5G サイバーセキュリティ ガイダンス

導入および範囲

5G をベースにした次世代通信サービスは、移動系超高速ブロードバンド、IoT 機器等の多数同時接続、超高信頼・低遅延通信を可能にし、広範囲をカバーする固定無線アクセスからコネクテッド インダストリーズやスマートシティまで、すべてを実現します。同時に、5G 固有のサービスベースのアーキテクチャにより、ネットワーク事業者はインフラストラクチャ管理のシンプル化、サービス提供の自動化、カスタマイズされた企業向けサービスから新たな収益の流れの創出が可能になります。5G は、スマートネーションの構築と経済成長の強化の基盤となっていますが、その反面でこの基盤は、5G のアーキテクチャ特性に関するリスクを伴い、大きな攻撃対象領域が開放されるユースケースが予想されています[1]。政府と業界パートナーが、重要なサービスの保護と 5G の社会的および経済的な全潜在能力の実現を目的として、5G インフラストラクチャにサイバーセキュリティ防御を設計することが非常に重要です。

このホワイトペーパーでは、事業者のコア ネットワーク インフラストラクチャに対する 5G のサイバーセキュリティリスクについて高レベルのインサイトを提供し、サイバーセキュリティ脅威に対抗するための 5G の強化に関する 6 つの重要な推奨事項を示します。これらの推奨事項は、5G 標準で定義された固有のセキュリティサービスに基づいて構築するセキュリティアーキテクチャ戦略を示しています。本ホワイトペーパーではユーザアクセス環境内のセキュリティには特に触れていませんが、5G サービスを活用する企業、産業、IoT ネットワークを強化するためのベストプラクティスとして、ガイダンスの多くを適用することができます。

5G の概要

3GPP（3rd Generation Partnership Project）内のワーキンググループで指定されている 5G クラウドネイティブ アーキテクチャは、次世代モバイルサービスのコア機能要素とインターフェイスを標準化します。5G は、分散環境で実行されるソフトウェア定義型ネットワーク（SDN）サービスおよび仮想ネットワーク機能（VNF）を構築したソフトウェア中心のアーキテクチャです。このアプローチにより、ユーザとコントロールプレーン機能の分離が促進され、5G キャリアは低い運用コストで、さらなるサービスの自動化、俊敏性、拡張性を実現できます。これに対し、4G は専用のハードウェア プラットフォームに接続されたモノリシック アプリケーションに基づいており、事業者がサービスを個別に拡張したりカスタマイズしたりすることが困難です。

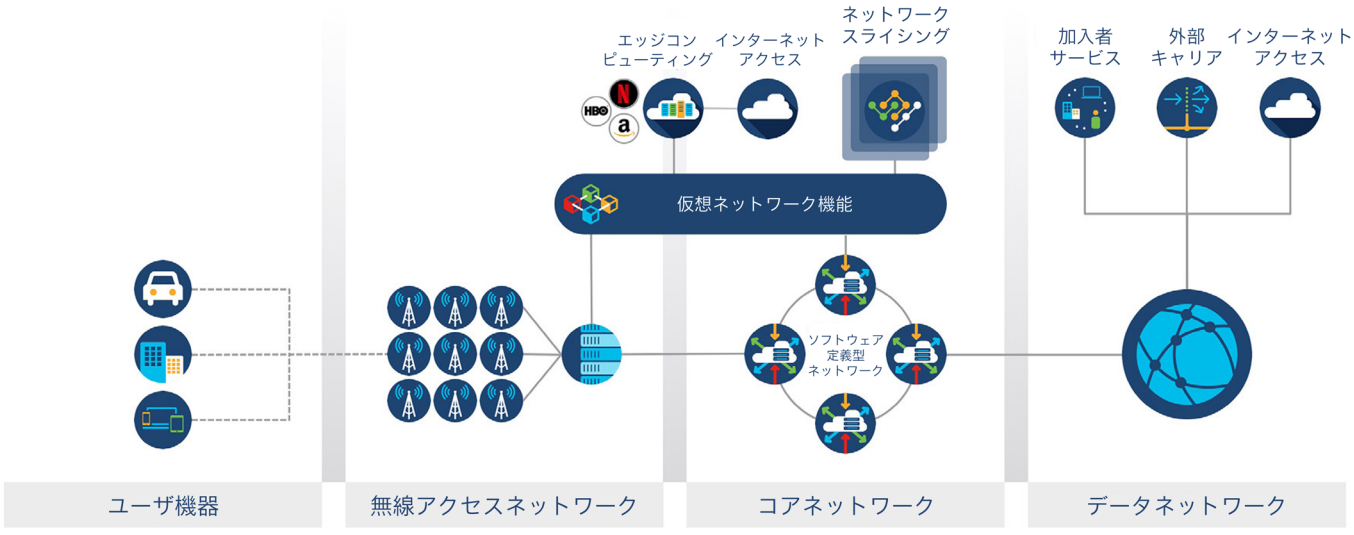
論理的な観点から見ると、5G アーキテクチャは、**ユーザ機器**、**無線アクセスネットワーク**、**コアネットワーク**、**データネットワーク**の 4 つの領域に分かれています。最も著しい 5G の進化が見られるのは、無線アクセスネットワークとコアネットワークです。無線アクセスネットワークは、4G の最大 20 倍の速さとユーザが高密度に存在した場合においても低遅延を提供する新無線技術を活用しています。コアネットワークは、分散型の柔軟で大容量なサービスバックボーンを提供し、これによってネットワークスライシング [2] やエッジコンピューティング [3] などの新たな 5G 機能を可能にします。つまり 5G は、モバイル ブロードバンド アクセスとパフォーマンスを拡大するプラットフォームを事業者に提供します。同時に、ネットワークを最適化して、より優れたコンシューマサービスを提供し、製造、物流、農業などで新しい企業向けサービスを実現します。

