サイバーセキュリティ対策の抜本的強化に関する提言

～サイバー有事前夜／AIのサイバー飽和攻撃に備えよ！～　概要

令和８年１０月２０日　自由民主党政務調査会 国家サイバーセキュリティ戦略本部

はじめに（基本認識と危機感）

・我が国の企業等に対するサイバー攻撃により個人情報の流出事案が急増。国民のプライバシーと財産が著しく脅かされており、不安が広がっている。今後これまでよりも影響の大きな事態が発生することも否定できない「サイバー有事前夜」とも言うべき重大な危機。
・重要インフラ企業に限らず、重要情報を大量保有する企業での対応強化も必要。
・生成AI等の急速な発展と普及に伴い、サイバー攻撃はより自律化・高度化しつつある。
・ゼロトラスト思想への転換、最先端技術の社会実装、平時からの積極的なサイバー防衛網の構築が急務。
・必要な予算確保と体制整備の実施。

政府全体に対する基本提言

官邸主導で「サイバー対処本部（仮称）」を立ち上げ、司令塔として迅速に本部会議を開催。不安の払拭へ。

（１）サイバー対処能力強化法の取組強化

自衛隊・警察の能力構築、官民協議会の活用、通信情報の利用、同盟国連携の加速

（２）経営層の意識改革と開示の充実

経営の最重要課題とし、平時からの体制構築を促す

（３）人材の育成・確保

「トップガン」人材の待遇のため、公務員の新たな人事・給与制度、実践演習を通じた人材の裾野拡大

関係省庁に対する個別提言

● NCO（国家サイバー統括室）

✓能動的サイバー防御の実行体制構築

✓サイバー攻撃情報の集約・分析及びインシデント対応力の強化

✓Project YATA-Shieldの推進（防御側もAI技術活用）

✓米国のAI事業者との連携

✓政府調達における対策強化

✓同盟国・同志国とのインテリジェンス共有

✓指揮権の発動

✓漏洩被害者への安全な連絡方法の確立

✓PQC（耐量子計算機暗号）移行の加速

● 内閣府AI室/AISI

✓産業界の安全なAI実装に向けた指針改訂

✓Project YATA-Shieldの推進

✓米国フロンティアAI事業者等との戦略的連携

● デジタル庁

✓ゼロトラスト思想の徹底とガバメントクラウドの厳格な監査

✓次世代認証基盤（DID/VC）及びマイナンバーカードの活用

✓マイナンバーカードの利用による本人確認の徹底
（マイナンバーカードの取得の義務付けの検討等）

● 経済産業省及び金融庁等

✓上場企業等の開示の充実（サイバーセキュリティに関する重要事項の有価証券報告書への記載の充実）

✓経営ガイドラインの厳格化

✓サプライチェーン防衛への投資支援と「サイバーお助け隊サービス」の拡充

✓サプライチェーン観測網の導入

✓ホワイトハッカーをはじめとするセキュリティ人材の育成と、AIを活用したペネトレーションテストの実現

✓OTシステム特化型サイバーセキュリティAIの開発と秘密計算技術の実装による安全なデータ利活用
（重要データを暗号化したままクラウド上で処理）

✓事業者におけるAIエージェントの安全な利活用に向けたガイドライン作成

✓ベンダーの対応能力、クライアント企業への支援能力の向上

✓信用情報機関への通報のワンストップ化の仕組みの整備の検討

✓金融分野における官民連携、防御力及びレジリエンスの強化

✓IoT製品やセキュリティ事業者のセキュリティ対策状況可視化

● 個人情報保護委員会

✓不正アクセスに関する個人情報保護法の厳格な執行（必要な場合の報告徴収、立入検査、勧告・命令）

✓保有する個人データの最小化　✓罰則の広報啓発　✓漏洩被害者への安全な連絡方法の確立

● 警察庁

✓攻撃者の特定能力の抜本的強化と体制拡充

✓国際共同捜査による犯罪インフラの無害化の主導

✓被害組織が相談しやすい環境整備等
