安全基準等策定ガイドライン（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
	「1 基本的な考え方」に係る意見	
1	本ガイドライン（案）は、深刻化・高度化するサイバー脅威に対し、重要インフラのレジリエンス確保やリスクベースの対策推進を目指すものであり、その方向性に深く賛同する。	賛同意見として承ります。
2	制御システムにおけるパッチ適用や多要素認証等の実施が困難な場合の補償的対策（代替セキュリティ管理策）について触れられているが、どの程度の補償的対策を講じれば「安全基準を満たした」とみなされるかの判断軸が曖昧であるところ、各項目の「解説」または1.3の注記において補償的対策に求められる実施の程度がわかるような記載を各項目の「解説」または1.3の注記に設けていただきたい。	御意見として承ります。補償的対策に求められる強度は分野や対象のシステム等により異なり得るところ、本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の詳細事項を記載するものであるという点を踏まえ、今後の各分野における安全基準等の検討を含め参考にさせていただきます。
3	本文・解説中に非常に多種多様な国内外のガイドラインが引用されているが、ガイドラインの冒頭または末尾（巻末資料等）に「主な参照ガイドライン・標準の目的別一覧（マッピング表）」を追加するか、1.5に趣旨を追記すべきではないか。	本ガイドラインにおいて、参照文書を含めて「解説」はあくまでも補足であり、これによって対策事項に係る対応方法を詳細に定め、一律の対応を求めるものではありませんが、御意見の内容については、今後の本ガイドラインの見直しの検討に当たって参考にさせていただきます。
4	重要インフラ統一基準に基づく既存の把握・分析又は評価の結果として、本ガイドラインの記載内容に関係する分野横断的な課題若しくは環境変化が確認された場合には、本ガイドライン1.6に基づく改定の要否を確認することが分かるようにしていただきたい。	本ガイドラインでは、1.6安全基準等策定ガイドラインの改定において、重要インフラ統一基準の見直し頻度を踏まえ、本ガイドラインについても適切な頻度において、技術や脅威等、重要インフラを取り巻く環境変化に応じた見直しを行うことを定めております。また、本ガイドラインの見直しに当たっては、重要インフラ統一基準に基づく把握・分析等のPDCAサイクルを通じて確認された課題等も含め考慮することが想定されます。
5	「講ずることが望ましい対策事項」のうち、費用、人材、技術的条件、脅威環境その他の変化し得る事情を理由として各分野の安全基準等へ反映しなかった事項については、次回の安全基準等の見直し又は既存の取組状況の把握・分析を行う際に再確認対象として識別できる状態としてはどうか。	御意見として承ります。本ガイドラインでは、「講ずることが望ましい対策事項」について、各分野における重要インフラ事業者等の対策状況等を踏まえ、所管省庁等において安全基準等への反映を判断することとしております。御意見の内容については、今後の各分野における安全基準等の検討や取組状況の把握・分析を含めた施策の実施に当たって参考にさせていただきます。
6	サイバーセキュリティ基本法の趣旨に照らせば、本ガイドラインは、単なる形式的チェックリストではなく、重要インフラの実効的な防護能力、復旧能力、サプライチェーン耐性、技術的自律性を高める基準として策定されるべきである。 特に、AIを悪用した攻撃の高度化、OSSサプライチェーンへの依存、海外クラウド・海外レジストリ・海外CI/CD基盤への依存、制御システムに対する攻撃、量子計算機時代に向けた暗号移行等を踏まえると、従来型の情報管理、境界防御、インシデント対応中心の基準だけでは不十分だと考えられる。	重要インフラ防護に係る御意見として承ります。本ガイドラインは、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の詳細事項を記載するものです。また、重要インフラ統一基準において、政府機関は、各分野における安全基準等の整備を含め、重要インフラ事業者等における分野・事業者横断的に講ずべき対策の推進を図るため必要な施策を実施することとしております。

7	重要インフラのサイバーセキュリティ確保は、一度の文書確認で完結するものではなく、資産管理、脆弱性管理、構成管理ログ管理、監査、インシデント対応、委託先管理、サプライチェーン管理と継続的に連動する必要がある。 そのため、本ガイドライン及びこれに基づく安全基準等は、人間向け文書に加えて、機械可読な形式でも提供すべき。	御意見として承ります。今後、所管省庁等において、各分野の安全基準等の整備やそれらの浸透に向けた取組の実施が想定されますが、重要インフラ事業者等においても、本ガイドラインや各分野の安全基準等の内容について対策へ反映いただけるよう、重要インフラ統一基準に基づく施策や関連ツールの充実化等を進めてまいります。
8	制御システム・OT環境では、可用性、安全性、リアルタイム性、長期稼働、認証済み構成の維持、ベンダー保守制約、停止困難性等のため、ITシステムと同一の対策をそのまま適用することが困難又は危険な場合がある。 したがって、本ガイドラインには、OTに対して対策を適用できない場合の「免除」ではなく、「代替統制」の考え方を明記すべき。 また、OT環境では、IT部門だけでなく、現場運用部門、設備部門、安全管理部門、保守ベンダー、メーカー、委託先を含む責任分界が重要である。	本ガイドラインでは、制御システムへの適用が容易ではない場合が想定される対策については、当該対策の（解説）等に、代替手段等を記載しております。例えば、3.6③-1（解説）において、パッチ適用等が不可能又はパッチ適用等によって可用性や安全性を損なうおそれのある制御システムについては、ネットワークの物理的又は論理的分離等を実施することとしています。 また、各対策事項は、原則として制御システムにも適用されることを想定しております（1.3）。
9	中小規模の団体も多く含まれる重要インフラ事業者等に対して、 本ガイドラインは、成熟度モデルに基づき、以下のように基準を階層化すべき。 ・最低限必須基準 ・標準基準 ・高度推奨基準 ・重要システム向け追加基準 ・OT向け追加又は代替基準 ・AI利用時の追加基準 ・サプライチェーン高依存時の追加基準 また、国は、重要インフラ事業者等が実装しやすいよう、以下の支援を提供すべき。 ・共通テンプレート ・機械可読チェックリスト ・小規模事業者向け簡易リスク評価手法 ・標準的な資産台帳項目 ・SBOM作成支援 ・共同SOC ・共同監査 ・共同訓練 ・インシデント報告様式の標準化 ・委託契約条項のひな形 ・分野別ベストプラクティス ・教育教材 ・自動診断ツール 重要なのは、基準を作ること自体ではなく、現場で継続的に実装され、改善され、監査可能になることである。	御意見として承ります。本ガイドラインでは、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事項を「講ずべき対策事項」、分野・事業者によっては直ちに実施することが困難である場合が想定されるが、可能な範囲で講ずることが望ましい対策事項を「講ずることが望ましい対策事項」として記載しており、後者については、所管省庁等が各分野における重要インフラ事業者等の対策状況等を踏まえ判断の上、安全基準等に規定することとなっております。 また、2.1③-1（解説）のとおり、現段階におけるセキュリティ対策の実施状況等の実態把握に際しては成熟度モデルを採用し、改善すべき対策の優先順位を明確化し、継続的なセキュリティ水準の向上を図ることとしております。 重要インフラ事業者等への支援策についても、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。

10	本案では、「講ずべき対策事項」と「講ずることが望ましい対策事項」が多数示されている一方、本ガイドラインは所管省庁等が各分野の安全基準等を策定するための参照文書であり、解説について一律の対応を求めるものではないことも記載されている。 このため、「講ずべき対策事項」という表現が、法令上の義務なのか、各分野の安全基準に盛り込むべき事項なのか、事業者に対する事実上の義務なのかについて、現場で混同される可能性がある。 法令上義務付けられる事項、行政上のガイドラインとして求める事項、リスクに応じて推奨する事項を明確に区分すべき。特に事業者の規模、サービスの重要度、想定される被害、既存システムの技術的制約等を考慮し、形式的に全事業者へ同一の対策を求めるのではなく、実質的なリスク低減につながる比例的な運用とすることを求める。	1.5に示すとおり、「講ずべき対策事項」は、所管省庁等が、本ガイドラインを参照しつつ、各分野の特性・実情等を踏まえて安全基準等を策定し、分野・事業者横断的なセキュリティ対策の水準の底上げ等を図ることを目的としております。 また、重要インフラ統一基準第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（1.1）。
11	政府が個人情報保護法緩和で国民の個人情報を無断で売り買いしておいて、「サイバーセキュリティ」も何も無いだろう。行政・企業やAI へのデータ提供を強要するなど言語道断。サイバーセキュリティの最大の欠陥は「人」だと言われる。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。
12	幾らセキュリティを強化したところで、国がネット監視などというプライバシー侵害を行っていては、全く無意味だろう。憲法に従い、通信の秘密を守れ。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。
13	本ガイドラインには、抽象的な努力義務や各分野任せの記述にとどまらず、現代のサイバーリスクに対応できる実効的な基準策定原則を明確に盛り込むべきである。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものです。また、重要インフラ統一基準において、政府機関は、各分野における安全基準等の整備を含め、重要インフラ事業者等における分野・事業者横断的に講ずべき対策の推進を図るため必要な施策を実施することとしております。
14	安全基準等策定ガイドラインは、各府省庁や各業界が形式的なチェックリストを作るための文書ではなく、分野横断的に最低限守るべき基準、継続的改善の方法、評価・監査の考え方、事故発生時の責任ある対応を示すべきである。	本ガイドラインは、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の詳細事項を記載するものです。また、重要インフラ統一基準において、政府機関は、各分野における安全基準等の整備を含め、重要インフラ事業者等における分野・事業者横断的に講ずべき対策の推進を図るため必要な施策を実施することとしております。
15	本ガイドライン案も、単独の文書としてではなく、基幹インフラ制度、政府統一基準、重要電子計算機に対する不正行為被害防止法制、経済安全保障推進法、デジタル社会形成基本法、個人情報保護法、各業法上の安全確保義務と接続するものとして整備されるべきである。	本ガイドラインは、サイバーセキュリティ基本法に基づき策定される重要インフラ統一基準の下で作成するものであり、重要インフラ統一基準においては「統一基準に基づき、重要インフラのサイバーセキュリティ強化を図るに当たっては、他法令との整合性に留意する」としております（例えば、本ガイドライン2.9②-9において同趣旨に基づく対策を記載）。
16	ゼロトラスト、最小権限、多要素認証、ネットワーク分離、バックアップのオフライン保管、復旧手順の定期演習、ログの集中管理、時刻同期、EDR、SIEM、異常検知、権限昇格の監視、重要データの暗号化、ランサムウェア対策、サプライチェーン侵害時の切替手順を安全基準に含めるべきである。特に、航空、医療、電力、通信、上下水道、金融、行政手続等では、単なる情報漏えい対策ではなく、サービス継続性、手動運用への切替、代替経路、災害時対応との統合が不可欠である。	本ガイドライン1.2では、「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」という点について考え方を述べています。 また、考え方の提示のみならず、個別の施策についても多岐にわたる対策項目の記述の中で定めております。

17	中小企業・地方自治体・医療機関・教育機関等に過度な負担を課さない実装支援が必要である。安全基準が高度化するほど専門人材や予算を持つ大規模組織と、小規模組織との格差が拡大する。結果として、重要な地域サービスが形式的準拠に追われ、実効的対策が進まないおそれがある。ガイドラインには、対象組織の規模、リスク、機能重要度に応じた段階的基準共通テンプレート、共同調達、共通監査、クラウド利用時の標準設定、自治体向け支援、人材育成、演習教材、相談窓口を位置付けるべきである。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものであり、今後、所管省庁等において、各分野の安全基準等の整備やそれらの浸透に向けた取組の実施が想定されますが、重要インフラ事業者等への支援策についても、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。
18	国民の「損害賠償請求権」を担保する規定の整備被害を受けた国民（住民・利用者）が、事業者および国に対して迅速かつ適切に損害賠償を請求できるよう、ガイドラインや関連する運用の中で「過失（セキュリティ義務違反）」の判断基準を明確にすべき。また、精神的苦痛に対する慰謝料や実際の金銭的被害に対する賠償金について、事業者が十分な補償能力（サイバー保険の加入義務化など）を備えるよう、具体的なインセンティブや規定を設けることを期待する。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。
19	海外製AIや通信アセットのソースコード・通信プロトコルを100%可視化させる。政府の厳格な事前監査をパスしない限り、インフラへの接続や輸入を一時停止（スタンドスティル）させる運用基準の策定を要求する。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。
20	インフラと外資AIの結合が招く非同意下の生体データ取得やステルス電磁波干渉を公式監査対象とし、深部の状況調査を実施する。市民の包括的拒否（オプトアウト）に対し、対象空間へのビーム照射等を物理的に回避・遮断（ヌリング）するシステム実装の義務化を要求する。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。
21	重要インフラの安全確保に向け、海外アセットの自己申告に依存せず、3大国家機関の最高次技術を横断動員する常設型能動監査基準の明文化を要求する。具体的には、NICTによる異常パケットの24時間逆探知および電磁界相殺（アクティブ・キャンセル）、産総研（AIST）による隔離環境でのコード監査、QSTによる電磁的干渉の臨床医学的検証（除外診断）と国家監査体制の確立をガイドラインへ実装すること。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。
22	先回り対策を永久に無効化する「情報通信防衛エコシステム」への段階的技術展開基準の追加防御アセットを一部の国家機関に固定した場合、外部からその測定限界を突いた対策（アップデート）を講じられるリスクがある。これを防ぐため、初期は3大国家機関の最高次技術を活用しつつ、中長期的にこれらの防衛・医療技術を国内の民間企業や大学へ段階的に移転・普及（エコシステム化）させる基準の追加を要求する。官民一体で常時検証・中和し続ける自律的な「情報通信防衛エコシステム」を構築することで、外部アセットによる予測不可能な先回り対策を永久に無効化し、最高次の技術主権を確立すること。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。
23	法人税・所得税・固定資産税等の大幅減税、サイバーセキュリティ投資の即時償却・税額控除の拡充、および日本人技術者・セキュリティ人材の育成・雇用に対する優遇税制を指針に明記すべき。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。
24	指針において「リスクベース」「分野の実情を踏まえ」と述べるだけでは甘い。行政事務を半減以上に削減することを数値目標化し、報告・申請のワンストップ化・デジタル完結・書類最小化・審査期間短縮を義務付けてください。国による把握・分析・評価・改善のPDCAも、民間負担を増やさない形に限定し、官僚主導の規制強化・事務肥大化を排除すべき。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。

