CLOUDFLARE

電子書籍

CISO向けSASE採用ガイド

高優先度のユースケースでSASEプラットフォームを評価する方法

サイバーレジリエンスを実現する使命

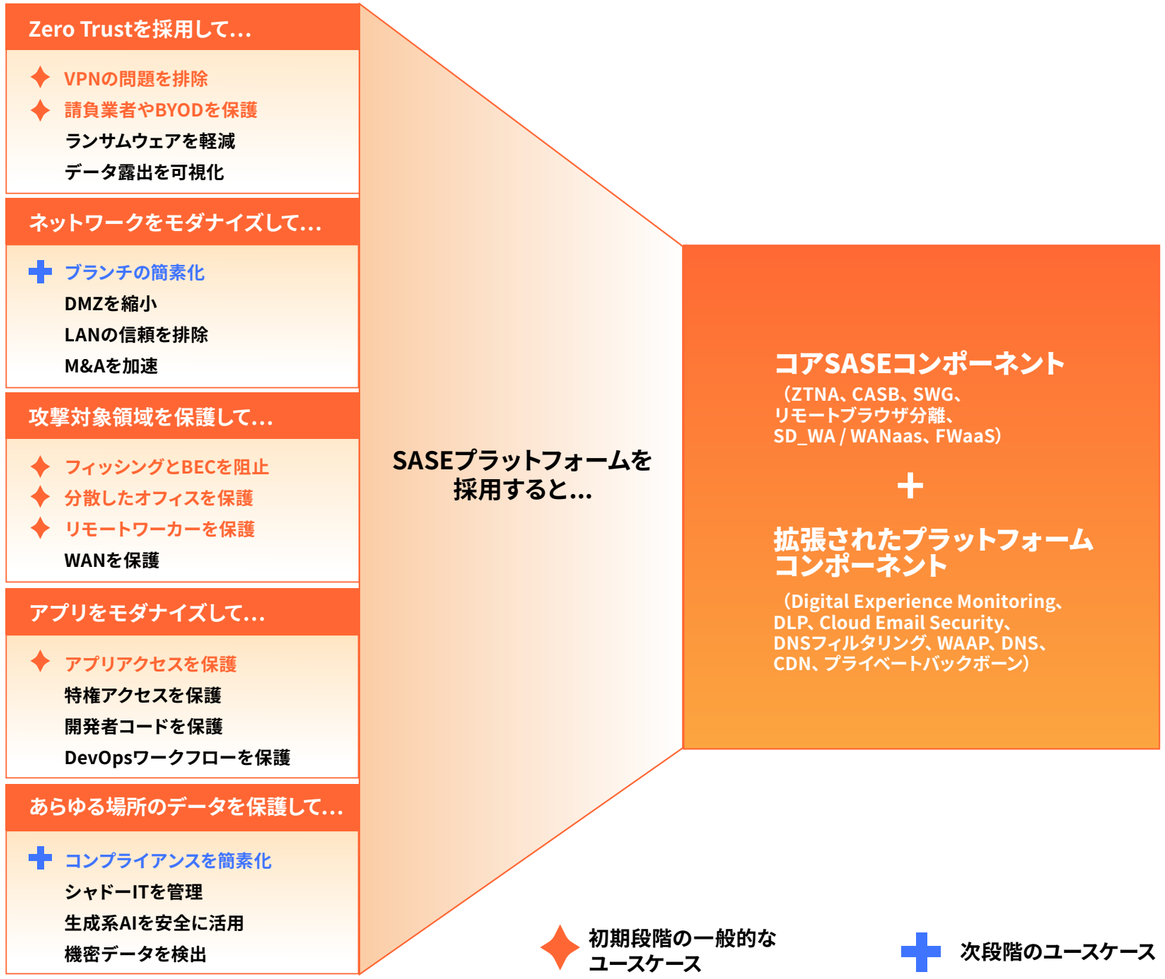
米国国立標準技術研究所（NIST）は、サイバーレジリエンスを、サイバーリソースを使用する、またはそれによって可能になるシステムの悪条件、ストレス、攻撃、侵害を予測し、耐え、回復し、適応する能力と定義しています。

