

Zscaler DNS Security



場所を問わず常にあらゆる DNS リクエスト (平文 DNS および暗号化 DNS) のセキュリティを確保し、すべてのユーザー、デバイス、ワークロードを保護

データシート

業界で最も包括的なクラウドネイティブ セキュリティ サービス エッジ(SSE)プラットフォームにより、平文DNSと暗号化DNSに対して優れたセキュリティ、可用性、パフォーマンスを提供します。

DNS は、インターネット接続の基盤となるシステムである一方、高度な攻撃やデータの持ち出しに悪用される重大な脅威ベクトルにもなっています。組織がハイブリッドワークやIoTを導入するなか、可視性のギャップや暗号化 DNS トラフィックを検査できないことで死角が生じ、次のような攻撃に対する脆弱性が生まれています。

- **DNS トンネリング**: マルウェアによって DNS リクエスト / レスポンス システムを悪用し、侵害されたシステムと攻撃者の間でコマンドをやり取りします。多段階攻撃では、追加のマルウェアペイロードが配信されます。また、盗まれたデータが最大 255 文字ずつ持ち出される場合もあります。
- **DNS スプーフィング**: 多くの場合、中間者 (MitM) 攻撃の手法を使って実行されます。DNS スプーフィングでは、DNS サーバー上の DNS エントリの変更や、DNS キャッシュへの偽の情報の入力などが行われます。結果として、標的となったユーザーは攻撃者の管理する詐欺サイトにリダイレクトされます。フィッシングのほか、ユーザーにワームやウイルスなどの悪意のあるソフトウェアをインストールさせるために使用されます。

を通じ、すべての DNS トラフィックをルーティングします。クラウドネイティブな Zscaler Zero Trust Exchange は、世界中の 160 以上のエッジ ロケーションでサービスを提供し、優れたパフォーマンスを実現します。Zscaler は、最適な DNS 解決を行うとともに、トップクラスの DNS フィルタリング、セキュリティ、水平方向の拡張性を持つ DNS-over-HTTPS (DoH) 検査、データ流出対策を実現できる唯一のセキュリティ ベンダーです。

DNS Security では、DNS リクエスト / レスポンスを制御するルールを定義できます。DNS トンネリングを検出、防止するとともに、次のことが可能になります。

- 使用されるプロトコルや暗号化技術を問わず、すべての DNS リクエスト / レスポンスを監視し、ポリシーを適用する (UDP、TCP、DNS over HTTPS を含む)
- ユーザー、グループ、部門、クライアントの場所、ドメインと IP アドレスの分類、DNS レコードタイプ、解決された IP の場所など、さまざまな条件できめ細かい DNS フィルタリングルールを定義する
- DNS トラフィックに対して条件に基づくアクションを施行する (トラフィックの許可またはブロック、特定の DNS サーバーへのリクエストのリダイレクト、DNS レスポンスの上書きによるユーザーのリダイレクトなど)

