ホワイトペーパー

SD-WAN を超えて：

企業 WAN としてのゼロトラスト・セキュリティと インターネット

SD-WAN、セキュアアクセス、脅威防御が一体となっている理由

Akamai

エンタープライズ WAN の将来

広域ネットワーク（WAN）は、コンピューター間通信のごく初期である 1960 年代から存在してきました。WAN は、テクノロジーの進化やトラフィック需要の増大に伴い、今も発展と強化を続けています。今日のエンタープライズにとって、WAN は統一された拠点横断ネットワークを実現するインフラストラクチャとなっています。

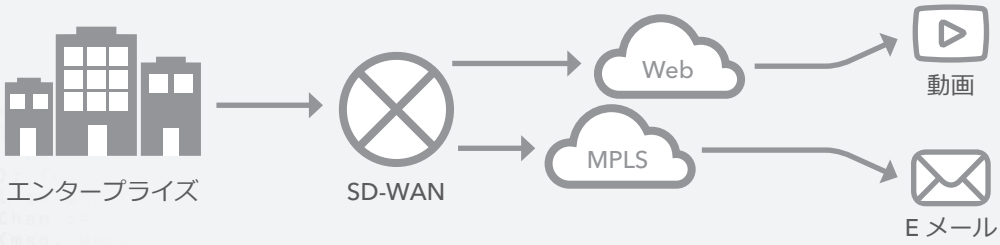
ただし、この重要な基礎構造には制約もあります。多くの場合、WAN では帯域幅が十分にないため、特定のアプリケーションのパフォーマンスに問題が生じたり、信頼性が安定しなかったりします。またビジネスにセキュリティ上のリスクをもたらす可能性もあります。さらに、WAN は専用線上、つまりサービスプロバイダーから借りた回線に構築されることが多く、サービスプロバイダーのインフラストラクチャでは、公衆インターネットのほかに、非同期転送モード（ATM）やマルチプロトコル・ラベル・スイッチング（MPLS）などの回線交換方式またはパケット交換方式が使用されています。パケット交換方式のほうがコストはいくらか低くなりますが、現状ではまだかなり費用がかかり、拡張にも適していません。

変わりつつある企業ネットワーク

エンタープライズはこのようなパフォーマンス、セキュリティ、コストの課題に対応するため、コスト削減と俊敏性の両方に役立つソフトウェア定義 WAN（SD-WAN）を採用しつつあります。

これは、元々データセンターで使用されていた新技術であるソフトウェア定義ネットワーキング（SDN）とネットワーク機能の仮想化（NFV）から発展したテクノロジーですが、すぐに企業の IT 部門によって組織間を接続するネットワークに採用されるようになりました。

簡単に言うと、SD-WAN は WAN のデータプレーンと制御プレーンを区分します。さまざまなデータ接続方式（MPLS、ATM、インターネット）が混在する WAN のパフォーマンスを監視し、現状のリンクパフォーマンス、接続コスト、アプリケーションやサービスのニーズに基づき、各トラフィックタイプに最も適切な接続を選択するのです。



SD-WAN の仕組み

SD-WAN が E メールを MPLS 経由でルーティングするのは、レイテンシーがそれほど重要視されず、ビット当たりの送信コストが最も安価であるためです。一方、SD-WAN はビデオ会議トラフィックについてはインターネット経由でルーティングし、ビット当たりの送信コストは高くなっても、最適なパフォーマンスと最小限のレイテンシーが保証されるようにします。

インターネットは新しい企業 WAN になり得るか？

公衆インターネットを含む複数のトランスポートサービスを使用する場合、SD-WAN は、明らかに柔軟性が高く、効率的で、コスト効果の高い手法です。公衆インターネットのようなトランスポートオプションにはパフォーマンスの保証や SLA がないため、SD-WAN ではパフォーマンスが重要視されないアプリケーションのみにインターネットを使用します。

インターネットの利用を拡大することで、企業 WAN トラフィックの効率やコスト効果を高め、セキュリティも強化するためには（さらに既存の SD-WAN 環境と共存できる方法でこれらを行うには）、インターネットに内在する制約を排除するアプローチを採用する必要があります。これを実現する 1 つの手段として、Edge プラットフォームを使用すれば、ビジネスアプリケーションをインターネット上で公開することなく、インターネット経由で安全、高速、確実に配信できます。この方法では、SD-WAN への既存の投資を最大限に活用しながら、さらに多くのトラフィックをインターネットに移行し、コストを軽減できます。

近年の企業ネットワークの状況を考えれば、エンタープライズトラフィックのうちインターネットにルーティングされる部分を拡大することは理にかなっています。クラウドワークロードの増大に、ユーザーやデバイスの多様化やモバイル化が加わり、ワークフローはすでにインターネットに大きく依存しています。しかも、この傾向はさらに拡大しつつあります。

