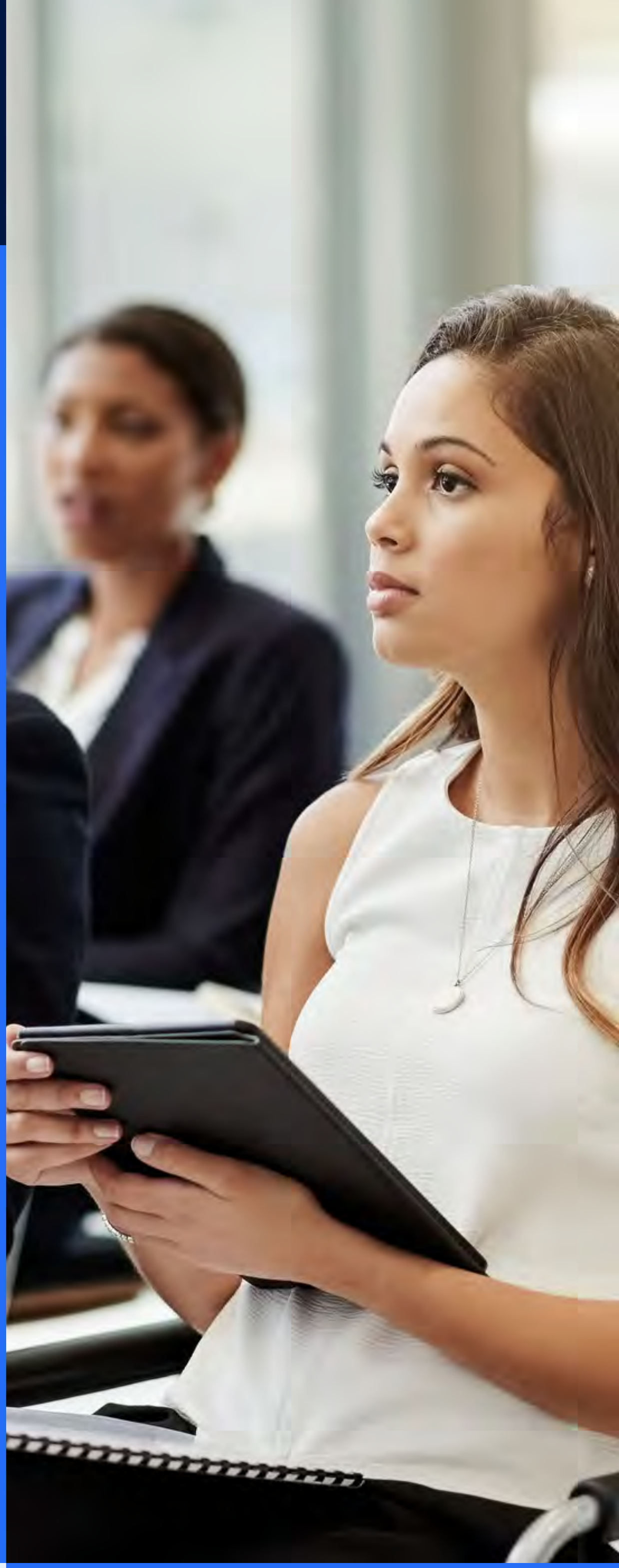
Zscaler Workload Communicationsのビジネス価値

クラウド ファイアウォールおよび仮想ファイアウォールとの比較



ホワイトペーパー

本書の要旨

現代のデジタル ビジネスは無数のワークロードに支えられています。ワークロードは、オンプレミス データ センター、パブリック クラウド インフラ、プライベート クラウド インフラまで、さまざまな環境で実行され、拡大し続けています。ビジネスの収益性、事業継続性、高品質のカスタマー エクスペリエンスを提供する能力はすべて、こうしたミッションクリティカルなワークロードの可用性とセキュリティにかかっており、サイバー攻撃(ランサムウェアなど)や脅威のラテラル ムーブメント、データ漏洩からこれを保護することは極めて重要です。

しかし、多くの組織は現在も業務に不可欠なワークロードを保護するために従来のソリューション アーキテクチャーを採用しています。一般に、このような場合は、ファイアウォール、SSL/TLSインスペクション エンジン、情報漏洩防止(DLP)ツールなど、複数の層を保護するための複数のサードパーティー ソリューションの実装が必要になります。そして、すべての送信トラフィックに対して一貫した検査とポリシーを施行するために、多くの組織は依然としてパブリック クラウドのワークロード トラフィックをオンプレミスのデータ センターにバックホールしています。この方法は、アーキテクチャーの複雑化、コストの増加、パフォーマンスの低下を招きます。もちろん、パフォーマンスが低下すれば、エンド ユーザーや顧客のエクスペリエンスも理想的な水準を下回ることになります。

