Cisco
Customer Experience

Ask the Experts

スタートアップガイド：ISE の製品概要
（Getting Started: Product Overview ISE）

Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

本日の学習内容：

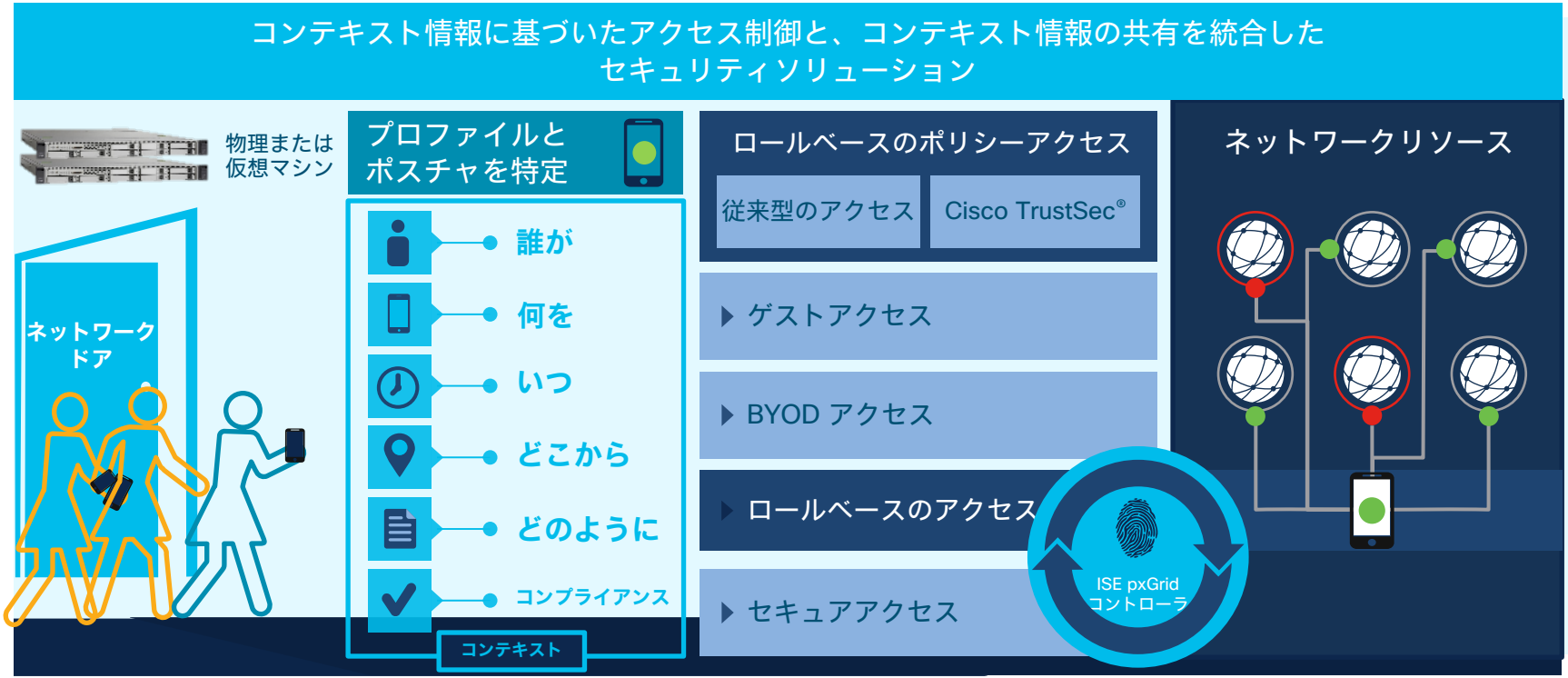
- Cisco ISE の主な機能
- Cisco ISE の認証および認可オプションの概要
- Cisco ISE プロファイリングとポスチャのさまざまな要素
- Cisco ISE でサポートされているセキュアアクセスのシナリオ

