MORI HAMADA

Data Security Newsletter

2025年2月17日

サイバー対処能力強化法案
～能動的サイバー防御（ACD）関連法案の概説～


弁護士 林 浩美
TEL. 03-5220-1811
hiromi.hayashi@morihamada.com

弁護士 蔦 大輔
TEL. 03-6266-8769
daisuke.tsuta@morihamada.com

弁護士 嶋村 直登
TEL. 03-6266-8977
naoto.shimamura@morihamada.com

弁護士 吉澤 法之
TEL. 03-5293-4892
noriyuki.yoshizawa@morihamada.com

Ⅰ. はじめに

2025年2月7日、内閣官房サイバー安全保障体制整備準備室は、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案（「サイバー対処能力強化法」。以下「新法」といいます。）及び同法律の施行に伴う関係法律の整備等に関する法律案（以下「整備法」といいます。）を国会に提出しました。いわゆる「能動的サイバー防御（ACD[1]）」に関する法律案です。

増大するサイバー攻撃の脅威に対応するべく、2022年12月16日に国家安全保障戦略が閣議決定され、同戦略では、「サイバー空間の安全かつ安定した利用、特に国や重要インフラ等の安全等を確保するために、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させる」ことや、「サイバー安全保障分野における情報収集・分析能力を強化するとともに、能動的サイバー防御の実施のための体制を整備する」ことが明記されました。

ここにいう能動的サイバー防御（ACD）を実現するため、2024年6月以降、内閣官房において「サイバー安全保障分野での対応能力の向上に向けた有識者会議」が設置され、全体会議が4回、テーマ別会合が9回開かれ、同年11月29日には、同有識者会議において、サイバー安全保障分野での対応能力の向上に向けた提言（「サイバー安全保障提言」）が公表されました。

[1] Active Cyber Defence の略。ただし、世界的に共通の定義がある概念ではなく、他国で言う ACD と、日本の報道でよくいわれる ACD が完全に一致するわけではありませんので、その点ご留意ください。

サイバー安全保障提言では、①「官民連携の強化」、②「通信情報の利用」、③「アクセス・無害化」、④「横断的課題」の 4 つのテーマについて述べられており、今般、これらの内容を主軸とした法律案が提出されました。主として、上記①及び上記②について、新法で新制度を創設し、上記③及び上記④について、警察官職務執行法や自衛隊法、サイバーセキュリティ基本法などの関連法の改正によって実現した形です。
新法及び整備法には、多くの新制度と制度改正、また、専門技術的な話が含まれているため、本レターでは、網羅的に取り上げることはせず、ポイントを絞って概説します。

Ⅱ. 政府と民間の情報共有制度（官民連携の強化）

1. 基幹インフラ事業者のインシデント報告義務

新法２章では、基幹インフラ事業者によるセキュリティインシデントの報告義務及びその前提として特定重要計算機の届出義務が規定されています。

基幹インフラ事業者には、経済安全保障推進法[2]に基づき、インフラサービスの提供に用いる制御システム等（特定重要設備・同法 50 条 1 項参照）を導入したり、その設備を他の事業者に維持管理又は操作させる（重要維持管理等の委託）際には、サービスの供給者や委託先に関する情報等を予め主務大臣に届出を行い、審査を受ける義務が課されています。同法にはインシデント発生時の報告義務の定めはありませんでしたが、今般、新法によってその義務が課されることとなります。

(1)特定重要計算機の製品名等の届出義務

経済安全保障推進法によって指定されている 15[3]の重要なインフラ分野のうち、個別に指定された特定社会基盤事業者（経済安全保障推進法 50 条 1 項、同法施行令 9 条。いわゆる「基幹インフラ事業者」を意味します。サイバーセキュリティ基本法上の「重要社会基盤事業者」（いわゆる「重要インフラ事業者」（後述Ⅵ.参照））とは異なる概念です）は、「特定重要電子計算機」を導入したときは、その製品名及び製造者名その他の主務省令で定める事項を事業所管大臣に届け出なければなりません（新法 9 条 1 項）。届出事項に変更があった際にも、軽微なものを除き、再度届出が必要になります（同条 3 項）。

