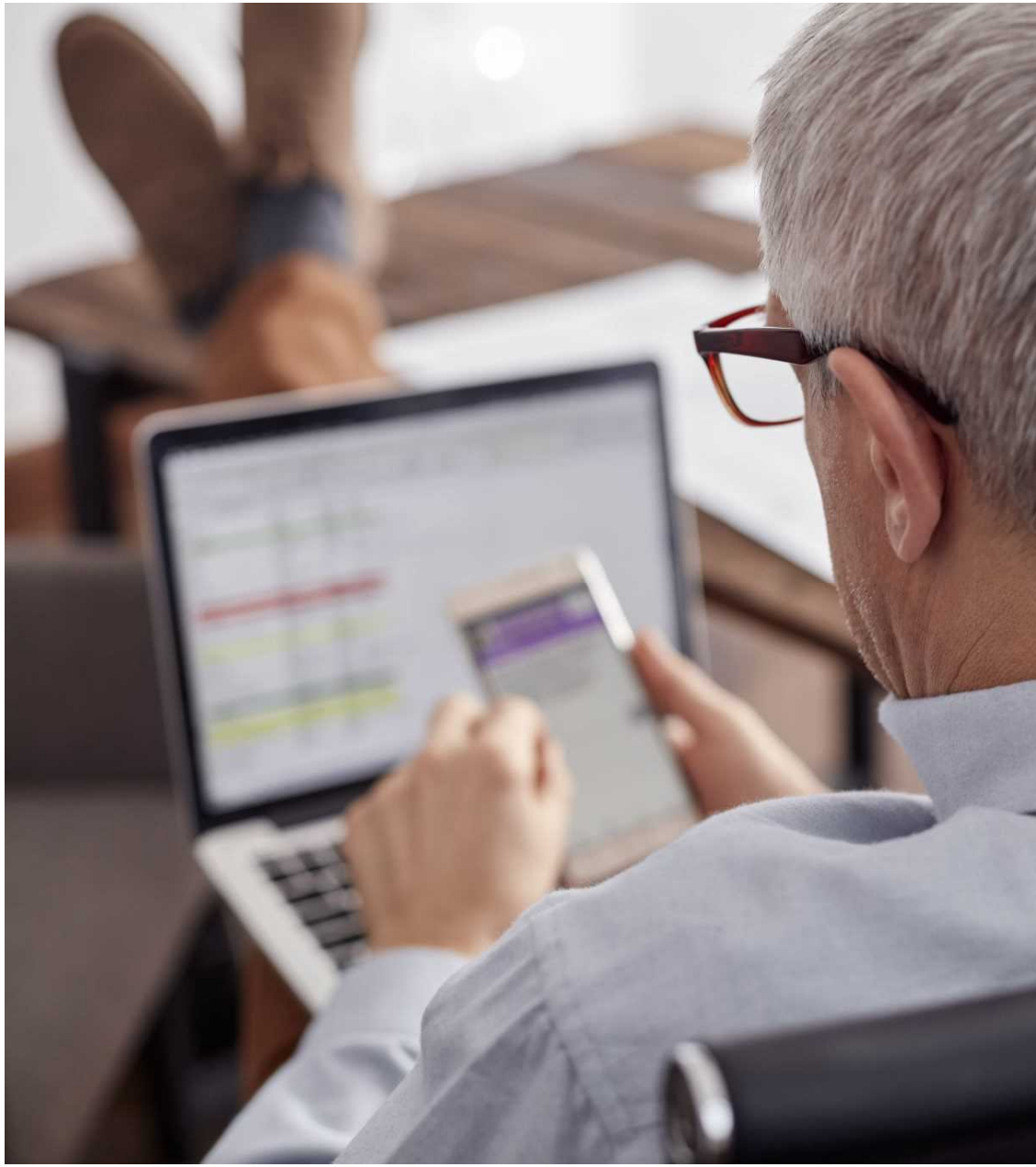
ニューノーマル時代のSecurity Posture
事業継続と説明責任のためのIT基盤の作り方

日本マイクロソフト株式会社
Chief Security Officer
河野省二, CISSP

Microsoft

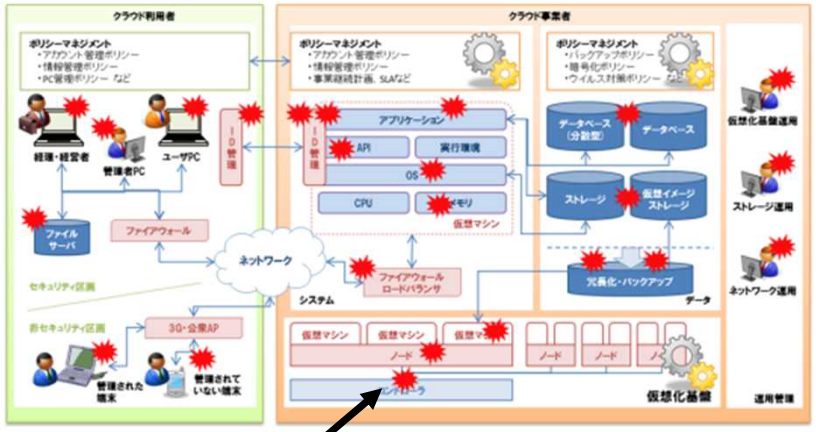
リモートワークのセキュリティとリモートアクセス

ネットワークセキュリティからの脱却



新しい環境のセキュリティはどう考えるか

1 新しい環境の想定モデルを作る



2 それぞれのポイントでの脅威を探す

構造的かつ潜在的な脆弱性、結合による脆弱性、人間の介入による脆弱性などを分析する

3 脅威に対応する脆弱性を低減する

利用者との通信、サーバ間の通信、リージョン間の通信における脅威

- 通信の傍受
- 中間者攻撃
- なりすまし

コンピュータ環境におけるネットワーク上の脅威

- ネットワーク管理の不備によるシステムダウン
- VLAN 構成におけるトラブルによるシステムダウン

流れるデータに応じて通信の暗号化を行うことができるように、SaaS、PaaS などでは 予めウェブサーバやアプリケーションサーバなどにおいて暗号通信を標準化もしくは オプションとして選択できるようにする

http://www.meti.go.jp/policy/netsecurity/downloadfiles/cloudseckatsuyou2013fy.pdf

リモートワークにおけるセキュリティ対策とは

リモートワークで失ったもの・・・ガバナンスの欠如

- 目の前に従業者がいないため、人員の把握や評価が難しい
- リモート環境では、ネットワークルールによるデバイスやデータの制御が難しい
- トラブルが目の前で発生していないため、迅速な対応が難しい

