Cisco Secure Access - DNS Defense（旧 Cisco Umbrella DNS）

手頃な価格、シンプルな展開と管理、優れた効果。

2025 年 5 月

目次

ランサムウェアやフィッシング攻撃を防ぐために、強力な DNS レイヤセキュリティが不可欠である理由

アメリカ合衆国サイバーセキュリティ・社会基盤安全保障庁（CISA）の表明によれば、成功した攻撃の 90% 以上がリンクまたは Web ページをきっかけとして始まっています。DNS プロトコルは、ドメイン名を IP アドレスと関連付けます。プロトコルやポートに関係なく、DNS 要求が IP 接続に優先されるため、DNS レイヤセキュリティは、要求が確立される前に要求を迅速に評価します。強力な DNS レイヤセキュリティにより、悪意のあるドメインへのアクセスや、ランサムウェアなどの脅威は、ネットワークやエンドポイントに到達する前にブロックされます。

現在、多くの組織が DNS 解決を ISP に委ねています。その一方で、企業によるインターネットへの直接接続とリモートワークの増加により、脅威防御、プライバシー、コンプライアンス、およびパフォーマンスに関する DNS の最適化がますます重要になっています。**パッチ適用プログラムなどの中核となる「セキュリティ対策」とともに、DNS レイヤセキュリティを強化することは、セキュリティ態勢を改善するための費用対効果の高い主要な方法です**。ファイアウォールに到達する前に脅威をブロックし、セキュリティチームが管理するアラートの圧力を大幅に軽減します。

世界トップクラスの DNS レイヤセキュリティがさらに向上

ネットワークセキュリティ態勢の大幅な改善には通常、費用と時間、そしてコストがかかります。SOC チームと DFIR チームが次々と発報するアラートに対応できなくなることが多いため、小規模な組織では、日常的な管理を必要としないセキュリティが求められています。

Secure Access - DNS Defense は、他に類を見ないセキュリティ製品です。**セキュリティはシンプルかつ効果的である必要があります**が、シスコはこのニーズに対応しています。40,000 人を超えるお客様が、毎日 8,000 億回を超える接続をシスコに委ねています。2024 年、GigaOM は、Cisco Secure Access - DNS Defense が DNS レイヤセキュリティ業界で首位を占めていることを発表しました。

さらに、DNS におけるリーダーシップが評価された結果、Miercom のベンチマークレポートの SSE 脅威有効性と DNS 遅延のランキングにおいて、シスコは第 1 位を獲得しました。

現在、シスコは先進的な取り組みを継続しており、AI ベース DNS トンネリングの拡張機能とドメイン生成アルゴリズム（DGA）検出の水準を引き上げています。

その結果トラフィックがファイアウォールに到達する前の DNS レイヤにおける優れた脅威保護により、より多くの攻撃者を阻止します。シスコは保護を強化し、セキュリティチームが直面するアラートの圧力を大幅に軽減します。

さらに、Cisco Secure Access - DNS Defense は、Cisco Umbrella DNS と比較して強化されたポリシーフレームワークと、SaaS API DLP およびクラウドマルウェアスキャンなどを備えており、シスコの DNS を中心とした以前のパッケージよりも強化されています。これらの機能強化は、追加のコストなしで提供されます。

基盤となるセキュリティと必要に応じた拡張の可能性

DNS 中心の態勢を維持するか、いずれ完全な Secure Access SSE、Cisco Universal Zero Trust Network Access（UZTNA）にアップグレードするか、あるいは市場を牽引するシスコのソフトウェア定義型 WAN（SD-WAN）を使用した Cisco Secure Access Service Edge（SASE）にアップグレードするかどうかは、お客様次第です。

Secure Access の Secure Internet Access（SIA）パッケージは、このデータシートに記載されているすべての DNS Defense 機能に加えて、Cisco ThousandEyesにより強化されたエクスペリエンス インサイト デジタ

ルモニタリング機能、フル DLP、クラウド アクセス セキュリティ ブローカ（CASB）、セキュア Web ゲートウェイ（SWG）、ブラウザ分離（RBI）、Firewall as a Service（FWaaS）などを備えています。Secure Access - DNS Defense には、業界初の統合型 ZTNA + VPN as a Service（VPNaaS）機能を備えた、Secure Access の Secure Private Access（SPA）パッケージの無料トライアル（100 シート限定）が含まれています。シスコのクラウド提供型セキュリティパッケージの比較については、リンクを参照してください。