特別社会基盤事業所管大臣は、届出を受けたときは、当該届出に係る事項を内閣総理大臣に通知します（新法同条 2 項、4 項）。ここにいう「内閣総理大臣」とは、整備法に基づき新たに設置されることとなる、司令塔たる内閣官房と実施部門たる内閣府が一体となって機能する新組織（現在の内閣官房内閣サイバーセキュリティセンター（NISC）を改組するもの。以下単に「新組織」といいます）を指すと考えられます（整備法

[2] 正式名称は「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和 4 年法律第 43 号）」
[3] 2024 年の法改正により、港湾運送が 15 番目の分野として加わりました（現時点では未施行）。

に基づく改正後の内閣設置法４条参照)。つまり、届出に関する情報は、各々の基幹インフラ所管省庁と新組織との間で連携される仕組みとなっています。

(2)特定重要計算機と特別社会基盤事業者

「特定重要電子計算機」とは、基幹インフラ事業者が使用する電子計算機(コンピュータはもちろん、そこに組み込まれるプログラムも含まれます(新法 2 条 2 項柱書))のうち、そのサイバーセキュリティが害された場合に、特定重要設備(具体的にはインフラの制御システムなど)の機能が停止し、又は低下するおそれがあるものとして政令で定めるものをいいます(新法２条２項２号及び同条３項参照)。

新法では、「特定重要電子計算機」を使用する基幹インフラ事業者を「**特別**社会基盤事業者」と定義しています(新法２条３項)。トートロジー的な印象もありますが、サイバーセキュリティが害されてもサービスの安定的供給を害する影響を持つようなコンピュータ・プログラムを保持していない基幹インフラ事業者は、経済安全保障推進法上の**特定**社会基盤事業者ではあっても、新法上の**特別**社会基盤事業者には該当しない、といったことも理論的にあり得ることを前提にしていると思われます。

もっとも、実際には、ここにいう特定重要電子計算機を保有しない基幹インフラ事業者はあまり想定されないと思われ、ほとんどの基幹インフラ事業者が、「特定重要電子計算機」を使用する「特別社会基盤事業者」に該当し、主務省令で定められる電子計算機について届出を行う必要が出てくるものと予想されます。したがって、本レターでは、特定社会基盤事業者および特別社会基盤事業者をあわせて「基幹インフラ事業者」といいます。

なお、届出が必要な特定重要計算機については、経済安全保障推進法に基づき既に届出を行っている特定重要設備に関する情報と重複する部分も出てくる可能性がありますが、新法では、経済安全保障推進法上の特定重要設備に影響を与えるような電子計算機について、より詳細に政府が情報を把握することを目的としているため、新法に基づき届出が必要となる範囲は、経済安全保障推進法に基づくものより広がる可能性があります。

(3)基幹インフラ事業者のインシデント報告義務

新法によって、基幹インフラ事業者は、「特定侵害事象」(不正アクセス行為等により特定重要電子計算機のサイバーセキュリティが害されること等・新法２条５項及び同条４項参照)又はその原因となり得る主務省令で定められる事象を知ったときは、その旨及び主務省令で定められる一定の事項を事業所管大臣及び内閣総理大臣(新組織)に報告する義務を課されます(新法５条)。

事業所管大臣は、特定重要電子計算機の届出やインシデントの報告に関して、命令(新法 6 条)、報告徴求(新法９条)、指導・助言(新法 10 条)を行う権限を持ち、内閣総理大臣(新組織)は、事業所管大臣に対して、新法６条に基づく命令をするよう意見を述べることができます(新法７条)。