25	本ガイドライン案が、完全な防御が困難であることを明確に認識し、レジリエンス、サプライチェーン管理、データ保護、バックアップ、対応・復旧等を包括的に整理していることを支持する。	賛同意見として承ります。
26	高性能AI登場による脅威レベルの進化にあわせてサイバーセキュリティ対策のベースラインを抜本的に見直し、一定規模以上の重要インフラ事業者については、全方位的な底上げを検討すべき。 現在、高性能AIの登場により、サイバー攻撃の大規模化、高速化、自動化、不休化といった脅威環境におけるパラダイムシフトが起きている。 このような状況において、パスワードのみによるアカウント認証・境界防御のみのパッチ未適用環境・ログの集中管理/保全の未実施のように、サイバーハイジーンのレベルで課題のある状況を見過ごし続けることで、我が国への甚大かつ大規模なサイバー攻撃が発生しうる状態を放置することとなる。 高性能AIのような新たな脅威の出現をきっかけとして、重要インフラ事業者に対して、これまで「当たり前」としていたサイバーセキュリティ対策のベースラインを適切に見直す必要があると考える。	本ガイドラインでは、1.6安全基準等策定ガイドラインの改定において、重要インフラ統一基準の見直し頻度を踏まえ、本ガイドラインについても適切な頻度において、技術や脅威等、重要インフラを取り巻く環境変化に応じた見直しを行うことを定めております。
27	一定規模以上の重要インフラ事業者については、制御システムのセキュリティ対策について、抜本的な底上げを求めるべき。 本文書における、抜本的に見直すべき制御システムのセキュリティ状況を以下に列挙する。 ・（性能問題などを理由とした）マルウェア対策が利用不可な製品利用の許容 ・セキュリティ対策を過度に犠牲とした可用性（安定稼働）の確保 ・認証機能未搭載製品・デフォルトパスワード変更不可製品の許容 ・ログ機能非搭載機器に関する利用の許容 ・パッチ未適用状態の許容 ・通信の非暗号化状態の許容 ・ネットワーク分離を根拠としたセキュリティ対策未実施機器利用の許容 ・ペネトレーションテストの未実施	御意見として承ります。本ガイドライン1.3に示す通り、「２　組織統治」以降に記載の各対策事項は、「［ITシステムのみ］」と記載しているものを除き、原則として制御システムにも適用されることを想定しております。
28	本案が対象とする「安全基準等」には、法令に基づく強制基準、政府の推奨基準、業界ガイドライン及び各事業者の内規までが含まれている。そのため、「講ずべき対策事項」が法的義務なのか、原則として実施すべき事項なのか、未実施理由を説明すれば足りる事項なのかが明確ではない。 対策項目ごとに、法的義務の有無、対象となる事業者・システム、適用時期、未実施の場合に必要な代替措置及び説明手続を一覧表で示すべき。また、ガイドラインへの不適合が直ちに経営者の善管注意義務違反等を意味するものではないことも明確にすべき。	1.5に示すとおり、「講ずべき対策事項」は、所管省庁等が、本ガイドラインを参照しつつ、各分野の特性・実情等を踏まえて安全基準等を策定し、分野・事業者横断的なセキュリティ対策の水準の底上げ等を図ることを目的としております。 また、重要インフラ統一基準第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（1.1）。
29	本案では「重要システム」の範囲を各事業者が定めることとされているが、事業者が費用等を理由に対象範囲を過度に狭く設定するおそれがある。重要システムに直接接続する周辺システム、認証基盤、遠隔保守設備、委託先及びクラウドサービスが対象外となれば、対策の実効性は確保できない。 国が重要度の判定基準及び全分野共通の最低対策を定め、特に重要度の高いシステムについては、定期的な第三者監査を原則とすべき。人員不足等を理由に自己点検のみで済ませることは、最重要システムについては認めるべきではない。	本ガイドラインでは、安全基準等における対象範囲の設定に当たっては、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よう求めています（1.3）。
30	電力、水道、交通、医療、工場等の制御システムでは、パッチ適用、暗号化又は監視ソフトの導入自体が、システムの停止や誤作動を引き起こす場合がある。 代替措置を認める条件、承認者、実施期限、記録方法及び第三者確認の方法を明確にした上で、各重要インフラ分野の特性に応じた附属書を策定すべき。	御意見として承ります。各対策事項について具体的に求められる内容は、分野や対象のシステム等により異なり得るところ、本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の詳細事項を記載するものであるという点を踏まえ、今後の各分野における安全基準等の検討を含め参考にさせていただきます。

31	クラウド対策の参考資料として2013年度版の資料が掲載されているが、現在のクラウド、ゼロトラスト、生成AI及び国外データ移転をめぐる環境とは大きく異なる。古い資料を参照資料として残す場合には、現在も有効な範囲を明示すべき。 また、AI対策、耐量子計算機暗号への移行等について、具体的な中間期限と実施工程を定めるべき。原則3年ごとの見直しだけでなく、重大な脆弱性、新たな攻撃手法又は技術革新が生じた場合に、随時改定できる仕組みが必要である。	本ガイドラインでは、1.6安全基準等策定ガイドラインの改定において、重要インフラ統一基準の見直し頻度を踏まえ、本ガイドラインについても適切な頻度において、技術や脅威等、重要インフラを取り巻く環境変化に応じた見直しを行うことを定めております。
32	本案は抽象的な概念論が多く、現場の壁に貼り出して誰もが直感的に使える「判断基準・切り分け手順・タイムスケジュール」を1枚にまとめた共通シート（別紙等）が存在しない。これでは、専門のITエンジニアがいない事業者や協力会社が対策を構築できずに孤立してしまう。政府は単に対策を丸投げするのではなく、各企業の進捗を確認し、実務に伴走する「政府公認のサイバーセキュリティ・コーディネーター」を組織内に配置し、現場を路頭に迷わせない仕組みを明記すべき。	御意見として承ります。各重要インフラ事業者等のサイバーセキュリティ対策促進に向け、重要インフラ統一基準に基づき、重要インフラ所管省庁において、各分野の安全基準等の浸透に向けた取組推進を含め、必要な施策を実施していくことを想定しています。
33	本ガイドラインでは、重要インフラ事業者等に求められる対策が詳細かつ網羅的に示されており、サイバーセキュリティ水準向上に大きく寄与するものと考える一方で、地方公共団体や中小規模事業者が重要インフラサービスを担うケースにおいては、人的・財政的資源が限られているため、全ての対策を同一レベルで実践することは困難である。そのため、対策事項を、 最低限実施すべき事項、段階的な成熟度向上を目指す事項、高度な組織向け事項等にを区分した「実装レベルモデル」を併せて提示することを要望する。	御意見のとおり、コスト・人材・専門知識等の観点から、必ずしも全ての事業者にとっては導入が容易ではないと考えられる対策もあり得ますので、本ガイドラインでは「講ずべき対策事項」とは別に「講ずることが望ましい対策事項」を記載し、後者については、所管省庁等が、各分野において重要インフラ事業者等の対策状況等を踏まえ判断の上、安全基準等に規定することを想定しています。
34	安全基準等策定ガイドライン（案）にて、重要インフラ事業者として具体的に対応すべき事項が記載されたことで、事業者のサイバーセキュリティ確保の取組や、各分野のばらつき解消・全体的な底上げの実効性が高まるものと考えている。 当社も、今後策定される安全基準等も見据えながら、本ガイドラインを参考に必要な対応を進めていく。	賛同意見として承ります。
35	講ずべき対策事項、講ずることが望ましい対策事項、と記載されているが、前者は「勧告」、後者は「推奨」と解釈してよいか。	本ガイドラインでは、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事項を「講ずべき対策事項」、分野・事業者によっては直ちに実施することが困難である場合が想定されるが、可能な範囲で講ずることが望ましい対策事項を「講ずることが望ましい対策事項」として記載しております（1.5）。
36	画一的かつ高度な安全基準が適用された場合、資金力や専門人材の乏しい地方の小規模なインフラ事業者が基準をクリアできず、事業からの撤退やサービスの縮小を余儀なくされるリスクがある。 これが結果として、地方における住民の生活利便性や生存権を脅かす「地方インフラの崩壊」を招かないよう、事業者の規模に応じた段階的な措置や柔軟な例外規定、伴走型の支援体制を担保すべきである。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものであり、今後、所管省庁等において、各分野の安全基準等の整備やそれらの浸透に向けた取組の実施が想定されますが、重要インフラ事業者等への支援策についても、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。
37	1.3「「閉域網だから安全」、「専用OSだから安全」、「独自技術仕様だから安全」といった過信…」について、より正確な見通しを得るためには、脅威モデリングの活用に関する指針を提示することで、システム管理者がセキュリティ態勢をより適切に評価できるようになる。	本ガイドラインでは、御指摘の点について、1.3で原則を示すとともに、例えば、2.9②-4にて外部委託におけるサイバーセキュリティに配慮した開発等の確認、3.4①-1等においてリスクアセスメントの実施及びその結果に基づくリスク対応の実施について定めております。
38	1.6「原則として３年に１度、見直しを行うこととされている」という点について、ここ数ヶ月で脅威の状況が劇的に変化していること（攻撃的なAIの脅威はその一例）を考慮すると、3年という更新間隔は、強固なセキュリティ体制を維持するには長すぎると懸念される。 本ガイダンスに加え、重大な事象や継続的な状況変化に対し、適時かつ追加的な指針を提示できる「迅速対応専門家パネル」の設置を推奨する。	本ガイドラインでは、1.6安全基準等策定ガイドラインの改定において、重要インフラ統一基準の見直し頻度を踏まえ、本ガイドラインについても適切な頻度において、技術や脅威等、重要インフラを取り巻く環境変化に応じた見直しを行うことを定めております。また、重要インフラ統一基準の改定等に際しては、有識者で構成されるサイバーセキュリティ推進専門家会議や重要インフラサイバーセキュリティ研究会の意見を聴取していくことを想定しています。

