「サイバー・フィジカル・セキュリティ対策フレームワーク(案)」のパブリックコメントで寄せられた御意見に対する考え方

NO		提出者(種別)	該当箇所	御意見	御意見に対する考え方
	1-1	法人	まえがき	「また、「Connected Industries」～増大させることになるが、」の部分を削除する。 【理由】 「柔軟で動的なサプライチェーンの構成」と「新たな付加価値を生み出す機会の増大」の関連がわかりにくい。Connected Industriesの説明資料には上記関連に関する直接的な記述は無い。むしろ、この一文を削除した方が、後半のサイバーセキュリティ対策の必要性に関する記述と素直につながるので、わかりやすくなる。 （参考資料）「Connected Industries」東京イニシアチブ2017、経済産業省、H29年10月2日	いただいた御意見を踏まえ、全体構成などの見直しも含めてまえがきを修正いたします。
	1-2	法人	第1章	1.1項に文章で記載している内容を、「概要」として、ポイントを簡潔に記載するようにまとめて、1.1項の前に入れるよう、構成を変更する。 【理由】 全体の流れ・目的・メリットがわかりにくい。 また、１．１項の説明文の論理展開に飛躍が多く、支離滅裂に感じられる部分が多い。「新たな付加価値」の部分を強調しているが、「生産性の向上」や「社会課題の解決」などConnected Industriesの説明資料に記述されている要素についても触れた方が理解しやすくなる。文中の細かな修正意見は以下の別項目に記載します。	いただいた御意見を踏まえ、全体構成などの見直しも含めて記載内容の修正を検討いたします。
	1-3	法人	第1章	「様々なつながりによる新たな付加価値を創出する「Connected Industriesの実現」」の部分を下記の表現に変更する。 「様々なつながりにより、新たな付加価値の創出・生産性の向上・社会課題の解決に寄与する「Connected Industriesの実現」」 【理由】 Connected Industriesの目的は、新たな付加価値創出だけではないので、間違って伝わらないように併記する方が良い。	いただいた御意見を踏まえ、全体構成などの見直しも含めて第1章を修正いたします。
	1-4	法人	第1章	「企業を中心に付加価値を創造するための一連の活動であるサプライチェーンも」の部分を以下の表現に変更する。 「従来のものづくりを中心としたサプライチェーンから、新たな付加価値を創造するバリューチェーンへと、」 【理由】 後の文章で「その姿を変えることになる」と書いているので、前段の文章では従来の狭義のサプライチェーンで説明した方が、論旨がすっきりとするため。	いただいた御意見を踏まえ、全体構成などの見直しも含めて第1章を修正いたします。
	1-5	法人	第1章	従来型のサプライチェーンとSociety5.0のサプライチェーンの違いについて、下記の説明文を追加する。 従来型のサプライチェーン：調達～製造までのモノづくり Society5.0のサプライチェーン：企画～サービス提供まで全てを含むバリューチェーン 【理由】 従来型のサプライチェーンと、Society5.0のサプライチェーンを同じ言葉で表現しているので説明文がわかりにくくなっているため。 また、NIST SP800-161で言及しているサプライチェーンは、IoT機器の部品・ソフトウェアのサプライヤ経由で侵入してくるマルウェアなど、従来型のサプライチェーンの部分への対策を主に着目しており、新たな付加価値との関連は薄いように思われる。 （参考資料）　米国のサプライチェーンのセキュリティ対策（３）　防衛取得研究（第八巻　第三号）防衛基盤整備協会　客員研究員　横山恭三氏 https://ssl.bsk-z.or.jp/kakusyu/pdf/26.12sapuraiche-nnhp.pdf	いただいた御意見を踏まえ、全体構成などの見直しも含めて第1章を修正いたします。
	1-6	法人	第3章 L1.001～ L1.008 L1.010 L1.013	「サイバーセキュリティマネジメントシステム（CSMS）」を以下の表現に変更する。 「産業用制御システムのサイバーセキュリティマネジメントシステム（CSMS）」 【理由】 CSMSは産業用オートメーションと制御システムが対象。110頁の用語集(2)にその旨記載があるものの、本文を見た時にCSMSがISMSのように広範囲に適用できるものと誤解を受けやすい。	いただいた御意見を踏まえ、制御システムを対象としたものと容易に理解できるよう、修正いたします。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
1	1-7	法人	第3章 L1.002	「サイバー保険活用する。」を「サイバー保険を活用する。」に変更する。 【理由】 エディトリアルな修正	いただいた御意見のとおり、修正いたします。
	1-8	法人	第3章 L2.002	「セキュリティ対策を考慮していないIoT機器を利用する。」を以下の表現に変更する。 「機器事業者が、セキュリティ対策は利用者側のネットワークで対策すべき課題と考える。」 【理由】 元の表現は利用者側の視点で書いている。セキュリティバイデザインはIoT機器を提供する事業者が、企画・設計段階でセキュリティリスクを考慮する行為なので、ここは機器を提供する事業者側の視点で書かれていないとおかしい。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	1-9	法人	第3章 L2.003	「機能安全を考慮した」　を　「安全性を考慮した」　に変更する。 【理由】 多くの機器の安全規格のベースとなっているIEC規格では、「機能安全」とは、電子制御装置（コントローラ、ソフトウェアなど）の保護機能・安全機能が正常動作することで製品の安全を担保する場合の、該当部分を指している。機械的な保護装置で機器の安全（一般に、発煙・発火・感電・傷害などが起こらない状態）が保てる場合は、機能安全を採用する必要が無い。 元の表現では、機能安全に頼る必要が無い機器が、危険なものであるという誤解を受ける。 （参考資料）　JIS C0508-4（IEC 61508-4規格の整合規格）における、機能安全の定義。 3.1.12 機能安全（functional safety） EUC及び EUC 制御系の全体に関する安全の うち，E/E/PE 安全関連系及び他リスク軽減 措置の正常な機能に依存する部分。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	1-10	法人	第3章 L2.012	「現場のIoT機器において、定期的に（起動時等）に、ウィルスチェックを行うことで、マルウェア感染被害を防ぐ」 の次に、下記の文章を追加する。 「IoT機器を提供する事業者においては、部品・ソフトウェアのサプライチェーンを通じて感染することがないよう、サプライチェーンのセキュリティ対策を実施する」 【理由】 組込みシステムでは、ウィルスチェックが可能なOSを使っているとは限らない。こういった場合は、機器・サービスのソフトウェアを開発～提供するプロセスにおけるサプライチェーンのサイバーセキュリティ対策でカバーすべき。	いただいた御意見を踏まえ、実施が望ましいけれども対策の実施が可能ではない場合があるものについては、「可能な場合」あるいは「することが望ましい」と追記するなど記載内容の修正を検討いたします。また、部品・ソフトウェアのサプライチェーンにおけるセキュリティの考慮については、L2.001～L2.004に記載しています。
	1-11	法人	第3章 L2.013	「IoT機器が不正に操作される。」 を下記の表現に変更する。 「開発時に発見できなかった脆弱性により、IoT機器が不正に操作される。」 【理由】 元の表現は、脆弱性対策の為にセキュリティパッチが必要になる要因を表現できていない。	いただいた御意見を踏まえ、修正いたします。
	1-12	法人	第3章 L2.015	「レビューする。。」　を　「レビューする。」　に変更する。 【理由】 エディトリアルな修正。	いただいた御意見のとおり、修正いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	1-13	法人	第3章 L2.019 L3.021	「Bluetooth等による無線接続の制限」 を下記の表現に変更する。 「Buletoothや無線LAN等による無線接続の制限」 【理由】 Bluetoothだけを特段強調する必要はなく、無線LANも同列の扱いにしておくべき。	いただいた御意見を踏まえ、修正いたします。
	1-14	法人	第3章 L2.020	IoT機器の稼働情報等を集中管理する仕組みの例として、現在TTCで取り組まれているホームネットワーク接続構成特定プトロコルの実証及び各IoT機器への実装を推奨する政策支援を期待します。 （規格名）　（一社）情報通信技術委員会　JJ.300.00　ホームNW接続構成特定プロトコル ITU-T G.9973として国際標準化済み 【理由】 本項目の要求を満たす具体的なプロトコルはあまり例が無く、本プロトコルの実用化・普及を促進するのが効果的と思われるため。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
2	2-1	法人	全体	サイバーフィジカルシステムによるスマート社会の実現に向けて、今回のフレームワークの策定は、我が国産業技術の先進性と、国際貢献へ取組みの一環性を進展させるたいへん意義ある施策と存じます。	本フレームワークに対する肯定的な御意見として承ります。
	2-2	法人	付録C	本フレームワークの用語の一部について、極力独自の定義は避け、特に理由がない限り、国際標準規格や日本工業規格に従うことが望ましいと考えます。また、国際標準規格に類似する用語があり、かつ定義が異なる場合には、用語集でその違いと定義の理由を説明することが望ましいと考えます。本フレームワークが目指すグローバルハーモナイゼーションの実現には、まず用語定義の混乱を避けることが重要と考えるためです。 一例として、第３章の「L1.001 セキュリティポリシーの策定、体制の整備」に出現する「セキュリティポリシー」を挙げます。「付録C 用語集（29）」で、「セキュリティポリシー」は「自組織や、関係者における役割と責任、情報の共有方法等を明確に定めたもの」と記述されています。 一方、ISO/IEC 27000には、「2.60 方針（policy）」が「トップマネジメントによって正式に表明された組織の意図及び方向付け」と記述されています。また、ISO/IEC 27001には、より詳細な定義がされています。このように、定義が異なります。	いただいた御意見を踏まえ、JISやISO/IECが発行する規格などを参考に用語の定義を修正いたします。
