No.		御意見の内容	御意見に対する考え方
1	1	本ガイドライン案は、ソフトウェアの開発、供給、運用に関わる「サイバーインフラ事業者」と、これを利用する「顧客（政府機関、重要インフラ事業者等）」の責務と役割分担を明確化することを目的としており、ソフトウェアサプライチェーン全体のレジリエンス向上を目指す構成となっています。以下、制度的整合性、実装可能性、普及施策の観点から評価と提案を述べます。 ガイドライン案の位置づけと制度的接続 サイバーセキュリティ基本法の改正（第7条第2項）により、情報システム等供給者に対する努力義務が新設され、本ガイドライン案はその具体化として位置づけられます。統一基準群、重要インフラ策定指針との対応関係が「部」「節」レベルで整理されており、制度間の整合性が高い構成です。特に「リスクマネジメント」「サプライチェーン管理」「平時の運用」など、両者が該当とされる節は優先的な整備対象と考えられます。 （提案）統一基準群、策定指針との読み替えガイドや、対応表（部、節、款レベル）の提供を希望します。 サイバーインフラ事業者と顧客の責務分担 サイバーインフラ事業者には、設計、開発、供給、運用の各フェーズにおいて、セキュアバイデザイン、セキュアバイデフォルトの原則に基づく責務が整理されています。顧客には、経営層によるリスク管理、セキュリティ要件の提示、予算確保など、調達・運用における主体的責務が明記されています。 （提案）顧客向けの調達・運用・予算確保支援ガイドや、契約設計テンプレートの提供を希望します。 要求事項の構成と実装可能性 要求事項はS(1)からS(6)の6カテゴリ、21項目に整理されており、各項目はさらに個別要求に分解されています。各要求事項は、SSDF（SP800-218）、NSAガイダンス、EU CRAなどの国際標準と対応関係が明示されており、技術的裏付けと制度的整合性が高い構成です。 （提案）SP800-218、NSA、CRAとの対応関係マッピング表（日本語版）や、準拠チェックリストの提供を希望します。 要求事項チェックリストの有効性と改善提案 チェックリストは、各要求事項を開発者、供給者、運用者、顧客の役割別に整理しており、実装支援、監査、契約設計において非常に有効です。S(1)からS(6)まで網羅されており、調達仕様書や自己適合宣言の基礎資料として活用可能です。 （提案）・チェックリストのExcel形式、CSV形式での提供 ・チェックの根拠となる役割分担表とのリンク付け ・チェック欄の活用方法に関するガイドの追加 ・情報連携、協力体制（S(5)）に関する事例集の提示 参考情報、用語定義、国際標準との整合性 NIST、NSA、CISA、ISO、ENISA、EU CRA、QUAD原則など、主要な国際標準との整合性が明示されており、制度的信頼性が高い構成です。用語定義も丁寧であり、SDLC、SBOM、DevSecOps、CVSSなど、技術的理解を支える内容となっています。 （提案）用語定義の図解版や、実装例付き解説集の提供を希望します。 検討体制と普及施策への期待 経済産業省、内閣官房、産業界、学識経験者、関連省庁が連携した検討体制が明示されており、制度設計の信頼性と透明性が確保されています。今後の普及施策として、自己適合宣言の仕組み化、チェックリストの活用、契約設計支援などが期待されます。 （提案）検討会の議事録、附属書、宣言様式の公開と、実装支援ツールの整備を希望します。 内部不正、人的リスクへの現実的対応 近年、企業における情報持ち出しや内部不正の事例が相次いでおり、セキュリティ対策において「完全に防ぐことは難しい」ことが現実です。そのため、「起きたときに早く気づき、被害を最小化する」ことが現実的な目標であり、本ガイドライン案においてもその視点が重要です。 S(4)-1.3から1.5（役割と責務の同意、トレーニング、見直し）やS(4)-6.2（開発用エンドポイントの保護）など、人的リスクへの対応が盛り込まれている点は評価できますが、今後は以下のような補完策も検討されることを希望します。 ・ゼロトラストモデルの徹底（最小権限、常時検証） ・行動分析による異常検知（SOC、EDRの活用） ・退職、異動時のアクセス権剥奪と監査 ・倫理教育と内部通報制度の整備 （提案）人的リスクに関する内部不正対応ガイドや、行動監視・監査の実装例の提供を希望します。	ご意見いただきありがとうございます。ご意見を踏まえ、統一基準群との関係の整理を優先し、他の主要な国際標準等との関係整理については、標準化動向などを踏まえつつ、今後の検討の参考にさせていただきます。その他、補足説明を含む各種ツール類等に関するご意見は、今後の参考といたします。
2	1	【概要】 本意見は、「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」が、ソフトウェアサプライチェーン全体のレジリエンス向上を目指すものとして重要な意義を有することを前提としつつ、現実のサイバー空間、とりわけスマートフォン・メールインフラ・デジタルデバイドの状況を踏まえると、現行案のままでは安全性と信頼性の確保が不十分であるという問題意識を述べるものです。具体的には、第一にスマートフォンに関する競争政策との整合性の観点、第二にメールインフラにおける送信側だけでなく受信側の責務の明確化と有害メール対策の位置付けの観点、第三に顧客のリスク管理能力を前提とした記載とデジタルデバイド・ITリテラシーの現状との乖離という観点から、ガイドライン案の補強や今後の制度化の方向性について意見・要望を申し上げます。 本ガイドライン案は、サイバーインフラ事業者と顧客の責務を整理し、ソフトウェアのライフサイクル全体におけるセキュアバイデザイン、セキュアバイデフォルト、サプライチェーンリスク管理、残存脆弱性への対応などを体系的に示している点で、方向性としては妥当であり、国内におけるソフトウェアセキュリティの底上げに資する枠組みだと考えます。一方で、現実のサイバー脅威環境は急速に悪化しており、特にスマートフォンとメールインフラに関しては、既に国民生活の基盤そのものとなっているにもかかわらず、競争政策や事業者の料金体系との関係で安全性・信頼性が十分に優先されていない状況があります。このギャップを埋めるためには、ガイドライン案が示す理念を一層具体化し、サイバーインフラ事業者の責務として「安全性・信頼性を最優先する」という原則を明確に書き込むことが不可欠だと考えます。 まず、スマートフォンにおいて利用される特定ソフトウェアに係る競争の促進に関する法律との関係です。同法は、スマートフォンOSやアプリストア等の競争促進を目的としていますが、現代のスマートフォンは単なる情報端末ではなく、銀行口座、マイナンバーカード連携、健康保険証、医療・行政・決済等を一元的に担う「個人の生命線デバイス」となっています。このようなデバイスに対し、競争促進の名の下にサイドローディングや外部ストアの解放など、OSレベルの統制を緩める方向性が取られる場合、サイバー空間全体のリスクは確実に増大します。本ガイドライン案では、サイバーインフラ事業者の責務としてセキュアな設計・開発・供給・運用やソフトウェアサプライチェーンの管理が掲げられていますが、スマートフォンOS事業者やアプリストア事業者も明確にサイバーインフラ事業者に含まれることを明示し、競争政策の要請があっても、安全性・信頼性を下回る水準まで保護機能を弱めてはならないという原則を記載することが望ましいと考えます。特に、API開放やアプリ配布経路の多様化が避けられないのであれば、それを前提とした強化された検証プロセスや署名検証、サンドボックスの高度化など、代替的なリスク低減策を、ガイドラインとして具体的に示す必要があります。 次に、メールインフラに関する送受信双方の責務についてです。本ガイドライン案では、ソフトウェアサービスやシステムを構成するソフトウェアも対象としており、メールサービス事業者やISP、携帯キャリア等もサイバーインフラ事業者に該当します。現状の日本では、SPF、DKIM、DMARCといった送信ドメイン認証技術が十分に普及していないことに加え、より深刻なのは受信側がそれらの結果を実効的な拒否基準として運用していない点にあります。送信側でSPFやDKIMが失敗しても、受信側がそのメールを平然と受け入れる運用が一般的であり、官公庁、地方自治体、金融機関等をかたるなりすましメールが恒常的に流通しています。メールの安全性はもはや個別企業の問題ではなく、国民全体の安全と直結するサイバーインフラの問題であり、本ガイドライン案においても、メールインフラ事業者の責務として、送信認証の実装だけでなく受信時の検証と規制をセキュアな運用の一部として明確に位置付けるべきだと考えます。 さらに、有害メール対策が多くの事業者において「有料オプション」とされている点も重大な課題です。現状では、キャリアメールやISPメールにおいて、高度な迷惑メールフィルタやなりすまし検知は追加料金を支払った利用者のみが利用できるケースが存在します。この構造は、セキュリティを本来の社会インフラではなく「付加価値サービス」として扱うものであり、所得格差がそのままサイバーリスク格差につながります。本ガイドライン案が、顧客によるリスク管理とセキュアな調達・運用を求めていることは理解しますが、その前提として、サイバーインフラ事業者が提供するサービスの標準仕様の中に、一定水準の有害メール対策を無償で含めるべきだという方向性を明示することが重要です。少なくとも、DMARCポリシーがrejectのドメインからの認証不一致メールや、明らかに認証に失敗しているメールを受信拒否するレベルの制御は、「追加料金で購入する高度なセキュリティ」ではなく、「最低限の安全性」としてガイドラインで取り扱う必要があります。 三点目として、デジタルデバイドとITリテラシーの問題があります。本ガイドライン案は、顧客側にもリスク管理やセキュリティ要件の合意、適切な製品・サービスの選定等の責務を求めていますが、現実には、中小企業、地方自治体の一部、医療・介護現場、さらには一般消費者に至るまで、ITリテラシーや人的リソースに大きな格差が存在しています。デジタルデバイドが解消されていない状況の下で、「顧客によるリスク管理」を前提に責務を配分すると、現場の能力と責任のギャップが拡大し、結果として被害はリテラシーの低い層に集中します。これは単なる教育課題ではなく、国家全体のサイバー・レジリエンスと公平性の問題です。 したがって、本ガイドライン案においては、顧客責務を記載する際に、サイバーインフラ事業者側の「セキュアバイデザイン」「セキュアバイデフォルト」の徹底を一層強調し、ユーザ側の設定や判断に依存しない形でリスクを低減する設計の重要性を明記することが望まれます。具体的には、危険な設定を標準にしないこと、複雑なセキュリティ設定を前提としたサービス設計を避けること、セキュリティ情報を専門家でない利用者にも理解しやすい形で提供することなどを、ガイドライン上の要求事項としてより明確に書き込むべきです。その上で、国全体としてデジタルデバイドの是正とITリテラシーの底上げを「任意の啓発」ではなく「実質的に強制力を持つ普及策」として早期に進める必要があることを、関連政策との関係整理として位置付けていただきたいと考えます。 最後に、本ガイドライン案は現時点では法的拘束力を持たない指針として位置付けられていると理解していますが、サイバーインフラ事業者が担う社会的役割の重大性、スマートフォンとメールインフラを中心とした脅威の深刻化、デジタルデバイドの固定化といった状況を踏まえると、一定の範囲については将来的な制度化も視野に入れて検討すべき段階に来ていると考えます。特に、メールインフラにおける送受信認証の実装と運用、スマートフォンOS・アプリストア事業者のセキュリティ責務、標準サービスとしての有害メール対策の提供などは、任意の努力義務にとどめるのではなく、国際的な動向も踏まえた法的枠組みとの接続可能性を、今後の検討事項としてガイドラインの中で示していただければ幸いです。 以上の観点から、本ガイドライン案が掲げる「ソフトウェアのライフサイクル全体にわたるレジリエンス向上」という目的を実効性あるものとするため、サイバーインフラ事業者の責務の具体化と、スマートフォン、メールインフラ、デジタルデバイドへの配慮に関する記載の補強をご検討くださるようお願い申し上げます。	ご意見いただきありがとうございます。 いただいたご意見は、本ガイドラインおよび普及施策の検討を進める上で今後の参考といたします。

No.		御意見の内容	御意見に対する考え方
3	1	・該当箇所 ・総論／1.2 ガイドラインの位置付け（ソフトウェアライフサイクル全体の安全性確保） ・求められる責務（開発者・供給者・運用者）全般 ・重要インフラの安全基準・行動計画との関係 ・要求事項チェックリスト・サプライチェーン管理部分（セキュア設計・透明性・残存脆弱性対応） これらはすべて、EMP・HPM・GMDなど電磁的広域障害によって機能停止し得る領域に直接関係するため。 ・意見内容 本ガイドライン（案）に、EMP（電磁パルス）、高出力マイクロ波（HPM）、太陽フレア（GMD）等の電磁的広域障害を、 「サイバーインフラ事業者が考慮すべき脅威」として明記し、次の項目を追記することを提案します。 1.ガイドラインの脅威認識に「電磁的広域障害」を追加 2.設計・開発・供給・運用の各段階に『電磁耐性確保（EMP/HPM/GMD耐性）』を要求事項として追加 3.サプライチェーン管理において、電磁耐性情報の共有とリスク評価を必須化 4.重要インフラ安全基準・行動計画との整合性の中に、EMP・電磁波BCPの検討を追加 これらにより、本ガイドラインの目的である「レジリエンス向上」「サプライチェーン保全」の実効性が高まると考える。 ・理由 1. 電磁的広域障害はソフトウェアライフサイクルの前提を破壊する ガイドライン案では、サイバーインフラ事業者がソフトウェアの設計・供給・運用の全段階で安全性を確保する責務を負うと定めている。 しかし、EMP・HPM・GMDが発生した場合、電子計算機・通信機器・制御装置が物理的に停止し、 ライフサイクル管理そのものが不可能化する。 これは、ガイドラインが目的とする「インシデント事前／事後対処」「残存脆弱性の管理」 を根本から無効化しうる。 2. 重要インフラ安全基準との連動性 ガイドライン案は、重要インフラ安全基準・行動計画を補完する立ち位置とされている【2:4 L1-L13】。 一方、電磁的障害は電力・通信・医療など全ての重要インフラに共通する脆弱性であり、実際に国際的には・米国：EMP Executive Order（2019）NATO：EMP Resilience Guidelinesなどで国家安全保障上の主要脅威として扱われている。 ガイドラインが国際基準と整合性を取るためにも、電磁耐性の明記は不可欠。 3. サプライチェーン全体が電磁波に弱い構造 ガイドラインは「透明性」「残存脆弱性対応」「供給者と顧客の連携」を強調しているが、電磁的障害が起こった場合、クラウド・データセンター・ネットワーク機器が同時停止し、サプライチェーン全体の可視性や連携基盤そのものが崩壊する。よって、本ガイドラインの目的である「ソフトウェアサプライチェーンの安全性確保」を実現するには、電磁耐性＝最低限の前提条件として扱う必要がある。	ご意見いただきありがとうございます。 いただいたご意見については、サイバーインフラ事業者に広く求める事項とするか慎重な検討を要することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
4	1	意見1：サイバーインフラ事業者の要求事項に Remote Attestation（RA）とハードウェアRoTの明示を希望 【該当箇所】 サイバーインフラ事業者に求められる「6つの責務」および「6つの要求事項」全般 （特にソフトウェアサプライチェーン管理、残存脆弱性への対処に関する部分） 【意見】 ソフトウェア・サプライチェーンのレジリエンス向上の観点から、Remote Attestation（RA）とハードウェアベースのRoot of Trust（例：TPM 2.0 等） を、ガイドラインの中で明示的に言及していただきたいです。具体的には、以下のような方向性を「要求事項」の例示として追記いただきたいです。 端末・機器・クラウドノード等について、起動時および稼働中の状態（ファームウェア／ブートローダ／OS／主要ミドルウェア）の測定・記録・検証を行う Remote Attestation 機構 を活用すること 測定値や秘密鍵の保護には、TPM 2.0 などのハードウェアルートオブトラストを活用し、ソフトウェア単体の防御に依存しない構成を推奨すること 【理由】 近年の攻撃は OS・アプリ層だけでなく、ファームウェアやブートチェーンの改ざん を起点とするケースが増えています。 セキュア・バイ・デザイン／デフォルトの考え方を実現するうえで、「正常な状態で起動していることをリモート側で検証できる構造」はサプライチェーン全体の信頼を担保する重要な要素です。 国内外で RA の標準化・実装事例（DHA、Keylime 等）が増えており、ガイドラインの中で RA／ハードウェアRoTを位置づけておくことで、サイバーインフラ事業者と利用者双方の期待値をそろえやすくなると考えます。	ご意見いただきありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
	2	意見2：量子耐性暗号（PQC）への移行方針をガバナンスの一項目として位置づけてほしい 【該当箇所】 ソフトウェアに関するガバナンスの整備、リスク管理・暗号管理に関する記述全般 【意見】 ガイドラインにおいて、サイバーインフラ事業者が担うガバナンスの一要素として量子耐性暗号（PQC）への中長期的な移行計画 を明記していただきたいです。例として、以下のような項目の追加・明確化を提案します。 長期にわたり利用されるソフトウェア・サービスについては、将来の暗号アルゴリズムの変更（例：PQC への移行）を見越した暗号アジリティ（アルゴリズム切替の容易性）の確保 を設計段階から考慮すること。 サイバーインフラ事業者は、国内外の標準化動向を踏まえ、利用者に対して 暗号移行のロードマップ（予定時期・影響範囲等） を説明できるよう努めること。 【理由】 重要インフラや行政・金融系システムでは、一度導入したソフトウェア・機器を 10年以上利用するケース も珍しくありません。量子コンピュータの実用化タイミングは不確実ですが、いざ移行が必要になった時に、暗号アジリティがないシステムはサプライチェーン全体のレガシーリスク となります。 ガイドラインの時点で「PQCそのものの実装を義務付ける」必要はないとしても、移行に備えた設計・ガバナンスの重要性 を明示しておくことは、サイバーインフラ事業者・顧客双方にとって有益だと考えます。	ご意見として承りました。 なお、サイバーセキュリティ戦略（令和７年12月23日閣議決定）において、「PQCへの移行については、政府機関等に限るものではなく、重要インフラ事業者等や民間事業者等においても考慮しなければならない課題であるため、関係府省庁の連携の下、必要な対応について検討を進め、円滑な移行を後押ししていく。」こととしております。
	3	意見3：署名鍵・ビルド環境・検証ポイントの「地理的管理・透明性」に関する記述を追加してほしい 【該当箇所】 ソフトウェアサプライチェーン管理、ステークホルダー間の情報連携・協力体制に関する部分 【意見】 サイバーインフラ事業者が行う ソフトウェア署名鍵の管理 ビルド／リリースパイプライン アップデート配信インフラ Remote Attestation の検証サーバ などについて、地理的な管理場所・管轄 を含めた透明性確保の方針をガイドラインに盛り込んでいただきたいです。 例としては、 重要インフラ向けソフトウェア・機器については、署名鍵・ビルド環境・検証サーバ等の所在国・リージョンを利用者が確認できるように情報提供すること。 利用者側が必要に応じて、「国内または信頼できる特定地域に限定した構成（いわゆる地理制限構成）」を選択できるようなアーキテクチャを検討すること。 といった方向性です。 【理由】 サイバー攻撃のリスクは技術要素だけでなく、地政学・管轄権・法制度 と密接に結びついています。 サプライチェーン全体のリスク評価・管理を行ううえで、「どの国・リージョンで署名鍵やビルド環境が管理されているか」は重要な判断材料となります。 ガイドラインに「地理的管理と透明性」の観点を含めておくことで、利用者側がリスク許容度に応じた構成（国内完結、特定リージョン限定 等）を選択しやすくなると考えます。	ご意見として承りました。 本ガイドライン案は、ソフトウェアの開発・供給・運用を行う「サイバーインフラ事業者」に求められる役割等について整理・解説し、当該事業者やその顧客（政府機関等及び重要インフラ事業者を始め、ソフトウェアの利用主体となる事業者等）がサイバーセキュリティ対策の実効性を確保するための参考となる考え方を示したものであるため、地理的管理・透明性については記載しておりません。
	4	意見4：チェックリスト・事例集に RA／TPM／PQC の活用例を盛り込んでほしい 【該当箇所】 ガイドラインの活用促進に向けたチェックリスト・今後の取組に関する部分 【意見】 経済産業省・国家サイバー統括室によるチェックリストや付属文書の整備 を予定されているとのことなので、その中に以下のような観点の設問・事例をぜひ含めていただきたいです。 「端末・機器・クラウドノードの起動状態を RA で検証しているか」 「TPM 等のハードウェアルートオブトラストを活用した鍵保護・測定ログ保護を行っているか」 「将来の PQC 移行を見据えた暗号アジリティを設計に織り込んでいるか」 「署名鍵・ビルド環境・RA 検証サーバ等の地理的管理方針を定めているか」 【理由】 ガイドライン本文はあくまで原則・考え方が中心になると思いますが、実際の事業者・利用者は チェックリストや具体事例を見ながら実装・運用を検討する ことが多いです。 RA／TPM／PQC／地理制限構成は、特にハードウェア・ファームウェア・OSレベルを扱う事業者にとって実務上重要な論点であり、チェックリストに明示することで、サプライチェーン全体の水準底上げに寄与すると考えます。	ご意見いただきありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。