現在では、パブリック クラウド ベンダーが提供するネイティブ セキュリティ機能を採用している組織も存在しますが、このアプローチは通常、人員配置の負担を増加させます。さらに、クラウド サービス プロバイダー(CSP)ごとに専用のセキュリティ インフラを実装するには、莫大なコストがかかります。

クラウドネイティブ、レガシーベース、マルチベンダーのいずれの戦略も厳しい限界を抱えており、脅威対策やデータ保護の一貫性に欠け、大きな複雑性と高い運用コストを伴います。これらのアプローチでラテラル ムーブメントを防ぐことはほぼ不可能であり、まして攻撃ライフサイクルの初期段階で阻止することなど、とても望めません。

しかし、これらに代わる優れたアプローチも存在します。最新のゼロトラスト アーキテクチャーを実装することで、ハイブリッド ワークロードのセキュリティを根本的に簡素化し、一貫した包括的な脅威対策とデータ保護を実現することが可能です。世界最大のインライン クラウド セキュリティ プラットフォームであるZscaler Zero Trust Exchangeは、ワークロード間およびワークロードとインターネット間のすべての通信に対して包括的なゼロトラスト保護を提供します。

Zscalerプラットフォームは、すべてのトラフィックをインラインで検査し、サイバー脅威とデータ漏洩を阻止します。アクセスを許可する前にすべてのアクセス要求のアイデンティティーとコンテキストを検証し、適切なポリシーをすべて適用したうえで、インターネット、SaaSアプリ、パブリック クラウド、プライベート クラウド内のワークロードへの接続を許可します。また、クラウド規模のTLSインスペクションによってゼロデイ攻撃を防止し、インライン データ保護とDNSインスペクションによってデータ漏洩を阻止します。厳格な制御により、ワークロードやサーバーが既知の危険な宛先や未知の宛先と通信することも防ぎます。Zscalerのアプローチは、組織のリソースを攻撃者から発見できないようにするとともに、攻撃対象領域を排除し、ラテラル ムーブメントを効果的に防止します。同時に、ワークロードをIP、ドメイン名、仮想プライベート クラウド(VPC)、VNet、またはユーザー定義タグで簡単にセグメント化できるようにし、最小特権アクセスの適用を簡素化します。

Zscaler Zero Trust Exchangeを利用することで、高コストのポイント製品の組み合わせを単一の包括的なクラウドプラットフォームに置き換え、オールインワンのアプローチを採用することが可能です。これにより、運用負荷を削減するだけでなく、ランサムウェアやデータ侵害のリスクも低減できます。結果として、IT部門やセキュリティ部門の生産性を向上させ、現在最も一般的な脅威による広範な損害からビジネスを保護することにつながります。

このホワイト ペーパーでは、Zscaler Workload Communicationsの展開に関連するコストとメリットについて見ていきます。特に以下の点に注目していきます。

- **ランサムウェアのリスク。**全世界の身代金支払い額は過去1年間で平均500%増加しており、この重大なリスクに対する備えが求められています。[1]潜在的な損失を軽減するための対策を取り、環境内でのラテラル ムーブメントを通じた有害なマルウェアの拡散を効果的に防ぐことが重要です。

- **データ侵害のリスク。**価値の高い知的財産、顧客情報、財務データの窃取を未然に防ぐことが求められます。有効なソリューションに投資することで、サイバー リスクを軽減することが可能です。

- **ツールと実装コスト。** 最もコストの高いソリューション、最も費用対効果の高いソリューションを確認します。

- **運用コスト。**複雑で扱いにくいツールの管理、ファイアウォール ルールの設定と更新、仮想プライベート ネットワーク(VPN)のトラブルシューティングに、IT部門やセキュリティ部門が年間でどの程度の時間を費やしているかが焦点となります。

[1] 出典：Sophos State of Ransomware 2024 Report、2024年4月

Zscaler Workload Communicationsのメリットの概要[2]