この報告義務に関しては、①報告対象事象、②報告手続、③報告事項について、全て主務省令で定めることとされており、条文のみでは詳細はほとんどわかりませんが、少なくとも、①の報告対象事象については、(i)新法 2 条 5 項に規定する特定侵害事象または(ii)その原因となり得る事象として主務省令で定めるもの、という 2 つの類型が挙げられている点に留意が必要です。後者については、確定的な事象ではなく、いわゆる「ヒヤリハット」に位置づけられるものも含まれ得るため、主務省令の定めが義務の範囲に大きく影響すると考えられます。次に、②の報告手続及び③の報告事項については、サイバー安全保障提言において、「被害組織の負担軽減と政府の対応迅速化を図るため、インシデント報告先の一元化や報告様式の統一化、速報の簡素化、報告基準・内容の明確化を進めるべき」とされているため、報告義務者となる基幹インフラ事業者の負担軽減が期待されます。

また、特定重要電子計算機の届出やインシデント報告に関する情報について、事業所管大臣及び内閣総理大臣(新組織)には安全管理措置義務が課されます(新法 8 条 1 項)。サイバー安全保障提言では、「報告された情報の利用目的の明確化、機密情報の流出防止、サイバーセキュリティ以外の目的での利用防止を図るべき」とされていますが、報告された情報の目的外利用の禁止などの規定は明示的に措置されていませんので、運用として目的外利用の禁止等が定められる可能性があります。

なお、義務主体となる基幹インフラ事業者に関して、2024 年 10 月 17 日現在、特定社会基盤事業者として指定されている事業者は 213 者(「特定社会基盤事業者として指定された者」)となります。この数字だけを見ると義務主体の数は少ないですが、この 213 者のサプライチェーンに含まれる事業者(システムの供給者や、システムの保守運用の委託を受けている事業者等)を含めると、その数は少なくないと思われます。今日では、サプライチェーンや委託先を狙った攻撃も多数発生しており、独立行政法人情報処理推進機構(IPA)が 2025 年 1 月 30 日に公開した「情報セキュリティ 10 大脅威 2025」においても、サプライチェーンや委託先を狙った攻撃は、組織向け脅威の第 2 位に位置づけられています。サプライチェーンに含まれる事業者において報告対象事象が発生した場合に、新法に基づく義務の対象となるかどうかは明確ではありませんが、いずれにせよ、基幹インフラ事業者がこの義務を履行するためにどのようなオペレーションを組むかは、検討が必要になると考えられます。

(4)基幹インフラ事業者の範囲

医療分野と地方公共団体による行政サービスについては、サイバーセキュリティ基本法に基づく「重要インフラ」分野には含まれていますが、現行の経済安全保障推進法にいう「基幹インフラ」には含まれていません。

しかし、港湾運送を基幹インフラ分野に含めた際の経済安全保障推進法の改正法案(2024 年)に係る衆議院・参議院附帯決議においては、医療と行政サービスについて基幹インフラ分野に含めることを検討すべきとされているため、今後、これらを基幹インフラ分野に含める法改正が行われる可能性もあると考えられます(衆議院:第 213 回国会閣法第 25 号 附帯決議)。

【現行の基幹インフラ分野と所管省庁】

電気（経済産業省）	ガス（経済産業省）	石油（経済産業省）	水道（国土交通省）	鉄道（国土交通省）
貨物自動車運送（国土交通省）	外航貨物（国土交通省）	航空（国土交通省）	空港（国土交通省）	電気通信（総務省）
放送（総務省）	郵便（総務省）	金融（財務省、金融庁等）	クレジットカード（経済産業省）	港湾運送（国土交通省）

2. 情報共有及び対策に関する協議会の設置

サイバー攻撃による被害の防止のための政府と民間との情報共有制度及び対策制度の一つとして、内閣総理大臣（新組織）および関係行政機関の長と重要電子計算機（新法 2 条 2 項）を使用する者や電子計算機及びそれに組み込まれるプログラムの供給者との間において、官民共同の協議会（以下「協議会」といいます。）を設置するものとされています（新法 45 条 1 項）。民間事業者については同意を得た者のみが構成員となります（同条 2 項）。この協議会は、サイバー安全保障提言にいう、「政府が率先して情報提供し、官民双方向の情報共有を促進すべき」とされていることを踏まえたものと考えられます。

