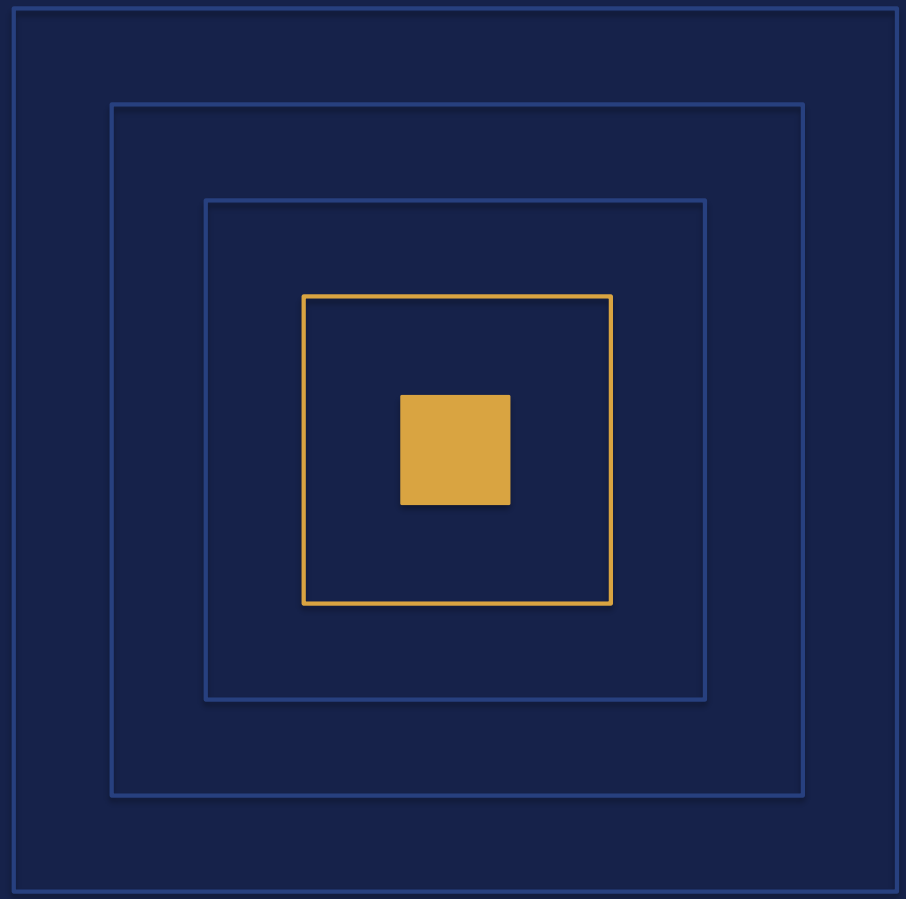
2026年10月1日施行

能動的サイバー防御法の全体像と上場会社の実務対応

サイバー対処能力強化法・同整備法
（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／令和7年法律第42号）



