「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（案）」等に関する意見の募集結果について

意見募集期間：2023年(令和５年)4月24日から同年5月23日まで　意見総数：13件（団体7件、個人6件）

No	団体名	対象	御意見の要旨	御意見に対する考え方	修正
1	個人	–	全体的に企業に対応を丸投げしている印象がある。政府関係の重要インフラで事件が発生した際には、地方自治体や省庁の公務員も事態収拾に関わると思われる。例えば人材育成の項など、そのような観点からも考えていただきたい。	安全基準等策定指針は、サイバーセキュリティ基本法(平成26年法律第104号)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」を踏まえて策定されるものであり、地方公共団体は重要インフラ事業者等に含まれますが、省庁は対象外です。	無
2	個人	指針	「1.1. 重要インフラにおけるサイバーセキュリティの確保の重要性」における「経営層は任務懈怠に基づく損害賠償責任を問われうる。」との記載について、「経営層」とは脚注1において「首長」も含まれるとされているところ、地方公共団体の首長の損害賠償責任が「任務懈怠」により発生することはないから、誤りではないか。	当該記載は会社法第423条第1項を念頭に置いたものであり、次のとおり修正します。 「経営層は、組織の意思決定機関が決定したサイバーセキュリティ体制が当該組織の規模業務内容に鑑みて不十分なことに起因して組織や第三者に損害が生じた場合、善管注意義務違反や任務懈怠（けたい）に基づく損害賠償責任を問われ得るなどの会社法・民法等の規定する法的責任やステークホルダーへの説明責任を負う。」	有
			「1.1. 重要インフラにおけるサイバーセキュリティの確保の重要性」における「障害の拡大防止」との記載について、重要インフラのサイバーセキュリティにおいて生じうるインシデントは「障害」に限らないから、不適当な表現ではないか。	障害が一例であることがわかるよう、次のとおり修正します。 「リスクマネジメントによる事前対応と、障害等が発生した際の被害の拡大防止・早期復旧といった危機管理の両面から」	有
			「1.2. 「安全基準等」とは何か」について、「安全基準等は、重要インフラ分野ごとにその特性に応じて策定され」との記載について、特に強制基準に関しては、分野を特定せず横断的に定められることもある（例えば、個人情報保護法に基づくもの）から、不適当な表現ではないか。	御意見のとおり、分野横断的に安全基準等が策定される場合もあり得ることから、「重要インフラ分野ごとにその特性に応じて策定され」との記載を削除します。	有
			「5.1.3.2. マルウェアからの保護」における「マルチエンジン型マルウェア検知ソフト」「ゼロトラスト型エンドポイントセキュリティ」については、情報システム・ネットワークのアーキテクチャ等により適切なマルウェア対策は異なることから、技術中立性を欠く記載をすべきではない。	御意見のとおり、情報システム・ネットワークのアーキテクチャ等により適切なマルウェア対策は異なることから削除することとし、手引書において例示することとします。	有
			「5.2.1. 従業員の管理」における「重要なシステムの構築・運用に携わる従業員について、リスクアセスメント結果を踏まえて配置・管理する」との記載について、「リスクアセスメント」がどのようなものなのか明らかにされていないため、重要インフラ事業者等において十分な対応が出来ず、又は過度な対策を想起させることにならないか。少なくとも、労働法制における差別の禁止との関係について整理すべきではないか。	「リスクアセスメント」とは、指針「4.2 リスクアセスメント」における取組を想定しています。対応としては、例えば、手引書に掲げた参考文献「ISO/IEC27002:2022」の「6.1 選考」においては、事業上の要求事項、アクセスされる情報の分類及び認識されるリスクに応じて、従業員の経歴を確認すること等が挙げられています。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
			「5.4.5. 多層防御」における「多層防御を導入する」との記載については、重要インフラに係る情報システムについて境界型セキュリティを講じることを想定し、ゼロトラスト型セキュリティを推奨しない旨を示すものか。そうであるとして、その理由は何か。	組織内外の境界に限らず複数の防御策を講じることを意図したものであり、ゼロトラスト型セキュリティを推奨しないものではありません。	無