協議会の構成員は、サイバー攻撃による被害の防止に資する情報を共有し、サイバー攻撃による被害の防止のための対策に関する事項及び被害防止情報を適正に管理するために必要な措置に関する事項等について協議を行います（同条 3 項）。協議会は、協議を行うため必要があると認めるときは、その構成員に対し、サイバー攻撃による被害の防止に関し必要な情報に関する資料の提出、意見の開陳、説明その他の協力を求めることができ、当該構成員は、正当な理由がある場合を除き、その求めに応じなければならなりません（同条 4 項）。また、構成員は、協議会の求めに応じて資料を提出するときは、当該資料の取扱いに関し意見を付すことができ、意見を付した構成員以外の構成員は、重要電子計算機に対する特定不正行為による被害を防止するため特に必要があると認めるときを除き、その意見に配慮しなければなりません（同条 6 項）。そして、構成員は、共有された情報については守秘義務を負います（同条 4 項、7 項）。

この協議会は、サイバーセキュリティ基本法 17 条に基づき設置されたサイバーセキュリティ協議会を廃止し、強化・新設するものという位置づけです（整備法による改正後のサイバーセキュリティ基本法[4]参照）。サイバー安全保障提言では、「情報共有を行う場合には、TLP[5]など情報共有ポリシーを設定することに加え、攻撃の背景や目的に関する情報などのうち、特に漏えいにより我が国の安全保障に支障を与えるおそれがある情報等を扱う場合にはセキュリティクリアランス制度を活用する等、適切な情報管理と情報共有を両立する仕組みを構築すべき」とされており、2024 年に成立し、2025 年 5 月 16 日に施行される重要経済安

[4] 整備法に基づきサイバーセキュリティ基本法は 2 段階で改正されます（整備法 12 条、13 条参照）。
[5] Traffic Light Protocol の略。情報の共有範囲を信号の色に見立てて定めるものであり、TLP:RED、TLP:AMBER、TLP:GREEN、TLP:CLEAR の 4 つの標示から構成されます。

保情報の保護及び活用に関する法律（いわゆる経済安全保障版セキュリティ・クリアランス法）の活用も示唆されています。新法上は特段セキュリティ・クリアランス制度に関する言及はありませんが、協議会が定める規約等（新法 45 条 8 項）において、関連する運用ルール等が定められる可能性があります。

Ⅲ. 通信情報の利用

1. 背景

サイバー攻撃者は、マルウェアに感染させるなどして乗っ取った通信機器を、攻撃指令を出すサーバ（「C&C（Command & Control）サーバ」と呼ばれます。）から操作することが多いと考えられています。しかも、こうした通信機器や C&C サーバの多くは、日本の執行管轄権の及ばない国外に所在すると推定されています。そして、通常の情報収集の手段では、どのような攻撃がどこから行われるかを事前に知ることが困難であることから、攻撃を受ける側での防御に限界があるとともに、アクセス・無害化等の能動的な防御対応も容易ではありません。したがって、被害を未然に防止するためには、通信情報を分析することにより、攻撃者の実態を把握することが必須となります[6]。

ただし、憲法 21 条 2 項では、通信の秘密が保障されているため、政府が通信の内容を取り扱うことには慎重な対応が求められます。例えば、通信の秘密の例外を定めた通信傍受法では、犯罪関連通信の傍受を行うことが認められていますが、その傍受は、既に行われた一定の犯罪を対象とし、また、裁判官が発する傍受令状が必要となることから、サイバー攻撃による被害を未然に防ぐ目的で通信傍受法を利用することはできませんでした。

そこで、新法は、独立機関であるサイバー通信情報監理委員会を設けることなどを初め、通信の秘密や個人のプライバシーに配慮しつつも、政府がサイバー攻撃の被害を防ぐ目的で、国内を経由する通信情報を取得、分析、そして利用することを可能としています。

