「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の一部を改正する命令案」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
本則	関係	
1	今回の改正案では、一部の特別社会基盤事業者について、届出及びサイバー侵害報告に関する経過措置を適用しないこととされています。 サイバーセキュリティ対策の重要性は理解しますが、経過措置を適用しないことは、対象事業者に対して通常よりも重い義務を直ちに課すこととなるため、その必要性及び合理性について十分な説明が不可欠であると考えます。 また、今回の改正理由として、経済安全保障推進法の改正との整合が示されていますが、他法令との整合性を図ることと、本命令において経過措置を適用しないことの必要性・相当性が直ちに導かれるものではありません。 経過措置は、新たに制度の対象となる事業者が、対象設備の確認、社内体制の整備、担当者の配置及び行政との連携体制を構築するための重要な準備期間として設けられているものと理解しています。 そのため、一部の事業者について経過措置を適用しないのであれば、 ＊ なぜ当該事業者については準備期間が不要と判断できるのか。 ＊ 経過措置を維持した場合、制度運用上どのような具体的支障が生じるのか。 ＊ 他の方法では目的を達成できない理由は何か。 について、本命令の改正理由として具体的に説明することを求めます。 また、経済安全保障推進法第53条第1項各号を引用するだけでは、自らが経過措置の対象となるのか否かを事業者が判断しづらい場合があります。対象となる事業者の考え方や具体例をガイドライン等で示し、制度の予見可能性を高めることを要望します。 さらに、災害、組織再編、大規模システム更新その他やむを得ない事情により、直ちに義務を履行することが困難な場合には、期限延長や個別判断など柔軟な対応が可能であることを明確にしてください。 加えて、本改正によって、 ＊ 事業者負担がどの程度増加したのか。 ＊ サイバー対策の実効性が向上したのか。 ＊ 想定外の課題が生じていないか。 について、一定期間経過後に検証を実施し、その結果を公表することを要望します。 制度変更により従来認められていた経過措置を縮小する以上、その必要性及び合理性について、対象事業者及び国民が理解できるよう十分な説明を行うとともに、制度運用後も継続的な検証と必要な見直しを実施することを求めます。	御質問の「なぜ当該事業者については準備期間が不要と判断できるのか」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」といいます。）第２条第２項及び第４条第２項第１号に基づく経過措置（以下単に「経過措置」といいます。）の趣旨は、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項に基づく特定社会基盤事業者の指定という外的要因によって新たに特別社会基盤事業者となった者に対し、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４条に基づく特定重要電子計算機の届出や法第５条に基づく特定侵害事象等の報告（以下「特定重要電子計算機の届出等」といいます。）に関する制度を理解して、これらに向けた準備を行う期間を確保することにあります。他方、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及び株式会社国際協力銀行法の一部を改正する法律（令和８年法律第38号。以下「経済安全保障推進法の一部改正法」といいます。）第１条による改正後の経済安全保障推進法第53条第１項各号のいずれかに掲げる事由により同法第50条第１項の主務省令で定める基準に該当することとなった者は、同項に基づく特定社会基盤事業者の指定がなされ、特別社会基盤事業者となることが当該指定の前に十分予見可能であるため、当該指定の前であっても、あらかじめ、特定重要電子計算機の届出等に関する制度を理解して、これらに向けた準備を行うことが十分可能であり、準備期間を設ける必要はないと判断したものです。 御質問の「経過措置を維持した場合、制度運用上どのような具体的支障が生じるのか」につきましては、経過措置を維持した場合、特定重要電子計算機や特定侵害事象等に関する情報を一定期間整理・分析することができなくなると考えられ、それにより特定重要電子計算機に対するサイバー攻撃による被害の防止のための対応が一部行えなくなることも考えられます。上記の具体的支障の要因が経過措置にあり、これを改正しない限り、上記の具体的支障が解消されないことから、他の方法で目的を達成することは難しいと考えております。 また、御指摘の対象となる事業者の具体例につきましては、様々なケースが想定されることから、こうしたケースについて網羅的に制度の運用に関する説明をお示しすることは困難ですが、当該事業者の考え方などについて頂いた御意見につきましては、今後の「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）」等の策定にあたり参考とさせていただきます。特定重要電子計算機の届出等にあたっては、期限までになされるよう事前に御準備ください。 本省令による改正後の規定の運用において課題等が生じた場合は、検証の上、必要に応じて制度の見直しも含め対応を検討してまいります。

No.	御意見の要旨	御意見に対する主な考え方
