

No.	御意見の要旨	御意見に対する主な考え方
1	サイバー攻撃の問題は、現代において多発している。 解決策 #1 重要機密事項の文書化推進。 #2 重要機密事項は、各自治体 各自治体の 図書館を設置して、閲覧可能にする。 #3 国民の知る権利の制定。 #4 国民の知る権利の啓蒙活動。 #5 デジタル化移行なら、日本国での、サイバーセキュリティの高度化。 #6 サイバーセキュリティの高度人材の確保。 #7 サイバーセキュリティ人材の労働環境の改善策制定。	頂いた御意見は、今後の参考といたします。
2	重要インフラのサイバーセキュリティ対策に関する意見書 この度、重要インフラのサイバーセキュリティ強化に関する意見募集に対し、以下の通り意見を提出いたします。 1. 被害額の適正な評価と罰則の強化 サイバー攻撃および物理的破壊・盗難に対する罰則を大幅に強化すべきです。現行の被害額算定は、ハードウェアや銅線などの資産価値のみに偏る傾向がありますが、実態はより深刻です。以下の項目を「被害額」として包括的に含め、それを基準とした厳格な罰則規定を設けることを求めます。 ・新システム導入および習熟のための研修コスト ・物理的復旧に伴う付帯施工費用 ・システム復旧までの営業損害および社会的損失 2 また、悪質な実行犯に対しては、日本への入国禁止措置等の実効性ある制裁を講じるべきです。 2. 企業における対策義務化と罰金制度の導入 企業側に対しても、サイバー攻撃や盗難に対する防御体制の構築を義務化すべきです。「被害を受けた企業」を単なる弱者として保護するのではなく、「対策不足であった企業」に対しては罰金を課す制度が必要です。これにより、企業が自発的かつ強力にセキュリティ体制を強化するインセンティブを政府が作り出すべきです。 3. 国民意識の向上と政府主導のシステム構築 日本では個人情報流出等の被害に対する損害賠償請求が低調であり、企業側の謝罪対応のみで事態が収束するケースが常態化しています。再発防止を求めるのは当然ですが、政府主導で日常的に堅牢なシステム構築を要求し、監視する体制を確立してください。 以上、重要インフラを守り、国民の安心を確保するための抜本的な改革を求めます。	頂いた御意見は、今後の参考といたします。
	意見1:汎用品(届出除外対象)の速やかな開示および解説書への例示追記について 1. 該当箇所 第3章 3-1-1 届出対象(21ページ) 「広く一般的に使用されている製品である場合(主務省令第2条第1項但し書き)」 2. 意見の要旨 「広く一般に使用されているものとして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」について、その指定基準の速やかな開示を求めるとともに、想定される具体的な製品カテゴリーを解説書に例示としてあらかじめ追記することを提案します。 3. 意見の具体的な理由 本制度の円滑な運用開始には、事業者が施行日(令和8年10月1日)に向けて、猶予期間内に届出対象資産を正確に洗い出す必要があります。何が届出不要の「汎用品」に該当するかの具体的な指定が遅れると、事業者の資産確認作業において二度手間や過大な負担が発生し、結果として期限内の適正な届出を妨げる要因になります。一般的な商用OSやオフィスソフト、主要なWebブラウザなど、広く流通していることが明白な製品については、解説書段階であらかじめ想定例として示しておくことが、事業者の早期準備を支援する上で極めて有効です。 4. 具体的な改善案(解説書への追記案) 解説書21ページ「『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』については、別途定める。」の後に、以下の一文を追記する。 「なお、ここで想定される汎用品の具体例としては、一般に広く普及しているオペレーティングシステム、Webブラウザ、オフィスソフト、および主要な商用クラウドサービスの基盤インフラ等が挙げられ、これらは速やかに告示等で具体的に示される予定である。」 意見2:特定重要設備等における「失敗した攻撃(試行)」に関する報告基準の明確化について 1. 該当箇所 第5章 5-2-1 特定重要設備等における特定侵害事象の原因となり得る事象(47ページから48ページまで) 「ロ」「ハ」「ニ」に関連する部分 2. 意見の要旨 セキュリティシステム(ファイアウォールやIDS・IPS、WAF、認証システム等)によって即時に検知および自動防御(ブロック)され、事業者の業務やセキュリティ監視体制に実質的な影響を与えなかった「自動化された無差別な攻撃試行」について、報告対象から除外することを明記するか、報告基準を明確化することを提案します。 3. 意見の具体的な理由 自動化されたボットスキャンや、辞書攻撃による不特定のログイン試行(識別符号の入力)などは、日常的に数十万件規模で発生しています。これらを「防御に成功し、試行が失敗した場合」も含めてすべて速報(3日から5日以内)の対象とすることは、事業者側の報告事務を麻痺させるだけでなく、政府側の受付・分析リソースに対しても膨大なノイズを送り込むことになり、真に警戒すべき組織的・深刻なインシデントの分析を遅らせる要因になります。 4. 具体的な改善案(解説書への追記案)	意見1につきまして、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（令和8年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省令第4号。以下「主務省令」という。）第2条第1項ただし書の広く一般に使用されているものは、「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（令和八年内閣府・総務省・法務省・財務省・厚生労働省・農林水産省・経済産業省・国土交通省告示第1号）」（以下「告示」という）で定めております。御意見を踏まえ、当該告示の内容を本解説にも記載いたしました。

No.	御意見の要旨	御意見に対する主な考え方
3	解説書の「特定侵害事象等の発生の認知」(51ページ)または「FAQ」(56ページ)に、以下のFAQを追記する。 「Q. セキュリティシステムによって自動的にブロックされ、組織としての特別な対応(セキュリティ警戒レベルの引き上げや、手動による緊急対応など)を要しなかった、無差別なログイン試行やスキャン行為なども報告対象となりますか。 A. いいえ。セキュリティシステムが正常に機能して即時に自動防御に成功し、システムへの実質的な影響や追加の調査・対応が不要であった自動化された無差別な試行行為については、報告の必要はありません。ただし、通常時を明らかに超える執拗な攻撃試行が検知され、事業者が警戒レベルを引き上げた場合などは報告の対象となります。」 意見3:外部委託先やクラウドサービスにおける「発生の認知」の起算点の明確化について 1. 該当箇所 第5章 5-5 特定侵害事象等の発生の認知(51ページ) 第7章 7-1 FAQ Q4(56ページから57ページまで) 2. 意見の要旨 特別社会基盤事業者が自ら直接管理・監視していないクラウドサービス(特にSaaS等)や、外部委託先が運用する設備において侵害が発生した場合の「発生の認知」の起算点について、「事業者自身が、クラウド事業者または委託先から侵害の具体的な事実通知を受領した時点」であることを解説書に明記することを提案します。 3. 意見の具体的な理由 責任分界点上、SaaS等のミドルウェアやOSへの侵害は、事業者が自社で能動的に検知することは不可能です。他者のインシデント通知の遅れや不具合によって事業者が侵害の発生を検知できなかった場合に、実際の事象発生日を起点に報告期限(速報の3日から5日以内)を起算されると、事業者側に予見不可能な不利益(報告遅延という法違反リスク)が生じます。起算点を事業者が客観的に認知した時点と明確に定義することが、公平かつ実務的な運用のために不可欠です。 4. 具体的な改善案(解説書への追記案) 解説書51ページ「5-5 特定侵害事象等の発生の認知」の末尾に、以下の解説を追記する。 「なお、特別社会基盤事業者が直接監視を行っていないクラウドサービス(SaaS等)や、管理・監視を外部委託している設備において侵害事象等が発生した場合の『発生の認知』の起算点については、サービス提供事業者や運用委託先から侵害の具体的な事実、および報告に必要な情報の具体的な通知を特別社会基盤事業者が現に受領した時点とする。」 意見4:共同利用・共同構築システムにおけるインシデント報告の簡素化(重複報告の回避)について 1. 該当箇所 第2章 2-1-1 特定社会基盤事業者が使用する電子計算機(8ページ) 「他の特別社会基盤事業者と共同利用している場合又は共同で構築されている場合」 第7章 7-1 FAQ Q3(56ページ) 2. 意見の要旨 複数の特別社会基盤事業者が共同で構築・利用しているシステムにおいて同一の侵害事象が発生した場合、関係する事業者が連名で、または代表する1社が他社の委託等を受けて一元的に報告書を提出することで、すべての共同利用事業者が報告義務を履行したものとみなす「連名報告・代表報告」のスキームを認めることを提案します。 3. 意見の具体的な理由 現行の案では、共同利用されている設備が侵害された場合、利用するすべての事業者に対して個別の届出・報告を求めています。しかし、同一のインシデントについて全く同じ内容の報告書(速報・詳報)が複数社から別々に提出されることは、事業者側にとって重複する事務負担であり、行政側にとっても重複した審査・登録が発生するため極めて非効率です。一元的な代表報告を認めることで、正確な情報が迅速に政府へ集約されます。 4. 具体的な改善案(解説書への追記案) 解説書56ページのQ3の回答(A.)の末尾に、以下の内容を追記する。 「ただし、共同利用する複数の特別社会基盤事業者が同一の侵害事象について報告を行う場合、関係事業者が合意の上で連名により報告を提出すること、あるいは運用を代表する1社が共同利用各社を代表して一元的な報告書を提出することにより、当該報告に係るすべての共同利用事業者が法第5条に基づく報告義務を満たしたものとみなす運用の簡易化を認める。」	意見2につきまして、御指摘のポートスキャン、辞書攻撃による不特定のログイン試行については、「ロ」、「ハ」及び「ニ」に該当する場合もあると考えられますが、御指摘のとおりこれらの行為はアタックサーフェスにおいては日常的に発生していると考えられ、報告対象とした場合特別社会基盤事業者の負担が過大になるため、「ロ」、「ハ」及び「ニ」は、本解説5-2に記載のとおり、特定重要設備等に該当する特定重要電子計算機において発生した事象に限り、報告対象としております。 意見3につきましては、本解説5-5において、「報告期限の起算は、サイバーインシデント発生を認知した日から行う」と記載しており、その認知方法の例として「D) 特定重要電子計算機に該当するクラウドサービス等について、クラウドサービス事業者等からインシデント通知があり、そのインシデントが特定侵害事象等と判定された。」と記載しております。 意見4につきまして、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。以下「法」という。）第4条の届出（以下「資産届出」という。）及び第5条の報告（以下「インシデント報告」という。）の主体は、特別社会基盤事業者であるため、御指摘の「代表報告」は認められません。また、御指摘の「連名報告」は、各特別社会基盤事業者において適切に届出対象となる電子計算機を把握し、管理いただく観点から、業種や事業者を問わず一律に認める考えはございませんが、御指摘も踏まえ、運用上支障がないことが確認できた業種・事業者については、個別に検討してまいりたいと考えております。
4	資料を読ませてもらったが、このルールを守る会社や企業、事業者、法人がいるとは思わない 人的災害のようなサプライチェーン攻撃を防御できない企業はUSBすら紛失する 現実で被害者救済を行っていないことを鑑みると、ランサムウェアの攻撃とその影響を軽視しているようにしか見えない 罰金や業務停止命令などの強い責任追及性が重要であるように思える ネットワークをすべて切断したら攻撃領域は存在しない。 wwwの理念に反してインターネットで月額金を徴収し、更にはランサムウェア攻撃に怯み、AIをのさばらせて金稼ぎに奔放するのならデジタル化もDXもやめたほうがいい	頂いた御意見は、今後の参考といたします。
5	特定侵害事象等の報告における利用者への影響及び代替手段の把握について 解説案6-4「報告事項」について、特定侵害事象等によるサービス利用者への影響及び代替手段の提供状況についても、報告に当たり把握することが望ましい事項として明記してください。 既存の報告様式には「業務への影響」や「サービス提供への影響、想定される最大リスク」等の記載欄がありますが、重要な社会基盤の停止又は機能低下による影響は、停止時間やシステムの稼働状況のみでは十分に把握できない場合があります。 例えば、医療、通信、交通、金融その他の国民生活に関係するサービスでは、同じ時間のサービス停止であっても、障害者、高齢者、持病があり服薬や継続的な医療を必要とする者、移動困難者、デジタル機器の利用が困難な者等について、生活、健康又は安全への影響がより大きくなる場合があります。 また、オンラインサービス又はスマートフォンアプリが利用できなくなった場合であっても、電話、対面窓口、紙による手続、代理人による手続その他の代替経路が確保されている場合と、実質的に利用手段が失われる場合とでは、社会基盤サービスへの影響は大きく異なります。 このため、「特定侵害事象等の概要」「特定侵害事象等への対応に関する事項」又は「その他特記事項」の記載例として、少なくとも次の事項を例示することを求めます。 ・利用者及び国民生活への影響の内容及び範囲 ・医療、福祉、交通等の継続的なサービス利用への影響 ・障害者、高齢者、移動困難者その他代替手段を利用しにくい者への特段の影響 ・電話、対面、紙、代理人手続等の代替手段の提供状況 ・代替手段におけるアクセシビリティ上の問題 ・利用者への周知、案内及び支援の実施状況 サイバー攻撃への対応能力を強化するためには、攻撃元、侵入経路、IoT等の技術的情報を分析することに加え、重要な社会基盤の機能低下が実際の国民生活にどのような被害を生じさせたかを把握し、事業継続及び代替手段の改善につなげることも重要です。 特に、平時からデジタルサービスを利用しにくい者ほど、サイバーインシデント時には代替経路を確保しにくい可能性があります。技術的な被害分析と利用者側の影響分析を併せて行うことができるよう、本解説に具体的な記載例を追加してください。	御指摘の役務への影響の詳細については、重要電子計算機に対する不正な行為による被害の拡大防止の観点からは一定程度有効ではあり、記載を拒むものではありませんが、特別社会基盤事業者の負担にも鑑み、現時点で一律に記載を求める考えはありません。

No.	御意見の要旨	御意見に対する主な考え方
6	件名 特定侵害事象等の報告制度における「報告負荷を利用した制度機能不全」への対策について 作成区分：個人研究メモ「ノノ研」 サイバー対処能力強化法に基づく報告制度について、重要インフラに対する攻撃情報を集約し、他事業者の防御に活用する方向性自体は重要であると考えます。 一方で、本制度には、報告件数を増やすことと、実際に対処可能な情報を増やすことが必ずしも一致しないという構造上の問題があります。 重要インフラは、分野・事業者ごとに設備構成、製品、運用条件等が異なります。そのため、「いつ、どこで、どの機器に攻撃があったか」という事実だけを多数収集しても、他事業者が取るべき具体的な対処へ直ちにつながるとは限りません。 他方で、攻撃者は小規模な攻撃や侵害試行を多数の事業者へ広く行うことにより、各事業者に調査、該当性判断、報告、追加照会への対応を発生させることができます。 その結果、 多数の攻撃試行 ↓ 多数の報告義務・調査業務 ↓ 行政・事業者の処理能力を消費 ↓ 重大事案が低価値・重複報告に埋没 ↓ 分析・注意喚起・対処が遅延 という、報告義務を利用した間接的な分散型サービス妨害が成立するおそれがあります。 これは単なる事務負担ではなく、攻撃情報を集約して早期警戒につなげるという制度目的そのものを、攻撃者が逆利用できる問題です。 このため、制度運用に当たっては、報告件数の増加を成果とせず、以下を中心に設計する必要があります。 同一・類似事象の自動集約及び重複排除 低重要度・既知の攻撃試行と、重大・新規事象の報告経路の分離 報告量が急増した場合に低優先情報を集約・延期する仕組み 攻撃事実だけでなく、検知方法、影響範囲、暫定対処、恒久対策へ変換する分析機能 他事業者へ横展開可能な情報のみを抽出して還流する仕組み 制度の評価指標についても、報告件数や情報収集量ではなく、収集情報のうち、実際に防御・検知・対処へ変換できた割合を重視すべきです。 報告入口だけを上げると、攻撃が増えるほど制度の処理能力が低下します。 報告制度と同時に、重複排除、優先順位付け、対処情報への変換、還流までを一体として整備することを求めます。	御指摘の「同一・類似事象の自動集約及び重複排除」につきましては、特別社会基盤事業者が行う類いの報告について官民連携基盤の整備により報告の窓口を一元化するとともに、共通様式による報告の受理を可能とするなど、特別社会基盤事業者に過度な負担とならないよう進めてきたところです。 また、御指摘の「低重要度・既知の攻撃試行と、重大・新規事象の報告経路の分離」「報告量が急増した場合に低優先情報を集約・延期する仕組み」につきまして、特別社会基盤事業者において事象の重要性や優先度を判断することが困難であると考えられるため、重要度や優先度によって特別社会基盤事業者の対応に差異を設ける考えはございませんが、「サイバー攻撃による被害が発生した場合の報告手続等に関する申合せ（令和7年5月28日関係省庁申合せ）」を通じた負担の軽減など、特別社会基盤事業者の負担の軽減を通じ、御指摘の逆利用が生じないよう努めてまいります。 その他、頂いた御意見は、今後の運用における参考といたします。
	意見本文 1. 結論 本制度の目的である 国家全体のサイバー対処能力強化 に賛同する。 一方で、制度の実効性を高めるためには、届出・報告制度の明確化に加え、USB等の可搬記憶媒体への対策、AIを活用した高度な脅威分析、情報共有基盤の効率化など、予防・検知・対応を一体的に推進する視点 が重要である。 制度のさらなる明確化と、事業者の実務負担との均衡に十分配慮した制度設計が図られることを要望する。 2. USB起点のサイバーリスクに関する背景 近年、USBメモリを起点としたサイバー攻撃や情報漏えいが、企業・官公庁・重要インフラにおける重大な経営リスクとなっている。 2026年7月：株式会社ニチレイでシステム障害が発生し、内部報告を契機としてインシデントが認知された。 2025年6月：陸上自衛隊で使用されていたUSBメモリからマルウェアが検出され、約1年間にわたり機密システムへ接続されていたことが判明。防衛省調査では漏えいは確認されなかったが、USBが重要システムへ影響し得ることが再認識された。 これらの事例は、従来型のウイルス対策ソフトやシグネチャ検知だけでは 未知の脅威への対応が不十分 であることを示している。 3. 提案：富岳ネクストAIを活用したUSBマルウェア・情報漏えい対策システム （1）USBリアルタイム解析 USB接続時に、実行ファイル・DLL・Officeマクロ・スクリプト・Autorun設定・ファイル構造・ハッシュ値を自動解析し、AIにより未知マルウェアの特徴分析を行う。	

No.	御意見の要旨	御意見に対する主な考え方
7	（2）AI振る舞い解析 疑わしいファイルを仮想環境で実行し、プロセス生成・レジストリ変更・権限昇格・外部通信・暗号化処理などをAIが解析。危険性が高い場合は実環境での実行を禁止する。 （3）感染拡大シミュレーション 富岳ネクストの計算能力を活用し、Active Directory、ファイルサーバ、クラウド、バックアップ、VPN、認証基盤への感染経路を推定し、初動対応の優先順位を迅速に決定する。 （4）自動防御・インシデント対応 危険判定時には、USB接続遮断、端末隔離、アカウント停止、EDR調査、SOC通知、SIEM集約、管理者アラートを自動実施し、初動対応を高速化する。 （5）脅威インテリジェンス共有 匿名化したマルウェア情報を官公庁・重要インフラ・民間企業・ISAC・SOCと共有し、全国レベルで脅威情報を相関分析する。 4. 導入効果 USB由来マルウェアの早期検知 未知・ゼロデイ攻撃への対応能力向上 感染拡大の抑止 インシデント対応時間の短縮 SOC運用負荷の軽減 情報漏えいリスクの低減 重要インフラの事業継続性向上 官民間の脅威情報共有の強化 5. まとめ USBメモリを起点とするサイバー攻撃は、行政機関・企業・重要インフラに重大な影響を及ぼす可能性がある。 富岳ネクストの高性能計算能力とAI分析技術を既存のセキュリティ基盤と組み合わせることで、未知の脅威への迅速な対応、感染拡大防止、情報漏えいリスク低減を実現できる。 段階的導入が可能であり、次世代の官民サイバーセキュリティ基盤として有効なソリューションとなる。	頂いた御意見は、今後の参考といたします。
	政策提言：デジタル・クリエイティブ産業特区（聖域）の創設に関する提案 【意見の対象となる案件名】 重要インフラ事業者等におけるサイバーインシデント法定報告の様式案に関する意見募集 【該当箇所】 サイバーインシデント法定報告義務化の運用体制、および経済安全保障推進法における特定重要技術の人材確保・基盤整備全般について 【御意見の要旨】 重要インフラへのインシデント報告法定化を実効化するには、サイバー防衛を担う高度IT人材・クリエイターの国内囲い込みが不可欠である。過剰介入の歴史（Winny事件等）による技術者の萎縮効果を完全に払拭し、我が国固有の資源である「圧倒的な生活インフラの質の高さ（住み心地）」をレバレッジとした、世界最高峰の待遇と免責を保証する「デジタル・クリエイティブ産業特区（聖域）」の即時創設を提言する。 【御意見および理由】 1. 提案の背景および問題意識（なぜ今、残機ゼロの危機なのか） （1）資本金格差における正面戦の構造的限界 現在、欧米の巨大IT企業（GAFAM等）はAIおよびデジタルインフラ分野へ毎年100兆円規模の投資を継続しており、中国の国策コンテンツ・IT企業も数兆から数十兆円規模の政府支援を背景に台頭している。これに対し、我が国政府が提示する「1兆円規模」のデジタル・半導体投資枠は、初動で大幅に後塵を拝した現状を鑑みても2桁不足している。正面からの資本金・物量戦による勝利は構造的に不可能であり、既存の延長線上の投資政策ではなく、ゲームのルール自体を逆転させる構造改革が不可欠である。 （2）「金子勇事件（Winny事件）」の後遺症による中間層の完全流出 2000年代初頭、我が国の司法および警察組織が卓越した天才開発者に対して不当な逮捕・裁判（著作権法違反幫助）を強行した歴史は、国内の技術者コミュニティに深刻な「萎縮効果」を定着させた。「新しい革新的な技術を作れば犯罪者にされる」というトラウマにより、過去20年間、本来我が国のデジタル基盤を支えるべき超一級の人材や優秀な技術者の中間層が挙って渡米、あるいは中国・中東等の外資企業へ流出した。結果として国内の開発現場は代替可能な労働者のみが残される空洞化に陥っている。一般的なインシデント報告の「法定化（規制強化）」を進める今だからこそ、開発者が安心して国内に留まる「法的な防壁」を同時に提示しなければ、残された僅かな技術人材の海外逃避をさらに加速させる。	

No.	御意見の要旨	御意見に対する主な考え方
	（3）キラーコンテンツにおける「手綱の喪失」と「デジタル小作人化」 我が国のデジタル・クリエイティブ産業（アニメ、声優、ゲーム、web3等）は世界トップのブランド力を誇りながらも、その流通システム（米国のOS・アプリプラットフォーム）や開発資本（中国等の外資）に美味しいところを全て拉致され、手綱を握られている。30%におよぶ高額な決済手数料を中間搾取され、国策で管理された外資コンテンツによって日本の文脈が都合よく消費される現状は、実質的な「文化の植民地化（デジタル小作人化）」に他ならない。 2. 具体的な政策案（性悪説に基づいた「待遇の逆転特区政策」と運用の現実解） 正面衝突を諦め、特定の限定地域において世界最高峰の経済・法的・スピード優遇を行う特区政策の即時導入を要求する。国際規制や省庁間のナワバリ、サクラ対策をすべてクリアするため、以下の3点をパッケージとして実施すべきである。 1. 経済待遇：市場価値に基づく「所得税・法人税ゼロ、年収1億円保証」の国策提供 国家戦略特区法を拡張し、指定特区内において、世界トップクラス of デジタル技術者・クリエイター個人の「所得税」および関連法人の「法人税」を100%免除（5から10年間の時限措置）とする。また、特に選別された人材には国費から年1億円の活動報酬を最低保証する世界最高峰のインセンティブを用意する。 * 厳格な審査・選別基準（サクラ・スパイ工作員対策）： 行政による主観的・天下りの選別を排除し、客観的市場価値に基づく「自動選別・段階的審査」を導入する。基準としては、世界的なオープンソースコミュニティ（GitHub等）における特定のリポジトリへの貢献度（コントリビューション数、スター数）、国際的なハッキングコンテスト（DEF CON等）での上位入賞実績、あるいは民間ベンチャーキャピタル等から一定額以上の資金調達を受けた開発プロジェクトの主導者とする。これにより、税金目当ての詐欺師や外国の工作員の潜入を完全に遮断する。 * 財務省折衝における財政不整合の回避（財源の現実解）： 本報酬の財源は国の一般財源（国民の税金）に依存せず、本特区創設によるデジタル貿易赤字の縮小（国内への還流利益）、および特区内での独自暗号資産の流通・決済から発生するネットワーク手数料（ガス代等）の一部を国庫に充当する独立採算スキームを構築し、財政的な持続可能性を担保する。 8 2. 法的待遇：「開発者・クリエイター100%免責・保護法」の制定 特区内で開発・公開されたソフトウェアやプロトコルについて、「開発者自身が犯罪を意図・直接実行した性質のもでない限り、第三者による悪用や悪意ある転用（著作権侵害、サイバー攻撃への悪用、マネーロンダリング等）が生じたとしても、開発者は刑事・民事の責任を100%完全に免除される」ことを明文化する（技術開発中立性の原則の法定化）。 * 法務省・警察庁との共存スキーム（法的・一貫性の確保）： 既存の刑法や著作権法を根底から覆して捜査権を奪うのではなく、内閣府・法務省・警察庁の合同協議のもと、「特区法に基づく司法判断の猶予および捜査限定ガイドライン」を明文化する。これにより、役所の古い天下り規制や現場を理解しない捜査機関の恣意的な介入・嫉妬によるイノベーションの破壊を完全に遮断し、世界一安全にチャレンジできる環境を保証する。 3. 経済的スピード：外資プラットフォームを回避する「暗号通貨・独自トークン決済の全面解禁と免税」 外資プラットフォームによる30%の決済手数料や中央集権的検閲を完全に回避するため、特区内で開発されたプロダクトやサービスに限り、独自の暗号資産（Web3/Cryptoトークン等）による決済・流通・資金調達（ICO/IEO）を全面解禁する。また、特区内での暗号資産同士の交換、および決済時に生じる利益にかかる法人税・所得税は完全に免除（非課税）とする。 * 金融規制および国際法への整合性（FATF対策）： 国際的なマネーロンダリングおよびテロ資金供与対策（FATF基準）に完全準拠するため、特区内決済システムと既存の法定通貨（銀行口座）との接続点（オン・オフランプ）において、分散型ID（DID）を用いた厳格な本人確認（KYC）および自動監視システムを義務付ける。これにより、国際的な租税回避地（タックスヘイブン・有害税制）との批判を完全に回避しつつ、世界最速の資金調達と経済的スピード待遇を保証する。 * 初期運用の地理的現実性（スモールスタートの設計）： 日本全土を一気に解放するのではなく、検証の容易性と物理的・電磁的隔離の観点から、既存の国家戦略特区（沖縄、関西圏、または福岡等）の一部エリアや、特定のデータセンター群を包含するバーチャル特区（サンドボックス型）から段階的に運用を開始し、リスクを段階的に管理する。 3. 政策導入による国家安全保障・経済上のメリット（大義名分） パブリックコメントの審査官および政策立案者が、法案の理由付けや予算要求書にそのまま引用できる「国家防衛・経済利益」の文脈でメリットを提示する。 （1）サイバー安全保障における「盾と矛」の自給自足と、本インシデント報告制度の実務的補強 有事の際、国家のインフラ防衛や情報戦を担う超一級の「ホワイトハッカー」および「防衛技術のコア」を国内に引き留め、自給自足する基盤が完成する。これにより、外資ベンダーへの安全保障上の依存（チョークポイント）を解消し、NISCや防衛省が直接連携できる高度サイバー人材の「プール（貯水池）」が特区内に自律形成される。 * 有事における義務（国家へのリターン設計）： 特区の恩恵（1億円保証、免税、免責）を受ける条件として、エンジニアは国との契約において「サイバー有事（国難規模のインシデント発生時）の際には、内閣官房または防衛省の要請に応じ、民間防衛エンジニア（サイバー義勇軍）として技術協力・解析に従事する義務」を課す。 * 本パブリックコメント案件への直接的貢献： 重要インフラ事業者が今般の制度（様式案）に基づいて国（NISC）に報告した高度な侵害事象（インシデント・攻撃手法）に対し、特区内の天才ハッカー勢が即座に共同解析・カウンターパッチ（防御プログラム）の開発を行う実務的な「即応体制」が確立される。結果として、本法定報告制度の効果を100%発揮させ、国家全体のサイバーレジリエンスを爆発的に高めることが可能となる。 （2）知財（IP）経済圏の防衛と「デジタル赤字」の劇的縮小 我が国のキラーコンテンツ（アニメ・ゲーム・漫画）が生み出す利益を、海外プラットフォームに中間搾取されことなく、直接国内の資本循環へ還流させる。これにより、拡大の一途を辿る我が国のデジタル貿易赤字（年間数兆円規模）に明確な歯止めをかけ、特区を起点とした新たな外貨獲得の超強力なエコシステム（生態系）が誕生する。 （3）我が国固有の国家資源「住み心地（生活インフラ）」をレバレッジとした人材の一極集中 欧米や新興国がどれだけ巨額の財政出動（物量戦）を行おうとも、我が国が持つ「世界最高水準の治安、洗練された医療、24時間正確に動く交通インフラ、豊かな食文化、アニメ等のエンタメ資産」という『非金銭的な生活価値（住み心地）』は、他国が数兆円を投じて一朝一夕には作れない最大の強み（チート資産）である。 トバイの人工的な息苦しさ（酷暑・監視社会）や、欧米の致命的な治安悪化・インフラ崩壊・物価高騰に直面し、精神をすり減らしている世界中の「天才」や、かつて海外へ流出した日本のブレインに対し、この最強の生活基盤に「経済的インセンティブ（免税・免責）」を掛け合わせる。これにより、最小の財政コストで世界のトップブレインを我が国へ一極集中させ、経済安全保障上の圧倒的な優位性を確立できる。規制強化の「引き締め」を行う今だからこそ、世界で最も開発者が優遇・保護される「聖域（逆張り特区）」を再定義し、技術先進国・日本のブランドを奪還すべきである。	頂いた御意見は、今後の参考といたします。

No.		御意見の要旨	御意見に対する主な考え方
9		【件名】 サイバーセキュリティ体制の強化および攻撃者に対する抑止力強化のための法整備について 【意見の概要】 企業におけるセキュリティ対策の法的な義務化および未対策企業への罰則導入、ならびにサイバー攻撃者に対する経済的・物理的制裁の強化を求める。 【意見の理由】 デジタル社会において、企業が管理する個人情報の漏洩は、国民生活に深刻な影響を与える問題である。しかし、現状では情報漏洩が発生しても、企業が謝罪や事後の通知を行うのみで済むケースが散見される。個人が企業に対して裁判等の法的措置をとることとはハードルが高く、結果として企業がセキュリティ対策を「コストカットの対象」と見なす構造が是正されていない。 この状況を打開するために、以下の施策を講じるべきであると考える。 1. 企業によるセキュリティ対策体制の義務化と罰則規定の整備 企業が日常的にサイバー攻撃への防御体制を構築することを法的義務とし、ガイドラインの遵守状況や対策の怠慢が確認された場合には、罰則を科す規定を設けるべきである。これにより、セキュリティ対策を経営の最優先課題として認識させ、コストカット対象となるリスクを排除する必要がある。 2. サイバー攻撃者に対する厳罰化と経済的ペナルティの導入 攻撃者側に対しては、不正に得た利益の没収に加え、被害企業の復旧費用や事業損失分を含めた損害賠償を請求できる法整備を行うべきである。これにより「攻撃が成功しても、摘発された際に被るマイナスが利益を大きく上回る」という状況を作り出し、攻撃への強力な抑止力とする。 3. 疑いのある攻撃者に対する国際的な制裁措置の検討 起訴に至るまでの立証が困難な場合であっても、関与が強く疑われる攻撃者に対しては、公告や公表を通じた入国禁止措置等の制限を課す仕組みを導入すべきである。物理的な行動制限を課すことで、攻撃者コミュニティ内での特定を容易にし、司法への情報提供や協力が得られやすい環境を醸成するべきである。 【結語】 国民のプライバシーを保護し、日本企業の国際的な信頼性を確保するためには、防御側（企業）の責任の明確化と、攻撃側（ハッカー）のリスク増大を同時に進める包括的なアプローチが必要不可欠である。本ガイドラインおよび関連法令において、上記のような毅然とした姿勢を盛り込んでいただくよう強く希望する。	頂いた御意見は、今後の参考といたします。
		一市民です。 本ガイドライン（案）に関して、以下の点について意見を申し上げます。 第一点：誤報告・誤認定があった場合の救済規定について 本制度では、特別社会基盤事業者が「特定侵害事象」と報告した場合に、政府が情報収集・分析を行います。 しかし、報告内容に誤りがあった場合、または政府側の判断に誤りがあった場合の救済規定・訂正手続きが本解説書に明記されていません。 誤った報告や誤認定によって事業者や関係者等に不当な不利益が生じた際の、迅速な救済と責任の所在を明確にすることを求めます。 第二点：アクセスログの記録と透明性について 政府が収集した通信情報・インシデント情報について、誰が・いつ・何の目的でアクセスしたかを改ざん不能な形で記録し、独立した第三者が検証できる仕組みの構築を求めます。 記録がなければ情報の適切な管理が確認できず、国民への信頼が損なわれます。 第三点：一般市民への影響の説明責任について 本制度は約257社の基幹インフラ事業者を対象としていますが、これらの事業者が扱う情報には一般市民の個人情報も含まれます。 市民の情報がどのように扱われ、どのように保護されるのかについて、一般市民にも分かりやすく説明する義務を制度に明記することを求めます。 以上、サイバー安全保障の強化という目的には賛同しますが、強力な情報収集権限には対応する救済制度と透明性の確保が必要不可欠であると考えます。 党派を超えた冷静な議論により、真に国民を守る制度となることを切に願います。 一市民より	第一点につきまして、御指摘の「政府側の判断」の指す内容が明らかではありませんが、御指摘の報告内容に誤りがあった場合については、本解説6-4において、「既に行った報告に誤報箇所があった場合は、統報等で訂正・補足することが望ましい」と記載しております。 第二点につきましては、今後の参考と致します。 第三点につきましては、資産届出やインシデント報告によりいただく情報には利用者の個人情報を一律に提出事項として求めるものではありません。
		【該当箇所】第2部 特定侵害事象等の報告に関する手続（または全般） 【意見の理由】本解説案において、特別社会基盤事業者による特定侵害事象等の報告（速報および詳報）の義務化が示されていますが、事象認知後の迅速な報告対応は、民間事業者および報告を受理する行政機関双方にとって、限られたサイバー防御リソース（人的資源）を著しく圧迫する懸念があります。特に、高度なサイバー攻撃が発生した緊迫局面において、定型的な報告書類の作成・微修正や、過去のインシデント事例・政府見解との整合性チェックといった「手作業による文書業務」に追われることは、一分一秒を争う本質的なサイバー対処・能動的防御への集中を妨げる最大の脆弱性となり得ます。民間および行政の業務リソースを100%サイバー防御の実務へ集中・迅速化させるため、実務運用の基盤にAI等の先端技術活用を織り込むべきです。 【意見の内容（具体的な提案）】特別社会基盤事業者からの報告受付、および行政側における情報集約・対処指示の運用体制（解説案に紐づくシステムおよび実務運用）について、以下の観点を明記、または仕様として反映することを求めます。報告・処理プロセスへの生成AI（RAGシステム等）の導入検討：過去のインシデント報告、閣議決定、公式見解等のデータベースを隔離環境で学習させた生成AI基盤を政府側に構築すること。これにより、事業者の質問通告や報告書作成の補助、および行政職員の受付・初稿作成業務を自動化・省力化し、白紙からの原稿作成や確認業務にかかる時間を抜本的に削減（最終チェックのみにシフト）する運用設計とすること。官民双方の対処能力迅速化に向けたシステム共通化：デジタル庁等と連携し、ガバメントクラウド等の安全な環境を用いたセキュアなAI答弁・報告書作成支援の基盤を共通システムとして整備すること。行政のリソース損失を最小限に抑え、本質的な防御力を最大化する運用のあり方を本解説の運用指針、または関連するシステム要件等に反映させるべきです。	頂いた御意見は、今後の運用における参考といたします。

