03

リスク管理

「基本方針」から読み解く サイバー対処能力強化法の 対応ポイント

サイバー対処能力強化法は、「官民連携の強化」と「通信情報の取得と利用」に係る制度の導入を盛り込んでいる。このほど閣議決定された「基本方針」はその具体的施策を示したものである。サイバー脅威が切迫する昨今の状況を踏まえ認識を変容し、本法に対応していくことが期待される。

2025年12月23日、サイバー対処能力強化法（以下、本法）の基本方針[1]が閣議決定された。本法は、「官民連携の強化」と「通信情報の取得と利用」に係る制度の導入を盛り込んでいるが、今回の基本方針はその具体的施策を示したものである。前者については、基幹インフラ事業者[2]に要請される届出等には入念な準備が必要となること、また幅広い事業者を対象として公助・共助を推進していくこと、また、後者では通信の秘密を尊重し、丁寧な説明を図りながら厳格な運用を行っていくこととされている。ただ、実務上の詳細については今後の政省令を待つ必要がある。ここでは今秋の法施行にあたり、ポイントを基本方針から読み解きたい。

官民連携の強化

「官民連携の強化」に関する施策には、基幹インフラ事業者による機器の届出とインシデント報告、及び他の事業者も交えた協議会運営ならびに情報提供がある。

【届出・報告】

機器の届出では、基幹インフラ事業へのサイバー攻撃の標的となりうる機器[3]を、2026年秋の施行から6か月以内に届け出ることが求められる[4]。経済安全保障推進法の導入審査よりも広範な機器の届出が必要となり、例えば特定重要設備[5]につながるファイアウォールやVPN装置、認証サーバ等も対象となる。また、ASPサービスやクラウドなどの基幹インフラ事業者が直接管理していない設備では、その所有者自身が制度の主旨を理解し調査を進めていくことも期待されている。

関連機器の調査にあたり、機器間のネットワークのつながりを辿っていくことで、調査範囲が無尽蔵に広がってしまうという懸念がある。想定される攻撃ルートから調査スコープを適切に設定し、所管省庁と対話を進める中で、届出対象となる機器を確定させていくといった作業が必要となろう。

インシデント報告では、不正アクセス行為等[6]による被害事象の報告が求められる。届け出た機器への被害事象はもれなく報告の対象となるため、届出対象機器の調査と併せて、ログ等から当該機器の被害情報の取得が可能かを確認しておく必要がある。また、特定重要設備においては、不正アクセス行為等による被害事象だけではなく、被害につながりかねない事象（不正な通信の発見、マルウェアの受信等）も報告対象となる。加えて、速やかな報告が求められることから、被害事象の検知やエスカレーションのみならず、所管省庁への報告等も含めた全社的な運用・管理態勢についても確認しておきたい。

【協議会と情報提供】

本法で立ち上げられる協議会では、被害防止に向けた情報共有と対策の協議が行われる。協議会への参加企業（以下、構成員）には、基幹インフラ事業者に加えて、システム・セキュリティ・製品等のベンダの参画も想定されている。運営面では、ワーキンググループによる情報共有や議論といった様々な形態での交流を通じて、構成員間の連携を推進していくことが企図されている。

構成員には、「提供用総合整理分析情報」が提供される。所管省庁を通じた情報提供だけではなく、必要と判断される場合には、同時に被害防止策の実施が要請される。この情報には、攻撃者の活動状況や機器の具体的な脆弱性といった秘密情報が含まれるため、情報管理の実施が義務付けられている。更に、一部の構成員へは攻撃の背景情報といったより秘匿性の高い情報を提供するこ

野村総合研究所　金融イノベーション研究部　©2026 Nomura Research Institute, Ltd. All rights reserved.