2	上位法である経済安全保障推進法と下位ルールである本命令の整合性を図る本改正案は法体系として極めて妥当であり、速やかに適用・施行されるべきと考えます。 また、事業承継等により新たに指定を受けた事業者に対する報告の経過措置（猶予）を適用除外とし、サイバーセキュリティ対策における空白期間をなくすという方向性についても強く賛同いたします。重要社会基盤における途切れのないリスク管理体制の構築を期待します。	賛同の御意見として承ります。
3	承継や組織再編に際して届出・報告義務の空白期間が生じた場合、サイバー攻撃や重大インシデントへの把握・共有・初動対応の遅滞につながるおそれがあります。そのため、事業承継等による対象事業の引継ぎに際し、指定直後から必要な届出・報告義務を適用する方向性は、我が国のサイバーセキュリティ及び経済安全保障の確保の観点から妥当と考えます。制度を実効的に機能させる観点から、以下の点を要望します。 第1に、経過措置の適用除外となる「経済安全保障推進法第53条第1項各号に掲げる事由により指定基準に該当することとなった者」について、事業者が自社の状況変化や事業拡大、組織再編等に照らして適用可否を迅速かつ的確に判断できるよう、具体的な事例や判断基準をガイドライン、FAQ、判断フロー等で示してください。制度改正後も関係事業者や業界団体への継続的な周知を行い、判断のばらつきが生じないよう配慮をお願いいたします。 第2に、特定重要電子計算機の導入届出や特定侵害事象の報告手続について、オンライン化及び利便性向上を要望します。指定後直ちに対応が必要となる事業者の事務負担を軽減し、迅速な情報共有を実現するため、ワンストップで利用できる電子申請・報告環境の整備を求めます。加えて、事業者側のインシデント管理システムやSOC運用基盤等とのデータ連携も見据えた仕組みとなることを期待します。 第3に、報告対象となる侵害事象の範囲や判断基準について、現場の運用担当者が迅速かつ適切に判断できるよう、具体例を交えた要領の提示を要望します。特に、初動対応時点では影響範囲や原因が確定していない事案、監視システムのアラートを起点として調査中の事案、誤検知の可能性が残る事案など、特定侵害事象への該当性判断に迷いやすいケースについても具体例を示してください。明確な基準は、報告の遅延や過剰な報告を防ぎ、制度の実効性向上につながると考えます。 第4に、クラウドサービス事業者、マネージドセキュリティサービス事業者、機器ベンダー等の外部事業者に起因する情報提供の遅れなど、特定社会基盤事業者の責に帰することができない事情により届出・報告に時間を要する場合には、事業者の置かれた状況を個別かつ具体的に考慮し、実態に即した柔軟な運用を要望します。正当な理由のある遅延に過度な不利益が生じないよう、運用上の考え方を示してください。 2026年7月28日	賛同の御意見として承ります。 また、御指摘の第１、第２及び第４の点につきましては、御指摘されたケースも含めて様々なケースが想定されることから、こうしたケースについて網羅的に制度の運用に関する説明をお示しすることは困難ですが、経過措置の適用可否などについて頂いた御意見につきましては、今後の「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）」等の策定にあたり参考とさせていただきます。本省令案の施行後においても様々な機会を捉え、制度の周知を図ってまいります。 また、報告手続に関する利便性等に関して頂いた意見については、今後の運用の参考と致します。

No.	御意見の要旨	御意見に対する主な考え方
4	本改正案は、特定侵害事象等の報告等に関する経過措置を見直し、一定の事業者について経過措置を適用しないものと理解します。経過措置の対象を整理すること自体には賛同します。 ただし、経過措置の対象又は対象外の判断が分かりにくい場合、事業者が「指定後6か月以内であるため報告不要」と誤解し、実際には報告義務がある事象について速報又は報告書の提出が遅れるおそれがあります。 そのため、指定日、基準該当日、設備導入日、特定侵害事象等の発生日又は認知日との関係を、具体例で示すべきです。 また、経過措置の対象外となる事業者については、いつから報告義務が発生するのか、どの窓口に、どの様式で、速報及び30日以内の報告書を提出するのかを明確にすべきです。 さらに、経過措置の対象又は対象外の判断については、後日の混乱を防ぐため、判断主体、判断時点、判断根拠を記録できるようにすべきです。これは、事業者の誤解を防ぐためだけでなく、当時の情報に基づいて合理的に対応した行政担当者を守るためにも必要です。	賛同の御意見として承ります。 また、御指摘の各日の関係の具体例につきましては、様々なケースが想定されることから、こうしたケースについて網羅的に制度の運用に関する説明をお示しすることは困難ですが、各日の関係について頂いた御意見につきましては、今後の「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）」等の策定にあたり参考とさせていただきます。 経過措置の対象外となる事業者については、経済安全保障推進法第50条第１項に基づく特定社会基盤事業者の指定がなされ、特別社会基盤事業者となった時点から法第５条に基づく特定侵害事象の報告義務が発生します。報告先の窓口については、特別社会基盤事業者にご案内いたします。報告様式は、主務省令第４条第２項に基づき、今後定めてお示しいたします。 経過措置の適用対象となるかの判断につきましては、今後策定する同解説等も踏まえて、各事業者において適切に御判断いただければと存じます。
