5G セキュリティ ソリューションガイド

モバイルネットワークの5Gへの移行における
セキュリティの確保と拡張性

5G のセキュリティガイド

5G は高速通信、低遅延、膨大な数の新たな IoT アプリケーションの実現、そして新たな 5G を活用したビジネスの実現をモバイル通信事業者にもたらします。一方で 5G の展開に伴うセキュリティ上の懸念は最大の課題となっています。ミッションクリティカルなアプリケーションやインフラストラクチャが悪意のある攻撃を受け、その結果サービスの混乱やネットワークの切断に陥る可能性があります。こうした事態が現実となった場合、経営に影響が出るだけでなく、ブランドイメージは深く傷つき、そして同時に企業評価が低下する可能性があります。IoT デバイス数の大幅な増加やサイバー犯罪者の影響の深刻さ、ボットネットから受ける高いリスクなどを踏まえると、進化を続けるモバイルネットワークを保護することは、5G 展開において戦略上重要です。モバイル通信事業者はセキュリティと、ネットワークパフォーマンスやコストなど様々なビジネス要件との間で適切なバランスをとる必要があります。

A10 ネットワークスの 5G セキュリティポートフォリオは、ネットワークが 5G に進化しクラウドおよびエッジネットワークが統合されてゆく過程において必要になる柔軟性、スケーラビリティ、および攻撃防御を兼ね備えた、費用対効果の高いセキュリティソリューションをモバイル通信事業者向けに提供します。A10 のポートフォリオは、サービスプロバイダレベルの包括的セキュリティスタックを提供するほか、モバイルネットワークに必要なさまざまな機能を提供します。このセキュリティスタックには、全てのネットワークピアリングポイントに対応したファイアウォール機能や、ディープパケットインスペクション（DPI）、キャリアグレード NAT（CGNAT）、IPv6 移行機能、DDoS 脅威に対する統合型攻撃防御機能、インテリジェントトラフィックステアリング機能、分析機能などが含まれています。

本ガイドでは、5G への移行を成功に導くために A10 が提供できる主要な 5 つのソリューション概要を紹介します。

- **Gi-LANセキュリティ**
- **モバイルローミングセキュリティ**
- **ネットワークスライシング**
- **全ネットワークを網羅したDDoS攻撃防御**
- **セキュアかつ効率的なMEC**

