The bridge to possible

# シスコと SASE：機能、概念、将来のビジョン

SASE の概要、SASE が重要な理由、Cisco SASEソリューション概要

中村 光宏
セキュリティ事業 シニアSEマネージャ

# 内容

- SASE を導入するべき理由
- SASE とは
- ユースケース
- SASE の成果
- シスコの SASE ビジョン
- シスコが選ばれる理由

# SASE を導入するべき理由

# 未来はどんどん進化していく


*の企業が、2023年まで現在のビジネスモデルが経済的に存続すると考えている。*

Source: The new digital edge: Rethinking strategy for the postpandemic era, McKinsey, May 2021

# ハイブリッドワークが組織のあり方を変える


*のCIOが、分散した従業員がアプリケーションにシームレスにアクセスできるようにすることが重要であり、高品質のコラボレーション体験を実現することが重要であると回答した*

Source: Accelerating Digital Agility Research (CIO Data) — Cisco, 2021

# アプリケーションは多様なIT環境に超分散している


*のCIOが、ユーザーデバイス、ネットワーク、クラウド、アプリケーションのセキュリティ、コントロール、ガバナンスを維持することが重要であると回答した*

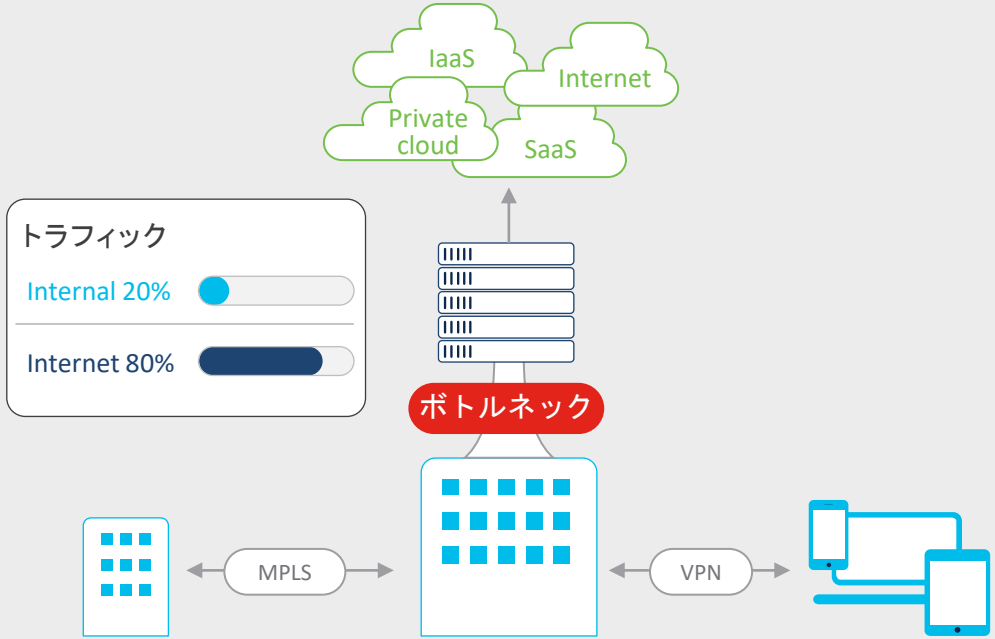

*のCIOは、シームレスなコンシューマーエクスペリエンスを提供するために、インサイトがこれまで以上に重要になると考えている*

Source: Accelerating Digital Agility Research (CIO Data) — Cisco, 2021


# 従来のネットワーキングモデルでは不十分

トラフィックパターンの変化がボトルネックと
パフォーマンスの課題を生み出している

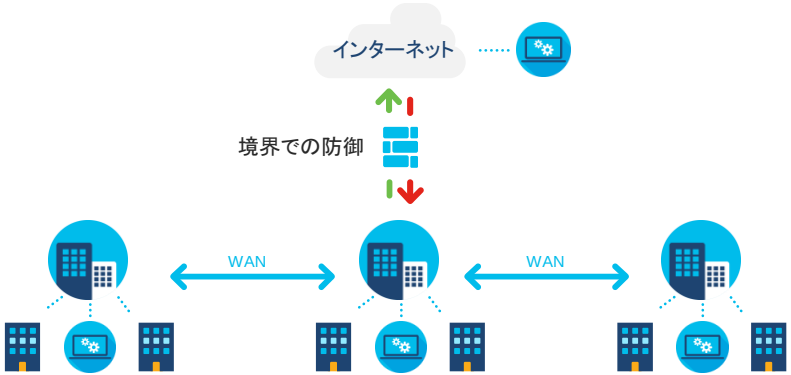
課題
- アプリのパフォーマンス
- ユーザーエクスペリエンス
- セキュリティの有効性
- # ツール/ベンダーの数
- 統合化




# ネットワークの変革

## クラウドが新たなデータセンター | インターネットが新たな企業ネットワーク

**拠点がベース**



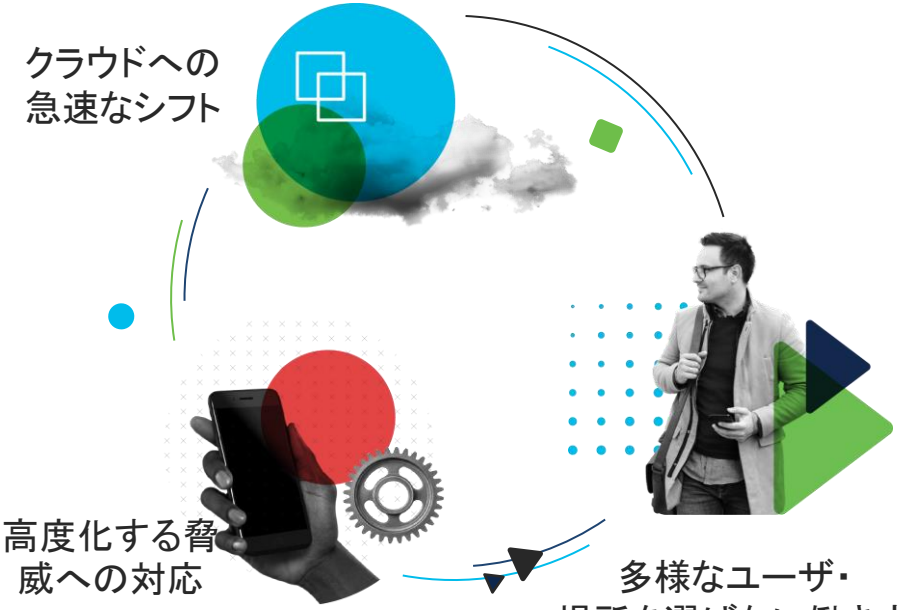

**ユーザ/デバイス⇔アプリケーション**


データセンター中心
境界セキュリティ
信頼されたネットワーク

NW Security

マルチクラウド＋インターネットが中心
境界はエッジに分散
ゼロトラストネットワーク

# ネットワーキングチームとセキュリティチームが抱えている課題




インフラがボトルネック


ゼロトラストモデルへのシフト

新たな統合アプローチが必要

# SASE とは

# お客様からの声

SASE がよくわからない！

ハイブリッド IT 環境があり、
すぐにクラウドに 100% 移行する
予定はない

ゼロトラストと
同じじゃないの？

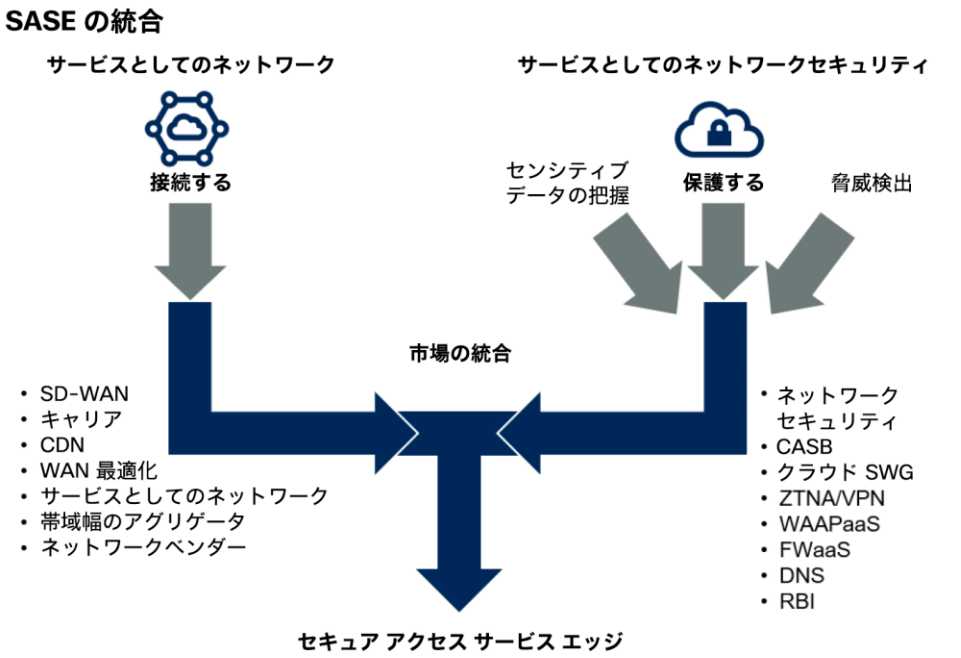
将来的に取り組む予定

新しい頭字語がど
んどん出てくる

トラフィック
がローカルで
突如発生する

クラウドエッジに
セキュリティを
押しつけている

# SASE とは？




CDN：コンテンツ配信ネットワーク、RBI：リモートブラウザ分離、WAAPaaS：サービスとしての Web アプリケーションおよび API 保護。
出典：Gartner 社
ID: 441737

## SASEとは

Secure な Web ゲートウェイ、
CASB、
Firewall、
Zero Trust Network Access
などの
クラウドネイティブなSecurity機能と
VPN および WAN 機能を
組み合わせた将来の
ネットワークアーキテクチャ
として提唱されたもの (2019年)

Gartner



https://www.gartner.com/doc/reprints?id=1-1OG9EZYB&ct=190903&st=sb [英語]

# アナリストはクラウドネイティブサービスへの移行に合意

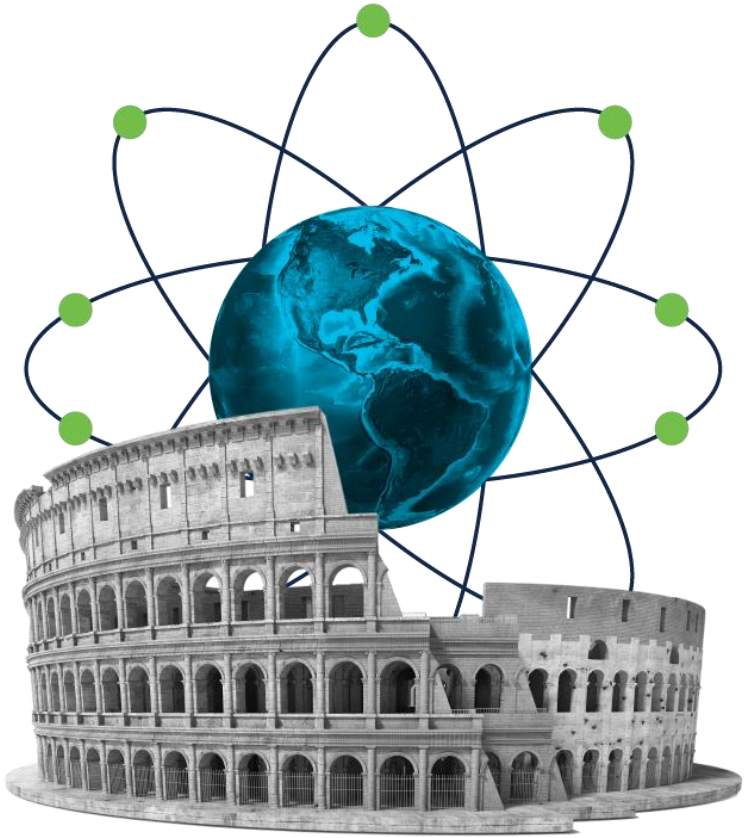
**この多機能アプローチには多くの名前がある**

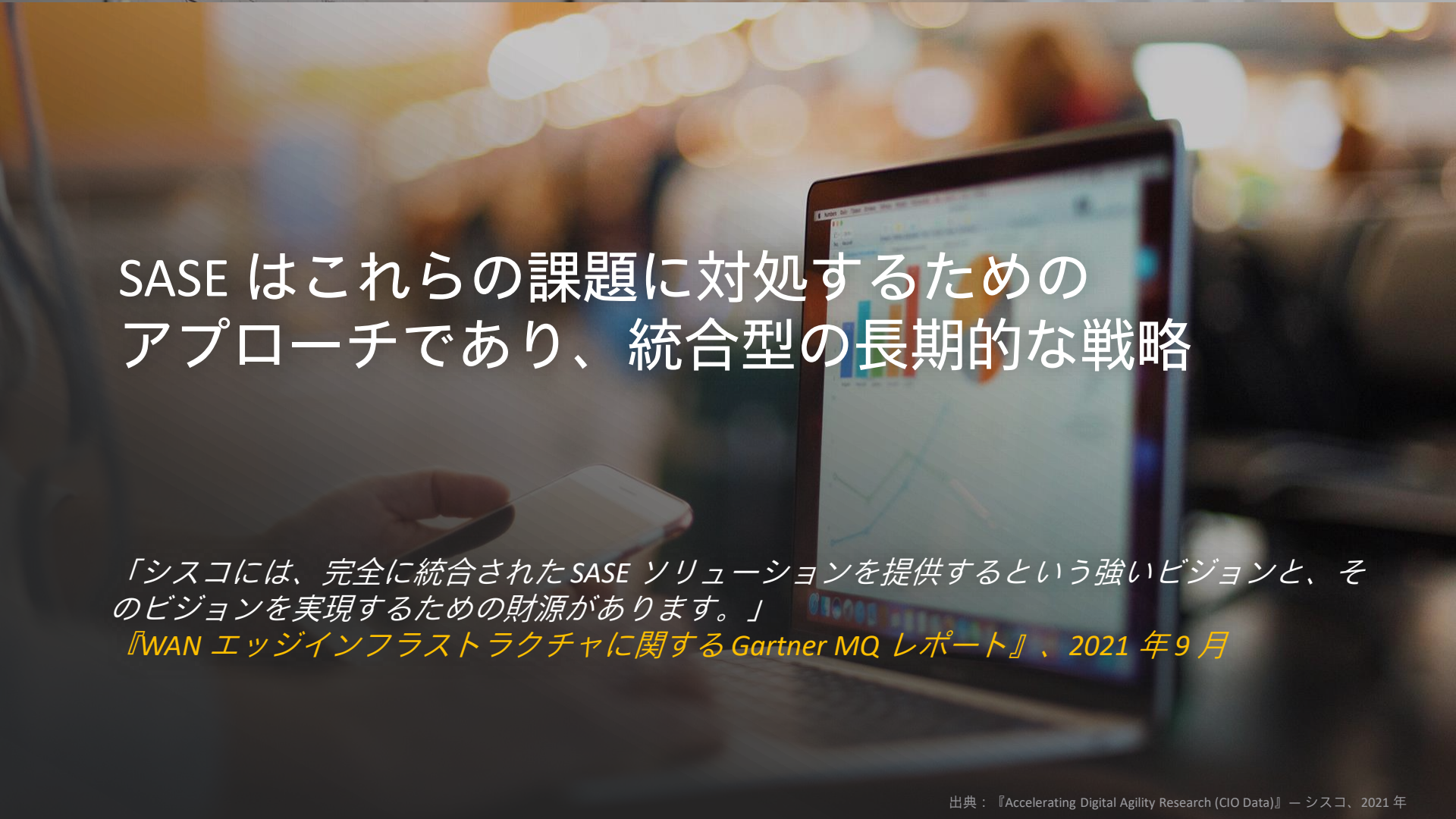
| | |
|---|---|
| Gartner | セキュア アクセス サービス エッジ（SASE） |
| FORRESTER® | ゼロトラストエッジ |
| IDC | クラウド セキュリティ ゲートウェイ |
| ESG | エラスティック クラウド ゲートウェイ |

**クラウドネイティブへの集約については完全に一致**

# アナリストによる SASE の定義

- トラフィックがクラウドエッジで検査される
- ユーザーとエッジデバイスはどこにでも配置でき、アクセスネットワークはインターネット
- ポリシーがユーザーを追従する
- 一貫したネットワークポリシーとセキュリティポリシーによるコンテキスト主導



