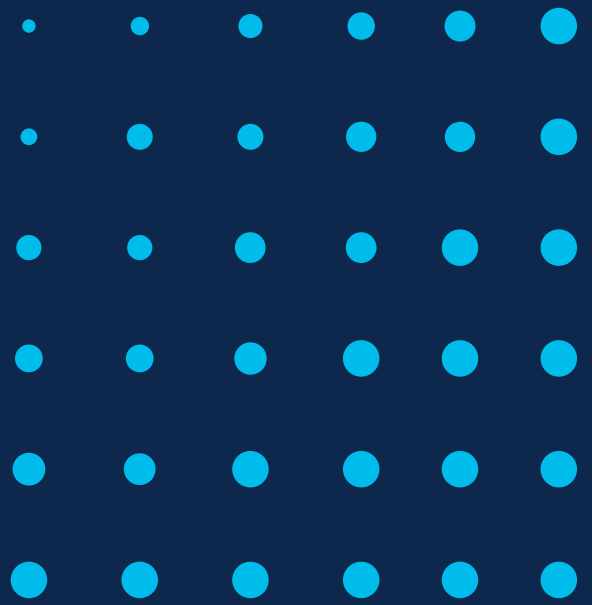
次世代のセキュリティ
境界ベースのセキュリティからの脱却

シスコシステムズ合同会社　セキュリティ事業
福留 康修、秦 寛樹
2022.1.20

Agenda

1. 働く環境をとりまく状況の変化
   - ハイブリッド型へシフト
   - セキュリティ境界の変化
   - エンドポイントの安全な接続と保護がより重要に
2. エンドポイントにおける対策強化
   - 今後更に狙われるエンドポイント
   - 運用課題を引き起こすコンパチビリティ問題
   - Cisco Secure Client による解決
3. エンドポイントにおける健全性の向上とデバイス管理の効率化
   - デバイスの健全性を条件にアクセスを許可する対策が主流に
   - MFAによって増えるデバイスのコストと管理が課題に
   - Cisco Secure Access by Duo による解決

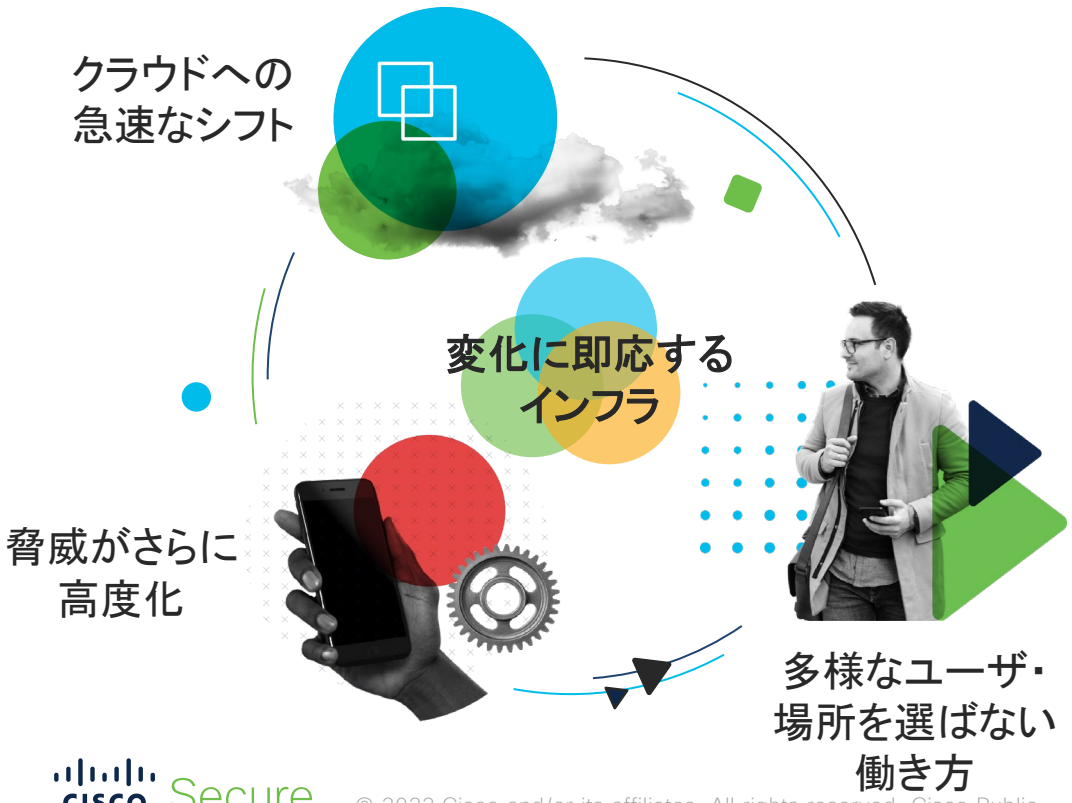
1. 働く環境をとりまく状況の変化



近況、お客様の課題

COVID-19により働き方が多様化し、デジタル化の推進によりクラウド利用が加速。ランサムウェアやサプライチェーン攻撃が進化・高度化する中で、ゼロトラストセキュリティモデルへのシフトが必要な状況。

デジタル化を取り巻く環境の変化



サイバーセキュリティの課題

在宅勤務で
サイバー攻撃が
600%に急上昇*1

実際のインシデントの
50%が
放置されている*2

多要素認証（MFA）を
使用している組織は
27% に過ぎない*2

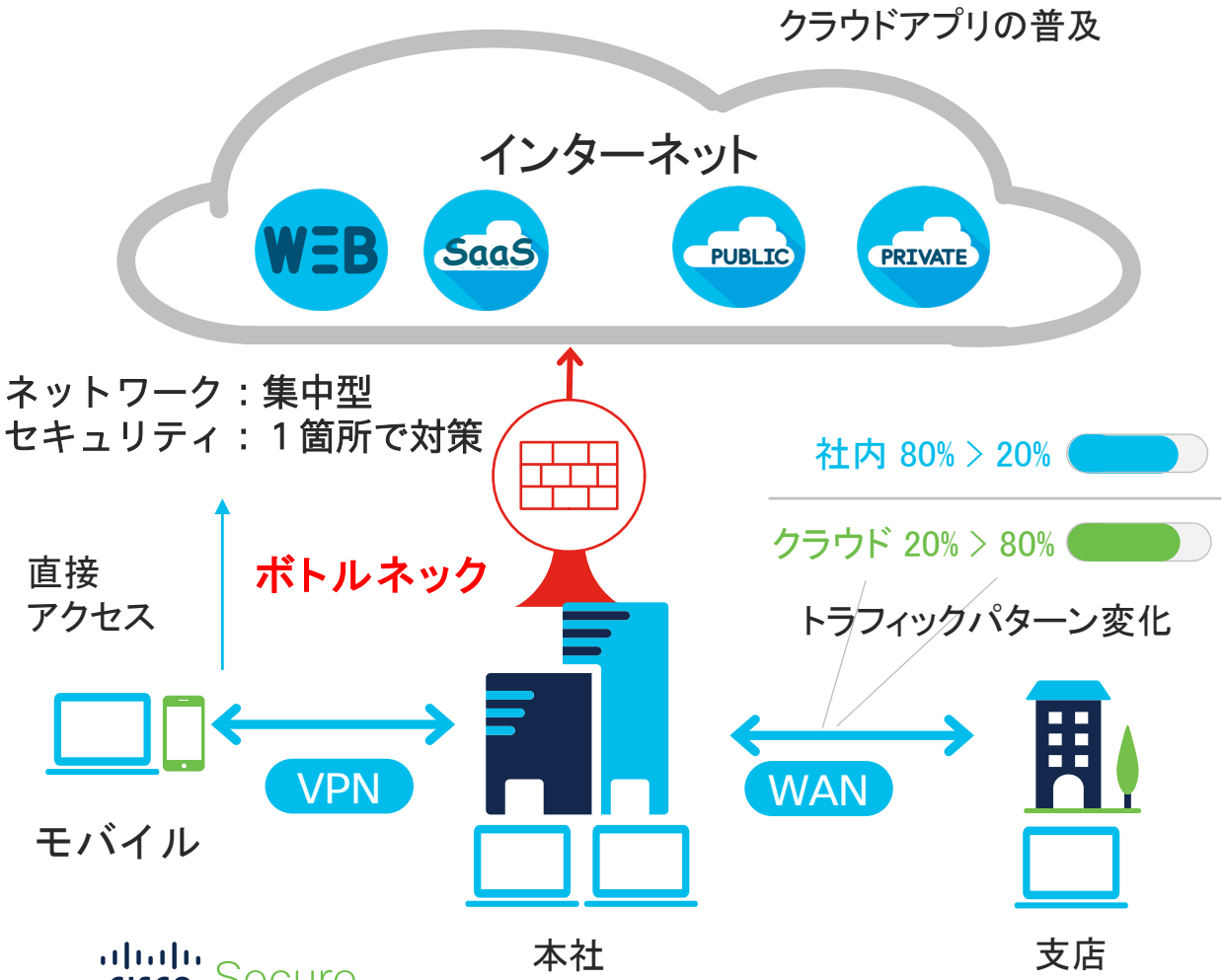
不正侵入の**61%**以上
はID/パスワードの漏洩
や弱いパスワードが
原因*3

