SSEソリューションの選択時に避けるべき7つの落とし穴

セキュリティサービスエッジ (SSE) を、ゼロトラストの基盤上に構築

著者紹介:
Sanjit Ganguli
Zscalerトランスフォーメーション戦略主任/フィールドCTO

Nathan Howe
Zscalerエマージングテクノロジー＆５G主任

提供:
zscaler

SSEソリューションの選択時に避けるべき7つの落とし穴

目次

SSEとはどのようなもので、なぜそれが大切なのか？

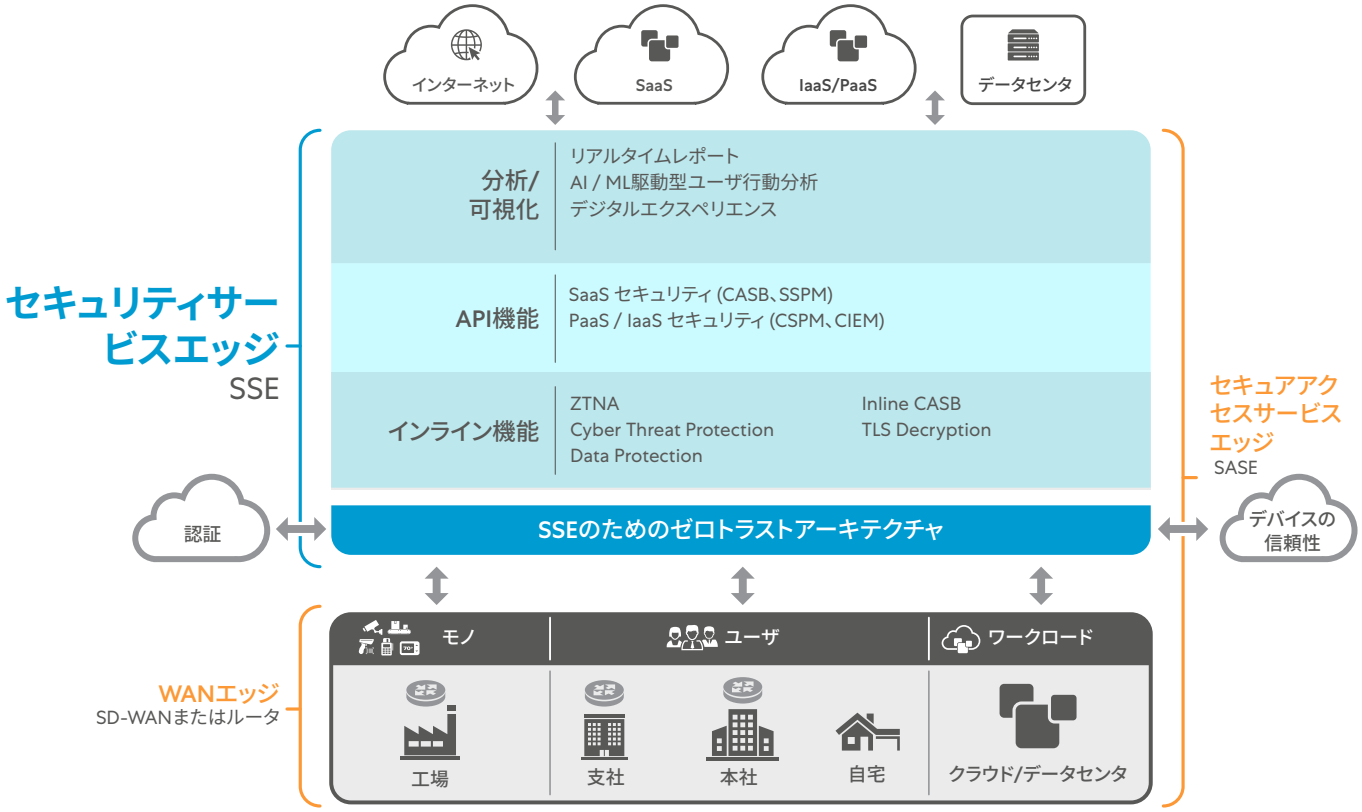


図1: SASE（Secure Access Service Edge）フレームワークは、ポリシーの決定と施行のためにSSEを含んでいます。
SASEは、要求元のエンティティからポリシーが適用されるセキュリティエッジまで、専用の接続ソリューションを使用する必要があります。

SSE（Security Service Edge）は、SASE（Secure Access Service Edge）フレームワークのコンポーネントとして、ポリシーの決定と執行を行うGartnerの仕様です。SSEは、統合および簡略化されたクラウド提供のセキュリティと接続性を約束します。

アーキテクチャがシンプルであることは、企業にとって常にメリットとなりますが、特にそのシンプルさが技術的負債を最小化し、ビジネスを加速させます。しかし、多くの組織では、セキュリティは不便なもので、ボトルネックを生む障害物、　敏捷性を制限する門番的存在、ビジネスの成功の妨げとなるものと見なされています。SSEは、そうした固定観念に対抗するものです。SSE環境では、セキュリティは保護と制御を提供し、ビジネスの進展を可能にします。

いくつかの背景を紹介すると、2019年に発表されたSASEフレームワークは、主にクラウドとモビリティの採用によって推進されるデジタル化の動きに企業を導くことを目的としています。SASEは、ネットワークアクセスとセキュリティを融合し、（高度に分散された）クラウドエッジから両方にサービスを提供します（図1参照）。このように、SASEは、セキュリティがもはや中央集権的ではなく、どこからでも安全な接続ができることを保証します。

携帯電話がさまざまな携帯/ワイヤレスネットワークに接続する方法を考えてみましょう。専用のネットワークルーティングソリューションがないにもかかわらず、ユーザは送信元と送信先の間のトラフィックに対してセキュリティ制御を要求します。同様に、企業のトラフィックを保護する場合、ユーザが接続するエッジ、ネットワーク、ロケーションは重要ではありません。SSEはこれを実現します。

サイバーセキュリティ企業は、すぐにSASEの流行に乗りました。一部のマーケティング担当者は、ブランディングのためにこの言葉をシニカルな形で流用し、SASEへの「アクセス」をすることが自社をSASE準拠（または競合他社を非準拠）にするとうそぶきました。つまり「私はネットワーク機能を持っているからSASEであり、ネットワークルートを構築していないあなたはSASEではない」という具合です。

図2: モバイルとクラウドの世界のために、エッジでポリシーベースの検証済みエンティティ間アクセスを提供します。SSEは、ファイアウォールやVPNを無効にしながら、パフォーマンスを犠牲にすることなく、エッジでユーザにセキュリティを提供することができます。

SSEは、企業のトラフィックを保護するために使用されるSASEサービス群のことを指します。SSEは、正しいユーザ（またはワークロード）が、安全かつ企業のIT管理の下で、正しいアプリケーションとサービスにアクセスすることを保証しますが、これらのサービスは、IaaSやPaaSのワークロード、SaaSアプリケーション、またはLinkedInやYouTubeなどのインターネットサービスです。サービスアクセスは、Zero Trust Access (ZTA) コントロールに従って許可されなければなりませんが、回避すべき落とし穴 その2 で詳しく説明されています。

これらの高い目標を達成するために、SSEソリューションプロバイダーは、一貫したポリシー、ゼロトラストアクセス、高速なデジタルクスペリエンスを提供する、グローバルで可用性の高い、スケーラブルでネットワークに依存しないソリューションを提供する必要があります。

このような機能性と可用性がなければ、SSEソリューションはユビキタスな保護と可用性を実現できません **(図2参照)。** SASEとは異なり、SSEは接続やアクセス方法を規定するものではなく、どのようなネットワーク上でも動作し、認可されたサービスがどこにあろうと、そのサービスに対して制御を提供することを前提としています。

SASEの理想は、接続性と保護性を融合させることですが、企業環境では、エンドユーザの従業員にとって透過的でなければ、その組み合わせはうまくいきません。ユーザからアプリケーション、アプリケーションからアプリケーション、ワークロードからワークロードなど、何から何まで、接続はダイレクトに行われます。ユーザは、「ああ、ネットワークに接続しないと仕事ができないんだ」と思うべきではなく、むしろ、「今、仕事を終わらせてしまう」ということに集中できるべきなのです。

この統合された理想は、従来のネットワークとセキュリティのインフラに依存する企業環境では、単純に達成することができません。この古いアーキテクチャモデルでは、セキュリティは一元管理され、データトラフィックは場所（リモートや支店など）、ソース（ユーザ、アプリ、ワークロードなど）、宛先（インターネット、クラウド、データセンタなど）に関係なく、まず企業ネットワーク経由でハードウェアアプライアンスベースのセキュリティコントロールの物理的な場所に接続、ルーティング（およびスルー）されなければなりませんでした。

SSE主導のデジタルトランスフォーメーションがもたらす真のビジネスバリュー

SSEの導入には、企業のデジタル変革が大きく必要となる場合があります。しかし、その変化を受け入れることで、目に見える効果を得ることができます。

管理：

SSEはゼロから始まります。SSEは、人、マシン、ワークロード、ネットワーク、エッジのそれぞれを検証します。行動分析学によって提供されるコンテキストと組み合わされた正しい識別がなければアクセスはできないため、企業にとっては何がまたは誰が社内サービスにアクセスするのかを管理できるようになります。

ダイレクトな接続：

SSEポリシーの施行は、発信元エンティティと宛先サービスの間のインラインに存在します。アクセスの判断は、ネットワークレベルではなく、アプリケーション単位で行われます。

ビジネス主導のセキュリティ：

どのエンティティがどのサービスに接続できるかというポリシーは、最小特権を使用して定義されます。ユーザ、マシン、ワークロードなどは、接続を許可されたものだけに接続でき、それ以上には接続できず、他の接続は一切できず、他のアクセスもブロックされます。

グローバルな施行：

SSEは、ポリシー、インサイトエンジン、外部学習（脅威の監視、偽装など）から得られるコンテキストに基づき、あらゆるエンティティがアクセス経路に制御を適用できるよう、グローバルな施行が可能である必要があり、これは企業の要件に合わせて拡張する必要があります。

総合的：

SSEは、トラフィックを大規模かつ詳細に検査するための完全なインライン評価を提供します。SSEは、高度な脅威からの保護、企業資産（クラウドとそれ以外）の防御、データ損失の防止、インライン制御の確保を実現します。必要に応じて、クラウドサービス内に保存されたコンテンツの制御を提供する必要があります。

攻撃対象領域の排除：

SSEは、攻撃対象領域を取り除くことで、企業資産への不要なアクセスや暴露を防ぎます。アクセスできないものを攻撃することはできません。

どこからでも：

SSEは、この接続性を企業のあらゆる部分に、どこからでも提供します。SSEは、ワークロード、モノ、マシンがコントロールを失うことなく移動、再配置、変換できるようにしながら、柔軟なユーザベースを保護し、接続します。

SSEは、優れて総合的な方法でビジネスの安全を確保するだけで、組織に変化をもたらす触媒となることができるのです。しかし、すべてのソリューションが同じように作られているわけではありません。SSEの導入を検討しているITリーダーは、組織がセキュリティを簡素化できるような適切なソリューションを評価し、選択する必要があります。

SSEへの企業デジタル変革の道のりで避けるべき7つの落とし穴があります。このような失敗を避けることで、ITリーダーはSSEの価値提案を実現するために適切なサービス、アーキテクチャ、機能を選択することができます。この道のりは、ネットワークに固定したり、サービスへの総合的なアクセスを許可したりするような、ビジネスのニーズを満たすための変革能力を制限する「古いやり方」からの脱却となるものです。

落とし穴 その1:
パフォーマンスと可用性を高めるグローバルなクラウドプラットフォームでの運用実績がないSSEソリューションを選択する

落とし穴 その2:
Zero Trust Architectureの基礎の上に構築されていないSSEソリューションを選択する

落とし穴 その3:
高度な脅威防御とDLPを約束する一方で暗号化トラフィックを大規模に検査できないSSEソリューションを選択する

落とし穴 その4:
柔軟性、拡張性、多様性を備えた展開および管理オプションがない「画一的」なSSEソリューションを選択する

落とし穴 その5:
アプリケーション接続を最適化したり、特定したりしないため、ありきたりのユーザエクスペリエンスしか提供できない**SSE**ソリューションを選択する

落とし穴 その6:
サードパーティベンダーのエコシステムとの統合やオーケストレーションが限定的なSSEソリューションを選択する

落とし穴 その7:
本番環境パイロットで価値を発揮しにくいSSEソリューションを選択する

どのような人が対象となるか？

SSEへの移行は、単なるセキュリティの変革ではなく、**セキュリティアーキテクト**以外にも関わってきます。この e-bookで説明するベストプラクティスは、**セキュリティアーキテクト**、**ネットワークアーキテクト** 、**企業アーキテクト** 、**クラウドアーキテクト** **アプリケーションアーキテクト**を対象としています。

その1
落とし穴

パフォーマンスと可用性を高めるグローバルなクラウドプラットフォームでの運用実績がないSSEソリューションを選択する

代わりに、以下のようなSSEソリューションを検討してください。

- SLAで保証されたパフォーマンス、可用性、スループット、機能を備えた、多様でグローバルな公共サービスポリシー実施エッジを提供している。このソリューションでは、お客様の拠点ごとにポリシーを適用します。
- 高水準の耐障害性、インフラ、地理的多様性、機能的能力、最適なユーザエクスペリエンスを備えたクラウドである。SSEサービスは、マネージドクラウドやDCプロバイダーの上で実行されるサービスではなく、キャリアニュートラルなデータセンタでインラインで提供されます。
- 顧客リファレンス、履歴レポート、サードパーティ認証、外部のオープンソースデータリポジトリによって検証された、確かな実績と透明性の高い規模、成長、配信の系統を持っている (https://www.peeringdb.com/org/12297)。

正しいSSEベンダーはこれをどのように実現するのか

何十億ものトランザクションに対応するマルチテナントのSSEプラットフォームの構築と運用は、コンピュータのレベルをはるかに超えるものであり、簡単なことではありません。SSEソリューションは、お客様の企業の保護、接続、実現に委ねられるため、組織のあらゆる部分に均一かつタイムリーにSSEサービスのセットを提供しなければなりません。

正しい SSE ソリューションは、グローバルに分散したサービスを通じて企業にサービスを提供します。アーキテクチャ上、最も効果的な配信方法は、プロキシベースのサービスを介して行われます。ネットワークの状態に固定されないプロキシサービスは、SSE をアプリケーションアクセスに配信することに重点を置き、規模に応じた検査などの洞察を、追加のプラットフォームにオフロードすることなく、より深く理解できるようにします **(落とし穴 その3を参照)**。

真のプロキシアーキテクチャは、現代の企業のスケール要件を達成するために、多大なR&Dの努力と何年もの改良を必要とすることに留意してください。適切なSSEソリューションには、プロキシアーキテクチャが拡張可能であることが示された大規模な導入事例が多数あるはずです。

このサービスは、企業のあらゆるデータ伝送機能が保護される、統一されたポリシーエッジのセットを通じて提供されなければならず、それは単にノード数ではなく、顧客が必要とするサービスを提供するSLA保証サイト数であるべきです。SSEプロバイダーは、ピアリングの不備やその他の理由でその地域のSLAを保証できない場合、パブリックPOPを提供するべきではありません。

SSEを採用することは、企業のセキュリティ、接続性、制御を信頼できるセキュリティベンダーに集約し、活性化し、責任を分担することを意味します。この共有モデルにより、ユーザ、ワークロード、サービス、支店などの保護と接続を実現する手段が簡素化されます。SSEプロバイダーは、定義された実証済みのSLAを提供し、企業の機能を確保すると同時に、保護を提供する必要があります。

企業向けサービスが接続する際、接続先の機能を消費するための効果的な経路が必要です。これは、キャリアニュートラルなデータセンタ内で非常に効果的なピアリングを行うSSEソリューションによってのみ達成できるものです。そのため、送信元や送信先の場所に関係なく、送信元と送信先の間のインラインで制御を行う必要があります。

セキュリティサービスを中央演算クラウド（多くの場合ハイパースケーラ）内でホストし、図3 に示すような入口ゲートウェイを持つソリューション（しばしばオンランプサービスと呼ばれる）は、分散した入口エッジに依存しますが、ポリシー制御とアプリケーションを集中的に処理するので、不要な遅延が生じ、ユーザエクスペリエンスが損なわれる結果となります。

