「重要電子計算機に対する不正な行為による被害の防止に関する法律に基づく特別社会基盤事業者による特定侵害事象等の報告等に関する命令案」に関する意見募集の結果一覧

No.	御意見の要旨	御意見に対する主な考え方
第１条（重要電子計算機）　関係		
1	米国ではList of Equipment and Services Covered By Section 2 of The Secure Networks Actで、米国FCC（通信系の規制）の対象リストの製品について、米国政府と取引のある企業及びその企業の委託先やサービス提供先まで合理的な範囲で要確認とされており、実態として米国で事業を行っている場合や、国内で米国企業へ通信サービスを提供している日本の通信事業者も当該法令の規制の影響を受ける可能性のあるグレーな状況と理解しています。 また、この法令は通信ネットワークのリスクを強く認識しており、日本の経済安全保障推進法やサイバー攻撃対処法では、主要な通信事業者は網羅されているものの、対象を基幹インフラの重要電子計算機等に限定しており、例えば金融機関等の基幹インフラ内の通信に専用線等を利用している場合や、金融機関等の基幹インフラ間で専用線等を利用している場合について、管理の対象から外れているかどうかも明確には管理できていない状況だと考えられます。 また、2026年3月27日にサプライチェーン強化に向けたセキュリティ対策評価制度に関する制度構築方針を公表するなど、政府としてもサプライチェーン対策の強化に取り組んでいる状況です。 ついては、今回の管理対象に、通信事業者が金融機関等の基幹インフラ内の通信に専用線等を利用している場合や、金融機関等の基幹インフラ間で専用線等を利用している場合も含める事で事案発生時の影響範囲を早期特定可能にすべきだと考えます。 なお、今回の意見対象ではありませんが、今後、基幹インフラについて、更なるサプライチェーン強化が求められる場合、経済安全保障推進法において、基幹インフラ事業者に対して影響がないことを確認するといった改善も考えられます。	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」といいます。）の対象となる重要電子計算機には、経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律（令和４年法律第43号。以下「経済安全保障推進法」といいます。）第50条第１項の規定に基づく指定を受けた金融機関の使用する電子計算機のうち、特定重要設備（同項に規定する特定重要設備をいいます。以下同じ。）と専用線等で直接又は間接に接続されているものも含まれます。
2	第一条および第四条一項二号における「間接接続」の定義を明確にして頂くことは可能か。弊社の様な特定重要電子計算機（クラウドも含む）提供事業者としては、同適応範囲を、管理及び制御プレーンまでに限定して頂きたいと考えるが、政府のご見解を伺いたい。	「間接に接続」とは、二の電子計算機が他の電子計算機を介して電気通信回線で接続されていることをいいます。 また、特定重要電子計算機については、特定重要設備との関係に着目して、特定社会基盤事業者（経済安全保障推進法第50条第１項に規定する特定社会基盤事業者をいいます。以下同じ。）が使用する電子計算機のうち、そのサイバーセキュリティが害された場合に、特定重要設備の機能が停止し、又は低下するおそれがあるものを規定しております。この観点から、御指摘の管理及び制御プレーンのほか、例えばネットワーク構成図を保存する電子計算機（第１条第１項第５号イ）等を規定しております。
3	経済安全保障推進法上の特定重要設備は本番環境が対象であることを踏まえ、以下の点をご教示いただきたい。 (1) 特定重要設備の試験環境・開発環境は、特定重要電子計算機の対象外という理解で相違ないか。 (2) 本番環境と試験・開発環境が同一の物理ネットワークセグメント内に構築されている場合であっても、試験・開発環境として明確に区別・管理されているものは対象外と解釈して差し支えないか。 (3) グループ内プライベートクラウド環境において、本番環境と試験・開発環境が同一の物理基盤上に論理的に分離されて構築されている場合、試験・開発環境に係る論理的な範囲は対象外という解釈でよいか。 (4) 仮に試験・開発環境が対象となる場合、本番環境と同等の届出・管理義務が課されるのか、それとも軽減された取扱いが認められるのかご教示いただきたい。	・(1)について (2)に該当する場合を除き、御理解のとおりです。 ・(2)について 本番環境の特定重要設備に対し、ルーティングを介さず通信可能である場合には、試験・開発環境にある電子計算機であっても、本省令案第１条第１項第１号の電子計算機の対象となります。 ・(3)について 御指摘の試験・開発環境から本番環境にデータを送信しえないよう論理的に制御されている場合は、本省令案第１条第１項第１号の電子計算機の対象外です。 ・(4)について 本番環境の特定重要電子計算機と同等の届出義務が課されます。
4	・全体として、「電気通信信号」は法律に出てくる「電気通信」と異なる概念なのか。同じであれば統一したらどうか。	「電気通信」とは、有線、無線その他の電磁的方式により、符号、音響又は影像を送り、伝え、又は受けることを指す一方、「電気通信信号」とは、当該電気通信において用いられる信号を指し、両者は異なる概念です。
5	1 1条1項柱書の「公衆の用に供されている」は電気通信事業者の一般の通信ネットワークを使って接続されている場合であっても論理的に分離された閉塞網としているものであれば該当するのですか？ 2 1条1項3号の「割り当てられる」とは誰によって割り当てられるものなのですか？「プログラム～が一定の基準に適合する」かを判断するのも結局は符号に置き換えて行われますので、プログラムと符号で分ける必要がわかりません。 3 1条1項5号 ネットワーク構成図が何か分かりませんので定義すべきです。	・１について 御指摘の閉域網は公衆の用に供されている電気通信回線に該当いたしません。 ・２について 本条文案は、「割り当てられる」という様態を規定しているものです。御指摘の「一定の基準に適合する」か否かの判断は様々な形態で行われるところ、それを網羅的に規定しているものです。 ・３について 電子計算機とこれらの間を接続する電気通信回線の概要を記載した図面です。詳細は、今後策定するガイドラインにおいて解説する予定です。

No.	御意見の要旨	御意見に対する主な考え方
6	１、特定重要電子計算機として特定重要設備と接続されている電子計算機があり、例外として「公共の用に供される電気回線での接続を除く」とあり、インターネットによる接続は２に含まないと整理している インターネットによる接続を除いている意図・目的をご教示頂きたい ２、第１条第１項第2号「ファイアウォール等（中略）であって、他のファイアウォール等を介さずに一号電子計算機に電気通信信号を送信するもの」の「等」の意図として、想定されているケース（L3スイッチのACL機能等）があれば明示頂きたい ３、ネットワーク構成図は、特定重要設備と直接的・間接的に接続されていない場合は、届出不要か判断が付き辛く明示頂きたい ４、「一号電子計算機又はこの項に規定する電子計算機（このロに掲げるものを保存するもの及び次号に規定するものを除く。）に係るアクセス制御機能（不正アクセス禁止法第二条第三項に規定するアクセス制御機能をいう。）を有する電子計算機」 上記定義において（このロに掲げるものを保存するもの及び次号に規定するものを除く。）とあるが、除かれる電子計算機をご教授願う	・１、について 特定重要設備とインターネット等の公衆の用に供されている電気通信回線を介して接続する電子計算機については、特定重要電子計算機として法第４条第１項の届出（以下「資産届出」といいます。）の対象とした場合、特別社会基盤事業者の負担となる一方、当該電子計算機のサイバーセキュリティが害されたとしても、直ちに特定重要設備の機能に影響を与えることはないと考えられるため、対象外としています。 ・２、について 「ファイアウォール等」の「等」は、一般的にファイアウォールと呼ばれる機器のみならず、WAF等も対象であることを明示する意図で規定したものです。なお、名称を問わず、ファイアウォール等の機能を有する機器は対象であり、御指摘のACL機能を有するＬ３スイッチも対象です。 ・３、について 第１条第１項第５号イのネットワーク構成図を保存する電子計算機については、特定重要設備と直接又は間接に電気通信回線で接続されていないものは対象外です。 ・４、について 識別符号を有する電子計算機（第１条第１項第５号ロ）及びアクセス制御機能を有する電子計算機（第１条第１項第６号）です。これらの電子計算機のアクセス制御機能を有する電子計算機は第１条第１項第６号の対象外です。
7	【質問】 第1条第1項第1号から第7号までの各電子計算機は、いわゆる本番環境の機器が対象になると認識していますが、災対（DR）用のように通常時には本番環境としては稼働させない環境も範囲に含む想定でしょうか。 【依頼】 第1条第1項第1号から第7号までの各電子計算機は、どのような機器が該当するか具体的に示していただけますでしょうか。 【質問】 第1条第1項第1号から第7号までの各電子計算機は、1号電子計算機（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という前提があると認識していますが、1号電子計算機の機能に影響を与える電磁的記録とはどのようなものを指しますでしょうか。プログラムやアプリケーションデータ、データベース上のデータ等、具体的にお教えいただけますでしょうか。 【質問】 第1条第1項第4号と第1条第1項第3号には、いずれも1号電子計算機に電気通信信号を送信する際に介されるファイアウォールを含むと認識していますが、その認識に相違ないでしょうか。相違ない場合、当該ファイアウォールをどのように区別するかお教えいただけますでしょうか。 【依頼】 第1条第1項第4号において、ガイドライン案を公開いただく際には、金融業界でイメージしやすい言葉で補足いただく等、ご検討いただけますでしょうか。	災害復旧サイト等の本番環境として稼働させない環境にある電子計算機についても、第１条第１項第１号から第７号までの要件に該当する電子計算機は対象です。 第１条第１項第１号から第７号までの電子計算機の具体例は、今後策定するガイドラインでお示しいたします。 電磁的記録とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものを指し、具体的には、御指摘のプログラムが記載された記録やアプリケーションデータ、データベースのデータ等、あらゆるデータが該当いたします。 第１条第１項第３号に規定するファイアウォール等は、同項第４号にも該当する場合があります。この場合、資産届出においては、様式第１中「特定重要電子計算機の区分」の欄において、両方に該当する旨規定していただければと存じます。 第１条第１項第４号のガイドラインに関して頂いたご意見は、今後のガイドラインの策定における参考といたします。
8	施行規則案第１条第１項第１号について 「経路制御」の定義中にある「電気通信信号を送信するに当たり、宛先に至る経路のうちから、経路の状況等に応じて最も適切と判断したものに電気通信信号を送信すること」とは、Ｌ３のルーティング機能を想定したもので、L2のスイッチングによる制御によって通信が特定重要設備に到達する範囲が本号に該当する という理解でよいでしょうか？	御指摘の「経路制御」は、ルーティング機能を規定したものであり、スイッチングによる制御は「経路制御」には含まれません。そのため、特定重要設備にデータを送信することができる電子計算機であって、当該データの送信に当たりスイッチングはされるがルーティングがなされないものは、本号に該当いたします。