	2-3	法人	付録B	本フレームワークでは「Society5.0」における全産業に共通的なセキュリティ対策を示すとされています。であれば、少なくとも直近のビジネスへの影響が大きいと考えられるサプライチェーンセキュリティとプライバシー保護について、参照を追加すべきかと存じます。 具体的には、本フレームワークの比較対象規格として、"ISO/IEC 27001"と並んで"NIST SP800-171"が挙げられています。SP800-171は、CUI（Controlled Unclassified Information）の機密性を守るための推奨要件を表す規格であり適用対象は限定的です。比較対象規格としては、完全性や可用性を含む、より一般的な管理策集である"NIST SP800-53"を挙げることが適切と考えます。また、本フレームワークで「Society 5.0」におけるサプライチェーンを広く取り上げるのであれば、CUIに限定されない一般製品向けの規格である"ISO/IEC 27036"や"NIST SP800-161"も、比較対象に挙げることが望ましいと考えます。 さらに、2018年５月25日に施行が予定されており、関係企業の大きな懸念となっているEUの一般データ保護規則GDPRについて、言及があることが望まれます。その関連で、プライバシー改善を盛り込んだ"NIST SP800-53 Rev.5 (draft)"に言及することも有意義と思われます。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO/IEC 27036やNIST SP800-161などその他の国際規格等との比較やGDPRとの関係に関しては、その内容を確認しつつ適切な対応を検討いたします。
	2-4	法人	第2章	本フレームワークの第２章「2.2. フレームワークの構成」に、「企業間のつながり（従来型サプライチェーン）【第１層】」との記述があります。この「従来型サプライチェーン」の語が指し示す対象に関して、誤解が生じる懸念があります。 すでに従来、多種多様なサプライチェーンが構築されています。「従来型サプライチェーン」に替えて、「モノの取引に伴う古典的サプライチェーン」のように記述すれば、素直に読みやすくなるのではないかと考えます。	いただいた御意見を踏まえ、全体構成などの見直しも含めて記載内容の修正を検討いたします。
	2-5	法人	第3章 L1.012	第１層の「L1.012プライバシー保護」には、国際的な基本原則「OECD８原則」に対する参照と対応の必要性が記述されています。「OECD８原則」は日米欧で既に理念としては採用済みです。本記述だけではこれから何をしてよいか分かりにくく、不十分であると考えます。例えば、前述のGDPRに関して、早急に対応する必要性があるのか、あるいは、どのような産業分野、条件においてどう考えられるのかの検討にも有用な記述になっていることが望ましいと考えます。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。また、GDPRとの関係に関しては、その内容を確認しつつ適切な対応を検討いたします。
	2-6	法人	第3章	各対策項目を、対策内容の類似性や従属性の観点で見直して、対策項目を必要最小限にして頂くことが望ましいと考えます。 具体例として、「L2.001」、「L2.002」、「L2.003」を挙げます。これらの対策例は「■対策ポイント」と「■構成要素毎の対策例」の記述内容が類似しています。一つの対策に纏めるか、或いは各対策の違いが明確になるように記述頂くことが望ましいと考えます。	いただいた御意見を踏まえ、類似の対策項目を可能な限り統合するなど全体構成などの見直しも含めて記載内容の修正を検討いたします。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
	2-7	法人	第3章	対策例の記述範囲を、対策主題に直接関連性のある範囲に限定すること、内容の整合性を保つことが望ましいと考えます。 記述範囲の例：「L2.020」の「○組織」に、「ネットワーク分離」の記述があります。ネットワーク分離は、「集中管理」を実装要件の一つですが、対策主題である「集中管理」と関係が薄いと思われます。ネットワークを介した不正アクセスの防止については、「L2.017」が挙げられており、その記述で十分ではないでしょうか。逆に「L2.020」で、ネットワーク分離の要件を記述する必要があれば、「■対策ポイント」にもその必要性を記述することが望ましいと考えます。 記述の整合性の例：「L2.020」の「○システム」に、ユーザーIDの採番が挙げられています。しかし、「○組織」や「○ヒト」には、これに対応する記述がありません。例えば「○組織」には「IoT機器の利用手順および管理手順を定める」と「IoT機器の管理手順に従い、各機器に利用者及びユーザーIDを割り当てる」、「○ヒト」には「IoT機器の利用手順に従い、ユーザー認証処理を実施する」等の記述が必要と思います。	いただいた御意見を踏まえ、構成要素ごとの対策を見直すなど全体構成などの見直しも含めて記載内容の修正を検討いたします。
	2-8	法人	第3章 L3.002 付録B	比較対象規格の「Subcategory ID」の内容が、第３章の対策例の内容と整合していない箇所があります。 具体的に「L3.002 耐タンパーデバイスを利用したIoT機器、サーバ等の導入」で、比較対象規格ISO/IEC 27001に「A.7.1.1, A.7.1.2, A.7.3.1」が挙げられています。同規格のA.7は「人的資源のセキュリティ」で、「A.7.1.1 選考」は「管理策　全ての従業員候補者についての経歴などの確認は，関連する法令，規制及び倫理に従って行わなければならない。また，この確認は，（中略）リスクに応じて行わなければならない。」とあります。L3.002」の「■対策の概要」「■対策ポイント」「■構成要素毎の対策例」には、このA.7.1.1に対応する対策の記述がありません。 逆に、「L3.002耐タンパーデバイスを利用したIoT機器、サーバ等の導入」には、ISO/IEC 27001「A.10 暗号」の管理策の記述がありませんが、必要ないでしょうか。 「付録B」は、他の標準規格との相互運用性を高め、本フレームワークが目標とするグローバルハーモナイゼーションを実現するために、必須かつ重要な情報であると考えます。それ故に、記述内容の正確性を確保し、最新情報に従って随時更新を図ることが必要と考えます。	いただいた御意見を踏まえ、付録Bについて再度確認し記載内容の修正を検討いたします。
	2-9	法人	全体	NISTのSP800-53やISO/IEC 27002は大部な仕様です。グローバルハーモナイゼーションの実現には、人手による突き合わせやチェックでは限界があると認識しています。標準規格および仕様分析業務の一部機械化、分析支援ツールの開発と民間での活用サービス支援等が進められることを期待します。cf. NISTのSCAP、OSCAL開発。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	2-10	法人	全体	本フレームワークの利用の仕方について、今後ガイドラインやベストプラクティスの発行、講習会やカンファレンス開催などの利活用を推進する施策の実施が期待されます。 NIST CSFの存在価値に、米国の政府機関のみならず広く産業界の事業者が、各自のサイバーセキュリティの取り組みを分析し、目標達成に向けたセキュリティ計画の検討に活用している点が挙げられます。NISTは、製造業向けに”NISTIR 8183”を発行し、”Cybersecurity Framework Workshop 2017”を開催するなど、普及支援を積極的に実施しています。本フレームワークが、内外の官民両分野の事業者に参照され、活用される仕様となるために、補足資料や関係資料の発行および普及施策の積極的な実施が期待されます。	いただいた御意見を踏まえ、本フレームワークが広く活用されるように、産業分野別での実装化へ向けた取組の促進、セミナーの開催等を実施してまいります。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	3-1	法人	全体	●費用に関する分析結果 サイバー・フィジカル・セキュリティ対策フレームワークについて、その57項目を中小企業が満たすためのシステムを構築するための見積もりを試算した。 ※前提 従業員数:300人(企業規模において中小企業を示す人員数の上限) 企業が保有するIoT機器:600台(Cisco社が2010年に試算した所有IoT機器1.8～2台/人を利用) その結果、総額約6.9億円を要することが判明した。内訳は以下。 L1 （企業間のつながり）：約1.3億円 L2 （フィジカル空間とサイバー空間のつながり）：約3.4億円 L3（サイバー空間におけるつながり）：約2.2億円 合計：約6.9億円 これに対し本フレームワークよりも厳格度が高いSP800-171（110項目）の約3倍のコントロール数であるSP800-53（325項目）の準拠に要する費用は平均3億円であるとされている。 ●高額化の要因 ・同じような対策を3階層で複数にわたって要求している ・要求レベルが中途半端であるが実現するには高機能な製品を導入せざるを得ない ・既存技術では実現不可能とも思われる実装が存在する（L3.010、L3.011等） 当研究所からは国際標準になる可能性が極めて高く、米国だけでなく欧州でも有効性が認められ始めているNIST SP800-171よりも対応コストが2倍以上もかかり、それでいてセキュリティが低くなってしまう経産省の今回のフレームワークは、再検討が必要と考える。 コスト低減策とセキュリティの強度を高めるたために専門家の意見をもっと取り入れて再検討することを提案する。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-2	法人	第3章	・アクセス制御 アカウントライフサイクルに沿った管理を規定できていない。さらに、アカウントタイプも特権と非特権の二種類のみで不足であり、最小特権や責務の分離を用いた対策も示せておらず、NISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-3	法人	第3章	・意識と訓練 各ユーザの責任や役割に基づいて、適した内容を設計しなければ、有効にセキュリティ意識を向上できず内部犯行を考慮できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
3	3-4	法人	第3章	・監査と責任追跡性 監査行為をセキュリティ向上に活用することを意図していない。監査対象とするセキュリティイベントの定義から実装の確認、そして監査レコードの分析とレビュー、さらには監査機能やレコード自体のセキュリティまで言及できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-5	法人	第3章	・構成管理 資産管理・構成管理の構築のみの規定であり、そこにセキュリティ強化という目的で構成設定と機能最小化を要求できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-6	法人	第3章	・識別と認証 全ユーザに多要素認証を要求し、セキュリティ的に脆弱な箇所を作りこむ可能性があるためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-7	法人	第3章	・インシデントレスポンス インシデント対応を訓練等で改善しつつ実際のインシデントに備え、さらに発生時の追跡記録によって継続的に改善できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