*1: Scott Galloway; MacAfee Report; Cisco; Zoom; Press Search; Cisco Analysis
*2:シスコ サイバーセキュリティ レポート シリーズ 2020
*3: Verizon Data Breach Report 2021

cisco Secure

リモートワーカーむけ環境におけるネットワーク利用の変化

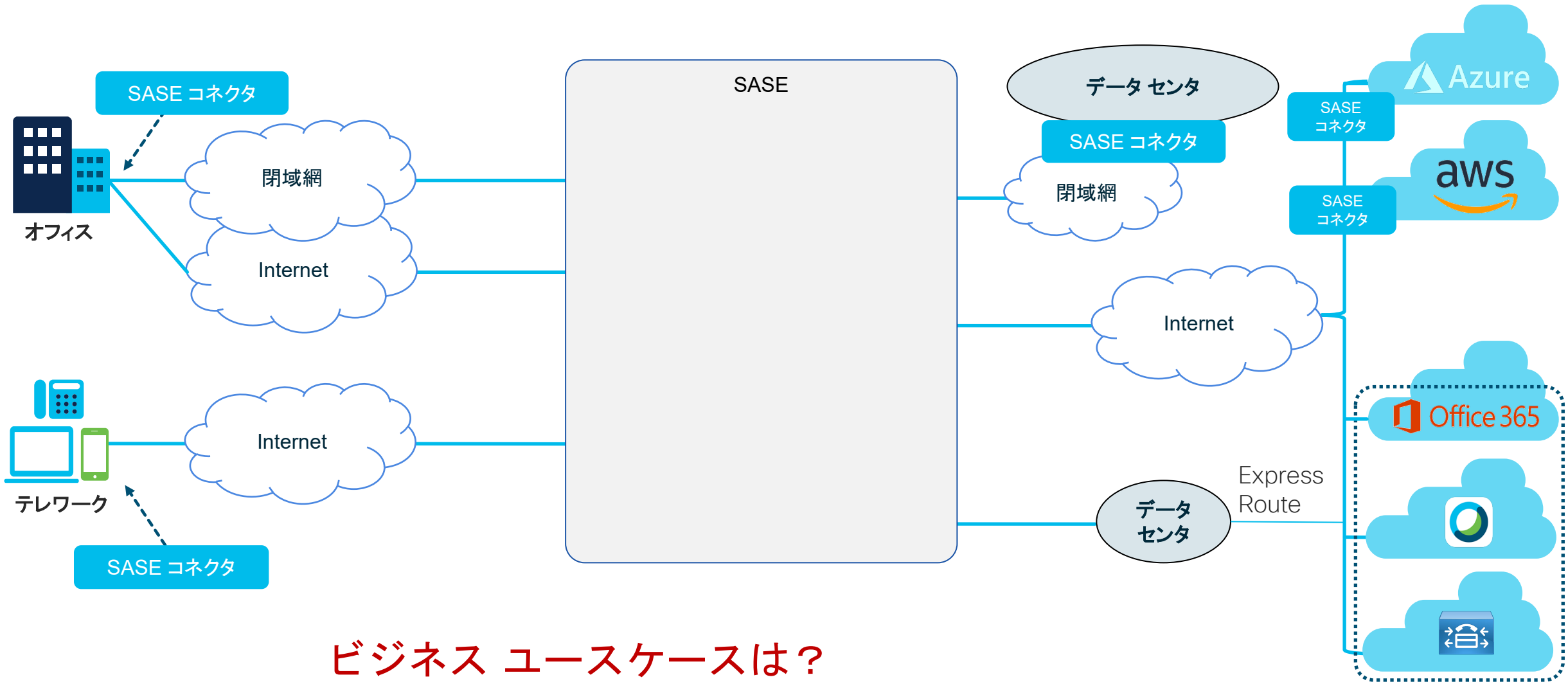
従来



これから

新たな対策の必要性

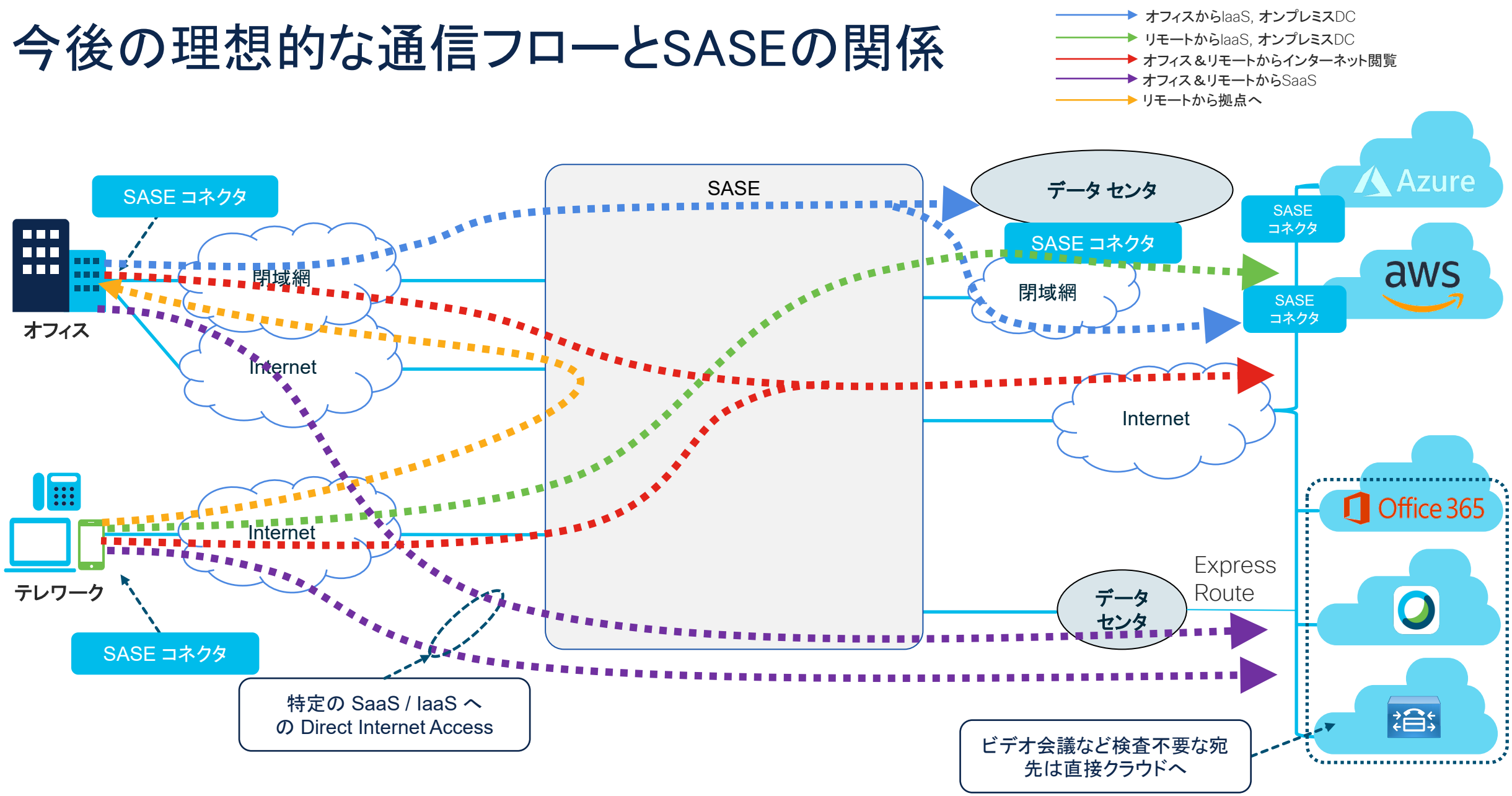
インフラストラクチャ概観（SASE）



ビジネス ユースケースは？
エンド・ツーエンドのトラフィックフローは？

※一部ロードマップ機能を含みます

今後の理想的な通信フローとSASEの関係



Multi Factor Authentication（多要素認証）、VPN レスアクセス、統合管理

※一部ロードマップ機能を含みます

いかに安全な環境を構築するか
ゼロトラストという考え方

境界型セキュリティの限界

多様化するアクセス環境において
- 適切なアクセス権を確保したい
- 拡大する攻撃対象を保護したい
- 広範囲な可視性を確保したい

課題に対処する新しい考え方

場所 ≠ 信頼

場所やネットワークを信頼しない

信頼性の再定義

1度限りの検証に頼らず継続確認する

アクセス制御

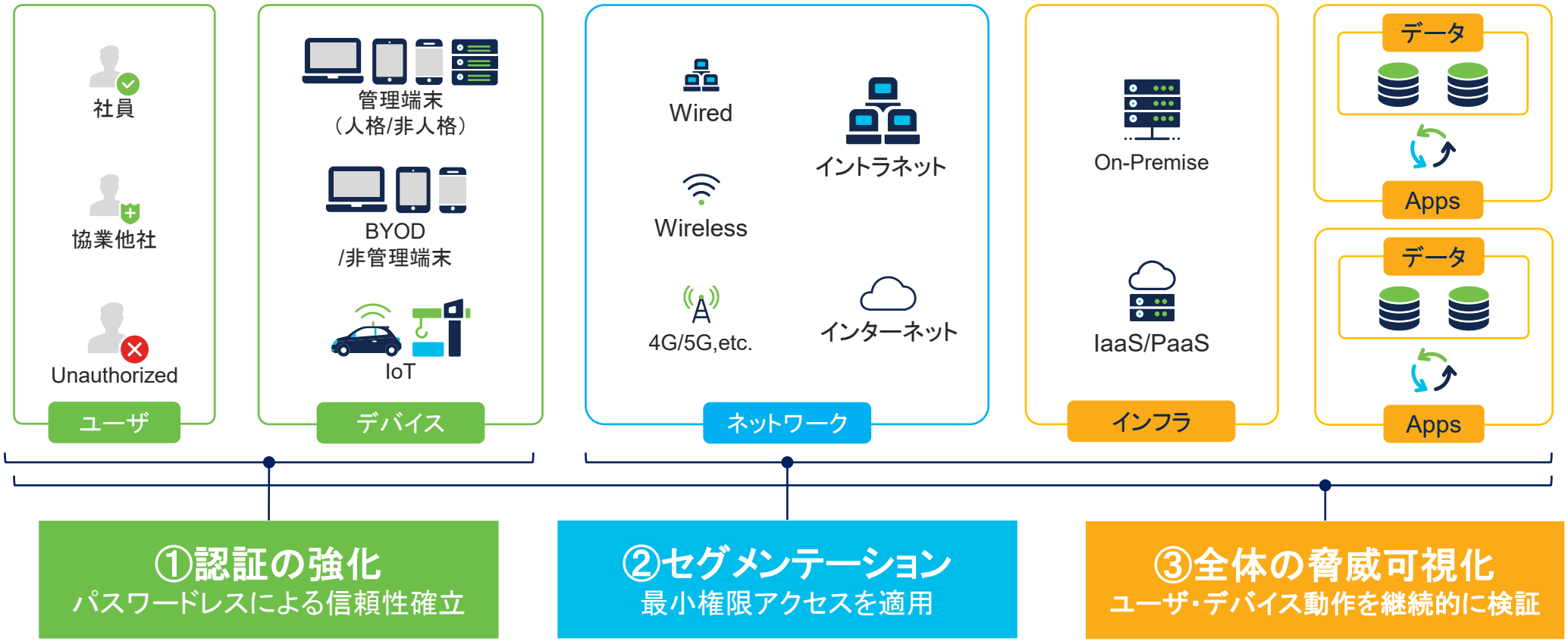
最小限の範囲を最小限の時間で制限

自動化ポリシー

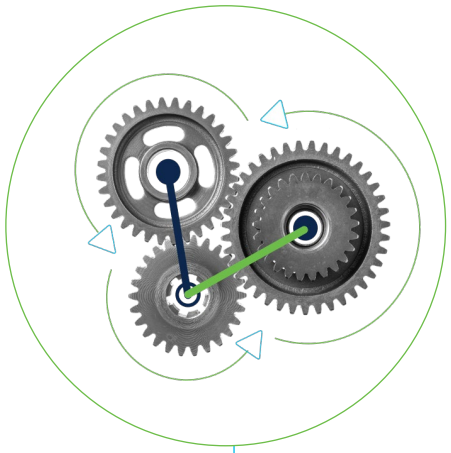
可視化された情報を利用したアクセスの調整

課題を解決する、ゼロトラストプラットフォーム概要

ゼロトラストプラットフォームでは、誰もが安全、便利、快適にネットワークにつながるために、認証強化、セグメンテーション、全体の脅威可視化に加え、運用・監視の自動化が重要