9	以下のとおり「電磁的記録を送信するに当たり経路制御がされないもの」を重要電子計算機と定義されていますが、具体的にどのような機器が対象となるのか明確にしていただきたく存じます。 ※命令案抜粋 特定重要設備に電磁的記録（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（以下「法」という。）第二条第八項第二号に規定する電磁的記録をいう。以下同じ。）を送信する機能を有する電子計算機であって、当該電磁的記録を送信するに当たり、経路制御（電気通信信号を送信するに当たり、宛先に至る経路のうちから、経路の状況等に応じて最も適切と判断したものに電気通信信号を送信すること（送信することのできる二以上の経路のうちから、宛先ごとに一に定められた経路に電気通信信号を送信することを除く。）をいう。次号において同じ。）がされないもの	機器の種類を問わず、ルーティングを介さずに、特定重要設備にデータを送信することのできる電子計算機が該当いたします。

No.	御意見の要旨	御意見に対する主な考え方
10	命令案第１条第１項第１号に規定する「経路制御がされないもの」について、以下の点をご教示いただきたい。 (1)「経路制御がされない」とは、宛先に至る経路を動的に選択する機能（BGP、OSPFなどの動的ルーティングプロトコル）を持たないことを指すという理解でよいか。 (2) 一般的なロードバランサーが行う負荷分散処理は「経路制御」に該当するか。また、スタティックルーティング（静的経路制御）のみを行う機器は「経路制御がされないもの」に該当するか。 (3)「経路制御がされるもの」（すなわち本号の対象外となるもの）の具体的な事例をご教示いただきたい。 (4)命令案第１条第１項第１号上の「経路の状況等に応じて」の「等」とは具体的にどのような場合を想定しているのかご教示いただきたい。	・(1)及び(2)について 動的・静的かによらず、電気通信信号を送信するに当たり、宛先に至る経路のうちから、経路の状況等に応じて最も適切と判断したものに電気通信信号を送信されている場合は経路制御がされていると解します。また、御指摘の「一般的なロードバランサー」において、「経路制御」が行われることは想定しておりません。 ・(3)について 例えば、物理的に別のＬ３スイッチ配下にある電子計算機や、物理的には同一のL3スイッチ配下にあるものの、別のVLAN上にある電子計算機が該当いたします。 ・(4)について 管理者が設定したルール等を想定しております。
11	命令案第１条第１項第３号に規定する「ファイアウォール等」について、以下の条件を全て満たす機器は対象外となるという理解で相違ないか。 (1) インターネット（公衆回線）への接続経路を持たないこと (2) 専用線または閉域網のみを使用していること (3) 社内システムに閉じたネットワーク上に配置されており、外部からの不正アクセスの経路となり得ないこと また、上記条件を満たす機器が特定重要設備に物理的に直接接続されている場合であっても、対象外という解釈でよいか。	御指摘の(1)から(3)までに該当する電子計算機であっても、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場合は対象です。
12	命令案第１条第１項第６号及び第２項第１号に規定する「アクセス制御機能を有する電子計算機」は、特定重要設備や特定重要電子計算機そのものへの管理者・オペレーターによるログインやシステムアクセスを制御する機能を有するものが対象であり、以下のものは対象外という認識で相違ないか。 (1) 一般の顧客・利用者がサービスを利用する際のID・パスワード認証、カード認証等のエンドユーザー向け認証機能 (2) 電子マネーサービスにおける残高照会・決済処理等のサービス機能に付随する認証処理 (3) 特定重要設備・特定重要電子計算機へのアクセス経路上に存在しない認証サーバー	・(1)及び(2)について 利用者向けか、認証に係る機能の種別によらず、他の特定重要電子計算機のアクセス制御機能を有するものは対象です。 ・(3)について 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おらず、かつ、本省令案第１条第２項第１号にも該当しない場合は、対象外です。
13	命令案第１条第１項第７号及び第２項第２号に規定する「アイ・ピー・アドレスを割り当てられた電気通信設備である電子計算機」は、外部（インターネット等）からの不正アクセスを制御することを主たる目的とした規定であると理解している。 この理解を前提とすると、以下の機器は対象外となる認識だが相違ないか。 (1) 内部ネットワークから外部ネットワークへの通信のみを制御し、外部からの着信を受け付けない機器 (2) インターネットに直接接続されておらず、専用線または閉域網のみに接続された機器であって、外部からの不正アクセスの経路となり得ないもの (3) グループ内プライベートクラウド環境内に配置され、インターネットとの接続点を持たない機器	御指摘の(1)から(3)までに該当する電子計算機であっても、グローバルIPアドレスを割り振られている場合は、対象です。
14	第一条第一号第七アイ・ピー・アドレスを割り当てられた電気通信設備である電子計算機 グローバルIPアドレスとした方が望ましいと思料します。	第１条第第１項第７号に規定するアイ・ピー・アドレスは、グローバルIPアドレスを指します。
15	（１）　省令案１条１項７号について 当該IPアドレスに係るホスト情報について、例えば管理用の環境、検証環境等実質的に非公開である場合や、公開されている期間がごく短い場合である場合等においても本号にするか。 （２）　省令案１条１項２号について 例えばACL等による通信制御によって論理的に一号電子計算機に電磁的記録が送信されない措置を講じている場合には、「電気通信信号を送信する」場合に該当しないと考えてよいか。	・（１）について 御指摘の場合でも、グローバルIPアドレスを割り当てられた電気通信設備である電子計算機に該当すれば、対象です。 ・（２）について ACL等による通信制御によって論理的に一号電子計算機に電磁的記録が送信されない措置が講じられている場合であっても、本省令案第１条第１項第２号の「電気通信信号を送信する」に該当いたします。
16	第一条に定められている重要電子計算機について、事業者間で届出対象に関する認識の齟齬が生じないよう配慮いただきたいと考えます。 あわせて、事業者が届出対応に向けた十分な準備期間を確保できるよう、施行前に本制度に関するガイドライン等を整備し、届出対象となる機器の範囲を具体例を交えて示していただくことを要望します。	御指摘を踏まえ、事業者間で認識の齟齬が生じないよう、第１条第２項第１号の電子計算機を「次号に規定する電子計算機に係るアクセス制御機能を有する電子計算機」に明確化しました。 また、該当する機器の具体例等を今後策定するガイドラインでお示しする予定です。
17	特定重要電子計算機について、具体的な製品・システムの該当事例を示した詳細なガイドラインや判断基準が今後策定される予定であるという認識で相違ないか。	御認識のとおりです。
18	第１条第１項第１号の内容は、「特定重要設備及び特定重要設備と同一のセグメントの機器」、第１条第１項第４号の内容は、「制御DMZに該当するセグメントの機器」が該当すると考えますが、特定重要設備が制御系システムの一部の場合と、情報系システムの一部の場合では対象となる範囲が大きく変わります。特定重要設備が制御系システムの一部の場合、情報系システムの一部となる場合のそれぞれの考え方について、解説資料等で具体的に解説いただきたく存じます。	頂いた御意見は、今後のガイドラインの策定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
19	ある会社の特定重要設備が同社のグループ会社内のプライベートクラウド環境に配置されており、物理的にはＬ３スイッチ配下で、特別社会基盤役務とは無関係な同社グループ内の他社（非特別社会基盤事業者）のサービスも混在している構成となっている場合、このような構成においては、命令案第１条第１項第１号及び第２号の規定をどのように解釈すべきか。物理的な接続構成を優先すべきか、あるいは、論理的な分離状況なども考慮すべきか、このケースにおける基本的な考え方をご教示いただきたい。	特定重要電子計算機は、法第２条第２項第２号に規定するとおり、特定社会基盤事業者が使用する電子計算機が対象です。また、電子計算機の範囲は、物理的な接続構成のみならず、本省令案第１条第１項第１号など、論理的な分離状況も踏まえ判断するものもございます。詳細は、今後策定するガイドラインをご確認ください。
20	特定重要設備（クラウドSaasサービス）のネットワーク構成図は、Saasサービスのフォルダ内に保存している。 この場合、ネットワーク構成図を保存する電子計算機として資産届出の対象とならない認識でよいでしょうか。 また、資産届出の対象は個社判断となりますでしょうか。または、各社届出の際に個別のヒアリング等があるのでしょうか。 資産届出を漏れなく対応したいと考えておりまして、判断箇所を教えていただけますと幸いです。	御指摘のサービスについて、インターネットを介して特定重要設備と接続している場合は、特定重要設備と公衆の用に供されている電気通信回線で接続されていることから本省令案第１条第１項第５号イには該当せず、資産届出の対象外です。 特別社会基盤事業者の使用する電子計算機のうち、いずれが本省令案等に規定する電子計算機に該当するかについては、今後策定するガイドライン等を踏まえ、特別社会基盤事業者において判断いただきたいと存じますが、疑義がございましたら御相談いただければと存じます。
21	特定重要設備およびその構成設備そのものがクラウドサービス、あるいはその他のサービス形態として特定社会基盤事業者に提供されている場合、第一条第一～七項の電子計算機は特定社会基盤事業者では把握しておらず、また、サービス提供者から特定社会基盤事業者を経由して届出する場合、特定社会基盤事業者の負荷が著しく高い上、セキュリティ上の機微情報の公開範囲を広げることにも繋がり、本法趣旨を鑑みた場合に本末転倒となる恐れがあることから、サービス提供者から直接届出を行わせる等の措置は必須と考える。 または、クラウド同様に特定重要電子計算機の製品名、製造者名はサービス提供者名を報告するものとしていただきたい。	法においては、資産届出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の上、提出いただければと存じます。 なお、特別社会基盤事業者以外の者が維持管理している特定重要電子計算機については、当該維持管理を行っている者の協力を得て届出を行う運用を検討しているところですが、あくまで特別社会基盤事業者において当該特定重要電子計算機を把握することを前提としております。
22	特定重要電子計算機を導入・変更した場合の届出については、対象範囲や詳細仕様をベンダーが把握している実態を踏まえ、事業者がベンダーから情報を収集した上で届出を行う方法に加え、事業者による確認を前提として、ベンダーから直接登録を行うことができる仕組みについてもご検討いただきたいと考えます。	法においては、資産届出の提出者はあくまで「特別社会基盤事業者」とされているため、あくまで特別社会基盤事業者において適切に提出すべき資産を確認いただくことが前提とはなりますが、その中で維持管理を行っている者の協力を得て届出を行う運用を検討してまいります。
23	・国産製品・サービスの活用促進と安全保障上の配慮について 本命令案はサイバー対処能力の向上を通じた国家安全保障の確保をも目的とするものであると理解しています。この性質を踏まえ、届出対象となる製品等について、国産品と非国産品とで取扱いに合理的な区別を設けることを、今後に向けた制度設計においてご検討ください。 例えば、電気通信事業法第27条の15等の規定においては、基幹的電気通信役務提供者に対し情報の保存場所や委託・再委託先の名称等の報告義務を課しており、データ主権やサプライチェーン・リスクの観点から安全保障上の配慮がなされていると承知しています。 本命令および今後の運用においても、同様の観点から、国内の法域内で開発・管理が完結している国産製品についてその信頼性を評価して届出要件の簡素化を検討いただく一方で、国外に拠点を持つ製品等について供給網やデータ管理の実態をより詳細に把握する枠組みを設けるなど、リスクベースでの差異化が考えられます。安全保障要件に基づく国内サイバーセキュリティ産業の育成と「トラステッド・コンポーネント」の確保を両立させる一助として政策的検討をお願いします。 併せて、実効性ある安全保障環境を構築するためには、単なる制度上の区別のみならず、海外製品に比肩しうる高度な機能を有する国産製品が継続的に提供される環境が不可欠です。現状、機能面等の理由から海外製品を選択せざるを得ない領域も存在することを踏まえ、安全保障要件をも満たす国産セキュリティ製品の社会実装拡大に向けた、官民一体での研究開発支援や投資の呼び込みについて、更に強力に推進いただくことを期待いたします。	資産届出は、特別社会基盤事業者に対して、脆弱性情報等の被害の防止のために効果的な情報を提供することその他政府による必要な対応を実施するために行うものであり、国産品であることをもって取扱いに差異をつける考えや資産届出において御指摘の供給網やデータ管理を把握する考えはありません。 その他、頂いた御意見は、今後の参考といたします。
