Cisco Umbrella

SASE をシンプルに実現する セキュア インターネット ゲートウェイ

Cisco Umbrella は、インターネット上の脅威を防御するための最前線として機能する
セキュア インターネット ゲートウェイ（Secure Internet Gateway；SIG）です。
DNS レイヤのセキュリティをベースに、セキュア Web ゲートウェイ（SWG）、クラウドアクセスセキュリティ制御（CASB）、
クラウド提供型ファイアウォール（CDFW）、データ漏洩防止（DLP）、リモートブラウザ分離（RBI）、
さらに脅威インテリジェンスも含めた幅広いセキュリティサービスを、単一のクラウドセキュリティとして提供します。

簡単に導入できる クラウドセキュリティ

クラウドで提供するセキュリティサービスだから
専用のハードウェアが不要で導入が簡単
メンテナンス不要で最新の脅威に対応可能

テレワークや ハイブリッドワークに最適

インターネット利用に欠かせない
DNS レイヤで提供するセキュリティだから
場所を問わずあらゆるユーザーを保護可能

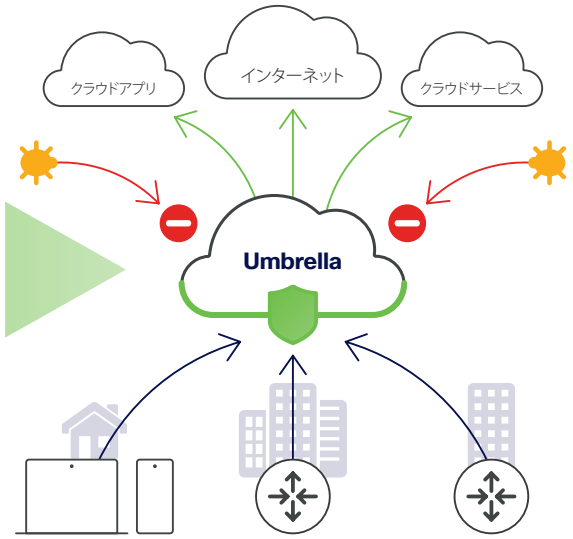
SASE を実現する 最もシンプルな出発点

ユーザーやデバイスの場所に制約されずに
フレキシブルに展開できるセキュリティだから
SASE を実現する出発点として最適

Cisco Umbrella の概要と特長

Cisco Umbrella とは

Cisco Umbrella は、インターネット上の脅威を防御するための最前線として機能するセキュア インターネット ゲートウェイ（Secure Internet Gateway;SIG）です。次のような幅広いセキュリティサービスを、一元管理できる単一のセキュリティ製品としてクラウドで提供します。



インターネット利用に欠かせない DNS レイヤのセキュリティをベースにしているため、場所を問わず、インターネットに接続するあらゆるネットワークやデバイスに適用可能。国内外を問わず、あらゆる拠点、および社内外を問わず、あらゆるユーザーを保護できます。

高速かつ高信頼、業界 No.1 のセキュリティ効果を誇るクラウドセキュリティサービス

グローバルに展開する Cisco Umbrella のクラウド（データセンター）は、1,000 以上のパートナー組織と提携して 6,000 以上のピアリングセッションを確立。ホップ数を削減し、遅延を短縮することで、これらのパートナー組織が提供するクラウドアプリやサービスへのアクセスパフォーマンスを向上させています。独立した調査会社によるテストでは、インターネットへの直接接続に比べて最大で 33% のパフォーマンス向上と評価されました *1。

さらに Cisco Umbrella の全データセンターは、Uptime Institute のティア 3 に準拠。堅牢な設備設計によって、DNS レイヤのセキュリティサービスは 2006 年以来、100% の稼動率で提供しています。

このような高速かつ高信頼のアーキテクチャを基盤に業界 No.1 のセキュリティ効果を実現し *2、次のような実績を積み上げています。

50 億以上
1 日に処理する Web レピュテーションリクエスト数

1 億 7,000 万以上
1 日にブロックする疑わしい DNS クエリ数

200 以上
1 年に発見する脆弱性数

1 億 300 万以上
1 日にブロックするマルウェア関連リクエスト数

5,000 万以上
1 日にブロックするフィッシング試行数

1,600 万以上
1 日にブロックするコマンド & コントロール リクエスト数

*1　参考：www.cisco.com/c/m/ja_jp/umbrella/cisco-umbrella-global-cloud-architecture.html
*2　出典：AV-TEST. ***AV-TEST Evaluates Secure Web Gateway & DNS-Layer Security Efficacy, DNS Tunneling Protection.***

設定からサポートまで日本語対応

Cisco Umbrella は、直感的に操作できるブラウザベースの管理ツール（**Cisco Umbrella ダッシュボード**）で設定管理できます。

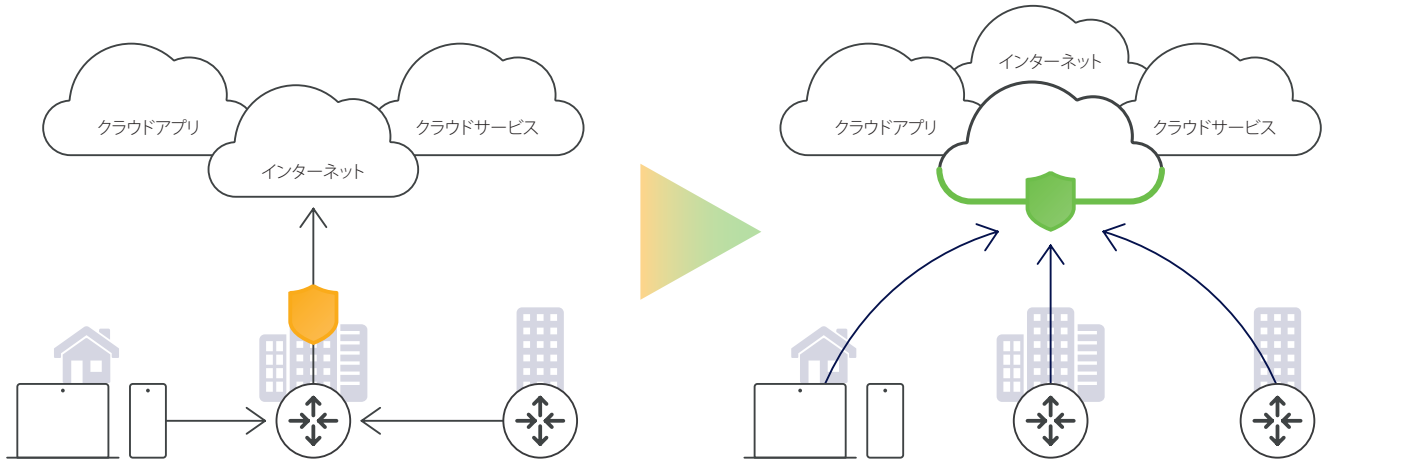
ダッシュボードに加えて、マニュアルなど各種ドキュメント、サポートも日本語に対応しています *1。

*1　新機能のユーザーインターフェイスやドキュメントは順次翻訳。

SASE のコア機能を提供

SASE とは

SASE（Secure Access Service Edge）とは、Gartner 社が「**包括的な WAN 機能と包括的なネットワークセキュリティ機能を組み合わせた新しいサービス**」と定義したセキュリティフレームワークです *1。社内外を出入りするユーザー（テレワーカー）やモバイルデバイスの増加、コワーキングスペースやタッチダウンオフィスなどの新しいオフィス環境、Microsoft 365 などのクラウドサービスの利用拡大など、新しい働き方や IT 環境に対応するために提唱されました。
SASE を実現するためのインフラ構成としては、本社やデータセンターにトラフィックを集約して境界セキュリティで保護する従来のアーキテクチャから、クラウドでネットワークとセキュリティを制御してトラフィックを集約せずに分散させたまま保護するアーキテクチャへとシフトすることが基本になります。