ただし、漏洩軽減コストを削減しつつ、サイバーレジリエンスを強化するためには、いくつかの課題があります。

- **サイバー犯罪者の手口は進化し続けている：**攻撃者がより高度なツール、技術、手順を開発するにつれ、企業が脅威の状況を保護することはますます困難になっています
- **IT環境は一層複雑化：**マルチクラウドアーキテクチャに接続するデバイスとアプリケーションの数が豊富なため、それらの環境の保護はコストがかかる複雑なプロセスになっています
- **社内チームが過負荷状態：**予算がひっ迫し、社内チームが過負荷状態になるにつれて、企業はリソースの制約に直面する可能性があります

これらの課題を克服するために、多くのCISOは、セキュアアクセスサービスエッジ（SASE）フレームワークに注目しています。従来のネットワーキングのアプローチとは異なり、SASEアーキテクチャは、セキュリティとネットワーキングを1つのクラウドプラットフォームに統合し、一貫した可視性とコントロールを実現します。SASEは、企業のデータセンターではなく、クラウドエッジにネットワーク制御を配置することで、企業は場所に関係なく、あらゆるユーザー、アプリ、デバイス、ネットワークに簡単かつ安全なアクセスを提供できます。

このガイドでは、サイバーレジリエンスを強化し、短期間で成果を上げるために、SASEの最も一般的なユースケースを取り上げ、SASEの導入を開始するための主なステップを説明します。



ユースケース#1：

Zero Trustネットワークアクセス（ZTNA）の導入

ハイブリッド型の勤務形態、マルチクラウド環境、非管理デバイスのために従来の境界ベースのセキュリティに依存すると、企業は制限された可視性、構成の矛盾、過剰なリスクに悩まされます。きめ細かいアクセス制御によって、どのエンティティもデフォルトで信頼されないようにするZero Trustのアプローチは、次のようにセキュリティ戦略の最新化に役立ちます。

従来のハードウェアベースセキュリティの代替

仮想プライベートネットワーク（VPN）などの従来のネットワーク境界制御は、スケーリングが難しく、可視性に影響し、セキュリティチームが攻撃を発見して修復することが困難な場合があります。SASEモデルは、Zero Trustネットワークアクセス（ZTNA）を導入することにより、安全な代替手段を提供します。また、グローバルクラウドネットワーク全体でネットワークトラフィックをルーティングして処理することで、エンドユーザー間の摩擦とラテラルムーブメントの両方を軽減するのに貢献します。

デバイスへのアクセス管理

請負業者、代理店、サプライヤーなどのサードパーティユーザーにアクセス権を提供すると、企業が誤って権限を過剰にプロビジョニングしたり、管理対象外のデバイスへのアクセスを許可したりする場合にリスクが生じる可能性があります。SASEを採用すると、企業はクライアントレスZero Trustポリシーを設定できます。これにより、サードパーティユーザーは必要なコンテンツにだけアクセスできるようになります。

ランサムウェアの攻撃を防ぐために

ランサムウェアは、ネットワーク全体に急速に広がる可能性があり、場合によっては、複数のネットワークや組織に広がることもあります。SASEは、感染が検出されるとすぐにネットワークとアプリケーションのアクセスを無効にすることで、ランサムウェア攻撃の拡大を防止します。「最小特権アクセス制御」というZero Trustの原則に支えられ、このアプローチは、攻撃者による権限の昇格とネットワーク内でのラテラルムーブメントを困難にします。

データ露出の制限

許可済みおよび無許可のアプリケーションでユーザーが機密情報をアップロードしたり配布したりすると、データの漏洩と流出が企業に深刻な脅威をもたらす可能性があります。SASEのZero Trustポリシーは、各ユーザーがアクセスできるアプリケーションを制限するとともに、一般的なSaaSスイートをスキャンして、機密データや設定ミスを検出することで、データの漏洩を防ぎます。

