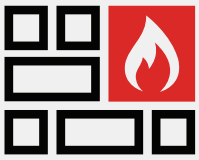
INDUSTRY INSIGHTS

ハイブリッドメッシュファイアウォール：今日の分散型企業に不可欠なソリューション

ハイブリッドメッシュファイアウォールとは

今日のサイバー犯罪者は、ほとんどの組織が分散型ネットワークにいくつものセグメントが存在し、一貫性のある可視性が欠如しているという事実を悪用しています。さらには、データセンター、キャンパス、クラウド、支社 / 拠点の環境の相互接続に伴って、水平方向のトラフィックが増加したため、ネットワークのある場所で侵害が成功すると、他の場所にすぐに移動できるようになりました。この課題の最も有効な解決方法は、ネットワークのすべての場所に完全に同一のセキュリティを導入することで、脅威の相関付けを一元化し、エンタープライズ IT の複数の領域に対して同時かつ協調型の保護を可能にすることです。しかしながら、さまざまなネットワークエコシステム間の複雑さや相違から、その実現は困難でした。Gartner® は、この問題を解決する手段として、ハイブリッドメッシュファイアウォール（HMF）の幅広い採用を提唱しています。



「2026 年までに、60% 以上の組織が 2 種類以上のファイアウォールを導入するようになり、ハイブリッドメッシュファイアウォールの採用が加速する」[1]

ハイブリッドメッシュファイアウォールでは、キャンパス、データセンター、仮想 / クラウド、FWaaS / SASE などのネットワークのあらゆる場所への重要な NGFW 機能の展開とリモート統合管理が可能になり、これにより、今日の動的で分散型のネットワークに対応し、拡張と適応が可能な単一の統合プラットフォームが構築されます。HMF では、IT ドメイン（企業サイト、パブリッククラウド、プライベートクラウド、リモートワーカー）の保護が統合管理コンソールから調整されます。この統合アプローチにより、サイバーセキュリティのスキルがすでに不足している状況においても、IT チームは、脅威検知とレスポンスの自動化、構成のオーケストレーション、ポリシーの適用を手動で時間をかけて行う必要がなくなります。

ハイブリッドメッシュファイアウォールに対するニーズ

Gartner は最新のネットワーク・ファイアウォールの Magic Quadrant ™ で、「2026 年までに 60% 以上の組織が複数のタイプのファイアウォールを導入するようになり、ハイブリッドメッシュファイアウォールの採用が加速する」と予測し、「クラウドファイアウォールや FaaS（Firewall-as-a-Service）の出現による、ネットワーク・ファイアウォールからハイブリッドメッシュファイアウォールへの進化に伴い、最適なベンダーの選択が困難な課題となっている」と指摘しています。

HMF ソリューションは、今日の IT 組織が直面する 4 つの重要な課題を解決することを前提に設計されています。

1. IT の複雑さの管理

現在の多くの NGFW は HMF の機能をサポートできないため、エンタープライズ IT のエンドユーザーは、企業サイト、パブリック / プライベートクラウド環境、リモートワーカーをサポートする異なるセキュリティソリューションを購入することになります。これにより、オペレーションの一貫性の欠如によって構成ミスなどが発生し、ネットワーク侵害につながる可能性があります。

2. サイバーセキュリティの人材不足

ポイント製品は、複雑なだけでなく導入に時間がかかるため、組織のリスクが増大します。複数のポイント製品を使用すると、サイバーセキュリティ IT 担当者が新しい機能やダッシュボードを習得するのに時間がかかります。世界的な人材のギャップによってサイバーセキュリティの分野で 3 分の 1 の人材を確保できていないことから、このことで企業がさらなるリスクに直面することになります。

3. 高度な脅威の急増

HMF のニーズを高くしている要因は、複雑さとサイバーセキュリティの人材不足だけではありません。現実としての脅威が高度なサイバー脅威という形で世界中で拡大し、このような高度な脅威の検知がこれまで以上に困難になっており、ビジネスの被害は増大するばかりです。高度な脅威の攻撃ベクトルは、Web、アプリケーション、コンテンツ、デバイスと広範囲にわたり、例えば、ランサムウェアは、オペレーショナルテクノロジー（OT）、政府機関、地方自治体、製造業、医療機関を始めとするあらゆる業種を混乱させ続けています。

4. AI / ML と脅威インテリジェンスの役割

複雑さ、手動の監視、脅威の拡大という問題を解決するには、協調型の保護が必要です。ファイアウォールでネットワークの異なる領域を保護するだけで十分ではありません。既知と未知の脅威からの保護に必要となる人工知能と機械学習（AI / ML）機能も必要です。AI / ML を活用したセキュリティを HMF に追加することで、アプリケーション、Web URL、ユーザー、デバイス、マルウェアなどを識別して分類し、ドメインへのポリシーの適用を自動化できます。AI / ML は HMF 自動化の中核であり、エンタープライズ IT の保護における手動の作業の大幅な削減を可能にします。

