# シスコによる 5G セキュリティ イノベーション

著者：Michael Geller、Pramod Nair

## はじめに

5G は、私たちの生活のほぼあらゆる側面に影響を及ぼします。これは、迅速化、拡大化、あるいは品質の向上に留まらず、5G を活用して、日々の生活のあらゆる場面で利用する、一連のサービスを実現するということです。今こそ、5G の利用に伴うセキュリティへの影響とサイバー リスクのプロファイルを考慮するときです。事業運営リスク、法的リスクおよび評判リスクは、5G トランスポートを提供する企業だけでなく、5G を活用したサービスを提供するすべての企業、国家および個人に関係します。サイバー リスク体制を評価し、今日の問題や、今後発生する課題に対する対処方法について、革新的な考えを実行に移すときがきました。IoT（Internet of Things）サービスの多くは 5G サービスを利用します。5G と IoT の接点から、既存の脅威の対象エリアが拡大し、サイバー リスクの観点から慎重に検討する必要があります。このホワイト ペーパーでは、セキュリティ セーフティネットを構築する際に伴う課題を解決するための革新的な考察を紹介します。セキュリティ セーフティ ネットは、5G ベースのサービスの導入と利用を成功に導くものです。

5G には、新しいエアー インターフェイスの導入と同様に、従来のモバイル ネットワークに新しいアーキテクチャ概念を応用することが求められます。5G モバイル ネットワークは、帯域幅が可変な異種アクセス ネットワーク、かつ柔軟な導入が可能なネットワークとなるように意図して設計されています。モバイル ネットワークの世代交代に関する一般的な理由（例えば、より低コストでのネットワーク テクノロジー導入）は別として、第 5 世代のモバイル ネットワークでは、モバイル サービス プロバイダーが、現在の運用モードとはまったく異なる運用モードをもたらす新しいビジネス モデルに向かって進化できるようにする必要があります。ただ、そのようなネットワークを保護するという観点から、問題点もあります。柔軟性が必要とされることから、ネットワーク上の脅威の対象も増大するのです。

セキュリティは、サービス保証の基盤となります。重要なサービスの提供に使用されるネットワークに対して攻撃者が与える脅威は、巧妙さ、俊敏性、破壊性を増し続けています。アプリケーションの配信に使用されるネットワークは収束を続けているため、脅威の全体的な集約状況を調べるとともに、ドメインごとに脅威と脆弱性を適切に分割することが重要になります。このような例には、従来のサービスとモバイル サービスにおいて、通信事業者のデータセンターとクラウドを活用しつつインフラストラクチャを共有し、運用の効率化およびサービスの提供を実現する、Evolved Packet Core（EPC）があります。シスコのアーキテクチャ革新と、IoT サービスなどの新しいサービス モデルのニーズに応える既存ネットワークの進化により、モバイル エッジ コンピューティングなどのテクノロジーが進化し、広域に分散された安全性の高いデータセンターに新しい要素である可視性と制御が導入され、進化した脅威に対処できるようになります。

コネクテッド アプリケーションを実現する「フル スタック」を適切に保護するために、可視性と制御という 2 つの基本要素が適用されます。可視性とは、キャリア クラウド（通信事業者が提供するクラウド）の情報を参照して、ベースラインとなる適切な動作と相関させ、その基準から偏差を測定する能力のことです。つまり、「計測できなければ管理できない」ということです。可視性の元となるデータは、従来のネットワーク測定（NetFlow、OpenFlow など）によりますが、キャリア クラウドにおけるあらゆる要素からエンド ユーザへのアプリケーションに至るまで、フローのあらゆる側面を測定する必要性によって、収集されるデータや収集場所が変化していきました。新しい可視性の例として、アプリケーション レベルのプローブの使用が挙げられます。これは合成的に生成され、ネットワークを移動するアプリケーションの動作を明確に把握するために利用されます。もう 1 つの例は、ネットワーク トポロジを表すほぼリアルタイムのデータベースを持つ Path Computation Element です。これに対し、DDoS 攻撃の重要なサービス クラスに対する潜在的な緩和対策の影響をプログラム的に判断するために問い合わせが行われます。すべてのテレメトリが収集されると、セキュリティ コントローラとワークフローによって分析され、ポリシーに基づいて、提案された緩和対策と制御を適用するかどうかが決定されます。当然のことながら、シスコでは継続的な学習を繰り返し行っています。Cisco Talos の研究チームは、脅威の調査と、シスコ製品の完全なポートフォリオに対する緩和ルールの導入により、お客様が競争に勝ち残るようにする一方、サービス プロバイダーの負担を軽減してコア コンピテンシーに集中できるようにします。

制御は、攻撃を軽減するために講じる措置を指します。制御の種類により、プロアクティブに行われるもの、攻撃後に適用されるものに分かれます。攻撃には 2 つのタイプがあります。ゼロデイ攻撃は、これまでにフィンガープリントがない脅威です。通常、キャリア クラウドとアプリケーションにおける既知の適正な動作（サービスを要求し、サービスの状態を要求する）に狂いが生じた場合、セキュリティ コントローラによって特定され、その後に攻撃を緩和するため、あるいは可視性を向上させるための措置が講じられます。攻撃者を適切に特定するための措置が行われることもあります。デイワン攻撃はシグネチャやフィンガープリントを持つ脅威であり、多くの場合、攻撃に対処するための緩和戦略が事前に存在します。制御は、キャリア クラウドに対する変更の形で、攻撃の影響を最小限に抑えるために、ホップごとの動作においてサービス品質の変更を適用します。また、可能な限り脅威の発信元に近いところに適用される物理および仮想セキュリティ アセットの形で、副次的な損害を最小限に抑えます。

アプリケーションを提供する事業者が抱える情報は、膨大です。情報の適用方法（クローズド ループによる反復プロセス）に関するイノベーションは、脅威の可視性と緩和に関する最新のイノベーションです。これにより、自動化、オーケストレーション、NFV がセキュリティに対応し、現在および今後のセキュリティ ニーズを解決します。クローズド ループによる反復プロセスの 3 つの要素は、ポリシー、分析、およびアプリケーション配信クラウド（アプリケーションから、サービス提供に使用されるネットワークに至るまでのトランザクション全体）です。通信事業者は革新的な方法を適用できるようになり、地理的位置情報を行動分析と関連付け、キャリア クラウドへの脅威に関連したポリシーと比較し、脅威の性質とその対処方法をより明確に特定することができます。可視性と制御が今日の高度な脅威に適切に適用されると、キャリア クラウドに一定レベルの保護が提供されます。私たちは、攻撃時にネットワークの安全性および復元力を保つために、進化、成長、スマート化を継続しなければなりません。

結局のところ、セキュリティとは、脅威をより迅速に発見、修正し、常に学ぶということです。

# 5G の新機能

5G は、4G/LTE の次世代となる 3GPP テクノロジーで、ワイヤレス モバイル データ通信向けに定義されています。3GPP Release 15 以降、3GPP において 5G の標準化定義が開始されました。3GPP Rel 15 の一環として、5G ネットワークの要求に対応するための新しい 5G 無線とパケット コアの進化が定義されています。[1] と [2] で、5G アーキテクチャの 3GPP 標準について詳しく説明します。

以下は、5G において重要な最終目標の一部です。

- 非常に高いスループット（1 ～ 20 Gbps）
- 超低遅延（1 ms 未満）
- 単位面積あたりの帯域幅（1000 倍）
- 大規模な接続性
- 高可用性
- 高密度なカバレッジ
- 低エネルギー消費
- マシン タイプ通信のバッテリー寿命を最大 10 年間まで向上

セキュリティに焦点を当てた「専門家チーム」が存在しますが、これは 5G アーキテクチャを推進する多くの組織の一部です。3GPP と NGMN の 2 つは、こうした組織に含まれます。これにより、重要な 5G セキュリティの内容がより広範な 5G アーキテクチャの進化に反映されます。これらの内容には、認証、暗号化、セキュリティ制御の配置と可視性の情報源が含まれます。これはすべて、5G アーキテクチャを推進する一連の新しいユース ケースによってもたらされます。

以下は、5G PPP（欧州委員会と欧州 ICT の共同イニシアチブ）によって定められた予測の一部です。

## 5G PPP により社会のネットワーク接続が今後も進展


出典：5G PPP

5G は無線および有線ネットワークを橋渡し（ブリッジ）し、無線アクセスからコアへ、大きなネットワーク アーキテクチャ変更を必要とする可能性があります。

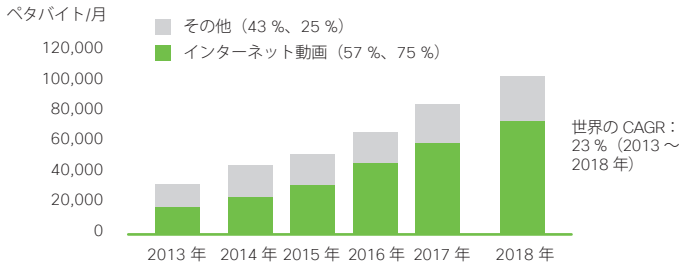
# シスコの 5G ビジョン

5G は、新しい可能性と能力を実現するイネーブラーです。新世代の 3GPP ワイヤレス モバイル データ通信技術は、新しいユース ケースと能力の土台を作ります。3G はデータ通信を対象にした最初の真のワイヤレス モバイル データ通信技術であるのに対し、4G は初の真のオール IP ワイヤレス データ通信技術でした。3G と 4G、どちらの通信技術もモバイル デバイス上のデータ通信の基盤となり、モバイル デバイス上のビデオ、e コマース、ソーシャル ネットワーク、ゲームなどのアプリケーションの普及につながりました。3G/4G での焦点は、主に消費者と企業向けのモバイル ブロードバンドを提供することにありました。

以下に、事業者が着目しているいくつかの傾向と、新たなビジネス機会を示します。

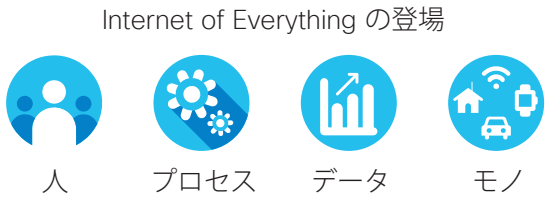
## 世界はモバイル時代に移行


## ビデオがもたらすアクセス トラフィックの増大




## クラウド コンピューティングの台頭


## IoE につながるデジタル化




新たなユース ケースが導入されると、新たな課題、複雑さ、脅威が浮き彫りになります。したがって、新しい 5G ネットワークでは、通信事業者が現在のニーズを管理するだけでなく、今後発生する新しいユース ケースによる新しいニーズを満たすための準備もしておく必要があります。5G は、モバイル ブロードバンドを強化するための高速データ接続だけでなく、企業向けの新たなユース ケースに対応できるいくつかの新しい機能を実現します。「エンタープライズ ネットワーク スライス」を確保することで、5G を使用する企業が、運用上および規制上の両方で安全に成果を出すために必要となる、数多くの新たな課題が露呈します。5G は、消費者および企業の加入者に高スループットの接続性を備えたサービスを提供するだけではありません。企業向けの新しいユース ケースの要件に対応できるようにすることで、通信事業者が新しい収益への道筋とビジネス機会を実現できます。シスコは、通信事業者が企業や官公庁のお客様のニーズに対応して多くの機能を備えることができるように、既存のユース ケースおよび新しいユース ケースをサポートする 5G の展開を想定しています。これらの新しいユース ケースの実現は、輸送からアプリケーションに至るまで、5G ネットワーク全体に広がるセキュリティの可視性と制御によって提供される「セーフティネット」を前提としています。5G は脅威に対する多数の新しい境界を提供しますが、さらに攻撃を厳しいものとするために、移動可能な一時的な境界となっています。

シスコは、標準化されたマルチベンダー環境でデータセンター、ネットワーク、モビリティの経済的側面における大規模な変化をサービス プロバイダーが活用する機会として、5G コアに興味を持ってみています。そこには、スライシングとより細分化された機能を利用したパーソナライズされたネットワークのような新しい機会を促進するモバイル コアにとって、非常に重要な変更が定義されています。5G は、新しい無線による大量スループットおよび低遅延を利用するためのフレームワークを提供します。

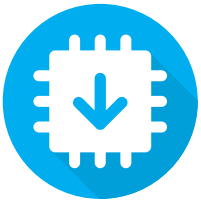
以下に、5G が対応するユース ケースの一部を示します。

運輸
自律走行車
自動車

IoT

拡張現実
仮想現実

スマート シティ
トラフィック管理
緊急サービス



ロボット製造

タッチ
インターネット

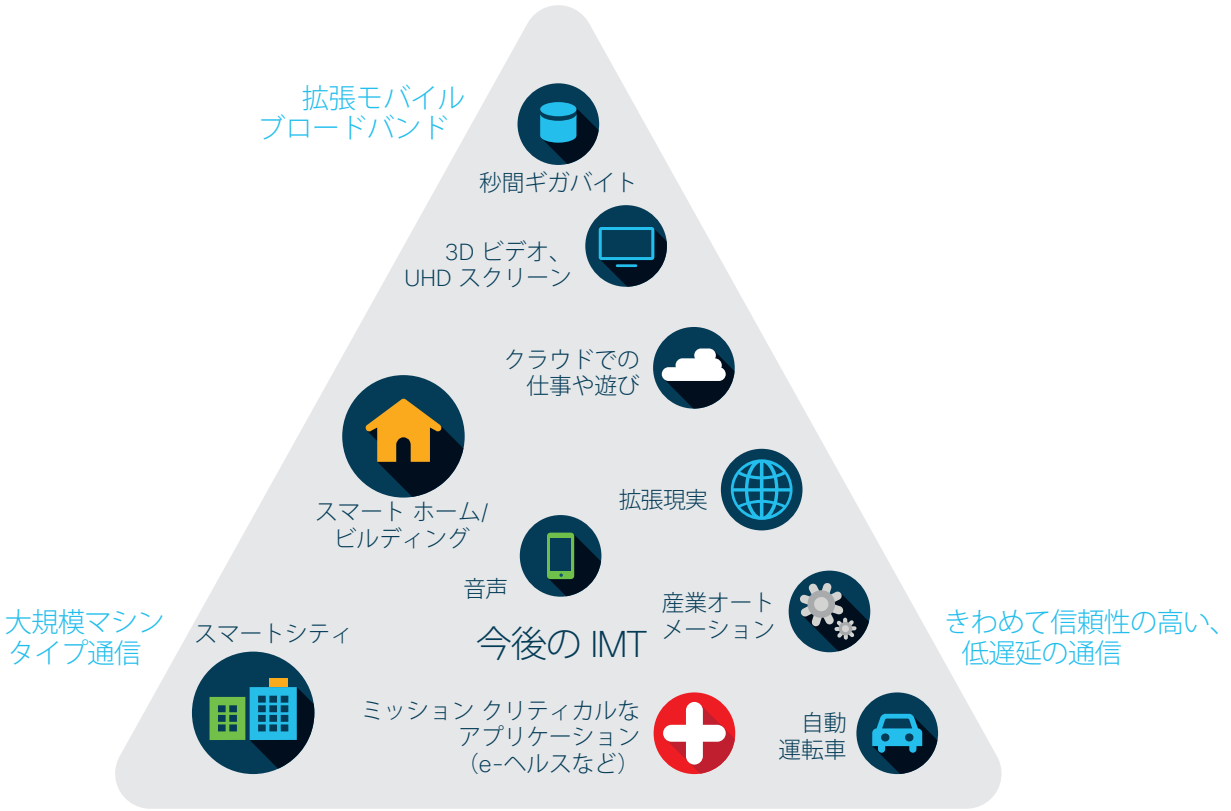
医療
フィットネス ヘルスケア

スマート グリッド
公益事業

政府/自治体

スマート オフィス

以下は、5G が対応するさまざまなユース ケース（出典：ITU）を示すチャートです。




出典：ITU

以下に、あらゆるユース ケースを対象にする 3 種類のユース ケース カテゴリを示します。

**拡張モバイル ブロードバンド（eMBB）：**5G 拡張モバイル ブロードバンド（eMBB）は、加入者に高速かつ高密度なブロードバンドを提供します。ギガビットの通信速度で、従来の固定回線サービスの代替手段となるものです。また、mmWave 無線技術（ミリ波）に基づく固定無線アクセスは、高密度を実現し、5G ワイヤレス接続によるビデオなどの高帯域幅サービスをサポートします。eMBB ユース ケースをサポートするためには、モバイル コアが必要とされるパフォーマンス密度、スケーラビリティ、セキュリティをサポートしなければなりません。

