# 重要インフラ統一基準（案）に関するパブリックコメントの主な結果一覧

意見のうち、パブリックコメントの対象となる案件についての意見のみ、意見の概要とこれらに対する考え方を掲載しています。

取りまとめの都合上、お寄せいただいた意見は適宜要約しております。

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第１部　総則」に係る意見（目的、適用範囲等）** | |
| 1 | ここでいう重要インフラ事業者“等”とは具体的に何を指しているのか。<br>サイバーセキュリティ基本法第12条第 2項第 3号は、”重要社会基盤事業者及びその組織する団体並びに地方公共団体（以下「重要社会基盤事業者等」という。）におけるサイバーセキュリティの確保の促進に関する事項”とある。このため、本文中に重要インフラ事業者等とある記載については、システムベンダを含むサイバー空間関連事業者との連携は要求していないとの理解でよいか。 | 「重要インフラ事業者等」はサイバーセキュリティ基本法第12条第２項第３号に規定する重要社会基盤事業者等、つまりは重要インフラ事業者及びその組織する団体並びに地方公共団体を指します。システムベンダ含むサイバー空間関連事業者は、ここでの「重要インフラ事業者等」には含まれませんが、重要インフラ事業者等がサイバーセキュリティ対策を実施する中でサイバー空間関連事業者とも連携していくことが求められます。 |
| 2 | 今後は、基幹インフラ事業者は全て重要インフラ事業者に含まれるという理解でよいか。例えば、現在は郵便事業は基幹インフラ事業であるが、重要インフラではないと理解しています。今回の指針により、郵便事業は重要インフラ事業として位置付けられるという理解でよいか。 | 御理解のとおりです。今般、本統一基準において、基幹インフラの対象範囲を原則として、重要インフラ防護の範囲に含めるとの整理をしております。その結果、新たに郵便分野が重要インフラ分野に位置づけられることとなります（第１部1.2）。 |
| 3 | 重要インフラと基幹インフラには指定された業界に差異があるため統一すべき。<br>例えば「港湾輸送」の業界が基幹インフラに指定されており、当該指定により実現すべきは途絶ない物流の実現と理解。<br>これを踏まえると、「輸送」のみならず積荷を保管する「倉庫業」まで含めて守ることが必要。<br>このように守るべき重要インフラ／基幹インフラのバリューチェーンを見極め、サービス継続のために指定すべき業界という観点で重要インフラと基幹インフラの差異を統一されたい。 | 本統一基準では、第１部1.2「統一基準の適用範囲」において、基幹インフラの対象範囲は原則として、重要インフラ防護の範囲に含めるとの整理を行っております。 |
| 4 | 「基幹インフラの対象範囲については、原則、重要インフラの防護範囲に含める」との記載について、（事業内容や法制度設備構成が異なる）多様な事業者が重要インフラの防護範囲に含まれることになる。<br>・根拠法令やシステム構成、保安・供給維持に関する考え方が事業者によって大きく異なるため、特定業界を前提とした規律を横断的に適用・一律の対応を求めることには運用上の課題が伴うおそれがあることを懸念している。<br>・インシデント報告等においては、個社のシステムセキュリティに関する機微情報の共有が求められる可能性があるが、情報管理や実務上の観点から現実的に対応が難しい場合も想定される。<br>・前述のような位置づけの事業者については、国の責任のもとで対応を指示したうえで、取組が進められることが必要であると考える。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。政府機関としては、各分野において、分野の特性・実情や、業法その他の制度・基準等も勘案しつつ、効果な施策の実施を図ることにより、分野・事業者横断的なセキュリティ対策の水準の底上げとともに、各分野におけるリスクベースの取組の更なる水準の向上を図ってまいります。 |

| | | |
|---|---|---|
| 5 | ここでいう特定される重要インフラ事業者は、基幹インフラ事業者（特定社会基盤事業者）とは異なり、指定されると理解した。特定される重要インフラ事業者は、基幹インフラ事業者のように公開して頂きたい。 | 重要インフラ所管省庁において、対象となる重要インフラ事業者等を特定することになるところ、具体の事業者名につきましては、セキュリティの観点から、これまで同様、公表することは控えさせていただきます。 |
| 6 | サイバー攻撃に対する対策を強化することはもちろんだが事業者側にも責任を持って対応してもらわなければ意味がない。<br>特に重要インフラは公営を維持し、不用意な民営化は避けるべきだと考える。民間企業も外資の割合を制限し、特に非友好国には厳しい制限が必要だ。<br>また、中国製の太陽光パネルや無線ルーター、ハブなどにバックドアがある疑いもあり、アメリカ並みにネットワーク製品ソフトウエアを制限する法案も必要だと思う。 | 重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野であり、その安定的な提供の確保が極めて重要であると認識しております。<br>また、サプライチェーン・リスク対策の重要性の観点において、本統一基準では、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしております。<br>政府としては、本統一基準の作成等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 7 | 今回の重要インフラ統一基準（案）は重要インフラを担う事業者に対して適用するセキュリティー基準かと思われるが、「国家の安全保障」が目的であり、「事業者選定」の段階の基準も追記すべき。<br>当然ながら、外資系企業や国内企業でも実質的に外国株主が主要な企業、外国人経営者などは国家にとってはリスクであることは明白である。<br>まずは事業者選定の段階、その後、事業者の経営チェック・改善、この順番が必要で、特に前者を徹底することで後者の省庁負担も大きく変わると思われる。<br>他方、例えば銀行システムのホストなど日本企業では賄いきれない業界もあることは承知しており、インフラ事業者が扱うシステムの内容については外資系企業の製品サービスもあり得るところ、事業者の経営体だけでなく、何の商品サービス使っているかについても緻密なチェックがなければ、国家の情報保護、安全保障は叶わない。<br>いうまでもなく、情報は一旦取られてしまえば取り返せるものではなく、国家、産業の命取りになることから、徹底した国家防衛の意識で制度設計をお願いしたい。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。本統一基準では、重要インフラのサイバーセキュリティ水準の継続的な向上の観点から、重要インフラ所管省庁は、実施計画において対象となる重要インフラ事業者等を特定することとしておりますところ、今後、各分野における具体化検討を進めてまいります。 |
| 8 | インフラ統一基準は、細部にわたってよく検討されていると考えるが、最大の懸念は、人材。官民連携も含めて、外国資本の企業や外国人を責任者に置いている部門で情報が盗まれたり悪用されたりしては、元も子もない。日本人による日本人のためのサイバーセキュリティでなければならない。帰化要件も含めて、関係者に外国人が入る混む隙を作らないように運用されることを強く要望する。 | 重要インフラサービスの安全かつ持続的な提供の重要性についての御意見として承ります。政府としては、本統一基準の作成等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 9 | ・重要インフラの定義に上がっている分野に自衛隊関連の施設が明記されていないことが気になる。役所や警察などが行政サービスに含まれているのは分かるが、別項目として明記すべき。<br>・また、機密に近い内容を扱う研究機関も保護すべき対象と言えるところ、大学などの独立行政法人の研究設備などは行政サービスとして扱うのは分かるが、私立大学の研究機関や企業の基礎研究部門なども同様に保護すべき対象であり、「教育機関」という括りも必要なのではないか。<br>・行政サービスや物流の定義が曖昧で分かりにくいです。例えば、信号などもハッキングを受ければ混乱を引き起こすと思われるところ、道路の管理は物流の中に入っているのか、行政サービスの中に入っているのかも曖昧であるほか、ガソリンの供給施設も化学であり、物流でもあると考えられ管轄が曖昧である。 | 重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野となります。 |

| | | |
|---|---|---|
| 10 | 近年は、AI、量子技術、半導体、宇宙、防衛関連技術、感染症研究等、安全保障上重要な研究開発が大学・研究機関・民間企業において数多く実施されており、研究データや研究設備自体が国家安全保障上の重要資産となっているが、本基準案では、教育・研究分野の位置付けがやや限定的に見受けられる。<br>国公立大学や独立行政法人のみならず、私立大学や民間企業の基礎研究部門についても、一定の場合には重要インフラに準じた保護対象として位置付ける必要があると考える。<br><br>さらに、「行政サービス」「物流」「化学」等の分類についても、一部で重複や曖昧さが存在しているように見受けられ、例えば、<br>◎信号制御システム<br>◎道路交通システム<br>◎ガソリン供給施設<br>◎港湾・空港関連システム<br>◎データセンター<br>等は、行政サービス、物流、エネルギー、通信等の複数分野にまたがる性質を有しており、現代インフラの相互依存性を踏まえると、単一分野のみで整理することが困難になっていると考える。ついては、<br>◎分類基準<br>◎所管整理<br>◎横断的連携体制<br>◎分野横断型インシデント対応<br>について、より明確化・可視化を進めることが望ましいと考える。 | 今般、本統一基準においては、重要インフラ防護範囲の見直しとして、基幹インフラの対象範囲については原則、重要インフラ防護の範囲に含めるとの整理を行っておりますが、御意見の内容については、今後の施策検討に当たって参考とさせていただきます。 |
| 11 | リスクベース・アプローチについて、事業者間で解釈のばらつきを防ぐ観点から、最低限求められる水準と事業特性に応じた上乗せ対応の関係をより明確化いただきたい。 | 御意見として承ります。御意見の内容については、安全基準等策定ガイドラインの作成や各分野における具体化検討に当たって参考とさせていただきます。 |
| 12 | グローバルに事業を展開する事業者の実務との整合性確保の観点から、NIST、ISO/IEC等の国際的フレームワークとの関係性を明示いただきたい。 | 本統一基準は、NIST Cyber Security Framework等も考慮しつつ作成しております。 |
| 13 | 本基準はスパイ防止法制定の足がかりのためのものか。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。 |
| 14 | 東証による株式業種分類（セクター）を利用し、利用状況のカウントは可能か。セクターごとの赤字、またどこに費用が掛かっているか、ピーク需要なども判断しやすくなるのでは。 | 本統一基準は、事業者等の経営状況を把握するための基準ではなく深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。 |
| 15 | 重要インフラとして16分野を挙げているが、そのどれもが、与党議員の為の私利私欲政策により、破綻を来している。政府こそが、日本のリスクであり、早急に改めよ。 | 重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野となります。 |

| | | |
|---|---|---|
| 16 | 農林水産省管轄となる食料品、農産品が重要インフラに指定されていない見解如何。 | 重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野となります。 |
| 17 | 重要インフラ16分野は、サイバーに関する規制のみではなく、重要経済安保として取り扱いを厳重警戒してほしい。<br>16分野の小型無人機等は飛行禁止とするよう小型無人機等飛行禁止法に基づき取り計らって欲しい。 | 本統一基準は、サイバーセキュリティ基本法に基づき作成するものであり、例えば、経済安全保障推進法や小型無人機等飛行禁止法に基づくものではございませんが、重要インフラのサイバーセキュリティ確保のための対策の一環として、情報セキュリティ対策や物理的なセキュリティ対策等も含まれています。 |
| 18 | 重要インフラ統一基準（案）の概要の「現状課題（分野・事業者によるばらつき）重要インフラ」の欄に以下を追加してはどうか。<br><br>国土交通省　道路　道路管理者・警察（交通制御）<br>国土交通省　下水道　下水道<br>国土交通省　河川　河川管理者 | 重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野となります。重要インフラの防護範囲については、引き続き、サイバー脅威の動向や分野・事業者の特性等を踏まえつつ、関係省庁と協議の上、検討を進めてまいります。 |
| 19 | 「重要インフラのサイバーセキュリティに係る安全基準等策定ガイドライン」を国家サイバー統括室が別途策定するとあるが、「重要インフラのサイバーセキュリティに係る行動計画」の２章に記載されている「重要インフラのサイバーセキュリティに係る安全基準等策定指針」との関係性がわかりにくく、混同を起こす可能性がある。当該指針、当該ガイドラインについて当該統一基準および当該行動計画との関係性もふくめて容易に把握できるような図の追記をお願いしたい。<br><br>重要インフラ所管省庁や各分野の業界団体等（以下「所管省庁等」という。）が策定する安全基準等とあるが、ここでいう「安全基準」というのは、例えば、電力であれば「スマートメーターシステムセキュリティガイドライン」が該当すると考えてよいか。<br><br>言葉の定義や、それぞれの言葉の関係性の不明さは、事業者等に理解しづらいため各省も含めた言葉の統一、用語集、関係図をまとめて頂きたい。 | 本統一基準及び安全基準等策定ガイドラインの作成に伴い、「重要インフラのサイバーセキュリティに係る安全基準等策定指針」（以下「安全基準等策定指針」という。）は廃止いたします。<br>また、電力分野における安全基準等には、「スマートメーターシステムセキュリティ安全基準等策定ガイドライン」も該当すると思われますが、具体的には今後、実施計画の策定等を通じて検討を進める予定です。 |
| 20 | 重要インフラを外資に売り渡した結果、水道料金が高騰した…という事例が海外で報告されている。企業は利益を求めていくためそこに任せるのでは無く、国民の生活の基盤となる重要インフラは国が責任を持って運営していくべきであり、民営化してはいけない。<br>特に外資に売り渡すのは日本の防衛戦力にも大きく関わってくるため、絶対に阻止し、国内の企業でも筆頭株主や株の半分以上が外資であるような企業には売らないようにする必要があると考える。 | 御意見として承ります。重要インフラは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものであることから、政府として、本統一基準の作成や運用等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 21 | 金融、航空、空港、鉄道、電力、ガス、行政サービス、水道、化学、石油、港湾、郵政、高速道路（道路公団）の民営化は反対。<br>郵政民営化が良い例である。民営化前まであった資産が民営化により消滅し、鉄道も国鉄を民営化したことにより、北海道のローカル線の赤字区間の整備が出来なくなって廃線となった。利益が上がる地域とそうではない地域を平均して運営出来ていたものを分割することで、格差が生まれ廃止や整備不足、整備不良につながっている。 | 重要インフラサービスの安全かつ持続的な提供の重要性についての御意見として承ります。重要インフラは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものであることから、政府として、本統一基準の作成や運用等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |

| | | |
|---|---|---|
| 22 | 安易に外資を入れることをせず、日本のための政治をしてほしい。 | 御意見として承ります。重要インフラは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものであることから、政府として、本統一基準の作成や運用等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 23 | ぜひ、安心出来る日本企業で、お願いしたい。 | 賛同意見として承ります。 |
| 24 | 民営化は反対。国営化にして利益よりも安全性を重視すべき。<br>もし仮に民営化するにしても、外国人が株所持の比率を多く占めている会社や、外国の会社に委託する事だけは反対する。<br>インフラは国の基幹となる重要な要素であり、利益重視にしたり外国に委ねるのはあってはならない事である。 | 御意見として承ります。重要インフラは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものであることから、政府として、本統一基準の作成や運用等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 25 | 重要インフラへの外資参入は、絶対に禁止すべき。民営であっても、利益優先になる可能性があるので、公的にオープンな形で慎重に検討していただきたい。 | 重要インフラサービスの安全かつ持続的な提供の重要性についての御意見として承ります。重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものであることから、政府として、本統一基準の作成や運用等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 26 | 国のインフラは全て、国民の安全のために保障されるべき。<br>利益の追求より、国民の安心安全のために外資は参入させないでほしい。そのために税金を支払っている。<br>人口が減少しようとも、減った分で賄えるようになるのは当たり前。その分しか必要ないのだから。<br>安易な外国人の受け入れにならないようにして欲しい。 | 重要インフラサービスの安全かつ持続的な提供の重要性についての御意見として承ります。重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野であり、その安定的な提供の確保が極めて重要であると認識しております。政府としては、本統一基準の作成等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 27 | 1　16分野全てを公営化<br>2　16分野全てに外国資金の関与を禁止 | 重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野であり、その安定的な提供の確保が極めて重要であると認識しております。政府としては、本統一基準の作成等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |

| | | |
|---|---|---|
| 28 | この考えに基本的に賛成であるが、懸念点は以下のとおり。<br><br>①国民の個人情報の保護を確実に担保すること。未犯の為という名目で、行き過ぎたインテリジェンス活動により、犯罪歴のない人まで必要以上に個人情報を取得されないか。国民のほぼ全員が、スマホを持っている現在において、時刻、位置情報、クレジットカード、医療機関や公共交通機関の利用、情報機器の利用頻度や内容、等いつでも丸裸に出来る状況にある。スパイ行為まがいの諜報活動をさせない為の罰則規定を同時に盛り込むべきである。最高責任者が内閣総理大臣であればそれを罰することまでしなければ、うやむやになってしまう。サイバー攻撃自体の線引きが難しいので、殊更に具体的な方法と内容が欠かせない。<br>②サイバー攻撃を国民に開示すること。１５の重要インフラ以外の、自衛隊、在日米軍の使用するコンピューターの保護とは具体的に何かがわからない。例えば２０２３年４月に宮古島沖でヘリコプターが突然墜落、機体が大破、乗員１０人全員死亡事故、ボイスレコーダーまで回収しながら国民には公表しない。政治的判断かもしれないが、これまでにも既にたくさんの防衛機密で済まされてきている。特定秘密保護法等を合わせてこれからも更に秘匿されないか。<br><br>今後の推進専門家会議には上記２点を切にお願いしたい。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。 |
| 29 | サイバーセキュリティの観点から公営化すべき。自国のものは自国で護り運営すべき。他国に奪われて搾取されてはならない。 | 重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野であり、その安定的な提供の確保が極めて重要であると認識しております。政府としては、本統一基準の作成等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 30 | ①口座乗っ取り事件は、単純なフィッシング詐欺では無く、高度に組織化されたハッカー集団による証券会社サイトを狙ったハッキング事件であることが、会員の被害報告から判明した。単に個人投資家が自己責任により被害に遭ったという問題ではなく、証券市場の信頼性に関わる問題が潜んでおり、即刻の全容解明と対策の為にも基幹インフラとしての位置付けと証券市場及び証券会社サイトの安全基準等や運営管理体制等の制度制定を強く希望する。<br>②不正アクセス等による証券口座乗っ取り被害の求償に於いて、証券会社ごとに補償水準・対応方針が大きく異なっている現状の改善が急務と思われる。<br>安心安全を担保する基幹インフラの統一基準の見直しの観点から、インターネット証券取引では、欧州連合の最低補償水準を義務付ける統一的な投資者補償制度が参考になる。また、ユーザー負担の観点からは自動車の自賠責保険的な制度制定等も一考。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものであり、特定の分野における被害の救済を目的としているものではありませんが、御意見のサイバー事案については、今後の施策の検討に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 31 | 2025年初頭より多発している証券口座の不正アクセスおよび乗っ取り被害において、金融庁の指導により各社が補償を検討してきたものの、現状では「全額」と「一部（半額～4分の1）」で補償水準に大きな格差が生まれている。<br>顧客は「証券会社が適切なセキュリティを担保している」という信頼のもとで口座開設をしており、フィッシング詐欺など手口が巧妙化する中、顧客の過失のみを理由に補償を減額することは、金融市場の信頼性を損なう。<br>ネット証券は利用者が多く、被害件数も多いことから、大手証券とネット証券で補償方針が分断されることは、消費者にとっての安心安全な資産形成の大きな障壁となる。<br><br>【具体的な要望】<br>1.補償水準の統一: 証券会社側が「多要素認証」等を導入していなかった場合、あるいは導入していても脆弱性があった場合は、原則として全額補償を義務付ける方針を指針に明記すること。<br>2.大手・ネット証券の格差解消: 会社ごとの対応差が、顧客の不公平感につながらないよう、統一的な基準に基づく補償方針を業界団体に徹底させること。<br>3.セキュリティ基準の厳格化: 不正なログインや不審な売買操作が発生した際、速やかに取引を停止するアラート機能の設置を義務付けること。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものであり、特定の分野における被害の救済を目的としているものではありませんが、御意見の対策事項については、今後の施策の検討に当たって参考とさせていただきます。 |
| 32 | 特定投資家の要件緩和は、投資家層の拡大を通じてスタートアップ支援を促進する施策として理解する。しかし、投資家層が広がるほど、オンライン証券における不正アクセス・口座乗っ取り等のリスクは増大し、投資者保護の観点から重大な課題が生じる。 よって、要件緩和と並行して、金融庁においてネット証券のセキュリティ基準強化および監督体制の改善を早急に検討すべきである。 | 御意見の内容については今後の施策の検討や実施に当たって参考とさせていただきます。 |
| 33 | 特定投資家（プロ投資家）への移行要件を緩和する際には、不正アクセス等による証券口座乗っ取り被害が国内で急増し、証券会社ごとに補償水準・対応方針が大きく異なっている現状を踏まえる必要があると考える。<br>特定投資家となった個人についても、不正アクセスに起因する損失については、単に現在の一般投資家向け水準に「合わせる」にとどまらず、少なくとも一定の統一基準に引き上げ、補償・調査・説明義務が確保されるよう、今後の監督指針等で明確にしていただきたい。<br>また、本改正の目的の一つが海外投資家の取り込みや国際的な資金供給の活性化にあるのであれば、欧州連合における統一的な投資者補償制度（投資者補償スキーム指令に基づき、各国に最低補償水準を義務付ける仕組みなど）に見られるように、一定の補償水準を制度として担保することが国際的には重視されている点も踏まえるべき。<br>日本国内で証券会社ごとに不正アクセス被害への補償・対応がバラバラなままでは、権利意識の高い海外投資家にとって、安心して投資行動をとれる環境とは言い難く、結果的に本改正の目的である海外資金の呼び込みにもマイナスに働きかねないため、特定投資家制度の見直しとあわせて、<br>・不正アクセス・口座乗っ取り被害に関する補償・調査・説明義務について、国内業者間での「最低水準の統一」を図ること<br>・その水準は、一般投資家・特定投資家・海外投資家を問わず適用される、国際的に見ても遜色のないものとすること<br>を、監督指針や関連ガイドラインの改正等を通じて位置付けていただきたい。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものであり、特定の分野における補償を目的としているものではありません。 |

| | | |
|---|---|---|
| 34 | 銀行口座と証券口座の連携サービスにおいて、利用者の明確な意思確認および認証が不十分なまま資金移動や金融商品の取引が行われる可能性がある現行の仕組みは、重大な資産被害を 招くおそれがあり、再発防止の観点から制度的な対応が必要である。<br><br>現行の制度および運用において、<br>・利用者が取引の有無や認証履歴を第三者的に検証できない構造となっている<br>・資金移動および取引時の本人認証が十分でない可能性<br>・取引および認証の記録が利用者側で検証困難であること<br>・銀行と証券会社の責任分界が不明確であること<br>といった課題が存在し、利用者保護の観点から不十分であることから、以下のとおり改善提案する。<br><br>・資金移動および金融商品取引における多要素認証の義務化<br>・取引および認証ログの保存と利用者への開示義務の明確化<br>・銀行と証券会社の責任分界の明確化<br>・利用者の明示的同意(都度承認)を必須とする仕組みの導入 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものであり、特定の分野における利用者保護を目的としているものではありませんが、御意見の対策事項については、今後の施策の検討に当たって参考とさせていただきます。 |
| 35 | 地震、火山噴火データなどを扱う、気象(庁)情報についても、追加するように要望する。 | 気象庁は政府機関であり、本統一基準ではなく、政府機関等のサイバーセキュリティ対策のための統一基準群に基づきセキュリティ対策を講じております。なお、本統一基準では、重要インフラサービスの継続的提供を不確かなものとするリスクとして自然災害リスクも含めており、また、第３部では、重要インフラサービスに関する外部環境及び内部環境の状況の整理、サイバーセキュリティリスク等情報について組織内外のコミュニケーション、災害による障害の発生を踏まえた対策等について講ずべきとしておりますところ、これら対策に当たっては、気象庁の提供する気象情報等の活用も想定されます。 |
| 36 | 現在の重要インフラ統一基準は、インフラを担う大手事業者の「設備投資の回収」や「サービス維持のコスト」といった、企業側の身勝手な言い訳を追認しすぎている。<br>電波、光回線、地上波放送網はすべて「国民共有の財産」であり、生存権に直結する「究極の生活必需品」である。全国民が加入を余儀なくされている現状を人質に取り、莫大な利益を上げ続けているにもかかわらず、さらなる値上げやユーザーへの負担転嫁を「自由競争」の名の下に好き勝手に容認する現状は、行政の明らかな不作為である。<br>公共財を使ったビジネスで暴利を貪りながら、負担だけを国民に強いる構造は「公共」という定義そのものと完全に矛盾している。重要インフラ基準においては、これら生活必需品の価格体系を電気・ガスと同様に国が厳格に監視・統制する仕組み（公共料金化）を大前提の基準として明記すべきである。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。 |
| 37 | サイバーセキュリティのイタチごっこが続く現代において、特定の巨大キャリアにインフラを依存することは国家的な脆弱性に直結する。本来であれば、MVNO（格安通信事業者）等の多様なプレイヤーが健全に競争し、ネットワークの流動性と冗長性（バックアップ機能）を高めるべきである。<br>しかし現状は、物理的インフラを握る大手がやりたい放題に市場をコントロールし、MVNOが不利になるような接続条件や不当な優遇措置を放置している。これは公正取引の精神にも、重要インフラの強靭化（レジリエンス）の理念にも逆行する行為である。重要インフラを担う事業者に対し、他社を技術的・経済的に排除することを厳禁し、構造的な公平性を担保する厳格なセキュリティ・公正競争基準を導入せよ。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。 |

| | | |
|---|---|---|
| 38 | 大手事業者が市場の寡占を維持するために多用している「端末の実質レンタル販売」や「固定回線・エネルギーサービスのセット割」は、消費者を心理的・物理的に縛り付ける巧妙な囲い込み戦略である。さらに、より良いサービスを求めて移動しようとする誠実な生活者を、不透明な「総合的判断」というブラックボックス審査によって拒否する現状は、市場の健全な流動性を著しく損なっている。<br>事業者のインセンティブ設計の失敗を、消費者のホッピング（乗り換え）のせいにするという責任転嫁を総務省や内閣官房は容認すべきではない。重要インフラ基準において、これら消費者の選択権を不当に狭める商慣習を「リスク要因」として定義し、徹底的に排除することを求める。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。 |
| 39 | 重要インフラの強靭化とは、既存の巨大企業や既得権益を守るためのものではない。限られた可処分所得の中で日々の生活を営み、額に汗して働く市民が、災害時にも経済的・物理的に見捨てられないための「防波堤」でなければならない。<br>通信の「公共料金化」による経済的アクセスの保障、セット割や実質レンタル販売による「デジタル監禁」の是正、そして技術が人間を縛るのではなく助けるための「移動と通信の自由」の確立。これら生活者の視点に根ざした合理的な基準を、本統一基準の根幹に据えることを強く要求する。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第２部　政府機関における施策の基準」に係る意見（PDCAサイクル等）** | |
| 40 | ①第2部2.3「評価・改善」において、戦略本部が行う評価に、安全基準等への準拠確認に加え、実際の攻撃シナリオに基づく耐性評価を含めるべきことを明記すべき。具体的には、分野横断的なサイバー攻撃対応演習の結果を評価に反映させる仕組みが考えられる。<br>②第2部2.2「把握・分析」における調査が事業者の自己申告に依存する場合、形式的な報告と実態の乖離が把握されない懸念がある。自己申告に加え、国家サイバー統括室または第三者機関による実動的な評価の仕組みを検討すべきである。<br>③評価結果の概要を公開し（事業者名の匿名化等の適切な配慮の上で）、社会全体の状況認識の向上と市場メカニズムによる改善圧力の確保に資する仕組みを設けるべき。 | PDCAサイクルにおける実効性確保に関する御意見として承ります。本統一基準はPDCAサイクルの実施により重要インフラのサイバーセキュリティ強化の実効性を図るものであり、その実現に向けてより効果的な「把握・分析」「評価・改善」の仕組みについて今後検討してまいります。 |
| 41 | 重要インフラに関する統一基準及び行動計画においては、事業者や自治体の自主努力に委ねるだけでなく、経営層、首長、所管省庁の責任として、安全性・信頼性に関する予算、人材、監査、訓練、バックアップ、復旧計画、委託先管理、メール受信基盤の認証検証体制、レガシーシステムの移行計画、基礎的セキュリティ機能の標準装備を明確に位置付けるべき。<br>あわせて、国は、重要インフラ分野ごとの安全基準を形式的に整備するだけでなく、自治体、中小規模の医療機関、地域事業者、物流関連事業者等が実際に実装できるよう、標準的な調達仕様、更新計画、監査項目、委託契約条項、復旧訓練手順、メール認証の受信時検証基準、技術資産の棚卸し様式、基礎的セキュリティ機能の標準要件、費用支援の考え方を具体化すべき。 | 御意見として承ります。本統一基準第２部2.1.1「施策の実施体制」では、PDCAサイクルを推進し、重要インフラのサイバーセキュリティ水準の継続的な向上を図ることとしており、第３部では、重要インフラ事業者等が分野・事業者横断的に講ずべき対策として規定されるべき事項を記載するとともに、3.1「基本的な考え方」では、経営層は、サイバーセキュリティインシデントが発生した場合に法的責任やステークホルダーへの説明責任を負う旨を記載しております。また、第２部2.1.2「取り組むべき施策」に記載の「安全基準等の浸透に向けた取組」についても今後、具体化の検討を進めてまいります。 |
| 42 | 「平時」と「通常時」の文言を合わせていただきたい。<br>2.1.2 取り組むべき施策（３）情報共有体制の強化についてには「通常時」との記載があり、3.6.1 事業継続計画等の脚注29は「平時」との記載がある。<br>また、サイバー攻撃は発覚までに時間を要する場合があり、どういう状況を平時もしくは通常時というかが曖昧だと考えるため、それらの定義を記載いただきたい。 | 御意見を踏まえ、第２部の記載に揃え、3.6.1①事業復旧計画の脚注29を「**通常時**のサービス水準までの完全復旧対応の方針。」に修正いたします。他の御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。 |
| 43 | 医療分野では中小医療機関の多さや人材不足、医療DXの進展によるシステム構成や運用形態の変化等の特性を有しているところ、各医療機関の自主対応だけでは限界がある。そのため、政府が行う「把握・分析」の取組の中で、補完的に全体状況を把握する仕組みを検討することが有効と考えられる。<br>具体的には、医療機関に過度な負担をかけない形で、政府が全体把握を行う仕組みを検討すること、その際には人手による対応を前提とせずITシステムを活用する形で常時監視・兆候把握する（平時から全体状況を把握する）という考え方もできるのではないか。<br><br>これらの取組により、医療機関のみならず、医療システムの開発、導入、運用に関わる関係者においても、セキュリティを十分に考慮した設計や運用を前提とする考え方が、より自然に共有されていく可能性がある。<br>また、医療DX基盤との接続や連携を前提としたシステムについて、平時からの状況・兆候把握を意識した設計や実装が促されることにより、個別対応にとどまらない形で、医療分野全体としてのセキュリティ水準の底上げにつながる可能性もある。 | 御意見として承ります。本統一基準第１部1.3「統一基準に基づく施策の改善」では、重要インフラ事業者等におけるサイバーセキュリティ対策の取組の向上のため、重要インフラ事業者等における取組の実施状況について調査し、施策の改善を進めることとしており、また、第２部2.1.2「取り組むべき施策」では、安全基準等の浸透に向けた取組を含め必要な施策を実施するとしております。事業者の負担に配慮しつつも、サイバーセキュリティ対策の取組向上を進めることが重要と考えております。 |
| 44 | 当該統一基準についてPDCAサイクルによる改定が重要であることは理解していますが、既設の重要インフラに対して改定された基準が適用される場合の費用面のインパクトについて各所轄省庁で基準を策定する場合に十分な考慮が必要な旨の記載をお願いしたい。例えば、後方互換性(旧基準の適用が一定レベルを満たしていることを許容)の維持、適用除外、猶予期間の設定等。 | 御意見として承ります。本統一基準に基づき、重要インフラ所管省庁は実施計画を策定することとなりますが、事業者に過度な負担とならないよう配慮していまいります。 |