導入事例

Zero Trustの導入

Fortune500に名を連ねる電気通信プロバイダーは、AWS、Azure、その他のクラウド環境でホストされた数百のアプリケーションにおいて、10万人を超える従業員のハイブリッドワーク環境を保護するために、CloudflareのSASEプラットフォームを使用しました。IDベースのZero Trustネットワークアーキテクチャ、セキュアWebゲートウェイ、統合型アクセス制御によって、複数のポリシー構築対応インターフェース、VPN、インターネットフィルタリングサービスを操作する必要なく、ユーザーを脅威から保護することができました。

ユースケース#2

攻撃対象領域を保護

デジタルトランスフォーメーションとリモートワークにより、攻撃対象領域は拡大し、内部リソースへのアクセスを必要とするユーザーの分散と非管理デバイスが増えています。しかし、オンプレミスのファイアウォールをクラウドに拡張したり、VPN経由でネットワークをスケーリングしたりすると、外部および内部の脅威への露出が増え、同時に可視性も低下する可能性があります。SASEアーキテクチャを導入すると、企業は「ペリメータレス」モデルをサポートするために可視性と制御を拡張し、次の方法で一貫した保護を適用することができます。

マルチチャネルフィッシングの回避

攻撃者は、ユーザーがクリックする場所の周りの警戒を下げがちなチャネルにフィッシング攻撃を仕掛けることが多く、特に狙われやすいのは、メールセキュリティ対策で通常は保護されないツールです。統合されたSASEプラットフォームにより、すべての環境で包括的な保護が可能になり、資格情報の窃取、アカウント乗っ取り、データ流出のリスクを軽減できます。

リモートワーカーの防御

リモートワークでは、ユーザーは複数の場所やデバイスから接続する必要がありますが、ユーザーを雇用する企業の目の届かないところで接続するケースが多いです。SASEアーキテクチャを導入すれば、企業は重要な環境とデータへの従業員やサードパーティのアクセスを保護でき、安全で生産的な「場所を選ばない働き方、どこでも勤務」のアプローチの実現に役立ちます。

ユーザーエクスペリエンスの向上

オフィスのトラフィックをスクラブ（浄化）する従来のアプローチでは、トラフィックを集中管理された企業のデータセンターにバックホールする必要があるため、遅延の発生や生産性の低下を招く可能性がありました。しかし、その代わり、ユーザーにインターネットへの直接アクセス権を与えることで、セキュリティリスクが生じ、一貫性のないユーザーエクスペリエンスが生じます。SASEは、あらゆるクラウドやインターネットへの直接接続をインテリジェントに管理・最適化し、可能な限りエンドユーザーに近い場所でポリシーと保護を適用します。

ワイドエリアネットワーク（WAN）の保護

一部のWANは、支店間のトラフィックのクラウドセキュリティをバイパスするため、セキュリティサービスとソフトウェア定義型WAN間の統合に関する要求は、当初の想定通りにならない可能性があります。SASEを導入すると、企業はオフィス、データセンター、パブリッククラウド、広範なインターネット内外のその他のロケーション間のトラフィックをフィルタリングし、検査することで、WAN経由の接続を簡素化し、安全性を確保することができます。

導入事例

拡大する攻撃対象領域の保護

Werner Enterprisesは、クラウド移行中、重要なビジネスやカスタマーサービスを中断することなく、シームレスにSASEサービスをデプロイしました。デプロイ後、同社は悪意のあるメールを50%以上削減するとともに、手作業によるメールトリアージ作業を1日数時間程度にまで抑えることができました。このため、同社のセキュリティチームは、より戦略的なビジネス目標に集中することができました。

ユースケース#3

あらゆるところでデータを保護

データがより多くの環境に分散するに伴い、企業はデータの追跡が困難になることが多いです。認可されていない生成AIやシャドーITを使用することで機密データが開示されると、セキュリティ侵害やデータ漏洩につながり、修復に費用がかかる可能性があります。SASEは、Web、SaaS、プライベートアプリケーション環境におけるデータの可視性と制御を統合し、企業が以下を実現できるよう支援します。