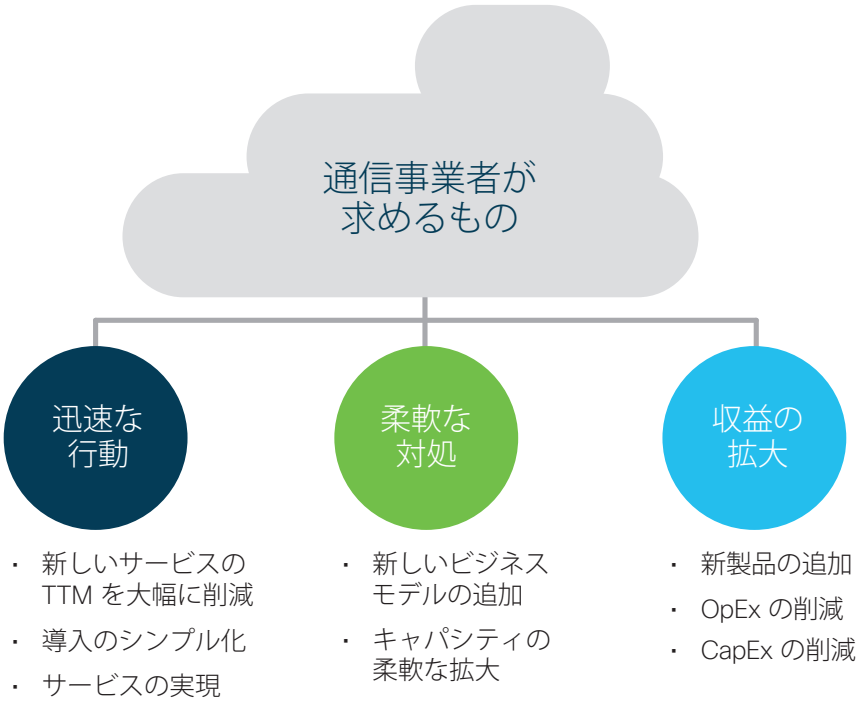
**超高信頼性の低遅延通信（ロボット、ファクトリ オートメーション）：**超高信頼性の低遅延通信（URLLC）は、拡張現実（AR）および仮想現実（VR）などを想定し、具体的には遠隔手術、遠隔医療、インテリジェントな輸送、産業オートメーションなどのミッション クリティカルなサービスに重点を置いています。5G は上記のような非常に機密性の高いユース ケースに対し、従来の有線接続に相当するワイヤレス技術を提供します。さらに、URLLC では、データ遅延要件を実現するために、制御プレーンおよびユーザ プレーン分離（CUPS）アーキテクチャを用いて、エンド ユーザに地理的に近い位置にモバイル コア ユーザ プレーン機能（UPF）を配置するよう求めています。

**大規模な IoT：**5 G における大規模な IoT は、さまざまなサービスと数十億の接続をサポートするニーズに対処するものです。IoT サービスは、比較的低い帯域幅を必要とするデバイス センサーから、携帯電話機と同様のサービスを必要とするコネクテッド カーまでさまざまです。ネットワーク スライシングは、サービス プロバイダーが企業に対して Network as a Service（NaaS）を有効にする方法を提供します。5G ネットワーク上で自社のデバイスやサービスを柔軟に管理することができます。

上記ユース ケースの特徴は、以下のとおりです。

- 深いカバレッジで効率的な低コスト通信を実現。
- 軽量デバイスの初期化と設定を実現。
- モバイル発信データのみの通信シナリオにおける、低頻度の小さいデータを効率的にサポート。

ニーズと要件が異なる複数のユース ケースがある場合、ネットワークの複雑さと通信事業者のコストが増大します。したがって、通信事業者がこうした異なるユース ケースに対応し、競合他社との差別化を図るためには、次のような機能が必要であるとシスコは考えています。

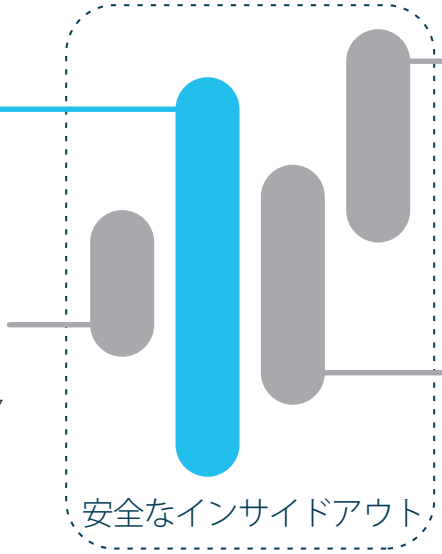



シスコは、上記のような通信事業者のニーズを念頭に置き、5G ソリューションを開発しています。シスコの戦略では、通信事業者をクラウド中心の世界へと導くことで、通信事業者がクラウド ネイティブ ソリューションのメリットを享受でき、そしてそれによって上に挙げたニーズを満たすことを目指しています。また、5G は単なる新しい無線ではなく、RAN とパケット コアの両方を含む包括的なエンドツーエンド ネットワークであり、通信事業者のニーズに対応できるよう進化する必要があるとシスコでは考えています。

通信事業者のネットワークを保護する上で非常に興味深いものの 1 つは、暗号化の役割における進化です。ほとんどのセキュリティ制御では可視性が必要です。これによってセキュリティ制御のポリシーに対する決定を行い、可能な限り発信元に近い脅威の緩和に利用して、脅威の副次的な被害を最小限に抑えます。現在、インターネット上の全トラフィックの約半数が暗号化され、今後数年間で増加する見込みです。シスコは、暗号化トラフィック分析に関するイノベーションにより、機械学習に基づくテクノロジー セットを提供し、このような 5G の進化的側面に対処します。

広域に分散しているデータセンターでは、脅威にさらされる機会が著しく拡大します。多くの攻撃者は、ターゲット ネットワークに侵入し、水平展開して損害を引き起こし、データを盗み出す APT（Advanced Persistent Threats: 標的型攻撃）を活用します。犯罪者やハッカーによる水平展開を非常に困難にするために、セグメンテーションを適用して、ネットワークの構造を使用してネットワークとアプリケーションを保護する必要があります。シスコのデータセンターは、アイデンティティ コントローラによる自動化を活用します。これは、セキュリティを動的に提供する必要があるすべてのネットワーク要素にプログラムで配信されます。これにより、単純なマトリックスを使用してポリシーを動的に適用できるため、ポリシーの手動適用に起因するエラーを回避できます。セグメンテーションは、5G ネットワーク全体、トランスポート、モバイル エッジコンピューティング、その他の主要サービスを提供する分散データセンター、および 5G アーキテクチャの他の部分にも適用されます。セグメンテーションの実現には、トランスポートにおけるセグメント ルーティングとデータセンターにおける TrustSec の 2 つのテクノロジーが使用されます。シスコはエンドツーエンドのセグメンテーションを独自に提供できます。

以下に、Cisco 5G ソリューション アーキテクチャの基本理念を示します。




### クラウドスケールのネットワーク
- 仮想化、プログラム制御
- シンプルさ
- サービスの速度
- オープン性・柔軟性

### 自動化およびオーケストレーション
- 自己最適化インフラストラクチャ
- 運用とサービス作成の最適化

### アクセス手段に依存しない
- 真の異種ネットワーク
- 高密度化トポロジ
- ライセンス/非ライセンスの併用
- Wi-Fi（屋内外）
- 3G、4G、5G LPWA など

### API の公開
- モバイル コアの長所を生かして構築
- ネットワークからデータを抽出
- 業種別の価値を創出
- 新しいビジネス モデルの実現

パケット コアの主要ベンダーとして、長年にわたり培ってきたノウハウを元に、シスコは 3GPP の標準化に関わってきました。また、第 2 世代から第 3 世代、そして第 3 世代から第 4 世代への移行を早い段階から目の当たりにしており、現在、4G から 5G への重要な移行のためにソリューションを定義し、リードするに最もふさわしいベンダーと言えます。

プラットフォーム ベースの VPC ソリューションは、世界において 40 以上のネットワークに展開され、シスコを主要な仮想パケット コア ベンダーの 1 つにしています。

シスコは、3GPP で標準化されるより前から、いくつかのパケット コアのコンセプトに取り組んでいます。それぞれのセキュリティへの影響については、以下で説明します。たとえば、2016 年と 2017 年の MWC（Mobile World Congress）では CUPS について実証するベンダーのうちの 1 社でした。同様の取り組みを続けているシスコは、5G ソリューションのプレスタンダード バージョンの導入を積極的に推進しており、NextGen 5G ネットワークのニーズを評価し、3GPP に準拠させ、結果的に標準に影響を与えています。

シスコの 5G ソリューションが通信事業者に選ばれる理由には以下ようなものが挙げられます。

| 仮想化 | オープン性 | 研究開発への投資 |
|---|---|---|
| 市場リーダー<br>主要な Tier1 事業者を含む<br>40 社以上での採用実績 | 市場リーダー<br>主要な Tier1 事業者を含む<br>40 社以上での採用実績 | クラウド ネイティブや<br>NFV テクノロジーにおける<br>相当規模の研究開発投資を実施 |
| **VNF ポートフォリオ** | **フル スタック** | **仮想化** |
| 包括的な「既製品の」<br>VNF カタログ | すべての機能をカバー<br>（クラウド上、クラウド配下） | クラウド ネイティブ技術が、<br>自動/分散/エッジ ベースの<br>インテリジェント ネットワークの<br>5G アーキテクチャ ビジョンと協調 |

3GPP は、5G ネットワーク向けに 5G 非スタンドアロン（NSA）、5G スタンドアロン（SA）という 2 種類のソリューションを定義しています。

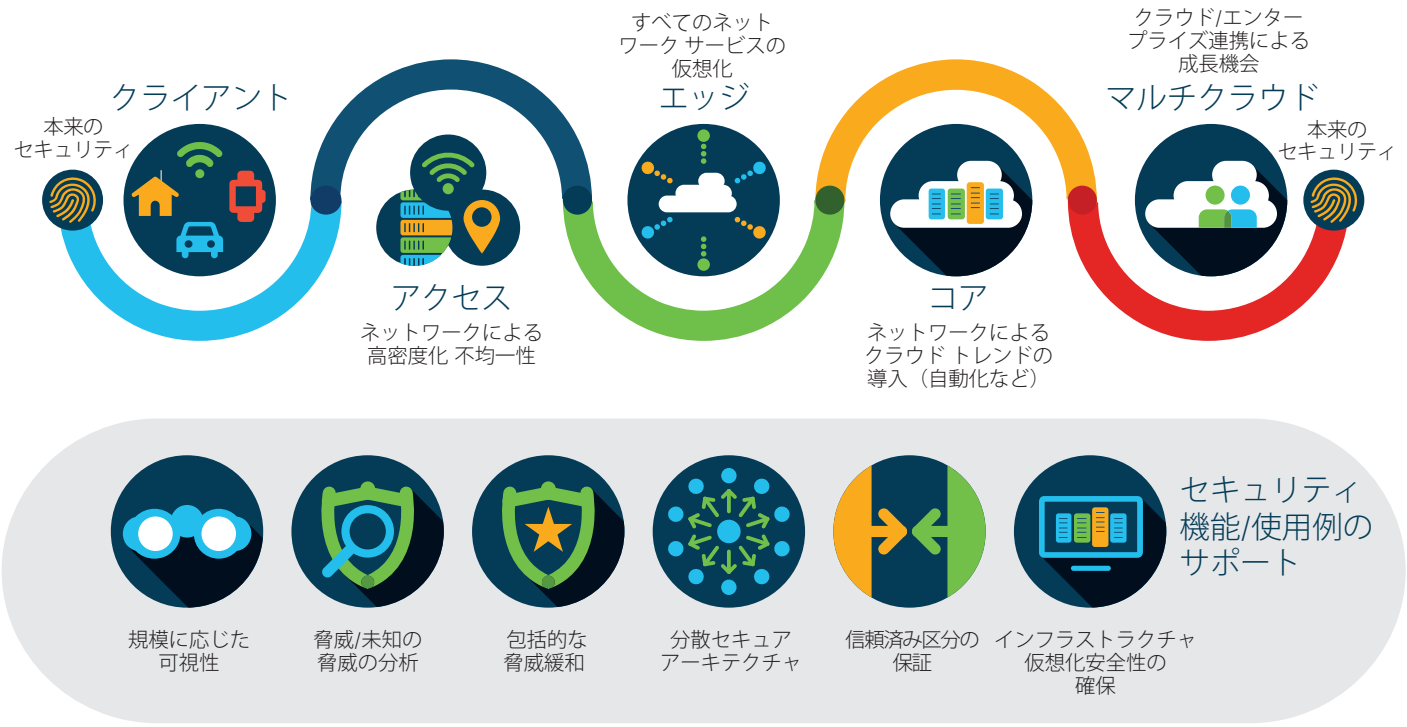
**5G 非スタンドアロン ソリューション（NSA）：**5G NSA 事業者は、既存の EPC パケット コアを活用して、3GPP リリース 12 デュアル コネクティビティ機能を使用して 5G NR をアンカーします。これにより、積極的に 5G に着手し、より短期間かつ低コストで 5G サービスの提供開始を目指す通信事業者を支援します。一部のユース ケースの初期段階では、5G NSA ソリューションで十分であると考えられます。しかし、5G NSA には、よりクリーンな真の 5G ネイティブ ソリューションを得るという点でいくつかの制限があり、すべての通信事業者が最終的には 5G スタンドアロン ソリューションに移行すると見込まれます。