もう 1 歩前進することで、安全で拡張性が高く効率的な企業 WAN をインターネットを通じて確立できるとしたら、どうでしょうか。

このホワイトペーパーでは、SD-WAN とゼロトラスト・セキュリティによってネットワークを変革するプロセスについて説明するとともに、SD-WAN を超えた進化として完全にインターネットベースの企業ネットワークを採用するにあたり、組織が現在どのような状況にあるかを判断する方法について考察します。

Edge プラットフォームを使用すれば、ビジネスアプリケーションをインターネット上で公開することなく、インターネット経由で安全、高速、確実に配信できます。

2023 年末までに、WAN エッジインフラストラクチャ刷新の取り組みは、その 90% 以上が従来のルーターではなく、仮想顧客構内設備（vCPE）プラットフォームまたはソフトウェア定義 WAN（SD-WAN）ソフトウェア／機器に基づくものとなります（現在の 40% 未満から拡大）。」

– Gartner、『Magic Quadrant for WAN Edge Infrastructure（マジッククアドラント WAN エッジインフラストラクチャ）』、2018 年 10 月

SD-WAN の価値

SD-WAN が提供する主な機能は、リンクのバランス、デバイスの自動設定、サードパーティーのセキュリティサービスの挿入です。これらの機能の価値、つまり、ユーザー体験の向上やリンクコストおよび OpEx の軽減は、ビジネスに大きな効果をもたらす可能性があります。これらについて明確に理解していただけるよう、図も示して説明していきます。

多数のベンダーがさまざまな SD-WAN 機能を提供していますが、それらは大きく 3 つのカテゴリーに分類できます。

1. **柔軟なリンク制御**
2. **管理機能**
3. **サービスの挿入**

柔軟なリンク制御

最初の機能である柔軟なリンク制御は、SD-WAN の第 1 原理です。多くの組織にとってクラウドが主な目標となっている今、プライベートネットワークを介してトラフィックをデータセンターにバックホールし、データセンターを事実上の集中管理制御ポイントとすることは現実的ではありません。SD-WAN は、動的ルート選択などのインテリジェントなトラフィック制御を使用することで、この課題を解決します。さらに SD-WAN は、ダイレクト・インターネット・アクセス（DIA）として知られるローカルまたはブランチのインターネットブレイクアウトを確立し、データセンターを経由せずにクラウドへトラフィックをルーティングできます。これにより、音声や動画を含めた従来型アプリケーションには MPLS リンクを指定し、クラウドアプリケーションとインターネットトラフィックは直接インターネットに接続することが可能になります。

