特別企画

サイバー対処能力強化法及び同整備法のポイント

本稿では、2026年に施行される「サイバー対処能力強化法及び同整備法」による中小企業への影響と金融機関にできる支援策を解説する。

露木 諒　インターネット・アカデミー 最高情報セキュリティ責任者（CISO）

サイバー攻撃の脅威は一企業の不利益にとどまらず、もはや国家の安全保障に関わる喫緊の課題だ。中でもランサムウェア（身代金要求型ウイルス）の攻撃が後を絶たず、トレンドマイクロ社の「セキュリティ成熟度と被害の実態調査　2024」によると、平均被害額は2億2000万円に上る。被害が連鎖し取引先やその先まで企業の業務が停止する「サイバードミノ」も増加傾向にある。

そんな中、2026年秋の施行が予定されている「サイバー対処能力強化法及び同整備法」は、大きな変革をもたらすと期待されている。しかし、多くの中小企業は同法について理解が追いついていないのが現状だ。

本稿では、金融機関の担当者として知っておくべき同法の概要と、中小企業にできる支援策について解説する。

① サイバー対処能力強化法及び同整備法の概要

日本におけるサイバーセキュリティのあり方を根本から変えることが期待される新法「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」（通称「サイバー対処能力強化法」。以下、強化法）と「サイバー対処能力整備法」（以下、整備法）が、2026年10月に施行される。

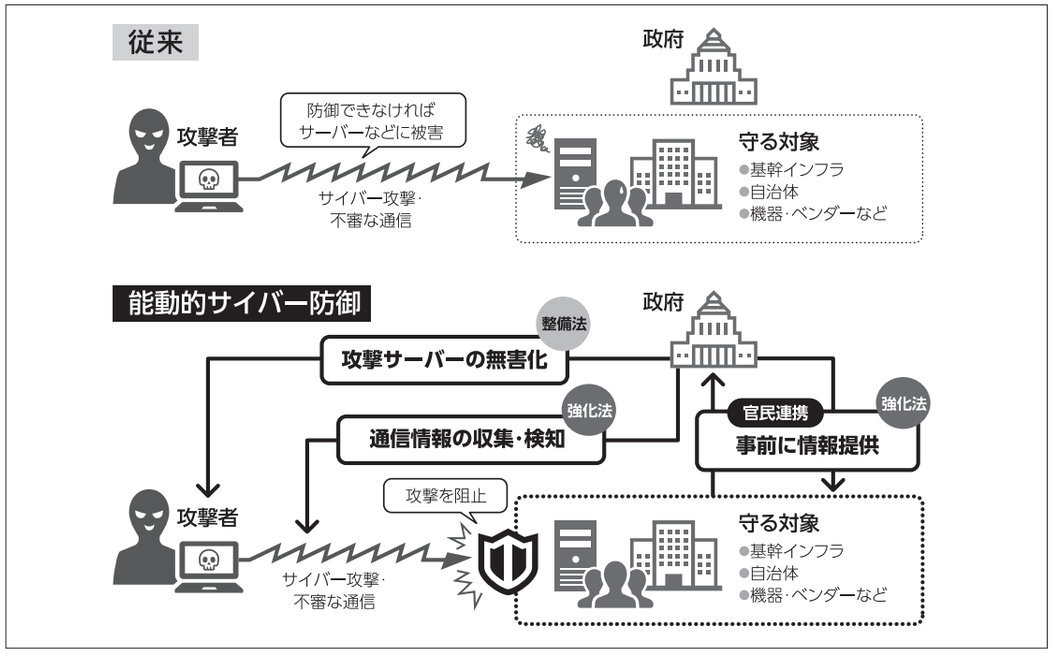
従来の日本のサイバー対策は、攻撃を受けてから対処する受動的なものがほとんどであり、能動的な対策が弱かった。そのため、世界水準と比べて10年は遅れていると言われてきた。その背景には、憲法第21条第2項において定められている「通信の秘密」や「不正アクセス禁止法」といった既存法制度との兼ね合いにより、攻撃の予兆段階で政府が積極的に介入することが困難だったことが挙げられる。