本日のトピック

1. Cisco ISE の紹介
2. セキュアアクセスの基礎
3. デモ：ポリシーの概要
4. ISE コンテキストと
   セキュアアクセスのシナリオ
5. デモ：ゲストアクセス

Cisco ISE の紹介

Cisco Identity Services Engine（ISE）の紹介



ISE のペルソナ

スタンドアロン ISE

ポリシー管理ノード（PAN）

- ISE 管理向けの一元管理機能
- すべての設定を変更できる複製ハブ

モニタリングおよびトラブルシューティング ノード（MnT）

- ノードのレポートとログの取得
- ISE ノードの Syslog コレクタ

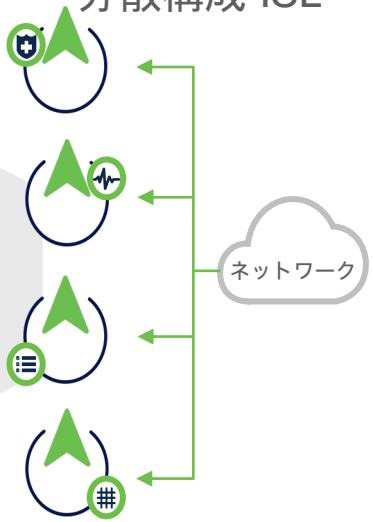
ポリシーサービスノード（PSN）

- ポリシー決定の実行
- RADIUS / TACACS+ サーバ

pxGrid コントローラ

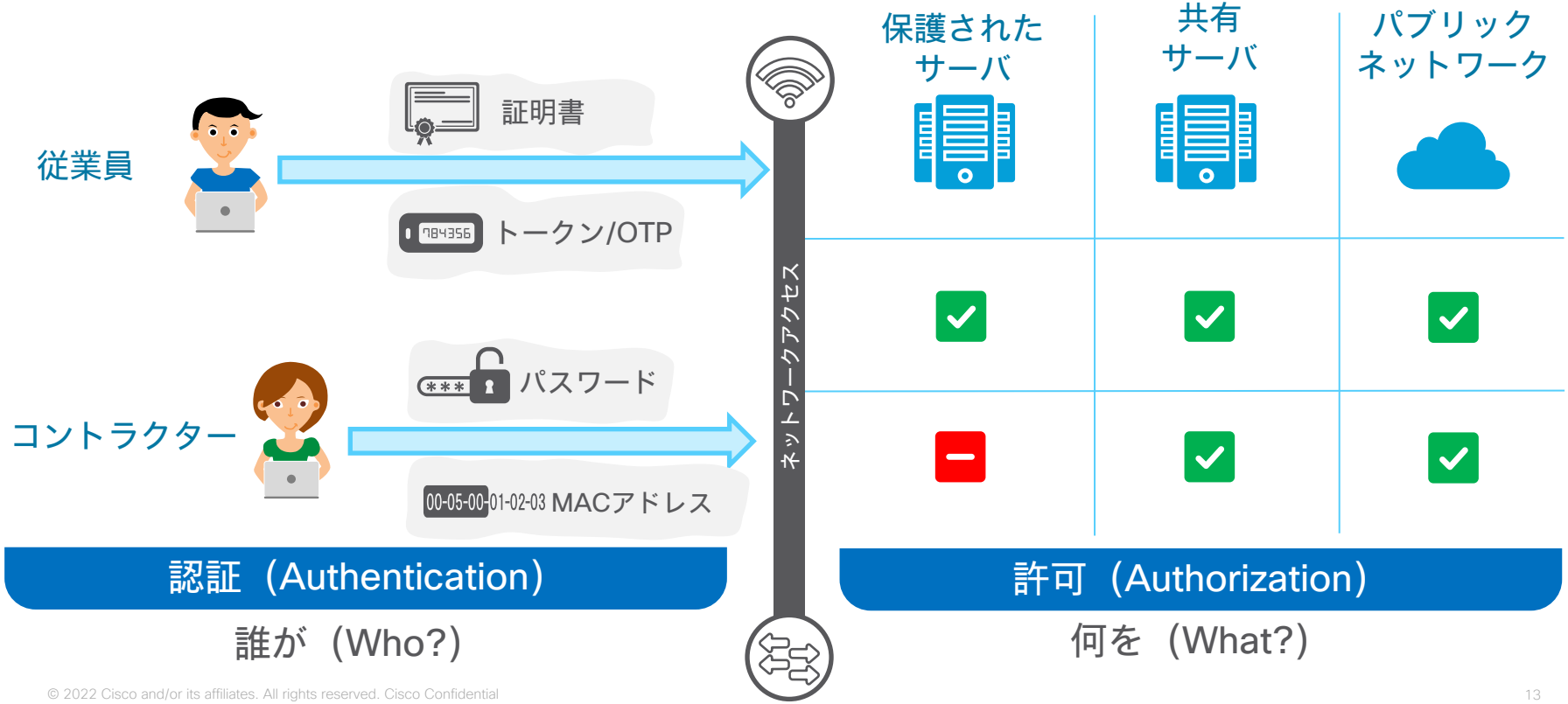
- コンテキストの共有を促進