機能と利点

機能	利点
DNS レイヤセキュリティ	DNS レイヤセキュリティを提供する競合 SSE ベンダーとは異なり、シスコは再帰 DNS サービスを運用しています。結果として、遅延が低減され、ユーザーエクスペリエンスが向上することが実証されました。DNS レイヤでフィルタ処理を行い、ネットワークやエンドポイントへの接続が確立される前に、ポートまたはプロトコル上で悪意のある不適切な接続先への要求をブロックします。 • すべてのネットワークデバイス、オフィスの場所、およびローミングユーザーやモバイルデバイスのインターネットアクセスを保護します。 • マルウェア、フィッシング、ボットネットなどの高リスクのアイテムを含むドメインへのアクセスをブロックします。 • アプリケーション検出、モニタリング、ブロッキング、リスクスコアリング。 • セキュリティ脅威や Web コンテンツの種類、および実行されたアクションごとに DNS アクティビティに関する詳細なレポートを提供します。 • 高度な人工知能により、DNS トンネリング技術の悪用を抑止し、攻撃者によるラテラルムーブメントを阻止し、データ漏洩に対するリアルタイムの検出と保護を実現します。 • 数千におよぶ場所やユーザーに対して迅速に運用を開始し、即時に保護できます。 • レポートと適用されたポリシーをユーザーレベルまで可視化します。
グローバル インフラストラクチャ	• Secure Access - DNS Defense には、50 以上の再帰 DNS リゾルバのグローバルネットワークが含まれており、ユーザーやネットワークに到達する前に脅威を阻止する高パフォーマンスのセキュリティを実現します。
セキュア Web ゲートウェイ（一部）	• カテゴリまたは特定の URL によるコンテンツフィルタリングを可能にすることで、ポリシーやコンプライアンス要件に違反する接続先をブロックします。 • Web トラフィックを選択的にプロキシして検査します。
SaaS API DLP	サードパーティの SaaS API（クラウド間）を使用して、機密データをスキャンおよび制御します。インターネットに向かうトラフィックの可視性は必要ありません。クラウドサービス内に存在する機密データを検出し、それらのサービスを継続的にモニタリングして機密データの追加を監視します。
クラウドマルウェアの検出	クラウドベースのファイル ストレージ アプリケーションからマルウェアを検出して削除します。悪意のあるファイルをエンドポイントに到達する前に検出することにより、保護を強化します。 • セキュリティ管理者の有効性と効率を高めます。 • アクティブ化すると、クラウドベースのサービス内にあるすべてのファイルがハッシュ化され、マルウェアのスキャンが自動的に実行されます。悪意のあるファイルには、修復、隔離、または削除の対象としてフラグが付けられます。 • Box、Dropbox、Webex®、Microsoft 365、および Google Drive、AWS S3、Azure をサポートします。

機能	利点
Talos 脅威インテリジェンス	世界最大の民間の脅威インテリジェンスチームの 1 つである Cisco Talos は、その脅威データの巨大なデータベースに対して AI、統計、および機械学習モデルを継続的に実行し、サイバー脅威に関する詳細なインサイトとコンテキストを提供します。Secure Access - DNS Defense の有効性を高めるため、Talos のリサーチが継続的に使用されています。
単一の管理およびレポートコンソール	インテントベースのルールを使用した統合セキュリティポリシーの作成と管理。時間の経過とともに DNS レイヤセキュリティを超える追加機能が必要になる場合、Cisco Secure Access 統合コンソールは、インターネットアクセス保護、パブリック SaaS アプリケーション、およびプライベート アプリケーション アクセスでポリシーを統合するための単一のポイントの役割を果たします。広範なロギングや、企業のセキュリティ オペレーション センター（SOC）へのログのエクスポート機能を提供します。 • あらゆるユーザーのあらゆるアプリに対するポリシーを一元的に定義。セキュリティポリシーの構築プロセスを簡素化し、組織全体でポリシー定義の一貫性を促進します。 • 統合されたソース（ユーザー、デバイス）と統合されたリソース（アプリケーション、接続先）により、アタッチポイントやアクセスするアプリケーションに関係なく、セキュリティポリシーがユーザーに対応するようになります。 • 継続的に行われるポリシー管理作業を削減します。 • 集約されたレポート作成機能により、可視化と検出までの時間が改善されます。 • SOC/セキュリティアナリストの調査プロセス全体を簡素化します。
デバイス サポート Secure Access - DNS Defense に含まれており、追加のコストは必要ありません。	• Windows および MacOS、iOS、Android 上の Secure Client。 • Cisco Security for Chromebook クライアント。

Cisco Secure Access：ソフトウェア サポート サービス

Cisco Secure Access には、Software Support-Enhanced 用の個別の在庫管理単位（SKU）が必要で、Software Support Premium へのアップグレードも可能です。

Cisco Software Support Enhanced

- テクニカルサポート（電話およびオンラインで Cisco クラウド セキュリティ サポートに 24 時間 365 日アクセス可能）。
- 技術的なオンボーディングと導入の支援。
- ソフトウェアアップデート。
- ソフトウェアの専門知識を持つ主要な連絡窓口。

Cisco Software Support Premium（推奨されるアップグレード）

Enhanced レベルの機能に加えて、以下が含まれます。

- Enhanced サポートよりも優先的にケースを処理。
- サポートケース分析。
- インシデント管理を実行するエキスパートの割り当て。

セキュリティソフトウェアを対象としたプロアクティブなコンサルティングや推奨に関するシスコのサポートサービスの詳細については、こちらをクリックしてご確認ください。

詳細情報

詳細については、Cisco Secure Access をご覧ください。

米国本社
カリフォルニア州サンノゼ

アジア太平洋本社
シンガポール

ヨーロッパ本社
アムステルダム（オランダ）

シスコは世界各国に約 400 のオフィスを開設しています。オフィスの住所、電話番号、FAX 番号は当社の Web サイト（www.cisco.com/jp/go/offices）をご覧ください。

Printed in USA C78-5130097-00 05/25