5G セキュリティポートフォリオのその他のソリューションの詳細については
www.a10networks.co.jp/Orion5G を参照してください。

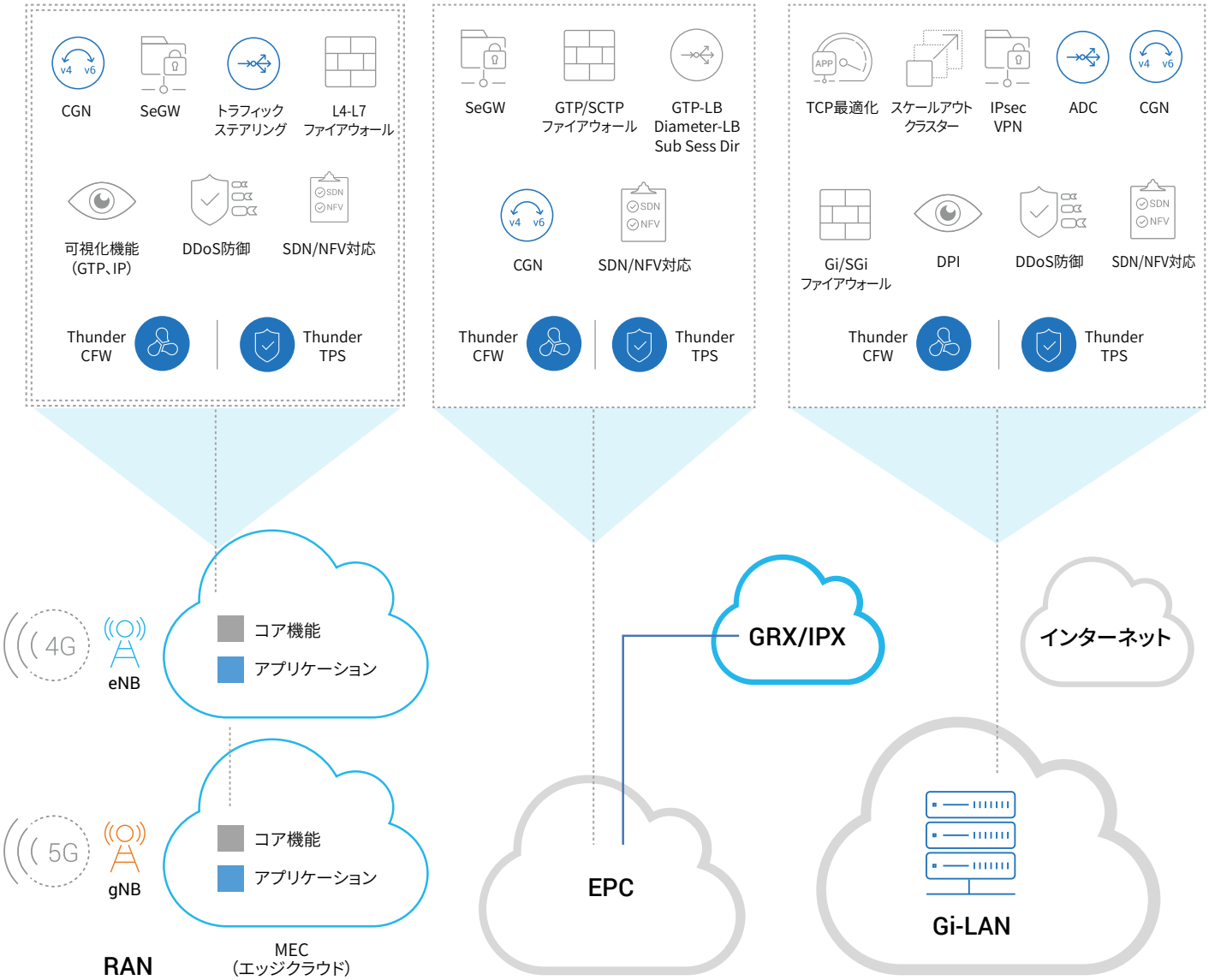

図1：A10が提供する4G、MEC、5Gネットワーク向けセキュリティポートフォリオ

Gi-LAN セキュリティ ー Gi/SGi ファイアウォール

ユースケース #1

モバイルサービスの利用者やネットワークに対する深刻な脅威は、インターネットインターフェース（Gi/SGi）経由で侵入します。トラフィック量、デバイスの数やサイバー犯罪者の増加に伴い脅威も増え続けています。

A10 のハイパフォーマンスセキュリティプラットフォーム、A10 Thunder CFW は、モバイルキャリアで要求されるパフォーマンスを実現しながら、搭載された Gi/SGi ファイアウォールによってインフラや利用者を保護します。この Gi/SGi ファイアウォールは、あらゆるサービス・プロバイダにおいて、現在から将来にわたるトラフィックの需要に対応することができます。

モバイルキャリアで必要とされるセキュリティやアプリケーションネットワーキングなどの複数機能を 1 台に集約することで、OPEX や CAPEX のコストを削減しながら、最高クラスのパフォーマンスと効率性、拡張性でモバイルインフラストラクチャを保護します。

さらにサービスプロバイダは、仮想アプライアンス A10 vThunder® を用いて仮想環境で Gi/SGi ファイアウォールを使用することも可能であり、用途に応じて自由に機能を選択し、柔軟かつ容易に、ソフトウェアベースの環境を実現することもできます。