分散構成 ISE

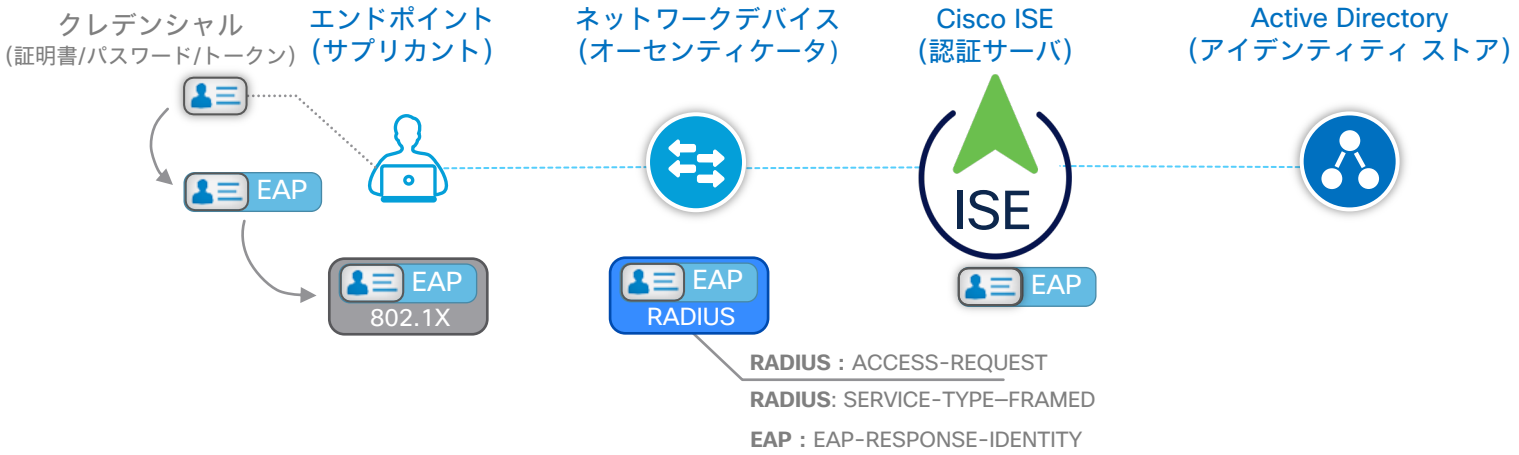


セキュアアクセスの基礎

ネットワーク アクセス コントロール



ISE 認証
802.1X の基礎

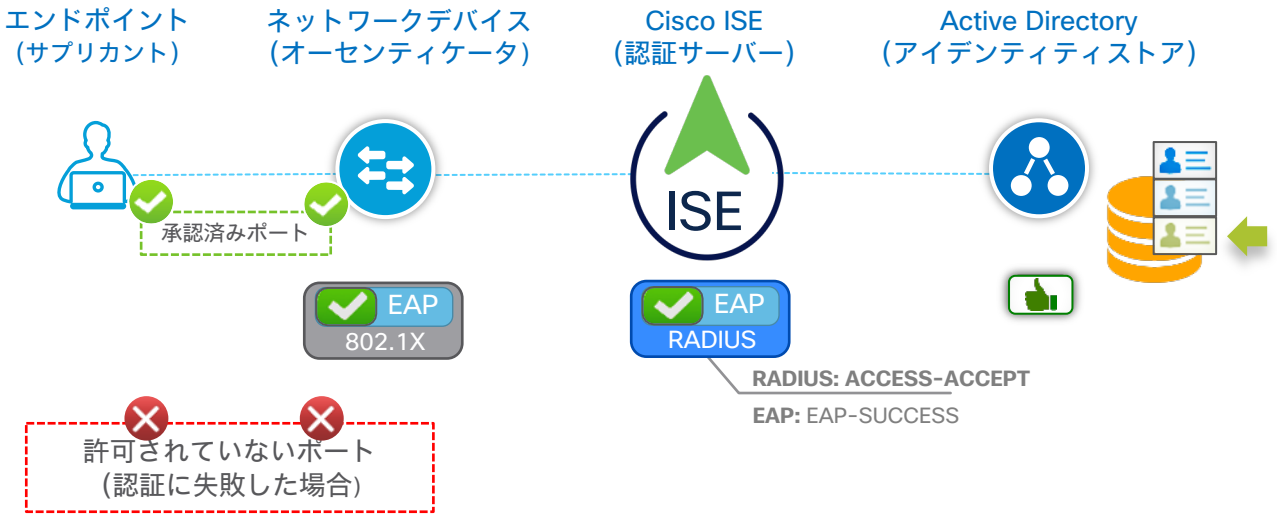


EAP：拡張認証プロトコル（Extensible Authentication Protocol）

サプリカント：オーセンティケータ（ネットワークデバイス）にクレデンシャルを提供するクライアントで実行されるソフトウェア

ISE 認証（続き）

802.1X の基礎

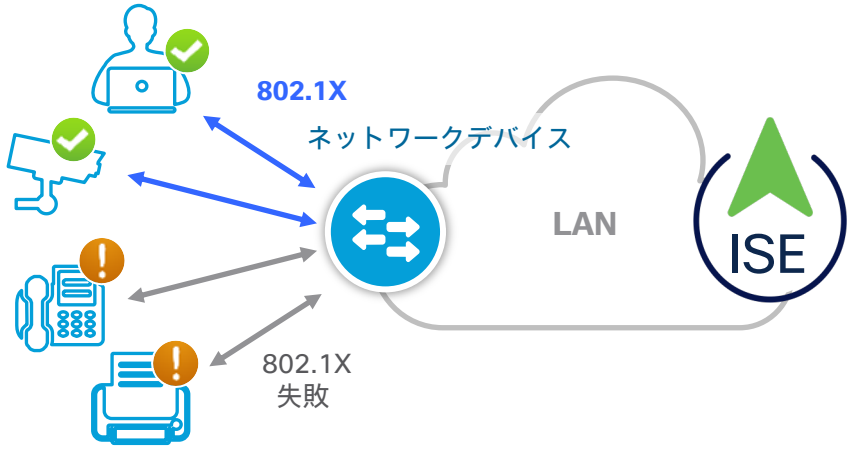


EAP：拡張認証プロトコル（Extensible Authentication Protocol）

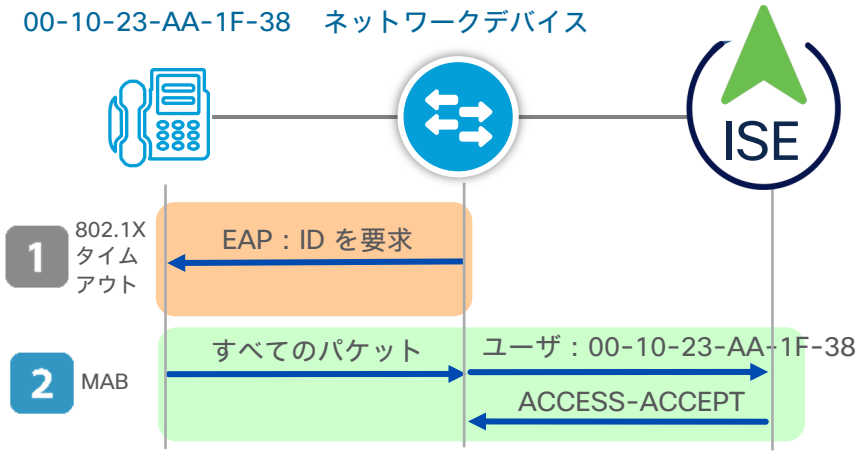
サプリカント：オーセンティケータ（ネットワークデバイス）にクレデンシャルを提供するクライアントで実行されるソフトウェア

