製造業が抱えるビジネス課題を
解決する、クラウドサービスの活用方法とは

亀谷 怜史

Partner Development Manager
アマゾン ウェブ サービス ジャパン株式会社
パートナーアライアンス統括本部

最初に

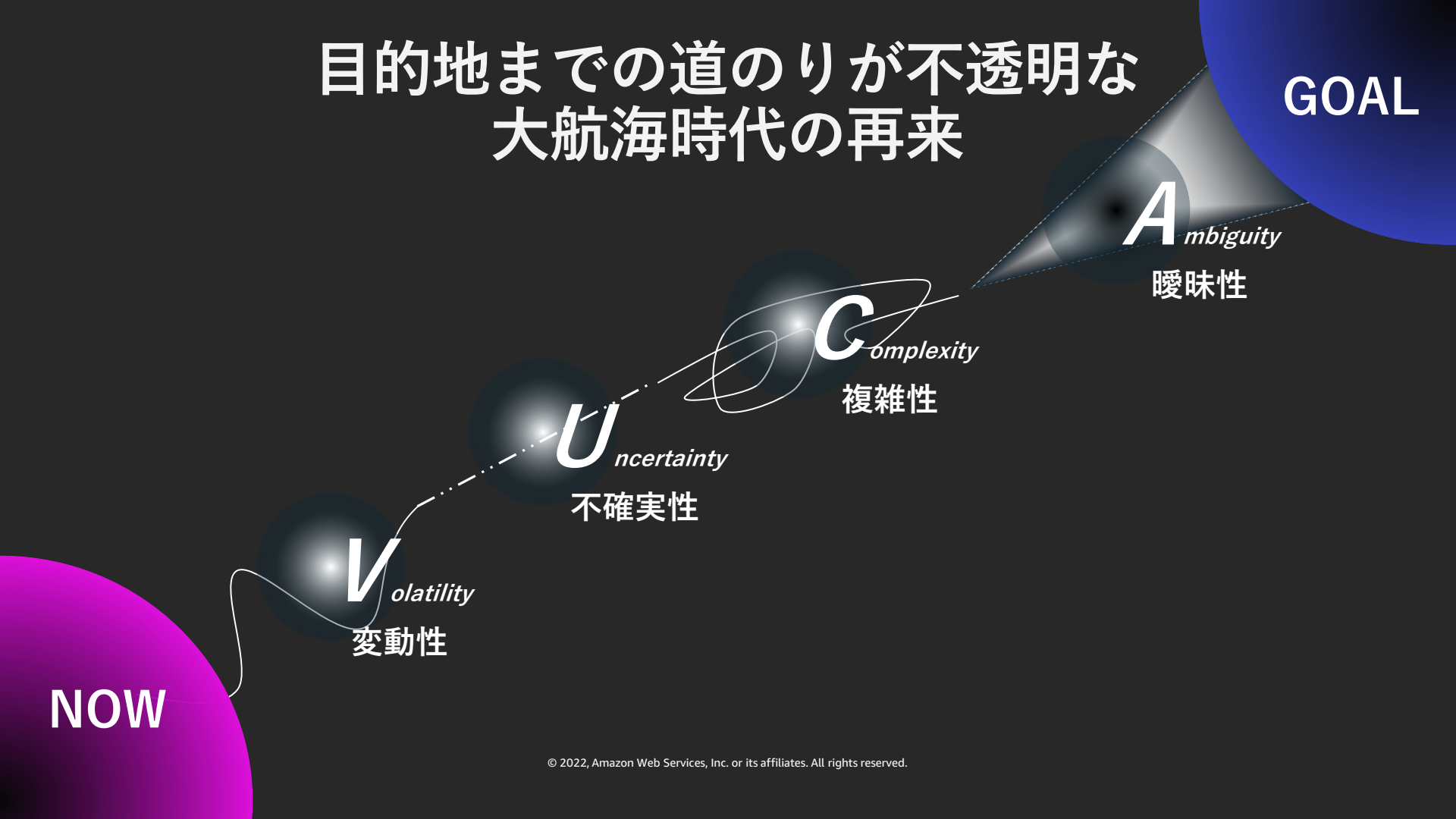
本日の資料のデータは2022/6/13の情報をもとに作成しております。最新情報、 AWSの各種サービスの詳細は弊社公式Webサイトよりご確認ください。

Agenda

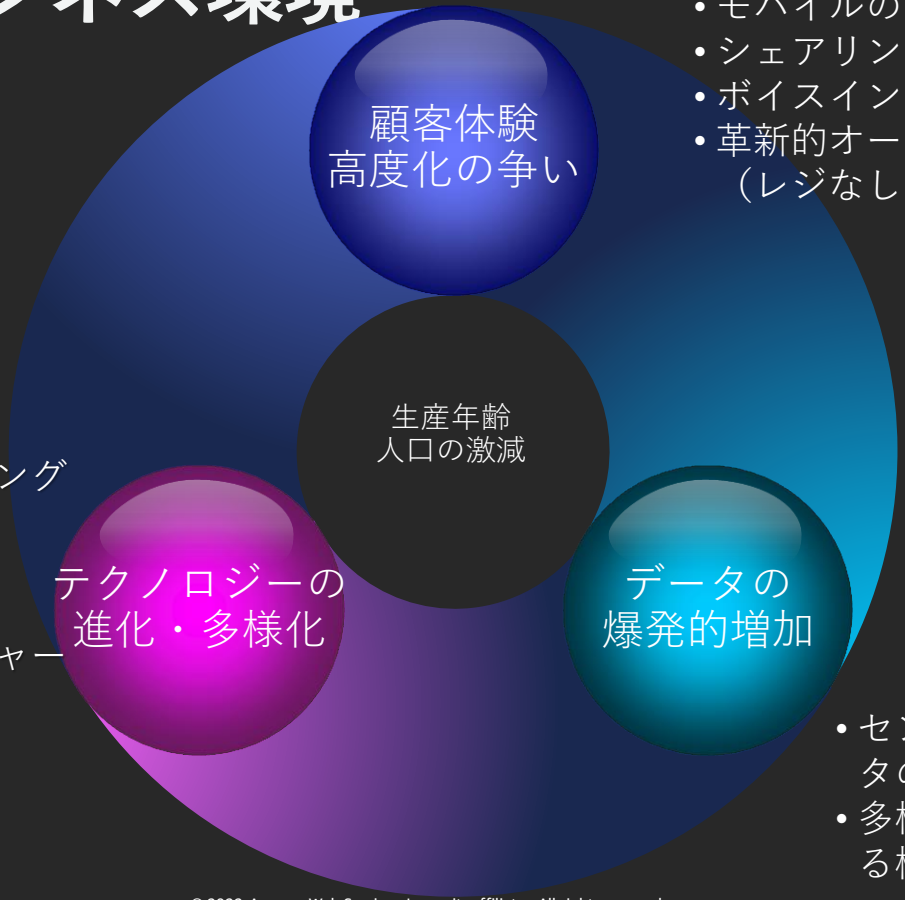
1. 製造業のお客様を取り巻く概況
2. 製造業におけるクラウド活用トレンド
3. 製造業でのクラウド活用事例
4. クラウド活用のステージへ

製造業のお客様を取り巻く概況

目的地までの道のりが不透明な大航海時代の再来



激変するビジネス環境



- モバイルのコモディティ化
- シェアリングエコノミーの定着
- ボイスインターフェースの到来
- 革新的オートメーションの兆し
  （レジなしコンビニ、自動運転車など）

- 機械学習／ディープラーニング
- 強化学習
- 仮想現実（VR）
- IOT
- サーバレス・アーキテクチャー
- ブロックチェーン
- 量子コンピュータ

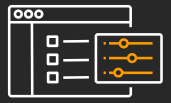
- センサーデータや非構造データの爆発的拡大
- 多様な分析により生み出される構造化データ