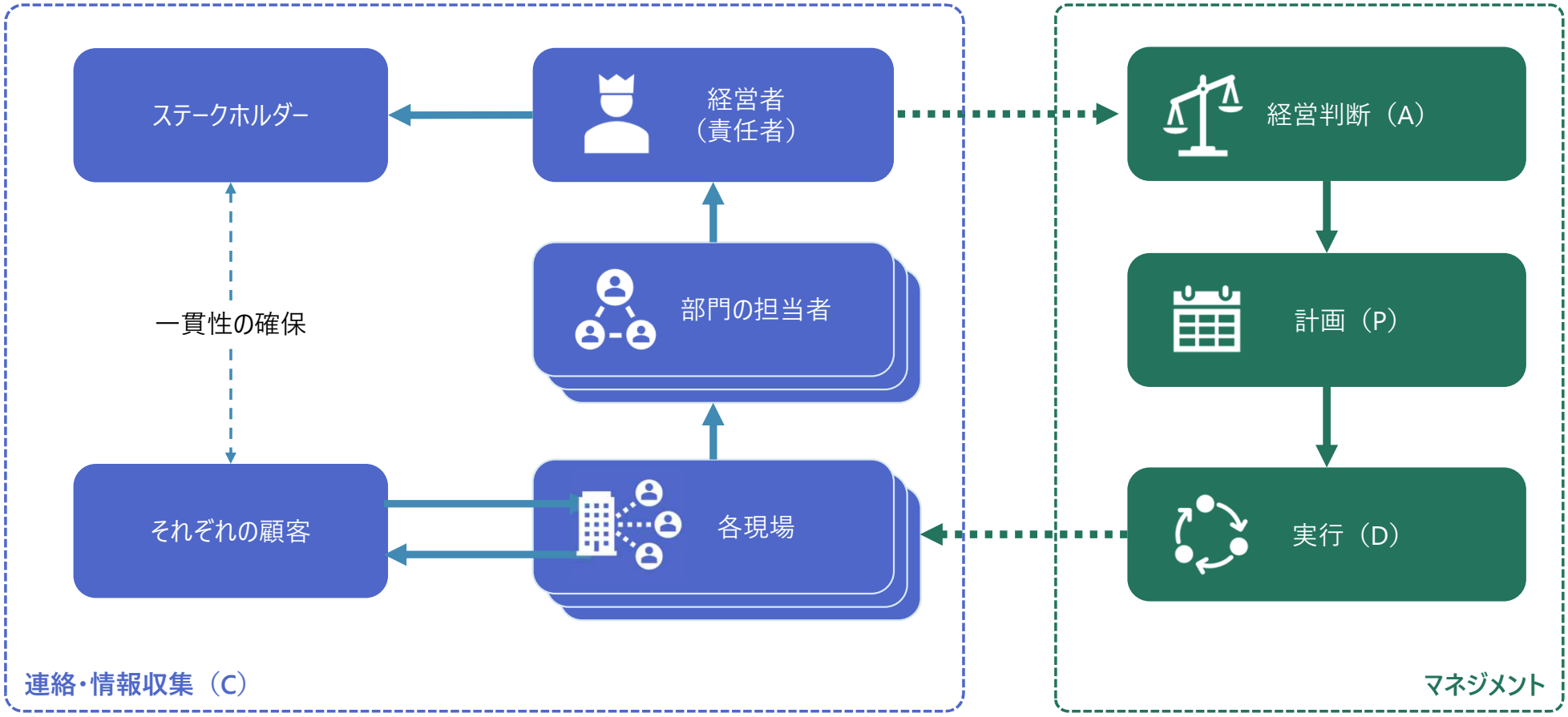
セキュリティの目的と実践

少し本質的なところに戻って考えてみる
のも良いかもしれません

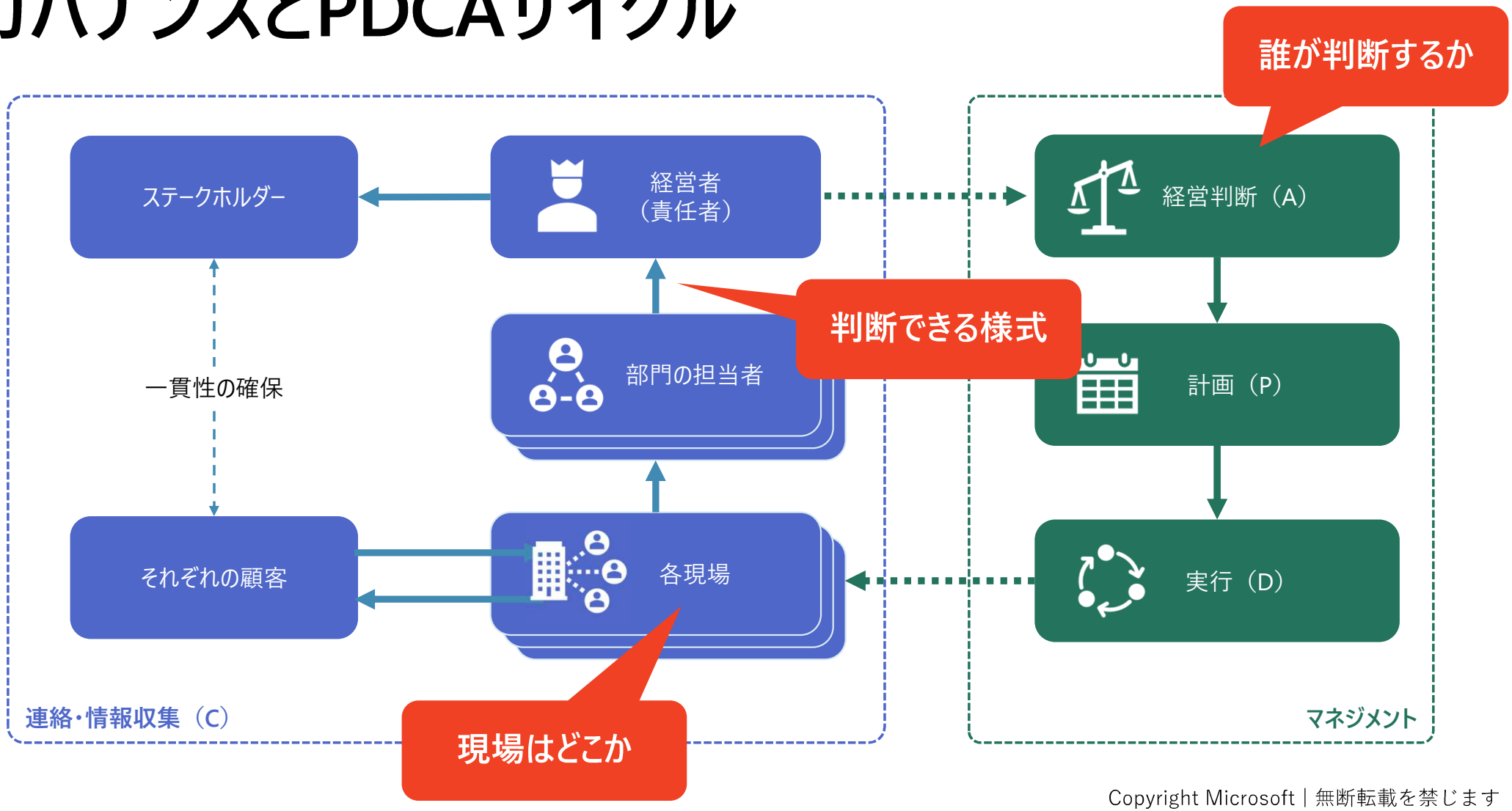
個別のセキュリティ対策ではなく、共通項を探る

説明責任を果たすためには全ての把握が必要、そして事業継続を行っていくためには、リアルタイムに適切な判断が必要。そしてガバナンスの意味の理解が必要になる

ガバナンスとPDCAサイクル



ガバナンスとPDCAサイクル



それぞれのガバナンスについて考える

ITガバナンス

ITが適切な状態にあるかどうかを判断し、問題があれば修正する

