Cloudflare vs. Zscaler比較
Zero Trust、SSE、SASEとその先

比較の概要

Zero Trust（ZT）、Security Service Edge（SSE）、Secure Access Service Edge（SASE）など、ネットワークとセキュリティの革新的なトレンドを実現するCloudflareとZscalerのサービス全般の機能比較を行ったものです。37の評価ポイントを5つのグループに整理しています。インターネットネイティブネットワークプラットフォーム、クラウドネイティブサービスプラットフォーム、SASEアーキテクチャを採用するサービス、ZT、SSE、SASEとその先に拡張するサービス、ネットワークオンランプです。一部の比較はより多くの文脈と明確さを必要とするため、最終ページに脚注を付けています。

より概念的な比較に関してはcloudflare.com/products/zero-trust/cloudflare-vs-zscalerをご覧ください。

インターネットネイティブなネットワークプラットフォーム

評価ポイント	Cloudflare	Zscaler	FN
どのお客様にもご利用いただけるデータセンターシティ	270	55	1
データセンター全体で異なるクラウド（コントロールプレーン）	1	～8	2
アップタイムに関するサービスレベル契約	100%	99.99～99.999%	3
すべてのエッジサービスでシングルパスインスペクションが可能	あり	なし	4
脅威研究所	あり	あり	-

クラウドネイティブサービスプラットフォーム

評価ポイント	Cloudflare	Zscaler	FN
構成可能なアーキテクチャ	あり	なし	5
単一ペインの管理インターフェース	あり	なし	6
サーバーレスコンピューティング開発プラットフォーム	あり	なし	7
FedRAMP認証取得中または認証済み	あり	あり	8

SASEアーキテクチャを採用するためのサービス

評価ポイント	Cloudflare	Zscaler	FN
Zero Trustネットワークアクセス（ZTNA）	あり	あり	-
クラウドアクセスセキュリティブローカー（CASB）	あり	あり	-
セキュアWebゲートウェイ（SWG）	あり	あり	-
Firewall as a Service（FWaaS）	あり	あり	-
L3〜7のトラフィックアクセラレーションを使用した WAN as a Service	あり	なし	9
オンプレミスSD-WAN	なし - パートナー	なし - パートナー	10

ZT、SSE、SASE、さらにその先を拡張するサービス

評価ポイント	Cloudflare	Zscaler	FN
クラウド型メールセキュリティ（CES）	あり	なし	-
リモートブラウザ分離（RBI）	あり	あり	11
データ損失防止（DLP）	あり	あり	12
侵入検知システム（IDS）	あり	あり	13
ネットワークとアプリケーションのDDoS攻撃対策	あり	なし	14
アプリケーションセキュリティ：WAFとボット検出	あり	なし	15
アプリケーションパフォーマンス：CDN、DNS、LB	あり	なし	-
クラウドセキュリティCWPP、CPSM、CIEM	なし	あり	16
サイバーディフェンス：サンドボックスとディセプション	なし	あり	-
デジタルエクスペリエンス監視（DEM）	なし	あり	-
特権付きリモートアクセス用のブラウザ内端末	あり	あり	17
SSHコマンドのログ記録	あり	なし	-

ネットワークオンランプ

評価ポイント	Cloudflare	Zscaler	FN
クライアントレスなブラウザベースのアクセス	あり	あり	-
デバイスへのクライアントソフトウェア	あり	あり	-
アプリケーションコネクターソフトウェア	あり	あり	18
分岐可能な接続用ソフトウェア	なし	あり	19
エニーキャストDNS、GRE、IPsec、QUIC、WireGuardトンネル	あり	なし	20
データセンターおよびオフィス向けプライベートネットワーク内部接続	あり	なし	-
インバウンドIPの中継（BYOIP）	あり	なし	-
IPv6オンリーの接続への対応	あり	なし	21
再帰DNSリゾルバ	あり	あり	-
デバイスクライアントとDNSリゾルバの自由公開	あり	なし	22

比較結果

グループスコア	評価ポイント	Cloudflare	Zscaler
全体	37	32	18
インターネットネイティブなネットワークプラットフォーム	5	5	1
クラウドネイティブサービスプラットフォーム	4	4	1
SASEを採用するためのサービス	6	5	4
ZT、SSE、SASEとその先を拡張するサービス	12	9	7
ネットワークオンランプ	10	9	5