2. 政府による情報の取得

政府による情報の取得は、基幹インフラ事業者との協定（同意）を必要とするパターンと、サイバー通信情報監理委員会の承認を条件に当該同意を必要としないパターンの 2 パターンがあります。サイバー通信情報監理委員会は、新法に基づき新設されるいわゆる 3 条委員会[7]となります。

[6] サイバー安全保障提言 5 頁参照

[7] 独自に意思決定を行う機関であり、他の 3 条委員会として、例えば公正取引委員会や個人情報保護委員会などが挙げられます。

(1)協定(同意)に基づく通信情報の取得

内閣総理大臣(新組織)は、基幹インフラ事業者との間で、当該基幹インフラ事業者を通信の当事者とする通信情報の提供を受けて、外内通信(国外から国内への通信)に係る通信情報を用いて、サイバーセキュリティの確保を図るために必要な分析を行い、その分析の結果を当該基幹インフラ事業者に提供することを内容とする協定を締結することができます(新法 11 条)。

(2) 同意を必要としない通信情報の取得

次に、基幹インフラ事業者との協定(同意)を必要としないパターンについては、次の 2 類型がありますが、いずれもサイバー通信情報監理委員会の事前承認が条件となります。

ア 外外通信(国内を経由し伝送される国外から国外への通信)分析のための取得

内閣総理大臣(新組織)は、外外通信であって、他の方法ではその実態の把握が著しく困難であるサイバー攻撃に関係するものが、特定の電気通信設備により伝送されていると疑うに足りる状況がある場合には、サイバー通信情報監理委員会の承認を受けて、当該電気通信設備から、内閣総理大臣(新組織)の設置する設備(以下「受信用設備」といいます。)に、通信情報が送信されるようにする措置をとることができます(新法 17 条)。

イ 外内通信又は内外通信(国内から国外への通信)の分析のための取得

内閣総理大臣(新組織)は、外内通信又は内外通信であって、サイバー攻撃に用いられていると疑うに足りる状況のある特定の外国設備と送受信し、又は当該状況のある機械的情報[8]が含まれているものの分析をしなければ被害防止が著しく困難であり、他の方法ではこれらの通信の分析が著しく困難である場合には、サイバー通信情報監理委員会の承認を受けて、これらの通信が含まれると疑うに足りる外国関係通信を伝送する電気通信設備から、受信用設備に、通信情報が送信されるようにする措置をとることができます(新法 32 条、33 条)。

3. 取得した情報の選別

内閣総理大臣(新組織)は、上記の手段で取得した通信情報を、プログラムなどの自動的な方法により選別することが求められています。具体的には、コミュニケーションの非本質的な情報(機械的情報)であって調査すべきサイバー攻撃に関係があるもののみを、サイバー通信情報監理委員会から承認を受ける際に定

[8] アイ・ピー・アドレス、通信日時、電子計算機に動作をさせるべき指令を与える情報(指令情報等)等、コミュニケーションの非本質的な内容の情報(新法 2 条 8 項参照)

めた基準に基づき選別し、それ以外の情報（例えば、コミュニケーションの本質的な情報など）は直ちに消去しなければなりません（新法 22 条、35 条）。なお、メールアドレス（ドメイン名以外の部分）を取り扱う際には、特定の個人を識別することができないように非識別化措置を講じる必要があります（新法 24 条）。

