

## 電気通信産業における AI の導入に関する原則【仮訳】

電気通信産業における人工知能 (AI) の導入に関する英国、オーストラリア、カナダ、日本、米国の共同声明。

英国、オーストラリア、カナダ、日本、米国は、電気通信に関するグローバル連合 (GCOT)<sup>1</sup>を通じて、全ての所管領域においてセキュリティ、成長、社会的利益を実現する方法で電気通信技術のイノベーションを支援するために協力している。

GCOT パートナーは、電気通信における AI の利用がイノベーションのための重要な機会であることを認識している。これらの機会には、ネットワークのパフォーマンスと効率の向上、セキュリティの強化、顧客満足度の向上、更には新たなアプリケーションと収益の機会が含まれる。同時に、GCOT パートナーは、AI が、安全・安心・信頼できる方法で導入され、個人の権利が保護され、知的財産権が尊重されるように取り組んでいる。この共同声明は、電気通信事業における AI の責任ある利用の原則を定めたものであり、産業界のリーダー、研究者、電気通信向け AI ソリューションを開発する人々を対象としている。GCOT パートナーは、これらの原則に沿って電気通信における AI を前進させるための産業界と学界のさらなる取組を歓迎する。

### 背景

2000 年代半ば以降、電気通信企業は AI 技術とその前身を導入し、運用の様々な側面に展開して、ネットワークの設計から顧客満足度の最適化まで、パフォーマンスを向上させ、コストを削減してきた。今後 10 年間及びその先まで、Future Networks が開発されるにつれ、電気通信ネットワークが、AI とデータ インフラが既存の非 AI ベースのエンティティへのアドオンではなく、全てのコンポーネントにわたって完全に統合された「AI ネイティブ」になるため、AI の役割は大幅に拡大することが期待される。

公衆及び民間の電気通信ネットワーク全体における AI の統合は、ネットワークの複雑性及びサービス提供の管理、リソース配分の最適化を支援する。この改善の 1 つの要素はエッジ推論であり、AI がデータをローカルで処理し、リアルタイムの意思決定を可能にし、遅延を減らす。これらの進展は、より高速で信頼性が高くセキュアな接続を提供することで産業界をサポートし、経済成長を促進し、デジタルインクルージョンを促進し、インフラの強靱性を高めることを可能にする。同時に、高度な AI システムの電気通信ネットワークへの導入は、安全性、セキュリティ、プライバシーに対処する必要がある。AI の導入は、ネットワークセキュリティと潜在的

---

<sup>1</sup><https://www.gov.uk/government/publications/global-coalition-on-telecommunications-joint-statement-of-intent-between-uk-australia-canada-japan-and-us/global-coalition-on-telecommunications-joint-statement-of-intent>

な攻撃の複雑性を高め、新たなリスクを引き起こしたり、既存のリスクを潜在的に深刻化させたりする。これらのリスクにより、実装される AI システムの整合性、機密性、アクセシビリティの管理が必要となる。

リスクを軽減しながら特定された利益を実現するために、GCOT パートナーは、電気通信事業者が自社の業務に AI 技術を安全・安心・信頼できる形で統合するための適切な措置を講じる必要があるという見解を共有している。これは、必要に応じて我々の国内規制機関と協力し、コンプライアンスと責任ある実装を確保することを含む。

近年、技術としての AI の安全で責任ある開発を確保することを目的として国際的な取組がいくつか行われている。2019 年に採択され 2024 年に改訂された OECD の AI 原則<sup>2</sup>は、包摂性、透明性、堅牢性、説明責任を強調し、AI ガバナンスの世界的な枠組みを確立する上で極めて重要であった。それ以来、高度な AI システムを開発する組織向けの広島プロセス国際指針及び行動規範<sup>3</sup>に関する G7 首脳のコミットメント、ブレッチリー宣言<sup>4</sup>、ソウル宣言<sup>5</sup>は、リスク管理、国際協力、安全性、プライバシー、説明責任を重視しながら、高度な AI システムに焦点を当て、これらのシステムがもたらす特定の課題に対処してきた。英国の国立サイバーセキュリティセンターも、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）及びオーストラリア、カナダ、日本を含む 17 か国の機関と共同で作成したセキュアな AI システム開発のためのガイドライン<sup>6</sup>を公開している。

