データセキュリティワーキンググループ
活動報告

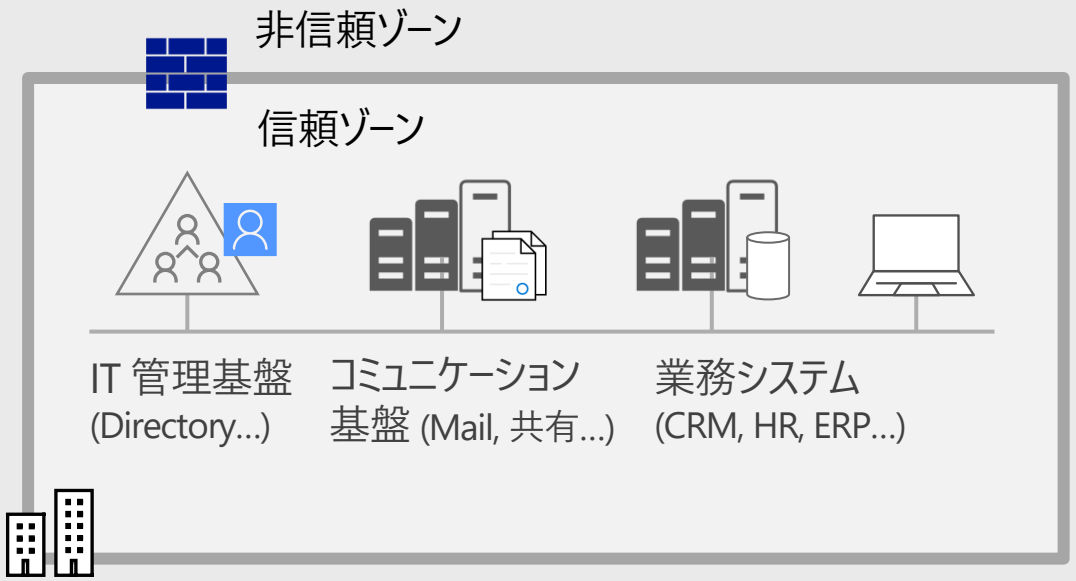
花村 実

セッションアジェンダ

- IT環境の変化とクラウドの発展
- 攻撃トレンドを踏まえた包括的なアプローチ
- ゼロトラストアーキテクチャ
- 暗号化・鍵管理
- モニタリング（今後）

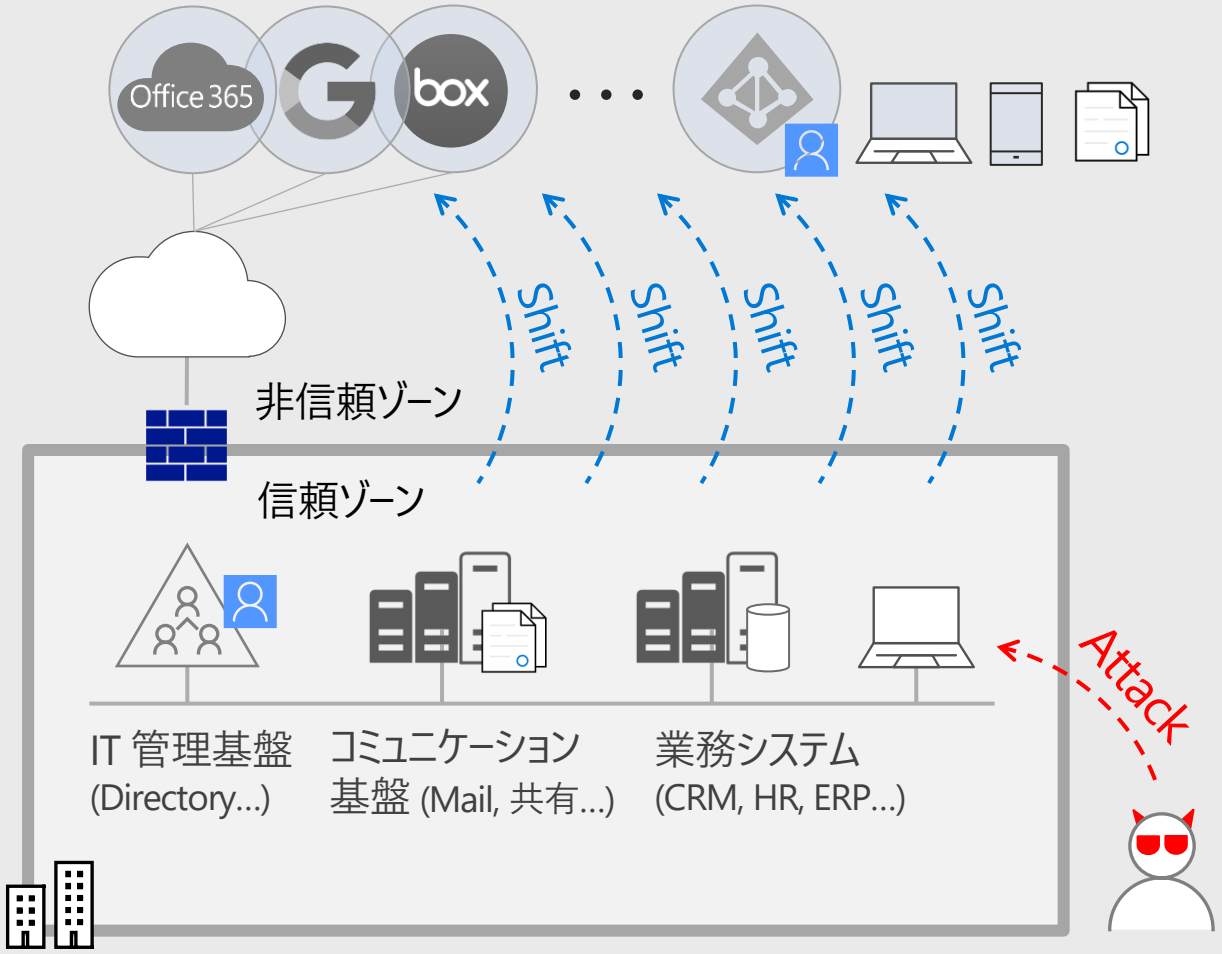
IT 環境の変化

1990年 – 2010年　ネットワーク境界モデル



IT 環境の変化

1990年 – 2010年　ネットワーク境界モデル → ネットワーク境界モデルの限界



システムのクラウドシフトが進み、
IT 環境が大きく変化

必要なモノが非信頼ゾーンに

攻撃の高度化、多様化により
信頼ゾーンへの侵入は日常的に

信頼ゾーンが信頼できない

マイクロソフトの社内環境とワークスタイル

マイクロソフト社内には、クラウドネイティブなネットワークが用意されており、社内外どこからでも生産性が高く安全な環境で働くことができます。ワークスタイル変革により、日本マイクロソフトは 10年間で 3倍以上の劇的な生産性向上を果たしています。

社内にもインターネット直結の高速ネットワークを用意

クラウドネイティブなワークスタイル

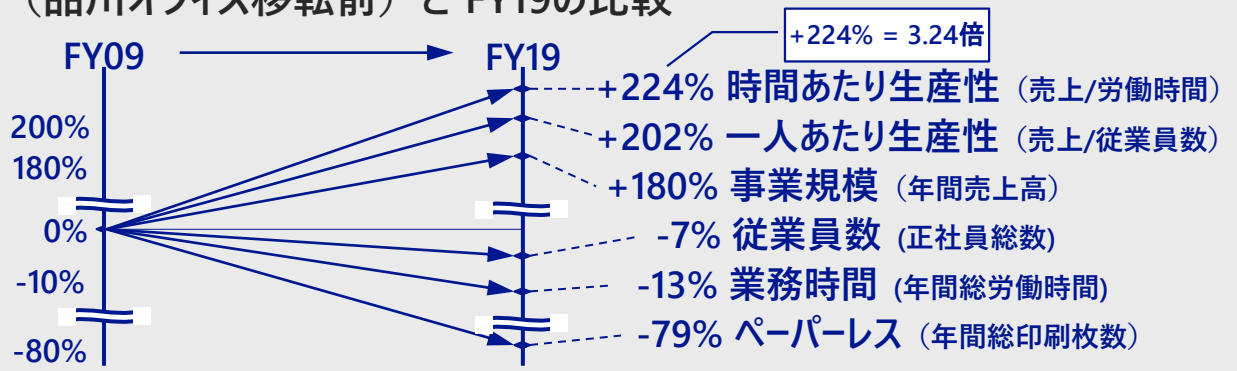
生産性の高いセキュリティ環境とルール

セキュリティ対策	社員の義務
強固なシングルID	コンプライアンス
多層防御	セキュリティ ポリシー
標的型攻撃対策	就業規則

利便性

セルフサービス IT / BYOD許可 / PC持出可

FY09（品川オフィス移転前）と FY19の比較



共有責任モデル (Shared Responsibility Model)

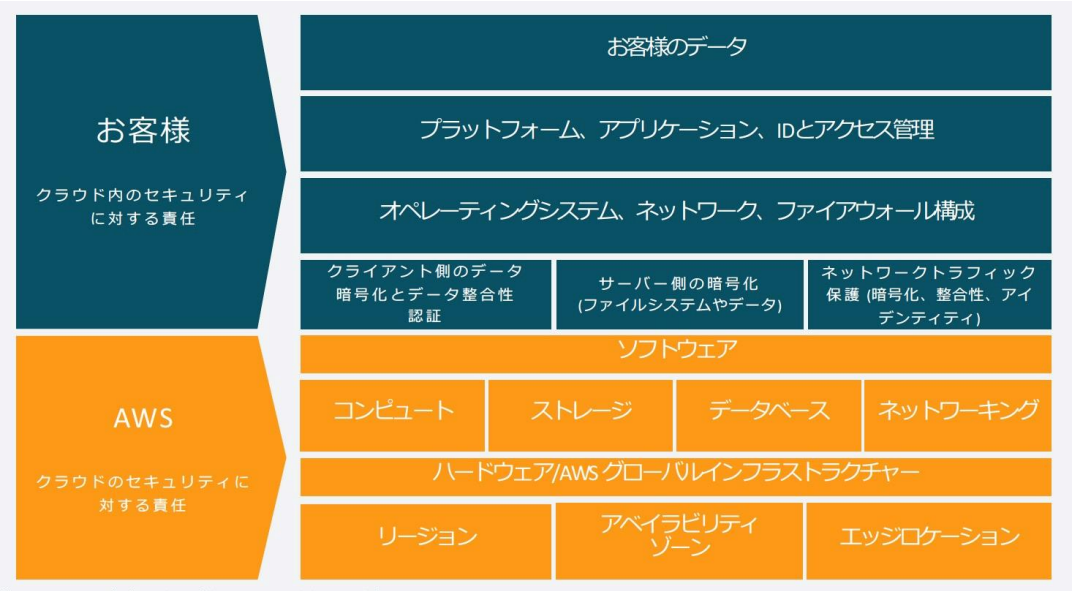
ユーザーの責任

データ
セキュリティ

インフラ
セキュリティ

プロバイダーの責任

共有責任モデル
責任共有モデル
共同責任モデル



AWS

https://aws.amazon.com/jp/compliance/shared-responsibility-model/

“内の”
vs
“の”

Azure

https://docs.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility

THALES

洗練化していく脅威

In the beginning

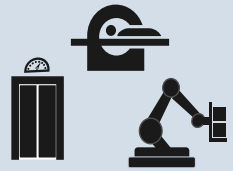
Isolated cases of nation-state espionage and young hackers exploring networks

Computing becomes pervasive

Computers used as tools to facilitate traditional offenses; hacking cases increase with motives becoming more diverse (e.g., fraud, hactivisim)

Today

Massive data thefts across verticals; rampant economic and military espionage; advanced persistent threats, destructive attacks



