cisco Secure

Duoで実現するZTNAとは

– 信頼するか・しないか、それが重要です！ –

シスコシステムズ合同会社
村上　英樹
2020年8月6日

Agenda

1. ゼロトラストが必要となった背景
2. ZTNA（ゼロトラストネットワークアクセス）
3. ZTNA に必要な機能
4. Duo による ZTNA導入シナリオ
5. まとめ

ゼロトラストが必要となった背景

デジタル化によって起こるIT環境の変化

- あらゆる場所にあるユーザ、デバイス、アプリケーション

企業境界の拡大による、脅威と複雑性の増大に直面している

実践的なセキュリティアプローチ
脅威対策とゼロトラストが攻撃を阻止

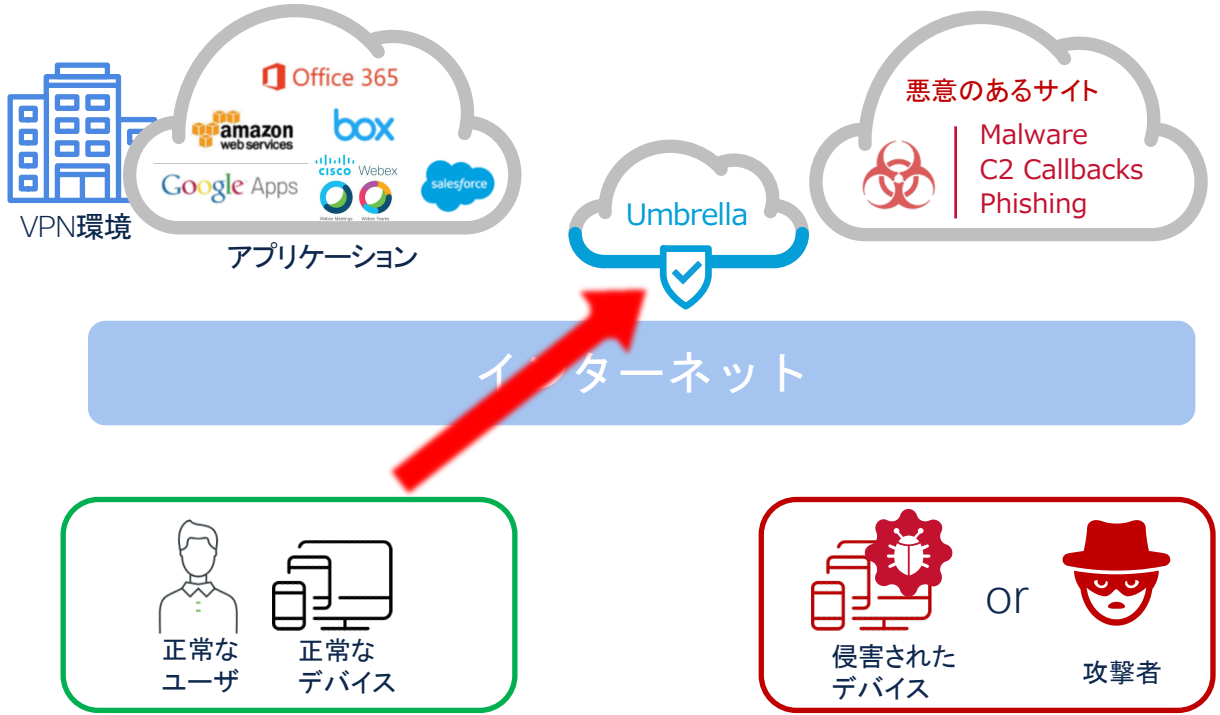
Threat-Centric
脅威対策

インテリジェンスを基にしたポリシーにより攻撃を防止(検出・調査・修正)するための基本的なセキュリティ

Trust-Centric
ゼロトラスト

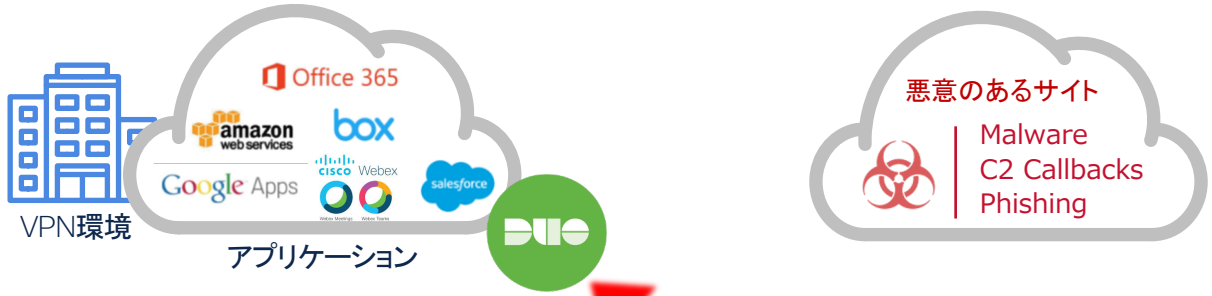
あらゆる場所、ユーザ、デバイス、アプリケーションに対して、アイデンティティを基に検証しアクセスを許可

脅威対策
悪意のあるサイトへの誘導は、Umbrellaで防御



Umbrella
正常な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DNSレイヤおよびWebプロキシで防御する。

ゼロトラスト
Duoによるユーザとデバイスの信頼に基づいた防御



インターネット

Duo Security

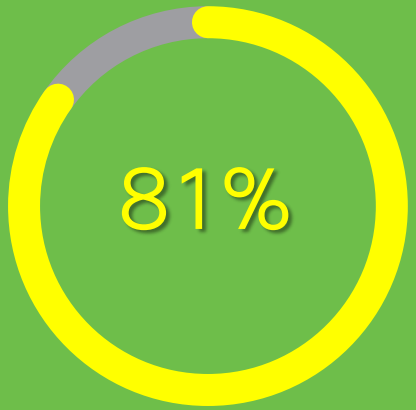
フィッシングやクラッキングで盗んだクレデンシャルを利用した攻撃者やマルウェアに侵害されたデバイスによる、VPN接続やクラウドおよびオンプレアプリへの侵入を防御する。

現実の脅威：不正侵入は、ID/パスワード漏洩から
セキュリティの新しいアプローチが必要とされる

Targeting Identity

81%のハッキングによる侵害は、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



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

テレワーク(オンライン授業)で必要なセキュリティ対策

テレワークを行う際のセキュリティ上の注意事項

掲載日：2020年 4月 21日
独立行政法人情報処理推進機構
セキュリティセンター

1. はじめに