同時に、電気通信における AI の導入に関して、産業界では多くの取組が行われてきた。ETSI の人工知能のセキュリティ保護（SAI）<sup>7</sup>に関する技術委員会は、AI モデルのセキュリティ保護に関するガイドラインや、電気通信分野に特化した AI/ML 技術の使用のセキュリティ面に関する継続的な技術レポートなどを含む、セキュリティの脅威を軽減することを目的とした技術仕様の開発に尽力してきた。

次世代モバイル ネットワーク アライアンスは、AI 駆動型自律ネットワークを実装するためのユース ケース、要件、及び構築上の原則に関するガイダンスを提供するガ

---

<sup>2</sup> <https://oecd.ai/en/ai-principles>

<sup>3</sup> <https://www.soumu.go.jp/hiroshimaaiprocess/en/index.html>

<sup>4</sup> <https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023>

<sup>5</sup> <https://www.gov.uk/government/publications/seoul-declaration-for-safe-innovative-and-inclusive-ai-ai-seoul-summit-2024/seoul-declaration-for-safe-innovative-and-inclusive-ai-by-participants-attending-the-leaders-session-ai-seoul-summit-21-may-2024>

<sup>6</sup> <https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development>

<sup>7</sup> <https://www.etsi.org/committee-activity/activity-report-sai>

イダンス「自動化及び自律システム構築フレームワーク – フェーズ 2」<sup>8</sup>を公開した。グローバル システム フォー モバイル コミュニケーション アソシエーションは、産業界が責任ある AI プラクティスを導入することを支援するよう設計された構造化されたガバナンス フレームワークである「責任ある AI 成熟度ロードマップ」<sup>9</sup>を開始した。

## 原則

これらの原則の目的は、AI システムとツールが業務全体で使用されるため、Future Telecoms 技術の開発と展開に関与する利害関係者を支援することである。

この共同声明は、電気通信における AI の導入に関する我々の共通の取組を調整し手引きする原則を定めるものであり、AI がもたらす機会をどのように捉え同時に危害やセキュリティリスクをどのように軽減するかを明らかにするものである。その目的は、これらの考慮と、電気通信事業に AI システムとプロセスを導入する際に発生するトレードオフの評価の重要性を強調することである。通信における利用のために AI を展開し、開発する者は、これらの原則が適用されるユースケースと運用を検討する必要がある。

### 1. イノベーションと競争

電気通信における AI システムは、知的財産権を尊重しながら、イノベーションを推進し、競争力のある革新的な電気通信市場を促進するために活用されるべきである。

イノベーションと競争を促進することは、ダイナミックな市場をサポートし、産業界が直面する商業上の課題に対処する技術の進歩にとって極めて重要である。電気通信におけるイノベーションとは、ネットワーク パフォーマンスの最適化、セキュリティの強化、様々なプラットフォームにわたるリソース管理の自動化、柔軟性と拡張性の促進を意味する。AI 主導のソリューションは、パフォーマンスを犠牲にすることなくスケールアップできるほど柔軟である必要があり、AI が小規模なローカル ネットワークと様々な種類の大規模なグローバル電気通信インフラ、特に、IoT デバイス、機械、自律システムなどのデバイスが飛躍的にスケールアップする 5G 及び将来世代ネットワークの両方を管理できるようにする。フェデレーテッド ラーニングなどの協調学習は、中小企業が直接データを共有することを避けデータのプラ

---

<sup>8</sup> <https://www.ngmn.org/publications/automation-autonomous-framework-phase-2.html>

<sup>9</sup> <https://www.gsma.com/solutions-and-impact/connectivity-for-good/external-affairs/responsible-ai/>

イバシーを維持しながら AI モデルを訓練することを可能にする。競争は、複数のプレーヤーによる多様な市場を確保し、消費者にとってより良いサービスと価格をもたらす、少数のサプライヤーへの依存を減らす。GCOT パートナーは、イノベーションを推進し、相互運用性を促進し、知的財産権を尊重し、電気通信サプライチェーン内での新規市場参入者の拡大を支援する、インフラ、データへのアクセス、スキル、研究開発への投資を奨励する。電気通信ネットワークにおいて使用される AI システムに適用される規制方策は、非差別的なものであり、かつ、正当な目的を達成するために必要である以上に貿易制限的でないものであるべきである。