	3-8	法人	第3章	・メンテナンス メンテナンスを行うことで悪影響が出ることを全く考慮していない。予めメンテナンス計画を立て正常性の根拠とし、さらにメンテナンス後の影響を監視すべきである。さらに、リモートメンテナンスの実施に関して多要素認証のみの防御であり、認証突破後の振る舞いに制限がないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-9	法人	第3章	・メディア保護 メディアの保管と保管されたメディアへのアクセス、メディア運搬時の制御なども考慮し、メディアのライフサイクルに渡って包括的に保護できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-10	法人	第3章	・人的セキュリティ アカウントライフサイクル管理の概念が無いため、人事イベント(異動、退職)に連動した対策を十分に規定できていない。また退職インタビューを規定していないため、無意識または悪意のある行為を防止できないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-11	法人	第3章	・物理的保護 物理的接触が許可される人員を特定し、そのリストのレビュー・承認の規定が無いため、不正な物理的アクセスを阻止出来ない。リモートサイトを考慮出来ていない。また、論理的対策と連動した包括的対策となっておらずNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
	3-12	法人	第3章	・リスクアセスメント アセスメント結果をセキュリティ改善に利用しておらず、パッチ適用時にもセキュリティ的な影響を考慮していないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-13	法人	第3章	・セキュリティアセスメント セキュリティ規定自体の変更や修正をレビュー、承認するフローや、セキュリティ規定の改竄検知の規定が存在しないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-14	法人	第3章	・システムと通信の保護 暗号保護の強度指定が無いために脆弱な実装となる可能性がある他、意図しない通信への防御、検知を要求しておらず、完全性保護のためとして規定されたチェックサムも単体では有効ではないため、機密性も完全性も保護不可能であるためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	3-15	法人	第3章	・システムと情報の完全性 悪意のあるコードの混入または実行へのヒューリスティックな検出や、外部からのファイル取込み時のリアルタイムスキャンが必要である。さらに、システム監視における収集ログのインシデント対応チームへの連携といった監視後の行動に連動させておらずNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	4-1	業界団体	全体	本フレームワークは、セキュリティ対策に関して、日本の産業界が参照する代表的な文書になると考える。示される対策が抜け漏れがないことが求められる。また、本フレームワークの要件をカバーすることで，既存フレームワークの要件を十分に満足することを示してほしい。 【理由】 記載されているセキュリティ対策がMECE(Mutually Exclusive and Collectively Exhaustive)を検証できないため。例えば，対象の各層におけるライフサイクル毎に，本フレームワークの要件をマッピングする。また，本フレームワークの要件を満足することで既存フレームワークの要件が満足されることを示す。これらにより本フレームワークが既存フレームと同等以上であることを示せる。また、製品・サービスのライフサイクルに相当する分類や、ISO27001の対策の分類、NIST Cyber Security FrameworkのIdentify/Protect/Detect/Respond/Recoverの分類等、網羅性を想起させる分類導入の検討が有用と考える。	いただいた御意見を踏まえ、セキュリティ対策の分類に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	4-2	業界団体	第2章	各層の対策ごとに、組織、人、モノ、データ、システム、プロシージャへの対策例が存在する。この対策例を抽出の考え方の説明を、３章の前に記載いただきたい。 【理由】 記述を具体的にしたために、未記載の具体例も容易に想起される。優先度の高いものが適切に選択されているのか判断できない。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	4-3	業界団体	第2章	各層の対策毎に、組織、人、モノ、データ、システム、プロシージャの項目を含める構成した考え方を３章の前に記載いただきたい。 【理由】 一般に、セキュリテイの適用対象が、組織、システム、機器と異なると読み手が異なる。IEC62443では組織、システム、機器毎に異なる文書とし、読み手毎に文書を分けている。一方、本文書は、個別の対策毎に適用対象がすべて含まれている。 例えば、本書前半に、縦軸に組織、人、モノ、データ、システム、プロシージャ、横軸にライフサイクルの表を作り、表の中に、記載の章・節を記載する等の案を検討することで、誰がどこを読めばわかりやすい構成に至るのではないか。ただし、組織・ヒト・プロシージャに対しては、ライフサイクルとは異なる分類が適切な可能性もある点を指摘しておく。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	4-4	業界団体	付録B	国際規格との対応がない項目、および本書にしか記載のない項目の明記と、その理由を記載する。 【理由】 対策実施者が既に国際規格の項目に対応している場合、本書と国際規格の対応付けがあれば、本書により追加の対策が不要か否か容易に判断できる。それに加えて、国際規格との対応付けは、本書が何に注力しているかや、日本の独自性の世界への説明にも必要である。 例えば、NIST SP800-171では、補足資料にて、NIST CyberSeurityFrameworkのサブカテゴリとの対応付けが記載されている。そして、NIST CyberSeurityFrameworkに記載されている項目が一部存在しないことを、「Confidentialityに注力している」、と記載している。 既存のメジャーな国際規格の例えば１つに記載されている全要件または全対策と対応付けることで、本書が言及しない項目があれば、その理由を明示することで、本書が何に注力しているかが明らかになる。また、本書にのみ記載されている項目があれば、それを示し、日本が独自に着目した対策として世界に説明することができる。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、いただいた御意見も踏まえ、国際規格等への対応がないものについては追記するなど丁寧に整理を進めてまいります。また、本フレームワークにしか記載のない項目については、本フレームワークがサイバーとフィジカルの転写機能やデータの安全管理などを明記したことによって違いが生じているところもあると思いますが、その点については対策の必要性を明記するようにするなど修正してまいりたいと考えています。
	4-5	業界団体	第4章	４章の位置づけを明記してください。特に、４章が、２章、３章とどのように関連するのかを明記してください。 【理由】 ４章は、３層構造への言及もなく、6つの適用対象/構成要素(組織、ヒト、モノ、データ、プロシージャ、システム)とも用語があっていない。本章の位置づけの説明の記載が必要である。セキュリティに言及しているので、３章と重複している可能性もある。図８では、サプライチェーンセキュリティを意識しているように思うが、サプライヤー、製造者、消費者、といった典型的な構成が明示されていないため、それも読み取れれない。組織や製品のセキュリティが専門の機関によって担保され、その証明書/認定書を参照できる仕組みが必要、という点を伝えたいのであれば、その仕組みを明確に記載し、かつ、前章との関係を明記する必要がある。	いただいた御意見を踏まえ、全体構成などの見直しも含めて記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
4	4-6	業界団体	第2章	「（1） 各事業者がフレームワークを活用することで期待される効果」で言う「各事業者」とは何か。 【理由】 事業者の本文中に定義がないため。対象事業者の分類が必要と考える。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	4-7	業界団体	第3章 L2.003	「L2.003 機能安全を考慮したIoT機器の導入」の記述を見直しが必要ではないか。また、安全の定義を明記するべきである。 【理由】 本項目で想定するリスクは，現状ほとんどの場合に当てはまると誤解される。ＩoT装置において、機能安全が必要となる条件・前提を明記して、対策が必要となるIoT装置を限定する記述を追記するべきである。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	4-8	業界団体	第3章	「３．必要なサイバー・フィジカル・セキュリティ対策」において，調達要件に関する規定がない。 【理由】 セキュアなシステムを構築するにはサプライチェーンにまで目を向ける必要がある。調達要件にセキュリティ要件を盛り込む必要性があることを，本フレームワークが示すことで読者に気付きを与えられると考える。	いただいた御意見を踏まえ、調達要件に係る規定に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	4-9	業界団体	第3章 L2.001 付録C	「EDSA認証(IEC 62443-4-2)」という記述は誤り。p.110の説明も修正が必要。 【理由】 EDSA認証は，ISCIによる認証であり，EDSA認証仕様（EDSA-100～EDSA-406）に基づく。これはIEC 62443-4-2と同等ではない。	いただいた御意見を踏まえ、修正いたします。
	4-10	業界団体	第3章 L3.017 L3.018	L3.017，L3.018と項目を分けずに，統合したらどうか。 【理由】 同一リスクに対して，同様の対象（通信経路）であり，対策も同等のため。	対象がL3.017ではIoT機器とサイバー空間との間の通信路、L3.018ではサイバー空間内と異なっているため、対策項目を分けておりましたが、いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	4-11	業界団体	第3章 L2.017 L2.018 L3.014 L3.016	「専用チャネル」について、具体的な意味や例を記載して頂きたい。 【理由】 専用チャネルという表現は意味があいまいなため。付録Ｃ用語集に説明を記載する。	いただいた御意見を踏まえ、説明の追加など記載内容の修正を検討いたします。