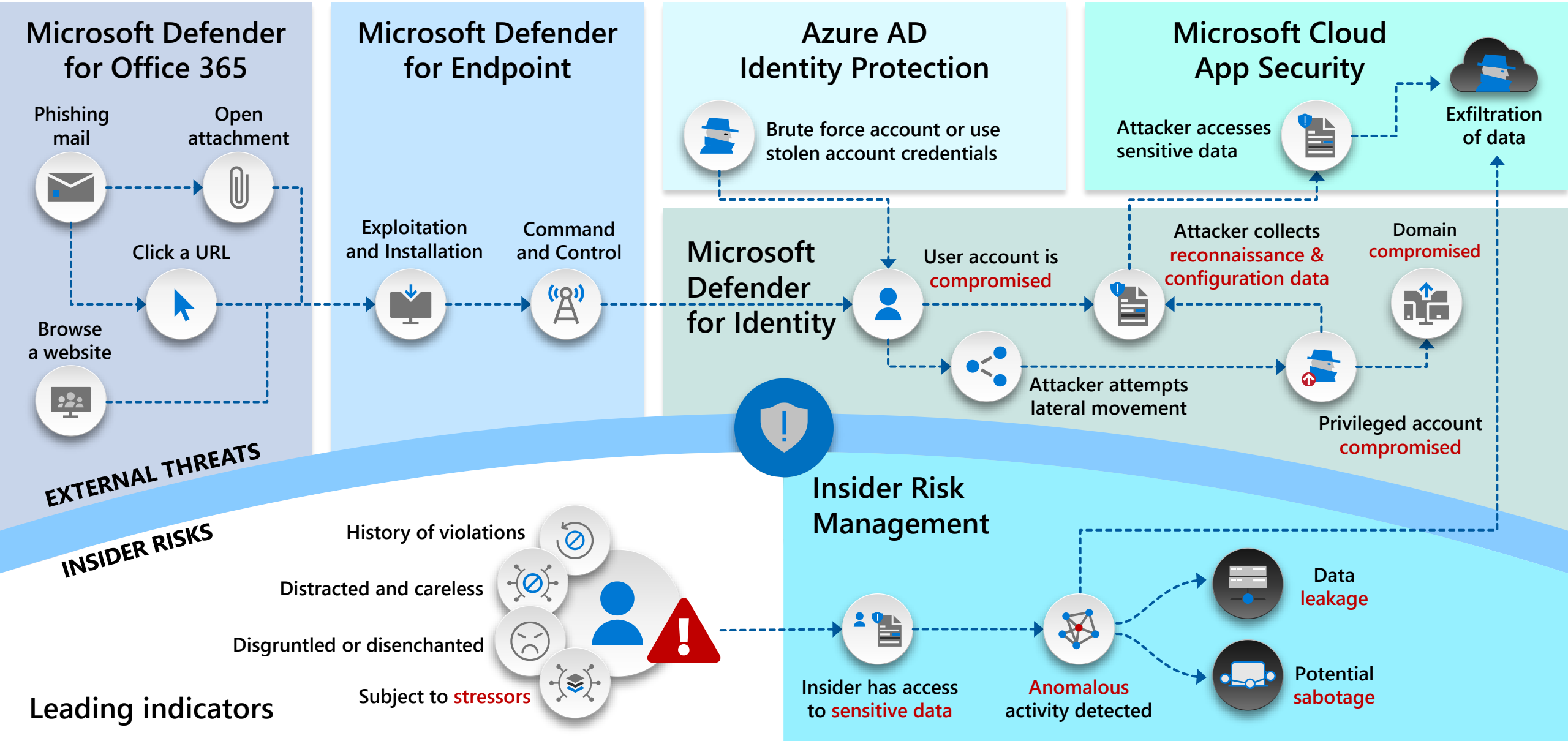
Future

Internet of Things enables new forms of large-scale attacks.

Militarization of Cyberspace continues.

Growth in cloud

多層防御 – 外部・内部


Microsoft Defender for Office 365
Phishing mail
Open attachment
Click a URL
Browse a website
Microsoft Defender for Endpoint
Exploitation and Installation
Command and Control
Azure AD Identity Protection
Brute force account or use stolen account credentials
Microsoft Cloud App Security
Attacker accesses sensitive data
Exfiltration of data
Microsoft Defender for Identity
User account is compromised
Attacker collects reconnaissance & configuration data
Domain compromised
Attacker attempts lateral movement
Privileged account compromised
EXTERNAL THREATS
INSIDER RISKS
Insider Risk Management
History of violations
Distracted and careless
Disgruntled or disenchanted
Subject to stressors
Leading indicators
Insider has access to sensitive data
Anomalous activity detected
Data leakage
Potential sabotage

データセキュリティ

- クラウドに持っていくデータに対する管理
- クラウド上にあるデータの保護と管理
  - ✓ アクセスコントロール
  - ✓ 暗号化
  - ✓ アーキテクチャ
  - ✓ 監視と警報
  - ✓ 追加的コントロール (DLP, ERMなど)
- 情報ライフサイクル管理に対応したセキュリティの適用
  - ✓ データの存在場所／収容場所の管理
  - ✓ コンプライアンスの確保
  - ✓ バックアップと事業継続

DOMAIN 1
クラウドコンピューティングコンセプトと
アーキテクチャー

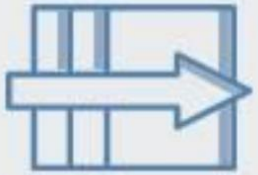
DOMAIN 2
ガバナンスと
エンタープライズマネジメント

DOMAIN 3
法的課題、契約
および電子証拠開示

DOMAIN 4
コンプライアンスと監査マネジメント

DOMAIN 5
情報ガバナンス

DOMAIN 6
管理要ダッシュボードと事業継続



DOMAIN 7
インフラセキュリティ

DOMAIN 8
仮想化とコンテナ技術

DOMAIN 9
インシデントレスポンス

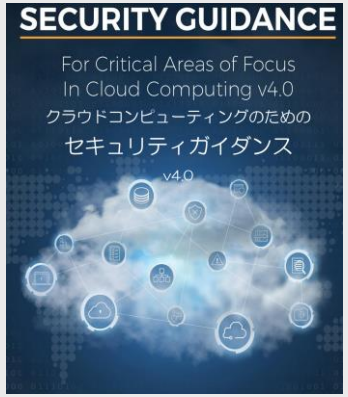
DOMAIN 10
アプリケーションセキュリティ

DOMAIN 11
データセキュリティと暗号化

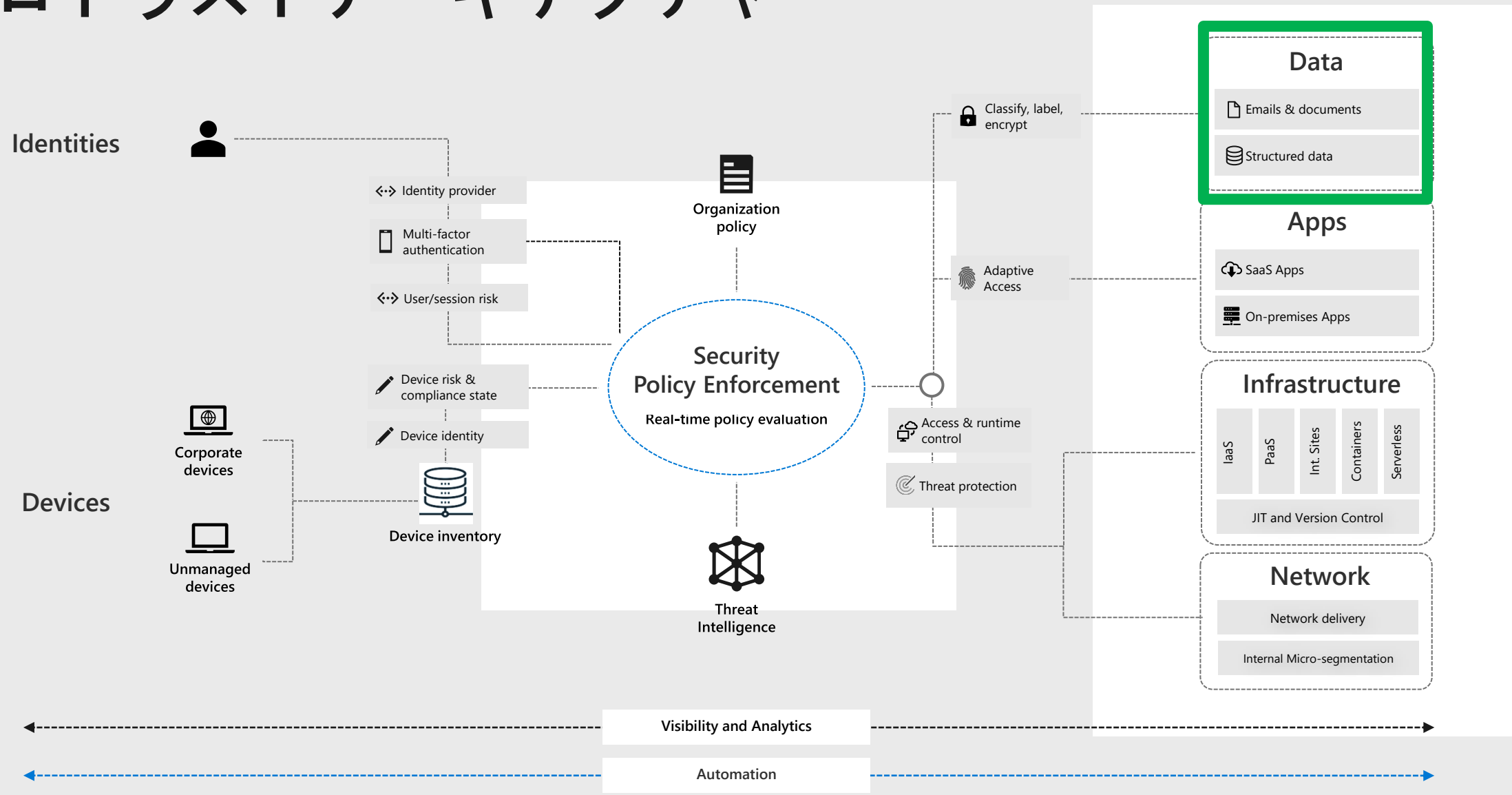
DOMAIN 12
アイデンティティ管理、
権限付与管理、アクセス管理
(IAM)

