\Orchestrating a brighter world NEC

「それって持続可能なセキュリティですか？」
～クラウドサービスをセキュアに活用するコツ～

https://jpn.nec.com/event/220720sec/index.html

2022年7月20日 12:05～12:50

日本電気株式会社
サイバーセキュリティ事業統括部

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

本日のタイムテーブル

12:05	はじめに（ご連絡事項など）
（25分）	クラウドシフトに伴うセキュリティリスクと対策 芝宮 礼継（CISSP / NEC サイバーセキュリティ事業統括部　マネージャー）
（15分）	クラウド時代に欠かせない！ ID管理の進め方 外山 英尚（CISSP / NEC サイバーセキュリティ事業統括部　マネージャー）
（5分）	質疑応答
12:50	（終了）

\Orchestrating a brighter world NEC

「それって持続可能なセキュリティですか？」
～クラウドサービスをセキュアに活用するコツ～

クラウドシフトに伴うセキュリティリスクと対策

日本電気株式会社
サイバーセキュリティ事業統括部
マネージャー 芝宮 礼継（CISSP）

クラウドシフトに伴うセキュリティリスクと対策

1. ますます高まるクラウドのリスク対策
2. クラウドの設定ミスに備える
3. 重要情報を保護する

1.ますます高まるクラウドのリスク対策

クラウド活用がDX推進・事業成長のカギ

クラウドファーストとする企業

66.4%

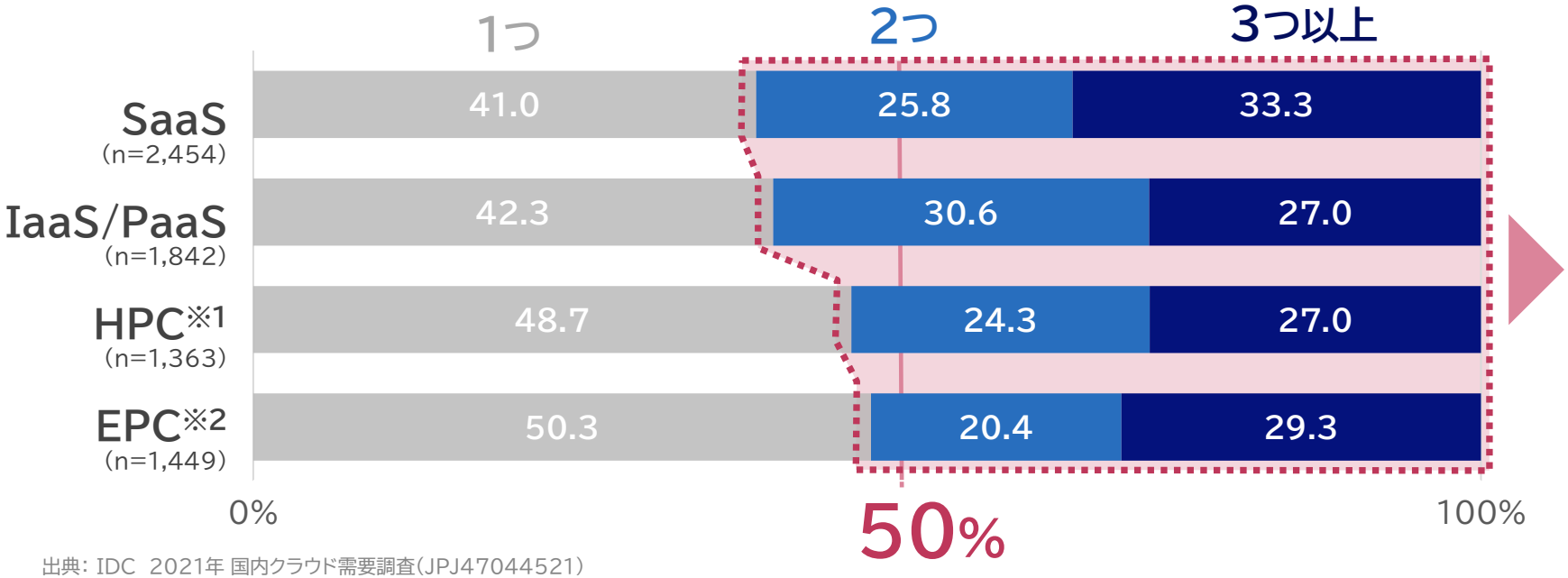
SaaSを利用する国内企業

46.1%

クラウド利用中の企業において
DX推進部門を設立している企業

39.9%

利用中のクラウドのベンダーや技術／サービスの総数



クラウドを利用中の企業の
半数以上は
マルチクラウド化

出典：IDC　2021年 国内クラウド需要調査(JPJ47044521)
※1 Hosted Private Cloud　※2 Enterprise Private Cloud

セキュリティリスクの変化　＜経営インパクト＞

DXが急速に進む一方で、**経済目的でのサイバー攻撃が激化**
あらゆるシステム・データが標的となり、**企業の事業継続が脅かされている**

ランサムウェア被害※

被害報告件数　約4倍
FY20下期21件→FY21下期85件
（警察庁に報告があった件数）

被害対象：企業規模を問わず広範に
大企業34%　中小企業54%

感染経路
VPN機器、リモートデスクトップからの
侵入 74%

脆弱性公表直後から
脆弱性を標的
としたアクセス急増

サイバー攻撃による経営インパクト（例）

基幹システム停止
決算発表を延期
製造業大手

国内十数工場
稼働停止
大手部品メーカー

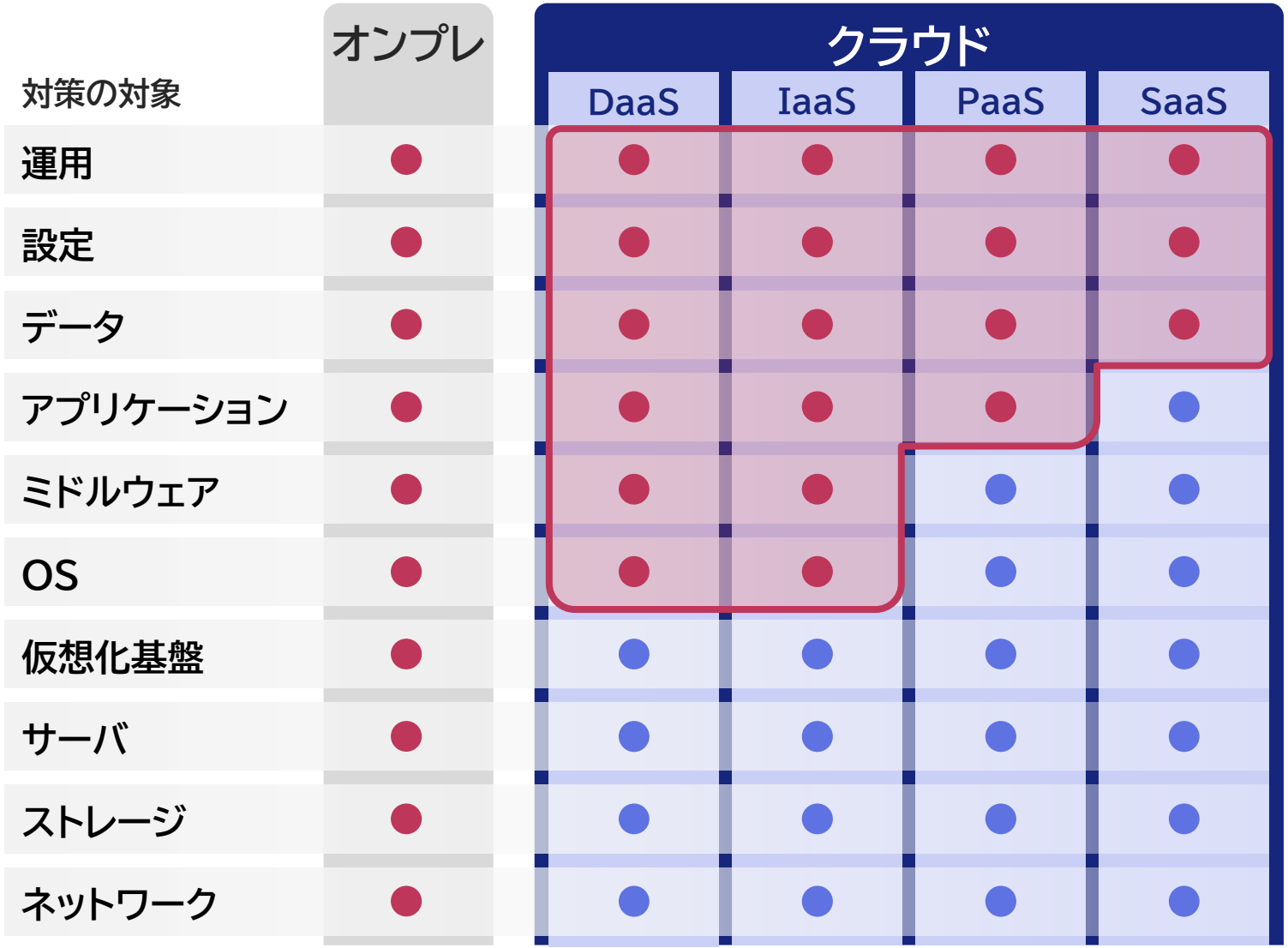
診療 数ヶ月停止
地域医療が 混乱
医療機関

サイバー攻撃の調査／復旧費用
特別損失 **数億円**
コンサル大手

DX化によりシステム間連携が進むことで、被害は1つの企業に閉じない

※ 出典：令和3年におけるサイバー空間をめぐる脅威の情勢等について（速報版）（警察庁　2022/2/10）　https://www.npa.go.jp/publications/statistics/cybersecurity/data/R03_cyber_jousei_sokuhou.pdf