脚注（FN）

1. cloudflarestatus.comおよびcloudflare.com/networkによると、Cloudflareは、270以上の都市にパブリックデータセンターを保有しています。多くの都市が、1つ以上のデータセンターからのサービスを受けていることになります。2022年1月現在、trust.zscaler.comおよびconfig.zscaler.comによると、Zscalerは、55の都市に73のパブリックデータセンターを保有し、13のデータセンターがパブリッククラウドなし、11のデータセンターが自動ジオプロキシミティが無効になっています。その他に挙げている77のデータセンターについては、公的に文書化されておらず、また、どの顧客も利用できないようです。
2. config.zscaler.com/zscaler.net/cenrによると、ZIAには7つ、ZPAは2つ、ZDXのような他の製品にはさらに多くの異なるクラウドがあるとされています。
3. ほとんどのサービスは稼働率を99.999%とするSLAでサポートされていますが、同社のDNSリゾルバーは稼働率を99.99%とするSLAしか提供されていません（出典）。
4. 例えば、プライベートセルフホストアプリケーションに対するリモートユーザーからのリクエストは、同一データセンター内にある同一のサーバーで、SWG、RBI、ZTNA、アプリセキュリティサービスによって一度に検査することが可能です。
5. コンポーザブルアーキテクチャーでは、プラットフォームで提供されるあらゆるサービスを任意の順序で採択できるとともに、これまでに導入済みのサービスと同時に相互運用が可能である必要があります。Zscalerでは、そのサービスのいくつかを独自のアーキテクチャで個別に実行するように設計されているため、このようなコンポーザブル性が損なわれており、Zscalerの記事でも、そのことが示されています（出典 1、出典 2）。
6. Cloudflareは、2022年4月にArea 1を買収しています。Area 1のメールセキュリティ管理をCloudflare Zero Trustの管理インターフェイスに統合するというものがロードマップに組み込まれています。Zscalerはメールセキュリティを提供していないため、このギャップは同等ではありません。しかし、Zscalerは、ZIAやZPAサービス、RBIなどのアドオンの多くに個別の管理インターフェイスがあります。
7. Cloudflare Zero Trustは、Cloudflare Workersをベースに、当社のエッジでV8の分離技術を搭載して構築されています。Zscalerは古いコンテナベースのアーキテクチャを使用しているため、開発に時間がかかり、新機能を提供する際のオーバーヘッドコストが余分にかかります。
8. 2022年6月現在、CloudflareはFedRAMPの段階がIn Progress（審査中）であるのに対し、ZscalerはAuthorized（認定）です。
9. Zscalerは、自社のネットワークバックボーン上でデータセンターからデータセンターへのトラフィックのスマートなルーティング、高速化できるとは主張していません。
10. Zscalerは分岐可能な接続用ソフトウェアを提供していますが、オンプレミスのSD-WAN機能を完全には提供しておらず、WANエッジインフラストラクチャに関するアナリストの調査にも登場していません。
11. Zscalerの標準的なRBI技術がピクセルのストリームを送信するのに対し、Cloudflareの特許取得済みネットワークベクターレンダリング技術は描画コマンドのストリームを送信します。また、2022年6月現在、Zscalerは4つのデータセンターでRBIを稼働させているのみです。これらの複合的な要因から、多くのインターネットやSaaSアプリケーションのユーザーエクスペリエンスを低下させています。
12. 2021年以降、Cloudflareは当社のZero Trustプラットフォーム内に、ネイティブにDLPサービスを構築してきました。2022年7月には、プライベートベータを開始しました。詳細を知りたい方はウェイトリストにご参加ください。パブリックベータは8月の開始を予定しています。
13. Cloudflare侵入検出は、現在プライベートベータプログラムでご利用いただけます。参加をご希望される方は、担当のアカウントチームまでお問い合わせください。
14. Zscalerには、DDoS対策サービスの提供はありません。すべてのクラウドネイティブサービスプロバイダーは、そのアーキテクチャに何らかのDDoS攻撃対策を組み込んでいますが、これでは最新のDDoS攻撃を効果的に軽減することはできません。Zero Trustを導入することで、アプリケーションがインターネット上に直接さらされることはなくなりますが、アクセスを許可された契約者や他のユーザーによってZTNAプロバイダーのネットワークを通じて行われるアプリケーションの攻撃を阻止することはできません。
15. 2022年3月、ZscalerはZTNAの提供する「ZPA」にインラインアプリケーション保護を追加したと発表しました。しかし、これはパブリックとプライベートの両方のアドレス指定可能なアプリケーションのための完全なWebアプリケーションファイアウォール（WFA）と同等なものではありません。また、ボット検出機能も不足しています。
16. 2020年から21年にかけて、Zscalerはクラウドワークロード保護プラットフォーム（CWPP）のEdgewise Networks、クラウドセキュリティ動態管理（CSPM）のCloudneeti、クラウドインフラエンタイトルメント管理（CIEM）のTrustdomeを買収しました。同社はこれらのクラウドセキュリティサービスを、Zero Trustサービスに統合していません。
17. CloudflareはSSHとVNCのブラウザ内端末を、ZscalerはSSHとRDPのブラウザ内端末を提供しています。Cloudflareの多くのお客様は、ブラウザでRDPを実行するためにApache Guacamoleを使用しています。
18. Zscalerはイメージを実行するため、仮想マシン用のインフラストラクチャを必要としますが、Cloudflareは仮想マシンの有無に依存しない実行可能なデーモンを提供します。
19. Zscalerは、そのイメージを実行するために仮想マシン用のインフラストラクチャを必要とし、トラフィックはZIAまたはZPAのどちらか一方を通過するだけで、両方を一度に通過させることはできません。
20. ZscalerはDNSの解決でのみAnycastをサポートしています。GREまたはIPsecトンネル用に、お客様は一意のIPアドレスをZscalerデータセンターごとに使用する必要があります。また、アプリコネクタとデバイスクライアントは、非AnycastのDTLSトンネルに依存しています。
21. Zscalerのデバイスクライアントは、同社のコミュニティフォーラムによると、IPv6オンリーの接続には対応していないとされています（出典）。
22. Zscalerは、無料のパブリックDNS解決（例：1.1.1.1）や暗号化IP通信（例：WARP）を提供していません。