| | | |
|---|---|---|
| 45 | 統一基準におけるPDCAサイクル青色のBOX（重要インフラ行動計画に基づく自主的な取組の促進）から「重要インフラ事業者等」のBOXの間に緑色と青色の２つの双方向矢印が記載されているが、これらはそれぞれどのような意味か不明確である。重要インフラ事業者等の観点でInput/Outputが何かわかるような説明を図２に追加することをお願いしたい。 | 本統一基準では、PDCAサイクルのプロセスを通じて、政府機関における施策の実施及び改善を図るとしているところ、重要インフラ行動計画に基づく政府機関の取組を、より効果的なものとすることを意図しております（緑色と青色の２つの矢印）。また、その取組は官から民への片方向のものではなく、官民の連携による双方向のものであることを意図しております（双方向の矢印）。図２はこのようなスキームをイメージしたものですが、PDCAサイクルのスキームについては、今後より分かりやすく発信できる資料を検討してまいります。 |
| 46 | これらの基準等およびガイドラインが1.3節のPDCAサイクルのどの場面で活用されるのか理解できるよう図２に説明を追加することをお願いしたい。 | 政府機関は本統一基準に基づき、「実施計画の策定」や「把握・分析」、「評価・改善」といったPDCAサイクルのプロセスを通じて、政府機関における施策の実施及び改善を図り、重要インフラ事業者等におけるサイバーセキュリティ対策の取組の向上につなげることにより、重要インフラにおけるサイバーセキュリティ強化の実効性を確保していくこととなります。<br>安全基準等策定ガイドラインは、所管省庁等が安全基準等を策定するに当たって参照するため、本統一基準の第３部について詳細事項を記載するものです。重要インフラ事業者等が分野・事業者横断的に講ずべき対策を、安全基準等において明示することにより、重要インフラ事業者等のほかサプライチェーンに関わる事業者等、重要インフラサービスに携わる全ての関係者において理解の共有が進み、必要な対応が行われることを目指しています。PDCAサイクルのスキームについては、今後より分かりやすく発信できる資料を検討してまいります。 |
| 47 | サプライチェーン全体のセキュリティ確保にあたっては、中小規模の取引先を含めた実務負担にも一定の配慮が必要と考えられるため、規模やリスクに応じた段階的な対応の考え方について整理が示されると実務上有益と考える。一律に同水準の対応を求めるのではなく、成熟度や影響度に応じた柔軟な考え方が整理されることが重要と考える。 | 御意見として承ります。本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るものですが、例えば第２部2.1.2「取り組むべき施策」では、重要インフラ事業者等における対策の促進を求めるに当たり、政府機関として、安全基準等の浸透に向けた取組の推進等を図ることとしております。御意見の内容については今後の施策の検討や実施に当たって参考とさせていただきます。 |
| 48 | 今回政府にて策定されることとなる「実施計画」等は、最終的には政府が重要インフラ事業者に自主的な取組を依頼する形になり、その実効性は重要インフラ事業者に委ねることになる。我が国の重要インフラサービスを途絶なく提供するためには、重要インフラ企業が使用するサービスや対応すべきベースラインセキュリティ施策の義務化等一定程度の規制を設けることも検討すべき。<br>また、規制のような対応だけでなく、重要インフラ事業者へのインセンティブもセットで検討すべき。ベースラインセキュリティ以上の高度なセキュリティ対策を実施することによって罰則を減免するなど、重要インフラ事業者による積極的な取組を促す制度を検討することで重要インフラ事業者によるセキュリティ向上が期待できると考える。 | 御意見として承ります。本統一基準を通じ、政府機関の施策のPDCAサイクルにより、重要インフラのサイバーセキュリティの実効性を確保してまいります。また、インセンティブに関する御意見については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 49 | 事業者の実務負担の適正化の観点から、既存制度との重複を回避するための調査・報告の効率化（例：共通質問項目の活用等）の考え方を明確化いただきたい。 | 御意見として承ります。今後、本統一基準に基づくPDCAサイクル等の具体化を進めていきますが、重要インフラ事業者等に過度な負担とならないよう考慮したうえで、本統一基準の作成や効率的な運用等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 50 | 実務適用性の確保の観点から、重要度に応じた段階的適用や柔軟な対応（例：例外管理や補完統制等）の考え方を明確化いただきたい。 | 御意見として承ります。重要インフラ事業者等による取組の実施状況等の把握に当たっては、成熟度モデルを採用するなど、継続的なセキュリティ水準の向上を図ることができる枠組みを検討してまいります。 |
| 51 | 重要インフラ統一基準（案）は、政府機関が取り組むべき施策についての統一基準という位置付けであると認識しましたが、今回の統一基準の作成を受けて、今後、重要インフラ所管省庁のガイドライン等が改定され、重要インフラ事業者はその改定に対応するという理解でよいか。この場合金融分野における資金決済CEPTORの重要インフラ事業者には、具体的な内容として改定後の「金融分野におけるサイバーセキュリティに関するガイドライン」に沿った対応が求められるということと理解してよいか。 | 御理解のとおりです。 |
| 52 | 医療分野においては、重要インフラ統一基準（案）や、これまでの行動計画、厚生労働省が示す医療情報システムの安全管理に関するガイドラインの趣旨・内容が、必ずしも十分に浸透しているとは言えないため、今後、医療分野における施策や活動を進めるに当たっては、医療が重要インフラとして位置付けられていること及び統一基準に沿った対応の必要性について、関係者への情報周知を強化していただきたい。<br>また、医療機関、特に小規模・中規模の医療機関においては、専任人材、予算、技術的支援が十分でない場合も多く、重要インフラ統一基準（案）で求められる内容を直ちに十分な水準で実装することが困難な場合があると考えられるため、基準の提示にとどまらず、実情に応じた段階的な対応や人材育成支援を併せて進めることが重要である。<br>その上で、医療分野では、診療放射線技師等を含む医療専門職を対象として、情報セキュリティの担い手の育成・活用に関する検討が進められている。（診療放射線技師は、医療情報、医療機器、画像情報システム、部門ネットワーク及び診療継続に関する実務知識を有しており、医療機関におけるサイバーセキュリティ対策の実効性を高める上で重要な役割を担い得る資質を有する。）したがって、医療分野におけるサイバーセキュリティ人材の育成・配置に当たっては、診療放射線技師を含む医療情報に通じた医療専門職を明確に位置付け、重要インフラ統一基準に沿って育成・活用を進めることが望ましい。 | 御意見として承ります。医療分野も含めた重要インフラの分野・事業者横断的なサイバーセキュリティ強化においては、本統一基準及び各分野の安全基準等を整備した上で、必要な取組についての効果的な運用と周知が重要であると考えております（例えば、本統一基準第２部2.1.2「取り組むべき施策」では、「安全基準等の浸透に向けた取組（対策を実装するための環境整備、小・中規模／地域事業者等への支援等）の推進」を図るとしております。）。<br>分野特性や実情等に応じた段階的な対応や人材・技術支援の可能性についても、関係省庁と連携しながら検討してまいります。御意見の内容については、今後の施策の検討や実施の推進に当たって参考とさせていただきます。 |
| 53 | 重要インフラ統一基準（案）の中で触れられているように、サイバーセキュリティ確保の取組やその水準は、分野・事業者によってばらつきが多く見られることはご案内のとおりである。各分野の事業者によって、サイバーセキュリティに関するリソースやスキルが大きく異なっていること、重要インフラ事業者の中には、中小企業・小規模事業者もありうることから、あらゆる事業者に対し、同レベルでの対応が期待されること、その対応が課題と承知している。<br>このことから、サイバーセキュリティ企業が行う各分野の事業者に対する支援等は、ますます重要なものになると考えられ、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ある。<br>重要インフラ統一基準（案）の概要資料において、夏頃に安全基準等策定ガイドラインの策定（国家サイバー統括室）が予定されているところ、当該ガイドラインの策定にあたっては、サイバーセキュリティ関係企業も理解を深め、その後の運用上における支障などを積極的に回避する観点から、適宜情報共有いただけるよう、何卒よろしくお願い申し上げたい。 | 賛同意見として承ります。安全基準等策定ガイドラインの作成に向けて、所管省庁等とも連携のうえ、重要インフラ事業等皆様への適切な情報共有を実施してまいります。 |

| | | |
|---|---|---|
| 54 | 今回取り纏めていただいた重要インフラ統一基準（案）は、重要インフラ行動計画に基づく内容が具現化された位置づけと認識しており、所管省庁が各分野に適した形で施策を推進することとなるため、各分野のばらつき解消と全体的な底上げを実現するという点で実効性が高まると考えている。<br>その一方で、今回の統一基準は政府機関向けと理解しているところ、官民双方向でのコミュニケーション強化が必要な中、事業者側への影響度合いが気になるところである。今後のガイドライン策定の段階にて、事業者側への影響および具体的な対応すべき事項などを明記頂くことを期待する。 | 御意見として承ります。本統一基準では、例えば、第２部2.1.2「取り組むべき施策」にて「官民・分野横断的な情報共有」を定めている他、2.2「把握・分析」では、施策の改善に向けた調査結果について「必要に応じて、セプター事務局や重要インフラ事業者等と調査結果等を共有しつつ、各分野における特性・実情等の観点から分析の深掘り」するとしており、官民双方向でのコミュニケーション強化を重要と考えております。今後、安全基準等策定ガイドラインの作成を含む具体化検討や、本統一基準に基づくPDCAサイクルの実施にあたって、官民双方向での密なコミュニケーションを図ってまいります。 |
| 55 | 統一基準における実地調査の実施に当たっては、既存の監督指針等との整合性を踏まえ、検査の運用について明確化いただきたい。<br>統一基準では、実地調査の実施が示されているところ、クレジット分野においては既に「割賦販売法（後払分野）に基づく監督の基本方針」にて立入検査の運用（※）について示されている。<br>（※）「Ⅲ－２ 検査官の行動規範」「Ⅲ－３ 検査に係る基本事項」 等<br>統一基準における実地調査についても、既存の監督指針等で立入検査の運用が明確化されている場合においては、当該運用と平仄が取られることを要望する。 | 御意見として承ります。実地調査に当たっては、重要インフラ所管省庁と協議の上、効果的な施策の実施が図られるよう検討してまいります。 |
| 56 | 2026年10月の施行時点における統一基準の適用について、各項目の充足の考え方を明確化いただきたい。<br>統一基準においては、「3.2 組織統治」から「3.6 対応及び復旧」に至る幅広い対策事項が示されているところ、各事業者においては現行の準拠状況を踏まえ、未準拠項目への対応を順次進めていくことが想定される。<br>一方で、これらの対策には、システム対応や体制整備等、一定の期間を要する性質のものが含まれていることから、施行時点において一律にすべての項目の充足を求める場合には、対応が困難となるケースも想定されるため、施行時点において求める水準や、完全な充足に向けた対応の進め方について、段階的な対応を前提とした考え方を示されることを要望する。 | 御意見として承ります。本統一基準は、PDCAサイクルを推進し、重要インフラのサイバーセキュリティ水準の継続的な向上を図り、深刻化するサイバー脅威に対する重要インフラの一層の防護を図るものです（第１部1.3、第２部2.1.1（２））。御意見の内容については今後の施策の検討や実施に当たって参考とさせていただきます。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第３部　安全基準等において規定されるべき事項／基本的な考え方」に係る意見** | |
| 57 | 重要インフラシステムは、ITの情報システムとOTの制御システムから構成されている。脚注20や23で付記的な記載ではなく、本文できちんと説明することが大切。現在の本文では、情報システムが全体的に前面に出ており（所々システム）となっていて、制御システムの記載がほぼ無くて、「制御システムは関係が無い、薄い」と誤解される恐れがある。制御システムでは、CIAでなくAICの順での考慮が大切のため。ファームウエアへの脆弱性対策も抜けることになる。 | 本統一基準における「情報システム」の定義は、「事務処理等を行うITを用いたシステム、フィールド機器や監視・制御システム等の制御系のシステム等を含むシステム全般」であるところ、OTの制御システムもこの定義に含まれることとなります。情報システムについての説明を含め、本統一基準第３部の詳細については今後、安全基準等策定ガイドラインにて記載する予定です。 |
| 58 | 情報システムの定義は、この統一基準に基づいて各省が制定する安全基準で同様の言葉が使われる場合は、同じ定義にして頂き、言葉の統一化を図っていただきたい。<br>例）水道分野における情報セキュリティ確保に係る安全ガイドライン<br>水道分野のガイドラインの情報システムの定義：<br>5）情報システム<br>ハードウェア及びソフトウェアから成るシステムであって、情報処理または通信の用に供するものをいう。サーバ装置、端末、通信回線装置、複合機、IoT 機器を含む特定用途機器（フィールド機器や監視・制御システム等の制御システム等で使われるものを含む）、ソフトウェアが含まれる。 | 本統一基準及び安全基準等策定ガイドラインにおける「情報システム」の定義は、重要インフラ行動計画における「情報システム」の定義と同一のものとなります。本統一基準第３部に定める各対策をどのような形で安全基準等に盛り込むかについては、関係法令の規定及び安全基準等の構成等を踏まえ、重要インフラ分野ごとに検討されることを想定しておりますが、事業者等への分かりやすさの観点にも配慮してまいります。 |
| 59 | 複数事業を有する企業においては、事業ごとにIT・運用体制が異なる実態もあるため、統一基準の適用範囲について、事業単位・会社単位・グループ単位といった整理の考え方を明確に示していただきたい。また、分野や事業特性を踏まえたリスクベースでの適用範囲の考え方についても、参考となる整理や例示があると、実務上の判断に役立つものと考える。 | 御意見として承ります。本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るものですが、例えば第３部3.1（３）「対象範囲」では、各分野においてリスクベースの考え方に基づく適切な範囲を設定するとしており、事業単位・会社単位・グループ単位といった安全基準等における適用の在り方については、各組織の構造やガバナンス体制を踏まえて適切に整理されるべきものと考えております。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 60 | 複数の事業領域を有する企業では、対象とするインフラ性やリスクの大きさが事業ごとに異なる場面がある。例えば、エネルギー供給に関わるシステムと、一般的な商取引に係るシステムでは、求められるセキュリティ対応の優先度や水準の考え方が異なるケースがある。このため、適用範囲の考え方が一定程度示されることで、各社における実務上の判断が行いやすくなると考える。 | 御意見として承ります。本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るものですが、例えば第３部3.1（３）「対象範囲」では、各分野においてリスクベースの考え方に基づく適切な範囲を設定するとしており、御意見の内容については、各分野における今後の具体化検討に当たって参考とさせていただきます。 |
| 61 | 弊社が提供する前払式支払手段である国際ブランドプリペイドカード（クレジットカードと同様、ブランドネットワークを利用した決済）では、国際ブランドのルール、PCIDSS（クレジットカード業界の国際セキュリティ基準）のようなブランドが共同で設定する基準が存在しますが、今回の統一基準（案）においては、国、業界のガイドラインと同様に整合性をとる対象に含まれる、と考えてよいでしょうか。 | 本統一基準の第３部「安全基準等において規定されるべき事項」等の検討に当たっては、分野・事業者横断的に講ずべき基本的な対策の徹底を図るとの観点から、国際標準等も考慮していますが、特定分野のルールに依拠したものではありません。他方で、第２部2.1では「各分野における特性・実情や、業法その他の法制度の施行状況等も勘案しつつ」実施計画を策定するとしており、また、第３部3.1では安全基準等における規定に当たっては「関係法令の規定及び安全基準等の構成等を踏まえ、分野ごとに検討されることを想定」し、「関連する各種規格、国内外のベストプラクティス等も適宜参照することが望ましい」としているところ、各分野における今後の安全基準等や実施計画等の検討に当たり、必要に応じて、特定分野のルール等を考慮することはあり得るものと考えています。 |