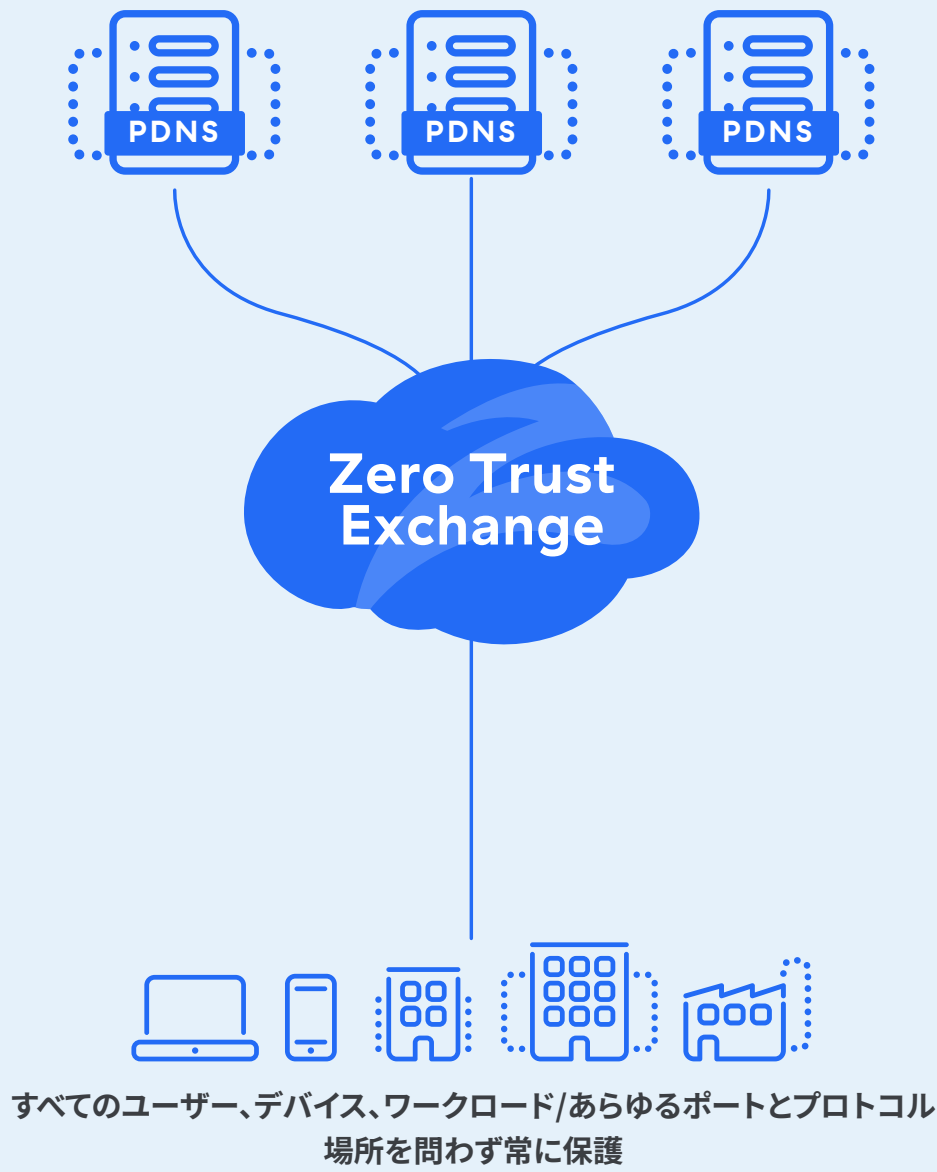
分散型の組織のための スケーラブルな DNS セキュリティ

Zscaler DNS Security は、Zscaler Zero Trust Exchange の一部である Zscaler Zero Trust Firewall

- DNS ベースの攻撃や DNS トンネルを介したデータ流出を検出、阻止する
- ドメイン解決に Zscaler Trusted DNS Resolver を使用し、セキュリティ態勢を強化する
- 平文トラフィックを暗号化 DNS に変換したうえで保護 DNS (PDNS) リゾルバーに送信して、宛先を問わずすべての DoH トラフィックを保護し、ポリシーを適用する
- プライマリー リゾルバーに障害が発生した場合にセカンダリー リゾルバーにリクエストをリダイレクトすることで、サードパーティー リゾルバーの可用性を最適化する
- 構成可能な DNS ECS により、ユーザーが正しい言語、コンテンツ、通貨で Web ページを利用できるようにし、ローカライズされた最適なユーザー エクスペリエンスを提供する

ZSCALER DNS SECURITY のメリット

- **隠れた攻撃を検出する AI 活用型の完全な検査。** 無制限のインライントラフィック検査、機械学習、ネイティブな TLS/SSL 復号により、ステルス性の高い脅威を防ぎ、悪意のある接続を終了させます。
- **すべてのポートとプロトコルにわたる DNS の完全な可視化。** 非標準ポートで隠されている場合も含め、暗号化された DNS トンネリングやその他の DNS ベースの脅威を検出、ブロックします。
- **オプションの解決機能を備えた安全な DNS。** Zscaler はユーザーやデバイス、DNS サービスを問わず、すべての DNS トラフィック (平文 DNS および暗号化 DNS) を検査します。オプションの DNS 解決により、セキュリティとパフォーマンスを強化するとともに、ベンダーの統合を簡素化します。
- **グローバルに展開されたエッジを通じたクラウド型の保護。** Zscaler Zero Trust Firewall は、Zscaler Internet Access™ と完全統合され、Zscaler Zero Trust Exchange™ の一部として機能し、優れたセキュリティとユーザー エクスペリエンスを提供します。
- **トップクラスの可用性。** 自動フェイルオーバーと構成可能なエラー処理により、信頼性の高い高速アクセスを維持します。
- **卓越したユーザー エクスペリエンス。** リクエストをエッジで解決し、最適な CDN を通じて現地の言語と通貨でコンテンツを配信することで、高速かつシームレスなユーザー エクスペリエンスを実現します。
- **フォレンジック的に完全な DNS ログ。** コンテキストが豊富なデータを通じてすべての DNS トランザクションを確実に調査できるようにし、コンプライアンス対応を支援します。
- **世界中の Zscaler のユーザーによって強化される保護。** 脅威インテリジェンスと AI/ML アルゴリズムは、世界最大のインライン セキュリティクラウドから得られるデータで強化され、リアルタイムで更新されます。
- **プロセスレベルの精度での DNS ポリシー適用。** DNS リクエストを行う正確なアプリケーション プロセスに基づいて DNS ポリシーを施行します。許可されていないプロセスや不審なプロセスからのリクエストをブロックし、マルウェアのなりすまし、DNS の悪用、内部脅威のリスクを軽減します。