## 2. 透明性、説明可能性、人間による監視

電気通信における AI システムは、透明性と説明可能性をタイムリーに優先し、明確な開示と理解しやすい意思決定プロセスを確保して、信頼と説明責任を構築する必要がある。

電気通信における AI システムが意味のある透明性と説明可能性を優先することは、特に電気通信がトラフィック管理、リソース配分、セキュリティ対応などの重要な機能を扱う役割を担っているため、信頼、説明責任、及び救済手段を構築する上で極めて重要である。透明性には、AI の利用を開示し、AI 主導の意思決定とトレーニング データの系統に関する明確な情報を提供することが含まれる。これは、エンドユーザー、ネットワーク事業者、知的財産所有者、規制当局、その他正当な利益を持つ組織を含む、様々な利害関係者にとって価値がある。例えば、顧客が課金に関する質問に答えるために AI システムとやり取りする場合、顧客は AI システムとやり取りをしていることを認識し、AI システムが決定を下す方法を理解し、間違いが発生した場合に救済手段を確保する。透明性は、電気通信サプライチェーン全体にわたり優先され、AI システムの提供者が、そのシステムの開発者、作成方法、トレーニングとテストデータのソース、従ったベストプラクティスと標準について、明確な情報を提供することを確保するべきである。

重要なプラクティスは、堅牢なガバナンス構造を確立し、AI ライフサイクル全体にわたって利害関係者を関与させ、定期的な監査、第三者機関のツール、バリューチェーンにわたる情報共有、明確な文書化、独立した評価を促進し、組織が悪影響を引き起こしたり、悪影響の一因となったりした場合に、シンプルで効果的なメカニズムを通じて影響を受けた個人に対し救済(public redress)を提供することを含む。

説明可能性とは、利害関係者が AI システムの意思決定プロセスにアクセスし、解釈し、理解できる範囲を指す。例えば、システムがネットワークトラフィックを再ルー

ティングして輻輳を防止したり、帯域幅を割り当てて特定のサービスを優先したりする場合、意思決定を理解し、結果に異議を唱えることができる。

もう一つの重要な考慮事項は、AI システムが、大規模な影響を及ぼす重要な機能や決定に対して、人間による監視と介入を維持するようにすることである。これは、人間が AI の決定に介入したり、上書きしたりできるよう、リアルタイムの自動回復と自己修復のサポートと、「キルスイッチ」シナリオを含む、フェイルオーバーメカニズムとのバランスをとることを意味する。これにより、人間の専門知識が自律システムに対して意味のある制御を維持することができ、これらの機能のワークフローと実行に影響を与える代替的決定をガイドしたり下したりすることができる。

### 3. プライバシー

電気通信における AI システムの使用は、プライバシーを守り、ユーザーデータを保護し、個人の権利を保護する必要がある。

AI システムにおけるユーザーのプライバシーの確保は、電気通信産業が個人の権利を守り、第三者とデータを使用したり共有したりする際にプロバイダーの資産を保護し、規制遵守と法的義務を維持するために不可欠である。プライバシーには、データ収集についてユーザーに通知し、ユーザーデータを保護し、特に共同センシングや通信ストランドなどの高度な機能を活用している AI システムが、個人情報処理する必要がある場合には責任を持って処理することを保証する堅牢で適切なガバナンス対策が含まれる。具体的には、これは、プライバシー保護技術を使用し、データの最小化や継続的な監視及び監査プロセスを含む堅牢なデータガバナンスと管理方法を実装することを意味する。これはまた、保護を可能にし、AI システムが進化する規範的及び法的プライバシー要件に準拠することを保証する継続的な改善プラクティスを導入することも意味する。

### 4. 公平性

電気通信における AI システムの使用は公平性を維持し、公平な結果を得るために不要なバイアスを最小限に抑えるよう努めるべきである。

電気通信では、公平性により、AI システムが多様なユーザーグループの特定のニーズに対応し、様々な経済状況や地理的な場所にわたる格差を緩和し、包摂性を促進することが保証される。公平性には、AI システムのバイアスを特定して緩和するガバナンス対策を実施し、全ての個人とグループが公正に扱われるようにすることが含まれる。具体的には、これには、公正で公平な結果を構成するものを定義するために幅広い利害関係者と連携すること、リリース前とリリース後の監査を実施する

