GCOT　６Ｇのセキュリティ及び強靭性に関する原則【仮訳】

１　GCOT　序文

次世代のモバイルネットワークである６Ｇは、すでにその姿を現しつつある。標準化の取組は依然として初期段階にあり、主要なサービスや要件はなお策定途上にあるとともに、その仕様は世代を通じて大きく進化していくことが見込まれる。しかし、IMT-2030 フレームワークと初期の 3GPP の６Ｇ研究に基づいて、いくつかの広範な予測を行うことができる。

- 人工知能（AI）は、ネットワーク性能の向上及び新たな利用者サービスの実現を可能とするため、ネイティブに活用される。
- モバイルネットワークは、外部センサーの統合と通信信号自体の活用を通じて、（基地局とユーザー端末双方の）センシング機能をサポートする能力を持つ。
- 地上系及び非地上系技術は、これまで十分にサービスが行き届いていない地域へのシームレスな接続性拡大と、ネットワークの強靭性向上を実現するため、より緊密に統合される。
- ５Ｇアドバンストシステムにおける周波数効率とエネルギー効率は、重要な優先事項となる。
- より多くのネットワーク機能が仮想化され、特定のハードウェアプラットフォームへの依存が低減されるとともに、ネットワーク資源の柔軟な展開が可能となる。
- 分離型アーキテクチャ及び標準化されたインターフェースにより、セキュリティの可視性が向上し、複数ベンダー間の統合が容易になる。

６Ｇに関する核心的な疑問の一つは、商業的な需要と、ネットワーク所有の総コストと新サービス展開の意欲とのバランスである。新世代の成功は、従来の世代と同様に、スマートフォンなどの大衆向け消費者機器での高い普及率と、それらを中心としたサービス提供の改善に大きく依存すると考えるのが妥当であろう。重要なことは、６Ｇの普及はネットワーク事業者にとっての商業的実現可能性にかかっている点である。これは周波数効率やエネルギー効率といった主要指標における性能によって決まるが、これらの指標は現在も徹底的な研究が続けられている。

しかし、６Ｇネットワークの開発は、純粋に商業的又は技術的な取組ではなく、より広範な公共的・戦略的関心事として理解されなければならない。６Ｇネットワークは、社会のデジタルインフラの重要な構成要素となり、製造業、運輸、エネルギーから医療、公共安全に至るまで、必須サービスや垂直産業を支える基盤となる。標準化プロセスは既にこの点をある程度認識しており、ITU の IMT-2030 フレームワークにおける包括的設計要素の中で社会的課題が特定されている。

６Ｇネットワークのセキュリティと強靭性は、この大きな枠組みにおいて極めて重要な側面である。公共・私有を問わず、６Ｇネットワークは世界中の人々の日常生活で重要な役割を担うようになる。我々の生活の多くは、その効率的で安全な運用に依存するようになる。これは政府や規制当局と同様に産業界にとっても重要である。消費者と企業が、６Ｇネットワークが安全で強靭なサービスを提供しユーザーデータのプライバシーを保護すると信頼できる場合にのみ、その商業的潜在能力を最大限に引き出すことができる。これらのネットワークは、各国の重要なインフラの一部を構成することから、設計段階においてセキュリティと強靭性を確保することが不可欠である。それは、経済的圧力にかかわらず、運用者が十分に安全で強靭なネットワークを維持できるよう支援する高い基準を設定するものである。

新たな機能や技術の発展により、通信システムはより広範で複雑化し、データ量も増加すると予想される。しかし、多くの場合、攻撃対象領域も同時に拡大し、悪意ある者にとっての攻撃機会や侵入経路も増えることになる。こうした新たなアーキテクチャや技術がもたらす課題に加え、４Ｇ、５Ｇシステムから引き継がれるセキュリティ上の課題も存在する。特に、既知の脆弱性を有する既存システムやプロトコルに依存する場合又は４Ｇ、５Ｇ等のシステムとの相互運用が継続されることでトラフィックが異なる保護レベルに晒される場合に顕著となる。６Ｇシステムのセキュリティが、レガシーシステムのセキュリティによって決定されることを許してはならない。これは後方互換性が要求される場合も含む。６Ｇシステムは、現在又は将来発生が予想されるセキュリティ脆弱性が特定されているレガシーシステムから十分に分離されなければならない。これにより、脅威のリスクを最小限に抑えるためである。さらに、脅威の状況は進化し続ける。例えば、６Ｇネットワークは、その展開期間を通じて、量子コンピューティングの高度化に直面する可能性があり、現在の通信インフラが依存しているセキュリティ及び暗号化の在り方が根本的に変容することになる。これらの課題は全て、システム設計と導入の可能な限り早い段階で取り組む必要がある。

ネットワークの強靭性はそれ自体が優先課題である。６Ｇネットワークを展開する各国は、困難な地理的条件や自然災害に起因するものか、市場の力学や集中化によって単一障害点や広範なサプライチェーン依存が生じるものかに関わらず、強靭性上の様々な課題に引き続き直面し続けるだろう。これらは、対象を絞った調達戦略や、供給者と運用者間のサプライチェーン依存関係に関する適切な情報共有といった措置を通じて、ある程度管理できる。しかし、ネットワーク供給の問題が発生した場合、ネットワーク供給における単一障害点のリスクは依然として低減が求められる。GCOT パートナーは、こうした課題に対応するため、各種の規制的取組や研究開発上の取組を既に進めている。例えば、カナダの「電気通信の信頼性アジェンダ」、日本の「革新的情報通信技術（Beyond 5G/6G）基金事業」、英国の「電気通信セキュリティ法」と「オープンネットワーク計画」、そして米国の「ワイヤレスサプライチェーン・イノベーション基金」などである。