（事業者等との信頼関係の醸成及び協力関係の構築）

✓個人情報漏洩事案における２次被害対策の徹底
（「警察庁推奨アプリ」の活用の周知）

● 総務省

✓通信事業者による対策の強化　✓NICTによる研究開発等の推進（サイバー攻撃手法の分析と周知）

✓機器の踏み台化等の防止　✓地方公共団体による対策と国による支援　✓量子暗号通信（QKD）の社会実装の加速

● 防衛省

✓「能動的サイバー防御（ACD）」を含むサイバー防衛能力の強化

✓重要インフラ等のシステムへの支援も見据えたスレット・ハンティング機能の強化
（自衛隊の任務遂行に不可欠な重要インフラ等システムの防護）

● 厚生労働省

✓医療現場におけるサイバー防衛の標準装備化　✓医療現場における専門人材の活用　✓重要インフラにふさわしい防御力の整備

● 消費者庁

✓消費者への注意喚起

● 国土交通省

✓重要インフラの安定的なサービスの確保

【おわりに】～国民の安全と我が国の産業競争力を死守する責務～

■サイバー空間の優劣は、国力を左右

来るべき「AIのサイバー飽和攻撃」を前に、政府は直ちに必要な予算措置及び法制化の検討に着手し、国民の安全と我が国の産業競争力を死守する責務がある。

■国内通信情報の利用検討を含む強い対応

サイバー対処能力強化法における外国関連通信情報の利用にとどまらず、国内通信情報の利用の検討も求める。

サイバーセキュリティ対策の抜本的強化に関する提言

～サイバー有事前夜／AI のサイバー飽和攻撃に備えよ！～

【国家サイバーセキュリティ戦略本部　提言】

令和 8 年 10 月 20 日
自由民主党政務調査会

１．　はじめに（基本認識と危機感）

昨今、我が国の企業等に対するサイバー攻撃が相次ぎ、おびただしい数の個人情報の流出事案が後を絶たない。これらの事態は、単なる個別企業のガバナンス不全や不祥事にとどまらず、国民のプライバシーと財産を著しく脅かすとともに、今後これまでよりも影響の大きな事態が発生することも否定できない、我が国の経済安全保障及び国家安全保障を根底から揺るがす「サイバー有事前夜」とも言うべき重大な危機である。とりわけ、重要インフラ業種として高度な対応を法的に求められている会社以外で、個人情報をはじめとする重要な情報を大量に保有している企業に広く不正アクセスが行われている実態があり、こうした企業における対応のレベルを上げることも急務となっている。

更に、生成 AI 等の最先端技術の急速な発展と普及に伴い、サイバー攻撃はより自律化・高度化しつつある。また、最近の攻撃は、中国製の AI モデルが使われているという報道もある。近い将来、AI が自動的にシステムの脆弱性を突き、防御側の処理能力を上回る規模で一斉に攻撃を仕掛ける「AI のサイバー飽和攻撃」が現実のものとなる。従来の「境界防御」にのみ依拠し、「被害を受けてから対処する」という受動的なアプローチだけでは十分に対応できなくなっている状況を認識し、こうした状況に応じた対応を果断に実施しなければならない。我が国が自由で安全なデジタル社会を維持するためには、官民一体の連携強化はもとより、ゼロトラスト思想への転換、最先端技術（AI、次世代暗号等）の社会実装、そして平時からの積極的なサイバー防衛網の構築が急務である。

よって、政府に対し、縦割りを排し、以下の施策を国家の最優先課題として速やかに実行すること、そしてその際、必要となる予算の確保や体制の整備を合わせて実施することを強く提言する。

２．　政府全体に対する基本提言（サイバー防衛基盤の抜本的強化）

サイバー緊急事態と認識し、官邸主導で「サイバー対処本部（仮称/事務局 NCO）」を立ち上げ、司令塔の役目を担い、重大な被害が生じた場合適宜迅速に本部会議を開催するなどして、全省庁を挙げた対策を加速し、国民の不安払拭に努めること。