	4-12	業界団体	第3章	対策を誰が実施するのか、誰が読み手なのか、わかるように構成を見直してほしい。 【理由】 読み手（対策実施者）が不明確なため。具体的には、IoT機器の項目(L2)では、機器製造開発者と機器利用者が実施することが混在している。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	4-13	業界団体	付録C	(16)公開鍵、(42)秘密鍵に、署名の検証、生成に関する説明が抜けている。また、（35)耐タンパーデバイスの説明は、「内部構造や記憶しているデータ等の改ざん・読み出しの困難さを備えるデバイス」として、読み出しの困難性にも触れる。 【理由】 読者に誤解を与えるため。	いただいた御意見を踏まえ、JISやISO/IECが発行する規格などを参考に用語の定義を修正いたします。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
5	5-1	個人	全体	本意見文は、貴省が策定・公表された「サイバー・フィジカル・セキュリティ対策フレームワーク(案)」(以下、「本FW」)に対して、本FWが志向する「グローバルハーモナイゼーション」が達成され得ないことを、国際的に広く認知されたサイバーセキュリティ基準であり、本FWが相互承認の対象としているNIST CSFやNIST SP800-171との不整合性を指摘することで、その修正・改善を求めるものである。 我々は、NIST CSFを初めとする国際標準的なサイバーセキュリティの考え方に対する誤った認識を持って作成された本FWが利用されることで、国際的に通用しないセキュリティ機能を持つ製品・サービスが生み出され、意図に反して競争力を失い、我が国産業の正常な発展への阻害要因となるばかりか、貴省が掲げるConnected Industriesの名の下に出された脆弱な製品・サービスがセキュリティインシデント発生に加担し、我が国全体の信用を失墜させる結果となることを懸念している。 5つの観点から本FWとSP800-171に明確な不整合が存在することを以下に示す。 1. サイバーセキュリティにおける機能概念 SP800-171には、NIST CSFで提示された「特定」、「防御」、「検知」、「対応」、「復旧」の5機能の概念をベースとして、サイバー攻撃に対して統合的に機能するレジリエントな防衛を可能としているが、本FWに示されたリスクや対策には、そのような概念が欠落した単なる対策の寄せ集めであるため、SP800-171と同等であるとは到底言えない。 また、本資料「付録B」に、NIST CSFやSP800-171との対応関係が示されているが、そもそも項目レベルで欠落が存在し、かつ本FWの同一対策番号にマップされたNIST CSFとSP800-171の対応関係が、NISTの正式出版物のものと異なる上に、各項目が所属するカテゴリのレベルで評価しても不整合であり筆舌に尽くし難い。	いただいた御意見のとおり、本フレームワークは、サイバー・フィジカルが融合した産業社会におけるセキュリティ対策の全体的な枠組を提示するものであり、民間企業がCUIを共有する場合に求められるセキュリティ対策を整理したNIST SP800-171と同じものではありません。 また、いただいた御意見を踏まえ、付録Bの対応表を修正いたします。
	5-2	個人	第2章	2. フレームワークの保護対象 SP800-171では、保護対象情報をCUIと称し、政府内・企業内生成情報や自然生成情報等を対象としているにも関わらず、本FWの保護対象情報は、「フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報」と限定的である。保護対象情報の定義と範囲は、情報の保管場所や保護強度の妥当性などを評価するために基本となる要素であるため、それらが異なるSP800-171と本FWにおいて、それらが適用範囲とする情報、システム、組織と制御策が志向するセキュリティ強度に大きな差異が生じている。 さらに、米国ではCUIを定義するための事務局や一種のデータベースまで整備して対象を明確にしているが、本FWでは対象情報が不明瞭であるために、有効に活用できるとは思えない。	いただいた御意見のとおり、CUIの保護を目的としたNIST SP800-171と本フレームワークとは位置づけが異なります。 価値創造過程に関わる6つの要素のひとつであるデータを、「フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報」と定義しておりますが、「保護対象情報」という観点では、第1層や第3層にて従来から存在する対策を中心に記載しています。 データについてその性格等に基づいて区分して管理すべきことについては、L3.022で明確に記載していますが、データの性格自体を本フレームワークで決めるものではありません。保護すべき情報の明確化については、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	5-3	個人	第2章	また、本資料「2.2. フレームワークの構造」で示された3階層の分類根拠が不明瞭であり、かつOSI参照モデル等の妥当性を一般的に認知されたモデルとの対応も無いため、それぞれに記述された対策の対象や利用目的が不明であり、分類意味が存在しない。そしてSP800-171にはそのような3階層の分類方法はそもそも存在せず、IoT機器に限った制御策もないため、等価とはならない。	いただいた御意見のとおり、CUIの保護を目的としたNIST SP800-171と本フレームワークとは位置づけが異なります。 三層構造の分類根拠は、P.7にお示ししている通り、「新たな付加価値のための一連の活動を視野に入れる」ことにあり、層毎に整理することで関係するステークホルダーが変わることに対応できるようにしています。
	5-4	個人	第2章 第3章	3．フレームワークの対策内容 本FWにおいて規定された対策内容を分析し、多くの項目においてマップされたSP800-171項目とは内容的に整合しないことが判明した。文面的に整合している項目もあったが、それらの多くは、SP800-171の要求文もしくは、SP800-171に紐付けられたSP800-53のコントロール文を部分的に引用して、「構成要素毎の対策例」に記述されるに留まるため、NISTの本来の意図を失っている。その証拠として、全く関係のない「対策の概要」「対策ポイント」が記述された本FWの項目に対して、NISTからの引用文が多々記載されている。 また、規定された対策内容や例を見るに、「2.2. フレームワークの構造」として示された「価値創造過程が展開する産業社会の三層構造」や「価値創造過程に関わる6つの要素」が対策内容や例を分類して示す上で機能不全であり、内容的にも混在している。	いただいた御意見を踏まえ、セキュリティ対策項目に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	6-1	法人	全体	●費用に関する分析結果 サイバー・フィジカル・セキュリティ対策フレームワークについて、その57項目を中小企業が満たすためのシステムを構築するための見積もりを試算した。 ※前提 従業員数:300人(企業規模において中小企業を示す人員数の上限) 企業が保有するIoT機器:600台(Cisco社が2010年に試算した所有IoT機器1.8～2台/人を利用) その結果、総額約6.9億円を要することが判明した。内訳は以下。 L1 （企業間のつながり）：約1.3億円 L2 （フィジカル空間とサイバー空間のつながり）：約3.4億円 L3（サイバー空間におけるつながり）：約2.2億円 合計：約6.9億円 これに対し本フレームワークよりも厳格度が高いSP800-171（110項目）の約3倍のコントロール数であるSP800-53（325項目）の準拠に要する費用は平均3億円であるとされている。 ●高額化の要因 ・同じような対策を3階層で複数にわたって要求している ・要求レベルが中途半端であるが実現するには高機能な製品を導入せざるを得ない ・既存技術では実現不可能とも思われる実装が存在する（L3.010、L3.011等）	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-2	法人	第3章	・アクセス制御 アカウントライフサイクルに沿った管理を規定できていない。さらに、アカウントタイプも特権と非特権の二種類のみで不足であり、最小特権や責務の分離を用いた対策も示せておらず、NISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-3	法人	第3章	・意識と訓練 各ユーザの責任や役割に基づいて、適した内容を設計しなければ、有効にセキュリティ意識を向上できず内部犯行を考慮できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
6	6-4	法人	第3章	・監査と責任追跡性 監査行為をセキュリティ向上に活用することを意図していない。監査対象とするセキュリティイベントの定義から実装の確認、そして監査レコードの分析とレビュー、さらには監査機能やレコード自体のセキュリティまで言及できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-5	法人	第3章	・構成管理 資産管理・構成管理の構築のみの規定であり、そこにセキュリティ強化という目的で構成設定と機能最小化を要求できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-6	法人	第3章	・識別と認証 全ユーザに多要素認証を要求し、セキュリティ的に脆弱な箇所を作りこむ可能性があるためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-7	法人	第3章	・インシデントレスポンス インシデント対応を訓練等で改善しつつ実際のインシデントに備え、さらに発生時の追跡記録によって継続的に改善できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