5	特定重要電子計算機の届出及び特定侵害事象等の報告に関する経過措置について、経済安全保障推進法第53条第1項各号のいずれかに掲げる事由により基準に該当することとなった事業者には適用しないこととする見直しは、重要な社会基盤に関する届出・報告の空白を抑制する観点から妥当であると考えます。 その上で、実務上、事業者が自ら経過措置の適用対象となるのか、又は適用除外となるのかを判断しやすくするため、施行時までに、具体的な判断例、Q&A、チェックリスト、相談窓口等を示すことを提案します。 本改正案では、経過措置の対象外となる場合が規定されていますが、実際の事業者側では、自社がどの時点で基準に該当することとなったのか、指定日・導入日・基準該当事由との関係をどのように整理すべきかについて、判断に迷う場面が生じ得ると考えます。 特に、複数の事業、グループ会社、委託先、既存システムの更新、段階的な導入などが関係する場合、経過措置の有無を誤って理解すると、必要な届出や報告が遅れるおそれがあります。一方で、過度に不明確なままでは、事業者側に過剰な事務負担や萎縮的な対応が生じる可能性もあります。 したがって、改正内容の趣旨を損なわない範囲で、経過措置が適用される場合と適用されない場合の典型例、判断に迷う場合の相談方法、届出・報告期限の起算点の考え方を分かりやすく周知することが望ましいと考えます。 また、施行後に相談窓口へ寄せられた事例のうち、事業者の判断に資するものについては、個別事業者や具体的なシステム構成が特定されないよう情報粒度を落とした上で、Q&Aや事例集に反映して公表することが望ましいと考えます。これにより、施行前に用意された判断例やチェックリストでは十分に拾えなかった実務上の論点についても、後続の事業者が適切に判断しやすくなると考えます。	賛同の御意見として承ります。 また、御指摘の典型例につきましては、御指摘されたケースも含めて様々なケースが想定されることから、こうしたケースについて網羅的に制度の運用に関する説明をお示しすることは困難ですが、経過措置の適用可否や起算点の考え方などについて頂いた御意見につきましては、今後の「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）」等の策定において参考とさせていただきます。 また、特定重要電子計算機の届出等に関する相談窓口を特別社会基盤事業者に周知するとともに、よくある相談につきましては、必要に応じてQ&A等として公表してまいります。

No.	御意見の要旨	御意見に対する主な考え方
6	特定重要電子計算機の届出及び特定侵害事象等の報告については、対象事業者であるか、対象となる電子計算機に該当するか、特定侵害事象等に当たるか、経過措置の適用又は適用除外に当たるか、また認知日をどの時点と整理するかなど、事業者が事故直後に判断すべき事項が多く、実務上判断に迷う場面が生じ得ると考えます。 そのため、事業者が事故発生時又は事故の疑いを認知した時点で、まず相談しやすい軽度の一次窓口として、AI又は対話型チェックツールを活用した相談支援窓口を整備することを提案します。 この窓口は、AIが報告義務の有無を最終判断するものではなく、事業者から、指定状況、対象業務、問題となったシステム、導入日、認知日、事故の種類、クラウド・委託先の関与、社会基盤サービスへの影響可能性などを聞き取り、報告義務や書類提出に該当する可能性がある項目を整理するものとすべきです。 その上で、一定のリスクが検出された場合、判断が困難な場合、又は社会基盤への影響が懸念される場合には、人間の相談窓口へ速やかに誘導し、相談時に必要となる事項を整理したメモを出力する仕組みが望ましいと考えます。 これにより、事業者が「報告対象か分からないため何もしない」という状態を避けやすくなり、行政側も、事業者から整理された情報を受け取りやすくなると考えます。また、AI又は対話型チェックツールの回答は最終判断ではないこと、機密情報や個人情報の入力を必要最小限にすること、人間窓口への誘導条件を明確にすることも併せて重要であると考えます。	特定重要電子計算機の届出等に関する相談窓口を特別社会基盤事業者に周知してまいります。 その他、頂いた意見については、今後の運用の参考と致します。
7	1．予見可能性を高める「FAQ・ガイドライン」の早期公表 「命令案.pdf」において、経過措置の対象外となる条件として「経済安全保障推進法第53条第1項各号に掲げる事由」が引用されていますが、これだけでは事業者が自社の該当性を瞬時に判断するのは困難です。 改善案 本命令の公布・施行にあわせ、「どのようなケース(例:企業の合併、事業譲渡、法的な位置づけの変更など)が不適用事由に該当するのか」を具体例で示したFAQやガイドラインを各府省のウェブサイト等で同時に公表する。 効果 事業者が自社の法的義務を即座に予見できるようになり、問い合わせの殺到を防ぐことができます。 2．8府省共管に伴う「一元的な受付窓口(ワンストップ化)」の明記 「(参考)命令案(概要).pdf」および「命令案.pdf」にある通り、本命令は内閣府をはじめとする8つの府省が共同で所管しています。特定侵害事象等の報告先は「特別社会基盤事業所管大臣及び内閣総理大臣」とされていますが、事業者がどこに連絡すべきか迷う可能性があります。 