資料31-1

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）について

KDDI株式会社

2021年 5月 13日

Tomorrow, Together

KDDI

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の全体概要

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の策定に当たって、5Gセキュリティに関する標準化機関や海外の政府当局等の検討動向の調査、検証環境を用いたセキュリティ脅威や脆弱性等の検証、対策要件の整理を実施。上記取組によって得られた知見等を、セキュリティ脅威分析や対策要件に反映するなどして、規定内容を拡充。

1．外部動向等の調査等

- 3GPPやITU-T等の国際標準化団体におけるセキュリティ検討動向やガイドライン策定状況を調査。
- 海外のBeyond5G/6G検討プロジェクト (FG NET-2030等) におけるセキュリティ検討動向を調査。
- 欧米政府当局における5Gセキュリティに関する政策動向、ガイドライン化の状況等を調査。
- 3GPPで検討中の5Gユースケースごとのセキュリティ課題を整理。
- MECや仮想化の進展による汎用ハードウェアやオープンソース利用にともなうセキュリティ課題を整理。

2．セキュリティ課題の検討及び実機検証

5G環境の特徴的な技術や活用形態におけるセキュリティ課題を検討し、実機を用いて検証。

- 4Gから5Gへのコア機能の拡張を想定し、コンテナ/VM混在環境の実装形態における脆弱性や攻撃可能性を整理し、検証環境を用いてペネトレーションテスト等で実証し、対策要件を整理。
- セキュリティ対策が不十分なローカル5G事業者が存在することを想定し、相互接続によって生じる脆弱性や攻撃可能性を分析、実機を用いてなりすましやファジングテスト等を行い、脆弱性や攻撃手法を検証。
- MEC機能の実装形において生じ得る脆弱性を検討し、通信パケット偽装したサービス妨害攻撃等の可能性を検証、対策手法を検討。

実証結果を反映

標準化の議論内容、他のガイドライン等との整合性を確認

3．対策等留意点の策定

昨年度版をベースに、外部動向調査や実機検証の結果を反映し、今年度版を策定。

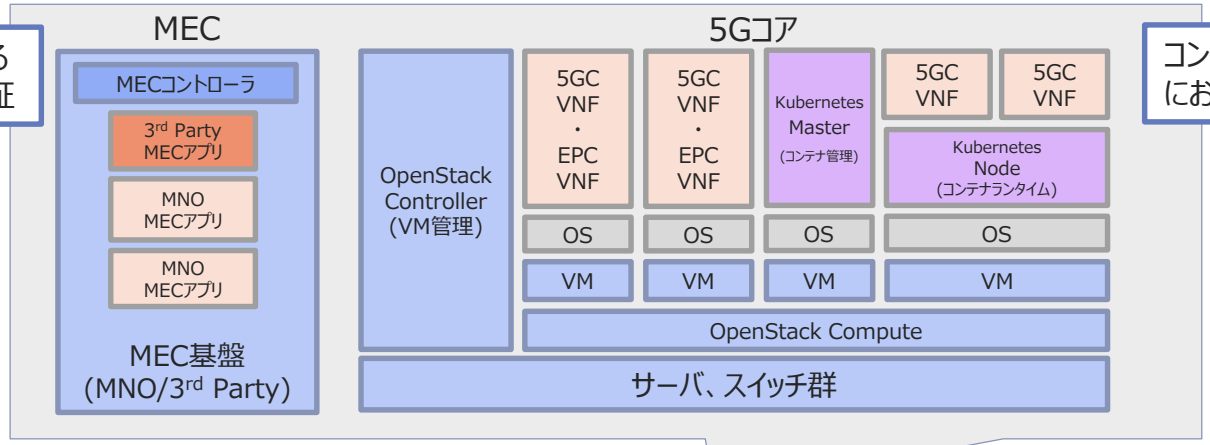
- STRIDE-LMモデルを使用して脅威を洗い出し、体系的に整理。
- 対策要件は、以下の分類で管理策(対策の基準)とガイダンス(対策のTIPS集)を整理。
  - 組織的・人的管理策
  - 運用管理策
  - 物理的管理策
  - 技術的対策