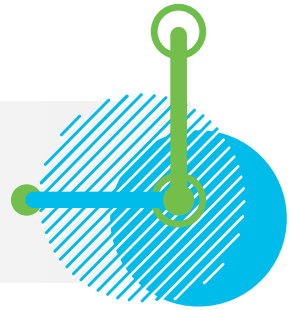
さらに重要になるエンドポイント セキュリティ



XDR

Zero Trust

SASE



エンドポイントセキュリティは、最新のセキュリティスタックに不可欠なコンポーネント

2.エンドポイントにおける対策強化

情報セキュリティ10大脅威 2021

出典IPA https://www.ipa.go.jp/security/vuln/10threats2021.html

昨年順位	個人	順位	組織	昨年順位
1位	スマホ決済の不正利用	1位	ランサムウェアによる被害	5位
2位	フィッシングによる個人情報等の詐取	2位	標的型攻撃による機密情報の窃取	1位
7位	ネット上の誹謗・中傷・デマ	3位	テレワーク等のニューノーマルな働き方を狙った攻撃	NEW
5位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	4位	サプライチェーンの弱点を悪用した攻撃	4位
3位	クレジットカード情報の不正利用	5位	ビジネスメール詐欺による金銭被害	3位
4位	インターネットバンキングの不正利用	6位	内部不正による情報漏えい	2位
10位	インターネット上のサービスからの個人情報の窃取	7位	予期せぬIT基盤の障害に伴う業務停止	6位
9位	偽警告によるインターネット詐欺	8位	インターネット上のサービスへの不正ログイン	16位
6位	不正アプリによるスマートフォン利用者への被害	9位	不注意による情報漏えい等の被害	7位
8位	インターネット上のサービスへの不正ログイン	10位	脆弱性対策情報の公開に伴う悪用増加	14位

- 「ランサムウェアによる被害」が1位
- 「テレワーク等のニューノーマルな働き方を狙った攻撃」が初登場で3位

更に狙われやすくなったエンドポイント
凶悪化するランサムウェア事情

- 『Talos Takes』エピソード#57：サービスとしてのランサムウェア（RaaS）のビジネスモデル (2021.6)
  - サービスとしてのランサムウェア（RaaS）とマクドナルドのフランチャイズには類似点があるのでしょうか。両者のビジネスモデルは皆さんが想像している以上に似ています。Colonial Pipeline 社を攻撃した DarkSide などのグループの活動に見られるように、RaaS モデルはここ数か月間にマルウェア攻撃の主流に。

    https://gblogs.cisco.com/jp/2021/06/talos-talos-takes-ep-57-ransomware-as-service/amp/

- ランサムウェア攻撃で「二重脅迫」や「大物狩り」の手法、研究者が注意喚起 (2021.8)
  - Cisco Secureのリサーチエンジニア Edmund Brumaghin氏は「Black Hat USA 2021」で、高い収益を得ようとする「big game hunting」（大物狩り）と呼ばれるトレンドの下、ランサムウェア実行犯の用いる戦術がさらに進歩していると述べた。
  - 脅威アクターはエンドポイントを通じて最初のアクセスポイントを確保した後、ネットワーク内を水平移動（ラテラルムーブメント）し、できる限り多くのシステムへのアクセスを得ようとすることが多くなっている。
  - 「彼らは自らの統制下に置いた環境を最大限に活用できるようになってはじめて、ランサムウェアを一斉に配備する」と述べ、「これにより、標的となった組織では単一のエンドポイントが侵害されるのではなく、サーバー側インフラの70～80%で同時に業務に支障が生じ、結果的に組織は身代金を支払わざるを得ない状況に追い込まれる。

    https://japan.zdnet.com/article/35174901/

Talosインシデント対応チーム タイムラインの典型例

0 ～ 6 日目

侵入開始・初期感染

マルウェア配布とフィッシングに最も使われるのは電子メール
悪意のあるサイトへの誘導
リモートワークで必要なサービスへの侵入
多機能な侵入ツール・エクスプロイト（exploit）の利用
管理者アカウントが侵害

7 ～ 13 日目

偵察行動・感染拡大

より価値のある対象を探す、より広範囲な対象を掌握する
内部状態の把握し、ログイン情報、機密情報を取得する
検出と防止を回避：仮想マシン起動、正規プログラムの利用
ファイヤウォール、ログ機能、各種セキュリティ機能を終了させる

14 ～ 21 日目

実行・被害

暗号鍵を交換して端末のデータを一斉に暗号化される
搾取された機密情報を晒すと脅迫する

原因特定・対応

インシデントレスポンス(IR)対応方針を協議
フォレンジクス、封じ込め、是正措置等の対応をサポート
ソリューション活用（AMP, Stealthwatch, Umbrella等）
再発防止へ向けたプロアクティブな対策アドバイス

Talosインシデント対応チーム

- 最初の侵入から実際の攻撃までの時間は不均一
- 侵入後に攻撃を防げる時間と可能性はある

新たな課題「コンパチビリティ（相性）問題」

1. セキュリティ製品間における動作競合（例）

S 社 EPP vs. 他社 EDR

P 社 VPN vs. 他社 SASE エージェント

F 社 VPN vs. N社 SASE エージェント

N 社 SASE エージェント vs. C社 DNS Security

C 社 VPN vs. C社 SASE エージェント

2. 検討・導入（予算）タイミングがバラバラ

解決策

エージェント数を減らす／統合する

シスコのユニファイド エージェント
Cisco Secure Client (CSC)

運用負担を下げ機能追加を楽にする

- 課題：セキュリティ機能を新たに追加するたびに、それぞれにエージェントソフトウェアが必要になり導入する作業が発生
- AnyConnect の次期リリースは AnyConnect 5.0 を包含する Cisco Secure Client となり、Secure Endpoint (AMP for Endpoints)と統合することが可能
- クラウドからの管理という選択肢を新たに追加
- 解決：CSC の登場により新たなセキュリティ機能追加のハードルが低下

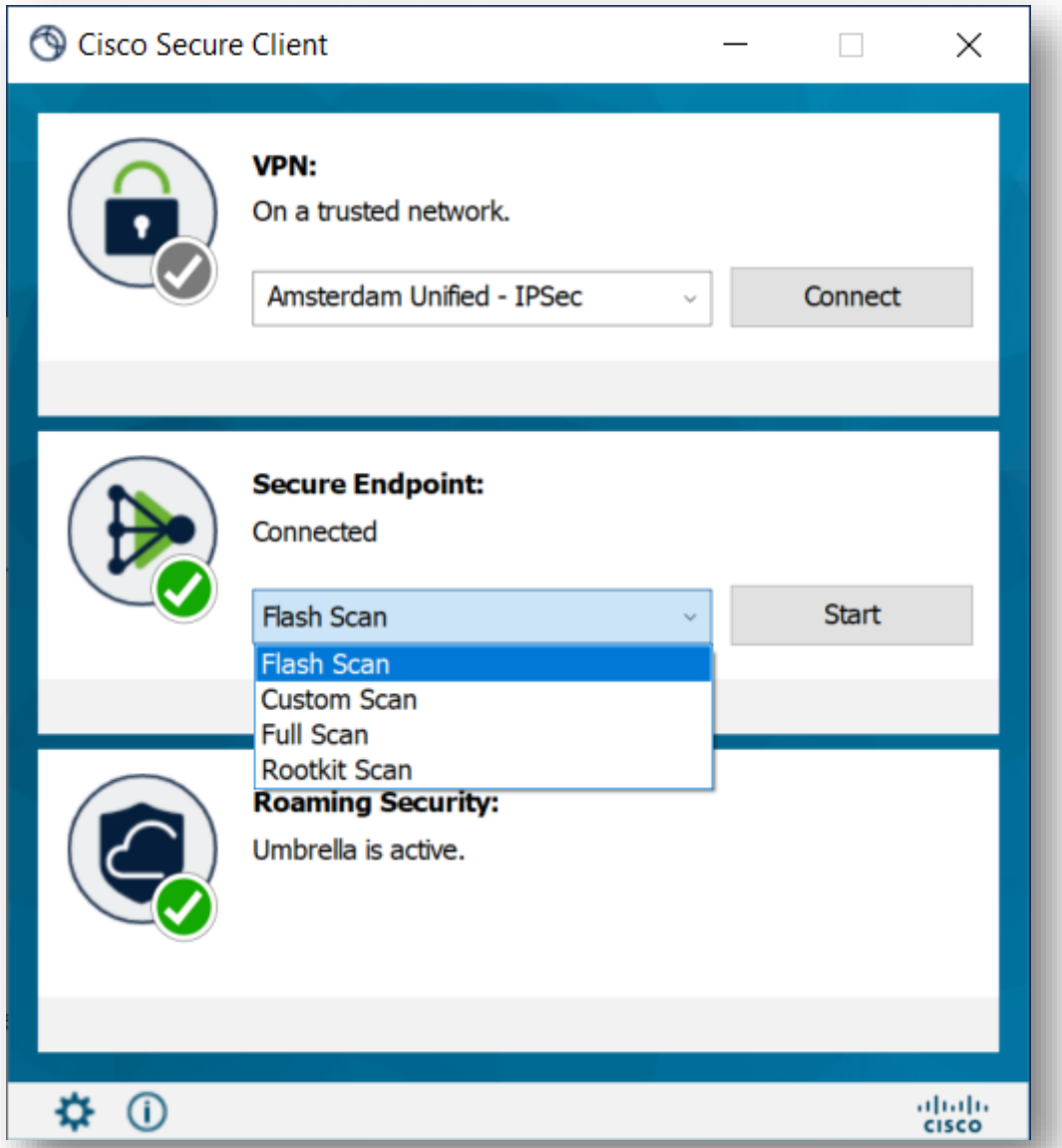
AnyConnect VPN

Cisco Umbrella

Secure Endpoint

CSC: 外観

Protection Status	Badge
Unknown	
Scanning	
Protected	
Unprotected	
Disabled	
Error	



