国家安全保障戦略等改定や日本成長戦略策定に向けた提言

平時・有事の区別のないサイバー空間における
我が国のサイバー対処能力の向上と社会全体のレジリエンス強化に向けて

【国家サイバーセキュリティ戦略本部　提言】

令和８年５月１４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

目的

サイバー情勢が厳しさを増す中、国際連携・官民連携の下、安全保障分野におけるサイバー対処能力の向上を図るため、昨年５月の通常国会において、我が党が主導したサイバー対処能力強化法・同整備法が成立した。

他方で、サイバー攻撃は、AI 等の新たな技術を取り込み、一段と巧妙化するとともに、国家背景のサイバー脅威が深刻化してきている。

こうした中、先の我が党の政権公約において、サイバーセキュリティなどの様々なリスクや社会課題に対し、戦略的に投資を行い、強い日本経済を実現すること、また、本年中に国家安全保障戦略を含む「三文書」を改定し、新たな時代に対応した防衛体制を構築する旨を掲げた。

これらを踏まえ、国家サイバーセキュリティ戦略本部では、今後想定される、政府における国家安全保障戦略等三文書の改定や日本成長戦略の策定を見据え、これまでの検討と議論の結果をまとめた提言を行う。

＜共通（安全保障関連／成長戦略関連）＞

１．情勢認識

現行の国家安全保障戦略策定時に比べ、安全保障環境が厳しさを増す中、技術革新とも相まって、内外でサイバー脅威が社会に及ぼす影響が質量両面で急速に拡大している。

具体的には、国家背景の脅威アクターによる、重要インフラへの侵入や情報窃取、民間犯罪集団と連携したサイバー攻撃が活発化してきている。これらの攻撃に際しては、有事における軍事活動と連動した重要インフラの機能破壊をも念頭に置いた事前偵察・侵入活動を展開していると言われている。また、ロシアによるウクライナ侵略以降、国際紛争に付随したサイバー攻撃も増加してきている。

昨年夏にイギリスで発生したジャガー・ランドローバー社へのランサムウェア攻撃では、同国経済への打撃などが目的であったと言われている。サイ

バー攻撃は、基幹インフラのみならず、経済活動を支えるサプライチェーン全体に影響を与え、継戦能力にも直結しうる脅威である。もはや平時・有事、軍事・非軍事の区別に意味はなく、平素から社会全体のレジリエンスを強化していく必要がある。

その他、生成 AI をサイバー攻撃に活用することで、攻撃の工程の大半が自動化されるなど、サイバー攻撃の構造が変化してきている。また、高度な脆弱性発見能力を持つ AI モデルも開発され、このような最先端 AI モデルを悪用したサイバー攻撃への懸念が広がっている。こうした技術革新は、サイバーセキュリティにとって利便性とリスク両面で大きな影響を及ぼす。

こうしたサイバー脅威に対応するべく、サイバーセキュリティ戦略（令和７年 12 月 23 日閣議決定）に盛り込まれた施策を推進し、サイバー対処能力の向上と社会全体のレジリエンス強化を進め、世界最高水準の強靱さを持つ国家を目指す。

＜安全保障関連＞

２．サイバー対処能力強化法等の着実な実施と制度の機動的な見直し

サイバー対処能力強化法・同整備法の施行により、官民連携の強化、通信情報の取得・利用、アクセス・無害化を柱とする能動的サイバー防御が可能になる。サイバーセキュリティ施策全般の強化が求められるなか、同法の着実な実施に向け、中核を担う内閣官房・内閣府、警察、防衛省・自衛隊が三位一体となり、各々の役割を適切に果たせるよう、体制整備を行うことが不可欠であり、必要な措置を着実にとっていく必要がある。

また、昨今のサイバー空間の急激な変化や技術変化等の影響も踏まえ、法の来年秋の完全施行から３年を目処とする法の見直しのタイミングを念頭に、後に述べるようなサイバー対処能力の更なる強化のために必要な検討を行うとともに、政省令・ガイドライン等を含めた制度について、必要な見直しは随時行っていくことが必要である。

＜安全保障関連＞

３．政府自体の基盤強化

サイバー対処の要となる政府自体の体制強化が不可欠である。平素から有事も想定し、政府の情報システム・ネットワークを防御・維持・向上させていくための措置を、リスクベースで、計画的に推進していく必要がある。

具体的には、政府内の情報セキュリティ体制の強化の一環として、自律的な運営・管理を確保した上で、機密性の高い情報を扱うために必要な情報保全・秘密保全措置を講じたクラウド（高機密ソブリンクラウド（仮））の導入を進める。具体的なクラウド技術の活用の在り方の検討を早急に進めるとともに、本年中に政府として最適な調達・契約・運用方法について一定の結論を得る。