コンプライアンス担当者向け解説セミナー｜2026年8月17日版
弁護士法人三宅法律事務所　弁護士　渡邉　雅之

EXECUTIVE SUMMARY

本日の結論 ― 「誰が対象か」を最初に切り分ける

1

対象判定は「業種」だけでは足りない

まず内閣府の「特定社会基盤事業者」指定リストを確認し、次に自社が「特定重要電子計算機」を使用するかを判定する。

2

2026年10月1日に始まる中核義務は2つ

特別社会基盤事業者には、①特定重要電子計算機の届出、②特定侵害事象等の報告が義務化。通信情報の制度は別フェーズ。

3

ベンダーにも「直接の法的役割」がある

機器・ソフト・クラウド等の供給者は法42条の脆弱性対応に加え、サイバーインフラ事業者GLも確認。委託先には契約上の迅速通知も不可欠。

初心者向け

まず6語だけ — これが分かれば、この後の話は追える

ITの細かな仕組みより、「何が攻撃され、誰が気づき、何を報告するか」を押さえれば十分

01 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。例：メール、会計、認証システム。

02 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やインターネットもネットワークの一種。

03 クラウド

自社に機器を置かず、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。

04 脆弱性

ソフトや設定の「弱点」。攻撃者に悪用されると、
侵入・情報窃取・停止につながる。

05 インシデント

セキュリティ上の事故・事象。侵入、マルウェア
感染、サービス停止などを含む。

06 ログ

システムの操作・通信などの「記録」。事故調査と
国への報告の重要な根拠資料になる。

法務・コンプライアンスが見るポイント

機器の細部ではなく、「対象資産」「認知の時点」「国への報告」「委託先との情報連携」を押さえる。

適用対象

この法律の民間事業者は「3層＋参考枠」で見る

中核の直接義務者

1 特別社会基盤事業者

届出・インシデント報告

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者。会社名の指定＋システム該当性の二段階。

別の直接的な法的役割

2 電子計算機等供給者／電気通信事業者

脆弱性対応・協議等

ベンダー等には脆弱性対応の要請・資料提出の求めへの努力義務。通信事業者には当事者協定等で協議応諾義務。

契約・運用上の波及

3 SIer（システム構築）・SOC（監視）・MSSP（運用代行）・保守・グループ会社等

迅速通知・ログ・調査協力

国への届出・報告主体でなくても、発注元が期限内に報告するため契約上の情報提供・初動協力が必要。

参考：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4・5条の義務者ではないが、法41条の情報提供・周知等の対象となり得る。

直接義務者の判定は「会社名 → システム」の2段階

STEP 1

自社（法人）が「特定社会基盤事業者」に指定されているか

2026年7月1日時点：258者

YES

STEP 2

指定事業に使う電子計算機に「特定重要電子計算機」があるか

所有でなく「使用」で判断

YES

RESULT

特別社会基盤事業者

法4条：届出
法5条：特定侵害事象等の報告

NO

中核の届出・報告義務はなし
（ただしベンダー等の別ルートを確認）

NO

「特別社会基盤事業者」には該当しない
※システム変更時は再判定

実務のコツ

「当社は電力会社／銀行だから対象」と業種だけで決めず、法人単位の指定を確認する。グループ会社が指定されていても、親会社が自動的に義務者になるわけではない。

内閣府：特定社会基盤事業者指定一覧／法2条2項2号・3項

対象業種

現行15分野・258者。医療は「16番目」として追加（施行前）

法律はまず分野を外縁として定め、さらに政令・省令の基準で絞り込み、事業所管大臣が法人を指定・告示する。

01 電気	02 ガス	03 石油	04 水道	05 鉄道
06 貨物自動車運送	07 外航貨物	08 港湾運送	09 航空	10 空港
11 電気通信	12 放送	13 郵便	14 金融	15 クレジットカード

医療

2026年6月17日改正法公布
政府は特定機能病院を念頭に段階的指定の方針
具体的な指定基準・施行日は今後確認

258者（2026年7月1日時点） → 会社名は内閣府の「特定社会基盤事業者として指定した者」で確認

※ 258者＝経済安保法上の「特定社会基盤事業者」。本法の届出・報告主体になるには、さらに特定重要電子計算機を使用して「特別社会基盤事業者」に該当する必要がある。

対象業者を具体化

指定基準の目安（1）― インフラ・交通は「業界全体」ではない

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、各広域水道企業団等
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、西濃運輸、福山通運
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、三菱倉庫など指定事業者多数
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

ポイント：同じ業界の会社が一律に対象になるのではない。まず「指定基準」と「指定済み法人名」を確認する。

内閣府「特定社会基盤事業者として指定した者」（2026/7/1現在）

対象業者を具体化

指定基準の目安（2）— 通信・金融・決済は対象会社がかなり限定される

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5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・ネット銀行など
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／東証・大阪取引所、JSCC、ほふり、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（JR東日本）、nanaco関係、PayPay、PASMO等
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