削減できるコストの総額

230万ドル
年間の削減額

30%
コスト削減率

サイバー リスクの軽減

50%
ランサムウェアによるリスクの低減率

40%
データ侵害リスクの低減率

運用の効率化

160万ドル
年間の人件費の削減額

65%
運用コストの削減率

サイバー リスクがビジネスに与える影響と潜在的な損失

サイバー犯罪は違法行為ではあるものの、最も収益性の高い活動の一つです。米国国立標準技術研究所(NIST)は、米国企業がサイバー攻撃によって被る年間の損失額は、最大で同国GDPの4%に上ると推定しています。[3]

サイバー犯罪による損失は、「史上最大の経済的富の移転」とも呼ばれており、2023年には全世界で総額8.15兆ドルに達したと推定されています。また、2028年までに年間13兆ドルを超えるとも予測されています。[4]サイバー犯罪を国に例えると、その経済規模は(米国と中国に次ぐ)世界第3位となります。[5]

この途方もない数字を踏まえれば、個々の被害組織における直接的な損害も莫大な額に上ることは想像に難くないでしょう。IBM Securityによると、米国のデータ侵害による平均損失額は2023年に過去最高の445万ドルに達しています。前年比で2.3%増加し、2020年以降では15.3%増加しています。ランサムウェア攻撃はこれらの侵害の約4分の1 (24%)を占め、被害1件あたりの損失は平均513万ドルでした。[6]

しかし、こうした膨大な数字も、サイバー犯罪がもたらす被害の全容を表すには十分ではありません。サイバー犯罪の被害には、ブランド イメージの低下や従業員の信頼失墜といった間接的な損失、そしてビジネス戦略の変更や組織の運用モデルの調整を迫られるなどといった波及的な影響など、定量化しにくいものも含まれます。すべてのビジネス リスクと同様、サイバー犯罪に関連するリスクを完全に回避することは不可能ですが、効果的に軽減することは可能です。

[2] 約10,000のクラウド ワークロードを実行している組織において、Palo Alto Networksの仮想ファイアウォールと同等のサードパーティーのファイアウォールを運用している場合との比較
[3] 出典：NIST、Evidence suggests that the U.S. loses hundreds of billions to cybercrime, possibly as much as 1% to 4% of GDP annually、2020年5月
[4] 出典：Statista、Estimated Cost of Cybercrime Worldwide 2018–2029、2024年6月
[5] 出典：International Monetary Fund、World Economic Outlook、2024年4月
[6] 出典：IBM Security、Cost of a Data Breach Report 2023

各関係者は、他の領域におけるリスク管理と同じように、攻撃の成功率を実証可能な形で低減する対策を導入することで、サイバーセキュリティ リスクを軽減できます。

サイバー リスクを軽減することで得られる価値を試算するには、サイバー攻撃が成功した場合に発生する経済的損失とその発生確率をモデル化する必要があります。そのうえで、それらのリスクを軽減するために必要な支出とのバランスを判断します。

その試算について詳しく見ていきましょう。

ランサムウェアのリスク

ランサムウェアのリスクは業界や地域によって異なり、製造、医療、小売/eコマースなど一部の業界では、発生率や侵害率が平均よりも著しく高くなっています。[7]ただし、いくつかのリスク要因は互いに相殺されます。非常に成熟したサイバーセキュリティ プログラムを導入している組織では、保護対策がそれほど充実していない組織よりもランサムウェア攻撃の成功率が低くなる一方、誰もが知るブランドを抱える大企業は、はるかに頻繁に攻撃対象となります。

多くのランサムウェア攻撃は、仮想プライベート ネットワーク(VPN)などのインフラの脆弱性を狙い、ラテラル ムーブメントを通じて重要な資産を探し出すことで成果を上げます。最近の脅威調査によると、過去1年間で56%もの組織がVPNの脆弱性を悪用したサイバー攻撃の標的となっています。[8]

ファイアウォールの脆弱性が生み出す重大なリスク

広く使用されているファイアウォールのベンダーから最近公表された共通脆弱性識別子(CVE)の例を以下に紹介します。

- **Palo Alto Networks (CVE-2023-6790):** Palo Alto Networksのオペレーティング システム(PAN-OS)におけるクロスサイト スクリプティング(XSS)の脆弱性です。これを悪用することで、リモートの攻撃者は管理者権限でブラウザーにログインしているかのようにJavaScriptペイロードを実行できます。

