参考資料１

５Ｇネットワーク構築におけるセキュリティに関する対策等の留意点
（令和２年度版）

2021 年 5 月 13 日

1 適用領域

本文書は、5G システム（5GS）の包括的な脅威モデル化と分析結果、および 5G ラボ環境で実施された実践的なセキュリティテストから得られた教訓に基づいて、ハイレベルなセキュリティガイダンスを参考情報として提供するものである。本文書は、5G 環境を導入・保守する事業者、および 5G ネットワーク機能（NF）やアプリケーションを実装する開発者を対象としている。

本文書は、総務省における令和元年度および令和二年度「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」業務の成果の一部として整理したものであり、今後、令和三年度末までに、本文書の内容について更なる規定の拡充を行う予定としていることから、規定内容が削除、変更、追加される可能性がある。

また、本文書は、５Ｇ システム運用者、５Ｇ システム開発者および５Ｇ 利用者に対して推奨するセキュリティ対策であり、「ガイダンス」として記載したセキュリティ対策は、実施のための必須基準ではないことに留意されたい。

2 用語と定義

本文書では、5G エコシステムの技術や概念に関連する以下の用語および定義を使用している。

3GPP	Third Generation Partnership Project、第三世代移動通信以降の標準化プロジェクト
5G コア	すべてを包含する 5G システムのコアネットワーク
5G NR	5G New Radio、3GPP で定義された 5G 無線技術を利用した無線アクセスネットワーク
5GS	5G System、5G UE、5G NR（無線アクセスネットワーク）、5G コアネットワークで構成されるエンドツーエンドの 5G ネットワーク
AF	Application Function、一般的なネットワーク機能で、3GPP のコア仕様の外で補助的なサービスを実行するもの。PCF を介して直接、または NEF を介して間接的に統合することができる。
AMF	Access and Mobility management Function、加入者認証、セキュリティ、位置情報管理のためのネットワーク機能
API	Application Programming Interface、ソフトウェアやハードウェアの機能を利用するためのインタフェース仕様
ARPF	認証に使用されるクレデンシャルを保持し、処理する AUSF の機能コンポーネント
AUSF	Authentication Server Function、UDM に格納されている加入者情報に対して加入者/UE を認証するネットワーク機能。
CP	Control Plane、モバイルネットワーク内のユーザプレーントラフィックの伝送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。アグリゲーション基地局やアグリゲーションノードとも呼ばれる。
(D)DoS	(Distributed)Denial of Service、不正なパケットや膨大なトラフィックを送信してサービスを停止させる悪意のある攻撃
DU	Distributed Unit、gNodeB の一部で、アンテナを含む無線部を指し、リモートステーションや分散ノードとも呼ばれる。
gNB	gNodeB、ユーザ機器と 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。分散型の展開では、RU、DU、CU で構成されている。
GTP	GPRS Tunnelling Protocol、GSM 用に設計された GPRS を伝送するために使用される IP ベースの通信プロトコル群で、UMTS、LTE、5G でも利用可能
HBRT	Hardware-based Root of Trust、耐タンパー性能を信頼の起点の機能を提供するハードウェア

IDS	Intrusion Detection System、ネットワーク上のパケットをキャプチャし、攻撃や侵入等の不正な通信を検知するシステム
IPS	Intrusion Prevention System、IDS の不正な通信の検知に加え、その通信の防御も行うことが可能なシステム
IPUPS	Inter PLMN UP Security、UPF の機能コンポーネント
JOSE	Javascript Object Signing and Encryption、2 者間で認証情報などを安全に転送する方法を提供することを目的としたフレームワーク
JWS	JSON Web Signature、JOSE の一部
JWT	JSON Web Tokens, JOSE の一部
LADN	Local Area Data Network、限られた地理的エリアで計算とストレージサービスを提供するローカライズされたネットワークリソース(例：マルチアクセスエッジコンピューティングの一部)。
MANO	Management and Network Orchestration、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	Mobile Equipment、UE のユーザ制御部分
MEC	Multi-access Edge Computing（Mobile Edge Computing とも言う)、ネットワークエッジにあるクラウドコンピューティング機能と IT サービス環境のことで、超低遅延・高帯域で提供できる。
N3IWF	Non-3GPP Interworking Function、信頼されていない非 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機能
NAS	Non-Access Stratum protocol、5G UE と AMF の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、3GPP が定めたセキュリティアーキテクチャで、同じセキュリティドメイン内の通信のセキュリティ確保、及び、異なる事業者間の接続におけるセキュリティドメイン間の相互接続のセキュリティ確保を規定
NEF	Network Exposure Function、3rd パーティの IP ネットワークとのインタフェースを行い、3GPP サービスを安全に露出させるためのネットワーク機能。
NF	Network Function、5G システムの明確な機能構成要素
NFV	Network Functions Virtualization、仮想ハードウェアの抽象化により、実際に運用されているハードウェアからネットワーク機能を分離する仕組み。
NFVI	Network Functions Virtualization Infrastructure、NFV 展開のベースインフラであり、基盤となる物理インフラと仮想化レイヤの両方で構成される。
NRF	Network Repository Function、利用可能なネットワークサービス、ネットワーク機能、およびそれらのプロファイルに関する情報を保存する中央ネットワークレジストリ。NF 登録、ディスカバリー、認証、認可などの主要なサー

	ビスを容易にする。
OS	Operating System、コンピュータの管理を行うソフトウェア基盤
PCF	Policy Control Function、ネットワークスライスへの加入者アクセス、サービス、サービス、QoS、データ使用量などの側面を制御するサービスおよびセキュリティポリシーの中央執行ポイント。
PDCP	Packet Data Convergence Protocol、レイヤ 2 の中で機能し、秘匿、正当性確認、順序整列、ヘッダ圧縮などを行うプロトコル
PKI	Public Key Infrastructure、公開鍵認証基盤と呼ばれ、公開鍵とその公開鍵の所有者の対応関係を保証する仕組みを提供
PRINS	Protocol for N32 Interconnect Security、2 つの SEPP 間の相互接続上の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、専用トラフィックのサービス品質を実現するための、トラフィックの優先順位付けとリソース予約。
RRC	Radio Resource Control protocol、レイヤ 3 で機能し、UE と無線局間での通信の制御を行うために使用
(R)RU	(Remote) Radio Unit 、 分散型 RAN 展開において、DU および CU から切り離された無線トランシーバーエレメント。
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 参照）。
SCP	Service Communication Proxy、5G コアネットワーク内のネットワーク機能を接続する接続性ファブリック（メッシュネットワークで一般的に実装されている）。
SDN	Software Defined Network、ネットワークプログラマビリティのための新しいアプローチ。オープンインタフェースを介してネットワークの動作を動的に初期化、制御、変更、管理する技術。
SEAF	Security Anchor Function、訪問したネットワークのルート鍵を格納する機能[24]で、高速な認証を可能にする。AMF とコロケーションすることができる。
SEPP	Security Edge Protection Proxy 、ネットワーク相互接続で実行される透過型セキュリティプロキシで、受信メッセージと送信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などの更なるセキュリティ機能を実行する。
SIDF	Subscriber Identity De-concealing Function、UE から送信された暗号化 SUCI を解読するネットワーク機能
SMF	Session Management Function、データ用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
SUCI	Subscription Permanent Identifier、プライバシーを強化するために UE と

	SIDF の間で暗号化された SUPI の保護された形態
SUPI	Subscription Permanent Identifier、グローバルにモバイルネットワークのユーザ/サブスクリプションを一意に識別するための識別子。IMSI (International Mobile Subscriber Identity) または NAI (Network Access Identifier) としてフォーマットすることができる。
TNGF	Trusted Non-3GPP Gateway Function、N2/N3 インタフェースを公開し、UE が非 3GPP アクセス技術（TNAP）を介して 5GC に接続できるようするための機能
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一つ。
UE	User Equipment、移動機器およびユニバーサル加入者 ID モジュールで構成される加入者の移動設備
UP	User Plane、モバイルネットワーク内でユーザデータを伝送するトラフィッククラス。
UPF	User Plane Function、パケットのルーティングや転送など、ユーザプレーンの操作を容易にするネットワーク機能
USIM	Universal Subscriber Identity Module、UE のホームネットワークオペレータ制御部分
VNF	Virtual Network Function、NFVI 上にデプロイ可能なネットワーク機能の実装

3 リファレンスモデルおよび脅威の分析

本章では、本文書による検討の基礎となる、5G システム、ネットワーク機能の仮想化、およびマルチアクセスエッジコンピューティングにおける参照モデルを紹介する。後の章で説明する脅威とセキュリティ管理策の導出における基本的な参照モデルとして利用される。また、本書では、汎用的な脅威モデルとしてよく知られている STRIDE-LM モデルに基づいて 5G システムおよびそのエコシステムに対する脅威を特定して対策要件を策定していることから、STRIDE-LM モデルについて紹介する。

3.1 節では、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し、5G システムの高レベルの信頼性とリスクの考慮事項を紹介している。**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を概説する。**3.3 節**では、主要な MEC の構成要素と、このアーキテクチャ特有のセキュリティ上の考慮事項を提供する。**3.4 節**では、STRIDE-LM の脅威モデリング技術を紹介する。**3.5 節**では、本書の作成時に考慮された脅威の主体をリストアップしている。

3.1 5G システム

3.1.1 ネットワークエンティティ

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**： モバイル機器（ME）および汎用加入者識別モジュール（USIM）で構成される。
- **Radio Access Network**： 複数の gNB で構成される。
- **Core Network**： 認証・認可、加入者のモビリティ、外部ネットワークへのデータ転送、レーティング、課金を含むモバイルネットワークの主要な機能で構成される。

本書では、上記の **Radio Access Network**（RAN；無線アクセスネットワーク）と **Core Network**（CN；コアネットワーク）に焦点を当てる。5G 仕様では、無線アクセスネットワークが分散配置される可能性があることから、gNB コンポーネントはさらに以下のサブコンポーネントに分解される。