中央にトラフィックを集約して境界セキュリティで保護

クラウドでネットワークとセキュリティを制御してトラフィックを分散および保護

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

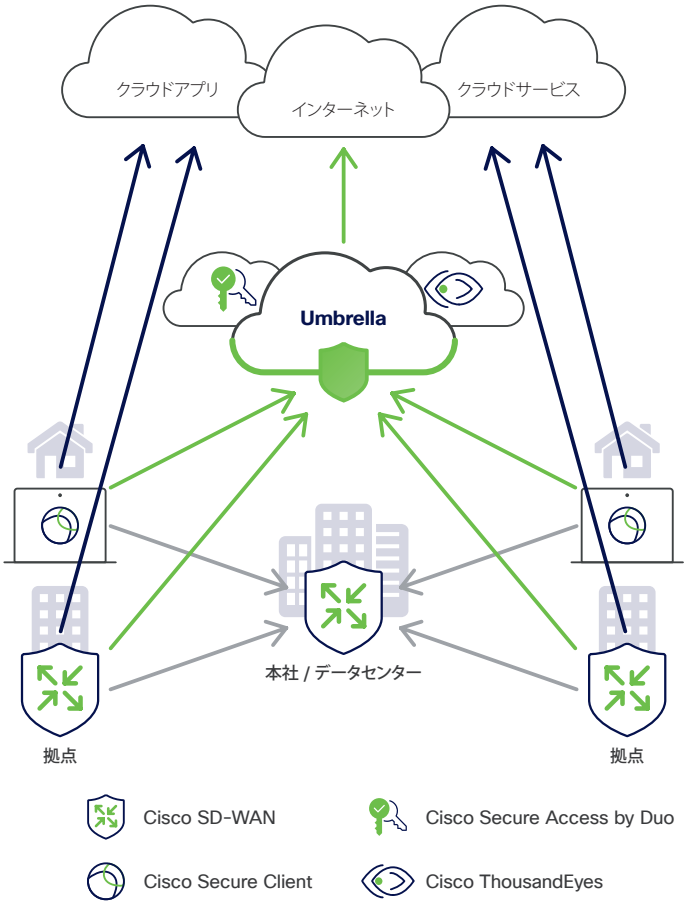
SASE の中核となる Cisco Umbrella

Gartner 社は、ユーザーエクスペリエンスを損なわずに提供すべき SASE のコア機能として次の機能を挙げていますが *1、ほとんどが Cisco Umbrella に含まれる機能です。

- SD-WAN
- **セキュア Web ゲートウェイ（SWG）** ✓
- **クラウドアクセスセキュリティ制御（CASB）** ✓
- **クラウド提供型ファイアウォール（CDFW、FWaaS）** ✓
- **機密データとマルウェアの検知** ✓
- **リモートブラウザ分離** ✓
- ゼロトラスト ネットワーク アクセス（ZTNA）

その他の機能も、Cisco SASE を構成する次のコンポーネントで提供可能です。

- **Cisco SD-WAN**（Powered by Meraki/IOS XE）
  あらゆるアプリやサービスへの接続を最適化
- **Cisco Secure Client**
  リモートアクセス VPN クライアントをベースとした
  シスコ セキュリティの統合エンドポイントエージェント
- **Cisco Secure Access by Duo**
  多要素認証でゼロトラスト ネットワーク アクセスを実現
- **Cisco ThousandEyes**
  ユーザー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
  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



Cisco SASE 接続イメージ

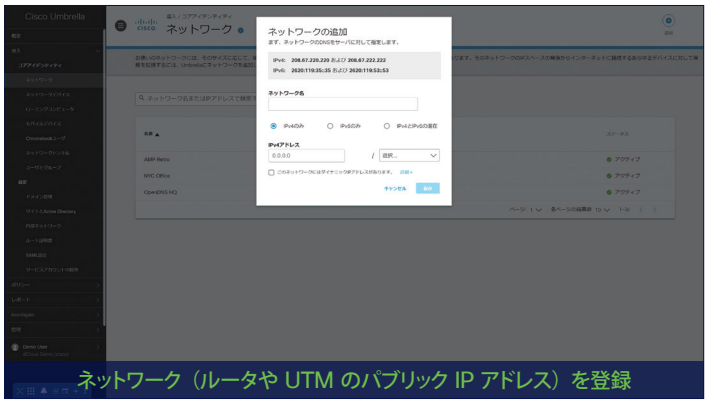
WEB Cisco SASE の詳細は、次の Web サイトをご覧ください。
www.cisco.com/jp/go/sase

*1　出典：Gartner. *2022 Strategic Roadmap for SASE Convergence.*

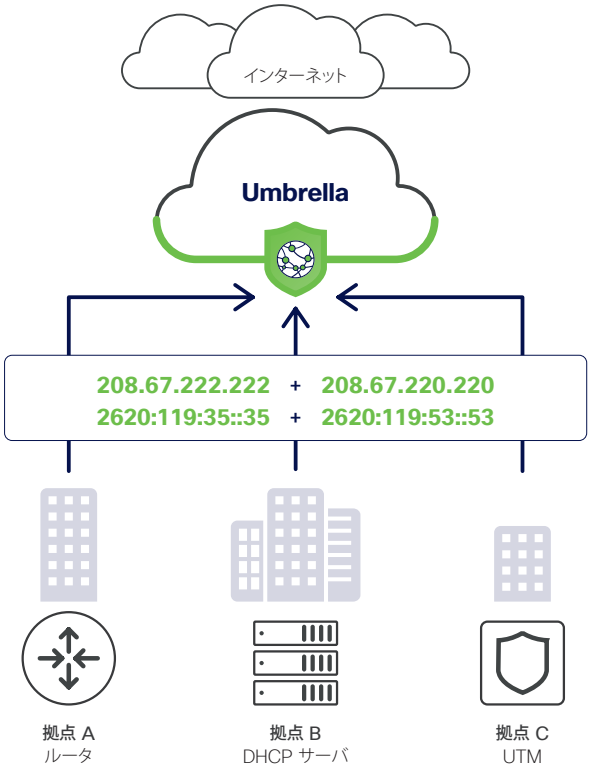
Cisco Umbrella だからできる！利用シーン

既存の環境はそのままに、全社に簡単かつ迅速に導入したい

クラウドで提供するセキュリティサービスであるため、専用のハードウェアが不要です。各サービスのベースとなる DNS レイヤセキュリティの場合は、各拠点の DHCP サーバやルータ、UTM の DNS 設定を変更して、Umbrella ダッシュボードに IP アドレスを登録するだけで OK。わずか数分で導入できます。導入後の運用管理もきわめてシンプルで、国内外に散らばる拠点（ネットワーク）やネットワークデバイス、およびユーザーデバイスのインターネット アクセス セキュリティを Umbrella ダッシュボードで一元管理することができます。