	6-8	法人	第3章	・メンテナンス メンテナンスを行うことで悪影響が出ることを全く考慮していない。予めメンテナンス計画を立て正常性の根拠とし、さらにメンテナンス後の影響を監視すべきである。さらに、リモートメンテナンスの実施に関して多要素認証のみの防御であり、認証突破後の振る舞いに制限がないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-9	法人	第3章	・メディア保護 メディアの保管と保管されたメディアへのアクセス、メディア運搬時の制御なども考慮し、メディアのライフサイクルに渡って包括的に保護できていないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-10	法人	第3章	・人的セキュリティ アカウントライフサイクル管理の概念が無いため、人事イベント(異動、退職)に連動した対策を十分に規定できていない。また退職インタビューを規定していないため、無意識または悪意のある行為を防止できないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-11	法人	第3章	・物理的保護 物理的接触が許可される人員を特定し、そのリストのレビュー・承認の規定が無いため、不正な物理的アクセスを阻止出来ない。リモートサイトを考慮出来ていない。また、論理的対策と連動した包括的対策となっておらずNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	6-12	法人	第3章	・リスクアセスメント アセスメント結果をセキュリティ改善に利用しておらず、パッチ適用時にもセキュリティ的な影響を考慮していないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-13	法人	第3章	・セキュリティアセスメント セキュリティ規定自体の変更や修正をレビュー、承認するフローや、セキュリティ規定の改竄検知の規定が存在しないためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-14	法人	第3章	・システムと通信の保護 暗号保護の強度指定が無いために脆弱な実装となる可能性がある他、意図しない通信への防御、検知を要求しておらず、完全性保護のためとして規定されたチェックサムも単体では有効ではないため、機密性も完全性も保護不可能であるためNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	6-15	法人	第3章	・システムと情報の完全性 悪意のあるコードの混入または実行へのヒューリスティックな検出や、外部からのファイル取込み時のリアルタイムスキャンが必要である。さらに、システム監視における収集ログのインシデント対応チームへの連携といった監視後の行動に連動させておらずNISTに劣る。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	7-1	業界団体	第1章	経済産業省 サイバーセキュリティ課にて策定されたサイバー・フィジカル・セキュリティ対策フレームワークについて、従来のアセットベースのリスクマネージメントではなく、サービスのバリューチェーンで考えていくことは非常に画期的な考え方であり、賛同する。 【理由】 これまで、各企業の責任分界点という従来の仕組みの議論が先行しており、スマートホーム分野での企業連携が進んでこないという状況であったが、今回のフレームワークは、オペレーション側からサイバーセキュリティを見るという点で、法人組織の枠ということではなく、実務としての連携という考え方ができ、本オペレーションに重点を置くというアプローチは非常に実効性があり、有効であると考えている。	本フレームワークに対する肯定的な御意見として承ります。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
7	7-2	業界団体	第2章	スマートホーム分野のセキュリティ対策を価値創造過程（バリュークリエイションプロセス）における三層構造で捉え、従来のサプライチェーンの活動範囲から拡張された付加価値を創造する活動のセキュリティ上のリスクを的確に洗い出すアプローチに賛同する。 【理由】 スマートホーム実現のためには各企業のつながりが不可欠であり、またスマートホームのシステムにおいては管理者が不在という脆弱性があり、本フレームワークは企業連携をセキュリティ対策の部分で支え、スマートライフの実現のための根幹となる部分であると考えている。 加えて、産業・家庭分野に分断されることなく、ネットワークで繋がった状態の中で実現されるスマートホームにおいては、家庭で起こり得るサイバーリスクが、そのまま社会インフラにも連結し、産業分野に対しても影響を及ぼすと認識しており、「全ての起点は家庭生活にある」という認識の下で、サイバーセキュリティの在り方を検討することが肝要であると考えている。	本フレームワークに対する肯定的な御意見として承ります。
	7-3	業界団体	第2章	フレームワークの特徴で挙げられているグローバルハーモナイゼーションを実現することはぜひ政府のリーダシップの下、推進していただきたい。加えて、フレームワークの社会実装に向けた政策の実現をお願いしたい。 【理由】 　フレームワークの実運用にあたっては、グローバルハーモナイゼーション及び具体的な政策等が重要であると考える。当協会においてもスマートライフ分野の特性にあったフレームワークの適用に向けて議論を進めていく予定であり、政府においても国際連携の推進やフレームワーク遵守によるセキュリティ確保を前提としたインセンティブの付与といった業界発展に資する政策を継続検討して頂きたい。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
8	8-1	個人	全体	都道府県警察のサイバー犯罪対策室の、人数は多くはないと思うので再犯を少くする為に、拘留刑とか、禁錮刑とかの罰則を、設定、願います。	本フレームワークの目的は、企業等が取り組むべきセキュリティ対策の全体的な枠組を提示するものであり、サイバー犯罪に対する刑罰を規定する目的をもったものではございません。
9	9-1	法人	第3章 L1.008	セキュリティインシデントとセキュリティイベントの概念を明確に分けて記述することで、内容を明瞭にすべきと考えます。以下の文でイベントとすべきところの修正を提案します。 【参考】　セキュリティイベントは不正な通信などの、個別に生じる事象を指す用語です。セキュリティイベントが生じたときに、それ自身あるいはその他のセキュリティイベントの状況などを分析し、セキュリティインシデントであるか否かを判断します。 【修正案】 ■対策の概要 ・ 不正通信などのイベントの検知体制の整備 ■対策ポイント セキュリティイベントの相関の分析、及び外部の脅威情報と比較した分析を行う手順を実装することで、セキュリティインシデントの発生を正確に特定する。 中略 ○ヒト ・ 発生したセキュリティイベントについて、セキュリティ管理者及び適切な関係者に報告する。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	9-2	法人	第3章	第2層はフィジカルからサイバーへの転送を対象としており、その具体的なモノはIoTデバイスと考えられます。第3層はIoTデバイスで生成されたデータがシステムとして処理され、他のデバイスへ受け渡される空間を対象としており、コンピュータ及び通信システムと理解できます。しかし、3.2と3.3ではこの概念が錯綜しているように読めてしまい、分かりにくく思います。 問題の第一は「IoT機器」の用語にあります。フィジカルからサイバーへの転送の機能を担うデバイスの意味と、デバイスを組み込んで情報通信処理を行う機器の二つの概念で「IoT機器」が用いられており、これが全体を分かりにくくしています。第2層に対してはIoTデバイス、第3層についてはIoTシステム（又はIoT機器システム）と使い分けることを提案します。 第2層をIoTデバイスとした場合、「L2 007 、L2.016 IoT、L2.017 、L2.018、L2.019、L2.020、L2.021」はいずれも、データ空間つまり第3層の対策であると考えます。 一方、L3.002はデバイスの問題ではないでしょうか？ また、L3.001は第2層にも適用すべき対策であると思います。	いただいた御意見を踏まえ、IoT機器の定義に関する記載内容の修正を検討いたします。 また、第2層の内容としては、IoT機器自体のみならず、IoT機器とサイバー空間をつなぐチャネルもスコープに収めているものと考えるため、L2 007 、L2.016 、L2.017 、L2.018、L2.019、L2.020、L2.021も範囲内と考えています。 さらに、いただいた御意見を踏まえ、L3.001及びL3.002の第2層への適用に関して検討いたします。
10	10-1	個人	第3章 L2.005	「■対策ポイント」の「IoT機器に対し…機器やサービスの間で使い回しのないパスワードへの定期的な変更等利用環境に適した設定値の使用を行うことで…」のうち「定期的な」を削除すべきと考えます。 【理由】 理由の第一は、近年、米NIST SP 800-63bでのアイデンティティ認証の考え方の大きな変化、及び国内でのNISCや総務省での啓発コンテンツでも見られる通り、パスワードの定期的変更について否定的な見解(ユーザへの負担増、攻撃性能の向上による安全な運用が困難になったこと等)が示されていることがあります。本書で言及しているNIST SP 800-53及び171では800-63bの考え方はまだ反映されていませんが、来年半ばぐらいまでには対応されると思われます。 第二に「IoT機器」の「パスワード」が具体的にどのようなものの何を実現するものなのかを指すのかが定かではないものの、ヒトがPCやWebサービスで使うログインパスワードと違い、広範囲に多数存在するIoT機器において管理画面接続用パスワード等は、各機器毎に異なるパスワードを設定し一人の管理者がこれを管理する場合、このパスワードを定期的に変更するとなると非常に手間がかかることから、管理者としては受け入れ難い要求と考えます。もしこの作業を軽減するための仕組みを入れるとしても、コスト増や新たなリスクを生み出す可能性があり、定期変更の遵守を優先する効果に見合うメリットがあるとは思えません。 第三に第一層及び第三層の対策や第二層の他の対策におけるパスワード管理に関する説明には「定期的変更」に関する記述はなく、この対策にのみ採用されていますが、その理由の記述がなく、納得性に欠けると考えます。 以上から、パスワードの定期的変更は(例示であったとしても)汎用性のある対策として掲示すべきではないと考えます。	いただいた御意見を踏まえ、修正いたします。
	11-1	法人	全体	1．ネットワーク社会の全体像について 本フレームワークは、新しいフレームワークだからこれを追加するという概念ではないと思います。 IoT機器とはネットワークに接続されるすべてのもの、活用例ではドローンが描かれているが、PC、スマートフォンなども含まれることを記載して、ネットワーク社会の全体像を明確にしていただいた方が良いと思います。 また、5Gが実装された社会では、サイバー攻撃がますますサプライチェーン全体に影響を及ぼし、データの安全性確保が必要となります、したがって、IoT機器だけでなく5Gについても言及すべきと考えます。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、活用例（ユースケース）は、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、検討してまいります。