- ITの構成やパフォーマンス
- IT責任者の判断
- 業務に関わる基盤全て

データガバナンス

データが適切な状態にあるかどうかを判断し、問題があれば修正する

- データ保護・利用状況
- データオーナー（サブジェクト）
- データが移動する全ての範囲

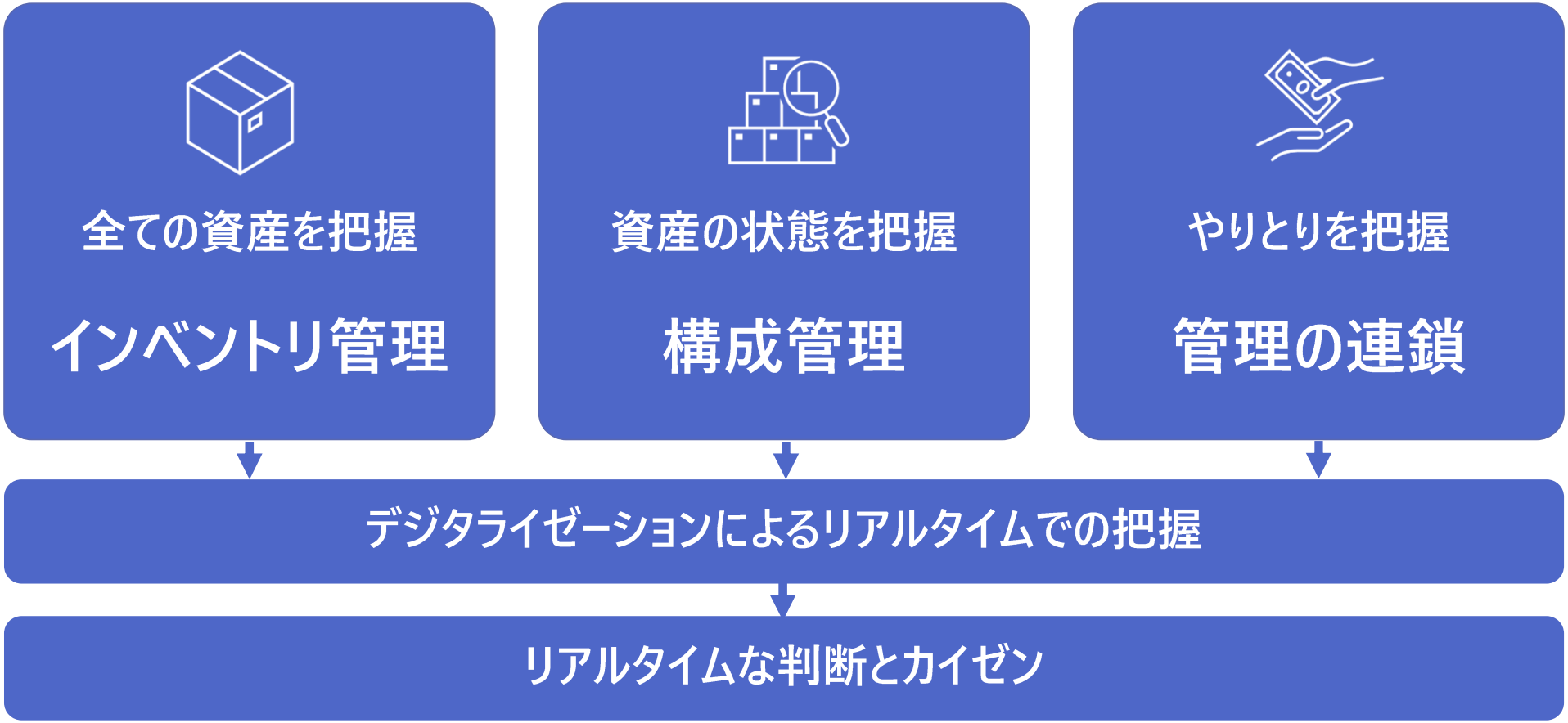
セキュリティガバナンス

セキュリティが適切な状態にあるかどうかを判断し、問題があれば修正する

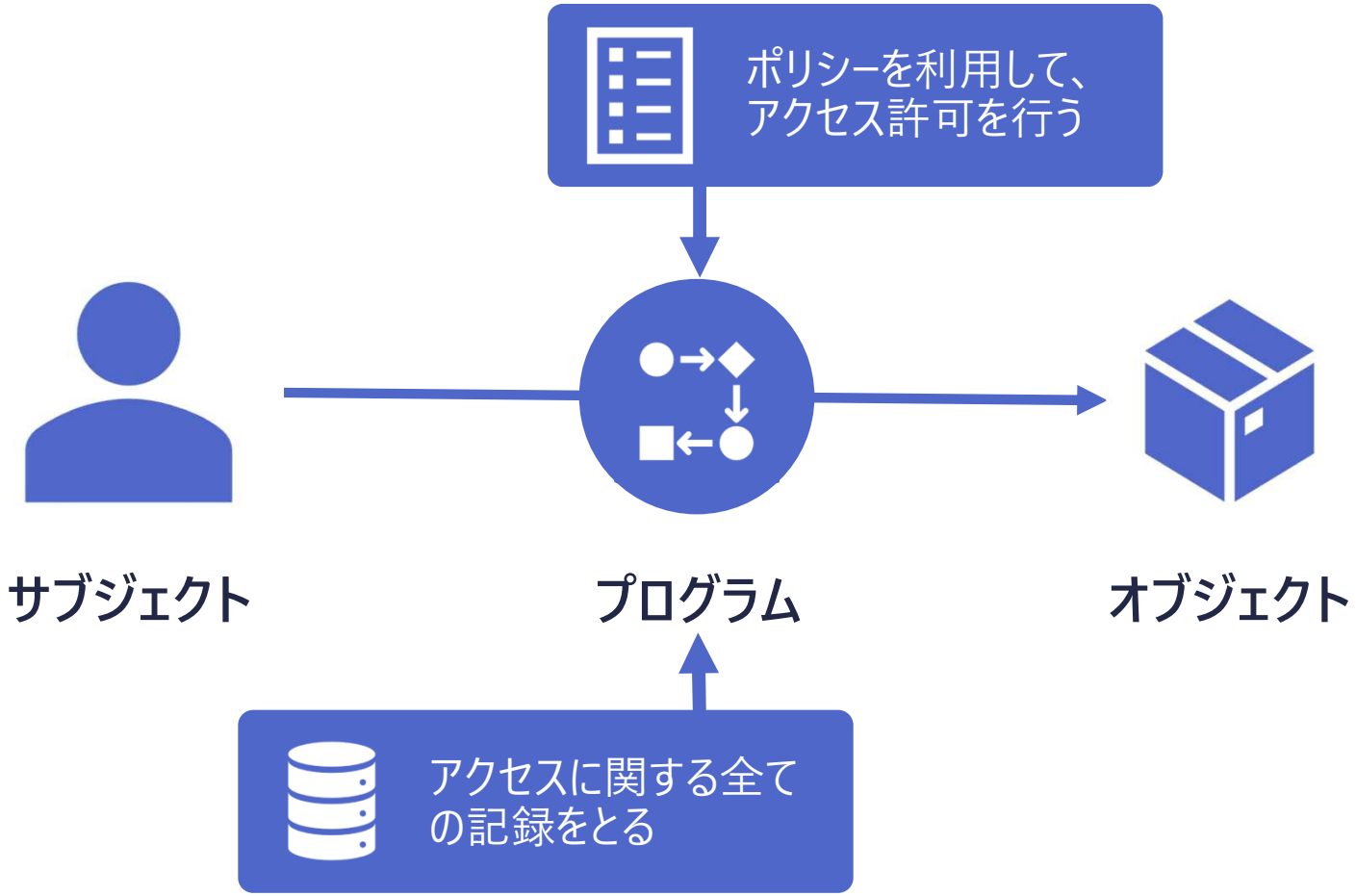
- 脅威・脆弱性・影響
- セキュリティの責任者
- サイバー空間、IT環境全て