ネットワーク（ルータや UTM のパブリック IP アドレス）を登録



ネットワークデバイスに Umbrella の DNS を設定

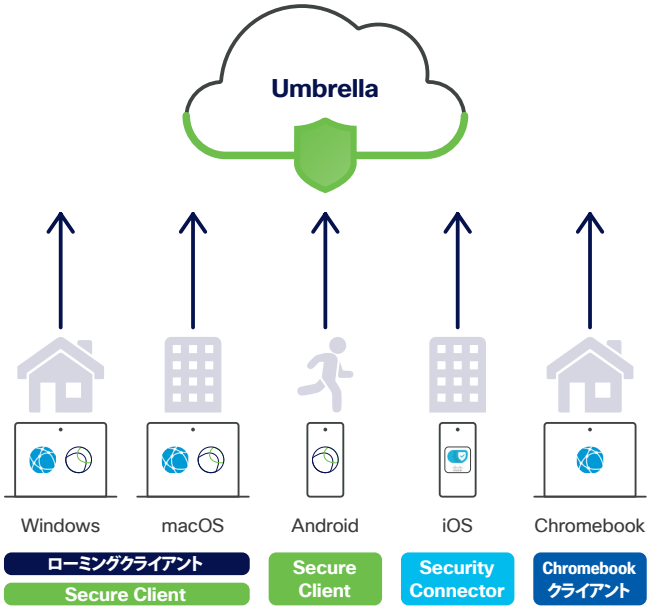
テレワークユーザーを VPN なしで手軽に保護したい

テレワークの普及によって、オフィス外で働くユーザーを保護することがかつてないほど重要に、そして困難になっています。テレワークユーザーを保護するための代表的な手段である VPN では、同じくすっかり普及した Microsoft 365 などのクラウドアプリの利用時にパフォーマンスが低下しがちという問題を抱えるからです。

Cisco Umbrella なら VPN なしで、しかもパフォーマンスを犠牲にせずにテレワークユーザーを保護できます。

専用のクライアントソフトウェアである **Cisco Umbrella Roaming Client** なら、Windows および macOS PC にインストールするだけで DNS レイヤのセキュリティで保護可能。シスコ セキュリティの統合エンドポイントエージェントである **Cisco Secure Client** なら、セキュア Web ゲートウェイ（Secure Web Gateway；SWG）による追加の保護も可能です。

また、その他にも Chromebook やスマートフォンなど、さまざまなユーザーデバイスを保護することができます。

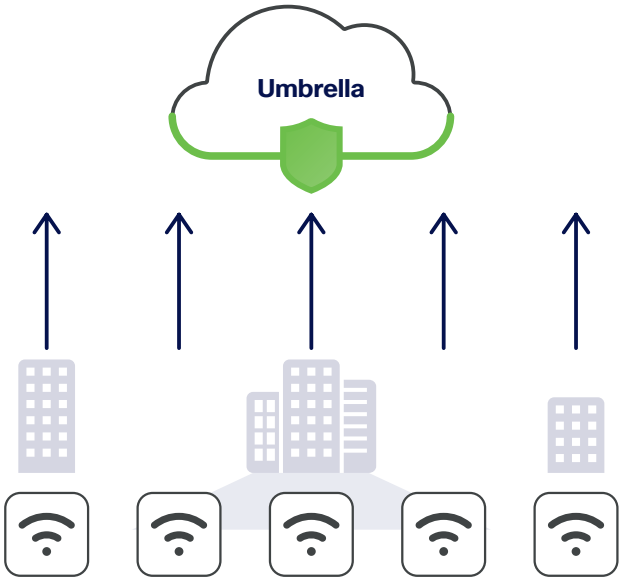


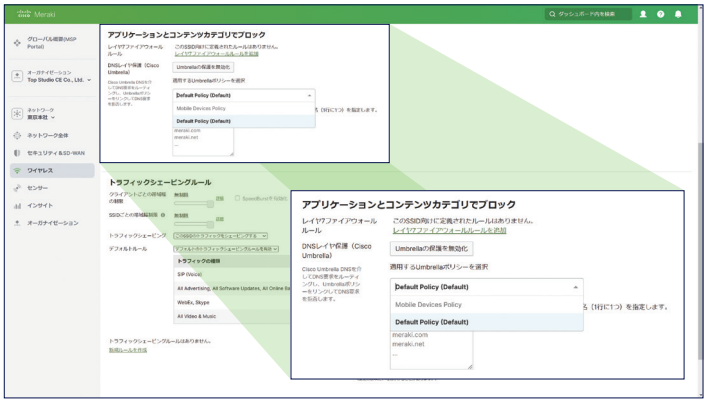
Secure Client のユーザーインターフェイス
VPN クライアントソフトウェア
AnyConnect をベースに
エンドポイントセキュリティ
Secure Endpoint など
シスコのセキュリティを統合可能

Wi-Fi セキュリティを手軽に強化したい

社員や顧客など、エンドユーザーのネットワーク接続が Wi-Fi メインの場合、Cisco Umbrella を導入する最もシンプルでコストパフォーマンスが高い選択肢が **Cisco Umbrella WLAN パッケージ**です。ワイヤレスアクセスポイント 5 台分のライセンス数から購入可能で、アクセスポイントに接続するユーザー数の制限なく、DNS レイヤのセキュリティで保護できます。

また、**Cisco Meraki MR クラウド管理型ワイヤレスアクセスポイント**、および **Cisco Catalyst 9100 シリーズ ワイヤレスアクセスポイント**の組み込みコントローラ（**EWC**）を含む **Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ**は、Cisco Umbrella と管理ツールレベルで統合可能です。たとえば、Meraki ダッシュボードから直接、SSID や既存のグループポリシーに Umbrella の DNS ポリシーを適用できます。





Meraki ダッシュボード
API で Umbrella と統合、「社内用」「ゲスト用」などの SSID 別に DNS ポリシーを設定可能

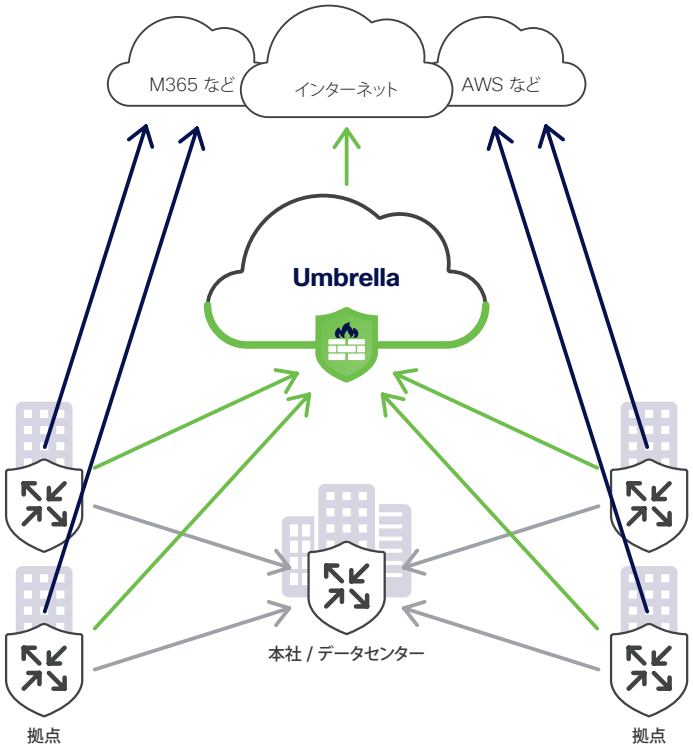
セキュリティをしっかり確保してローカルブレイクアウトを導入したい

Microsoft 365 などのクラウドアプリやサービスの利用拡大に伴って、拠点からのインターネットアクセスを本社やデータセンターに集約しない、ローカルブレイクアウト［または直接インターネットアクセス（Direct Internet Access；DIA）］の導入も拡大しています。

ローカルブレイクアウトにはアプリパフォーマンスやサービス品質の低下を避けられるメリットがある一方で、セキュリティを確保するためにコストがかかるなどのデメリットもあります。たとえば、各拠点に UTM を追加するようなハードウェアベースの対策では、ハードウェアの購入や保守に伴うコスト、運用に伴う管理者の手配や負担など、さまざまな課題が発生します。

Cisco Umbrella の DNS レイヤセキュリティなら、このような課題に悩まされることなく、シンプルかつ低コストで各拠点からのインターネット アクセス セキュリティを強化できます。