- **Palo Alto Networks (CVE-2024-3400):**同じくPAN-OSの脆弱性であり、この脆弱性を悪用することで、未認証ユーザーが同ソリューションの保護対象のネットワークに侵入できます。脅威の研究者はこの脆弱性を狙った攻撃を多数確認しており、[9]脆弱性スコアはCVEの最高値である10となっています。

- **Ivanti (CVE-2023-46805とCVE-2024-21887):**この脆弱性を悪用することで、リモートの攻撃者は認証の回避やリモート コマンド インジェクション攻撃を実行できるようになります。これらの脆弱性の重大性から、米国サイバーセキュリティ インフラストラクチャー セキュリティ庁(CISA)は、影響を受けたVPNを介して接続されているデバイスとの接続を直ちに切断しました。

[7] 出典：Verizon、2024 Verizon Data Breach Investigations Report
[8] 出典：Zscaler、2024年版 VPNリスク レポート
[9] 出典：Palo Alto Networks、More on the PAN-OS CVE-2024-3400、2024年4月

- **Fortinet (CVE-2024-2172とCVE-2024-23323):** Fortinetのすべてのファイアウォールで稼働しているオペレーティング システム「FortiOS」に存在する重大な脆弱性です。これらを悪用することで、影響を受けるシステム上でのリモート コード実行が可能になります。Fortinetはこれらの脆弱性に対応するセキュリティ アップデートのリリースに伴い、脆弱性は実際に悪用されている可能性が高いと報告しています。[10]

- **Check Point (CVE-2024-24919):** Check Point Security Gatewayソフトウェアの脆弱性です。これを悪用することで、リモート アクセスVPNやモバイル アクセス ソフトウェアが有効になっている場合、Check Point Security Gatewayを通過する情報にアクセスすることが可能になります。

IBMの最新レポート『Cost of a Data Breach Report』のデータによると、ハイブリッド環境やマルチクラウド環境における平均的なランサムウェア攻撃による損失は511万ドルになると想定されています。[11]ただし、この数字は全業界の平均であり、実行されるクラウドワークロードが少ない小規模な組織における想定損失額はこれよりも少ないものになります。

この想定に基づくと、ランサムウェア被害に遭う確率が年間15%の組織では、平均で年間1,022,000ドル相当のランサムウェア関連の損失が発生することになります(実際には、このような損失が毎年発生するわけではありませんが、大規模な攻撃が成功した場合、平均して5年ごとにまとめて511万ドルもの損失が発生することになります)。

同じ論理で、ランサムウェア攻撃の被害に遭う確率が20%の組織では、ランサムウェア関連の損失が平均して年間2,555,000ドル発生することになります。一方、被害に遭う確率が年間25%の組織の損失は、平均5,110,000ドルとなります。

脅威の研究者の見解によると、大規模な組織はランサムウェア攻撃に遭うリスクが高いだけでなく、インシデントに大規模なコンピューティング インフラが関係するため、損失はより大きなものになると考えられます。[12]

大手セキュリティティ ベンダーのファイアウォール ソリューション、サービスとして提供されるファイアウォール機能、またはパブリック クラウド ベンダーのネイティブ ファイアウォールは、いずれも脅威のラテラル ムーブメントを100%阻止することはできず、これらを運用している組織ではランサムウェア攻撃の一部が最終的に成功することが予想されます。

対照的に、アーキテクチャー設計にゼロトラスト アプローチを採用している組織は、このアプローチの性質上、すべての脅威のラテラル ムーブメントを阻止できます。

実際、Zscaler Zero Trust Exchangeを実装してワークロード通信を保護しているお客様は、組織全体のランサムウェアのリスクを平均40%削減しています。なお、より複雑なIT環境を持つ大規模な組織では、ランサムウェアのリスクをさらに大幅に削減できます。

[10] 出典：CISA、サイバーセキュリティ アドバイザリー、Fortinet Releases Security Advisories for FortiOS、2024年2月
[11] 出典：IBM Security、Cost of a Data Breach Report 2023
[12] 出典：Zscaler、2024年版 VPNリスク レポート

これらの試算から、ランサムウェア被害に遭う確率が年間15%、20%、25%の組織(それぞれ小規模、中規模、大規模)で想定される年間の損失額をを表にまとめると以下のようになります。[13]従来型のセキュリティ ソリューションはいずれもすべてのラテラル ムーブメントを阻止することはできないため、想定損失額はどのソリューションを前提とした場合でも変わりません。