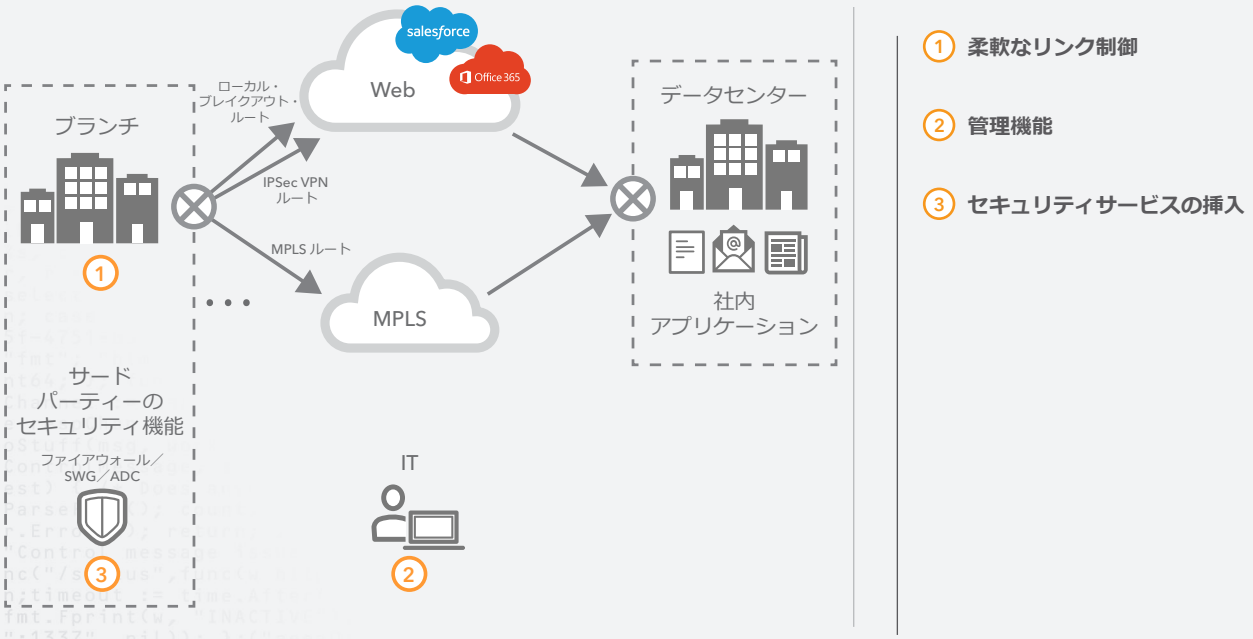
管理機能

SD-WAN ベンダーは、ネットワークデバイスの運用と管理をシンプルにする管理機能も提供できます。1990 年代以降、エンタープライズ WAN はマルチレイヤースイッチやルーターなどのネットワークデバイスで構成され、これらのデバイスは主に機器単位で管理されてきました。つまり、管理者は組織全体の数百台から数千台にものぼるデバイスを個別に設定、保守し、各デバイスのソフトウェアスタックを監視する必要があるのです。たとえデバイスが動的にルーティング情報を交換したり、ルーティングプロトコルを使用して高可用性を確立したりしても、その労力は甚大です。SD-WAN では、1 つの集中管理用コンソールですべてのデバイスを管理できます。

サービスの挿入

一部の SD-WAN プロバイダーはサービス挿入に特化しています。WAN の最小要件は、IP で到達可能であること、つまり組織を横断するレイヤー 3 ネットワーク接続であることです。しかし、ネットワーキングの進化に伴い、セキュリティ機能、たとえばファイアウォール、侵入防御システム（IPS）、アプリケーション配信制御なども同様に進化してきました。以前は、これらの機能をネットワークに追加するために複雑なルーティング設計が必要でした。このようなサービスを提供するデバイスは多くの場合、Open Shortest Path First（OSPF）、Border Gateway Protocol（BGP）のような動的ルーティングプロトコルに対応していないため、静的ルーティングと再配信の複雑な組み合わせが生じていたのです。SD-WAN を使えば、これらのテクノロジー（多くの場合、サードパーティーを通じて配信されます）を、共通のポータルを通じて簡単に設定し、管理できるようになります。

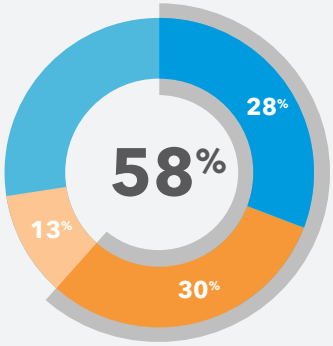
SD-WAN のビジネス価値



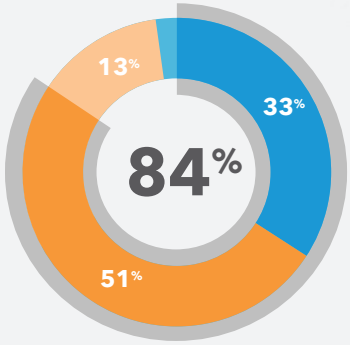
新たなモデル：ゼロトラスト・セキュリティ

新しいアーキテクチャには新しいセキュリティが必要です。トランザクションがクラウドやインターネットに移行するのに伴い、ネットワークは高度に分散し、アタックサーフェス（攻撃の対象となり得る領域）が追加されていきます。アプリケーション、ユーザー、データ、デバイスが従来の制御ゾーンの外に移動していくと、これまでの信頼できるエンタープライズ境界は意味を失います。そのため、企業の境界に依存するセキュリティモデルはもはや成立しません。新しい防御戦略は、ワークロードや従業員が分散している現状に適したソリューションでなければなりません。

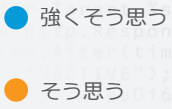
どの程度同意しますか？同意しませんか？



「分散したクラウドネットワークやモバイル／リモートユーザーによる今日のテクノロジーエコシステムでは、ネットワーク境界は防御不能である」



「デジタル変革には、従来の（境界ベースの）セキュリティ戦略に対する調整が必要となる」



Forrester Research、『Build Your Zero Trust Security Strategy With Microsegmentation（マイクロセグメンテーションでゼロトラスト・セキュリティ戦略を構築）』、2018 年 9 月

ゼロトラスト・セキュリティ・モデルでは、「内側」は存在せず、すべてのユーザーとデバイスが等しく信頼できないものと想定されています。あらゆるアクセスリクエストに認証と許可が必要です。アプリケーションやデータは検証が終わるまで配信されず、検証後も、配信は一時的なもので、その範囲も限られています。このセキュリティフレームワークは、すべてのアプリケーションをインターネットにさらされているものとして扱い、ネットワークは侵害されうるもので敵意に満ちた環境であるとみなします。さらに、可視化も重要です。完全なロギングおよびふるまい分析は必須の機能といえます。

ゼロトラスト・セキュリティの基本原則：

- **場所やホスティングモデルに関係なく、すべてのリソースへの安全なアクセスを保証する**
- **アプリケーションアクセスについては「最小権限」と「デフォルト拒否」の戦略を採用する**
- **管理下と管理外の両方のアプリケーションへのトラフィックを検査し、記録することで、悪意ある活動を特定する**

