

ゼロトラストのその次へ

- サイバーハイジーンのためのマルチクラウド基盤の考え方

日本マイクロソフト株式会社

Chief Security Officer

河野省二, CISSP





ゼロトラストの整理を簡単に・・・

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

さまざまなゼロトラスト

ゼロトラスト
ネットワーク

境界防御の限界

ゼロトラスト

静的アクセス制御の限界

ゼロトラスト
アーキテクチャ

リアルタイムガバナンス

IT部門やセキュリティ部門の都合の良い解釈で遠回りした数年間・・・

ゼロトラストの目的はガバナンスとサイバーハイジーン

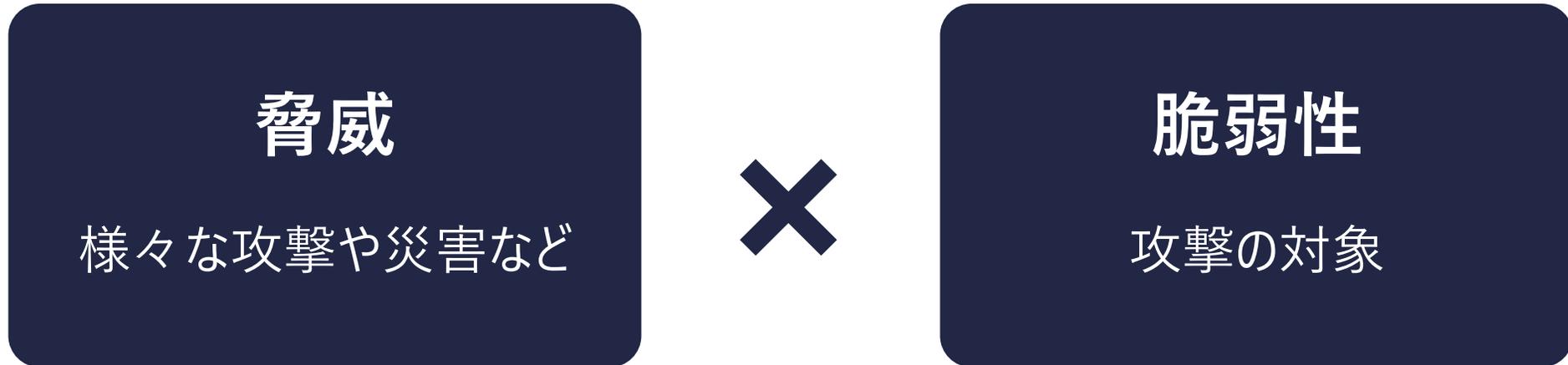


サプライチェーン全体でこれらの対策を実施することで、攻撃に強い社会を作ることができる



どんな攻撃があっても事故が起きないようにするには

事故が起きるのは「脆弱性」があるから



攻撃が増加しても、巧妙になっても、攻撃の対象となる「脆弱性」がなければ、攻撃は成功しない

事故が起きるのは「脆弱性」があるから

安全の証明 = 脆弱性がないことの証明

攻撃が増加しても、巧妙になっても、攻撃の対象となる「脆弱性」がなければ、攻撃は成功しない

脆弱性を許容できる範囲に維持する



攻撃が増加しても、巧妙になっても、攻撃の対象となる「脆弱性」がなければ、攻撃は成功しない



脆弱性対策アプローチを一元化するために

ソフトウェアの脆弱性管理

Common Vulnerabilities and Exposures (CVE)

脆弱性

放置されている

ソフトウェアに脆弱性が見つかったら、修正プログラムを適用する。修正プログラムができていない、もしくはパッチが充てられていない状況を確認するためにCVEがある。マルウェア対策などには有効だが、攻撃全体を見ることは難しい

クラウドサービスの脆弱性管理

Cloud Security Posture Management (CSPM)

セキュリティ対策の状態

クラウドサービスは修正プログラムをユーザ側で適用する必要がないため、CVEのような概念は必要ない。その代わりに、セキュリティ対策が期待通りになっているかを確認することで、脆弱性管理を行う。マルチクラウドにおけるセキュリティに課題がある

侵入に対する脆弱性管理

Attack Surface Reduction (Management)