データプライバシー規制コンプライアンスの簡素化

大規模言語モデル（LLM）やその他のAIツールの台頭により、ユーザーデータを保護するためのコンプライアンス基準も進化する必要があります。SASEは、データ管理を統合することによってデータの安全性とプライバシーを確保します。これにより、セキュリティチームは規制対象のデータクラスをロックダウンし、侵害のリスクを軽減して、厳格なデータ要件への継続的なコンプライアンスを保証することができます。

生成系AIを安全に使う

より多くの企業がAIを導入するにつれ、機密データが流出するリスクも高まります。セキュアWebゲートウェイとインラインクラウドアクセスセキュリティブローカーを備えたSASEアプローチを導入すると、セキュリティチームはAIアプリケーションの使用を検出して承認したり、データ漏洩のリスクを負う不適切な設定をスキャンしたり、分離されたWebブラウザでAIアプリを実行してデータの入出力を制限したりすることができます。

シャドーITの管理

シャドーITは、それを使用する組織によって管理または保護されていない無許可アプリケーションであり、機密データがそれらの場所に移動したり経由したりする際にリスクをもたらす可能性があります。SASEは、インラインクラウドアクセスセキュリティブローカー（CASB）を介してトラフィックをプロキシサーバーに送ることでこのリスクを最小限に抑え、すべての接続とリクエストを記録して無許可のアプリケーションの存在を明らかにし、企業がそれらのアプリへのアクセスと使用方法を制御できるようにします。

機密データの保護

SASEアーキテクチャを導入すると、企業は機密データがIT環境に出入りする様子を検出して制御することができます。これには、アプリのスキャンと規制対象の個人データや知的財産のトラフィック検査、フィッシングやランサムウェアなどのインターネット脅威のブロック、データの窃取や不慮の漏洩に対する追加の保護実装などが含まれます。

導入事例

あらゆるところでデータを保護

Applied Systemsは2,500名を超える従業員のセルフホスト型アプリケーショやインフラへのアクセスを保護するために、SASEサービスを導入しました。この新しいアプローチにより、同社のセキュリティチームは、ユーザーのさまざまなニーズに応じて厳格な制御を適用できると同時に、データがAIツールとどのように共有されるかを制御できるようになります。

SASEソリューションの選択：

シングルベンダー統合 vs. マルチポイントソリューション

シングルベンダー型SASEプロバイダーは、ネットワーク機能とセキュリティ機能を単一のクラウド配信サービスに集中させます。これにより、企業はさまざまなポイント製品を統合し、アプライアンスを排除して、一貫したポリシーを確実に適用することができます。マルチベンダー型SASEの導入は、単一ベンダーアプローチと同様の結果をもたらす場合もありますが、複雑度とコストが増大し、内部の可視性と柔軟性が低下することが多いです。

これらの機能を統合プラットフォームに一元化することで、SASEの真の目的を達成できます。それは、総所有コストを削減し、変化するビジネスニーズに容易に適応できる、簡素化された効率的なネットワークおよびセキュリティインフラストラクチャの実現です。