| | | |
|---|---|---|
| 62 | （意見内容）<br>運用環境と開発・試験環境を分離するとあるが、すべての情報システムを対象とすることはコスト面で非現実的と考える。システムの重要度に応じて対応するなどのレベル感を示していただきたい。<br>（理由・背景）<br>コスト増が見込まれるため。 | 安全基準等における対象範囲の設定に当たっては、重要インフラのレジリエンスを確保し、国民生活や経済社会活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する観点から、各分野において、重要インフラサービスを提供するために必要な情報システムや、重要インフラサービスに与える影響の度合い、さらにはサプライチェーン・リスクなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定いただくことを想定しています。 |
| 63 | （意見内容）<br>マルウェアを検出及び予防する仕組みを整備と記載があるが、既存システム全てに整備することは非現実的ではないか。必須の場合、補助金等による費用負担について、ご検討いただきたい。<br>（理由・背景）<br>コスト増が見込まれるため。 | 安全基準等における対象範囲の設定に当たっては、重要インフラのレジリエンスを確保し、国民生活や経済社会活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する観点から、各分野において、重要インフラサービスを提供するために必要な情報システムや、重要インフラサービスに与える影響の度合い、さらにはサプライチェーン・リスクなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定いただくことを想定しています。 |
| 64 | （意見内容）<br>セキュリティの確保に必要なログを記録・管理と記載があるが、既存システム全てに整備することは非現実的ではないか。必須の場合、補助金等による費用負担について、ご検討いただきたい。<br>（理由・背景）<br>コスト増が見込まれるため。 | 安全基準等における対象範囲の設定に当たっては、重要インフラのレジリエンスを確保し、国民生活や経済社会活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する観点から、各分野において、重要インフラサービスを提供するために必要な情報システムや、重要インフラサービスに与える影響の度合い、さらにはサプライチェーン・リスクなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定いただくことを想定しています。その上で、例えば、システム及びネットワーク機器等のアクセス・認証ログや通信ログなど、セキュリティの確保に必要なログを記録・管理いただくことを想定しています。 |
| 65 | （意見内容）<br>サービス仕様が変わる際には影響を確認するとあるが、すべての変更仕様を確認するのは非現実的であると考える。セキュリティ面で影響のある仕様変更など対象を明確にするなど検討いただきたい。<br>（理由・背景）<br>確認対象が広範囲に及び負担となるため。 | 安全基準等における対象範囲の設定に当たっては、重要インフラのレジリエンスを確保し、国民生活や経済社会活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する観点から、各分野において、重要インフラサービスを提供するために必要な情報システムや、重要インフラサービスに与える影響の度合い、さらにはサプライチェーン・リスクなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定いただくことを想定しています。その上で、サービス仕様が変わる際には、サービス運用者等からサービス更新時の影響に関する説明を受け、組織への影響を把握すること等が必要と考えています。 |

| | | |
|---|---|---|
| 66 | 統一基準と既存の関係法令及び各分野の安全基準等との関係性について、役割分担及び整理の考え方を明確化いただきたい。<br>統一基準は、政府機関の施策に関する基準として位置付けられ、各分野の安全基準等を通じて事業者の取組に反映される構造となっている。<br>他方、クレジット分野においては、経済産業省に加え、事業者によっては金融庁の監督指針・ガイドラインへの対応が求められるなど、複数の制度・所管の下で運用が行われている。<br>このため、統一基準が各省庁の施策や基準に反映される過程において考え方に差異が生じた場合、対応の重複や実務上の解釈のばらつきが生じる可能性がある。<br>この点を踏まえ、既存制度との整合性を前提として、統一基準の位置付け及び各制度との関係性について整理・明示されることを要望する。 | 御意見として承ります。ご理解のとおり、本統一基準の第３部は、重要インフラ事業者等が分野・事業者横断的に講ずべき対策として「安全基準等において規定されるべき事項」を定めたものであり、各分野の重要インフラ事業者等は、直接的には引き続き各分野における安全基準等を参照いただくことを想定しております。各分野の安全基準等への反映に向けては引き続き、重要インフラ所管省庁とも連携の上、検討・調整を進めてまいります。 |
| 67 | 統一基準の適用対象となる事業者及び対象システムの範囲について、実施計画の策定に当たり、分野ごとの考え方を示していただきたい。<br>統一基準では、実施計画において対象事業者等を特定する仕組みが採用されており、分野・事業者の具体的特定が必要とされている。<br>クレジット分野はサービス提供形態が多様であるため、対象範囲の考え方が明確化されることにより、関係者間の認識の統一及び円滑な対応に資すると考え得るため、<br>実施計画策定に当たっての対象範囲の考え方について、分野ごとに整理を示されることを要望する。 | 御意見として承ります。本統一基準では、例えば第３部3.1（３）「対象範囲」において「各分野において、重要インフラサービスを提供するために必要な情報システムや、重要インフラサービスに与える影響の度合い、さらにはサプライチェーン・リスクなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定」するとの考え方を示しております。実施計画の策定に向けては、重要インフラ所管省庁と連携しつつ、分野の特性・実情を踏まえ、検討・整理を進めてまいります。 |
| 68 | 資産特定および目録の作成において、重要インフラの構成要素が多様化している現状を踏まえ、「ソフトウェア」および「外部サービス」の把握範囲を以下のように具体化、あるいは例示することを提案する。<br>「ソフトウェア」資産の最小単位： 単なる製品名（OSやミドルウェア名）にとどまらず、それらを構成するライブラリやオープンソースソフトウェア（OSS）等のコンポーネント単位（SBOMの管理）までを管理対象に含めること。<br>「外部サービス」の網羅性： 組織が正式に契約しているものだけでなく、業務部門等が個別に利用するサービス（SaaS等）も含めて継続的に特定・可視化すること。 | 御意見として承ります。安全基準等における対象範囲の設定に当たっては、重要インフラのレジリエンスを確保し、国民生活や経済社会活動に重大な影響を及ぼすことなく、重要インフラサービスの安全かつ持続的な提供を実現する観点から、各分野において、重要インフラサービスを提供するために必要な情報システムや、重要インフラサービスに与える影響の度合い、さらにはサプライチェーン・リスクなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定いただくことを想定していますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 69 | 第3部 3.1（3）「対象範囲」において、安全基準等における対象範囲の設定の考え方として、以下の趣旨を追記することを提案する。「個々の事業者は規模的に重要インフラ事業者に該当しない場合であっても、その集合体として重要インフラサービスの提供に基幹的な役割を担う実態があるものについては、所管省庁において当該集合体としての影響度を踏まえ、安全基準等及び施策の対象として取り込むものとする。」 | 施策の実施体制（重要インフラ事業者の特定）及び対象範囲の設定に関する御意見として承ります。御意見の内容については今後の施策の検討や実施に当たって参考とさせていただきます。 |
| 70 | 第3部 3.1（4）「関係主体の役割」について、安全基準等に記載されるべき関係主体として、以下の趣旨を追記することを提案する。「分散型電源等、事業主体自身が統括的なサイバーセキュリティ管理を担うことが現実的でない領域については、事業主体に代わって当該領域におけるサイバーセキュリティを統括的に担う主体（以下「統括的セキュリティ管理主体」という。）を関係主体の一として位置付け、その役割及び事業主体との責任関係を明記することが望ましい。」 | 施策の実施体制（重要インフラ事業者の特定）及び関係主体の役割に関する御意見として承ります。御意見の内容については今後の施策の検討や実施に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 71 | 第3部 3.1（3）「対象範囲」のうち、「『閉域網だから安全』との過信」に係る注意喚起部分について、以下の趣旨を追記することを提案する。「当該注意喚起は、業界自前の閉域インフラ（電力保安通信網等）を利用する事業者層を主に想定するものである。これに対し、公衆網に直接接続している事業者層（分散型電源を運用する事業者の多くがこれに該当する）については、閉域網への収容と多層防御を組み合わせた対策を所管省庁の施策として促進することが有効と考えられる。安全基準等の整備においては、両者の区別を踏まえた対策の方向性を整理することが望ましい。」 | 施策の実施体制（重要インフラ事業者の特定）及び対象範囲の設定に関する御意見として承ります。御意見の内容については今後の施策の検討や実施に当たって参考とさせていただきます。 |
| 72 | 攻撃者の初期侵入経路はPC・サーバーからモバイル端末へ構造的にシフトしているが、本基準案ではPC・サーバー向け記述に比してモバイル領域の保護要件が極めて薄く、以下5点を提言する。<br><br>[意見1]MDMを起点とした包括的モバイル管理の必須化<br>[意見2]OS・アプリ脆弱性の自動検知と自動隔離の必須<br>[意見3]モバイル脅威防御(MTD)/モバイルEDRの必須化<br>[意見4]ゼロトラスト/ZTNA基盤の強い推奨化(脱VPN)<br>[意見5]業界別付録における具体要件の明文化 | 御意見として承ります。本統一基準案第１部1.3「対象範囲」においては、安全基準等における対象範囲の設定に当たり、各分野において、重要インフラサービスを提供するために必要な情報システムや、重要インフラサービスに与える影響の度合いなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定することとしております。御意見の内容については、今後の施策の検討に当たって参考とさせていただきます。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第３部　安全基準等において規定されるべき事項／組織統治」に係る意見** | |
| 73 | 重要インフラの設計、開発、運用という核心的な業務から外国機関の影響を受ける可能性のある人的要素を排除し、日本国籍者に限定することで、内部不正による致命的なリスクを未然に防ぐべきであり、重要インフラの安全性を担保するため、以下の措置を統一基準に明記することを提案する。<br><br>1. 重要システムの核心部（設計、機密ソースコード作成、特権権限による運用等）に従事する者は、日本国籍者に限定すること。<br>2. 日本国籍者であっても、セキュリティ・クリアランス制度に基づき、外国政府や外国機関との不透明な利害関係、および二重国籍の有無を厳格に精査すること。<br>3. 重要インフラ事業者およびその供給者（ベンダー）との契約において、重要業務への外国人の関与、および海外再委託を禁止する条項を義務付けること。 | 内部不正対策及びサプライチェーン・リスク対策の重要性に関する御意見として承ります。本統一基準では、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしております。 |
| 74 | 医療分野の重要インフラ事業者となる「大学附属病院」等において、本基準案でセキュリティ対策の重責を担うとされる「経営層」とは、大学本体の「学長・理事」を指すのか、それとも医療機関の長である「附属病院長・副病院長等」を指すのか、ガイドライン等で明確にお示しいただきたい。<br>大学等の「親組織」自体は重要インフラに指定されていない一方で、その内部組織である附属病院が重要インフラに指定されている場合、両者間でセキュリティ基準に関する認識のズレが生じ、実務上の問題（予算や人員配置の権限による壁など）が発生することが懸念されます。こうした組織形態に対する方針や、親組織の理解を促すための施策等があればお示しいただきたい。 | 本統一基準及び安全基準等策定ガイドラインにおける「経営層」とは、「組織の代表者として統括責任を負う者（CEO、理事長、首長等）、組織の業務を執行する者、及び、もしあれば、取締役会・理事会等」を指すこととしており、これには重要インフラ事業者等による事業の運営及び意思決定に責任を有し、必要な資源配分等を決定できる立場の者が含まれることが想定されます。その上で、各分野・事業者において具体的に誰を指すのかは、今後検討を進める各分野の安全基準等の規定や実施計画等を踏まえながら、個別に判断されるものと考えています。 |
| 75 | サイバーセキュリティの観点から、重要インフラの基準を統一することは構わないが、重要インフラとされたもののうち、少なくとも安全保障にかかわる分野については、外国資本や外国人技術者等が関わることなく進めていただきたい。また、事業者や使用製品についても国内に限る条件を付与していただきたい。 | サプライチェーン・リスク対策の重要性に関する御意見として承ります。本統一基準では、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしております。 |
| 76 | 新規や既知脆弱性への積極的な対策をソフトウエア提供者などに求めるよう契約書に明記して欲しい。SBOMへの対応についても触れて欲しい。 | 御意見として承ります。本統一基準においては、重要インフラ事業者等に脆弱性管理を行うことを求めるとともに、サプライチェーン・リスク管理として、製品・サービスの調達・利用に当たり、サイバーセキュリティに関する要求事項を整理するよう求めています。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 77 | 重要インフラが外国資本や外国勢力により実質的に支配・影響を受けることは、サイバー攻撃以外の手段（情報流出、バックドア設置、緊急時のサービス停止指令など）による国家安全保障リスクを極めて高めることになる。本統一基準の策定を契機に、重要インフラの「所有・運営主体」に関する根本的な再定義を行うべきであり、具体的には、以下の点を強く要望する。<br><br>1. 重要インフラ16分野について、「公営化すべき分野」と「民営化は可とするが外資を一切排除すべき分野」を明確に再定義すること。<br>2.民営化が認められる分野においても、外国資本による株式取得・経営支配を厳格に排除する仕組みを導入すること。例:外国投資家による議決権割合の上限設定、重要設備・システム・データ管理に関する最終決定権の日本資本・日本人への確保、経済安全保障推進法との連携強化）<br>3. 統一基準の中に「サプライチェーン全体を通じた国家安全保障リスク管理」の観点を明記し、外国製ハードウェア・ソフトウェアの使用制限やベンダー審査の厳格化を義務づけること。 | 御意見として承ります。重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野であり、その安定的な提供の確保が極めて重要であると認識しております。政府としては、本統一基準の作成や運用等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。<br>また、サプライチェーン・リスク対策の重要性の観点において、本統一基準では、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしております。 |
| 78 | 本統一基準（案）が、重要インフラにおけるサイバーセキュリティ対策を分野横断的に底上げし、サプライチェーン全体を含めたリスク管理を強化する方向性については、重要インフラサービスの安定的な提供の観点から妥当であると考える。<br>一方で、クレジット分野においては、決済サービスの提供にあたり、国内ネットワークに加え、国際ブランドネットワークやクラウドサービス等の外部サービス事業者等が不可欠な構成要素となっており、これらはサービス継続性の観点から極めて重要な役割を担っている。<br>このため、対象範囲の整理にあたっては、個別事業者単位ではなく、決済ネットワークや接続基盤等、重要サービスを構成する機能単位での整理が重要であり、実施計画においてその考え方を明確化することが望ましい。<br>また、サプライチェーン管理については、委託先や供給者に加え、海外事業者を含めた対応が求められているが、特に国際的に展開されるサービス基盤については、我が国の重要インフラとしての位置付けを踏まえた対応の在り方について、より整理が必要と考える。<br>その際、当該基盤が重要インフラサービスに与える影響の大きさに鑑み、単に個別事業者の対応努力に委ねるのではなく、実効性あるセキュリティ確保の観点から、関係主体全体を視野に入れた枠組みや関与の在り方について検討がなされることが望ましい。<br>あわせて、制度の運用にあたっては、国内事業者のみに過度な負担が偏ることのないよう、公平性に十分配慮した枠組みとすることが重要と考える。 | 賛同意見として承ります。本統一基準の第３部では、サプライチェーン・リスク対策の重要性の観点から、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしております。また、第２部2.1.2「取り組むべき施策」では、「重要インフラ防護の適切な実施のためには、重要インフラ事業者等における、組織統治の一部としての障害対応体制の整備による、経営層 をはじめとする組織全体としての取組等の推進や、組織の壁を越えたサプライチェーン全体でのセキュリティの向上等を推進する必要がある」ことから政府機関として「障害対応体制の強化」を推進することとしております。御意見の内容については、安全基準等策定ガイドラインの作成を含め、今後の施策の検討に当たって参考とさせていただきます。 |
| 79 | 本統一基準（案）は、重要インフラ事業者を主対象としているが、第3部においては「サプライチェーンに関わる事業者等」にも対応を求める構成となっている。一方で、サプライヤーや外部委託先となる非重要インフラ事業者（例：商社、ITサービス提供事業者等）に求められる対応水準・責任範囲が必ずしも明確ではなく、結果として契約実務や対応コストの解釈にばらつきが生じる懸念がある。欧米（EU NIS2 指令、米国 NIST SP800-53/CSF 等）では、重要事業者とサプライヤーの責任分界点や最低限求めるセキュリティ要件が明示されている事例が多い。これを踏まえ、日本においても、安全基準等策定ガイドライン等において、重要インフラ事業者と直接関与する主要サプライヤー、一般的な委託・調達先といった区分ごとに、「最低限求められるセキュリティ対策の水準」や「契約で求めるべき主な要求事項（例：事故報告、脆弱性対応、監査協力）」を整理・明示することを検討いただきたい。 | 御意見として承ります。本統一基準第３部3.2.9「サプライチェーン・リスクマネジメント」に記載のとおり、サプライチェーン・リスクマネジメントへの対応は重要と考えております。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 80 | サイバー攻撃そのものへの対策だけでなく、企業経由でスパイ行為・破壊工作が行われる可能性にも配慮して、これらの施設には外資を入れないようにすべき。また、既に民営化されているものは、将来的には再国営化も視野に入れるべき。 | サプライチェーン・リスク対策の重要性に関する御意見として承ります。本統一基準では、サプライチェーン・リスク対策の重要性の観点において、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしております。 |

