「重要電子計算機に対する不正な行為による被害の防止に関する法律施行令案」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		
第１条全般		
1	＞重要情報と電気通信回線で直接又は間接に接続されているもの等 とあるが、いわゆるオンプレミスなら妥当な文言であるが、ことガバメントクラウドにおいては、そのクラウドの性質上、間接に接続されているという点において、際限がない解釈が出来る。（猶更に付すなら、当然にデータの所在もはっきりしない場合もある。） これについて「間接に接続されている」という定義について詳細と具体例を説明願う。	政令案第１条第１項第１号及び第４項の「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。なお、これらに係る重要電子計算機については、「間接に接続」という要件に加えて、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」といいます。）第２条第２項第１号イからホまでに掲げる者又は同項第３号に規定する事業者が使用する電子計算機であることも要件として規定しているため、重要電子計算機の範囲が際限なく広がることはありません。
2	対象範囲および接続性 施行令案は、「重要電子計算機」の範囲として、重要情報を記録する電子計算機に加え、電気通信回線により直接又は間接に接続されている電子計算機を含めることとしています。これは、重要情報を記録する電子計算機のみならず、当該システムに到達するための経路となり得る接続システムも含めて保護対象とすべきことを適切に反映するものです。信頼された接続関係を悪用して高価値の標的に到達するという、現代の攻撃手法の実態とも整合します。 一方で、対象範囲を引き続きリスクベースに維持し、影響の小さいシステムにまで対応が過度に広がることにより、重要な領域への重点化が損なわれることを回避する必要があります。このため、「間接に接続されている」との要件については、保護対象システムの機密性・完全性・可用性に対して実質的な影響を及ぼし得るシステムを捕捉する趣旨であることを、条文又は政府の解釈指針として明確化いただくことを推奨します。具体的には、管理系又はコントロールプレーンに該当するシステム、ID基盤、管理コンソール等、保護対象機能に実質的な影響を与え得るシステムが想定されます。 また、施行令案の運用においては、重要電子計算機の範囲がテナント又は提供サービスの範囲（委託範囲）で整理され、無関係な他テナントや無関係な共有プラットフォーム構成要素が、当然に対象として取り扱われないことが重要です。規制対象となる組織は、共有プラットフォーム上でログ等のテレメトリを処理するマネージドセキュリティサービス（例：SIEM、MDR、脅威ハンティング）への依存を高めています。法の趣旨を維持しつつ、これら実効性の高い検知・対応能力の採用を不必要に阻害しないため、クラウド基盤、マネージドセキュリティサービス基盤、マルチテナント型プラットフォーム等が、その性質上当然に重要電子計算機の範囲に含まれると解されないよう、範囲の境界を明確化いただきたいと考えます。	政令案第１条第１項第１号及び第４項の「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うところ、これは重要情報を記録する電子計算機と電気通信回線で間接に接続されている電子計算機のサイバーセキュリティが害されれば、当該間接に接続されている電子計算機を入り口として当該重要情報を記録する電子計算機のサイバーセキュリティも害されることで、重要情報の管理に関する事務の実施に重大な支障が生ずるおそれがあることを踏まえたものであり、御指摘のリスクベースの観点からも当該間接に接続されている電子計算機を重要電子計算機の範囲に含めることは適当であり、これは法第２条第２項第１号柱書又は第３号の規定の趣旨とも整合的であると考えています。この点については、「重要電子計算機に対する特定不正行為による被害の防止のための基本的な方針」（令和７年12月23日閣議決定）において考え方をお示ししたところです。
3	「重要電子計算機」の範囲が極めて広範かつ抽象的に定義されており、「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」まで含まれる点については、対象が事実上無限定に拡張されるおそれがあります。このような定義は、事業者にとって自らが規制対象となるか否かを事前に判断することを困難にし、過剰な対応や活動の萎縮を招くおそれがあります。対象範囲については、より明確かつ限定的な基準を設け、法的予測可能性を確保すべきです。	法第４条に基づく届出等の規制の対象となる政令案第１条第３項の電子計算機については、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すべからく対象となるわけではなく、同項第１号から第３号までに定めるもののみが対象となります。その上で、頂いた御意見は、同項第２号及び第３号に基づき、主務省令において、重要電子計算機の範囲の詳細を定めるにあたり参考といたします。

No.	御意見の要旨	御意見に対する主な考え方