また、サイバー攻撃は政府機関等の本府省のみならず、その外局や地方支分部局、施設等機関、在外公館も対象になりうることから、これらの機関を含めた情報システム・ネットワークのセキュリティを向上させる。

その他にもサイバーセキュリティ対策やインシデントに関する情報などを迅速に共有できるよう、政府機関間の連携を強化する。

＜安全保障関連＞

４．サイバー対処能力の更なる強化

国家インテリジェンス機能の抜本的強化が必要とされる中、サイバー分野においても、情報こそがサイバー対処の肝であり、とりわけ攻撃者に係るサイバーインテリジェンスの機能強化が急務である。

その上で、平素より、国が要となって、民間も含む我が国の力を結集し、同盟国・同志国との連携の下、防御側に係る施策と攻撃者に対抗する施策を車の両輪として、攻撃者に対して継続的にコストを賦課し、深刻化するサイバー脅威をシームレスに防御・抑止を図る。

具体的には、政府及び官民間でのサイバー情報の収集・集約・分析・提供及びサイバー空間での対処をより強力に行うための仕組みを構築していくこととし、その中で、国家安全保障の観点から、サイバー空間における情報収集及び対処のあり方について検討を行う[1]。

また、国家サイバー統括室を司令塔として、サイバー攻撃キャンペーンに対して多様な能動的な措置（テイクダウン、パブリックアトリビューション、アクセス・無害化措置など）を適宜適切に講じるための関係府省庁等との連携や体制等を確立する。

---

[1] 自由民主党インテリジェンス戦略本部において、本年の夏頃までにインテリジェンス全体について提言を行う予定である。

そのほか、AI 等の活用による適切かつ迅速なインシデントハンドリングの実施や官民双方のサイバー対処人材の活用などサイバー攻撃に対抗できる体制構築を進め、サイバー対処能力強化法に基づく官民連携の枠組みも活用しながら、官民対処のあり方を検討する。

また、同盟国・同志国との情報共有や連携強化を進めるとともに、サイバー犯罪対策を推進する。

＜安全保障関連＞

５．認知戦、偽･誤情報への対応

認知戦[2]に関しては、社会の分断等を生じさせようと、サイバー攻撃、偽・誤情報の流布、物理的な攻撃等が組み合わせて行われている中、近年、AI 等の技術の進展と相まって、ボットネット等も利用した偽・誤情報の大量拡散が容易に実行されるようになり、外国勢力による影響工作の脅威は深刻化してきている。我が国における自由で公正な民主主義を守り抜くため、国民のリテラシーの向上を図るとともに、こうした脅威に対して実効的な対応を行っていくことが不可欠である。

生成 AI 技術の悪用等により悪質化・巧妙化していく外国勢力による情報干渉にも対応できるよう、民間の分析ツール等のアセットも最大限活用し、政府における情報収集・分析力を強化すべきである。また、民間有識者やシンクタンク等とのコネクションも強化し、多角的に情報収集・分析を行うべきである。

現在、外国勢力による偽情報拡散を含む影響工作に対しては、内閣官房副長官の下、関係省庁が連携して対策を講じているが、インターネット空間における情報干渉の飛躍的な増大にも即応できるよう、政府の対応体制を強化していくことが重要である。現在審議されている国家情報会議設置法案が成立すれば、国家情報局がインテル省庁の保有する多種多様な情報を集約・分析し、より高度な分析が可能になることにも鑑み、政府内の連携も一層強化すべきである。

---

[2] 偽情報の流布や、政府の信頼低下や社会の分断を狙った情報の拡散などにより、人の認知に働きかけ、世論や政府の意思決定に影響を及ぼす情報戦。

情報干渉への対応は、民間ネットワークの活用も重要であることから、プラットフォーム事業者との適切な情報共有のあり方を制度面も含めて検討するなど、プラットフォーム事業者を始めとする民間事業者との連携も強化すべきである。

＜成長戦略関連＞

6．社会全体のサイバーレジリエンス強化･確保

サイバー攻撃の対象は、政府機関にとどまらない。民間企業への攻撃は、複雑なサプライチェーンを通じ、様々な製品・サービスの停止をもたらし、我が国の成長を阻害する恐れがある。平素から官民連携の強化を通じ、社会全体のレジリエンスを強化することにより、戦略 17 分野の成長投資を下支えし、我が国の成長を推進していく。

具体的には、危機管理投資・成長投資の投資対象分野は必ずしも基幹インフラのみに限られないため、基幹インフラ以外にも、安全保障上大きな影響を及ぼしうる重要セクターへのサイバーセキュリティ確保のための対応を強化する。

また、サイバー攻撃の被害は、サプライチェーン等を通じ、面的に拡大することから、個別での対策が困難となりがちな、地方公共団体、中小企業、医療、大学などにおいて、人材、ノウハウ、基盤等の共有化等を進め、サイバーセキュリティ対策を底上げしていく。