ゼロトラスト・セキュリティの実装をサポートする 2 つの主なコンポーネント：

- **ID 認識型プロキシ - 安全なアプリケーションアクセス**
- **セキュア・インターネット・ゲートウェイ - ユーザーの保護**

ID 認識型プロキシ - 安全なアプリケーションアクセス

ユーザー、データ、アプリケーションがクラウド上に存在し、SD-WAN が実現するダイレクト・インターネット・アクセス（DIA）によって接続が提供されているのなら、なぜセキュリティと DMZ スタックもクラウドに移行しないのでしょうか。ゼロトラストを活用すれば、管理下のアプリケーションに安全にアクセスできるようにしながら、管理外のユーザーによるアプリケーションアクセスに関連したリスクも緩和できます。

現在、社内アプリケーションへのアクセスにシンプルな VPN 設定を選択している場合は、ログインしているユーザーに対してネットワーク全体への IP レベルのアクセスを許可している可能性が高いと考えられます。これは非常にリスクが高く、ゼロトラスト・セキュリティの原則に反します。コールセンターの従業員にソース・コード・リポジトリへのアクセス権は必要でしょうか。自社の課金システムを使用している業務請負業者に、クレジットカード処理端末へのアクセス権を持たせる必要があるでしょうか。アクセス権の付与は、役割を果たすために必要なアプリケーションに対するもののみに制限すべきです。従来の VPN では、このようなきめ細かいアクセス制御はできません。それどころか、ハブアンドスポーク方式のネットワークモデルに依存し続ける必要があります。

ID 認識型プロキシ（IAP）のアーキテクチャでは、クラウドベースのプロキシを通じてアプリケーションへのアクセス権が提供されます。アイデンティティと認証は、「知る必要がある」という最小権限の原則に基づいてエッジで発生します。これはソフトウェア定義境界（SDP）を通じたアクセスと似ていますが、IAP ではアプリケーションレイヤー（レイヤー 7）の標準 HTTPS プロトコルが使用されます。

IAP が役立つ 2 つの用途

複数の国にまたがるトランザクションに CDN を統合し、 アプリケーションの応答を改善する

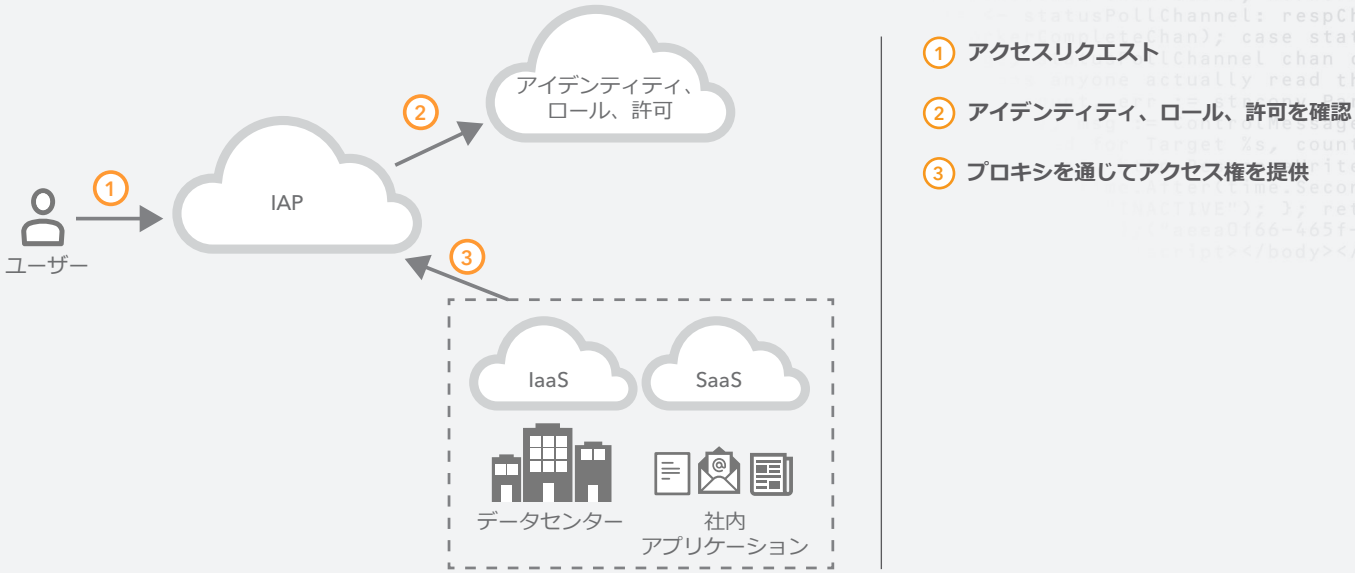
または

Web Application Firewall（WAF）を使用して、 SQL インジェクションやクロスサイトスクリプティングなどの一般的な脆弱性に対して社内ウェブサーバーを保護する