GCOT パートナーは、進行中の標準化作業及び将来的な６Ｇネットワークの展開に当たり、進化し続けるセキュリティ及び強靭性上の課題に十分配慮する必要があることに合意する。（現行のモバイルネットワークと同様に）国家インフラの中核を担うこととなる６Ｇに期待される技術革新は、初期段階から根本的な保護策及びリスク軽減策を講じることを不可欠とする。そのためには、政府、通信事業者、それを支えるクラウドやデータインフラを含むシステム供給者の取組も求められる。また、必要に応じて国内及び地域の規制当局との緊密な連携を図り、官民連携を通じて脅威に関する共通理解と強固なコンプライアンスを確保することも重要である。

２　成果と目的

本声明は、６Ｇシステムの開発に際して優先的に考慮すべきセキュリティ及び強靭性に関する重要事項を示すことを目的とする。高い次元において、６Ｇシステムは以下のような積極的なセキュリティと強靭性に関する成果を提供すべきである。

1. **封じ込め（Containment）**：６Ｇシステムは、悪意ある行為者やソフトウェアがネットワーク内で拡散する能力を制限する。
2. **機密性（Confidentiality）**：６Ｇシステムは設計上、ユーザーデータのプライバシーを保護するように構築されており、機密性をもってデータを処理・提供できる。例えば、物理的に安全でないデータ又は不特定の経路を介して共有されるデータであっても、盗聴や攻撃者から安全である。
3. **完全性（Integrity）**：６Ｇシステムは、データの完全性を維持し、ネットワークを通過するデータに何らかの変更が生じた場合、それが検知可能であることを保証する。同様に、ネットワークインフラ自体の完全性も保証されなければならない。
4. **強靭性（Resilience）**：６Ｇシステムは測定可能な強靭性を備え、困難な状況下においても利用者へのサービス提供を維持できる。特に緊急通報や初動対応者向けの音声・データサービスといった要件は、６Ｇ移行時に将来を見据えた設計が必須である。これには安全で強靭性のあるサプライチェーンも含まれる。
5. **規制遵守（Regulatory Compliance）**：６Ｇシステムの運用者は、関連する国内規制や法令の要件を満たすことができる。

以下の原則は、６Ｇがこれらの成果を達成するための主要な技術的手段の一部を示すものである。第３節及び第４節の序文は、それぞれセキュリティと強靭性に関する包括的な枠組みを提供し、続く小節では具体的な原則が示される。各原則は各節の冒頭に灰色で記載され、その下に説明文が続く。

これらの原則は、GCOT における継続的な協力の指針となるが、関係する全ての利害関係者に対し、各国の管轄における重要課題を示す指針としても意図されている。

６Ｇの発展は、通信分野全体を巻き込む協働の取組となるものである。このためGCOT パートナーは、産業界、学術界をはじめとする関係者が、標準化及び展開の初期段階からこれらの原則を十分に考慮するよう取り組むことを強く奨励する。

３　セキュリティに関する原則

６Ｇシステムはセキュリティを基盤原則として、開発から導入、そして最終的な運用に至る全段階で考慮される形で構築される必要がある。６Ｇシステムは、前世代よりも安全であることを意識的に設計され、既存システムに依存する部分ではレガシー脆弱性を管理しなければならない。セキュリティ対策は、現在及び将来の脅威を適切に検証した上で策定されるべきであり、６Ｇシステムのアーキテクチャや全体的なシステム要件に関する決定は、早期段階で実現すべきセキュリティモデルと、その進化の必要性を適切に考慮しなければならない。

６Ｇが約束する接続性、成長、革新は、ネットワークが安全であり、ユーザーの信頼が損なわれない場合にのみ完全に実現される。公共ネットワークは、かつてないレベルの悪意あるサイバー活動に直面している。その性質はますます高度化しているため、ネットワーク上で伝送される機密情報が適切なレベルで保護されるよう、十分なセキュリティ対策を実施することが不可欠である。これらのネットワークが重要国家インフラを構成・支えるものであり、それに応じたセキュリティ確保が必要である。優れたセキュリティは単なる追加の技術要件ではなく、次世代技術の成功と普及を決定づける基盤となる柱である。

新たなモバイル技術は、過去の世代におけるネットワーク設計と実装を推進してきた前提条件や作業慣行を批判的に検証する機会をもたらす。６Ｇが「セキュア・バイ・デザイン（設計段階からのセキュリティ）」であるという理念は現在広く浸透しているが、初期の６Ｇシステムが開発されるにつれ、我々は５Ｇで得られた進歩を基盤として、理論から実践へと移行することが不可欠である。セキュリティを最初から正しく理解し、アーキテクチャやソリューションに統合しなければ、サードパーティシステムやレガシーシステムとの安全な相互運用を含め、後からシステムを改修したりパッチを当てたりするコストは、通信事業者にとっても、消費者の安全と信頼にとっても、到底許容できないものとなる。６Ｇは、セキュリティのために明確かつ論理的分離を設け、前世代や同世代ネットワークへの暗黙の信頼を回避するよう設計・実装される必要がある。例えば、仮想移動体通信事業者（MVNO）のホスティングやレガシー信号処理への後方互換性が、６Ｇシステムのセキュリティ

保証を低下させてはならない。第３．１節及び第３．２節では、ゼロトラストの原則[1]に沿って、６Ｇシステムの基盤アーキテクチャにセキュリティを組み込むため、内部インターフェースと外部インターフェースをそれぞれどのように保護するかを論じる。

