「重要インフラのサイバーセキュリティに係る行動計画（案）」に対する意見募集の結果について

意見募集期間：令和4(2022)年1月28日から2月28日まで　意見総数：24件（団体8件、個人16件）

御意見の要旨	御意見に対する考え方	修正
○　総論について		
（事業者に対する規制・支援）		
重要インフラ事業者に対し、次の義務を課すべき。 ・役員へのCIO、CISO、CDOの設置 ・システム管理部門の設置 重要インフラ事業者に対し、次の補助金を求める。 ・サイバーテロ対策に関する補助金 ・専門的なセキュリティ人材派遣についての補助金 ・サイバーセキュリティアセスメントについての補助金	本行動計画は、サイバーセキュリティ基本法（平成26年法律第104号）第12条の規定に基づき策定するサイバーセキュリティ戦略を踏まえ、同法第14条（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）及び第26条第1項第5号（サイバーセキュリティ戦略本部の所掌事務）の規定に基づき策定するものであり、いただいた御意見については検討の対象外です。	無
外資の重要インフラへの参入は禁止すべき。		
サイバー空間関連事業者等の民間事業者に対する義務またはインセンティブに言及すべきだと考える。		
（重要インフラ事業者等以外への展開）		
サイバーセキュリティの取り組みは、重要インフラ組織だけでなく全ての産業組織にとっても効果的であると考えられているため、他の全ての組織にも展開されることを検討いただきたい。	本行動計画は、サイバーセキュリティ基本法（平成26年法律第104号）第12条の規定に基づき策定するサイバーセキュリティ戦略を踏まえ、同法第14条（重要社会基盤事業者等におけるサイバーセキュリティの確保の促進）及び第26条第1項第5号（サイバーセキュリティ戦略本部の所掌事務）の規定に基づき策定するものです。	無
○　計画期間内の取組について		
（組織統治）		
インシデント対応やリスク管理の観点から各組織における組織統治が重要であることに同意する。加えて、各組織の経営陣は説明責任を負うことを言及するべきだと考える。	いただいた御意見については、「Ⅳ.2安全基準等の整備及び浸透」において、内閣官房は、組織に応じた対策状況や、経営層の関与状況等の実態をより正確に把握することが重要であるとの認識のもと、重要インフラ事業者等による自主的な取組を促進する最適な手法を検討することとしており、今後の参考とさせていただきます。	無
会社に生じる損害として、情報漏えい、改ざんなどが記載されているが、業務妨害等を受けて本来提供すべきサービスが停止することも要因として含めても良いのではないか。		
実際に定められたとおりに運用されていることを確認することは重要なため、監視方法やツール、マネジメント・レビュー時の重要なポイントを列挙するなど、運用状況を知るための具体的な実施方法を示すことが有効だと考える。通常の監査で行われる記録の確認だけでは、「定められたとおりに運用がされていないこと」を経営層が知る仕組みとして弱い。		
（CSIRTの効果的な運用）		
インシデント発生時にCSIRTに最も期待される役割の1つは"迅速な復旧"である為、原因解析・影響範囲の調査に加えて「復旧」も明記した方が良い。如何に素早く復旧できるかが重要である。	いただいた御意見については、「Ⅳ.1. 1.2 (2)CSIRTの効果的な運用」において、障害が発生した場合など有事の際の対応に復旧の概念も含まれています。また、「Ⅳ.3. 3.3重要インフラ事業者等の更なる活性化」において、ISAC連携等による自動化を含めた分野間・官民連携の枠組みの整備の検討が期待されるとしています。	無
重要インフラサービス障害に迅速に対応するため、企業内のCSIRT設置・整備について賛同する。国内においては慢性的にセキュリティ人材が不足しているため、OTセキュリティ人材の育成と併せて、AI や機械学習を利用した分析の仕組みや、ツールによるインシデント対応フロー自動化・業務効率化を検討頂く必要があると考える。		
（防護範囲）		
今後、一部の「クラウドサービス等の外部サービスを提供する事業者」などが実質的には重要インフラとして扱われるようになることも想定されるため、重要インフラの見直しが機動的かつ継続的に行われることを希望。	いただいた御意見については、「Ⅳ.1. 1.4重要インフラに係る防護範囲の見直し」において、重要インフラ分野の見直し等の継続的な取組を行っていくこととしています。	無
（安全基準等の整備）		
行動計画を効果的に実施するために、必須となる最小要件、認定、ガイドラインなどのレベルで実施すべき項目を分類することを推奨する。	いただいた御意見については、「Ⅳ.2安全基準等の整備及び浸透」において、「図2　重要インフラ防護に関する安全基準等に係る体系」のとおり各文書の整備を進めており、安全基準等策定指針、安全基準等の継続的改善及び関連文書等の作成に取り組むこととしています。	無
安心かつ安全な情報共有のため、各組織とその個人に必要とされるセキュリティクリアランスについても言及するのが良いと考える。	いただいた御意見については、今後の参考とさせていただきます。	無

