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）

本文書は、総務省における令和元年度「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、５Ｇ環境（アプリケーションを含む）の構築にあたる開発者、５Ｇの運用にあたるオペレータ、さらに５Ｇ環境を活用する利用者のために、５Ｇ環境における想定脅威に基づいたセキュリティ対策を参考情報として提供するものである。

構成としては、第 1 節に各構成要素に対して共通に適用する必要があるセキュリティ対策を、第２節に「仮想化基盤、MEC、ネットワークスライス」のためのセキュリティ対策を、第３節に「５Ｇコアネットワーク」のためのセキュリティ対策を、第４節に「基地局、Air-Interface」のセキュリティ対策を示す。なお、第２節から第４節については、令和二年度以降に調査・検討等を充実させる予定であるため、本文書では、概要レベルの記述に留めている。

本文書は、５Ｇシステム運用者、５Ｇシステム開発者及び５Ｇ利用者に対して推奨するセキュリティ対策であり、実施のための必須基準ではないことを注記する。

１．５Ｇ構成要素のための共通的なセキュリティ対策

【共通対策１】５Ｇセキュリティのポリシー

セキュリティ対策：

５Ｇセキュリティのポリシーを定義し、経営陣が承認し、公開し、従業員及び関連する外部の関係者に伝達し、計画された間隔又は重大な変更が発生した場合にレビューする必要がある。

対策の目的：

ビジネス要件、利害関係者の期待及びリスク環境での関連する法律と規制に従って、５Ｇセキュリティの管理の方向性とサポートを提供する。

ガイダンス：

５Ｇ サービス提供者又は５Ｇ サービス開発者は、５Ｇ セキュリティに対してコミットするため、５Ｇセキュリティのポリシーを定義する必要がある。５Ｇセキュリティのポリシーは、以下の内容を含むことが望ましい。

a）５Ｇサービスの提供における組織の責任
b）内部及び外部の利害関係者とその期待の整理
c）関連する法律及び規制
d）リスク環境の把握

また、５Ｇセキュリティのポリシーには、以下に関する記述を含める必要がある。

e）５Ｇセキュリティの定義
f）５Ｇセキュリティの目標（サービス提供者、サービス開発者等の）
g）組織内の５Ｇセキュリティの役割と責任

５Ｇセキュリティのポリシーは、情報セキュリティや５Ｇセキュリティ技術に関連し、５Ｇセキュリティインシデントを引き起こす可能性がある５Ｇサービスを把握し、それらに対処するものである必要がある。また、５Ｇセキュリティのポリシーでは、内部及び外部の利害関係者の安全に影響を与えるインシデントについても考慮する必要がある。

【共通対策２】組織のための対策

セキュリティ対策：
５Ｇのセキュリティの役割と責任を定義し、割り当てる必要がある。

対策の目的：
５Ｇサービス提供者又は５Ｇサービス開発者内で、５Ｇセキュリティの実装と運用を開始及び制御するための管理フレームワークを確立する。

ガイダンス：
５Ｇのセキュリティの役割と責任の割り当ては、５Ｇセキュリティのポリシー([共通対策１])に従って行う必要がある。
５Ｇセキュリティの役割と責任には、次のものが含まれる。
a）リスク管理活動
b）５Ｇシステム、設備、サービスのセキュリティ対策の設計
c）５Ｇシステム、設備、サービスの開発と運用におけるセキュリティ対策の実装と運用
d）サプライヤーとの関係の管理
e）認識、教育、トレーニングプログラム
f）インシデント管理プログラム

役割と責任は文書化され、組織内で広められ、必要に応じて見直され、更新される必要がある。

【共通対策３】安全な５Ｇシステムエンジニアリングの原則

セキュリティ対策：
５Ｇシステムの開発には、セキュリティ機能の設計と実装、多層防御、システムとソフトウェアの強化に対応するセキュアな５Ｇシステムを設計するための原則を適用する必要がある。