3	一般社団法人セキュアIoTプラットフォーム協議会	指針	サプライチェーン管理の観点から、業務委託先の選定には、経済安全保障に基づくセキュリティクリアランスの観点も考慮すべきだと思われます。	御意見を踏まえ、「4.1 組織状況の理解」の「関係法令」に次の脚注を追加します。 「例えば、重要インフラの事業法、個人情報の保護に関する法律（平成15年法律第57号）、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）等。」	有
		手引書	サプライチェーン管理の観点から、業務委託先の選定には、経済安全保障に基づくセキュリティクリアランスの観点も考慮すべきだと思われます。	御意見を踏まえ、「6.6. サプライチェーン・リスク対応」に次の記載を追加します。 「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針（令和５年４月28日閣議決定）におけるリスク管理措置の例が参考になる。」	有
			「11.2.3. テレワーク・遠隔制御」について、利用者側での対策に加えて、管理体制、ネットワーク環境、物理的な施設・作業環境に配慮された安全なテレワークサイトを選択することが必要であることを記載した方がよいと思います。	今後の参考とさせていただきます。	無
4	株式会社東芝	手引書	「6.4.サプライチェーン・リスク対応」の（リスク管理策例）の「部品の供給役務の継続提供の担保」について、部品を永久に供給することを保証すべき、と言っている様に見えるが、実際には難しいと考える。また、「6.4.サプライチェーン・リスク対応」と経済安全保障法で特定社会基盤事業者や特定重要設備の供給者が”リスク管理措置”で求められる対策との関係を明確にしていただきたい。	御意見を踏まえ、「6.6. サプライチェーン・リスク対応」の「部品の供給役務の継続提供の担保」を「部品の供給役務の継続提供の担保又は代替手段の検討」に修正します。また、次の記載を追加します。 「「特定妨害行為の防止による特定社会基盤役務の安定的な提供の確保に関する基本指針（令和５年４月28日閣議決定）」におけるリスク管理措置の例が参考になる。」	有

5	個人	–	PDFは最低限でもしおり付きPDFで公開すべき。これによりデジタルでの可読性が向上する。できれば英国政府のようにPDFを禁止して、htmlでの公開も検討すべきでは。また、改定であるため、前版との改定履歴付きの版も公開すべきではないか。これにより前版で活用していた方々が違いだけを効果的、効率的に対応できる可能性が高くなる。	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
		指針	「情報セキュリティ」という用語が「サイバーセキュリティ」に変更されている。これ自体は賛成である。しかし、サイバーセキュリティは、サイバーセキュリティ法の定義では情報セキュリティの中でサイバーに特化したものだけと定義され、情報セキュリティの方が用語の示す範囲が広くなるような定義になっている。しかし、実際はサイバーセキュリティは、情報セキュリティを全て含有し、情報、情報システムの危害に注目するのではなくて、事業の継続性を含めた広い危害を考慮したものであり、観点が異なるような意味で使われている。このあたりを明確に記載したほうがいいのではないか。	「3. 組織統治におけるサイバーセキュリティ」において、任務保証の観点から取り組むべきことを記載しています。また、「1.3 安全基準等策定指針の位置付け」において、安全基準等策定指針において使用する用語は重要インフラのサイバーセキュリティに係る行動計画において使用する用語の例によることとしています。	無
			「3.1. 組織方針」と経産省のサイバーセキュリティ経営ガイドラインをもう少し対比させた記載にしたほうがわかりやすくなるのではないか。	「3.組織統治におけるサイバーセキュリティ」において、経済産業省「サイバーセキュリティ経営ガイドライン」が参考になる旨を記載しています。	無
			JIS、ISO、IEC等で禁止されているぶら下がり段落(hanging paragraph)の文章構成になっている箇所が散見される。例えば、3.1章がある場合は、3章の直下には文章を書かないようにする必要がある。本書はJIS等ではないが、JIS等ではさまざまな経験、知識から誤解を受けにくい文書構成等にしてきている経緯があると推する。このため、特に明確な合理的な理由がない限りは、それに従った記載にしたほうがいいのではないか。	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
