参考資料１

５Ｇセキュリティガイドライン第１版

2022 年 4 月 22 日

本文書は、総務省事業「５Ｇネットワークにおけるセキュリティ確保に向けた調査・検討等の請負」（受託者：KDDI 株式会社）により作成したものです。

1. 適用領域

1.1 本ガイドラインの目的

本書は、5G システム（5GS）のセキュリティを実際に確保するための包括的なガイダンスを提供する。本書で記載されているセキュリティ脅威と推奨される緩和策は、脅威モデリング分析及び、5G のラボ環境で実施された実践的なセキュリティテストの結果に基づく。

本書は、3GPP で定義されている 5G スタンドアロン（5G SA）システムと、5G 展開のための基盤を形成することが期待されている仮想インフラストラクチャ及び関連する管理システムに焦点を当てる。さらに、技術面のみではなく、5G サービスのセキュリティに影響を与える人やプロセスの側面も考慮されている。推奨されるセキュリティ対策は、関連する確立されたスタンダード及びベストプラクティスを参照し、ハイレベルに記述されている。

なお、本書は、総務省における 2019 年度、2020 年度、及び 2021 年度「5G ネットワークにおけるセキュリティ確保に向けた調査・検討等の請負」の業務の一環として作成されたものである。

1.2 本ガイドラインの想定読者

本書は、主に電気通信サービスプロバイダ及び 5G システムを展開して運用するその他の組織（以下「オペレータ」という）による使用を想定している。さらに、いくつかのセキュリティ対策は、5G システムコンポーネントのセキュアな設計、実装、及び保守に直接関連しているため、本書には、5G テクノロジーの実装者（以下「サプライヤ」という）に対する推奨事項も含まれている。

2. 序論

2.1 用語の解説

2.1.1 脅威の用語

(1) 脅威

脅威は、STRIDE-LM 脅威モデルに従って分類される。このアプローチは、一般的な STRIDE モデルをベースに、以下表 1 に示すハイレベルな脅威を考慮している。

表 1 ：STRIDE-LM の脅威モデル及び関連するセキュリティ目的

脅威	関連するセキュリティ目的
なりすまし	認証
改ざん	完全性
否認	否認防止
情報漏えい	機密性
サービスの拒否	可用性
特権の昇格	許可
ラテラルムーブベント	ネットワークの分離

一般的な STRIDE の側面に加えて、悪意を持つ行為者が既にシステムの一部を侵害している状況での攻撃拡大に起因する脅威も含まれる。5G システムの複雑性と複数の外部エンティティへの露出の増加を考えると、セキュリティを確保するためにはネットワークの分離とセキュリティ境界でのポリシーの実施が非常に重要である。

(2) 脅威アクター

脅威アクターとは、意図的または非意図的に、5G システムに対する脅威を実現化させる可能性のある個人またはグループをいう。その役割とアクセス可能なレベルに応じて、特定の攻撃ベクトルにアクセスし、異なるタイプの攻撃を実行できることが想定される。本書では、以下のように脅威アクターを分類する。:

- 内部アクター：
  - 不注意なインサイダー（Ⓝ）
  - 悪意のあるインサイダー（Ⓜ）
- 外部アクター：

- サプライヤ及びサービスプロバイダ（Ⓢ）
- 企業及び利用者（Ⓒ）

・ その他の外部関係者（Ⓞ）（個人ハッカー、犯罪組織等）

本書では、脅威アクターの能力レベルの違い（例えば、スクリプトキディ、専門スキルを持つ個人、国家関与アクター）は考慮せず、特定の脅威に対してセキュリティを確保するための基本的な保護策を概説することに限定している。読者は、それぞれの環境に合わせてカスタマイズした詳細なリスク評価を実施し、必要に応じてセキュリティ対策を強化することが推奨される。

2.1.2 セキュリティ対策の用語

（1）セキュリティ対策ドメイン

セキュリティ対策ドメインは、緩和すべきセキュリティ上の課題に関する性質に基づいて、セキュリティ対策をグループ化するために使用される。テクノロジーのみでなく、人やプロセスに関する考慮事項も含まれる。本書では、以下の対策ドメインを使用する。:

- 組織的な対策
- 人的な対策
- 運用における対策
- 物理的な対策
- 技術的対策

（2）制御タイプ

制御タイプは、情報セキュリティインシデントの発生に関して、特定のセキュリティ対策がいつ使用されるかを記述する。以下のタイプの制御を含む。:

- **予防的**：セキュリティインシデントの発生を防ぐために、インシデントが認知される以前に実施される制御
- **探知的**：セキュリティインシデントの発生時にインシデントを特定するために、システムの運用中に継続的に実施される制御
- **是正的**：セキュリティインシデントの影響を最小化し、不利な状況から回復するなどの目的で、インシデントの発生中及び発生後に実施される制御

（3）セキュリティの概念

セキュリティの概念は、特定のセキュリティ対策が特定のセキュリティ脅威にどのように対処するかを説明する。本書では、ISO/IEC TS 27110 [01]によって定義されている用語を使用し、以下のように概念を定義している。:

- **識別**：人、運用、能力、物理的及びソフトウェア資産に対するサイバーセキュリティリスクを管理するための必要な組織的な理解を深める。「識別」機能により、組織はリスクに重点を置き、優先順位を付けることができる。
- **防御**：重要なビジネスサービスを確実に提供するための適切な保護対策を検討し、実施する。「防御」機能により、組織は潜在的なサイバーセキュリティイベントがもたらす影響を抑制または阻止できる。
- **検知**：サイバーセキュリティイベントの発生を識別するのに適した対策を検討し、実施する。「検知」機能により、組織はセキュリティインシデントをタイムリーに発見できる。
- **対応**：サイバーセキュリティインシデントが発生した場合に対処するための適切な対策を検討し、実施する。「対応」機能により、組織はインシデントの影響を抑制または阻止できる。
- **復旧**：レジリエンスを実現するための計画を策定・維持し、サイバーセキュリティインシデントによって阻害されたあらゆる機能やサービスを復元するために適切な対策を検討し、実施する。「復旧」機能により、組織はサイバーセキュリティインシデントからの影響を軽減するために、タイムリーに通常のオペレーションにリカバリできる。

Note：「セキュリティ概念」と呼ぶ用語は、NIST Cybersecurity Framework [02]によって採用された用語である「セキュリティ機能」と同じ意味で使用できる。

2.2 本ガイドラインの構成

本書の残りの部分は、3 つの主要な章で構成されている。

第 3 章では、5G システムの技術的な基礎を紹介する。これには 5G システムのハイレベルなアーキテクチャ、仮想化されたネットワークの展開に関する考慮事項、及びサービスプロビジョニングモデルであるネットワークスライシングとマルチアクセスエッジコンピューティング等が含まれている。

第 4 章では、STRIDE-LM 脅威モデルに分類することで、本書の作成時に特定された脅威を要約する。各脅威には固有の脅威 ID が割り当てられ、その脅威を与える脅威アクター

にリンクされる。

第 5 章では、推奨されるセキュリティ対策について、2.1.2 項で概説する主要な対策ドメインに分類して説明する。各対策には、それを指示、実施することが期待される責任者が割り当てられる。また、対処すべき脅威も参照している。さらに、3.5 節で述べる 5G システムの影響評価に基づくハイレベルな優先順位付けが含まれている。

2.3 本ガイドラインの使い方

本書は 5G システムをセキュアに展開するための出発点となる。5G システムに対するセキュリティ上の脅威と関連するセキュリティ対策を構造化して提示することにより、共通のセキュリティ上の課題を特定し、対処するための実用的なアドバイスを読者に提供することを目的としている。本書では、各セキュリティ対策を詳細に明示するのではなく、読者がセキュリティ対策の優先順位付けと実装をそれぞれのシナリオと関連するセキュリティリスクに適合させることを前提としている。本書を組織の継続的なリスク管理活動の一部として使用するための典型的なアプローチは、以下のとおりである。

1. **識別する：**

   まず、脅威分析とリスク評価（TARA；Threat and Risk Assessment）を実施することで、個々の 5G システム展開におけるセキュリティリスクの状況を評価する。完全な詳細を目指すのではなく、ハイレベルな評価から始めて、反復的に改善する。この最初のステップで考慮すべき主な事項は以下のとおりである。:

   - 5G ネットワークのユーザーは誰か（公的なのか私的なのか等）
   - ネットワークインフラストラクチャとサービスへのアクセスが必要なエンティティはどれか（例えば、社内スタッフ、システムインテグレータ、3rd パーティのサービスインテグレーション）
   - 5G システム上にどのようなユースケースと関連データが伝送されるか（例えば、マシン間の通信、モバイルブロードバンド、音声）
   - 異なる 5G システムのコンポーネントはどこに実装されているか(プライベート、ハイブリッド、共有インフラストラクチャ等)

2. **優先順位付けする：**

   ステップ 1 の識別結果に基づいて、本書に記載されている関連するセキュリティ対策を選択する。提供された重要度を出発点として活用し、個々のリスクプロファイルに応じてセキュリティ対策の優先順位を調整する。このプロセスには、次のような様々な考慮事項が必要となる。:

   - 問題となっている 5G システム上の高いインパクト、発生可能性の高いリスクは何か
   - どのセキュリティ対策が何らかの形で既に存在しているか
   - 既存のセキュリティ対策はどれくらい成熟しているか

Note：正確なシナリオによっては、特定のセキュリティ対策が本書に含まれない場合や、記載されていることと関連性がない場合がある。この文書の目的は、脅威とセキュリティ対策

の完全なリストではなく、合理的なベースラインを提供することである。

3. **適応させ、拡大する：**

セキュリティ対策の優先順位が決定したら、具体的な実施計画を策定する。セキュリティ対策の章に示されている指針は、基本的なベストプラクティスの概要として理解するべきである。参照された外部リソースを使用して、既存のセキュリティ対策の完全性を確認し、個々のリスクプロファイルに基づいてそれらを補完する。

4. **レビューし、改善する：**

5G システムのリスク環境は、新たな脆弱性や、システムの利用方法や利用者の登場によって、常に進化している。このため、5G システムのリスク評価を定期的に見直し、セキュリティ対策の適切性を繰り返し評価する必要がある。

3. 主要技術の概説

本章では、本書の対象となる主要な技術を紹介する。**3.1 節**は、脅威モデルの一部である 5G ネットワーク機能をリストアップする。**3.2 節**では、ETSI NFV 参照モデルの主要なコンポーネントと、異なる展開シナリオにおける信頼関係について概説する。**3.3 節**では、ネットワークスライシングの概念を紹介する。**3.4 節**では、主要な MEC 構成要素と、このアーキテクチャ固有のセキュリティ上の考慮事項を説明する。**3.5 節**では、セキュリティ対策の優先順位付けを導くために、異なる 5G システムドメインのハイレベルな重要度を提供する。

3.1 5G システム

3.1.1 3GPP 5G システム

3GPP で定義されている 5G システムは、以下の 3 つのネットワークドメインを含む。:

- **User Equipment（UE）：**モバイル機器（ME）及び汎用加入者識別モジュール（USIM）で構成される
- **Radio Access Network（RAN）：**UE をコアネットワークに接続させる機能を持ち、複数の gNB で構成される
- **Core Network（Core）：**モバイルネットワークの主要機能（認証・認可、加入者のモビリティ、外部ネットワークとのデータ転送、レーティング、課金等）を可能にするネットワーク機能で構成される

本書では、上記の RAN（無線アクセスネットワーク）と Core（コアネットワーク）に焦点を当てる。5G 仕様では、RAN の分散配置が許可されているため、gNB はさらに以下のサブコンポーネントに分解される。:

- **Radio Unit（RU）：**デジタル・フロントエンド、物理層、ビームフォーミング機能を実装
- **Distributed Unit（gNB-DU）：**物理層、データリンク層、（実装に依存するが）gNB ロジックの一部を処理
- **Centralized Unit（gNB-CU）：**RRC や PDCP 等の上位層プロトコルを管理

5G コアネットワークは、パブリックモバイルネットワークの中枢機能を共同で提供する複数のネットワーク機能で構成されている。5G コアネットワークは、選択したネットワークサービスを 3rd パーティのアプリケーション機能や外部データネットワークに公開することで、柔軟性、スケーラビリティ、拡張性を可能にする API による通信を実

現している。

本書では、5G スタンドアロン（5G SA）展開の以下のネットワーク機能に焦点を当てる。:

- **AMF**：UE と AUSF 間の認証を仲介し、モビリティを管理する
- **SMF**：加入者のエンドツーエンド PDU セッションを管理する
- **AUSF**：UDM に格納されたデータに対して加入者認証を実施する
- **UPF**：UE と外部データネットワーク間のユーザープレーントラフィックを転送する
- **UDM**：ホームネットワークに加入者情報（恒久的なセキュリティ・クレデンシャルを含む）を保存する
- **SEPP**：相互接続メッセージにセキュリティを強制し、メッセージフィルタリングやレート制限等の更なるセキュリティ機能を実行する
- **NEF**：制御されたネットワークサービスについて、3rd パーティネットワークへの開示を可能にする
- **NSSF**：スライスを検出及び選択することで AMF をサポートする
- **AF**：ネットワークのコア機能以外のサービスを実行する汎用ネットワーク機能; 外部の 3rd パーティから提供される場合がある
- **NRF**：利用可能なネットワーク機能、サービス機能、及び NF インスタンスヘルス情報に関する情報を保存する
- **SCP**：コアネットワーク内の NF への接続性を提供する

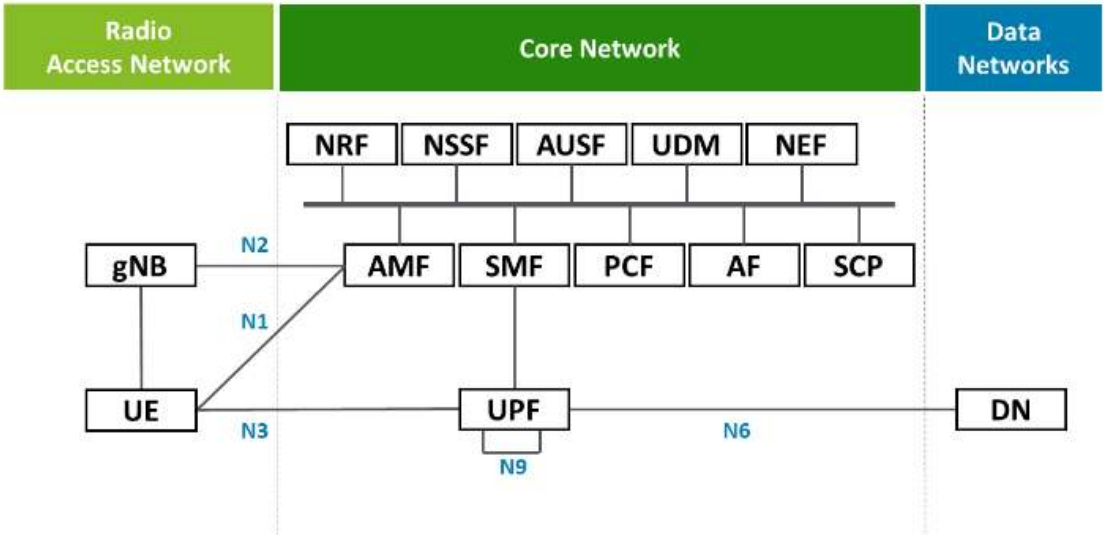

図 1：5G システムの概要

図 1 は、3GPP [03]で規定されている参照点でラベル付けされた通信の論理的な流れと、上述したネットワーク機能を示している。

5G 通信サービスを提供するために必要なこれらの専門的なネットワーク機能以外にも、モバイルオペレータは様々な支援システムを運用している。例えば、ネットワーク保守運用システム、加入者管理システム、課金システムがある。通常、個々のネットワーク要素を直接制御することはないが、これらのサポートシステムでは、ハイレベルなオーケストレーションとライフサイクル管理が行われる。したがって、それらのセキュリティとの関連性も考慮する必要がある。

3.1.2 O-RAN

O-RAN Alliance は、技術仕様の策定に取り組むもう一つの業界フォーラムである。3GPP とは対照的に、O-RAN は相互運用可能な無線アクセスネットワークの展開に焦点を当てている。「O-RAN」という用語は、O-RAN Alliance の特有の仕様やそれに準拠する機器を指すが、「Open RAN」 や「Open vRAN」等の他の用語が同じ意味で使用されることもある。前者は細分化された相互運用可能なすべての RAN 技術を説明し、後者はさらに仮想化の側面を強調したものである。以降、O-RAN 仕様の詳細について言及する場合を除き、一般的な用語である Open RAN を本書では使用する。

O-RAN Alliance は、可能な限り 3GPP システムに準拠した仕様の開発を目指している [04]。したがって、図 2 に示す論理アーキテクチャでは、両方の組織によって規定されたインタフェースを使用する。CU や DU 等の 3GPP コンポーネントに相当する O-RAN に加えて、O-RAN 仕様には、オーケストレーションや最適化タスクをサポートする付加的なシステムコンポーネントについても記載されている。このようなコンポーネントは以下を含む。:

- Service Management and Orchestration（SMO）Framework：
  ・FCAPS（障害、設定、アカウンティング、パフォーマンス、及びセキュリティ）を含む O-RAN コンポーネント、及び O-Cloud 管理とオーケストレーションの管理
  ・SMO フレームワークの一部または直接統合された Non-RT RIC 機能の提供
  ・管理タスクの最適化と自動化等の追加機能を提供するために、Non-RT RIC を使用するいわゆる rApps のホスト
- **Non-Real Time Radio Intelligent Controller（Non-RT RIC）：**
  ・関連する機械学習（ML）モデルの管理を含む RAN 最適化

・Near-RT RIC 情報のエンリッチメントのサポート

- **Near-Real Time Radio Intelligent Controller（Near-RT RIC）：**
  ・下位レベルにおいて応答時間の速い細粒度の（例えば個々のセルや UE に基づく）RAN 最適化
  ・O-RAN コンポーネントから収集したデータに基づいて追加機能を提供するいわゆる xApps のホスト；例えばハンドオーバーやトラフィックステアリング等の RAN 機能の最適化等がある

3GPP システムのための垂直に統合された従来の RAN と比較して、Open RAN と O-RAN は、安全にこれらを展開することにおいても影響を与える際立った特性を持っている。それらの特性は以下ように要約できる。:

- **Mix-and-Match Technology：**異なるベンダーから様々な RAN コンポーネントを調達することができる
- **Softwarization and virtualization：**多数のシステムコンポーネントはソフトウェア内に実装され、特別なハードウェアを必要としない為、COTS 技術でシステムコンポーネントを仮想化することができる
- **Intelligence inside the RAN：**O-RAN の重要なコンポーネントとしては、rApps と xApps によるインテリジェントな自動化と拡張性が挙げられる

Open RAN のセキュリティへの影響については、本書の付録 A にて詳しく説明する。

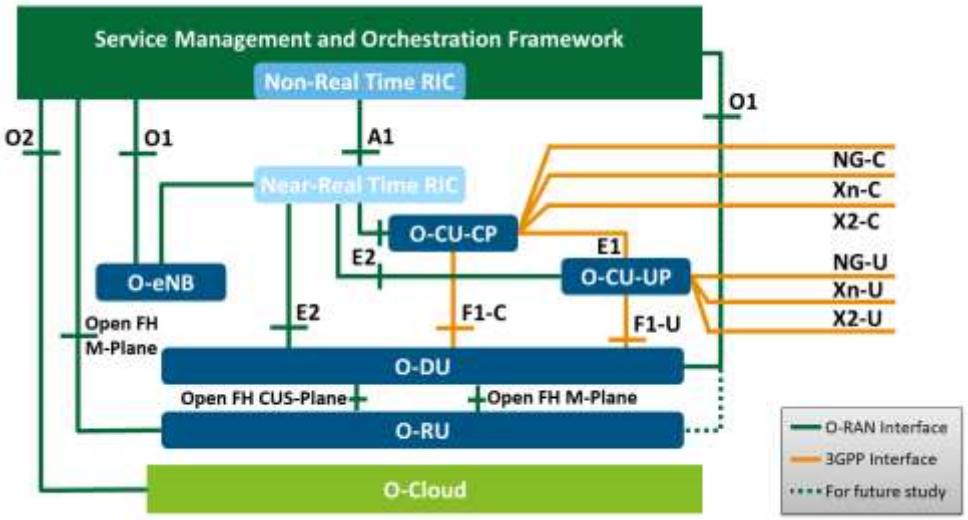

図２：O-RAN アーキテクチャ［04］

3.2 ネットワーク機能の仮想化（NFV）

ネットワーク機能の仮想化（NFV）は、仮想化と SDN をベースにした通信ネットワークを展開するためのアーキテクチャフレームワークである。従来の一体化（モノリシック）なアプライアンスの代わりに、仮想ネットワーク機能（VNF）は演算、ストレージ、ネットワーキング等の基本的なサービスを提供するコモディティハードウェアの共通仮想プラットフォーム上で動作する。

ETSI で規定されている NFV の参照モデルは図 3 に示される。

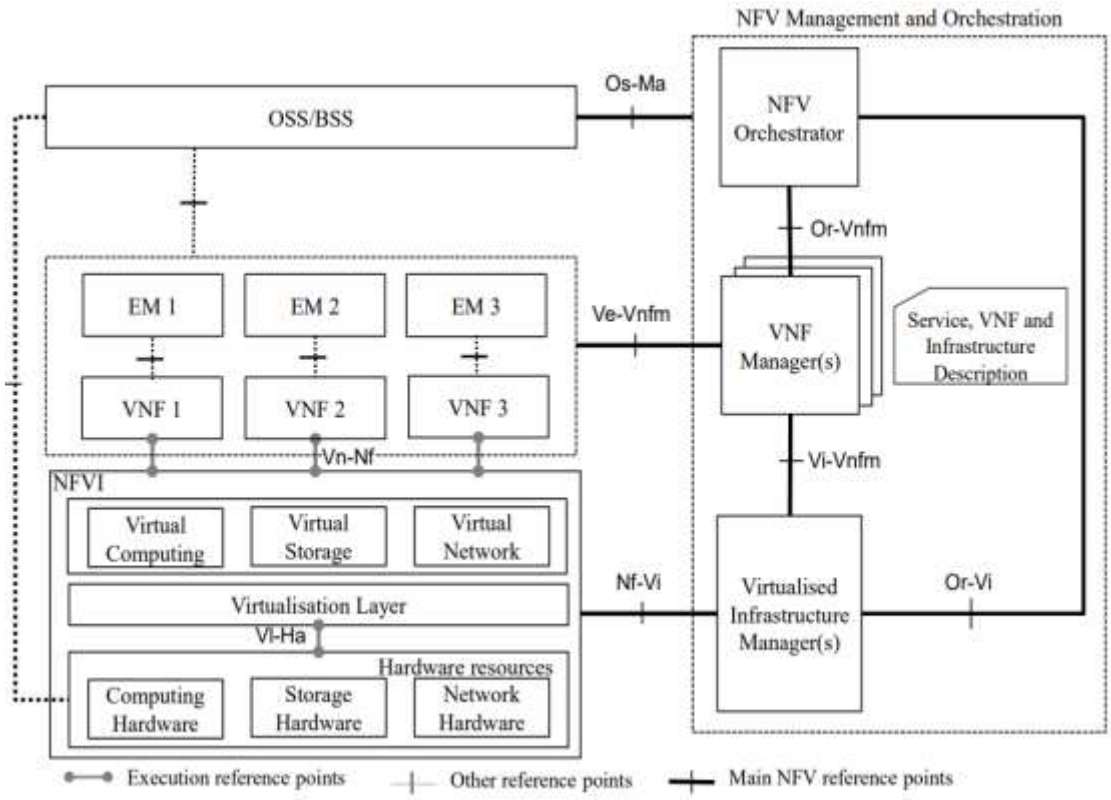

図 3：ネットワーク機能仮想化リファレンスモデル [44]

5G の展開では、多くの 5G ユースケースで必要とされる柔軟性と弾力性を実現するために、NFV に大きく依存することが予想される。セキュリティの観点から見ると、NFV への移行にはメリットとデメリットの両方がある。メリットとしては、共通のインフラストラクチャ・スタックとそれに伴う合理化された管理により、セキュリティポリシーの実施、設定とパッチ管理、ネットワーク全体の運用の可視性が大幅に向上する。デメリットとしては、仮想化レイヤでは、物理ホストと仮想ワークロードの両方を保護するためのセキュリティ