改善案 実際のインシデント発生時や届出の際に、事業者が迷わず迅速に手続きできるよう、「オンライン(e-Gov等)での一括申請窓口」や「各府省共通のワンストップ受付体制」が整備されていることを、命令の案内文や手引きに明記する。 効果 「事象の認知後、速やかに」というタイトな報告義務に対して、事業者が迅速に行動できるようになります。 3．報告様式(フォーマット)の事前公開 「命令案.pdf」第4条第2項において、特定侵害事象等の報告は「特別社会基盤事業所管大臣及び内閣総理大臣が定めてる様式による報告書」を提出して行うと定められています。 改善案 この報告書の様式(フォーマット)を、命令の施行を待たずに意見募集(パブリックコメント)の期間中、または公布後すぐにサン	御指摘の具体例については、様々なケースが想定されることから、こうしたケースについて網羅的に制度の運用に関する説明をお示しすることは困難ですが、経過措置の該当性について頂いた御意見につきましては、今後の「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）」等の策定にあたり参考とさせていただきます。 その他、頂いた意見については、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
	プルとして事前公開する。 効果 経過措置が適用されず、指定直後から即座に報告義務を負うことになった事業者であっても、事前に社内のセキュリティインシデント対応フロー(ログの収集項目など)を様式に合わせて準備・構築しておくことが可能になります。 4. 意見募集(パブリックコメント)における入力負担の軽減 「意見募集要項.pdf」では、電子メールでの提出において「ウイルス対策のため添付ファイルは不可(本文直接入力)」と制限されています。 改善案 添付ファイルを一律で禁止する代わりに、e-Govの意見提出フォーム内に「命令案のどの部分に対する意見か(第2条関係、第4条関係、附則関係など)」を選択できるドロップダウンメニューを設けるか、メール本文にコピー&ペーストして使える「簡易的な意見記入テンプレート(テキスト形式)」を別紙様式とは別に提示する。 効果 事業者側はテキストデータのみであっても構造化された意見を整理しやすくなり、事務局側にとっても、集まった意見の分類・集計作業が大幅に効率化されます。	
8	事業の引き継ぎを使って、サイバー攻撃の報告義務に空白ができるのは危ないので、改正には賛成です。 ただし、引き継ぎ直後でも現場が迷わず報告できるように、「何を、いつ、どこまで報告するのか」や、前の事業者からの情報引き継ぎルールを明確にすべきです。	賛同の御意見として承ります。 また、民間事業者間の情報の引継ぎについて、国が一律にルール等を定める考えはございませんが、他の特別社会基盤事業者から事業を承継した特別社会基盤事業者に対しても、制度の周知に努めてまいります。
9	特定侵害事象等の報告に関する経過措置について、経済安全保障推進法第53条第1項各号のいずれかに掲げる事由により基準に該当することとなった事業者には適用しないこととする見直しは、重要な社会基盤に関する被害把握の空白を抑制する観点から妥当であると考えます。 その上で、経過措置がなお適用される事業者についても、重大性が高いと考えられる事象、社会基盤への影響が懸念される事象、又は報告義務の有無について判断に迷う事象が発生した場合には、法的な報告義務の追加ではなく、任意の事前相談又は任意の情報提供を促す運用上の案内を整備することを提案します。 サイバーインシデントの初動段階では、影響範囲、原因、侵害の有無、委託先やクラウドサービスとの関係などが直ちに明らかにならない場合があります。そのため、経過措置により報告不要とされる期間であっても、社会基盤への影響が大きい可能性のある事象について、事業者が「報告対象ではないから何もしない」と判断してしまうことは望ましくないと考えます。 一方で、経過措置の趣旨は事業者の移行期負担を緩和する点にもあるため、任意相談や任意情報提供を実質的な追加義務のように扱うべきではありません。あくまで、重大性が高い場合、影響範囲が不明な場合、又は判断に迷う場合に、早期に相談できる窓口や連絡方法、相談時に最低限整理しておく情報を示すことが望ましいと考えます。 また、任意相談又は任意情報提供を行わなかったこと自体に一律の不利益を課すことは、経過措置の趣旨との関係で慎重であるべきと考えます。一方で、経過措置期間中に重大な特定侵害事象等が発生し、事前相談が行われていなかった場合には、事後検証において、当時の判断根拠、確認した事実関係、影響範囲の見積り、内部確認体制、相談を行わなかった理由、再発防止策等を整理することが望ましいと考えます。 その際、事業者が平時から準備しやすいよう、上記のような確認項目について、義務的な追加報告様式ではなく、事後検証時の観点例又は参考フォーマットとして示すことが考えられます。これにより、任意相談を形式的な制度にとどめず、重大事象の早期把握につながる実効的な導線としつつ、経過措置の趣旨との均衡も保ちやすくなると考えます。	賛同の御意見として承ります。 その他、頂いた意見については、今後の運用の参考と致します。

No.	御意見の要旨	御意見に対する主な考え方