5G アーキテクチャ

新たなサービス
- 移動系超高速ブロードバンド
- 超高信頼・低遅延
- 大規模な Internet of Things（IoT）

次世代無線
- ピーク時 20Gbps スループット
- 低帯域から mmWave スペクトラムへ
- マルチ入力、マルチ出力/ビーム フォーミング

仮想コア
- クラウドネイティブ アーキテクチャ
- ネットワークスライシング
- エッジコンピューティング サービス



5G ネットワークアーキテクチャ

5G サイバーセキュリティリスク

5G は、現時点で既存する通信およびエンタープライズ ネットワークで発見されたものと同じサイバーセキュリティリスクの多くの影響を受けやすくなっています。さらに 5G は、技術、関係者、運用の複雑なエコシステムが原因で、コアネットワークサービスに対する新たな攻撃方法のリスクにさらされています。これには次のようなものがあります。

- **サービスベースのアーキテクチャ**：5G は、通信サービスをどのように構築し提供するかという点において、大きな変革を示しています。基本的に 5G アーキテクチャは、分解、仮想化、分散ネットワーク機能に基づいています。これらの機能は、コンテナ化されたアプリケーション、オープンインターフェイス、オーケストレーション プラットフォームを利用し、サービスの提供を調整します。これらのインフラストラクチャの抽象化により新たな攻撃ポイントがさらされ、高度な仮想環境でのセキュリティ制御の実装と管理における課題が生じます。

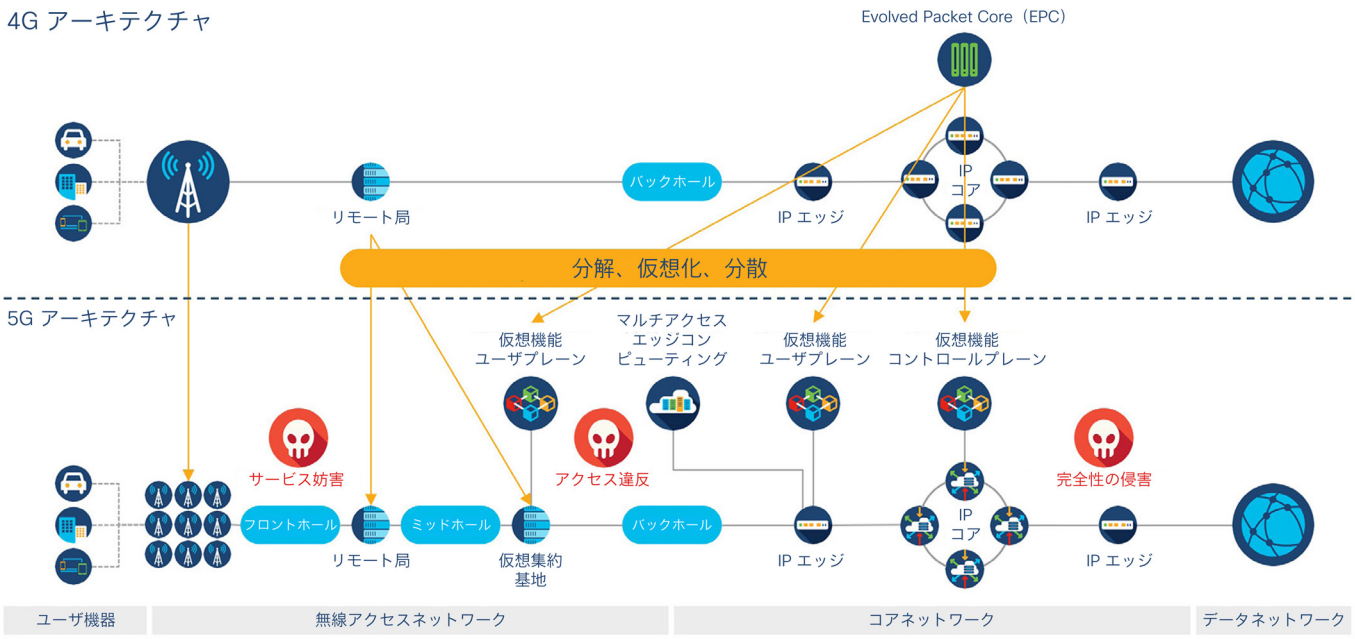
- **API ベースの通信**：5G サービスベースのアーキテクチャは、アプリケーション プログラミング インターフェイス（API）を活用して、サービス機能間の通信を可能にし、インフラストラクチャの展開、設定、管理を最適化します。不十分なコード化または安全でない API によりコアサービスが攻撃にさらされ、5G ネットワーク全体がリスクにさらされる可能性があります。