また、**Cisco Umbrella SIG** なら、セキュア Web ゲートウェイやクラウド提供型ファイアウォール（Cloud-Delivered FireWall；CDFW）など、各拠点からのインターネットアクセスに必要なセキュリティをまとめて導入できます。

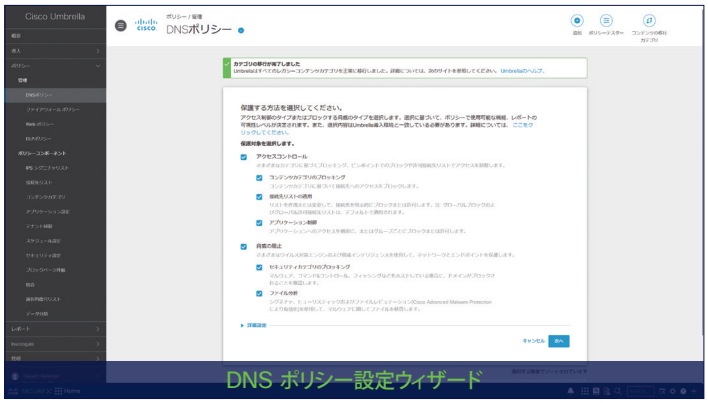


各拠点から特定アプリ / サービスには直接接続
それ以外のインターネットには Umbrella 経由で接続
本社 / データセンターには VPN 接続

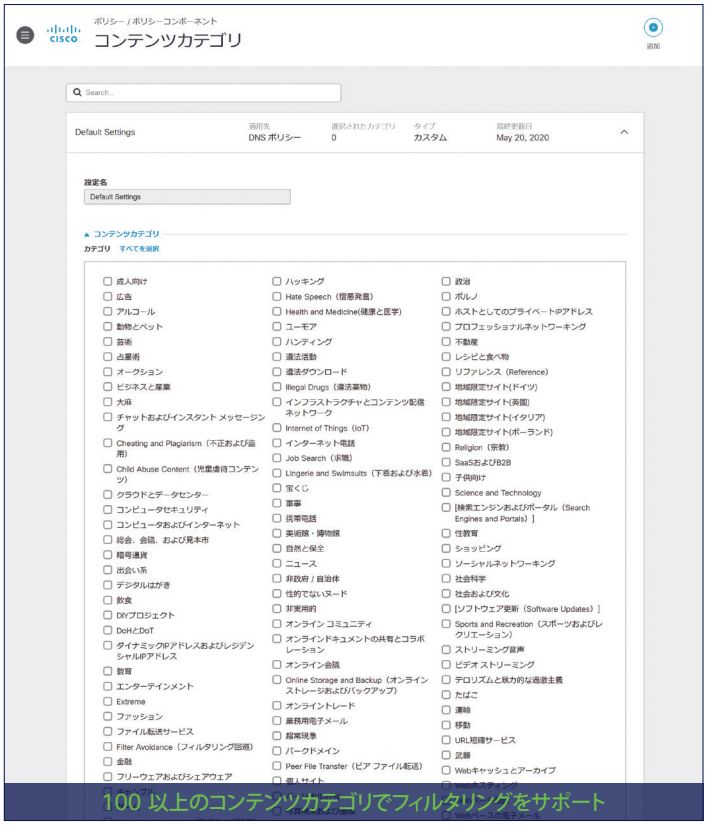
インターネット アクセス ポリシーを柔軟に設定したい

オフィスネットワークの社員用やゲスト用、テレワークユーザー用など、保護対象に応じて柔軟にポリシーを設定してインターネットアクセスを制御できます。たとえば、次のようなきめ細やかな設定が可能です。

- マルウェアやフィッシングなど、危険な Web サイトへのアクセスをブロック
- 特定のコンテンツを含む Web サイト（コンテンツカテゴリ）へのアクセスをブロック（フィルタリング）
- 特定のアプリやアプリカテゴリへのアクセスを許可 / ブロック
- 特定の接続先へのアクセスを許可 / ブロック
- 危険なファイルのダウンロードをブロック



DNS ポリシー設定ウィザード



100 以上のコンテンツカテゴリでフィルタリングをサポート

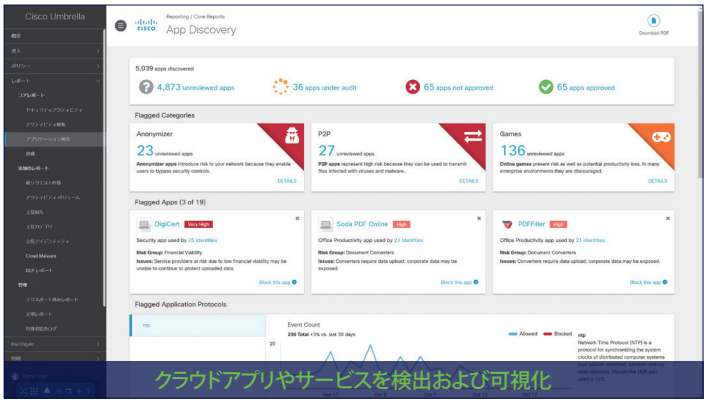
クラウドアプリやサービスの利用を可視化して制御したい

クラウドアプリやサービスの利用拡大に伴って、組織として関知していない、あるいは許可していない利用もまた増加し、セキュリティやコンプライアンス上のリスクとなっています。

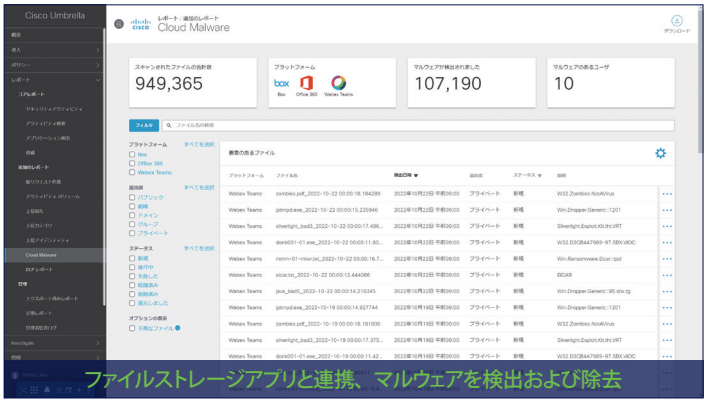
Cisco Umbrella では、クラウドアプリやサービスの可視化と制御もサポート。次のような対策ができるようになります。

- 各クラウドアプリやサービスのリスクレベルを評価する
- リスクが高いクラウドアプリやサービスを特定する
- クラウドアプリやサービスのベンダーの信頼度を確認する
- クラウドアプリやサービスの利用を個別またはカテゴリ別に許可 / ブロックする
- クラウドアプリやサービスのユーザー操作を制御する（アップロードやファイル添付、投稿の禁止など）

さらに Webex や Microsoft 365 など特定のプラットフォーム（ファイルストレージアプリ）に関しては、ファイルをスキャンしてマルウェアを検出および除去する機能も提供します。



クラウドアプリやサービスを検出および可視化



ファイルストレージアプリと連携、マルウェアを検出および除去

常に最新のセキュリティを適用したい

セキュリティ製品を選定するにあたっては、それらが利用するデータベースの規模や、データを分析して実効性のある知見を蓄積するインテリジェンスの有無が重要な判断基準となります。これらが、サイバー攻撃など脅威の検知率、あるいは誤検知率のような指標を左右するからです。

Cisco Umbrella が使用するデータベースには **Cisco Talos** による知見がリアルタイムで反映されるため、常に最新かつ最先端のデータベースによってインターネットアクセスを保護できます。

