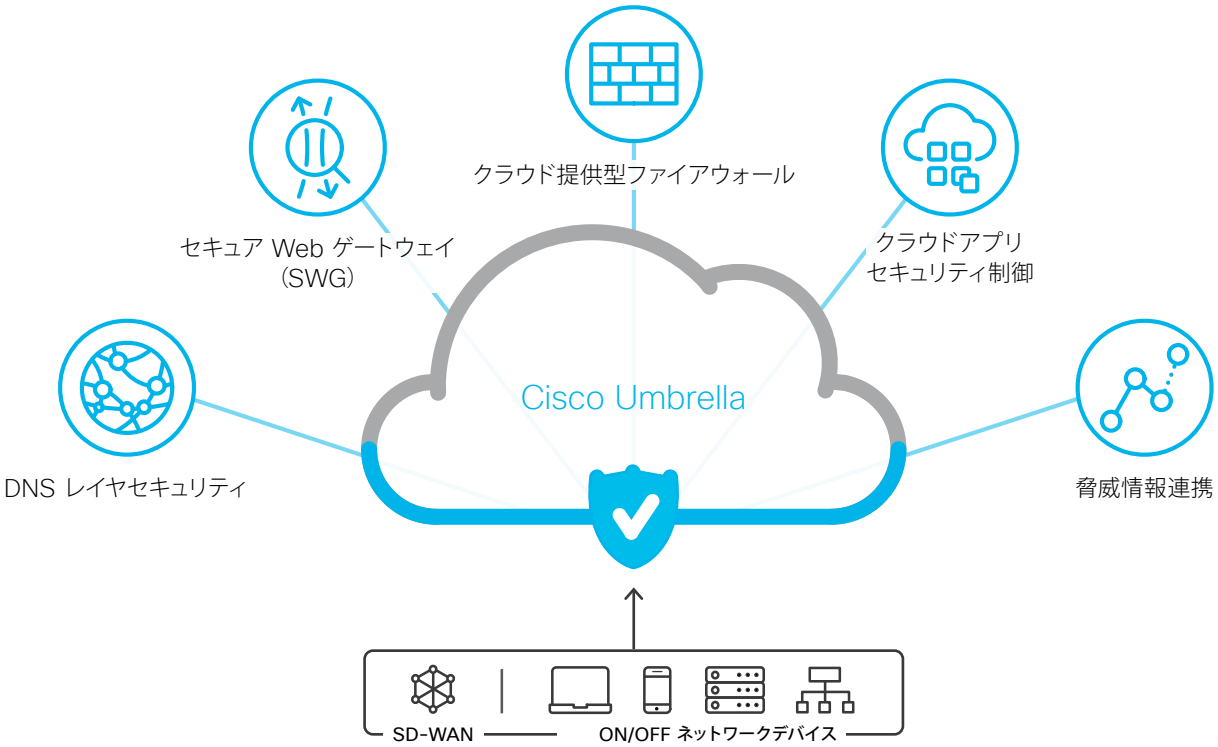
脅威防御の最前線をクラウドで提供するセキュア インターネットゲートウェイ

Cisco Umbrella

208.67.222.222 + 208.67.220.220
2620:119:35::35 + 2620:119:53::53



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、サンドボックスも含めた、幅広いセキュリティサービスを提供します。
本社、拠点などの場所、移動中、VPN の ON/OFF を問わず、あらゆるユーザ、そしてデバイスを保護できる、
最も簡単かつ迅速に導入可能なクラウドセキュリティです。

かんたん導入

最新の脅威にも迅速に対応できる
クラウドベースのインテリジェンス
専用のハードウェアが不要で導入も簡単

働き方改革に最適

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
あらゆるデバイス / ユーザを保護可能

わかりやすいレポート

グラフィカルなレポートを
Web ダッシュボードとメールで提供
手軽に、かつ安心して運用可能

Cisco Umbrella の概要と特長

DNS レイヤセキュリティをはじめ いま必要な対策がすべて揃ったクラウドセキュリティ

DNS レイヤ セキュリティ　フルプロキシ　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

Cisco Umbrella は、DNS レイヤセキュリティをはじめ、フルプロキシ、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、いま必要な対策がすべて揃ったクラウドセキュリティです。Cisco Talos などの脅威インテリジェンスと連携し、DNS および URL ベースで危険なサイトへの通信をブロックします。