対策の目的：

５Ｇシステムの開発においてセキュリティが設計及び実装されることを保証するため。

ガイダンス：

５Ｇ サービス開発者は、安全な５Ｇ システムを設計するための原則を持つことが必要である。この原則では、５Ｇ利用者や、５Ｇサービス提供者、ネットワーク上のその他の外部エンティティに影響を与える可能性を考慮して、５Ｇシステムのリスクを特定する必要がある。リスクの特定には、５Ｇシステムのさまざまな側面を考慮する必要がある。想定されるリスクを以下に例示する。

a）ネットワークを介した５Ｇシステムと外部エンティティ間のインタフェース
b）システムの運用と保守における内部犯行（詐欺や悪用等）
c）外部エンティティから取得した製品及びサービスの品質問題
d）５Ｇシステム及びデバイスへの物理的アクセス

原則は、５Ｇシステム開発で考慮されるセキュリティ対策のうち、以下の領域に対処する必要がある。

e）セキュリティ機能
f）システムとソフトウェアの要件の強化
g）多層防御の要件、つまりセキュリティ機能の階層化された設計
h）モニタリングとロギングの機能（[共通対策６]と関連）

この原則は､以下のセキュリティ設計の概念を持つ５Ｇシステムの開発に適用する必要がある。

i）デフォルトで安全：この概念は、調達とシステム構成中に利用できる最も安全なオプションを選択するための要件をカバーする。例えば、

- 攻撃サーフィスの最小化
- 安全なサプライチェーンの使用
- 標準、ベストプラクティスの活用及び検証済みコードの再利用
- システムの強化と最小限の特権での動作

j）防御の厳格さ：この概念は、システムの設計における注意と完全性を保証するための要件をカバーする。例えば、

- 多層防御（多層）
- 幅（多様性）の防御、均一な保護
- システムの区画化（ネットワークセグメンテーション等）
- カプセル化を使用して機能へのアクセスの適切管理
- ハニーポットの使用を含む、異常の監視、検出、報告
- 脆弱性の評価とペンテスト
- 安全なエンジニアリング手法の使用
- 適切、かつタイムリーなパッチの適用

k）説明責任：この概念は、運用中に資産へのアクセスを許可及び監視する際の注意を確実にするための要件をカバーする。また、次のような既知の脆弱性を報告及び軽減する責任も含む。

- 適切な接続先とセキュアな接続の実施
- 職務の分離の確保
- 監査証跡の確立と保護
- 透明性の実践（ベンダーの開示、違反の開示等）

l）耐障害性：この概念は、セキュリティインシデントに対抗する能力又はセキュリティインシデントから回復する能力を確保するための要件をカバーする。例えば、

- 冗長性のための設計
- 可用性の管理
- 違反の想定
- 脆弱性の管理
- バックアップとリカバリ
- 規模（ボリューム）のテスト。

【共通対策４】安全な開発環境と手順

セキュリティ対策：
安全な開発環境と手順を５Ｇシステムの開発に適用する必要がある。

対策の目的：
開発中の５Ｇシステムへの不安要素の導入を回避するため。

ガイダンス：

開発環境には、システム開発に関連する人、プロセス、テクノロジー、設備が含まれる。

５Ｇサービス開発者は、個々の５Ｇシステム開発の取り組みにおけるリスクを評価し、以下を考慮した安全な開発環境を確立する必要がある。

a）環境で働く職員
b）適用された開発方法論、ソフトウェア及びデータ処理プロセス
c）外部委託された製品及びサービスの使用
d）物理的及びネットワーク環境
e）他の開発及び運用上の取り組みとの共存

また、５Ｇサービス開発者は、リスクを軽減するために開発環境と関連する手順を決定する必要がある。手順は、開発作業に携わるすべての担当者が理解する必要がある。

【共通対策５】５Ｇ設備とシステム設計の検証

セキュリティ対策：

５Ｇ設備と５Ｇシステムの設計と実装を検証する必要がある。

対策の目的：

５Ｇ設備と５Ｇシステムのセキュリティと安全性を確保するため。

ガイダンス：

５Ｇシステムは、５Ｇ設備とその他の機器で構成される。５Ｇサービス開発者又は５Ｇサービス提供者が５Ｇ設備を取得し、統合して５Ｇシステムを構築する場合は、５Ｇ設備と統合５Ｇシステムが意図したとおりに機能することを確認する必要がある。

