次世代のビジネスおよびテクノロジ ソリューションに
関する、独立した立場による市場調査および
競合分析（サービス プロバイダとベンダー向け）

HEAVY READING
WHITE PAPER

5G セキュリティ戦略での考慮事項

ジュニパーネットワークス向け *Heavy Reading* ホワイト ペーパー

JUNIPER NETWORKS

著者：HEAVY READING、チーフ アナリスト、ジム・ホッジズ氏

はじめに

5G がさまざまなレベルで大きな変革をもたらすことは確かです。5G は単なるネットワーク速度を表すものではなく、IoT（モノのインターネット）ベースのアプリケーションへの対応を始めとした多様な新しいサービスや垂直アプリケーションの実現を象徴する言葉でもあります。大幅なイノベーションを受けて RAN、コア、トランスポート アーキテクチャが設計されました。一方で、セキュリティは依然としてサービス プロバイダにとって最大の懸念事項となっており、5G の進化戦略を策定する際に独自のデバイス要件やアプリケーション要件のセキュリティへの影響を考慮する必要があります。

さまざまな業界に 5G ネットワークをスムーズに提供するにはセキュリティが欠かせません。5G ネットワークでは、膨大な数のデバイスを接続し、セキュリティ ニーズの異なる多様なアプリケーションやお客様にサービスを提供します。5G アプリケーションとその規模/スループット/遅延要件は多岐にわたるため、セキュリティ管理とセキュリティ ポリシーにおいて効率性、一貫性、正確性のバランスを取るのは困難です。さらに、MEC（マルチアクセス エッジ コンピューティング）、仮想化、CUPS（制御プレーンとユーザー プレーンの分離）、ネットワーク スライシングの導入により、サービス プロバイダが対処しなければならない新たな攻撃対象領域が発生しています。

このホワイト ペーパーでは、5G のまったく新しい機能とセキュリティへの影響に加え、5G に移行する際にサービス プロバイダに生じるセキュリティ関連の課題とチャンスについて説明します。

4G と比較した 5G の新機能

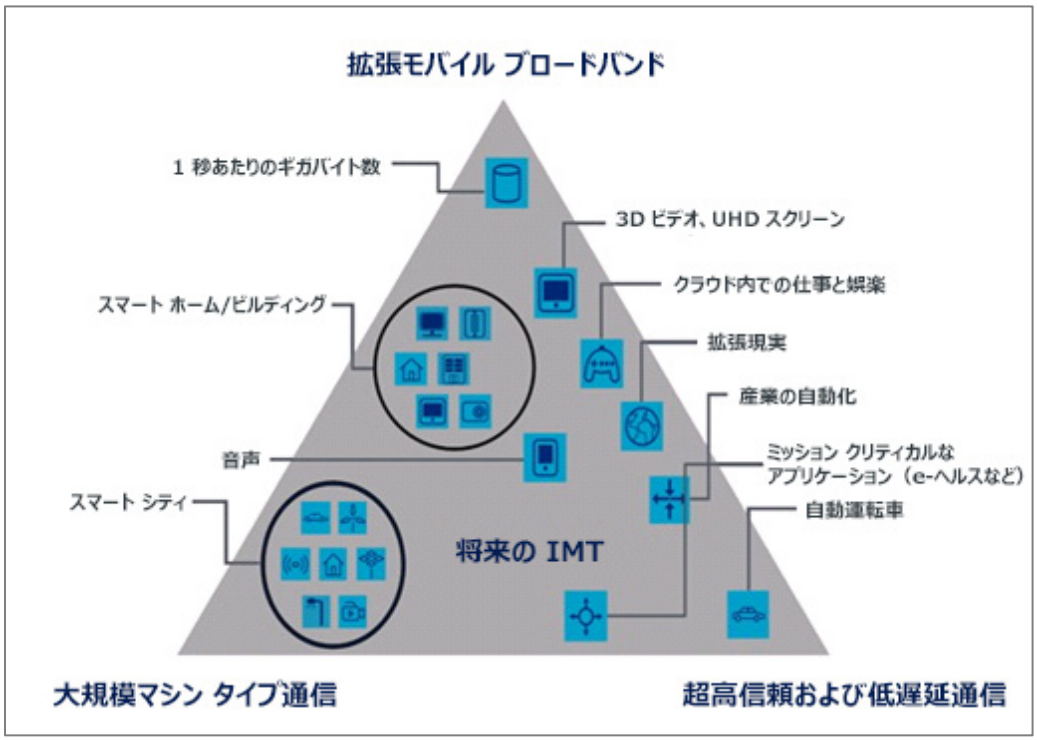
5G が目標とする優れたパフォーマンスには、1 ミリ秒の遅延と 10 Gbps のピーク データ レートが含まれます。どちらも 4G ネットワークからの飛躍的な改善を表すものです。こうした壮大なパフォーマンス目標は、5G ネットワークのセキュリティ パフォーマンスの進化にさまざまな影響を及ぼしています。