クラウドにおける責任範囲(責任共有モデル)



セキュリティ対策の責任範囲

- ●・・・契約者(対策が必要)
- ●・・・クラウド事業者

クラウドサービス利用であっても
ソフトウェアの不具合対策や
設定の責任は

全てユーザ

より一層、

セキュリティ対策が重要に

クラウドシフトで今後対策すべきポイント

課題	対策ポイント	
クラウドサービスの頻繁な機能アップデート サービス仕様の理解不足による設定ミス	ワークロードの**設定**管理	サイバーハイジーン
クラウドシフトにより、データの格納場所・アクセス元が分散、 ガバナンスが困難に サービス種別を問わず、クラウド上のデータ保護は、ユーザ責任	**情報**管理	重要情報管理、データガバナンス
境界防御の限界、ゼロトラストの考え方で全てのアクセスを検査 SaaS利用の加速に伴う、ID体系の統一化	**ID**管理	目的や方針の明確化

2.クラウドの設定ミスに備える

クラウド環境でも変わらないリスクと高まるリスク

変わらないリスクの代表例

脆弱性を突いた外部からの不正侵入

- IaaS環境においてはオンプレミスと同様
  プラットフォーム/アプリケーションの脆弱性対処は
  ユーザ責任

オンプレミス

IaaS

高まるリスクの代表例

設定ミスに起因した情報漏えい

- クラウド環境では設定ミスが情報の漏えいに直結
- 一方で、日々進化するクラウドに対してセキュアな
  設定を維持し続けることが難しくなりつつある

SaaS

脆弱性への対策を
最初から考慮しておくことが必要

クラウド活用を前提とした
設定管理の仕組みが必要

クラウド環境におけるセキュリティインシデント

脆弱性が起因ではなく、ユーザ側の設定ミスが起因でのインシデントが発生

WAFの設定ミスに起因したAWS環境への不正アクセス（2019年7月）

米金融大手が利用していた
WAFに設定ミスが存在

不正アクセス者は設定ミスを悪用し、
WebAP攻撃によりAWS EC2の
インスタンスメタデータへの接続に成功

個人識別情報（PII）を含む数百GBもの情報が漏えい（1億人以上が被害）

IaaS/PaaS（クラウドストレージ）の設定ミスによる顧客データ公開、漏えい

Amazon S3の**アクセス権限の設定ミス**によるデータ公開

Azure Blob storage**の設定ミス**

米大手小売 数十万人以上の顧客データ、百数十GB（2021年3月）

ジャーナリストやスポーツ選手の個人情報漏えい（2021年2月）

SaaSの設定不備に起因した第三者によるアクセス（2020年12月）

Salesforceの設定不備で
情報流出の可能性を相次ぎ発表

- **大手ECサイト最大百数十万件**
- **大手キャッシュレス決済サービス最大数千万件など**

金融庁やNISC（内閣官房サイバーセキュリティセンター）から注意喚起発出

AWS環境の設定ミスに起因した個人情報の漏えい（2022年7月）

2年以上にわたり、個人情報がGoogle検索で丸見え状態

事象　与信管理サービスを提供する企業の教育システムの一部情報がインターネットに公開され
インターネット検索エンジンに**25**万人の会社名および氏名が表示

期間　2020年2月から2022年6月までの**2**年以上

原因　AWS移行時の**ネットワークの設定ミス**

- **初めて自社のみで**AWSにシステム移行
- **個人情報の洗い出し**が不十分
- **セキュリティ対策見直し**が不十分
- **チェック体制**が不十分

出典:リスクモンスター株式会社　2022/7/5 サイバックス Univ.システム連携用サーバーの個人情報漏えいについて
https://www.riskmonster.co.jp/rm_sys/uploads/2022/07/サイバックスUniv.システム連携用サーバーの個人情報漏えいについて.pdf

クラウド設定ミス防止への対策

分散・巨大化・複雑化、煩雑なアップデートへの対応など、従来の管理方法の限界
クラウド設定管理ツールの活用が有効

なぜ、クラウド設定ミスが多発するのか

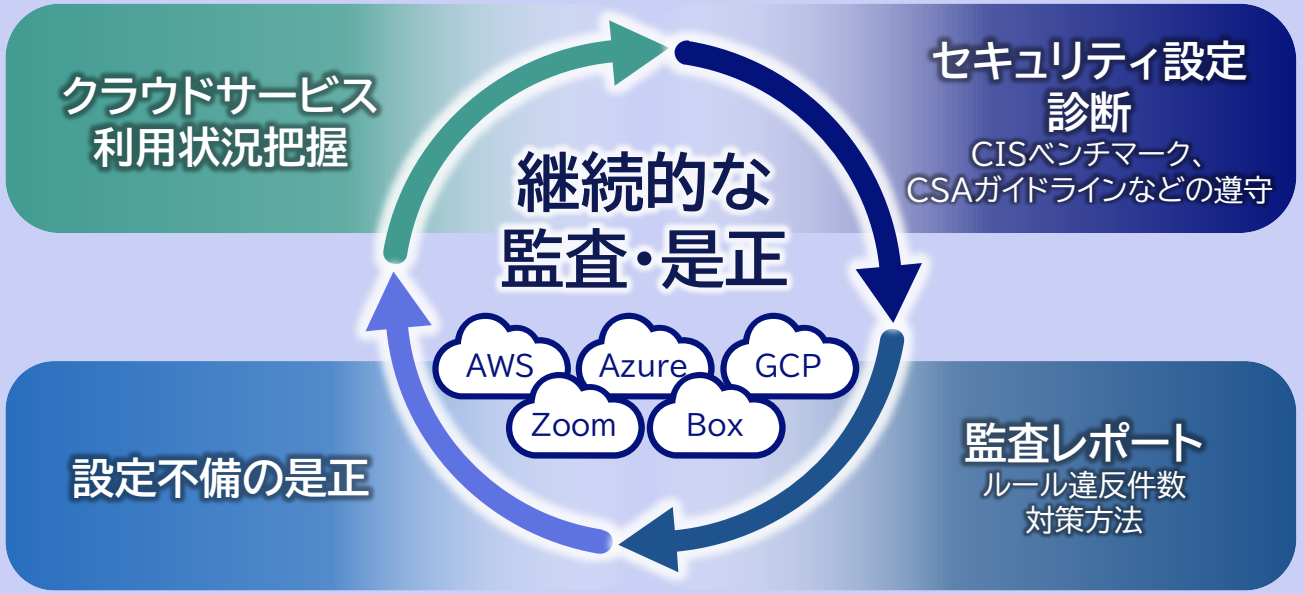
ワークロード管理の複雑性増大
・複数のIaaSをマルチクラウドとして活用
・PaaS、コンテナ、サーバレス活用

頻繁、煩雑なアップデート
・事業者側タイミングでのアップデート
・頻度が多く設定変更が把握しきれない
・DevOps適用によるリリースサイクル短縮化

IT部門での実態把握が困難
・SaaS利用急増で管理が追い付かない
・運用が事業部門任せ、実態が把握できない

クラウド設定管理ツールの活用による対策

設定不備などを自動で可視化、是正



CSPM(Cloud Security Posture Management)、SSPM(SaaS Security Posture Management)

