# シスコセキュリティ 取り組みと今後の戦略

シスコシステムズ合同会社
セキュリティ事業開発　冲中恒雄

2024/9/19

# セキュリティベンダーとしてのシスコ

セキュリティは

## シスコの最重要戦略


AIとSecurityに徹底的にフォーカス

シスコセキュリティ事業の概況

- 2023年度シスコセキュリティ事業規模 **約6,000億円**
- 過去4年間セキュリティ領域に **約9,000億円投資**
- 民間のセキュリティ研究機関で**世界最大規模** **Cisco Talos**を保有し、**約500名**の分析官が所属、**毎日5,500億件**のセキュリティイベントを観測
- 1995年からセキュリティ関連企業を**37社**買収
  →業界屈指の広範囲なセキュリティーポートフォリオを保有
- Cisco Talosのメンバーを中心とした**約600名**の従業員がウクライナを支援

# シスコセキュリティを支える強力データベース

## TALOS:世界最大規模のセキュリティインテリジェンス&リサーチチーム


**200億**
1日の脅威ブロック数

TALOS

**200以上のゼロデイ脆弱性**
1年間の検出数（全く新しい脅威）

### 圧倒的なデータ量

**6000億**
1日あたりの電子メールメッセージ数

**280万**
1日あたりのマルウェアのサンプル

**160億**
1日に監視されるWebリクエスト

**5500億**
1日あたりの観測されるセキュリティイベント

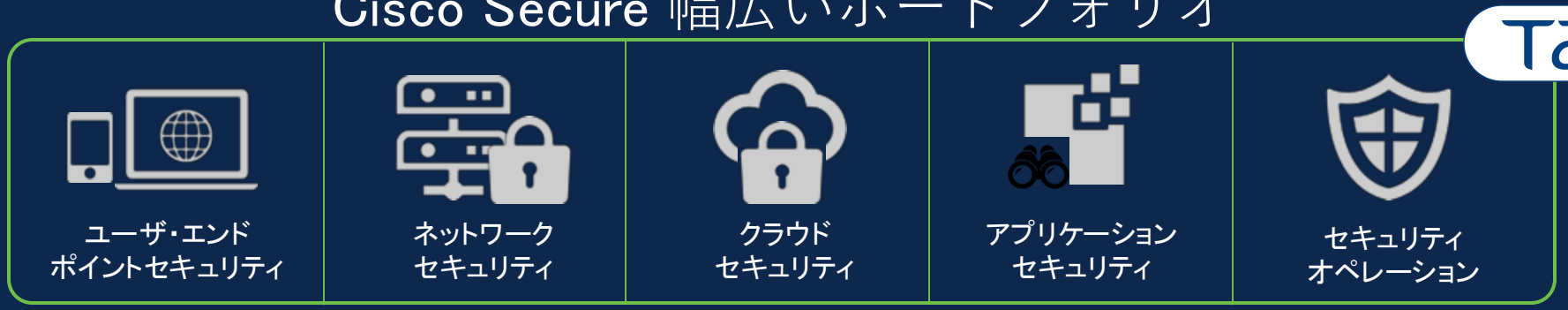
### 世界最大規模の組織

**500人以上**
フルタイムの脅威インテリジェンス担当者

**100社以上**
脅威インテリジェンスパートナー

# シスコセキュリティのソリューション ラインアップ

## Cisco Secure 幅広いポートフォリオ




### ユーザ・エンドポイント セキュリティ

- Cisco Secure Client (AnyConnect VPN/ポスチャ/ 通信可視化EPP/EDR)
- Cisco Security Connector (iOS 端末保護)
- Duo (MFA/SSO/ZTNA)
- Oort (ITDR)

### ネットワーク セキュリティ

- Secure Firewall & IPS
- Secure Email
- ISE (統合認証サーバ)
- Secure Network Analytics (NDR)
- Meraki MX (UTM)
- クラウド型DDoS対策 & WAF
- Cyber Vision (OTセキュリティ)

### クラウド セキュリティ

- Umbrella (クラウドプロキシ)
- Secure Access (SSE)
- Cisco Secure Connect (SASE)
- Secure Cloud Insights (CSPM/CAASM)
- Multi Cloud Defense (ex.Valtix)