すべての前世代の技術と比較して、5G は多種多様な導入事例に対応できるように設計された初のモバイル アーキテクチャです。特定のドメインとそれに伴う導入事例をどのように構成するかについて構造を提示するために ITU（国際電気通信連合）は 5G サービス階層を公開しました。

図 1 に示すように、この階層では 5G サービスが 3 つのドメインに分かれています。従来の eMBB（拡張モバイル ブロードバンド）と、2 つの新ドメインの mMTC（大規模マシン タイプ通信）および URLLC（超高信頼/低遅延通信）です。ドメインごとに独自のセキュリティ要件があります。そうしたさまざまなアクセスとサービスの需要を 1 つの統合された 5G ネットワーク経由で保護するのが難しいのは当然です。

たとえば、5G はスマート シティの基盤であるトラフィック センサーや V2I（路車間通信）サービスなどの大規模な IoT アプリケーションの稼働を可能にします。ハッカーによるそうしたデータへのアクセス、IoT デバイスのハイジャック、サービスの中断を防ぐことが重要です。

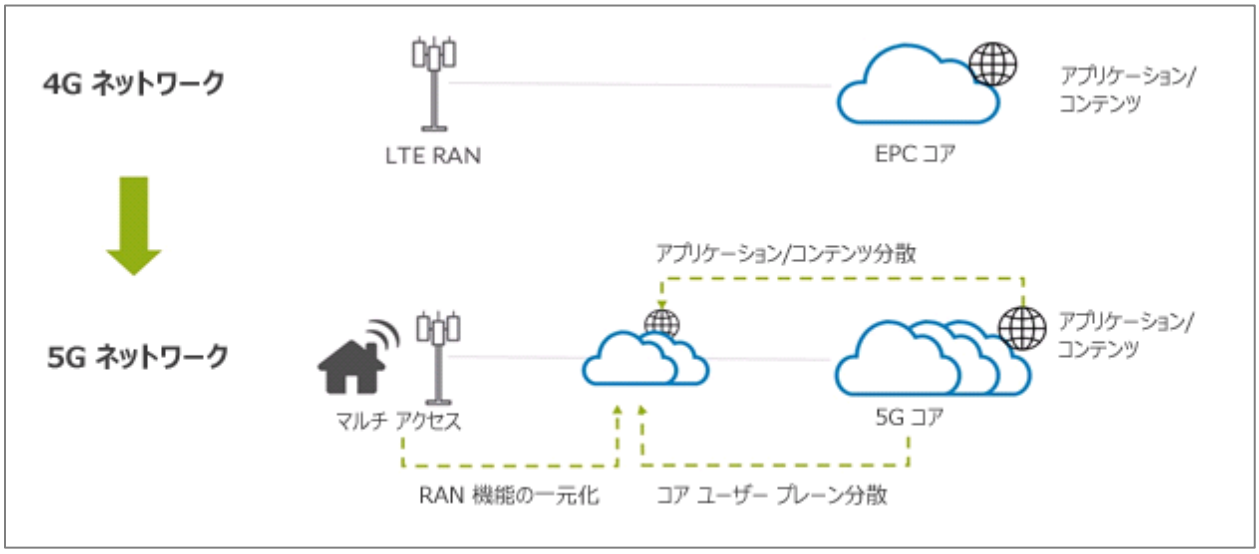
図 1：ITU の 5G サービス階層



出典：*ITU-R M.2083-0*

こうした異なるパフォーマンス メトリックを達成するために、5G には MEC、CUPS、ネットワーク スライシングなどの新たなネットワーク設計アプローチが採り入れられています。**図 2** に示すようなこうしたネットワーク アーキテクチャの変化に伴い、セキュリティ アーキテクチャも進化させる必要があります。新たなテクノロジの導入により、セキュリティ戦略で対処すべき新たな攻撃対象領域が発生しています。これらの潜在的リスクのシナリオについて、次のセクションで説明します。

図 2：4G から 5G へのネットワーク アーキテクチャの進化



出典：『*Interpretation of Figure from 5G Americas, The Evolution of Security in 5G*』

戦略での考慮事項 1：セキュリティ パフォーマンスとセキュリティ運用の拡大が必要

4G と同様に、5G も一度に刷新できるものではありません。5G は 4G と共存しながら進化し、今後 10 年間は論理的発展の段階が続きます。そのため、4G は今後も長年にわたり存続するでしょう。

その証拠に、GSMA は 4G が 2025 年にも依然としてグローバル接続の 59% を占めると予測しています。* 5G の導入の大半は 5G NSA（非スタンドアロン）アーキテクチャで始まり、 5G サービスの稼働を迅速に開始するために 5G RAN と既存の 4G コアが組み合わせて使用されます。