			「4. リスクマネジメントの活用と危機管理」において「自組織」との用語が多用されている。自組織内のリスクを管理、対応することは最低限必須だが、自組織以外も含めたサプライチェーンにおいてリスク管理をすることが重要である。「4.4. サプライチェーン・リスクマネジメント」には記載されているが、4章の最初においても、サプライチェーンを意識した記載に修正すべきではないか。特にサイバーセキュリティ経営ガイドラインの指示9にも示されている内容と整合を図ったうえで、記載を修正すべきではないか。	「3.3 経営リスクとしてのサイバーセキュリティリスクの管理」及び「4.4 サプライチェーン・リスクマネジメント」において、サプライチェーン全体にわたるセキュリティ対策への目配りや、サプライチェーン全体での方策の実効性を高めることとしています。	無
			「4.3.1. リスク対応の決定」における「マチュリティモデル」という用語について、単純に「能力成熟度モデル」といった記載の方がわかりやすいのではないか。	わかりやすさの観点から、「マチュリティモデル」を「成熟度モデル」に修正します。	有
			「4.6. 人材育成・意識啓発」における「サイバーセキュリティは全員参加」は非常に重要な考えだが、それ以外に専門家の育成、活用も必要になる。情報処理安全確保支援士の活用とそれをキャリアパスになるような記載を追加し、多くの方々が情報処理安全確保支援士を目指すようになるとよいのではないか。	「4.6 人材育成・意識啓発」において、情報処理安全確保支援士等の資格取得等を推進することが望ましい旨を記載しています。	無
			「5.4. 技術的対策」に多層防御等の記載があるが、特に重要インフラ事業者にとってはネットワークをZoneにわけたセグメント、Segregation、Conduit等のネットワークの物理的、論的分離等が有効な場合が多いと思われる。多層防御に記載するか別の章で明記するのがよいのではないか。	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
			「5.5.2 クラウドサービス利用時の対策」における「クラウドサービス提供者との責任範囲等を明確にする」との記載は非常に重要な点だと思う。最近は、クラウドでの危害の原因の1つとして、クラウドに接続するために事業者側がCloseなネットワークに穴を開けて接続し、その穴が狙われる場合が多いと思う。通常、クラウド事業者側ではなく、それに接続する事業者側の責任と位置付けられる可能性が高い。しかし、そのような事業者は従前Closeなネットワークで外部との接続を持たない等でセキュアに運用していて、かつ、セキュリティに関して知識、経験が低い可能性も高い。通常、接続機器はVPN機器であり、その脆弱性が放置されての危害が多発しているため、クラウド接続時の事業者のネットワークでの接続機器の設定、保守の確認を追加した方がよいと思う。	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
		手引書	「4. 組織の状況の特定」において、組織又は自組織に限らずサプライチェーンを考慮した特定が必要になる。自組織が関与している事業(重要インフラサービス)に関してリスクを検討していく必要があるのではないか。	「4.組織の状況の特定」において、自組織の重要インフラサービス提供に係る特性の明確化を行うこととしています。	無
			「5.1. リスクアセスメントの実施」の「リスクに対する態度」の脚注として「リスクのアセスメントを行い、最終的にリスクを保有する、取る又は避ける、という組織の取組のこと。」と記載されている。ISO31000のリスク対応に合わせる記載等にした方がよいのでは。	ISO31000:2009からISO31000:2018への改定に伴い「リスクに対する態度」「リスク許容度」の用語が削除されたことを踏まえ、当該用語及び脚注を削除します。	有
			「5.2. 制御システムのリスクアセスメント」における「セキュリティリスクを考慮し外部ネットワークに接続していない環境で運用していても、災害、自然故障、管理不良等により制御システムの可用性が低下するリスクがある。」との記載について、その通りだと認識している。さらに、最近は制御システムの領域においてもクラウドの活用や、装置のリモート保守等で外部と接続する機会が増加している。外部接続が増加している点とそのときの注意事項等も追記しておいた方がよいのではないか。	指針「4.2 リスクアセスメント」において、制御システムに汎用機器が用いられ、また、遠隔監視・制御等のために外部と接続される場合があることを念頭に、制御システムについても適切にリスクアセスメントを実施することとしています。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