SSEベンダーは、完全かつ大規模でスケーラブルなクラウドプラットフォームを実証している必要があります。SLAにとどまらず、SSEプラットフォームは、スケーラビリティ、安定性、可用性、地理的配置などのエビデンスを提供する必要があります。このレビューを検証するために、公に提供された過去のデータを参照し、既存の顧客に話を聞き、その経験を理解します。

ユニフォームエッジポリシーの実施

SSEベンダーの一連のサービスエッジは、ポリシーエンフォースメントを提供する必要がありますが、規模の大きいクラウドベースのネットワークへの接続性のエッジにはなり得ず、中央執行インフラへのトラフィック経路もしくは「オンランプ」に限られます。 このような仕組みは、高効率で低遅延のサービスを提供するという目的を達成できません。

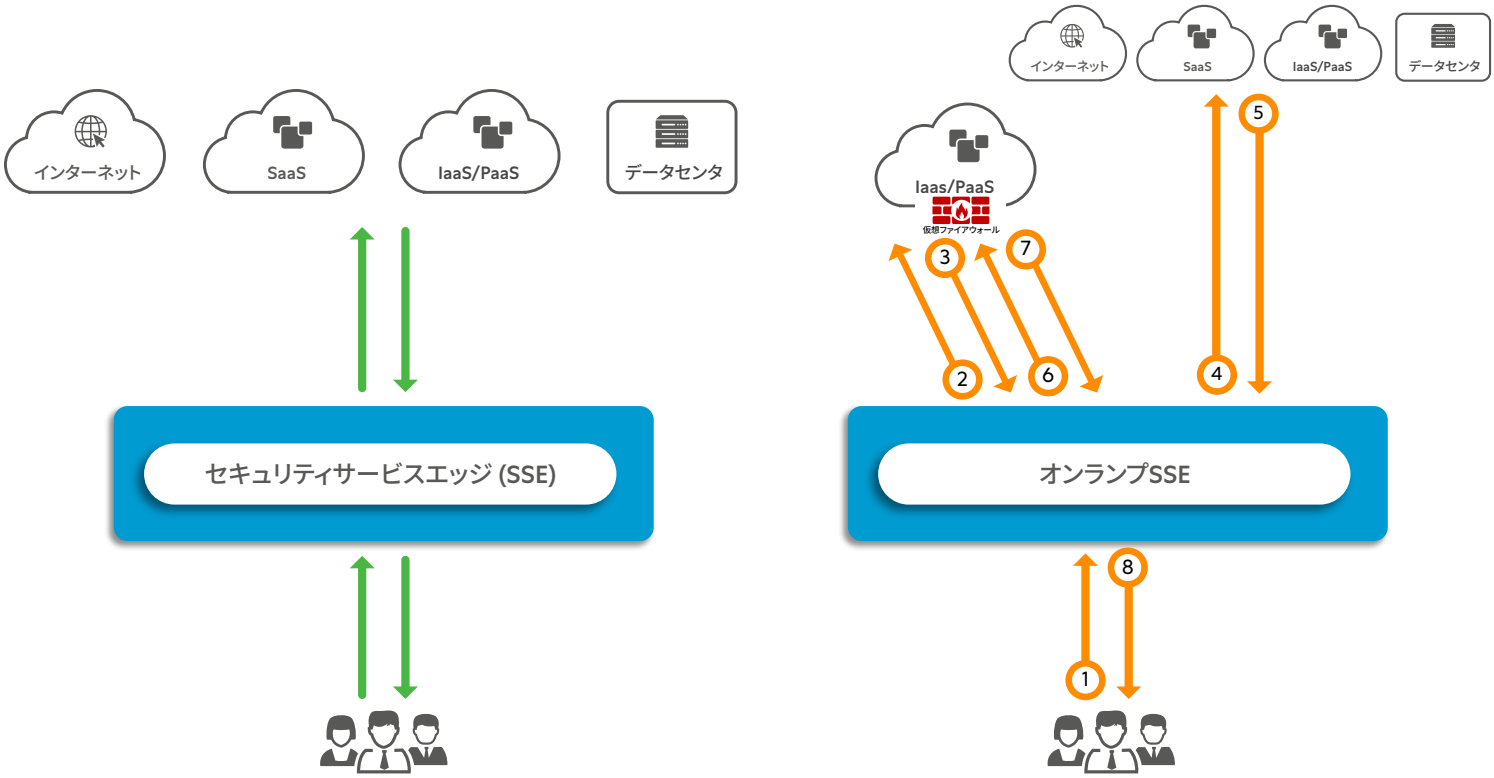


図3: インラインSSEサービス（左）は、インラインでトラフィックにセキュリティ制御を適用します。オンランプセキュリティコントロール（右）は、エッジで入口ゲートウェイを提供し、クラウドコンピュータがホストする中央のコントロールに転送するだけで、遅延と非効率性が増し、ユーザエクスペリエンスの質が悪くなってしまいます。

ベンダーは、エッジの必要性を確保しながら、以下のデザイン上の考慮事項に対処する必要があります。

- キャリアニュートラルなデータセンタ内の重要なピアリングロケーションでホスティングされるため、送信元と送信先間のレイテンシーが最小であること。SSEベンダーを評価する際には、PeeringDBのような公開リファレンスやパートナーの導入事例から得られた統計を確認すること **(パートナー統合の詳細については、落とし穴 その6を参照)**。
- 有効なSLAでサポートされていること。これにより、ビジネス機能の安定性が確保され、SSEベンダーがSLAを保証するために地域で活動していることが示されます。
- オンプレミスやエッジコンピュートノード内など、地域の事情でより微妙なデプロイメントが必要な場所では、顧客ごとに非公開でデプロイする **(落とし穴 その4に詳細が記載されています)**。
- スループット増加の歴史的経路を実証する。
- 可用性と冗長性を確保するためにアクティブ-アクティブモードでデプロイされるフォールトトレランスを提供します(ベンダーは公開サービスエッジを監視および保守し、継続的に利用できるようにしています)。
- お客様のトラフィックがインフラ内の他のコンポーネントに渡らないように、またデータがディスクに保存されないように、データプライバシーを推進します。
- すべてのエッジで企業リソースの均一な制御を行い、リモートエッジからのトラフィックを中央のロケーションにルーティングまたは「オンランプ」しない。
- 脅威を検知すると、すべての企業向けサービスを保護するグローバル規模の保護を実施

⚠ 注意すべき点

- 強制力を持たないパブリックエッジ代わりに、計算資源が利用可能な大規模な執行データセンタにトラフィックをオンランプする。
- 各エッジの機能や容量を共有することなく、100´sのパブリックエッジを主張。
- 可用性、スループット、回復力に関するSLAがないエッジ。
- マルチテナントのないエッジサービスで、オンランプ/ルートで他の場所へのトラフィックを強制。
- 規模の大きい顧客でのデプロイメント
- サービスの安定性と可用性に関する一般に消費可能な情報がないサービス

成果:

現在のビジネス、そしてより重要な将来の目標に向けて拡張性のあるSSEソリューションを選択することは、重要な投資です 。拡張性とは、単にビルドアウトするための仕組みではなく、より重要なのは、以下のようなソリューションを選択することで、ビジネスの機能、安定性、保護を犠牲にすることなく、企業のニーズに対応することです。

- グローバルで多様なデプロイメントのエビデンスと透明性を提供。
- SSEサービスの損失または劣化に関するSLAを文書化し、検証している。
- 自社と同じ規模や複雑さを持つ顧客に対して数多く展開している。
- 公開ツール(例:PeeringDB)を使用した、各PoPの公開および閲覧可能な情報を持っている。
- トラフィックをヘアピンすることなく、すべてのサイトですべての重要な機能を提供。
- 送信元と送信先の間のインラインで保護。
- インフラや運用および機能の耐性を考慮して設計されている。
- 複数のサイトにおいて、複数の形態で消費可能。

その2
落とし穴

ゼロトラストアーキテクチャの基盤上に構築されていないSSEソリューションを選択する

代わりに、以下のようなSSEソリューションを検討してください。

- 場所やネットワークに関係なく、文脈的に検証されたIDにのみアクセスを許可するようにして下さい。この最少特権パスは、ユーザーだけでなくすべてのサービスが対象です。企業は、許可されたソースを正しいSSE制御によって有効な宛先に接続することで、脅威者がしばしば悪用する横方向の動きを排除することができます。
- セッション単位のダイナミックなアクセス接続のみにフォーカスします。ゼロトラストは、ファイアウォールやSD-WANなどのネットワークサービスでは実現できません。ネットワークに依存しないオーバーレイである必要があります。
- 企業の資産を不正なソースに公開しないことで、攻撃対象領域を減らし、すべてのサービスに正しい制御が適用されるようにします。

正しいSSEベンダーはこれをどのように実現するのか

すべての企業コミュニケーションにおけるゼロトラストは、いかなるソース（ユーザ、サードパーティー、ネットワークなどを含む）からいかなる宛先へのアクセスも、そのための明確な許可と承認がない限り認めないということを意味します。

企業内でゼロトラストを実現することは、従来、ソースと宛先を接続する共有ネットワークコンテクストのために困難でした。2 つのエンティティを相互接続するために物理ネットワークパスまたは論理ネットワークパスのいずれかに依存しています。図4 は、これらの共有物理的懸念の概要を示しています。SD-WANやファイアウォールでは、ゼロトラストを構築したり追加したりすることはできません。

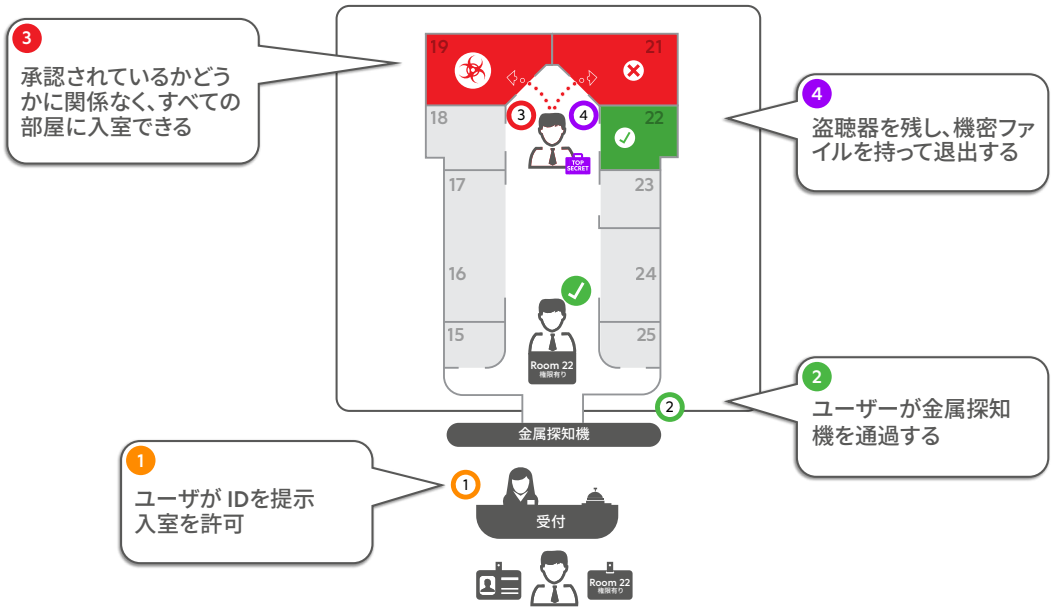


図4: アクセスを可能にしない方法-ネットワークセキュリティの古い世界の例え話。ユーザを企業ネットワークに接続することは、付き添いのない訪問者が本社内を歩き回り、機密データを盗み出す可能性があるようなものです。

SSEは、ワークロードに対する企業全体のユーザアクセスと制限の実施を支援します。これらの管理を従業員以外にも拡大することで、露出した攻撃対象や横方向の脅威の動きなどのリスクから企業を保護することができます。

他にもいろいろありますが、ゼロトラストアーキテクチャは、図5 が示すように、各リクエスタがセッションごとに正しい宛先と通信することを保証し、きめ細かい制御を実施します。このようなルールには、送信元と送信先のエンティティの知識が必要であり、ほとんどの企業がゼロトラスト（およびSSE）化をユーザベースから始めるのはそのためです。ユーザにはしばしばIDが割り当てられ、様々なサービスとの差別化を図ることができます。しかし、ネットワークがフラットで、公開され、オープンであるため、ネットワークを共有しているというだけで、ユーザがより多くの情報にアクセスできるようになるリスクは、企業の安定性にとって大きな懸念材料となっています。

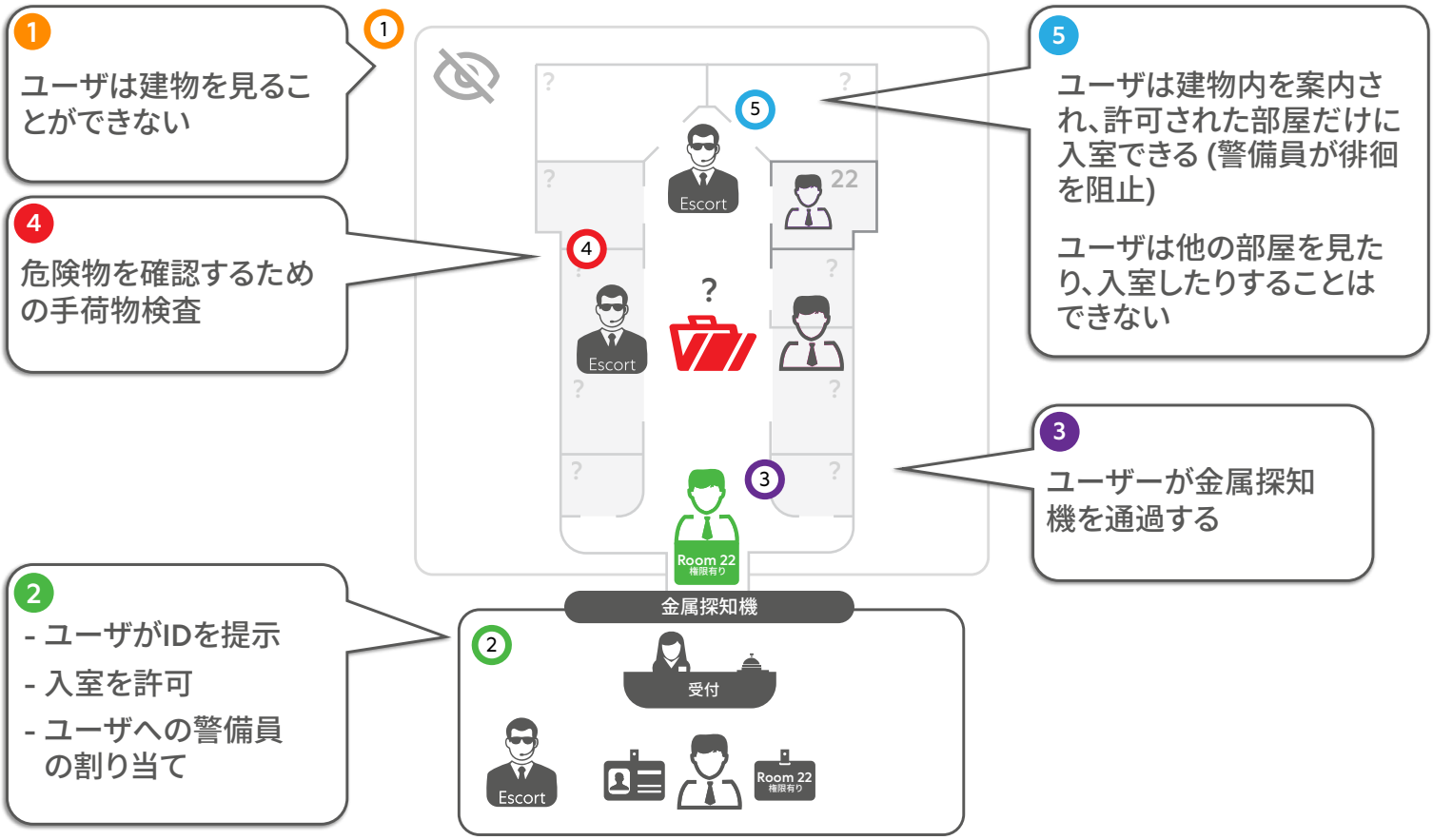


図5: アクセスを提供する正しい方法は、エンドツーエンド制御によるものです。ゼロトラストアクセスとは、目隠しをした訪問者を本社の会議室に案内し、外に出るまで付き添うようなものです。訪問者は勝手に歩き回ったりすることはできません。

