弁護士法人　三宅法律事務所

Miyake　& Partners

デジタル・ガバナンス／サイバーセキュリティニュース　No.10

2026 年 10 月 1 日施行
サイバー対処能力強化法

―「自社は対象か」から始める、上場会社の届出・報告・契約実務 ―

平素より格別のご高配を賜っていることに、厚く御礼申し上げる。

2025 年 5 月 16 日に成立し、同月 23 日に公布された「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」（令和 7 年法律第 42 号。一般に「サイバー対処能力強化法」又は「能動的サイバー防御法」と呼ばれる。）について、特別社会基盤事業者による特定重要電子計算機の届出及び特定侵害事象等の報告に関する主要規定が、2026 年 10 月 1 日から施行される。[1]

本法及び同時に成立した整備法による制度は、政府の情報収集・分析、官民の情報共有、一定の通信情報の利用、警察・自衛隊等によるアクセス・無害化措置などを含む大きな制度であるが、上場会社の法務・コンプライアンス担当者にとって最初の問いは、「当社には、何が直接適用されるのか」である。業種名だけで判断すると対象会社を見落とす一方、逆に、基幹インフラ企業と取引があるだけで自社にも届出義務があると誤解するおそれがある。

本ニュースレターでは、サイバーセキュリティを専門としない法務・コンプライアンス担当者を念頭に、①適用対象、②最低限必要な IT・セキュリティ用語、③特定重要電子計算機の考え方、④届出・インシデント報告、⑤IT ベンダー・クラウド・保守委託先への波及、⑥上場会社のガバナンス対応を、できる限り平易に整理する。なお、政令・主務省令は公布済みであるが、2026 年 8 月 17 日時点では、制度解説案、報告様式等の案及び届出除外対象の指定案がなおパブリックコメント中である。[2][3][4][8][9]

令和 8 年 8 月 17 日
弁護士法人三宅法律事務所

本ニュースレターに関するご質問・ご相談
弁護士法人三宅法律事務所
弁護士　渡邉雅之（執筆者）
TEL 03-5288-1021　FAX 03-5288-1025
Email: m-watanabe@miyake.gr.jp

【目次】

1　はじめに――「うちはインフラ企業ではない」で終わらせない

「当社は電力会社でも銀行でもないので、この法律は関係ないのではないか。」――今回の制度を検討するとき、最も避けたいのは、この段階で検討を終えてしまうことである。

確かに、2026 年 10 月 1 日から始まる届出・インシデント報告の中核的な直接義務は、経済安全保障推進法上の「特定社会基盤事業者」のうち、一定の重要なコンピュータを使用する「特別社会基盤事業者」に課される。しかし、法律はこれだけではない。IT 機器、ソフトウェア、クラウド等を供給する事業者には、脆弱性対応に関する別の法的役割がある。また、SOC、MSSP、SIer、保守事業者等は、発注元が法定期限内に国へ報告するため、契約上、より早い通知・ログ提供・調査協力を求められる可能性がある。

最初に確認すること
「当社は何業か」ではなく、①当社又はグループ会社が経済安保法上の指定法人か、②当社が重要システムを使用しているか、③当社が重要インフラ企業へ IT 製品・クラウド・監視・保守等を提供していないか、の順で確認する。

2　まず結論――民間企業への影響は「3 層」で見る

【図表 1】本法における民間事業者の位置付け

層	主な事業者	法的・実務的な意味
第 1 層 中核の直接義務者	特別社会基盤事業者	法 4 条の届出、法 5 条の特定侵害事象等の報告が中心。まず自社の指定状況と対象システムを確認。
第 2 層 別の直接的役割	電子計算機等供給者、電気通信事業者	ベンダーには脆弱性対応の要請や報告・資料提出への努力義務等（法 42 条）。通信事業者には通信情報制度に関する協議等。
参考枠 情報提供等の対象	重要情報を保有する事業者等	特定秘密・重要経済安保情報等を保有する事業者が使用する一定の電子計算機も「重要電子計算機」に含まれる（法 2 条 2 項 3 号）。法 4 条・5 条の義務者ではないが、法 41 条に基づく「周知等用総合整理分析情報」の提供・周知等の対象となり得る。
第 3 層 契約・運用上の波及	SIer、SOC、MSSP、保守、グループ会社、その他取引先	自ら法 4 条・5 条の義務者でなくても、発注元の法定報告を支える迅速通知、ログ提供、原因調査等が契約上求められ得る。

したがって、「法の直接対象ではない」と「何も対応しなくてよい」は同じ意味ではない。法務・コンプライアンス部門は、まず自社の法的位置付けを確定し、その後に契約・委託先管理への波及を確認する必要がある。

3　「能動的サイバー防御」とは何か――企業に「反撃権」を与える法律ではない

「能動的サイバー防御」という言葉から、攻撃を受けた企業が攻撃者のサーバーへ侵入し、反撃できるようになる法律だと受け取られることがある。しかし、その理解は適切ではない。

【図表 2】法律の 5 つの柱

柱	内容	法務担当者の理解
① 官民連携	重要事業者の届出・報告、官民の情報共有、ベンダー脆弱性対応	2026 年 10 月対応の中心
② 通信情報の利用	一定の国外関係通信等を分析し、攻撃検知・防止に活用	別フェーズで施行
③ 分析情報等の提供	政府が分析した脅威情報・脆弱性情報を事業者へ還元	企業側の防御に活用
④ アクセス・無害化	警察・自衛隊等が攻撃用サーバー等へアクセスし、悪用を止めるための措置	政府の権限。直接の根拠は主として整備法（令和 7 年法律第 43 号）による警察官職務執行法 6 条の 2 等の改正。民間企業に「ハックバック」の権限を与えるものではない
⑤ 組織・監督体制	国家サイバー統括室（NCO）、サイバー通信情報監理委員会等	制度の司令塔・監督