			「11.4.5. 多層防御」について、各機器はセキュリティが不足するものも多い。特に重要インフラ事業者にとっては従前はCloseな環境が多かった。しかし、最近、クラウド、リモート保守等で外部と接続する機会が増えたので、ますます、ネットワークをZoneにわけたセグメント、Segregation、Conduit等のネットワークの物理的、論的分離等が有効な場合が多いと思われる。多層防御に記載するか別な章で明記しておくのがいいのではないか。	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

6	株式会社DataClasys	指針	「5.5.1 ランサムウェア対策」に情報漏洩対策に関する記載を追加してはどうか。 （理由）ランサムウェア攻撃の多くは不正な暗号化による事業停止だけでなく、同時に情報窃取も行われています。復旧のためのバックアップだけでなく二重恐喝に備えた情報漏洩対策も同時に実施することを明記した方がよいと考えます。	「5.5.1 ランサムウェア対策」における脆弱性対策、ネットワークの分割等により、情報漏えいの防止にも寄与すると考えます。	無
		手引書	「11.4.4.1. 機微なデータの取り扱い」に機微データの暗号化管理に関するより詳細な記述を追加してはどうか。 （理由）機微データの暗号化保護と表現するとパスワードにより解除できるシステム（パスワード付きZip等）が想定されますが、パスワード設定は下記の理由から適切な手法と言えない可能性があります。 ・一定の桁数以上でないと容易に解析可能である ・使い回しを避け、ファイル毎に個別のパスワードを設定する必要がある ・暗号化する、しないが個人の判断に委ねられるため、実効性の乏しい対策になってしまう可能性が高い またディスクレベルでの暗号化も一度OSにログインすれば自由にデータを取り出すことができてしまうため、機微データ保護の観点では適切と言えません。それ故、例えば ・パスワードに頼らない暗号化技術を用いる ・IRM等のデータと鍵を分離して管理する技術を利用する ・自動で暗号化できるシステムを選択する などの表現を加え定義を明確化することで、より実効性のある暗号化を選択できるようにするのがよいと考えます。	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
7	デル・テクノロジーズ株式会社	指針	「5.1.3.2. マルウェアからの保護」に以下文言を対策例として追記検討願います。現状記載のマルウェア検知ソフトはあくまで検知に関する部分であり、早期回復における重要となるデータ復旧に繋がるバックアップシステムについても必要と考えているためです。 「対策として、早期回復に繋げる復旧用のデータを安全に保護し、そのデータ(バックアップデータ)に対してウイルスに侵されていないデータかどうかの分析検証機能を有すること。」	「5.1.3.2. マルウェアからの保護」における「マルチエンジン型マルウェア検知ソフト」「ゼロトラスト型エンドポイントセキュリティ」については、情報システム・ネットワークのアーキテクチャ等により適切なマルウェア対策は異なることから削除することとします。 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。	有
			「5.5.1. ランサムウェア対策」に以下文言を追記検討願います。昨今のランサムウェアはバックアップシステムへの攻撃も増えておりますため、攻撃からの防御についてとより迅速＆確実な復旧が可能となる仕組みが必要と考えているためです。 「・セキュリティ対策として、バックアップデータはCIFS／NFSプロトコルで簡易的にアクセスできない仕組みを実装していること。 ・セキュリティ対策として、バックアップシステムはwindowsやLinux等汎用OSではなく、独自OS採用が望ましい。」	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