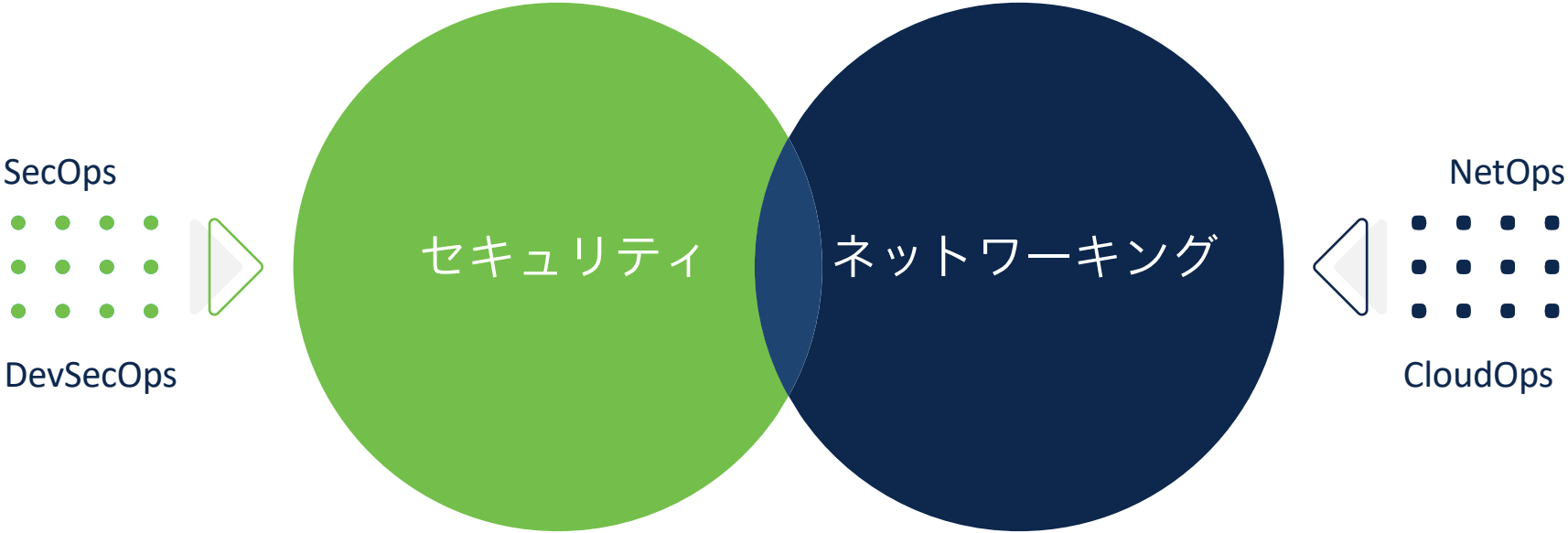


# SASE はこれらの課題に対処するための アプローチであり、統合型の長期的な戦略

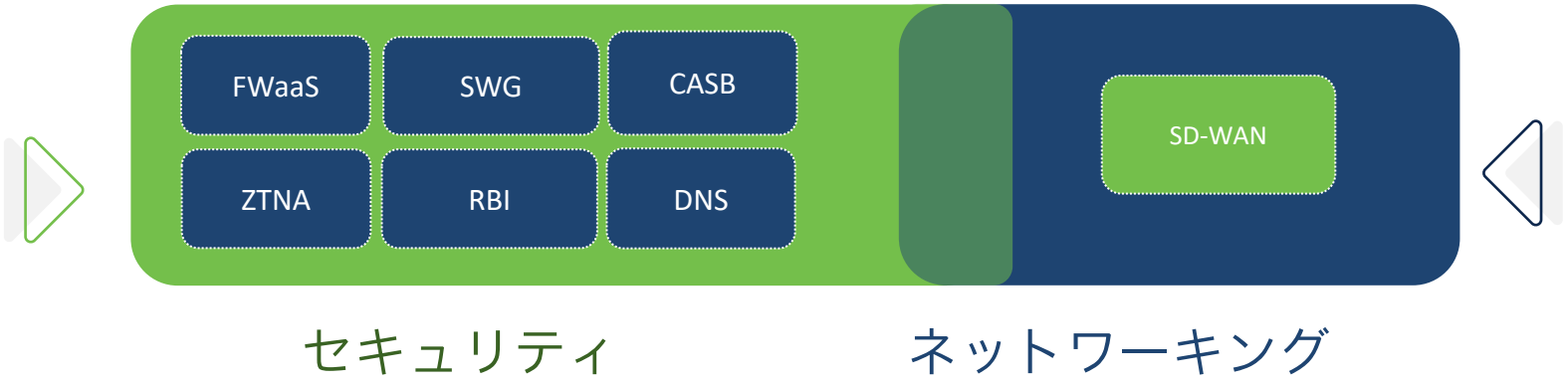
*「シスコには、完全に統合された SASE ソリューションを提供するという強いビジョンと、そのビジョンを実現するための財源があります。」*
*『WAN エッジインフラストラクチャに関する Gartner MQ レポート』、2021 年 9 月*

出典：『Accelerating Digital Agility Research (CIO Data)』— シスコ、2021 年

# SASE：クラウドでのネットワーキングとセキュリティの統合



# SASE：クラウドでのネットワーキングとセキュリティの統合



# SASE でできること

- ユーザーやアプリの場所を問わず、セキュアな接続をサービスとして提供
- どこからでもシームレスかつセキュアに、ユーザーを必要なアプリやデータに接続
- ユーザーの作業場所を問わず、アクセスを制御して適切なセキュリティ保護を適用

*2025 年までに少なくとも 60% の企業が、ユーザー、ブランチ、エッジアクセスを含めた SASE を採用するための明確な戦略とタイムラインを掲げるでしょう。*

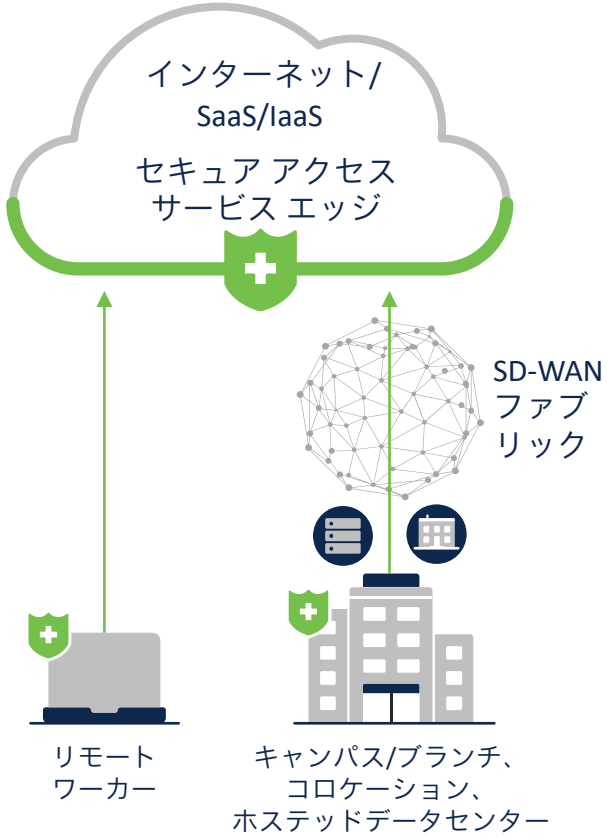
Gartner『2021 Strategic Roadmap for SASE Convergence』

# SASE のユースケース

# SASE の主要なユースケース

## リモートワーカーの保護

- あらゆる場所からアプリケーションやデータにシームレスに接続
- インターネットとクラウドアプリケーションに安全にアクセス
- ユーザーを認証し、デバイスの健全性を確認
- すべてのリモートワーカーに最適な接続環境とアプリケーション エクスペリエンスを提供




## セキュアエッジ

- さまざまな場所にあるオフィスからアプリケーションに簡単に接続
- 数千のユーザと拠点すべてに SD-WAN ファブリックをプロビジョニング
- アプリケーションへの安全なアクセスと、ダイレクト インターネット アクセスの安全な利用
- ISP、SaaS、パブリックおよびプライベート アプリケーション全体の問題を特定して解決

# お客様の成果

# SASE でお客様が実現できること：
## クラウドでのネットワーキングとセキュリティの統合

### セキュアなアクセスが可能な接続環境

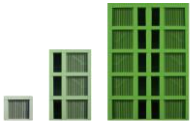
1 つのサービスで、すべてのビジネス拠点、リモートワーカー、デバイス、ワークロードを対象とした統合セキュリティを実現

### ゼロトラスト ネットワーク アクセスの導入

セッションごとにデバイスのユーザ ID と健全性を確認

### 最良のユーザーエクスペリエンスを提供

ユーザからあらゆるネットワークやクラウドのアプリケーションまで、エンドツーエンドでオブザーバビリティを確保して異常を修復



### ビジネスの俊敏性向上

クラウドを活用して複雑さを排除し、グローバルな拡張性を迅速に提供

### パフォーマンスの最適化

きわめて高速で信頼性の高いセキュアなパスを確立

# SASE アーキテクチャ実現へのプロセス

ネットワークと
セキュリティの
統合サービス

柔軟な利用モデル

クラウドネイティブ
のマイクロサービス
ベース アーキテク
チャ

SASE：セキュア アクセス
サービス エッジ

効果的な
セキュリティと
脅威防御

グローバルでの
評価および連携

すべてのデバイスや
エージェントを
サポート

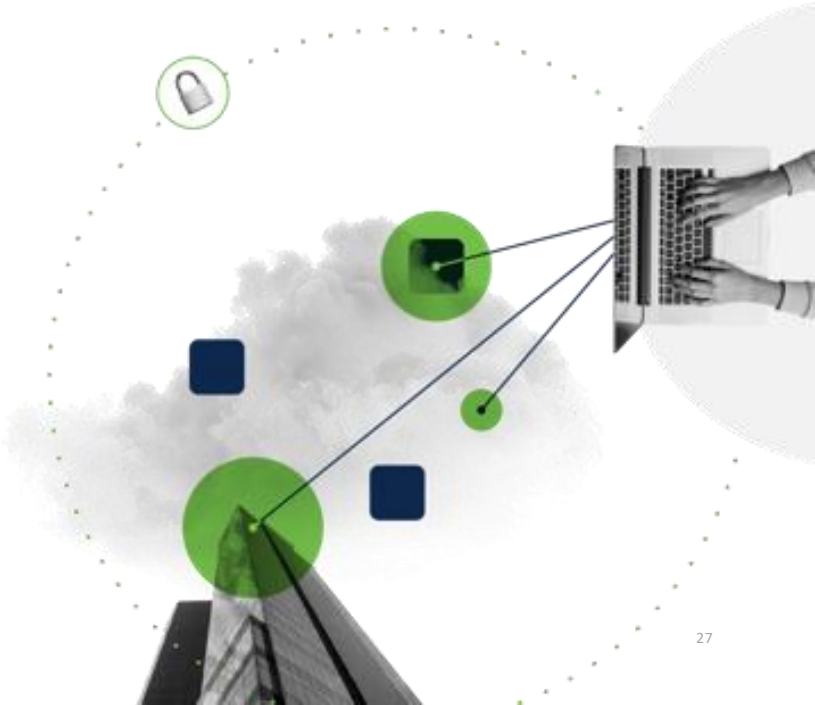
# お客様独自の方法で
# ニーズに合わせて SASE を導入

# シスコのビジョン

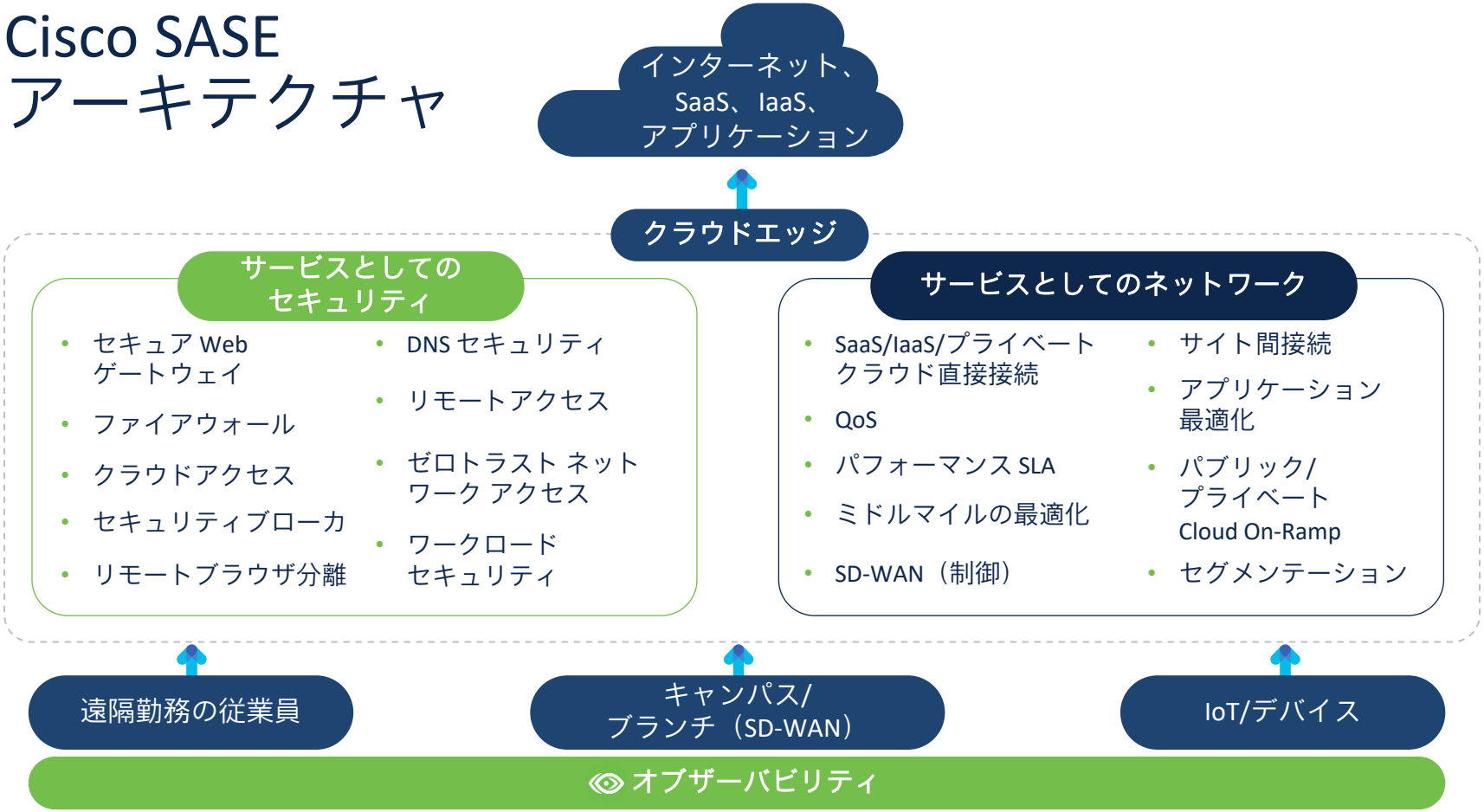
# SASE のビジョン

クラス最高のネットワーキング、セキュリティ、オブザーバビリティの各機能を単一のサブスクリプションサービスに集約します。

ユーザーの勤務場所にかかわらず、あらゆるアプリケーションに、すべてのネットワークからセキュアにアクセスできるようにします。

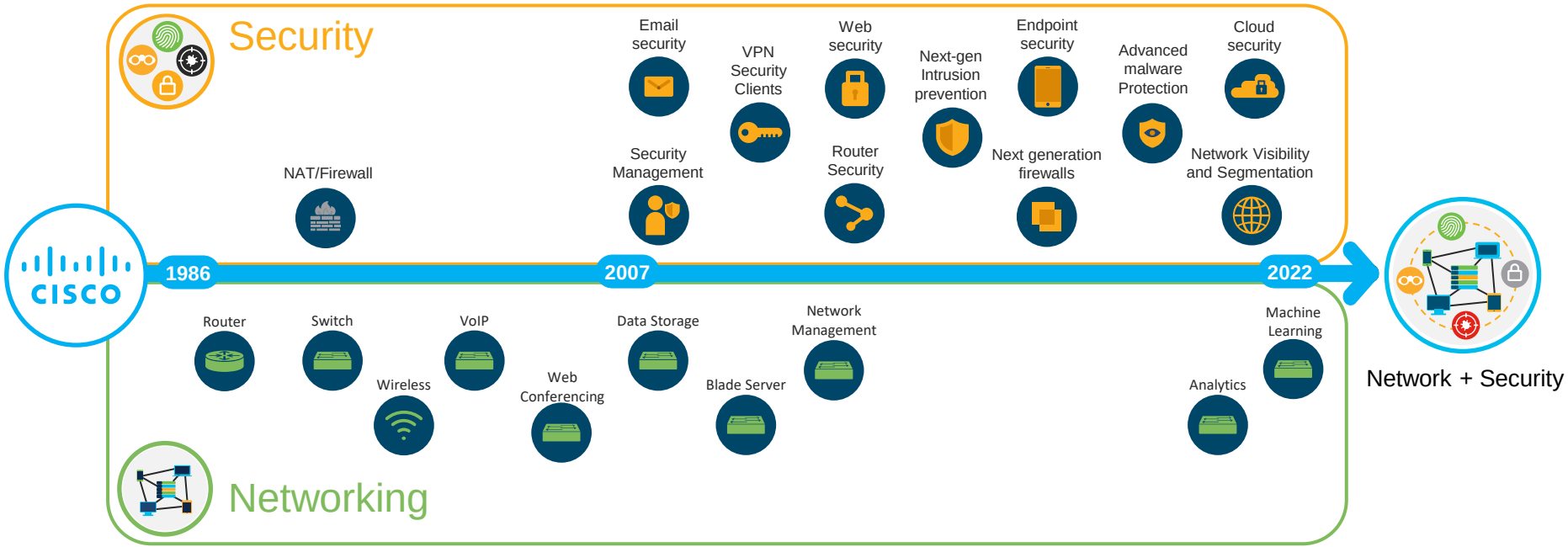


# Cisco SASE アーキテクチャ

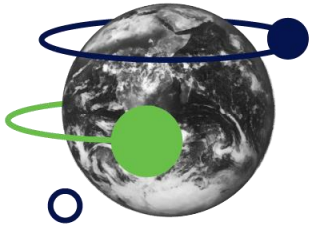


# シスコが選ばれる理由

# Cisco understands networking AND security



# SASE はシスコの DNA に組み込まれている



## ネットワーキング

最大の SD-WAN
ソリューションプロバイダー

WAN Edge Magic Quadrant のリーダー（2020 年）

## セキュリティ

フォーチュン 100 社すべてで
セキュリティを保護

2 年連続の
ゼロトラストリーダー

## オブザーバビリティ

クラウドコンピューティング
ベスト製品賞を受賞（2021 年）

インターネットとクラウドネットワークに
関する最大規模の総合的な見解

# ネットワークとセキュリティのイノベーターとして実績

2021 Best Security Company
SC Media

2021 WAN Edge
Magic Quadrant

2021 Cloud Computing Product of the Year
ThousandEyes

2020 CRN Tech Innovators
SASE

2020 Zero-Trust eXtended Ecosystem
Forrester Wave

Securing
100%
of the
Fortune 100

80%of
the internet traffic through Cisco's infrastructure
.