No.		御意見の内容	御意見に対する考え方
5	1	［意見］ステークホルダーの追加 ・該当箇所 P6の表３のステークホルダーの欄 および P7の図1のステークホルダーの欄。 ・意見内容 ステークホルダーに法規制当局を入れる。 ・理由 P24の（４）人材・プロセス・技術の整備で「法令順守」とあるので、監督する行政組織もステークホルダーになると考えられるから。	ご意見いただきありがとうございます。 本ガイドラインのステークホルダーは、ソフトウェアの開発、供給、運用に直接関与する主体とその活動を支援する関連機関を中心に整理しています。 法規制当局につきましては、法令順守の観点から重要な存在ではあるものの、「その他関連機関」の一部として明示はしておりません。 そのため、原案のとおりとさせていただきます。
	2	［意見］法令、ガイドラインがまとまった資料を希望 ・該当箇所 P99の5.5項以降について ・意見内容 他の法令やそれらと本ガイドラインとの関係について説明してある部分が、とてもわかりやすかった。 本ガイドラインに関することから少し外れるが、他の法令・ガイドラインについても、このような相互の関係性をイメージできるような資料があるとわかりやすい。 また、法令やガイドラインの対象者（例えば、メーカー、重要インフラ事業者、重要インフラ以外の事業者、販売者など)が把握できるようになっていると、さらに良い。 ・理由 サイバーセキュリティに関する国内の法令やガイドラインが多くなっているので、どこかでまとめて公開してあると理解しやすいから。	ご意見いただきありがとうございます。 ご意見を踏まえ、統一基準群との関係の整理を優先し、他の主要な国際標準等との関係整理については、標準化動向などを踏まえつつ、今後の検討の参考にさせていただきます。
6	1	・該当箇所 ガイドラインp-75の一番下 ・意見内容 「販売代理店は、ソフトウェア製造業者/IOT製造業者から情報提供があった場合には、製品の重大な脆弱性通知を顧客に行う。」の下に「販売代理店は、顧客が使用しているソフトウェアの情報を管理して、顧客のソフトウェアに該当した脆弱性情報を提供する仕組みの構築を行う。」を追加する。 ・理由 顧客としては、IT/OT/IOT機器等のハードウェア製品の内部に組み込まれている ・ソフトウェア ・バージョン ・ソフトウェアの使用方法 等、多くの脆弱性情報と突合させて、脆弱性対応する事はとても困難な作業となる。 一般的な事例としては、自動車会社のリコール情報提供等、など実現している事例も多くある。 また、DCSベンダーが行う保守契約では実現している事例もある。	ご意見いただきありがとうございます。 ご指摘の通り、顧客ごとの利用環境に合わせた脆弱性情報の提供は、セキュリティ対策を進めるうえで有用と認識しております。 一方、本ガイドラインが対象とする一般的な「販売代理店」には、保守契約を伴わない製品販売を行う事業者も含まれます。これら全ての事業者に対し、顧客ごとのソフトウェア管理を行う仕組みを一律に求めることは過大な負担となり、市場の実態にそぐわない恐れがあります。 そのため、適切な情報の提供を役割とする、原案のとおりとさせていただきます。
7	1	P21 （４） ソフトウェアに関するガバナンスの整備の最終行 「法令を遵守する。」を削除 〈理由〉 事業運営において法令を遵守することは当然の責務であるが、ガイドラインの全般をとおしてこの節に特記されていることに違和感があります。もし、記述するのであれば、「ソフトウェアに関するガバナンスの整備」において念頭にある「法令」について具体例を示した方が良いと考えます。それによって、読者にとっても意義のあるドキュメントになると考えます。	ご意見いただきありがとうございます。 事業運営において法令を遵守することが当然の責務として記載しております。 そのため、法令を遵守するとする、原案のとおりとさせていただきます。
	2	P22 （６） 顧客の経営層のリーダーシップによるリスク管理とソフトウェア調達・運用 P22 上から５行目 「セキュリティ改善を目的とするコミュニティや協力体制の活用」を以下に修正 「顧客、サイバーインフラ事業者を含む関係者間におけるセキュリティ改善を目的とするコミュニティや協力体制の積極的な活用」 〈理由〉 「セキュリティ改善を目的とするコミュニティや協力体制の活用」とあるが、顧客の経営層にとって「セキュリティ改善を目的とするコミュニティ」とは必ずしも明示的では無いと推察する。想定する「セキュリティ改善を目的とするコミュニティ」を例示することが望ましい。また、「セキュリティ改善を目的とするコミュニティ」から一方通行で情報を入手するのではなく、こうしたコミュニティ活動は各企業の善意により成り立っている側面もあることから、コミュニティの健全な発展に対して顧客企業としても賛同・協賛・協力を行う双方向の活動が必要であることを明示することが望ましい。	ご意見いただきありがとうございます。 ご意見の通り、顧客企業が参照すべきコミュニティの具体例を示すことは重要と考えます。ガイドラインとしての読みやすさを考慮し、本文ではなく「5.3 取組例」において具体的な連携先として次の内容を追加いたします。 「ISAC（SoftwareISAC など）やCSIRT 協議会に参加、民間企業の有志団体が集まったコミュニティ、地域のセキュリティコミュニティを通じた連携」 また、双方向の活動（貢献）が必要であるとのご指摘を踏まえ、当該箇所の責務の記述を以下のとおり修正し、積極的な姿勢を明確化します。 「ソフトウェアセキュリティ改善を目的とするコミュニティや協力体制に積極的に参画及び活用する。」
	3	P48 S(6)-2.4 予算確保 現在の記述の下に以下を追加 例えば、納品直前のコンポーネントに漸弱性を発見するなど予見が難しい状況についても、柔軟に対応できる予算を確保する。 〈理由〉 サードパーティーのコンポーネントに起因する脆弱性が、納品前や運用期間中に発見された場合には、開発会社と顧客企業で協調して対応する必要がある。納品直前にコンポーネントに脆弱性が発見された場合には変更に伴う再テストやリリース時期の変更などが求められるが、開発会社によっては予見しようが無い課題であることから、顧客企業としては追加対応費用について柔軟に交渉に応じる姿勢が求められる。完成責任を伴う請負契約の場合であっても例外的な措置として費用負担の交渉などに応じることが求められる。また、保守サポート期間のすぎたソフトウェアやコンポーネントを顧客が追加費用を負担することで延命させることがあるが、業界の健全な発展を踏まえると望ましいことではなく、慣行として排除すべきである。	ご意見いただきありがとうございます。 ご意見の通り、費用負担の面においても事業者と顧客が協調して対応する必要があります。 御意見を踏まえ、5.3の取組例に次の内容を追加いたします。 「OSSやサードパーティ製コンポーネント等において開発・運用期間中等に脆弱性が発見される等のリスクを予見し相応のコスト準備をする。」
8	1	現時点ではサイバー攻撃によるシステム等の被害を完全に防げるまでには至っていないと考えられることを考慮すると、サイバーインフラ事業者や顧客、関係者の役割や責務として、サイバー攻撃によりシステムが被害を受けた後の対応に関する役割や責務も必要と感じます。 また、その場合安易にサイバー攻撃者の要求に従って身代金を支払ってしまうことなどがないよう、何らかの規定や仕組みが必要と思います。そして身代金を支払うなどサイバー攻撃者の要求に従ってしまうことは、サイバー攻撃者を肥太らせ、次なる他者への攻撃も助長してしまうため、可能なら『禁止』又は『原則禁止』にすべきと考えます。	ご意見いただきありがとうございます。 ご意見の通り、システムが被害を受けた後の対応も重要な事項であると認識しております。 本ガイドラインの責務においても、インシデント対応を念頭においており、また、「サイバー攻撃被害に係る情報の共有・公表ガイダンス」等を活用し、関係当局と連携することの重要性についても言及しています。 そのため、原案のとおりとさせていただきます。
9	1	・該当箇所 ガイドライン案P.6 表3 サイバーインフラ事業者及びステークホルダーの分類 サイバーインフラ事業者 - 供給者 - 顧客にソフトウェア製品、ソフトウェアサービス、組み込みソフトウェア（ハードウェア製品を含む）、あるいはこれらのソフトウェアで構成されるシステム・サービスを提供する事業者・人員9 注釈9 供給者内に、開発者・運用者が含まれるケースもある。また、サイバーインフラ事業者に販売会社が含まれるケースでは、供給者に準じた責務が求められる。 ・意見内容 上記のとおり、ソフトウェア製品および組み込みソフトウェアの供給者をすべて販売会社も含んだ一括りで記載されていますが、これらは開発側と販売側を同じカテゴリで区分することで、同じ程度の責務を負うことが定義づけられております。 しかしながら、販売会社に開発側と同じ要件やコードベースの個別要求は事実上難しく、販売会社の責務の負荷が大きく、また多くの販売会社が対応できない事項であると思われます。 本表の供給者から、販売会社を除外するか、もしくは開発側と販売側の責務・役割を明確に変更し定義するべきと考えます。	ご意見いただきありがとうございます。 販売会社は顧客との直接的な接点となるため、供給者としては、必要な情報を顧客へ伝達すること、契約におけるセキュリティ要件の明確化等のサプライチェーン管理および情報連携に関わる責務を担っていただくことを想定しております。 一方で、ご懸念の、コードベースの管理やセキュアな設計・ビルドといった開発工程に深く関わる要求事項は、開発者を対象としており、供給者には求めておりません。現在の分類においても役割と責務は実態に合わせて分担可能な構造となっております。 そのため、原案のとおりとさせていただきます。

No.		御意見の内容	御意見に対する考え方
10	1	・該当箇所 Overall ・意見内容 We agree that organizations, including government agencies, should focus on improving their cybersecurity and resilience and that many of the recommendations contained in the draft document advance our shared goal. However, we see an opportunity to achieve this goal while reducing the risks of negatively impacting harmonization and consequently negatively impacting cybersecurity. Harmonizing requirements across governments strengthens both government and private-sector cybersecurity in many ways, including by: ・Enabling governments to track and compare incidents and campaigns with precision. ・Allowing businesses, especially small and mid-sized firms, to redirect compliance costs into better security innovations. ・Refocusing governments from developing new, overlapping, duplicative, or contradictory requirements, to supporting cybersecurity operations ・Shifting the cybersecurity culture away from paperwork and toward secure design, effective risk management, and resilience. (2) (2) BSA's "Resilience Through Recovery: Elevating Backup in Cybersecurity Preparedness" https://www.bsa.org/files/policy-filings/10212025bsaresilencecybersec.pdf ・理由 While clearly thoughtful and well intentioned, in general, the draft document's current approach of combining, adapting, and reinterpreting requirements from other documents will necessitate further interpretation by industry and create confusion, duplication, and complexity. A more effective path would be to require direct compliance with the US National Institute of Standards and Technology's Secure Software Development Framework, the BSA Framework for Secure Software, or similar documents, and then – if necessary for cybersecurity purposes - The BSA Framework for Secure Software: https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf -BSA's Cyber Policies for Cyber Purposes - How Choice Improves and Politics Degrades Cybersecurity": https://www.bsa.org/files/policy-filings/0418205bsacyberpolpur.pdf	ご意見いただきありがとうございます。 ご意見の通り、NIST SP800-218（SSDF）等は非常に有用な標準ですが、これらは主に「ソフトウェア開発」に焦点を当てたものです。一方で、本ガイドラインは、開発、供給、運用、そして顧客による利用に至るまでのサプライチェーンとライフサイクル全体を対象範囲としております。また、我が国のIT産業構造における委託構造を踏まえるため、単一の既存取組を参照するだけではなく、様々な取組を参照する必要があります。 そのため、NISTをはじめとする複数の国際標準を参照しつつ、事業者と顧客の責務を明確化しました。 これにより、国際標準に準拠している事業者は、大きな負担なく本ガイドラインへの適合を確認でき、かつ日本特有の実情に即した実効性を確保できるよう設計しています。 また、本ガイドラインは、サプライチェーン全体のサイバーセキュリティ確保とレジリエンス向上を目的としており、要求事項において、セキュアな開発プロセスの確立、脆弱性管理、透明性の確保といった技術的なセキュリティ対策とリスクベースのアプローチに主眼を置いており、製品・サービスのセキュリティ品質を可視化することを通して、顧客による適切な製品・サービス選択を促進するものと考えております。 そのため、原案のとおりとさせていただきます。
	2	・該当箇所 Page 66 of English version,5. Reference Information　S(2)-1.3 Risk assessment of software components5.4. Examples of measures implemented to meet requirements / / (2) Life cycle management and assurance of transparency / S(2)-1.1Arrangement of software components ・意見内容 The meaning of the requirement to adopt third-party software component that meet the "in-house requirements" is unclear. Mandating the exact same requirements may be nearly impossible in third parties because of the strength of the security requirements software developers apply to their own code. Developers should be rewarded for continuously strengthening their own security, whereas this requirement brings that approach into question. Notably, the Cyber Resilience Act in the European Union mandates that developers conduct due diligence to verify the conformity of third-party components, which is a more effective approach. ・理由 -BSA Response to the Cybersecurity and Infrastructure Security Agency's Request for Comment on 2025 Minimum Elements of a Software Bill of Materials: https://www.bsa.org/policy-filings/us-bsa-response-to-the-cybersecurity-and-infrastructure-security-agencys-request-for-comment-on-2025-minimum-elements-of-a-software-bill-of-materials The above was in response to the following request for comment: https://www.federalregister.gov/documents/2025/08/22/2025-16147/request-for-comment-on-2025-minimum-elements-for-a-software-bill-of-materials	ご意見いただきありがとうございます。 本ガイドラインにおいてご指摘の要求事項は、サードパーティ製コンポーネントを採用するにあたり、自社製品のセキュリティ品質を確保するために必要な「受入基準」を組織として明確にし、その基準に基づいて選定・評価を行うことを求めているものです。サードパーティに対して開発者（自社）と全く同一の開発プロセスや内部規定の遵守を強制することを求めているものではありません。 なお、ご意見にありますように、EUサイバーレジリエンス法等で求められる「デューデリジェンス」を実施するためには、あらかじめ適切な判断基準（要件）を定義した上で、適合性を確認する必要があり、本個別要求は、まさにそのデューデリジェンスの実践を促すものです。 そのため、原案のとおりとさせていただきます。
	3	・該当箇所 Page 67 of English version /　5. Reference Information/ 5.4. Examples of measures implemented to meet requirement / / (2) Life cycle management and assurance of transparency /S(2)-1.3 Risk assessment of software components ・意見内容 The requirement to "acquire and analyze provenance information for respective software components and assess risks result from components" is, unfortunately, premature given the current status of software bills of materials (SBOMs). For example, important work is ongoing at the US Cybersecurity and Infrastructure Security Agency – in conjunction with experts from academia, industry, and other governments – to define a set of minimum elements for an SBOM. This requirement may create unrealistic expectations and confuse customers who are not as deeply involved with the development and deployment of SBOMs as experts at METI. ・理由 -BSA Response to the Cybersecurity and Infrastructure Security Agency's Request for Comment on 2025 Minimum Elements of a Software Bill of Materials: https://www.bsa.org/policy-filings/us-bsa-response-to-the-cybersecurity-and-infrastructure-security-agencys-request-for-comment-on-2025-minimum-elements-of-a-software-bill-of-materials The above was in response to the following request: https://www.federalregister.gov/documents/2025/08/22/2025-16147/request-for-comment-on-2025-minimum-elements-for-a-software-bill-of-materials	ご意見いただきありがとうございます。 ご意見のとおり、SBOMに関する標準化や環境整備は現在進行形の課題であると認識しております。 一方、本ガイドラインでは、サプライチェーンリスク管理の一環として、利用するコンポーネントの出所を把握し、それに伴うリスクを評価することにあり、SBOMの現状の成熟度や実務上の制約を考慮し、組織間で合意形成を図りながら段階的に取り組むことを推奨する内容となっております。 ご指摘の箇所は、その要件を満たすための取組例を示しているものです。SBOMは推奨事項であり、現状において全てのケースでSBOMの完全な導入を強制するものではございません。 そのため、原案のとおりとさせていただきます。なお、5.4章の取組例にSBOMが必須と誤解する可能性がある記載を見直します。
	4	・該当箇所 Page 70 of English version 5. Reference information / 5.4. Examples of measures implemented to meet requirements / S(2)-2.3 Sharing of release provenance data ・意見内容 The requirement to "collect, protect, maintain, and share provenance data for all components of respective releases" is, unfortunately, premature given the current status of software bills of materials (SBOMs). For example, important work is ongoing at the US Cybersecurity and Infrastructure Security Agency – in conjunction with experts from academia, industry, and other governments – to define a set of minimum elements for an SBOM. Further, the document should distinguish between providing SBOMs to a customer when requested and proactively sharing for multiple reasons including revealing information like configurations and integration strategies which may qualify as trade secrets or information like dependencies which may increase security risks. ・理由 -BSA Response to the Cybersecurity and Infrastructure Security Agency's Request for Comment on 2025 Minimum Elements of a Software Bill of Materials: https://www.bsa.org/policy-filings/us-bsa-response-to-the-cybersecurity-and-infrastructure-security-agencys-request-for-comment-on-2025-minimum-elements-of-a-software-bill-of-materials The above was in response to the following request: https://www.federalregister.gov/documents/2025/08/22/2025-16147/request-for-comment-on-2025-minimum-elements-for-a-software-bill-of-materials	(同上)