| | | |
|---|---|---|
| 81 | 我が国の重要インフラサービスを止めないことを目的に、重要インフラ事業者を守るサイバーセキュリティサービスについては、サービスが政府の定める基準を満たすか審査する制度を創設すべき。<br>例えば政府は以下のような基準を考慮すべき。<br>- サービスの技術的優位性<br>- サービスを構成する機器や運用等の経済安全保障の考慮<br>- サービスにおけるデータの取り扱い方法<br>- サービス提供している会社のガバナンス<br>今後策定される予定の「実施計画」等によって、重要インフラ事業者は当該審査をクリアしたサービスのみを利用／調達するように定め、一定基準以上のサイバーセキュリティ対策を効果的に実現すべき。<br>またこの制度により、重要インフラ企業によるサービス選定の負荷を低減するメリットも考えられる。<br>サイバーセキュリティサービスの品質基準については、現状経産省の情報セキュリティサービス審査登録制度が存在するが、当該制度は経済安全保障の観点、データの取り扱い及び会社のガバナンスについては触れられていないため、更新が必要と認識。 | サプライチェーン・リスク対策の重要性に関する御意見として承ります。御意見いただきました情報セキュリティサービス審査登録制度については、経済産業省が所管する制度となりますが、今後の施策の検討や実施の推進に当たって参考とさせていただきます。 |
| 82 | 経営層の関与について、意思決定・監督機能と実務運用機能の役割分担を明確化し、実効的なガバナンス確保につながる記載としていただきたい。 | 御意見として承ります。本統一基準では、経営層の責任により経営リスクとしてサイバーセキュリティリスクの管理等を求めることとしています。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 83 | 近年の攻撃動向を踏まえ、サプライチェーン・リスクの対象範囲について再委託先やクラウドサービス等を含む多層的な関係主体を考慮するとともに、調達・契約等を通じたセキュリティ要求事項の具体化（例：インシデント通知、監査対応等）や継続的な評価・管理（例：定期的な再評価等）の考え方を明確化いただきたい。 | 御意見として承ります。サプライチェーン・リスク対策の重要性の観点において、本統一基準では、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを行うこととしております。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 84 | 統一基準案では、経営層がサイバーセキュリティリスクを理解・評価できる体制を整備すること、CISO等の任命を経営層の責任で行うこと、必要な資源を投資として配分することが示されている。システム監査は、技術的な脆弱性診断やチェックリスト確認にとどまらず、経営層によるリスク認識、資源配分、委託先管理、インシデント対応、事業継続、継続的改善が有効に機能しているかを、独立した立場から評価するものである。<br>その点から経営層がサイバーセキュリティ対策の有効性、妥当性、継続的改善の状況について説明責任を果たすための保証・助言機能としてシステム監査は不可欠である。<br>また「自己点検」という表現は、実務上、監査を実施しない口実として使われる懸念がある。自己点検は、監査の代替ではなく、やむを得ない場合の暫定的又は補完的手段に限定すべきである。重要システムについては、公認システム監査人（CSA）等の専門性を有する者によるシステム監査の実施を、統一基準又は安全基準等策定ガイドラインに明記すべきである。 | 御意見として承ります。本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るものであり、その中で監査対応も定めておりますが、分野・事業者によっては、監査に係る要員や工数等の確保が難しい場合も想定されるところ、その場合であっても少なくとも自己点検を行うこととしております。ただし、それによって監査等が形骸化することなく自組織に有効なものとなるよう、実施方法の選択は、経営層の責任において行うこととしております。 |

| | | |
|---|---|---|
| 85 | 「サイバー脅威の深刻化が進む中、あらゆるサイバー攻撃から完全に防御することは困難であるところ、事前対応によるサイバー攻撃の防御・抑止のみならず、障害等が発生した際の影響を許容範囲内に抑制するレジリエンスの確保が必要」とあるとおり、サイバーセキュリティ対策においてゼロリスクの実現は困難であるも、これら備えは重要な課題である。<br>太陽光発電市場におけるPCSのように、海外勢がワールドワイドに製品バラエティを展開しており圧倒的な量産効果によって日本勢との価格差も大きくなっていることから、価格面や供給面で優位に立つ海外製品に頼らざるを得ない分野があるというのも実情。このような分野においては、実質的に特定の国の製品を排除するような運用は市場に要らぬ混乱をもたらす可能性が高く、エネルギー自給率向上や電源多様性確保の重要性の観点から国として然るべきリスク管理を行いつつ、安全が担保できるものは引き続き取り入れていくことができるようにしていただくことと共に、産業政策など措置によって我が国の産業競争力強化を更に進めて頂きたい。 | 本統一基準では、海外製品の規制ではなく、例えば、サプライチェーン・リスク対策の重要性の観点において、経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを行うこととしております。政府としては、本統一基準の作成等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |
| 86 | 適正な情報セキュリティマネジメントシステム（ISMS）を構築運用し、PDCAサイクルにより対策の有効性を確保することは、重要インフラを担う企業・組織に必須のことである。ISMSにおける対策の有効性を確実にするための評価（PDCAのCに該当）に自己点検では不十分であり、監査、それも公的監査制度に基づく適正な監査を経営層に行わせるべきである。更に、適正な監査を業界として定義し評価することで、監査に基づき経営層がサイバーセキュリティ対策に十分な説明責任を果たし、国民が安心できるようにすることが望ましい。<br>ついては、原文の（難しい場合には少なくとも自己点検）を削除し、適正な監査を実施する旨の記述を行うべき。 | 御意見として承ります。本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るものであり、その中で監査対応も定めておりますが、分野・事業者によっては、監査に係る要員や工数等の確保が難しい場合も想定されるところ、その場合であっても少なくとも自己点検を行うこととしております。ただし、それによって監査等が形骸化することなく自組織に有効なものとなるよう、実施方法の選択は、経営層の責任において行うこととしております。 |
| 87 | （意見内容）<br>可能な範囲と記載はあるが、セキュリティに関することを公開することでサイバー攻撃者に利用されることも想定されるのではないか。<br>（理由・背景）<br>具体的な技術的詳細の公表は控えるべきではないか。可能な範囲がないと判断し公表しないことも認められるのであれば問題なし。 | 本統一基準では、情報開示について、一律の公表を求める趣旨ではなく、攻撃者の攻撃を助長する可能性等を考慮の上、情報の開示の対象・内容や開示タイミングを適切に決定いただくことを想定しております。 |
| 88 | 「情報開示」における開示範囲については、事業者間で一定の基準を設け、開示内容の水準を揃えることを検討いただきたい。<br>統一基準では、「可能な範囲でサイバーセキュリティに関する取組を開示する」とされているが、その具体的範囲が各事業者の判断に委ねられる場合、開示内容にばらつきが生じる可能性がある。<br>こうしたばらつきは、開示情報に応じた攻撃対象の選別や、開示水準が相対的に低い事業者が狙われるといったリスクにつながることも懸念される。<br>また、クレジット分野では既にサイバーセキュリティに関する取組の公表に係るガイドライン（サイバーセキュリティ経営ガイドライン）が存在しており、開示範囲に係る考え方の基準になっているものと思料するため、既存の開示ルールとの整合を図り、分野内における取扱いの統一が確保されるよう検討されることを要望するもの。 | 御意見として承ります。具体的な開示範囲・内容について、一律の公表を求めることは現時点で想定しておらず、攻撃者の攻撃を助長する可能性等も考慮しつつ、事業者ごとに個別に判断いただくことを想定しております。また、その際には、御意見で言及いただいた安全基準等策定ガイドラインや「サイバー攻撃被害に係る情報の共有・公表ガイダンス 」（令和５年３月８日サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会）等も参照いただくことが想定されます。 |

