すべきかを理解し、かつ、実践する必要がある。

本ガイドラインは、実際の組織におけるロール管理のあるべき姿を追求し、そもそもロールとは何か、ロールの種類、ロールの構造はどうあるべきか、ロールの設計および運用はどう行うべきか？をまとめたものである。

（アイデンティティ管理ワーキンググループ　リーダ　宮川 晃一）

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

「ロール管理の考え」必要性は変わらない

昔から変わらないのは？
ロール管理でもアンチパターン

「似たもの同士ロール」

“十分な検討を行わず、その場その場で必要なロールを作成した。結果、類似のロールが乱立している。

「増殖していくロール」

“ロールの見直し・削除・修正する適切なプロセス・仕組みがない。結果、ロールが増殖・爆発している。”

「メンバ不明ロール」「使用目的不明ロール」

“ロールのメンバがわからない。”
“ロールが使われているかわからない”

引用元：エンタープライズロール管理解説書（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_guideline/index.html

失敗例（アンチパターン）は変わらない

ロール管理　大きく変わったのは？

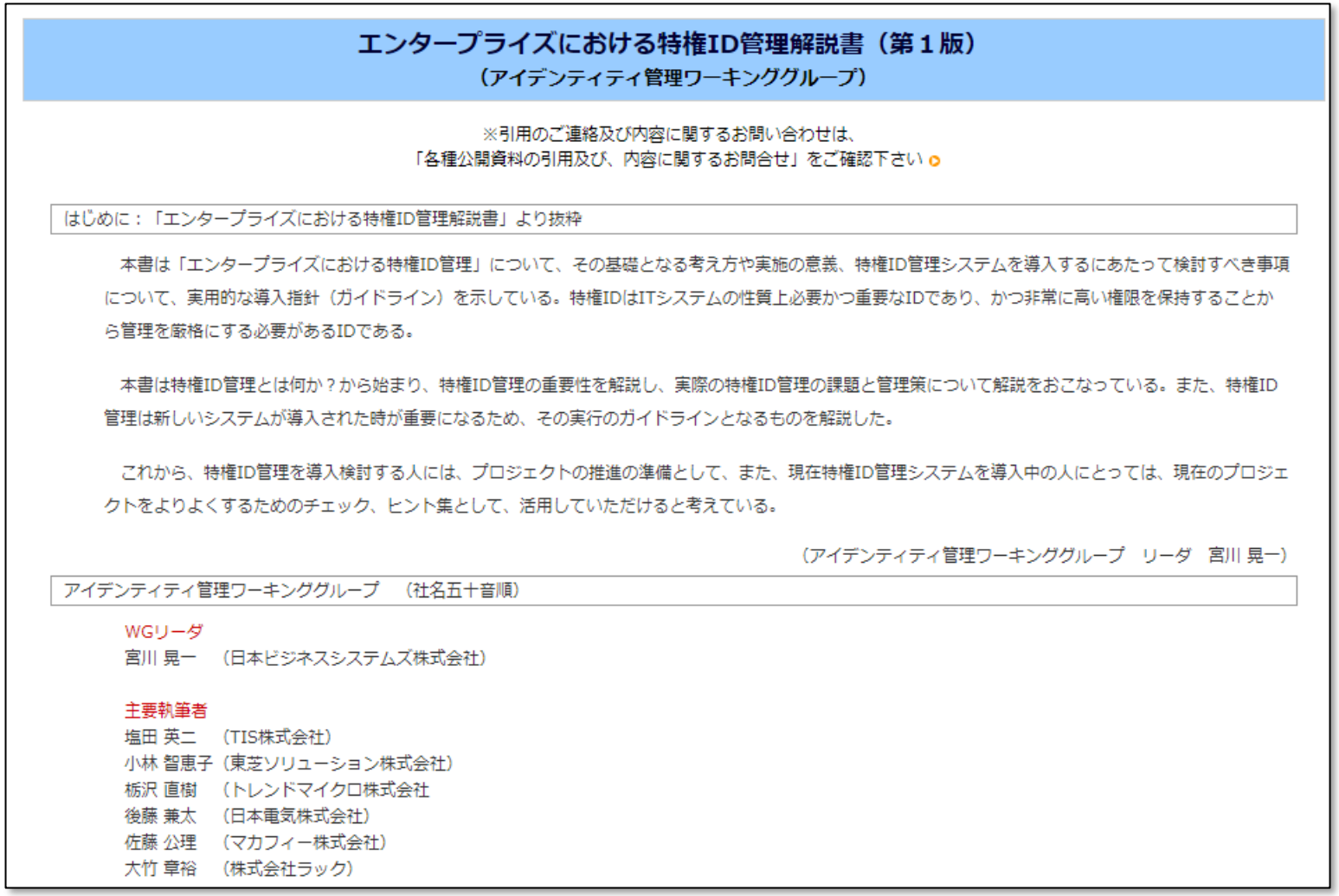
設計できるもの（社内システム用のアクセス権）から
最初から決まっている・存在するもの（SaaS やIaaS のアクセス権）へと管理対象が広がり、
より効率的・効果的なロール管理が必要になってきた。