No.		御意見の内容	御意見に対する考え方
	5	・該当箇所 P77 of English version/　. Reference Information /5.4. Examples of measures implemented to meet requirements /(3) Prompt responses to remaining vulnerabilities / S(3)-2.3 Security recommendations ・意見内容 The requirement to “report to authorities as specified” is unclear and may conflict with other leading approaches. Effective coordinated vulnerability disclosure minimizes risk to technology users by establishing processes that increase the likelihood that information about vulnerabilities becomes public simultaneously with patches or other remediations that enable users to protect themselves and should be managed pursuant to existing internationally recognized standards like ISO/IEC 29147 and 30111 directly, rather than to, for example, the CRA. ・理由 Reason（If possible, attach or include supporting references or sources.） -The BSA Framework for Secure Software Ver. 1.1: https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf -ISO/IEC 29147:2018/ Information technology — Security techniques — Vulnerability disclosure: https://www.iso.org/standard/72311.html -ISO/IEC 30111:2019 / Information technology — Security techniques — Vulnerability handling processes: https://www.iso.org/standard/69725.html	ご意見いただきありがとうございます。 本ガイドラインにおいて「関連する制度の指定にしたがって当局に報告する」と記述している意図は、事業者が活動する国や地域において適用される法規制や公的な枠組み（制度）を遵守することを求めているものです。 例えば、日本国内における「情報セキュリティ早期警戒パートナーシップ」など、特定の法制度下では、脆弱性情報の当局や公的機関への報告が推奨されております。 ISO/IEC等の国際標準に基づくプロセスと矛盾するものではなく、こうした公的な調整機関への適切な報告を通じて、より広範なステークホルダー間での調整が可能となり、結果として顧客のリスク低減につながると考えております。 そのため、原案のとおりとさせていただきます。
	6	・該当箇所 Page 83 of English version /　5. Reference Information/ 5.4. Examples of measures implemented to meet requirements / (4) Arrangement of human resources, processes, and technologies / S(4)-2.3 Sharing of cost recognition and budgeting ・意見内容 The requirement to “Secure necessary budgets to ensure security based on policy” should acknowledge, explicitly, that this activity should be risk-based. ・理由 -Cybersecurity Management Guidelines for Japanese Enterprise Executives Ver. 3.0: https://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v3.0_en.pdf -The BSA Framework for Secure Software Ver. 1.1: https://www.bsa.org/files/reports/bsa_framework_secure_software_update_2020.pdf -NIST SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities https://csrc.nist.gov/pubs/sp/800/218/final	ご意見いただきありがとうございます。 本ガイドラインにおきまして、個別要求S(4)-2の取組例において、「サイバーセキュリティに関する残存リスクを許容範囲以下に抑制するための方策を検討し、その実施に必要となる資源（予算、人材等）を確保した上で、具体的な対策に取り組む」と記述しております。 これにより、予算確保の活動がリスクを含む様々な要素を踏まえて行われるべきであることを具体例に基づき示しております。 そのため、原案のままとさせていただきます。
	7	・該当箇所 Relevant Section（Clearly indicate the section of the Guidelines to which the comments relate.） P70-72 of English version / 5.4. Examples of measures implemented to meet requirements/ (2) Life cycle management and assurance of transparency / /S(2)-3 Establishment of security requirements among stakeholders ・意見内容 Some of the itemized requirements, descriptions and example measure within S(2)-3 vary from cross mapped NIST Secure Software Development Framework (SSDF) objectives PO 1.3 and PW4.4 in ways that cause confusion for how they might be implemented. We recommend more directly adopting language for this section from the objectives and tasks in the SSDF to promote greater alignment and understanding. If there is desire to require something beyond what is in the SSDF, it would be helpful to explicitly identify where the guidance is choosing to expand beyond the SSDF. ・理由 -NIST SP 800-218 - Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities https://csrc.nist.gov/pubs/sp/800/218/final	ご意見いただきありがとうございます。 本ガイドラインにおきまして、S(2)-3は、単なるソフトウェア開発プロセスにおけるコンポーネント採用基準の定義にとどまらず、開発者、供給者、運用者、および顧客といった異なる組織間での「契約」や「合意形成」を通じたサプライチェーンリスク管理を意図して策定しております。 そのため、当該セクションの策定にあたりましては、SSDFのみならず、より広範なサプライチェーンリスク管理を扱うガイドライン類の要素を統合しております。 SSDFとの対応関係は、参照すべき関連項目を示したものであり、必ずしも要件が完全に一致することを意図したものではございません。 そのため、原案のとおりとさせていただきます。
11	1	「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」に対する意見募集につきまして、パロアルトネットワークス株式会社（以下「当社」という。）として以下の通り意見を提出させていただきます。 1　既存の国際標準との整合性と自己宣言について（日本語版P108-118） ○ISMS、NIST SP800-218、CRAなどの既存の国際標準との整合性を十分に図った上で作成いただき感謝いたします。 ○当社といたしましては、これら既存の国際標準への準拠は、本ガイドラインの要件を満たすための根拠となるものであり、したがって、それらに準拠している事業者はその旨の自己適合宣言を行うことが可能であると認識しております。 ○そうであるならば、既存の国際基準を満たしている事業者が自己適合宣言を行う際に確認が二度手間にならないように、その旨やその他注意点をガイドラインに明記いただけるとありがたく存じます。	ご意見いただきありがとうございます。 本ガイドラインは、特定の認証制度そのものではなく、幅広い事業者が参照すべき指針として策定しており、具体的な第三者監査・認証制度、および調達要件との接続は、今後の検討課題と認識しております。
	2	2 「Secure AI by Design」の促進について：ガイドラインと国際的な潮流との一致について（日本語版 P89-91） ○生成AIの普及を受けたソフトウェアの開発・提供等におけるサイバーセキュリティ確保は国際的にも議論の途上であり、本件ガイドラインのスコープではないと理解いたしますが、P89-91でコラムという形で一定カバーされており本ガイドラインは非常に先進的な内容と考え、生成AI時代のサイバーセキュリティの確保の重要性にも配慮されていると考えます。 ○また、2025年12月23日に閣議決定されました「サイバーセキュリティ戦略」におきましては、AIに係る安全性の確保（Security for AI）、AIを活用したサイバーセキュリティ確保（AI for Security）、AIを悪用したサイバー攻撃への対処の３つの観点を踏まえて今後のルール形成や社会実装等を総合的に推進するとされているところです。 特に当社におきましては、「Secure AI by Design（設計段階からのAIセキュリティ）」のアプローチを通じて、AIエコシステム自体の保護が重要と考えています。 ○具体的には、AIの導入は新たな攻撃対象（攻撃サーフェス）を生み出すため、以下の4つの重要事項に対処する包括的なセキュリティ戦略が必要です。 ・外部AIツールの保護：「シャドーAI」の把握と、プロンプトインジェクションなどの攻撃からの保護。 ・AIインフラとデータの保護： インフラ、モデル、データセットのリスク評価と継続的なテスト。 ・AIアプリの安全な構築と展開： 開発段階からのセキュリティ統合とレッドチーミング（攻撃シミュレーション）。 ・AIエージェントの監視と制御： 自律型エージェントに対するアイデンティティ管理と異常行動の監視。 ○日本におきましては今後ともG7広島AIプロセスのような国際的な議論をフォローアップ・先導していくことを期待しております。 ○本ガイドラインの正式策定後も、AI特有のセキュリティ要件につきまして、経済産業省におかれましては継続的な注視をお願いいたします。あわせて、米国（NIST等）や欧州等の国際的な規格や政策枠組みと歩調を合わせ、将来的にはこれらの要件を機動的にガイドラインの本則を評価・拡充していくプロセスを確立するよう強く要望させていただきます。 ○最後にご参考として、米国下院金融サービス委員会で当社が提出した宣誓供述書を共有させていただきます。 ・2025年12月10日 米国下院金融サービス委員会公聴会 https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=410915 ・2025年12月10日 米国下院金融サービス委員会公聴会の当社の書面陳述資料 https://docs.house.gov/meetings/BA/BA00/20251210/118735/HHRG-119-BA00-Wstate-WhitmoreW-20251210.pdf	ご意見いただきありがとうございます。 ご意見にありましたAIエコシステム保護のための視点は、重要であると認識しております。 ご要望いただきました今後の対応につきましては、G7広島AIプロセスをはじめ、米国や欧州等の国際的な規格・政策枠組みの進展を、経済産業省として継続的に注視してまいります。 技術の進展が著しいAI分野におきましては、セキュリティ要件も流動的であることを踏まえ、将来的にこれらの国際標準と歩調を合わせつつ、本ガイドラインの内容を機動的に評価・拡充していくプロセスを確立し、我が国の産業界が適切な対策を講じられるよう検討します。

No.		御意見の内容	御意見に対する考え方
12	1	本ガイドライン（案）は、サイバーインフラを構成する事業者に求められる基本的な考え方や役割について、常識的かつ妥当な観点から整理されたものと理解しています。そのうえで、ガイドラインの実効性向上および多様な事業形態への配慮という観点から、以下数点の意見を述べます。 1．役割分類（開発者・供給者・運用者）に関する配慮について ガイドラインでは、サイバーインフラ事業者を「開発者」「供給者」「運用者」に分類し、それぞれの役割に応じた責務を整理しています。この整理は全体像を把握するうえで有用である一方、実務においては、単一の組織がこれら複数の役割を兼務するケースも多く存在します。 特に、クラウド型サービスや SaaS 型のセキュリティサービスを提供する事業者においては、ソフトウェアの開発、サービスの提供、ならびに運用・監視までを一体的に担う事業モデルが一般的となっています。このような事業者にとって、役割ごとに責務を切り分けることが現実的でない場合も発生し得るかと考えております。 ガイドラインにおいて、役割を兼務する事業者（SaaS 事業者モデル）の存在を前提とした補足的な説明や考え方を示していただくことで、より幅広い事業形態に対応可能な指針となると考えます。 加えて、役割を兼務する場合においても責務が「重複して増加する」と解釈されるのではなく、サービス提供の実態に応じて合理的に統合・整理できる旨を明示いただくことで、事業者側の過度な負担や誤解などを防ぎ、実効性の高い運用に繋がると考えます。 またガイドライン（案）では「供給者側に開発者・運用者が含まれるケースもある」と整理されていることから、当該ケースを代表例に責務・要求事項の適用方法（適用単位・責務の整理例・顧客との役割分担の進め方など）をもう1段階、具体化いただくことを要望します。	ご意見いただきありがとうございます。 ご指摘の点につきまして、本ガイドラインでは、「1.4. 役割分担の考え方」および「1.5. 代表的なユースケース例」において、クラウドサービスプロバイダ等が開発者・供給者・運用者の役割を兼務するケースを具体的に想定しております。 特に表4や図4においては、一つの事業者が複数の役割（主体）を担う場合の関係性を示しており、役割の兼務を前提とした整理を行っております。 したがって、現行の記述においてもクラウド事業者のモデルには対応可能であると考えており、原案のとおりとさせていただきます。
	2	2．脆弱性対応および情報提供に関する実務上の留意点について ガイドラインでは、脆弱性の把握・対応および利用者への情報提供の重要性が示されており、この方向性自体には強く賛同するものです。一方で、クラウド型サービスにおいては、脆弱性への対処が事業者側で迅速に完結し、利用者側で特段の対応や判断を要しないケースも少なくありません。 このような場合においても、一律に詳細な情報開示や通知を求める運用とした場合、利用者にとっての情報過多や、実務上の負荷増大につながる可能性を懸念するものです。また、脆弱性の内容によっては、開示のタイミングや範囲について慎重な配慮が求められる場合もあります。 そのため、ガイドラインにおいては利用者による対応や判断が必要となる場合を中心に、適切な情報提供を行うという考え方を基本とし、具体的な運用については各事業者の判断や利用者との取り決めに委ねるなどの柔軟性へのご配慮をお願いします。 加えて、利用者側の対応が不要なケースにおいても、事業者が内部的に実施すべき「記録・トレーサビリティ（対応履歴・影響範囲・再発防止策など）」を明確にしつつ、外部への公開については影響とリスクとに応じた階層化（サマリ通知・個別問合せ対応・透明性レポートなど）を推奨する形とすることで、透明性と安全性との両立が可能になると考えます。 また、脆弱性情報の公開が攻撃誘発に繋がり得る点は、得にクラウドサービスでは重要であり、ガイドライン（案）においても「開示のタイミング・範囲を慎重に判断する必要がある」旨を利用者に対しても理解を促す記述として補足いただくことで、現実的且つ安全な運用が促進されると考えます。	ご意見いただきありがとうございます。 ご意見の通り、クラウドサービスにおいては、事業者側で対処が完結し、利用者側での作業が不要なケースが多く存在します。また、脆弱性情報の開示が攻撃の呼び水となるリスクにつきましても、事業者・利用者双方が認識し、慎重に判断すべき重要なポイントであると認識しています。 つきましては、いただいたご提案を反映し、以下の追記を行います。 ・脆弱性情報の提供については、開示のタイミングや範囲について慎重な配慮が求められる場合もある。
	3	3．国際的な制度・基準との整合性について 本ガイドラインの実効性をさらに高め、国内事業者の国際競争力を強化するため、主要な海外制度との整合性確保に引き続きのご配慮をお願いします。特にクラウド型セキュリティサービスにおいては、国際的に共通する要求事項との整合性が、サービスの信頼性向上および国際的な展開の前提となります。 EU サイバーレジリエンス法（CRA）や NIST SSDF などの主要な海外制度との対応関係を整理し、本ガイドラインにおける各要求事項の位置づけを明確化することは、事業者にとって非常に意義であり、国内外で共通した高いセキュリティ水準の確保が進み、結果としてガイドラインの実効性向上にも大きく寄与するものと考えます。 加えて、国内企業が国際市場で信頼を得る上では、単に「対応関係を示す」だけでなく、第三者監査・認証（SOC2・ISO/IEC 27001 など）や調達要件との接続を明確化することが実務上は重要です。特に重要インフラや政府調達などにおいては、要求事項が監査・証跡に落ちる形で整理されることで、導入側の負担軽減と普及促進に繋がると考えます。 また、ガイドライン（案）が今後、政府機関・重要インフラの調達などで参照される可能性が示されていることを踏まえ、事業者が満たすべき事項が調達仕様として「過度に固定化」されないよう、国先基準と同様に「リスクベース」「成熟度に応じた段階的な適用」の考え方（優先度など）を補足いただくことを要望します。	ご意見いただきありがとうございます。 ご意見の通り、国際競争力強化のためには海外制度との整合性が不可欠です。本ガイドラインでは、5.7章に主な国際標準・規制案との対応関係を整理しており、事業者の皆様は各要求事項が国際的な基準の中でどのような位置づけにあるかを明確に確認いただける構成としております。 一方で、本ガイドラインは、特定の認証制度そのものではなく、幅広い事業者が参照すべき指針として策定しており、具体的な第三者監査・認証制度、および調達要件との接続は、今後の検討課題と認識しております。
	4	4．「顧客との役割分担」を実効化するための契約・運用面の「補足」について 本ガイドライン（案）は「顧客と事業者の役割分担」や「正確な情報共有」を重視しており、この整理は非常に重要だと考えます。 一方でクラウド型サービス / SaaS においては、顧客が運用を直接は担わないケースも多く、役割分担が「契約条項（SLA・責任共有モデル・免責事項・ログの保持期間・委託範囲など）」に強く依存します。 このため、ガイドライン（案）において、役割分担を顧客と合意形成する際の最低限の観点（責任共有モデルの明示・インシデント時のエスカレーション・サードパーティの委託管理など）を「推奨項目」として示していただくことで、実務への落とし込みが容易になり、より高い実効性が担保されると考えます。 以上 2025年12月25日 株式会社サイバーセキュリティクラウド 一般社団法人サイバーセキュリティ連盟	ご意見いただきありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
13	1	■1：表4 関連事業者の想定と責務区分・役割の例示 ▼意見内容：どのようにステークホルダ間で役割を調整していくか、契約書やSLAの調整例、具体的な契約ひな型も含めて例示するのはいかがか。 ▼理由：表4に例示されてはいるが、実際の開発においては複雑に責務が入り組んでいるような契約形態もあることが想定されるため。	ご意見いただきありがとうございます。 4.2章に記載の通り、具体的な適用レベルは、顧客が求めるセキュリティ水準や契約要件と整合させて決定することが重要です。 したがいまして、現状の記述を維持し、各事業者が自社の提供する価値とリスク、および顧客との合意に基づいて、主体的にご判断いただく形とさせていただきます。 いただいた御意見は今後の参考といたします。
	2	■2：4.1. 要求事項の要求パッケージ化（最低限/標準パッケージ） ▼意見内容：事業規模、サービス停止時の社会的影響度、取り扱うデータの機密性などに応じて、どちらのパッケージを適用すべきか、より客観的で具体的な判断基準を示すのはいかがか。 ▼理由：自社が最低限/標準どちらに対応すべきかの定義が、あいまいであると、対応計画も適切に立てられないことが想定されるため。	ご意見いただきありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 したがいまして、そのいただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
	3	■3：S(6)-2 顧客経営層のリーダーシップによるソフトウェアの調達、運用 ▼意見内容：開発者、顧客の協働でのリスク分析を具体的にどうすると良いか、howが具体例として提示されるとよいのではないか。 ▼理由：開発者の視点では顧客に要件を具体化することを求められるメリットある一方、現実的、客観的・要件が求められるか懸念があるため。	ご意見いただきありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
	4	■4：1.3. 適用対象　(3) システムを対象とした一般的な役割分担の想定（プライム事業者、サブ事業者 ） ▼意見内容：グローバルなサプライチェーンにおいて、このガイドの要求事項をいかに現実的に適用していくか、その考え方や具体的な進め方のガイダンス整備が必要ではないか。 ▼理由：図1 プライム事業者、サブ事業者 は日本国内に限定されず、海外の事業者の場合、日本の下請法や商慣習で動いていないケース（例：海外SaaSベンダー⇒自国の法令・ガイダンスに沿って提供するケース）も想定されるため。	ご意見いただきありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。