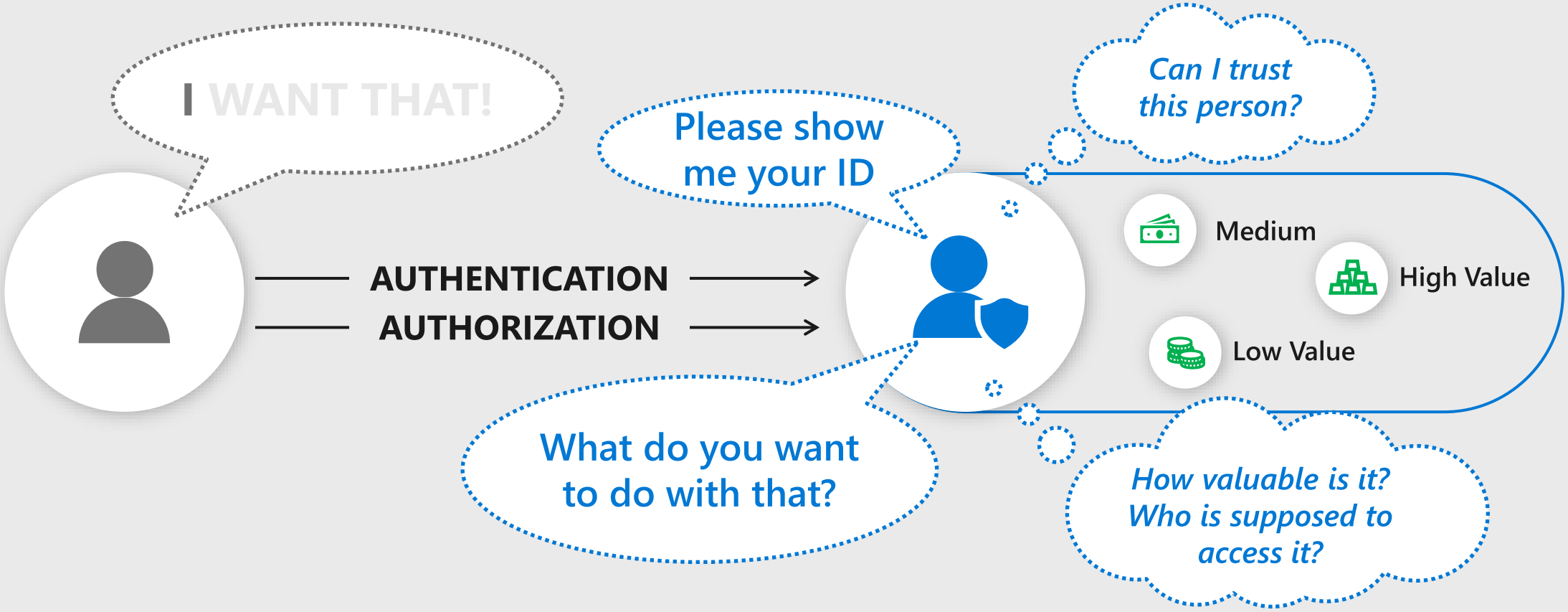
DOMAIN 13
Security as a Service

DOMAIN 14
関連技術

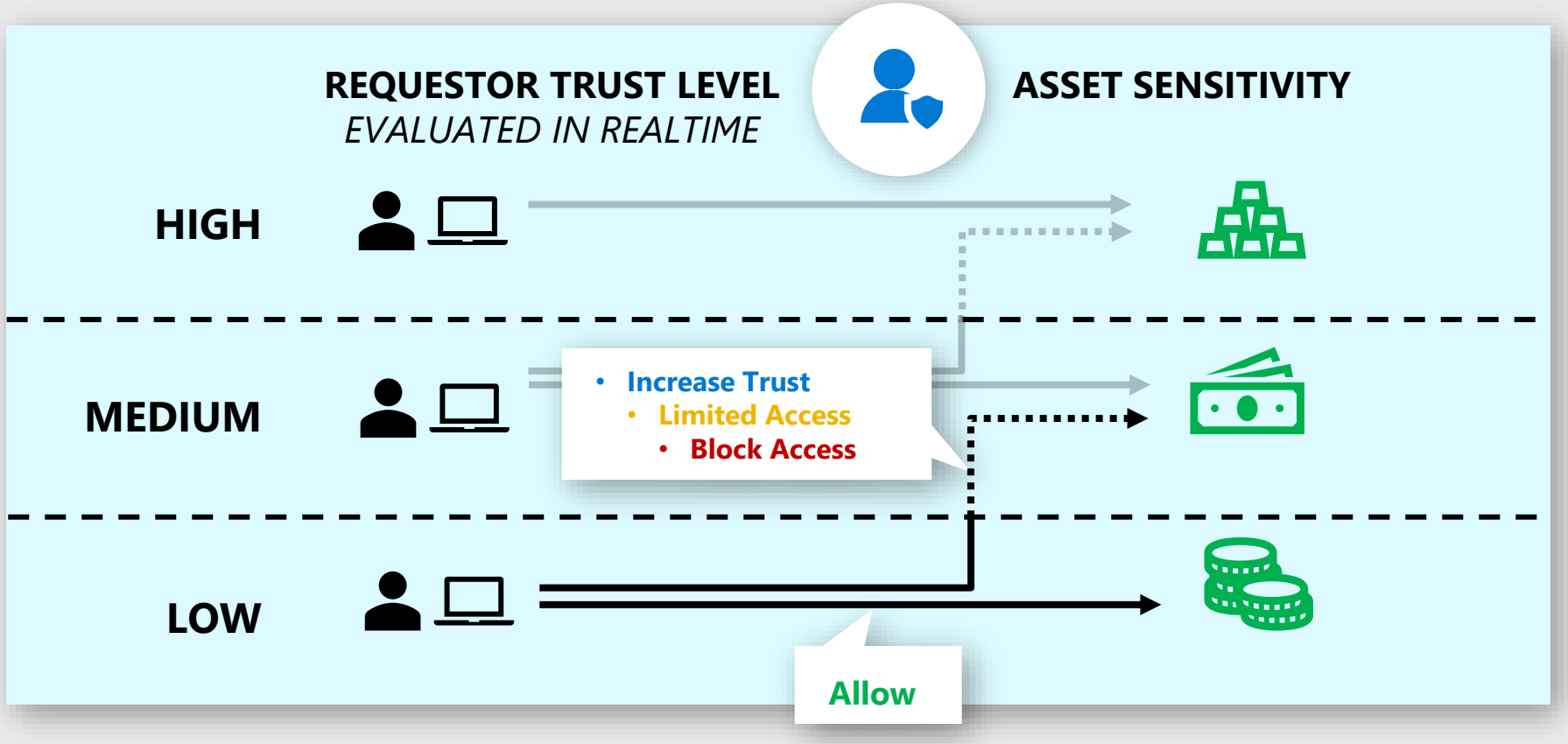


ゼロトラストアーキテクチャ

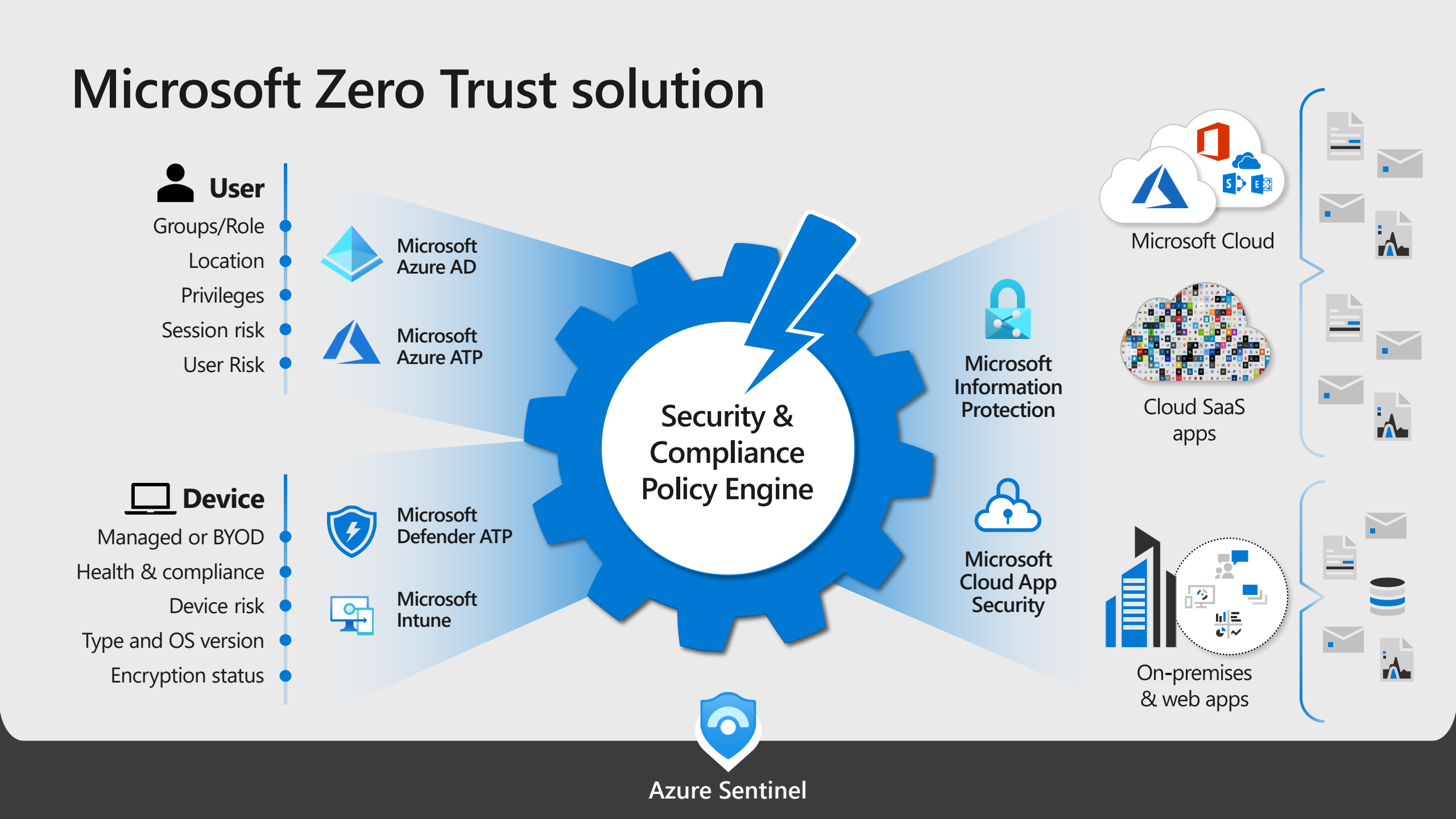



I WANT THAT!
Please show me your ID
AUTHENTICATION
AUTHORIZATION
What do you want to do with that?
Can I trust this person?
Medium
High Value
Low Value
How valuable is it? Who is supposed to access it?

What is Zero Trust (Access Control) All About?



Microsoft Zero Trust solution



THALES

データ保護と鍵管理

そもそも、なぜ暗号鍵管理が必要なのか?

自社の資産(データ)保護が主題

- 機密データの保護 → ビジネスの継続性確保・業界の規制への準拠 (PCI DSS等)
- 個人データの保護 → 社会的責任・法令順守 (個人情報保護法、GDPR等)

最も有効だと考えられている方法が暗号化による保護

暗号化データの安全性を担保するのが「暗号鍵」

暗号鍵管理の目的

暗号化による資産(データ)の保護 → ビジネス全体の保護

法令の中の鍵管理

サイバーセキュリティ関係法令 Q&A ハンドブック Ver1.0 (2020年3月)

- https://www.nisc.go.jp/security-site/files/law_handbook.pdf

- Q47 暗号の利用と情報管理等 (抜粋)
  - 暗号を利用するにあたっては、適切な強度の暗号を選択すること、**復号するための鍵について適切に管理すること**、危殆化が生じている暗号を利用しないことが必要である。
  - 一度暗号化された情報を再度意味内容が理解できるようにすることを復号というが、復号にあたっては、鍵が必要である。情報を暗号化したとしても、鍵が流出してしまうと、その流出した鍵を利用して第三者が復号することが可能になるなど、情報を暗号化した意味がなくなってしまう。そこで、**鍵の適切な管理も重要**である。
  - **復号鍵が適切に管理されていること**とは、①暗号化した情報と復号鍵を分離した上で、復号鍵自体の漏えいを防止する適切な措置を講じていること、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されることのいずれかを満たすことが必要である。
  - 一定の情報に対してサイバーセキュリティに関する義務が課されている法律は、金融分野、医療分野、労働分野などに多岐にわたっている。

個人情報保護法と鍵管理

「個人情報の保護に関する法律についてのガイドライン」及び「個人データの漏えい等の事案が発生した場合等の対応について」に関するＱ＆Ａ（抜粋）

- https://www.ppc.go.jp/files/pdf/170530_faq_rouei.pdf

- 「漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合」
- 暗号化等の技術的措置が講じられた情報を見読可能な状態にするための手段が適切に管理されているといえるためには、①**暗号化した情報と復号鍵を分離**するとともに**復号鍵自体の漏えいを防止する適切な措置を講じている**こと、②遠隔操作により暗号化された情報若しくは復号鍵を削除する機能を備えていること、又は③第三者が復号鍵を行使できないように設計されていることのいずれかの要件を満たすことが必要と解されます。

NIST (米国国立標準技術研究所) 発行の情報セキュリティ関連文書

鍵管理における推奨事項 SP800-57

- https://www.ipa.go.jp/files/000055490.pdf
- https://www.ipa.go.jp/files/000055491.pdf

