シスコが実現する統合ネットワークセキュリティ制御：Cisco Security Cloud Control と Common Policy のご紹介

シスコシステムズ合同会社
セキュリティ事業
ソリューションズエンジニア
豊島 かおり

分散する脅威ベクトル 〉サイロ化したセキュリティ運用

“

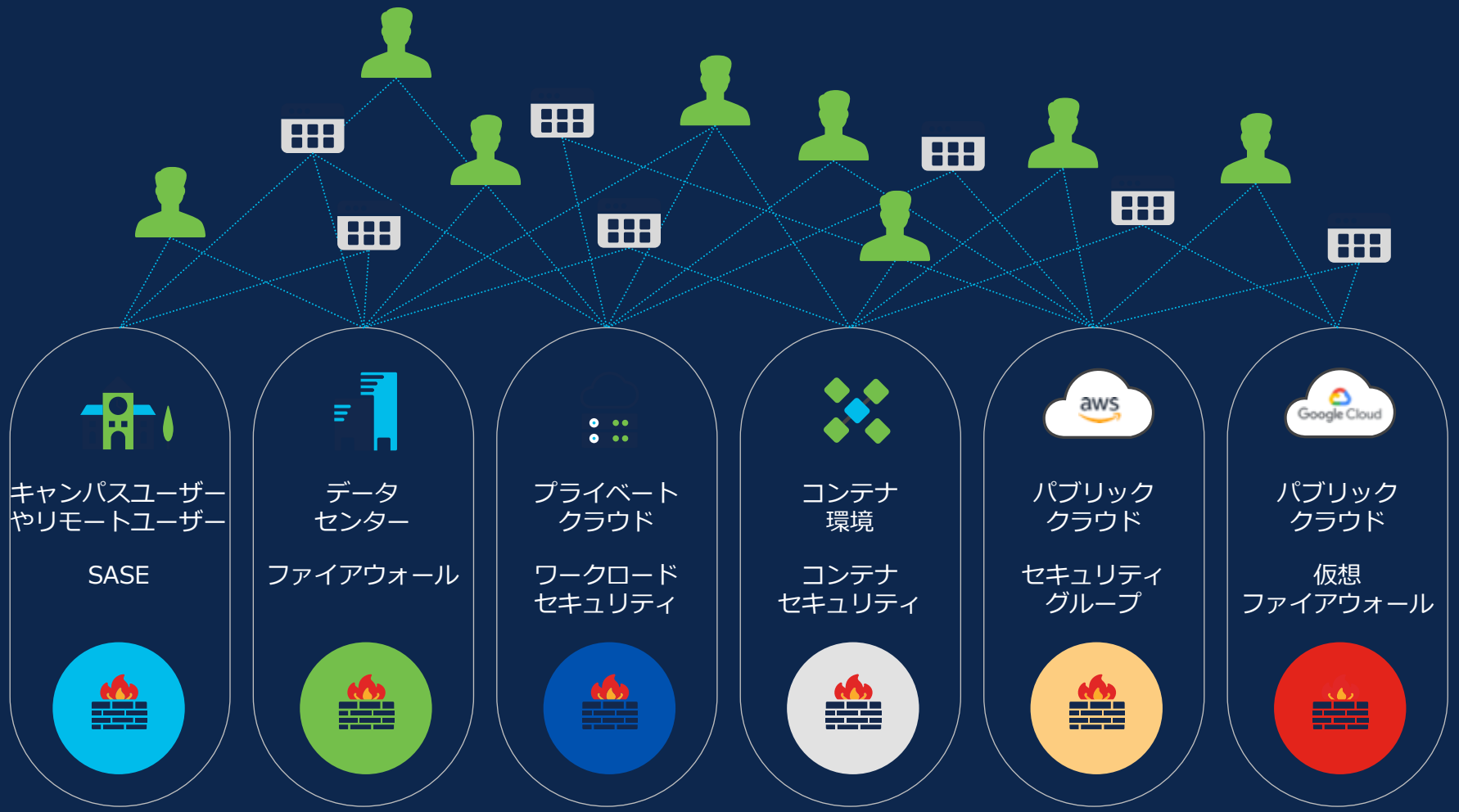
目的のデータを取得するまでに**色々な場所にアクセスする必要**があります

“

異常時にはほぼリアルタイムで、**さまざまなシステムをくまなく調査する必要があり**、これは非常に困難です

IT チームの課題

ハイブリッド環境全体にまたがるツールおよびポリシーの複雑さ



複数のチームと組織

複数の動的環境をカバー

それぞれごとに異なるポリシーモデルと適用ポイント

ポリシー制御が一貫性を失いサイロ化して孤立

複雑さがセキュリティの盲点を生む

複雑な
ルール

010110
110010
001011

設定ミス

スキルセット
トの需要

脆弱なセキュリティ態勢

アウテージ/ダウンタイム

リアクティブプロセス

ネットワーク・ダウンタイムの平均コストは1時間当たり30万ドル

Cisco Security Cloud Control

2025年 3月末 正式リリース

Cisco Security Cloud Control

統合セキュリティ管理

Secure Firewall ASA

Secure Firewall Threat Defense

Multicloud Defense

Hypershield

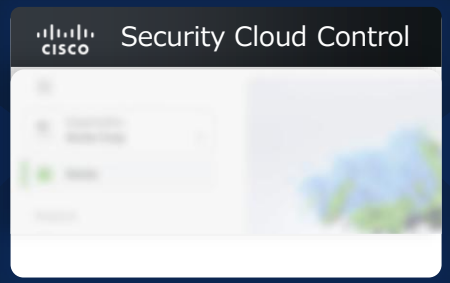
Secure Access

Secure Workload

AI Defense

旧CDO (Cisco Defense Orchestrator) から
2024年11月にリブランディング済み

and more…
拡張予定



共通のエクスペリエンス

集中プロビジョニング と
ロールベースアクセス制御

ユニファイド AI
アシスタント

Cisco Security Cloud Control 基本構造

https://www.cisco.com/site/us/en/products/security/security-cloud-control/index.html#tabs-35d568e0ff-item-194f491212-tab