IAP の主な構成要素は、ユーザーとデバイスの信用を検証するアイデンティティソース（認証）と、何へのアクセスが許可されるか（許可）です。このアイデンティティソースは社内ディレクトリーやクラウドベースのアイデンティティプロバイダーをベースにすることができます。ユーザーのアイデンティティを検証する前に、デバイスのセキュリティ状態を調べることもできます。たとえば、証明書の所有、最新 OS の稼働、パスワードによる保護、適切なエンドポイント検知・応答ソリューションがインストールされ稼働していることなど、アクセスしようとしているデバイスが特定のセキュリティ基準を満たしているかどうかを確認できます。

他のアクセステクノロジーと比べて、IAP には大きなメリットがあります。それは、ユーザーを検証するだけでなく、ユーザーのトラフィックを検査し、個々のアプリケーションへのリクエストを止めて、検証し、許可できる点です。トランザクションをプロキシで終端すれば、追加サービスを統合することで、ユーザー体験とアプリケーション保護を強化できます。

ID 認識型プロキシ（IAP）



さらに、IAP はファイアウォールのルールではなくアプリケーションレベルのアクセス制御に依存しているため、設定されるポリシーに、ポートや IP だけでなく、ユーザーやアプリケーションの意図を反映させることも可能です。SDP と同様、アプリケーションや他のアセットをクラウド内やファイアウォールの背後に隠すことができます。また、ウェブアプリケーションへのアクセスはクライアントレスです。

クラウドの採用が広まるにつれて、社内アプリケーションを移行する際の課題が注目を集めるようになってきました。多くの組織は、クラウドネイティブのアプリケーションと従来のアプリケーションに同じようにクラウドを活用しようとして苦闘しています。IAP は、ネイティブ SaaS アプリケーションのユーザー認証に利用できるだけでなく、データセンター内の従来のアプリケーションを本質的に「SaaS 化」するためにも使えます。さらに、プロキシを利用することで、一気にすべてを置き換えるという最終手段を採らなくても、クラウドへの移行とアプリケーションの最新化を進めることができます。つまり、系統的なアプローチで少しずつゼロトラストを導入し、古い境界ベースの制御や従来の VPN に関連したテクノロジーの負債を減らしていくことができるのです。

セキュア・インターネット・ゲートウェイ - ユーザーの保護

ゼロトラスト・セキュリティ・モデルへの移行における重要な要素の 1 つは、管理下にないアプリケーションにユーザーがアクセスしても、ユーザーの安全が維持されることです。インターネットでクリックをするたびに、その陰には膨大な数のサイバー脅威が潜んでいます。以前、ユーザーが企業ネットワークや管理対象のデバイスに結び付けられていたときには、マルウェア、ランサムウェア、フィッシングに対する防御はシンプルでした。エンドポイントでアンチウィルスを展開し、データセンターに機器のスタックを設置し、検査と制御のトラフィックをバックホールしていました。

複数の場所にユーザーがいる場合は、インターネットが企業ネットワークの選択肢となります。クラウドベースの SIG は安全な入口を提供し、ユーザーがどこにいても事前対応型の保護をユーザーに提供します。

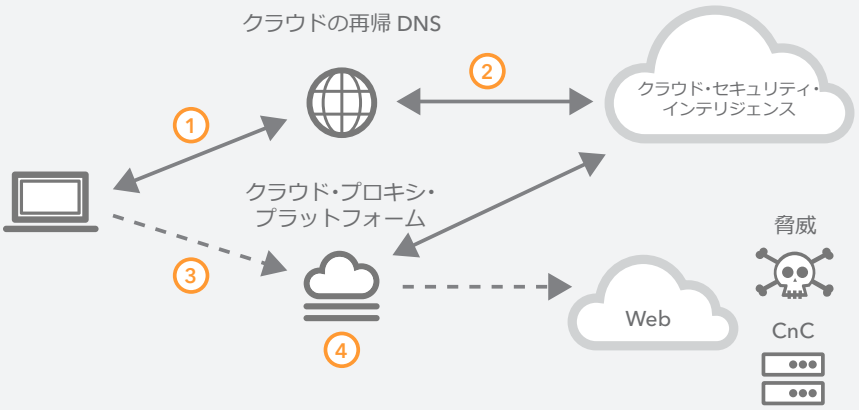
しかし、ユーザーは建物の外に出て、デバイスは管理下になくなり、インターネットが企業ネットワークの選択肢になりつつあります。DIA 接続は、制御と検査を集中管理するセキュリティソリューションを時代遅れなものにしてしまいます。代替として、各インターネットブレイクアウトでセキュリティ機器のスタックを複製する方法があります。しかし、ほとんどのエンタープライズにとって、ロジスティックの面でも予算の面でも、現実的とはいえません。さらに、もっと問題と思われるのは、このアプローチには複雑さが内在しているため、セキュリティの欠陥が導入され、ゼロトラストのベストプラクティスとはまったく異なる設計になる点です。