製造業におけるチャレンジ

新しい利益源泉の創出

OEE の改善と
生産の最適化

サプライチェーンの最適
化による在庫削減



データの開放と洞察の活
用

労働人口の不足、
スキルの空洞化

コンプライアンスの遵守と
知的財産の保護

サステナビリティ

コスト削減

＋COVID-19による
概況変化への対応

従業員の安全と健康

あらゆる領域を
デジタル化

未来の予測

オペレーションの
精度をより高める

製造業における
クラウド活用トレンド

製造業の業務領域では幅広くAWSを活用

マーケティング 販売

市場調査
製品企画
需要の創出
製品・サービスの販売
マーケティングや販売データ分析

エンジニアリング 設計

製品・サービスの設計開発
製品・サービスのテスト
生産の準備と基盤検証
サービス提供の準備と検証

生産

生産計画
需給ロジスティクスの管理運営
製品の製造・組立て
受注への対応

サプライチェーン

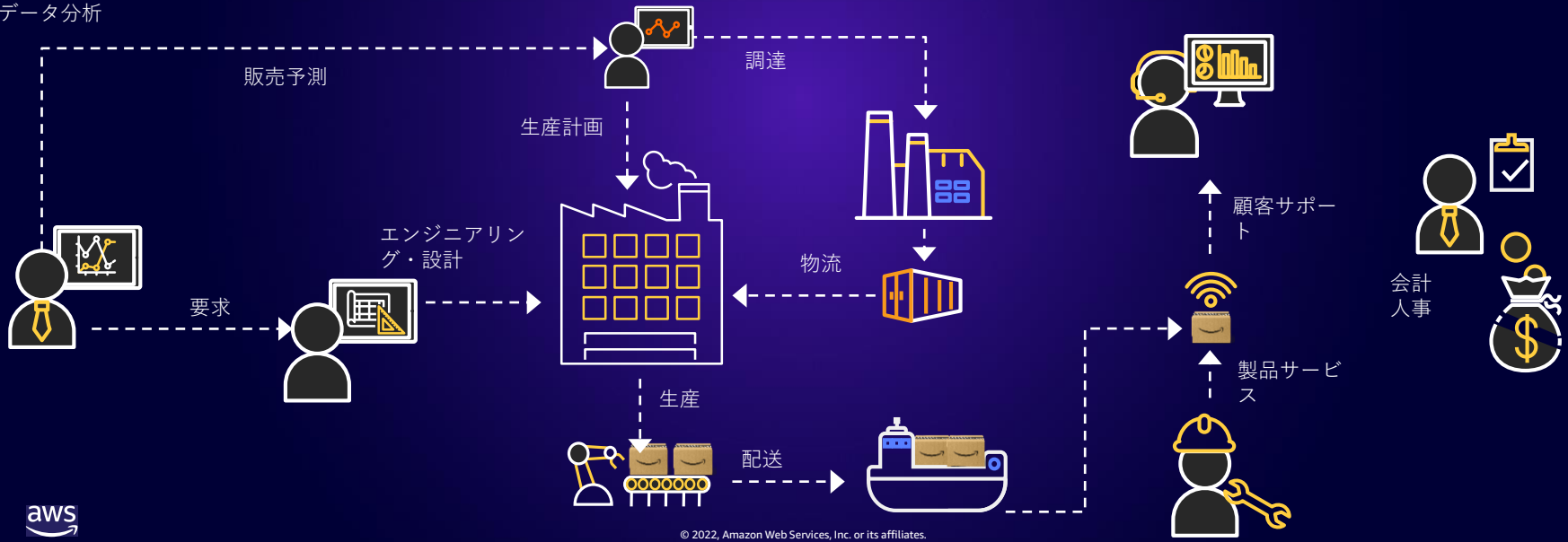
製品供給の基盤
製品サポートや製品資料の管理
在庫と配送の管理

サービスチェーン（製品サービス）

Smart Product
保守の技術情報管理・計画
サービス契約・保証
サービス品質の報告と分析
顧客サポート

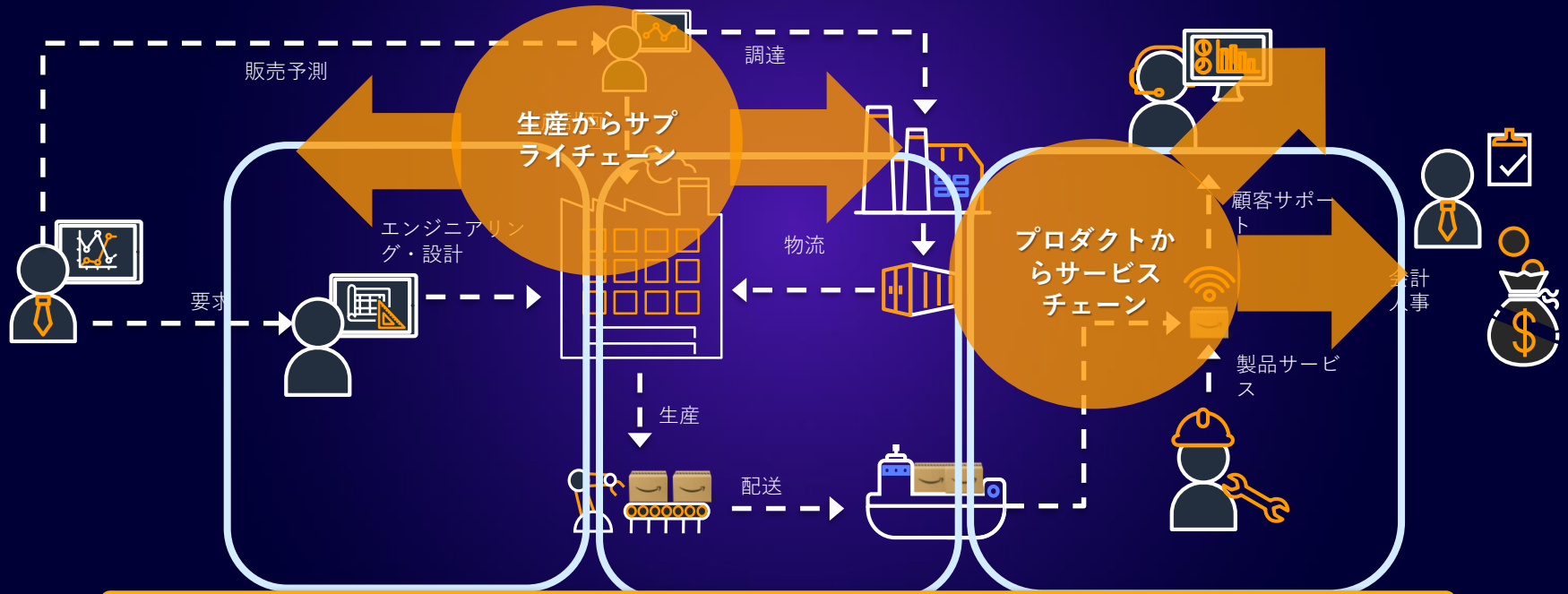
ビジネスオペレーション

総務サービス
ビジネス管理
人事サービス
ICTサービス



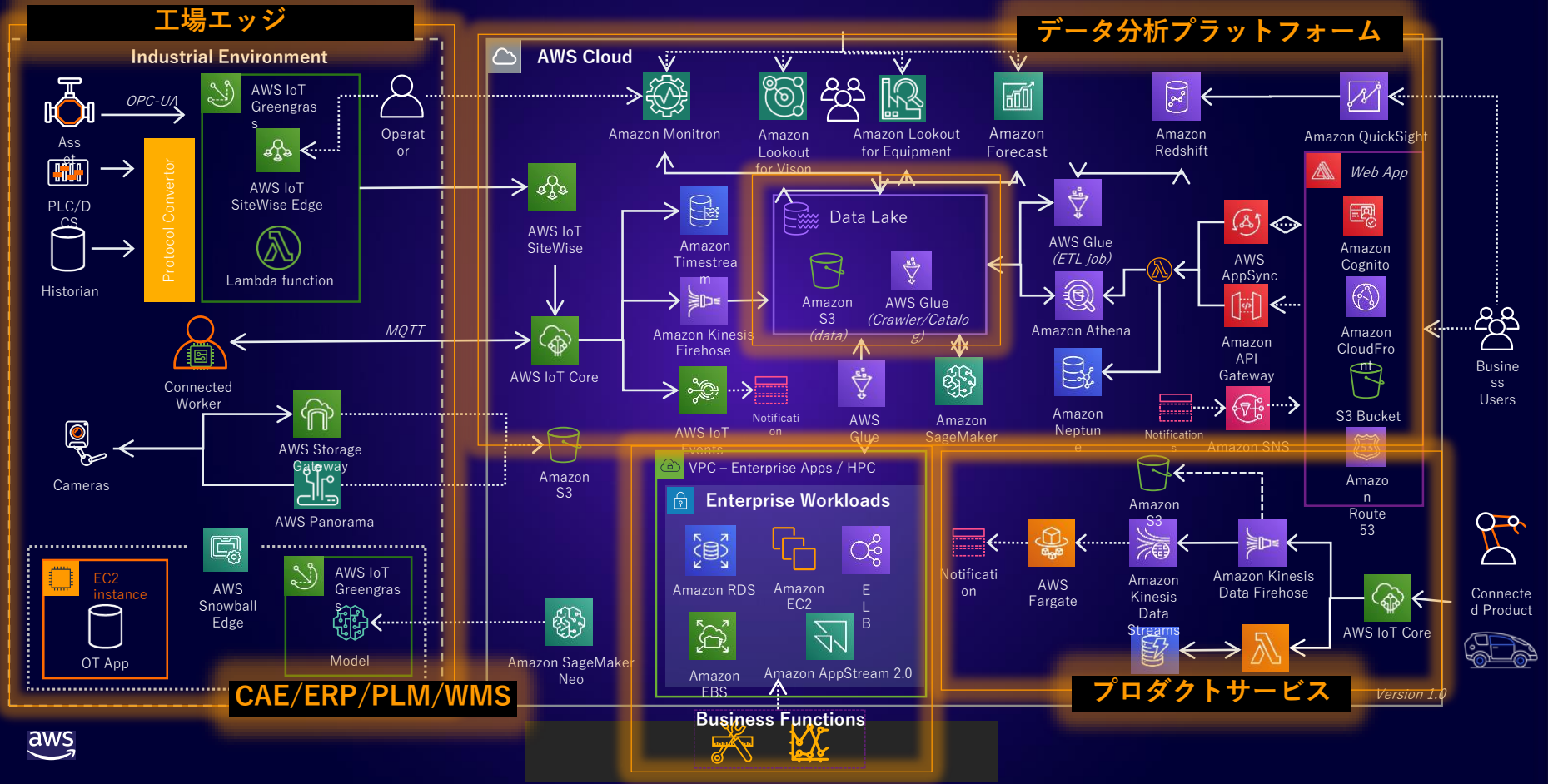
広がりはじめるデータの連携と多領域での活用

マーケティング・販売　エンジニアリング・設計　生産　サプライチェーン　サービスチェーン　ビジネスオペレーション



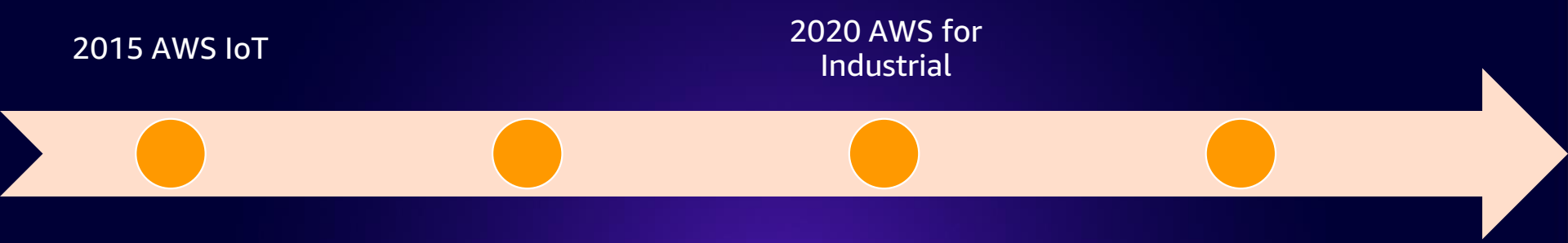
データを中心とした多領域化が進んでいる

製造業の業務領域をカバーする多様なAWSサービス



様々な製造業のお客様がAWSを活用

製造業のお客様におけるAWS活用の変遷



個別システムでの活用	適用システムの拡大	Innovation領域への展開
社内システムでの活用	基幹系を含む情報システム移行	事業横断データレイク
Product as a Service	IoT共通基盤	Smart Factory
CAE領域	研究開発共通基盤	ソリューション・アセットのサービス化
	CAD/CAM	業務領域の拡大