- **企業、産業、IoT サービス**:5G は、従来の消費者向けスマートフォンから高度なエンタープライズサービスへの移行を示しています。5G は、従業員のモビリティ向上、自動化、および無数の新たなアプリケーションなどを実現する企業、産業、IoT のユースケースに適用されることが期待されます。これらの環境に 5G を組み込むには、エンドユーザネットワークと 5G サービスインターフェイスとの間において深いレベルでの統合が必要となり、企業のオーナー（特に、重要な情報インフラストラクチャ事業者）と 5G キャリアの両方が新たなリスクにさらされます。最終的にネットワークの中断、機密データの盗難や改ざんといった攻撃が成功すれば、これまでの世代よりもはるかに大きな経済的および社会的影響を及ぼすかもしれません。たとえば、産業用機器および IoT 機器は多くの場合、レガシー機器に依存し、適切なサイバーセキュリティ保護が欠如しているため、特に脆弱です。脆弱な機器に対する攻撃は、実社会への影響力を持つ 5G ネットワークに依存する重要サービスに影響を及ぼす可能性があります。反対に、乗っ取られた産業用機器または IoT 機器の大規模な集合体を操作して、5G インフラストラクチャに対する攻撃を開始させ、すべてのユーザのサービスを中断することが可能です。

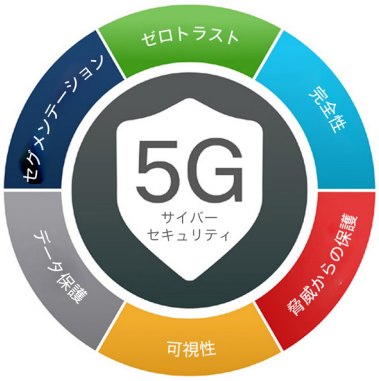
- **マルチアクセス エッジコンピューティング**：高速、超高信頼性、低遅延のサービスを促進するために、5G はエッジコンピューティングを採用しており、パフォーマンスを要求されるアプリケーションをエンドユーザの近くに配置します。実際には、事業者は、モバイル無線アクセスノードの近く、もしくは企業の顧客データセンターやサードパーティのクラウド環境内にある仮想化データセンターにおける独自のインフラストラクチャ内にユーザ向けのアプリケーションを配置できます。この分散型アプローチにより、運用上の境界が曖昧になり、セキュリティ対策の複雑さが増す可能性があります。さらに、エッジコンピューティングは、5G インフラストラクチャと統合したアプリケーションサービスに対する新たな攻撃の機会につながり、さらなる攻撃経路を生み出し、攻撃の脅威をコア 5G サービスへ向かわせる可能性があります。

サイバーセキュリティのリスクは、脅威の性質に影響を受けます。脅威は、攻撃者がシステムの脆弱性や弱点を侵害する方法によって定義され、システムの機密性、完全性、可用性に影響を与えます。5G インフラストラクチャにはさまざまな脅威が存在しますが、その影響に応じて、3 つの広範なカテゴリに分類できます。