	11-2	法人	第3章 L2.018 L3.003 L3.007 L3.015 L3.016	2．本フレームワークに不足している部分について (1)サイバーキルチェーンの概念 現在のPCを中心としたネットワーク運用の最大の課題である攻撃者の潜入が前提での記載がありません。悪意ある攻撃に対してリスクを低減するための項目と内容が整理されていますが、その対策を攻撃が潜ってしまった場合の対応、サイバーキルチェーンの概念が不足していると考えます。例えば、既知のマルウエアなどによる攻撃、既知の情報を前提とした対策のみの記載となっています。今後の攻撃者の武装能力の向上スピードは増加する傾向にあり、未知のマルウエアやグレーレピュテーションへの対応をL2.018,L3.003,L3.007,L3.015,L3.016に追記していただき、サプライチェーンへの普及を図るべきだと思います。 未知の情報を早期に獲得し、社会が共有することで社会全体が安全になるエコシステム構築のために、このサイバーセキュリティフレームワークにはサイバーキルチェーンの概念がなくてはならないことだと思います。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
11	11-3	法人	第3章 L2.006 L2.007 L2.014 L2.019 L3.017 L3.018 L3.019 L3.021	(2)セキュリティ強度について セキュリティ強度について言及がないため、実装するセキュリティ対策(プロセス、製品、体制など)の差が生じます。結果的に、本フレームワークを参照として構築したセキュリティ対策がグローバルサプライチェーンに求められている対策とかい離し、セキュリティ対策への追加投資、さらには、対応までの時間がかかることで国内産業のグローバル競争力低下を招く可能性があります。 例えば、アクセス制御では、従来の国内で実装されているアクセス制御以上の細かな制御が必要であることは読み取れません。L2.006, L2.007, L2.014, L2.019へ特権IDや責任の分離について記載すべきと考えます。また、システムの通信の保護においては、意図しない通信が発生した後の防御、検知に対する規定もなく、サイバーセキュリティ経営ガイドラインV2.0で追加されている検知、対応、復旧領域が薄いため、L3-017~019,L3.021へ意図しない通信が発生した場合の検知、対応を記載すべきと考えます。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しながら複数お示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別に具体的な検討に取り組みながら、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。 特権IDや責任の分離については、主にL3.023に記載しています。意図しない通信が発生した場合の検知、対応については、L3.016、L3.017 構成要素毎の対策例、L3.019、L3.020 対策ポイントおよび構成要素毎の対策例にて記載しています。
	11-4	法人	全体	(3)セキュリティインシデントの適切な情報共有 GDPR(EU一般データ保護規則)や米DoD「DFARS 252.204-7012」では72時間以内の報告義務があることから、グローバルのデファクトスタンダートに合わせた目標時間の設定が必要だと考えます。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、インシデント報告義務等は、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、検討してまいります。
	11-5	法人	第3章 L3.010 L3.011	3. 実装技術について ・L3.010、L3.011についてはIoT機器と定義された全てのものが実装できるわけではないため実現が難しいです。	いただいた御意見を踏まえ、実施が望ましいけれども対策の実施が可能ではない場合があるものについては、「可能な場合」あるいは「することが望ましい」と追記するなど記載内容の修正を検討いたします。
	11-6	法人	全体	・中小企業も対策が可能なセキュリティフレームワークであることから、クラウドサービス利用にも言及が必要です。ただし、クラウドサービスは、グローバルハーモナイゼーションの実現のためにもグローバル標準の技術が採用されていることが必須です。	政府において、クラウドサービスの安全性評価について本年度から検討を開始する予定であり、その検討内容やいただいた御意見も踏まえて、本フレームワークの記載内容についても検討いたします。
	12-1	法人	全体	論じようとしている問題領域を明確にするため、「サイバー・フィジカル・セキュリティ対策」の定義が必要ではないか。本案のようなタイトルでは、例えば，「サイバー・フィジカル両面からのセキュリティ対策」や「サイバー・フィジカル・システムのためのセキュリティ対策」など様々な解釈がありえてしまうため、より明確な定義について説明を追加いただきたい。	いただいた御意見を踏まえ、全体構成などの見直しも含めて修正いたします。
	12-2	法人	全体	セキュリティ対策のフレームワークとしては、米国NISTのサイバー・セキュリティ・フレームワークが一般の評価を固め始めているところ、これとは異なるフレームワークを提唱するのであれば、NISTのフレームワークと比べていかなる点に本案の特徴があるのか、あるいは、どのようにNISTのフレームワークと使い分けて欲しいと考えているのかを明示的に示された方がよろしいのではないか。 米国NIST：サイバー・セキュリティ・フレームワーク https://www.nist.gov/cyberframework また，サイバー・フィジカル・システムのセキュリティ対策については，ENISAから「Baseline Security Recommendations for IoT」の白書が出ており、ENISAは，欧州地域内の専門家に対する相当に網羅的なヒアリングなどを含む時間をかけた調査を経てこの白書をまとめたとしているところ、本書では，IoTシステムのアーキテクチャをモデル化し、その各コンポーネントに存在する攻撃界面を分析することによりリスクを分析し、必要なセキュリティ対策を洗い出している。そのようなENISAの白書と比べると，本案にはモデル化や脅威分析の観点（後述）が不足しているように思えるため、再考いただきたい。 ENISA： Baseline Security Recommendations for IoT https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot	本フレームワークは、サイバー・フィジカルが融合した産業社会を三層構造でとらえることで、より全体的なモデルを提示していることに特徴があり、米国NISTのサイバー・セキュリティ・フレームワークと矛盾するものではなく、整合性を確保することを前提に更に検討を進めてまいります。その際、海外におけるほかの取組についても更に参考として内容を充実させたいと考えています。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
12	12-3	法人	第3章	第１層に示される従来型のサプライヤチェーンに対する問題では、主に個別主体のポリシや体制が問われているが、これはこれまで、IoTセキュリティガイドライン等で示されている個々の主体における注意ポイントを脱していないように見える。また、各項目はISMS及びCSMSのみの議論にとどまっているが、これらは個々の主体に対する従来からの問題点の再確認であり、相互信頼をするための枠組みへの言及が必要ではないか。例えば、NIST IR 8200では、ISO/IEC 27036:2014,20243:2015, ISO 28000:2007 などのルールを参照し、Supply Chain Risk Management (SCRM) を説明している。 Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT) https://csrc.nist.gov/publications/detail/nistir/8200/draft また、相互信頼の考え方の具体例として、各IoT 製品に対する製品評価や、その準拠が考えられる。これについては、既に下記調査にて、経済産業省による検討がされているものと考えられ、これへの言及をされるとよいのではないか。 IoT機器のセキュリティ評価等調査 http://www.meti.go.jp/meti_lib/report/H28FY/000582.pdf そのうえで、NIST IR 8200 の「Annex D」で示されているような、各分野別・製品別の個別の規格との連関で考えるべきであるが、各主体が、どこまで何を行っているのかをお互いに同じ言葉で説明ができることが望まれ、それは、「ISMSやCSMSに準拠」という以外にも求めるべき相互信頼について記述しておくことが望まれるのではないか。例えば自動車分野における SAE J3061 などの規格のように、それぞれの分野で検討が進みつつある。 SAE J3061：Cybersecurity Guidebook for Cyber-Physical Vehicle Systems https://www.sae.org/standards/content/j3061/	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、NIST IR 8200などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	12-4	法人	第3章	本文書で記載される第２層に対する注意点は、従来の個々の製品に対する注意点をまとめたものとなっており、期待される枠組みではないように思われる。確かにそれらは重要な役割を担うが、既存の「IoT セキュリティガイドライン」（総務省、経済産業省）や「つなが世界の開発指針」（IPA）にて説明されている項目であり、さらに説明の必要性はないものと考えられる。これからSociety5.0社会が実現された後の脅威であるため、移り変わってしまう可能性があるため、例えば、価値創造過程で起きうるべき脅威に備えられるように、製品への設計時からの脅威分析を行い、セキュアバイデザインを組み込むことも必要ではないかと考えられる。 IoT脅威分析チュートリアル https://www.ipa.go.jp/files/000055835.pdf 第３層で足りないことは、サイバー空間においてデータの由来は全く問えないことから、諸外国の動き (ENISA, NIST 等) 米欧などの主要な認証制度との整合性を確保することや、インシデントマネージメントの考えを仕組みの中に自然と組みこむことが重要ではないかと考えられる。また、データの属性に含まれると考えられるプライバシーへの言及もみられないため、GDPRなどの対応も念頭に入れ、ENISAなどで議論されるIoTに対するプライバシーについての議論を盛り込むことも必要ではないか。	セキュリティバイデザインについては、L2.002にて対策項目を設けていることから、紹介いただいた文献も参照しつつ今後検討を進めてまいりたいと考えています。 主要な認証制度との整合性確保に関しては、今後、EU等の動向も踏まえ、内容を充実させていきたいと考えています。 プライバシー保護については、L1.012およびL3.022にて言及していますが、いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	12-5	法人	全体	本文書が中小企業を含めた全産業におけるサプライヤチェーンを対象とすることから、従来のビジネスとの兼ね合いを考える必要性はあると考えられ、適切なコンサルタントがそれぞれの業態にあった提案を可能とできるよう、既存のルールとの関係性について触れておくことが望ましいのではないか。例えば、NIST IR 8200 では、System Security Engineering のほか、機能特徴ごとにシステムを分け、それぞれの単位で求められている国際規格を列挙されており、参考資料としての記載だけではなく、クロス比較できると、既に投資した標準対応も活かして対応できる。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、NIST IR 8200 などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	12-6	法人	全体	全体的に、ベンダーが行う対策、エンドユーザーが行う対策等がひとくくりの主体で記載されているため、区別していただきたい。	いただいた御意見を踏まえ、主体を明確にするなど全体構成などの見直しも含めて記載内容の修正を検討いたします。