攻撃が成功するポイント

ネットワークセキュリティや多層防御においては攻撃されるポイントを明確にし、それらを削減していくことで脆弱性のない環境を構築したいと考えていた。Surfaceといいながらも、その考え方はPoint的なものが多い

サービスレベルの脆弱性管理

多層防御 + サイバーキルチェーン

対策の単位を定義

単体のソフトウェア対策では十分ではないことから、レイヤーセキュリティを前提としたセグメントを定義し、それぞれのセキュリティ対策を計画。レイヤー間の関連性については十分に対応できなかった



ここまでやってるのに事故が起きてるのはなぜか

ゼロトラストによるセキュリティ対策の統合アプローチ

ゼロトラスト アーキテクチャー

常に信頼できる状態

これまでバラバラだった様々な管理をまとめ、常に信頼できる状態を維持していくことを目的に、脆弱性管理の関連性を明確にした。しかし、境界防御の代替手段として捉えられることによって、本質的なアプローチができないことが多かった



ゼロトラストと多層防御は相性が悪い

真のサイバーハイジーンを実現するためのアプローチ



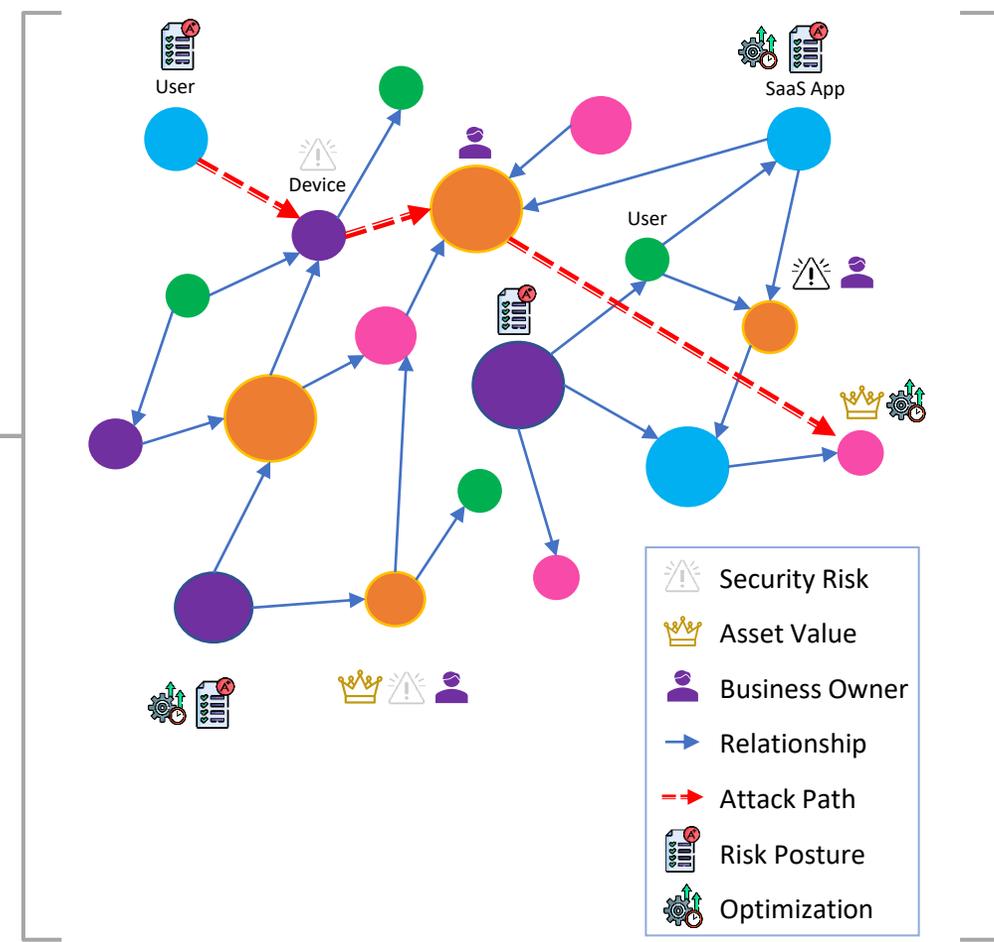
組織における包括的な弱点の把握と攻撃の予兆管理 = Exposure management