そのため、サービス プロバイダの 5G セキュリティ戦略では、まず既存の 4G ネットワーク セキュリティを評価して、4G と 5G の両方で実装を一貫させる必要があります。こうした評価の論理的な開始点は、4G ネットワーク セキュリティのパフォーマンスが、5G NSA からのネットワーク容量の増加に対応できるかどうかを判断することです。ほとんどの場合、セキュリティをアップグレードして、物理インフラストラクチャをスケール アップし、仮想インフラストラクチャをスケール アップおよびスケール アウトする必要があります。

こうしたパフォーマンス強化に投資しなければ、セキュリティがネットワーク パフォーマンス全体のボトルネックになってしまいます。製品レベルでは、スループット、接続規模、セッション確立率などのセキュリティ パフォーマンスを、3G/4G Gi/SGi ファイアウォール、SEG（セキュリティ ゲートウェイ）、Gp/S8 ローミング ファイアウォールなどの最新モバイル セキュリティ導入事例に向けて評価する必要があります。

検証が必要な事例としてほかに、DDoS（分散サービス拒否）攻撃からの保護があります。IoT の進歩に伴い、接続デバイスはその並外れた接続規模と一般に制限されたセキュリティ機能によって急速にハッカーの絶好の標的となりつつあります。

たとえば、2016 年に Mirai IoT ボットネットは世界中で約 10 万台の接続デバイスのセキュリティを侵害しました。それらのデバイスは、DNS（ドメイン名システム）サービス プロバイダの Dyn に対して 1.2 Tbps のピーク容量で DDoS 攻撃を開始し、4 時間を超えるサービスの中断とダウンタイムを発生させました。しかし、Mirai はまだ序の口にすぎませんでした。それ以降、JenX、Hajime、Satori、Reaper などの変種が登場し、ますます巧妙化して防御が困難になっています。

残念ながら、5G の導入によって利用可能な帯域幅を拡大することで問題が悪化し、より堅牢なネットワークでもセキュリティ侵害を受けた接続デバイスから攻撃トラフィックが生成されます。高ボリュームの DDoS 攻撃は頻度、規模、巧妙さが増し、アウトオブバンドのスクラビング センターや手動操作といった従来の防御手段は不適切で非常に高コストなものになっています。

攻撃防御コストはデータ トラフィックのボリュームと直接関連しているため、高ボリュームの攻撃を受けた場合、疑わしいトラフィックをスクラビング センターにリダイレクトすると、遅延が長くなり、コストがかさみます。サービス プロバイダは、インテリジェントでコスト効率に優れた検知および攻撃防御プロセスを自動化するテレメトリ、機械分析、ネットワークベース攻撃防御を取り入れた最新の DDoS 防御アプローチの採用を検討する必要があります。