製造業でのクラウド活用事例

日立 Astemo 様

グローバルに稼働している PLM およびその周辺システムを AWS へ移行

AWS 移行によるコスト効果は絶大で、従来のデータセンター契約を解約することができました。
内製強化のための人件費や開発費を含めても、
オンプレミスシステムと比べた**総コストは約 5 分の 1 に低減**されています。

AWS の学習を含む 2 ヶ月間の準備期間を経て
移行を開始し、96 の仮想サーバーと
8 個のデータベース環境の上で稼働して
る 26 のアプリケーション群の移行を
わずか 4 ヶ月で完了しました。

「私はいつも “プロフェッショナルたれ” と言っています。事業部の要求どおりにベンダーへ依頼して、ただ契約書にハンコを押すだけでは意味がありません。また、せっかく作ったシステムも、使ってもらえなければ評価されません。**自ら考えて、オーナーシップを持って実行し、結果に責任を持つプロフェッショナルでなければ“価値がない”と言っています。**事業部門のニーズを受け止めて、効果的なシステムを作り、ちゃんと使ってもらえるようにアピールするためには、知識やスキルが欠かせません」（里山氏）

エーザイ 様

機密情報である“化合物情報”をクラウド環境に移行

“「ビッグデータを活用するには、オンプレミスにこだわり続けているわけにはいきません。AWSなら解析へのフレキシビリティさ とセキュリティ確保が確実に保て、情報漏洩のリスクがないことを経営トップに論理的に説明することで理解を得ました。”