統一ナビゲーション

あらゆるSBG製品が新しい左ナビ構造にマッピングされ、製品間のナビゲーションが利用可能

共通コアサービス

グローバル検索、AIアシスタント、ヘルプおよびドキュメント、ダッシュボード、ガイド付きオンボーディングなど

マイクロアプリホスト

ランタイムのマイクロアプリをホスト

プロビジョニングとアクセス管理

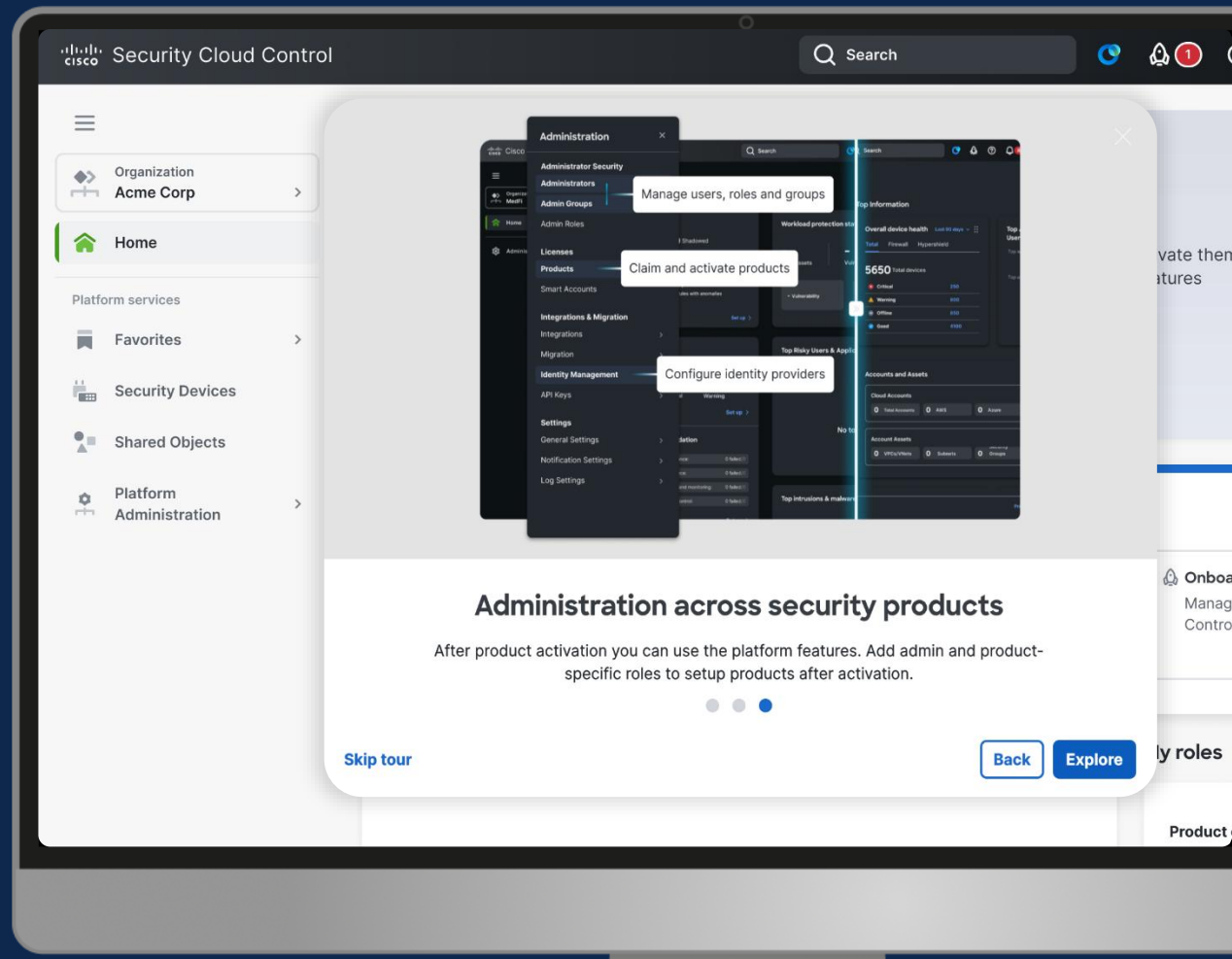
プロビジョニング、RBAC、統合テナント、地域選択

統合インターフェイスと
セキュリティ運用の高度化

学習・運用時間の短縮
複数製品で一貫性のあるユーザエクスペリエンス
シンプルなオンボーディングで運用の複雑性を排除

セキュリティとコンプライアンスの拡張
包括的なロールベースアクセス制御とシームレスなIDP連携

AIを活用したプロアクティブな運用
共通の対話型インターフェイスや予見にAIを活用



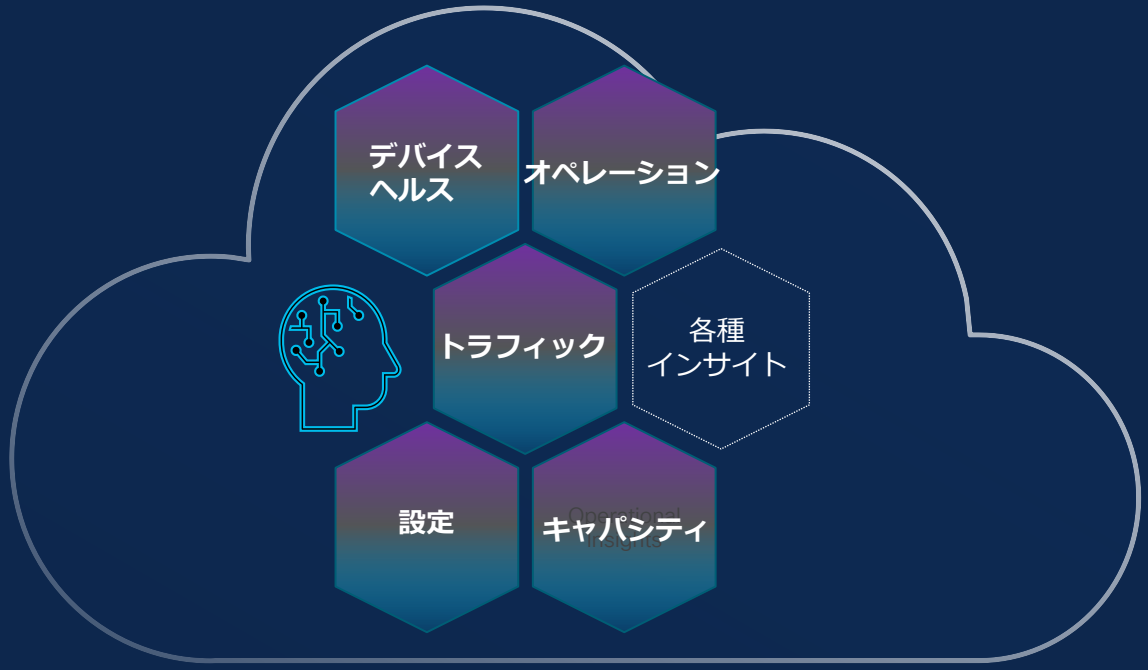
*UI design subject to change

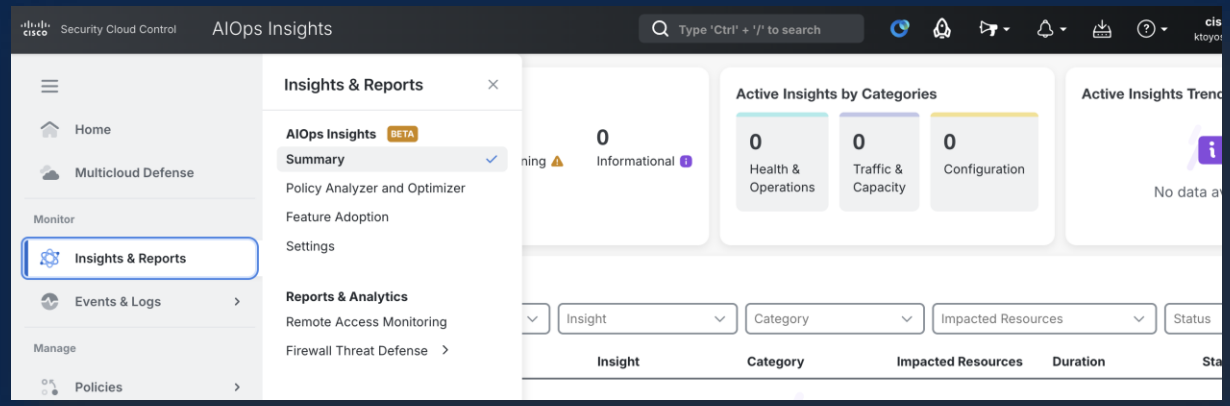
AIOps Insights

搭載済み

Security Cloud Controlの管理情報から得られる各種インサイトを通知

- AI が導くベストプラクティスでセキュリティ態勢を改善する
- リスクベースの優先順位付けにより、解決までの平均時間を短縮する
- 機能利用情報からセキュリティ投資を最大限に活用する