---

* GSM Association『*The Mobile Economy 2019*』

パフォーマンスに加え、セキュリティ運用は PNF（物理ネットワーク機能）と VNF（仮想ネットワーク機能）により拡張して分散型の Telco クラウド環境に対応する必要があります。そのためには、物理ドメインと仮想ドメインの両方を管理して両ドメインの統合ビューを提供する統合セキュリティ管理システムが必要です。つまり、セキュリティ管理ではシステム全体にわたる包括的な可視化が必要になります。この戦略のもう 1 つの構成要素は、プログラム可能なセキュリティ ポリシーを通じて自動ポリシー オーケストレーションを活用し、サービスレベル契約を満たす信頼性の高いセキュアなネットワークを確立することです。

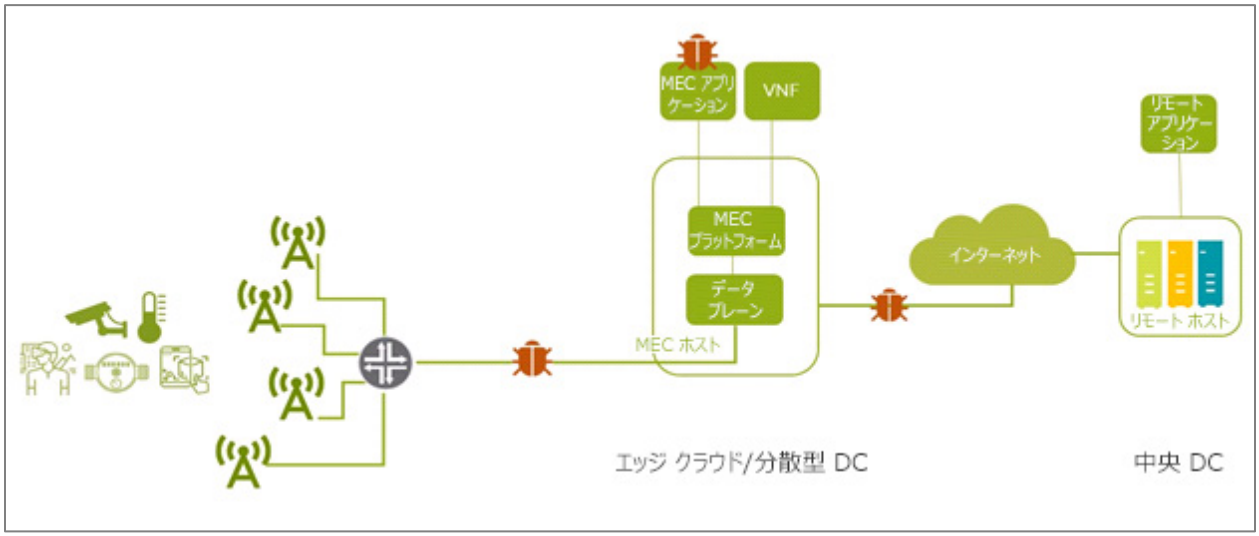
さらに、5G インフラストラクチャには異種混合性と複雑さがあることから、複数のドメインの複数のレベル（スライス、サービス、リソースとの関連付けなど）でセキュリティを適用する必要があります。そのため、セキュリティの自動化とオーケストレーションはサービス プロバイダがセキュリティ運用上の課題に先手を打つ上で不可欠なものとなっています。

戦略での考慮事項 2：ネットワーク アーキテクチャの進化と新たな実現技術により新たな攻撃対象領域が発生

エッジ コンピューティングは、クラウド コンピューティングの進化版です。アプリケーションのホスティングとデータ処理を中央データ センターからモバイル アプリケーションに近いネットワーク エッジに移動させるものです。エッジ コンピューティングは、5G の厳しい要件、特に低遅延と帯域幅の効率化が重要な導入事例に対応するための柱です。