ユーザや重要なビジネス資産の保護など、すべてのビジネスユースケースを考慮し、すべてのトラフィックにSSE制御を適用します。以下の4つの接続値（図6参照）のリスク度合いを動的かつコンテキストに沿って検討した上で、接続を確立します。

接続の開始者

ユーザ／デバイス／ネットワークのアイデンティティと信頼性とは？このアイデンティティは、このソースへのアクセスをどのように区別し、どのような条件の下で行うのか？

例： 人事部のサラは、社内でホストされている経費システムだけでなく、クラウドでホストされている人事システムにもアクセスする必要があります。彼女のアイデンティティとデバイスの信頼性が、アクセスを取得するために定義された権利である限り、SSEプラットフォームを通じてアクセスが許可されます。

ポリシーの管理

どこで、どのように、どのコントロールを適用するのか？制御の基準には、経路の有効性、開始者のリスクと信頼、要求された宛先の機能、企業の方針が含まれます。

例：ピエールは Salesforce にアクセスするための有効な ID を持っていますが、彼の会社は彼にデータのダウンロードや操作ではなく、閲覧のみを求めています。このため、SSEソリューションでは、ピエールにアプリケーションのコンテンツを表示するためのアクセス権のみを与え、それ以上のアクセス権は与えません。

接続先

リクエスタがアクセスしているのはどのサービスか？公開されたSaaSなのか、それとも内部のワークロードなのか？どのような制御を行うのか？アクセスは、アイデンティティと制御ポリシーのコンテキストに基づいて変更することができます。

例： 有効なイニシエータは、特定のクラウド PaaS サービスにアクセスする承認を持っている場合があり、それがクラウド サービスの場合、SSE はワークロードを検査して企業秘密が漏れないことを確認します。同じイニシエータは、同様の信頼性を持つ内部サービスにはたらきかけることができ、追加の制御なしに、シンプルにイニシエータとサービスの接続を確立します。

接続の確立

最後に、これまでのインプットをもとに、ワークロード、ネットワークやエッジの能力、企業で定義されたポリシーなどを条件として洞察し、アクセスを確立します。SSE ソリューションは、場所の変更などのバリエーションを識別し、適用可能な最適な経路でアクセスを誘導する必要があります。

例: ソース、コントロール、宛先が検証されると、そのセッションのための接続が構築され、それ以上には発展しません。セッションごとの執行のエンドツーエンドのフローは、図6 に概説されています。

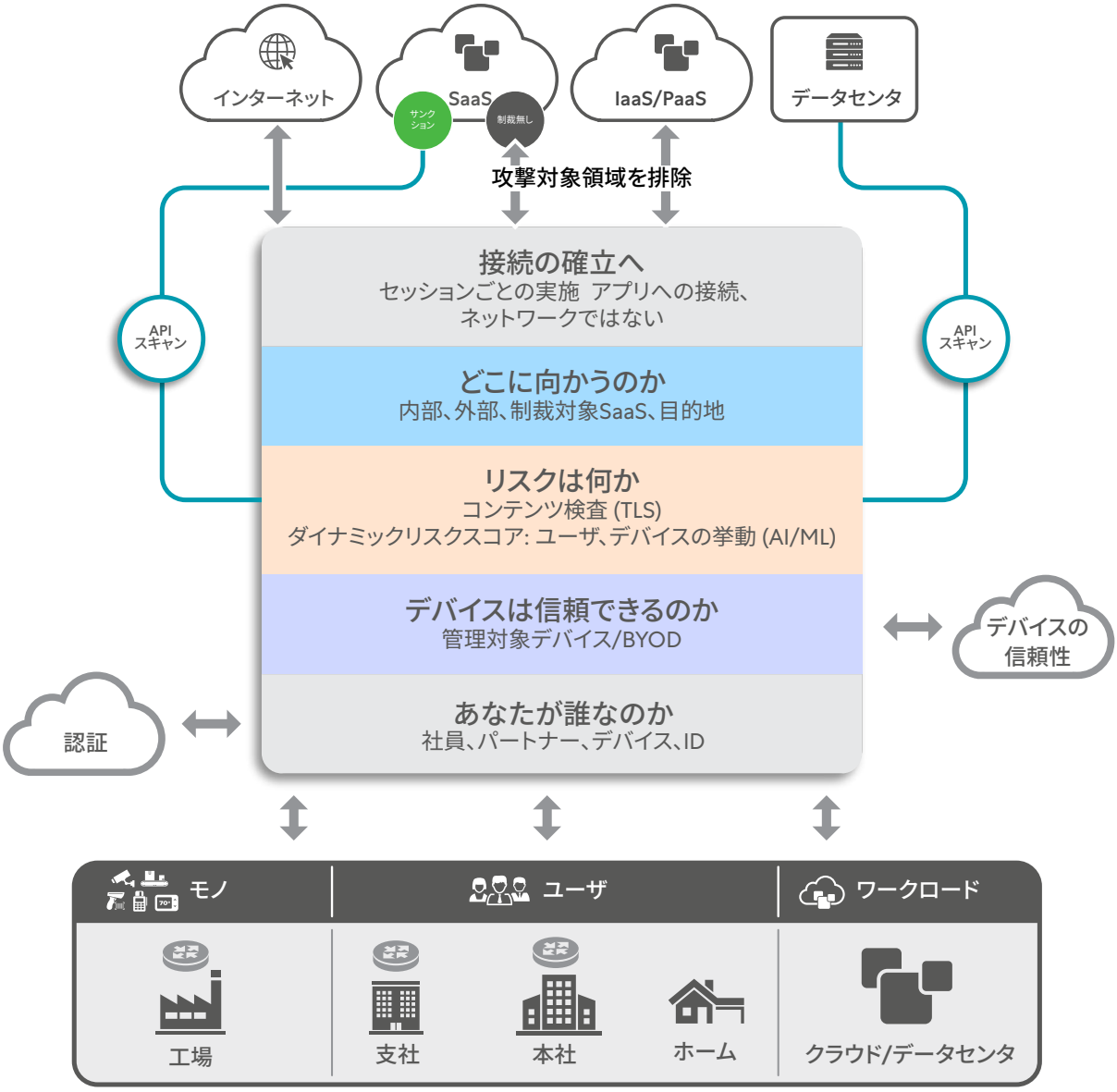


図6: ゼロトラストアーキテクチャのステップ。各ステップにおけるポリシーの制御と実施を示す。

SSEソリューション内で接続制御を定義することで**正しいソースのみが正しいSSEソリューションを通じて正しいデスティネーション**を消費できるようにします。このようにSSEを最小限の権限で使用することにより、企業には以下のような複数のメリットがも たらされます。

- 正しいSSEコントロールを正しいソースに適用する
- SSEで保護されたサービスは、不正なソースにさらされることがなく、サイバーセキュリティのリスクを低減する
- 無駄の削減例：LinuxサーバーがWindowsパッチシステムに接続することを許可しない
- フローのきめ細かな可視化と学習 - ネットワークIP間ではなく、アクセス要求ごと
- ネットワークではなく、IDに基づくアクセスの統合により、ネットワーク機能（およびインフラ）の合理化が可能

SSEの段階的な道のりは、ゼロトラストを通して以下の様に実現されます：

以下のすべてのユースケースで制御を実現し、ユーザベースの制御のみを実現するSSE ソリューションを選択することで、すべてのビジネス機能にわたって保護を拡張できます(図7参照)。

ユーザからワークロード

ワークロードへのユーザアクセスを可能にするということは、ユーザアクセスからネットワークコンテキストを取り除くと同時に、ユーザによってアクセスされているワークロードを可視化することができるということにつながります。このコンビネーションが、一般的に最も早く価値を発揮します。

アプリケーション環境全体におけるユーザのきめ細かな制御を検討します。例えば、YouTubeのようなインターネットサービスは、組織の広報チームに限定することができます。

企業向けサービスのインベントリーをより発展させ、エコシステム全体を決してユーザーベースに公開することなく、分離されたOTやR&Dプラットフォームへのアクセスなど、よりきめ細かいルールを可能にします。

サードパーティのアクセス

サードパーティパートナーにゼロトラストアクセスを導入することで、従来のパートナーアクセスにつきものであったネットワーク接続のリスクと露出した攻撃対象が取り除かれます。ゼロトラストの最小特権制御により、信頼されていないデバイスや個人所有のデバイスからのパートナーへのアクセスを、特別に指定されたアプリケーションのみに制限することができ、同時に、アクセスされているものをより明確に可視化することができます。

SSEソリューションのサードパーティー制御は、アクセス制御のための複数のメカニズムを提供する必要があります。選択肢としては、複数のIDプロバイダから特定のアプリケーションを経由した認可されたクライアントアクセス、ブラウザのみの隔離されたアクセス、第三者に提示されるレンダリング画像へのアクセスの完全隔離（BYODのようにユーザーデバイスにピクセルをストリーミング）などがあります。

ワークロードからワークロードへ

ワークロード間制御とは、アプリケーションやサービスへのアクセス要求のことです。一般的に、Windows機器は、LinuxではなくWindowsのパッチを要求します。したがって、どのシステムが何にアクセスできるかを分類することは、企業にとって非常に重要になります。

ユーザと同様に、ワークロード制御は、サービスを利用するために有効なIDを提供する必要があります。ワークロードがPaaSベースのIoT/OTサービスなどのパブリックリソースを消費する場合、セキュリティエッジはそのコンテキストを検証および理解し、悪用しようとするものをブロックしなければなりません。

逆に、作業負荷がローカルのプライベートサービスにアクセスする場合、ゼロトラスト検証に従ってIDを承認した後、インラインのSSE制御によってのみ行うことができます。

ロケーションからロケーション

アクセスや制御が企業全体で進化するにつれ、サイト間接続のためのゼロトラストを検討してください。一連のサービスをネットワーク、サイト、VPCなどに分離する必要があります。所在地と既知のサイトとの接続は、共有ネットワーク上で実行されるべきではありません。ゼロトラストは、有効なロケーションが、別のロケーション内の有効なワークロードのセットに接続することを可能にします。ゼロトラストは、ネットワークリンク層のアクセスを使用せず、どのサイト、VPC、VLANなどでも一様にアプリ間の接続を求めます。

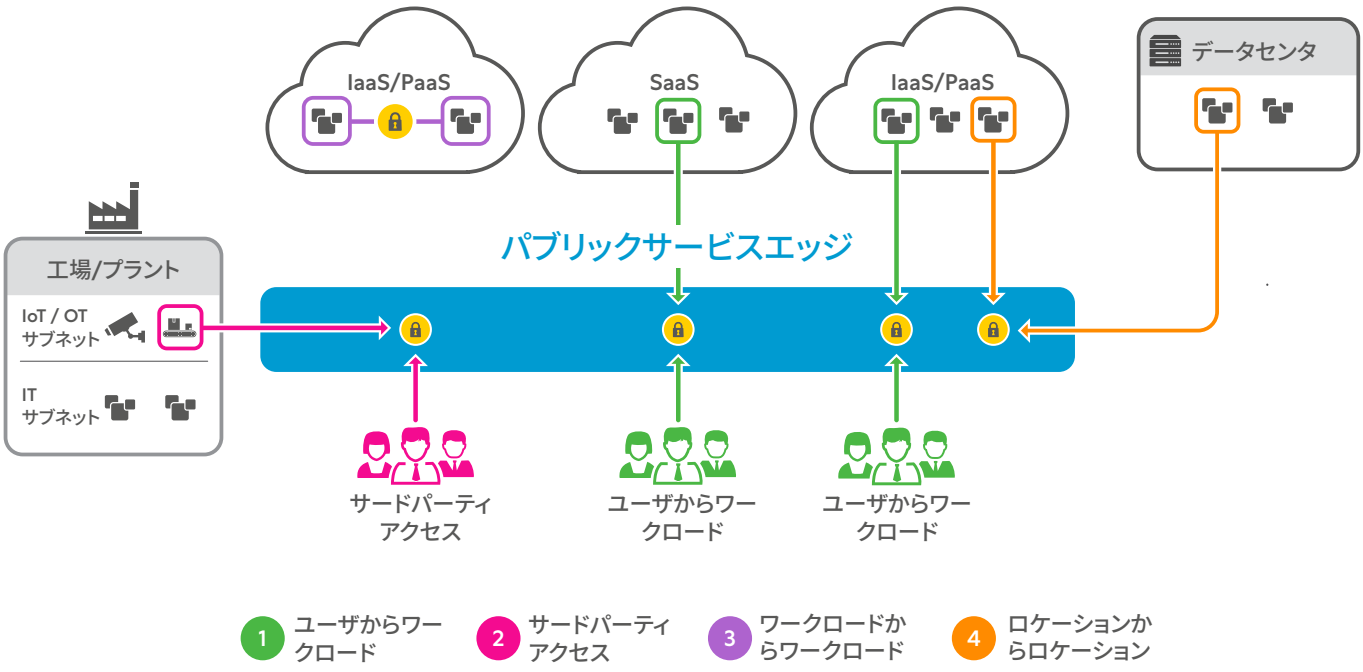


図7: 企業のセグメンテーションのための提案されたアプローチ。ゼロトラスト導入の一環として、管理、学習、さらなるセグメンテーション、隔離といった段階的なアプローチを可能にする

最近の例として、セキュリティ研究者が Log4j のゼロデイ脆弱性を発見したとき、脆弱性のある Apache Java ベースのログユーティリティを実行しているすべての顧客が、完全なリモートコード実行のリスクにさらされました。しかし、ゼロトラストアーキテクチャを採用することで、内部アプリはインターネットから完全に見えなくなり、攻撃者がそれを見つけて悪用することができなくなり、Apache Log4jの影響を受けやすいバージョンもこの脆弱性や将来の脆弱性から保護されるようになりました。**ゼロトラストは、許可されたユーザのみがアプリにアクセスできるようにし、ユーザからアプリ、アプリからアプリへのマイクロセグメンテーションによって横方向の移動を防ぎ、インバウンドとアウトバウンドの両方のトラフィックを検査することができます。**

これは、コロニアルパイプラインの攻撃でも同様で、盗まれたVPN認証情報（MFAが有効になっていない）によって、ハッカーはネットワーク上を横方向に移動し、機密データにアクセスすることができたのです。許可されたユーザーのみをネットワークではなくアプリケーションに接続するゼロトラストアーキテクチャにより、ユーザーとアプリケーション、アプリケーションとアプリケーションの通信をセグメント化し、横方向の移動を防止します。

⚠ 注意すべき点

- NIST Special Publication 800-207のようなゼロトラストアーキテクチャの原則に従わないSSEサービスは避けてください。
- SSEサービスが、ユーザーだけでなく、すべての企業リソースに対してゼロトラスト制御を提供することを確認します。
- ゼロトラストは、ファイアウォールやSD-WANの機能ではありません。ネットワークに依存せず、またネットワークにとらわれません。ネットワークに依存するプロバイダーのSSEは、ゼロトラストアーキテクチャの欠陥にさらされる可能性があります。
- ゼロトラスト管理は、ゼロアクセスから開始するようにします。
- 企業のあらゆる側面に対応して、ゼロトラストコントロールをビジネスの一部分に限定しないようにして下さい。

成果：

企業とそのユーザを保護するには、知る必要のある最小限の権限でアクセスを提供する方法でアプローチする必要があります。**SSEソリューションを選択する際には、ゼロトラストを基本制御とする必要があります。**そうすることで、次のようなことが可能になります。

- SSEベンダーは、すべての企業向けサービスを保護し、アクセスを許可する前にエンティティのアイデンティティを検証します。
- ネットワーク接続を強制するようなソリューションは避けるべきで、どこでもネットワークに依存しないアクセスが必要です。
- SSEサービスは、お客様のプライベートエンタープライズサービスに対して、攻撃対象領域ゼロを実現します。