ハイブリッドメッシュファイアウォールに求められるもの

一元的で統一された管理

HMF の最も重要なメリットは、任意のツールを使用した脅威の検知、ポリシーの管理、ネットワークのあらゆる場所で脅威へのレスポンスの自動オーケストレーションが可能になることです。企業サイト、パブリッククラウド、プライベートクラウド、リモートワーカーなどの異なるドメインで異なるダッシュボードが必要であるのであれば、そこには HMF は存在しません。

統合管理により、ドメインが調整されて、単一のエンタープライズ IT セキュリティソリューションに統合されるため、企業サイトからクラウド、リモートワーカーまでのシンプルで自動化された保護が可能になります。また、分散するネットワーク・ファイアウォールの管理の要件は組織ごとに異なるため、アプライアンス、VM、SaaS、マネージドファイアウォールサービスなどのあらゆるフォームファクターをサポートしている必要があります。

HMF はさらに、ネットワークオペレーションセンター（NOC）とセキュリティオペレーションセンター（SOC）のチームの作業を一元管理により統合し、攻撃対象全体の管理と監視を可能にするものでなければなりません。

ASIC を搭載するアプライアンス

ネットワークのどのような環境にも、固有のセキュリティの課題があります。企業サイトには、ユーザーエクスペリエンスに影響することなく一貫性のある保護を保証する、セキュリティ機能の拡張が可能なアプライアンスが必要です。HMF がネットワークボトルネックの原因となるべきではありません。

パフォーマンスを追求する今日の組織は、クリティカルなセキュリティサービスの速度の向上を可能にする、強力な ASIC（特定用途向け集積回路）を搭載するアプライアンスを必要としています。カスタム ASIC を搭載するセキュリティアプライアンスは、ファイアウォール、VPN、IPS、さらには SSL やディープパケットインスペクション（DPI）などのリソースを多用する多くの機能をオフロードできるため、ネットワークパフォーマンスに影響することなく、多層型のセキュリティ制御で企業サイトを保護できます。

クラウドネイティブファイアウォール

クラウドネイティブファイアウォールは、IaC（Infrastructure-as-Code）として IaaS 環境に展開されたパブリッククラウドアプリケーションのワークロードを保護します。クラウドネイティブの HMF をクラウド環境に追加することで、可視性が向上すると同時に、ファイアウォールソフトウェアインフラストラクチャの構成、プロビジョニング、保守が不要になることで、ネットワークセキュリティオペレーションのワークロードも軽減され、セキュリティチームがポリシー管理に集中できるようになります。

バーチャルファイアウォール

バーチャルファイアウォールは、ソフトウェア定義型データセンターやマルチクラウド環境における仮想化された環境を保護する目的で広く利用されており、最も安価で最も移植性の高いソリューションであるため、IT 担当者はバーチャルファイアウォールをクラウドからクラウドへ迅速に移動することができます。しかしながら、HMF ソリューションのバーチャルファイアウォールにより、ソフトウェア定義型データセンターの包括的なセキュリティエコシステムがさらに強化され、統合プロセスの支援と同時に、ステートフルファイアウォールにとどまらないさまざまなサイバーセキュリティサービスを利用して環境を脅威から保護できるようになります。