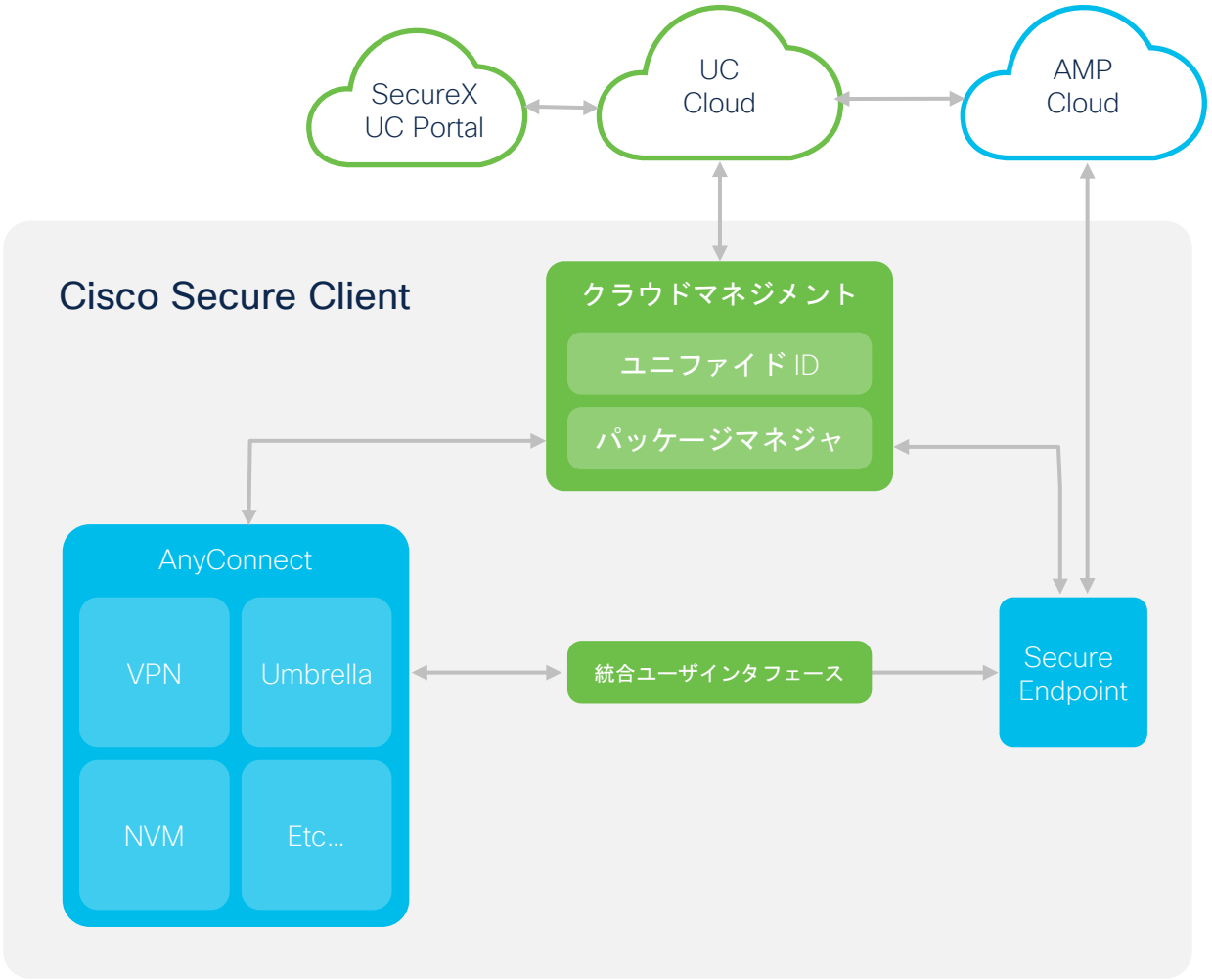
*画面は予定です。変更されることがあります。

Cisco Secure Client
アーキテクチャ概要

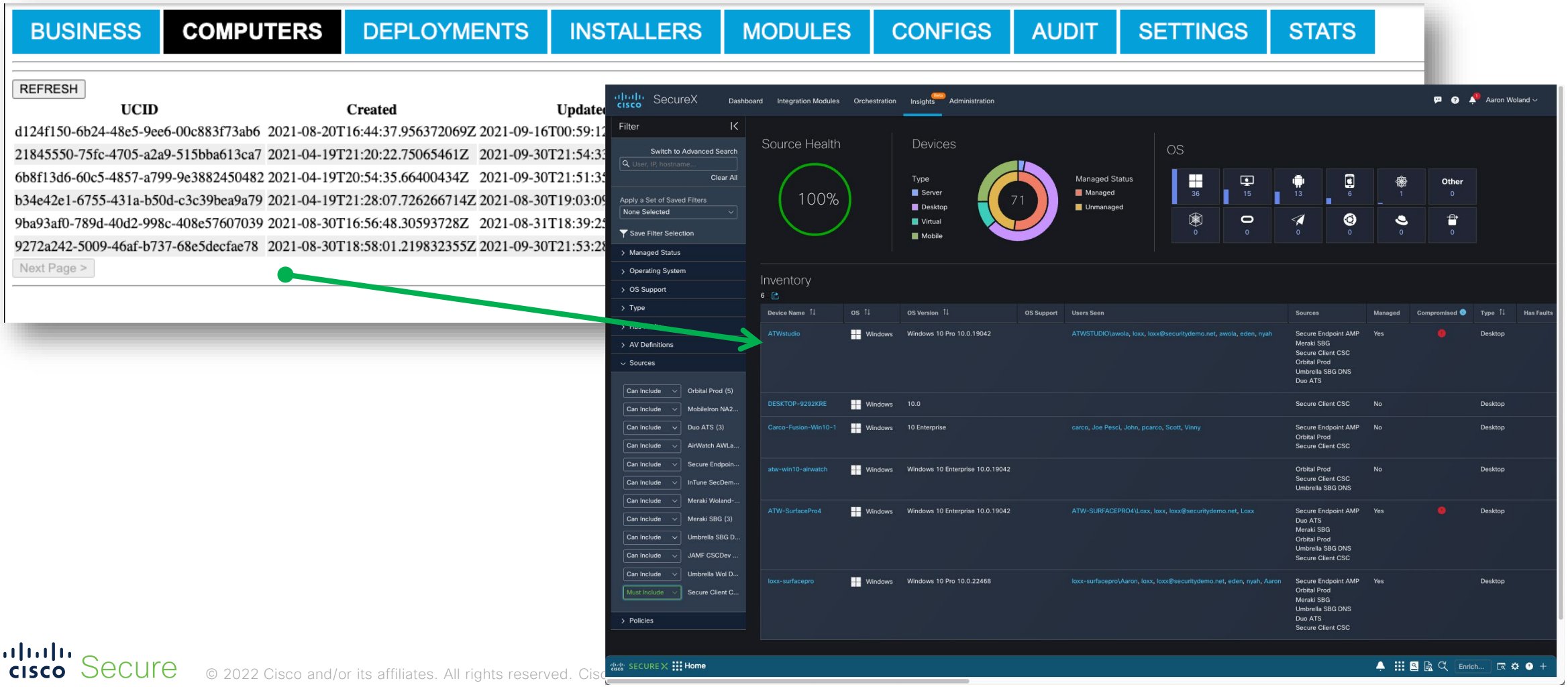
- 既存のコンポーネントと変わらない部分
- AnyConnectとSecure Endpoint 機能を搭載

- 新たに開発中の部分
- エージェントはUnified IDで管理（エンドポイント一意に決まるID）

Cisco Secure Client を構成するコンポーネント



SecureX Device Insights で可視化するエンドポイント



AnyConnect アップグレードによりクラウド管理に対応

- AnyConnect をアップグレードすることで Secure Client に移行でき、これによってこの統合エージェントソフトウェアのクラウドによる管理が可能
  - SecureX は無償で利用可能
  - SecureX device insights も利用可能

シスコのユニファイドエージェントにおける優位性

シスコの強み

どこからでも、どんなデバイスでも、どんなアプリでも、シスコはお客様のセキュリティ対策を最も包括的に最もシンプルに実現します。世界最大規模のセキュリティインテリジェンス Cisco Talos により、お客様のデジタル化をお守りします。