ソリューション例と監査ポリシーの例

ソリューション例

CSPM（Cloud Security Posture Management）

IaaS/PaaSの設定管理

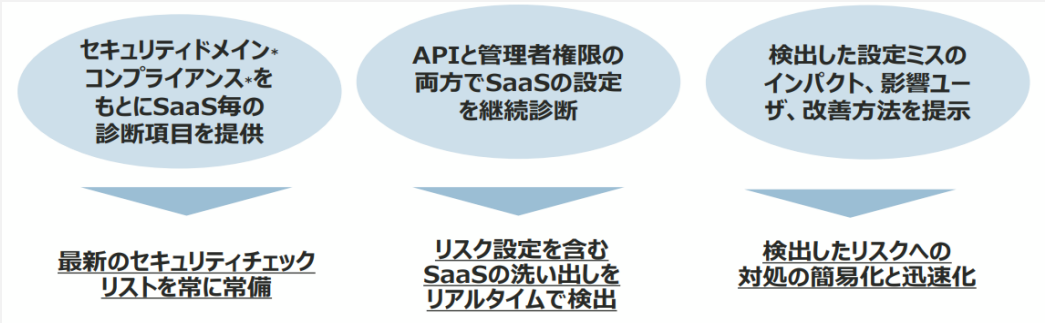
各クラウドプラットフォームのAPI経由で → セキュリティ設定状況を自動的に可視化 → 必要に応じて自動対処やレポートを作成

PaloAlto Prisma Cloud　利用イメージ

SSPM（SaaS Security Posture Management）

SaaSの設定管理

Office 365やBOX等のSaaSの設定状況の見える化、リスク洗い出し



Adaptive Shield　利用イメージ

監査ポリシー例

Prisma Cloud　利用の場合

ポリシー	チェック内容
コンフィグ	● IAMユーザにMFAが有効化されていない → クラウドベンダのセキュリティ推奨事項 ● S3バケットのアクセスログが有効化されていない → 監査、コンプライアンス要求の際に必要 ● VPCフローログが無効になっている → インシデント発生時などにネットワークトラフィックログ解析が有効 ● IAMパスワードポリシーが設定されていない、設定されているパスワードポリシーの強度が弱い、 パスワードの期限が90日以上 → パスワードに関する設定の強度を標準以上に保つ ● セキュリティグループでSSH、RDPがインターネットからの通信が許可されている
ネットワーク	● インターネットからの通信を許可しているサーバもしくはDBインスタンスが発見された → 外部から直接アクセスを許可すべきでないインスタンスをチェック ● DDoS攻撃を受ける可能性のあるMemcacheが発見された →バージョン1.5.5以下のMemcacheにDDoS攻撃の脆弱性があるため ● BitcoinやEthereumマイニングで利用されるポートへの内部からの通信を検知 → 既にビットコインマイニングの可能性が検知された
イベント監査	● ルートユーザの利用が発見された → ルートユーザの利用は非推奨 ● 各種セキュリティ的に重要なコンフィグの変更が発生 → 変更の妥当性を確認
アノマリ	● 数千キロ離れた場所から数分後に同じアカウントでログインが成功している ● いつも利用しているOS、ブラウザと違う環境からログインしている ● いつもはS3バケットしか利用していないアカウントがEC2やIAMにアクセスしてきた

3.重要情報を保護する

組織として守らなければならない情報資産

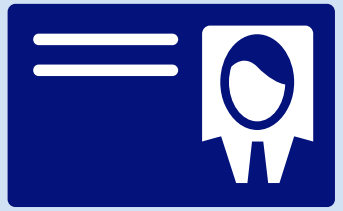
知財・研究

技術情報

顧客情報

営業秘密情報

経営情報/財務会計/人事・給与



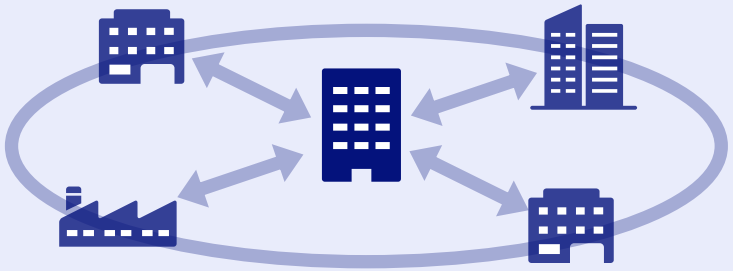
社内システム(アカウントなど)

企業価値・競争力の源泉となる重要情報

重要情報管理を取り巻く環境の変化

地政学リスク、経済安全保障

個人情報保護法・GDPR
などの法令順守



サプライチェーン
取引先との情報共有

多様な働き方

「情報管理」と「有効活用」の バランスの変化

今考えるべきデータガバナンス

守るべき情報がオンプレミスからクラウド上へ移行、
社外からのリモート接続が増加して従来のネットワーク境界中心の対策では限界

安全だけでなく“安心”を考慮したデータガバナンス

- データを海外で保存していた事が問題に（どこに保管しているか）
- 国内サーバのデータを海外従業員が閲覧可能で問題に（誰がアクセスしているか）
- 転職者が前職のデータを持ち込んで訴訟に（どんなデータ）

データ重要度・機密性を考慮したクラウドサービス選定

- 米国クラウド法が適用される事業者のクラウドサービス利用の場合、国内外に関わらず米政府がデータ開示要求可能
- 重要度や機密性によっては、国産基盤やオンプレでのデータ保管が必要
- クラウド上で保存されているデータを適切なユーザのみ閲覧可能とする仕組みが必要

重要情報の管理プロセス

年次サイクルの管理プロセスで重要情報を管理運用

重要情報の指定

- 「企業秘密管理規程」を基に、事業部門単位に「重要情報判定基準」を作成
- 「重要情報判定基準」を全社で可視化

重要情報の管理運用

- 「重要情報判定基準」を基に保有する情報に秘密区分を指定し、運用
- 「最高機密事項管理台帳」、「極秘事項管理台帳」を作成
- これらの台帳を全社で可視化

重要情報の点検

- 重要情報の管理運用に関する点検を実施
  必要に応じて改善を実施
- 点検結果を全社で可視化

重要情報管理の監査

- 内部監査部門による監査を受審し、必要に応じて改善を実施
- 内部監査部門は、経営陣へ監査結果を報告

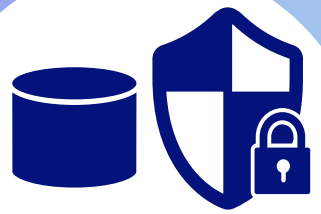
【参考】NECグループの重要情報保護に対する取組-全体像

ガバナンス(重要情報管理ルール制定、体制構築、情報の見える化)と
IT対策(多層防御)により重要情報を保護

ガバナンス

ポリシー策定、運用

- 重要情報管理ルール制定
- 重要情報管理体制構築
- 重要情報の見える化
- 重要情報管理ライフサイクル



重要情報
保護

IT対策(多層防御)

ユーザ・デバイス識別基盤

認証基盤

マイクロセグメンテーション/SDP

- 暗号化対策
- トラッキング
- アクセス制御
- ネットワーク分離

システムに対するリスク評価

SDP(Software-Defined Perimeter)