設定からサポートまで 日本語対応

直感的に操作できる、わかりやすい Web ベースのダッシュボードに加えて、マニュアルやサポートも日本語対応。*1
手軽に導入可能、かつ安心して運用可能です。

*1　一部の画面/インターフェイスは翻訳中。

高速！DNS パフォーマンス

Cisco Umbrella は、純粋な DNS サービスとしても非常に優れたパフォーマンスを誇ります。Prospect One 社が提供する DNS パフォーマンス分析「DNSPerf」のパブリック DNS リゾルバ部門では、常に上位にランクインしています。

WEB www.dnsperf.com

どこにいても、あらゆるデバイスをカバー

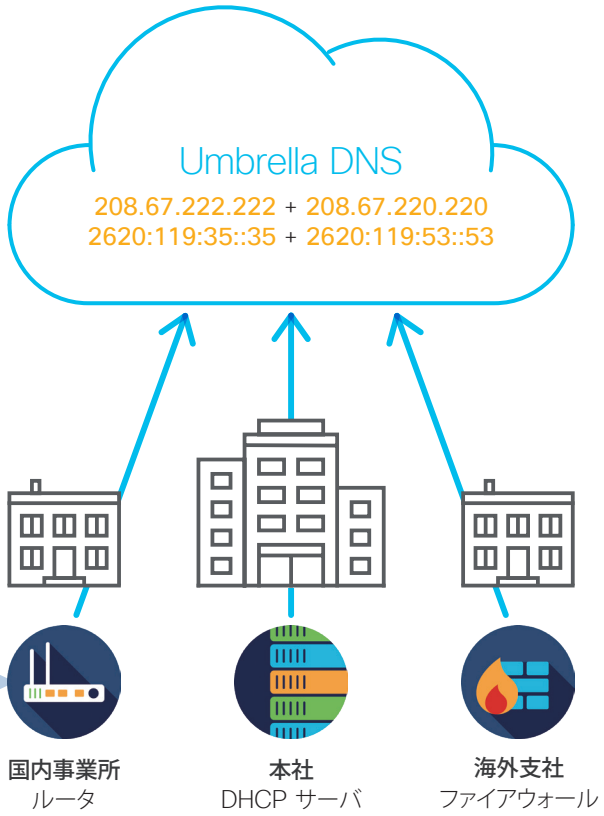
インターネット利用に欠かせない DNS レイヤセキュリティであることから、インターネットを利用するあらゆるデバイス、あらゆるネットワーク（場所）に適用可能なため、働き方改革に取り組む企業に最適です。

また、ファイアウォールやアンチウイルスのような既存のセキュリティと競合または重複することなく、簡単にアドオンしてネットワークの防御を強化できます。

クラウドセキュリティだからできる！利用シーン ❶

既存環境はそのままで全社のネットワークにかんたんに導入したい

クラウドサービスである Cisco Umbrella には、**ハードウェアの設置やソフトウェアのインストールが不要**です。DHCP サーバやルータ、ファイアウォールの DNS 設定を変更するだけで、わずか数分で導入できます。
国内外に散らばる支社、事業所、工場など各拠点への導入もスムーズで、DNS の設定後は Web ダッシュボードから一元管理できます。

