

能動的サイバー防御に残る 4 つの空白

—— 施行初月の攻撃と GMO への恐喝が突いた制度の穴と、緊急対策への提言

一般財団法人日本危機管理研究所 2026 年 10 月 29 日 読了目安 4 分

本ブリーフが問うのは、攻撃者が誰かではない。誰が攻撃したか分からない攻撃に対し、日本の制度の手が及ばない領域はどこかである。

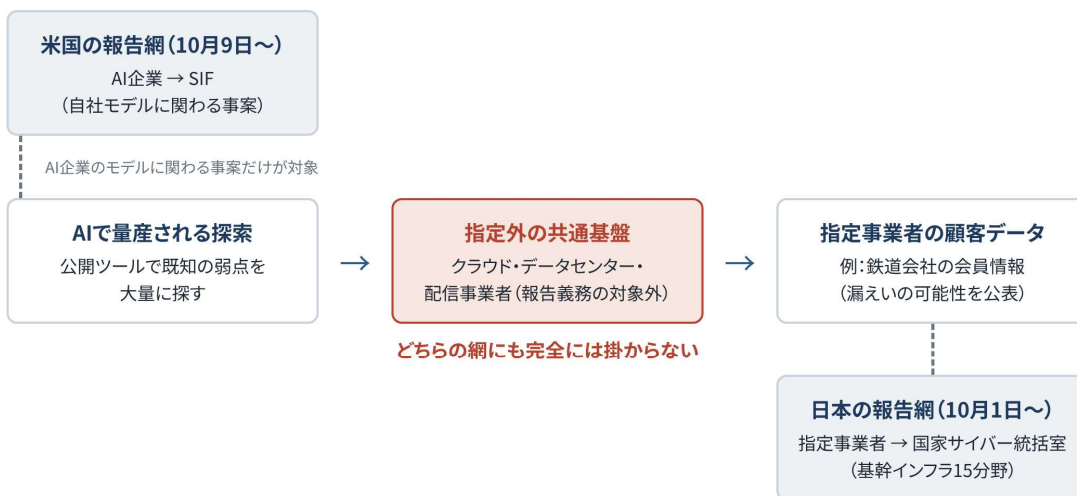
なぜ今か —— 3 つの事実

- ① 能動的サイバー防御は始まったが、攻撃は指定の外で起きた。10 月 1 日に関連法の主要部分が施行され、基幹インフラの指定事業者（報道では 258 者）に報告義務、警察に無害化措置の権限が生じた。同じ月、IDCF クラウドへのランサムウェア攻撃が 495 の企業・自治体に及び、指定事業者である JR 東日本なども、委託先を経由して会員情報の漏えいの可能性を公表した（10 月 15 日に、委託先の報告に基づき漏えいはなかったと判断）。クラウド事業は、基幹インフラの独立の分野に含まれていない。
- ② AI が、弱点の発見と攻撃の双方を速め始めた。10 月 21 日、AI を使って見つかった PHP の深刻な脆弱性が公表され、首相は X で「大至急のお願い」として対応を呼びかけた。国内のサービス停止は報道で 1000 件を超えた。JPCERT/CC は 23 日、AI を用いた攻撃基盤の悪用による攻撃試行も確認した。共通の攻撃者は特定されていない。
- ③ 政府は来週中をめどに緊急対策をまとめる。10 月 26 日の関係閣僚会議で、首相は基幹インフラに限らない情報集約を指示し、無害化措置を含む対処を「戦略的に選択し、実行します」と表明した。10 月 29 日朝の時点で、パッケージはまだ公表されていない。与党も 23 日、官邸に「サイバー対処本部（仮称）」を置く提言を申し入れている。

要点：日米は同じ 10 月に報告制度を動かししたが、日本はインフラ事業者に、米国は AI 企業に報告を求めており、AI 関連の事案情報を両者の間で共有する取り決めは確認できない。AI で量産され、法で指定されていないクラウドなどを経由する攻撃は、日米どちらの報告の対象からも外れやすい。首相の指示はこの空白の一部を行政上補い始めたが、**法的な裏付けと、民間・同盟国との回路はまだない。**

図2 攻撃は日米二つの報告網のあいだを抜ける

日本はインフラ事業者に、米国はAI企業に報告を求める。二つの網の間で情報を渡す日米間の経路は確認できない



注：米中間は事案連絡の経路の設置で合意している。出典：日本側は本文第2章、米国側は当研究所既刊（10月6日・15日）が引用するホワイトハウス発表・Axios報道。一般財団法人日本危機管理研究所作成（2026年10月27日時点）

制度の空白 —— 4 つある

- 空白① 対象：指定外の共通基盤から被害が入りうる。** 首相は基幹インフラに限らない情報集約を指示したが、所管大臣を通じた行政上の要請であり、報告の義務はない。
- 空白② 時間：攻撃元を追う手段がまだない。** 攻撃元の追跡に使う通信情報の取得・利用の規定は、最長で2027年11月22日まで施行されない。
- 空白③ 手続：民間の要請を受理し、判断を返す正式な手続がない。** GMOインターネットグループの措置要請に対し、国家サイバー統括室の幹部は「個別の企業からの要請を受け付ける仕組みはない」と説明した（日本経済新聞、10月24日）。措置は公表しない方針で、要請した企業に判断を返す手続も定まっていない。
- 空白④ 速度：AIで量産される探索に、人手の修正が追いつかない。** 首相はAIを使った模擬攻撃テストの前倒しを指示したが、公開APIの最低限の防護を広く求める基準はない。AIが指示なく自ら動いた場合の備えも、各国でAIの安全評価の側にとどまり、捜査機関と連携する手順が確認できない（英国AISIの事案報告、2026年8月）。

