サイバー安全保障政策の方向性に関する提言

令和６年９月３日
自由民主党政務調査会
経済安全保障推進本部
デジタル社会推進本部
安 全 保 障 調 査 会
情報通信戦略調査会

国家安全保障戦略（令和４年12月16日国家安全保障会議決定・閣議決定）において、「武力攻撃に至らないものの、国、重要インフラ等に対する安全保障上の懸念を生じさせる重大なサイバー攻撃のおそれがある場合、これを未然に排除し、また、このようなサイバー攻撃が発生した場合の被害の拡大を防止するために能動的サイバー防御を導入する」と明記されている。そのためのサイバー安全保障分野での対応能力向上に関する政策については、政府は、以下の方向性を踏まえ、関連法律案を確実に次期臨時国会に提出することが可能となるよう検討を加速すべき旨、提言する。なお、より広範なサイバー安全保障分野の施策に関しては、本提言内容を超えた様々な課題があることから、今後引き続き検討を続け、多様な状況に対応していくとの覚悟をもって我が国のサイバー安全保障に万全を期すことを求める。

１．官民連携について

① 高度な侵入・潜伏能力を備えたサイバー攻撃から、我が国のインフラ機能と安全保障を確保するため、政府が率先し被害防止に必要な情報を提供すべき。
② このため、セキュリティクリアランス制度を活用し、政府と基幹インフラ事業者等による新たな情報共有枠組みを創設すべき。
③ 基幹インフラ事業者がサイバー攻撃を受けた場合、政府に報告することを義務づけるほか、機微技術保有者など、基幹インフラ事業者以外の者についても、必要に応じ新たな情報共有枠組みへの参加を得て、同様の報告を求めるべき。
④ 基幹インフラ事業者のうち、特に重要な者については、政府とのリアルタイムでの情報連携を図るため、攻撃可能性を示す予兆情報を認知した場合、政府に報告することを義務づけるべき。
⑤ 政府の対応迅速化と被害組織の負担軽減のため、政府の報告窓口のワンストップ化（共有先の一元化や様式の統一化）、簡素化を進めるべき。
⑥ 基幹インフラ事業者に対し、自らの情報システムの重要なデジタル機器・サービス等を

特定し、政府に登録する義務を課すとともに、政府は、当該機器等の脆弱性や悪用情報を基幹インフラ事業者に迅速に提供すべき。

⑦ デジタル機器・サービスのベンダに対して、脆弱性対応に関する責務を規定するとともに、脆弱性への対応要請を行う権限を政府に付与するなど、脆弱性対策を抜本的に強化すべき。

２．通信情報の利用について

① 外国政府主体が関与する高度かつ重大なサイバー攻撃に対処するには、欧米主要国のように、平素から、政府が通信情報を収集・分析することが必要。

② こうした取組を導入するためには、憲法第 21 条の「通信の秘密」との関係を整理する必要があるが、「通信の秘密」との関係では、重大なサイバー攻撃への対処という公共の福祉の観点から、必要最小限の通信情報の利用が可能。また、通信情報の利用について通信利用者の同意がある場合も利用が可能。

③ 以上を踏まえ、通信情報の利用に関する制度は、欧米主要国を参考に、サイバー攻撃防止の実効性を踏まえつつ、国民の権利との関係が整理されたものにすべき。

④ 具体的には、サイバー攻撃の分析に必要不可欠な外国関連の通信については、サイバー攻撃対処のための通信情報の利用の対象とすべき。また、関連通信の収集・分析に当たっては、コンピュータのフィルタリング機能を活用することにより、不必要な情報が迅速に廃棄される一方、必要な攻撃関連情報が抽出され、分析の対象となるよう確保すべき。

⑤ 他方、メール・添付ファイルの件名・本文に通常のメッセージとして書かれるようなコミュニケーションの本質的な内容は、サイバー攻撃対処のために分析する必要はないことから、分析対象から除外すべき。

⑥ 通信情報の利用には、電気通信事業者の協力が不可欠。通信情報の利用は国の責任であることを明確にした上で、必要な法的根拠を整備すべき。

⑦ 国民からの理解を得るに当たり、通信情報の利用の詳細を公開することは攻撃者に政府の「手の内」を明かす行為になり不適切であることから、政府内に高度な独立性や専門性が確保された監督機関を設置すべき。

