2026 年 11 月 27 日　全 6 頁

能動的サイバー防御＝「反撃」なのか

サイバー対処能力強化法から読み解く日本の新たなサイバー防御

イノベーション企画部　シニアセキュリティ・スペシャリスト　　横平 健

1　はじめに

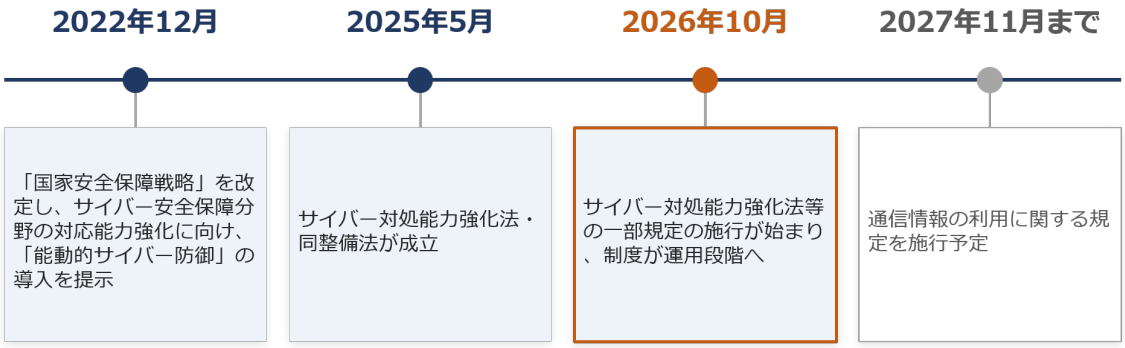
サイバー攻撃の脅威が深刻化する中、その対処に向けた新たな枠組みとして、日本では「能動的サイバー防御」が制度化された。その言葉からは、攻撃者のシステムに侵入して攻撃を阻止する、いわゆる「ハックバック」[1]をイメージする人も少なくないだろう。しかし、能動的サイバー防御を、攻撃者への「反撃」という側面だけで捉えると、その全体像を見誤るおそれがある。

こうした仕組みが導入された背景には、重要インフラの機能停止や破壊等を目的とした重大なサイバー攻撃が、国家を背景とした形でも行われるなど、安全保障上の大きな懸念となっていることがある。政府は 2022 年の国家安全保障戦略でサイバー安全保障分野の対応能力を強化する方針を示し、その具体化として 2025 年に「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（サイバー対処能力強化法）」とその整備法が成立した[2]。2026 年 10 月 1 日からは一部規定の施行が始まり、制度は実際の運用段階に入った。

[1] ハックバック（hack back）とは、サイバー攻撃を受けた際に攻撃者のシステムに直接侵入して反撃や妨害を行う行為を指す。日本では企業や個人によるハックバックは不正アクセス禁止法等に抵触するおそれがある。
[2] 内閣官房「サイバー安全保障に関する取組（能動的サイバー防御の実現に向けた検討など）」（2026 年 11 月 25 日閲覧）

株式会社大和総研 本社　〒135-8460 東京都江東区冬木 15-6
このレポートは投資勧誘を意図して提供するものではありません。このレポートの掲載情報は信頼できると考えられる情報源から作成しておりますが、その正確性、完全性を保証するものではありません。また、記載された意見や予測等は作成時点のものであり今後予告なく変更されることがあります。㈱大和総研と大和証券㈱は、㈱大和証券グループ本社を親会社とする大和証券グループの会社です。内容に関する一切の権利は㈱大和総研にあります。無断での複製・転載・転送等はご遠慮ください。

図表１　能動的サイバー防御をめぐる制度整備の流れ



（出所）各種政府公表資料を基に大和総研作成

制度が動き始めた今、改めて考えたいのが「能動的サイバー防御とは何か」である。攻撃者のシステムに直接対処する仕組みに注目が集まりやすいが、能動的サイバー防御はそれだけを意味するものではない。本稿では、制度の全体像を整理しながら、日本のサイバー防御がどのように変わろうとしているのか、そして企業はその変化を自らのサイバー対策にどう生かすべきかを考える。

2　能動的サイバー防御とは何か

サイバー攻撃への対応というと、企業が自らのシステムを監視し、不正アクセスやマルウェア感染を検知した場合に、その封じ込めや復旧を行う姿がまず思い浮かぶ。しかし、高度化するサイバー攻撃に対して、個々の組織が攻撃を受けてから対応するだけでは、被害を十分に防ぐことが難しくなっている。

こうした課題に対応するために整備されたのが、能動的サイバー防御の仕組みである。特徴は、攻撃を受けた組織が自らのシステムの中だけで対処するのではなく、政府が官民から集まる情報を分析し、必要に応じて攻撃に使われるサーバ等にも対処することで、重大な被害の未然防止や拡大防止を図る点にある。

制度の全体像は、大きく①官民連携の強化、②通信情報の利用、③アクセス・無害化措置の三つに整理できる。

第一の「官民連携の強化」では、基幹インフラ事業者[3]による資産情報の届出やインシデント報告の義務、官民が情報を共有するための協議会などが設けられている。政府と事業者が情報を共有し、それを具体的な対策につなげることで、サイバー攻撃による被害の防止を図るものである。