- **Radio Unit**、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**、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。
- **Centralized Unit**、RRC や PDCP など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、API による通信を利用しており、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 IP ネットワークに

公開することで、柔軟性、拡張性、拡張性を実現している。本書では、5G スタンドアロン（5GSA）展開の以下のネットワーク機能に焦点を当てる。

- **UPF**：UE 間のユーザプレーントラフィックを外部データネットワークに転送する
- **AMF**：UE と AUSF 間の認証を仲介し、モビリティを管理する
- **SEAF**：サービングネットワークのルートキーを保持するセキュリティアンカー
- **SMF**：加入者のエンドツーエンド PDU セッションの管理
- **AUSF**：UDM に格納されたデータに対して加入者認証を実施
- **SIDF**：暗号化された SUCI を復号化する。一般的には AUSF と併設
- **ARPF**： 5G 認証ベクタの生成と通信を担当する UDM コンポーネント
- **UDM**：ホームネットワークに加入者情報を保存、恒久的なセキュリティ・クレデンシャルを含む
- **NRF**：利用可能なネットワークサービス、ネットワーク機能とそのプロファイルに関する情報を保存
- **PCF**：ネットワークスライスへの加入者アクセス、サービス、QoS、データ利用などの側面を制御するサービスおよびセキュリティポリシーの実施
- **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などの更なるセキュリティ機能を実行する
- **NEF：**サードパーティネットワークへの制御されたネットワークサービスの露出を可能にする
- **AF**：3GPP のコア仕様の外で補助的なサービスを行う汎用ネットワーク機能。
- **SCP**：コアネットワーク内の制御プレーン NF への接続性を提供

上述したネットワーク機能と、3GPP 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を図 1 に示す。

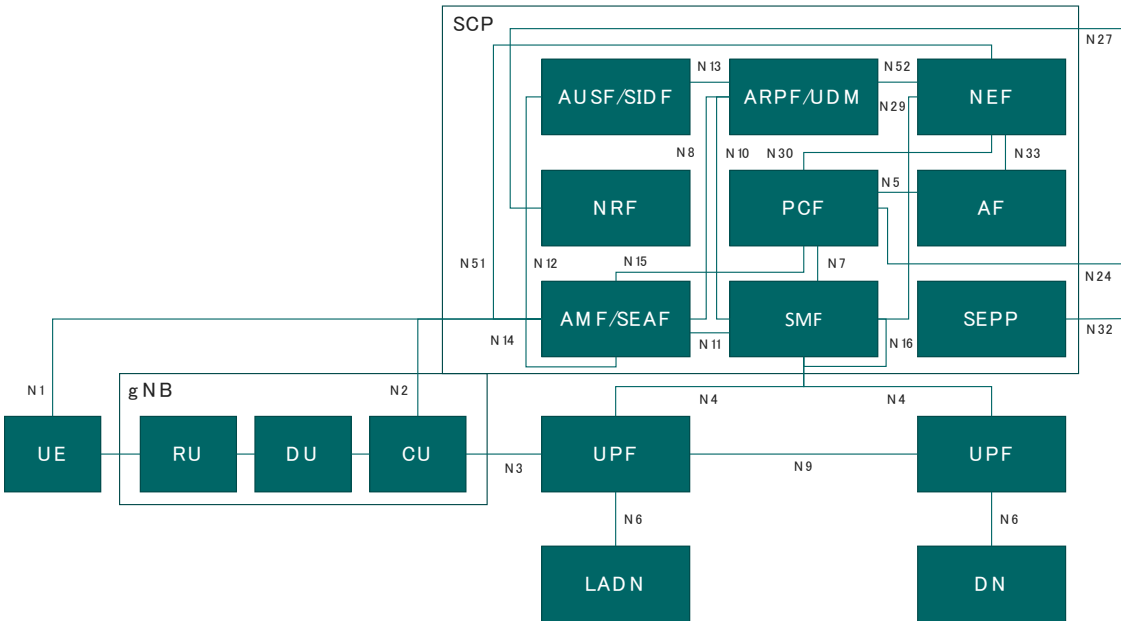

図 1 ネットワーク機能を示す簡略化された 5G システム[01]

3.1.2 信頼に関する考察

複雑なシステムにおけるセキュリティの基本的な検討事項は、信頼の問題、その確立、および個々のシステムコンポーネント間の信頼関係である。サービス層では、図 2 に示すように、5G システムは、一方の側に 5G UE（ME と USIM で構成)、もう一方の側に 5G ネットワーク（特に ARPF/UDM）という形で、2 つの本質的な信頼アンカーを含んでいる。USIM と UDM は共に、5G 認証フレームワークを使用してネットワークと加入者間の信頼関係を確立するための基礎となる加入者のパーマネント識別子とパーマネント鍵を保持している。

同様に、個々のネットワーク機能間、およびネットワーク機能ソフトウェアとコンピュートインフラストラクチャ間のネットワーク内での信頼性も保証される必要がある。5G によって促進される高度な機能分散と分散型のデプロイモデルにより、これらのセキュリティ対策はより重要なものとなる。例えば、コアネットワークの中央機能よりも信頼性が低いと考えられるネットワークエッジ上のネットワーク機能は、2 つのドメイン間の強力な相互認証だけでなく、信頼境界でのセキュリティポリシーの実施も必要となる。無線アクセスネットワークコンポーネントの展開モデル（たとえば、特殊なハードウェアに緊密に結合された従来の RAN、または集約されていない SDN ベースの RAN)、および関連するセキュリティ対策に応じて、この境界は下の図 2 に示すように、分散ユニットと集中ユニットの間に配置される場合と配置されない場合がある。

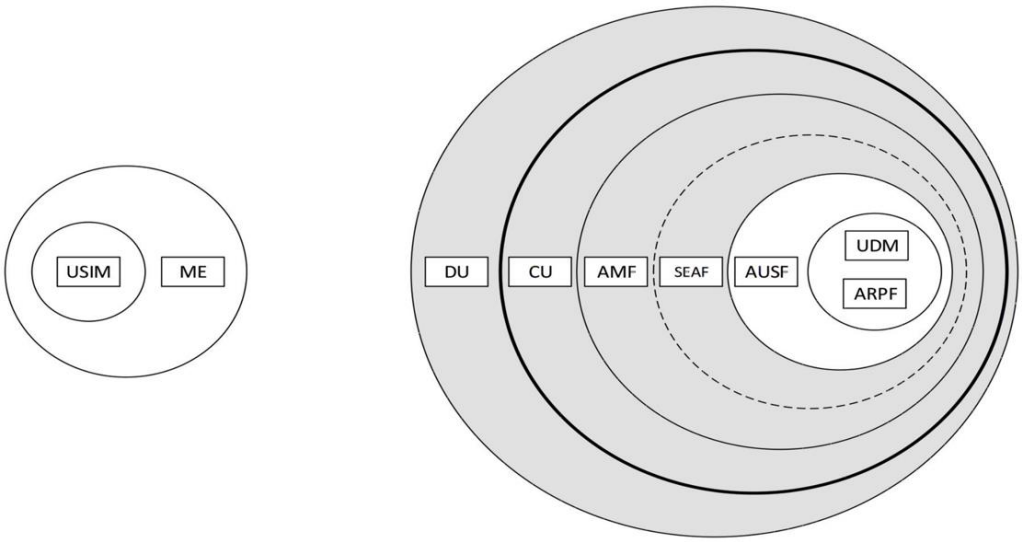

図 2 ： 5G 非ローミングシナリオの信頼モデル[24]

3.1.3 リスク･エクスポージャー

図 1 に示されるハイレベルの 5G アーキテクチャは、具体的な展開モデルとは独立した、個々のネットワーク機能のセキュリティリスク評価の基礎となる。以下の表 1 は、特にリスクの高いコンポーネントを強調して、潜在的な影響とリスク・エクスポージャーの推定値を示している。

推定数とは、商用展開で一般的に見られる 1 つのタイプの NF の数を意味する。**機密データの取扱い**とは、特定の NF タイプが、加入者またはネットワーク自体に関連する保護が必要なデータを処理するか否か、つまり保存または送信するか否かを示している。**データ流出の影響**および**利用不能の影響の**列は、ネットワーク機能インスタンスごとのセキュリティインシデントの深刻度を示す。**リスク・エクスポージャー**は、悪意のある行為者に対する各 NF タイプにおける露見の度合いを示す。

表 1 ： 5G ネットワーク機能のリスク･エクスポージャーとインシデント影響の推定値

		推定数	機密データの取扱い	データ流出の影響	利用不可の影響	リスクのエクスポージャー
5G NR	gNB	大（数万～数十万）	有り	小	小	高
	UPF	中（数百～数千）	有り	中	中	高
	AMF/SEAF	小（数十～数百）	有り	大	大	高
	SMF	小（数百）	有り	小	大	低
	AUSF/SIDF	小（数十まで）	有り	大	大	低
	ARPF/UDM	小（数十まで）	有り	大	大	低
5G Core	NRF	小（数十まで）	有り	大	大	中
	PCF	小（数十まで）	有り	大	大	低
	SEPP	小（数十まで）	有り	小	大	高
	NEF	小（数十まで）	有り	大	大	高
	AF	中（数百～数千）	潜在的に	中	中	中
	SCP	小（数十まで）	有り	大	大	中

なお、上記の表において色がついている 5 G ネットワーク機能においては、リスクのエクスポージャーの度合いが高く、インシデントの影響も大きいため、注意が必要である。

3.2 ネットワーク機能の仮想化（NFV）

ネットワーク機能仮想化（NFV）は、仮想化とソフトウェア定義ネットワーキングをベースにした通信ネットワークを展開するための概念的なアーキテクチャである。ネットワーク要素は、モノリシックなアプライアンスの代わりに、計算、ストレージ、ネットワークなど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。