10	本改正案において、特定重要電子計算機の届出に関する経過措置を見直すことは、重要な社会基盤に関する届出の空白を抑制する観点から妥当であると考えます。 その上で、特定重要設備又は構成設備である特定重要電子計算機について、導入等計画書又は緊急導入等届出書等の提出をもって届出書の提出に代えることができる場合の実務上の判断について、記載例、Q&A、チェックリスト等を示すことを提案します。 特に、クラウド・コンピューティング・サービスを利用する場合には、サービス名称、提供事業者名、契約上の名称、利用プラン名、サブサービス名、管理画面上の表示名、販売代理店又は再委託先の関与などが複数存在することがあります。そのため、命令上求められる「クラウド・コンピューティング・サービスの名称」や「提供する事業者名」と、事業者が通常管理している契約情報・システム台帳上の名称が、どのように対応するのか判断に迷う場合があると考えます。 また、オンプレミス設備、クラウドサービス、外部委託先の運用サービス、既存設備の更新、段階的な構成変更などが組み合わされる場合には、特定重要設備、構成設備、特定重要電子計算機の対応関係をどの単位で整理すべきかが分かりにくくなる可能性があります。 このような実務上の迷いにより、本来は届出書の提出に代えることができる場合に重複した書類作成が生じたり、逆に代替可能性を誤解して必要な届出が不足したりすることは望ましくありません。 したがって、改正内容の趣旨を損なわない範囲で、例えば、クラウドサービスを利用する場合の記載例、複数サービスを組み合わせる場合の整理例、名称や提供事業者名が契約書・サービス画面・請求書等で異なる場合の確認方法、導入等計画書等で届出書の提出に代えることができる場合とできない場合の典型例を示すことが望ましいと考えます。 これにより、事業者の事務負担を必要以上に増やすことなく、届出内容の正確性を高め、制度運用の安定性を確保しやすくなると考えます。	同上
11	悪質な事業者に対して、厳しい報告義務を課す方針は賛成です。しかし、厳しく監視や規制をされた事業者が、海外に情報を流したりしないか心配です。日本の国益を守るため、海外へのデータ転移等の監視の強化や、日本と価値観を同じくする国同士で情報漏洩の抜け穴をふさぐ仕組みを作ることが必要であると思います。地政学的に日本は野心ある国に囲まれています。日本を守るための適切な事業者管理をお願いいたします。	同上
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
12	本命令案の公示にあたり、サイバーセキュリティ対策やシステム管理のあり方について、以下の点から重大な懸念を抱き、強く意見を述べさせていただきます。 第一に、専門的なシステムや「重要電子計算機」を標的とした対策の名のもとで、際限のないセキュリティ対応や不正防止の強要がもたらす「いたちごっこ」の構造的な限界に対する強い懸念です。どれほど高度な対策や規制を重ねようとも、デジタル空間における不正行為や脅威が完全になくなることはなく、終わりなきシステムのイタチごっこが繰り返されるだけです。実態の伴わない形式的な規制や報告義務の強化は、際限のないコストと労力を社会に強いるものであり、その負担が最終的に一般市民の生活基盤や経済活動に重くのしかかることは到底容認できません。 第二に、こうした技術的対策や管理の強化が、結果として国民生活のあらゆる場面における過度なデジタル化や個人情報の紐付けを一層加速させる口実として利用されていることに対する強い懸念です。これ以上の過剰な便利さやデジタル管理を望まない多くの一般市民にとって必要なのは、いたちごっこを続ける監視社会の肥大化ではありません。行政が優先すべきは、特権的なIT・デジタル業界の論理や終わりなきシステム管理の追求に迎合することではなく、一般市民のプライバシーと平穏な暮らしを守り、過重な負担を強いらない現実的な社会経済基盤の維持です。 最後に、すべてのセキュリティ関連およびデジタル管理の制度運用において、終わりなきイタチごっこを生む過剰な規制の強行や、個人情報の過度な紐付けを推し進める姿勢を速やかに改めるよう強く求めます。行政の役割は、国民をデジタルシステムや監視の網に従属させることではなく、一般市民の生活の安全と権利を第一に守る公正で持続可能な社会基盤を堅持することであると強く訴えます。	主務省令においては、経済安全保障推進法第50条第１項に基づく特定社会基盤事業者の指定という外的要因によって新たに特別社会基盤事業者となった者に対し、特定重要電子計算機の届出等に関する制度を理解して、これらに向けた準備を行う期間を確保するため、経過措置を規定しているところです。他方、経済安全保障推進法の一部改正法第１条による改正後の経済安全保障推進法第53条第１項各号のいずれかに掲げる事由により同法第50条第１項の主務省令で定める基準に該当することとなった者は、同項に基づく特定社会基盤事業者の指定がなされ、特別社会基盤事業者となることが当該指定の前に十分予見可能であるため、当該指定の前であっても、あらかじめ、特定重要電子計算機の届出等に関する制度を理解して、これらに向けた準備を行うことが十分可能であり、準備期間を設ける必要はないと考えられます。このため、本省令案は、当該基準に該当することとなった者に関し、経過措置を適用しないこととしたものです。 このように、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、主務省令を制定し、改正しているところであり、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。 また、本省令案は御指摘のデジタル化や個人情報の紐付けを求めるものでもございません。