- 1 すべてのDNSトラフィックをZscalerに転送して、可視性を確保するとともに、160拠点以上のポイントオブプレゼンスでポリシーを施行
- 2 平文DNSをDNS-over-HTTPS (DoH)で暗号化し、プライバシーとセキュリティを確保
- 3 DoHトラフィックを保護DNS (PDNS)リゾルバーに転送し、悪意のあるドメインへのリクエストを分析およびブロック
- 4 セカンダリーPDNSリゾルバーへのフェイルオーバーを提供し、高可用性を確保
- 5 エラー処理を改善し、構成可能な形で提供

概要：脅威対策とDNS関連の課題の解決

DNSセキュリティの課題 / 問題の領域	脅威 / 問題の詳細	DNSセキュリティソリューション
安全で最適化されたDNS解決		
ユーザー、デバイス、ワークロード、サーバー	認証済みおよび未認証のユーザー、ヘッドレスIoTデバイス、サーバー、ワークロードはすべて安全なDNS解決が必要	DNS Securityの展開アーキテクチャは、ZIA DNS Securityへのあらゆるタイプのトラフィック転送に対応
再帰DNSの不確実な可用性、DoSリクエストフラッド、NXDOMAIN攻撃	リモート/ハイブリッドおよびオフィス/拠点の従業員は、安全で信頼性が高く低レイテンシーのDNS解決が必要	ユーザーに最も近いZscaler Trusted Resolver (ZTR)による、可用性の高い最適化されたDNS解決
信頼できない未承認のリゾルバーやDNSハイジャック	クライアントからサードパーティーのDNSリゾルバーに対する国際的なアクセスまたはブロードバンドルーターやカフェのホットスポットを介したアクセス、デバイスの侵害と悪意のあるDNSの使用	信頼できるパブリックリゾルバー、保護DNSリゾルバー、またはZscaler Trusted Resolverへの直接DNSリクエスト