⑧ 必要な秘密保持を確保しつつも、通信情報分析の結果をできる限り国民や企業に共有し、国全体のサイバー防御能力向上とサイバー防御への理解の促進を実現すべき。

⑨ 法制度のほか、取得した通信情報を十分活用できるよう、施設・設備の充実や分析官のレベルアップを通じ、分析能力を向上させていくべき。

３．アクセス・無害化措置について

① ひとたび攻撃が行われれば被害が瞬時かつ広範に拡散するサイバー攻撃の特性を踏まえれば、重大なサイバー攻撃の未然防止や被害拡大防止の視点が極めて重要。
② このため、被害が発生してから令状を取って捜査を行う刑事手続では対処できず、被害発生のおそれを認知し次第、被害防止の措置がとれるように権限を整備すべき。状況に応じた措置を即時的に実施する、いわばサイバー版の警察官職務執行法のようなものを検討すべき。
③ 重大なサイバー攻撃に対処するため、我が国の持てる能力を最大限活用することが重要であり、内閣官房を司令塔として機能させつつ、能力を有する防衛省・自衛隊及び警察をアクセス・無害化措置の実施主体とすべき。
④ 武力攻撃に至らない状況を念頭に置き、警察は平素から、自衛隊は公共の秩序維持の観点から必要に応じ、的確に措置を実施できるよう制度を構築すべき。
⑤ 外国政府主体が関与する高度かつ重大なサイバー攻撃に有効に対処するため、有事へのエスカレーションも念頭に置きつつ、平素から、柔軟かつシームレスに対応できるよう、「事態認定方式」ではない新たな自衛隊の行動類型を整備すべき。
⑥ 我が国のサイバー対処能力は有限であることを踏まえ、防護対象としては、通信・電力などのインフラを始め、国民の生命・安全に関わる基幹インフラを重視すべき。
⑦ 我が国の講じる措置が国際法に違反することはあってはならない。アクセス・無害化に当たっては、国際法との整合が図られるよう運用すべき。
⑧ 措置整備に当たっては国民の理解が得られることが重要。運用の実効性に配意しつつ、措置の適正性を確保し得る制度を構築すべき。
⑨ 運用の実効性確保のため、措置の実施に関しては、攻撃者側に我が方の動きが悟られ攻撃者側が秘匿等の対策を行うなど、相手方を利することがないよう、我が方の活動に係る情報の公表には特段の留意を図るべき。
⑩ 措置に当たっては、攻撃者側を常に意識し、その意図等の見積もりが不可欠。サイバーに限られない幅広いインテリジェンスの活用と深い分析能力を獲得すべき。
⑪ 措置の成功には高度人材によるプロフェッショナルな仕事が不可欠であり、人材育成についても特段の配慮を行うべき。

４．横断的課題

① サイバーセキュリティ戦略本部の機能強化を図るべき（民間有識者参画の場と分離し、全大臣を構成員とし、各省に対する強力な権限を付与すべき）。
② 「欧米主要国と同等以上の能力」を獲得すべく、「司令塔」組織への権限付与、サイバー安全保障政策・運用（特にアクセス・無害化）を担当する大臣の設置の制度的担保、分析等への AI の積極的活用を含め、政府全体の予算・体制・能力を抜本的に強化すべき。

③ グローバルなサイバー空間は有志国と連携して安全に保つことが重要。我が国の関係機関がそれぞれのカウンターパートと密接に連携する中で、必要な措置が講じられるべき。

④ サイバーセキュリティ人材の育成・確保を図るため、求められる知識や技術を明確化するとともに、キャリアパスの明示などにより、魅力あるキャリアとすべき。同時に、官民の人材交流を進めるべき。また、人材育成や対処能力向上に資するメカニズム（エコシステム）を構築するため、同盟国・同志国も含めた国際的な官民枠組みへの参画等に積極的に取り組むとととともに、国内外の図上や実践形式の演習の実施や参加をすべき。