【概要説明】 NIST及びNIST発行の情報セキュリティ関連文書

- https://www.ipa.go.jp/security/publications/nist/nist_publications.html
- 翻訳文書 https://www.ipa.go.jp/security/publications/nist/

- SP800シリーズは、CSDが発行するコンピュータセキュリティ関係のレポートです。米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書ですが、 内容的には、セキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応など、セキュリティに関し、幅広く網羅しており、政府機関、民間企業を問わず、セキュリティ担当者にとって有益な文書です。(IPAサイトより引用)

データに対する責任はユーザにある、しかし・・・

100%

全ての組織が、クラウド内の機密データの少なくとも一部が、暗号化保護されていないと回答

クラウド内の全機密データのうち、暗号化で保護されているのはわずか57%

わずか

57%

「より多くの機密データがクラウド環境に保存されると、データセキュリティ リスクが増大する。しかし、かなりの量のデータが露出しているにもかかわらず、データを暗号化やトークン化している率は低い」
- IDC

Source: 2020年 タレス データ脅威レポート
dtr.thalesesecurity.com

CCM v3.0.1 に記載されているクラウド鍵管理について

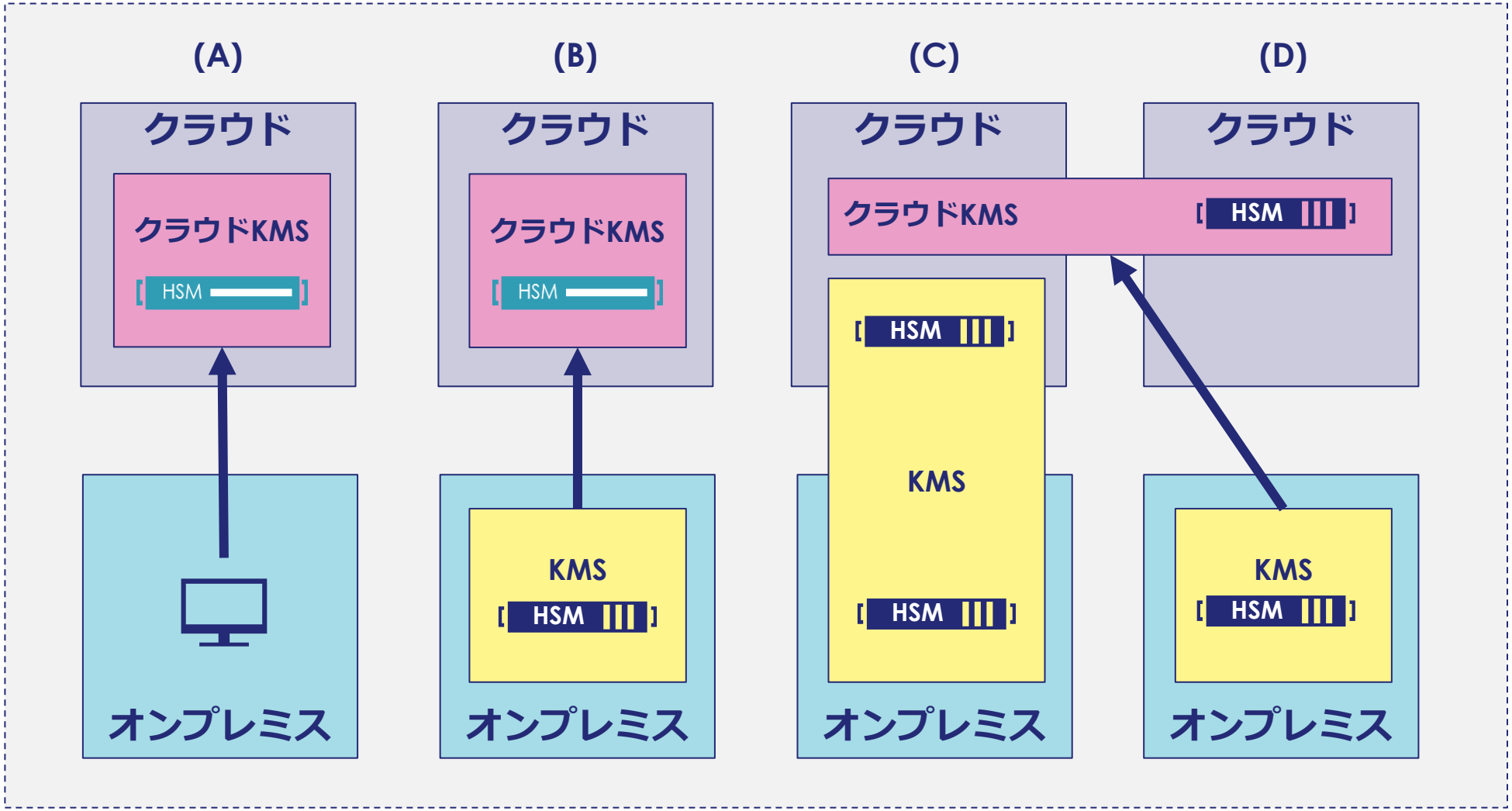
Cloud Controls Matrix (CCM)

- ガイダンスの14領域におけるセキュリティコントロールのフレームワーク
- バージョン3.0.1 (2017年10月リリース)
- 暗号化と鍵管理については EKM-01 ~ EKM-04 に定義
- https://cloudsecurityalliance.org/research/cloud-controls-matrix/
- https://cloudsecurityalliance.org/artifacts/ccm-translation-in-10-languages/

Control ID	Control Domain
EKM-01	暗号化と鍵管理: 権限付与
EKM-02	暗号化と鍵管理: 鍵生成
EKM-03	暗号化と鍵管理: 機密データの保護
EKM-04	暗号化と鍵管理: 鍵の保管とアクセス

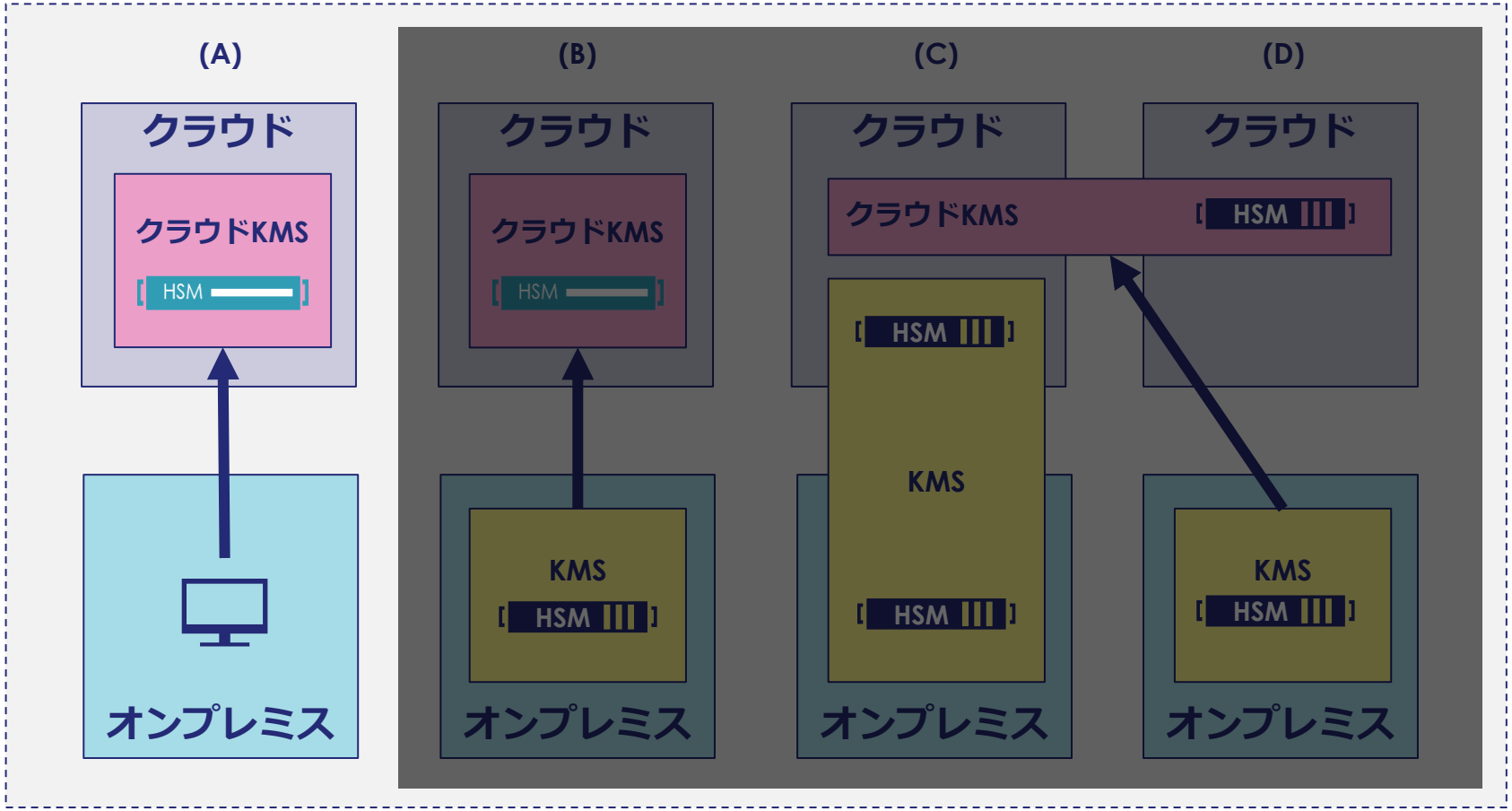
オープンな検証済みの形式かつ標準アルゴリズムであるプラットフォームやデータに適した暗号化方式(AES-256など)を使用しなければならない。
鍵は（当該クラウド事業者の）クラウド内に保管するのではなく、クラウドの利用者または信頼できる鍵管理事業者が保管しなければならない。
鍵の管理と鍵の使用は、異なる責務として分離されなければならない。

クラウドサービスと鍵管理システムの運用パターン



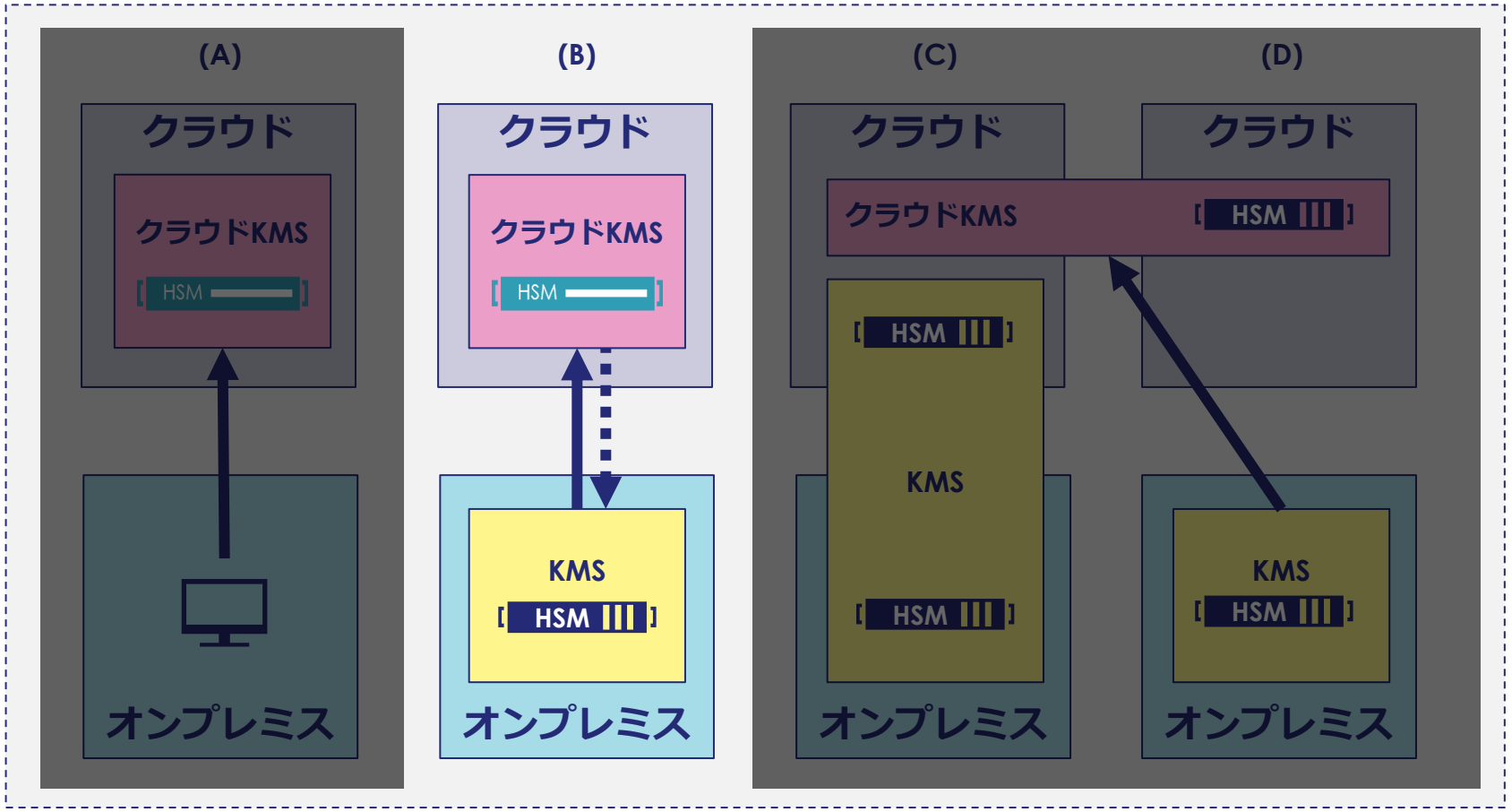
HSM クラウド HSM　　HSM プライベート HSM　　KMS: 鍵管理システム

