「見える化通信」では、難しそうで見えづらい政策課題の中身を月に一回紹介します。

見える化通信

急がれる能動的サイバー防御
通信の秘密との関係整理が必要

近年のサイバー攻撃の巧妙化や、頻発する重要インフラへの攻撃に対応するため、政府は能動的サイバー防御の導入に向けた議論を始めています。早ければ、秋の臨時国会に提出される予定です。

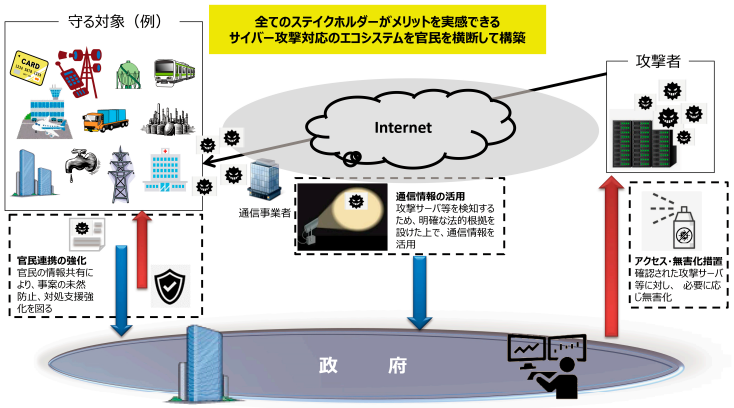
電機連合　総合産業・社会政策部門

急がれる能動的サイバー防御

能動的サイバー防御（注1）とは、サイバー攻撃の兆候段階で相手のシステムに入って対処することを言います（図表1）。近年、身代金の要求型や機微情報の搾取など攻撃手法が巧妙化していることに加え、医療機関や空港、変電所などの重要インフラへの攻撃も多発していることを受け、能動的サイバー防御の導入に向けた議論が進んでいます。

■図表１　能動的サイバー防御のイメージ

「国民生活の基盤をなす経済活動」や「社会の安定性」をサイバー攻撃から守るため、能動的なサイバー防御を実施する体制を整備する。



出所）内閣府サイバー安全保障分野での対応能力の向上に向けた有識者会議資料

（注1）アクティブ・サイバー・ディフェンス（ACD）。発電所や公共交通機関などの重要インフラ施設や政府機関へのサイバー攻撃を防ぐため、政府が日常的にネット空間を監視する仕組み。

「通信の秘密」の保護との関係整理が必要

今年6月に始まった政府内の有識者会議での議論では、能動的サイバー防御を導入するための課題として、①官民連携の強化、②通信情報の活用、③アクセス・無害化措置などが示されています（図表2）。整理が必要な法令は多く、憲法やサイバーセキュリティ基本法、不正アクセス禁止法などが挙げられます。

■図表２　能動的サイバー防御の課題

課題	内容	整理が必要な法令の例
①官民連携の強化	高度な侵入・潜伏能力に対抗するため、政府の司令塔機能、情報収集・提供機能の強化が不可欠	サイバーセキュリティ基本法、各種業法
②通信情報の活用	悪用が疑われるサーバー等の検知には、「通信の秘密」を最大限に尊重しつつも、通信情報の活用が不可欠	憲法21条（通信の秘密）
③アクセス・無害化措置	重大なサイバー攻撃の未然防止・拡大阻止を図るためには、政府に侵入・無害化の権限を付与することが不可欠	不正アクセス禁止法

出所）有識者会議資料をもとに電機連合作成

最大の論点は、憲法21条が保証する「通信の秘密」の保護との関係です。「通信の秘密」とは、信書や電話、通話、電子データなどの内容や宛先を第三者が知ってはならないことを言い、同条はその保護を保証しています。

法改正にあたっては、「通信の秘密」に例外をつくり、大量のデータ送信など攻撃の兆候があった段階で相手側システムへの監視、侵入が可能になる法的根拠をつくる案がありますが、その際に必要な要件や手続きの規定、独立した第三者機関や国会が関与する仕組みの確保が必要だとの意見が挙がっています。

なお、米国や英国などは「安全保障上の必要性」を要件に事業者の通信情報を活用する根拠法をもっています。また、米国は政府機関や主要インフラの保護について官民の調整を担う組織も創設しています。

早ければ秋の臨時国会提出、丁寧な検討を

能動的サイバー防御は2022年末の「国家安全保障戦略」で導入方針が明記され、2024年の通常国会で関連法案の提出がめざされたものの見送られた経緯があります。

有識者会議での議論がまとまれば、早ければ秋の臨時国会へ法案が提出される予定です。サイバー防御を実効性あるものにしつつ、「通信の秘密」の保護との関係を考慮した丁寧な検討が必要です。