用語：アクセス・無害化
攻撃に使われているサーバー等へ一定の法的権限に基づきアクセスし、攻撃に利用できない状態にする措置をいう。企業が自己判断で攻撃者のシステムへ侵入することを認める制度ではない。

4　直接の義務者は誰か——「会社名 → システム」の 2 段階判定

届出・報告義務の対象を判定する際は、業種だけを見るのではなく、次の 2 段階で確認するのが分かりやすい。

【図表 3】直接義務者の判定フロー

段階	確認事項	結論
STEP 1	自社（法人）が、経済安全保障推進法上の「特定社会基盤事業者」として指定されているか。	NO → 原則として法 4 条・5 条の中核義務者ではない。ベンダー等の別ルートを確認。
STEP 2	指定事業に使用する電子計算機の中に「特定重要電子計算機」があるか。所有ではなく「使用」で判断。	YES →「特別社会基盤事業者」として届出・報告義務の対象。

2026 年 7 月 1 日時点では、経済安全保障推進法上の「特定社会基盤事業者」は 258 者である。[5] もっとも、258 者すべてについて、あらゆるサーバーや PC が本法上の届出・報告対象になるわけではない。指定法人であることに加え、具体的なシステムが「特定重要電子計算機」に当たるかを判定する。

グループ会社に注意
子会社が指定されていても、親会社が自動的に法 4 条・5 条の義務者になるわけではない。他方、グループ共通クラウドや認証基盤を指定子会社が「使用」している場合には、システム単位の検討が必要である。

5　どの業種・事業者が指定されるのか

現行制度では、電気、ガス、石油、水道、鉄道、貨物自動車運送、外航貨物、港湾運送、航空、空港、電気通信、放送、郵便、金融、クレジットカードの 15 分野が対象である。2026 年 6 月 17 日公布の改正法では医療分野が追加された。政府は、特定機能病院を念頭に指定する方針を示しているが、2026 年 8 月 16 日時点では当該追加部分は施行前であり、具体的な指定基準は今後の政省令等を確認する必要がある（公布から 1 年 6 月を超えない範囲内で政令が定める日から施行）。[5][10]

重要なのは、同じ業界の企業が一律に指定されるわけではないことである。分野ごとに規模・シェア・設備等の基準があり、事業所管大臣が法人を指定する。以下は、対象判定の入口となる主な基準の要約である。

【図表 4】主な指定基準の目安（インフラ・交通）

分野	主な指定基準（要約）	指定事業者の例
電気	一般送配電・送電等は全者。発電は設備ごとの出力 50 万 kW 以上等	東京電力 PG、関西電力送配電、JERA 等
ガス	一般ガス導管：メーター30 万個以上／製造：20 万㎥/h 以上等	東京ガス NW、大阪ガス NW、JERA 等
石油	石油精製（蒸留設備保有）は全者／LPG 輸入シェア 1%以上等	ENEOS、出光興産、コスモ石油等
水道	給水人口 100 万人超／水道用水供給は 1 日最大 50 万㎥超	東京都、横浜市、大阪市、広域水道企業団等
鉄道	第一種鉄道事業：旅客営業キロ 1,000km 以上	JR 東日本・東海・西日本・北海道・九州
貨物自動車	車両 5,000 台以上＋全国各地への輸送能力	ヤマト運輸、日本通運、佐川急便等
外航貨物（外航海運）	輸送量シェア・運航隻数シェアがいずれも 10%以上	日本郵船、商船三井、川崎汽船
港湾運送	年 80 万 TEU 以上の港湾のコンテナターミナルで荷役	上組、山九、三菱倉庫など
航空・空港	航空：運航便数シェア 25%以上／空港：年間旅客 1,000 万人以上等	ANA・JAL／成田、新関西、関西エアポート、福岡等

【図表 5】主な指定基準の目安（通信・金融・決済）

分野・業態	主な指定基準（要約）	指定事業者の例
電気通信	第一種指定設備／海底ケーブル 10%以上／5G 認定／メッセージ 6,000 万人以上等	NTT 東西、NTT ドコモ、KDDI、ソフトバンク、楽天 M、LINE ヤフー等
放送・郵便	放送：自社制作 25%以上＋対象世帯 25%以上／郵便：郵便事業者全者	NHK、民放キー局／日本郵便
銀行	預金 10 兆円以上 OR 口座 1,000 万以上 OR ATM1 万台以上	3 メガ、りそな、ゆうちょ、主要地銀・ネット銀行等
資金移動	利用者 1,000 万人以上 AND 年間取扱額 4,000 億円以上	PayPay、メルペイ
保険	生保：支払 1 兆円以上 OR 契約 2,000 万件以上／損保も同規模基準	日本生命、第一生命、東京海上日動、損保ジャパン等
証券等	一種金商：預り資産 30 兆円以上 OR 口座 500 万以上／取引所・清算機関・振替機関・資金清算機関等にも別途基準	SBI、野村、大和、楽天、SMBC 日興、みずほ、MUFGMS／東京証券取引所、大阪取引所、日本証券クリアリング機構、証券保管振替機構、全銀ネット等
前払式支払	年間発行額 1 兆円以上 AND 加盟店 1 万店以上	Suica 関係、nanaco 関係、PayPay、PASMO 等
クレジットカード	会員契約 1,000 万以上 AND 年間取扱高 4 兆円以上	JCB、三井住友カード、楽天カード、PayPay カード、クレディセゾン等