ISE 認証
MAC 認証バイパス（MAB）

サプリカントのないエンドポイントは 802.1X の認証に失敗

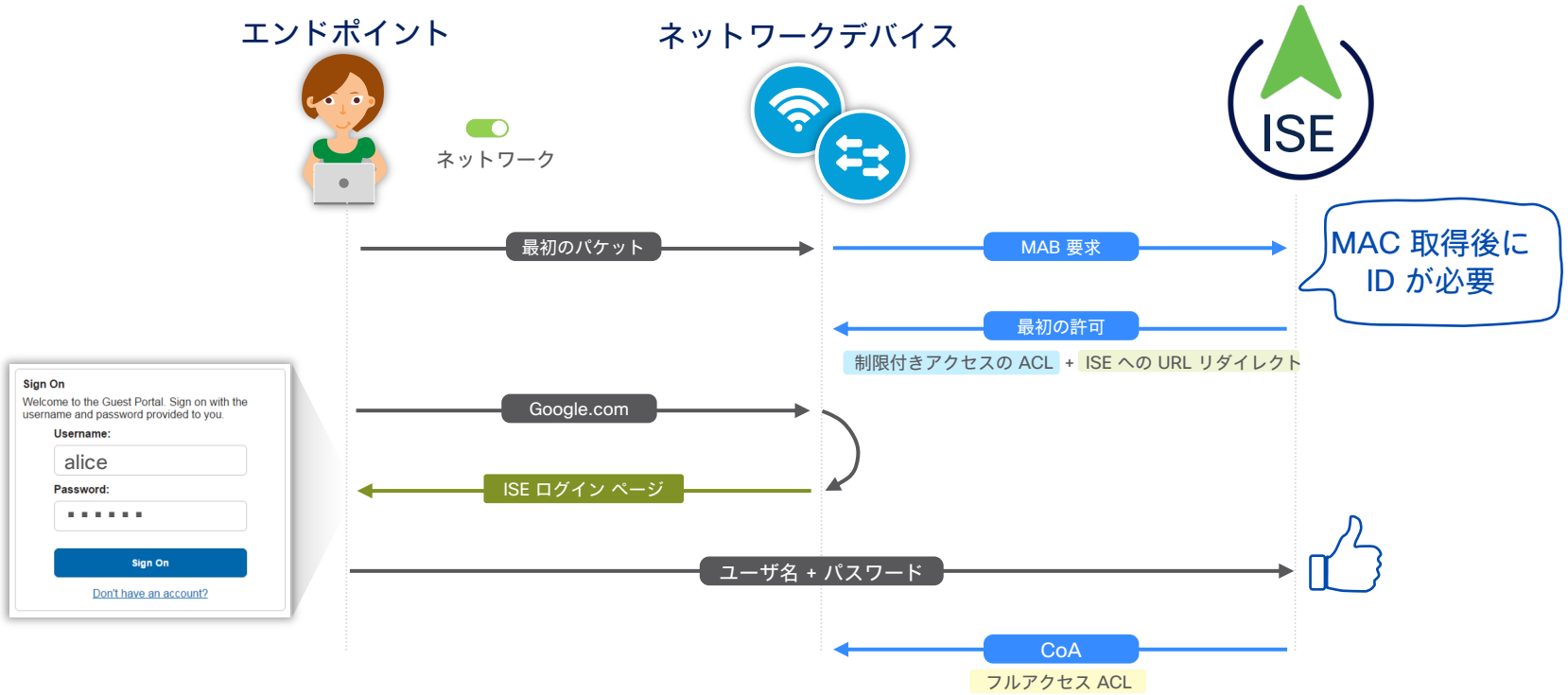


*既知*の MAC アドレスのバイパス

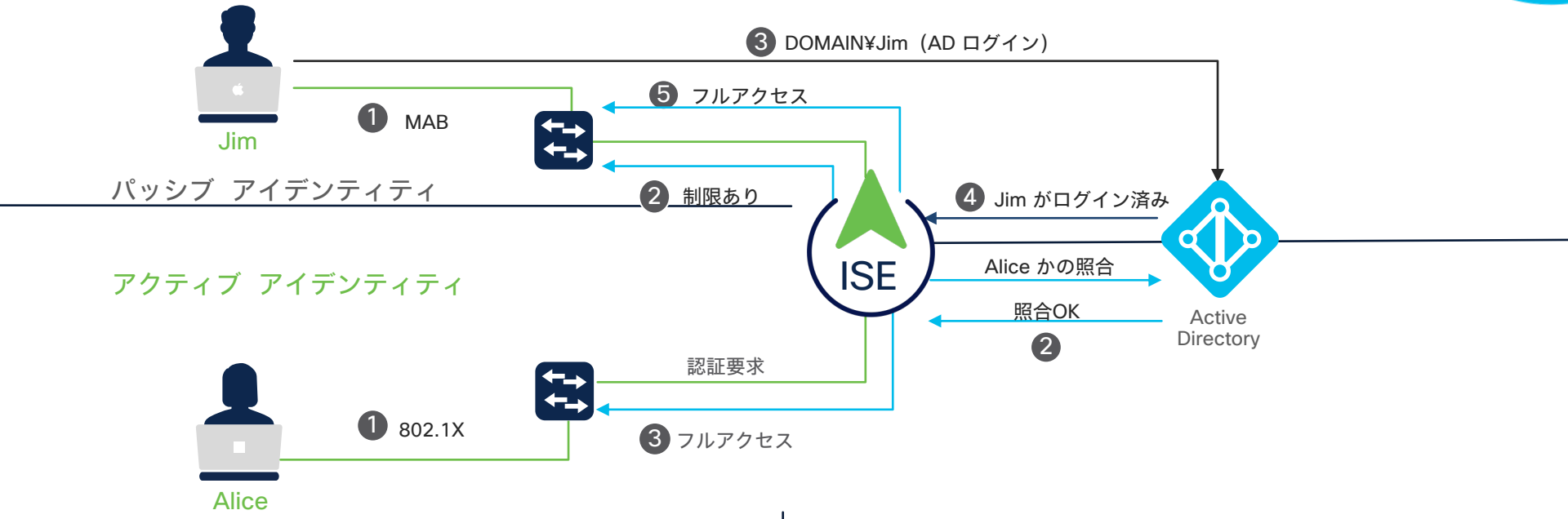


MAB が MAC データベースを要求 | ISE はMAC データベースを動的に作成

ISE 認証
セントラル Web 認証（CWA）



アクティブ アイデンティティと パッシブ アイデンティティ



アクティブ アイデンティティ

ISE とクライアント間のユーザマッピングへの IP は 、RADIUS と一緒に**802.1X**、**Web 認証**、**リモートアクセス VPN** などを経由