ETSI で MEC（マルチアクセス エッジ コンピューティング）を扱っている ISG（Industry Specification Group）は、MEC の技術標準を規定しました。この技術標準は、5G NSA、分散コンピューティング、ネットワーク機器/コンピューティング サーバー仮想化を始めとした多種多様なテクノロジに対応します。これらのテクノロジはすべて、サービス プロバイダが分散型アプリケーションを導入できるオープン エコシステムを採用しています。ただ残念なことに、**図 3** に示す MEC 環境の異種混在性と多様性により、MEC システム全体にとって大きな脅威となり得る悪意のある攻撃やプライバシー侵害のさまざまな新しいベクトルが発生しています。

図 3：MEC の攻撃対象領域



出典：ジュニパーネットワークス

好ましい導入モデルは、VNF と同じ物理プラットフォーム上で MEC アプリケーションを実行することです。これらの MEC アプリケーションがモバイル サービス プロバイダによって管理されていないサードパーティ アプリケーションである場合は、それらの MEC アプリケーションによって、ネットワーク機能に必要なリソースが使い果たされるという懸念が生じます。

また、アプリケーションの設計が不完全だと、分散されたデータ センターに侵入するための攻撃ベクトルをハッカーに提供してしまい、そのプラットフォーム上で実行されているネットワーク機能に影響が及ぶおそれがあります。同様に、攻撃者側も同じ手段を達成するための悪意のあるアプリケーションを挿入する可能性があります。機密性の高いセキュリティ アセットのセキュリティがエッジの仮想化された機能で侵害されると、攻撃者はそれらのアセットを不正に再利用して接続したり、なりすましや傍受、データ操作などの攻撃を実行したりする可能性があります。

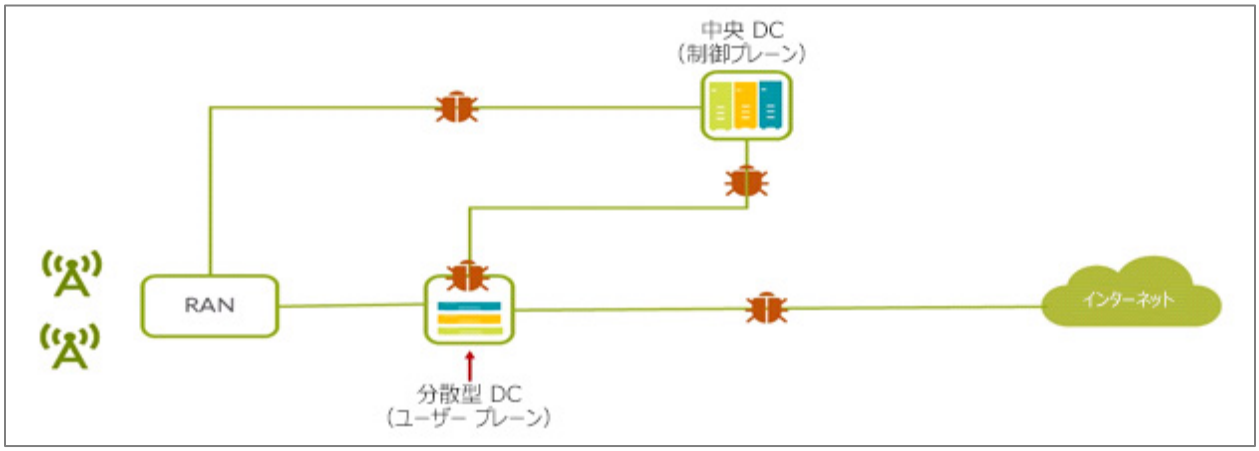
こうした攻撃方法は新しいものとは限りません。しかし、MEC アーキテクチャが新しいことから、セキュリティ問題のリスクと重大さが十分に理解されていない可能性があります。そのため、ベンダーを選定するときや大規模な商用エッジ クラウドを展開する前に、サービス プロバイダはセキュリティ ソリューションが初期導入時のさまざまな脅威ベクトルに対応できる柔軟性を備えていることを確認する必要があります。