上表はあくまで入口である。実際の該当性は、最新の指定一覧と各分野の法令・告示を確認する必要がある。

6　似た名前に注意——「重要インフラ」「特定社会基盤」「特別社会基盤」

【図表 6】似ている 3 つの用語

用語	意味	このニュースレターでの重要性
重要インフラ事業者等	サイバーセキュリティ政策上の概念。重要インフラ行動計画等で用いられる。	経済安保法の指定制度と同じではない。
特定社会基盤事業者	経済安全保障推進法で指定された法人。特定重要設備の導入・重要維持管理等の委託について事前届出・審査を受ける。	本法の中核義務者を絞り込む第 1 段階。
特別社会基盤事業者	上記の指定法人のうち、特定重要電子計算機を使用する者。	法 4 条の届出、法 5 条のインシデント報告の中心。

覚え方

「特定社会基盤事業者＝会社単位の指定」「特定重要電子計算機＝システム単位の該当性判定」「両方がそろうと特別社会基盤事業者」と捉えると整理しやすい。なお、特定重要電子計算機は国が個別に指定するものではなく、政令の要件に照らして事業者が自ら判定する点に注意が必要である。

7　法務担当者のためのサイバー用語早見表

法務・コンプライアンス担当者が、ネットワーク機器の設定方法まで理解する必要はない。ただし、「何が攻撃されるのか」「誰が最初に気づくのか」「どの記録を残すのか」を理解するため、最低限の用語は押さえる必要がある。

【図表 7】まず押さえる基本用語

用語	平易な意味	法務上なぜ重要か
サーバー	社内外の利用者にデータや機能を提供するコンピュータ。メール、会計、認証等。	「対象システム」の中心になる。
ネットワーク	コンピュータ同士を通信でつなぐ仕組み。社内 LAN、インターネット等。	重要設備へ到達できる経路を考える。
クラウド	外部事業者のサーバー等をインターネット経由で利用する形態。	自社所有でなくても「使用」していれば検討対象となり得る。
脆弱性	ソフトウェアや設定上の「弱点」。	悪用される前に修正・通知・ベンダー対応が必要。

用語	平易な意味	法務上なぜ重要か
パッチ	脆弱性や不具合を修正する更新プログラム。	いつ適用したか、適用できない理由を説明できることが重要。
インシデント	セキュリティ上の事故・事象。侵入、感染、サービス停止等。	報告義務・危機対応の入口。
ログ	操作・通信等の「記録」。	原因調査、報告、訴訟・監査の証拠になる。
アラート	監視ツールが不審な動きを検知した警告。	アラート＝法的な「認知」ではない点に注意。

【図表 8】攻撃・監視・組織に関する用語

用語	意味
マルウェア	悪意あるソフトの総称。ウイルス、スパイウェア、ランサムウェア等を含む。
ランサムウェア	データを暗号化したりシステムを停止させたりし、復旧等と引換えに金銭を要求する攻撃。
DDoS	多数の端末から大量通信を送りつけ、Web サイトやサービスを利用しにくくする攻撃。
不正アクセス	盗んだ ID・パスワードや脆弱性を使い、権限なくシステムへ侵入する行為。
EDR	PC やサーバー上の不審な挙動を監視・検知する仕組み。
SOC	セキュリティのアラートを常時監視・分析する組織又はサービス。
CSIRT	インシデント発生時の調査、封じ込め、復旧、社内調整等を担うチーム。
SIer	企業のシステムを設計・構築・導入する事業者。
MSSP	セキュリティ監視・運用を継続的に代行する事業者。SOC サービスを含むことがある。
SLA	サービス水準を契約で定めるもの。稼働率、障害対応、通知時間等を定める。

【図表 9】ネットワーク周辺の用語

用語	意味
FW（ファイアウォール）	通信を許可・遮断する「門番」。
WAF	Web アプリケーションへの攻撃を検知・遮断する仕組み。
VPN	社外 PC 等から社内システムへ安全に接続するための仕組み。
DMZ	外部公開サーバーを社内ネットワークから分離する中間領域。
セグメント	ネットワークを論理的に区切った一区画。
AD／IDaaS	社員の ID・パスワード・アクセス権限をまとめて管理する認証基盤。
DR サイト	災害・障害時に業務を継続・復旧するための予備システム拠点。
アプライアンス	特定用途向けにハードウェアとソフトウェアが一体となった専用機器。

8　特定重要電子計算機――重要設備「そのもの」だけではない

「特定重要電子計算機」と聞くと、発電設備、金融の勘定系、通信設備等を直接制御しているコンピュータだけを想像しがちである。しかし、施行令・主務省令及び 2026 年 7 月 15 日公示の制度解説案は、重要設備へ到達する入口、認証基盤、中継機器、同一ネットワーク区画、重要データ保存系なども含めて考える枠組みを示している。[2][3][4]

【図表 10】重要設備本体以外に検討が必要となる例

類型	例	なぜ重要か
A　インターネット接続口（アタックサーフェス）	Web・メール、FW、WAF、VPN 等	攻撃者が外部から侵入する入口になり得る。制度解説案は、インターネットとの接続口に置かれ、グローバル IP アドレスが割り当てられた一定の機器等を[A]「インターネットとの接続口の機器（アタックサーフェス）」として、特定重要電子計算機の一類型に整理している。
B　認証・認可基盤	AD、IDaaS 等	ID を奪われると、重要設備への正規アクセスに見せかけられる。
C　DMZ・中継	公開系サーバー、中継機器	公開システムから内部へ横展開される経路になり得る。
D　通信制御	ルータ、スイッチ、内部 FW 等	重要設備への通信を制御している。
E　同一セグメント	重要設備と同じネットワーク区画の機器	1 台の侵害が横展開の足掛かりになる。
F　重要データ保存	認証情報、ネットワーク構成、設定情報等の保存系	攻撃に必要な情報を奪われる可能性がある。
G　定期入力系	USB、クラウド等から重要設備へ定期的にデータ入力する系統	外部由来のデータを通じた侵害経路となり得る。