その3
落とし穴

高度な脅威防御とDLPを約束する一方で暗号化トラフィックを大規模に検査できないSSEソリューションを選択する

代わりに、以下のようなSSEソリューションを検討してください。

- パフォーマンスへの影響を最小限に抑えながら、実運用規模でのトラフィックのSSL/TLSインスペクションを提供。そのためには、スケーラブルなプロキシアーキテクチャが必要です。
- インスペクションから得られる深い洞察を捉え、分析することで、暗号化されたトラフィックに対する高度な脅威防御を適用し、データ損失防止のための高度なデータ分類ポリシーを適用。
- ユーザ、モノ、ワークロードなどから暗号化されたものを含むすべてのトラフィックを検査。

正しいSSEベンダーはこれをどのように実現するのか：

SSEベンダーは、暗号化されたトラフィックを含むすべてのトラフィックを実稼働環境で検査する能力がなければ、クラス最高の高度な脅威防御とデータ損失防止を実現したと主張することはできません。

この分野では、ソリューションの基本的なアーキテクチャに大きく依存するため、SSEベンダーの主張には注意が必要です。この点においては、クラウドプロキシーをゼロからクラウドネイティブとして構築したSSEベンダーが明らかに優位に立ちます。

インターネットトラフィックの大部分（推定約85%）が暗号化されているため、SSEベンダーは、暗号化されたチャネルがもたらすセキュリティリスクの急激な増加に直面して、必要な脅威保護とデータ損失防止を適切に行うために、このトラフィックを大規模かつ詳細に検査する必要があります。なぜ規模に応じたSSL/TLS復号化が重要なのでしょうか (図8参照)。

- SSL/TLS暗号化により、ウイルスやスパイウェアなどの有害なコンテンツが隠蔽される可能性があります。
- 攻撃者は、TLSやSSLで暗号化したウェブサイトを構築したり、よく知られた信頼できるSSLやTLS対応サイトに悪意のあるコンテンツを注入したりします。
- SSL/TLSは、組織からの機密財務書類の送信など、データ漏洩を隠蔽することができます。
- SSL/TLSは、法的責任クラスに属するWebサイトの閲覧を隠すことができます。
- HTTPS を使用するオンラインサービスとの間のトラフィックを制御および検査する機能は、組織のセキュリティ態勢の重要な一部となっています。

図 8: 一部のベンダーが採用しているパススルーアーキテクチャでは、暗号化されたトラフィックを大規模に検査することはできません。これは、基本的なセキュリティチェックポイントが、悪意のある貨物があるかどうかトランクをチェックせずに車を通過させるのに似ています。

このようなリスクを考えると、SSEベンダーのアーキテクチャは、完全なインバウンドおよびアウトバウンドコンテンツ分析を提供し、クラウドのどこで検出された脅威も即座にブロックするSSL/TLSの中間者プロキシとして機能するように拡張する必要があります。

組織を狙う攻撃者は、Dropbox、Box、OneDrive、GDriveなどの正規のストレージサービスプロバイダを悪用して、悪意のあるペイロードをホストするなどのツール、テクニック、手順を進化させ続けています。これらの接続は、悪意のあるペイロードを提供する際に、これらの有名ベンダーのワイルドカードSSL/TLS証明書を使用し、検査されない場合は、攻撃が成功することになります。悪意のあるペイロード（実行ファイル、オフィス文書など）は、基本的なフィンガープリントの検出を回避することを目的としているため、性質上ポリモーフィックでもあります。SSE ベンダーのアーキテクチャは、これらのSSL/TLS 暗号化接続からペイロードを完全に抽出でき、正確な検出のためにこれらのファイルを解凍し難読化できる必要があります (図9参照)。

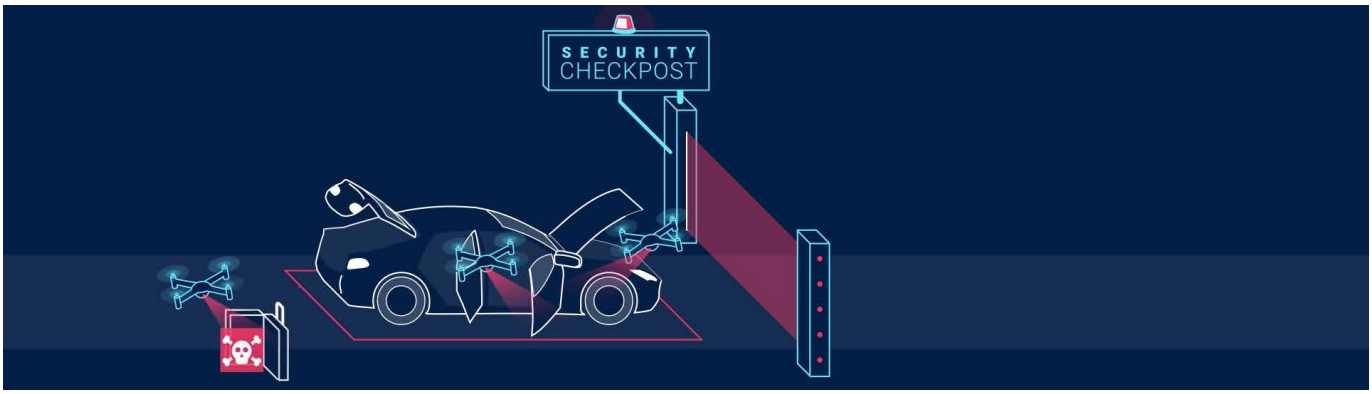


図9: 右のSSEベンダーは、プロキシアーキテクチャを使用して、すべてのトラフィックのSSL/TLSの完全検査を行います。これは、セキュリティ検問所を通過する前に停止して完全に検査する自動車と同様です。

この脅威対策は、オープンソース、商用、民間のソースにまたがる多くの業界の脅威フィードを活用し、頻繁にセキュリティアップデートを行う必要があります。

脅威のブロックに加え、規模に応じた検査により、高度なデータ損失防止が可能になります。**SSEベンダーは、データの分類機能で評価されるべきです。**基本的なメカニズムとして正規表現（regex）が含まれている必要がありますが、個人、健康、機密データを損失から保護するためには、すべてのクラウドデータチャネルで機密データを迅速に発見し分類することが必要条件となります。この分類にはSSL/TLSインスペクションが必要であり、次のような高度な機能を実現します。

- **完全一致データ**：SSE はインデックステンプレートを使用して、構造化データソースから事前に定義された基準に一致するレコードを識別します。
- **ドキュメントフィンガープリント**.SSE は、アウトバウンドトラフィックを評価する際に、完全にまたは部分的に一致するドキュメントを識別するためにドキュメントリポジトリを使用します。
- **OCR（光学式文字認識）**.SSEは、画像ファイル、埋め込み画像、スクリーンショット、手書きテキスト内の機密データを検出し、すべてのクラウドベースのデータ流出経路を閉鎖します。
- **機械学習.** 事前学習済みのアルゴリズムは、データの感度について判断します。

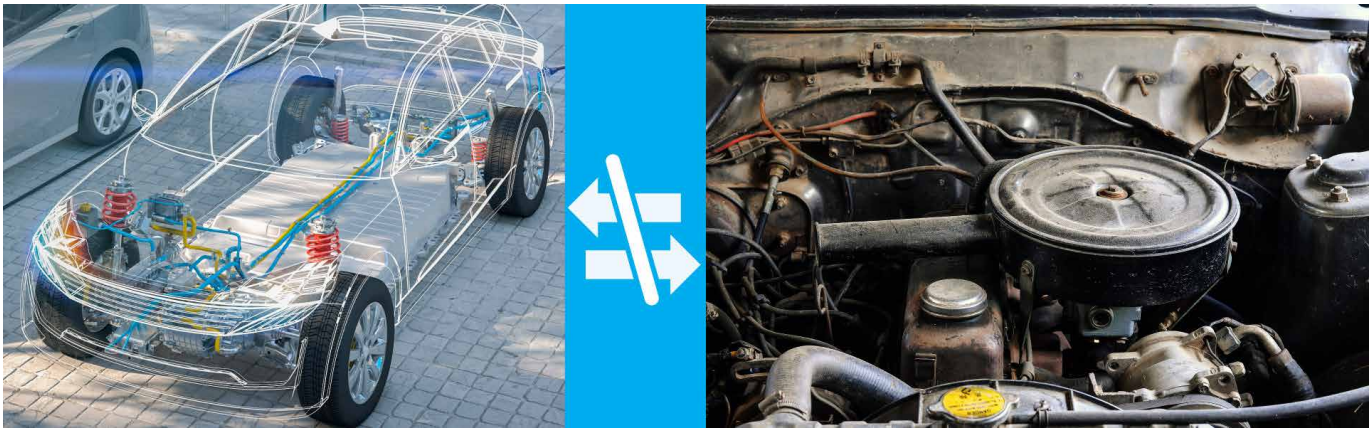


図 10: 内燃エンジンが電気自動車のように機能するように改造できないのと同様に、レガシーアーキテクチャに SSL/TLS 検査のような機能を付加するベンダーには注意が必要です tion

SSEには、クラウドサービスのユーザとアプリの間のポリシーを監視および実施するためのクラウドアクセスセキュリティブローカー（CASB）機能があり、暗号化トラフィックをインラインで検査できることには多くの利点があります。検査には、SaaSプロバイダーのAPIをスキャンして静止状態のデータを保護する「アウトオブバンド」と、移動中のデータをスキャンする「インライン」の2種類があります。インライン検査では、無許可のアプリへのデータのアップロード、無許可のデバイスへのデータのダウンロード、悪意のあるコンテンツのダウンロードやアップロードを防ぐことができるため、後者には特に注意を払う必要があります。また、SSEベンダーは、豊富なクラウドアプリの定義、ファイルタイプの制御、およびリスク属性に基づくきめ細かいアクセス制御を可能にする必要があります。

非常に多くのクラウドアプリケーションの採用により、今日、組織の機密データは広く分散されています。データ流出経路の上位2つは、クラウドデスクトップと個人用電子メールアプリケーションです。優れたSSEベンダーは、不正ユーザが個人のBox、Dropbox、その他のクラウドデスクトップに機密データをアップロードする際に、コンテキストに基づく完全な可視化と強制力を提供する必要があります。また、GmailやHotmailなどの個人向けや無認可のウェブメールサービスでのデータ流出も止めるべきです。

SSE ベンダーの違いが明らかになるのは、SSL/TLS トラフィックを解読および検査する能力が、トラフィック需要に応じて弾力的に拡張できること 、このレベルの検査をパフォーマンスを気にせずに提供できること、これらすべてを実現できるのは、最初からスケールを考慮して構築されたプロキシベースの SSE ソリューションだけです(図10参照)。

SSEベンダーがどのようにこれを実現しているかを掘り下げることが重要です。各パケット検査の遅延を最小限に抑えるため、ベンダーは、パケットを一度メモリに置き、それぞれ専用のCPUリソースを持つ検査サービスが同時にスキャンを実行できるシングルパスアーキテクチャを採用する必要があります。シリアル化された物理および仮想アプリケーションでこれらの検査をサービスチェーンするベンダーは、各ホップで処理のペナルティを受け、各パケットに過剰な遅延が適用される危険性があります。

これらのアーキテクチャの利点は、TLS 1.3 のような新しい規格にも適用されなければならず、真のプロキシアーキテクチャは、クライアントとサーバへの2つの別々の接続とインラインになる利点を持っています。これにより、オブジェクト全体を再構築してスキャンすることができるため、高度な脅威防御、DLP、サンドボックスの適用が可能になります。TLSのバージョンと暗号のアップグレードが、ベンダーのクラウド内でシームレスに処理されることを確認するようにします。ハードウェアベースのベンダーによっては、新しい暗号のサポートに伴う追加負荷を処理するために、アプライアンスのリフレッシュを強制する場合があります。

証明書の管理についても、複雑化する可能性があるため、考慮する必要があります。SSEベンダーは、自社の証明書を使用することも、自分の証明書を持ち込むこともできるようにし、APIを介して2つの証明書を交換できるようにする必要があり、証明書は、様々なサービスエッジの間で自動的に複製される必要があります。

SSEベンダーは、SSL/TLS検査機能を既存のNGFWに付加する可能性がありますが、このようなベンダーには固有の規模の問題があるため注意が必要です。これは、インスペクション機能を持つNGFWをCSPのコンピュートノード上の仮想インスタンスにリフト&シフトしているベンダーにも影響します。

⚠ 注意すべき点

SSEベンダーのSSL/TLS検査能力を評価する場合、発生する遅延が許容範囲であることを必ず確認するようにします。残念ながらノンクラウドネイティブのアーキテクチャは、特にTLS 1.2以前のバージョンを使用する時は大幅なパフォーマンス低下を招きかねません。**データプライバシーも懸念されるため、規制上の制約とベンダーの対応方法を理解するようにします。** SSEベンダーは、プライバシー制約の範囲内で、特定のデータタイプを簡単に除外できるようにする必要があります。SSEベンダーは、ユーザデータをクラウドに保存してはいけません。

SSEベンダーは、SSL/TLS検査機能を既存のNGFWに付加する可能性がありますが、このようなベンダーには固有の規模の問題があるため注意が必要です。これは、インスペクション機能を持つNGFWをCSPのコンピュートノード上の仮想インスタンスにリフト&シフトしているベンダーにも影響します。また、帯域外CASB機能と限定的なインライントラフィックインスペクションを組み合わせているベンダーには注意が必要です。静止中のデータと移動中のデータを保護することは非常に重要です。

SSEベンダーがどのように証明書を管理しているかを評価し、証明書のピン留めが問題になる可能性があることを認識しましょう。

SSL/TLSインスペクションの実装は、さまざまな理由から、ビジネスにとって歴史的に困難なものでした。**SSEベンダーは、最も信頼できるエキスパートとして、SSL/TLSインスペクションを有効にする際にガイダンス、理解、および実装を提供することが必要です。SSL/TLS検査**というものは、SSEの世界ではセキュリティよりもスピードを犠牲にしてはならないので必要不可欠です。

成果:

SSL/TLSを最小限の遅延で大規模に検査することで、クラウドの力を活用して機密データを特定し保護しながら脅威をブロックする能力を大幅に向上させます。正しいクラウドネイティブアーキテクチャを持つSSEベンダーだけが実現できます。

- パフォーマンスへの影響を最小限に抑えながら、本番環境下ですべてのトラフィックをSSL/TLSで検査し、脅威とデータの徹底的な防御を実現します。
- シングルメモリスキャンアーキテクチャにより、大規模な復号化のための独自のスケーラビリティのメリットを提供します。
- SSL/TLSの検査を実現するための手順や課題をお客様に案内する豊富な経験があります。

その4
落とし穴

柔軟性、拡張性、多様性を備えた展開および管理オプションがない「画一的」なSSEソリューションを選択する

代わりに、以下のようなSSEソリューションを検討してください。

- データセンタ、パブリッククラウド、プライベートクラウド、エッジコンピュートノード、オンプレミスなど、アプリケーションがホストされている場所を問わず、ユーザとアプリケーションを保護するための柔軟な導入モデルを提供します。
- 管理対象/非管理対象エンドユーザのデバイスやモノでアプリケーションにアクセスするユーザに対する保護を実現します。
- 同じサイバー脅威とデータ保護を拡張し、同じクラウド内または複数のクラウドにまたがる他のすべてのワークロード間通信を保護します。

正しいSSEベンダーはこれをどのように実現するのか：

SSEソリューションの評価者は、SSE保護を適用する最適な方法を理解するために、環境の準備状況を評価する必要があります。多様な導入シナリオに対応するため、SSEベンダーは、パブリックサービスエッジとプライベートサービスエッジの両方を可能にする必要があります。

正しいSSEベンダーはこれをどのように実現するのか：

SSEソリューションの評価者は、SSE保護を適用する最適な方法を理解するために、環境の準備状況を評価する必要があります。多様な導入シナリオに対応するため、SSEベンダーは、パブリックサービスエッジとプライベートサービスエッジの両方を可能にする必要があります。

ほとんどのユーザは、ベンダーの パブリックサービスエッジ を経由してSSEに接続することになります。これらは、統合されたセキュリティを提供する、フル機能の安全なインターネットゲートウェイとプライベートアプリケーションブローカーです。すべてのトラフィックを双方向に検査してマルウェアを検出し、セキュリティ、コンプライアンス、およびファイアウォールポリシーを適用します。このため、ユーザがどこにいても、あらゆるデバイスからアクセスすることができます。