(A) クラウドネイティブ型



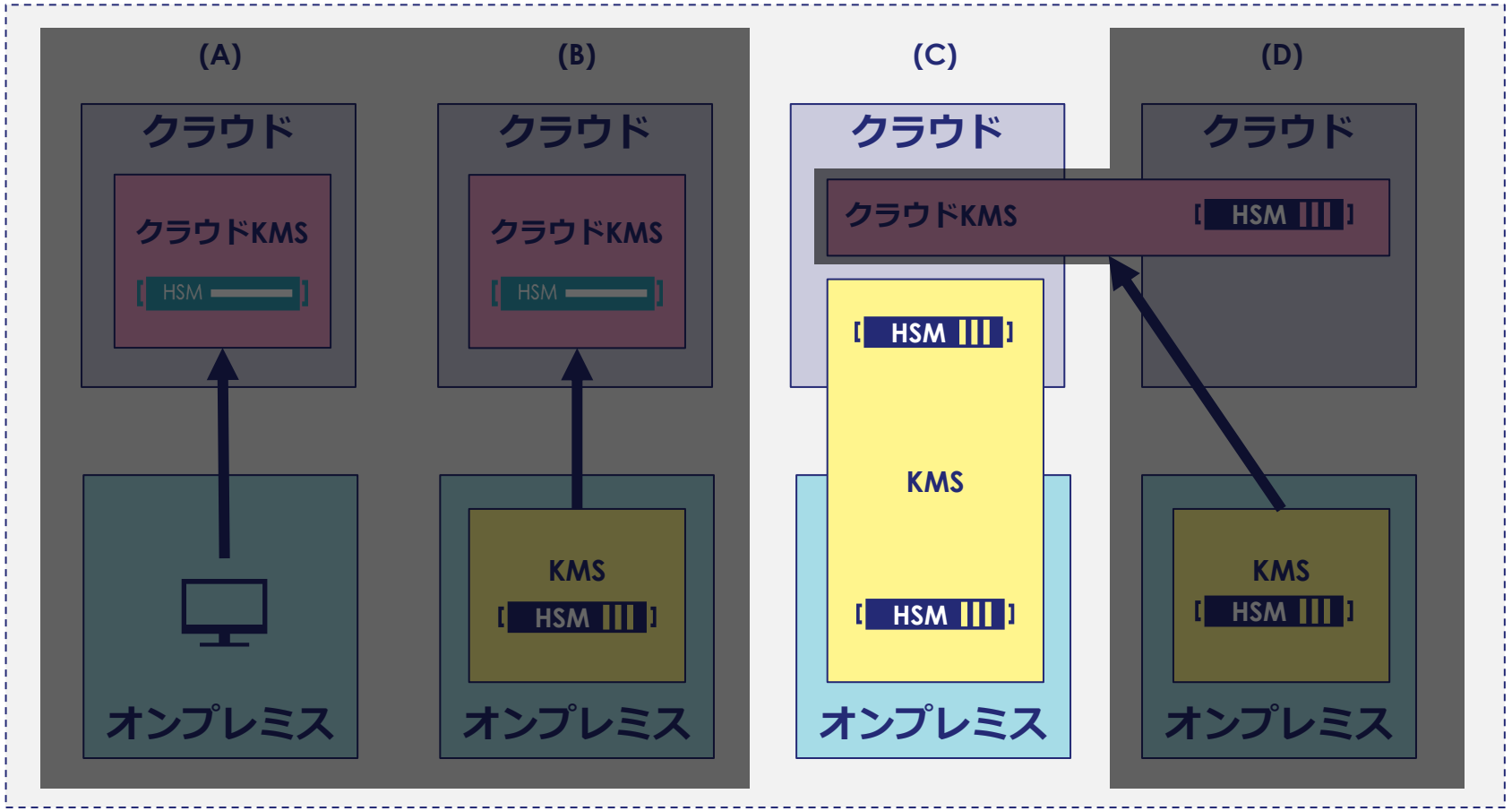
同じクラウド内で、クラウドKMS(HSMを含む)を活用する

(B) 外部鍵作成型



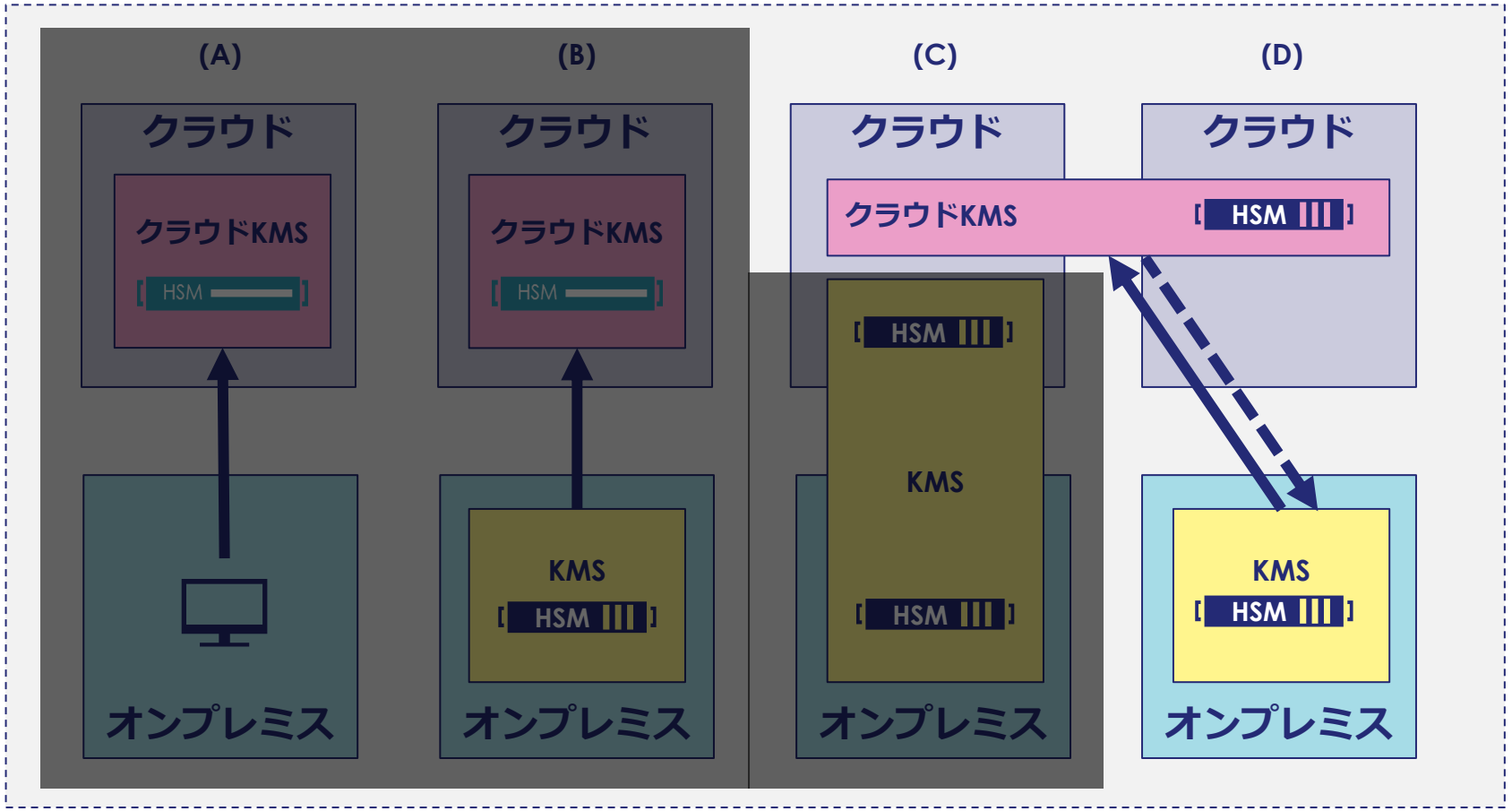
(A)を拡張して、外部のKMSからキーマテリアルをインポートできるようにする

(C) 外部鍵管理システム使用型



所有組織の制御下にあり、クラウドプロバイダーのデータセンター内で物理的にホストされている専用(プライベート)HSMを備えたクラウドKMS

(D) マルチクラウド鍵管理システム型

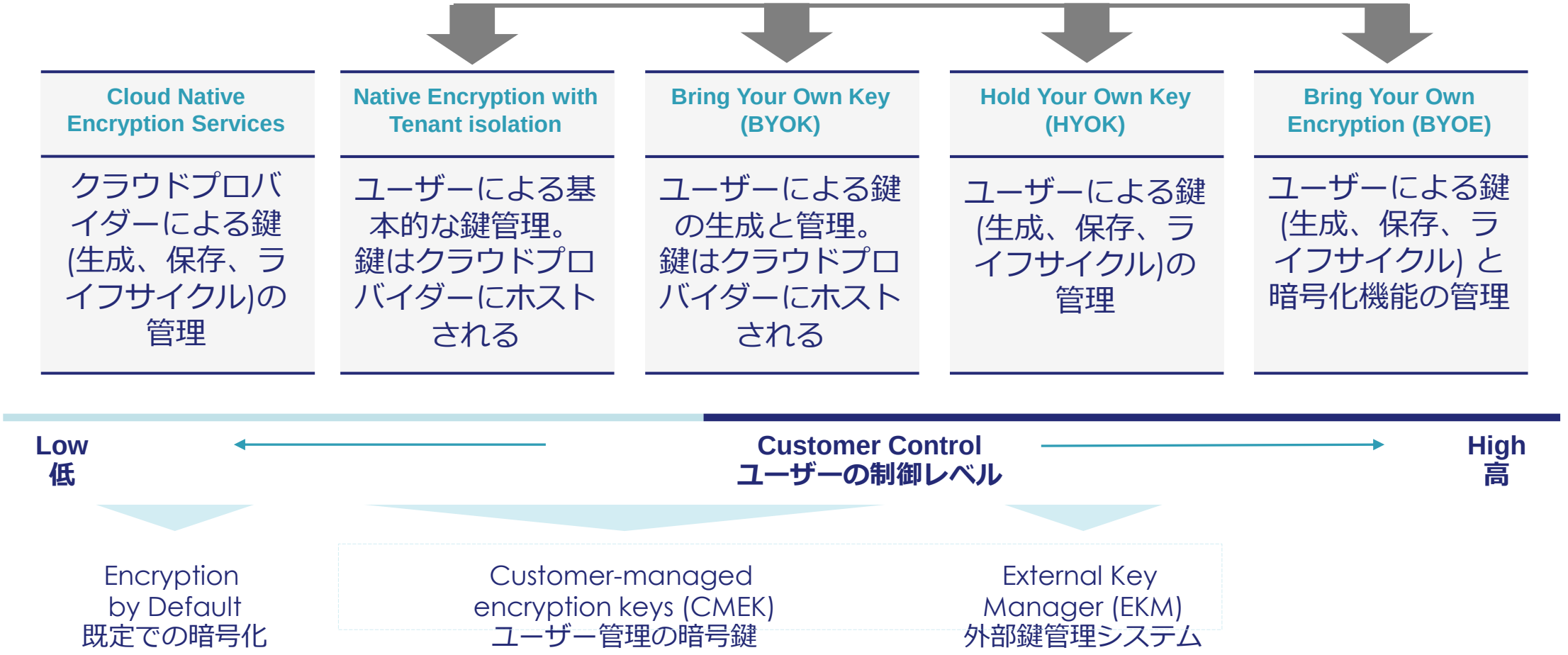


オンプレミスのKMSが、オンプレミスまたはクラウドでホストできるマルチクラウドKMS統合/管理に使用され、HSMなどのオンプレミス暗号化モジュールにリンクされている

