ユースケース

支社のダイレクト・インターネット・アクセス（DIA）接続でのセキュリティの確保

エグゼクティブサマリー

現在の常時オンラインのデジタルな世界では、多数の企業の支社やサテライトオフィスが、世界中に物理的に分散しています。

つまり、こうしたエンタープライズユーザーは、企業ネットワークに単独で接続されているわけではないのです。エンタープライズのトラフィックは、トラフィックの宛先やユーザータイプ、デバイスに関係なく、しばしば、コストの高い WAN サービスを経由して中央の 1 か所に送信されています。また、アクセスされるエンタープライズアプリケーションは、データセンターからハイブリッドクラウド環境へと移行しているため、トラフィックが中央の 1 か所から折り返すことで、さらに非効率になります。

ほぼ

80%

支社からネットワークにアクセスする、エンタープライズ組織の分散された従業員の割合 [1]

そのため、支社を擁するエンタープライズ組織はますますダイレクト・インターネット・アクセス（DIA）を使用して、日常業務やビジネスクリティカルな業務でパブリックインターネットに接続する依存度が高くなっています。レガシーな WAN リンクや MPLS に代わるものとして、DIA はクラウドファーストや SaaS 重視の環境でエスカレートする帯域幅要件に対応しながら、複雑さを軽減し、同時にコストも抑止できます。

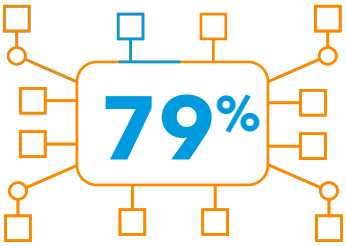
緊急性

DIA 接続の保護

DIA 接続は高いインターネットパフォーマンスを促進し、ユーザー体験を向上させますが、ウェブトラフィックを保護する新たなアプローチを必要とします。企業の支社向けのウェブトラフィックのセキュリティ確保は、これまでは、エンタープライズファイアウォールやセキュア・ウェブ・ゲートウェイ（SWG）などのオンプレミスのハードウェア機器を使用して、検査や制御用にトラフィックを中央の 1 か所にバックホールすることで、実現されてきました。しかし、DIA の使用により、そうした集中管理や検査手法に依存していた従来のセキュリティソリューションは、時代遅れになっています。代わりに、各支社のファイアウォール、エンドポイントのウイルス対策ソリューション、複製のハードウェアと機器スタックを地域全体で組み合わせることが、頻繁に行われています。しかしこうした方法では、IT 部門による管理がすぐに困難になります。さらに、一貫したパフォーマンスを維持できないことが多く、保守コストも高くなります。結局のところ、こうした継ぎはぎの防御では、支社とユーザーを高いリスクに晒すことになる可能性があります。

そして当然のことながら、背後に常に存在しているのは、危険度の増した、セキュリティ侵害を受けるリスクが日々高くなっているサイバー脅威環境です。

それでは、支社の DIA 接続のセキュリティを簡単に確保し、悪化するセキュリティ侵害から防御するにはどうすればよいのでしょうか。



自組織が、関連するセキュリティ問題を解決するよりも速い速度で、新たなテクノロジーを導入していると報告している、ビジネスリーダーの割合 [2]

70%

重大インシデントを経験した企業が、3 年以内に再建できないか、倒産に追い込まれる割合 [3]

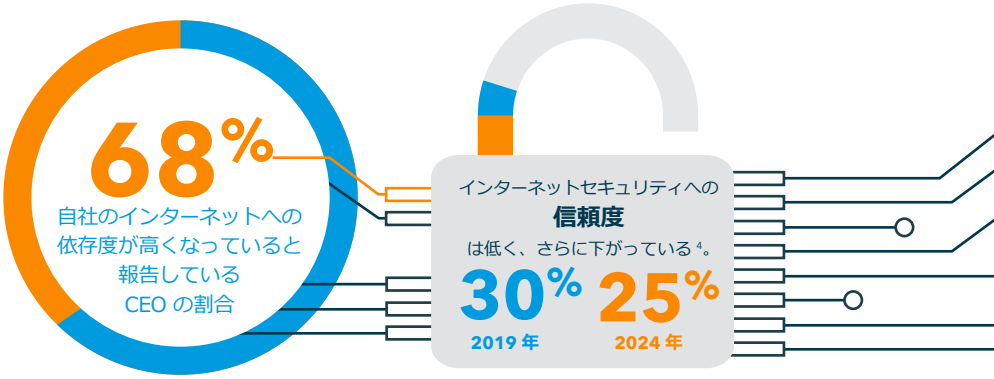
ソリューション

安全な DIA 接続を確立するためのクラウドの使用

このニーズに応えるのが、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）です。このソリューションを導入すれば、すべてのユーザーとデバイスが、所属、タイプ、場所に関係なくインターネットに安全に接続されているとともに、マルウェア、ランサムウェア、フィッシング、DNS データ窃盗、高度なゼロデイ攻撃から防御されていることを、セキュリティチームが確認できます。この SIG プラットフォームは、ライブの脅威インテリジェンスとドメイン・ネーム・システム（DNS）を活用して、インターネットアクティビティを完全可視化し、ユーザーが企業ネットワークの内外のいずれにいるかに関係なく、すべてのポートとプロトコルの脅威を阻止します。

さらに、クラウド配信のソリューションである SIG は、簡単かつ迅速な展開、設定、拡張を通じて、支社のセキュリティを強化します。グローバルなエンタープライズ全体のアップデートとポリシーの変更が、統合された管理ポータルからわずか数分で実施でき、100% のコンプライアンスを確立できます。また、導入が必要なハードウェアやソフトウェアがないため、継続的な管理をごく短時間で行えます。

さらに、プロキシ経由で良性と悪性のトラフィックの両方を検査する SWG とは異なり、SIG は DNS を初期セキュリティ・コントロール・ポイントとして使用して、リスクの高いトラフィックのみをプロキシに送信して検査します。安全なトラフィックは、インターネットに直接送信されます。この方法により、パフォーマンスが向上し、レイテンシーが発生しなくなるとともに、すべてのトラフィックをプロキシ転送する結果として生じるウェブサイトやアプリケーションの不具合の数を減らすことができます。その結果、クラウドベースの SIG は、セキュリティインシデントや誤検知の数も少なくなり、ヘルプデスクへのリクエストを最小限に抑えることができるため、その分の IT リソースを解放して他のより戦略的なビジネス要件に割り当てることができます。



Akamai が提供する、支社の DIA 接続を保護するためのクラウドベースで簡単に管理できるソリューションの詳細については、**akamai.com/etp** をご覧ください。

出典

1) https://www.riverbed.com/document/fpo/Key-Requirements-for-SD-WAN-RVBD-WP.Final.pdf
2)「Accenture Strategy 2019 Report: Securing the Digital Economy, Reinventing the Internet for Trust（デジタル経済のセキュリティの確保、信頼に向けたインターネットの改革）」
3) https://dataconomy.com/2018/03/12-scenarios-of-data-breaches/
4)「Accenture Strategy 2019 Report: Securing the Digital Economy, Reinventing the Internet for Trust（デジタル経済のセキュリティの確保、信頼に向けたインターネットの改革）」