**5G スタンドアロン（SA）ソリューション：**5G SA では、すべての新しい 5G パケット コアが導入されています。はるかにクリーンなソリューションであり、いくつかの新しい機能が組み込まれています。ネットワーク スライシング、CUPS、仮想化、自動化、マルチ Gbps サポート、超低遅延などが 5G SA パケット コア アーキテクチャに標準の状態で組み込まれます。

シスコは、5G 非スタンドアロン（NSA）および 5G スタンドアロン（SA）ネットワークの両方に対応するパケット コア ソリューションのポートフォリオを提供します。通信事業者が 4G から 5G への段階的な移行をスムーズに実現できるような 5G パケット コア ソリューションを考案することが、シスコの目標です。

## セキュリティ イノベーションと 5G のソート リーダーシップ

### Cisco 5G - 並行開発セキュリティ ロードマップ




上記の図が示すように、セキュリティはシスコの 5G 戦略の基本的な側面です。Cisco 5G ネットワークでセキュアな成果を実現する基本セキュリティ ファブリックには、5 つの側面があります。進化的な面、革新的な一面もあります。まとめると、通信事業者および消費者に対して重要な 5G ベースのサービス向けに一定レベルのサービス保証を提供することで、現在および今後の脅威対象に対処します。

セキュリティ イノベーションとソート リーダーシップの 5 つの重点分野は、次のとおりです。

1. 5G と IoT の脅威対象（現在と今後）を詳細化するアーキテクチャと信頼境界
   a. 企業と 5G スライスとが接触する場所
   b. SP の IT 部門と 5G とが接触する場所
2. 5G ネットワークのセキュリティに影響を与えるテクノロジー トレンドとアーキテクチャ
3. スケーリングする可視性
4. 脅威/ダーク スレットの分析
5. 包括的な脅威緩和

これらの 5 つの分野については、本ホワイト ペーパーの残りの部分で扱います。

以下の図は、これらの 5 つの分野を 5G の運用上のセキュリティ要件に当てはめたものです。

水際での脅威の阻止

作業場所を問わずユーザを常に保護

ネットワークにアクセスできるユーザの制御

ネットワークのセグメンテーションのシンプル化

問題を迅速に特定して解決

# アーキテクチャ、テクノロジー トレンド、信頼境界 – 5G と IoT の脅威対象（現在と今後）

## 5G と進化するアーキテクチャ

5G では新しいアーキテクチャを採用し、既存のネットワーク コンセプトをアーキテクチャに適用しています。これらのアーキテクチャ シフトの中には、クラウド運用に合うように、モバイル アーキテクチャを事実上最新にしているものがあります。このようなシフトの一例として、コントロール プレーンとユーザ プレーンの分離（CUPS）が挙げられます。一方、いくつかの新しいユース ケースを認識した結果生まれたシフトもあります。このようなシフトの例が、拡張現実と仮想現実（AR/VR）です。この場合、ローカライゼーションや、ネットワーク エッジでの処理遅延時間の短縮（MEC）の必要が生じます。この項目では、5G に対するさまざまな 5G アーキテクチャ イネーブラについて概説しているわけですが、当然、これらのアーキテクチャ コンセプトのすべてを 5G ネットワークに同時に適用する必要はありません。現実的には実情に応じた判断と適切な機会が求められるため、シスコではさまざまな通信事業者の遵守するアーキテクチャが複数存在することを想定しています。これは、サービス プロバイダーが採用するセキュリティ アーキテクチャ全体に影響を及ぼします。

進化しつつあり、さまざまな通信事業者によって検討されているアーキテクチャ イネーブラの一部を以下に示します。

## CUPS

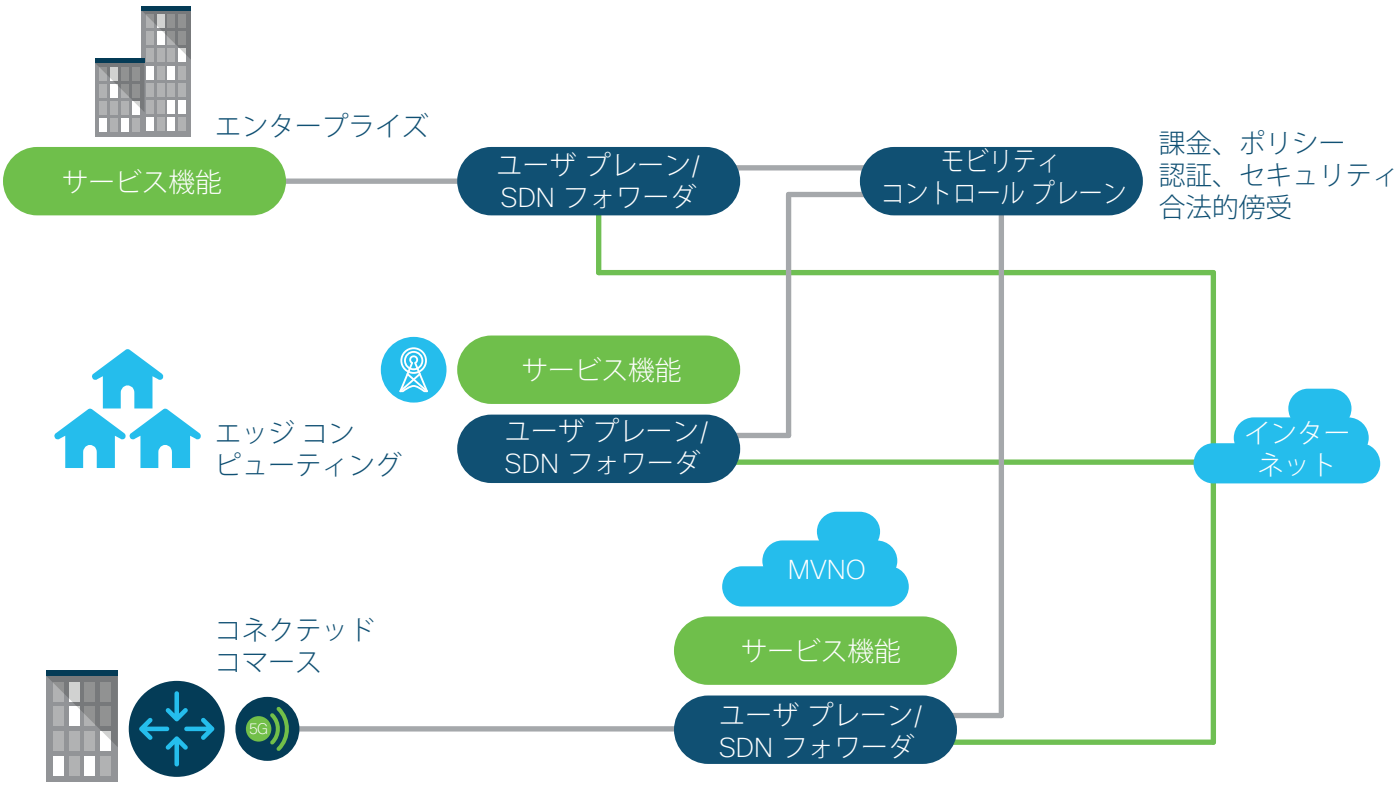



図 1. CUPS アーキテクチャの概要

Control Plane User Plane Separation（CUPS）アーキテクチャ（図 1 参照）により、コア要素の分散が可能になります。機能の利用効率の向上や、一定の SLA サービス要件下での最適なネットワーク機能配置などにつながります。CUPS はまた、トラフィック ディメンションに基づいて効率的なネットワーク機能のスケーラビリティを実現します。

## MEC

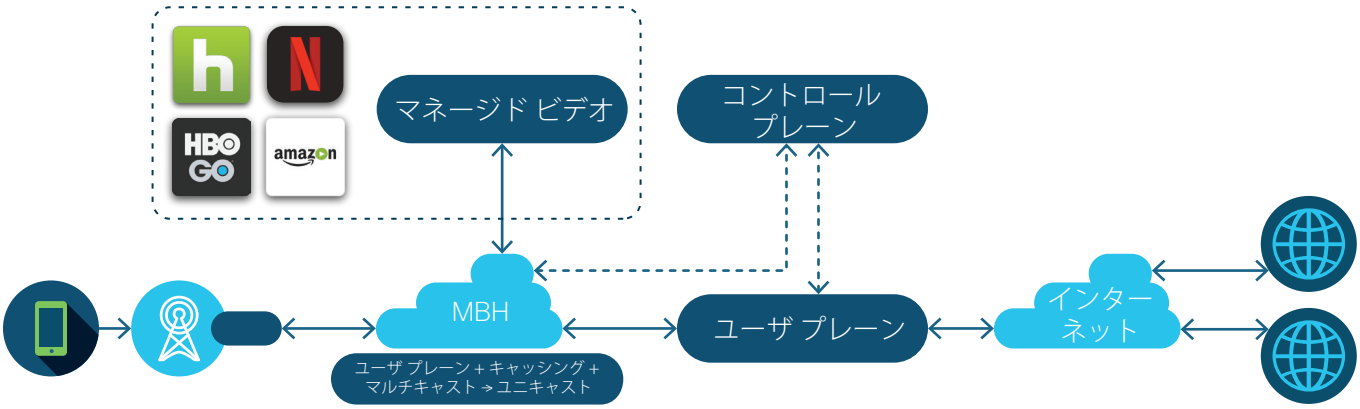



図 2. MEC アーキテクチャの概要

モバイル エッジ コンピューティング（MEC）は、CUPS アーキテクチャを再利用して、ユーザ プレーン機能とアプリケーションをネットワーク エッジの近くに配置することができます（図 2 参照）。さらに、MEC アーキテクチャでは、ユーザ アプリケーションとサービスをユーザの近くに配置することができるため、低遅延のユース ケースを実現できる可能性があります。オフロードなどのネットワーク トラフィック管理メカニズムでも、MEC ベースのアーキテクチャのメリットを享受できます。

## CRAN

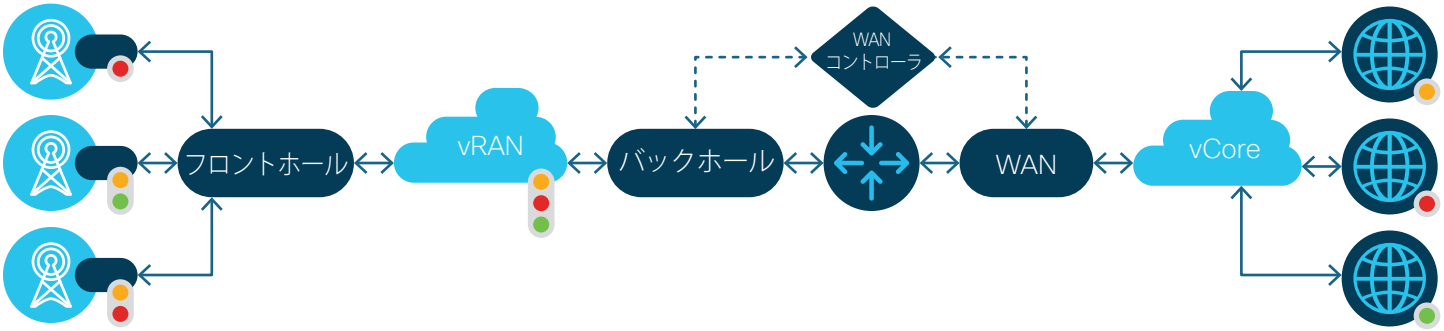



図 3. CRAN アーキテクチャの概要

クラウド無線アクセス ネットワーク（CRAN）アーキテクチャでは、アクセス ネットワークにおいて、コントロール プレーンとユーザ プレーンを分離する形がとられます。これにより、分割したアクセス アーキテクチャが可能になります。このアーキテクチャにより、RAN 処理の一部は実質的に「中央」エッジ クラウド ロケーションで行われ、残りの処理はリモート無線ヘッド（RRH）のような「物理的」リモート ロケーションで行われます。これで、トランスポート ネットワークにおいてフロントホールとバックホールが分割されます（図 3 参照）。CRAN アーキテクチャを、ネットワーク スライシング、クラウド ネイティブ コアと組み合わせて、より柔軟な 5G ユース ケースを実現することもできます。

## ネットワーク スライシング

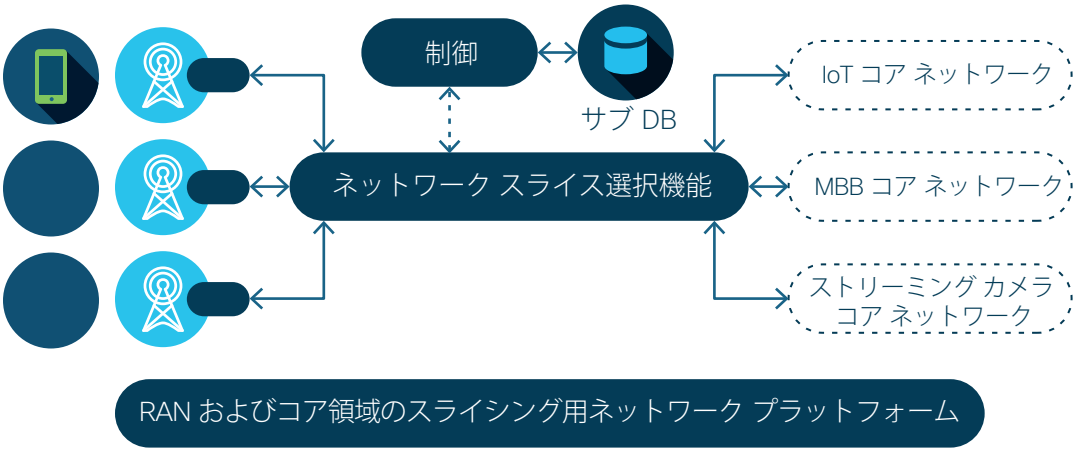



図 4. ネットワーク スライス アーキテクチャの概要

ネットワーク スライシングは、共通の物理インフラストラクチャ上で、複数の論理ネットワークを独立したビジネス オペレーションとして仮想的に設定して実行する、(自動) ネットワーク機能です (図 4 参照)。ネットワーク スライシングは、今時点ではエンタープライズでのユース ケースはまれですが、5G ネットワークの基本的なアーキテクチャ コンポーネントであり、5G ユース ケースの大部分を満たすと期待されます。