### アプリケーション セキュリティ

- Secure Application (RASP)
- Secure Workload (ex.Tetration)
- Panoptica (Container Security)

### セキュリティ オペレーション

- Talos (脅威インテリジェンス)
- Cisco Secure XDR (XDR)
- CVM（リスクベース脆弱性管理）
- Managed SIEM Service（運用支援サービス）
- その他、セキュリティ アドバイザリー サービス等の支援サービス

# シスコセキュリティ事業 最近の取り組み

## シスコはセキュリティ / AI にフォーカス

セキュリティは
**シスコの最重要戦略**


- FY24 Q3 セキュリティ売り上げ昨対比36%成長
- 1995年からセキュリティ関連企業を37社買収し、業界で最も広範囲なセキュリティポートフォリオを保有
- 23年買収＋買収意向表明**12社中7社がセキュリティ**関連

## 世界最大規模のセキュリティ研究機関： Cisco Talos

- 世界最大規模の民間セキュリティ研究機関であるCisco Talosを保有し、約500名の分析官が所属
- 毎日4,000億件のセキュリティイベントを観測
- RSA Conference 2024でのSOCを担当
- Paris 2024にてOfficial Cyber Security Infrastructure Partner
- Cisco Security AIを強化開発中

## 日本でのサイバーセキュリティ事業を強化


2024年6月21日

コーポレート
シスコ、日本のナショナルセキュリティとデジタルレジリエンスの強化に向けCoEを開設

Press Release

Japanese | English

シスコ、日本のナショナルセキュリティとデジタルレジリエンスの強化に向け
サイバーセキュリティ センター オブ エクセレンス(CoE)を開設

概要

- サイバーセキュリティ センター オブ エクセレンス (CoE)を東京に開設し、ナショナル サイバーセキュリティ アドバイザーの任命、日本における Cisco Talosインテリジェンス チームの展開、そして、日本のサイバーセキュリティ人材の育成を推進します。
- 同センターでは、加速するデジタル化やサイバーセキュリティの脅威の増大による課題に企業や組織が対処できるよう支援し、日本全国でデジタルレジリエンスの強化を目指します。
- シスコネットワーキングアカデミー プログラムの実績に基づき、今後 5 年間で新たに 10 万人の IT およびサイバーセキュリティの学習者に研修を提供する意欲的な目標を設定しました。

シスコシステムズ合同会社（本社：東京都港区、代表執行役員社長：濱田 義之、以下 シスコ）は本日、日本のサイバーセキュリティおよびデジタルレジリエンスの強化に取り組む シスコ サイバーセキュリティ センター オブ エクセレンス (CoE) を東京に開設することを発表しました。同センターはサイバーセキュリティポリシーの策定、脅威インテリジェンスの連携強化、サイバーセキュリティ領域の優れた人材の育成に向けた研修の拡充といった重要な役割を担います

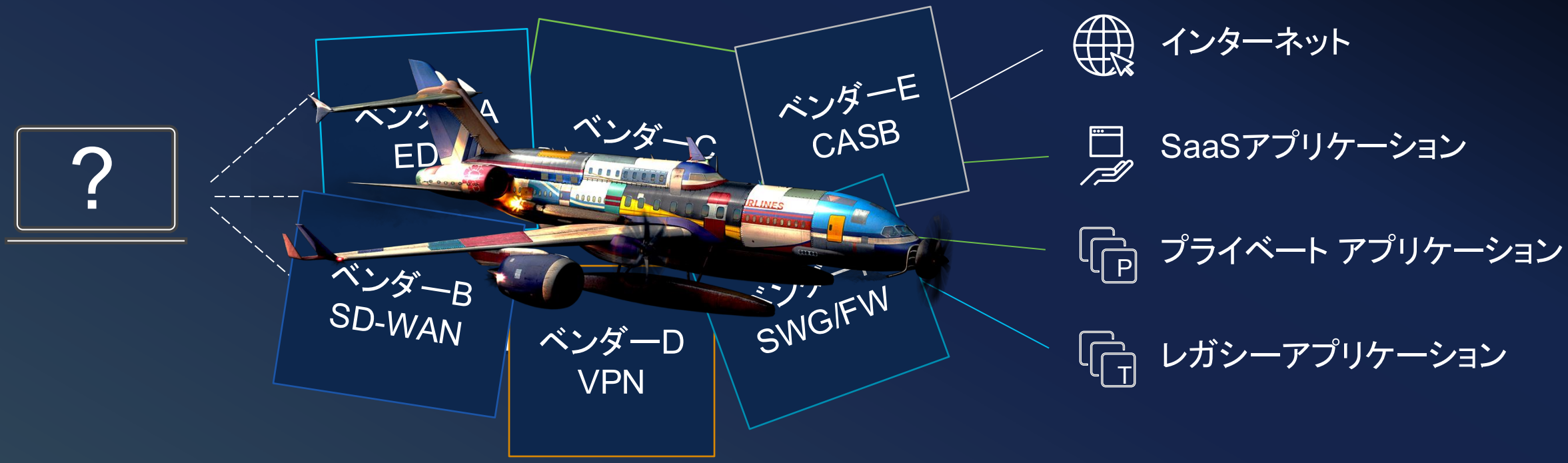
- 都内に「サイバーセキュリティ・センター・オブ・エクセレンス（CoE）」を設置
- Cisco Talosを日本に常駐
- ナショナル・サイバーセキュリティ・アドバイザリーを任命
- 今後5年間で10万人のIT及びサイバーセキュリティ学習者に研修を提供