＜電子メールに係る通信情報を、コミュニケーションの本質的な情報又は非本質的な情報に分類した例＞

黄色ハイライト部分が「コミュニケーションの本質的内容」に相当。

情報のカテゴリー	分類	通信情報の具体例
送信者メールアドレス	非本質的	From: hanako1@example.jp ※非識別化が必要
宛先メールアドレス	非本質的	To: taro2@cas.go.jp ※非識別化が必要
件名	本質的	Subject: 重要書類の送付について（至急）
送信日時	非本質的	Date: 2012/03/25 10:37
送信元メールアドレス（システムエラー時の返信先）	非本質的	Return-Path: <mail-system@example.jp> ※非識別化が必要
受信側組織内の伝送の記録	非本質的	Received: from mail.cas.go.jp ([198.51.100.3]) by aa00bb01.cas.go.jp id <20120325103715817.****.****60@aa00bb01.cas.go.jp >; Sun, 25 Mar 2012 10:37:15 +0900
受信側メールサーバでの迷惑メール判定結果	非本質的	Authentication-Results: cas.go.jp; spf=pass reason=policy; sender-id=pass reason=policy
送信側メールサーバから受信側メールサーバへの伝送の記録	非本質的	Received: from example.jp (mail. example.jp [203.0.113.1]) by cas.go.jp with ESMTP id D098B19 for <taro2@cas.go.jp>; Sun, 25 Mar 2012 10:37:15 +0900 (JST) ※メールアドレスについて非識別化が必要
送信側組織内の伝送の記録	非本質的	Received: from hnkwinpc ([192.0.2.6]) by mail.example.jp with ESMTP id D098A05; Sun, 25 Mar 2012 10:37:03 +0900 (JST)
送信側で付した番号	非本質的	Message-ID: <IMTw1fOIffff0KsJ@example.jp>
本文の符号化の方式	非本質的	MIME-Version: 1.0 Content-Type: multipart/alternative ; boudary= ”_Part_28873_0A61” Content-Transfer-Encoding: 7bit
本文	本質的	内閣官房サイバー準備室 御中

（実際には符号化されて伝送。右欄は復号化後の内容。以下同じ。）		お世話になっております。 添付の至急ご確認をお願いします。 〇〇花子 拝
添付ファイル内 （技術的には本文の一部）	本質的	重要書類.docx
添付ファイルの内容 （技術的には本文の一部。通常は表示されない不正コマンドが含まれる場合がある）	添付ファイルの内容は本質的だが、不正コマンドは非本質的	これは重要書類です。直ちに保存して、なるべく多くの方に共有をお願いします。よろしくお願いします。 84 a7 f3 9b 61 c1 08 99 27 1d 44

（出典：令和 7 年 2 月内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法案及び同整備法案について」より）

4. 取得した通信情報の厳格な取扱い

内閣総理大臣（新組織）は、取得した通信情報に関し、選別前の通信情報を利用し又は提供すること、及び、選別後の通信情報についても、関係行政機関に分析協力を要請する場合、アクセス・無害化を行う行政機関に提供する場合等を除いては提供することが禁止されており（新法 23 条）、安全管理措置義務も必要となります（新法 26 条）。また、2 年以内の範囲で保存期間を設定する必要があります（新法 25 条）。

Ⅳ. 分析情報・脆弱性情報の提供等

内閣総理大臣（新組織）は、基幹インフラ事業者から届出された特定電子計算機の情報及び報告されたインシデント情報（新法 2 章）、選別された後の通信情報（新法 5 章、7 章）、協議会を通じて得た情報（新法 9 章）、その他の情報（外国政府から提供された情報等）を整理及び分析をすることができます（新法 37 条）。

この整理及び分析された情報については、その情報の守秘性に応じて 3 つのカテゴリーに分けて、それぞれ、(a)国の行政機関、(b)協議会、(c)特別社会基盤事業者及び電子計算機等の供給者に提供されることになっています。具体的には、(a)通信情報や秘密を含み得る情報については総合整理分析情報として国の行政機関に（法 38 条）、(b)通信情報は含まないが秘密は含み得る情報については提供用総合整理分析情報として協議会の構成員等に提供されます（新法 45 条）。そして、(c)通信情報や秘密は含まない情報については周知等用総合整理分析情報として、基幹インフラ事業者、重要電子計算機の使用者及び重要電子計算機等の供給者に対し、提供、周知又は公表がなされます（新法 40 条～42 条）。

なお、コンピュータやプログラム、情報通信ネットワーク又は電磁的記録媒体などの情報システム供給者に

は、利用者のサイバーセキュリティ確保のための設計・開発、情報の継続的な提供等に努めるものとするという責務規定が置かれます（整備法による改正後のサイバーセキュリティ基本法（以下「改正サイバーセキュリティ基本法」といいます。）7 条 2 項）

