セッションに関するご質問

アンケートフォームにご記入ください。

担当営業やシスココンタクトセンターまでにお問い合わせください。

今後のシスコセキュリティウェビナー

https://www.cisco.com/c/ja_jp/training-events/events-webinars/webinars.html

毎週木曜日開催を予定。

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

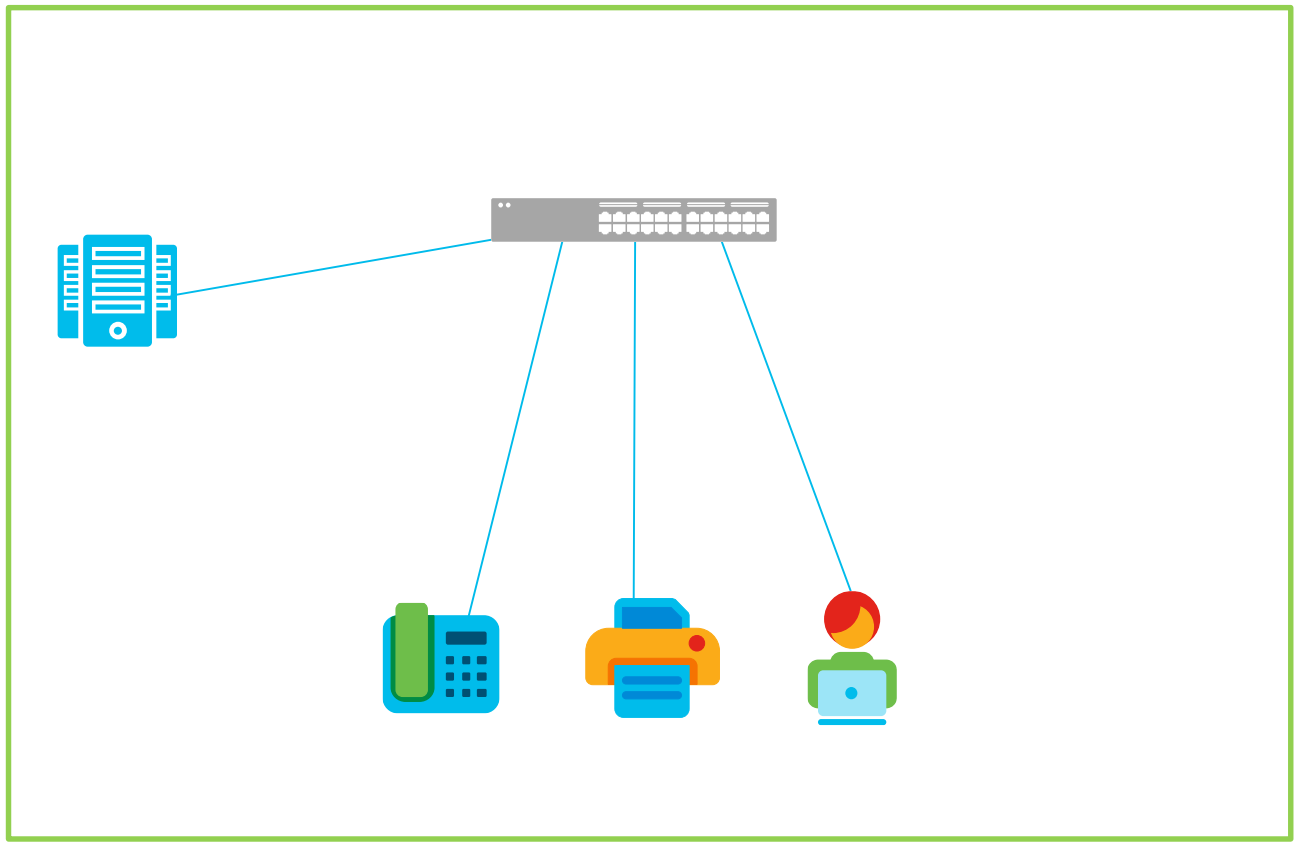
cisco Secure

30分でわかる ネットワークポリシー制御

シスコウェビナー セキュリティシリーズ

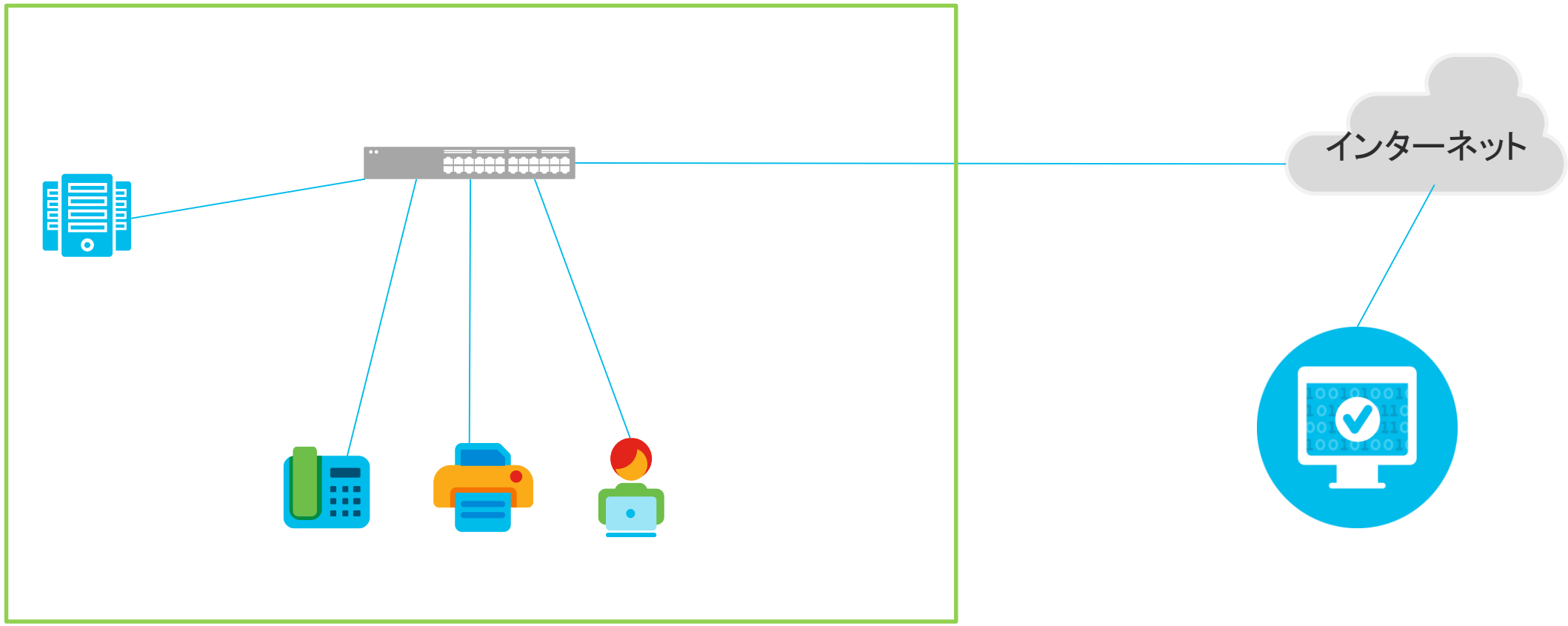
シスコシステムズ合同会社
浅井達也
2020年 6月25日

ワークプレイスのIT化



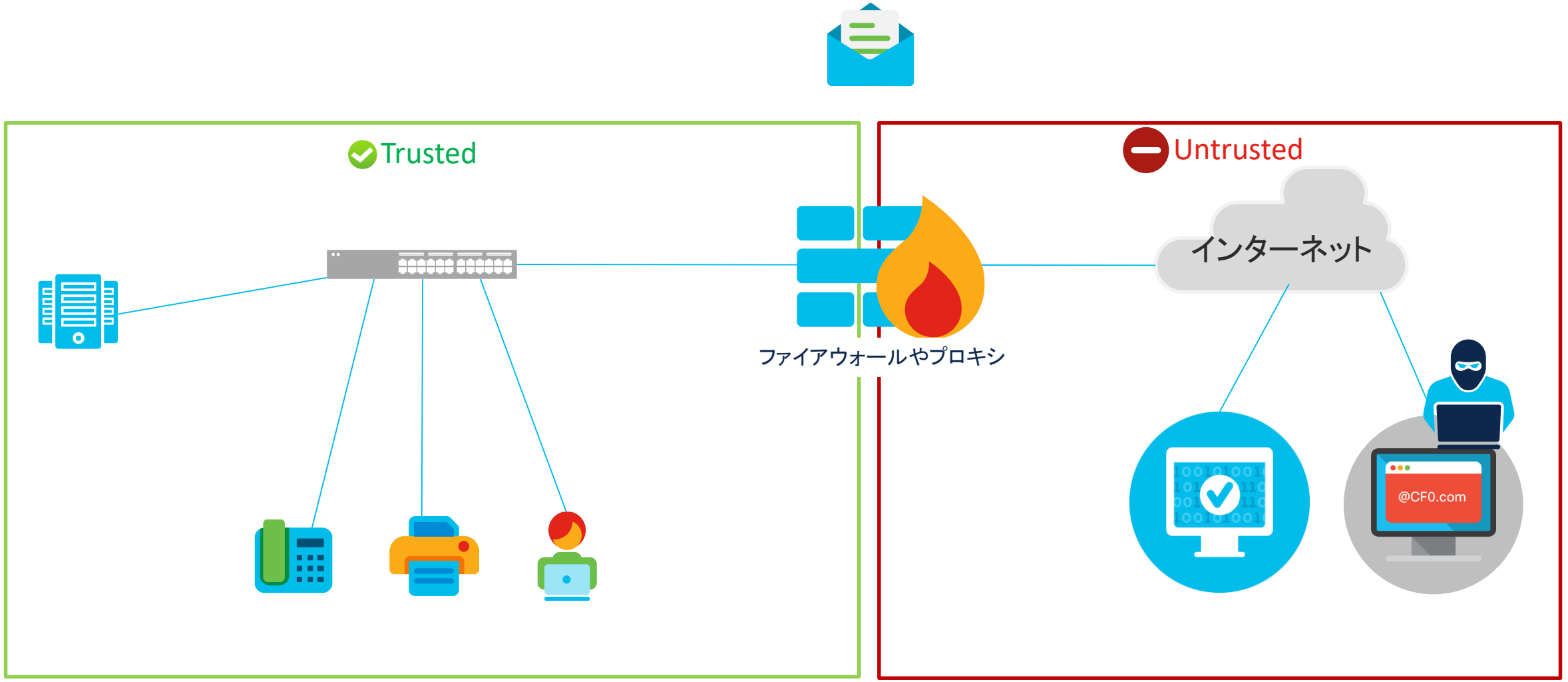
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