注意：ここに示すのは判定の入口。法4条・5条の中核義務は、指定法人がさらに「特定重要電子計算機」を使用する場合に生じる。

内閣府「特定社会基盤事業者として指定した者」（2026/7/1現在）

用語の罠

「重要インフラ」「特定社会基盤」「特別社会基盤」は別物

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

重要インフラの行動計画等で用いられる枠組み。経済安保法の指定制度と同一ではない。

特定社会基盤事業者

経済安全保障推進法の指定事業者

特定重要設備の導入・維持管理等について事前届出・審査を受ける。2026/7/1時点258者。

特別社会基盤事業者

サイバー対処能力強化法の中核義務者

上記の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者。届出・インシデント報告を負う。

実務上は

① 指定法人を確認 → ② 特定重要電子計算機を確認 → ③ 本法の中核義務へ

背景

なぜ今、この法律なのか

国が「攻撃後の支援」だけでなく、情報収集・分析・官民共有・通信情報の利用・アクセス／無害化まで含む制度を整備した点が最大の変化

258者

経済安保法上の
指定事業者（2026/7/1）

15分野

現行の対象分野
（医療は追加予定）

2026.10.1

届出・報告の
中核規定が施行

上場会社の視点

「自社は基幹インフラではない」で終わらない。IT製品・クラウド・保守・SOC等を供給していれば法42条の供給者対応が問題となり、委託先なら発注元の報告期限に合わせた通知義務が契約に降りてくる。

全体像

法律の5つの柱 ―「民間の義務」と「政府の権限」を分ける

1	官民連携の強化	届出・報告／協議会／ベンダー脆弱性対応	民間に直接関係
2	通信情報の利用	当事者協定・一定の国外関係通信の取得	別フェーズ
3	分析情報・脆弱性情報の提供	政府分析を事業者・ベンダーへ還元	民間のメリット
4	アクセス・無害化（攻撃基盤の停止）	警察・自衛隊等が攻撃用サーバ等へアクセスし、悪用を止めるための措置（整備法による政府側の権限）	政府の権限
5	組織・監督体制	NCO（国家サイバー統括室）、サイバー通信情報監理委員会	政府の体制

①は企業実務の中心。②通信情報は別施行。④アクセス・無害化は2026年10月1日施行だが、警察・自衛隊等の政府側の権限である。

いつから

施行スケジュールと「何が確定・未確定か」

確定済み

- 施行日：2026年10月1日
- 施行令（令和8年政令47号）
- 主務省令（令和8年8府省令4号）
- 新規導入の届出期限：原則4か月以内
- 施行時既存機：2027年3月31日まで

2026年8月17日時点で最終化途上

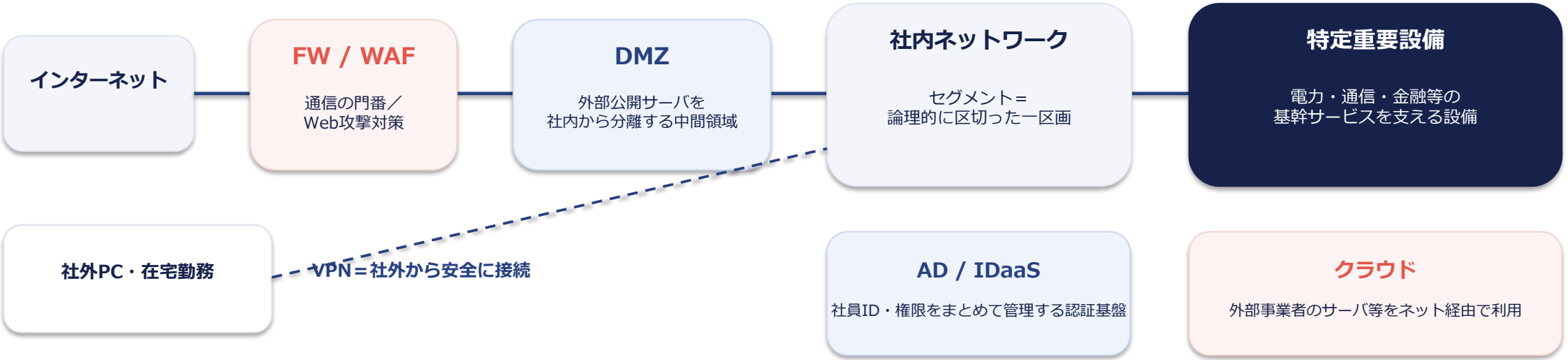
- **報告様式等の案：8月17日0時まで**
- **制度解説案：8月19日0時まで**
- **届出除外対象の指定案：8月25日0時まで**
- **確定法令と案を区別して社内規程を更新**