どのようなガバナンスにおいても「現場」を正しく把握し、そこからどのように情報を入手するかが重要になる。

現場をすべて把握するための仕組みづくり



やりとりを全て把握するための仕組みづくり



完全仲介を行う場所で取れるデータが変わってくる

ネットワーク

ネットワークを集約して、出口と入り口を一つにすることで、完全仲介の仕組みを構築する

- ファイアウォールの設定
- ネットワーク属性とイベント

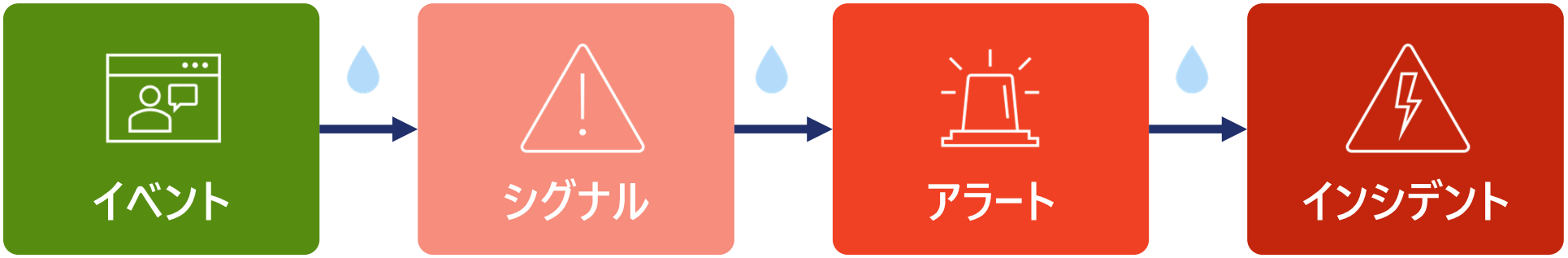
AND / OR

ユーザ・エンティティ

ID管理サービスで、ユーザやエンティティを管理し、全てのアクセスを仲介する

- アクセス制御ポリシー
- ユーザとエンティティの属性とイベント

インシデントをすべて把握するためには



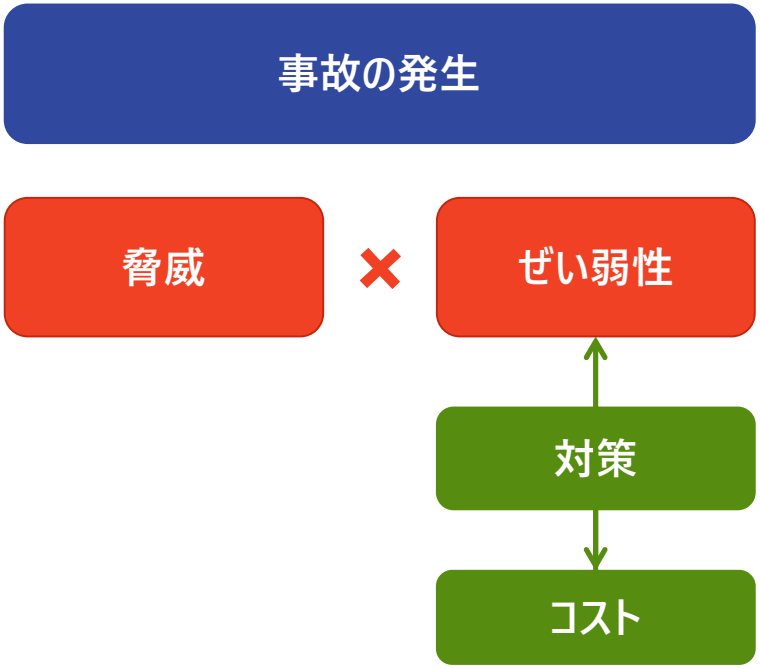
インシデントはイベントログの中の怪しい情報をまとめあげることで、検出される

すべてのインシデントを把握するためには、すべてのイベントを記録しておく必要がある。いわゆるセキュリティログというのは、シグナルやアラートだけをまとめたもので、その有効性を図るためには、イベントログを正確に取得しておく必要がある

