Cisco Secure Networking：
セキュアなキャンパスネットワーク

シスコシステムズ合同会社
エンタープライズネットワーキング事業
セールススペシャリスト

渡部 周一

Power of the Platform

ネットワークのプラットフォームが一貫したユーザー体験と
自動化、インテリジェンス、API 主導のエコシステムを適用して
実現するもの

シンプルな運用

Secure Networking

ハイブリッドワークと
サステナビリティ

現在の世界はハイブリッド

空港

自家用車や交通機関

ブランチ

会社

自宅

どこからでも接続可能

ユーザー、デバイス、モノ

＝ハイブリッド＝

アプリケーション

どこにでも展開可能

データセンター

プライベートクラウド

aws

Microsoft Azure

Google Cloud

コンテナ

ハイブリッドな世界が今日のビジネスを変革

ハイブリッド環境の実現に向け、直面する課題

インターネットアクセスに 100% 移行した企業は皆無

企業にはエンタープライズ LAN、LAN、WAN で接続された物理的な拠点が存在

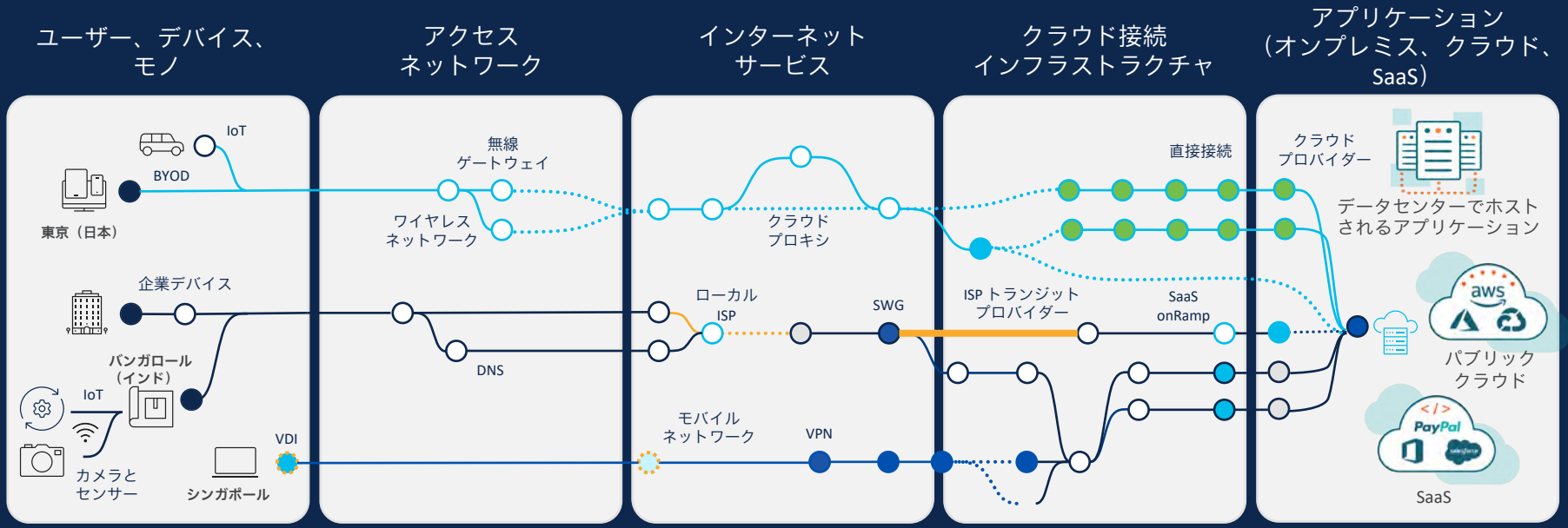
企業には SaaS、パブリッククラウド、プライベートクラウドの各アプリケーションが混在