第２条（特定重要電子計算機の届出）　関係		
24	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は、適時アップデートが行われることが一般的であり、変更の都度、届出を要する運用となれば、手続が著しく煩雑となることも懸念されます。内閣府におかれては、詳細な要件を画一的に定めるのではなく、各事業の監督官庁と事業者からの意見も十分に踏まえながら、実態に即した柔軟な運用ガイドラインを整備いただくことを要望します。	ガイドラインついては、特別社会基盤事業者の皆様と密に意見交換を実施しながら、また、特別社会基盤事業者の負担にもよく留意しつつ、実態に即したものとなるよう、策定を進めてまいります。
25	2条に「次に掲げる特定重要電子計算機」として特定重要電子計算機に組み込まれたOS等とあるが、特定重要電子計算機に包含される特定重要電子計算機という概念があるのか。	法第２条第２項において、同項第２号の電子計算機に組み込まれたプログラムも重要電子計算機の対象としており、特定重要電子計算機に組み込まれたプログラムも特定重要電子計算機の対象です。

No.	御意見の要旨	御意見に対する主な考え方
26	本法律の運用開始の前に導入されている特定電子計算機も届出の対象という認識であるが、例えば、２０年前に導入して現在も使用している製品も届出の対象か。 既に市場に出している製品について、事業者がサイバー対処能力強化法に基づき政府に届け出た機器については、何を届け出たのかベンダーが認知する、事業者が電子計算機等のベンダーに通知を義務付けてほしい。 なぜなら、サイバー対処能力強化法において、新たに脆弱性対応が電子計算機等のベンダーに対して求められるため、何が届けられて対象となっているのか把握しておく必要があるため。 アプライアンスＨＷの具体的な事例は、業界別のガイド等に示されるか。	御指摘の20年前に導入して現在も使用している製品も届出の対象です。御指摘の通知については、法において義務付けられておりませんが、頂いた御意見は、今後の制度の運用における参考といたします。アプライアンスの考え方については、今後策定するガイドラインでお示ししたいと考えております。
27	・システム廃止に伴う資産届出の判断が付きづらい為、法施行前後で分けて示して頂きたい ・事業者側でミドルウェアの対象が判断付きにくいため、予め製品シェア等から届出製品の選択肢を示す方法を検討願う	法施行前に特定重要電子計算機を使用しなくなった場合は、当該特定重要電子計算機については届出不要です。法施行後に特定重要電子計算機を使用しなくなった場合は、法第４条第３項の変更の届出（以下「変更届出」といいます。）の対象であると解します。 その他、頂いた御意見は、今後の制度の運用における参考といたします。
28	命令案第２条第１項ただし書きに規定する「当該特定重要電子計算機が一の特別社会基盤事業者若しくは複数の特別社会基盤事業者のうち、親法人等（略）が同一であるもの若しくは一方の者が他方の者の親法人等であるものの事業の用に供されるもの」の定義について、以下の点をご教示いただきたい。 (1) 特定の事業者のために個別にオーダーメイドで設計・製造された設備・システムを指し、市場に広く流通している汎用のOS・ミドルウェア・ハードウェアを組み合わせて構築されたシステムは、該当するという理解で相違ないか。または、たとえ特定事業者のみが利用する環境であっても該当しないという理解となるか。 (2) グループ会社内の複数の事業者（特別社会基盤事業者である当社を含む）が共同利用するプライベートクラウド環境を使用しており、当該環境は汎用のOS・ミドルウェアを使用して構築されている。このような環境は、該当するか。または、該当せず、したがって本ただし書きの適用対象外（すなわち届出義務あり）という理解となるか。また、仮に届出義務がある場合、届出の単位（物理サーバー単位か、論理サービス単位か等）についてご教示いただきたい。 (3) プライベートクラウド環境において、特別社会基盤事業者のサービスと非特別社会基盤事業者のサービスが論理的に分離されて混在している場合、届出の対象となるのは特別社会基盤事業者のサービスに係る論理的な範囲のみと解してよいか。	・(1)について 御指摘の箇所は、OS・ミドルウェア・ハードウェア等の単位で、一の特別社会基盤事業者等の事業の用に供されるものを資産届出の対象外とするものです。市場に広く流通しているOS・ミドルウェア・ハードウェア等で構成されたシステムは届出の対象です。 ・(2)について 資産届出の対象です。届出の単位は、アプライアンス製品を除き、OS・ミドルウェア・ハードウェア等の単位で届出いただければと存じますが、これらが「クラウド・コンピューティング・サービス」に該当する場合は、当該クラウド・コンピューティング・サービスの名称等を届出いただく必要があります。 ・(3)について 御指摘のとおりです。
29	複数の特定社会基盤事業者のうち、議決権をベースとした親子関係のある複数の特定社会基盤事業者の場合は専用設計品として届出の対象外とあるが、ある特定社会基盤事業者が独自に構築した特定重要電子計算機を受委託契約により他の特定社会基盤事業者が利用するケースも存在。当該独自構築の特定重要電子計算機については、委託先で管理・運用されており、脆弱性情報提供という目的を踏まえると委託元への情報提供は必要ないと思われるため、受委託契約により複数の特定社会基盤事業者が利用するケースについても専用設計品として届出対象外として頂きたい	御指摘の場合は一の特定社会基盤事業者と同視できる者ではないことから、届出対象外として規定しておりません。
30	ある会社が、VPN機器や認証基盤について、特別社会基盤事業者である同社を含む同社グループ全体で共有している構成を採用している。このような共有環境下において、当該機器を「特定重要電子計算機」として取り扱うにあたり、どのような基本的な考え方で届出や管理を行うべきか、ご教示いただきたい。 特に、グループ環境下での適用イメージについて、伺いたい。	御指摘の機器等を共有する特別社会基盤事業者全てにおいて、資産届出を行う必要がありますが、届出にあたっては、特別社会基盤事業者の負担にもよく留意しつつ、運用してまいります。なお、当該機器等が当該グループ内のみの事業の用に供されるものである場合には、第２条第１項但書に基づき届出が不要になる場合があります。
31	該当条項は運用上の便宜を図る趣旨のものとして意義があるものと考えます。一方、より実行性を上げるために、届出例外とする「広く一般に使用されているもの」について、事業者、業態の特性を踏まえて具体的な事例の提示をお願いしたく存じます。 ※命令案抜粋 （略）ただし、当該特定重要電子計算機が一の特別社会基盤事業者若しくは複数の特別社会基盤事業者のうち、親法人等（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施行令（令和四年政令第三百九十四号）第十条第三項に規定する親法人等をいう。以下この項において同じ。）が同一であるもの若しくは一方の者が他方の者の親法人等であるものの事業の用に供されるものである場合又は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である場合は、この限りでない。	御指摘の「広く一般に使用されているもの」の具体的な対象については、今後別途お示しいたしますが、業態・事業者問わず広く一般に使用されているものを想定しております。
32	命令案第２条第１項ただし書きに規定する「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、以下の点をご教示いただきたい。 (1) 指定の具体的な選定基準（例：市場シェア、普及台数、業界標準規格への準拠等）はどのようなものか。 (2) 事業者が自社の使用製品について「広く一般に使用されているもの」に該当するか否かを事前に確認できる手続き（事前照会制度等）を設ける予定はあるか。 特に(2)について、事業者が届出義務の有無を適切に判断するためには、施行前に確認できる仕組みが不可欠と考えるが、いかがか。	御指摘の「広く一般に使用されているもの」の具体的な対象については、今後別途お示しする予定です。

No.	御意見の要旨	御意見に対する主な考え方
33	特定重要電子計算機の届出において、特定社会基盤事業者以外の者が維持管理し、複数の特定社会基盤事業者が利用している特定重要計算機について、同一の内容を複数の特定社会基盤事業者から届出を行う必要性はないことから、下記の基本方針の記載も踏まえて、当該維持管理を行っている事業者から直接届出を行う事も可能として頂きたい 〇基本方針第4章第2節（1） また、特定重要電子計算機の届出を求めるに当たっては、特別社会基盤事業者の負担にも配慮する。例えば、機器更新等により特定重要電子計算機の届出情報に変更があった場合に特別社会基盤事業者に求める対応や、特別社会基盤事業者自らが直接管理していない特定重要電子計算機に係る届出については、その特別社会基盤事業者の対応に係る負担の大きさにもよく留意しつつ、実情に応じた合理的な制度設計・運用となるよう努めることとする	法においては、資産届出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の上、提出いただければと存じます。 なお、特別社会基盤事業者以外の者が維持管理している特定重要電子計算機については、当該維持管理を行っている者の協力を得て届出を行う運用を検討しているところですが、あくまで特別社会基盤事業者において当該特定重要電子計算機を把握いただくことを前提としております。
34	【依頼】 特定重要電子計算機の届出運用は、システム構成によっては対象となる機器が膨大に存在し、負荷が非常に高くなる場合があると想定されます。機器グルーピングを許容いただく等、負荷を考慮した運用を検討いただけますでしょうか。	同一の製品名の製品については、重ねて記載することを不要とするなど、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、運用してまいります。
35	本政省令（案）における特定重要電子計算機の届出に関し、届出対象が多く、機器の詳細仕様の把握が必要となるため、ベンダーの協力が必要不可欠だと考えております。そういった中で、各ベンダーに対してヒアリングを実施しており、一部ベンダーからは対応可能との回答をいただいております。一方で、対応可否が判明していないベンダーも存在しており、必ずしも一律に準備が整っている状況とは言えません。このような実態を踏まえ、今後のガイドラインや説明会等において、ベンダーに対して基盤インフラ事業者への協力を促すようなご対応をお願いできればと思います。	頂いた御意見は、今後のガイドラインの策定等における参考といたします。
36	2条4項5項3条3項　経済安全法とは法律も目的も違う中で、なぜ届出書の流用が認められるのですか。 経済安全法は社員の国籍等のセンシティブ情報が届出書面に記載されていて、そのような情報が経済安全法の担当職員以外に伝わるのは適切ではないため、反対です。個人情報やプライバシーとの関係で問題はないのでしょうか。	第２条第４項等は、特別社会基盤事業者の負担の軽減の観点から、法と経済安全保障推進法とで制度の趣旨や対象となる機器の範囲、提出書類の記載の粒度等が異なることを前提としつつ、経済安全保障推進法第50条第１項に基づく導入等計画書等のうち一定の要件を満たすものを法に基づく届出書として扱うことができるとするものです。特別社会基盤事業者において、そのような取扱いを希望しない場合には、通常どおり、本省令案様式第１による届出書を提出いただければと存じます。