こと、多様で代表的なデータセットを使用すること、意思決定プロセスの透明性を確保することが含まれる。これには、AI システムの開発者と電気通信分野においてそれを展開する者との間の効率的な透明性の開示が含まれる。これは、AI システムの作成に使用されたトレーニングデータの出所、AI システムのテスト方法、バイアスの緩和の有無・方法、当該システムの範囲に関する情報を含む。この情報共有により、電気通信事業者が業務における信頼と包摂性を育むことに完全に貢献することができる。

## 5. セキュリティと強靱性

電気通信におけるAI システムは、サイバー脅威から保護し、データの完全性を確保し、運用の安定性を維持するように設計される必要がある。

AI 駆動型システムはトラフィックパターンを監視し、潜在的なセキュリティ リスクを示す異常を検出できるため、侵害への対応が迅速になる。AI はまた自然災害やシステム障害などの様々な危険に対する強靱性を高めるために活用することができ、様々なシナリオで継続的な運用と迅速な復旧を保証する。同時に、私たちは AI システムとプロセスが、デザイン上及びデフォルトでセキュリティが組み込まれた状態で展開されるようにしなければならない。AI システムのセキュリティと強靱性の要件は、電気通信事業者がサイバー脅威から保護し、運用の安定性を維持し、事業継続と国家の重要なサービス継続計画のためにサービス提供の中断を最小限に抑えるために不可欠である。セキュリティがなければ、AI の急速な導入と組み込みが続くと、トレーニング データセットの汚染やバックドア攻撃などの敵対的攻撃に対する脆弱性が生じる可能性がある。これらのシステムはまた、継続的な運用を維持し、過度の依存を回避するために、混乱に耐え、そこから回復できなければならない。強靱性には、AI モデルに内在するコンセプトやデータドリフトといった問題に対処し、時間が経過しても正確で効果的な状態を維持できるようにすることも必要である。具体的には、強靱性には、リアルタイムの脅威検知や自動対応システムなど、AI を活用した高度なサイバーセキュリティ対策の導入が必要である。また、信頼できるソースからモデルを導入し、定期的なセキュリティ監査を実施し、導入前、導入中、導入後に採用した AI モデルのテスト、検証、確認を行うことも意味する。また、可能であれば、複数のネットワークや事業者に影響を与える電気通信 AI システムのセキュリティ インシデントや脆弱性に関する情報を共有することも意味する。

最後に、AI は、サイバー犯罪者が電気通信システムやネットワーク上で音声複製詐欺や音声認証の無効化などの不正または悪意のある活動を行うための新しい手段を提供する。電気通信サービス プロバイダーと電気通信事業者は、信頼できる発信者 ID プログラムの実装、AI によって可能になった不正活動の情報や指標の共有、タイ

ムリな対応に関して事業者やセクター間で協力する新しい方法の発見に向けた取組を継続する必要がある。

## 6. 環境持続可能性

電気通信におけるAIシステムは、ネットワークの環境持続可能性を向上させるために使用され、システム自体の環境への影響を最小限に抑えるように設計される必要がある。

電気通信分野におけるAI、特に生成AIの導入は、エネルギー消費と二酸化炭素排出を増加させ、環境上の課題を引き起こす可能性がある。一方、AIと機械学習アルゴリズムは、エネルギー消費を最適化し、ネットワークの設計と運用の効率を改善することで、ネットワークの持続可能性を高めることができる。これを達成するため、電気通信企業は、AIシステムのエネルギー消費及びトレーニングデータソースを含む、開発者からの持続可能性に関する包括的な情報を必要とする。環境への配慮をコストと報酬の決定に組み込むことは、AIの導入が運用効率を高めるだけでなく、企業の持続可能性の目標にも沿ったものになることを保証する。環境持続可能性には、効率の改善、エネルギー消費の削減、再生可能エネルギー源の利用促進によってAIシステムの環境への影響を最小限に抑えることが含まれる。具体的には、これは、よりエネルギー効率の高いAIシステムとプロセスを導入すること、AIの非生産的な利用を制限すること、推論中や活動が少ない時間帯のエネルギー消費を最小限に抑えること、機械学習を使用してデータセンターの運用を最適化すること、そして可能であれば、AIインフラに電力を供給するために低炭素または無炭素エネルギーに投資することを意味する。