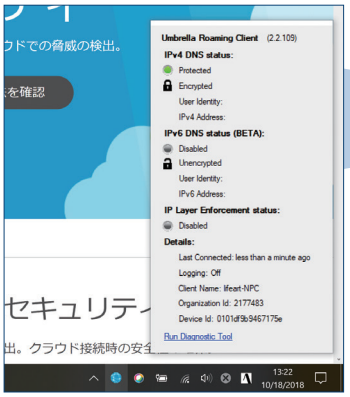


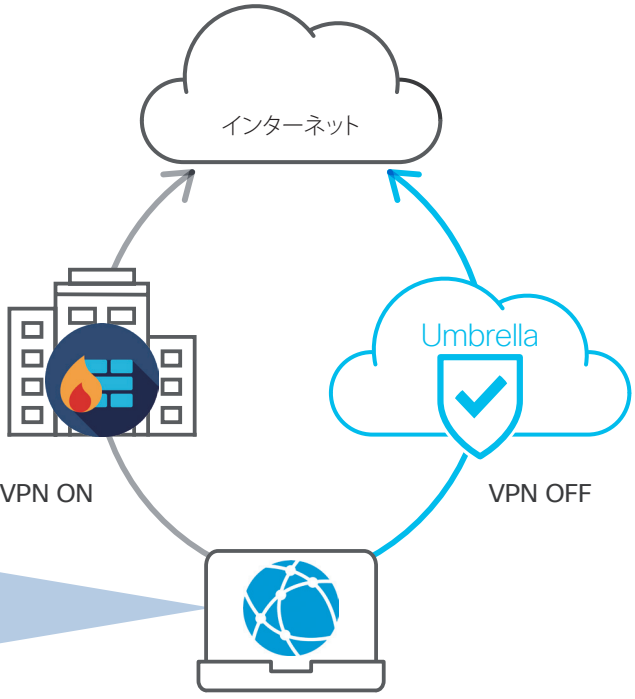
クラウドセキュリティだからできる！利用シーン ❷

働き方改革に！オフィス外の社員を VPN なしで保護したい

外出中のモバイルワークや在宅ワークなど働き方が変化するとともに、社外のリモートワーカーを適切に保護することが、より重要に、そして困難になっています。リモートワーカーへの代表的なセキュリティ提供手段である VPN が、常に ON になっているとは限らないという実態があるからです。企業のノート PC ユーザの 8 割が「VPN を使用しないことがある」と答えた調査結果もあります *1。
したがって、たとえ VPN が OFF でもセキュリティを提供できる新たな手段が必要です。Cisco Umbrella では、軽量のクライアントをノート PC にインストールするだけで、**VPN の ON/OFF にかかわらず常に社内ネットワークと同等のセキュリティを提供**できます。

*1　出典:IDG Research Services, 2016. Your users have left the perimeter. Are you ready? (cs.co/IDG-survey)



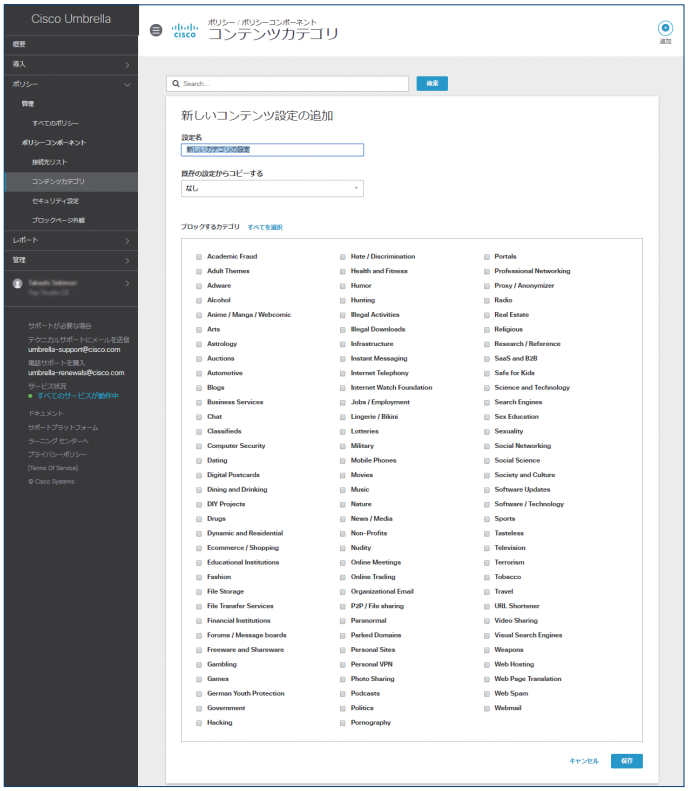


クラウドセキュリティだからできる！利用シーン ❸

かんたんにアクセスポリシーを設定したい

Cisco Umbrella では、リモート アクセス用やゲスト アクセス用など、**目的に応じて柔軟にカスタマイズ可能なポリシー**を作成および適用できます。たとえば次のようなきめ細やかな設定を、わかりやすいウィザードに従って作成できます。

- 「DNS レイヤのセキュリティを適用したい」「コンテンツフィルタリングを適用したい」などの目的に応じた設定
- 「マルウェアをホストしているサイトをブロック」「フィッシングサイトをブロック」「有害な可能性があるドメインをブロック」「クリプトマイニングをブロック」など、セキュリティカテゴリに応じた設定
- コンテンツフィルタリング設定：ブロックしたいコンテンツを含むサイトを「高」「中」「低」のカテゴリグループで選択、または右のように個別のカテゴリで選択