## 24年3月Splunkの買収完了・連携開始

- Cisco Talosの脅威インテリジェンスをSplunk ESに組み込み
- Cisco XDRとSplunk ESを連携
- **オブザーバビリティの強化による可視性の向上**
- **ネットワークインフラストラクチャ再構築**
- **AIを活用**：セキュリティ、IT運用、エンジニアリングチームの効果と効率の向上

# セキュリティをとりまく現状の課題

異なるコンソールを使用して、異なる種類のポリシーを複数の場所で管理




**ネットワーク**と**セキュリティ**を**一体で考える**重要性が高まっている

シスコはグローバルで安全・快適・シンプルな

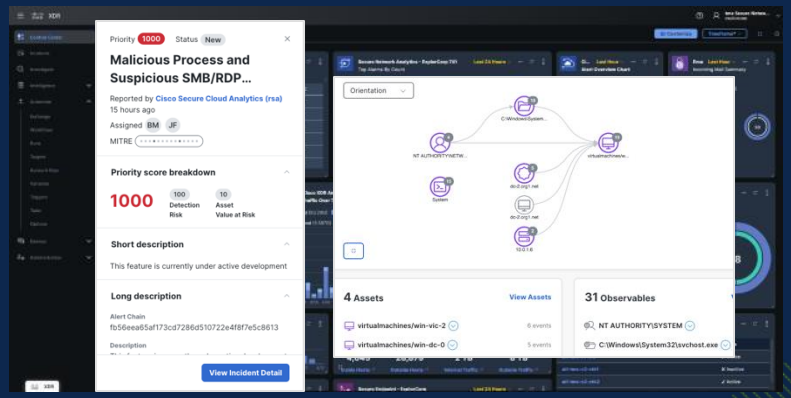
セキュリティプラットフォームを提供します

# リアルタイム脅威検知対処：早期の検知・対処を実現するXDR

テレメトリーやログ情報の収集

- ネットワーク認証
- PaaS/IaaS
- メール
- 総合認証基盤
- FW
- SIEM
- エンドポイント
- 拠点ネットワーク

## Cisco XDR



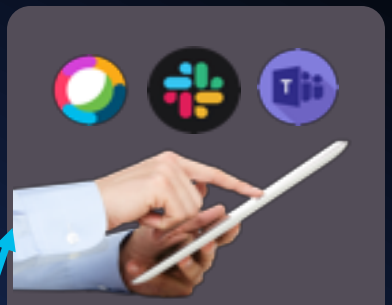

相関関係を分析

インシデントの優先付け

対処のワークフロー

### マルチベンダー環境をサポート

CROWDSTRIKE / paloalto NETWORKS / COHESITY / Microsoft / TREND MICRO / aws / SentinelOne / cybereason / Google Cloud



チームへの通知

自動での隔離

ネットワーク

自動での隔離

ユーザ・デバイス


The bridge to possible