キャッシュ ポイズニング、DNS スプーフィング	DNS リゾルバーが正規のドメインに対して、悪意のある IP アドレスを提示	IP レスポンスを個別に分類、DNSSEC 解決は Zscaler Trusted Resolves で実行
DNS セキュリティとフィルタリング		
暗号化された DNS over HTTPS (DoH) によるセキュリティ回避	脅威アクターがセキュリティを回避するために DNS を暗号化、または DoH を使用して未承認のサードパーティー リゾルバーを指定	すべての DoH を復号および検査し、DNS ポリシーを適用
DNS トンネリング	脅威アクターが DNS トンネルを使用してデータを持ち出す、あるいは同様の手法でコマンド&コントロール サーバーと通信	DNS トンネルを特定して良好 / 不良 / 不明に分類、dnscat や iodine などの特定のトンネルの IPS を検出
DNS リクエストにおけるプロセス コンテキストの欠如	一般的に、従来の DNS セキュリティポリシーは DNS リクエストを生成する特定のアプリケーション プロセスに対する可視性に欠け、マルウェアが正規のアプリになりすましたり不正なプロセスを使用したりして、検出されずに DNS リクエストを開始することが可能	正確なアプリケーション プロセスに基づいて DNS ポリシーを施行。不正なプロセスや不審なプロセスからの DNS リクエストをブロックすることで、マルウェアによるなりすまし、DNS の悪用、内部関係者による悪用などのリスクを軽減
危険な Web コンテンツ	ユーザーが、会社をリスクにさらす、または生産性の低下を招く Web カテゴリ（ヘイト、ポルノ、違法コンテンツなど）にアクセス	リクエスト時のドメインとレスポンス時の IP の両方を分類し、高リスクのカテゴリをブロック
新規登録ドメイン	リスクや悪意のあるコンテンツまたは攻撃キャンペーンに使用されることが多い新規ドメイン (30 日未満)	分類し、ポリシーを適用
シンクホールへのリダイレクト	シンクホールまたはデセプションの場所に、構成可能な条件に一致するリクエストやレスポンスを送信	ポリシー アクションとして、A/AAAA レスポンスを選択した場所にオーバーライドしてシンクホール化
新たに確認されたドメイン、戦略的にエイジングされたドメイン、新たに復活したドメイン	長期間存在したのちに突然アクティブになりマルウェアや攻撃キャンペーンに悪用されるドメイン、アクティブな状態から非アクティブになり (10 日以上) その後再びアクティブになったドメイン	ドメインを分類し、ポリシーを適用
架空ドメインまたはドメイン ルックアップ	意図的に低速化された権威ネームサーバーが DNS リゾルバーに対する DoS 攻撃として機能	Zscaler Trusted Resolver の高い可用性とネームサーバーに対する保護、DNS 監視のためのクラウドベースのアーキテクチャーによる無制限の拡張性



ボットネットのコールバックや発見された / 既知の悪意のあるドメイン	指示を受けるため、またはその他の悪意のある目的で、侵害されたエンドポイントがボットネットへの接続を試行	ThreatLabz と機械学習アルゴリズム、脅威フィードの監視により、悪意のあるドメインを検出、分類、ブロック。IPS 検出を活用して C2/ ボットネット通信を特定
非標準 DNS または DNS のなりすまし	侵入やデータの持ち出し、セキュリティ回避を目的に、改ざんされた DNS トラフィック、または通常の DNS を装った非 DNS トラフィックを悪用	DNS の RFC 仕様への準拠状況を監視、DNS を装ったトラフィックを DPI ベースで検出
ドメイン生成アルゴリズム (DGA) または辞書 DGA	生成されたドメインを使用した C2 またはその他の悪意のあるアクティビティ	ボットネット、悪意のあるドメイン、フィッシング、その他のドメインまたは IP 側のカテゴリーに分類し、ポリシーを適用
不正または異常なレコード タイプ	特定のエンドポイントには特定の DNS レコード タイプが必要であるものの、すべてのエンドポイント (ユーザー、プリンター、メール サーバー) が呼び出しレコード タイプや攻撃対象領域の拡大につながり得る疑わしいレコード タイプを使用できる必要はない	任意の DNS レコード タイプに対して条件付きでアクションを実行 (通常はポリシーに組み込まれる / 例: ユーザー エンドポイントの場合は MX レコード タイプを許可する必要はない)
望ましくない A/AAAA レスポンス	リゾルバーが特定のドメイン、リクエスト タイプ、カテゴリーなどに対して、不適切な IP または不特定の IP を返す	DNS ポリシーに基づいて A/AAAA レスポンスを上書き
ファスト フラックス	ドメインと IP をすばやく入れ替え	ボットネット、悪意のあるドメイン、フィッシング、その他のドメインまたは IP 側のカテゴリーに分類し、ポリシーを適用
望ましくない国のドメイン ホスティング	危険とみなされる国でホストされているドメイン	IP に基づいて地理的情報を特定してブロック

DNS の可視化とレポート

ログとダッシュボード	定期的かつ悪意のある DNS アクティビティ、使用状況の可視化	リクエスト、レスポンス、エラー処理、通知のためのフォレンジック的に完全なログ
------------	---------------------------------	--

民間、政府機関、業界の厳格な標準に準拠



Zscaler は、CISA および NSA が推奨する Protective DNS リゾルバーへの安全な転送暗号化のすべての基準を満たしています。

- ✔ マルウェアドメインをブロック
- ✔ フィッシングドメインをブロック
- ✔ マルウェアドメイン生成アルゴリズム (DGA) への対策
- ✔ 機械学習やその他のヒューリスティックを活用して脅威フィードを増強
- ✔ コンテンツフィルタリング
- ✔ SIEM 統合またはカスタム分析用の API アクセスをサポート
- ✔ Web インターフェイス ダッシュボード
- ✔ DNSSEC を検証
- ✔ DoH/DoT に対応
- ✔ グループ、デバイス、ネットワークごとにカスタマイズ可能なポリシーを有効化