分散されたコア攻撃対象領域

4G EPC（Evolved Packet Core）への CUPS の導入は、5G コア アーキテクチャへの進化に向けた重要なステップです。CUPS は 3GPP Release 14 規格の一部となっています。既存の 4G EPC を用いてネットワーク上にユーザー プレーン リソースを分散させることができるためです。これを、5G コア ネットワークの新しいサービスベース アーキテクチャを最終的に導入する前に実行することができます。CUPS を使用すれば、事業者は EPC ノードの制御プレーン リソースとユーザー プレーン リソースを単独で見つけて拡張できます。これは、動画のような広帯域アプリケーションで適切に機能します。コアのユーザー プレーンはエンド ユーザーの近くにあるため、事業者は中央データ センターまではるばるトラフィックをバックホールする必要はありません。そのため、遅延を短縮し、バックホール コストを削減することができます。

CUPS は正確には 5G 機能ではありませんが、5G ネットワークの導入に伴う新たな信頼境界線や脅威対象領域に準拠しています。つまり、**図 4** に示すように、Sx や SGi などのどのインターフェイスも DoS 攻撃や DDoS 攻撃の標的になり得るということです。

図 4：分散されたコア攻撃対象領域



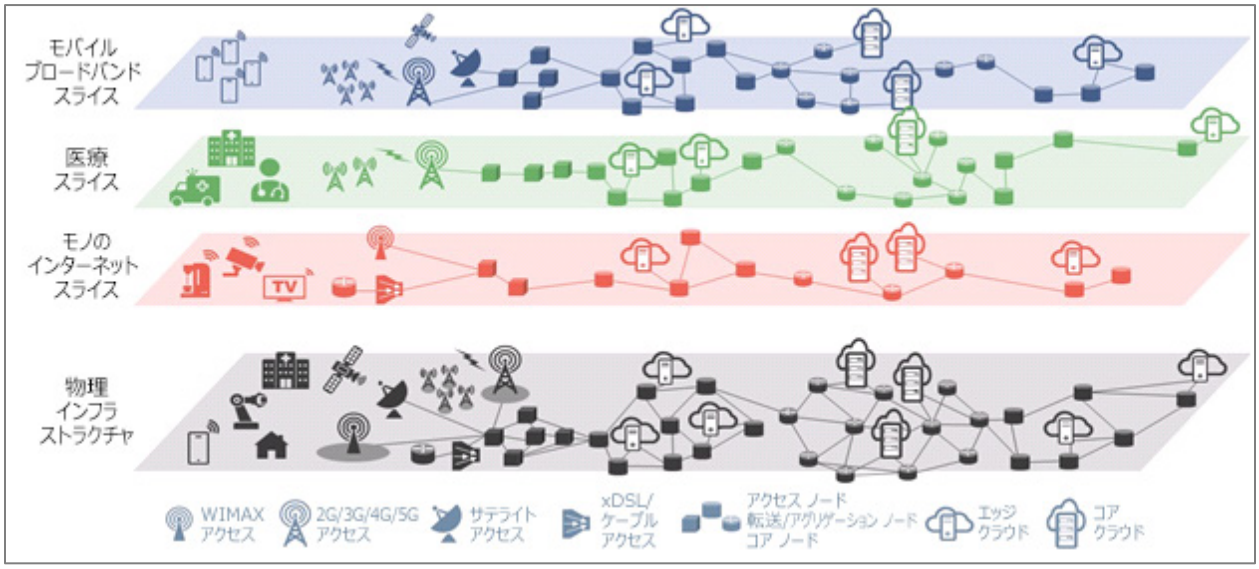
出典：ジュニパーネットワークス

ネットワーク スライシングの攻撃対象領域

ネットワーク スライシングは、共有物理ネットワーク インフラストラクチャ上で複数の論理ネットワークを実行できる特定の仮想化形式です。ネットワーク スライシングを使用すれば、モバイル サービス プロバイダは、ネットワーク リソースをパーティション化して、多種多様なユーザーによって異なるパフォーマンス要件や機能要件が存在するさまざまな導入事例に対応できます。さらに、1 つの物理インフラストラクチャ上でこうした導入事例を多重化することもできます。