インターネットの業務への利用



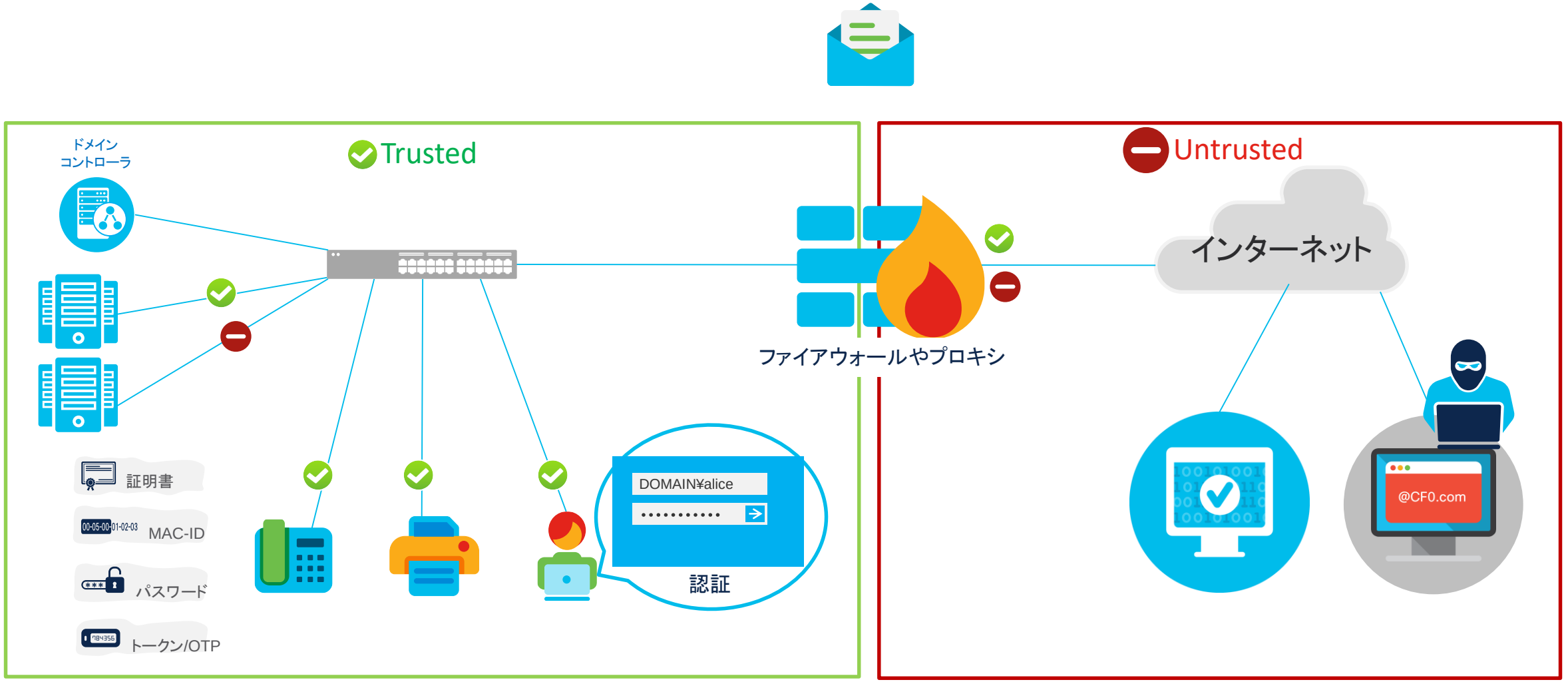
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

セキュリティ境界



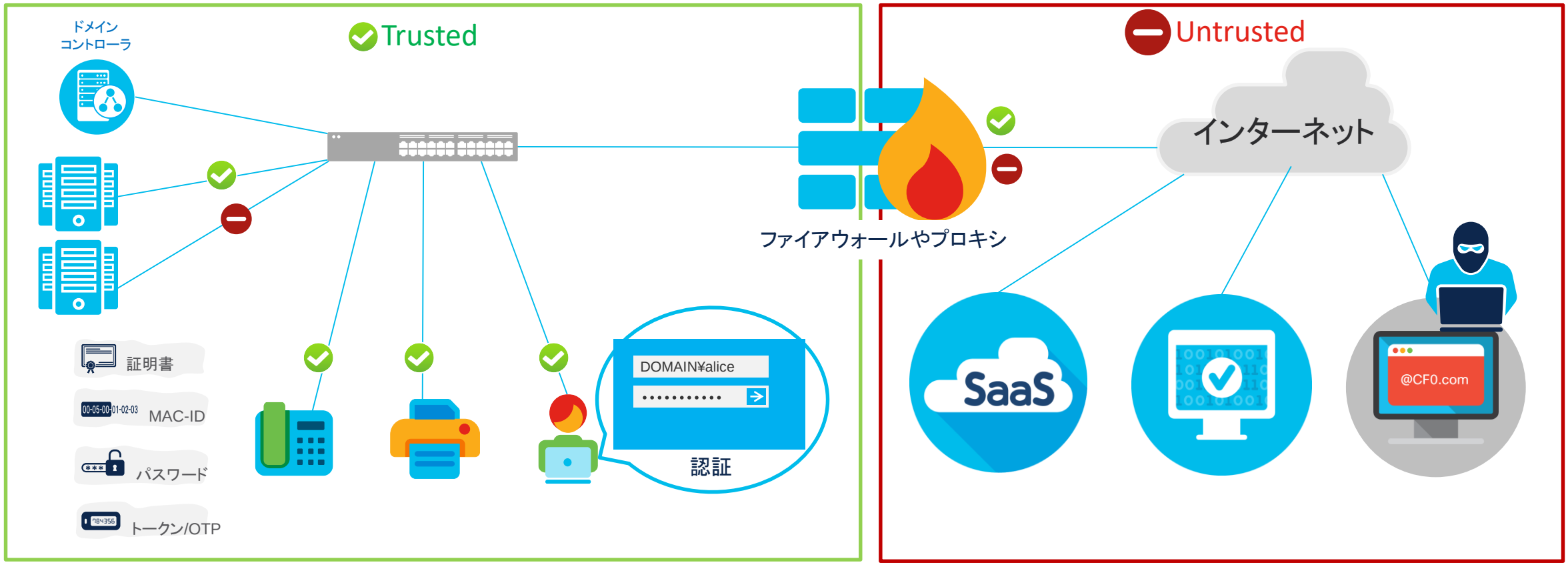
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

業務のIT化が進む



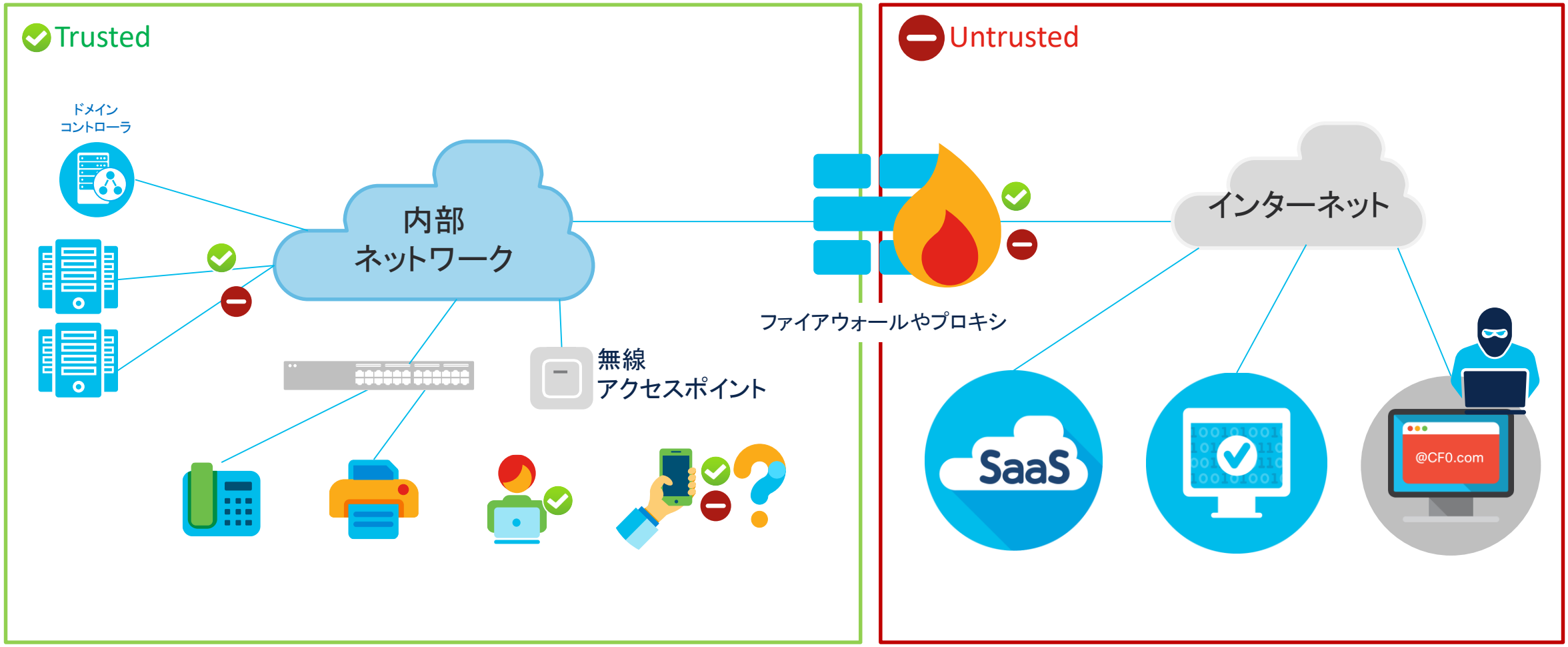
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