	意見の概要	意見に対する考え方
	「2 組織統治」に係る意見	
39	供給者・委託先の管理にあたって、委託先企業の規模、取扱データの重要度、およびアクセス権限の程度に応じたリスクベースのグラデーション（段階的・優先順位付けした適用）を許容し、中小企業等への対策要請にあたっては、政府やIPAが提供する支援施策や標準的なチェックシートの活用を推奨する等、過度な実務負担とならないよう配慮する旨を2.9①および2.9②の「解説」に追記すべき。	本ガイドラインでは、2.9②-1において、サプライチェーン・リスクに関するリスクアセスメントを実施し、リスクに応じた対応（供給者や委託先の選定・管理・対策の助言等）を行うこととしています（2.9②-6においても、供給者・委託先の重要度を踏まえて優先順位付けの判断基準を定め、適用することとしています。）。また、2.9②-1の（解説）において、政府機関が提供する中小企業等への支援施策（サイバーセキュリティお助け隊 等）の活用等について記載しております。
40	「CISO等はCIO等と兼務ではなく専任者として任命することを検討する」と記載されているが、特に地方の事業者や中規模インフラ事業者においては、セキュリティ人材の深刻な不足により専任CISOの確保が極めて困難であることから、2.5.1②-1の「解説」において、CISO等の専任化の検討にあたっては、組織の規模、業務内容、およびリスクの状況を考慮し、人材資源の制約等により専任者の配置が困難な場合であっても、適切な権限と責任が与えられ、経営層へ直接報告できる体制が確保されているときは、兼務や外部専門組織・グループ全体の体制を活用した補完を妨げるものではない旨の補足をいただきたい。	本ガイドラインでは、2.5.1②-1の（解説）において、「牽制も含めたCISO等の機能の実効性の確保の観点から、CISO等をCIO等と兼務ではなく、専任者として任命することが考えられるところ、組織の規模等も考慮の上、検討する」ことを記載しております。
41	OS、コンテナ、暗号ライブラリ、ネットワークスタック、監視ツール、ビルドツール、CI/CD、データベース、AI基盤、Web基盤等、重要システムの多くはOSSなしには成立しない。 したがって、OSSは単なる無償の外部部品ではなく、重要インフラを構成する基盤的サプライチェーンとして扱うべき。 国として、重要インフラ向けに、検証済みOSSパッケージ、国内ミラー、署名検証基盤、脆弱性情報連携基盤、長期保守パッケージ基盤を整備・推奨することが望ましい。 また、重要インフラ事業者等がOSSを利用する際には、「OSSを使っているか否か」ではなく、「どのOSSを、どの経路から、どの検証を経て、どの責任分界で、どの更新体制により利用しているか」を管理対象とすべき。	御意見として承ります。本ガイドラインでは、2.9③-1において、OSSを含め、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選定基準の整備や要求事項の整理を求めております。また、③-4において「不正機能等の埋め込みに係る脅威に対応するための対策」の実施を記載しております。御指摘の点については、上記観点における詳細な対策事項と認識しておりますところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
42	本案2.9では、海外拠点について、現地の法令や文化等を踏まえたリスク対応を行うとし、その具体例として、法制度や実施体制が十分でないこと、法執行が不透明であること、権力が独裁的であること、国際的な取決めを遵守しないこと等のカントリーリスクが挙げられている。 この考え方は重要だが、どのような場合に供給者・委託先の利用を制限し、あるいは追加的な安全措置を求めるのかについて、具体的な判断基準が示されていない。 重要インフラは国民生活及び国家安全保障に直結することから、単なる価格や技術水準だけではなく、当該事業者が所在する国・地域の法制度、政府による企業やデータへのアクセス権限、司法及び法執行の透明性、国際的ルールの遵守状況、政府から企業への影響力等を含めた経済安全保障上のリスクを評価すべき。 特にリスクが高いと判断される供給者については、代替調達先の確保、ネットワーク分離、重要情報へのアクセス制限等を講じることを、安全基準等に明記することを求める。	各重要インフラ分野・事業者で想定されるサプライチェーン・リスクとその対応は、各分野・事業者の特性・実情等によって様々であることから、一義的な記載はせず、各分野・事業者においてリスクアセスメントを実施することが重要であると考えています。その上で、各分野での安全基準等においては、必要に応じ、より具体的な記載をされることもあり得るものと考えています。
43	本案では、サプライチェーンに参加する中小企業に対し、大企業が対策を要請するだけではなく、具体的な助言・支援を行うことや、政府の支援施策を利用することが示されており、この方向性には賛成するが、重要インフラ事業者が高度なセキュリティ基準を委託先に求める結果、その費用や人的負担が中小企業に一方的に転嫁されれば、取引先から中小企業が排除されたり、形式的な対応のみが増えたりするおそれがある。 そのため、大企業等が取引先に追加的なサイバーセキュリティ対策を求める場合には、その必要性及びリスクに応じた合理的な水準とするとともに、費用負担、技術支援、共同対策等を含めた支援を行うことを明確にすべき。 また、共通評価制度や標準様式を活用し、発注者ごとに異なる調査・報告を中小企業へ重複して求めない仕組みを構築することを求める。	本ガイドラインでは、2.9②-1（解説）において、独占禁止法及び取適法を考慮したパートナーシップ体制を構築する点を記載するとともに、①-1（解説）において、供給者・委託先のセキュリティ対策の状況把握に係る第三者による評価検証結果の活用による把握の負担軽減についても記載しております。

44	本案では、不正機能等の埋め込みに対する対策について、SBOMの作成・提供を調達先に求めることなどが例示されているが、「講ずることが望ましい対策事項」とされている。 しかし、重要インフラを構成するソフトウェアや機器について、どのソフトウェア部品が使用され、どのような脆弱性が存在し得るのかを把握できない状態は、サプライチェーン攻撃への対応上大きな問題であり、特に国民生活や国家安全保障への影響が大きい重要システムについては、SBOM又はこれと同等のソフトウェア構成管理、脆弱性発見時の通知、製品のサポート期間、更新・変更時の通知、安全な開発体制の確認等について、「望ましい対策」にとどめず、原則として求めるべき対策として位置付けることを検討すべき。	御意見として承ります。「講ずることが望ましい施策」は、分野・事業者によっては直ちに実施することが困難である場合が想定されるが、機微な情報を取り扱っている、標的にされやすい等の理由から特にセキュリティリスクの高いサービス・事業者・分野等において必要になると考えられる対策など、可能な範囲で講ずることが望ましい対策事項と定義しており、不正機能等の埋め込みに係る脅威に対応するための対策はこれに該当するものと考えています。その上で、御意見はSBOMを含むソフトウェアの構成管理等の重要性と認識しており、今後の各分野における安全基準等の検討に当たって参考にさせていただきます。
45	安全基準には、SBOM（Software Bill of Materials）の作成・更新・提出、依存関係の継続的監視、既知脆弱性への対応期限、サポート切れ部品の使用禁止又は例外管理、コード署名、成果物署名、改ざん検知、再現可能ビルド、セキュアなCI/CD、パッケージレジストリの信頼性確認を含めるべき。 特に、重要インフラで用いられるソフトウェアについては、納入時点の一回限りの確認では不十分であり、運用期間中に新たに判明する脆弱性に対応する継続的義務を求めるべきである。	本ガイドラインでは、2.9③-1において、ソフトウェアを含む製品・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選定基準の整備や要求事項の整理を行うことを求めております。また、（解説）において、SBOM等の代表的な制度及びガイドライン等を参照の上、必要な対策を講ずる点を補足しています。
46	ガイドラインには、調達仕様書に盛り込むべき最低限のセキュリティ要件を例示すべきである。具体的には、SBOM提出、脆弱性対応体制、セキュリティ更新の提供期間、重大脆弱性発見時の通知期限、ログ取得機能、監査協力義務、第三者検証の受入れ、クラウド利用時のデータ所在と権限管理、委託先・再委託先管理、廃棄時のデータ消去、契約終了時の移行支援を含めるべきである。また、ベンダー固有技術への過度な依存を避けるため、標準仕様、オープンフォーマット、API、データ可搬性、相互運用性を評価項目に含めるべきである。	本ガイドラインでは、2.9③-1において、ソフトウェアを含む製品・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選定基準の整備や要求事項の整理を行うことを求めております。また、（解説）において、代表的な制度及びガイドライン等を参照の上、必要な対策を講ずる点を補足しています。その際、調達仕様書に盛り込むべき対策については、各分野の安全基準等に基づき、各事業者等において想定されるリスク等を踏まえつつ必要に応じて選定することを想定しております。
47	事案発覚時には「何が、いつ、どのように漏洩したか」という正確な事実関係の公表、および経営トップによる公式な謝罪記者会見の迅速な実施を、ガイドライン上の明確な「義務」として規定してください。	重要インフラ統一基準の第３部では、所管省庁等が策定する安全基準等において、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しているところ、本ガイドラインは、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の詳細事項を記載するものです。 事案発覚時の情報開示については、攻撃者の攻撃を助長する可能性等を考慮し得るところ、2.7①-1において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ともに、被害拡大防止には、公表に限らず関係主体間での情報共有が重要であるところ、3.3①-1において行動計画に基づく情報共有の手引書及び「サイバー攻撃被害に係る情報の共有・公表ガイダンス」も踏まえて組織外との情報共有を実施する点を記載しております。
48	中国製機器に加え、中国人による遠隔操作・データ不正取得・ランサムウェア連携・内部犯行のリスクを、すべての対策フェーズ（組織統治・識別・防御・検知・対応復旧）で最優先リスクとして位置づけ、排除を義務化すべき。	重要インフラ統一基準は、特定の国や企業の製品を排除するものではありませんが、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の観点において、本ガイドライン2.5.4では、重要インフラ事業者等における役職員の管理を求め、また、2.9では、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。

49	「安全基準等策定ガイドライン（案）」および統一基準関連を抜本的に改め、中国製品排除・中国人排除・日本人ファースト・大幅減税・行政事務大幅削減を核心に据えた内容とすることを強く求める。これらを反映しなければ、本制度は形骸化し、重要インフラの真の防護と国家・国民の安全を確保できない。	重要インフラ統一基準は、特定の国や企業の製品を排除するものではありませんが、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の観点において、本ガイドライン2.5.4では、重要インフラ事業者等における役職員の管理を求め、また、2.9では、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。
50	重要インフラ事業者自身が高度なセキュリティ対策を実施していても、委託先、再委託先、クラウドサービス事業者、保守事業者等を経由して重要情報に到達されれば、サプライチェーン全体としての防御は成立しない。そこで、供給者・委託先の選定や契約上の要求事項、第三者評価等において、 ・重要データを必要以上に保持しないこと ・重要データを一か所に利用可能な状態で集中させないこと ・データの所在・保管方法を把握すること ・暗号化等による保護を行うこと ・必要に応じて秘密分散等によるデータの分散・無意味化を検討すること ・一部のシステム又は事業者が侵害されても、それだけでは重要情報を復元・利用できない構成を検討すること 等を、リスクに応じたデータ保護策として位置付けることが有効と考える。 また、今後SCS評価制度がサプライチェーン企業のセキュリティ水準を可視化する仕組みとして活用されていくのであれば、将来的には「侵入防止能力」だけでなく、「侵害発生後に重要データへの被害をどこまで限定できるか」という耐侵害性・被害最小化の観点についても、評価項目又は評価の参考事項として検討することを要望する。	御意見として承ります。供給者・委託先の選定等については、本ガイドライン2.9において、サプライチェーン・リスクマネジメントの実施を求めております。御指摘の点については、上記観点における詳細な対策事項と認識しておりますところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
51	供給者・委託先などのサプライチェーンセキュリティ対策については、政府などの第三者がセキュリティ認証を与えた事業者が提供する製品・サービスの調達をベースラインとすべき。（例：JC-STAR、ISMAP/ISMAP-LIU、情報セキュリティサービス基準適合サービスリスト、サイバーセキュリティお助け隊、SCS評価制度など） 本文書では、サプライチェーン・リスクマネジメントの観点で参考とすべきガイドラインを多数例示している一方で、重要インフラ事業者において、全てのガイドラインを理解し、セキュリティレベルを維持していくことはきわめて困難であると考えられる。 このため、政府などの第三者機関によってセキュリティ認証を与えた供給者・委託先の製品・サービスリストを調達ベースラインとして活用を促していくことにより、重要インフラ事業者全体のセキュリティレベルの底上げが期待できる。また、重要インフラ事業者における供給者・委託先の選別に関する経営コスト削減にも寄与することが期待できる。	本ガイドラインでは、2.9①-1及び2.9③-1（解説）において、供給者・委託先などのサプライチェーンセキュリティ対策に関して、代表的な制度及びガイドライン等を参照の上、必要な対策を講ずる点を補足しております。
52	一定規模以上の重要インフラ事業者については、重要システムの利用権限を持つ事務従事者に対して、一定のシステム利用適性確認（いわゆるバックグラウンドチェック）を観点として挙げるべき。 IPAの発行する「情報セキュリティ10大脅威」では、11年連続で「内部不正による情報漏えい」が挙げられている。このような、人にまつわる脆弱性への対策の一つとして、利用者に対するシステム利用の適格性確認の観点についても検討する必要がある。	御意見として承ります。本ガイドラインでは、2.5.4①-1において、役職員（特に重要システムの構築・運用に携わる職員）について、情報やシステムの重要度に応じて、配置・管理することを求めております。
53	発注者に対し、必要な費用の適正な負担、技術支援、十分な準備期間及び共同実施を求めるべき。また、取引上の立場を利用して、合理的な移行期間を設けず取引を停止したり、対策費用を価格に反映させなかったりすることを防ぐ規定が必要。 国としても、共通の無料評価ツール、標準契約書、相談窓口、補助金及び専門家派遣制度を整備すべき。	本ガイドラインでは、2.9②-1（解説）において、独占禁止法及び取適法を考慮したパートナーシップ体制を構築する点を記載するとともに、①-1（解説）において、供給者・委託先のセキュリティ対策の状況把握に係る第三者による評価検証結果の活用による把握の負担軽減について記載しております。 また、2.9②-1の（解説）において、政府機関が提供する中小企業等への支援施策（サイバーセキュリティお助け隊等）の活用等についても記載しております。