ここで重要なのは、「自社保有サーバーだけ」を棚卸ししないことである。グループ会社所有、外部クラウド、海外所在、共同利用、DR サイト等であっても、指定事業者が実際に「使用」し、法令上の要件を満たせば検討対象となり得る。

実務上のポイント
資産台帳は「所有者」ではなく、「誰が何の業務のために使用しているか」「重要設備へどのようにつながっているか」という観点で作る必要がある。

9 義務① 特定重要電子計算機の届出

特別社会基盤事業者は、特定重要電子計算機について、所定の事項を事業所管大臣へ届け出る必要がある。経済安全保障推進法の「特定重要設備の導入等計画書」が原則として事前届出・審査であるのに対し、本法の届出は導入後の資産把握という性格が強い点が異なる。

【図表 11】届出実務の要点

項目	内容
届出期限	新規導入：原則として導入から 4 か月以内。施行時に既に存在する対象機器：2027 年 3 月 31 日まで。
届出事項の例	製品名、製造者名、特定重要設備との関係、機器類型、クラウドの場合はサービス名・提供者名等。
届出対象の考え方	制度解説案では、アプライアンス（特定用途の専用機器）はハードウェアの製品名・製造者名を届け出る一方、それ以外の機器は OS・ミドルウェア・アプリケーション等のソフトウェアが対象とされ、ハードウェア及びファームウェアは対象外とされている。
注意点	一社又は同一の親法人等を持つ事業者の事業専用で、製品情報が市場に出回っていない専用設計品は除外され得る。もっとも、一般製品の設定変更やアドオンのみでは通常この除外に当たらず、汎用品も自動的に外れるのではなく、両大臣が対象外として指定したものが除外される。届出除外となった場合でも「特定重要電子計算機」自体から外れるとは限らず、インシデント報告の対象にはなり得る。

2026 年 8 月 16 日時点で最終化途上の事項
・報告様式等の案：意見募集は 8 月 17 日 0 時まで[8]
・制度解説案：意見募集は 8 月 19 日 0 時まで[4]
・届出除外対象となる製品等の指定案：意見募集は 8 月 25 日 0 時まで[9]
政令・主務省令は公布済みであるが、実務運用に直結する上記資料は施行前に最終版を再確認する必要がある。

実務では、情報システム部門の資産台帳と、経済安保法対応の調達・導入台帳を別々に管理するのではなく、同じ資産 ID・システム ID を使って連携させることが有効である。

罰則との関係
届出・報告について直ちに刑事罰が科される構造ではなく、法 6 条に基づく是正命令に違反した場合に 200 万円以下の罰金の対象となる（法 83 条）。また、法 9 条に基づく報告若しくは資料の提出をせず、又は虚偽の報告等をした場合は 30 万円以下の罰金の対象となり（法 84 条）、いずれについても法人に罰金刑を科す両罰規定が置かれている（法 86 条）。[1]

10 義務② 特定侵害事象等の報告

【ケース】クラウド側が先に異常を検知したが、3 日後に自社へ通知された

A 社は特別社会基盤事業者であり、特定重要電子計算機の一部をクラウドサービス上で利用している。クラウド事業者は月曜日に当該システムの不審な通信を検知したが、契約には「セキュリティ事故を速やかに通知する」としか定められておらず、A 社への連絡は木曜日となった。A 社は木曜日に初めて具体的な情報を受け、事実確認と法 5 条の報告要否の検討を開始した。

【問】この 3 日間は「クラウド事業者の問題」で済むか。

【結論】済まない。 法 5 条の直接の報告義務者は A 社である。クラウド事業者自身が法 5 条の義務者であるとは限らず、3 日後の通知が契約違反となるかも契約条項による。しかし、委託先が先に異常を検知し得る以上、A 社は、一次通知の期限、24 時間連絡先、ログ・証跡の提供、社内へのエスカレーションを契約・運用で具体化しておく必要がある。通知期限が曖昧であったなら、委託先管理・インシデント対応ガバナンスという A 社側の問題でもある。なお、法令上の「認知」がいつ成立したかは個別の事実関係により判断され、機械的なアラート発報や委託先の検知時点と常に一致するわけではない。

このケースが示すのは、「クラウドへ監視・運用を委託したこと」と「法定報告を行える体制まで委託できること」は別問題だという点である。以下、まず法 5 条の報告対象を整理し、その後に「認知」と委託先からの通知設計を確認する。

本法の報告義務は、「セキュリティ製品からアラートが出たら全部報告する」という制度ではない。次の順番で判定する。

【図表 12】報告要否の 3 段階判定

順番	確認事項	考え方
1	対象となった機器は「特定重要電子計算機」か	NO であれば本法 5 条の報告対象外。ただし、他法令・業法・任意報告は別途検討。
2	特定侵害事象又は省令上の「原因となり得る事象」か	DDoS、ランサムウェア、不正アクセス等を法令上の類型に照らして判定。攻撃が失敗し認証が突破されなかった場合や、マルウェアが即座に駆除された場合であっても、一定の重要な類型の機器については「原因となり得る事象」として報告対象となり得る。
3	省令上の除外に該当しないか	省令が定める除外に当たる事象は報告対象外となる。ただし「未遂であれば一律に報告不要」ではなく、除外は法令・解説案が定める範囲に限られる。

