「ゼロから信頼性を創り上げる」セキュリティの新たなアプローチ

シスコ ゼロトラストセキュリティ

――働き方改革やデジタル化など、近年、企業や組織のネットワーク利用のあり方が大きく変化しています。
それに伴い、従来の境界型セキュリティだけに頼るアプローチは限界に近づきつつあります――

――ネットワークの過去から現在へ――

社内の信頼できるユーザが安全なデバイスで、社内のリソースにアクセスする、
ファイアウォールなど社内外の境界に位置するセキュリティで社外からの脅威を防御し、社内の安全と信頼性を確保する――
――これまでは、このような「**安全で信頼できる社内**」と「**危険な社外**」という前提や目的に基づく、**境界型のセキュリティアプローチが一般的**でした。

しかし、**現在では、この前提や目的が崩れつつあります**。

来訪者など**多様なユーザ**、さらに BYOD や IoT など**多様なデバイス**によるアクセスも発生し、
アクセス先のリソースが**クラウドなど社外に点在**するようになり、さらにアクセス元も外出先や自宅、パートナー企業に拡大するなど、
社外からの柔軟なアクセスが求められるようになっています。

その結果、次のような課題が生まれています。

多様化する各ユーザ / デバイスに
適切なアクセス権を与えたい

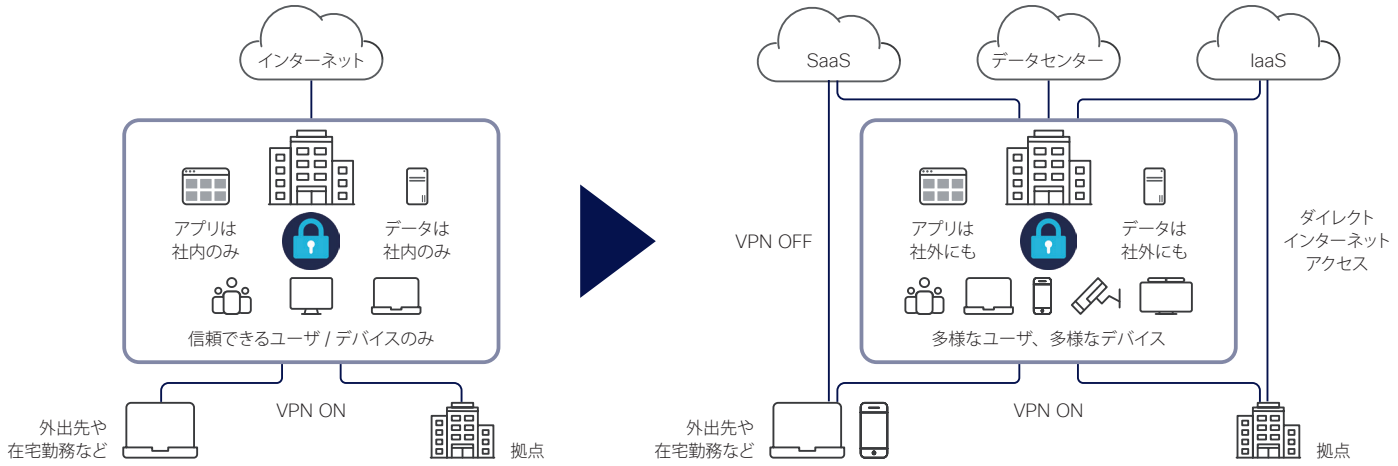
従来の境界をまたいで拡大する
攻撃対象を保護したい

従来の境界をまたいで生じうる
潜在的なリスクを可視化したい

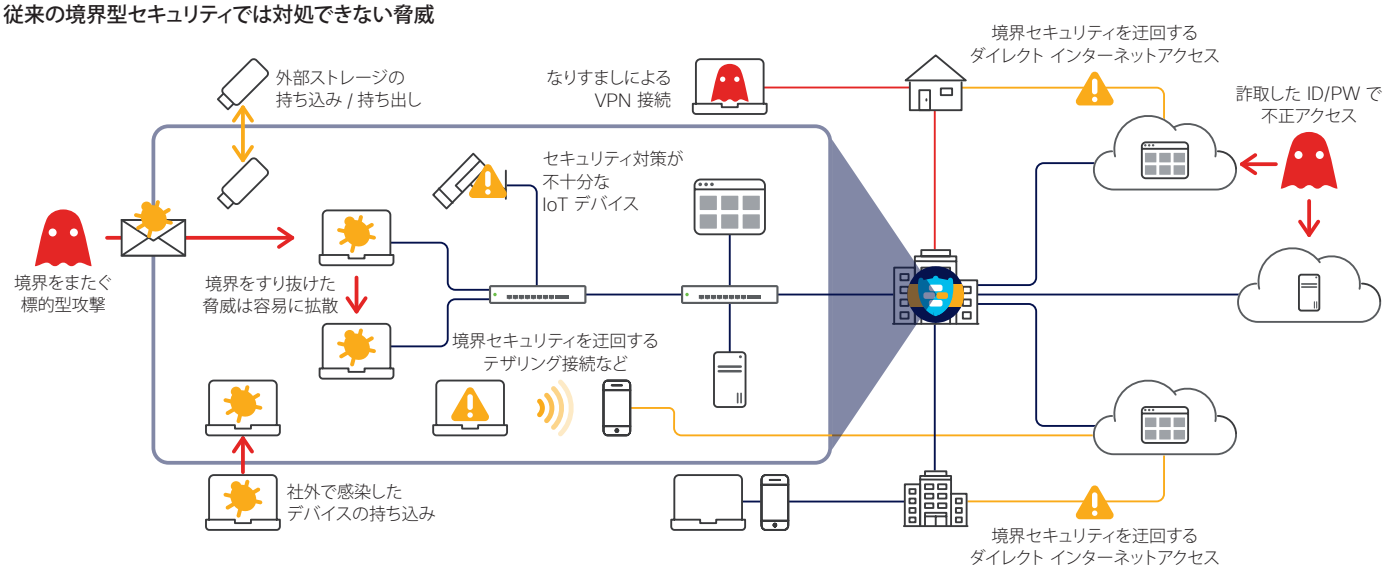
――このような新しい課題に対処できるアプローチとして着目されているのが「**ゼロトラスト**」セキュリティです――