（１）サイバー対処能力強化法に基づく取組の強化

自衛隊・警察の能力の構築加速、官民協議会の積極的活用、通信情報の利用の着実な施行、同盟国・同志国との連携強化を加速すること。

（２）経営層の意識改革と開示の充実

サイバーセキュリティは「IT 部門の業務」ではなく「経営の最重要課題（アジェンダ）」である。上場企業等の経営層に対し、事案発生時の説明責任だけでなく、平時からの体制構築を強く促すこと。

（３）国家の盾となるサイバーセキュリティ人材の育成・確保

国家を背景とする高度なサイバー攻撃に対抗し得る「トップガン」人材の不足は、国家的なアキレス腱である。政府・公的機関において、民間の高度なサイバー人材（ホワイトハッカー等）の市場価値に見合った待遇を用意できるよう、硬直的な公務員制度を打破する新たな人事・給与制度（ジョブ型雇用の本格導入等）を創設すること。併せて、実践的なサイバー攻防演習を通じた人材の裾野拡大を図ること。

３．　関係省庁・機関への個別提言（アクションプラン）

AI によるサイバー飽和攻撃を含む未知の脅威に対抗し、優位性を確保するため、関係各機関は以下の役割を強力に遂行すること。

（１）NCO（国家サイバー統括室）：国家サイバー防衛の「司令塔」として

- 能動的サイバー防御の実行体制構築：脅威の探知・分析からインシデントの無害化に至るまでの実動オペレーション体制（官民の専門家からなるタスクフォース、高度技術を有する民間企業や AI の積極的活用等）を実効的に稼働させること。
- 同盟国・同志国とのインテリジェンス共有：ファイブ・アイズ等の同盟国のサイバー専門機関（米国 CISA 等）と連携し、機微な脅威情報（アトリビューション等）の共有関係を更に発展させること。得られた情報を国内の重要インフラ事業者等へ速やかに提供・警告するハブ機能を極大化すること。
- サイバー攻撃情報の集約・分析及びインシデント対応力の強化：一連のサイバー攻撃の情報を集約・分析し、これを踏まえてサイバー攻撃の手法や脆弱性に関して、分かりやすく効果的な情報提供を可能な限り一元的に行い、被害の未然防止・拡大防止に取り組むこと。また、政府関係機関情報セキュリティ横断監視・即応調整チーム（GSOC）による政府機関等の監視体制・インシデント対応力の更なる強化・高度化を図ること。

- 指揮権の発動：重大インシデント発生時には、NCO が各省庁の権限を横断的に統括し、初動対応や被害拡大防止の陣頭指揮を執る法的・実務的スキームを強化すること。
- 「Project YATA-Shield」の推進：次世代 AI モデルにおいて懸念される AI の悪用によるサイバー攻撃の自律化・高度化等のリスク（いわゆる「Mythos 問題」）に AISI と連携していち早く対応すること。防御側も AI 技術を活用し、脆弱性の早期発見・対応等の対策強化を行う「Project YATA-Shield」を強力に推進すること。
- 漏洩被害者への安全な連絡方法の確立：個人情報などの漏洩が行われた際、被害者である個人等への連絡を行う行為が、フィッシング詐欺の温床となりかねない懸念が持たれている。被害者に対してどのような形で通知をすればこうした懸念が生じないか、技術面も含めて個人情報保護委員会や産業界と協力して安全な連絡方法を確立すること。
- 米国の事業者との連携：OpenAI、Google、Anthropic 等の米国の主要フロンティア AI 事業者と直接の連携窓口を構築し、AI を政府機関等の情報システムの点検に活用し、脆弱性診断・優先順位付け等の迅速化・高度化を目指すこと。
- 政府調達における対策強化：必要なサイバーセキュリティ対策を施した機器・クラウド等の調達や委託先の選定を一層推進すること。そのため、必要な対策レベルを満たす製品や事業者を容易に判別できるよう、対策状況の可視化を進めること。
- 耐量子計算機暗号（PQC）移行の加速：欧米主要国は、影響の大きいシステムを 2030/2031 年頃までに PQC へ移行するとされており、我が国政府機関等においても、優先度が高いと判断するシステムについて、早期の期限を定めて移行を加速すること。