そのほか、セキュリティパッチやソフトウェア更新等のサポートが終了したレガシーシステムへの対応、セキュリティ製品・サービスの信頼性確保を含め、情報システムのセキュリティを継続的に確保するとともに、仮にサイバー攻撃を受けたとしても民間事業者等の自らの製品・サービスの提供が長期間にわたり停止することを回避するため、民間事業者等の業務継続計画の整備等を促進する。

質・量両面での人材を強化することに加え、サイバーセキュリティにおける自律性確保のため、技術・研究開発を進め、国内産業の基盤を強化する。また、AISI（AI セーフティ・インスティテュート）の機能強化を図りつつ、AI におけるデータポイズニングに対する対策を含め、AI・量子技術など先端技術への対応とその活用を進める。特に、高度自律型 AI を活用したサイバ

一攻撃に対しては、その攻撃のスピードや規模がこれまでより増加しうることから、対策の抜本的強化を進めることが急務である（別添参照）。

　また、中長期的に、サイバー脅威への対応が拡大することが見込まれる中、官民で、その対応が成長に必要な投資との認識を共有した上で、官民が協力した持続可能なサイバーセキュリティ確保のあり方を検討する。

別　添

高度自律型 AI の脅威に対するサイバーセキュリティ対策の抜本的強化について

１．　背景と問題意識

高いサイバー攻撃能力を持つとされる Anthropic 社の Claude Mythos Preview の公表を受け、高度自律型 AI によるサイバー攻撃の脅威が世界的に注目されている。攻撃のスピード・規模が劇的に増加する脅威に加え、Mythos 相当の品質のオープンモデルの登場まで数ヶ月程度になるという予測から、国家のサイバーセキュリティにおける新たな脅威に直面している。

我が国としても、Anthropic 社の Claude Mythos Preview を始めとするフロンティア AI モデルによる、脆弱性の発見・修正等のサイバーセキュリティ性能の急速な向上に対し、これに備えて、国家安全保障の観点も踏まえ、各国政府・関係機関と連携し、政府一体となって、重要インフラ事業者やソフトウェア事業者等の迅速な対応を、即刻促していくことが非常に重要である。

２．　金融分野における先行的な取り組みと他の重要インフラ等への拡大

この非常事態に対応するため、先行して取り組む分野を定め、まず体制の構築を目指す。国家安全保障の観点と攻撃対象へのなりやすさから、相互接続性が高く、リアルタイムで処理されている金融分野で実施するのが適当である。金融庁が官民連携の枠組み（いわゆる金融の「日本版 Project Glasswing」）を構築したところであり、この枠組みを用いて日本として高度自律型 AI の脅威に対する体制を構築し、他の重要インフラ等への拡大を行う。

まずは金融分野において、IT 業界やネット金融等のメンバーも入れた専門部会を設置するとともに、国家サイバー統括室（NCO）、AI セーフティ・インスティチュート（AISI）と連携して、対応を深化させ体制の構築を目指していくのが適当である。

その上で、その他の重要インフラ等分野を含め、NCO が中心となって各省庁の施策全体をパッケージとして打ち出し、政府が一体となって実行していくべきである。Anthropic Claude Mythos Preview に限らず今後リリースされるモデル（Preview を含む）を国としてアクセス可能とし、早期に対応できる体制を構築していくプロジェクトの立ち上げを早急に目指すべきである。

３．高度自律型 AI の脅威に対する体制構築

体制構築に当たっては、①高度化する AI を活用したシステムやソフトウェアの脆弱性の発見・修正等の対応、②発見された脆弱性のパッチ等の対応が必要となる重要インフラ事業者等への対応が必要になると考えられる。

①　高度化する AI を活用したシステムやソフトウェアの脆弱性の発見・修正等の対応

・海外政府機関・ビッグテック等との連携（情報収集等）
【NCO、関係省庁】

・ソフトウェア事業者等への働きかけ（脆弱性の早期発見・対応）
【経産省、NCO】

・AISI による技術支援等（フロンティア AI モデルの評価、安全ガイドラインの作成・提供、各国 AISI との連携）
【内閣府、AISI、NCO】

・技術開発推進　【内閣府、総務省、経産省】

・AI を活用したサイバー防衛能力の強化　【防衛省】

②　発見された脆弱性のパッチ等の対応が必要となる重要インフラ事業者等への対応

・重要インフラ事業者等で注意すべき内容の周知　【NCO】

・いわゆる金融の日本版「Project Glasswing」の他分野への展開
【NCO、重要インフラ所管省庁等】

・政府情報システムでの対応　【デジタル庁、関係省庁】

・自治体情報システムでの対応　【デジタル庁、総務省、関係省庁】

・人材育成支援　【経産省、関係省庁】