よりシンプルで、高速かつコスト効果の高い方法で DIA トラフィックのセキュリティを確保するためには、クラウドベースのセキュア・インターネット・ゲートウェイ（SIG）を使用します。SIG は、インターネットへの安全な入口であり、リスクの高いトラフィックを制御および検査するためにプロキシすることで、高度な脅威に対抗し、ユーザーがどこにいても事前対応型の保護を提供します。このような保護は、すべての DNS リクエストを個々に調べて、悪意あるドメインへのリクエストはブロック、安全なドメインへのリクエストは通常どおりに処理、また、リスクのあるドメインへのリクエストはクラウドプロキシに転送して、さらに検査を進めるという方法で実現します。

この最後の段階では、プロキシは HTTPS リクエストを受信すると、リクエスト先 URL をクラウドベースの脅威インテリジェンス・ナレッジ・ベースと照合し、悪意ある URL をブロックします。高リスクカテゴリーに分類されているその他のリクエスト先 URL の場合、プロキシはそのウェブコンテンツを複数のマルウェア分析エンジンによるインラインペイロード分析に送ります。これらの分析エンジンは、シグニチャ、シグニチャレス、機械学習などの検知テクニックを使用して、既知の脅威および未知のゼロデイ脅威を特定し、ブロックします。検知手法がいくつかあるため、コンテンツのタイプに応じて最適なエンジン（または複数のエンジン）にペイロードを転送できます。これにより、最適な検知率が確保され、誤検知率が減ります。

重要なのは、この方法はセキュア・ウェブ・ゲートウェイ（SWG）のような従来型のセキュリティ機器によるアプローチとはまったく異なる点です。SWG はすべてのインターネットトラフィックをプロキシし、良いものも悪いものも検査するため、複雑なウェブページや重たい HTTPS コンテンツの場合は特に悪影響をもたらす可能性があります。このような従来型のアプローチでは、パフォーマンスが低下し、レイテンシーが生じるほか、すべてのトラフィックをプロキシ転送する結果として Web サイトやアプリケーションの不具合の数が増大します。SWG 方式では、セキュリティインシデントや誤検知が増えることで、ヘルプデスクへのリクエストが増大し、IT リソースが占有されるケースも少なくありません。

セキュア・インターネット・ゲートウェイのアーキテクチャ



1. **DNS ルックアップ**
2. **安全、悪意がある、疑わしいにドメインを分類**
3. **疑わしいドメインをクラウドプロキシにリダイレクト**
4. **URL 脅威インテリジェンスとペイロード分析**

スマート・セレクティブ・プロキシなら、インターネットへの入り口とセキュリティの最初のレイヤーの両方に DNS を活用できます。安全なトラフィックはインターネットに直接送り、悪意のあるトラフィックはブロックし、リスクの高いトラフィックのみをプロキシできるようにすることで、次のようなメリットが実現されます。

- **セキュリティのシンプル化**
- **レイテンシーの削減、パフォーマンスの向上**
- **ウェブページやアプリケーションの破損の削減**

低リスクのネットワーク変革：SD-WAN 環境にゼロトラストを実装

インターネットベースのアーキテクチャへの移行を進めている組織の多くは、SD-WAN が実現の鍵だと考えています。SD-WAN は高度なリンク制御が可能なうえ、MPLS の所有による経済的な負担が軽減される可能性があるからです。ブロードバンドまたはワイヤレスのネットワークを使用して MPLS 接続を強化または補完し、ハイブリッド WAN を構築することもできますが、すでに DIA がある場合は、同じアプローチのセキュリティモデルを採用するほうが理にかなっています。

SD-WAN を採用する企業は、境界ベースのフレームワークからエッジでのゼロトラストベースのフレームワークへ、セキュリティを進化させる必要があります。今、私たちは進化のどの地点にいるのでしょうか。そして次に訪れるものは何でしょうか。

SD-WAN に関連したネットワーク状況は、エンタープライズ組織の方針や長期戦略に応じて、通常、次の 3 つのいずれかに該当します。

1. **ブレイクアウトを集中管理する従来型のプライベート WAN：つまり SD-WAN は検討中で未実装**
2. **ハイブリッド実装：既存サイトは従来型プライベート WAN 、新しいブランチは SD-WAN**
3. **主として SD-WAN**

ゼロトラストのセキュリティアプローチはこれらのすべての状況に適応できます。ただし、SD-WAN の実装を検討している、または実装を進めているエンタープライズは、実際のビジネス・ネットワーク・ツールとしてすでにインターネットを利用している可能性があり、その場合は自社ネットワーク環境にゼロトラスト・セキュリティ戦略を採用する準備ができていると考えられます。