新型コロナウイルス感染症(COVID-19)の影響により、ICTを用いて自宅でも業務が行えるような環境を整えて、社員等を出社させずに事業継続を図る動きが急速に進んでいます。このような環境で働くテレワーク勤務者に向けたセキュリティ上の注意事項をご案内します。

テレワークには様々な利用環境があります。代表的なのは、自宅のパソコン等を用いてリモートデスクトップや仮想デスクトップで社内での業務用端末と同じ利用環境（テレワーク環境）を実現する方法です。

一方でそのような本格的な環境が提供されていない状況で自宅勤務を実施されている場合もあると思います。このページでは、そのような場合における注意事項も説明します。

https://www.ipa.go.jp/security/announce/telework.html

警視庁　安全な暮らし　交通安全　相談・お悩み　手続き

トップページ → 安全な暮らし → 情報セキュリティ広場 → 注目情報 → テレワーク勤務のサイバーセキュリ

テレワーク勤務のサイバーセキュリティ対策！

更新日：2020年4月16日

テレワークで勤務をされる方へ

サイバーセキュリティ対策

テレワークで使用するパソコン等（タブレット、スマートフォン）

サポートが終了しているOS（オペレーティングシステム）のパソコンを使用しない。

Windows7、WindowsVista、WindowsXPは、すでに脆弱性等に対するサポートがされていないため、マルウェア（ウイルス）に感染するリスクが高くなります。

ウイルス対策ソフトを必ず導入する。

マルウェア（ウイルス）の感染防止のために必ず導入しましょう。

https://www.keishicho.metro.tokyo.jp/kurashi/cyber/joho/telework.html

National Security Agency | Cybersecurity Information

Selecting and Safely Using Collaboration Services for Telework

Criteria to Consider When Selecting a Collaboration Service

1. Does the service implement end-to-end encryption?
2. Are strong, well-known, testable encryption standards used?
3. Is multi-factor authentication (MFA) used to validate users' identities?
4. Can users see and control who connects to collaboration sessions?