これまでの世代進化と同様に、５Ｇシステムのパラダイムには継続的な改良が期待される。これには、従来のシステムから引き継いだサイバーセキュリティ設計上の課題や、実環境での導入によって浮き彫りになった問題の解決も含まれる。同時に、６Ｇは新たな課題や脅威をもたらすと予想される。例えば、（第３．３節で論じるとおり）より大量に保護すべきデータソースの増加、そしてセキュリティを強化しつつも危険に晒す可能性のあるAIやセンシング能力などである。これには、3GPPなどの主要な６Ｇの標準化団体の範囲外に一部位置する可能性のある技術（AI 等）も含まれる。しかし、そのセキュリティは、６Ｇの成功した安全な導入に不可欠となる。

導入されるあらゆる革新技術は、６Ｇネットワークが依存するサードパーティサービスを含め、導入初日からセキュリティを確保し、ユーザーデータのプライバシーを尊重することが不可欠である。そのためには脅威モデルの再検討と、規格準拠と真の運用上の強靭性を検証できる強力なテスト環境が必要となる。サイバーセキュリティへの取組と使用するツールも、現在及び将来の新たな脅威からユーザーを保護するため、進化を続けなければならない。これには、第３．４節で論じる暗号関連の量子コンピューティングの出現も含まれる。

３．１．　セキュリティ監視、認証及び認可

> ６Ｇシステムは、境界セキュリティから脱却し、ゼロトラストの原則に沿ったより細分化された機能レベルのセキュリティへ移行すべきである。ネットワークの継続的なセキュリティ監視と効果的なログ記録により、ネットワーク構成要素が侵害される可能性を動的に評価する必要がある。これには、使用前の検証を原則とし、各構成要素のアクセスをその機能遂行に必要なデータのみに制限する、堅牢な個々のネットワーク構成要素の認証及び認可を組み合わせる必要がある。

６Ｇは５Ｇの流れを継承し、ネットワーク機能の仮想化をさらに推進し、ソフトウェアを基盤となるハードウェアプラットフォームから切り離し、ネットワーク機能を様々な汎用コンピューティングプラットフォーム上でホストすることを目指している。多くの場合、クラウドコンピューティング（パブリック、プライベート、ハイブリッドのいずれか）の規模と柔軟性を活用し、多数のネットワーク機能やその

[1] NIST SP 800-207, Zero Trust Architecture (ZTA) (https://csrc.nist.gov/pubs/sp/800/207/final).

他のアプリケーションを同一のコンピューティングプラットフォーム上でホストする。また、複数の異なるベンダーの機器やソフトウェアを単一のモバイルネットワークスタックに統合することへの支援も高まるだろう。さらに、ネットワーク管理における AI の統合が進み、より高度な検知機能が導入されることで、ネットワーク全体で多様な種類のデータがより多く公開されるようになる。これにより、ネットワークサービスのサードパーティや消費者との新たな関係性が構築され、それに依存するようになる。

（第３.３節、第４.３節及び第４.４節で論じたとおり）これらの傾向は、イノベーションと強靭性の両面で、いくつかの潜在的な利益をもたらす。しかし同時に、従来の境界防御型セキュリティでは対応が困難な、再構築され、しばしば拡大した攻撃対象領域も生み出している。これは、ゼロトラストアーキテクチャの重要な側面への順守を必要とする。すなわち、境界だけでなくネットワーク内部においても堅牢なセキュリティ保護と認証が求められる。５Ｇで既に認識されているように、６Ｇは「システム内部」のものは自動的に信頼できるという設計前提から脱却しなければならない。ネットワーク機能は、他のネットワーク機能やデータソースへのアクセスを許可される前に、定期的に堅牢な認証を受けなければならない。アクセスは特定のタスクに対してのみ許可され、承認ポリシーは特定の状況やデータの重要性に応じて適切に設定される。これは、収集や配布における新たなセンシングデータのプライバシーに関する考慮事項など、異なるデータタイプの固有の機微性を考慮に入れるべきである。認証は基盤となるプラットフォームにも拡張され、安全なルートと信頼の連鎖を備えるべきである。

これに加え、運用担当者はネットワーク構成要素や主体（例：ユーザー端末、AI エージェント）を監視し、異常な活動や未申告機能の実行を検知できる必要がある。潜在的な侵入を早期に発見し、認証ポリシーを適切に更新することで、悪意ある主体がネットワーク内を拡散し機密データを流出させる能力を制限する。それには、６Ｇシステムが無線アクセス網とコアネットワークの両方から情報を調査・分析し（場合によってはオペレーターの監視システムに公開し）、監視とインシデント検知を可能にしながら、ユーザーのプライバシーを保護する必要がある。これには、分離境界を越えた潜在的な攻撃を監視するための十分な観測可能性も含まれるべきである。例えば、基盤プラットフォームの脆弱性を悪用してホストされたネットワーク機能を攻撃するケースや、ネットワークスライス間で悪意のある行為者が横方向に移動するケースが挙げられる。

ネットワーク機能とアプリケーションに対する堅牢なセキュリティ基準がここで重要な役割を果たす一方で、展開モデルとアーキテクチャもまた、3GPP やその他の標準化されたネットワーク機能が存在する物理的・デジタルインフラを十分に保護する必要がある。これには厳格な構成管理が含まれ、すべてのネットワーク構成と機能が導入時から強固なセキュリティ基準に準拠し、設定ミスを防ぐために継続的に