4	【意見】重要電子計算機の範囲におけるクラウドサービスの明確化について 意見内容：「重要電子計算機」の定義において、「（対象事業者が）使用する電子計算機」という文言が含まれておりますが、これには事業者が利用するクラウドサービス（IaaS/PaaS/SaaS等）を構成する基盤的な電子計算機も含まれると解釈しております。つきましては、クラウドサービスが対象に含まれることを明確にするとともに、その特定にあたっては、クラウドサービス事業者が管理する「物理的・仮想的リソース」と、利用者が管理する「データ・アプリケーション」の責任分界点を踏まえた運用がなされるよう、ガイドライン等で明確化することを要望いたします。 理由： 本政令案第1条第1項は、重要情報を記録する電子計算機やこれに接続された電子計算機を対象としています。現代の重要インフラや行政システムにおいてクラウド利用は不可欠ですが、クラウドサービスにおいては、ハードウェアやハイパーバイザー等の基盤部分はクラウド事業者が管理し、その上のシステムは利用者が管理するという「責任共有モデル」が一般的です。対象範囲の解釈に疑義が生じないよう、明確化が必要だと考えます。	御指摘の重要電子計算機には、クラウドサービスを使用しているものも含まれます。また、責任共有モデルに基づきクラウドサービス事業者が管理する範囲であっても、国、地方公共団体、特定社会基盤事業者等が使用するものであって、政令案の要件に該当するものは、重要電子計算機に含まれます。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。
5	重要電子計算機の範囲とクラウドの責任共有モデルについて 本政令案第1条における「直接又は間接に接続されている電子計算機」の定義に関し、省令やガイドライン等においてクラウドサービスが包含されるかの確認、また、包含する場合は、該当するクラウドサービスの種類の明確化を求めます。さらに、法の適用にあたっては、クラウドサービスの利用における責任共有モデルを前提とし、クラウドサービス事業者が管理する領域(物理インフラストラクチャ、ネットワーク、ハイパーバイザーなどの物理・仮想基盤)と、利用者が管理する領域(アプリケーション、利用者のデータ、セキュリティの設定など)の責任分界点をガイドライン等で明確にすることを要望します。この明確化は、効果的なコンプライアンスとセキュリティの実現に不可欠です。	同上
6	区分判定の明確化 施行令案における区分は概ね明確に定義されている一方、実装主体となる組織が、自組織のシステムが施行令上の範囲に該当するかを判断するに当たっては、具体的な技術的判定基準を示す補足的なガイダンス文書があることが有益です。これにより、分野横断で一貫した適用が確保されると考えます。	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。
7	第一条に、「重要情報を記録する電子計算機及び当該電子計算機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、実際の運用にあたり具体的な対象を特定する際は、「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」（基本方針第４章２節(1)）の趣旨をふまえ、対象が不要に拡大することのないよう運用していただきたい。	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。
第１条第３項関係		
8	重要インフラへの重点化 施行令案第1条第3項において、経済安全保障の枠組みに基づく特定社会基盤事業者が使用する電子計算機等を対象に含めることは、当該分野に対する脅威が進化している現状を踏まえたものであり、適切であると考えます。あわせて、技術および脅威環境の急速な変化に対応できるよう、定義および運用上の考え方が十分な柔軟性を有することを確保いただくことが望ましいと考えます。	政令案第１条第３項の電子計算機のうち、同項第２号及び第３号の電子計算機の範囲の詳細については主務省令で定めることとしており、頂いた御意見は、主務省令の制定及び今後の制度の運用における参考といたします。
9	・「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」について、「直接に接続」、「間接に接続」の定義の違いをそれぞれ明確にしていただきたく存じます。 （備考） （例）特定重要設備Ａとともにネットワーク機器Ｂに接続する設備Ｃ（特定重要設備以外）があり、設備Ｃは設備Ａに対して通信不可である場合の設備Ｃは、「間接に接続」に該当するか等	「直接に接続」とは、二の電子計算機が他の電子計算機が介在することなく電気通信回線で接続されている場合を、「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場合をいいます。 御記載の例の場合は、設備Cは設備Aに対して間接に接続されていると解されます。 なお、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すべからく特定重要電子計算機となるわけではなく、政令案第１条第３項第１号から第３号までに定めるもののみが対象となります。