https://media.defense.gov/2020/Apr/24/2002288653/-1/-1/0/CSI-SELECTING-AND-USING-COLLABORATION-SERVICES-SECURELY-SHORT-FINAL.PDF

コンプライアンスへの対応

PCI-DSS 3.2 Section 8.3 のMFA要件

ISO 27001に準拠したすべての個人および企業のデバイスの可視化

NIST 800-63 と 800-171 のアクセスセキュリティ要件

強固なセキュリティを実現するFIPS準拠の暗号アルゴリズム

E-prescription を承認する際の、DEAのEPCS要件

PHIへのアクセスに使用されている個人のデバイスを可視化

ZTNA
(ゼロトラストネットワークアクセス)

ゼロトラスト ネットワークアクセス

ゼロトラスト = “Never Trust, Always Verify”

ゼロトラスト ネットワークアクセスとは

ZTNAは、**リソースへの制御されたアイデンティティおよびコンテキストを認識したアクセスを提供し、攻撃の対象領域を削減します。** ZTNAによって分離され、接続性が向上し、アプリケーションをインターネットに直接公開する必要がなくなります。

- ネットワークアクセスのための十分な信頼性を確立するためには、IPアドレスや位置情報は実用的ではない
- 適応性のあるアイデンティティを認識した精密なアクセスを提供する
- VPNの置き換えがZTNAの一般的なドライバー (SDP, IAP)

ZTNA に必要な機能

ZTNA (Zero Trust Network Access) に必要な機能
ゼロトラストのコンポーネントをベースにしたDuoの機能

- コントロールプレーン ▶ Duo Cloud

  [BeyondCorp*]
  - User/Device Inventory DB
  - Access Control Engine
  - Certificate Issuer
  - Trust Inference

  ユーザ・多要素認証管理(パスワードレス)、ユーザポリシー、デバイス可視化とポリシー、アプリケーションへのアクセス制御、PKI、ログ管理、トラストモニター

- 認証・認可 ▶ Duo Central

  [BeyondCorp*]
  - Single Sign-On

  シングルサインオン、ユーザ信頼、デバイス信頼

- ゼロトラストプロキシ ▶ Duo Network Gateway

  [BeyondCorp*]
  - Access Proxy

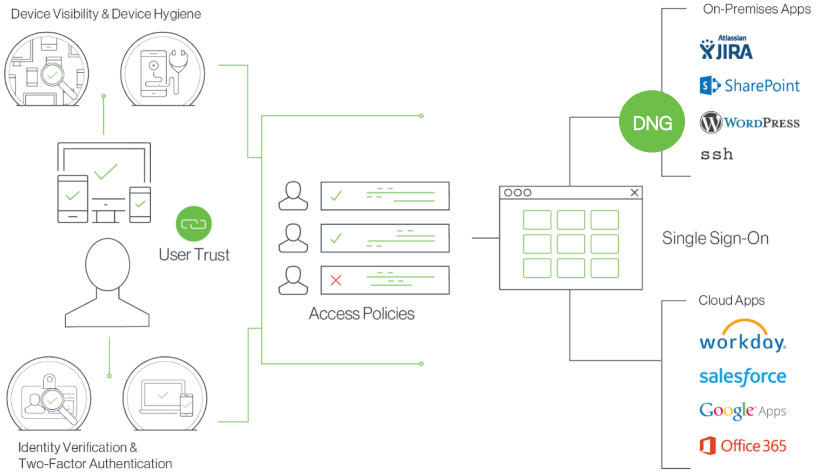
  リバースプロキシ、暗号化、内部アプリケーションを保護、Identity-Aware ProxyとしてVPNレス環境を提供

*参考情報
https://storage.googleapis.com/pub-tools-public-publication-data/pdf/43231.pdf