監視・維持されることを保証する。さらに、標準や規制は、通信ネットワークが重要国家インフラ（CNI）として位置付けられることに伴う主権に関する懸念の高まりを緩和できるよう、クラウド展開を調整可能なものとして保証しなければならない。

３．２．　安全な外部インターフェース

> ６Ｇシステムは、外部（レガシーを含む）ネットワーク、サブネットワーク、その他のシステムとのインターフェースにおいて強固なセキュリティをサポートすべきである。これにより、ユーザーデータのプライバシーと完全性及びホームネットワークのセキュリティを維持しつつ、ローミングユーザーに対する現地の規制要件にも準拠し続ける必要がある。また、６Ｇシステムの全体的なセキュリティは、ホームネットワーク事業者の管理外にあるネットワークやシステムのセキュリティを前提とすべきではない。

現在サービスが行き届いていない地域への接続性拡大は、６Ｇの目標である。これは ITU が「ユビキタス接続性」を IMT-2030 の主要利用シナリオに指定したことからも明らかである[2]。これを実現するため、加入者はより広範な「ネットワークのネットワーク」の一部として６Ｇを利用することになる。ユーザーデータは、PLMN（公衆移動通信網）、サブネットワーク、衛星・地上システム間、そして 3GPP と非 3GPP アクセス方式（主に WLAN/Wi-Fi）の間を移動する。これには、セキュリティ課題を抱えるレガシーシステムや、ユーザーのホームキャリアの管理外にあるネットワークも含まれる。

同時に、モバイル事業者が収益源の多様化を模索し、他の産業が接続性の向上による生産性向上を推進する中で、６Ｇでは e ヘルス、スマート製造、自動運転車などのいわゆる垂直アプリケーション支援への注力が再燃するだろう。これに伴い、一般的なスマートフォン、スマートウェアラブル、分散型 IoT など、接続デバイスの多様化が加速する。その多くは、非常に低コストな生産と極めて低いエネルギー消費を実現する必要がある。これらの異なるデバイスには、それぞれが扱うデータや動作環境に特有のセキュリティ要件、ハードウェアとソフトウェアの制約、（ハードウェアとソフトウェアの更新・リフレッシュを考慮した）大きく異なるデバイス更新サイクルが存在し、セキュリティ設計時にはこれらを全て考慮に入れる必要がある。さらに、「AI as a Service」やプログラマブルなアプリケーション・プログラミング・インターフェース（API）といった機能・サービスの実現には、（第３．

[2] Recommendation ITU-R M.2160-0 (11/2023) - Framework and overall objectives of the future development of IMT for 2030 and beyond (https://www.itu.int/rec/R-REC-M.2160-0-202311-I/en).

３節でも論じたとおり）ネットワーク外へのデータ公開を可能とする新たな外部インターフェースが必要となり、潜在的な攻撃対象領域が拡大する。

こうした多様なシステムとの相互運用性は、６Ｇの全体的なセキュリティパラダイムへの後付けとして扱うことはできず、その本質的な要素でなければならない。通信事業者は、この複雑で高度に異種混在したネットワーク群をユーザーデータが通過する際、その完全性とプライバシーを維持できなければならない。異なるネットワーク間、サブネットワーク間、外部アプリケーションとのインターフェースは適切に保護され、自社の管理下外にあるシステムのセキュリティ弱点が広範なネットワークに及ぼす潜在的な影響を制限する必要がある。これには包括的な API 監視とガバナンスも含まれる。これは、第３．１節で概説した内部インターフェースの保護に関するゼロトラストアプローチを基盤とするものである。ただし、関連するメカニズムはローミングユーザーに対する規制要件にも準拠すべきである。

インターフェース自体を超えて、６Ｇシステムからのデータ公開はユーザーのプライバシーを最大限に保護し、データ最小化の原則に準拠すべきである。これにより、サードパーティのネットワークやサービスは、許可された機能を果たすために必要なデータのみにアクセスできることを保証する。これには厳格なデータ分類、適切な暗号化（適切な場合には、静止時及び使用時を含む）、明確なデータライフサイクル管理方針などの対策が含まれる。

３．３．　セキュリティのための AI と安全な AI

> ６Ｇシステムは、AI 駆動の仕組みを活用し、潜在的なサイバーセキュリティ脅威やインシデントをより迅速かつ効果的に監視し対応すべきである。同時に、電気通信分野における AI システムは、安全かつ確実な方法で開発、導入、運用されるべきである。

GCOT は既に「電気通信産業における AI の導入に関する原則」[3]において、AI システムを６Ｇシステムに安全に統合し、継続的なセキュリティ監視と対応に活用する必要性を指摘している。

AI は６Ｇシステムのサイバーセキュリティ強化に重要な機会を提供する。ネットワーク内の AI（「ネットワークのための AI」）は、６Ｇネットワークが悪意ある行動に対応するために必要な監視と対応能力を提供し、潜在的な侵害をより早期に検知

[3] Global Coalition on Telecommunications: principles on AI adoption in the telecommunications industry (https://www.gov.uk/government/publications/global-coalition-on-telecommunications-principles-on-ai-adoption-in-the-telecommunications-industry/global-coalition-on-telecommunications-principles-on-ai-adoption-in-the-telecommunications-industry).