AIP統合ラベルによる情報ラベリング・暗号化

AIP統合ラベルにより、情報（ファイル）単位での暗号化・アクセス権管理、トラッキングによる利用状況のトレース等を実現

※ AIP：Microsoft Azure Information Protection

実施内容

- 企業秘密管理規程を踏まえたファイルのラベリング
- 情報区分に応じた自動暗号化とアクセス管理（Officeファイル以外も含む）

実現価値

- クラウドや、リモートPCからデータが流出しても情報漏えいを防げる
- 情報区分応じた印刷禁止、添付禁止、保管場所の制御

AIP クラウドベースのデータ保護ソリューション AIP

- コンテンツにラベルを適用してドキュメントや電子メールの検出、分類、および保護

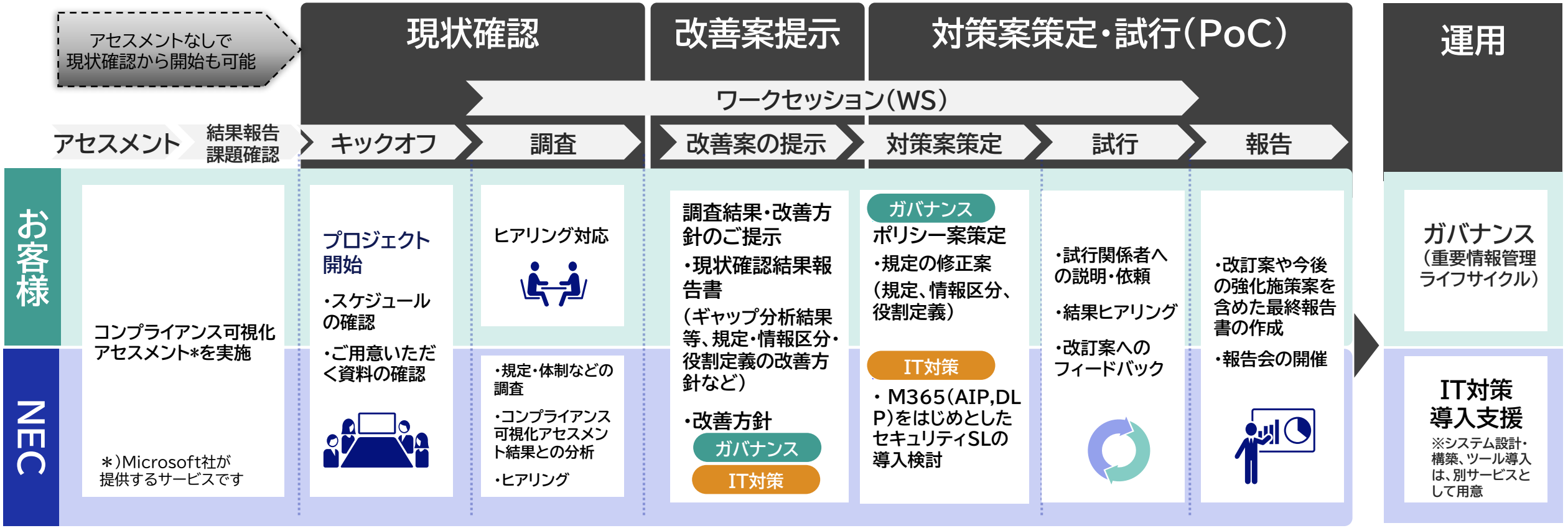
AIPの運用性を強化する InfoCage FileShell

- OfficeやPDF以外も拡張子を変えずに暗号化、利便性維持
- ローカルやファイルサーバ格納時の自動保護

ポリシーに従った柔軟で利便性を損なわない重要情報管理を実現

重要情報保護 現状確認・改善案提示サービス

アセスメント結果に基づき、課題を整理し「ガバナンス」「IT対策」両面における対策をご提案



【ユースケース】Microsoft 365 E3における重要情報保護

NECのM365セキュリティのプロフェッショナルによる支援と独自の付加ツールで、現実的な対策を実現

導入先情報

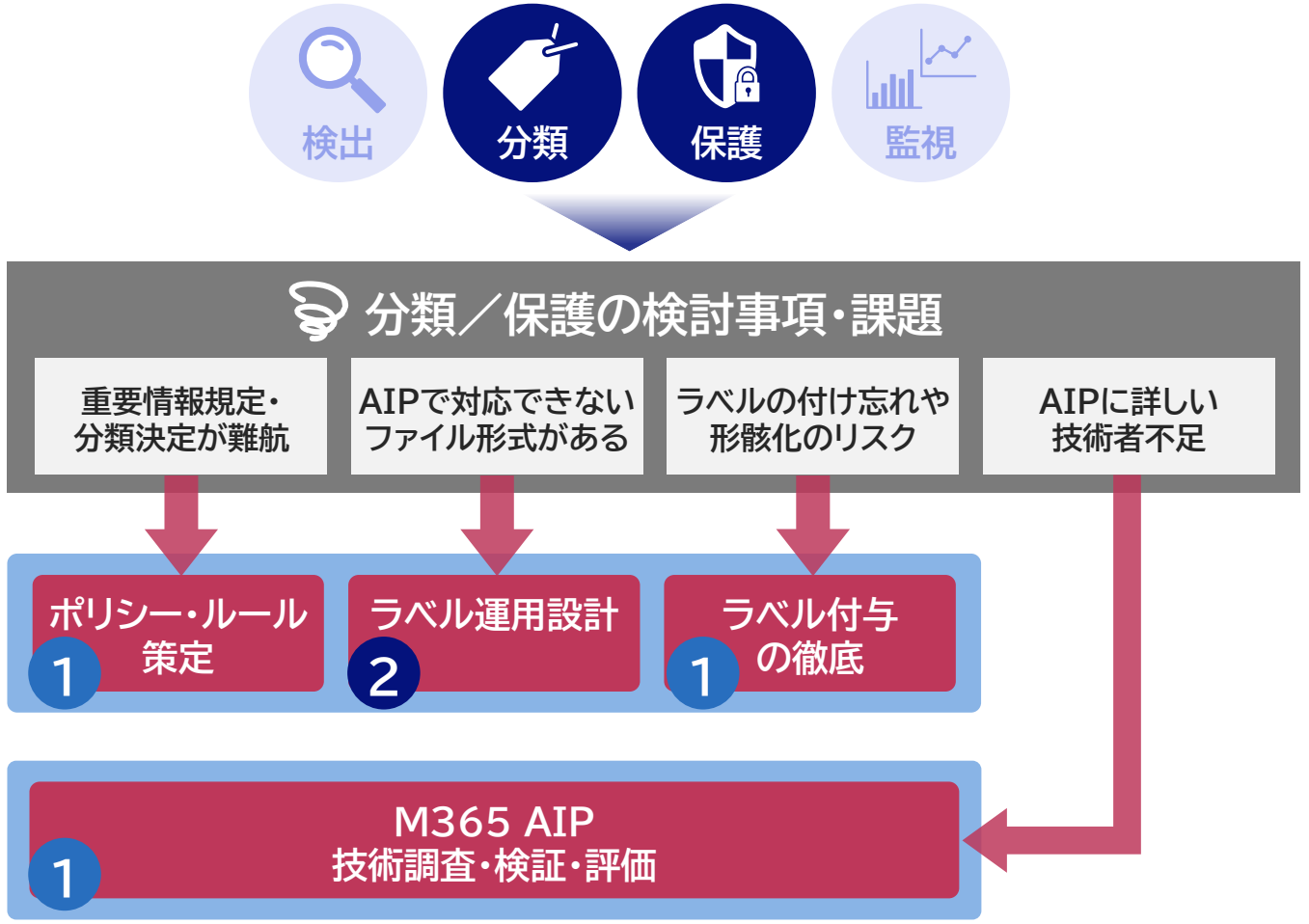
- 業種　：製造業
- 従業員数　：約3000名

NECのご支援内容

1 M365セキュリティ プロフェッショナルによる活用支援
- 運用実績のある管理方法・区分例の提示
- 効果的なポリシー設計や運用パターンの提示

2 NEC独自のAIP付加ツールの提供
(InfoCage FileShell)

M365 E3（AIP）を使った場合の機密情報保護のイメージ



\Orchestrating a brighter world NEC