セキュリティ態勢 – ランサムウェア			
	小規模	**中規模**	**大規模**
VPN関連のランサムウェア攻撃を受けるリスク(1年あたり)	15%	20%	25%
ランサムウェア攻撃による平均損失額	1,022,000ドル	2,555,000ドル	5,110,000ドル
Zscalerによるランサムウェアのリスク低減率	40%	50%	60%
Zscalerによって削減されるランサムウェアによる潜在的な損失(1年あたり)	**61,320ドル**	**255,500ドル**	**766,500ドル**

データ侵害のリスク

Cyentia Instituteが収集したデータによると、全業界の平均的な組織がデータ侵害に遭う確率は毎年14%です。[14]データ侵害に関連する損失には、調査や事業中断に伴う費用が含まれます。より具体的には、収益と顧客の喪失のほか、ネットワークの修復と復旧、フォレンジック、通知、規制上の罰金と罰則に関連するコストが発生します。

どのファイアウォールやクラウド ベンダーのネイティブなデータ保護ソリューションも、完璧ではありません。この1年の間にも、数々のCVEが複数の主要サイバーセキュリティ ベンダーのファイアウォール ソリューションに影響を与えています。そのなかには、前述のCVE-2024-3400も含まれます。この脆弱性は、脅威の研究者によって記録された複数のゼロデイ攻撃で悪用されています。[15]

Ciscoも最近、同社のファイアウォール ソリューションに影響を与える重大な脆弱性を公表しました。これにはCVE2024-20553とCVE-2024-20358(Cisco Adaptive Security Appliance (ASA)とCisco Firepower Threat Defense (FTD)ソフトウェアに影響)などが含まれます。[16]

2022年には、攻撃者がFortinetのFortiOSソフトウェアに含まれる重大な脆弱性を悪用して認証メカニズムを回避し、同社のファイアウォールで保護されているはずのネットワークが不正アクセスを受けました。[17]

サードパーティーのファイアウォール ソリューション、as a Service型のソリューション、クラウド ベンダーのネイティブ機能を運用している小規模な組織では、データ侵害による年間の損失額はそれぞれ798,000ドル、950,000ドル、914,000ドルになることが想定されます。損失額に差があるのは、一般的に、各タイプのファイアウォールが、異なる環境に展開されるためです。たとえば、オンプレミスのファイアウォールを使用している場合、大量のデータがオンプレミスに保存されていることを示唆します。一方、パブリック クラウド ベンダーのネイティブ ソリューションを使用している場合、ほとんどのデータがパブリック クラウドに保存されていることを示唆し、侵害による平均損失額は大きくなります。[18]

[13] 今回の分析では、クラウド環境の規模や成熟度に応じて組織を3つのカテゴリーに分類しています。「小規模」グループの組織は、クラウドで実行するワークロードが約1,000、データの保管量が月間5 TB、運用するリージョン数が5とします。「中規模」グループの組織は、クラウドで実行するワークロードが10,000、データの保管量が月間30 TB、運用するリージョン数が25とします。「大規模」グループの組織は、実行するワークロードが20,000、データの保管量が月間100 TB、運用するリージョン数が50とします。

[14] 出典:Cyentia Institute、Information Risk Insights Study、2022年

[15] 出典:Cybersecurity Dive、Palo Alto Networks fixes maximum security, exploited CVE in firewalls、2024年4月

[16] 出典:英国国家サイバーセキュリティ センター、Exploitation of vulnerabilities affecting Cisco firewall platforms、2024年4月

[17] 出典:Avertium、Flash Notice: Critical Fortinet Zero-Day Vulnerability Exploited in the Wild、2022年12月

[18] 出典:IBM Security、Cost of a Data Breach Report 2023

Zscaler Zero Trust Exchangeのようなゼロトラストベースのアプローチを採用している組織では、これらのリスクが平均で40%削減されます。

セキュリティ態勢 – データ侵害			
	小規模	中規模	大規模
データ侵害の発生リスク(12か月)	14%	14%	14%
データ侵害による平均損失額:サードパーティーのファイアウォールの場合	798,000ドル	1,995,000ドル	3,990,000ドル
データ侵害による平均損失額: サードパーティーのクラウド ファイアウォールの場合	950,000ドル	2,375,000ドル	4,750,000ドル
データ侵害による平均損失額: パブリック クラウドのネイティブ ファイアウォールの場合	914,000ドル	2,285,000ドル	4,570,000ドル
Zscalerによるデータ侵害のリスク低減率	40%	40%	40%
データ侵害による潜在的な損失の削減額(1年あたり): Zscalerとサードパーティーのファイアウォールの比較	**44,688ドル**	**111,720ドル**	**223,440ドル**
データ侵害による潜在的な損失の削減額(1年あたり): Zscalerとas a Service型ソリューションの比較	**53,200ドル**	**133,000ドル**	**266,000ドル**
データ侵害による潜在的な損失の削減額(1年あたり): Zscalerとクラウドネイティブ ファイアウォールの比較	**51,184ドル**	**127,960ドル**	**255,920ドル**