（２）内閣府 AI 室/AISI（AI セーフティ・インスティテュート）：AI×サイバー領域の「専門機関」として

- 産業界の安全な AI 実装に向けた指針改訂：サイバー攻撃への守りを強化しながら、企業の AI 実装を進めていくための実践的な指針とするべく、先般 AISI が策定した「AI インシデントレスポンスアプローチブック」を早期改訂すること。
- 「Project YATA-Shield」の推進：次世代 AI モデルにおいて懸念される AI の悪用によるサイバー攻撃の自律化・高度化等のリスク（いわゆる「Mythos 問題」）に NCO と連携していち早く対応すること。防御側も AI

技術を活用し、脆弱性の早期発見・対応等の対策強化を行う「Project YATA-Shield」を強力に推進すること。（再掲）

- 米国フロンティア AI 事業者等との戦略的連携：米英等の各国 AISI と連携し、AI によるサイバー攻撃の自律化・自己進化等の潜在リスクへの対応の検討や AI の不透明な挙動やリスクの可視化・評価等を進めるとともに、AI のリスク情報を共有する体制を整備する。更に、OpenAI、Google、Anthropic 等の米国の主要フロンティア AI 事業者と直接の連携窓口を構築するとともに NCO 等と連携し、AI エージェントによる脆弱性診断のみならず、AI による脆弱性解消（パッチをあてる）の自動化や自律化の確立を目指すこと。また、防御側による AI の利用により、不正アクセスや被害を把握する能力の向上が行われるように事業者と協力して検討を行うこと。

（３）デジタル庁：国のデジタル基盤とトラストの「守護者」として

- ゼロトラスト思想の徹底とガバメントクラウドの厳格な監査：国や自治体のシステムに対し、従来の境界防御にのみに依拠しない「ゼロトラストアーキテクチャ」の考え方を踏まえたセキュリティ対策を迅速に推進すること。また、ガバメントクラウドを提供する国内外のベンダーに対する厳格なセキュリティ監査を定期的かつ機動的に実施し、サプライチェーンリスクを完全に排除すること。
- マイナンバーカードの利用による本人確認の徹底：不正アクセス事案において、運転免許証の券面コピーで本人確認を実施していたことで個人情報漏洩が発生した。また、犯罪収益移転防止法・携帯電話不正利用防止法において、2027 年４月には、対面での本人確認におけるマイナンバーカード等 IC チップ読取義務化等が施行される。このような状況を踏まえ、デジタル認証サービスと対面確認アプリを用いてマイナンバーカードの行政分野のみならず、民間分野における利活用を法規制分野に限らず幅広い分野において加速させ、安全・確実な電子的本人確認を推進すること。その際、民間事業者からのサービス等利用に関する相談について、相談件数の急増に対応できるように体制を強化すること。そして、それにとどまらず、マイナンバーカードの社会実装が進展してきている現状を受けるとともに、安全度の高い本人確認手段を普及させる観点からも、マイナンバーカードの取得の義務付けを検討すること。その際、マイナンバーカードを活用したサービスの拡充、民間利用の促進、生体認証が可能となるスマートフォン搭載の推進、デジタルに不慣れな方々への支援、広報の強化も合わせて進めること。また、マイナンバーカードの利用拡大に当

たっては、安全性の一層の向上に向けてマイナンバーカード及びその関連システムのセキュリティ及び運用管理について、専門家による検証を含む総点検を実施すること。そして、点検結果に基づき、必要な予算・人材を確保しつつ、対策を実行すること。

- 次世代認証基盤（DID/VC）及びマイナンバーカードの活用：マイナンバーカード（JPKI）の民間システムへの組み込みを促進する。更に、情報漏洩に強く改ざん耐性のあるweb3時代のトラスト基盤として、分散型ID(DID)及び検証可能なクレデンシャル（VC）の有用性を検証すること。