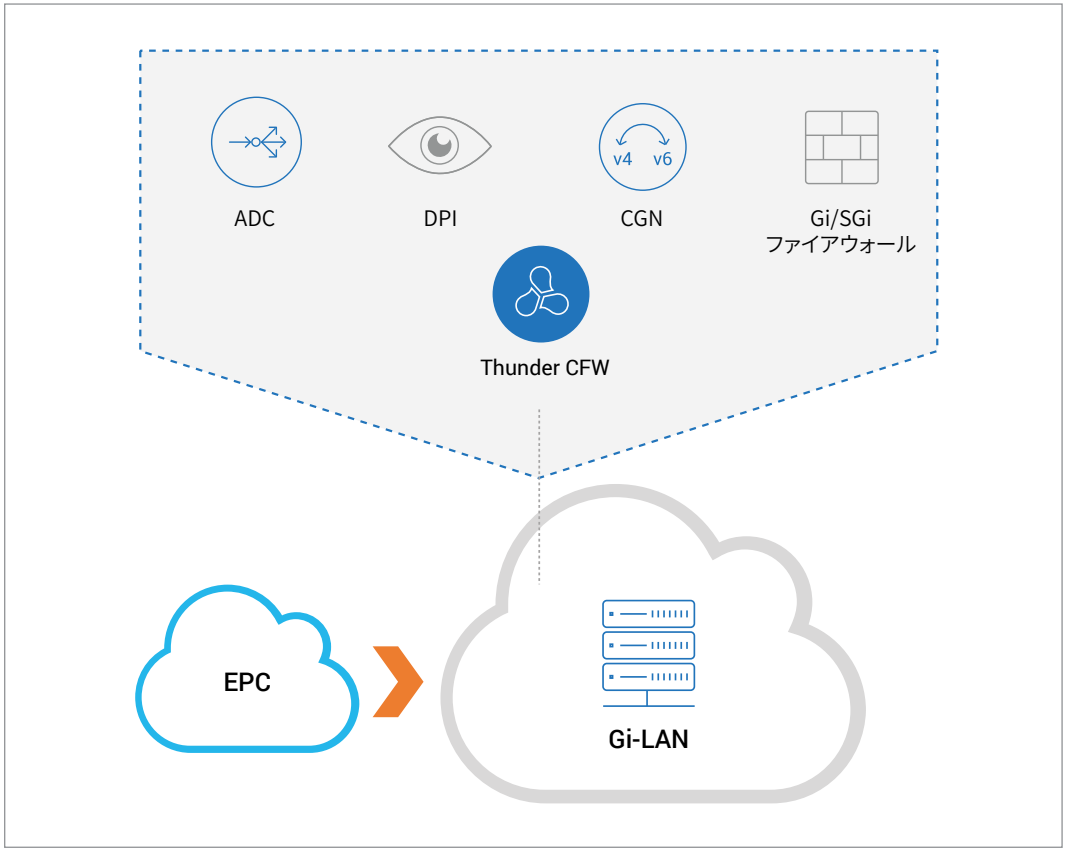

図 2：ネットワークインフラストラクチャを保護する Gi-LAN ソリューション

モバイルローミングのセキュリティ ー GTP ファイアウォール

ユースケース #2

ローミングやその他の EPC インターフェースで使用される GTP プロトコルには、複数の既知の脆弱性があり、悪意ある人物（または組織）により悪用される危険に常にさらされています。利用者の接続先がどこであれ、どのようなデバイスであれ、どのようなネットワークからのアクセスであれ、モバイル通信事業者は、セキュリティの課題に対応しつつ、利用者にシームレスな利用環境を提供しなければなりません。

A10 の GTP ファイアウォールは、プロトコルに通常と異なる挙動が見られる場合、不正なメッセージ、およびその他の不審なインジケータに対し、ステートフルインスペクション、レートリミット、トラフィックのフィルタリングなど幅広いセキュリティ機能を提供します。GTP ファイアウォールは、不正使用、守秘義務違反、無効なメッセージ、不審な接続点からの DDoS 攻撃などといった GTP プロトコルの脆弱性をついた攻撃や、その他のさまざまな脅威からネットワークを保護します。