インターネット利用の急増



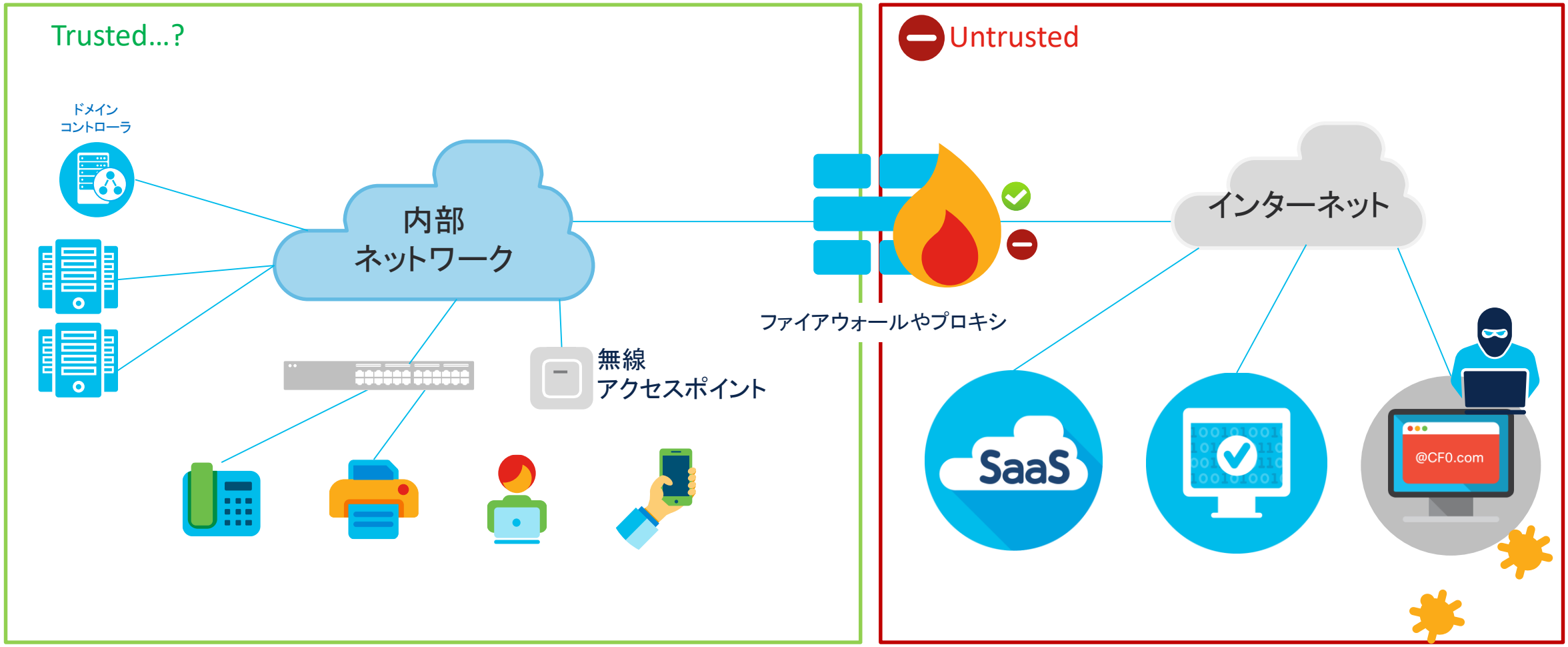
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

端末の多様化



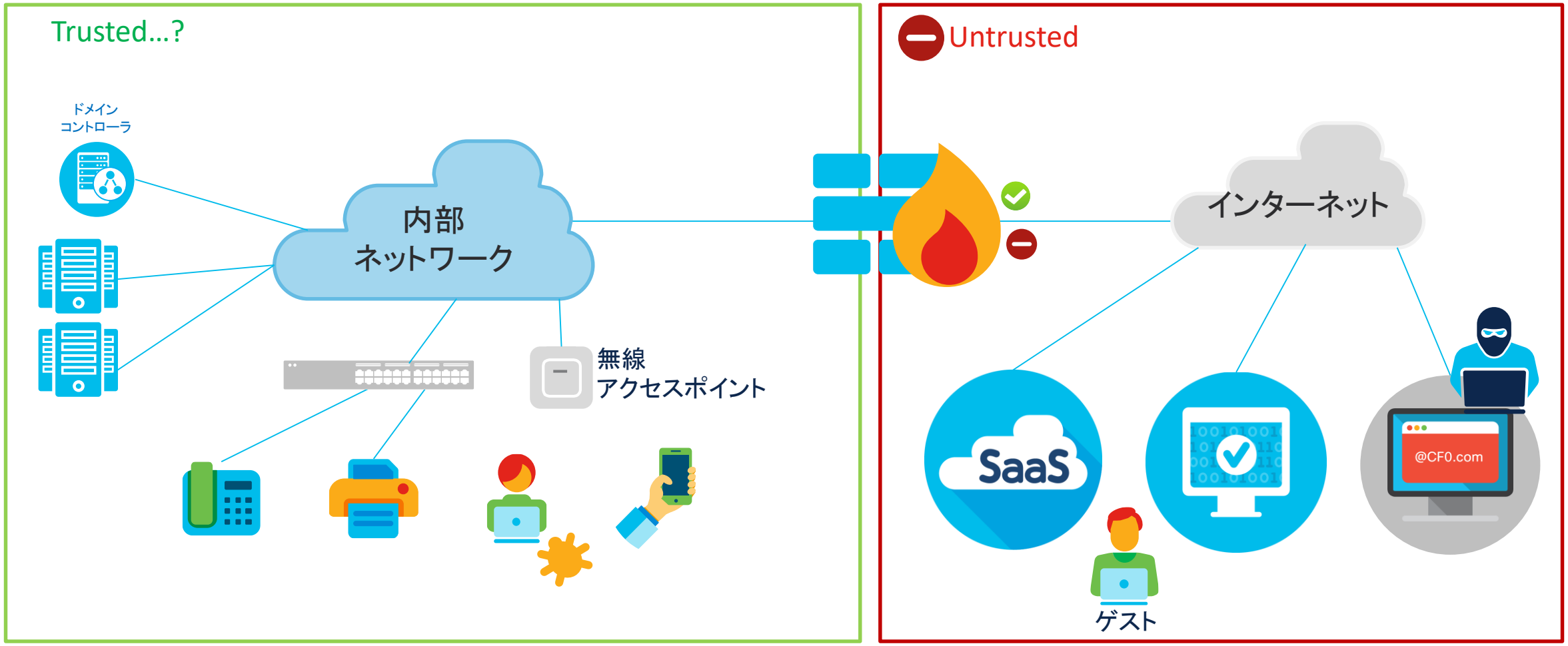
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

モビリティのニーズ



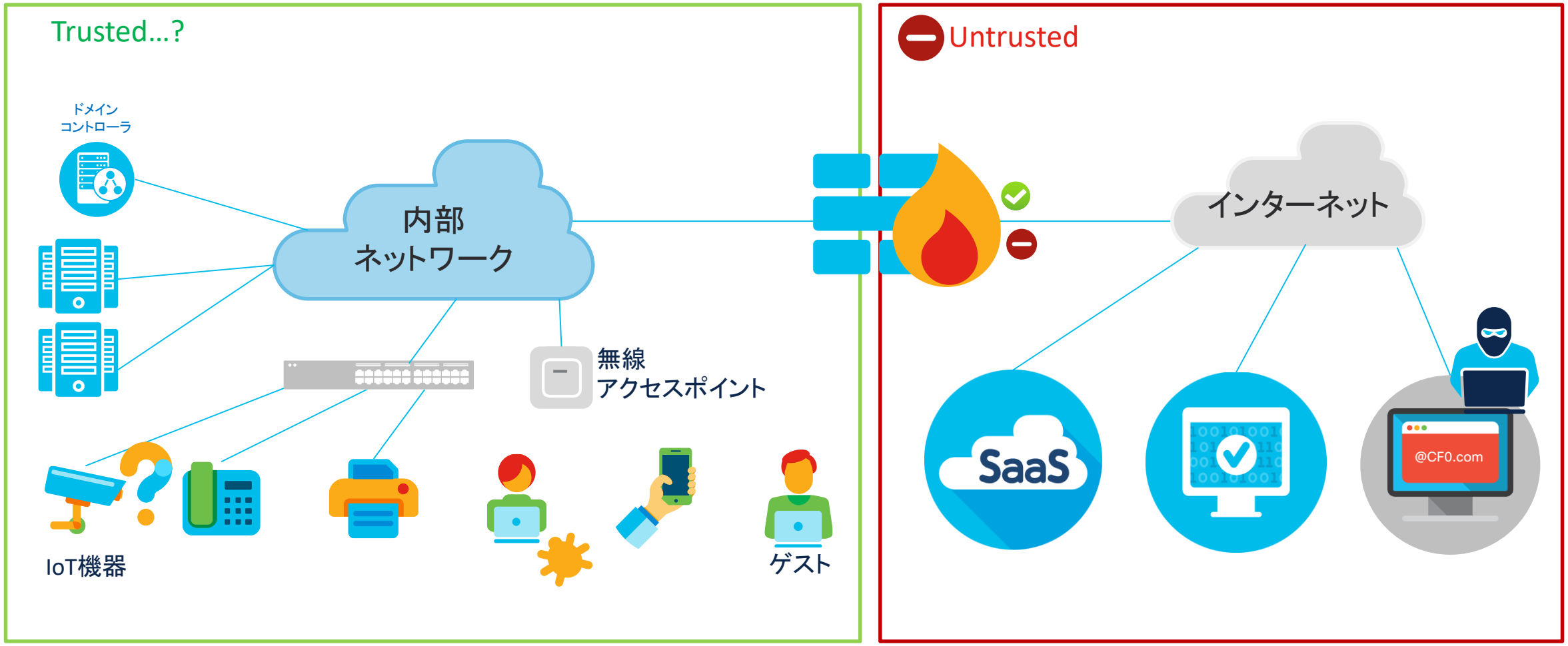
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ゲストアクセス



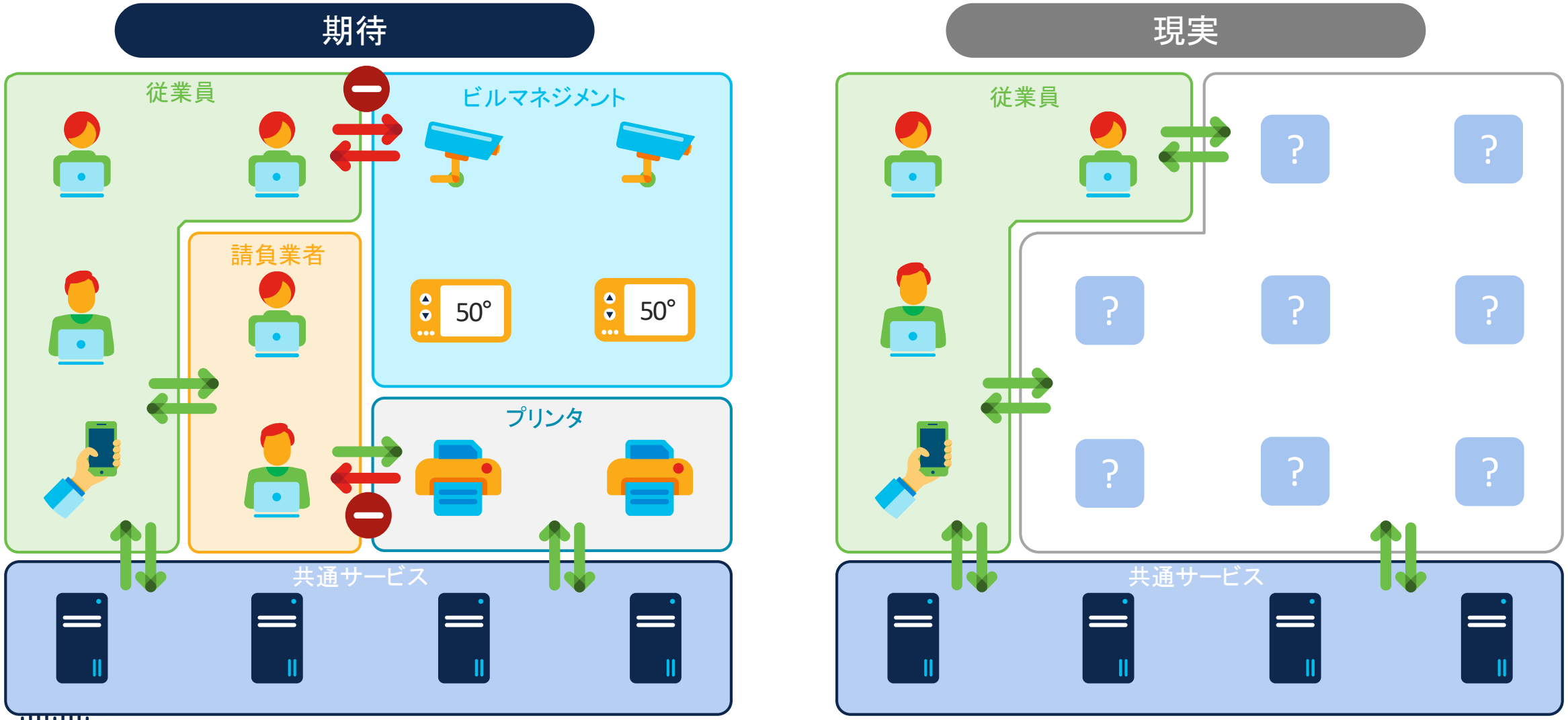
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