多くの通信事業者は、企業ごとのネットワーク スライスの提供を検討していますが、現在行われている企業に対する APN の提供とは異なります。企業が 5G スライスを扱うポイントを考慮すると、多くのセキュリティ面に対処する必要があります。シスコは、今日のエンタープライズ セキュリティにおいて重要な役割を担っており、その対象を 5G スライスにまで拡大することができます。これらの分野は、次のとおりです。

| | |
|---|---|
| アイデンティティ、ネットワーク アクセス コントロール、セグメンテーション | 企業における Cisco Identity Services Engine |
| アイデンティティを共有するためのユニファイド トランスポート | pxGrid による一貫したアイデンティティ サービスの提供/共有 |
| 企業における 5G 接続へのシームレスな移行 | IP ビデオ/音声での Wi-Fi から 5G へのハンドオフ |
| 一時的なエンタープライズ エッジの保護 | 仮想/クラウド セキュリティ サービスの対象範囲を拡大 |
| アプリケーション境界の保護 | API セキュリティとデータ損失防止の拡張 |
| 脅威の俊敏性と対応のためのセグメント化 | セグメント化された企業ネットワークへの 5G スライスの追加 |

前項で説明したアーキテクチャ コンセプトを 5G アーキテクチャに組み合わせることで、5G の脅威の対象が拡大します。脅威の対象が拡大する理由には、主なものでも複数ありますが、その中からいくつか例を挙げます。

- ネットワークの物理的構造が変化しており、(今後の)アプリケーションやユース ケースでは、ローカライゼーションや遅延に備え、ストレージの場所をエッジに近づけたり、近い場所を計算したりすることが必要になります。つまり、実質的には、これまでは利用できなかった新しい公開済み実行サイトともいえるものが必要になります。
- ネットワーク機能の構造が物理的実装から仮想的な実装に変更されており、仮想化コンポーネントの機能を分散型エッジと集中型のコア クラウドに配置できます。
- SDN(ソフトウェア定義型ネットワーク)、SDA(ソフトウェア定義型アクセス)、SDR(ソフトウェア定義型無線)などの柔軟なソフトウェア ベースのアーキテクチャ イネーブラに重点が置かれています。

つまり、この状況をまとめると、5G の脅威対象の大部分は、ネットワーク アーキテクチャがより柔軟でインターネットに開放されていることに起因すると考えられます。図 5 は、5G アーキテクチャにおける上記の特性(CUPS、MEC、CRAN、スライシング)について、脅威の観点から示しています。

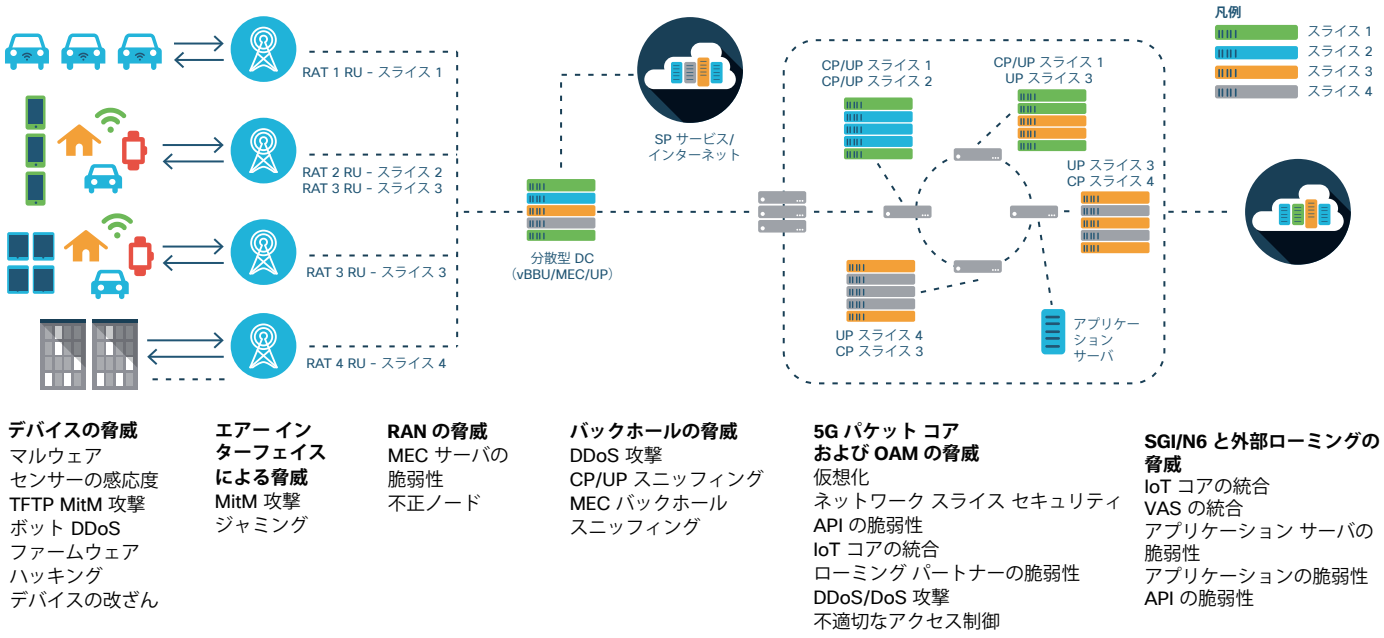



図 5. 5G アーキテクチャの脅威の対象

当然のことながら、特定のユース ケースを 5G アーキテクチャに適用してみると、そのユース ケースの脅威対象がどのようなものかを分析できます。図 6 は、その一例であり、5G IoT ネットワーク アーキテクチャのエンドツーエンドの脅威対象を示しています。

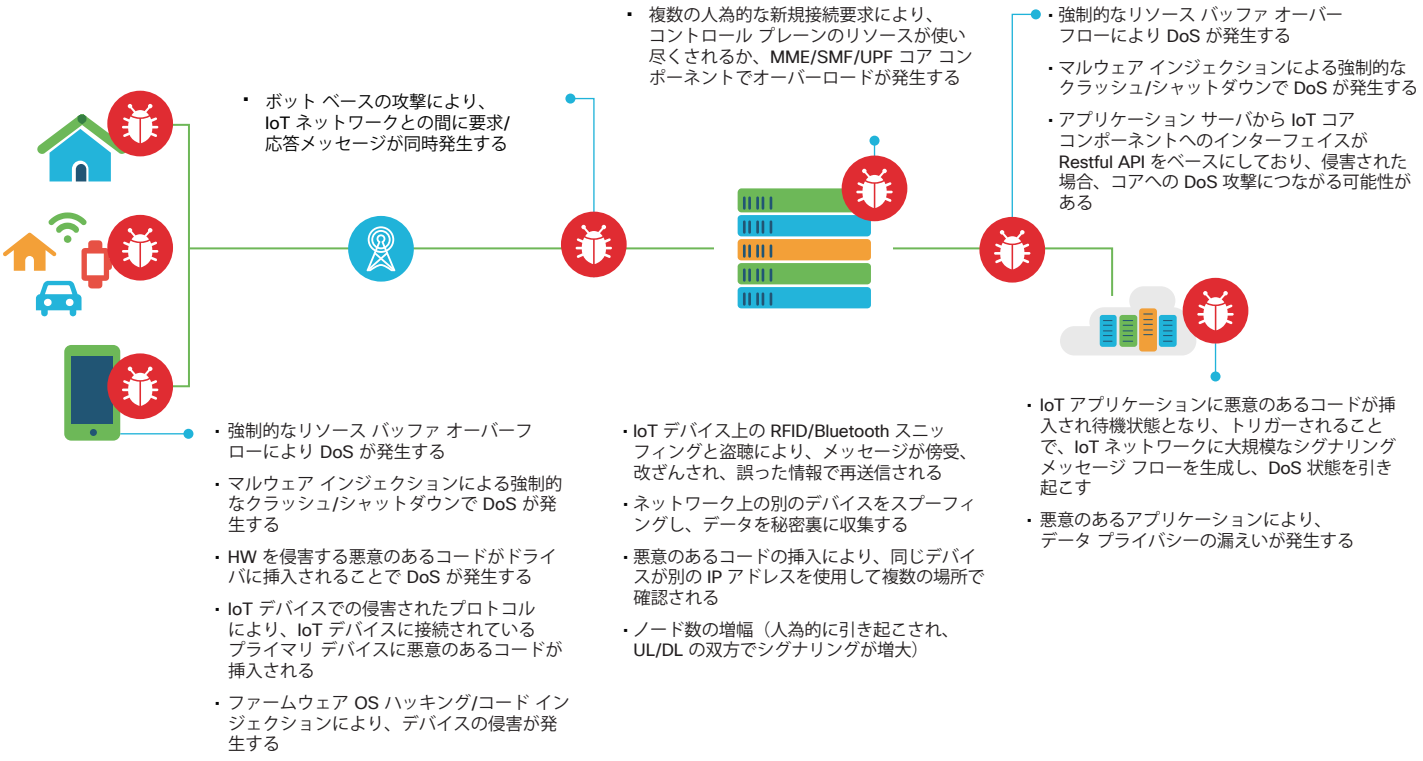



図 6. 例 - 5G IoT の脅威対象

上記 2 つの図で、異なるコンポーネント間の脅威の対象を明確に示しています。詳しくは以下で説明します。

M2M、産業オートメーション、IoT デバイスなどのさまざまなユース ケースで独自の無線アクセス技術が使用されます。つまり、WLAN などの 3GPP および非 3GPP テクノロジーと新しい 5G 無線アクセスを組み合わせ、デバイス電力消費の効率を改善し、低コスト デバイスに求められる低帯域幅を実現します。低コスト デバイスには、ファームウェアや OS のハッキングのような脅威を軽減するセキュリティ機能（組み込みのトラスト アンカーなど）はありません。そのようなデバイスを使用する大部分のケースでは、企業が管理するクレデンシャルと AAA を使用してモバイル ネットワーク事業者がアクセスを提供します。このようなデバイスは、中間者攻撃（MitM）、ファームウェアおよび OS のハッキング、スヌーピング/スニッフィング攻撃、ボットネット タイプの攻撃（IoT デバイスが通信事業者のモバイル ネットワーク コンポーネントで信号過負荷をかける）を受けやすいものです。

5G では、機能とアプリケーションがネットワーク上を移動する可能性があります。たとえば、モバイル エッジ コンピューティング（MEC）では、ユーザ プレーン（UP）およびセルラー機能がネットワークのエッジに移動します。この新しいアーキテクチャでは、IP 接続は、3GPP で定義されている N6 インターフェイスなどの通信事業者ネットワークのエッジで終端します。現在の DNS 解決およびコンテンツ配信ネットワークの機能も、ネットワークのエッジの近くに配置される可能性があります。そうすることで、低遅延を必要とするユース ケースでみられる多くの課題が緩和されます。このようなアプリケーションの例としては、コネクテッド カーのアプリケーションが挙げられます。コンテンツが通信事業者ネットワーク内にある複製から配信されるため、ビデオ コンテンツをエンドツーエンドで（ユーザ エンドからビデオ サーバまで）暗号化して最適化するのです。ただ、これはモバイル ネットワーク事業者にとって、脅威となる対象が新たに増えることを意味します。

サーバやキャッシュに対する従来の攻撃（HTTP 応答の分割による攻撃など）以外にも、新たな脅威が発生します。たとえば、サービス妨害（DoS）攻撃により、通信事業者の保証する遅延に関するサービス レベル契約から大きく逸脱する可能性があります。このシナリオでは、低遅延のアプリケーション（ビデオ キャッシングなど）を使用する多くの加入者に対応するため、ネットワークのエッジに相当量のキャッシュが展開されます。そのため攻撃者は、通常のユーザがあまり使用しないコンテンツへリクエストを送ることで、これらのキャッシュを簡単に飽和状態に陥らせることができます。その結果、ローカル キャッシュの内容が、加入者の使用できない「役に立たない」コンテンツでいっぱいになる可能性があります。このような攻撃は、従来からあるインフラストラクチャのハードウェア コンポーネントに対する攻撃、アプリケーションの脆弱性、適切に保護されていない API、アーキテクチャ内の不正なノードなどの脆弱性に起因して発生する可能性があります。

また、5G コア アーキテクチャにより、まったく新しいセキュリティ上の脅威が生じます。5G ユース ケースで構築される仮想化モバイル ネットワーク コンポーネントや分離スライスが脆弱性の原因となる可能性があります。SCEF（Service Capability Exposure Function）や NEF（Network Exposure Functions）などの 3GPP の規定する公開機能を使用して、モバイル ネットワークのコア コンポーネントをサードパーティ製アプリケーションや外部のインターネット側インターフェイスに公開している場合なども脅威の対象となることが考えられます。5G に向けたさまざまなアーキテクチャの進化には、既存の 3GPP インフラストラクチャとの相互接続も必要です。インフラストラクチャの例としては、Mobility Management Entity（MME）、Serving Gateway（SGW）、Packet Gateway（PGW）、LTE で使用されている 3GPP および非 3GPP アクセス用の AAA サーバや Home Subscriber Server（HSS）などの加入者認証/認可インフラストラクチャがあります。そして、このようなインフラストラクチャの増加にともない、脅威の対象範囲も拡大しています。最近では、Stream Control Transmission Protocol（SCTP）や GPRS Tunneling Protocol（GTP）プロトコルがネットワーク スライスでの DoS/DDoS 攻撃に利用され、人為的にリソースを使い果たされる場合があります。またスライスに関しては、暗号化実装に関連するクラスへの攻撃に起因したサイド チャネル攻撃があります。ネットワーク スライス マネージャやオーケストレーション層に対する偽装攻撃、Control Plane User Plane Separation（CUPS）アーキテクチャにおけるコントロール プレーンでのシグナリング フラッド攻撃などもみられ、SCEF および NEF 3GPP コンポーネントと通信する API やアプリケーションを保護することが求められます。