- **サービス妨害**：仮想的または物理的な方法によってサービス停止を引き起こす攻撃。例として、ハードウェアの破壊、無線信号の妨害、トラフィックフラッディングなどがあります。
- **アクセス違反**：不正なシステムアクセス、データ操作、またはデータ侵害につながる攻撃。例として、システム設定への悪意のある変更、ソフトウェアの脆弱性のエクスプロイト、通信ハイジャック、および機密データの漏えいなどがあります。
- **完全性の侵害**:ハードウェア、ソフトウェア、通信、および操作の改ざんによってインフラストラクチャの完全性に影響を与える攻撃。例として、システムデバイスにおける悪意のあるハードウェアコンポーネントの移植、オペレーティング システム コードの変更、データの修正、組織のセキュリティポリシーの回避などがあります。



4G と 5G のアーキテクチャの違いおよび脅威の影響



5G のサイバーセキュリティリスクを軽減する 6 つの推奨事項

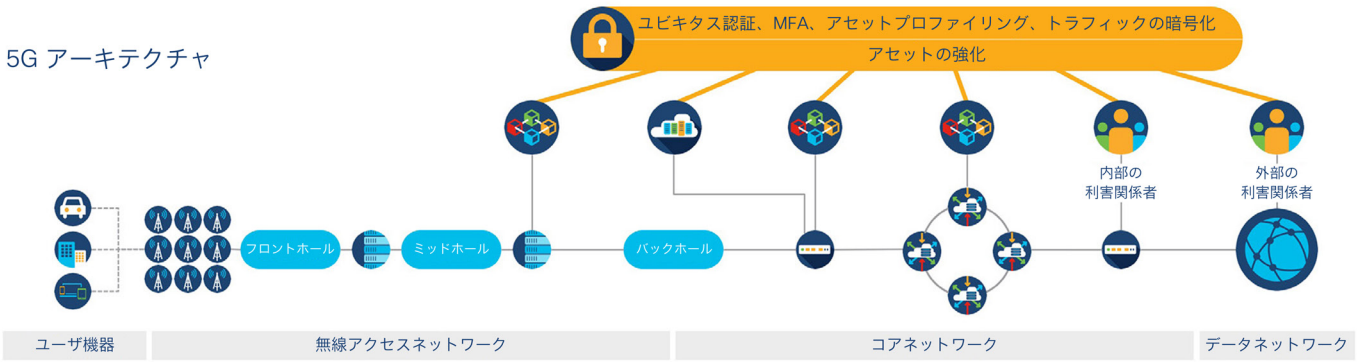
5G は、現代のエンタープライズ ネットワークとクラウドサービスの構築に使用されるものと同じテクノロジーとアーキテクチャアプローチの多くを活用しています。しかし、これまでのいくつかの 5G ネットワークの導入では、確立されたサイバーセキュリティのベストプラクティスとアーキテクチャパターンはまだ出現していません。そのため、5G の導入は、企業およびクラウド環境で採用されている成熟したサイバーセキュリティ標準に基づいて構築する必要があります。たとえばNIST サイバーセキュリティ フレームワークや ISO 情報セキュリティ マネジメント システムなどです。また事業者は、信頼できる製品を導入して使用するために、国際的に認められた製品テスト、保証、認定制度（コモンクライテリアなど）を活用する必要があります。セキュリティベースラインとしての国際標準および 3GPP 標準により、5G 事業者は、上記のリスクに対応するためのアーキテクチャ戦略の一環として、攻撃対象領域の削減、脅威の継続的な軽減、データとプライバシーの保護を目的とする、サイバーセキュリティに関する次の 6 つの重要な推奨事項を採用する必要があります。

ゼロトラスト

5G インフラストラクチャを信頼できない環境[4]として扱い、アクセスを許可する前に、ネットワーク内外のすべての領域（ワークフォース、職場、ワークロード[5]）における全アセット間のインタラクションを明示的に認証および許可して保護し、必要最小限に制限します。アセットのセキュリティ状況（Security Posture）を継続的にモニタし、それに応じてアクセス権を調整します。主な機能は次のとおりです。