37	「経済安全保障推進法に基づく届出がある場合に特定重要電子計算機の届出を代替できる」趣旨は運用上の便宜を図るものであり、事業者の実務負荷等を勘案いただいたものと認識しております。 一方で、実際に作業する際は「対象となる特定重要電子計算機の洗い出し」を行ったうえで、「経済安全保障推進法における特定重要設備として届出を行っているものを省く」というプロセスも考えられ、その場合は却って実務負荷が増すこととなります。 こうした中、命令案では「当該特定重要電子計算機に係る第一項の規定による届出書の提出に代えることができる。」と規定されているため、当該届出代替を用いるかどうかは事業者が判断でき、用いない場合は経済安全保障推進法における特定重要設備として届出を行っているものも含めた全量版の特定重要電子計算機を対象としてもよいという理解でよろしいでしょうか（特定重要電子計算機をより網羅的に届け出ることは法の趣旨にも合致するものと思料）。 ※命令案抜粋 特定重要設備又は構成設備（略）である特定重要電子計算機に係る第一項の届出書については、経済安全保障推進法第五十二条第一項又は第十一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（略）には、当該届出に係る同条第一項に規定する導入等計画書（略）又は同条第十一項に規定する緊急導入等届出書（略）及び特別社会基盤事業者の連絡先を記載した書面の提出をもって、当該特定重要電子計算機に係る第一項の規定による届出書の提出に代えることができる。	御理解のとおりです。
38	第2条第4項等において、経済安全保障推進法に基づく届出書の提出をもって本法における届出に代えることができるとされている点については、事業者の事務負担の軽減に資する措置として、一定の合理性があるものと受け止めております。 他方、経済安全保障推進法と本法は、その設置主旨や申請基準等が異なることから、共同運用されることで申請・審査基準が厳格な方に一律に合わせられ、事業者負担が増大することが想定されます。制度化・運用にあたっては、事業者に過度な負担が生じぬよう両法の主旨に照らして合理性のある適切な運用がなされることを要望します。	第２条第４項等は、法と経済安全保障推進法とで制度の趣旨や対象となる機器の範囲、提出書類の記載の粒度等が異なることを前提としつつ、経済安全保障推進法第50条第１項に基づく導入等計画書等のうち一定の要件を満たすものを法に基づく届出書として扱うことができるとするものであり、御指摘のように、法と経済安全保障推進法のうち厳格な方に運用を合わせるものではありません。 その上で、頂いた御意見は、今後の制度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
39	命令案第２条第２項から第４項に規定する届出方法の特例について、以下の点をご教示いただきたい。 (1)「経済安全保障推進法の規定による届出書のうち一定のもの等をもって代えることができる」とあるが、代替可能な届出書の具体的な種類・様式があればご教示いただきたい。 (2) 代替可能な場合、本命令案の様式第一による届出書の提出は不要となるという理解でよいか。また、代替届出書に本命令案固有の記載事項（特定重要電子計算機の区分等）が含まれていない場合の取扱いはどうなるか。 (3) 経済安全保障推進法に基づく届出と本命令案に基づく届出を一本化・統合して提出できる仕組みを整備する予定はあるか。事業者の届出負担軽減の観点から、可能な限り一本化を図っていただきたい。	・(1)について 経済安全保障推進法第52条第１項に規定する導入等計画書又は同条第11項に規定する緊急導入等届出書（いずれも経済安全保障推進法の規定による変更をしたときは、その変更後のもの。また、これらの計画書等に記載した特定重要設備又は構成設備（特定重要設備の一部を構成する設備、機器、装置又はプログラムであって、経済安全保障推進法第52条第２項第２号ハに規定する特定妨害行為の手段として使用されるおそれがあるものをいいます。以下同じ。）の名称が資産届出すべき特定重要電子計算機の製品名と同一であり、かつ、当該特定重要設備又は構成設備の供給者の名称又は氏名が当該特定重要電子計算機の製造者名と同一である場合に限る。）及び特別社会基盤事業者の連絡先を記載した書面です。 ・(2)について 第２条第４項による代替措置が行われた場合には、様式第１による届出書の提出は不要です。特定重要電子計算機の区分については、本特例の対象となる電子計算機は、令第１条第３項第１号の電子計算機であることが自明であるため、別途記載いただく必要はありません。いずれにせよ、具体の手続については、今後策定するガイドライン等で御案内いたします。 ・(3)について 頂いた御意見は、今後の制度の運用における参考といたします。
40	省令第2条（特定重要電子計算機の届出）第4項について、「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、導入等計画書及び特別社会基盤事業者の連絡先を記載した書面の提出をもって、届出書の提出に代えることができる」とありますが、「特別社会基盤事業者の連絡先を記載した書面」というのは、様式第一の１のみを記載して提出するということでしょうか。	様式第１の１．の「連絡先」に相当する内容を記載した書面を提出いただければと存じます。
41	2条4項に変更をしたときは変更後のものとあるが、変更を反映した届出書を新たに作るということか。	変更を反映した届出書が提出されていない場合には、経済安全保障推進法第52条第１項に規定する導入等計画書又は同条第11項に規定する緊急導入等届出書及び当該変更に係る届出書等を提出いただく運用を想定しております。
42	経済安保法の導入届出を行った場合、導入等計画書・緊急導入等届出書の書面をもって当該特定重要電子計算機の届出書の提出に代えることができる旨の記載あるが、再度の届出書提出も事業者負担となり不要と整理願いたい	頂いた御意見は、今後の制度の運用における参考といたします。
43	【意見内容】 特定重要電子計算機の届出事項である「製品名」について、詳細な型番等ではなく、シリーズ名や概括的な製品名称といった、機器を過度に特定しない粒度での記載とさせていただきたい。 【理由】 1. セキュリティリスク増大防止 具体的機器名を外部システムへ提出・集約させることは、万一情報が漏えいした場合のセキュリティリスクが高いため。 2. 変更届出の頻発防止 届出の粒度が詳細すぎる場合、マイナーな機器更新やパッチ適用のたびに変更届出が必要となり、運用が煩雑となるため。 3. 概括的な名称であても制度目的（脆弱性対応）は達成可能なため 脆弱性情報の早期共有と注意喚起という目的は、詳細な型番まで把握せずとも、シリーズ名や概括的な製品名称が登録されていれば、該当事業者への連絡や、対応を促すことは可能なため。	「製品名」については、使用されている製品の種類を一意に特定するための型番等を記載いただきます。詳細は、今後策定するガイドラインでお示しいたします。
44	・クラウドサービスにおいて詳細の機器情報を聴取しないのは、機器の脆弱性起因でサイバー攻撃を受けた時に、責任分解モデルにおいて事業者（クラウド利用者）は責任を伴わないという考え方に依るものか ・クレジットカード会社システムは、PCIDSS（※）のセキュリティ国際基準を準拠しており、その認定をもって安全性を確保していると見做すことができ、本法案に伴う資産届出対象外と整理できないか。 資産情報の定期届出に関する業務負荷の増加や、届出した資産情報の外部流出に伴うサイバー攻撃被害を懸念 ※PCIDSS要件5にてアンチウィルスソフトの利用、要件6にて脆弱性への対応を規定	クラウドサービスにおいては、利用者が機器情報の詳細を把握できない場合が多く、制度の実効性を確保することが困難と考えられるため、製品名等ではなく当該クラウドサービスの名称を記載いただくこととしております。 御指摘の国際基準その他の認定を受けた電子計算機であっても、資産届出いただくことは、特別社会基盤事業者に対して、脆弱性情報等の被害の防止のために効果的な情報を提供することその他政府による必要な対応を実施するために必要であるため、当該認定を受けたことをもって資産届出の対象外とする考えはありません。
第３条（変更の届出）　関係		

No.	御意見の要旨	御意見に対する主な考え方
45	経済安保法（以下、旧法）における「特定重要設備」とサイバー対処能力強化法　（以下、新法）の「特定重要電子計算機」の重複定義に関する運用方針について、当局のご意向や運用上の柔軟性についてご教示いただけますでしょうか。 「特定重要設備」として届け出ている機器の一部が、新法の「特定重要電子計算機」にも該当し、同一機器を両法に個別に登録した場合、以下の通り「変更届出」の要件が異なるため、実務上の不整合や管理ミス（届出漏れ）を懸念しております。 タイミングの差：　旧法は「事前審査」、新法は「事後4ヶ月以内の届出」であり、同一の製品変更に対して異なるタイムラインでの管理が求められる。 変更範囲の差：　片方の法律では「軽微な変更」とみなされる内容が、他方では「要届出」となる可能性があり、現場の判断に混乱が生じる。	御指摘のタイミングの差については、経済安全保障推進法に基づく届出書類のうち一定の要件を満たすものを法第４条第３項に基づく届出書類としても取り扱うなど、御指摘の管理における負担も踏まえた運用を行ってまいります。 変更範囲の差については、経済安全保障推進法上軽微な変更とされている事項であって、変更届出の対象となる事項はございません。他方、本省令案第３条第４項において軽微な変更として変更届出を不要としている特別社会基盤事業者の名称の変更については、経済安全保障推進法第50条第３項に基づく届出の対象です。これは、特定社会基盤事業者の名称の変更は、同条第２項の規定に基づき公示されるため、事業者の届出負担の軽減の観点から、変更届出は不要としたものです。その上で、御指摘の現場の混乱が生じないよう、今後とも制度の周知を図ってまいります。
46	命令案第３条第４項において、特別社会基盤事業者の名称の変更が軽微な変更として届出不要とされているが、これ以外に届出不要となる事項について、以下の点をご教示いただきたい。 (1) 以下の変更は届出不要な軽微な変更に該当するか。 特定重要電子計算機のOSやミドルウェアのマイナーバージョンアップ（セキュリティパッチ適用を含む） クラウドサービスの利用プランの変更（機能・性能の変更を伴わないもの） 特定重要電子計算機の物理的な設置場所の変更（同一データセンター内での移設等） 特定重要電子計算機の冗長構成の変更（台数の増減等） (2) セキュリティパッチの迅速な適用を促進する観点から、セキュリティ対応に係るバージョンアップについては届出不要とする、または事後報告で足りるとする取扱いを検討いただきたい。	変更届出は、本省令案第２条第５項の規定により届け出た事項（製品名、製造者名等）であって、特別社会基盤事業者の名称以外の事項に変更があった場合に届け出るものです。届出事項の詳細は、今後策定するガイドラインでお示しいたします。なお、資産届出も変更届出もいずれも事後の届出です。
47	「軽微な変更」を除き変更の届出が必要となっており、「軽微な変更」とは特別社会基盤事業者の名称変更のみとされています。 この整理でいくと、特定重要電子計算機に対してセキュリティーパッチ適用（セキュリティ向上による変更）、部位故障による部品取替え（メンテナンスによる変更）、設定値変更や機能変更（運用上の変更）、すべてにおいて変更の届出が必要になると読み取れます。 これらの対応は、サイバーセキュリティ及び設備の安定運用を維持・向上させるために日常的に実施されるものであり、すべてを変更届出の対象とすることは事業者の実務負担が過度となるおそれがあります。 変更届出が必要となる範囲について、実務上の考え方をガイドライン等で明確化していただきたいと考えます。	変更届出は、本省令案第２条第５項の規定により届け出た事項（製品名、製造者名等）であって、特別社会基盤事業者の名称以外の事項に変更があった場合に届け出るものです。その上で、いただいた御意見については、今後のガイドラインの策定等における参考といたします。