セキュリティのバズワード？

サイバーハイジーンとか、ゼロトラスト、
171などの話をここから進めていきます

ぜい弱性管理とサイバーハイジーン

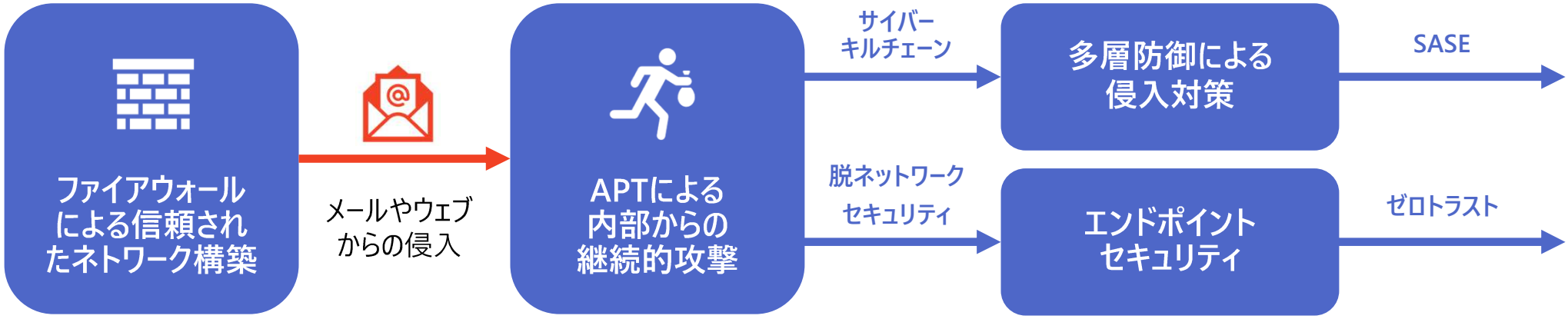


事故が発生するのは脅威とぜい弱性が合致するから

- 脅威は外部にあるためにコントロールすることが難しい（抑止）
- ぜい弱性は内部にあるためにコントロールが可能。ぜい弱性を低減することをセキュリティ対策という（防止）
- セキュリティ対策にはコストが発生するため、費用対効果を考慮する必要がある

脆弱性がない状態もしくは許容できる状態を維持することを「**サイバーハイジーン**」という

APT攻撃による境界型防御の限界



TCP/IP v4を利用するにあたってネットワークのアクセス制御をファイアウォールで行っていた

アプリケーション層からの攻撃はフィルタリングできず、新たなフィルタリングを検討しなくてはならなくなった

ネットワークセキュリティを拡張する形とエンドポイントセキュリティを充実させる形の2つに分かれ、SASEとゼロトラストにつながっている

ゼロ トラスト ネットワークとは何か

ゼロ トラスト ネットワーク

ファイアウォールで守られたローカルネットワーク

信頼できなくなりました・・・

理由その1：ファイアウォールはIPアドレスとポート番号でフィルタリングしている
理由その2：攻撃はウェブやメール経由で行われている
理由その3：VPN経由で内部に侵入することが難しくなくなってきた

信頼できないのはネットワークだけではない

ゼロ トラスト ~~ネットワーク~~

匿名でのインターネット利用は信用できない

理由その1： 攻撃のほとんどがなりすまし
（アカウント、メール、ファイル、アプリのなりすましなど）

理由その2： 脅威の変化により、セキュイリティのベストプラクティスが役に立たない

エンティティの動的な検証と、リスクに応じた動的ポリシーの実践

ゼロ トラストが提唱された背景と解決の方向性

複雑なIT環境

- ネットワークに依存しない環境からのITサービス利用
- 複数組織による資産の共有による組織を超えた信頼性の確保

ITガバナンスの再構築

- 個々の環境の適切な把握
- 境界型防御における残存リスクの把握
- 組織を超えた信頼性を確保するための資産管理基盤

画一的なセキュリティ対策の限界

- エンティティの増加に伴う攻撃対象の増加
- 環境に応じたセキュリティ対策が求められている

リスクに応じて変化できる対策

- リスクの継続的な分析と評価
- リスクが最小限に抑えられた環境を維持するための継続的な認証と承認

NIST SP800-207におけるゼロ トラストの基本原則

1. 全てのデータソースとコンンピュータサービスはリソースとみなされる
2. 場所に関係なく全ての通信が保護される
3. 個々のリソースへのアクセスはセッションごとに設定される
4. リソースへのアクセスはモニタリング可能な属性を利用した動的ポリシーによって決定される
5. 完全性とセキュリティの状態管理のために、全ての資産をモニタリングする
6. 全てのリソースの認証は事前に厳密に行われ、動的な認可が与えられる
7. ネットワークにおいても同様に多くの情報を収集し、セキュリティの状態を改善する