データセンターは引き続き社内アプリケーションの提供にとって重要

企業にはユーザー、デバイス、モノが混在

お客様の環境には管理対象と管理対象外のデバイス、ユーザー、モノが存在

シンプルなニーズには、複雑さとリスクが潜在



セキュリティ

エンドツーエンドの可視性

一貫したエクスペリエンス

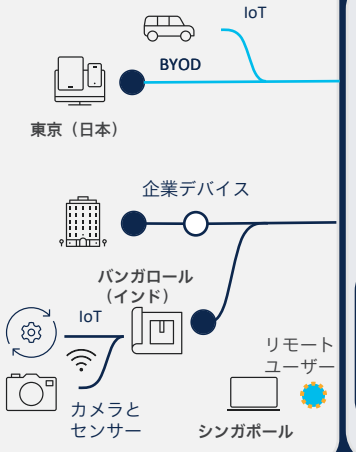
Power of the Platform

すべての複雑さとリスクを管理する鍵はネットワーク

ユーザー、デバイス、モノ

リモート　ブランチ　キャンパス

オンプレミス、DC アプリ/クラウドアプリ、SaaS



ネットワークは、ユーザーを
アプリケーションに接続する橋であり、接続されているすべての
ものを確認できる唯一のコントロールポイント

データセンターでホストされるアプリケーション

パブリッククラウド

SaaS

Power of the Platform

現在のネットワークは各ドメインで、ポリシーと可視性が分断

セキュリティに対する企業の現在の寄せ集めのアプローチが状況をさらに複雑化

ビジネス環境や IT 環境の中に製品が増えることで複雑化が進行

- データ漏洩
- ランサムウェア
- ラテラルムーブメント
- Web の脅威
- ログイン情報の盗用
- スパム

76

1 社で使用されているセキュリティツールの平均数

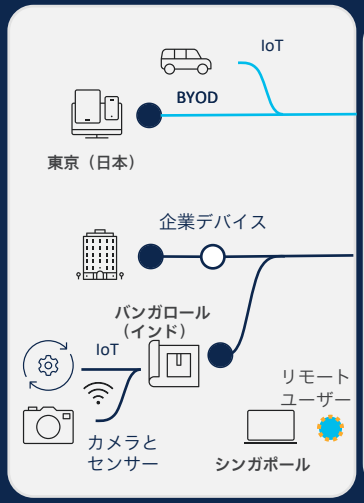
78%

多数のセキュリティツールの存在がサイバーセキュリティの複雑性を高めていると報告している組織*

*出典：『Keys to Successful SSE』、ESG グローバル調査。2023 年 6 月

企業に必要なのは一貫性のあるアイデンティティ、ポリシー、可視性、適用

リモート　ブランチ　キャンパス



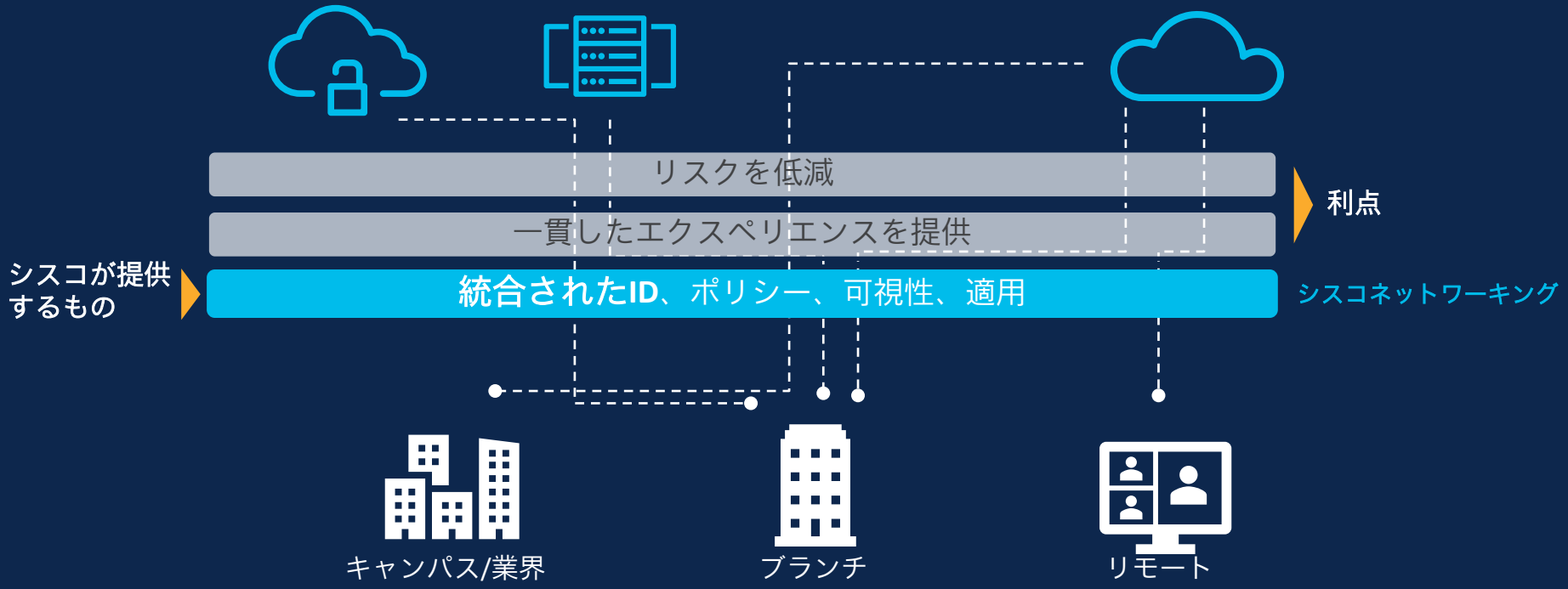
ユーザー、デバイス、モノの間の単一アイデンティティ

アプリケーション / ネットワークアクセス用の
アイデンティティ主導型ポリシー