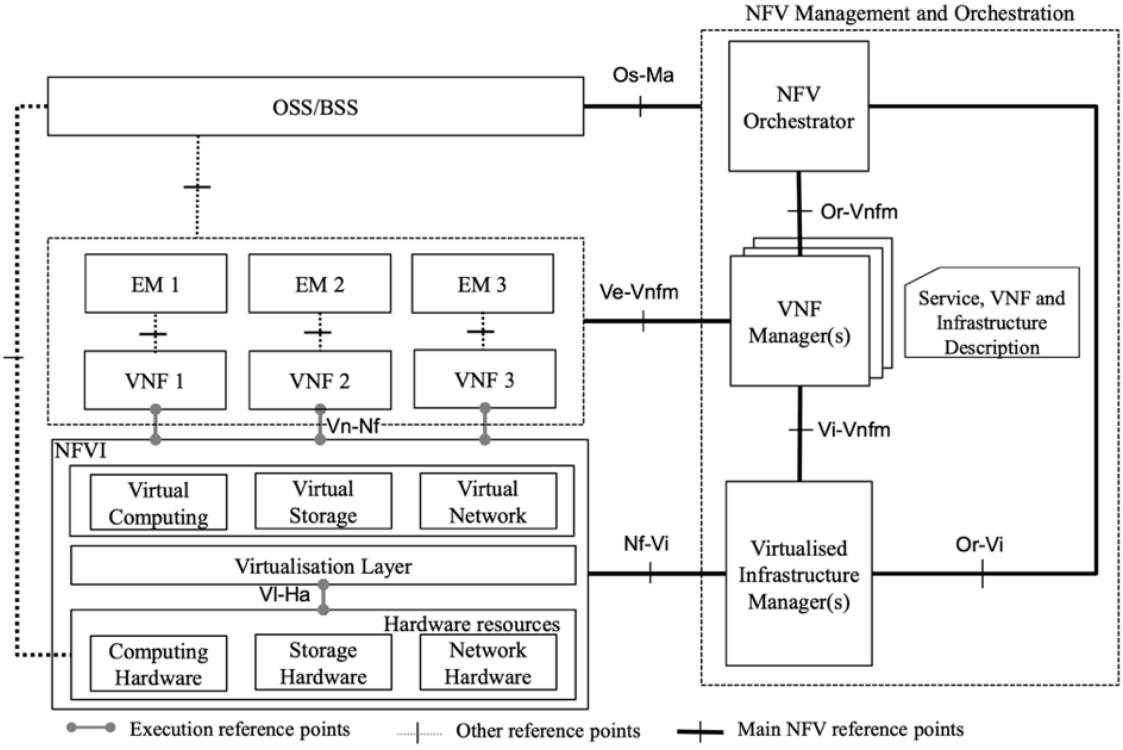

図 3：ネットワーク機能仮想化リファレンスモデル[08]

5G の導入では、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。一方では、共通のテクノロジー・スタックとそれに伴う管理の合理化により、セキュリティ強化レベル、構成とパッチ管理、ネットワーク全体の運用の可視性が大幅に向上する。逆に、仮想化レイヤは、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を必要とする別のレベルの複雑さを導入することになる。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）オペレータが別個の組織である場合に特に重要である。

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

- モバイルネットワークオペレータは、NFVI と同様に仮想ワークロードを制御し、管理およびオーケストレーション（MANO）を含む。
- モバイル ネットワーク オペレータは仮想ワークロードを制御するが、NFVI と MANO のプロビジョニングと管理はサードパーティに依存している。

後者のシナリオは、マルチアクセス・エッジ・コンピューティングなど、分散型の小規模なデプロイメントに最も適していると考えられる。

3.3 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（MEC）は、モバイル・エッジ・コンピューティングとも呼ばれ、エンドユーザに地理的に近い場所でクラウドコンピューティング機能を提供することで、高スループットかつ超低遅延のアプリケーションを実現することを目的としたアーキテクチャ概念である。このように、MEC は NFV と密接に結びついており、図 4 に示されるように、NFV と大きく重なるリファレンスモデルにも反映されている。

NFV の展開全般に適用される考慮事項は別として、MEC サービスと展開モデルは、以下に示すようなセキュリティに関連するいくつかの特徴を示している：

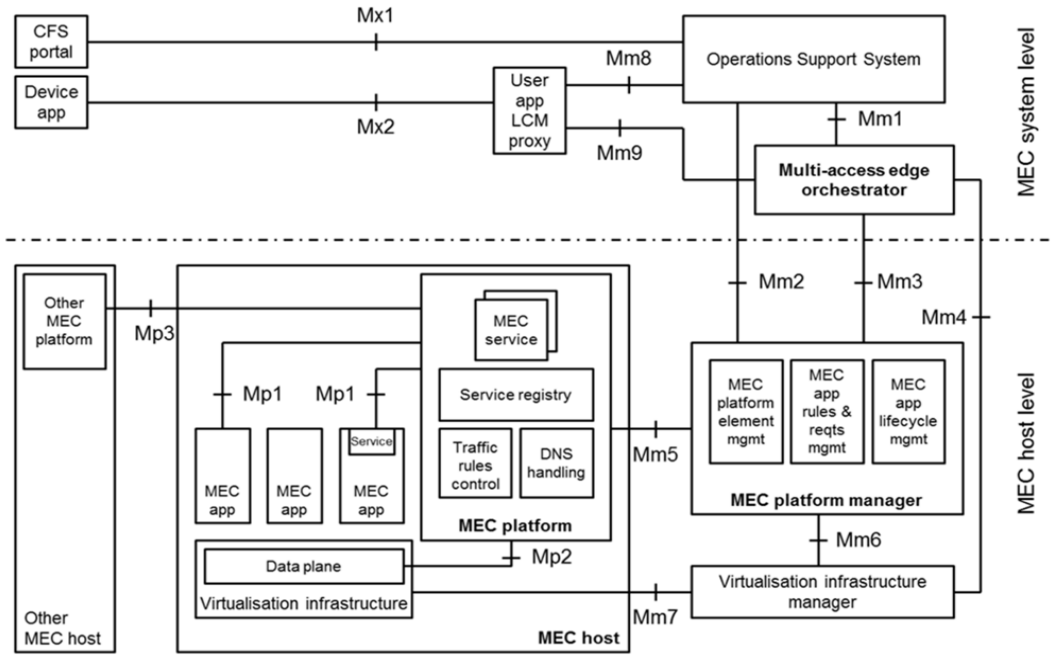

図 4: マルチアクセスエッジコンピューティング参照モデル[07]

- MEC プラットフォーム上で動作するサード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サードパーティのアプリケーション機能(AF)を伴うことがある。この機能は、加入者に対する意図的または意図しないサービス拒否(DoS)への扉を開く。
- 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（大幅に）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。
- エッジデプロイメントの物理的なセキュリティ制御が限られている場合、中央の 5G コアネットワーク機能よりも弱いレベルの保護を提供する可能性が高く、MEC プラットフォームはローカル攻撃の影響を受けやすくなる。

3.4 脅威の分析

5G システムの脅威モデリングに使用される STRIDE-LM モデルについて簡単に説明する。本書の作成時に考慮された脅威の主体をリストアップする。

3.4.1 構造化された脅威モデリングの必要性

5G ネットワークは、複数の同時実行コンポーネントで構成されており、相互に、また多数の外部エンティティと継続的に相互作用する。このような複雑なシステムを安全に設計するためには、構造化された方法論を使用することが鍵となる。脅威モデリングは、潜在的な脅威と脆弱性を特定し、適切な緩和策を開発するための体系的なアプローチを提供する。

3GPP によって定義された 5G 仕様は、技術的なセキュリティ管理のセットを文書化しているが、これは基本的な安全策を構成しているにすぎず、網羅的なものではないことに注意が必要である。実際の 5G ネットワークの展開、設定、運用には、それぞれのセキュリティ課題が存在し、慎重に検討する必要がある。特に、仕様と実際の運用との間のギャップを埋めるために、次の脅威モデリングの活用が試みられている。

3.4.2 STRIDE-LM モデル

本書では、STRIDE-LM モデルを用いて、5G システムに対する脅威を分類・記述している。このアプローチは、一般的な STRIDE モデルをベースに、以下表 2 の脅威を考慮している。

表 2 ： STRIDE-LM の脅威と関連するセキュリティ目標

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	認可
ラテラルムーブメント	ネットワークの分離

一般的な STRIDE の側面に加えて、悪意のある行為者がすでにシステムの一部を侵害している状況での攻撃の拡大に起因する脅威も含まれる。5G システムの複雑さと複数の面での露出の増加を考えると、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は、安定した信頼性の高い展開を確実にするために非常に重要である。

3.5 脅威アクター

どのような攻撃者からシステムを守るべきかによって、攻撃のベクトル、能力、リソースは大きく異なる。本書では、以下のようなタイプの脅威アクターが存在することを想定している。

- **内部攻撃者**：個人的な動機で、または第三者の代理人として、意図的にネットワークに危害を加える現在の従業員または元従業員。
- **ビジネスパートナー**：ハードウェアまたはソフトウェアのコンポーネントを供給している現在または過去のビジネスパートナーで、供給された製品を介して、またはそれらに暴露された情報を悪用することで、システムに悪影響を与えようとする。
- **好奇心旺盛な人たち**：明らかな欠陥や事前にパッケージ化されたセキュリティ上の欠点を使ってシステムを悪用しようとする、熟練していない個人。
- **プロのハッカー**：標的型攻撃を実行することができる熟練した個人であり、一旦侵入に成功すると、ツールを駆使し、システムへのアクセス可能範囲を拡大する。
- **組織的犯罪**：ネットワークとそのサービスを利用して、個人的な（多くの場合、金銭的な）利益を得るために協調した計画を実行している人々のグループ。
- **国家アクター**：膨大なリソース、ゼロデイエクスプロイトへのアクセス、高度な永続的な脅威ツールを持つ情報機関に支えられた攻撃者。

なお、自然災害や環境災害などのセキュリティ上の問題については、意図せずに発生した原因や関連する管理は本文書の対象外とする。

4 セキュリティ対策（管理策）

本章では、5G ネットワークの開発、統合、運用に関連する推奨セキュリティ対策（管理策）について説明する。セキュリティ対策は、前章で概説した特定の脅威に対応しており、該当する場合には、それらの脅威（攻撃など）を想定した対策となっている。

