02

リスク管理

サイバー対処能力強化法の特定重要電子計算機とインシデント報告対象

サイバー対処能力強化法の命令案では特定重要電子計算機の定義やインシデント報告の対象が明文化され、幅広い領域を対象としていることが読み取れる。当事者となる金融機関にはサイバー安全保障分野での対応能力向上という目的を改めて認識することが望まれる。

2026年10月1日より制度運用開始

2026年3月17日、サイバー対処能力強化法及び同整備法[1](以下、本法）の政令[2]が閣議決定され、先般、5月28日には命令案[3]に関する意見募集の結果が公表されるなど制度整備が着々と進みつつある。本法は2026年10月1日より施行される。施行開始から逆算すると、基本方針、政省令を踏まえたガイドラインが公表されてもよい時期ではあるが、本稿執筆時点ではまだ公表されていない。実務への影響が大きいガイドラインは未公表ではあるが、間近に迫った施行開始に向け、事前に少しでも準備に資するよう、ほぼ確定と思われる「特定重要電子計算機の範囲」と「インシデント報告の対象」に絞ってポイントを整理しておきたい。

特定重要電子計算機の範囲

2025年12月8日の有識者会議の資料[4]において指定される特定重要電子計算機はA～Fに類型化されている。

また、政令の規定は

①経済安全保障推進法における特定重要設備[5]

②特定重要設備と直接または間接に接続されている電子計算機[6]

③特定重要設備にデータ（電磁的記録）入力が可能な電子計算機[7]

と要約できる。

類型A～Fは上記の説明で大体の概念は掴むことができるが、類型Cの解釈について重要なポイントを指摘しておきたい。類型Cに該当する見込みの命令案第1条第4項は「特定重要設備に送信される電磁的記録を一時的に保存する機能を有する電子計算機であって、ファイアウォール等を介してのみ当該電磁的記録を送受信することができるもの及び当該ファイアウォール等」と定義されている。ここで、特定重要電子計算機の範囲を特定するにあたってポイントとなるのが③および類型Cに記載のある「電磁的記録」の解釈である。

「電磁的記録」とは、具体的にはプログラムが記載された記録やアプリケーションデータ、データベースのデータ等、あらゆるデータが該当する[8]。つまり経済安全保障推進法（以下、経済安保）対象システムを稼働させるための実行モジュールやセキュリティパッチ等も含まれると考えると、③はリリースする実行モジュールを作成する開発環境で、本番環境の特定重要設備にデータ（電磁的記録）を送信し得るものは本法の対象となる。

また、類型Cには、開発した実行モジュールや配布されたセキュリティパッチ等を経済安保対象システムに反映させるためのライブラリ管理システムも含まれると考える。これについてもライブラリ管理システムに接続している開発環境で、特定重要設備にデータを送信し得るものは対象となる。意見募集の結果では、特定重要設備に対し、ルーティングを介さず通信可能である場合を除き、開発環境は対象外であると書かれている[9]。しかし、

図表1　特定重要電子計算機の類型

A：インターネットとの接続口（アタックサーフェス）の機器等
B：特定社会基盤役務の提供に係るシステムの認証を提供する機器等
C：「特定重要設備」を含むセグメントのDMZ等
D：「特定重要設備」を含むセグメントへのアクセスを制御する機器
E：特定重要設備又は当該特定重要設備と同一セグメントの機器
F：A～Eの特定重要電子計算機に係る重要データ（認証情報等）を保存している機器

（出所）内閣府「サイバー対処能力強化法（官民連携）の施行に向けた考え方の案（資料5）」のP.4を基に野村総合研究所にて一覧化

NOTE

1) 正式名称は「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」「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」。
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の施行期日を定める政令」及び「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」。
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案」。
4) 資料5サイバー対処能力強化法（官民連携）の施行に向けた考え方の案。
5) 政令第1条第3項1号。
6) 政令第1条第3項2号。
7) 政令第1号第3項3号。
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案」に関する意見募集の結果一覧No.7。
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案」に関する意見募集の結果一覧No.3。
10) 命令案第4条第1項第1号ロ～ホ。

③のように、特定重要設備にデータ入力が可能なものは対象となるため、ITベンダーの持ち帰り拠点における電子計算機も調査する必要があることに留意しておきたい。

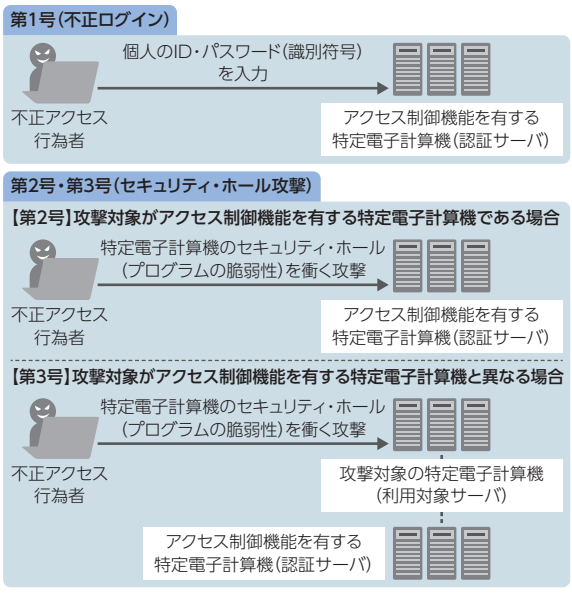
インシデント報告の考え方

経済安保対象システムにおいては、予兆を含むインシデント報告が必要となる。命令案にて特定侵害事象につながる事象が定義された[10]。これらは不正アクセス禁止法における第2条第4項「不正アクセス行為」につながる事象を定義したものと想定される。警視庁ウェブサイト「不正アクセス行為の禁止等に関する法律の解説」が参考となるため以下に引用させていただく。

不正アクセスが発生していない状態でこれらにつながる事象を機械的に検知するのは非常に難しい。どのような状態がこれらの予兆に該当するか事前の検討、取り決めが必要となる。

例えば、パスワードポリシーに違反するログイン試行をモニタリングする、セキュリティ対策ツールで攻撃コードが含まれる通信を検知する、等の対策が考えられるが、インターネットトレードのような経済安保対象システムの場合、これらの事象は日常的に検知して、既に機械的に防御している可能性もある。検知後のインシデント報告も考慮して、現実的に運用可能な範囲で効果的な予兆を定義しておくことが重要だ。

図表2　不正アクセス行為の類型

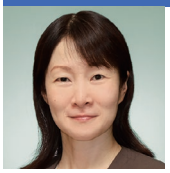


（出所）警察庁「不正アクセス行為の禁止等に関する法律の解説」

実効性のある運用開始に向けて

このように、特定重要電子計算機の特定、インシデント報告のいずれにおいても、定義次第で対象は膨大な量となる。一方で、昨今のサイバー攻撃事例ではサプライチェーンの一端の機器を踏み台にして重要なシステムに攻撃を仕掛けて甚大な影響を及ぼすセキュリティインシデントが多数発生している。本法は、境界防御型セキュリティが突破される脅威を考慮し、内部リスク、サプライチェーンリスクも対象としている。民間企業としては経済安保対象システムの監視基準やセキュリティ構成を今一度、再確認して徹底した安全管理措置を実施する必要がある。

Writer's Profile



鳥居 麻美 Asami Torii

金融リスク管理部長
専門はIT全般統制
focus@nri.co.jp