変化するビジネス、IT 環境、そして脅威

ファイアウォールや IPS など、境界型セキュリティで守られた安全な社内ネットワークから危険な社外ネットワーク（インターネット）に接続する、それが従来のビジネスのあり方であり、IT 環境でした。外出先など物理的な社外からでも、インターネットを利用する場合には VPN で境界型セキュリティを経由することが基本的な考え方でした。現在では、働き方改革の推進やクラウド利用の拡大によって、境界型セキュリティを経由しないダイレクト インターネットアクセスが増加しています。また、社内外を出入りするユーザやモバイルデバイスの増加、さらに IoT など、ネットワークに接続するユーザやデバイスも多様化しています。その結果、境界型セキュリティでは対処できない新たな脅威がどんどん生まれてきています。



従来の境界型セキュリティでは対処できない脅威



シスコ ゼロトラストセキュリティ

「**ゼロトラスト**」（zero trust）は、2010 年に Forrest Research 社が発案した概念枠組みです。「**決して信頼するな、常に検証せよ**」（never trust, always verify）という基本概念に基づき、従来の境界型セキュリティアプローチのように**安全で信頼できる社内**と**危険な社外**という前提ではなく、社内外の**あらゆる領域が潜在的に危険である**という前提でセキュリティを実装するアプローチです。

シスコのゼロトラストセキュリティは、企業や組織の IT を「**あらゆるユーザとデバイス**」「**あらゆるアプリ**」「**あらゆる場所**」の 3 つの領域に分けて保護対象とし、ゼロトラストの基本概念を各領域で適用します。