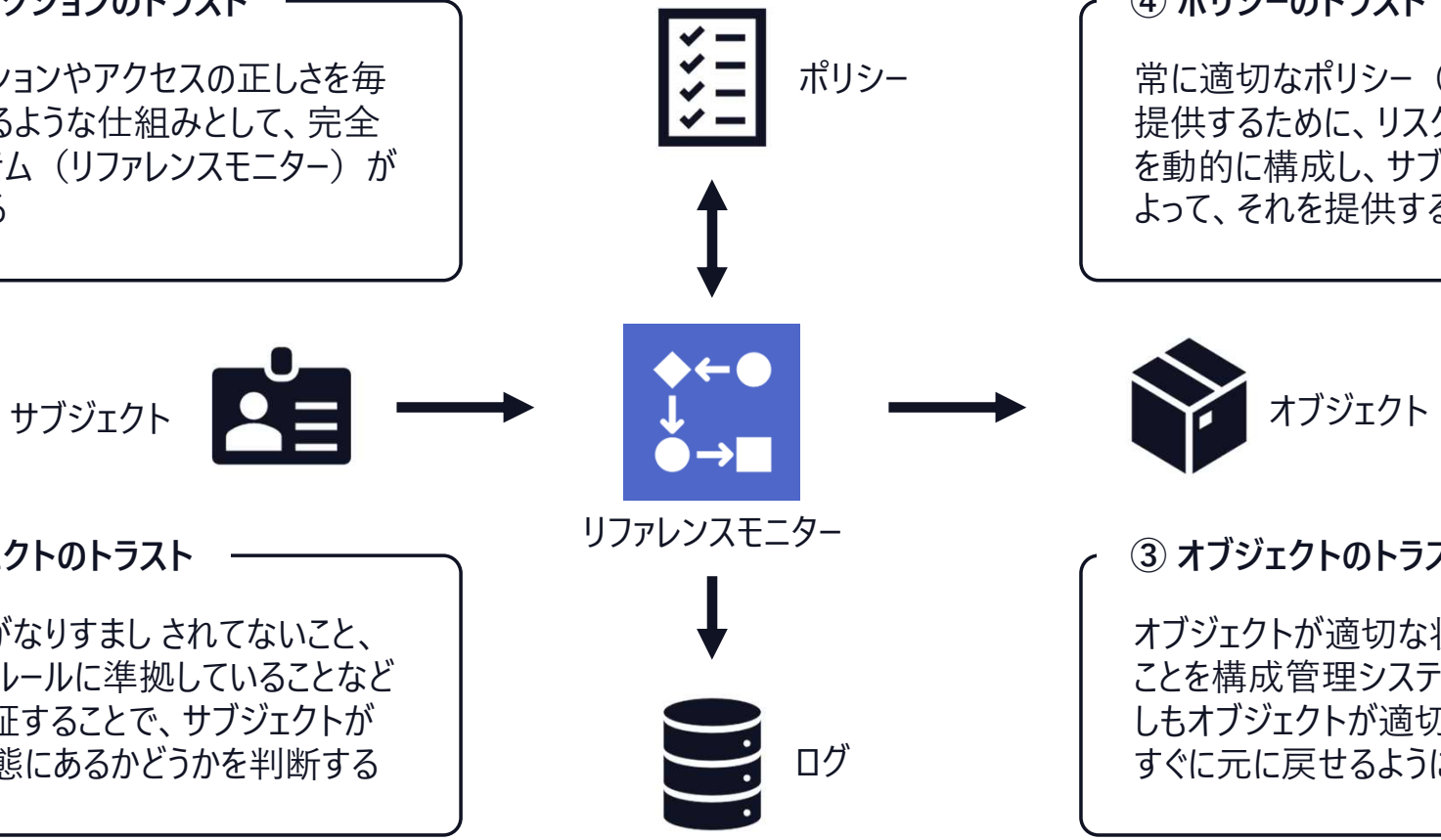
ゼロトラストの実践のために

① トランザクションのトラスト

トランザクションやアクセスの正しさを毎回検証するような仕組みとして、完全仲介システム（リファレンスモニター）が必要になる

② サブジェクトのトラスト

アカウントがなりすまし されてないこと、デバイスがルールに準拠していることなどを毎回検証することで、サブジェクトが適切な状態にあるかどうかを判断する



④ ポリシーのトラスト

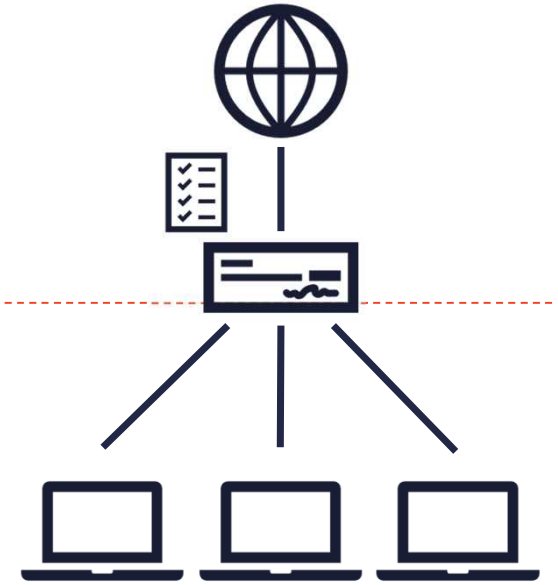
常に適切なポリシー（判断基準）を提供するために、リスクに応じてポリシーを動的に構成し、サブジェクトの属性によって、それを提供する

③ オブジェクトのトラスト

オブジェクトが適切な状態になっていることを構成管理システムで判断する。もしもオブジェクトが適切でない場合にはすぐに元に戻せるようにしておく

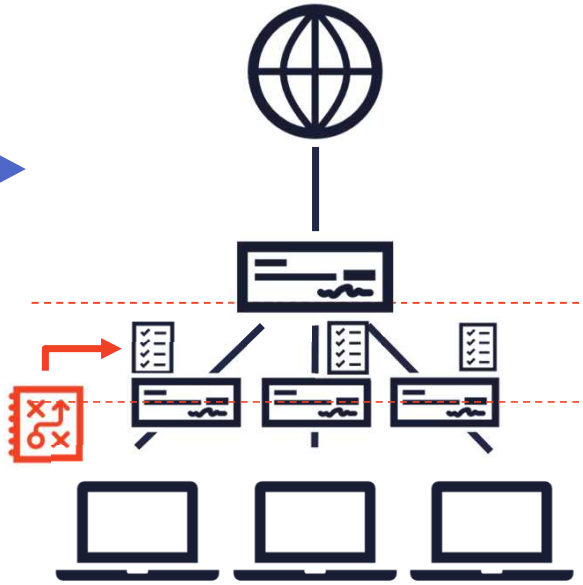
ローカルブレイクアウト - マイクロセグメンテーションの効率化

典型的な境界型防御



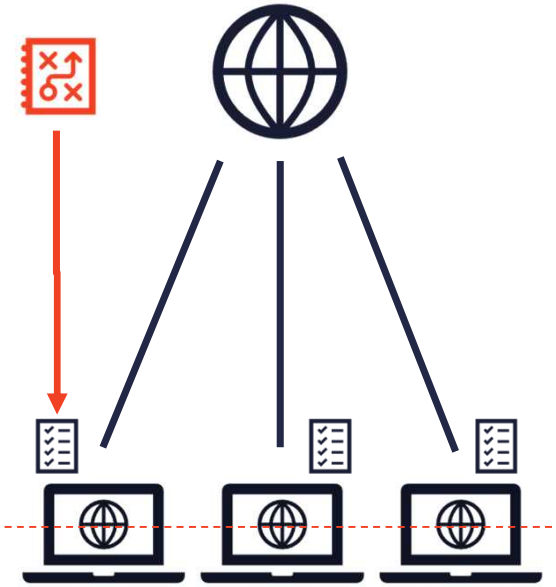
ファイアウォールによって配下のPCやサーバは共通のセキュリティポリシーが適用される。結果として、一番厳しいポリシーが全てに適用されるか、全てが甘くなる。

マイクロセグメンテーション



個別のポリシーを適用するために端末単位にファイアウォールを設置。ポリシーマネージャから個別のポリシーを配信。SDNを使ってさらに効率化をした

ローカルブレイクアウト



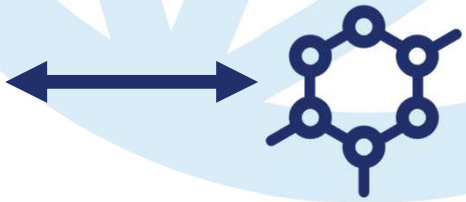
端末の中にファイアウォールが導入されたことで、直接インターネットに接続しても問題のない状態を作り、さらに効率化ができるようになった

