Cisco **S**ecure **A**ccess **S**ervice **E**dge ソリューション

ハイブリッドワーク時代に求められる シンプルでセキュアなネットワークサービス

「**働き方改革**」や「**デジタル化**」などの掛け声に、ゆっくりと着実に呼応してきた企業、そしてネットワーク。
たとえば**テレワークやクラウドサービスの導入**が進みましたが、それらは多くの場合、あくまでも**従来のネットワーク設計をベース**に実現されました。
すなわち、**従業員が出社して、社内のアプリケーションやデータを利用することが主たるユースケース**として設計されたネットワークです。

それがいま、パンデミックの到来によって、**従来の設計の限界を露呈**しています。
テレワークは社会的な要請もあってユーザが急増し、それに伴うオンライン会議の需要増など、クラウドサービスも利用が急拡大しました。
その結果、**本社やデータセンターにトラフィックを集約する従来のネットワーク**では、中央のネットワークデバイスがボトルネックとなり、
それによる通信品質の低下を回避するためのセキュリティ管理外のインターネットアクセスが増加するなど、
ユーザエクスペリエンス、セキュリティ、可視化などの管理性を含む、**さまざまな観点で問題が発生**しています。

さらにパンデミックの収束後に予想されるのは、元の状態への回帰ではなく、**ハイブリッドワークなど自由な働き方へのシフト**です。
つまり、現在の問題は決して一過性のものではなく、**継続的に取り組むべき課題**として、たとえば次のように認識する必要があります。

社内外を問わず、どこからでも、
どこへでも、快適にアクセスできる

社内外を問わず、どこからのアクセスでも、
どこへのアクセスでも、安全に制御できる

社内外を問わず、どこからのアクセスでも、
どこへのアクセスでも、可視化して管理できる

――これらの課題をまとめて解決できるだけでなく、段階的に導入できるソリューションが、Cisco SASE です――

いま SASE が求められる理由

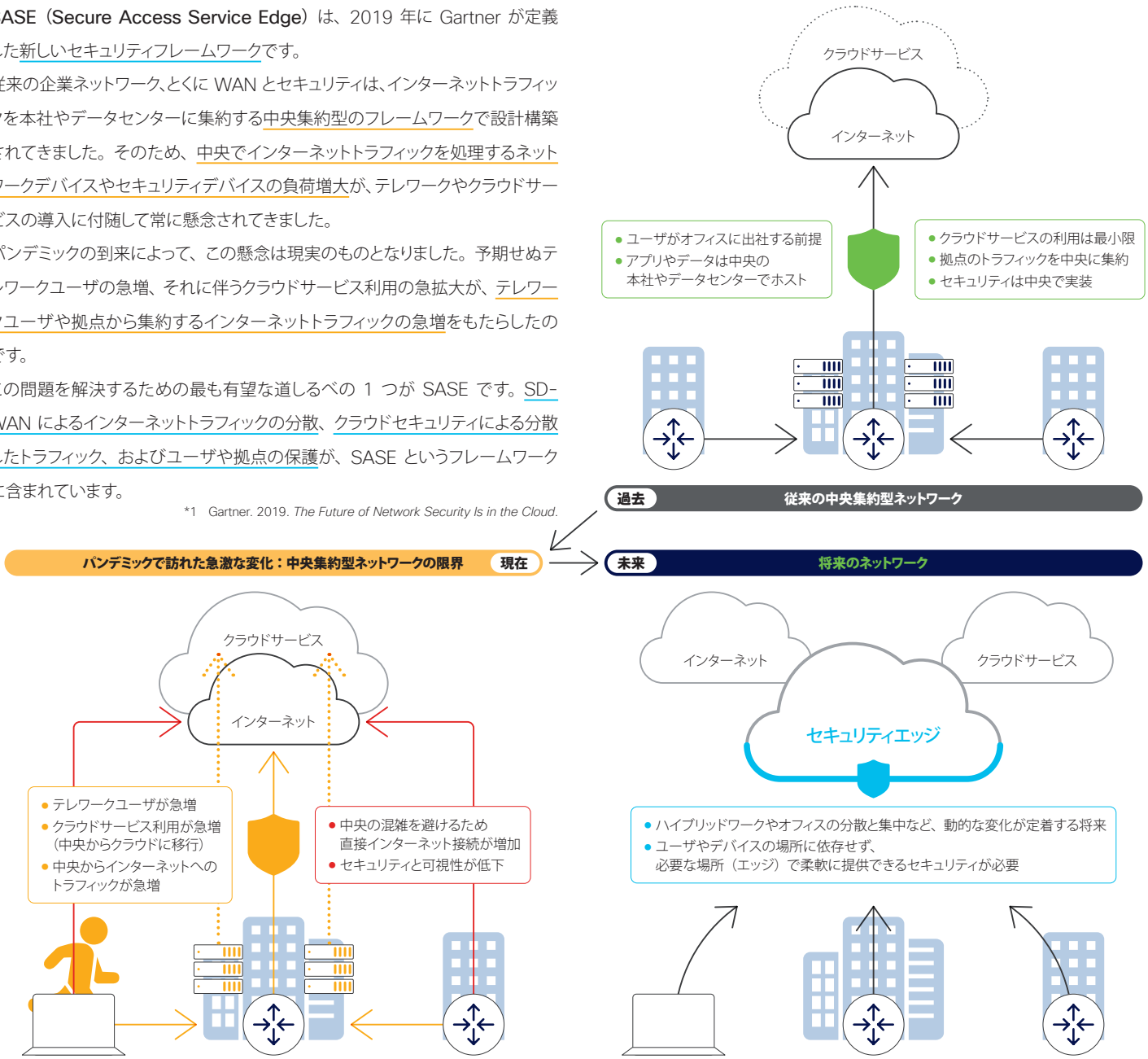
SASE（Secure Access Service Edge）は、2019 年に Gartner が定義した新しいセキュリティフレームワークです。