政令・主務省令は公布済み。一方、実務を左右する解説・様式・届出除外指定は2026年8月17日時点で最終化途上である。

用語を図で整理

「特定重要電子計算機」の頁を読む前に ― 社内ネットワークの超基本

次頁のA～G類型は、設備本体だけでなく「入口・認証・中継・同じネットワーク区画」まで見る考え方である。



なぜ設備本体以外も見るのか

攻撃者は「正面玄関」だけを狙いません。VPNや認証基盤を突破し、DMZや同じセグメントを経由して重要設備へ到達することがある。

義務①の前提

「特定重要電子計算機」は、設備本体だけではない

特定社会基盤事業者が「使用」する電子計算機のうち、特定重要設備の機能停止・低下につながり得るもの。所有者が誰かではなく、実際の使用関係で見る。

①　特定重要設備そのもの／構成機器
制御・基幹設備を構成するコンピュータ

A　接続口（アタックサーフェス）
Web・メール、FW、WAF、VPN等。インターネットとの接続口に置かれ、一定のグローバルIPを持つ機器等。

B　認証・認可基盤
AD・IDaaS等（社員ID・権限をまとめて管理する認証基盤）

C　DMZ（公開系の中間領域）・中継
特定重要設備があるネットワーク区画にアクセス可能

D　通信制御
当該セグメントへの通信を制御する機器

E　同一セグメント（同じネットワーク区画）
特定重要設備と同じセグメントの機器

F　重要データ保存
認証情報・ネットワーク構成等を保存

G　定期入力系
USB・クラウド等から設備へ定期データ入力

「自社保有サーバだけ棚卸し」は危険

グループ会社所有・クラウド・海外所在・共同利用・災害時の予備サイト（DRサイト）でも、「特定社会基盤事業者が使用」し要件を満たせば対象になり得る。

※A～Gは2026年7月15日公示の制度解説案の整理。Aは「インターネットとの接続口の機器（アタックサーフェス）」という特定重要電子計算機の一類型である。

義務①　届出対象と「報告対象」は同じではない

特定重要電子計算機

インシデント報告の母集団

そのうち「届出対象」

- アプライアンス：ハードウェアの製品名・製造者名を届出
- それ以外：OS・ミドルウェア・アプリ等のソフトウェアを届出（ハードウェア・ファームウェアは対象外）
- 専用設計品や、両大臣が指定する製品等は届出除外となり得る

重要　届出除外でも「特定重要電子計算機」自体から外れるとは限らず、法5条のインシデント報告対象になり得る。

届出期限

原則	導入から 4か月以内
施行時に既存	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・機器類型
- クラウド：サービス名・提供者名等