4.1 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。**4.2 節**では、主に組織の人員に関係する対策について詳述する。**4.3 節**では、安全な運用と維持管理のための対策を概説する。**4.4 節**では、物理的セキュリティの基本的な安全対策を指摘する。**4.5 節**では、技術的な対策として、一般的なものと特定のシステムドメインに特有のものを述べる。

4.1 組織のための管理策

4.1.1 セキュリティ組織

制御タイプ	予防的
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、認可、セグメンテーションと分離
セキュリティの概念	識別、保護

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 サービスプロバイダは、情報セキュリティを確保するための組織を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
- 上記ポリシーや手順などのルールの全社的な遵守の徹底
- セキュリティコンセプトや対策のフレームワーク作成
- ハードウェア・ソフトウェア技術部品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）
- 脅威管理とインシデント対応

ビジネス全体にとっての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：-

4.1.2 5G セキュリティポリシー

制御タイプ	予防的
関連するセキュリティ目的	認証、認可、完全性、機密性
セキュリティの概念	識別

管理策： 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て、5G ネットワークのセキュリティを確保するための方向性を示すことが望ましい。

ガイダンス： 5G サービスプロバイダは、ネットワーク、そのユーザ、およ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 5G セキュリティポリシー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および規制
- 組織独自の企業ルールおよび規制
- 内外利害関係者の利益
- 会社全体としてのリスクおよび 5G サービスの対象

ポリシーの内容は、5G のセキュリティを管理可能なものにするなど、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領域
- 5G に関連したセキュリティ目標
- 5G サービスの提供における役割と責任
- コミュニケーション＆レポーティング体制

ポリシーは一元的に利用可能であり、各従業員に周知されることが望ましい。例えば、5G システム内のデータ分類や暗号化ガイドラインなど、より頻繁に変更が予想されるセキュリティ案件に対応するために、個別のポリシーを策定することも一案である。

参考文献：-

4.2 人的管理策

4.2.1 ポジティブなセキュリティ文化

制御タイプ	予防的
関連するセキュリティ目的	認証、機密性、完全性
セキュリティの概念	識別、保護

管理策：セキュリティは組織にとって阻害要因ではなく、ビジネス推進において重要であるとの認識に基づき、日々の業務にセキュリティをシームレスに統合するための企業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や優先順位に柔軟に対応するために、セキュリティは組織の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。
セキュリティを前向きにとらえる組織文化を醸成する取り組みには、以下のようなものがある。

- 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意識を高め、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。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ため。
- 良い行動の認識や報酬化：ポジティブな動機づけは、不正行為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ある。
- 学習の奨励：従業員はセキュリティを恐れず、その逆に学習を奨励し、日々の仕事の中で自信を持ってセキュリティを扱うようにすることが望ましい。

参考文献：-

4.2.2 セキュリティ教育と意識向上

制御タイプ	予防的
関連するセキュリティ目的	認証、認可、機密性
セキュリティの概念	識別、保護、検出

管理策：従業員が 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ようにすることが望ましい。

ガイダンス：
組織は、セキュリティの目的、問題点、および潜在的な脅威（攻撃）に対する意識を高め、管理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に関する教育・意識向上を醸成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（概念や手法等）がいくつか導入されているため、セキュリティの教育、啓蒙については、技術供給者やサービス事業者にとって重要となる。新しい技術的・運用的な側面の例としては以下がある。

- 無線アクセスネットワークの一部を含むクラウドネイティブな展開
- ウェブ技術と API ドリブンコミュニケーション
- サード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

どのような意識向上・教育のための活動を行えばよいかという観点では、以下の点を考慮して設計することが望ましい：

- リスクとセキュリティの根拠の説明：根底にある動機と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。
- 従業員の日常業務との関連性の定義：活動で得た情報を自分の日常業務における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インパクトは大きくなる。
- 定期的なリフレッシュと繰り返し：攻撃者の戦略やセキュリティ対策（管理策）は常に変化する。セキュリティトレーニングの内容は、この変化を反映させ、定期的に組織に伝えていくことが望ましい。

参考文献：[15]

4.2.3 セキュリティインシデントの報告

制御タイプ	探知
関連するセキュリティ目的	機密性、完全性、可用性
セキュリティの概念	検出

管理策：従業員がセキュリティ上の不備やインシデントを一元的な窓口に報告するためのプロセスを確立し、推進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、既存の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、各従業員が従うべき明確なインシデント報告プロセスを用意して、対応を開始すべき責任のある部署に迅速に通知することが重要となる。セキュリティインシデント報告プロセスを確立するためには、以下の点を考慮することが望ましい：

- 可視性と使いやすさの確保：各従業員は、報告とインシデント報告のための指定された方法を理解している必要がある。迅速な行動を促すために、できる限り簡易に実施することが望ましい。
- 説明責任の奨励: 誰もが、影響を受ける可能性があるからといって、インシデントレポートを作成しようとすることを恐れるべきでは無い。脅迫や隠ぺいは、隠れたセキュリティ問題の温床となる。

参考文献：-

4.2.4 契約におけるセキュリティの枠組み

制御タイプ	予防・是正
関連するセキュリティ目的	守秘義務
セキュリティの概念	保護

管理策：従業員、請負業者、その他のビジネスパートナーと情報を安全に共有するために必要な法的保護措置を提供することが望ましい。

ガイダンス：機密情報やその他機微な情報を外部に公開することは、時には避けられない。特定の 5G のユースケースでは、ネットワーク機能の公開に重点が置かれ、リソースのプールと共有の強化が必要となる可能性が高いため、5G サービスプロバイダは、これまで以上に多様なパートナーとのインタフェースをとることになると考えてよい。したがって、必要な場合にはいつでも、交換された情報を慎重に取り扱うことを両当事者に義務付ける法的強制力のある方法で行うことが重要となる。このような措置の例としては、以下のようなものがある：

- 組織と自社の従業員との間の秘密保持条項
- 組織と外部のビジネスパートナーとの間の秘密保持契約

参考文献：-

4.3 運用の管理策

4.3.1 セキュアなソフトウェア開発

制御タイプ	予防的
関連するセキュリティ目的	認証、認可、機密性、完全性
セキュリティの概念	保護

管理策：関連するすべての資産と情報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：実稼働での使用を目的としたソフトウェアの開発プロセスでは、安全で信頼性の高いシステム構築を促進することが望ましい。そのためには、セキュリティ要件を最初から考慮し、適切な優先度を割り当てる必要がある。開発者は、以下のような安全なソフトウェア開発の原則に精通していることが望ましい。

- アタックサーフェスの最小化
- 適切な認証
- 入力の検証
- 機密データの暗号化
- デフォルトのセキュリティ確保：システムユーザに明示的にセキュリティを有効にすることを強制しないようにする。その代わりに、必要に応じて特定のセキュリティ機能をオプトアウトするオプションを与える。
- 説明責任：以下により慎重に資産や情報へのアクセスを行うこと。
  - ・最小特権の使用の義務化
  - ・職務分掌の確保
  - ・監査証跡の整備と保護
- 透明性：以下による情報セキュリティ問題における責任の実践
  - ・隠すことによるセキュリティへの非依存
  - ・脆弱性の開示
  - ・違反行為の開示

近年多く活用されている開発アプローチの *DevSecOps* は、（操作に適したコードを設計することに加えて）開発者の中心的な責任とすることで、セキュリティをより重視している。さらに、開発と統合のプロセス全体を通して必須のセキュリティ機能（例えば、静的コード分析、手動コードレビュー、脆弱性スキャン）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。

参考文献：-

4.3.2 セキュアシステム工学

制御タイプ	予防的
関連するセキュリティ目的	可用性、セグメンテーションと分離
セキュリティの概念	保護

管理策：組織のエンジニアリングプロセスにおいて、安全なシステム開発の原則が組み込まれていることを確実にすることが望ましい。

ガイダンス：ソフトウェア開発と同様に、システム設計と統合は、5G サービスの安全性を確保する上で重要な役割を果たしている。5G システムサプライヤと 5G サービスプロバイダにおけるエンジニアリング・チームは、以下のような安全なシステム開発の原則に精通することが望ましい。:

- 設計におけるセキュリティ：設計プロセスの初期段階から、セキュリティリスクとその対策を考慮に入れる。
- 防御の深層化：多層の防御モデルを適用して、単一の障害点を回避することで、セキュリティ管理の冗長性を確保する。
- 回復力：以下を実施することにより、システムがセキュリティインシデントへ対応したり、セキュリティインシデントから回復したりする能力を確保する。
  ・冗長性と高可用性
  ・耐障害性とフェールセーフ
  ・バックアップとリカバリー

参考文献：-

4.3.3 セキュリティ保証

制御タイプ	予防・是正
関連するセキュリティ目的	認証、認可、機密性、完全性、可用性、セグメンテーションと分離
セキュリティの概念	識別、保護

管理策: ハードウェアおよびソフトウェアにより構成されるシステムコンポーネントの継続的なセキュリティ評価と、それに続く特定された弱点の軽減のための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 技術サプライヤや 5G サービスプロバイダは、5G システムとその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、期待されるセキュリティ要件を満たしていることを確認する必要がある。

- セキュリティの強化：以下によりシステムとそのサービスの安全な構成を強化する。
  - ・不要なインタフェースとポートの不使用化
  - ・不要な機能やコンポーネントの無効化や削除
  - ・不要なアカウントや資格情報の削除
- 脆弱性管理：システムの弱点を特定し、以下の方法で軽減する。
  - ・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
  - ・適切な改善策の初期化
- ペネトレーションテスト：既存の弱点を悪用し、複雑な攻撃チェーンを再構築するような実際の攻撃者の行動を把握するための、詳細で手動によるセキュリティ監査
- バックドアの発見：サードパーティの技術コンポーネントに内在する意図的なセキュリティ上の弱点を検出すること。例えば以下が有効となる。
  - ・ソースコードが利用可能な場合は、静的コード解析
  - ・実行パスと状態遷移の解析
  - ・バイナリサンドボックス化の活用