脅威の対象となるもう 1 つの要素としては、現在、モバイル ネットワーク事業者が通信事業者間の相互接続に使用して、加入者間でのローミングを可能にしているピアリング ポイントやローミング インターフェイスなどの外部向きインターフェイスが挙げられます。ローミング契約は通信事業者の間で結ばれるものであり、ローミング トラフィックをローカル側で終了させる場合には制約があります。また、GTP トンネルは既存ネットワークのローミング パートナー内部から確立されます。つまり、ローミング パートナーのネットワークに対する悪意のある攻撃は、ホスト ネットワークを危険にさらします。

サードパーティ ネットワークを使用してトラフィックをバックホールする/サードパーティ ネットワークからバックホールをリースする場合には、Gi/SGi インターフェイスが侵害された一部のサードパーティ ネットワークと統合され、モバイル ネットワークを攻撃にさらすことになります。

また、5G アーキテクチャにも適用されるセキュリティ上の規制があります。たとえば、ヨーロッパでは、新しい一般データ保護規制（GDPR）が 2018 年 5 月に施行されました。GDPR を遵守するためには、パーソナル データ（個人を特定、または特定を可能とするものなど）の収集、保管、処理を行う企業はすべて、多くの義務に従う必要があります。GDPR を遵守しなければ、多額の罰金が科せられます。既存の 5G アーキテクチャや今後のアーキテクチャにおけるさまざまなコンポーネントが複数のレベルで個人データをやりとりするため、GDPR への適合性を確保するには、5G アーキテクチャにおいてセキュリティとプライバシーに配慮し、脅威への対応を中心にすえたアプローチを取ることが必須です。

## シスコのポートフォリオを使用した 5G および進化するアーキテクチャにおける脅威の緩和

モバイル ネットワーク事業者アーキテクチャにおけるパケット コアの進化により、分散 UP コンポーネントのセキュリティ、ネットワーク スライスのセキュリティ、分散データセンターのセキュリティ、DDoS セキュリティ、API セキュリティ（パケット コア機能に外部アプリケーションから API 経由で到達できるため）、強化された NFV インフラストラクチャの使用、パケット コア トラフィック フロー内のトラフィック フローの可視化の強化、パケット コアでの DDoS 攻撃を防止するための DDoS 攻撃対策の強化、中央 DC/パケット コアのセグメンテーションと NGFW 機能の改善、ユーザ アクセス制御の強化などの必要性が生じます。

コントロール プレーンとユーザ プレーンの分離は、分散配置モデルに大いに役立ちます。モバイル ネットワークのパケット コア ノードでは、仮想化により、複数のデータセンターに分散して展開できる柔軟性がもたらされます。ネットワーク リソースを効率的に使用するために、最適な配置に応じて機能を集中機能と分散機能に分けることができます。仮想化機能と NFV のセキュリティは、NFV に配置される仮想機能のセグメンテーションとライフサイクル管理による、仮想化コンポーネント間の分離状況に大きく依存します。NFVI は、セキュア ブート、トラスト アンカーなどのセキュリティ方式によってもたらされます。

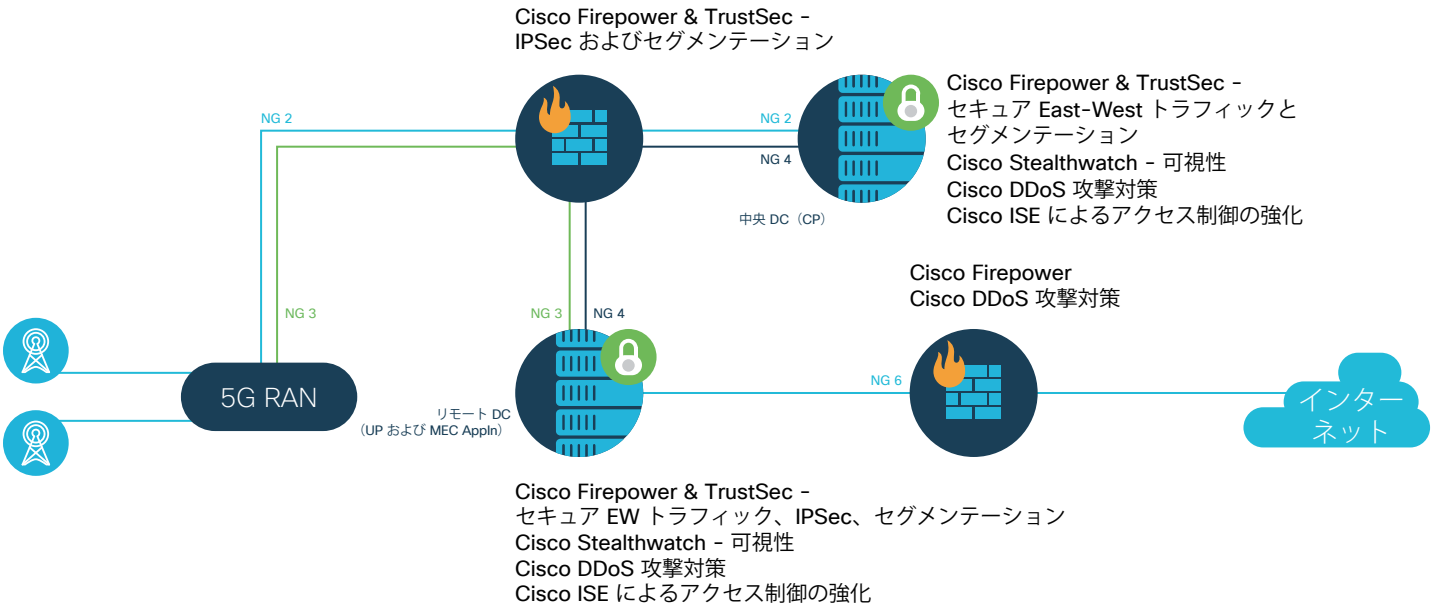



図 7. 5G アーキテクチャに適用されるシスコのセキュリティ ポートフォリオ

一般的な物理インフラストラクチャ上で事実上独立したビジネス運用として複数の論理ネットワークを実行できるネットワーク スライシング アーキテクチャでは、スライス間の高分離、スライスのコンポーネント内の分離（スライス内の他のコンポーネントに脆弱性の拡散を防ぐため）、悪意のある攻撃に備えたスライス間の分離も必要としています。

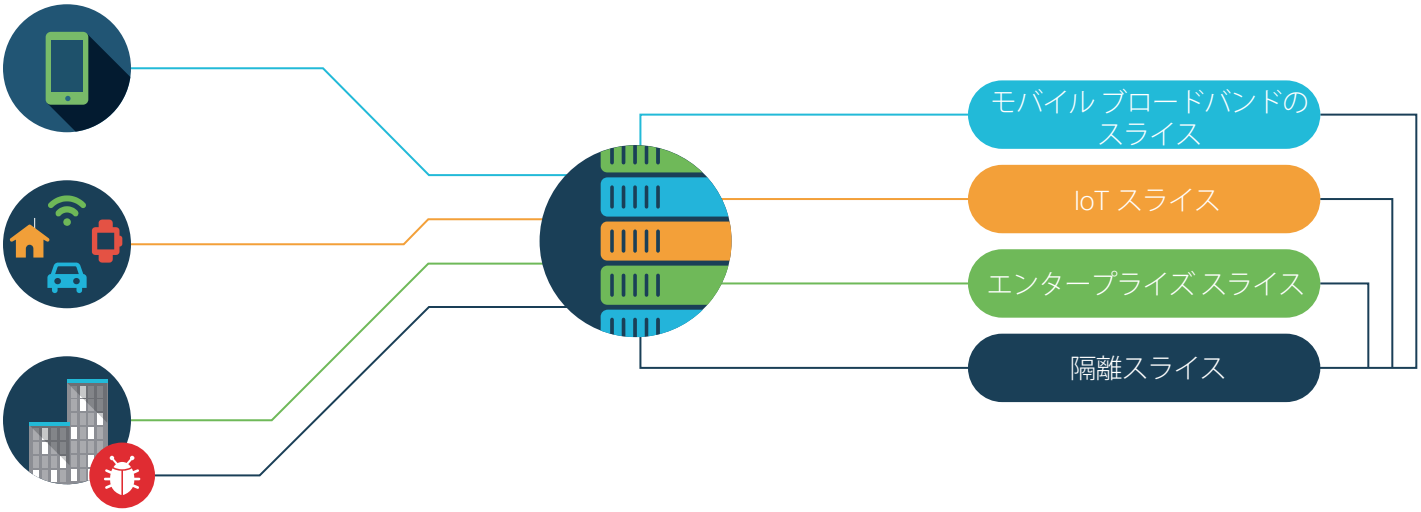



図 8. ネットワーク スライシングによる脅威の緩和

ネットワーク スライスでは、次に示すように、スライス内およびスライス間のセキュリティを有効にする隔離スライスも許可する必要があります。シスコのセグメンテーション技術を使用したデータセンターにおいてセグメント ルーティングを使用することで、トランスポートでの上記の隔離スライスの実装が可能になります。シスコのアーキテクチャは、これらの 2 つのセグメンテーション手法を結合し、エンドツーエンドのセグメント化されたネットワークを提供し、脅威の検出と管理において可視性と俊敏性を実現します。セグメント ルーティングと TrustSec 全体で、ソフトウェア定義型セグメンテーションが提供されます。ソフトウェア定義型セグメンテーションにより、ユーザ、アプリケーション、デバイス向けのアクセス ポリシーを適用することが可能です。これは、IoT デバイス、M2M ベースのデバイス、エンタープライズ ネットワーク デバイスにも適用できます。5G アーキテクチャのデータセンター部分では、ソフトウェア定義型セグメンテーションでセグメント ルーティングが活用され、TrustSec を使用すると、シスコの Identity Services Engine によってセキュリティ グループ タグの定義・管理が可能です。Identity Services Engine では、TrustSec グループ情報を他のグループベースのポリシー スキームと共有することもでき、トラフィックのセグメント化と定義されたネットワーク インターフェイス間の通信の制限が可能です。このセキュリティ アプローチにより、長大な IP アドレスのリストに依存しがちなネットワーク セキュリティを柔軟性の高い自動化モデルに移行させることができ、未知の脅威や拡大する脅威に対してより優れた管理と効果的な対応が実現します。

バックホールと RAN アーキテクチャの進化により、エンドポイント保護や高度なマルウェア防御、DNS ベースの保護やスクラビング、IoT 用デバイスの安全な制御と管理、eNB と gNB 間または gNB 間のインターフェイスを保護する DDoS セキュリティや分散 SecGW 機能、悪意のあるサーバへアクセスするデバイスのブロック、エアー インターフェイス脆弱性対策としての RAN ベンダーによるジャミング対策制御技術、などのデバイス セキュリティの強化が求められています。

MEC サーバと分散型データセンターを保護するため、シスコでは、強化されたセグメンテーションを使用したバックホールと分散型データセンターによる脅威緩和を推奨しています。これは、ソフトウェア定義型セグメンテーションとユーザ アクセス制御、リモート データセンターに MEC サーバと vBBU が導入されている場合の DDoS 攻撃対策、リモート データセンター内のネットワーク フロー可視性の強化などによります。

モバイル ネットワーク コンポーネントが仮想化され、NFVI 上に展開したり、クラウド内のマイクロサービス コンポーネントとして展開したりできるようになるため、データセンターとクラウド コンポーネントを保護することが重要になっています。データセンターを保護するには、データセンター内のすべてのコンポーネントを、境界の安全とは別に保護する必要があります。NFVI インフラストラクチャのセキュリティが関連するコンポーネントとなり、NFVI ハードウェアのハードニング、E-W セキュリティの確保、VNF 間の隔離などの VNF/コンテナ セキュリティ、仮想機能における悪意のある動作の検出、サードパーティ製アプリケーションと API の保護、ネットワーク インターフェイスの保護とセグメント化、インターフェイスのローミングとピアリング、ユーザ アクセスとオーケストレーション レイヤの保護が関係します。

## SDN/NFV のセキュリティ

制約は、ソリューション全体にわたりさまざまな方法で適用されます。仮想機能の提供に使用するデータセンターまたはクラウドを検討し、サービス提供に対するシステム アプローチを形成する場合、セキュリティの分離、可視性および制御を保証するためのセグメンテーションが必要です。これらのセキュリティ制御の自動化、セキュリティ制御によって保護されるインフラストラクチャの変更、その他の主要なネットワーク運用とセキュリティ運用のタスクは、提供ソリューションの重要な機能です。SDN/NFV の保護に使用される 8 ステップのプロセスについて、以下の図で説明します。

セキュリティ アーキテクチャでは、NFVi の基盤を活用してレイヤ状の構成がとられ、そこにアプリケーション（EPC もしくはその他）が垂直方向に組み込まれる形になります。したがって、NFVi 自体、および NFVi 上で実行され NFVi 向けに編成されたアプリケーションを保護する上で、下の図に示されるような 8 ステップのプロセスを通じて、特にスライスを扱う場合に体系的なセキュリティ アプローチが提供されることになります。各ネットワーク スライスに含まれている特定の機能には、対象分野に特化した独自機能とセキュリティ上の懸念点が存在しますが、ネットワーク スライシングの「影響分野」を制御するための全体的なアプローチについては、下の図で説明されています。

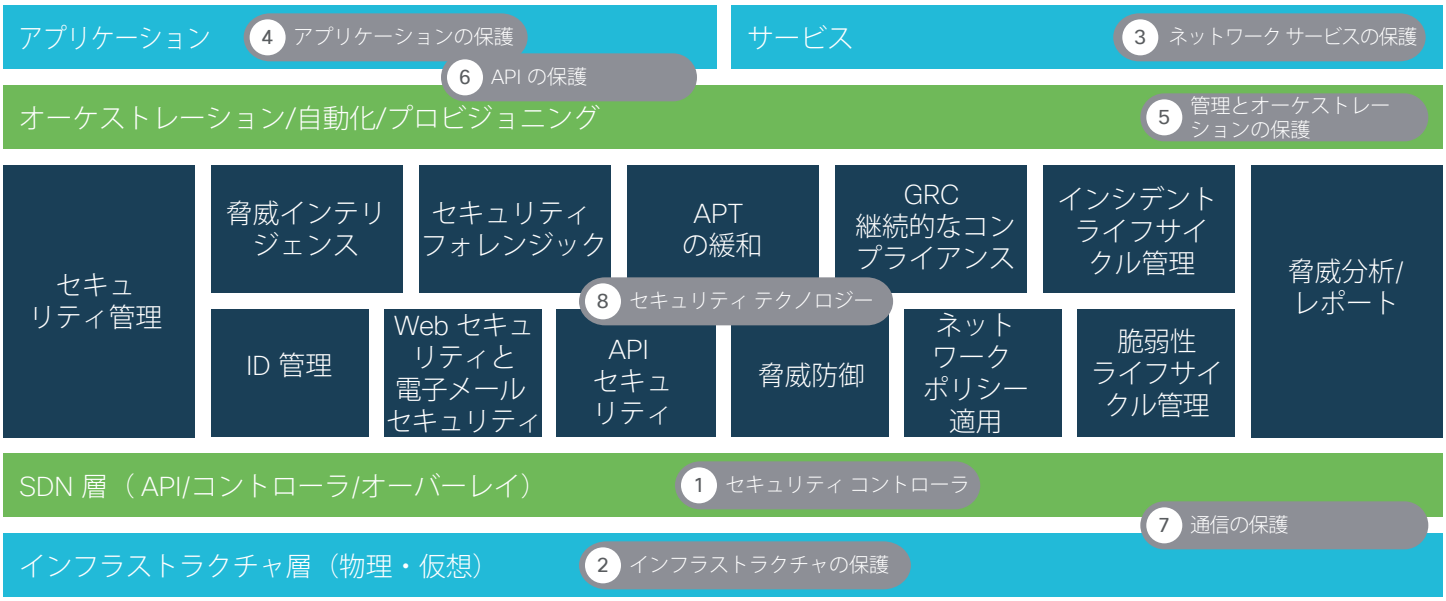



図 9.