例えば、EDR がマルウェアを検知して自動隔離したケースでも、どの特定重要電子計算機で起きたか、重要設備との接続関係がどうなっているかによって評価が変わり得る。したがって、SOC の検知基準と、法 5 条に基づく報告要否の判定基準を同一にするのではなく、「検知 → エスカレーション → 法的判定」という段階を分ける必要がある。

11 「認知」とは何か——アラートが鳴った時点とは限らない

報告のタイミングを考えるうえで重要なのが、「認知」である。2026 年 7 月 15 日公示の制度解説案は、単なる機械的なアラート発報ではなく、内容を踏まえて法 5 条の事象に該当すると合理的に判断できる状態を重視する整理を示している。[4]

【図表 13】典型的な初動フロー

段階	担当の例	何をするか
① 検知	EDR、SOC、クラウド事業者、保守委託先	不審な動きや障害を検知。
② 事実確認	SOC、CSIRT、情報システム部門	誤検知か、どの機器か、影響範囲はどこかを確認。
③ 法的判定	CSIRT＋法務・コンプライアンス＋責任者	特定重要電子計算機か、法定事象か、除外事由がないかを判定。
④ 国への報告	所管部門＋法務等	事業所管大臣及び内閣総理大臣へ報告（法律上の報告先は内閣総理大臣であり、実務を担う組織が国家サイバー統括室（NCO））。

主務省令は、速報を認知後「速やかに」と定め、詳報は認知日から 30 日以内とする。制度解説案は、こ

の「速やかに」を、DDoS は可能な限り速やかに、ランサムウェアその他は認知日から 3～5 日以内と具体化している。[3][4]

最も詰まりやすいポイント
クラウド事業者や SOC が最初に異常を把握しても、自社への通知が遅ければ法的判定も遅れる。契約上の通知期限、一次連絡先、24 時間連絡方法、ログ保存・提供を事前に決める必要がある。

12 他法令・業法・適時開示との重複

同じサイバー事案について、複数の報告・開示が必要になることがある。ここで重要なのは、制度ごとに別の事故対応フローを作らないことである。「一つのインシデント票」を作り、そこから各制度へ分岐させる方が実務的である。

【図表 14】同一事案で検討し得る主な報告・開示

制度	報告・開示先	主な対象	実務上の注意
サイバー対処能力強化法	事業所管大臣＋内閣総理大臣（事務は国家サイバー統括室（NCO））	特定侵害事象等	速やかな速報＋30 日以内の詳報等。
業法・分野別ガイドライン	金融庁、総務省、国交省等の所管当局	事故、サービス障害、サイバー攻撃等	業界ごとに対象・期限が異なる。
個人情報保護法・番号法	個人情報保護委員会等	一定の個人データ・特定個人情報の漏えい等	「システム停止」と「個人情報漏えい」は別の判定軸。
適時開示・IR	証券取引所・市場	投資判断に重要な事実	国への報告＝直ちに適時開示、ではない。事業・業績影響等を別途判断。
経済安全保障推進法	事業所管大臣	特定重要設備の導入・維持管理等の委託	一般的なサイバー事故報告制度ではなく、主眼は事前届出・審査。

なお、DDoS 及びランサムウェアについては、関係省庁間で共通様式による報告負担の軽減が進められている。[6] もっとも、共通様式を使えば各法令の報告時期や要件が同じになるわけではない。社内では、法令ごとの「報告要否」「期限」「決裁者」を一覧化しておく必要がある。

13 IT ベンダー・クラウド・SIer・SOC・保守事業者への波及

基幹インフラ事業者ではない上場会社でも、自社の事業が「IT を供給する側」に回ると、本法との距離が一気に近くなる。

【図表 15】立場別の影響

立場	法的・契約上の位置付け	準備しておくこと
電子計算機等供給者	ハード、ソフト、クラウド等の供給者。脆弱性が特定重要電子計算機へ影響する場合、電子計算機等供給事業所管大臣から必要措置の要請を受け得る（法 42 条 2 項）。報告・資料提出の求めに応じる努力義務がある（法 42 条 4 項・5 項）。国外に所在する供給者にも適用される（法 42 条 6 項）。	対象製品、構成情報、既知の脆弱性、パッチ、問い合わせ窓口を整理。
SIer・保守	顧客システムの構築・変更・保守を担う。顧客の届出事項や事故調査に必要な情報を保有していることが多い。	変更通知、構成管理、保守ログ、緊急連絡、再委託管理。
SOC・MSSP	顧客より先に侵害を検知する可能性が高い。	一次通知期限、アラートの重要度、ログ提供、24 時間連絡、証拠保全。
一般取引先	対象システムと無関係な商材・役務提供者は、取引があるだけで法 4 条・5 条の義務者にはならない。	ただし、発注元のセキュリティ調達基準・契約条項の強化には注意。

(1)「脆弱性」と「パッチ」を契約でどう扱うか

脆弱性が見つかった場合、顧客が知りたいのは「弱点がある」ことだけではない。影響する製品・バージョン、悪用の可能性、暫定回避策、修正プログラム（パッチ）の提供時期、適用時の停止時間等である。法務部門は、これらを誰が・どの経路で・いつまでに提供するかを契約又は運用ルールに落とし込む必要があ

る。

(2)クラウドでは「責任分界」を確認する

クラウドでは、物理サーバーやネットワークの一部を事業者が管理し、OS・アプリケーション・ID 設定等の一部を利用企業が管理するなど、責任が分かれる。この「どこからどこまでが誰の責任か」を責任分界と呼ぶ。障害や侵害が起きた後に初めて確認するのでは遅いため、SLA・利用規約・個別契約を平時に確認しておく必要がある。