54	サイバーセキュリティに関する取組やインシデントの発生状況を「可能な範囲」で公表するという規定だけでは、事業者によって開示水準に大きな差が生じる。一方、システム構成や防御上の弱点を過度に公表すれば、新たな攻撃を誘発する危険がある。 公表が必要となる重大性の基準、公表時期、最低限の公表項目、公表してはならない情報及び利用者への個別通知が必要となる場合を、国が統一的に示すべき。	本ガイドライン2.7①-1（解説）に記載の通り、情報開示の対象・内容や開示のタイミングは、攻撃者の攻撃を助長する可能性等を考慮の上、適切に決定される必要があると考えております。その上で、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」等を参照いただくことを想定しています。
55	特定国製機器（バックドア等のリスクが懸念されるもの）の原則使用禁止、またはSBOM（部品構成表）の義務化を基準に明記すべき。同時に、安全なインフラを維持するため、国が主導してセキュリティ要件を満たす「国産機器・ソフトウェア」の開発支援や導入補助を行い、サプライチェーンの安全保障（デジタル・ソブリン）を日本国内で完結させるべき。	サプライチェーン・リスク対策の重要性の観点において、本ガイドライン2.9では、重要インフラ事業者等においてサプライチェーン・リスクマネジメントを求めることとしております。
56	重要システム統一基準及び安全基準等策定ガイドラインの今後の運用に当たっては、重要インフラ事業者及び関係事業者が本ガイドラインをより実務的に活用できるよう、特に、サプライチェーンを構成する多様な事業者との連携や役割分担については、実際の運用において判断に迷う事例も想定されることから、具体的な適用事例や考え方の充実や適宜な情報発信及び見直しを期待する。	賛同意見として承ります。サプライチェーン・リスクマネジメントを含め、所管省庁等を中心に、各分野の安全基準等の整備やそれらの浸透に向けた取組の実施を進めてまいります。
57	当社は、政府に対して以下を提言する。 •重要インフラ分野全体で使用できる、標準化されたサプライヤーセキュリティ質問票および証拠提出様式を策定すること •サプライヤー保証において「一度収集し、何度でも利用する」モデルを導入すること •広く認められた第三者認証、独立した保証報告書および標準化された評価制度への依拠を明示的に認めること •同等の国際的な保証の枠組みを認めること •サプライヤーが安全で再利用可能な保証ポータルを通じて証拠を提供できるようにすること •サプライヤーの重要度、システムへのアクセス、データの機微性および潜在的な運用上の影響に応じて、保証要件を階層化すること •サービス、脅威環境またはサプライヤーのリスクプロファイルに重大な変更がない限り、評価を繰り返さないこと •重複した評価を防ぐため、提案されている「サプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）」を、[10] 国内外の既存の枠組みと連携させること	御意見として承ります。本ガイドラインでは、2.9①-1及び2.9③-1（解説）において、供給者・委託先などのサプライチェーンセキュリティ対策に関して、SCS評価制度など、代表的な制度及びガイドライン等を参照の上、必要な対策を講ずる点を補足しておりますが、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
58	当社は、政府に対して以下を提言する。 •分野横断的に一貫して使用できる、リスクベースのモデル契約条項を公表すること •列挙された契約事項が、すべての調達において義務付けられるものではないことを明確にすること •事業者に対し、サービスのリスクおよび重要性に応じて条項を選択するよう求めること •広く認められた第三者保証報告書によって通常の監査要件を満たせるようにするとともに、サイバーセキュリティ監査要件上必要な場合には、ISO/IEC 27001などの国際的な監査基準と整合させること •監査対応の負担はセキュリティへの注力を弱めるため、顧客による直接監査は、他の保証手段では対応できない、根拠のある重大なリスクが存在する例外的な状況に限定すること •監査について、機密保持、対象範囲、セキュリティおよび頻度に関する合理的な制限を適用すること •再委託先への義務の適用を、重要サービスの提供に実質的に関与する事業者に限定すること •他の顧客または共有インフラのセキュリティを損なう情報の開示をサプライヤーに求めないこと •既存契約に対して十分な移行期間を設けること	重要インフラ統一基準は、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ます。 また、本ガイドラインでは、2.9②-1（解説）において、独占禁止法及び取適法を考慮したパートナーシップ体制を構築する点を記載するとともに、①-1（解説）において、供給者・委託先のセキュリティ対策の状況把握に係る第三者による評価検証結果の活用による把握の負担軽減についても記載しております。

59	当社は、以下を提言する。 •認証を調達の自動的な条件とするのではなく、証拠の一形態として維持すること •調達主体が同等の国際認証および保証を受け入れること •日本の制度をグローバルな基準と相互運用可能なものとし、重複した試験を避けること •制度が対象製品またはサービスをカバーしていない場合には、代替的な証拠を認めること •製品のリスクおよび想定用途に比例した要件とすること •認証状況を理由として、セキュリティアップデートや最新の代替製品の適時な調達が妨げられないようにすること •新たな制度を導入する際には、移行措置および既存製品等の適用除外（グランドファザリング）を設けること •ラベルまたは認証のみに依拠するのではなく、製品全体のセキュリティ能力およびライフサイクルを調達判断において考慮すること	本ガイドラインでは、2.9③-1で、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選定基準の整備や要求事項の整理を行うことを講ずべき対策事項としています。その解説では、JC-STAR等の認定制度を参照の上、調達・利用にかかる選定基準の整備を行うことが望ましいとしていますが、認証の取得を必須としているものではなく、また、認証制度が活用できない場合や補足的な要求事項の整理に当たっては、各種ガイドラインを参照しながら、選定基準を整備することを想定しています。
60	当社は、政府に対して以下を提言する。 •特にリスクの低い製品およびサービスについて、サプライヤーによる自己適合宣言を有効な証拠として認めること •広く認められた独立した認証を標準的な保証形態として受け入れ、追加証拠の提出は製品またはサービスの重要度およびリスクによって正当化される場合に限ること •安全な開発に関する標準的な自己適合宣言書の様式を提供すること •安全な開発に関する期待事項を、広く認められた国際基準および慣行と整合させること •一律の固定した期限を課すのではなく、リスクベースのパッチ適用を維持すること •直ちにパッチを適用することで安全性、可用性または相互運用性に影響が生じ得る場合には、検証済みの代替的管理策を認めること •協調的な脆弱性開示を支援し、サプライヤーに脆弱性の調査、検証および修正を行うための合理的な期間を認めること •新たに報告された問題、確認済みの脆弱性、実際に悪用されている脆弱性、および重大なインシデントを区別すること •SBOMおよび詳細な脆弱性情報を不適切な開示から保護すること •ライフサイクル管理に関する責任共有を強化すること	本ガイドラインでは、2.9①-1（解説）において、供給者・委託先のセキュリティ対策の状況把握に係る第三者による評価検証結果の活用による把握の負担軽減についても記載しております。 また、3.6③-1で、攻撃者にAIが悪用されることにより、脆弱性の発見から悪用まで短時間で行われ、また、多数の脆弱性対応が必要となることも踏まえた上で、情報システムへのパッチ適用に関する作業方針・内容を確立するとともに、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ことを求めています。 さらに、4.4.2②では、ソフトウェアのサポート対象バージョンへの更新を計画的に実施し、サポート対象バージョンへの更新が困難な場合には、補完的な措置を講じるとともに、サポートが得られるソフトウェアを利用したシステム・ビジネスプロセスへの移行を検討することを求めています。
61	当社は、以下の要素に基づいてサプライヤーを分類することを提言する。 •支援するサービスの重要度 •重要システムへのアクセス •機微情報へのアクセス •運用上の依存度 •代替可能性 •集中リスク •サプライヤーの業務中断または侵害による潜在的な影響	本ガイドラインでは、2.9②-1で、サプライチェーン・リスクに関するリスクアセスメントを行った上で、リスク対応を行うことを求めています。御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
62	当社は、事業者に対して以下を求めることを提言する。 •特定されたリスクに対応するために必要な情報のみを収集すること •適切なアクセス制御を用いてサプライヤー情報を保護すること •第三者への再開示を制限すること •必要に応じて、一部を非開示（マスキング）とした資料または要約した資料を受け入れること •安全な証拠交換の仕組みを使用すること •営業秘密または商業上保護される情報を保護する適用法令に基づき、情報を保護すること •保存期間および削除時期を定めること •他の顧客または共有インフラを危険にさらす可能性のある情報の提出を求めないこと	本ガイドラインでは、2.9②-1で、サプライチェーン・リスクに関するリスクアセスメントを行った上で、リスク対応を行い、また、②-2で、供給者・委託先の選定に当たっては、遵守すべきサイバーセキュリティ要件を明確化するとともに、重要度に応じて、契約書等に明記することを求めています。御意見の内容は、主として、個別の契約において定められるべきものと認識しています。

63	2.6①-1（解説）において、「専門能力を有する者」のレベルを明確にするため、別箇所で記載されているように情報セキュリティサービス基準の要件を参照してはどうか。	2.6①-1（解説）の該当部は「独立性及び専門的能力を有する者」について定めるものではなく、そのような者による監査が困難な場合の対応を定めているものとなります。
64	2.9①-1（解説）における「サプライチェーンに係る供給者・委託先等の管理（サードパーティリスク管理）においては、供給者・委託先等が遵守すべきサイバーセキュリティ要件を明確化の上、重要度に応じ、契約やSLA（サービスレベルアグリーメント）等（以下「契約書等」という。）に明記することが重要である。」という記述は、②-2（p.41）と重複する内容であるため、1-1での記載は不要ではないか。	対象の記載は、サプライチェーン・リスクマネジメントのプロセス全般を通じて、供給者・委託先等が遵守すべきサイバーセキュリティ要件を明確化の上、契約書等に明記することが重要であることを踏まえ、記載しているものになります。
65	2.9②-2（解説）について、他の個所でもペネトレーションテストが求められているため「脆弱性診断やペネトレーションテスト等」と表現してはどうか。	御意見として承ります。2.9②-2（解説）の「脆弱性診断等の実施及び報告」の「等」にはペネトレーションテストも含まれますが、2.9②-2が「講ずべき対策事項」であることを踏まえ、明示まではしておりません。
66	2.9②-3について、履行状況の確認方法について、解説で例示してはどうか。	御意見として承ります。2.9②-3における詳細な対策事項と認識しておりますところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
67	今後のサービスや製品調達の際には、SCS評価制度で星を取得していることが前提となってくると思われる。2.9③-1解説部分にSCS評価制度の記載がないのは製品・サービスにフォーカスしているからか。	2.9③-1が製品（情報システムを構成する機器等を含む。）・サービスの調達・利用に当たっての対策事項である点は御理解のとおりです。
68	重要インフラ事業者に対して厳格な安全基準やシステム改修が求められる結果、莫大なコンプライアンスコストが発生することが懸念される。 民間企業におけるこのコストが、電気料金、通信費、医療費などのサービス価格の値上げや、公的支援を通じた税負担という形で、巡り巡って国民の家計を圧迫するおそれがある。 事業者に対する過度なコスト強要を防ぐための国による支援策や、費用対効果の検証メカニズムを明記すべきである。	御意見として承ります。なお、本ガイドラインでは、深刻化するサイバー脅威に対し「セキュリティ対策に必要な資源（予算・人材等）について、組織の社会的責務を果たすため、また、組織の価値を維持・増大していく上で、組織活動におけるコストや損失を減らすためにも必要不可欠な投資であるとの考え方のもとで配分する。」ことを講ずべき対策事項に定めております。
69	重要インフラのセキュリティ対策基準の強化にあたっては、形骸化した多重下請け構造（いわゆる中抜き）や、過度に海外の特定ITベンダー・セキュリティ製品への依存を招かないような仕組みを強く求める。 厳格な基準の義務化が、結果として国内の中小・現場企業への適切な予算配分を阻み、中間マージンによるコスト肥大化を招くことや、国内に資金やノウハウが蓄積されず外資へ富が流出することは、経済安全保障上の観点からも重大な懸念である。 したがって、透明性の高い調達プロセスの確保と、国内の技術力・人材育成を直接支援する方針を明確に位置づけるべきである。	重要インフラ統一基準は、特定の国や企業の製品を排除するものではありませんが、サプライチェーン・リスク対策の重要性の観点において、本ガイドライン2.9では、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。
70	サイバーセキュリティ方針は社内規定として策定すべきか。	各分野・事業者によって様々考えられるため、まずは各分野の安全基準等を確認いただく必要がありますが、一般論としては、サイバーセキュリティ方針は社内規定として定めるほか、必要に応じてホームページ等で公開することも考えられます。

71	2026年度末にサプライチェーン強化に向けたセキュリティ対策評価制度（SCS評価制度）の運用が開始されるが、重要インフラシステムの調達時に事業者側発注要件として、重要インフラ統一基準や安全基準等策定ガイドライン等で★３や★４の取得を今後、必須化、推奨化する可能性はあるか。	SCS評価制度も含め、関連制度の活用方法等については引き続き検討してまいります。 なお、本ガイドラインにおける（解説）は、あくまでも参照のための補足であり、これによって対策事項に係る対応方法を詳細に定め、一律の対応を求めるものではございません（1.5）。
72	事業者が重要システムの調達や業務委託先の選定時に留意すべき条件として、懸念国の国名やベンダ名を米国のエンティティリストのような一覧で提示してもらえないか。製品・サービス調達にあたって、選定初期段階でリスクの高い製品やベンダーを即座に除外（または優先調査）できるため、事業者側の製品・サービス評価・選定期間を大幅に短縮できるとともに、重要インフラ事業者のリスク低減にもつながる。	重要インフラ統一基準は、特定の国や企業の製品を排除するものではありませんが、本ガイドラインの2.9では、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、その（解説）において代表的な制度及びガイドライン等を参照の上、必要な対策を講ずる点を補足しています。
73	国防に関わることなので、特に重要インフラは犯されないよう、外国人は関わらせない。罰則を厳しくする。	重要インフラ統一基準は、特定の国や企業の製品を排除するものではありませんが、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の観点において、本ガイドライン2.5.4では、重要インフラ事業者等における役職員の管理を求め、また、2.9では、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	「組織が設定したリスク許容度と対応策に応じた資源の配分となっているかを確認」するためのレビューは関連する情報を収集した上で行う必要があり、レビューを単独で行うことは適切とは言えない。「後述の監査と組み合わせて実施することが考えられる」等、考え方を解説内で説明すべきではないか。	本ガイドラインでは、2.5.2資源の確保・①-2 （解説）において、「レビューに係る体制については、内部・外部も含め、自組織に有効的と考えられる体制を選択し、実施することが考えられる」としているところ、情報の収集等のレビューに必要な体制についても検討されることを想定しております。なお、2.6①-1では、監査は、経営層の責任において実施することを明記しております。
75	2.5.2①-2（解説）で用いられる「有効的と考えられる」という表現は一般的な表現ではないので、「有効と考えられる」でよいのではないか。	御意見を踏まえ修正いたします。
76	p.38 2.9 サプライチェーンリスクマネジメントにおける「講ずべき対策事項」として「サプライチェーンの依存関係の把握」とあるが、それに相当する解説がないように思われる。解説として、どのような観点での依存関係を把握すべきかを具体的に記載すべき。（供給依存、技術依存、特定サービスへの依存など）	御意見を踏まえ、2.9①-1（解説）において、依存関係の把握を行うに当たっての観点について追記いたします。