し、効率的な是正措置を支援できる。これにより、現行の「異常検知」システムを改善する。デジタルツインなどの隣接する技術の発展も、将来的に AI セキュリティツールの機能強化を支える可能性がある。

同時に、AI システムとプロセス（外部でホストされているものを含む）は、AI ライフサイクル全体に強固なセキュリティを組み込んで設計・展開されなければならない。これには、トレーニングデータの品質と出所の検証が含まれる。また、ネットワーク内のセキュリティインシデントへの対応が監督され適切であることを保証しなければならない。適切なセキュリティ要件がなければ、ネットワークにおける AI の活用が、トレーニングデータセットの汚染やバックドア攻撃といった新たな脅威ベクトルや攻撃に対する脆弱性を増大させる可能性がある。これは、各国における関連する業界主導又は研究主導の取組を参照することが可能である。

６Ｇシステムへのエージェント型 AI の統合は、将来のネットワークにおける重要な特徴となる見込みである。これらのエージェントがネットワーク全体でどのように動作し、相互に、また既存のネットワーク機能とどのように連携するか、どのように管理され、ネットワーク情報で更新され続けるかは、依然として議論の的である。エージェント型システムは、顧客への高度なネットワーク性能と個別化されたサービス提供においてネットワーク事業者に大きな利点をもたらす可能性があり、ネットワーク内で記録された異常行動の検知・解決においても有用なツールとなり得る。同時に、エージェントシステムは堅牢な脅威モデリングと分析に基づいて設計され、強固な制御・認証・保証メカニズムと併せてシステムに統合されることが極めて重要である。

AI システムやエージェントが自律的に実行できる行動に対して、どのような制約が適切か、また、AI サービスが失敗した場合の安全な復旧メカニズムについて、検討しなければならない。第３．１節及び第３．２節で概説したセキュリティメカニズムもここには同様に適用される。これは、エージェント認証と認可が業界標準の実践に基づいていること、それらの間の通信が適切に保護されていること、そして重要国家インフラに組み込むに値する十分な堅牢性を備えていることを保証しなければならず、3GPP や IETF といった標準化団体間の効果的な連携を必要とする。

技術そのものを超えて、AI エージェントの導入においては、訓練、導入、監督、更新における人的ミスから生じる潜在的なリスクを適切に考慮しなければならない。同時に、その機能を遂行するために十分なネットワークデータへのアクセスを可能にしておく必要がある。また、AI エージェントが処理するタスクに対する明確な責任の所在を決定することにも課題がある。

一般的に、「ネットワークのための AI」機能の有効化においても注意が必要である。例えば、潜在的なネットワークリソースを活用してサードパーティの計算タスクやモデルトレーニングを完了させる場合などが該当する。６Ｇシステム内でサードパ

ーティの AI サービスによって、又はそのために使用されるデータの完全性は、第３．２節で定められた要件に沿って、常に維持され検証されなければならない。

３．４．　量子の安全

> 我々は６Ｇが、米国国立標準技術研究所（NIST）によって標準化されたものなど、広く受け入れられている量子安全暗号アルゴリズム／技術に基づき、導入当初から量子安全暗号をサポートすることを期待する。これは適切な標準化プロセスを通じて、強力な国際協力のもとで実施されるべきである。

暗号は移動通信ネットワークのセキュリティを支える極めて重要な基盤であり、機微なデータの機密性と完全性を確保するとともに、不正アクセスを防止するための強固な認証機構を支えている。各世代の移動通信においては、計算能力の向上や新たに発見された効率的な攻撃手法を踏まえ、使用される暗号アルゴリズムが再検討され、更新されてきた。しかし、多くの場合、既存アルゴリズムの根本的な構造を変更することなく、パラメータ（例えば最小鍵長）の更新のみにより対応することが可能であった。現在使用されている公開鍵暗号（PKC）の多くは、依然として1970年代の創設以来その中核を成してきた整数因数分解や離散対数計算といった数学的困難性に依拠している。

量子コンピューティングの登場は、暗号分野における大きな転換点を示すものであり、量子力学の特性を利用して従来型コンピュータとは根本的に異なる方法で計算を行うことを可能とする。理論的には、暗号的に関連性を有する量子コンピュータ（CRQC：Cryptographically Relevant Quantum Computer）と呼ばれる大規模な汎用量子コンピュータは、現代の公開鍵暗号（PKC）の基盤となっている多くの数学的問題を効率的に解き、既存の暗号アルゴリズムのセキュリティを損なう可能性が示されている。現時点において、既存の量子コンピュータは PKC アルゴリズムを脅かすほど高度には至っていないものの、６Ｇシステムの導入にあたっては量子安全暗号アルゴリズム／技術への移行が予想される時間軸を慎重に考慮すべきである[4]。さらに、収穫後解読型の脅威も存在する。これは、悪意のある行為者が暗号化されたデータを保存し、十分な性能を持つ量子コンピュータが利用可能になった時点で復号する手法である。これにより、量子攻撃に対して理論的に脆弱なアルゴリズムで暗号化された機密データが、現在送信されている時点で危険に晒される。したがって、より広範な基盤技術（例えば、IETF の関連インターネットプロトコルなど）が十分に迅速に開発・提供される場合、６Ｇは導入当初から量子耐性暗号をサポートする

[4] UK NCSC Timelines for migration to post-quantum cryptography (https://www.ncsc.gov.uk/guidance/pqc-migration-timelines).

