

WHITE PAPER

ハイパースケールデータセンター セキュリティ

ハイパースケールコンピューティングを阻害する、
ネットワークとセキュリティの制約



概要

デジタルイノベーション（DI）によって処理されるデータ量が増加し、アプリケーションの消費が加速し続けています。さまざまな業界において、多様なユースケースに対応するためにハイパースケールコンピューティングが採用されています。たとえば、ゲノム研究や航空宇宙研究などの高度な研究機関では、大規模なデータセットをネットワーク経由で転送する機能が必要です。一方、e コマース企業では、ハイパースケールアーキテクチャを使用してサイバーマンデーなどの休日に急増する接続を管理しています。

ハイパースケールデータセンターにおいては、こうしたニーズを満たすネットワークインフラストラクチャが採用されていますが、ネットワークのボトルネックを引き起こすことが多いという理由でセキュリティは組み込まれていません。既存のセキュリティソリューションは、ハイパースケールデータセンターのニーズへの対応に苦戦しています。既存の次世代ファイアウォール（NGFW）がネットワークのボトルネックとなっているため、ネットワークのエンジニアリングおよび運用担当のリーダーの多くは NGFW の利用を避けています。結果として、そうした企業は攻撃にさらされ、法規制へのコンプライアンスを達成できなくなっているのです。

はじめに

DI への取り組みとビジネスニーズによって、エンタープライズデータセンターの使用方法和、達成しなければならないパフォーマンス指標は変化しました。新しいネットワーク機能に対する需要に適応することが、ハイパースケールデータセンターの進化を促進しています。

ハイパースケールデータセンターは、効率的なスケーリングが可能で増大するビジネスニーズに合わせてダイナミックに稼働するデータセンターです。ハイパースケールアーキテクチャは、膨大な処理能力と天文学的なパフォーマンスが必要とされる、これまででないビジネスニーズに対応することを前提に設計されています。ビジネスニーズは業界によって異なります。ハイパースケールアーキテクチャは、次のような分野で必要とされています。

- **医薬品、石油・ガス、航空宇宙業界における最先端の研究**：高度な研究にビッグデータや ML（機械学習）アルゴリズムを使用するには、40 Gbps と 100 Gbps の「エレファントフロー」を送信する機能が必要です¹。
- **ダイナミックな e コマースとオンラインゲーム**：ショッピングシーズン、オンラインでの確定申告、ゲームなどのイベントに伴って接続が急増すると、毎秒膨大な数のユーザー接続を処理する機能が必要です²。
- **大規模エンタープライズ**：仮想化を使用して極めてスケーラブルな仮想ネットワークを作成しようとする組織では、大規模なネットワークセグメンテーションと同時に、物理 / 仮想両方のプラットフォームでホスティングされるサービス間の通信が必要です。
- **証券取引所**：電子取引インフラストラクチャでは、できるだけ遅延を引き起こすことなく市場データを受信する必要があります³。
- **ハイパースケーラー（大規模でグローバルなテクノロジー企業）**：クラウドデータセンター間的高速なデータセンター相互接続には、データのプライバシーと機密性を実現するための高スループットの IPsec トンネル機能が必要です⁴。

多くの場合、これらの業界の企業は必要とするネットワークインフラストラクチャに投資してきました。しかし、既存の NGFW ではハイパースケールアーキテクチャの大規模な拡張性とパフォーマンスのニーズを満たせないため、前述のようなニーズに対応できるセキュリティソリューションの調達には困難です。このため、セキュリティ機能がビジネスの足手まといになること、あるいはネットワークインフラストラクチャのスループットと待ち時間を最適化できなくなることを懸念する組織は、セキュリティ機能を無効化することになります。

ハイパースケールアーキテクチャの課題

ハイパースケールデータセンターはさまざまな業界に導入されており、幅広いユースケースとビジネスニーズに対応しています。いずれの導入環境にも、ハイパースケールセキュリティの課題が存在します。

攻撃に対して脆弱な大規模ネットワークフロー

人工知能（AI）と ML アプリケーションでは、アルゴリズムのトレーニングとテストのために膨大なデータセット（多くの場合、数テラバイト⁵）が必要です。製薬、バイオテクノロジー、ゲノム、石油・ガス業界の研究機関はすべて、このような大規模なデータセットを研究で使います。これらの研究機関がデータを処理し分析するには、大規模なデータセットをネットワーク経由で効率的に送信できなければなりません。しかし、そのようなデータセットを効率的に送信するには、40 Gbps を超えるネットワーク帯域幅が必要です。

研究機関は理論上、ルーターとスイッチをベースにして構築されたハイパースケールネットワークアーキテクチャを活用することで、必要な帯域幅を提供できます。ただし、これらのデバイスはセッション状態を追跡したり、脅威を特定するためにトラフィックのインスペクションを実行したりしません。DDoS（分散型サービス拒否）攻撃が増加する中、これらのデバイスもまた攻撃に対して脆弱です。