搭載済み

Policy analyzer and optimizer

ポリシーを自動で分析し
最適化方法を提案

設定ミスの最小化
ダウンタイムの最小化

ファイアウォールのパフォーマンスを向上

ポリシーの展開と更新をスピードアップ

AIアシスタントとの連携を支援

ルールの重複、非表示、広すぎるルールなどの問題に対処

全体的なセキュリティ態勢の改善

今月正式リリース

ユニファイド AI アシスタント

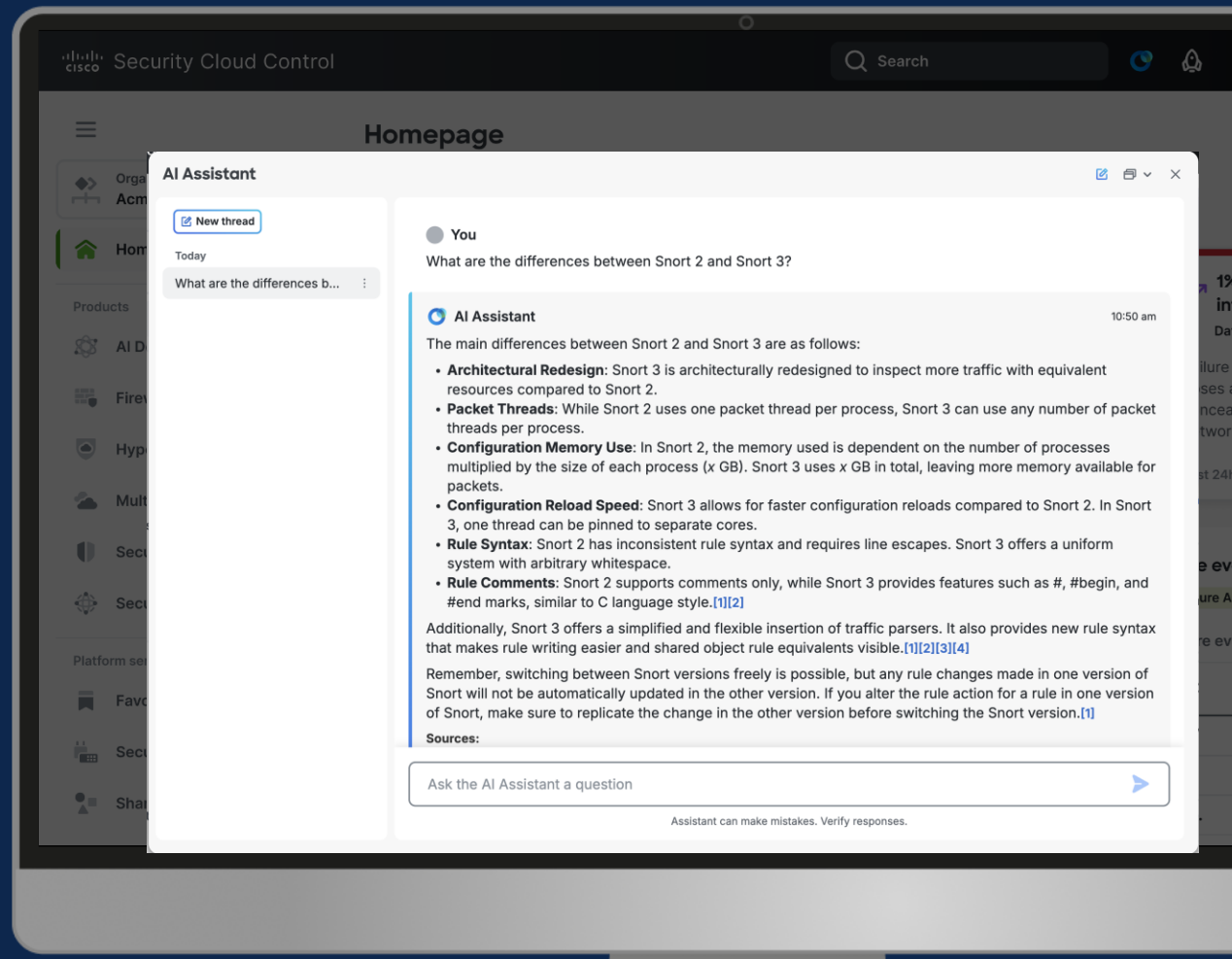
単一の対話型インターフェイス

Security Cloud Control で 1つの統合アシスタントが複数のセキュリティ製品 ※ へのインサイトを提供

※ Secure Firewall, Secure Access, Hypershield

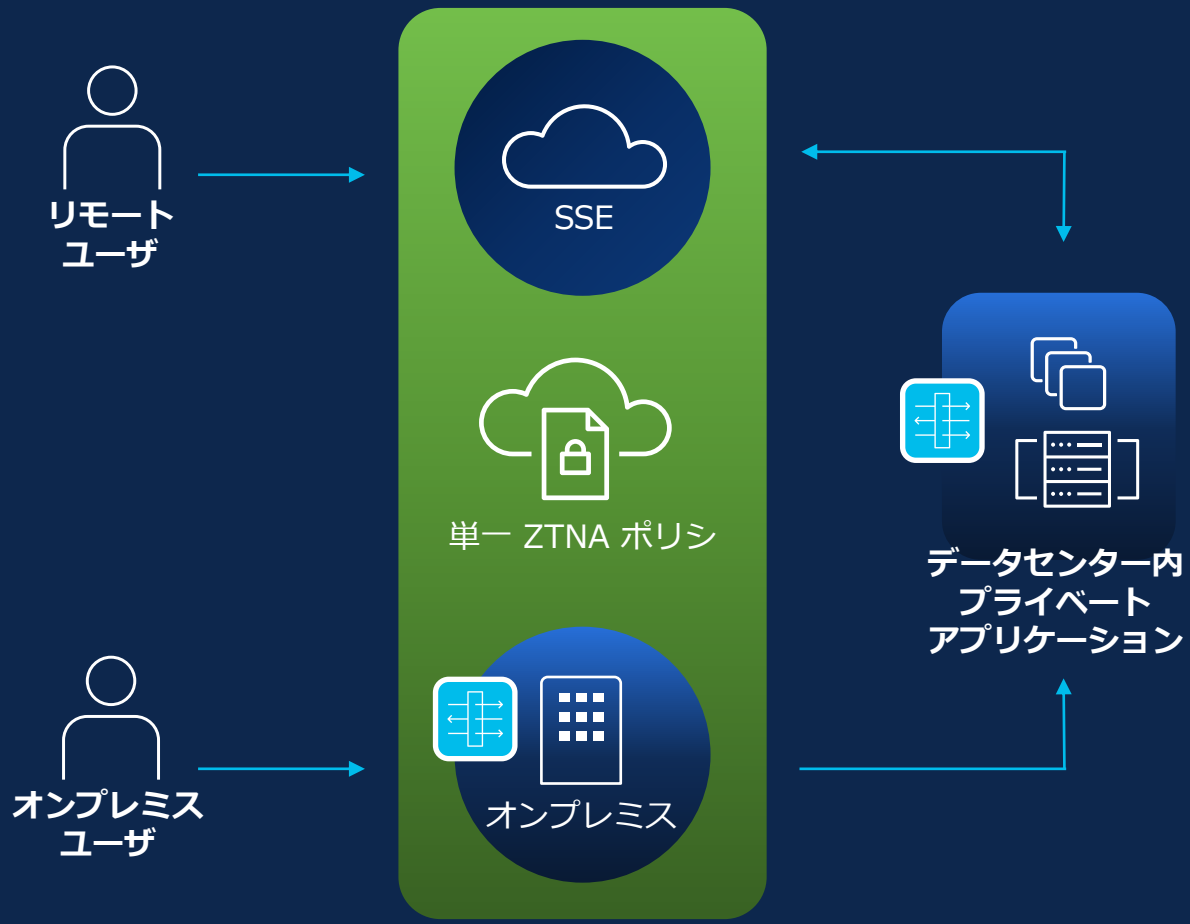
統合されたナレッジハブ

包括的なガイダンスのための製品横断的なドキュメントへのアクセス



*UI design subject to change

Hybrid ZTNA: SSE と Secure Firewall の ZTNA統合



- Cisco セキュアファイアウォールの機能拡張：オンプレミスユーザへのZTNAアクセス、プライベートアプリケーションのインスペクション
- 単一の 共通 ZTNA ポリシを Security Cloud Control から自動的に配信
- 既存ユーザの方への追加投資や追加コストは不要

宛先やアプリケーションや 回線遅延に応じて、クラウド or オンプレ宛に動的に接続先変更が可能に
より低遅延に、高速に、セキュアな ZTNA を実現

Cisco Common Policy

“Improving the Nation’s Cybersecurity”

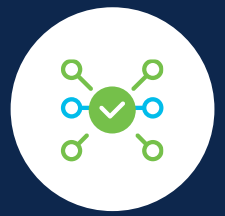
- 大統領令（EO）14028 - Sec. 10. の定義

- 「ゼロ・トラスト・アーキテクチャは、包括的なセキュリティ監視、きめ細かなリスクベースのアクセス制御、システム・セキュリティの自動化をインフラストラクチャの全側面にわたって協調的に組み込み、動的な脅威環境の中でリアルタイムでのデータ保護に集中する。
- 「デバイスが侵害された場合、ゼロ・トラストは被害を確実に食い止めることができる。」

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

人によって
ゼロトラストの
解釈が異なる

SASE / ZTNA



セグメンテーション

エンドポイントセキュリティ

ファイアウォール

アイデンティティ

セグメンテーションを求めるコンプライアンス要件の例

参考資料

ISO 27001：情報サービス、ユーザー、情報システムのグループは、ネットワーク上で分離されるべきである

Control A.13.1.3 (Segregation in networks)

Other related Control: A.13.1.1, A.13.2.1, A.14.1.2, A.14.1.3

ISO 27002：ISO 27001の管理実施に関するガイダンスを提供し、いくつかの勧告を行う

・大規模ネットワークを個別のネットワーク・ドメイン（セグメント）に分割する

・物理的、論理的な分離を考慮する

・ドメイン境界の定義

・ドメイン間のトラフィックルールの定義

・認証、暗号化、ユーザーレベルのネットワークアクセス制御技術を使用する

・組織のネットワークやセグメントとビジネスパートナーのネットワークとの統合を検討する

NIST Cybersecurity Framework (CSF) / Special Publication (SP) 800-53, 800-171, 1800-27 / NISTIR 8374

PROTECT Identity Management, Authentication, and Access Control (PR.AC-5): Network integrity is protected (e.g. network segregation, network segmentation)

SOC 2 CC6: 論理的および物理的なアクセス制御

CC6.1 –ネットワーク・セグメンテーションは、企業の情報システムの無関係な部分を互いに分離することを可能にする

PCI DSS 要件 11.3.4

ネットワークのセグメンテーションは必須ではないが、カード会員データ環境（CDE） を他のネットワークと区別するために実装することを推奨する（重要なセキュリティ対策）。

CDE には、カード会員データ（CHD）またはその他の機密支払認証データを保存、処理、および／または伝送する人、プロセス、および技術が含まれる。システムコンポーネントには、有線および無線のネットワークデバイス、サーバ、コンピューティングデバイス、およびアプリケーションが含まれる。

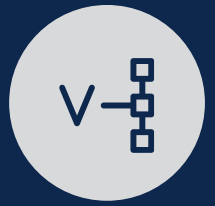
マクロ

マイクロ

エージェントベース

セグメンテーションの解釈は人によって異なる

ファイアウォール

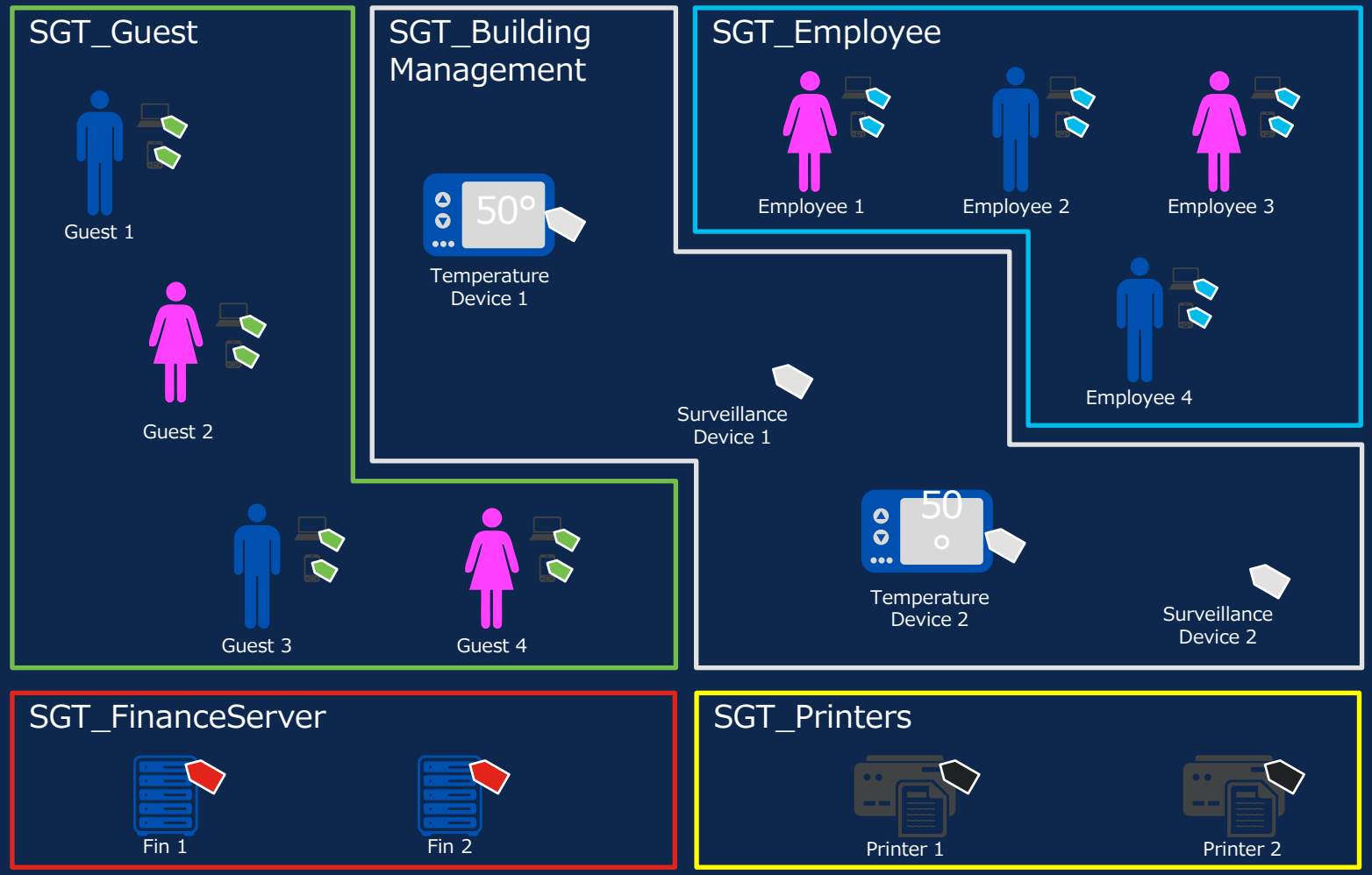


VLAN

本セッションの範囲：セグメンテーションで実現したいことはなにか

共通の役割とポリシーを示す”論理セキュリティグループ”