(3)「サイバーインフラ事業者ガイドライン」——法 42 条対応を平時の開発・供給体制に落とし込む

2026 年 3 月 31 日、経済産業省及び国家サイバー統括室(NCO)は「サイバーインフラ事業者に求められる役割等に関するガイドライン」を策定した。同ガイドラインにいう「サイバーインフラ事業者」とは、ソフトウェアの開発・供給・運用を行う事業者を広く捉えるためのガイドライン上の概念であり、法令に基づき個別指定される事業者類型ではない。クラウドサービス、組込みソフトウェア・ファームウェア、システム・サービスの構成要素として提供されるソフトウェアも射程に含まれる。[12][13]

同ガイドラインは、サイバー対処能力強化法の施行ガイドラインそのものではないが、同法・整備法による制度改革と密接に関係する。第一に、整備法によるサイバーセキュリティ基本法の改正により、情報システム等の供給者には、利用者によるサイバーセキュリティの確保に必要な支援を行う努力義務が新設された(同法 7 条 2 項)。同ガイドラインは、この規定を踏まえ、供給者側の平時の取組を具体化するものである。第二に、同ガイドライン 5.7 は、サイバー対処能力強化法 42 条との関係を明示している。サイバーインフラ事業者が同条の「電子計算機等供給者」として情報提供、必要措置の要請又は報告・資料提出の求めの対象となるかは、ソフトウェア等の供給先に応じて判断され、現に重要電子計算機に用いられているものだけでなく、将来的に用いられる蓋然性が高いものも含まれ得る。[13]

【図表 16】サイバーインフラ事業者ガイドラインが示す 6 つの取組領域

取組領域	平易な意味	法務・コンプライアンスの着眼点
① セキュアな設計・開発・供給・運用	設計段階からセキュリティを組み込み、開発・テスト・供給・運用までライフサイクル全体で安全性を確保する。	仕様書・委託契約でセキュリティ要件、テスト、修正責任等が明確か。
② ソフトウェアサプライチェーンの管理	OSS や外部コンポーネントを含む構成情報を把握し、供給者・再委託先を含めてリスクを管理する。	SBOM 等の構成情報、再委託・外部部品の管理、顧客への情報提供を確認する。
③ 残存脆弱性への速やかな対処	脆弱性を収集・評価し、修正プログラム(パッチ)の開発・配布、顧客通知等を行う。	脆弱性受付窓口、PSIRT、パッチ提供、緊急通知の手順を契約・規程に反映する。
④ 人材・プロセス・技術の整備	セキュリティに必要な人材、社内プロセス、技術的な仕組みを継続的に整備する。	責任者・権限・教育・レビュー体制が明確か。
⑤ ステークホルダーとの関係強化	顧客、取引先、セキュリティコミュニティ等との情報共有・協力関係を構築する。	脆弱性・事故情報を誰に、いつ、どこまで知らせるかを事前に決める。
⑥ 顧客によるリスク管理・セキュアな調達	顧客側も供給者を適切に選定し、安全な設定・運用を行うことが求められる。	調達基準、SLA、サポート期間、EOL(サポート終了)後の対応を確認する。

【図表 17】法務担当者が押さえておきたい供給者側の用語

用語	平易な意味	法務上のポイント
セキュア・バイ・デザイン	製品・サービスの設計段階から安全性を組み込み、後から対策を付け足すだけにしない考え方。	仕様・開発委託契約の段階でセキュリティ要件を合意しているかが問題となる。
セキュア・バイ・デフォルト	顧客が追加の費用や複雑な設定をしなくても、初期状態から安全に利用できるようにする考え方。	危険な初期設定を顧客任せにしていないか、初期設定・マニュアル・責任分界を確認する。
SBOM	Software Bill of Materials(ソフトウェア部品表)。製品に含まれるソフトウェア部品やバージョン等を一覧化するもの。	新たな脆弱性が公表された際に、自社製品への影響を迅速に確認する手掛かりとなる。

OSS	Open Source Software。ソースコードが公開され、一定のライセンス条件の下で利用・改変できるソフトウェア。	自社開発部分だけでなく、製品に組み込んだ OSS の脆弱性・バージョンも管理する必要がある。
ファームウェア	機器の内部に組み込まれ、機器を制御するためのソフトウェア。ルータ、IoT 機器、専用装置等で用いられる。	ハードウェア製品でも、内部ソフトの更新・脆弱性対応が必要となることを理解する。
PSIRT	Product Security Incident Response Team。自社製品・サービスの脆弱性やセキュリティ事故への対応を担う組織・機能。	脆弱性の受付、評価、修正、顧客通知、当局対応を一本化する窓口として機能する。

したがって、ソフトウェアを開発・販売・提供・運用する上場会社では、法 42 条に基づく政府からの要請への対応だけを準備すれば足りるわけではない。平時から、セキュア・バイ・デザイン／デフォルト、ソフトウェア構成管理、脆弱性の受付・評価・修正・通知、サポート終了（EOL）までを一連のプロセスとして整備する必要がある。なお、SBOM は上記ガイドラインで活用が示される重要な手段であるが、サイバー対処能力強化法がすべての事業者に一律の SBOM 作成・提供義務を課すものではない。

14　通信情報の利用とアクセス・無害化――施行時期と主体を分けて理解する

本法・整備法による制度全体には、通信情報の利用と、警察・自衛隊等によるアクセス・無害化が含まれる。ただし、両者をまとめて「2026 年 10 月 1 日より後に施行される制度」と理解するのは正確ではない。通信情報関係の規定は公布日（2025 年 5 月 23 日）から 2 年 6 月以内、すなわち 2027 年 11 月 23 日までに別途施行される。他方、アクセス・無害化に関する整備法上の権限は 2026 年 10 月 1 日に施行される。もっとも、これは警察・自衛隊等の政府側の権限であり、民間企業に反撃権やアクセス・無害化の実施義務を与えるものではない。[11]