	意見の概要	意見に対する考え方
	「3 識別」に係る意見	
77	3.6等の脆弱性管理規定において、防御側におけるAI技術や自動化（SOAR等）を活用した脅威検知・一次対応の自動化を推進する記述を追加してはどうか。	AIを活用したセキュリティ対策は重要であり、高性能AI活用の社会への浸透状況を踏まえた中長期的な対策であると認識しています。この点については、7①-3-1の（解説）に記載しております。
78	3.6③ではAIの悪用等に備えた「迅速なパッチ適用」が強調されている一方、4.4.1では「事前承認」や「事前テスト」の実施が求められている。ミッションクリティカルなシステムではパッチの事前検証に時間を要するため、実務において両者の要件が衝突するリスクがあるところ、3.6③の「解説」に、対処優先順位及び一時的な緩和策に関する記述を追記できないか。	本ガイドラインでは、3.6③-1の（解説）において、迅速なパッチ適用等が困難な場合には、リスクに応じて、例えば、可能なパッチ適用頻度の設定や、3.6②-2の脆弱性悪用のリスクを低減する対策等を採用・文書化し実施することとしています。それらを踏まえつつ、パッチ適用に関する作業方針・内容を確立することとしています。
79	一定規模以上の重要インフラ事業者については、情報システム全体の定期的な脆弱性診断を必須とすべき。 本書にて、個別機器の脆弱性診断は必須項目として挙げられているものの、「情報システム全体」に関する定期的な脆弱性診断は「推奨項目」とされている。 攻撃者の脅威レベルが劇的に高まる現代において、情報システム全体の定期的な脆弱性診断は、重要インフラサービスを担保するためには、サイバーハイジーンの一つとして取り扱われるべき必須のセキュリティ対策となっている。	本ガイドラインでは、3.6②において、重要インフラ事業者等の運用するシステムの性質等も加味しつつ、定期的な脆弱性診断の実施及び、診断の実施が困難な場合における代替措置について定めております。
80	重要インフラ事業者等から政府へ共有する情報の最小化・匿名化、安全な提出経路、政府内での閲覧権限、利用目的、第三者提供、保存期間、削除方法及び漏えい時の責任を明確にすべき。また、善意により速やかに報告した事業者が、報告したこと自体を理由として不合理な不利益を受けない仕組みも必要である。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものですが、御意見の内容については、今後の情報共有の在り方の検討に当たって参考にさせていただきます。
81	概要ファイルの7ページに記載されている事業者と政府間での情報共有について、報告と共有の間にいくつもの部署を通じての連絡となる場合、情報伝達に差異が発生するリスク、また伝達の遅延リスクも考えられると思う。 伝達遅延と伝達の差異に対する防止策などは具体的にあるか。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものですが、御意見の内容については、今後の情報共有の在り方の検討に当たって参考にさせていただきます。
82	脆弱性への対応策として、迅速なパッチ適用が困難な場合の代替措置の例に、「IPS（侵入防止システム）等を活用し、ネットワークレベルで脆弱性を突く通信を検知・遮断する仕組み（仮想パッチ / Virtual Patching）」を明記することを要望する。	本ガイドライン3.6②-2（解説）の「対象となる情報機器と重要システム等を構成するネットワークとの通信を監視し、当該脆弱性を悪用する不正な通信を遮断する機器又はソフトウェアを導入する」には、仮想パッチの適用も含まれることを想定しているところ、明確化の観点から、その旨を（解説）に追記いたします。
83	当社は、本ガイドラインにおいて以下を明示的に確認することを提言する。 •OTの管理策は、安全性を考慮したリスク評価を通じて選定すべきであること •変更は導入前にテストすべきであること •直接的な実施が重大な運用リスクを生じさせる場合には、代替的管理策を認めること •ネットワークセグメンテーション、安全なリモートアクセス、監視および資産の可視性が、代替的なリスク低減策となり得ること •分野別基準は、サイバーセキュリティと運用工学の双方の専門知識を踏まえて策定すべきであること	本ガイドラインでは、制御システムへの適用が容易ではない場合が想定される対策については、当該対策の（解説）等に、代替手段等を記載しております。例えば、3.6③-1（解説）において、パッチ適用等が不可能又はパッチ適用等によって可用性や安全性を損なうおそれのある制御システムについては、ネットワークの物理的又は論理的分離等を実施することとしています。 また、各対策事項は、原則として制御システムにも適用されることを想定しております（1.3）。
84	3.6②-1（解説）について、昨今のセキュリティ情勢を踏まえ「クラウドサービス」も含めるべきではないか。	御意見を踏まえ、3.6②-1（解説）に、クラウドサービスにより構築されるシステムも含まれ得る点を追記いたします。

85	3.6②-3において、対策事項にペネトレーションテストが挙げられているが、ペネトレーションテストは実施対象となる機器やシステムの種別、稼働状況によってテストで確認する観点やテスト実施時の注意点が異なると思われる。代表例としてWebシステム、ネットワーク機器、ActiveDirectory環境などに対するペネトレーションテストを実施する際の観点や注意点などの解説を追加いただけないか。	御意見として承ります。各対策事項について具体的に求められる内容は、分野や対象のシステム等により異なり得るところ、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
86	3.6③-1（解説）について、対策事項がパッチ適用のみに終始しているので「防御側もAIを活用して短期間で脆弱性を洗い出すサイクルを生み出す」などを含めてはどうか。	本ガイドラインでは、7①-3-1(解説)で、中長期的な対策として、高性能AI活用の社会への浸透状況を踏まえながら、高性能AIを活用したサイバーセキュリティ対策の強化（例：脅威検知・インシデント対応・脆弱性発見等）を含め、基本的な対策の更なる徹底を推奨しています。
87	3.1.1①-1（解説）における5番目の項目（ASM）および6番目の項目（SBOM）について、参照先は記載されているが、対策事項として何を実施すべきかが不明確と考える。これらの導入を検討することを求めているとの理解でよいか。	本ガイドラインにおける（解説）は、あくまでも対策に当たって参照するための補足事項であり、これによって対策事項に係る対応方法を詳細に定め、一律の対応を求めるものではございません（1.5）。
88	3.4①-1（解説）における3番目の項目で資産ベースおよび事業被害ベースのリスク分析について言及されているが、サプライチェーンや設計開発プロセスに対するリスク分析の必要性についても記載すべき。	本ガイドラインでは、御指摘の点について、2.9②-1及び2.9②-4等で定めております。
89	3.6③-1について、「情報システム」には、制御システムも含まれるとの理解でよいか。 その場合、「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」と記載されているが、制御システムにおいてパッチ適用が困難な場合は、機器の更改（リプレイス）を実施すべきという解釈になるのか。 制御システムでは、運用上の制約からパッチ適用が困難な場合があり、またリプレイスについても経済合理性の観点から容易ではないケースがある。そのため、ネットワーク分離やアクセス制御の強化等の代替的なリスク低減策を講じる場合もあると考える。このような対応も認められるのか明確化していただきたい。	本ガイドラインにおける「情報システム」には、「制御システム」が含まれます（1.3）。 各対策事項について具体的に求められる内容は、分野や対象のシステム等により異なり得ると想定しております。 本ガイドラインでは、3.6③-1（解説）に、パッチ適用等が不可能又はパッチ適用等によって可用性や安全性を損なうおそれのある制御システムについては、ネットワークの物理的又は論理的分離等の代替手段を使用することを記載しております。
90	3.6③「攻撃者にAIが悪用されることにより…」について、AIに関する脅威には、重要な第3のカテゴリーが存在する。それは、AIエージェントの誤動作に起因する予期せぬ有害な挙動であり、敵対的攻撃とは異なる重大な脅威となる。この脅威に対する最善の防御策は、エージェントをサンドボックス内で動作させることである。	本ガイドラインでは、AIの悪用リスクに備えた対策については7①-3-1で記載しています。また、AIシステム・サービス利用時の対策については、7①-2-1で、例えば不正操作によってAIの振る舞いに意図せぬ変更又は停止が生じることのないよう、AIの機密性・完全性・可用性を維持し、その時点での技術水準に照らして合理的な対策を実施することを求めています。
91	3.1.1③について、「ネットワーク境界構成図、データの流れ図等を作成・維持管理する。」とあるが、産業用プロトコルでの通信を把握する目的とすれば制御システムを構成する機器についてはすべて網羅したものを作成する必要があるか。また、同じシステムでも設置場所により構成が変わる場合もすべて図を作成する必要があるか。	3.1.1③のネットワーク構成図については、資産のネットワーク接続関係や配置場所を整理することを通じて、例えば、リスクアセスメントやインシデント発生時の影響評価等に用いることが考えられます。 図面に必要な情報やその粒度等は、その用途や事業者等個別の事情により異なり得るところ、一般論としては、物理的な機器を全て網羅する必要はなく、大まかな論理構成を示すことで足りる場合も想定されます。

	意見の概要	意見に対する考え方
	「4 防御」に係る意見	
92	AI技術の進展は、重要インフラのサイバーセキュリティに大きな影響を与えている。本ガイドラインでは、AIを単に新たな技術動向として扱うのではなく、重要インフラにおけるリスク管理対象として体系的に位置付けるべき。 AI関連リスクは、少なくとも以下の3類型に分けて整理すべき。 ・攻撃者がAIを利用するリスク ・防御側がAIを利用する場合のリスク ・AIを含む重要システムそのもののリスク AIを悪用した攻撃を前提として、以下の対策を明記すべき。 ・ フィッシング耐性の高い認証方式 ・ 多要素認証の強化 ・ メール・メッセージの真正性確認 ・ 異常ログイン検知 ・ 振る舞い検知 ・ 脆弱性管理の迅速化 ・ 攻撃シナリオの継続的更新 ・ 生成AIを用いた模擬攻撃・訓練への対応 ・ 職員・委託先へのAI悪用型攻撃に関する教育 防御目的でAIを利用する場合、以下の統制を含めるべき。 ・ AI利用目的の明確化 ・ 入力データの範囲管理 ・ 機密情報・個人情報の取扱い管理 ・ 誤検知・過検知・見逃しの評価 ・ 自動遮断・自動復旧等における人間の関与 ・ モデル更新時の影響評価 ・ 判断根拠又は説明可能性の確保 ・ ログ保存 ・ 外部AIサービス利用時の契約・保存・再学習条件確認 ・ ベンダーロックイン及びサービス停止リスクへの備え AIシステムを構成する以下の要素を資産管理・リスク評価の対象として明記すべき。 ・ モデル ・ 学習データ ・ 評価データ ・ プロンプト ・ システムプロンプト ・ RAG用データ ・ ベクトルデータベース ・ 推論API ・ 外部ツール連携 ・ エージェント実行環境 ・ モデル供給元 ・ データ供給元 ・ ログ及びフィードバックデータ AIシステム特有のリスクとして、以下を管理対象に含めるべき。 ・ プロンプトインジェクション ・ データ汚染 ・ モデル改ざん ・ 学習データ漏えい ・ 推論APIの不正利用 ・ 機密情報の出力 ・ 外部ツールの不正実行 ・ RAG経由の誤情報混入 ・ AIエージェントによる過剰権限行使 ・ モデル供給元・API供給元の停止又は仕様変更	本基本的な対策の徹底の重要性とAIのセキュリティ対策に係る御意見と認識しました。御意見の中で記載いただいている主な対策については、基本的な対策として「4 防御」を中心に記載しております。また、AIのセキュリティ対策については、本ガイドラインでは、7①-2においてAIシステム・サービス利用時の対策、①-3において高性能AIの悪用リスクに備えた対策について規定するとともに、（解説）において、参考となるより具体的な事項について記載しておりますが、今後も、社会における動向等を踏まえながら、必要に応じて本ガイドラインを更新してまいります。