特定の ID に特定のポリシーを適用

アイデンティティとポリシー適用のためのエンドツーエンドの可視性

Cisco Secure Networking：
ゼロトラストをベースに構築された最適なネットワーク



Cisco Secure Networking ：
ネットワークとセキュリティをともに考慮



リモート　ブランチ　キャンパス

人々、場所、モノ

キャンパス / ブランチ / リモートネットワーク

ファイアウォールとゲートウェイ

オンプレミス、DC アプリ/ クラウドアプリ、SaaS

統合されたID、ポリシー、可視性

Cisco Identity Service Engine
ポリシーベース認証プラットフォーム

Cisco Secure Network Analytics
トラフィックの可視化、脅威の検出


Cisco Secure Endpoint と Duo
クラウド / ネットワークへのセキュアなアクセス

Catalyst Center
キャンパスにおけるセグメンテーション作成と適用

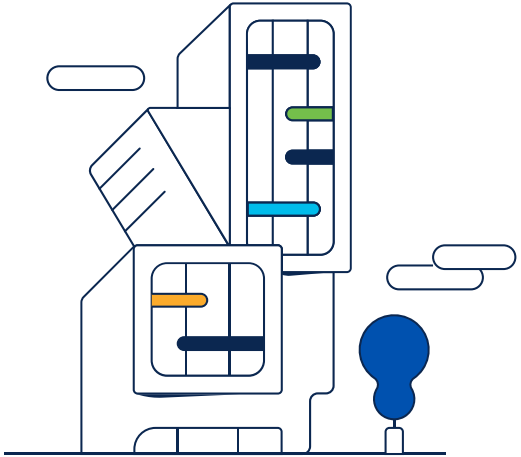
Catalyst SD-WAN
セキュアクラウド・WAN接続

Cisco Meraki
クラウド提供型セキュアキャンパス & SD-WAN

Firepower と Meraki MX
次世代キャンパス・DC ファイアウォール

Secure Access
ハイブリッド DC・SaaS 向けのクラウド提供型セキュリティ

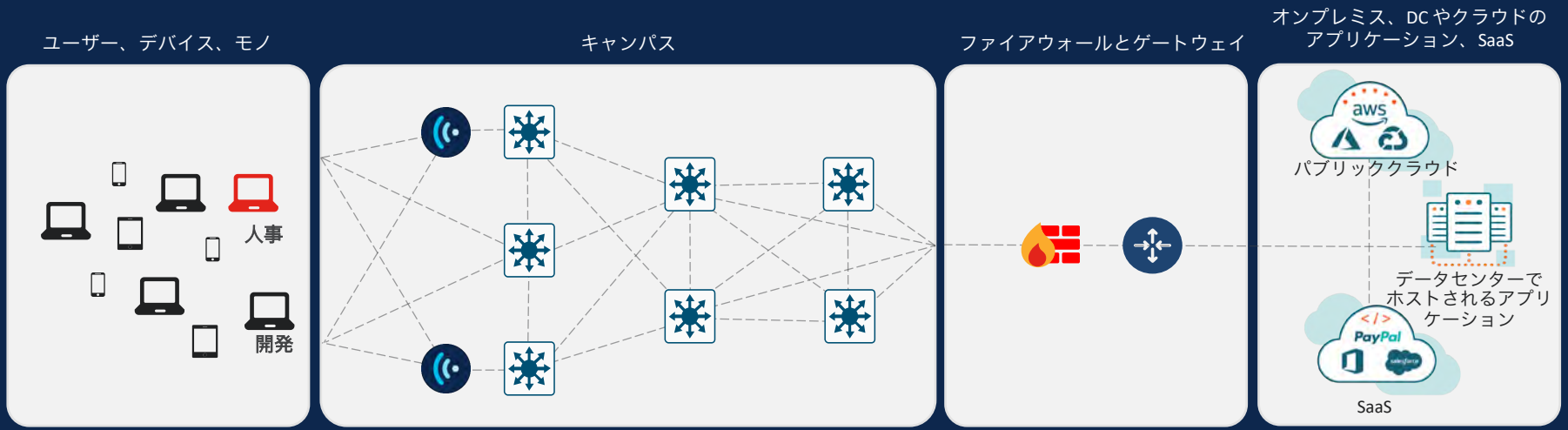
キャンパスでの活用事例



キャンパスシナリオ：攻撃者が脆弱性をエクスプロイトすればネットワークへのアクセスが可能

Lisa
人事コーディネータ

なりすましの
ユーザー



キャンパスシナリオ：セキュリティインシデント（1/3）

Lisa
人事コーディネータ

なりすましの
ユーザー

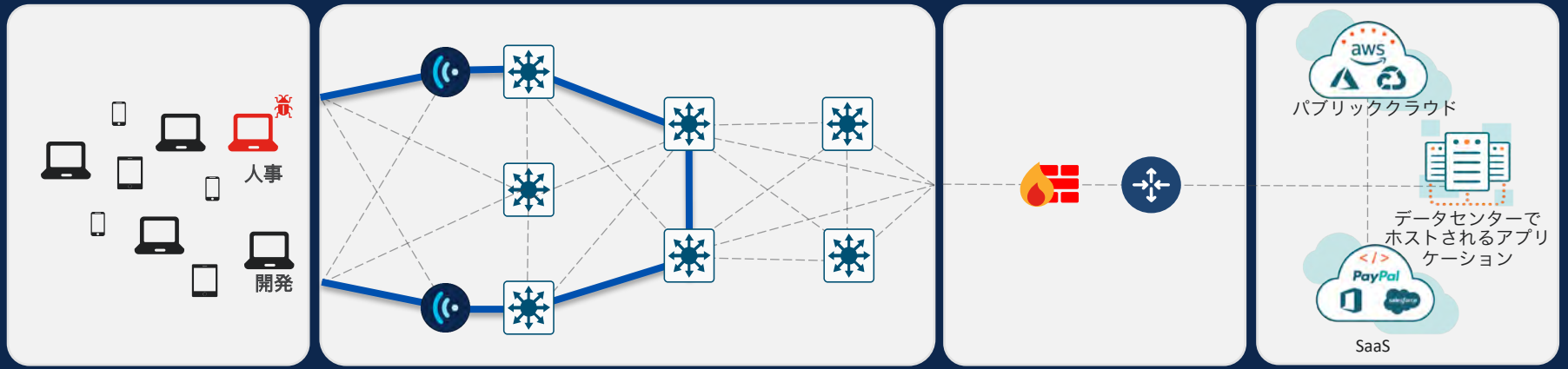
1 攻撃者が**ユーザーになりすまし、暗号化されたトラフィック内に隠れて**さらなる検出を回避