５Ｇサービスの開発者と５Ｇサービス提供者は、次のことを行う必要がある。

a）検証が必要な５Ｇ設備、機能、インタフェースの特定

b）検証テストの計画

c）テストの実行

検証では、確立された基準を用いた適合性評価を実施する。適合のための５Ｇ設備又は機器の認証は、検証をサポートする証拠として使用できる。

【共通対策６】モニタリングとロギング

セキュリティ対策：

５Ｇ設備とシステムの状態、イベント、ネットワークトラフィックを監視してログに記録する必要がある。

対策の目的：

５Ｇデバイスとシステムの異常とインシデントを検出して追跡する。

ガイダンス：

モニタリングとロギングは、次の側面に対処するように設計及び実装する必要がある。

a）５Ｇシステム及び設備の状態、イベントやネットワークトラフィックを監視、記録するための機能及び操作

b）ログを分析するための機能とプロセス

c）検出された異常やインシデントによって引き起こされるシステム、人間及び組織の対応

監視、記録の対象となる状態、イベント及び通信には、次のものを含めることができる。

d）セキュリティ

・ 利用者認証
・ ５Ｇ設備の場所
・ ５Ｇシステム構成の変更
・ ネットワークトラフィック
・ プロセッサとメモリの使用量
・ 攻撃と不正アクセスの兆候
・ 故障
・ データの検知、作動の不正又は意図しない操作を示す値

e）信頼性

・ ５Ｇ設備又はシステムの停止
・ 環境条件、例えば温度と湿度

コンピューティング、ストレージ及び通信に利用可能なリソースを検討する必要があり、監視とロギングの機能を設計する際には、監視とロギングのさまざまなニーズを優先する必要がある。また、リソースと機能が制限されていて、自己監視とロギングが実行できない５Ｇ設備があることに注意する必要がある。これらの設備の場合、監視とロギングは、５Ｇシステムのサーバ又はネットワークノードで実行されるように設計する必要がある。

また、５Ｇシステムのログをログシステムに収集して、管理と運用を容易にすることができる。５Ｇの構成要素の疑わしい動作を早期に特定するために、必要な５Ｇ構成要素をロギング及びモニタリングアクティビティに含める。これには、不正アクセスの兆候や、データの不正操作等のモニタリングが含まれる。

【共通対策７】ログの保護

セキュリティ対策：

５Ｇ設備とシステムのログは、漏洩、破壊及び意図しない変更から保護する必要がある。

対策の目的：

ロギングの機能と信頼性を確保するため。

ガイダンス：

５Ｇ設備及びシステムのログの保護を設計及び実装する必要がある。ログを保護するための対策には、次のものがある。

・ ログファイルのアクセス制御
・ ログを処理するデバイス又はシステムのアクセス制御
・ ログ媒体を収容する施設の物理的アクセス制御
・ ログを処理するための手順の実施
・ ログの冗長構成

・ ログの破壊又は変更の検出（ハッシュ値の使用等）
・ ログの暗号化
・ タイムスタンプを含むログのエントリ
・ システムプロセスを除くすべてに対して「読み取り専用」化の実施

【共通対策８】５G サービスの提供における安全な設定と構成

セキュリティ対策：

５G サービスは、安全な設定と構成で提供する必要がある。

対策の目的：

提供中の５G サービスのセキュリティを確保するため。

ガイダンス：

５G サービスの初期設定と構成は、５G セキュリティポリシーに従って設計する必要がある。

５G サービスの提供において、関連する設定と構成は次のとおりである。

・ ソフトウェアのバージョンとパッチ
・ 開いているポートとネットワークサービス
・ サービスの機能とデータへのアクセス制限等。

【共通対策９】運用中のアップデートの適用

セキュリティ対策：

５G 設備とシステムのソフトウェアとファームウェアを更新するメカニズムを設計、実装、運用する必要がある。

対策の目的：

５G 設備と５G システムのソフトウェアとファームウェアを更新するためのセキュリティを確保するため。

ガイダンス：

５G サービスの開発では、５G 設備のソフトウェアとファームウェアを更新するメカニズムを基本機能として設計、実装する必要がある。また、ソフトウェアとファームウェアをロールバックするメカニズムも、更新に失敗したときに設計、実装する必要がある。