93	本ガイドラインには、重要システム及びその構成要素の新規開発・大規模改修において、Rust等のメモリ安全性を備えたプログラミング言語、型安全な設計、静的解析、ファジング、形式手法、サンドボックス化、権限分離等を優先的に採用する旨を明記すべき。 特に、外部入力を処理する部分、ネットワーク境界に近い部分、認証・認可・暗号・ログ処理・ファイル解析・プロトコル処理・制御命令変換等の高リスク領域については、メモリ安全性を明示的な評価項目とすべき。	御意見として承ります。本ガイドラインでは、2.9②-4において、サイバーセキュリティに配慮した開発等の方針の遵守状況を委託先に対して定期的に、又はリスクに応じて適宜確認すること、また、4.4.3において、情報システムの取得・開発・保守に関する対策を記載しております。御指摘の点については、上記観点における詳細な対策事項と認識しておりますところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
94	本案4.7では、クラウドサービスの認証、アクセス制御、暗号化、鍵管理、バックアップ、ログ管理等の確認を求めているが、重要インフラに関するデータについては、技術的な安全性だけでなく、データがどの国・地域に保存されるのか、どの国の法令・司法権の影響を受けるのか、国外から管理者権限によるアクセスが可能なのかといった問題も重要である。 したがって、重要度の高いシステムにクラウドサービスを利用する場合には、少なくとも、データの保存場所、準拠法・裁判管轄、国外からの管理者アクセスの有無、再委託先、データの国外移転、暗号鍵の管理主体について確認することを明記すべき。 特に国家機能や国民生活への影響が極めて大きい情報については、国内保管を含め、我が国が実効的な管理権限を確保できる仕組みを検討することを求める。	本ガイドラインでは、4.3.1や4.3.2において、システムのリスクアセスメントに応じてデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行うこと、クラウドサービス等利用時には、国内外の法令等の存在に留意すること、暗号鍵の利用方針や管理方針を策定すること等を規定するとともに、（解説）において、参考となるより具体的な事項について記載しております。
95	通信の監視やログの取得・分析については、憲法に定める通信の秘密を侵害するおそれがないよう、明確な歯止めを設けるべき。 また、監視が過度に行われれば、政府への批判や政治的意見の表明など、表現の自由を萎縮させるおそれがある。さらに、合法的で健全なデモ・集会・市民活動が監視や記録の対象となり、その活動を妨げることがあってはならない。 そのため、以下をガイドラインに明記することを求める。 ・通信・ログ情報の利用目的をサイバーセキュリティ対策に限定すること。 ・必要性・相当性・最小限性の原則に基づき、不必要な通信情報や個人情報を取得・保存しないこと。 ・取得した情報を、政治活動、政府への批判、表現活動、合法的なデモ・集会等の監視や評価に利用しないこと。 ・保存期間、第三者提供及び目的外利用について明確な制限を設けること。 ・通信監視やログ取得について、独立性のある第三者による監査・検証を可能とすること。 サイバーセキュリティの強化を理由として、通信の秘密、表現の自由、健全なデモ・市民活動が不当に制限されることのないよう、明確な権利保障と歯止めをガイドラインに盛り込むことを求める。	重要インフラ統一基準及び本ガイドラインは、深刻化の進む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ことを目的として、例えばセキュリティの確保に必要なログの記録・管理等を含め、各分野の安全基準等において、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したものとなります。
96	安全基準等の策定に当たっては、Rust等のメモリ安全性を備えた言語の採用、既存C/C++資産に対するサンドボックス化、ファジング、静的解析、動的解析、形式検証、未定義動作検出、セキュアコーディング基準の適用を明示すべきである。直ちに全システムの置換を求めるのではなく、新規開発、外部入力を処理する部分、権限境界、暗号・認証・通信部分、長期運用される重要コンポーネントから優先的にメモリ安全化を進める段階的方針を示すべきである。	本ガイドラインでは、4.4.3②-2において、情報システムの取得・開発・保守時におけるサイバーセキュリティを確保するための手順・環境等の整備を求めており、（解説）において、セキュアコーディングに係る基準、セキュリティ技術・アーキテクチャに係る設計標準等の手順・環境等の整備について補足しています。
97	安全基準には、OSSの棚卸し、ライセンス確認、脆弱性管理、保守状況確認、重要OSSへの支援、フォーク又は代替可能性、国内ミラー、署名付きパッケージ、再現可能ビルド、長期保守体制を含めるべきである。特に、暗号ライブラリ、OS、コンパイラ、ランタイム、ネットワークスタック、認証基盤、データベース等については、国家的な重要依存関係として扱い、公共部門と民間が連携して保守・検証・人材育成を進めるべきである。	御意見として承ります。本ガイドラインでは、4.4.2①-2にて、OSSを含む情報システムで利用するハードウェア・ソフトウェアについて、セキュリティを保って管理するための手順を策定することを求めており、（解説）において、対策実施に当たってのより詳細な情報について補足しておりますところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。

98	暗号化された情報についても、正規利用時には復号可能であり、認証情報や権限等が攻撃者に取得された場合には、データへ到達されるリスクを考慮する必要がある。 4.3「データのセキュリティ対策」において、暗号化に加えて、 ・秘密分散等によるデータの分散・無意味化 ・単一の保管場所から完全な情報を取得できない構成 ・端末への重要データの非保持化 ・侵害された端末やストレージから取得されたデータ単体では復元・利用が困難となる構成 等についても、情報の重要度やシステムの特性に応じて検討する技術的選択肢として例示すべき。	御意見として承ります。暗号化以外も含むデータのセキュリティ対策については、本ガイドライン4.3.1①-1において、リスクアセスメントに基づくデータの管理方針策定、①-2においてリスクアセスメントに応じたデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理の実施を求めております。御指摘の点については、上記観点における詳細な対策事項と認識しておりますところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
99	4.2「意識向上とトレーニング」だけではなく、4.3「データのセキュリティ対策」等においても、「利用者の注意・判断・手作業への依存を可能な限り低減する」というHuman-Centered Cybersecurityの観点を取り入れるべき。	御意見として承ります。御意見の内容については、引き続き諸外国の動向等を把握しつつ、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
100	4.3.3では、バックアップデータをバックアップ元とは異なるセグメントやオフラインで保管すること等が示されており、これはランサムウェア等によるデータ破壊からの復旧に非常に重要な対策である。 一方、近年のランサムウェアでは、データを暗号化・破壊するだけでなく、情報を窃取した上で公開等を示唆することによって圧力をかける手法も想定する必要がある。 バックアップは「データを失わない」という可用性の確保には極めて有効だが、既に窃取された機密情報の悪用・公開を防ぐものではないため、「破壊されても復旧できる」という対策と、「窃取されても利用可能な情報として取得されにくい」という対策を組み合わせることが、重要インフラのレジリエンス向上に有効と考える。	本ガイドラインでは、「窃取されても利用可能な情報として取得されにくい」という対策として、例えば、4.3.2①に示すデータの暗号化を求めております。
101	本案89ページの「重要システムについて、年1回以上の定期的なバックアップ」という基準は、重要インフラのデータ保護基準としては不十分。システムイメージのバックアップと、日々更新される業務データのバックアップとを明確に区別すべき。 データや業務の重要度に応じて、許容できるデータ損失時間（RPO）及び復旧目標時間（RTO）を設定し、複数世代・複数拠点での保存、オフライン又は改ざん不能なバックアップ、定期的な復旧テストを求めるべき。バックアップリカバリー検査についても、単に「実施を検討する」のではなく、重要システムでは定期的に実施することを原則とすべき。	御意見を踏まえ、本ガイドライン4.3.3①-1に、「年１回以上」は、分野・事業者横断的に重要システム全般を対象とした最低限の頻度の趣旨であること、また、バックアップ対象データの特性の考慮について追記いたします。 また、御意見を踏まえ、本ガイドライン4.3.3①-2（解説）に、イミュータブルバックアップや、異なる媒体や環境での保存について追記いたします。 その他の御意見については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
102	国民生活や国家安全保障に関わる重要なデータについては、保存国・地域、運用管理者の所在国、事業者の実質的支配者、適用される外国法、外国政府によるアクセスの可能性、暗号鍵の管理主体等を確認することを必須とすべき。 特に重要度の高いデータについては、原則として国内で保存し、重要インフラ事業者側が管理する暗号鍵で保護することを基本とすべき。国外保存を認める場合は、リスク評価、経営層の承認、国内バックアップ及び緊急時の国内代替手段を求めるべき。 特定の外国クラウド事業者への過度な集中やベンダーロックインを避けるため、データ移行可能性、契約終了時のデータ返還、サービス停止時の代替手段を選定基準に含めること。	本ガイドラインでは、4.3.1①において、リスクアセスメントに応じたデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行う点を、また、4.3.1②において、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、国内外の法令や評価制度等の存在について留意する点を講ずべき対策事項として求めております。御指摘の点については、これらの観点における詳細な対策事項と認識しております。
103	日本の重要インフラ事業者が、対象事業者として指定され、資産届出、インシデント報告、監査対応等を求められる一方、日本の重要インフラにクラウド、ソフトウェア、通信機器その他の重要な製品・サービスを提供する外国事業者には、直接的な義務が十分に及ばない可能性がある。 日本側の事業者にだけ行政対応費用と事故責任を負わせるのではなく、重要な外国の供給者に対しても、国内責任者又は国内窓口の設置、インシデント報告、脆弱性情報の提供、ログ及び証拠の保全、監査への協力、サービス終了時のデータ返還等を求めるべき。	本ガイドラインでは、2.9において、サプライチェーン・リスクマネジメント、4.7において、クラウドサービス利用時の対策を求めております。また、4.3.1①において、リスクアセスメントに応じたデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行う点、4.3.1②において、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、国内外の法令や評価制度等の存在について留意する点を講ずべき対策事項として求めております。御指摘の点については、これらの観点における詳細な対策事項と認識しております。

104	本案にはDNSに関連する明示的な要件は十分に示されていない。特に、NISTが2026年3月に公表した最終版「SP 800-81 Rev. 3 Secure Domain Name System (DNS) Deployment Guide」（以下「SP 800-81r3」）及び、2026年5月26日にNISTのOLIRカタログにFinalとして掲載された「SP 800-81-r3-to-Cybersecurity-Framework-v2.0」の内容を、本案及び本案を参照して策定される安全基準等に反映すべき。	御意見として承ります。本ガイドラインでは、例えば4.4.2①で、情報システムで利用するハードウェア・ソフトウェアの個々の設定について把握・理解し、安全性の確保に努めるほか、セキュリティを保って管理するための手順を策定することとしています。御意見は、その観点での詳細な対策事項と認識しているところ、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
105	本案4.4.4（1）-4は、EDR及びNDRの導入及び運用を定めている。これらについて、5.1「監視・分析体制の整備」においても、検知の体制を構成する手段として言及すべき。	御意見として承ります。EDR及びNDRの導入・運用は、検知体制を構成するための多岐にわたる手段の１つとして考えられますところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
106	「重要システムについて、年1回以上の定期的なバックアップを実施する。」という記述について、ITシステムと制御システムとを書き分けるべきである。その上で、ITシステムについては、目標復旧時点（RPO）に基づいて取得の間隔を設定すべき旨を明記すべきである。	御意見を踏まえ、本ガイドライン4.3.3①-1について、「年１回以上」は、分野・事業者横断的に重要システム全般を対象とした最低限の頻度の趣旨であること、また、バックアップ対象データの特性の考慮について追記いたします。
107	「マルチエンジン型のマルウェア検知ソフトの利用」という表現を改めるべきである。複数の検知エンジンの併用に限定されない、検知手法の多層化を示す表現とすべきである。	御意見を踏まえ、本ガイドライン4.4.4①-2について、マルチエンジン型のマルウェア検知ソフトに限定されない表現に修正いたします。
108	従来のワクチン型対策から脱却し、身元の不明な端末からのアクセスを完全に遮断するゼロトラスト認証の義務化、およびAIを活用した異常行動検知（EDR/XDR）の導入推奨をガイドラインに盛り込み、攻撃を利用者の負担なしにシステム手前でシャットアウトする仕組みを評価基準に加えるべき。	認証については4.1.2、EDRの導入等については4.4.4に対策事項を設けているところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
109	政府の『骨太方針2026』に示されたオンチェーン推進の動きと連動し、過去データの改ざんや消去が構造上100%不可能な「国産ブロックチェーン（ProgmatやAstar等）」をインフラのログ保存やバックアップ基盤に採用することを推奨し、数時間での超高速復旧を可能にする強靭なレジリエンス（回復力）を確保することを要望する。	4.3.3のとおり、バックアップデータは、バックアップ元のシステムと異なるセグメントやオフラインで保管する等、切り離して補完し、データの重要度に応じて保存方法、保存期間、世代管理の方法を定めることとしております。御意見は、その観点での詳細な対策事項と認識しているところ、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
110	バックアップデータを切り離して保管する手法の例として、「ネットワークからの物理的または論理的な隔離」に加え、「管理者権限が奪取された場合であっても、データの変更・削除が論理的に不可能な仕組み（イミュータブルバックアップ／イミュータブルストレージ）の活用」を追記することを要望する。	御意見を踏まえ、本ガイドライン4.3.3①-2（解説）に、イミュータブルバックアップや、異なる媒体や環境での保存について追記いたします。
111	「被害が発生した際の攻撃の拡散に備えた対策として、ネットワークのセグメンテーション（重要インフラの分離）を行う」という項目について、「講ずることが望ましい対策事項」から「講ずべき対策事項」へ移動させることを要望する。あわせて、ネットワークレベルの大枠の分離にとどまらず、「システムやワークロード単位での論理的な分離（マイクロセグメンテーション）を実施する」旨の追記を提案する。	攻撃の被害抑制のためにマイクロセグメンテーションは重要な対策と認識していますが、ネットワークの細分化は、コスト・人材・専門知識等の観点から、必ずしもすべての事業者にとって導入が容易とは言い難く、講ずることが望ましい対策事項としております。