ユーザー、デバイス、モノ

キャンパス

ファイアウォールとゲートウェイ

オンプレミス、DC やクラウドの
アプリケーション、SaaS

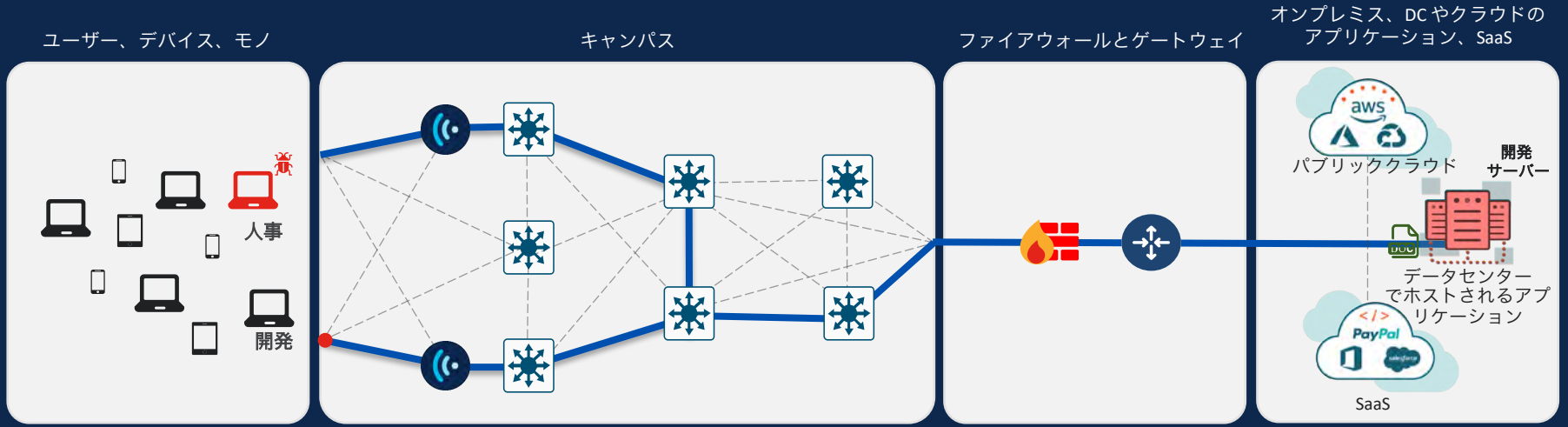


キャンパスシナリオ：セキュリティインシデント（2/3）

Lisa
人事コーディネータ

なりすましの
ユーザー

1. 攻撃者が**ユーザーになりすまし、暗号化されたトラフィック内に隠れて**さらなる検出を回避
2. 攻撃者が**ラテラルムーブメント**により開発者の特権アクセスを獲得し、製品の機密データを窃取

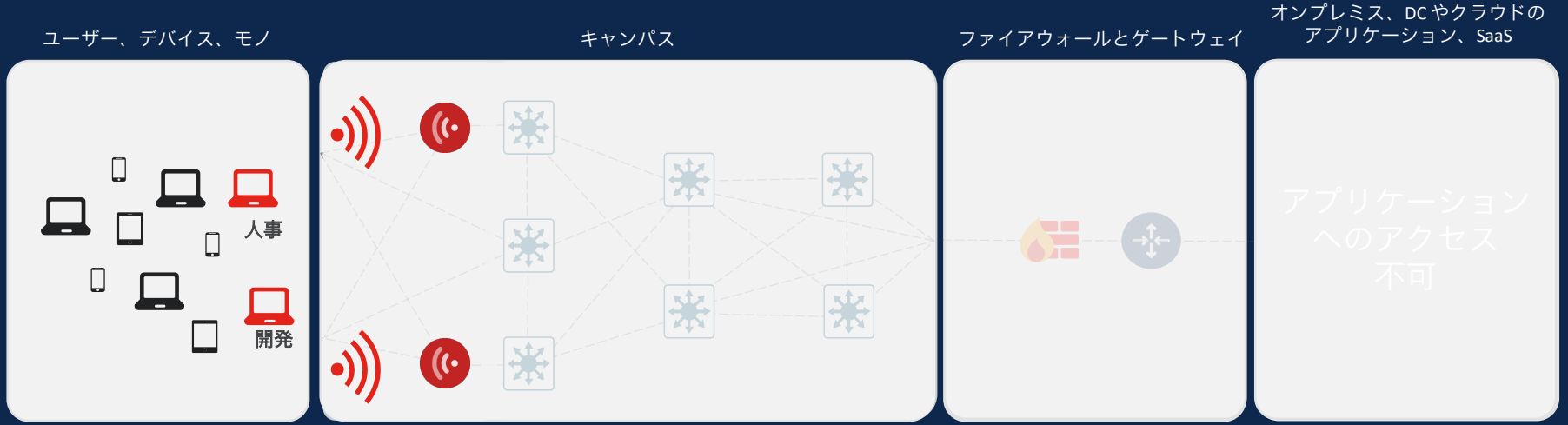


キャンパスシナリオ：セキュリティインシデント（3/3）

Lisa
人事コーディネータ

なりすましの
ユーザー

1. 攻撃者が**ユーザーになりすまし、暗号化されたトラフィック内に隠れて**さらなる検出を回避
2. **攻撃者がラテラルムーブメント**により開発者の特権アクセスを獲得し、製品の機密**データ**を**窃取**
3. 攻撃者が**ワイヤレス侵入攻撃**を使用してワイヤレス インフラストラクチャを遮断



Cisco Secure キャンパスの場合のシナリオ

Cisco Secure Networking：キャンパス（1/4）

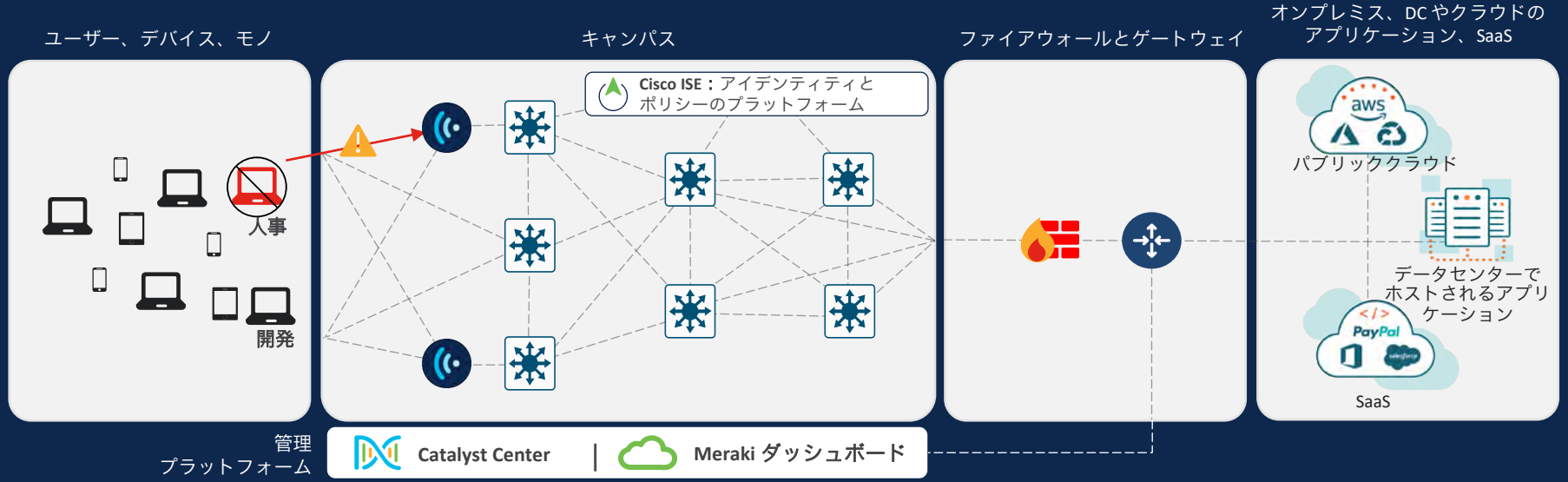
1 攻撃者がユーザーになりすまし、暗号化されたトラフィック内に隠れてさらなる検出を回避