- **アセットの強化**：ローカルアクセス制御、設定、サービスをロックダウンするベストプラクティスに従って、各アセットの攻撃対象領域を削減します。
- **ユビキタス認証および承認**：ユーザ ID、デバイスタイプ、地理的なロケーションやネットワーク アクセス ロケーションを含むコンテキスト要因を考慮した、すべてのアセット間のアクセスを認証および承認します。マシンデバイスやアプリケーション ワークロードなどの非ユーザアセットでは、証明書ベースの認証と認可（権限付与）を活用できます。
- **多要素認証（MFA）**：複数の強力なメソッドを使用し、デバイスタイプ、地理的なロケーションやネットワークロケーションを含むコンテキスト要因を考慮した、アセット（アカウント名とパスワードとワンタイムトークンなど）へのユーザアクセスを認証および認可します。
- **アセットプロファイリング**：すべてのアセットのセキュリティ状況（Security Posture）を検証して追跡し、評価されたリスクに基づいてアクセスを許可または拒否します。
- **トラフィックの暗号化**：強力な暗号化技術を使用して、すべてのアセット間の通信を保護します。

5G アーキテクチャ

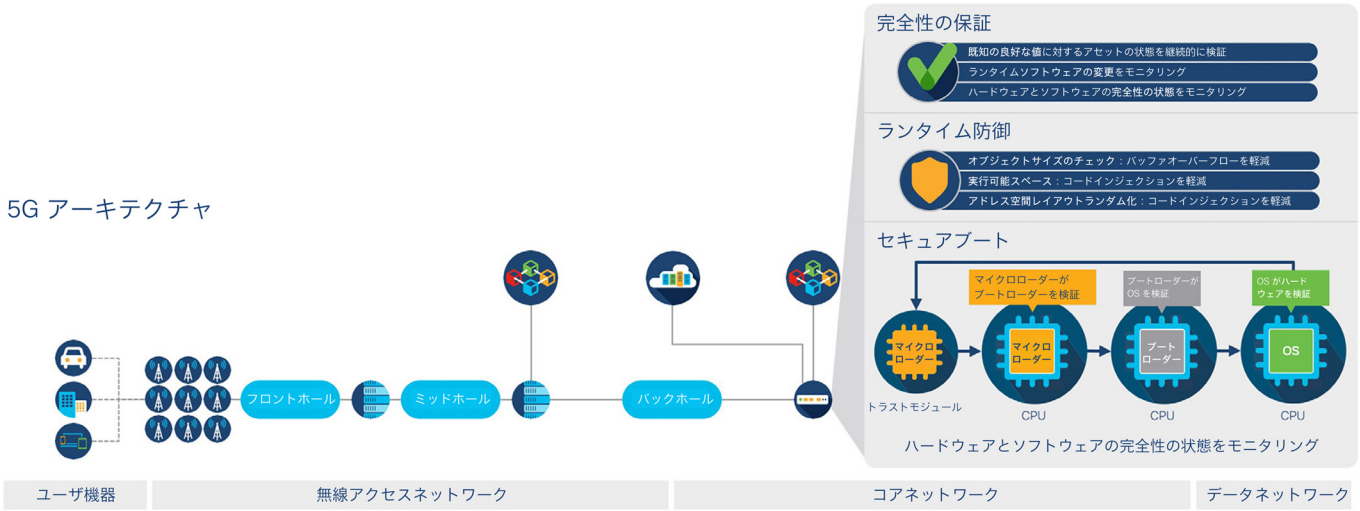


ゼロトラスト環境

完全性

ベンダーのサプライチェーンのセキュリティとセキュアな開発プラクティスを検証し、信頼できる製品を採用します。ハードウェア、ソフトウェア、運用の完全性を継続的にモニタして、インフラストラクチャとサービスの改ざんを検出し、軽減します。主な機能は次のとおりです。

- **ベンダーのセキュリティ評価**：ベンダーのサプライチェーンのセキュリティプログラム強度を検証し、製品開発および管理のライフサイクル、脆弱性とデータ漏えい、情報セキュリティプラクティス全体を保護します。また、ベンダーが管理する施設でベンダーの設計と実装を直接評価してテストすることで、製品のセキュリティを検証するのも賢明な方法です。
- **セキュアブートとランタイム**：アセットが、ハードウェアのトラストアンカーやソフトウェアイメージ署名といった改ざん対策技術に基づいたセキュアなブートプロセスを活用するようにして、ハードウェアおよびソフトウェアコンポーネントの信頼性と完全性を確保します。アセットはランタイム防御を採用して、実行中のプロセスの完全性を確保し、バッファオーバーフローやコードインジェクションなどのメモリベースの攻撃を軽減する必要があります。
- **完全性の確保**：ハードウェアとソフトウェアを継続的にモニタして、完全性を検証します。迅速な修正措置を可能にする検証可能な証拠に基づいて、改ざんの問題を検出します。
- **運用の完全性**：適切なポリシー、ガバナンス、および運用プラクティスを実装して、内部者による不正使用を検出し防止します。