展開と運用のコスト

Zscaler Workload Communicationsは、Zscaler Zero Trust Exchangeを基盤とし、ハイブリッド ワークロードのセキュリティを根本的に簡素化します。よりシンプルなアプローチを通じ、実装と管理に伴う負荷とコストを低減します。

このソリューションは、パブリック クラウドおよびオンプレミス データ センターのワークロードにおける対インターネットおよびワークロードの送信トラフィックを保護し、あらゆる場所で一貫した脅威対策とデータ保護を確保します。Zscaler Workload Communicationsを使用することで、ユーザーおよびアプリケーションを対象とするセキュリティ ポリシーを、さまざまなテクノロジー環境にわたって容易に標準化できます。また、Infrastructure as Code (IaC)テンプレートなどの広範な自動化を活用し、展開を簡素化します。

接続の合理化とコスト削減

Zero Trust Exchangeのようなインライン クラウド セキュリティ プラットフォームに切り替えることで、ほぼすべての組織において、さまざまなコストを大幅に削減、または完全に排除できます。これには、以下に関連するコストが含まれます。

- **クラウド/仮想ファイアウォール:**クラウド ワークロードを保護するために、多くの組織はPAN Virtual Firewall、PAN Cloud Firewall、AWS Network Firewall、Microsoft Azure Firewall、その他多数の仮想ファイアウォールを展開しており、ユーザー単位で毎年サブスクリプション費用が発生しています。このアプローチはスケーラブルであり、追加の物理アプライアンスを展開することなく、トラフィックの急増(季節的な増加を含む)をサポートします。また、ファイアウォールの集中管理ツールも不要になります。

  Zscalerのお客様は、クラウド ワークロードを保護するための専用ファイアウォールを展開する必要がなく、このコストを完全に削減できます。

- **トラフィックのバックホール：**多くの組織は現在もワークロードの送信トラフィックを検査して保護するために、パブリック クラウドから自社のデータ センターにトラフィックをバックホールしています。これを実現するには通常、AWS、Azure、GCPと組織のデータ センター間に専用のネットワークを構築する必要があります。これには、DX/ExpressRoutesの構築や、クラウドの送信トラフィックを保護するために必要なオンプレミスのハードウェアとインフラへの投資が求められます。

  Zscalerのお客様は検査のためにデータ センターにトラフィクをバックホールする必要がなくなり、関連コストは一切発生しません。

- **マルチクラウド サポート：**ほとんどの組織はAWS、Microsoft Azure、GCPなどの複数のクラウド サービス プロバイダー(CSP)を利用しています。各プロバイダーの環境は異なるため、セキュリティ部門は通常、CSPごとに別々のセキュリティ ツールの実装し、固有のスキルを習得するほか、セキュリティ ポリシー各クラウドに1つずつ複製します。また、複数のクラウド間で重複するIPアドレスを確立するには時間とリソースがかかります。

  Zscalerのお客様は単一のクラウド型セキュリティ プラットフォームを活用し、複数のクラウドで実行されているワークロードを保護できるため、CSPごとのツールやリソースは不要になります。

- **VPN接続：**VPC、リージョン、パブリック クラウドにまたがるワークロード間の安全な接続を実現するために多くの場合、VPN接続が導入されます。ZscalerはVPN接続の必要性とそれに伴うすべてのコストを排除します。

- **TLSインスペクション：**多くの組織は、SquidやBlue Coatのプロキシやクラウド ファイアウォールといった専用のインスペクション ツールを展開しています。これらのアプライアンスは高額になることがあるだけでなく、レイテンシーの増加やスループットの低下によってパフォーマンスに悪影響を与える可能性もあります。