通信情報制度については、特別社会基盤事業者や電気通信事業者が当事者協定に関する協議を求められた場合、正当な理由がない限り協議に応じる義務が問題となる（法 11 条 2 項、法 13 条）。他方、協定の締結自体は任意とされている。なお、特別社会基盤事業者以外の一般の利用者も、内閣総理大臣との間で当事者協定を締結し、自社が使用する電子計算機のサイバーセキュリティ確保のための分析結果（個別分析情報）の提供を受けることができる（法 12 条）。この場合、協議に応じる義務は課されていない。企業内では、「2026 年 10 月の届出・報告対応」と「別施行の通信情報制度対応」を別プロジェクトとして管理すると分かりやすい。

法務担当者向けの切り分け
まず 2026 年 10 月 1 日に企業側で間に合わせるべきなのは、①対象判定、②特定重要電子計算機の棚卸し、③届出、④インシデント報告フロー、⑤委託先契約である。アクセス・無害化の権限も同日に施行されるが、これは政府側の権限である。通信情報制度は別施行として、企業内の対応プロジェクトを分けて管理する。

15　上場会社のガバナンス・契約実務

【図表 18】法務・コンプライアンス部門が確認すべき 6 項目

項目	確認事項
① 取締役会・内部統制	自社の対象判定、資産台帳、報告体制の整備状況を経営会議・取締役会へ報告し、判断経緯を記録しているか。
② 開示・IR	国への法定報告と適時開示を分けて判断できるか。サービス停止、個人情報漏えい、業績影響等を含む開示基準があるか。
③ 内部監査・監査役等	指定事業者該当性、特定重要電子計算機の網羅性、届出・報告期限、委託先 SLA を監査項目に入れているか。
④ グループ会社管理	指定された子会社の国への報告を、親会社承認待ちで遅らせないルートになっているか。
⑤ 契約・調達	ベンダー通知期限、ログ保存、脆弱性・パッチ、再委託、クラウド責任分界、監査・調査協力を標準条項に反映したか。

項目	確認事項
⑥ 規制ウォッチ	政令・省令は確定済みである一方、2026 年 8 月 16 日時点では制度解説案・報告様式等の案・届出除外対象の指定案が最終化途上。各パブリックコメントの最終版を施行前に再点検する担当者を決めているか。

(1)契約条項で最低限確認したい事項

・通知対象となるインシデント・脆弱性の範囲

・発生又は検知から一次連絡までの時間(例:重大事象は〇時間以内)と、24 時間連絡先

・ログ・証跡の保存期間、形式、提供方法

・原因調査、フォレンジック、影響範囲特定への協力

・パッチ・暫定回避策・脆弱性情報の提供

・再委託先・海外クラウドから必要情報を取得できること

・当局報告、監査、取締役会報告に必要な情報提供

(2)「何時間以内に通知」と書けばよいか

本法が、すべての委託先に一律の「〇時間以内通知」を直接義務付けているわけではない。必要な時間は、顧客側の法定報告期限、24 時間監視の有無、対象システムの重要性等を踏まえて設計する。重要なのは、「速やかに」だけで終わらせず、一次連絡のトリガーと時間軸を具体化することである。