経済性
複雑なインフラ全般をカバーする
最もシンプルなゼロトラスト

セキュリティ
世界最大規模のセキュリティ
インテリジェンスによる防御

信頼性
中長期でのゼロトラスト化を
ご支援する長年の実績と信頼性

世界最大規模の組織

400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

世界最大規模の
セキュリティインテリジェンス

TALOS

圧倒的なデータ解析量

6000億
1日あたりの電子メールメッセージ数

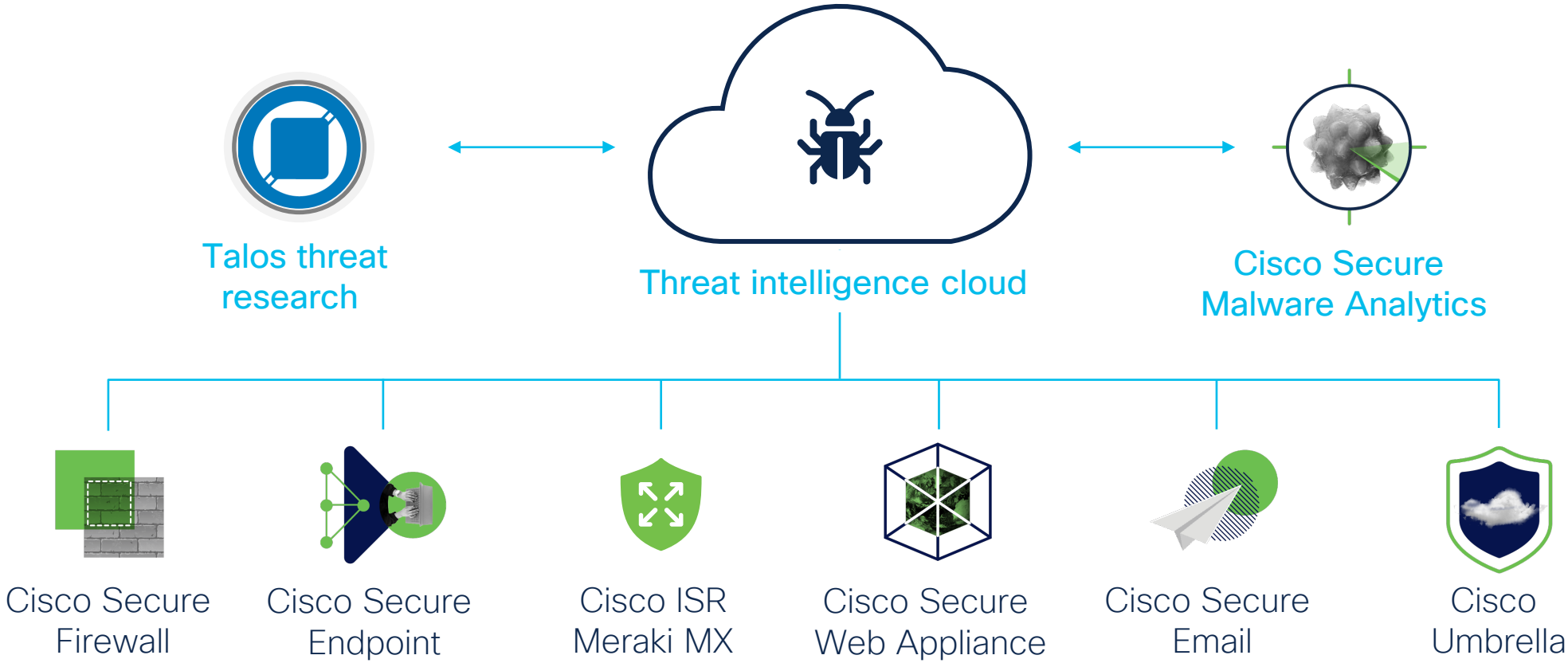
200億
1日の脅威ブロック数

160億
1日に監視されるWebリクエスト

180以上のゼロデイ脆弱性
1年間の検出数（全く新しい脅威）

cisco Secure

一度でも観測された脅威をいたるところでブロックする シスコ セキュリティ ポートフォリオ



Cisco SecureX (XDR) でセキュリティ運用を自動化

分析・調査・修復の可視化、自動化、簡素化を実現

- Ciscoセキュリティ製品ご利用で無料で利用可能
- 15分ですぐ開始（クラウドネイティブ）
- お客様環境内の脅威を半分の時間で検出[1]
- 100時間節約（一元的な可視化と自動化）
- 対応/修復にかかる時間を85%短縮[2]

シスコは、お客様のエクスペリエンスのシンプル化、導入成功への後押し、将来への対応に貢献すべく努力しています。

[1] 出典：TechValidate 社

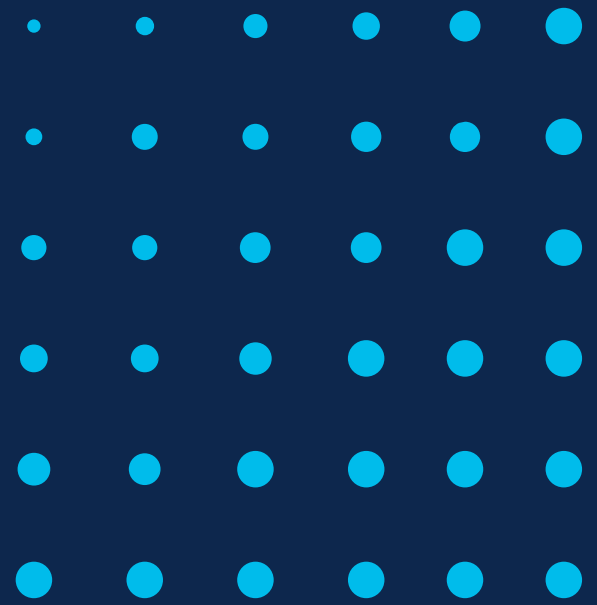
[2] 出典：シスコ内でのシミュレーションに基づく

まとめ

SASE / ゼロトラストに対応し、コンパチビリティ問題を無くすユニファイド エージェント、それが

Cisco Secure Client

3. エンドポイントにおける健全性の向上とデバイス管理の効率化



複雑化するエンドポイントの環境

- エンドポイントを管理するため、及びセキュリティを担保するため、多くのサービスやエージェントが必要になっており、環境が複雑化している。

ユーザの情報

IDP

各種クラウドサービス

クラウドサービスの管理

アクセスデバイスの情報

IT資産管理

インターネット

インターネットの管理

MFAデバイスの情報

MDM、EMM

VPN

VPNの管理

セキュリティ対策

ウィルス対策、EDR等

パスワード管理

パスワードの管理

デバイスの健全性チェックとは？なぜ必要なの？

46%

脆弱性にパッチを適用していないためにインシデントが発生した組織

- Cisco Cyber Security Report

デバイスの状態の可視化、およびコントロールができていないことが原因

Cyber Hygiene（サイバーハイジーン）

関連するすべてのIT資産の「衛生状態」を維持・管理していくための仕組み・取り組み

インベントリ管理、脆弱性管理、構成管理（パッチ適用含む）　etc.

デバイスに潜む脆弱性・設定上の欠陥をなくしていくことで攻撃されるリスクを軽減させる

2021 Duo Trusted Access Report

800 million
Authentications per Month

36 million+
Devices

400,000+
Unique Applications

- 本レポートでは、北米、中南米、ヨーロッパ、中東、アジア太平洋地域の顧客基盤から得られた、3,600万台以上のデバイス、400,000以上のアプリケーション、約8億件の月間認証データを分析
- 2020年6月1日から2021年5月31日までの期間で調査

Source: https://www.cisco.com/c/dam/en/us/products/se/2021/10/Collateral/duo-trusted-access-report.pdf

データ分析サマリー

MFA でパスワードの強化が継続

多要素認証は強力さを保ちながら、従来のパスワードのみのセキュリティを強化し続けています。Duo の MFA の利用は、この 1 年で 39% 増加しました。

クラウドでの利用が増加

クラウドアプリケーションに対する認証は、認証全体の 13% から 15% に増加しました。

生体認証の拡大

71% を超えるスマートフォンで生体認証が有効になっていて、スマートフォン全体で 12% 増加しています。

古いソフトウェアを搭載したデバイスの認証拒否

古いソフトウェアを搭載したデバイスの認証が拒否される件数は、2020 年から 2021 年の間に 33% 増加しました。

ブロックされた場所

デバイスベースのポリシーを導入している組織の約 74% が、中国とロシアからのアクセスを制限しています。

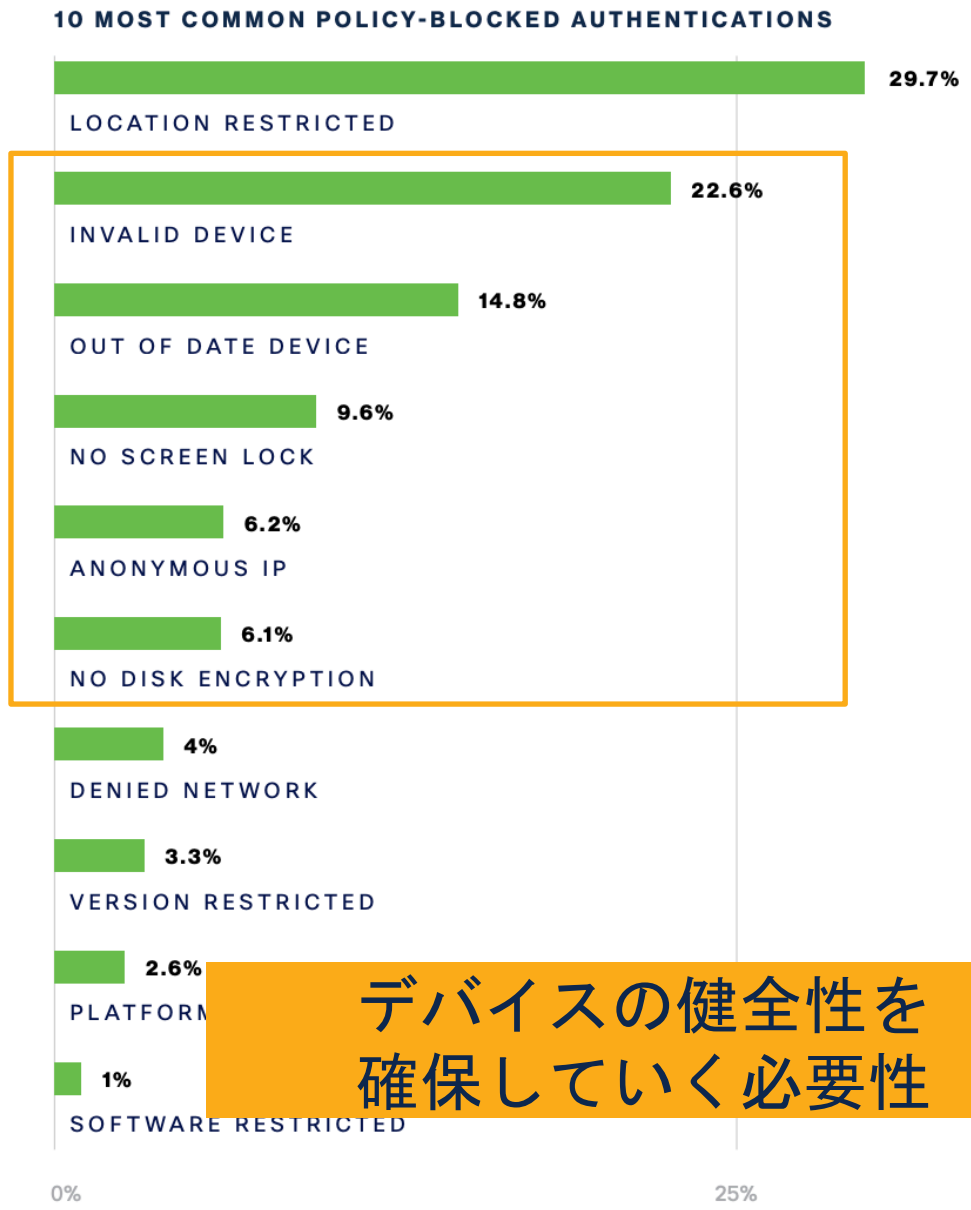
ハイブリッドアプローチを採用している企業が増加

リモート アクセス アプリケーションを使用している企業の割合は、2020 年 3 月から 8 月にかけてピークをわずかに下回っていますが、その後の 9 ヵ月間で、平均月間認証数ベースで 15% 高い状態が続いています。