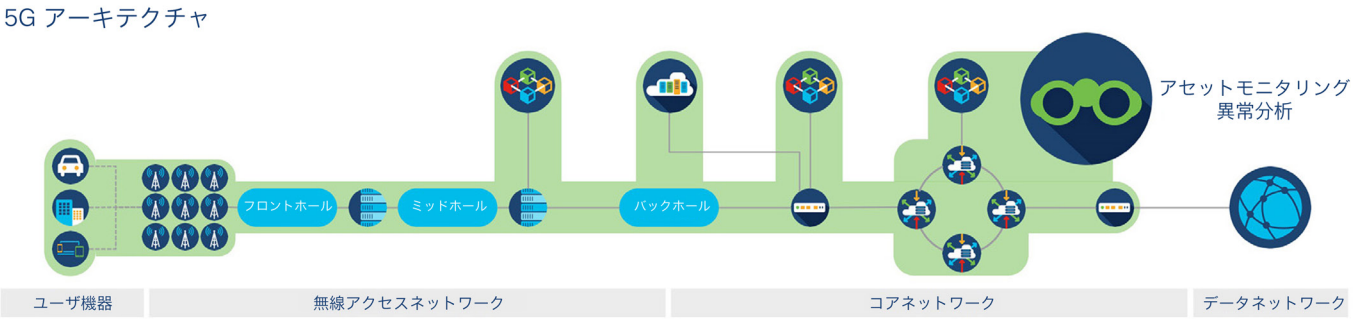


アセットの完全性の保護

可視性

インフラストラクチャ全体で完全な可視性を実現して、すべてのアセットを特定し、アセットのセキュリティログ、異常な動作、通信パターンを継続的にモニタして潜在的なセキュリティリスクを明らかにします。主な機能は次のとおりです。

- **アセットのモニタリング**：エンドポイント、ネットワーク、サーバのデバイスおよびアプリケーションなどの全アセットについて、セキュリティの追跡、ロギング、テレメトリ、一元化されたモニタリングを可能にします。
- **異常分析**：機械学習システムを活用して、アセットの異常な動作または通信パターンをモニタし、検出します。脅威検査のネットワークトラフィックの暗号解読は、許容できない遅延をもたらしたり、プライバシー要件に違反したりする可能性があるため、暗号化されたトラフィックフローの異常を検出するように機械学習の手法を調整する必要があります。



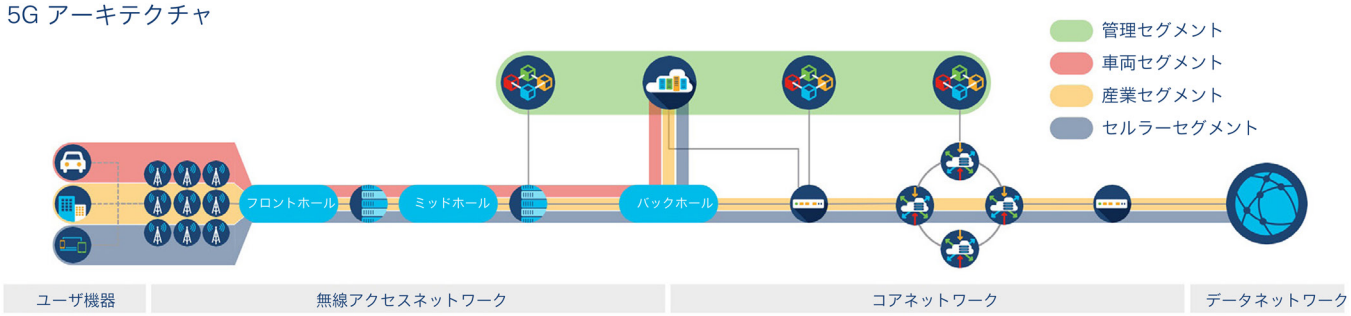
インフラストラクチャ全体の可視性

セグメンテーション

エンドツーエンドのセグメンテーションを実装してアセットグループを区分し、攻撃対象領域を削減して、侵害の影響を制限します。主な機能は次のとおりです。

- **ソフトウェア定義型セグメンテーション**：ネットワーク統合アクセス制御およびポリシーサービスを活用する論理的なセキュリティグループにアセットを配置して、グループ間の通信フローを制限します。5G ネットワークスライシング機能は、エンドツーエンドのセグメンテーション戦略のコンポーネントとして活用する必要があります。
- **ネットワークおよびアプリケーション ファイアウォール**：ファイアウォールゲートウェイを実装して、重要なアセットまたはアセットグループ間のトランザクションを検査して、明示的に許可または拒否します。