経済安保法の「導入等計画書＝事前審査」と、本法の「導入後の届出」を同じ社内資産台帳で連携させる。

主務省令2条／解説案3-1-1, 3-1-2, FAQ Q1

攻撃・検知の用語

法務が意味だけ押さえる ― 「アラート」から報告判断まで

用語を暗記する必要はない。「どんな攻撃か」「誰が最初に気づくか」を理解すれば、報告フローが見える。

01 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、ランサムウェアなどを含む。

02 ランサムウェア

データを暗号化したりシステムを止めたりして、復旧と引換えに金銭を要求する攻撃。

03 DDoS

多数の端末から大量通信を送りつけ、Webサイト等を利用しにくくする攻撃。

04 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。

検知・対応する側の用語

EDR PCやサーバ上の不審な動きを監視・検知する仕組み

SOC セキュリティのアラートを監視・分析する組織／サービス

CSIRT インシデント発生時の調査・復旧・社内調整を担う対応チーム

EDR等がアラート → **SOCが確認・分析** → **CSIRT・法務が報告要否を判断**

重要：アラート発報 ＝ 法的な「認知」ではない

CASE STUDY

クラウド側が先に検知。3日後に自社へ連絡 — 誰の問題か？

仮想事例

A社＝特別社会基盤事業者。特定重要電子計算機の一部をクラウドで利用し、監視も委託している。

DAY 0

クラウド側が
不審な通信を検知

契約

「事故は速やかに通知」
時間軸は明記なし

DAY 3

A社へ初めて
具体的に連絡

A社

事実確認→
法5条の報告要否を検討

Q　この3日間は「クラウド事業者の問題」で済むか？

① 法定義務

法5条の直接の報告義務者はA社。
委託しても国への報告主体は変わらない。

② 契約・運用

3日後の通知が契約違反かは条項次第。
だから通知期限・24時間連絡・ログ提供を具体化する。

③ 「認知」

法令上の「認知」時点は個別事情で判断。
アラートや委託先の検知と機械的に同一ではない。

教訓：委託しても、「報告責任」と「報告できる体制の設計」までは委託できない。

※ クラウド事業者が法42条の「電子計算機等供給者」に該当するかは、別途そのサービス・供給関係に即して検討する。

義務② 「すべてのアラート」を国に報告するわけではない

判定は「対象機器か → 法定の事象か → 除外に当たらないか」の順に行う。

1 侵害されたのは特定重要電子計算機か？

NO → 本法5条の報告対象外
（他法・任意報告は別）

→

2 特定侵害事象または省令上の「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
法定類型に照らして判定

→

3 省令上の除外に該当しないか？

未遂のみの一部事象など
報告対象外となる場合がある

例：EDRが即時隔離したマルウェア

特定重要設備そのもの／同一セグメントの機器なら報告対象となる場合がある一方、それ以外の特定重要電子計算機では当該事象だけでは報告不要とされる例が示されている。

→ SOCの検知基準と「法5条の報告判定基準」は分ける。ただしエスカレーションは即時に。

報告手続

速報・詳報の2段階。委託先の「最初の認知」がボトルネックになる

報告先

事業所管大臣 ＋ 内閣総理大臣
（NCOが実務を担う）

速報　法令：認知後「速やかに」

解説案による具体化

- DDoS：可能な限り速やかに
- ランサムウェア・その他：認知日から3〜5日以内

詳報　認知日から 30日以内

「認知」の実務

単なるアラート発報ではなく、内容を踏まえ「法5条の事象に該当すると合理的に判断できる状態」。ただし判断は迅速に行う。

契約チェック

- 通知対象となる事象
- 通知方法・一次連絡先
- 発生／認知から通知までの時間
- 必要ログ（操作・通信記録）・証跡の保存／提供

クラウドの契約形態によって、自社と事業者の責任分界が異なる。サービス水準（SLA）・利用規約の通知条項を確認。

実務上の最大の論点

報告義務の重複 ― 経済安保法は「事故報告」ではない

同じサイバー事案でも、報告先・期限・目的が異なる。社内では「一つのインシデント票」から各制度へ分岐させる。

サイバー対処能力強化法	業法・分野ガイドライン	個人情報保護法／番号法	適時開示・IR
報告先 所管大臣＋内閣総理大臣	報告先 各所管当局等	報告先 個人情報保護委員会	報告先 取引所／市場
対象 特定侵害事象等	対象 事故・サービス障害等	対象 一定の漏えい等	対象 投資判断上重要な事実
期限 速やかな速報＋30日以内の詳報	期限 分野ごとの基準・期限	期限 速報・確報等、別基準	期限 法定報告とは別に判断

経済安全保障推進法　主眼は「特定重要設備の導入・維持管理等の委託」の事前届出・審査。一般的なサイバーインシデント報告制度ではない。ただし資産・調達フローは本法と連携させる。

基幹インフラ以外への波及

ベンダーは「単なる間接影響」だけではない

電子計算機等供給者

直接の法的役割あり

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に影響する場合、所管大臣から必要措置の要請を受け得る。報告・資料提出を求められたときは応じる努力義務。国外供給者にも適用あり。

クラウド／SIer（構築）／SOC・MSSP（監視・運用代行）

契約＋運用が核心

委託先が先に侵害を認知することがある

発注元（特別社会基盤事業者）が法5条報告を行うため、迅速通知、ログ（操作・通信記録）・証跡、原因調査、影響範囲の情報共有が必要。サービス水準（SLA）・利用規約を要確認。