国全体で求められる能動的サイバー防御

しかし、強化法・整備法が施行されれば、サイバー攻撃の被害を未然に防ぐ「能動的サイバー防御」の体制を構築でき、国全体で強大な防御態勢が実現できると期待されている。

強化法・整備法の柱になるのは、官民連携の強化、通信情報の収集・検知、攻撃サーバーの無害化の三つである。これら三つを組み合わせることで能動的サイバー防御の実現を目指すことが、強化法・整備法の狙いだ（**図表1**）。

図表1　能動的サイバー防御の仕組み



（出所）内閣府の資料を基にインターネット・アカデミー作成

強化法で定められる義務と罰則

強化法では官民連携の強化のため、「基幹インフラ事業者」に対しサイバーセキュリティ対策に関する届け出や報告を義務付けている。

強化法における「基幹インフラ事業者」とは、「経済安全保障推進法」に基づき指定された15業種の事業者のことで、具体的には電気・ガス・石油・水道・鉄道・貨物自動車運送・外航貨物・航空・空港・港湾運送・電気通信・放送・郵便・金融・クレジットカードの関連事業者を指す。

強化法で定められた義務の主要例は、次のとおりである。

・特定重要電子計算機の事前届出（導入・変更時）

サイバー攻撃に悪用されるリスクがある計算機や設備を導入・変更する場合、国（業種ごとに異なる主務官庁）に届け出を行う。

・インシデントの早期報告

サイバー攻撃の兆候や被害（特定重要電子計算機の機能停止・低下）が発生した場合、政府への迅速な報告が求められる。

・体制整備および関連企業への要請

脆弱性（ぜいじゃくせい）を見いだし対策を徹底する。必要に応じて、関連企業（委託先である保守管理業者やITベンダー等）に対して体制整備を要請する。

強化法では、違反した場合の罰則も定められている。

例えば、サイバー攻撃の報告義務に違反したり是正命令に従わなかったりした場合は200万円以下の罰金が、調査への資料提出を拒否した場合は30万円以下の罰金が課される。加えて、秘密漏洩（ろうえい）に対しては拘禁刑が課される可能性がある。

② 中小企業への影響と求められる対応

基幹インフラ事業者が注意すべきは、自社のみならずITベンダーやサプライチェーン上の委託先などを含む安全性を政府に報告する義務が生じる点である。委託先である中小企業がサイバー対策を怠り、サプライチェーン上の「弱点」となった場合、元請企業は法令遵守のために取引の停止や契約解除を選択せざるを得なくなる。

従来、こうした選択は、自然災害による物流網の寸断や地政学的要因による原材料不足に起因するケースが一般的だった。しかし、近年はデジタル化に伴い、最も警戒すべきリスクが「サイバー攻撃による供給網の分断」へと変質している。

サイバー攻撃におけるサプライチェーン・リスクの最大の特徴は、「セキュリティが最も弱い箇所」が攻撃の足場にされる点である。攻撃者は大企業や基幹インフラ事業者を正面から攻撃するのではなく、あえて防御の薄い取引先の中小企業や保守管理業者を標的にするのだ。

一度中小企業のネットワークに侵入すれば、信頼関係に基づいて接続された元請企業のシステムに容易に到達できてしまう。具体的な手法としては取引先を装ったビジネスメール詐欺、中小企業が使用する汎用ソフトウェアの脆弱性を突いた攻撃などがある。

中小企業に求められる高難易度の対応

強化法・整備法への対応は、従来の情報セキュリティ対策とは次元が異なるレベルだ。その難しさの本質は、単なる「ツールの導入」ではなく、「高度な運用体制の構築」と「継続的な情報開示」が求められる点にある。