ピュア ゼロ トラストの実現

ゲートウェイタイプのセキュリティソリューションからの脱却

ネットワーク上のセキュリティサービスは
全て端末に持ってくることができるようになった

脅威インテリジェンスによる
リアルタイム保護



ビルトインセキュリティ機能

- ファイアウォール
- URLフィルター
- CASB　など

セキュアOSによる完全仲介

- UEBA - ふるまい分析
- 動的ポリシー制御
- サンドボックス　など

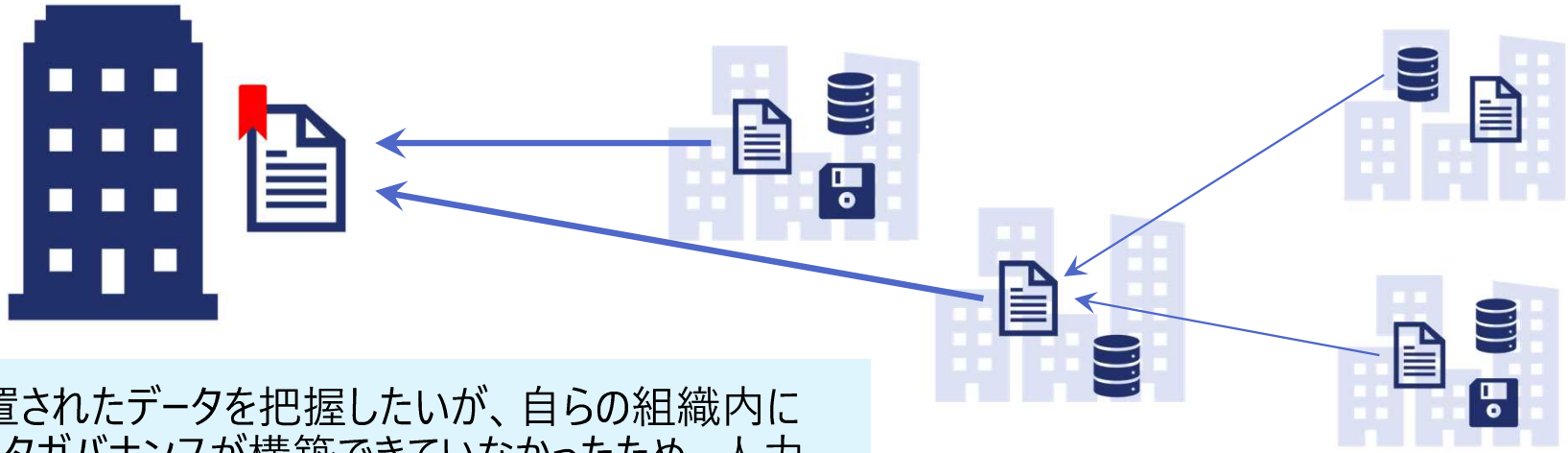
米政府におけるデータガバナンス – NIST SP800-171

Unclassified information (CUI) in nonfederal information systems

政府の機密情報

政府機密分類ではないが、関連する情報

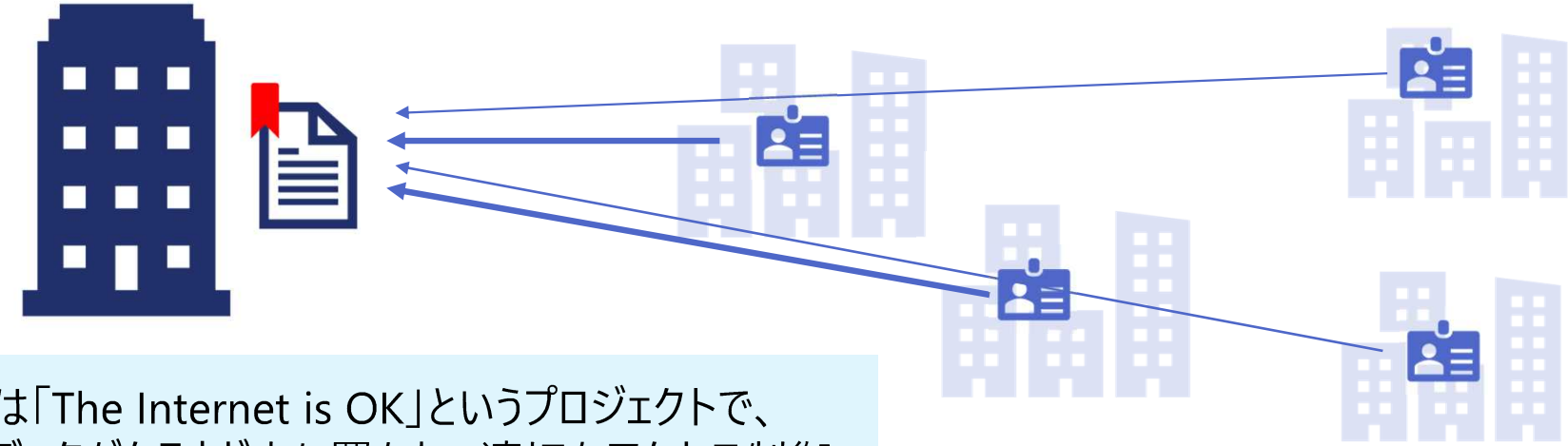
連邦政府の情報システム外に存在する



バラバラに配置されたデータを把握したいが、自らの組織内にないため、データガバナンスが構築できていなかったため、人力で把握せざるをえない状況

データガバナンスのこれからの方向性

データの利用範囲を明確にし、アクセス権を設定することで、データオーナーがいつでもデータのを把握し、適切な管理ができるようになっている



英国政府では「The Internet is OK」というプロジェクトで、70%以上のデータがクラウド上に置かれ、適切なアクセス制御により、データガバナンスが実現している