- ユーザーの役割、デバイスの種類などの属性を活用したビジネスベースのグループ割り当て
- 論理セキュリティグループごとにネットワークアクセス権限を制限するポリシーを定義



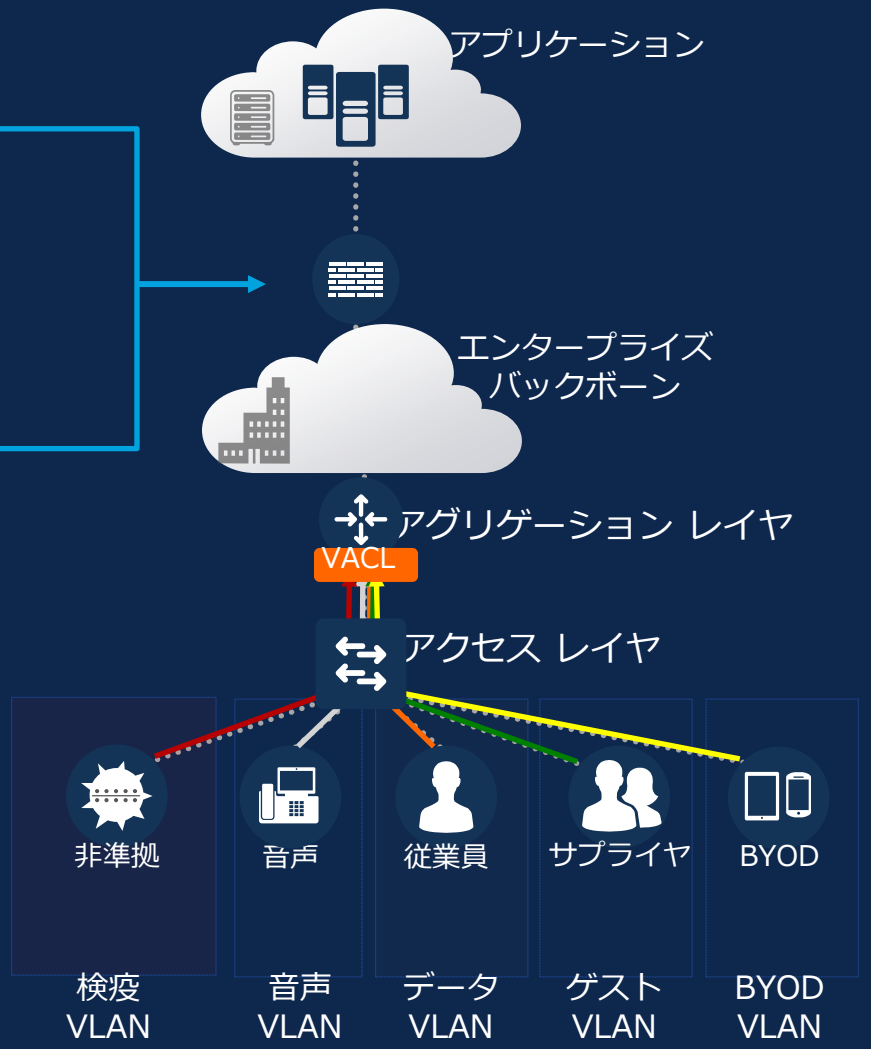
ネットワークセグメンテーションの現在

```
access-list 102 deny udp 167.160.188.162 0.0.0.255 gt 4230 248.11.187.246 0.255.255.255 eq 2165
access-list 102 deny udp 32.124.217.1 255.255.255.255 lt 907 11.38.130.82 0.0.31.255 gt 428
access-list 102 permit ip 64.98.77.248 0.0.0.127 eq 639 122.201.132.164 0.0.31.255 gt 1511
access-list 102 deny tcp 247.54.117.116 0.0.0.127 gt 4437 136.68.158.104 0.0.1.255 gt 1945
access-list 102 permit icmp 136.196.101.101 0.0.0.255 lt 2361 90.186.112.213 0.0.31.255 eq 116
access-list 102 deny udp 242.4.189.142 0.0.1.255 eq 1112 19.94.101.166 0.0.0.127 eq 959
access-list 102 deny tcp 82.1.221.1 255.255.255.255 eq 2587 174.222.14.125 0.0.31.255 lt 4993
access-list 102 deny tcp 103.10.93.140 255.255.255.255 eq 970 71.103.141.91 0.0.0.127 lt 848
access-list 102 deny ip 32.15.78.227 0.0.0.127 eq 1493 72.92.200.157 0.0.0.255 gt 4878
access-list 102 permit icmp 100.211.144.227 0.0.1.255 lt 4962 94.127.214.49 0.255.255.255 eq 1216
access-list 102 deny icmp 88.91.79.30 0.0.0.255 gt 26 207.4.250.132 0.0.1.255 gt 1111
access-list 102 deny ip 167.17.174.35 0.0.1.255 eq 3914 140.119.154.142 255.255.255.255 eq 4175
access-list 102 permit tcp 37.85.170.24 0.0.0.127 lt 3146 77.26.232.98 0.0.0.127 gt 1462
access-list 102 permit tcp 155.237.22.232 0.0.0.127 gt 1843 239.16.35.19 0.0.1.255 lt 4384
```