５G サービスの利用とサポートにおいて、ソフトウェア/ファームウェア更新パッケージには、更新プロセスが始まる前に、デジタル署名、署名証明書、署名証明書チェーンがデバイスによって検証されており、更新の整合性保護と機密保持に使用される暗号化キーは、安全に管理され、適切に操作される必要がある。

更新が失敗した場合、該設備は最後の既知の適切な構成にロールバックする必要がある。

【共通対策 10】DoS/DDoS 対策の適用

セキュリティ対策：

５Ｇシステムの様々な構成要素に対し、システム資源/帯域の枯渇、アプリケーションの使用不可等をもたらす攻撃に対抗するため、DoS/DDoS の脅威対象となる箇所を特定し、DoS/DDoS による資源やアプリケーションの機能不全を低減するための対策を行う必要がある。

対策の目的：

５Ｇシステムを DoS/DDoS 攻撃から保護するため。

ガイダンス：

大量のパケットを送り込み、ネットワーク帯域幅やネットワーク設備のリソースを消費させ、機能停止/低下を狙った DoS/DDoS 攻撃に対しては、DoS 攻撃の早期検知、攻撃パケットの検知と駆除、DoS 攻撃の分散化等、多くのセキュリティ対策が存在する。攻撃対象となる構成要素に応じ、適切な DoS 対策を実施することが必要となる。

また、TCP や HTTP 等のプロトコルで予想される動作を利用して、MEC 等のアプリケーションに過剰な負荷をかけ、正常な処理を妨げるアプリケーション DoS 攻撃に対しては、上位レベルでの検知機能の配備及び必要なネットワーク帯域の確保等の対策をとることが重要となる。

【共通対策 11】利害関係者間の責任の境界

セキュリティ対策：

５Ｇシステム及び５Ｇサービスのセキュリティに対する、５Ｇサービス開発者、５Ｇサービス提供者及びその他の利害関係者それぞれの役割を決定し、関係者間で合意する必要がある。

対策の目的：

５Ｇシステムとサービスの提供と使用に参加するエンティティを含む５Ｇシステムとサービスのセキュリティを確保するため。

ガイダンス：

セキュリティにおける５Ｇサービス開発者と５Ｇサービス提供者の役割は、５Ｇサービスプロビジョニングにおけるそれらの役割とともに決定する必要がある。５Ｇサービス開発者は、５Ｇサービスの開発、実装、テスト及び統合においてセキュリティの役割を持つ必要がある。５Ｇサービス提供者には、５Ｇサービスの管理と運用におけるセキュリティの役割が必要である。

５Ｇサービス開発者と５Ｇサービス提供者の役割には、必要に応じてセキュリティに関連する役割を割り当てる必要がある。

２．NFV、MEC、ネットワークスライスのためのセキュリティ対策

５Ｇでは、NFV、ネットワークスライス、MEC 等の技術を活用することで、多様なサービスの実現が期待されている。一方、５Ｇでは汎用ハードウェアやオープンソースソフトウェア（OSS）の利用、コンテンツ事業者、利用者端末への一部コア機能の解放が検討されており、従来の移動体通信網とは異なる脅威への対処が求められる。

安全な通信基盤とサービスを提供するには、NFV、ネットワークスライス、MEC において、以下のセキュリティ及び関係課題の解決等が必要である。

- 通信事業者外部に開放する API、管理インタフェースの堅牢化
- クラウドコンピューティングを参考にした、マルチテナント環境における利用者・サービス分類隔離技術の確立
- MEC における通信網内での第三者アプリケーションの動作を想定した分離・隔離・制限技術の確立
- NFV／スライス／エッジ・コンピューティングにおけるセキュリティ監査基準と監査手法の策定