セキュリティの計画を立てる

これからのセキュリティ対策を計画するために、どのように方針を設定するか

Security Posture – セキュリティの状態管理

脆弱性のない環境を作る

デジタルガバナンス

全ての資産の状態をリアルタイムに把握し、アクセス権を維持する

サイバーハイジーン

脆弱性のない状態を維持し、異常を検知したらすぐに修正する

IDベースのゼロ トラスト

インシデント対応の軽量化

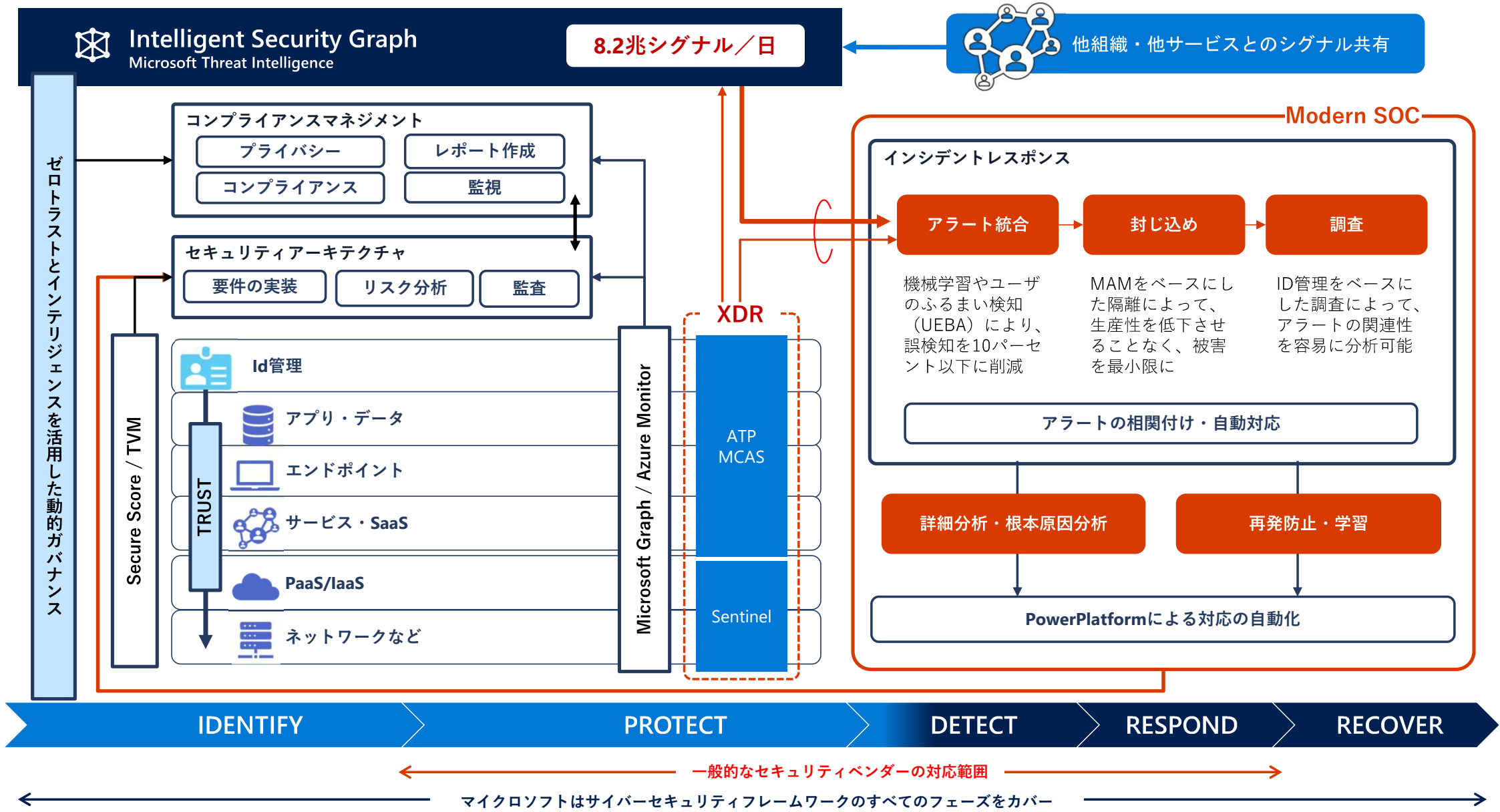
脅威インテリジェンス

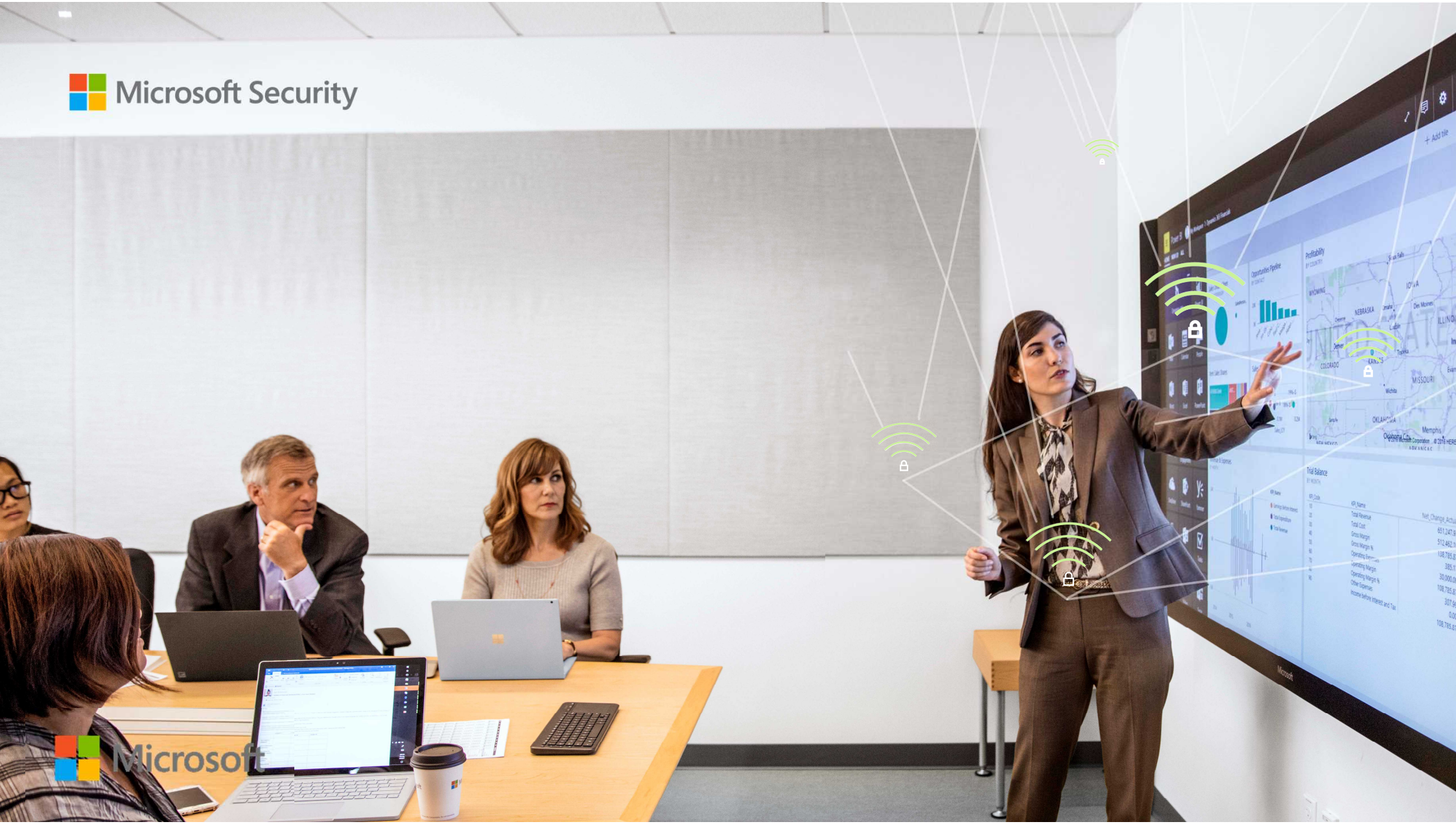
世の中の脅威を把握し、予兆管理、事前対応を行う

対応の自動化

自動化された対応の共有により、専門家の知見を生かす

Modern SOC


Intelligent Security Graph
Microsoft Threat Intelligence
8.2兆シグナル／日
他組織・他サービスとのシグナル共有
ゼロトラストとインテリジェンスを活用した動的ガバナンス
コンプライアンスマネジメント
プライバシー
レポート作成
コンプライアンス
監視
セキュリティアーキテクチャ
要件の実装
リスク分析
監査
Secure Score / TVM
TRUST
Id管理
アプリ・データ
エンドポイント
サービス・SaaS
PaaS/IaaS
ネットワークなど
Microsoft Graph / Azure Monitor
XDR
ATP
MCAS
Sentinel
Modern SOC
インシデントレスポンス
アラート統合
封じ込め
調査
機械学習やユーザのふるまい検知（UEBA）により、誤検知を10パーセント以下に削減
MAMをベースにした隔離によって、生産性を低下させることなく、被害を最小限に
ID管理をベースにした調査によって、アラートの関連性を容易に分析可能
アラートの相関付け・自動対応
詳細分析・根本原因分析
再発防止・学習
PowerPlatformによる対応の自動化
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER
一般的なセキュリティベンダーの対応範囲
マイクロソフトはサイバーセキュリティフレームワークのすべてのフェーズをカバー


Microsoft Security
Microsoft