資料２－４

中間取りまとめを見据えた論点整理のイメージ（案）

令和８年11月19日

事　　務　　局

中間取りまとめを見据えた論点整理のイメージ（案）

～通信事業者によるサイバー防御の抜本的強化に向けて～

１．通信分野におけるデータ保護を巡る現状認識

※初回会合の構成員コメント等を踏まえ、事務局において たたき台として作成

［構成員の主な意見］

- **通信事業者には、「インフラのインフラ」としてデータ保護・セキュリティ上の強い役割が期待される。**
- 国民利用者のリスクを減らし、通信の役割が適切に果たされるようにするため、**サイバー防御の優先度を高め、規制上の手当てやAIの活用を含めた対策を講じていくことが必要。**
- AIが自律的に行動し、人間による制御が不可能になるフロンティアAI時代の到来により、**攻撃側が防御側よりも圧倒的に有利な「非対称性」に対する危機感を共有し、将来を見据えた議論が必要。基本的な対策に加え、フロンティアAIならではの課題への対応も求められる。**
- AIの普及により、通信事業者が取り扱うトラフィックの性質が大きく変容し、これまでのように**正常と異常を見極めることが困難になることを前提として、技術と制度の両面からの対応を講じていくべき。**
- サイバー攻撃の実態を踏まえれば、**すべての攻撃がフロンティアAIモデルによるものではないことに留意**しつつ、**AI全般の悪用を念頭に置いた検討が必要。**
- Data Free Flow with Trustを推進する上でも信頼の確保が大きな課題。**通信の秘密や特定利用者情報に関する現行制度は一定の役割を果たしてきたが、漏えい自体を未然に防ぐための施策を進める必要がある。**
- 現下の状況に鑑み、**できることから対応していくべきであり、**検討会の成果として、必要に応じて公表や対策を出し実務を支援していくべき。
- 検討会として、**現に起きている問題に対して必要な事項については速やかに意見を取りまとめ、随時、総務省、関係機関、事業者等に対応を促していくべき。**
- **金融分野での先行的な取組が参考になる**ので、得られた知見や経験の共有が重要。

［考え方（案）］

- 社会経済活動において通信事業者が果たす役割が大きいことに鑑み、通信インフラのサイバー防御については、**制度整備やAIの活用を含め、他分野に先駆けた積極的な対応が求められるのではないか。**
- 昨今のサイバーセキュリティをめぐる情勢は深刻度を増しており、新たなステージにあるという認識のもとで対策講じていくことが求められるのではないか。特に、**情勢変化のスピード感を踏まえ、できるところから対応していくという考え方を取るべきではないか。**
- AIの能力向上を念頭に、適切にリスクを把握した上で、AIによって量的に変化したリスクを踏まえた**基本的対策の徹底と、フロンティアAIによって質的に変化したリスクを先取りした対策を分けて、講じていく必要があるのではないか。**

2．フロンティアAI時代において求められる技術面の対策の在り方

［構成員の主な意見］

- AIを用いた攻撃が後を絶たず、**対策へのAI活用は不可欠。脆弱性対応においてAIを用いたセキュリティ対策が広がっていくことが望ましい。**
- **高度なAIを活用できるかどうかが、防御能力を大きく左右する可能性がある。**
- AIは「質より量」のスケーリング則に基づいて開発されてきたものであり、AIが人間以上の脆弱性発見能力を有することは自明であるが、**発見された脆弱性の評価・トリアージは、引き続き人間の価値観により人間が行わなければならない**。 AIの影響を冷静に捉え、変えるべき業務プロセスとそうでないものを分類し、**情報通信基盤の実態とインシデントの影響を勘案し、制度設計の検討を行うべき**。
- 実効性の観点からは、形式的な体制整備を一律に求めるのではなく、**中小事業者への支援・業界でのサポート等も含めた議論が必要。**
- AIの能力向上に伴い、人間がAIを攻撃の道具として利用する場合だけでなく、**AIが自律的に外部システムに働きかけ、人間が気付かないまま想定外の被害を発生させるリスクも考慮する必要がある。**また、AIの成果が高度化し、人間の専門家による理解・検証が困難になる可能性もある。
- AIエージェントや自動化ツールが短期間に大量・高頻度にアクセスを行うことで、通信トラフィックのパターンが大きく変容し、正常・異常の区別が難しくなっている。**攻撃通信を見分けるために通信の観測の対象を広げる必要性が生じている一方で、そのためには通信の秘密の保護との関係も併せて整理しなければならない**。
- **侵入を完全に防ぐことを前提とせず、侵入された後も被害を局所化し、重要なサービスを継続させる設計が必要。**
- 事故防止のためには**単一の対策を完全なものとみなさず、多数の手当てを講じる必要がある。**そして、手当ての内容を検討するには、スイスチーズモデルを念頭に、インシデントを多方向から分析することが重要。
- AIと関係なく、クラウドやスマートデバイスを前提とした情報システムでは、ゼロトラストアーキテクチャが主流となりつつあり、**常に侵入されている可能性を前提に、システム構築と運用ガバナンスの精緻化を進めるべき。**