たとえば、**図 5** に示すように、業種別 IoT や医療業界固有のアプリケーションといったさまざまなサービスに対応する個別のアプリケーション スライス タイプを作成できます。

図 5：5G ネットワーク スライシング



出典：*IEEE『Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges』*

ネットワーク スライシングは 5G ネットワークで重要な役割を果たすと見込まれています。5G が多数の導入事例と新サービスに対応するためです。こうした新たな導入事例とサービスは機能面でネットワークにさまざまな要件を生じさせます。パフォーマンス要件は、ITU 5G サービス階層（**図 1** を参照）に示したように、スループット、サービス品質、遅延、セキュリティの点で大きく異なる可能性があります。

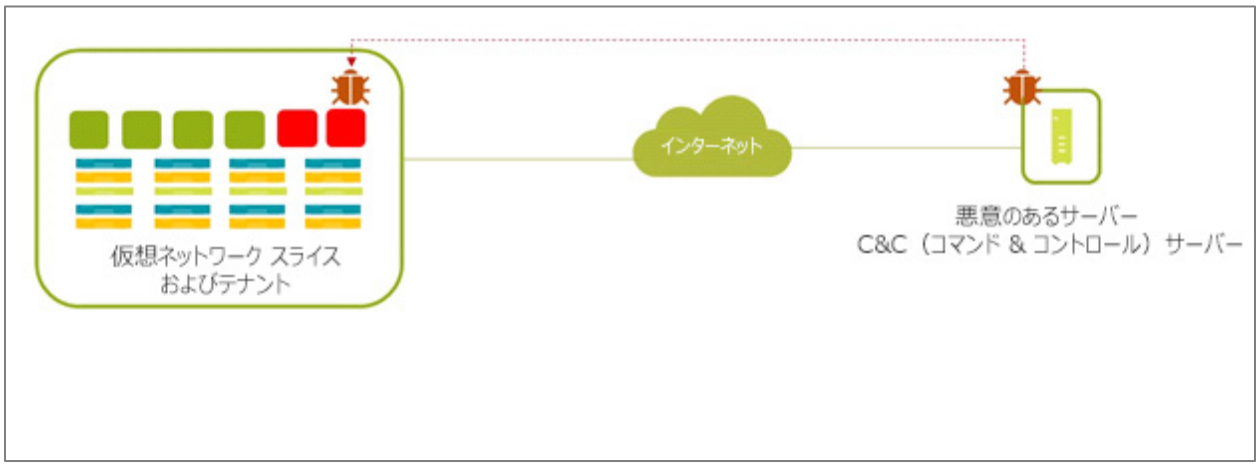
5G でよく挙げられる例の 1 つは、物理ネットワークを共有して、大量の IoT アプリケーション、MBB（モバイル ブロードバンド）アプリケーション、URLLC アプリケーションを同時実行することです。たとえば、IoT は通常、非常に多くのデバイスをサポートしますが、各デバイスのスループットは非常に低い場合があります。それとは対照的に、MBB のサポートするデバイスははるかに少ないものの、各デバイスは超広帯域のコンテンツを送受信します。

こうした異なるサービス スライス パフォーマンス プロファイルは、セキュリティ プロトコルの選択とポリシーの実施に直接影響します。例として、あるスライス内のサービスに非常に長いバッテリー駆動時間が必要な場合、それは何らかの形でセキュリティ プロトコルに制約を課します（再認証の実行頻度など）。別の例では、あるスライス内のサービスにプライバシー保護が必要な場合、徹底したセキュリティ手順が必要になります（一時 ID の頻繁な再割り当てなど）。

さらに、サービス プロバイダはそれらのスライスをどのようにして適切に相互分離するかを考える必要があります。主なセキュリティ上の懸念事項の 1 つは、セキュリティの「低い」スライスを経由して幅広いネットワークへのアクセスを可能にする攻撃者です。

図 6 に示すように、攻撃シナリオの中には、あるスライスのリソースを使い果たす攻撃者が関与するものがあります。そうすることで、攻撃者は複数のスライスに共通するリソースを使い果たし、他のスライスで DoS やサービス低下を生じさせる可能性があります。