検証環境を用いた実機検証（全体概要）

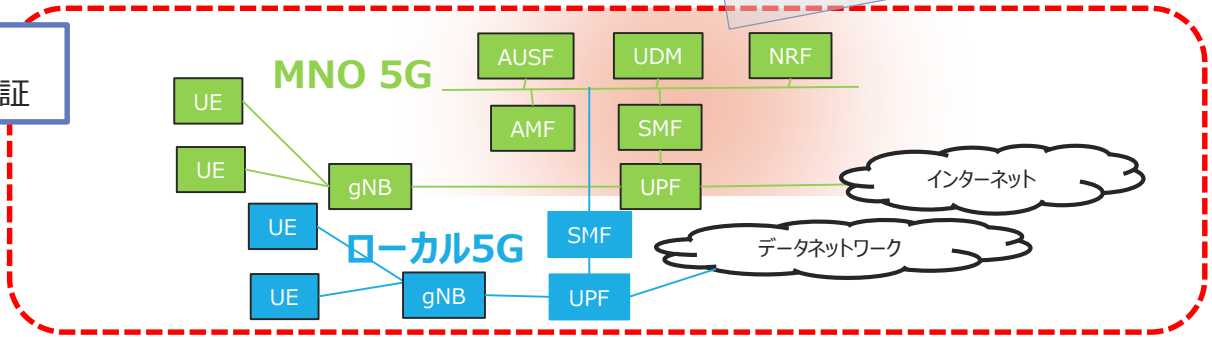
5G仕様に基づくセキュリティ分析と検証に加え、仮想化基盤、MEC基盤のセキュリティ、サプライチェーンセキュリティを含む5Gネットワークの構築・運用の全体像を考慮した検証を実施し、検証結果を対策等留意点に反映した。

MEC環境における脆弱性評価・検証

コンテナ・仮想化混在環境における脆弱性評価・検証



5Gコアにおける脆弱性評価・検証



評価・検証結果について

検証環境を用いたセキュリティ脅威の評価・検証の結果を規定にフィードバック。

評価・検証作業	セキュリティ脅威（抜粋）	対策要件の検討結果	対策等留意点への反映例
コンテナ・仮想化混在環境における脆弱性評価・検証	・OSS（オープンソースソフトウェア）の利用範囲が拡大することで、頻繁に脆弱性が見つかる ・コンテナ・VM混在環境は、コンテナ・VMどちらか一方でも脆弱性があると内部侵入後に侵入範囲を拡大される ・スライス・MECの利用拡大により、ネットワークの構造がダイナミックに変化し、内部侵入拡大リスクは更に複雑化する	・運用において自社管理のデータベースを活用し、アセット情報と脆弱性を管理する ・ネットワークをファイアウォール等で分離し、ネットワークの境界におけるアクセス制限を実施することで、侵入の阻害と拡大防止を図る	• 4.3.4項 インベントリと構成管理 • 4.5.2項 仮想化における対策の各項
5Gコアにおける脆弱性評価・検証	・セキュリティ保護が有効になる前の初期登録メッセージにおいて不正パラメータ送信によるサービス妨害の可能性がある ・加入者情報を窃取された場合、緊急登録を利用した ・なりすましを実行される可能性がある	・AMFが不正な初期NASメッセージも適切に処理する ・SUPIを保護する ・UE登録手順において不正なUEの登録要求を排除する	• 4.5.4.3項 初期NASメッセージの保護 • 4.5.4.4項　加入者プライバシ
MECにおける脆弱性評価・検証	・低遅延サービス実現のためコンテナアプリからDPDK等を用いたネットワークインタフェースカードの直接制御を許可すると通常のパケットフィルタ機構がバイパスされ、パケットの宛先や送信元を偽装しクライアントやMEC基盤上の別のコンテナに攻撃される	・ネットワークインタフェースカード上でのフィルタ等、カーネル内での処理をバイパスされても適用されるアクセスコントロールを実装する	• 4.5.5.2項 MECアクセスコントロール

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の更新

昨年7月公表の「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（令和元年度版）※」をベースに、
３章リファレンスモデルを追加、5G環境におけるセキュリティ脅威を詳細に分析した結果を反映するなどして、記載を更新。

※ 総務省サイバーセキュリティタスクフォース(第25回) 資料25-4

旧版 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（令和元年度版）

前書き 位置づけ、適用対象等を説明

対策要件

1. 5G構成要素のための共通的なセキュリティ対策として、共通対策11項目を規定
2. NFV、MEC、ネットワークスライスのセキュリティ対策を概説し、対策の留意点10項目を規定
3. 5Gコアネットワークのためのセキュリティ対策3項目を規定
4. 基地局、Air-Interface のためのセキュリティ対策の概要を記載

付録 本文で用いられる用語・略語

更新

新版 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）

1章 適用領域 適用範囲、目標、対象、位置づけを説明

2章 用語と定義 本ドキュメントで使用する用語・略語等を説明

3章 リファレンスモデルおよび脅威分析

1）脅威分析、インパクト分析モデルとして、5G基本ネットワーク機能の参照モデル、NFV参照モデル、MEC参照モデルを規定
2）STRIDE-LMを用いた脅威分析の手法について解説
3）脅威の主体になるものとして「脅威アクター」を整理
4）5Gコアの信頼モデルとコンポ―ネントごとのリスクエクスポージャーを整理