セキュアなオンボーディング

Cisco ISE がユーザー認証とデバイスプロファイリングを行い、有効なユーザーとデバイスのみにネットワーク接続を許可

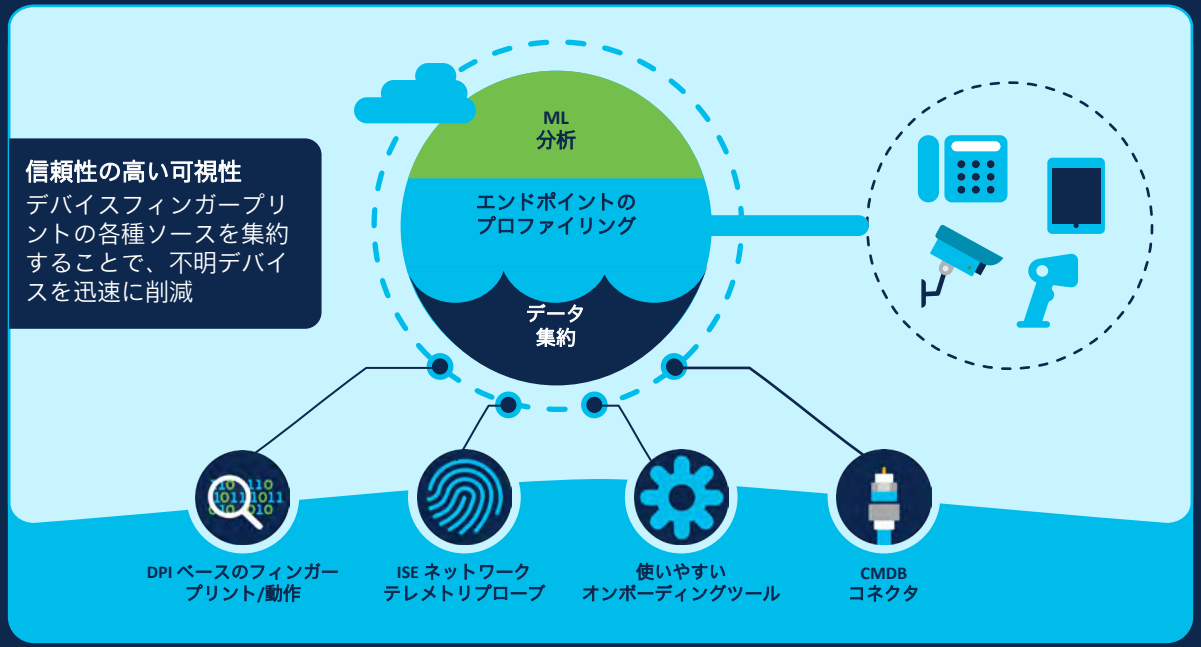
AI エンドポイント分析

Cisco Catalyst Center が AI 主導の分析を活用し、未知のデバイスからのネットワーク接続を阻止



Cisco AI End Point Analytics の詳細

AI 主導の分析とネットワーク主導のディープ パケット インスペクション（DPI）により次世代のエンドポイントの可視性を実現



Cisco AI Endpoint Analytics は、機械学習、DPI、統合の各機能により、これまでにない**きめ細かいエンドポイントの識別**とラベリングを実現

これらの高度なセキュリティ制御が組織にもたらすメリットは、**全体的なリスクの軽減**、コンプライアンスの範囲の縮小、マルウェアのラテラルムーブメントの制限、ランサムウェアなどの脅威の封じ込め