適応型ポリシー制御

ブロックが発生した要因

1. ロケーション
2. 不正なデバイス
3. 最新でないデバイス
4. スクリーンロックされていない
5. 匿名 IP
6. ディスク暗号化していない
7. 拒否されたネットワーク
8. バージョンによる制限



デバイスの健全性を
確保していく必要性

国内でサイバー攻撃の被害が増加

身代金ウイルスで電子カルテ使えず混乱…徳島・半田病院 診療全面再開に２か月

国内１１病院がコンピューターウイルス「ランサムウェア」の被害を受けていたことが明らかになった。そのうちの一つ、徳島県つるぎ町立半田病院では８万人以上の患者の電子カルテが使えなくなり、患者たちも不安を募らせる深刻な事態に直面していた。

手書きで作り直し

「こんな田舎の病院を狙うなんて想定外だ」

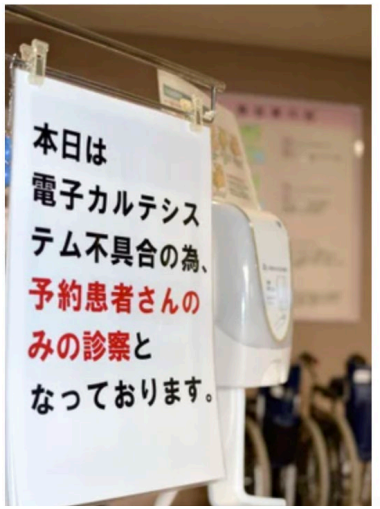
半田病院（１２０床）の丸笹寿也事務長（５５）はため息をついた。

同病院は１０月３１日未明、**身代金要求型コンピューターウイルス「ランサムウェア」に感染。約８万５０００人分の電子カルテのデータが暗号化され、氏名や年齢、治療内容、投薬履歴などの基本情報が失われた。**院内のプリンターからは「身代金を払わなければ、盗んだデータを公開する」との英文の脅迫文が刷り出された。

https://www.yomiuri.co.jp/local/kansai/news/20211229-OYO1T50000/

「身代金」ウイルス、国内１１病院が被害…救急搬送や手術に支障も

世界各地で重要インフラがサイバー攻撃にさらされる中で、国内で２０１６年以降、少なくとも１１病院がコンピューターウイルス「ランサムウェア」による被害を受けていたことが、読売新聞の取材でわかった。救急搬送の受け入れや手術の停止、外来診療の制限などの被害が出ており、医療機関が攻撃対象になっている実態が浮き彫りになった。



被害は１６年１件、１７年３件、１８年１件、１９年１件、２０年０件だったが、２１年は５件に急増。身代金を支払った病院は確認されなかった。すでに各病院では対策を講じている。厚生労働省はサイバー攻撃を受けた医療機関に報告を求めているが、発生件数は公表しておらず、ほかにも被害を受けたケースがあるとみられる。

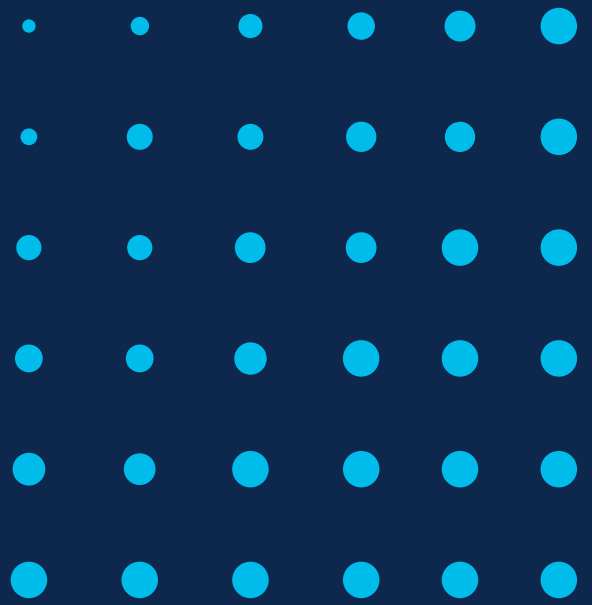
１７年までの被害は、病院の業務用パソコンのメールが送受信できなくなったり、ファイルが開かなくなったりするなど比較的軽微なものが多かった。

１８年以降は、**電子カルテや医事会計、コンピューター断層撮影法（ＣＴ）で撮影した画像の管理といった病院内の基幹システムが機能停止に陥る被害が確認**されるようになった。

https://www.yomiuri.co.jp/national/20211228-OYT1T50173/

エンドポイントにおける健全性の向上

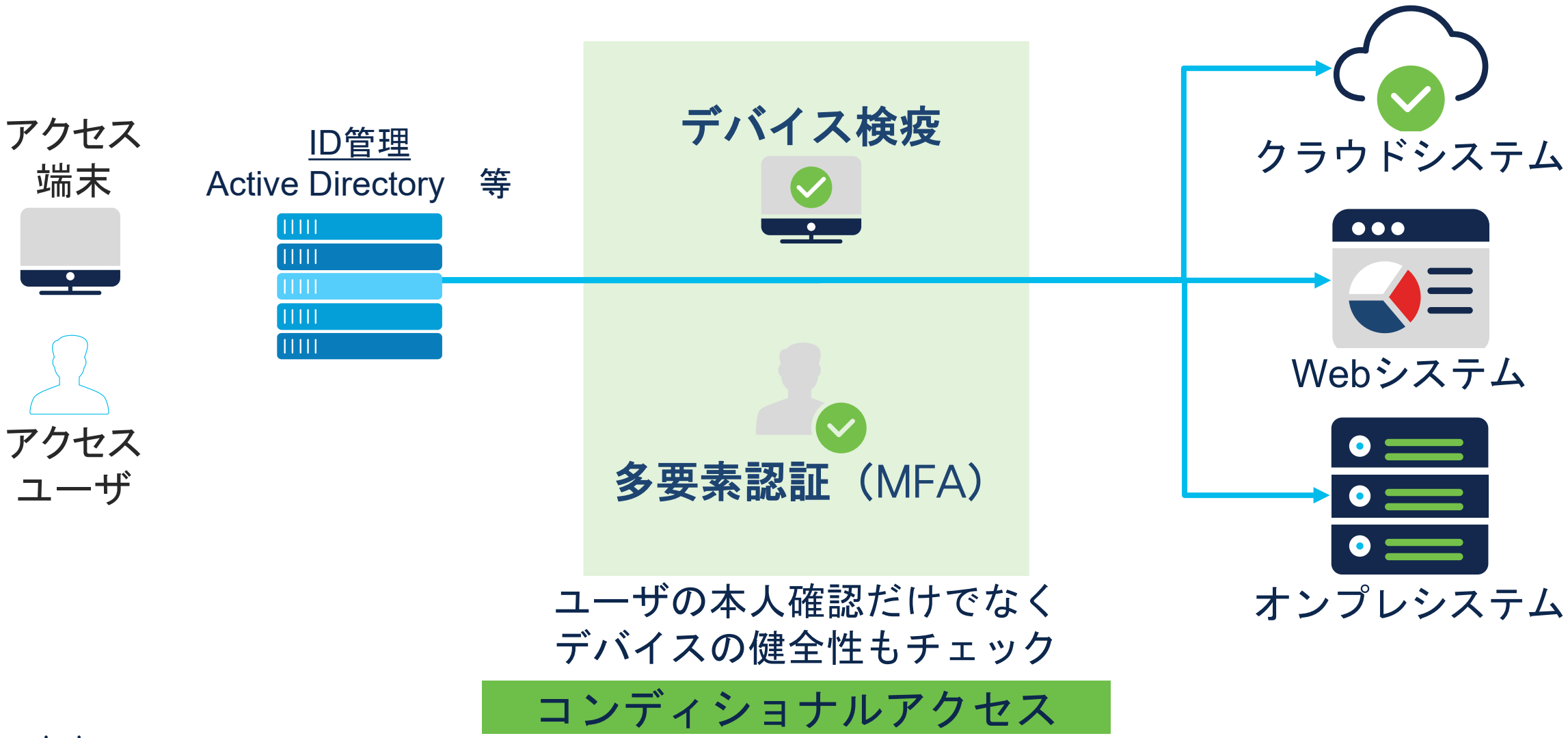
→コンディショナルアクセス



情報資産へのアクセス

ユーザの信頼性の担保(MFA)だけでは不十分

情報資産へのアクセス時にデバイス健全性を確認



ユーザの本人確認だけでなく
デバイスの健全性もチェック

コンディショナルアクセス

一般的なコンディショナルアクセス

- ✓ 「どこから」「誰が」「どのデバイスで」「どのアプリケーションに」の情報をID管理情報、IT資産管理、MDMからデバイス情報を取得した上で、ユーザ及びデバイスにアクセスする条件を設定して、アクセスさせる。

統合ID管理（IDP）

企業で保有するユーザ情報、組織情報やクレデンシャル情報を体系的に管理し、端末情報や認証制御も行う

IT資産管理

企業のパソコンや機器の情報を一括で管理。端末のアプリケーションやファイルの制御も可能。

モバイルデバイス管理 （MDM、EMM）

企業で保有するモバイルデバイスの情報を一括で管理。端末のアプリケーションやファイルの制御も可能。紛失時のロックやワイプも可能

ユーザの情報

アクセスデバイスの情報

MFAデバイスの情報

条件を設定し、信頼できるユーザ及びデバイスのみをアクセスさせる

情報ソースの整理や連携に課題

- ✓ IDP、IT資産管理、MDMはそれぞれ目的を持って、システム化されており、グループに応じた管理レベルを合わせることが困難となっている。

ID管理　機能例

ID管理の機能

ドメインの管理
ドメイン間の連携管理
アクセス権限管理（共有フォルダへのアクセス等）
シングルサインオン
AD用証明書管理
クレデンシャルの管理（ID/パスワード、MFA等）
パスワードポリシーの管理
ユーザ情報の管理(会社名、部署、電話番号等)
グループの管理(OU、OU間の管理)
AD連携構成の管理（フォレスト、ツリー）
ポリシーの管理
端末管理(インストール制限、USB制限等)
認証ログの管理
クライアントアプリの制限の管理
etc…