V. アクセス・無害化

1. 背景

サイバー攻撃は、現実空間における危険とは質的に異なり、実際にある危険が潜在化し認知しにくいという特徴があります。また、潜伏の高度化により、攻撃者の意図次第でいつでもサイバー攻撃が実行可能になるとともに、ネットワーク化の進展により、一旦攻撃が行われれば、被害が瞬時かつ広範に及ぶおそれがあります。しかし、実際にこうしたインシデントが起こってから令状を取得し、捜査を行う刑事手続では、被害の未然防止・拡大防止には対応できません。

そこで、従来より、災害時の避難措置や危険物による切迫した事態への対処など、必要に応じて関係機関が相互に連携することを含めて、令状を必要とすることなく、危害防止のために臨機応変かつ組織的に対処する際に機能してきた警察官職務執行法（以下「警職法」といいます。）を参考に、整備法では、サイバー攻撃による重大な危害を防止するための警察・自衛隊による措置等を可能とし、その際の適正性を確保する手続を新たに定めています[9]。これらの活動には、令状を不要とする代わりに、原則としてサイバー通信情報監理委員会の承認が必要とされており、これにより業務の適正手続を担保しています。

アクセス・無害化のステップ（イメージ）

① アクセス：
攻撃に使用されているサーバー等が持つ脆弱性を利用するなどして、遠隔からログインを実施。
※なお、当該サーバー等が攻撃者によって現に乗っ取られているような場合には、（攻撃者自身が自ら侵入に利用した弱点を塞ぐことをしていない限り）非正規の侵入手段が存在するものと想定される。

② 攻撃のためのプログラム等の確認：
インストールされているプログラム一覧、作動している攻撃のためのプログラム等を確認。

③ 無害化：

[9] 以上、サイバー安全保障提言 10-11 頁

当該サーバー等が攻撃に用いられないよう無害化。
（無害化の方法の例）
・インストールされている攻撃のためのプログラムの停止・削除
・攻撃者が当該サーバー等へアクセスできないよう設定変更など

（出典：令和７年２月内閣官房サイバー安全保障体制整備準備室「サイバー対処能力強化法案及び同整備法案について」より）

2. 警察によるアクセス・無害化措置

（1）アクセス・無害化措置の実施条件

警察によるアクセス・無害化措置の実施条件は、警察庁長官が指名する警察官（サイバー危害防止措置執行官）が、サイバー攻撃又はその疑いがある通信等を認めた場合であって、そのまま放置すれば、人の生命、身体又は財産に対する重大な危害が発生するおそれがあるため緊急の必要があるときです（整備法による改正後の警職法（以下「改正警職法」といいます。）6 条の 2 第 2 項）。

（2）アクセス・無害化措置の内容

サイバー危害防止措置執行官は、アクセス・無害化措置として、そのサイバー攻撃の送信元等である電子計算機の管理者その他関係者に対し、危害防止のため通常必要と認められる措置であって電気通信回線を介して行うものをとることを命じ、又は自らその措置をとることができます（改正警職法 6 条の 2 第 2 項）。

（3）手続的要件

サイバー危害防止措置執行官が、上記の措置をとる場合には、原則として、サイバー通信情報監理委員会の事前承認を得ることが必要です（改正警職法 6 条の 2 第 4 項本文）。ただし、当該承認を得る時間的余裕がないなどの特段の事由がある場合には、事前承認に代わって、措置の実施後速やかに、サイバー通信情報監理委員会に通知することが求められます（改正警職法 6 条の 2 第 4 項但書及び 9 項）。

また、措置の対象となる電子計算機が国内に設置されていない可能性が高い場合には、警察庁の警察官のみが措置をできることになっており、さらに、外務大臣との事前協議が求められます（改正警職法 6 条の 2 第 3 項）。