13	サイバーセキュリティ対策の強化と周知啓発に関する提言 【提言の趣旨】 現在検討されているサイバー攻撃報告制度の実効性を高めるため、報告された情報の単なる蓄積に留まらない「原因究明・知見の共有」の仕組み化と、国民に届く効果的な周知広報、および次世代のセキュリティ人材育成を提案する。 【具体的な提言内容】 1. 報告情報の有効活用と知見のデータベース化 現状の報告制度では、報告後の対応が個別の対処に終始し、知見が社会全体に還元されていない懸念がある。 AI等の活用による分析： 報告された経緯や手口をAIで解析し、原因究明を迅速化すること。 ナレッジベースの構築： 収集した攻撃手口や対応策を、専門知識がない事業者や個人でも容易に検索・理解できる形式（データベース）で公開し、類似被害の未然防止を図ること。 2. 国民に届く周知広報手法への転換 政府が公表する専門用語の多いPDF資料は、被害のリスクがある層には届きにくい。 デジタルネイティブな発信： SNSやYouTubeを活用し、攻撃の脅威と対策を視覚的かつ平易に解説すること。 メディアと連携した広報： ドキュメンタリー番組（例：警察密着番組の形式等）と連携するなど、エンターテインメント性を交えた、国民の関心を引きやすい周知活動を行うこと。 3.「サイバーセキュリティ人材育成大会」の開催による人材発掘 理系分野への関心喚起と、官民で活用可能な高度人材の発掘を目指し、国主導のイベントを開催することを提案する。 大会の開催： 年に一度の「サイバー対策育成大会（仮称）」を開催し、高額な賞金等を設定することで、技術力のある人材を呼び込む。	頂いた意見については、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
	三方よしの構造： 国： セキュリティ人材の確保と育成。 国民： 高度技術者の認知とサイバー防衛意識の向上。 参加者： 実力に対する適切な評価と社会的地位の向上。 これにより、セキュリティ業界の活性化と国民の理系教育への関心向上を同時に達成できる。 【結論】 サイバー攻撃は今や国民生活のすぐ隣にある脅威です。単なる「報告義務化」という制度的な枠組みにとどまらず、得られた情報を「生きた知見」として社会に還元する仕組みと、国民が自発的に学びたくなるような魅力的な育成・広報戦略を講じることを強く要望します。	
	「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の一部を改正する命令案」について、以下のとおり意見を提出します。 【意見】 本件は、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について、重要電子計算機に対する不正行為による被害防止を実効的に進めるための命令改正案であると理解しています。 重要インフラや特別社会基盤事業者におけるサイバーセキュリティ対策では、侵入防止、検知、報告、復旧が重要であることは当然ですが、それだけでは十分ではないと考えます。近年は、ランサムウェア、内部不正、委託先・再委託先からの流出、クラウド設定不備、端末紛失、外部記憶媒体の紛失、生成AIを利用した流出情報の分析・悪用などにより、侵害発生後の被害拡大が深刻化しています。 特定侵害事象等の報告制度においては、「侵害が発生したか」「どの設備に影響したか」「どのように復旧するか」だけでなく、「侵害により外部に出た可能性のあるデータが、単体で復元・悪用可能な状態だったか」「重要データが分散・無意味化されていたか」「被害を限定する設計がされていたか」という観点も重要だと考えます。 重要インフラの運用情報、制御情報、認証情報、設備情報、顧客情報、障害対応情報、ログ、バックアップデータ等が漏えい・改ざん・悪用された場合、単なる情報漏えいにとどまらず、社会機能の停止、二次攻撃、なりすまし、重要設備への追加攻撃につながるおそれがあります。そのため、重要電子計算機に関する制度では、侵入・検知・報告に加え、漏えい時の被害最小化を安全管理の基本的な考え方に含めるべきです。 暗号化は重要な基礎対策ですが、鍵管理、権限設定、運用ルール、委託先・再委託先での取扱いには人が関与します。そのため、設定ミス、鍵管理不備、誤送信、端末紛失、クラウド設定不備、委託先での取扱いミスを完全に防ぐことは困難です。	

No.	御意見の要旨	御意見に対する主な考え方
	また、重要インフラ事業者において情報システム部門や管理部門がセキュリティルールを定めていても、実際の現場運用では、業務上の利便性、作業負荷、理解不足、例外対応、緊急時対応等により、ルールが十分に徹底されない場合があります。重要データを端末に保存しない、重要ファイルを必ず暗号化する、鍵やパスワードを適切に管理する、といった運用を現場担当者や委託先担当者の判断・注意に委ねるだけでは、人為的ミスやルール逸脱を完全に防ぐことは困難です。	