		手引書	「11.1.3.3. バックアップ」について、バックアップ元とのセグメント分割においてはネットワークに繋がっている状態での対策となり、セグメント分割するスイッチ等が攻撃を受ける可能性は否定できません。そのため、重要なデータはネットワークから隔離したオフライン保管を明確に記載した方が良いかと考えております。 文言案 「・重要度の高いバックアップデータはバックアップ元と繋がらないネットワークから隔離したオフライン環境にて保護を可能な限り行う。その他システムと異なるセグメントにする等ネットワーク分離を行う等、保存方法、保存期間を定める。また、定期的に復旧テストを実施する。 ・保護しているバックアップデータに対して、ウイルスに侵されていない復旧に用いるべき正しいデータを検知する仕組みを実施する。」 何れも昨今脅威を増しているランサムウェア被害について、侵入された後の迅速かつ確実な事業”復旧”に必要なバックアップシステムとして単なるバックアップデータの保管ではなく上記のような具体的な対策を明確にすることで、よりシステム化検討をする上でも参考になるかと考えております。	物理的・論理的な分離のいずれを採用するかについては、組織ごとのリスク等に応じて検討されるものと考えています。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
8	サイバートラスト株式会社	指針	「4.4. サプライチェーン・リスクマネジメント」について、調達には情報システムの構成部品の安全性確認や真正性担保のためにIEC62443やSP800シリーズなどの国際安全基準の機器レベルに求められるサイバーセキュリティ対策に加えて、機器に組み込まれるソフトウェアについてもSBOMやコード署名を活用した継続的なサプライチェーン管理が求められる。	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
			「5.1.3.6. 脆弱性の管理」について、既知の脆弱性の対策と未知の脆弱性の早期発見の為の定期的かつ継続的な運用サイクルが必要です。そのため情報システムのスキャン、脆弱性の可視化、対応を自動化するための脆弱性管理ツールの導入が望まれる。	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
			「5.1.4. システムの取得・開発・保守」について、保守作業等のメンテナンスに関わる対策として、境界線防御に加えゼロトラストアーキテクチャを考慮した機材調達・システム構成・保守運用が必要である。	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
			「5.5.2. クラウドサービス利用時の対策」について、データが海外のクラウドサービスに格納される場合も、国内の準拠法を適用するためにも、日本国内で日本司法管轄権内で運用される認証局による鍵管理が必要。	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

		手引書	「6.4. サプライチェーン・リスク対応」について、 ・調達には情報システムの構成部品の安全性確認や真正性担保のためにIEC62443やSP800シリーズなどの国際安全基準の機器レベルに求められるサイバーセキュリティ対策に加えて、機器に組み込まれるソフトウェアについてもSBOMやコード署名を活用した継続的なサプライチェーン管理が求められる。 ・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した方がよいと考える。 →参照するサイバーセキュリティ規格が不明瞭であり、IEC62443やSP800-171,82,53等具体的な参照規格を記載すべき。 ・不正機能等の埋め込みに係る脅威に対応する必要があると考える。 →不正等の埋め込みは導入時のみならず運用・保守でも発生する前提が不可欠であり、それらに対する要件を付記すべき。	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
			「11.1.3.1. 運用の手順及び責任」について、既知の脆弱性の対策と未知の脆弱性の早期発見の為の定期的かつ継続的な運用サイクルが必要。そのため情報システムのスキャン、脆弱性の可視化、対応を自動化するための脆弱性管理ツールの導入が望まれる。	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
			「11.1.4. システムの取得・開発・保守」について、保守作業等のメンテナンスに関わる対策として、境界線防御に加えゼロトラストアーキテクチャを考慮した構成が必要である。	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
			「11.4.1. 利用者アクセスの管理」について、ユーザーアカウントに管理権限を割り当てず、管理権限も用途ごとに設定することが必要だと考える。（バックアップ用、システム設定閲覧用、システム設定変更用等）。 また離職者のアカウント管理として、全てのバッジ、キーカード、トークン等を失効させ、安全に返却させる。離職者が保有する全てのユーザーアカウントと、組織情報へのアクセスを無効にするなどの対策が必要。	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