16 施行日までの立場別チェックリスト

【図表 19】A 特別社会基盤事業者

・内閣府の指定事業者一覧で、自社・子会社を法人単位で確認する。

・特定重要電子計算機を、重要設備本体だけでなく、VPN、認証基盤、DMZ、同一セグメント、クラウド、DR サイト等まで含めて棚卸しする。

・資産台帳を「届出対象／届出除外／報告対象」の観点で整理する。

・施行時既存機について 2027 年 3 月 31 日までの届出準備を行う。

・速報・詳報の判定者、代行者、休日夜間の連絡ルートを明確化する。

・個情法、業法、IR を一つのインシデント票から分岐できるようにする。

・クラウド、SOC、保守先の通知・ログ・調査協力条項を見直す。

・取締役会・監査役等への定期報告を設定する。

【図表 20】B ベンダー・クラウド・受託者

・自社が法 42 条の「電子計算機等供給者」に当たる製品・サービスを整理する。

・サイバーセキュリティ基本法 7 条 2 項及びサイバーインフラ事業者ガイドラインに照らし、自社が開発者・供給者・運用者のどの役割を担うかを整理する。

・SBOM、OSS・ファームウェアの構成管理、脆弱性開示、PSIRT、パッチ提供、EOL(サポート終了)までの体制を点検する。

・重要インフラ顧客が利用する製品・バージョン・構成情報を把握できる体制を整える。

・脆弱性情報、既知の影響、パッチ、暫定回避策を迅速に提供できる責任者・窓口を定める。

・政府からの要請・報告・資料提出に対応する社内窓口を定める。

・インシデント一次通知のトリガーと時間軸を SLA・契約に明記する。

・ログ・事故解析情報の保存期間と提供条件を合意する。

・再委託先・海外クラウドから必要情報を取得できるか確認する。

・一般顧客向け契約と、特別社会基盤事業者向け契約の差分を整理する。

【図表 21】C その他の上場会社

・自社が指定法人でないことを最新一覧で確認する。

・グループ会社に指定法人がないか確認する。

・自社が重要インフラ企業へ IT・クラウド・監視・保守等を提供していないか確認する。

・重要インフラ顧客との契約で、新しい通知・監査・脆弱性条項の追加要請が来ていないか確認する。

・既存のサイバーインシデント対応規程に、個情法・業法・IR の判断表を組み込む。

優先順位

①対象判定 → ②資産台帳 → ③報告・通知フロー → ④契約 → ⑤取締役会・監査、の順で進めると整理しやすい。

17 よくある誤解 5 選

誤解 1 電力・銀行等の 15 分野に属する会社であれば、すべて本法 4 条・5 条の届出・報告義務を負う。

【正しくは】業種だけでは決まらない。まず特定社会基盤事業者として法人が指定され、さらに特定重要電子計算機を使用しているかを確認する。

誤解 2 クラウド上のシステムは自社所有ではないため、特定重要電子計算機にはなり得ない。

【正しくは】所有ではなく「使用」が重要である。要件を満たせばクラウドも対象になり得る。

誤解 3 EDR が 1 件アラートを出した時点で、必ず国への報告義務が生じる。

【正しくは】アラートと法的な「認知」は同義ではない。対象機器・法定事象・除外の順に判定する。

誤解 4 IT ベンダーは、特別社会基盤事業者でなければ本法上の法的役割を一切負わない。

【正しくは】電子計算機等供給者には、脆弱性への必要措置の要請（法 42 条 2 項）や、報告・資料提出の求めに応じる努力義務（法 42 条 4 項・5 項）が問題となる。

誤解 5 「能動的サイバー防御法」により、サイバー攻撃を受けた民間企業が攻撃者のサーバーへ自由に侵入できるようになる。

【正しくは】アクセス・無害化は法定要件の下で警察・自衛隊等が行う政府の権限であり、民間企業にハックバック権限を与えるものではない。

18 おわりに

本法対応の出発点は、まず自社が法 4 条・5 条の直接の義務者であるかを正確に判定することである。特別社会基盤事業者であれば、特定重要電子計算機の棚卸し、届出、特定侵害事象等の報告体制が中心課題となる。他方、直接の義務者でない上場会社でも、電子計算機等供給者、クラウド・SIer・SOC・保守事業者として、法的又は契約上の対応が必要となる場合がある。

施行日までの実務では、①対象判定、②資産台帳、③報告・通知フロー、④委託先・ベンダー契約、⑤取締役会・監査の順に整備すると整理しやすい。政令・主務省令は既に公布されているが、制度解説案、報告様式等の案及び届出除外対象の指定案は 2026 年 8 月 16 日時点で最終化途上にある。これらの最終版が公表された段階で、施行前にもう一度、社内規程・届出対象・報告フローを再点検することが重要である。

また、ソフトウェアの開発・供給・運用を行う企業にとっては、本法 42 条だけでなく、サイバーセキュリティ基本法 7 条 2 項及びサイバーインフラ事業者ガイドラインを一体として捉えることが重要である。法 42 条が政府による脆弱性情報の提供、必要措置の要請及び報告・資料提出の枠組みを定めるのに対し、同ガイドラインは、そのような事態に迅速に対応できるよう、平時の開発・供給・運用プロセスを整備するための実務的な指針と位置付けることができる。[12][13]

19 主な参考資料

[1] 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（令和 7 年法律第 42 号）
https://laws.e-gov.go.jp/law/507AC0000000042

[2] 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施行令（令和 8 年政令第 47 号）
https://laws.e-gov.go.jp/law/508CO0000000047/20261001_000000000000000

[3] 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に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令

https://laws.e-gov.go.jp/law/508M60000F5A004/20261001_000000000000000
[4]「サイバー対処能力強化法に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する制度の解説（案）」に関する意見募集（2026 年 7 月 15 日公示）
https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&Mode=0&id=095260710
[5] 内閣府「基幹インフラ役務の安定的な提供の確保に関する制度」（2026 年 7 月 1 日時点の指定事業者等）
https://www.cao.go.jp/keizai_anzen_hosho/suishinhou/infra/infra.html
[6] 国家サイバー統括室「サイバー攻撃時の報告様式の統一について（DDoS 攻撃、ランサムウェア事案）」
https://www.cyber.go.jp/policy/group/cyber/policy.html
[7] 内閣府「サイバー安全保障」
https://www.cao.go.jp/cybersecurity/index.html
[8]「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に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令第四条第二項の特別社会基盤事業所管大臣及び内閣総理大臣が定める様式案」等に関する意見募集
https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&Mode=0&id=095260700
[9]「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に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令第二条第一項ただし書の特別社会基盤事業所管大臣及び内閣総理大臣が指定するもの」（案）に関する意見募集
https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&Mode=0&id=095260720
[10] 内閣官房「第 3 回基幹インフラに関する検討会合 議事のポイント」（2026 年 7 月 7 日）
https://www.cas.go.jp/jp/seisaku/keizai_anzen_hosyohousei/r8_dai17/shiryo1-9.pdf
[11] 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（令和 7 年法律第 43 号）
https://www.shugiin.go.jp/internet/itdb_housei.nsf/html/housei/21720250523043.htm
[12] 経済産業省・国家サイバー統括室「『サイバーインフラ事業者に求められる役割等に関するガイドライン』の日本語版・英語版を策定しました」（2026 年 3 月 31 日）
https://www.meti.go.jp/press/2025/03/20260331001/20260331001.html
[13] 経済産業省・国家サイバー統括室「サイバーインフラ事業者に求められる役割等に関するガイドライン」（2026 年 3 月 31 日）
https://www.cyber.go.jp/pdf/council/cs/ciip/yakuwari/guideline-20260331.pdf

※ 本ニュースレターは、2026 年 8 月 16 日時点で公表されている法令・資料に基づく一般的な解説である。制度解説案、報告様式等の案、届出除外対象の指定案等は今後変更される可能性がある。個別の事案については、最新の法令・告示・所管省庁の資料を確認の上、個別に判断されたい。

以上