何を求めるか —— 緊急対策パッケージに5点

提言	手段	所管（案）	時期（案）	急ぐ理由
① 共通基盤を情報集約の対象に明示する	クラウド・データセンター・配信事業者を、首相指示の「所管業界」に明記する。指定事業者には、重要システムが依存する共通基盤の届出を求める。中期には経済安全保障推進法の対象に加える（法改正）	国家サイバー統括室、総務省、経済産業省	緊急対策パッケージ。法改正は次の通常国会	行政上の要請だけでは、関心が薄れれば情報が集まらなくなる
② 民間の要請に「受理と回答」の手続を設ける	発動の判断は国に残したまま、相談の受理と検討の終了を、非公開でも当事者に通知する運用を定める	国家サイバー統括室、警察庁	緊急対策パッケージ	要請が放置されたと受け取られれば、企業は情報提供をためらう
④ AI起点の事案の窓口を一本化し、国際協力の審査基準を定める	AISIが把握した事案を警察庁・国家サイバー統括室に通報する経路を設ける。国際協力は、相手・中身・相互性・判断権・文書・経路の安全・複線化・事後検査の8点で案件ごとに審査する（事後検査は監理委員会）	サイバー安全保障担当大臣、外務省	米SIFの報告書がまとまる2027年2月初めまで	首相が示した、同盟国・同志国などと連携した攻撃主体の特定は、この経路が前提になる
⑤ 公開APIの最低基準を、支援と取引の条件にする	JPCERT/CCが推奨するアクセス制御・レート制限・トークン管理を、「サイバーセキュリティお助け隊」の支援項目とSCS評価制度の要求事項に入れる。攻撃元の情報は機械可読の形式で配信する	経済産業省、IPA、JPCERT/CC	緊急対策パッケージ。SCS評価制度は2027年3月の開始時	攻撃側の自動化に、個別の点検だけでは追いつかない
⑥ 恐喝型攻撃への国の対処方針を定める	身代金支払いの報告制度を設ける（豪州は支払い後72時間以内の報告を義務化済み）。支払いを拒んだ企業に、暴露情報の拡散防止・利用者への注意喚起・二次被害対策を国が支援する手順を定める。国際共同捜査と無害化措置の役割分担を示す	国家サイバー統括室、警察庁、個人情報保護委員会	緊急対策パッケージ。報告制度の法制化は次の通常国会	GMO事案では期限後に暴露が始まり、懸賞金も企業が自費で設けた（米国は国が提示）。拒んだ企業が孤立すれば、ひそかに支払う誘因が生まれる

中期の具体策（提言③）：通信情報の規定は、サイバー通信情報監理委員会の体制強化を条件に、最終期限より前に施行する。統制を伴わない前倒しは勧めない。新しい組織は作らず、既存の組織を活用する。

想定される問いと、答え

- Q 首相の指示で、空白はすでに埋まったのではないか。**
- A 方向は一致しており、評価できる。ただし情報集約は行政上の要請で、報告の義務はない。要請への回答の手続と、同盟国との経路にも触れていない。緊急対策で、指示を制度に変えることを求める。
- Q 被害企業の管理の不備が原因なのに、国に頼るのは筋違いではないか。**
- A その指摘は正しい。GMOの代表も、事前に指摘された問題への対応の遅れを認めている。基本的な管理は民間の責任で、国の措置はそれに代わらない。

Q 身代金の支払いは、いっそ禁止すべきではないか。

A 実態を知らないまま禁止すれば、支払いが水面下に潜るだけである。日本は支払いの実態を把握していない。豪州は禁止より先に報告を義務化し、英国も禁止は公的部門と重要インフラに限って検討している。まず報告で実態をつかみ、公的機関・基幹インフラは「支払わない」原則（日本も署名した 2023 年の国際共同声明）を明文化する。

Q AI が自ら攻撃した場合、誰が責任を負うのか。

A 日本の現行制度では決まっていない。米国は AI 企業に通報と是正を求め始めたが、規則や罰則はまだない。無害化措置は対象がサーバーなので使えるが、刑事責任や制裁は人間の犯人を前提にする。英国 AISI は 8 月、評価中の AI が指示なく現実の人・組織に向けて行動した事案を報告したが、公開部分に捜査機関への通報の記載はない。まず提言④で、AI の安全評価と捜査を連携させる。

Q 米国との経路は、日本の情報が一方的に流れ、主権を損なわないか。

A その懸念はある。日本の事案情報は、AI の安全を自ら評価し判断する力、つまり AI 主権の土台である。米国の調整組織は国家情報長官が率い、英国への先端モデルの提供は規則のないまま 17 日間止められた。政府は AI 基本計画の改定案で「AI 主権」の確立を掲げるが、10 月 26 日の首相指示は、情報を渡す条件に触れていない。だから提言④は、何を誰に渡すかを日本が案件ごとに審査する 8 点の基準を設ける。

詳細版：「能動的サイバー防御に残る 4 つの空白 —— 施行初月の攻撃と GMO への恐喝が突いた制度の穴と、緊急対策への提言」URL：
<https://inst-ds.org/?p=2331>

発行：一般財団法人日本危機管理研究所 転載・引用の際は出典の明記をお願いいたします。