Cisco Secure Networking：キャンパス（2/4）

Lisa
人事コーディネータ

なりすましの
ユーザー

1 攻撃者はユーザーになりすまし、暗号化されたトラフィック内に隠れて
さらなる検出を回避

セキュアなオンボーディング

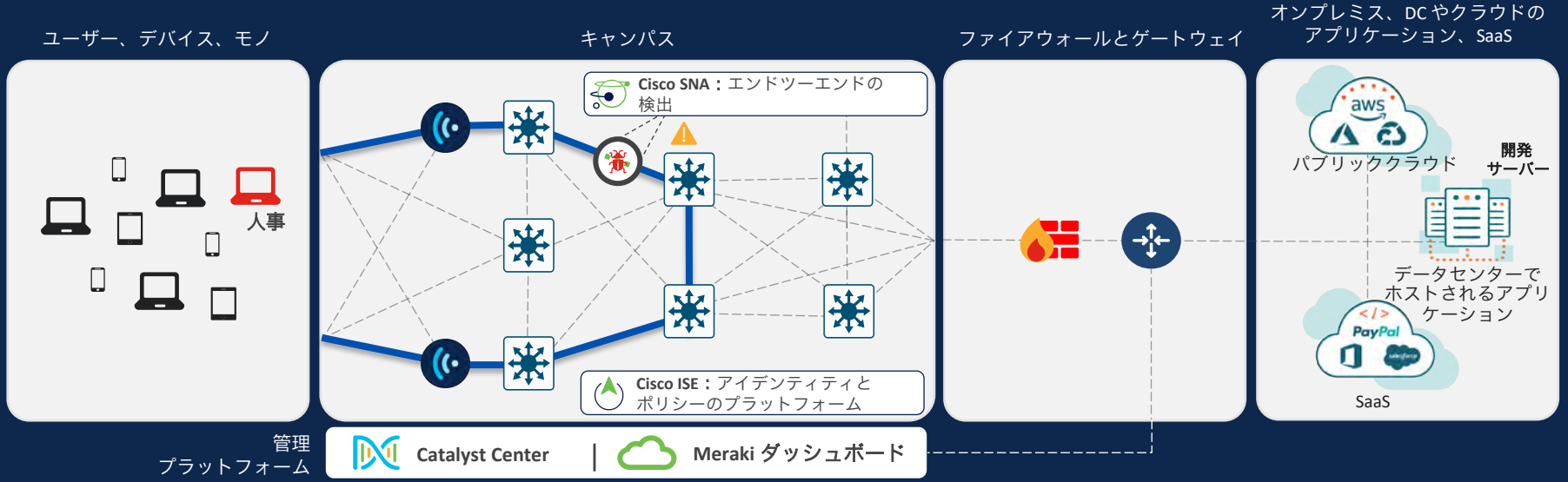
Cisco ISE がユーザー認証とデバイスプロファイリングを行い、有効なユーザーとデバイスのみにネットワーク接続を許可

エンドポイント分析

Cisco Catalyst Center が AI 主導の分析を活用し、未知のデバイスからのネットワーク接続を阻止

脅威の可視化

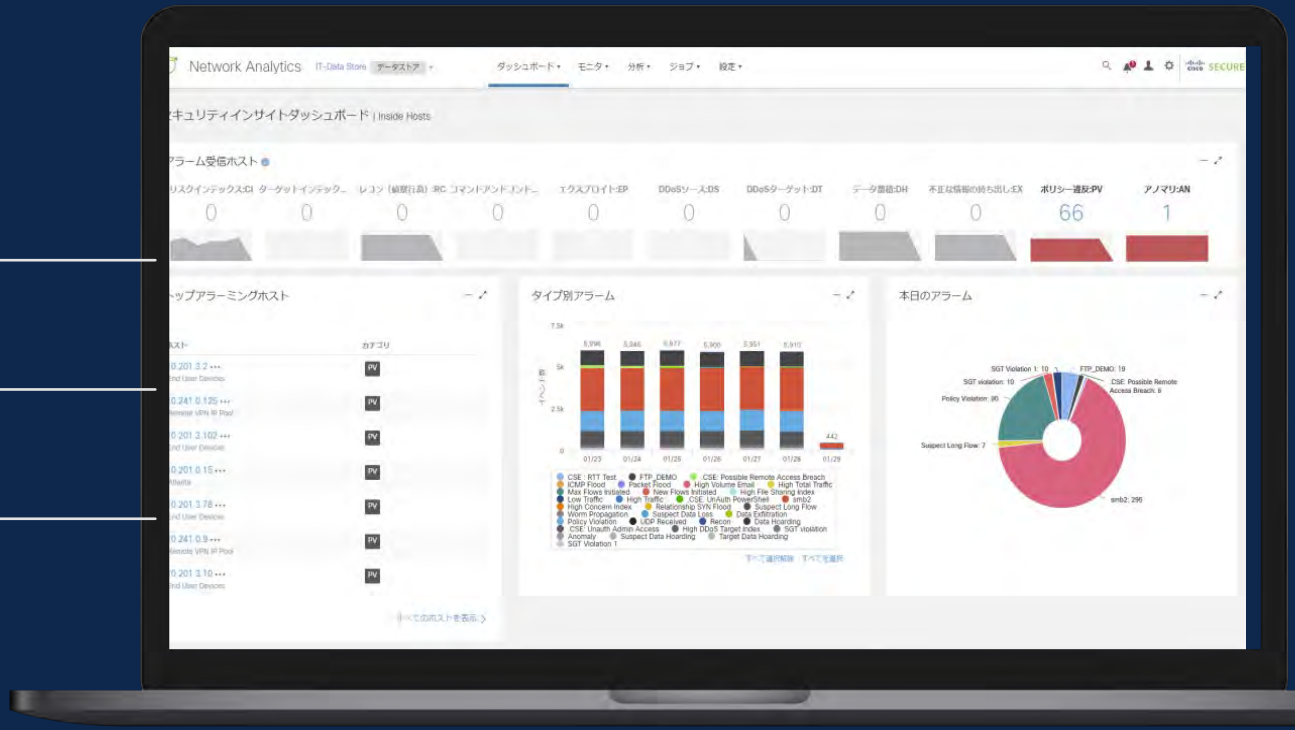
Cisco SNA が広範囲にわたるネットワークの可視性とセキュリティ分析により、拡張されたネットワークとクラウドを保護



Cisco Secure Network Analytics の詳細

3 次元での優先順位付け

- アラートの重大度
- アセットの価値
- 信頼性



Cisco Secure Network Analytics の詳細

ネットワーク全体にわたるふるまい分析により、高度な脅威を迅速に特定

あらゆる場所で可視化を実現

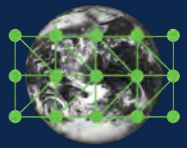
クラウド内の拡張ネットワーク全体や、リモートワーカーをつなぐネットワークをエンドツーエンドで可視化し、あらゆるソースからのエンタープライズテレメトリを分析