<u>ロール管理自体の深化・進化が必要</u>

クラウド等の複雑なアクセス権への対応
変わらない失敗例を解決する方法（棚卸・分析）

特権ID管理　今昔

特権管理　昔から行われている



エンタープライズにおける特権ID管理解説書（第１版）
（アイデンティティ管理ワーキンググループ）

※引用のご連絡及び内容に関するお問い合わせは、
「各種公開資料の引用及び、内容に関するお問合せ」をご確認下さい

はじめに：「エンタープライズにおける特権ID管理解説書」より抜粋

本書は「エンタープライズにおける特権ID管理」について、その基礎となる考え方や実施の意義、特権ID管理システムを導入するにあたって検討すべき事項について、実用的な導入指針（ガイドライン）を示している。特権IDはITシステムの性質上必要かつ重要なIDであり、かつ非常に高い権限を保持することから管理を厳格にする必要があるIDである。

本書は特権ID管理とは何か？から始まり、特権ID管理の重要性を解説し、実際の特権ID管理の課題と管理策について解説をおこなっている。また、特権ID管理は新しいシステムが導入された時が重要になるため、その実行のガイドラインとなるものを解説した。

これから、特権ID管理を導入検討する人には、プロジェクトの推進の準備として、また、現在特権ID管理システムを導入中の人にとっては、現在のプロジェクトをよりよくするためのチェック、ヒント集として、活用していただけると考えている。

（アイデンティティ管理ワーキンググループ　リーダ　宮川 晃一）

アイデンティティ管理ワーキンググループ　（社名五十音順）

WGリーダ
宮川 晃一　（日本ビジネスシステムズ株式会社）

主要執筆者
塩田 英二　（TIS株式会社）
小林 智恵子（東芝ソリューション株式会社）
栃沢 直樹　（トレンドマイクロ株式会社
後藤 兼太　（日本電気株式会社）
佐藤 公理　（マカフィー株式会社）
大竹 章裕　（株式会社ラック）

- 特権IDが、
  企業にとって大事、
  ということは変わっ
  ていない

引用元：エンタープライズにおける特権ID管理解説書（第１版）（アイデンティティ管理WG）| JNSA
https://www.jnsa.org/result/2016/idm_pum/index.html