セキュリティ保証のための活動は定期的に実施されるべきである。その優先順位は、リスクアセスメントの結果に基づいて決定されることが望ましい。

参考文献：-

4.3.4 インベントリと構成管理

制御タイプ	予防的
関連するセキュリティ目的	完全性、可用性
セキュリティの概念	識別

管理策：5G エコシステム全体のハードウェアおよびソフトウェアにより構成されるシステム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：5G サービスプロバイダは、すべてのハードウェアおよびソフトウェアにより構成されるシステム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（サードパーティのクラウドプロバイダ上で動作するソフトウェアなど）が含まれる。記録すべき関連情報としては、以下のものが含まれる：

- 固有のシステム識別子
- システムタイプ
- IP アドレス（またはその他のネットワークアドレス）
- 処理されたデータとその保護要件
- 責任ある組織・管理者
- 組織内の連絡先

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・管理できる構成データベースを保有することが望ましい。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実装してもよいし、インベントリと定期的に同期される別個のエンティティとして実装してもよい。構成データベースに一般的に記録される情報には、以下のようなものがある：

- 固有のシステム識別子
- IP アドレス（またはその他のネットワークアドレス）
- インストールされているオペレーティングシステムとアプリケーション（パッチレベルを含む）
- 既存のライセンスと必要なライセンス
- 外部とのコミュニケーション関係
- 他のシステムへの依存性
- システムサプライヤ/開発者の情報（連絡先を含む）

システムインベントリおよ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も実施できる。記録されたデータの正確性を確保するために、関連する日付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およ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：-

4.3.5 変更管理

制御タイプ	予防的
関連するセキュリティ目的	完全性
セキュリティの概念	保護

管理策：5G ネットワーク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 サービスプロバイダは、5G エコシステムへの変更に明確な責任者があり、変更が計画され、レビューされ、セキュリティ組織を含む関連する利害関係者によって承認されることを保証するために、厳格な変更管理を確立することが望ましい。実行されたすべての変更の記録は、適切な時期に渡って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。

- 最上級のセキュリティ構成の定義：堅牢な構成は、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 (4.1.1 項参照) により提供されること。
- 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を割り当てること。
- リモート認証の利用：システムのリモート認証機能を使用して、セキュリティ関連の構成パラメータを定期的に検証すること。

参考文献：-

4.3.6 セキュリティ監視

制御タイプ	探知
関連するセキュリティ目的	認証、機密性、完全性、可用性
セキュリティの概念	保護

管理策：5G ネットワーク全体のセキュリティ関連イベントの可視体制を確立し、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：運用セキュリティは、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、すべてのシステムコンポーネントのセキュリティ関連情報を記録、収集、分析することが望ましい。モバイルネットワークの場合、以下の活動が含まれる。

- システムログとアラームの収集の一元的な実施
- 異なるソースからのデータ間の相関分析（内部および外部の両方、例：脅威インテリジェンス・フィード）
- 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
- 対応が必要なイベントのインシデント管理ツールへの記録
- システムのログや警報の適切な期間に渉る保持（法令や社内規定に基づく）

参考文献：-

4.3.7 パッチ管理

制御タイプ	予防的
関連するセキュリティ目的	認証、認可、可用性
セキュリティの概念	保護

管理策：5G システムの本番環境を構成する製品群への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し、実施することが望ましい。

ガイダンス：ソフトウェアは、必然的にエラーがないわけではなく、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。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、進行中の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完全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。

- 特定された脆弱性や新たにリリースされたパッチに関するサプライヤ/開発者の発表をフォローする。
- 外部の脅威情報源を活用する。
- 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り、可能な限り早期にパッチを実装する。
- 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、4.3.5 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：-

4.3.8 バックアップとリカバリーの手順

制御タイプ	予防的、是正
関連するセキュリティ目的	可用性
セキュリティの概念	リカバリー

管理策：5G システムコンポーネント（すべてのデータ、メタデータ、構成を含む）の現在の状態を定期的に把握し、必要に応じて以前の状態に効率的に復元できるようなプロセスと手順を構築し、実施する。

ガイダンス：5G ネットワークのような複雑なシステムの運用中には、情報セキュリティインシデント、自然災害、またはそれに類する事象によって、以前のシステム状態に復元しなければならない様々な状況が存在する可能性がある。これらに備えて、5G サービスプロバイダは、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とそのための技術的な対策を実装する必要がある。バックアップを作成した後は、以下のような対策を実施して、保存されているデータを保護する。

- バックアップコピーを冗長化して物理的な分離保管
- 保存されたバックアップへのアクセス許可者の制限
- 保存されたバックアップの機密性と完全性の確保
- 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：-

4.4 物理的な管理策

4.4.1 安全な施設設計

制御タイプ	予防的
関連するセキュリティ目的	可用性、認証
セキュリティの概念	保護

管理策：処理されたデータや各種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 システムの構成要素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その建設は、収容されたシステムを物理的な危害から保護するために実施することが望ましい。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コンセプトとしては、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：-

4.4.2 物理的アクセスの制限

制御タイプ	予防的
関連するセキュリティ目的	認証、認可
セキュリティの概念	保護

管理策：必要な場合にのみ、権限を与えられた人員に 5G システムのコンポーネントへの物理的なアクセス権を提供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、権限を与えられた担当者にのみ許可される。このためには、これらの権限を与えられた担当者を一意に認証する必要がある。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ことが望ましい。

- 施設への物理的アクセスの許可は、個人の立場や役割に応じて行うこと。
- 本人は、組織の規定に基づき、多要素認証にて本人確認を行うこと。
- 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。

一度許可が与えられると、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。発行されたすべてのクレデンシャルの正確性を確保するために、認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、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：-

4.4.3 物理アクセスの監視

制御タイプ	探知
関連するセキュリティ目的	認証、認可
セキュリティの概念	検出

管理策：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維持することが望ましい。

ガイダンス：5G サービスプロバイダは、許可された人員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。このためには、以下を実施することが望ましい。

- 身元や根拠、訪問時間など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、記録の適切な期間に渡る保存

参考文献：-

4.4.4 情報フロー制限

制御タイプ	予防、探知
関連するセキュリティ目的	守秘義務
セキュリティの概念	保護、検出

管理策：5G システムコンポーネントを収容する施設への情報フローを制御し、制限することが望ましい。

ガイダンス：5G サービスプロバイダは、5G プラットフォームへの直接の物理的アクセスが、悪意のあるコンポーネントの混入や機密情報の窃取に悪用されないことを保証する必要がある。このためには、以下のような対策が考慮できる。

- 明示的な許可なく電子記憶媒体の持ち込み／持ち出しを制限すること
- 記録用機器（携帯電話、デジタルカメラなど）の施設内への持ち込みの禁止
- 位置情報技術を使用して、組織が定義した資産の位置と移動を監視すること

参考文献：[20]

4.5 技術的対策

4.5.1 共通の技術的対策

4.5.1.1 安全な暗号アルゴリズム

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性
セキュリティの概念	保護

管理策：安全な暗号アルゴリズムを使用して、転送中および保存中の情報を確実に保護することが望ましい。

ガイダンス：5G サービスプロバイダは、サービスと関連データを保護するために使用される、許容できる暗号化アルゴリズムの概説をポリシーとして定義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。

- 許可された暗号ハッシュアルゴリズム
- 許可された対称暗号およ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（楕円曲線暗号を採用する場合）
- 最小鍵長

特に 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提供することが望ましい。

- RRC と NAS の秘匿アルゴリズム
- RRC と NAS の整合性アルゴリズム
- PDCP 秘匿アルゴリズム
- PDCP 整合性アルゴリズム
- SUPI 秘匿アルゴリズム
- (D)TLS, IPsec, JOSE 暗号スイート（鍵交換などを含めた暗号関連情報）

参考文献：-

4.5.1.2 アイデンティティ管理および公開鍵インフラストラクチャ

制御タイプ	予防的
関連するセキュリティ目的	認証，認証
セキュリティの概念	識別

管理策：5G ネットワークおよび関連するクレデンシャルや許可の運用と維持に使用されるデジタル ID のために、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 サービスプロバイダは、すべてのシステムアカウントの識別子、クレデンシャル、役割、および識別子を処理する一元 ID 管理システムに、すべてのシステムユーザが登録されていることを確実に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（すなわち、役割、特権）のプロビジョニング、変更、およ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
- 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）
- 信頼された当事者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：-

4.5.1.3 安全な鍵管理

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性
セキュリティの概念	保護

目的:5G システムコンポーネントにおいてローカルに格納される暗号鍵を保護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、暗号のための秘密情報（鍵など）を保存する必要がある。したがって、5G 技術サプライヤおよび 5G サービスプロバイダは、次に示すような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では、安全な暗号化モジュールを利用すること。
- 暗号モジュールの内部にのみ鍵を格納し、モジュール内部で鍵を使用すること。
- 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できるようにすること。
- 機密性の高い鍵関連情報については、その寿命後に安全に廃棄すること。

参考文献：[21]

4.5.1.4 セキュアブート手順

制御タイプ	予防的
関連するセキュリティ目的	完全性
セキュリティの概念	保護

管理策：起動時におけるロー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、Hardware-Based Root of Trust などのようなシステム内にハードウェアベースの信頼のための根幹が存在することが必要となる(4.5.2.1 参照)。5G 技術サプライヤ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: 第 3 者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 (セキュアブートとしても知られる):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 サービスプロバイダは、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に取得された情報を考慮に入れるかのいずれかによって、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：-

4.5.1.5 ファイル完全性の監視

制御タイプ	予防的
関連するセキュリティ目的	完全性
セキュリティの概念	保護

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は、起動時にシステムの完全性を検証するために使用することができるが（4.5.1.4 参照）、運用中の意図しない変更を防ぐことはできない。この目的のため、5G 技術サプライヤは専用のソフトウェアを搭載することにより、システムの変更を継続的に監視し、監視結果を定義されたベースラインと比較することが望ましい。5G 技術サプライヤおよび、5G サービスプロバイダは、異なるシステムタイプごとにファイル完全性のためのベースライン・ポリシーを定義し、構成ファイルやアプリケーションデータなどのすべての関連データをカバーし、ファイル完全性監視ソリューションのアラートを監視し、違反行為にタイムリーに対応して、潜在的なインシデントを軽減することが望ましい。