- スタティック ACL
- ルーティング
- 冗長性
- DHCP スコープ
- アドレス
- VLAN

従来のセグメンテーションの限界

- トポロジに基づいたセキュリティ ポリシー
- 高いコストと複雑なメンテナンス



適用
IP ベース ポリシー ACL、ファイアウォール ルール

伝播
VLAN タグ/IP アドレス/VRF を利用して、ネットワークでセグメント コンテキストを伝播

分類
スタティック/ダイナミック VLAN 割り当て

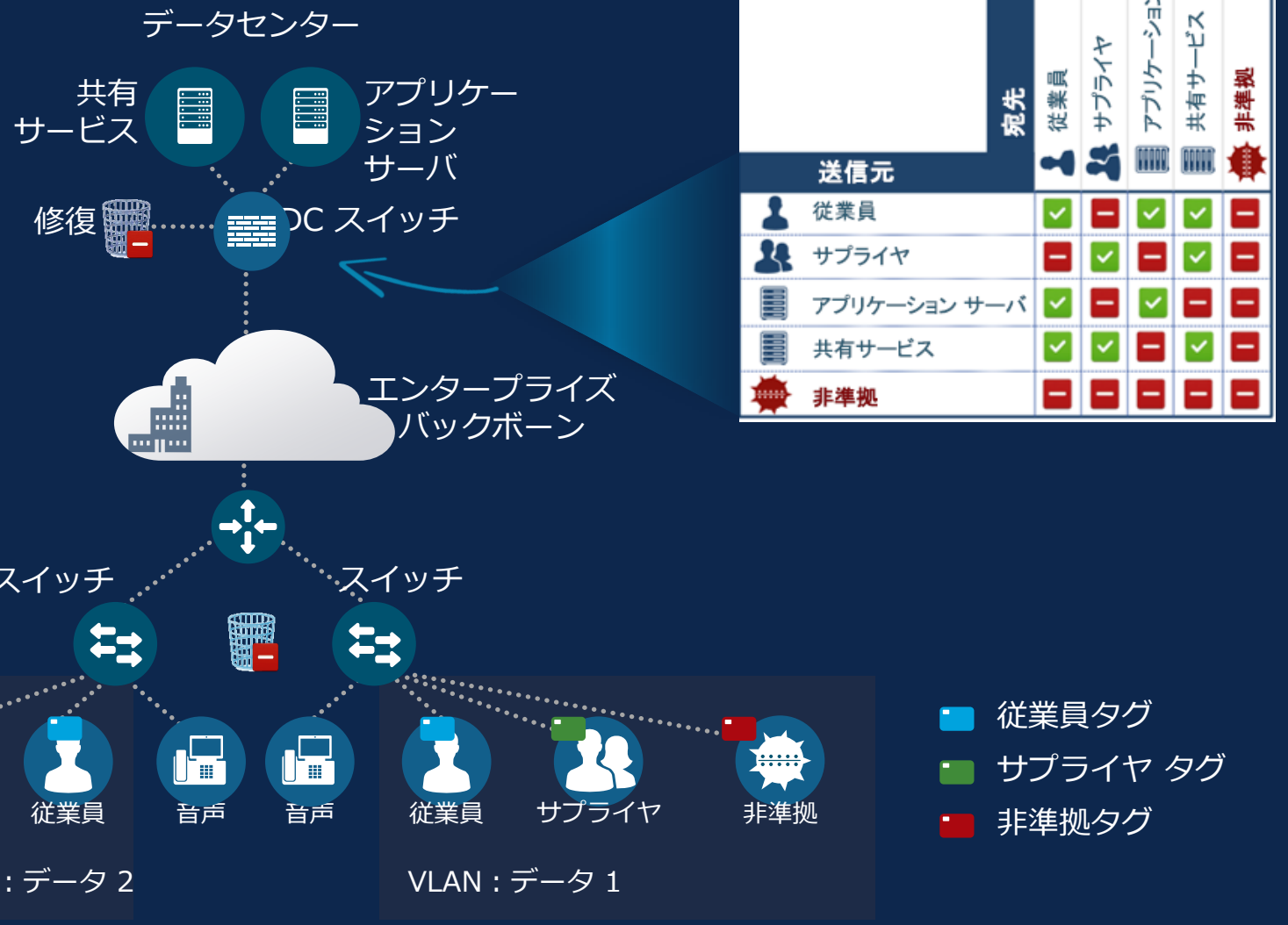
セキュリティグループ属性に基づく“タグ”によるトラフィック制御

2009年～
Cisco TrustSec としてサポート開始

“Security Group Tag (SGT) ” の導入

”SGT” はトポロジや場所に依存せず、直接エンドポイントの論理グループと紐づく

アクセスポリシーとネットワーク構造を分離し、制御ルールを簡素化する



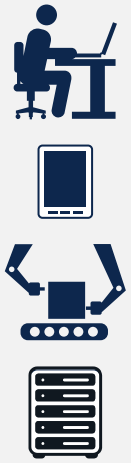
送信元 \ 宛先	従業員	サプライヤ	アプリケーション サーバ	共有サービス	非準拠
従業員	✓	−	✓	✓	−
サプライヤ	−	✓	−	✓	−
アプリケーション サーバ	✓	−	✓	−	−
共有サービス	✓	✓	−	✓	−
非準拠	−	−	−	−	−

セキュリティグループタグ(SGT)で通信制御を行う方法

ソフトウェア定義型セグメンテーション

SGTが有効なネットワーク

エンドポイント



Classification - 分類

静的な分類
(スタティックマッピング)

エンドポイント
識別

動的な分類
(802.1x認証他)

セキュリティ
グループ
タグ

Propagation – 伝播

データプレーン
(インラインタギング他)

コントロールプレーン
(SXP または pxGrid)

混在環境

スイッチ

ルータ

ファイア
ウォール

Enforcement – 適用

アクセス
ポリシー制御

脅威の隔離

集中管理

セキュリティグループ アクセスポリシー管理

セキュリティグループタグ管理

ISE

Cisco Identity Services Engine (ISE)

SGT/SGACL サポートプラットフォーム

参考資料

https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/policy-platform-capability-matrix.pdf

Classification

- Catalyst 9200, 9300, 9300-M, 9400, 9500, 9600
- IE 9300
- IE 4000
- IE 3100, 3200, 3300, 3400
- IE 2000
- IR 8340
- WLC 9800
- WLC 8510, 8540
- WLC 5760
- WLC 5508, 5520
- vWLC
- AP x700, x800, 9100
- Catalyst 8000V, 8200, 8300, 8500
- ISR 1000, 4000
- ASR 1000
- CSR
- CGR 2010, CGS 2500
- ASAv, FTDv
- CSF 1200, 3100, 4200
- FP 1010, 1100, 2100, 4100, 9300
- ISA 3000
- MS390, MS130X/R
- MR30H/33/42/42E/52/53/53E/74/84, MR36/36H/44/45/46/46E/55/56/57/76/86
- CW916x
- MX64/65, MX67/68, MX84/100, MX75/85/95/105, MX250/450
- Z3/4/C
- ISE

Propagation

- Catalyst 9200, 9300, 9300-M, 9400, 9500, 9600
- IE 9300
- IE 4000*
- IE 3100*, 3200*, 3300*, 3400
- IE 2000*
- IR 8340
- WLC 9800
- WLC 8510*, 8540*
- WLC 5760
- WLC 5508*, 5520*
- vWLC*
- AP x700, x800, 9100
- Catalyst 8000V, 8200, 8300, 8500
- ISR 1000, 4000
- ASR 1000
- CSR
- CGR 2010, CGS 2500
- ASAv, FTDv
- CSF 1200, 3100, 4200
- FP 1010, 1100, 2100, 4100, 9300
- ISA 3000
- MS390, MS130X/R
- MR30H/33/42/42E/52/53/53E/74/84, MR36/36H/44/45/46/46E/55/56/57/76/86
- CW916x
- MX64/65, MX67/68, MX84/100, MX75/85/95/105, MX250/450
- Z3/4/C
- ISE

Enforcement

- Catalyst 9200, 9300, 9300-M, 9400, 9500, 9600
- IE 9300
- IE 3400, 4000
- IR 8340
- WLC 9800
- WLC 8540
- WLC 5760
- WLC 5520
- vWLC**
- AP x700, x800, 9100
- Catalyst 8000V, 8200, 8300, 8500
- ISR 1000, 4000
- ASR 1000
- CSR
- CGR 2010
- ASAv, FTDv
- CSF 1200, 3100, 4200
- FP 1010, 1100, 2100, 4100, 9300
- ISA 3000
- MS390, MS130X/R
- MR30H/33/42/42E/52/53/53E/74/84, MR36/36H/44/45/46/46E/55/56/57/76/86
- CW916x
- MX64/65, MX67/68, MX84/100, MX75/85/95/105, MX250/450
- Z3/4/C
- Secure Web Appliance