61M
endpoints protected

70%
SD-WAN
market share

840k+
networks protected

40k+
WAN Edge customers

The bridge to possible

# 場所にしばられない働き方

## SASE でネットワークとセキュリティを刷新

Shigeru Kimura
セキュリティ事業 アーキテクト/エバンジェリスト

# 場所にしばられない働き方

## SASE でネットワークとセキュリティを刷新

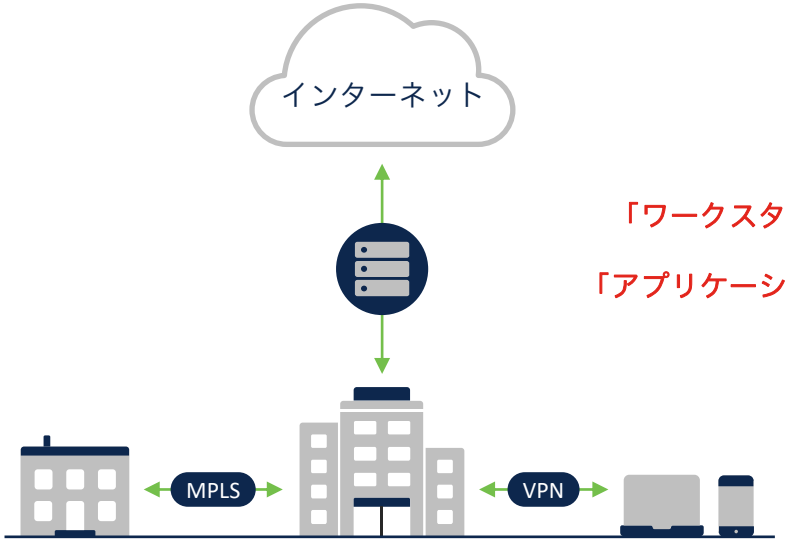
## アジェンダ

- ネットワークと
  セキュリティの変革
- 組織の課題
- 課題に取り組むための
  主なユースケース
  - リモートワーカーの保護
  - エッジ（遠隔地）の保護

# ネットワークとセキュリティの変革

# ネットワークとセキュリティの変革

## 以前

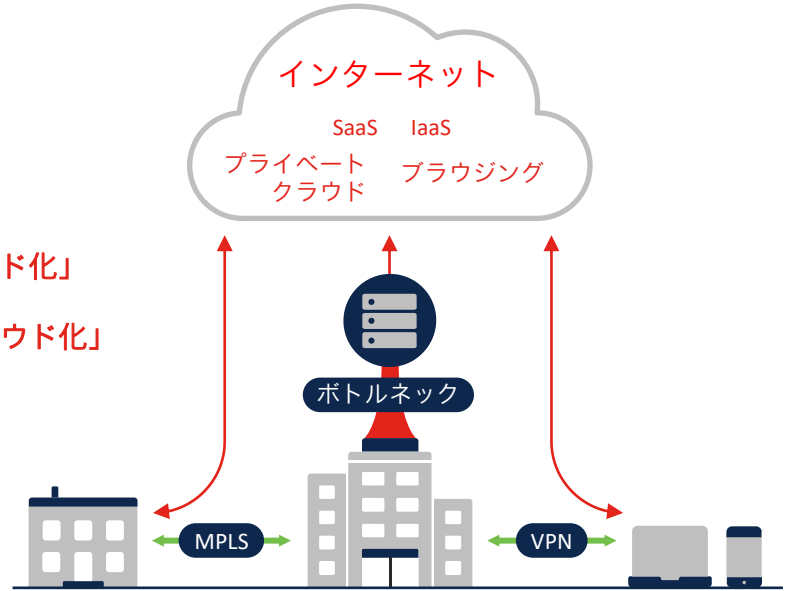



アプリケーション：データセンターでのホスティング
ユーザー：社内ネットワークに接続して業務を行う
ネットワーク：集約されている
セキュリティ：セキュリティスタックがオンプレミスに配置されている

「ワークスタイルのハイブリッド化」

「アプリケーションのマルチクラウド化」

## 変化




アプリケーション：クラウドでのホスティングが増加
ユーザー：ネットワーク外での業務が増加
ネットワーク：分散化が進んでいる
セキュリティ：セキュリティの確保に差がある

# 変革はメリットも課題ももたらす

- 今日のネットワークは分散化されている
- ユーザーとアプリケーションはクラウドを採用済み
- セキュリティとネットワーキングもクラウドに移行中

**80%**
ダイレクト インターネット アクセス（DIA）に移行中の組織の割合

**76%**
SD-WAN を広範囲または限定的に使用している組織の割合

**42%**
セキュリティ導入に 1 か月以上かかっている分散拠点の割合

**68%**
最近受けた攻撃の侵害の原因が分散拠点とローミングユーザーだったと回答した人の割合

# 組織の課題

# ネットワーキングチームとセキュリティチームが抱えている課題

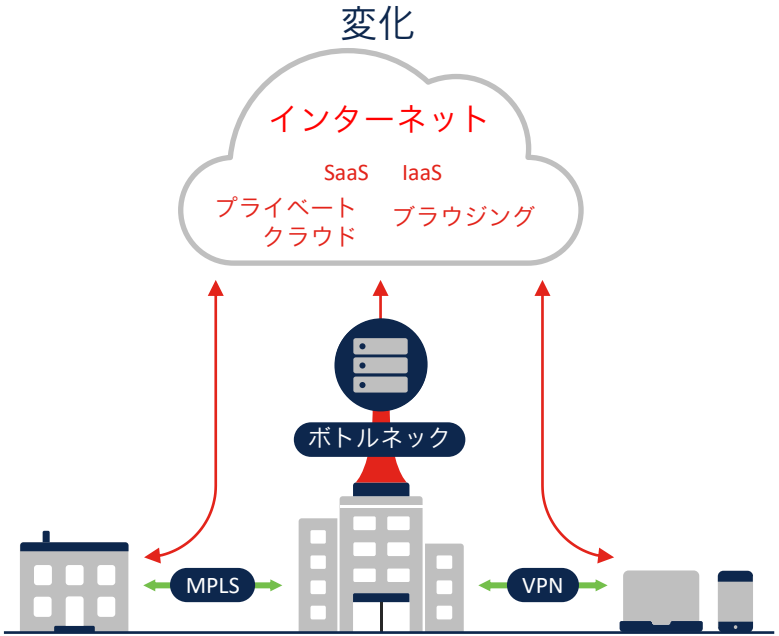
ユーザーを
アプリケーション
とデータに接続

進化する脅威
媒体からの保護

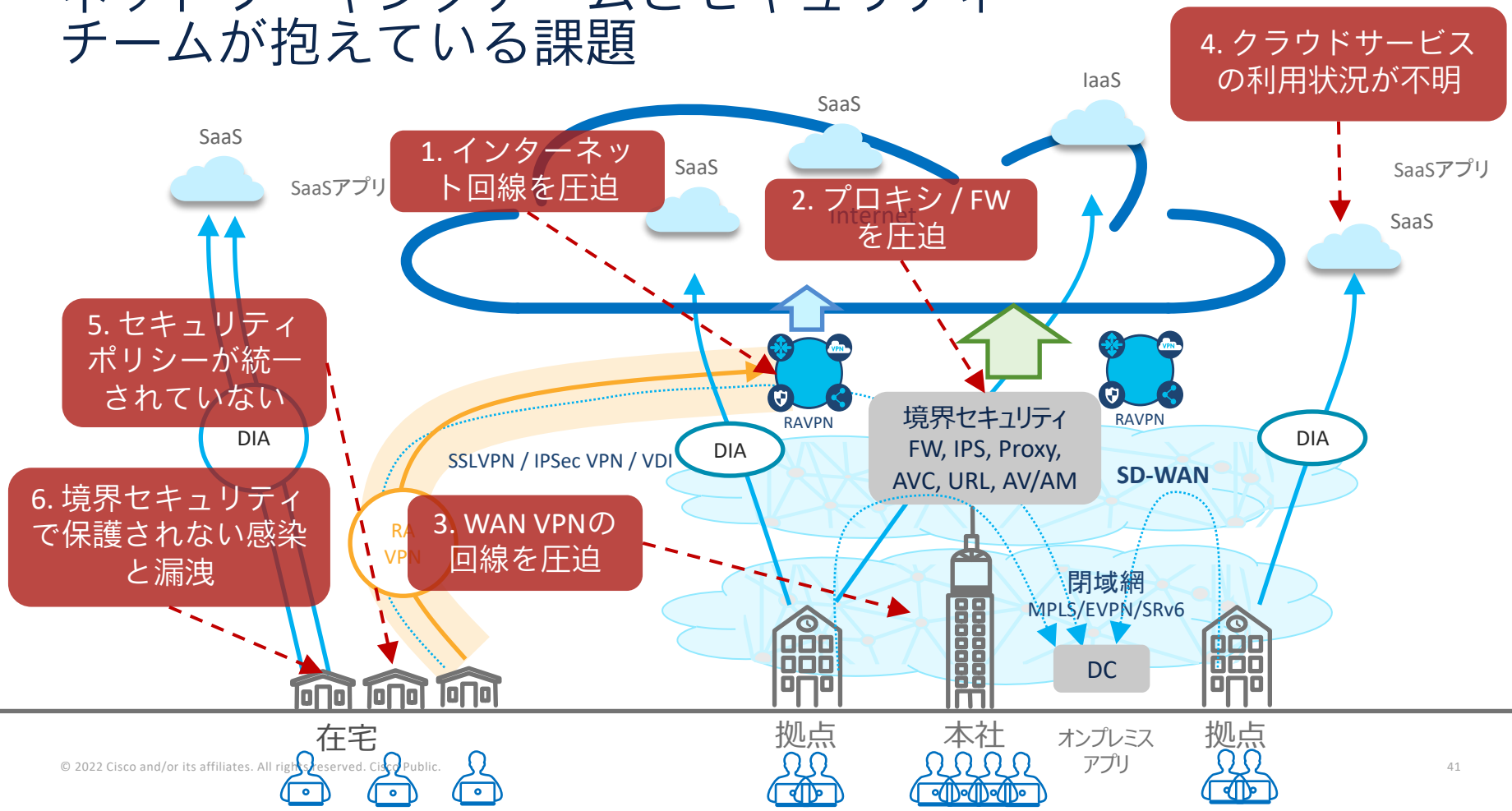
高品質なユーザー
エクスペリエンスの
提供

新たな統合アプローチが必要

# ネットワーキングチームとセキュリティチームが抱えている課題



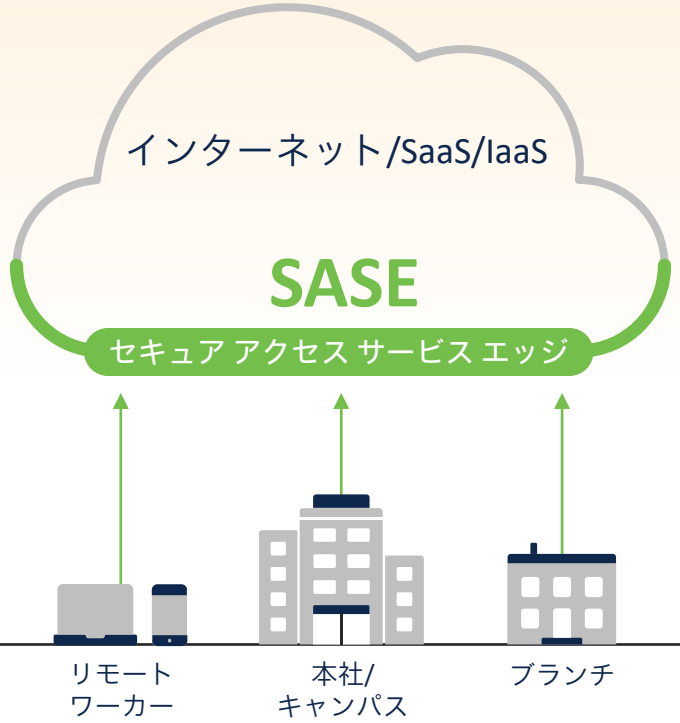
# ネットワーキングチームとセキュリティチームが抱えている課題



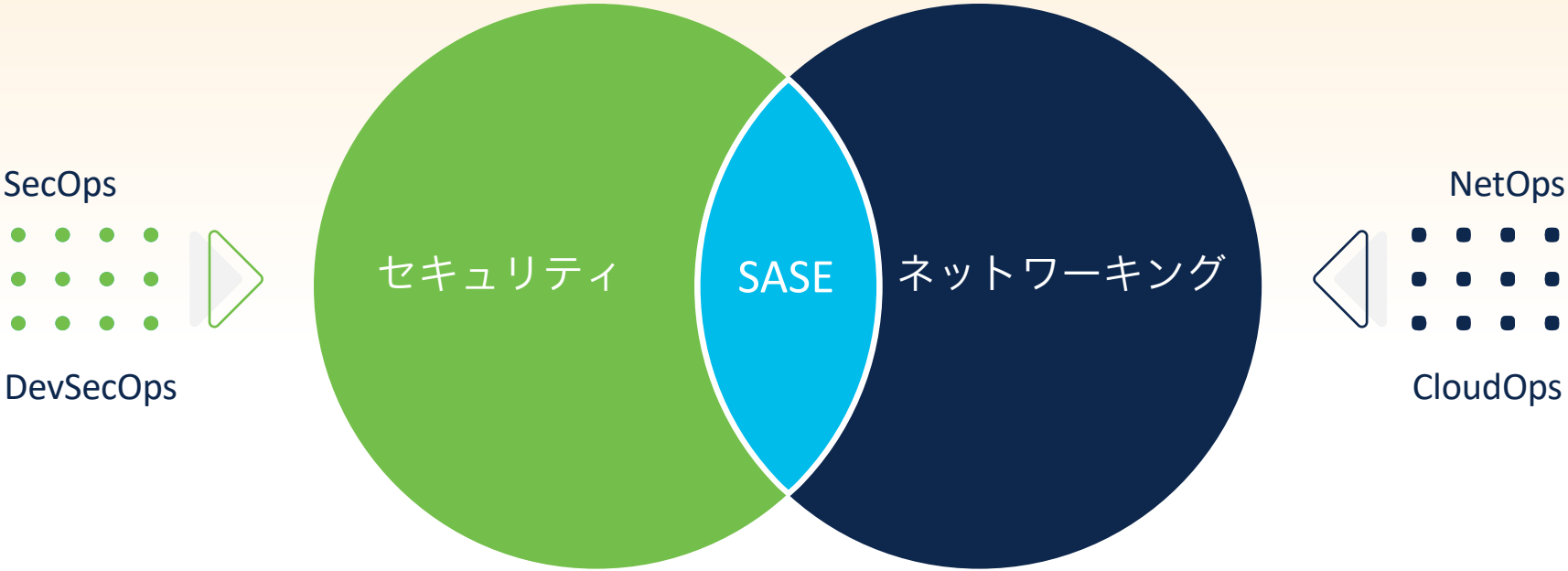
# SASEへのとは？ - 今日の環境はクラウドが中心

## セキュア アクセス サービス エッジ（SASE）アーキテクチャがますます必要に

- **ネットワーキング機能**と**セキュリティ機能**を**クラウドで集約**する
- あらゆる環境の必要なアプリケーションやデータに、ユーザーが**どこからでも接続**できるようにする
- アクセス制御と、適切かつ**継続的なセキュリティ保護**の適用を行う



# SASE：クラウドでのネットワーキングとセキュリティの統合



# SASE に関する 3 つの キーワード - “C”

## Connect（接続）

場所を問わず安全でシームレスな
アプリケーションとの接続を提供

## Control（コントロール）

ゼロトラストのアクセスを確立し、
脅威に対する優れた防御で保護

## Converge（統合）

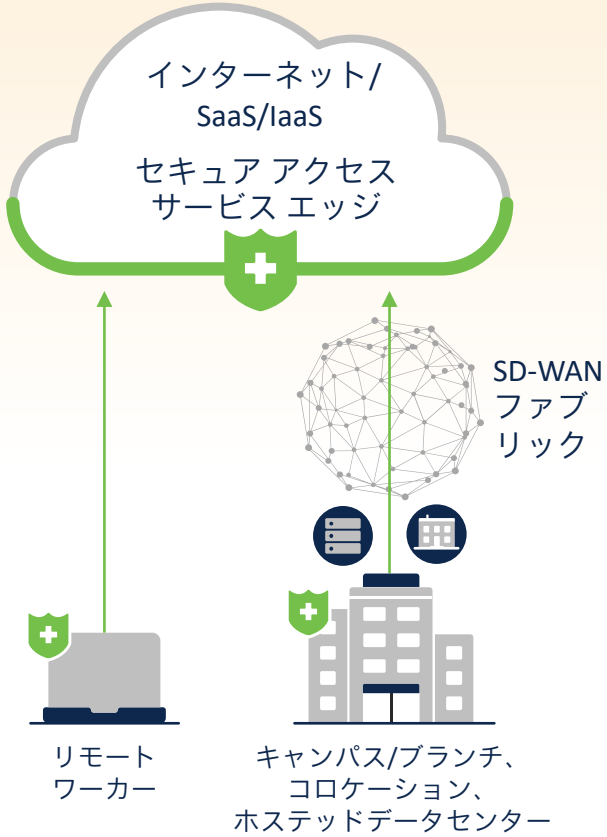
クラウド提供型のネットワーキングと
セキュリティを統合

# 課題に取り組むための主なユースケース

# SASE の主要なユースケース

## リモートワーカーの保護

- あらゆる場所からアプリケーションやデータにシームレスに接続
- インターネットとクラウドアプリケーションに安全にアクセス
- ユーザーを認証し、デバイスの健全性を確認
- すべてのリモートワーカーに最適な接続環境とアプリケーションエクスペリエンスを提供