と予想される。ただし、移行期限は各国によって異なる可能性がある。やむを得ない遅延が生じる場合、６Ｇシステムはそれに伴うリスクを管理するための適切な対策を講じるべきである。

この移行の一環として、新たに提案される量子安全暗号は、６Ｇシステムにとって重要であるため、研究コミュニティによる適切な精査に付されることが極めて重要である。例えば、NIST が自身の最初のポスト量子暗号アルゴリズムを策定する過程においては、提案アルゴリズムが８年間にわたり複数回の審査を経た後に初の標準が公表された[5]。提案されるあらゆる解決策は、特に重要通信などの分野において、その実現可能性とネットワーク性能に対する信頼性を確保するため、厳密に検証されなければならない。

より高い暗号的俊敏性のサポートを含む、新たなアルゴリズム／技術への移行は、適切な標準化プロセスを通じて進められるべきである。これにはIETF、3GPP、O-RANアライアンスなど幅広い標準化団体が関与し、暗号化方式、関連する暗号プリミティブ、プロトコル、鍵管理手法に関する現行の推奨事項を見直すことになる。

適切な量子安全な暗号アルゴリズム／技術が開発され広く受け入れられた場合、従来の非対称暗号は体系的に特定され、段階的に廃止されなければならない。新規アルゴリズムの導入は、全ての関連するネットワーク機能や要素に対して、暗号部品表（CBOM）又は暗号在庫リストを通じて包括的に追跡されるべきである。これは共有されたベストプラクティスによって支えられるべきであり、国際協力が不可欠となる。

４　強靭性に関する原則

６Ｇは、設計段階から強靭性を組み込み、障害発生時においても、公共安全、重要インフラ、消費者向けサービスの継続性を確保できるように構築されなければならない。そのためには、単なる保護にとどまらず、知的な適応や迅速な復旧を含める必要がある。これらの機能を有効にするためには、国際的に標準化された定量的指標を通じて検証し、各国・各地域において推進可能な信頼性ある性能基準を確立することが不可欠である。

世界経済がモバイルネットワークの途切れない運用に一層依存する中で、サービス途絶の影響は格段に深刻化している。将来の６Ｇシステムは、サイバー攻撃からの防御を超えて、根本から強靭性を備えて設計されなければならない。強靭性とは多

[5] US NIST Post-Quantum Cryptography project (https://csrc.nist.gov/projects/post-quantum-cryptography).

面的な能力であり、ネットワークインフラを被害から保護するのみならず、状況変化に知的に適応する力（多くの場合 AI の活用を伴う）、そして自然災害や人為的障害（AI 関連を含む）の後に遅滞なく復旧する力を包含する。これには、停電などの重要な支援サービスへの支障が含まれる。真に強靭なネットワークとは、障害を予測し、耐え、迅速に復旧できるものである。これにより、公共安全、重要インフラ、緊急通報などの不可欠な行政サービス、産業、消費者に対するサービスの継続性が確保される。

この実現のためには、強靭性を基礎的原則として扱い、標準化の初期段階から運用試験に至るまでシステムライフサイクル全体に「レジリエンス・バイ・デザイン（設計段階からの強靭性）」を組み込むことが不可欠である。GCOT パートナーは、この取組を、抽象的な理念にとどまる強靭性を、国際標準に支えられた達成可能な工学的目標へと具体化するものと位置付けている。そのためには、定量的に測定する手法を開発し、「完全復旧までの時間」や「特定の脅威シナリオ下でのサービス可用性」といった標準化された指標を確立することが必要である。これにより、関係者はシステムの堅牢性を評価・検証し、各国・各地域における説明責任を確保するとともに、国家政策や規制要件の策定に資することができる。強靭性を定量化することは、厳しい環境下でも最低限のサービス水準を維持するための第一歩である。これには、異なる故障モードが互いにどのように関連しているかを考慮し、復旧を著しく妨げる連鎖故障を回避するためのシステムを設計・導入することが含まれる。これらの強靭性の能力は、英国通信庁（Ofcom）の「通信事業者向けネットワークサービス強靭性ガイドライン」[6]や米国連邦通信委員会（FCC）の「強制災害対応イニシアチブ」[7]といった国家レベルの指針を必要に応じて参照しつつ、各国の要件に基づき国内レベルで構築・管理される。

強靭な設計の重要な運用成果の一つは、安全なフェイルオーバー能力である。これは、危機時に重要サービスの継続性を維持するための知的なプロセスであり、第４.１節で論じる。これは、ネットワーク内部における通信の動的優先付けや、必要に応じて衛星などの代替アクセスネットワークや代替キャリアへの円滑な切替えを含む。GCOT パートナーは、第４.２節で論じるように、この重要な能力が、妥協なき強靭なタイミングや同期など、絶対的な技術的安定性の基盤の上に築かれなければならないことを強調する。適用可能な場合、６Ｇシステムの信頼性を最適化し、必要時に安全なフェイルオーバーを迅速化するためには、強靭性のある AI を活用すべきであり、これは第４.３節で論じる。

---

[6] UK Ofcom Network and Service Resilience Guidance for Communications Providers (https://www.ofcom.org.uk/internet-based-services/network-security/resilience-guidance).

[7] U.S. Federal Communications Commission (https://www.fcc.gov/wireless-network-resiliency-during-disasters).