IT資産管理 機能例

IT資産管理の機能

OSアップデート
デバイスの使用制限
ソフトウェア
デバイスログの管理
デバイスの使用制限の管理
操作ログの管理
マルウェア対策ソフトとの連携
データの暗号化
メンテナンス（リモート）
モバイル機器管理
レポート作成
サーバの監査
etc…

MDM資産管理 機能例

MDMの機能

モバイルデバイス一括管理(OS等)
アプリケーションの一括管理
ファイルのダウンロード制限
コンテンツ管理、配信
端末の紛失、盗難対策
セキュリティ対策
端末利用ログの可視化
etc…

各システム間での情報連携、組織管理の統一化は設定、運用が煩雑

同じグループポリシー適用が困難

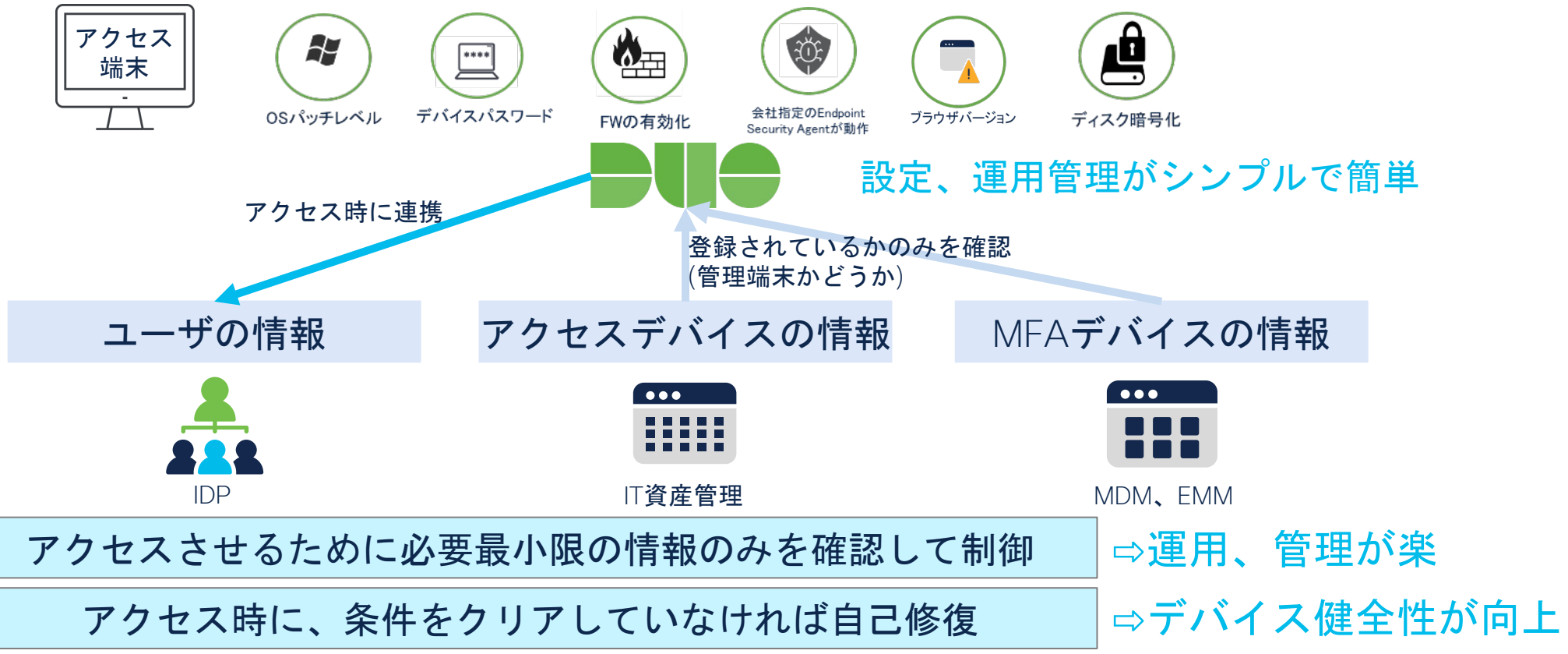
解決策

Best：全ての管理ソースを完全連携して
統合的な管理を行なっていく⇨実現可能？

代案：全ての管理を密結合で実現するのではなく、
必要な情報のみを疎結合で実現する

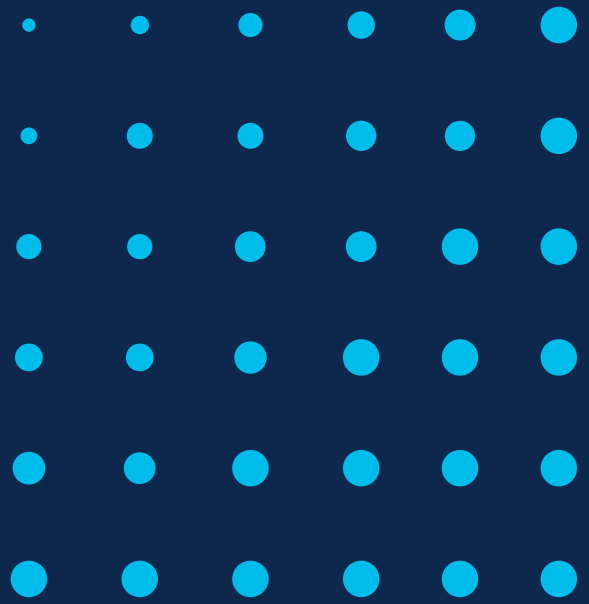
Duo のコンディショナルアクセス

✓ Duo は運用が煩雑な密結合を排除し、最低限のシステム連携で、アクセス端末から必要最小限の情報を取得することでコンディショナルアクセスを実現している。



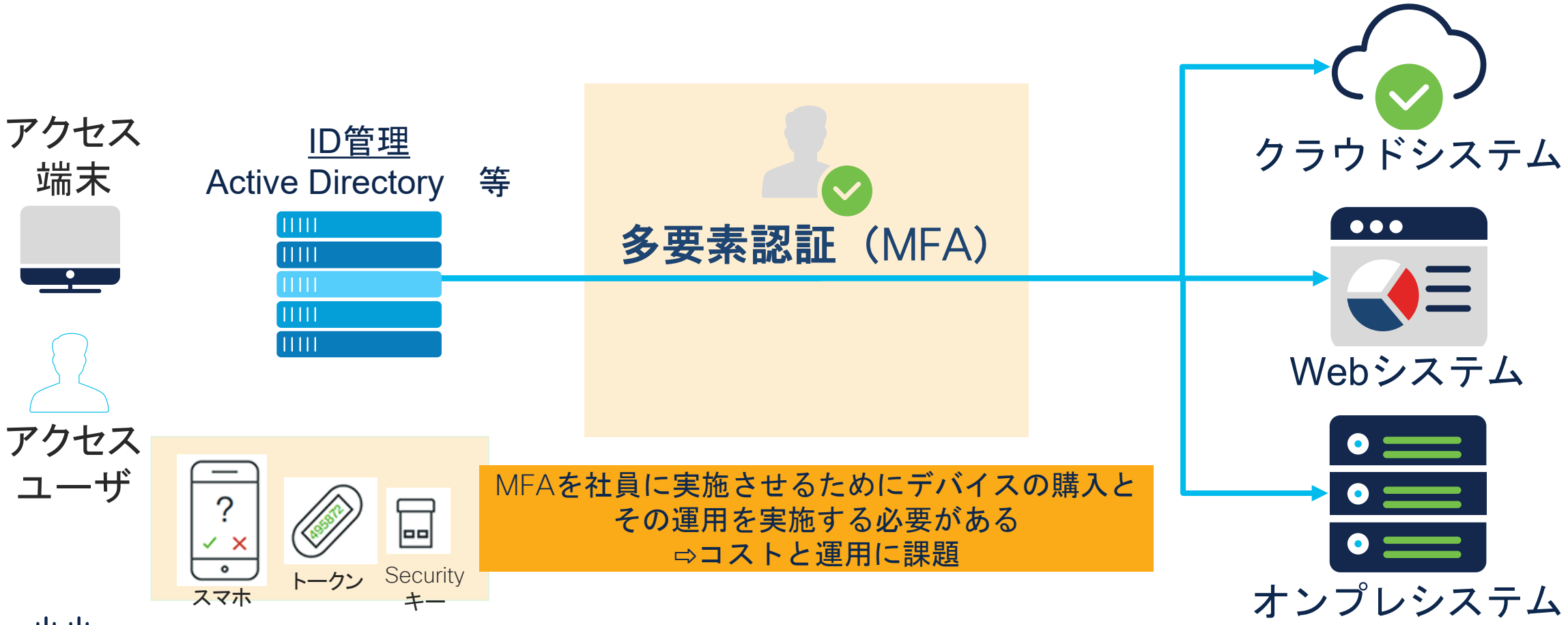
デバイス管理の効率化

→パスワードレス認証



エンドポイント（MFAデバイス）の問題

- 社内の情報資産へアクセスさせる際に、多要素認証（MFA）を実施するために、社員に新たなデバイスを付与する必要がある。（コストと運用に課題）



事例：お客様事例（放送業界）

課題

パンデミック対策としてテレワーカーの範囲が広がり、VPN 利用者が急増。 なりすましや不正利用などセキュリティへの懸念が高まる

ソリューション

DuoはADとの同期が簡単、ユーザーをADで一元管理できることで社内展開も容易。アペンドモードでユーザーのシンプルな操作性を実現

結果

扱うシステムに関わらず安全なテレワーク環境を整えるため、全 VPN ユーザーをDuo による多要素素認証に移行

テレワーク環境からの安全な社内システムの利用が可能に

今後

Duoの豊富な連携性により他サービスへの適用および、SSO などユーザーの利便性と安全性を高めるサービス提供を検討

検討時：MFAデバイスについて

・全員に社給のスマホは配っていない。配る予算はない。
・個人のスマホのBYODで利用するしかない
・個人のスマホを持っていない担当者もいる

⇨スマホの予算、購入後の運用（個人差、管理者側の問い合わせ対応が大きい課題）、

パスワードに関する問題

- クラウドの利用型のサービスが増えることによって、環境が複雑化し、パスワードは管理者にとっても、エンドユーザにとっても負担となっている。

面倒でコストが掛かる	ユーザーエクスペリエンス	セキュリティ
		
20-50%	190	61%
ヘルプデスク: パスワードに関連する チケットの割合	# of passwords : 企業に勤める人が使用 する平均のパスワード数	不正侵入の60%以上は ID/パスワードの漏洩や、 弱いパスワードが原因
- Gartner Group	- LastPass Research	- Verizon Data Breach Report 2021