機能の概要

Zscaler DNS Security (Standard) は、Zscaler Internet Access に完全に統合された機能として、Essentials Platform (ZS-ESS-PLATFORM) と Zscaler Platform (ZS-PLATFORM) 両方のライセンスに含まれています。

高度な機能を有効にするには、ZIA-FIREWALL ライセンス (ZS-CTP-1) を追加する必要があります。このライセンスを追加すると、1,000 を超えるファイアウォール/DNS ルール、エンドポイント アプリ制御、ユーザー アイデンティティに基づくポリシー制御、カスタム ルールを備えた IPS セキュリティ、DNS トンネル保護などの機能が提供されます。

高度な機能を使用するには、少なくとも Essentials Platform と ZIA-FIREWALL (ZS-CTP-1) ライセンスが必要です。

既存のお客様 (従来の非プラットフォーム SKU を使用している場合) は、ZIA-FIREWALL ライセンスを追加するだけで Advanced Firewall にアップグレードできます。



DNS セキュリティ機能	Standard	Advanced
Zscaler Trusted Resolver (ZTR) 世界 160 拠点以上のデータ センターを基盤とし、ジオローカライズされた高速 DNS 解決を提供。ほとんどのパブリック リゾルバーよりも高速なパフォーマンスと広範なカバレッジを実現	✓	✓
DNS ポリシーとフィルタリング基準	最大 64 ルール	最大 1,000 ルール以上
ユーザーのアイデンティティ、時間、場所、送信元 / 宛先 IP アドレス (IPv6 など)	✓	✓
一般的なドメインの分類とフィルタリング (アダルト、ギャンブル、暴力など)	✓	✓
セキュリティ分類とフィルタリング (マルウェア、C2、ボットネット コールバック、DGA ドメイン、悪意のあるコンテンツ、フィッシング、新たに登録 / 確認されたドメインなど)	✓	✓
DNS リクエストの種類 : A、AAAA、MX、NS、CNAME、TXT などを含むすべての DNS 属性	✓	✓
国に基づくポリシー	✓	✓
TCP、UDP、または DNS over HTTPS の検査	✓	✓
DNS ゲートウェイを使用したフェイルオーバーによる高可用性	✓	✓
シンクホールの解決	✓	✓
ダッシュボードとレポート作成機能	✓	✓
トランザクション単位の詳細かつフォレンジック的に充実したログ記録	✓	✓
アクション : 許可、ブロック、リクエストのリダイレクト、レスポンス	✓	✓
エンド ユーザー通知 (EUN)	✓ DNS アクションの Web 通知	✓ ファイアウォール、DNS、IPS アクションに関する ZCC の通知
プロセスの精度を高めるエンドポイント アプリ制御	-	✓
クリアテキスト DNS の DNS over HTTPS (DoH) への変換	-	✓

DNS トンネルの検出と分類	-	✓
アプリケーションと DNS プロバイダーの分類 (例: Google DNS、NextDNS、DoHUnknown)	-	✓
ジオローカライズされた DNS 解決のための 構成可能な ECS インジェクション	-	✓
	Essentials Platform (ZS-ESS-PLATFORM) または Zscaler Platform (ZS-PLATFORM) ライセンスに含まれる	ZIA-FIREWALL の アドオン ライセンス (ZS-CTP-1) が必要

Zscaler について

Zscaler (NASDAQ: ZS) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™ プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 160 拠点以上のデータセンターに分散された SSE ベースの Zero Trust Exchange™ は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、zscaler.com/jp をご覧いただくか、Twitter で [@zscaler](https://twitter.com/zscaler) をフォローしてください。

© 2025 Zscaler, Inc. All rights reserved. Zscaler™ および zscaler.com/legal/trademarks に記載されたその他の商標は、米国および/または各国の Zscaler, Inc. における (i) 登録商標またはサービス マーク、または (ii) 商標またはサービス マークです。その他の商標はすべて、それぞれの所有者に帰属します。



**Zero Trust
Everywhere**