Cisco Talos は、最先端のセキュリティ調査能力を持つ、世界最大の研究機関の 1 つです。Cisco Talos の強みは、脅威の全体像を捉えて進行中の事態を把握し、データに基づいて適切な知見を得られることです。データサイエンティストやエンジニアなど、シスコが誇る最強の専門家たちが日々、新旧のマルウェアサンプルなど膨大な脅威情報を分析し、未知の脅威に対しても迅速に、かつ正確な知見を積み重ねています。

6,250 億
1 日に分析する Web リクエスト数

200 以上
1 年に発見する脆弱性数

140 万以上
1 日に分析する新マルウェアサンプル数

300 億
1 日に分析する端末イベント数

84 万
保護するネットワーク数

6,700 万
保護するメールボックス数

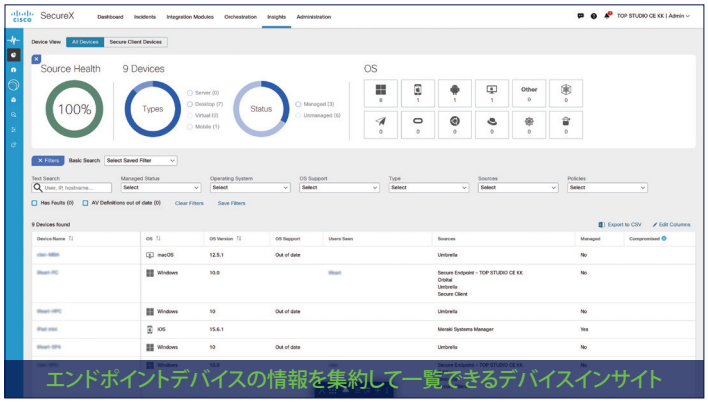
8,700 万
保護する端末数

他のセキュリティ製品と連携させたい

Cisco Umbrella を契約すると、シスコの各種セキュリティ製品やサードパーティ製品と連携して情報を集約する統合プラットフォーム **Cisco SecureX** を無料で利用することができます。より広範かつ詳細な可視化と優れた自動化によって、脅威の迅速な検知、調査、対応を実現する XDR（Extended Detection & Response）製品です。

また、Cisco SecureX は、連携製品から得られた情報によるエンドポイントデバイスのインベントリ管理や、**Cisco Secure Client** インストーラのカスタマイズもサポートします *1。


各種セキュリティ製品の情報を集約して一覧できるダッシュボード


エンドポイントデバイスの情報を集約して一覧できるデバイスインサイト


Secure Client インストーラをカスタマイズして作成可能 *1

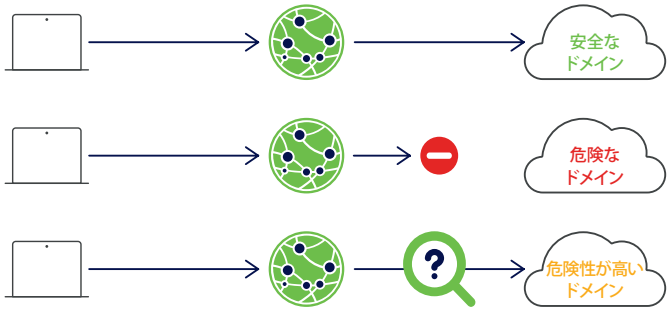
*1　2022 年 10 月現在、Windows 10/11 用インストーラをサポート。

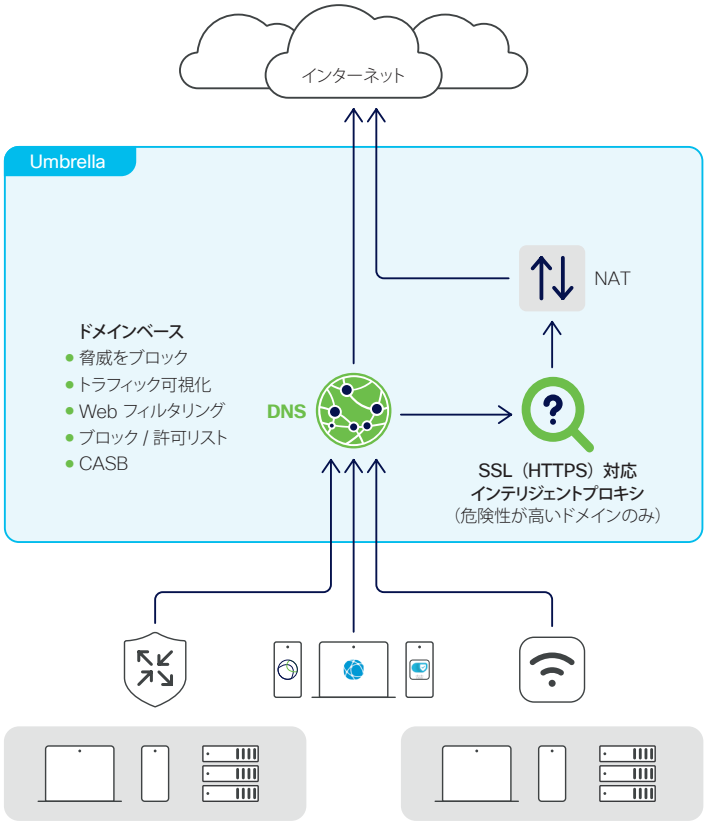
Cisco Umbrella 機能紹介

DNS レイヤセキュリティ

インターネット利用に欠かせない DNS のメカニズムを利用した、Cisco Umbrella のベースとなるセキュリティです。一般的な DNS は、ユーザーがある Web サイトを閲覧する場合に、その Web サイト（ドメイン名）に対応した IP アドレスを応答する役割を担っています。Cisco Umbrella の DNS は 1 日あたり約 6,000 億もの DNS リクエストを処理しますが、その統計 / 分析情報から特定のドメイン名が危険かどうかを判定し、危険な場合には IP アドレスを応答しないことで、危険な Web サイトへの接続をブロックします。

また、ドメインベースの Web トラフィック可視化、Web フィルタリング、ブロック / 許可リスト、およびクラウドアプリの検出とブロック（**CASB**）をサポートするほか、危険性が高いドメインへの接続ではプロキシを経由して（**インテリジェントプロキシ**）、Web トラフィックやファイルの検査とブロックもサポートします。

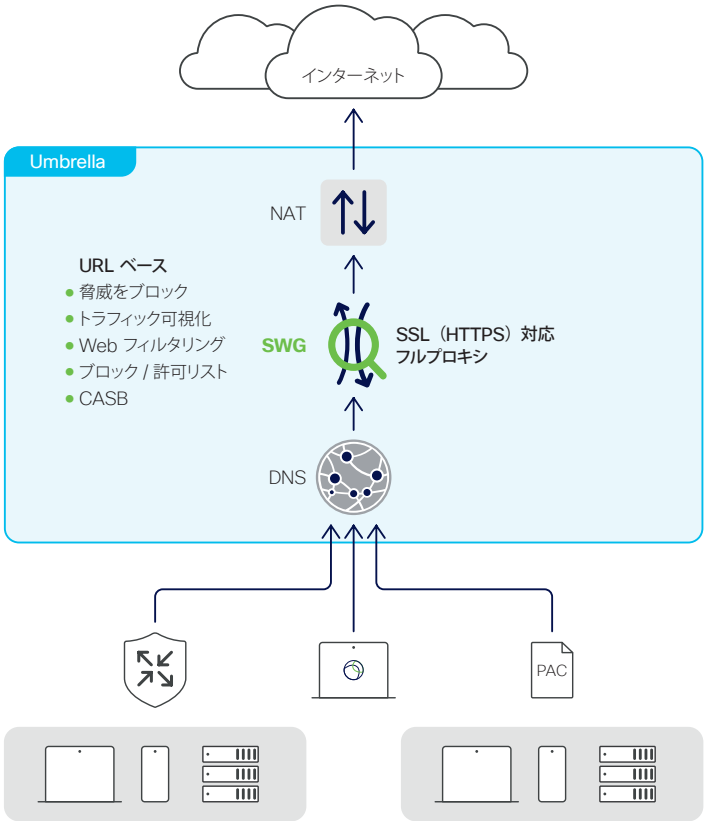




セキュア Web ゲートウェイ（Secure Web Gateway；SWG）

プロキシ経由で全 Web トラフィックを検査することで（**フルプロキシ**）、ドメインベースの DNS レイヤセキュリティよりも詳細な URL ベースでの保護、可視化、および制御を実現します。