48	第三条の規定に従い、特定社会基盤事業者が自らの特定重要電子計算機（の導入）、及びそれに係る特定重要設備等について変更があった場合に関しそれぞれ報告義務があるとのことだが（様式第一、様式第二）、例えば特定社会基盤事業者に対して、特定重要電子計算機（クラウド等のサービス）を提供する事業者において、技術的に軽微な変更があった場合（例えば、セキュリティのアップデートやパッチの適用）についても、特定社会基盤事業者はその変更について政府に報告する義務を有するかご教示願いたい（当該パッチ等について事前通知が特定重要電子計算機提供事業者から必要となった場合、同事業者の負担が高まるだけでなく、運用の速度や高セキュリティ体制の確保にも悪影響を与える可能性がある）。	変更届出は、本省令案第２条第５項の規定により届け出た事項（クラウドサービスの場合は、クラウドサービスの名称、提供事業者名等）に変更があった場合に届け出るものです。御指摘のセキュリティパッチ適用等であって、当該事項に変更がない場合には、届出の必要はありません。
49	第二条４項の導入届出同様に、事業者負担観点から経済安保法上で提出した際は改めての届出は不要として頂きたい	頂いた御意見は、今後の制度の運用における参考といたします。
第４条（特定侵害事象等の報告）　関係		
50	施行規則第４条第１項に規定されている報告を要する「特定侵害事象等」について、ガイドラインや運用の中で、可能な限り、対象範囲を明確にしていただくことを要望いたします。	頂いた御意見は、今後のガイドラインの策定や制度の運用における参考といたします。
51	関係府省の法令整備が進むことで、サイバーセキュリティの能力が強化されていくものと認識しており、弊社としても、これまでの知見を活かして積極的に寄与していく所存です。 特定侵害事象等の報告については、官民の情報共有のかなめになるものと認識しているところ、報告の対象となる事象がどのような状況になった際に報告が必要になるか、具体的に示されるのでしょうか。 例えば、特定重要設備を構成する特定重要電子計算機に攻撃者のアクセスが到達してきた場合、インフラ事業の根幹の部分が侵害されるリスクは非常に高いと考えられ、かつ、サイバーセキュリティ対策に資する情報なので、報告すべきと考えられます。しかしながら、基幹インフラ事業者にとって根幹の業務停止や縮退運転などの実害がない場合、正常と判断され報告しないことも考えられます。 基幹インフラ事業者にとって判断しやすい、運用に係る解釈やガイドラインなどが必要になるものと考えます。ガイドライン等が作成される場合は、運用上の支障を積極的に回避する上でも、逐次情報共有を頂けると幸甚でございます。	同上

No.	御意見の要旨	御意見に対する主な考え方
52	「アクセス制御機能を有する特定重要電子計算機」 「当該アクセス制御機能に係る他人の識別符号」 とあるが、ID,PWでログインする機能をもてば、アクセス制御機能を有する特定重要電子計算機という解釈か。仮にその機能を無効化すれば、アクセス制御機能は持たない電子計算機という理解か。	御理解のとおりです。
53	条文ではイ～ニ（不正アクセス禁止法の文言を流用している模様）の事象とホ（その痕跡）いうことですが、そもそもこれらの事象（とその痕跡）を把握することが十分にできない対象システムについてはどのように解釈すればよいのか。 検知するために、能動的な対応（検知するためにセキュリティ監視の仕組み、SOCの導入を要求が求められるのか。また、検知できない場合は、報告する必要はないのか。 「イ　正当な理由がないのに、特定重要電子計算機に対し、特別社会基盤事業者が当該特定重要電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録を受信させる行為が行われる事象」については、人による不正行為や過失によるMalware感染が対象となると理解してよいか。具体事例を示していただきたい。 「ハ　当該アクセス制御機能による特定利用」とは、どのような制限が特定利用になるのか具体例は今後ガイド等で提示されるという理解でよいか。 「ニ　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」のとはどのようなものを指すのか具体的な事例は今後ガイド等で提示されるか 条文第四条３．五　特定侵害事象等に関する技術的な事項　については、具体的にどのような内容を報告するのか、今後ガイド等で提示されるか。 サイバー対処能力強化法で新たに求められる特定侵害事象等の報告については、事業者やベンダーは対応のための費用負担が発生することになるので、政府としての財政面での支援策も検討して頂きたい。法令対応として中小企業など立場が弱いベンダーが一方的に費用負担することになる恐れもあることから配慮いただきたい。	御指摘のようなセキュリティ監視の仕組み等を整備することが一般的には望ましいですが、法第５条に基づく報告（以下「インシデント報告」といいます。）においては、検知せず、認知しなかった事象については、報告を求めるものではありません。 第４条第１項第１号イの具体例は、人が故意により特定重要電子計算機にマルウェアを受信させた場合が対象となります。第４条第１項第１号ハ及びニの具体例については、今後策定するガイドラインでお示しする予定です。御指摘の報告内容については、今後制定する告示及び様式でお示しいたします。 また、個々の事業者の対応に要する費用を支援することは困難ですが、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、運用を進めてまいるとともに、資産届出等が円滑に行われるよう、特別社会基盤事業者からの相談等に適切に対応してまいります。
54	第４条第１項第１号イ～ニ 同号ホと同様、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に限定すべき。即ち、サイバーセキュリティを害され、外部からの侵入によってなされるものに限り、特別社会基盤事業者の従業者等の内部による行為は報告の該当外とするのが望ましいと思料。	第４条第１項第５号ロにおいて、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に限定している趣旨は、サイバーセキュリティ対策では防げないような物理的な手段により他人の識別符号を窃取する行為を対象外とするためであり、御指摘の内部による行為を報告の該当外とするものではありません。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に限定する規定の有無にかかわらず、御指摘の内部による行為も報告の対象です。
55	以下事象の具体的な事例をお示しいただきたく存じます。 ※命令案抜粋 電気通信回線で直接又は間接に接続されている他の特定重要電子計算機が有するアクセス制御機能によりその特定利用を制限されている電子計算機に対し、電気通信回線を通じてそ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	例えば、特定重要電子計算機が他の電子計算機の認証を行っている場合に、当該認証に係る脆弱性を衝くような特殊な情報又は指令が当該他の電子計算機に入力される事象が該当いたします。
56	以下「痕跡が記録される事象」について、解説資料等で具体的に解説いただきたく存じます。 ※命令案抜粋 特定侵害事象又はイからホまでに掲げる事象の痕跡が記録される事象 前号に掲げる特定重要電子計算機以外の特定重要電子計算機特定侵害事象の痕跡が記録される事象	頂いた御意見は、今後のガイドラインの策定における参考といたします。
57	当報告では痕跡が記録された事象を報告するようになりますが、その中には技術的な事項等を報告するようになっています。 事業者としては、弱点や脅威を開示することにより更なる脅威の拡大は許容できません。 どこまでの報告が必要なのかを具体的化していただくとともに、当該情報の報告フロー、政府内での取扱い、共有範囲、保存期間を整理いただくとともに、報告者の保護を配慮いただいた内容をガイドライン等で明確化していただきたいと考えます。	報告内容の詳細については、今後制定する告示及び様式でお示しいたします。報告先は、事業所管省庁及び内閣府となりますが、具体については今後ご案内いたします。 また、ご指摘のとおり、報告いただいたことによりかえって事業者が脅威にさらされることはあってはならないと考えており、報告いただいた情報については、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。その他、頂いた御意見は、今後の制度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
58	命令案第４条に規定する特定侵害事象等の報告について、以下の点をご教示いただきたい。 (1)「発生を認知した後、速やかに」の「速やかに」の具体的な目安（時間・日数）はどの程度か。他法令（例：個人情報保護法における速報義務の「3～5日以内」等）との整合性も踏まえてご教示いただきたい。 (2)「認知」とは具体的にどのような状態を指すか。以下のいずれの時点が「認知」に該当するか。 セキュリティ監視システムがアラートを検知した時点 担当者がアラートを確認した時点 担当者が特定侵害事象等に該当すると判断した時点 経営層・責任者が報告を受けた時点 (3) 初動報告（速やかな報告）と30日以内の詳細報告の記載内容の違いについてご教示いただきたい。特に、初動報告の段階で判明していない事項については記載不要という理解でよいか。 (4) 特定侵害事象等が発生したシステムがクラウドサービス上にある場合、クラウドサービスプロバイダーからの通知を受けた時点が「認知」となるという理解でよいか。	・(1)・(2)について 今後策定するガイドラインにおいてお示ししたいと考えております。 ・(3)について 御理解の点が違いとなります。 ・(4)について 御理解のとおりです。
59	以下のとおり「刑法（明治四十年法律第四十五号）第二百三十四条の二第二項の罪に当たる行為」（未遂）の場合はインシデント報告対象外と読み取れますが、当該記載に関する具体的な想定をご教示いただきたく存じます。 ※命令案抜粋 特定重要電子計算機（一号電子計算機並びに第一条第一項第一号及び第二号に規定するものを除く。）に対する法第二条第四項第三号に該当する行為（刑法（明治四十年法律第四十五号）第二百三十四条の二第二項の罪に当たる行為に係るものに限る。）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事象（他の特定不正行為（法第二条第四項に規定する特定不正行為をいう。）に係る事象又は当該事象の痕跡が記録される事象に該当するものを除く。）	具体的な事例としては、DDoS攻撃があったものの、特定重要電子計算機の動作が阻害されることがなく、また、不正アクセスやマルウェアの実行もない場合が報告対象外となります。
60	・重要インフラのサイバーセキュリティに係る行動計画に基づく各省からの連絡フローと新法における報告フローの整合について、新法上の報告書を提出した場合は、事業社側の負荷軽減として重要インフラ行動計画に基づくサイバーセキュリティ事案の報告を兼ねるものとしていただきたい。	頂いた御意見は、今後の制度の運用における参考といたします。
61	特定重要電子計算機に対する特定侵害事象等の報告について、特定社会基盤事業者以外の者が維持管理し、複数の特定社会基盤事業者が利用している特定重要計算機で発生した特定侵害事象について、同一の内容を複数の特定社会基盤事業者から届出を行う必要性はないことから、下記の基本方針の記載も踏まえて、当該維持管理を行っている事業者から直接届出を行う事も可能として頂きたい	特別社会基盤事業者以外の者が維持管理している特定重要電子計算機については、あくまで各特別社会基盤事業者において特定侵害事象等に係る情報を把握することを前提に、当該維持管理を行っている者の協力を得て届出を行う運用を検討しているところです。