112	4.6.1①-7を「講ずることが望ましい対策事項」から「講ずべき対策事項」へ移動させることを要望する。また、記載内容について「ワークロード単位でのきめ細かい通信制御（マイクロセグメンテーション）の実装等により、ネットワークセグメントを細分化し、マルウェアの水平移動（ラテラルムーブメント）を阻止すること」といった具体的な修正を提案する。	攻撃の被害抑制のためにマイクロセグメンテーションは重要な対策と認識していますが、ネットワークの細分化は、コスト・人材・専門知識等の観点から、必ずしもすべての事業者にとって導入が容易とは言い難く、講ずることが望ましい対策事項としております。
113	現在の記載（1-2等）には、「オフラインでの保管」や「バックアップリカバリー検査」に該当する要素は盛り込まれているが、「複数の異なるメディア（媒体）への保存」や「遠隔地（オフサイト）での保管」、さらにランサムウェア対策として近年重要視されている「イミュータブル（不変・書き換え不可）なストレージ等での保管」といった要素も指針に含めてはどうか。	御意見を踏まえ、本ガイドライン4.3.3①-2（解説）に、イミュータブルバックアップや、異なる媒体や環境での保存について追記いたします。
114	人間に紐づくアカウントに加えて、「ノンヒューマンID（サービスアカウント、APIキー、RPA・Bot用ID等）」の対策事項についても指針に含めてはどうか。	御意見として承ります。4.1.1アカウント管理における詳細な対策事項と認識しておりますところ、御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
115	4.7 クラウドサービス利用時の対策において、ガバメントクラウド利用時の責任共有モデル、自治体とベンダー間の責任分界、標準化システム利用時の設定管理責任についても参考例を追加していただきたい。	御意見として承ります。各対策事項について具体的に求められる内容は、分野や対象のシステム等により異なり得るところ、今後の各分野における安全基準等の検討とあわせて、本ガイドラインや関連資料における参考例の提示等、検討を進めてまいります。
116	重要インフラ分野における人材不足が深刻化している現状を踏まえると、セキュリティ監査、リスクアセスメント、CSIRT運営支援、演習・訓練支援、インシデント対応助言などにおいて、登録セキスペの外部専門家活用をより積極的に記載することが望ましい。	御意見として承ります。本ガイドライン4.2.1①（解説）において、情報処理安全確保支援士資格の活用についても記載しておりますが、具体的に求められる内容は、各分野の特性や実情等を踏まえ、各分野において検討されるべきものと認識しております。
117	当社は、分野別基準において以下を実施することを提言する。 •個別のテクノロジーではなく、セキュリティ上の成果を定めること •同等の管理策を認めること •クラウドネイティブおよびゼロトラスト・アーキテクチャに対応すること •テクノロジーの進化に応じた最新化を認めること •将来的に陳腐化する可能性のある管理策へ事業者を固定化しないこと	本ガイドラインでは、2.9③-1で、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選定基準の整備や要求事項の整理を行うことを講ずべき対策事項としています。
118	重要インフラのサイバーセキュリティを強化する必要性は理解するが、その目的があることと、人に関する情報を集め、長期間保存し、政府機関へ共有することが許されるかは別問題である。 取得目的、対象者、取得項目を必要最小限に限定し、人事評価、労務管理、思想・信条の推知等への目的外利用を禁止すべき。保存期間は情報の種類ごとに上限を定め、不要な情報は速やかに削除すべき。政府機関等への提供は、具体的な法的根拠と必要性、提供先、対象情報、利用目的、保存期間、再利用・再提供、廃棄方法を明らかにし、記録を残すべき。個人を識別する必要がなければ仮名化・匿名化し、アクセスを必要最小限に制限すべき。その保護を自己点検だけで済ませず、独立性のある監査を行い、不利益な利用をする場合は本人への説明、訂正及び異議申立ての機会を保障すべき。	重要インフラ統一基準及び本ガイドラインは、深刻化の進む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ことを目的として、例えばセキュリティの確保に必要なログの記録・管理等を含め、各分野の安全基準等において、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したものとなります。
119	4.1.1①-4における「離職等によりアカウント管理が不要になった場合」との記述は、正しくは「離職等によりアカウントが不要になった場合」ではないか。	御意見を踏まえ修正いたします。

120	バックアップの頻度について、年１回は一般的な情報システムではかなり少ないという印象だが、重要インフラのシステムに特有の事情等があるのか。	御意見を踏まえ、本ガイドライン4.3.3①-1について、「年１回以上」は、分野・事業者横断的に重要システム全般を対象とした最低限の頻度の趣旨であること、また、バックアップ対象データの特性の考慮について追記いたします。
121	4.4.3①-1ではセキュリティ・バイ・デザインについて触れられているが、リスクアセスメントの観点からも言及すべき。 これに関連して、サプライチェーンや設計開発プロセスのリスク分析に有効な手法について、参考となる文献やガイドラインを記載していただきたい。	本ガイドラインでは、御指摘の点について、4.4.3①-1（解説）において参考となる文献やガイドラインとともに記載しております。
122	4.1.2①-4の記載において、「デフォルトパスワード」と「デフォルト認証情報」が使い分けられているが、これは意図的なものであるとの理解でよいか。	御意見を踏まえ、4.1.2認証・アクセス制御・①-4記載の「デフォルト認証情報」は、「デフォルトパスワード」に修正いたします。

	意見の概要	意見に対する考え方
	「5 検知」に係る意見	
123	一定規模以上の重要インフラ事業者については、脅威ハンティングの実施を必須することを検討すべき。 本書では、Living off the Land戦術（システム内寄生戦術）に対する対策に関する言及があるが、Living off the Land戦術は、脅威ハンティングを実施しないと検出することが極めて難しい。 当戦術の被害事例が増加している状況から、必須の取組み事項として検討すべき。 なお、7/31に決定した「脅威ハンティングの普及促進・実施等に係る基本方針」のもと、政府においては重要インフラ事業者に対して脅威ハンティング活動を強力に支援していくことが期待される。	御意見として承ります。政府としては、「脅威ハンティングの普及促進・実施等に係る基本方針」（令和８年７月31日 サイバーセキュリティ戦略本部決定）を策定したところです。他方、重要インフラ統一基準（第３部）及び本ガイドラインは、各分野の安全基準等において、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について記載しているものです。脅威ハンティングに関する取組の状況を踏まえつつ、今後、重要インフラ統一基準及び本ガイドラインにおける記載を検討してまいります。
124	「5.3 事象の分析」の講ずることが望ましい対策事項（1）-2を、講ずべき対策事項に位置付けるべき。同項の内容は、SIEM等のツールを活用し、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分析を可能な限り自動化することである。	御意見として承ります。5.3①-2におけるSIEM等ツールの活用を通じた事象分析の自動化は、セキュリティ管理体制の高度化にあたり重要な施策と認識しておりますが、コスト・人材・専門知識等の観点から、必ずしもすべての事業者にとっては導入が容易ではないと考えられる対策であると考えられることから、「講ずることが望ましい対策事項」のままとしております。御意見の内容については、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。
125	外部委託により早期検知の体制を整備する場合、委託先の「対策の具体的な内容」の把握が求められている。この把握すべき内容について、解説において確認項目を例示すべきである。例として、次の5点が考えられる。 （ア）監視の対象範囲（対象とする資産、ログの種類及び取得の範囲） （イ）検知の手法及び検知できない事象の範囲 （ウ）検知から委託元への通知までの目標時間 （エ）委託元へのエスカレーションの基準 （オ）分析を担当する要員の体制及び対応の時間帯	御意見を踏まえ、5.1①-2における「委託先で実施している対策の具体的な内容」に関して把握すべき内容について、解説において参考となり得る情報を追記いたします。
126	監視を実施する対象の例（ネットワーク及びネットワークサービス）に、外部との境界における通信（North-Southトラフィック）だけでなく、「内部ネットワークにおけるシステム間通信（East-Westトラフィック）の振る舞いの可視化と監視」を明記することを提案する。	本ガイドライン5.2①-2（解説）では、継続的な監視を実施することが想定される対象を例示しているところ、御指摘の観点を含めて考えることができるものと考えております。

	意見の概要	意見に対する考え方
	「6 対応及び復旧」に係る意見	
127	重要インフラサービスにおける実際の現場では判断に躊躇が生じ、初動遅れにつながるリスクがあることから、6.2.4①-1の「解説」において、事業継続計画（BCP）やコンティンジェンシープランの策定時に、システム停止に伴う社会的・業務的影響と攻撃拡散リスクを秤にかけるための『事前判断基準』をあらかじめ整理する点を示していただきたい。	本ガイドラインでは、6.1事業継続計画等において、事業継続計画等の策定を規定するとともに、6.1①-1の（解説）では、当該計画等の中で、重要インフラサービスを許容可能な時間内に許容可能な水準まで復旧させることを目的とし、復旧に向けた目標水準、優先順位、その他の方針、手順、態勢等を定める必要があることについて記載しております。また、事業継続計画等の策定に当たり、「【別紙】対処態勢整備に係るサイバー攻撃リスクの特性並びに対応及び対策の考慮事項」を参照することも考えられる旨記載しております。
128	本案では、インシデントについて関係法令等に基づく報告を行うとともに、基幹インフラ事業者についてはサイバー対処能力強化法に基づく報告義務にも留意するとされている。 重要インフラにおけるサイバー攻撃情報を迅速に政府等へ共有することは必要だが、所管省庁、警察、関係機関等への報告制度が複数存在する場合、同一のインシデントについて異なる様式で繰り返し報告することは、まさに復旧対応に人員を集中させるべき緊急時に事業者の負担となる可能性がある。 政府内で可能な限り報告様式及び窓口を統一し、一度提出された情報については関係行政機関間で共有するなど、重複報告を避ける仕組みを構築すべき。 また、「どの程度の事象を、いつまでに、どこへ報告するのか」を可能な限り明確化し、事業者が判断に迷わない制度とすることを求める。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものですが、御意見の内容については、今後の情報共有の在り方の検討に当たって参考にさせていただきます。
129	重要インフラ事業者には、サイバーセキュリティ基本法、サイバー対処能力強化法及び経済安全保障推進法等による複数の制度が適用される可能性がある。 同じ設備やインシデントについて、異なる省庁に対し、それぞれ異なる様式・期限で届出や報告を求めることは、緊急時の事業者に過大な負担を与え、初動対応や復旧を遅らせるおそれがある。 一つの窓口への報告によって関係省庁への報告を完了したものとみなすワンストップ制度を設けるべき。また、報告対象となる事象の定義、重大性の基準、報告期限及び様式を可能な限り統一し、一つの法制度に基づいて行った報告を他の制度でも有効な報告として取り扱うべき。 統一できない場合には、各制度の対象、報告先、期限及び法的効果を一覧化し、事業者が判断できる資料を公表すること。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものですが、御意見の内容については、今後の情報共有の在り方の検討に当たって参考にさせていただきます。
130	政府機関への情報共有には、システム構成図、IPアドレス、フォレンジック報告書、利用者属性、住民情報、患者情報、営業秘密等が含まれる可能性がある。 資料提出や情報共有を求める場合には、必要性及び法的根拠を記載した書面による要求を原則とし、提出情報を必要最小限に限定してください。また、受領した情報について適切な保護措置を講ずることを明記すべき。 善意により速やかに報告した事業者が、報告したこと自体を理由として不合理な不利益を受けない仕組みも必要である。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものですが、御意見の内容については、今後の情報共有の在り方の検討に当たって参考にさせていただきます。
131	「検知から30分以内にサイバー攻撃か否かを事業者内で判断する仕組みの構築」および「確定後15分以内に政府窓口へ即時報告（発生報・経過報・完報のメーリングリスト化を含む）」を明確なルールとして義務化することを強く求める。	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものですが、御意見の内容については、今後の情報共有の在り方の検討に当たって参考にさせていただきます。
132	6.2.4①-3を「講ずることが望ましい対策事項」から「講ずべき対策事項」へ移動させることを要望する。あわせて、「封じ込めの実施を判断する際の検討要素」の具体例として、『マイクロセグメンテーション等の論理的なアクセス制御技術を活用し、物理的なネットワーク遮断を行わずに、被害を受けた範囲のみを迅速に隔離・封じ込める手段の確立』といった要素を追記することを提案する。	攻撃の被害抑制のためにマイクロセグメンテーションは重要な対策と認識していますが、ネットワークの細分化は、コスト・人材・専門知識等の観点から、必ずしもすべての事業者にとって導入が容易とは言い難く、講ずることが望ましい対策事項としております。

133	当社は、政府に対して以下を提言する。 •報告対象インシデント、重大な影響およびサービス中断について共通の定義を設け、可能な限り他の法域における類似の定義と調和させること •分野横断的に報告様式および報告チャンネルを調和させること •同一の事象について複数の当局への報告が必要な場合、「一度報告する」仕組み、または一つの報告を複数の当局へ配信する共通プラットフォームを採用すること •初回通知後に検証済みの最新情報を提供する段階的報告を採用し、初回通知および検証済み通知に関する国際的な報告基準と整合させること •関係するサービスに影響する重大なインシデントであることを組織が合理的に確認した時点から、報告期限を起算すること •調査の進展に応じた情報の更新を認めること •政府に対する法令上の報告と、顧客に対する契約上の通知を明確に区別すること •顧客への通知を、当該顧客のサービス、システムまたはデータに重大な影響を及ぼすインシデントに限定すること •サプライヤーが合理的に管理できない状況について責任を負うべきではないことを認めること •機密情報、秘匿特権（弁護士・依頼者間秘匿特権等）の対象となる情報、個人情報およびセキュリティ上機微な情報を保護すること •顧客ごとに独自の取決めを求めるのではなく、共通の連絡・エスカレーション用テンプレートを策定すること	御意見として承ります。本ガイドラインは、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の詳細事項を記載するものですが、御意見の内容については、今後の情報共有の在り方の検討に当たって参考にさせていただきます。
134	6.2.3①-2（解説）において、業界全体のレジリエンス強化につなげるため、業界ISACでインシデント事例を共有することを解説で推奨してはどうか。	業界ISACを含めた情報共有組織の活用については、本ガイドライン3.3において定めております。
135	6.2.4①-1について、封じ込めについて記載があるが通信遮断、システム停止の判断は難しい。停止判断基準の明確化（トリガー）、権限（誰が止めるか）、最小限の遮断箇所の事前確認（どこまで止めるか）等、封じ込めについては詳細に事前に決めておくことが他にもあると思われるのでその点についても触れてもらいたい。	御意見として承ります。各対策事項について具体的に求められる内容は、分野や対象のシステム等により異なり得るところ、今後の本ガイドラインの見直しや各分野における安全基準等の検討に当たって参考にさせていただきます。