対策が必要となるため複雑さが増している。これは、仮想ネットワーク機能（VNF）オペレータと NFV インフラストラクチャ（NFVI）プロバイダが異なる場合に特に重要である。

本書では、実世界での展開の大部分をカバーしている NFV 環境における 2 つの潜在的な運用モデルを想定する。:

- モバイルネットワークオペレータが、NFVI や仮想ワークロード及び MANO（Management and Orchestration）を制御する
- モバイルネットワークオペレータが仮想ワークロードとネットワークオーケストレーションを制御するが、NFVI と関連する管理システムの操作は 3rd パーティに依存している

組織は、これらのオペレーティングモデルのいずれか 1 つのみに依存するとは限らない。例えば、中央ネットワーク機能のために独自のインフラストラクチャを管理しているネットワークオペレータが、マルチアクセスエッジコンピューティング等の特定のユースケースで 3rd パーティのクラウドサービスを利用する場合がある。

3.3 ネットワークスライシング

ネットワークスライシングは、指定された加入者グループに特定のサービスレベルの仮想プライベートネットワークを提供するサービス配信概念である。これらのいわゆるネットワークスライスは、共有 5G インフラストラクチャ上でプロビジョニングされ、他のデータトラフィックから分離される。すべての加入者からアクセスできる場合と、利用する前にスライス固有の追加認証が必要な場合がある。

スライス分離の実装方法によって、ソフトスライシングとハードスライシングを区別できる。ソフトスライシングとは、IP レイヤ上の専用トンネルを使用するなどして、異なるデータプレーンを論理的に分離することである。一方、ハードスライシングとは、各ネットワークスライスインスタンスに専用リソース（仮想または物理）を配備することである。それによって、2 つのスライス間のリソース競合を回避し、より高度な分離を実現する。

3.4 マルチアクセスエッジコンピューティング（MEC）

マルチアクセスエッジコンピューティング（Multi-Access Edge Computing；MEC）は、エンドユーザーに地理的に近い場所でのクラウドコンピューティング機能を提供することを目的としたアーキテクチャ概念である。ユーザープレーンアプリケーションをネットワ

ークエッジ上で実行することで、5G オペレータは超低遅延かつ高スループットの接続性を提供できる。このようなサービスから恩恵を得ると期待されるユースケースには、コネクテッドカー、仮想現実（VR）や拡張現実（AR)、クラウドゲーミング等がある。

MEC の概念はエッジでのワークロードの効率的な展開、拡張、移行を容易にする仮想化と密接に関連する。これは、図 4 に示す（ETSI NFV 参照モデルと大きく重なる）ETSI による MEC 参照モデルにも反映されている。

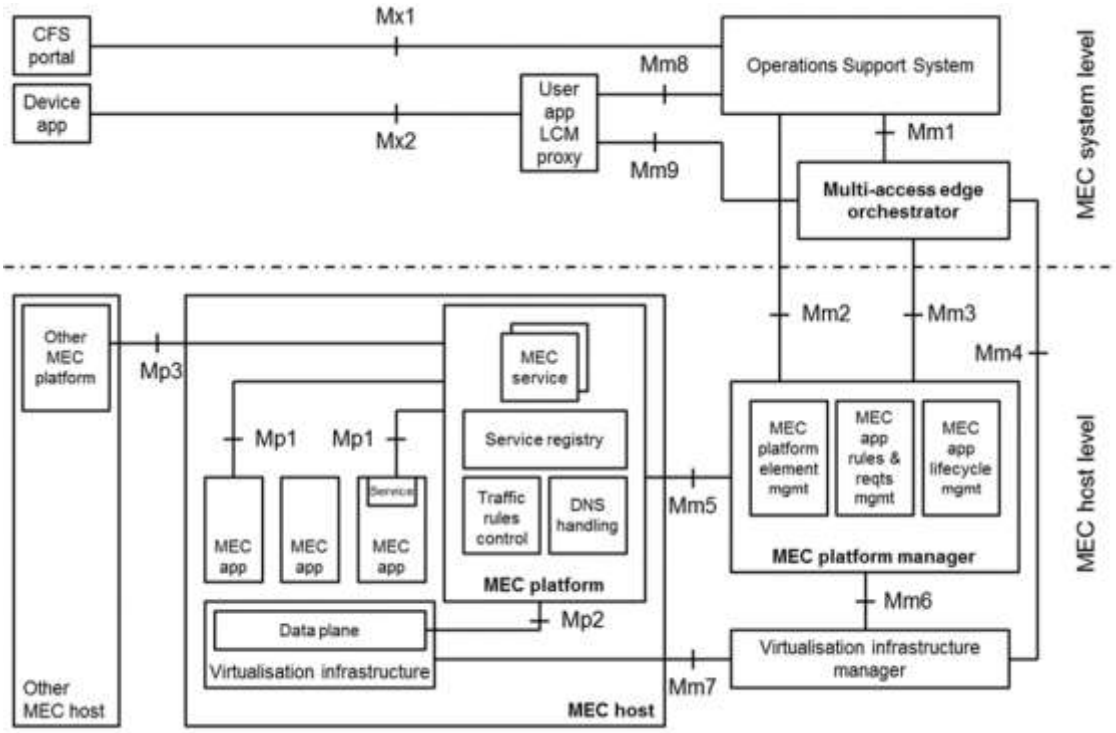

図 4：マルチアクセスエッジコンピューティング参照モデル［43］

NFV の展開全般に適用される考慮事項は別として、MEC サービス及び展開モデルは、セキュリティに関連するいくつかの特有の性質を示している。:

- MEC プラットフォーム上で動作する **3rd パーティ製ソフトウェア**は、標準的なネットワーク機能に課せられたセキュリティ要件を満たしていない可能性がある。MEC アプリはモバイルネットワークの不可欠な部分として配備されているため、加入者データとモバイルネットワーク自体の両方にセキュリティ上の悪影響を及ぼす可能性がある。
- **AF アシストルーティング** MEC アプリは、PCF を介して直接、または NEF を介し

て間接的にルーティングの決定に影響を与える 3rd パーティのアプリケーション機能（AF）を伴うことがある。この機能を悪用するか、または不十分なセキュリティのもとで運用することでサービス拒否（DoS）につながる可能性がある。

- 個々のローカルエリアデータネットワーク（LADN）の**コンピューティングリソースが制限**されていると、攻撃者は DoS 攻撃を容易に行うことができるようになる。しかし、このような攻撃が MEC サービスに与える影響は、地理的に狭い範囲に限定されると考えられる。
- エッジ展開での**物理的なセキュリティ対策が限られる**場合、中央の 5G コアネットワーク機能と比較して弱いレベルの保護になる可能性が高く、MEC プラットフォームはローカル攻撃を受けやすくなる。

3.5 5G システムドメインの重要度

特定の資産に関連するリスクの計算には、通常、潜在的脅威の影響と可能性の推定が含まれる。しかし、十分なデータがない場合、定量的評価に必要な信頼できる脅威の可能性の数値を得ることは困難である。逆に、可能性の定性的推定は、非常に主観的になってしまう。このような制限があるため、本書では、特定のシステムドメインが侵害された場合のセキュリティへの影響を分析することにする。5G システムのアーキテクチャと特定のネットワークエンティティによって処理されるデータに基づいて、潜在的なセキュリティへの影響を合理的な確実性で評価することができる。

5G システムにおけるセキュリティへの影響レベルは、加入者数及びインシデント時に影響を受けるデータの重要度と相関することが分かる。例えば、侵害されたコアネットワーク機能はおそらく多くの加入者に影響を与えるが、gNB は特定の地域の人々にのみ影響を与える。gNB におけるデータ漏えいは、センシティブなユーザー通信に影響を与える可能性があるが、コアネットワークにおける特定のネットワーク機能は、例えば、長期的なクレデンシャルデータの漏えい等、加入者通信全体のセキュリティに非常に大きな影響を与える。したがって、以下の表 2 は、5G システムドメインあたりのデータ漏えい、データ改ざん、及びネットワークエンティティの利用不可における推定される影響をまとめたものである。ドメインの全体重要度は、3 つのカテゴリの中で最も重要な影響の推定値に等しい。

このハイレベルな分類は、5G ネットワークにおけるサイバーセキュリティに関する EU の協調的リスク評価[45]に沿っている。2019 年に欧州委員会によって公表されたこの報告書は、欧州加盟国によって実施されたセキュリティリスク評価の結果である。

表１：５Ｇシステムドメインの重要度

システムドメイン	ネットワーク機能／エンティティの例	データ漏えいの影響	データ改ざんの影響	利用不可の影響	全体重要度
5G Core Network	AMF, SMF, UPF, AUSF, UDM, NRF, SCP, SEPP, etc.	Critical	Critical	Critical	Critical
NFV Management and Support Systems	NFV Orchestrator & Security Manager, VNF Managers, etc.	High	Critical	Critical	Critical
5G Radio Access Network	gNB, non-3GPP Access	High	High	High	High
(Non-MANO) Support Systems	Rating/Billing, etc.	High	High	Moderate	Moderate/High
Transport & Transmission Functions	Routers, Switches, etc.	Moderate	Moderate	High	Moderate/High
Internetwork Exchanges	External data networks, e.g., public internet, edge clouds	Moderate	Moderate	High	Moderate/High

図５は、5G システムの様々なドメインと、関連する重要度レベルの仮定をエンドツーエンドで示している。この図から、システムの完全性、可用性、及びデータの機密性に直接影響を与える中央ネットワークコンポーネントが最も重要な保護対象であると推論できる。

重要度評価は、セキュリティ対策の優先順位を示す指標として理解される必要がある。本書では表３に示すように、一般的にセキュリティ対策の優先順位は対象とするドメインのセキュリティの重要度と同じであると想定している。これらドメインにある特定のネットワーク機能または構成要素には、より低いか、またはより高い保護要件が存在する場合がある。

表３：重要度と対策の優先度の関係

ドメインの重要度	関連セキュリティ対策の（指標的）優先度
Critical	Critical
High	High
Moderate/High	Moderate/High

第 2 章で概説したように、個々のセキュリティ対策の優先度は、例えば、5G オペレータ及び 5G 技術サプライヤによって実施される包括的なリスク評価の一部として扱い、システムの状況に従って決定する必要がある。

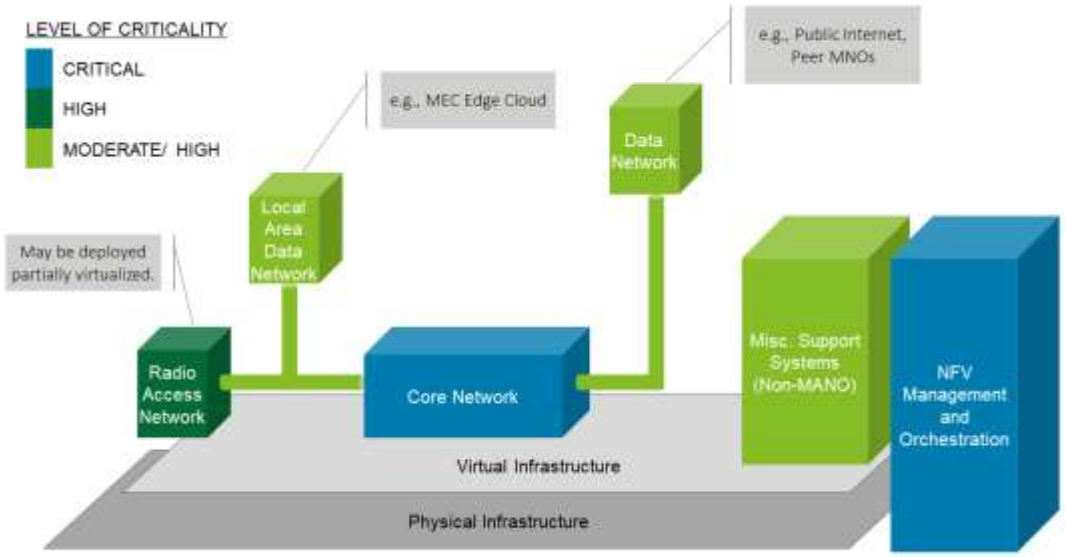

図５：5G システムにおける異なるネットワークドメインの重要度

4. セキュリティ脅威の分析

本章では、5G システムの特定された脅威及び STRIDE-LM モデルに基づいたサポートテクノロジーについて説明する。**4.1 節**は、5G システムのすべての領域において一般的に適用できる共通のセキュリティ脅威を記述する。**4.2 節以降**では、個々のシステムドメインにおける特定の脅威について説明する。

4.1 一般的なセキュリティ脅威

4.1.1 なりすまし

4.1.1.1 ネットワークのなりすまし

脅威 ID	#TC_S_01
関連脅威アクター	ⓂⓈⒸⓄ

通信パーティ間の認証が厳密に実施されていない場合、5G ネットワークの複数レイヤでプロトコルを狙ったなりすまし攻撃が発生する可能性がある。よく知られている例として、MAC のなりすまし、IP のなりすまし、ARP のなりすまし、DNS ポイズニング等がある。:

- MAC のなりすまし：攻撃対象デバイスの MAC アドレスを偽装することで、ネットワーク認証レベルのアクセス制限をバイパスする。
- IP のなりすまし：ヘッダー情報のソース IP を、偽の IP アドレスやなりすました IP アドレスに置き換える。
- DNS ポイズニング：DNS データ（IP アドレスやドメイン名）を改ざんし、詐欺サイトに誘導する。

4.1.1.2 ソフトウェアパッケージのなりすまし

脅威 ID	#TC_S_02
関連脅威アクター	ⓂⓈⒸⓄ

悪意のあるアクターは、標的組織の IT インフラストラクチャに侵入するために、3rd パーティ製のソフトウェアコンポーネントまたはソフトウェアアップデートになりすます場合がある。ソフトウェアのオリジナルソースを確実に検証できないと、サプライチェーンへの攻撃が誘導され、さらなる攻撃が実行される可能性がある。

4.1.1.3 フィッシング

脅威 ID	#TC_S_03
関連脅威アクター	ⓂⓈⒸⓄ

なりすまし攻撃は、必ずしもテクノロジーを標的としているわけではなく、人を欺こうとする場合もある。いわゆるフィッシング攻撃では、Web サイトのなりすまし、電子メールのなりすまし、電話を介した音声フィッシング（ビッシング）等の方法が使われる。このように、フィッシング攻撃はソーシャルエンジニアリングの特定の種類と考えることができる。フィッシングが成功すると、機密情報や制限されたサービスの利用等の特権を窃取され、以下を含む影響を与える。:

- ウェブサイトへなりすましアクセスされ、機密情報が侵害される
- 窃取されたパスワードでアカウントが乗っ取られ、制御喪失する。

4.1.2 改ざん

4.1.2.1 転送中のデータの改ざん

脅威 ID	#TC_T_01
関連脅威アクター	ⓂⓈⒸⓄ

データがネットワークを介して交換されるときの意図しない情報の改変は、プロトコル自体の完全性保護が欠如しているか、または受信側が受信した情報の完全性の検証に失敗したことによって起こる場合がある。管理トラフィック（管理権限アクセス、設定、ログデータ等を含む）にとって、転送中のネットワークデータの完全性を確保することが特に重要である。このような状況は、例えば以下の要因で起こり得る。:

- ネットワークプロトコルの実装または設定の不備
- 安全でない暗号アルゴリズムの使用
- 暗号鍵の侵害

4.1.2.2 物理プラットフォームの改ざん

脅威 ID	#TC_T_02
関連脅威アクター	ⓂⓈⓄ

攻撃者がセキュリティ・コプロセッサ（co-processors）や内部通信チャネル等の基本的なシステムコンポーネントを侵害しようとすることで、コンピューティングプラットフォーム自体を標的とすることもある。これらの攻撃は、システム全体の物理的な保護が不十分であったり、不要なハードウェア・インタフェース（デバッグポート等）が露出していたりすることで実現される。

4.1.2.3 ソフトウェアパッケージの改ざん

脅威 ID	#TC_T_03
関連脅威アクター	ⓂⓈⓄ

ソフトウェアパッケージ（ソースコード、バイナリ、コンテナイメージ、仮想マシンイメージ等）は、ライフサイクルの複数の段階で改ざんされる可能性がある。このような改ざんは、開発の初期段階から、調達、保管、配備、最終的な運用に至るまでの様々な過程で起こり得る。

このような改ざんは、例えば以下のような悪意のある行為によって引き起こされる。:

- 内部または外部の者によってソースコードが改ざんされる。
- ソフトウェア開発環境または構築環境において、最終版のソフトウェアがリバースエンジニアリングによって改ざんされる。

最悪のケースとしては、攻撃者はソフトウェア製品を改変して悪意のあるコードや脆弱性を「バックドア（偶発的または意図的なバックドア。例えば、5G システムへの不正侵入、情報搾取、不正操作等を可能とする不正プログラム）」として使い、サプライチェーンのさらに下流においてさらなる攻撃が実行されることが想定される。

4.1.2.4 保存されたデータの改ざん

脅威 ID	#TC_T_04
関連脅威アクター	ⓃⓂⓈⓄ

バイナリソフトウェアパッケージと同様に、システム上に保存されている他の形式のデータも改ざんされる可能性がある。特にシステムまたはサービスの設定ファイルを標的とする場合は、これらの情報を変更することで、後続のセキュリティ脅威を容易に発生させることができることから特に深刻である。例えば、以下のような行為によって引き起こされる。

- 運用者の不注意による意図しないデータ変更
- 5G ネットワーク機能やクラウド基盤を含むシステムコンポーネントを制御可能な内部アクターによる意図的なデータ改ざん
- 悪意ある侵入者による意図的なデータ改ざん

改ざんの標的となるデータとしては、ユーザーデータ、アプリケーションバイナリ、ログファイル、その他が含まれるが、特に深刻なのは、システムやサービスのコンフィグレーションファイルである。これらのデータの改ざんは、以降のセキュリティ脅威を容易に増進させるおそれがある。

4.1.2.5 データポイズニング

脅威 ID	#TC_T_05
関連脅威アクター	ⓂⓈⓄ

人工知能（AI；Artificial Intelligence）や機械学習（ML；Machine Learning）を活用したソフトウェアアプリケーション（セキュリティ関連アプリケーション等）が増えている。このクラスのアルゴリズムの機能は、AI/ML モデルのトレーニングに使用されるデータセットに大きく依存する。悪意のあるアクターがこれらのトレーニングデータに影響を与えると、例えば以下を例とするアプリケーション全体のパフォーマンス劣化を及ぼす可能性がある。この脅威は、組織自身が制御するモデルのみでなく、外部サプライヤのモデルにも適用される。

- スパムメールフィルタの判定を誤らせる
- 侵入検知の能力を弱めることで、例外検知に欠陥を与える

4.1.3 否認

4.1.3.1 ログデータの改ざん

脅威 ID	#TC_R_01
関連脅威アクター	ⓂⓈⓄ

信頼性の高いシステムログデータは、効率的なセキュリティ運用を行うための中核となる。したがって、この情報は、保存中及び転送中の改ざんから保護する必要がある。ログファイルの完全性を脅かす一般的な脅威として、データ発信元でのローカルストレージの使用、セキュアでないプロトコルを介したログファイルの転送、または中央のロギングサーバーの保護不備が上げられる。

4.1.3.2 アカウントの乗っ取り

脅威 ID	#TC_R_02
関連脅威アクター	ⓂⓄ

正規ユーザーのアカウントは、悪意のあるアクターに乗っ取られると、攻撃を容易に実行するために悪用される可能性がある。このような攻撃のよく知られた事例としては、ビジネスメール詐欺（BEC）とリモートアクセスシステムの悪用が上げられる。アカウントの乗っ取りは、脆弱な認証情報の使用、秘密情報の漏えい、多要素認証の欠如によって容易になる。

4.1.4 情報漏えい

4.1.4.1 暗号解読攻撃

脅威 ID	#TC_I_01
関連脅威アクター	ⓃⓂⓈⓄ

暗号化は、ネットワーク上で転送されるデータの機密性を担保するために重要である。ただし、適切に実装及び設定されていない場合、暗号化制御は、標的型攻撃に対して適切な保護を提供できず、場合によっては誤ったセキュリティ機能を与える可能性がある。

暗号化制御に対する一般的な攻撃には、次のものがある。:

- 衝突攻撃；例えばハッシュ関数に対する攻撃として、異なる入力から同一のハッシュ値を導出させるハッシュ衝突がある。
- Oracle 攻撃；Oracle の弱点を悪用してシステムや処理データを摂取する攻撃。
- 総当たり攻撃；トライ&エラーを繰り返すことで認証処理を突破する攻撃。

4.1.4.2 サイドチャネル攻撃

脅威 ID	#TC_I_02
関連脅威アクター	ⓈⒸⓄ

攻撃者は、秘密のチャネルを使用してセキュリティ対策を回避し、システム上の追加情報を窃取することができる。これにより、直接的なセキュリティインシデントを発生させるか、または攻撃者に追加情報が提供されることで、その情報を基にした連続攻撃にも使用されるおそれがある。考えられるサイドチャネルは次のとおり。:

- システムの電力消費
- 放出される電磁波
- 放出されるサウンド

サイドチャネル攻撃は、物理システムのみでなく、ネットワークスライス等の仮想化されたワークロードや通信インフラストラクチャにも関連する。例えば、同一ハードウェア上で動作するワークロード間の分離が不十分であると、隣接するワークロードに関するリソース利用や上記を例とする情報を得ることが可能となり、サイドチャネル攻撃が行われる可能性がある。

4.1.4.3 システムのフィンガープリンティング

脅威 ID	#TC_I_03
関連脅威アクター	ⓂⓄ

システムは、秘密のチャネルを介した場合よりも、よりあからさまに情報を晒すこともある。システムが適切に保護されていない場合、攻撃者はシステムの公開されたコンポーネントや機能、デバッグメッセージ、または一般的な応答動作を分析して、セキュ

リティ関連の情報を推測する可能性がある。特に、ネットワークプロトコルの実装(TLS、SSH、SNMP 等)、Web サーバー、アプリケーションサーバー等、ネットワークと接続するオペレーティングシステムサービスとアプリケーションに関連する。

4.1.4.4 悪意のあるソフトウェア

脅威 ID	#TC_I_04
関連脅威アクター	ⓃⓂⓈⒸⓄ

マルウェアとも呼ばれる悪意のあるソフトウェアには多様な形式があり、機密性を含む様々なセキュリティ目的を侵害できる。5G システムにおいては、ネットワーク製品や電子メールサーバー等のビジネスサポートシステムを標的にする場合がある。悪意のあるソフトウェアの一般的な例として、ルートキット、ワーム、トロイの木馬、ランサムウェア等がある。ランサムウェアについては、サービスの拒否に関する脅威分析の項において詳細に説明する。

攻撃者は、サプライチェーンのさらに下流にある政府機関や企業等の被害者を攻撃するために、悪意のあるソフトウェアをテクノロジベンダーに展開しようとすることもある。5G ネットワークにおいて期待される機密性、完全性、可用性が提供されなくなることで、5G のユースケースや提供されるアプリケーションの資産や利用者の生命に影響を与えることが考えられる。

4.1.4.5 ソーシャルエンジニアリング

脅威 ID	#TC_I_05
関連脅威アクター	ⓃⓄ

ソーシャルエンジニアリングとは、他人を欺いて機密情報を漏えいさせる行為を指す。フィッシングよりも一般的な用語で、様々な形式の情報収集や口実を伴い、最終的には攻撃を実施するために被害者に接触する。このような手法を用いて、攻撃者は、例えば 5G オペレータの従業員のアカウントを侵害し、特権を悪用してネットワークやサービスへの攻撃を試みる。

4.1.4.6 意図的なデータ侵害

脅威 ID	#TC_I_06
関連脅威アクター	ⓂⓈ

特権を持つインサイダーが、機密データを自ら侵害するか、3rd パーティによる不正アクセスを支援することで、意図的な情報漏えいを引き起こすケースがある。特権を持つインサイダーには、現役のスタッフ、現在勤務していないが情報にアクセスできる元従業員、及びサービスを提供するために一定レベルのアクセスを必要とするサービスプロバイダが含まれる。