* Speaker only

** APs in FlexConnect mode only

アクセス制御 ポリシードメイン

Meraki

Security

SASE/SSE

Cisco Secure Access

Microsoft 365

aws

Google Cloud

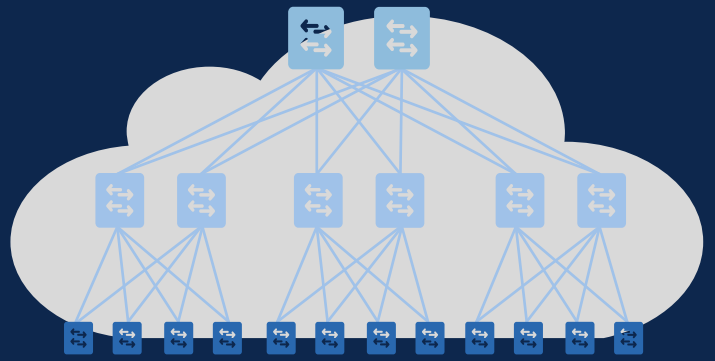
Azure

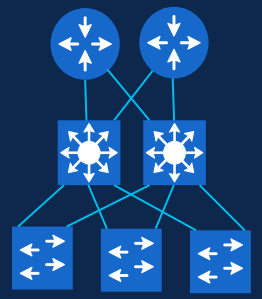
vmware by Broadcom

Cloud and External Services

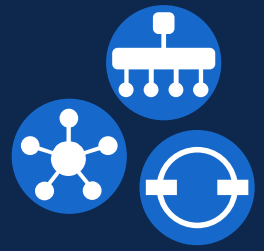
Catalyst Center

SD-Access

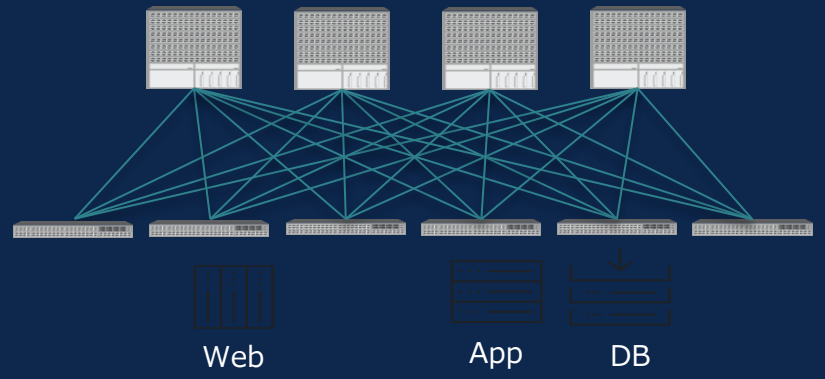




Non-Fabric



SD-WAN



Data Center / ACI

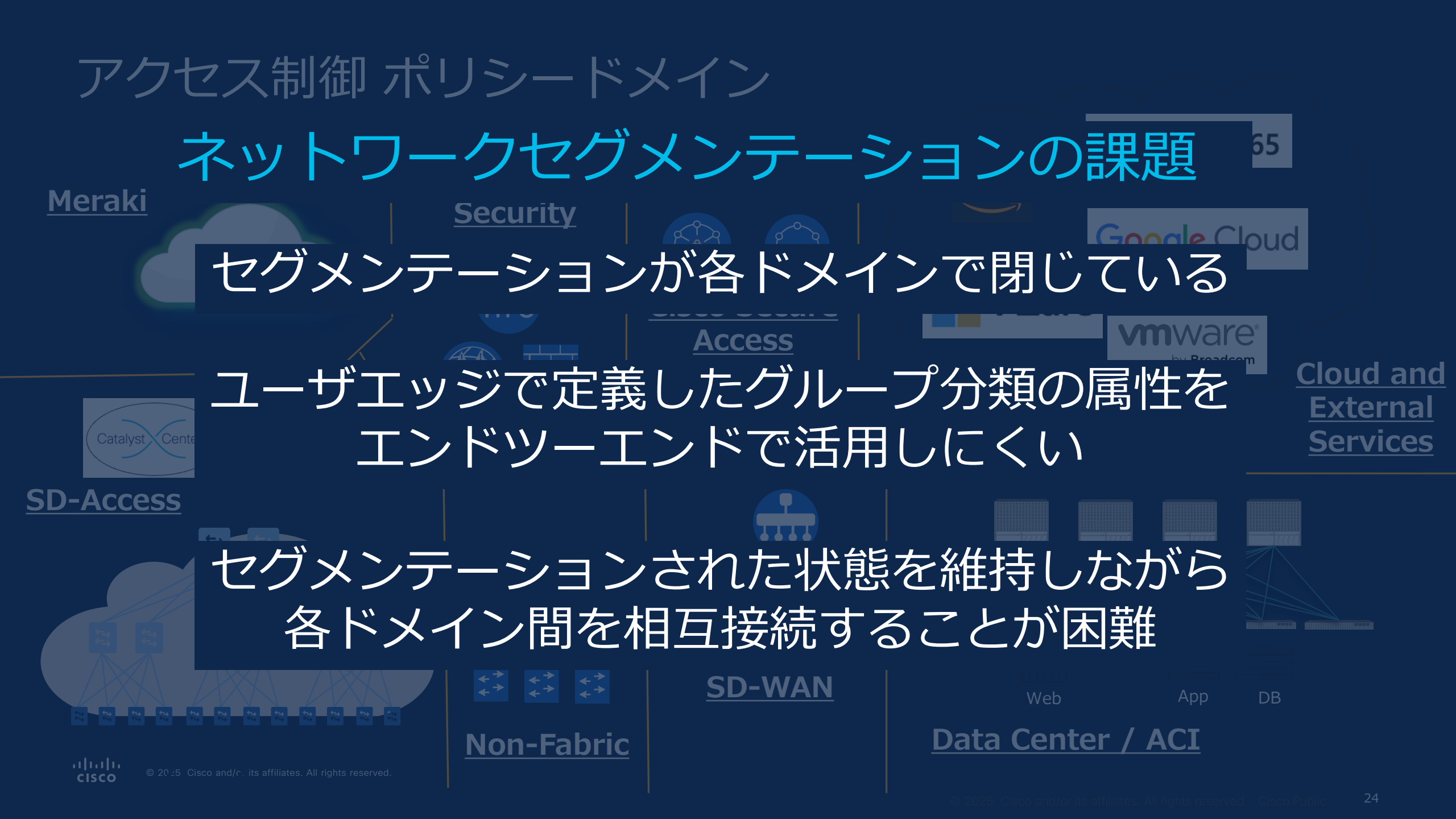
アクセス制御 ポリシードメイン

ネットワークセグメンテーションの課題

セグメンテーションが各ドメインで閉じている

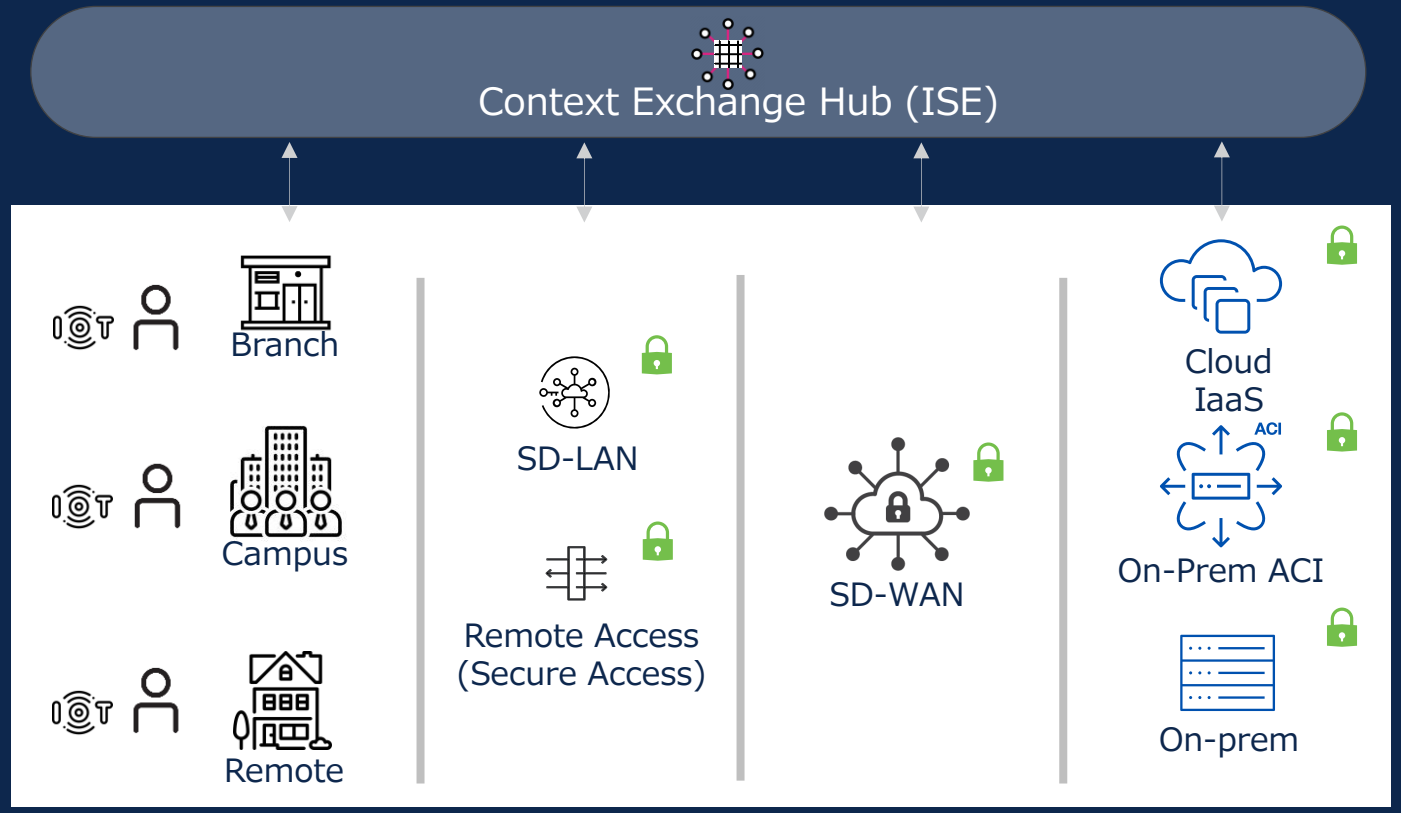
ユーザエッジで定義したグループ分類の属性を
エンドツーエンドで活用しにくい

セグメンテーションされた状態を維持しながら
各ドメイン間を相互接続することが困難



Cisco Common Policy

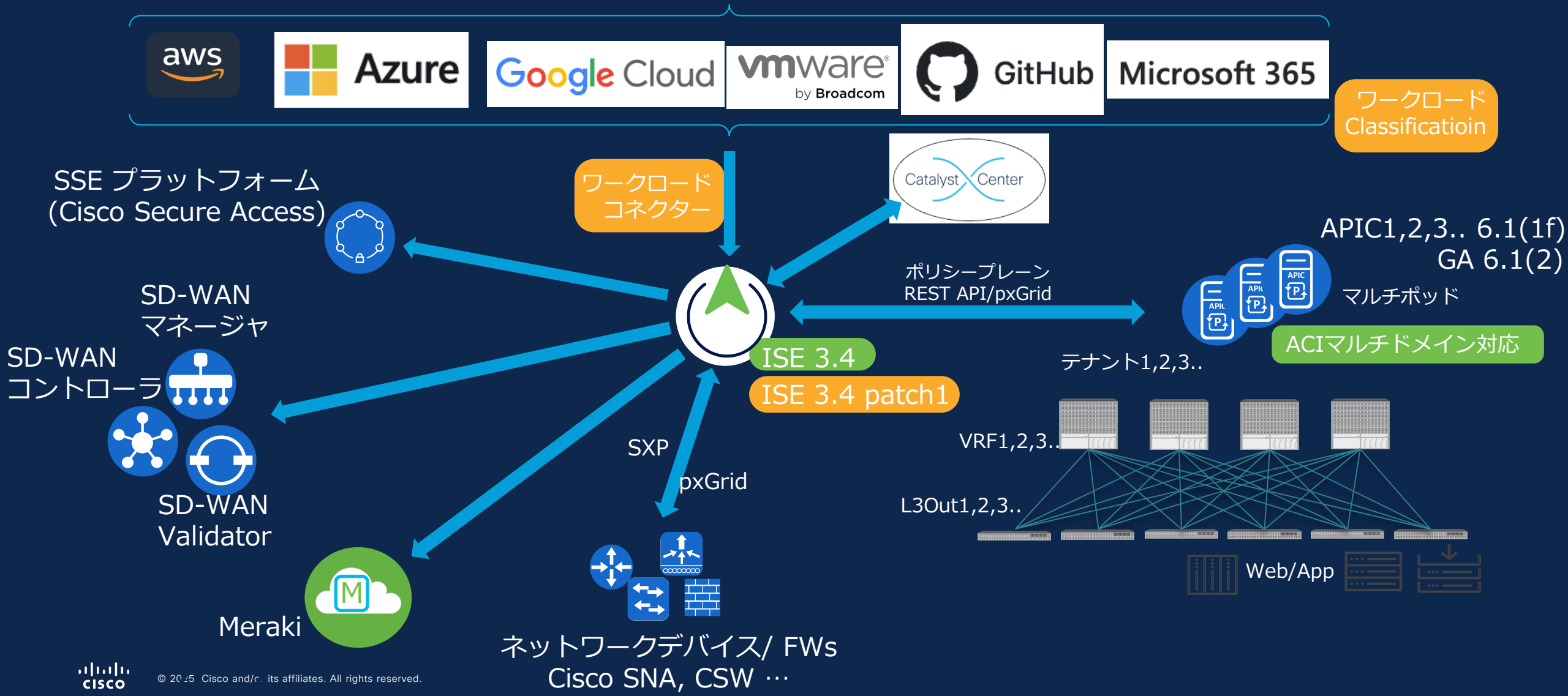
ポリシーエンフォースメントポイント:
一貫したポリシーを適用



- 各ローカルドメインにコンテキストアウェアな環境を構築し、コンテキストを標準のセキュリティグループタグ(SGT)として格納する
- 各ローカルドメインを超えて、あらゆる場所でコンテキストを共有
- タグを活用し、一貫したコンテキストベースのポリシーを各ポリシーエンフォースメントポイントにて適用し、シンプルで統一されたポリシー体験を実現