4章 対策（管理策）

- 5Gネットワークの開発、構築、運用に関連して推奨されるセキュリティ対策について、管理策とガイダンスの2段階構成で規定
- 旧版の共通対策は、「組織的な管理策」、「人的な管理策」、「物理的管理策」に分類して詳細を規定
- 旧版のNFV、MEC,ネットワークスライス、5Gコア、基地局、Air-Interfaceのセキュリティ対策は、運用管理策と技術的対策に分類して詳細を規定

リファレンスモデル

- セキュリティ脅威及び管理策の導出するための基本参照モデルを設定。
- 5Gネットワークの基本アーキテクチャとして、3GPPの参照モデル（図1）を使用して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記載。
- 次に、NFV（ネットワーク機能仮想化）におけるセキュリティ脅威を分析するために、ETSI NFV参照モデルの主要なコンポーネントで構成される参照モデルを設定し（図2）、異なる展開シナリオにおける信頼関係について解説。
- さらに、MEC（マルチアクセスエッジコンピューティング）の主要な構成要素からなるETSI MEC参照モデル（図3）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記載。

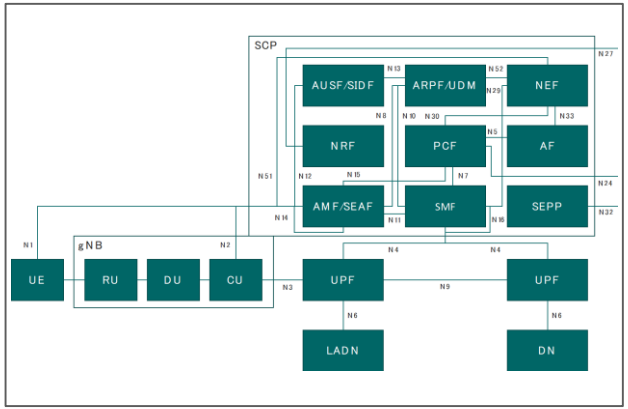


図1 5G基本アーキテクチャ参照モデル

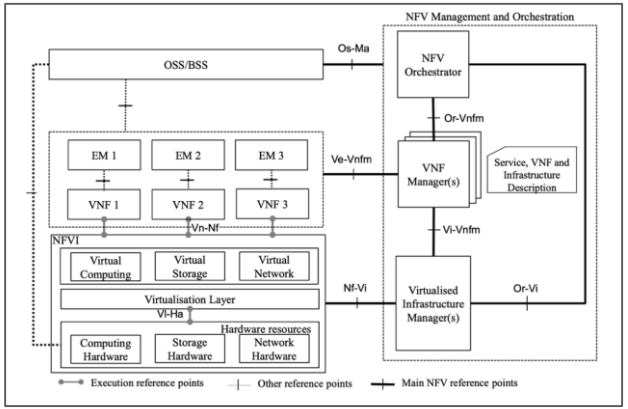


図2 NFV参照モデル

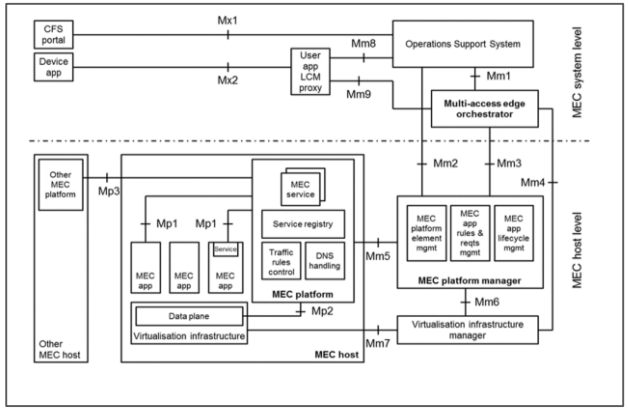


図3 MEC参照モデル

脅威分析の実施

- 3GPPの5G仕様では技術的なセキュリティ管理セットが文書化されているが、これは基本的対策を構成しているにすぎず、網羅的なものではない。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り、特に、仕様と実際の運用との間のギャップを埋めることが重要である。
- 本ドキュメントの策定に当たっては、そういった課題を解決するために、STRIDE-LMモデル(図4)を用いて体系的な脅威モデリングを行い、脅威と脆弱性を特定した。
- また、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ことから、図5に示す脅威アクター(脅威の主体) を整理した。

脅威	脅威に対応したセキュリティ目的
なりすまし	認証
改ざん	完全性の確保
否認	否認防止
情報漏えい	機密性の確保
サービスの拒否	可用性の確保
特権の昇格	適切な認可
ラテラルムーブメント	ネットワークの分離

図4　STRIDE-LMモデル

脅威アクター	脅威アクターの説明
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。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。
好奇心旺盛な者	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。