4.1.5 サービスの拒否

4.1.5.1 Volumetric 攻撃

脅威 ID	#TC_D_01
関連脅威アクター	Ⓞ

Volumetric 攻撃は、他の通信ピアのサービス拒否を引き起こすために、標的となるシステムのネットワーク帯域幅をすべて使用しようと試みる。十分に高い帯域幅を到達させるために、これらの攻撃は通常、広く分布された多数のクライアントが標的システムに向けてトラフィックを送信する方法を使用して実施される。一般的な Volumetric 攻撃には、次のものがある。:

- ICMP フラッド；DoS 攻撃の 1 つの形態。攻撃者は大量の ICMP パケットを短時間に標的とするシステムに送信する。
- UDP フラッド；DoS 攻撃の 1 つの形態。攻撃者は大量の UDP パケットを短時間に標的とするシステムに送信する。
- リフレクション増幅攻撃；DDoS 攻撃の 1 つの形態。標的とするシステムのオーバーロード状態を引き起こすために、膨大な数の公衆システムにリクエストを送信し、その応答を標的となるシステムへ集中させる。

4.1.5.2 プロトコルに対する攻撃

脅威 ID	#TC_D_02
関連脅威アクター	◎

プロトコルレベルのサービス拒否攻撃（プロトコル DoS 攻撃）は、メインメモリやコンピューティング能力等、標的システム自体のリソースを占有することによって、サービス品質に悪影響を与えようとする。そのために、ネットワークプロトコルやその実装の弱点を利用することが多い。プロトコル DoS 攻撃の例を次に示す。:

- SYN フラッド；DoS 攻撃の 1 つの形態。攻撃者は大量の SYN パケットを標的とするシステムへ送り、多数のコネクションを設定させることでシステムのリソースを消費させる。
- IP フラグメンテーション攻撃；DoS 攻撃の 1 つの形態。攻撃者は、IP フラグメンテーションメカニズムを悪用して、ネットワークリソースの全帯域を消費させる。
- Ping of Death（PoD）；DoS 攻撃の 1 つの形態。標準外の不正な ping メッセージを送信する攻撃。

4.1.5.3 アプリケーション層に対する攻撃

脅威 ID	#TC_D_03
関連脅威アクター	◎

アプリケーション層に対する攻撃は、上位のシステム層を狙い、受信側のアプリケーションをクラッシュさせることでサービス拒否状態を作り出そうとする。したがって、このタイプの攻撃は、通常、攻撃可能な実装の脆弱性によって容易になる。アプリケーション層 DoS 攻撃のために利用される可能性があるエントリポイントとしては、アプリケーションサーバー、Web サーバー、ネットワーク上で通信する他のアプリケーションが考えられる。想定されるアプリケーションレイヤに対する DoS 攻撃としては、例えば以下が考えられる。:

- Slowloris 攻撃；DoS 攻撃の 1 つの形態。攻撃者は、大量の HTTP コネクションを標的とするシステムへ送り、すべてのリソースを消費させることでサービス停止を費い起こす。
- R.U.D.Y.攻撃；DoS 攻撃の 1 つの形態。攻撃者は、HTTP ポストメッセージを悪

用し、大量のデータを非常にゆっくりと送信することで、システムリソースを消費させる。

4.1.5.4 物理的な妨害行為

脅威 ID	#TC_D_04
関連脅威アクター	ⓂⓄⓈ

サービス拒否は、コンピューティングプラットフォーム自体またはそれに接続したネットワークインフラストラクチャに対する物理的損傷によって引き起こされる場合もある。特に、従来の集中型ネットワーク機能よりも物理的な保護が少ないネットワークエッジ（RAN や MEC コンポーネント等）でのシステム展開に関連する。また、5G における RAN アーキテクチャの進化により、アタックサーフェイスが増加する可能性がある。さらに、妨害行為や破壊行為の対象となる可能性があるものとしては、ネットワークのコンポーネント自身のみではなく、電源等のサポートシステムやユーティリティも上げられる。

4.1.5.5 ランサムウェア等の行為

脅威 ID	#TC_D_05
関連脅威アクター	ⓃⓄ

ランサムウェアは、システムデータを暗号化し、ロック解除のための身代金が支払われない限り、ユーザーのアクセスを制限する特別な形式の悪意あるソフトウェアである。一旦システムが感染すると、通常は同じネットワーク内の他のホストにも拡散する。

電子メールの添付ファイルや、web サイトの広告またはリンクに不正なスクリプトを埋め込むことで、従業員をだまし、知らないうちにランサムウェアをシステムにダウンロードさせる行為に誘導する。また、技術管理用のチャネル等、外部のサプライヤから顧客へ別のチャネルを介して拡散する可能性がある。IT ドメインにおける初期のランサムウェア感染は、5G ネットワークへも同様に広がる可能性があり、ネットワークサービスの可用性に影響を与えることが考えられる。

悪意のあるソフトウェアの感染によって、攻撃者は様々な脅迫により、身代金を支払

わせる。例えば、ネットワークサービスを妨害する攻撃、アカウントの乗っ取り、機密情報を公開するなどが考えられる。さらに、こういった攻撃は、異なる手法が二重三重に組合されて実行される。

4.1.5.6 法律違反

脅威 ID	#TC_D_06
関連脅威アクター	Ⓞ

公共のモバイルネットワークを運用するための基本的な前提条件は、現地の法律や規制のコンプライアンスに遵守することである。法規制が規定した基本的なセキュリティ要件が効果的に実施されない限り、モバイルネットワークサービスの提供は許可されない。

4.1.6 特権の昇格

4.1.6.1 垂直的な特権の昇格

脅威 ID	#TC_E_01
関連脅威アクター	ⓂⓄⓈ

垂直的な特権の昇格（権限昇格）は、本来の制限よりも高いレイヤの権限を取得することを目的としている。この攻撃では、まず攻撃者は標的システムへの限定されたアクセス権を持っていることが前提となる。攻撃者は、セキュリティ対策を侵害または回避することで、追加の権限を取得できる。

4.1.6.2 水平的な特権の昇格

脅威 ID	#TC_E_02
関連脅威アクター	ⓂⓄⓈ

水平的な特権の昇格は、他のパーティに限定されたリソースまたはサービスに関する

アクセス取得を目的とするなりすまし攻撃の一種であり、アプリケーションはユーザーとの通信において、誤ったセキュリティコンテキストに基づき正規のアクションを実施する。攻撃者は、アカウントの乗っ取り（4.1.3.2 項参照）に成功すると、水平的な特権の昇格を試み、結果として、正規のユーザーが受けられるサービスを攻撃者に提供することとなる。

4.1.7 ラテラルムーブメント

4.1.7.1 ネットワークラテラルムーブメント

脅威 ID	#TC_L_01
関連脅威アクター	ⓂⓈⒸⓄ

悪意のあるアクターは通常、最初の侵入後にネットワーク内での活動範囲を拡大しようとする。検知を回避しようと試みながら IT インフラストラクチャ内を移動する行為を、ネットワークラテラルムーブメントと呼ぶ。これは、例えばサプライチェーンのある時点で発生した最初の侵害の後に続いて、接続された顧客環境までに影響を与えるなど、組織の境界を越えて拡散する攻撃も含まれている。

悪意のあるアクターと同様に、悪意のあるソフトウェアも組織の IT インフラストラクチャ内でさらに拡散する可能性がある。これを行うためには、必ずしも直接的なネットワーク接続を当てにするとは限らず、代わりに、リムーバブルストレージメディア、電子メール、共有ストレージ等の代替チャネルを介して広めることができる。

4.2 NFV インフラストラクチャと MANO に対する脅威

4.2.1 なりすまし

4.2.1.1 NFV ワークロードのなりすまし

脅威 ID	#TM_S_01
関連脅威アクター	ⓂⓈ

NFVI の配備時にソフトウェア証明書の検証に失敗すると、攻撃者は、関連する MANO コンポーネントを制御して、有害な NFV ワークロードをプロビジョニング（投入）しようとする可能性がある。このようなインシデントは、例えばインサイダーや 3rd パーティのシステムインテグレータにより意図的に発生する場合や、VNF イメージが改ざんされた時に意図せずに発生する場合がある。2 つ目のシナリオについては、「VNF イメージの改ざん」を参照されたい。

4.2.2 改ざん

4.2.2.1 VNF イメージの改ざん

脅威 ID	#TM_T_01
関連脅威アクター	ⓂⓈⓄ

ソフトウェアの改ざんにより、VNF イメージへの悪意のあるコードの挿入や VNF イメージの脆弱性につながる可能性がある。これは、サプライヤから顧客へソフトウェアが提供される際や、ソフトウェアが顧客の VNF イメージライブラリに保存されている間等、サプライヤの IT 環境の様々なポイントで発生する。攻撃者がこれらのいずれかの段階で VNF イメージを改ざんすると、その VNF イメージから作成されたすべての VNF インスタンスが影響を受ける。

4.2.2.2 MANO コンポーネント間の転送データ改ざん

脅威 ID	#TM_T_02
関連脅威アクター	ⓂⓄ

MANO コンポーネント間の完全性保護の欠如によって、悪意のあるアクターに転送中のデータを改変されてしまうと、ネットワークの大部分に影響を及ぼすセキュリティインシデントにつながるおそれがある。このようなデータには、ネットワーク（セキュリティ）ポリシー、管理及びオーケストレーションコマンド、モニタリングデータが含まれる。この脅威は、特に、MANO エンティティが個別のエンティティによって制御され、トラフィックがセキュリティドメイン間で交換されるシナリオにおいて深刻である。例として、5G オペレータによるハイレベルのネットワークオーケストレーション、外部インフラストラクチャプロバイダによる NFVI オーケストレーション等が考えられる。

4.2.3 情報漏えい

4.2.3.1 信頼できない NFV ワークロード

脅威 ID	#TM_I_01
関連脅威アクター	ⓂⓈ

仮想化レイヤは、ホスト OS と物理プラットフォームを NFV ワークロードから分離することで、重要なセキュリティ機能を実装する。しかし、VNF 内の特定の機能を有効にするためには、場合によっては、仮想化層を介さずにプラットフォームの一部を直接仮想ワークロードにさらす必要がある。このような機能は、増加するホストシステムへのアクセスを信頼されていないソフトウェアに悪用されるリスクを増大させる。例としては、以下のようなものがある：

- シングルルート I/O 仮想化（SR-IOV）により、仮想化されたソフトウェアが物理ネットワークハードウェアに直接アクセスできるようになる
- ホストとゲストのオペレーティングシステム間の共有フォルダ
- ホストソケットへの直接アクセス（Docker デーモンソケット等）

4.2.3.2 VNF スプロール

脅威 ID	#TM_I_02
関連脅威アクター	ⓈⓃ

仮想環境の配備により、開発者や運用スタッフは必要に応じて追加のリソースを容易にプロビジョニングできる。ただし、新しいワークロードを無制限に作成すると、全体に一貫したセキュリティ基準を強制することが難しくなり、インシデントの検知や対応等の運用上のセキュリティタスクが複雑になる。アタックサーフェイスが増加するに伴い可視性が低下すると、エコシステム全体のリスクが増加することになる。

4.2.4 サービスの拒否

4.2.4.1 NFV ワークロードによるリソースの枯渇

脅威 ID	#TM_D_01
関連脅威アクター	ⓃⓂⓈ

NFVI を介した仮想化ワークロードに対する使用量の割り当てが不十分であると、リソースが枯渇し、全体的なサービス品質に悪影響を及ぼすことがある。これは、悪意のあるワークロードが意図的にサービスの拒否を発生させようとすることのみでなく、正当なワークロードが基本的な使用率より多くのリソースを消費することによっても発生する場合がある。このようなリソース割り当ての失敗は、仮想化レイヤにおけるソフトウェアの脆弱性や、単に 5G オペレータによる不適切な設定によって引き起こされる可能性がある。

4.2.4.2 サービスプロバイダの利用不可

脅威 ID	#TM_D_02
関連脅威アクター	Ⓢ

NFV インフラストラクチャが外部インフラストラクチャプロバイダによって提供されるシナリオでは、モバイルネットワークサービスは 3rd パーティの可用性に大きく依

存する。したがって、提供されたインフラストラクチャが使用不可になる等、3rd バーティィによるサービスレベル契約（SLA）の違反は、モバイルネットワークに脅威をもたらす。

4.2.5 特権の昇格

4.2.5.1 ゲスト―ホスト間のエスケープ

脅威 ID	#TM_E_01
関連脅威アクター	ⓒⓞ

ハイパーバイザ及びコンテナエンジンは、仮想ワークロードをホストシステムから分離し、双方を仲介するソフトウェアレイヤである。この分離が仮想化されたワークロードによって任意のポイントで破られたり、回避されたりすると、悪意のあるソフトウェアが NFVI を侵害する可能性がある。ハイパーバイザの侵害は、ホストマシンのソフトウェアスタックに潜在する様々な脆弱性が原因となるが、過去の事例としは、ハードウェアエミュレーションの欠陥や、ハイパーバイザ管理ツール、グラフィックドライバーの欠陥も含まれている。

4.2.6 ラテラルムーブメント

4.2.6.1 NFVI／MANO 内のラテラルムーブメント

脅威 ID	#TM_L_01
関連脅威アクター	ⓂⒸⓄ

悪意のあるアクターが攻撃の及ぶ範囲を広げるためにシステムを侵害する方法を用いるのと同様に、中央の仮想化インフラストラクチャの侵害によってもネットワークのラテラルムーブメントを容易にすることができる。特に、以下のような NFV システムコンポーネントで実行される。:

- 仮想化レイヤ；攻撃者が既知の仮想化技術上で展開されている異なる仮想ワークロードにも攻撃を広げることができる
- MANO；適切にセグメント化されていない場合、ネットワークの広範な部分に対

する攻撃手法を提供する。特に重要なのは、異なる信頼レベル（例えば、MEC と 5G コアの間）を展開するための共有 MANO ドメインである。

4.3 NFV ワークロードに対する脅威

4.3.1 なりすまし

4.3.1.1 なりすまされたホストプラットフォーム

脅威 ID	#TW_S_01
関連脅威アクター	ⓃⓈ

なりすまされたソフトウェアがセキュリティインシデントの発生源となるだけではなく、正規のソフトウェアが信頼できないハードウェアプラットフォーム上で実行された場合にも、同様の脅威が存在する。NFV 環境がホストの信頼度の保証が得られない場合は、重要なネットワークコンポーネントが、信頼度の低いレベルのセキュリティドメインに実装される可能性がある。5G システムにおいて、これは、例えば、ネットワークスライス等、要求されるセキュリティ水準が高い機能のためのリソースが、セキュリティの低いインフラストラクチャ（例として、エッジクラウド）上で処理され、保存されることを意味する。この状況は、例えば、信頼できない環境で個人情報が処理されている状況と同じであり、法令遵守の問題につながる可能性がある。

4.3.1.2 なりすまされた MANO 通信

脅威 ID	#TW_S_02
関連脅威アクター	ⓈⒸ

VNF と VNF マネージャ間のインタフェースは、VNF インスタンスと NFV 環境間の主要な通信インタフェースとなる。この論理チャネル上の認証は、移行、スケーリング、プロビジョニング解除等の多様な管理タスクに必要な、VNF と MANO ドメイン間のセキュアな通信のための重要な前提条件である。これらのタスクのセキュリティが保証されないと、攻撃者が VNF ライフサイクル管理に干渉するおそれがある。

4.3.2 改ざん

4.3.2.1 アクティブな VNF イントロスペクション

脅威 ID	#TW_T_01
関連脅威アクター	ⓂⓈ

VNF イントロスペクションは、仮想化レイヤを介して仮想ワークロード内の情報を監視し、改変するための強力なツールまで提供する。しかし、この機能へのアクセスが十分に制御及び監視されない場合、悪意のあるアクターによって VNF や処理されたデータが改ざんされる等、容易に悪用されることがある。このような悪意のあるアクターは、社内の運用スタッフである場合もあれば、クラウドプロバイダの担当者である場合もある。

4.3.3 情報漏えい

4.3.3.1 受動的な VNF イントロスペクション

脅威 ID	#TW_I_01
関連脅威アクター	ⓂⓈ

VNF イントロスペクションの誤用による改ざんのリスクと同様に、この機能を悪用して仮想ワークロードや処理されたデータに関する機密情報を抽出し、受動的な攻撃を行うことができる。

4.3.3.2 NFV ワークロード間のコミュニケーション

脅威 ID	#TW_I_02
関連脅威アクター	ⓂⓈ

仮想化されたワークロードとホストシステムの分離に加えて、仮想化レイヤはまた個々の VNF ワークロード自体も分離する必要がある。システムがこの分離を確保でき

ない場合、共有システムメモリ、キャッシュ、または常設ストレージ内の情報が、同じシステム上のピア VNF インスタンスからアクセスできる可能性がある。この種の侵害の最も顕著な例は、メルトダウン攻撃 [05]である。

4.4 無線アクセスネットワーク（RAN）に対する脅威

4.4.1 なりすまし

4.4.1.1 不正な基地局

脅威 ID	#TR_S_01
関連脅威アクター	◎

攻撃者は、ユーザー機器と gNB の間の中間者攻撃を実施するために、正規の無線伝送インフラを偽装することがある。他の正規の基地局よりも強力な信号を被害デバイスに送信するための悪意のトランシーバー（送受信機）が必要なため、これらの攻撃は、非常に狭い場所に限定される性質を持つ。モバイルハンドセットに対する偽装が成功し、このような偽基地局を介してサービングネットワークに接続された場合、暗号化されていないトラフィックを含むトラフィックが悪意のあるアクターにさらされ、任意のメッセージの改ざんが可能になる。

4.4.2 改ざん

4.4.2.1 ユーザー機器またはネットワーク機能のダウングレード

脅威 ID	#TR_T_01
関連脅威アクター	◎

ダウングレード攻撃では、通信ピアの下位互換性を悪用し、特定のプロトコルにおける潜在的にセキュリティの低い構成パラメータで接続しようと試みる。3GPP 無線アクセスネットワークにおいて、これは特に UE とネットワーク間の RRC 及び NAS セッションの確立に関連する。

4.4.2.2 ユーザープレーンのトラフィック改ざん

脅威 ID	#TR_T_02
関連脅威アクター	◎

5G NR を介して転送されたユーザープレーンデータは、攻撃者によって改変される可能性がある。近年のセキュリティ研究では、完全性保護が欠如した状態は、エアインタフェースに深刻な攻撃を仕掛けるために悪用される可能性があることが示されている[06]。コントロールプレーンのトラフィックとは対照的に、ユーザープレーンの完全性保護は 5G 技術仕様のオプション機能であり、ネットワークオペレータはネットワーク配備時に確実に有効にする必要がある。RAN でのユーザープレーンのトラフィックの保護に影響を与える要因としては、コンフィグレーション・パラメータの性能の低さや、以下のようなものがある：

- フロントホール、ミッドホール、またはバックホールのトランスポート層の保護の欠如
- 最大帯域幅未満のレートでユーザープレーンの完全性保護のみをサポートする UE 実装

4.4.2.3 コントロールプレーンのトラフィック改ざん

脅威 ID	#TR_T_03
関連脅威アクター	◎

上記のプロトコル設定パラメータの改変よりも一般的なアプローチとして、攻撃者は、UE とネットワーク間のセッション全体を通してコントロールプレーンのトラフィックを改ざんしようとする可能性がある。このような攻撃は、以下ように RAN ネットワークの実装またはコンフィグレーションが、すべての通信インタフェース上で完全性を厳密に確保していない場合等に可能となる。:

- RRC 及び NAS プロトコルの不正なパラメータ選択の禁止の失敗
- フロントホール、ミッドホール、及び/またはバックホールのトランスポート層保護の欠如

4.4.3 情報漏えい

4.4.3.1 サブスクリプション識別子の盗聴

脅威 ID	#TR_I_01
関連脅威アクター	◎

5G オペレータは、長期識別子が平文でエアインタフェース上に表示されないようにする必要がある。これに失敗すると、5G SUPI 秘匿化機能の無効化や、平文 SUPI によるページングを許可する RAN の実装を通して、悪意のあるアクターによって識別子が記録され、さらなる攻撃に悪用されるリスクが生じる場合がある。

4.4.3.2 ユーザープレーンのトラフィックの盗聴

脅威 ID	#TR_I_03
関連脅威アクター	◎

無線上及び無線アクセスネットワーク内のユーザーデータの機密性を保つことは、加入者のプライバシーを保護するための基本的な要素である。これに失敗すると、無線インタフェース上で盗聴されるか、無線ネットワークコンポーネントを制御して、重要な情報が漏えいするおそれがある。この脅威を可能とする潜在的な脆弱性としては、例えば以下がある。:

- Null 暗号化アルゴリズムを許可する UE-gNB 間の PDCP ユーザープレーンのセキュリティポリシー
- 異なる RAN コンポーネント間のトランスポート層における保護の欠如

4.4.3.3 コントロールプレーンのトラフィックの盗聴

脅威 ID	#TR_I_02
関連脅威アクター	◎

コントロールプレーンのトラフィックが適切に保護されていない場合、攻撃者はネットワーク自体の情報、またはそのユーザーに関する情報（設定パラメータや機能等）を窃取し、後続の攻撃のために使用できる。機密性保護の失敗は、次に示すプロトコルス

タックの複数のレイヤで発生する可能性がある。:

- Null 暗号化アルゴリズムを許可する RRC/NAS コントロールプレーンのセキュリティポリシー
- 異なる RAN コンポーネント間のトランスポート層における保護の欠如

4.4.4 サービスの拒否

4.4.4.1 無線通信のジャミング及び干渉

脅威 ID	#TR_D_01
関連脅威アクター	◎

ジャミングとも呼ばれる無線通信の干渉及び無線信号のブロックは、無線ネットワークの固有の脅威である。このような攻撃は、gNB ネットワークコンポーネントや個々のモバイルハンドセットを標的にすることができる。ライセンスを得た周波数帯域上で通信する悪意のない無線送信機によって、意図せずに不定期な干渉が発生することもある。これらの攻撃は、その性質上、狭い地域に限定される。

4.4.4.2 ミッドホール及びバックホールネットワークに対する攻撃

脅威 ID	#TR_D_02
関連脅威アクター	◎

UE と gNB の間のエアインタフェースを攻撃する代わりに、攻撃者は個々の RAN コンポーネント間、または RAN とコアネットワークの間の接続を乗っ取ろうと試みることもある。これらのインタフェースのトランスポートネットワークは、例えば統合アクセス、バックホール、ダークファイバ、イーサネット等があり、多岐に渉る。

4.5 コアネットワークに対する脅威

4.5.1 なりすまし

4.5.1.1 ユーザープレーンのトラフィックのなりすまし

脅威 ID	#TN_S_01
関連脅威アクター	ⓒⓞ

UPF は、ユーザープレーンのトラフィックを直接処理する唯一の 5G コアネットワークの構成要素である。複数のセキュリティドメインにわたる様々な場所（異なる LADN とのルーティングを処理するユーザー側のネットワークエッジ等）に配置されやすいことを考えると、UPF インスタンス間の相互認証は不可欠である。相互認証がないと、次のようなセキュリティ上の脅威が発生する可能性がある。:

- gNB と UPF インスタンス間のなりすまし（N3 インタフェース）
- 異なる UPF インスタンス間のなりすまし（N9 インタフェース）
- UPF と他のデータネットワーク間のなりすまし（N6 インタフェース）

なりすまし攻撃は、UPF による相互認証が適切に実施されない場合に可能となる場合がある。異なる UPF インスタンス間でそのような攻撃が実行されるシナリオを想定すると、例えば LADN にて動作する不正なアプリケーションがローカル DNS リゾルバのキャッシュを改ざんすることが可能であるとして、この DNS リゾルバが信頼されていない MEC ワークロードや 3GPP の NF と共有されていると仮定すると、NF インスタンスがなりすまされる可能性がある。これは、N6 や N9 等の 3GPP インタフェースのみでなく、管理通信等の他の通信チャネルにも関係することに留意しておく必要がある。

4.5.1.2 コントロールプレーンのトラフィックのなりすまし

脅威 ID	#TN_S_02
関連脅威アクター	ⓒⓞ

ユーザープレーンのトラフィックと同様に、コントロールプレーンのトラフィックもなりすまし攻撃の対象となる可能性がある。このような攻撃の標的になりうるのは以下である。:

- 内部 NF 間のインタフェース
- ピアモバイルネットワークに公開されるインタフェース（例： SEPP 間の N32）
- 他のデータネットワークに公開されるインタフェース(例：NEF と AF 間の N33)
- レガシーインターワーキングのためのインタフェース(例：5G AMF と 4G MME 間の N26)