## セキュアエッジ

- さまざまな場所にあるオフィスからアプリケーションに簡単に接続
- 数千のユーザと拠点すべてに SD-WAN ファブリックをプロビジョニング
- アプリケーションへの安全なアクセスと、ダイレクトインターネット アクセスの安全な利用
- ISP、SaaS、パブリックおよびプライベート アプリケーション全体の問題を特定して解決

# リモートワーカーの保護

## ユースケース

# 課題例：リモートワーカーの保護

1. **ユーザー体感に影響を与えず**リモートワーカーを保護するのは困難、**VPN を利用しないユーザの許容**とセキュリティの確保が課題
2. アクセス許可前に、**ユーザーIDとデバイス正常性**の確認が課題
3. リモートワーカーとアプリ間で生じる体感原因を特定する手段がない
4. 専用アプライアンスは高価であり、導入、管理維持、拡張が困難である場合がある

# 組織のニーズ

人数が変動するリモートワーカーやハイブリッドワーカーに対し、

「一貫したレベルのセキュリティ」
「一貫したレベルのパフォーマンス」

を提供する効果的かつ効率的な方法を求められる。

# ユースケース：リモートワーカーの保護

## シスコの Umbrella、AnyConnect、Duo、ThousandEyes で実現できる機能

### Connect（接続）

- Web と SaaS アプリケーションに直接向かうインターネットトラフィックを保護
- VPN を利用せずに頻繁に利用される個人のアプリにアクセス
- すべての社内アプリケーションに安全にアクセス

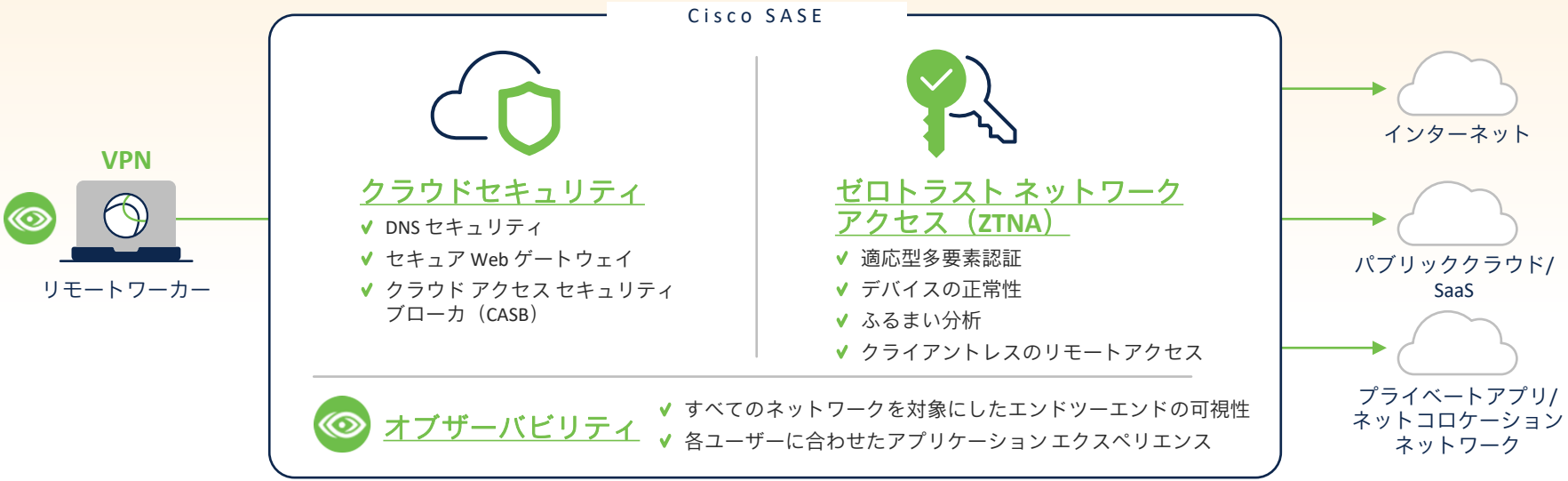
### Control（コントロール）

- セキュリティポリシーとアクセスポリシーを一貫して適用
- ユーザーのアイデンティティとデバイスの状態を確認

### Converge（統合）

- すべてのユーザー、アプリケーション、ネットワークから実用的な洞察を入手して可視性を実現
- 複数のデバイスと場所にまたがるリモート ユーザー エクスペリエンスをシンプル化
- 単一のエージェント（現在 1 億 5,000 万台のデバイスに導入）で複数のサービスを提供

# ユースケース：リモートワーカーの保護
## 機能



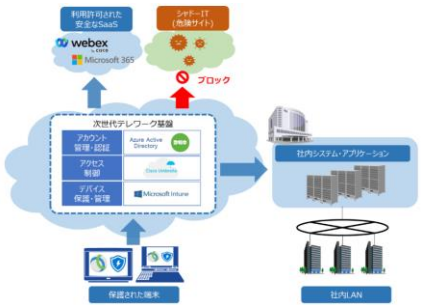
# お客様のケーススタディ：ドコモ・システムズ

https://www.docomo-sys.co.jp/news/pdf/PressRelease20210826.pdf

ドコモ・システムズ株式会社

## 課題

- 既存 リモートアクセスシステムからの認証強化、ゼロトラスト化を行いたい
- 既存の VDI システムからのリモートアクセスからの多様化を行いたい
- テレワーク端末の開放とインターネットアクセスの脅威の発見と阻止、シャドー IT のリスク軽減、ポリシー適用の簡素化が課題である




## ソリューション

- **SASE**
- **Cisco Umbrella**
- **Cisco Secure Access by Duo**
  - 他要素認証
  - デバイストラスト
  - VPNレスアクセス
- **Cisco Secure Firewall ASA**
- **Cisco Any Connect VPN**

## 成果

- すべてのユーザー、デバイス、拠点のインターネット アクティビティを包括的に可視化
- アプリケーションをきめ細かく制御し、リスクの高いアクティビティを防止
- Web トラフィックの検査・制御、ポリシーコンプライアンスの確保、隠れた脅威の阻止が可能に
- シスコの統合セキュリティアーキテクチャにより、調査と脅威対応を効率化
- セキュアなダイレクト インターネット アクセス（DIA）を介してクラウドアプリケーションとワークロードへのアクセスを高速化

# セキュアエッジ
## ユースケース

# 課題例：セキュアエッジ

1. ユーザー、デバイス、アプリ、データの攻撃対象がますます拡大し、領域全体でのネットワークとセキュリティの管理が課題
2. 構成の複雑さが、一貫性のないパフォーマンスとユーザー体感に影響している
3. パフォーマンスの問題特定が困難
4. 遠隔拠点とアクセス方法に適用されるポリシーに一貫性がなく、ギャップが生じている
5. ダイレクト インターネット アクセス（DIA）と SaaS の使用の増加により、セキュリティに新たなギャップが生じ、リスクが増大する

# 組織のニーズ

統合されたネットワーキングとセキュリティを導入することで

「リスクを軽減」し、
「同時にパフォーマンスを向上」させて、
「環境を簡素化したい」と、

考えています

# ユースケース：セキュアエッジ

## シスコの SD-WAN、Umbrella、Duo、ThousandEyes で実現できる機能

### Connect（接続）

- ゼロタッチプロビジョニング、インテリジェントなパス選択、自動 Cloud onRamp により、**ユーザーをマルチクラウド環境のアプリケーションに接続**する、クラウド提供型 WAN アーキテクチャ

### Control（コントロール）

- 安全で信頼性が高く、高速なインターネット接続を実現する**クラウド提供型セキュリティ**
- オンプレミス、クラウドベースを問わず、すべてのアプリケーションへの**ゼロトラストアクセス**

### Converge（統合）

- すべてのユーザー、アプリケーション、ネットワークから実用的なインサイトを取得して**オブザーバビリティを実現**
- ネットワーキングとセキュリティの統合による迅速な導入**とシンプルな利用**

# ユースケース：エッジの保護

## 機能

# 代表的なユースケースの両方を保護

## リモートワーカーの保護

- あらゆる場所からアプリやデータにシームレスに接続
- インターネットとクラウドアプリに安全なアクセス
- 認証を強化しデバイスの健全性を確認：ゼロトラスト
- すべてのリモートワーカーに最適な接続環境とアプリ体感を提供

## セキュアエッジ

- さまざまな場所にあるオフィスからアプリに簡単接続
- 数千のユーザと全拠点に SD-WAN ファブリックをプロビジョニング
- アプリおよびダイレクト インターネット アクセスの安全化
- ISP、SaaS、Public/Private クラウド アプリ全体の問題を特定し解決

# シスコの SASE アーキテクチャで実現できること：
## クラウドでのネットワーキングとセキュリティの統合

### セキュアなアクセスが可能な接続環境

すべてのビジネス拠点、リモートワーカー、デバイス、ワークロードが接続できる環境

### 優れたアプリケーションエクスペリエンスの創出

ユーザからあらゆるネットワークやクラウドのアプリケーションまで、エンドツーエンドでオブザーバビリティを確保して異常を修復

### パフォーマンスの最適化

きわめて高速で信頼性の高いセキュアなパスを確立

### ゼロトラスト ネットワークアクセスの導入

セッションごとにデバイスのユーザ ID と健全性を確認

### ビジネスの俊敏性向上

クラウドを活用して複雑さを排除し、グローバルな拡張性を迅速に提供

SASE Academy セッション 3「ゼロトラスト：本人確認を行い、ハイブリッドワークプレイスのセキュリティを強化」では、SASE のユースケースについてさらに深く掘り下げます。

The bridge to possible

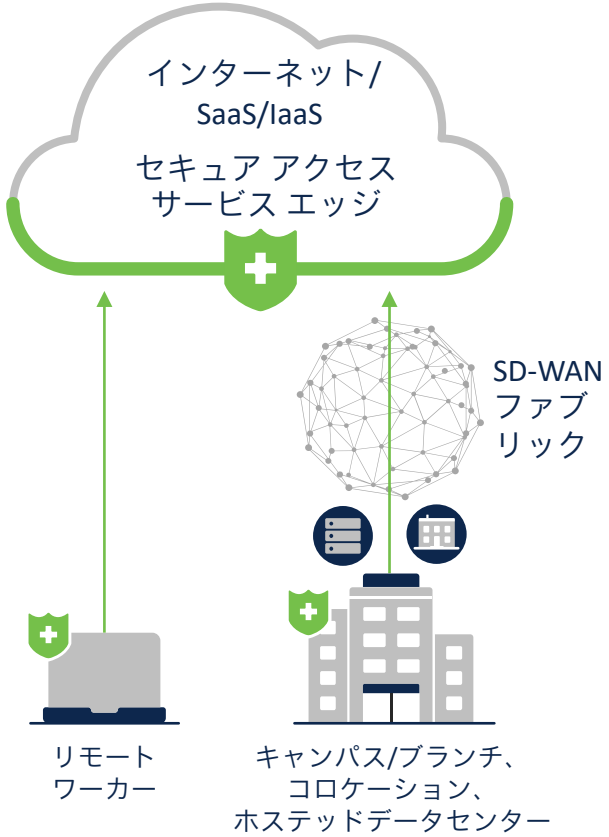
# SASE Academy
# ゼロトラスト：ハイブリッドワークプレイスのセキュリティを強化

システムズ合同会社 セキュリティ事業
テクニカルソリューションズアーキテクト
浅井達也

# SASE の主要なユースケース

## リモートワーカーの保護

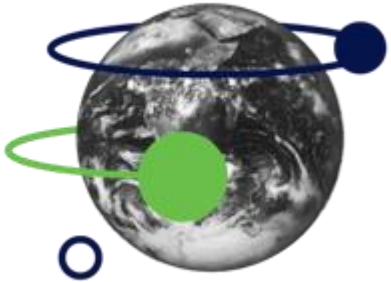
- あらゆる場所からアプリケーションやデータにシームレスに接続
- インターネットとクラウドアプリケーションに安全にアクセス
- ユーザーを認証し、デバイスの健全性を確認
- すべてのリモートワーカーに最適な接続環境とアプリケーション エクスペリエンスを提供




## セキュアエッジ

- さまざまな場所にあるオフィスからアプリケーションに簡単に接続
- 数千のユーザと拠点すべてに SD-WAN ファブリックをプロビジョニング
- アプリケーションへの安全なアクセスと、ダイレクト インターネット アクセスの安全な利用
- ISP、SaaS、パブリックおよびプライベート アプリケーション全体の問題を特定して解決

# シスコ独自の方法でお客様を支援



ネットワーキング

最大の SD-WAN
ソリューションプロバイダー

セキュリティ

フォーチュン 100 社すべてで
セキュリティを保護

ゼロトラスト

2 年連続の
「ゼロトラスト」リーダー

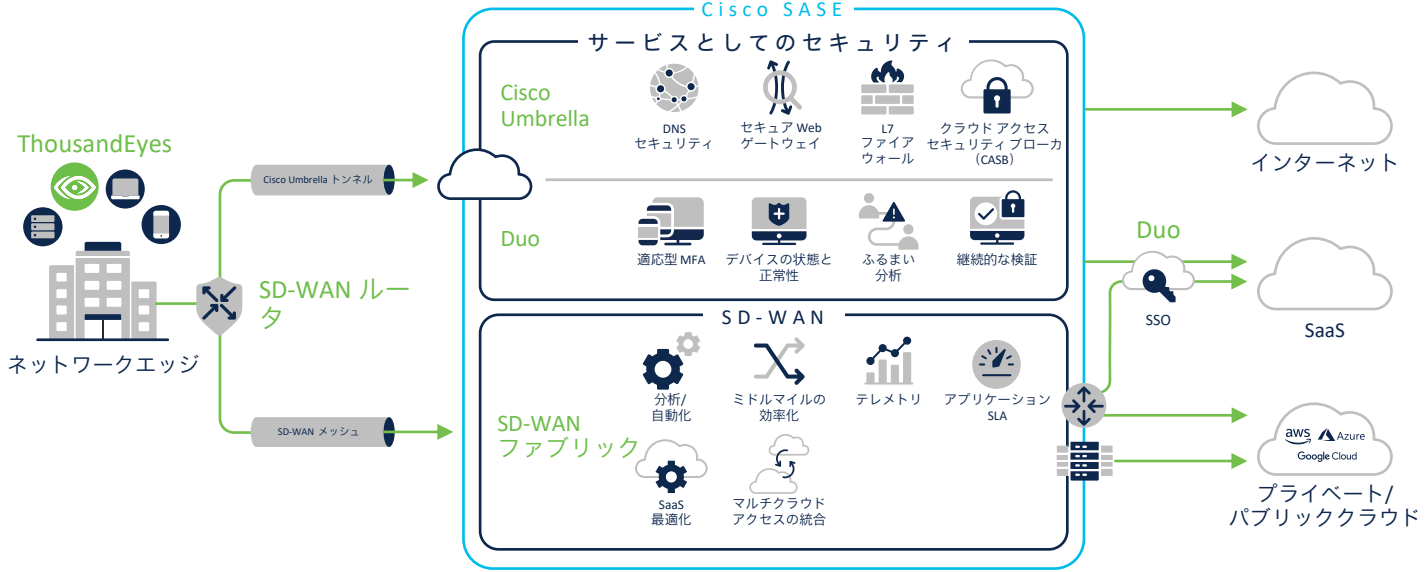
# シスコの SASE アーキテクチャのコンポーネント


オブザーバビリティ：ThousandEyes

# ユースケース：エッジの保護

**中核的機能**

- クラウドセキュリティ
- ゼロトラスト セキュア アクセス
- SD-WAN ルータ
- テレワーカーゲートウェイ
- 既存のゲートウェイ
- オブザーバビリティ




## Connect（接続）

- 任意のネットワークエッジ（オフィス全体、単一オフィス、本社）から提供されるソフトウェアデファインド トランスポート
- SASE への暗号化されたトランスポートが実現するダイレクト インターネット アクセス
- SD-WAN ファブリックを介した動的パスの選択
- SD-WAN と O365 間のテレメトリ交換によるアプリ認識型インテリジェントパスの選択

## Control（コントロール）

- インターネットおよび SaaS へのあらゆるアウトバウンドトラフィックを保護するクラウド セキュリティ スタック
- ユーザーおよびデバイス向けのゼロトラストを前提としたアプリケーションアクセスの確立

## Converge（統合）

- ネットワークとセキュリティのシンプルかつ迅速な導入
- ゼロタッチプロビジョニング
- クラウドを介して提供される共通のセキュリティポリシー
- SecureX によるネットワーク全域での応答の自動化
- ThousandEyes によるすべてのネットワークとサービスに対する共通のオブザーバビリティ