以下の[対策 12]から[対策 21]までは、NFV、MEC、ネットワークスライスのセキュリティ向上のための対策例である。

【対策 12】セキュリティハイジーン（の取組）

セキュリティハイジーンは、多様な利用者から接続される MEC 等の環境を健全な状態に保つために５Ｇシステム管理者と運用者等が実施するべき対策であり、セキュリティ課題の解決、改善のためのベストプラクティスを含むものである。

【対策 13】セキュア API やセキュアなコア技術要素の活用

５Ｇで運用される多くの基盤環境においては、API を規定することにより、他サービスやアプリケーションへの機能提供を行っている。上記の[共通対策３]（安全な５Ｇシステムエンジニアリングの原則）に基づく、セキュアな API 設計及び運用を実施し、[共通対策５]に基づく機能検証を実施する必要がある。

【対策 14】強力な境界セキュリティの導入

MEC 等の環境においては、複数の構成要素によってシステム環境が構成されており、上記の[共通対策３]（安全な５Ｇシステムエンジニアリングの原則）に基づき、セキュリティ対策としての境界セキュリティを強化することが必要となる。これにより、境界外からのマルウェア侵入やサイバー攻撃を防ぎ、境界内のネットワークの通信で不正なアクセスがないか否かの検査を実施することが必要となる。

【対策 15】セキュアなオーケストレーションと自動化の導入

仮想化環境において、仮想サーバ(ノード)やアプリケーションの設定を統合的に行う、あるいは運用を自動化する目的となるオーケストレーション機能を対象とした攻撃に対抗する必要がある。特に、統合的な運用を行う際に、仮想サーバ間、仮想サーバとアプリケーション間等の管理設定に課題が多いことから、安全な設定管理を徹底することが必要となる。
また、オーケストレーション機能による複雑な構成要素を自動管理する場合、管理システムに対する設計的、運用的、人的な問題によるインシデントの管理、運用に関連する対策の実施が必要となる。

【対策 16】QoS（Quality of Service）によるポリシー管理

上記の[共通対策１]に掲げたセキュリティ対策（５G セキュリティポリシー）によって導出される QoS ポリシーに対して、５G サービス品質を確保するためのセキュリティ関連のポリシー管理を適切に実施することが必要となる。

【対策 17】セキュアなネットワークスライス機能

関連する上記の共通対策群を活用し、なりすましホストプラットフォームによるネットワークスライスの脅威及びスライスの制御奪取，スライスの破壊，悪用される脅威に対してセキュリティ対策を充実することが必要である。さらに、スライス間での情報漏洩や DoS/DDoS 攻撃によるスライス資源逼迫等の脅威に対する管理面の対策の実施も必要となる。

【対策 18】セキュアな OS 管理及びアプリケーションアップデート

セキュリティを確保した OS 管理及び稼働するアプリケーションのセキュリティ確保を目的としたセキュアなアップデートを実施することが必要となる。

【対策 19】MEC 等における健全な構成管理

多様な構成要素からなる５G の環境においては、５G サービスを安全に提供するための健全な構成管理が必要となり、関連する[共通対策３、５、８]に基づく具体的なセキュリティ対策の実施が重要となる。

【対策 20】５G 事業者によるネットワークセキュリティ監視

いかにセキュリティ設計を十分に実施し、十分な境界防御、多層防御等のセキュリティ対策を実施している場合でも、新たな脅威（攻撃）や事前には十分に考慮できていなかった環境

（システム）設定により、セキュリティが低下することが考えられる。このため、特に５Ｇネットワーク事業者にとっては、５Ｇシステムの健全性の確保を継続するために、ネットワークのセキュリティ監視を実施することが重要となる。

【対策 21】仮想化環境の脆弱性低減のためのセキュリティ

仮想化環境で上げられる脆弱性を突いた攻撃に対抗するために、多種多様なセキュリティ対策が必要となる。以下に掲げるセキュリティ対策の実施を考慮する必要がある。

- 仮想化環境で使用するソフトウェアの健全性検証の事前実施
- 仮想化基盤の最新化の確保（対応済の脆弱性混入の排除）
- 不正なイメージの登録等を防止するための仮想化環境の健全性の確保
- 適切な認証技術及びアクセス制御技術の活用による仮想化基盤のログイン管理、アクセス管理の強化
- 仮想化環境で交換されるデータへの盗聴、改ざん等の防止対策の実施
- 適切なネットワーク設定及びそれらの検証の実施
- 仮想化基盤のアクセス機能の健全性検証、ペネトレーションテスト等を実施　等