- 公共サービスのエッジでトラフィックを保護し、企業ポリシーを適用するインターネット。
- お客様の組織のベストプラクティスに基づき、アクセスおよび再認証のポリシーを適用した内部アプリケーション。

図11: SSEベンダーは、パブリックとプライベートの両方のサービスエッジオプションを提供する必要があり、また、集中管理で互いに調和して機能する必要があります。

これらの公共サービスエッジは、重要なフォールトトレランス機能を持ち、可用性と冗長性を確保するためにアクティブ-アクティブモードでデプロイされることが重要です。ベンダーは、公共サービスエッジを監視および保守し、継続的に利用できるようにする必要があります。データのプライバシーを確保するため、お客様のトラフィックはインフラ内の他のコンポーネントに渡してはならず、データは決してディスクに保存してはいけません。

しかし、公共サービスエッジが要件を満たさない状況が発生する可能性があるため、SSE ベンダーは プライベートサービスエッジ オプション(図11参照) を提供しなければなりません。このオプションは、公共サービスエッジのアーキテクチャと機能を組織の敷地内または私的な場所に拡張し、公共サービスエッジと同じ中央制御ポリシーを活用します。

インターネットへの安全なアクセスのために、プライベートサービスエッジを組織のデータセンタに設置し、そのトラフィック専用とすることができますが、SSEベンダーが管理および保守し、組織からのタッチはほぼゼロであるべきです。このデプロイメントモードは通常、特定の地政学的要件を持つ組織や、その組織のIPアドレスをソースIPアドレスとして必要とするアプリケーションを使用する組織に有益です。

内部アプリケーションへのアクセスでは、プライベートサービスエッジがユーザとアプリケーション間の接続を同様に管理し、パブリックサービスエッジと同じポリシーを適用します。サービスはオンサイトまたはパブリッククラウドでホストされますが、ここでもSSEベンダーによって管理されます。このデプロイメントモデルでは、アプリとユーザが同じ場所にいる場合、アプリケーションの遅延を減らすのに有効であるため（公共サービスのエッジに行くと余計な遅延が増える）、4つの壁の中でのゼロトラストを可能にします。また、このオプションは、インターネットへの接続が失われた場合にも、生存のためのレイヤーを提供します。SSEベンダーは、企業のデータセンタやローカルのプライベートクラウド環境にデプロイメントするためのイメージを配布する必要があります。

内部アプリケーションをゼロトラストで保護するために、SSEベンダーは、アプリケーションサーバーとパブリックおよびプライベートなサービスエッジの間に安全で認証されたインターフェースを作成する方法を提供する必要があります。**このメカニズムは、いくつかのフォームファクターで利用できる必要があります**：企業データセンタ、VMwareなどのローカルプライベートクラウド環境、Amazon Web Services (AWS) EC2などのパブリッククラウド環境での標準の仮想マシン (VM) イメージまたはコンテナデプロイメント、対応するLinux ディストーションにインストール可能なパッケージなどです。

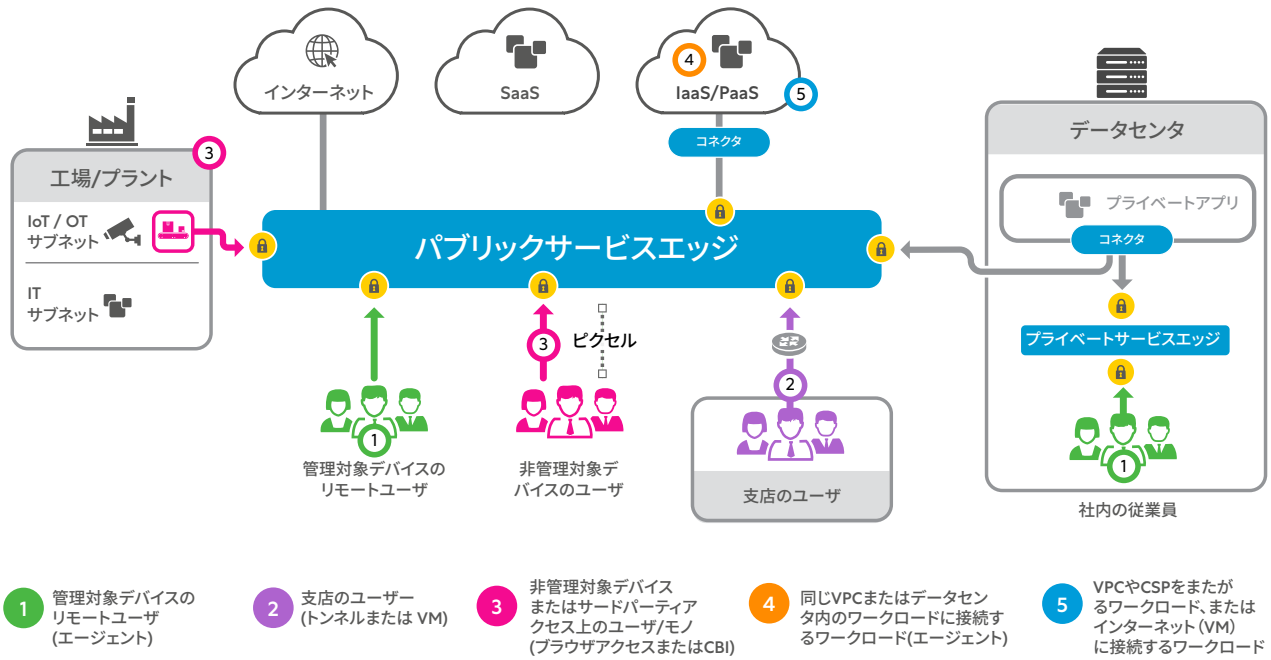


図12: SSEベンダーは、エージェントやVMを介して、リモートユーザ、支店のユーザ、本社のユーザ、ワークロードと通信するワークロードなど、多くの導入および管理モードをサポートする必要があります。

SSE ポリシーを管理および実施する場所が決まったら、次にユーザとワークロードにどのようにこの保護を提供するかを検討します。様々なシナリオを検討することが重要です（図12参照）。

管理対象デバイスのリモートユーザの場合、SSEベンダーは、安全なインターネットアクセスのためにサービスエッジにトラフィックを転送する単一の統合エージェントを提供する必要があります。このエージェントは、内部リソースへのきめ細かいポリシーベースのアクセスも提供する必要があります。これらはすべて、エージェントに内蔵されたインテリジェンスを使用して自動的に実行される必要があります。また、Wi-Fiや携帯電話ネットワーク上のユーザのモバイルトラフィックを保護する必要があります。SSEサービスは、ユーザがインターネットにアクセスする際に、組織のセキュリティおよびアクセスポリシーを適用し、企業のアプリケーションやサービスにアクセスするための安全なトランスポートを確立します。このエージェントが、ユーザが信頼できるネットワークに接続したことを検出できること、および信頼できるネットワークが検出された場合、ポリシーに従ってエージェントがそのサービスを無効にする必要があるかどうかを確認します。これらのエージェントが、Windows、MacOS、Linux、iOS、Androidなど、幅広いオペレーティングシステムをサポートすることを保証するようにします。

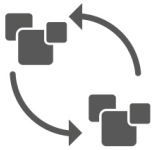
支店のユーザの場合、サービスエッジにトラフィックを転送する一般的な方法は、GRE または IPSecトンネルを経由する方法です。しかし、SSEベンダーは別の方法を提供する必要があります。支店にインストールされた仮想マシンは、これらのトンネルの複雑さと継続的な管理を簡素化し、顧客が管理するルータブルネットワークを削除することで横方向の脅威の動きを排除することができます。導入は自動化され、SLA監視とフェイルオーバーが組み込まれたサービスエッジへの柔軟なトラフィックステアリングポリシーが含まれている必要があります。このオプションは、中規模および大規模の支店や、ローカルサービスを提供する支店に適しています。

すべてのユーザをリモートユーザのように扱うという以前のオプションは、ローカルサービスが提供されない小規模な支店（コーヒーショップのモデルを考えてみてください）に対して考慮されるべきです。最近の出来事で支店の重要性が変化したことを考えると、社内ネットワークに誰も入れない、横移動の可能性を防ぐという意味で、このオプションは望ましいと思われます。

非管理対象デバイス上のユーザ/モノ、またはサードパーティによる内部ウェブアプリケーションへのアクセスについては、SSEベンダーはエージェントをインストールする必要なく、同様のSSE保護を提供する必要があります。このようなユーザは、ユーザ認証にウェブブラウザを利用し、DNSゾーンにアプリケーション固有のCNAMEを公開してゼロトラスト保護を提供し、ウェブブラウザが自動的にこれらのリクエストをリダイレクトできるようにする必要があります。また、SSEベンダーは、クラウドブラウザアイソレーション（CBI）機能を統合し、あらゆる場所で非管理対象デバイスのエージェントレスセキュリティを実現する必要があります。副次的な効果として、これによって脆弱なリバースプロキシの必要性が完全に回避されます。

CBIの場合、管理者は認可されたクラウドリソースのSSO設定をSSEベンダーにリダイレクトするように設定します。その後、ユーザが個人またはサードパーティのエンドポイントから当該クラウドリソースにアクセスしようとすると、そのトラフィックはソフトウェアのインストールなしに自動的にCBIに送信されます。ユーザデバイスに送信されるピクセルにコンテンツをレンダリングし、ダウンロード、コピー、貼り付け、印刷を防止することができます。これにより、ユーザは非管理対象エンドポイントから、情報漏えいやマルウェアのアップロードのリスクなしに、コンプライアンス要件を尊重しながら業務を遂行することができます。

同じVPCまたはデータセンタ内のワークロードに接続するワークロードについては、従来のネットワークセグメンテーションが答えとなりました。机上の論理としては理にかなっているものの、実際にネットワークセグメンテーションを実現するのは困難であり、**SSE** ベンダーは、ユーザからアプリケーションへの保護をワークロード間の通信に拡張する必要があります。ワークロード自体にエージェントをインストールすることで、**SSE** プロバイダはネットワークを変更することなく、リスクを判断してアイデンティティベースの保護をワークロードに適用し、環境の変化に自動的に適応するポリシーを備えていなければなりません。



VPCやCSPを越えて、あるいはインターネットに接続するワークロードの場合、SSE ベンダーは、ユーザ向けに提供される同様の SSE 保護を、これらの作業負荷にも再び拡張する必要があります。そのため、SSEベンダーは、通常は仮想マシン（パブリッククラウドまたはオンプレミスのハイパーバイザーで利用可能）を介して、サービスエッジへのトラフィック転送を簡素化するメカニズムを提供する必要があります。その結果、インターネットにアクセスするワークロードのサイバー脅威とデータ保護、およびあるクラウドのワークロードが別のクラウドのワークロードにアクセスする際のゼロトラストプロテクションが実現します。このアプローチにより、SSEベンダーは複数の製品（Webプロキシ、ファイアウォール、NATゲートウェイ、URLフィルタリングなど）を1つのソリューションに統合することができます。

IaaSおよびSaaS環境における静止データの保護の場合、SSEベンダーは、CASB、クラウドインフラエンタイトルメント管理（CIEM）、クラウドセキュリティポスチャ管理（CSPM）の分野でもソリューションを提供し、人気の高いSaaSおよびIaaSアプリケーションでAPIベースのスキャンを実行できるようにしなければなりません。これにより、クラウド環境内の設定ミスや不適切なパーミッションの特定と修正が可能になり、さらにSaaSやIaaSプラットフォームの監査とスキャンにより、データと脅威を保護することができます。SSEベンダーは、これらの帯域外の機能をインライン機能と密接に連携させて提供し、静止データと移動中のデータに一貫したポリシーを適用する必要があります。

単一のSSEベンダーがこのような広範な保護を提供する利点は、中央のコントロールプレーンで管理でき、企業ポリシーがすべてのユーザ/モノからアプリケーション、ワークロードからワークロードの通信に均等かつ動的に適用されることです。

⚠ 注意すべき点

SSE技術の導入は、組織の環境の複雑さに大きく依存します。**したがって、ユーザの場所、行動、アクセス要件、およびアプリケーション要件を理解することが非常に重要です。**また、中国のような特定の国では、インターネットの規制により、柔軟な展開モデルでも克服できないようなパフォーマンスに関する独自の課題が存在します。SSEベンダーは、このような課題に対処するための革新的なソリューションを提供する必要があります。

成果：

これらの柔軟で多様かつスケーラブルなオプションを正しく導入することで、ユーザーやモノがどこにいても、またアプリケーションがどこでホストされていても、セキュリティサービスエッジのあらゆる利点を組織に提供し、さらにはアプリケーション自体の中でそのような保護を拡張することもできます。

- 単一のSSEベンダーがこのような広範な保護を提供する利点は、中央のコントロールプレーンで管理でき、企業ポリシーがすべてのユーザ/モノからアプリケーション、ワークロードからワークロードの通信に均等かつ動的に適用されることです。
- 管理対象デバイスの保護を、非管理対象のBYODやサードパーティーのアクセスにも拡大することで、契約社員や従業員がより柔軟に対応できるようになります。
- ワークロード間のセキュリティは、他のワークロード、他のクラウド、またはインターネットにアクセスするアプリケーションに対して、DevOpsとCloudOpsのエンジニアに同じゼロトラスト保護を提供します。

その5
落とし穴

アプリケーション接続を最適化したり、UX低下の原因を特定したりしないため、ありきたりのユーザエクスペリエンスしか提供できないSSEソリューションを選択する

その代わりに、以下のようなSSEベンダーを検討してください：

- 透明性が高く、認証が容易で、常時稼働しており、SSEプラットフォームのエンドユーザが快適なユーザエクスペリエンスを利用していることを客観的な指標で確認できる。
- エンドユーザエクスペリエンスの低下を、エンドポイント、ネットワーク、アプリケーション、セキュリティスタックなどの根本原因に関連付ける。
- Microsoft 365などの人気SaaSベンダーとのパートナーシップを活用し、公共サービスエッジとアプリケーションプロバイダーのネットワーク間のレイテンシーを最小化する

正しいSSEベンダーはこれをどのように実現するのか：

SSEベンダーは世界中に拠点を持ち、プロバイダーやアプリケーションベンダーとインターネット上でピアリング交換を行っているため、従来のセキュリティスタックに必要なバックホールやヘアピンの代わりに、強力なセキュリティサービスを提供することができます。

このようなアーキテクチャ上のメリットに加え、SSEベンダーは、ユーザのエンドポイントやアプリケーションのデータパスにおける存在感に基づいて、エンドユーザクスペリエンスを測定および診断できるユニークなポジションにいます。これらの利点により、SSEベンダーはユーザのエンドポイントから見たユーザクスペリエンスを把握し、公共サービスのエッジインフラを活用することで、より深い診断と拡張性を提供することができます。

モニタリングソリューション（一般に **Digital Experience Monitoring** または DEM と呼ばれる）を既存のエージェントやクラウドインフラに統合している SSE ベンダーに注目します。エージェントを追加する必要がある、または統合が緩やかなソリューションを提供しているベンダーは、同じレベルの可視性と診断を提供することはできません。

SSEベンダーが提供するDEMソリューションは、場所を問わず、あらゆるユーザやアプリケーションのエンドユーザパフォーマンスの問題をエンドツーエンドで可視化し、トラブルシューティングできるような、幅広いものである必要があります。さらに、エンドユーザのデバイス、ネットワーク、およびアプリケーションのパフォーマンス問題を把握することで、ネットワーク、セキュリティ、デスクトップ、ヘルプデスクチームの継続的な監視を可能にする必要があります。**これは、機械学習ベースのスコアリングアルゴリズムで可能にする必要があり、ユーザ、アプリケーション、オフィス、地理的位置などによって正常または異常なユーザクスペリエンスを追跡します。**

このモニタリングは、ウェブアプリケーションのレスポンスタイムを把握するためのレイヤー7、パス、レイテンシ、パケットロスに関するホップごとの把握を含むネットワーク挙動を理解するためのレイヤー3など、複数のレベルで行う必要があります。この分析には、SSEベンダーのクラウドの自己診断も含まれ、SSEホップが異常な遅延を引き起こしている場合、およびそのタイミングを特定する必要があります。最後に、このソリューションはユーザのエンドポイントデバイスの状態を把握し、スコアリングドロップの原因となるデバイスイベントを特定する必要があります **(図13を参照)**。