[3] 基幹インフラ事業者とは、経済安全保障推進法に基づき、電気、金融、航空など、国民生活や経済活動の基盤となる 15 分野において、国が一定の基準に基づき指定する事業者（特定社会基盤事業者）をいう。

第二の「通信情報の利用」は、サイバー攻撃の実態を把握するため、法律に定められた要件と手続きの下で政府が通信情報を利用する仕組みであり、2027 年 11 月までに施行される予定である[4]。憲法で保障される「通信の秘密」等に関わることから、法律上の枠組みや独立機関による監督の下で運用される。

第三が「アクセス・無害化措置」である。攻撃に使用されるサーバ等に一定の措置を講じ、重大な被害の発生を防止する仕組みである。この仕組みが、一般に「能動的サイバー防御」と聞いて最も想起されやすい部分といえる。

図表 2　能動的サイバー防御の全体像（三つの柱）



（出所）各種政府公表資料を基に大和総研作成

3　「反撃」だけでは捉えられない能動的サイバー防御

これら三つの柱に共通するのは、サイバー攻撃による被害が発生した後に対処するだけでなく、攻撃の兆候や脅威を早期に把握し、被害の未然防止・軽減へと対処を広げる点にある。そのために重要となるのが、官民が保有する情報の活用である。

一つの企業が把握できる情報には限界がある。自社への不正アクセスの痕跡やマルウェア、通信ログなどを分析することはできても、その攻撃が自社だけを狙ったものなのか、他社にも同様の攻撃が行われているのか、あるいはより大規模な攻撃活動の一部なのかを判断することは容易ではない。

これに対し、政府には各企業から報告されるインシデント情報に加え、外国政府等との連携によって得られる情報や、政府機関に対する攻撃情報などが集約される。さらに、今後、通信情報の利用が始まれば、そこから得られる情報も分析に加わることにな

[4] 通信情報の利用に関する規定は、公布の日（2025 年 5 月 23 日）から起算して 2 年 6 か月を超えない範囲内において、政令で定める日から施行されることとされている。e-Gov 法令検索「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」附則第 1 条第 4 号（2026 年 11 月 25 日閲覧）

る。こうした複数の情報を組み合わせて分析することで、個々の企業だけでは捉えにくい脅威を早期に把握し、必要な対処につなげることが可能になる。

こうして見ると、能動的サイバー防御は、「攻撃を受けてから反撃する」仕組みというよりも、「情報を基に先回りして被害を防ぐ」仕組みとして捉える方が、その全体像を理解しやすい。

4　アクセス・無害化措置は「反撃」なのか

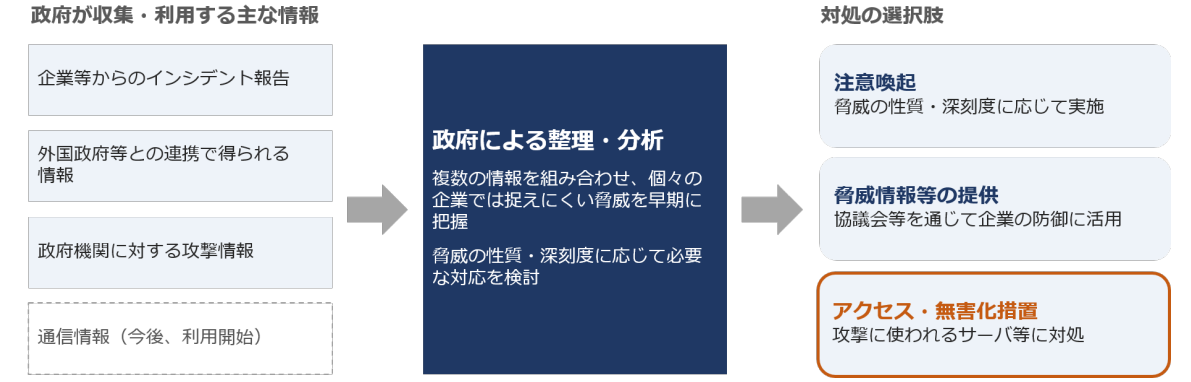
もっとも、能動的サイバー防御の中で、これまでのサイバーセキュリティ政策との違いが際立つのが「アクセス・無害化措置」である。

アクセス・無害化措置では、一定の要件の下で攻撃に使用されているサーバ等にアクセスし、攻撃に使われるプログラムの停止・削除やサーバのシャットダウンなど、必要な対処を行うことが可能となっている。警察が中心的な役割を担い、国外からの高度に組織的・計画的な攻撃などに対しては、自衛隊が警察と共同で対処する仕組みも設けられている。

こうした措置は、攻撃に使用されているサーバ等に直接働きかけるという性質から、「能動的サイバー防御」という言葉と相まって、攻撃者に対する「反撃」と結び付けて捉えられやすい。しかし、制度上の位置付けに着目すると、その目的は攻撃者への報復ではなく、サイバー攻撃による重大な被害の発生を防止することにある。アクセス・無害化措置は、この目的のために法律に定められた要件や手続きに基づいて国が実施する公的な措置である。