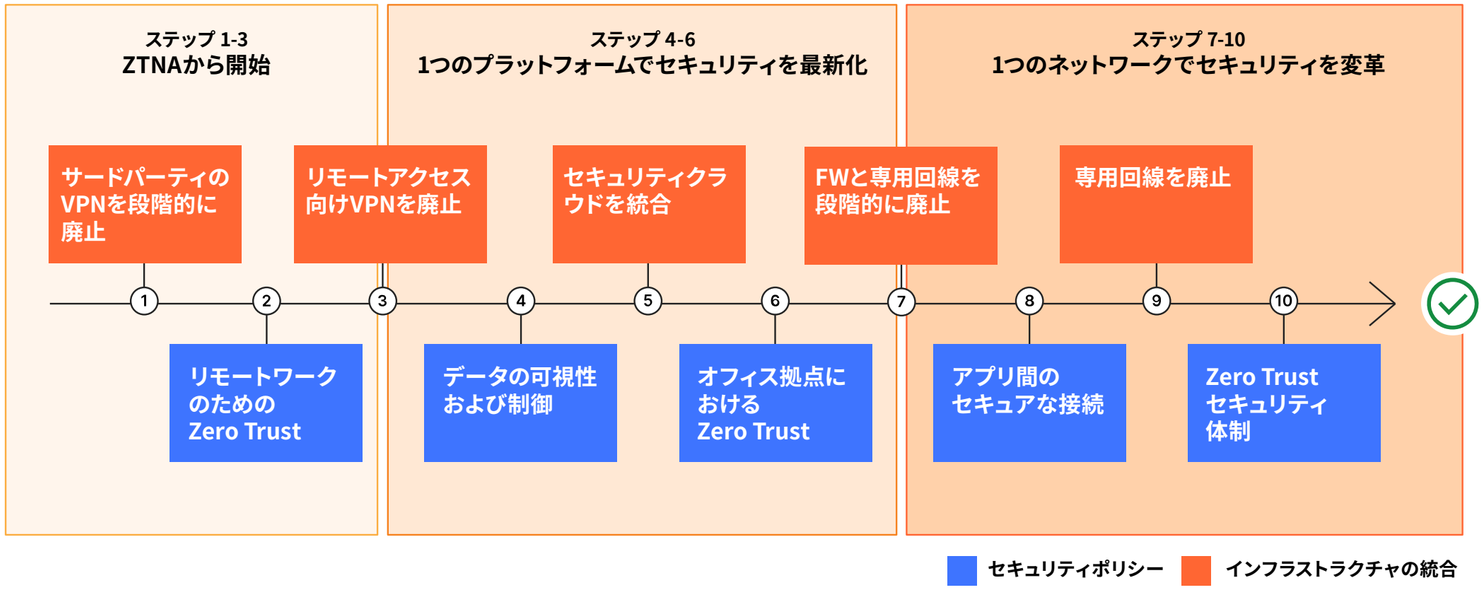
SASEプロバイダー候補を評価する際に問うべき質問：

1. アプリケーショントラフィックは、脅威および機密データ検出エンジンによって、シングルパスで復号化および検査されるか？デプロイメントに関する補足説明はあるか？
2. SaaSスイートを介したすべてのデータフローと通信は、全チャネル（インラインおよび帯域外のWebおよびメールアクティビティ）において保護されるか？
3. リモートブラウザ分離はすべてのユーザーとアプリに対して有効になっているか？これにより生産性にどのような影響があるか？追加料金はかかるか？
4. ネットワークオンランプに基づいてバイパスされるセキュリティ機能はあるか？
5. マルチテナントクラウドアーキテクチャ全体で、顧客のトラフィックが分離され、非公開の状態が維持されることを保証できるか？
6. どのようなデータローカライゼーション機能を利用できるか？データローカライゼーションを有効にすると、ローカライズされた地域外に接続するリモートユーザーに遅延が発生するか？
7. 脅威インテリジェンスフィードをアーキテクチャに統合できるか？プラットフォームは脅威インテリジェンスフィードからの誤検知をどのようにして減らすのか？
8. どのようなユーザー/デバイスリスクスコアリングとアナリティクスを利用できるか？リスクスコアをすべてのアプリケーションに均一に適用できるか？

CloudflareがSASEを提供する方法

統合型SASEプラットフォームへの移行を完了するために、多くの企業がCloudflareを信頼しています。Zero Trustネットワークアーキテクチャの構築から着手し、当社のプラットフォーム全体にIDとコンテキストベースの接続を一貫して組み込むことができるSASEプロバイダーは、Cloudflare以外にありません。

完全なSASEアーキテクチャに向けた長期的ロードマップは、以下の例に似たフローに従うかもしれません。



Cloudflareは、世界310以上の都市にまたがるグローバルネットワークによって支えられ、CISOがエンタープライズグレードのセキュリティ、レジリエンス、パフォーマンスを実現できるよう支援します。当社のシングルコントロールプレーンは、複数のセキュリティドメインにまたがりポイントソリューションを統合するため、企業はセキュリティ運用を簡素化し、進化する脅威に対して一貫した保護を確保することができます。

CloudflareおよびCloudflare SASEプラットフォームの詳細については、当社のWebサイトをご覧ください。

メール：enterprise@cloudflare.com
ウェブサイト：cloudflare.com/ja-jp