No.	御意見の要旨	御意見に対する主な考え方
10	重要電子計算機の範囲 ・経済安全保障推進法における特定社会基盤役務の届出対象範囲との整合性・違いの明確化。	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項に基づき指定された特定社会基盤事業者が使用する重要電子計算機の範囲については、政令案第１条第３項において規定しております。具体的には、経済安全保障法に基づく届出義務がある特定重要設備の一部を構成する電子計算機等（同項第１号）のほか、特定重要設備にはあたらないものの、その電子計算機の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として、同項第２号及び第３号の電子計算機を規定しております。
11	【意見】ISMAP等の既存評価制度の活用による措置の免除・簡素化について 意見内容： 本政令案第1条第3項は、「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（経済安全保障推進法）」に基づく特定社会基盤事業者を対象としています。同法や他の政府調達基準と同様に、本政令における「重要電子計算機」の防護措置や安全性確認においても、政府情報システムのためのセキュリティ評価制度（ISMAP）に登録されているサービスについては、監査や報告義務の一部を免除、あるいは既存の書類で代替可能とする措置を講じるよう要望いたします。 理由： 重要インフラ事業者が迅速かつ安全にクラウドを導入するためには、重複する監査や報告による負担を軽減する必要があります。経済安全保障推進法との整合を図り、ISMAP等の国際標準に準拠した第三者認証を活用することは、官民双方の事務コスト削減とセキュリティ水準の維持に寄与します。	ISMAPに登録されているクラウドサービスであっても、法第４条に基づく届出等をいただくことは、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、現時点において、ISMAPに登録されていることをもって届出等の義務を免除し、又は既存の書類で代替する考えはございませんが、導入するクラウドサービスの管理に関して頂いた御意見は、主務省令の制定及び今後の制度の運用における参考といたします。
12	既存の認証制度の活用について 特別社会基盤事業者が、「重要電子計算機に対する不正な行為による被害の防止に関する法律」（以下「本法」）の第4条に基づく、特定重要電子計算機の届出を行う際、クラウドサービスに関する情報が届出事項に含まれる場合、経済安全保障推進法上の特定重要設備の導入計画書等の届出の運用と同様に、政府情報システムのためのセキュリティ評価制度(ISMAP)等の第三者認証を活用することを求めます。ISMAP登録済みのクラウドサービスは、ISO/IEC 27001、27002、27017の基準に基づく約1,200の管理策について既に厳格なセキュリティ評価を受けています。これらのサービスに関しては、安全性確認に係る監査や書類提出の一部を免除・簡素化し、迅速な導入と事務負担の軽減を図るべきです。このアプローチにより、堅牢なセキュリティ保証を維持しながら管理負担を軽減できます。	同上
13	・「特定重要設備の一部を構成する電子計算機」が具体的に何を指すのか、明確にしていただきたく存じます。 ・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第52条第２項第２号ハに該当する電子計算機という理解でよろしいでしょうか。 （備考） 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第52条第２項第２号 ハ　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特定妨害行為（特定重要設備の導入又は重要維持管理等の委託に関して我が国の外部から行われる特定社会基盤役務の安定的な提供を妨害する行為をいう。以下この章において同じ。）の手段として使用されるおそれがあるものに関する事項として主務省令で定めるもの	経済安全保障推進法第50条第１項に規定する特定重要設備が電子計算機その他の設備等により構成されている場合に、当該電子計算機を指します。

No.	御意見の要旨	御意見に対する主な考え方
14	（認識） 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（公布から1年6月以内に施行）第4条において、 特定重要電子計算機を導入した際に、主務省令で定めるところにより、届出が求められる予定であるところ、 同法第2条2項2号及び同法施行令（案）第1条3項1号において、 『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』が特定重要電子計算機の一つとなる。 （現行の施行令（案）省令（案）には除外規定等は無い状況と認識） （意見） 特定重要設備であっても、インターネットと物理的分離しているかつ、施行令（案）第1条3項3号 （インターネットと接続口を有するシステムとUSB等による一定期間ごとの入力が無い）に該当しない場合は、 法第4条（特定重要電子計算機の届出）の対象外とできる旨の規定をすべきではないか。 （理由） インターネットと物理的分離しているかつ、施行令（案）第1条3項3号（インターネットと接続口を有するシステムとUSB等による一定期間ごとの入力が無い）に該当しない場合に、想定しているリスクが存在しないため、法第4条の届出を求める根拠がないのではないか。	政令案第１条第３項第１号の電子計算機については、御指摘のインターネットと物理的分離しているかつ、インターネットと接続口を有するシステムとUSB等による一定期間ごとの入力が無い機器であっても、USBその他の機器による一時的な接続も考えられるなど、一定のリスクを排除できないことから、重要電子計算機に該当することとしております。その上で、個別事業者向けの専用設計品等に関しては届出を不要とする、経済安全保障推進法第52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本法第４条に基づく届出書として扱うこととするなど、特別社会基盤事業者の負担も踏まえた制度設計・運用をしてまいります。
15	特定社会基盤事業者が使用する電子計算機のうち、本制度の対象となる電子計算機の特定について、本号において「主務省令で定めるもの」とされています。予備調査等を踏まえて、各分野の主務所管行政にて詳細が検討されるものと承知していますが、事業者の実態や本制度の実効性の観点等を踏まえた整理となるよう、ご留意をお願いいたします。	頂いた御意見は、主務省令の制定及び今後の制度の運用における参考といたします。
16	各号に定める「主務省令で定めるもの」については、実質的に公開しているといえない検証環境や、セグメントが論理的に分かれていると評価し得る場合等も考慮していただき、過度に適用対象を拡大せずに実務的な影響を抑制いただけるよう、ご留意いただきたい。	頂いた御意見は、主務省令の制定及び今後の制度の運用における参考といたします。
17	第１条第３項第３号の箇所は、これまで説明されてきた、政令で定める特定重要電子計算機の類型(3)「USB等を用いて、特定重要設備及び特定重要設備と接続されている電子計算機にデータを入力可能な電子計算機のうち、主務省令で定めるもの」に相当すると認識している。当該箇所の指す電子計算機は、特定重要設備とNW的に接続されていないという前提があり、USBなどの物理媒体や、Webでのデータ転送サービスなどインターネットを通じて"のみ"特定重要設備にデータの入力が可能なシステムを指しているという理解で合っているか。可能であれば、具体的にどのようなシステムを想定しているか例示いただきたい。	政令案第１条第３項第３号に規定する重要電子計算機は、同項第１号及び第２号を除く電子計算機が該当し、また、典型的な例としては、御指摘のUSBなどの記録媒体やインターネットを通じて特定重要設備にデータの入力が可能なシステムが該当いたします。
18	第一条3項三号の規定について、具体的にどのような設備を想定されているかをご教示いただきたい。	典型的な例としては、USBなどの記録媒体やインターネットを通じて特定重要設備にデータの入力が可能なシステムが該当いたします。
第１条第４項関係		

No.	御意見の要旨	御意見に対する主な考え方
19	適用対象となる主体および「重要情報」の範囲に関し、解釈の確認のため意見提出いたします。 同条項は、法第二条第二項第三号に基づき、「重要電子計算機」のうち「重要情報を保有する事業者等が使用するもの」の範囲を具体化する規定であると理解しております。 この点、「重要情報」とは同条第二項第一号に定義される情報を指すものと整理しておりますが、うち「重要経済安保情報」については、重要経済安保情報保護活用法に基づき、国から指定・提供・管理を受けている場合が該当するとの理解で差し支えないか、確認させていただきたく存じます。 また、法第二条第二項第三号に規定される「サイバー攻撃を受けた場合に重要情報の管理業務に重大な支障が生ずるおそれがあるもの」について、仮に事業者が本条項の対象となる場合、重要情報に係る設計書等が格納されたファイルサーバーや、これに接続する関連システム等が、想定される「重要電子計算機」に含まれるのかについて、考え方を確認しておきたいと考えております。	前段について、法第２条第２項第３号の「重要情報を保有する事業者」に該当する者としては、例えば、重要経済安保情報の保護及び活用に関する法律（令和６年法律第27号）第10条第１項の規定により重要経済安保情報の提供を受けた適合事業者が挙げられます。 後段について、重要情報を記録する電磁的記録が保存されたファイルサーバやこれと電気通信回線で接続している情報システムの情報処理の用に供される電子計算機は、重要電子計算機に当たり得ると考えられます。
第２条（情報の整理及び分析等の事務を委託することができる法人）　関係		
20	第二条において、委託先と指定された2法人については、特定社会基盤事業者にとって最重要な機微情報を取り扱う観点から、国家公務員と同等以上の守秘義務（退職後含む）や雇用の安定性の確保など、情報管理のための対応が必要と考える。	法第72条第４項は、同条第１項又は第２項の規定による事務の委託を受けた者の役員若しくは職員又はこれらの職にあった者について、正当な理由がなく、当該委託に係る事務に関して知り得た秘密を漏らし、又は盗用してはならない旨規定しているほか、法第82条において、当該秘密を漏らし、又は盗用した者は、２年以下の拘禁刑又は100万円以下の罰金に処することとされており、情報の取扱いを担保しております。