Duoによる
ZTNA導入シナリオ

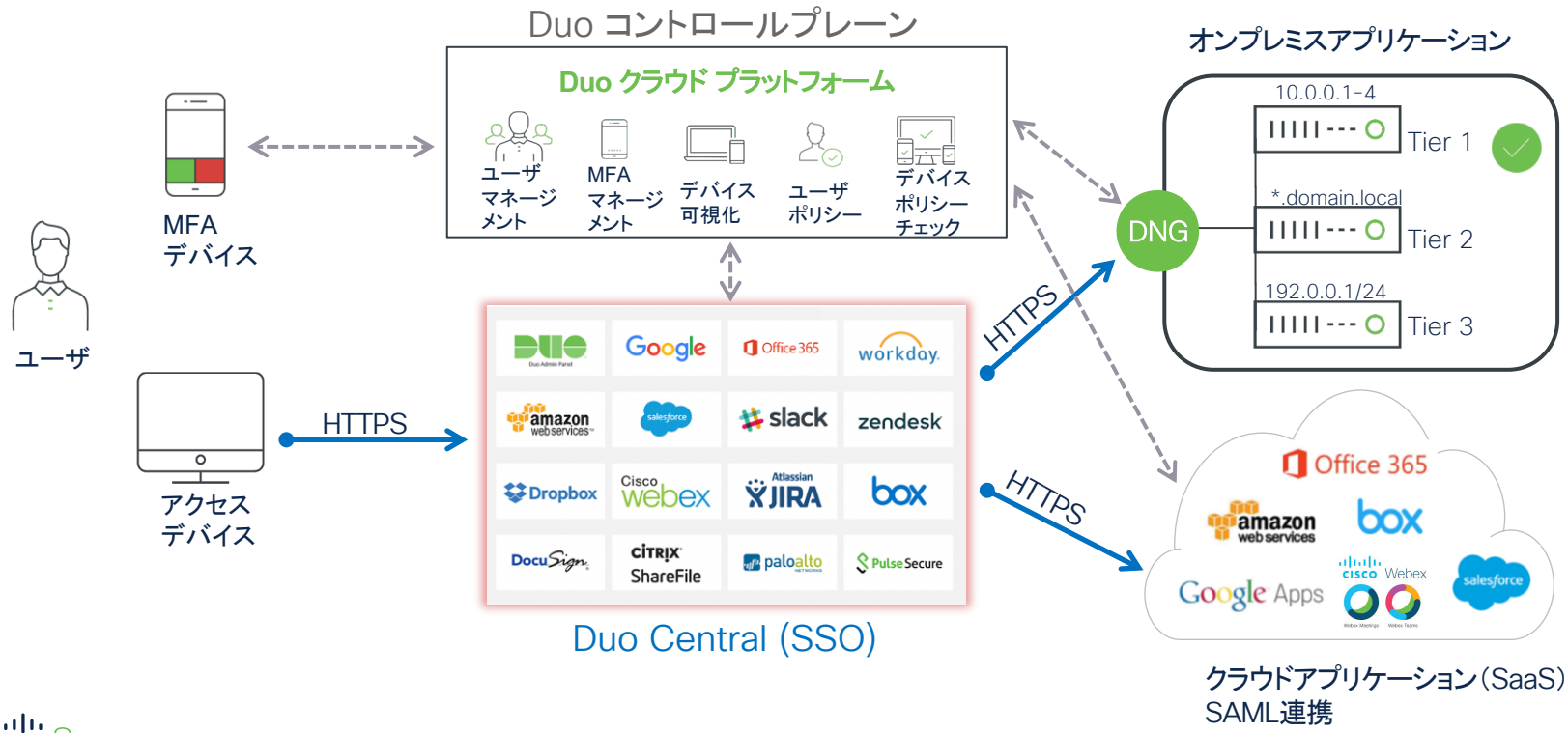
アプリケーションへシームレスでセキュアなアクセス
- SSO, 多要素認証, デバイス可視化, ゼロトラストプロキシ -