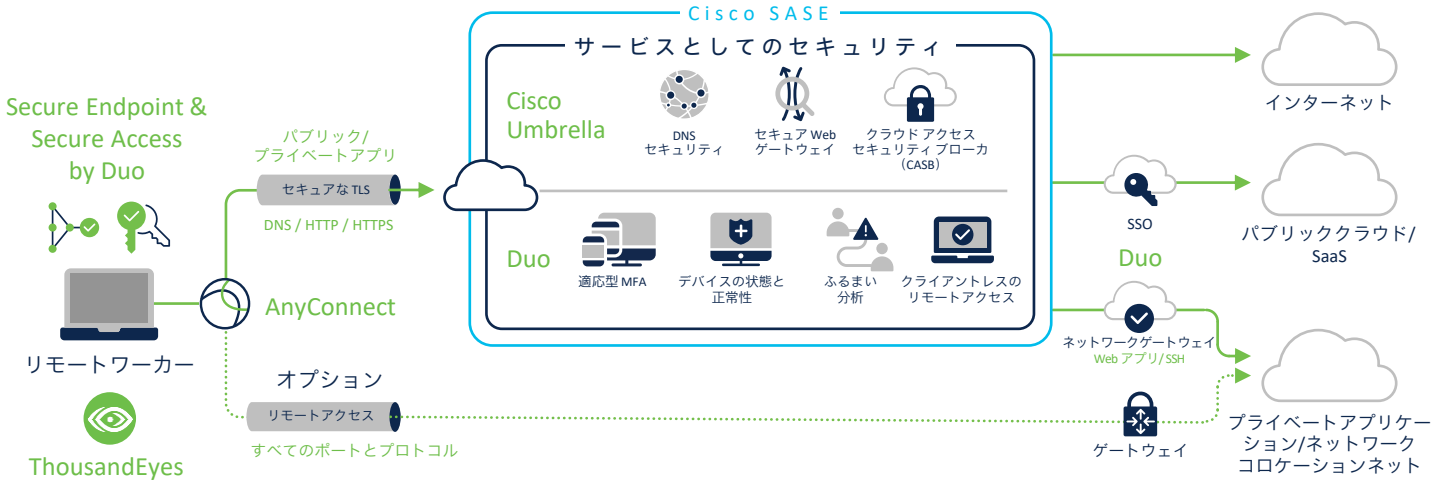
# ユースケース：リモートワーカーの保護

**中核的機能**

- クラウドセキュリティ
- ゼロトラスト セキュア アクセス
- リモートアクセス + ZTNA
- オブザーバビリティ

**強化機能**

- MDM
- エンドポイント セキュリティ




## Connect（接続）

- 内部アプリへのセキュアな RA-VPN スプリットトンネリング
- DNS および Web トラフィックのクラウドセキュリティへのリダイレクト
- ゼロトラスト ネットワーク アクセス（ZTNA）のための Duo Network Gateway を使用した VPN レスの Web/SSH アプリケーションアクセス

## Control（コントロール）

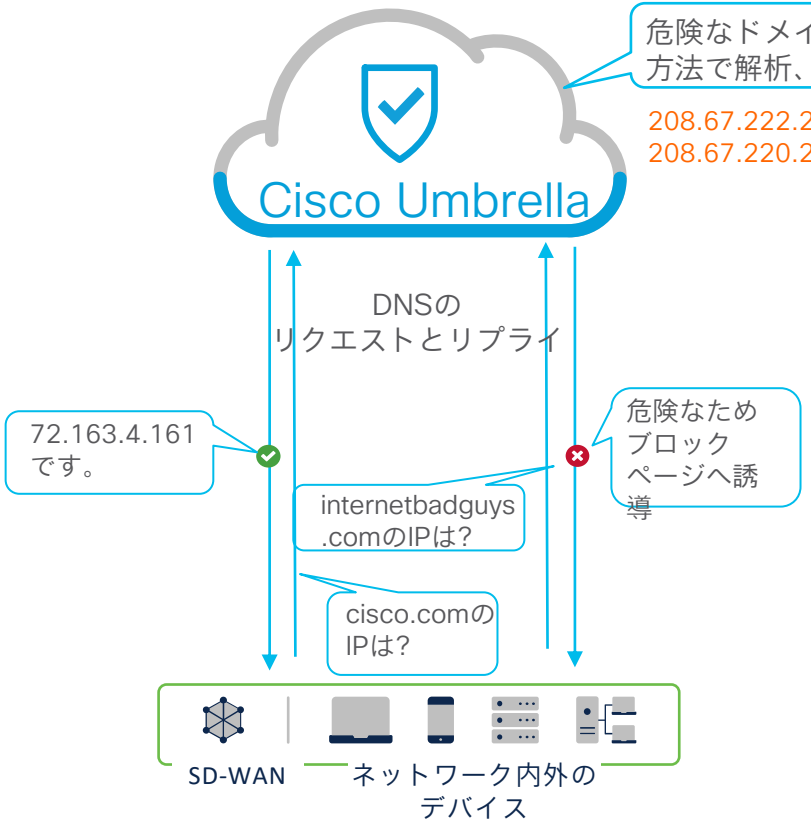
- ユーザー/デバイスからアプリへのゼロトラスト セキュア アクセス
- WWW/SaaS アプリへのセキュアなアウトバウンド ユーザー トラフィック
- エンドポイントの保護（マルウェア対策）

## Converge（統合）

- 接続とセキュリティを両立するシンプルな統合環境
- クラウドを介して提供される共通のセキュリティポリシーと可視性
- 共通の SecureX プラットフォームによる可視性、オーケストレーション、拡張検出および応答（XDR）
- ThousandEyes によるすべてのネットワークとサービスに対する共通のオブザーバビリティ

# Umbrella/クラウド セキュリティ

# Cisco UmbrellaはDNSの仕組みを利用

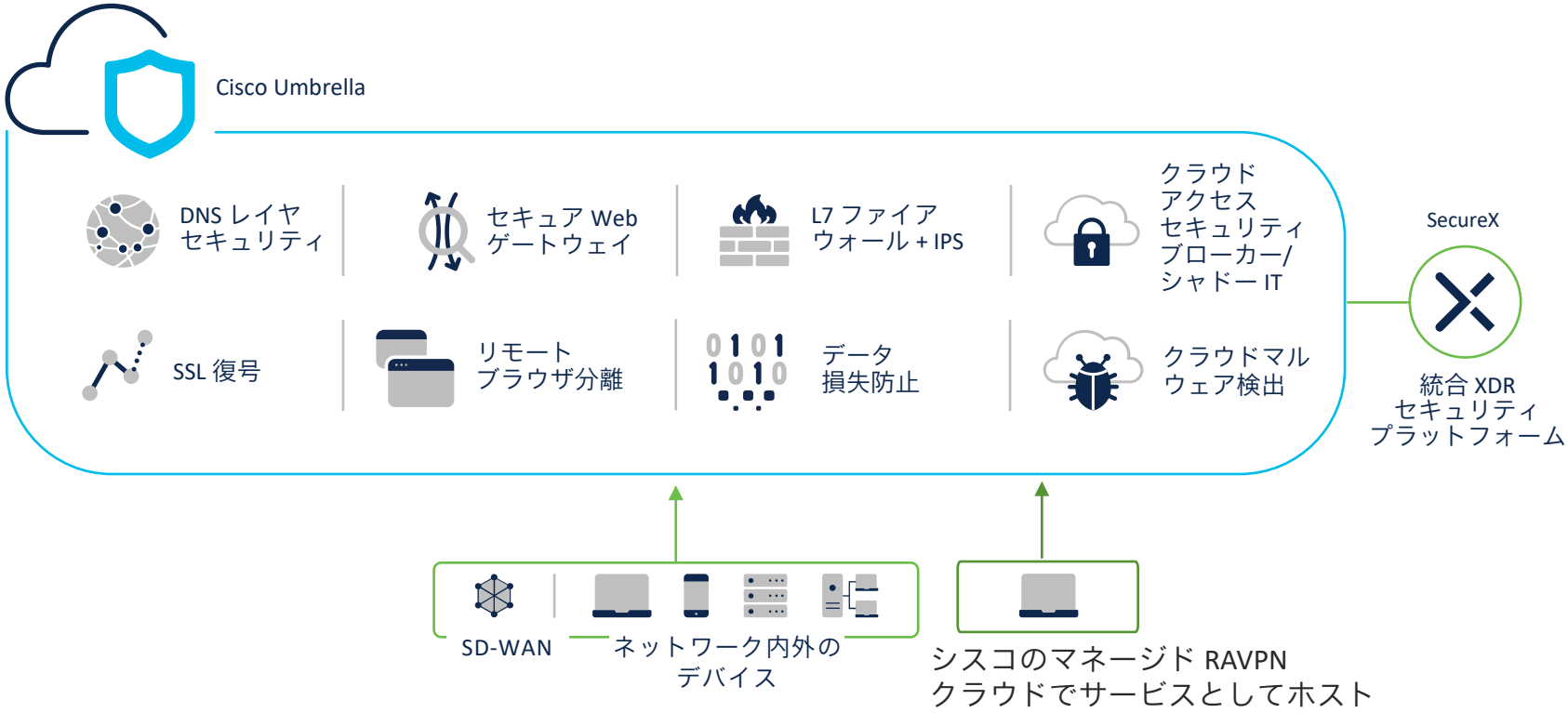



- Cisco Umbrella は DNSサーバ:
- 問い合わせられたドメインが危険ならブロック
- 安全なドメインなら、正規のIPを応答

- 導入が容易
  - DNS問い合わせ先がCisco Umbrella に
    なるように設定するだけで導入可能

- 幅広い防御
  - DNSを使うデバイスは全て防御対象(IoTも)
  - ポートやプロトコルに関わらず防御の対象

# Cisco Umbrella の機能



# Cisco Talos 脅威インテリジェンスで全体的なセキュリティの有効性が向上

シスコがより多くの脅威を分析することで、お客様はさらに多くの脅威をブロックし、迅速に対応できるようになります。

- Cisco Talos は世界最大クラスの脅威インテリジェンス組織
- 400 人を超える専属の脅威研究者とデータサイエンティスト

AV-TEST
The Independent IT-Security Institute
Magdeburg Germany

Cisco Umbrella を 1 位に選出、競合他社よりも一貫して優れたパフォーマンスを発揮していると評価

| セキュア Web ゲートウェイテスト | Cisco Umbrella | Zscaler | Palo Alto | Netskope | Akamai |
|---|---|---|---|---|---|
| **総合的な検出率** | **96.39** | **89.67** | **73.15** | **61.90** | **58.43** |

検出率（高いほど良い）

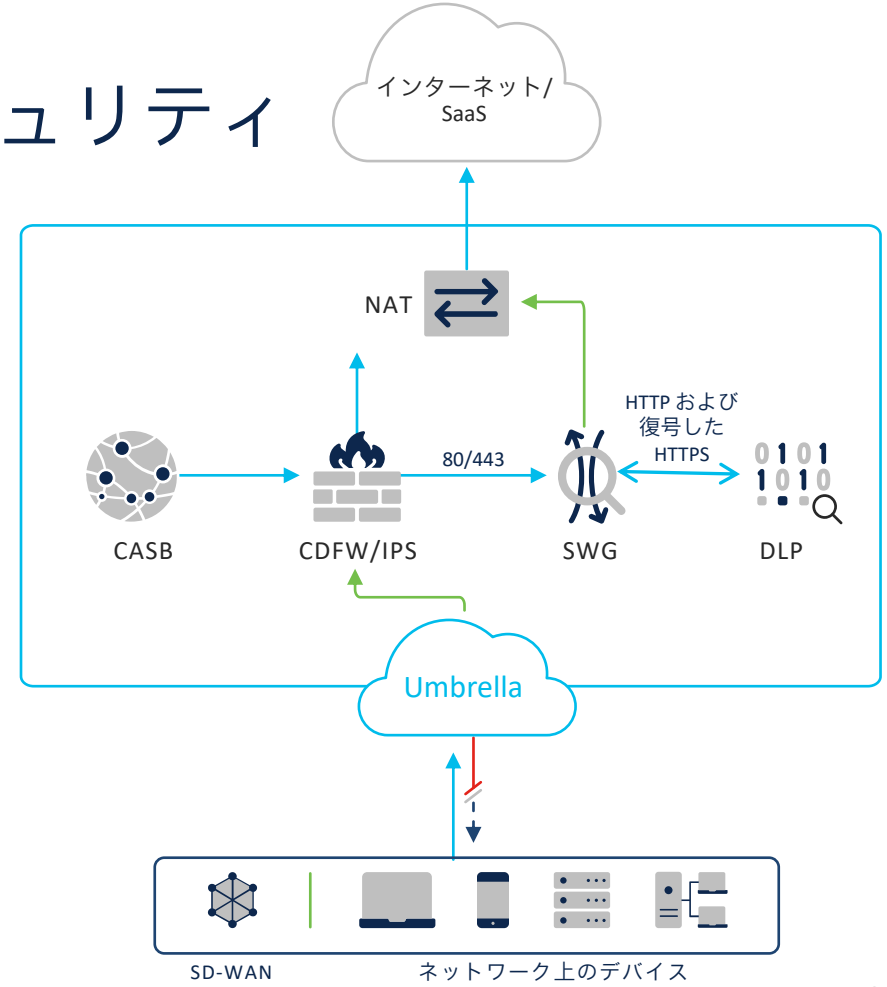
# フル機能のクラウドセキュリティ

## クラウド提供型ファイアウォール（CDFW）
**侵入防御機能**を備えたレイヤー 7 ファイアウォール

## セキュア Web ゲートウェイ（SWG）
**リモートブラウザ分離**と SaaS テナント制御機能を備えた Web セキュリティ制御

## データ損失防止（DLP）
アウトバウンド Web トラフィック内の**機密データの監視やブロック**

## クライアント アクセス セキュリティ ブローカー（CASB）
シャドー IT アプリケーション制御と**クラウド マルウェア防御**



# インライン型 DLP (Inline DLP)
## クラウド ネイティブ プロキシ DLP

接続性、ルーティング、SSL 復号化に SWG を活用

堅牢な DLP 分類

- 80 以上の内蔵データ分類
- カスタムキーワード

柔軟な DLP ポリシー

- 定義されたデータ分類を利用し、特定のアイデンティティと宛先に対して適用

レポーティング

- ID、ファイル名、宛先、分類、パターンマッチ、抜粋、トリガールールなどわかりやすく表示
- Umbrella に統合されたユーザ インタフェース


Cisco Japan Youtube公式チャンネル
DLP機能も統合のSWG | Cisco Umbrella
https://youtu.be/dCaBSHGLEgI

# シャドー IT 可視化と制御
# App Discovery 機能

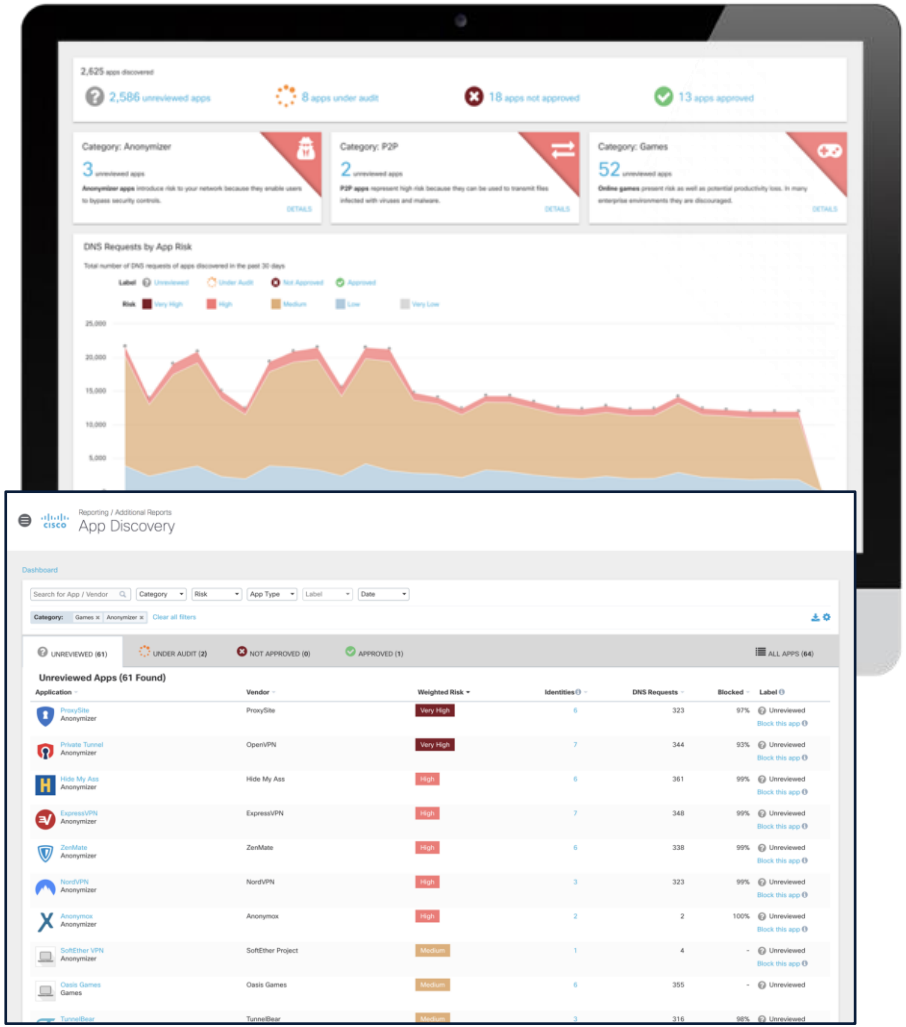
- 使用中のクラウドアプリケーションの全リスト
- アプリのリスクスコアやベンダー、アプリケーション、証明書、リスク要因に関する詳細情報を表示
- ユーザー数と送受信のトラフィック量(SWGも併用の場合)
- これをApp Discoveryからブロック対象にすることが可能