| | | |
|---|---|---|
| 89 | 重要インフラ事業者が重要インフラシステムの機器やサービスを調達する際、セキュリティ上の懸念がある国やベンダーを事業者単独で判断することは情報収集能力の点からも非常に困難です。<br>そのため、政府において「リスクが高い」と判断される懸念事項やベンダーの基準、あるいは具体的なリスト（例：諸外国の禁輸リストに準ずるもの等）を明確に示していただくことを希望します。<br>また、同項目において「関係者間の理解共有」が謳われていますが、事業者側だけの努力では限界があるため、機器やサービスの供給側（ベンダー・メーカー）が果たすべきセキュリティ上の責務についても、より踏み込んだ規定、あるいは明確化を検討して頂きたく存じます。 | 御意見として承ります。サプライチェーン・リスク対策の重要性の観点において、本統一基準では、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしております。御意見の内容については、安全基準等策定ガイドラインの作成を含め、今後の施策の検討や実施の推進に当たって参考とさせていただきます。 |
| 90 | サイバーセキュリティに関する取り組みの情報開示は、社会的な信頼を得るために重要ですが、具体的にどのような項目をどの程度開示するのが適切か、判断に迷うケースがあります。<br>開示することが望ましいとされる具体的な項目例や、開示にあたっての留意事項などが示されれば、より透明性の高い情報公開が可能になると考えられます。 | 情報開示は、社会への説明責任やステークホルダーからの評価としての経営マネジメント等の観点の一方で、攻撃者の攻撃を助長する可能性等も考慮しつつ、個別に判断されるものであり、一律の公表を求める整理には馴染まないものと考えております。<br>サイバー攻撃被害に係る情報の共有・公表の具体的な方法や留意点等については、「サイバー攻撃被害に係る情報の共有・公表ガイダンス 」（令和５年３月８日サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会）等を参照の上、事業者ごとに個別に判断することを想定しております。 |
| 91 | 「重要インフラサービス障害に繋がる可能性のある事象」の検知に関し、現場のOT部門（運行・設備管理部門）においては、発生した事象が機器の故障なのか、サイバー攻撃に起因するものなのかを即座に判別することが極めて困難です。<br>専門的な知識を持つIT部門やCSIRTとの連携をスムーズにするためにも、現場レベルで初期判断が可能となるような、具体的な判断基準や切り分けのためのフロー図などを整備・共有いただくことを強く要望いたします。 | 御意見として承ります。本統一基準では、サイバーセキュリティリスクの管理について、サイバーセキュリティを担当する部署及び職員を決定するとともに責任及び権限を割り当てることとしており、その際には、ITシステムと制御システムの担当者間での適切なコミュニケーションを図ることが望ましいと考えております。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 92 | サプライチェーン・リスクマネジメントや製品調達において、原産国の属性による一律の制限や、一部の海外メーカーが直ちには取得困難な特定の国内セキュリティ認証（JC-STAR制度等）を必須要件とするのではなく、ネットワーク分離や運用統制等の代替措置を含めた、以下のような「システム全体での総合的なリスク管理」を許容する旨を、ガイドライン等で明確化していただきたい。<br>・機器単体の認証のみに依存するのではなく、ネットワークの物理的・論理的隔離といった「システム構成上の多層防御」によるリスク低減の評価<br>・厳格なアクセス制御、継続的な監視、迅速な脆弱性対応といった「運用面での統制」によるセキュリティの担保<br><br>分野ごとの実態や技術成熟度を踏まえ、「段階的なリスク低減措置」や「運用面での統制」を組み合わせることにより、「本質的な安全性」と「安定的なインフラ運用」を両立させるアプローチについても、今後の制度運用や「安全基準等策定ガイドライン」の整備の中で明確に許容・検討されることを強く期待する。 | 御意見として承ります。御意見の内容については、安全基準等策定ガイドラインの作成や各分野における安全基準等や実施計画の具体化検討を含め、今後の施策の検討や実施の推進に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 93 | 経営層によるリスク評価・モニタリングの実効性を担保するため、取締役会や経営会議等の場において、リスク報告の実施、管理状況の記録、およびモニタリング頻度の明確化を求めるべき。<br>リスクファイナンスの検討に際しては、インシデント発生時の業務停止期間や経済的損失を具体的にシミュレーションし、被害額想定に基づいた投資判断を経営層が行うべきである旨を明記すべき。 | 御意見として承ります。本統一基準では、経営層の責任により、経営リスクとしてサイバーセキュリティリスクの管理を行うことを求めていますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 94 | 供給者・委託先の把握、リスクアセスメントの実施にあたっては、クラウドサービス、物理機器、保守運用サービスといった「供給形態の特性」やリスクの大きさに応じた「リスクベース・アプローチ」によるサプライチェーンの依存関係のセキュリティ把握・対応を求めるべき。<br>また、供給者・委託先のセキュリティ対策の状況の把握の際には、すべての供給者・委託先に同一の調査手法による回答を求めるのではなく、クラウドサービスであれば第三者評価情報の活用や調査、物理機器であれば認証取得状況の確認など、既存の客観的指標を「把握」のエビデンスとして活用を推奨するなどの記載を提案する。 | 御意見として承ります。第３部2.9「サプライチェーン・リスクマネジメント」においては、サプライチェーン全体を俯瞰した上で必要なサイバーセキュリティ確保を行うこと、また、リスクや関与の程度に応じた供給者・委託先の対策実施状況等を想定しておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 95 | 重要インフラ防護においては、サイバー攻撃への対策のみならず、設備運営主体、委託先企業、クラウド基盤、サプライチェーン等を通じた情報流出・妨害工作・依存性リスクにも配慮する必要がある。<br>特に重要インフラを担う事業者については、<br>◎資本構成<br>◎外国資本による影響力<br>◎業務委託先<br>◎機器調達<br>◎ソフトウェア供給網<br>等を含めた経済安全保障上の観点が不可欠であると考える。 | 御意見として承ります。本統一基準では、経営層の責任において、経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしておりますが、御意見の内容については今後の施策検討に当たって参考とさせていただきます。 |
| 96 | 重要インフラ16分野におけるサイバーセキュリティ対策の統一基準の策定を強く支持する。国家を背景とした深刻なサイバー脅威に対し、より積極的な関与に転じる方針は極めて重要である。しかし、真のレジリエンス（任務保証）を確保するためには、システム上の防護だけでなく、重要インフラの所有・運営主体の安全性が大前提となる。安全防護の観点から、以下3点のような外資の排除やインフラの公営化の再定義について、政府の施策基準に明確に盛り込むべき。<br><br>1. 所有・運営主体における外資排除と公営化の再定義<br>2. 行政サービスや上下水道の実質民営化プロセスの見直し<br>3. サプライチェーン・リスクにおける資本・所有構造の管理 | 重要インフラ分野とは、他に代替することが著しく困難なサービスを提供する事業が形成する国民生活及び経済活動の基盤であって、その機能が停止し、又は低下した場合に国民生活又は経済活動に多大な影響を及ぼすおそれが生ずるものとして、業種ごとに指定する分野であり、その安定的な提供の確保が極めて重要であると認識しております。<br>その上で、サプライチェーン・リスク対策の重要性の観点において、本統一基準では、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを求めることとしております。<br>政府としては、本統一基準の作成等を通じて、重要インフラのサイバーセキュリティの確保に一層取り組んでまいります。 |

| | | |
|---|---|---|
| 97 | 「供給者・委託先のセキュリティ対策の状況の把握」が求められているが、把握した内容を誰が・どのような形で集約・確認するかの仕組みがない。<br>特定の供給者に対する制裁・輸出規制・法的強制等によりサービスが突然停止または制約される事態が生じた後に、各事業者は把握していたが所管省庁には全体像がなかったという状況が生じれば、行政の説明責任が問われる構造になる。<br>この種の事態は、不正アクセスやマルウェアといった技術的な攻撃行為とは異なり、攻撃者が存在しないまま構造的依存の断絶として生じる。現文書のインシデント概念はこの種の事態を十分に射程に収めていない。<br>供給元の法的管轄・実効支配の所在を含む依存構造の把握結果を、実施計画の中で所管省庁が定期的に集約・確認する仕組みを明記することを求める。2027年春夏の実施計画策定段階での具体化が可能である。 | サプライチェーン・リスク対策の重要性に関する御意見として承ります。本統一基準では、重要インフラ事業者等において経営リスクとしてのサイバーセキュリティリスク管理、サプライチェーン・リスクマネジメントを行うこととしておりますが、御意見の内容については今後の施策の検討や実施の推進に当たって参考とさせていただきます。 |
| 98 | 重要インフラの安全性は、外部からの基準移植によってではなく、当該インフラが根ざす地域の実情と技術的蓄積から生成される部分が大きい。<br>日本は地震・台風・水害という災害列島の経験から、インフラの冗長性・地域分散・自律復旧を安全設計の原則としてきた。特定拠点への集中依存が脆弱性を生むという認識は、この経験に根ざしている。<br>サイバーセキュリティにおいても同じ原則が成立する。特定の技術基盤・プラットフォームへの集中は、サイバー攻撃においても、制裁・輸出規制・法的強制による供給断絶においても、同様の単一障害点リスクをもたらす。攻撃者の有無にかかわらず、集中依存という構造そのものが脆弱性である。<br><br>安全基準等および安全基準等策定ガイドラインの策定にあたり、技術基盤の多様性と地理的・管轄的分散を安全性の積極的要件として明示することを求める。これは特定の事業者・国の排除を意図するものではなく、集中依存という構造的脆弱性を制度的に可視化し、自律的な選択を保障するものである。<br>あわせて、統一基準の適用範囲を必要最小限に限定し、地域・現場の判断が入る余地を制度的に確保することを求める。全てを基準で覆うことは想定外の事態への応答能力を損ない、かえって重要インフラの脆弱性を高める。基準の改定時には適用範囲の拡大を厳格に審査し、現場から適用除外を申請できる経路を設けることを併せて求める。 | 御意見として承ります。本統一基準では、経営層から担当者層まで、それぞれが役割と責任を果たし、リスクベースの考え方に基づき、重要インフラのサイバーセキュリティ確保に取り組むことが重要であるとの考え方を示すとともに、各分野の安全基準等における対象範囲の設定に当たっては、重要インフラサービスの安全かつ持続的な提供を実現する観点から、各分野において、重要インフラサービスを提供するために必要な情報システムや、重要インフラサービスに与える影響の度合い、さらにはサプライチェーン・リスクなどを踏まえ、リスクベースの考え方に基づく適切な範囲を設定するとしております。 |
| 99 | 重要インフラ事業者におけるサイバーセキュリティは、国民生活、社会経済活動及び国家安全保障に重大な影響を及ぼし得ることから、内部監査は単なる自主点検ではなく、経営レベルでセキュリティ対策の有効性を継続的に確認・改善するための重要な統制活動として位置付ける必要があると考える。本統一基準（案）では、「監査（難しい場合には少なくとも自己点検）」との記載に留まっているが、重要インフラ向け基準としては、監査の独立性、頻度、経営関与、改善フォローまで含め、より具体的な要求事項を明記することが望ましい。<br>特に、リスクベースに基づく定期監査（少なくとも年1回以上）、重大システム変更や重大インシデント発生時の追加監査、監査結果の経営層報告、是正措置のフォローアップ、OT／制御系を含む重要システムやサプライチェーンを対象とした監査等を要求事項として明確化すべきである。<br>3.2.6「監査・モニタリング」において、<br>例えば、制御系ネットワーク分離の有効性確認、委託先に対するアクセス権管理状況の監査、バックアップからの復旧訓練結果の検証、演習後の改善状況確認など、実効性確認を伴う監査が重要となる。また、レジリエンス強化の観点から、クリティカルな脆弱性に誘引される最新の脅威や攻撃手法が確認された場合には、それらを踏まえたインシデント対応計画、事業継続計画、復旧計画等の見直し状況についても監査対象とすることが重要である。<br>さらに、「自己点検」を監査の代替的手段として位置付けるのであれば、今後策定されるガイドライン等において、その実施条件や評価方法を具体化することが望ましい。例えば、内部監査部門や情報セキュリティ委員会等が自己点検結果を厳格に評価し、重大な課題又は不備が確認された場合には、内部監査人による詳細監査を実施するなど、実効性を担保する運用指針を整備することを推奨する。 | 御意見として承ります。本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るものであり、その中で監査対応も定めておりますが、分野・事業者によっては、監査に係る要員や工数等の確保が難しい場合も想定されるところ、その場合であっても少なくとも自己点検を行うこととしております。ただし、それによって監査等が形骸化することなく自組織に有効なものとなるよう、実施方法の選択は、経営層の責任において行うこととしております。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第３部　安全基準等において規定されるべき事項／識別」に係る意見** | |
| 100 | 重要インフラのサイバーセキュリティ対策において、脆弱性対策の重要性は十分に認識されているものの、現場においては「認識されているにもかかわらず対応できない」という構造的課題が存在しているため、単なる対策の提示にとどまらず、確実に実施される仕組みの制度化が必要と考える。特に、定期的な脆弱性対応を強制力をもって実施できる枠組み（定期脆弱性対応日）の導入を提案する。 | 御意見として承ります。脆弱性対策については、「3.3.6 脆弱性の管理」に規定しておりますところ、御意見の内容については、安全基準等策定ガイドラインの作成やPDCAサイクルの仕組みの具体化を含め、今後の施策の検討に当たって参考とさせていただきます。 |
| 101 | サイバーセキュリティに関して根拠法や省庁横断的なプラットフォームの設置による一元的サイバーセキュリティの管理の枠組みを希望する。（NACCS/府省共通ポータルの枠組みに類似したものをイメージ。）<br>各根拠法で求められる a. 政府への届出 b.（インシデント対応などの）報告・連絡 c. 政府から対象事業者への情報共有　これらを一元的に対応できるプラットフォームがあることで、、重要な情報共有や通知などの抜け漏れがなくなるほか、届出では同じ情報が省庁横断的に共有され、手続き面でも簡素化や手戻り、二重投入がなくなるものと想定。 | 御意見として承ります。重要インフラ事業者等による報告や政府機関による情報共有等のあり方に関しては、事業者の過度な負担とならないよう配慮しつつ、検討を進めてまいります。 |
| 102 | 3.3.4 リスクアセスメントにペネトレーションテストやTLPTを記載いただきたい。<br>特にTLPTは、金融業界を中心にレジリエンスの向上に有効な手法として一定の評価がされており、重要インフラ事業者への導入を推進するためにも取り組むべき施策の一つに挙げていただきたい。 | 本統一基準では、任務保証の考え方に基づくリスクアセスメント（リスクの特定・分析・評価）の実施や脆弱性リスクに応じた対策を求めることとしているところ、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 103 | 重要インフラにおける外部接続点・操作経路を安全管理上のインターフェースとして明確化し、入出力・権限範囲・通信先・ログ取得・承認条件等を管理対象に含めるべき。<br>これは共通インターフェース管理によって障害や攻撃に対する代替性・拡張性・追跡可能性を高めるとともに、教育・運用上の負担低減を含む関係者間の共通認識を形成することを目的とする。<br>また、今後重要インフラの運用に組み込まれ得るAIについて単体のサービスやモデル性能だけで評価するのではなく、参照する情報・接続するツール・実行可能な操作・外部通信・ログ取得を含む「アーキテクチャ全体の構成要素・接続境界・権限境界を明確化して管理することが必要である」という趣旨も含む。<br><br>具体的には、以下2つの点を軸として検討を要望する。<br>- 重要インフラにおける外部接続点・操作経路を安全管理上のインターフェースとして定義すること<br>- 生成AI及びAIエージェントの活用も視野として、資産管理・権限制御・ログ管理・人間承認等の対象を明確化すること | 本統一基準では、ネットワーク構成図やデータの流れ図等も含む資産管理や、アクセス制御やログの取得等を求めていますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 104 | 以下の2点について規定の明確化・強化を求める。<br>（1）セキュリティ対策ソフトウェアの稼働確認に関する規定の追加<br>現行の規定では「資産目録を作成・維持管理する」にとどまっているが、組織が必須と定めたセキュリティ対策ソフトウェア（マルウェア対策、EDR等）について、ネットワーク上の全端末においてインストールおよび稼働していることを継続的に確認・検証できる仕組みを整備することを明記するべきである。<br>（2）資産目録の「常時監視」に基づく維持管理の明確化<br>現行の記載にある「維持管理」について、月次等の定期的な更新では有事における情報鮮度が不足する懸念がある。資産目録は常時監視（継続的な自動検出・更新）を前提とした維持管理を行うことを基本とするよう、規定を強化するべきである。 | 御意見として承ります。御意見の箇所は「資産の管理」に係る対策事項（3.3.1）ですが、本統一基準では、マルウェアからの保護（3.4.4.4）や監視・分析体制の整備（3.5.1）、継続的監視の実施（3.5.2）についても定めております。 |
| 105 | ホルムズ海峡問題で、石油や港湾、航空等の海外重要インフラ依存が日本の重要インフラへ大きな影響を与えている。関係国の政府や重要インフラ事業者との情報共有や連携強化を推進するような記載が欲しい。 | 重要インフラを取り巻く社会環境やサイバーセキュリティ動向等を踏まえた対応が重要であると考えており、本統一基準では、政府機関は、重要インフラ事業者等との緊密な情報共有体制の維持・強化や各国政府等との情報共有等、協力・連携の強化を推進することとしております。 |