「それって持続可能なセキュリティですか？」
～クラウドサービスをセキュアに活用するコツ～

クラウド時代に欠かせない！ ID管理の進め方

日本電気株式会社
サイバーセキュリティ事業統括部
マネージャー 外山英尚（CISSP）

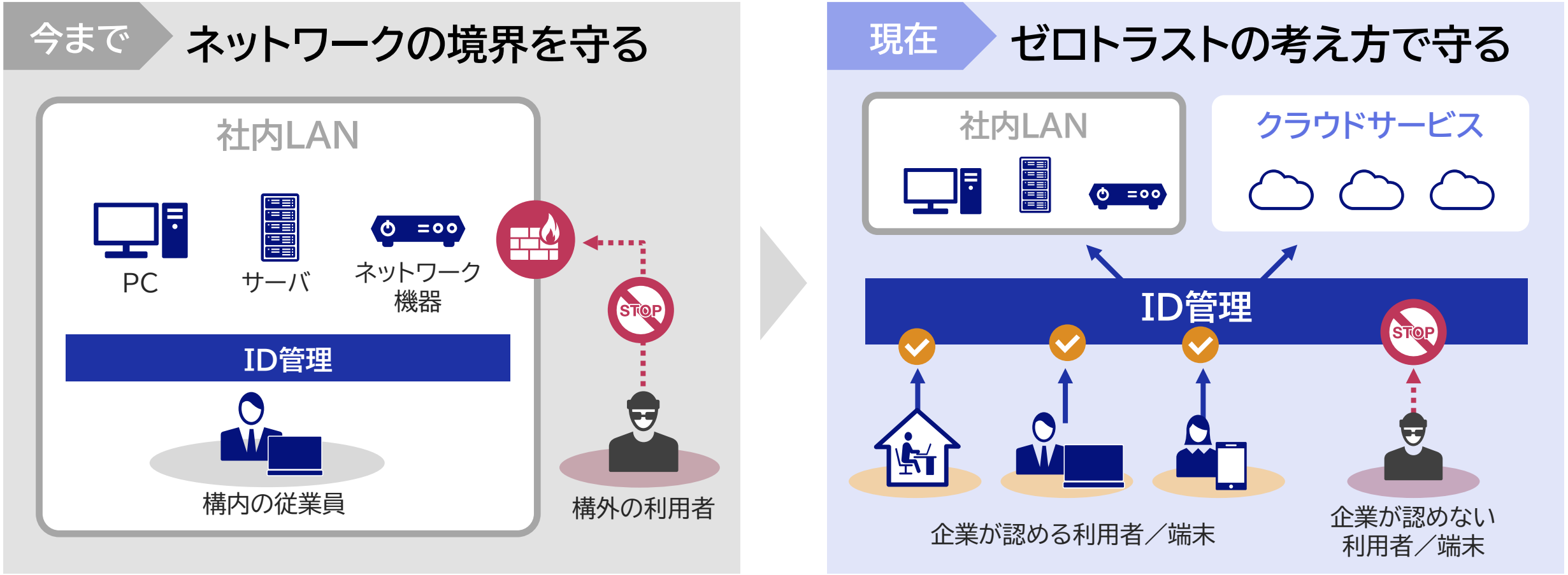
クラウド時代に欠かせない！ ID管理の進め方

1. 注目されるID管理
2. 導入のポイント
3. 事例と効果
4. NECのソリューション例

1. 注目されるID管理

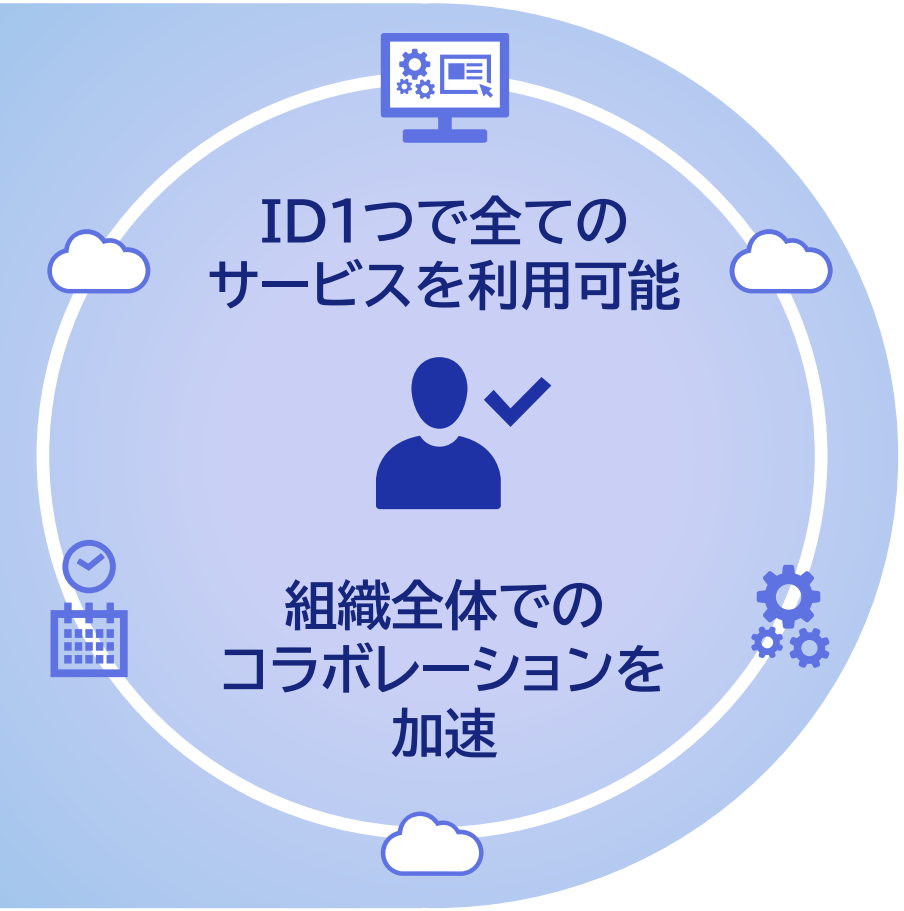
クラウド利用拡大とID管理の変化

- クラウドサービスの活用に伴い、安全性を担保する概念がネットワークの境界から身元の確認に変化
- ID管理の対象も従業員だけでなく、協力会社、サプライヤーなど拡大



ID管理に期待されること

- ゼロトラスト環境向けのセキュリティ対策だけでなく、利用者や管理者の業務効率向上
- クラウド活用の推進と、適切な情報共有が進むことになり事業拡大効果もあり



利用者

- 1回の認証で複数システムのログイン可能
- 複数のID情報を記憶する必要がない
- 様々な方法(生体認証)によりパスワードレス運用の実現

管理者

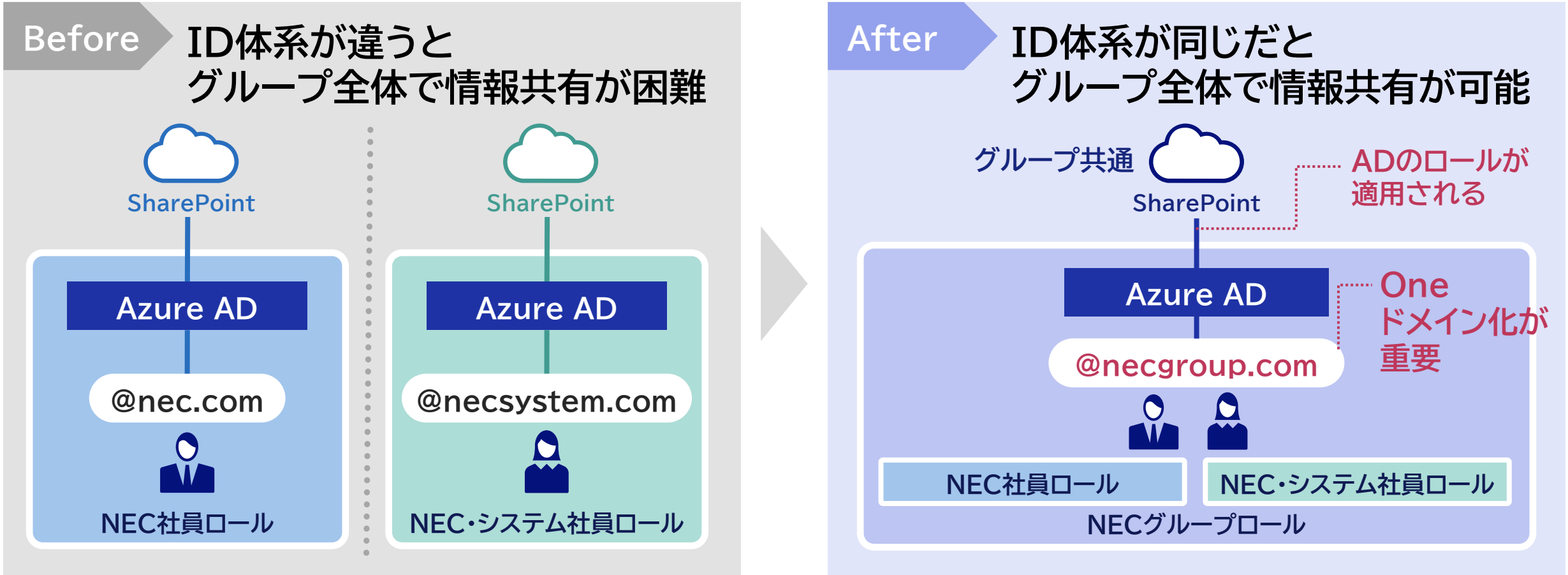
- パスワード問い合わせ対応負荷が激減
- ID統合で管理負荷軽減によるヒューマンエラーの防止
- 様々な方法(生体認証)でより高度なセキュリティを実現

経営者

- 組織全体で同一テナントのグループウェアSaaSを活用可能となり、事業加速

ID体系統合の必要性

ID体系が統合されていない場合やドメインが異なる場合、
情報共有サイトの利用に制約あり



統合ID管理と統合認証基盤の役割

統合認証基盤

アクセス者の身元確認と、認証した事実と情報をシステムへ渡す

認証機能

- ID／PW、多要素認証などにより利用者の識別と正当性検証を行う

認証連携機能(フェデレーション/SSO)