（４）経済産業省及び金融庁等：産業政策とルールの「推進役」として

- 上場企業等の開示の充実：上場企業等の経営層に対し、事案発生時の説明責任だけでなく、平時からの体制構築を強く促すこと。金融庁等が、サイバーセキュリティに関する重要情報の有価証券報告書への記載の充実を促進するとともに、当該記載を行うことの重要性を上場企業等に広く浸透させること。併せて、本年７月に改訂されたコーポレートガバナンス・コードに沿って、上場企業におけるサイバーセキュリティリスクへの対応を含めた全社的リスク管理体制の整備を促すとともに、整備状況をフォローアップすること。その際、経営陣の一角として権限を持った CISO（最高情報セキュリティ責任者）を設置し、サイバーセキュリティリスク対応を高度化している事例なども取り上げてサイバーセキュリティ対策の高度化が広く行われるようにすること。
- 経営ガイドラインの厳格化：上場企業に対し「サイバーセキュリティ経営ガイドライン」の遵守を強く求め、CISO 設置や、ゼロトラスト環境への移行、平時からのインシデント対応計画（IRP）の策定を令和９年３月に運用開始予定のサプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）に合わせて促進すること。
- サプライチェーン防衛への投資支援と「サイバーセキュリティお助け隊サービス」の拡充：令和９年３月に運用開始予定のサプライチェーン強化に向けたセキュリティ対策評価制度（SCS 評価制度）を大企業の委託先管理手法として推奨するとともに、サプライチェーンの弱点となりやすい中小企業への支援を抜本的に強化すること。現在実施している「サイバーセキュリティお助け隊サービス」事業の補助メニューや対象枠を大幅に拡充し、全国の中小企業が安価かつ容易にセキュリティ対策を導入できる環境を整備すること。広くセキュリティ人材の育成を加速化するため、SCS 評価制度の推進を通じた中小企業におけるセキュリティ対策の推進や、情報処理安全確保支援士の充実と同支援士と中小企業とのマッチン

グを通じて、中小企業のセキュリティを担う人材の裾野を広げるエコシステムの構築を図ること。

- サプライチェーン観測網の導入：慢性的なセキュリティ人材不足に悩む中小企業を高度なAIサイバー飽和攻撃から守るため、サプライチェーン企業が参加する観測網を導入し、人間の専門家に代わって24時間365日監視すること。これにより、異常検知を早期の対策に繋げるとともに、他の参加企業への攻撃の連鎖を防ぐ、集団的防御プラットフォームの構築・運用を進めること。サイバーセキュリティお助け隊サービスが同プラットフォームと緊密に連携することにより、企業の対策強化が確実なものとなることにも留意しつつ、取組の実現を図ること。
- ホワイトハッカーをはじめとするセキュリティ人材の育成と、AI を活用したペネトレーションテストの実現：IPAに設置された国内最高レベルのホワイトハッカー育成施設であるICSCoEにおいて、重要インフラを始めとする主要業界トップのセキュリティ人材、いわゆるトップガン人材を継続的に育成し、トップガン人材が各業界の守り手として、高性能AIも活用したペネトレーションテストを通じたセキュリティ強化を実現すること。各業界のトップガン人材の連携を促進し、業界横断で我が国の防御能力の向上を実現すること。中小企業においてもAIを活用したセキュリティ強化の取組が可能となるよう、サイバーセキュリティお助け隊サービスにおいてAIを活用したセキュリティサービスを提供すること。
- OT システム特化型サイバーセキュリティ AI の開発と秘密計算技術の実装による安全なデータ利活用：事業活動の継続に必要不可欠となるOT分野のセキュリティ確保に向けて、他国の技術に過度に依存せず、自律的なセキュリティ確保が実現可能となるよう取り組むこと。このため、国産のOTシステム特化型サイバーセキュリティAIの技術・研究開発を検討・推進するとともに、こうしたAIを安心して利用できるよう、重要データを暗号化してクラウドに送信し、暗号化データのままクラウド上で処理を行う、秘密計算技術の技術・研究開発を検討・推進すること。
- 事業者におけるAIエージェントの安全な利活用に向けたガイドライン作成：AI エージェントは企業の業務効率化に資する一方、意図せぬ挙動により企業の経済活動に悪影響を与える可能性があるため、企業が安全にAIエージェントを利活用できるような指針を検討すること。
- ベンダーの対応能力、クライアント企業への支援能力の向上：個人情報等を扱う企業等のシステムを担っているベンダー企業等において、先端的な不正アクセスへの対応能力を向上させるとともに、クライアント企業への支援を迅速に行えるように体制の整備を促すこと。