- URL ベースで Web トラフィックを可視化
- URL ベースで Web フィルタリング
- URL ベースでブロック / 許可リストをカスタマイズ可能
- URL ベースでクラウドアプリを検出およびブロック（CASB）
- アップロードやファイル添付、投稿の禁止など、一部のクラウドアプリではユーザー操作を制御可能
- すべてのファイルを検査およびブロック
- Cisco Secure Malware Analytics（クラウドサンドボックス）によるファイル分析をサポート
- ファイル種別に応じてブロック
- ドメインおよびアプリケーションベースで SSL（HTTPS）検査から除外可能



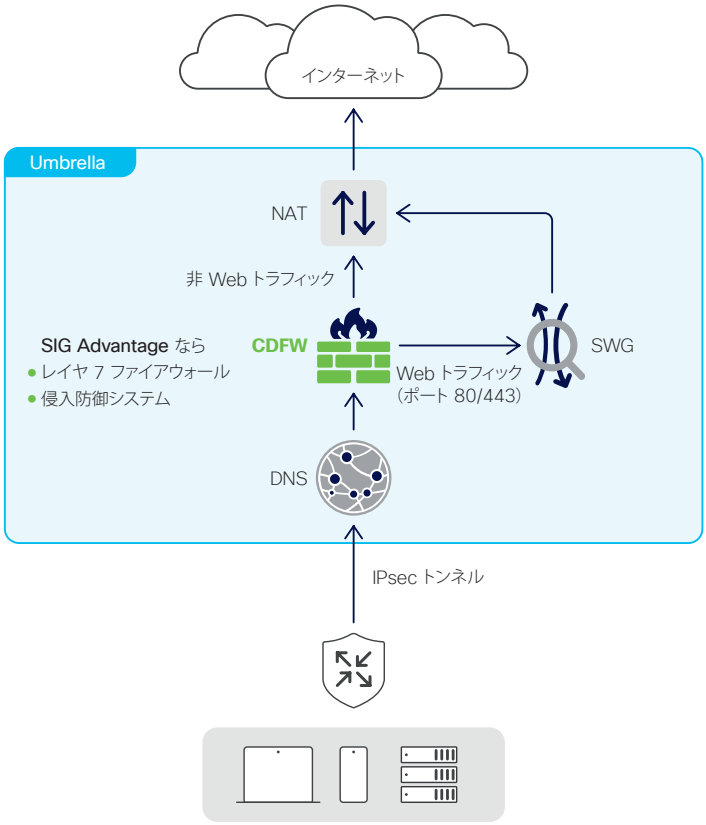
クラウド提供型ファイアウォール（Cloud-Delivered FireWall；CDFW）

インターネット送信に使用するポートとプロトコルを可視化および制御するレイヤ 3 & 4 ファイアウォールに加えて、Umbrella SIG Advantage ではアプリを可視化および制御するレイヤ 7 ファイアウォール、さらに侵入防御システム（Intrusion Prevention System；IPS）もサポートします。

- クラウドベースではない約 2,800 のアプリを可視化（継続的に追加）
- Snort 3 IPS、40,000 以上の膨大なシグネチャを使用（Cisco Talos から継続的に追加）
- 不必要なトラフィックや望ましくないトラフィックを、ポート、プロトコル、さらにアプリおよび IPS ベースのポリシーで制御（許可 / ブロック）

クラウド提供型ファイアウォールを使用するためには、Cisco Secure Firewall や Cisco Meraki MX、Cisco ISR、Cisco Catalyst 8000 など、IPsec 対応デバイスとのトンネル設定が必要になります。

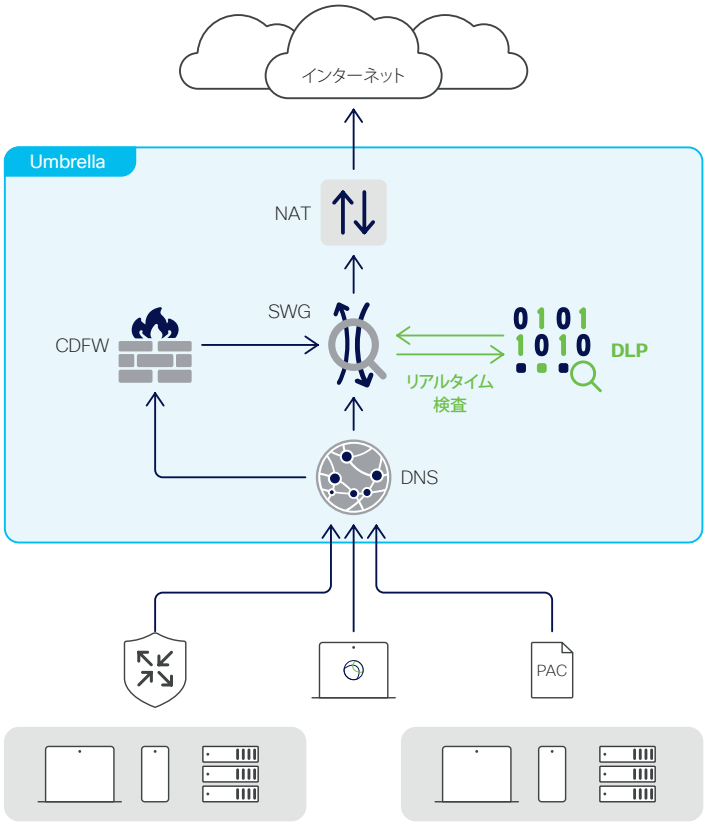
Cisco SD-WAN（Powered by IOS XE）および Cisco Meraki MX では、API 連携によって Umbrella クラウドとのトンネルを簡単に確立できます。

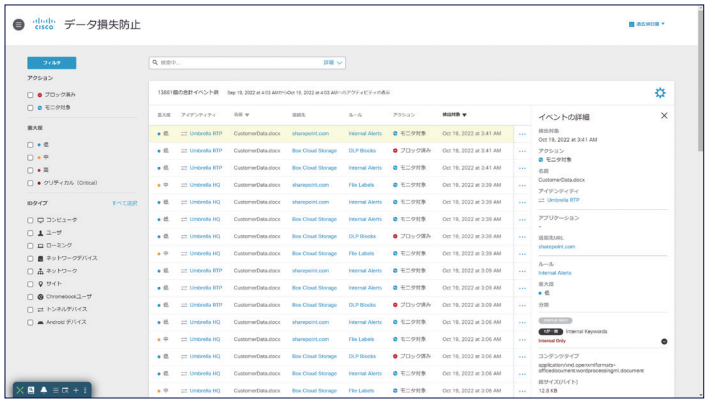


データ漏洩防止（Data Loss Prevention；DLP）

セキュア Web ゲートウェイと連携して Web トラフィックをリアルタイムで検査し、機密データの有無をモニタリング、および機密データが流出する前にブロックします。