従来の企業ネットワーク、とくに WAN とセキュリティは、インターネットトラフィックを本社やデータセンターに集約する中央集約型のフレームワークで設計構築されてきました。そのため、中央でインターネットトラフィックを処理するネットワークデバイスやセキュリティデバイスの負荷増大が、テレワークやクラウドサービスの導入に付随して常に懸念されてきました。

パンデミックの到来によって、この懸念は現実のものとなりました。予期せぬテレワークユーザの急増、それに伴うクラウドサービス利用の急拡大が、テレワークユーザや拠点から集約するインターネットトラフィックの急増をもたらしたのです。

この問題を解決するための最も有望な道しるべの 1 つが SASE です。SD-WAN によるインターネットトラフィックの分散、クラウドセキュリティによる分散したトラフィック、およびユーザや拠点の保護が、SASE というフレームワークに含まれています。

*1　Gartner. 2019. *The Future of Network Security Is in the Cloud.*



Cisco SASE フレームワーク & コンポーネント

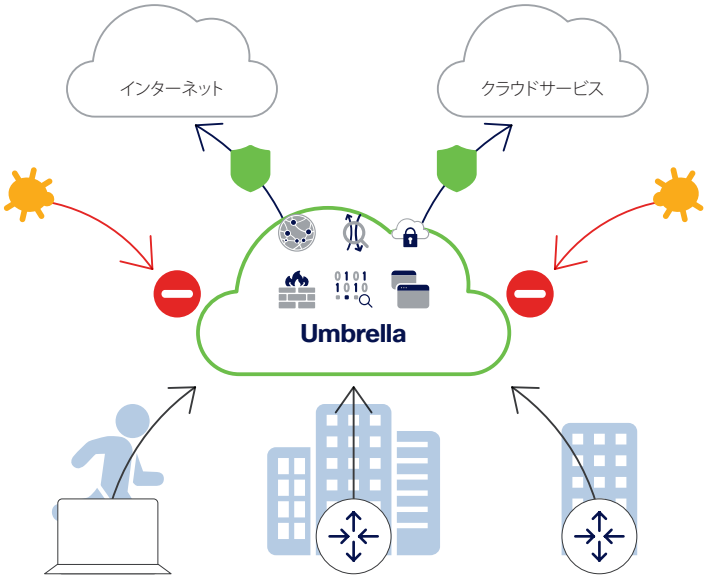
Cisco SASE は、Gartner 社が定義した*1「**包括的な WAN 機能と包括的なセキュリティ機能を組み合わせた新しいサービス**」を発展させた、次のようなフレームワークとコンポーネントで構成されます。

*1　Gartner. 2019. *The Future of Network Security Is in the Cloud.*

Cisco Umbrella

Cisco Umbrella は、Cisco SASE の中核となるクラウドセキュリティです。テレワークや拠点などユーザやデバイスの場所を問わず、インターネットやクラウドサービスへのアクセスを保護する**セキュア インターネットゲートウェイ**［Secure Internet Gateway（SIG）］として機能します。単一のクラウドダッシュボードで一元管理できる、次のようなセキュリティサービスを提供します。