GTP ファイアウォールは、A10 の 5G ソリューションポートフォリオの一部です。GTP ファイアウォールは GTP トラフィックを転送する複数のインターフェースに実装することができます。最も基本的なユースケースとしては、S5-Gn と、S8-Gp（ローミング）インターフェース上で利用されます。

GTP ファイアウォールはスケーラビリティを提供し、止まらない運用を支援すると同時に、情報漏えい、不審なパケット攻撃、詐欺、DDoS 攻撃など、アクセスネットワークおよび GRX/IPX 相互接続における GTP インターフェースを介した GTP ベースの攻撃から利用者およびモバイルコアを保護します。

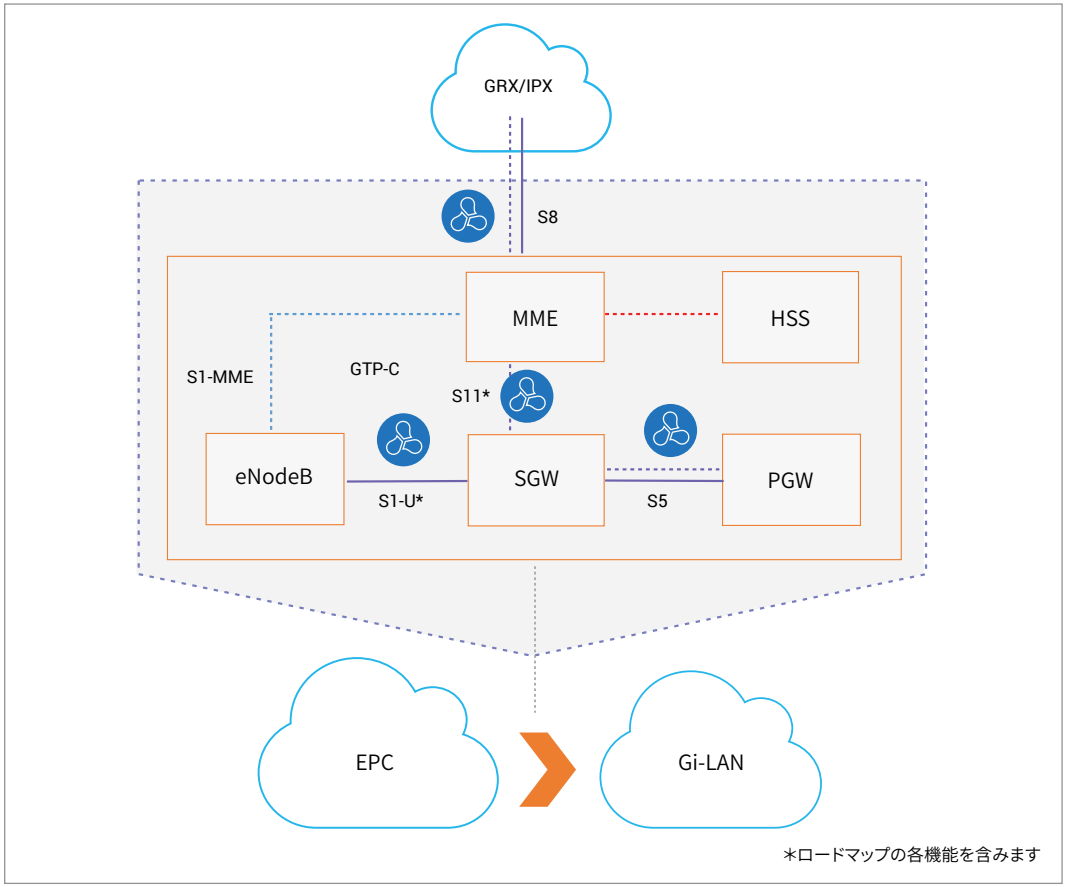

図 3：GTP ベースの攻撃から利用者とネットワークを保護する GTP ファイアウォール

ネットワークスライシング ー インテリジェントなトラフィックステアリング

ユースケース #3

ネットワークスライシングにより、モバイル通信事業者は、共通インフラはそのままに、多様なサービスの展開に向けてセキュリティなどの機能を各業種のアプリケーションに適した状態で提供することが可能になります。ネットワークスライシングでは、サービスごとにネットワークが分離されるため、各サービスを独立して構築し、セキュアに管理を行い、堅牢な形で提供することができます。