クラウドデータの暗号化 – 制御可能なレベルを理解する

タレスのソリューションにて実装できる機能レベル

THALES



THALES

Azure Information Protection（AIP）とは

組織内外でのドキュメント ライフサイクル全体にわたる機密データの包括的な保護

検出
ポリシーに基づいた
機密データのスキャンと検出

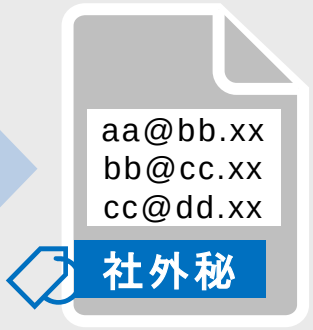
分類
データを分類し、機密レベルに
応じてラベルを適用

保護
暗号化、アクセス権限に基づく
保護を適用

可視化/監視
アクセス権のはく奪と
保存状況のレポーティング

データを作成/保存、内容を自動的に検出

内容に基づいて自動的に分類(ラベル付与)



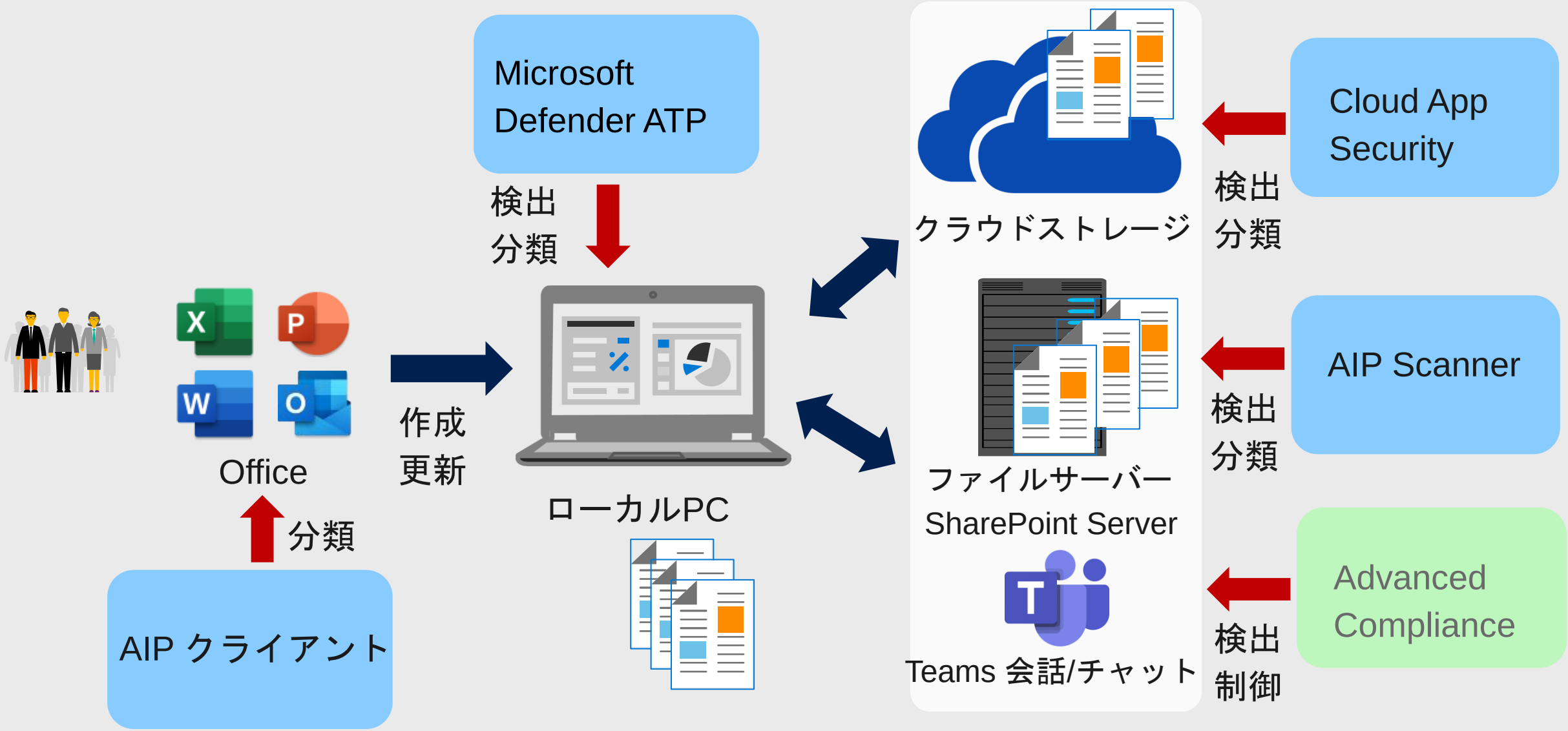
ラベルに基づき暗号化、権限を設定

ファイルの追跡とアクセス権限はく奪

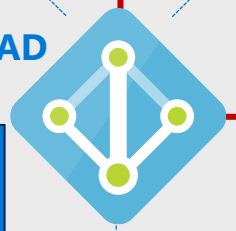
ファイルの保存場所と分類ラベルごとの個数を定量的に把握

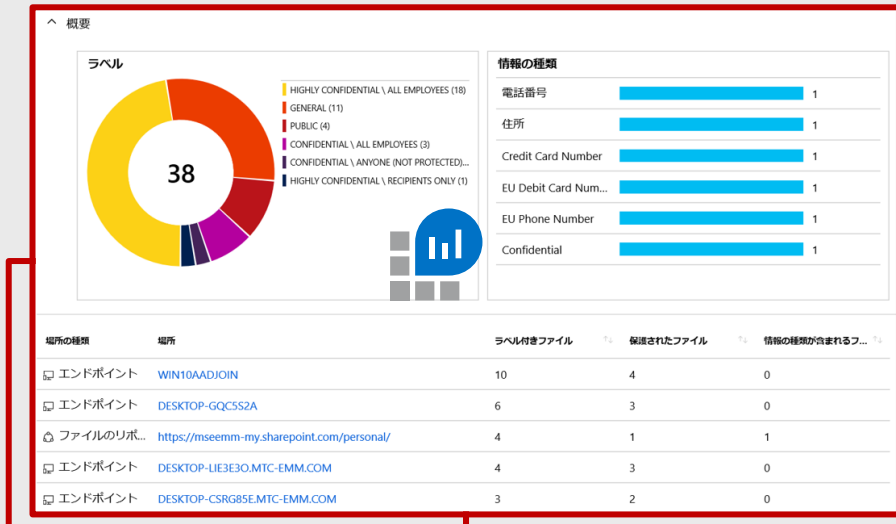
保存場所に依存せずに個人情報の可視化する

Microsoft Information Protectionにより、様々な場所での自動検出とラベリングを実施



[AIP+MCAS+MDATP]個人情報の可視化





ファイルの保存場所や付与された分類ラベルごとに、個人情報を含むファイルが何件あるか検出して確認が可能

- ファイルサーバ：**AIP P2**
- ローカルPC：**MDATP**
- クラウド：**MCAS**

Microsoft Cloud App Security

・クラウドサービスのカタログ情報
・クラウドサービス内でのアクティビティの可視化
・シャドーITの検出(MDATP連携)
・AIPラベルのスキャン
・SaaS内での機密情報の可視化
・異常行動検知など

Azure Information Protection

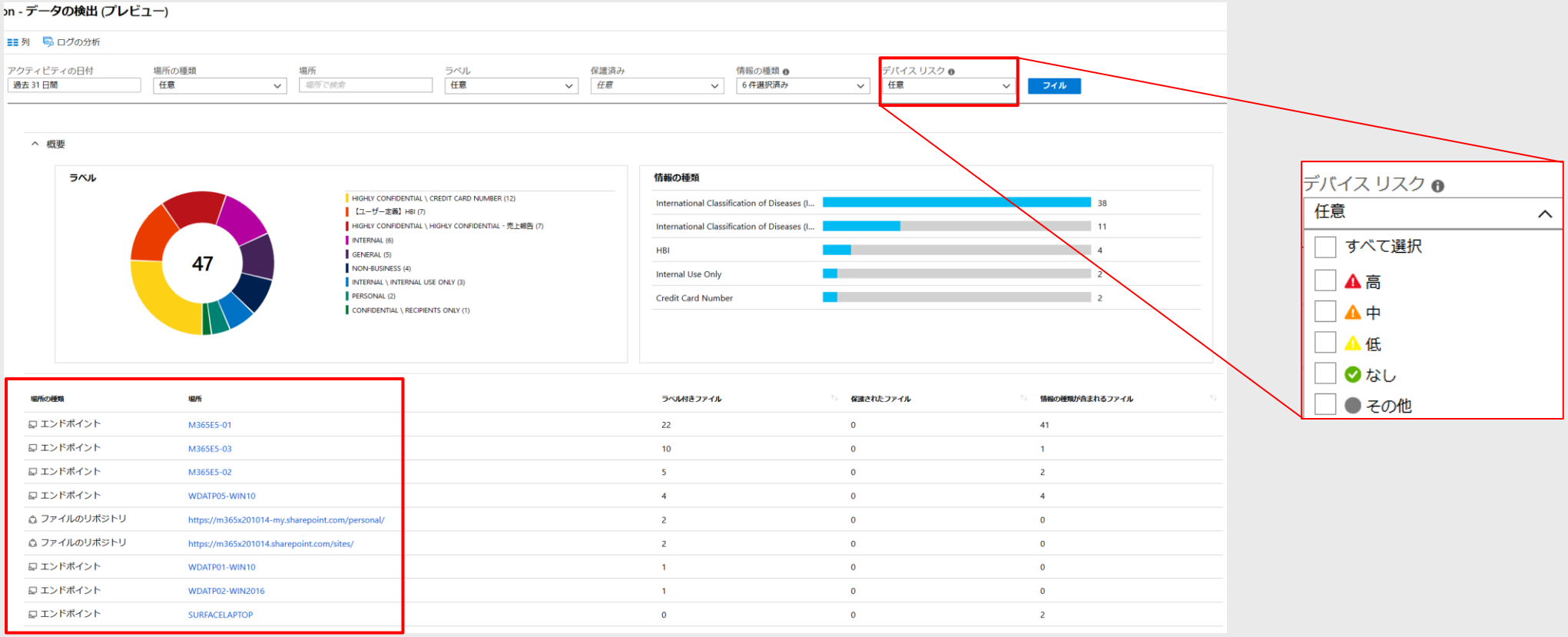
・ファイルの暗号化
・データ分類ラベルに基づいたファイルのアクセス制御
・ファイルのアクセス履歴追跡とアクセス権はく奪