＜参考＞

Cisco サポート　コミュニティ

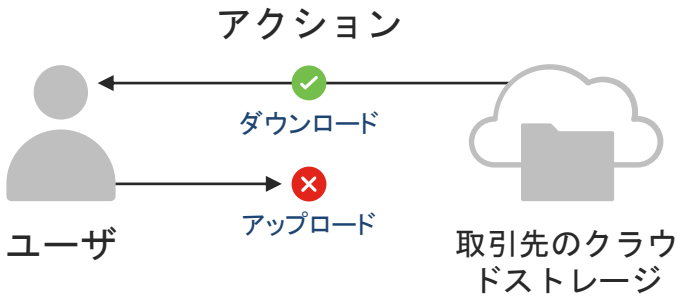
- Umbrella: App Discovery と Application Settings

https://community.cisco.com/t5/-/-/ta-p/3725234



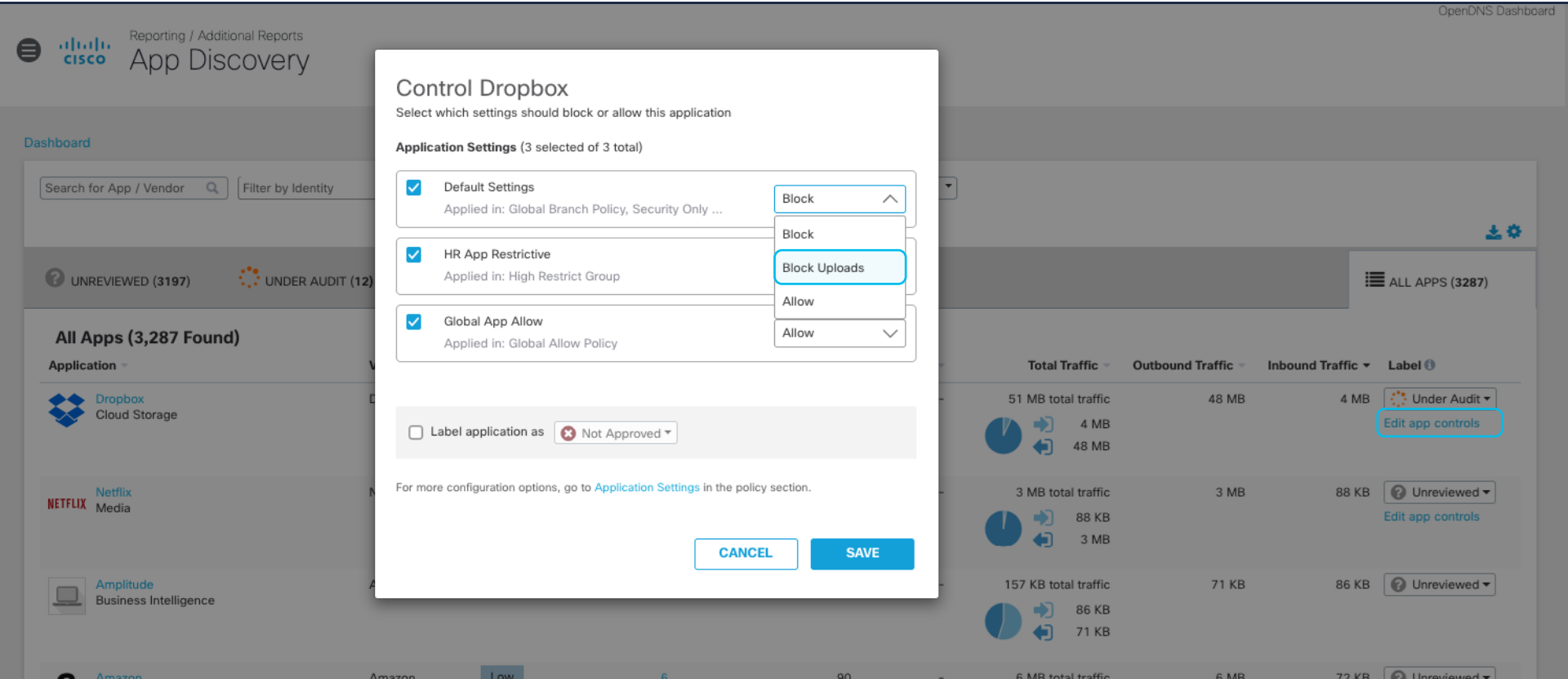
# 人気の高い SaaS アプリケーションをきめ細かく制御

- 投稿/シェア をブロック（ソーシャル メディア）
- 添付をブロック (ウェブ メール)
- アップロードをブロック (クラウドストレージ、コラボレーション、オフィス生産性、コンテンツ管理、メディアアプリ)




box twitter Dropbox Messenger Gmail facebook LinkedIn
Google Drive SlideShare YouTube vimeo WhatsApp smartsheet PASTEBIN

# 高度なアプリ制御


OpenDNS Dashboard
Reporting / Additional Reports
App Discovery
Dashboard
Search for App / Vendor
Filter by Identity
UNREVIEWED (3197)
UNDER AUDIT (12)
ALL APPS (3287)
All Apps (3,287 Found)
Application
Total Traffic
Outbound Traffic
Inbound Traffic
Label
Dropbox
Cloud Storage
51 MB total traffic
48 MB
4 MB
Under Audit
Edit app controls
Netflix
Media
3 MB total traffic
3 MB
88 KB
Unreviewed
Edit app controls
Amplitude
Business Intelligence
157 KB total traffic
71 KB
86 KB
Unreviewed
Control Dropbox
Select which settings should block or allow this application
Application Settings (3 selected of 3 total)
Default Settings
Applied in: Global Branch Policy, Security Only ...
Block
HR App Restrictive
Applied in: High Restrict Group
Block
Block Uploads
Allow
Global App Allow
Applied in: Global Allow Policy
Allow
Label application as
Not Approved
For more configuration options, go to Application Settings in the policy section.
CANCEL
SAVE

# クラウドネイティブで、超高速なパフォーマンスを実現

## Umbrella のクラウドセキュリティ

- ISP、CDN、SaaS プラットフォームとの 1,000 以上の ピアリングパートナーシップ：最速最短のルート
- 主要アプリケーションのパフォーマンスを最大 50% 向上、遅延を 73% 短縮
- シームレスなフェールオーバーとダウンタイム不要のメンテナンスを実現するシンプルなトンネル（単一の IP BGP エニーキャスト）などのイノベーション
- コンテナ化されたクラウドネイティブ アーキテクチャにより、拡張性と信頼性が向上

# Cisco Umbrellaを利用するとパフォーマンスが上がる

- セキュリティ機能が追加されるとパフォーマンスが下がる？

テストの結果、インターネット経由でセキュリティ機能を追加せずに直接SaaSアプリケーションを利用する場合よりも、セキュリティ機能を併用したCisco Umbrellaを経由して利用した場合の方がパフォーマンスが改善した

Sample metrics / all locations worldwide aggregated:

- インターネットで直接接続するよりもBoxへのトラフィックが33%高速化
- インターネットで直接接続するよりもAWSコンソールへのトラフィックが22%高速化
- インターネットで直接接続するよりもSalesforceへのトラフィックが21%高速化

Cisco Umbrellaは一貫性があり、均一で、ユーザエクスペリエンスを予測しやすいものにします
https://learn-umbrella.cisco.com/analyst-reports/catchpoint-evaluates-cisco-umbrella-performance

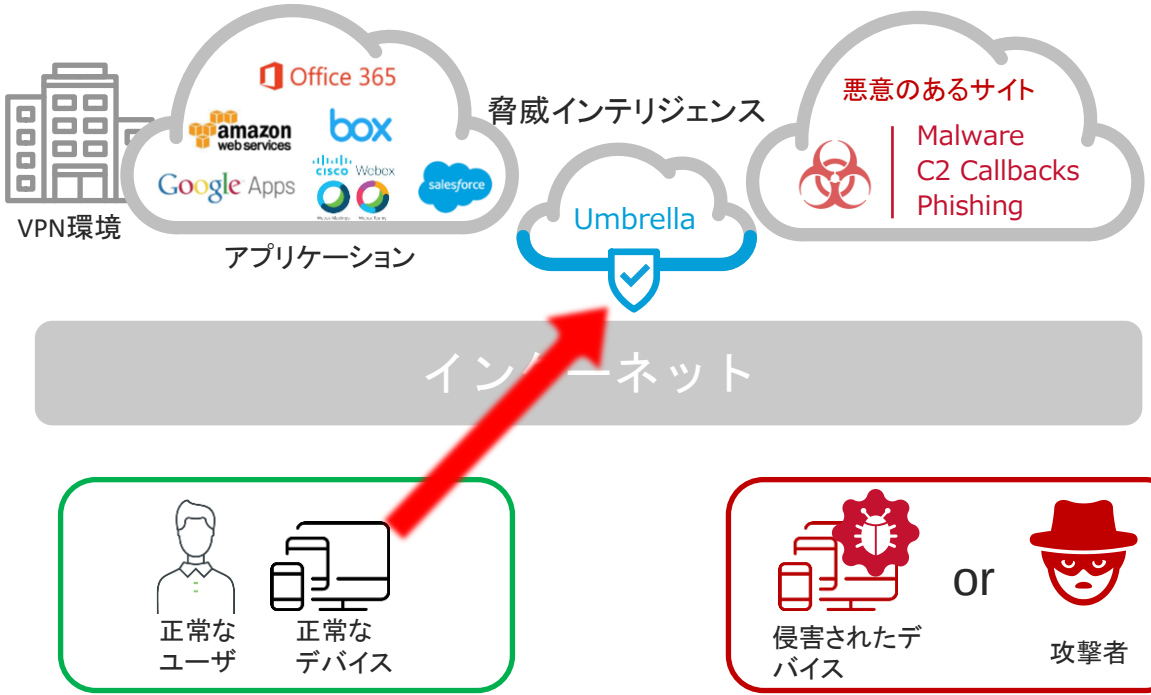
# ハイブリッドワークプレイスのアプリケーション

ユーザは分散
在宅勤務・オフィス・外出先

異なる接続方法

アプリケーションは様々な場所に存在する
-オンプレミス, SaaS

# Umbrella 脅威インテリジェンスを活用した一貫したセキュリティポリシーによる防御




## Cisco Umbrella

- 脅威インテリジェンス/インターネットレピュテーションを利用したセキュアなDNS/SWGサービス
- ユーザとデバイスが、悪意のあるサイト（Malware/C2/Phishing）へ誘導されのを防ぐ
- ユーザ/デバイスの場所によらず防御（Webプロキシ/DNS）を提供

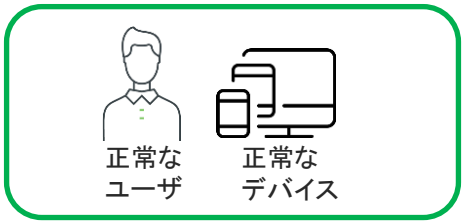
アクセス主体の場所にかかわらない

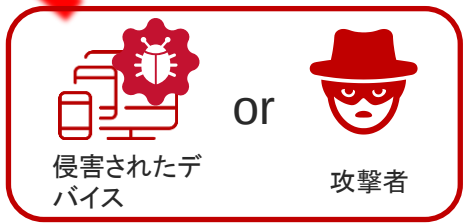
# Cisco Secure Access by Duoによるユーザとデバイスの信頼に基づいた防御

リソースの場所にかかわらず


Cisco Secure Access by Duo

- フィッシングやクラッキング対策
- VPN/SaaS/オンプレアプリへの侵入防御
- ユーザの真正性とデバイスの健全性の同時に検証
- リソースへのアクセスごとの検証を可能に




ハッキングによる侵害の81%は、パスワード漏洩や弱いパスワードなど、クレデンシャルに関連している

*Verizon Data Breach Investigations Report

アクセス主体の場所にかかわらない





* https://gblogs.cisco.com/jp/2020/06/unpacking-2020s-verizon-dbir-human-error-and-greed-collide/

# どんなアプリケーションもセキュアに

独自アプリケーション(APIs)

Microsoft 環境

Cloud サービス

Unix デバイス (SSH セッション)

内部アプリケーション(VPN)

クラウドアプリケーション

Webアプリ

SAML 2.0アプリケーション

Integration documents are available at duo.com/docs

# Cisco Secure Access by Duo

ユーザの信頼性

WITH 多要素認証(MFA)

デバイスの可視性 & 信頼検証

WITH エンドポイントのヘルス・管理ステータス

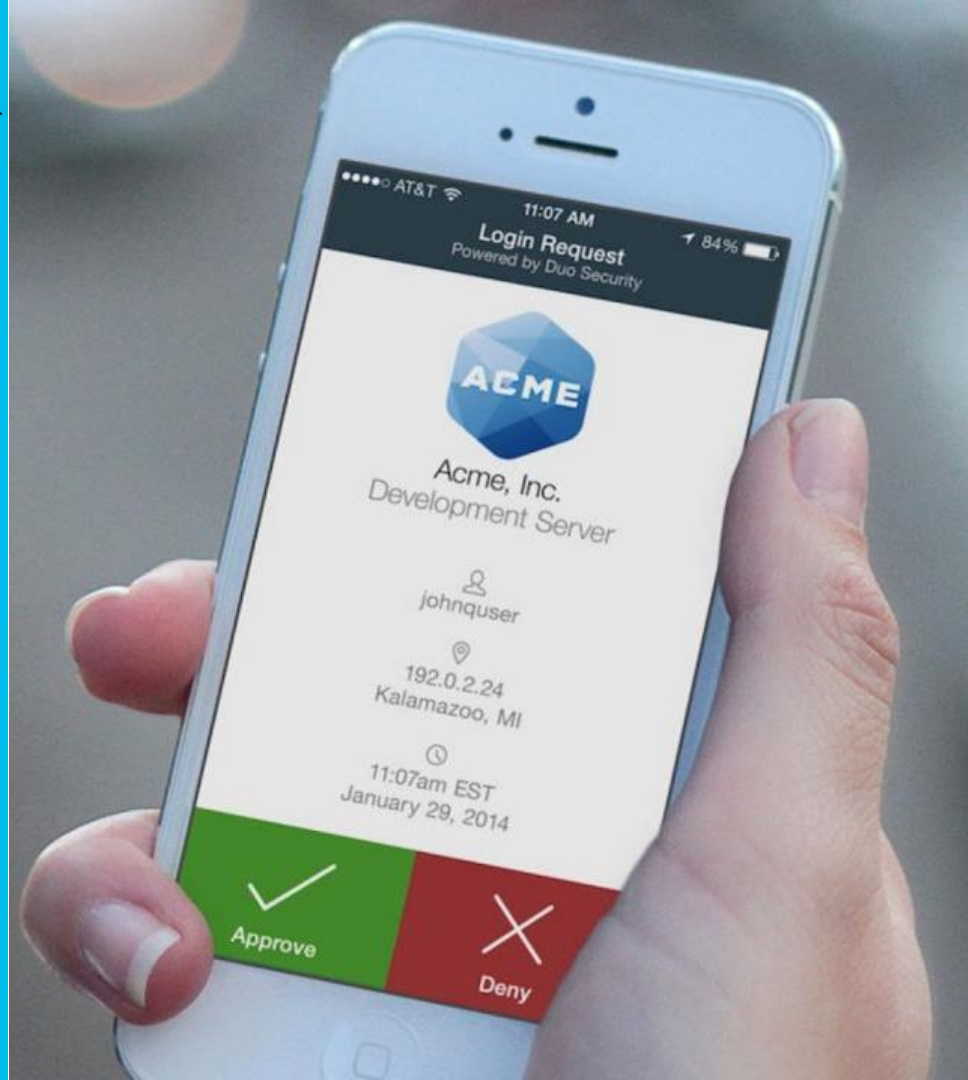
すべてのアプリケーションに
アクセスポリシーを強制

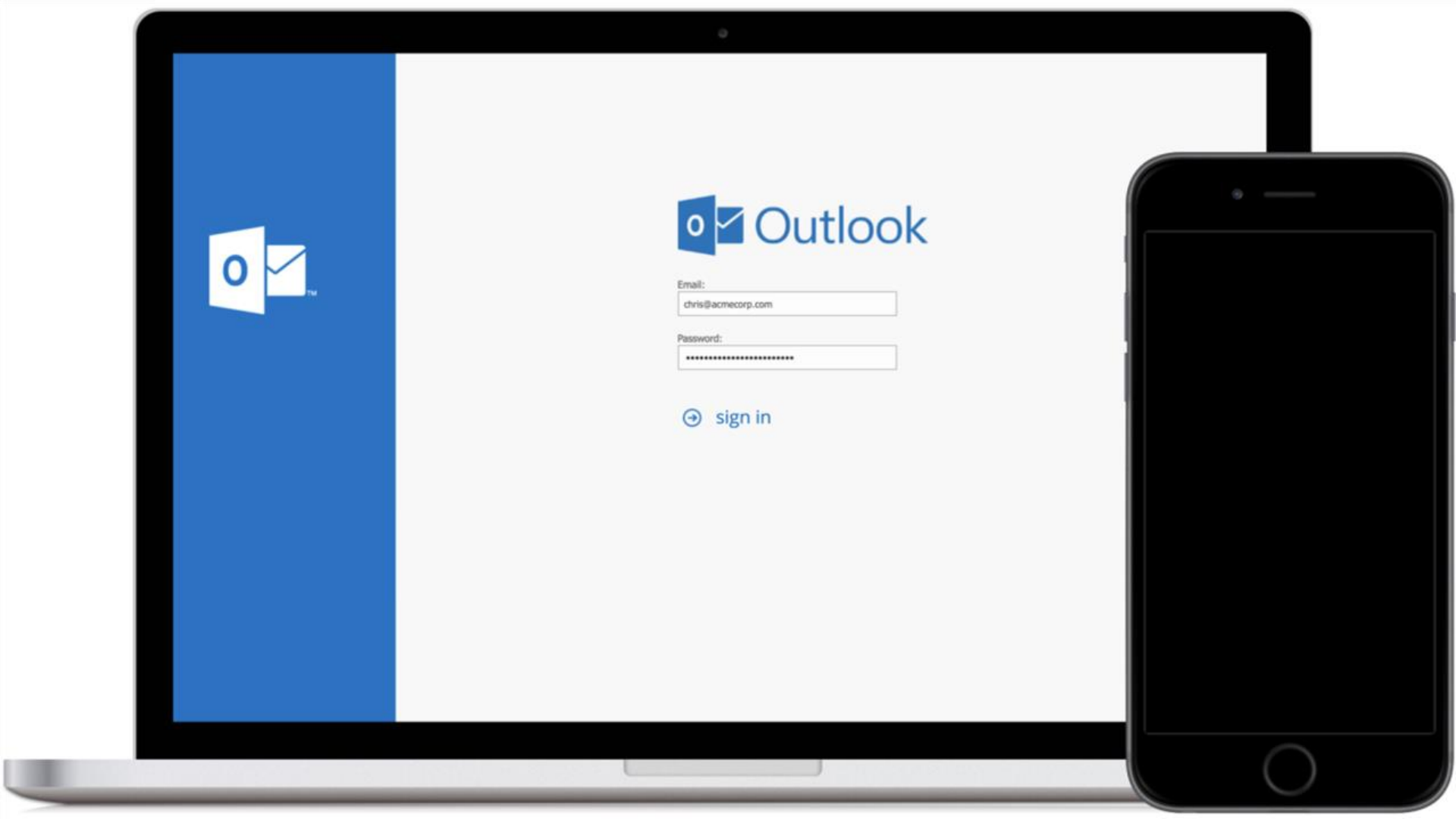
WITH 種類横断的にアクセスコントロール適用:
Windows, Mac, iOS, Android