さらに、これらの接続を介して送信されるデータは機密情報であることが多く、EUのGDPR（一般データ保護規則）やHIPAA（医療保険の携行性と責任に関する法律）などのデータ保護法の対象となっています。これらの法律はさまざまなアクセス制御を義務付けています。つまり、ファイアウォールなどのセキュリティテクノロジーを介してネットワークトラフィックをルーティングする必要があります。ただし、多くのNGFWは10 Gbpsの接続帯域幅でさえも処理できていません。結果として、プライバシー保護法に従ってこのような大規模なネットワークフローを保護するために、研究機関は高価なネットワーク帯域幅の大部分を浪費することになります。

イベントに伴う接続急増によって機能不全に陥る、順応性のないセキュリティ

前述の例と異なり、その他の業界では、個々の接続の量自体は、企業がごく短時間に処理する接続の総数に比べると、決して膨大ではありません。しかし、ブラックフライデーやサイバーマンデーなどの主要なショッピングシーズンのECサイトでは、24時間にわたって莫大なユーザートラフィックが発生します。そのトラフィック件数は、1年で2番目に件数の多い日の1.5倍に及びます⁷。

また、確定申告のシーズン、大規模イベントのチケット販売開始日、春節などの休日、およびオンラインゲーム（特に数百人のプレイヤーが30分間同時に参加するオンラインゲーム）環境においても、同様にイベントベースの接続増加が発生します。

これに対し、ハイパースケールアーキテクチャであれば、オンライン納税申告者、小売業者、およびゲームホスティングサービスは毎秒数百万件の着信接続を受け入れ、効率的に処理できます。ハイパースケールの投資対効果は簡単に説明できます。接続の切断やレスポンスの遅れが発生すると、売上が減少しブランドイメージが急速に低下する可能性があります。たとえば、ページの読み込み時間が1～3秒間遅れると、サイトを離脱する顧客は平均で32%増加します⁹。

しかし、研究機関と同様に、ネットワークのパフォーマンスは問題の半分にすぎません。これらの組織はネットワーク接続を保護する必要があるのですが、大半のNGFWにはこのように急増した接続を処理する機能がありません。ネットワークパフォーマンスのニーズに応えるためには、複数のNGFWアプライアンスを導入する、あるいはセキュリティ機能を完全に無効にするかの選択を迫られることになります。

極めてスケーラブルで仮想化されたサービスを実行するための課題

企業は極めて俊敏にサービスを立ち上げ、生産性を高め収益を獲得できなければなりません。ROIのメリットを最大化するには、物理/仮想両方の資産の相互運用に対応する必要があります。

仮想化されたサービスをVXLAN（Virtual eXtensible Local Area Network）などの極めてスケーラブルなテクノロジーを活用することによってすべてセグメント化し、VLANでは不可能な大規模スケーリングを実現できます。仮想化されたサービスは、多額の運用コストをかけることなく、スケールアップとスケールダウン、および移動が可能です。多くの場合、これらのサービスは既存の物理インフラストラクチャ上の他のサービスとの通信に不可欠です。最新の（ソフトウェアベースの）ソリューションは、不十分なパフォーマンスや遅延が原因でサービスの提供に多くの時間を要するという問題があります。

数百万ドルの損失につながりかねないファイアウォールの遅延

株式市場の取引や競技ゲームをはじめとする業界では、ネットワーク遅延を最小限に抑えることが極めて重要です。ネットワークトラフィックのラウンドトリップタイム（RTT）にわずかでも遅延発生すると、収益性やパフォーマンスに大きく影響する可能性があります。

このため、金融業界の組織は一般的にデータセンターへの遅延が極めて小さいネットワークインフラストラクチャに投資します。電子取引インフラストラクチャで許容される遅延は、わずか5 μ s以下です¹⁰。遅延の影響を受けやすいコンテキストでは、多くの組織がネットワークスループットのセキュリティを犠牲にしてNGFWを監視モードで構成しています¹¹。



1年間で2,000エクサバイトを超える膨大な医療データが生成されている中⁶、ネットワークのパフォーマンスとセキュリティが重要な課題となっています。



マルウェア攻撃は2019年末のショッピングシーズン中に63%急増しました⁸。

高速のデータセンター相互接続には高スループットの IPsec 接続が必要

クラウドサービスプロバイダー、および CDN（コンテンツ配信ネットワーク）を運用する組織にとって、複数の地域サイト間でデータを複製する機能は不可欠です。組織が地域サイトを使用して保存データの完全なコピーをホストする主な理由には、耐障害性の向上、顧客の要求に対するレスポンスの遅延低減、そしてプライマリデータセンターの負荷軽減が挙げられます。