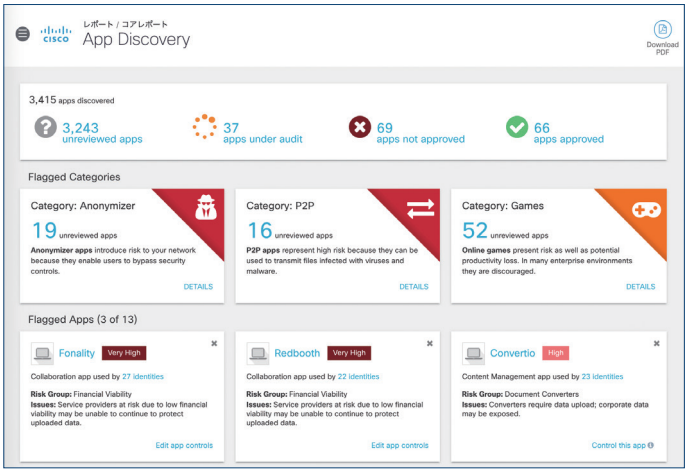


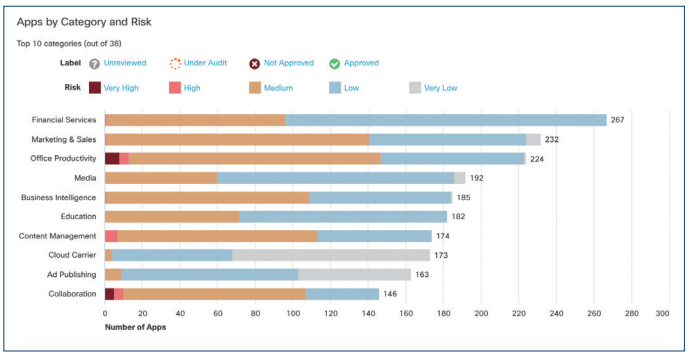
クラウドセキュリティだからできる！利用シーン ❹

シャドー IT を見える化したい

Cisco Umbrella では、マルウェアやフィッシングに関連がありそうな通信アクティビティ（リクエスト）など、脅威に関するさまざまな情報を可視化できますが、「**アプリケーション ディスカバリ**」機能によって、クラウドアプリケーションやサービスの利用状況も可視化することができます。
この機能によって、たとえば社員がクラウドアプリケーションを勝手に使用する「シャドー IT」について、次のような対策が可能になります。

- 各アプリケーションのリスクレベルを評価する
- リスクが高いアプリケーションを特定する
- アプリケーションベンダーの信頼度を確認する
- ユーザデータやリスクスコアなど各種レポートに基づいて、アプリケーション利用の最適化または利用不可の判断材料にする
- 既存アプリケーション利用のモニタリングや新規アプリケーション利用の発見によって、無秩序なクラウドアプリケーション利用を防止する
- 不要なアプリケーションをカテゴリ別または個別にブロックする



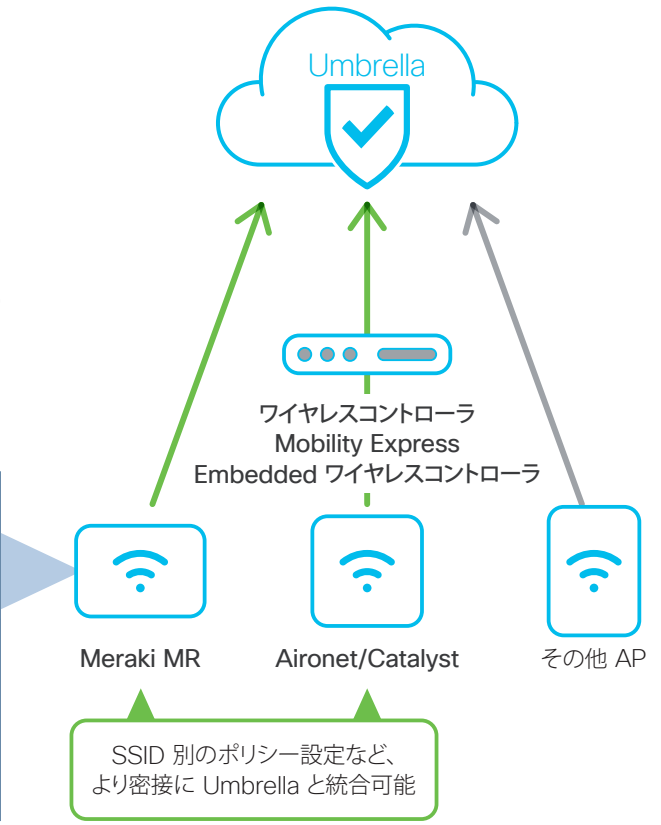


クラウドセキュリティだからできる！利用シーン 5

Wi-Fi セキュリティをかんたんに強化したい

社員や顧客など、エンドユーザ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数の制限なく保護できます。

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**、**シスコ ワイヤレスコントローラ**、**Cisco Mobility Express**、および **Cisco Embedded ワイヤレスコントローラ**では、Cisco Umbrella と管理ツールレベルでの統合が可能です。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 ポリシーをリンクできます。