どのようにゼロトラストを実装すれば目標とする将来の状態を実現できるのかを明らかにするために、現在のアーキテクチャについて調べてみましょう。

ブレイクアウトを集中管理する従来型のプライベート WAN

SD-WAN への移行の目的が、コスト、俊敏性、柔軟性など、インターネットベースのネットワークアーキテクチャがもたらすメリットであるなら、SD-WAN を完全に省いて、直接ゼロトラストのフレームワークに移行する方法も一考の余地があります。IAP を使用すれば、所在地に関係なく、ゼロトラストベースのアプリケーションアクセスが可能になります。また、SIG はユーザーに安全なインターネットアクセスを提供します。いずれも組織が各インターネットブレイクアウトにセキュリティスタックを構築する必要はありません。

ただし、留意すべき点が 1 つあります。すでに VoIP やビデオ会議など、インターネット・クラウド・サービス・プロバイダーを介したリアルタイムサービスに対応している企業は、インターネットベースのネットワークおよびアクセスアーキテクチャを完全に採用することが理想的と考えられます。このようなサービスがまだ主としてオンプレミスにある場合は、ロケーション間にある程度の「プライベート」ネットワーキングを維持するケースもあり得ます。これはプライベート（MPLS ベース）のこともあれば、SD-WAN ベースの場合もあります。

従来型 WAN と SD-WAN のハイブリッド

この場合、組織はすでに、より効率的なインターネットベースのアーキテクチャへの第 1 歩を踏み出しているといえます。

このような環境では、ユーザートラフィックがどのように処理されているかを理解することが重要です。

- **ユーザーはリモートオフィスから直接インターネットにアクセスしていますか？それともインターネットリンクが使用されるのはコアサイトへ戻るネットワーキングのみですか？**
- **主なユーザーアプリケーションはどこにありますか？オンプレミス、データセンター、クラウドのどれですか？**
- **クラウドを使用している場合、ユーザーはどのような方法でこれらのアプリケーションに接続していますか?ブランチから DIA を経由していますか?あるいは直接接続リンクにバックホールしていますか?**
- **SaaS アプリケーションの利用はどの程度の範囲に広がっていますか？**
- **ブランチレベルの DIA の場合、各ロケーションのセキュリティスタックはどの程度包括的ですか？**

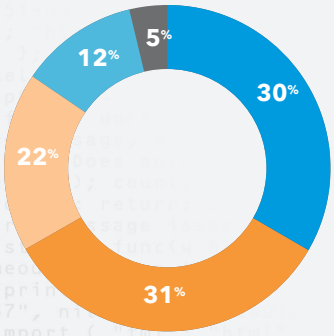
答えはもちろん、ユーザートラフィックの処理に応じて異なります。このように、ネットワーク移行の複雑さの程度はさまざまなのです。しかし、どのような状況でも変わらないことが 2 つあります。インターネットの利用は増加していくということと、境界ベースのセキュリティからゼロトラスト・モデルへの移行が必要であるということです。

たとえば、リモートオフィスから何らかの DIA 接続がある場合、SIG は、集中管理型のセキュリティスタックに保護を追加するとともに、スタックの一部に置き換わることで、複雑さとコストを軽減できます。

ユーザーがクラウドベースのアプリケーションにアクセスする場合は、IAP ベースのアプローチをとれば、組織のセキュリティ対策を強化しつつ、ユーザー体験を向上させることができます。また、CDN を使用してインターネットを介したアプリケーションへの直接アクセスを可能にすることにより、アプリケーションのパフォーマンスが向上する可能性もあります。

リモートオフィスの DIA を可能にして、ゼロトラスト・セキュリティの原理を採り入れることにより、引き続き従来型 WAN から SD-WAN への移行を進めることができます。

ソフトウェア定義（SD-WAN）ネットワークテクノロジーの利用に関する現在の事業計画は？



- 現在使用している
- 来年中にテストする
- 今後 2 年間での採用を計画中
- 利用を検討しているが、まだ計画はしていない
- 検討も計画もしていない

Forrester Research、 『Digital Transformation Drives Distributed Store Networks to the Breaking Point （デジタル変革によって分散店舗ネットワークは限界点へ）』、 2018 年 4 月