あらゆるユーザ

- 自社の従業員
- パートナー社員
- ゲスト（来訪者）

高度なユーザ認証

あらゆるデバイス

- 会社支給
- 個人所有（BYOD）
- IoT（モノ）

デバイスの信頼性を評価

あらゆるアプリ

- オンプレミス
- ハイブリッドクラウド
- パブリッククラウド

通信を検閲

あらゆる場所

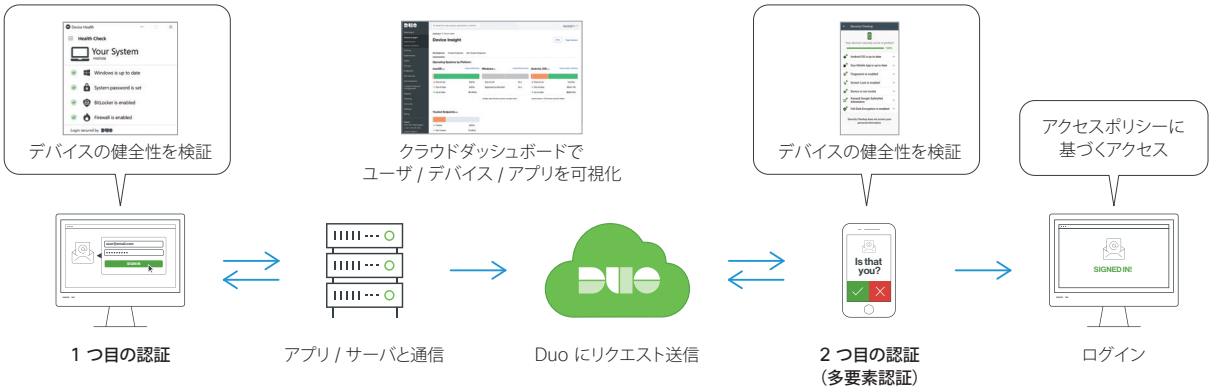
- オフィス
- 自宅
- オン / オフ VPN

最小権限でアクセスを許可

あらゆるユーザとデバイスのためのゼロトラスト：Cisco Duo セキュリティ

Cisco Duo セキュリティは、場所を問わず、**あらゆるユーザとデバイス**があらゆるアプリケーション（クラウド、オンプレミス、VPN）にアクセスする際に機能するゼロトラストセキュリティです。

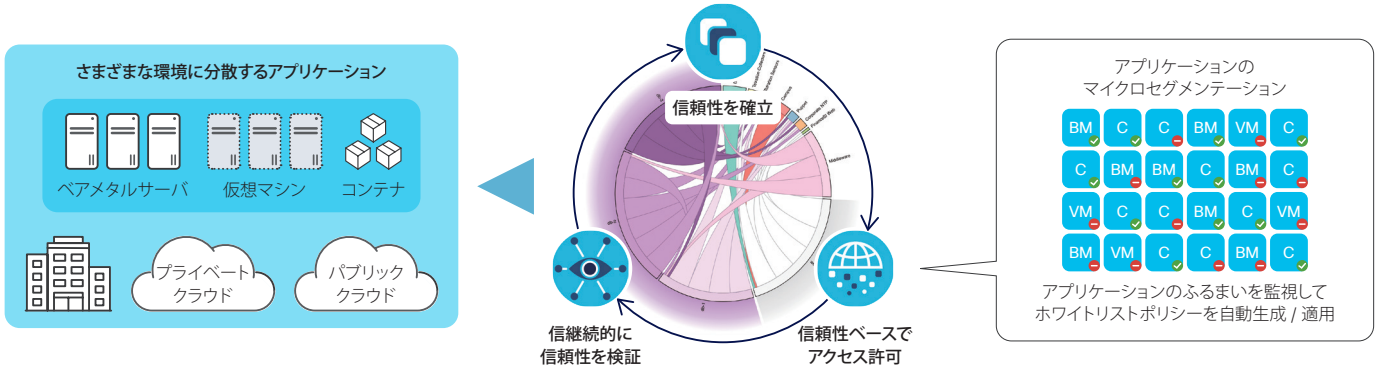
- **多要素認証**（Multi-Factor Authentication；MFA）によってユーザアイデンティティを検証
- **デバイスを可視化**して、セキュリティ健全性などに基づいて信頼性を確立
- 柔軟かつきめ細やかな**アクセスポリシー**によって、アプリケーションへのアクセスを制御



あらゆるアプリのためのゼロトラスト：Cisco Tetration

Cisco Tetration は、オンプレミス、ハイブリッドクラウド、パブリッククラウドを問わず、**あらゆるアプリ**やサービスが他のシステムと通信する際に機能するゼロトラストセキュリティです。