ここからは、中小企業に求められる強化法・整備法への対応のどのような点が困難なのか、三つの項目に分けて解説していく。

①透明性ある情報提供体制の構築

これまでのセキュリティ対策は、ウイルス対策ソフトの導入などで「自社を守ること」が第一にあった。しかし、強化法・整備法の影響下では、政府や元請企業に対し自社のネットワークが安全であると証明し続けることが求められる。

特に、攻撃の予兆を検知するための通信ログの保存や事案発生時の迅速な情報提供体制の構築は、専門知識を持つ人材が不足しがちな中小企業にとって負担が大きい。

②コスト負担と投資対効果（ROI）の見えにくさ

セキュリティ対策は企業にとって直接的な利益を生まず、「不測の事態を防ぐ」ための投資というのがその本質である。強化法・整備法に対する経営者の理解度が低い場合、コストの大きさやROIの見えにくさが体制構築の障壁になり得る。

③サプライチェーン全体にわたる「証明」の連鎖

基幹インフラ事業者から「再委託先のセキュリティも担保せよ」と求められた場合、自社の管理だけでなく、委託先の指導・監査まで行わなければならない。この管理責任の連鎖が中小企業の現場担当者の負担を重くし、難易度を引き上げる要因になっている。

図表2　強化法・整備法への対応に活用できる補助金・助成金の一例

補助金・助成金	説明	補助額
IT導入補助金 （セキュリティ対策推進枠）	IPAが公表する「サイバーセキュリティお助け隊サービス」等の導入費用を補助する制度	5万円～150万円 （補助率1/2以内）
自治体独自の助成金	東京都の「サイバーセキュリティ対策促進助成金」など、地域によっては国よりも手厚い支援が存在する場合がある	最大1,500万円 （サイバーセキュリティ対策促進助成金の場合）

（出所）インターネット・アカデミー作成

③ 金融機関にできる提案と支援策

中小企業が強化法・整備法に対応する際の障壁は、「コスト」と「専門知識の不足」にある。金融機関の担当者には、これらを解消するための支援が期待される。

実務的な支援フローとしては、①現状把握、②自己診断の推奨、③補助金や専門家とのマッチング支援が考えられる。

①現状把握

取引先に対し、元請企業からセキュリティ基準の要求が来ていないかヒアリングし、現状を把握する。

②認定制度や自己診断の推奨

情報処理推進機構（IPA）の「SECURITY ACTION」の取得、経済産業省の「DX推進指標」の自己診断の実施などを取引先に推奨する。これらの取得・実施は強化法・整備法が求める「安全性の証明」の基礎であり、セキュリティ体制の整備状況を社外に提示できる。

サイバー保険の付帯提案が重要

③補助金や専門家とのマッチング支援

国や自治体の補助金を活用することで、セキュリティ対策への初期投資を抑えられる（**図表2**）。追加の費用については、自行庫からの融資やリースを提案し、サイバー保険の付帯提案も行う。

万が一、インシデントが発生した場合に強化法・整備法が定める報告義務を果たすには、調査や再発防止策の策定が求められ、多額の費用の発生が見込まれる。これらを補償するサイバー保険の提案は、債権保全の観点からも重要だ。

ITコーディネーターやITベンダーなど、専門家とのマッチングも提案したい。渉外担当者として適切な「つなぎ役」を果たすことが、地域の金融機関としての信頼獲得につながる。

強化法・整備法への対応を単なるリスク回避ではなく、信頼獲得のための「攻めの投資」ととらえることが重要だ。金融機関の担当者には、取引先の不安を成長への意欲に変える、一歩踏み込んだ提案が求められる。●

露木 諒 つゆき・りょう
インターネット・アカデミー　最高情報セキュリティ責任者（CISO）

金沢大学院卒。IT研修講師として活躍後、同社のCISO就任。台湾やスリランカなどアジア各国で提供するサイバーセキュリティ研修の講座開発も担当