  ZscalerにはTLSインスペクション機能が含まれているため、追加のアプライアンスやソリューションに費用をかける必要はありません。さらに重要な点として、インスペクションを有効にしてもパフォーマンスの低下を招きません。

- **データ保護：**ミッションクリティカルなアプリケーションをクラウドに移行する際に機密データを保護する一般的な戦略として、DLPツールやサービスの展開が挙げられます。

  ZscalerにはDLP機能が組み込まれており、パブリック クラウドやその他の環境のワークロードを保護できます。

ここからは、Zscalerのよりシンプルなアプローチがテクノロジーと運用コストに与える影響をさらに詳しく見ていきます。ここまでに見てきたコスト削減効果とサイバー リスクの軽減に伴う損失削減効果を合わせることで、Zscaler Workload Communicationsがもたらす総合的な経済価値を試算できます。

コストの最適化：ソフトウェアとアプライアンス

Zscaler Zero Trust Exchangeは、ワークロード セキュリティに対する最新のアプローチを通じて、攻撃対象領域を排除するとともに、インラインでの完全なコンテンツ検査およびDLPを提供し、直接接続を実現して脅威のラテラル ムーブメントが不可能な環境を実現します。これらはすべてインライン クラウド プラットフォームで実現されるため、高額なアプライアンス、ソフトウェア ライセンス、MPLS接続は必要ありません。

組織の規模によっては、年間で最大300万ドル以上を削減できます。[19]廃止できる可能性のあるツール、ソリューション、サブスクリプションの一部を以下に紹介します。

- MPLS回線(ネットワーク終端に関連するコストも削減可能)
- クラウドネイティブ ファイアウォール(AWS、Microsoft Azure、GCPなどのプロバイダーが提供するもの)
- as a Service型のファイアウォールのサブスクリプション費用(SSLインスペクションなどの機能を含む)
- 従来型ファイアウォールのコスト
- ネットワーク アドレス変換(NAT)ゲートウェイ
- データ保護/情報漏洩防止(DLP)ソリューション
- クラウドネイティブの仮想プライベート ネットワーク(VPN)ソリューション
- TLSインスペクション ソリューション

コストの最適化：運用コストと人件費

サイバーセキュリティにおけるスキル ギャップは、業界や地域を問わず依然として深刻な問題であり、全世界の情報セキュリティ関連職の空席を埋めるには400万人の人材が必要と推定されています。[20]AWS、Azure、GCP環境での実務経験を持つ実務担当者は特に不足しており、これらのプロフェッショナルの人件費は1時間あたり約200ドルに上ると試算されます。また、必要なフルタイムの人材は、小規模な組織で3人、中規模な組織で6人、大規模な組織で8人と推定されます。

Zscalerを使用すると、前述のすべてのクラウド ソフトウェア ソリューションと比較して、運用サポートに必要な労働時間を平均で60～65%削減できます。

運用サポート(人件費)

	小規模	中規模	大規模
想定人員数	3	6	8
想定時給	200ドル	200ドル	200ドル
想定年間労働時間	2,080	2,080	2,080
年間人件費	1,248,000ドル	2,496,000ドル	3,328,000ドル
Zscalerによる削減率	60%	65%	65%
Zscalerによって削減されるコスト	**61,320ドル**	**255,500ドル**	**766,500ドル**

[19] コストは次を含む複数のソースから試算されています：MPLSとインターネットの価格比較ツール(CarrierBid Communications、2024年)、AWS価格計算ツール(Amazon Web Services)、Microsoft Azure Marketplace、Cloud Next Generation Firewallの価格表(Google Cloud)、クラウドNGFW価格見積もりツール(Palo Alto Networks)。

[20] 出典：World Economic Forum、Strategic Cybersecurity Talent Framework、2024年4月

Zscaler Zero Trust Exchangeによるワークロード通信保護がもたらすビジネス価値の総合的な試算

これまでに挙げたコスト削減効果が実際のお客様の環境でどのように積み上がるかを詳しく見てみましょう。サードパーティーの仮想ファイアウォールを使用しているケースから順に、これまでの分析で検討してきた小規模、中規模、大規模の3つの組織規模におけるコスト削減効果を比較していきます。

組織規模の想定：		
	クラウド ワークロードのおよその数	展開規模
小規模	1,000	2つのCSP
中規模	10,000	3つのCSPと少数のアベイラビリティー ゾーン
大規模	20,000	3つのCSPと多数のアベイラビリティー ゾーン