SSEベンダーは、ユーザのエンドポイントやアプリケーションのデータパスにおける存在感度に基づいて、エンドユーザエクスペリエンスを測定および診断することができるユニークな立場にあるのです。

Microsoft TeamsとZoomの品質パフォーマンスの監視とトラブルシューティング

TeamsやZoomが多くの企業でコラボレーションやコミュニケーションの主要プラットフォームとなる中、音声や映像の品質問題の測定と診断がより一層急務となっています。SSEベンダーが提供するDEMソリューションは、ZoomやMicrosoft Teamsなどの一般的なUCaaSアプリケーションと連携し、音声やビデオの品質メトリクスを取り込み、深いホップバイホップのネットワーク解析やエンドポイントデバイス解析と連携できることが必要です。これらのデータを組み合わせることで、DEMソリューションでは品質に問題があるものを特定し、問題の根本的な原因を明らかにすることができます。

さらに、DEMはSSEベンダーのクラウドの規模を活用し、テレメトリー試験のプロキシとキャッシュに使用することで、アプリケーションへの影響を最小限に抑えながら、すべてのエンドユーザーから数分ごとに詳細なデータを収集できるようにする必要があります。

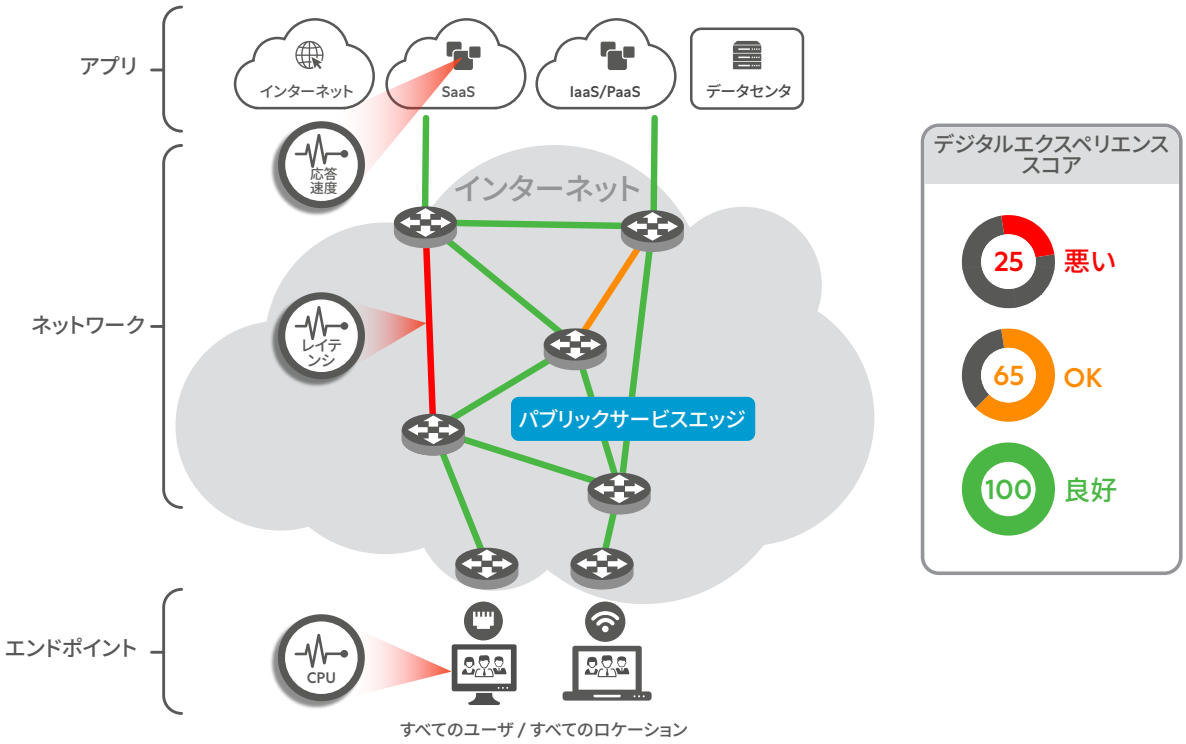


図13: SSEプラットフォームの一部として組み込まれたDEMソリューションは、エンドユーザの視点からユーザクスペリエンスの品質を独自に可視化し、エンドポイント、ネットワーク、アプリケーションの問題を明らかにする必要があります。

データセンタ中心の監視アプローチをとり、ユーザデバイスから直接ではなく、固定された場所からメトリックを収集する従来の監視ツールに注意が必要です。このアプローチでは、ユーザデバイス、ネットワーク経路、またはアプリケーションに基づくパフォーマンスの統一ビューが提供されず、ユーザとアプリケーションがデータセンタや企業ネットワーク上にない場合は、ほとんど可視化されません。これらのツールは情報のサイロを作り、コンテキストを共有しないため、ユーザエクスペリエンスに対する可視性が断片的になり、トラブルシューティングに時間がかかるようになります。データセンタ用に最適化されたポイントモニタリングツールでは、インターネット上のエンドユーザのパフォーマンス問題を検出、トラブルシューティング、および診断するための可視性にギャップがあります。一方、SSEプラットフォームに組み込まれた最新のDEMソリューションでは、根本原因の分析に最も幅広いデータを提供します（図14参照）。

DEMソリューションは、品質問題を抱える人々を特定し、問題の根本原因を提供する必要があります。

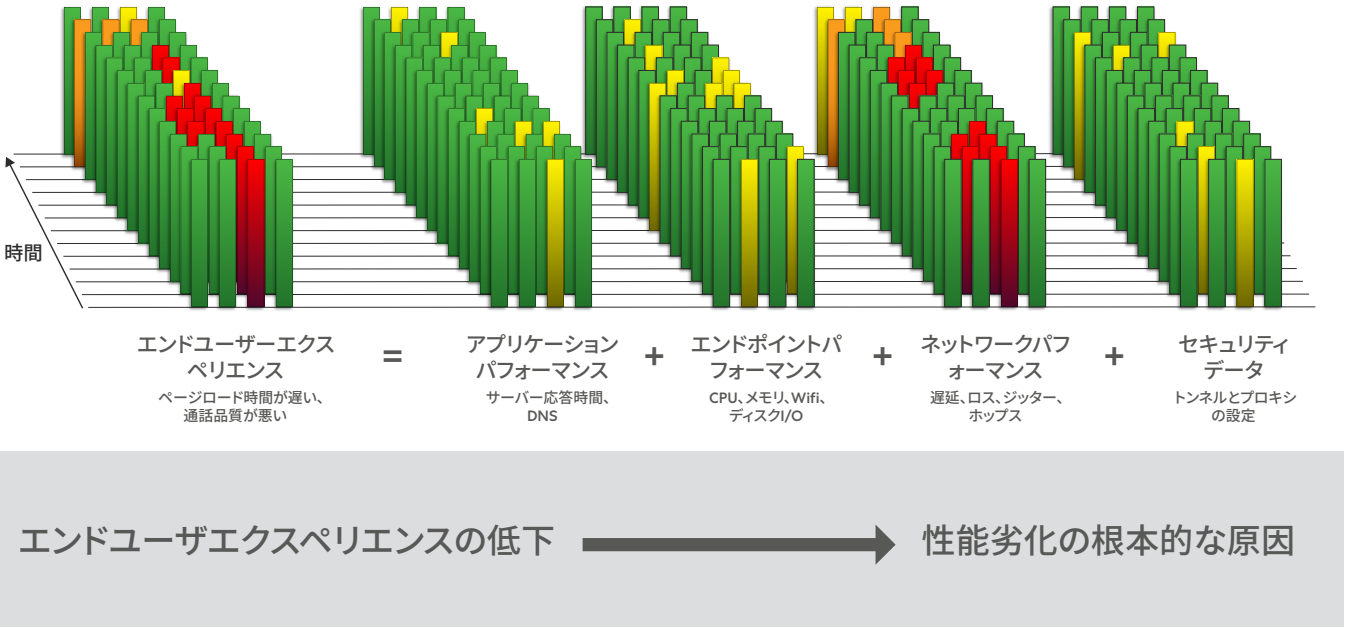


図13: SSEプラットフォームの一部として組み込まれたDEMソリューションは、エンドユーザの視点からユーザクスペリエンスの品質を独自に可視化し、エンドポイント、ネットワーク、アプリケーションの問題を明らかにする必要があります。

M365のユーザエクスペリエンスを最適化する

総合的なSSEは、エンドユーザエクスペリエンスの測定や診断にとどまらず、Microsoft 365のような人気の高いSaaSアプリケーションのパフォーマンスを最適化することができます。しかし、ほとんどの企業ではハブ&スポークのネットワークとExpressRouteでトラフィックを中央でルーティングしています。さらに、M365からのユーザトラフィックはネットワーク使用率を40%増加させますが、ほとんどの企業のインターネットエグレスインフラストラクチャはそのタスクに対応しておらず、ユーザエクスペリエンスは損なわれています。Microsoftでは、最適なパフォーマンスとコストを実現するために、インターネットへの直接接続と、ローカルインターネットブレイクアウトを可能にするSSEベンダーのアーキテクチャを推奨しています。

図15: Microsoftは、パフォーマンスとコストの面で最適な方法として、SSEの信条に沿ったインターネット直接接続を推奨しています（出典：Microsoft.com）。

しかし、アーキテクチャは重要です。SSEベンダーのプレゼンスポイントは世界中にあり、プロバイダーやアプリケーションベンダーとのピアリング関係は、高速接続と低遅延アクセスのためにエッジをユーザーにより近づける必要があります。SSEベンダーは、ほとんどの主要取引所でMicrosoft 365と直接ファイバー接続し、遅延を往復で約1〜2ミリ秒に抑え、多数のロングライフ接続を処理できるよう拡張し、迅速なファイルダウンロードを可能にし、少ないホップで高速DNS解決を提供していることを確認する必要があります(図15参照)。

M365トランザクションは、SSEソリューションで保護することが特に重要ですが、OneDriveやSharePointなどのアプリケーションの検査は、機密データの損失防止に有利というのがその理由です。また、M365アプリケーションとの間で行われたすべての通信の完全な監査証跡を提供します。ただし、Teamsのような特定のM365アプリケーションは、このトラフィックの多くがUDP経由の音声/動画であることを考えると、検査する必要がない場合があることに注意してください。

⚠ 注意すべき点

WFA (場所を問わずに仕事をする) の世界では、有線および無線ネットワークのグローバルメッシュで優れたアプリケーションパフォーマンスを提供するためのチェーンに、多くの弱いリンクが存在します。ユーザエクスペリエンスを最適化することは、優れたアーキテクチャやUXの問題を測定および診断する専用のツールセットをもってしても困難です。重要なアプリケーションを使用する際に、何が許容できるユーザクスペリエンスであるかについて、エンドユーザとの間で合理的な期待値を設定することが不可欠となります。そして、この期待値をもとに、監視および管理するためのベースラインを構築することが肝要です。

ユーザエクスペリエンスの問題を診断することは、科学というより芸術です。優れたツールとアーキテクチャが必要ですが、データを解釈して対処する適切なスキルセットを持つかどうかも重要です。 SSEベンダーが提供するDEMツールは、ほとんどの問題の原因 (Wi-Fi、ISP、バックボーン、エンドポイント、またはDNSの問題) を明らかにしますが、一部の問題については、エスカレーションと追加のデータセットが必要になります。たとえば、根本的な原因を突き止めるには、ログやパケットトレースが必要な場合があります。また、まったく解決しない問題もありますが、これは至極正常なことです。

トラフィックをヘアピンするベンダーには注意が必要です。SSEベンダーのデータセンタは、すべてコンピュートとインスペクションが可能で、より高速で優れたユーザクスペリエンスを可能にする必要があります 。クラウドネイティブアーキテクチャは、トラフィックを検査するためにトラフィックをいくつかの集中した場所にヘアピンしてはいけません。たとえば、メルボルンにユーザが現れたら、脅威防御とデータ保護サービスを用いてローカルでトラフィック検査を行い、シドニーやシンガポールといった他の地域にバックホールさせないようにします。ハイパースケーラでクラウドを運用しているSSEベンダーは、多くの場合、ユーザトラフィックを毛嫌いしています。ハイパースケーラには120のエッジポイントがあるかもしれませんが、そのうちの80パーセントは、SSEのポリシー制御を実施できる少数のハイパースケーラデータセンタにトラフィックを送るためのオンランプである可能性が高いのです。何台のデータセンタがオンランプで、何台のデータセンタが実際にポリシーを適用できるかを理解することが重要です。

成果:

デジタル、ネットワーク、セキュリティなど、あらゆる変革の成功は、エンドユーザがそれをどのように体験するかによって決まります。SSEプロジェクトの最終的な目標は、脅威への露出を減らし、機密データを保護しながら、エンドユーザエクスペリエンスを向上させることです。したがって、理想的な結果はユーザエクスペリエンスを向上させるSSEベンダーの能力がDEMの可用性で測定できるというものですが、ヘアピンからデータセンタへの移行やVPNからの脱却は、ユーザエクスペリエンスを向上させる方法として受け入れられているため、これは容易なことです。

- SSEソリューションは、ユーザエクスペリエンスを近代化し、ヘルプデスクのエクスペリエンスを更新する必要があります。ユーザエクスペリエンスに対する積極的なアプローチを活用することで、ユーザから苦情が来る前にヘルプデスクが対応できるようになります。
- SSEソリューションは、TeamsやZoomなどのコラボレーションプラットフォームにおけるリアルタイムのオーディオおよびビデオパフォーマンスに関する洞察を提供する必要があります。
- SSEソリューションは、アプリケーション層、エンドポイント層、ネットワーク層からメトリクスを収集し、異常を発見して根本原因を特定する必要があります。
- SSEベンダーは、自社のクラウドとMicrosoft 365のような人気のあるデスティネーションとの間に最小限のホップを提供する必要があります。

その6
落とし穴

サードパーティベンダーのエコシステムとの統合やオーケストレーションが限定的なSSEソリューションを選択する

その代わりに、以下のようなSSEベンダーを検討してください：

- CSP、SD-WAN、IAM、SOAR/SIEM、EDRなどのエコシステムと堅牢なAPIで統合し、最適な保護とユーザエクスペリエンスを確保します。
- これらの統合を活用することで、自動化とオーケストレーションを実現し、運用の複雑さとオーバーヘッドを削減することができます。
- ポートフォリオ内およびサードパーティとの統合が不十分なソリューションを寄せ集めて、技術的負債を増やさないようにして下さい。

正しいSSEベンダーはこれをどのように実現するのか：

技術的負債に悩む企業の多くは、その多くが相互運用性のないベンダー技術を長年にわたって調達してきたことに起因していることを認識しています。

さらに悪いことに、単一のベンダーが提供するいわゆる「プラットフォーム」は、実際には統合されておらず、ダッシュボード以上の真の統合を持たない、買収したポイント製品の集合体です。多くの場合、これらのベンダーテクノロジーは、運用に専門的なスキルを必要とし、付随するテクノロジーとの脆弱な共存を維持する必要があります。SSEは、単一ベンダーが提供するクラウド上の統一セキュリティプラットフォームにより、こうした技術的負債の多くを解消することができます。このようなビジョンを持っていても、SSEは補完的な技術のエコシステムの中で生きており、ベンダーはこのエコシステムとの相互運用性を第一の目的として考えなければなりません (図16参照)。このエコシステムは、他のセキュリティ、ネットワーク、クラウドの各ソリューションから幅広く構成されています。

図16：サードパーティとの統合で豊富なエコシステムを持たないベンダーと砂漠で一緒にならないようにしましょう。これは、技術的負債、限られた相互運用性、脆弱な（アジャイルではない）セキュリティスタックにつながるからです。

迅速、簡単、かつ安全な導入と統合を確実にするために、SSEベンダーは、以下の分野のリーダーとの統合を提供する必要があります。

- クラウドサービスプロバイダー（CSP）、IaaS/PaaSとSaaSの両方
- EDR（エンドポイントディテクションアンドレスポンス）
- SD-WAN
- Identity and Access Management（IAM：アイデンティティとアクセス管理）
- セキュリティ情報およびイベント管理（SIEM）/セキュリティオーケストレーション、自動化、および応答（SOAR）
- オーケストレーション
- ツール