図5　脅威アクターの想定

信頼モデルとリスクエクスポージャーの整理

- 5Gのような複雑なシステムにおけるセキュリティを検討するために、個々のシステムコンポーネント間の信頼関係を信頼モデルとして整理する。図6に示すように、UE (MEとUSIMで構成) と5Gコア (特にARPF/UDM) によるトラストアンカー間の相互認証と信頼境界のポリシー運用により、コントロール手法を確立する。
- また、サイバー攻撃等を受けた場合に、リスクが顕在化する可能性の度合いについて、NFタイプごとに整理した (図7) 。脅威分析、対策整理において、特にリスクの高いNFを中心に対策を講じることを推奨する。

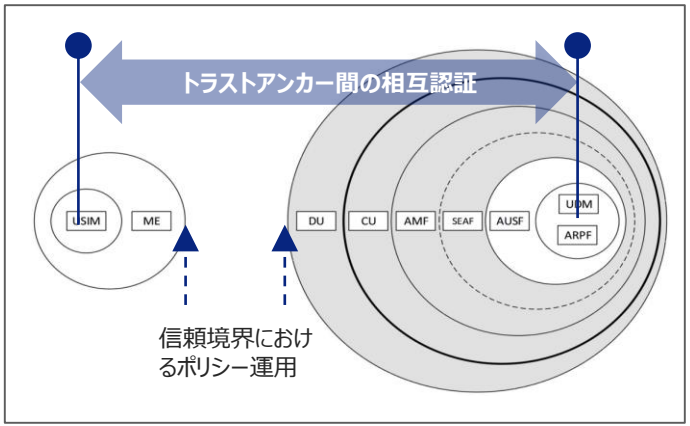


図6 信頼モデル

NFタイプ		NFの推定数	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
5Gコア	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
	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

図7 リスクエクスポージャーの整理

※リスクが高いものを黄色で表示

セキュリティ対策の規定

- 対策要件は、以下の分類ごとに整理して規定
  - 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
  - 主に組織の人員に関係する統制
  - 安全な運用と維持管理のための対策
  - 物理的セキュリティの基本的な安全対策
  - 技術的な対策

- 各セキュリティ対策の性質や個別のセキュリティ目的や対策の概念等の属性が分かるよう、対策要件ごとに以下の属性情報を付記。

制御タイプ	**予防、探知、是正 等**
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、否認防止 等**
セキュリティの概念	**識別、保護、検出 等**

- 個々の対策要件において、管理策とガイダンスを規定し、基準を示すだけではなく、対策の実装案等の情報を提供。

＜管理策＞
- セキュリティ対策の目的や資産等のあるべき姿を普遍的に規定したもの。対策の要件を具体的に示すものではない。
- ここで示す管理の状態が破られることでセキュリティリスクが高まるおそれがあることを説明している。

＜ガイダンス＞
- コントロールを適切に実現するか、または強化するための具体的な方策を示したもの。
- 本ドキュメントの利用者個々の環境において適用可能な要件、必要な要件を選択して実行する。

セキュリティ対策の規定概要

組織の管理策		組織の明確な役割と責任を確立すること、法令、業務要件、利害関係者の期待等に応じたポリシーを示すことなどを規定。
人的な管理策		企業のセキュリティ文化の醸成、セキュリティ教育、インシデント対処等について規定。
運用管理策		セキュアなソフト開発、インベントリ確立、セキュリティ監視、パッチ管理、バックアップ／リカバリー手順等、5Gネットワークにおけるセキュリティ運用に関連する要件を規定。
物理的な管理策		5Gコンポーネントへの物理的アクセスの制限や可視化等、施設関連のセキュリティ対策を規定。
技術的対策	共通	安全な暗号アルゴリズムの利用、IDやクレデンシャル情報、鍵情報等の適切な管理、セキュアブート手順の推奨、通信ピア間の相互認証、セキュアなAPI設計等について規定。
	仮想化	ホストと仮想化ワークロード間の信頼性、NFVIホストや仮想化レイヤの堅牢化、セキュアなVNF設計、MANOセキュリティ(管理トラフィックのセキュリティ)等について規定。
	RAN	ユーザプレーン、コントロールプレーンの保護、ミッドホール／バックホールセキュリティ、非3GPPアクセスの安全性確保等について規定。
	5Gコア	ユーザプレーン、コントロールプレーンの保護、初期NASメッセージの保護、加入者情報の保護、相互接続点(N32)のセキュリティ、ネットワークスライスの厳密な分離等について規定。
	MEC	MECアプリの監査、MECアプリへの不正アクセスの防止、MECコントロールプレーン・ユーザプレーンのトラヒック保護、MECワークロードの相互分離等について規定。

対策要件の記載例

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：
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。**

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。


Tomorrow, Together
KDDI