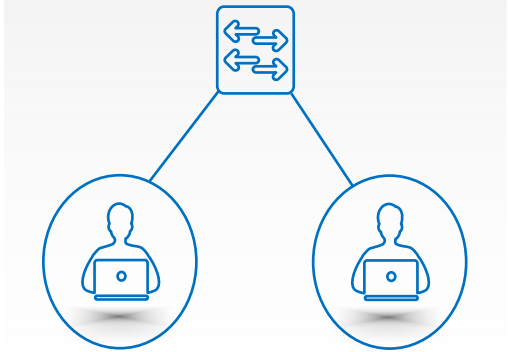
パッシブ アイデンティティ

パッシブ方式を介したユーザマッピングへの IP は、Active Directory によるイベント API、**WMI イベント**、Active Directory エージェント、**Syslog**、**SPAN** セッションなど

ISE 認可
RADIUSに加えて

DACL または名前付き ACL

ダウンロード可能な ACL（有線）または
名前付き ACL（有線+ワイヤレス）

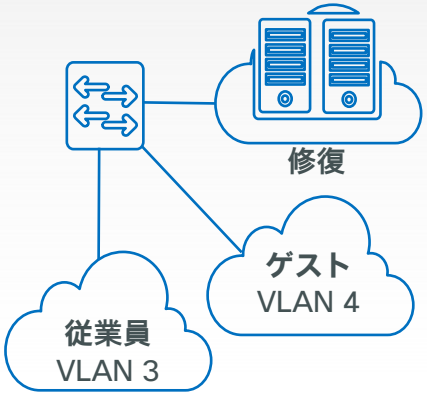


従業員
permit ip
any Ip

コントラクター
deny ip host
<protected>
permit ip any Ip

VLAN

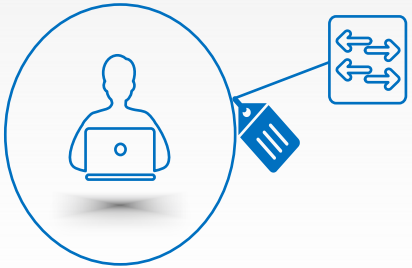
ダイナミック VLAN 割り当て



ポート単位 / ドメイン単位 /
MAC 単位

セキュリティ グループ タグ

Cisco TrustSec

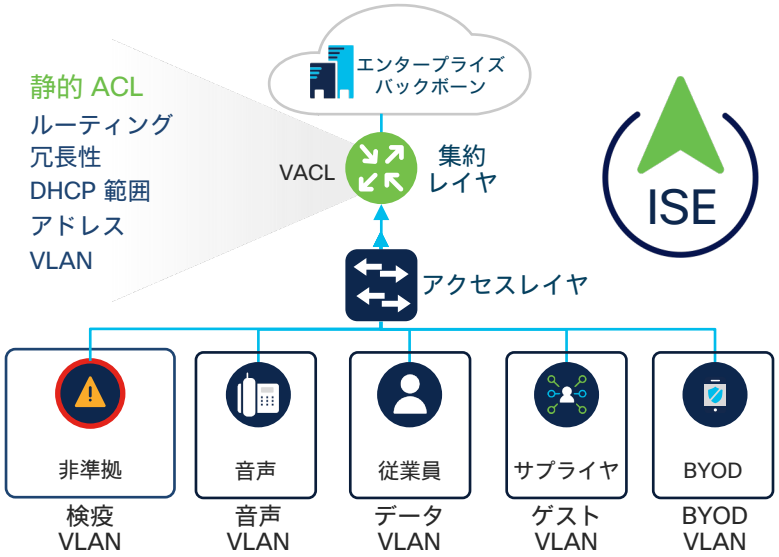


16 ビット SGT 割り当てと
SGT ベースのアクセス制御

グループベースのポリシーで セグメンテーションを簡素化

従来のセグメンテーション

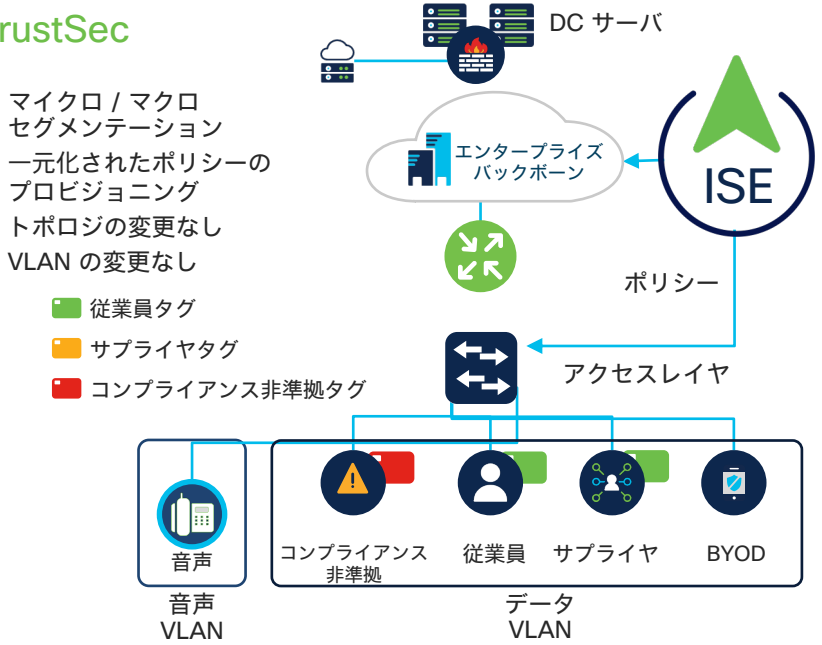
静的 ACL
ルーティング
冗長性
DHCP 範囲
アドレス
VLAN



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

TrustSec

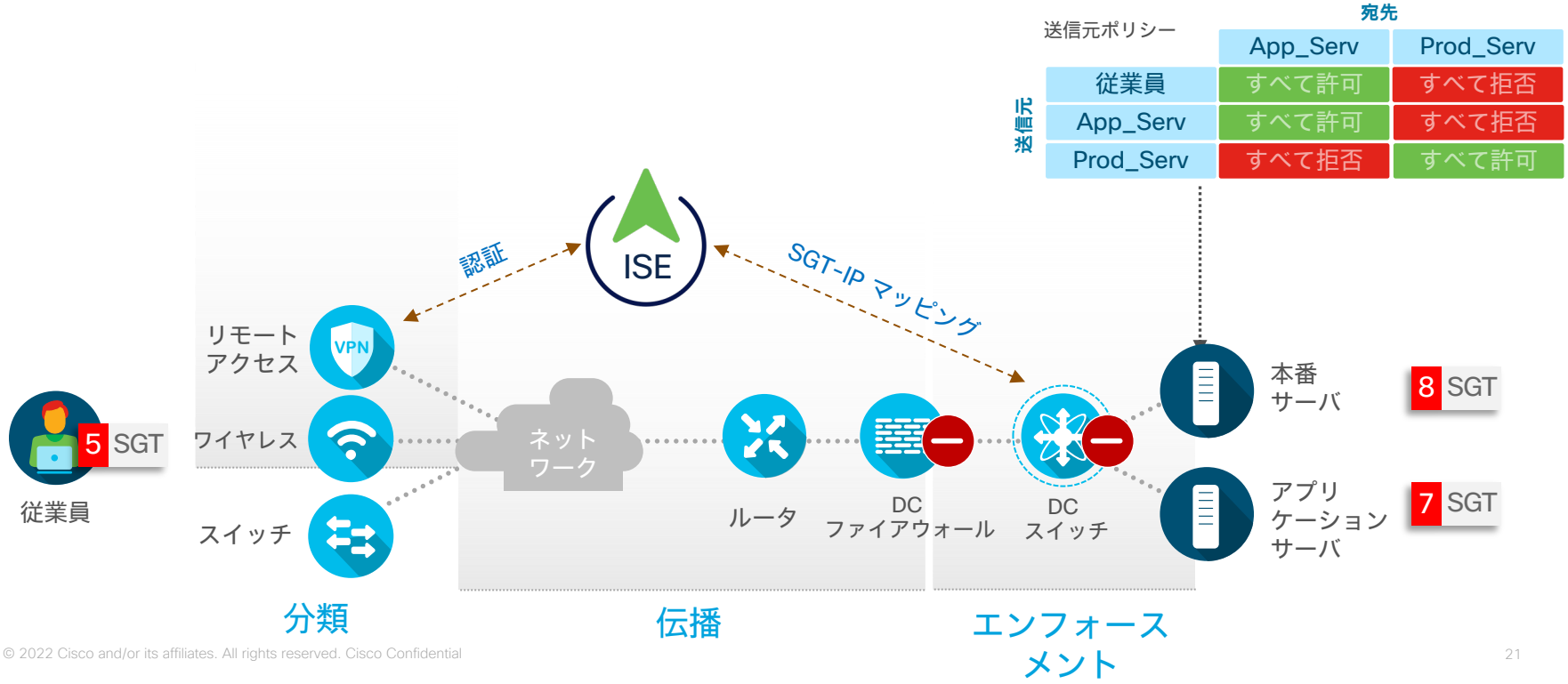
マイクロ / マクロ
セグメンテーション
一元化されたポリシーの
プロビジョニング
トポロジの変更なし
VLAN の変更なし