IoT機器のネットワーク利用



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

セグメンテーション: 期待と現実

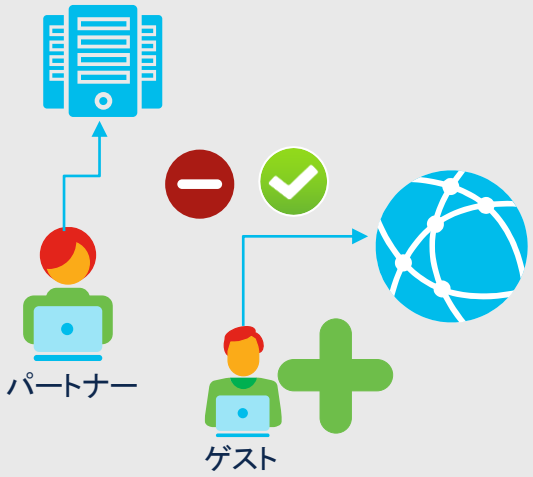


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

多様化したデバイスの種類に応じたセグメンテーションポリシー

企業PC、配布スマホ、持ち込み端末やIoTを区別したポリシーが必要

認証に成功しても、許可するのは最低限のアクセス

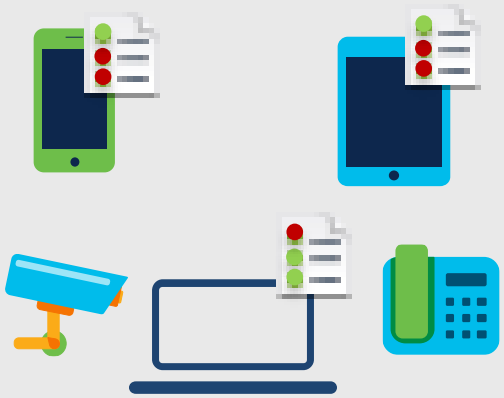


ユーザ/デバイスの信頼性は変化

常に侵害は発生し得る

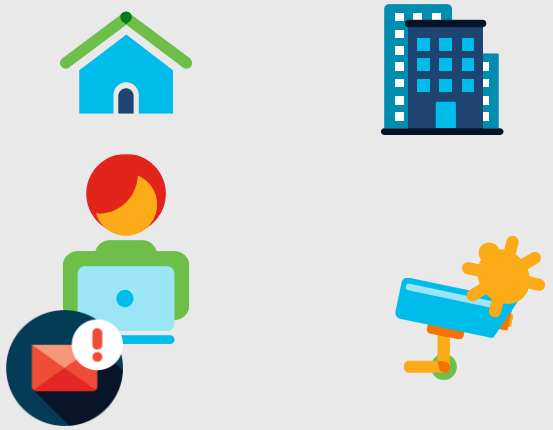
ユーザ/デバイスは境界を行き来する

脅威の存在/ポリシーへの準拠の状態を常にチェックする



ユーザも多様化

利用期間も役割も異なる従業員・請負業者・ゲストが同じネットワークを利用する



接続形態に依存しない包括的なシステムが必要

無線・有線・VPN・ゲスト

接続形態に左右されない一貫したセキュリティポリシーを施行できる統合認証基盤が必要

なぜワークプレイスにゼロトラストか？

	脅威	ゼロトラストソリューション
1	**認可されていない端末や基準を逸脱したデバイスが**生産性を阻害する	端末の信頼性が評価されるまでネットワークアクセスを許さない（認証とシステムヘルスの評価）
2	ネットワークへのアクセスが制限されていないIoTデバイスは、インフラ全体を脆弱に	必要最低限なサービスに絞った限定アクセスを提供するマクロおよび**マイクロセグメンテーション**
3	侵害されたエンドポイントから、**ラテラルムーブメント**によってネットワーク内の他の資産に感染	信頼性を**継続的に評価**し、適応的な制御を適用して**リアルタイムで脅威を切り分**ける