A10 は 5G におけるネットワークスライシングの各種シナリオを想定し、拡張性に富んだセキュリティソリューションを提供します。モバイル通信事業者は 5G への移行に備えて今からネットワークスライシングのコンセプトを利用し始めることができます。

A10 の 5G ソリューションでは、トラフィックステアリングおよびアプリケーション配信をインテリジェントに行うことができます。このソリューションは無線アクセスの種類、IP アドレス、DNS アドレス、デバイスタイプ、宛先、利用者 ID やその他のパラメータなど、複数の条件に基づく特定のタイプのトラフィックを識別します。そして、これらトラフィックを、より詳細に脅威解析およびスクラビングを行うことができる脅威防御プラットフォームなどの付加価値サービスプラットフォームへリダイレクトします。リダイレクトは静的ポリシーまたは動的に実行することができます。

このソリューションは、ネットワーク全体への不必要な検査にかかる負荷を軽減し、さまざまに発展を続けるそれぞれの 5G のユースケースに対してセキュリティを強化し、収益増加の機会を増やすことができます。

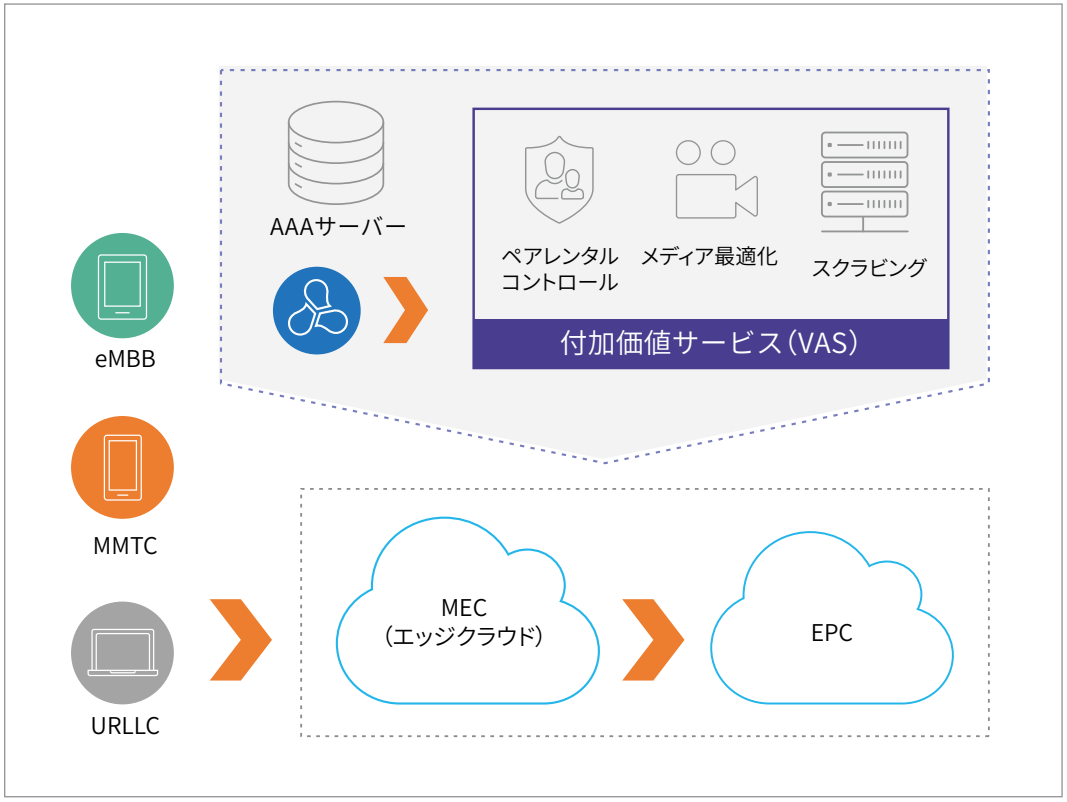

図 4：トラフィックをスライシングされた付加価値サービスに転送するインテリジェントトラフィックステアリング

ネットワーク全体の DDoS 検知・緩和システム

ユースケース #4

モバイル通信事業者は常にネットワークの可用性を高い状態に維持する必要があります。DDoS 攻撃は標的のモバイルネットワークや利用者に対し、インフラストラクチャの処理性能を上回る大量のメッセージを一気に送りつけることにより（フラッド攻撃）、サービスの低下やネットワークダウンを発生させます。