3. 自衛隊によるアクセス・無害化措置の概要

アクセス・無害化措置は、警察ではなく、自衛隊が警察と共同して行うことも認められています。

その概要を説明すると、まず、その要件は、内閣総理大臣が、一定の重要電子計算機に対する攻撃であって、日本国外にある者による特に高度に組織的かつ計画的な行為と認められるものが行われた場合において、自衛隊が対処を行う特別の必要があると認めるときです。そして、その措置として、内閣総理大臣は、当該重要電子計算機への被害を防止するために必要な措置であって電気通信回線を介して行うもの（通信防護措置）をとるべき旨を命ずることができます。この命令を受けた部隊等は、警察と共同して当該通信防護措置を実施することになります。手続については改正警職法が準用され、原則としてサイバー通信情報監理委員会の事前承認を要するという点は警察による措置と同様です（以上、改正自衛隊法 81 条の 3、91 条の 3 及び 95 条の 4）。

VI. 横断的課題（組織・体制整備）

サイバーセキュリティについての組織体制を強化するため、改正サイバーセキュリティ基本法では、サイバーセキュリティ戦略本部の組織構造が再編成されます。

サイバーセキュリティ戦略本部は、これまで内閣官房長官を本部長として、一部の国務大臣のみを本部員としていましたが、改正後は、内閣総理大臣を本部長とし、全ての国務大臣を本部員とする組織に改組するとともに、別途、有識者から構成されるサイバーセキュリティ推進専門家会議が設置されます（改正サイバーセキュリティ基本法 28 条、30 条、30 条の2）。国家安全保障戦略では、サイバーセキュリティ戦略本部の事務局として機能する内閣官房内閣サイバーセキュリティセンター（NISC）を改組するとされていますが、こちらは政令（内閣官房組織令）で措置される予定です。

また、改正サイバーセキュリティ基本法では、サイバーセキュリティ戦略本部の所掌事務も見直され、いわゆる重要インフラ事業者等のサイバーセキュリティ確保に関して国の行政機関が実施する施策の基準の作成と、国の行政機関、独立行政法人及び指定法人の情報システムに対する不正な活動であって情報通信ネットワーク又は電磁的記録媒体を通じて行われるものの監視及び分析が追加されます（同法 26 条 1 項 3 号、4 号）。

ここにいう重要インフラ事業者とは、サイバーセキュリティ基本法3条1項に規定される「重要社会基盤事業者」です。通信・電力・金融などの 15 分野に属する事業者の一部の事業者を指し、基幹インフラ事業者とは若干範囲が異なりますが、どちらも我が国において重要性の高いインフラであることは変わりません。

現状、サイバーセキュリティ基本法 14 条及び 26 条 1 項 5 号に基づき、「重要インフラのサイバーセキュリティに係る行動計画」及びその下位規範として「重要インフラのサイバーセキュリティに係る安全基準等策定指針」が公表されています。改正サイバーセキュリティ基本法 26 条 1 項 3 号にいう重要インフラ事業者に関する施策の基準が何を指すかは条文からは明確ではありませんが、この行動計画等に明確な法的根拠を与えている、または、行動計画等を発展させて新たな基準・ガイドラインを策定する可能性があると考えられます。

Ⅶ. 施行期日

新法は、原則として公布から 1 年 6 か月以内に施行され（新法附則 1 条柱書）、整備法も新法の施行日と同日に施行されますが（整備法附則 1 条柱書）、新法に基づくサイバー情報監理委員会の設置は公布から 1 年以内（同条 3 号）、「通信情報の利用」（上記Ⅲ）については、公布から 2 年 6 か月以内（同条 4 号）とされています。また、整備法に基づくサイバーセキュリティ戦略本部の改組等については公布から 6 月以内とされています（整備法附則 1 条 2 号、新法附則 1 条 2 号）。

なお、基幹インフラ事業者による特定重要電子計算機に関する届出（4 条 1 項）については経過措置があり（新法附則 4 条）、基幹インフラ事業者は、現に導入している特定重要電子計算機に関する製品名や主務省令で定められる事項について、新法の施行の日から 6 月以内に所管大臣に届け出る必要があります。