FaaS（Firewall-as-a-Service）

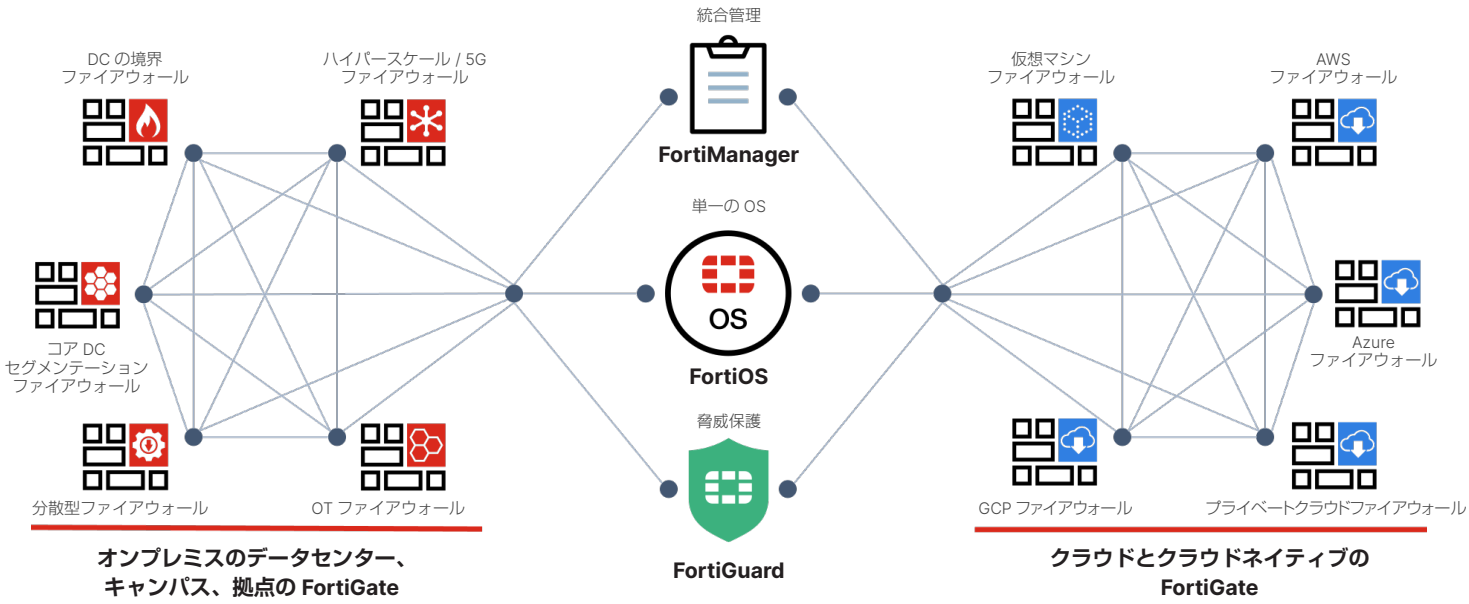
FaaS（Firewall-as-a-Service）は、クラウドベースのサービスとして提供される、IT インフラストラクチャの簡素化と拡張を可能にするファイアウォールソリューションです。FWaaS には、オンプレミスに導入するハードウェアファイアウォールと多くの共通点があり、Web フィルタリング、高度な脅威保護、IPS、DNS セキュリティなど、NGFW のすべての機能を利用できます。また、FWaaS ソリューションとして展開される HMF は、その独自の機能を分散するユーザーやデバイスに拡張し、スケーラビリティと一元的な制御をほぼ瞬時に実現します。

単一のオペレーティングシステム

ネットワークエッジの急速な拡大により、ベンダーやポイントソリューションのスプロール化という課題がさらに深刻化しています。異なるポイントソリューションは、連携することも情報を共有することもできないため、一貫性のあるセキュリティポリシー、エンドツーエンドの可視化、自動化を実現することはできません。また、ハイブリッド、ハードウェア、ソフトウェア、XaaS（X-as-a-Service）の多数のソリューションの維持と監視は、セキュリティチームに多くの負担を強いることになります。

HMF の基盤である単一のオペレーティングシステムにより、多数のテクノロジーとユースケースが簡素化された単一のポリシーと管理フレームワークに統合されます。統合管理コンソールによって、フロントエンドのオペレーションが統一され、単一のオペレーティングシステムによって、アプライアンス、バーチャルファイアウォール、クラウドネイティブのファイアウォール、FWaaS エージェントなどのさまざまな導入環境のバックエンドの相互運用が可能になります。

ハイブリッドメッシュファイアウォール



ハイブリッドメッシュファイアウォールの価値

ハイブリッドメッシュファイアウォールは、エンタープライズ IT に計り知れない多くのメリットをもたらします。これには、IT オペレーションの効率化、サイバーセキュリティオペレーションの簡素化、組織リスクの低減、サイバーセキュリティスキルギャップの解消、既知および未知のサイバー脅威に対するレジリエントな防御、AI / ML による自動化と調整、TCO の削減などが含まれます。

最適なハイブリッドメッシュファイアウォールの選択

すべての組織が HMF を理解しているわけではありません。さまざまな宣伝文句が溢れる現状で、企業の IT 購入担当者が意味ある情報を見つけるのは時には困難です。多くの場合、HMF と宣伝しているものの、その実体は、不完全なソリューションの寄せ集めであったり、どのような環境でも動作する保証がないニッチなポイント製品であったり、ハイブリッドの機能が欠如した従来型のファイアウォールであったり、相互運用性のないソリューションの集まりであったりします。

組織が必要とするのは、NGFW の機能、多様なフォームファクターを選択できる柔軟性、高度な ASIC テクノロジーによる高速化と拡張性、導入環境間の一貫性と相互運用性を保証する共通のオペレーティングシステム、最新の脅威に常に対応する高度な AI ベースのサービス、さらには、管理、オーケストレーション、レスポンスが統合されたソリューションです。この条件を満たす HMF であれば、多様なフォームファクターから選択でき、場所、環境、時間の制限なく、単一ソリューションとして運用し、データの相関付けやレスポンスが可能になります。

[1]「Magic Quadrant for Network Firewalls」、Gartner、Rajpreet Kaur、Adam Hils、Tom Lintemuth 共著、2022 年 12 月 19 日（英語）：https://www.fortinet.com/resources/analyst-reports/gartner-network-firewalls

フォーティネットジャパン合同会社

〒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