14	重要インフラでは、平時だけでなく障害時、災害時、サイバー攻撃対応時にも、迅速な復旧や現場対応が求められます。そのような場面では、通常時以上に例外対応や一時保存、ファイル共有が発生しやすくなります。だからこそ、人にルールを守らせるだけではなく、通常どおり業務を行うだけで、重要データが自動的に保護される仕組みが必要です。 たとえば、所定の保存領域に通常どおり保存するだけで、システム側が自動的にデータを分散・無意味化し、流出したデータ単体では復元・悪用されにくい状態にする仕組みは、「人任せにしない安全管理措置」として、特別社会基盤事業者の被害最小化に資すると考えます。 つきましては、命令案及び今後の制度運用において、以下の観点を検討対象に含めることを要望します。 1.特定侵害事象等の報告において、外部に流出又は流出のおそれがあるデータが、単体で復元・悪用可能な状態だったか、又はデータ無意味化・秘密分散・分散保管等により被害が限定される状態だったかを確認できる観点を含めること。 2.重要電子計算機に関係する運用情報、認証情報、制御情報、ログ、顧客情報、バックアップデータ等について、流出したデータ単体では意味を持たず、復元・悪用されにくい状態にする「データ無意味化」「秘密分散」「分散保管」等の技術的対策を、安全管理措置の選択肢として検討すること。 3.特別社会基盤事業者、委託先、再委託先、クラウド環境、保守事業者、バックアップ環境、端末、外部記憶媒体等からの流出を想定し、侵害発生後の被害を最小化する設計を重視すること。 4.サイバー攻撃への対応を「侵入を防ぐ」「検知する」「報告する」「復旧する」に限定せず、「万一侵害されても、重要データが単体では悪用されにくい状態にしておく」という観点を制度解説や実務運用に明確に位置付けること。 5.重要インフラ事業者の現場担当者や委託先担当者が個別に暗号化対象や鍵管理を判断しなくても、所定の保存領域に通常どおり保存するだけで、システム側が自動的にデータを分散・無意味化し、保護する仕組みを検討すること。 6.ルール策定、教育、監査だけに依存するのではなく、通常業務・緊急時対応・復旧作業の中で自然に安全な取扱いとなる、人任せにしない安全管理措置を重視すること。 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、分散保管といった技術カテゴリを、重要電子計算機及び重要インフラのサイバー被害防止・被害最小化のための選択肢として検討していただきたいという趣旨です。 重要インフラのサイバー安全保障では、攻撃を完全に防ぐことを前提にするだけでなく、侵害が発生することを前提に、社会的影響を最小限に抑える設計が重要です。本命令案及び今後の制度運用においても、「漏えい・侵害時の被害最小化」の観点をより明確に反映していただくことを要望します。	同上

No.	御意見の要旨	御意見に対する主な考え方
15	「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の一部を改正する命令案」に対し、以下の意見を提出します。 1. 特定侵害事象の報告事項に、影響を受けたソフトウェアの実装言語およびそのランタイム・主要依存ライブラリの言語別構成を含めるべきです。 御庁には釈迦に説法ですが、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++に起因します。CISA/NSAの共通認識では全CVEの約70%がこのクラスです。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++）、そしてPyTorch・numpy・cryptography等のネイティブ拡張（C/C++/CUDA）に依存しており、ソフトウェア供給連鎖全体として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で実装されており、実質的にCPython + PyTorch + 各種ネイティブ拡張のスタックに依存しています。サイバー対処能力強化法の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、規制の実効性と説得力の観点から看過できない矛盾です。報告事項への実装言語・依存構成の追加は、この矛盾を可視化し是正する第一歩となります。 本命令は特別社会基盤事業者による「特定侵害事象等の報告」を定めるものであり、事象の根本原因分析と再発防止が目的です。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等）は、C/C++等のメモリアンセーフ言語に起因します。米国CISA/NSAの共通認識では、全脆弱性の約70%がメモリ安全性に起因するとされています。報告事項に対象ソフトウェアの実装言語を含めることで、メモリ安全言語（Rust等）への移行のエビデンスが蓄積され、中長期的なサイバー対処能力の強化につながります。 参考： デジタル庁が公開された GenAI （Python+TypeScript）をRust言語で置き換えたリファレンス実装がこちらとなります -- https://github.com/cool-japan/oxigenai/ 2. 国際的な政策動向を踏まえ、メモリ安全なプログラミング言語の採用を政府として推進すべきです。 - 米国ONCD（国家サイバー長官室）は2024年、重要インフラのソフトウェアにメモリ安全言語の採用を求める報告書を発表 - DARPAは2023年、C/C++からRustへの自動変換を研究するTRACTORプログラムを開始 - EUサイバーレジリエンス法（2024年施行）は「secure-by-design」を製品の法的要件として規定 - Microsoftは「Year of Rust 2025」を掲げ、WindowsカーネルのRust化を開始 日本としても、内閣府サイバー安全保障担当が所管する本命令の枠組みにおいて、国際標準に整合したメモリ安全性の確保を明確に位置づけることを求めます。 ＜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）	同上