Microsoft Defender ATP

・Windows Defenderの管理
　・Defenderウイルス対策、Exploit Guard等
・エンドポイントの詳細痕跡調査(EDR)
・シャドーIT検知(MCAS連携)
・ソフトウェアインベントリ収集
・脆弱性(パッチ)管理
・AIPラベルのスキャン
・リモート調査(Live Response)など

[AIP+MCAS+MDATP]個人情報の可視化：データの検出

- ラベルが付与されたファイルがどこにどれだけ保存されているか確認可能



デバイスのリスクレベルに応じて優先的に保護すべきファイルに絞ることも可能。

- （例）役員や経理部等のデバイスがリスクレベル「高」の場合、そのデバイスに保存されている情報もリスクにさらされている可能性が高い
- （例）デバイスにファイルを保存する運用もリスクを伴うため、クラウドへデータを保存することも検討

モニタリング：CSPM、CWPP

CSPM
(Cloud Security Posture Management)

マルチクラウドの
セキュリティポスチャを管理

セキュア スコア | ポリシーと コンプライアンス | 高度な 自動化

Azure Defender

Leveraging Azure Arc

CWPP
(Cloud Workload Protection Platform)

Azure Defender による
ハイブリッドクラウドの保護

脆弱性の 管理 | 高度な クラウド防御 | 脅威検知 と対処

クラウドセキュリティの一元化

クラウド態勢管理 – Azure Security Center

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

マルチクラウド環境サポート

Azure 、AWS、GCP環境のSecurity Posture を一元管理、インベントリ

セキュアスコア

組織全体のセキュリティの状態を可視化するための数値指標を導入

コンプライアンスチェック

Azure CIS、PCI DSS 3.2、ISO 27001、SOC TSP NIST SP 800-53 R4、SWIFT CSP CSCF-v2020、UKO および UK NHS、Canada PBMM

ガバナンス・リスク・コントロール プロフェッショナル

リスクとコンプライアンスを評価します。

IT /セキュリティ プロフェッショナル

プロテクションを実装します。

CSPM

(Cloud Security Posture Management)

マルチクラウドの
セキュリティポスチャを管理

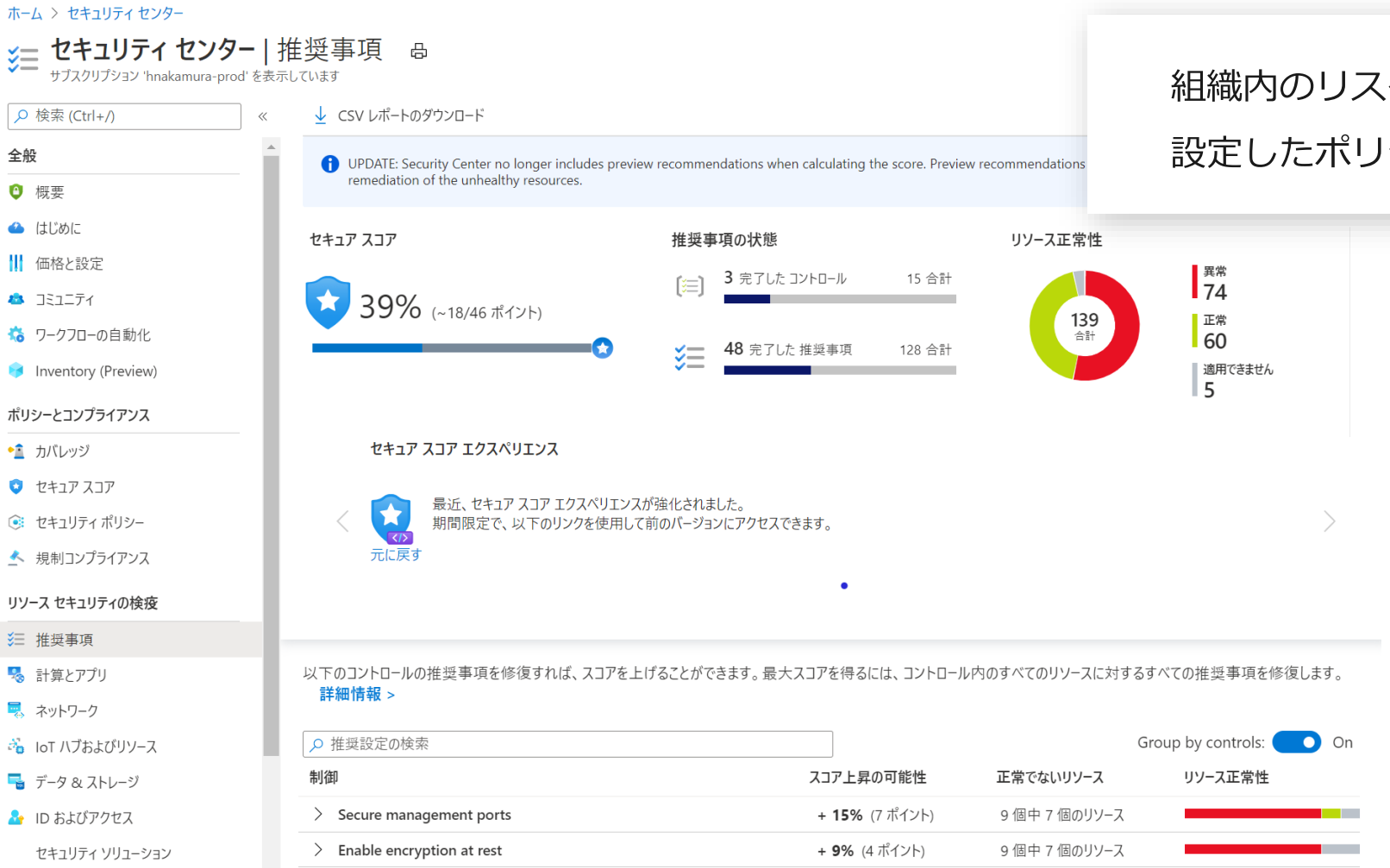
セキュア スコア	ポリシーと コンプライアンス	高度な 自動化

主な機能

- Azure、AWS、Google マルチクラウドサポート
- セキュアスコアによるリスクの可視化を提供
- 豊富なコンプライアンスチェックの自動化、可視化
- Azure セキュリティ・ベストプラクティスの提供

セキュアスコア

組織全体のセキュリティの状態を可視化するための数値指標を導入
　個々の項目に、重要度やセキュリティベストプラクティスから点数が設定



組織内のリスクの特定に利用

設定したポリシーに基づき、改善点を修正

ワークロード保護 – Azure & ハイブリッドのワークロド

IDENTIFY | PROTECT | DETECT | RESPOND | RECOVER

Azure Defender for Server

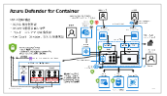
Azure環境、オンプレ環境、
AWS環境のサーバー保護

Azure Defender for SQL

脅威の検知、脆弱性評価を実施

Azure Defender for Containers

AKS、ACRのセキュリティ機能を提供



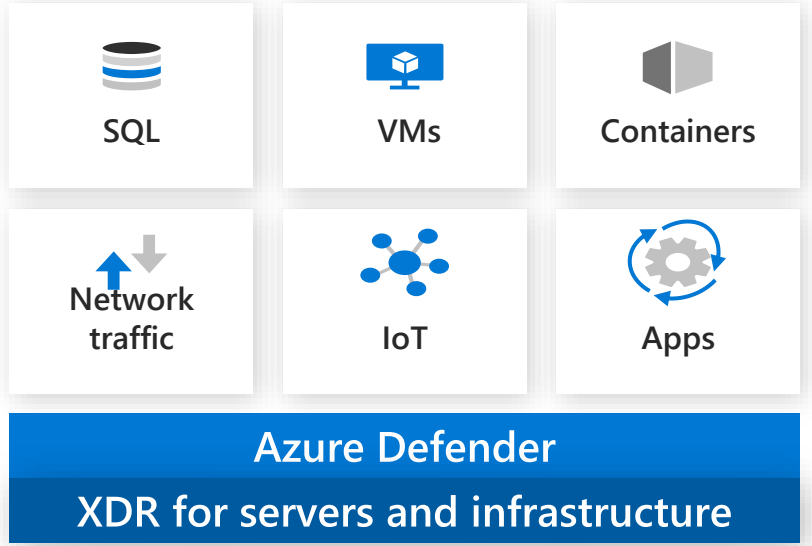
Azure Defender for Storage

Storage / Files の脅威検知機能を提供

Azure Defender for IoT

エージェントレス IoT/OT セキュリティ (Coming soon)

ハイブリッド クラウドのワークロード向けの組み込みの保護



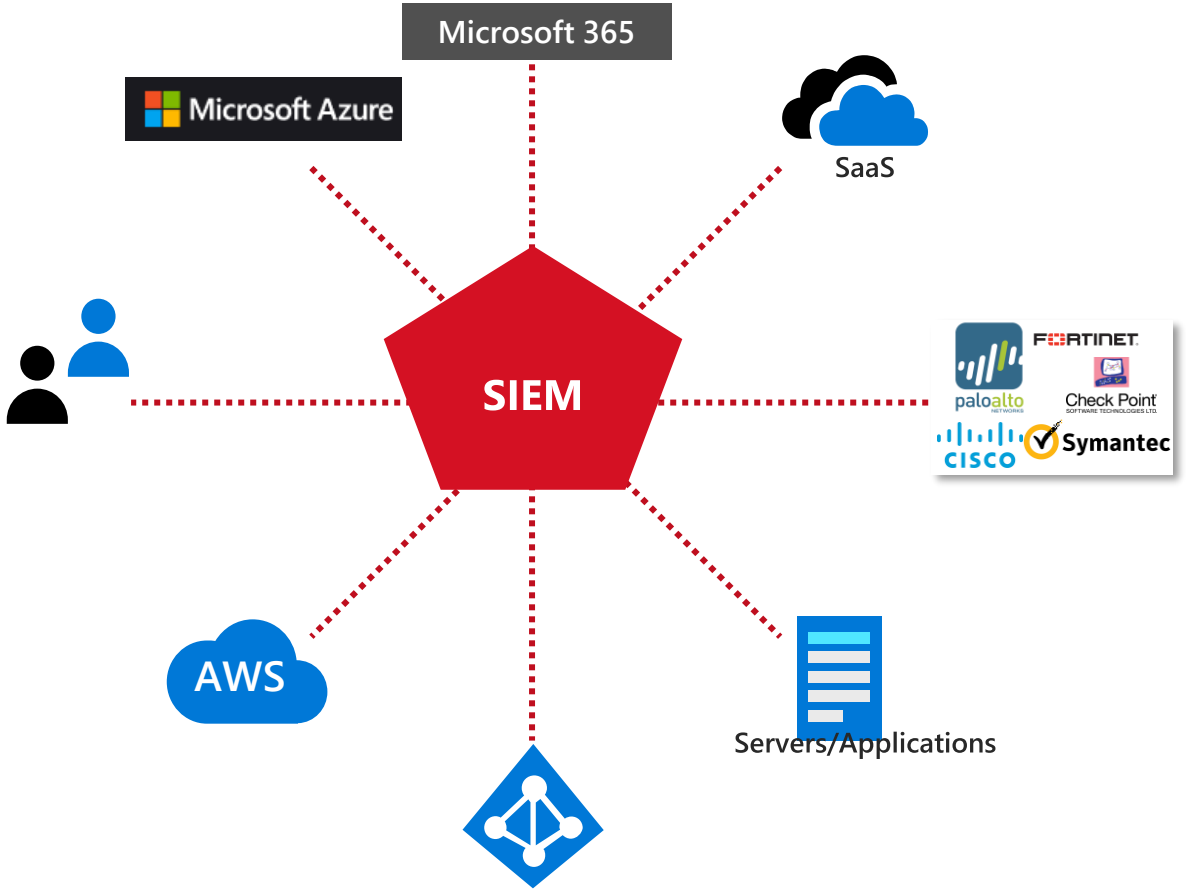
主な機能

- Azure とハイブリッド ワークロードを高度かつインテリジェントに保護
- Azure Defender for Server (EDR) を利用したサーバ保護
- 脆弱性評価エンジンによるスキャン
- Azure 環境のPaaS向け脅威防御を提供
- 検出したアラートはAzure Security Centerで管理可能。また、Azure Sentinelとの連携によるアラートの一元管理が可能