標的型攻撃はあらゆるネットワークピアリングポイント経由で実行される可能性があり、特定のネットワーク装置や主要顧客の重要なアプリケーションをターゲットにして、大容量／小容量のトラフィックが入り混ざった複雑な攻撃を行います。攻撃量増加への対策として必要以上にネットワーク装置を用意したり、攻撃されている期間にトラフィックを単純にブロックしたりするだけではコストがかかってしまう上、重要なトラフィックにおいてサービス拒否が発生してしまう可能性があります。モバイル通信事業者には、重要なトラフィックのサービス拒否を起こさせないために、全モバイルネットワークにまたがって DDoS 攻撃などのインフラストラクチャへの攻撃を素早く検出し攻撃を緩和することができる、費用対効果が高く、包括的な対応策が必要です。

A10 の 5G セキュリティソリューションでは、DDoS 対策のフルオートメーション化と独自の高精度な検知機能を提供する、One-DDoS Protection を提供しています。DDoS 対策専用アプライアンス A10 Thunder TPS™による、ネットワーク境界部分でのフローベースの攻撃検知と DDoS 攻撃の緩和、各所に設置された A10 Thunder CFW を始めとする Thunder シリーズによる、高精度なパケットベースの検知を実現する分散型検知機能を組み合わせて、一連の DDoS 防御サイクルをオートメーション化します。これにより、サービスプロバイダは多層型の DDoS 攻撃防御が可能になります。さらに Thunder CFW には、シグナリングフラッド攻撃や特定インフラへの標的型攻撃に対する防御機能が統合されています。

攻撃者がターゲットをダウンさせることに成功する前に、あらゆる種類と規模の攻撃を検出・緩和する多層防御により、各サービスプロバイダは完全な DDoS 耐性を確保し、セキュリティを強化することができます。