5G コアネットワーク信号を介するなりすまし攻撃は、ネットワーク機能が通信ピアの ID の適切な検証に失敗した場合に発生する。TLS ハンドシェイク時に表示される ID の他に、JSON オブジェクトの内部や OAuth 2.0 アクセストークン等のアプリケーション層のメッセージにも ID が含まれている。したがって、すべてのネットワーク層で NF の ID が検証されることが重要である。

特定の展開シナリオでは、5G コアネットワークに、NF インスタンス間の信号メッセージを動的にルーティングする Service Communication Proxy（SCP）も含まれるかもしれない。このため、適切に保護されていない場合は悪用可能な攻撃インタフェースが攻撃者によって追加される。これらのインタフェースは次を含む。:

- NF と SCP 間の通信
- 内部 SCP コンポーネント間の通信
- 異なる SCP インスタンス間の通信

4.5.1.3 なりすまされた登録要求

脅威 ID	#TN_S_03
関連脅威アクター	◎

攻撃者は、なりすまされた登録要求をネットワークに送信することで、正規の加入者になりすますことができる。このような攻撃は、事前に記録された正規の加入者の SUPI を使用するか、ランダムに生成された SUPI 値を使用して実施できる。大量の不正な登録要求によって、例えば次のような理由でネットワークの可用性とサービス品質が低下する可能性がある。:

- コアネットワーク機能上の高い負荷
- 不正な形式の SUPI/SUCI 値の処理時に予期しない誤作動の発生

4.5.2 改ざん

4.5.2.1 ユーザープレーンのトラフィックの改ざん

脅威 ID	#TN_T_01
関連脅威アクター	ⓂⓄ

5G コア内のユーザープレーンデータを伝送するインタフェースにおいて、完全性保護の欠如は、重要な個人情報の漏えいにつながる。RAN 内のトラフィックよりも露出は少ないが、クラウド展開への移行のため、次のとおりオペレータのコアネットワークインタフェース内で対策を実施することが強く推奨される。:

- 異なる UPF インスタンス間の N9 インタフェース
- UPF と他のデータネットワーク間の N6 インタフェース（公共のインターネットや LADN 等）

4.5.2.2 コントロールプレーンのトラフィックの改ざん

脅威 ID	#TN_T_02
関連脅威アクター	ⓂⓄ

正確な展開シナリオに依存するものの、5G コアネットワークは内部と外部の双方で複数のネットワークドメインやセキュリティドメインにわたって展開される可能性がある。故に、コントロールプレーンインタフェースの完全性保護は、ネットワーク機能間で交換される信号トラフィックの意図しない改変を防止するために非常に重要である。特に、次のインタフェースに適用される。:

- 内部 NF 間のインタフェース
- ピアモバイルネットワークに公開されるインタフェース（例： SEPP 間の N32）
- 他のデータネットワークに公開されるインタフェース(例: NEF と AF 間の N33)
- レガシーインターワーキングのインタフェース（例：5G AMF と 4G MME 間の N26）
- NF と SCP 間の通信
- SCP 内部コンポーネント間の通信
- 異なる SCP インスタンス間の通信

4.5.3 情報漏えい

4.5.3.1 ユーザープレーンのトラフィックの盗聴

脅威 ID	#TN_I_01
関連脅威アクター	ⓂⓄ

ユーザープレーンのトラフィックを伝送するインタフェース間で機密性が適切に保護されていないと、情報漏えいに関連するセキュリティインシデントが発生するおそれがある。これは、異なる UPF インスタンス間の N9 インタフェースや、UPF と他のデータネットワーク間の N6 インタフェース（公共のインターネットや LADN 等）で起こり得る。これらのインタフェースの不十分な保護は、例えば、以下の要因によって発生する。:

- IPsec のようなネットワークセキュリティプロトコルの実施の欠如
- ネットワークセキュリティプロトコルの実装不備

4.5.3.2 コントロールプレーンのトラフィックの盗聴

脅威 ID	#TN_I_02
関連脅威アクター	ⓂⓄ

5G コアネットワーク機能間の暗号化アルゴリズムの欠陥は、5G コアネットワークのすべての API 主導インタフェースの情報漏えいにつながり、潜在的に以下のチャネルのコントロールプレーンのトラフィックを公開する可能性がある。:

- 内部 API 駆動の NF 間のインタフェース
- レガシーインターワーキング用のインタフェース（AMF と 4G/LTE MME 間の N26 等）
- ピアモバイルネットワークに公開されるインタフェース（SEPP 間の N32）
- 他の IP ネットワークに公開されるインタフェース（NEF と AF の間の N33）
- NF と SCP 間のインタフェース
- SCP コンポーネント間の内部インタフェース
- SCP インスタンス間のインタフェース

4.5.4 サービスの拒否

4.5.4.1 信号スパイク

脅威 ID	#TN_D_01
関連脅威アクター	Ⓒ

サービスの拒否は、5G コアネットワークとの通常の信号通信を介する正規なモバイルエンドポイントによって引き起こされる可能性がある。これは特に、同じ通信パターンを持つ大多数の IoT デバイスが同時に大量の信号送信を開始する場合（一次認証等）の M2M 通信で関係する。

4.5.5 特権の昇格

4.5.5.1 OAuth2.0 認証フレームワークに対する攻撃

脅威 ID	#TN_E_01
関連脅威アクター	ⓈⒸⓄ

5G コアネットワークは、ネットワークサービスへのアクセスを制御し、NF 間の認証情報をセキュアに伝達するために OAuth 2.0 認証フレームワークを使用する。複数の異なるパーティ（ロール）を含むトークンベースのフレームワークである OAuth 2.0 認証は、悪意のあるアクターが制限されたリソースへのアクセスを得るために、標的にされる可能性がある。攻撃者は、例えば、次のようなタイミングに、付与された権限を昇格しようと試みる場合がある。:

- NRF によるサービス検出中に：制限されたサービス、またはサービス提供者に関する情報を要求
- アクセストークンの要求中に：制限されたサービス、サービス提供者、スライスへのアクセスを要求
- サービスへのアクセス中に：アクセストークンの改ざん、アクセスまたはリフレッシュトークンへの侵害、アクセストークンによって許可されていないサービス運用の実行の試行等

4.5.6 ラテラルムーブメント

4.5.6.1 サービスメッシュインスタンスの中のラテラルムーブメント

脅威 ID	#TN_L_01
関連脅威アクター	ⓈⓄ

SCP はコアネットワークにおけるコントロールプレーン通信のための中央ルータの役割を担うため、すべてのネットワーク機能に接続する必要がある。しかしながら、5G コア全体に影響を及ぼす可能性のある単一障害点のシナリオ（SPOF）が発生するため、特に大規模なネットワーク展開では、SCP を複数のインスタンスに分割することが望ましい。

4.6 ネットワークスライシングに対する脅威

4.6.1 なりすまし

4.6.1.1 スライス識別子のなりすまし

脅威 ID	#TNS_S_01
関連脅威アクター	ⓒⓞ

ネットワークスライシングを使用して、別個のサービスレベルを持つ分離したネットワークエクスペリエンスを提供するという概念は、5G エコシステムの核心部となる。したがって、特定のスライスの固有のリソースにアクセスするときは、UE とネットワーク機能の双方の強力な認証が特に重要である。スライス認証に関連する潜在的なセキュリティインシデントは、以下の状況において進展するおそれがある。:

- スライス固有のサービスアクセス時における UE のスライス識別子のなりすまし
- スライス固有サービス登録時における NF のスライス識別子のなりすまし
- NF による通信ピア（UE／ピア NF）のスライス識別子の検証の失敗

4.6.1.2 スライス管理通信のなりすまし

脅威 ID	#TNS_S_02
関連脅威アクター	ⓢⓞ

ネットワークスライスは、モバイルネットワークオペレータの担当者のみでなく、顧客によっても管理される可能性が高い。スライス管理の特定の部分は外部パーティに公開することが考えられるため、このインタフェースはなりすまし攻撃を受けやすい。例えば、ネットワークスライスの顧客は、自らのスライスインスタンスを管理することは可能であるが、スライスマネージャーとの通信をなりすますことで、他の顧客のスライスインスタンスの管理方法を取得しようと試みることが考えられる。

4.6.2 情報漏えい

4.6.2.1 スライス固有情報の漏えい

脅威 ID	#TNS_I_01
関連脅威アクター	ⓒⓞ

効率的なスライス分離は、許可されたユーザーのみに対するスライス固有のリソースへのアクセス、及び個々のネットワークスライスインスタンスの分離で構成される。この分離がネットワークスライスインスタンスのライフサイクルを通じて厳密に実施されない場合、権限のないユーザーやネットワークエンティティに対して情報が漏えいする可能性がある。このような情報漏えいは、例えば以下の場合に起こる。:

- サービスの発見中：要求している NF がアクセス可能なスライスのみに NRF が応答するように制限することに失敗した場合
- アクセストークンの要求中：要求している NF がアクセス可能なスライスのみに NRF がアクセストークンを生成することに失敗した場合
- アクセストークンの検証中：NF がスライス固有のサービスを提供する前に、受信したアクセストークンの適切な検証に失敗した場合

4.6.3 サービスの拒否

4.6.3.1 ネットワークスライスに対する DoS 攻撃

脅威 ID	#TNS_D_01
関連脅威アクター	ⓒⓞ

特定のネットワークスライスインスタンスのサービス品質に影響する状況は、異なる原因によって発生する可能性がある。例えば個々の加入者は、アクセスを取得した後に特定のネットワークスライスのリソースを「内部から」飽和させることができる（スライス内 DoS)。これは、意図的なものであれ意図的でないものであれ、クライアントによるサービスの悪用の例である。

他方、スライスの分離が不十分な場合、異なるネットワークスライスインスタンスが同じプラットフォームを共有してリソースを奪い合う場合、互いに悪影響を及ぼす可能性がある（スライス間 DoS)。

4.6.3.2 ネットワークスライス間通信におけるセキュリティポリシー

脅威 ID	#TNS_D_02
関連脅威アクター	Ⓒ

ネットワークスライスインスタンスは、単一のモバイルネットワークドメインを超えて広がり、加入者のためにホームネットワークとサービスネットワークの両方で一貫性のあるサービスレベルの確保を要求する場合がある。ローミングのシナリオでは、ホームネットワークオペレータはアクセスネットワークを制御しないため、正しい動作をしないサービスネットワークは、期待されるサービスレベル及び関連するセキュリティ保証の実施に失敗することがある。

4.6.4 特権の昇格

4.6.4.1 異なるセキュリティポリシーを持つネットワークスライス

脅威 ID	#TNS_E_01
関連脅威アクター	ⒸⓄ

ネットワークスライスは、ユーザーの要件に応じて異なるサービスレベルを示すことが期待される。これはパフォーマンスの側面である場合もあるが、再認証の実行頻度等、セキュリティ目的を含む場合もある。したがって、セキュリティレベルの低いネットワークスライスによって他のネットワークスライスのセキュリティが低下しないようにする必要がある。これは、UE が異なるセキュリティレベルのスライスに同時にアクセスするシナリオにおいて特に重要である。

4.7 MEC に対する脅威

4.7.1 なりすまし

4.7.1.1 MEC 管理通信のなりすまし

脅威 ID	#TE_S_01
関連脅威アクター	ⓈⒸⓄ

MEC プラットフォームに展開されているワークロード及び MEC プラットフォーム自体は、アプリケーション開発者やクラウドプラットフォームプロバイダ等の外部のパーティによって部分的に制御される場合がある。これらの環境における管理通信を標的としたなりすまし攻撃は、MEC サービスへの不正アクセス、利用不可、またはその他のセキュリティ上の影響につながる可能性がある。

4.7.2 改ざん

4.7.2.1 MEC コントロールプレーンデータの改ざん

脅威 ID	#TE_T_01
関連脅威アクター	ⓈⒸⓄ

MEC 関連のコントロールプレーンのトラフィックの改ざんは、MEC アプリケーション及びエッジプラットフォーム自体に潜在的な影響を与える。特に、DNS レコードやデータキャッシュ等、MEC ワークロードによって部分的に影響を受けるデータに対する改ざんが考えられる。例えば、MEC ワークロードが LADN 内の DNS リゾルバのキャッシュを改ざんできるとした場合、他の MEC ワークロードが悪意あるサイトへ誘導されるなどの攻撃を受けることが考えられる。

4.7.3 情報漏えい

4.7.3.1 LADN におけるセンシティブな資産の処理と保管

脅威 ID	#TE_I_01
関連脅威アクター	ⓈⒸⓄ

特定の MEC アプリケーションの性質上、正確な位置データ等の取扱注意なユーザー情報を処理することは避けられない。エッジ展開の増加を考慮すると、このような情報が転送中及び保管中に適切に保護されていない場合、重大なプライバシー侵害につながる可能性がある。

4.7.3.2 想定外の MEC ワークロード

脅威 ID	#TE_I_02
関連脅威アクター	Ⓒ

5G オペレータ環境に展開された MEC ワークロードは、IP アドレスや使用可能なサービス等、内部ネットワークトポロジーに関する情報を収集することが考えられる。悪意ある MEC 開発者は、このような情報を密かに抽出し、標的に対するさらなる攻撃を実施するために悪用する可能性がある。

4.7.4 サービスの拒否

4.7.4.1 AF 支援ルーティングの悪用

脅威 ID	#TE_D_01
関連脅威アクター	Ⓒ

ネットワークエッジに展開された MEC アプリは、5G コアネットワークに統合された 3rd パーティのアプリケーション機能(AF)によってサポートされる場合がある。AF は、比較的に時間の影響を受けにくい管理タスクを実行し、UPF ルーティングの決定に影響を与えることができる。AF 支援ルーティング機能が悪用されると、加入者は MEC アプリやその他のネットワークサービスが利用できなくなる可能性がある。

4.7.4.2 MEC ワークロードとネットワーク機能間のリソース共有

脅威 ID	#TE_D_02
関連脅威アクター	Ⓒ

特定の展開シナリオでは、3rd パーティの MEC アプリが、gNB CU 等の内部 RAN コンポーネントを備えた共通プラットフォーム上の LADN で実行される場合がある。これら 2 つのドメイン間の厳密な分離が確保されない限り、MEC アプリは、意図的または非意図的に、内部 RAN コンポーネントに影響を与える可能性がある。

4.7.4.3 MEC UserApps の悪用

脅威 ID	#TE_D_03
関連脅威アクター	Ⓞ

ETSI 仕様書 [07]によれば、MEC システムはいわゆる UserApps をサポートする場合がある。UserApps は、加入者のユーザー機器において実行されるアプリケーションであり、MEC プラットフォームにおいて実行される MEC アプリケーションに影響を与える可能性がある。5G オペレータの環境内のワークロードに対する外部パーティによる制御は、多数の MEC アプリケーションをインスタンス化するために悪用される可能性があり、潜在的に DoS 状態に繋がるかもしれない。

4.7.5 特権の昇格

4.7.5.1 LADN における合法的通信傍受機能の侵害

脅威 ID	#TE_E_01
関連脅威アクター	Ⓒ

従来のモバイルネットワークでは、合法的傍受（LI）機能は通常、非常にセキュアな環境である 5G オペレータのコアネットワーク内で実装される。MEC の導入により、5G コアネットワークの一部 (UPF) がネットワークエッジに展開される。このような場合、重要な LI 機能がより大きなセキュリティリスクに晒される可能性がある。

4.7.6 ラテラルムーブメント

4.7.6.1 LADN 中のワークロードの移動

脅威 ID	#TE_L_01
関連脅威アクター	ⓃⓂⒸ

ネットワークエッジ上のワークロードは、セキュリティ／信頼レベルが異なる可能性がある複数の局部 LADN に展開されることが想定される。MEC エンドユーザーの位置によっては、ワークロードがネットワークカバーエリアを通してエンドユーザーを「追跡」することもある。このシナリオでは、意図的であろうとなかろうと MEC ワークロードが十分なセキュリティ／信頼レベルを満たさない LADN に展開されるか、またはその逆の場合にセキュリティ問題が発生する可能性がある。

5. セキュリティ対策要件

本章では、5G 技術の開発、統合、及び 5G システムの運用に関連する推奨されるセキュリティ対策について説明する。セキュリティ対策は、前章で概説した脅威に対応する。

5.1 節では、組織レベルで実施することが推奨されるセキュリティ対策について述べる。**5.2 節**では、主に組織の人員に関係する対策を詳述する。**5.3 節**では、安全なネットワーク運用と維持管理のための対策について概説する。**5.4 節**では、物理的システムセキュリティのための基本的な安全対策を指摘する。**5.5 節**では、技術的な対策として、一般的なものと特定の 5 G システムドメインに特有のものを述べる。

5.1 組織的な対策

5.1.1 セキュリティ組織

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	識別，防御
関連するセキュリティ目的	認証，完全性，否認防止，機密性，可用性，許可，ネットワークの分離
関連する脅威	複数

管理策：5G サービスと組織のセキュリティを確保するための明確な役割と責任を確立することが望ましい。

ガイダンス：5G オペレータは、情報セキュリティを確保する専門の部門を組織内に設けることが望ましい。当該組織がセキュリティ上の利益を効果的に推進し、実施できるようにするために、他の技術部門から切り離すことが強く推奨される。その責任は明確に定義され、特に以下の事項を含む。:

- セキュリティポリシー、手順、プロセスの開発（「セキュリティポリシーのフレームワーク」 参照）
- 上記ルールの全組織的な遵守の徹底
- セキュリティ概念や対策のフレームワーク作成
- ハードウェア・ソフトウェア技術コンポーネントのセキュリティ保証（セキュリティテスト、セキュリティ強化、脆弱性管理を含む。「セキュリティ保証」参照）
- セキュリティ運用（ネットワーク全体のセキュリティ関連情報の監視・分析。「セキュリティ監視」参照）

・ 脅威管理とインシデント対応（「セキュリティインシデントの報告と対応」及び「脅威インテリジェンス」 参照）

ビジネス全体にとってセキュリティの重要性は明確であるため、セキュリティに対する説明責任は、会社のリーダーの中の専任の幹部が負うことが望ましい。

参考文献：-

5.1.2 セキュリティポリシーのフレームワーク

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	識別
関連するセキュリティ目的	認証，完全性，否認防止，機密性，可用性，許可，ネットワークの分離
関連する脅威	#TC_D_06

管理策：セキュリティポリシーは、適用される規則や規制、業務要件、利害関係者の期待に応じた 5G システムのセキュリティを確保するために、作成されることが望ましい。

ガイダンス：5G オペレータは、5G システム、そのユーザー、及び処理されたデータをどのように保護するかを規定するためのセキュリティポリシーフレームワークを確立することが望ましい。この文書は、以下の点を考慮する。:

- 現地立法の関連法令及び規制
- 組織独自の企業ルール及び規制
- 組織と 5G サービスが対象となるセキュリティリスク

ポリシーの内容は、5G システムに関連するセキュリティとリスクの管理について、以下に示すようなハイレベルなガイダンスを提供することが望ましい。:

- 「5G セキュリティ」の定義と適用範囲
- 5G に関連したセキュリティ目的
- 5G サービスの提供における役割と責任
- 内部セキュリティ報告及び連絡体制
- 外部機関への報告義務（例えば、規制機関に対して）

セキュリティポリシーは、組織内のすべての人員が一元的に利用可能であり、企業のリーダーによって奨励される必要がある。サブポリシーは、暗号化アルゴリズムに関する推奨事項等、より頻繁に変更されることが予想されるセキュリティの側面をカバーするために作成される場合がある。

参考文献：-

5.1.3 契約におけるセキュリティ

優先度	Critical
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御, 対応
関連するセキュリティ目的	機密性, 可用性
関連する脅威	#TM_D_02, #TC_I_06

管理策：セキュリティに関する法的安全対策は、組織と 3rd パーティ間の取引において確立されることが望ましい。

ガイダンス：5G 展開は、システムライフサイクルを通して異なる 3rd パーティが関与する必要がある複雑な技術エコシステムといえる。この外部パーティとの契約の種類は、単一方向のサービス提供から重要な情報の相互共有、処理に至るまで、大きく異なる場合がある。したがって、機密性や可用性に関するセキュリティ要件を、法的に有効な形で把握することなどが重要である。このような契約の例を以下に示す。:

- 組織と外部ビジネスパートナー間の秘密保持契約（NDA）
- 組織と外部の 5G オペレータ間のサービス品質保証（SLA）
- 組織とその従業員間の守秘条項

参考文献：-

5.1.4 組織のリスク管理

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	識別
関連するセキュリティ目的	認証，完全性，否認防止，機密性，可用性，許可，ネットワークの分離
関連する脅威	複数

管理策：組織は、セキュリティリスクを評価し、脅威を緩和するための実装を指導するリスク管理プログラムを確立することが望ましい。

ガイダンス：5G 技術サプライヤと 5G オペレータは共に、継続的なリスク管理プロセスの存在と実行を確保することが望ましい。最初のステップとして、脅威と組織への潜在的影響の特定を含めることが望ましい。このようなリスクは、以下のような異なる領域から発生する。:

- サプライチェーンの側面を含む技術リスク
- 規制及びコンプライアンスのリスク
- 財務リスク
- 運用リスク
- レピュテーションリスク

その次に、既知のリスクは評価され、優先順位付けされることが望ましい。この優先順位付けは、組織の個々のリスク許容度によっても導かれることが望ましい。これらのステップに基づいて、特定されたリスクを管理するための戦略を発展させることができる。リスク環境は常に変化するため、この戦略は継続的に再評価され、改善されることが望ましい。

参考文献： [08] SA-14, PM-8, PM-9, PM-11

5.1.5 事業継続計画（BCP）

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	復旧
関連するセキュリティ目的	可用性
関連する脅威	#TM_D_02

管理策：組織は、重大なインシデントから回復し、不利な状況で製品とサービスを提供し続けることができるように、予防的方法を講じることが望ましい。

ガイダンス：事業継続計画（BCP）は、破壊的イベントによる損害の軽減を目的とする色々な準備手順で構成されている。このような事象には、自然災害、サプライチェーンの中断、及びユーティリティの故障が含まれる。主要な事業プロセスのレジリエンシと継続性を確保するために、事業継続計画では、スタッフ、情報資産のセキュリティを考慮することが望ましい。

5G オペレータに関連する具体的な例としては、クラウドサービスプロバイダに関連するリスクをどのように取り扱うかが上げられる。一旦 5G ネットワークの多くの部分が共有された公共インフラストラクチャに展開されると、サービスの中断（クラウドサービスプロバイダにおける中断、クラウドサービスへの接続の中断等）は 5G サービスに重大な影響を与える可能性がある。このリスクを最小限に抑えるために、技術的対策と非技術的対策の双方を、特にサプライヤ戦略、ネットワークアーキテクチャ、及びレジリエンシ計画の一部として考慮することが考えられる。本書の対象とする具体的な BCP セキュリティ対策としては、以下がある。:

- ベンダーのデューデリジェンス（5.1.6 項）
- バックアップ及び復旧手順（5.3.8 項）
- セキュアな設備デザイン（5.4.1 項）

参考文献： [08] (section 3.6)

5.1.6 ベンダーのデューデリジェンス

優先度	Critical
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	識別
関連するセキュリティ目的	完全性
関連する脅威	#TM_I_01, #TW_I_02, #TC_I_04, #TC_I_06

対策案：5G 技術サプライヤ及び 5G オペレータは、組織の技術サプライチェーンに関連するサイバーセキュリティリスクを特定し、管理するためのプロセス及び手順を実施することが望ましい。

ガイダンス：サイバーセキュリティにおけるベンダーのデューデリジェンスは、直接的及び間接的なサプライヤに関連するセキュリティリスクを特定、評価、軽減する体系的なプロセスである。

ベンダー選定プロセスには、客観的な基準に基づいた複数の潜在的ベンダーの比較を含めることが望ましい。サイバーセキュリティのデューデリジェンスを実施することにより、技術サプライヤがセキュアで信頼できる製品やサービスを調達できることを保証される必要がある。このプロセスは、次の事項を含む。:

- 組織自体に関する情報の収集（企業プロフィール、株式所有構造、M&A、会社が準拠する法律及び規制、セキュリティ認証、既知のセキュリティインシデント等）
- 組織の製品とサービスに関する情報の収集（セキュリティ証明書、セキュリティ文書、直接的なテスト、トライアル等）
- 収集された情報及び当製品または当サービスに基づくサプライヤに関連するサイバーセキュリティリスクの評価