- 連携先アプリケーションへ正しく認証したことを伝え、SSOを実現する

統合ID管理基盤

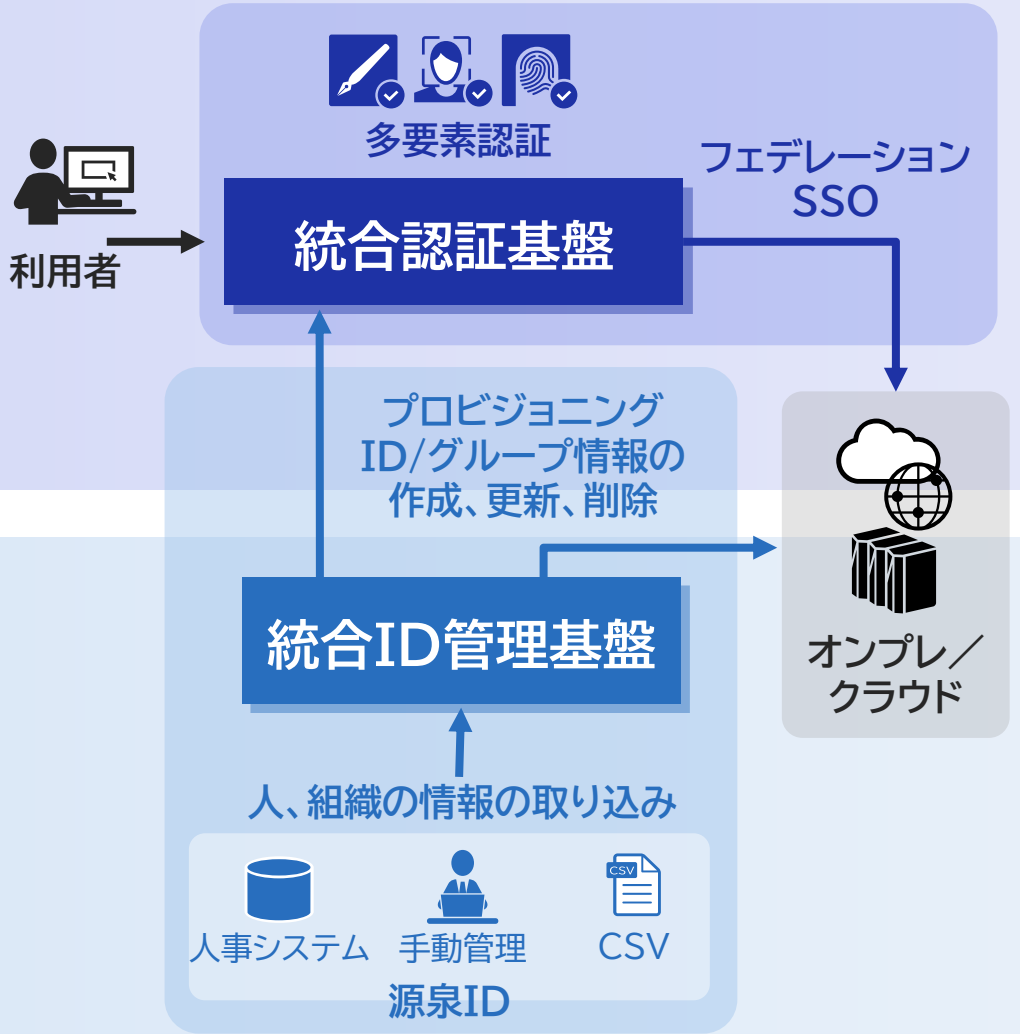
認証／認可の前提となるID情報を正しく保持し鮮度を維持する

利用者情報のライフサイクル管理

- ID情報を源泉(人事システムなど)から正しく取り込む
- 人事イベントなどのユーザ管理業務による変更に追随する

ID同期機能(プロビジョニング)

- 連携先アプリケーションへ、利用ポリシーに合わせて認証や認可に使うID情報を同期する、グループ情報を登録する



2. 導入のポイント

ポイント①　システム化の目的

システム化の目的(通常は複数)に合わせて、導入スコープを選定

目的例			統合認証基盤	統合ID管理基盤
セキュリティ向上	**認証強度の高い認証**	• パスワードレス、多要素認証	○	
	ゼロトラスト環境	• どこからでも/モバイルからでも 業務システムへアクセス	○	
	適切なアカウントとアクセス権の管理（ガバナンスなど）	• 実在するユーザの立場、職務に応じて適切なアクセス権の付与とはく奪		○
業務効率化	**利便性**	• 認証情報の集約＆シングルサインオンにより、シームレスな業務環境の実現 • さよなら、パスワードリセット申請＆対応	○	
	運用効率	• 人事イベントと同期した自動ID管理、ID管理業務の集約		○
	クラウドサービスの利用推進	• 認証統合し、社内部門、関係会社で共通のクラウドサービス(テナント)を使える環境にし、組織全体の業務効率の向上 • ノーモア クラウド毎のID/PW	○	○

ポイント②　実現の方向性を定める

Display Only

統合ID管理/統合認証基盤の実現の方向性を決定する事で、現状のシステム、将来像の明確化、業務に必要な機能を明確にすることが重要

詳細情報をご希望
または
ご質問・お問い合わせがございましたら、
以下までお願いいたします。

NEC　サイバーセキュリティ戦略統括部
セミナー事務局
cyber@seminar.jp.nec.com

ポイント③　統合ID管理PJの特性を理解して対策を行う

Display Only

多くの関係者を巻き込むことになるため、
PJの目的と実現イメージ、スケジュールを関係者と共有しながら進める

詳細情報をご希望
または
ご質問・お問い合わせがございましたら、
以下までお願いいたします。

NEC　サイバーセキュリティ戦略統括部
セミナー事務局
cyber@seminar.jp.nec.com

もし、3つのポイントを行わずに進めると…

① システム化の目的 ×　② 実現の方向性を定める ×　③ PJの特性を理解して対策 ×

セキュリティ面の不安

- 不要なIDが残存、IDの情報が不正確
- 利用現場に合わない認証方式

業務負荷増大

- 1つのシステムを使うのにも関わらず
  認証基盤と連携先システム双方でユーザ管理業務が必要
- IDの標準化を行わなかったため
  統合ID管理基盤/統合認証基盤が使えなかった
- 人事業務に関連したイベントに対処できないID管理システム
- システム導入の期間延長や改修費の増加