62	複数の特定社会基盤事業者が共通して使用している特定重要設備について、インシデント報告事案が発生した場合、複数の特定社会基盤事業者から重複した報告を避けるため以下2点についてご検討をお願いしたい。 ・特定社会基盤事業者が所有している自社設備を他の特定社会基盤事業者が使用しいてるケースにおいて、その設備を所有している基盤事業者がインシデント報告をおこなうことにより他の事業者の報告を不要としていただきたい。 ・外部事業者が所有している特定重要設備を特定社会基盤事業者が使用している場合、その特定重要設備の供給者からのインシデント報告を可能としていただきたい。	特別社会基盤事業者が使用している電子計算機を他の特別社会基盤事業者も使用している場合においては、当該他の特別社会基盤事業者も報告が必要ですが、報告にあたっては、特別社会基盤事業者の負担にもよく留意しつつ、運用してまいります。 特別社会基盤事業者以外の者が維持管理している特定重要電子計算機については、あくまで各特別社会基盤事業者において特定侵害事象等に係る情報を把握することを前提に、当該維持管理を行っている者の協力を得て届出を行う運用を検討しているところです。
63	特定侵害事象等の発生を認知した後の「速やかな報告」については、実務上、事業者におけるインシデント対応（被害拡大防止、放送の継続及び復旧）を最優先とすることが重要であると考えます。 このため、第一報の段階では、発生の事実、影響の概要、当面の対応状況等の基礎的かつ必要最低限の情報で足りることとし、原因の特定、侵入経路の分析、影響範囲の確定等の詳細については、調査が進み次第、続報として順次報告することが認められる取扱いとしていただくことを要望いたします。	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。
64	運用面での要望となるが、インシデント報告に関し、法令上問題なく報告できる体制を構築・維持する観点から、政府主催の訓練（※）で簡易に定期的に確認できる機会を設定することをお願いしたい。(※訓練は既に多くの重要インフラ事業者の参加実績がある全分野一斉演習など既存の訓練の場で活用することが望ましい)。 これにより担当替えに伴い正しいインシデント報告ができなくなるリスクを低減させるなど、政府および重要インフラ事業者双方にメリットがあると考える。	頂いた御意見は、今後の制度の運用における参考といたします。
65	インシデント発生時の負担軽減の観点から、令和8年5月28日の「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」に基づき、報告様式の共通化や窓口の一元化に向けて取り組むことをお願いしたい。	インシデント報告の様式については、「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）で定める共通様式とする予定です。また、報告窓口の一元化についても、所要の調整を進めてまいります。

No.	御意見の要旨	御意見に対する主な考え方
66	保険会社においては、別途法令に基づき「障害発生等報告書（保険会社向けの総合的な監督指針別紙様式集II－３－１４（１））」を提出しています。 事業者の事務負荷軽減の観点から、「障害発生等報告書」による報告と本法における報告について、同一フォーマット（紙面）や同一画面（システム）での報告が可能となるよう、ご検討いただきたく存じます。 そのうえで、障害発生等報告書による報告と本法における報告の関係性について、解説資料等において明確にしていただきたく存じます。例えば、第４条第２項第１号、第２号又は第３号の規定に該当する事案について、本法における報告は不要と理解しておりますが、「障害発生等報告書」による報告が必要なケースはあると思われます。複数の法令等に基づく対応が求められることで報告漏れが発生する懸念もあることから、セキュリティインシデントの内容に応じどのような対応が求められるかについて、統一的にわかりやすく示していただけると非常にありがたく存じます。	頂いた御意見は、今後の制度の運用における参考といたします。
67	報道機関である基幹放送事業者が「特別社会基盤事業者」に指定されているところ、本命令案４条によって定義された特定侵害事象の報告が一律に義務付けられることにより、憲法２１条や放送法３条で保障される報道の自由や放送番組編集の自由が制約される懸念があります。従って、本命令案４条について、報道機関である基幹放送事業者が報道目的で取得した情報については、「特定侵害事象等の概要」（４条３項３号）や「その他特記事項」（同７号）に該当し得る場合を含め、報告対象とならないことを、何らかの方法で明確にしていただきたいと考えます。 このことは、今後設置される「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）にも関係します。すなわち、特別社会基盤事業者である基幹放送事業者が、協議会の構成員となった場合、報告義務（同条５項）や守秘義務（同条７項）が課されることになります。しかし、現在のところ、報道目的で取得した情報が報告義務の適用除外になるのかや、協議会で提供された情報と同一あるいは関連する情報を取材により独自に取得した場合にこれを報じても守秘義務違反に問われないのかなど、報道の自由への配慮がどこまでなされるのかについて、明らかにされていません。 サイバー対策能力強化法の制度趣旨については、賛同するところではありますが、報道機関である基幹放送事業者を特別社会基盤事業者に指定するのであれば、それにより、報道の自由や番組編集の自由が制約されることのないよう、十分な配慮が必要と考えます。 同様のことは、今後開始予定の「通信情報の利用」（法１７条以下）にも当てはまります。報道機関の通信情報がその意に反して安易に取得されることとなれば、報道の自由や取材源の秘匿の侵害につながることが懸念されます。委員会の審査（法４７条）において、報道機関の報道の自由が考慮されることが明示されるなど、慎重かつ透明性の高い運用を強く希望します。 そのためにも、まずは、本命令案４条について、報道機関である基幹放送事業者が報道目的で取得した情報については、「特定侵害事象等の概要」（４条３項３号）や「その他特記事項」（同７号）に該当し得る場合を含め、報告対象とならないことを、何らかの方法で明確にしていただきたいと考えます。	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。 協議会等について頂いた御意見については、今後の参考といたします。
68	・放送事業者は報道機関として「国民の『知る権利』に奉仕するもの」であり、最高裁も「報道のための取材の自由も憲法21条の精神に照らし、十分尊重に値するものといわなければならない」としています。そのため、政府が報道機関の取材行為や報道活動を制限するようなことはあってはならないと考えます。 ・報道機関が取材で知り得た情報を、守秘義務が原因で報じられないことや、政府への協力として報じないことを求められることは、政府から独立的な立場である報道機関の存立基盤を根底から揺るがすもので、「権力監視」「国民の知る権利への奉仕」といったジャーナリズムの役割が果たせなくなるという重大な懸念があります。 ・その点から、特定侵害事象の報告義務について、報道機関として、報道の自由、取材の自由を不当に制約しないかと深く憂慮します。報道目的で取材の上取得した情報は報告対象の事案の対象外であることを明確にすべきと考えます。 ・また、官民連携で情報共有と対策の協議を行う協議会において、守秘義務を伴う情報を共有するとの説明がありますが、「守秘義務」と「報道の自由」との関係が不明確であり、「守秘義務」を理由に報道機関の取材行為や報道活動、番組編集の自由を制限・干渉しないよう、報道の自由への配慮を明らかにすべきと思料します。 ・合わせて、「取得通信情報の取扱い」についても、取材源の秘匿等報道機関の活動が不当に制約されないよう、報道の自由の尊重を明確にし、慎重な運用を強く求めます。	同上
69	○弊社を含む基幹放送事業者は、特別社会基盤事業者に指定されており、法5条及び命令案4条により、特定侵害事象等の報告が義務付けられます。弊社としては、この際に報道の自由や番組編集の自由、取材源秘匿の原則等の侵害がないようにする必要があると考えます。そのため、弊社を含む基幹放送事業者が報道目的で取得した情報については、報告義務の対象とならないことを何らかの形で明確にするよう強く要望します。 ○今後設置される協議会に基幹放送事業者が構成員等として参加する際、報道の自由や番組編集の自由、取材源秘匿の原則等の侵害がないように、以下を要望します。 第一に、報道目的で取得した情報は、関連法令により課せられる報告及び守秘義務の対象外とすること。 第二に、協議会での提供情報と、基幹放送事業者の独自取材情報が同一または関連する場合にも報道の自由を妨げないこと。	同上

No.	御意見の要旨	御意見に対する主な考え方
70	◆報道目的の情報の適用除外について ・特定侵害事象の報告義務は、報道の自由や番組編集の自由を制約するおそれがある。そのため、取材等、報道目的で取得した情報は明確に報告対象外と位置付けるべきである。 ◆守秘義務と報道活動の関係性の明確化について ・協議会における守秘義務と、独自取材による報道との関係が明確になっておらず、本来報じるべき社会的に重要な事象まで「協議会で得た秘密」とされる懸念がある。独自取材が「守秘義務違反」に問われないように制度運用における報道の自由への配慮を明文化すべきである。 ◆通信情報利用における適切な運用の担保について ・通信情報の取得にあたっては、個別情報（通信の内容）を取得しないという法令上の原則が確実に遵守されていることを担保する必要がある。そのため、国による通信情報の具体的な運用状況などについて定期的に報告を行う仕組みを設けるべきである。 ◆資料の提供その他の協力について ・協議会の規約案には「構成員は、正当な理由がある場合を除き、資料の提供等の求めに応じなければならない。」とあるが、報道機関としての「取材源の秘匿」が「正当な理由」に含まれるのか明示すべきである。	同上
71	「基幹インフラ事業者」としての構成員には「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」や「情報源の秘匿」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、協議会への参加によって、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。 加えて、「協議会構成員等による秘密の不正な利用・漏えいの行為」、「基幹インフラ事業者がインシデント報告等を行わず、是正命令を受けてもなお対応しない場合」、「基幹インフラ事業者がインシデント報告等に関連し、資料提出等を求められても対応しない場合」について「罰則」規定が設けられていますが、報道機関としての「報道の自由」、「取材源の秘匿」などの価値に照らし合わせて、それらが侵害されることは決してあってはならないと考えます。	法第６条の命令及び法第９条の資料の提出の求めは、特別社会基盤事業者自らが使用する電子計算機に関してインシデント報告を行わなかった場合や、当該電子計算機のインシデント報告の施行に必要な限度で当該特別社会基盤事業者に対し、関係する資料の提出等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サイバーインシデントが発生したことを認知した場合に関して当該命令や当該資料の提出の求めを行うことはありません。 協議会について頂いた御意見については、今後の参考といたします。
72	命令案第４条第１項に規定する特定侵害事象の報告義務を履行するにあたり、前提として事業者において事象を検知するためのセキュリティ対策の導入が必要と考えられるため、以下2点について確認したい。 (1) 当該検知体制の整備に関して、本命令案または関連するガイドライン等において、具体的な技術的要件や最低基準が定められる予定はあるか。 (2) 仮に検知体制が未整備であった場合に特定侵害事象を認知できなかったとしても、それ自体が本法令上の義務違反とはならないという理解で相違ないか。すなわち、本条の報告義務は「認知した場合」に発生するものであり、検知体制の整備自体は本命令案の直接の義務対象ではないという解釈でよいか。	御指摘の検知体制の整備は法令上の義務ではなく、本省令案及び関連するガイドライン等において、要件や基準等を定める予定はありません。