エンドツーエンドのサプライチェーンのセキュリティの確保は、ベンダー選択プロセスを以って終了する訳ではない。この最初のステップに続いて、調達プロセス及びソリューションのライフサイクル全体にもサプライチェーンセキュリティを組み込む必要がある。例えば以下。:

- 契約におけるセキュリティ（5.1.3 項）
- 製品セキュリティのメンテナンス（5.2.3 項）
- セキュリティ保証（5.3.3 項）

参考文献： [09],[10]

5.2 人的な対策

5.2.1 セキュリティ教育及び意識向上

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	識別，防御
関連するセキュリティ目的	認証，許可，機密性
関連する脅威	#TC_I_05, #TC_S_03

対策案：従業員に対して、5G システムやサービスに関連するセキュリティリスクを理解・特定し、適切な注意を払って管理できるために必要な訓練が提供されることが望ましい。

ガイダンス：組織は、セキュリティ目的、問題、及び潜在的な攻撃に対する意識を高め、セキュリティ対策やセキュリティインシデントへの正しい対応方法を教育することで、従業員がセキュリティを正しく理解して対応できるようにすることが望ましい。5G への移行に伴い、通信業界では比較的新しい技術的・運用的側面がいくつか導入されているため、セキュリティ教育や啓蒙が、5G 技術サプライヤや 5G オペレータにとって特に重要となる。新しい技術的・運用的な側面の例としては以下がある。:

- RAN の一部を含むクラウドネイティブな展開
- Web 技術と API 主導の通信
- 3rd パーティとオープンソースソフトウェアの多様なエコシステム

教育や啓蒙活動は、以下の考慮事項を念頭に置いて計画するとよい。:

- 役割と責任を明確にする：各自の役割と責任を理解していれば、従業員はセキュリティ対策に従う可能性が高くなる
- セキュリティリスクを伝える：根底にある動機や関連するリスクが十分に理解されていれば、従業員はセキュリティ対策に従う可能性が高くなる
- 日常業務との関連性を確保する：伝達された情報を各自の責任に簡単に結びつけることができれば、どんなトレーニングでも影響は大きくなる
- 定期的にリフレッシュや繰り返しを行う：攻撃者の戦略やセキュリティ対策は常に変化する。セキュリティトレーニングの内容は、この変更を反映させ、定期的に組織に伝えていくことが望ましい

参考文献： [11]

5.2.2 ポジティブなセキュリティ文化

優先度	High
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	識別，防御
関連するセキュリティ目的	認証，機密性，完全性
関連する脅威	#TC_I_05, #TC_S_03

対策案：セキュリティは阻害要因ではなく、ビジネスの実現要因として認識し、日々の業務にセキュリティをシームレスに統合するよう組織文化を醸成することが望ましい。

ガイダンス：セキュリティの確保は決して一回限りの活動ではなく、変化するリスク環境と優先順位に対応するために、関係者全員による持続的かつ継続的な取り組みである。このように、セキュリティを全従業員の中核的責任として確立することは、ビジネス全体のセキュリティを確保する上で重要な役割を果たす。ポジティブなセキュリティ文化をサポートするイニシアチブには、次のものがある。:

- リーダーシップチームによる模範：組織の経営陣は、セキュリティポリシーに対する認識を高め、自らもセキュリティポリシーを遵守することが望ましい
- セキュリティの利便性向上：セキュリティをできるだけ邪魔にならず、使いやすいものにするように努力する。セキュリティ対策に柔軟性が欠けたり複雑だったりすると、人はそれを回避しようとする
- 良い行動の認識や報酬化：ポジティブな動機づけは、不正行動時のネガティブな補強よりも大きな影響を与えることが多い
- 学習を奨励し、ミスを非難しない：従業員はセキュリティを恐れず、日々の仕事の中でセキュリティを学び、自信を持って扱うことを奨励されることが望ましい

参考文献： [12]

5.3 運用における対策

5.3.1 セキュアなソフトウェア開発プロセス

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証，許可，機密性，完全性
関連する脅威	#TC_T_03, #TC_S_02, #TC_T_05

対策案：関連する資産とその結果としてのソフトウェア製品の保護を確実にするため、セキュアなソフトウェア開発プロセスを確立することが望ましい。

ガイダンス：ソフトウェア開発プロセスは、安全で信頼性の高い製品の製造を促進することが望ましい。これには、変更の追跡、バージョン管理、情報資産の保護等、ソースコード管理の基本的なベストプラクティスが含まれる。

開発及び統合プロセス全体を通して、必須のセキュリティチェックポイントを置くことは、一定レベルのセキュリティ成熟度を強化するのに役立つ。これらのプロセスは、静的コード分析、依存性チェック、既知の脆弱性のスキャン等を一部自動化したツールによってサポートされることが望ましい。

ソフトウェア製品のパッケージングと提供に際して、5G 技術サプライヤは、制御されたビルド環境とプロセスを構築することにより、再現性や明確な監査証跡を確保しておくことが望ましい。ソフトウェア製品の完全性を保証し、お客様が元のソースを検証できるようにするため、最終版には一意のリリース識別子を割り当て、暗号化署名することが望ましい。

参考文献： [13] (sections 7.1-7.6, 7.8), [14], [15]

5.3.2 製品セキュリティの保守

優先度	Critical
責任者	サプライヤ
制御タイプ	予防的，是正的
セキュリティの概念	識別，防御，対応
関連するセキュリティ目的	機密性，完全性，可用性，認証，許可
関連する脅威	複数

対策案：5G 技術サプライヤは、運用期間中に製品のセキュリティを維持するためのプロセスと手順を実装することが望ましい

ガイダンス：製品のセキュリティに対するサプライヤの責任は、その製品の納入で終わるわけではない。特にモバイルネットワークやその他のインフラストラクチャコンポーネントにおいては、継続的な製品セキュリティ管理が不可欠である。これには、技術的なセキュリティパッチのみでなく、次のような新たに発見された弱点や脆弱性を管理するためのプロセスや手順も含まれる。:

- セキュリティに関する顧客からのお問い合わせ窓口の設置
- 新たに発見されたセキュリティ脆弱性の特定と評価
- 利用可能になったセキュリティ修正に対する顧客への随時通知、安全なセキュリティ修正の配布

参考文献： [13] (section 7.7), [10]

5.3.3 セキュリティ保証

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	識別，防御
関連するセキュリティ目的	認証，許可，機密性，完全性，可用性，Segmentation & Segregation
関連する脅威	#TC_I_01, #TC_I_03, #TC_I_04, #TC_D_03, #TC_E_01, #TC_E_02

対策案：ハードウェア及びソフトウェアコンポーネントの継続的なセキュリティ評価と、特定された弱点の軽減のためのプロセスと手順を実施することが望ましい。

ガイダンス：5G 技術サプライヤ及び 5G オペレータは、5G システムとその技術コンポーネントのセキュリティを評価するプロセスを確立し、関連するセキュリティ要件を満たしていることを確認することが望ましい。この目標をサポートできるアクティビティは次のとおり。:

- ソフトウェアの分析：以下により、技術コンポーネントに内在するセキュリティ上の弱点（偶発的または意図的な「バックドア」）を検出する
  - ソースコードが利用可能な場合、静的コード分析
  - プログラムの実行パスと状態遷移の解析
  - バイナリサンドボックスや連続ランタイム分析
- ソフトウェアの強化：以下により、システムサービスのセキュアな設定を強化する
  - 不要なインタフェースとポートの閉塞
  - 不要な機能やコンポーネントの無効化や削除
  - 不要なアカウントと資格情報の削除
- 脆弱性管理：以下の方法でシステムの弱点を特定し、軽減する
  - 認証済みセキュリティスキャンの実行
  - システム環境に応じた脆弱性の優先順位付け
  - 利用可能なセキュリティパッチの適用か、エクスプロイトを軽減するための代替手順の実行
- ペネトレーションテスト：
  - 弱点を悪用し、より複雑な攻撃チェーンを構築することで、実際の攻撃者の行動をシミュレートする詳細な手動のセキュリティ監査
- ファジングテスト：
  - 動作確認のためのテストケースを補完するものとして、想定外のケース（edge

ケース）のテストを実行することによって、セキュリティ上の欠陥を特定する

上記の活動は、5G 技術サプライヤのセキュアなソフトウェア開発プロセスを行うための必須的な部分である。しかし、セキュリティ保証は、システムのライフサイクルを通して 5G オペレータの責任でもある。これは、サプライヤが実装した製品セキュリティを有効化するためである。一方、脅威や脆弱性は常に変化しているため、効果的なセキュリティ保証には継続的な取り組みが必要になる。この目的のために、5G オペレータは、各 5G コンポーネントが本番環境に展開される前に通過するべき独自のセキュリティテストカタログや自動化されたテストパイプラインの構築を検討することが望ましい。

参考文献： [10], [16]

5.3.4 アセット管理

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	識別
関連するセキュリティ目的	可用性，完全性，機密性
関連する脅威	#TM_I_02

管理策：5G システム全体を通じて、ハードウェア及びソフトウェアコンポーネントの完全かつ最新のインベントリを確立し、それを維持することが望ましい。

ガイダンス：セキュリティを確保するための基本的な前提条件は、アセットを可視化することである。このため、5G オペレータは、ハードウェア及びソフトウェアコンポーネントに関するセキュリティ関連情報を保存するシステムインベントリを構築することが望ましい。これには、内部ネットワーク内のシステムとネットワーク外のシステム（外部クラウドインフラストラクチャ上で動作するソフトウェア等）が含まれる。記録すべき関連データとしては、以下のものが含まれる。：

- システムタイプ
- システム識別子とアドレス（FQDN、IP アドレス等）
- 処理されたデータと関連する保護要件
- 責任のある組織（組織内の連絡窓口を含む）

この基本的なシステムインベントリに加えて、組織は、各システムの構成パラメータに関する情報を追跡できるデータベースも保持することが。このデータベースは、システムインベントリの一部として、またはシステムインベントリと同期して保持される別個のレコードとして実装される場合がある。このような構成データベースに一般的に記録されるデータには、以下のものがある。:

- オペレーティングシステムとインストールされているアプリケーション（パッチレベルを含む）
- 他のシステムとの通信関係と他のシステムへの依存
- 関連秘密情報（公開鍵証明書、パスワード等)
- 関連ソフトウェアライセンス
- システムサプライヤの情報（連絡窓口を含む）

システムインベントリ及び構成データベースの作成は、半自動化されたツールによってサポートされる。記録されたデータの正確性を確保するために、関連するデータストアへの上記情報の必須登録を含むシステムコンポーネントのプロビジョニング及び更新のための定義された手順をもつことが望ましい。

参考文献：-

5.3.5 変更管理

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	可用性
関連する脅威	#TM_I_02

管理策：5G システムで実行された変更の明確なトレーサビリティを可能にするプロセスと手順を確立し、実施することが望ましい。

ガイダンス：5G エコシステムにおける変更について、その責任者が明確にされており、変更計画が事前にレビューされ、セキュリティ組織を含む関係者によって承認されているべきであり、そのため、オペレータは、厳格な変更管理の手順を確立することが望ましい。また、実施された変更の記録は、適切な期間保存されることが望ましい。変更の記述には、以

下のような遡及的なトレーサビリティを可能にする十分な情報を含む。:

- 変更理由
- ウィンドウの変更
- 詳細な変更手順
- 影響を受けるシステムとサービス
- オーナーと連絡窓口

セキュリティ関連の構成パラメータに関しては、以下の実施が推奨される。:

- 強化された構成テンプレートの定義:強化された構成及びソフトウェアイメージは、標準的なオペレーティングシステムとサービスのために、セキュリティ組織（「セキュリティ組織」 参照）と協力して作成されることが望ましい
- 変更と例外の記録：推奨されるセキュリティ構成からの例外はすべて記録し、予想される修復時間が割り当てることが望ましい
- セキュリティ構成に対する定期的な検証：構成パラメータを定期的に評価するために、リモート認証機能を使用することが望ましい。

参考文献：-

5.3.6 パッチ管理

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証，許可，可用性
関連する脅威	#TC_I_04

対策案：5G システムの本番環境でソフトウェアパッチを実施するための構造化されたプロセスと手順を構築することが望ましい。

ガイダンス:ソフトウェアは、エラーがないことはなく、常に変化する環境に存在するため、継続的なメンテナンスと修正が必要となる。したがって、5G オペレータは、ソフトウェアパッチを管理するための体系的なプロセスを実装することで、運用に悪影響を与えないようにしながら、セキュリティ関連の更新をタイムリーかつ高信頼に展開できるようにしていくことが重要である。セキュリティパッチ管理プロセスを設計する際には、以下の点を考

慮することが望ましい。:

- ソフトウェアを定期的にスキャンして既知の脆弱性を検出する(「セキュリティ保証」参照)
- 特定された脆弱性や新にリリースされたパッチに関するサプライヤ／開発者の発表に従う
- 可能な限り早期にパッチを実装し、優先順位を決定するためにリスクベースのアプローチをとる
- 本番システムにパッチを適用する前にパッチの事前検証を実施する
- システム全体のパッチレベルを追跡し、パッチ例外についてはすべてを文書化する

セキュリティパッチの実施は、「変更管理」の項で説明したものと同じプロセスに従うものとする。

参考文献： [17]

5.3.7 セキュリティ監視

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	探知的
セキュリティの概念	検知
関連するセキュリティ目的	認証，機密性，完全性，可用性
関連する脅威	#TC_R_01, #TC_L_01

管理策：5G システム全体にわたるセキュリティ関連イベントの可視性を確立し、セキュリティインシデントをタイムリーに特定して対応できるようにすることが望ましい。

ガイダンス：セキュリティ監視は、システムの運用中に発生するセキュリティイベントを特定し、管理することに重点を置いている。そのためには、システムコンポーネントのセキュリティ関連情報を収集、記録、分析することが重要である。5G システムにおいては、以下の活動が含まれる。:

- 潜在的なセキュリティインシデントの証拠を発見するための、フロー監視、シンクホール、ネットワークベースの IDS 等の方法を使用したネットワーク通信の監視、5G システムコンポーネント自体（NRF、SCP 等）の監視
- システムログやアラートの形式でシステムイベントの監視(「安全なログファイルの

収集と保存」参照)。5G システムコンポーネントに加えて、監視されるシステムとして、専用のセキュリティ要素（ファイアウォール、ハニーポット等）も含まれる場合がある
- 集中データストアへのセキュリティ監視データの記録
- 異なるデータソースからのセキュリティ関連情報の相関
- セキュリティイベントの分析とリスクベースの優先順位付け
- インシデント管理ツールでの対応が必要なイベントの追跡

セキュリティ監視アーキテクチャへの統合は、5G システムにシステムコンポーネントを展開するために必須の前提条件であることが望ましい。UE 測定や gNB のログやアラート等、システムの動作中に収集されたデータを監視することも、効果的に防ぐことができない攻撃（例えば、#TR_S_01：不正な基地局、#TR_D_01：無線通信のジャミング及び干渉）の検出に役立つ。

5G オペレータが上記の監視タスクを実行するために重要なのは、5G 技術サプライヤによる監視機能の実装である。サプライヤは、システムの挙動を包括的に検証するために必要な情報を収集しレポートするための能力を適切に実装することが望ましい。

参考文献： [18] (section 2.1)

5.3.8 バックアップとリカバリの手順

優先度	High
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	復旧
関連するセキュリティ目的	可用性
関連する脅威	#TC_I_04, #TC_D_05

管理策：5G システムコンポーネント（アプリケーションデータ、構成、メタデータを含む）の現在の状態について、定期的なセキュリティコピーを作成し、必要に応じて以前の状態に効率的に復元でできるようにするためのプロセスと手順を実装することが望ましい。

ガイダンス：5G システムの運用中には、情報セキュリティインシデントやその他のイベントによって、以前のシステム状態に復元しなければならない様々なシナリオが存在する可

能性がある。これらのシナリオに備えて、5G オペレータは、定期的にシステムのバックアップを取ることができるようなプロセスや技術的対策を実装することが望ましい。一旦このようなバックアップを作成した後は、以下を例とする対策を実施し、保存されているすべてのデータを保護する。:

- 冗長化し、物理的に分離されたバックアップコピーの保管
- 保存されたバックアップへのアクセスを許可された担当者に制限
- 保存されたバックアップの機密性及び完全性の保護
- バックアップが効果的に復元できることの定期的な確認

バックアップを復元するためのプロセスと手順は、定期的に訓練することが望ましい。

参考文献：-

5.3.9 セキュリティインシデントの報告と対応

優先度	Critical
責任者	オペレータ
制御タイプ	探知的
セキュリティの概念	検知
関連するセキュリティ目的	機密性, 完全性, 可用性
関連する脅威	#TC_L_01, #TC_I_04, #TC_D_05

管理策：セキュリティインシデントを主要な連絡窓口に報告し、それらを効率的に管理できるプロセスと手順を確立することが望ましい。

ガイダンス：成熟した組織であっても、セキュリティ対策ですべてのインシデントを防止できるわけではない。このような状況では、組織がセキュリティへの影響を最小限に抑えるために迅速に特定し対応できるような明確なプロセスと手順を用意することが不可欠である。セキュリティインシデントの報告及び対応プログラムを設立する際、5G オペレータは以下のベストプラクティスを考慮することが望ましい。:

- インシデント対応（IR）ポリシーの確立：従業員の主な責任、プロセス、及び期待事項を文書化し、この情報を組織内に普及する
- IR ポリシーに基づいた具体的な IR 計画の策定：インシデント発生時の IR チーム間の連携、報告体制、トリアージ、エスカレーション基準について十分に理解する必要がある

- 説明責任の奨励と脅迫しないこと：すべての従業員は潜在的な波及のためにインシデントを報告することを恐れるべきではない。脅迫はセキュリティ問題の隠ぺいの温床を生み出す

多くの国では、公的な 5G システムのオペレータが、重大なセキュリティインシデントを報告するように国の規制当局より義務付けられている。

参考文献： [19], [20]

5.3.10 脅威インテリジェンス

優先度	Moderate/High
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	識別
関連するセキュリティ目的	認証，完全性，否認防止，機密性，可用性，許可
関連する脅威	#TC_I_04, #TC_D_05

対策案：新たに発見された脅威及び脅威アクターに関する情報を、新たな脅威に早期に対応できるよう利用することが望ましい。

ガイダンス：脅威インテリジェンスとは、新たに出現した脅威、脅威アクター、攻撃スキームに関するすべての情報の総称である。このような警告をできるだけ早く受信して分析することで、組織はセキュリティ対策の準備状況を確認して、セキュリティリスクを軽減することができる。
このような脅威情報のソースとしては、保有サービス、情報共有コミュニティ、公然とアクセスできるリソース（DNS レコード、ソースコードリポジトリ、テキストのペースト等）が上げられる。

参考文献： [18] (section 2.2), [21]

5.3.11 情報フローの制限

優先度	High
責任者	オペレータ
制御タイプ	予防的，探知的
セキュリティの概念	防御，検知
関連するセキュリティ目的	機密性
関連する脅威	#TC_I_06

対策案：5G ネットワークに関連する内部システムや施設との出入りの情報フローは、制御及び制限される必要がある。

ガイダンス：5G オペレータは、内部組織と外部組織間で交換される情報を識別、分類、監視するためのセキュリティ対策を実施すべきである。このような情報漏えい対策（DLP；Data Loss Prevention）の機能は、ネットワーク機能が 3rd パーティに公開されている場合（例えば、NEF、セキュリティエッジ保護プロキシを介して)、常に 5G システムに関連するが、オペレータの ICT インフラストラクチャ（メールサーバー等）においても重要である。

論理的な DLP に加えて、5G オペレータは、5G インフラストラクチャへの直接アクセスが悪意のあるコンポーネントの侵入や機密情報の窃取に悪用されないように、物理的な対策をさらに検討する必要がある。このためには、以下のような対策が含まれる。:

- 明示的許可なく電子記憶媒体の施設への持ち込み／持ち出しを制限すること
- 記録用機器（携帯電話、デジタルカメラ等）の施設内への持ち込み禁止
- 組織が定義したアセットの位置と移動の監視

参考文献： [08] (section 3.1)

5.4 物理的な対策

5.4.1 安全な施設設計

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	可用性, 認証
関連する脅威	#TC_T_02

対策案:処理されたデータとプラットフォーム自体のセキュリティを促進できるように、5Gシステムコンポーネントの物理環境を設計することが望ましい。

ガイダンス：5G コンポーネントを収容する施設の設計と建設は、収容されたシステムを物理的な被害から保護することに役に立つべきである。これには、施設の地理的位置、その周辺環境、部屋のレイアウトや内部構造、設置される物理的なセキュリティ管理が含まれる。包括的なセキュリティ概念としては、以下の点が考慮できる。:

- 物理的な危害や危険から効果的に保護されることができる施設立地の選定
- 施設内とその周辺の層状のセキュリティ境界の定義
- 指定出入口の定義
- 重要度に基づいたシステムの物理的なセグメンテーション
- 必須のセキュリティゲートウェイの実装

参考文献： [22] (section C), [08] (section 3.11)

5.4.2 物理的なアクセスの制限

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証, 許可
関連する脅威	#TC_T_02, #TC_D_04

対策案：5G システムコンポーネントへの物理的なアクセスは、許可された担当者に制限することが望ましい。

ガイダンス：ネットワークを介したリモートアクセスと同様に、5G システムへの物理的なアクセスは、許可された担当者のみに許可される必要がある。この認可を効果的に実施するためには、これらの個人を一意に認証することが望ましい。したがって、施設への物理的アクセス許可の付与は、以下の活動に先立って行われる必要がある。:

- 施設への許可は、個人の立場や役割に応じて行うこと
- 個人は、組織の規定に基づき、多要素認証にて本人認証を行うこと
- 組織は、施設にアクセスするための個人用のクレデンシャルを発行すること

アクセス許可が付与されると、アクセスクレデンシャルは例外なくその都度検証される必要がある。発行されたクレデンシャルの正確性を確保するために、許可された要員のリストは定期的に見直されることが望ましい。役割または雇用形態の変更により、個人が施設にアクセスする資格を失った場合は、施設のアクセスリストから削除される必要がある。

参考文献： [23] (section C), [08] (section 3.11)

5.4.3 物理的なアクセスの監視

優先度	Critical
責任者	オペレータ
制御タイプ	探知的
セキュリティの概念	検知
関連するセキュリティ目的	認証，許可
関連する脅威	#TC_D_04

対策案：5G コンポーネントを収容する施設への物理的アクセスを完全に可視化し、そのトレーサビリティを確保することが望ましい。

ガイダンス：5G オペレータは、許可された担当者であるか訪問者であるかにかかわらず、システムコンポーネントを収容する施設にアクセスした人の詳細な監査証跡を確立する必要がある。これは、以下の対策を実施することで実現できる。:

- 身元、理由、及び訪問時間を記録したアクセスログの管理
- 施設内での来訪者の無秩序な移動の防止
- 施設内外のビデオ監視技術を採用し、記録の適切な時間に渡る保存

参考文献： [23] (section C), [08] (section 3.11)

5.5 技術的対策

5.5.1 一般的な対策

5.5.1.1 セキュアなシステム工学

優先度	Critical
責任者	サプライヤ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性, 完全性, 可用性
関連する脅威	#TC_I_03, #TC_D_02, #TC_D_03, #TC_E_01

管理策：セキュアなシステム設計と開発の原則が、組織のエンジニアリングプロセスに統合されていることを確実にすることが望ましい。

ガイダンス：セキュリティバイデザイン（SBD：Security By Design）の原則に従い、5G 技術サプライヤは、製品設計や開発プロセスの初期段階からセキュリティのベストプラクティスを推進及び実施することが望ましい。各 5G ネットワーク製品は、その管理下にある情報を保護するための安全対策を提供するのみでなく、ID 管理やアクセス管理、ログ収集システム等、5G オペレータが提供する一元的なセキュリティ管理との統合もサポートする必要がある。セキュアな製品開発に関する基本的な推奨事項は以下のとおり。:

- システムの攻撃対象領域の最小化;
- 受信したすべての入力の検証
- 適切なアクセス制御の実施
- 重要な情報の暗号化

5G システムは API による通信を利用するため、5G 技術サプライヤはこれらの通信インタフェースに基本的なセキュリティ衛生を適用することについて、特に注意を払う必要がある。これには以下の設計と開発の安全対策が含まれる。:

- 各 API エンドポイントが必要最小限の情報のみを公開するように確保
- API 仕様に反する着信要求のコンプライアンスについて検証
- レート制限機能の実装

参考文献： [24], [14], [25], [26]

5.5.1.2 セキュアなネットワーク工学

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	可用性, Segmentation & Segregation
関連する脅威	#TC_D_01, #TC_L_01, #TM_L_01

管理策：セキュアなネットワーク設計の原則が、組織のエンジニアリングプロセスに統合されていることを確実にすることが望ましい。

ガイダンス：5G オペレータのエンジニアリングチームは、以下のセキュアなネットワークアーキテクチャと設計の原則を確保することに精通していることが望ましい。：

- セキュリティバイデザイン：設計プロセスの初期段階からセキュリティリスクと要件を考慮する
- 多層防御：単一点障害を回避する階層型防御モデルを適用することで、セキュリティ対策の冗長性を確保する
- フォールトトレランスとレジリエンス：システムが悪条件でも正常に運用し続け、悪条件に抵抗したり、または悪条件から綺麗に回復したりできることを保証する（「バックアップとリカバリの手順」参照）

参考文献： [16]

5.5.1.3 安全な暗号化アルゴリズム

優先度	Critical
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性, 完全性
関連する脅威	#TC_I_01

管理策：安全な暗号化アルゴリズムを使用して、転送中及び保存中の情報を保護することが望ましい。

ガイダンス：5G サプライヤ及び 5G オペレータは、サービスと関連するデータを保護するために使用される、許容できる暗号化プリミティブを指定することが望ましい。このようなポリシーには、以下のような情報を含める。:

- 許可された暗号化ハッシュアルゴリズム
- 許可された対称暗号及び非対称暗号アルゴリズム
- 楕円曲線暗号のための許容曲線
- 最小鍵長

暗号化アルゴリズムのセキュリティは時間と共に変化するため、組織が採択した暗号化アルゴリズムが必要なセキュリティレベルを満たしているか否かについて、定期的に確認することが望ましい。

5G サービスに関しては、暗号関連のポリシーまたは 5G セキュリティポリシーのいずれかで、以下の点についてのガイダンスを含むことが推奨される。:

- RRC と NAS 機密性アルゴリズム
- RRC と NAS 完全性アルゴリズム
- PDCP 機密性アルゴリズム
- PDCP 完全性アルゴリズム
- SUPI 秘匿アルゴリズム
- (D)TLS、IPsec、JOSE 暗号スイート

参考文献： [27]

5.5.1.4 アイデンティティ及びアクセス管理

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	識別
関連するセキュリティ目的	認証, 認証
関連する脅威	#TC_R_02, #TC_E_01, #TC_E_02, #TW_T_01, #TW_I_01

管理策：5G システム、関連するクレデンシャル、及び許可の運用と維持に使用されるデジタルアイデンィティのための、信頼できる唯一の情報源を確立することが望ましい。

ガイダンス：5G オペレータは、すべてのユーザーアカウントの識別子、クレデンシャル、役割、及び権限を処理する中央 ID 管理システムに、システムユーザーを登録することが望ましい。アカウントの乗っ取りや悪用を防ぐために、そのようなシステムは以下の機能をカバーする。:

- 新規導入システムの自動登録
- システムアカウントと関連データ（役割、特権等）のプロビジョニング、変更、及びデプロビジョニング
- セキュリティポリシー（例：パスワードの長さ、パスワードの年齢、多要素）に従った認証と認可の実施
- 各要素とインタフェースに対して、一意のアイデンティティ割り当て
- アイデンティティのセルフサービス（例：パスワードのリセット、委任）
- 信頼されたパーティとのアイデンティティフェデレーション
- 任意のアカウント活動に関連する監査機能

これらの論理的な ID と、デジタル証明書または実際の暗号鍵（具体的には、秘密鍵／公開鍵のペア）と紐づけて管理することを強く推奨する。ここで、デジタル証明書や実際の暗号鍵は、ID に対する数学的証明を与えるために使用される。

参考文献：-

5.5.1.5 鍵管理

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性，完全性
関連する脅威	#TC_R_02

管理策：5G システムによって使用される暗号化のための秘密情報を安全に管理し、保存することが望ましい。

ガイダンス：暗号鍵によって処理された情報を保護するために、5G システムコンポーネントは、暗号化のための秘密情報（プライベート鍵、パスワード、トークン等）を処理する必要がある。これらの秘密情報が許可されていないパーティに公開されないようにするためには、適切な技術策が必要になる。

したがって、5G 技術サプライヤ及び 5G オペレータは、次に示すような保護対策を実施することにより、そのような情報が常に保護されていることを確実にすることが望ましい。:

- 機密性の高い鍵を扱うシステムコンポーネントに、安全な暗号化モジュールが存在することを保証すること
- 安全な環境内のみで鍵全体を保存して使用することで、鍵の完全性及び機密性を保証すること
- 鍵情報が暗号化モジュールの外で利用可能な場合は、常に代替手段（暗号化、非暗号化、または物理的なメカニズム）を用いて同じ保護レベルを確保すること
- 機密性の高い鍵関連情報は、その寿命後に安全に廃棄すること

特にクラウドネイティブな展開では、秘密管理を単純化するための 1 つのアプローチとして、一元化されたクレデンシャルストアや「ボールト」の使用が上げられる。特定のシナリオでは、これらの関数は、取扱注意なマテリアルを扱い、他のワークロードに代わって暗号化運用を実行するための実行可能なオプションである場合がある。それにも関わらず、適切なレベルのセキュリティを確保するために、ハードウェアベースのセキュリティ要素によりこれらの関数を引き続きサポートする必要がある。

参考文献： [28], [16]

5.5.1.6 セキュアブート手順

優先度	Critical
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	完全性
関連する脅威	#TC_T_04

管理策：起動時における低レベルのファームウェアと OS コンポーネントの正確性を保証することが望ましい。

ガイダンス：5G 技術サプライヤは、ブート手順中にシステムの完全性を検証できるような管理策が利用できることを確実にすることが望ましい。これには、Trusted Platform Module（TPM）等のようなシステム内に信頼の基点（Root of Trust）が存在することが必要となる。システムの完全性を保証する方法としては、以下のようなものが考えられる。:

- 測定されたブート：3rd パーティによって検証可能な低レベルのシステム測定値を記録すること
- 信頼されたブート(セキュアブートとも呼ばれる)：ブート手順の各ステップを期待値に対して暗号学的に検証すること

5G オペレータは、このような管理策が効果的に利用されていることを確実にすることが望ましい。すなわち、信頼されたブート手順においては、非準拠システムのブートアップを禁止するか、または測定されたブート中から取得された情報を禁止するかのいずれかを考慮することによって、そのシステムに置かれている信頼を決定することになる。

参考文献：-

5.5.1.7 システム完全性の監視

優先度	High
責任者	サプライヤ，オペレータ
制御タイプ	探知的
セキュリティの概念	検知
関連するセキュリティ目的	完全性
関連する脅威	#TC_T_04

管理策：システム運用中にローカルに保存された情報の正確性を確実にすることが望ましい。

ガイダンス：セキュアブート手順を補完するために、5G 技術サプライヤは、ホストベースの侵入検知システム（IDS)等のセキュリティソフトウェアを採用することが望ましい。このセキュリティソフトウェアは、システムの変化を継続的に監視し、検出結果を既知の「良好な状態」と比較できる。さらに、5G 技術サプライヤは、特定のシステムタイプのデフォルトの良好な状態を定義することで、構成ファイルやアプリケーションデータ等の関連データまでをカバーできる。5G オペレータは、システムのアラートを監視し、不正行為にタイムリーに対応してインシデント発生の可能性を軽減することが望ましい。

参考文献：-

5.5.1.8 セキュアな管理通信

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	完全性，機密性，認証
関連する脅威	#TC_S_01, #TW_S_02, #TN_S_01, #TC_T_01

管理策：すべての運用ツールとプロトコルが、通信ピア間の相互認証、転送データの機密性及び完全性を提供することを確実にすることが望ましい。

ガイダンス：ネットワーク管理トラフィックは、アクセスクレデンシャル、構成データ、監視データ等、5G 展開に関する最も重要な情報をいくつか含んでいる。そのため、5G オペレータは、以下の保護対策を実施することで、これらの重要な情報が保護されていない状態で送信されないことを確実にすることが望ましい。:

- 組織の暗号化ポリシーに従って、管理プロトコルが安全な暗号化アルゴリズムを利用することを保証すること
- 厳格な相互認証を実施し、理想的には組織の PKI に結びつけること
- 安全でないレガシープロトコル（Telnet、ファイル転送プロトコル、SNMPv2 等）の使用を禁止すること

参考文献：-

5.5.1.9 安全なログファイルの収集と保存

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	完全性，機密性
関連する脅威	#TC_R_01

管理策：システムログデータの作成、転送、中央リポジトリへの保存時における保護を確実にすることが望ましい。

ガイダンス：5G オペレータは、セキュリティ監視の取り組みによりネットワークの実際の状況をタイムリーに得ることができるように、配備されたシステムを通じて収集されたシステムログデータの正確性を確実にすることが望ましい。そのためには、以下のような予防処置を講じることが推奨される。:

- ログ生成モジュールを共通の時間ソースと同期させること
- ログ生成モジュールの報告状況を継続的に監視すること
- 実行的なログレベルの定義と構成（タイムスタンプ、リソース ID、アドレス情報、要求元のエンティティ（名前またはサービス）、アクセス要求の結果等（許可、拒否）の必要な最小限の情報を含む）
- 可能な限り、ロギング出力に機密データを記録しないようにすること
- ログファイルをローカルに保存しないこと。代わりに、生成後すぐに一元管理用データリポジトリにデータを転送すること
- 完全性と理想的には機密性保護を提供するプロトコルを介したログファイルの送信を確保すること
- 一元管理用ログデータリポジトリへのアクセスを制限し、保存されたデータが遡って改ざんされないようにすること
- 組織のルール及び地域の規制に従って適切なログ保存期間を設定すること

上記の推奨事項を専用のロギングポリシーに取り込むことが望ましい。具体的には、ログの生成、転送、保存、分析、及び最終的な削除において期待される挙動と必要なセキュリティ対策をポリシーに記載することが推奨される。

参考文献： [29]

5.5.2 仮想化の対策

5.5.2.1 ハードウェアベースの信頼の基点（Root of Trust）

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性, 完全性
関連する脅威	#TC_T_02, #TW_S_01

管理策：機密性の高い暗号化運用を実行する物理ホストと仮想ワークロードの双方に、信頼の基点を確保することが望ましい。

ガイダンス：機密情報や重要な暗号機能は、ハードウェアベースの信頼の基点（HBRT）によって保存またはサポートされることが望ましい。したがって、仮想ワークロードは、セキュリティエレメント（外部からの解析攻撃に耐えるセキュリティ能力を持った半導体製品等）やトラステッドプラットフォームモジュール（TPM）機能を含むハードウェアセキュリティモジュール等、HBRT を使用することが考えられる。当該要素は、次の要件を満たすことが望ましい。:

- 物理的にも電子的にも耐タンパー性とタンパーエビデント性（解析等が行われた痕跡が残る性質）を備えていること
- 信頼性の高い証明書に基づいた、攻撃に対する耐性を検証すること
- 暗号化及びセキュリティ機能のためにワークロードで使用されるハードウェアベースの計算エンジンを含むこと
- 個々のワークロードに対して HBRT 機能の独立したインスタンスを提供することができること

HBRT と NFVI ホスト間の通信に関しては、以下のセキュリティ保護対策を実施することが望ましい。:

- 各 HBRT をそれのホストシステムに組込み変化を検出すること
- HBRT と他のコンポーネント間のすべてのインタフェース（物理的または論理的）を、改ざん、盗聴、リプレイ、または同様の攻撃から保護すること。
- ホストは、その HBRT が改ざんされたか否かを検出できる能力を持つこと

この要件は、セキュリティプロトコル（PDCP、NAS 等）を終了するか、または機密情報を保存する 5G システムのワークロードに特に関連する。

参考文献： [30]

5.5.2.2 NFVI ホストの堅牢化

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性，完全性，可用性
関連する脅威	#TM_I_01

管理策：５Ｇシステムに関連する仮想ワークロードをホスティングするシステムは、定義されたセキュリティベースラインに基づいて構成及び運用されることが望ましい。

ガイダンス：すべてのシステムに適用すべき一般的な堅牢化対策に加えて、NVFI ホストは、その上で実行されるワークロードに起因する追加的なリスクにさらされる。ホストマシン自体を保護し、上記のワークロード間の分離を確実にするために、5G オペレータは、以下の保護対策が適用されていることを確実にすることが望ましい。:

- ホストがハードウェアによるメモリ管理とダイレクトメモリアクセス機能を提供していること
- OS レベルのアクセス制御（SELinux、sVirt 等）を設定して、仮想ワークロードに機能制御を適用すること
- ワークロード間でメモリページの共有を可能にするホストメモリ重複排除技術を無効にすること
- 仮想ワークロードのバイナリイメージのローカルキャッシュの禁止
- プロビジョニング解除後すぐに、ホストが仮想ワークロード及び関連するすべてのファイルの安全な消去を実行すること
- 組織の暗号化ポリシーに従って、ホストが安全でない暗号化アルゴリズムを仮想ワークロードに提供することを禁止すること

参考文献： [30]

5.5.2.3 仮想化レイヤの堅牢化

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	可用性, 許可, Segmentation & Segregation
関連する脅威	#TM_I_01, #TM_D_01, #TM_E_01, #TM_L_01, #TW_I_02

管理策：仮想化レイヤにおいて、NFVI ホスト及び仮想ワークロードを保護するための適切なセキュリティ対策を実施することが望ましい。

ガイダンス：仮想ワークロードのリソース割り当てと分離を担当する主なコンポーネントであるハイパーバイザでは、それぞれのゲストシステムのリソース使用量を厳密に制限するように構成することが望ましい。ホストシステムの可用性を確保し、ワークロードのサービスレベルを保証するために、仮想プラットフォームのオペレータは、仮想化レイヤが以下の事項を満足することを確実にすることが望ましい。:

- 他に対して特定のワークロードに優先順位をつけることができること
- 定義されたメモリ、計算、ネットワークの制限を実施することができること
- ワークロードに対し最小限の物理リソースを保証できること
- 物理リソースの過剰コミットを防止するように設定されていること
- 特権モードではなく、ユーザー空間でデバイスドライバを実行するように設定されていること
- ハイパーバイザのメモリ重複を無効にするように設定されていること

参考文献： [30], [31]

5.5.2.4 MANO セキュリティ

優先度	Critical
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性，完全性，認証, Segmentation & Segregation
関連する脅威	#TM_S_01, #TM_T_02, #TC_T_03, #TM_T_01, #TW_S_02

管理策：NFV 環境及びその基盤となる計算インフラストラクチャを制御する管理トラフィックのセキュリティを確実にすることが望ましい。

ガイダンス：MANO コンポーネントは、NFV 展開のバックボーンを形成し、最も機密性の高い情報の一部を送信、保存する。MANO は、必然的にほぼすべてのコンポーネントと統合されているため、MANO に影響を与えるセキュリティインシデントは、NFV エコシステム全体に容易に影響を及ぼす可能性がある。この重要性を考えると、5G 技術サプライヤは、設計及び実装の際に、以下のセキュリティ推奨事項に従うようにすることが望ましい。:

- 各 MANO エンティティは、1 つ以上の MANO トラストドメインに割り当てられること
- すべての MANO インタフェースでは、相互認証を厳格に実施すること
- 内部 MANO インタフェースを介して転送されるデータで、機密性及び完全性を保護すること
- NFV イメージライブラリに保存された VNF イメージの不正な変更、削除、挿入を防止すること

本番使用時には、仮想インフラストラクチャのオペレータは、異なる MANO エンティティを分割することで、トラストドメインとその関係が適切に実装されていることを確実にすることが望ましい。例えば、以下を確認することが考えられる。:

- 展開シナリオに基づいた個別の MANO 信頼ドメインの定義
- 異なる MANO 信頼ドメイン間の信頼関係の定義
- 信頼関係が定義されていない MANO の信頼ドメインが、直接または間接的な影響を互いに与えないようにすること

参考文献： [32]

5.5.3 RAN の対策

5.5.3.1 ユーザープレーンの保護

優先度	High
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性, 完全性
関連する脅威	#TC_T_01, #TR_T_02

管理策 : ユーザー機器と 5G 基地局間のユーザープレーンのトラフィックの機密性及び完全性を確保することが望ましい。

ガイダンス：5G オペレータは、無線アクセスを介して転送されるユーザープレーントラフィックの完全性が保護されていることを確認し、エアインタフェース上のデータや RAN システムコンポーネントで処理されるデータにおいて、改ざんを防止する必要がある。この際、以下に注意すること。:

- PDCP セキュリティポリシーが効果的に暗号化と完全性保護を実施することを確認すること
- 組織の暗号化ポリシーに従って、安全な暗号化アルゴリズムを使用すること
- RAN コンポーネントが 5G UE から提供された不正な構成パラメータを受け入れないことを検証すること（例えば、無効な RRC/NAS 完全性保護、不正なアルゴリズム識別子、その他の不正な形式のメッセージを検証する）

参考文献： [33], [16]

5.5.3.2 コントロールプレーンの保護

優先度	High
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性, 完全性
関連する脅威	#TR_T_03

管理策：ユーザー機器と 5 G 基地局間、及びユーザー機器と AMF 間のコントロールプレーントラフィックの機密性及び完全性を保護することが望ましい。

ガイダンス：5G オペレータは、コントロールプレーンのトラフィックが、無線区間または 5G NR コンポーネント間で保護されていない形で転送されないようにする必要がある。この情報を、盗聴や改ざんから保護するために、以下の管理を遵守することが望ましい。:

- RRC 及び NAS のセキュリティポリシーが暗号化アルゴリズムと完全性保護を効果的に実施していること
- 組織の暗号化ポリシーに従って、安全な暗号化アルゴリズムを使用すること
- 5G NR コンポーネントが 5G UE から送信された不正な構成のパラメータを受け入れないこと

参考文献： [33]

5.5.3.3 ミッドホール及びバックホールのセキュリティ

優先度	High
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証, 機密性, 完全性
関連する脅威	#TC_T_01, #TR_T_02, #TR_T_03, #TR_I_02, #TR_I_03

管理策：5G NR システムコンポーネント間の相互認証、及びトランスポートレベルでの機密性及び完全性を保護することが望ましい。

ガイダンス：5G 技術サプライヤと 5G オペレータは、5G NR コンポーネント間のすべてのインタフェースにおいて、相互認証、機密性及び完全性の保護が提供されていることを確認する必要がある。これは、ユーザープレーンとコントロールプレーンのトラフィックを保護する以外に、運用･管理トラフィックを保護するためにも役立つ。3GPP 仕様[33]によると、この保護は、以下の方法によって実現できる。:

- gNB-DU と gNB-CU 間のコントロールプレーンインタフェース（F1-C インタフェース）には、IPsec または DTLS を使用する
- gNB-DU と gNB-CU 間のコントロールプレーンインタフェース（F1-U インタフェース）には、IPsec を使用する
- gNB-CU-UP と gNB-CU-CP 間のインタフェースには、IPsec または DTLS を使用する
- 個々の gNB のコントロールプレーンインタフェース（Xn-C インタフェース）には、IPsec または DTLS を使用する
- 個々の gNB のユーザープレーンインタフェース（Xn-U インタフェース）には、IPsec を使用する
- gNB と 5G コア間のコントロールプレーンインタフェース（N2 インタフェース）には、IPsec または DTLS を使用する gNB と 5G コア間のユーザープレーンインタフェース（N2 インタフェース）には、IPsec を使用する

参考文献： [33]

5.5.3.4 アクセスネットワークの冗長性

優先度	High
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	可用性
関連する脅威	#TR_D_02

管理策：ネットワークアーキテクチャ及び配備において、冗長性を組み組むことで、異常時でもネットワークの可用性を確保することが望ましい。

ガイダンス：冗長性対策は、5GNF、ルータやスイッチ、通信リンク等の個々のシステムコンポーネントに障害が発生した際に、ネットワークのレジリエンシを向上させるのに役立つ。これは、ネットワーク構成要素の到達可能性が制限されるアクセスネットワークに特に

関連する。冗長性対策には、以下のような例があるが、異なる種類の障害シナリオを防止するために、複数のレベルで実装されることが望ましい。:

- NF、ルータ、スイッチ等のネットワーク構成要素の冗長構成
- 物理リンクの冗長構成
- 論理接続の冗長構成

異なるオプションを評価し、必要な投資やセキュリティリスク、被害防止等を考慮して適切なオプションを選定するために、5G オペレータはネットワーク設計の早い段階で冗長性対策を組み込む必要がある。

参考文献：-

5.5.3.5 安全な非 3GPP アクセス

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証, 機密性, 完全性
関連する脅威	#TC_S_01, #TC_T_01

管理策：信頼されていない非 3GPP アクセスネットワークを介して接続する 5G コアとモバイルハンドセット間の信頼確立とその後の通信の安全を確保することが望ましい。

ガイダンス：5G システムはアクセスネットワークに依存しないため、クライアントは様々なアクセスネットワーク技術を介して 5G コアに接続することができる。そのようなネットワークがホームネットワークオペレータによって信頼されているか否かによって、ユーザー機器は EAP-5G プロトコルを介して、信頼された非 3GPP ゲートウェイ機能（TNGF）または非 3GPP インターワーキング機能（N3IWF）に接続することになる。５Ｇオペレータは、非 3GPP アクセス上の 5G UE とコアネットワーク間の通信を保護するために、以下のガイダンスを遵守することが望ましい。:

- 3GPP セキュリティフレームワーク及び／または組織のセキュリティポリシーに基づいて、非 3GPP アクセスネットワークの信頼レベルを決定すること
- 信頼できる非 3GPP アクセスが使用されている場合は、加入者の USIM に信頼できるネットワークのリストを構成すること
- 組織の暗号化ポリシーに従って、TNGF 及び N3IWF で安全な暗号化アルゴリズム

を使用すること

参考文献： [33]

5.5.4 コアネットワークの対策

5.5.4.1 ユーザープレーンの保護

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証，機密性，完全性
関連する脅威	#TC_T_01, #TN_T_01, #TN_I_01

管理策：ユーザープレーンのトラフィックが、5G コアまたは 5G コア内部に接続しているインタフェースを介して保護されずに転送されることがないようにすることが望ましい。

ガイダンス：ユーザープレーンデータの保護は、5G NR のみに関連する訳ではない。展開シナリオによっては、5G コアネットワークの特定の部分（特に UPF）も、信頼性の低い環境で実行される場合がある。これらのシナリオでは、確立されたセキュリティプロトコルを使用することで、すべての外部通信が保護される必要がある。したがって、5G オペレータは、関連するすべてのコアネットワークインタフェース上でユーザープレーンのトラフィックの相互認証、機密性及び完全性を保護することが望ましい。

- UPF を 5G NR に接続するインタフェース（N3 インタフェース）
- 異なる UPF インスタンスを接続するインタフェース（N9 インタフェース）
- UPF を LADN または外部ネットワークに接続するインタフェース（N6 インタフェース）

3GPP TS 33 501 では、上記のインタフェースを保護するために他のセキュリティ手段が提供されていない場合は、NDS/IP（Network Domain Security/IP network layer security）を使用すると規定している。NDS/IP に加えて、5G では、UPF インスタンスを介して他の 5G オペレータとの通信を保護する方法として、Inter PLMN UP Security（IPUPS）機能も導入している。UPF の論理的な部分である IPUPS は、N9 インタフェース上の着信トラフィックに、例えば以下を含む GTP-U セキュリティを適用することが考えられる。:

- 3GPP プロトコル標準に対する GTP-U メッセージの有効性の検証
- GTP-U メッセージにアクティブな PDU セッションのトンネルエンドポイント識別子が含まれていることの検証

3GPP で規定されている制御を超えて、5G オペレータは、5G システムとその加入者を保護するために、ユーザープレーン通信に関連するさらなる管理を実施することも考えられる。

参考文献： [33], [34]

5.5.4.2 PLMN 内の信号セキュリティ

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証，機密性，完全性
関連する脅威	#TC_T_01, #TN_S_02, #TN_T_02, #TN_I_02