SIEM はエンタープライズのセキュリティに関わるログを集約

SIEM

Security Information Event Management

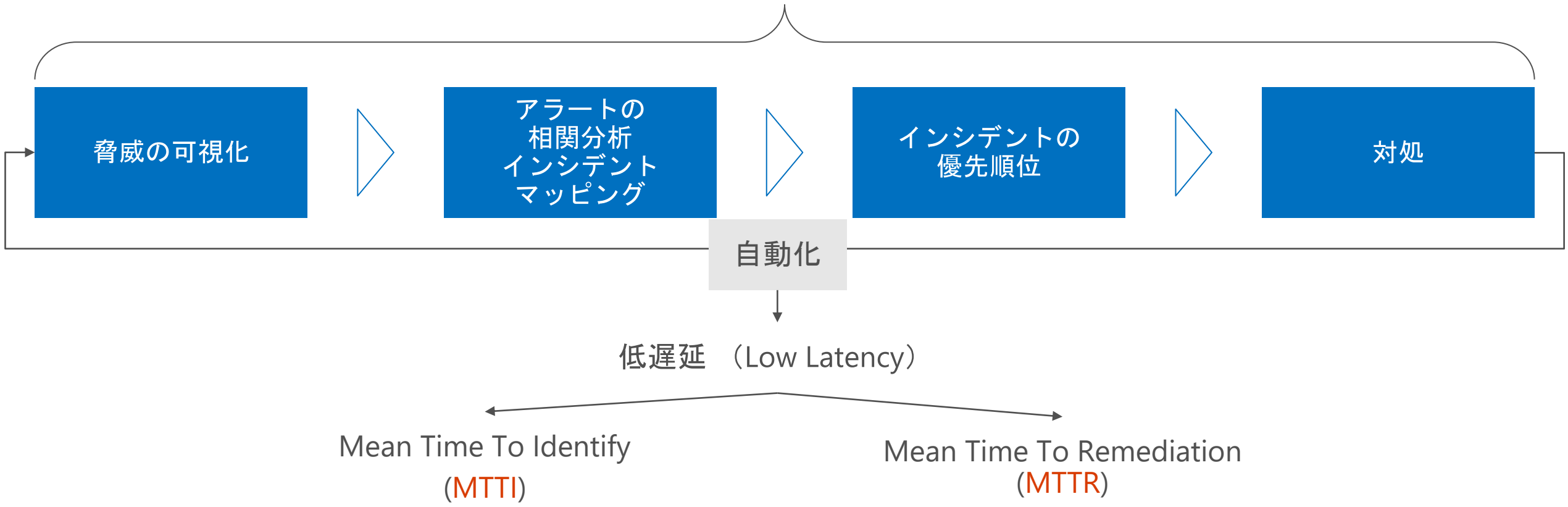


セキュリティ運用負荷軽減を実現するために...

SOAR

Security **O**rchestration **A**utomation **R**esponse

セキュリティ製品間の連携　手動 → 自動　自動調査＆対処



脅威の検知

検知

ビルトイン機械学習 (ML) モデル

- Geo Location Anomaly Detection (GLAD)
- 異常な SSH / ADFS / RDP / RAS ログイン

Geo Location Anomaly Detection (GLAD)

過去のログイン履歴を記録する

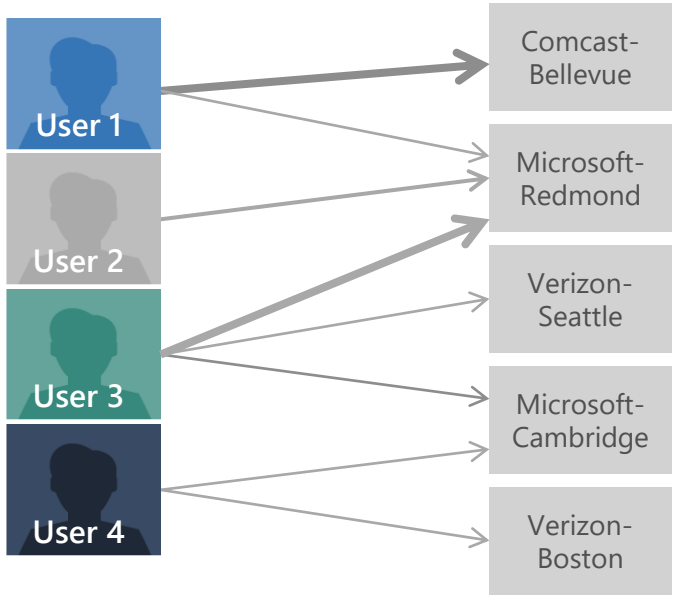
45日間の履歴から分析
アクセス 頻度 / 時間に基づいて重み付け

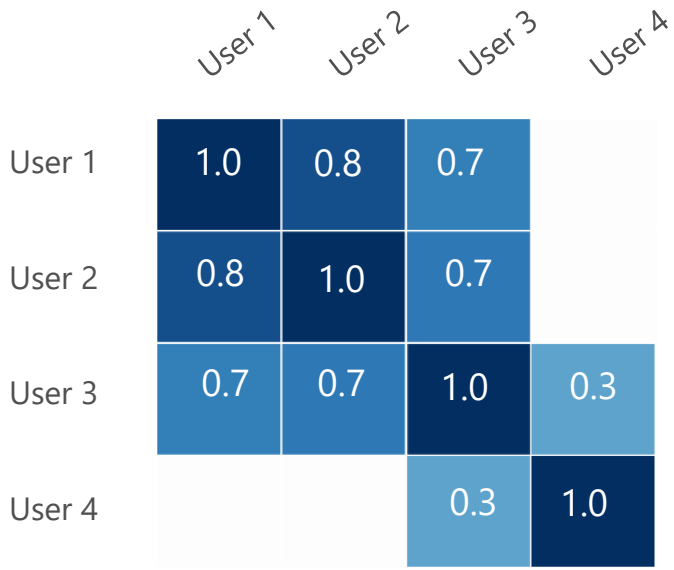
過去のログイン履歴を計算

アクセス場所間の部分マッピング
テナント内で制約

アクセス可能な場所を推測

他の同様の地域への部分的なマッピング





User	Location	Reachability
User 3	Comcast-Bellevue	965.0
User 3	Comcast-Redmond	875.0
User 3	Microsoft-Redmond	978.0
User 3	Verizon-Seattle	425.0
User 3	Verizon-Bellevue	350.0
User 3	Microsoft-Cambridge	275.0
User 3	Verizon-Boston	152.0

Threat Investigation
脅威の分析・調査

調査

各Entity の関係性を自動抽出し、ヴィジュアルに調査
タイムラインの表示により、インシデントの時系列を把握

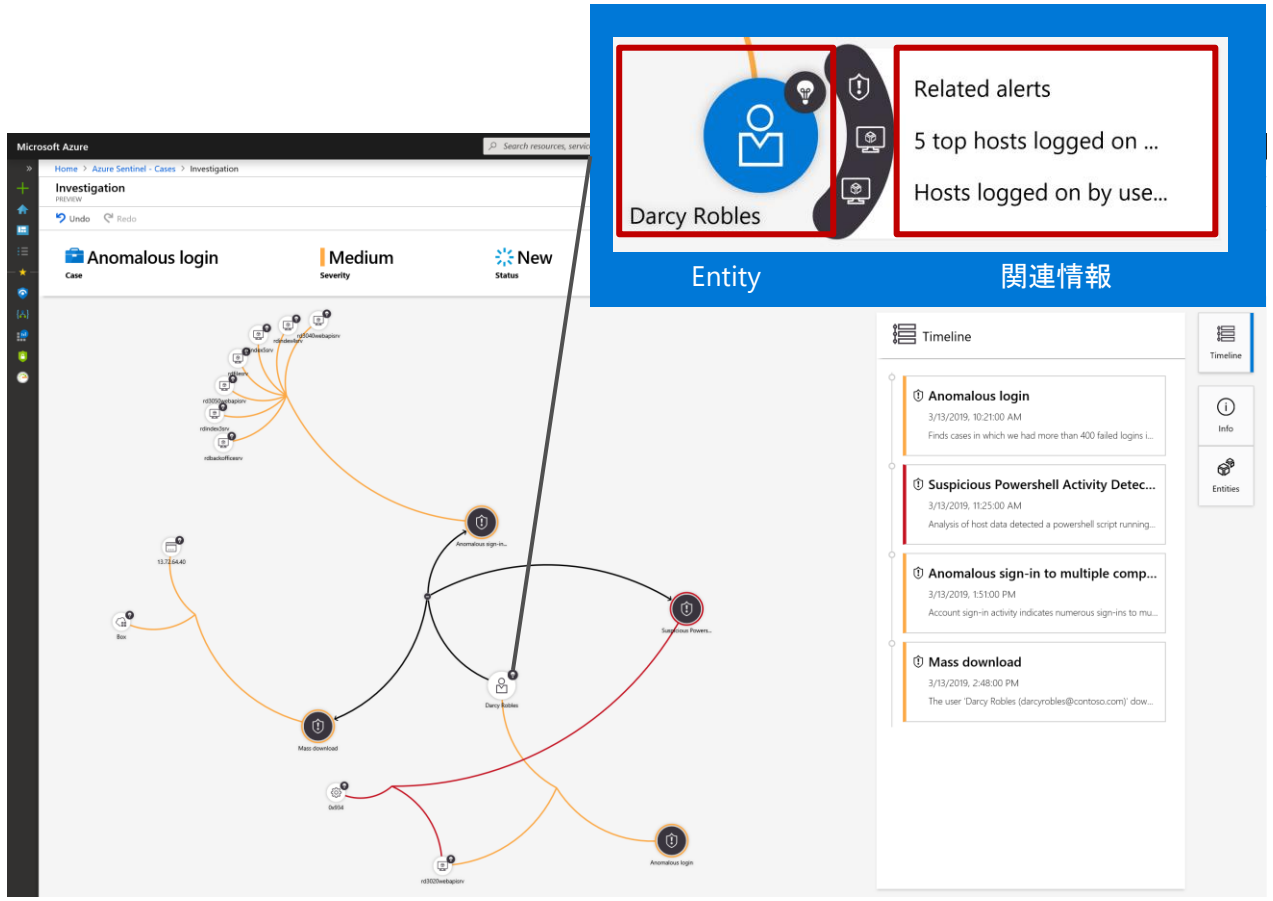
ユーザ
1. **関連するアラートの表示**
2. **ログオン履歴 TOP 5 の端末の表示**
3. **インシデント時のログインした端末一覧の表示**

端末
1. 関連するアラートの表示
2. ログオンしたアカウント一覧を表示
3. 最もアクセスされていないドメイン TOP 5 を表示

IP アドレス
1. 関連するアラートの表示
2. インシデント時にアクセスしていた端末 TOP 5 の表示
3. 過去最もアクセスしていた端末 TOP 5 の表示

プロセス
1. 関連するアラートの表示
2. 最も特定のプロセスを実行していない端末 TOP 5 の表示
3. プロセスを実行している全ての端末一覧

アプリ
1. 関連するアラートの表示
2. アプリを最も使っているユーザ TOP 5 を表示
3. アプリを最も使っていないユーザ TOP 5 を表示



Entity を自由に指定
クエリを活用し、各Entity に対する任意の関連情報の表示

Questions?