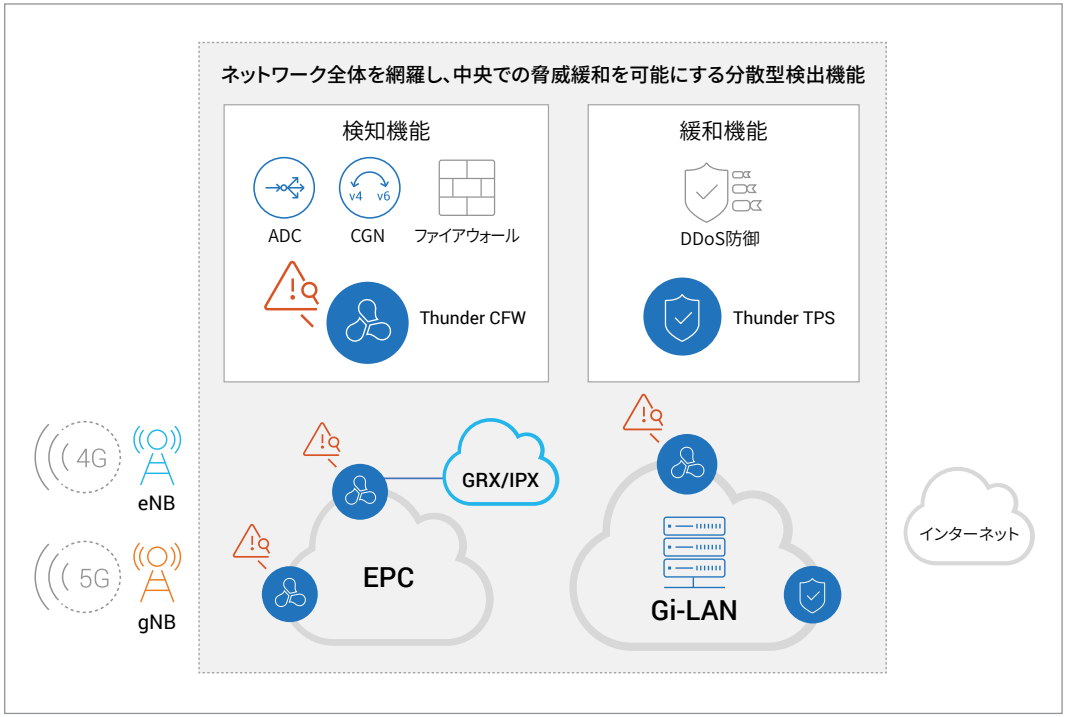

図 5：Thunder TPS と Thunder CFW による、業界最先端の DDoS 検知・緩和機能

セキュアで高機能な MEC

ユースケース #5

マルチアクセスエッジコンピューティング（MEC）は、5G への移行計画に組み込まれるアーキテクチャです。MEC アーキテクチャではネットワークトラフィックの処理を中央のデータセンターやモバイルコアに代わって、よりユーザーに近い場所に設置された複数の拠点（エッジ）で行います。数千ものノードを有する分散型アーキテクチャでは管理上の困難が増すため、導入、管理、およびセキュリティや運用の変更の際には、高水準の自動化と解析機能が必要です。

A10 Thunder CFW は、ソフトウェアまたはハードウェアで、ファイアウォールや CGNAT、IPv6 移行、トラフィックステアリングなどの機能を高性能かつ低遅延で提供します。これまで個々のアプライアンスで提供されていた機能の多くが、単一のアプライアンス、仮想インスタンス、ベアメタル、またはコンテナに集約された形で提供されます。

使用可能な設置スペースと消費電力を超えることなく、費用対効果の高い、高性能なセキュリティを確保できます。A10 ネットワークスの ACOS オペレーティングシステムは、あらゆるフォームファクタを提供することで、最大の柔軟性と一貫性のある導入を実現します。一元化された管理および解析機能により運用が簡素化され、TCO（総保有コスト）の低減を実現しています。