5G アーキテクチャ

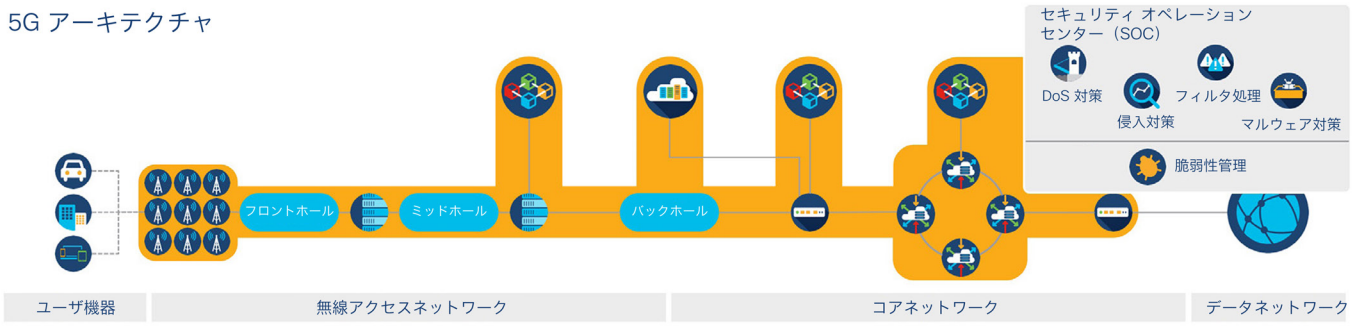


ソフトウェア定義型セグメンテーション

脅威からの保護

機械学習機能に支えられた防御型のセキュリティ対策と継続的なモニタリングを実施し、インシデント対応業務を確立して、アセットに対する脅威を検出し軽減します。主な機能は次のとおりです。

- **脆弱性管理**：国際的に承認された標準と、協調的な脆弱性の開示と処理におけるベストプラクティスを採用し、セキュリティの脆弱性（ソフトウェアのパッチ適用など）を適切なタイミングで効果的に特定、軽減、および修復します。
- **サービス妨害防御システム**：ネットワークトラフィックをモニタして、ネットワークフラッディング攻撃を検出し軽減します。
- **侵入検知および侵入防止システム**：ネットワークトラフィックをモニタして、不正アクセスまたはシステムの脆弱性を悪用する試みを検出し軽減します。
- **悪意のあるトラフィックフィルタリング システム**：ネットワークトラフィックをモニタして、スパムまたは悪意のあるドメインおよび Web サイトとの通信の試みといった悪意のある、もしくは不要なトラフィックをブロックします。
- **マルウェア対策システム**：ネットワークトラフィック、エンドポイント、サーバのデバイスをモニタして、マルウェアファイルまたはマルウェアの実行を検出しブロックします。
- **セキュリティ オペレーション センター (SOC)**: セキュリティ侵害の迅速な検出および軽減を担う、一元化されたセキュリティモニタリング、インシデント対応、脅威インテリジェンス組織を確立しています。セキュリティ運用をシンプル化および合理化する、統合されたサイバーセキュリティ機能および自動化ツールを採用しています。



脅威からの保護サービス

データの保護とプライバシー

前述の推奨事項に記載されている多くの重要な機能を活用し、ポリシー主導型のセキュリティプラクティスおよびセキュリティ対策を実装してデータとプライバシーを保護します。データの保護とプライバシーは、ユーザの権利を保護し、不正なデータアクセスまたはデータ使用からデータを保護するためのポリシー、プラクティス、技術的コントロールの適用を意味します。機密データのアクセスと処理を行うことを保証するために、セキュリティポリシーとセキュリティ対策は、規制要件とベストプラクティスに一致する方法で適用される必要があります。データの保護とプライバシーは、違反または侵害が発生した場合に取られる手順や、該当する法律および規制に従って、被害を封じ込め、影響を受けた当事者に通知するための軽減および回復手順にも対応する必要があります。