| | | |
|---|---|---|
| 106 | サイバー対処能力強化法に基づく新たな官民連携の協議会は、この情報共有体制とは位置づけが違うのか。 | 本統一基準における情報共有体制は、重要インフラサービス障害に係る情報及び脅威や脆弱性情報を幅広く共有し、より多くの重要インフラ事業者等が速やかな防護策を講じるための官民・分野横断的な枠組みとなります。<br>一方、新たに立ち上げられる官民連携の協議会は、サイバー対処能力強化法に基づき、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の情報共有と対策の協議を行うことを目的とし、基幹インフラ事業者とベンダー等の一部で構成される枠組みとなります。 |
| 107 | 重要インフラに関連する設備は長期利用を前提とするものが多いため、基準改定時における既存設備への適用について、経過措置や優先順位の考え方が示されると実務上有益と考える。また、新設設備と既存設備の取扱いの違いや、更新計画に応じた段階的対応の考え方についても整理が示されることで、実務上の判断に資するものと考える。 | 御意見として承ります。例えば、本統一基準の第３部3.3.4「リスクアセスメント」において、「組織状況と資産を踏まえ、任務保証の考え方に基づくリスクアセスメント（リスクの特定・分析・評価）を実施」するとの考え方を示しておりますが、御意見の内容については今後の施策の検討や実施に当たって参考とさせていただきます。 |
| 108 | デジタル環境の高度化を踏まえ、資産管理の対象範囲について、従来のIT資産に加え、クラウド設定やAPI、認証情報等の多様な情報資産を含む考え方を明確化いただきたい。 | 御意見として承ります。本統一基準では、情報システム、ソフトウェア、情報等の資産の特定等を行うこととしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 109 | 効果的なリスク低減の観点から、脆弱性対応における優先順位付けの基本的な考え方（例：資産重要度や外部露出状況の考慮等）を明確化いただきたい。 | 御意見として承ります。本統一基準では、脆弱性情報を踏まえ、運用中の情報システムに対する影響の有無を確認しつつ、情報システムへのパッチ適用に関する作業方針・内容の確立等を行うこととしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 110 | （意見内容）<br>定期的な脆弱性診断を実施と記載があるが、実施頻度や実施方法が不明確である。脆弱性診断の実施にノウハウが必要な場合は、外部に委託する必要がある。<br>（理由・背景）<br>現場などでは脆弱性診断に関する専門知識を持つ社員が不在のため。<br>大きな負担なく、容易に実施できる内容であれば問題なし。 | 本統一基準では、リスクアセスメントの結果等を踏まえて定期的に脆弱性診を定期的に行うことを求めていますが、システム運営上の制約等により脆弱性診断が困難である場合には、リスクに応じた措置を講じることとしております。 |
| 111 | 脆弱性の影響確認およびパッチ適用の実効性を担保するため、ソフトウェアの構成情報を管理する「SBOM（ソフトウェア部品表）」の作成・維持管理、およびそれを用いた脆弱性情報の照合・管理を、標準的な運用手法として明記することを提案する。 | 御意見として承ります。本統一基準では、脆弱性の管理に当たって、情報システムへのパッチ適用に関する作業方針・内容を確立することを定めています（第３部3.3.6）が、例えば、ソフトウェアの調達において透明性の確認を必要とする場合はSBOMの作成及び提供を調達先に求めることも想定されます。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第３部　安全基準等において規定されるべき事項／防御」に係る意見** | |
| 112 | サイバー攻撃が物理的な破壊活動や自然災害と組み合わされる「ハイブリッド事態」を想定し、システム上のログ（ITデータ）だけでなく、現場の水位計や目視による物理的状況（OTデータ）との「照合（ファクトチェック）」を検知・分析のプロセスに明記し、データの改ざんに惑わされない「感知能力」の向上を義務付けるべき。 | 物理的な破壊活動や自然災害への対策も重要と考えており、本統一基準では、入退、装置、データ等の管理やネットワークのセキュリティ確保等、物理的な対応を含むセキュリティ対策や災害対策を講じることとしています。 |
| 113 | サプライチェーンの末端（零細企業）や地方の消防・救急等の現場は、予算や人員の制約から本基準の遵守が困難。単なる努力義務や助言に留まらず、国による「感知」ツールの直接提供や、物理・サイバー両面を想定した「抜き打ち的な官民合同訓練」への参加支援など、実効的なリソース投入をセットで検討すべき。 | 御意見として承ります。現在行っている全重要インフラ分野を対象とした「全分野一斉演習」等の演習機会の確保を引き続き実施するとともに、本統一基準第２部2.1.2「取り組むべき施策」に記載の「安全基準等の浸透に向けた取組」の実施等を通じて、重要インフラ事業者等におけるサイバー事案対処の実効性確保に努めてまいります。 |
| 114 | 海外クラウドサービスへの集中リスクへの対応として、統一基準の第3部において、以下を安全基準等に含めるべきことを明記すべき。<br>①クラウドサービスの依存度評価（事業者の所在国、法的管轄、制御機能の所在を含む）の実施。<br>②有事を想定した代替運用手順の策定。<br>③重要度の高いシステムにおけるマルチクラウドまたは自営基盤の維持の検討。 | 御意見として承ります。クラウドサービス利用時の対策については、「3.4.7 クラウドサービス利用時の対策」に規定しておりますところ、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 115 | 3.4.3.2 暗号を活用した情報管理<br>暗号の利用方針や暗号鍵の管理方針（危殆化時の対応を含む。）を策定する。<br>という記載について、データの暗号化管理をするということはデータベース暗号化を必須要件とするという理解でよいか。<br>ランサムウェアへの二重脅迫を想定する場合、国防、社会的影響を想定しデータ暗号化は必須要件とするべき。 | 御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 116 | 国防に影響があると国・社会的な影響が大きいシステム（特に運用リスクの大きい制御系システム）は米国法の影響を受けるクラウドサービス（一部の米国ハイパースケーラ）を制限する必要があるのでは。基準案の3.4.7にはそういった運用主権の担保の観点からの記載が抜けている。 | 御意見として承ります。本統一基準では、重要インフラ事業者等におけるデータのセキュリティ対策として、インターネットを介したサービス（クラウドサービス等）を利用する際には、国外の法令等の存在について留意することとしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 117 | 「インフラストラクチャ（ネットワーク等）の対策」のタイトルは、「ネットワーク等の対策」で良いのでは。インフラストラクチャの示す内容が分からない。インフラストラクチャの説明もない。 | 「インフラストラクチャ」は、ネットワークを含む通信基盤・設備を想定しております。 |
| 118 | ・「良質なパスワード」を「ランダム生成されたパスワード」に変更（利用者にとっての「良質」とは覚えやすいことであるため）<br>・「多要素認証」を「多要素認証または電子署名」に変更<br>・「活用等により、」のような提案ではなく、「を導入し、」として強制させる。<br>・出荷時に設定された初期パスワードを使用させないことを追記する。<br>・「アクセスを制限する」を「アクセスを必要最小限の使用者に制限する」に変更 | 御意見として承ります。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 119 | クラウドサービスや外部委託先へデータを預ける際の確認事項として、ISMS等の国際規格認証の取得状況、SOC2等の監査レポート、ISMAP等の公的評価制度等、第三者性のある認証・監査・評価を活用することを明記してはどうか。 | 御意見として承ります。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 120 | バックアップデータの保護に関して、「バックアップ元と異なるセグメントやオフラインで保管する」ことに加え、「バックアップ取得用の通信を一方向のみに制限する」「世代管理を行う」など、より踏み込んだネットワーク分離やデータの不変性（イミュータビリティ）の確保を要件として明記するのはどうか。 | 御意見として承ります。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 121 | 「重要インフラ統一基準（案）」の実効性をさらに高める観点から、セキュアDNSの導入に関する意見を提出する。これらの対策はすでに技術的な有効性が実証されているものであり、「国家安全保障戦略（令和4年12月16日閣議決定）」に掲げられた、サイバー安全保障分野での対応能力を欧米主要国と同等以上に向上させるという目標に直接的に合致するもの。<br>意見1は本統一基準第３部 3.4.6.1「通信のセキュリティ」への追加意見、意見2,3,4,5はそれぞれ詳細な機能要件として記載しており、必要に応じて安全基準等策定ガイドラインへの反映を想定している。<br><br>意見１：3.4.6.1節にセキュアDNS要件を明示的に追加すること<br>意見２： PDNSを推奨セキュリティ管理機能として明記すること<br>意見３：DNSSECおよびDNS暗号化（DoT/DoH/DoQ）を基本的なプロトコル保護として必須化すること<br>意見４：専用かつ論理的に分離されたDNSインフラストラクチャを義務付けること<br>意見５：検知とインシデント報告にDNSおよびDHCPのログデータを組み込むこと | 御意見として承ります。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 122 | 不正アクセス対策の強化の観点から、重要性に応じた強固な認証手段（例：多要素認証等）を原則とする方向性を明確化いただきたい。 | 御意見として承ります。本統一基準では、情報やシステムの重要度に応じた認証等を求めていますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 123 | アクセス制御の実効性向上の観点から、特権的な権限の管理（例：特権IDの制御や利用状況の監査等）に関する考え方を明確化いただきたい。 | 御意見として承ります。本統一基準では、情報やシステムの重要度に応じたアクセス制御等を行うこととしていますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 124 | インシデント対応及び検知能力の向上の観点から、ログの保全性・完全性を確保するための基本的要件（例：改ざん防止や適切な保管等）の方向性を明確化いただきたい。 | 御意見として承ります。本統一基準では、セキュリティの確保に必要なログを記録・管理するとともに、改ざん・消去されないよう管理することとしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 125 | レジリエンス確保の観点から、バックアップの有効性（例：復元可能性や耐改ざん性等）を確保するための方向性を示すことが望ましい。 | 御意見として承ります。本統一基準では、システムイメージやデータ等に対するバックアップの方針・手順の整備や、バックアップデータの適切な保管検討等を行うこととしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 126 | クラウド利用の拡大を踏まえ、責任分担の明確化に加え、利用者側の管理責任（例：設定管理やアクセス制御等）に関する基本的な考え方を示すことが望ましい。 | 御意見として承ります。本統一基準では、クラウドサービス利用時に、責任共有モデルを理解するとともに、サービス提供者との責任範囲等を明確にする等定めていますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 127 | クラウド利用終了時のリスク低減の観点から、データの取扱い（例：データ消去や残存リスクへの対応等）に関する基本的な留意事項を明確化いただきたい。 | 御意見として承ります。本統一基準では、クラウドサービス利用終了時におけるデータの取扱い（論理的な廃棄）について確認等を行うこととしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 128 | 分野特性を踏まえ、特に金融・決済分野においては、可用性に加えデータ完全性や不正防止の観点も重要であることを明確に位置付けることが望ましい。 | 御意見として承ります。本統一基準では、情報の分類、システムのリスクアセスメントに応じたデータ管理等を行うこととしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成や各分野における安全基準等や実施計画の具体化検討を含め、今後の施策の検討に当たって参考とさせていただきます。 |
| 129 | （意見内容）<br>国内外の法令や評価制度等の存在について留意とあるが、国外の法令や評価制度等はどのような観点で留意する必要があるのか示していただきたい。<br>（理由・背景）<br>職場内に国外の法令や評価精度等を調査するノウハウがないため。 | 今後策定する安全基準等策定ガイドラインにおいて、所管省庁等が安全基準等を策定するに当たって参照するための詳細事項を記載する予定です。 |
| 130 | 重要インフラシステムの多くは、安全確保のために外部ネットワークから遮断された閉域網で運用されています。<br>こうした特殊な環境下でマルウェアを検出し、適切にアラートを発報する仕組みを整えることは、コストや運用負荷の面で大きな課題となっています。<br>各事業者が手探りで対応するのではなく、閉域網の特性を考慮した低コストかつ運用しやすい標準的な構築事例（ベストプラクティス）を提示いただくことが可能であれば、業界全体の底上げに繋がると考えます。 | 御意見として承ります。御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただくとともに、関係省庁間でベストプラクティスを共有するなどして、分野・事業者横断的なセキュリティ水準の底上げを図ってまいります。 |
| 131 | クラウドサービスの利用にあたっては、責任共有モデルに基づき、利用者が責任を持つ範囲（設定管理、データ保護、AI利用管理等）について、導入時のみならず、運用フェーズにおいても継続的にリスク状況を可視化する体制を整えるべき。<br>特に、既存サービスへのAI機能の追加といった仕様変更や、新たな脆弱性の発生を適時把握できるよう、外部の評価情報や自動管理ツール等を活用した、動的なリスクモニタリングを実効性ある管理手法として位置づけることを提案する。 | 御意見として承ります。本統一基準では、クラウドサービス利用時に、責任共有モデルの理解や、サービス提供者との責任範囲等の明確化、サービス使用が変わる際の影響の確認等を定めています（第３部3.4.7）が、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 132 | 「責任共有モデルを理解し、クラウドサービス提供者との責任範囲等を明確にする」としているが、相手が外国法に服する事業者である場合、当該事業者が自国政府の法的命令に服してデータの開示・遮断等を行ったとき、日本の行政が実効的な関与をする手段を持たない可能性がある。その場合、行政の実効的な対処ができないまま説明責任だけが残る。<br><br>これは技術的なサイバー攻撃への対処の問題ではなく、法的管轄の外側で起きる構造的な問題である。責任共有モデルの理解だけでは対処できない性質を持つ。<br><br>経済安全保障推進法における基幹インフラ設備の事前審査制度との整合性を踏まえ、重要インフラの中核システムに用いるクラウドサービスについて、日本国の法的管轄が実効的に及ぶことを確認するプロセスを安全基準等に盛り込むことを求める。 | データのセキュリティ対策に当たっての留意点に係る御意見として承ります。本統一基準では、国内外の法令や評価制度等の存在について留意した上で、クラウドサービス等のインターネットを介したサービスを利用するよう求めています。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第３部　安全基準等において規定されるべき事項／検知」に係る意見** | |
| 133 | 効果的な監視の実現のため、重要度に応じた監視対象や優先度の考え方（例：認証失敗や特権操作等の重要イベント）を示すことが望ましい。 | 御意見として承ります。本統一基準では、重要インフラサービス障害に繋がる可能性のある事象（サイバー攻撃、情報システムの異常状態等）を早期検知するための監視・分析体制の整備を行うこととしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 134 | （意見内容）<br>早期検知するための監視・分析体制を整備と記載があるが、どのような体制が求められるかなどレベル感を示していただけるか。<br>（理由・背景）<br>内容次第では現行体制で対応が難しいため。 | 御意見の内容については、安全基準等策定ガイドラインの作成を含め、今後の施策の検討に当たって参考とさせていただきます。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第３部　安全基準等において規定されるべき事項／対応及び復旧」に係る意見** | |
| 135 | 本基準において、インシデント発生時に国が迅速に事実関係を認定し、公式に情報を発信する「事実の番人」としての役割を強化すべき。また、119番通報への妨害（電話爆撃）等の事態において、消防・救急が迅速に「本物の通報」を判別し、国民の不安を解消できる具体的な運用基準を策定すべき。 | 御意見として承ります。サイバー攻撃が行われた場合には、関係省庁と連携しつつ迅速に状況を確認し、攻撃の特性や深刻度に応じ、被害のさらなる拡大や深刻化を防ぐため、必要な情報提供や注意喚起等を行ってまいります。 |
| 136 | IT-BCPは、IT-BCP/OT-BCPとしては。脚注も変更要。 | 本統一基準における「情報システム」の定義は、「事務処理等を行うITを用いたシステム、フィールド機器や監視・制御システム等の制御系のシステム等を含むシステム全般」であり、OTの制御システムもこの定義に含まれることとなります。文中ではIT-BCPを例示してはいるものの、ご指摘のとおり、OTの制御系システムも含めた業務継続の観点が重要であると認識しており、OT-BCPは「事業継続計画等」に含むものとして整理しております。 |
| 137 | 危機管理にはメディアや広報など社会コミュニケーションについても触れて欲しい。 | 危機管理やインシデント発生時におけるコミュニケーションの重要性に関する御意見として承ります。本統一基準では、インシデント発生時における組織内外との情報共有や危機管理における事業継続計画等に従った初動から復旧までの対応を求めることとしております。 |
| 138 | インシデント発生時、基幹インフラ事業者は復旧に経営資源を集中させるべき危機的な状況にある。<br>その際、基幹インフラ事業者の保守を行っているサイバーセキュリティベンダーは、平時より当該事業者へセキュリティサービスを提供しており、インシデント発生状況を詳細に把握し、正確に状況報告が可能である。加えて、専門家の観点で、他事業者のサイバー防御に資する情報を選別して報告することが可能であるというメリットがある。<br>また、逆にインシデント報告に対する官からのフィードバック情報をサイバー防御にタイムリーかつ効果的に反映するためのサイバーセキュリティベンダーによる技術的支援が可能となる。<br>インシデントの代理報告を認めるのは、一定程度の技術的・ガバナンス的基準が満たされたサイバーセキュリティベンダーとすべきであり、「１．サイバーセキュリティサービス審査制度を創設すべき」に記載したサイバーセキュリティサービス審査制度に合格したセキュリティベンダーとすべき。<br>なお、重要インフラ事業者の業法等に基づくインシデント報告義務においても、サイバーセキュリティサービス審査制度に合格したベンダーからの代理報告を認めることで、基幹インフラ事業者の場合と同様の効果が期待できる。 | 御意見として承ります。なお、本意見がサイバー対処能力強化法に基づくインシデント報告義務に係るものであれば、基幹インフラ事業者は同法に基づいて適切に報告いただく必要があります。 |
| 139 | 実効的な復旧対応を可能とする観点から、重要サービスの優先度に応じた復旧目標（例：RTO/RPO等）の設定に関する考え方を明確化いただきたい。 | 御意見として承ります。本統一基準では、事業継続に及ぼす影響を踏まえ、事業継続に関する悪影響を許容範囲に抑制するための初動から完全復旧までの対応方針の整備等を行うこととしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |

| | | |
|---|---|---|
| 140 | 迅速かつ適切な情報共有の観点から、インシデント報告の判断基準やタイミング（例：初動報告と確報の区分等）を明確化するとともに、影響範囲が未確定な段階での速報と後続報告を前提とした運用の在り方についても考慮することが望ましい。 | 御意見として承ります。本統一基準では、インシデントについて関係法令に基づく報告や、組織内外との情報共有等を行うこととしております。御意見の内容については、安全基準等策定ガイドラインの作成や、重要インフラ行動計画に基づく情報共有の手引書見直しを含め、今後の施策の検討に当たって参考とさせていただきます。 |
| 141 | 現在の安全保障環境においては、従来型のサイバー攻撃のみならず、通信妨害、海底ケーブル攻撃、衛星利用妨害、サプライチェーン侵害、情報窃取、民間企業を経由した浸透工作等を含む「ハイブリッド型脅威」への対応が重要となっている。特に近年は、民生インフラと防衛インフラの境界が急速に曖昧化しており、港湾、空港、通信、電力、クラウド、物流、衛星通信等の民間インフラが、自衛隊・海上保安庁・在日米軍等の運用基盤としても機能する状況となっており、本統一基準においても、公開可能な範囲において、<br>◎防衛省・自衛隊等との連携体制<br>◎有事を想定した官民共同対応<br>◎防衛関連施設周辺インフラとの整合<br>◎地方自治体を含めた統合的危機管理体制<br>等について、一定の基本的方向性を明示する必要があると考える。<br><br>防衛上の機密性に配慮し、具体施設名や詳細運用を公開文書に記載しないこと自体は理解できるが、防衛分野との制度的連携の考え方が見えにくいことは、地方自治体やインフラ事業者側における危機管理上の不安要素にもなり得る。 | 政府機関としては今後、官民で連携しつつ、本統一基準等を通じて、障害対応体制の強化等を推進し、深刻化するサイバー脅威に対する重要インフラの一層の防護を図ってまいります。 |
| 142 | どれほど高度なサイバー防衛を施しても、大規模な災害やインフラの複合的機能不全（ブラックアウト）は回避できない。その際、電子制御や燃料供給に依存する現代の交通網は完全に麻痺する。<br>この最悪のシナリオにおいて、外部のエネルギーやネットワークに依存せず、個人の自律的な移動と物流を維持できる唯一の手段は「自転車」である。重要インフラ統一基準はデジタル領域に偏重せず、ローテクでありながら最も強靭な生存インフラとして、都市の無電柱化（電線の地下構造物化）と一体となった「完全分離型の自転車専用空間の確保」を評価指標に組み込むべきである。 | サイバーインシデントが事業継続に及ぼす影響を踏まえ、事業継続に関する悪影響を許容範囲に抑制するといった観点は重要であり、本統一基準では、事継続計画等へサイバーセキュリティを組み入れるなど、インシデントへの対応及び復旧体制の構築を求めることとしております。 |
| 143 | 現在の重要インフラ統一基準は、高度化するサイバー攻撃に対して「防御壁を厚くする」という発想に偏重している。しかし、セキュリティ対策の本質は、常に攻撃側が先手を持ち、防御側が後手に回る終わりのない「イタチごっこ」である。どれほど堅固なシステムを構築しても、技術的・人為的限界により「必ず突破される」という前提に立つべきだ。<br>このイタチごっこの限界を克服するために必要なのは、単一の強固なシステムではなく、侵害された際に即座に代替可能な「市場の流動性（モビリティ）」と「冗長性」である。<br>現在、通信業界等で見られる大手事業者による市場の寡占、および不透明な審査基準（いわゆる総合的判断）や複雑な契約による消費者の囲い込みは、国民が迅速に他社回線へ避難する「選択の自由」を奪っている。これは単一障害点（Single Point of Failure）を国家規模で放置しているに等しい。重要インフラ基準においては、事業者が消費者を不当に拘束する商慣習を排除し、有事の際にも国民が「繋がる自由」を行使できる流動性の確保を最重要要件として明記すべきである。 | 本統一基準では、事業継続計画等にサイバーセキュリティを組み入れるなど、インシデントへの対応及び復旧についても求めることとしています。 |

| | | |
|---|---|---|
| 144 | サイバー攻撃や大規模災害によって、電力、通信、そして自動車や鉄道などの交通インフラが同時に機能停止（ブラックアウト）する事態は十分に想定される。その際、電子制御や燃料供給に依存する現代のモビリティは一瞬にして硬直化し、道路網を塞ぐ障害物へと変貌する。<br>このような「最悪のシナリオ」において、唯一機能し続けるのは、外部のエネルギーや通信ネットワークに依存しない「個人の自律的な移動手段（自転車）」である。<br>重要インフラ統一基準は、ハイテクなデジタル防衛に終始するのではなく、ローテクでありながら最も強靭な「生存のための物理インフラ」として、自転車の活用推進を位置づけるべきである。具体的には、都市の強靭化（レジリエンス）の評価指標として、災害時に自動車に依存せず移動・物流を維持できる「完全分離型の自転車専用空間の確保」や、鉄道等の公共交通とのシームレスな連携（サイクル・トレイン等の平時からの標準化）を盛り込むべきだ。 | サイバーインシデントが事業継続に及ぼす影響を踏まえ、事業継続に関する悪影響を許容範囲に抑制するといった観点は重要であり、本統一基準では、事継続計画等へサイバーセキュリティを組み入れるなど、インシデントへの対応及び復旧体制の構築を求めることとしております。 |
| 145 | 物理的およびサイバー的な脅威から基幹通信網・デジタル放送網を守るため、無電柱化（電線の地下構造物化）は最優先の課題である。歩道を占拠する電柱を撤去して生まれた空間を、前述の「自転車専用道」として活用することは、物理的な移動の安全保障に直結する。<br>さらに、地下の共同溝に収容される光回線や放送網を、民間企業の私有財産の延長として放置するべきではない。地下化という大規模な公的投資を行う機会を捉え、これらを国や自治体が直接管理・監督する「公的情報回廊（公共化）」として再定義する基準を設けるべきである。これにより、一部の巨大資本によるインフラの独占と私物化を防ぎ、サイバー攻撃に対しても国家主導で迅速な統制と復旧が可能となる強靭な情報基盤が成立する。 | 本統一基準は、深刻化するサイバー脅威に対し、分野・事業者横断的に講ずべき基本的な対策の徹底を図るために、重要インフラ事業者等におけるサイバーセキュリティの確保に関し政府機関が実施する施策についての統一的な基準を定めるものとなります。また、サイバーインシデントが事業継続に及ぼす影響を踏まえ、事業継続に関する悪影響を許容範囲に抑制するといった観点は重要であり、本統一基準では、事継続計画等へサイバーセキュリティを組み入れるなど、インシデントへの対応及び復旧体制の構築を求めることとしております。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **「第３部　安全基準等において規定されるべき事項／技術・脅威の動向等を踏まえた対策」に係る意見** | |
| 146 | ①AIの判断過程は外部からの検証が困難であり、誤った判断の原因特定と是正が難しい。第3部3.2「組織統治」において、AIが運用判断に関与する場合の人間による監督体制の確保を要件として明記し、サービスの停止・継続・縮退運転等の最終判断権限が人間に留保されることを原則とすべき。<br>②AIシステムは敵対的入力やデータポイズニング等、従来とは異なる攻撃手法に脆弱である。特に深刻なのは、AIが正常に動作しているように見えながら誤った出力を続けるという、検知困難な障害モードが生じ得る点である。第3部3.5「検知」にAI固有の異常動作の検知手法を、3.4「防御」にAIへの入力データの完全性保護を含めるべき。<br>③重要インフラで使用されるAIの多くは海外の基盤モデル上に構築されており、学習データや内部パラメータは事業者側から検証できない。第3部3.7において、AIシステムの供給元の信頼性評価と、基盤モデル更新時の影響評価を安全基準等に含めるべき。 | 御意見として承ります。本統一基準の第３部では、AI技術も含めた技術・脅威の動向等を踏まえた対策を講ずることとしておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 147 | 昨今、AIを活用した脆弱性解析ツールの普及により、脆弱性情報の公開後から実際の攻撃コードの開発・悪用までのリードタイムが著しく短縮している。特に悪用が確認済みの脆弱性については、時間軸を定めない「迅速な対応」の記述では、重要インフラ事業者における優先度判断や内部承認プロセスの基準として機能しにくい。「情報システムへのパッチ適用に関する作業方針・内容を確立する。迅速なパッチ適用が困難な場合には、可能なパッチ適用頻度の設定や脆弱性リスクの高い機器の更改等、リスクに応じた措置を講じる。」とあるが、積極的に悪用が確認されている脆弱性（Known Exploited Vulnerability）については、具体的な適用期限を伴う時間軸を明示するべきである。例えば「積極的に悪用が確認されている脆弱性に係る重要パッチについては、原則として把握後2週間以内に適用・確認を完了すること」といった文言を追加することを求める。 | 本統一基準では、脆弱性の管理については、リスクに応じた措置を講じることとしています（第３部3.3.6）が、御意見の内容については、安全基準等策定ガイドラインの作成を含め今後の施策の検討に当たって参考とさせていただきます。 |
| 148 | 技術・脅威の動向等を踏まえた対策には、サイバーセキュリティ戦略にも記載されている AI、量子技術等の新たな技術革新の説明も追加して欲しい。 | AIや耐量子計算機暗号（PQC）に関する具体的な対策を含め、第３部に記載の対策事項については、別途策定する安全基準等策定ガイドラインにおいて詳細事項を記載する予定です。 |
| 149 | 重要インフラ分野におけるシステム環境は、オンプレミス中心の構成から、クラウド、SaaS、コンテナ、サーバレス等を含むクラウドネイティブ環境へ急速に移行しているところ、「脆弱性管理」を従来型のCVE管理やパッチ適用管理のみとして整理した場合、現代的なリスクを十分に把握できない可能性がある。<br>そのため、統一基準における「脆弱性管理」については、CVEベースの管理に限定せず、設定不備・権限リスク・公開状態等を含む「Exposure Management（露出リスク管理）」の観点を含めることを提案する。<br>加えて、クラウドサービス、SaaS、生成AIサービス等の利用を前提とした継続的な可視化・監査・権限分析・利用統制の必要性についても明示されることが望ましいと考える。 | 御意見として承ります。本統一基準では、脅威情報及び脆弱性情報の収集とともに、クラウドサービス利用時の対策等についても定めておりますが、御意見の内容については、安全基準等策定ガイドラインの作成を含め、今後の施策の検討に当たって参考とさせていただきます。 |

| | 意見の概要 | 意見に対する考え方（案） |
|---|---|---|
| | **その他（重要インフラ行動計画等）** | |
| 150 | 重要インフラ所管省庁とは具体的にどの省庁がそれにあたるのか全ての府、省、庁、委員会をもれなく列挙いただきたい。 | 重要インフラ行動計画の別紙５ 定義・用語集のとおり、重要インフラ所管省庁とは、各分野を所管する金融庁、総務省、厚生労働省、経済産業省及び国土交通省となります。 |
| 151 | 用語の定義集をAPPENDIXでつけて頂きたい。 | 本統一基準では定義や補足が必要と想定される用語については、各ページの脚注に記載させていただいておりますが、重要インフラ行動計画の見直しに合わせて、同計画中の「定義・用語集」の更新等を検討してまいります。 |
| 152 | 本文書において、「情報システム」及び「重要システム」については脚注で定義されていますが、それ以外に「システム」単独で用いられている箇所が複数存在し、その意味するところが不明である。英語の語義からすると人間による対応の仕組みなども含まれ、重要インフラ業種においてもコンピュータ制御以外のシステムも存在し得ることから、本基準において意味するところを明示する必要があると思う。また、「リスクファイナンス」については定義無しで用いられていますが、同様に本基準において想定しているファイナンスについての説明があるほうがわかりやすくなると思う。<br>本文書では用語定義をすべて脚注で示していますが、初出箇所以外では定義されているかの把握が困難になるデメリットもあるため、政府機関向け統一基準と同様に冒頭に用語定義をまとめて示すことも検討してはいかがか。 | 本統一基準では定義や補足が必要と想定される用語については、各ページの脚注に記載させていただいておりますが、今後、重要インフラ行動計画の見直しにおいて、同計画中の「定義・用語集」の更新等を検討してまいります。 |