			「11.4.3. 技術的脆弱性の管理」について、 ・外部から取得した情報システムの場合には、供給者に脆弱性の報告や取扱い及び開示を実施することを要求することが必要。 →定期的に報告や開示する事を要求する。と記載修正すべき。基本的には月次定期報告が望ましいと考える。 ・適用可能な更新、パッチ等がない又はその他の理由により修復が困難な場合には、次のような管理策を検討すべきだと考える。 →設備の利用停止、入れ替えを追記した方がよいと思われます。	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
			「11.4.4.2. 暗号化通信及び電子署名」について、改行位置等の体裁を修正すべき。	改行位置等の体裁について修正します。	有
9	パロアルトネットワークス株式会社	手引書	「11.1.3.2. マルウェアからの保護」について、攻撃の拡散に備えた対策例として、ネットワークセグメント分割（重要インフラの分離）、IPS/プロキシサーバ（不審な外部通信の遮断）、EDR（影響範囲の特定と被害端末の隔離）等とありますが、設備にはインターネットに繋げない端末やアプリケーションがアップデートできなくEDRの導入が現実的でない場合があります。不正侵入から実害を防ぐために、ネットワークへの侵入を検知し、分析および対処を行うことができる機能(Network Detection and Responseを想定)の実装をご検討頂けないでしょうか。	御意見を踏まえ、次のとおり修正します。 「被害が発生した際の、攻撃の拡散に備えた対策例として、ネットワークセグメント分割（重要インフラの分離）、 IPS/プロキシサーバ（不審な外部通信の遮断）、 EDR（影響範囲の特定と被害端末の隔離）、 NDR（ネットワーク全体の包括的な監視と脅威検知）等がある。」	有
		指針/手引書	手引書「11.4.2. 情報システム等のアクセス制御」のとおり、悪用可能なサービスについては特にインターネット上に公開しないよう制限することは有効な対策と考えております。これらインターネットに公開されているサービスや公開サーバ自体が意図せず公開されていないか、もしくは公開サーバ及びサービスが未承認の資産でないか、といった点も監視、管理する必要があると考えております。指針「5.1.1.1. 資産に対する責任」において未承認の資産がネットワークに接続・運用されていないか監視対処すると記載されており、こちらに含まれるものと考えますが、内部からの監視と、外部からの監視双方併用することで網羅的に監視、対処することが可能と考えておりますため、攻撃対象領域管理の必要性についても、指針「5.1.1.1. 資産に対する責任」又は「5.1.3. 運用の管理」内に明記いただくことで、具体的な対策のイメージがつきやすくなるものと考えますため、攻撃対象領域管理の追記についてご検討いただけますと幸いです。	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

10	エムオーテックス株式会社	指針	「3.6. 監査 ・モニタリング」の「脆弱性診断、ペネトレーションテスト等を実施すること」について、診断も1度やれば充分という性質のものではないため、後段の2文と合わせ「定期的に脆弱性診断、ペネトレーションテスト等を実施すること」としてはいかがでしょうか。	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
			「5.1.3.2. マルウェアからの保護」に「ゼロトラスト型エンドポイントセキュリティ」という聞きなれないワードが突然出てきて違和感を覚えました。また、他の章と比べ手引書との整合性がとれていないので、マルウェア対策に有効なNDRを追加した以下の修正案でいかがでしょうか。 （修正案） 5.1.3.2. マルウェアからの保護 ・マルウェアを検出及び予防する仕組みを整備し、マルウェアに感染した場合でも早期回復を図るための対策及び手順を確立する。 ・マルウェアの検知率向上が期待されるマルチエンジン型のマルウェア検知ソフトの利用やシステム負荷を抑えつつ未知の脅威に対応できることを特徴とするマルウェア対策製品等の導入を検討する。 ・攻撃の拡散に備えた対策の導入を必要に応じて検討する。対策の例として、ネットワークセグメント分割（重要システムの隔離）、IPS／プロキシサーバ（不審な外部通信の遮断）、EDR（影響範囲の特定と被害端末の隔離）やNDR(ネットワーク全体の包括的な監視と脅威検知)等がある。	「5.1.3.2. マルウェアからの保護」における「マルチエンジン型マルウェア検知ソフト」「ゼロトラスト型エンドポイントセキュリティ」については、情報システム・ネットワークのアーキテクチャ等により適切なマルウェア対策は異なることから削除することとし、手引書において例示することとします。	有