Exposure Managementによるサイバーハイジーン

- CMDB
- servicenow
- Vulnerability Management
- tenable.io
- Email Security
- proofpoint AVANAN
- Identity Security
- okta CROWSTRIKE
- Endpoint Security
- CROWSTRIKE
- SaaS Security
- OBSIDIAN ADAPTIVE SHIELD
- Application Security
- snyk Checkmarx
- Cloud Security
- palocalto WIZ
- External Attack Surface
- palocalto CYCOGNITO
- Threat Intelligence
- Recorded Future

- アセットメタデータ
- 運用状況
- 構成データ
- ポリシー
- セキュリティ調査
- サービス状態

エンティティ把握の解像度を向上
整理、正規化、集約、重複排除、コンテキスト



攻撃パス分析

従来のサイロ化されたアプローチからの脱却、攻撃者の視点を考慮して脆弱性対策の優先順位を決定

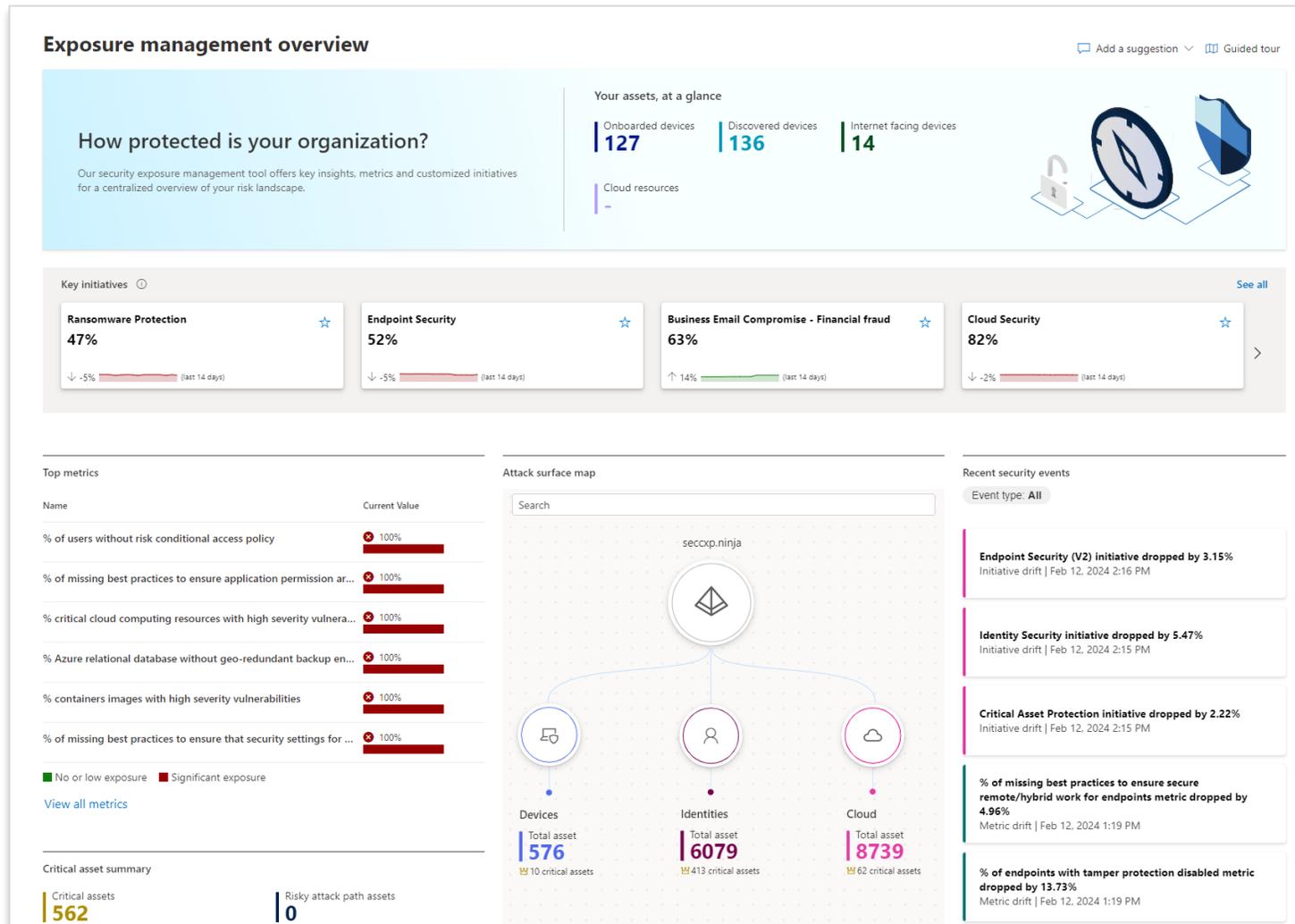
Attack Surface管理

組織の資産を継続的に判別、コンテキストを整理、管理し、攻撃者の視点を提供

一元管理

セキュリティ状況を把握し、既成概念にとられない洞察力で担当者からの問いに積極的に対応

Exposure Managementによる弱点の一元管理



個別のセキュリティ管理の関連づけによる新たな発見と対応

- 脆弱性管理
- Attack Surface管理
- クラウドサービスセキュリティ
- エンドポイントセキュリティ
- アイデンティティセキュリティ
- CASB
- 電子メールセキュリティ
- OT/IoTセキュリティ
- 資産管理
- 構成管理

マルチクラウド・オンプレミス統合管理



マルチクラウドポスチャ-管理

ISOやNISTなどの標準対応状況

規制・コンプライアンス管理

Microsoft Azure (プレビュー) リソース、サービス、ドキュメントの検索 (G+/) Copilot

ホーム > Microsoft Defender for Cloud

Microsoft Defender for Cloud | 規制コンプライアンス

11 サブスクリプションを表示しています

検索 レポートのダウンロード コンプライアンス標準の管理 クエリを開く 経時的なコンプライアンス プ

全般

クラウド セキュリティ

- セキュリティ態勢
- 規制コンプライアンス**