73	・特定侵害事象等に係る届出・報告の効率的運用について 特定社会基盤事業者が諸法令に基づく各報告業務を円滑かつ実効的に遂行していくため、報告実務の効率化が図られるべきとの観点より引き続きの運用効率化を検討いただけますと幸いです。 インシデント報告については、報告フォーマットの汎用化に向けた対応が進められていることと承知しております。その上で、報告プロセスのオンライン化や、API連携等による技術的な自動提出の検討など、実務に即した仕組みの構築を更に進めて頂くようお願いします。 特に、経済安全保障推進法に基づく届出事項や、既存の事案報告制度との共通化・互換性の確保が重要です。一度の入力で複数の法的義務を充足できる、あるいは既存の報告を一部転用・参照できるようなシステムを構築頂くことを通じ、事業者・行政双方の事務コスト低減と、迅速かつ確実な情報共有の両立が図られるものと考えます。	頂いた御意見は、今後の制度の運用における参考といたします。
様式　関係		
74	命令案様式第一の記載要領４に記載のある「クラウド・コンピューティング・サービスの取扱い」について、以下の点をご教示いただきたい。 (1)「クラウド・コンピューティング・サービス」には、たとえば「グループ企業が自社グループのためにのみ運営するプライベートクラウド」も含まれるか。それとも、不特定多数の事業者に提供されるパブリッククラウドサービスのみを指すか。 (2) グループ内プライベートクラウドを使用している場合、「クラウド・コンピューティング・サービスを提供する事業者名」として記載すべき者は誰か（グループ内のクラウド運営会社か、特別社会基盤事業者自身か）。 (3) クラウドサービスを利用している場合の特定侵害事象発生時の報告義務について、報告義務を負うのは特別社会基盤事業者のみか、それともクラウドサービスプロバイダーも独立して報告義務を負うか。 (4) 特定侵害事象がクラウドサービスプロバイダー側の設備に起因する場合、特別社会基盤事業者の報告義務の範囲はどこまでか。クラウドサービスプロバイダーから情報提供を受けられない場合の取扱いについてもご教示いただきたい。	・(1)・(2)について 御指摘のクラウド・コンピューティング・サービスの扱いについては、今後ガイドラインでお示ししたいと考えております。 ・(3)について 特別社会基盤事業者のみがインシデント報告の義務を負います。 ・(4)について 御指摘の設備であっても、特定重要電子計算機に該当する場合には、インシデント報告の義務があります。この場合、特別社会基盤事業者は、御指摘のクラウドサービスプロバイダーからの通知等により、特定侵害事象等の発生を認知した場合に報告の義務を負います。

No.	御意見の要旨	御意見に対する主な考え方
75	様式第一の記載要領に、「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添付すること。」とありますが、具体的にどのような資料が想定されるか、ガイドラインに具体例を記載いただくことを要望いたします。	頂いた御意見は、今後のガイドラインの策定における参考といたします。
76	特定重要電子計算機届出書及び特定重要電子計算機変更届出書について、法人である届出者には法人番号を提示させる方が良いのではないかと考える。 その方が、行政によっての届出者についての一意な特定・追跡（履歴確認）が容易になり、行政の能率の向上が期待できるのではないかと考える。	御指摘の届出書の提出対象である特別社会基盤事業者は、特定社会基盤事業者として経済安全保障推進法第50条第１項に基づき指定された者の内数であり、一意に特定できるため、法人番号の記載は求めないこととしております。
全般・その他　関係		
77	サイバー攻撃がさらに巧妙化・高度化する現状を鑑み、「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」に関する施策は必要かつ重要であると考えます。 本法律の施行を進めるに当たり、官民双方にとって有益かつ継続的な取組とするため、対応する企業に過度な負担とならないよう、配慮をお願いいたします。 また、今後策定いただくガイドラインの内容についても、官民で密に意見を交換し、企業からの意見を十分考慮いただくよう、お願いいたします。	ガイドラインの策定や制度の運用にあたっては、特別社会基盤事業者の皆様と密に意見交換を実施しながら、また、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まいります。
78	官民連携を強化し、我が国全体のサイバーセキュリティ能力の向上を図ることの重要性は理解する。 一方で、目下、多様かつ高度なサイバー攻撃が日々発生しており、各事業者のサイバーセキュリティ部門はその対応に相当のリソースを割いているのが現状である。こうした状況に鑑みれば、制度対応に過度な負担が生じることにより、結果として本来優先されるべき日常的なサイバーセキュリティ対応が手薄になるような事態は避けるべきである。そのため、制度に起因する負荷は可能な限り軽減されるべきと考える。 また、届出の対象となる設備に関する情報は、通常、外部に公開されない極めて機微性の高い情報である。万が一それらの情報が漏洩した場合、攻撃者に対して従来取得困難であった内部情報を提供する結果となり、かえって新たなセキュリティリスクを生じさせるおそれがある。 したがって、今後、ガイドライン等で提出を求める情報について特定していくプロセスにおいては、各事業者によって異なるネットワーク構成・設備構成に照らして、制度の目的達成に真に必要な範囲に限定できるよう、柔軟な運用とするべきと考える。 さらに、基本方針において「特定重要電子計算機の届出情報に関しては、内閣府が横断的に管理し、例えば脆弱性情報や特定侵害事象等の報告情報との照合など、必要な整理・分析を行った上で、特別社会基盤事業者に対して、脆弱性情報等の被害の防止のために効果的な情報を提供することその他政府による必要な対応を実施するために活用する」と示されている。現在、多くの事業者ではベンダから脆弱性情報を有償で入手し、自社の取り組みとして脆弱性対応を実施している状況である。本制度により、国全体のサイバーセキュリティ強化を図るという観点からは、外国政府等から得られる情報、地政学的情勢等の攻撃の目的や背景に関する情報等、民間では収集が難しい情報などを収集・分析し、事業者のサイバー対処能力強化につながる情報を提供いただくことを期待する。 また、届出により収集された情報の活用については、被害の未然防止や早期対応にどの程度寄与したのか、提供された情報が実効的に活用されているかを、 一定期間経過後に検証・評価することが不可欠であると考える。	ガイドラインの策定や制度の運用にあたっては、特別社会基盤事業者の負担や事業者によるネットワーク構成等の違い等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まいります。情報提供等について頂いた御意見は、今後の制度の運用における参考といたします。
79	国家レベルでのサイバー防衛力の向上という観点から賛成寄り。しかし何らかの欠点が出て来た場合、支援などの対処が必要です	頂いた御意見は、今後の制度の運用における参考といたします。
80	本命令における「特別社会基盤事業者」とは、経済安保法で定められた「特定社会基盤事業者」と同様、との理解で宜しいか？	本省令案における「特別社会基盤事業者」とは、御指摘の特定社会基盤事業者のうち、法第２条第２項第２号に該当する重要電子計算機を使用するものをいいます。

No.	御意見の要旨	御意見に対する主な考え方
81	本法令の施行にあたり、特別社会基盤事業者として求められる組織体制・内部規定の整備について、以下の点をご教示いただきたい。 (1) 特定重要電子計算機の特定・リスク評価・届出・報告プロセスの確立に関して、具体的な運用体制のモデルケースや推奨事項があればご教示いただきたい。 (2) 施行日（令和８年10月１日）までに事業者が整備すべき体制・規定の最低限の要件はどのようなものか。 (3) 施行後も体制整備が完了していない事業者に対して、一定の猶予期間や段階的な適用が認められる予定はあるか。 (4) 施行前に十分な周知・支援をいただきたいと考えるが、事業者向けの説明会・相談窓口・Q&A集の公表など、事業者の準備を支援するための施策を講じる予定はあるか。	・(1)について 今後策定するガイドラインにおいてお示しする予定です。 ・(2)について 資産届出及びインシデント報告を行えるよう準備いただければと存じます。 ・(3)について 法附則第４条において、施行日時点で特定重要電子計算機を既に導入済みの特別社会基盤事業者については、資産届出の届出期限を施行日から６月以内（令和９年３月31日まで）とする経過措置が設けられております。 ・(4)について 引き続き事業者向けの説明会を実施するとともに、ガイドラインの策定を行う予定です。また、ご不明点などがございましたら、御相談いただけますと幸いです。
82	本法令の目的は「重要電子計算機に対する不正な行為による被害の防止」であり、特にサイバー攻撃によるシステム間の連鎖的な機能不全や、サプライチェーン全体への広範な被害波及を防ぐことにあると理解している。この認識で相違ないか。 この理解を前提とすると、本法令が主として想定する脅威は、外部からの不正アクセスや標的型攻撃による重要インフラへの直接的な侵害であり、内部ネットワーク内での通常の業務通信や、特定重要設備と直接的な接続関係を持たないシステムは、本法令の主たる規制対象として想定されていないという解釈でよいか。 また、本法令の規制対象の範囲を画する際に、「被害の波及可能性」や「攻撃経路としての蓋然性」が重要な判断基準となるという理解で相違ないか。	法の目的は、特定社会基盤事業者の使用する重要な電子計算機（そのサイバーセキュリティが害された場合に特定重要設備の機能が停止し、又は低下するおそれがあるもの）等に対する特定不正行為（マルウェアの実行、不正アクセス等）による被害の防止を図るためのものです。御指摘の内部ネットワーク内での通常の業務通信は特定不正行為の対象ではありません。 また、重要電子計算機には、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ている電子計算機（令第１条第３項第２号及び本省令案第１条第１項）のほか、特定重要設備による情報処理の用に供される電磁的記録を作成するために用いられる電子計算機（令第１条第３項第３号及び本省令案第１条第２項）も含まれます。 これらは、当該電子計算機のサイバーセキュリティが害された場合に特定重要設備の機能が停止し、又は低下するおそれがあるかという観点から規定したものです。
83	本法令の目的が「重要電子計算機に対する不正な行為による被害の防止」であると理解しております。この目的を達成する上で、特にどのような種類の被害、とりわけ広範囲な機能不全といった事態を最も重視し、懸念されているのか、ご教示願いたい。	重要電子計算機へのマルウェアの実行、不正アクセス、業務妨害等による特定重要設備の機能の停止又は低下です。
84	サイバー対処強化法（通称）第2章において、特定重要計算機の製品名やインシデント情報の届出が求められているが、これらの情報はシステム構成や脆弱性を推知され得るものであり、サイバー攻撃者にとって有益な情報となり得る点に強い懸念がある。 同法においては、情報漏洩に関する罰則規定が設けられているものの、罰則の存在のみでは十分な抑止策とは言い難い。届出情報および報告情報を安全に管理するためには、取扱者限定、アクセス制御、ログ管理等、具体的かつ実効性のある技術的・運用的対策の整備が不可欠と考える。 届出・報告を行う事業者が安心して制度に協力できるよう、情報漏洩防止を目的とした明確な情報管理基準の策定ならびに、関係機関に対する厳格な運用の徹底を国として要請することをお願いしたい。	特別社会基盤事業者が安心して資産届出及びインシデント報告を行えるよう、届出された情報等の安全管理を徹底することは重要と考えており、頂いた御意見は、今後の制度の運用における参考といたします。