既存のトポロジを活用したセキュリティポリシーの
自動化で運用コストを削減

Cisco TrustSec

セキュリティ グループ タグ（SGT）でのセグメント化



ISE コンテキストとセキュアアクセスのシナリオ

- プロファイリング
- ゲスト
- BYOD
- ISE 準拠：ポスチャ

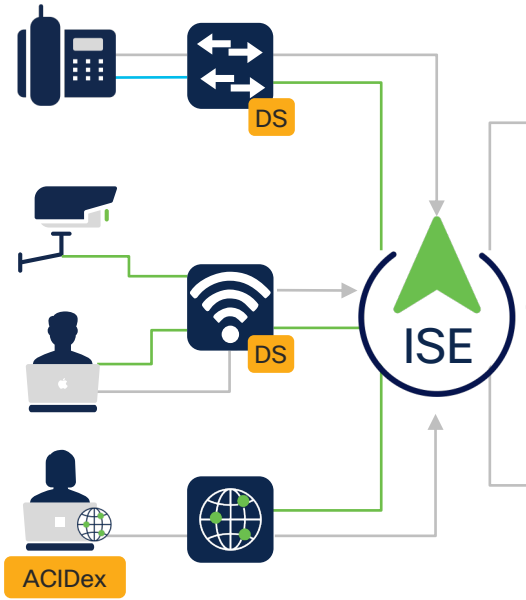
Cisco ISE がこれらすべてを把握する仕組み

Cisco ISE では、誰が、何を、いつ、どこで、どのように行うかを把握

プローブによるコンテキストの構築

Cisco ISE のプロファイリングサービスが、ネットワークに接続されているデバイスを識別

エンドポイントが、
デバイスタイプを
示す関連データを送信



デバイス プロファイリング向けの ISE データ収集メソッド

アクティブなプローブ：Netflow | DHCP | DNS | HTTP | RADIUS | NMAP | SNMP | AD

デバイスセンサー：CDP| LLDP | DHCP | HTTP | H323 | SIP | MDNS

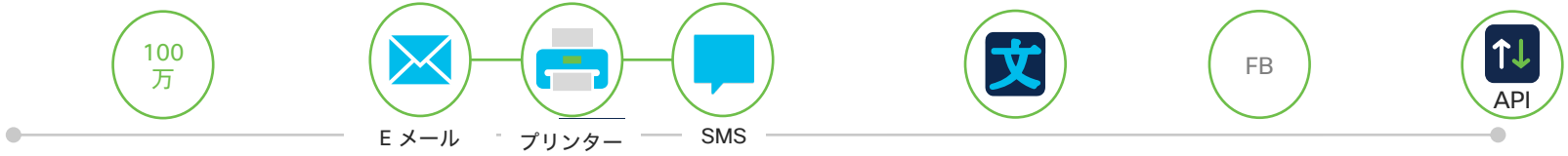
AnyConnect：ACIDex

フィードサービス
（オンライン / オフライン）

MAC Address	IPv4 Address	Username	Hostname	Endpoint Profile
00:22:BD:D3:5B:2F	10.34.75.13			Cisco-IP-Camera
00:02:4B:CC:D6:63	10.35.68.203			Cisco-IP-Phone
5C:F9:38:AA:1F:90	10.32.2.127	jim	Jim-Air	Apple-MacBook
30:46:9A:2E:C3:F0	10.86.98.138	host/ALICE	win7pc	Microsoft-Workstation