- エーザイ株式会社 hhc データクリエーションセンター データサイエンスラボ
ディレクター瀬能 敬司 氏

AWS 導入事例

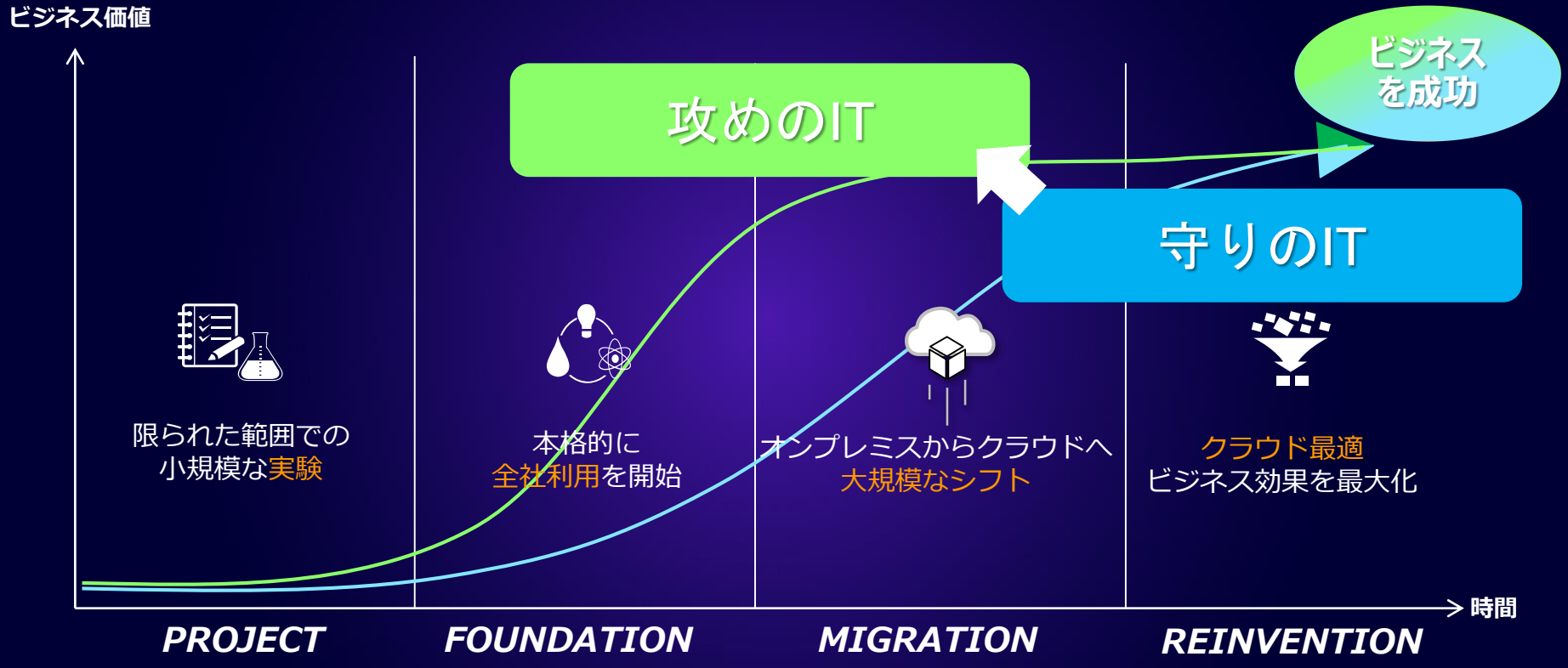
エーザイ株式会社

機密性の高い創薬の研究開発に
ハイパフォーマンスコンピューティング（HPC）を活用

https://aws.amazon.com/jp/solutions/case-studies/eisai/

クラウド活用のステージへ

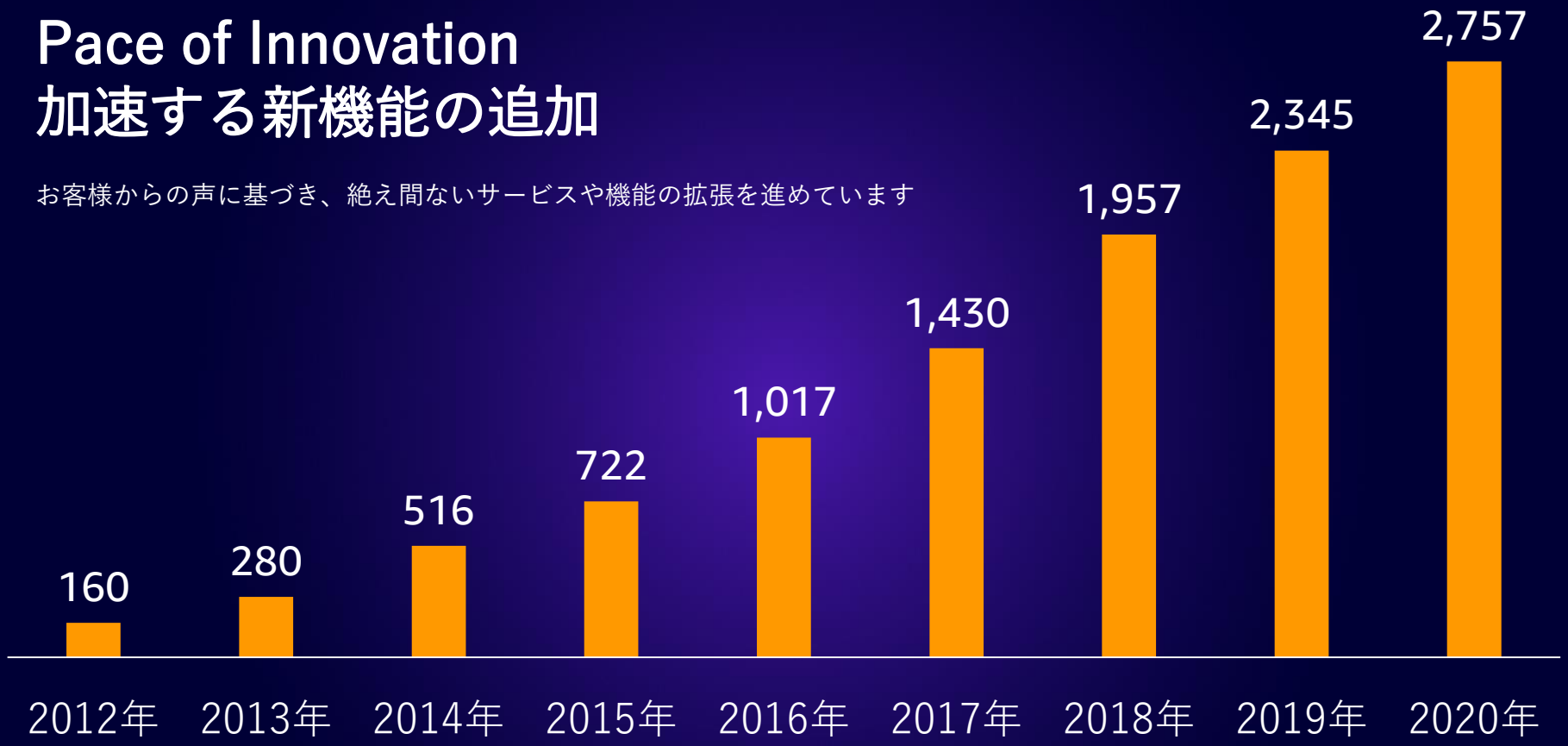
クラウドジャーニーにおける4つのステージ



200 を超えるサービスであらゆるワークロードをサポート

Pace of Innovation
加速する新機能の追加

お客様からの声に基づき、絶え間ないサービスや機能の拡張を進めています



THE Paris...
CLIMATE 10 years
PLEDGE Early

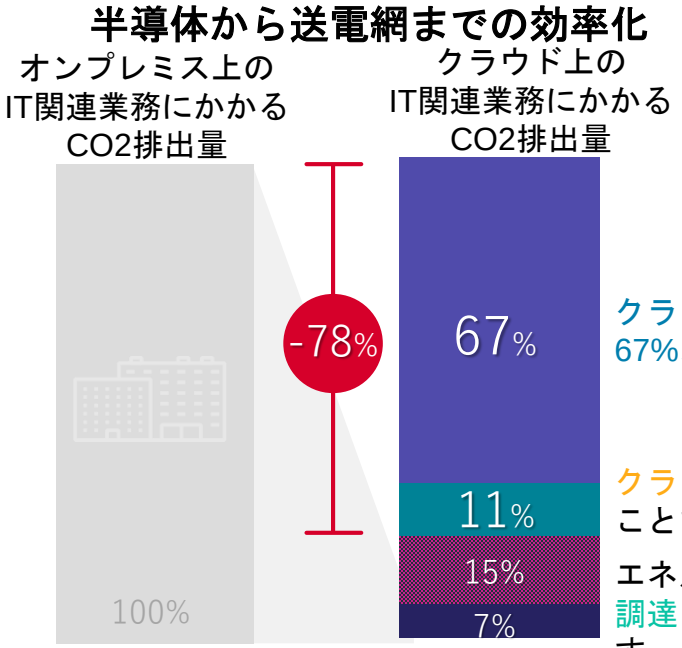
2025年までに再生可能エネルギーの
電力比率を100% に

2030年までに
50% の配送で炭素ゼロ化

2040年までに
炭素ゼロ化を100% 達成

調査レポートの主なポイント

アジア太平洋地域（APAC）において企業のワークロード（IT関連業務）をオンプレミス（自社所有）の**データセンターからクラウドに移行すると、エネルギー消費量とそれに付随する二酸化炭素（CO2）排出量を78%も削減できる可能性があります。**



クラウドサーバーを使用するとサーバーのエネルギー効率が5倍以上になるため、67%以上という最大のエネルギー削減につながります。

クラウドデータセンター施設では、より効率的に電力や冷却システムを使用することで、さらに11%の削減が可能となり、エネルギー削減率は78%に近づきます。

エネルギー需要に応じてクラウドサービスプロバイダーが再生可能エネルギーを調達した場合、クラウド上のIT関連業務にかかるCO2排出量をさらに削減 できます。

451 Research
S&P Global
Market Intelligence

クラウド活用が進む理由

俊敏性
数百数千のサーバーを
数分で展開、いつでも終了

コスト削減
初期投資不要な
従量課金

弾力性
需要に応じてスケール
キャパシティー予測が不要

幅広い機能
お客様の声による
新サービス提供と機能改善

グローバル規模の展開
わずか数分で
世界中にデプロイ

高いセキュリティ
セキュリティはAWSの
最優先事項

多数の国際的認証をもつ秘匿性高いデータセンター

秘匿性が高いデータセンターの詳細は非公開

- AWSのデータセンターは、さまざまなお客様の重要資産を保護するため、詳細な設置場所等は一切非公開、AWS社員にも公開されていない
- 物理セキュリティは、境界防御レイヤ(防御壁、監視カメラ等)、インフラストラクチャレイヤ(電力ジェネレータ、空調設備、消火設備等)、データレイヤ(アクセス制限、特権管理、脅威検出機器等)といったレイヤ毎に必要とされる物理セキュリティを実装

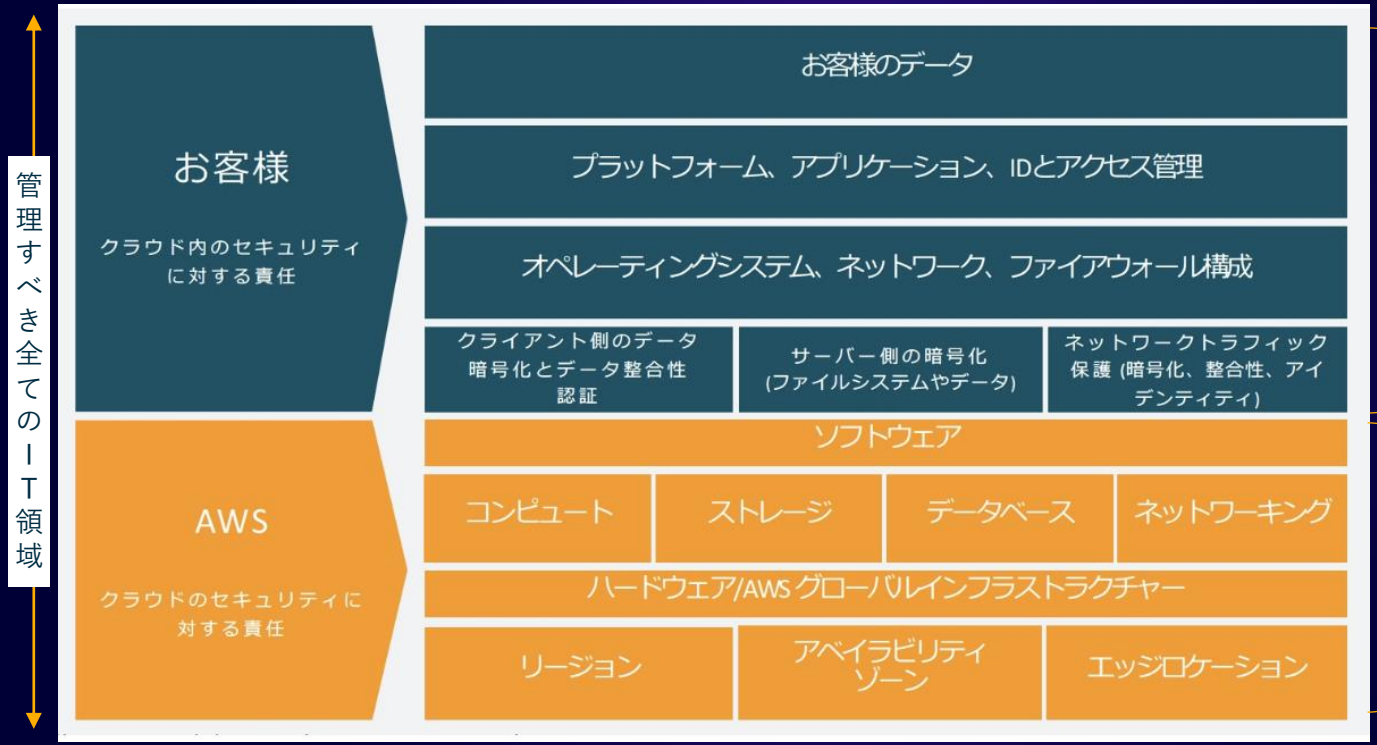
非公開であるがゆえ
様々な国際的認証や評価を受けている

- データセンターの物理アクセスセキュリティのコンプライアンス準拠状況は独立した第三者（外部監査人）によって定期的に実施
- お客様がAWSのデータセンター監査を実施することなく、データセンター監査を実施したのと同じ効果を得ることが可能
- 監査結果や準拠状況は、AWSのお客様であれば無償で入手可能*

* 所定の手続きがあります

「責任共有モデル」の採用で責任の曖昧さを排除

AWSの責任共有モデル(概念図)



AWS クラウドセキュリティ

AWSはクラウドコンピューティングの先駆者として、セキュリティを最優先事項としてお客様のイノベーションに迅速に対応可能な
クラウドインフラストラクチャーを創造してきました。セキュリティ機能の実装や厳格なコンプライアンス要件へ対応で
お客様は最も柔軟かつセキュアなクラウドコンピューティング環境を実現可能です

AWS コンプライアンスプログラム

セキュリティとコンプライアインスのためにAWSに導入されている堅牢な
管理は、独立した監査人によって評価されています。これにより、AWSは
お客様のコンプライアンス要件への準拠をサポートします

コンプライアンスプログラムの例

AWS コンプライアンスプログラム
https://aws.amazon.com/jp/compliance/programs/

クラウドセキュリティのためのサービス

AWSの提供するセキュリティ、ID、コンプライアンスのための
包括的なサービスと機能を活用いただくことでセキュリティと
コンプライアンスの要件を満たす能力を向上させることができます

- アイデンティティ & アクセス管理
- 脅威の検出と継続的なモニタリング
- インフラストラクチャとデータの保護
- インシデントへの対応
- コンプライアンス


Thank you!