参考文献：-

4.5.1.6 セキュアな管理通信

制御タイプ	予防的
関連するセキュリティ目的	完全性、機密性、認証
セキュリティの概念	保護

管理策：
通信ピア間の相互認証、および転送されたデータの機密性と完全性を提供する運用ツールとプロトコルの使用を確実なものと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、監視データなど、5G 導入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 サービスプロバイダは、以下の具体的なセキュリティ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（4.5.1 項参照）に従って、管理プロトコルが安全な暗号アルゴリズムを利用することを保証すること。
- 常に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（4.5.1.2 参照）。
- 安全でないレガシー管理プロトコル（Telnet、ファイル転送プロトコル、シンプルネットワーク管理プロトコルバージョン 2 など）の使用を禁止すること。

参考文献：-

4.5.1.7 安全なログファイルの収集と保存

制御タイプ	予防的
関連するセキュリティ目的	完全性、機密性
セキュリティの概念	保護

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

ガイダンス：5G サービスプロバイダは、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 5G システム全体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なものにすることが望ましい。
そのためには、以下のような対策を講じることが推奨される。

- すべてのログ生成モジュールを共通の時間ソースで同期させること。
- すべての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。
- 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の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の保護を提供するプロトコルを介してログファイルの送信を確実にすること。
- 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。

上記の推奨事項を専用のロギングのための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、およ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管理策をポリシーに記載することが推奨される。

参考文献：[22]

4.5.1.8 セキュアな API 設計

制御タイプ	予防的
関連するセキュリティ目的	機密保持、認可
セキュリティの概念	保護

管理策：可能な限り回復力を持たせ、必要最低限の情報公開を実施するために、セキュリティを考慮したサービス API を設計することが望ましい。

ガイダンス：API 駆動型通信が 5G コアネットワーク機能でより広く採用されるようになると、5G 技術サプライヤや 5G サービスプロバイダは、セキュリティインシデントを防止するために、これらのインタフェースに基本的なセキュリティ対策を最初から適用することが望ましい。これには、以下のような具体的な管理策が含まれる。

- 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すること。
- 使用量のクォータを適用し、クォータを超えるクライアントを一時的にブロックまたは抑制すること。
- API の仕様に対する受信リクエストのコンプライアンスを検証すること。

参考文献：[23]

4.5.1.9 API アクセス制御

制御タイプ	予防的
関連するセキュリティ目的	認証、認可
セキュリティの概念	保護

管理策：API エンドポイントが通信相手同士を適切に認証・認可することが望ましい。

ガイダンス：5G 技術サプライヤおよび 5G サービスプロバイダは、外部に公開されているすべての API エンドポイントにおいて、要求元に対する認証と認可を厳格に実施することを確実にすることが望ましい。3GPP セキュリティ仕様に従って、許容可能な認証方法は以下のとおり。

- TLS を用いたトランスポート層での認証
- NDS/IP による暗黙の認証

3GPP 仕様に反して、物理セキュリティによる暗黙の認証は、多層防御のセキュリティ原則に違反するため、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。3GPP セキュリティ仕様に従って、ローカル NF ポリシーまたは JSON Web Tokens (JWT) のいずれかに基づいて認証を行うことができる。機密データを扱う API では、常にトークンベースの認証を利用することが推奨される。このようなトークンの実装および設定においては、以下の注意事項を遵守することが望ましい。

- すべてのトークンには、有効期限が設定されていること。
- すべてのトークンは、定義されたスコープを持つこと。
- 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。

参考文献： [02], [03]

4.5.2 仮想化における対策

4.5.2.1 ハードウェアベースの信頼の基点

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性
セキュリティの概念	保護

管理策: ホストシステムと仮想ワークロードの双方で実行されるセキュリティ運用において信頼できる基盤を確保することが望ましい。

ガイダンス: 5G サービスプロバイダは、セキュリティ運用がハードウェアベースの信頼の基点(HBRT)に根ざしているか、またはそれにより直接実行されているかを確認することが望ましい。したがって、すべての NFVI ホストは、セキュアエレメント（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機能（TPM：生成した暗号化鍵を保有するセキュリティデバイス等）を含むハードウェアセキュリティモジュールなど、何らかの形式の HBRT を実装することが望ましい。これらは、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。
- 信頼性の高い認証手順に基づいた、攻撃に対する耐性を検証すること。
- 暗号化およ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 とホストシステム間の通信に関しては、以下のセキュリティ対策を実施することが望ましい。

- 各 HBRT は、攻撃などの変化を検出するために、そのホストシステムに組み込まれていること。
- 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）は、改ざん、盗聴、リプレイ、または同様の攻撃から保護されていること。
- ホストは、その HBRT が改ざんされたかどうかを検出できる能力を持つこと。

参考文献： [10]

4.5.2.2 NFVI ホストの堅牢化

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性、可用性
セキュリティの概念	保護

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、強固なセキュリティベースラインに基づいて運用および管理されていることが望ましい。

ガイダンス:4.3.3 項に記載されている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対する対策が必要となる。ホストマシン自体を保護し、ワークロード間の分離を確実にするために、5G サービスプロバイダは、以下の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 など) を設定して、仮想ワークロードに機能制御ができるようにすること。
- 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と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：[10]

4.5.2.3 仮想化レイヤの堅牢化

制御タイプ	予防的
関連するセキュリティ目的	可用性、認可
セキュリティの概念	保護

管理策：仮想化レイヤで NFVI ホストおよび仮想ワークロードの保護を支援するための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運用者は、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排除技術を無効にするように設定されていること。

参考文献：[10],[17]

4.5.2.4 セキュアな VNF の設計と開発

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性、認証
セキュリティの概念	保護

管理策：取り扱う情報を保護し、5G システムを安全に運用できるように、VNF コンポーネントを設計・開発・パッケージ化することが望ましい。

ガイダンス：設計によるセキュリティの原則に従い、5G 技術サプライヤは、VNF の設計と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の採用を促進することが望ましい。理想的には、VNF 自体が、その管理下にある情報を保護するための対策を提供するだけでなく、5G サービスプロバイダが提供する主要なセキュリティ管理（アイデンティティ＆アクセス管理、ロギング、リモート認証など）との統合をサポートすることが望ましい。セキュアな VNF 開発のための推奨事項には、以下のようなものがある。

- VNF は、基盤となるプラットフォームのセキュリティ対策に依存するのではなく、すべてのデータとプロセスの機密性を保護するように設計されること。
- VNF は、仮想化ホストの HBRT の使用をサポートすること。
- VNF コンポーネントは一意の認証クレデンシャル情報を使用すること。
- VNF コンポーネントは、セキュリティ強化の対象とすること（4.3.3 項参照）。
- VNF は機密データ、メタデータ、プロセスを特定することができること。
- VNF は、定義されたトラストドメインに割り当てることができること。
- VNF イメージは暗号を用いた電子署名がなされていること。

参考文献：[09], [16]

4.5.2.5 MANO セキュリティ

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性、認証、セグメンテーションと分離
セキュリティの概念	保護

管理策：NFV 環境およ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 のコンポーネントは、NFV 導入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および保存する。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 に影響を及ぼす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、設計および実装の際に、以下のセキュリティ推奨事項が守られていることを確実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は、完全性保護と機密性保護を実施すること。
- NFV イメージライブラリは、保存された VNF イメージの不正な変更、削除、挿入を防止できること。

本番使用時には、仮想インフラストラクチャの運用者は、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。

- 複数の MANO トラストドメインの定義
- 異なる MANO トラストドメイン間の信託関係の定義
- 信頼関係が定義されていない MANO の信頼ドメインの間で、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：[11]

4.5.2.6 仮想ネットワークセキュリティ

制御タイプ	予防的
関連するセキュリティ目的	セグメンテーションと分離
セキュリティの概念	保護

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機能低下を招かないようにすることが望ましい。

ガイダンス：従来のワイヤレス環境では、セキュリティ対策の実装が物理的なアプライアンスの形でネットワーク内に配置されることが多く、トラフィックがアプライアンスを強制的に通過しなければならなかった。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により、これらの対策の実装箇所は目に見えにくくなるが、セキュリティ境界の希薄化をもたらしてはならない。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テーションを保証するために、5G サービスプロバイダは以下の推奨事項を遵守することが望ましい。

- 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と統合されたファイアウォールを使用すること。
- 標準的な管理プロトコルに基づく集中型またはフェデレート型の SDN コントローラを使用すること。
- 管理トラフィックのために専用の仮想スイッチと NIC を使用すること。
- 物理ネットワークへのオーバーレイベースのセグメンテーション（例：VLAN を利用したセグメンテーション）を実施すること。
- 可能であれば物理ネットワークでのネットワーク監視ツールを活用すること。

参考文献：[18]

4.5.3 無線アクセスネットワークにおける対策

4.5.3.1 ユーザプレーンの保護

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性
セキュリティの概念	保護

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

ガイダンス：5G サービスプロバイダは、無線アクセスを介して転送されるユーザプレーンのトラフィックに対して完全性保護策が適用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、意図しない変更を防止する必要がある。これには、以下の注意事項が含まれる。

- 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（4.5.1.1 参照）に従って、安全な暗号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。

参考文献：[03]

4.5.3.2 コントロールプレーンの保護

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性
セキュリティの概念	保護

管理策：ユーザ機器と 5G 基地局間および、ユーザ機器と AMF 間のコントロールプレーントラフィックの機密性と完全性を確保することが望ましい。

ガイダンス：5G サービスプロバイダは、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、盗聴や意図しない変更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 および NAS のセキュリティポリシーが暗号化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（4.5.1.1 参照）に従って、安全な暗号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：[03]