［考え方（案）］

- **AIが人間以上の脆弱性発見能力を有することを前提に、通信事業者において脆弱性の発見・分析をはじめとするセキュリティ対策にAIを積極的に活用し、事業全体に与えるリスクという観点から適切に評価した上で、具体的な対策につなげていく必要があるのではないか。**
- **脆弱性の評価など人間が行わなければならない対策がある一方、中小事業者には人的・財務的な経営資源に限界があることから、中小事業者に対する支援を検討していくべきではないか。**
- **対策を行う前提として、AIによって変容したトラフィックパターンも踏まえ、自社ネットワークが晒されている脅威をタイムリーに観測する必要があるのではないか。**
- **侵入を完全に防御することは困難であり、常に侵入されている可能性があるという認識のもと**、認証・アクセス制御等を組み合わせた**多層的防御を実装し、ネットワークそのものを堅牢化していく必要があるのではないか。**

3．新たな通信エコシステムを踏まえたガバナンスの対策の在り方

経営課題としてのセキュリティ対策について

［構成員の主な意見］

- データ保護・セキュリティを経営上の重要課題として位置付け、**経営陣がリスクを適切に認識し、人材育成を含む必要な経営資源を配分するとともに、取締役会が経営管理体制やその実効性を監督することが重要**。ガバナンス実効性向上のため、監査役・内部監査部門の監督機能強化と連携も必要。
- 事故の根本要因は、最終的には組織のマネジメントに行き着く。**経営者のガバナンスに加え、安全確保のための予算配分や人材配置など、組織全体としてセキュリティに必要な経営資源を振り向けることが重要**。
- 事業者がサステナブルかつ自律的にセキュリティ対策を向上させ、業界全体として取組を進めるため、**セキュリティに経営資源が振り向けられるような仕組みが重要**。
- 実際にセキュリティ対策を進める上で**企業内に対策の「旗振り役」が存在するか**が重要。
- 実効性の観点からは、形式的な体制整備を一律に求めるのではなく、**中小事業者への支援・業界でのサポート等も含めた議論が必要。**

［考え方（案）］

- 全ての対策の根底には経営ガバナンスの強化があるという認識のもと、データ保護・セキュリティを**経営上の重要課題として位置付け**、**人材・予算等のリソースの確保**や、**実効的なモニタリングの体制の整備を求めるべきではないか**。
- その際、**一律の体制整備を求めるのではなく、事業規模、サービスの重要性、リスクに応じたガバナンスの水準を示す必要があるのではないか**。**また、企業内にセキュリティ対策を進めるための人的・財務的な経営資源が不足する中小事業者に対する支援も併せて議論し、業界全体の対応能力向上につなげていく必要があるのではないか。**