AnyConnect Identity Extension（ACIDex）| デバイス センサー（DS）

ゲストアクセスの概要



サポートされる
ゲストアカウント数

ゲストアカウントの
通知オプション

ポータル言語の
カスタマイズ

ソーシャルメディアの
ログインサポート

REST によるゲスト
アカウントの管理

3 種類のゲストアクセス

ホットスポット

ログイン情報不要の即時
インターネットアクセス

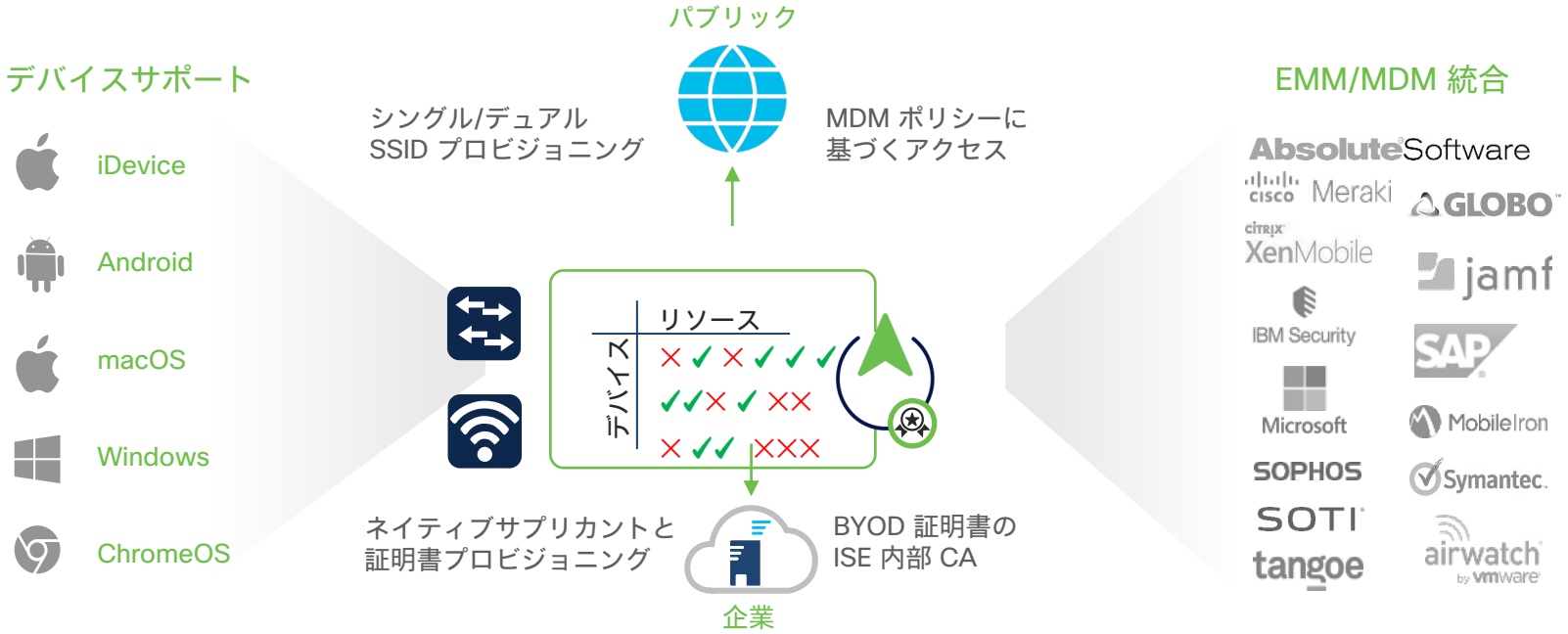
セルフ登録

ゲストによるセルフ登録、
スポンサーによるアクセス承認可能

スポンサー承認型ゲストアクセス

認定スポンサーがアカウントを
作成し、クレデンシャルを共有

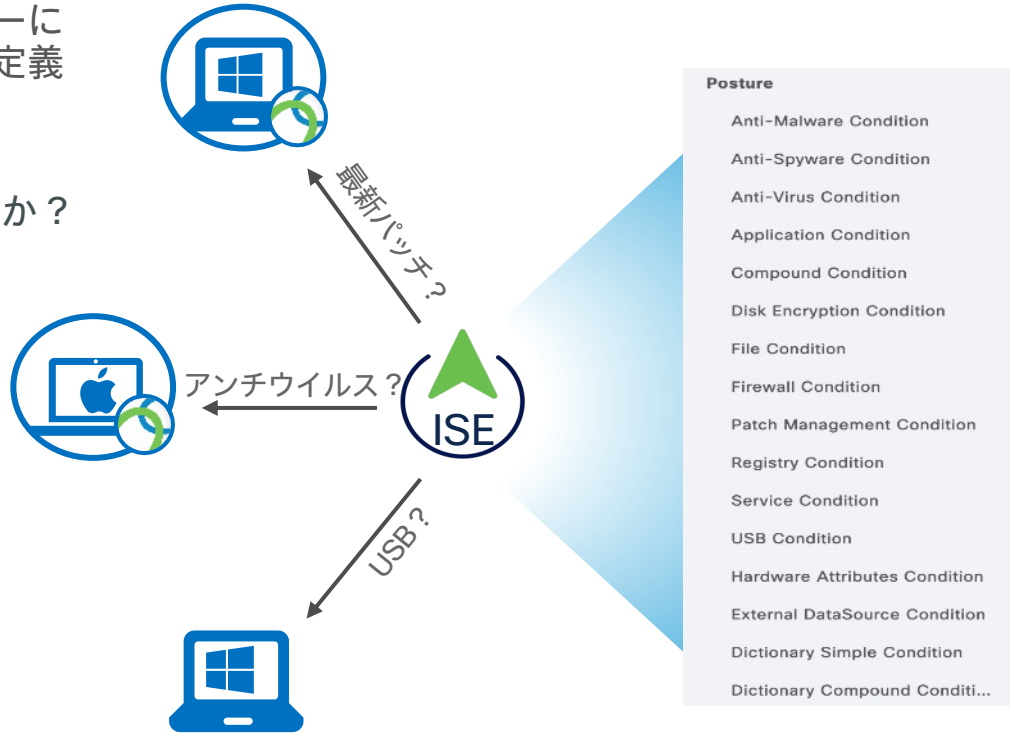
Bring Your Own Device (BYOD： 個人所有デバイス持ち込み)



EMM：エンタープライズモビリティ管理 | MDM：モバイルデバイス管理

ポスチャとは？