4.5.3.3 ミッドホールおよびバックホールのセキュリティ

制御タイプ	予防的
関連するセキュリティ目的	認証、機密性、完全性
セキュリティの概念	保護

管理策：5G NR システムコンポーネント間の相互認証を確保し、転送される情報のトランスポートレベルでの機密性と完全性を確保することが望ましい。

ガイダンス：5G 技術サプライヤと 5G サービスプロバイダは、5G NR コンポーネント間のすべてのインタフェースに相互認証、機密性、および完全性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別の機能レイヤを提供するだけでなく、運用と管理のトラフィックを保護するためにも役立つ。3GPP 仕様によると、このセキュリティ機能は、以下のインタフェースで IPsec または (D)TLS のセキュリティを確保することにより実現できる。

- 分散 RAN アーキテクチャ（すなわち、F1-U、F1-C、および E1 インタフェース）を活用して実装する gNB-DU と gNB-CU コンポーネント間のインタフェース
- 個々の gNB-CU コンポーネント間、または gNB と ng-eNB 間のインタフェース（すなわち、Xn または X2 インタフェース）
- 5G コアに接続するインタフェース（すなわち、N 2 および N 3 インタフェース）

参考文献：[03]

4.5.3.4 安全な非 3GPP アクセス

制御タイプ	予防的
関連するセキュリティ目的	認証、機密性、完全性
セキュリティの概念	保護

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 コアと携帯端末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事業者によって信頼されているか否かによって、ユーザ装置は、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 サービスプロバイダは、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（[03]）および/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 アクセスを使用する場合は、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(4.5.1.1 参照)に従って、TNGF および N3IWF で安全な暗号アルゴリズムを使用すること。

参考文献：[03]

4.5.4 コアネットワークにおける対策

4.5.4.1 ユーザプレーンの保護

制御タイプ	予防的
関連するセキュリティ目的	認証、機密性、完全性
セキュリティの概念	保護

管理策：ユーザプレーンのトラフィックが、5G コアに接続しているインタフェースや内部のインタフェースを介して保護されていない状態で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：ユーザデータの保護は、5G NR と 5G コアネットワークの接点における保護にはとどまらない。特に UPF の柔軟な展開に特徴づけられる、5G の展開における分散型の基本的な特性により、これらの機能がすべての外部通信に対して確立されたセキュリティプロトコルに依存することになる。したがって、5G サービスプロバイダは、関連するすべてのコアネットワークインタフェース（すなわち、すべてのコアネットワークインタフェース）で IPsec を使用して、ユーザプレーントラフィックの相互認証、機密性、および完全性を確保することが望ましい。

- UPF と 5G NR を接続するインタフェース（すなわち、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（すなわち、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（すなわち、N6 インタフェース）

一般的な IPsec 保護に加えて、5G は 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、以下を含む GTP-U セキュリティを確保する。

- 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

参考文献：-

4.5.4.2 コントロールプレーンの保護

制御タイプ	予防的
関連するセキュリティ目的	認証、機密性、完全性
セキュリティの概念	保護

管理策：5G コア内部のコントロールプレーンシグナリングのセキュリティを確保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、個々の通信相手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 サービスプロバイダは、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が、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、および完全性の確保が含まれる。

- サービス登録時およ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 展開がコアネットワークシグナリングに SCP を使用する場合、4.5.4.8 のセキュアサービスメッシュに関する管理策に加えて、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内部通信
- 異なる SCP インスタンス間の通信

参考文献：-

4.5.4.3 初期 NAS メッセージの保護

制御タイプ	予防的
関連するセキュリティ目的	完全性
セキュリティの概念	保護

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確保することが望ましい。

ガイダンス：5G では、5G UE が既存のセキュリティ環境を使用して保護された必要な情報要素を転送するか、セキュリティ環境がない場合、限られた情報要素の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している。NAS セキュリティ環境が確立されると、AMF は UE に対して、元のクリアテキストメッセージと一緒に保護された形で完全な初期 NAS メッセージを再送信するように要求することができ、AMF は受信した情報の完全性を検証することができる。
5G 技術サプライヤと 5G サービスプロバイダは、最初の NAS メッセージの完全性チェックに失敗した場合、新しい認証手順を開始することで、AMF の実装が 3GPP 技術基準で指定されたとおりに動作することを確認することが望ましい。

参考文献：[03]

4.5.4.4 利用者のプライバシー

制御タイプ	予防的
関連するセキュリティ目的	機密性
セキュリティの概念	保護

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 および 5G コアネットワーク NF 以外のパーティへのサブスクリプションパーマネント識別子 (SUPI) の公開を防止するセキュリティ対策を導入している。これは、SUPI を暗号化して Subscription Concealed Identity (SUCI) を形成し、SUPI による加入者ページングの使用を禁止し、代わりに 5G Global Unique Temporary Identifier (5G-GUTI) に依拠することで達成される。これらの制御を効果的に実施するために、5G サービスプロバイダ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：

- 秘匿化された SUPI の計算が USIM 内部で行われるか、ME 内部で行われるかを、5G セキュリティポリシーで詳述すること。
- USIM 内のサブスクリプションプロファイルを準備し、どこで SUCI 秘匿化を実行するか、どのような秘匿化スキームを使用するかを指定すること。
- 5G コアネットワークが、UE が緊急サービスにアクセスする場合を除き、ヌルスキームを使用して生成された SUCI を受け入れないようにすること。
- 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を提供すること。

一時的な加入者 ID について：

- 5G-GUTI の頻繁な再割り当てを実施すること。
- 5G-GUTI のランダム成分である 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を保証すること。

参考文献：[03]

4.5.4.5 相互接続のセキュリティ

制御タイプ	予防的
関連するセキュリティ目的	認証、機密性、完全性
セキュリティの概念	保護

管理策：コントロールプレーン・シグナリング・トラフィックとネットワークエッジを、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：N32 インタフェースは、5G ネットワークが外部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、インバウンドの N32 メッセージの制御も実施することで、セキュリティ・エンフォースメント・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 サービスプロバイダは、N32 インタフェースに関して以下の注意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(4.5.1.1 参照)に従って、安全な暗号アルゴリズムを使用した暗号スイートの使用を確実にすること。
- 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、仲介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実施すること。
- 受信 N32 メッセージのためのクロスレイヤーのなりすまし防止メカニズムを実施すること。
- 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実施すること。

参考文献：[03]

4.5.4.6 ホームコントロールの強化

制御タイプ	予防的
関連するセキュリティ目的	認証、認可
セキュリティの概念	保護

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プロバイダは、プライマリ認証の実行結果（認証が成功したかどうかに関わらず）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 サービスプロバイダがこの機能を利用するために、5G 技術サプライヤは、UDM の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 サービスプロバイダは、明示的な認証確認を必要とする不正行為が発生しやすいシナリオを特定し、5G セキュリティポリシーに文書化することが望ましい。UDM は、十分に最近の成功した認証確認を受信した後にのみ、これらの手順を許可するように構成する。情報を Nudm_UECM_Registration 手順にリンクする方法の例は、3GPP 技術仕様書（[03]、6.1.4.1a）に記載されている。

参考文献：[03]

4.5.4.7 サービスメッシュのセキュリティ

制御タイプ	予防的
関連するセキュリティ目的	認証、機密性、完全性、セグメンテーションと分離
セキュリティの概念	保護

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うことで、5G SCP のセキュリティを確保することが望ましい。

ガイダンス：サービス・コミュニケーション・プロキシは、5G コアネットワークの重要な要素であり、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、メッセージ・ルーティング、サービス・ディスカバリ、ロードバランシングなどの基本的な通信タスクをサポートする。5G コアを正しく機能させ、可用性を確保するために重要な役割を果たすため、5G サービスプロバイダは SCP 自体のセキュリティを確保することが不可欠である。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 コアネットワークを、サービスを提供するセキュリティドメインに応じて複数の SCP インスタンスに分割すること。
- ネットワークの機密性の高い領域では、レイヤ 3 で 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複製すること。
- 個々の SCP コンポーネントのリソース使用制限を定義し、実施すること。
- 以下のような SCP に関連する運用データの収集と集中記録を確実に行うこと。
  - ・システムコンポーネントあたりのリソース使用（例えば CPU 負荷、メモリ使用量）
  - ・メッセージの統計情報（例えば受信したメッセージ数、拒否したメッセージ数、受け入れたメッセージ数）
  - ・通信ピアに関する情報（例えば接続された NF、アクティブ/無反応な NF の数、毎秒送信されるメッセージの数）

参考文献：[19]

4.5.4.8 ネットワークスライスの厳密な分離

制御タイプ	予防的
関連するセキュリティ目的	機密性、可用性、セグメンテーションと分離
セキュリティの概念	保護

管理策: 異なるネットワーク スライス間で効果的な分離を行うことが望ましい。

ガイダンス：スライス A でアクセス可能な情報がスライス B でアクセスできないようにし、スライス A の危殆化が自動的にスライス B の危殆化につながることはなく、スライスが他のスライスのパフォーマンスや可用性に影響を与えないようにする。ネットワークスライシングにより、5G サービスプロバイダは、共通の物理ネットワーク・インフラストラクチャ上に多重化された、独自のサービス、リソース、SLA を持つ複数の仮想ネットワークを提供することが可能になる。ネットワークスライシングの具体的な実装は、明確に定義された、あるいは標準化された技術というよりは、アーキテクチャ上の概念であり、5G の展開によって異なる形態（メッセージ・タギング、VLAN、VPN など）になることが予想される。いずれにしても、5G 技術プロバイダは、効果的なスライス分離とスライスデータとメタデータの機密性を確保するために、以下を含む一定のセキュリティ上の注意事項を遵守することが望ましい。

- マルチベンダおよ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）の設計と開発。
- 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、および異なるスライスオーケストレータ間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と最大値を定義できるようにすること。
- 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確実に行うこと。
- スライス間の暗号分離を確実に行うこと。