3. 事例と効果

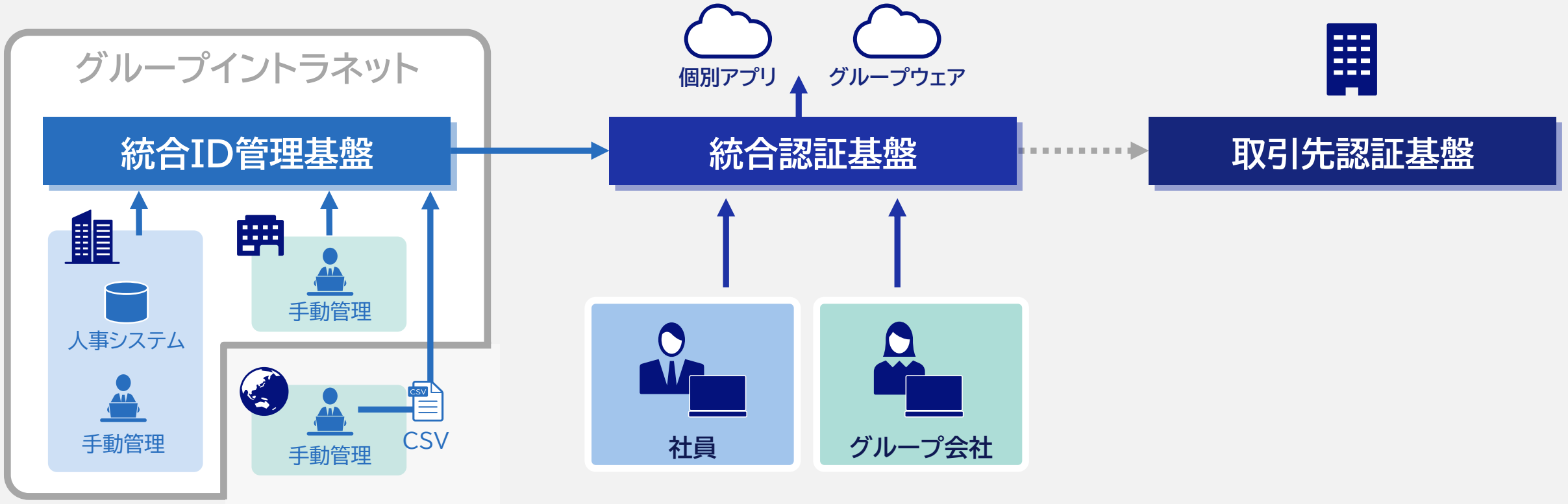
グルーバル全体での情報共有推進に向けた認証基盤

グローバル企業間での情報共有の推進に向け、統合認証基盤の実現イメージ（構成案、企業間の連携内容）を整理

グループ全体での
ガバナンス統一

どのシステムにも
同じIDでログイン可能に

取引先認証基盤への
認証連携



4. NECのソリューション例

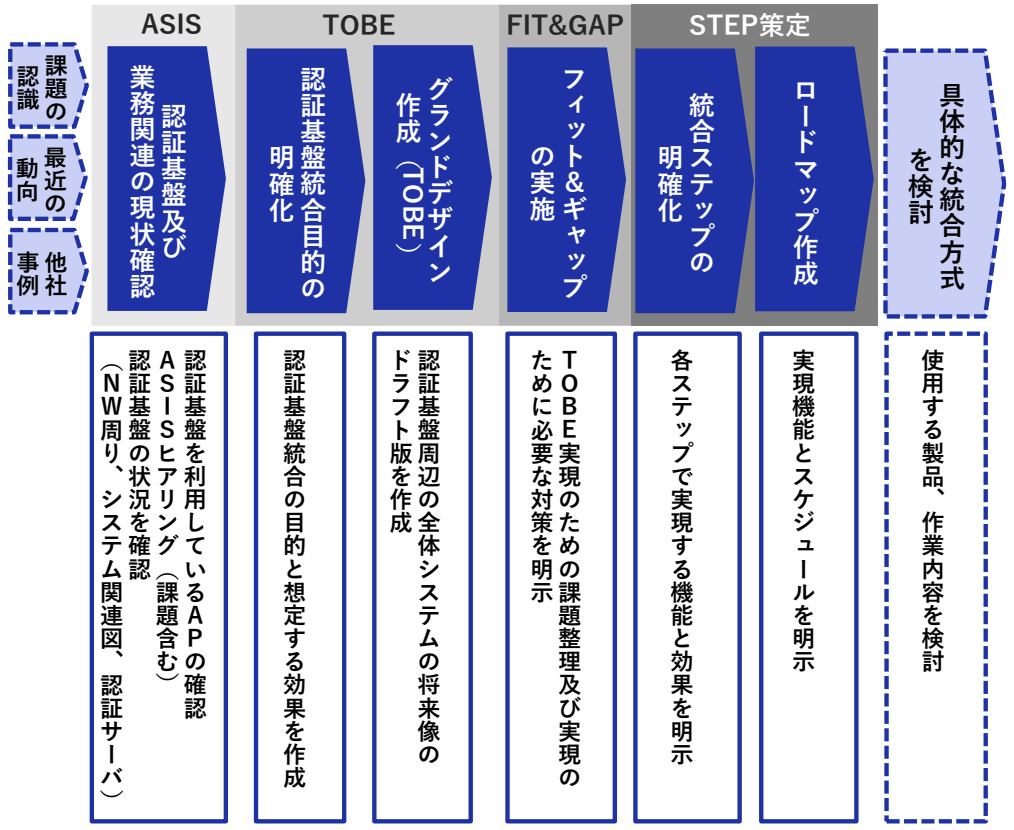
DXオファリング

クラウド型統合ID管理 企画・ポリシー策定支援サービス

コンサル

グループ企業の従業員ID統合のための、共通アクセス制御のポリシー立案や標準化を支援
ID管理運用コストを削減し、利便性の向上を図ることで、クラウドシフト/リフトを強力に後押し

サービス提供イメージ



お客様の課題

・テレワーク環境整備や業務システムのクラウド化を進めたい
・IDやアクセス制御、認証の考え方が組織ごとに異なることで発生している、運用コストの増大を解消したい
・ID管理の必要性を経営陣に説明できない

期待効果

・業務システムのクラウド化やテレワーク環境整備による働き方改革の実現
・ID管理の運用コストの低減と利便性の向上

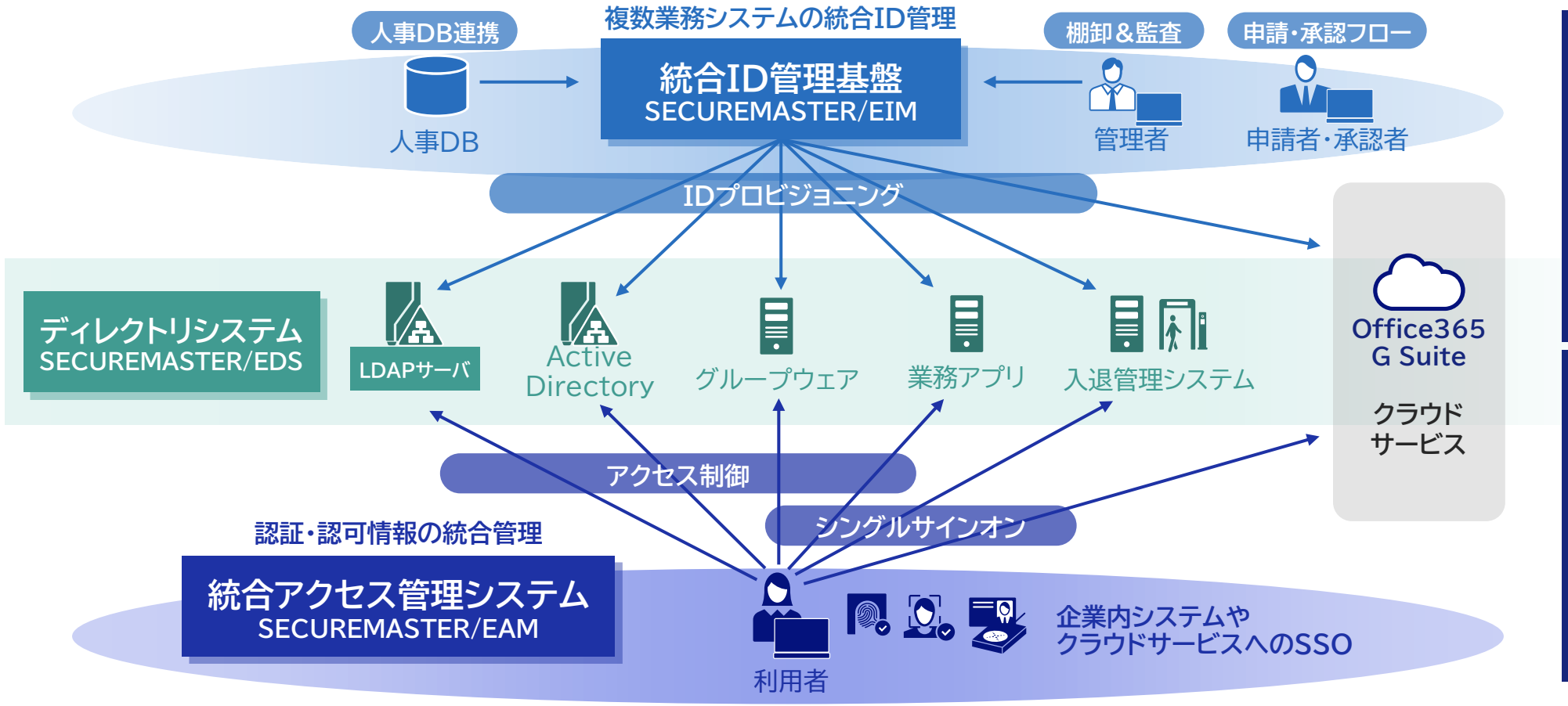
NECの特徴

・認証基盤構築に必要なデータマネジメントとID管理の両方の知見を持つコンサルタントがリーダーとして推進
・大手企業30社以上に対してコンサルティングを実施

WebSAM SECUREMASTER

統合ID管理基盤

- ID情報や認証・認可を統合管理、企業内システムやクラウドサービスへのシングルサインオンを実現
- ユーザ情報の管理コスト削減、セキュアなID・権限管理を実現。シングルサインオンで利便性が向上