- ワークロード保護
- データのセキュリティ
- Firewall Manager
- DevOps セキュリティ

管理

Microsoft cloud security benchmark Australian Government ISM PROTECTED

Microsoft cloud security bench
Australian Government ISM PR
AWS Brazilian General Person
AWS California Consumer Priv
AWS CRI Profile v1.2.1 (Previe
AWS CSA Cloud Controls Matri
AWS CSPM (Preview)
AWS Foundational Security Be
Azure CSPM (Preview)
Canada Federal PBMM
CIS Amazon Elastic Kuberne:
CIS Azure Foundations v1.1.0
CIS Azure Foundations v1.3.0
CIS Azure Foundations v1.4.0

Microsoft Defender for Cloud からの推奨事項 - 規制コンプライア
び検証するのはお客様の責任です。これらのサービスには、**ライセンス条項**
Microsoft cloud security benchmark は 6 個のサブスクリプションに

すべてのコンプライアンス コントロールを展開する

- NS. ネットワーク セキュリティ
- IM. ID 管理
- PA. 特権アクセス
- DP. データ保護
- AM. 資産管理
- LT. ログ記録と脅威検出
- IR. インシデント対応

各国・業界の規制を分析

Microsoft Cloud Security
Benchmark

それぞれの規制に再マッピング

各サービスでのリアルタイム監査

必要に応じて修正

セキュリティ対策の一元化によるガバナンス

Exposure
Management



XSPM

予防的対策による
サイバーハイジーンの実現

Threat
Management



XDR + SIEM

インシデント対応の自動化と
深い洞察の実現

SIEMとかUEBAとか・・・ではない基盤構築

SIEM

セキュリティログから
何がわかるの？

侵入検知主体の記録

XDR

複数のサービスの
セキュリティ基準をどうする？

いつもと違う状態の記録

UEBA

行動を管理するための
基準は？

アクセス管理の記録

ゼロトラストの目的 = サイバーハイジーン（脆弱性のない状態）

グラフデータベースによるリアルタイムガバナンス、マイクロサービスによるレジリエンス