No.		御意見の内容	御意見に対する考え方
14	1	1．P3 ・該当箇所：1.2節 「本ガイドライン（案）は、顧客（政府機関等及び重要インフラ事業者等を含む）にIT/OT システム、ソフトウェア製品又はICT サービスを提供するサイバーインフラ事業者とそのサプライチェーンにおいて、ソフトウェアを対象とした効果的なサプライチェーン上のサイバーセキュリティ対策を進めるため、事業者と顧客との間での適切な役割分担の下で、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものである。」 ・意見内容：このガイドラインは、基幹インフラ事業者は顧客ではないという理解でよいか。（例えば、放送、郵便、港湾運送、貨物自動車運送、外航貨物（海運）は重要インフラ事業者ではないという理解）	ご意見いただきありがとうございます。 本ガイドラインにおける顧客は、政府機関や重要インフラ事業者に限定されるものではなく、IT/OTシステムやソフトウェア製品・サービスを利用する幅広い事業者を対象としております。 ご指摘の「（政府機関等及び重要インフラ事業者等を含む）」という記述は、社会的な影響の大きさから特に本ガイドラインの活用が期待される主体を例示したものであり、これらに該当しない事業者を対象外とする意図ではございません。
	2	2．P4 ・該当箇所：1.2節 「サイバーインフラ事業者とともに進めるリスク対応のコストには、ソフトウェアサプライチェーンにおいて他の関連事業者が実施するセキュリティ対策が組み込まれる価値に対する対価が含まれる点は留意が必要である。また、顧客自らのリスク管理、及びセキュアな調達・運用のプロセスやリソースを整備する必要があるなど、相応の投資が必要になる。」 意見内容：顧客においても、事業を進める上でのソフトウェアのセキュリティ確保の重要性を認識するとともに、本ガイドライン（案）の要求事項に関連した取組を特に意識し進めることで、リスク対応のコストの膨張を適正にコントロールしつつセキュリティを強化する姿勢が重要である」とあるが、相応の投資を相応の費用に修正すべきと考えます。	ご意見いただきありがとうございます。 本ガイドラインは、『サイバーセキュリティ経営ガイドライン Ver 3.0』における重要 10 項目の考え方と整合性を図っております。 ご指摘の箇所における記述は、顧客自らがリスク管理を行い、セキュアな調達・運用のためのプロセスやリソースを整備する行為を対象としております。これらは将来にわたって組織のレジリエンスを高めるための資産形成的な側面を持つことから、「投資」という表現を採用しております。 一方で、ご意見にも引用いただきました通り、その後の文脈におきましては「リスク対応のコストの膨張を適正にコントロールしつつ」と記述しており、日々の運用における「コスト」意識の重要性についても併せて言及しております。経営層に対して積極的なリソース確保を促す投資の側面と、現場における効率化を促すコストの側面の両方を使い分けております。 そのため、原案通りの記載とさせていただきます。
	3	3. ・該当箇所：1.4節 ・意見内容：SW開発や運用にかかわる役割において、顧客インフラシステムのリスクアセスメントを行う場合の役割分担の考え方を示していただきたい。	ご意見いただきありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
	4	4．P9 ・該当箇所：1.4節 ・意見内容：図２に記載がある契約と、表４にある関連事業者の想定と責務区分についてそれぞれの契約がどの責務区分・役割をカバーするのが理想的なのか示していただきたい。	ご意見いただきありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
	5	5．P15 ・対豪箇所：1.5節 ・意見内容：運用保守サービスにおけるユースケースの事例と概念図を追加していただきたい。 ・理由：記載がないため。	ご意見いただきありがとうございます。 本ガイドラインにおきましては、運用保守を独立したフェーズとして切り出すのではなく、ソフトウェアおよびシステムのライフサイクル全体（開発・供給・運用）の流れの中で、統合的に役割を捉えた例として、記載しております。これにより、運用保守サービスを含む一般的な委託形態は網羅されていると考えております。 いただいた御意見は今後の参考といたします。
	6	6．P19 ・該当箇所2.1節 ● 顧客の経営層のリーダーシップによるリスク管理 顧客の独立した主体的な取組及びサイバーインフラ事業者との契約に基づく協力的な取組によるリスク管理 既知の脆弱性への対処及び緩和策を主体的に実施するためのリソースの割当てと整備セキュリティ改善を目的とするコミュニティや協力体制の活用について 意見内容：顧客はサイバーインフラ事業者に適切な対価を払うことを盛り込むということについても言及していただきたい。 理由：参照）経済産業省と公正取引委員会は2022年10月28日付で「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」という指針を公表し、発注側がサプライヤーにサイバー対策を過剰に要求し、対価を支払わない場合は下請法違反（優越的地位の濫用等）になるので、契約で費用負担を明確にし、きちんと支払うようにと注意喚起しています。	ご意見いただきありがとうございます。 本ガイドラインでは、サプライチェーン全体のセキュリティを確保するためには、顧客が事業者に対して適切な対価を支払うことが不可欠であると認識しております。 そのため、1.2章に、「リスク対応のコストには、ソフトウェアサプライチェーンにおいて他の関連事業者が実施するセキュリティ対策が組み込まれる価値に対する対価が含まれる点は留意が必要である」と明記しております。また、顧客の責務としても適切な予算確保を求めております。 なお、顧客と事業者間の関係性構築の観点で、ご提示頂いた文書については、最新の文書を公開しておりますので、「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説」を補足します。
	7	7．P25 ・該当箇所：3.1節図7 ・意見内容：図７について、説明をほそくしていただきたい。 ・理由：図７の外側の３つの殻が何を表現していたいのか、説明がなく、よくわからないため。 例：・3.2節および5.4節に登場する図には記載がない。 ・白抜きの部分はどう解釈する（何かの観点で対象外？） ・中心部のライフサイクルに記載の用語と位置がずれているのは何か意味があるか？	ご意見いただきありがとうございます。 「３つの殻」は対象とするフェーズを意図しています。また、白抜きの部分は当該節で解説するカテゴリ部分のみを色付けして強調（ハイライト）したものです。 なお、概念図であるため、中心部のライフサイクルに記載の用語とは、位置にずれが生じています。 上記の点を補足いたします。
	8	8．P25 ・該当箇所：3.1節図7 ・意見内容：色の使い方を改善して頂きたい。 ・理由：差異の小さな色彩を使用していて醜く、誤解を与える可能性あり、中心部のライフサイクルの色が青から灰色にグラデーションされているが、その意味が明示されておらず、きわめて感覚的である。	ご意見いただきありがとうございます。 現代のソフトウェア開発においては、開発と運用の境界は曖昧になりつつあり、各フェーズが断絶することなく連続的に循環します。グラデーションは、このフェーズ間の切れ目のない連続性と役割の融合・連携を表現しています。 上記の点を補足いたします。
	9	9．P25 ・該当箇所：3.1節図7 ・該当箇所：中心部のライフサイクルに記載で、要件定義・設計分析・計画の矢が運用者から開発者に流れているが、本来は顧客からではないでしょうか。 ・理由：顧客の運用を支援する事業者から直接聞くのは違和感があるため。	ご意見いただきありがとうございます。 ご意見の通り、ビジネス上の要求や最終的な利用要件は「顧客」から提示されるものですが、本図における当該矢印は、運用フェーズで得られた技術的なデータや知見を開発プロセスへ還流させる継続的な改善サイクル（DevOps等）を表現しております。 なお、顧客からの要件提示やガバナンスにつきましては、図の下段に配置した「顧客」のレイヤーに関与する構造として表現しております。 したがいまして、現在の「運用者の役割」からの矢印を維持し、原案通りの記載とさせていただきます。
	10	10．P27 ・該当箇所3.2（1）S(1)－1.4 ・意見内容：リスクベース定期的確認において、全体システムの一部を担当している場合に、システム全体リスク評価を当該開発者が行うのは困難であり、本来は顧客行うべき作業と考えます。 理由：特に担当外のシステムに改変がなされた場合は開発者が知りえない変更となる。また、担当部分のみを行うとして、SWアーキテクチャーが変わらない場合に定期的に評価を行うのは開発者の大きな負担となる。例えば、SWやシステム構成等の変更があるタイミングでの実施ではどうか（定期的に行う必要性が高いのは新たな脆弱性がでる場合であるが、こちらS(2)－1.4やS(3)―1.3でカバーされている認識）。	ご意見いただきありがとうございます。 本要求事項は、顧客と合意した開発者の担当するソフトウェアを対象としたリスク分析・評価のレビューを求めることを意図しており、顧客が管理するシステム全体のリスク評価を開発者が代替して行うことを求めているものではございません。 また、それに加えて定期的な確認を求めている理由は、設計時にやむを得ず「例外」として承認された事項やリスク受容された項目は、時間の経過とともに状況が変化し、許容できなくなる可能性を棚卸しすることにあります。 なお、「定期的」の頻度については、ソフトウェアの種別等を踏まえて事業者と顧客間で適切に合意することを意図しており、過度な負担を求めるものでもございません。 そのため、原案のとおりとさせていただきます。

No.	御意見の内容	御意見に対する考え方
11	11．P33 ・該当箇所：3.2(2) S(2)- 3 ・意見内容：セキュリティ要件の確立について、合意する相手に一般的に顧客であることを図にも明記すべきと考えます。 理由：解説文にはその旨記載があり、それに合わせる。	ご意見いただきありがとうございます。 本要求事項 S(2)-3 は、開発・供給・運用において利用するコンポーネントやサービスを提供する「サードパーティ（供給者、再委託先等）」との間での要件確立を対象としております。 これらの要件については、そもそもサイバーインフラ事業者が製品・サービスを納入する「顧客」との間での要件合意を踏まえたものであるのはもちろんのことです。 仮に、「顧客」を特記すると、本要求事項が「顧客との合意」のみを対象とするなど誤解を招く懸念がございます。 そのため、原案のとおりとさせていただきます。
12	12．P37 ・該当箇所：3.2(3) S(3)-1 ・意見内容：継続的な脆弱性調査について、一般的に顧客が実施するべきであることを図にも明記すべきと考えます。 理由：解説文にはその旨記載があり、それに合わせる。	ご意見いただきありがとうございます。 本ガイドラインにおきましては、要求事項を対象者ごとに明確に区分して定義しております。ご指摘の箇所において、顧客が実施するのが一般的である旨を記述しておりますのは、通常は顧客が行う業務を、事業者が『運用者』として受託・支援する場合には、事業者が本要求事項（S(3)-1）を履行する必要があるという、事業者の適用範囲を明確化するための文脈でございます。 なお、顧客自身が主体となって実施すべき脆弱性対応やリスク管理につきましては、別途 S(6)-1に規定しております。 そのため、原案のとおりとさせていただきます。
13	13．P36 ・該当箇所：3.2(3) S(3)－1.4 ・意見内容未検出の脆弱性は特定できないはずなので、「新たな脆弱性の特定」とすべきと考えます。また、定期的ではなく、出荷前、更新時など実施のタイミングをより現実的にしていただきたい。 ・理由：SWアーキクチャが変わらない場合や顧客などからの報告がない場合に定期的にコードレビュー、分析、テストを行うのは開発者の大きな負担となるため。	ご意見いただきありがとうございます。 本項目における「未検出の脆弱性」とは、リリースや出荷時の検査では発見されず、その後もソフトウェア内に潜伏している脆弱性を指しております。ご提案の「新たな脆弱性」という表現に変更いたしますと、新規開発や修正に伴って「新しく混入した脆弱性」のみを指すように限定的に解釈される懸念がございます。既存のコードベースに潜む、これまで見過ごされてきたリスクを特定するという趣旨を明確にするため、現在の表現を維持させていただきます。 また、「出荷前・更新時」の対応につきましては、主に S(1)-3テスト等において求めるものであり、本個別要求はリリース後の運用・保守フェーズにおいて、検査技術の進歩に合わせて潜在的なリスクを洗い出すことを目的としているため、「定期的」な実施が必要不可欠であると考えております。なお、「定期的」の頻度については、ソフトウェアの種別等を踏まえて事業者と顧客間で適切に合意することを意図しており、過度な負担を求めるものでもございません。 そのため、原案のとおりとさせていただきます。
14	14．P37 ・該当箇所3.2(3) S(3)－2.2 ・意見内容：脆弱性へのリスク対応については、セキュリティ対策の「実装」を明確に定義すべきと考えます。 ・理由：セキュリティパッチ等の対策方法を準備すると認識しています。実際の適用の要否や時期は、システムのサービス影響も勘案して、顧客と協議することが必要となるため。	ご意見いただきありがとうございます。 本ガイドラインにおきまして、S(3)-2.2 は主に「開発者」に求められるタスクとして定義しており、脆弱性を解消するための修正プログラムの作成や、技術的な回避策を確立する行ことを指しております。 ご意見にあります「実際の適用の要否や時期」の判断、および顧客環境への適用作業につきましては、本項目の次のステップであるS(3)-2.3もしくは、S(6)として整理しております。 そのため、原案のとおりとさせていただきます。
15	15．P38 ・該当箇所：3.2(3) S(3)-3 ・意見内容：対処結果を組織のプロセス改善に活用について、一般的に顧客が実施するべきであることを図にも明記すべきと考えます。 理由：特に顧客が策定したプロセスが原因の場合は、開発者・運用者による改善は困難であり、解説文にはその旨記載があり、それに合わせるため。	ご意見いただきありがとうございます。 ご指摘のS(3)-3は、事業者の役割であり、事業者が、脆弱性やインシデントの経験を基に、自らのソフトウェアプロセスを見直し、再発防止を図ることです。 ご指摘の箇所において、顧客が実施するのが一般的である旨を記述しておりますのは、通常は顧客が行う業務を、事業者が受託・支援する場合には、事業者が本要求事項（S(3)-3）を履行する必要があるという、事業者の適用範囲を明確化するための文脈でございます。 なお、顧客自身が主体となって実施すべき脆弱性対応やリスク管理につきましては、別途 S(6)-1に規定しております。 そのため、原案のとおりとさせていただきます。
16	16．P40 ・該当箇所：3.2（4）S(4)-2 ・意見内容：解説文に「ソフトウェアの開発に関わる要件の共有、とあるが、少なとも顧客と共有すべきと考えます。 理由：開発者がだれと共有するか不明であり、それによって「労力の重複を最小化」するロジックが不明確であるため。	ご意見いただきありがとうございます。 ご指摘の箇所は、セキュリティポリシーや開発基準を、組織内の全ての開発チーム・要員および開発パートナーに対して横断的に展開・共有することにあります。 これを通じて、プロジェクトごとに個別のセキュリティ基準をゼロから策定する手間を省くことを解消することによる開発サイドの効率化を目指すものです。 なお、ご提案にあります「顧客との要件共有」につきましては、重要であると認識しており、S(6)において顧客が主体に事業者と共有することとしています。 そのため、原案のとおりとさせていただきます。
17	17．P41 ・該当箇所：3.2(4) S(4)-3 ・意見内容：プロセス・運用ポリシーの確立と法令順守について、に一般的に顧客が実施するべきであることを図にも明記すべきと考えます。 理由：解説文にはその旨記載があり、それに合わせるべきと考えるため。	ご意見いただきありがとうございます。 ご指摘のS(4)-3は、事業者の役割であり、事業者が、脆弱性やインシデントの経験を基に、自らの運用サービスのプロセスを見直し、再発防止を図ることです。 ご指摘の箇所において、顧客が実施するのが一般的である旨を記述しておりますのは、通常は顧客が行う業務を、事業者が受託・支援する場合には、事業者が本要求事項（S(4)-3）を履行する必要があるという、事業者の適用範囲を明確化するための文脈でございます。 なお、顧客自身が主体となって実施すべき脆弱性対応やリスク管理につきましては、別途 S(6)-1に規定しております。 そのため、原案のとおりとさせていただきます。
18	18．P42 ・該当箇所：3.2(4) S(4)-4 ・意見内容：プロセス・運用基準の策定について、に一般的に顧客が実施するべきであることを図にも明記すべきと考えます。 ・理由：解説文にはその旨記載があり、それに合わせるべきと考えるため。	ご意見いただきありがとうございます。 ご指摘のS(4)-4は、事業者の役割であり、事業者が、脆弱性やインシデントの経験を基に、自らの運用サービスのプロセスを見直し、再発防止を図ることです。 ご指摘の箇所において、顧客が実施するのが一般的である旨を記述しておりますのは、本来顧客が主体となって行うべき基準に基づく意思決定等を、事業者が受託・支援する場合には、事業者が本要求事項（S(4)-4）を履行（支援）する必要がある」という文脈で記述したものです。 なお、顧客自身が主体となって実施すべき基準管理につきましては、別途 S(6)が該当します。 そのため、原案のとおりとさせていただきます。