21	この一般社団法人へ随意契約により委託する理由を明確にすべきです。 一般社団法人ＪＰＣＥＲＴコーディネーションセンターは今回の法律によって「政府の事務」を担うことになります。これにより、これまでの「中立な民間組織」という立ち位置と、「国の安全保障の一翼」という役割をどう両立させていくかが、今後の信頼維持のポイントになると考えられます。「中立な民間組織」としての顔と、「国家安全保障の執行機関」としての顔。この二律背反する役割の両立は、JPCERT/CCにとって史上最大の舵取りとなります。 これまでのJPCERT/CCは、企業が「お上に知られたくないが、助けてほしい」と駆け込める「駆け込み寺」でした。しかし、国の事務を代行するとなれば、その「信義」のあり方が変容せざるを得ません。 信義則です。結局はそこに行きつきます。信義則」という抽象的な倫理規範を、サイバー安全保障法のような技術的な法案に具体的に反映させるには、「誠実な者には報酬（保護）を、不誠実な者には不利益を」という仕組みを、条文や運用指針（ガイドライン）に落とし込むことが鍵となります。	事務を委託する法人として一般社団法人ＪＰＣＥＲＴコーディネーションセンターを定める理由は、法第41条に規定する事務及び法第42条第１項に規定する事務について十分な技術的能力及び専門的な知識経験を有することとともに、当該事務を確実に実施することができる法人であるためです。一般社団法人ＪＰＣＥＲＴコーディネーションセンターについては、これまでもサイバーセキュリティ基本法施行令（平成26年政令第400号）第６条に基づきサイバーセキュリティ戦略本部の事務の一部を受託しており、本法に基づき委託する事務についても確実に実施することができると考えております。その上で、「信義則」の指す内容が明らかではありませんが、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。
附則　関係		

No.	御意見の要旨	御意見に対する主な考え方
22	法律施行令の１０月１日からの施行に反対します。 そもそもこの施行恵理案では、１０月１日施行としながら、何を施行するのかが理解できません。 この施行令案では、「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」のうちの重要電子計算機の範囲、事務の委託などの一部のみが規定されています。 政府は本年１月９日、「攻撃元サーバーに入り込み無害化する措置を１０月１日から可能とする方針」を発表したと報道されていますが、この施行令案には書かれていない部分についての情報が、わかりません、 １０月１日から「侵入・無害化する措置」を可能とするというのであれば、今回、パブコメにかけられている施行令案と同時に、無害化の方針を公表し、意見の公募を行うべきです。 細切れにして「よくわからない」状態のままパブコメにかけるのはフェアではありません。 よってこの施行令の１０月１日からの施行に反対します。	本意見公募は、「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施行令案」を対象とするものです。本政令案は法が定める政令への委任事項について規定するものであり、また、御指摘の「措置」は同法の定めによるものではありません。 本政令案は、法の施行の日から施行することとしており、アクセス・無害化措置等に係る規定を整備する重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律（令和７年法律第43号）も、同法附則第１条柱書により、同日から施行することとなります。当該施行の日については、本政令案と別に制定される「重要電子計算機に対する不正な行為による被害の防止に関する法律の施行期日を定める政令」により定められることとなり、これを令和８年10月１日とすることを予定しています（本意見募集における「関連資料、その他」欄参照）。なお、同令は行政手続法（平成５年法律第88号）第３条第２項第１号に該当するため、意見公募手続の対象外です。
23	重要電子計算機に対する不正な行為による被害の防止に関する法律施行令の１０月１日からの施行に反対します。 理由 １、この施行令案で規定されているのは、「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」（以下同法と略）のうちの重要電子計算機の範囲、事務の委託などの一部です。この施行日は本年１０月１日とされています。 しかし、報道によれば、政府は本年１月９日、「攻撃元サーバーに入り込み無害化する措置を１０月１日から可能とする方針」を発表したとされています。これは、この施行令で規定されていない部分については、後で政令などで対応するということと思われます。 １０月１日から「侵入・無害化する措置」を可能とするというのであれば、この施行令案と同時に、無害化の方針を公表し、意見の公募をおこなうべきです。 ２、この意見公募の資料の施行令案（概要）では、「第３　施行期日等」では「公布日：令和８年３月下旬（予定）　施行日：法の施行の日（令和８年１０月１日）」と書かれていますが、この「公布日：令和８年３月下旬（予定）」とは何の公布でしょうか。具体的に明らかにされていません。ことによったら「侵入・無害化」に関する規定でしょうか。 もしか「侵入・無害化」にかかわるものでしたら、問題があります。 ３、同施行令案は、１０月１日施行としながら、何を施行するのか不明です。このような施行令を認めることはできません。重要電子計算機に対する不正な行為による被害の防止に関する法律施行令の１０月１日施行に反対します。	１及び３について 同上 ２について 「関連資料、その他」として添付した「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施行令案（概要）」における「公布日」は、本政令案の公布日を指します。アクセス・無害化措置等に係る規定を整備する重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律は令和７年５月23日に公布されています。
全般・その他　関係		

No.	御意見の要旨	御意見に対する主な考え方
24	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、主務省令にて具体化される、重要インフラの停止等につながるおそれのある電子計算機の届出範囲や内容、報告が必要なインシデントの範囲や報告期限などについても、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。	法の施行に向けた主務省令の制定等にあたっては、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、検討を進めてまいります。
25	異議なしで良い提案だと感じました。 最近SNSでの乗っ取りやフィッシング詐欺のニュースを耳にしてすごく不安でした。 私のような若い世代でも安心してSNSを使えるようにしていただきたいです。 この対策で少しでも国民を救ってほしいです。 陰ながら応援しています。	政令案への賛同の御意見として承ります。
26	「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」およびこれを実施する施行令案を通じて、重要な情報システムのサイバーセキュリティ態勢を強化しようとする日本政府の取組を評価します。重要インフラおよび必須サービスを標的とするサイバー脅威は、引き続き高度化・大規模化しており、これに対応する明確かつ実効的な枠組みを整備することは不可欠です。 また、国家安全保障および公共の安全にとって特に重要なシステムに対し、保護措置を重点的に講じるという日本のリスクベースのアプローチを支持します。このアプローチは、影響の大きいシステムを優先して保護しつつ、重要度の相対的に低い資産に対して不必要な対応負担を生じさせないという、国際的なベストプラクティスとも整合します。	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。
27	施行令案を通じて重要な情報システムの安全性を高めようとする日本の取組を支持します。効果的なサイバーセキュリティには、リスクベースかつインテリジェンス主導のアプローチが不可欠であり、技術的対策、組織的な準備および国際的な協力を組み合わせることが重要であると考えます。 今後の施行・運用の過程において、産業界との継続的な対話を通じて、保護措置が実効的で、現実的であり、変化する脅威環境と整合し続けることを期待します。	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。
28	本施行令は、電力、通信、金融、行政情報システム等、我が国の国家機能及び国民生活の基盤を成す重要インフラを広く対象とするものであるにもかかわらず、これらの重要電子計算機の中枢的管理・運用に従事する者に関する国籍要件又は忠誠確保に関する基準が明文化されていません。重要インフラの中枢的職務は、非常時において国家主権や安全保障に直結するものであり、日本国の法秩序に全面的に服し、国家に対する法的義務を負う者を中心に担わせることには合理性があります。国籍要件等を制度上明示せず、運用に委ねる構造は、透明性を欠き、結果として恣意的又は不統一な取扱いを招くおそれがあるため、少なくとも中枢的管理権限に関しては、明確な要件を設けるべきです。	法においては、御指摘のシステムに関する業務に従事する者の資格要件は定められていないため、法の委任に基づき定める本政令案においても、そのような制度を定める予定はございません。

No.	御意見の要旨	御意見に対する主な考え方