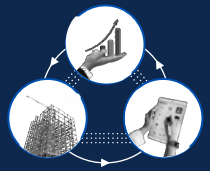
独自の脅威検出

マルチレイヤの機械学習機能とふるまいモデリング機能を組み合わせることで、内外の脅威を検出

暗号化トラフィック分析

暗号化されたトラフィックを復号せずに分析してマルウェアを検出し、ポリシーのコンプライアンスを確保





スマートなセグメンテーション

論理的なビジネス機能グループを活用し、コンテキスト情報に基づくアラームを通じてセグメンテーションポリシーの有効性をモニター

迅速な脅威対応

自動対応機能を利用して関連するポリシーを適用することで、ネットワークを活用して感染したホストを削除

Power of the Platform

Cisco Secure Networking：キャンパス（3/4）

Lisa
人事コーディネータ

なりすましの
ユーザー

2 攻撃者がラテラルムーブメントにより開発者の特権アクセスを獲得し、製品の機密データを窃取

セキュリティグループタグ（SGT）
Cisco ISE が、信頼ネットワーク内で各ホストに対してアイデンティティソースとして SGT を適用

動的セグメンテーション
Cisco SD-Access が、SGT に基づいてユーザートラフィックのセグメンテーションを自動化。セグメンテーションにより不正なラテラルムーブメントを抑止

セキュアポリシーの適用
Cisco SD-Access と Cisco ISE が、単一のネットワークファブリックを介して、ワイヤレスと有線のネットワークにあるアプリケーションに、共通のユーザーポリシーとデバイスポリシーを自動的に展開