No.	御意見の内容	御意見に対する考え方
19	19. 該当箇所：全体 ・意見内容：取引先であるサイバーインフラ事業者とリスク対応の責務と役割を明確化し、契約により取り決めた手続に従って統合的にリスクを管理することが求められる。契約には、費用負担についても明記すべきと考えます。その際は、適切な対価を払うべきという点にも注意するというような事についても言及していただきたい。	ご意見いただきありがとうございます。 本ガイドラインにおきましては、サプライチェーン全体のセキュリティ対策を実効性あるものにするためには、顧客が適切なコストを負担し、事業者へ対価を支払うことが不可欠であると認識しております。 そのため、1.2章において、「リスク対応のコストには、ソフトウェアサプライチェーンにおいて他の関連事業者が実施するセキュリティ対策が組み込まれる価値に対する対価が含まれる」と明記しております。 また、顧客に対する個別要求S(6)-2.4において、契約に係る予算確保を求めています。 そのため、原案のとおりとさせていただきます。
20	20．P26～ ・該当箇所：3.2節全般 ・意見内容：定期的作業として以下の項目に記載があるが、適切な期間はまちまちであるため、それぞれ理想的な期間の目安を記載すべきと考えます。S(1)-1.4、S(1)-4.4、S(2)-1.4、S(3)-1.4、S(4)-1.5	ご意見いただきありがとうございます。 本ガイドラインにおきましては、多種多様なソフトウェアや事業形態を対象としていることから、実施頻度を一律の期間で規定することは適当ではないと考えております。 なお、「定期的」の頻度については、ソフトウェアの種別等を踏まえて事業者と顧客間で適切に合意することを意図しており、過度な負担を求めるものでもございません。 そのため、原案のとおりとさせていただきます。
21	21．P49～ ・該当箇所：４.1節　表5 ・意見内容：SBOM共有の必要性ついてP68で議論がされている一方でS(2)-2.3は「最低限要求」とされている。本要件の実施の社会的環境が整うまでは「標準要求」のみのレベルとしてはいかがでしょうか。 ・理由：本要件の実施の社会的環境が未整備のため。	ご意見いただきありがとうございます。 ご意見のとおり、SBOMに関する標準化や環境整備は現在進行形の課題であると認識しております。 一方、本ガイドラインでは、サプライチェーンリスク管理の一環として、利用するコンポーネントの出所を把握し、それに伴うリスクを評価することにあり、SBOMの現状の成熟度や実務上の制約を考慮し、組織間で合意形成を図りながら段階的に取り組むことを推奨する内容となっております。 ご指摘の箇所は、その要件を満たすための取組例を示しているものです。SBOMは推奨事項であり、現状において全てのケースでSBOMの完全な導入を強制するものではございません。 そのため、原案のとおりとさせていただきます。なお、5.4章の取組例にSBOMが必須と誤解する可能性がある記載を見直します。
22	22．P49 ・該当箇所：４.1節　表5 ・意見内容：S(3)-1.4を「定期的」に実施を「最低限要求」とするという記載を見直していただきたい。 ・理由：「定期的」に実施を「最低限要求」とすると担当者に大きな負担となるため。	ご意見いただきありがとうございます。 ソフトウェアのコード自体に変更がない場合であっても、攻撃手法の高度化等により、リリース時には検知されなかった脆弱性が後になって発見されるケースは多々ございます。これらを放置することはセキュリティ上の重大なリスクとなるため、最低限の責務として「定期的な確認」を求めております。 また、本ガイドラインにおきましては、多種多様なソフトウェアや事業形態を対象としていることから、実施頻度を一律の期間で規定することは適当ではないと考えております。 なお、「定期的」の頻度については、ソフトウェアの種別等を踏まえて事業者と顧客間で適切に合意することを意図しており、過度な負担を求めるものでもございません。 そのため、原案のとおりとさせていただきます。
23	23．P52 ・該当箇所：4.2節 ・意見内容：4.2 節は「注意事項」となっているが、ここは「注意」する項目ではなく前提条件(もしくは推奨事項）となるべきではないでしょうか。	ご意見いただきありがとうございます。 4.2節は、要求事項を、各事業者が実務に適用する際の手順や、判断に迷いやすいケースにおける補足を示すことを目的としております。 前提条件については、主に1章にて説明し、推奨事項は、3章にて説明することで、区別しています。 そのため、原案のとおりとさせていただきます。
24	24．P99～ ・該当箇所：５章 ・意見内容：5.5 節～5.8節に他のガイド等との関係性について述べられていますが、経済安保推進法 第3章およびこれに基づく「基幹インフラ役務の安定的な提供の確保に関する制度」との関係性を記載していただきたい。	ご意見いただきありがとうございます。 サイバーセキュリティ基本法の改正（第7条第2項）により、情報システム等供給者に対する努力義務が新設され、本ガイドライン案はその具体化として位置づけられ、ご指摘の経済安保推進法とは直接的な関係性を有しておりません。
25	25. ・該当箇所：5.4 セキュリティ対策に伴う費用の考え方 セキュリティ対策に伴う費用について顧客の理解を得るためには、サイバーインフラ事業者自身の利益配分だけではなく、顧客のセキュリティ向上を踏まえた提案が必要となる。また、顧客への費用に関する啓発活動とともに、増加費用の明細（システム開発又は改修の場合は、かかるコストの見積り、クラウドの場合は適用するサービスメニューの追加）と必要性に関する顧客への説明責任が求められる。顧客とサイバーインフラ事業者の両者が、セキュリティ対策の必要性やコストについて、相互の認識を合わせることが重要であり、顧客とサイバーインフラ事業者との間の役割分担、開発環境や用語整備による業界内の共通化・標準化、対象システムのライフサイクルにわたるコミュニケーションなどにより、理解を醸成することが望まれる。（関連する要求事項：S(1)-1 全般） ・意見内容：上記に加えて、経済産業省と公正取引委員会は、2022年10月に「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」についても言及すべきと考えます。	ご意見いただきありがとうございます。 ご意見の通り、顧客のサイバーインフラ事業者の両者が認識をあわせることが重要であり、ご提示いただいた指針は重要な文書であると認識しております。 最新の文書を公開しておりますので、顧客のサイバーインフラ事業者間の関係性の構築の観点で、こちらを参照するようにします。 「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップ構築促進に向けた想定事例及び解説」を補足します。
26	26. ・該当箇所：5.5節 ・意見内容：JCS-TAR★３ではSBOMも要件となっており、JC-STARとの関連性、位置づけも明記していただきたい。	ご意見いただきありがとうございます。 サイバーセキュリティ基本法の改正（第7条第2項）により、情報システム等供給者に対する努力義務が新設され、本ガイドライン案はその具体化として位置づけられます。そのため、JC-STARをはじめとする主要な国内外の標準等との関係整理については、標準化動向などを踏まえつつ、今後の検討の参考にさせていただきます。
27	27. ・該当箇所：表５ ・意見内容S(4)-2.3 費用認識の共有と予算化において、開発者にだけチェックが入っているが、表６の顧客に求められる要求事項についても本項目を追記すべきと考えます。 ・理由：契約でサイバーインフラ事業者に求める項目についての適切な対価を準備することが必要と考えるため。	ご意見いただきありがとうございます。 ご意見にあります通り、顧客がサイバーインフラ事業者に対して適切な対価を支払うための予算を確保することは極めて重要であると認識しております。 ご指摘の S(4)-2.3は、事業者がセキュリティ対策や環境整備に必要な内部予算を確保することを意図した項目となっております。 一方で、顧客が契約に基づき適切な対価を支払うための予算確保につきましては、S(6)にて規定しております。 役割分担の明確化の観点から現在の構成を維持し、原案通りの記載とさせていただきます。
28	28. ・該当箇所：全体 ・意見内容：このガイドラインに対応する顧客に求められる対応も記載すべきと考えます。	ご意見いただきありがとうございます。 本ガイドラインにおきましては、サプライチェーンセキュリティの確保には、事業者のみならず、発注者・利用者である「顧客」の主体的な関与と責任分担が不可欠であると認識しております。そのため、2.2章、3章において、顧客向けの責務および要求事項を既に明確に規定しております。 そのため、ご意見にあります「顧客に求められる対応」を主要な構成要素の一つとして既に盛り込んでいるため、原案通りの記載とさせていただきます。

No.		御意見の内容	御意見に対する考え方
	29	29. ・該当箇所：3.2節(要求事項)と５.4節(各項の取組例と事例の解説) ・意見内容：要求事項毎に各項の取組例と事例の解説を記載して見やすくしていただきたい。 ・理由：要求事項、および各項の取組例と事例の解説が分離していて読みにくいため。	ご意見いただきありがとうございます。 3章の「要求事項」は、サイバーインフラ事業者に求められる要求事項を定義したものであり、手段を限定するものではありません。一方、5章の「取組例」は、達成するための手段や参考情報を例示したものです。 これらを同一箇所に記載いたしますと、特定の取組例が必須の要求事項であるかのように誤認され、各事業者様が自社の環境や技術特性に合わせて最適な実装方法を選択する柔軟性を損なう懸念がございます。 読者の皆様にはページを行き来いただくご不便をおかけする側面があることは重々承知しておりますが、これらを明確に区別し、柔軟な活用を促す観点から、現在の構成を維持し、原案通りの記載とさせていただきます。
15	**1**	意見1: 第三者認証の複合的取得に関する要件の明確化 該当箇所 - 第2章 2.2 責務 (1) セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用（20ページ） - 第3章 3.1 要求事項の全体像 (4) 人材・プロセス・技術の整備（23-24ページ） 意見内容 重要な社会活動を支える情報システムにおいては、情報セキュリティ及び個人情報保護に関する第三者認証を複合的に取得し、継続的な監査・改善が行われていることを、望ましい要件として明確に位置づけることが有効と考えます。 具体的には、ISO/IEC 27001（情報セキュリティマネジメントシステム）、SOC 2 Type II（可用性・セキュリティ管理の運用有効性）、ISO/IEC 27701（プライバシー情報マネジメントシステム）等の国際的に認知された認証を複数組み合わせることで、情報管理・運用体制・サービス品質を多面的に担保する枠組みが構築されます。 理由・根拠 1. ISO/IEC 27001の国際的位置づけと政府調達における重要性 ISO/IEC 27001は、世界150カ国以上で70,000件以上の認証が発行されている情報セキュリティマネジメントシステムの国際標準です（ISO Survey 2022）。 【出典】 - ISO/IEC 27001:2022 - Information security management systems https://www.iso.org/standard/27001 ISO/IEC 27001認証は、政府機関・軍事機関・医療機関等が法令により、ベンダーに高水準の情報セキュリティを証明することを要求する際に頻繁に求められる基準となっています。 【出典】 - "Government, military, or healthcare organizations are often required by law to only work with those vendors who can prove a high standard of information security, and ISO/IEC 27001 certification is often asked for." GoodAccess: ISO 27001 Compliance Guide https://www.goodaccess.com/blog/iso-27001-compliance 2. SOC 2 Type IIによる可用性・継続的運用監視の重要性 SOC 2 Type IIは、米国公認会計士協会(AICPA)が定める信頼サービス基準に基づき、セキュリティ・可用性・処理の完全性・機密保持・プライバシーの5つの基準について、一定期間にわたる運用有効性を第三者が監査する枠組みです。 特に「可用性(Availability)」基準では、以下の要素が評価されます： - 24/7/365の継続的なシステム監視 - 冗長性とフェイルオーバーメカニズム - 災害復旧計画(DRP)と事業継続計画(BCP)の策定・定期テスト - 復旧時間目標(RTO)と復旧時点目標(RPO)の文書化 - バックアップとレプリケーションの実施 【出典】 - "Availability ensures systems and data remain accessible and operational when needed. It's not about 24/7 uptime, but about proactive planning for resilience and disaster recovery. This includes backup systems, failover processes, capacity management, and environmental threat assessments." Bright Defense: SOC 2 Compliance Requirements https://www.brightdefense.com/resources/soc-2-requirements/ - "Continuous 24/7 monitoring conducts over a million monthly checks, ensuring ongoing control assessment for cloud services." Sprinto: SOC 1 vs SOC 2 vs SOC 3 Comparison https://sprinto.com/blog/soc-1-soc-2-soc-3/ 3. 複合認証による多層的セキュリティガバナンスの有効性 単一の認証にとどまらず、複数の国際標準認証を組み合わせることで、組織の情報セキュリティ・プライバシー・可用性の各側面を包括的に担保できます。 【出典】 - "Cloud and SaaS providers often pursue SOC 2 Type II attestation alongside ISO 27001 to demonstrate real-world control effectiveness over time." CreateQ: ISO Certification 27001 and 9001 https://www.createq.com/en/software-engineering-hub/iso-certifications - "A 2023 ISACA survey found that 73% of global compliance leaders now view ISO certification as a 'strategic differentiator' rather than a cost, citing benefits like operational clarity, board engagement, and shortened procurement cycles." 同上	ご意見いただきありがとうございます。 ご指摘の通り、ISO/IEC 27001、SOC 2 Type II、ISO/IEC 27701等の国際的な認証制度は、組織のマネジメントシステムや運用状況を客観的に証明する手段として重要であり、政府機関等や重要インフラにおいて、これらの制度で求められているセキュリティ対策の水準も参考としながら、必要な対策を講じているものと認識しております。 しかしながら、本ガイドラインは、多種多様な業種・規模のサイバーインフラ事業者を対象としており、対策の適用にあたっては、対象となるシステムやソフトウェアの特性に応じ、顧客との共同作業を前提としたリスクベースのアプローチを基本原則としております。 特定の認証規格、あるいはそれらの複合的な取得を一律に「望ましい要件」として規定してしまいますと、例えば個人情報を扱わないシステムに対してプライバシー関連認証を推奨することになるなど、個別のリスク特性や事業環境にそぐわない過剰な要求となったり、認証取得自体が目的化してしまう懸念がございます。 したがいまして、ガイドライン本文への特定の認証の組み合わせの明記は行わず、原案通りの記載とさせていただきます。

No.	御意見の内容	御意見に対する考え方
2	意見2: セキュア・バイ・デフォルトの具体的要件強化 該当箇所 - 第3章 3.2 要求事項 S(1)-1 設計時のリスク評価と対策の追跡（27ページ） - 第3章 3.2 要求事項 S(1)-2 セキュアなビルド（28ページ） 意見内容 「セキュア・バイ・デフォルト」の原則において、利用者および管理者の操作負荷や人的リスクを低減する仕組みが、初期設定段階から組み込まれていることを、より明確な要件として位置づけることが重要と考えます。 具体的には、認証情報管理に過度に依存しない仕組み、誤操作を防止する設計、管理負荷を抑制する自動化機能などが、初期状態から実装されている必要があります。 理由・根拠 1. NISTサイバーセキュリティフレームワークにおけるセキュア・バイ・デザインの位置づけ NIST Cybersecurity Framework 2.0では、セキュリティをシステム設計の初期段階から組み込むことの重要性が強調されています。 【出典】 - "The NIST Cybersecurity Framework (CSF) 2.0 - Organizations must proactively identify and address weaknesses." NIST: The NIST Cybersecurity Framework (CSF) 2.0 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf 2. 人的エラーがサイバーセキュリティの最大の脆弱点である実証研究 人的エラーは、サイバーセキュリティにおける最も脆弱な要素であることが広く実証されています。 【出典】 - "Human error has been widely demonstrated as the weakest link in cyber security. Therefore, all employees should receive regular training to increase their awareness of information security issues and the purpose of the ISMS." IT Governance: ISO/IEC 27001:2022 – Information Security Management https://www.itgovernance.co.uk/iso27001 この課題に対し、セキュア・バイ・デフォルト設計により、初期状態から安全に利用可能なシステムを提供することで、人的ミスのリスクを大幅に低減できます。	ご意見いただきありがとうございます。 ご意見の通り、人的エラーはセキュリティ上の主要な脆弱点であり、設計段階からこれらを低減する仕組みを組み込むことは極めて重要であると認識しております。2章等において、セキュアバイデフォルトの原則に則ることを大前提として規定しております。 一方で、本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
3	意見3: 通信手段の冗長性確保に関する要件の明確化 該当箇所 - 第2章 2.2 責務 (1) セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用（20ページ） - 第3章 3.2 要求事項 S(1)-4 サービスのモニタリング（30ページ） 意見内容 重要な社会活動を支えるシステム、特に防災・緊急時対応・事業継続に関わる分野では、単一の通信手段や経路に依存しない設計が必須と考えます。 複数の通信手段（SMS、音声通話、モバイルデータ、電子メール等）を併用可能とすることで、回線障害や混雑時におけるリスク低減が図られます。 理由・根拠 1. FEMA（米国連邦緊急事態管理庁）による複数通信経路の推奨 FEMAは、災害時のレジリエンスと冗長性を確保するため、複数の通信手段を活用することを推奨しています。 【出典】 - "Resilience and redundancy in communications help to ensure the uninterrupted flow of information. Resilience is the ability of systems to withstand and continue to perform after damage or loss of infrastructure. Redundancy is achieved through the duplication of services." FEMA Emergency Management Institute https://training.fema.gov/is/courseoverview.aspx?code=IS-2200&lang=en - "Utilizing multiple pathways for public alerts increases the likelihood that the message will successfully reach the public. IPAWS is structured to facilitate this functionality." FEMA: Integrated Public Alert & Warning System https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system 2. 緊急通信における多チャネルアプローチの科学的根拠 緊急時における効果的な警告には、複数の通信チャネルを協調的に使用することが不可欠です。 【出典】 - "Effective warning requires the coordinated use of multiple channels of communication. For most people the first warning received captures their attention and triggers a search for corroboration, but cannot be relied on to elicit the desired behavior." Wikipedia: Emergency communication system https://en.wikipedia.org/wiki/Emergency_communication_system - "Multi-channel communication: Effective systems use multiple communication channels to ensure message delivery even if one channel fails. This redundancy is crucial for reaching all stakeholders in a timely manner." Crises Control: Emergency Communication Systems https://www.crises-control.com/blogs/emergency-communication-systems-3/ 3. 日本の大規模災害における通信システムの教訓 2011年の東日本大震災では、地上回線と携帯電話回線が機能しなかった地域でも、インターネットや衛星電話が通信手段として機能しました。 【出典】 - "In areas with infrastructure still intact, even though both landline and mobile phone lines were not functioning as might be expected, the Internet was still accessible. In the hardest hit areas, particularly Sendai and other areas of Miyagi, Iwate, and Fukushima Prefectures, satellite phones were often the only form of communication that functioned reliably." Wikipedia: Emergency communication system https://en.wikipedia.org/wiki/Emergency_communication_system	ご意見いただきありがとうございます。 通信手段の冗長性確保は重要な事項と認識しております。 一方で、本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。