３．５Ｇコアネットワークのためのセキュリティ対策

想定する５Ｇコアネットワークの脅威に基づき､以下のセキュリティ対策の実施が必要となる。なお、多くの対策は、第１節及び第２節で述べたセキュリティ対策と同等な対策の実施がなされることとなる。特に、第２節で述べた[対策 13]から[対策 21]のセキュリティ対策については、５Ｇコアネットワークにおいても同様に適用される。

以下の[対策 22]から[対策 24]までは、５Ｇ コアネットワークのセキュリティ向上のための対策例である。

【対策 22】セキュアな５Ｇコアの通信管理

５Ｇ コアネットワークの運用において、セキュリティを十分に考慮することが必要となる。例えば、以下のような対策が必要となる。

- 健全なネットワーク設定の実施（不要ポートの不開放等）
- 利用される暗号化環境の検査の実施（最新の脆弱性情報等に基づく）
- コア外からの不正アクセス排除のため、適切なファイアウォールの設定の実施　等

【対策 23】コア内でのアクセス制御及び特権管理

上記の[対策 22]に含まれるが、５Ｇコアネットワークにおけるアクセス管理及び特権管理の適切な実施並びにモニタリングによるログ分析により、常時不正なアクセス等の検知・対応が必要である。例えば、以下のような対策が必要となる。

- 運用者毎の特権付与、権限管理の実施
- 特権や利用者への有効期限の適用
- 適切なアクセスログ管理の実施

【対策 24】コア内で利用されるアプリケーションのセキュリティ管理

５Ｇコアネットワークで動作する多様なアプリケーションに内在する脆弱性をついた攻撃を防止する必要がある。特に、第三者が開発したアプリケーション等、事前の検証が十分でないアプリケーションが攻撃のターゲットとなる。このため、アプリケーションに与えられる権限管理やアプリケーションの実行管理を徹底する必要がある。

例えば、以下のような対策が必要となる。

- アプリケーションへの権限管理の徹底
- コンテナ基盤内でのアプリケーション実行管理（高度認証等）の実施　等

４．基地局、Air-Interface のためのセキュリティ対策

基地局、Air-Interface のためのセキュリティ対策については、脅威分析を含め、令和二年度以降に充実させる予定である。しかし、基地局、Air-Interface においても、多くの対策は、第 2 節で述べた共通セキュリティ対策と同等な対策の実施がなされることとなる。以下に、令和二年三月末現在、考慮できる基地局、Air-Interface のためのセキュリティ対策を列挙する。

- 多様な利用者から接続される RAN 環境を健全な状態に保つための取組（[対策 12]と同等の対策）
- RAN における相互認証機能の活用・実施
- RAN 上を流れるデータの秘匿性を確保（暗号化の対策等）
- RAN 上のデータの完全性確保のための保護施策
- RAN における健全な構成管理の実施
- ５G 事業者によるネットワークセキュリティ監視の実施（[対策 20]と同等対策）

[付録] 本文で用いられる用語、略語

- MEC：Mobile Edge Computing/Multi-access Edge Computing、計算機資源を利用者端末の近くに分散配置する技術
- RAN：Radio Access Network、５Ｇのコアネットワークと UE との間の CU、DU、RU 等の機器により構成される無線アクセスのためのネットワーク
- DDoS/DoS：Distributed Denial of Service/Denial of Service、サービス不能攻撃
- NFV：Network Function Virtualization、ネットワーク機能仮想化、ネットワークで必要な機能を専用の機器ではなく汎用サーバ上の仮想マシン等で動作させネットワークに組み込む
- QoS：Quality of Service、帯域制御に用いる技術。QoS により特定の通信を優先することで、他の通信に影響されず広帯域もしくは低遅延で転送可能となる

以上