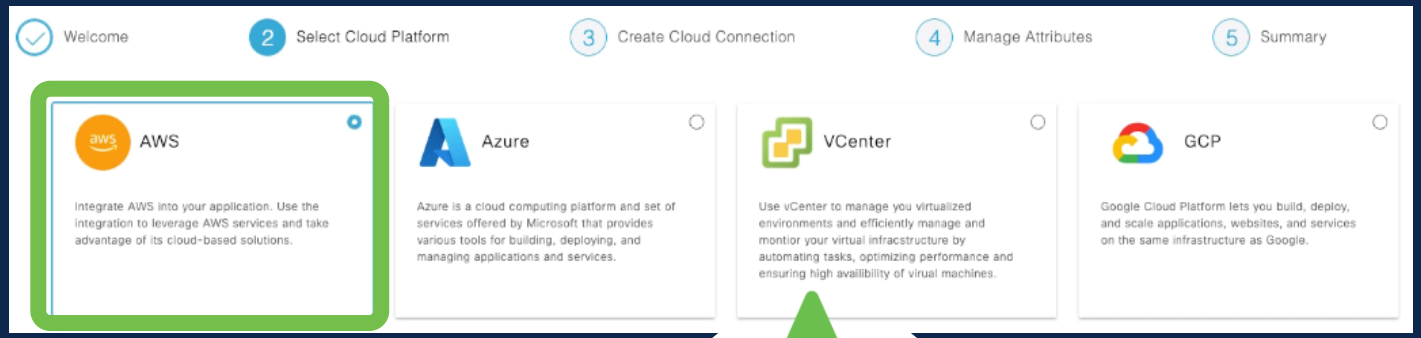
複数のエンフォースメントポイントに対応した、オンプレミスのアプリとクラウドのワークロードのための
コンテキストアウェアポリシー環境を実現

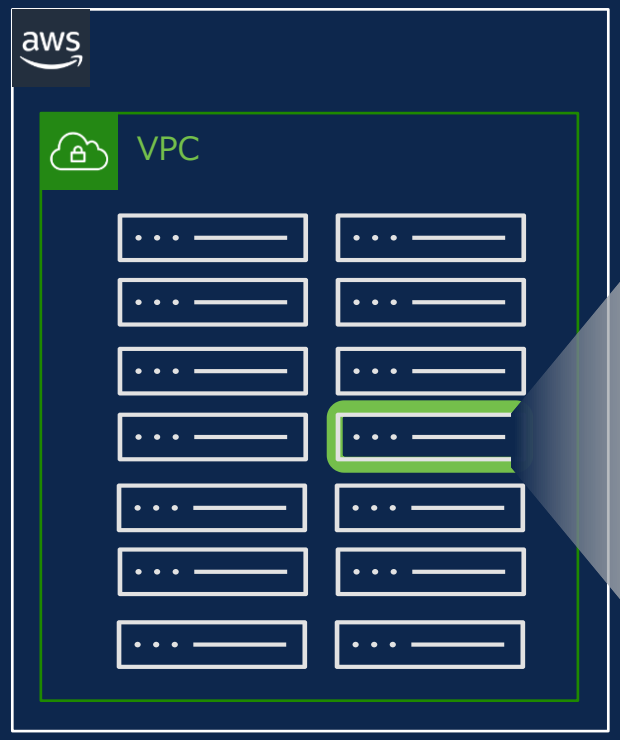
Cisco ISE がドメイン間のポリシーコンテキストハブとして動作



クラウドワークロード情報によるタグ分類

ISE 3.4P1





Workload Attributes
- VPC
- Created
- State
- Name
- Application
- Version
- Owner
- OS
- IP
- Service
- Stage
- …

ISE ディレクトリ
- Name
- Application
- IP
- Service
- Stage

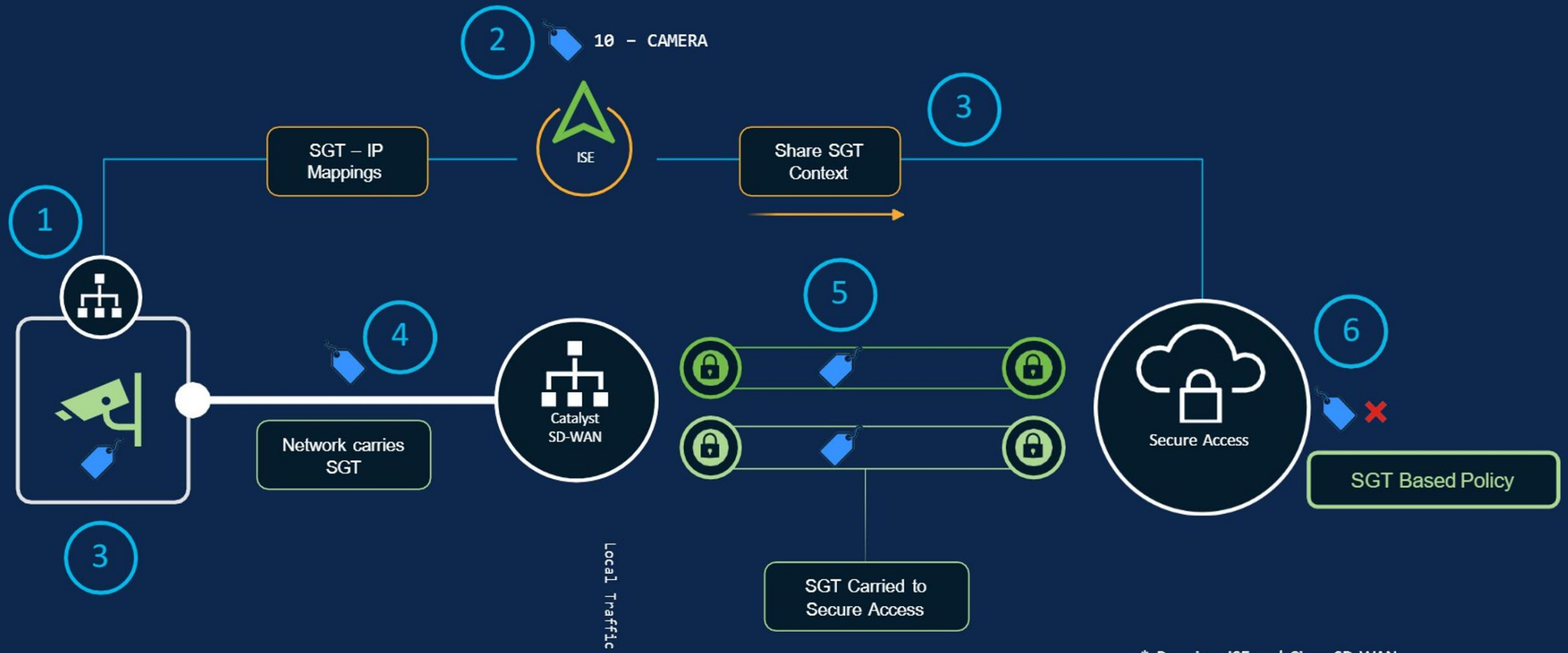
ISE

分類ポリシ

- プライマリ SGT
- セカンダリ SGT
- SXP: SGT-to-IP

サポート済み

Cisco Secure Access と Cisco ISEの連携 (1/2)