さらに、システム全体は強固かつ安全な産業基盤によって支えられる必要がある。したがって、多様で安全かつ強靭性のあるサプライチェーンを育成することは、長期的な脆弱性を低減する戦略において極めて重要である。これには、５Ｇオープン RAN の強固な基盤を活かし、６Ｇがオープンで相互運用可能であることを確保し、マルチベンダーRAN をサポートすることが含まれる。これは第４.４節で論じる。しかし、より広範な６Ｇサプライチェーンにおける強靭性も考慮すべきである。これには、非地上系ネットワークなど、新技術を６Ｇシステムに統合することで生じる新たなサプライチェーンも含まれる。

これらの基盤的、構造的、運用的な層に一体的に対処することで、このアプローチは、悪条件下においても社会・経済・政府の重要サービスの継続性を維持するよう設計された６Ｇネットワークを提供することを目指す。

４.１.　安全なフェイルオーバー

> ６Ｇシステムは、障害を自律的に検知し、容量の許す範囲で、利用者の有効な接続性を維持するために代替アクセスネットワーク（他の通信モードやキャリアを含む）を通じてトラフィックを迂回させる機能を備えるべきである。また、その際には重要度に応じてトラフィックを動的に優先付けることが求められる。

ネットワーク機器に対する障害リスクは、基地局自体だけでなく、光ファイバーバックホールや電源供給などの支援インフラの損傷、ネットワーク運用における人的ミス、ソフトウェア更新の問題も含まれる。自然災害のような事態においては、地上移動体インフラを迅速に復旧させることが困難な場合があり、その結果、通常の利用者サービスの中断が長期化するとともに、緊急対応活動にも支障を及ぼす可能性がある。したがって、特に地上インフラへの依存度が低い、代替アクセスネットワークと他キャリアが運営するネットワークの統合は、将来の移動通信ネットワークの強靭性を強化する上で重要な鍵となる。

その際、ネットワークは必要に応じて、これら代替アクセスネットワークに迅速かつ安全にフェイルオーバーする能力を備え、利用者のダウンタイムを最小限に抑えることが求められる。これには、割り当てられた重要度水準に基づいてトラフィックを動的に優先付ける仕組み、容量が大幅に低下した際にも重要な通信を維持する仕組み、単一障害点をエンドツーエンドで管理する仕組みが含まれるべきである。緊急通報の場合、これらの代替アクセスネットワークは着信ローミング要件も満たさなければならない。さらに、過負荷を避けるため代替ネットワーク間で負荷を分散する仕組みと、こうした状況下でユーザー端末が偽基地局に自動接続するのを防ぐ堅牢なセキュリティ対策も必要である。

４．２．　強靭性のある位置、ナビゲーション、タイミング

> ６Ｇシステムは、GNSS 信号受信が妨害された場合にネットワークへの影響を軽減するため、補完的かつ拡張的な非 GNSS 位置、ナビゲーション及びタイミング（PNT）システムを導入すべきである。

現行の移動通信ネットワークは、正確なタイミング及び同期のために、GPS をはじめとする従来型の全地球航法衛星システム（GNSS）に大きく依存している。しかし、これらのシステムは妨害（ジャミング）やなりすまし（スプーフィング）に脆弱である。このような障害のリスクは、６Ｇでは、例えば、産業プロセスにおける協働ロボットのようなアプリケーションや、ネットワークセキュリティプロトコルにおけるタイミングと同期の要件などにおいて、一層厳格化されるタイミング及び位置精度（及びジッタなど）が求められる可能性があるため、こうした混乱のリスクはさらに増大する。６Ｇシステムのタイミング同期要件を適切に定義し、理解することが重要である。

将来の移動通信ネットワークにおいて、GNSS の故障時に代替となる高精度時刻システムの冗長性を追加せずに、現行の GNSS 機能のみに依存することは、重大な強靭性リスクをもたらす。６Ｇ仕様の策定においては、代替的な位置・航法・時刻（PNT）供給源と、ネットワーク全体での PNT 情報配信メカニズムを検討すべきである。これには、低軌道衛星（LEO）などの代替衛星源や地上系技術によるものも含まれる。また、GNSS 障害発生時に異なる時刻配信メカニズムを同期させるため、UTC（協定世界時）へのトレーサビリティも考慮すべきである。

４．３．　強靭性のための AI 及び強靭な AI

> ６Ｇシステムは、自然災害等の障害発生時にシステムの可用性を維持し、重要サービスを知的に優先付けるために AI を活用する方法を探求すべきである。６Ｇシステムにおけるこのような AI の導入は、時間の経過に伴っても効果的に機能し続けるよう設計されるべきであり、そのためには、６Ｇシステムのライフサイクル全体にわたり、AI モデルを試験・検証・修正するための明確かつ強固なプロセスを確立することが必要である。

AI は自然災害やシステム障害を含む多様な脅威に対する強靭性を高め、さまざまな状況下での継続的な運用と迅速な復旧を可能にするために活用できる。例えば、AI

は重要なサービス向けにネットワークリソースの優先順位付けをより動的かつ知的に行うことを可能にする。これには、利用可能な異なるアクセスネットワーク間でリソースを調整することも含まれる。例えば、第４．１節で論じた安全なフェイルオーバーの支援などである。

同時に、これらの AI システム自体も、障害に耐え、復旧し、継続的に運用できる能力を備え、過度な依存を回避しなければならない。AI はネットワークに統合されるべきであり、その方法は、AI システムが故障し始めた場合にネットワーク機能への混乱を制御し、AI システムの障害が修正された際に円滑な復旧を可能にするものであるべきである。強靭性を確保するためには、AI モデルに内在する概念ドリフトやデータドリフトの問題に対処することが必要である。これにより、時間の経過とともに正確性と有効性を確保し、AI システムが訓練データの誤りに頑健であることが保証される。

そのためには、信頼できる情報源からの AI モデルの導入、定期的なセキュリティ監査、導入前・導入中・導入後を通じた AI モデルの試験・検証・確認が必要である。さらに、複数のネットワークや事業者に影響を及ぼす電気通信 AI システムにおけるセキュリティインシデントや脆弱性に関する情報を、可能な限り共有することも重要である。加えて、通信事業者は、ネットワーク内の AI システムによる障害や過度の是正措置に起因する強靭性上の課題を十分に認識し、ネットワーク管理において常に人間による介入が可能となるよう確保しなければならない。[8]