セキュリティを知ることで踏み出す、クラウドジャーニーの第一歩

2022年6月17日

NEC サイバーセキュリティ事業統括部
マネージャー　石野 直人

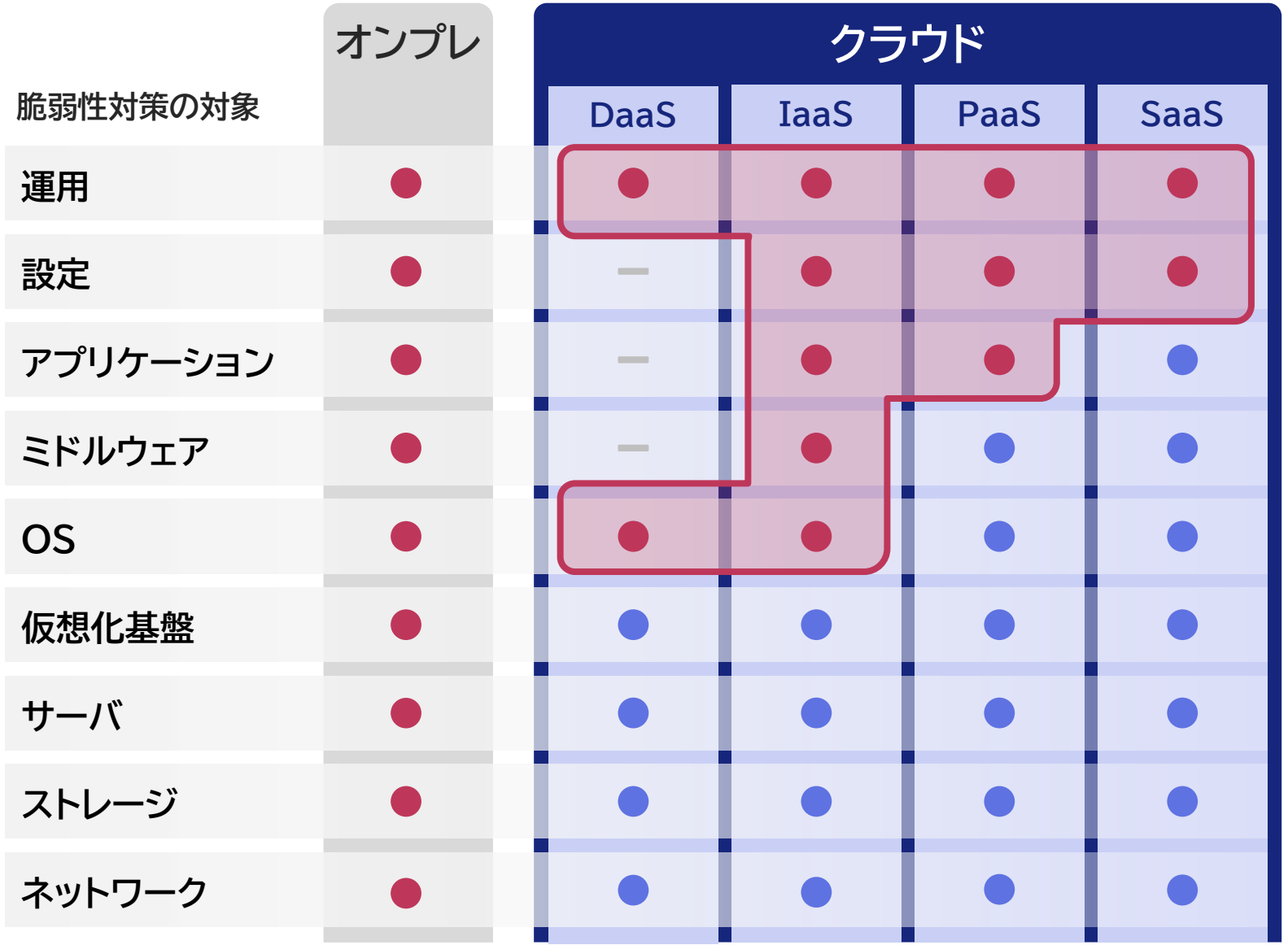
本日お伝えしたいこと

クラウド「責任共有モデル」に沿って
セキュリティ対策を実施する

クラウド導入に向けたリスク可視化と
クラウド活用ルールや体制の整備

脆弱性やクラウド設定ミスに備える

クラウドにおける責任範囲(責任共有モデル)



DaaS:Desktop as a Service
IaaS: Infrastructure as a Service
PaaS: Platform as a Service
SaaS: Software as a Service

脆弱性対策の責任範囲

●・・・契約者(脆弱性対策が必要)

●・・・クラウド事業者

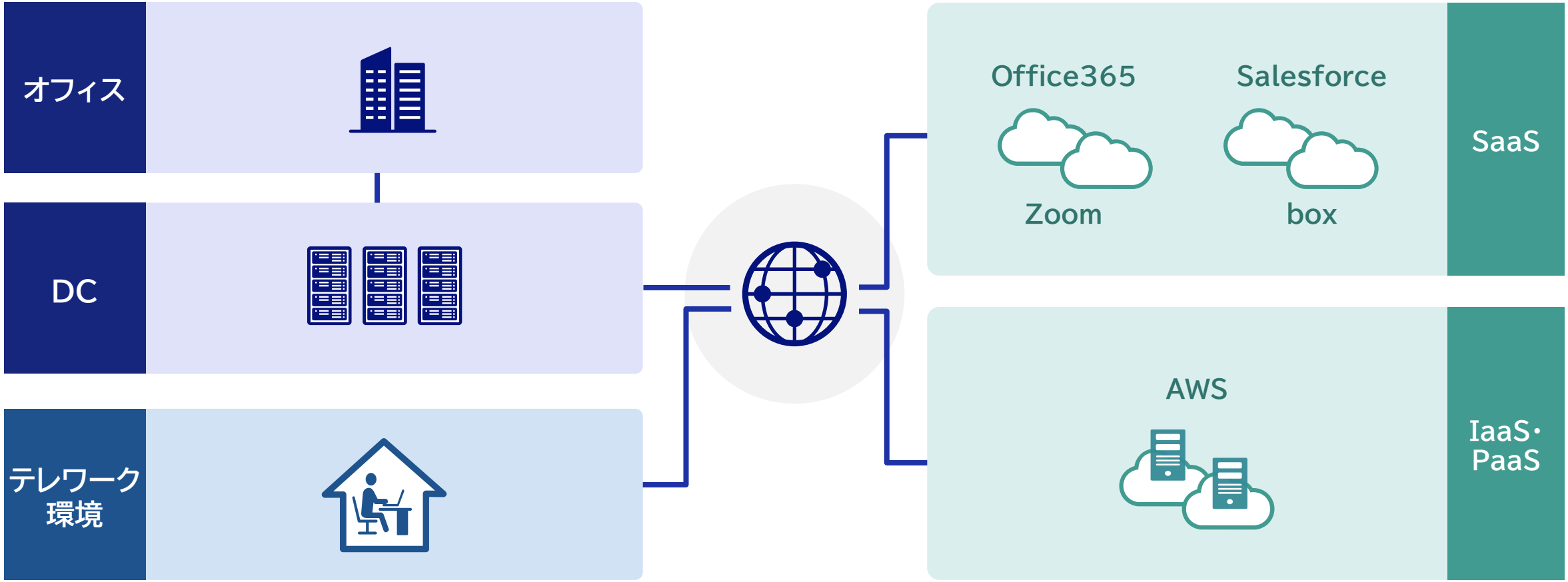
オンプレではNW～運用まで
全部契約者の責任

クラウドにすれば
契約者責任の範囲は狭まる
ただし、契約者責任の所は
自分達で対策が必要

クラウド導入に向けて実施するべき事項

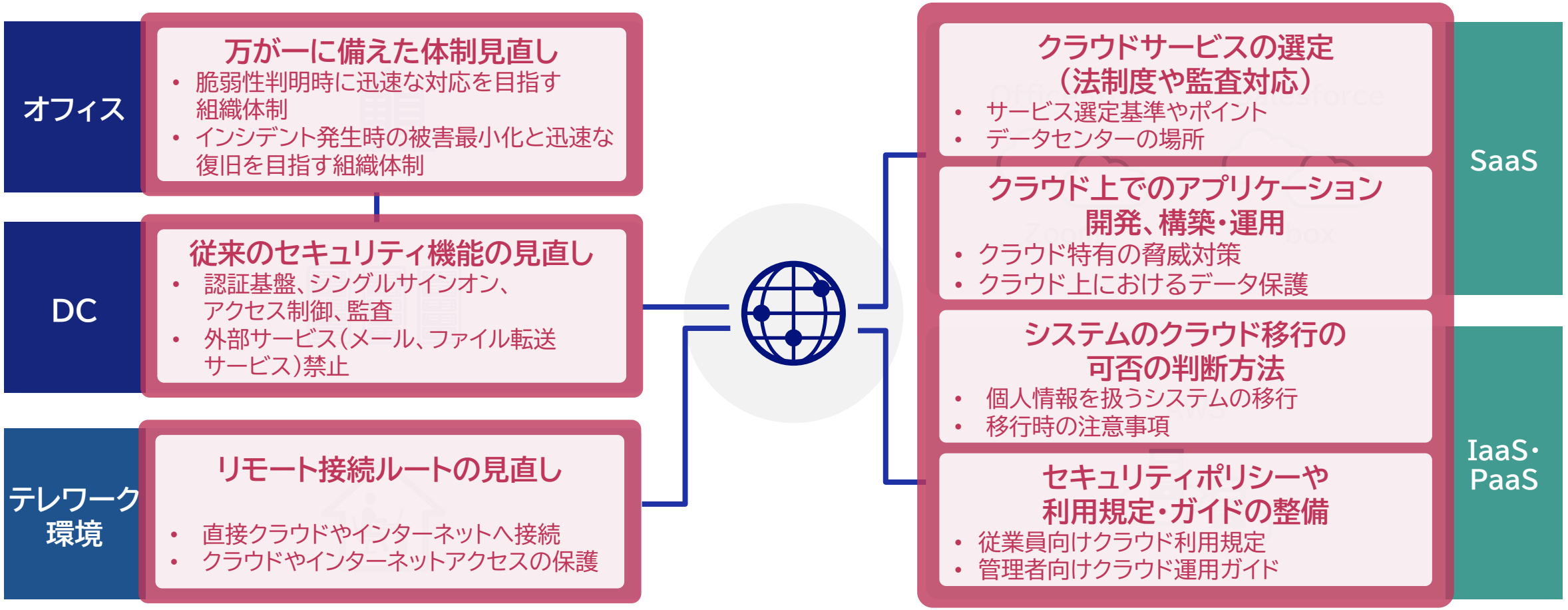
クラウドシフトにあたっての課題

クラウド導入時にセキュリティ観点で考慮すべき事項



クラウドシフトにあたっての課題

クラウド導入時にセキュリティ観点で考慮すべき事項



上流からのアプローチ(セキュリティ対応方針整理)