これらの統合により、SSEベンダーと隣接するベンダーとの間でオーケストレーションが可能になり、複雑さやTCOの削減、セキュリティ態勢の向上が期待できます(図17参照)。

クラウドサービスプロバイダー（IaaS/PaaS、SaaS）

クラウドに移行する社内アプリケーションやクラウド上でネイティブに構築されるアプリケーションについては、SSEベンダーはAWS、GCP、Azureなどの主要なIaaS/PaaSプロバイダーを統合し、これらのアプリケーションへのゼロトラストの安全なリモートアクセス接続を提供しなければなりません。このようにすることで、これらのアプリケーションはインターネットに公開されることがなく、権限のないユーザーからは完全に不可視となり、ネットワークを拡張するのではなく、インサイドアウト、ポリシーベースの接続を介して接続することができます。

このアプローチでは、リモートアクセスVPNを経由せずに直接クラウドにアクセスでき、ネットワークのセグメンテーションを複雑にすることなく、クラウドプロバイダーのスケールメリットを活用することが可能です。仮想アプライアンスや物理アプライアンスに依存せず、ゼロトラストの利点を生かして攻撃対象領域を排除します。

一般的なSaaSアプリケーションの場合、SSEベンダーはワンクリックで統合できるようにする必要があります。Microsoft 365の場合、SSEベンダーの統合は、リストされたM365アプリのすべてのMicrosoft IPレンジとドメインをマッピングし、エンドユーザーのトラフィックをそのクラウドに透過的に転送することを可能にする必要があります。また、Microsoft 365とのピアリングにより、往復時間の短縮、スケールの向上、ファイルのダウンロードやDNSの解決の高速化を実現します。

SSEとServiceNowなど他のSaaSベンダーとの連携により、データ保護を向上させることができます。SSEベンダーは、新規および既存のServiceNowデータをスキャンすることで、DLPポリシーに基づいて機密データを特定し、機密データファイルのアウトバウンドアップロードをブロックする必要があります。ServiceNow Security Incident Responseとの統合により、カスタムブロックリストの更新を含む対応アクションのオーケストレーションが可能です。高リスクのIP、ドメイン、URLを手動の介入を必要とすることなくブロックでき、クラウドの構成ミスを解消することで侵害のリスクを軽減できます。

エンドポイントディテクション&レスポンス

SSEベンダーは、様々なエンドポイントセキュリティパートナーと統合し、テレメトリーの共有、相互の可視性の向上、対応のオーケストレーションを行う必要があります。このような統合により、ゼロトラストを効果的かつ効率的に実施するための深層防護が可能になります。

この統合により、ユーザーのアイデンティティ、ロケーション、デバイスのポスチャーを評価し、適切な条件付きアクセスポリシーを自動的に実行する機能が提供される必要があります。さらに、クロスプラットフォームの相関関係とワークフローにより、調査や対応を迅速化することができます。その内容は、以下の通りです：

- デバイスの健全性を評価し、適切なアクセスポリシーを自動的に実行。
- ゼロデイ脅威を特定し、エンドポイントテレメトリーとの関連付けにより影響を受けるデバイスを特定し、クロスプラットフォームの検疫ワークフローで迅速な対応を実施。
- 効果的な検知と意思決定のために、エンドポイントとネットワークのコンテキストを考慮した脅威の調査。

SD-WAN

SSEベンダーは、SD-WANベンダーと統合して、支店からのトラフィックルーティングを簡素化し、安全なローカルインターネットブレイクアウトを簡単に確立できるようにする必要があります。

SSE/SD-WANの共同ソリューションは、インターネットやビジネスに不可欠なアプリケーションへのセキュアでポリシーベースのアクセスを可能にし、クラウドアプリケーションやオープンインターネットに接続する場所と時間を問わず、すべてのユーザーに同一の保護を提供することができるのです。SD-WANソリューションは、API連携によりSSEと統合することが可能です。この統合ソリューションによって、支社においては、データセンタの中央DMZにバックホールすることなく、クラウドやインターネットトラフィックの急増に対応し、アジャイルハイブリッドWANアーキテクチャを使用したネットワークトランスフォーメーションと堅牢なセキュリティが実現します。

SSEベンダーは、ネットワークにとらわれず、どのネットワークアンダーレイソリューションとも排他的に結びつかないことが重要です。実際、SD-WANのメリットの多くはその「ソフトウェア定義」機能によるものですが、必ずしもWANが本質的に企業ネットワークを拡張し、脅威の横移動を可能にするわけではありません。SSEの意思決定者は、企業ネットワークを支店まで拡張し続ける理由を慎重に評価し、より安全な代替アプローチ（インターネットのみなど）を検討する必要があります。

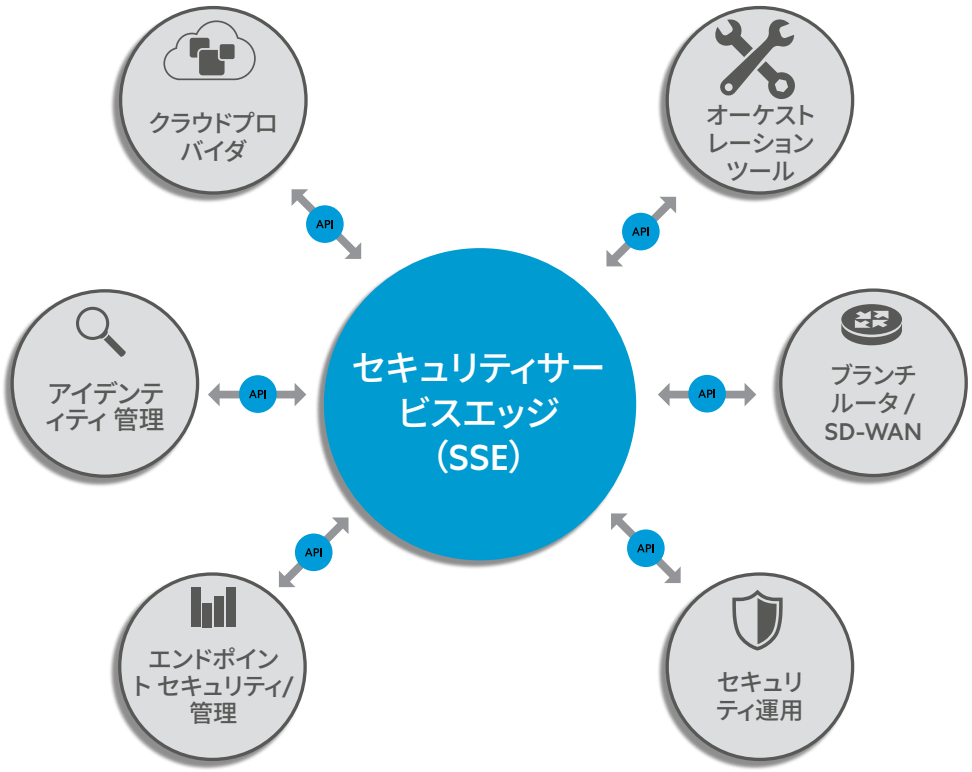


図 17: SSEベンダーは、様々な機能においてベストオブブリードのプレーヤーと統合する必要があります。

アイデンティティとアクセス管理

SSEベンダーは、IAMとの統合により、デバイスのポスチャーに応じたゼロトラストアクセスや、より効果的な企業全体の脅威防御を実現する必要があります。

SAML（Security Assertion Markup Language）などの標準を使えば、簡単に統合を展開できることになります。ユーザーは、インターネットや内部のアプリケーションへのアクセスを認証し、安全に行うことができる必要があります。IAMはSSOとMFAを組み合わせてエンドユーザーのアプリケーションへのアクセスを管理し、SSEベンダーは接続の安全性を確保します。SCIM（System for Cross-domain Identity Management）プロトコルに対応し、ユーザーグループや職務の変更、退社に伴うアカウント削除など、すべてのユーザー情報を2つのシステム間で同期させることができます。

SIEMとSOAR

SSEベンダーは、情報の充実と自動化により、効率的かつ効果的なリスクおよびコンプライアンス管理を可能にするために、SIEMおよびSOARベンダーとの統合を含める必要があります。

SSEベンダーは、オンプレミスおよびクラウドベースのSIEM/SOARソリューションにログデータをほぼリアルタイムで送信し、複数のソースからのログの相関関係を促進する機能を備えていなければならず、これにより企業はネットワーク全体のトラフィックパターンを分析できるようになります。さらに、企業はSIEMのログデータを活用して、長期的な履歴分析（6ヶ月以上）を行うことができなければなりません。これにより、ローカルのログをアーカイブすることで、法規制への準拠を保証します。

オーケストレーションツール

Infrastructure as Code (IaC) と DevSecOps により、セキュリティチームは「シフトレフト」を余儀なくされているため、SSE ベンダーはオーケストレーション用の API を提供する必要があります。ここでは、ゼロトラストアクセスのインスタンス化がアプリケーションデリバリーのライフサイクルの一部であり、オーケストレーションスクリプト（AnsibleやTerraformなど）、特にユーザからアプリケーション、ワークロードからワークロードのセグメンテーション設定によって可能になる内部アプリケーションに焦点を当てます。このようなオーケストレーションにより、ゼロトラスト機能は、ソフトウェア開発者が使用するアジャイル手法に合致するようになります。

Infrastructure as Code (IaC) と DevSecOps により、セキュリティチームは「シフトレフト」を余儀なくされているため、SSE ベンダーはオーケストレーション用の API を提供する必要があります。

⚠ 注意すべき点

SSEの意思決定者は、API 統合の深さ、更新頻度を評価し、将来の統合を妨げる可能性のある市場の変化（買収したベンダーが競合相手になるなど）を監視する必要があります。特にレガシーツールとの統合には専門的な能力が必要なため、組織内のスキルが不足していないかどうかを認識する必要があります。

成果：

SSEベンダーは、APIベースの豊富なサードパーティ統合機能を提供することで、最善のソリューションを編成する能力から生まれる運用効率と、ベンダーロックインの可能性を低減することができます。

- 主要なエコシステムプレーヤー（CSP、SD-WAN、IAM、SOAR/SIEM、EDRなど）と統合するSSEベンダーは、技術の将来性を確保し、技術的負債を軽減することができます。
- 統合されたベンダーによるオーケストレーテッドエコシステムは、運用の複雑さやオーバーヘッドを軽減し、オペレーターのミスを減らすことができます。
- 買収によってソリューションポートフォリオをまとめたSSEベンダーは、製品革新に遅れがちで、サードパーティとの相互運用性に欠けることが多くなります。

その7
落とし穴

本番環境パイロットで価値を発揮しにくいSSEソリューションを選択する

その代わりに、以下のようなSSEベンダーを検討してください：

- 単一の統合エージェントを提供し、世界中のユーザーに近い場所に存在するサービスエッジへのアクセスと一元化された使いやすいUIによるシームレスなアクセスを可能にするソリューション。
- SSEプラットフォームの様々な側面を、最小限の追加導入要件で試用。
- 販売後の労力を最小限に抑え、ソリューションが完全に導入された時点で意図したとおりに動作するという確信を提供。

図 18: SSEベンダーのテストドライブは、おもちゃのレプリカではなく、本物を使うようにします。SSEベンダーのソリューションの価値を証明できるのは、実稼働環境での試験運用だけです。

正しいSSEベンダーはこれをどのように実現するのか：

SSEプラットフォームを採用するには、セキュリティアーキテクチャを見直す必要があるため、SSEベンダーの選定を軽んじてはいけません。そのため、SSEベンダーの真の実力を理解し、お客様の本番環境に対応できる能力が重要です。その手軽さは、このプラットフォームのアーキテクチャを象徴しています。

SSEベンダーを検討する際には、試験運用に必要なステップを理解しておきましょう。適切なSSEベンダーであれば、SSEのサービスエッジにトラフィックを転送する方法を見つけ、SSEベンダー自身のクラウドに引き継ぐというプロセスになるはずです。SSE管理者が行うべきことは、転送メカニズムの確立、基本ポリシーの設定、認証、およびレポート作成以外の最小限の手順であるべきです。当然ながら、高度なポリシー設定にはより多くの時間がかかります。

この試験には、一連のビジネス成果を取り上げ、セキュリティ、ネットワーク、デスクトップ（例えば、エンドポイントエージェントのインストール）など、さまざまなチームのメンバーが参加する必要があります。しかし、これらのチームの積極的な関与は最小限にとどめるべきですが、その理由は結局のところ、SaaSソリューションの取得を目指しているという点にあります。SSEベンダーが、複雑なルーティングシナリオを試験的に処理するために、特にネットワークチームに深い関与を要求する場合は要注意です。

総合的なSSEソリューションの試験運用を計画する際には、ビジネス目標を反映した順次アプローチを行ってください。

1. 既存のセキュリティ体制、既存のポリシー、ネットワークインフラとアプリケーションの要件、認証技術、トラフィックフォワーディングのオプション、容量をレビューする。
2. 試運転を実行するソースユーザー/サービスのセットと、デスティネーションアプリケーションのセットを特定する。
3. これらのユーザーに対してトラフィック転送を有効にする。最も一般的な方法はシングルエージェントですが、ブランチロケーションからトンネルを作成することも可能です。選択したプライベートアプリケーションの前にバーチャルマシンを導入
4. Identity Providerの統合をプロビジョニングして、ユーザー認証を設定します。
5. 脅威対策、サンドボックスポリシー、ブラウザコントロールポリシー、URLポリシー、クラウドアプリポリシー、ファイルタイプコントロール、SaaSのAPI統合、ファイアウォールポリシーなど、標準テンプレートを使用して脅威対策やデータ損失対策を設定します。
6. プライベートアプリケーションのサーバーディスカバリーと、それらのアプリケーションのアクセスポリシーを設定します。これは、試運転の目的のために*.*ポリシーにすることができます。
7. SSL/TLSインスペクション、アドバンストポリシー、CBI、DEM、CSPMなどの追加機能を設定することができます。

上記の手順はすべて簡単で、SSEベンダーは短時間（おそらく数日）で、大規模なルーティングや設定の見直しをすることなく、達成できるはずです。実際の本格的な導入には、さらなるステップ、高度なポリシー設定、さまざまなタイプのアプリケーションやエンドポイントへの対応、他のエージェントやテクノロジーとの統合や共存などが必要になりますが、SSEベンダーは、簡単か上手く実行されたパイロット版を通じて、プラットフォームの価値を示すことができるはずです。

試用期間中、SSEベンダーは、この文書で詳述されている6つの 以前のプラクティスに沿って、以下を証明することができなければなりません。

- **高い可用性とパフォーマンスで運用される、エンドユーザーへのレイテンシーが最小限のグローバルクラウドインフラである** ベンダーは、このクラウドを大規模に運用する能力を示し、フェイルオーバーの効果を実証する必要があります。
- **すべてのユーザセッションに対するゼロトラストであり**、プライベートアプリケーションの保護から、パブリックアプリケーション、さらにはワークロード間通信（試用期間に要求される場合）までカバーする。
- **暗号化トラフィックへのピアリングによる高度な脅威防御とDLP**。証明書の管理には試験的にいくつかの追加ステップが必要かもしれませんが、ベンダーが SSL/TLS 検査を最小限のレイテンシーで行えることを証明することは、あるSSE ベンダーと他のベンダーを差別化する優れた方法です。
- **柔軟なデプロイメントオプション** である。これは試験運用の一部ではないかもしれませんが、SSEベンダーは、場所やアプリケーションに関係なく、すべてのユーザを保護する計画を提供しなければなりません。プライベートサービスエッジや請負業者向けのCBIのデプロイを理解する必要があるかもしれません。確認すべき重要なポイントは、SSEベンダーのデプロイメントモデルによって、分散した従業員やアプリケーションの要件を満たすことができるかどうかです。

- **最適なユーザエクスペリエンス**。この指標は、使いやすさ（例えば、エンドユーザがエージェントとどのようにインターフェースするか）から、SSEプラットフォーム上でパブリックおよびプライベートアプリケーションにアクセスする際の一般的なユーザエクスペリエンスまで、多岐にわたります。ベンダーは、エンドユーザのパフォーマンスに関する幅広い問題（Wi-Fi、ISP、CPUなど）を測定および診断できる必要があります。この測定／診断機能は、新たなエージェントを導入することなく、SSEプラットフォームに直接組み込まれる必要があります。
- **サードパーティベンダーの統合** 。これも試用版の一部ではないかもしれませんが、ベンダーはログデータを外部のSIEMツールに統合する方法、または既存のEDRツールと統合する方法を提供する必要があります。SSEベンダーは、導入されているツールのエコシステムを分析し、実際のデプロイメントが始まった時点で統合するための推奨事項を提供する必要があります。