一般の取引先

自動的な届出・報告義務はない

対象システムと無関係な商材・役務の提供者等

「基幹インフラ企業と取引がある」だけで法4条・5条の義務者になるわけではない。ただし発注元の調達基準や契約条項としてセキュリティ要件が波及し得る。

供給者は法42条だけでなく、サイバーセキュリティ基本法7条2項と「サイバーインフラ事業者ガイドライン」を平時の体制整備に落とし込む。

サイバーインフラ事業者GL ― 法42条と平時の体制をつなぐ

同ガイドラインは強化法の「施行ガイドライン」そのものではないが、同じ制度改革の中で供給者側の役割を具体化する重要な関連指針である。

① サイバーセキュリティ基本法7条2項

整備法により、情報システム等の供給者に「利用者のサイバーセキュリティ確保に必要な支援」を行う努力義務が新設された。

② サイバーインフラ事業者GL

ソフトウェアの開発・供給・運用を行う事業者を広く想定し、設計・開発・供給・運用の平時の体制を具体化する。

③ 強化法42条

重要電子計算機に用いられる電子計算機・プログラム等の供給者に、脆弱性情報の提供、必要措置の要請、報告・資料提出の枠組みがかかる。

法務の結論

「政府から要請が来たら動く」だけでは遅い。法42条に対応できるよう、平時から開発・供給・運用プロセスを整える。
※「サイバーインフラ事業者」はガイドライン上の概念であり、法令による個別指定事業者ではない。