NOTE

1) 「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」(2025年12月23日閣議決定)。その活動概要は「サイバー対処能力強化法（官民連携）の施行に向けた考え方の案」(内閣府政策統括官（サイバー安全保障担当）、2025年12月）も参照。
2) 経済安全保障推進法で指定される「特定社会基盤事業者」のうち、特定重要電子計算機を使用するものを「特別社会基盤事業者」と呼ぶ。これらの事業者は実質的に同一であることから、本稿では総称して「基幹インフラ事業者」と表現している。
3) 「特定重要電子計算機」と言い、サイバー攻撃の被害を受けた際に、特定重要設備の運用に重大な支障が生ずるおそれのある設備のことをいう。
4) 既設のものも含めたすべての設備が対象。なお、施行6か月後以降は、設備の導入または変更後4か月以内に届出することが求められる。
5) 経済安全保障推進法（経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律）における、主要なサービスの中枢を担う情報システムのこと。
6) 「特定不正行為」といい、マルウェアの配置や不正アクセス、その他サイバー攻撃を通じた業務妨害のこと。また、特定不正行為により重要電子計算機のサイバーセキュリティが害されることを「特定侵害事象」という。
7) 特定不正行為に関係があると認められる通信のこと。
8) 「機械的情報」と言い、IPアドレスや不正に関する指令情報等、意思疎通の本質的な内容ではない情報のこと。
9) 「経済安全保障に関する総合的な調査研究及び官民協議会」(経済安全保障法制に関する有識者会議（第13回、2025年12月16日))。

とも視野に入れ、セキュリティ・クリアランス（以下、SC）制度を活用していくことも想定されている。

一方、協議会に参画しない事業者へも、秘密情報を含まない「周知等用総合整理分析情報」が、内閣府から所管省庁を通じて提供される。社会的影響の大きい事業者への有益な情報の共有や、広範な事業者に向けた公表による注意喚起・ガイドラインの周知等が想定されている。

協議会は、今春頃より構成員の候補者への案内が開始され、今秋に立ち上がる予定となっている。構成員への指名が想定される事業者は、どの組織が参画し協議会で得た情報をどのように管理し活用するか等、体制面を検討しておくことが望まれる。

加えて、SC取得の打診を受けた際の方針についても検討しておきたい。SC取得には、物理区画や規程の整備、専門組織の設置や従業員の適正評価に配慮した人事制度の見直しなど複数のハードルがある。ただ、それ以前に「昨今のサイバー攻撃リスクをどのように認識すべきか？」「SC情報をどのように活用しサイバー対処能力を高めていくべきか？」といった、そもそもの議論を深めておくべきだろう。

通信情報の取得と利用：当事者協定

「通信情報の取得と利用」は、他の施策から更に1年後（公布から2年6ヶ月以内）に施行される。通信情報の取得には、「当事者協定の締結に基づく場合」と「電気通信事業者の協力による場合」の2つがあるが、ここでは一般事業者に関わりのある前者について説明する。

当事者協定は、内閣府との間で、国外から国内設備への通信（外内通信）情報を提供する一方で、それを用いたサイバーセキュリティの確保に資する分析情報の提供を受けるものである。通信情報の提供では、「不正が疑われる通信[7]のうち」「不正の内容に関する情報[8]のみを自動的に選別し」「それ以外の情報は消去」する等、厳格な条件と手続きが定められている。また、遵守状況をサイバー通信情報監理委員会で検査する等により、通信の秘密を尊重するよう配慮されている。

内閣府は、重要性の高い基幹インフラ事業者等から協議を求め、その際に丁寧な説明を行う。締結は任意だが、その判断には経営レベルでの検討が必要であろう。

「法令遵守」から「公助・共助」へ

厳しい安全保障環境を鑑みて、高市総理は2025年10月24日の所信表明で、2026年中に安全保障戦略三文書の改定を目指す考えを示した。また、経済安全保障法制においても、官民協議会[9]の必要性が協議されている。公助・共助を目的とした官民連携は、現在では、安全保障戦略の中で広く求められている。

経済安全保障推進法をはじめとした制度対応が増加傾向にある中、官には実効性と民間の負担軽減を両立する運用を期待したい。サイバー脅威が切迫しているのは事実であり、民間には官民連携への積極的な参画が望まれよう。安全保障戦略への認識の変容が求められている。

Writer's Profile

上杉 信孝 Nobutaka Uesugi
金融リスク管理部
エキスパートリサーチャー
専門は金融分野のリスクマネジメント
focus@nri.co.jp