No.	御意見の要旨	御意見に対する主な考え方
	解説には以下の記載があるが、「この対応に留意する」ではどのような対応が必要なのか不明瞭であるため、具体例を明示されたい。 (以下引用) 12 クラウドサービスを使用する場合 日本国外に存在する場合 なお、諸外国においてはデータの国内保管義務や国外へのデータ移転を制限する（いわゆるデータローカライゼーション）法律が施行されていることがあるため、この対応に留意する。	御指摘の「この対応に留意する」とは、「日本国外に存在する場合」における留意点を記載したものであり、「クラウドサービスを使用する場合」における留意点を記載したものではありません。その上で、個別の外国の法令に基づく必要な対応について、該当する外国の法令を個別に確認いただきますようお願いいたします。 (参考) 個人情報保護委員会「諸外国・地域の法制度」https://www.ppc.go.jp/enforcement/infoprovision/laws/を参考として追記することも考えられます。
	本制度に基づく特定重要電子計算機の届出については、届出様式、記載例及び制度解説において、特別社会基盤事業者が平時から運用している資産管理台帳、構成管理台帳、脆弱性管理台帳、インシデント対応マニュアル等との対応関係を、より明確に示すことを求めます。 本制度は、政府が特定重要電子計算機に関する情報を事前に把握し、脆弱性情報や攻撃情報の迅速な共有、注意喚起、被害拡大防止に活用する点で重要な制度であると考えます。一方で、政府に提出する届出情報の範囲、粒度、形式が、事業者内部で実際に保有・管理している情報と大きく異なる場合、事業者側では、届出のたびに内部資料との照合、形式変換、再整理、関係部署への確認が必要となります。その結果、記載漏れ、更新漏れ、誤記、解釈の不一致が生じるおそれがあります。 特に、重要インフラ分野では、特定重要設備、接続機器、認証基盤、クラウドサービス、委託先管理機器、遠隔保守経路等が複雑に関係している場合があります。そのため、届出対象の判断及び届出内容の更新を正確に行うためには、事業者が既に保有している内部管理情報と、届出情報との対応関係を確認しやすくすることが重要です。 13 ついては、制度解説又は別添資料において、届出項目と、資産管理台帳、構成管理台帳、脆弱性管理台帳、インシデント対応手順書等との項目対応表を示すことを提案します。 また、既存の内部資料を届出資料として活用できる場合の例、追加で整理が必要となる項目、提出時に不要な詳細情報の範囲を示すことが望ましいと考えます。あわせて、CSV等の機械可読形式で管理しやすい標準項目例を示すことで、事業者側の二重管理や手作業による転記を減らすことができます。 さらに、届出情報には、システム構成、通信経路、製品情報、管理主体等、悪用されれば攻撃の手掛かりとなり得る情報が含まれます。したがって、政府側における保管方法、アクセス権限、利用目的、第三者提供の範囲、統計化・公表時の秘匿処理、漏えい時の通知等についても、可能な範囲で制度解説上明確化することを求めます。 届出制度は、単に事業者から政府へ情報を提出させる仕組みではなく、事業者内部の安全管理を強化し、政府との情報共有を円滑にする仕組みとして運用されるべきです。内部管理情報と届出情報の互換性を高めることは、届出内容の正確性を高めるだけでなく、事業者が正直かつ迅速に届出を行う実務上及び心理上のハードルを下げる効果もあると考えます。	御指摘の資産管理台帳、構成管理台帳、脆弱性管理台帳、インシデント対応手順書等は、事業者によって様々であると考えられますので、資産届出の届出事項との対応関係をお示しすることは困難です。 本解説1-1に記載のとおり、本解説は法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説するものであり、御指摘の安全管理の記載は馴染まないものと考えておりますが、法第8条の規定も踏まえ、安全管理措置を徹底してまいります。
	本制度においては、クラウドサービス、委託先会社、共同利用システム、保守事業者等が関与する場合の責任分界及び情報共有体制について、制度解説上、より具体的な記載を追加することを求めます。 制度解説案では、委託先会社が管理している特定重要電子計算機、共同利用している特定重要電子計算機、クラウドサービスで構成される特定重要電子計算機等についても、一定の場合に届出又は報告の対象となることが示されています。 しかし実務上、特別社会基盤事業者が自ら直接監視・把握できない領域も多くあります。委託先、共同利用先、クラウドサービス事業者、保守事業者等からの通知及び情報共有がなければ、届出及び報告を適切に行うことは困難です。 そのため、制度解説において、契約上又は運用上確認すべき事項を、チェックリスト又は標準条項例として示すことを提案します。 具体的には、どのような事象が発生した場合に通知を受けるべきか、通知期限、通知方法、休日・夜間を含む緊急連絡経路、報告に必要な技術情報の範囲、ログ・フォレンジック結果等の共有可能性、費用負担及び対応範囲の考え方を明確にすることが望ましいと考えます。 14 特に、中小の委託先や保守事業者に対して、過度な無償対応、過大な調査義務、過剰な資料提出が転嫁されることは避けるべきです。本制度の実効性を高めるためには、特別社会基盤事業者だけでなく、委託先やクラウドサービス事業者を含む供給網全体で、無理なく情報共有できる責任分界を整備する必要があります。 また、近年のサイバー攻撃では、機器やネットワークに対する技術的攻撃だけでなく、関係者を騙して認証情報を入力させる、保守要員や委託先を侵入口として悪用する、特権アカウントや退職者アカウントを利用する、内部者又は協力者を通じてアクセス経路を確保するなど、人的経路を伴う攻撃も重要です。 したがって、人的経路そのものを独立した届出対象とする必要まではないとしても、侵入経路、原因となり得る事象、報告事項、事後分析項目の例示として、認証情報の詐欺、特権アカウントの悪用、委託先・保守要員経由の侵入、内部者化又は協力者化の疑いを明記することを求めます。 本制度は、特別社会基盤事業者単体の管理だけで完結するものではなく、クラウド、委託、共同利用、保守、人的経路を含む複合的な攻撃面を前提に設計される必要があります。責任分界と人的経路を明確化することで、報告遅延、情報不足、責任の押し付け、現場の萎縮を防ぎ、制度全体の実効性を高めることができると考えます。	御指摘の委託先会社が管理している特定重要電子計算機等につきましては、本解説5-5において、「インシデント発生を初期に認知することになる自社外組織から、どのような場面でどのようなインシデント通知が為されるかを確認することが望ましい（例：SLA定義書、クラウドサービス利用規約、システム共同利用契約書等）。」と記載しているところです。頂いた御意見は、今後の運用における参考といたします。

No.	御意見の要旨	御意見に対する主な考え方
15	本制度に基づく特定侵害事象等の報告については、「認知した時」の判断基準をより明確化するとともに、正式な速報の前段階として、攻撃を受けた可能性がある段階でも低負担に情報共有できる予備通報又は早期警戒共有の仕組みを設けることを求めます。 制度解説案では、監視におけるイベントやアラートの発報のみをもって直ちに認知とはせず、当該イベントやアラートの内容等を踏まえ、特定侵害事象等に該当すると合理的に判断できる状態を「認知」とする旨が示されています。この整理自体は妥当であると考えます。 しかし実務上は、SOCによる検知、EDR等の監視装置のアラート、クラウドサービス事業者からの通知、委託先からの断片的な連絡、利用者からの異常申告などが、時系列上ばらばらに発生することがあります。これらの情報が、どの時点で報告期限の起算点となる「認知」に至るのかが不明確であると、事業者は過少報告と過剰報告の間で迷うことになります。 そのため、制度解説において、少なくとも次の区分について具体例を追加することを提案します。 第一に、アラート又は外部通知があったが、特定侵害事象等に該当するか未判定であり、まだ認知に至らない段階。 第二に、調査の結果、特定侵害事象等に該当すると合理的に判断でき、報告期限の起算点となる段階。 第三に、クラウドサービス事業者、委託先、共同利用先等から通知を受けた場合に、通知受領時点と自社での該当性判断時点の関係をどのように考えるべきか。 第四に、速報後に誤検知、影響範囲の縮小、事象分類の変更、原因の訂正が判明した場合の取扱いです。 また、重要インフラ防護の観点からは、「攻撃を受けた可能性がある」「標的型攻撃の兆候がある」「委託先又はクラウドサービス事業者から調査中の通知を受けた」といった段階でも、政府と早期に情報共有できる通路があることが望ましいと考えます。 ただし、この段階の情報共有を通常の義務報告と同じ扱いにすると、誤検知や不確実な情報で大量に報告され、事業者側にも政府側にも過大な負担が生じるおそれがあります。そのため、正式な速報とは別に、低負担かつ保護付きの「予備通報」又は「早期警戒共有」の仕組みを設けることを提案します。 予備通報においては、事業者が「調査中」「影響範囲未確定」「攻撃可能性あり」として共有できるようにし、後日、誤認や訂正が判明した場合でも、合理的な初動判断に基づく善意の共有であれば不利益に扱わないことを明記すべきです。 本制度の目的は、事業者を萎縮させることなく、重要インフラに関するサイバー攻撃情報を早期に共有し、被害拡大を防止することにあると考えます。そのためには、認知時点の予見可能性を高めるとともに、不確実な段階でも安全に相談・共有できる制度上の余白を設けることが重要です。	御指摘の第一及び第二につきましては、本解説5-5において、「発生の認知とは、監視におけるイベントやアラートの発報のみをもって直ちに該当するものではないが、当該イベントやアラートの内容等を踏まえ、法第5条における特定侵害事象等に該当すると合理的に判断できる状態を指す。」と記載しております。「特定侵害事象等に該当すると合理的に判断できる状態」とは、本解説5.の特定侵害事象等の範囲に当てはまると判断できる場合を指し、具体的に該当する事象の例については、本解説の当該箇所においてお示ししております。 御指摘の第三につきましては、本解説5-5において、「報告期限の起算は、サイバーインシデント発生を認知した日から行う」と記載しており、また、その認知方法の例として「D) 特定重要電子計算機に該当するクラウドサービス等について、クラウドサービス事業者等からインシデント通知があり、そのインシデントが特定侵害事象等と判定された。」との記載のとおり、通知受領を持って認知するのではなく、通知内容を踏まえて特定侵害事象等に当てはまると判断した場合に特定侵害事象等の発生を認知したこととしております。 御指摘の第四につきましては、本解説6-4において、「既に行った報告に誤報箇所があった場合は、続報等で訂正・補足することが望ましい」と記載しております。 その他、早期の情報共有について頂いた御意見は、今後の運用における参考といたします。
16	本制度に基づく届出及び報告については、将来的に、AIを活用した入力支援、対象判定支援、記載内容の確認支援、過去届出との差分管理等を行う窓口又は支援機能を整備することも検討に値すると考えます。 特定重要電子計算機の届出及び特定侵害事象等の報告は、対象範囲の判断、機器情報の整理、クラウド・委託先との関係整理、変更届の管理、速報・詳報・続報の区分など、事業者側に一定の実務負担を生じさせます。AIを活用した窓口により、届出項目の案内、入力漏れの確認、過去届出との差分抽出、関連マニュアルやFAQへの誘導が行われれば、事業者側の負担軽減、記載ミスの減少、届出・報告の迅速化に資する可能性があります。 一方で、AI窓口を設ける場合には、次の点について特に慎重な設計が必要です。 第一に、AIによる案内や判定支援が、行政としての正式な判断なのか、単なる入力支援なのかを明確にする必要があります。AIの回答を信頼して届出対象外と判断した結果、後に報告漏れや届出漏れと扱われるような事態は避けるべきです。 第二に、AIが誤った案内、不完全な分類、過度に断定的な回答を行った場合の責任関係を明確にする必要があります。特に、対象該当性、認知時点、速報要否、提出すべき情報の範囲については、最終判断を事業者に残すとしても、AI窓口の表示内容が事業者の判断に強い影響を与えるため、注意が必要です。 第三に、AI窓口へ入力される情報には、システム構成、製品情報、通信経路、インシデントの兆候、委託先情報等、機微な情報が含まれる可能性があります。そのため、入力情報の保存範囲、学習利用の有無、アクセス権限、ログ管理、第三者提供、削除手続、漏えい時の通知について、明確に定めるべきです。 第四に、AI窓口が事業者側の実務をかえって複雑にしないよう、既存の資産管理台帳、構成管理台帳、脆弱性管理台帳、インシデント対応マニュアル等と接続しやすい形式にする必要があります。AI上でしか管理できない独自形式が増えると、内部資料との照合や監査証跡の管理が困難になります。 第五に、AIによる自動判定又は自動作成に依存しすぎること、現場担当者が制度趣旨や判断基準を理解しないまま届出・報告を行うおそれがあります。そのため、AI窓口は単なる自動化手段ではなく、根拠条文、判断理由、参照箇所、未確認点を示し、担当者の理解と確認を支援する設計とすべきです。 第六に、AI窓口を利用できない事業者、又は利用に不安がある事業者のために、人による問い合わせ窓口、紙又は通常の電子様式による提出方法、説明会資料、FAQ等の代替手段を維持することが必要です。 AI窓口の導入は、届出・報告の省力化、迅速化、記載品質の向上に資する可能性があります。しかし、対象該当性や報告要否に関する行政上の責任境界、AI回答の位置付け、機微情報の保護、監査証跡、人による確認手段を明確にしなければ、かえって事業者の萎縮、誤判断、情報漏えい、責任不明確化を招くおそれがあります。 したがって、AIを活用した届出・報告支援を整備する場合には、AIを最終判断主体とするのではなく、事業者と行政双方の確認作業を補助する入力支援・整理支援・差分確認支援として位置付け、その限界と利用条件を制度解説又は運用資料に明記することを求めます。	頂いた御意見は、今後の運用における参考といたします。

No.	御意見の要旨	御意見に対する主な考え方
17	「アプライアンス以外の電子計算機に組み込まれたオペレーティングシステム、ミドルウェア及びアプリケーション」が届出対象とされていますが、Excel・PowerPoint・Word等のいわゆるオフィスソフトウェアのほか、Adobe Acrobat Reader、セキュリティソフトウェア、メーカーサポートソフト、各種体験版ソフトウェア等の、PCにあらかじめインストールされている汎用アプリケーション程度のもまで届出対象に含まれるとの理解でよろしいでしょうか。 また、これらが届出対象に含まれる場合、Excel・PowerPoint・Word等については利用ライセンスが付与されておらず実際には使用していないものの、ソフトウェア自体はPCにプリインストールされているケースが多く見受けられます。 このような「実際には使用していない、またはライセンスがなく使用できないものの、プリインストールされているソフトウェア」についても、届出対象となるのでしょうか。 プリインストールソフトウェアは個別に調達・購入するものではなく、資産管理台帳等にも登録されていない場合があるため、届出対象として認識されにくいものと考えられます。 負担軽減の観点から、実際に使用していないソフトウェアについては届出対象外としていただきたいと考えますが、いずれにせよ、プリインストールソフトウェアの取扱いについて誤解が生じないよう、対象範囲をQ&Aやガイドライン等で明確化いただくことを要望します。	本解説2-1-2に記載の通り、ハードウェアに指令を与えるソフトウェアを対象としております。資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております資産届出に関する相談窓口までお問合せください。
18	4-3-2 ステップ3-2 システム概略図（詳細版）の作成 の掲載パターンについて違和感があります。 図 5 - 図11に「クラウド」の記載がありますが、aws等のクラウドのサービスについては、「インターネット」を経由して利用しているものだと考えられます。 図5-図11の图案の記載されている図の場合、ルータを経由した事業者内への侵害は、必ずクラウドを経由されるように見えます。しかし実際には「クラウド」に対する侵害は「インターネット」経由「ルータ」に対する侵害は「インターネット」（もしくはその先にある「クラウド」から「インターネット」経由）で行われることとなり、侵害の実態を把握するために不適切な図に見えます。「クラウド」-「インターネット」-「ルータ」となるような図、もしくは「インターネット」に「クラウド」が含まれるような図が適切ではないでしょうか。 一方、国内の電気通信事業者等で、クラウドと回線サービスを一体になって提供している場合においては、解説案に掲載されているパターンで問題がないと考えられます。注意書きや説明を付与することが必要ではないでしょうか。	クラウドから公衆の用に供されている電気通信回線を経由しないことを認識しやすいように作成したものととなります。御意見を踏まえ、本解説4-3-2の図に説明を記載いたしました。
19	「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）」に関して、特別社会基盤事業者におけるセキュリティ体制の強化および実効性のある罰則・対策について以下の通り意見を述べます。 1. 特別社会基盤事業者に対する日常的なセキュリティ体制構築の義務化と厳罰化 ・重要インフラ等を支える特別社会基盤事業者に対し、単発的な届出や報告にとどまらず、日頃からセキュリティ対策を継続的に実施するシステム体制の構築を厳しく義務付けること。 ・国や第三者機関による監査等で対策の不備や怠慢が判明した場合には、形式的な改善指導や謝罪にとどまらず、抑止力として機能するよう国の罰金を大幅に厳罰化し、実効性を担保すること。 2. サイバー攻撃・侵害事象を引き起こす外部の犯罪者およびグループに対する強力なペナルティ ・特別重要電子計算機等に対するサイバー攻撃や不正行為を行った者に対し、法的な罰則を一層強化すること。 ・海外からの攻撃等により身柄の拘束や逮捕が困難な場合であっても、関与が判明した個人や、身代金を要求するなどの犯罪グループに属する団員すべてを対象に、日本への入国禁止等の厳しい措置を速やかに講じること。 ・完全な立証が困難であっても、警察等の調査により攻撃への関与の可能性があると認定された段階で同様の不利益（渡航制限等）を科す仕組みを取り入れることで、組織内部からの牽引力・犯罪抑止力を高めること。 総じて、特別社会基盤事業者に対しては厳格な体制義務と罰則によって内側からのセキュリティを高めると同時に、攻撃者側に対しては実態として強い不利益を被らせる枠組みを構築することを強く要望する。	頂いた御意見は、今後の参考といたします。
	【該当箇所】 「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（特定重要電子計算機の届出及び特定侵害事象等の報告）（案）」全体。 特に、特定重要電子計算機の範囲、特定重要電子計算機の届出、3-2.変更届出、補足事項 届出手順の一例、5-5.特定侵害事象等の発生の認知、報告手続、7-1.FAQに関する意見です。 【意見】 本解説案は、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を認知した際の報告が円滑に行われるよう支援し、サイバーセキュリティの確保をより確実にするためのものと理解しています。この目的自体には賛同します。 一方で、ITシステムやクラウドサービスは、導入時点の構成がそのまま続くとは限りません。運用中に、ネットワーク接続、使用目的、認証方式、API連携、クラウド機能、保守方法、バックアップ方法、委託先又は共同利用先が変わることがあります。そのため、初回整理では、事業者内部の実務整理として「届出対象外」「任意届出又は相談」「社内記録のみ」と扱っていた機器又はサービスが、後日の構成変更により、「新たな届出」「変更届出」「任意届出又は相談」「社内記録」「確認中」のいずれかで扱べき状態に変わる場合があります。 ただし、「該当する可能性がある場合」や「届出が必要かどうかを再確認する」といった抽象的な表現だけでは、技術的には可能性を完全に否定できない変更まで広く確認対象となり、事業者側の負担が過大になるおそれがあります。また、行政側の確認資源にも限りがあり、全ての構成変更を行政が個別に確認する運用は現実的ではありません。事業者側においても、構成変更のたびに複雑な書類作成や確認待ちが生じれば、安全対応、障害回避、運用改善が遅れるおそれがあります。 しかし、負担軽減だけを優先すると、特定重要設備との接続、データ入力、操作、認証、保守、外部到達性、復旧・継続、委託先又は共同利用先との関係が変わった場合まで軽く扱われ、安全保障上重要な経路を見落とすおそれがあります。したがって、本解説案又はFAQでは、抽象的な再確認条件だけでなく、構成変更後に何を確認し、その結果をどの扱いにするかについて、対応関係を一覧的に示すことが望ましいと考えます。 なお、本意見は、新たな独立台帳の作成、全ての構成変更に対する行政確認、又は事前承認制度の創設を求めるものではありません。また、「任意届出又は相談」及び「確認中」は、新たな法令上の届出区分を設ける趣旨ではなく、事業者が既存台帳やFAQ上で実務上の扱いを整理するための便宜的な区分として示すものです。特定重要設備との関係が実際に変わらない変更は、既存の変更管理台帳、資産管理台帳、インシデント管理台帳等への社内記録で足りる場合があることを明確にし、行政確認又は相談を、特定重要設備への影響経路が変わる変更、判断に迷う境界事例、緊急安全対応後の確認、事故後検証に集中させる趣旨です。 構成変更後に確認すべき事項としては、例えば、特定重要設備そのもの又はその一部になったか、特定重要設備と直接又は間接に接続したか、特定重要設備へ送るデータの種類・経路・頻度が変わったか、特定重要設備に入力されるデータを作成するようになったか、認証・権限管理・特権ID・管理者操作に関わるようになったか、保守用接続・遠隔操作・設定変更に使うようになったか、外部API・外部クラウド・インターネット等から到達できる範囲が変わったか、DR・バックアップ・監視・障害時切替に使うようになったか、委託先、クラウド事業者、共同利用先が変わり、通知先や責任分担が変わったか、以前に「社内記録のみ」とした理由が構成変更によって成り立たなくなったか、などが考えられます。 これらに該当する場合には、変更後の実際の役割に基づき、「新たな届出」「変更届出」「任意届出又は相談」「社内記録」「確認中」のいずれで扱うかを確認することが望ましいと考えます。一方で、特定重要設備との接続、データ入力、操作、認証、保守、外部到	

No.	御意見の要旨		御意見に対する主な考え方
20	達性、復旧・継続に影響しない表示変更、名称変更、料金プラン変更、軽微な設定変更等については、原則として既存台帳への社内記録で足りる場合があることも併せて示すべきです。この整理により、「ゼロリスクでなければ全て確認」という運用を避けつつ、特定重要設備への影響経路が実際変わった変更を拾いやすくなると考えます。 さらに、対応関係を一覧的に示す際には、届出を要する場合だけでなく、社内記録で足りる場合、確認中としてよい場合、事後相談で足りる場合も同時に示すことが重要です。届出に該当する例だけを示すと、事業者は安全側に倒して全てを届出又は相談に寄せる可能性があります。反対に、社内記録で足りる例だけが強調されると、実際には特定重要設備への影響経路が変わった変更まで軽く扱われるおそれがあります。重い扱いと軽い扱いを対で示すことにより、過少対応と過大対応の双方を避けられると考えます。 構成変更後の扱いは、少なくとも五つに分けることが有用です。第一に、これまで届け出ていなかった機器又はサービスが特定重要設備そのもの又はその一部になった場合、又は特定重要設備との接続、データ入力、認証、保守、復旧等に実質的に関わるようになった場合の「新たな届出」です。第二に、既に届け出ている機器又はサービスについて、接続先、送るデータ、認証範囲、保守方法、クラウド機能、委託先、共同利用先などが変わり、届出内容と実際の構成が変わった場合の「変更届出」です。第三に、法令上の届出が必要か明確でないが、特定重要設備との関係が近く、後から特定重要設備の停止又は低下に関係するおそれを行政側も把握しておくことが有用な場合の「任意届出又は相談」です。第四に、特定重要設備との接続、データ入力、操作、認証、保守、復旧・継続に影響しない変更であり、既存台帳等に記録すれば足りる場合の「社内記録」です。第五に、どれに当たるか判断が分かれる場合の「確認中」です。 確認中の場合は、直ちに無理に結論を出すのではなく、どの点が不明かを記録し、必要に応じて所管省庁、委託先、クラウド事業者、共同利用先等へ確認した上で扱いを決めることが望ましいと考えます。この五区分は、事業者に新しい義務を広げるためではなく、扱いを軽くできる変更と、注意して扱うべき変更を分けるためのものです。特定重要設備との関係が変わらない変更まで行政相談に回すと、相談件数が増え、行政側の確認資源が本来に重要な変更に向かいにくくなります。他方で、社内記録のみとしてよい範囲が曖昧なままでは、事業者ごとに判断が割れ、安全保障上重要な変更が軽く扱われるおそれがあります。そのため、五区分の考え方をFAQで例示し、最低限確認すべき観点を共通化することが望ましいと考えます。 また、確認対象は、理論上の可能性ではなく、変更後の構成で実際に特定重要設備との関係が変わった場合を中心に整理すべきです。技術的には、多くの変更について「可能性がない」と断定することは困難です。そのため、「可能性が完全に否定できない」という理由だけで全ての変更を重く扱うと、行政側、事業者側の双方に過大な負担が生じ、かえって安全対応や障害回避を遅らせるおそれがあります。 さらに、サイバー攻撃対応や脆弱性対応では、短時間で判断し、実行しなければならぬ場合があります。攻撃遮断、脆弱性対応、障害回避、認証強化、漏えい拡大防止など、遅れると安全性が下がる変更については、届出又は変更届出の扱いを確認する前であっても、先に実施できることをFAQ等で示すことが望ましいと考えます。その上で、実施後に、変更日時、対象、変更内容、実施理由、特定重要設備との関係、届出又は変更届出の要否を記録し、必要がある場合には、事後に届出、変更届出又は所管省庁への相談を行う扱いが考えられます。合理的な安全対応であったことを確認できる記録が残っている場合には、事後対応であったことを直ちに手続違反又は不適切対応として扱わない考え方も重要です。 判断記録については、新しい独立台帳を作るのではなく、既存の変更管理台帳、資産管理台帳、インシデント管理台帳等を使うことが現実的です。通常の変更については、変更日、対象機器又はサービス、変更内容、変更後に確認した項目、五つの扱いのいずれにしたか、判断理由、判断した部署又は担当者を残せば足りる場合が多いと考えます。特定重要設備への影響が大きい変更、扱いに迷う変更、緊急安全対応として先に実施した変更、後から扱いを変更した変更、事故後に確認が必要になった変更についてののみ、変更前後の扱い、影響範囲、相談先、事後対応にした理由、後から扱いを変更した理由等を追加すればよいと考えます。既存の台帳や資料で同じ内容を確認できる場合には、二重に記録する必要はありませんが、後からどの資料を確認すればよいかが分かるよう、既存資料又は既存台帳との関係を示すことが望ましいと考えます。 また、記録項目を示す場合には、項目名だけでなく、その項目が何の確認機能を担うのかも併せて示すことが望ましいと考えます。例えば、「変更後に確認した項目」は、特定重要設備との関係が変わったかを後から確認するためのものであり、「扱いの結果」は、新たな届出、変更届出、任意届出又は相談、社内記録、確認中のどれで処理したかを再現するためのものです。将来、事業者の台帳や管理システムが更新された場合でも、これらの確認機能が失われないよう、最低限残すべき情報を示すことが有用です。 報告手続についても、届出、変更届出、認知時点の判断が報告手続へ円滑につながるよう、FAQ等で補足することが望ましいと考えます。例えば、速報時点では対象機器が不明であったが後に特定重要電子計算機又はそれに関係する機器が特定された場合、速報時点では影響範囲が限定的と考えていたが後に特定重要設備の停止又は低下に関係する可能性が判明した場合、委託先、クラウド事業者、共同利用先等から追加情報を受けて、発生時刻、通知時刻、受領時刻、判断時刻又は報告時刻を補足する必要が生じた場合、速報時点では不明だった侵入経路、攻撃手口、影響範囲、復旧状況等が後から判明した場合などは、速報後の続報又は詳報で判明した範囲を補足できることを示すと、事業者は未確定事項を抱えていても速報しやすくなると考えます。 この場合、速報時点で不明な事項が残っていること自体を問題視するのではなく、判明済みの事項、不明な事項、確認先、確認予定、続報で補足する事項を分けて扱うことが重要です。特に、委託先やクラウド事業者からの通知を起点に認知する場合には、事業者が実際に知った時刻、委託先から通知を受けた時刻、内部で特定重要設備との関係を判断した時刻、行政へ報告した時刻がずれることがあります。このような時刻のずれを、速報、続報又は詳報で補足できると示すことで、認知時点をめぐる過度な萎縮を避けつつ、行政側も事案の時系列を把握しやすくなると考えます。 FAQの具体例としては、次のような内容を追加することが考えられます。初回整理では社内記録のみとしていた端末が、後から特定重要設備と接続され、特定重要設備へデータを送るようになった場合には、変更後の構成で、特定重要設備と接続し、その機能に影響するデータを送信又は入力するかを確認し、新たな届出又は変更届出の要否を確認することが望ましい、と示すことが考えられます。届出又は変更届出をしない扱いにする場合でも、変更日、対象機器、変更内容、確認した項目、扱いの結果、判断理由を記録することが望ましいと考えます。 また、クラウドサービスの契約オプション変更により、認証機能、API連携、ログ保存、外部接続、データ保存範囲が変わった場合には、単なる料金プラン変更なのか、特定重要設備との接続、特定重要設備へ入力されるデータの作成、認証又は権限管理、外部からの到達性、保守又は復旧機能に関わる変更なのかを分けて確認することが望ましいと考えます。特定重要設備との関係が変わらない表示機能や契約名称の変更については、社内記録で足りる場合があることも併せて示すべきです。 さらに、脆弱性対応や攻撃遮断のため、届出又は変更届出の扱いを確認する前に緊急で構成変更を行う必要がある場合には、安全性の確保又は被害拡大防止のために先に実施できること、実施後速やかに変更日時、対象、変更内容、実施理由、特定重要設備との関係、届出又は変更届出の要否を記録すること、必要があれば事後に届出、変更届出又は相談を行うことを示すことが望ましいと考えます。 一度「社内記録のみ」とした機器又はサービスであっても、用途変更により、特定重要設備との接続、特定重要設備へ入力されるデータの作成、認証又は権限管理、保守用接続、外部到達性、復旧・継続機能に関わるようになった場合には、新たな届出又は変更届出の対象になり得ることも明示すべきです。反対に、変更後の扱いが判断できない場合には、無理に結論を出すのではなく、「確認中」として記録し、どの点が不明かを残した上で、必要に応じて所管省庁、委託先、クラウド事業者、共同利用先等へ確認する扱いが望ましいと考えます。 以上のように整理すれば、全ての変更を重く扱うことを避けつつ、特定重要設備への影響経路が実際に変わった変更を見落とすにくくなります。また、行政側は全ての変更を個別確認するのではなく、特定重要設備の停止又は低下に直結し得る変更、判断に迷う境界事例、緊急安全対応後の確認、事故後検証に確認資源を集中できます。これにより、制度対応の負担を増やすぎず、特定重要電子計算機及び関連する接続関係を継続的に把握し、サイバーセキュリティの確保という本制度の目的に資すると考えます。		資産届出については、本解説3-2-1において、「四半期ごとに特定重要電子計算機の棚卸しを行い、1月でその結果をとりまとめ届け出るといったことも可能」とお示し、また、4. において届出手順の一例をお示しているところです。それ以外の詳細については、事業者ごとに電子計算機の管理の状況等が異なると考えられることから、現時点では、一律に方法をお示しする考えはございません。
21	「当該特定重要電子計算機が……広く一般に使用されているものとして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」として、マイクロソフト・コーポレーションのWindows 及び Windows Serverのみを指定したのは何故か。 Linux系OSも相当程度利用されているのではないかとと思われるが、こちらについては多数のディストリビューションがあり、特定のOSを指定することは難しいという理解で良いか。 また、ミドルウェアについて指定しなかった理由は何か（例えば、マイクロソフトのSQL Serverも指定できたのではないか。）。		資産届出いただく趣旨は、政府が特別社会基盤事業者の特定重要電子計算機の資産状況について把握しておくことにより、内閣総理大臣が特別社会基盤事業者に対し適切な情報共有を行うなど、特定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必要な対応を行うためです。 例えば、政府において、特定重要電子計算機の脆弱性情報を把握した場合、その脆弱性情報と同項に基づき届け出られた特定重要電子計算機の情報を照合させることにより、脆弱性のある特定重要電子計算機を使用する特別社会基盤事業者に対し、脆弱性情報を提供することが可能となります。 他方、業界、事業者問わず、広く一般に使用されている電子計算機については、資産状況を把握せずとも、全ての特別社会基盤事業者に脆弱性情報を提供することで、特別社会基盤事業者は必要な措置を講じることが可能です。そのため、告示では、特別社会基盤事業者の負担の軽減の観点から、資産届出を不要とする電子計算機を指定することとしております。 以上の趣旨を踏まえ、告示では、業界、事業者問わず広く使われており、かつ、特に主務省令第1条第1項第6号及び第2項第1号に規定する電子計算機において使われていることが想定されるなど、特別社会基盤事業者の負担軽減の効果が高いマイクロソフト・コーポレーションのWindows及びWindows Serverを指定することといたしました。
22	制度の解説は、法令を適切かつ統一的に運用するための重要な資料であり、実際の制度運用に大きな影響を与えるものです。そのため、法律や命令の趣旨を逸脱することなく、制度の対象や運用方法を明確に示し、拡大解釈の余地を可能な限り排除した内容とすることが重要であると考えます。 特に、特定侵害事象等の報告及び届出については、対象となる事象、報告の範囲、報告時期等をできる限り具体的に記載し、事業者によって解釈や運用に差が生じないよう配慮していただきたいと思います。曖昧な記載が残れば、必要以上の報告や事業者の過度な萎縮、さらには制度趣旨を超えた運用につながるおそれがあります。 また、制度への信頼を確保するためには、運用の透明性及び説明責任を十分に確保することが重要です。制度の運用状況については可能な範囲で公表し、運用上の課題が確認された場合には継続的な検証及び見直しを実施する旨を、制度の解説においても明確に示していただくことを求めます。 制度の実効性は、制度そのものだけでなく、どのように運用されるかによっても左右されます。制度の趣旨を超えた運用や拡大解釈を防ぎ、国民や事業者が安心して制度を理解し対応できるよう、明確で分かりやすい解説となることを期待します。		可能な限り対象を具体的に記載し、制度の趣旨を超えた運用につながらないよう努めてまいります。また、本解説は、本解説1-1に記載のとおり、法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説をするものであり、御指摘の安全管理の記載は馴染まないものと考えておりますが、法第8条の規定も踏まえ、安全管理措置を徹底してまいります。