- PII、PCI、PHI を含む 80 以上の機密データ識別子を利用可能（しきい値や近接度の設定によって、誤認識を軽減可能）
- 任意のキーワードやパターンなど、ユーザー定義の辞書を作成可能
- 特定のアイデンティティや宛先に適用するなど、カスタマイズ可能なポリシー
- インライン DLP と API ベース DLP を単一のダッシュボードで管理可能
- SSL（HTTPS）トラフィック対応
- 機密データを含むトラフィック（イベント）関する詳細なレポートを利用可能

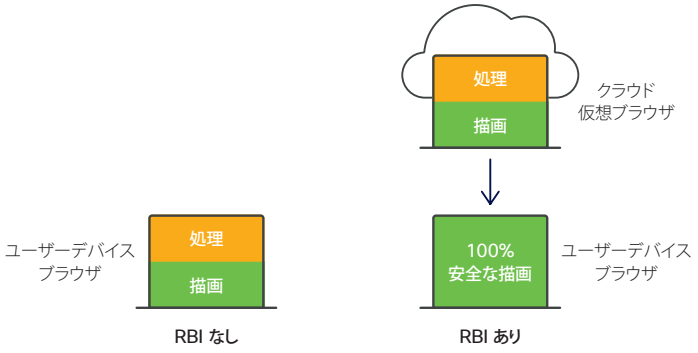


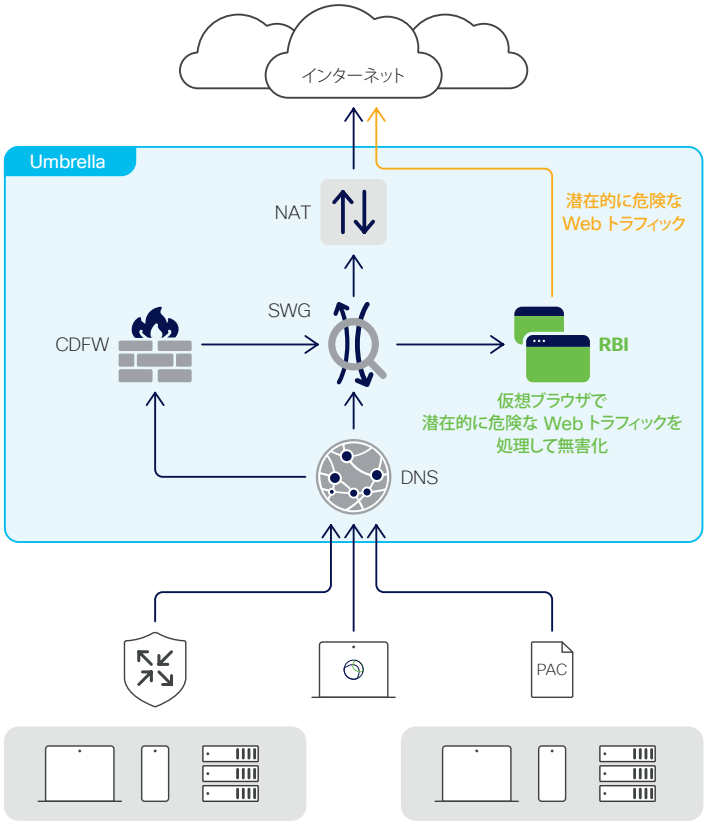


リモートブラウザ分離（Remote Browser Isolation；RBI）

プログラムの実行などのブラウザ機能をユーザーデバイスから切り離されたクラウドの仮想ブラウザで提供することで、潜在的に危険な Web トラフィックを無害化してユーザーを保護します。次の 3 つのオプションから選択できます。

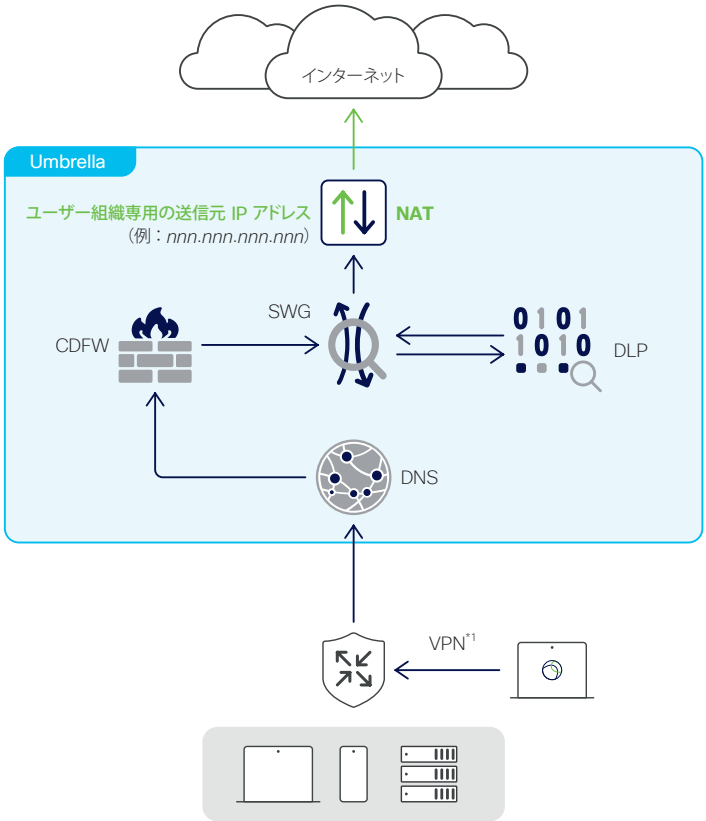
- **Isolate Risky**
  未分類、または潜在的に危険なカテゴリの Web サイトへのブラウザアクセスをユーザーデバイスから分離
- **Isolate Web Apps**
  Box や Slack、Gmail など特定のアプリ、または SNS やファイルストレージなど特定カテゴリのアプリへのブラウザアクセスをユーザーデバイスから分離
- **Isolate Any**
  任意の宛先（ドメイン、URL、IP アドレス）、任意のカテゴリの Web サイト、任意のアプリへのブラウザアクセスをユーザーデバイスから分離





ユーザー組織専用の送信元 IP アドレス NEW

Cisco Umbrella SIG では、全ユーザー組織共用の送信元 IP アドレスを使用します。この IP アドレスは一定の範囲で可変するため、Microsoft 365 などのクラウドアプリやサービス側で厳格な送信元 IP アドレス制限を必要とする組織向けに、組織専用の送信元 IP アドレスもオプションで提供します。
組織専用の送信元 IP アドレスは、各拠点ネットワークから IPsec トンネルで接続する[*1] Umbrella データセンターの数、および各地域の障害復旧用データセンターの数だけ契約する必要があります。導入にあたっては、宛先ドメインの設定など追加の設定管理は一切不要です。



*1　2022 年 10 月現在、Secure Client でユーザー組織専用の送信元 IP アドレスを使用する場合は、IPsec トンネルで Umbrella データセンターに接続するネットワークへの VPN 接続が必要。
エニーキャストによる VPN レスでの専用 IP アドレス利用は近日サポート予定。

Cisco Umbrella 製品パッケージ機能比較

Cisco Umbrella 製品パッケージ概要

Cisco Umbrella は、セキュリティのレベルや範囲に応じて、次の 4 つの製品パッケージから選択することができます。

DNS セキュリティ Essentials

- DNS レイヤのセキュリティ
- ドメインベースの Web フィルタリング
- クラウドアプリの検出とブロック

DNS セキュリティ Advantage

DNS セキュリティ Essentials に加えて

- SSL 対応インテリジェントプロキシ
- 危険なファイルをブロック（危険性が高いドメインのみ）
- 脅威インテリジェンス（Umbrella Investigate）

SIG Essentials

DNS セキュリティ Advantage に加えて

- SSL 対応フルプロキシ
- URL ベースの Web フィルタリング
- 危険なファイルをブロック
- クラウドアプリの検出とブロック（アプリ別にユーザー操作を制御可能）
- レイヤ 3 & 4 ファイアウォール
- リモートブラウザ分離（オプション）
- ユーザー組織専用の送信元 IP アドレス（オプション）