サイバー攻撃、セキュリティガイドライン、個人情報・プライバシー保護を整理

サイバー攻撃対応

クラウドの重大セキュリティ脅威
11の悪質な脅威

1. データ侵害
2. 設定ミスと不適切な変更管理
3. クラウドセキュリティアーキテクチャと戦略の欠如
4. ID・資格情報・アクセス・鍵の不十分な管理
5. アカウントハイジャック
6. 内部者の脅威
7. 安全でないインターフェースとAPI
8. 弱い管理プレーン
9. メタストラクチャとアプリストラクチャの障害
10. クラウド利用の可視性の限界
11. クラウドサービスの悪用・乱用・不正利用

出典:一般社団法人日本クラウドセキュリティアライアンス(CSAジャパン)
https://www.cloudsecurityalliance.jp/site/?p=20247

セキュリティガイドライン

＜政府機関向け＞
- 内閣官房:デジタル・ガバメント推進標準ガイドライン
- NISC 政府機関統一基準
- 政府情報システムにおけるクラウドサービスの利用に係る基本方針(クラウド・バイ・デフォルト)

＜重要インフラ向け＞
(情報通信,金融,航空,空港,鉄道,電力,ガス,政府・行政サービス,医療,水道,物流,化学,クレジット及び石油)
- 各分野別セキュリティガイドライン

＜民間企業向け＞
- 経産省 サイバーセキュリティ経営ガイドライン、サイバー・フィジカル・セキュリティ対策フレームワーク
- NIST Cyber Security Framework、SP800シリーズ(171など)

＜クラウドサービス事業者向け＞
- 総務省 クラウドサービス提供における情報セキュリティ対策ガイドライン
- ISO/IEC 27017(クラウドサービスセキュリティ)」

個人情報・プライバシー保護

- 個人情報保護法
- 個人情報保護法ガイドライン
- EU:GDPR
(一般データ保護規則)

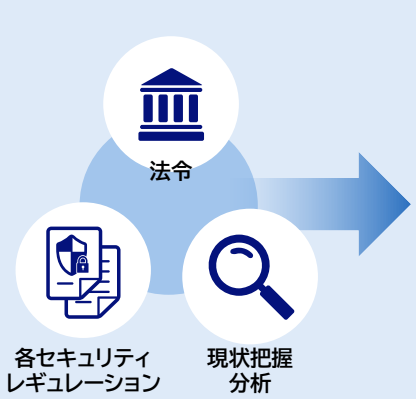
クラウド導入における3つの対策ポイント（マネジメント・コンサル領域）

① 現状分析・リスク可視化し対策ポイントを整理する

- 組織・社内制度・システムのセキュリティリスク／対策状況の現状把握
- 業界のセキュリティレギュレーションに準拠したセキュリティ対策とロードマップ策定

サイバー攻撃による被害の最小化及び事業継続

サービス：
セキュリティリスクアセスメントサービス



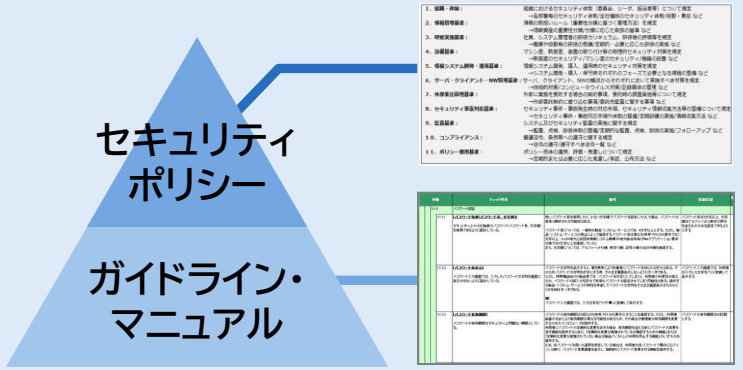
アセスメント結果、ロードマップ

② セキュリティ対策ルールやクラウド利用ルールを整備する

- サイバーセキュリティ対策に向けた適切なポリシー策定
- セキュリティの企業統治強化、対外的な説明責任の確立

サイバーセキュリティ対策整備をルール面から強化

サービス：
セキュリティポリシー策定支援サービス

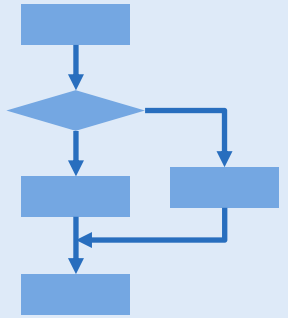


③ 万が一に備えて運用プロセスや体制を整備する

- 現状のインシデント対応状況確認
- あるべき姿として、プロセスや実施手順、体制の整備

セキュリティインシデント発生時の被害拡大防止と迅速な復旧

サービス：
セキュリティインシデント対応
体制・プロセス整備支援サービス



インシデント対応
プロセス整備

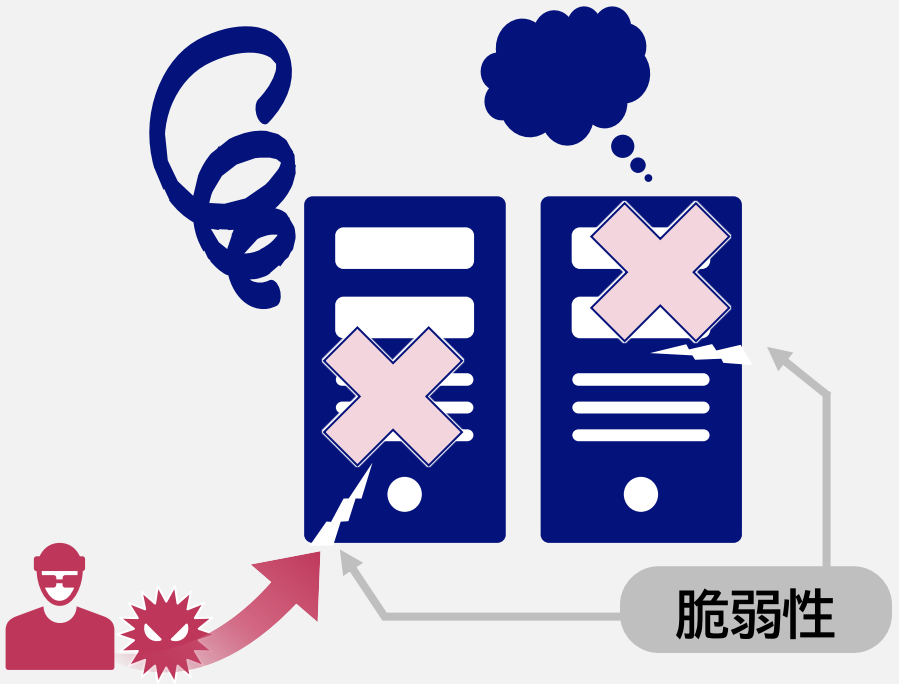
インシデント対応
体制整備

次々に発生する脆弱性に備える

脆弱性とは？

ソフトウェアの不具合や設計上のミスが原因となって発生した
情報セキュリティ上の「弱点」や「欠陥」

脆弱性対策を放置すると・・・



- 不正侵入
- 情報漏洩
- データ改ざん
- 乗っ取り
- システム破壊

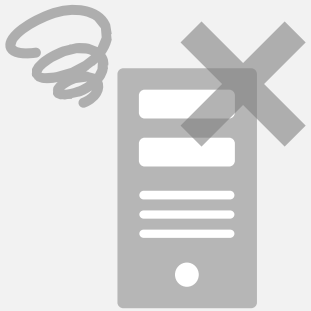
正常な状態を維持しつづける

脆弱性は「なくならない」
前提での対応

脆弱性対策①：サーバやPCの脆弱性に備える

OSやミドルウェアの重大な脆弱性

- 2022/4 Apache Struts2
  リモートよりコードの実行可能な脆弱性
- 2022/3 Spring4Shell
  「Spring Framework」のコアモジュールに
  リモートよりコードの実行可能な脆弱性
- 2021/12 Apache Log4j
  リモートよりコードの実行可能な脆弱性
- 2021/10 Apache HTTP Server
  攻撃者が許可なくデータの保管場所を読み出したり、
  リモートよりコードの実行可能な脆弱性
- 2020/8 Microsoft Netlogon（Zerologon）
  ドメイン管理者権限を取得される可能性がある脆弱性



重大な被害を及ぼすような脆弱性が
次々と発生

Webサービスにおける情報漏えい事案

- 2022/3 食品会社 オンラインショップ
  サイト利用者164万人の情報流出の疑い
  ネットワーク機器の脆弱性を悪用され、侵入された可能性が高い
- 2022/1 カード決済代行
  Webアプリケーションの脆弱性が原因で、
  最大約46万人分のクレジットカード情報が漏えい
- 2021/11 独立行政法人 学習管理システム
  社外サイトの 既知の脆弱性が原因で、
  約1.4万人の個人情報が漏えいした可能性が高い
- 2021/11 カジュアルウェア オンラインショップ
  脆弱性を悪用した不正アクセスで、
  会員24万7600人分の個人情報が流出