No.	御意見の要旨	御意見に対する主な考え方
	「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（特定重要電子計算機の届出及び特定侵害事象等の報告）（案）」に対し、以下の意見を提出します。 ＜本解説に「ソフトウェアのメモリ安全性確保」に関する章を新設することを求めます＞ 特定重要電子計算機の届出にあたり、事業者が当該システムのセキュリティを自己評価する指針として、以下の項目を解説に盛り込むべきです。 1. ソフトウェア供給連鎖（サプライチェーン）のメモリ安全性評価 サイバー攻撃の主要な侵入経路であるメモリ安全性の脆弱性（バッファオーバーフロー、use-after-free、データ競合等）はC/C++に起因し、CISA/NSAの共通認識では全CVEの約70%を占めます。PythonやTypeScriptは表層的にメモリ安全ですが、CPythonインタプリタ（C）、V8エンジン（C++）、PyTorch・numpy・cryptography等のネイティブ拡張（C/C++/CUDA）に依存しており、供給連鎖全体ではメモリ安全性が担保されていません。 この点、デジタル庁が公開するOSS「源内（GenAI）」（github.com/digital-go-jp/genai-ai-api）もPython/TypeScriptで実装され、CPython + PyTorch + 各種ネイティブ拡張のスタックに依存しています。法執行を担う府省庁自身がメモリ安全性を供給連鎖レベルで確保していないソフトウェアを政府AI基盤として展開していることは、本制度の実効性と説得力の観点から看過できない矛盾です。 参考： 源内 GenAI の Pure Rust リファレンス実装 --- https://github.com/cool-japan/oxigenai/ 2. 届出事項への実装言語・依存構成の追加 「特定重要電子計算機」の届出模式に、以下を評価項目として含めることを推奨します。 23 - 当該システムの実装言語（ランタイム含む） - 主要依存ライブラリの言語別構成 - メモリ安全性評価の有無 これにより、事業者自身がソフトウェア供給連鎖のリスクを可視化でき、中長期的なメモリ安全言語（Rust等）への移行のエビデンスが蓄積されます。 3. 国際的な政策動向との整合 - 米国ONCD（2024年）：重要インフラソフトウェアにメモリ安全言語の採用を勧告 - DARPA TRACTOR（2023年?）：C/C++からRustへの自動変換を研究 - EUサイバーレジリエンス法（2024年施行）：secure-by-designを域内販売の法的要件化 - Microsoft「Year of Rust 2025」：WindowsカーネルへのRust投入を開始 各国がメモリ安全言語への移行を国家戦略として位置づける中、本解説においてもソフトウェアのメモリ安全性を「特定重要電子計算機」のセキュリティ評価の一要素として明記することを強く求めます。 --- ＜ 参考資料＞ - 「Rust for 2030 -- メモリ安全言語によるサイバーセキュリティ強化ロードマップ」https://ja.kaccy.net/rust.pdf - 源内 GenAI Rustリファレンス実装: https://github.com/cool-japan/oxigenai/	頂いた御意見は、今後の運用における参考といたします。
	本解説案について、特定社会基盤事業者が直接所有する設備だけでなく、グループ会社等が所有する設備、クラウドサービス、日本国外に存在する設備、共同利用設備及び災害復旧サイトまで対象となり得ることを明示した点は、実際の情報システムの構成に即したものであると考えます。また、ハードウェアだけでなく、ファームウェア、オペレーティングシステム、ミドルウェア及びアプリケーションも特定重要電子計算機に含まれ得るとの整理についても、サイバーセキュリティ上妥当であると考えます。 一方、届出対象については、アプライアンスの場合はハードウェアが対象とされ、組み込まれた各種プログラムは届出対象外とされています。また、アプライアンス以外の電子計算機では、オペレーティングシステム、ミドルウェア及びアプリケーションが対象となる一方、ハードウェア及びファームウェアは届出対象外とされています。さらに、法定の届出事項は主として製品名及び製造者名であり、バージョン、保守期限、遠隔管理経路等までは明示されていません。 しかし、実際の脆弱性情報は、同一製品であってもハードウェアリビジョン、ファームウェア、オペレーティングシステム及び組み込まれたライブラリのバージョンによって該当性が異なります。製品名と製造者名だけでは、脆弱性が公表された際に対象設備を迅速に抽出できない可能性があります。 このため、法定の届出事項そのものを直ちに増やすことが困難である場合でも、本解説における「望ましい資産管理項目」として、型番、ハードウェアリビジョン、ファームウェア及びソフトウェアのバージョン、導入日、サポート終了日、SBOMの有無、脆弱性情報の連絡先、更新プログラムの署名鍵を管理する主体、遠隔保守の有無及び接続先、保守を実施する国又は地域、代替製品の有無並びに想定交換日数を例示することを求めます。 クラウドサービスについても、サービス名及び提供事業者名だけでなく、利用リジョン、データ及びログの保存地域、再委託先、管理者アクセスが可能な国又は地域、障害又は侵害発生時の通知時間、契約終了時のデータ返却及び消去方法を管理項目として示すことが適切です。解説案自身も、クラウド事業者との責任分界及び通知条件をSLA、SLO又は利用規約で確認することが望ましいとしています。 製造者の所在地又は国籍だけで安全性を一律に判断することは適切ではありません。他方で、製品の設計主体、ソースコードの管理主体、更新用署名鍵の保有主体、遠隔保守権限、準拠法、最終的な親法人及び代替調達可能性は、経済安全保障上の客観的な評価項目となります。外国法令により、事業者に対して政府機関への技術的支援又は協力が義務付けられ得る法域もあるため、サーバーが日本国内に存在することだけでリスクが解消されるとは限りません。個人情報保護委員会の外国制度調査においても、中国のネットワーク運営者には公安機関又は国家安全機関への技術的支援及び協力義務がある旨が整理されています。	御指摘の「望ましい資産管理項目」につきましては、表3「任意で届け出ることが望ましい事項」のバージョン情報において、「当該資産のバージョン情報（OS/ファームウェア/ソフトウェアのバージョン等）を記入する。」としております。 御指摘のクラウドについての報告の考え方につきましては、本解説7-1 Q4に記載しているとおりです。 広く一般に使用されている電子計算機につきましては、本解説3-1-1に記載のとおり、告示で指定するものについて、特定重要電子計算機の届出は不要です

No.	御意見の要旨	御意見に対する主な考え方
24	したがって、国内製品を無条件に優遇し、国外製品を一律に排除するのではなく、国内での設計検証、脆弱性対応、ファームウェア更新、修理及び代替調達が可能かという「国内運用継続性」を評価する仕組みが必要です。ルーター、L3スイッチ、ファイアウォール、VPN装置及び認証基盤について、国内で保守できる製品が複数存在する場合は複数供給者を確保し、代替がない場合は交換用機器の備蓄又は移行計画を求めることが合理的です。 資産管理負担について、仮に一事業者が特定重要電子計算機を1,000件保有し、初回の詳細登録に1件10分を要するとすれば、作業量は約167時間です。年1回の確認を1件3分とすれば、年間約50時間です。人件費を1時間5,000円と仮定した場合、初回約84万円、年間約25万円となります。これは試算にすぎませんが、重大インシデント発生時に20人が8時間対応した場合の160人時間とほぼ同程度です。したがって、適切な資産台帳の整備負担は、重大事故1日分程度の対応工数であり、社会基盤事業者にとって過大とは言いきいと考えます。 一方、広く一般に使用される同一製品を多数の事業者が重複して登録することは非効率です。政府が製品名、製造者名、型番、脆弱性情報及びサポート期限を管理する共通製品マスターを整備し、事業者は自社の台数、設置場所、バージョン及び接続関係だけを登録する方式が合理的です。これにより、届出負担と情報の不統一を同時に抑制できます。 報告期限については、解説案では発生を認知した後「速やかに」第一報を提出し、認知日から30日以内に詳細な報告書を提出する構成です。 しかし、クラウド、委託先又は共同利用設備では、特別社会基盤事業者自身が侵害を直接認知できず、管理事業者からの通知を待つ場合があります。各事業者の契約条件によって通知時期が異なると、「速やかに」の起点そのものが不均一になります。 そこで、法的期限を変更するものではない運用上の目安として、重大性が高い事象については、委託先又はクラウド事業者から特別社会基盤事業者への通知を原則12時間以内、行政への概要報告を認知後24時間以内、判明事項の更新を72時間以内、最終報告を30日以内とする標準モデルを解説に示すことを求めます。事実関係が不明な段階では、未確定事項であることを明記して報告できるようにすれば、早期報告と正確性を両立できます。 共同利用設備については、解説案上、利用する複数の特別社会基盤事業者がそれぞれ報告義務を負います。責任主体を明確にする考え方には賛成しますが、同一事象について内容の異なる報告が重複すると、行政側の照合作業が増えます。共通のインシデント番号を付与し、代表事業者が技術的事実を一括報告し、各利用事業者が自社への影響及び対応のみを追記できる共同報告様式を設けることが適切です。 以上から、本解説に、製品名及び製造者名だけでは把握できないソフトウェア構成、遠隔管理、法的及び技術的支配、供給継続性並びに国内代替能力に関する管理項目を追加するとともに、委託先通知及び初動報告の定量的な目安を示すことを求めます。経済安全保障の目的は、特定国の製品を形式的に排除することではなく、日本国内で重要設備を検証し、更新し、修理し、代替できる能力を平時から維持することにあると考えます。	脆弱性情報等の届出は重要です。 報告期限の起算点につきましては、本解説5-5において、サイバーインシデント発生を認知した日としており、その認知方法の例示として「特定重要電子計算機に該当するクラウドサービス等について、クラウドサービス事業者等からインシデント通知があり、そのインシデントが特定侵害事象等と判定された」と記載した上で、「基幹インフラ事業者が速やかにインシデント発生を認知する体制整備が不可欠」と記載しております。 複数の特別社会基盤事業者が共同で利用している電子計算機につきましては、当該複数の特別社会基盤事業者が報告いただく必要がありますが、当該複数の特別社会基盤事業者間で情報を連携いただいた上で報告いただいて差し支えございません。 その他、頂いた御意見は、今後の運用における参考といたします。
25	■全般 各事業者が、2027年3月末までの初回届出や、インシデント報告を行う過程で、今回のガイドライン案では情報が不足している点等が出てくるのではと思われるため、そうした点を踏まえ、ガイドラインを適宜改定いただくことを希望します。 ■P.41 5-1-1 マルウェアの供用（法第2条第4項第1号、第5項） 「マルウェアが実行され得る状態」とはどのような状態であるかをより具体的に示していただくことを希望します。	本解説につきましては、サイバーセキュリティに関する情勢や特別社会基盤事業者の状況も踏まえ、適宜、改訂したいと考えております。また、御指摘を踏まえ、「マルウェアが実行され得る状態」を本解説5-1-1に追記しました。
	<<「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（特定重要電子計算機の届出及び特定侵害事象等の報告）（案）」（案件番号095260710）に対する意見>> <第1 意見の概要> 本解説案は、サイバー対処能力強化法に基づき、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を円滑に行わせ、特別社会基盤事業等におけるサイバーセキュリティの確保をより確実にするための実務指針として重要である。 しかし、本解説案には、現代のサイバー攻撃の主要な根本原因であるソフトウェア供給連鎖、実装言語、ランタイム、主要依存ライブラリ、SBOM（Software Bill of Materials）、及びメモリ安全性に関する観点が十分に盛り込まれていない。 本解説案は、特定重要電子計算機に組み込まれたオペレーティングシステム、ミドルウェア及びアプリケーションを届出対象として整理している。他方で、製品名及び製造者名だけでは、当該システムの実質的なリスクを把握するには不十分である。特定重要電子計算機の脆弱性は、しばしば表面上の製品名ではなく、その内部に含まれる実装言語、ランタイム、OSSライブラリ、ネイティブ拡張、暗号ライブラリ、コンテナイメージ、ファームウェア等の複合的な供給連鎖に由来するからである。 よって、本解説に「ソフトウェア供給連鎖及びメモリ安全性に関する補足事項」を追加し、届出及び報告における推奨確認項目として、実装言語、ランタイム、主要依存ライブラリ、SBOMの有無、メモリ安全性評価の有無を明記することを求める。 <第2 立法趣旨との関係> サイバー対処能力強化法制の立法趣旨は、単にサイバー攻撃発生後の報告件数を増やすことではなく、官民の情報共有を通じて被害拡大を防ぎ、重要インフラの機能維持を確保し、再発防止と国家全体のサイバー対処能力を高める点にある。 国会審議においても、同法案は、官民の情報共有、インシデント報告、通信情報の利用、アクセス・無害化措置等を通じ、政府及び重要インフラのサイバー防御を強化する制度として説明されている。また、政府側答弁では、サイバー攻撃が発生した場合における被害組織の負担軽減と政府の対応迅速化が極めて重要であり、インシデント報告先の一元化、報告様式の統一化、報告基準・報告対象の明確化を進める必要がある旨が繰り返し述べられている。 この立法趣旨からすれば、本解説案は「事業者に何を報告させるか」を形式的に整理するだけでは足りない。事業者負担を抑えつつ、政府が集約した報告情報から、どのような技術的要因が特定侵害事象等を生じさせているのかを分析できる構造にする必要がある。すなわち、報告制度は、迅速な初動対応のための制度であると同時に、中長期的なリスク低減のための政策データ収集制度でもあるべきである。 この観点から、実装言語、ランタイム、主要依存ライブラリ、SBOM、メモリ安全性評価の有無を、少なくとも任意又は推奨の確認事項として整理することは、同法の立法趣旨に正面から合致する。 <第3 国会審議で示された「事業者負担」との調和> 本提案は、特別社会基盤事業者に過大な義務を課すものではない。国会審議では、迅速な報告と事業者負担のバランスが重要であること、報告窓口の一元化や報告様式の統一化によって被害組織の負担を軽減する必要があることが確認されている。 したがって、本意見は、直ちに特定のプログラミング言語の使用を義務付けるものでも、全ての依存ライブラリを逐一報告させるものでもない。提案するのは、以下のような段階的・実務的な整理である。 第一に、届出時には、既に事業者が資産管理、脆弱性管理、構成管理、クラウド管理、委託先管理等のために保有している情報を活用し、主要構成要素の実装言語、ランタイム、主要依存関係、SBOMの有無を任意又は推奨事項として整理する。 第二に、特定侵害事象等の報告時には、原因分析に資する範囲で、影響を受けたソフトウェアの実装言語、主要依存ライブラリ、既知脆弱性、メモリ安全性に関する問題の有無を補足記載できるようにする。 第三に、初動報告では最低限の情報にとどめ、詳細な供給連鎖情報は続報又は事後分析として提出可能にする。これにより、迅速性と分析可能性を両立できる。 このように、本提案は、事業者負担を増やすものではなく、既存の資産管理・SBOM・脆弱性管理の流れを報告制度に接続するものである。 <第4 メモリ安全性を明記すべき理由>	

No.	御意見の要旨	御意見に対する主な考え方
26	サイバー攻撃の多くは、ソフトウェアの欠陥、とりわけメモリ安全性に起因する脆弱性を利用して行われる。バッファオーバーフロー、use-after-free、ダングリングポインタ、二重解放、データ競合等は、C/C++等のメモリ非安全言語に典型的に見られる脆弱性であり、長年にわたり重大なサイバー攻撃の原因となってきた。	
	この問題は、単にアプリケーションがPythonやTypeScriptで書かれていれば解決するものではない。PythonはCPythonインタプリタに、JavaScript/TypeScriptはV8等のエンジンに依存し、機械学習、画像処理、暗号、圧縮、データベース、ネットワーク処理等の多くはC/C++又はCUDA等で書かれたネイティブ拡張に依存している。表層的な開発言語だけを見ても、供給連鎖全体のメモリ安全性は把握できない。	
	重要インフラにおいては、OS、ミドルウェア、アプリケーション、コンテナ、仮想化基盤、クラウドサービス、監視ツール、認証基盤、暗号ライブラリ、ファームウェアが相互に接続される。したがって、特定重要電子計算機の安全性を評価するには、製品名・製造者名に加え、ソフトウェア供給連鎖の構成と、そのメモリ安全性上のリスクを把握することが不可欠である。	
	＜第5 欧米の政策動向＞	
	米国では、メモリ安全性は国家サイバー戦略上の重要課題として位置付けられている。2024年、米国ホワイトハウス国家サイバー長官室（ONCD）は“Back to the Building Blocks: A Path Toward Secure and Measurable Software”を公表し、技術メーカーがメモリ安全なプログラミング言語を採用することにより、脆弱性の一類型を根本から減らすべきであると提言した。同報告書は、Morris Worm、Slammer、Heartbleed等、過去の重大インシデントがメモリ安全性脆弱性と深く関係してきたことを指摘し、プログラミング言語をサイバー空間の基礎構成要素として捉え直している。	本解説は、本解説1－1に記載のとおり、法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説をするものであり、御指摘の補足事項を本解説に記載する考えはありません。また、御指摘のアプライアンスに組み込まれたソフトウェアやファームウェアも含め、本解説2-1に記載のとおり特定重要電子計算機に当てはまらない電子計算機についても任意での届出を行うことが可能です。
	また、CISA及びNSAは、メモリ安全言語に関するガイダンスを継続的に公表し、重要インフラ組織及びソフトウェア製造者に対し、メモリ安全性ロードマップの策定、言語レベルの保護、ライブラリ支援、ツール整備、開発者教育等を求めている。これは、サイバーセキュリティをエンドユーザーの運用努力だけに委ねるのではなく、製品・ソフトウェアの設計段階から脆弱性を作り込まない“secure by design”へ責任を移す国際的潮流である。	その他、頂いた御意見は、今後の参考といたします。
	EUにおいても、Cyber Resilience Actが2024年に発効し、デジタル要素を有する製品について、企画、設計、開発、保守を含むライフサイクル全体でのサイバーセキュリティ要件を導入した。同規則では、脆弱性管理、インシデント報告、製品ライフサイクルを通じた安全性確保が重視され、報告義務は2026年9月、主要義務は2027年12月から適用される。これは、重要インフラや接続機器において、ソフトウェア供給連鎖と脆弱性管理が法的義務として組み込まれる方向を示している。	
	したがって、日本のサイバー対処能力強化法制においても、単なるインシデント報告様式の整備にとどまらず、ソフトウェア供給連鎖、SBOM、メモリ安全性、secure-by-designを政策的に接続することが不可欠である。	
	＜第6 中国の動向との比較＞	
	中国も、サイバーセキュリティ法及び重要情報インフラ安全保障条例により、重要情報インフラ運営者に対し、技術的措置その他必要な措置を講じ、サイバー攻撃、侵入、破壊等から重要情報インフラを保護する義務を課している。中国の制度は、国家安全保障、サイバー主権、重要情報インフラ保護を強く前面に出す点で、日本・米国・EUとは制度思想を異にするが、重要インフラの供給連鎖と技術的管理を国家的課題として捉えている点は共通している。	
	日本は、過度な統制型モデルを採るべきではない。しかし、重要インフラの安全確保において、事業者任せの任意対応だけでは不十分である。日本が採るべき方向は、中国型の包括的統制ではなく、欧米型の透明性、相互運用性、説明責任、SBOM、メモリ安全性、secure-by-designを重視する開かれた制度設計である。	
	そのためにも、本解説案には、特定重要電子計算機の届出・報告を通じて、ソフトウェア供給連鎖のリスクを可視化し、政策的に分析可能な形で蓄積する観点を明示すべきである。	
	＜第7 アプライアンス及びファームウェアについて＞	
	本解説案では、アプライアンスについてはソフトウェアとハードウェアを包含した設備が届出対象となり、アプライアンスに組み込まれた各種プログラムは届出対象外とされている。また、アプライアンス以外の電子計算機についても、ファームウェアは届出対象外とされている。	
	この整理は、届出実務を簡素化する観点からは理解できる。しかし、サイバーリスクの実態から見ると、ファームウェア、BIOS/UEFI、ネットワーク機器の組み込みソフトウェア、ストレージ装置、監視装置、認証装置等は、攻撃者にとって極めて重要な侵入口となり得る。特に重要インフラにおいて、アプライアンスやファームウェアを一律にリスク評価の外に置くことは適切でない。	
	したがって、届出対象そのものを拡大しない場合であっても、補足事項として、アプライアンス及びファームウェアについても、供給者、バージョン、更新方針、SBOMの有無、既知脆弱性管理、メモリ安全性上の懸念を、事業者が可能な範囲で把握することが望ましい旨を明記すべきである。	
	＜第8 具体的提言＞	
	一 本解説の補足事項又は参考資料に、「ソフトウェア供給連鎖及びメモリ安全性の確認」という項目を追加すること。	
	二 特定重要電子計算機の届出時に、任意又は推奨事項として、主要構成要素の実装言語、ランタイム、主要依存ライブラリ、SBOMの有無、メモリ安全性評価の有無を整理することが望ましい旨を明記すること。	
	三 特定侵害事象等の報告において、原因分析に資する範囲で、影響を受けたソフトウェアの実装言語、依存関係、既知脆弱性、メモリ安全性上の問題の有無を記載できる欄又は補足説明を設けること。	
	四 初動報告では迅速性を優先し、詳細な供給連鎖情報は続報又は事後分析として提出可能とする運用を明記すること。	
	五 アプライアンス製品及びファームウェアについて、届出対象外と整理する場合であっても、重要インフラのリスク評価上は供給連鎖情報の把握が望ましい旨を補足すること。	
	六 政府は、報告情報を集計・分析する際、個別事業者名又は製品名を不必要に公表するのではなく、技術類型、実装言語、依存関係、脆弱性種別等の統計的傾向として整理し、重要インフラ全体の安全性向上に資する形でフィードバックすること。	
	七 将来的には、特定重要電子計算機に関する届出・報告制度を、SBOM、脆弱性管理、メモリ安全性ロードマップ、secure-by-design調達基準と接続し、日本全体の重要インフラ・ソフトウェア供給連鎖の安全性向上に活用すること。	
	＜第9 結論＞	
	本解説案は、サイバー対処能力強化法の実効性を左右する重要な実務文書である。国会審議で示されたとおり、同法制においては、被害組織の負担軽減、政府の対応迅速化、報告様式の統一化、報告対象の明確化が重要である。しかし、それと同時に、報告制度は、特定侵害事象等の技術的原因を分析し、同種事象の再発防止と中長期的なサイバー対処能力強化につなげるものでなければならない。	
	欧米では既に、メモリ安全言語、SBOM、secure-by-design、ソフトウェア供給連鎖管理が国家的なサイバー政策の中心に位置付けられている。中国も、制度思想は異なるものの、重要情報インフラの技術的保護を国家的課題として捉えている。日本が重要インフラの安全を実質的に確保するためには、形式的な製品名・製造者名の把握にとどまらず、ソフトウェアの実装構造、依存関係、メモリ安全性を可視化する制度運用が必要である。	
	本提案は、直ちに特定の実装言語を義務付けるものではない。事業者が自らのリスクを把握し、政府が政策的傾向を分析し、重要インフラ全体として安全な実装へ移行するための基礎情報を整備する提案である。	
	よって、本解説に、ソフトウェア供給連鎖及びメモリ安全性に関する補足事項を明記することを強く求める。	
	以上	

No.	御意見の要旨	御意見に対する主な考え方
27	●P50 5-3-3の9行目の「上記…の事象までには至らないものの、」という記載の「…」の部分ですが、参照箇所がないように見受けられます。丸囲み数字3は、正しくは5-3-3でしょうか。 ●P51 「法第5条では、特定侵害事象（又は当該特定侵害事象の原因となり得る事象）の発生を認知した時に報告を求めている。発生の認知とは、監視におけるイベントやアラートの発報のみをもって直ちに該当するものではないが、当該イベントやアラートの内容等を踏まえ、法第5条における特定侵害事象等に該当すると合理的に判断できる状態を指す。」とあります。報告様式の「発覚日時」には、この状態に至った日時を記載することでよいでしょうか。	・P50につきまして 御意見を踏まえ修正しました。 ・P51につきまして 御理解の通りです。
28	・今後設置される協議会に放送事業者が構成員等として参加する際や通信情報の利用の際に、報道や番組編集の自由への制約、及び報道の自由を支える取材源の秘匿の侵害につながるものとならないよう重ねて要望します。	頂いた御意見は、今後の運用における参考といたします。 なお、報道の自由等の取扱いについては最大限尊重してまいります。
29	今次のご照会のありました、法令等の具体的な指針として定められた解説（案）につきまして、法律の施行に向け大変時宜を得たものであり、また、4月に実施された「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際の意見等を反映いただいており、弊社として賛同いたします。その上で、運用にあたっては、多々判断に迷う事案も出てくると考えられることから、パブコメ等情報公開の上、継続的な見直しをお願いいたします。	頂いた御意見は、今後の運用における参考といたします。
30	提出者：一般社団法人 日本貿易会 情報システム委員会 要旨：商社自体は「特別社会基盤事業者」に該当しないが、商社も事業者へ重要設備を納入する中間業者（サプライヤー）として介し影響が想定されることから、以下の意見を提出する。 1. 意見内容：海外グループ会社が所有又は運用する電子計算機、及びグローバル共通クラウド基盤を利用する場合に、特別社会基盤事業者が届出等のために取得・記載すべき情報の範囲を明確化いただきたい。 【理由】解説案では、他組織（グループ会社等）が所有する場合、日本国外に存在する場合、クラウドサービスを使用する場合も該当し得る旨が示されている。一方、海外拠点・海外グループ会社が管理するシステムでは、日本法人が詳細な機器情報、構成情報、契約情報を取得できない場合がある。 2. 意見内容：SaaS等のクラウドサービス利用時に、サービス提供事業者から侵害の事実の通知を受けて初めて認知可能な場合は、当該通知を受領した時点を報告期限の起算点とすることを明記いただきたい。 【理由】SaaSでは契約者がアプリケーション、ミドルウェア、OSへの侵害を能動的に認知できない場合があるとされている。報告期限の起算点が明確でないと、契約者側で認知不能な期間について過度な負担が生じる。 3. 意見内容：ランサムウェア事案及びその他サイバー攻撃事案の速報期限である「認知した日から3から5日以内」について、被害拡大防止、証拠保全、業務継続対応を優先できるよう、少なくとも重要情報が未確定の場合は把握済み事項のみで速報可能である旨をより明確化いただきたい。 【理由】大規模インシデントでは、初動時点で攻撃範囲、侵入経路、影響システム、IoC等が確定していないことが多い。詳細情報の整理を優先しすぎると、封じ込めや業務継続対応に支障が生じるおそれがある。 4. 意見内容：IoC、攻撃手口・侵入経路、システム構成図、攻撃の時系列、フォレンジック結果報告書等については、速報段階では把握済みの範囲で足り、未確定情報は詳報又は続報で補足・訂正できることを、本文又は記載例で明確化いただきたい。 【理由】解説案では、報告事項が未把握又は未確定である場合は報告時点で把握できている範囲を記載すればよい旨、既報告の誤報箇所は続報等で訂正・補足することが望ましい旨が示されている。	・1.、につきまして 本解説2-1-1に記載の通り、対象となる電子計算機が日本国外に存在する場合は、諸外国においてデータの保管や移転制限に関する法律が施行されていることもあるため、この対応に留意が必要です。資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております資産届出に関する相談窓口までお問合せください。 ・2.、につきまして 本解説5-5のD)に記載の通り、クラウドサービス事業者等からインシデント認知があり、そのインシデントを特別社会基盤事業者が特定侵害事象等と判定した場合が、報告期限の起点となります。 ・3.、及び4.、につきまして 本解説6-4に記載の通り、「報告事項の全量が未把握又は未確定である場合は、報告時点で把握できている事項を記載すればよい」「また、既に行った報告に誤報箇所があった場合は、続報等で訂正・補足することが望ましい」としております。
31	【提出者に関する注記】 以下の意見は、当職が、特定重要電子計算機の供給者となり得る事業者の代理人弁護士として提出するものであり、当職ら自身の意見ではありません。 【対象箇所】 「2-1-1 特定社会基盤事業者が使用する電子計算機」 【意見】 1. 本項では、「特定社会基盤事業者が使用する電子計算機」には、特定社会基盤事業者が所有している電子計算機以外のものも含まれうるとした上で、そのような場合の例として、（ア）「実質的に他組織（グループ会社等）が所有している場合」、（イ）「クラウドサービスを使用する場合」、（ウ）「日本国外に存在する場合」、（エ）「他の特別社会基盤事業者と共同利用している場合又は共同で構築されている場合」及び（オ）「災害復旧サイトである場合」が並列的に記載されている。しかし、（ウ）「日本国外に存在する場合」及び（エ）「共同利用又は共同構築されている場合」は、（イ）「クラウドサービスを使用する場合」に含まれる場合が多いと考えられるため、（ウ）及び（エ）が（イ）のサブカテゴリーであるのか、それとも（イ）とは独立した項目であるのかを明確にしていきたい。 2. 本項では、上記（ア）「実質的に他組織（グループ会社等）が所有している場合」に関し、届出等に必要情報の提供を他組織に求める場合に当たって、独占禁止法、中小受託取引適正化法及び特定受託事業者に係る取引の適正化等に関する法律に違反しないよう留意すべき旨が記載されている。もっとも、この留意事項は、グループ会社等が機器を所有する場合に限らず、クラウドサービス事業者、システムベンダーその他の供給者に情報提供を求める場合にも共通して妥当するため、その旨を明確にしていきたい。 3. また、供給者から提供を求める情報には、システム構成、開発環境等の営業秘密その他の機微な技術情報が含まれうることから、不正競争防止法上の営業秘密の保護にも言及いただきたい。 4. 供給者の営業秘密を特別社会基盤事業者に開示することが適切でない場合に備え、経済安全保障推進法に基づく届出と同様に、特別社会基盤事業者が供給者による直接提出を利用する旨を届け出た上で、供給者が機微な情報を所管大臣に直接提出できる仕組みを設けていただきたい。	・1.、につきまして （ウ）及び（エ）は（イ）と独立した項目です。 ・2.、につきまして 御意見を踏まえ修正しました。 ・3.、及び4.、につきまして 資産届出等をしていただくにあたり、不正競争防止法に留意すべき場面が想定しづらいことから、本解説には記載していませんが、疑義等ございましたら、特別社会基盤事業者向けに設置しております資産届出に関する相談窓口にご相談いただきますようお願いいたします。

No.	御意見の要旨	御意見に対する主な考え方
32	本案に強く反対する。 サイバー攻撃への対策が必要であること自体は否定しない。しかし、「サイバー安全保障」を理由として、民間事業者から政府に報告される情報の範囲を拡大し、政府による情報把握を強化することには重大な懸念がある。 特に問題なのは、サイバー攻撃に関する報告の中に、個人情報、通信に関する情報、企業秘密、システム構成、脆弱性情報など、極めて機微性の高い情報が含まれる可能性があることである。 政府が報告を受けた情報を、誰が、どの目的で、どの期間保有し、どの機関と共有できるのかが不明確なまま制度を運用すべきではない。 「サイバー攻撃対策」という目的が、行政機関による情報収集の際限のない拡大を正当化する根拠にはならない。 また、民間事業者に過大な報告義務を課すことで、本来サイバー攻撃への対応に投入すべき人的・金銭的資源が行政報告のために消費されることも懸念する。 報告対象、報告内容、情報の利用目的、保存期間、第三者提供、他省庁との共有、目的外利用の禁止について、国民にも事業者にも明確に分かる形で厳格な制限を設けるべきである。 安全保障を理由に政府が取得できる情報を拡大する制度には、強い歯止めが必要である。 十分な権利保障と透明性が確保されていない現状で本案を進めることには反対する。いったん撤回し、政府による情報収集権限の範囲と監視・監督制度を根本から見直すことを求める。	頂いた御意見は、今後の参考といたします。 資産届出やインシデント報告により頂いた情報につきましては、法において、内閣総理大臣が整理及び分析を行った上で、必要があると認めるときは、国の行政機関や特別社会基盤事業者等に提供できるとされております。また、当該情報については、法第8条に基づく安全管理措置を講じてまいります。
33	本案に強く反対する。 サイバー攻撃への対策が必要であること自体は否定しない。しかし、「サイバー安全保障」を理由として、民間事業者から政府に報告される情報の範囲を拡大し、政府による情報把握を強化することには重大な懸念がある。 特に問題なのは、サイバー攻撃に関する報告の中に、個人情報、通信に関する情報、企業秘密、システム構成、脆弱性情報など、極めて機微性の高い情報が含まれる可能性があることである。 政府が報告を受けた情報を、誰が、どの目的で、どの期間保有し、どの機関と共有できるのかが不明確なまま制度を運用すべきではない。 「サイバー攻撃対策」という目的が、行政機関による情報収集の際限のない拡大を正当化する根拠にはならない。 また、民間事業者に過大な報告義務を課すことで、本来サイバー攻撃への対応に投入すべき人的・金銭的資源が行政報告のために消費されることも懸念する。 報告対象、報告内容、情報の利用目的、保存期間、第三者提供、他省庁との共有、目的外利用の禁止について、国民にも事業者にも明確に分かる形で厳格な制限を設けるべきである。 安全保障を理由に政府が取得できる情報を拡大する制度には、強い歯止めが必要である。 十分な権利保障と透明性が確保されていない現状で本案を進めることには反対する。いったん撤回し、政府による情報収集権限の範囲と監視・監督制度を根本から見直すことを求める。	同上
34	公的機関や民間企業でインターネットに関する接続機器を国産の機器を使用し 中国製品徹底的に排除を求める。 日本を守る為 法律の改正やを拡大解釈しても早急に対処を願う。	頂いた御意見は、今後の運用における参考といたします。
35	5-3-1 DDoS 攻撃事案 について確認させていただきます 1.「機能停止又は機能低下」の有無は、利用者への全般的なサービス影響の有無だけでなく、重要システムの性能指標や防御措置の発動状況等も踏まえて判断するとの理解でよいか。また、i・iiの判定に疑義がある場合には、法定報告の要否を厳格に切り分けるのではなく、保守的に報告することを妨げないとの理解でよいか。 2.DDoS攻撃により機能停止・機能低下には至らなかったものの、そのおそれがあった事象について、法令上の報告義務がない場合であっても、脅威情報の共有を目的とした任意報告を行うことは可能か。また、その場合、速報・詳細の双方が必要となるのか、簡易な情報提供で足りるのかを明確化されたい。 3.DDoS攻撃について、速報時点では機能低下またはそのおそれがあると判断して報告したものの、後続調査の結果、実際の機能影響が限定的であり、法令上の報告対象に該当しないことが判明した場合、当該速報の提出自体は適切なものとして扱われるか。また、その場合に必要な詳細・続報の提出方法や、報告の取下げ・訂正の要否を明確化されたい。	・ 1. につきまして御理解の通りです。 ・ 2. につきまして任意報告は可能です。その場合、速報のみでも問題ございませんが、情報の分析等の観点から可能な限り詳細も報告ください。 ・ 3. につきまして本解説6-4に記載の通り、「既に行った報告に誤報箇所があった場合は、続報等で訂正・補足することが望ましい」としております。