図 6：スライス枯渇攻撃シナリオ



出典：ジュニパーネットワークス

戦略での考慮事項 3：収益の差別化要因や成功要因としてのセキュリティ

サービス プロバイダの 5G セキュリティ戦略における最終的な考慮事項は、セキュリティを活用してネットワークの導入を差別化および収益化する方法です。

ネットワーク スライシングなどの 5G 機能により、IoT アプリケーションへの依存度が高い製造業や運輸業など多くのセグメントで大幅な増益が促進されます。消費者とは異なり、そうした業界の多くには厳しいセキュリティ要件が存在します。そのため、これまでは多くの業界が独自のプライベート ネットワークを構築して接続していました。こうした垂直市場への 5G 製品/サービスの導入を成功させるには、サービス プロバイダは顧客ニーズに対応して懸念を解消するセキュリティ機能を重視する必要があります。

IoT については、サービス プロバイダには企業での IoT の検討に参加する有効な手段があります。それは、接続です。IoT 接続の可能性自体もかなり大きなものですが、サービス プロバイダはほかの多くのチャンスをフルに活かすことができます。たとえば、セキュリティです。セキュリティは、IoT を導入する企業にとって、依然として最大の懸念事項であるとともに、技術的な障壁でもあります。

こうした業界の企業の多くは、アプリケーションのセキュリティを確保するための人材を社内で用意できず、独自のセキュリティ要件への支援をサービス プロバイダに依頼します。これを重要なステップとして、サービス プロバイダは、基本的な接続サービスの提供の域を超え、魅力的なサービスに IoT の接続とセキュリティを提供できるように進化を遂げられます。

セキュリティが収益の成功要因として位置付けられるもう 1 つの領域は、5G SECaaS（Security as a Service）です。5G の魅力の大半は、さまざまな業界が共有インフラストラクチャを使用することでコスト効率の向上を実現できることにあります。依然として自身でセキュリティを管理したい業界もあれば、一部のセキュリティ サービスを 5G ネットワークにアウトソーシングしてさらなるコスト削減を果たすことを選択している業界もあります。こうしたサービスには、ネットワークでのポリシーの適用（ファイアウォール、デバイス アクセス コントロールなど）や、ネットワークが提供する認証/ジオロケーション アサーションの利用があります。

Software-Defined Networking と仮想化テクノロジにより、アプリケーション別やユーザー別のセキュリティ設定の導入が可能になっています。5G サービス プロバイダは、アプリケーション別の接続を相互に分離させることで、付加価値サービスとしてのモニタリング分析やディープ パケット インスペクションなどのセキュリティ機能をカスタマイズされたユーザーごとに提供できます。

同様に、サービス プロバイダが MEC やエッジ クラウド環境でサードパーティ アプリケーションをホストするシナリオでは、そうしたアプリケーションにセキュリティ/保証サービスを提供するチャンスがあります。提供できるサービスの例として、インストール時、アップグレード時、サーバー再起動時におけるアプリケーションの整合性保証チェックの実行があります。ほかに、ユーザー識別用の信頼性の高いサードパーティ製 MEC アプリケーションへのセキュリティ サービス API の公開などもあります。

まとめ

セキュリティは、5G サービスの提供を成功させるために不可欠な要素です。サービス プロバイダは、セキュリティ戦略を 5G の進化ロードマップに欠かせないものとして入念に計画する必要があります。

現在のモバイル ネットワーク セキュリティのパフォーマンスと運用は、ボトルネックとなるのではなく、5G の要件に対応してスケール アップおよびスケール アウト可能になる必要があります。さらに、エッジ コンピューティング、CUPS/分散コア、ネットワーク スライシングが新たな攻撃対象領域を発生させるため、サービス プロバイダは脅威を防御できる適切なセキュリティ対策を実施する必要があります。5G と IoT の時代のセキュリティは、単なる責任とみなすべきではありません。サービス プロバイダはセキュリティを重要なサービス差別化要因と不可欠な収益創出要因として位置付けることを検討すべきです。