Duo Central + DNG



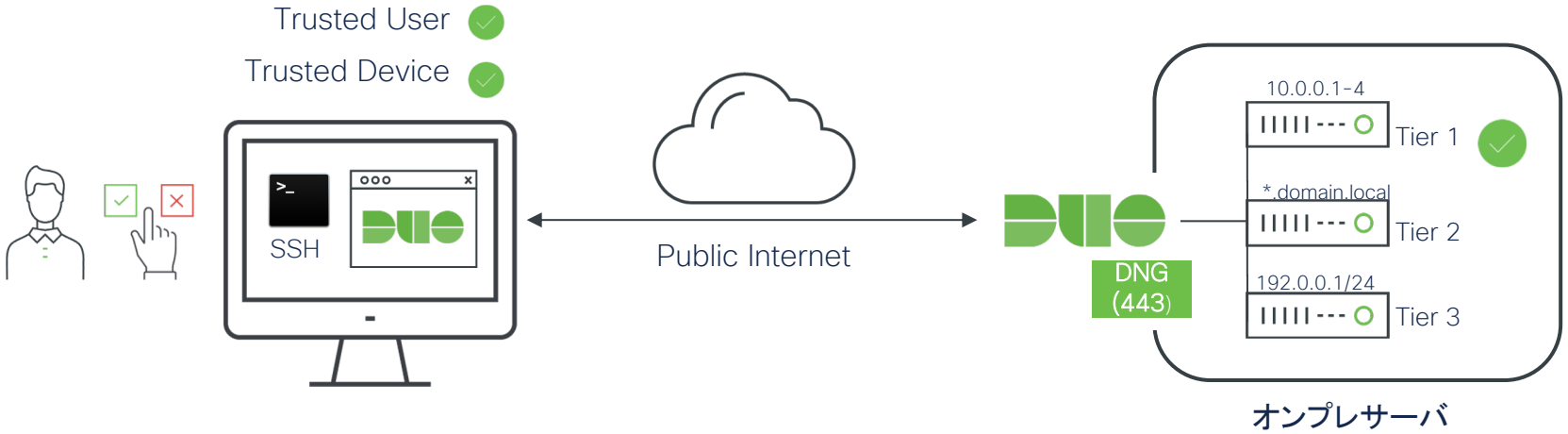
- シングルサインオン(SSO):
  クラウドアプリ、オンプレアプリへの
  アクセスは、SSOのポータルから
- 多要素認証:
  MFAにより、ユーザの信頼
- デバイス可視化:
  デバイス健全性、管理対象デバイス
- ゼロトラスト プロキシ
  IAP (Identity-Aware Proxy):
  DNG(Duo Network Gateway) が
  リバースプロキシを提供

Duo ゼロトラスト アーキテクチャ
Duoクラウドによる制御



Duo Network Gateway: リバースプロキシ

VPNレスによる内部HTTP/S と SSH サーバへのゼロトラスト アクセス

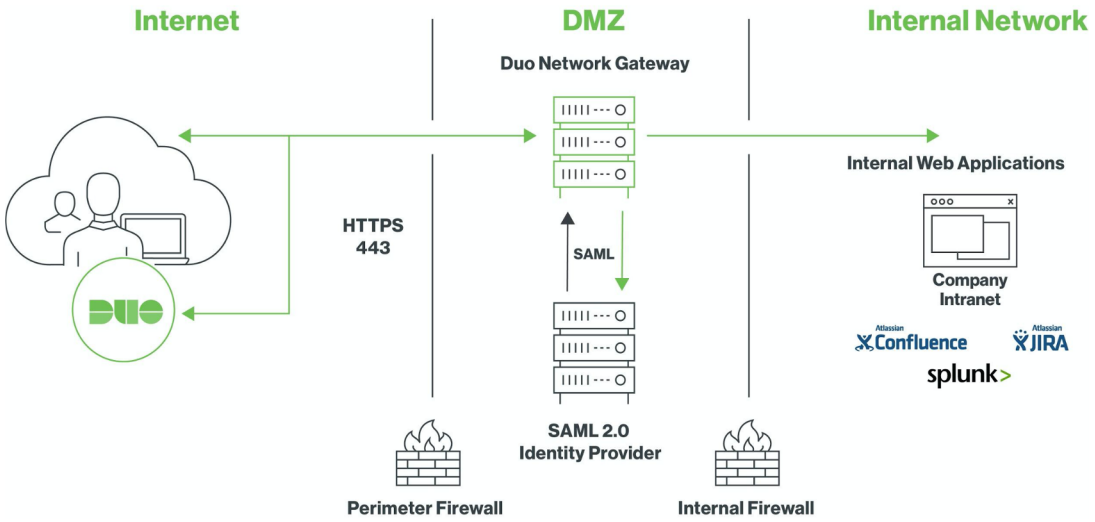


内部ネットワークとパブリッククラウドへのアクセスをセキュアにするために、
Duo Beyond (Duo Network Gateway) を利用する

amazon web services™ Google Cloud Platform Microsoft Azure

Duo Network Gateway (DNG) の導入

- DMZにDNGをデプロイ
- プライマリ認証のための SAML IdP を 構成
- 保護された内部(Internal) Webアプリケーション用にパブリックDNSエントリを作成し、DNGのパブリックインターフェースに向ける
- ユーザは、ブラウザを利用してDNG経由で内部(Internal)アプリケーションにアクセス