No.	御意見の要旨	御意見に対する主な考え方
36	(1)ガイドラインの該当箇所：6-1 インシデント報告義務が発生するタイミングについて明確化いただきたい。特に、特定重要電子計算機の届出前に発生した事象についても報告対象となるのか、または届出済みの特定重要電子計算機で発生した事象のみが報告対象となるのかを明示いただきたい。 (2)ガイドラインの該当箇所：6-1 サイバー対処能力強化法において、インシデント報告の届出範囲となる「特定重要電子計算機」以外にも、「貸金業者向けの総合的な監督指針」や「割賦販売法(後払分野)に基づく監督の基本方針」において、サイバーセキュリティ事案が発生した際には、当局宛の「障害発生等報告書」の提出に関する報告が求められている。インシデント報告を行う際には、法令によって当局宛の届出方法が異なる事態を避ける為、報告方法の一本化を希望する。「特定重要電子計算機」以外の事案に関しても、今後構築予定の「官民連携基盤」での届出を行えるようにしていただきたい。 (3)ガイドラインの該当箇所：2-2-2 5-2 「特定重要電子計算機」の用語について、届出制度とインシデント報告制度で対象範囲が異なるにもかかわらず同一の用語が使用されているため、対象機器の誤認を招くおそれがある。制度ごとの対象範囲が明確に分かるよう、用語の区別又は補足説明をお願いしたい。	・(1)につきまして 資産届出の有無に関わらず、特定重要電子計算機に対する特定侵害事象等を認知した場合はインシデント報告が必要です。 ・(2)につきまして 関係省庁申合せに基づき、インシデント報告、その他の共通様式に記載の手続に関する官公署への報告等に際して、被害組織は共通様式又は別途法令等で定める様式に添付する形で報告等を行うことが可能とする予定です。また、官民連携基盤の整備により報告の窓口を一元化するとともに、共通様式による報告の受理を可能とする予定です。 ・(3)につきまして 特定重要電子計算機は法令上使用されており、法令と異なる用語を用いるとかえって混乱を招く恐れがあることから、用語を分ける考えはございません。その上で、御指摘の誤認を招かないよう、本解説2-1において、「特定重要電子計算機に該当する場合であっても、第4条に基づく届出の対象とならない場合があり、詳細は、3-1-1を参照されたい」と記載するなどしております。
37	特定重要電子計算機の届出や特定侵害事象等の報告により事業者から提供される情報について、適切な安全管理措置の下で取り扱われるとともに、その利用目的がサイバーセキュリティに限定され、共有範囲も必要最小限のものとすることが明確にされるよう求めます。特に、報告事項やログ等から情報提供者や内部告発者等の取材源が特定されるようなことがあってはならず、報道機関における取材情報の保護や取材源の秘匿に配慮した運用がなされるべきと考えます。 また、近く設置される協議会に報道機関が構成員として参加する場合、課せられる守秘義務が、報道機関の取材行為や報道活動、番組編集の自由に対する制限や干渉とならないよう配慮を求めます。併せて、今後予定されている「通信情報の利用」についても、報道の自由および取材源の秘匿を阻害することがないよう、慎重な運用を強く求めます。	資産届出やインシデント報告により頂いた情報について、法第8条に基づく安全管理措置を講じるとともに、法第8章の規定に基づき他の行政機関等に情報提供する際には、法第43条に基づき報告者の権利利益の保護に配慮するなど、法の規定に基づき適切に取り扱います。また、特定侵害事象等の報告は、取材源の報告を求めるものではありません。 その他頂いた御意見は、今後の運用における参考といたします。 なお、報道の自由等の取扱いについては最大限尊重してまいります。
38	「5-3-1 DDoS 攻撃事案」（p49）に関して、「DDoS攻撃による機能停止又は機能低下」の報告対象範囲について、以下2点をご教示いただきたい。軽微な事象まで報告対象とする場合、事業者の事務負担が過大となるほか、当局側でも重要な脅威の選別が困難になる懸念があるため、報告の判断基準を明確化していただきたい。 1. 報告対象の限定 本規定は、全ての攻撃を対象とするのではなく、特定重要電子計算機の稼働に実質的な影響（機能停止又は機能低下）が生じた場合のみを報告対象と解釈してよいか。 2.「機能低下」の定量的定義 「機能低下」と判断する具体的な基準（レスポンス遅延率やサービス影響範囲の閾値等）があればご教示いただきたい。	意見1につきまして、DDoS攻撃について、「（特定重要設備の）機能停止又は機能低下には至らなかった」ケースなど、日常的に発生している軽微な事象については、本解説5-2に記載のとおり、特定重要設備等に該当する特定重要電子計算機において発生した事象に限り、報告対象としております。 なお、DDoS攻撃による「（特定重要設備の）機能停止又は機能低下が発生した」ケースについては、仮に軽微であっても特定侵害事象に該当するため、報告対象となります。 意見2につきましては、「機能低下」の基準については、一律に定めることが困難であることから、通常の使用において支障が生じた場合を想定しております。

No.	御意見の要旨	御意見に対する主な考え方
	○項目 2-2-2 2. 特定重要設備と接続されている電子計算機（政令第1条第3項第2号及び主務省令第1条第1項） ○確認 該当項目は資産届出を行う際の特定重要電子計算機の該当性の検討にあたり、理解の助けになるものと存じます。 特定重要設備に接続されている「特定重要電子計算機」の対象につきまして、特定重要設備と設計上通信関係がある機器を指すものと理解しておりますが、相違ございませんでしょうか。 不正アクセスにより本来想定されていない通信が生じる可能性も加味し、到達可能性が否定できない機器についても一律に間接的に特定重要設備に接続されている「特定重要電子計算機」とみなすことは、対象機器の範囲が際限なく拡大するため、対応困難となります。 ○項目 2-2-2 2. 特定重要設備と接続されている電子計算機 [F] 特定重要電子計算機に関する重要データを保存している機器（主務省令第1条第1項第5号） ○確認 類型Fにつきましては、以下 1. 2. の両方を満たしたものが届出対象になるものと理解しております。 1. 特定重要設備と直接又は間接で通信関係があるもの 2. ネットワーク構成図や認証情報を保存している そのため、例えばネットワーク構成図を保存しているものの特定重要設備と通信関係がない機器については、届出対象外であると理解しておりますが、相違ございませんでしょうか。 ○項目 3-1-2 届出期限（主務省令第2条第1項等） ○意見 届出期限が明記されたことにより、今後の機器届出の計画が立てやすくなったものと理解しております。 一方で、特定重要設備の導入によって新たに「特定重要電子計算機」に該当することとなった設備につきまして、届出期限の起算日が当該設備に係る経済安全保障推進法上の届出を行った日を基準とするのか、当該設備が業務上の本番稼働を開始した日を基準とするのか明確でないため、この点について解説にてお示しいただけますと幸いです。 ○項目 3-1-4 届出事項（主務省令第2条第5項） (e)特定重要電子計算機の製造者名 ○確認 届出書の当該記載事項のうち「特別社会基盤事業者の名称」につきまして、経済安全保障推進法に係る基幹インフラ制度の届出対応では登記上の名称を記載しているところ、本届出におきましても同様に通称ではなく登記上の名称を記載すべきでしょうか。 (例) 通称：IBM 登記上の名称： （海外法人の場合）International Business Machines Corporation （日本法人の場合）日本アイ・ビー・エム株式会社 加えて、製造者が海外ベンダである場合、日本法人の名称と海外法人(本社)の名称のいずれを記載すべきかにつきましても、確認させていただきたく存じます。 ○項目 3-2-4 記載例（主務省令様式第2） ○確認 主務省令様式第2について、届出書本体の資料形式はA4サイズに限定されている一方で、別紙については特段言及がないところ、Excelファイル形式等の任意の形式で構わないという理解でよろしいでしょうか。 また、制度の解説案P.26に記載の主務省令様式第1については資料形式を指定する文言は記載されていないところ、主務省令様式第2と同様と考えてよろしいでしょうか。 ○項目 5-2 特定重要設備等における特定侵害事象の原因となり得る事象 ○確認 制度の解説案P.46には、「特定侵害事象の原因となり得る事象」として、特定重要電子計算機については「サイバー攻撃の成否を問わず、攻撃の試行を認知した場合も報告対象としている」との記載があります。特定重要設備又は特定重要設備と同一セグメントの機器（以下、特定重要設備等）にまで攻撃が到達するには、インターネットとの接続口の機器などに対する不正アクセスや社内ネットワーク内で不正通信を監視・遮断する仕組み等を通過する必要がありますが、特定重要設備等まで攻撃が到達していない限りにおいては、報告対象外ということでしょうか。 こうした不正アクセスは日常的に遮断しているものであり、仮に報告対象となる場合、被害組織の過度な報告負荷軽減という趣旨にも反するのではないかと考えております。 ○項目 5-2-1 特定重要設備等における特定侵害事象の原因となり得る事象【イ】 ○意見 制度の解説案P.47には、特定重要設備又は特定重要設備と同一セグメントの機器に導入している「アンチウイルス製品等のリアルタイムスキャンによる即日削除やコード実行停止がされた場合も含む」との記載がありますが、リアルタイムスキャンによる削除やコード実行停止ができれば、5-1 で定義されている「特定侵害事象」（重要電子計算機に対する特定不正行為により、当該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）の原因とはなり得ないと考えるところ、こうしたケースも報告が必要とされる理由を明記いただきたい。 ○項目 5-2-1 特定重要設備等における特定侵害事象の原因となり得る事象【二】 ○意見 特定重要設備又は特定重要設備と同一セグメントの機器で、行為が失敗し認証が突破されなかった場合も報告対象となる理由を明記いただきたい。 たとえば、「被害が発生せずとも、不正行為が行われた状況、つまり何らかの脆弱性等で特定重要設備又は特定重要設備と同一セグメントの機器にまで到達されている状況は、当該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となるため」等が考えられるかと存じます。	・2-2-2につきまして 「特定重要設備と設計上通信関係がある機器を指すもの」が具体的に何を意味するものが明らかではありませんが、「特定重要設備と電気通信回線で直接又は間接に接続されている電子計算機であって、当該特定重要設備に対し、当該特定重要設備の機能に影響を与える電磁的記録を送信する機能を有するもの」であれば対象となります。 ・2-2-2[F]につきまして 概ねご理解の通りですが、より正確な理解のため主務省令第1条第1項第5号や本解説2-2-2[F]をご覧ください。 ・3-1-2につきまして 届出対象となる特定重要電子計算機の要件を満たす電子計算機として使用を開始した時点が起算点となります。 ・3-1-4につきまして 前段については、経済安保推進法と同様に登記上の名称で記載ください。後段については、製造者が海外ベンダである場合は、海外法人（本社）の名称をお願いします。 ・3-2-4につきまして 主務省令様式第1及び第2のいずれもA4サイズとなります。また、別紙のサイズは任意ですが、A4又はA3サイズを推奨します。その他のファイル形式は問いません。 ・5-2につきまして 御指摘の「サイバー攻撃の成否を問わず、攻撃の試行を認知した場合も報告対象としている」との記載は、その直前の「特定重要設備等に該当する特定重要電子計算機」に関するものです。なお、特定重要設備等まで攻撃が到達してなくとも、特定重要設備等以外の電子計算機において発生した特定侵害事象及び特定侵害事象の痕跡が記録される事象は報告の対象となります。 ・5-2-1【イ】につきまして 仮にリアルタイムスキャンによる削除やコード実行停止ができなかった場合は、特定侵害事象になりうるためです。 ・5-2-1【ニ】につきまして 仮に情報又は指令の入力により電子計算機が作動し、利用が制限されている電子計算機が利用できるようになった場合には、特定侵害事象になりうるためです。 ・5-5につきまして 本解説5-5に記載の通り、発生 の認知とは、監視におけるイベントやアラートの発報のみをもって直ちに該当するものではなく、当該イベントやアラートの内容等を踏まえ、特定侵害事象等に該当すると合理的に判断できる状態を指しております。

No.	御意見の要旨	御意見に対する主な考え方
	○項目 5-5 特定侵害事象等の発生の認知 ○意見 「認知」の起算点について、単なる機械的検知ではなく、合理的な初期トリアージ後の時点であることを明確化いただきたい。具体的には次の解釈を制度の解説又はQ&Aに明記いただきたい。 あるいは、「認知」と「疑義を把握した段階」を区別いただきたい。 ----- 「認知」とは、単なる機械的アラート又は未確認の外部通報をいうものではなく、事業者が合理的な初期トリアージを行い、特定侵害事象等に該当する相当の蓋然性を把握した時点をいう。初期段階で確定していない事項は暫定情報として報告し、調査の進展に応じて訂正・補充できるものとする。 ----- ○項目 7-1 FAQ Q3. ○意見 複数の特別社会基盤事業者が共同で利用している電子計算機に関するインシデントが発生した場合、各事業者が個別にインシデント報告を作成・提出することとなりますと、報告内容にばらつきが生じるおそれがあるものと懸念しております。 つきましてはこうした共同利用サイトに係るインシデントについては、例えば電子計算機を運用している1社がインシデント報告を作成し、これを関係各社に共有した上で、各社がそれぞれ当該報告内容に基づきインシデント報告を提出するといった運用が可能かご教示ください。 ○項目 共同利用サービス・委託先サービスを利用する場合の届出事項 ○意見 共同利用サービス・委託先サービスを利用する場合の「使用」の考え方及び届出粒度について明確化いただきたい。そのために、解説案又はQ&Aにおいて以下を明確化いただきたい。あるいは、利用企業が通常把握している情報による届出方法を具体例で示していただきたい。 ----- 共同利用サービス（共同利用センター型、グループ共通サービス、SaaS型サービス）、委託先サービス（事務委託システム、BPO利用システム、外部運用基盤）を利用する場合の届出対象及び届出粒度について、具体例を用いて明示いただきたい。 ----- ○項目 特定侵害事象等の報告、申合せ目的、NCO共有、官民連携基盤 ○意見 早期報告者へのフィードバック、不利益防止、訂正可能性を明確化いただきたい。そのために、制度の解説に以下を明記いただきたい。 それが難しい場合は、早期報告を促進する観点から、可能な範囲で当局に集約された参考情報や注意喚起情報についてフィードバックいただける仕組みを期待します。 ----- 事業者が合理的な調査に基づき早期報告、暫定報告、訂正報告を誠意に行った場合、後日判明した事実に基づく訂正を不利益に扱わない。政府側は、可能な範囲で類似事例、IoC、封じ込め・復旧上の助言、関係機関調整状況等を報告者へフィードバックする。 ----- ○項目 全般 ○確認 提供いただいた脆弱性情報の取り扱いにつきましては、各社における対応状況は何かの方法でご報告をさせていただく運用など想定されていますでしょうか。 仮に想定されている場合、対応状況のご報告に際してご指定のタイミングや様式等があればご教示いただけますと幸いです。	・7-1Q3につきまして 複数の特別社会基盤事業者が共同で利用している電子計算機につきましては、当該複数の特別社会基盤事業者が報告いただく必要がありますが、当該複数の特別社会基盤事業者間で情報を連携いただいた上で報告いただいて差し支えございません。 ・「共同利用サービス・委託先サービスを利用する場合の届出事項」につきまして 共同利用サービスや委託サービスについても、本解説7-1 Q3に記載のとおり資産届出の対象となります。届出粒度につきましては、本解説3-1-4を参照ください。 ・「特定侵害事象等の報告、申合せ目的、NCO共有、官民連携基盤」につきまして 本解説6-4に記載の通り、「既に行った報告に誤報箇所があった場合は、続報等で訂正・補足することが望ましい」としております。また、報告いただいた情報は、特別社会基盤事業者への情報提供等に活用いたします。 ・「全般」につきまして 提供した脆弱性情報の取扱いに関しては、具体的な運用を検討中です。
	1. 基本的な考え方 電気、通信、金融、鉄道その他の重要な社会基盤に対するサイバー攻撃は、一事業者の問題にとどまらず、国民生活、経済活動及び国家安全保障に重大な影響を及ぼす可能性があります。 特定重要電子計算機を把握し、特定侵害事象が発生した際に政府へ迅速に報告して攻撃情報を共有する制度の整備には賛成します。 一方、本制度によって政府にはシステム構成、IPアドレス、ソフトウェア、脆弱性、侵入経路、マルウェア、フォレンジック情報等の極めて重要な情報が集約されることになります。 したがって、事業者側だけでなく、政府、委託先、クラウド事業者等を含め、外国政府その他の外部勢力から重要情報を保護することを制度の重要な柱として明確にしてください。 2. 汎用品であることだけを理由として安全と判断しないこと 解説案では、広く一般的に使用される製品について一定の場合に届出を不要とする仕組みが示されています。 しかし、広く普及していることと、国家安全保障上安全であることは必ずしも同一ではないと考えます。 特に、外国政府の強い影響下にある企業が製造・提供する機器、ソフトウェア、クラウドサービス等については、一般的に普及している製品であっても、外国法による情報提供義務、遠隔アクセス、アップデート機能、バックドア、不透明な通信、サプライチェーン等のリスクを検証する必要があります。 したがって、汎用品として届出を不要とする場合でも、製造・提供企業及びその実質的支配者、外国政府との関係、適用される外国法、データ送信先、遠隔管理機能、更新経路、脆弱性対応等を踏まえた安全保障上のリスク評価を行ってください。 3. 特定国・企業に由来するリスクを客観的に評価する制度を設けること 単に外国製であることのみを理由として一律に排除するのではなく、国家安全保障上の具体的リスクに基づいて判断できる制度を求めます。 例えば、製造企業等が所在する国の法制度により政府・情報機関への情報提供又は協力を求められる可能性、外国政府による企業への実質的支配・影響、過去の重大な脆弱性・不正アクセス等への対応状況、ソースコードやアップデート経路の透明性、国外サーバーとの通信、遠隔操作機能、再委託先等を総合的に評価してください。 その結果、日本の重要社会基盤に使用することについて重大な安全保障上の危険性が認められる国・企業・製品等については、汎用品であっても届出除外の対象とせず、必要に応じて使用制限、追加的安全措置又は代替製品への移行を求められる仕組みを検討してください。	

No.	御意見の要旨	御意見に対する主な考え方
40	4. 外国企業・外国クラウドへの重要情報流出を防止すること 重要インフラで外国企業のクラウド、ソフトウェア、保守サービス等を利用する場合には、外国政府等による情報取得リスクを十分に評価してください。 特に、重要データの保存場所、国外移転、国外からの遠隔アクセス、管理者権限、暗号鍵の管理、ログの保存場所、障害・攻撃時の情報共有先等を把握することを求めます。 契約上「日本国内で保存する」とされているだけで安全と判断せず、外国企業本社や国外の技術者等が実質的にアクセス可能かについても確認してください。 重要度の高い情報については、国内保存、国内処理及び国内からの運用を原則とすることも検討してください。 5. 委託・再委託・再々委託まで把握すること 重要インフラ事業者自身が十分な対策を行っていても、委託先、再委託先等から侵入されれば意味がありません。 特別社会基盤事業者からシステム開発会社、クラウド事業者、保守事業者、さらにその再委託先へ業務が移ることで、重要情報へのアクセス経路が国外へ延びる可能性があります。 そのため、重要システムについては直接契約先だけでなく、重要情報又はシステムへアクセス可能な再委託・再々委託先まで把握し、所在地、実質的支配者、外国政府との関係、アクセス権限等を確認できる制度としてください。 事業者が把握できない再委託を安易に認めないことも必要と考えます。 6. ソフトウェア更新・遠隔保守を重要なリスクとして扱うこと 現在安全であることだけでなく、導入後に製品の性質が変化する可能性にも注意が必要です。 ファームウェア、OS、アプリケーション等の自動更新機能を通じて、製造元が重要システムへ新たなコードを配布できる場合があります。 また、遠隔保守機能が存在すれば、国外から重要設備へ接続できる可能性があります。 特定重要電子計算機について、更新サーバー、電子署名、更新内容、遠隔アクセス権限等を適切に管理し、重要設備については無条件の自動更新や恒常的な国外遠隔アクセスを制限することを検討してください。 7. 政府に集約される情報を最高水準で保護すること	・2. につきまして 資産届出いただく趣旨は、政府が特別社会基盤事業者の特定重要電子計算機の資産状況について把握しておくことにより、内閣総理大臣が特別社会基盤事業者に対し適切な情報共有を行うなど、特定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必要な対応を行うためです。 例えば、政府において、特定重要電子計算機の脆弱性情報を把握した場合、その脆弱性情報と同項に基づき届け出られた特定重要電子計算機の情報を照合させることにより、脆弱性のある特定重要電子計算機を使用する特別社会基盤事業者に対し、脆弱性情報を提供することが可能となります。 他方、業界、事業者問わず、広く一般に使用されている電子計算機については、資産状況を把握せずとも、全ての特別社会基盤事業者に脆弱性情報を提供することで、特別社会基盤事業者は必要な措置を講じることが可能です。そのため、告示では、特別社会基盤事業者の負担の軽減の観点から、資産届出を不要とする電子計算機を指定することとしております。 以上の趣旨を踏まえ、告示では、業界、事業者問わず広く使われており、かつ、特に主務省令第1条第1項第6号及び第2項第1号に規定する電子計算機において使われていることが想定されるなど、特別社会基盤事業者の負担軽減の効果が高いマイクロソフト・コーポレーションのWindows及びWindows Serverを指定することといたしました。 ・7. 及び8. につきまして 御指摘については、法第8条に基づく安全管理措置を講じてまいります。 ・9. につきまして 2. で回答の告示につきましては、今後の電子計算機の使用状況等を踏まえ、必要に応じ、見直してまいります。 ・11. につきまして 御指摘の報告内容に誤りがあった場合については、本解説6-4において、「報告事項の全量が未把握又は未確定である場合は、報告時点で把握できている事項を記載すればよい。また、既に行った報告に誤報箇所があった場合は、続報等で訂正・補足することが望ましい」と記載しております。 ・その他につきまして 頂いた御意見は、今後の運用における参考といたします。
	本制度により政府へ報告される情報には、攻撃元・攻撃先IPアドレス、システム構成、ソフトウェアの種類・バージョン、脆弱性、侵入経路、マルウェア、フォレンジック情報等が含まれます。 これらが一括して漏えいすれば、日本の重要インフラを攻撃するために悪用される危険があります。 政府内部においても必要最小限の者だけがアクセスできるよう権限を厳格に管理し、アクセスログを保存・監査してください。 また、政府が情報管理・システム運用等を民間企業へ委託する場合には、委託先・再委託先まで同等以上の安全基準を適用し、国外からのアクセスや外国政府等への情報流出を防止してください。 8. 内部者による情報流出への対策を強化すること サイバー攻撃は外部からだけでは限りません。 事業者、委託企業及び政府の内部者が、正当なアクセス権限を悪用して重要情報を持ち出す可能性についても対策が必要です。 特定重要電子計算機及び政府に集約された重要情報へのアクセスについて、最小権限、職務分離、多要素認証、アクセス記録、異常アクセス検知等を徹底し、重要情報の大量取得・持出し等を早期に発見できる制度を求めます。 9. 汎用品の指定を定期的に再評価すること 一度「広く一般的に使用される製品」として届出不要になった製品についても、永久に安全と判断すべきではありません。 新たな脆弱性、製造企業の資本関係の変更、外国政府との関係、外国法の変更、重大なサイバー事案等によってリスクは変化します。 したがって、汎用品の指定について定期的な再評価を行い、安全保障上のリスクが高まった場合には速やかに指定を見直せる制度としてください。 緊急性の高い脆弱性や安全保障上の問題が判明した場合には、通常の定期見直しを待たず、使用事業者への注意喚起、追加対策、届出対象化等を実施できる仕組みを求めます。 10. 国内で代替できる重要技術を育成すること 安全保障上問題のある外国製品等への依存を減らすには、単に使用を禁止するだけでは十分ではありません。 重要インフラを支えるサーバー、ネットワーク機器、クラウド、セキュリティ製品、ソフトウェア等について、国内で代替可能な技術・企業・人材を育成する政策も必要です。 特定の外国企業又は外国製品へ過度に依存し、問題が発覚しても短期間で切り替えられない状態そのものをサプライチェーン上のリスクとして評価してください。 重要設備について代替可能性を把握し、必要に応じて複数調達先の確保や国内技術への移行計画を策定することを要望します。 11. 重大な虚偽報告・隠蔽と善意の迅速報告を区別すること サイバー攻撃発生直後には全容を把握できないため、速報段階で情報が不完全であることを過度に問題視すれば、事業者が報告をためらう可能性があります。 善意による迅速な速報については、その後の続報による訂正・補足を認め、積極的な情報共有を促してください。 一方、重大な侵害を認識しながら故意に報告しなかった場合、重要事実を隠蔽した場合、虚偽報告を行った場合等については厳格に対応してください。 12. 事故後の検証と他の重要インフラへの展開 重大な侵害事象が発生した場合には、単に報告を受けて終了するのではなく、原因、侵入経路、悪用された脆弱性、委託構造、製品・サービス、対応上の問題等を分析してください。 同種の設備を使用する他の特別社会基盤事業者に同様の危険が存在する場合には、機密情報を適切に保護しながら速やかに必要な防御情報を共有してください。 特に広く普及している汎用品に重大な脆弱性等が確認された場合には、多数の重要インフラへ同時に影響する可能性を考慮し、迅速な横断的対応を求めます。 13. 総括 重要インフラのサイバーセキュリティでは、「広く普及している製品だから安全」「大手企業だから安全」「クラウドだから安全」と機械的に判断すべきではありません。 特に外国政府の影響、外国法による情報提供義務、企業の実質的支配関係、国外へのデータ送信、遠隔管理、ソフトウェア更新、委託・再委託構造等を含めて具体的なリスクを評価することを求めます。 その結果、国家安全保障上の重大なリスクが客観的に確認された製品・サービスについては、一般に広く普及している汎用品であっても届出除外の対象とせず、追加的な安全措置、使用制限又は代替製品への移行を求められる制度としてください。 同時に、日本国内で重要インフラを支える技術・企業・人材を育成し、特定の外国企業・外国製品へ過度に依存しない体制を構築することを要望します。 本制度によって集約される情報そのものが国家安全保障上極めて重要であることを踏まえ、事業者だけでなく政府及びその委託先についても最高水準の情報管理、アクセス管理及びサプライチェーン管理を義務付け、日本の重要社会基盤に関する情報が外国政府その他の外部勢力へ流出・不正取得されない制度とすることを強く要望します。	

No.	御意見の要旨	御意見に対する主な考え方
41	令和8年8月16日 内閣府政策統括官（サイバー安全保障担当）付 御中 件名 「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（特定重要電子計算機の届出及び特定侵害事象等の報告）（案）」に対する意見 提出者の立場 減税派かつ日本人ファーストの立場から、国民負担の最小化と国家安全保障の徹底を最優先に、是々非々で意見を提出します。 ----- ### 一、の評価（是とする点） 本案は、特別社会基盤事業者に対し、特定重要電子計算機の届出と特定侵害事象等の報告を義務付けるものであり、以下の点で評価できます。 - 重要インフラのサイバー攻撃リスクを可視化し、迅速な対応を促す枠組みは、国民生活の基盤を守る上で必要不可欠です。 - 届出・報告の方法を官民連携プラットフォーム等で統一しようとする姿勢は、事業者の事務負担を一定程度軽減する方向性を示しており、減税派として「無駄な行政コストを増やさない」点で支持します。 - 経済安全保障推進法との重複回避を明記している点も、二重負担を避ける現実的な配慮として是とします。 ただし、これらは「最低限の守りの仕組み」に過ぎません。現状のままでは、中国をはじめとする敵対勢力によるサプライチェーン汚染や内部からの情報漏洩に対して、極めて脆弱です。以下、日本人ファーストの観点から、国民の生命・財産・主権を守るために不可欠な強化策を、是々非々で提案します。 ----- ### 二、是々非々の改善提案 #### （1）中国製品の排除を義務付けること（強く是） 現状の問題点 本案では、特定重要電子計算機の届出時に「製品名・製造者名」を記載させるに留まっています。これでは、中国製ハード・ソフト・ファームウェアが大量に混入したまま、重要インフラが稼働し続ける危険を放置しています。 提案 - 特別社会基盤事業者が使用する特定重要電子計算機（Type1から3全て）について、中国（香港・マカオ含む）製または中国資本企業が製造・供給する製品・部品・ソフトウェアの使用を原則禁止する。 - 例外は、代替不可能であることが客観的に証明され、かつ独立した第三者機関による徹底的なセキュリティ監査を受けた場合に限る。 - 既存導入分についても、移行計画の提出を義務化し、3年以内の完全排除を求める。 是とする理由（減税派・日本人ファースト 中国製品はバックドアや脆弱性を意図的に埋め込まれるリスクが極めて高く、一度侵入されれば復旧コストは天文的になります。排除することで、将来の巨額な被害対応費用（税金投入）を未然に防ぎます。日本人ファーストの観点からも、自国の重要インフラを敵対国の技術に依存させることは主権の放棄に等しい。 非とする余地 短期的な調達コスト増は避けられませんが、中長期的には国産・同盟国製品へのシフトが産業育成と税収増につながります。コスト増を理由に先送りすることは、減税派の立場から「目先の安さに囚われて将来の大増税を招く」愚策です。 #### （2）外国人および帰化人の雇用廃止（強く是） 現状の問題点 本案は機器・事象の報告に終始し、人的セキュリティに全く触れていません。重要インフラの現場やシステム管理に外国籍者や帰化人が従事している実態は、スパイ行為の温床です。 提案 - 特別社会基盤事業者の特定重要電子計算機の管理・運用・保守・監視に関わるすべての職位について、日本国籍を有し、かつ帰化していない者（出生による日本国民）のみを雇用・配置することを義務付ける。 - 既に雇用されている外国人・帰化人については、移行期間を設けた上で、段階的に解雇または配置転換を命じる。 - 違反した場合、事業者に対する行政処分と、個人に対する刑事罰を設ける。 是とする理由 サイバー攻撃の多くは「内部協力者」を介して実行されます。外国人・帰化人は本国や親族への圧力を受けやすく、忠誠心の担保が困難です。日本人ファーストの原則として、国民の生命線を守る職は、純然たる日本国民が担うべきです。 減税派としても、一度重大インシデントが起きれば、復旧・補償・再発防止に膨大な税金が投入されます。予防コストとして人的排除を徹底することは、財政健全化に直結します。 非とする余地 即時解雇による訴訟リスクや一時的な人手不足は発生しますが、これは「安全保障を人件費で測る」本末転倒な議論です。国家の存続が危うい状況で「多様性」を優先する余裕はありません。 #### （3）通信傍受による犯罪者の特定を強化すること（是）	

頂いた御意見は、今後の運用における参考といたします。

No.	御意見の要旨	御意見に対する主な考え方
	現状の問題点 報告義務だけでは、攻撃者の特定・検挙に至りません。サイバー犯罪者は匿名性の高い通信手段を悪用しています。 提案 - 特定侵害事象が報告された場合、警察・公安当局が関連する通信を迅速に傍受できるよう、通信傍受法の特例をサイバー対処能力強化法に明記する。 - 重要インフラに関する通信については、事前令状の要件を緩和し、事後報告で足りる緊急傍受を可能とする。 是とする理由 犯罪者を特定・処罰できなければ、報告制度は「被害の記録」に終わります。日本人ファーストとして、加害者を確実に検挙し、再発を抑止することは当然の責務です。 減税派としても、未検挙のまま被害が拡大すれば、保険料や税金での補填が増えるだけです。 非とする余地 プライバシー侵害の懸念はあります。しかし、重要インフラのサイバー攻撃は「戦争行為」に近いものであり、平時の個人通信と同列に扱うべきではありません。透明性のある事後審査制度を併設すれば、濫用は抑制可能です。 ##### （4）重要書類・データの持ち出し禁止と、紛失者への刑事罰創設（強く是） 現状の問題点 本案は電子計算機の届出と侵害事象の報告に限定され、紙・電子を問わず重要情報の物理的・論理的持ち出しに関する規制がありません。 提案 - 特別社会基盤事業者が保有する特定重要電子計算機に関する設計図、設定情報、ログ、認証情報等の重要書類・データについて、事業所外への持ち出しを原則禁止する。 - やむを得ない場合は、厳格な許可制とし、暗号化・追跡機能を義務付ける。 - 故意または過失により紛失・漏洩させた者に対し、刑事罰（懲役・罰金）を新設する。過失の場合でも「重大な過失」として処罰対象とする。 是とする理由 情報漏洩の最大の経路は「持ち出し」と「紛失」です。これを放置すれば、届出・報告制度は形骸化します。日本人ファーストの立場から、国民の安全を脅かす情報の流出は、国家への背信行為として厳罰化すべきです。 減税派としても、漏洩後の対応費用（調査・補償・システム再構築）は結局税金で賄われます。予防的な刑事罰は、最もコスト効率の高い抑止力です。 非とする余地 現場の利便性が低下するとの声は出るでしょう。しかし、利便性を優先して国家が危険に晒されるなら、それは本末転倒です。厳格なルールこそが、長期的な安定と税負担軽減を実現します。 ----- ### 3. 総括（減税派・日本人ファーストの結論） 本案は「報告の仕組みを整える」という点で一定の是としますが、 - 中国製品の排除 - 外国人・帰化人の排除 - 通信傍受の強化 - 重要情報持ち出し禁止と紛失者の刑事罰 という本質的な防御策を欠いています。これらを盛り込まなければ、報告制度は「攻撃されてから記録するだけ」の形骸化したものになり、結果として国民の税金をより多く浪費することになります。 日本人ファーストの原則に立ち、 「日本の重要インフラは、日本人によって、日本と同盟国の技術で守り抜く」 という明確な方針を本案に明記することを強く求めます。 短期的なコストや利便性の低下を恐れて本質を先送りすることは、減税派としても「将来の大増税を招く無責任な選択」です。是々非々で、守るべきは守り、排除すべきは排除する。それが真に国民の負担を減らし、国家を存続させる道です。 以上、意見とします。	
42	p42 不正指令電磁的記録供用に該当しない例が2つ示されているが、いずれもダウンロード後にマルウェアの実行がなされれば、行為者の行為は不正指令電磁的記録供用に該当する可能性があると考えられる。なぜこれらが該当しないと言い切れるのか。 例1はむしろ典型事案だと思うし、例2はダウンロード者に実行する意思がなくても現に実行されれば供用に当たるはずである（他の罰条に見られる被害者等の主観要件はない）。 本解説は法務省クレジットの文書であり、刑法の解釈を示すものとして刑事実務上も意義があるためここで明確にしておきたい。	本解説1-1に記載のとおり、本解説は法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説するものであり、他の法令解釈を示すものではありません。 御指摘の通り、本解説5-1-1の該当しない例としては不正指令電磁的記録供用に該当する可能性があると考えられますので、記載について修正いたしました。
43	8頁目に「法第2条第2項第2号に規定する重要電子計算機」とありますが、法第2条第2項第2号では重要電子計算機を定義していません。指し示すものが必ずしも明確ではないため、表記を適正化すべきではないでしょうか。	御意見を踏まえ修正しました。
44	ガイドライン全体にわたり、事業者の報告手続きに関する負担軽減を図る方針に賛同します。今後は報告基準の明確化や汎用品（届け出不要対象）の告示等を通じて負担軽減策を明示的に具体化することを要望します。 サイバー対処能力強化法に基づく情報共有・対策のための協議会については、構成員には「守秘義務を伴う被害防止に関する情報を共有するとともに、必要な情報共有を求めることが可能」とされていますが、報道機関としての「報道の自由」、「取材源の秘匿」などの民主主義の根幹をなす価値を損なうものでないことが確約される必要があると考えます。 また、協議会の構成員になることによって、報道機関として独自の取材源、取材活動により、正当な手段によって取得した情報を報道する行為まで制限されることはあってはならないと考えます。	報告対象の具体例につきましては、本解説5.でお示しするとともに、御指摘の汎用品につきましては、告示でお示ししており、本解説3-1-1に本告示の内容を記載いたしました。 その他、頂いた御意見は、今後の参考といたします。 なお、報道の自由等の取扱いについては最大限尊重してまいります。