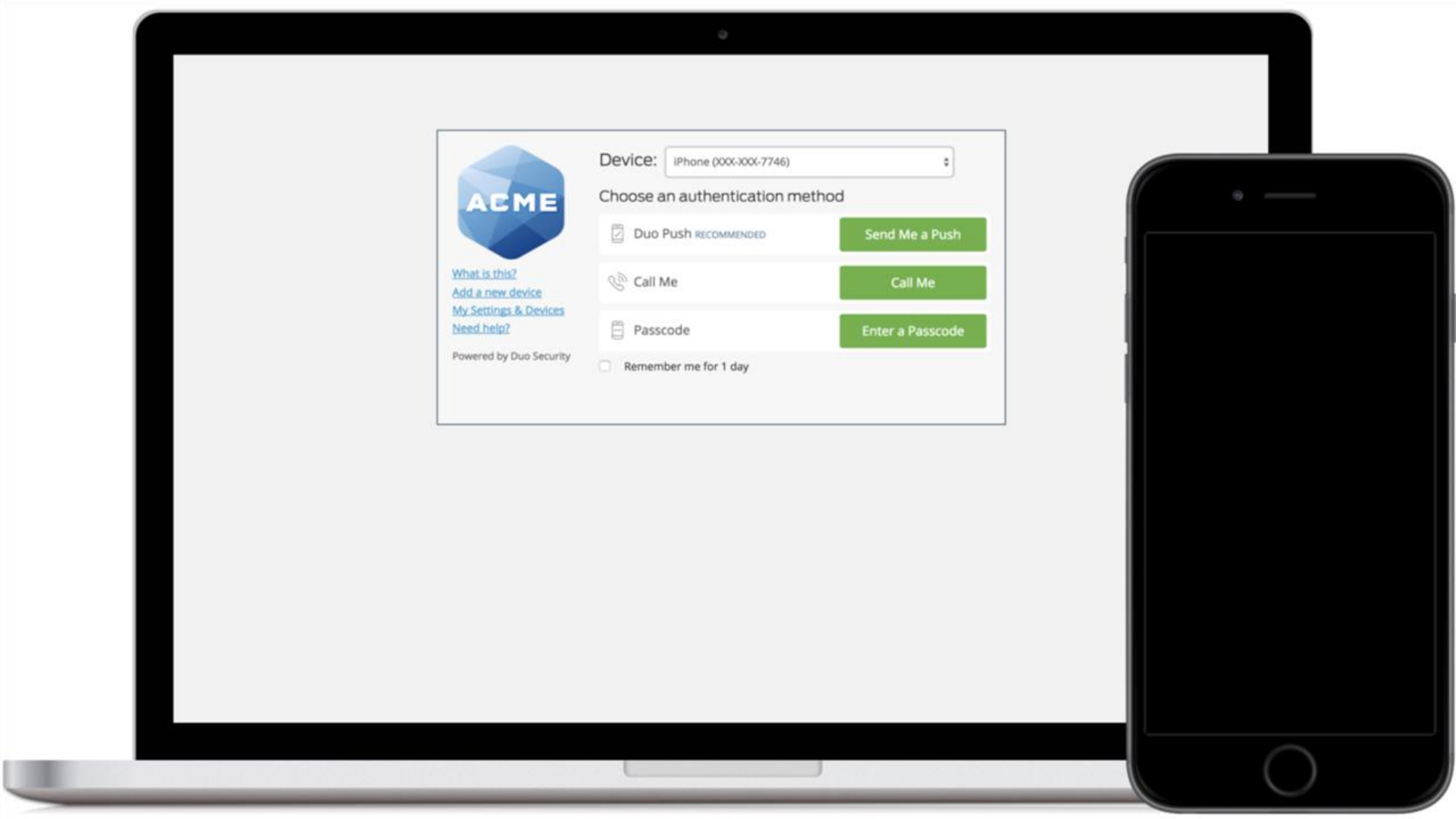
# ゼロトラストセキュリティ

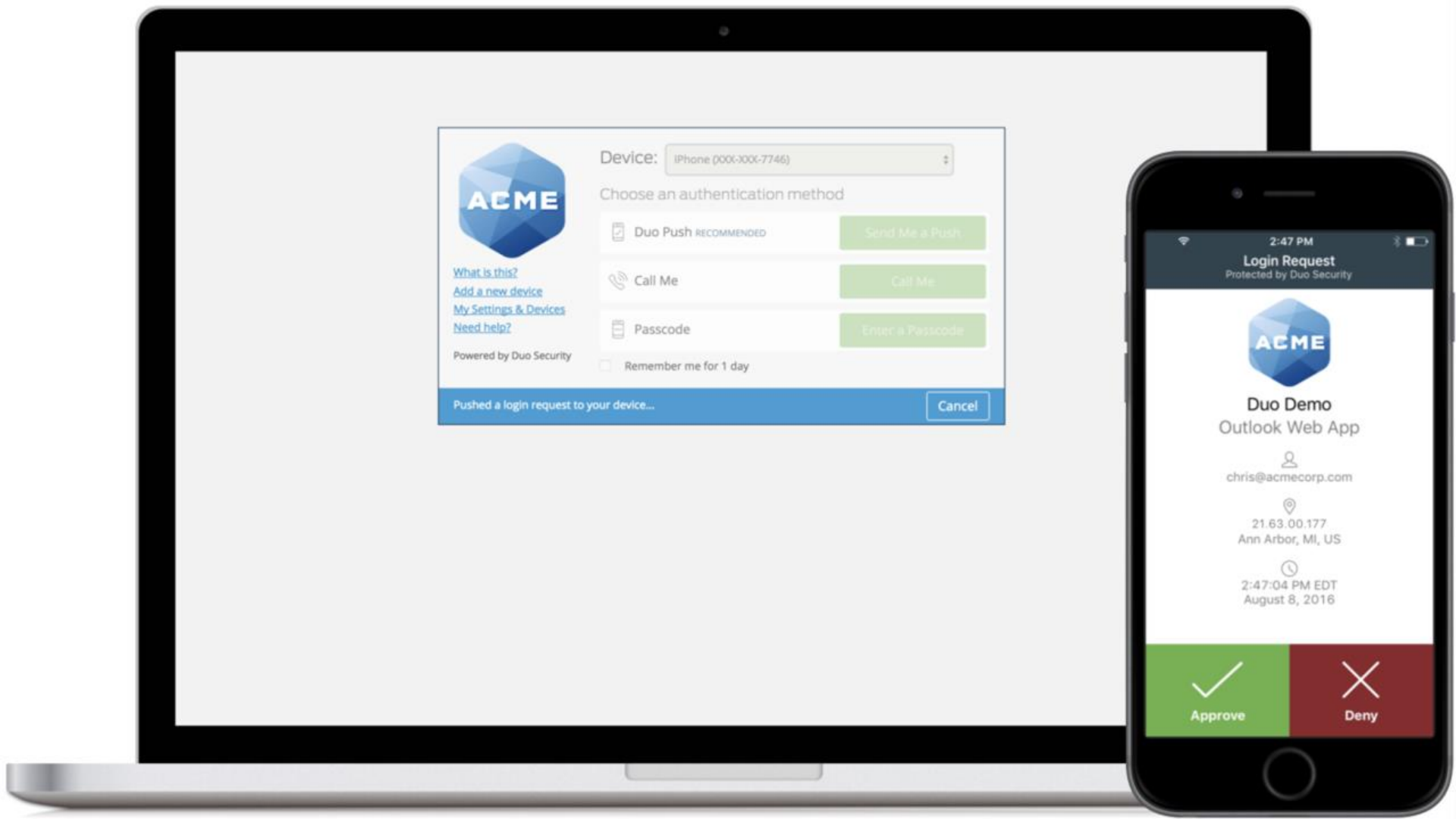
## 本人性の検証 を MFA で

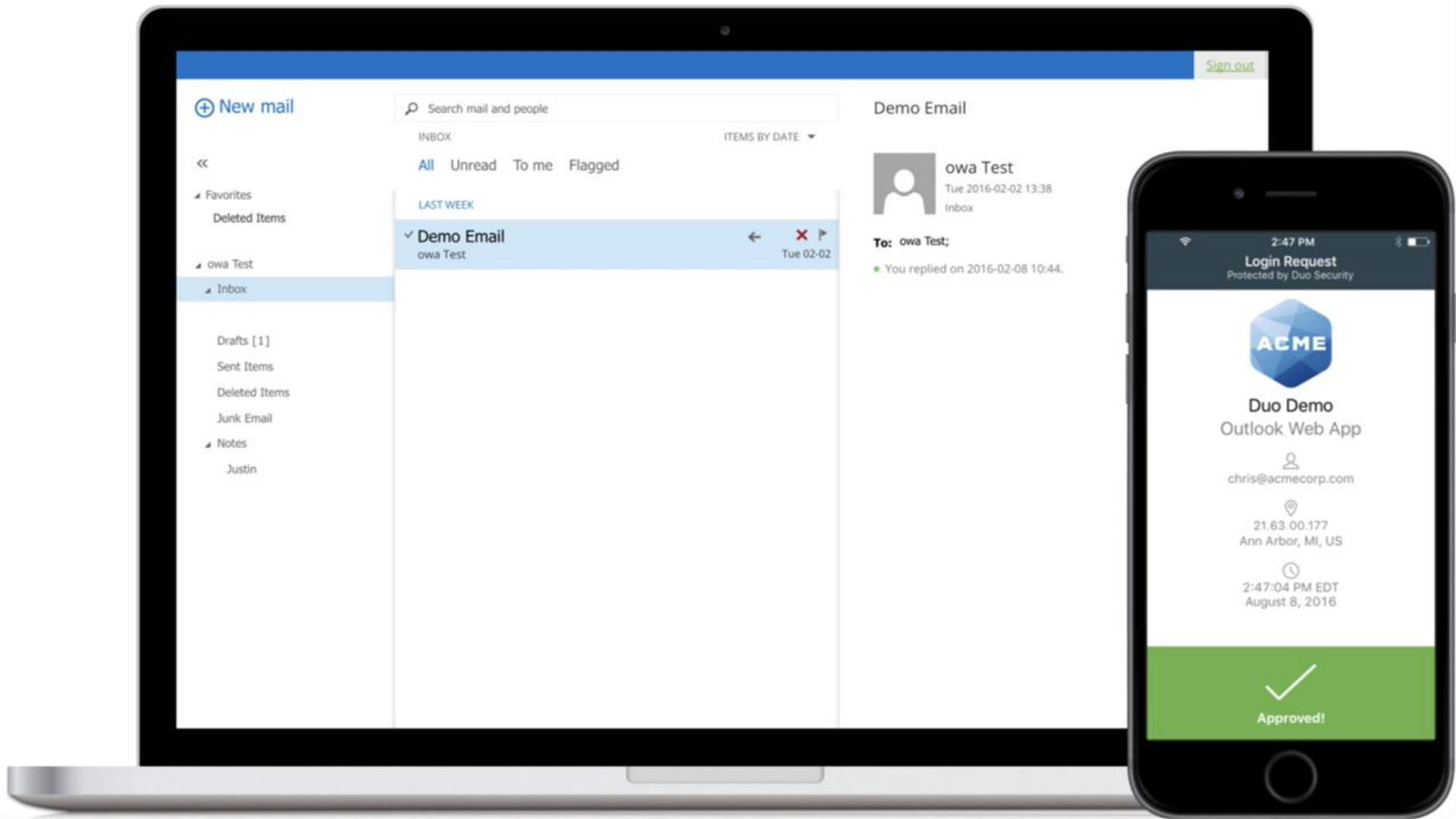
- 既存の認証に多要素認証を簡単に追加できる
- ユーザは数分で自己登録
- 多様な認証方法を提供




Outlook
Email:
chris@acmecorp.com
Password:
sign in

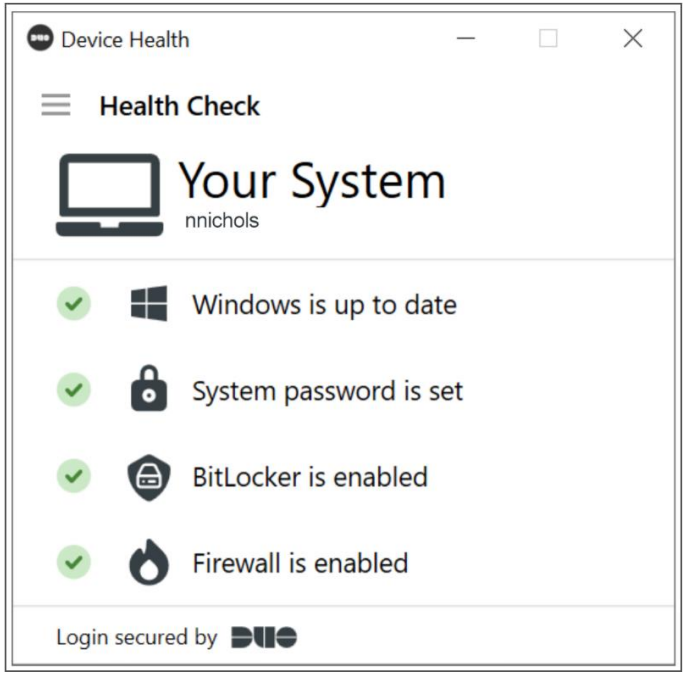

ACME
Device:
iPhone (XXX-XXX-7746)
Choose an authentication method
Duo Push RECOMMENDED
Send Me a Push
Call Me
Call Me
Passcode
Enter a Passcode
Remember me for 1 day
What is this?
Add a new device
My Settings & Devices
Need help?
Powered by Duo Security

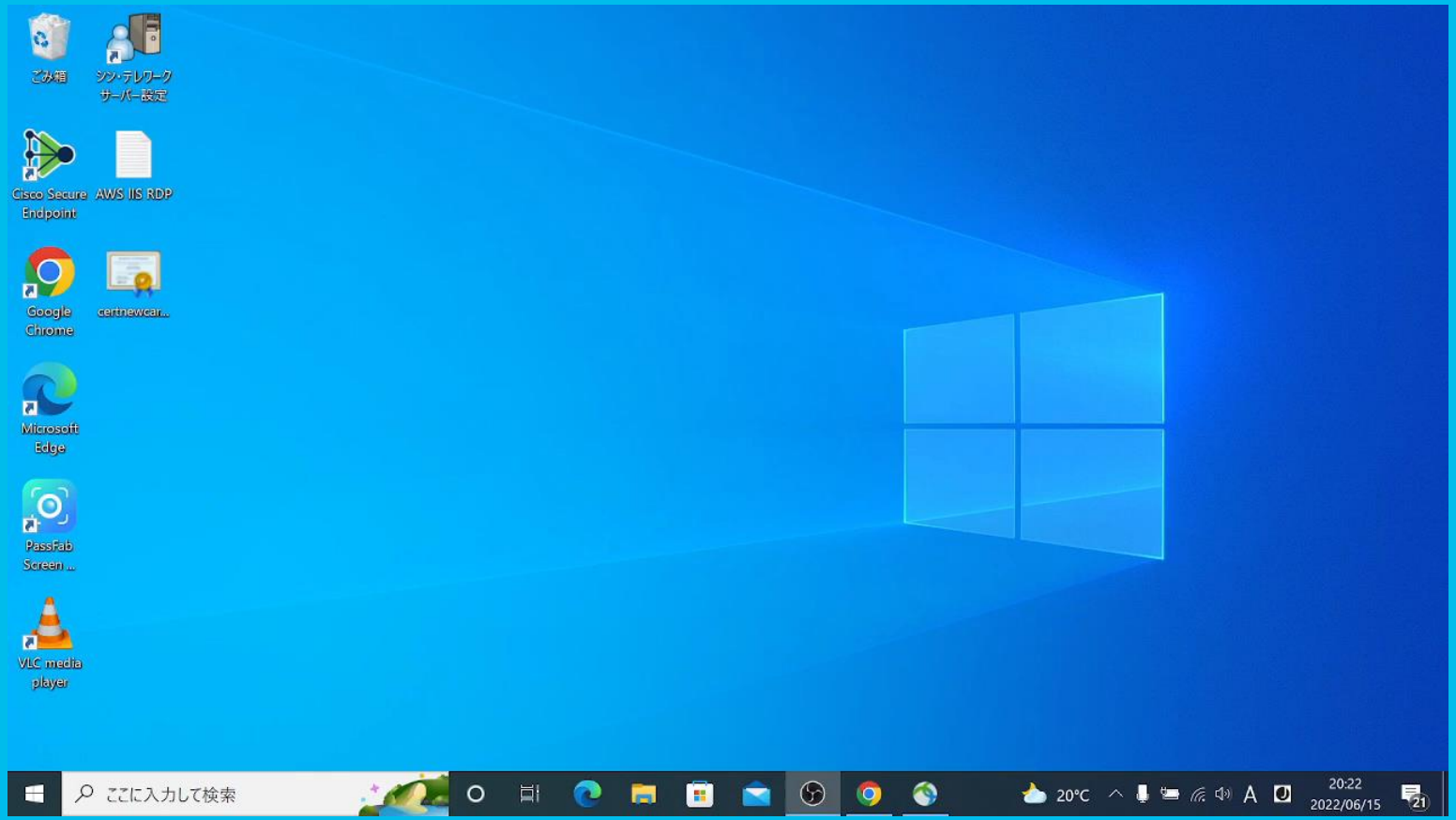

ACME
Device:
iPhone (XXX-XXX-7746)
Choose an authentication method
Duo Push RECOMMENDED
Send Me a Push
Call Me
Call Me
Passcode
Enter a Passcode
What is this?
Add a new device
My Settings & Devices
Need help?
Powered by Duo Security
Remember me for 1 day
Pushed a login request to your device...
Cancel
2:47 PM
Login Request
Protected by Duo Security
ACME
Duo Demo
Outlook Web App
chris@acmecorp.com
21.63.00.177
Ann Arbor, MI, US
2:47:04 PM EDT
August 8, 2016
Approve
Deny