29	通信情報や電磁的記録の整理・分析を前提とする本制度については、表現の自由及び通信の秘密（憲法第21条）との関係で慎重な検討が必要です。本政令は、形式的には検閲制度を設けるものではありませんが、通信情報等が包括的に収集・分析され得る構造となっていることから、利用者や事業者に「監視されている」との認識を生じさせ、結果として表現活動や通信行為に対する萎縮効果をもたらす、いわゆる実質的検閲に該当するおそれがあります。 とりわけ、情報収集・分析の範囲、手法、利用目的、及び第三者提供の有無について、法律又は政令上の明確な限定や、独立した第三者機関による監督・検証の仕組みが十分に示されていない点は重大な懸念事項です。サイバーセキュリティ対策の必要性は否定されるべきではありませんが、その名の下に表現の自由や通信の秘密が過度に制約されることのないよう、権限行使の範囲と限界をより明確に定める必要があります。	本政令案は、法が定める政令への委任事項について規定するものです。 なお、法においては、通信情報の利用は一定の電子計算機に対する不正な行為による被害の防止を目的とする場合に認められており、利用の対象となる通信情報を通信の当事者のコミュニケーションの本質的な内容を理解することができないと認められる情報に限定することなど、通信情報の取得及び取扱いに係る各種の手続や条件、制限等の規律を定めるとともに、独立性を有する機関であるサイバー通信情報監理委員会が、同意によらずに通信情報を利用するための措置の実施に係る承認の求めに対する審査や、通信情報保有機関が法の規定を遵守して通信情報を取り扱っているかどうかについての検査等を行い、これらを通じて通信情報保有機関における通信情報の適正な取扱いを監理することで、重要電子計算機に対する不正な行為による被害の防止のための措置の適正な実施を確保することとしています。
30	【意見】インシデント報告等における情報開示範囲（責任分界点）の限定について 意見内容： クラウドサービスが「重要電子計算機」として指定された場合、将来的に発生しうるインシデント報告等の義務については、クラウド事業者が技術的にアクセス可能かつ管理権限を持つ範囲に限定されるべきであるという点を、今後の主務省令やガイドライン策定の前提として考慮いただくよう要望します。 理由： クラウドサービスにおいては、顧客（利用者）が保存するデータの中身や、顧客が構築したアプリケーション内部の挙動に対し、クラウド事業者はプライバシー保護および技術的な制約（暗号化等）によりアクセスできません。したがって、被害発生時の報告等は、事業者が検知・確認可能なインフラストラクチャの稼働状況や基盤レベルの侵害事実に限定されることが、実効性のある法運用のために不可欠です。	御指摘については、クラウドサービスの種類（SaaS、PaaS、IaaS）に応じ、それぞれの責任分界点の範囲内でご協力いただくことを想定しており、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。
31	インシデント報告義務について 特別社会基盤事業者が、本法の第5条に基づく特定侵害事象等の報告義務を果たすにあたり、クラウドサービス事業者が協力を求められた場合、協力できる範囲については、技術的に管理権限を有する範囲、具体的にはハードウェア、ハイパーバイザー、プラットフォームコンポーネント等のインフラ層に限定されるべきです。クラウドサービスの利用における責任共有モデルに固有のプライバシー保護要件と技術的制約により、クラウドサービス事業者は利用者のデータやアプリケーション内部にアクセスすることができません。省令やガイドライン等において、当該報告義務の影響がそのようなクラウドサービス事業者のアクセスを前提としないことを明確化し、セキュリティとプライバシー保護の両立を図ることを要望します。	同上
32	特定重要電子計算機を利用するシステムにおいて、AIによる自動処理が導入される場合、当該AIが処理を停止し人手対応へ移行した事象についても、インシデント報告の対象範囲に含めることを検討いただきたい。 現状、インシデント報告は不正アクセスや障害等の「異常事態」を想定していると考えられるが、AIシステムにおいては「判断を控えて人間に委ねる」動作が、セキュリティ上の適切な設計として機能する場合がある。 具体的には、以下の区別を報告様式に反映することを提案する。 ・情報不足や信頼性不足により処理を停止したもの ・判断がシステムの権限・責任範囲を超えるために人手に委ねたもの この区別を構造化された形式で記録・報告することにより、事後の監査・原因分析において、AIの誤動作と適切な判断停止を区別でき、重要インフラ全体のセキュリティ水準向上に資すると考える。	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。

No.	御意見の要旨	御意見に対する主な考え方
33	実施ガイダンス 地域や分野による解釈や運用のばらつきを低減し、一貫した対応および調達要件を支えるため、全国共通の実施ガイダンス（例：中央FAQや解釈照会・エスカレーションの仕組み）を整備することを推奨します。 施行日は2026年10月1日とされており、概要資料では公布が2026年3月下旬（予定）とされています。範囲や運用上の期待値に影響するガイダンスおよび下位規程については、可能な限り早期に公表することが望ましく、理想的には施行日の少なくとも6か月前までに提示されることが、実効的な準備に資すると考えます。 セキュリティテレメトリ／ログの国外処理・保管に関する留意点 セキュリティ監視・分析は、24時間365日の運用およびグローバルな脅威相関に依拠しています。このため、多くの組織は一部のセキュリティテレメトリを国外で処理しており、SIEMログデータが国外に保管される場合もあります。暗号化、厳格なアクセス制御、監査、テナント分離、最小化、保存期間管理等の適切な技術的・組織的安全管理措置が講じられている場合には、国外処理・国外保管が法令遵守と両立し得ることを、公式ガイダンスにおいて明確に確認いただくことを推奨します。	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。