No.	御意見の要旨	御意見に対する主な考え方
45	弊社は、貴府のサイバー対処能力強化法及びその省令、ガイドライン等の制定を含む、特定不正行為による被害の防止に向けた活動を支持いたします。弊社は、本法の主旨に基づく適切な対応を通じて、貴府及び関係省庁における本法の円滑な施行に貢献させていただきます所存です。つきましては、次の点について確認させていただきたく存じます。 意見 1 【対象箇所】 「2-2-2 2特定重要設備と接続されている電子計算機（政令第 1 条第 3 項第 2 号及び主務省令第 1 条第 1 項）」及び「4-3-2 ステップ3-2 システム概略図（詳細版）の作成」 【意見】 2-2-2 [D] の解説では「通信経路にある全てのアクセス制御機器が対象ではなく、あくまで特定重要設備の直近にあるものが対象であること（中略）」旨の説明がございました。一方、4-3-2の図8においては、[E] の外側にある複数の多段階で構成されたFWがいずれも [D] に相当するもののように記載されていますが、これは2-2-2 [D] の説明からどのように解釈すればよろしいでしょうか。 意見 2 【対象箇所】 「3-1-4 届出事項（主務省令第 2 条第 5 項）」及び「3-1-5 記載例（主務省令様式第 1）」 【意見】 3-1-5の記載例にある「特定重要設備の区分」につきまして、3-1-4の該当項目の説明には「特定重要電子計算機が経済安全保障推進法の主務省令で規定する特定重要設備のうち、どの特定重要設備に関連するものかを記載する（複数記載可）」とあります。特定重要設備は、金融分野においては主務省令「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に基づく特定社会基盤事業者の指定等に関する内閣府令」の第一条の各号で規定されているものと理解しております。3-1-4の「どの特定重要設備に関連するものかを記載する」につきましては、当該主務省令の第一条の各号に基づき記載するということになりますでしょうか。 その場合、例えば、第一種金融商品取引業においては、 「第一種金融商品取引業に係る業務のうち、取引所金融商品市場における有価証券の売買若しくは市場デリバティブ取引又はこれらの媒介、取次ぎ若しくは代理（主務省令第一条第八号イ）を行う設備」といった内容を記載することが求められているということになりますでしょうか。 3-1-5の記載例では「○○設備」とだけ記載されていますが、3-1-4の説明内容から具体的にどのような内容を記載すればよいか、明確にいただけると幸いです。 意見 3 【対象箇所】 「3-1-4 届出事項（主務省令第 2 条第 5 項）」 【意見】 3-1-4の表 3 で言及されている「ソフトウェア」につきまして、「資産分類としてのソフトウェア」と「一般名詞としてのソフトウェア」の 2 種類の意味があるように思われました。 3-1-4届出事項の表 3 の「届出対象分類」にて、「アプライアンス製品/ソフトウェア/クラウドサービス/その他」として言及されているソフトウェアは、「資産分類としてのソフトウェア」との認識です。 一方、同表 3 の「バージョン情報」にて、「当該資産のバージョン情報（OS/ファームウェア/ソフトウェアのバージョン等）を記入する」におけるソフトウェアは「一般名詞としてのソフトウェア」と存じます。これは、ミドルウェアやアプリケーションなどのような、「資産分類としてのソフトウェア」よりも詳細な対象に関する情報の記載を期待されているものと想像しております。 このような同一の言葉でも指し示す対象が異なるものについては、その違いが分かるように説明いただけると幸甚です。 意見 4 【対象箇所】 「3-1-4 届出事項（主務省令第 2 条第 5 項）」及び「2-1-2 電子計算機に組み込まれたプログラム」 【意見】 3-1-4の表 3 の「バージョン情報」では、「当該資産のバージョン情報（OS/ファームウェア/ソフトウェアのバージョン等）を記入する」と、ファームウェアのバージョン等の記載に関する言及があります。 一方、3-1-1 では、アプライアンス製品はソフトウェアとハードウェアを包含した設備が届出対象であり、アプライアンスに組み込まれた各種プログラムは届出の対象外とあります。もし、ここでいう各種プログラムが、2-1-2で言及の「ファームウェア/OS/ミドルウェア/アプリケーション等」のことを指すのであれば（※）、アプライアンス製品において、ファームウェア単体での届出は不要なように思われました。 また、同じく3-1-1において、アプライアンス以外の場合についても「ファームウェアは届出の対象外」とされています。 以上より、ファームウェアのバージョンの記載が求められるのはどのようなケースかが判然としない（ファームウェア単体としてそのバージョンを記載するケースが必ずしも明確ではない）ようにも思われるのですが、どのような場合にファームウェアのバージョン情報の記載が望まれますでしょうか。 ※2-1-2にて、「特定重要電子計算機には、当該電子計算機に組み込まれたプログラム（電子計算機に対する指令であって、一の結果を得ることができるように組み合わせられたものをいう。）を含むとしており、ハードウェアのみならず、ファームウェア、オペレーティングシステム、ミドルウェア、アプリケーション等、ハードウェアに指令を与える無体物も特定重要電子計算機に含まれる」と言及されています。 意見 5 【対象箇所】 「2-2-2 2特定重要設備と接続されている電子計算機（政令第 1 条第 3 項第 2 号及び主務省令第 1 条第 1 項）」 【意見】 2-2-2の「[B] 特定重要電子計算機に係るシステムの認証を提供する機器」に関して、認証・認可には、特定重要設備の構成設備であるOS及びミドルウェアならびにネットワーク機器に関する認証・認可を行う機器と、特定重要設備の構成設備のうちいわゆる業務アプリケーションレベルの認証・認可を行う機器が含まれると思料いたします。 「サイバーセキュリティが害された場合において、特定重要設備の機能が停止し、又は低下するおそれがあるもの」を対象とするのであれば、前者の認証・認可を行う機器が2 [B] に該当するものと理解いたしますが、後者（業務アプリケーションレベル）の認証・認可を行う機器も2 [B] の対象となりますでしょうか。 意見 6 【対象箇所】 「2-2-2 2特定重要設備と接続されている電子計算機（政令第 1 条第 3 項第 2 号及び主務省令第 1 条第 1 項）」 【意見】 2-2-2の「[C] 特定重要設備を含むセグメントのDMZその他当該セグメントにアクセス可能な機器」に関して、当該機器を経由して、経済安全保障推進法における重要維持管理等の委託先等所有のネットワークに接続され、定期的に特定重要設備の構成設備、業務アプリケーションの更新、OS・ミドルウェアの更新を行います。この場合、当該更新に用いる機器（踏み台サーバ等）は [C] に該当し、届出が必要な重要電子計算機にあたると思料いたします。 このとき、当該更新に用いる機器へアクセス可能な環境下にある、重要維持管理等の委託先等所有の2 [B] 及び2 [A] は、同じく届出が必要な特定重要電子計算機にあたりますでしょうか。 意見 7 【対象箇所】 「2-2-3 3USB やクラウドサービス等の特定重要設備にデータを入力可能な電子計算機（政令第 1 条第 3 項第 3 号及び主務省令第 1 条第 2 項）」 【意見】 2-2-3にて、「例えば、特定重要設備の保守等の目的で、作成したデータ」を、定期的に当該特定重要設備に入力する場合は該当するとされています。この「保守等の目的で、作成したデータ」に、特定重要設備のソフトウェアの機能改善に資するデータ（いわゆる「パッチ」）などは、含まれますでしょうか。 また、定期的にとありますが、「定期的」と考える期間の目途・目安はございますでしょうか。	・意見 1 につきまして 頂いた御意見を踏まえ、図 8 を修正させていただきます。 ・意見 2 につきまして 経済安全保障推進法における導入計画書の「設備の種類」と同一の記載となります。 ・意見 3 につきまして 頂いた御意見を踏まえ、表 3 の「届出対象分類」を修正させていただきます。 ・意見 4 につきまして ファームウェアはアプライアンス製品以外において任意で届け出ることが望ましい事項としております。 ・意見 5 につきまして 御指摘の機器はいずれも②[B]の特定重要電子計算機に該当いたします。 ・意見 6 につきまして 御質問の電子計算機が届出対象か否かについては、各電子計算機の具体的な使用や委託の状況等によるため、一律に考え方を示すことは困難ですので、資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。 ・意見 7 につきまして パッチの適用も含まれます。また、「一定の期間」は、特定重要設備の使用環境等に応じて様々なケースが想定されるため、目安をお示しする考えはございません。

No.	御意見の要旨	御意見に対する主な考え方
46	本意見募集について、弊社内で設備主管部門から集約した意見を以下の通り4点入力させていただきます。 ----- 可搬型機器の取扱いについて 【該当箇所】 2-2-2 特定重要設備と接続されている電子計算機 【意見】 [特定重要設備と電気通信回線で直接又は間接に接続されている電子計算機]が対象とされていますが、可搬型端末や保守用パソコン等、一時的に接続される機器についても対象に含まれるか明確にしてください。 【理由】 設備に常設されている電子計算機と、一時的に接続される機器とでは管理方法や対象範囲の考え方が異なるため、制度上の対象範囲を明確にする必要があると考えます。 ----- 「広く一般的に使用されている製品」の指定時期について 【該当箇所】 3-1-1 広く一般的に使用されている製品 【意見】 [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]とありますが、当該指定について、制度開始までにいつ頃実施・通知される予定であるか示していただきたい。 【理由】 事業者においては届出対象設備の選定や管理方法の整理が必要となるため、対象製品の指定時期を早期に明確化いただきたい。 ----- 核物質防護情報との関係について 【該当箇所】 4 補足事項 【意見】 機器構成図及び機器管理リスト等の情報整備並びに政府への提出について記載されていますが、原子力発電所においては、当該情報に核物質防護情報(PP情報)に該当する内容が含まれる場合があります。このため、当該情報の提出に関して、原子力規制庁との制度的な調整が行われているか明確にしてください。 【理由】 原子力施設においては、セキュリティ上の観点から厳格に管理される情報が存在するため、関係法令・規制との整合性を事前に確認する必要があると考えます。 ----- 類型[D]における[直近]の解釈について 【該当箇所】 2-2-2 類型[D] 【意見】 [通信経路にあるすべてのアクセス制御機器が対象ではなく、あくまで特定重要設備の直近にあるものが対象]とされていますが、[直近]の具体的な範囲を明確にしてください。 例えば、特定重要設備から専用回線及び専用設計の計算機を経由し、一方向通信装置(情報ダイオード)へ接続される構成の場合、対象となるのは特定重要設備から見て最も近い情報ダイオード又はUTM等のいずれか一つと理解してよいのか、ご教示いただきたい。 また、通信経路上に存在する専用設計の計算機が、受信した情報の転送先を制御する機能を有する場合には、当該計算機が対象となり、一方向通信装置(情報ダイオード)は対象外となるのかについても明確にしてください。 さらに、図7においては、[直近]との説明がある一方で、類型[D]に該当する製品としてL3SW、SW、データダイオード等の複数機器が対象として記載されているように見受けられます。この点について、2-2-2[D]の説明との関係性を整理し、[直近]の考え方と図7の記載内容との整合性を明確にしてください。 【理由】 対象設備の範囲に関する解釈によって届出対象が大きく変わるため、事業者間で判断が分かれないう、具体例を含めた明確な基準が必要であると考えます。	・「可搬型機器の取扱いについて」 一時的に接続される機器についても対象に含まれ得ます。 ・「「広く一般的に使用されている製品」の指定時期について」 御指摘の汎用品につきましては、告示でお示ししており、本解説3-3に本告示の内容を記載いたしました。 ・「核物質防護情報との関係について」 資産届出は主務省令第2条で規定されております。主務省令を制定にあたっては、原子力規制庁を含む各省庁と協議を行っております。また、個別の資産届出について、原子力規制庁との制度的な調整を行う予定はありません。 ・「類型[D]における[直近]の解釈について」 御指摘の直近の具体的な範囲は、本解説の該当箇所に記載のとおり、ファイアウォール等であって、他のファイアウォール等を介さずに①の電子計算機に電気通信信号を送信するものが該当いたします。 また、「情報ダイオード」等は、当該ファイアウォール等に当てはまる機器の例を示したものです。また、この例示に当てはまらない場合でも、接続元のIPアドレスやセグメントを参照し、通信を許可、又は拒否すべきか制御を行う機器に該当する場合は対象ですが、不適当な通信を通過させない機能を有さず単に転送先を振り分けるだけのような機能であれば対象ではありません。 その上で、資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。
47	自社が所管する電子計算機の中には、他社（特定社会基盤事業者かどうかは問わない）の電子計算機（クラウドサービスを含む）と接続されているケースがある。他社の電子計算機が電気通信回線（公衆の用に供されているものではない）で接続されているのであれば、特定重要電子計算機となり得る可能性があるが、この場合、以下の懸念事項がある。国家及び国民の安全をサイバー攻撃から守るため、民にとって重要なのは自社所管の特定重要電子計算機に対し対策を行うことであり、また当該重要電子計算機の情報を官に提供することである。これにより、官は各特定社会基盤事業者が対象とする特定重要電子計算機の情報を収集することが可能となる。したがって、特定重要電子計算機の対象は自社が所管する電子計算機とすべきである。 【懸念事項】 ・脆弱性情報等を受け取ったとしても、他社の電子計算機であるため、何もできない（活用できない） ・他社の電子計算機の詳細が機微情報であることによる情報の開示の困難性が発生し、届出できない可能性あり ・届出対象の電子計算機が重複すること、また接続先に複数の他社が存在する場合は、重複の数が増加する ・届出変更の確認を他社に行う、あるいは他社から届出変更の確認が届くこととなり、運用の煩雑化につながる（接続先に複数の他社が存在する場合、都度届出の確認が届くこととなる）	特定重要電子計算機は、法第2条第2項第2号の規定及び本解説2-1-1の記載のとおり特定社会基盤事業者が使用している電子計算機が対象となります。特定社会基盤事業者が所有していない機器であっても、特定社会基盤事業者が使用している場合には、適切に情報を把握し、届け出ていただいた上で、国が脆弱性情報その他の情報を提供した場合には、委託先等に連携する、監視を強化するなど適切に対応いただくことが、重要電子計算機に対する不正な行為による被害を防止するために重要であると考えております。

No.	御意見の要旨	御意見に対する主な考え方
48	1. 共同利用されるシステムに係る届出について 複数の特別社会基盤事業者が共同で利用するシステム又はサービスについては、共同利用型サービスとして提供される性質上、サービス提供者が、利用者である特別社会基盤事業者に対して、詳細なシステム構成その他の機密性の高い情報を開示しない場合が多いと考えられる。 本制度においては、特定重要電子計算機に係る届出に際し、特定重要電子計算機と他の特定重要電子計算機又は特定重要設備との関係を示すシステム概略図等の提出が求められている。 このような情報には、サービス提供者にとって機密性の高い情報が含まれる場合があり、利用者である特別社会基盤事業者を経由して提出することが困難なケースが想定される。 また、経済安全保障推進法に基づく特定重要設備の導入等に係る手続においても、設備の供給者が保有する機微な情報について、その機密性に配慮した情報提出の枠組みが設けられている。 このため、複数の特別社会基盤事業者が共同利用するシステム等について、サービス提供者が保有するシステム構成その他の機密性の高い情報については、当該サービス提供者から特別社会基盤事業所管大臣等に直接提出できる仕組みを設けていただきたい。 その際、特別社会基盤事業者による届出と、サービス提供者から直接提出される情報とを、政府側で適切に紐付けることができる仕組みとすることを要望する。 2. 共同利用されるシステムに係る特定侵害事象等の報告について 複数の特別社会基盤事業者が共同利用するシステム又はサービスにおいて特定侵害事象等が発生した場合、現行の制度案では、各特別社会基盤事業者がそれぞれ報告主体となるものと理解している。 しかし、共同利用型サービスの場合、サイバーインシデントに関する技術的な情報を最も早く、かつ詳細に把握する主体は、サービス提供者である場合が多い。 このような場合に、サービス提供者から各特別社会基盤事業者への情報提供を経た上で、各事業者がそれぞれ事実関係を確認し、特別社会基盤事業所管大臣及び内閣総理大臣に報告する運用とすると、各事業者における確認内容や判断の相違等により、政府への報告までのリードタイムが長期化するおそれがある。 また、同一の事象について複数の特別社会基盤事業者から重複した報告が行われることにより、特別社会基盤事業者、サービス提供者及び政府のいずれにとっても事務負担が増加する可能性がある。 このため、複数の特別社会基盤事業者が共同利用するシステム又はサービスについては、サービス提供者から特別社会基盤事業所管大臣及び内閣総理大臣に対して、技術的事項等を直接報告できる仕組みを設けていただきたい。 特に、迅速な情報共有が必要となる特定侵害事象等については、サービス提供者からの直接報告を可能とすることが、被害の拡大防止及び政府による迅速なサイバー脅威分析にも資すると考える。	資産届出及びインシデント報告の提出者はあくまで「特別社会基盤事業者」とされており、法の趣旨を踏まえ、特別社会基盤事業者において適切に資産を管理し、又は特定侵害事象等の発生を認知した上、提出いただければと存じます。
49	政令第一条第三項第一号並びに当該箇所に紐づく解説より、特定重要設備は電子計算機とその他設備から構成されるものと認識している。であれば、図 1 において、特定重要電子計算機とはならない特定重要設備が存在すると考えており、図 1 の修正が必要である。	頂いた御意見を踏まえ、本解説2-1に注記を記載いたしました。
50	意見等は以下の通りです。 1. 今後の制度改革に関する（パワーポイント形式の場合）資料の構成だが、サイバーセキュリティの他の法律との位置づけをわかるようにまず最初のページに入れて頂けないか。 理由：サイバー対処能力強化法に関する説明も並行されて行われることが多く、また、「能力強化法」の説明においても、資産登録などは、経済安保推進法と重なるところも出てきている。今後、官民連携基盤で手続的には一定の統一がなされるのかと推察するが、一方で、言葉が微妙に異なるケースが多い。（特定社会基盤事業者（経済安保）/特別社会基盤事業社（能力強化法））、重要インフラ事業者（サイバーセキュリティ基本法）、基幹インフラ事業者（経済安保推進法）。サイバーセキュリティ関係の他の法律との関連がより理解しやすいように、説明資料に入れ込んでいただけないか。 2. 同様に資料の構成だが、実務的なサマリーを入れ込んで頂けないか。つまり、To Doを抜き出したもの。 理由：他の法律の説明も並行されるケースも多く（そちらでもコメントさせて頂く予定だが）、実務上、事業者が対応しなければならないことや、変更の影響が及ぶ点については、サマリーの形で冒頭に入れて頂けないか。資料はそもそも「法律や制度の改正」を逐一説明する意図で書かれているのだと認識するが、ボリュームが多く読み込んで理解するのに一定の時間が必要、事業者が対応すべきこと、影響が出ること、いつからそれに対応する必要があるのか、これらをサマリーとして入れて頂ければ実務者にとってはありがたく、万が一の対応もれも減少するのではと考える。 3. 経済安保推進法における導入等計画書の届出とサイバー対処能力強化法の資産届出との位置づけを明確にして頂きたい 理由：同上、能力強化法の資料を見ると、27ページ目以降に、経済安保推進法の導入等計画書に関する言及があるが、「基幹インフラ制度の技術的解説」で受信した資料では、届出のシステム化の変更について、の説明しかなく、官民連携基盤との位置づけ、あるいは全く別なのかが不明。 4. 特定重要設備を共同使用している場合の報告 説明会において、インシデント報告の場合は、共同使用している設備に問題があった場合、それぞれが報告する、あるいは、代表者が報告する際に他の事業者も連名で、というケースが考えられうる、とのことだった。「資産登録」は制度の解説8ページにある通り、共同使用者も全員対象になると認識している。さすれば、運用上は、共同使用者は、「代表事業者」に登録内容を聞いて、同じ内容を各社登録する、という運用と理解したがその認識で良いか。（もし、代表事業者だけで良い、となると、「経済安保推進法の導入等計画書」と矛盾が生じると考える。 5. 広く一般的に使用されている製品である場合の対応（解説21ページ） 届出不要とする、汎用品において、MS社のWindows/Windowsサーバーを含めていただいたことは非常に良いと考える。一方、MS社の製品は他にもSQLサーバなど、ITシステムを運用する上でほぼ必須のものがある。また、日本メーカー製のサーバ、世界標準のメーカーのサーバ等のハードウェアも対象として拡大できないか。 官民連携基盤において、サイバーセキュリティ関係の報告・届出（業法、能力強化法、経済安保推進法、サイバーセキュリティ基本法）が一元的に統一され、省庁や関係機関間での共有、また、事業者で共通する申請で、現在はそれぞれに工数のかかっているものが、システム内部で統合されること、この点に強い期待を持っておりますので、よろしく願い申し上げます。	・1. つきまして 本解説は、本解説1-1に記載のとおり、法第 2 条第 2 項第 2 号、第 4 条及び第 5 条の届出等に関する事項等を解説をするものであり、これらは御指摘の他の制度とは別個の制度です。 ・2. つきまして 御指摘の対応しなければならないことについて、網羅的に示すことは困難ですが、本解説の構成については1-3においてお示ししており、法そのものの概要についても、内閣府ウェブサイトにおいて公表しております。 ・3. つきまして 本制度と御指摘の導入等計画書の届出は別個の制度です。その上で、本解説3-1-6に記載の通り、経済安全保障推進法第52 条第 1 項又は第11 項の規定による当該特定重要設備の導入の届出を行っている場合には、導入等計画書や特別社会基盤事業者の連絡先を記載した書面をもって、特定重要電子計算機のうち、特定重要設備又は構成設備であるものの届出書に代えることができます。 ・4. つきまして 複数の特別社会基盤事業者が共同で利用している電子計算機につきましては、当該複数の特別社会基盤事業者が報告いただく必要がありますが、当該複数の特別社会基盤事業者間で情報を連携いただいた上で報告いただいて差し支えございません。 ・5. つきまして 資産届出いただく趣旨は、政府が特別社会基盤事業者の特定重要電子計算機の資産状況について把握しておくことにより、内閣総理大臣が特別社会基盤事業者に対し適切な情報共有を行うなど、特定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必要な対応を行うためです。 例えば、政府において、特定重要電子計算機の脆弱性情報を把握した場合、その脆弱性情報と同項に基づき届け出られた特定重要電子計算機の情報を照合させることにより、脆弱性のある特定重要電子計算機を使用する特別社会基盤事業者に対し、脆弱性情報を提供することが可能となります。 他方、業界、事業者問わず、広く一般に使用されている電子計算機については、資産状況を把握せずとも、全ての特別社会基盤事業者に脆弱性情報を提供することで、特別社会基盤事業者は必要な措置を講じることが可能です。そのため、告示では、特別社会基盤事業者の負担の軽減の観点から、資産届出を不要とする電子計算機を指定することとしております。 以上の趣旨を踏まえ、告示では、業界、事業者問わず広く使われており、かつ、特に主務省令第 1 条第 1 項第 6 号及び第 2 項第 1 号に規定する電子計算機において使われていることが想定されるなど、特別社会基盤事業者の負担軽減の効果が高いマイクロソフト・コーポレーションのWindows及びWindows Serverを指定することといたしました。 なお、本告示で指定する電子計算機につきましては、今後の電子計算機の使用状況等を踏まえ、必要に応じ、見直してまいります。 官民連携基盤に関していただいた御意見につきましては、今後の参考と致します。

No.	御意見の要旨	御意見に対する主な考え方
51	本解説案には重大な問題があります。 重要インフラをサイバー攻撃から保護するため、必要な情報共有やインシデント報告を行うこと自体の必要性は否定しません。しかし本案は、事業者から政府へどのような情報を提出させるかについては極めて詳細に規定している一方、政府が取得した情報を誰が、何の目的で利用し、どの機関と共有し、いつまで保存し、どのように削除し、その利用が適正だったかを誰が検証するのかという、国家側に対する歯止めが著しく不十分です。 このような片面的な制度設計には強く反対します。 本案では、特定重要電子計算機について、製品名、製造者名、クラウドサービス名・提供事業者名、システム相互の関係が分かる資料等の届出を求めています。さらに任意事項として、バージョン情報、グローバルIPアドレス、資産の管理主体等の提供を推奨し、グローバルIPアドレスについては、政府が保有するサイバー脅威情報と突合して潜在被害の発見等の分析を行うことまで明記されています。 また、特定重要設備等については、侵入や被害が実際に成功した場合だけでなく、認証突破に失敗した攻撃試行等も報告対象となり得ます。さらに法定報告の対象外であっても、標的型攻撃の痕跡等について任意報告を推奨しています。 インシデント報告では、攻撃元・攻撃先のIPアドレスやポート、URL、ドメイン、脆弱性情報、システム構成、攻撃対象アカウントID及び利用者属性、フォレンジック調査報告書等の提供まで想定されています。 これらは単なる一般的な「事故報告」ではありません。我が国の重要インフラについて、そのシステム構成、接続情報、管理主体、脆弱性、認証関係、攻撃状況等の極めて機微性の高い情報を、政府に継続的に集積させる制度です。 それにもかかわらず、本解説案では、収集後の情報管理について、それに見合う具体的かつ厳格な統制が示されていません。 これは看過できません。 第一に、取得した情報の利用目的を、当該サイバーインシデントへの対応及びサイバーセキュリティ確保に真に必要な範囲へ厳格に限定してください。目的外利用を原則として禁止し、捜査、治安、情報活動その他別目的への転用を認める場合には、その法的根拠、対象、要件、手続及び監督制度を明示すべきです。「政府内部で利用する」というだけで無制限な転用を許してはなりません。 第二に、取得情報を閲覧できる行政機関及び職員を必要最小限に限定し、他機関への提供、共有及び再共有について、対象機関、目的、要件を明文化してください。「関係省庁」という曖昧な概念の下で機微情報が政府内を横断的に流通することを認めるべきではありません。 第三に、情報の種類ごとに保存期間を明示し、利用目的を終えた情報を確実に削除する義務を設けてください。将来何かに利用できる可能性があるという理由だけで、重要インフラの詳細な情報を長期間蓄積することは許されません。 第四に、誰が、いつ、どの情報を閲覧・利用・提供したのかについてアクセスログ及び提供記録を保存し、政府内部から独立した立場による監査と事後検証を可能にしてください。不適切な閲覧、共有、目的外利用が判明した場合の責任及び是正措置も明確にすべきです。 第五に、「任意」「望ましい」とされる情報について、提出しなかったことを理由として不利益な取扱いを行わないことを明記してください。行政機関が事業者に対して提出を「推奨」する以上、形式上任意であっても、事実上断りにくい関係が生じることは容易に想定できます。任意提出を利用して法定の収集範囲を事実上拡張することは認められません。 第六に、アカウント利用者の属性、フォレンジック調査報告書、ネットワーク・システム構成その他の機微情報については、その情報がなければ具体的なサイバー対策を実施できない場合に限り取得するという、厳格な必要最小限原則を明記してください。 第七に、政府から事業者に対して行われる追加照会についても、目的、法的根拠、必要性、回答を求めることのできる情報の範囲を明確にしてください。「内容の確認」等の名目で、当初の報告範囲を超えて際限なく情報提供を求めることができる制度にしてはなりません。 第八に、政府自身が大量の重要インフラ情報を保有することで生じるリスクについても正面から評価してください。重要インフラのネットワーク構成、IPアドレス、製品・バージョン、管理主体、脆弱性、攻撃履歴等が一か所又は限られた行政機関に集積されれば、その情報基盤そのものが極めて価値の高い攻撃対象となります。漏えい、内部不正、不正アクセス等が発生した場合には、制度がサイバーセキュリティを高めるどころか、重要インフラ全体の新たな脆弱性を生みかねません。政府側にも、事業者に求めるのと同等以上の厳格な安全管理措置と説明責任を課すべきです。 サイバーセキュリティの必要性は、行政による情報収集を無限定に正当化する理由にはなりません。 「安全保障」「サイバー対策」という目的が重要であるからこそ、権限と情報が政府に集中する制度には、より強い統制、透明性、監督、検証可能性が必要です。 本案は「事業者に何を提出させるか」を詳細に定めるだけでなく、政府についても、 誰が取得するのか、何のために利用するのか、誰と共有するのか、いつまで保存するのか、いつ削除するのか、誰が監査するのか、違反時に誰が責任を負うのか を同じ水準で明確に規定すべきです。 必要最小限収集、厳格な目的限定、共有・再共有制限、保存期間と削除義務、アクセスログ、独立した監査、任意提供に関する不利益取扱い禁止を明文化しないまま本制度を運用することには、強く反対します。	本解説は、本解説1-1に記載のとおり、法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説をするものであり、御指摘の安全管理の記載は馴染まないものと考えておりますが、法第8条の規定も踏まえ、安全管理措置を徹底してまいります。

No.	御意見の要旨	御意見に対する主な考え方
52	【意見書】 「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（特定重要電子計算機の届出及び特定侵害事象等の報告）（案）」に関する意見 内閣府政策統括官（サイバー安全保障担当）付 御中 私は減税派および「日本人ファースト」の立場から、標記解説（案）に対し意見を提出いたします。 本解説（案）は、特別社会基盤事業者に対し、特定重要電子計算機の届出および特定侵害事象等の報告を義務付ける制度の運用指針を示すものです。サイバーセキュリティ強化自体は重要ですが、以下の点から強く懸念し、修正を求めます。 １． 減税の観点からの反対意見 本制度は、事業者に新たな届出・報告義務を課し、システム改修や専門人材の確保、報告作業の増加を強いるものです。これにより企業の事務負担・コストが大幅に増大し、最終的に製品・サービス価格の上昇や、公的支援の拡大を通じて国民の税負担増を招きます。減税を求める立場から、過剰な規制・報告義務の追加には反対します。届出・報告の対象範囲を最小限に絞り、既存の報告制度との重複を徹底的に排除し、事業者の負担を増やさない運用としてください。国の行政コストも最小化し、税金の無駄遣いを避けてください。 ２． 日本人ファーストの観点からの要望 特別社会基盤事業（重要インフラ）は日本の安全と経済の根幹です。外国資本や外国人が実質的に支配する事業者を対象から厳格に排除、または特別な監視・制限を課してください。外国企業による重要電子計算機の運用やデータ管理は、技術流出・スパイ活動のリスクを高め、日本人の利益を損ないます。届出・報告の際に、事業者の資本構成・役員の国籍・実質支配者を明示させ、日本人による運営を優先する仕組みを導入すべきです。 ３． その他の問題点と追加要望 - 特定侵害事象の定義や報告期限が曖昧だと、現場の混乱と過剰報告を招き、さらに負担増となります。明確かつ最小限の基準を定めてください。 - サイバー攻撃の多くが外国（特に特定の国）由来である実態を踏まえ、報告情報を迅速に防衛・公安機関と共有し、加害国への対抗措置（外交・経済制裁含む）に直結させる運用を明記してください。 - 関連して、重要インフラ周辺の土地・施設が外国人に取得されている事例（例：山口県笠佐島など、自衛隊基地近傍の離島）は、サイバー攻撃の拠点化リスクを高めます。こうした土地の収容（国有化）を推進し、物理・サイバーの両面で日本人ファーストの安全保障を徹底してください。 形式的な届出・報告の強化だけでは不十分です。事業者負担を増やさず、日本人の安全と国益を最優先とした実効的な制度としてください。	特定侵害事象の定義や報告期限について、特別社会基盤事業者において、混乱が生じないよう本解説において可能な限り具体的に記載するように努めてまいります。その他頂いた御意見は今後の参考といたします。
53	１． 報告手続きの運用について 特定侵害事象等の報告様式の統一化などにより、報告者の手続きの負担軽減を図る趣旨は理解するところです。法の想定する官民連携をさらに実効的なものとするためには、報告後の各主務省庁からの問い合わせ等についても、報告者の対応の負担を軽減するため、政府側の窓口を一元化するなど合理的な調整が図られることを要望します。 ２． 提供情報の管理について 特定重要計算機の届出や特定侵害事象等の報告により事業者から提供される情報については、適切な安全管理措置の下で取り扱われるとともに、その利用目的がサイバーセキュリティに限定され、提供される情報の共有範囲も必要最小限のものとすることが明確にされるよう求めます。 ３． 報道の自由への配慮について 近く設置される「被害防止のための情報共有及び対策に関する協議会」（法４５条）の構成員となった場合の守秘義務（同条7項）や、今後開始が予定されている「通信情報の利用」（同１７条以下）が、報道の自由への制約及び報道の自由を支える取材源の秘匿の侵害につながるものとならないよう強く要望します。	・ １．につきまして 今後の制度の運用における参考といたします。 ・ ２．につきまして 資産届出やインシデント報告により頂いた情報について、法第８条に基づく安全管理措置を講じるとともに、法第８章の規定に基づき他の行政機関等に情報提供する際には、法第43条に基づき報告者の権利利益の保護に配慮するなど、法の規定に基づき適切に取り扱います。 ・ ３．につきまして 今後の参考と致します。なお、報道の自由等の取扱いについては最大限尊重してまいります。
54	1.類型Dの電子計算機について「通信経路にある全てのアクセス制御機器が対象ではなく、あくまで特定重要設備の直近にあるものが対象であること」とご説明いただいており、当方では、特定重要設備と他のシステム又はネットワークとの間で通信許可制御を行う唯一の機器を想定しておりました。 一方、図8では、特定重要設備と同一ネットワークセグメントにあるL3SW-1に加え、特定重要設備のDMZに設置されたFWや、リモートオペレーションセンターのFWについても、類型Dに該当することが示されています。 ここでいう「あくまで特定重要設備の直近にあるもの」の判断基準について、具体例も含めてご教示いただけますでしょうか。 2.図4～図11にはシステム概略図（詳細版）が記載されていますが、理解向上のため、図中に特定重要設備についても図示いただくことをご検討いただけますでしょうか。	頂いた御意見を踏まえ、図4～図11を修正しました。
55	「任意」、「望ましい」と記載されている届出、報告については、「届出を行う特別社会基盤事業者」や「関連システムの情報を収集したり、報告をする上で協力を得るべき関係者」の過度な負担とならない範囲で行う旨を記載いただけないでしょうか。 「任意で届出・報告」を求めるだけではなく、本制度がめざす「基幹インフラにおけるサイバーセキュリティ確保、対応力強化」のために、負担に配慮した運用を併せて目指すべきと考えます。具体的には以下の箇所です。 ・p.7 特定重要電子計算機ではない機器についても任意での届出を行うことが可能である。 ・p.14 以下の機器は特定重要電子計算機に含まれないが、法目的に照らすと、アタックサーフェスに類する機器として任意で届出を行うことが望ましい。 ・p.24 表３ 任意で届け出ることが望ましい事項 ・p.32 届出対象となる特定重要電子計算機の特定、システム概略図と資産一覧の整備、及び政府への提出を行うことが望ましい。 ・p.33 システム概略図は以下の二つを作成することが望ましい。 ・p.51 以下のような事象があった場合については任意による報告を行うことを推奨する。 ・p.58 可能な限りマルウェア検体を提出することが望ましい。	「任意」及び「望ましい」と記載している届出、報告については、特別社会基盤事業者においてサイバー攻撃のリスク低減に資するものであり、趣旨を鑑みて各事業者において判断頂きたいと考えております。
56	p.13 図のタイトルで「特定重要設備とUSB で定期的なデータのやり取りがある場合」とありますが、図では「USB等で～」となっています。実際はUSBに限定するものではないので図の記載が適切と考えます。図の記載に合わせてタイトルを「USB等で」と修正いただけないでしょうか。	御指摘につきまして、記載を修正いたしました。