ユーザー、デバイス、モノ

SGT
人事
開発

キャンパス

ポリシー | 開発 | その他
人事

Cisco ISE：アイデンティティとポリシーのプラットフォーム

ファイアウォールとゲートウェイ

オンプレミス、DC やクラウドのアプリケーション、SaaS

パブリッククラウド
開発サーバー
データセンターでホストされるアプリケーション
SaaS

管理プラットフォーム

Catalyst Center | Meraki ダッシュボード

Cisco SD-Access

ゼロトラストワークプレイス機能で IoT デバイスとユーザーによるネットワークアクセスを管理しセキュリティを確保

ネットワークのシンプル化

ネットワーク プロトコル スタックを 15 ～ 20 から **3** に削減

コンバージェンス

有線とワイヤレスのポリシーを統合

ZTN

ゼロトラスト ネットワーク

ネットワーク セグメンテーションの機能として実現

HA

L3 プロトコルにより HA を向上

自動化

Cisco DNAC がネットワーク運用をシンプル化

動的セグメンテーション

ユーザーポリシーの適用をシンプル化

シームレスでシンプルな L2 ワイヤレス モビリティ

キャンパスファブリックのどこへでも移動可能

LISP

他のファブリックソリューションと比較して**拡張性**が向上

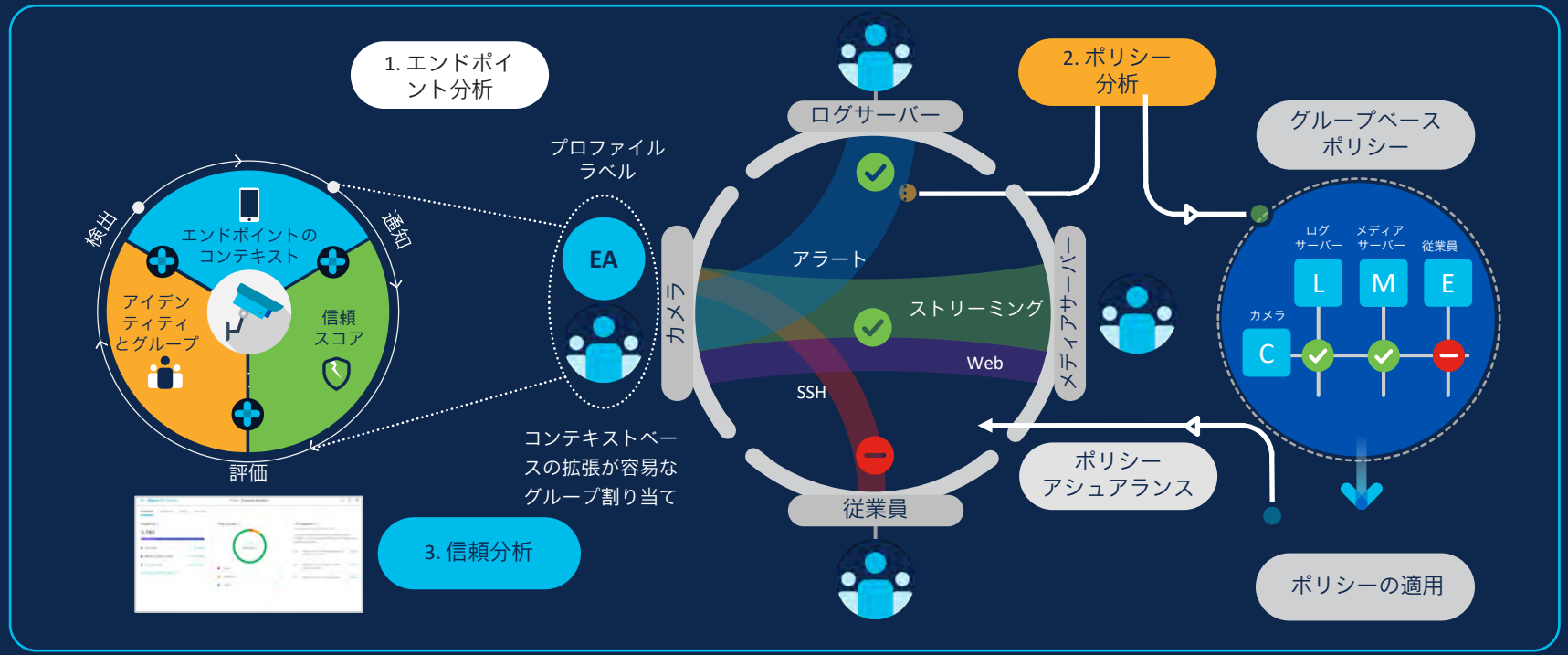
IT と OT の

コンバージェンス

SDA アーキテクチャの機能として実現

Cisco Catalyst Center と ISE

可視性主導のセグメンテーションですべてを実現



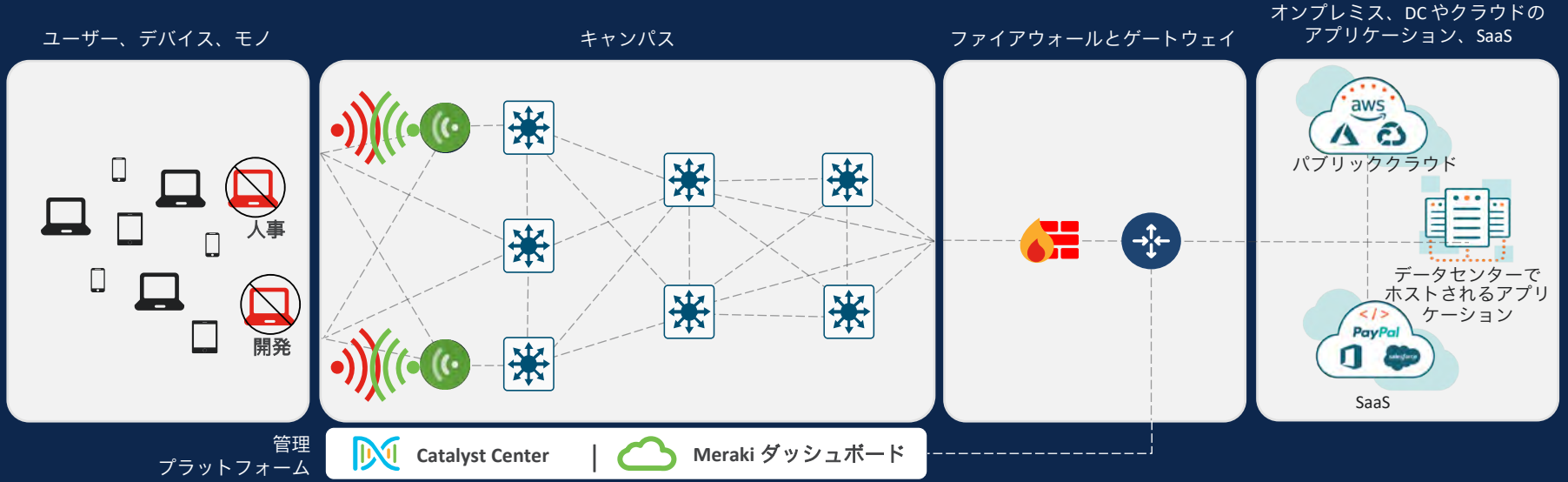
Cisco Secure Networking：キャンパス（4/4）

Lisa
人事コーディネータ

なりすましの
ユーザー

3 攻撃者は**ワイヤレス侵入攻撃を使用して**ワイヤレス インフラストラクチャを遮断

Wi-Fi 侵入検知	Wi-Fi 侵入防御	不正ワイヤレスの隔離
Cisco WIDS が、攻撃、脆弱性、パフォーマンスを検出する広範なライブラリを備えた高度なアプローチでワイヤレス攻撃を検出	Cisco WIPS ソリューションが、セキュリティ攻撃者をネットワークから排除し、不正アクセスポイントをロックアウトすることで、一部の攻撃をさらに軽減	Cisco Catalyst Center と Meraki クラウド管理プラットフォームが、さらに、有線ネットワークから不正アクセスポイントを排除



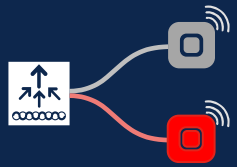
ワイヤレス IPS

専用のスキャン無線を使用してすべての脅威を継続的モニタリング

有線ネットワーク攻撃

有線ネットワーク上の不正デバイス

不明 | 悪意がある



- スイッチポートのトレース
- RLDP

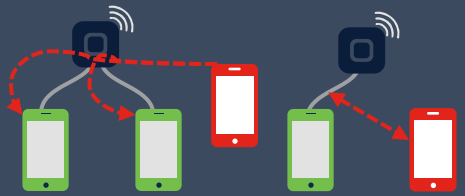
無線攻撃

不正アクセスポイント | Honeypot や Evil Twin | AP MAC スプーフィング

- 不正アクセスポイントの管理

基本的なワイヤレスセキュリティ

サービス妨害 | 偵察 | クラッキングツール



- WIPS

高度なワイヤレスセキュリティ

非 802.11 干渉源

電子レンジ | Bluetooth
レーダー | 電波妨害装置

- Cisco CleanAir

非 Wi-Fi 干渉源の可視化

これまでのシナリオのまとめ

人々、場所、モノ

キャンパス / ブランチ / リモートネットワーク

ファイアウォールとゲートウェイ

オンプレミス、DC アプリ/クラウドアプリ、SaaS

統合されたID、ポリシー、可視性

Cisco Identity Service Engine
ポリシーベース認証プラットフォーム

Cisco Secure Network Analytics
トラフィックの可視化、脅威の検出

Cisco Secure Endpoint と Duo
クラウド / ネットワークへのセキュアなアクセス

Catalyst Center
キャンパスにおけるセグメンテーション作成と適用

Catalyst SD-WAN
セキュアクラウド・WAN接続

Cisco Meraki
クラウド提供型セキュアキャンパス & SD-WAN

Firepower と Meraki MX
次世代キャンパス・DC ファイアウォール

Secure Access
ハイブリッド DC・SaaS 向けのクラウド提供型セキュリティ

シスコがマルチベンダーの複雑さを軽減

Cisco Secure Networking がもたらす成果

サイバーセキュリティ脅威によるリスクの軽減 › ユーザー体験の向上 › 管理のシンプル化

ネットワーク、セキュリティ密に連携できるソリューションを備えた単一ベンダー

マルチベンダー運用による複雑さとコストを削減