			「5.4.2. 情報システム等のアクセス制御」について、昨今、多要素認証を突破される攻撃が増えてきており、改めて有効性が見直されている「接続元IPアドレスを制限する」を追加してはいかがでしょうか。	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
			「5.5.2. クラウドサービス利用時の対策」について、ユーザーの意思とは関係なくサービス仕様が変更され、設定値のセキュリティレベルが下がる可能性も考慮し、2つの内容をマージした以下の記載としてはいかがでしょうか。 （修正前） ・ 情報公開等の設定にミスがないか確認する。 ・ サービス仕様が変わる際には影響を確認する。 （修正後） ・ サービス仕様変更によりセキュリティレベルが下がる可能性を考慮し、情報公開等の設定に問題がないか定期的に確認する。	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
			「5.5.1. ランサムウェア対策」「5.5.2. クラウドサービス利用時の対策」について、昨今のセキュリティ動向の変化が激しい時代に、すべての企業の担当者が常に最新の動向を把握することは困難であるため、ぞれぞれの章に以下を追加するのはいかがでしょうか。 ・動向を把握した専門家に定期的な第三者評価を実施すること	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
			「5.5.1.ランサムウェア対策」について、ランサムウェアの事案では、クライアントやサーバ「端末」の脆弱性対策も重要ですが、入口としてVPN機器経由の事例が多く報告されています。このため、「端末」以外の対策として以下も追記／修正してみてはいかがでしょうか。 （追記／修正案） ・端末は、速やかなパッチ適用等による脆弱性対策を講じる ・ネットワーク機器は、ファームウェア更新による脆弱性対策を講じる	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
		手引書	「6.4. サプライチェーン・リスク対応」の「信用できるサービスの選定」に関して「クラウドサービスの場合はISMAPに登録されている」等、信用できるサービスの基準を明記してはいかがでしょうか。	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

			「11.1.3.4. ログ管理」について、ログの取得対象（システム及びネットワーク機器、セキュリティ対策システム）の明記、及び保管だけでなくログ管理で必要とされる「定期分析」「変更管理（改ざん検知）」についても明記してはいかがでしょうか。なお、ログの保存期間については、最低期間（1年）なども明記してはいかがでしょうか。※参考：JPCERT／CC 「高度サイバー攻撃への対処におけるログの活用と分析方法」P13 （修正例) 11.1.3.4. ログ管理 ・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、セキュリティ対策システムのイベントなどセキュリティの確保に必要なログを、検知及びインシデント対応で使用するために収集し、保存する。 ・保存したログは、定期的または適宜点検及び分析を行う。 ・ログを改ざん、削除から保護するための対策を行う。また、イベントログなど重要なログソースが無効化された場合、セキュリティ担当者に通知する。ログ機能が非搭載の制御システムについては、制御システムとの間の通信ログを収集する。 ・ 収集したログはツールや中央システム（SIEM等）に一元的に保存され、許可された管理者のみがアクセスできるようにする。ログの保存期間については、関連するガイドラインや、想定するリスクに基づき設定する。	御意見を踏まえ、次のとおり修正します。 「11.1.3.4. ログ管理 ・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、セキュリティ対策システムのイベントなどセキュリティの確保に必要なログを、検知及びインシデント対応で使用するために収集し、保存する。 ・定期的又は適宜、保存したログの点検及び分析を行う。 ・ログを改ざん、削除から保護するための対策を行う。また、イベントログなど重要なログソースが無効化された場合、セキュリティ担当者に通知する。ログ機能が非搭載の制御システムについては、制御システムとの間の通信ログを収集する。 ・収集したログはツールや中央システム（SIEM等）に一元的に保存され、許可された管理者のみがアクセスできるようにする。ログの保存期間については、関連するガイドラインや、想定するリスクに基づき設定する。」	有