6つの取組領域 ― 「製品を出したら終わり」ではない

01 セキュアな設計・開発・供給・運用

設計段階から安全性を組み込み、テスト・供給・運用までライフサイクル全体で管理。

02 ソフトウェアサプライチェーン管理

OSS・外部コンポーネント・再委託先を含む構成とリスクを把握。

03 残存脆弱性への速やかな対処

受付・評価・パッチ開発・配布・顧客通知を一連のプロセス化。

04 人材・プロセス・技術の整備

責任者、権限、教育、レビュー、ツールを継続的に整える。

05 ステークホルダーとの関係強化

顧客・取引先・コミュニティと脆弱性・事故情報を適切に共有。

06 顧客のリスク管理・セキュアな調達

顧客側も調達基準、SLA、サポート期間、EOL後の扱いを確認。

法務・コンプライアンス：仕様書・委託契約・SLA・サポート条件に「誰が、いつまでに、何をするか」を落とし込む。

供給者側の6語 — 契約・調達で意味を押さえる

セキュア・バイ・デザイン

設計段階からセキュリティを組み込む。

仕様・開発委託契約の時点で要件を合意。

セキュア・バイ・デフォルト

初期状態から安全に使えるようにする。

危険な初期設定を顧客任せにしない。

SBOM

Software Bill of Materials＝ソフトウェア部品表。

脆弱性公表時に「自社製品に入っているか」を素早く確認。

OSS

Open Source Software。公開ソースを一定条件で利用・改変。

自社開発部分だけでなく組込みOSSの脆弱性も管理。

ファームウェア

機器内部に組み込まれ、機器を制御するソフト。

ハード製品でも内部ソフトの更新・脆弱性対応が必要。

PSIRT

Product Security Incident Response Team。

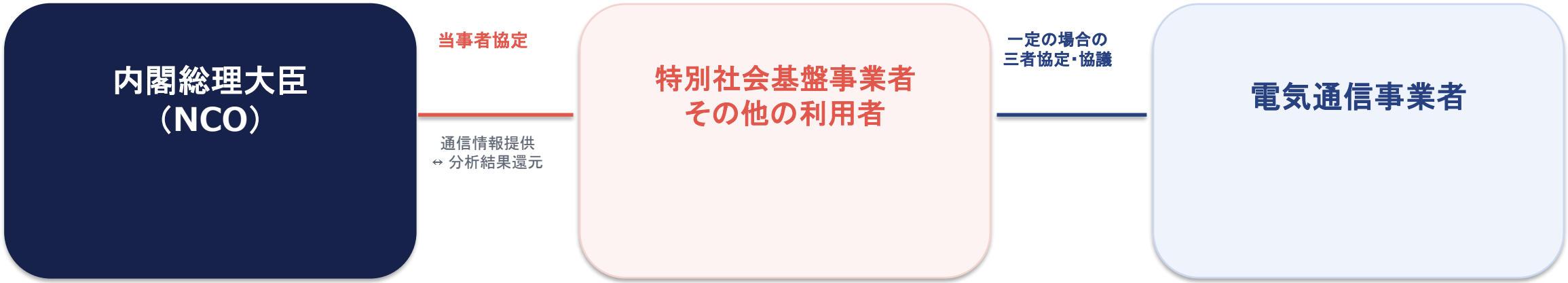
製品脆弱性の受付・評価・修正・顧客通知・当局対応の窓口。

注意：SBOMは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。
加えて、EOL（End of Life＝サポート終了）後の脆弱性対応を契約・調達段階で確認する。

施行時期を分ける

通信情報の利用は別施行 ― アクセス・無害化と混同しない

通信情報関係は公布から2年6月以内（2027年11月23日まで）に別途施行される。2026年10月1日の届出・報告対応とはプロジェクトを分ける。



- 協定の締結自体は任意。特別社会基盤事業者は、求められた場合に正当な理由なく協議を拒めない。
- 電気通信事業者にも一定の場合の協議応諾義務。一般の利用者も任意で協定を締結し、分析結果の提供を受け得る。
- 通信情報関係は2027年11月23日までに別施行。

アクセス・無害化：2026年10月1日施行／警察・自衛隊等の政府側の権限。民間企業に「反撃権」を与えるものではない。

コンプライアンス部門の視点

上場会社のガバナンスにどう落とすか

1 取締役会・内部統制

対象判定、資産台帳、報告体制の整備状況を取締役会・経営会議へ。判断経緯を記録する。

2 開示・IR

国への報告と適時開示は別判断。障害・個人情報漏えい・業績影響等と合わせて開示基準を設計。

3 内部監査・監査役

「指定事業者か」「特定重要電子計算機の網羅性」「期限内届出・報告」「委託先のサービス水準（SLA）」を監査項目へ。

4 グループ会社管理

義務主体は指定された法人。親会社報告を待って国への法定報告が遅れないエスカレーションを作る。

5 契約・調達

通知期限、ログ保存、脆弱性・パッチ、SBOM等の構成情報、再委託、サポート期間・EOL、クラウド責任分界を標準条項へ。

6 規制ウォッチ

政令・省令は確定済み。制度解説・報告様式・届出除外指定は8月時点で最終化途上。GL・評価チェックリストも供給者側で活用する。

施行日までに何をするか ― 立場別チェックリスト

A 特別社会基盤事業者（中核義務者）

- [ ] **内閣府の指定事業者一覧で法人単位の該当性を確認**
- [ ] **特定重要電子計算機をA～G等の類型で棚卸し**
- [ ] 届出対象／届出除外／報告対象の3区分で資産台帳を作る
- [ ] 既存機を2027年3月31日までに届け出る準備
- [ ] 速報・30日詳報の判定者と代行者を明確化
- [ ] 業法・個情法・IRを一元化したインシデント票へ
- [ ] クラウド／SOC（監視）／保守先の通知・ログ条項を改定
- [ ] 取締役会・監査への定期報告を設定