- 信用情報機関への通報のワンストップ化の仕組みの整備の検討：情報漏洩の被害者が被害の拡大を止めるために信用情報機関に対して通報することが行われているが、対応を徹底するためには複数機関への通報が必要となっており、負担を強いられている。信用情報機関同士の連携を促し、ワンストップで通知が済むような仕組みの構築を民間団体とともに検討すること。
- 金融分野における官民連携、防御力及びレジリエンスの強化：金融システムの安定性を確保していく観点から、金融機関等において経営陣の関与の下、要請文（５月 22 日）で示した「短期的な対応」を着実に進めるとともに、ガイドライン等で示している多層防御やインシデント発生時の備えといった基本的なサイバーセキュリティ対策を着実に実施することを促すこと。また、金融業界全体のレジリエンス強化に向けて、業界横断的なサイバーセキュリティ演習の実施や、金融 ISAC 等を通じた知見の共有等の取組を強化すること。
- IoT 製品やセキュリティ事業者のセキュリティ対策状況可視化：政府や民間企業が安心して IoT 製品やセキュリティサービスを調達できるよう、それらのセキュリティレベルを可視化する制度を構築すること。具体的には、IoT 製品を認証する JC-STAR 制度の拡充や、セキュリティサービスを提供する事業者を対象とした制度の検討・実施に取り組むこと。

（５）個人情報保護委員会：国民の権利を守る「監視体制」として

- 不正アクセスに関する個人情報保護法の厳格な執行：大規模な個人情報漏洩事案において、企業側の初動報告の遅れや事態の過小評価（隠蔽体質）が見られた場合には、速やかな報告徴収や立入検査の実施と、厳正な勧告・命令を躊躇なく行うこと。
- 保有する個人データの最小化：安全管理措置や、本人確認等のために取得した画像等の保存期間・保存方法などに関する基本ルールについて、必要な業種に関し、その事業所管省庁とともにガイドライン等としてまとめ、企業が不要な個人データをむやみに保持しないように行動変容を促すこと。
- 罰則の広報啓発：「個人情報の保護に関する法律等の一部を改正する法律」（令和８年法律第 56 号）により、不正アクセス行為による個人情報の不正取得に対する罰則が新設されたところ、その実効的な広報啓発に取り組むこと。
- 漏洩被害者への安全な連絡方法の確立：個人情報などの漏洩が行われた際、被害者である個人等への連絡を行う行為が、フィッシング詐欺の温床

となりかねない懸念が持たれている。被害者に対してどのような形で通知をすればこうした懸念が生じないか、技術面も含めて NCO や産業界等と協力して安全な連絡方法を確立すること。