管理策： 5Ｇコア内部のコントロールプレーン信号を保護することが望ましい。

ガイダンス:5G コアのアーキテクチャは、柔軟性と拡張性を念頭に置いて設計されており、API 駆動型通信の採用や、コントロールプレーンネットワーク機能間のメッシュネットワーキングを可能にする SCP の（オプションの）統合によって特徴づけられている。これまでは静的な参照点を介して通信していたものが、個々の通信ピアにセキュリティ確保の責任を負わせるゼロトラストネットワークへと変化している。
この変更の結果、5G オペレータがコアネットワーク内のすべての通信フローに対して強力な暗号化対策を実施することは、これまでのモバイル世代以上に重要になっている。これには、以下のような通信中の相互認証、機密性及び完全性の保護が含まれる。:

- サービス登録時及びサービス発見時の NF-NRF 通信
- サービスアクセス時の NF-NF 通信

5G 展開が 5G コアネットワーク NF 間の間接通信に SCP を使用する場合、以下のインタフェースにも同じ推奨事項が適用される。:

- NF と SCP 間の通信
- SCP コンポーネント間の通信

- 異なる SCP インスタンス間の通信

参考文献： [33]

5.5.4.3 PLMN 間の信号セキュリティ

優先度	Critical
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証, 機密性, 完全性
関連する脅威	#TC_S_01, #TN_E_01

管理策：PLMN 間のコントロールプレーンのトラフィック及びネットワーク自体は、モバイルネットワーク間の相互接続インタフェース上の脅威から保護することが望ましい。

ガイダンス：5G システムにおける N32 インタフェースは、外部パーティへさらされる主なポイントの 1 つである。セキュリティエッジプロテクションプロキシ（SEPP）は、アウトバウンドトラフィックへの暗号化保護の適用はもちろん、インバウンド N32 メッセージの制御も実施することで、セキュリティ対策ポイントとして機能する。このリンクを介して転送される情報とネットワーク自体を不正な要求から保護するために、5G 技術サプライヤと 5G オペレータは、N32 インタフェースに関して以下の事項を遵守することが望ましい。:

- PRINS または TLS セキュリティプロトコルを使用すること。中間者がメッセージの内容にアクセスする必要がない場合は、TLS によるエンドツーエンドの保護が強く推奨される
- N32 メッセージの保護に TLS を使用する場合：
    - 組織の暗号化ポリシーに従って、安全な暗号化アルゴリズムを使用した暗号スイートの使用を保証すること（5.5.1.3 項参照）
- N32 メッセージの保護に PRINS を使用する場合：
    - SEPP 保護ポリシーでは、中間者がアクセスすることが明示的に要求されている情報要素を除き、すべての情報要素の暗号化を確実に行うこと
    - SEPP が、SEPP 保護ポリシーで指定された要件に準拠しない、またはメッセージ検証に失敗したすべての受信メッセージを拒否することを確実にすること
- 受信 N32 メッセージのレート制限を適用すること
- 受信 N32 メッセージのためのクロスレイヤのなりすまし防止メカニズムを適用する

こと
- 外部エンティティとの通信において、SEPP によるトポロジーの秘匿化を適用すること

SEPP の PLMN 間のセキュリティは、双方のローミングパートナーが 5G SA を運用している場合にのみ使用できる。ホームネットワーク、または訪問先ネットワークのいずれかが前世代のコアで動作するシナリオでは、PLMN 間の信号が Diameter や SS7 等のレガシープロトコルを介して転送される。

参考文献： [33], [35], [16]

5.5.4.4 API アクセス制御の実施

優先度	Critical
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証, 許可
関連する脅威	#TN_E_01, #TC_E_02, #TNS_I_01

管理策：5G NF の API エンドポイントが通信ピアを適切に認証・認可することが望ましい。

ガイダンス：5G ソフトウェアサプライヤ及び 5G オペレータは、5G NF のすべての API エンドポイントとその他のネットワークコンポーネントにおいて、要求元に対する認証と認可を厳格に実施することが望ましい。3GPP セキュリティ仕様において許容されている認証方式は以下のとおり。:
- TLS を用いたトランスポート層での認証
- NDS/IP による暗黙的認証

ノート: 3GPP 仕様に反する物理セキュリティによる暗黙的認証は、多層防御のセキュリティ原理に違反するため、推奨されない。

サービスにアクセスするための明示的な認証は、常に必要とされる。特に NF API においては、OAuth 2.0 認証フレームワークに基づくトークンベースの認証を利用することが推奨される。認証トークンを発行及び検証するネットワーク関数（NRF と NF サービスプロデューサ）は、アクセスを認める前に、NF サービスの利用者を適切に認証する必要がある。こ

れには、OAuth 2.0 トークンに関連する次のベストプラクティスが含まれる。:

- すべてのトークンには、適切な有効期限が設定されていること
- すべてのトークンは、明確に定義されたクライアントと対象ユーザーを指定すること
- すべてのトークンは、制限されたスコープを持つこと
- すべてのトークンは、特定のネットワークスライスにおいてのみ有効であること
- トークンは、3GPP TS 33.501 で規定されている JSON Web Signatures（JWS）に基づくメッセージ認証コードで保護されていること

5G NF に直接組み込まれた API セキュリティ機能に加えて、5G オペレータは、セキュリティ目的のための専用セキュリティ要素 (API セキュリティゲートウェイ等) をネットワークの主要な場所に展開することも考えられる。特に注意すべき NF API としては、NRF 及び UDM があげられる

参考文献： [27], [36]

5.5.4.5 初期 NAS メッセージの保護

優先度	High
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	完全性
関連する脅威	#TR_T_03

管理策： UE と AMF 間で転送される初期 NAS メッセージの完全性を保証することが望ましい。

ガイダンス：5G は、5G UE が既存のセキュリティコンテキストを使用して保護された必要な情報要素を転送するか、またはセキュリティコンテキストがない場合に限定された情報要素セットのみを送信することを可能にすることで、セッション確立時の初期 NAS メッセージの保護を可能にする。NAS セキュリティコンテキストが確立されると、AMF は、元のクリア・テキスト・メッセージと一緒に、保護された形式で最初の NAS メッセージ全体を再送信するように UE に要求でき、AMF は受信した情報の完全性を検証できる。
5G 技術サプライヤ及び 5G オペレータは、初期 NAS メッセージの完全性チェックが失敗した場合、新しい認証手順を開始することによって、AMF 実装が 3GPP 技術標準で規定さ

れているように動作することを主張する必要がある。

参考文献： [33]

5.5.4.6 加入者のプライバシー

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性
関連する脅威	#TR_I_01, #TN_S_03

管理策：5G システムにおける加入者のパーマネント識別子の保護を確実にすることが望ましい。

ガイダンス：5G では、認証に関与する UE 及び 5G コアネットワーク NF 以外のパーティへの Subscription Permanent Identifier（SUPI）の公開を防止するセキュリティセーフガードを導入している。これは、SUPI を暗号化して Subscription Concealed Identity（SUCI）を形成し、サブスクライバのページングを禁止し、代わりに 5G Global Unique Temporary Identifier（5G-GUTI）に依存することによって実現される。これらの制御を効果的に実施するために、5G 事業者は以下の推奨事項を遵守することが望ましい。

SUPI 秘匿化について：

- 隠された SUPI の計算が実行されるべき 5Ｇセキュリティポリシー、すなわち、USIM または ME の内部で記述すること
- SUCI 隠匿を実行する場所と使用する隠匿スキームを指定するための USIM 内の加入プロファイルの準備
- UE が緊急サービスにアクセスする場合を除き、ヌルスキームで生成された SUCI を 5Ｇコアネットワークが受け付けないようにする
- すべての 5Ｇ UE に SUPI 秘匿化のためのホームネットワーク公開鍵の提供

一時的な加入者 ID について:

- 5G-GUTI の頻繁な再割当ての実施
- 5G-GUTI のランダムな構成要素である 5G-TMSI が、十分なエントロピーと予測不可能性を保証するプロセスで生成されることの保証

参考文献： [33], [16]

5.5.4.7 サービスメッシュセキュリティ

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	可用性, Segmentation & Segregation
関連する脅威	#TN_L_01

管理策: ソフトウェア定義メッシュネットワークのベストプラクティスに従って 5G SCP のセキュリティを確保する必要がある

ガイダンス: サービスコミュニケーションプロキシ（Service Communication Proxy）は、5G コアネットワークの重要な要素で、すべてのコントロールプレーンネットワーク機能に接続し、サービスディスカバリ、メッセージルーティング、ロードバランシング等の基本的な通信タスクをサポートする。NF 間通信のためのその重要な役割を考えると、SCP 自身のセキュリティを確保することは 5G オペレータにとって不可欠である。そのためには、以下のセキュリティ対策を遵守することが望ましい。:

- 5G システムのセキュリティドメインに従って、セグメント化された複数の SCP インスタンスを分散する方法で SCP を展開
- SCP サービスメッシュによって作成されたネットワークセグメンテーションを、特にネットワークの非常に機密性の高い領域で、レイヤ 3 で実装する
- 個々の SCP コンポーネントのリソース使用制限の定義と適用
- SCP に関連する次のような運用データを確実に収集し、一元的に記録する:
    - システムコンポーネントごとのリソース使用率（CPU 負荷、メモリ使用量等）
    - メッセージ統計情報（受信されたメッセージ、拒否されたメッセージ、受け入れられたメッセージの数等）
    - 通信ピアに関する情報（接続された NF、アクティブ/非応答の NF の数、1 秒あたりに送信されたメッセージの数等)

参考文献： [37]

5.5.4.8 ホームコントロールの強化

優先度	Moderate/High
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証, 許可
関連する脅威	#TC_S_01

管理策:加入者に代わってホームネットワークに送信される不正要求を防止することが望ましい。

ガイダンス：5G システムでは、加入者のホームネットワークのオペレータは、プライマリ認証の実行結果（認証が成功したか否かに関わらず）を、UDM による確認を必要とする後続の手順にリンクさせることができる。5G オペレータがこの機能を利用するためには、5G 技術サプライヤは、UDM 実装の一部として認証確認を利用できる機能を提供することが望ましい。
5Gオペレータは、明示的な認証確認を必要とする不正行為が発生し易いシナリオを特定し、それらを 5G セキュリティポリシーに文書化する必要がある。UDM は、直近の正常な認証確認を受け取った後にのみ、これらの手順を許可するように構成する必要がある。情報を Nudm_UECM_Registration 手順にリンクする方法の例については、3GPP の技術仕様に記載されている。

参考文献： [33]

5.5.4.9 DDoS 対策

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	可用性
関連する脅威	#TC_D_01, #TC_D_02, #TN_D_01

管理策：DDoS 攻撃や意図しないトラフィック急増のリスクがあるネットワーク機能は、過

剰なトラフィック負荷から保護することが望ましい。

ガイダンス：多くの 5G NF は、5G システムにおけるその機能と位置のため、DDoS 攻撃の対象となるリスクが特に高い。これには、AMF、N3IWF/TNGF、UPF/IPUPS、NRF、NEF 等のネットワーク機能､及びSCP やSEPP 等の他のネットワークエンティティが含まれる。これらのコンポーネントの可用性を確保するために、5G オペレータは次の推奨事項に従うことが望ましい。:

- 次のような冗長性と適切なフェイルオーバー戦略をネットワークアーキテクチャに組み込む。:
  - 論理システムの冗長性
  - 地理的なシステムの冗長性
  - リンクの冗長性
- 保護を必要とするネットワーク機能の直接の露出を避け、受信トラフィックが複数のインスタンス間で負荷分散されていることを確認すること
- 専用のセキュリティ要素とネットワーク機能の両方で、レート制限及びトラフィックシェーピング技術を採用
- 仮想展開ユニットが、現在の使用率に基づいて、特定の制限内でスケールアップまたはスケールダウンできるようにする

参考文献：-

5.5.5 ネットワークスライシングの対策

5.5.5.1 ネットワークスライスの分離

優先度	Critical
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	可用性, Segmentation & Segregation
関連する脅威	#TNS_D_01, #TC_I_02, #TNS_D_02

管理策：サポートするプラットフォームやアプリケーションを含むネットワークスライスは、互いに効果的に分離することが望ましい。

ガイダンス：ネットワークスライシングにより、5G オペレータは、共通の 5G システム上で多重化された独自のリソース、サービス及び SLA を使用して、複数の仮想ネットワークをプロビジョニングできる。特定の技術というよりもアーキテクチャの概念であるが、ネットワークスライシングは、メッセージ・タグ付け、VLAN、または VPN を利用するなど、異なる方法で実装することができる。効果的なスライスの分離とは、個々のスライスインスタンスが他のインスタンスのパフォーマンスや可用性に影響を与えないことを意味する。この要件を達成するために、5G 技術サプライヤは、次のようなセキュリティ上の注意事項を遵守することが望ましい。:

- マルチベンダー及びマルチテナント環境に適した管理フレームワーク（スライスオーケストレータを含む）の設計及び開発
- ネットワークスライスオーケストレータとスライスインスタンス間及び異なるスライスオーケストレータ間での安全な通信の実施
- 各スライスのネットワークリソースの最小値及び最大値を定義できるようにする
- スライス固有のトラフィックの論理的に分離された処理とスライス固有のデータの保存を保証する
- スライス間の暗号分離を確実に行う

同時に、5G 事業者は、共有プラットフォーム上で異なるネットワークスライスを提供するリスクを評価し、それに応じてネットワークを設計する必要がある。上位レベルでは、5G オペレータにはスライスの分離に 2 つの選択肢がある。:

- ソフトネットワークスライシング:同じリソースを共有するスライスインスタンス。オペレータのポリシーに従ってソフトウェアにサービス品質が適用される
- ハードネットワークスライシング：専用のリソースを使用してインスタンスをスライスするため、2 つのインスタンスが互いに影響し合うことはない

参考文献： [38]

5.5.5.2 仮想ネットワークセキュリティ

優先度	Critical
責任者	オペレータ
制御タイプ	予防
セキュリティの概念	防御
関連するセキュリティ目的	Segmentation & Segregation
関連する脅威	#TNS_S_02, #TNS_D_01

管理策:物理ネットワークから仮想ネットワークへの移行がセキュリティ対策の低下をもたらさないことを保証することが望ましい。

ガイダンス:従来のネットワーク展開では、トラフィックが通過するセキュリティ適用ポイントに物理アプライアンスが配置されることがよくある。純粋に仮想的な、つまりソフトウェアで定義されたネットワークへの移行は、これらの物理的な対策ポイントを目立たなくするが、セキュリティ境界が希薄になる訳ではない。5G オペレータは、トラフィックフローの効果的な分離と仮想ネットワークのセグメント化を保証するために、次の推奨事項に従うことが望ましい。:

- スタンドアロンのファイアウォールではなく、仮想化管理プラットフォームに統合されたファイアウォールを使用する
- 標準の管理プロトコルを使用した中央集中型または統合型 SDN コントローラの使用
- 管理トラフィック用の専用仮想スイッチ及び NIC の使用
- オーバーレイベースのセグメント化（例：VLAN の使用）を物理ネットワークに適用
- 可能であれば、物理ネットワークでネットワーク監視ツールを使用する

参考文献： [39]

5.5.5.3 ネットワークスライスアクセス制御

優先度	Critical
責任者	サプライヤ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証，許可，機密性
関連する脅威	#TNS_S_01, #TNS_I_01, #TC_E_02

管理策：特定のネットワークスライスインスタンスに関連付けられたリソースは、当該スライスのクライアントのみがアクセスできるようにすることが望ましい。

ガイダンス：同じネットワーク関数が複数のネットワークスライスからの情報を処理する可能性があるが、特定のスライスインスタンスに制限されたリソースは、その外部に公開されるべきではない。このレベルのアクセス制御を確保するには、5G サプライヤがネットワーク通信で厳密な認証とスライス固有の認可を実施する必要がある。
この対策は、例えば、要求されたネットワークスライスインスタンスを検証する時の加入者とネットワークとの間の通信のみでなく、NF 間の通信にも関連する。

参考文献：-

5.5.5.4 ネットワークスライスのセキュリティポリシー

優先度	Critical
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証，許可，機密性
関連する脅威	#TNS_E_01

管理策：UE が異なるセキュリティ要件を持つ複数のスライスに加入している場合、セキュリティポリシーはより高いレベルでセキュリティを保証するネットワークスライスを危険にさらさない方法で実施されることが望ましい。

ガイダンス：ネットワークスライスでは、さまざまなパフォーマンス要件のみではなく、セ

キュリティレベルも定義できる。UE はネットワークオペレータの管理ドメインの外にあり、異なるネットワークスライスと並行して通信する可能性があるため、高セキュリティのスライスのセキュリティ要件が、低セキュリティのスライスのセキュリティ要件よりも優先されることが重要である。これに関連する設定パラメータの例を次に示す。:

- 再認証の頻度
- 無線加入者のプライバシー
- 強化されたホーム制御

一般に、5G オペレータは、ネットワークスライスが顧客自身によって管理されているか否かにかかわらず、すべてのネットワークスライスが満たすべき最小限のセキュリティ基準を定義することが望ましい。

参考文献： [38]

5.5.6 MEC の対策

5.5.6.1 MEC アプリケーション監査

優先度	Moderate/High
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	識別
関連するセキュリティ目的	認証, 機密性, 完全性
関連する脅威	#TE_I_01, #TE_I_02

管理策：5G 事業者は、ネットワーク及び処理される通信データのセキュリティを確保するために、3rd パーティの MEC アプリケーションが満たすべきセキュリティ要件を定義することが望ましい。

ガイダンス：5G システムで動作するソフトウェアで実施することが推奨されている一般的なセキュリティ確保の活動に加えて、MEC アプリケーション及びサポート AF は、専用の監査プロセスの対象となるべきである。このようなプロセスでは、加入者データの保護に関する基本的なセキュリティ基準が満たされているか否かを検証することが望ましい。したがって、5G オペレータは、以下を実施することが望ましい。:

- 5G オペレータの MEC 環境に自社のソフトウェアを配備することを希望する MEC

アプリケーション開発者が満たすべきセキュリティ要件(例えば、セキュアな通信、鍵管理、ID 及びアクセス管理）に関する要件を規定する
- 処理される情報の種類（位置データ、ユーザーの音声/映像等)、データの分類、アプリケーション層のセキュリティ管理、LADN での保持時間等、MEC アプリケーションのセキュリティ関連仕様について、適切なドキュメント類を開発者に要求する
- 上記のセキュリティ要件への準拠の証明を MEC アプリケーション開発者に要求するか、または積極的な検証を実施する

参考文献： [40]

5.5.6.2 MEC アクセス制御

優先度	Moderate/High
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	認証, 許可
関連する脅威	#TE_S_01

管理策：MEC アプリケーションへの不正アクセスを防止することが望ましい。

ガイダンス：マルチアクセスエッジコンピューティングは、通信処理の往復時間が短縮されるため、エンドユーザーとの距離が近くなることでメリットが得られる特定のユースケースを支援する視点で期待されている。したがって、これらのアプリケーションへのアクセスは、特定のサービスに加入している特定のユーザーグループに限定される。5G オペレータ及び MEC アプリケーション開発者は、MEC アプリケーションへのアクセスを複数のレベルで制限することが望ましい。以下に例を示す。:
- PCF によって、要求側 UE が MEC サービスへのアクセスを許可されていることを確認する
- SMF が、ユーザーデータを正しい LADN (加入者に最も近い LADN である可能性が高い)に導くタスクを行う
- ローカル UPF によって、MEC アプリケーションの関連するトラフィックフィルタに一致するユーザープレーントラフィックのみを転送する
- MEC アプリ自身によって、アプリケーション層で加入者の認証と認可を行う

MEC アプリケーションを使用したモバイルユーザーの認証では、5G セカンダリ認証も使用できる。このメカニズムにより、外部パーティは、OTT（Over The Top）サービスへのアクセスを許可する前に、追加の EAP ベースの認証手順を実行できる。

参考文献： [40]

5.5.6.3 MEC 制御データの保護

優先度	Moderate/High
責任者	サプライヤ, オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性, 完全性
関連する脅威	#TE_S_01, #TE_T_01

対策案：MEC コンポーネント内部または外部との間で通信されるコントロールプレーンデータの改ざんを防止することが望ましい。

ガイダンス：コントロールプレーントラフィックは、他のネットワークドメインと同様に、機密性及び完全性の保護を必要とする。MEC シナリオでは、サービス設定、アクセスコントロールリストまたはポリシー及び DNS レコードが含まれる場合がある。5G オペレータ、MEC アプリケーション開発者及び MEC プラットフォームオペレータは、以下のセキュリティ対策を遵守することにより、このようなトラフィックの保護を確実にすることが望ましい。:

- 外部インタフェースと内部 MEC コンポーネント間の両方のトランスポート層で、相互認証、機密性及び完全性の保護（MEC アプリケーションとプラットフォーム間、MEC プラットフォームとプラットフォームマネージャ間等）
- 特に重要な制御データに対して、アプリケーション層の完全性を保護し、必要に応じて機密性の保護も実施する。例えば、DNS レコードには DNSSEC を使用したり、時刻データには NTS を使用したりする
- コントロールプレーントラフィックを保護するために使用される暗号化のための秘密情報を適切な安全な環境に保存する

参考文献： [41], [42]

5.5.6.4 MEC ユーザーデータの保護

優先度	Moderate/High
責任者	サプライヤ，オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	機密性，完全性
関連する脅威	#TE_I_01

管理策：ユーザープレーントラフィックは、通信中及び MEC 環境内で保護する必要がある。

ガイダンス：MEC コンポーネントは、ネットワークエッジに配置されているため、中央のネットワーク機能よりも物理的なセキュリティが弱いものであると考えられる。したがって、MEC エコシステム内で交換または保存されるユーザープレーントラフィックの暗号化を実施する理由は、これまで以上に多く存在する。5G オペレータ、MEC アプリケーション開発者及び MEC プラットフォームオペレータは、共同して以下のセキュリティ対策を実施することが望ましい。:

- MEC 環境の外部と内部の両方でユーザーデータを伝送するインタフェースの暗号化と完全性の保護
- ユーザープレーンのトラフィックを保護するために使用する暗号可のための秘密情報を適切な安全な環境に保存
- 永続的なストレージに書き込む前に機密性の高いアプリケーションデータを暗号化
- 自己暗号化ストレージデバイスの活用

参考文献：-

5.5.6.5 MEC 環境の分離

優先度	High
責任者	オペレータ
制御タイプ	予防的
セキュリティの概念	防御
関連するセキュリティ目的	Segregation & Segmentation
関連する脅威	#TE_D_02, #TE_I_02, #TE_E_01, #TE_L_01

管理策：MEC 環境と周囲のネットワークコンポーネントとの間の厳密な分離を確実にすることが望ましい。

ガイダンス：仮想化レイヤ上で MEC ワークロードを分離することに加えて、MEC 配置と周囲のネットワーク機能との間にも厳密な分離が必要である。MEC リファレンス・アーキテクチャは柔軟な導入オプションが可能なため、MEC コンポーネントを RAN またはコア NF いずれかと共存させることができる。このようなシナリオでは、5G オペレータ及び MEC プラットフォームオペレータは、以下のような管理を実施することにより、厳格な分離を実施することが望ましい。:

- 可能であれば、MEC コンポーネントは、他のネットワーク機能と物理的にも論理的にも分離したプラットフォーム上で実行する
- 完全な分離を実現できない場合は、次のような複数のレイヤで厳密に論理的な分離を確保する：
    - MEC コンポーネント用の専用の仮想化トラストドメインを定義して、仮想化レイヤが別々のホスト上で実行できるようにする
    - 専用の MANO トラストドメインを定義し、管理情報を完全に分離して、他のドメインに影響を与えないようにする

同様に、ユーザープレーン通信やコントロールプレーン通信等のさまざまなトラフィックカテゴリにも、厳密な分離を適用することが考えられる。例えば、MEC アプリケーション及び UE からアクセスするユーザーは、MEC プラットフォームの管理インタフェース及びサービスにアクセスできないようにする。このような分離は、異なるシステムレイヤで提供される可能性があるが、5G オペレータは、多層防御の概念に従ってこの対策を実施するとよい。

参考文献： [40]

5.5.6.6 サードパーティによる MEC アプリの制御された管理

優先度	Moderate/High
責任者	サプライヤ，オペレータ
制御タイプ	予防的，探知的
セキュリティの概念	検知，防御
関連するセキュリティ目的	許可，可用性
関連する脅威	#TE_D_01