その実現には、ネットワークの同期をサポートする地域サイト間の高帯域幅リンクである DCI（データセンター相互接続）が必要です¹²。クラウドサービスプロバイダーと CDN は機密データを送信することが多いため、これらのリンクは多くの場合 IPsec トンネルとして実装されます。ただし、それと同時に、レイヤー 4 のネットワークセキュリティではネットワークリンクと同じスループットで NGFW が IPsec トラフィックを処理する必要があります。プライベートリンクは 40 Gbps を超える IPsec スループットを実現できることから、これらのリンクを保護する NGFW が同等のスループットを実現できない場合、システムのボトルネックになる可能性があります。

結論

効率とカスタマーエクスペリエンスの向上を目的とした DI の取り組みにおいては、組織のネットワークインフラストラクチャを進化させることが重要です。ハイパースケールデータセンターは、大規模なネットワークフロー、接続の急増、およびその他のユースケースをサポートするように設計されています。

ハイパースケールネットワークアーキテクチャの導入が進む中、多くの組織はハイパースケールセキュリティの実現というさらに困難な課題に直面しています。ネットワークのボトルネックを解消する目的で NGFW を無効にする、あるいは監視モードにすると、攻撃に対して無防備になるだけでなく、データ保護の法規制へのコンプライアンスに違反してしまう可能性があります。

ハイパースケールデータセンターには、規模の拡大に伴って拡張可能なセキュリティソリューションが不可欠です。40 Gbps のエレファントフローや毎秒数百万件の接続の処理、大規模な仮想環境の俊敏なセグメント化に対応できるセキュリティソリューションでなければ、ハイパースケール環境において効果を発揮することはできないのです。



- ¹ [Digital innovation: A review and synthesis], Rajiv Kohli 氏、Nigel P. Melville 氏、Information Systems Journal、2018 年 1 月 29 日（英語）：<https://onlinelibrary.wiley.com/doi/epdf/10.1111/isj.12193>
- ² [The Best Days for Holiday Sales: A Guide for Businesses], Marisa Sanfilippo 氏、Business News Daily、2019 年 12 月 2 日（英語）：<https://www.businessnewsdaily.com/10220-holiday-sale-days.html>
- ³ [セキュアで高速なパフォーマンスを実現する FortiGate 次世代ファイアウォール：フォーティネットが業界最小の遅延とジッターレートで電子取引プラットフォームへの接続を保護]、フォーティネット、2020 年 4 月：https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/ja_jp/SB-Secure-Communications.pdf
- ⁴ [What is DCI?], Ciena、2019 年 5 月 16 日（英語）：<https://www.ciena.com/insights/what-is/What-is-DCI.html>
- ⁵ [Machine Learning and HPC in Pharma Research and Development], Mohammad Shaikh 氏、Harsha Gururkar 氏、Super Computing 2019、2019 年 11 月（英語）：https://sc19.supercomputing.org/proceedings/bof/bof_pages/bof156.html
- ⁶ [How Big Data Will Unlock the Potential of Healthcare], Jeff Desjardins 氏、Visual Capitalist、2018 年 7 月 26 日（英語）：<https://www.visualcapitalist.com/big-data-healthcare/>
- ⁷ [The Best Days for Holiday Sales: A Guide for Businesses], Marisa Sanfilippo 氏、Business News Daily、2019 年 12 月 2 日（英語）：<https://www.businessnewsdaily.com/10220-holiday-sale-days.html>
- ⁸ [63% Malware Spike During Black Friday and Cyber Monday], Security Magazine、2019 年 12 月 12 日（英語）：<https://www.securitymagazine.com/articles/91425-malware-spike-during-black-friday-and-cyber-monday>
- ⁹ [Find Out How You Stack Up to New Industry Benchmarks for Mobile Page Speed], Google、2017 年 3 月（英語）：<https://www.thinkwithgoogle.com/intl/en-aunz/advertising-channels/mobile/au-mobile-page-speed-new-industry-benchmarks/>
- ¹⁰ [セキュアで高速なパフォーマンスを実現する FortiGate 次世代ファイアウォール：フォーティネットが業界最小の遅延とジッターレートで電子取引プラットフォームへの接続を保護]、フォーティネット、2020 年 4 月：https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/ja_jp/SB-Secure-Communications.pdf
- ¹¹ [The NGFW Today: A Staple of Network Security in Spite of Challenges], Jason Pappalexis 氏、NSS Labs、2019 年 3 月 11 日（英語）：<https://www.nsslabs.com/blog/2019/3/11/the-ngfw-today-a-staple-of-network-security-in-spite-of-challenges/>
- ¹² [What is DCI?], Ciena、2019 年 5 月 16 日（英語）：<https://www.ciena.com/insights/what-is/What-is-DCI.html>
- ¹³ [セキュアで高速なパフォーマンスを実現する FortiGate 次世代ファイアウォール：フォーティネットが業界最小の遅延とジッターレートで電子取引プラットフォームへの接続を保護]、フォーティネット、2020 年 4 月：https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/ja_jp/SB-Secure-Communications.pdf

FORTINET®

フォーティネットジャパン株式会社

〒106-0032

東京都港区六本木 7-7-7

Tri-Seven Roppongi 9 階

www.fortinet.com/jp/contact

お問い合わせ