No.	御意見の要旨	御意見に対する主な考え方
57	p.13-14 2-2-1 (1)特定重要設備である電子計算機又は特定重要設備の一部を構成する電子計算機（一号電子計算機）の以下の文章について、「特定重要設備を構成する電子計算機」と「構成設備である電子計算機」で違いはあるのでしょうか。「構成設備である電子計算機もこれに含まれる」とあえて記載しているようにみえるため、その理由、意図についてご教示ください。 ----- 具体例としては、特定重要設備が複数の電子計算機から構成された一連のシステムを指す場合に当該複数の電子計算機が該当する。構成設備である電子計算機もこれに含まれる。	「特定重要設備の一部を構成する電子計算機」には、構成設備である電子計算機も含まれますが、構成設備の範囲や事業者の状況によっては、両者は完全に一致するものではないため、御指摘の箇所のような記載としております。
58	p.14 2-2-2 (2)特定重要設備と接続されている電子計算機 「ここという電気通信回線とは、有線又は無線、現実又は仮想、管理組織のいずれも問わない。」とありますが、「管理組織」の意味について教えてください。	御指摘につきまして、「有線・無線、物理・仮想の別を問わず、その管理主体も問わない。」に修正いたしました。
59	p.17 [F] 特定重要電子計算機に関する重要データを保存している機器 「一部の特定重要電子計算機のネットワーク構成図しか保存しないものは、(イ)に該当しない」について、 ・「一部」しか保存していなければ非該当となるのはどのような理由によるものでしょうか。考え方の説明が必要と思います。 ・「一部」とはどのような意味でしょうか。解釈のばらつきが生じないよう、何が欠けると「一部」になるのか明確に記載する必要があると思います。 ・同様に、(ロ)についても「全部を保存しているものでなければ対象外」と読めますので、「全部」或いは「一部」の定義を明確にする必要があると思います。	ネットワーク構成図には、社内外の説明用の概念図のようなものから機器の詳細が記載されたものまで様々なものが想定されますが、特に機密性が高く、よりピンポイントでの攻撃が可能になるグローバルIPアドレス又はプライベートIPアドレス入りのものであって、説明用などのために一時的に保存されるものを除くもののみを対象としております。「一部の特定重要電子計算機」とは、特別社会基盤事業者の使用する特定重要電子計算機のうち、一部という趣旨です。 また、識別符号を保存する電子計算機には、一の利用者の識別符号のみを保存しているものや業務のため一時的に保存しているものまで様々なものが想定されますが、特に流出した場合に影響の大きい、一の電子計算機の利用に係る全ての識別符号を保存するものであって、一時的に保存しているものを除くもののみを対象として規定しております。 頂いた御意見を踏まえ、本文を修正いたします。
60	p.17 2-2-3 (3)USB やクラウドサービス等の特定重要設備にデータを入力可能な電子計算機における「特定重要設備の保守等の目的で、作成したデータを定期的にUSB を介して特定重要設備に入力する場合～」について、 ・法の主旨から考えると非定期（例えば、何かの条件を満たしたときに入力するなど）の場合に対象外としてよいのでしょうか。 ・「定期的」の定義（例えばどれくらいの期間以内を想定しているかなど）を具体的に示す必要があると思います。	1つ目につきましては、御理解の通りとなります。 2つ目につきましては、「一定の期間」は、特定重要設備の使用環境等に応じて様々なケースが想定されるため、目安をお示しする考えはございません。
61	p.17 2-2-3 [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）」では、「具体例は、2-2-2 [A] のとおりである」とされており、2-2-2 [A] において具体的な対象機器が例示されていることから、その範囲を理解することができます。 一方、2-2-3 [B] については、「2-2-3 [A] に係るアクセス制御機能を有する機器が該当する」との記載にとどまり、具体的にどのような機器を想定しているのかが明確に読み取れません。2-2-3 [B] の具体例は、2-2-2 [B] における「具体的には、」以降に記載されている機器を指すとの理解でよいでしょうか。 また、読み手が対象範囲を理解できるよう、2-2-3 [B] においても具体例を明示する、もしくは該当箇所を示すなど、記載の見直しをご検討お願いします。	御理解の通りとなります。 また、御意見を踏まえ、「具体例は、2-2-2 [B] のとおりである。」を記載いたしました。
62	新制度の運用が報道の自由への制約及び取材源の秘匿の侵害につながることはないよう、以下の2点について、「制度の解説（案）」等に明記されることを要望いたします。 1．報道機関が取材等の報道目的で取得した情報については、法第5条に基づく「特定侵害事象等の報告」の対象外であることを明確に記載すること。 2．法第45条に基づく協議会において共有された情報と関連する事象であっても、独自取材により取得した情報の報道は、同条第7項の守秘義務違反に問われないこと、及び同条第5項の協力義務を拒める「正当な理由」に取材源の秘匿が含まれることを明示すること。	・1．につきまして 御指摘の特定侵害事象等の報告は、特別社会基盤事業者自らが使用する電子計算機において特定侵害事象等の発生を認知した場合に報告を求めるものであり、放送事業者が報道機関として取材等を通じて他の特別社会基盤事業者が使用する電子計算機において特定侵害事象等が発生したことを認知した場合に報告を求めるものではありません。また、本解説は、法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説をするものであり、分野横断的な内容を記載しております。 ・2．につきまして 頂いた御意見については、今後の参考といたします。 なお、報道の自由等の取扱いについては最大限尊重してまいります。

No.	御意見の要旨	御意見に対する主な考え方
63	p.28 3-2 変更届出（法第4条第3項、主務省令第3条）にて、「任意で届け出ることが望ましい事項に変更があった場合には、変更届出を提出することが望ましい。」とあり、負担に配慮したものと推察するが、任意としても一旦届出したものについては、変更届出を必須としないと、古い情報が混在して実態がわからず、返って混乱を招くと思われる。	御意見を踏まえ、修正させていただきます。
64	p.29 3-2-2 届出方法において、届出は官民連携基盤を介して行うと記載がある一方、「資産届出情報を格納したDVD 等による届出などの手続きについては、所管省庁に確認を行う。」とありますが、所管省庁によっては官民連携基盤以外の方法で届出を行う必要があるということでしょうか。届出は官民連携基盤に一元化すべきではないでしょうか。	原則として官民連携基盤により御提出いただきたいと考えておりますが、それ以外の方法で提出するニーズも想定し、当該箇所のように記載しております。
65	p.23 3-1-4 届出事項のところで、届出に必要な添付資料として、「各特定重要電子計算機と他の特定重要電子計算機又は特定重要設備との関係を示す資料（システムの概略を記載した資料等～(中略)～詳細なネットワーク構成図の提出は必須ではない。）を提出しなければならない。」とあるが、届出時に提出する「特定重要設備との関係を示す資料」として何が必須なのかが曖昧である。 現状の記載では、事業者（或いはその担当者）の判断や解釈がバラつくことが予想され、必要以上に詳細な情報を提出したり、逆に情報が不足し手戻りが発生するなど、過度な負担に繋がる可能性がある。「特定重要設備との関係を示す資料」には何を記載しなければならないのか、必須項目を具体的に示していただきたい。	本解説3-1-5の記載例で示している各特定重要電子計算機と他の特定重要電子計算機又は特定重要設備との関係を示す資料を想定しております。資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。
66	p.32 4. 補足事項 届出手順の一例において、「システム概略図と資産一覧の整備、及び政府への提出を行うことが望ましい。」とありますが、提出が必須なのはシステム概略図のうち「全体図」でしょうか。政府としてできるだけ柔軟に、広く情報収集する必要性は理解できますが、そうであっても最低限何を記載しなければならないのかを明確にする必要があると考えます。必須項目が曖昧ですと届出情報の過不足により、手続きの手戻りなど、事業者、所管省庁双方にとって過度な負担に繋がると考えます。届出の際の「システム概略図」として提出しなければならない「必須項目」を明確にさせていただきようお願い致します。 なお、事業会社で「詳細図」レベルの整理、把握は必要と思いますが、「詳細図」の提出を求めることは、届出情報の内容・レベルを鑑みると過剰ではないでしょうか。事業会社で把握しておくべきこと、届出が必要なこと(必須項目)は分けて記載をしていただけないでしょうか。	同上
67	○制度の解説案P.16「E.特定重要設備と同一セグメントの機器」（イ）には、「なお、同一サブネット、又は同一VLAN上の機器であっても、何らかの方法（論理的な方法を含む。）で通信が一方化されており、1の電子計算機への通信が行えない場合は該当しない。」とあります。 1の電子計算機にメーカーがあらかじめ通信定義を設定し、同一サブネット上の他の機器から送信されたデータを受信・取り込まない構成についても「通信の一方化」に該当する場合は、ネットワークインターフェース等で通信方向を制限する場合に限らず、1の電子計算機側の通信定義により受信を制限する場合も「一方化」に含まれることが分かるよう、具体例等を記載いただきますようお願いします。 ○制度の解説案P14 2-2-2 2 特定重要設備と接続されている電子計算機の説明について、特定重要設備と電気通信回線で間接に接続されている電子計算機であっても、その通信経路上に、特定重要設備から当該電子計算機への方向にのみ通信可能となるデータダイオードが設置されており、当該電子計算機から特定重要設備側へデータを送信できない構成となっている場合、当該電子計算機が特定重要電子計算機に関する重要データを保存しており、P.16 F（イ）の機器の条件を満たす場合であっても、2の電子計算機に該当しないことから、類型Fにも該当しないと考えられる。 具体的には、P.38 図7の構成となるが、上記認識に齟齬がなければ、オンプレ環境の社内システムサーバーに相当する電子計算機が、データダイオードの通信を受信する側に接続されている場合、情報系に、当該電子計算機が特定重要電子計算機に関する重要データを保存している場合であっても、2の電子計算機に該当しない場合には類型Fの対象とならないことについて、読み取れるよう具体例等を記載いただきますようお願いします。 ○制度の解説案P 1 4に記載する、2-2-2 2 特定重要設備と接続されている電子計算機（政令第1条第3項第2号及び主務省令第1条第1項）において、「特定重要設備と電気通信回線で直接又は間接に接続されている電子計算機」とあるが、可搬型保守用パソコン等、特定重要設備に一時的に接続する機器が対象外となる場合には、「一時的」とみなされる期間・接続態様の考え方について、例えば、障害対応等の緊急作業や保守・点検作業を行う間のみ接続するよう社内規定等で明記して実施している場合は除くなど、具体例を含めて明確に記載いただきますようお願いします。 ○原子力プラントに係る情報については、実用発電用原子炉の設置、運転等に関する規則の第9 1条第2項第27号に定める「特定核燃料物質の防護に関する秘密」に該当し、核物質防護情報の取扱いの観点から、情報公開できないものが含まれる。法に抵触する部分となるため、本制度に基づく届出やインシデント報告対応にあたっては、原子力規制庁との情報開示範囲について調整・連携のうえ、原子力規制庁と認識合わせした「特定核燃料物質の防護に関する秘密」は除くなどをガイドラインへ明記頂きたい。 ○インシデント報告は、法令・ガイドライン上、サイバー被害発生の速報と詳報は、「事業所管大臣及び内閣総理大臣に報告する」とされ、事業所管大臣宛の報告様式1から3の中で、N C Oにも情報共有可否記載欄が設けられています。 N C Oへの情報共有「否」とした場合、内閣総理大臣やN C Oへの提出を別途実施する必要があるのかも踏まえ、（10月1日から）サイバー攻撃時の報告様式の統一について予定されている事から、ガイドラインへ、報告様式統一後の省庁やN C Oや内閣総理大臣への報告についての明確な記載をお願いします。 ○ガイドラインのF A Qでは、「特定重要電子計算機に該当する電子計算機であれば、届出を行っていないくても報告対象となる」とされていますが、「資産届出未完了の場合であっても、特定重要電子計算機に該当すると事業者が判断するものについては報告義務が生じること」逆に「事業者として、該当しないと判断したものについては、報告義務が生じないこと」および「経過措置期間中の報告要否の判断方法・報告方法」について、ガイドラインへの明記をお願いします。	・2-2-2[E]につきまして ご質問の「通信の定義により受信を制限する場合」とは具体的に何かが明らかではないため、一律に考え方を示すことは困難です。資産届出の窓口まで詳細をお示しの上でご相談ください。 ・2-2-2（一つ目）につきまして システム概略図（詳細版）は、システム構成全体も考慮する必要があるため、ご提示いただいた内容では具体例をお示しすることは困難です。 ・2-2-2（二つ目）につきまして 接続の頻度や期間は該非判定の条件ではありません。 ・「原子力プラントに係る情報」につきまして 頂いた御意見は、今後の施策の参考といたします。 ・「インシデント報告」につきまして インシデント報告は、本解説6-1において明記しているとおり、事業所管大臣及び内閣総理大臣に対して行ってください。また、御指摘の報告様式については、各様式の記載の手引きに明記しているとおり、「共有等を希望しない」とした場合でも、法の規定に基づき内閣官房国家サイバー統括室等に情報共有されることがあります。 ・FAQにつきまして 7-1 Q1の「特定重要電子計算機に該当する電子計算機」には当然に資産届出が未完了の特定重要電子計算機（当該届出について経過措置が適用されるものも含む。）も含みますので、あえて明記しておりません。また、特定重要電子計算機に該当するかどうかは、政令及び主務省令の規定に基づき判断されます。その他、疑義がございましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。

No.	御意見の要旨	御意見に対する主な考え方
	1. 該当箇所：特定重要電子計算機の届出方法及び特定侵害事象等の報告方法 1. 意見・要望：特定重要電子計算機の届出方法及び特定侵害事象等の報告方法については、ともに「官民連携基盤」を介した提出が想定される。届出期限や報告期限が特例を含めて厳格に定められている中で、「官民連携基盤」の導入に関する詳細（例、システムにログインするためのユーザーIDの付与やパスワードリセット、届出事項・報告事項の登録、修正・変更方法等含む）について、特別社会基盤事業者への説明会の開催が急務と考える。また、その際、関連ベンダーのオブザーバー出席（聴講）も可能となるよう検討いただきたい。 2. 該当箇所：「官民連携基盤」 2. 意見・要望：特別社会基盤事業者が導入・運営する重要な社会インフラは、役務の安定供給が求められる。「官民連携基盤」には、個々の特別社会基盤事業者の最重要情報が格納・集積されることになるため、当該情報へのアクセスが出来る者に関しては、そのシステムベンダーを含め、国家公務員の同等の守秘義務を課すことが望ましいと考える。そのためには、同時に、国家公務員と同等の就業保障（身分保障）の提供が求められると考える。特に、特定侵害事象等の報告に関する情報漏洩は、二次被害を誘発する可能性もあり、不安なく情報提供が可能となるよう、実効性のある対策を講じるとともに、その対策内容については、少なくとも特別社会基盤事業者に十分な説明が必要と考える。 3. 該当箇所：P.11の類型の全体像 3. 意見・要望：特定侵害事象の例としてDDoS攻撃が挙げられている一方で、その主要な受け口である外部CDNが届出対象の類型に入っていないように見受けられます。特に、公衆網除外規定（[A]）が適用される範囲とCDNの位置付けについて明確化いただきたい。 4. 該当箇所：p.15 2.2.2[C]「監視サーバー」 4. 意見・要望：「監視サーバー」という記載があるが、監視サーバーは通常、アタックサーフィス上にはなく、運用管理セグメント（業務セグメントとは分離されており、外部からの到達性はないセグメント）に設置されているケースが多く見受けられる。「監視サーバー」を「踏み台サーバー、FTPサーバー」と並列に列記することで、運用管理セグメントの機器も届出対象になると誤認されないよう記載いただきたい。 5. 該当箇所：p.25「バージョン情報」 5. 意見・要望：「任意に届け出ることが望ましい」事項が列記されており、特別社会基盤事業者（以下、事業者）ごとに提出情報の粒度が異なることが許容されている一方で、政府による情報活用や注意喚起は制度全体として運用されることになる。このため、ある事業者が詳細な情報（例、バージョン情報）を提供したとしても、制度全体の実効性が情報量の少ない別の事業者のケースによって制度運用の実効性が制約される可能性があり、追加的な情報提出と事業者が得られる便益との関係が必ずしも明確ではないと考える。 68 特に、本制度は新たに導入が検討されているものであり、現時点では制度運用の実効性や、収集された情報がどのように活用されるのが十分に明らかでない。 多くの事業者にとって、法令対応に伴う情報収集・提出は一定の運用負担を伴う。任意とはいえ、提出情報の範囲を拡大する場合には、その負担に見合う形で、当局による情報活用や事業者へのフィードバックが実際に向上することを示す必要があると考える。 加えて、「広く一般に使用されている製品」は届出対象外とあり、届出対象となる製品については、バージョン情報の提出が任意とされていることから、例えば、オペレーティングシステムを例にとっても、当局が保有する情報の粒度には相当のばらつきが生じることが想定される。このような状況において、詳細情報を提出した事業者に対して十分に精緻な情報提供や注意喚起を行うことが実務上可能なのか、また制度全体としてどの程度の効果が期待できるのかはやや懸念がある。 6. 該当箇所：p.25「バージョン情報」 6. 意見・要望：特定重要電子計算機の届出事項としてバージョン情報の提出を求める場合、届出時点において既知の脆弱性を含むバージョンが利用されている可能性がある。この場合には併せて、当該脆弱性に対するOSSソースコードの修正等何らかの対処や緩和策等により、脆弱性の発現を抑止するための措置を記入すべきと考える。 また、本制度では政府による脆弱性情報の提供を目的としているが、あわせてEOS（End of Support）及びEOL（End of Life）情報の提供についても検討いただきたい。EOS/EOLとなった製品については、脆弱性情報が存在せず安全なのか、又は脆弱性情報が提供されていないだけで実質的にリスクが存在するのかを判断することは困難である。 7. 該当箇所：p.28「変更届出」 7. 意見・要望：「変更届出が必要なのは、届け出た情報（製品名、製造者名等）に変更があった場合のほか、特定重要設備が撤去されない限りにおいては、当該特定重要設備に係る新たな特定重要電子計算機の導入についても変更届出の対象となる」とあるが、例えば、一度、導入し、稼働済の設備のメーカー名の変更を把握することは、海外ベンダーの機器等を想定しても、必ずしも容易ではないため、特別社会基盤事業者の義務・責務とするのは相応しくない。また、「撤去」の時点まで変更届出の管理対象とするのは、特別社会基盤事業者に過度な負担がかかる為、公共のサービス・役務を供することがなくなった時点（例えば、インターネット切断や使用停止）とする検討は出来ないか。 8. 該当箇所：p.30 3-2-4「変更事由が発生した期間」 8. 意見・要望：ある特定の「期日」に変更事由が発生することは想定されるが、変更事由が発生した「期間」とは具体的にどの時点からどの時点を想定した届出が期待されているのかを明確化いただきたい。 9. 該当箇所：p.56、7-1 FAQ(Q5)「日本国外に存在する場合」 9. 意見・要望：侵害された特定電子計算機が日本国外に存在する場合も、特定侵害事象等の報告の対象とされているが、FAQにもあるように、データローカライゼーション規制等により、日本政府の要求事項と、日本国外政府の要求事項の板挟みとなり、民間企業では対応が困難な状況に直面することが予想される。そうしたケースに陥らないよう、日本政府からの他国政府への働きかけを強化することが必須であると考え。また、板挟みにあった場合には、その状況になる前段階であっても、民間企業からの相談を受け付け、日本政府からの当該外国政府・企業への働きかけを通じ、日本政府が主体的に必要な情報を入手する体制の整備が必要と考える。	・1. 及び2. につきまして 頂いた御意見は、今後の参考といたします。 ・3. につきまして 主務省令第1条柱書に記載のとおり、「主務省令で定める電子計算機は、特定重要設備と電気通信回線（公衆の用に供されているものを除く。）で直接又は間接に接続されている電子計算機（令第一条第三項第一号に掲げるものを除く。）であった」と定義されており、一般的にCDN（Contents Delivery Networkと理解）は自社環境（オリジンサーバ等）とインターネット経由で接続されていると承知しており、その場合においては特定重要電子計算機に該当しないものと考えています。 ・4. につきまして 監視サーバについては、御意見の通り、運用管理セグメントに設置されているケースが多いところですが、政令で重要電子計算機は、特定重要設備と電気通信回線で直接又は間接に接続される電子計算機を対象としていることから、誤認は生じないと考えております。 ・5. から7. までにつきまして 頂いた御意見については、今後の運用における参考といたします。 ・8. につきまして 変更届出については、変更の日から4月以内の届出が必要としております。個々の機器において変更が生じる度に変更届を行うことは、事業者に多大な負担が想定されることから、本解説3-2-1に記載のとおり、「例えば、四半期ごとに特定重要電子計算機の棚卸しを行い、1月でその結果をとりまとめて届け出るといったことも可能である。」としているところです。本解説3-2-4「変更事由が発生した期間」とは、この四半期を指しております。 ・9. につきまして 頂いた御意見については、今後の運用における参考といたします。

No.	御意見の要旨	御意見に対する主な考え方
69	解説案の項目（解説案のページ数、項番、項目）毎に分けて、以下のように意見いたします。 なお本提出フォームでは丸文字が使用不可のため、解説案からの抜粋に際し、丸文字の数字を全角数字に変更しております。 【解説案項目】 P.8、2-1-1、「クラウドサービスを使用する場合」 P.17、2-2-3、「３ USB やクラウドサービス等の特定重要設備にデータを入力可能な電子計算機（政令第１条第３項第３号及び主務省令第１条第２項）」 【意見】 SaaS型クラウドサービス上に、特定重要電子計算機の全体がわかるIPアドレス入りネットワーク構成図を保存する場合、類型２ F「ネットワーク構成図を保存する機器」として、クラウドサービス全体、テナント、サイト、ライブラリ等のどの単位を届出対象として整理すべきが明確化いただきたい。 また、単なる設計図書、設備保全資料、一部構成図、IPアドレスを含まない構成図を保存する場合は対象外と理解してよいか、具体例を示していただきたい。 【解説案項目】 P.15、2-2-2、「[B] 特定重要電子計算機に係るシステムの認証を提供する機器（主務省令第１条第１項第６号）」 【意見】 OT環境では、IT系とは別にDCS、EWS、HMI、保守端末等の認証・認可を行う専用のDomain Controller等を設置する場合がある。 このようなOT専用認証基盤が、特定重要電子計算機へのアクセス制御を行う場合、設置場所が制御系DMZの内側又は特定重要設備に近い領域であっても、類型２ B「特定重要電子計算機に係るシステムの認証を提供する機器」に該当するとの理解でよいか、具体例を示して明確化いただきたい。 【解説案項目】 P.15、2-2-2、「[C] 特定重要設備を含むセグメントのDMZ その他当該セグメントにアクセス可能な機器 （主務省令第１条第１項第４号）」 【意見】 IT環境とOT環境の間に設置される制御系DMZ等において、踏み台サーバーのように人がアクセスするための中継機器に加え、FTPサーバー、データ連携サーバー、監視サーバー、ウイルス定義ファイル配信サーバー等、計算機同士で定期的又は自動的に通信を行う機器が存在する場合がある。 解説案では、特定重要設備又は構成設備に対してアクセス制御機器によってのみ中継される通信（参照、更新、コマンド送付、データ送信等）を行う機器として、踏み台サーバー、FTPサーバー、監視サーバー等が例示されているが、類型２ Cの対象は人によるアクセス中継に限定されず、機器間・システム間のデータ連携やファイル配信を行う機器も含まれるとの理解でよいか。 また、対象となる通信の種類、例えば参照、更新、コマンド送付、データ送信、定義ファイル配信、監視データ収集等について、対象・対象外の具体例を示していただきたい。 【解説案項目】 P.15、2-2-2、「[C] 特定重要設備を含むセグメントのDMZ その他当該セグメントにアクセス可能な機器 （主務省令第１条第１項第４号）」 【意見】 類型２ C「特定重要設備を含むセグメントのDMZその他当該セグメントにアクセス可能な機器」について、解説案ではISA/IEC 62443におけるIndustrial DMZ（L3.5）として定義される領域にある機器と捉えてもよい旨が記載されている。 一方、実際のOT環境では、明確なIndustrial DMZ（L3.5）を設けず、Level 3のセグメント内に、Level 4との通信を行い、かつ特定重要設備又は構成設備に対する参照、更新、データ送信等の中継するサーバを配置している場合がある。 このような場合、当該機器がDMZ又はL3.5に明確に配置されていないくても、特定重要設備又は構成設備に対する通信の中継を担い、アクセス制御機器を介してのみ当該通信を行う場合には、類型２ Cに該当するとの理解でよいか。 また、Level 3内の監視サーバー、データ連携サーバー、FTPサーバー等について、対象となる場合と対象外となる場合の具体例を示していただきたい。 【解説案項目】 P.16、2-2-2、「[D] 特定重要設備を含むセグメントへの通信を制御する機器（主務省令第１条第１項第３号）」 【意見】 類型２ D「特定重要設備を含むセグメントへの通信を制御する機器」について、解説案では、通信経路上の全てのアクセス制御機器ではなく、特定重要設備の直近にあるものが対象とされている。 一方、実際のOT環境では、UTM、Firewall、L3SW、ACL付きL3SW等の複数のアクセス制御機器が多段に配置されている場合がある。 このような場合に、類型２ Dの対象となる「直近」の機器は、物理的な配置ではなく、特定重要設備又は一号電子計算機に対する通信について、最終的に許可又は拒否を判断するアクセス制御機器と理解してよいか。 また、UTMの下位にLevel 3セグメントがあり、さらに特定重要設備又は一号電子計算機との間にFirewallが設置されている場合、類型２ Dの対象はUTMではなく当該Firewallとなるのかなど、「直近」の判断基準（論理的距離、通信経路上の最終アクセス制御点等）の明確化とともに、多段構成における具体例を示していただきたい。 【解説案項目】 P.16、2-2-2、「[E] 特定重要設備と同一セグメントの機器（主務省令第１条第１項第１号及び第２号）」 【意見】 類型２ E「特定重要設備と同一セグメントの機器」について、解説案では、類型１ の電子計算機と同一サブネット又は同一VLAN上の機器と捉えてもよいとされ、通信が一方向化され類型１ の電子計算機への通信が行えない場合は該当しないとされている。 一方、実際のOT環境では、特定重要設備又は一号電子計算機と同一サブネット又は同一VLAN上に、HMI、EWS、Historian、保守端末、監視サーバ、バッチ配信サーバ、ウイルス対策管理サーバ、各種ネットワーク機器等が多数存在する場合がある。 このような場合、通信の一方向化やアクセス制御等により類型１ の電子計算機への通信が制限されていない限り、同一サブネット又は同一VLAN上で類型１ の電子計算機へ通信可能な電子計算機は、原則として類型２ E（イ）に該当するとの理解でよいか。 また、同一セグメント上のL2スイッチ、HUB、監視専用機器、読み取り専用機器、バッチ配信サーバ、ウイルス対策定義ファイル配信サーバ等について、対象となる場合と対象外となる場合の具体例を示していただきたい。 【解説案項目】 P.16、2-2-2、「[F] 特定重要電子計算機に関する重要データを保存している機器（主務省令第１条第１項第５号）」 【意見】 類型２ F「特定重要電子計算機に関する重要データを保存している機器」について、対象となるネットワーク構成図及び認証情報の範囲を、事業者が実務上判断できるよう具体例を示していただきたい。 具体的には、ネットワーク構成図について、特定重要電子計算機の総体に係る図であってもIPアドレスが記載されていないものは対象外との理解でよいか。また、IPアドレス一覧、機器一覧、資産台帳、通信先一覧等のリスト形式の資料は、「ネットワーク構成図」に該当しないとの理解でよいか、対象となる場合と対象外となる場合の具体例を示していただきたい。 また、認証情報について、IDのみを記載した一覧、権限一覧、アカウント一覧等は、パスワード、秘密鍵、トークン等を含まない限り、類型２ F（ロ）の認証情報を保存する機器には該当しないとの理解でよいか。 さらに、DCS等の産業制御システムベンダーが納入する完成図書、設計図書、保守資料等の中に、特定重要電子計算機に係るID、パスワード、初期パスワード、保守用アカウント情報等が記載されている場合、当該資料を保存する機器が類型２ F（ロ）に該当するの、資料の形式や保存目的も含めて具体例を示していただきたい。 【解説案項目】 P.16、2-2-2、「[F] 特定重要電子計算機に関する重要データを保存している機器（主務省令第１条第１項第５号）」 【意見】 「総体に係るネットワーク構成図」の範囲及び保存主体の考え方を明確化いただきたい。 ・SharePoint ・CMDB ・Visio ・Excel ・Wiki に大量に保存される場合がある。どこまでが対象となるかが不明である。 【解説案項目】	・2-1-1及び2-2-3につきまして クラウドの届出については、本解説3-1-4 届出事項の(d)特定重要電子計算機の製品名において、「クラウドサービスを使用する場合は、当該クラウドサービスの名称（EC2、RDS など）を記載する。」としており、業務カテゴリレベルでのサービス名称の記載して頂くことと考えております。また、記載の通り、単なる設計図書等は類型２ Fの対象とはなりません。 ・2-2-2[B]につきまして 御理解の通りですが、類型②[B]に該当するかどうかは、システム構成全体を通しての判断が必要です。資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。具体例の記載につきましては、今後の運用も踏まえ、検討いたします。 ・2-2-2[C]につきまして 御理解の通りですが、類型②Cに該当するかどうかは、システム構成全体を通しての判断が必要です。資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。具体例の記載につきましては、今後の運用も踏まえ、検討いたします。 ・2-2-2[D]及び[E]につきまして 御理解の通りです。具体例につきまして、システム構成は事業者によって様々であることから、今後の運用も踏まえて、各特別社会基盤事業者に誤解が生じない記載となるように今後の検討とさせていただきます。資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。 ・2-2-2[F]（一つ目）につきまして 御理解の通りです。具体例につきまして、今後の運用も踏まえて、各特別社会基盤事業者に誤解が生じない記載となるように今後の検討とさせていただきます。資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。 ・2-2-2[F]（二つ目）につきまして 総体に係るネットワーク構成図の範囲及び保存主体によって取り扱いの違いは想定しておりませんが、資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。 ・3-1-1につきまして 主務省令第２条第１項ただし書の広く一般に使用されているものは別途告示で規定しております。ご意見を踏まえ、当該告示の内容を本解説にも記載いたしました。 ・5-1-1（一つ目）につきまして 御指摘の「リアルタイムスキャンにより即時削除された場合」と「感染後にEDRが即時隔離・削除した場合」は概ね同一の事象を指します。インシデント報告の対象は、５、 特定侵害事象及び特定侵害事象の原因となり得る事象です。5-1-1の御指摘の記載は、この事象が特定侵害事象の対象にはならないことを示したものです。御指摘の7-1Q7に記載のとおり、①特定重要設備又は②[E]特定重要設備と同一セグメントの機器については、特定侵害事象の原因となり得る事象の一つに該当し、報告の対象となります。