今日のネットワークにおいては、「ネットワーク」そのものに対して、アプリケーションによる成果の実現と、そのアプリケーション固有の動作を安全に行えることが求められます。上の図では、ネットワークに対するアプリケーションからの要求を保護し、ネットワークでのプログラマビリティを通じて成果を実現するプロセスについて説明しています。SDN、NFV、仮想化を提供するまでに進化したネットワークにおいては、サービスの安全な配信に関連した 8 つの脅威の層があります。これはすべての脅威を網羅したリストではなく、脅威を示す関連カテゴリのグループです。

シスコは、図 10 に示すように、データセンターや通信事業者のクラウドにおけるオーケストレーション コンポーネントの保護など、エンドツーエンドのアーキテクチャを保護するための多層型セキュリティ コンポーネントを提供しています。

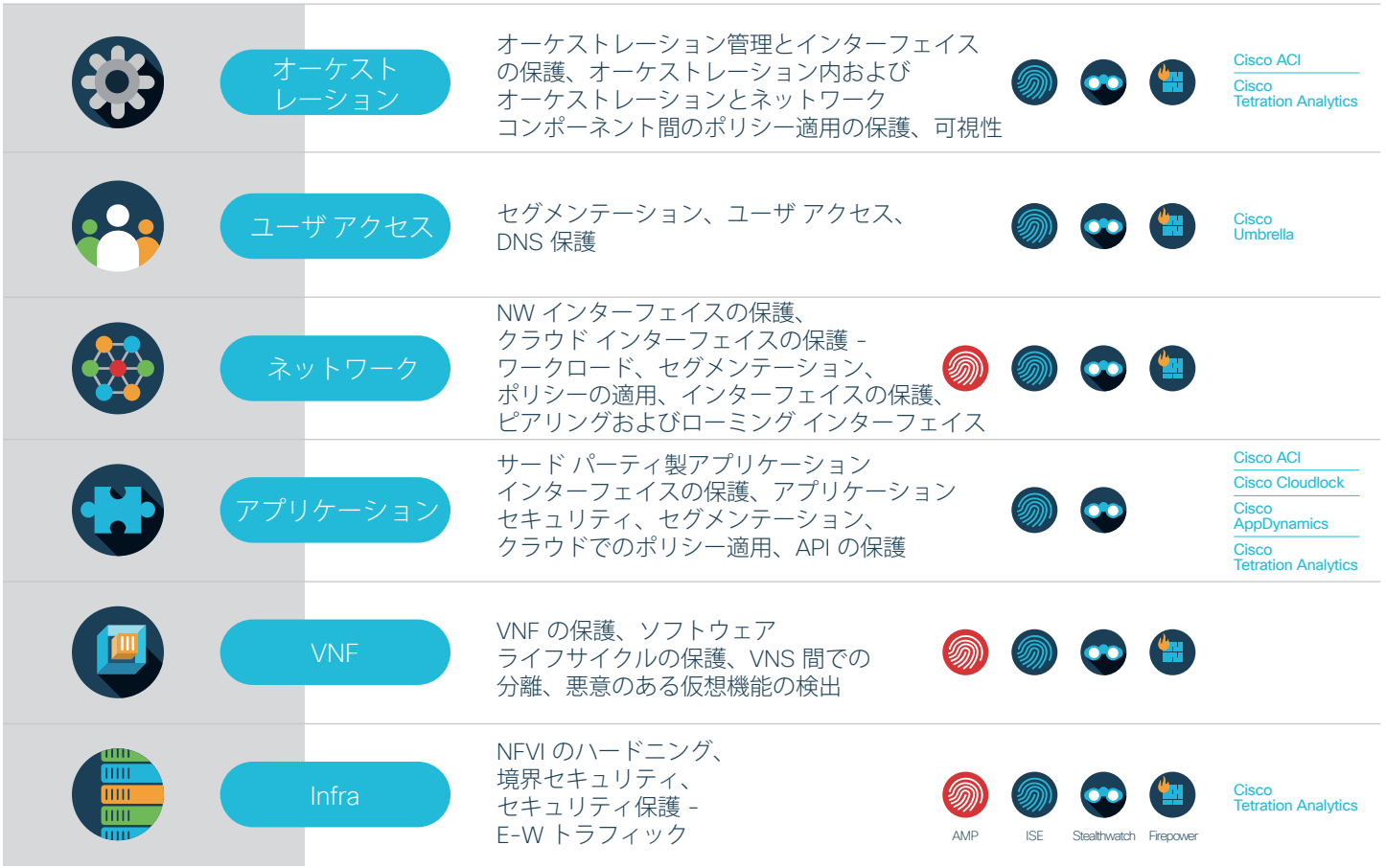



図 10.

ネットワークがハードウェアとソフトウェアの間で分割されたソフトウェア ベースのものとなることを考えると、オーケストレーション レイヤのセキュリティを確保することが、これからのアーキテクチャにおいて非常に重要になります。つまり、5G の導入に際しては、クラウドおよび仮想化通信テクノロジー、SDN、インダストリー 4.0（Internet of Things）などが考慮されることになり、ネットワーク管理とオーケストレーションに影響が及びます。

上の図は、5G とそのサービスが実行される分散データセンター インフラストラクチャの実現と運用に対する階層化されたアプローチを示しています。最下層では、Cisco Tetration を介してアプリケーション ホワイトリストとトラフィック パターンの可視性が提供されます。通信事業者が通常のベースラインにおけるパターンを可視化できるようになり、ゼロ トラスト アプローチやアプリケーション ホワイトリストの手法を利用して、安全な接続を実現できます。また、Tetration では、ある時間帯にインフラストラクチャでなにが発生していたかを再生できる、いわばネットワーク上のデジタル ビデオ レコーダのような機能も提供しています。インフラストラクチャ レイヤの上位には、オーケストレーション、サービスの提供や配置を行う NFV インフラストラクチャがあります。Cisco NFV インフラストラクチャは、マルチベンダーのオーケストレーション、サービス配置と保証、データセンターとクラウドのサービスに対する高度なネットワーキングをサポートします。インフラストラクチャ レイヤと NFV インフラストラクチャ レイヤは、ともに水平方向の基盤を提供します。そして、すべてのサービスが、この水平方向の基盤に対して垂直方向に組み込まれることになります。これにより、オーケストレーション機能において、シスコがネットワークとの緊密な統合を活用して分散型データセンター ノードなどの最適なワークロード配置を実現できるため、可能な限り脅威の発信元に近い適切な場所に適切なタイミングでセキュリティ制御を配置することが可能になります。

図 11 に示すように、オーケストレーション レイヤは、アーキテクチャの従来のコンポーネントと 5G コンポーネントを管理し、アーキテクチャのセキュリティ オーケストレーション機能と相互に作用したり、当該機能を包含したりします。

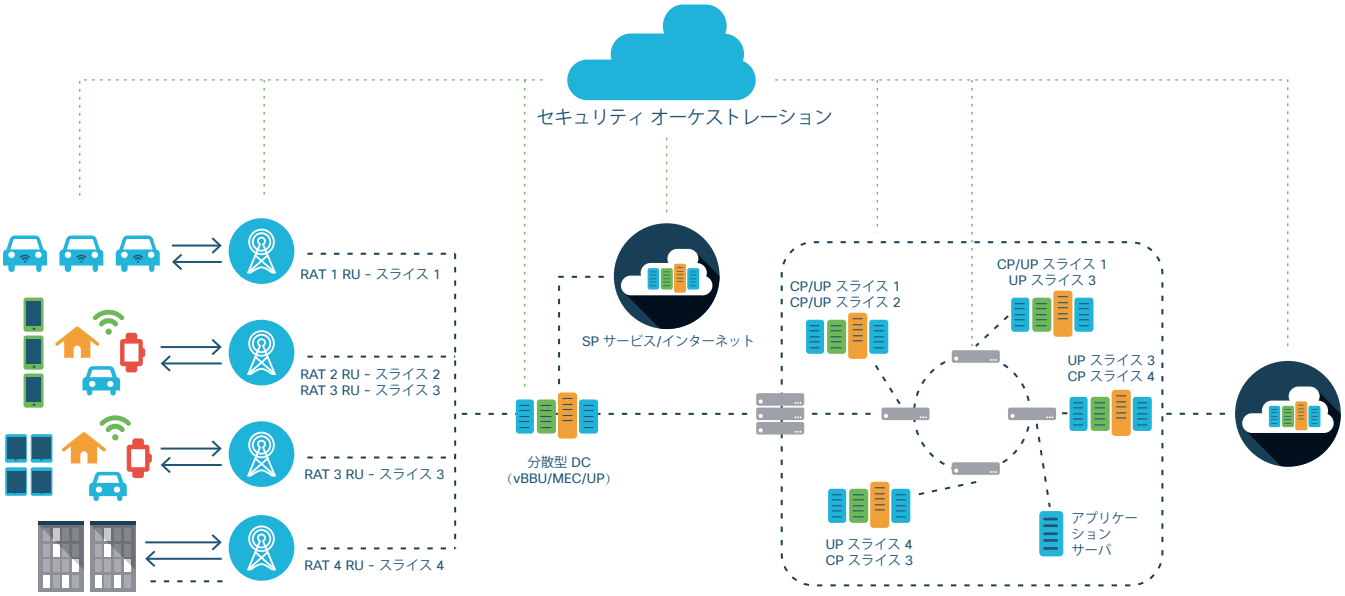



図 11.

これにより、適切なポリシー、セグメンテーション、ユーザ アクセス制御、可視性の向上など、オーケストレーション レイヤのセキュリティ強化が必要になります。また、シングル ポイント障害を防ぐという観点でオーケストレーション用アーキテクチャを考慮することも求められます。これは、以下に示すように、オーケストレーション アーキテクチャをクローズド ループとすることで実現できます。図 12 のようにメッシュ アーキテクチャを応用することで、セキュリティ ポリシーがオーケストレーション レイヤでグローバルに適用されるようにするだけでなく、個々のコンポーネントにも適用されるようにします。

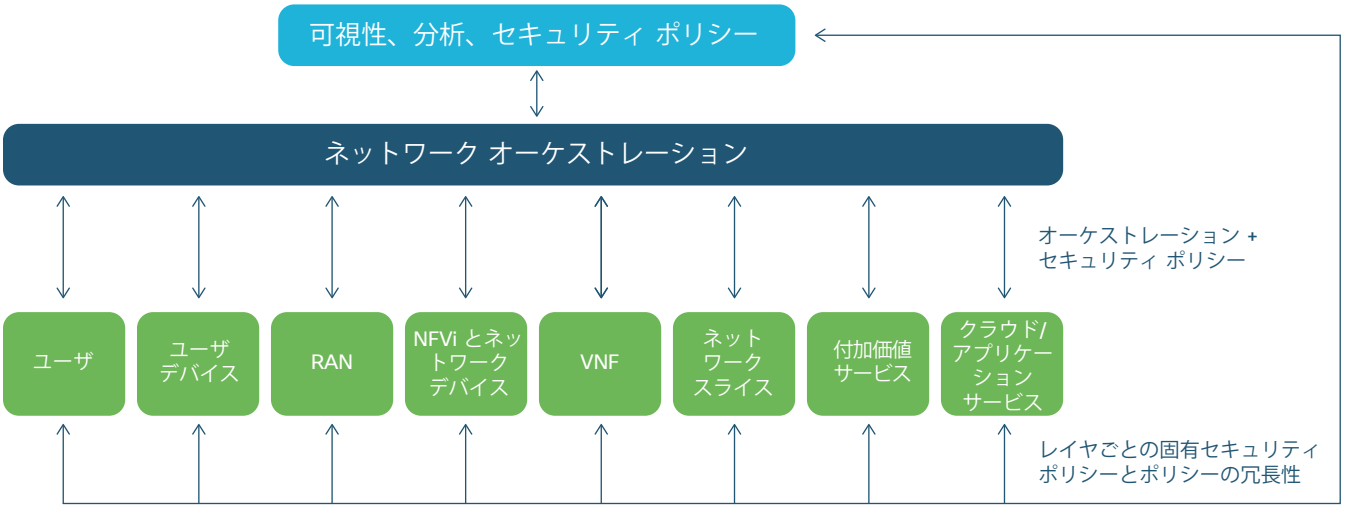



図 12.