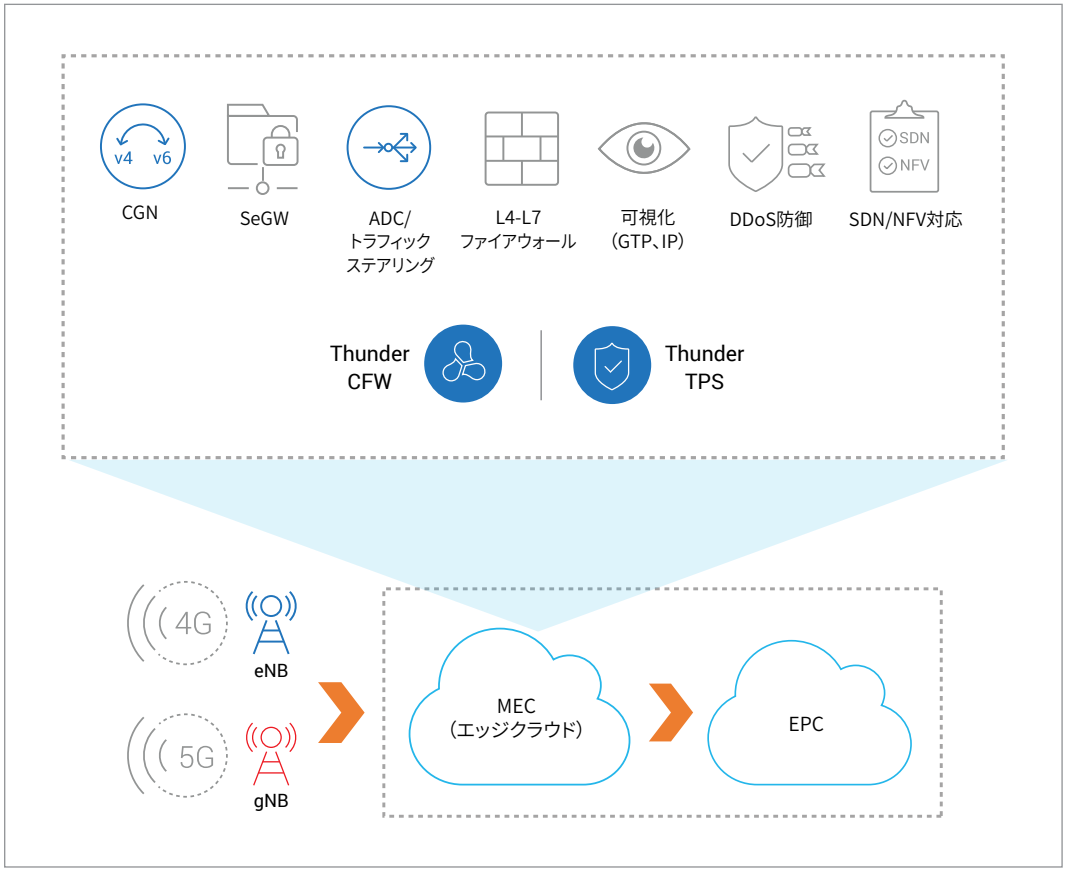

図 6：Thunder CFW 、Thunder TPS による省スペース / 省エネルギーの MEC 環境ソリューション

A10 のソリューション ー 5G への旅の良きパートナーとして

A10 は、5G ネットワークの各種シナリオを想定し、高度にスケーラブルなセキュリティソリューションを提供します。堅牢なファイアウォール、DDoS 緩和・検知テクノロジは、個々のネットワークトポロジ（4G、5G-NSA、MEC、5G SA）に応じて、さまざまなフォームファクタ（物理、仮想、ベアメタル、コンテナ）で導入することが可能です。

A10 Thunder CFW は、最も高い要求水準の 5G ユースケースにおいても、高いファイアウォールのコネクションレート、低遅延、スループット、および同時セッション数を、コンパクトかつ柔軟なフォームファクタで提供します。

A10 Thunder TPS はマルチベクトル型 DDoS に対するフルオートメーション化された防御ソリューションとして、規模の大小やネットワークの種類によらず、サービスの可用性を確保します。

5G に向けてネットワークを進化させるモバイル通信事業者に対し、A10 の 5G セキュリティポートフォリオはディープパケットインスペクション機能を備えたファイアウォール、キャリアグレード NAT、インテリジェントなトラフィックステアリングおよび解析を、業界最先端の DDoS ソリューションと組み合わせることにより最大の柔軟性、スケーラビリティ、および保護を提供します。

本ソリューションガイドでは、A10 の 5G ソリューションポートフォリオに含まれるキーソリューションのうち 5 つを抜粋して紹介しています。
サービスプロバイダ向けソリューションに関する、より詳細な情報については **www.a10networks.com/solutions/service-provider/** を参照してください。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks（NYSE: ATEN）はセキュアアプリケーションサービスにおけるリーディングカンパニーとして、高性能なアプリケーションネットワーキングソリューション群を提供しています。お客様のデータセンターにおいて、アプリケーションとネットワークを高速化し可用性と安全性を確保しています。A10 Networks は 2004 年に設立されました。米国カリフォルニア州サンノゼに本拠地を置き、世界各国の拠点からお客様をサポートしています。

A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。　詳しくはホームページをご覧ください。

URL：http://www.a10networks.co.jp/
Facebook：http://www.facebook.com/A10networksjapan

LEARN MORE
ABOUT A10 NETWORKS

CONTACT US
a10networks.co.jp/contact

A10ネットワークス株式会社
www.a10networks.co.jp

Part Number: A10-BR-20111-JA-01 FEB 2020