No.	御意見の要旨	御意見に対する主な考え方
	P.20-21、3-1-1、「届出対象（主務省令第2条第1項）」 【意見】 主務省令第2条第1項但し書きでは、「広く一般に使用されているもの」として指定された製品は届出対象外とされているが、現時点では指定基準及び指定製品リストの公表時期が明確ではない。 汎用品指定の有無は、事業者における届出対象の特定、資産一覧の整備、関係部門・委託先との調整工数に大きく影響する。 ついては、以下の点を明確化いただきたい。 1. 「広く一般に使用されているもの」として指定する際の判断基準 2. 指定製品リストの公表時期、公表方法及び更新頻度 3. 産業制御システム分野で広く使用されているDCS、SCADA、PLC関連製品、OS、ミドルウェア、ファイアウォール、認証基盤等も指定対象となり得るか 4. 指定製品に設定変更、アドオン、個別カスタマイズを行った場合の取扱い 制度施行に向けた準備期間を確保するため、指定基準及び指定製品リストを制度施行前のできる限り早期に公表いただくことを要望する。 【解説案項目】 P.41、5-1-1、「マルウェアの供用（法第2条第4項第1号、第5項）」 【意見】 5-1-1では、マルウェアがリアルタイムスキャンにより即時削除された場合等は該当しないとされる一方、FAQ Q7では、感染後にEDRが即時隔離・削除した場合でも報告対象とされています。 両者の違いは、マルウェアが実際に動作したか、又は実行され得る状態に置かれたかによるものと理解してよいか。 事業者が判断できるよう、実行前検知、実行後検知、感染後隔離、メール添付、Webダウンロード等の具体例を示していただきたい。 【解説案項目】 P.41、5-1-1、「マルウェアの供用（法第2条第4項第1号、第5項）」 【意見】 5-1-1と5-2-1[イ]はともに「マルウェアのダウンロード」や「不正コード実行」に言及しており、事業者にとって両者の境界が必ずしも明確ではない。 特に、マルウェアがダウンロードされたもののEDRやアンチウイルス製品により隔離された場合、メール添付ファイルが保存された場合、WebShellやスクリプトが配置された場合等について、どの時点をもって「実行され得る状態」と判断するのか、より具体的な事例を示していただきたい。 また、5-1-1（特定侵害事象）と5-2-1[イ]（原因となり得る事象）の判定基準を事業者が統一的に適用できるよう、両者の違いが分かる具体例の追加をご検討いただきたい。 【解説案項目】 P.46-48、5-2、「特定侵害事象の原因となり得る事象（法第5条）」 【意見】 「特定侵害事象の原因となり得る事象」の判断基準について、初動調査段階における報告要否を事業者が判断できるよう、具体例を追加いただきたい。 例えば、特定重要設備を直接構成しない拠点、情報系システム、周辺システム又は委託先管理環境において不正アクセス、マルウェア感染、認証情報窃取等の疑いが確認されたものの、初動段階では特定重要電子計算機への侵害、当該機器への通信経路、情報窃取の有無、又は特定重要設備への影響が明確でない場合が考えられる。 このような場合、単なる疑い又は初期アラートの段階ではなく、どの程度の事実確認又は蓋然性をもって、本制度上の「認知」となり、報告が必要となるのかを明確化いただきたい。 特に、類型1 特定重要設備、類型2 E同一セグメントの機器、類型2 A・2 C・2 D等の周辺機器、及び特定重要電子計算機に該当しない周辺システムで侵害の疑いが確認された場合について、報告対象となる場合と対象外となる場合の一般化されたケースを示していただきたい。 【解説案項目】 共通 【意見】 官民連携基盤には、特定重要電子計算機の資産情報、システム構成、バージョン情報、グローバルIPアドレス、インシデント報告内容、IoC、フォレンジック結果等、重要設備への攻撃に悪用され得る機微情報が集約される。 当該基盤又は運用委託先で情報漏えい、不正アクセス、内部不正等が発生した場合、複数の特別社会基盤事業者に重大な影響が及ぶおそれがあるため、政府側で講じる安全管理措置を具体的に明示いただきたい。 具体的には、アクセス権限管理、暗号化、ログ監視、委託先管理、第三者評価、保存期間、削除方法、事故発生時の通知基準・通知期限・通知内容、責任分界を明確化いただくことを要望する。（経営の視点からの要望である）	・5-1-1（二つ目）につきまして 本解説5-1-1と5-2-1[イ]との違いは、5-2-1[イ]や7-1 Q7にあるとおり、後者はマルウェアの即時隔離・削除が行われた場合等も含む点です。 ・5-2につきまして 御指摘の特定侵害事象等の発生の認知については、本解説5-5において、「監視におけるイベントやアラートの発報のみをもって直ちに該当するものではないが、当該イベントやアラートの内容等を踏まえ、法第5条における特定侵害事象等に該当すると合理的に判断できる状態を指す。（略）なお、サイバーインシデントの発生の主な認知方法の例としては、以下が挙げられる。」として類例を示しております。また、特定重要電子計算機に該当しない計算機への侵害は、本解説5-4に記載のとおり報告義務の対象外ですが、任意でご報告頂くことを妨げるものでございません。 ・「共通」につきまして 本解説は、法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説をするものであり、御指摘の安全管理の記載は馴染まないものと考えておりますが、法第8条の規定も踏まえ、安全管理措置を徹底してまいります。
	1. P12 図2 意見内容 ・特定重要電子計算機の供給者がリモート保守を行うために設置したVPN装置は、特定重要電子計算機に該当するのか（報告対象か）。 理由 ・届出対象・報告対象を明確にしたいため。 ----- 2. P14～15 第1条第1項第7号の説明 意見内容 第7号の推奨事項の解説として、 なお、以下の機器は特定重要電子計算機に含まれないが、法目的に照らすと、アタックサーフェスに類する機器として任意で届出を行うことが望ましい。 5. （中略） 6. 1.、2.、及び5.に関する電気通信のうち、異常な電気通信を制限する機器（IPS等） ※なお、電気通信の監視のみ行う機器（IDS等）は本定義に該当しないものとするが、電気通信を制限する機能及び電気通信を監視する機能の双方を保有する場合は、活用している機能に関わらず本定義に該当するものとする。 とあるが、「電気通信の監視のみ行う機器（IDS等）は本定義に該当しないもの」における「本定義」とは、第1条第1項第7号を指す理解で正しいか。 すなわち、	

No.	御意見の要旨	御意見に対する主な考え方
70	(1) 監視機能のみのIDSは届出不要 (2) 監視機能と通信制限機能の双方を有するIDSは届出が推奨（望ましい） という理解でよいか。 もし「本定義」が第1条第1項第7号を指すのであれば、(2)は該当機器となるため、「推奨」ではなく「必須」と読めることから、誤解を防ぐために「本定義」が何を指すのか明確化いただきたい。 ----- 3. P20 3-1-1 届出対象 意見内容 アプライアンスの具体的な事例を示していただきたい。 理由 現状の説明では何が届出対象かが不明。 ----- 4. P21 3-1-1 広く一般に使用されている製品である場合 意見内容 Windows及びWindows Serverを届出対象外とした場合、当該OSに係る重大脆弱性又はゼロデイ脆弱性が確認された際に、政府は特別社会基盤事業者が保有する特定重要設備への影響をどのように把握し、協会の仕組みを通じて情報提供を行うことを想定しているのか。 理由 下記によると、マイクロソフト コーポレーションのWindows及びWindows Serverは対象外であるため。 https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000318051 ----- 5. P21 3-1-2 届出期限 意見内容 「届出期限は、原則特定重要電子計算機を導入した日から4か月以内である。」とあるが、「導入」の解釈は、経済安全保障推進法の「基幹インフラ役務の安定的な提供の確保に関する制度」に基づき、各分野のガイドラインで定義されている「導入」と同じ理解でよいのか。 理由 導入の定義は、経済安全保障推進法に基づく届出において、分野ごとに定義（タイミング）が異なるため。 ----- 6. P25 表中「バージョン情報」欄（情報の内容） 意見内容 資産のバージョン情報（OS、ファームウェア、ソフトウェアのバージョン等）とある。一方、P20ではファームウェアは届出対象外となっている。 これはどのように解釈すればよいか。 届出義務がない資産に対するバージョン情報が推奨事項となっているように読めるが、届出義務がないものについても資産として届出することを推奨しているという理解で正しいか。 ----- 7. P25 表中「バージョン情報」欄（情報の内容） 意見内容 バージョン情報としてどこまでの詳細度を期待しているのか例示いただきたい。 例えばCPE 2.3ではVersionの下位階層（5層目～11層目）が定義されており、脆弱性を特定するにはVersion情報のみでは不足する場合が多い。 脆弱性情報をどのレベルで抽出して連絡することを想定しているのか、望ましい記載レベルを示していただきたい。 理由 脆弱性情報の通知精度や事業者側での管理レベルを明確にするため。 ----- 8. P27 3-2 変更届出 （関連：P40 4-5-1 ステップ5-1 システム概略図の届出） 意見内容 4-5-1で提出する概略図について、構成変更に伴い概略図の記載内容が変更された場合は、変更届出の対象ではないという理解でよいか。 OS更新、機器更改、ネットワーク構成変更等について、どの範囲を変更届出の対象として想定しているのか。	・1. につきまして 記載の事例については、特定重要電子計算機の対象となり得ますが、システム構成全体を通しての判断が必要と考えますので、資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。 ・2. につきまして グローバルIPアドレスが割り当てられてないという前提になりますが、電気通信の制限機能を有する機器（IPS等）は任意届出を推奨しており、電気通信の監視機能を有する機器（IDS等）は任意届出の対象ではありません。 ・3. につきまして 例えば、ネットワークサービスを提供する機器等を指しております。また、アプライアンスの考え方は、本解説3-1-1 届出対象（主務省令第2条第1項）にお示しております。 ・4. につきまして 資産届出いただく趣旨は、政府が特別社会基盤事業者の特定重要電子計算機の資産状況について把握しておくことにより、内閣総理大臣が特別社会基盤事業者に対し適切な情報共有を行うなど、特定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必要な対応を行うためです。 例えば、政府において、特定重要電子計算機の脆弱性情報を把握した場合、その脆弱性情報と同項に基づき届け出られた特定重要電子計算機の情報を照合させることにより、脆弱性のある特定重要電子計算機を使用する特別社会基盤事業者に対し、脆弱性情報を提供することが可能となります。 他方、業界、事業者問わず、広く一般に使用されている電子計算機については、資産状況を把握せずとも、全ての特別社会基盤事業者に脆弱性情報を提供することで、特別社会基盤事業者は必要な措置を講じることが可能です。そのため、告示では、特別社会基盤事業者の負担の軽減の観点から、資産届出を不要とする電子計算機を指定することとしております。 以上の趣旨を踏まえ、告示では、業界、事業者問わず広く使われており、かつ、特に主務省令第1条第1項第6号及び第2項第1号に規定する電子計算機において使われていることが想定されるなど、特別社会基盤事業者の負担軽減の効果が高いマイクロソフト・コーポレーションのWindows及びWindows Serverを指定することといたしました。 ・5. につきまして ある電子計算機を特定重要電子計算機として使用を開始した日となります。 ・6. につきまして 御理解の通りです。ファームウェアは任意で届け出ることが望ましい事項としております。 ・7. につきまして 様々な製品が存在するため、バージョン情報の記載粒度を一律に規定することは困難です。資産届出にあたり疑義がありましたら、特別社会基盤事業者に案内しております相談窓口までお問合せください。 ・8. につきまして ネットワーク概略図等の各特定重要電子計算機と他の特定重要電子計算機又は特定重要設備との関係を示す資料につきましても、御指摘の本解説3-2の「届け出た情報」に該当するため、変更があった場合は、変更届出が必要です。当該資料については、OS更新、機器更改、ネットワーク構成変更等により各特定重要電子計算機と他の特定重要電子計算機又は特定重要設備との関係に変更があった場合は変更届出が必要です。 ・9. につきまして 御理解の通りとなります。公衆の用に供されている電気通信回線を経由しないことを示しております。図については補足を記載いたしました。 ・10. につきまして 本解説は法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説するものであり、各特別社会基盤事業者

No.	御意見の要旨	御意見に対する主な考え方
	理由 P28の文言から、上記は変更届出の対象外と理解しているため。 「変更届出が必要なのは、届け出た情報（製品名、製造者名等）に変更があった場合のほか、特定重要設備が撤去されない限りにおいては、当該特定重要設備に係る新たな特定重要電子計算機の導入についても変更届出の対象となる。」 ----- 9. P36～P39 図6～図11 意見内容 図6～図11において、クラウドがインターネットを経由せずに社内ITシステムとルータを介して接続しているように見える。 これは閉域網又は専用回線で接続されていることを示しているとの理解でよいか。 また、これらの図はインターネットVPNを想定していないとの誤解を受ける可能性があるため、クラウドとルータ間の接続について図中に補足説明を付してはいかか。 ----- 10. P41 5. 特定侵害事象等の範囲 （関連：P46 5-2 特定侵害事象の原因となりうる事象） 意見内容 特定侵害事象の原因となり得る事象を認知するために、特別社会基盤事業者に対してどの程度の監視体制を想定しているのか。 例えば、特定重要設備への影響を把握するためにSOCのような継続監視を前提としているのか、あるいはインシデント発生時の調査で偶然発見したものでもよいのか。 理由 報告のタイミングを正確に把握したいため。 ----- 11. P48 5-2-2 特定重要設備以外における特定侵害事象の原因となり得る事象 意見内容 「蓋然性が高い」とは、5-1の特定侵害事象が発生したと判断できる直接的なエビデンスはないものの、例示されている間接的なエビデンスから発生したと判断した状態との理解でよいか。 否の場合は、蓋然性の高さを判断する基準又は具体的な事例を示していただきたい。 理由 報告のタイミングを正確に把握したいため。 ----- 12. P53 6-1 報告対象 意見内容 法律第5条及び主務省令第4条第2項で求められる報告対象と、法律第45条に基づく協議会構成員に求められる報告対象事象は異なるという理解でよいか。 理由 報告内容の違いを明確にしたいため。 ----- 13. P56 7-1 FAQ 意見内容 (1) 「特定重要電子計算機に該当する電子計算機であれば、届出を行ってなくても報告対象となる」と記載があるが、特定重要電子計算機であるが届出対象外の電子計算機については、事業者が特定重要電子計算機に該当すると判断した一覧等を保管しておけばよいという理解でよいか。 (2) 設備の供給者はどのようにしてその事実を知ることができるのか（電子計算機等供給者も協議会の構成員となる場合があるとの理解）。 (3) 届出対象の電子計算機と届出対象外の電子計算機で、特定侵害事象の報告に係る様式や手続きに違いはないという理解でよいか。	の監視体制について規定するものではありませんので回答は控えさせていただきます。なお、認知については、本解説5-5で記載の通り特別社会基盤事業者が知り得る状況となった時となります。 ・ 11. につきまして 御理解の通りとなります。 ・ 12. につきまして 法第45条第5項は、協議会の要請に基づき報告をするものであり、報告内容等についても協議会において決められるものとなります。 ・ 13. につきまして (1)につきましては、特別社会基盤事業者において適切に法第 5 条の報告を行っていただければ、御指摘の一覧等の保管を義務づけるものではありません。(2)につきましては、法第42条第 1 項等に基づき、内閣総理大臣等が電子計算機等供給者に対し、情報提供等を行う場合があります。また、特別社会基盤事業者と電子計算機等供給者との間で必要に応じ情報共有いただくことも妨げません。(3)御理解のとおりです。

No.	御意見の要旨	御意見に対する主な考え方
71	特定重要設備を含む特定重要電子計算機について、弊社を含む特別社会基盤事業者が当該電子計算機を所有しておらず、かつ監視・運用を第三者に委託している形態が想定されます。これを踏まえ、弊社から以下の3点について意見、要望いたします。 (1)所有・運用形態を踏まえた直接報告(所有者又は委託先からの報告)の必要性について このような形態において、資産届出および特定侵害事象等の報告で要求されている情報を、特別社会基盤事業者自身が保有・取り扱うこと自体が、セキュリティ上のリスクとなり得ると考えます。例えば、アタックサーフェスに関する情報が流出した場合、攻撃者による事前偵察の精度が向上し、特定妨害行為の成立可能性が高まることが想定されます。この影響は、情報の流出元となった特別社会基盤事業者にとどまらず、当該特定重要電子計算機を利用するすべての特別社会基盤事業者に波及する可能性があります。このため、特定重要電子計算機の所有者又は監視・運用の委託先から、主務大臣等に対して直接報告を行うことを可能とする制度設計を要望いたします。 (2)契約実務を踏まえた雛形文書の公開について 前述の通り、報告主体を特別社会基盤事業者とするか、特定重要電子計算機の所有者又は委託先とするかに関わらず、本命令案への対応にあたっては、所有者又は委託先に対し協力を求める必要が生じると想定されます。その結果、既存契約の変更や、新たな覚書等の締結が必要となるケースが多く発生することが見込まれます。 この点について、経済安全保障推進法の基幹インフラ制度において雛形文書が公開されていることと同様に、本命令案への対応に資する雛形文書(契約変更例、覚書例等)のご提供いただけることを要望いたします。 (3)クレジットカード業態(サービス利用型設備)を踏まえた制度整理について 弊社を含む多くのクレジットカード事業者において、共同利用され、かつ同様の形態で提供されている設備が存在すると考えられます。 具体的には、「経済産業省関係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に基づく特定社会基盤事業者等に関する省令」(令和5年経済産業省令第41号)第1条第11号において特定重要設備として定義されている、取引認証設備(同号ロ)及び代行信用照会等設備(同号ハ)について、他事業者が当該設備を所有し、特別社会基盤事業者はサービス利用契約に基づき利用する形態が一般的です。 この場合、経済安全保障推進法の基幹インフラ制度における特定重要設備の導入・重要維持管理等委託に加え、本法に基づく資産届出および特定侵害事象等の報告制度において、委託契約を前提とした対応をサービス利用者の立場から一方的に求めることは、契約上・実務上ともに困難なケースが想定されます。また、対応義務を強く求めた場合、相手方がサービス提供を継続できなくなる可能性が生じ、基幹インフラ役務の提供そのものに支障をきたすおそれ否定できません。 以上を踏まえ、クレジットカード事業の業態を考慮し、サービス利用型の特定重要電子計算機については、委託契約の存在を前提としない、資産届出および特定侵害事象等の報告制度の考え方を示していただけることを要望いたします。	頂いた御意見につきましては、クレジットカード業界の実態を踏まえ、今後の検討とさせていただきます。
72	該当箇所 P21 広く一般的に使用されている製品である場合（主務省令第2条第1項但し書き） 意見 別途定める汎用品については、実際の届出状況に照らし、実態に応じた範囲になるよう柔軟に見直す運用とすることを要望いたします。 該当箇所 P27 経済安全保障法に基づく導入等届出を行っている場合の取扱い（主務省令第2条第4項） 意見 「経済安全保障推進法第52条第1項又は第11項の規定による当該特定重要設備の導入の届出を行っている場合には、以下の書類をもって、特定重要電子計算機のうち、特定重要設備又は構成設備であるものの届出書に代えることができる。」という点について、経済安全保障推進法に基づく導入等の届出について既に審査が完了したものは、事業者による重複した届出手続を避ける観点や届出の抜け漏れを避ける観点から、当該届出に係る情報を本制度における特定重要電子計算機の届出情報として自動的に登録・連携し、事業者が改めて届出書類を提出する必要がない仕組みとしていただくことを要望いたします。 上記のような自動的な情報連携が困難な場合には、経済安全保障推進法に基づく導入等の届出を行い、導入する設備が確定しているものについては、実際の設備の導入前であっても、本制度における特定重要電子計算機の届出を行うことを可能とする運用が望ましいと考えます。 該当箇所 P27 変更届出（法第4条第3項、主務省令第3条） 意見 変更届出について、例えば製造者の社名変更があった場合、当該製造者に係る届出済みの設備を個別に列挙して変更内容を全て記載する方式ではなく、製造者の社名変更についてのみ届け出ることが可能な方式としていただくことを要望いたします。 例えば、X社からY社への社名変更があった場合、「A設備：X社→Y社」「B設備：X社→Y社」「C設備：X社→Y社」のように対象設備ごとに変更内容を記載するのではなく、「X社→Y社」と社名変更の事実を一度記載することで、当該製造者に係る届出済みの全設備について変更届出を行ったものとして取り扱うなど、事業者の事務負担を軽減する運用としていただきたいと考えます。 該当箇所 P56 共同利用している特定重要電子計算機が侵害された場合も報告の対象となるか。 意見 「複数の特別社会基盤事業者が共同で利用している特定重要電子計算機が侵害された場合、当該複数の特別社会基盤事業者が特定侵害事象等の報告をする必要がある。」との記載について、ネットワークの共同構築等で、他の事業者が所有・管理する電子計算機を利用又は経由している場合であっても、当該電子計算機やその周辺機器に関する情報を、利用する事業者が必ずしも把握できるとは限りません。 特に、サービス上の競合関係にある他の事業者が所有・管理する電子計算機については、機器構成等に関する情報が経営上の機微情報に該当し得ることから、情報開示を依頼した場合であっても、必要な情報の共有を受けることが困難なケースが多く想定されます。 加えて、双方の自社設備として届出済みの情報を共有先事業者からも重複して届出等を行うこととなるため、このような共同利用に係る機器については共有先事業者からの届出及びインシデント報告を対象外としていただくことが必要といたします。仮に双方の事業者を届出等の対象とする場合であっても、共有先事業者が利用している機器については、当該機器を所有・管理する特別社会基盤事業者が届出又はインシデント報告を行う際に、備考欄等に他の事業者も当該機器を利用している旨を記載することをもって共有先事業者からの届出又はインシデント報告とみなすなど、政府としても実質的に影響確認が可能であることから、実態に即した制度設計に配慮いただくことを要望いたします。 該当箇所 P58 個人データ漏えい等に伴う個人情報保護法に基づく報告及び番号法に基づく報告 意見 「個人情報の保護に関する法律（平成15年法律第57号）第26条第1項の規定による個人データの漏えい等に係る報告等は、被害組織が(1)DDoS攻撃事案に該当する事象については別添様式1、(2)ランサムウェア事案に該当する事象については別添様式2、(1)(2)の事象以外の事象については別添様式3を用い、又は別途法令等で定める様式に添付する形で報告等を行うことを可能とする。」とされていますが、報告の形態については、既存の運用もあることから、一度の報告で本法律に関するインシデント報告と個人情報の漏洩に関する報告を同時に実施する形態（権限の委任を受けた事業所管省庁宛を含む）と、従来通りの報告形態の両方を許容していただくことを要望いたします。	・「広く一般に使用されている製品である場合」につきまして 御指摘の汎用品につきましては、告示でお示ししており、本解説3-1-1に本告示の内容を記載いたしました。また、告示につきましては、今後の電子計算機の使用状況等を踏まえ、必要に応じ、見直してまいります。 ・「経済安全保障法に基づく導入等届出を行っている場合の取扱い」につきまして 経済安全保障推進法第52条第1項又は第11項の規定による当該特定重要設備の導入の届出を行っている場合には、資産届出と重複した手続きとならないように官民連携基盤での連携などの制度設計を行っているところですが、御意見につきましては、今後の参考とさせていただきます。 ・「変更届出」につきまして 御意見につきましては、今後の参考とさせていただきます。 ・「共同利用している特定重要電子計算機が侵害された場合も報告の対象となるか。」につきまして インシデント報告の主体は、特別社会基盤事業者であるため、代表報告は認められません。また、連名報告は、各特別社会基盤事業者において適切に届出対象となる電子計算機を把握し、管理いただく観点から、業種や事業者を問わず一律に認める考えはございませんが、御指摘も踏まえ、運用上支障がないことが確認できた業種・事業者については、個別に検討してまいりたいと考えております。 ・「個人データ漏えい等に伴う個人情報保護法に基づく報告及び番号法に基づく報告」につきまして 官民連携基盤を利用した報告については、本法に基づくインシデント報告と個人情報の漏洩に関する報告を同時に行う形態や従来の運用に基づいた報告など、報告ルートを利用者側で設定可能です。

No.	御意見の要旨	御意見に対する主な考え方
73	p.55 6-4 報告事項で報告事項として記載されている「IoC（侵害の痕跡）」は、以下の様式の記載と合わせて「「インディケーター情報」とした方が用語が統一され分かり易いと思います。 ・関係省庁申合せ別添様式 2 、 4、 事案に関する技術的な事項（攻撃技術情報）：（ 5 ）ランサムウェアの特徴（インディケータ情報） ・関係省庁申合せ別添様式 3 、 4、 事案に関する技術的な事項（攻撃技術情報）：（ 3 ）サイバー攻撃等の特徴（インディケータ情報）	様式に合わせ「インディケーター情報（侵害の痕跡）」に修正いたしました。
74	本件関連の制度案等の公表および意見募集にあたり、現在日本社会を深刻に蝕む経済格差の拡大というすべての元凶、およびセキュリティ対策やサイバー攻撃への対応を名目として、次々と新たな管理枠組みや形式的な報告義務・コストの負担が現場や事業者に押し付けられている現状に対する重大な懸念から、以下の通り強く意見を述べさせていただきます。 第一に、重要インフラやシステムに対するサイバー攻撃の防止や被害報告という大義名目の下で、実態の伴わない形骸化した管理基準や複雑な様式・報告の義務化を際限なく重ねていくアプローチは、まさに終わりのない「いたちごっこ」の行政運用の極みであるという点への強い批判です。物価高や生活苦に喘ぎ、日々の生活を守るだけで精一杯である一般の社会経済活動に対し、実効性の乏しい監視・管理の網や過剰なシステム対応コストを強いる構造は、現場の萎縮を招くだけでなく、格差に苦しむ社会の構造的矛盾をさらに悪化させるものです。 第二に、行政や関係省庁が真に注力すべきは、形骸化したルールの微修正や、監視・管理の肥大化による安全保障の美名の下での負担増大ではありません。最優先されるべきは、格差の拡大によって日々疲弊している勤労者や生活者の生活防衛であり、過度な経済的負担や不条理なシステム運用に縛られない、公平で透明性の高い社会経済基盤の構築です。金儲けや管理偏重の社会構造を改め、国民生活全体の公平性と納得感を担保する政策運営へと直ちに舵を切ることを強く求めます。	本制度の制度設計や運用にあたっては、例えば、特別社会基盤事業者が行う類似の報告について官民連携基盤の整備により報告の窓口を一元化するとともに、共通様式による報告の受理を可能とするなど、特別社会基盤事業者の負担にもよく留意しつつ、重要電子計算機の被害の防止のために必要かつ合理的な制度となるよう進めており、御指摘のような際限のない対応を求めるものではございません。
75	【該当箇所】 1-1「目的」 6-4「報告事項」 7-1「FAQ」 8-2「参考となる他ガイドライン」等 【意見】 本解説において、サイバーセキュリティ対策を「侵入を防ぐ」「異常を検知する」「報告する」「復旧する」という観点だけでなく、万一侵入や情報窃取が発生した場合にも、取得された重要データそのものを復元・悪用されにくい状態にしておく「侵害後の被害最小化」の観点を、より明確に位置付けることを要望します。 特に特別社会基盤事業者が扱う情報について、暗号化、秘密分散、データ無意味化、分散保管等により、一部のデータが外部へ取得された場合でも、そのデータ単体では内容を復元・利用しにくい状態にする技術的対策を、安全管理措置又は参考となる実装例の一つとして解説することを検討していただきたいです。 また、特定侵害事象等の報告においても、「情報が流出したか」だけでなく、次のような事項を確認できることが重要だと考えます。 1. 外部に取得された情報が、そのまま内容を読み取れる状態であったか。 2. 暗号化、秘密分散、データ無意味化等の技術的保護が適用されていたか。 3. 取得されたデータ単体で、重要情報、個人情報、認証情報等を復元・悪用できる状態であったか。 4. 暗号化されていた場合、復号鍵や認証情報等も侵害された可能性があるか。 5. 秘密分散等が行われていた場合、他のデータ片や復元に必要な情報まで侵害されているか。 6. 技術的保護措置が、職員や委託先担当者による個別の判断・操作を必要とする仕組みであったか、それとも通常の保存操作等によってシステム側で自動的に適用される仕組みであったか。 【理由】 本解説案では、クラウドサービスを利用する場合や、他組織が所有する電子計算機、国外に存在する電子計算機等についても対象となり得ることが示されています。 また、SaaS等のクラウドサービスでは、データやユーザーアカウント等について利用者側が責任を負う領域もあるとされています。 重要インフラのデジタル化やクラウド利用が進むほど、サイバー攻撃を完全に防止することだけでなく、「侵入された場合に何が起るか」をあらかじめ考えたデータ保護設計が重要になると考えます。 例えば、攻撃者がシステムへ侵入しデータを外部へ取得した場合でも、そのデータが平文でそのまま利用可能な場合と、取得されたデータ片単体では意味を持たず、他のデータ片等がなければ復元できない場合とでは、社会的な被害の大きさが大きく異なります。 したがって、特定侵害事象等の重大性を把握する際には、攻撃経路や脆弱性だけでなく、「取得された情報が実際に利用可能な状態だったのか」を確認することが重要だと考えます。 また、暗号化機能やセキュリティルールが存在していても、職員や委託先担当者が、その都度、 ・どの情報を暗号化するか ・どの場所に保存するか ・どのように共有するか ・暗号鍵をどのように管理するか を判断・操作しなければ保護されない仕組みでは、操作漏れ、設定漏れ、誤保存、緊急時の例外的な取扱い等が発生する可能性があります。 重要インフラでは、サイバー攻撃、災害、障害等の緊急時には、通常とは異なる作業や情報共有が発生する可能性もあります。 そのため、人が常に正しく判断し、ルールを完全に守ることだけに依存するのではなく、所定の保存領域に通常どおり保存することで、システム側が自動的にデータを保護する「人任せにしない安全管理措置」も重要だと考えます。 例えば、秘密分散やデータ無意味化等を用いて、通常の業務操作の中で自動的にデータを分散し、一部が外部へ取得されても単体では復元・悪用されにくい状態にする仕組みは、そのための技術的選択肢の一つになり得ると考えます。 これは、暗号化、認証、多要素認証、アクセス制御、EDR、ログ監視、ネットワーク分離、バックアップ等の既存対策を不要とするものではありません。 これらの従来対策に加えて、 「侵入される可能性がある」 「人はミスをする可能性がある」 「委託先やクラウドから情報が流出する可能性がある」 ことを前提とし、万一情報が取得された場合にも被害を最小限にする多層的なデータ保護を求めるものです。 本解説案の用語説明でも、サイバーセキュリティについて、情報の漏えい、滅失又は毀損の防止その他の情報の安全管理に必要な措置を講じ、その状態を適切に維持管理することが含まれています。 この考え方をさらに具体化し、 「重要情報が外部へ取得された場合に、そのデータ単体で復元・悪用可能であるかを確認する」 「侵害を完全には防げない場合に備え、データそのものを利用困難な状態にする技術的対策も検討する」 という観点を、本解説の安全管理及び報告に関する説明に加えていただくことを要望します。 また、参考となるガイドラインや実装例を示す際には、暗号化だけでなく、秘密分散、データ無意味化、分散保管等の技術カテゴリについても、侵害時の被害最小化という観点から紹介することを検討していただきたいです。 特定の企業や製品の採用を求めるものではありません。 秘密分散、データ無意味化、分散保管、システムによる自動的な保護といった技術カテゴリを、「侵入防止」「検知」「復旧」と組み合わせる多層的なサイバーセキュリティ対策の選択肢として検討していただきたいという趣旨です。 以上	本解説は、本解説1-1に記載のとおり、法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説をするものであり、御指摘の事項を本解説に記載する考えはありませんが、頂いたご意見につきましては、今後の施策の参考とさせていただきます。

No.	御意見の要旨	御意見に対する主な考え方
	■意見① 【Page】 16 【Chapter】 2-2-2 ②特定重要設備と接続されている電子計算機（政令第 1 条第 3 項第 2 号及び主務省令第 1 条第 1 項） 【F】 特定重要電子計算機に関する重要データを保存している機器（主務省令第 1 条第 1 項第 5 号） 【該当箇所】 (イ)ネットワーク構成図を保存する機器 ここでいうネットワーク構成図は、(i)特定重要電子計算機（(イ)ネットワーク構成図を保存する機器を除く。）の総体にかかるもののうち(ii) IPアドレス（ここでは、いわゆるグローバルIPアドレスのほか、ローカルIPアドレスも含む。）が記載されているものであって(iii)一時的に保存されるもの以外のものに限られる。 【意見内容】 本文書においては、「②特定重要設備と接続されている電子計算機」の条件に適合しないため届出対象外として整理されている一方で、重要データとして例示される「ネットワーク構成図」は、実態としてシステムインテグレーション（SI）委託先企業がシステム設計・保守のために保有しているケースが多い。 データの重要性を鑑み、SI委託先企業がネットワーク構成図（重要データ）を保管する場合においても、そのデータ保存機器を特定重要電子計算機として指定すべき。 国家を背景とする攻撃者は、サプライチェーン攻撃として、最終攻撃目標（政府・基幹インフラ事業者など）を直接攻撃せず、そのサプライヤーを踏み台とすることで最終攻撃目標に対する攻撃を達成することが広く知られている。これまで我が国においても中央省庁の重要データを狙ったサプライチェーン攻撃は複数観測されている。 このため、SI委託先企業でネットワーク構成図（重要データ）を保管する場合においても、基幹インフラ事業者と同様に特定重要電子計算機の指定をし、本法において防護措置を図っていくことが求められる。 ■意見② 【Page】 20 【Chapter】 3-1-1 届出対象（主務省令第 2 条第 1 項） アプライアンス以外の電子計算機の場合 【該当箇所】 アプライアンス以外の電子計算機については、当該電子計算機に組み込まれたオペレーティングシステム、ミドルウェア及びアプリケーションが届出の対象となり、ハードウェアは届出の対象外である。なお、ファームウェアは届出の対象外である。 【意見内容】 ①BIOSを含むファームウェアは対象外とされているが、ファームウェアについては資産届出項目として検討すべき。 ファームウェアの脆弱性は、永続性確保の手段として攻撃者から高度な攻撃に悪用される事例が数多く報告されている。またこの攻撃の多くはセキュリティソフトによる検知が困難であり、本法により第一に対策を講ずべき対象である。 ②ハードウェアが届出の対象外とされているが、高度なサイバー攻撃手法として、ハードウェア特性の脆弱性を突いた攻撃（物理的タンバリング・サイドチャネル攻撃）が知られており、資産届出対象として挙げることを検討すべき。 ■意見③ 【Page】 24 【Chapter】 3-1-4 届出事項（主務省令第 2 条第 5 項） 表 3 任意で届け出ることが望ましい事項 【該当箇所】 （項目名のみ列挙） ・届出対象分類 ・（添付資料上の）システム名又は領域名 ・（添付資料上の）機器名 ・アプライアンス製品の概数 ・バージョン情報 76・グローバルIPアドレス ・資産設置環境の管理主体 ・管理主体と届出者の関係性 【意見内容】 ①①政府側において事業者へ効果的に脆弱性情報を展開する観点から、任意届出とされている以下項目は届出を必須とすべき。 ・アプライアンス製品の概数 ・バージョン情報 ・グローバルIPアドレス ・資産設置環境の管理主体 ・管理主体と届出者との関係性	・意見①につきまして 御指摘の通り、2-2-2[F]につきましては、特定重要設備と接続されている電子計算機を対象にしております。特定重要設備と接続がない委託先等への重要データの保存については、本法の対象外となっているところであり、御意見につきましては、今後の施策の参考とさせていただきます。 ・意見②につきまして アプライアンス以外の電子計算機について、ハードウェアの情報については、利用者が把握できない又は把握するための負担が大きい場合が多く、制度の実効性を確保することが困難と考えられるため、ファームウェアは対象外としていたところ です。御意見につきましては、今後の施策の参考とさせていただきます。 ・意見③につきまして 利用者が情報を把握及び届出にあたっての負担が大きい場合が多く、制度の実効性を確保することが困難と考えられるため、任意届出としているところです。御意見につきましては、今後の施策の参考とさせていただきます。 ・意見④につきまして 官民連携基盤を使用する届出については、別途、登録用に整理したCSVファイルの提供を予定しているところで、情報の管理が行いやすいように検討を進めております。 ・意見⑤につきまして 御意見につきましては、今後の施策の参考とさせていただきます。

No.	御意見の要旨	御意見に対する主な考え方
	②届出項目の入力・運用方式を見直すべき。 当届出項目は多岐に渡る一方で、すべての内容を「備考欄」に記載することを求めている。このことで、事業者における届出状況の維持管理に大きな支障をきたすことや、迅速に策を講ずべき大規模攻撃キャンペーンの発生時、政府において事業者資産状況の把握が困難となることが推測される。 例えば「バージョン情報」は、事業者では運用において高頻度の更新が予測されるが、他の任意届出項目とともに備考欄記載を更新していくことは現実的な運用ではない。また政府においてもバージョン情報はバッチ適用状況把握と対処指示に大いに役立つ一方で、備考欄記載のため、一刻を争う状況下において迅速な状況把握・事業者への指示は容易ではない。 このため、官民連携基盤システム上で、届出事務作業・届出済みの内容把握が容易になるよう、政府・事業者、両者の目線で抜本的に運用プロセスを見直すべき。 ■意見④ 【Page】 30 【Chapter】 3-2-4 記載例（主務省令様式第2） 【該当箇所】 — 【意見内容】 例示される届出書フォーマットは、大量の入力項目を直観的に取扱いにくいユーザーインターフェイスとなっている。 このため、大規模な資産届出を行う事業者にとっては、運用の過程において、過去にどのような届出を行ったかを容易に把握・維持することが困難となるケースが生じうると考えられる。 官民連携基盤システムでは、官民連携基盤システム上で、事業者において届出事務作業・届出済みの内容把握が容易になるよう、政府・事業者の利用者目線で運用プロセス・入力インターフェイスを検討すべき。 ■意見⑤ 【Page】 51 【Chapter】 5-5 特定侵害事象等の発生の認知 【該当箇所】 C) フォレンジック調査、脅威ハンティング等の活動により、サイバー攻撃を受けていた痕跡が確認され、その痕跡から想定される発生事象が特定侵害事象等と判定された。 【意見内容】 基幹インフラ事業者において、脅威ハンティングなどの高度なサイバー攻撃痕跡を検知する活動が定期的かつ能動的に行われるよう、対応を義務化すべき。 一般的にフォレンジック調査、脅威ハンティングを行なうトリガーは、何らかのインシデント発生時、何らかのインシデント兆候を検知した時に限られ、事業者による特定侵害事象の発生の認知は「受動的」にしか行われていないのが実情である。 そのような状況において、「特定侵害事象の発生の認知」を事業者による受動的活動に委ねていると、本法の目的としていた国家を背景とする高度な潜伏型攻撃について、能動的に検知・対処することはできず、事業者による定期的な脅威ハンティング活動を義務化することが求められる。 なお政府においては、7/31に開催されたサイバーセキュリティ戦略本部（第6回）にて決定した「脅威ハンティングの普及促進・実施等に係る基本方針」に則り、事業者に対して脅威ハンティング活動を強力に支援していくことが期待される。	