（６）警察庁：サイバー犯罪に対する「捜査と特定（アトリビューション)」の最前線として

- 攻撃者の特定（アトリビューション）能力の抜本的強化と体制拡充： 警察庁の「サイバー特別捜査部」等の体制を更に拡充し、資機材の充実強化や人材育成等も通じて、高度なフォレンジック技術や AI を活用した捜査能力を極大化すること。特に国家を背景とする攻撃に対しては、防衛省や NCO 等の関係機関と密に連携し、攻撃の背後にいる組織・国家を正確に特定し、政府としての公表（パブリック・アトリビューション）の基盤となる確固たる証拠保全及び解析体制を確立すること。
- 国際共同捜査による犯罪インフラのテイクダウン（無害化）の主導：ランサムウェア・グループなど多国籍化・分業化するサイバー犯罪組織を壊滅させるため、FBI（米連邦捜査局）やユーロポール等、各国の法執行機関との国際共同オペレーションに主導的に参画すること。犯罪者が利用するインフラ（C2 サーバー等）のテイクダウン（無害化）や、不正に取得された暗号資産の追跡を積極的に実行し、「日本を狙うサイバー攻撃は割に合わない」という強力な抑止力を発揮すること。
- 被害組織が相談しやすい環境整備等：企業・団体に対して情報漏洩事案を起こさないよう必要なセキュリティ対策の実施を働き掛けるとともに、攻撃を受けた被害企業・団体が躊躇なく警察に相談・通報できるよう、事業者等との平素からの信頼関係の醸成及び協力関係の構築を NCO や事業所管省庁の協力を得て推進するほか、初動対応や事業継続（復旧）を支援する視点を持ち事案の対処に当たること。また、捜査過程で得られた攻撃の手口（TTPs：Tactics, Techniques & Procedures：戦術・技術・手順）等を、NCO 等とも連携しつつ、受け手の民間事業者にとって冗長にならないやり方で還元し、社会全体の防御力向上に寄与するエコシステムを構築すること。
- 個人情報漏洩事案における２次被害対策の徹底：個人情報の漏洩に遭った方々が更なる被害を受けることがないよう、セキュリティ対策の再確認を国民に広く呼び掛けるとともに、なりすましによる口座の開設等を防ぐため、関係省庁と連携し、各事業者における本人確認の徹底を促進すること。また、特殊詐欺の犯人が流出した個人情報を悪用し架電することも考えられるため、特殊詐欺対策に有効な「警察庁推奨アプリ」の活用の

周知を図るほか、被害に遭っているのではないかと不安を感じる方々からの相談等に適切に対応すること。

（７）総務省：「サイバー空間そのものである情報通信ネットワーク」と地方公共団体を所管する立場として

- 通信事業者による対策の強化：デジタル社会のあらゆるデータを取り扱い、基幹インフラの担い手である通信事業者において先導的に実効性ある、積極的なインフラ防護策をとることが急務であり、総務省における検討を迅速に行い、可能なものから機動的に実施すること。
- NICT による研究開発等の推進：情報通信研究機構（NICT）は、今般のサイバー攻撃の分析を行い、原因の一つとしてスマートフォン等のアンドロイドアプリを使用するサービスへの攻撃手法を特定して、必要な対策を周知しており、こうした NICT の分析能力を更に高度化すべく、NICT による AI×サイバーに関する研究開発、分析人材・対処人材の育成、脅威情報の収集、分析能力の活用・強化、脆弱性診断の活用等を一層推進するとともに、そのための研究・分析環境の整備を進めること。また、NICT の分析結果を必要な関係者に迅速かつ的確に共有するとともに、研究成果の効果的な展開に向け、民間企業との連携・協調を一層強化すること。
- 機器の踏み台化等の防止：AI の普及・進化等によりサイバー攻撃が相次ぐ中で、多数の一般利用者の機器が「踏み台」として悪用され攻撃基盤の一部となり得る状況に対応するため、攻撃基盤を特定し、その悪用を防止するための環境整備を進めること。
- 地方公共団体による対策と国による支援：地方公共団体は、住民生活に欠かせない様々なサービスを提供するとともに、個人情報など重要な情報を保有しており、そのサイバーセキュリティの確保は極めて重要である。総務省は地方公共団体に対し、CISO 等によるガバナンス体制の下、担当課が独自に導入したものや委託先企業が運用するものを含め、全てのウェブシステムとそのセキュリティ対策を把握するよう要請した上で、業務継続の必要性に応じて、脆弱性対応が完了するまでの一時的なサービス停止や、取り扱う必要のない情報を取り扱わないことなどを検討するよう求めること。併せて、基本的な脆弱性対応の徹底に加え、AI を活用した脆弱性診断とその結果を踏まえた対応を促すこと。更に、地方公共団体がこれらの対策を実際に講じられるよう、地方公共団体及び委託先企業に対し、必要な情報提供や支援を行うこと。
- 量子暗号通信（QKD）の社会実装の加速：政府機関や重要インフラ等の機微なデータを取り扱う重要機関間の通信の安全性を一層高めるため、機