パスワードレスへの移行を検討したいが、デバイスの置き換え、管理側の負荷が大きい

解決策

デバイス管理の効率化
⇨アクセスデバイスで認証

パスワードレスへの移行の管理負荷
⇨視覚的にパスワードレスへエンドユーザ自身の選択で移行する

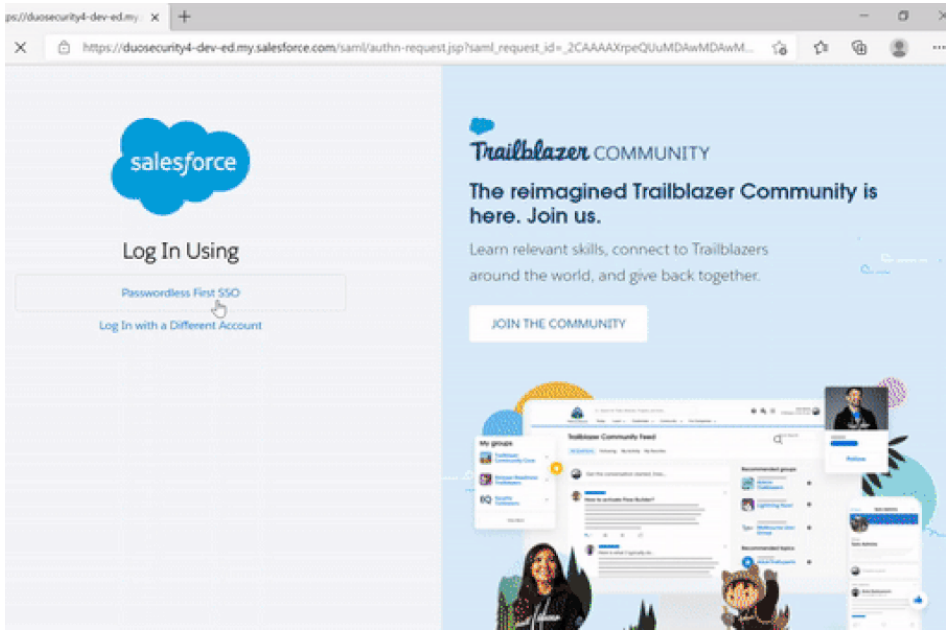
Verify
User Trust

Passwordless SSO

問題点：
誰もがパスワードに依存した認証のリスクを理解している。課題は、より安全で使いやすい認証方法にスムーズに移行すること。

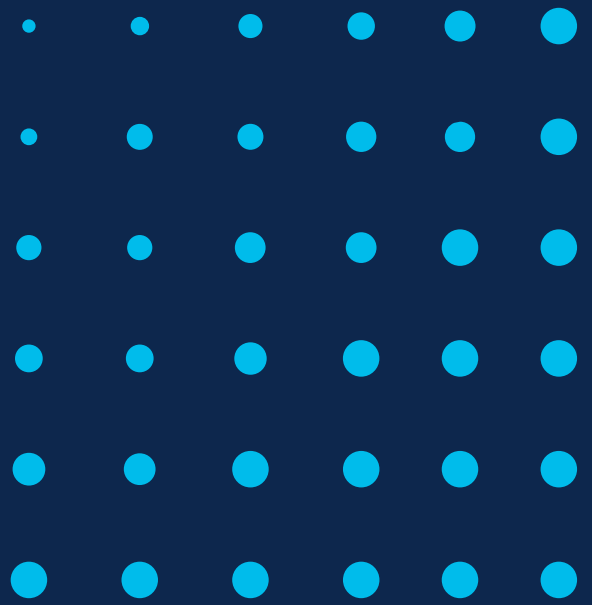
解決策：
パスワードレス認証は、ユーザーのアイデンティティを単一かつ強力に保証し、ユーザーの信頼性を確保する。
Duoは、パスワードレスには以下の要素も必要だと考えている。

- エンドユーザーが直感的に操作でき、かつ信頼感を得られる
- 現在のテクノロジースタックとセキュリティ戦略の強化
- ヘルプデスクのコストと負担の軽減

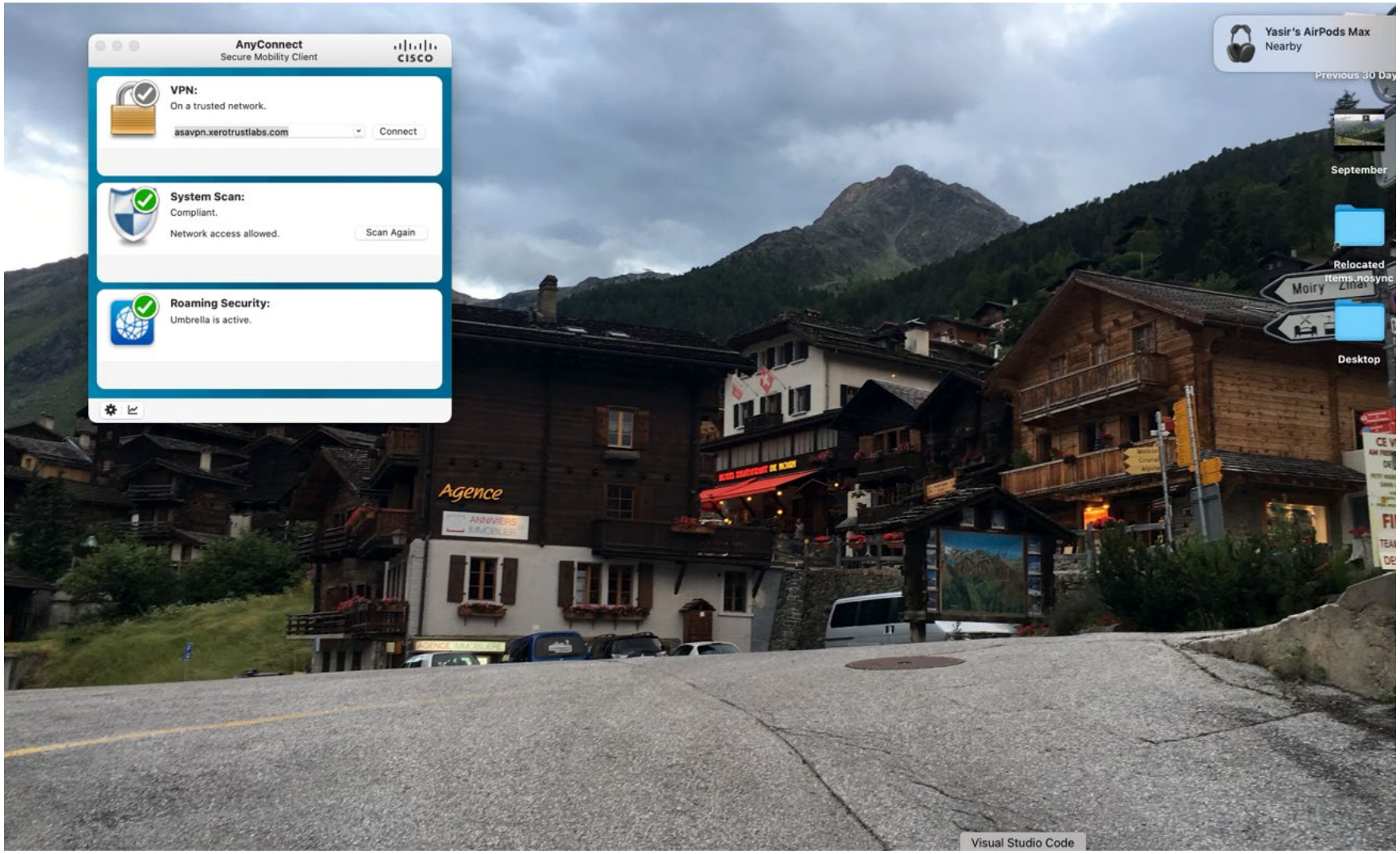


ロードマップ： 12月から Public Preview、GAは今年前半(7月/2022)

Duo PasswordLess Demo



Passwordless (Anyconnect)デモ



パスワードレスによるデバイスの効率化

- パスワードレスの導入により、デバイスの効率化を実現するとともに、エンドユーザ及び管理者の負荷を軽減することが可能となる。

エンドユーザ

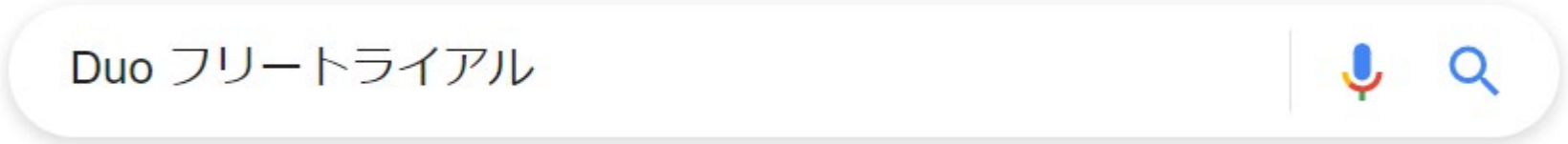
- MFAデバイスを保持する必要なし
- MFAデバイスのメンテナンス不要
- パスワードを一定期間で変更する必要がない（パスワードを覚えておける）
- パスワードの入力負荷軽減
- ID/パスワードの漏洩懸念の払拭
- ID/パスワードのシステムごとの記憶負荷の軽減

管理者

- MFAデバイス購入不要
- MFAデバイスの管理、運用が不要
- パスワードを一定期間で変更する際の運用、問い合わせ負荷軽減
- パスワードの問い合わせ負荷軽減
- ID /パスワードの漏洩対策の軽減
- セキュリティリスクの軽減

- ご質問は、本ウェビナー終了後に表示されますアンケートに　ご記入ください。
  追ってご連絡差し上げます。

- Duoの30日間フリートライアルをぜひお試しください！



で検索

または
https://www.cisco.com/jp/go/tryduo


cisco
Secure