	意見の概要	意見に対する考え方
	「7 技術・脅威の動向等を踏まえた対策」に係る意見	
136	AIモデルやデータパイプライン自体の保護に関する指針を「7 技術・脅威の動向等を踏まえた対策」または「3.1 資産の管理」に追加してはどうか。	本ガイドラインでは、7①-2-1において、AIシステム・サービス利用時には、AIの機密性・完全性・可用性を維持し、その時点での技術水準に照らして合理的な対策を実施することを求めています。ご指摘の事項は、当該対策事項及びその（解説）に関連するものと考えております。
137	本案では、AIの脆弱性を完全に排除することはできないことを踏まえ、情報やシステムの重要度に応じて「人間の判断を介在させる程度についても検討する」とされているが、電力、通信、金融、交通、医療その他の重要インフラについて、サービス停止、安全制御、アクセス遮断等の重大な判断をAIのみで自動的に行わせることは、誤判断や外部からの不正操作が発生した場合に大きな被害につながるおそれがある。 そのため、国民の生命・身体、財産又は重要インフラサービスの継続に重大な影響を及ぼす判断については、単に「人間の判断を介在させる程度を検討する」にとどめず、原則として人間による確認、承認又は緊急時の介入・停止が可能な仕組みを確保することを明記すべき。 また、AIがどのような情報に基づいて判断したのかを事後的に検証できるよう、入力、出力、操作等の記録を保存することも必要である。	本ガイドラインの7①-2-1では、例えば不正操作によってAIの振る舞いに意図せぬ変更又は停止が生じることのないよう、AIの機密性・完全性・可用性を維持し、その時点での技術水準に照らして合理的な対策を実施することとし、（解説）において、「重要インフラサービスの安全かつ継続的な提供の観点から、関連する情報や情報システムの重要度に応じて、人間の判断を介在させる程度についても検討する」としているところ、重要度に応じて人間による確認、承認又は緊急時の介入・停止が可能な仕組みの確保についても検討されることも想定しております。
138	本案では、重要インフラ事業者についても原則2035年を目標としてPQCへの移行を検討するとされている一方、具体的な移行手順については、現在政府機関や各業界で検討中とされている。 重要インフラでは長期間利用されるシステムも多く、暗号方式の変更にはシステム更改、機器交換、委託先との調整等に長期間を要する可能性がある。 2035年という目標だけを示すのではなく、政府として、対象となるシステムの優先順位、調達段階で求める暗号方式、移行手順、既存システムへの対応、事業者への技術的・財政的支援等について、早期に具体的なロードマップを示すべき。	御意見として承ります。PQCへの移行の具体的な進め方（ステップ）については、現在、政府機関等や各業界分野において検討が進められているところ、重要インフラ分野・事業者横断的には、それら動向を確認しながら対応していくことを想定しております。
139	PQCへの移行において、一定規模以上の重要インフラ事業者についてはクリプトインベントリ作成・対応の優先順位付けのすみやかな実施を必須とすべき。 本内容は推奨項目として記載されているが、PQCへの移行のためには長い準備期間がかかるため、この第一段階となるクリプトインベントリ作成は喫緊の必須対応項目となる。 なお、当文書では米国において2035年を期限としたPQC移行計画との記載があるが、2026年6月22日の米国大統領令において、この期限が鍵交換：2030年末、デジタル署名：2031年末と大幅に繰り上げられている。	本ガイドラインでは、7①-4-2において、クリプト・インベントリの作成及び優先順位に応じた移行の進め方の検討を求めております。
140	「パッチ適用等が困難なシステムについては、例えば、中長期的なリプレイス（迅速な脆弱性対応が可能なクラウド環境への移行等も含む。）を視野に入れた対策を検討することも考えられる。」という記載について、『（迅速な脆弱性対応が可能なクラウド環境への移行等も含む。）』の部分を削除し、単に「中長期的なリプレイスを視野に入れた対策を検討する」といった表現に留めることを要望する。	本ガイドラインにおける（解説）は、特定のインフラ形態への移行を推奨するものではなく、あくまでも参照のための補足であり、これによって対策事項に係る対応方法を詳細に定め、一律の対応を求めるものではございません（1.5）。

141	外部AIサービス利用時のリスク対応策に加え、「機密性の高いデータや制御システムと連携するAI基盤においては、データ主権とガバナンスを自組織で完全に統制できるオンプレミス・プライベートクラウド型AI環境（Private AI）の構築・運用を有効な対策として推奨する」旨の追記を提案する。	本ガイドラインでは、4.3.1①において、リスクアセスメントに応じたデータの適切な保護や保管場所の考慮をはじめとした望ましいデータ管理を行う点を、また、4.3.1②において、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、国内外の法令や評価制度等の存在について留意する点を講ずべき対策事項として求めております。御指摘の点については、これらの観点における詳細な対策事項と認識しております。
142	当社は、AI関連の義務について以下を提言する。 •リスクベースかつ技術中立的なものとすること •AIがシステムおよびサービスのリスクに与える影響に焦点を当てること •日本の「AI事業者ガイドライン」および広く認められた国際基準と整合させること •基本的なサイバーセキュリティ義務との重複を避けること •AIが重要な意思決定に影響する場合には、人間による監督およびフェイルセーフ運用を認めること •テクノロジーの進化に応じて、柔軟なガイダンスを通じて更新すること	本ガイドラインでは、7①-2-1で、AIシステム・サービス利用時の対策に関して記載しているところ、御意見については、その（解説）に関連するものと認識しています。また、「4防御」等に記載する各セキュリティ対策を講じた上で、AIシステム・サービス利用をすることを想定しています。
143	当社は、暗号技術の棚卸し（暗号インベントリ）の整備、暗号アジリティ、および耐量子計算機暗号（PQC）への移行計画の策定を支持する。ただし、移行は国際的に調整され、以下を反映したものであるべき。 •標準の成熟度 •相互運用性 •製品の提供状況 •データの機微性および機密性を維持すべき期間 •システムの重要度 •運用上の制約 •導入済みインフラのライフサイクル	本ガイドラインでは、7①-4(解説)のとおり、重要インフラ事業者等のPQCでは移行については、政府機関等や各業界分野における検討の動向を確認しながら対応していくことを想定しています。御意見の内容については、今後の対応に当たって、参考にさせていただきます。
144	AI主導の敵対者に対抗するには、脆弱性を発見し、仮想パッチを作成し、数分以内に大規模に保護を展開し、攻撃が兵器化される前にブロックする、自動化されたAIネイティブのアプローチへと移行する必要があると考えるところ、既存のCVEや新しい未開示の脆弱性データ等を活用したプロアクティブな仮想パッチの適用は少なくとも「講ずることが望ましい対策事項」に位置付けられるべきと考える。	御意見を踏まえ、本ガイドライン7①-3-1（解説）において、制御システム等へのパッチ適用等が困難な場合は、例えば仮想パッチの適用等のリスク低減策の実施が求められる旨を追記いたします。

	意見の概要	意見に対する考え方
	その他（重要インフラ統一基準等）	
145	基準には定期見直しの周期、重大インシデント後の臨時見直し、外部専門家・事業者・利用者・研究者からの意見聴取、改定履歴の公開、適用除外の理由公開を定めるべきである。また、評価については、自己点検に偏らず、第三者監査、レッドチーム演習、ペネトレーションテスト、机上演習、サプライチェーン監査、委託先監査を組み合わせるべきである。評価結果の全部を公開できない場合でも、分野別の成熟度、主な改善事項、重大リスク、改善期限等は、国民に説明可能な形で公表すべきである。国民生活に不可欠なサービスの安全性は、単なる企業秘密や行政内部資料として閉じるべきではない。	重要インフラ統一基準に定める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。重要インフラ統一基準及び本ガイドラインでは、定期的な脆弱性診断（3.6②）、演習・訓練への参加の推進（4.2.1①-5）等を盛り込んでいるほか、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、その実現に向けて効果的な「把握・分析」「評価・改善」の仕組みを構築してまいります。
146	国が定期的に事業者の対策状況を監査・実地確認するような、強制力のある厳格なチェック体制をガイドライン内に明記すべき。	重要インフラのサイバーセキュリティ対策の推進に当たっては、まずは重要インフラ事業者等による自主的・積極的な取り組みが重要であるところ、政府としても、それら取組を促進するとともに、重要インフラ統一基準を通じた政府機関における施策の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強化の実効性を確保してまいります。
147	今回の意見公募では、「安全基準等策定ガイドライン（案）」だけが対象とされ、その前提となる重要インフラ統一基準及びその概要は参考資料として意見募集対象外とされている。 しかし、重要インフラ統一基準の概要には、対象となる分野・事業者の特定、政府機関による調査・評価、複数法制度の関係など、ガイドラインの内容を左右する重要事項が含まれている。統一基準が2026年7月31日に既に決定され、その後に詳細部分だけについて意見を募集する手続では、国民が制度の根幹について意見を述べる機会が十分とはいえない。 今後、重要インフラ統一基準を改定する際には、原則としてパブリックコメントを実施していただきたい。また、今回のガイドライン案に対して提出された意見が統一基準の内容にも関係する場合には、単に「意見募集対象外」として扱わず、統一基準の見直しに反映又は引き継ぐ仕組みを設けるべき。	重要インフラ統一基準の策定に当たっては、令和８年（2026年）４月21日～５月17日の期間で意見募集を行っており、80者から164件の御意見を頂戴しております。また、サイバーセキュリティ推進専門家会議、重要インフラサイバーセキュリティ研究会といった会議の有識者からも御意見を頂戴した上で策定しています。詳細はNCOホームページをご覧ください。
148	参考資料5ページでは、具体的な重要インフラ事業者をバイネームで特定する必要があるとされている。一方、10ページでは、実施計画において対象事業者等を特定するとされている。 どの文書によって正式な指定が行われるのか、指定基準、指定前の通知、事業者が事情を説明する機会、指定に対する異議申立て、指定解除及び定期的な見直しの手続が明らかではない。 指定の客観的基準、判断主体、指定手続、見直し時期及び不服申立手続を明文化すべき。個別事業者名を公表すると攻撃リスクが高まる場合には非公表とすることも考えられるが、少なくとも指定基準と手続は公表すべき。 また、医療機関等について、単に規模が小さいことだけを理由として対象外にするのではなく、地域での代替可能性、他の医療機関との接続状況、保有する情報の重要性、地方における役割等を踏まえて判断すべき。	重要インフラ統一基準2.1.1において、「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」するとしているところ、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。
149	参考資料では、重要インフラ統一基準は2026年10月施行予定である一方、各省庁の実施計画は2027年夏を目途に策定するとされている。 実施計画が策定されるまでの間、どの事業者が対象となり、どの基準に基づいて準備・対応すべきかが明確ではない。事業者を指定し、具体的な対策を求める前に、十分な準備期間を設けるべき。 実施計画の策定・公表後、事業者の規模、既存システムの更新時期、必要な人員・予算等を考慮した経過措置を設け、遡及的又は即時の対応を求めないようにすべき。	御意見として承ります。重要インフラ事業者等の過度な負担とならないよう、重要インフラ所管省庁と連携し、適切なスケジュールの下で対策を進めてまいります。

150	参考資料のPDCAでは、政府機関が実施計画を策定し、施策を実施し、評価案を作成し、政府の戦略本部が評価を決定する構造になっている。政府が自らの施策を政府内部だけで評価するのでは、評価が形式的になるおそれがある。評価指標、評価頻度、未達成時の改善期限及び責任主体をあらかじめ公表すべき。 評価に当たっては、独立した専門家、対象事業者、地方公共団体、中小の委託先、重要インフラの利用者等から意見を聴く仕組みを設けるべき。また、個別事業者の機密情報を保護した上で、分野別及び分野横断的な評価結果、未達成事項及び改善状況を国民に公表すべき。	サイバーセキュリティ基本法に基づき、サイバーセキュリティ戦略本部による重要インフラ統一基準に基づく施策の評価に当たっては、有識者で構成されるサイバーセキュリティ推進専門家会議の意見を聴取することとされています。こうした会議での意見聴取を含め、重要インフラ統一基準に基づくPDCAサイクルの実効性を確保するための仕組みを検討してまいります。
151	形式的な基準の遵守に終始するあまり、現場の柔軟な対応や新たな技術・サービスの迅速な導入が阻害されるおそれがある。セキュリティの確保と、国民が享受するサービスの利便性や迅速性がトレードオフにならないよう、形骸化したチェックリストの強要ではなく、実効性重視の柔軟な運用指針を徹底してほしい。	御意見として承ります。重要インフラ統一基準に基づく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確保してまいります。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。