まとめ

5G は実装件数が限られていて、不明点の多い発展中のアーキテクチャです。はっきりしているのは、どのような形であっても、サイバーセキュリティは、信頼でき、復元力のある 5G サービスを実現するための基盤となるということです。政府 / 自治体の規制当局およびネットワーク事業者は、サイバーセキュリティのベストプラクティスと機能が、最初から 5G インフラストラクチャおよび運用に設計されていることを保証するために相互に協力する必要があります。イノベーションのペースに合わせて脅威が絶えず進化する中で、ネットワーク事業者は、ゼロトラストという考え方で 5G の構築にアプローチし、インフラストラクチャと運用の完全性を最優先に考え、ネットワーク全体の可視性を確保し、トラフィックフローを適切に区分し、攻撃から継続的に防御し、データ保護とプライバシーをサービスの中核に据えることが非常に重要です。

参考資料

3GPP TS 23.501 リリース 15、2019 年 12 月

3GPP TS 33.501 リリース 15、2018 年 6 月

ENISA「5G ネットワークへの脅威（THREAT LANDSCAPE FOR 5G NETWORKS）」、2019 年 11 月

「5G サイバーセキュリティに関する EU ツールボックス（EU toolbox on 5G Cybersecurity）」、2020 年 1 月（https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468）

NIST「重要インフラのサイバーセキュリティを改善するためのフレームワーク 1.1 版（Framework for Improving Critical Infrastructure Cybersecurity V1.1）」、2018 年 4 月

NIST「SP-800-207 [ドラフト版]：ゼロトラストアーキテクチャ（SP-800-207 [DRAFT] - Zero Trust Architecture）」、2019 年 9 月

NIST「SP 800-190：アプリケーションコンテナ セキュリティ ガイド（SP 800-190 - Application Container Security Guide）」、2017 年 9 月

「5G のセキュリティの進化：モバイル脅威の「スライス」（The Evolution of Security in 5G – A "Slice" of Mobile Threats）」、2019 年 7 月（https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper-07-26-19-FINAL.pdf）

「Cisco NFVI およびオーケストレーション ソリューションによる楽天クラウドプラットフォームの実現（Enabling Rakuten Cloud Platform with Cisco NFVI and Orchestration Solutions）」、2019 年 2 月（https://blogs.cisco.com/sp/enabling-rakuten-cloud-platform-with-cisco-nfvi-and-orchestration-solutions）

「Cisco Security による 5G Core（5GC）および Evolved Packet Core（EPC）の保護（Securing the 5G Core (5GC) and Evolved Packet Core (EPC) with Cisco Security）」、2019 年 3 月（https://www.cisco.com/c/en/us/solutions/collateral/service-provider/service-provider-security-solutions/white-paper-c11-742166.html）

「シスコによる 5G セキュリティイノベーション（5G Security Innovation with Cisco）」、2018 年 6 月（https://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/service-provider-security-solutions/5g-security-innovation-with-cisco-wp.pdf）

注釈

[1] *5G には、新たなユースケースに基づく大きな攻撃対象領域があり、以前のアーキテクチャ（3G や 4G など）とはアーキテクチャ上および運用上の違いがあります。しかし、5G のための 3GPP セキュリティ標準には、このリスクを軽減する特別な機能とメカニズムが含まれています。ベンダーと事業者はすべての 5G 導入に関して、これらの特徴を慎重に考慮する必要があります。*

[2] *ネットワークスライシングにより、共有インフラストラクチャ全体に複数の異なる仮想ネットワークを作成できます。*

[3] *エッジコンピューティングにより、パフォーマンスが要求されるアプリケーションをエンドユーザの近くに配置できます。これについては、このドキュメントの後半で詳しく説明されています。*

[4] *ゼロトラストは、包括的なアクセスセキュリティモデルであり、ネットワーク上の要素間の暗黙的な信頼を前提とすることを意図的に回避します。さまざまな外部の関係者が、管理、メンテナンス、またはモニタリングの目的でインフラストラクチャ コンポーネントまたはサービスにアクセスする必要があるため、これは 5G で特に重要です。たとえば、企業ユーザは、5G スライス管理サービスへのアクセスを選択する必要があります。サードパーティベンダーは、設定またはトラブルシューティングのためにコンポーネントを選択するのにアクセスが必要になります。適切に実装された場合、ゼロトラストは適切な関係者アクセスを提供し、不正使用から 5G サービスを保護します。*

[5] *ワークフォース領域では、アプリケーションへのユーザおよびデバイスアクセスを扱います。ワークプレイスの領域では、ネットワーク全体のユーザおよびデバイス接続を扱います。ワークロード領域では、アプリケーションとサービスとの間の接続を扱います。*