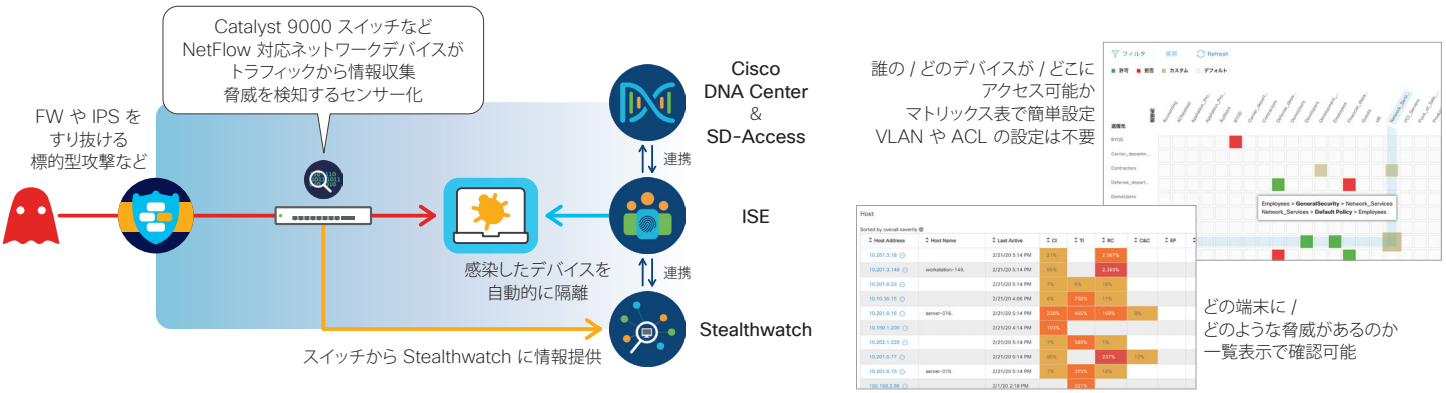
- ワークロードとその通信を可視化して信頼性を把握、正常な状態をポリシーとして定義（**信頼性を確立**）
- アプリケーションのマイクロセグメンテーションで脅威を封じ込め、拡散を抑制（**信頼性ベースでアクセス許可**）
- セキュリティ侵害の兆候を継続的に監視して、ポリシー違反時にはアラートを通知、通信を遮断（**継続的に信頼性を検証**）



あらゆる場所のためのゼロトラスト：シスコのセキュアなネットワーク

シスコのセキュアなネットワーク（**ネットワークセンサー**と SD-Access）は、**あらゆる場所**、すなわちネットワークに、IoT を含むあらゆるユーザ / デバイスがアクセスする際に機能するゼロトラストセキュリティです。

- **NetFlow 対応ネットワークデバイス**が脅威を検知するセンサーとして稼動
- アクセス可否をマトリックス表で簡単設定、VLAN や ACL を使わずに**ネットワークセグメンテーション**を実現
- 脅威の所在を一目で確認、感染したデバイスは**自動的に隔離**



シスコ ゼロトラストセキュリティ製品ポートフォリオ

Cisco Duo セキュリティ、Cisco Tetration、シスコのセキュアなネットワークが、シスコ ゼロトラストセキュリティの保護対象となる 3 つの領域「あらゆるユーザとデバイス」「あらゆるアプリ」「あらゆる場所」に対応する主要製品 / ソリューションです。さらにもう 1 つ、Cisco Umbrella がゼロトラストを補完します。

Cisco Duo セキュリティ（あらゆるユーザとデバイスを保護）

適応型の多要素認証とデバイス可視化を実現するソリューションです。信頼できるユーザとデバイスだけがアプリケーションにアクセスできるようにポリシーを適用し、情報漏洩のリスクを軽減します。

Cisco Tetration（あらゆるアプリを保護）

アプリケーションの依存関係やプロセスにおけるふるまいを事実ベースで可視化してホワイトリストポリシー自動生成し、マイクロセグメンテーションによってアプリケーションを保護します。