スケーラビリティとリソースの効率的な使用という仮想化のメリットを活用すれば、図 13 に示すように、通信事業者のクラウド アーキテクチャがさらに進化し、モバイル ネットワーク事業者によって導入された既存のクラウド ベースのマイクロサービス コンポーネントにおける迅速なサービス展開と改善が可能になります。

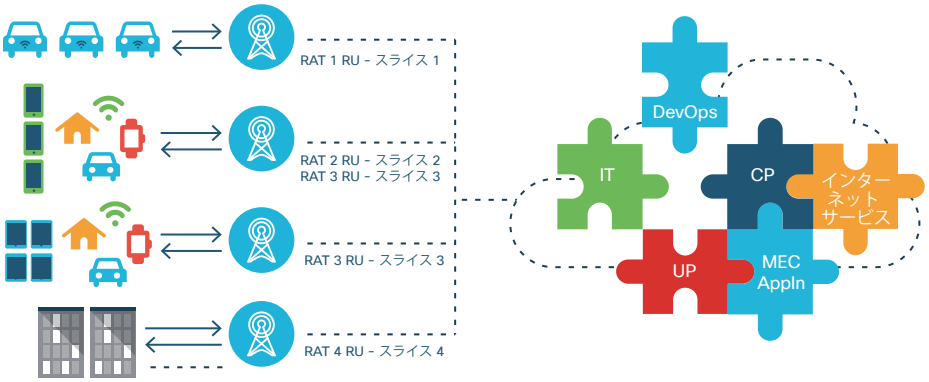



図 13.

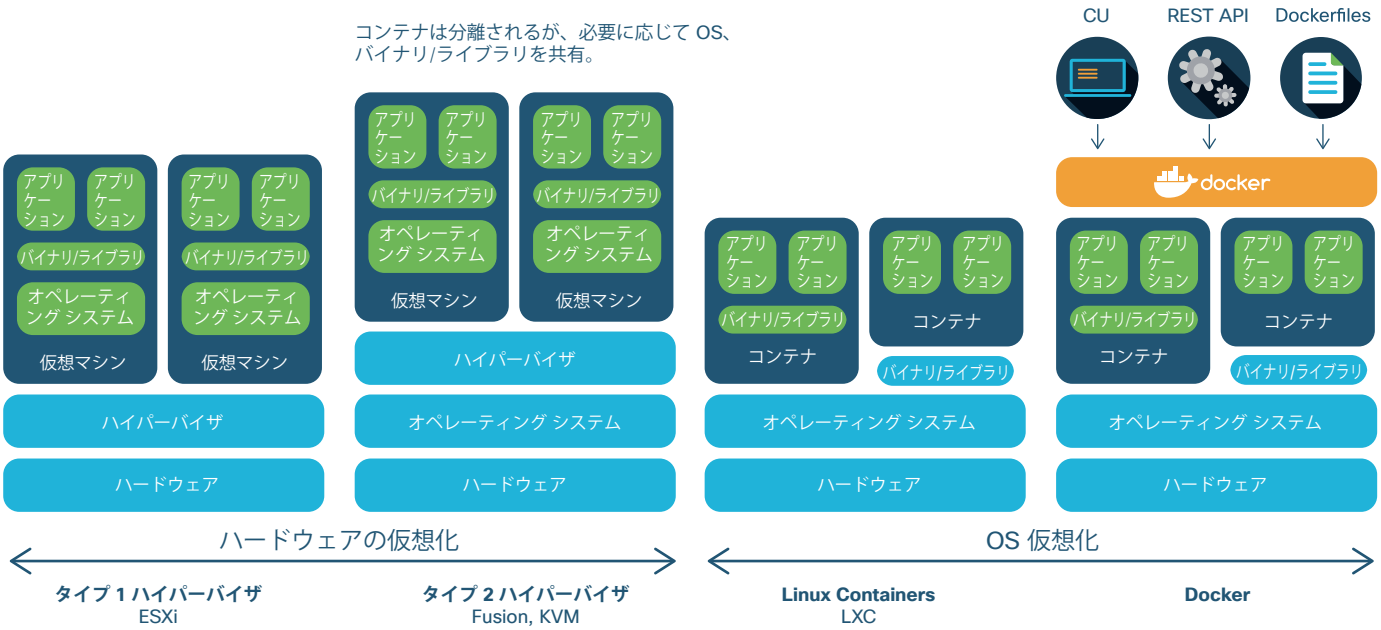
5G ネットワーク コンポーネントのクラウド展開により、クラウド インフラストラクチャ内のマイクロサービス コンポーネントにセキュリティ上の要件が生じます。これらは DevOps チームによって定期的に更新され、セキュリティ ポリシーがサービスに適用されます。サービスは、キャパシティ要件に応じて継続的にスケールイン/スケールアウトされます。Cisco Stealthwatch Cloud は、5G コンポーネント間のフローの可視性を強化でき、通信事業者のクラウド アーキテクチャ内で悪意のあるトラフィックからの脅威を緩和できます。

5G は仮想化サービス セットとして動作し、マイクロサービスとコンテナが統合されるため、DevOps におけるセキュリティ指針を考慮する必要があります。とりわけ SecDevOps モデルの検討が必要です。シスコは、CSDL（Cisco Secure Development Lifecycle）を利用して、開発、テスト、配信をすべてタイムリーに行い、開発時の各主要段階でセキュリティ上の要件が確実に満たせるようにしています。CSDL は、ネットワーク上の主な信頼済みの区分と、その上で実行されるアプリケーションが完全に保護されていることを、ドキュメント化されたプロセスとゲートによって担保します。

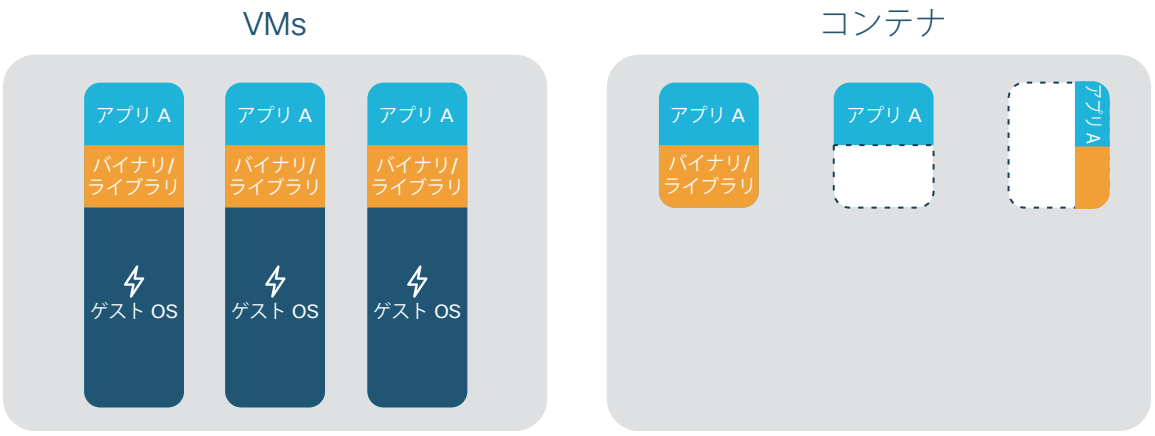
マイクロサービスの機能と特徴について詳しく説明します。

- アプリケーションを、相互接続レベルの低い小さなサービス セット（マイクロサービス）に分割
- 各サービスに、注文管理、報告、支払いなどのアプリケーション機能を個別に実装
- REST などの API を通じて、マイクロサービス間での通信を実行
- コンポーネント間の結びつきが緩やかであることから、異なる開発チームが独立して作業でき、迅速なコード リリースを行うことができるため、CI/CD が可能
- 通常、これらのマイクロサービスは、Linux または Docker コンテナでパッケージ化
- コンテナはステートレスであることが必須。Cassandra などと同様に、アーキテクチャの別のレイヤにデータは格納

仮想マシン間のトラフィック保護は、コンテナのセキュリティ保護よりも高度な機能になります。コンテナのマイクロサービス レベルでの可視性と制御に関する手法はありますが、運用上の BCP（ベスト コモン プラクティス）が必要です。次の図では、VM とコンテナの使用方法の違いを示します。




コンテナとマイクロサービスは、コンテナが仮想マシンに比べ運用面ではるかに効率的で「動作が軽い」ことから、今後のワークロードの仮想化を考えると好ましい方法と言えます。次の図で、その理由を示しています。




**VMS**
すべてのアプリ、アプリのコピー、アプリのわずかな変更のたびに、新しい仮想サーバが必要

**元のアプリケーション**
（スペース、リソースを消費する OS が不要。もしくは再起動の必要なし）

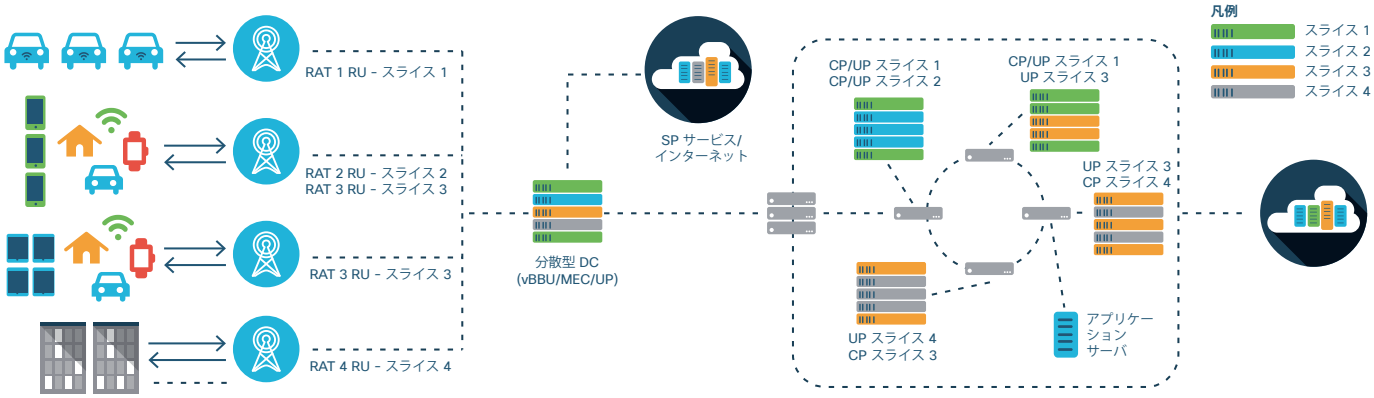
**アプリケーションのコピー**
OS なし。バイナリ/ライブラリを共有可能。

**変更されたアプリケーション**
ユニオン ファイルシステムでは、コンテナ A 間の差異のみを保存可能

サービスの保護方法を検討する場合、境界と信頼済み区分をすべて保護する必要がありますが、DevSecOps のセキュリティを考慮する際には、セキュリティ アプローチと制御についてさらに補完する必要があります。次のような点が挙げられます。

- CI/CD と統合されるアプリケーション セキュリティ
  - 静的コード分析（Veracode など）
  - 動的分析（Fortify WebInspect などの Web アプリケーション検査ツール）
- 自動化インフラストラクチャ
  - 自動化ツールとオーケストレーション ツールの整備
  - キーやロールの整備（Ansible with Vault）
- インフラストラクチャのセキュリティ
  - 構成管理とハードニング（Terraform、Ansible、Puppet）
  - ビルド プロセス中の Docker のセキュリティ検証

シスコは、モバイル ネットワーク事業者の進化するネットワークを保護するためのエンドツーエンドのセキュリティ アーキテクチャを提供しています。上の図は、ネットワークを保護するために展開できるさまざまなコンポーネントを示しています。




| デバイスの脅威 | エアー インターフェイスによる脅威 | RAN の脅威 | バックホールの脅威 | 5G パケット コアおよび OAM の脅威 | SGi/N6 と外部ローミングの脅威 |
|---|---|---|---|---|---|
| | | | Stealthwatch | | |
| | | | Umbrella | | |
| | | | Tetration | | |
| | | | Firepower | | |
| | | | ISE + TrustSec | | |
| | | | AMP | | |

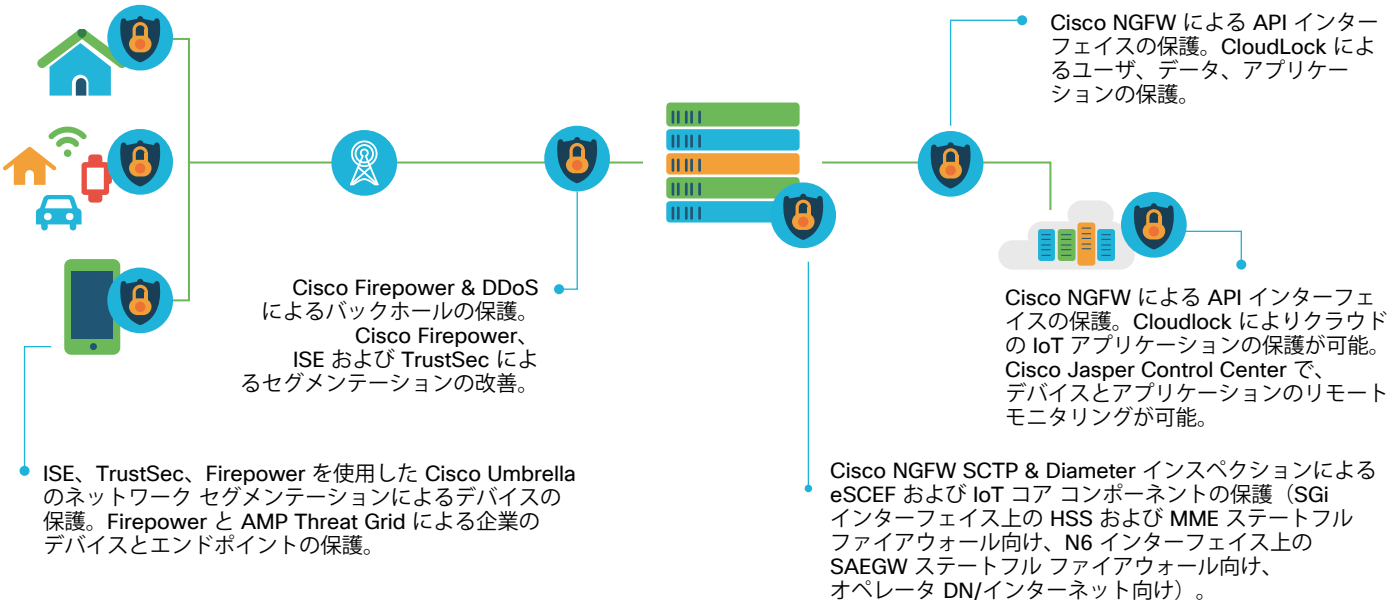



図 15. IoT 脅威の緩和

# 脅威/ダーク スレットの分析

ここまでで、5G ネットワークの適切なセキュリティ運用に関して、トラフィックの可視性がどれだけ重要であるかが把握できたことと思います。では、その可視性が失われたとすればどうでしょうか。トラフィックが悪意のあるものである、またはマルウェアを含んでいるかどうかを判断するにはどうしたらよいでしょうか。その答えは、Cisco ETA、つまり暗号化トラフィック分析を利用することです。https://www.cisco.com/c/dam/global/ja_jp/solutions/collateral/enterprise-networks/enterprise-network-security/nb-09-encrytd-traf-anlytcs-wp-cte-en.pdf を参照し、暗号化トラフィック分析について詳しく見ていきましょう。