- ポスチャが企業のセキュリティポリシーに対するコンプライアンス遵守の状況を定義
  - システムは最新の Windows パッチを実行しているか？
  - 最新のウィルス対策ソフトはインストールされているか？
  - 最新のスパイウェア対策ソフトウェアがインストールされているか？



キーポイント

ISE は 4 つのペルソナで構成される

ISE はさまざまな認証および認可オプションをサポート

ISE はプロファイリングを使用してネットワークに関するコンテキストを取得

ISE はゲストアクセスと BYOD をサポート

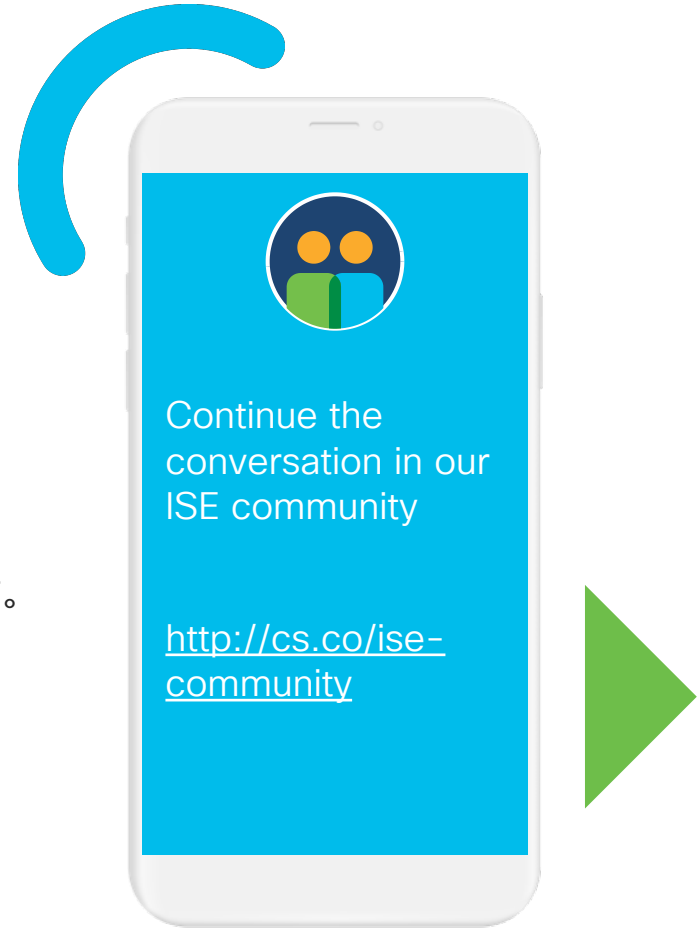
ISE のポスチャ機能によりクライアント端末のコンプライアンスポリシーを提供

Resources

Cisco ISE お役立ちリンク集

https://community.cisco.com/t5/-/-/ta-p/4527229

※本日のATXs以外のリソースリンクも確認できます。




Cisco
Customer Experience