通信エコシステムを踏まえた外部事業者の管理について

［構成員の主な意見］

- サプライチェーンリスクを踏まえ、**委託先となる事業者が講じるべき措置も含めたガバナンスの具体化が必要**。
- **個々の事業者のガバナンスだけではエコシステム全体のリスクを十分管理できない**可能性がある。エコシステム全体を誰が管理し、責任を負うかを整理し、中核的事業者、政府・当局を含め、**各主体の影響力・管理可能性・能力に応じた責任分担を明確化する必要がある**。
- **中小事業者には人的・財務的な経営資源に限界があり、全事業者に一律に高い規律を課すことは必ずしも実効的ではない**。
- **多様な事業者が通信サービスに関与する中でも、利用者に通信役務を提供する通信事業者が安全性・信頼性の確保について第一義的な義務を負うと考えるべき。**通信事業者が直接コントロールできる範囲を見極め、通信事業者が行うべき管理（委託先の選定、契約上の手当て、継続的なモニタリング等）と外部事業者との責任分担について議論する必要がある。
- **外部委託を含む多層的な体制では、直接管理から間接管理へと重心が移ることを踏まえ、責任の所在と観測可能な範囲を整理する必要がある**。
- 外部委託に伴い情報システムの運用やデータ管理に複数の事業者が関与する場合には、**各事業者の役割・責任を明確にし、データの一体的な管理や対策の実施を担保する必要がある**。

［考え方（案）］

- 通信事業が外部事業者が多数関与するエコシステムに移行しているという認識のもと、まずは、**利用者に通信役務を提供する通信事業者が安全性・信頼性の確保について第一義的な責任を負うことを確認する必要があるのではないか。**
- 通信事業者には、再委託先を含むサプライチェーンとデータの流れを把握した上で、**委託先の選定、契約上のセキュリティ要件、継続的なモニタリング、インシデント時の連携を通じた、実効的な委託先管理**を求めるべきではないか。**委託先が中小事業者となる場合には、リソースが限定的である点について考慮が必要ではないか。**
- その際、**通信事業者自らが実施し直接的に管理すべき業務の範囲と、外部事業者に委託し間接的に管理を行うことが可能な業務の範囲を整理したうえで、委託先管理の在り方や責任分界点を明確化する必要があるのではないか**。

4．包括的かつ実効的な対策を可能とする制度の在り方（1／3）

［構成員の主な意見］

- インシデントに対する執行制度は、事業者による事前の対策を促す効果が期待でき、非常に重要性が高い一方で、結果責任を問いかねない面もある。結果ではなく**事故発生に至るプロセスを適切を評価し、前向きな取組を促す姿勢が、執行当局にも必要となってくる**。
- 事故調査の目的は再発防止であり、**発生した事象に対する責任追及とは峻別した調査**を行うことが大前提。
- **中小事業者には人的・財務的な経営資源に限界があり、全事業者に一律に高い規律を課すことは必ずしも実効的ではない。企業規模だけでなく、サービスの重要性、社会的影響、リスクに応じた規律とし**、確保すべき安全性の水準と、そのための組織体制・手段を分けて議論することが必要。**加えて、中小事業者に対する支援、業界としてのサポートも同時に検討することが望ましい**。
- **高度なAIを活用できるかどうかが防御能力を大きく左右する可能性がある一方、全ての通信事業者が最先端のAIや専門人材を確保できるとは限らない**ため、規律によって対策を求めるだけでなく、**AIを活用した脆弱性対策の標準化、ガイドラインの整備、技術・知見の共同利用など、業界全体で協力していく仕組みが必要**。
- **規制だけでなく、事業者の自主的な取組を制度上適切に位置付け、行政がこうした取組を適切に考慮することで、自主的な取組へのインセンティブとし、セキュリティ水準の全体的な向上につなげることが重要。**
- **インフラのインフラである通信事業者には、データ保護・セキュリティの強い役割が期待されるところ、本来期待されながら必ずしも手が及んでいなかった対策にまで事業者が取り組めるよう、インセンティブを含めた制度設計を行い、同時に事業者が経営資源を振り向けられるような仕組みにすることが重要。**
- 新たな制度を検討するに当たっては、電気通信事業法上の技術基準、個人情報保護法、サイバーセキュリティ基本法、会社法上の内部統制等の**既存規律との具体的なギャップを明らかにする必要がある**。その上で、**対象事業者、対象となるリスク、求める管理措置について、事業規模だけでなくサービスの性質やリスクに応じた制度設計を行うことが重要**。
- 通信事業者と外部事業者との関係を検討する際には、実際のセキュリティ上のオペレーションが実効的に作用するように、各当事者が協働できる仕組みを考える必要がある。**その制度的な手掛かりとして、電気通信事業法上の特定利用者情報規律(安全管理措置やガバナンスに関する仕組み)を活用しつつ、今後のさらなるリスクの発展・変化に対応できる仕組みを議論していくべき**。