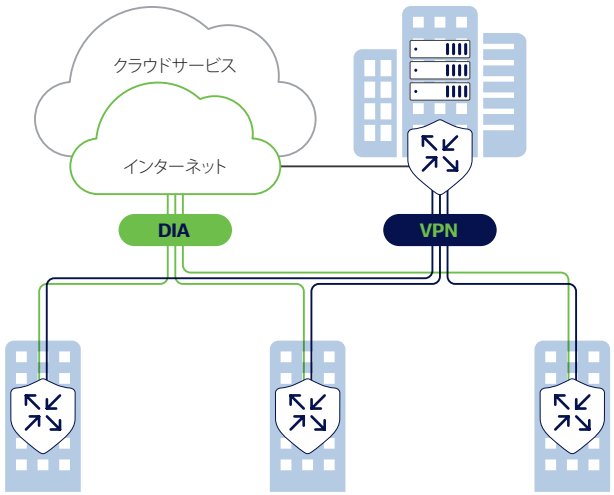
- DNS レイヤセキュリティ
- セキュア Web ゲートウェイ（SWG）
- クラウドアプリセキュリティ制御（CASB）およびクラウドマルウェア検知 / 除去
- レイヤ 7 アプリおよび侵入防御システム対応クラウド提供型ファイアウォール
- データ漏洩防止（DLP）
- リモートブラウザ分離（RBI）



Cisco SD-WAN

拠点の場所や数、利用可能な回線を問わず、インターネットやクラウドサービス、データセンターなど、あらゆるアプリケーションやデータへの接続を最適化する SD-WAN（Software-Defined WAN；ソフトウェア定義型 WAN）。Meraki MX と**シスコ ルータ**（**エッジプラットフォーム**）の 2 つのプラットフォームから選択できる Cisco SD-WAN には、次のような共通の特長があります。

- **一元管理**：Meraki MX はクラウドベースのダッシュボード、シスコ ルータ（エッジプラットフォーム）はクラウドまたはオンプレミスベースのコントローラ（ダッシュボード）で一元管理可能
- **ゼロタッチプロビジョニング**：拠点の新設や移設に伴う設置場所での設定作業が不要、ハードウェアをつなぐだけで OK
- **インテリジェントな WAN 回線（通信経路）利用**：アプリケーション別に使用する WAN 回線（光回線かモバイル回線か）や通信経路［直接インターネット接続（DIA）か VPN か］を指定できるだけでなく、通信品質などに応じた自動選択もサポート
- **ビルトインセキュリティとクラウドセキュリティ**：侵入防御システムやコンテンツフィルタリング、高度なマルウェア防御など、ハードウェアにビルトインされたセキュリティサービスを利用できるだけでなく、クラウドセキュリティ Cisco Umbrella を統合可能

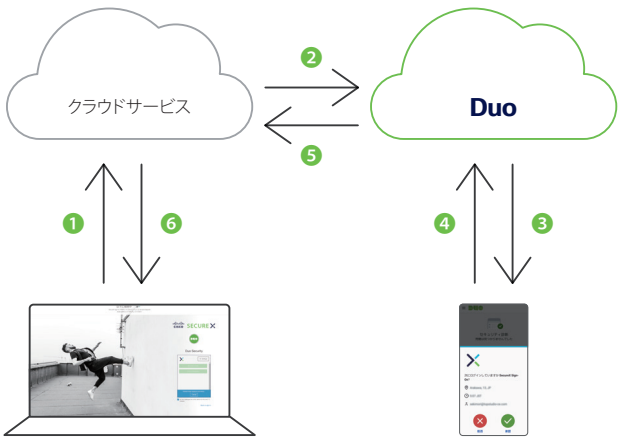


SD-WAN によるインテリジェントな WAN 回線（通信経路）利用
例：本社（データセンター）のサーバや特定のクラウドサービスは VPN 経由
その他のクラウドサービスは直接インターネット接続（DIA）

Cisco Secure Access by Duo

テレワークの推進やクラウドサービスの利用拡大に伴い、アプリケーションやデータ、ネットワークにアクセスしようとしているユーザが「**本人である**」という信頼性を確立することが、ますます重要になっています。Cisco Secure Access by Duo は、この信頼性を**多要素認証（Multi-Factor Authentication；MFA）**によって確保するクラウドベースのセキュリティサービスです。

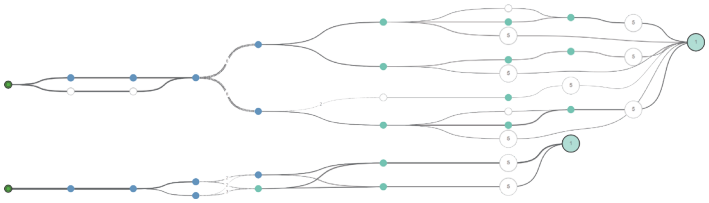
ユーザの多要素認証だけでなく、デバイスのセキュリティ健全性など、さまざまな条件に基づく柔軟なアクセスポリシーもサポート。ユーザの場所移動、BYOD を含むマルチデバイス利用など、ハイブリッドワークでは不可避となる多様なセキュリティコンテキストに対応できます。