参考文献：-

4.5.4.9 DDoS 対策

制御タイプ	予防的
関連するセキュリティ目的	可用性
セキュリティの概念	保護

管理策：意図しないトラフィック急増の標的型 DDoS 攻撃による過剰なトラフィック負荷からネットワーク機能を保護することが望ましい。

ガイダンス： 5G システムにおいては、提供する機能とネットワーク内の論理的な位置に起因し、DoS 攻撃があると高いインパクトを受けるネットワーク機能が存在する。多くの場合、1 つ以上のセキュリティドメインの交差点に位置しており、AMF、N3IWF/TNGF、UPF/IPUPS、SCP、NRF、NEF、および SEPP などのネットワーク機能が含まれる。これらのコンポーネントの可用性を確保するために、5G サービスプロバイダは以下の推奨事項に従うことが望ましい。

- 以下を含む、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こと。
  ・論理システムの冗長性
  ・地理システムの冗長性
  ・リンク冗長性
- 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るが、すべての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。
- レート制限やトラフィックシェーピングの技術を、専用のセキュリティ要素とネットワーク機能の両方に採用すること。

参考文献：-

4.5.5 MEC における対策

4.5.5.1 MEC アプリケーションの監査

制御タイプ	予防的
関連するセキュリティ目的	認証、機密性、完全性
セキュリティの概念	識別

管理策：サードパーティの MEC アプリケーションが 5G サービスプロバイダにより設定された要件を満たし、ネットワークと処理された通信データのセキュリティを確保することが望ましい。

ガイダンス：5G エコシステム (4.3.3 項参照) で動作するすべてのソフトウェアに推奨される一般的なセキュリティ確保の活動に加えて、MEC アプリケーションとそれをサポートする AF は、専用の監査プロセスを受けることが望ましい。このようなプロセスは、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どうかを検証する必要がある。したがって、5G サービスプロバイダは、以下を実施することが望ましい。

- 5G サービスプロバイダの MEC 環境にソフトウェアを展開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、例えば安全な通信、鍵管理、完全性、アクセス管理などを規定すること。
- 処理される情報の種類（例えば、位置情報、ユーザの音声／映像)、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 での保持時間など、開発者による 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文書化を要求すること。
- MEC アプリケーション開発者に上記のセキュリティ要件に準拠していることの証明を要求するか、または積極的な検証を実施すること。

参考文献：-

4.5.5.2 MEC アクセスコントロール

制御タイプ	予防的
関連するセキュリティ目的	認証、認可
セキュリティの概念	保護

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、ユーザエンドユーザとの距離が近くなることで利益を得られる特定のユースケースの支援という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・グループに限定される。5G サービスプロバイダと 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が複数のレベルで制限されていることを確認することが望ましい。例えば、以下の確認事項がある。

- PCF により、要求する 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こと。
- SMF によって、ユーザデータを正しい LADN（最も加入者に近いもの）に誘導する役割を果たすこと。
- ローカルな UPF により、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 UP トラフィックのみを転送すること。
- MEC アプリ自身によって、アプリケーション層上で加入者の認証と認可を行うこと。

MEC アプリケーションにおける加入者認証は、5G のセカンダリ認証を利用することもできる。この仕組みにより、オーバーザトップサービスへのアクセス許可前に、外部利用者が追加的な EAP ベースの認証手続きを実施することができる。

参考文献：-

4.5.5.3 MEC 制御データの保護

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性
セキュリティの概念	保護

管理策：MEC コンポーネントの内部および外部との間でやりとり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のトラフィックは、他のネットワークドメインと同様に、機密性と完全性の確保が必要である。MEC のシナリオでは、これにはサービス構成、アクセス制御リストやポリシー、DNS レコードが含まれる場合がある。5G サービスプロバイダ、MEC アプリケーション開発者、LADN プラットフォーム事業者は、以下のセキュリティ対策を遵守することで、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。

- トランスポート層の相互認証、機密性、完全性の確保を、外部インタフェースと内部 MEC コンポーネント間の両方で実施すること（例：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など）。
- 特に重要な制御データに対して、アプリケーション層での完全性と必要に応じた機密性の確保を実施すること。例えば、DNS レコードに DNSSEC を使用したり、時刻データに NTS を使用したりすること。
- コントロールプレーンの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こと（4.5.1.3 参照）。

参考文献：[05], [12]

4.5.5.4 MEC ユーザデータの保護

制御タイプ	予防的
関連するセキュリティ目的	機密性、完全性
セキュリティの概念	保護

管理策：MEC 環境内での転送中および保存中のユーザプレーントラフィックを保護することが望ましい。

ガイダンス：MEC の導入は、ネットワークエッジに近接しているため、中央のネットワーク機能に比べて物理的なセキュリティは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プレーンのトラフィックに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 サービスプロバイダ、MEC アプリケーション開発者、LADN プラットフォーム事業者は、共同で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、ユーザデータを運ぶインタフェースの秘匿性と完全性を確保すること。
- ユーザ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化のための秘密情報を適切な安全環境に保存すること（4.5.1.3 参照）。
- 永久記憶装置に書き込む前に、機密性の高いアプリケーションデータを暗号化すること
- 自己暗号化記憶装置を活用すること。

参考文献：-

4.5.5.5 MEC アイソレーション

制御タイプ	予防的
関連するセキュリティ目的	セグメンテーションと分離
セキュリティの概念	保護

管理策：MEC 環境と周辺のネットワークコンポーネント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：仮想化レイヤによって必要とされる MEC ワークロードの相互分離に加えて、MEC 配置と周囲のネットワーク機能との間には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展開オプションを可能にしているため、MEC コンポーネントを RAN またはコア NF のいずれかと同居させることができる。このようなシナリオでは、5G サービスプロバイダは、以下のような対策を実施することで、厳密な分離を実装することが望ましい。

- 可能であれば、MEC コンポーネントは、物理的にも論理的にも他のネットワーク機能とは別のプラットフォーム上で実行されること。
- 完全な分離ができない場合は、以下のように複数のレイヤで厳密に論理的に分離するようにする：
  - ・MEC コンポーネント用に専用の仮想化トラストドメインを定義し、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こと。
  - ・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こと。

参考文献：-

4.5.5.6 制御されたトラフィックステアリング

制御タイプ	予防的
関連するセキュリティ目的	認可
セキュリティの概念	保護、検出

管理策: MEC アプリケーション、サポートする AF、および加入者間の相互作用が適切に制御されたものであることを確実にすることが望ましい。

ガイダンス：5G システムでは、サードパーティの AF が PCF と統合することで、直接または NEF を介して間接的に、ユーザプレーンのトラフィックのルーティング決定に積極的に影響を与えることができる。この機能は、意図的または非意図的な AF の誤動作によってサービスに悪影響を及ぼす可能性があるため、PCF は、すべての受信要求に対して厳格な検証と認可を実施する必要がある。したがって、5G 技術サプライヤや 5G サービスプロバイダは、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。

- NEF および/または PCF のセキュリティポリシーの施行、特定の AF が影響を及ぼすことを許可された MEC サービスおよびモバイル加入者を指定すること。
- AF/NEF と AF/PCF 間の通信の報告と監視を実施すること。

参考文献：-

5 参考文献

[01] 3GPP, TS 23.501 V16.7.0, *Technical Specification Group Services and System Aspects; System architecture for 5G System (5GS)*; Stage 2, Dec 2020

[02] 3GPP, TS 33.210 V16.4.0, *Network Domain Security (NDS); IP network layer security*, Jul 2020

[03] 3GPP, TS 33.310 V16.6.0, *Network Domain Security (NDS); Authentication Framework (AF)*, Dec 2020

[04] 3GPP, TS 33.501 V16.5.0, *Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system*, Dec 2020

[05] Arends, R. Austein, R. Larson, M. Massey, D. Rose, S. RFC 4033, *DNS Security Introduction and Requirements*, Mar 2005

[06] Rupprecht, D., Kohls, K., Holz, T., Pöpper, C., *Breaking LTE on Layer Two*, May 2019

[07] ETSI, GS MEC 003 V2.1.1, *Multi-access Edge Computing (MEC); Framework and Reference Architecture*, Jan 2019

[08] ETSI, GS NFV 002 V1.2.1, *Network Functions Virtualisation (NFV); Architectural Framework*, Dec 2014

[09] ETSI, GS NFV-SEC 009 V1.1.1, Report on use cases and technical approaches for multi-layer host administration, Dec 2015

[10] ETSI, GS NFV-SEC 012 V3.1.1, *System architecture specification for execution of sensitive NFV components*, Jan 2017

[11] ETSI, GS NFV-SEC 014 V3.1.1, *Security Specification for MANO Components and Reference points*, Apr 2018

[12] Franke, D., Sibold, D., Teichel, K., Dansarie, M., Sundblad, M., RFC 8915, *Network Time Security for Network Time Protocol*, Sep 2020

[13] Igor Smolyar, Muli Ben-Yehuda, and Dan Tsafrir, *Securing Self-Virtualizing Ethernet Devices*, 24th USENIX Security Symposium, 2015

[14] Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., Hamburg, M., *Meltdown: Reading Kernel Memory from User Space*, 2018

[15] NIST, SP 800-50, *Building an Information Technology Security Awareness and Training Program*, Oct 2003

[16] NIST, SP 800-125, *Guide to Security for Full Virtualization Technologies*, Jan 2011

[17] NIST, SP 800-125A Rev. 1, *Security Recommendations for Server-based Hypervisor Platforms*, Jun 2018

[18] NIST, SP 800-125B, *Secure Virtual Network Configuration for Virtual Machine (VM) Protection*, Mar 2016

[19] NIST, SP 800-204, *Security Strategies for Microservices-based Application Systems*, Aug 2019

[20] NIST, SP 800-53 Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, Sep 2020

[21] NIST, SP 800-57 Part 1 Rev. 5, *Recommendation for Key Management: Part 1 - General*, May 2020

[22] NIST, SP 800-92, *Guide to Computer Security Log Management*, Sep 2006

[23] OWASP Foundation, OWASP API Security Top 10 2019, *The Ten Most Critical API Security Risks*, Dec 2019

[24] Prasad, A. R., Arumugam, S., Sheeba B, Zugenmaier, A., *3GPP 5G Security*, Journal of ICT Standardization Vol.6, Mar 2018