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ワークプレースゼロトラストセキュリティ 5つの柱

エンドポイント可視性

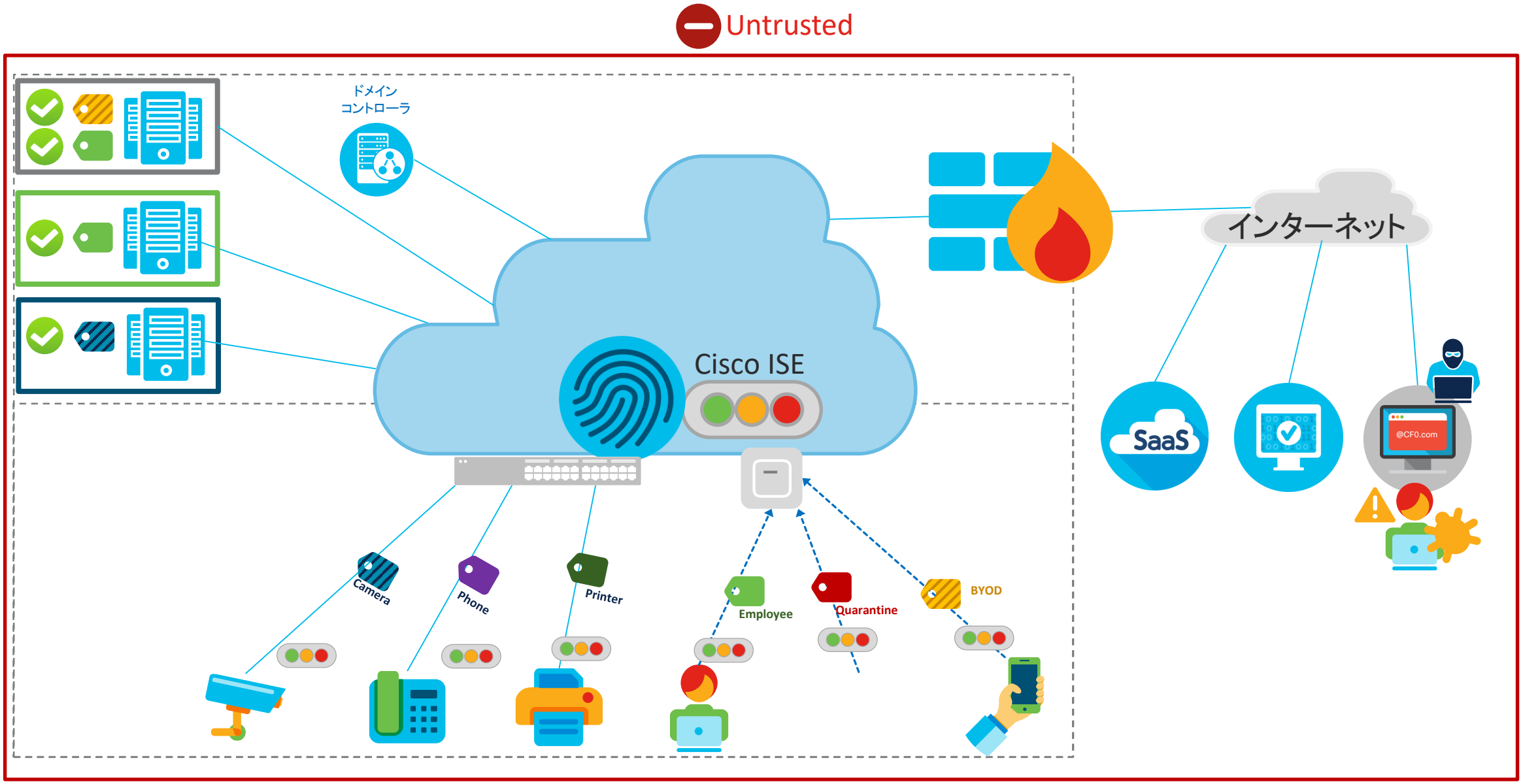
セキュアアクセス

ネットワークセグメンテーション

エンドポイントコンプライアンス

脅威の迅速な封じ込め

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

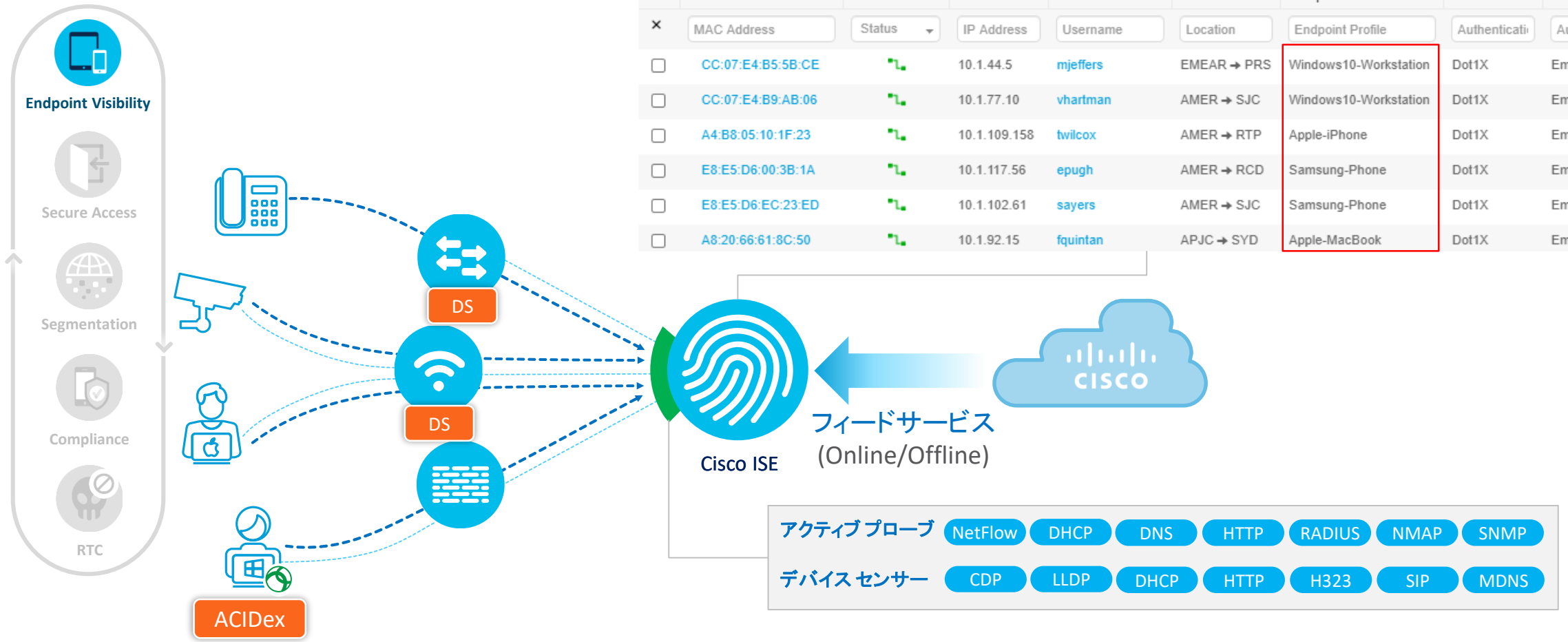


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco ISEのプロファイリング

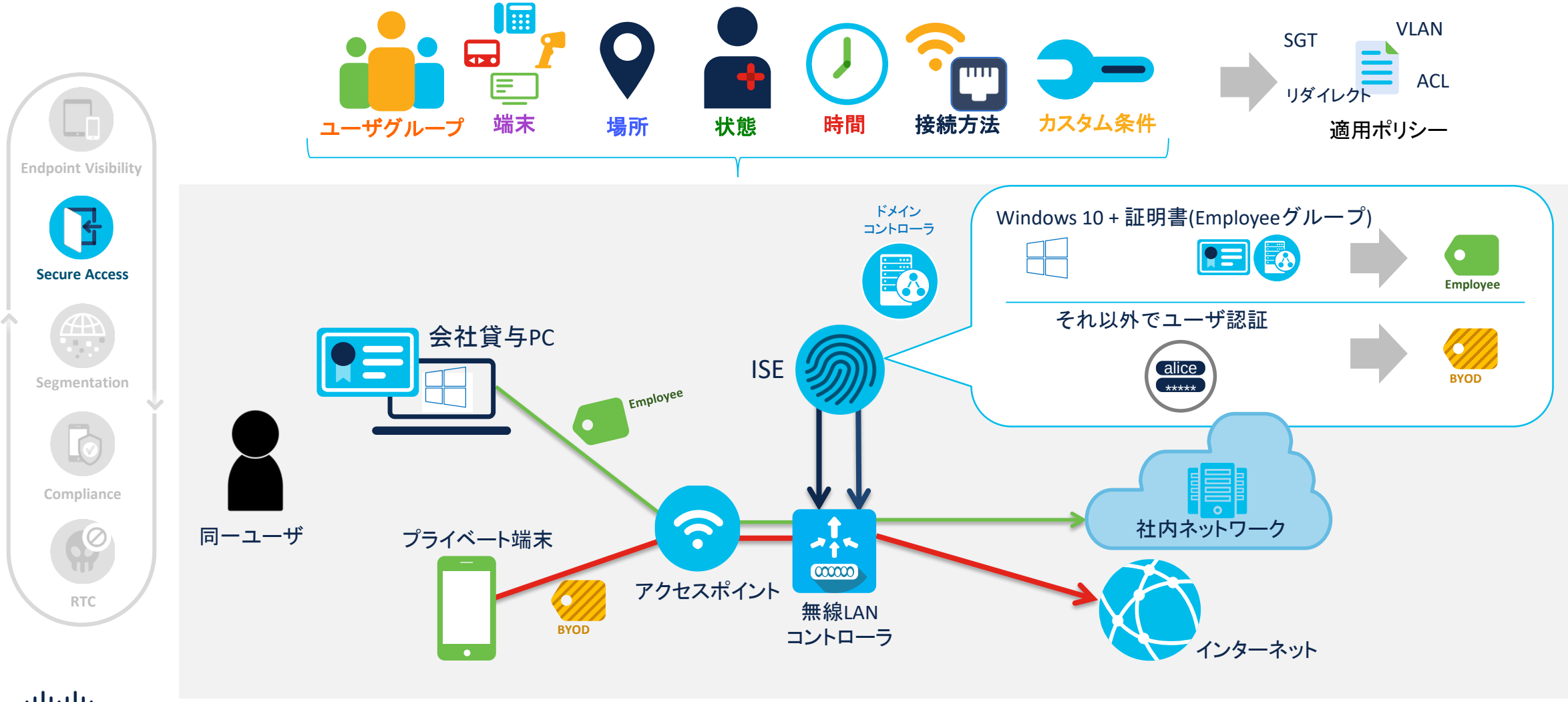
ネットワーク上のMACアドレスやエンドポイントが送信する様々なデータから機器を自動プロファイリング

MAC Address	Status	IP Address	Username	Location	Endpoint Profile	Authentic...	Authorizatio...
CC:07:E4:B5:5B:CE		10.1.44.5	mjeffers	EMEAR → PRS	Windows10-Workstation	Dot1X	Employee
CC:07:E4:B9:AB:06		10.1.77.10	vhartman	AMER → SJC	Windows10-Workstation	Dot1X	Employee
A4:B8:05:10:1F:23		10.1.109.158	twilcox	AMER → RTP	Apple-iPhone	Dot1X	Employee
E8:E5:D6:00:3B:1A		10.1.117.56	epugh	AMER → RCD	Samsung-Phone	Dot1X	Employee
E8:E5:D6:EC:23:ED		10.1.102.61	sayers	AMER → SJC	Samsung-Phone	Dot1X	Employee
A8:20:66:61:8C:50		10.1.92.15	fquintan	APJC → SYD	Apple-MacBook	Dot1X	Employee



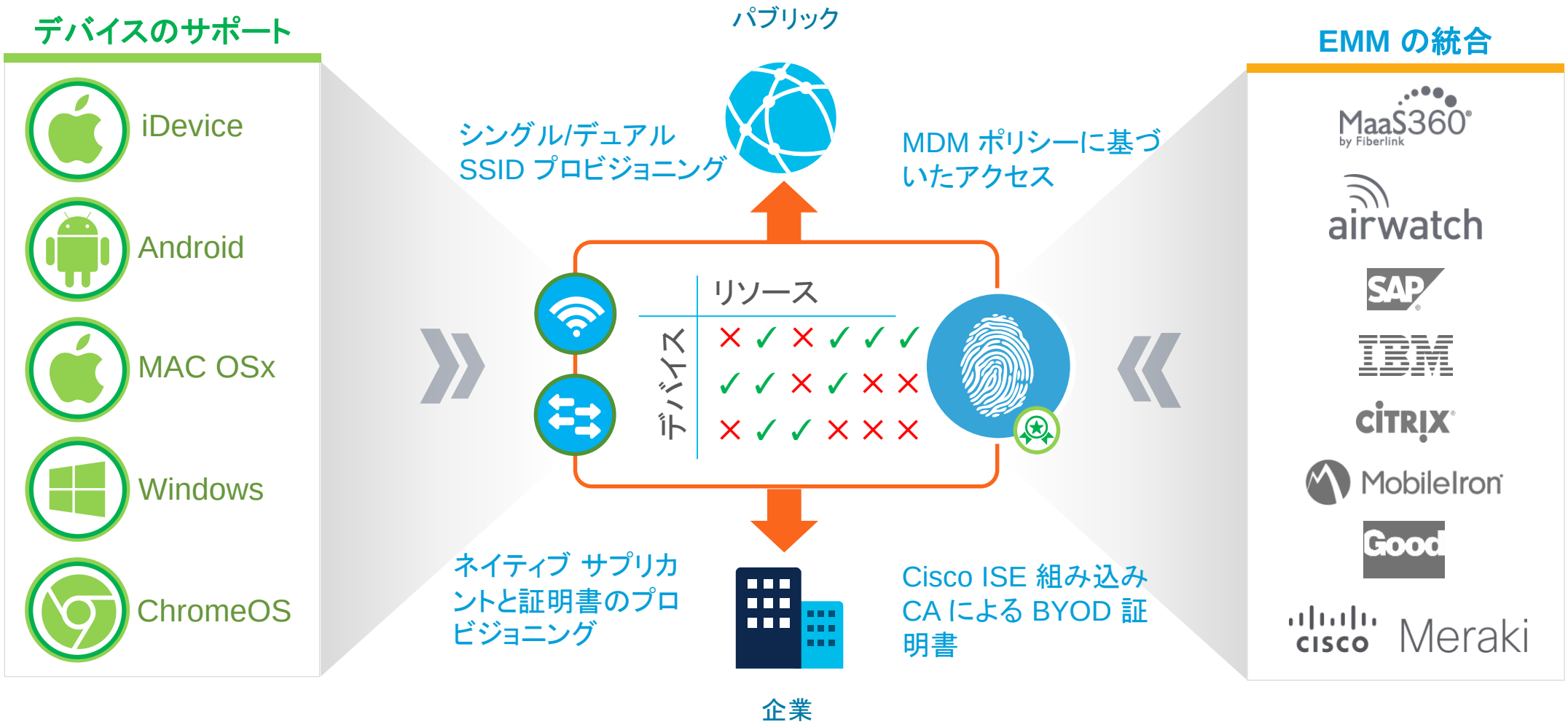
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