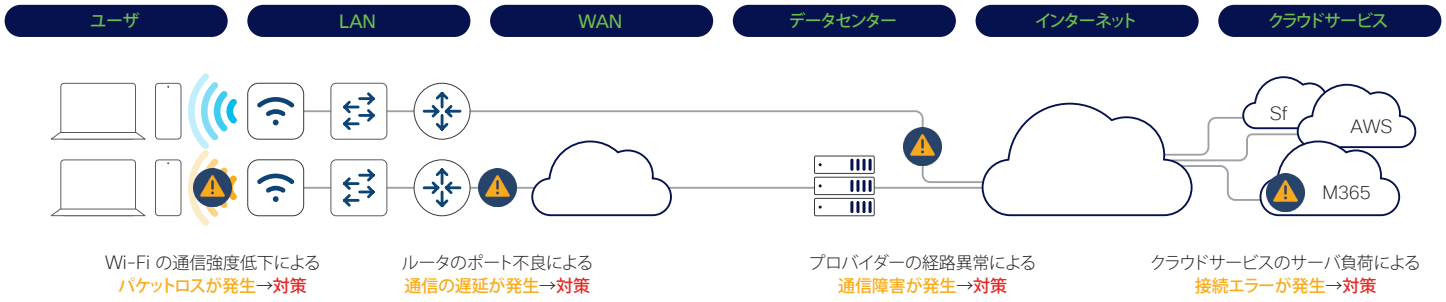
1. 実際にクラウドサービスを使用するデバイスで 1 つ目の認証
2. Duo に 2 つ目の認証要求を送信
3. 認証デバイスに 2 つ目の認証を要求（プッシュ通知）
4. 認証デバイスで 2 つ目の認証（プッシュ通知に応答）
5. クラウドサービスに 2 つ目の認証成功を送信
6. アクセスを許可

Cisco ThousandEyes

Cisco ThousandEyes は、SASE を補完する「**オブザーバビリティ（可観測性）**」ソリューションです。自社管理ではないネットワークも含めたあらゆるネットワークにわたって、アプリケーション パフォーマンスなどユーザエクスペリエンスに影響を及ぼすあらゆる要素を可視化するだけでなく、パフォーマンス低下や接続障害の原因などのインシデントに対策するための実用的なインサイトを提供します。



ThousandEyes で見える世界
例：パスの可視化



Cisco SASE バンドル

Cisco SASE は、4 つの製品カテゴリの一部から段階的に導入する、スモールスタートが可能です。

2 つ以上の製品カテゴリからまとめて導入する場合は、お得なディスカウント価格で購入できる **Cisco SASE バンドル**を推奨します。

Umbrella

- サブスクリプション ライセンス
  - Umbrella SIG Essentials
  - Umbrella SIG Advantage
- アドオン サブスクリプション ライセンス
  - レイヤ 7 アプリ対応 クラウド提供型ファイアウォール *1
  - インライン DLP（データ漏洩防止）*1
  - リモートブラウザ分離 (Isolate Risky)
  - リモートブラウザ分離 (Isolate Web Apps)
  - リモートブラウザ分離 (Isolate Any)

SD-WAN

Powered by Meraki

- ハードウェア
  - Meraki MX
  - Meraki Z
- サブスクリプション ライセンス
  - Enterprise
  - Advanced Security
  - Secure SD-WAN Plus
  - Insight

Powered by IOS XE

- ハードウェア
  - ISR 1000 シリーズ *2
  - Catalyst 8000 シリーズ *3
- サブスクリプション ライセンス
  - Cisco DNA Essentials
  - Cisco DNA Advantage

Secure Access by Duo

- サブスクリプション ライセンス
  - MFA
  - Access
  - Beyond

ThousandEyes

- サブスクリプション ライセンス
  - クラウド & エンタープライズ エージェント
  - エンドユーザモニタリング
  - インターネットインサイト

Ciosco SASE の詳細は、Web サイトをご覧ください。

WEB www.cisco.com/jp/go/sase

*1　Umbrella SIG Essentials 用アドオン（Umbrella SIG Advantage ではデフォルトでサポート）。
*2　バンドル対象は一部の製品モデル（Viptela OS モデルも選択可能）。*3　バンドル対象は一部の製品モデル。

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
cisco.com/jp/go/vdc_callback

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

2281-2111-000-TO