85	法が想定する官民連携が有効に機能するためには、民間事業者が情報を提供しやすい環境を整える必要があり、そのためには、報告対象となる事象を明確化すると共に、報告事項や報告様式を統一化するなどして、報告者の手続的負担の軽減を図ることが望ましいと考えます。この点、本命令案が、重要電子計算機の範囲を定め（1条）、特定重要電子計算機の届出方法や届出事項・変更等に関する事項を定め（２条・３条）、また、特定侵害事象等の報告対象や報告事項についても定めていることは（４条）、情報の提供に関する実体や手続について一定の明確化をなすものと理解します。 一方で、提供された情報の安全管理については、「安全管理のために必要かつ適切な措置」を講ずることが法で定められているにとどまり（法８条１項）、また、利用の制限についても職員の秘密漏えいの禁止を定めるにとどまっており（同２項）、事業者から提供された情報が目的外で利用されないための制度的な保障については不透明なままです。民間事業者が情報を安心して提供しやすい環境を整える観点から、報告・共有を受けた情報の具体的かつ明確な管理指針を何らかの形で策定すると共に、目的外利用を防ぐための具体的な方策についても何らかの形で策定し、公表すべきと考えます。	同上
86	○法8条は、特別社会基盤事業者が報告した情報について、職員及び元職員が「正当な理由なく（中略）秘密を洩らし、又は盗用してはならない」と禁止していますが、明確な管理指針や目的外利用を防ぐ具体的方策を設けるなどし、実効性ある情報管理を図るよう要望します。	同上
87	情報の安全管理の具体化要求について。国へ提供される資産情報の安全管理措置や目的外利用防止に関して現在の規定は抽象的である。事業者が安心して情報を提供できるよう、より具体的な管理指針や防止策を事前に公表すべきである。	同上
88	本命令の運用に当たっては、特定社会基盤事業者に過度な事務負担が生じることのないよう、十分配慮いただくことを要望します。対象となるシステム環境は事業者ごとに多岐にわたるため、届出・報告において過度に詳細な技術要件や資料提出を一律に求める運用がなされた場合、現場の実務に大きな支障を来すおそれがあります。 また、本制度を円滑に運用していくためには、監視体制の強化、脆弱性対応、訓練の実施、人材の確保など、追加的な投資や体制整備が求められるものと認識しております。制度の目的を着実に達成する観点から、これらに伴う費用負担に対し、補助金や税制措置等を含む継続的な支援の枠組みの整備についても、別途検討いただくことを要望します。	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、運用してまいります。 また、個々の事業者の監視体制の強化等に係る費用を支援することは困難ですが、資産届出等が円滑に行われるよう、特別社会基盤事業者からの相談等に適切に対応してまいります。

No.	御意見の要旨	御意見に対する主な考え方
89	・対象製品・侵害兆候等の定義の更なる明確化 本制度を円滑に運用し、事業者が実効性のある協力を継続実施していくために、何が「特定侵害事象」に該当し、どの製品が対象となるのかについて、施行までにさらなる予見可能性の向上が必要であると考えます。 例えば、WAF（Web Application Firewall）等のセキュリティ製品についても、条件を満たす場合に対象に含まれると理解しているところですが、こうした判断を事業者がより自律的に行いやすいよう、具体的な製品カテゴリや機能要件、あるいは例示としての製品リストを一覧形式で提示いただけますと、解釈のばらつきを防ぎ、円滑な制度開始に貢献するものと存じます。 また、侵害兆候に関しては、単なる不正アクセスの試行と、国家背景を持つ組織的な攻撃の前兆としての兆候を峻別するためのガイドラインを要望します。検知ログの種類や異常挙動の具体例、閾値設定の考え方等が技術的詳細レベルで明示されることにより、事業者は過少・過剰報告を防ぎ、質の高い情報提供を実現できるようになります。併せて、判断に迷うケースに対応するための相談窓口やFAQの整備もご検討ください。	頂いた御意見は、今後のガイドラインの策定及び制度の運用における参考といたします。
90	今回の省令案においては、届出方法の項においては届出の主体については明記がないものと認識しておりますが、基幹インフラ事業者以外の維持管理事業者からの直接届出については、今後の政省令公布時に具体的な運用方法がご提示される予定はございますでしょうか。 弊社を含むクレジットカード事業者においては、取引認証設備および代行信用照会等設備について、他事業者が所有および維持管理を行う設備を、サービス利用契約に基づき利用しています。これらの設備に関しては、経済安全保障推進法の基幹インフラ制度においては届出対象が業務アプリケーションのみに限定されており、特定社会基盤事業者はサービス提供事業者が維持管理するサーバやミドルウェア等の機器類については、開示されている情報はございません。一方で、今回のサイバー対処能力強化法においては、現時点では特定重要設備の種類を鑑みた対象の制限はなく、広く設備に関する機密度の高い情報の開示を維持管理事業者へ求める必要があり、開示が困難とされるケースが想定されます。また、機器名やそれらに対する特定侵害事象を、サービス利用者である複数の特定社会基盤事業者へ開示することはセキュリティ上の懸念もあるかと思料します。 上記より、特定社会基盤事業者自身が維持管理を行わない設備、特にサービス利用契約に基づき使用する設備については、維持管理を行う事業者からの直接報告を可能としていただくことを希望します。	法においては、資産届出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の上、提出いただければと存じます。 なお、特別社会基盤事業者以外の者が維持管理している特定重要電子計算機については、当該維持管理を行っている者の協力を得て届出を行う運用を検討しているところですが、あくまで特別社会基盤事業者において当該特定重要電子計算機を把握いただくことを前提としております。
91	クレジット分野における代行・認証設備は、当社がサービス利用契約に基づき利用者として利用しているものであり、設備の構成や運用に関する詳細情報はサービス提供者が管理しています。 このため、届出を目的として利用者の立場からサービス提供者へ詳細な情報提供を求めることは、契約関係上困難である場合も多く、提供条件を超える要請と認識された場合には、サービスの継続利用が困難となる可能性も考えられます。 その結果、特定重要設備としての利用自体が阻害されるおそれもあることから、基幹インフラ制度の運用にあたっては、利用者が把握・取得可能な情報の範囲や、サービス継続性への影響を踏まえ、利用者に過度な情報取得義務を課さない柔軟な整理/運用が望ましいと考えます。	同上
92	他社管理の特定重要電子計算機について、以下のとおり考慮事項が想定されますので、それぞれの方針についてご検討いただけますようお願い申し上げます。 ○クレジットカード業態固有の課題(サービス利用契約) 弊社を含む多くのクレジットカード事業者が共同利用し、かつ同様の形態であると思料するが、特定重要電子計算機に該当しうる「取引認証設備(特定重要設備類型：ロ)」や「代行信用照会等設備(特定重要設備類型：ヘ)」等は、他事業者が所有し、特定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である。 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/重要維持管理委託等に加え、本法の資産届出/インシデント報告制度において、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る。対応義務を強要した場合、ひいては相手方からサービス提供を拒否され、基幹インフラ役務の提供に支障をきたす可能性も否めない。 前述のクレジットカードの業態をふまえ、サービス利用型の特定重要電子計算機については、委託契約を前提としない資産届出/インシデント報告制度の考え方を示していただきたい。 ○バイパス報告の必要性 特定重要設備を含む特定重要電子計算機は弊社の所有資産でなく、監視運用も委託しているため、資産届出およびインシデント報告で要求されている情報を、弊社を含む特定社会基盤事業者で取り扱うこと自体がセキュリティ上のリスクとなりうる(例:アタックサーフェスの情報が流出した場合、攻撃者の事前偵察精度が向上し、特定妨害行為の成立可能性が高まる。これは、流出元となる特定社会基盤事業者のみならず、当該の特定重要電子計算機を利用するすべての特定社会基盤事業者に影響を及ぼす可能性がある。)と思料するため、所有者または委託者からの直接報告(バイパス報告)を可能とさせていただきたい。 ○雛形提供 また、前述について事業者提出とするか所有者または委託先から提出するかに関わらず、本法案の対応について所有者または委託先に協力を求めるための既存契約の変更や覚書の締結が必要になると想定されるため、経済安全保障法と同様に雛形文書の公開をしていただきたい。	・「○クレジットカード業態固有の課題(サービス利用契約)」及び「○バイパス報告の必要性」について 同上 ・「○雛形提供」について 頂いた御意見は、今後の制度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
93	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(同号ヘ)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も否定できません。 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。	同上
94	・官民連携によるサイバー対処能力の強化に向けた補足 制度の実効性を高め、継続的な改善を図る観点から、以下の2点についても併せて具申いたします。 官民連携枠組にて検討中のことと存じますが、エコシステム全体での防御力向上のため、事業者からの報告に対し、国から当該兆候に関連する脅威インテリジェンス（IoCや分析結果）を迅速にフィードバックしたり、匿名化した事例共有を進めたりする仕組みの強化を要望します。 また、善意に基づき合理的判断で報告を行った事業者が不利益を被らないことを保証する免責規定をご検討ください。積極的な情報提供を行う事業者への優遇措置などのインセンティブも検討いただければ、制度の形骸化を防ぎ、より実効性のあるサイバー対処能力向上の基盤が構築されていくことと存じます。	頂いた御意見は、今後の制度の運用における参考といたします。
95	協議会については、今後ガイドライン等で詳細が示されるものと理解しておりますが、加入により提出を求められる資料や、被害防止のために共有される情報等について、具体的に示していただきたいと考えます。 協議会については、現時点で規約や構成員に関する情報が限られているため、機密情報の管理方法について示していただければと存じます。 また、協議会での判断により外部に情報公開する場合があれば、その基準等もご教示いただければと思います。	頂いた御意見は、今後の参考としたします。
96	幾らコンピュータのセキュリティを上げた所で、内部に汚職・不正を日常的にやらかす大臣や役職者が居て、国民の不利益になる様な事をやっているのだから、意味が無いでしょう…。 ウィルスだのハッキングだの、入られて困る様な 危険な施設 (原発・ミサイル施設など) が有る事自体、国民への脅威です。 軍国化・原発再開などという馬鹿げた政策をやめて、最初から安全な環境を作れば良いだけでしょう。	法においては、資産届出やインシデント報告の義務等を規定するとともに、届出又は報告された情報等を国が整理・分析し、特別社会基盤事業者等に対して脆弱性情報等のサイバー攻撃による被害の防止のために効果的な情報を提供することとしています。本省令案は、当該届出及び報告の対象、方法等を定めるものです。法及び本省令案に基づく取組等を着実に実施することにより、我が国のサイバー対処能力を強化することができ、ひいては国民の安全や国民生活の安定に寄与すると考えております。