業界内におけるスキルや人材不足を考慮し、必要となるオーバーヘッドの少ないSSEベンダーを優先的に採用します。

SaaS型セキュリティベンダーの利点は、通常社内のスタッフが行っている業務をSSEベンダーに任せることができることです。試用期間は実装、管理、SSEソリューションのアップデートにどの程度の労力がいるかを明確に示唆することが出来る必要があります。

⚠ 注意すべき点

- 試運転ではあらゆる可能性を試すことはできませんし、実際の配備では予期せぬ問題が発生する可能性があります。
- SSEベンダーが顧客中心に考えていることを確実にして、実装にあたっての問題を克服しようとする姿勢を示しましょう。
- 試運転版ではスケールを見ることができない可能性が高く、破壊されてしまうケースを見ることもできないかもしれないことを忘れないでください。SSEベンダーは、試験運用中に酷いネットワークやルーティングの問題が露呈することを避けることができます。正しいSSEベンダーは、機能するためにネットワークルートに一切依存しないベンダーであるべきです。
- SSEベンダーが所有するものと、自社が所有するものと、必要な管理のオーバーヘッドを考慮してください。その上で、本番展開に必要な労力と、ソリューションの継続的なメンテナンスに必要な労力を把握しましょう。
- SSEベンダーの中には、真のSaaSでない場合もあります。SSEソリューションの管理は、総所有コスト（TCO）が最も低くなるようにすることで、特に大半のIT組織が直面している人材スキル不足の現状においてはこれは重要です。

成果：

価値ある試運転版というものは、SSEソリューションの導入が容易であること、本番環境でのパフォーマンスが高いこと、そして目的を達成できることを証明します。

- SSEベンダーは、ソリューションをシームレスに試験的に導入することができるため、本格的な導入に適しています。TCOの削減を目標に、単一の統合エージェント、グローバルなサービスエッジへのアクセス、集中的で使いやすいUIなど、ソリューションの継続的なメンテナンスを容易にするための要素が揃っています。大規模な導入には時間と労力が必要ですが、それを最小限に抑えるベンダーと組むことを目標にすべきです。
- SSEのアーキテクチャとデザインは、最小限の追加導入要件（追加のエージェントやVMなど）で、簡単に機能を追加できるようにする必要があります。こうすることで、バイヤーはSSEに段階的にアプローチすることができ、フェーズ間の移動に負担がかかる必要はありません。
- 最終的には、SSEベンダーが本番環境にスムーズに導入でき、避けられないトラブルにも対応してくれると確信することが目標です。顧客を重視し、実績のあるアーキテクチャを持つベンダーは、セキュリティとネットワークの変革への投資を成功させるための最良の手がかりとなります。

決断するのはあなた自身です

企業が新しい道に惜しみなく投資するような「ビッグバン」がやってくるというのは、非常に稀です。そのため、企業はSSEを実現するために、慎重なアプローチを考慮する必要があります。エンタープライズSSEの範囲（https://trust.zscaler.com を通して公に共有されているもの）、想定されるすべてのユーザ、サーバー、デバイスなどへの対応は、「落とし穴その2」で説明されています。以下に、SSEの採用について、同世代の人たちがどのように取り組んできたかについてが説明されています：

参考A:

お客様がZscaler SSEプラットフォームを導入し、以下の点についてゼロトラストコントロールの実現を目指した。

- エンドユーザーのプライベートサービスへのきめ細かなアクセス
- インライン検査やデータ保護などを含む、エンドユーザー向けインターネットセキュリティ
- ユーザーをネットワークから完全に排除したネットワーク変換
- ワークロード、インターネット、プライベートアクセスの保護
- 第三者によるアクセス制御の制限

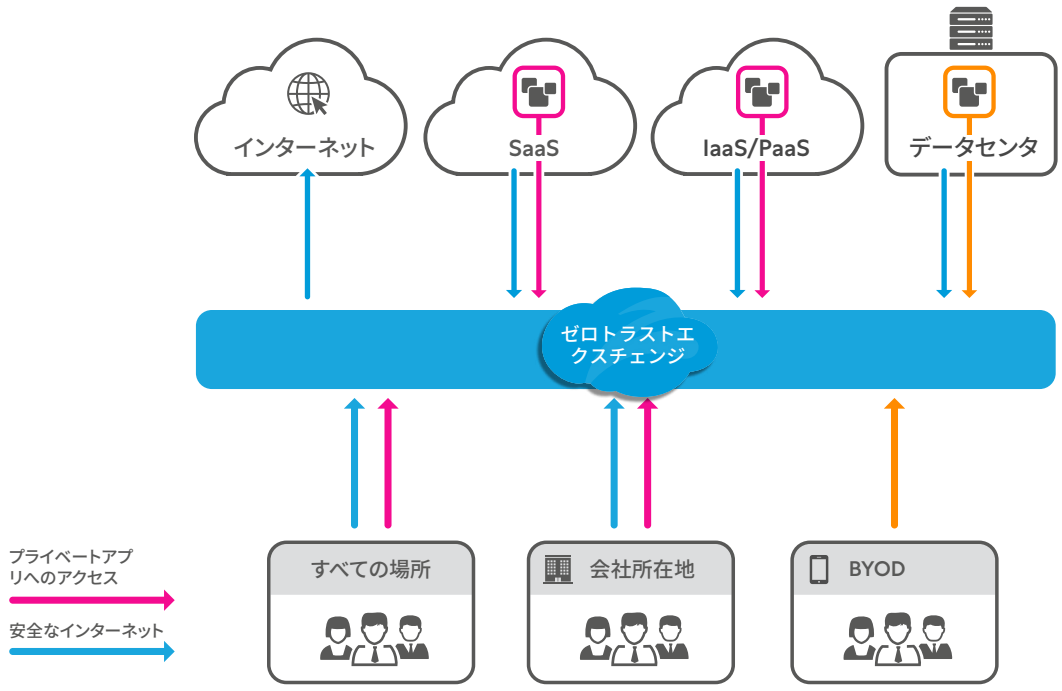


図 19: Zscaler を使用したエンタープライズデプロイメントの接続性をハイレベルで表現しています。

SANDVIK

「VPNをゼットスケーラーのゼロトラストネットワークアクセスソリューションに置き換えることで、5日足らずで2万人の従業員をスムーズかつ安全に、コスト効率よくWFAに移行させました」

Sandvik Groupサイバーセキュリティ&テクノロジー部門 サービスマネージャー Michael Alvmarken氏

reckitt

「ゼットスケーラーのクラウドインフラストラクチャとZIAやZPAとのネイティブ統合を活用することで、エンドユーザに関する最高のデータインサイトを得られるようになりました。」

- Reckitt Benckiserのエンタープライズアーキテクチャ担当ディレクタ、John Dawes氏

SIEMENS

「トラフィックをバックホールすることなく、インターネットへのダイレクト接続を利用することで、70%のコスト削減を達成できる見込みです。」

Siemensのグローバルインフラストラクチャポートフォリオ担当バイスプレジデント、Frederik Janssen氏

参考B:

- お客様は、Zscaler SSEプラットフォームを以下の目的で導入されました:
- すべてのインターネットサービス(クラウドとそれ以外)へのアクセスの完全な可視化
- 企業の知的財産の損失を制限するための完全なインラインコントロール
- デジタルエクスペリエンスによる在宅勤務中のユーザーアクセスの監視

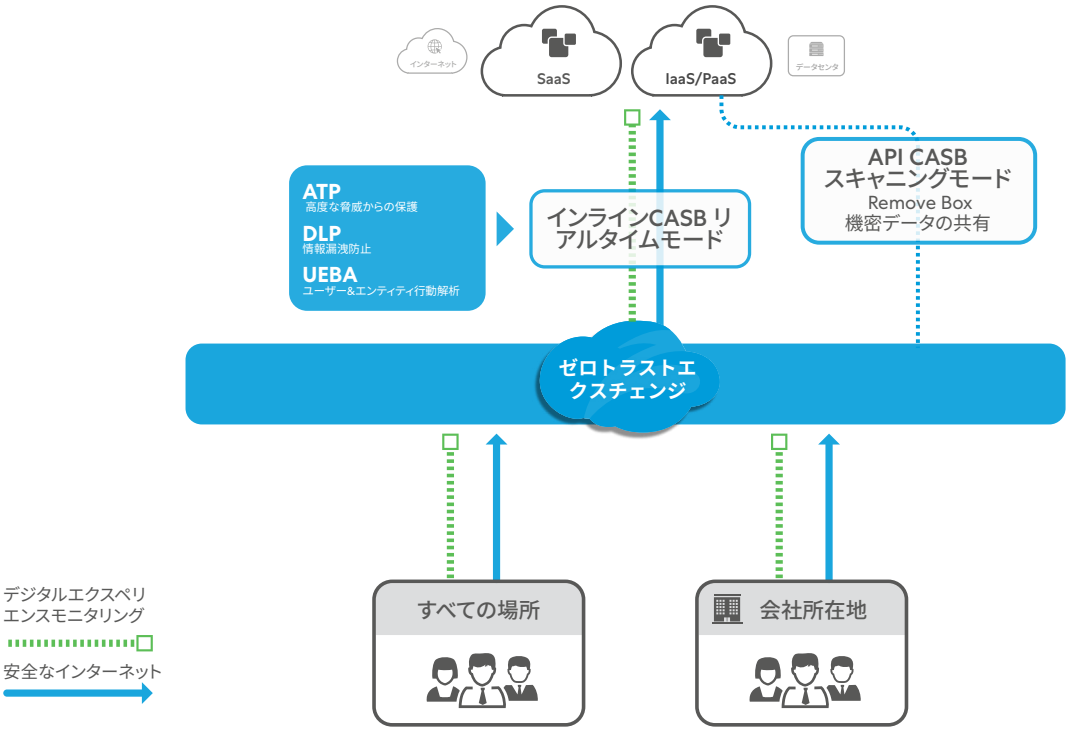


図 20: Zscaler によるインライン検査と体感モニタリングの例。

ciena

「Zscaler Digital Experienceは我々にとって、あらゆる場所で生産的に働くために不可欠なサービスです。これまでにユーザが抱えていた問題の25%を解決できました。ZDXをすべてのユーザエクスペリエンスの問題を解決する出発点と使用することで、95%の根本原因を特定できるようになりました。」

- Cienaプリンシパルセキュリティアーキテクト、Ed DeGrange氏

SIEMENS

「商取引や不正の問題であれ、ウェブサイト上のものであれ、内部不正であれ、すべては財務的な影響を及ぼすものであり、だからこそセキュリティはその一部でなければなりません。」

Siemensのグローバルインフラストラクチャポートフォリオ担当バイスプレジデント、Frederik Janssen氏

BOMBARDIER

「Zscaler Advanced Cloud Sandboxがあれば、IT部門に重い負担をかけることはありません。今日の人材マーケットは非常に厳しく、採用は非常に困難であるため、これは非常に重要なことです。」

ボンバルディア社 CISO Mark Ferguson氏

参考C:

お客様は、Zscalerのプラットフォームを使用して、非ITサービスのきめ細かい保護を実現:

- 従業員および第三者のオペレーション技術(OT)に対するゼロトラスト
- OTからワークロード
- クラウドからワークロード

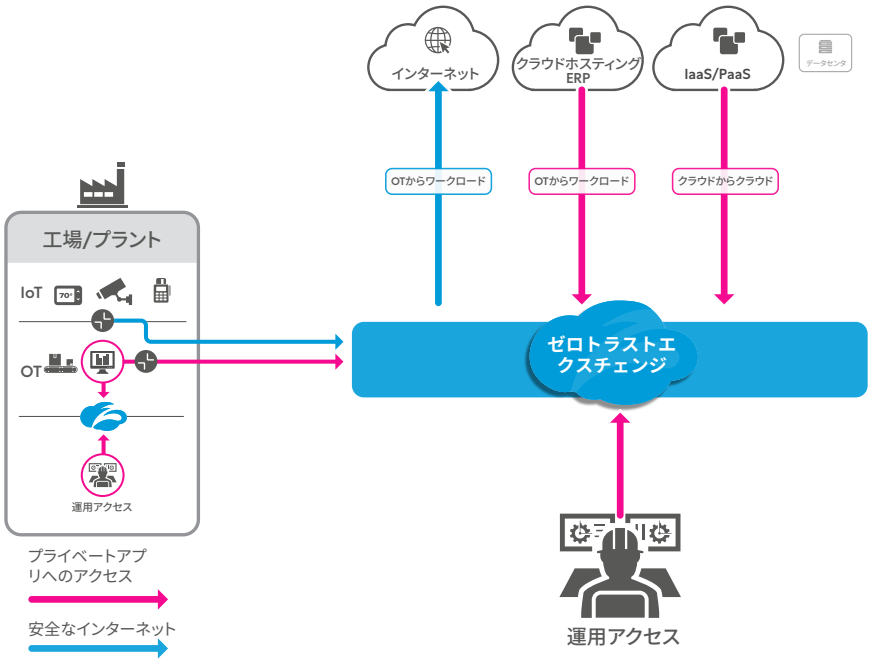


図 20: Zscaler によるインライン検査と体感モニタリングの例。

要点

SSEベンダーは、サービスの損失または劣化に基づく文書化されたSLAを提供しなければならない。

SSEソリューションは、インライン、グローバル、キャリアニュートラルなピアリングポイント内のすべてのサイトで実施され、顧客への最も効果的なパスを確保する必要がある。

SSEベンダーは、あらゆるプロトコルを介して、許可されたすべての企業ユーザ、ワークロード、デバイスに対してゼロトラスト制御を提供しなければならない。

SSEソリューションは、どのようなネットワーク上でもアグノスティックにサービスを提供する必要がある。

SSEベンダーは、最小限のレイテンシーを確保し、すべてのウェブトラフィック（TLS 1.3まで）を完全に可視化できるプロキシクラウドアーキテクチャを通じて、インライン検査を提供する必要がある。

SSEソリューションは、大規模な復号化のための独自のスケーラビリティの利点のために、単一のメモリスキャンアーキテクチャを通じて複数のセキュリティ制御を提供する必要がある。

SSEベンダーは、そのソリューションを一元的に管理し、顧客の所在地、地域、地域性、機能のカスタマイズに対応した複数の形態でデプロイできるように提供しなければならない。

SSEソリューションは、非管理対象のBYOD、サードパーティ、パートナーのアクセスに対して、従業員と同じレベルのきめ細かい制御による保護を提供するように拡張する必要がある。

SSEベンダーは、企業向けサービス（Teams、Zoomなど）のパフォーマンス問題を監視および診断し、ユーザクスペリエンスを最適化する必要がある。

SSEソリューションは、アプリケーションパス、エンドポイント、ネットワーク層からメトリクスを収集して異常を特定し、サポートチームに洞察を提供する必要がある。

SSEベンダーは、クラス最高のエコシステムプレーヤー（CSP、SD-WAN、IAM、SOAR/SIEM、EDRなど）と統合し、企業の全体像に完全な詳細制御とセキュリティをもたらす必要がある。

SSEソリューションは、これらのベンダーと統合し、運用のオーバーヘッドを最小化するオーケストレーションを提供する必要がある。

SSEベンダーは、企業が必要とする機能とロケーションを本番環境でシームレスに試験運用することができなければならない。

SSEソリューションは、ハードウェアやエージェントを追加することなく簡単に拡張でき、企業が段階的なアプローチでSSEの利用を拡大できるようにする必要がある。

SSEの詳細については、こちらをご覧ください。

著者紹介

Sanjit Ganguli (VP, Transformation Strategy / Field CTO) and Nathan Howe (VP, Emerging Technology& 5G)
Gartner, Nestle, Riverbed, Verizonなどの企業と世界規模に渡るキャリアを持ち、クラウド、セキュリティ、変革、新興技術の分野においてリーダーシップを発揮しつつ革新的視点をもたらしている。