被害に遭った組織はいずれも、さらなる
セキュリティ対策強化や再発防止を表明

脆弱性対策①：サーバやPCの脆弱性に備える3つのポイント

① 構成情報の可視化とパッチ管理（サイバーハイジーン（衛生管理））

- 業務端末やサーバなどIT資産の構成の可視化
- 脆弱性パッチ適用を的確に実施

数百、数千台あっても迅速に該当サーバ・PCを特定し、リスク管理

商材例：
ActSecureセキュリティリスク管理サービス

② OSやミドルウェアの脆弱性に備えるために、IPSを導入する

- セキュリティパッチを早急に適用することが難しい場合に、暫定的にセキュリティ担保するための仕組み
- 脆弱性の自動検出、保護ルールの自動適用

重大な脆弱性が発生しても、慌てず安心して対処

商材例：
トレンドマイクロ DeepSecurity、CloudOne WS※

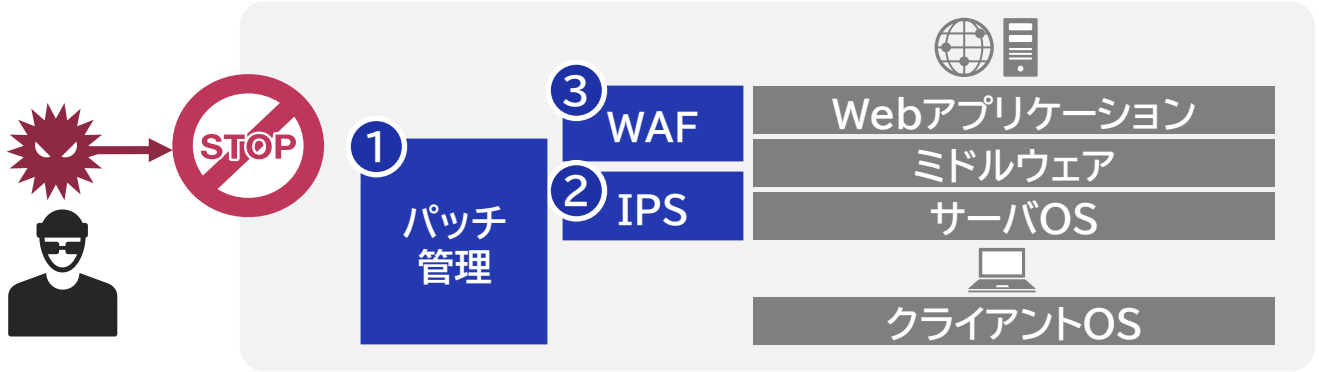
※ Cloud One - Workload Security

③ Webアプリケーションの脆弱性に備えるために、WAFを導入する

- SQLインジェクションなどのアプリケーションの脆弱性を突いた攻撃のみならず、ミドルウェアの脆弱性に対する不正通信を検知・遮断

重大な脆弱性が発生しても、慌てず安心して対処

商材例：
InfoCage SiteShell



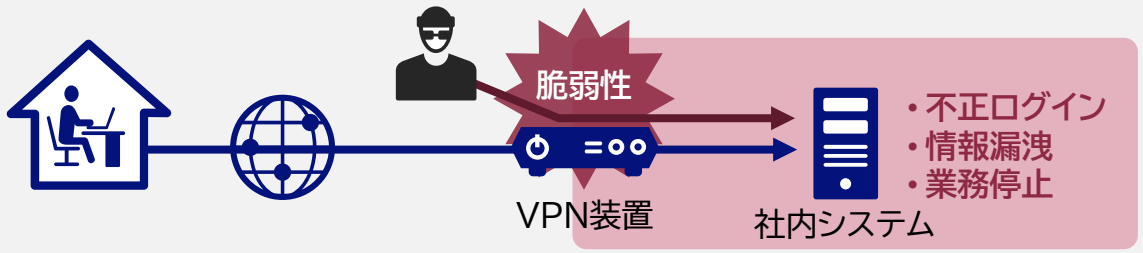
脆弱性発生後はスピード勝負！
時間をかけずにリスク低減！

脆弱性対策②:リモートアクセス環境からの不正侵入に備える

既知の脆弱性を修正していないVPN装置が、サイバー攻撃の標的となる

VPN脆弱性の被害事例

- 2022/3　**自動車部品メーカー 取引先工場の生産停止**
  リモート接続機器の脆弱性が原因でファイルサーバが不正アクセスを受け、取引先や外部ネットワークを遮断
- 2021/9　**Fortinet社製のVPN認証情報が流出**
  日本含め世界で8.7万台分
  （2年前の脆弱性が修正されてない機器からの流出）
- 2020/11　**600超の組織にサイバー攻撃**
  テレワークや遠隔操作に使われる情報機器の欠陥が悪用され、少なくとも607の国内企業や行政機関などがサイバー攻撃を受けていた
- 2020/10　**ゲーム会社にてランサムウェア被害**
  海外の旧型VPN装置への攻撃を足掛かりに社内へ不正侵入された



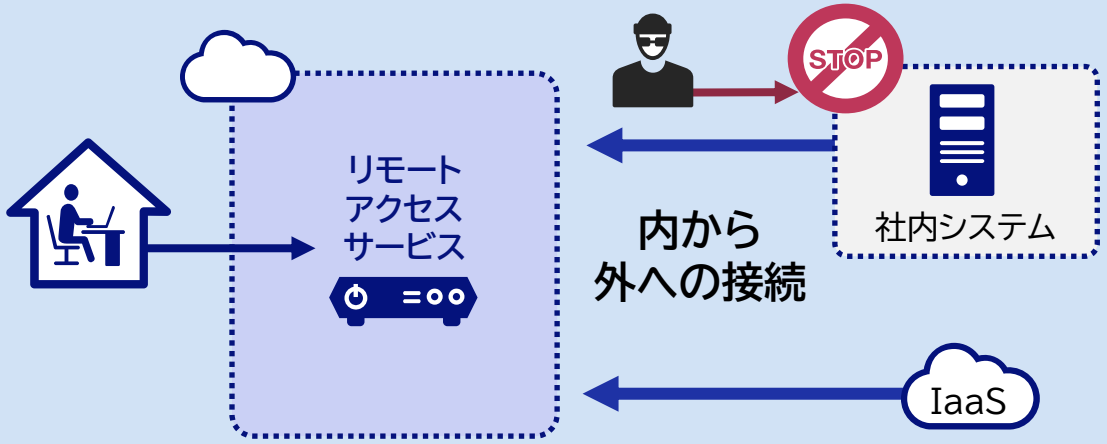
ランサムウェアの被害と感染経路

感染経路	VPN機器、リモートデスクトップからの侵入 **74%**
被害件数	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**%

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)

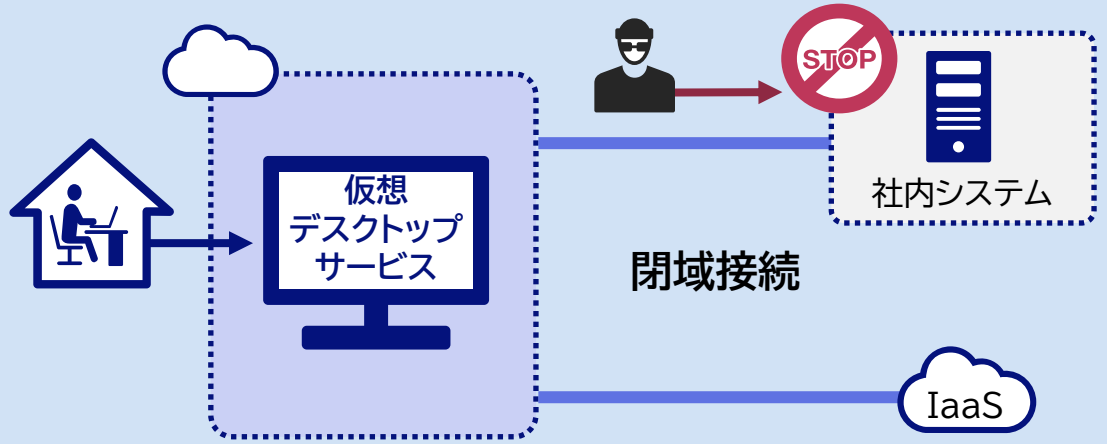
脆弱性対策②:2つの”脱VPN”

クラウド型リモートアクセスサービス（SDP）



サービス:Zscaler Private Access

クラウド型仮想デスクトップサービス



サービス:クラウド型仮想デスクトップサービス

安全性
社内システムへ
不正侵入できない

導入や運用負担の軽減
ユーザが増加しても、柔軟にユーザ拡張
脆弱性対応から解放

快適性
社内ネットワークを経由せずに
直接クラウドへアクセス

脆弱性対策③：定期的なリスク評価

ビジネス環境の変化に応じ高度化するサイバー攻撃への耐性の把握及び適正化するために、定期的な診断とリスク評価が有効

脆弱性診断

健康診断

義務付けられた年に一回の定期健診

- ツールやガイドライン等に従って**定型的なテストケースに基づいた作業**、検査内容について業者による差異は少ない
- 検査結果のわかりやすさについては業者により違いがある