No.	御意見の内容	御意見に対する考え方
4	意見4: クラウドインフラの冗長性・可用性確保に関する要件の明確化 該当箇所 - 第3章 3.2 要求事項 S(1)-1.1 リスクベースのセキュリティ要件の定義（27ページ） - 第3章 3.2 要求事項 S(4)-6 技術:セキュアな開発環境の整備（44ページ） 意見内容 重要な社会活動を支える情報システムにおいては、基盤となるインフラについて、十分な冗長性・耐障害性・拡張性を備えたクラウド環境を活用し、物理設備や運用体制も含めて高い可用性を確保していることが重要です。 特定事業者や限定的な環境に依存しない構成、マルチリージョン・マルチアベイラビリティゾーン構成による地理的分散が望まれます。 理由・根拠 1. 主要クラウドプロバイダーにおけるマルチAZ・マルチリージョン構成の標準 AWS、Microsoft Azure、Google Cloud Platformの3大クラウドプロバイダーは、高可用性を実現するため、複数のアベイラビリティゾーン(AZ)と複数のリージョンを提供しています。 【出典】 - "AWS, Azure and GCP all have uptime SLAs of 99.9% for a single VM and 99.99% for a pair of VMs spread across two AZs. An uptime SLA of 99.999%, which is only 5 minutes of downtime per year, is achievable by combining the multi-AZ approach, double redundancy, active-active HA." FlashGrid Inc.: Multi-AZ vs. Multi-Region in the Cloud https://www.flashgrid.io/news/multi-az-vs-multi-region-in-the-cloud/ 2. マルチリージョン冗長性の重要性 単一リージョン内のマルチAZ構成だけでは、大規模災害（地震、津波、戦争等）に対する完全な災害復旧は実現できません。真の災害レジリエンスには、複数リージョンにわたる冗長性が必要です。 【出典】 - "Regional outages do happen, and in those cases, it is important to be able to recover your business critical applications to an alternate region. Implementing a multi-AZ architecture in AWS is not enough to achieve true disaster resilience." Arpio: Multi-Region Redundancy for AWS Disaster Recovery https://arpio.io/multi-region-redundancy/ - "Multi-cloud environments enhance disaster recovery (DR) capabilities by enabling cross-cloud redundancy. Businesses should implement multi-region replication and automated failover strategies to ensure high availability." Cogent: Maximizing SAP with Multi-Cloud https://www.cogentinfo.com/resources/maximizing-sap-with-multi-cloud-the-best-of-aws-azure-and-gcp 3. NISTフレームワークにおける重要インフラの可用性・レジリエンス NIST Cybersecurity Frameworkは、重要インフラのサイバーセキュリティにおいて、可用性とレジリエンスの向上を中核的目標として位置づけています。 【出典】 - "The Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security." NIST: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11	ご意見いただきありがとうございます。 クラウドインフラの冗長性・可用性は重要な事項と認識しております。 一方で、本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、特定のプラットフォーム（パブリッククラウド）に固有の構成技術（マルチリージョン等）であり、対象範囲の汎用性を損なう懸念がございます。より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
5	意見5: 24時間365日監視体制および異常検知機能に関する要件の明確化 該当箇所 - 第3章 3.2 要求事項 S(1)-4 サービスのモニタリング（30ページ） - 第3章 3.2 要求事項 S(4)-3 プロセス:運用ポリシーの確立と法令順守（41ページ） 意見内容 重要な社会活動を支えるサービスにおいては、サービス提供基盤に対して、24時間365日体制での監視および異常検知が行われ、迅速な初動対応が可能な体制が整備されていることが必須と考えます。 これは単なる障害対応にとどまらず、予兆検知や被害最小化の観点でも重要です。 理由・根拠 1. SOC 2における継続的監視の要件 SOC 2 Type IIでは、24/7/365の継続的なシステム監視とセキュリティ運用センター(SOC)の設置が、可用性とセキュリティの基準を満たすために求められます。 【出典】 - "RPE's Type 2 SOC 1 and SOC 2 Data Center offers 24/7/365 US-based engineering and support, top-tier security, high availability, and scalability." RPE Solutions: Type 2 SOC 1 and SOC 2 Data Center https://www.rpesolutions.com/type-2-soc-1-and-soc-2-data-center/ - "Our SOC is organised into different teams of specialists, depending on the severity of the threat. This reduces the time required to detect and respond to threats. With an average response time of just 12 minutes and a 75% reduction in false positives, our SOC delivers precision and reliability." Wizard Cyber: 24/7 SOC Services https://wizardcyber.com/24-7-soc/ 2. 継続的監視によるインシデント早期検知と対応時間の短縮 24時間365日の監視体制により、セキュリティインシデントや性能劣化を早期に検知し、迅速に対応することが可能になります。 【出典】 - "Continuous monitoring: Routinely track system performance and detect service degradations. Security monitoring: Centralized logging, anomaly detection, and real-time alerting for suspicious behavior." Venn: SOC 2 Compliance in 2026 https://www.venn.com/learn/soc2-compliance/ - "Monitoring and incident response: Continuous surveillance of systems to detect and address security breaches or policy violations quickly, minimizing damage and downtime." InfraCloud: A Comprehensive Guide to Achieving SOC 2 Compliance https://www.infracloud.io/blogs/achieving-soc-2-compliance-comprehensive-guide/	ご意見いただきありがとうございます。 ご意見の通り、重要な社会活動を支えるサービスにおいて、継続的な監視と迅速な初動対応が可能な体制を整備することは極めて重要であり、SOC 2 Type II等で求められる基準は、そのための有効なモデルの一つであると認識しております。 しかしながら、本ガイドラインは、多種多様な重要度・性質を持つソフトウェアおよびサービスを対象としております。そのため、全ての「重要な社会活動を支えるサービス」に対して一律に24時間365日の有人監視体制等を必須要件として規定することは、サービスの特性やコスト対効果の観点から、必ずしも最適解とならないケースも想定され、具体的な監視レベルや対応時間（SLA）については、顧客との合意形成によって決定されるべきものであると考えております。 したがいまして、原案通りの記載とさせていただきます。

No.	御意見の内容	御意見に対する考え方
6	意見6: サービスレベル合意(SLA)における免責事項の適切性確保 該当箇所 - 第2章 2.2 責務 (1) セキュリティ品質を確保したソフトウェアの設計・開発・供給・運用（20ページ） - 第3章 3.2 要求事項 S(2)-3 関係者間のセキュリティ要件の確立（34ページ） 意見内容 重要な社会活動を支えるサービスにおいては、障害発生時の対応範囲や責任の所在が明確であり、サービスレベルに関する指標において、基盤停止等の重要事象が適切に扱われていることが重要です。 免責事項が過度に広範となることは、利用者側のリスク管理上の課題となります。 理由・根拠 1. SOC 2における可用性基準とSLA SOC 2の可用性(Availability)基準では、サービス提供者が契約またはSLAで規定された通りにシステムが利用可能であることを保証する責任を負います。 【出典】 - "The availability principle refers to the accessibility of the system, products or services as stipulated by a contract or service level agreement (SLA). This principle does not address system functionality and usability, but does involve security-related criteria that may affect availability." Imperva: What is SOC 2 https://www.imperva.com/learn/data-security/soc-2-compliance/ 2. クラウドサービスにおける責任共有モデルの明確化 主要クラウドプロバイダーは「責任共有モデル(Shared Responsibility Model)」を採用していますが、サービス事業者は自身が提供するサービス層における可用性と復旧について責任を持つ必要があります。 【出典】 - "Per their Shared Responsibility Model, AWS is accountable for the physical infrastructure it operates and the managed services it provides, but their customers are responsible for their own resiliency when assembling their cloud environments." Arpio: Multi-Region Redundancy for AWS Disaster Recovery https://arpio.io/multi-region-redundancy/	ご意見いただきありがとうございます。 ご意見の通り、重要な社会活動を支えるサービスにおいて、障害発生時の責任範囲が不明確であったり、免責事項が不当に広範であることは、利用者にとって重大なリスク管理上の課題となり得ると認識しております。 しかしながら、本ガイドラインは、多種多様な重要度・性質を持つソフトウェアおよびサービスを対象としております。そのため、SLAにおける具体的な免責事項の範囲や賠償責任の条件につきましては、サービスの性質、コストおよび利用者と提供者間の商取引上の合意によって個別に決定されるべき事項と考えております。 したがいまして、原案通りの記載とさせていただきます。
7	意見7: 過去の重大セキュリティ事故・障害履歴の評価制度化 該当箇所 - 第3章 3.2 要求事項 S(6)-2 顧客経営層のリーダーシップによるソフトウェアの調達、運用（該当ページ記載あり） - 第2章 2.2 責務 (6) 顧客の経営層のリーダーシップによるリスク管理とソフトウェア調達・運用（21-22ページ） 意見内容 重要な社会活動を支える情報システムの調達においては、過去に重大な情報セキュリティ事故や利用者影響の大きい事象が発生している場合、その再発防止策や改善状況が客観的に説明可能であり、調達時に適切に評価される仕組みが必要と考えます。 これにより、同様の事故を繰り返すリスクを低減し、より信頼性の高いサービス提供者を選定することが可能になります。 理由・根拠 1. NISTサイバーセキュリティフレームワークにおける継続的改善の重要性 NISTフレームワークでは、過去のインシデントから学び、継続的に改善するプロセスが重視されています。 【出典】 - "Cybersecurity can be an important and amplifying component of an organization's overall risk management. NIST CSF promotes a culture of continual improvement in information security practices." NIST: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf 2. ISO/IEC 27001における是正措置と継続的改善 ISO/IEC 27001では、セキュリティインシデント発生後の是正措置と、再発防止のための継続的改善が要求されています。 【出典】 - "ISO/IEC 27001 promotes a culture of continual improvement in information security practices. Regular monitoring, performance evaluation, and periodic reviews help organizations adapt to evolving threats and enhance their ISMS effectiveness." Wikipedia: ISO/IEC 27001 https://en.wikipedia.org/wiki/ISO/IEC_27001 3. 調達時のリスク評価における過去実績の重要性 政府調達および企業調達において、ベンダーの過去のセキュリティインシデント履歴と対応実績を評価することは、リスクベースの意思決定において不可欠です。 【出典】 - "Customers using a multi-cloud environment can have a strategy to prepare for potential outages. Organizations that protect their applications and databases demonstrate commitment to data security through regular audits and documented remediation." AWS Blog: Failover Microsoft Azure workloads to AWS using AWS Elastic Disaster Recovery https://aws.amazon.com/blogs/storage/failover-microsoft-azure-workloads-to-aws-using-aws-elastic-disaster-recovery/ 総括 以上の7つの意見は、いずれも特定の技術や事業者を想定するものではなく、今後のデジタル社会において、公共性の高い分野で利用されるソフトウェア・サービス全般に共通して求められる基本的な考え方です。本ガイドラインにおいて、これらの方向性が明確に示されることを期待いたします。 出典一覧 ISO/IEC 27001関連 1. ISO/IEC 27001:2022 - Information security management systems　https://www.iso.org/standard/27001 2. GoodAccess: ISO 27001 Compliance Guide　https://www.goodaccess.com/blog/iso-27001-compliance 3. CreateQ: ISO Certification 27001 and 9001　https://www.createq.com/en/software-engineering-hub/iso-certifications 4. IT Governance: ISO/IEC 27001:2022 ? Information Security Management　https://www.itgovernance.co.uk/iso27001 5. Wikipedia: ISO/IEC 27001　https://en.wikipedia.org/wiki/ISO/IEC_27001 SOC 2関連 6. Bright Defense: SOC 2 Compliance Requirements　https://www.brightdefense.com/resources/soc-2-requirements/ 7. Sprinto: SOC 1 vs SOC 2 vs SOC 3 Comparison　https://sprinto.com/blog/soc-1-soc-2-soc-3/ 8. Venn: SOC 2 Compliance in 2026　https://www.venn.com/learn/soc2-compliance/ 9. InfraCloud: A Comprehensive Guide to Achieving SOC 2 Compliance　https://www.infracloud.io/blogs/achieving-soc-2-compliance-comprehensive-guide/ 10. RPE Solutions: Type 2 SOC 1 and SOC 2 Data Center　https://www.rpesolutions.com/type-2-soc-1-and-soc-2-data-center/ 11. Imperva: What is SOC 2　https://www.imperva.com/learn/data-security/soc-2-compliance/ NIST Cybersecurity Framework関連 12. NIST: The NIST Cybersecurity Framework (CSF) 2.0　https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf 13. NIST: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1　https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf 14. NIST: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1　https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11 緊急通信・多チャネル通信関連 15. FEMA Emergency Management Institute　https://training.fema.gov/is/courseoverview.aspx?code=IS-2200&lang=en 16. FEMA: Integrated Public Alert & Warning System　https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system 17. Wikipedia: Emergency communication system　https://en.wikipedia.org/wiki/Emergency_communication_system 18. Crises Control: Emergency Communication Systems　https://www.crises-control.com/blogs/emergency-communication-systems-3/ クラウドインフラ冗長性関連 19. FlashGrid Inc.: Multi-AZ vs. Multi-Region in the Cloud　https://www.flashgrid.io/news/multi-az-vs-multi-region-in-the-cloud/ 20. Arpio: Multi-Region Redundancy for AWS Disaster Recovery　https://arpio.io/multi-region-redundancy/ 21. Cogent: Maximizing SAP with Multi-Cloud　https://www.cogentinfo.com/resources/maximizing-sap-with-multi-cloud-the-best-of-aws-azure-and-gcp 22. AWS Blog: Failover Microsoft Azure workloads to AWS using AWS Elastic Disaster Recovery　https://aws.amazon.com/blogs/storage/failover-microsoft-azure-workloads-to-aws-using-aws-elastic-disaster-recovery/24/7 監視体制関連 23. Wizard Cyber: 24/7 SOC Services　https://wizardcyber.com/24-7-soc/	ご意見いただきありがとうございます。 ご意見の通り、重要な社会活動を支える情報システムの調達において、過去のインシデントから教訓を得て改善プロセスが回っているかを確認することは、信頼性の高い事業者を選定するために極めて重要であると認識しております。 一方、本ガイドラインにおきましては、S(3),(4)等の要求事項を通じて、ご提案の趣旨である「過去の経緯や改善状況を踏まえた調達」を推奨する構成としております。 したがいまして、過去の事故履歴のみを切り出して一律の評価要件とするのではなく、顧客が対象システムの重要度に応じて行う「総合的なリスク評価」の一部として、事業者の改善姿勢や実績を評価すべきであるという考えに基づき、現在の記述を維持し、原案通りの記載とさせていただきます。

No.		御意見の内容	御意見に対する考え方
16	1	（意見①）運用フェーズにおける振る舞いベースの継続的監視の明確化 ・該当箇所 第3章 （1）セキュアな設計・開発・供給・運用 （3）残存する脆弱性の速やかな対処 ・意見内容 本ガイドライン（案）では、設計・開発段階におけるセキュリティ確保や、脆弱性管理を通じたリスク低減の重要性が整理されている。 一方、実際のサイバーインシデントの多くは、設計上は正当であり、既知の脆弱性が顕在化していないソフトウェアやシステムが、運用段階において想定外の通信や挙動を示すことにより発生している。 そのため、設計・供給段階での対策を前提としつつも、運用フェーズにおいて、実際の通信・挙動を継続的に把握し、事前定義やシグネチャに依存しない形で異常を検知・評価する仕組みが、サイバーセキュリティレジリエンス向上の観点から重要であることを、ガイドライン上でより明確に位置付けることが望ましい。 ・理由 本ガイドライン（案）第1 章では、サイバー攻撃の起点が多様化し、ソフトウェアのライフサイクル全体にリスクが潜在することが示されている。 ➢NIST SP 800-218（Secure Software Development Framework）では、設計・開発段階の対策に加え、運用中の異常な振る舞いを継続的に把握・対応する必要性が整理されている。 https://csrc.nist.gov/publications/detail/sp/800-218/final ➢米国CISA「Secure by Design」では、静的対策に加え、実運用における継続 的なリスク管理の重要性が示されている。 https://www.cisa.gov/securebydesign	ご意見ありがとうございます。 本ガイドラインでは、要求事項S(1)-4、S(3)-1等、S(4)-3において、運用フェーズにおける継続的な監視体制の整備や、リスクに応じた対応を求めております。 ご指摘の「振る舞いベースの継続的監視」は有効な対策の一つと認識しておりますが、本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。 いただいた御意見は今後の参考といたします。
	2	（意見②）SBOM 等による構成管理の限界と、運用時評価の補完 ・該当箇所 第3章 （2）ライフサイクル管理、透明性の確保 ・意見内容 SBOM 等を用いたソフトウェア構成の可視化は、サプライチェーン上の透明性を確保する上で重要な取組である。一方で、SBOM は「どのソフトウェアが含まれているか」を示すものであり、「どのように利用され、どのような挙動を示しているか」までは評価できない。 実運用においては、正規のソフトウェアコンポーネントが、想定外の通信先への接続や、通常とは異なる時間帯・頻度で動作することにより、リスクが顕在化する場合がある。 そのため、SBOM による構成管理を前提としつつ、運用中の挙動を継続的に評価・補完する視点について、ガイドライン上で補足的に言及することが有用。 ・理由 ➢経済産業省「SBOM 導入に関する手引」では、SBOM は構成管理の基盤であり、運用時のリスク評価を直接代替するものではないことが示されている。 https://www.meti.go.jp/press/2024/08/20240829001/20240829001-1r.pdf ➢米国CISA においても、SBOM はセキュリティ対策の一要素であり、単独で安全性を保証するものではないと整理されている。 https://www.cisa.gov/sbom ➢MITRE ATT&CK では、正規機能や通信を悪用する攻撃（Living off the Land）が多数整理されている。 https://attack.mitre.org/techniques/T1105/	ご意見ありがとうございます。 ご指摘の通り、SBOM等による構成管理と、運用時における挙動の監視は、相互に補完し合う重要な要素であると認識しております。 本ガイドラインでは、これらの要素をフェーズに応じて整理しており、運用中の挙動の継続的な評価は、要求事項S(1)-4等で規定して、SBOM等による構成管理は、要求事項S(2)において規定しております。したがいまして、本ガイドライン全体として、S(2)で構成管理の透明性を確保しつつ、S(1)-4で運用時の実挙動を監視するという多層的な対策を求めていることから、ご意見の趣旨は既に包含されているものと考えます。 そのため、原案通りの記載とさせていただきます。
	3	（意見 ③）IT／OT／IoT 環境における非侵襲・業務影響最小化前提の明確化 ・該当箇所 第1章 第3章 1.3 適用対象（IT／OT／IoT を含む点） （3）残存する脆弱性の速やかな対処 ・意見内容 本ガイドライン（案）では、IT／OT／IoT を含む幅広い環境が対象とされている。特にOT や重要インフラ環境では、以下制約が存在する。 ①パッチ適用が困難 ②エージェント導入が制限される ③通信遮断が業務停止につながる このような環境においては、システムに影響を与えない形で状況を把握し、業務影響を最小化しながら段階的にリスク低減を図るアプローチが現実的な対応となる。 IT とOT で前提条件が異なる点について、ガイドライン上で補足説明を加えることで、実務への適合性が一層高まると考える。 ・理由 ➢ガイドライン（案）ではOT も対象に含まれているが、IT とOT の運用制約の違いについては詳細な整理がなされていない。 ➢NIST SP 800-82（ICS Security）では、可用性・安全性を最優先とした段階的な対策の重要性が示されている。 https://csrc.nist.gov/publications/detail/sp/800-82/rev-3/draft ➢IEC 62443 シリーズにおいても、OT や重要インフラ環境における可用性・安全性を考慮したサイバーセキュリティ対策のフレームワークを提供していることが公開 https://en.wikipedia.org/wiki/IEC_62443 https://niccs.cisa.gov/training/catalog/tonex/iec-62443-industrial-automation-control-systems-iacs-cybersecurity	ご意見ありがとうございます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。いただいた御意見については、より具体的な取組内容に相当すると考えます。また、こうした多様な環境に対応するため、一律の対策ではなく、対象となるシステムやサービスの特性に応じたリスクベースのアプローチを求めております。 OT環境における制約や特性を踏まえ、事業者がリスク評価に基づき、非侵襲的な監視や代替策を含めた適切な手段を選択することを前提とした記述となっております。 したがいまして、ご意見の趣旨は既にガイドラインの考え方に包含されているものと考え、原案通りの記載とさせていただきます。
	4	（意見④）検知後の説明可能性とステークホルダー間の合意形成支援 ・該当箇所 第3章 （5）サイバーインフラ事業者・ステークホルダー間の関係強化 ・意見内容 インシデント対応においては、単に検知・遮断・復旧を行うだけでなく、なぜその挙動が異常と判断されたのか、どこまで影響が及んだのかを関係者間で共有・説明できることが重要である。 特に、運用担当者、現場部門、経営層、外部委託先など、多様な関係者が関与する環境では、説明可能性が担保されない場合、迅速な判断や合意形成が困難となる。そのため、検知後の対応における説明性・可視性の確保について、ガイドライン上で補足することが有用である。 ・理由 ガイドライン（案）では、ステークホルダー間の連携強化が重要とされている。 ➢NIST AI Risk Management Framework では、AI を用いた判断における説明可能性（Explainability）と透明性が信頼性確保の要素として整理されている。 https://www.nist.gov/itl/ai-risk-management-framework ➢OECD AI 原則においても、透明性・説明責任が重要な原則として示されている。 https://oecd.ai/en/ai-principles	ご意見ありがとうございます。 多様な関係者が関与する環境において、迅速な判断と合意形成のために説明可能性が重要であると認識しております。 本ガイドラインは、ステークホルダーへの説明や情報共有のあり方についても、システムのリスクや関係者の特性に応じて個別に最適化されるべきものと考えております。 要求事項S(3)において、利害関係者に対するコミュニケーション計画を定めることとしており、ステークホルダーが求める情報の粒度や説明のレベルの定義を通じて、判断根拠の可視化等を促進する合意形成プロセスを設計するものと考えます。 一方で、本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。