サードパーティーのファイアウォール[21]			
	小規模	中規模	大規模
サードパーティーのファイアウォールのライセンスとアプライアンスの年間コスト	209,394ドル	1,046,970ドル	2,093,940ドル
運用コスト	1,248,000ドル	2,496,000ドル	3,328,000ドル
ランサムウェア攻撃による損失	1,022,000ドル	2,555,000ドル	5,110,000ドル
データ侵害による損失	798,000ドル	1,995,000ドル	3,990,000ドル
サードパーティーのファイアウォール(PANの仮想ファイアウォール)の年間総コスト	**3,277,394ドル**	**8,092,970ドル**	**14,521,940ドル**
Zscalerによって削減されるコスト	**944,202ドル**	**2,316,590ドル**	**2,847,080ドル**
削減率	**28.8%**	**28.6%**	**19.6%**

サードパーティーのAS A SERVICE型ファイアウォール[22]			
	小規模	中規模	大規模
サードパーティーのas a Service型製品の年間コスト	159,492ドル	832,464ドル	1,676,820ドル
運用コスト	0	0	0
ランサムウェア攻撃による損失	1,022,000ドル	2,555,000ドル	5,110,000ドル
データ侵害による損失	950,000ドル	2,375,000ドル	4,750,000ドル
サードパーティーのファイアウォール(PANのas a Service型ファイアウォール)の年間総コスト[23]	**2,131,492ドル**	**5,762,464ドル**	**11,536,820ドル**
Zscalerによって削減されるコスト	**154,012ドル**	**500,964ドル**	**309,320ドル**
削減率	**7.2%**	**8.7%**	**2.7%**

[21] ここでは例としてPalo Alto Networksの仮想ファイアウォールを使用しています
[22] ここでは例としてPalo Alto Networksのクラウド ファイアウォールを使用しています
[23] Palo Alto Networksのas a Service型ファイアウォール(SSLを含む)、NATゲートウェイ、クラウドネイティブVPN接続のライセンス コストが含まれます

パブリック クラウド プロバイダーのネイティブ ファイアウォール[24]			
	小規模	**中規模**	**大規模**
ネイティブ ファイアウォール(AWS)のコスト	163,434ドル	758,964ドル	1,840,080ドル
運用コスト	0	0	0
ランサムウェア攻撃による損失	1,022,000ドル	2,555,000ドル	5,110,000ドル
データ侵害による損失	914,000ドル	2,285,000ドル	4,570,000ドル
ネイティブ ファイアウォール(AWS)の年間コスト[25]	**2,099,434ドル**	**5,598,964ドル**	**11,520,080ドル**
Zscalerによって削減されるコスト	**257,434ドル**	**422,424ドル**	**462,500ドル**
削減率	**11.7%**	**7.5%**	**4.0%**

なお、サイバー攻撃による非定量的な損失については、この試算に含めることができません。また、従業員の生産性やビジネス アジリティーに関連するパフォーマンス向上の影響も測定していませんが、こうした非定量的なメリットも注目に値します。一般的に、意思決定者は、複数のポイント ソリューションをZero Trust Exchangeのような単一のプラットフォームに統合することで得られるコスト上のメリットを認識しています。しかし、ラテラル ムーブメントの排除、セキュリティ運用部門の業務の簡素化、一貫した包括的な脅威対策とデータ保護を実現するソリューションがビジネスにどのような価値をもたらすかについては、認識が不十分である可能性があります。

さまざまな理由からクラウド インフラを導入する組織が増えていますが、クラウド移行にあたっては、ワークロード保護に対して新しい考え方が求められます。最新のゼロトラスト アーキテクチャーは、現代の組織が直面する最大のリスクの一部を軽減するプロセスを根本的に簡素化しました。運用と管理の負荷を軽減しながら、クラウド ワークロード セキュリティにおける最大の課題を克服するためには、このアプローチが不可欠です。

[24] ここではAWSのファイアウォールを使用しています
[25] クラウドネイティブ ファイアウォール(AWS/Azure/GCP)とクラウドネイティブVPN接続のライセンス コストが含まれます

Zscalerについて
Zscaler (NASDAQ: ZS)は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。Zscaler Zero Trust Exchange™プラットフォームは、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界150拠点以上のデータ センターに分散されたSSEベースのZero Trust Exchange™は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp**をご覧いただくか、Twitterで**@zscaler**をフォローしてください。

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/jp**

Zero Trust Everywhere