4．包括的かつ実効的な対策を可能とする制度の在り方（2／3）

［構成員の主な意見］

- 従来から必要とされてきた対策の徹底と、フロンティアAIによる新たな脅威への対応を分けて考える必要があるべきであり、**前者は実効性を高める問題、後者は規律の基準や考え方そのものを見直すという問題である。**そして後者については、脅威の急速な変化により、技術基準が短期間で陳腐化し、基準を満たしても安全とは限らなくなることを踏まえながら、**技術基準や規律の考え方そのものを見直す方向で検討することが必要である**。
- データ保護については個人情報保護法が大きな役割を果たし、経済安全保障推進法でもデータセキュリティに関する制度の検討が始まるなど、データの保護とセキュリティの確保は複数の法制度が担っている。制度の検討に当たっては、**データ保護・セキュリティを担う複数の法制度について、それぞれの目的・制度の違いを踏まえつつ相互に連携させる必要がある**。事業者の負担に配慮するとともに、制度間に隙間が生じないよう留意すべき。
- 通信事業者が保有するデータは、電気通信事業法や個人情報保護法では必ずしもカバーされていないデータも含めて**経済安全保障上の重要性を有し、これらのデータには不正アクセス等の非合法な手段による取得のリスクと合法的な手段によるデータの移転リスクも存在する**。
- **AIに対して過剰反応するのではなく、AIや情報通信基盤の実態、インシデントがサービスや社会に与える影響、インシデントへの対処としてのシステムの制限・一時停止による影響等を把握した上で**、必要な制度設計・法改正を検討すべき。
- **遮断や一時停止は攻撃への有効な手段となる一方、正規の利用者の通信品質にも影響を与える。対策の強さと利用者の通信品質のバランスをどう設計し、その判断を利用者・社会にどう説明するかについて、制度面から丁寧に議論する必要がある。**
- 将来、AIをサイバー防御に活用していくとすれば、**その能力をどこまで海外に依存し、どの分野でソブリン性を維持するのかが問われ、AIによるサイバー防御における日本の戦略的自律性の在り方も隠れた論点となり得る。**

4．包括的かつ実効的な対策を可能とする制度の在り方（３／３）

［考え方（案）］

- 制度を構築するに当たっては、**発生したインシデントに対して事後的に行った原因分析の結果を、当該事業者及び業界全体の前向きな取組に効果的に還元できるような、インシデント対応ライフサイクルを意識した制度の在り方を検討すべきではないか**。
- 事前対策としては、（前記２・３で挙げたような）**脆弱性診断の実施、多層的防御の実装、委託先管理**等の、これまでも有効と考えられてきた対策を着実に実施していくことが考えられるのではないか。事後対策としては、**インシデントが発生した場合の事後的な情報提供・共有の在り方**を整理する必要があるのではないか。
- 包括的かつ実効的な対策を可能とする制度の検討に当たっては、企業規模やサービスの影響等を踏まえた**リスクベースの議論が必要ではないか**。**大規模事業者については対策の実施を制度に基づいて担保し、他方でリソースが限定的な中小規模事業者については対策の実施を可能とするための支援を検討していくべきではないか**。
- **制度の内容として、事業者の自主的な取組を促すことができるような仕組みも検討する必要があるのではないか。**
- **具体的な制度の在り方の議論においては、既存の電気通信事業法上の特定利用者情報規律における安全管理措置や安全・信頼性規律、ガバナンスに関する仕組みを手掛かりとしつつ、既存の規律との具体的なギャップを明らかにし、今後のさらなるリスクの発展・変化に対応できる仕組みを議論していくべきではないか。**
- **サイバー攻撃を受けた場合等におけるサービスの一時停止については、**他の分野での取組も参考としつつ、**被害拡大防止や重要な設備・データの保護に当たっての有効性と国民生活及び社会経済活動への影響を比較衡量し、発動条件や発動範囲、利用者・社会全体への説明等を慎重に検討すべきではないか。**
- 将来的に、通信事業者におけるサイバー防御にAIを活用していく際には、**我が国の戦略的自律性の在り方も念頭に置く必要があるのではないか。**