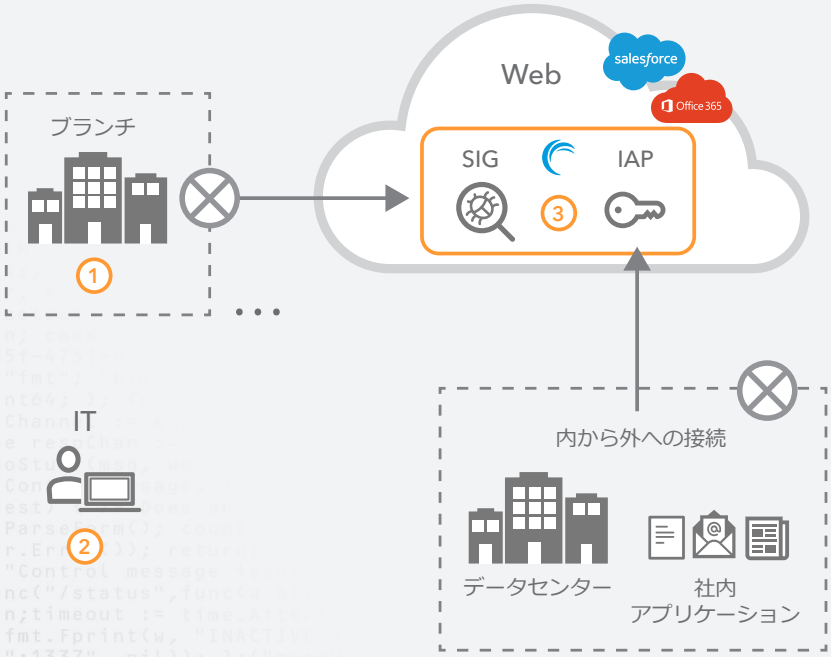
主として SD-WAN

この状態の組織は、従来のプライベート WAN ネットワークから脱却しており、オフィス内の通信にサイト間のインターネットリンク全体のインテリジェントルーティングを使用し、DIA のメリットを完全に活用していると考えられます。このような企業ではすでに、ほとんどのサイトがインターネットアクセスに依存しているため、SD-WAN を越えてネットワークを進化させることが今後の論理的な方向性といえます。

それでは次のステップは何でしょうか。まず、アプリケーションをインターネットに移行することにより、MPLS への依存を軽減し、俊敏性とコスト効率を高めます。DIA 環境であっても、社内アプリケーションには IAP を通じてアクセスできます。アプリケーションがすでにクラウド環境にある場合、これらのアプリケーションにアクセスするために、データセンターにトラフィックをバックホールしてからセントラルロケーションでブレイクアウトする（直接接続タイプのトポロジーの利用など）ことは意味がありません。

最後に、この環境は純粋なインターネットベースの接続とアクセス、つまり、「オンプレミスでもクラウドベースでも、すべての社内アプリケーションに IAP 経由でアクセスできる」という将来の方向性によく適しています。SIG を使えば、すべてのユーザートラフィックのセキュリティを確保できます。さらに、インターネットベースのプロバイダーが音声や動画などのリアルタイム通信を提供する場合、最終的には SD-WAN や企業 WAN でさえも完全に排除できる可能性もあります。これにより、コストと複雑さが軽減するとともに、ゼロトラストのアーキテクチャモデルを利用することでセキュリティも強化できます。

ゼロトラスト・セキュリティ・モデルを使用したインターネットベースのアーキテクチャの価値



1. **最もシンプルなネットワークアクセス**
   - インターネットアクセスのみ
   - 外から内へのアクセスはない
2. **管理機能**
   - 一元的な管理
   - デバイスの監視
   - ユーザーの監視
3. **セキュリティ制御の強化**
   - ゼロデイ攻撃の防御
   - 集中管理型の AAA（認証、許可、アカウンティング）
   - クライアントの状態のチェック
   - フィッシング、マルウェア、CnC の防御

ビジネスを変革する

すでにリスクと複雑さが蔓延している環境への露出が拡大しているというのが、今のビジネスの現実です。プライベート WAN 上のハブアンドスポーク方式のトランザクションで管理するネットワークモデルは、境界ベースのエンタープライズ防御と同様に時代遅れです。ネットワークとセキュリティの両方のアーキテクチャを進化させる必要があります。現在は SD-WAN を使用することで、企業ネットワークのトラフィックの処理を効率化し、ワークロードをクラウドに移行できますが、これが最終的なネットワークモデルというわけではありません。近い将来には、インターネットが企業 WAN になります。

SD-WAN と、適切なゼロトラスト対応セキュリティおよびアクセスサービスを使用することが、企業ネットワークとしてのインターネットに移行していくための最初の一歩だと Akamai は考えています。SD-WAN を Akamai Intelligent Edge Platform と組み合わせることで、アクセスポリシーやセキュリティポリシーを広く適用し、インターネット経由で高速かつ信頼性の高いエンドユーザーアプリケーション体験を実現できます。

Akamai はお客様のネットワークとセキュリティの進化を後押しできます。Akamai のゼロトラスト・アセスメントについての詳細は、担当のアカウントチームにお問い合わせください。ゼロトラスト変革にどこから着手し、どのように進めればよいか、Akamai のセキュリティエキスパートが具体的な推奨情報をご提案します。また、移行を推進するリソースについては、**ゼロトラストをすぐに実装するためのシンプルな 3 つの方法**をご覧ください。

Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、ウェブ／モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 /24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com/jp/ja/、blogs.akamai.com/jp/ および Twitter の @Akamai_jp でご紹介しています。全事業所の連絡先情報は、www.akamai.com/jp/ja/locations.jsp をご覧ください。公開日：2019 年 6 月。