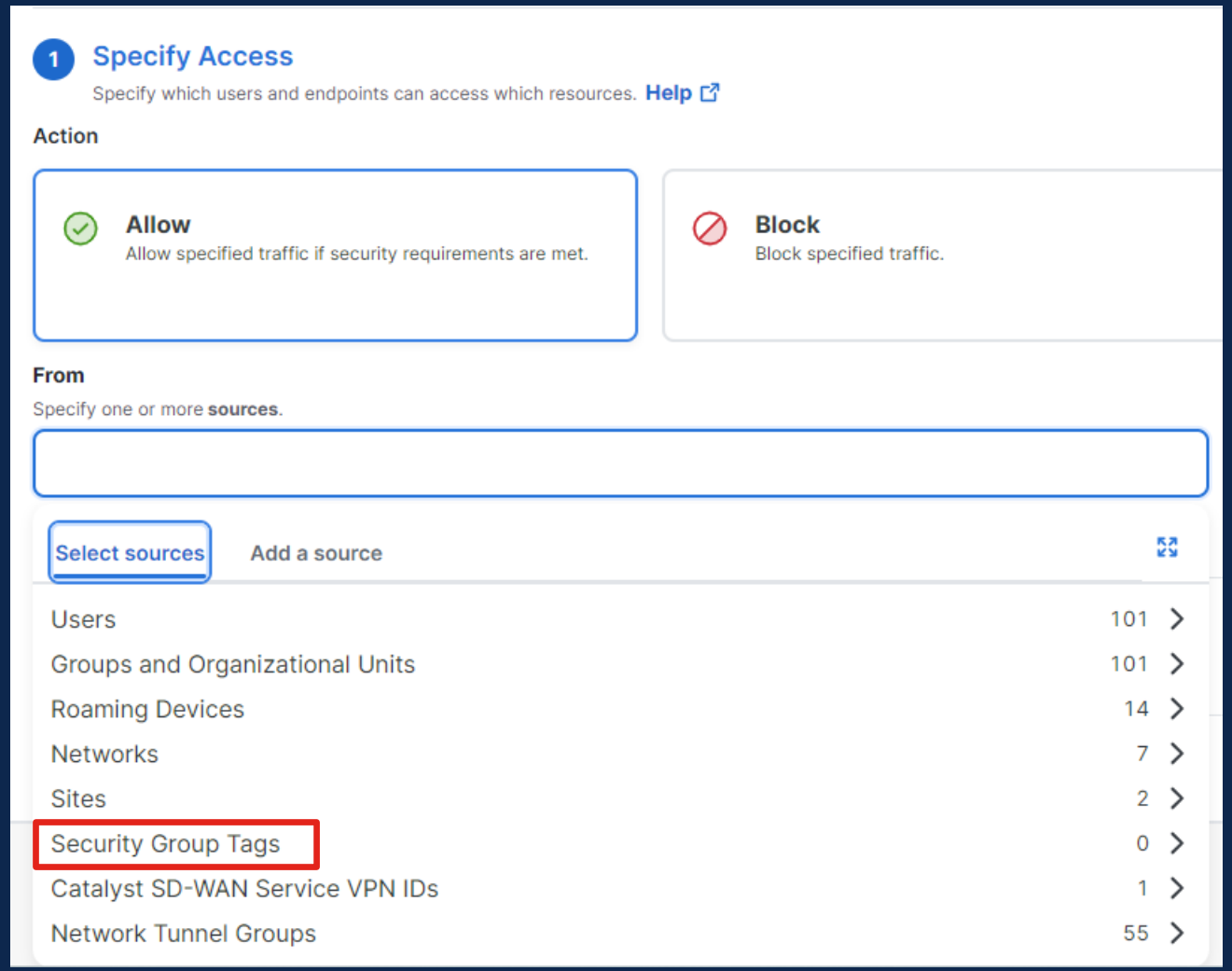
ユースケース例 : IoT デバイスの通信を識別してSSEで制御

サポート済み

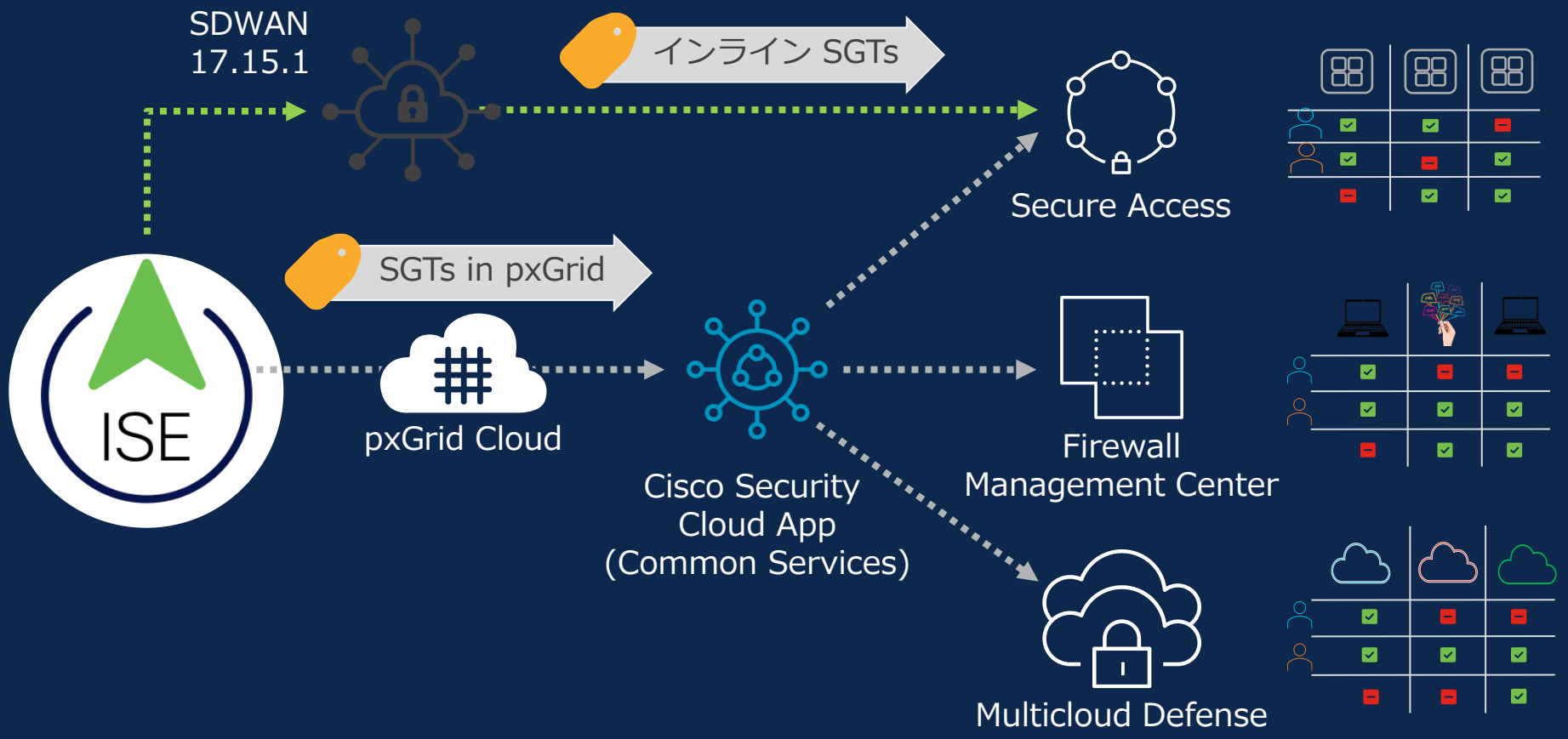
Cisco Secure Access と Cisco ISEの連携 (2/2)

ISE を使用してネットワーク内のトラフィックの分類にセキュリティグ ループタグ (SGT) を定義および使用する場合、Secure Access アクセス制御ルールのソース照合基準として SGT の選択が可能

これにより、IP アドレスやネットワーク オブジェクトではなく、セキュリティ グループ メンバーシップに基づいてアクセスをブロックまたは許可することが可能



Cisco セキュリティクラウドサービスへのコンテキスト共有

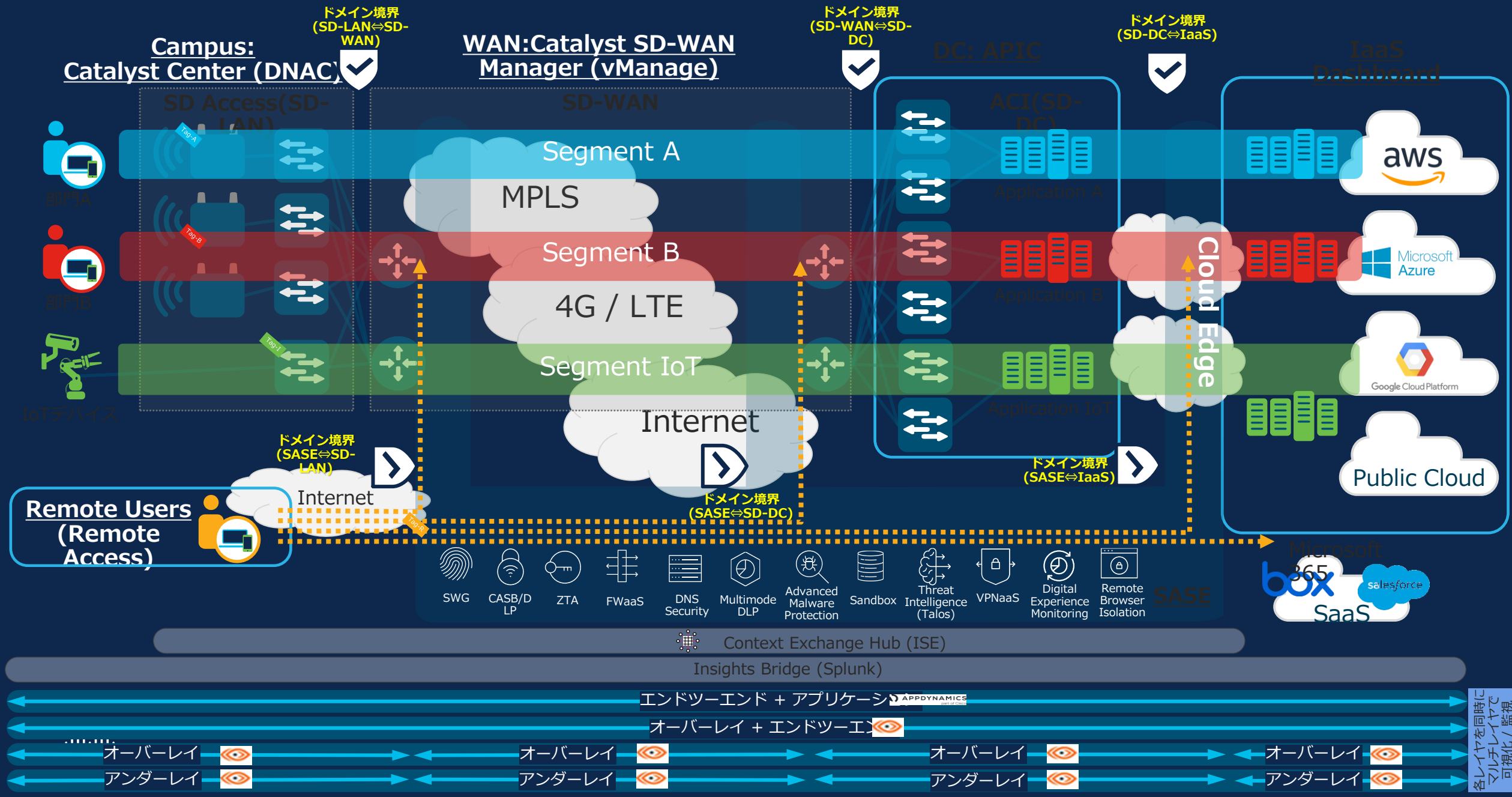


サポート済み

機能拡張予定
※ FMCとオンプレISE連携は対応済み

Security Group Tags (SGTs) は オンプレミスネットワークとセキュリティサービスの共通言語へ

マルチドメイン・コモンポリシー・マルチレイヤマネージメントへ




CISCO