能動的サイバー防御法における基幹インフラ事業者への影響

能動的サイバー防御法における「官民連携の強化」は経済安全保障推進法の対象である大手金融機関等や電子計算機器等の供給者にとって、大きな影響がある。予兆を含めたサイバーセキュリティインシデント検知時の連携強化、脆弱性に関する政府との情報共有および速やかな報告が必要となる。

能動的サイバー防御法の公布

近年、サイバー攻撃は巧妙化・深刻化しており、サイバー攻撃通信数や被害数は増加傾向にある。具体的な事例では2022年、大阪急性期・総合医療センターがVPN機器を侵入経路とするランサムウェア攻撃を受けて発生したシステム大規模障害や、2024年、JALへのサイバー攻撃による国内線・国際線の一部遅延等が挙げられる。ITシステムを高度に侵害し、密かに情報窃取やシステム破壊を行うという攻撃に対し、従来の受動的な防御策（ファイアウォールや侵入後の動きを検知するIDS/IPS等）では対応が難しくなってきている。

このような現状を背景に、2025年5月23日、サイバー対処能力強化法及び同整備法（以下、能動的サイバー防御法）[1]が公布された。この法律は、通信情報を利用・分析し、官民連携を強化して攻撃予兆の段階で、攻撃元のサーバにアクセスし、必要に応じて攻撃を無害化する、というまさに能動的な防御策を実施するための体制作りを目指したものである。

なお、法律は、基幹インフラ事業者を対象としており、経済安全保障推進法（以下、経済安保法）の対象となる金融機関（メガバンク、大手地銀、保険会社等）にも大きく関係する。経済安保法の一つの柱である「特定社会基盤役務の安定的な提供の確保に関する制度[2]」における特定社会基盤事業者、特定重要設備は、能動的サイバー防御法の特別社会基盤事業者、特定重要電子計算機器とほぼ同義であり、経済安保法対象の基幹インフラ事業者は、能動的サイバー防御法での要請に応じる必要がある。

また、本法律で取り扱う情報（インシデント情報や通信情報等）についても適切な管理が必要となるため、官民連携での情報共有には「重要経済安保情報保護活用法（セキュリティ・クリアランス）[3]」が活用される可能性が高く、同時に留意する必要がある。

「官民連携」の影響

能動的サイバー防御法は、「官民連携の強化」「通信情報の利用」「攻撃者のサーバ等への侵入・無害化」「NISC[4]の発展的改組」等の観点で整備されている。この4つの観点のうち、基幹インフラ事業者および電子計算機器等の供給者[5]への関連が強いものは「官民連携の強化」である。その主要な内容は次の通りである。

【電子計算機器の届出およびインシデント報告】

基幹インフラ事業者は、すでに導入している特定重要電子計算機[6]について、その製品名、製造者名等を事業所管大臣に法律施行日から6か月以内に届け出なければならない。また、特定重要電子計算機のインシデント情報やその原因になりうる事象を認知したときは、事業所管大臣及び内閣総理大臣に報告しなければならない。

2025年5月29日に開催された政府のサイバーセキュリティ戦略本部が、サイバー攻撃による被害が発生した際の各種報告様式等を公開しているが、報告内容は重要インフラサービスへの業務影響から攻撃の技術的情報（攻撃の種類や送信元情報、通信量等）まで多岐にわたる内容となっている。

また、能動的サイバー防御法の発動にあたっては、サイバー攻撃の「予兆」の段階で関係機関が情報を集約し、分析・対応するとされている。基幹インフラ事業者

NOTE

1) 正式名称は「重要電子計算機に対する不正な行為による被害の防止に関する法律」「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律」。
2) 国の外部から行われるサイバー攻撃脅威からインフラ事業を守ることを目的とし、一定の基準に該当する事業者（特定社会基盤事業者）を指定し、国が定めた重要設備（特定重要設備）の導入・維持管理の委託をする際に、事前に届け出を行い、審査を得る制度。
3) 重要経済安保情報を適確に保護する体制を確立した上で収集・整理・活用するために、「重要経済安保情報の指定」「事業者へのその情報提供」「その情報の取扱者の制限」等について定める制度。
4) 内閣サイバーセキュリティセンター。National Center of Incident Readiness and Strategy for Cybersecurityの略。
5) 電子計算機等：重要電子計算機もしくは当該電子計算機に組み込まれるプログラム。電子計算機等供給者：電子計算機等の供給を行う者（生産者、輸入者、販売者、提供者）。
6) そのサイバーセキュリティが害された場合に、特定重要設備の機能が停止し、または低下するおそれがある一定の電子計算機。

および重要電子計算機器等の供給者は「予兆」も含めた速やかなインシデント報告に対応するために、連絡体制の強化、組織内CSIRTの有効性の再点検が必要となる。

【構成員としての協議会への参加】

政府は、情報共有・対策のため基幹インフラ事業者、電子計算機等の供給者、その他内閣総理大臣が必要と認める者（あらかじめ同意を得たものに限る）を構成員とする協議会を設置する。協議会を通じ、構成員は守秘義務を伴う被害防止に資する情報の共有と、必要な情報に関する資料の提出が要請される。協議会で取り扱う情報は、具体的には報告されたインシデント情報や選別後の通信情報、協議会自身を通じて得た情報等が挙げられる。

協議会の構成員には、通信情報を含まないが秘密を含み得る情報（提供用総合整理分析情報）も提供されるため、協議会で知り得た被害防止情報の適切な管理とその他の必要な取り組みが求められる。そのことから、セキュリティ・クリアランスにも関連すると想定される。

基幹インフラ事業者や電子計算機器等の供給者がセキュリティ・クリアランスを取得するには、計画策定や推進部署の決定、社内規定・人事制度の改定、高機密データを取り扱うための物理的なセキュリティインフラの整備等、多方面での整備が必要になると推察される。セキュリティ・クリアランスを取得するためのハードルや必要性、ビジネス上のメリット等を踏まえて慎重な経営判断が必要となるだろう。

脆弱性情報の提供等、通信情報の利用

政府が脆弱性を認知したときは、能動的サイバー防御法に基づき当該電子計算機等の供給者に対して脆弱性に関する情報が提供される。また、特定重要電子計算機に関するものであれば、電子計算機等の供給者に対し、必要な措置が要請され、電子計算機機器等の供給者はその求めに応じるよう努めなければならない。

具体的には、導入時に届け出ている機器のバージョン情報等から脆弱性に該当するものである場合のパッチ適用やバージョンアップの要請等が想像されるが、サービスへの影響を踏まえた相談や助言が円滑に行えるように官のみ、民のみではなく平時から官民関係性の強化も必要だと考える。

また、サイバー攻撃の実態を把握するための通信情報は、基幹インフラ事業者との協定（同意）に基づき利用、分析される。インターネットとの接点となるVPN装置など、重要設備に関連するネットワーク機器についても、機種名やバージョン情報等の届け出を求められることから、能動的サイバー防御法は、経済安保法と比べるとより通信にフォーカスした制度設計となっている。

2027年の制度施行に向けて

施行期日は2026年11月23日を超えない範囲内において政令で定める日となり、2025年中には基本方針が策定される。官民の情報共有の体制づくりはこれからであり、今後の整備状況に注視しながら官民一体となって施策の検討・課題に取り組むことが求められている。

Writer's Profile

鳥居 麻美 Asami Torii
金融リスク管理部
エキスパートコンサルタント
専門はIT全般統制
focus@nri.co.jp