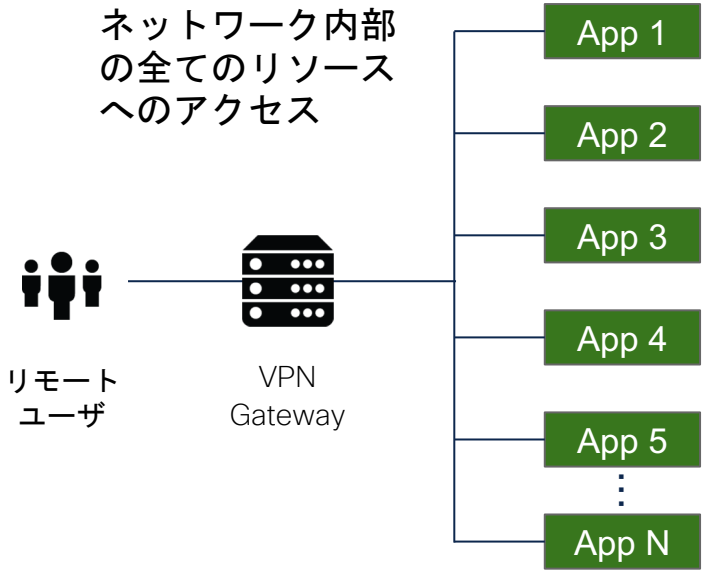
ネットワークとアプリケーションへのアクセス

門番ではなく、ボディーガード

VPN

VPN のアプローチ:

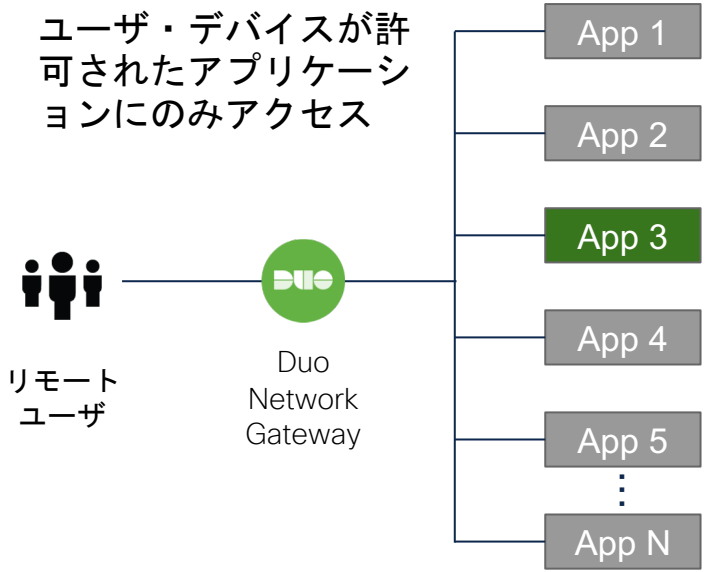
ネットワーク内部の全てのリソースへのアクセス



Duo Network Gateway

Duo のアプローチ:

ユーザ・デバイスが許可されたアプリケーションにのみアクセス



まとめ

シスコは、ゼロトラストと脅威対策を提供します！

どのような対策が必要か?	シスコのセキュリティソリューション
漏洩したクレデンシャルによる不正アクセスからの保護	Duo Security (MFA)
どこからでも、アプリケーションやリソースへのシンプルかつ強力なアクセス制御の提供	Duo Security (**デバイス可視化**, **適応型ポリシー**, SSO, DNG)
ユーザ、アプリケーションを脅威から保護	Duo Security (**トラストモニター**), Umbrella, AMP, CES(Email)

無償でDuoをご利用いただけます！

注）Duo Beyond機能をご利用の場合、ライセンスのアップグレードが必要となりますので、担当営業までご連絡ください。

■30日間フリートライアル申し込みサイト

https://www.cisco.com/c/m/ja_jp/duo/trial.html


cisco
Secure