暗号化トラフィックの急激な増加により、脅威の状況が変化しています。多くの企業がデジタル化されるにつれ、情報を保護する主な手段として、おびただしい数のサービスとアプリケーションが暗号化を利用しています。具体例として、暗号化トラフィックは前年比の 90 % 以上増加し、2015 年に 21 % だった Web サイトの暗号化トラフィックは 2016 年には 40 % 以上を占めています。Gartner は、2019 年には 80 % の Web トラフィックが暗号化されると予測しています。

ビジネスにおいてオンラインでの通信と処理にインターネットを利用する企業では、暗号化技術がプライバシーとセキュリティの実現に貢献してきました。同じ暗号化が使用され、ネットワーク事業者がトラフィックを確認して、それが悪質なものかどうかを判断することは非常に難しくなっています。モバイル、クラウド、Web アプリケーションは、キーと証明書を使って適切に実装された暗号化メカニズムによりセキュリティと信頼性を確保しています。しかし、暗号化の恩恵を受けるのは企業だけではありません。攻撃者はこの恩恵を、検出の回避と悪意のあるアクティビティの保護に活用したのです。

ネットワーク全体の可視化はますます難しくなり、従来の検出方法ではデータを検査対象にできないことが想定されます。デジタル ビジネスが暗号化によってどれほど保護されているか、または保護されていないかを同時に評価できるようにし、悪意のあるトラフィックと無害なトラフィックを分別するための評価も行う必要があります。Gartner は、2019 年に発生するマルウェアの活動の半数が何らかのタイプの暗号化を使ってマルウェアの配信、コマンド アンド コントロール、またはデータ漏えいを隠すと考えています。

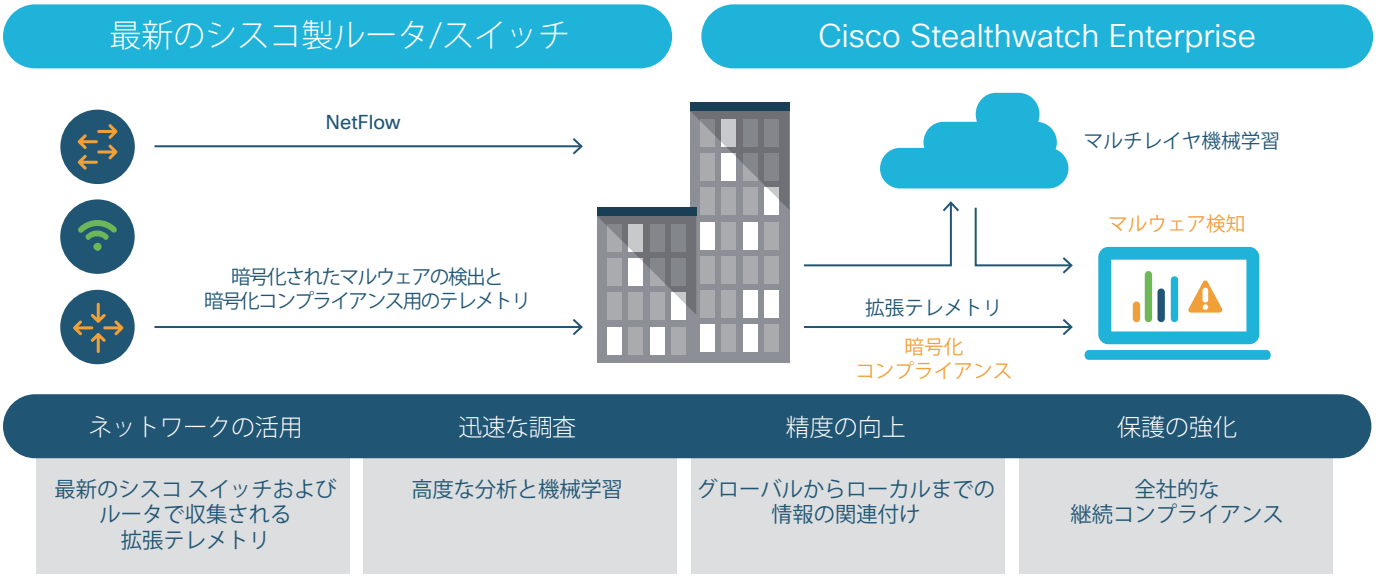
今ある組織の大多数が、暗号化トラフィック内の悪意あるコンテンツを検出するソリューションを持っていません。また、ネットワーク インフラストラクチャ全体に展開できるソリューションをネットワーク速度の低下なしに実装するツールやリソースが不足しています。

脅威の検査時に復号、分析、再暗号化を一括して行う従来の方法は、パフォーマンスやリソースを考えると、常に実践または実現できるとは限りません。ただし多くの場合、悪意のあるフローを特定する高度な分析技術を使って、復号技術による詳細な調査を実施できます。

どのようなときも、デジタル化されたビジネスがどれほど暗号化されているのか、またはされないままなのかを明確にはできません。トラフィックが暗号化されている場合、特定のセキュリティ ポリシーへの対応を求めるコンプライアンス要件を満たすように暗号化されるのが一般的です。

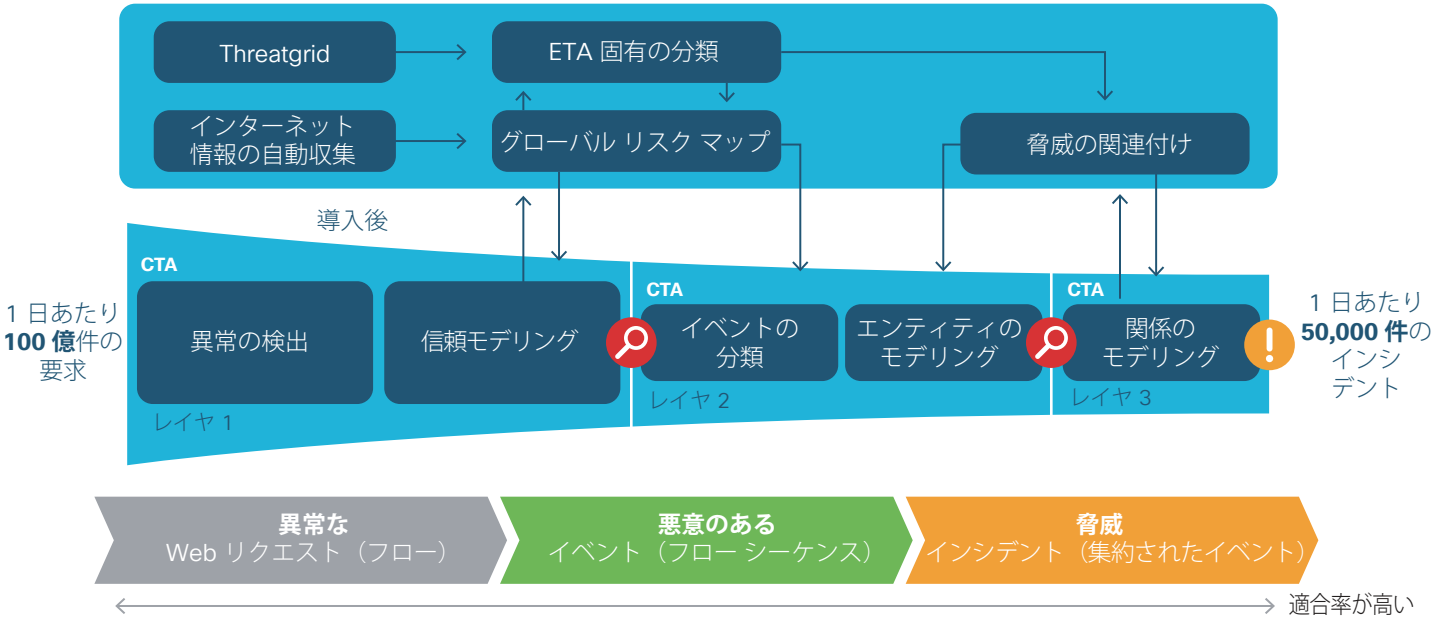
従来のフロー モニタリングでは、フローのアドレス、ポート、バイト数とパケット数のレポートによってネットワーク通信の概要を表示できます。それに加え、内部フロー メタデータまたはフローの内部で発生したイベントにまつわる情報は、フロー監視フレームワーク内で収集や保存、分析できます。トラフィックが暗号化されていると、DPI が今後実行可能ではないため、このデータは特に重要となります。暗号化トラフィック分析と呼ばれるこの内部フローのメタデータは、フロー内のメッセージの長さや到着時間など、プロトコル詳細とは独立した新しいタイプのデータ要素またはテレメトリを使って導き出されます。これらのデータ要素には、暗号化および非暗号化フローの両方に等しく利用できるという便利な性質があります。

暗号化トラフィック分析は、これらのデータ要素または内部フロー テレメトリを使って暗号化トラフィック内のマルウェア通信を特定する手段であり、一括復号を行わなくても暗号化フローの健全性を維持できます。

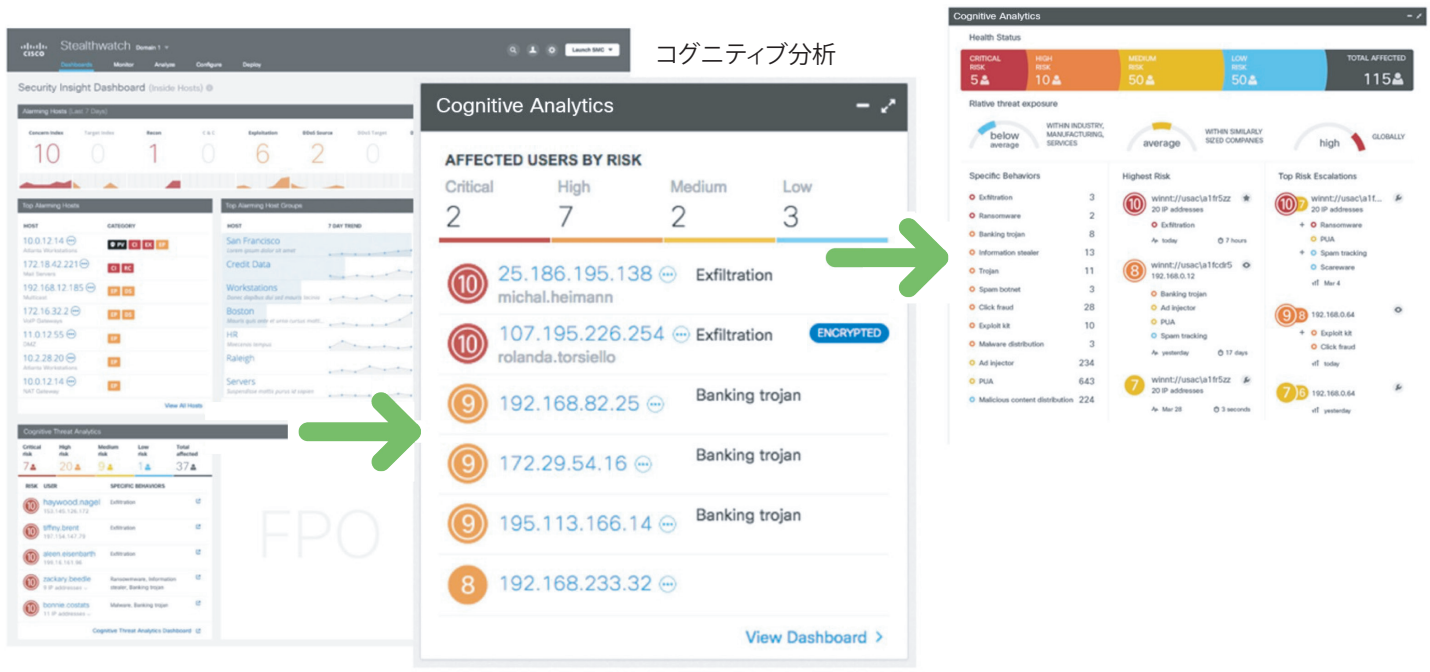



このホワイト ペーパーでは先に Stealthwatch について言及しましたが、興味深いことに、可視性を提供するプラットフォームが ETA 機能のコアであるという点では同じです。5G ネットワークのセキュリティ ファブリックを提供するツールの間で統合と継続性を維持するという点は、シスコの 5G セキュリティ アーキテクチャにおける重要な概念になります。

次の 2 つの図では、主な機能、機械学習の役割、ETA プロセスのさまざまな要素がどのように連携して機能するかについて説明しています。




拡張コグニティブ分析のダッシュボード ビュー




ETA は、セキュリティと保護されているネットワークをあらゆる段階で統合する必要がある理由を示した格好の例です。アプリケーション、クラウド、データセンター、ネットワーク、エンドポイントがすべて、安全な統合システムとして扱われます。セキュリティの観点から見た各部分の統合については、本ホワイト ペーパーの前半で説明しています。

# 比類のない脅威分析とインテリジェンス

Talos チームは、お客様の人材、データ、そしてインフラを保護します。Talos の研究者、データ科学者やエンジニアは、新旧の脅威情報をすべて収集することで、攻撃やマルウェアに対する保護を提供します。シスコのセキュリティ エコシステム全体を支えるのは、この Cisco Talos です。シスコのリサーチおよび脅威サービスは、プラットフォームに強化するだけでなく、通信事業者との統合における重要な要素でもあり、セキュリティ オペレーション センターの主要機能やインシデント対応の両面で、通信事業者の脅威対応システムを一層効果的なものとします。

Talos は、エンドツーエンドの脅威インテリジェンスと調査を提供します。


Talos の研究は包括的であり、通信事業者とその顧客に常に先んじています。



数十万の顧客


数千万のユーザ

197 億
1 日にブロックされる
脅威の数

300
脅威研究者


数百の
脅威分析エンジン

結論から言えば、5G のセキュリティは、エンドツーエンドの可視性と制御を備えた統合アプローチです。現在取り上げている重点分野について、以下の図でまとめています。


シスコのセキュリティ テクノロジーにより、検出までの平均時間はますます短縮され、通信事業者が安心してすぐにサービスを展開できるようになりました。