特権ID管理　今昔

昔

監査対応

「特権ID管理」

今

サイバーセキュリティ対策

「特権アクセス管理」

特権ID管理　今昔

昔

オンプレ、OS/DB

IT管理者/開発者/運用者

パスワード

貸出

作業の録画

今

オンプレ＋IaaS/PaaS/SaaS

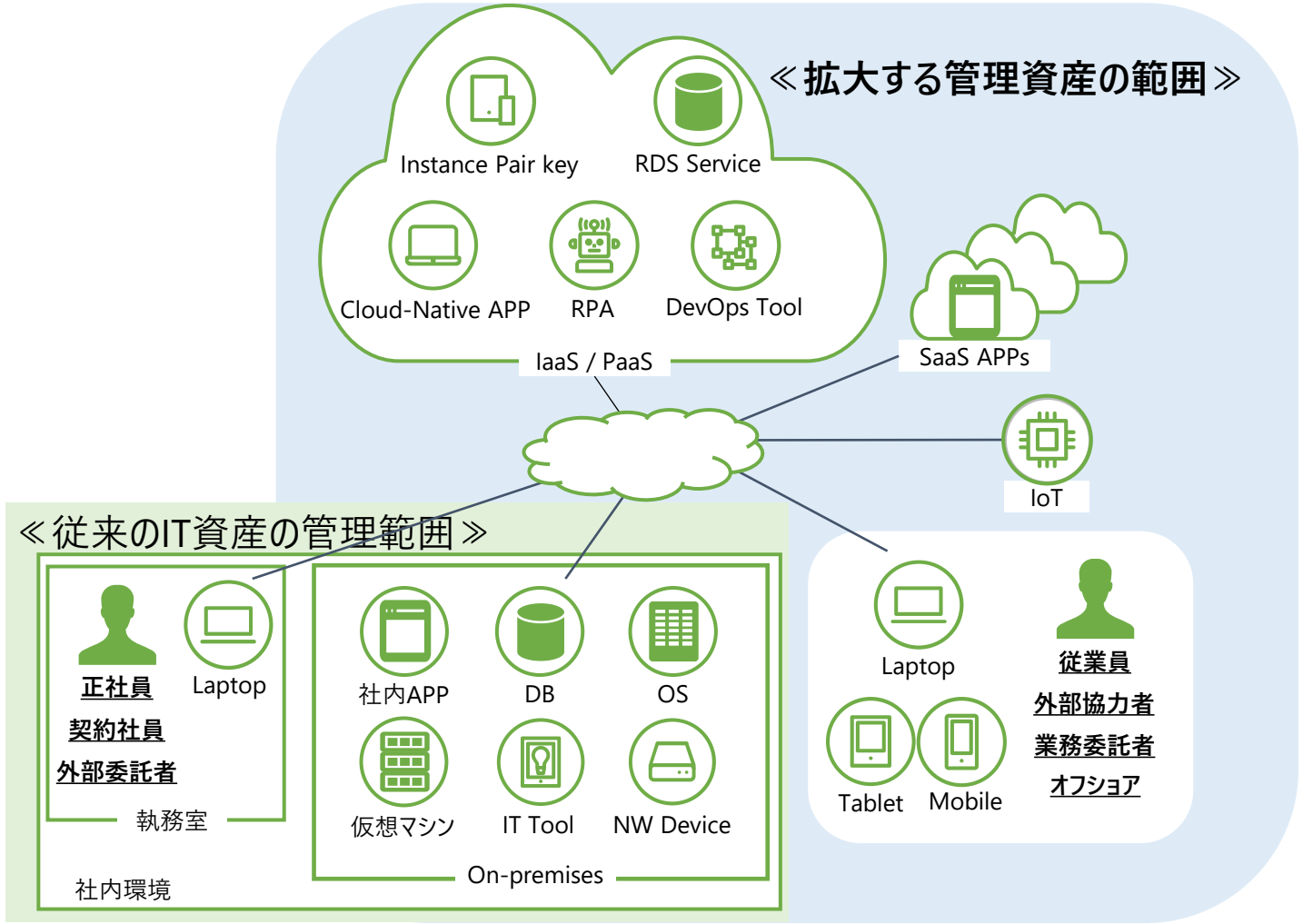
IT管理者、開発者、運用者、委託先、パートナー、人ではないアカウント（サービス/RPA/組込み）

パスワード+鍵+トークン

貸出・短期間

作業の録画＋不正操作検知・制御

拡大するIT管理資産の範囲と特権



① IT資産の存在場所が多様化

- 従来はNWで守られた範囲内にIT資産が存在したが、今後はその範囲外の　**広域NWにIT資産が存在**する
- IoTによる他企業とのサービス連携を実現した場合、**サプライチェーン全体で保護**　する必要がある