Sign out
New mail
Search mail and people
INBOX
ITEMS BY DATE
All
Unread
To me
Flagged
Favorites
Deleted Items
owa Test
Inbox
Drafts [1]
Sent Items
Deleted Items
Junk Email
Notes
Justin
LAST WEEK
Demo Email
owa Test
Tue 02-02
Demo Email
owa Test
Tue 2016-02-02 13:38
Inbox
To: owa Test;
You replied on 2016-02-08 10:44.
2:47 PM
Login Request
Protected by Duo Security
ACME
Duo Demo
Outlook Web App
chris@acmecorp.com
21.63.00.177
Ann Arbor, MI, US
2:47:04 PM EDT
August 8, 2016
Approved!

# Duo Device Health Applicationによるデバイスの正常性・状態チェック

- ユーザーのデバイスがデバイスヘルスポリシーのセキュリティ要件を満たしていない場合、 Duo Device Health Applicationは、アプリケーションのデバイスヘルスポリシーに合わせてセキュリティポスチャを修正するための手順をユーザーに提供します。





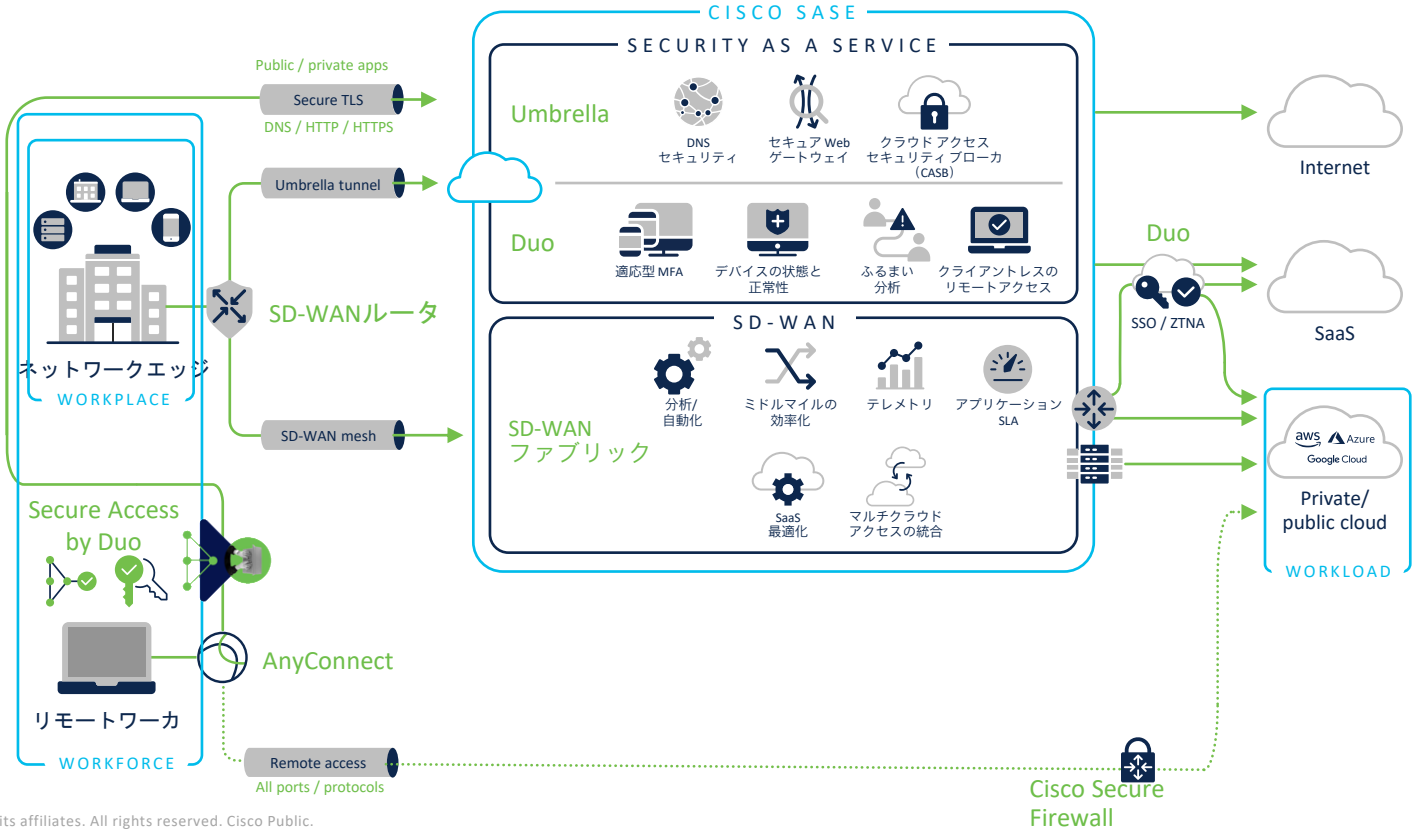
# SASE アイデンティティ：ゼロトラストワークフォース

## Secure Access by Duo

| 適応型多要素認証とパスワードレス | デバイスの状態と正常性 | 最小限の特権アクセス | 継続的な検証 | ふるまい分析 |
|---|---|---|---|---|
| ✓ | ✓ | ✓ | ✓ | ✓ |
| ユーザーの本人確認 | ログイン前にエンドポイントを評価し、正常性を確保させる | ゼロトラスト：アプリケーションのログインごとにセキュリティ態勢を確保 | ログインのたびに、継続的にセキュリティを分析 | 通常とは異なる疑わしいログイン/アクセスアクティビティを検出してレポート |

あらゆるユーザー、あらゆるデバイス、あらゆるアプリケーションが対象

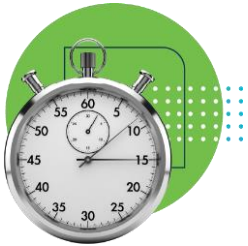
# Cisco SASEアーキテクチャ



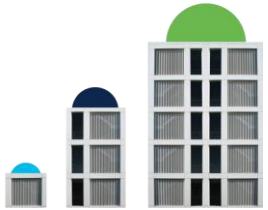
# Cisco Secure Managed Remote Access

# Cisco Secure Managed Remote Access

ベストオブブリードの
AnyConnect ベースの
リモートアクセス VPN



フルマネージドの
シンプルさ、無制限の
拡張、迅速な価値実現

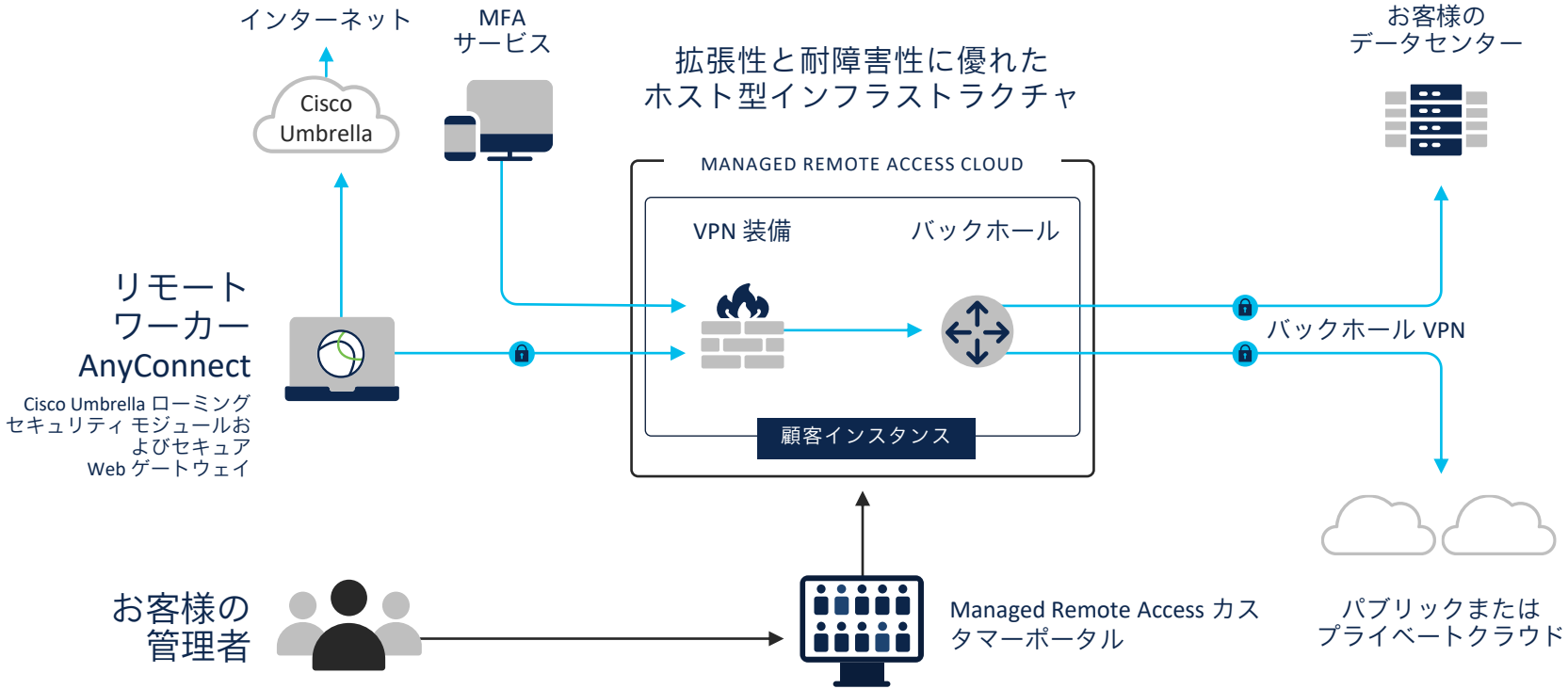


クラウドサービスと
して提供されるため
ハードウェアの購入や
管理が不要

シスコの信頼性、
確実性、サポート

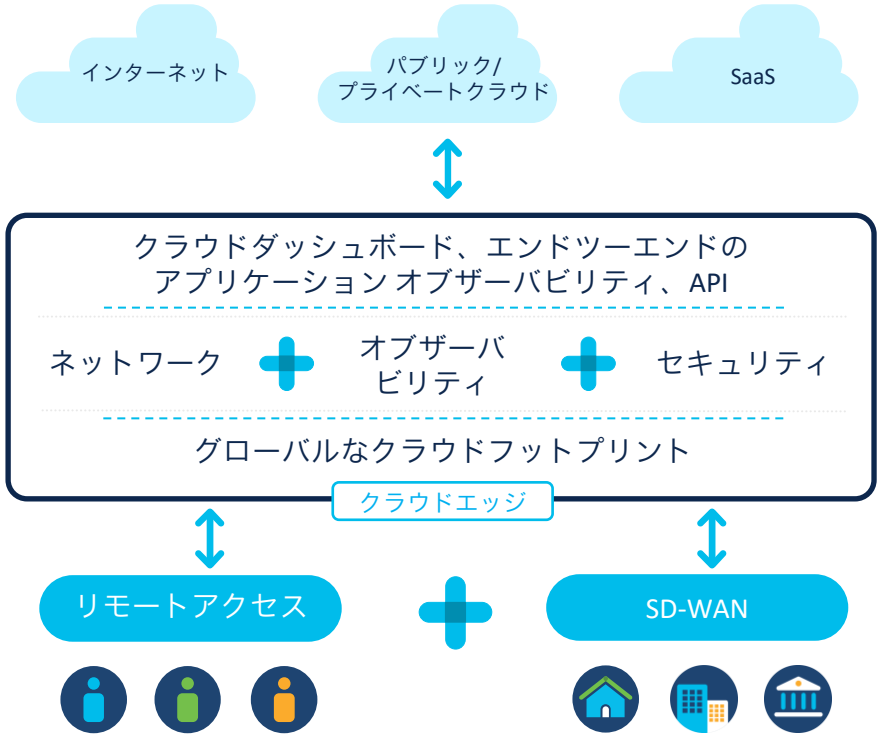
**拡張性に優れたセキュアなリモートアクセスサービスを
世界規模で提供**

# 仕組み



# シスコの PLUS SASE ビジョン

- ビジネスニーズに対応した柔軟な消費モデルで提供される単一のサブスクリプション
- デバイスや場所を問わず、あらゆるアプリケーションにシームレスかつ安全にアクセス
- クラウドで提供される効率的なセキュリティ機能とネットワーク機能
- グローバルなクラウドフットプリント
- 未来：プレミアムサービス、完全な Network-as-a-Service スタックへの拡張性

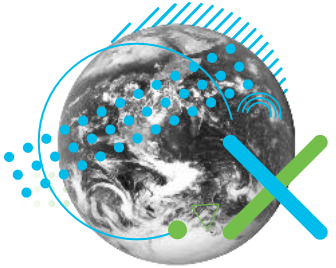


# どこから始めますか？

詳細：cisco.com/go/sase

リモートワーカーを保護

セキュアなクラウドエッジ



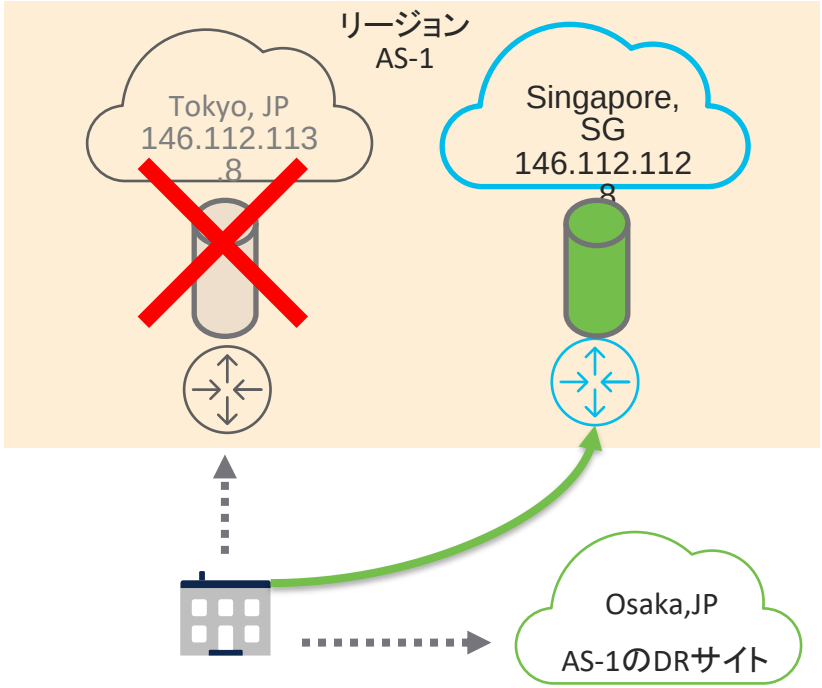
セキュリティ機能を
クラウドに移行

## ニーズに合わせた SASE

# Q&A

# Cisco UmbrellaのIPsec フェイルオーバー

## 設定すべきIPsecトンネルは1本でシンプル / 障害発生時は自動で切り替わり




- Cisco Umbrellaのデータセンターはそれぞれのリージョンでペアとなるデータセンターが存在する
- もしデータセンターに障害が起きた際は、そのペアのデータセンターが自分のIPアドレス宛てのIPsecに加え、障害が起こっているサイト宛てのIPsec通信も処理を始める
- さらにリージョン全体の障害があった場合にはそれぞれのリージョンに対して用意されているDRサイトがトラフィック処理を引き継ぐ
- 運用がシンプル
  - 通常時からIPsecトンネルは単一のデータセンター向けに1本作成しておけばよい（バックアップサイトへのIPsecトンネルは不要）
  - フェイルオーバー時に設定変更やルート切り替えのの操作は不要


The bridge to possible