			「11.1.3.2. マルウェアからの保護」及び「別紙　サイバー攻撃リスクの特性③ 」について、取引先／委託先からの不正侵入のインシデントが増えており、何が脅威となるか分からない、という前提であれば、自社のNWを如何に見守っておくか、不正因子に気づくかがポイントとなります。医療系でのランサム事案やVPN経由での侵入も増えており、エンドポイント対策や入口のアクセス制限では対処できないケースがあるので、ネットワークキャプチャで、社内NW全体を監視し、即座に検知／対処することで被害の未然防止や抑制も検討していく必要があると考えられます。NDRを追加した以下の通りに修正してはいかがでしょうか。 （修正前） (P22) EDR12（影響範囲の特定と被害端末の隔離）等がある。 (P34) EDR1（影響範囲の特定と被害端末の隔離）等がある。 （修正後） EDR（影響範囲の特定と被害端末の隔離）やNDR(ネットワーク全体の包括的な監視と脅威検知)等がある。	御意見を踏まえ、次のとおり修正します。 「被害が発生した際の、攻撃の拡散に備えた対策例として、ネットワークセグメント分割（重要インフラの分離）、 IPS/プロキシサーバ（不審な外部通信の遮断）、 EDR（影響範囲の特定と被害端末の隔離）、 NDR（ネットワーク全体の包括的な監視と脅威検知）等がある。」	有
			「11.2.2. 委託先管理」について、「アクセスさえる情報」との誤字があります。	「アクセスされる情報」に修正します。	有
			「11.4.2.2. パスワード 管理」の「ハードコードされている等、デフォルトパスワードの変更が不可能な場合、代替セキュリティ管理策を実施し、ログインのアクセスログを監視する。」について、日本国の重要インフラで扱われるハードウェア・ソフトウェアであるなら、パスワード変更できないものは使うべきではないと考えます。また、本記載と同節内の以下記載が矛盾します。「・自組織のサービスや資産に関して、一意かつ個別のパスワードを設定する。利用者に対し、アカウント、アプリケーション、サービス等でパスワードを再利用させないようにする。」	一意かつ個別のパスワードの設定を前提としつつ、パスワードを変更できない場合について記載したものです。パスワードを変更できない機器等の禁止については、今後の参考とさせていただきます。	無
			「11.4.2.3 多要素認証の活用」の「SMSによる多要素認証は、他の選択肢が可能な場合を除きできるだけ避けるようにする。」について、SMSによる多要素認証は、他の選択肢が可能な場合に、できる限り避ける。という意味と理解しました。このため、以下例のように修正が必要と考えます。 （修正案) SMSによる多要素認証は、やむを得ない場合を除きできるだけ避けるようにする。	御意見のとおり修正します。	有
			指針に合わせ、暗号鍵の取り扱いについての言及を記載してはいかがでしょうか。 ※指針には以下の記載があるため、手引きには具体的な手順を示すべきです。 （指針） 5.4.3. 暗号を活用した情報管理 ・ 暗号の利用方針や暗号鍵の管理方針を策定する。	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
			「別紙　サイバー攻撃リスクの特性⑥]について、「サイバー攻撃に対して十分な検知策を講じていない場合」以降の表現を見ると巧妙な検知回避により検知が遅れるというような表現であり、昨今ではこのような回避により、一定の対策を講じていても検知できないケースがあります。このため、検知策を「講じていない」という表現に違和感があります。以下の通り修正してはいかがでしょうか。 （修正案） サイバー攻撃に対して十分な検知策を講じていたとしても、攻撃を認識できず長期間にわたり攻撃を受け続ける可能性がある。	検知が困難な攻撃が行われることにより、長期間にわたり攻撃を受け続ける可能性があることを意図した記載であり、検知策の効果に関するものではありません。	無
11	個人	指針	11ページの脚注19の冒頭「サイバーセキュリティ基本法」について、４ページの脚注３の例と同様に法律番号を記載した方がよい。	御意見のとおり修正します。	有
		手引書	7ページの13行「当たって」と、15ページの８行「あたり」とは、どちらかに字句を統一したほうがよい。	御意見を踏まえ、「当たり」に修正します。	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。