1.『ICT サイバーセキュリティ政策の中期重点方針』の公表

要約

- 総務省は、所管する通信、放送、自治体、データ流通基盤を対象に『ICT サイバーセキュリティ政策の中期重点方針』を公表した。
- 4 つの重点事項を設定し、サイバーセキュリティ対策を強化する方針。
- 各分野の取り組みに加え、生成 AI の急速な普及、量子コンピュータの進展による新たなサイバーリスクに対して今後の取り組みの方向性が示された。

公表された方針の概要

総務省は 2024 年 7 月 31 日、『ICT サイバーセキュリティ政策の中期重点方針(*1)』を公表しました。本方針は、2030 年頃を見据えたセキュリティ対策について議論し、一般からの意見募集（2024 年 7 月 2 日から同年 7 月 19 日）を経て、17 件の意見を参考にして最終的に決定されました。なお、本方針は総務省の所管する通信、放送、自治体、データ流通基盤についての現状と今後の取り組みの方向性がまとめられています。

サイバーセキュリティを巡る主な課題を 4 点あげ、『経済安全保障推進法』の施行（2024 年 5 月）や『AI 事業者ガイドライン(*2)』の策定（2024 年 4 月）などの政府の動きを背景に中期重点方針が示されています。

サイバーセキュリティを巡る主な課題	説明
厳しさを増す国際情勢とサイバー攻撃リスクの高まり	国際情勢が悪化し、サイバー攻撃のリスクが増大。ロシアのウクライナ侵攻やハマスによるイスラエルに対する攻撃により、国際的な対立が複雑化。重要インフラのサイバーセキュリティ強化と国際協力が急務。
多様化・複雑化するサプライチェーンとアタックサーフェスの増加	グローバルバリューチェーンの拡大により、製品を安く生産する一方で、サイバーリスクも増加。委託先企業の不十分なセキュリティが情報漏洩を引き起こし、複雑化するサプライチェーンに対する適切な対策が必要。
セキュリティ人材の確保	日本企業の約9割、約11万人のセキュリティ人材が不足していると推計。人材は大都市（特に東京圏）に集中している傾向があり、地域に特化した人材育成が急務。
生成AI等の新たな技術への対応	サイバーセキュリティでは新技術への対応が重要。特に生成AIは偽情報やプライバシー侵害のリスクがあり、量子コンピュータの発展も従来の暗号を脅かす。これらに対する適切なセキュリティ対策が求められる。

総務省が中長期的に取り組むべき4つの重点事項

- 重要インフラ等におけるサイバーセキュリティの確保
- サイバー攻撃対処能力の向上と新技術への対応
- 地域をはじめとするサイバーセキュリティの底上げに向けた取組
- 国際連携の更なる推進（国際連携全般、人材育成支援）

出典：総務省『ICTサイバーセキュリティ政策の中期重点方針(*1)』を基に大和総研作成

(*1) 総務省『ICT サイバーセキュリティ政策の中期重点方針』

(*2) 総務省・経済産業省『AI 事業者ガイドライン』

示された今後の取り組みの方向性

重点事項「重要インフラ等におけるサイバーセキュリティの確保」において、以下に、総務省の所管分野の中から、通信とデータ流通基盤に絞り、現状と今後の取り組みを整理しています。

カテゴリ	現状の説明	今後の取り組みの方向性
1. 通信	情報通信ネットワークは国民生活や経済活動に不可欠だが、サイバー攻撃の脅威が高まっている。	IoTボットネット対策や通信サービスのセキュリティ対策、サプライチェーン対策を強化する必要がある。
	IoTボットネット対策 マルウェアに感染したIoT機器がサイバー攻撃に悪用される問題がある。脆弱な機器を減らし、C&Cサーバを見つけて対処する対策を強化する必要がある。	**ネットワークセキュリティ技術** RPKI、DNSSEC、DMARC(*1)などの認証技術があまり導入されていない。これらを導入しやすいガイドラインを作成し、企業の導入状況を見える化して普及を促進する。
	サプライチェーン対策 OSSの利用が増えているため、サプライチェーン全体のセキュリティが重要。SBOM(ソフトウェア部品表)を導入して脆弱性への対応を迅速に進める。	**スマートフォンアプリの対策** **情報漏洩事案への対応** **5Gネットワークのセキュリティ**
2. データ流通基盤	クラウドサービスのセキュリティ対策が重要で、設定ミスによる情報漏えいが多発。	ISMAPの登録促進やトラストサービスの普及を進め、安全なデータ流通基盤を整備する。
	クラウドサービス ガイドラインの普及とISMAP登録を進める。	**トラストサービス** eシールやタイムスタンプの認定制度を整備し、電子データの安全な流通を推進。

出典：総務省『ICTサイバーセキュリティ政策の中期重点方針』を基に大和総研作成

また、重点事項の「サイバー攻撃対処能力の向上と新技術への対応」では、生成 AI の急速な普及、量子コンピュータの進展による新たなサイバーリスクに対して今後の取り組みの方向性を示しています。

- **AI とセキュリティの方向性**

総務省は、生成 AI の急速な普及に伴い、AI 技術に関連するセキュリティリスクを回避・低減するための取り組み(Security for AI)と、AI 技術をセキュリティ対策に効果的に活用すること(AI for Security)の両方に取り組む必要性を示しています。そのために、総務省と経済産業省が策定した『AI 事業者ガイドライン』に基づいた新しいガイドラインを整備し、AI セキュリティ情報の発信の重要性を認識しています。これは、具体的なプロジェクトを通じて AI 活用の効果を示すことの重要性が示唆されています。

- **耐量子計算機暗号(PQC：Post-Quantum Cryptography)(*2)の方向性**

総務省は、量子コンピュータの進化に伴う現代暗号の危殆化リスクへの対処を重要視しています。具体的には、NICT(国立研究開発法人情報通信研究機構)における暗号安全性評価に関する研究開発の取り組みを充実させ、PQC への移行を推進し、暗号技術の安全性評価や監視の強化を進めています。

最後に

テクノロジーの進化により、私たちの利便性が向上する一方で新たなサイバーリスクが発生します。今後のセキュリティ対策では、特に生成 AI が重要な役割を果たします。生成 AI はデータ分析や脅威検出の精度を向上させる一方で、その利用に伴うリスクも考慮しなければなりません。また、PQC は量子コンピュータの進化に対応するための新たな暗号技術として、通信の安全性を確保するために必要不可欠です。これらの技術を適切に導入し、リスクを管理することが、今後のサイバーセキュリティの強化につながります。本方針は総務省の所管分野を対象としていますが、業種や業態に関係なく取り組むべき課題であり、さまざまな業種や業態を横断して連携していくことが求められます。政府のサイバーセキュリティに対する取り組みや考え方がまとまっているため、関心のある方はご一読をお勧めします。

（蓮見　将生）

(*1) RPKI はインターネットのルーティングを安全にする仕組み、DNSSEC はドメイン名の情報を正確に保つための技術、DMARC はメールのなりすましを防ぐためのルールを設定する方法です。

(*2) 大和総研『耐量子計算機暗号とは何か　移行のために知っておきたいこと』