No.		御意見の内容	御意見に対する考え方
	5	（意見⑤） ・該当箇所 第2章 2.1. 責務と役割分担の考え方 ・意見内容 企業に対し「監視・評価の仕組み整備」を求めており、ここにAIによる異常検知を組み込むことが有効です。サプライチェーン全体のセキュリティ水準向上に向け、AIによる異常検知を推奨する記載を追加すべき。 ・理由 ガイドライン（案）では、サプライチェーンのセキュリティ水準向上が強調されている。 取引先やメールを介した攻撃が増加しており、従来のルールベース対策では検知が困難です。AIによる振る舞い検知は、ベンダー攻撃やBEC（ビジネスメール詐欺）を早期に発見し、サプライチェーン全体のリスク低減に寄与します。 ENISA（欧州ネットワーク情報セキュリティ庁）の「AI Threat Landscape 2025」では、AIが攻撃側にも防御側にも影響を与えており、BECやサプライチェーン攻撃の高度化に対抗するため、行動分析やAIベースの検知モデルが必須と指摘。 https://socket.dev/blog/enisa-s-2025-threat-landscape-ai-reshapes-cyber-attacks	ご意見ありがとうございます。 高度化するサイバー攻撃への対抗策として、AI技術を活用した異常検知が有効な選択肢の一つであると認識しております。 一方で、本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。技術の進展は速く、AI以外にも有効な検知技術が登場する可能性があります。そのため、特定の技術を推奨・指定することは避け、技術中立的な記述とすることが適切であると考えます。 したがいまして、原案通りの記載とさせていただきます。
	6	（意見⑥） ・該当箇所 第5章 5.4. 要求事項に対する取組例 （３）残続する脆弱性の速やかな対処 S(3)-2.3 セキュリティ勧告 ・意見内容 インシデント検知から隔離までの迅速な対応を標準要件として明記すべき。 ・理由 ガイドライン（案）では、迅速な対応が強調されている。 攻撃の検知から対応までの時間短縮は、事業継続性に直結します。AIによる自動対応は、数秒で隔離を実現し、被害拡大を防止します。これにより、企業のレジリエンス強化が可能となります。 ・理由 ➢IPAのサイバーセキュリティ経営ガイドライン Ver 3.0では、インシデント対応の迅速化が事業継続計画（BCP）の重要要素とされています。 ➢Gartnerにより、AIによる自動化がSOCの負荷を軽減し、インシデント対応のスピードを劇的に向上させることで、企業のレジリエンスを高めると指摘されています。	ご意見ありがとうございます。 インシデント検知後の迅速な対応や被害拡大防止措置の重要性については、深く認識しております。 ご意見を頂きました 要求事項S(3)-2.3は、脆弱性に関する情報を、利用者や供給先に適切に提供・開示することを目的とした項目です。ご指摘にある「検知から隔離までの対応」は、要求事項「S(3)-1.1等においてインシデント対応を含む脆弱性対応に関する体制を設置し、必要な役割、責務、プロセスを整備することを求めており、ご意見の趣旨である迅速な対応プロセスについては、これらの責務と個別要求の中で具体化されるべきものと考えます。 本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものとして検討を進めております。 したがいまして、原案通りの記載とさせていただきます。
17	1	１．ソフトウェアやサービス選定時のポイントについて ガイドライン案 P.97 の取組例において、ソフトウェア製品のセキュリティ実装に関する証明情報(SBOM、SSDF の実装適合性を証明する自己適合証明書など)を要求・確認することが示されている点は、極めて重要であると考えます。 この取り組みをより実効性のあるものとするため、「セキュリティ適合性評価制度(自己適合宣言や第三者認証を含む)」を、これらの証明情報を評価する際の有用な判断指標として位置づけることを提案いたします。	ご意見ありがとうございます。 実効性を高める観点から評価制度の重要性は認識しております。 いただいた御意見は、本ガイドラインおよび普及施策の検討を進める上で今後の参考といたします。
	2	２．重大なサイバーセキュリティ不具合やインシデント発生時の届出体制について 公的機関への報告義務がある場合、報告窓口が一元化されることが望ましいと考えます。しかしながら、現状ではインシデントの内容に応じて複数の機関への報告が必要となっており、事業者にとって負担となっています。 具体的には、以下のように報告先が分散しています。 (1) 個人情報漏えい → 個人情報保護委員会(PPC) (2) ウイルス感染・不正アクセス → 情報処理推進機構(IPA) (3) DDoS 攻撃など重大インシデント → 国家サイバー統括室(NCO) このような状況を改善するため、関係機関を横断した一括報告窓口の整備を検討いただくことを要望いたします。	ご意見ありがとうございます。 インシデント発生時における事業者の報告負担を軽減し、迅速な情報共有を図るための窓口一元化のついては、その重要性を認識しております。 しかしながら、本ガイドラインは、サイバーインフラ事業者及び顧客に求められる責務（基本理念に類する事項）を示すものであり、ご要望いただきました公的機関における一括報告窓口の整備といった行政側の体制や制度設計そのものについては、本ガイドラインの記述範囲を超える事項となります。 いただいたご意見は、今後のサイバーセキュリティ政策や関連制度のあり方を検討する上で参考といたします。
	3	３． ガイドラインの実効性確保について ガイドラインや制度が現場において形骸化することを防ぐため、定期的なガイドライン改訂の仕組みを設けていただくことを提案いたします。サイバーセキュリティを取り巻く環境は急速に変化しており、継続的な見直しと更新が不可欠であると考えます。	ご意見ありがとうございます。 サイバーセキュリティを取り巻く環境は変化が激しく、ガイドラインの内容を陳腐化させないことが実効性確保において重要であるとのご指摘、深く認識しております。 国内外の動向に合わせて適宜見直しを行うことを検討いたします。
18	1	（該当箇所：P.20-48） 本ガイドラインは、ソフトウェアサプライチェーンのサイバーセキュリティ強化、レジリエンス向上に向けて重要であり、本施策の主旨に賛同致します。本ガイドラインの目的を達するためには、各対象者がその役割や責務を認識することがまず重要と考えます。その点に関して、「2.2 責務」や「3.2 要求事項」において「サイバーインフラ事業者が認識すべき責務」が記載されていますが、「開発者」、「供給者」、「運用者」の何れの責務、要求事項なのか、それぞれ表3の分類に従い、「開発者」、「供給者」、「運用者」何れの責務、要求事項かを示していただくと、その対象がより誤解なく伝わると考えます。具体的には以下の箇所になります。 ・「2.2 責務」について「開発者」、「供給者」、「運用者」などの主語が明記されていない。 ・「3.2 要求事項」について、図中で複数ハイライトしている項目は対象がわかりづらい。主語も明記されていない。 →例えば、S(1)-4では、「開発者」と「運用者」がハイライトされており、各個別要求事項がどちらの要求事項なのか曖昧。 ・ ステークホルダ・対象に関する用語不統一の個所があります。（例：「利用者」と「顧客」、「開発者」と「ベンダー」など）	ご意見ありがとうございます。 ・役割について 本ガイドラインでは、対象とするソフトウェアの特性や契約形態等に応じて個別具体的に実際の開発・供給・運用における役割分担が決定されるべきものとして整理しております。ご指摘の「3.2 要求事項」において複数の役割をハイライトしている箇所につきましても、モニタリング可能な機能の実装と監視運用のように、複数の役割がそれぞれの立場から連携して取り組むことが求められる事項であることを意図しております。各個別要求事項に対して一律に特定の役割のみを主語として固定することは、多様なサプライチェーン形態における実務上の柔軟な適用を阻害することが懸念されるため、原案通りの記載とさせていただきます。 ・用語について 本ガイドラインでは、ソフトウェアライフサイクルの各フェーズや契約関係における文脈に応じ、その役割やニュアンスを表現するために意図的に使い分けています。 例えば、「顧客」は契約や調達の主体としての責務を強調する場合に、「利用者」はソフトウェアやサービスを実際に利用・操作する実態に着目した場合に使用しております。 これらを厳密に一つの用語に統一することは、かえって各場面における具体的な役割や責務の所在のニュアンスを損なう懸念があります。 上記の方針に基づき、再度確認を行い、必要な更新を行います。
	2	（該当箇所：P.20-22） 本ガイドラインは、ソフトウェアサプライチェーンのサイバーセキュリティ強化、レジリエンス向上に向けて重要であり、本施策の主旨に賛同致します。本ガイドラインの目的を達するためには、その責務の内容・範囲を対象者に正しく認識いただくことが重要です。そこで、p.22-22の「責務」ににおける抽象的な表現について、「責務」として何をどこまで求めているのかを具体的に示して頂くと、解釈のバラツキに起因した混乱、過大な負荷が抑えられると考えます。（p.20 「"最低限の"セキュリティソフトウェア標準」、p.21「"健全に"連携」、p.22「契約に基づく"協力的な"取り組み」、p.22「"合理的な"合意」） 例えば、「最低限のソフトウェアセキュリティ標準」では、その解釈によってはサイバーインフラ事業者に過大な負荷となることが懸念されます。そうならないように、「最低限のソフトウェアセキュリティ標準」に関する指針、考え方を提示いただけないでしょうか。	ご意見ありがとうございます。 「責務」の具体化による解釈のバラツキ防止の重要性について認識しております。 本ガイドラインは、サイバーインフラ事業者及び顧客が認識すべき「基本理念」や「大枠の方向性」を示すことを目的としております。そのため、包括的な表現を用いております。 一方で、ご指摘いただきました「具体的に何をどこまで求めるか」という点につきましては、第3章「3.2 要求事項」において具体的なアクションを規定しております。 実際の運用にあたっては、第3章および第4章の具体的な要求事項と照らし合わせて解釈いただくよう、ガイドライン全体の構成をご理解いただけますと幸いです。なお、今後整備予定の評価チェックリストではより具体的な判断ができるように配慮する予定です。 そのため、原案通りの記載とさせていただきます。

No.	御意見の内容	御意見に対する考え方
3	本ガイドラインは、ソフトウェアサプライチェーンのサイバーセキュリティ強化に向けて、顧客を含めて役割・責務を定めた点で画期的であると考えます。これがさらに実効性を持つようになるためには、予算確保にとどまらず、必要なコストを転嫁した価格で双方が積極的に価格交渉に応じ、円満に合意することも併せて必要であり、双方の重要な責務のひとつと考えます。（S(4)-2.3やS(6)-2.4で、開発者、顧客双方での予算確保が定められていますが、価格交渉については言及されていません）役割や責務に加えて、適切な価格交渉、負担についても、顧客、サイバーインフラ事業者双方が取り組めるよう何らかの指針を示していただけないしょうか。	ご意見ありがとうございます。 適切な価格交渉と合意形成が、双方の重要な責務であることについて、その重要性を認識しております。 本ガイドラインでは、健全な価格交渉の土台となる「相互理解」と「原資の確保」について、以下の通り規定しております。 事業者においては、「増加費用の明細と必要性に関する顧客への説明責任」について言及し、顧客に対しては、「リスク対応、及び関連する契約に係る予算を継続的に確保する」ことを求めています。 これらは、事業者がコストの根拠を示し、顧客がそれに応じる予算を持つという、適切な価格交渉を行うための前提条件を整えるものです。本ガイドラインとしては、これら責務の履行を通じて、実質的な価格交渉が促進されるものと考えております。 したがいまして、具体的な交渉指針の追加は行わず、原案通りとさせていただきます。
4	（該当箇所：P.22） P.30「S(1)-4 サービスのモニタリング」では、「利用ソフトウェアのモニタリングシステムの整備、及びモニタリングと評価の支援などは、ソフトウェア利用主体である顧客が実施するのが一般的である」と記載されています。このモニタリングが、顧客の責務のどこに対応するのか分かりづらいと思います。これは顧客の責務の「リスク管理」に含まれるものでしょうか。含まれるのでしたら、その旨の記載がある方が理解しやすいと思います。	ご意見ありがとうございます。 ご指摘の「モニタリング」が、顧客の責務のどこに対応するかという点について、分かりやすさが重要であるとのご指摘、理解いたします。 本ガイドラインでは、「モニタリング」は、顧客の責務である「リスク管理」および「ソフトウェア調達・運用」を実現するための具体的な活動として包含されているものと整理しており、いただいた御意見については、より具体的な取組内容に相当することから、原案のとおりとさせていただきます。
5	（該当箇所：P.30　3.2.要求事項（１）セキュアな設計・開発・供給・運用など） S(1)-4などで、「顧客が実施することが一般的な事項」と記載されているものについて、「顧客が実施すること」として個別要求に記載しなくてよいでしょうか。S(2)-3、S(3)-1、S(3)-3、S(4)-1、S(4)-3、S(4)-4も同様です。	ご意見ありがとうございます。 ご指摘の箇所における「顧客が実施するのが一般的である」といった記述は、当該要求事項においてサイバーインフラ事業者に求められている「支援」や「機能提供」が、どのような利用シーン等において必要となるかを説明するための背景情報として記載するもので、顧客への直接的な要求を意図したものではありません。 また、顧客自身が果たすべき責務については、S(6)の要求事項として整理しております。 従いまして、原案のとおりとさせていただきます。
6	（該当箇所：P.27　3.2.要求事項（１）セキュアな設計・開発・供給・運用） 「個別要求」として、ソフトウェアの開発者に対して「セキュリティ要件を定義する」ことが求めていますが、一方で、p.48 S(6)-2にも「セキュリティ要件を定義する」とあります。セキュリティ要件は顧客が定義するものと考えますので、p.27では、例えば「顧客から提示されたセキュリティ要件に基づき～」などを追加し、両者の関係性を明確にしていただきたいです。	ご意見ありがとうございます。 開発者と顧客の関係性におけるセキュリティ要件定義の整合性についてのご指摘、理解いたします。 本ガイドラインは、特定の顧客向けの受託開発だけでなく、不特定多数の利用者を想定したソフトウェア製品やクラウドサービスの開発も対象としております。後者の場合、特定の「顧客から提示された要件」が存在しない段階で設計・開発が進められるため、開発者自身が想定される脅威やリスクを分析し、自律的にセキュリティ要件を定義する必要があります。 一方、ご提案の記述を追加した場合、こうした製品・サービス開発において開発者が果たすべき要件定義の責務範囲が狭められて解釈される恐れがあります。 受託開発等の場合における顧客要件との整合性については、取組例（P.59）にある「顧客と合意すべきセキュリティ要件を全社ルールとして事前に定める」「ヒアリングを通じて適切なセキュリティ要件を合意する」といった記述で補完されていると考えますので、本文については原案通りの記載とさせていただきます。
7	（該当箇所：P.34　3.2.要求事項（２）ライフサイクル管理、透明性の確保） 「S(2)-3」で、「IT製品」とありますが、要求事項の中で「IT製品」となっているのはここだけで、他と用語が統一されていないようです。	ご意見ありがとうございます。 ご指摘の通り、「S(2)-3」においてのみ「IT製品」という用語が使用されており、ガイドライン全体での用語の統一が図られていないことを確認いたしました。 本ガイドラインはソフトウェアを対象としていることから、当該箇所の「IT製品」を、サードパーティ製ソフトウェアに修正し、用語の統一を図ります。
8	（該当箇所：P.34　3.2.要求事項（２）ライフサイクル管理、透明性の確保） 「S(2)-3.2」で、「サプライチェーンセキュリティ要件」とありますが、「サプライチェーンセキュリティ要件」の定義が必要だと思います。	ご意見ありがとうございます。 「サプライチェーンセキュリティ要件」の具体的な内容が分かりにくいとのご指摘、理解いたしました。 当該箇所（S(2)-3.2）の記述において、読み手が要件の範囲を具体的にイメージできるよう、具体的な例示を本文または注釈として追記し、サプライチェーン上で連鎖させるべき要件の内容を明確化いたします。
9	（該当箇所：P.38　3.2.要求事項（３）残続する脆弱性の速やかな対処） 「S(3)-3」で、「脆弱性に基づき、開発と運用のプロセスを見直す」とありますが、運用プロセスは、「脆弱性に基づき見直す」ものではなく、「根本原因に基づき見直す」ものではないでしょうか。	ご意見ありがとうございます。 当該箇所は、脆弱性を端緒として分析を行い、特定された根本原因に対処するという意図で記述しておりました。分析プロセスを経て得られた知見を活用する旨を明確化いたします。
10	（該当箇所：P.52　4.2. 役割分担に応じた要求事項の適用に関する注意点） どちらの要求パッケージを選択するかの判断は、「4.2. 役割分担に応じた要求事項の適用に関する注意点」で「サイバーインフラ事業者は、～求められる要求事項の達成度合い（要求パッケージの標準、最低限）を定め、～」とあることから、サイバーインフラ事業者で行うものと読み取れますが、達成度合いはサイバーインフラ事業者だけではなく、顧客と合意のもと行われるものではないでしょうか。	ご意見ありがとうございます。 要求パッケージの選択において、顧客との合意が重要であると認識しております。 本ガイドラインは、受託開発のみならず、不特定多数の顧客に提供されるソフトウェア製品やクラウドサービスも対象としております。こうした製品・サービスにおいては、事業者が自らの製品・サービスのセキュリティ水準（達成度合い）をあらかじめ仕様として「定め」、顧客がその水準を評価して選定・契約するというプロセスが一般的と考えます。個別の契約において合意が必要な場合は当然に含まれますが、ガイドラインの記述としては、多様な提供形態を包含するため、事業者が主体的に水準を決定するという現在の表現を維持し、原案通りとさせていただきます。
11	（該当箇所：P.89　5.4. 要求事項に対する取組例（４）人材・プロセス・技術の整備） AI関連のコラムの位置づけが不明確だと思います。p.80「S(4)-1.4 各役割のトレーニング」に言及があるように、積極的な導入を推進する意図でしょうか、もしくはリスクとして考慮することを期待してのものでしょうか。参考情報だとは思いますが、コラムの意図、位置づけをはっきりさせた方が正しく伝わると考えます。	ご意見ありがとうございます。 AI関連のコラムの意図や位置づけを明確にすべきとのご指摘、理解いたします。 当該コラムは、AI技術がソフトウェア開発の生産性を向上させるメリットと、不適切な利用がセキュリティ品質の低下を招く負の側面の両面を併せ持っている現状を示すことを意図しております。AI導入を一律に推奨するものでも、単なるリスクとして忌避すべきものとするものでもなく、事業者がこれらの両面を理解した上で、適切に活用・管理することを期待しております。 そのため、原案通りの記載とさせていただきます。