34	脅威インフォームド・ディフェンス 重要電子計算機に対する不正な行為による被害の防止および軽減措置の実効性をさらに高める観点から、リスクベースの運用アプローチとして、脅威インフォームド・ディフェンス（Threat-Informed Defense）の採用を奨励することを提案します。 脅威インフォームド・ディフェンスとは、各組織の役割、機能、セクターに関連する現実的な攻撃主体の行動様式および脅威シナリオに基づき、予防、検知および対応の措置を優先順位付けするアプローチです。これにより、最も悪用されやすい攻撃技法に対して資源を重点的に配分でき、早期検知、対応の有効性および全体的なレジリエンスの向上につながります。 特定の技術や統制実装を規定するのではなく、拘束力のないガイダンスにより、各組織が自組織の監視、検知および対応能力が、関連する脅威シナリオや攻撃技法とどのように整合しているかを示すことを奨励することが適切であると考えます。 能力構築 保護対象となる組織が現代的かつ高度なセキュリティ対策を実装・運用できるよう、人材育成および組織能力の強化に継続的に取り組むことが重要です。	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。
35	届出・手続き ・同一メーカー継続導入時の手続きの簡素化。 ・海外製品の安全性確認とホワイトリスト化による届出負担の軽減。 審査・評価 ・追加セキュリティ実装費用（脆弱性診断やアプリ改修）の支援。 ・法対応のための審査用資料作成の支援。 付帯措置・支援策 ・国によるセキュリティ監視センターの提供などの実務支援。 ・インシデント報告に対する技術支援や対策情報の提供。	「届出・手続き」について 同一メーカー継続導入時の手続についての御意見は、今後の制度の運用における参考といたします。また、法第４条に基づく届出情報については、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活用するものであり、その観点からは、御指摘の「安全性確認」や「ホワイトリスト化」を行う考えはございません。 「審査・評価」について 法は、経済安全保障推進法とは異なり、届出内容について審査を実施するものではありません。また、個別の事業者のセキュリティ費用を支援することは困難ですが、法第４条に基づく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。 「付帯措置・支援策」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
36	上記条文において定められる電子計算機の範囲について、解釈により各地方港湾における港湾運送事業者が該当しうる可能性がある。 港湾運送事業者の大半は中小企業であることを踏まえ、以下の対応を切に要望する。 １）セキュリティリテラシー向上に対し、経営層の関与を促進するための施策について 一般論として中小企業においては経営層におけるサイバーリスクへの理解や危機感が十分に醸成されていない現状にあり、事業者責任の強化に際して、当該リスクに対し経営層が積極的に関与する環境の醸成が必要と考える。 ・経営層向けの分かりやすい解説資料 ・物流・港湾業に特化したサイバー事故の想定事例 ・経営判断に直結する「被害額・操業停止リスク」の可視化 などを国および業界団体主導で整備することを要望する。 ２）セキュリティ対策・DX導入コストへの補助について 本政令に基づく対応には、 ・システム更新　・セキュリティソフト・監視体制導入 ・外部専門家の活用 など、多額の初期費用および継続的運用コストが発生する。 特に、荷役機械・現場オペレーションへの投資が優先される港湾運送業では、IT投資の回収が見えにくく、経営判断が進みづらいことから、以下のような支援策を講じることを強く要望する。 ・中堅・中小事業者向けの補助金・助成制度の拡充 ・港湾業界共通で利用可能な標準的セキュリティ基盤の整備 ３）専門部署・人材不足を前提とした制度設計について 地方港の港湾運送事業者は多くが中小企業であり、情報システムやセキュリティを専門とする部署・担当者を配置することが困難であることから、高度なインシデント対応や常時監視体制を単独事業者で構築することは、実情に照らし合わせると非現実的と言える。 本政令および関連法規の運用においては、その実効性を担保するためにも、中小企業者における実現可能性を念頭に置いた制度設計を要望する。	本政令案第１条第３項に規定する重要電子計算機は、経済安全保障推進法第50条第１項に基づき指定された特定社会基盤事業者が使用する電子計算機が対象であり、年間コンテナ取扱量が80万TEU未満の港湾における港湾運送事業者など、特定社会基盤事業者に指定されていない者が使用する電子計算機については対象外となりますが、頂いた御意見は、今後の運用における参考といたします。