コンテキストに基づく統合ポリシー管理



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

デバイスオンボーディング
（証明書・ネットワーク/MDM プロファイルのキッティング）



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

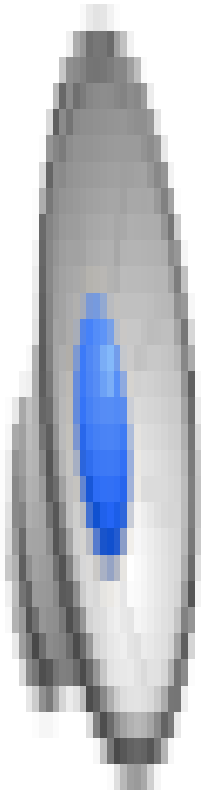
EMM：エンタープライズ モビリティ管理 | MDM：モバイル デバイス管理

証明書自動配布の流れ

ユーザがIT管理者の手を借りず迅速にスマートデバイスを業務利用開始

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

デモ



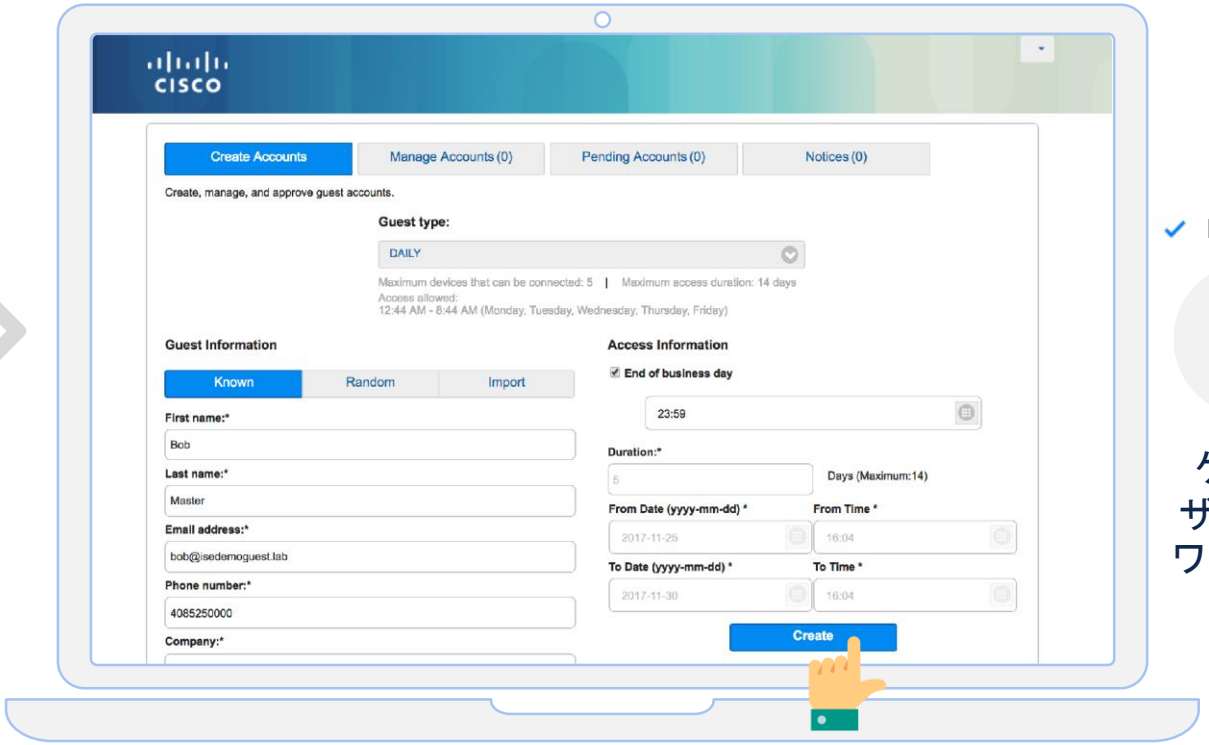
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

スポンサー型ゲストアクセスのフローの例

正社員/営業

スポンサーがスポンサーポータルにログイン

ゲストユーザ向けにアカウントを発行
発行権限: 有効期限 1日
登録情報: ゲスト氏名, メールアドレス



スポンサーがゲストアカウントを作成

ISE-Guest

ゲストユーザーがネットワークに接続

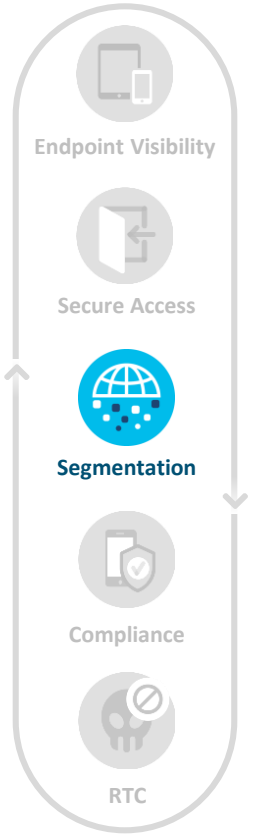
提供されたアカウントでゲストがログイン

ゲストアカウントタイムアウト

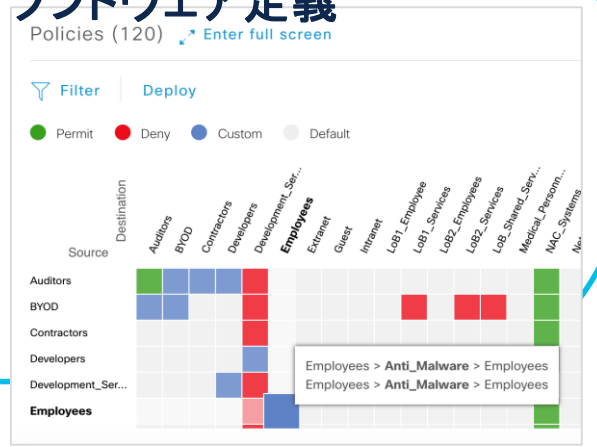
スポンサーはゲストにクレデンシャルをEmail、プリント、SMSのいずれかの方法で通知

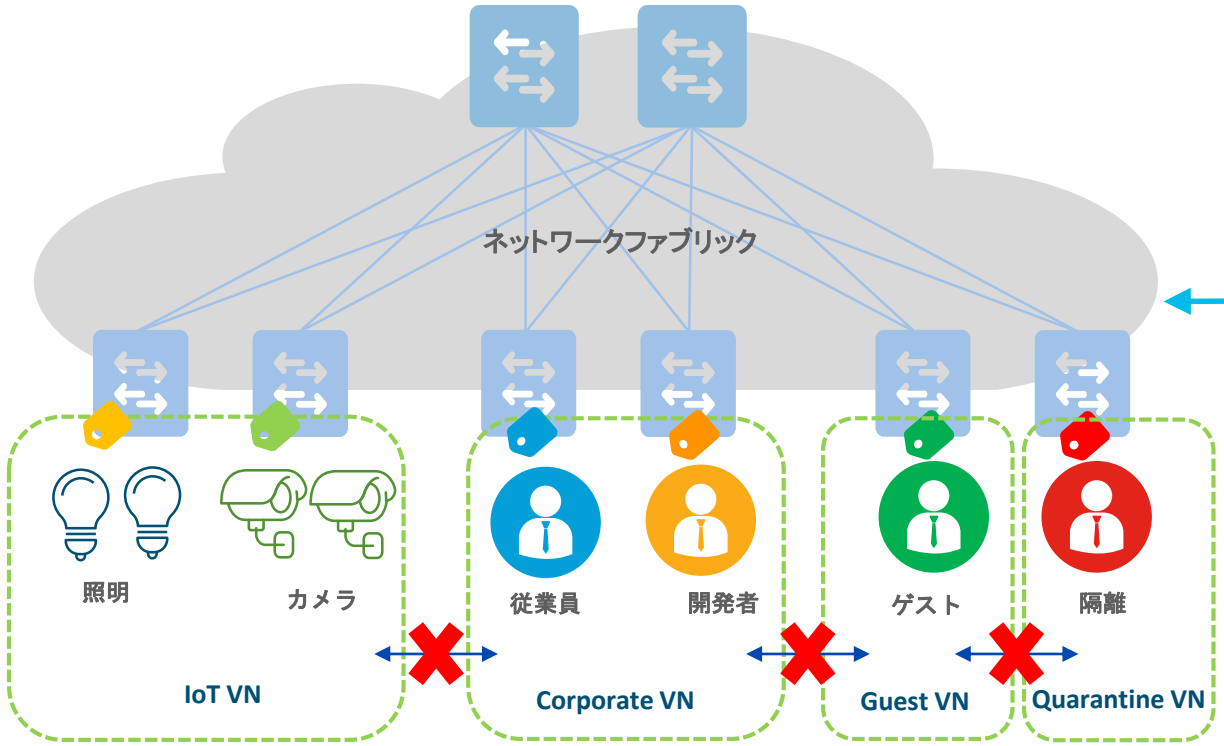
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

SD-Accessでセグメンテーションを自動化



マイクロセグメンテーションポリシーをソフトウェア定義



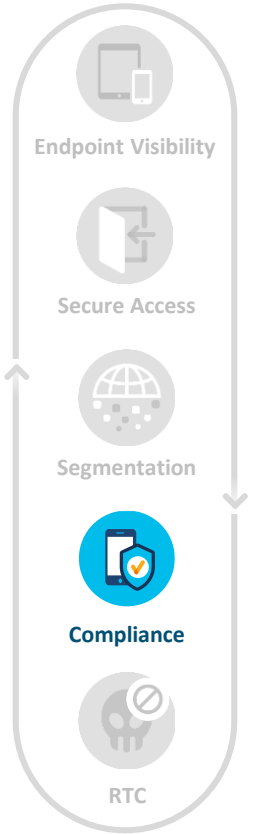


トポロジに依存しないファブリック

- 認証・認可のポリシーを設定に変えてネットワークファブリックへ自動展開
- 最低限の通信が許されるマイクロセグメンテーション

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

ポスチャ アセスメント



ポスチャ:

組織のセキュリティ ポリシー準拠状況

ポスチャ フロー

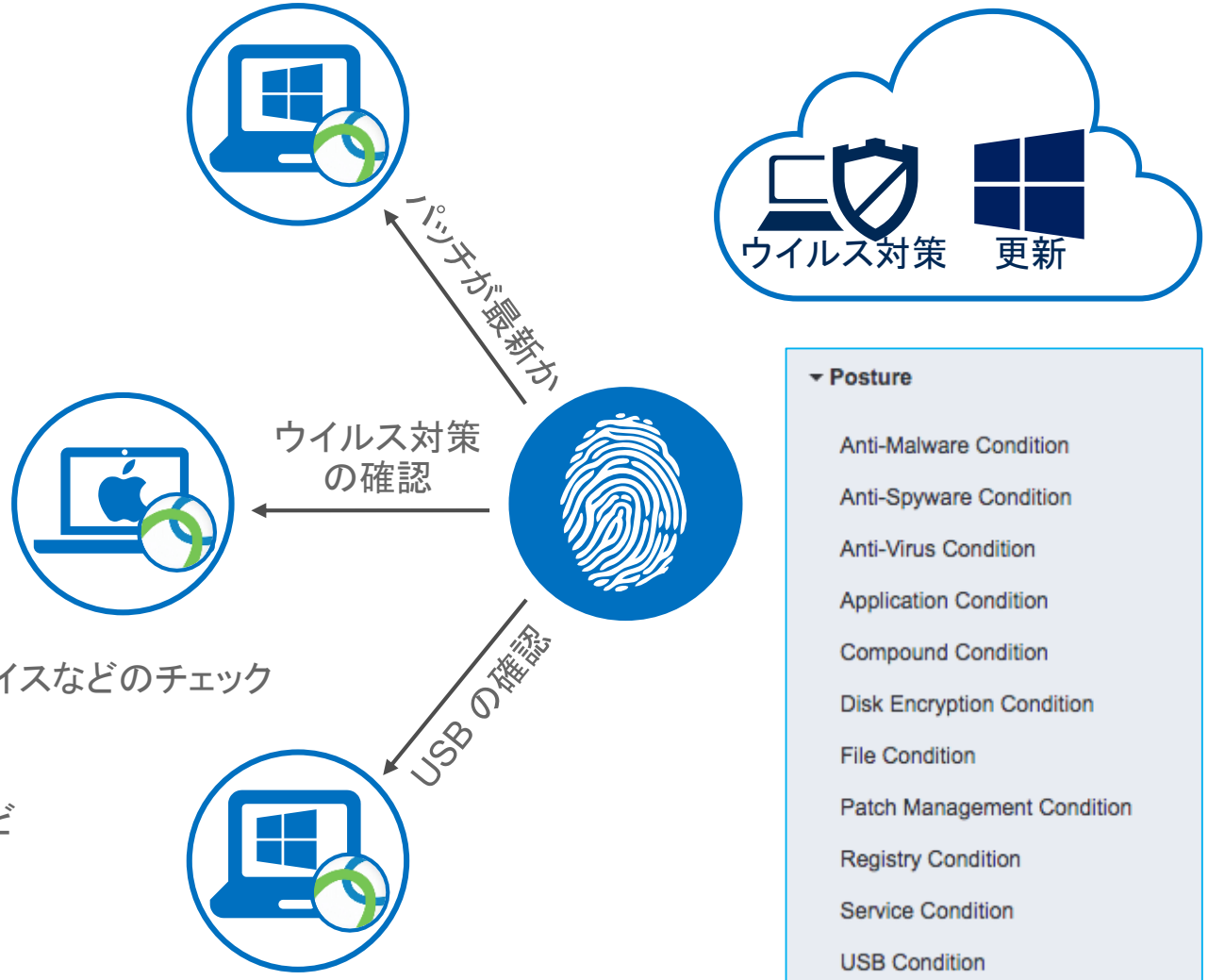
ユーザ/デバイスの認証
ポスチャ:不明/非準拠?

検疫
制限付きアクセス:VLAN/dACL/SGT

ポスチャ アセスメント
ホットフィックス、AV、PIN ロック、USB デバイスなどのチェック

修復
WSUS、アプリの起動、スクリプト、MDM など

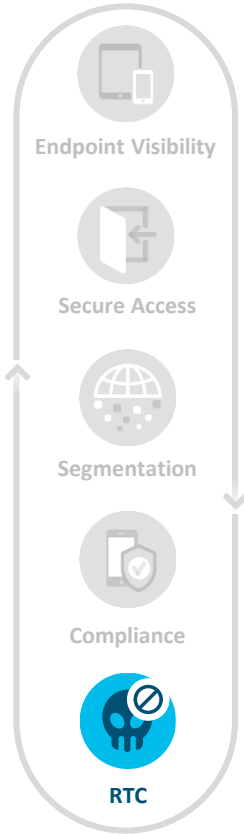
認可の変更
フル アクセス:VLAN/dACL/SGT



- **Posture**
  - Anti-Malware Condition
  - Anti-Spyware Condition
  - Anti-Virus Condition
  - Application Condition
  - Compound Condition
  - Disk Encryption Condition
  - File Condition
  - Patch Management Condition
  - Registry Condition
  - Service Condition
  - USB Condition