管理策：MEC アプリケーションと、サポートする 3rd パーティアプリケーション機能及び/又は MEC UserApps との間の相互作用を監視し、適切に制御することが望ましい。

ガイダンス：5G システムでは、3rd パーティが MEC プラットフォームや関連するトラフィックルーティングのワークロードに積極的に影響を与えることができる。この機能は、外部 AF と UserApps の誤動作によってサービスへの悪影響を及ぼす可能性があるため、これらのエンティティからのすべての要求を検証することが推奨される。したがって、5G 技術サプライヤ、MEC プラットフォームオペレータ及び 5G オペレータは、以下のようなセキュリティ対策を実施することが望ましい。:

- 特定 AF が影響を及ぼす可能性がある MEC サービス及びモバイル加入者を指定し、NEF 及び PCF においてセキュリティポリシーを適用する
- MEC プラットフォーム全体に渉る MEC アプリケーションインスタンスのトレーサビリティ
- 特に AF や MEC UserApps などの外部エンティティによって制御される場合に、MEC アプリケーションインスタンスにおけるリソース制限の適用
- 5G ネットワーク（MEC プラットフォームを含む）と、AF や MEC User Apps などの外部エンティティとの間の通信の継続的な監視

参考文献：-

6. 用語と定義

3GPP	Third Generation Partnership Project、第三世代以降の移動体通信の標準化プロジェクト
5G Core	5G システムのコアネットワーク、 特定のタイプのネットワーク機能(UPF、AMF 等)が含まれている
5G NR	3GPP で定義された 5G 無線技術を利用した 5G 新無線アクセスネットワーク
AF	コア 3GPP 仕様外の付加サービスを実行する汎用ネットワーク機能であるアプリケーション機能。PCF を介して直接、または NEF を介して間接的に組み込むことができる
AMF	アクセスモビリティ管理機能、加入者認証・セキュリティ・位置情報管理用ネットワーク機能
API	Application Programming Interface、サービスと製品の相互通信を可能にする一連のファンクション及びプロシージャである
ARPF	認証に使用される資格証明を保持及び処理する AUSF の機能コンポーネント
AUSF	Authentication Server Function、UDM に格納されたサブスクライバ情報に対してサブスクライバ/UE を認証するネットワーク機能
CP	コントロールプレーン、モバイルネットワーク内のユーザープレーントラフィックの送信を管理するためのシグナリング情報
CU	Centralized Unit、gNodeB の一部であり、複数の DU に接続する無線のベースバンド部分を指す。集約ベースステーションまたは集約ノードとも呼ばれる
(D)DoS	（分散型）サービス拒否攻撃、不正なパケットまたは大量のトラフィックを送信してサービスを停止する悪意のある攻撃
DPDK	データプレーン開発キット、ユーザー空間ライブラリとドライバで構成され、パケット処理を高速化する
DU	分散ユニット、gNodeB の一部であり、アンテナを含む無線部分を指し、リモートステーションまたは分散ノードとも呼ばれる
gNB	gNodeB、ユーザー装置と 5G コアとの間でトラフィックを送受信する 5G 無線基地局である。分散展開では、RU、DU 及び CU で構成される。
GPRS	汎用パケット無線サービス、セルラーネットワークを介してデータを転送するために使用される
GTP	GPRS Tunneling Protocol、GSM、UMTS 及び LTE ネットワークで使用される
HBRT	ハードウェアベースの信頼のルート、コンピュータシステムのすべて

	の安全な運用が信頼する基盤
IDS/IPS	侵入検知/防御システム、ネットワークトラフィックの分析と監視によるネットワークへのサイバー攻撃の検知/防止
IPUPS	PLMN UP 間セキュリティ、UPF の機能コンポーネント
JOSE	Javascript オブジェクトの署名と暗号化、特定のクライアントに関する認証情報をターゲットシステムに提供する
JWS	JSON Web 署名、任意のデータへの暗号署名に使用される JOSE の一部である
JWT	JSON Web トークン、JSON データの署名と暗号化を規定するオープン標準である JOSE の一部
LADN	Local Area Data Network、ローカル化されたネットワークリソースで、限られた地理的エリア（例えば、マルチアクセスエッジコンピューティングの一部として）に対して計算及びストレージサービスを提供する
MANO	管理とネットワークオーケストレーション、NFV 環境の管理、運用、最適化のための統合アーキテクチャ
ME	移動機器、 UE のユーザー制御部分
MEC	マルチアクセスエッジコンピューティング（Mobile Edge Computing にもなる）、クラウドコンピューティング機能、及びネットワークのエッジでの IT サービス環境により、超低レイテンシと高帯域幅を実現できる
中間者攻撃	2 つの通信パートナー間の悪意のある行為者が、送信された情報を抽出または修正するために、それぞれ相手として装う中間者攻撃
MNO	移動体通信オペレータ、無線音声・データ通信を提供
N3IWF	非 3GPP インターワーキング機能、信頼できない非 3GPP アクセスネットワークを 5G コアに接続するために使用される
NAS	Non-Access Stratum protocol、5G UE と AMF 間でコントロールプレーンデータを交換するために使用される
NDS	Network Domain Security
NEF	ネットワーク公開機能、3rd パーティの IP ネットワークとインタフェースし、3 GPP サービスを安全に公開するためのネットワーク機能
ネットワークスライス	モバイルネットワークの物理インフラストラクチャを、それぞれ異なる QoS レベルを提供できる複数の仮想ネットワークに分割できるようにする技術概念
NF	ネットワーク機能、5G システムの明確な機能の構成要素
NFV	ネットワーク機能仮想化、仮想ハードウェア抽象化を使用して、ネットワーク機能を実行するハードウェアから分離する

NFVI	ネットワーク機能仮想化インフラストラクチャ、基盤となる物理インフラストラクチャと仮想化レイヤの両方で構成される、NFV 導入の基本インフラストラクチャ
NFVO	NFV Orchestrator、NFV 環境の高度な管理及び構成タスクを処理する
NGMN Alliance	次世代モバイルネットワークアライアンス、ワイヤレスネットワークの次の進化のためのソリューションの共通のビューを開発するための候補技術を評価するオープンフォーラム
NRF	ネットワークリポジトリ機能、使用可能なネットワークサービス、ネットワーク機能、及びそのプロファイルに関する情報を格納する中央ネットワークレジストリのこと。NF 登録、検出、認証、認可等の主要サービスを容易にする
OAM	運用、管理及び保守、システムの運用、管理及び保守に関連するプロセス、アクティビティ、ツール及び標準
OAuth2.0	5G システムで採用されているトークンベースの認証フレームワーク
Open5GCore	5G コアネットワークのオープンソース実装
OpenStack	仮想化によって IaaS（Infrastructure as a Service）環境を構築するためのオープンソースプラットフォーム
OS	Operating System
PCF	Policy Control Function、サービスの集中的な実施ポイント及びネットワークスライスへの加入者アクセス、サービス、QoS、データ使用等の側面を制御するセキュリティポリシー
PDCP	Packet Data Convergence Protocol、ユーザー/コントロールプレーンデータの転送、ヘッダー圧縮、暗号化及び完全性保護を上位レイヤに提供する
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network、すべての地上局ベースの無線ネットワークサービス
PRINS	Protocol for N32 Interconnect Security、2 つの SEPP 間の相互接続でシグナリングデータを保護するために使用されるセキュリティプロトコル
QoS	Quality of Service、トラフィックの優先順位付けとリソース予約により、専用トラフィックのサービス品質を実現する
RRC	Radio Resource Control protocol、UE と基地局間のコントロールプレーン通信に使用される
(R)RU	（Remote）Radio Unit、分散 RAN 配置で DU 及び CU から分離された無線トランシーバ要素
RAN	Radio Access Network、無線技術を利用したアクセスネットワーク。

	5G では、複数の gNB で構成される（5G NR を参照）
REST	Representational State Transfer、Web サービスで一般的に使用されるソフトウェア設計の事実上のスタンダード。この文脈では、主に RESTful API を指す。
SCP	Service Communication Proxy、5G コアネットワークのネットワーク機能を接続する接続ファブリック（一般的にメッシュネットワークによって実装される）
SDN	Software Defined Network、ネットワークプログラム可能性のための新しいアプローチ。オープンなインタフェースを介してネットワーク動作を動的に初期化、制御、変更及び管理するテクノロジー
SEAF	Security Anchor Function、アクセスしたネットワークのルートキーを格納する Network Function。これにより、高速認証が可能になる。AMF と併用してもよい
セキュリティ制御	物理的財産、情報、コンピュータシステム、またはその他の資産に対するセキュリティリスクを回避、検出、対処、または最小限に抑えるための高度な保護手段または対策
セキュリティ対策	関連するセキュリティコントロールを達成するための特定のセーフガードまたは対策
SEPP	Security Edge Protection Proxy、ネットワーク相互接続で透過的なセキュリティプロキシ。送受信メッセージにセキュリティを適用し、メッセージフィルタリングやレート制限等の追加のセキュリティ機能を実行する
SIDF	Subscriber Identity Deconcealing Function、UE によって送信された隠された SUCI を復号化するネットワーク機能
SIEM	Security Information and Event Management
SMF	Session Management Function、データの仮想化通信パスのセッションを管理するネットワーク機能
SNMP	Simple Network Management Protocol、ネットワークデバイス間で管理情報を転送するために使用される
SR-IOV	Single-root input/output virtualization
SSH	Secure Shell Protocol、リモート・マシンへの安全なアクセスと通信を提供する
SUCI	Subscription Concealed Identifier、UE と SIDF の間で暗号化され、プライバシーを強化する SUPI の保護された形式である
SUPI	Subscription Permanent Identifier、モバイルネットワークユーザー/サブスクリプションをグローバルに一意に識別する。形式は、IMSI（International Mobile Subscriber Identity）または NAI（Network Access Identifier）がある

TLS	Transport Layer Security Protocol、アプリケーション層データの通信セキュリティを提供する
TNGF	Trusted Non-3GPP Gateway Function
UDM	Unified Data Management、加入者データとプロファイルを保持するAUSF のネットワーク機能の 1 つ
UE	User Equipment、モバイル機器と Universal Subscriber Identity Module で構成される加入者のモバイルファシリティ
UP	User Plane、モバイルネットワーク内でユーザーデータを伝送するトラフィッククラス
UPF	User Plane Function、パケットルーティングや転送のようなユーザープレーン動作を容易にするネットワーク機能
USIM	Universal Subscriber Identity Module、hUE のホームネットワークオペレータ制御部
VIM	Virtualized Infrastructure Manager、NFVI コンポーネントの制御、管理、及び監視に使用される
VNF	Virtual Network Function、NFVI に導入可能なネットワーク機能の実装
VNFI	Virtual Network Function Image
VNFM	VNF Manager、VNF インスタンスに関連するライフサイクル管理タスクを処理する

参考文献・参照ウェブサイト

[01] "ISO/IEC TS 27110 - Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines," 2 2021.

[02] NIST, "NIST Cybersecurity Framework," no. V1.1, 4 2018.

[03] 3GPP, "TS 23.501 - Technical Specification Group Services and System Aspects; System architecture for the 5G System (5GS); Stage 2," no. V16.7.0, 12 2020.

[04] ORAN Alliance, "O-RAN Architecture Description," no. v05.00, 2021.

[05] M. S. M. G. D. P. T. H. W. M. S. K. P. G. D. Y. Y. H. M. Lipp, "Meltdown: Reading Kernel Memory from User Space," 2018.

[06] NIST, "SP 800-125B - Secure Virtual Network Configuration for Virtual Machine (VM) Protection," 3 2016.

[07] ETSI, "GS MEC 002 - Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements," no. V2.2.1, 1 2022.

[08] NIST, "SP 800-204 - Security Strategies for Microservices-based Application Systems," 8 2019.

[09] NIST, "SP 800-161 - Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (Draft)," 10 2021.

[10] ENISA, "Threat Landscape for Supply Chain Attacks," 7 2021.

[11] NIST, "SP 800-150 - Guide to Cyber Threat Information Sharing," 10 2016.

[12] NCSC, "You shape security," no. V1.0, 2 2019.

[13] GSMA, "PRD FS.16 - Network Equipment Security Assurance Scheme – Development and Lifecycle Security Requirements," no. V2.0, 2 2021.

[14] NCSC, "Secure development and deployment guidance," no. V1.0, 11 2018.

[15] CISA, "Defending Against Software Supply Chain Attacks," 4 2021.

[16] ENISA, "Security in 5G Specifications – Controls in 3GPP," 2 2021.

[17] NIST, "SP 800-40 Rev. 3 - Guide to Enterprise Patch Management Technologies," 7 2013.

[18] ENISA, "Proactive detection – Measures and Information sources," 5 2020.

[19] NCSC, "Incident Management," 9 2019.

[20] D. K. K. H. T. P. C. Rupprecht, "Breaking LTE on Layer Two," 5 2019.

[21] NIST, "SP 800-92 - Guide to Computer Security Log Management," 9 2006.

[22] Attorney-General's Department, Australian Government, "PSPF policy 16: Entity facilities," 5 2019.

[23] Attorney-General's Department, Australian Government, "PSPF policy 15: Physical security for entity resources," 5 2019.

[24] ETSI, "GS NFV-SEC 009 - Report on use cases and technical approaches for multi-layer host administration," no. V1.1.1, 12 2015.
[25] NIST, "SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations," 9 2020.
[26] NIST, "SP 800-125A Rev. 1 - Security Recommendations for Server-based Hypervisor Platforms," 6 2018.
[27] 3GPP, "TS 33.210 - Network Domain Security (NDS); IP network layer security," no. V16.4.0, 7 2020.
[28] OWASP Foundation, "OWASP API Security Top 10 2019 - The Ten Most Critical API Security Risks," 12 2019.
[29] NIST, "SP 800-50 - Building an Information Technology Security Awareness and Training Program," 10 2003.
[30] ETSI, "GS NFV-SEC 012 - System architecture specification for execution of sensitive NFV components," no. V3.1.1, 1 2017.
[31] NIST, "SP 800-57 Part 1 Rev. 5 - Recommendation for Key Management: Part 1 – General," 5 2020.
[32] ETSI, "GS NFV-SEC 014 - Security Specification for MANO Components and Reference points," no. V3.1.1, 4 2018.
[33] 3GPP, "TS 33.501 - Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G System," no. V16.5.0, 12 2020.
[34] GSMA, "PRD FS.37 - GTP-U Security".
[35] GSMA, "PRD FS.36 - 5G Interconnect Security".
[36] 3GPP, "TS 33.310 - Network Domain Security (NDS); Authentication Framework (AF)," no. V16.6.0, 12 2020.
[37] NIST, "SP 800-125 : Guide to Security for Full Virtualization Technologies," 1 2011.
[38] NGMN, "5G Security Recommendations Package #2: Network Slicing," 4 2016.
[39] NIST, "SP 800-61 - Computer Security Incident Handling Guide," 8 2012.
[40] NGMN, "5G Security - Package 3: Mobile Edge Computing / Low Latency / Consistent User Experience," 10 2016.
[41] R. A. R. L. M. M. D. R. S. Arends, "RFC 4033 - DNS Security Introduction and Requirements," 3 2005.
[42] D. S. D. T. K. D. M. S. M. Franke, "RFC 8915 - Network Time Security for the Network Time Protocol," 9 2020.
[43] . ETSI, "GS MEC 003 - Multi-access Edge Computing (MEC); Framework and Reference Architecture," no. V2.2.1, 12 2020.
[44] ETSI, "GS NFV 002 - Network Functions Virtualisation (NFV); Architectural Framework," no. V1.2.1, 12 2014.

[45] NIS Cooperation Group (NIS CG), “EU coordinated risk assessment of the cybersecurity of 5G networks,” 10 2019.

付録 A：Open RAN セキュリティに関する考慮事項

Open RAN のセキュリティ面は、技術の開発以来、多くの議論の対象となっている。一部の議論によれば、モバイルネットワーク事業者が RAN ソフトウェアについて多様な制御が可能になったことは、全体としてはるかに安全なシステムとなったことに等しい[46]と言われている。一方で、他の議論として、付加的なインタフェース、複雑さ、そして RAN コンポーネントの開発から統合に至るまでのセキュリティを単一のパーティで保証することができないことなどにより、攻撃対象が増加し、より大きなセキュリティリスクをもたらす[47]とされている。

以下において、仮想化されて相互運用可能な RAN ネットワークの構築に特化した主要なセキュリティ上の考慮事項の概説し、それらを処理する方法に関するハイレベルなガイダンスを提供する。

(1) 技術的な観点

技術的な観点から見た Open RAN の最も根本的な相違点は、**RAN 機能がソフトウェア化され、基盤となるプラットフォームの仮想化が強調されるようになった**ことである。これらの概念は既にモバイルコアネットワークで多く採用されているが、これらを RAN の大部分に適用することは新しい展開と言える。これにより、RAN ソフトウェアの複雑さと攻撃対象が増加すると同時に、従来は現場のハードウェアコンポーネントの内部に含まれていた多くの RAN ロジックの物理的な露出を軽減することができる。展開のタイプに応じて、コアネットワークのためにすでに導入されている仮想化とクラウドセキュリティのベストプラクティスを Open RAN 展開にも採用することが期待されている。

次に、共通の仮想プラットフォームに RAN エコシステムの大部分を展開することで、**一貫したセキュリティ体制を適用することが大幅に容易になる**。オペレータは、管理ツールとオーケストレーションツールの助けを借りて、各ワークロードの場所、構成、セキュリティ強化のステータス、及びその他のセキュリティ関連データを決定できる。理想として Open RAN の展開は、運用スタッフが構成を一度指定すると、管理ツールとオーケストレーションツールがポリシーの適用を行うといったポリシーベースのセキュリティも活用するだろう。

最後に、Open RAN は**運用面のセキュリティに対して更なる利点を持つ**ことが期待される。システムコンポーネントが標準化されたプロトコルを介して通信し、汎用ハードウェア上で実行されることを考えると、垂直に統合された RAN ソリューションと比較して、ネットワーク資産と交換されたデータの運用的な可視性が向上される。同様に、汎用技術の広範な使用により、IT 環境において使用される多くのデファクトの標準ツールとの統合も可能になる。これは、ID とアクセス管理、ログ収集、脆弱性スキャン等の必須のセキュリティ制御に役立つ。

上記について言えるのと同様に、Open RAN 技術に関連するセキュリティリスクは存在する。初期の開発段階においては、他の技術仕様、つまり 3GPP 仕様による開発と比較すると、Open RAN 仕様は、まだ完璧なセキュリティ観点のガイダンスを提供していない[48]。仕様策定の努力と産業界全体の改善が必要とされる間も、今日既に個々の組織において、安全でないネットワークプロトコルを排除するなど、確実なベストプラクティスが実行されている。Open RAN 展開におけるセキュリティ対策の詳細については、(3) 項で述べる。

(2) プロセス的な観点

RAN 技術スタックの変更とは別に、Open RAN への移行によって、ネットワークの展開と管理のためのオペレータのプロセスが大幅に変更されることが予想される。

ネットワークオペレータが展開中や統合中にどの程度の制御を適用したいかに応じて、オペレータは、**テスト、検証、及びセキュリティ保証のためにより多くの責任を負う**必要がある。RAN コンポーネントとそれをサポートする管理及びオーケストレーションシステムは単一のソースによって提供されない可能性があるため、相互運用可能性と一貫したセキュリティ体制を確保することは MNO の責任になる。これを効率的に行うために、ネットワークオペレータは広範なテストの実施や検証能力を確立する必要がある。このような付加的な努力を容易にこなせないネットワークオペレータは、これらのタスクの一部を 3rd パーティのシステムインテグレータにアウトソーシングするかもしれない。Open RAN のいくつかの利点を利用できるようにする実行可能なオプションだが、このアプローチは、ネットワークソフトウェアをより多く制御できるという利点を相殺する。

Open RAN がもたらすこのような利点の 1 つは、**ソフトウェアのロールアウトプロセスに対する制御の増加**である。これにより、オペレータが垂直統合型 RAN よりも迅速にソフトウェアアップデートやセキュリティパッチを展開できるようにする。例えばオペレーティングシステム内のソフトウェアコンポーネントにアップデートが必要な場合、オペレータは RAN ベンダーがこのパッチを提供するまで待つ必要はない。その代わりに、自分でアップデートを統合してテストすることができる。本番環境でのパフォーマンスを検証するために、ネットワークの一部にのみアップデートを展開することも可能である。したがって、RAN ソフトウェアと基盤となるプラットフォームに対する制御の増加は、アップデートとパッチのサイクルを短縮できる。

もちろん、展開や統合プロセスにおける上述の変更には利点だけがあるわけではない。これらはネットワークオペレータに付加的な複雑さをもたらす。サプライヤのリストが多様化すると、**マルチベンダー管理がさらに複雑になる**。O-RAN 仕様書は Open RAN システムの主要なインタフェースについて説明しているが、すべてのシステムコンポーネント間の相互運用可能性を確保し、すべての管理ツールや操作ツールをサポートするための取り組

みを依然として要求するだろう。これには異なるサプライヤの数に応じて複雑さが追加され、一つの Open RAN 展開にどの程度の多様性が適切であるかはまだ分からない。

潜在的には、多数の異なるベンダーを同時に統合するよりもはるかに重要なのは、必要に応じて、ベンダーを切り替えられることである。Open RAN 技術サプライヤを選定する際に、セキュリティは非常に重要な役割を果たす。ソフトウェア定義ソリューションやオープンソース技術の利用拡大と同時に標準化範囲の拡大により、多くの新たなベンダーが通信市場に参入できるようになった。これは一般的にポジティブな発展である同時に、**適切なベストプラクティスを満たさない製品やサービスを提供する未熟なベンダーの参入**につながる可能性がある。

(3) まとめ

前項で説明したように、ネットワークオペレータが RAN 展開をより詳細に制御できることが、Open RAN の高い評価の主な理由である。O-RAN のような取り組みは基本的な技術的枠組みを確立しようとしているが、この新しい概念を採用するための正解は一つではない。代わりにネットワークオペレータは、Open RAN の利点のうちどれが彼らにとって最も重要であるかを判断し、それに応じて技術やプロセスを開発する必要がある。以下に、Open RAN の採用を検討しているネットワークオペレータに対して、セキュリティを確保する方法についてハイレベルなガイダンスを提供する。:

- Open RAN 展開を採用する主な動機（例えば制御の最大化、セキュリティの向上、CAPEX の削減等）を決め、それに応じて、引き受けるべき責任のレベルを決定する
- Open RAN 技術仕様の範囲外で、Open RAN ベンダーが遵守することが期待されるセキュリティ要求を定義し実行する
- 認証及びアクセス管理、権限管理を含むゼロトラストのベストプラクティスを促進するためのセキュリティ管理フレームワークを開発する
- 上述したセキュリティ機能を統合し、関連する標準（例えば O-RAN、3GPP）に準拠していることを保証するネットワークアーキテクチャを設計する
- ベンダーが安全な製品とサービスを提供できるように、ベンダーの安全な開発プロセスとライフサイクルプロセスについて適切なデュ―デリジェンスを実施する
- 新しいソフトウェアリリースを効率的・継続的に導入するためのインテグレーションとテスト能力及び関連プロセスを確立する
- xApps/rApps の許可を最小限とする
- ソフトウェアセキュリティ、仮想化、クラウド等の分野に関連するチームの内部スキル開発を促進する
- 一貫したセキュリティ保証と効率的なセキュリティ監視、変更とパッチ管理を適

用する運用モデルを設計する

本文書の第 5 章に記載されている以下のセキュリティ制御は、上記のハイレベルなガイダンスに直接関連している。Open RAN 展開を安全にするために必要な注意事項は以下のみではない。ここでは、上記の推奨事項を実施するために必要な具体的な制御について概説している。

- 5.1.6　ベンダーのデュ―デリジェンス
- 5.5.1.1　セキュアなシステム工学
- 5.5.1.2　セキュアなネットワーク工学
- 5.2.1　セキュリティ教育及び意識向上
- 5.3.1　セキュアなソフトウェア開発プロセス
- 5.3.3　セキュリティ保証
- 5.3.7　セキュリティ監視
- 5.3.5　変更管理
- 5.3.6　パッチ管理

参考文献

[46] Altiostar, "Security in Open RAN," 1 2021.
[47] Ericsson, "Security Considerations of Cloud RAN," 8 2021.
[48] BSI, "Open RAN Risk Analysis," no. 1.2.1, 2 2022.

以上