Cisco SD-Access（あらゆる場所を保護）

Cisco Identity Services Engine（ISE）

ユーザ / デバイスに対するロールベースのアクセスコントロールとデバイスポスチャを提供する認証ポリシー管理システムです。

Cisco Stealthwatch

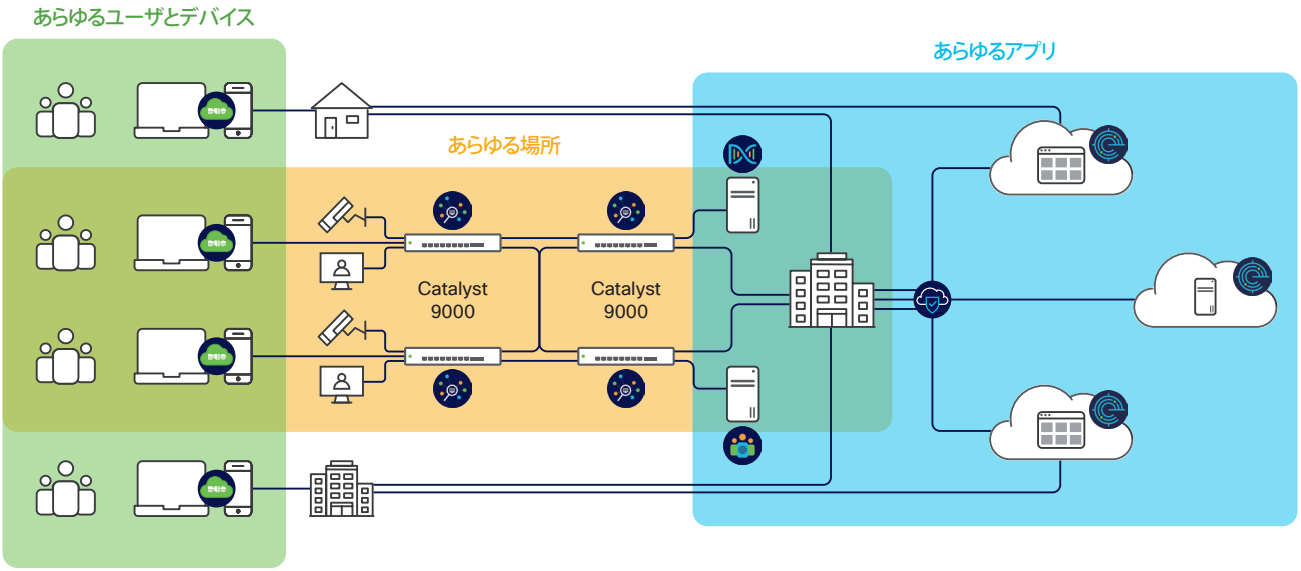
ネットワークデバイスが生成する NetFlow を活用し、ネットワーク / トラフィック全体を可視化して脅威を検出します。Cisco Catalyst 9000 シリーズの場合、暗号化されたトラフィックからでもマルウェアを検出できます。

Cisco DNA Center

ネットワークデバイスの運用管理をできる限り自動化することで、管理者の負担削減、設定ミスやトラブルの低減、障害の早期発見と対応の簡素化および短縮化を実現するネットワークコントローラです。

Cisco Umbrella（あらゆるユーザ、デバイス、アプリ、ネットワークを保護）

インターネットに接続する、あらゆるユーザ、デバイス、アプリ、およびネットワークを保護するセキュア インターネット ゲートウェイです。DNS レイヤセキュリティをベースに、セキュア Web ゲートウェイ（SWG）、クラウド提供型ファイアウォール、クラウドアプリセキュリティ制御、サンドボックスなど、幅広いセキュリティサービスを提供します。



また、シスコは、信頼性や保護を拡張するさまざまな製品を提供しています。

シスコ ゼロトラストセキュリティは、これらの製品と統合することによって、**より包括的なゼロトラストを実現**します。

- Cisco Firepower NGFW（次世代ファイアウォール）
- Cisco AnyConnect（リモートアクセス VPN）
- Cisco AMP（高度なマルウェア防御）
- Cisco Threat Grid（高度なサンドボックスと脅威インテリジェンス）
- Cisco E メールセキュリティ & Cisco Web セキュリティ

ゼロトラスト アドバイザリサービス

次のような課題を抱えるお客様を対象に、現状分析やロードマップ作成など、ゼロトラストの導入、計画、検討を支援します。

- ゼロトラストの導入を検討しているが、何から実施すればよいかわからない
- グローバル基準との比較で自社のセキュリティ対応状況を可視化 / 把握したい
- 働き方改革でリモートワークを導入するが、セキュリティ対策に不安がある

シスコ ゼロトラストセキュリティの詳細は、次の Web サイトをご覧ください。

www.cisco.com/jp/go/zero-trust

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp

シスコ コンタクトセンター

自社導入をご検討されているお客様へのお問い合わせ窓口です。
製品に関して | サービスに関して | 各種キャンペーンに関して | お見積依頼 | 一般的なご質問

お問い合わせ先

お電話での問い合わせ
平日 10:00-12:00, 13:00-17:00
0120-092-255

お問い合わせウェブフォーム
https://www.cisco.com/jp/go/vdc_callback

2161-2005-000-TO