微情報の盗聴・改ざんを確実に防ぐ量子暗号通信（QKD）について、耐量子計算機暗号（PQC）に加えた二重の防護技術としての導入が急務であることから、東名阪 QKD ネットワークの整備を加速すること。

(8) 防衛省：国民の生命、財産と我が国を守る立場として

- 「能動的サイバー防御（ACD）」を含むサイバー防衛能力の強化：自衛隊の指揮統制・情報システムのみならず、国民の社会、経済活動の基盤をなす国や基幹インフラなどに対する重大なサイバー攻撃を未然に防止するため、攻撃元サーバーに対して能動的にアクセスし、脅威を取り除く「アクセス・無害化措置」のための能力をはじめ、サイバー防衛能力の強化に取り組むこと。
- 重要インフラ等のシステムへの支援も見据えたスレット・ハンティング機能の強化：平時から有事に至るまで、サイバー攻撃をシームレスに抑止・防止するため、自衛隊が運用する情報システムを対象に行ってきたスレット・ハンティング能力を更に強化するとともに、新たに策定された「脅威ハンティングの基本方針」も踏まえ、国民の生活・経済活動を守り、自衛隊の任務遂行を確実にする上で不可欠な重要インフラ等のシステムを防護するため、必要な能力整備を行うこと。

(9) 厚生労働省：医療機関の防護と地域医療継続の「支援役」として

- 医療現場におけるサイバー防衛の標準装備化：医療機関におけるサイバーインシデントに特徴的な、外部からの攻撃ルートの把握・管理、多要素認証の実装、その他のセキュリティ強化を迅速に進める必要がある。その際、セキュリティ投資を診療報酬等に転嫁しにくい我が国の医療保険制度の特性を踏まえ、必要なセキュリティ経費に対する補助や、対策の実施を支援する伴走型支援体制を整備すること。
- 医療現場における専門人材の活用：セキュリティ人材の確保が困難な医療分野においては、IPA 登録人材等の外部専門人材の活用により専門知見・技術を補完するとともに、医療現場における人材育成や攻防演習、指導者育成施策を通じて人材活用と能力向上を推進すること。
- 重要インフラにふさわしい防御力の整備：医療分野は重要インフラであるが、今後の基幹インフラ指定等も見据え、特定機能病院に対するセキュリティ点検を実施するとともに、改善状況の継続的なフォローアップを行うことで、安定的かつ強靭な医療提供体制を整備すること。

（10）消費者庁：消費者の安全・安心を確保する立場として

- 消費者への注意喚起：消費生活相談情報を取りまとめ、関係省庁に共有するとともに、関係省庁と連携して、消費者の被害・二次被害の防止に向けて必要な注意喚起を行うこと。

（11）国土交通省：社会経済活動を支える重要インフラを所管する立場として

- 重要インフラの安定的なサービスの確保：国民生活と経済活動を支える航空、空港、港湾、鉄道、水道、物流の安定的なサービス提供を確保するため、アタックサーフェスマネジメント（ASM）によるリスク情報提供、インシデント発生時の駆けつけ支援、相談窓口の設置等の取組を着実に推進すること。また、官民及び事業者間でサイバー脅威に関する情報や対応ノウハウの共有を進め、各事業者のサイバーセキュリティ対策の実効性向上を図ることで、重要インフラ全体のレジリエンス向上に繋げること。

４．　おわりに

サイバー空間における防衛力の優劣は、今後の我が国の国力を左右する最大の決定要因の一つである。来るべき「AI のサイバー飽和攻撃」の脅威を前に、政府においては本提言の各項目について直ちに必要な予算措置及び必要となる法令の検討に取り掛かり、国民の安全と我が国の産業競争力を死守する責務を果たすよう強く求める。とりわけ、現在及び今後の重篤な被害の発生に鑑みれば、サイバー対処能力強化法における外国関連通信情報の利用では不十分な場合において国内通信情報を被害の防止のために利用することなどについての検討を行うことも辞さずに対応することを求める。