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

脅威中心型 NAC



ポスチャを評価

脆弱性データがエンドポイントのポスチャを外部から識別

制御の拡大

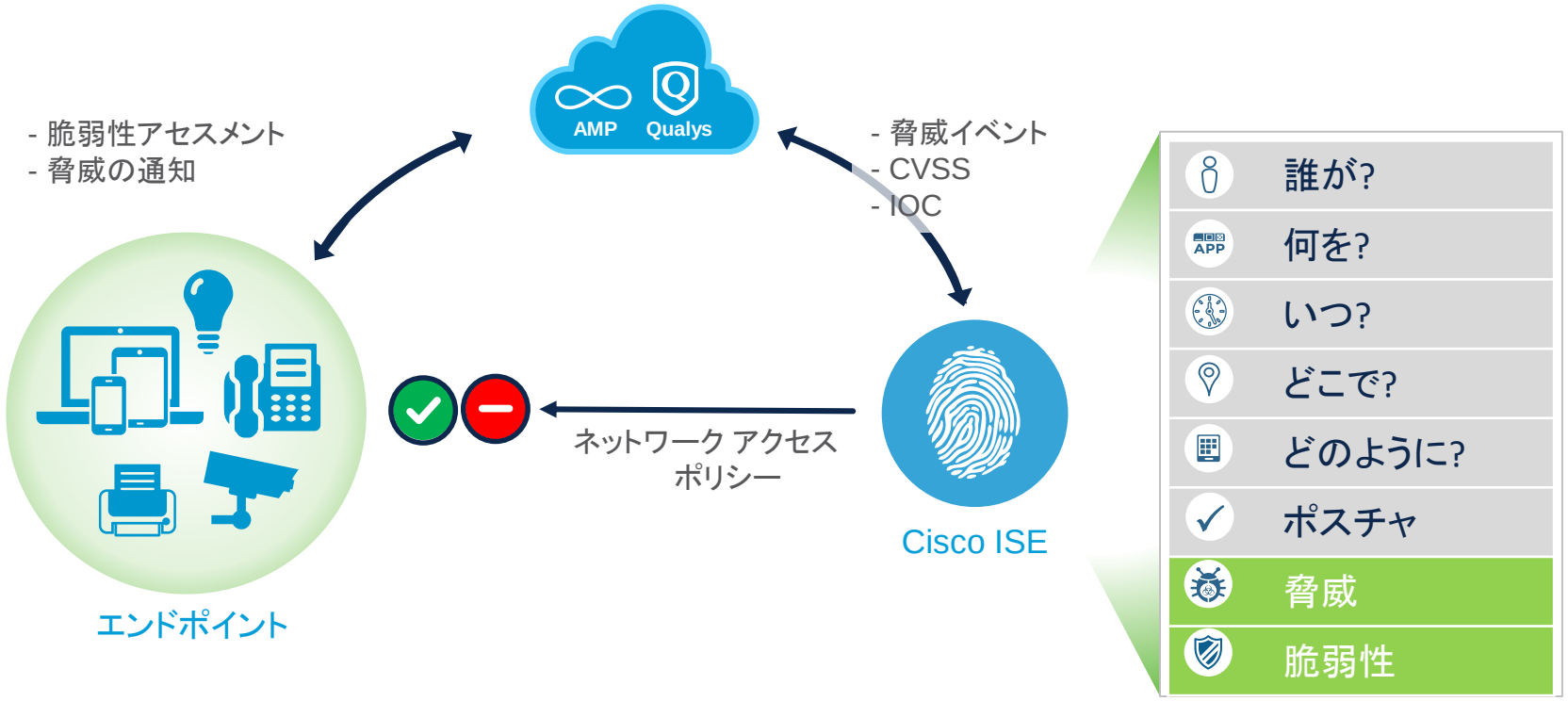
脅威インテリジェンスと脆弱性アセスメントのデータを活用

迅速な応答

脆弱性データと脅威メトリックに基づいたリアルタイムのポリシー更新を自動化

脅威および脆弱性属性に基づいて Cisco ISE 承認ポリシーを作成

侵害されたエンドポイントや脆弱なエンドポイントをセグメント化して修復することでデータ漏洩を防止

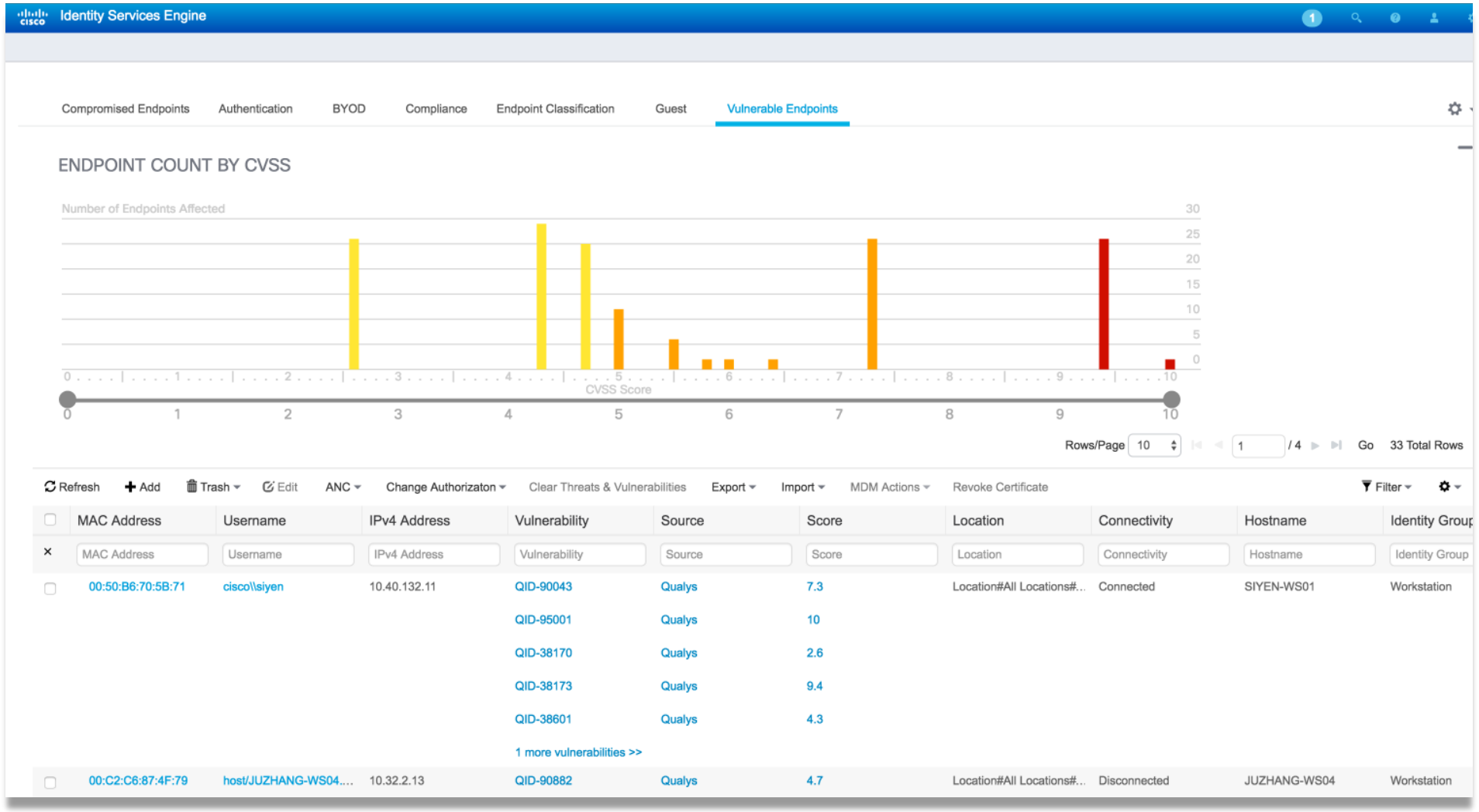


© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

共通脆弱性評価システム（CVSS）| 侵害の兆候（IOC）

「脆弱なエンドポイント」

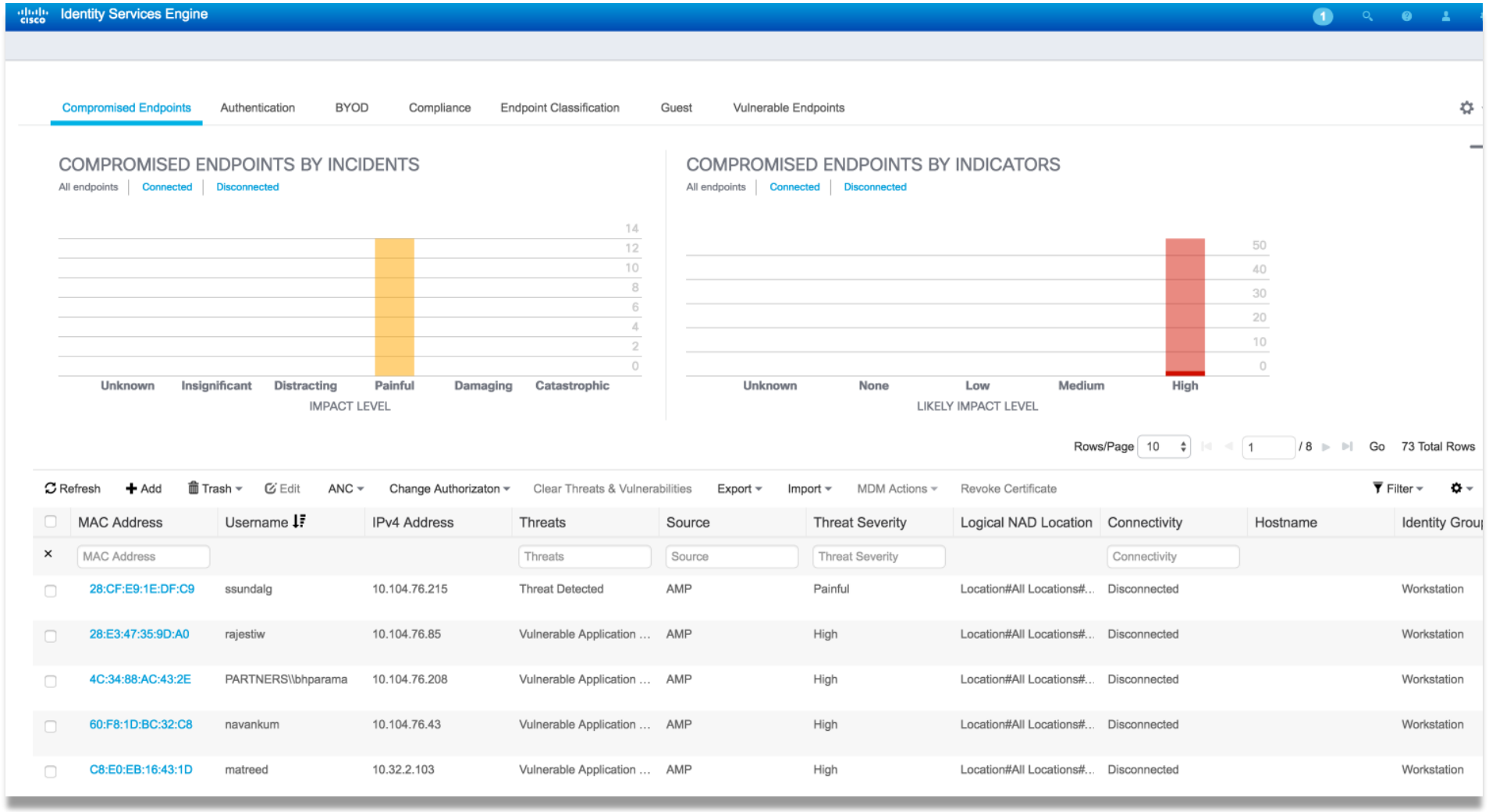
共通脆弱性評価システム（CVSS）ベース



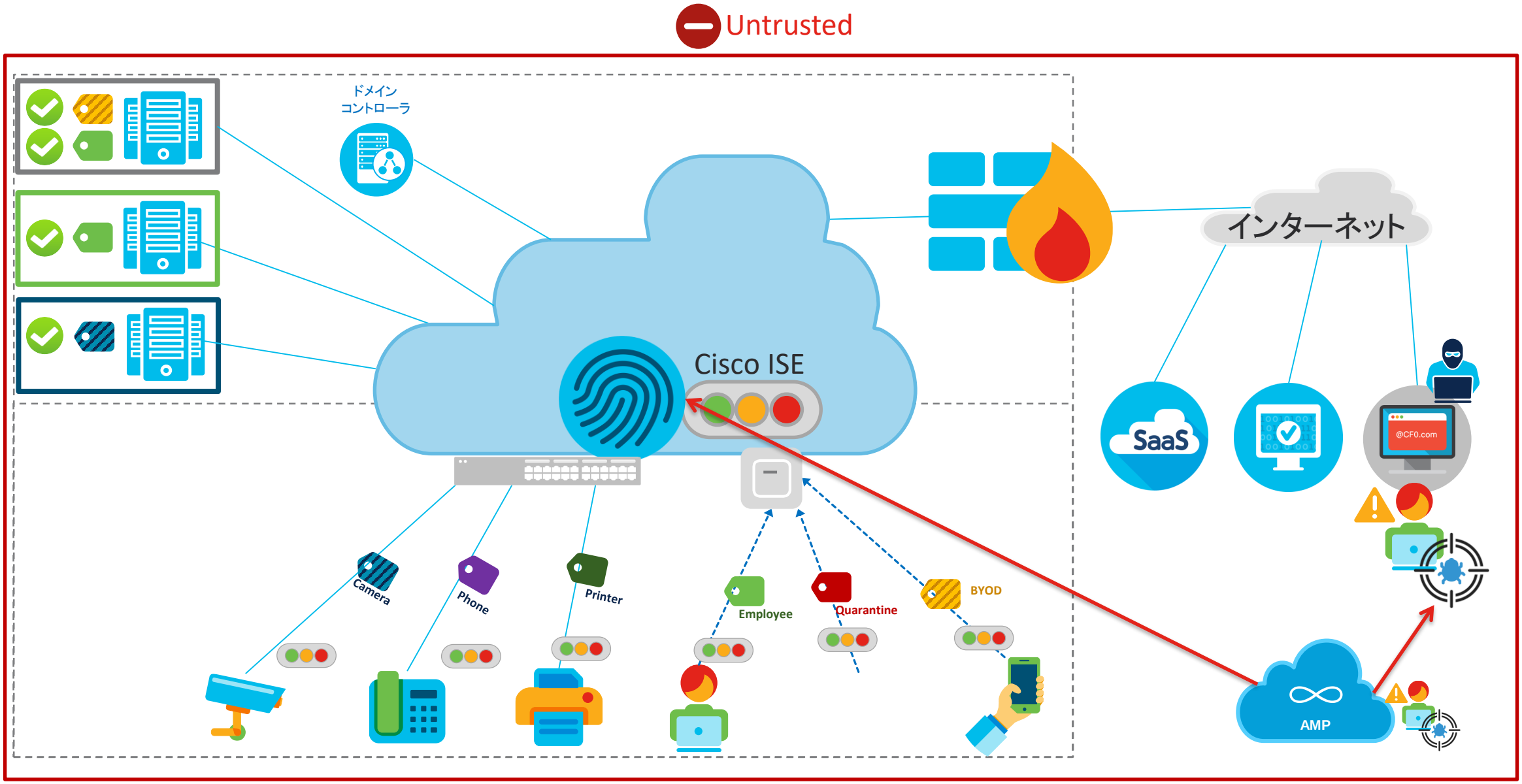
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

「侵害されたエンドポイント」

インシデント/インジケータ ベース



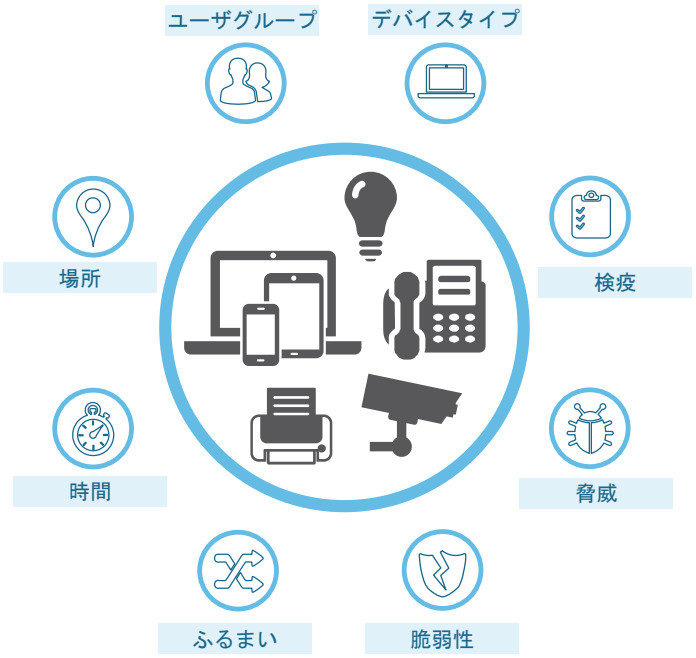
© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public



© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public

「信頼」に基いた戦略的なアクセス管理

Cisco Identity Services Engine



可視性と意思決定を強化

ソフトウェア定義型セグメンテーション、
サービス アクセスおよび権限付与


CISCO

© 2020 Cisco and/or its affiliates. All rights reserved. Cisco Public