御意見の要旨	御意見に対する考え方	修正
（情報共有体制）		
民間企業における脅威情報の共有が異なるセクターの当事者である企業等にも適用されるべきだと考える。	いただいた御意見については、「Ⅳ.3. 3.2情報共有の更なる促進」において、ナショナルサートの枠組みの強化の検討と整合性を保つこととしており、今後の参考とさせていただきます。	無
セプター、重要インフラ事業者、重要インフラ所管官庁及び内閣官房では、メールや電話等による情報共有が行われていると推測する。Webサービスを基盤とした情報共有ポータルサイトの活用を検討することを提案する。メールや電話では提供された二次加工しなければ活用できないため、1分1秒を争う事態に迅速に対応するためにデジタル化を行う必要があると考える。また、いつでも、どこでも、どんなデバイスからでも情報にアクセスすることが可能なポータルサイトの運用は、行動が制限される被災時においても有効な手段になると考える。このポータルサイトは、デジタル庁と連携した活動として行う事で、セキュリティ確保が適切に講じられた運用が期待できる。	いただいた御意見については、「Ⅳ.3. 3.3重要インフラ事業者等の更なる活性化」において、ISAC連携等による自動化を含めた分野間・官民連携の枠組みの整備の検討が期待されており、今後の参考とさせていただきます。	無
（リスクマネジメントの活用）		
自組織のビジネス環境における独自脅威を把握することで脅威に対抗する防御対策を特定しやすくなることから、プロファイルの特性に、脅威情報を追加することを提案する。	脅威情報は、「Ⅳ.1. 1.2 障害対応体制の強化に向けた取組」で検討すべきものと考えます。	無
サイバー攻撃手法の高度化に対応するために、サイバーインテリジェンスの強化・活用を特に経営レベルも巻き込み推進していくことを提案する。迅速に脅威情報を把握することで動的に変化する攻撃に対応すること、自組織のプロファイルに伴う将来リスク分析を行う事でプロアクティブな防護対策に取り組むこと、グローバルな視点でのインテリジェンス活動が重要である。 環境変化として、重要インフラにおいてもクラウドサービス利用は浸透すると言われているため、クラウドサービスを前提にした人材育成、リスクマネジメント、事故対応も網羅する計画策定を提案する。	本行動計画では、「Ⅲ.重要インフラを取り巻く環境変化と行動計画に関する基本的な考え方」及び「Ⅳ.1. 1.2 障害対応体制の強化に向けた取組」において、サプライチェーン等を含め、将来の環境変化を先取りした包括的な対応に係る取組を推進することとしています。具体的には、「Ⅳ.4. 4.1 リスクマネジメントの推進」において、経営層主体のもと、自組織の特性（プロファイル）を把握し、自組織に適した防護対策を実施することやサプライチェーン等を含め社会を取り巻く環境は常に変化していることを念頭に「Ⅳ.4. 4.2 環境変化におけるリスク把握」にある環境変化調査や相互依存調査を実施することとしています。	無
（人材育成）		
「内閣官房は、（中略）サイバーセキュリティに係る演習・訓練、資格取得等の具体的な人材育成策を推進する。」とあるが、サイバーセキュリティに係る演習・訓練については文書内の他の箇所に記載があるのに対し、サイバーセキュリティに係る資格については特に記載がなく、どのような資格をなにを目的として取得するのか分かりにくいと感じる。取得する資格のリストを別紙として添付するなどしてはどうか。	本行動計画は取組方針を記載するものであり、具体の資格のリストは記載していません。	無
○　用語・定義について		
・５７ページのサイバーセキュリティ関係省庁の「原子力発電所」について：原子力規制庁が所管している原発以外の原子力施設は対象外か？	重要インフラ分野の一つである電力分野との関係性において記載しているものであり、原子力発電所以外の原子力施設は対象外です。	無
別紙５「定義・用語集」における「サイバー空間関連事業者」の定義において、「サイバーセキュリティ基本法第７条に規定されるサイバー関連事業者のうち、重要インフラサービス提供に必要な情報システムに関係するサプライチェーン等に関わる」事業者として「クラウドサービス等の外部サービスを提供する事業者」が追記される。これにより、「クラウドサービス等の外部サービスを提供する事業者」において行動計画上の取組みが新たに必要となるとともに、クラウドサービスを利用する重要インフラ事業者等における取組みにも影響することが考えられる。その理解を促す観点から、本文において、「クラウドサービス等の外部サービスを提供する事業者」が「サイバー空間関連事業者」の定義に追加された旨とその趣旨について説明しては如何か。	クラウドサービス等の外部サービスへの依存度の増加を踏まえ、サプライチェーン等に関わる事業者にクラウドサービス等の外部サービスを提供する事業者が含まれることを明確化したものです。サプライチェーン等に関わる事業者については「Ⅰ.3. 3.3 (3) サプライチェーン等に関わる事業者」に記載しており、現行記載で十分と考えます。	無
○　その他について（表現の修正）		
・４７ページの表の「対象となる重要システム例」欄の「あつせん」は「あっせん」の誤記か？ ・５８ページの情報システムの「ＩＴ」は、他の箇所の例と同様に半角で「IT」と記載したほうがよい。	「あつせん」の記載については、割賦販売法における記載を用いています。 「ＩＴ」の記載については、御意見のとおり修正します。	有
別紙2のクレジット分野の「システムの不具合が引き起こす重要インフラサービス障害の例」欄について、「カード情報又は個人情報の大規模漏えい」を「カード情報又は信用情報の大規模漏えい」に修正して欲しい。他の重要インフラ分野の「システムの不具合が引き起こす重要インフラサービス障害の例」には、「個人情報の大規模漏えい」などという表記はないため、ことさらクレジット分野においても表記することは適切ではない。仮に「カード情報」以外の「大規模漏えい」を記載するのであれば「個人情報」ではなく、業界の特殊性を踏まえた「信用情報」の方がより適切な表現であり、望ましいと考える。	割賦販売法改正（令和３年４月施行）を踏まえ、「特定信用情報提供業務」を重要インフラサービスに追加することに伴い、法を踏まえた記載の適正化の観点から、御意見のとおり修正します。	有

その他の御意見の提出もありましたが、今回の案に直接関係のないものでした。