	12-7	法人	全体	各個別項目の解説の前に、各項目を俯瞰できるよう、レイヤー毎の対策項目一覧が付記されると見通しを立てやすのではないか。	いただいた御意見を踏まえ、対策項目一覧を追記するなど全体構成などの見直しも含めて記載内容の修正を検討いたします。
	12-8	法人	第3章	プライバシーデータ、プライバシーの観点についての項目がL1にしかなく、L3に記載がないが、項目を設けるべきではないか。	いただいた御意見を踏まえ、L3におけるプライバシーに関して記載内容の修正を検討いたします。
	12-9	法人	第2章	「正確に」「転写」されることについてのイメージを得やすいように、具体的な事例を記載いただきたい。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	12-10	法人	第2章	「ヒト」「データ」「モノ」のイメージを得やすいように、具体的な事例を記載いただきたい。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	12-11	法人	第2章	「セキュリティ対策の項目を列挙したプロファイル」という表現が唐突に出てくるので、プロファイル記載事例等の解説が必要ではないか。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
	12-12	法人	第3章 L1.003	自社のセキュリティインシデントに対して、自社のみで対応していくようにも読めてしまう恐れがあるが、一般的には、外部のベンダ、組織の支援を受けて対応していくものであるので、このあたりを記載追加いただきたい。	セキュリティインシデント発生時には自社だけでなく外部組織と連携しつつの対応が一般的と考えられるため、いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	12-13	法人	第3章 L1.004	サポート期間の確認と、サポート終了後の対応について検討する必要がある。	サプライヤーとの保守契約を考える上で、重要な内容と考えられるため、いただいた御意見を踏まえ、L1.004の記載内容の修正を検討いたします。
	12-14	法人	第3章 L1.007	盗難を想定した物理的なセキュリティに関する記載が欲しい。 L2.008 のような内容。	施錠等、盗難に備えた物理的なセキュリティ対策は、L2.008およびL3.006に記載しています。L1.007については、あくまで「資産管理」について記載しています。
	12-15	法人	第3章 L1.008	インシデントの検知、分析を自社で実施するようにと読めてしまうため、アウトソーシングについても明記すべき。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	12-16	法人	第3章 L1.013	以下のように修正いただきたい。（インシデント情報のみでなく、脆弱性情報等幅広い情報入手を求めるため） 「JPCERT/CCなどから最新のセキュリティインシデント情報を」 ↓ 「JPCERT/CCなどから最新のセキュリティ関連情報を」	いただいた御意見を踏まえ、修正いたします。
	12-17	法人	第3章 L2.005	以下のように修正いただきたい。 「IoT機器を設置する前に、デフォルトの初期設定値を確認する」 ↓ 「IoT機器を設置する前に、初期設定値をデフォルトから変更する」	いただいた御意見を踏まえ、修正いたします。
	12-18	法人	第3章 L2.015	「禁止するソフトウェアの一覧(ブラックリスト)を用いて、利用するソフトウェアを制限する 」 の箇所について、IoT機器でブラックリストを用いると言うことは、定期的なブラックリストの更新が必要となり、更新漏れ等から、新たなリスクの引き金となるのではないか。	いただいた御意見を踏まえ、修正いたします。
	12-19	法人	第3章 L2.018	「接続元のMACアドレス、IoT機器の設置場所、アクセス時間・頻度等の情報をもとにした不正接続の有無の確認 」 ⇒広域ネットワークを経由した時点で接続元のMACアドレスはなくなるので、不適当ではないか。	いただいた御意見を踏まえ、「MACアドレス」を「IPアドレス」に変更するなど記載内容の修正を検討いたします。
	12-20	法人	第3章 L2.019 L3.021	・MACアドレスフィルタリングが例示されているが、MACアドレスは任意に設定が可能なので、フィルタ条件としては不適当である。特に無線環境では通信の傍受が可能であり、正規の機器のMACアドレスを調べるのは容易なため、適当ではない。 ・ESSIDも盗聴可能なので、これを設定したことでセキュリティが特段向上することはない。 ・LPWAといった広域の無線通信については触れないのか？ 本項目は「L3.021 不正な無線接続への対応」においても同様。	いただいた御意見を踏まえ、L2.019およびL3.021において、対策ポイントからMACアドレスフィルタリング、ESSIDを削除することを検討いたします。また、LPWAの影響については、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、検討してまいります。
	12-21	法人	第3章 L3.001	サービスが何を指しているのか文章からでは不明確なので例示が欲しい。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	12-22	法人	第3章 L3.003	サイバー空間への不正ログインとは、クラウドやWebサービスへの不正ログインのことを指すのか、具体的なイメージが得られないため、具体例をいくつか記載すべきではないか。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	12-23	法人	第3章 L3.004	UDPプロトコルでセンサからのデータを吸い上げる場合は、送信元の識別は不可能であり、TCPで実装すれば良いが、多量のセンサを収容する場合はこうした実装は困難ではないか。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	12-24	法人	第3章 L3.005	小型のセンサのようなケースでは、電子証明書のような物での認証は困難ではないか。	いただいた御意見を踏まえ、実施が望ましいけれども対策の実施が可能ではない場合があるものについては、「可能な場合」あるいは「することが望ましい」と追記するなど記載内容の修正を検討いたします。
	12-25	法人	第3章 L3.007	データが許容範囲内であっても改ざんによって不都合が発生するケースがあるのではないか。	いただいた御意見を踏まえ、異常の事例として、改ざんの痕跡がある場合を追記するなど記載内容の修正を検討いたします。
	12-26	法人	第3章 L3.017	本項目のほか、下記項目との重複感があるため、一つにマージするべきではないか。 L3.018 サイバー空間における暗号化通信 L3.019 サイバー空間における送受信情報(データ)の暗号化	対象がL3.017が通信路、L3.018がデータと異なっているため、対策項目を分けておりますが、いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	12-27	法人	第3章 L2.005 L2.006 L2.007	本項目についても同上（重複感があるため、一つにマージするべきではないか。）	いただいた御意見を踏まえ、対策項目の分離・統合など記載内容の修正を検討いたします。
	12-28	法人	付録B	NIST IR 8200や同文書内に多数の基準群が引用されているところ、付録B掲載の４ガイドラインのみを今回の比較対象として選定された理由についてご教示いただきたい。	付録Aに記載の参考文献リストより、従来のサプライチェーンに加え、価値創造過程(バリュークリエイションプロセス)におけるセキュリティ対策を考える上で重要と考えられるものを選定しています。
13	13-1	業界団体	全体	既にガイドライン類（※）が多数あり、事業者にとっては他のガイド類や今回のフレームワークを参照するだけでも、負担が大きい。 　それぞれのガイドラインの記述内容に重複があるため、関係性の整理を行い、各ガイド類・フレームワークの内容を事業者が適切に参照し、セキュリティ対策を推進できるようにしてほしい。 （※）一例：NISC「サイバーセキュリティ戦略」、NISC「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針」、総務省「IoTセキュリティ総合対策」、総務省/経産省「IoTセキュリティガイドライン」、IPA「IoT開発におけるセキュリティ設計の手引き」	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	13-2	業界団体	第1章	電力分野の例で図中に「サイバー空間（電力供給をコントロール）」とあるが、サイバー空間で供給をコントロールするイメージが掴みづらい。接続の矢印に「分析結果による制御」と記述されていることも踏まえ、サイバー空間の表現として「コントロール」の表現を削除し、例えば、 ・サイバー空間（電力情報等） ・サイバー空間（電力需給に関する情報等） としてはどうか。合わせて、図左側の「運転情報をコントロール」についても「運転情報等」としてはどうか。 　また、図中フィジカル空間の「電力会社」という表現は、旧一般電気事業者だけを想起してしまう。 　現在の電力業界は、新電力やアグリゲーター、小売事業者といった多彩なプレイヤーが参入していることから、例えば、「電力事業者」のようにより幅広い表現としてはどうか。	いただいた御意見を踏まえ、図の表現を修正いたします。