No.	御意見の要旨	御意見に対する主な考え方
	意見： Business Software Alliance(ビジネス・ソフトウェア・ライアンス、以下BSA)（１）は、政府が特別社会基盤事業者のサイバー防御・対処能力の強化に向けて取り組みを継続していることを高く評価するとともに、「サイバー対処能力強化法」に基づく届出および報告義務をより明確にするために本解説案が公表されたことを歓迎します。 BSAは、エンタープライズソフトウェア産業を代表するグローバルな業界団体であり、サイバーセキュリティ、人工知能（AI）、クラウドストレージサービス、量子技術、その他の先進的技術をリードする企業を代表しています。BSAの会員企業は最先端のセキュリティツールを提供し、政府や産業界全体で採用されているソフトウェアセキュリティのベストプラクティスの多くを開拓してきました。BSAは会員企業と共に、世界各国の政府と緊密に連携しながら、サイバーセキュリティ政策の策定に取り組んでいます。こうしたグローバルな経験に基づき、以下のとおり、意見を提出します。 [提言] 制度の実効的な運用を支援する観点から、BSAは、特別社会基盤事業者とテクノロジー提供事業者との間の責任分担について、さらなる明確化を行うとともに、侵害事象報告要件についても、リスクベースで、リスクに見合った比例的かつ国際的なベストプラクティスと整合した制度となるよう、追加的な見直し・改善を求めます。 <法定の届出・報告義務を負う主体が特別社会基盤事業者であると明確化すること> 本解説案においては、クラウドサービスが特定重要計算機に含まれることも踏まえ、特定重要計算機の届出および特定侵害事象等の報告義務が特別社会基盤事業者に課されるものであることを明示すべきです。 本解説案では、特別社会基盤事業者が、クラウドサービス事業者、回線事業者、システム運用や監視等を担当する委託先事業者等の外部関係者から提供される情報に依拠し得ることを適切に認識しています。他方で、法令上の義務はあくまでも特別社会基盤事業者に課されるものであり、対象となる製品やサービスを提供していることのみを理由として、その義務がテクノロジー提供事業者に及ぶものではないことを明確にすべきです。 クラウドサービス事業者やその他のテクノロジー提供事業者は、契約上の取決めや運用面での連携を通じて、顧客による法令遵守やセキュリティ対応を日常的に支援しています。しかしながら、法制度上、届出や報告に関する責任の所在が不明瞭になることは避けるべきです。規制対象となる社会基盤事業者とテクノロジーやサービス提供事業者間の責任分担を明確化することは、制度の実効性向上、侵害事象発生時の混乱防止、さらには重複した報告の回避にもつながると考えます。 そのため、本解説案に以下の文言を含むことを推奨します。 「クラウドサービス、委託事業、その他の第三者サービスが特定重要電子計算機として特定された場合であっても、法第２条、第4条および第5条に基づく届出・報告義務は、特別社会基盤事業者が負う。テクノロジーやサービス提供事業者は契約上の取決め等を通じて必要な協力を行うが、それらを提供していることのみを理由として、これらの義務を負うものではない。」 <報告対象となる特定侵害事象等の「痕跡」の範囲を明確化すること> BSAは、特別社会基盤事業者に影響を及ぼすサイバー脅威を早期に把握できるよう支援しようとする政府の取組を支持します。しかしながら、「特定侵害事象の痕跡」および「特定侵害事象の原因となり得る事象」に関連する義務については、さらなる明確化が望まれます。 現行の解説案では、ランサムウェア、不正アクセス、DDoS攻撃といった確認済みの侵害事象だけでなく、特定重要設備等に関連して、一定の攻撃の試み、マルウェアの送達事象、認証情報の窃取、さらにはそれらが発生した可能性を示す痕跡が存在する場合についても報告対象となるように読めます。しかし、こうした試みや事象は、実際のセキュリティ侵害ではなく、未確認の、失敗に終わった、あるいは自動的に防御・遮断された挙動を示しているにすぎない場合が多いことに留意することが重要です。 今日の脅威環境においては、最新のセキュリティオペレーションセンター（SOC）は、遮断された接続試行、認証の失敗、無害化されたマルウェアなどを含む数百万件の「事象」を日々処理しており、こうした件数はAIを活用したサイバー脅威の進展に伴い、今後さらに増加すると見込まれます。こうした事象は、確認済みの侵害事象とは本質的に区別されるべきです。 現代のセキュリティ監視システムは大量のアラート、指標、および潜在的な検知結果を生成するため、報告義務が発生する前に、どの程度の分析、確信の度合、または検証が求められるのかについて、さらなる明確化が必要です。 定常的なスキャン、侵入未遂、自動的に遮断された接続、無害な異常検知、重複検知、誤検知などは、いずれもセキュリティ監視システム上に証跡や痕跡を残す可能性があります。しかし、そのような検知結果は、必ずしもマルウェアが実行されたこと、不正アクセスが発生したこと、あるいは事業運営に影響が生じたことを意味するものではありません。 報告制度の実効性を確保するとともに、過剰な報告件数の発生を防ぐ観点から、報告対象となる痕跡については、実際に侵害事象が発生した、又は合理的にみて発生した可能性が高いと判断される場合に限られることを明確化するよう推奨します。 この考え方は、他の法域で採用されているリスクベースのインシデント報告制度とも整合性があります。こうした制度では、合理的な調査を通じて確認され、かつサイバーセキュリティリスク管理上重要なインシデントに報告対象を限定しています。これにより、政府の対応能力を圧迫し、報告情報全体の有用性を損なうような、実質的な価値の乏しい報告の大量発生を防ぐことができます。 ５－５では、フォレンジック調査や脅威ハンティングによる確認など、侵害事象の発生を認知する事例が示されていますが、以下の点を明確化することを推奨します。 「特定侵害事象の痕跡については、特別社会基盤事業者が合理的な評価を行った結果、当該痕跡が、特定侵害事象又は特定侵害事象を引き起こすおそれのある事象が発生したと結論づけるための信頼できる根拠を提供すると判断した場合に、報告対象となる。」 さらに、解説において、以下を区別する実務上の具体例を示すことを推奨します。 （１）報告対象となる、特定侵害事象の発生が疑われる痕跡（２）報告対象とならない、定常的な活動、不成功に終わった攻撃の試み、又は自動的に遮断・緩和された活動 加えて、「痕跡」について正式な定義を設け（例：「対象となる侵害事象を裏付ける技術的証跡として認識されるもの」）、併せて、客観的な認識基準を示すことを奨めます。 <リスクに応じた、国際整合性を踏まえたインシデント報告制度の推進> 本解説案は、システムの分類、報告対象事象、および報告義務について詳細な整理をしています。BSAは、サイバー脅威に関する状況認識の向上という解説案の目的を評価する一方で、報告要件の簡素化を継続的に進め、適切な範囲で既存の国際的に確立されたサイバーセキュリティインシデント報告制度との整合を図ることを推奨します。 国際的な実務との整合性を高めることにより、以下の効果が期待されます：（１）コンプライアンス対応の複雑さの軽減（２）より効率的なインシデント対応（３）組織が重要なサイバーセキュリティ事象にリソースを集中することによる、報告の質の向上（４）グローバルに統合されたシステム全体における、より効果的なサイバーリスク管理の促進。 このため、BSAは、運用・機密性・完全性・可用性に実質的な影響を及ぼす事象に重点を置き、リスクベースのアプローチを採用するとともに、サイバーセキュリティ上の結果に実質的な影響を及ぼさない低リスク又は推測的な事象については報告義務の対象外とすることを推奨します。 また政府が、報告義務の目的が重大なサイバーセキュリティリスクの把握及び低減を支援することにあることを明確化するとともに、その運用が国際的に認知されたインシデント報告の実務およびリスクの大きさに応じた適切な原則に沿ったものとなるよう、指針を示すことを推奨します。 [結論] BSAは、本解説案の目的を支持しつつ、（１）特別社会基盤事業者とテクノロジー提供事業者との間の責任分担（２）侵害事象の痕跡の扱い（３）国際的な実務と整合した比例的かつリスクベースの考え方にに基づく侵害事象報告義務の運用について、さらなる明確化を推奨します。 これにより、本制度の実効性を高めるとともに、規制対象事業者及び提携するテクノロジー提供事業者にとっての不確実性を低減することができます。我々は、日本のサイバー対処能力の更なる強化に向け、今後も政府と連携していけることを期待しています。 [注釈] （１）Business Software Alliance（https://bsa.or.jp/（日本サイト）、www.bsa.org（グローバルサイト））は、アメリカ合衆国、ヨーロッパ、アジアの20を超える市場で活動し、あらゆる分野の産業また一般消費者がイノベーションの恩恵を受けられるよう、テクノロジーに対する信頼を構築する政策を推奨する業界団体です。BSAの会員には以下の企業が含まれます：Adobe, Alteryx, Amadeus, Amazon Web Services, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cloudflare, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Morisawa, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., TrendAI, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.	・「<法定の届出・報告義務を負う主体が特別社会基盤事業者であると明確化すること>」につきまして 資産届出及びインシデント報告の主体が特別社会基盤事業者であることについては、法第４条及び第５条や本解説3-1、6-1等に明記しております。その上で、これらの届出等にあたっては、本解説4-1-2や5-5に記載のとおり、関係する事業者で必要な調整等をいただくことが望ましいと考えております。 ・「<報告対象となる特定侵害事象等の「痕跡」の範囲を明確化すること>」につきまして 御指摘の一定の攻撃の試み、マルウェアの送達事象、認証情報の窃取、さらにはそれらが発生した可能性を示す痕跡が存在する場合につきましては、指摘のとおり日常的に発生していると考えられ、仮にアタックサーフェスを含む全ての特定重要電子計算機で発生した事象を報告対象とした場合、特別社会基盤事業者の負担が過大になるため、特定重要設備の機能の低下又は停止へのリスクを踏まえ、本解説5-2に記載のとおり、特定重要設備等に該当する特定重要電子計算機において発生した事象に限り、報告対象としております。その他、頂いたご意見につきましては、実際の運用も見ながら今後の本解説への反映を検討させていただきます。 ・「<リスクに応じた、国際整合性を踏まえたインシデント報告制度の推進>」につきまして 頂いたご意見につきましては、実際の運用も見ながら今後の本解説への反映を検討させていただきます。

No.	御意見の要旨	御意見に対する主な考え方
	1 全体（特にP7以降、P62以降） 本ガイドラインでは、巻末に用語集が設けられている一方、本文中では、 ・「特定重要設備の機能が停止し、又は低下する」 ・「特定重要設備の機能に影響を与える」 ・「特定重要設備に影響を及ぼす」 など、意味が近接する表現が複数用いられており、それぞれが同一の概念を指すのか、又は異なる趣旨を有するのかが必ずしも明確ではありません。 また、 ・「電子計算機」 ・「特定重要電子計算機」 ・「一号電子計算機」 ・「クラウドサービスを使用する電子計算機」 などについても、本文と用語集を照らし合わせながら理解する必要があり、届出対象及び報告対象を判断する上で解釈に差異が生じるおそれがあります。 このため、事業者が制度を一貫して理解・運用できるよう、可能な限り用語集上の定義を引用又は参照するなど、各記載がどの概念を指しているのかをより明確にしていきたいです。 2 P8「2-1-1 特定社会基盤事業者が使用する電子計算機」 「クラウドサービスを使用する場合」の見出しの直下に説明文がなく、その後「日本国外に存在する場合」「他の特別社会基盤事業者と共同利用している場合又は共同で構築されている場合」「災害復旧サイトである場合」が続いているため、これらが「クラウドサービスを使用する場合」の具体例なのか、又は独立した留意事項なのか判然としません。 事業者が特定重要電子計算機への該当性を適切に判断できるよう、見出しと本文との対応関係が明確となるよう記載をご検討いただきたいです。 例えば、 ・「クラウドサービスを使用する場合」の説明を追記する ・「日本国外に存在する場合」以下を独立した見出しとして整理する ・又は箇条書き・階層構造を見直す など、文書構成上の整理を行うことで、事業者による誤解や解釈のばらつきの防止につながると考えます。 3 P8「クラウドサービスを使用する場合」 P23～24「届出事項」 ガイドラインでは、クラウドサービスを利用する場合も特定重要電子計算機の対象となり得ることが示されており、届出事項としてはクラウドサービス名（例：EC2、RDS等）を記載することとされています。 一方、クラウドサービスについては、利用形態や責任分界点（SaaS、PaaS、IaaS等）が多様であり、利用事業者が管理・運用する範囲も異なります。 そのため、特定重要設備の機能に影響を及ぼす形で利用されるクラウド上の電子計算機については、事業者が自社のシステム構成、依存関係及び運用実態を踏まえて対象該当性を判断し、届出対象を整理する考え方であることを明確化いただきたいです。 また、FAQ等において、クラウドサービスの責任分界点を踏まえた具体例を示していただくことで、事業者の負担軽減につながると考えます。 4 P14「2-2-2[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）」 「インターネットとの接続口の機器」については、「グローバルIPアドレスを利用して電気通信が到達可能な機器」と記載されている一方で、「グローバルIPアドレスを割り当てられているものは対象」との記載もあり、対象要件として「グローバルIPアドレスの付与」と「インターネットからの到達可能性」の関係が必ずしも明確ではありません。 このため、対象要件はグローバルIPアドレスが割り当てられていることに加え、インターネットから当該機器又は当該機器の通信機能に実際に到達可能であることである旨を、より明確に記載いただきたいです。 また、対象要件がグローバルIPアドレスが割り当てられていることに加え、インターネットから当該機器又は当該機器の通信機能に実際に到達可能であることである場合、以下の場合は、対象機器に含まれないという理解で良いでしょうか。 ・グローバルIPアドレスを内部識別用として利用している場合 ・当該プレフィックス又はホストへの経路がインターネットへ広告されていない場合 ・ネットワーク設計上、インターネットから当該機器への到達性が確保されていない場合 これらは、実質的にインターネットからの攻撃対象（アタックサーフェス）とはならない構成であり、対象範囲を明確化することで、事業者及び政府の負担軽減につながると考えます。 5 P20「3-1-1 届出対象」 P24「3-1-4 届出事項」 ガイドラインでは、アプライアンス以外の特定重要電子計算機について、OS、ミドルウェア及びアプリケーションを届出対象としており、届出事項として「製品名」及び「製造者名」を記載することとされています。 一方、現在のシステム開発・運用では、一般に流通するソフトウェアや各種OSS等を組み合わせて、自社向けシステムやサービスを構築することが一般的です。 このような構成においては、届出時に「製品名」及び「製造者名」をどの単位で整理することを想定しているかが必ずしも明確ではありません。 そのため、製品名・製造者名の記載単位について、代表的な構成例を用いてFAQ等で明確化いただきたいです。 例えば、 ・市販ソフトウェアを利用する場合 ・OSSを利用したシステムを構築している場合 ・クラウドサービス上でアプリケーションを運用している場合 などについて、届出単位の考え方を例示いただくことで、事業者間で統一的な届出運用に資すると考えます。 6 P24～26（届出事項・任意提出事項） 届出事項及び任意提出事項として求められているシステム概略図、グローバルIPアドレス、バージョン情報、資産管理主体等は、事業者の攻撃対象（アタックサーフェス）、システム構成及びセキュリティ管理状況の把握につながる高度に機微な情報であると考えます。 これらの情報について事業者が安心して提供できるよう、 ・情報の利用目的 ・共有範囲（関係行政機関を含む） ・保存期間 ・アクセス権限	・1につきまして 本解説では、法令上の用語や定義を引用し、用語の解釈について不整合が生じないように作成しているものとなります。運用後の特別社会基盤事業者の意見も踏まえ、見直しを行って行くことを考えております。 ・2につきまして 「クラウドサービスを使用する場合」は、独立した項目となりますが、記載が分かり難いため修正いたしました。 ・3につきまして 特別社会基盤事業者が特定重要電子計算機についてクラウドサービスを使用する場合については、利用形態や責任分界点によらず、届出対象となるため、利用形態や責任分界点を踏まえた対象の考え方については記載しておりません。 ・4につきまして 「インターネットからの到達可能性」の記載につきましては、御指摘のグローバルIPアドレスと同様の符号を内部識別用に利用している場合を除く趣旨のものです。頂いたご意見につきましては、実際の運用も見ながら今後の本解説への反映を検討させていただきます。 ・5につきまして 本解説1-1に記載の届出対象の粒度で提出いただければと存じますが、疑義がありましたら特別社会基盤事業者に案内しております相談窓口までお問合せください。 ・6につきまして 本解説1-1に記載のとおり、本解説は法第2条第2項第2号、第4条及び第5条の届出等に関する事項等を解説するものであり、御指摘の安全管理の記載は馴染まないものと考えておりますが、法第8条の規定も踏まえ、安全管理措置を徹底してまいります。

No.	御意見の要旨	御意見に対する主な考え方
78	・暗号化その他の保護措置 ・アクセスログ・監査の実施 ・漏えい又は不正アクセスが発生した場合の通知・対応 などの情報管理に関する考え方を、ガイドライン又は別途公表される運用文書等において明確化いただきたいです。	・7につきまして バージョン情報の届出は任意であるため、その具体的方法についても当然任意で差し支えありません。
	7 P24～26「3-1-4 届出事項」 ガイドラインでは、バージョン情報については任意事項とされており、可能な範囲で記載することが望ましいとされています。	・8及び9につきまして 変更届出の対象については、本解説3-2に記載のとおり、3-1により届け出た情報に変更があった場合であり、当該変更があったか否かで判断いただければと存じます。
	一方、現在のシステム運用では、セキュリティパッチ適用、ローリングアップデート、コンテナイメージ更新、ノード入替等により、ソフトウェア及び実行環境のバージョンが頻繁に変動することが一般的です。	また、任意で届け出ることが望ましい事項に変更があった場合の考え方については、御指摘も踏まえ、本解説3-1に追記しました。
	このため、運用中の全ての資産について、詳細なバージョン情報を継続的かつ網羅的に把握・更新することは、実務上現実的ではありません。	変更届出については、変更の日から4月以内の届出が必要としております。個々の機器において変更が生じる度に変更届を行うことは、事業者に多大な負担が想定されることから、3-2-1に記載のとおり、「例えば、四半期ごとに特定重要電子計算機の棚卸しを行い、1月でその結果をとりまとめて届け出るといったことも可能である。」としているところです。
	そのため、 ・バージョン情報については、届出時点で把握可能な範囲での記載を想定していること ・継続的な更新を前提とするものではないこと ・又は、詳細なバージョン情報の記載が困難な場合の取扱い について、ガイドライン又はFAQ等で具体例を示していただきたいです。	・10につきまして 御指摘のとおり、エンドポイント、ネットワーク機器等において様々な形でスキャンが実施されると承知しています。例示いただいたものを含めて、検知等される形態1つずつに係る特定侵害事象等への該当性をお示すことは困難であるため、インシデント報告の対象となるか判断に迷うケースがございましたら、その際に所管省庁又は国家サイバー統括室に相談いただくようお願いいたします。なお、特定侵害事象の原因となり得る事象もインシデント報告の対象となりますので、特定重要設備・類型Eの機器においてはマルウェアが受信される事象でも対象となりますので申し添えます。
	8 P28～30「3-2 変更届出」 ガイドラインでは、届出事項に変更があった場合には変更届出を行うこととされていますが、ソフトウェアについて、どのような変更を変更届出の対象として想定しているかが必ずしも明確ではありません。	・11につきまして 御意見を踏まえ修正させていただきます。
	実務上は、ソフトウェアの保守・運用に伴い、アップデート、バージョン更新、製品更新等が発生しますが、どのような変更について変更届出を行うことを想定しているか判断が難しい場合があります。	・12につきまして 事業者ごとにサービス内容や保有電子計算機、ネットワーク構成が異なることから、機能低下が発生した又は機能低下のおそれがあったと判断する基準や考え方を一律に規定することは困難です。
79	このため、変更届出を要する代表的な変更例及び通常の保守・運用として取り扱う変更例について、FAQ等で具体例を示していただきたいです。	
	9 P28～30「3-2 変更届出」 ガイドラインでは、届出事項に変更があった場合には変更届出が必要とされており、変更届出が不要となるものとしては、特別社会基盤事業者の名称変更が示されています。	
	一方、実務上は、セキュリティパッチの適用、ソフトウェアのマイナーバージョンアップ、設定変更等、通常の保守・運用に伴う変更が日常的に発生します。また、任意提出事項としてバージョン情報等を提出することが望ましいとされている一方で、当該情報に変更があった場合には変更届出を提出することが望ましいとされており、通常運用に伴う変更について、どの範囲まで更新を想定しているかが必ずしも明確ではありません。	
	このため、事業者の実務負担や運用実態も踏まえ、 ・変更届出が必要となる代表的な変更 ・通常の保守・運用の範囲として変更届出を要しない変更 ・任意提出事項について、通常運用に伴う変更が生じた場合に期待される更新頻度・更新方法 などについて、FAQ等に具体例を示して明確化いただきたいです。	
	また、日常的に発生する変更については、一定期間内の変更をまとめて更新する運用が許容されるか否かについても考え方をお示しいただくことで、事業者の負担軽減につながると考えます。	
	10 P42「5-1-1 マルウェアの供用」 ガイドラインでは、「マルウェアが実行され得る状態に置かれること」が特定侵害事象に該当するとされる一方、アンチウイルス製品等のリアルタイムスキャンにより「即時削除された場合」は該当しないとされています。	
	一方、現在のEDR・NGAV等では、ファイルのダウンロード後、メモリ展開時、プロセス生成時又は実行開始直後など、様々なタイミングで検知・遮断が行われます。	
80	このため、例えば、 ・ファイルはダウンロードされたものの、実行前に検知・隔離された場合 ・ファイルがメモリ上に展開された直後に検知・ブロックされた場合 ・プロセス生成後、実際の不正動作前に終了させられた場合 などが、「実行され得る状態」に該当するのか、それとも「即時削除」に該当するのかについて、具体例を用いて明確化いただきたいです。	
	判断基準を明確化いただくことで、事業者間で統一的な報告運用が可能になるものと考えます。	
	11 P43「5-1-2 不正アクセス」 P43における「識別符号」の説明では、 「次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたもの」 と記載されていますが、「次のいずれか」の内容は同ページ中には記載されておらず、次ページ（P44）に掲載された不正アクセス禁止法第2条第2項各号を参照する必要があります。	
	そのため、読者がP43の説明のみを参照した場合でも内容を理解できるよう、 ・「次のいずれか」として各号を本文中に記載する ・又は「不正アクセス禁止法第2条第2項各号」といった参照を付記する など、参照関係を明確化いただきたいです。	
	法令の趣旨を正確に理解し、報告対象の判断を適切に行う観点からも、参照先を明確にすることが望ましいと考えます。	
	12 P46「5-1-3 業務妨害等」 P50「5-3-1 DDoS攻撃事案」 ガイドラインでは、「機能停止又は機能低下には至らなかったが、そのおそれがあるDDoS攻撃」が報告対象とされていますが、「おそれがある」と判断する際の考え方が必ずしも明確ではありません。	
	事業者によっては、サービス特性やシステム構成が大きく異なることから、応答時間、処理能力、通信量、利用者影響等、評価指標も様々ですし、DDoS攻撃の検知に用いる指標や閾値は、事業者ごとにサービス特性、ネットワーク構成及び防御設備が異なることから、観測する通信量（bps、pps等）や各種監視指標も様々です。	
81	このため、 ・「機能低下」と判断する際の基本的な考え方 ・「おそれがある」と判断する際の基本的な考え方 ・客観的な判断指標の例 ・又は事業者が自ら定める運用基準に基づいて判断することを想定しているか について、FAQ等で明確化いただきたいです。	
	判断の考え方を明確化いただくことで、事業者間で報告基準の解釈を統一し、制度の適切な運用に資すると考えます。	

No.	御意見の要旨	御意見に対する主な考え方
	13 P47～49「5-2-1 特定重要設備等における特定侵害事象の原因となり得る事象」 5-2-1の[□]～[ニ]では、不正アクセス禁止法第2条第4項に規定される不正アクセス行為の成立には至らない場合であっても、認証情報の入力やアクセス制御回避を試みる行為を報告対象としていることから、5-1-2より広い範囲を対象としているように読めます。 一方で、事業者が実施するペネトレーションテスト、脆弱性診断、レッドチーム演習等においても、認証情報の入力やアクセス制御回避の試行が行われる場合がありますが、これらは報告対象外という理解で良いか。 14 P48「5-2-1 [イ]」 ガイドラインでは、5-2-1[イ]において、「アンチウイルス製品等のリアルタイムスキャンによる即時削除やコード実行停止がされた場合も含む」とされています。 一方、現在の企業ネットワークでは、マルウェアや不正ファイルは、端末上のアンチウイルス製品だけでなく、ネットワーク境界に設置されたファイアウォール、メールゲートウェイ、Webゲートウェイ、IPS等により、自動的に検知・遮断されることが一般的です。 このため、例えば、 ・メールゲートウェイで自動的に隔離・削除された場合 ・ファイアウォール又はIPSにより通信が遮断された場合 ・機械的なばらまき攻撃がネットワーク境界で遮断され、端末やサーバまで到達しなかった場合 についても、5-2-1[イ]の「即時削除やコード実行停止がされた場合」に含まれるのか、又は報告対象外となるのかについて、具体例を用いて明確化いただきたいです。 事業者による報告対象の判断を統一し、過不足のない報告運用につなげる観点からも、判断の考え方をFAQ等で示していただくことが望ましいと考えます。 15 P48「5-2-1[□]」 5-2-1[□]では、「アクセス制御機能に係る他人の識別符号が入力される事象」が報告対象とされていますが、パスワードプレー攻撃やブルートフォース攻撃のように、自動化された大量の認証試行が短時間に繰り返される場合の報告単位が明確ではありません。 このため、例えば、 ・同一の攻撃主体による一連の認証試行 ・同一キャンペーンと判断される大量のログイン試行 については、DDoS攻撃では一連の攻撃をまとめて報告する考え方と同様に、認証攻撃についても一連の攻撃をまとめて報告して良いか。 16 P49「5-2-1[ハ]」 5-2-1[ハ]では、アクセス制御機能による特定利用の制限を免れることができる情報又は指令が入力される事象が報告対象とされていますが、日常的に発生する攻撃試行との関係が必ずしも明確ではありません。 現在、多くの事業者では、IPS、WAF等のセキュリティ製品により、脆弱性を悪用する通信や認証回避を試みる通信が自動的に検知・遮断される運用が一般的となっています。 このため、 ・IPSやWAF等により正常に検知・自動遮断された攻撃試行 ・利用者影響やシステム侵害に至らなかった攻撃試行 についても、一律に報告対象となることを想定しているのか、又は一定の判断基準を設けることを想定しているのかについて、考え方を明確化いただきたいです。 また、代表的な対象例・対象外例をFAQ等で示していただくことで、事業者間で統一的な報告運用が可能になるものと考えます。 17 P49「5-2-1[ホ]」 5-2-1[ホ]では、「特定重要電子計算機のアクセス制御機能に係る他人の識別符号が取得される事象」が報告対象とされ、具体例として「認証情報がサイバー攻撃者に窃取された場合」が示されています。 一方、認証情報の窃取については、事業者自らのシステム上で窃取を確認できる場合だけでなく、外部の脅威インテリジェンス、ダークウェブ監視サービス等により認証情報の流通を把握する場合もあります。 このため、 ・自社システム上では認証情報の窃取事実を確認できない場合 ・外部情報により認証情報の流通又は販売が確認された場合 について、「特定重要電子計算機のサイバーセキュリティを害することによって行われるもの」ではない、という理解で良いか。	・13につきまして 御理解の通りとなります。 ・14につきまして 御指摘のとおり、エンドポイント、ネットワーク機器等において様々な形でスキャンが実施されると承知しています。例示いただいたものを含めて、検知等される形態1つずつに係る特定侵害事象等への該当性をお示することは困難であるため、インシデント報告の対象となるか判断に迷うケースがございましたら、その際に所管省庁又は内閣府サイバー安全保障担当に相談いただくようお願いいたします。なお、特定侵害事象の原因となり得る事象もインシデント報告の対象となりますので、特定重要設備・類型Eの機器においてはマルウェアが受信される事象でも対象となりますので申し添えます。 ・15につきまして 本解説6-2に追記いたしました。 ・16につきまして 御指摘のとおり、エンドポイント、ネットワーク機器等において様々な形でスキャンが実施されると承知しています。例示いただいたものを含めて、検知等される形態1つずつに係る特定侵害事象等への該当性をお示することは困難であるため、インシデント報告の対象となるか判断に迷うケースがございましたら、その際に所管省庁又は内閣府サイバー安全保障担当に相談いただくようお願いいたします。なお、特定侵害事象の原因となり得る事象（※）もインシデント報告の対象となりますので、特定重要設備・類型Eの機器においては、マルウェアが受信される事象でも対象となりますので申し添えます。 （※）特定重要設備・類型Eの機器：マルウェアが受信される事象【第4条第1項第1号イ】＋マルウェアが実行された痕跡を認知した場合【第4条第1項第2号】特定重要設備・類型E以外の機器：マルウェアが実行された痕跡を認知した場合【第

No.	御意見の要旨	御意見に対する主な考え方
	18 P50～55（DDoS攻撃事案、報告対象、報告期限） ガイドラインでは、DDoS攻撃について、機能停止又は機能低下が発生した場合に加え、機能停止又は機能低下のおそれがある事案についても対象として整理されていますが、「機能低下」の判断基準が必ずしも明確ではありません。 近年では、多くの事業者がAuto Scaling、負荷分散、CDN、DDoS対策サービス等を利用しており、これらの防御機能が正常に動作した結果としてサービス影響を回避できる事例も日常的に発生しています。 このため、例えば、 ・Auto ScalingやScale Outによりサービス影響を回避した場合 ・DDoS対策サービスやCDNにより攻撃を吸収した場合 ・通常の防御機能により利用者影響なく処理できた場合 などについては、報告対象外という理解で良いでしょうか。 報告対象の考え方が明確になることで、事業者及び政府の負担軽減となり、真に共有すべき事案に関する迅速な情報共有にも資するものと考えます。 19 P52「5-5 特定侵害事象等の発生 の認知」 P57～58 FAQ（クラウドサービス） ガイドラインでは、クラウドサービス事業者からの通知により特定侵害事象等を認知する場合があること、またクラウドサービス事業者からの通知内容等をあらかじめ確認することが望ましい旨が記載されています。 一方、外部クラウドサービスでは、サービス形態や契約内容によっては、本法に基づく速報期限（認知後3～5日以内等）を前提とした迅速なインシデント通知が保証されていない場合があります。 このため、クラウドサービス事業者からの通知遅延により、特別社会基盤事業者が特定侵害事象等を期限内に認知できなかった場合の報告義務の考え方について、FAQ等で明確化いただきたいです。 例えば、 ・報告期限の起算点となる「認知」の考え方 ・クラウドサービス事業者からの通知を契機として認知する場合の取扱い ・利用事業者に期待される合理的な対応 などを示していただくことで、クラウドサービス利用事業者における適切な運用に資すると考えます。 20 P55「6-2 報告期限」 DDoS攻撃事案については、「認知後に可能な限り速やかな報告を行う」とされていますが、「可能な限り速やか」の考え方が必ずしも明確ではありません。 実際のインシデント対応では、初動対応やサービス復旧対応が最優先となる場合も多く、速報のタイミングについて判断に迷うことが想定されます。 このため、 ・「可能な限り速やか」と考える際の基本的な考え方 ・初動対応との優先関係 ・速報に求められる情報量 ・速報を提出するタイミングの目安 について、FAQ等で明確化いただきたいです。 事業者が適切な初動対応を行いつつ、政府への迅速な情報共有を実現する観点からも、運用上の考え方を示していただくことが望ましいと考えます。 21 P53～56「6. 報告手続」 一般的なサイバー攻撃事案では、単一のインシデントの中で、複数の特定侵害事象又は特定侵害事象の原因となり得る事象（5-1及び5-2）が段階的に発生し、それぞれを認知する時点も異なることが想定されます。 一方、ガイドラインでは速報・続報・詳細による報告運用が示されていますが、報告単位について、一つのインシデントを単位とすることを想定しているのか、それとも個々の特定侵害事象等ごとに報告することを想定しているのかが必ずしも明確ではありません。 このため、同一インシデントにおいて新たな特定侵害事象又は特定侵害事象の原因となり得る事象を認知した場合には、一つのインシデントを単位として報告を継続し、新たに判明した内容については続報として報告する運用を想定しているかについて、FAQ等で明確化いただきたいです。 報告単位の考え方を明確化いただくことで、事業者間で統一的な運用が可能となり、政府における情報集約・分析の効率化にも資するものと考えます。	4 条第 1 項第 2 号】 ・17につきまして ダークウェブ上で真正性が不確かな認証情報が存在するといった場合のみでは、特定侵害事象が生ずる可能性を示唆するものでありますが、当該事象自体が特定侵害事象の原因となり得るまでは断定できませんので、報告対象外となります。 ・18につきまして 事業者ごとにサービス内容や保有電子計算機、ネットワーク構成が異なることから、機能低下が発生した又は機能低下のおそれがあったと判断する基準や考え方を一律に規定することは困難です。 ・19につきまして 本解説5-5において、「報告期限の起算は、サイバーインシデント発生を認知した日から行う」と記載しており、また、その認知方法の例として「D) 特定重要電子計算機に該当するクラウドサービス等について、クラウドサービス事業者等からインシデント通知があり、そのインシデントが特定侵害事象等と判定された」との記載のとおり、通知受領を持って認知するのではなく、通知内容を踏まえて特定侵害事象等に当てはまると判断した場合に特定侵害事象等の発生を認知したこととしております。 ・20につきまして 初動対応を優先いただくものと考えております。事案の対応状況等を考慮した上で可能な限り速やかに報告をお願いします。また、主務省令第4条第3項において、速やかに報告する場合においては、同項第3号から第7号までに掲げる事項については、報告をしようとする時点において認知しているものに限り、報告すれば足りることとしております。 ・21につきまして 御指摘を踏まえ本解説に追記いたしました。