クラウドセキュリティだからできる！利用シーン 6

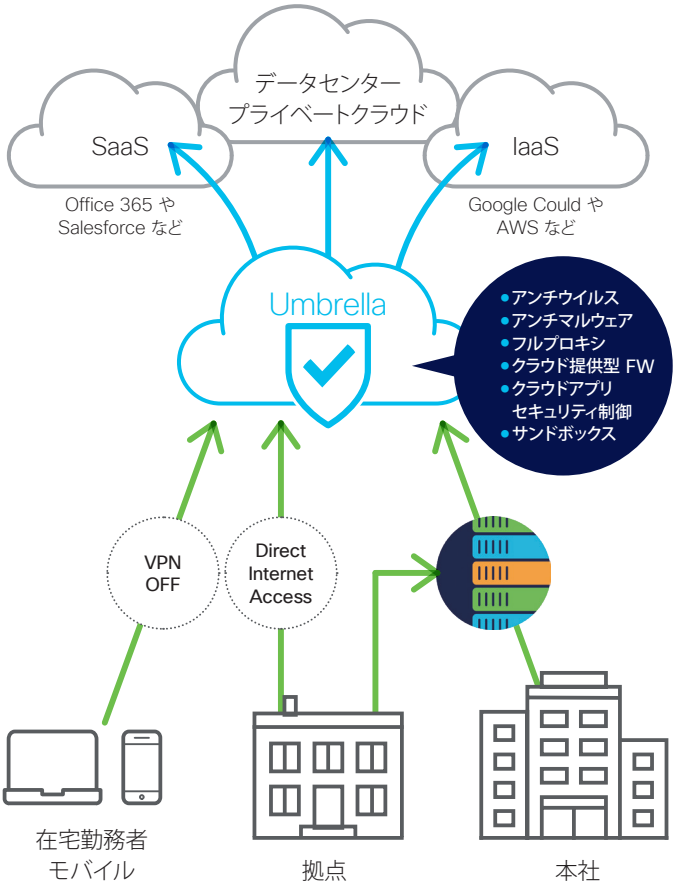
拠点からの直接インターネットアクセス（DIA）をセキュアにしたい

クラウド アプリケーション / サービスの企業利用が拡大するに伴って、拠点からのインターネット接続を VPN で本社に集約しない、**直接インターネットアクセス**［Direct Internet Access（DIA）］（またはローカルブレークアウト）もまた増加しています [*1]。これには、限定された帯域幅や遅延によって概して低速な VPN によってもたらされる、アプリケーション パフォーマンスやサービス品質の低下を敬遠するなど、さまざまな理由が挙げられます。しかし、たとえばユーザの利便性向上と引き換えに、大きなセキュリティリスクを抱えることにもなります。

そのため、各拠点のセキュリティを増強する必要がありますが、高性能なセキュリティアプライアンスの導入など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てしまいます。

Cisco Umbrella なら、このような課題に悩まされることなく、**低コストかつシンプルに導入および運用可能**です。また、**Cisco ISR 1100/4000 シリーズ**、**Cisco Meraki MX シリーズ**、**Cisco Viptela OS ルータ**などと連携することで、フルプロキシやクラウド提供型ファイアウォールなどセキュア インターネットゲートウェイ（SIG）のフル機能を、必要な拠点に展開できます。

*1　参考資料:IDC, 2017. Network Evolution and Market Outlook.



Cisco Umbrella 購入ガイド

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。
ユーザ数またはデバイス数に応じたライセンスを、1 ～ 5 年のサブスクリプション期間で購入できます。