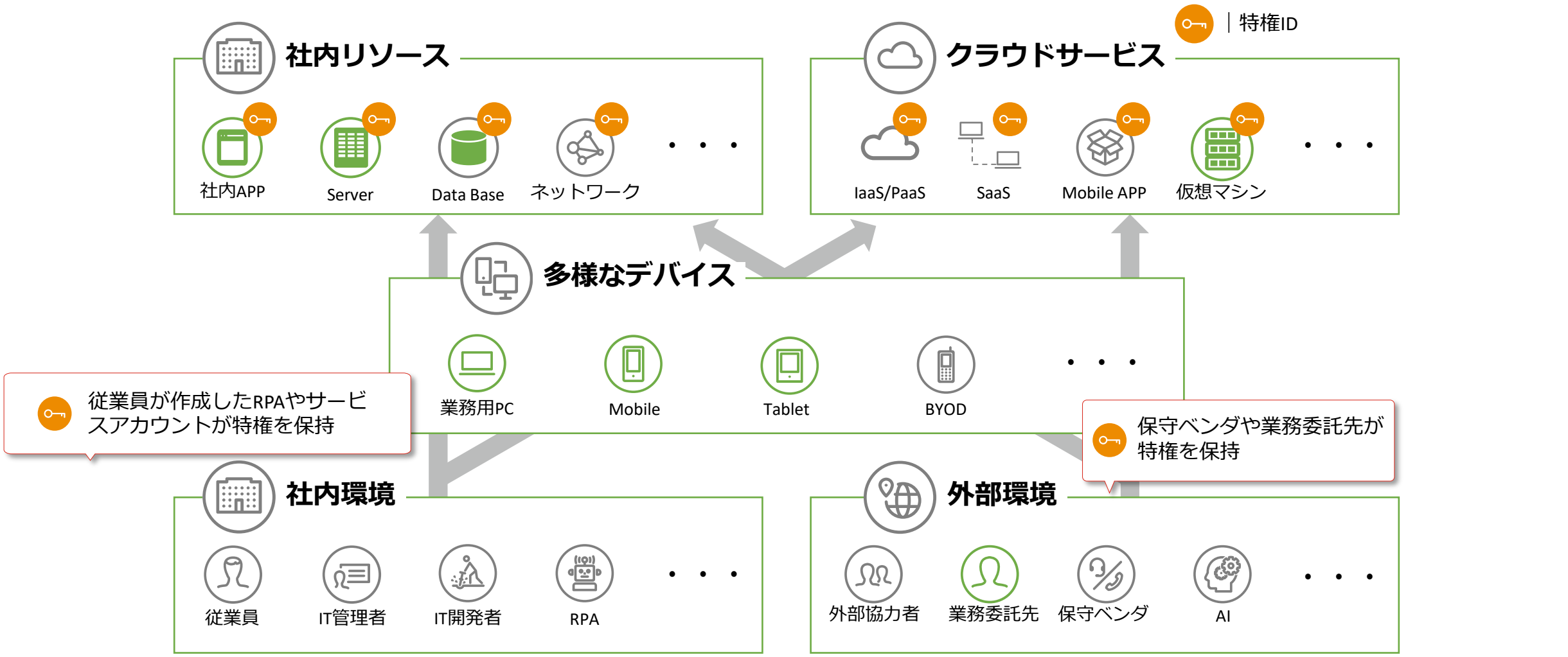
② ID/PW以外の管理の必要性

- 人が利用するID/PWのみならず、**Robotやサービス/埋め込みアカウントが利用するID/PWを管理**する必要がある
- **EC2キーペア、APIのアクセスキー、SSHキー等を利用した特権利用を管理**する必要がある