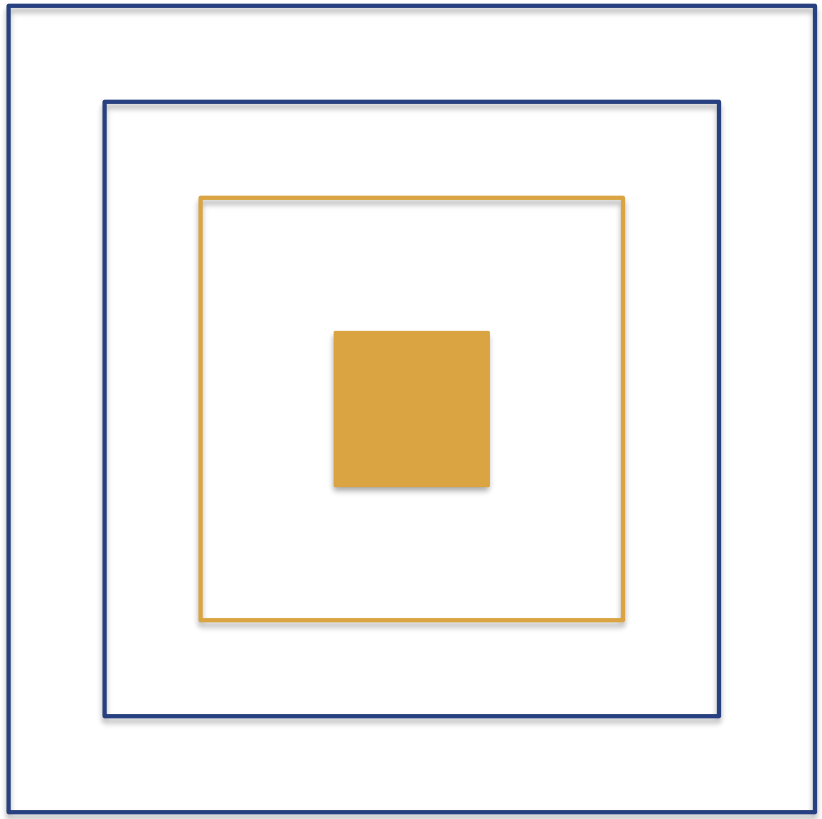
B ベンダー・クラウド・受託者

- [ ] **自社が法42条の「電子計算機等供給者」に当たる場面を整理**
- [ ] **脆弱性要請・報告／資料提出の政府窓口を決める**
- [ ] セキュア・バイ・デザイン／デフォルト、SBOM等の構成管理、脆弱性・パッチ情報を迅速に出せる体制
- [ ] PSIRT等の脆弱性受付・評価・修正・顧客通知の窓口を統一
- [ ] インシデント一次通知の時間軸をSLA・契約に明記
- [ ] ログ・事故解析情報の保存期間と提供条件を合意
- [ ] 再委託・海外クラウドからの情報取得可否を確認
- [ ] サイバーインフラ事業者GLの評価チェックリストで開発・供給・運用体制を点検

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

まとめ

- 対象は「業種」ではなく、まず指定法人、次に特定重要電子計算機の有無で判定する。
- 2026年10月1日の中核義務は、特別社会基盤事業者の資産届出と特定侵害事象等の報告。
- ベンダーは法42条に加え、サイバーセキュリティ基本法7条2項とサイバーインフラ事業者GLを平時の開発・供給・運用へ落とし込む。
- 政令・主務省令は公布済み。制度解説・報告様式・届出除外指定の最終版を施行前に再確認する。



本資料は2026年8月17日時点の公表資料に基づく一般的解説。制度解説案・様式案等は今後変更される可能性があります。

参考資料

主な公的資料（2026年8月17日時点）

1	**サイバー対処能力強化法（令和7年法律第42号）**	法2・4・5・11～17・41・42条等
2	**同整備法（令和7年法律第43号）**	警察官職務執行法・自衛隊法・基本法等を改正
3	**施行令（令和8年政令第47号）＋主務省令（令和8年8府省令第4号）**	対象範囲・届出期限・報告手続
4	**内閣府「特定社会基盤役務の安定的な提供の確保に関する制度」**	15分野・258者・医療追加
5	**内閣府ほか「サイバー対処能力強化法に基づく制度の解説（案）」**	A～G類型、届出・報告実務、FAQ
6	**内閣府「報告様式案」等／「届出除外対象の指定案」**	2026年8月時点パブコメ中
7	**経産省・NCO「サイバーインフラ事業者に求められる役割等に関するGL」**	基本法7条2項・法42条との接続
8	**同ガイドライン 評価チェックリスト等**	開発・供給・運用体制の自己点検

※ 制度解説案・様式案・届出除外対象の指定案は2026年8月17日時点で最終化途上。用語の平易な補足は法務・コンプライアンス担当者向けの一般的説明である。