SIG Advantage

SIG Essentials に加えて

- レイヤ 7 ファイアウォールと侵入防御システム *1
- データ漏洩防止 *1
- 無制限のクラウドサンドボックス（Secure Malware Analytics）

*1　Umbrella SIG アドオンライセンスで SIG Essentials に追加可能。

Cisco Umbrella 製品パッケージ機能比較

セキュリティサービス / 機能			DNS セキュリティ		SIG	
			Essentials	Advantage	Essentials	Advantage
DNS レイヤセキュリティ	マルウェアやフィッシング、ボットネット、その他の危険性が高いドメインをブロック		✓	✓	✓	✓
	エンフォースメント API によって SecureX、Splunk や Anomali などと統合、カスタムリストに基づいてドメインをブロック		✓	✓	✓	✓
セキュア Web ゲートウェイ（SWG）	SSL（HTTPS）対応インテリジェント（セレクティブ）プロキシ（危険性が高いドメインのみ）			✓	✓	✓
	SSL（HTTPS）対応フルプロキシ				✓	✓
	Web（コンテンツカテゴリ）フィルタリング	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	カスタマイズ可能なブロック / 許可リスト	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	アンチウイルスエンジンおよび Advanced Malware Protection（AMP）データによって危険なファイルをブロック			危険性が高いドメインのみ	✓	✓
	無害なファイルが危険なファイルに変化しても把握できる、遡及可能なセキュリティ				✓	✓
	ユーザー組織専用の送信元 IP アドレス NEW（Umbrella DC でユーザー組織専用の送信元 IP アドレスを提供）				オプション	オプション
クラウドアクセスセキュリティ制御（CASB）	クラウドアプリの検出とブロック	ドメインベース	✓	✓	✓	✓
		URL ベース			✓	✓
	クラウドアプリ別にユーザー操作を制御（アップロードやファイル添付、投稿の禁止など）				✓	✓
	Webex や Microsoft 365 など特定のプラットフォーム（ファイルストレージアプリ）と連携してファイルをスキャン、マルウェアを検出および除去				2 アプリ	4 アプリ *1
クラウド提供型ファイアウォール（CDFW）	レイヤ 3 & 4 ファイアウォール（IP/ ポート / プロトコルの可視化と制御）				✓	✓
	レイヤ 7 ファイアウォール（アプリの可視化と制御）および侵入防御システム（IPS）				オプション	✓
	IPsec トンネル終端対応				✓	✓
データ漏洩防止（DLP）	Web およびクラウドアプリのトラフィックをインラインまたは API 経由で検査、機密データを保護				オプション	✓
リモートブラウザ分離（RBI）	疑わしい Web サイトへのブラウザアクセスをユーザーデバイスから分離				オプション	オプション
	特定の Web アプリへのブラウザアクセスをユーザーデバイスから分離				オプション	オプション
	任意の宛先へのブラウザアクセスをユーザーデバイスから分離				オプション	オプション
脅威インテリジェンス（Umbrella Investigate）	Umbrella Investigate のアクセス権			5 ログイン	5 ログイン	5 ログイン
	疑わしいドメイン、URL、IP、ASN、およびメールアドレスに関する脅威インテリジェンス			✓	✓	✓
	Investigate API によって他のツールやシステムにドメイン、URL、IP、およびファイルに関する脅威インテリジェンスを送信（1 日あたり 2,000 リクエスト）			✓	✓	✓
	SecureX との統合（API）	レポーティング API およびエンフォースメント API	✓	✓	✓	✓
		すべての API		✓	✓	✓
脅威インテリジェンス（Secure Malware Analytics）	Secure Malware Analytics のアクセス権					3 ユーザー
	クラウドサンドボックスで疑わしいファイルを分析				1 日あたり 500 サンプル（簡易分析）	無制限（詳細分析）
	任意のサイトにおける動作を分析					✓
	高度な検索（マルウェアサンプル、アーティファクト、レジストリ、URL など）					✓
XDR（SecureX）	SecureX のアクセス権		✓	✓	✓	✓

*1　継続的に追加。

Cisco Umbrella 製品型番

Cisco Umbrella 製品型番

Cisco Umbrella は、組織の大小を問わず簡単に導入および運用できる、SaaS モデルで提供されます。

Cisco Umbrella 製品パッケージは、保護対象となるユーザー数に応じたライセンスを 1 ～ 5 年のサブスクリプションとして契約します。また、保護対象となるアクセスポイント数に応じた Cisco Umbrella WLAN ライセンスや特定の機能を追加するためのアドオンライセンスも契約できます。

Cisco Umbrella ライセンス *1

製品型番	製品説明	ライセンス単位	最低数量
UMB-DNS-ESS-K9	Umbrella DNS セキュリティ Essentials ライセンス	ユーザー	1 ～
UMB-DNS-ADV-K9	Umbrella DNS セキュリティ Advantage ライセンス	ユーザー	1 ～
UMB-SIG-ESS-K9	Umbrella SIG Essentials ライセンス	ユーザー	1 ～
UMB-SIG-ADV-K9	Umbrella SIG Advantage ライセンス	ユーザー	1 ～
UMB-WLAN	Umbrella WLAN ライセンス	アクセスポイント	5 ～

*1　1、3、または 5 年間のサブスクリプション。CCW では UMB-SEC-SUB が必要。詳細は発注ガイドを参照。

Cisco Umbrella SIG アドオンライセンス *1

製品型番	製品説明	ライセンス単位	最低数量
UMB-RESERVED-IP NEW	ユーザー組織専用送信元 IP アドレス ライセンス	IP アドレス	2 ～
UMB-L7-CDFW	レイヤ 7 ファイアウォール & IPS ライセンス *2	ユーザー	1 ～
UMB-DLP	DLP ライセンス *2	ユーザー	1 ～
UMB-RBI-RISKY	RBI（Isolate Risky）ライセンス	ユーザー	1 ～
UMB-RBI-WEBAPP	RBI（Isolate Web Apps）ライセンス	ユーザー	1 ～
UMB-RBI-ALL	RBI（Isolate Any）ライセンス	ユーザー	1 ～

*1　1、3、または 5 年間のサブスクリプション。CCW では UMB-SEC-SUB が必要。詳細は発注ガイドを参照。
*2　Umbrella SIG Essentials 用アドオン（Umbrella SIG Advantage ではデフォルトでサポート）。

Cisco Umbrella サポートサービス

Cisco Umbrella の契約時には、サポートサービスも契約する必要があります。必要なサポートに応じて、3 つのサービスレベルから選択することができます。

Cisco Umbrella サポートサービス提供比較

サポート	Solution Support *1	Enhanced	Premium
24 時間 365 日のテクニカルサポート（電話またはオンラインでケースを申請）	✓	✓	✓
シビラティ（重大度）1 および 2 の電話によるケース申請に対する対応目安	30 分	30 分	15 分
ソフトウェアのアップデート	✓	✓	✓
Umbrella Knowledge Base などオンラインリソースのアクセス権	✓	✓	✓
ケースの優先対応		Solution Support より優先	最優先
複数製品のサポートを調整する一次連絡窓口	✓	✓	✓
設定ガイダンスなど導入支援		✓	✓
機能活用ガイダンスや定期的な設定レビューなど運用支援		✓	✓
学習およびトレーニング		✓	✓
サポートケース分析			✓
シスコの専門家（専任サービスマネージャ）による技術支援			✓

*1　提供準備中。

WEB 14 日間の無料トライアルをぜひお試しください！
engage2demand.cisco.com/LP=26357

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 9:00 - 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
cisco.com/jp

2347-2210-005-TO