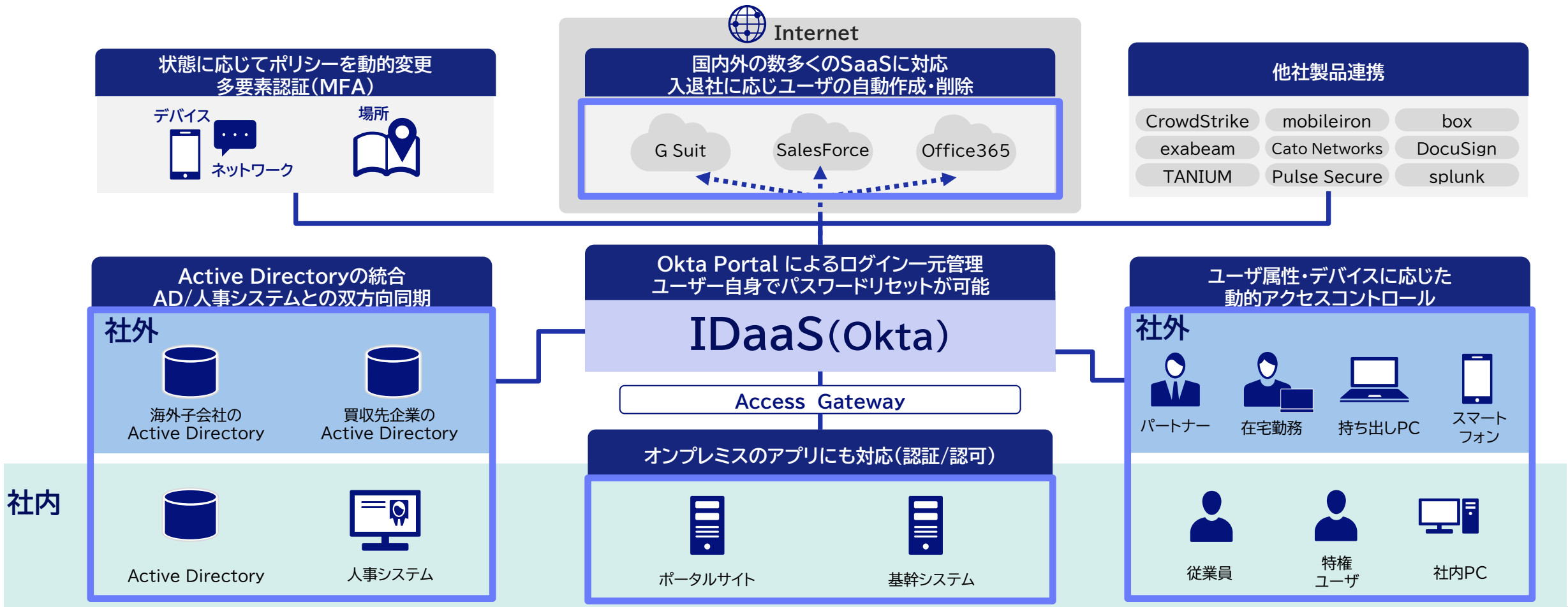
導入実績
900社
以上

複雑な
ID管理業務に
対応可能

Okta Identity Cloud

統合認証基盤

クラウド型のID管理サービス（IDaaS）。認証に利用するIDをクラウド上で管理し、SSO（シングルサインオン）や多要素認証を実現

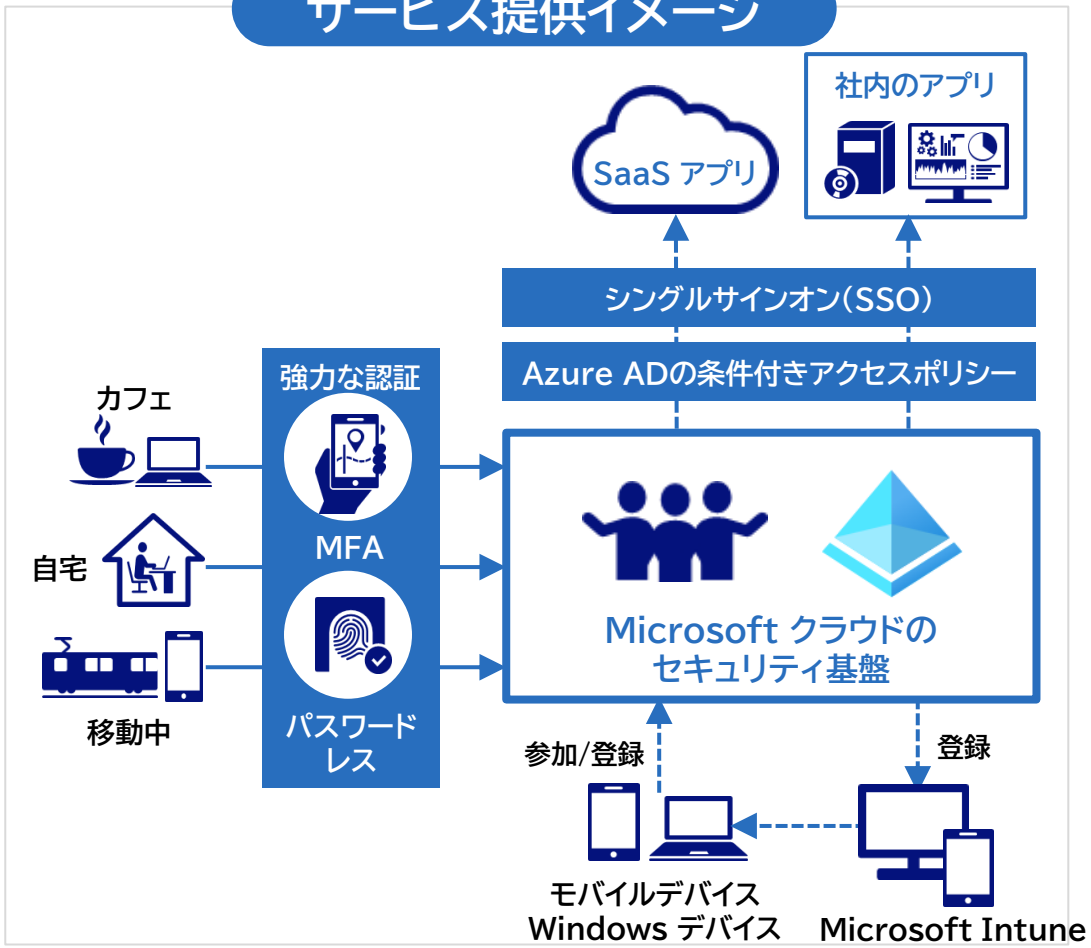


クラウド認証基盤のセキュリティ強化 - Azure AD

統合認証基盤

Microsoft社が提供するAzure ADを利用したIDaaSを構築
セキュアに業務システムを利用するために多要素認証やアクセス制御を実現

サービス提供イメージ



お客様の課題

・業務システムごとのパスワード管理によるパスワード漏洩リスクを防止したい
・増えるデバイスで、増加する情報漏洩リスクを防止したい

期待効果

・各業務システムのパスワード管理を集約で、パスワード漏洩のリスク低減
・不正端末からの情報漏洩リスク、組織外への情報流出リスクを低減

NECの特徴

・多くの導入構築実績を持つSI部隊が対応するため、高品質のデリバリーが可能
・NEC 365マネージドサービスとあわせてOffice365導入から一気通貫で提供可能

本日のまとめ

課題	対策ポイント	
クラウドサービスの頻繁な機能アップデート サービス仕様の理解不足による設定ミス	ワークロードの**設定**管理	サイバーハイジーン
クラウドシフトにより、データの格納場所・アクセス元が分散、 ガバナンスが困難に サービス種別を問わず、クラウド上のデータ保護は、ユーザ責任	**情報**管理	重要情報管理、 データガバナンス
境界防御の限界、ゼロトラストの考え方で全てのアクセスを検査 SaaS利用の加速に伴う、ID体系の統一化	**ID**管理	目的や方針の 明確化

関連製品ページ

- クラウド設定ミス防止
  - SaaSセキュリティ設定管理プロフェッショナルサービス（SSPM）
    https://jpn.nec.com/cybersecurity/professionalservice/assessment/sspm.html
  - Adaptive Shield（SSPM製品）
    https://jpn.nec.com/adaptive-shield/index.html
- AIP統合ラベルによる情報ラベリング・暗号化
  - ActSecureクラウドセキュアファイルサービス
    https://jpn.nec.com/actsecure/acts securefile.html
  - InfoCage FileShell
    https://jpn.nec.com/infocage/fileshell/
- ID管理
  - WebSAM SECUREMASTER
    https://jpn.nec.com/websam/securemaster/
  - Okta Identity Cloud
    https://jpn.nec.com/okta/index.html

ご参加いただき、誠にありがとうございました。

講演内容・ご紹介製品／ソリューション等に関する
ご質問・お問い合わせがございましたら、
以下までお願いいたします。

NEC　サイバーセキュリティ戦略統括部
セミナー事務局
cyber@seminar.jp.nec.com


Orchestrating a brighter world
NEC