Cisco Umbrella DNS セキュリティ Essentials ライセンス *1 NEW

製品型番	製品説明
UMB-DNS-ESS-K9	Umbrella DNS セキュリティ Essentials ユーザ別ライセンス

*1 UMB-SEC-SUB が必要。

Cisco Umbrella DNS セキュリティ Advantage ライセンス *1 NEW

製品型番	製品説明
UMB-DNS-ADV-K9	Umbrella DNS セキュリティ Advantage ユーザ別ライセンス

*1 UMB-SEC-SUB が必要。

Cisco Umbrella セキュア インターネットゲートウェイ Essentials ライセンス *1 NEW

製品型番	製品説明
UMB-SIG-ESS-K9	Umbrella SIG Essentials ユーザ別ライセンス

*1 UMB-SEC-SUB が必要。

Cisco Umbrella WLAN ライセンス *1

製品型番	製品説明
UMB-WLAN	Umbrella WLAN アクセスポイント別ライセンス（5 AP ～）

*1 UMB-SEC-SUB が必要。

Cisco Umbrella Roaming ライセンス *1

製品型番	製品説明
UMB-ROAM	Umbrella Roaming デバイス別ライセンス（10 デバイス～）

*1 UMBRELLA-SUB が必要。

Cisco Umbrella Branch ライセンス *1

製品型番	製品説明
UMB-BRAN-1100	Cisco ISR 1100 シリーズ用 Umbrella Branch ライセンス
UMB-BRAN-4221	Cisco ISR 4221 用 Umbrella Branch ライセンス
UMB-BRAN-4321	Cisco ISR 4321 用 Umbrella Branch ライセンス
UMB-BRAN-4331	Cisco ISR 4331 用 Umbrella Branch ライセンス
UMB-BRAN-4351	Cisco ISR 4351 用 Umbrella Branch ライセンス
UMB-BRAN-4431	Cisco ISR 4431 用 Umbrella Branch ライセンス
UMB-BRAN-4451	Cisco ISR 4451 用 Umbrella Branch ライセンス
UMB-BRAN-RV	Cisco RV ルータ用 Umbrella Branch ライセンス

*1 UMBRELLA-SUB が必要。

Cisco Meraki MR シリーズ用アップグレードライセンス *1 NEW

製品型番	製品説明
LIC-MR-UPGR-1YR	アドバンスドライセンスへのアップグレードライセンス（1 年間）
LIC-MR-UPGR-3YR	アドバンスドライセンスへのアップグレードライセンス（3 年間）
LIC-MR-UPGR-5YR	アドバンスドライセンスへのアップグレードライセンス（5 年間）

*1 Meraki ダッシュボードで Umbrella DNS セキュリティを利用できる、アドバンスドライセンスへのアップグレードライセンス（Umbrella ダッシュボードは利用不可）。事前に定義された 7 種類の組み合わせポリシーのみ利用可能（カスタマイズ不可）。

Cisco Umbrella パッケージ機能比較

主要パッケージのセキュリティサービス		DNS セキュリティ Essentials	DNS セキュリティ Advantage	SIG Essentials
DNS レイヤ セキュリティ	フィッシング、マルウェア、ボットネット、および危険なカテゴリ（マイニングや新規ドメインなど）に属するドメインをブロック	●	●	●
	パートナー（Splunk、Anomali など）インテグレーションやエンフォースメント API によるカスタムリストに基づいてドメインをブロック	●	●	●
	DNS をバイパスする C2 コールバック対策として直接 IP トラフィックをブロック	-	●	●
セキュア Web ゲートウェイ（SWG）	Web トラフィック検査用プロキシ	-	危険なドメインのみ	●
	SSL（HTTPS）トラフィックの復号化および検査	-	危険なドメインのみ	●
	Web フィルタリング	カテゴリベース ドメインベース	カテゴリベース ドメインベース	カテゴリベース 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	ドメインベース	IP ベース URL ベース
	Cisco Talos などからのフィードに基づいて URL をブロック、アンチウイルスエンジンと Cisco AMP のデータに基づいてファイルをブロック	-	危険なドメインのみ	●
	Cisco Threat Grid クラウドのサンドボックス環境を使用して疑わしいファイルを分析（200 ファイル～ / 日）	-	-	●
	無害なファイルが危険なファイルに変化しても特定できる、遡及的セキュリティ	-	-	●
クラウド提供型 ファイアウォール	レイヤ 3 および レイヤ 4 ポリシーで特定の IP/ ポート / プロトコルをブロック	-	-	●
	IPsec トンネル終端対応	-	-	●
クラウドアプリ セキュリティ制御	シャドー IT を検出およびブロック	ドメインベース	ドメインベース	URL ベース
	アプリケーション別にきめ細やかな制御（アップロード / ファイル添付 / 投稿の禁止など）が可能なポリシー	-	-	●

簡単なご登録で、Cisco Umbrella を 14 日間無料でお試しいただけます。

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

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
http://www.cisco.com/jp/go/vdc_callback

2120-1912-01A-TO