No.		御意見の内容	御意見に対する考え方
	12	表現・用語の統一などについてコメントさせていただきます。 ・P.27 「リスク情報」は他に合わせて「リスク」とした方がよいと思います。(「リスク情報」の記載はこの箇所のみ) ・P.27 「リスクへの適合性」とありますが、リスクは基準がありませんが、それに対する「適合性」との表現は適切でしょうか。 ・P.34 「リスク対処」は他に合わせて「リスク対応」とした方が良いと思います。(「リスク対処」の記載はこの箇所のみ) ・P.35 「ソフトウェアのセキュアな利用方法を保証するための情報～」について、「保証するもの」とは限らないと思いますので、「ソフトウェアをセキュアに利用するための情報」と一般化した表現の方がよいと思いますが、いかがでしょうか。 ・P.42 「セキュリティを確保(保障)する」とありますが、「確保」と「保障」は意味が違うと思います。「確保」が適切ではないでしょうか。 ・P.45 「サプライチェーン先」は「取引先」のことだと理解しました。そうであれば「取引先」とした方が伝わりやすいと思います。	ご意見ありがとうございます。 ・「リスク情報」 ご指摘の通り、S(1)-1.1で「リスクベースの分析・評価」を行っている文脈を受け、その結果である「リスク」そのものに対応するという表現に統一することで、文脈をより明確にします。 ・「リスクへの適合性」 ご指摘の通り、「リスク」は準拠すべき基準そのものではないため、「適合性」という表現は不適切です。リスクに対して適切に対処されているかを確認するという意図に合わせて修正します。 ・「リスク対処」 ガイドライン全体を通して一貫した表記に修正します。 ・「保証」 ご指摘の通り、情報提供のみで利用方法を「保証」することは困難であり、開発者が利用者に情報を提供してセキュアな利用を「支援する・可能にする」という文脈が適切であるため、表現を一般化します。 ・「セキュリティを確保(保障)する」 ご指摘の通り、確認基準のみで「保障」することは困難であり、表現を一般化します。 ・「サプライチェーン先」 「サプライチェーン先」という用語は一般的ではなく伝わりにくい可能性があるため、文脈に合わせて、より具体的で平易な表現に変更します。
19	1	1.本ガイドラインへの趣旨への賛同 (ア)AWSは、「サイバーインフラ事業者に求められる役割等に関するガイドライン（案）」において示されている日本政府によるサイバーセキュリティ強化政策を支持し、そこで示されているデジタル社会の安全・安心な発展に向けた取り組みに賛同します。 (イ)近年のサイバー攻撃の高度化・巧妙化に対応するため、政府が主導してサイバーインフラ事業者の役割を明確化し、包括的なセキュリティ対策の推進を図る本ガイドラインの策定は重要な意義を持つと考えます。 2.階層化責任フレームワークへの賛同 (ア)本ガイドラインが採用している階層化された責任フレームワークと責任共有モデルに基づくアプローチについて、賛同いたします。開発者・供給者・運用者の3つの役割を明確に定義し、各レイヤーにおける責任を体系的に整理したことで、現代のクラウドコンピューティング環境における複雑なセキュリティ課題に対する実効性のある解決策が提示されていると考えます。 (イ)特に、サービスタイプに応じて差別化された義務レベルを設定している点は、技術的現実と運用実態を適切に反映した合理的なアプローチであり、実際のコンプライアンス実装において高い実用性を持つものと考えます。 (ウ)この責任共有モデルは、クラウドサービスの本質的特性である多層アーキテクチャと複数ステークホルダー間の協調を適切に認識しており、効果的なサイバーセキュリティ実現のための基盤として機能するものと期待しております。 3.SBOM要件に関する懸念と配慮要請 (ア)しかしながら、ガイドライン案が事業者側に情報開示義務を課している一方で、利用者側の責任が不十分に定義されていることを懸念します。ガイドラインP.1で挙げられた3つの事例のうち2つ（ソフトウェアベンダーA社の事件とB病院の事例）は、サプライチェーン攻撃の問題ではなく、利用者側の選定ミスや使い方の問題といえるのではないでしょうか。 (イ)クラウドサービス利用形態はNIST SP800-145でのIaaS/PaaS/SaaSの定義では対応しきれない状況が生じています。利用規約やサービス条件で既に必要な情報は提供されているため、追加の情報開示要求は過剰ではないかと考えます。 (ウ)ソフトウェア部品表（SBOM）の過度な提供義務については、クラウドサービスプロバイダーにとって技術的・経済的負担が過大となる重大な懸念があります。 (エ)現代のクラウドサービスは、数千から数万のソフトウェアコンポーネントで構成されており、直接依存だけでなく、推移的依存（transitive dependencies）まで含めると、単一のサービスで数万の依存関係が存在する場合があり、それらは多層的かつ動的に変化します。また、共有インフラ上で複数の顧客サービスが稼働するマルチテナント環境では、顧客ごとに異なるSBOMを生成・管理する必要があり、運用負荷が指数関数的に増大します。各コンポーネントの出所情報、バージョン、ライセンス、依存関係を正確に把握し、リアルタイムで更新・維持するには、SBOM生成ツールの導入・運用、専門人材の確保・育成、継続的な検証・更新プロセスの構築、顧客への提供・問い合わせ対応など、多大な投資が必要です。こうしたコストは特に中小規模CSPにとって事業継続を脅かす水準となる可能性があります。 (オ)ガイドライン案では「必要に応じてSBOMを提出する」といった曖昧な表現にとどまり、提供範囲や詳細度が明示されておらず、事業者間の対応のばらつきや法令違反リスクが懸念されます。 (カ)詳細なSBOM情報は攻撃者に有益な情報を提供するリスクがあり、機密性の高い技術情報として厳格な管理が必要です。使用ソフトウェアの具体的バージョン情報による既知脆弱性を持つコンポーネントの特定、攻撃経路分析に必要な依存関係情報の開示、標的攻撃を促進する可能性がある詳細なシステム情報の提供はリスクを増大させます。こうした情報は攻撃者が既知の脆弱性を持つ特定のソフトウェアバージョンを特定し、依存関係を理解し、開示されたアーキテクチャ情報に基づいて標的化された悪用戦略を開発することが可能になる懸念があります。SBOMは機密性の高い技術情報であり、その管理にはアクセス制御の厳格化、情報漏洩対策、第三者提供時の契約管理といった対策が必要です。事業者が内部でセキュリティ情報を管理することには賛成ですが、外部への公表・届出は効果が低いのではないでしょうか。 4.具体的な改善提案 (ア)上記の懸念を踏まえ、以下の対応を提案いたします。 (イ)まず、提供範囲・詳細度の明確化として、SBOMに含めるべき情報の具体的範囲（直接依存のみか、推移的依存を含むか）の明示、詳細度のレベル（パッケージ名とバージョンのみか、ライセンス情報や依存関係図の提供要否）の明確化、更新頻度の基準（メジャーバージョンアップ時のみか、パッチ適用時も含むか）の設定が必要です。 (ウ)また段階的導入として、初期段階では主要コンポーネントのみを対象とした簡易版SBOMから開始する段階的実装をおこなうこと、業界標準フォーマット（SPDX、CycloneDX等）の推奨と統一をすること、自動化ツール活用に関するベストプラクティスの提示と技術支援することを提案いたします。 (エ)そして、事業規模・サービス特性に応じた柔軟な対応が必要であり、中小規模CSPへの配慮（猶予期間の設定、技術支援措置、段階的要件適用）、マネージドサービス、SaaS、IaaSなどサービス形態に応じた要件の差別化、リスクベースアプローチによる重要度に応じた要件の調整が検討されるべきです。 (オ)またセキュリティへの配慮とリスク管理として、SBOM情報の取扱いに関するセキュリティガイドラインの策定、必要最小限の情報提供原則の明確化、情報開示範囲の適切な制限と機密性保護措置が必要です。 (カ)SBOM生成とメンテナンスに費やされるリソースは、セキュア・バイ・デフォルト構成の強化、包括的な使用ガイダンスと顧客サポートの充実、迅速な脆弱性対応システムの構築、直接的な顧客運用サポートの向上といった実用的なセキュリティ措置により効果的に配分される可能性があります。これらの代替アプローチは、透明性目標を達成しながら実装負担を削減し、より実用的なセキュリティ改善をもたらす可能性があります。 (キ)P.21の「顧客に求められる責務」に、適切なソフトウェア・サービスの選定と使い方を採択する責任を記載することが必要です。事業者が提供する情報をもとにソフトウェアやサービスを選定・変更する最終責任は利用者にあるため、顧客の責任範囲をより広く再定義することも必要です。 5.結語と継続的協力の意思表明 (ア)SBOM提供の重要性は十分理解しておりますが、現状のガイドライン案では提供範囲・詳細度が不明確であり、CSPの技術的・経済的負担が過大となる懸念があります。実効性のある制度とするため、上記提案を踏まえた要件の明確化と段階的導入を強く要望いたします。 (イ)AWSといたしましては、日本のサイバーセキュリティ強化という重要な政策目標の実現に向け、政府との建設的な対話を継続し、技術的専門知識を活用した実用的で効果的な実装アプローチの構築に積極的に協力してまいります。また、業界全体のセキュリティ向上に向けた取り組みにも引き続き貢献していく所存です。 (ウ)本ガイドラインが、日本のデジタル社会の安全・安心な発展に寄与する実効性の高い制度として確立されることを期待し、その実現に向けて最大限の協力をお約束いたします。	ご意見をいただき、ありがとうございます。 クラウドサービスの多層的な構造や運用実態において、詳細なSBOMの提供が一律に義務付けられた場合、技術的・経済的な負担が過大となる懸念については深く理解いたします。また、SBOM情報が攻撃者に悪用されるリスクへの配慮が必要である点もご指摘の通りです。 本ガイドラインは、SBOMの提供そのものを自己目的化しているのではなく、サプライチェーンを通じた透明性の確保とリスク管理の実効性を高めることを目的としております。 必ずしもソースコードやSBOMそのものを納品・流通させることだけを手段とはしておらず、供給者が内部で厳格に管理し、脆弱性が発見された際に迅速に通知・対処する体制が契約等で担保されていれば、それが「セキュアなソフトウェア流通の仕組み」として認められる余地を持たせております。 一律の詳細規定を設けることは、クラウドサービスのような動的な環境における柔軟な対応を阻害する恐れがあるため、原案通りの記述とし、具体的な提供内容は各事業者間の契約やリスク評価に基づいて決定されるべきものと考えます。 また、セキュリティ確保において、事業者だけでなく、利用者（顧客）側が適切な選定や利用を行う責任が重要であるとのご指摘、強く賛同いたします。 この点につきましては、個別要求S(6)において、顧客の主体的な取組と意思決定の責務を規定しております。 したがって、ご意見の趣旨は現在の記述に十分に反映されているものと考え、原案通りとさせていただきます。

No.		御意見の内容	御意見に対する考え方
20	1	1. はじめに：本ガイドライン（案）の目的と課題意識 本ガイドライン（案）は、ソフトウェアのライフサイクル全体におけるサイバーセキュリティ確保とレジリエンス向上を目指すものであり、特にサイバーインフラ事業者（クラウドサービスプロバイダ等を含む）と顧客の間で適切な役割分担と責務のあり方を整理・解説するという目的を在日米国商工会議所（ACCJ）は高く評価します。 クラウドサービスは、一般的に責任共有の考え方に基づいて成り立っており、セキュリティリスクの増大に対応するためには、この責任分界点を明確にし、各主体がそれぞれの責務を効率的かつ効果的に果たすことが不可欠です。 ACCJは、この指針の方向性を支持しつつ、クラウドサービス事業者がその役割を最大限に発揮し、顧客のセキュリティ体制を効果的にサポートするための観点から、以下のコメントを提出します。 2. 賛同する主要な点：責任共有と顧客責務の明確化 (1) 責任共有モデルの明確化への賛同 本ガイドライン（案）が、事業者と顧客が互いの役割を認識し、正確な情報を共有して対策を共に講じることで、サイバー攻撃への対応力強化につながるという基本的な考え方を明確に示している点に賛同します。 クラウドサービスにおいては、運用の責任を分担・共有することが一般的です。（例えば、サービスプロバイダがインフラ上に構築したシステムの運用を担当し、サービスの利用者がアプリケーションの運用を担当するなど）。 この責任分界点を契約やポリシーによって明確に定めることは、事業運営の透明性と、インシデント発生時の迅速な対応のために極めて重要です。 (2) 顧客側（利用者）の主体的なリスク管理と予算確保（S(6)の評価） 顧客側に対して、経営層のリーダーシップによる主体的なリスク管理（S(6)-1）と、適切な予算の継続的な確保（S(6)-2.4）を責務として求めている点を強く支持します。 セキュリティ対策に伴うコストは、ソフトウェアサプライチェーンにおいて組み込まれる価値に対する対価であり、顧客側によるリスク管理に対する主体的な取組みと、それに伴う費用（リソース）の確保も不可欠であるという共通認識を促すことは、健全なセキュリティ市場の形成に資すると考えます。 3. 運用の課題と改善提案：責任分界点の明確化とサポートの最適化 本ガイドライン（案）の実効性を高めるためには、クラウドサービス特有の多層的な構造を踏まえ、責任分界点を厳格に定義し、事業者の役割を顧客サポートに最適化することが肝要です。 (1) 多層的なサプライチェーンにおける責任分界点の厳格な定義（S(2)-3.1, S(4)-3 関連） クラウドサービスは、IaaS/PaaSを提供するインフラ事業者、その上でSaaSを提供するサービスプロバイダ、そしてその利用者（顧客）が多層的に関わる複雑な構造をもちます。 ● 契約による役割の明確化: 責任共有モデルに基づき、顧客が主体的に運用する範囲、サービスプロバイダに委ねる運用責任の一部、およびこれらの分界点を契約（利用規約とSLA）で明確に定める重要性をガイドラインにおいてさらに強調すべきです。 ● 運用ポリシーの活用: 運用者となるサイバーインフラ事業者（クラウド事業者）は、顧客との契約に基づき運用支援を実施する場合に、ソフトウェアを適用したサービス運用ポリシーを明確に定義し維持すること（S(4)-3.1）が必要です。これにより、顧客側も、インフラ事業者によるサービス運用インフラの保護範囲を明確に把握でき、顧客として要求事項を満たすための運用を円滑に行うことができます。 (2) ソフトウェア部品表（SBOM）の義務化に関する慎重な検討の要望（S(2)-2.3 関連） 本ガイドライン（案）では、利用者による脆弱性対策のため、SBOMの段階的な採用などを通じた構成情報の共有（S(2)-2.3）が求められています。しかしながら、パブリッククラウド事業者の視点を踏まえると、SBOMの共有を必須の要求事項とすることについては、現時点では時期尚早であるというのがACCJの見解です。 ● コストと実効性の課題: SBOMの生成、維持、共有には、相応の工数とコストが発生します。また、SBOMを本格的に組織間で共有するためには、情報の範囲、フォーマット、およびソースコードの法的権利保護に関する統一的なルール整備が不可欠であり、現状、その成熟度は不十分です。 ● 顧客サポートの最適化: 顧客がSBOMを真に活用できる体制を整えるには、さらなるリソース整備が必要です。それよりも、クラウド事業者は、脆弱性が管理されたソフトウェア（バイナリやサービス）が流通する標準的な仕組みの構築と、迅速なサポート体制の最適化に注力すべきです。 (3) 顧客のセキュアな利用を最適化する情報提供（S(2)-4, S(3)の強化） SBOMのような詳細な構成情報の共有を必須としない代替として、クラウド事業者は、顧客のセキュリティ態勢向上に直結する実用的なサポートに特化すべきです。 ● セキュアな利用ガイダンスの徹底（S(2)-4）：ソフトウェアをセキュアに導入・設定・操作するための情報を提供することで、顧客の設定ミスなどのリスクを低減させることが期待できます。クラウド事業者は、セキュアなデフォルト設定の実装と、それを補完するわかりやすい構成ガイドを継続的に提供することにリソースを集中すべきです。 ● 残存脆弱性への迅速かつ効率的な対処（S(3)）：開発者は、脆弱性開示ポリシーを整え、パッチの開発と配布、顧客への確実な通知の仕組みを整える責務を有しています。クラウド事業者は、検知した脆弱性に対し、リスク対応を迅速に計画し実装すること（S(3)-2.2）に特化し、顧客の運用部門がセキュリティ勧告に従った配備を遅滞なく実施できるよう支援体制を最適化すべきです。 4. 結論 本ガイドライン（案）が提唱する「セキュアバイデザイン」と「責任共有」の理念は、日本のサイバーレジリエンス向上に不可欠です。 ACCJは、契約に基づく責任分界点の明確化、セキュアな利用に関するガイダンスへの注力、および迅速な脆弱性対応を通じて、パブリッククラウド事業者を含むステークホルダーが顧客のセキュリティ確保を最適化できる環境づくりに、建設的な提言を通じて貢献していく所存です。SBOMのような運用上の負担が大きい要求事項については、その実効性について引き続き慎重な議論が必要であり、まずは顧客の運用負担軽減に直結するサポート体制の強化を優先することを提案します。	ご意見をいただき、ありがとうございます。 クラウドサービスの多層的な構造における責任分界点の明確化、及びSBOM提供に伴う技術的・経済的な課題に関するご指摘、深く理解いたします。 本ガイドラインは、SBOMの提供そのものを自己目的化しているのではなく、サプライチェーンを通じた透明性の確保とリスク管理の実効性を高めることを目的としております。 ご指摘のSBOM（S(2)-2.3）につきましては、本文中で「段階的な採用などを通じて」と記述しており、一足飛びの義務化を求めるものではありません。供給者が内部で厳格に管理し、脆弱性が発見された際に迅速に対処する体制が契約等で担保されていれば、それが「セキュアなソフトウェア流通の仕組み」として認められる余地を持たせております。 したがって、本ガイドラインは、ご提案いただいた「脆弱性が管理されたソフトウェアが流通する仕組み」や「契約による責任分界点の明確化」を否定するものではなく、むしろ推奨する枠組みとなっております。 各事業者間の契約やリスク評価に基づいて最適な手段が決定されるべきという考えに基づき、原案通りの記述とさせていただきます。