No.	御意見の要旨	御意見に対する主な考え方
	日本の金融インフラ、とくに地方銀行のサイバー防御力・本人確認体制・AML（マネロン対策）の水準が地域によって大きく異なり、反社会勢力・外国勢力・ブローカー・不正送金などに悪用されるリスクが高い現状を改善するため、国として統一的な基準を設け、世界標準の安全保障レベルへ引き上げることを強く希望します。 日本は銀行数が多く、特に地方銀行は人員・予算・技術力の差が大きく、サイバー防御や本人確認の精度が均一化されていません。この構造が、犯罪者や外国勢力にとって「狙いやすい金融インフラ」になってしまっていると感じます。 民間レベルでも、盗難免許証を使った不正契約が実際に起きており、本人確認の精度が十分ではないと痛感しました。行政でも、兄弟の写真が取り違えられたマイナンバーカードが発行されるなど、本人確認の基盤が不十分なまま運用されている事例があります。こうした弱点は、金融インフラにおいては致命的です。 （1）国が「最低サイバー基準」を法律で義務化すること ガイドラインではなく、以下の項目を法律で義務化し、全国の銀行が必ず達成すべき最低ラインを明確にするべきです。 侵入検知システム（IDS/IPS）の導入 多要素認証の義務化 外部委託先のセキュリティ監査 年次の第三者ペネトレーションテスト インシデント発生時の報告義務 ログの長期保存 勘定系システムの更新基準の統一 世界ではすでに標準化されている項目です。日本だけが遅れている状況を改善する必要があります。 （2） 基準未達の銀行は「共同センター（共同server）」へ移行させること 合併は地域事情から難しいため、機能統合が現実的です。 勘定系 AML サイバー監視 本人確認 ログ管理 これらを共同センター化することで、地方銀行の弱点を一気に解消できます。 世界ではすでに採用されている方式であり、日本でも導入すべきです。	

No.	御意見の要旨	御意見に対する主な考え方
	（3）国のSOC（監視センター）を地銀向けに提供すること 地方銀行は人員も予算も不足しており、自前で高度な監視体制を維持することが困難です。 国がSOCを設置し、地銀はログを送るだけで監視・分析が可能になる仕組みが必要です。 これにより、全国の銀行の防御力が均一化され、サイバー攻撃や不正送金の早期発見が可能になります。 （4） 政府から銀行へ「危険人物データ」をリアルタイム配信する仕組み 世界ではすでに標準化されていますが、日本では未整備です。 指名手配 国際手配（ICPO） 反社情報 外国勢力関連 不正送金の過去履歴 偽造身分証のパターン	
16	技能実習生の失踪情報 留学生ブローカーの情報 これらを銀行の本人確認システムと照合できれば、犯罪者や外国勢力による悪用を大幅に防げます。 （5） 本人確認の強化（顔認証＋救済策の整備） 顔認証は強力ですが、現状は救済策が弱く、自治体で写真取り違えなどの事故が起きています。 本人確認の精度を高めるため、以下を義務化するべきです。 顔認証の事前照合 発行前の自動チェック 顔認証失敗時の多段階救済策 高齢者向けの端末仕様 自治体職員の研修統一 地域での登録サポート体制 金融インフラの本人確認は、国家安全保障の根幹です。	同上

No.	御意見の要旨	御意見に対する主な考え方
	（6） 高齢者の多い地域への段階的導入 地方は高齢者が多く、急な導入は混乱を招きます。 そのため、段階的導入が必要です。 都市部 → 先行 地方都市 → 次 高齢化地域 → 最後に導入 移行期間は3？5年 顔認証と暗証番号の併用期間を設ける これにより、混乱を最小化できます。 （まとめ） 日本の金融インフラは、 「銀行数が多い」「地方銀行の防御が弱い」「本人確認の精度が低い」 という構造的な弱点を抱えています。 これらを放置すれば、 不正資金・外国勢力・反社・ブローカーなどの資金流入が続き、 国家安全保障に深刻な影響を与えます。 そのため、国が主導して以下を進めるべきです。 最低サイバー基準の義務化 基準未達銀行の共同センター化 国のSOC提供 危険人物データの銀行への配信 顔認証の強化と救済策の整備 高齢者への段階的導入 世界基準で「悪い人に利用されない金融インフラ」を構築するため、 国として強力な指導と統一基準の整備をお願いしたいです。 以上	

No.	御意見の要旨	御意見に対する主な考え方
17	ＴＯＳシステムを利用しているだけの港湾運送事業者に、サイバーセキュリティを求められても限界がある。ＴＯＳシステムの提供者に対するセキュリティ強化を求めていただきたい。また、重要インフラとして位置付けるなら、完全クローズドシステムとすべきである、ＵＳＢメモリですら使用しない。システムの更新はしない。システムの買替のみとする。	同上
18	TOSシステムの運用会社が所有・稼働する同システムは、もはや岸壁クレーンやフォークリフト等と並ぶ不可欠な「港湾輸送インフラ」であり、これが機能しなければ現代の港湾物流は成立しません。現行の港湾運送事業法がデジタルインフラやその運用会社を想定していない点は、現状の物流実態から著しく乖離しており、早期に解消すべき大きな課題です。従来のハードウェア中心の法規制にとどまることなく、実質的な輸送の要を担っているTOSシステム運用会社を港湾運送事業者として位置づけるよう、時代に即した法改正に向けて主導的かつ速やかに動くべきです。	同上