③ 利用者、利用端末の多様化

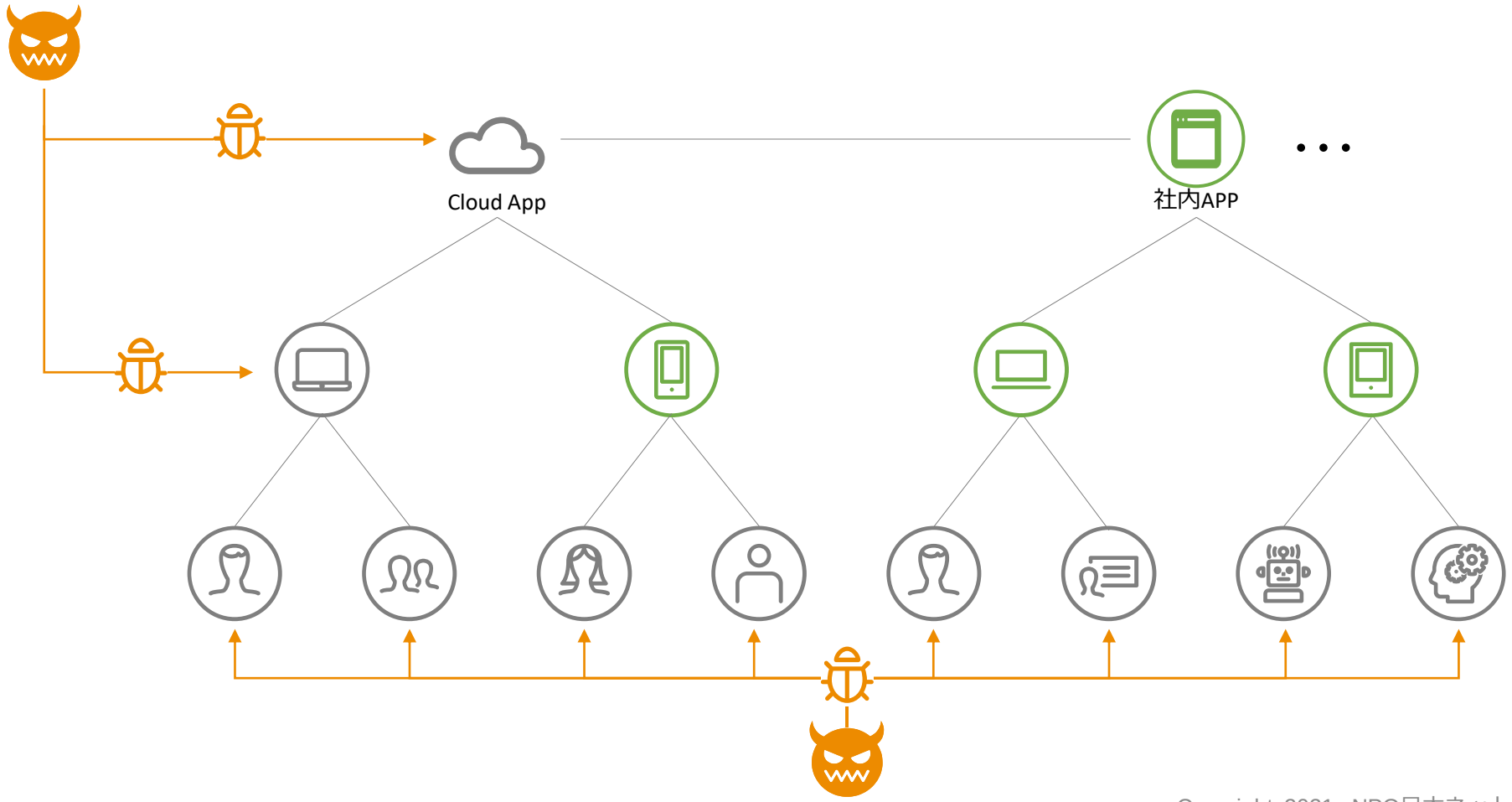
- 業務委託者や海外オフショア等**利用ユーザが多様化**する
- 自宅等社内以外の環境やモバイル/ タブレット等**接続端末が多様化**する