脆弱性やセキュリティ機能の不足を
「網羅的に洗い出す」ことを目的とし、
既知の脆弱性や設定の不備を検知する

ペネトレーションテスト

専門医による診断

健康診断だけではわからない病気の早期発見が目的

- **実施者のスキルや熟練度によって、テストの成果が異なる**
- セカンド・オピニオンとして別の業者に実施させることで未発見の問題点が検知されることもある

「脆弱性を悪用する」ことで
攻撃者がその目的を達成する（侵入する）
ことが可能であるかを検証する

脆弱性対策③:リスクハンティングサービス

ビジネス継続に関わるリスクを包括的に評価し対策を提示することで、リスク低減を支援

ペネトレーションテスト:攻撃者視点で侵入(システム被害)の可否を確認

機密情報の窃取　サービス停止　管理者権限奪取　…

アプリケーション検査

システム上で動くWebアプリや、個別アプリの脆弱性検査

プラットフォーム検査

システムを構成する製品/OSSの既知の脆弱性検査

ネットワーク検査

システムに繋がるネットワークの脆弱性検査

セキュリティスペシャリストチーム

- 専門資格※を保有
- 国内外コンテストで表彰

脆弱性検査等の各種ツールを活用
企画設計フェーズから仕様書や設計書等の各種ドキュメント内容を確認

ハードウェアも含めたシステム全体からみたセキュリティリスクや
人権・プライバシーへの配慮不足等、ビジネス継続に関わるリスクを包括的に評価し対策提示

*CISSP, GIAC, 情報処理安全確保支援士等

クラウド設定ミスに備える

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

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）

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

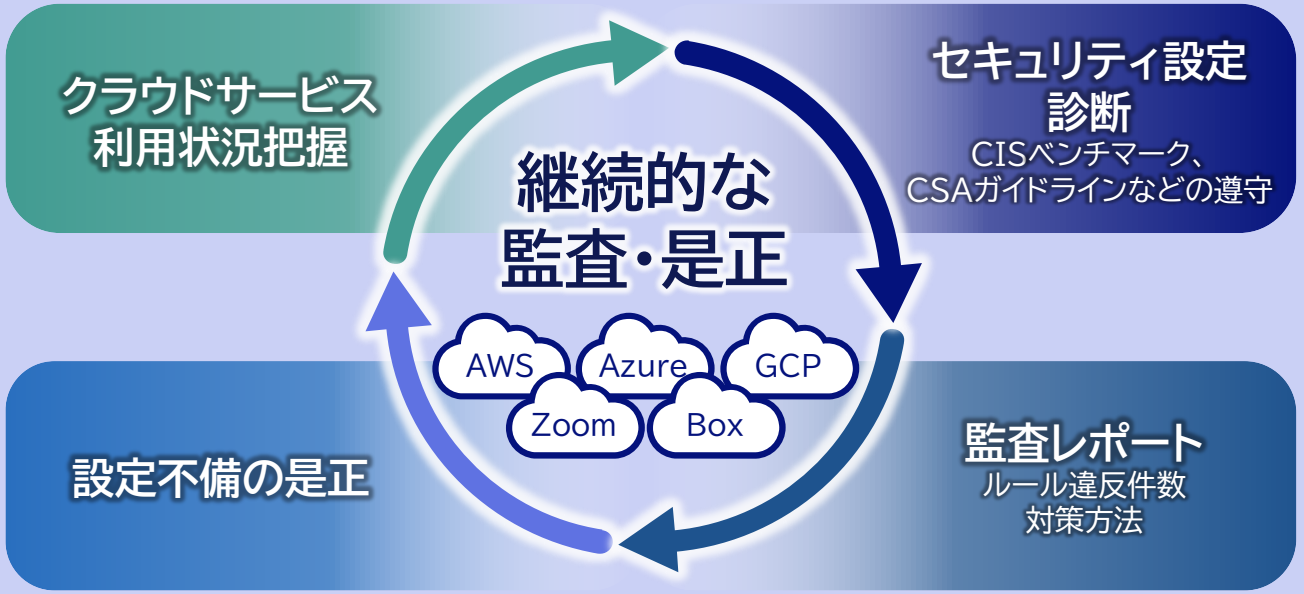
ワークロード管理の複雑性増大
・複数のIaaSをマルチクラウドとして活用
・PaaS、コンテナ、サーバーレス活用

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

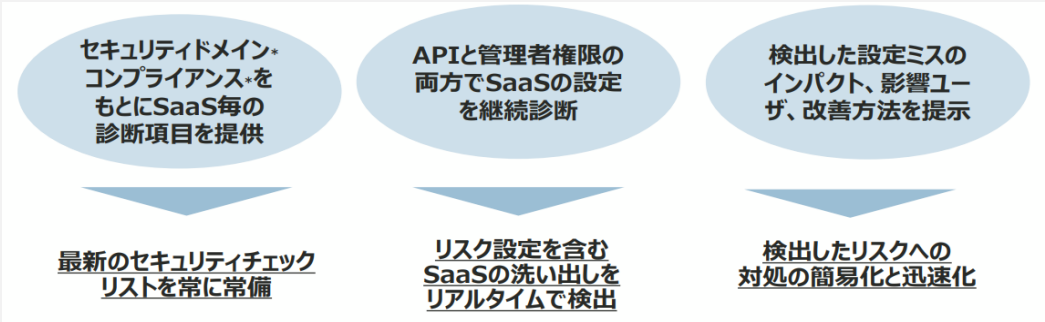
各クラウドプラットフォームのAPI経由で → セキュリティ設定状況を自動的に可視化 → 必要に応じて自動対処やレポートを作成

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

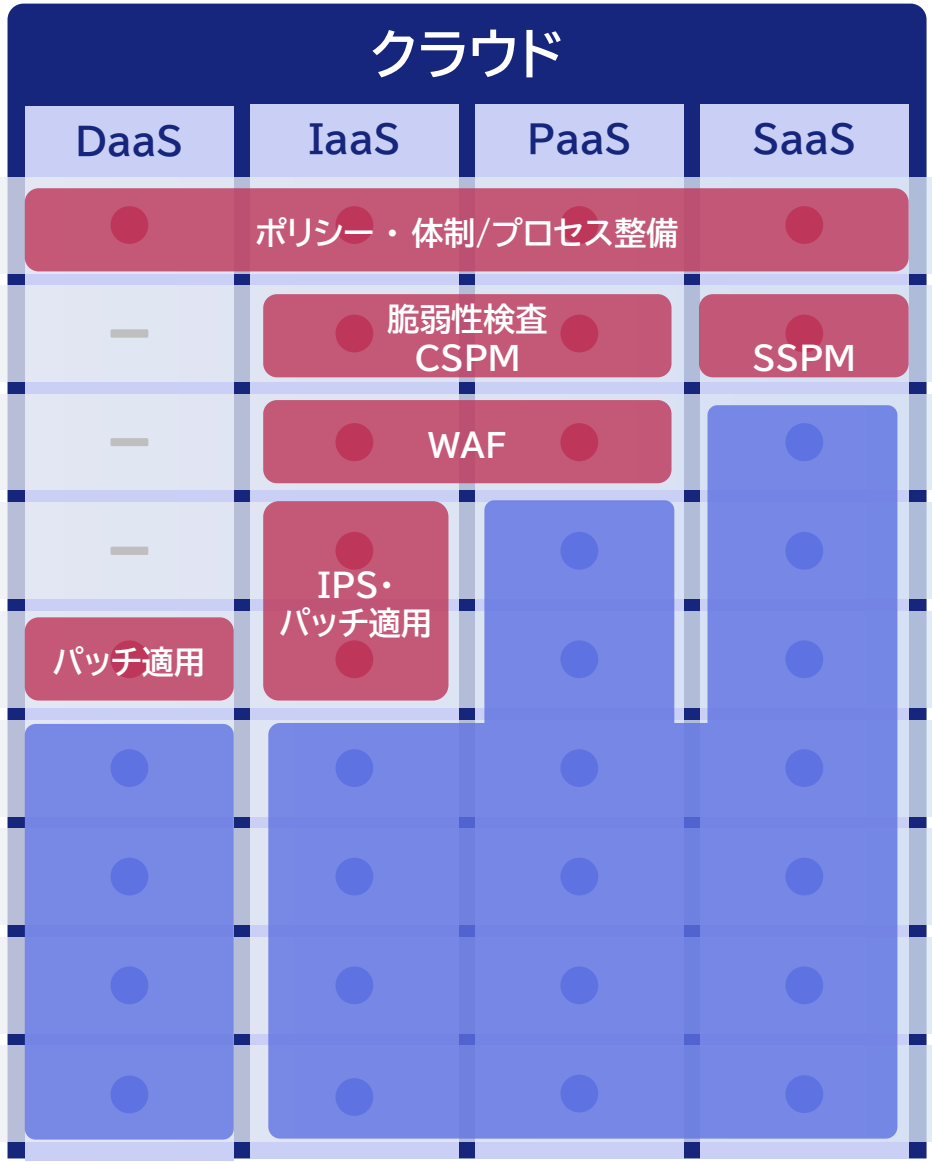
監査ポリシー例

Prisma Cloud　利用の場合

ポリシー	チェック内容
コンフィグ	● IAMユーザーに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

まとめ

クラウドにおける脆弱性対策の責任範囲と対策手段



脆弱性対策の対象	主な脆弱性対策のための製品・サービス
運用	セキュリティポリシー策定支援サービス セキュリティインシデント対応 体制・プロセス整備支援サービス
設定	リスクハンティングサービス CSPM(Prisma Cloud)、SSPM(Adaptive Shield)
アプリケーション	Web脆弱性(WAF:Site Shell)
ミドルウェア	サーバー脆弱性(IPS:Deep Security、CloudOne WS)
OS	サーバー脆弱性(IPS:Deep Security) セキュリティリスク管理サービス(SRMサービス)
仮想化基盤	
サーバ	
ストレージ	
ネットワーク	SDP(Zscaler Private Access) VDI(クラウド型仮想デスクトップサービス)

脆弱性対策の責任範囲
- ●…契約者(脆弱性対策が必要)
- ●…クラウド事業者

本日のまとめ

クラウド「責任共有モデル」に沿って
セキュリティ対策を実施する

クラウド導入に向けたリスク可視化と
クラウド活用ルールや体制の整備

脆弱性やクラウド設定ミスに備える

NECではクラウド移行だけでなく、
セキュリティも含め様々なノウハウ、SLがございます
ぜひNEC・AWSと一緒にクラウド活用を始めましょう


Orchestrating a brighter world
NEC