[8] これは、各国における関連する産業及び研究の取組を再び参照することができる。

４．４． オープン性と相互運用性

６Ｇシステムは、オープン RAN アーキテクチャと原則を実現し、オープンかつ標準化されたインターフェースを通じて、初期段階からマルチベンダーによる６Ｇ RAN をサポートすることを保証すべきである。さらに、６Ｇの開発及び導入においては、コアネットワークや仮想化ネットワーク機能など、追加的なサプライチェーン集中化の懸念が特定された場合、その緩和策（さらなる分解や追加のオープンインターフェースを含む）を検討すべきである。これらはすべて、以下の原則に準拠する必要がある。

- **オープンな分離**（open disaggregation）： 異なるベンダーからのモジュール式で柔軟なネットワーク構成要素を可能とすること。
- **標準準拠**（standards-based compliance）： 異なるベンダー間の互換性及び相互運用性を確保すること。
- **相互運用性の実証**（demonstrated interoperability）：ネットワークの性能及び機能を検証すること。
- **実装中立性**（implementation neutrality）： ベンダーロックインを回避し、革新と多様性を促進すること。

第３節で述べたとおり、本世代の移動通信は、ネットワーク機能の分離が進展しており、大規模な機能をより小さな個別モジュールに分割するとともに、ソフトウェアを基盤ハードウェアから切り離す動きがみられる。オープン RAN は、O-RAN アライアンスの取組（3GPP 仕様を基盤とする）を通じて、RAN 構成要素間にオープンかつ標準化されたインターフェースを定義し、複数の異なるベンダーの RAN 構成をより容易に統合することが可能となった。

従来の単一ベンダーによる RAN モデルと異なり、ネットワークの個別構成要素や特定のネットワークサービスを異なるベンダーが供給できるようにすることは、市場参入の障壁を低減し、移動体通信事業者（MNO）がネットワーク機器とサービスを調達する際の供給多様性を高めるものである。これは、世界的なサプライチェーンの混乱によって生じ得る強靱性上のリスクを低減するうえで重要な一歩であり、必要に応じて MNO が代替供給者へ移行する際のコストや困難を軽減することにつながる。さらに、モバイルネットワーク内における供給者の多様性が高まることで、特定機器に内在するシステム的課題、例えばソフトウェアの不具合、悪意のあるサイバー活動、その他の供給障害を緩和することが可能となる。

ネットワーク内部においても、分離は個別構成要素の単純化を促し、その重要度や相互依存性を（完全に排除はしないが）低減させる傾向があり、時間の経過ととも

に強靭性を高めることが期待される。さらに、明確に定義されたインターフェースは、ネットワーク動作の可視性と監視を向上させ、異常動作の検出と調査を容易にするとともに、セキュリティ試験ツールの開発を一層容易にする。しかし、よりオープンで相互運用性の高いアーキテクチャは、攻撃対象領域を拡大し、悪意のある攻撃者にとって新たな侵入経路を生み出す可能性もあり、この点は適切に対処されなければならない。我々は既にここで前向きな進展を確認しており、オープン RAN セキュリティの開発においては、堅牢な脅威モデリングに基づき、NIST のゼロトラストアーキテクチャ [9]と CISA のゼロトラスト成熟度モデル [10]の原則に沿った、セキュリティが重視されている。これは、第３．１節及び第３．２節に沿って、内部及び外部の脅威の両方に対する防御のための強固な基盤を提供する。

５Ｇにおいては世代の中途で登場したこともあり、3GPP 仕様の公表と、それに対応するオープン RAN 仕様の策定との間には常に遅延が存在してきた。しかし、６Ｇにはリスクがあり、もしこのような遅延が続き、６ＧオープンRAN 仕様が 3GPP の対応する初期６Ｇ仕様より大幅に遅れて公開される場合、市場に最初に投入される６Ｇ機器は真のマルチベンダー相互運用性を十分に実現できないだろう。これによりベンダーは単一ベンダーRAN へ回帰する可能性があり、５Ｇ時代において達成されたマルチベンダーRAN への進展の大半が失われることになる。

６Ｇにおいて導入の初期段階からマルチベンダーの相互運用性を実現するには、3GPP と O-RAN アライアンスの緊密な連携が不可欠である。これは組織レベルだけでなく、両組織の代表者間の実務レベルでも同様である。GCOT の「オープン RAN に関する認証原則」[11]で示されているように、堅牢な相互運用性試験と認証もこのアプローチの重要な要素となるべきである。これに加えて、６Ｇの開発及び導入においては、既存又は新興のサプライチェーン集中化懸念に対処するため、ネットワークの他の領域における緩和策（さらなる分散化を含む）を検討すべきである。これには仮想化ネットワーク機能をホストするプラットフォームやインフラへの新たな依存関係又はモバイルネットワークコアのさらなる分散化が含まれる可能性がある。

---

[9] NIST SP 800-207, Zero Trust Architecture (ZTA) (https://csrc.nist.gov/pubs/sp/800/207/final).
[10] CISA Zero Trust Maturity Model (ZTMM) (https://www.cisa.gov/zero-trust-maturity-model) .
[11] Global Coalition on Telecommunications: Open RAN certification principles (https://www.gov.uk/government/publications/global-coalition-on-telecommunications-open-ran-certification-principles/global-coalition-on-telecommunications-open-ran-certification-principles).