政府は、我が国を標的とするサイバー攻撃について情報を収集・分析し、脅威の性質や深刻度に応じて、注意喚起や攻撃に使われるサーバへの対処など、必要な対応を検討する体制を整備している。したがって、アクセス・無害化措置だけを切り出して「反撃」と捉えるのではなく、脅威の把握・分析に基づいて国が取り得る対処の選択肢の一つとして捉えることが適切である。

図表３　能動的サイバー防御における情報活用と対処の流れ



（出所）各種政府公表資料を基に大和総研作成

5　企業は「能動的サイバー防御」をどう生かすか

ここまで見てきたように、アクセス・無害化措置は国が主体となって実施する。そのため、企業の立場から能動的サイバー防御を考える場合、より身近なのは、「官民連携の強化」を自社の防御にどう生かすかという点である。

制度上の義務の対象となる基幹インフラ事業者には、一定の資産情報の届出やインシデントの報告などが求められている。しかし、官民連携は、企業から政府への一方向の情報提供にとどまるものではない。企業や政府機関、海外の関係機関などから集約した情報を政府が分析し、そこから得られた脅威情報等を企業に還元することで、具体的な防御につなげていくことも官民連携の狙いの一つである。

また、こうした情報提供は、直接的な義務を負う基幹インフラ事業者だけに限られるものではない。制度では、官民で脅威情報等を共有するための協議会が設けられている。協議会では、情報の機微度に応じて共有方法を使い分け、秘匿度の高い情報を限定された相手に提供する一方、必要な加工を施した脅威情報等をより幅広く共有する仕組みも設けられている[5]。これにより、直接的な義務の対象ではない企業にとっても、政府が収集・分析した脅威情報等を、自社のサイバー対策に取り入れる機会が広がると考えられる。

ただし、重要なのは、情報を受け取ること自体ではなく、それを実際の防御行動につなげることである。例えば、特定の製品の脆弱性や攻撃に関する情報が提供されても、その製品を自社のどのシステムや端末で利用し、どの業務を支えているのかを把握できていなければ、自社への影響や対応の優先順位を速やかに判断することは難しい。

[5] 協議会には、「協議会フレンズ」と呼ばれる、脅威情報等を幅広く共有するための枠組みが設けられている。内閣官房国家サイバー統括室・内閣府政策統括官（サイバー安全保障担当）「サイバー対処能力強化法等の施行について」（2026 年 9 月）3 頁（2026 年 11 月 25 日閲覧）

そのため企業においては、自社が保有・利用する IT 資産と、それが支える業務との関係を平時から把握しておくことが重要となる。その上で、外部から得られた脅威・脆弱性情報と自社の状況を照合して影響や緊急度を判断し、パッチの適用や監視の強化など、必要な対策に迅速につなげられる態勢を整えておくことが望まれる。

能動的サイバー防御によって、政府が企業に代わってサイバー攻撃から守ってくれるようになるわけではない。官民連携によって得られる情報を実際の防御に生かすためにも、企業自身が平時から必要な備えを進めておくことが求められる。

6　おわりに

サイバー攻撃の脅威は一段と深刻さを増している。2026 年 9 月以降、国内の幅広い分野で不正アクセスや大規模な情報漏えいが相次いでいる[6]ことを受け、政府は 2026 年 11 月 6 日の関係閣僚会議で「サイバーセキュリティ緊急対策パッケージ」[7]を取りまとめた。同パッケージは、サイバーセキュリティの強化を特定の組織や業界だけの問題とせず、社会全体で取り組むべき課題と位置付け、情報の収集・分析と、その結果を対策に活用する循環を通じて、我が国全体の対処能力を高める方針を示している。

こうした状況を踏まえると、官民連携が果たす役割は一層大きくなる。個々の企業だけでは捉えにくい脅威を、官民が持つ情報を通じて早期に把握し、得られた知見を広く共有することが、被害の未然防止や拡大防止につながる。

そのためには、政府が企業の対策に役立つ情報を迅速に提供するとともに、企業もそれを自社への影響と結び付け、具体的な防御行動へとつなげていかなければならない。サイバーセキュリティの強化は、政府や一部の企業だけで完結するものではない。官民がそれぞれの役割を果たし、社会全体で対処能力を高めていくことが求められる。

「攻撃を受けてから守る」だけでなく、「情報を基に先回りして守る」。官民が必要な情報を共有し、それを実際の防御に生かす力を社会全体で高めていくことが、これからの日本のサイバー防御を支える基盤となる。

---

[6] 国内で相次ぐサイバー攻撃の動向や、その脅威の深刻化については、以下のレポートを参照されたい。
坂本博勝「AI によるサイバー攻撃の嵐」（大和総研、2026 年 11 月 10 日）

[7] サイバーセキュリティに関する関係閣僚会議「サイバーセキュリティ緊急対策パッケージ」（2026 年 11 月 6 日）