分散する特権

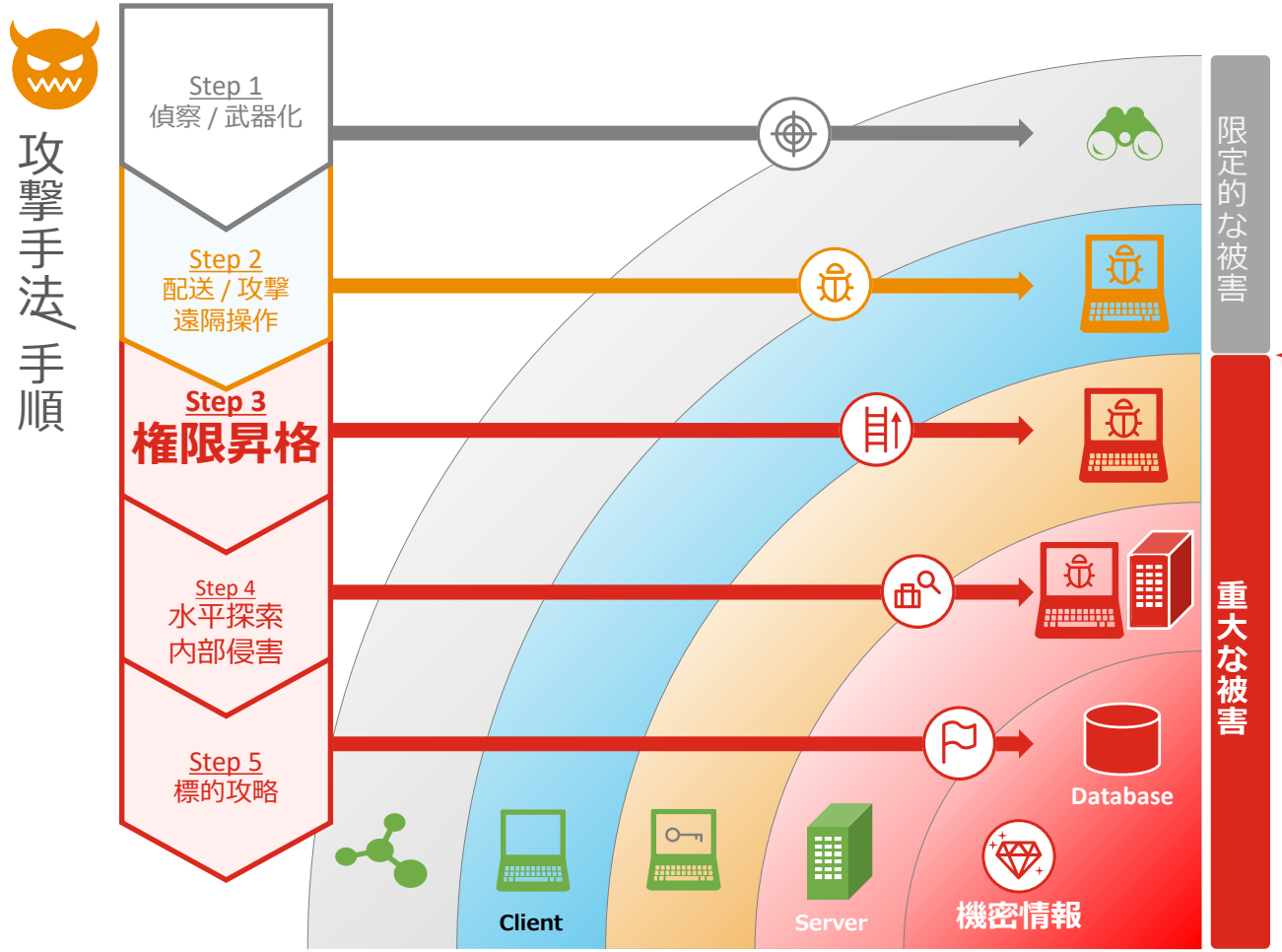


だからこそ難しい防御

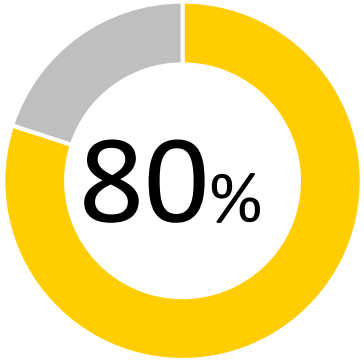
複雑化するIT環境は脅威の侵入経路を増大させる



サイバーセキュリティ対策としての特権管理



特権の奪取と昇格が被害拡大の境界となる



セキュリティ被害の80%は特権の認証情報を利用している*

*調査会社フォレスター情報

特権ID管理　今昔

昔

監査対応

「特権ID管理」

今

サイバーセキュリティ対策

「特権アクセス管理」

まとめ

再発見したのは？

まとめ

- IT環境の変化、アイデンティティ管理の必要性
  - **クラウドシフト等で複雑化する環境では、アイデンティティがアクセス境界となる**
- アイデンティティ管理　今昔
  - **継続的に、アイデンティティ情報を確認・レビューし、最小権限の原則を維持することが必要**
- ロール管理　今昔
  - **ロール管理の考えの必要性は変わらない**
  - **ロール管理自体の深化・進化が必要**
- 特権ID管理　今昔
  - **特権ID管理は、今後サイバーセキュリティ対策として扱い、スコープの広がりやリスクを勘案したうえで対応する必要がある**

まとめ

サイバーセキュリティ対策・ITガバナンスの視点から
アイデンティティ管理を変革していきましょう！