	13-3	業界団体	第1章	本文を「米国では、NIST3が2014年2月に策定した特に重要インフラに対するサイバーセキュリティ対策の全体像を示したフレームワーク（Cybersecurity Framework）の改訂版が2018年4月に公開された」と変更してはどうか。 【理由】 　NIST Cybersecurity Framework Version 1.1は、2018年4月16日に改訂版が公開されている。（https://www.nist.gov/news-events/news/2018/04/nist-releases-version-11-its-popular-cybersecurity-framework）	いただいた御意見を踏まえ、修正いたします。
	13-4	業界団体	第2章	フレームワークの特徴として、「想定されるリスクと必要な対策のコストのバランスをイメージできるような内容にする」とあるが、１２頁以降の具体的な対策の内容において、このバランスをイメージするのが難しい。 　「コストの観点」での評価や解釈等について、各セキュリティ対策に項目を設けるまたは補足すれば、理解が深まり、一層活用の幅が広がるのではないか。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	13-5	業界団体	第3章	対策の概要や対策ポイント、構成要素ごとの対策例について、重複した記載が多い。特にＬ２とＬ３のIoT機器に関する対策においては、重複記載が多く活用上懸念があるため、内容整理や記載方法の工夫が望ましいのではないか。	いただいた御意見を踏まえ、第2層、第3層を中心に、各層ごとに実施すべき内容の差異がわかりやすく表現されるよう全体構成などの見直しも含めて記載内容の修正を検討いたします。
	13-6	業界団体	第3章 L1.013	セキュリティインシデント発生時には、JPCERT/CCなどのセキュリティ機関だけでなく、業界内で情報共有を行い、インシデント防止につなげることが必要であるため、「JPCERT/CCなど」だけでなく「関係事業者やJPCERT/CCなど」としてはどうか。	いただいた御意見を踏まえ、修正いたします。

NO		提出者 （種別）	該当箇所	御意見	御意見に対する考え方
	13-7	業界団体	第3章	「IoT機器」について 「産業に求められるセキュリティ対策の全体像」とするためには、対象をIoT機器に限定する必要はないのではないか。（セキュリティを確保すべき機器の全てがインターネットに接続されているわけではなく、IoT機器の定義に当てはまらない機器も存在する） 仮に「IoT機器」とする場合は、IoT機器以外の機器については、フレームワークの対象外と考えてよいか。（IoT機器を対象とするのであれば、その旨を「２．サイバー・フィジカル・セキュリティ対策フレームワークの考え方」等に明記しておくべきではないか）	本フレームワークは、インターネットに接続するIoT機器以外の機器におけるセキュリティ対策についても記載しており、IoT機器以外の機器についてもフレームワークの対象内であると考えています。いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	13-8	業界団体	第3章 L2.001	EDSA認証を取得した機器は少ないため、例示を行わず「第三者機関による評価を取得したIoT機器や自己適合確認により安全性を確認されたIoT機器の選択」としてはどうか。 また、「自己適合確認」という表現は、特定の制度を意識しているのか、制度とは関係なくメーカー等が自らセキュリティが確保されていることを宣言することを指しているのか等、内容が分かりづらいため、補足してはどうか。 【理由】 EDSA認証済み製品（http://www.cssc-cl.org/jp/certified_devices/index.html http://www.isasecure.org/en-US/End-Users/ISASecure-Certified-Devices）	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	13-9	業界団体	第3章 L2.011	対策ポイントについて、機器を遠隔地に設置しないケースも考えられるため、全ての機器に記録の遠隔確認機能が必要となるような記述をせず、「ソフトウェアの起動の記録は遠隔からも確認できることが望ましい」などとしてはどうか。	いただいた御意見を踏まえ、修正いたします。
	14-1	法人	第4章	・サイバー・フィジカル・セキュリティ対策 においては、Society5.0の実現に向けてのインターネットの信頼（トラスト）のチェーンの構築が重要であり、信頼されたモノ・データ及びそれらを提供する組織をサプライチェーンの中で公開するインフラの構築が重要である。 ・この点から、サイバー・フィジカル・セキュリティ対策 フレームワークの92ページ「４．信頼の確保に向けて」に記載された「トラストリスト」の必要性については、当協会として全面的に賛同するものである。 ・加えて、サイバー・フィジカル・セキュリティ対策 におけるセキュリティ要件への適合のレベルを示す概念として、「トラスト」という用語を導入することを提案したい。 ・「トラストリスト」については、信頼できる企業情報を登録する必要がある。様々な方法があると思料されるが、例えば、国が運営する法人インフォメーションが公開する企業情報に加えて、地方公共団体や民間団体等が有する既存の多種多様な企業情報の中から、その信頼性を客観的に評価できるものを抽出し、信頼できるサプライヤー等を選ぶことができる「法人認証データベース」を構築してはどうか。 ・このような「トラストリスト」又は「法人認証データベース」は、公平・中立な機関が運用を行うことが、信頼（トラスト）のアンカーの役割を果たす上で重要であり、官民の役割分担、適切な法制度の整備の必要性についても幅広く検討されるべきであると考える。	本フレームワークに対する肯定的な意見として承ります。 また、いただいた御意見を踏まえ、信頼の構築に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
	14-2	法人	第3章 L2.004	【原文37ページに対する意見】 ・サプライチェーン等における模倣品・不正品の混入防止の観点から、「IoT機器やソフトウェアのサプライヤーを特定し・・・」、「正規品であることを確認するために、IoT機器やソフトウェアのサプライヤーを識別し、認証する」ことを確実に手段の記載が重要である。 ・具体的には、正規品を提供するサプライヤーの特定や識別のためには、信頼できるサプライヤーをリスト化して、信頼できる中立機関が運営する企業認証データベースに登録してはどうか。 ・IoT機器やソフトウェアのIDの採番に際しては、それらの所有者又は管理者等と紐づけるため、法人番号と組み合わせたID体系を構築するべきである。 【原文37ページに対する修正・追記案】 L2.004 IoT機器における正規品の導入 ■対策の概要 ・ IoT機器のサプライヤーにより、正規であることが認証されたIoT機器の導入 ・ ソフトウェアのサプライヤーにより、正規であることが認証されたソフトウェアの導入 ・正規のIoT機器やソフトウェアのサプライヤーをリスト化して、信頼できる企業データベースに登録 ■対策ポイント 正規のIoT機器であることを検証できるIoT機器を利用することで、模倣品等の品質や信頼性が低いIoT機器の利用による、不正な情報(データ)の混入や誤動作の発生、故障頻度の上昇に伴う業務運用効率の低下等を防ぐ。同様に、正規のソフトウェアであることを検証できるソフトウェアを利用することで、模倣品等の品質や信頼性が低いソフトウェアの利用によるマルウェア感染や、不正確な情報(データ)の混入に伴う業務運用効率の低下等を防ぐ。 ・ IoT機器やソフトウェアには、一意であることを示すためのID(識別子)や重要情報(秘密鍵、電子　証明書等)が含まれる ・ 正規品であることを確認するために、IoT機器やソフトウェアのサプライヤーを識別し、認証する(完全性の検証等) ・信頼できるIoT機器やソフトウェアのサプライヤーをリスト化して信頼できる企業データベースに　登録する ・ IoT機器やソフトウェアが正規品であることを定期的(起動時等)に確認する ■構成要素毎の対策例 〇組織 ・ IoT機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。 ・ 信頼できるIoT機器やソフトウェアのサプライヤーを特定・リスト化し、信頼できる企業データベースに登録する。 ・ 正規品であることを確認するために、信頼できる企業データベースに登録されたサプライヤーのリストを参照し、信頼できるIoT機器やソフトウェアのサプライヤーを識別し、認証する。 〇モノ ・ IoT機器やソフトウェアには、一意であることを示すためのID(識別子)や重要情報(秘密鍵、電子証明書等)が含まれる。 ・ 電子証明書は、IoT機器やソフトウェアのユースケースに応じた有効期限を定める。 ・ IoT機器やソフトウェアは、搬送中の改ざん・漏えいを検知(又は抑止)する手段とともに納品される。 - 物品：セキュリティ便、プロテクトシール等 - 電送：暗号化、電送データ全体のハッシュ値等 〇プロシージャ ・ 正規品であることを確認するために、IoT機器やソフトウェアのサプライヤーを識別し、認証する。 ・ IoT機器やソフトウェア IoT機器やソフトウェアが正規品であることを定期的(起動時等)に確認する。 〇システム ・ IoT機器の機能の設計、開発、実装、修正において、セキュリティリスクを考慮したシステム開発ライフサイクルを導入する。 ・ IoT機器やソフトウェアのサプライヤーを特定し、そのサプライヤーから正規品を導入する。 ・ IoT機器やソフトウェアを一意に識別できるID(識別子)を採番する。その際、IoT機器やソフトウェアの所有者、管理者等の企業と紐づけるため、法人番号と組み合わせたID体系を構築する。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
14	14-3	法人	第4章	【原文92ページに対する意見　1】 ・「構成要素についてのセキュリティの確保」とは、構成要素を管理する主体が、別途設定されるセキュリティ要件への適合を図ることであり、「その確認」とは、その適合性を信頼できる主体が評価すること（以下、「適合性評価」と言う。）である。 ・信頼できる主体が構成要素を管理する主体と同一である場合は、自己宣言であり、一般に「信頼」のレベルは低い。信頼できる第三者の主体が適合性評価を行うことを「認証」と言い、自己宣言に比べて一般に「信頼」が高くなる。 【原文92ページに対する修正・追記案　1】 ４．信頼の確保に向けて ４．１．フレームワークにおける信頼（トラスト）の確保の考え方 サイバーフィジカルシステムのセキュリティを確保するため、それぞれの構成要素についてのセキュリティ要件の設定及び当該要件への適合性評価の仕組みを確立し、セキュリティ要件の確保(信頼の創出)とその確認(信頼の証明)を繰り返し行い、信頼のチェーンを構築、維持することで、価値創造過程全体の信頼（トラスト）を向上させる。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	14-4	法人	第4章	【原文92ページに対する意見　2】 ・モノ・データ等のセキュリティ要件への適合は、それらの生成時点だけではなく、価値創造過程全体を通して、一貫して評価又は確認される必要がある。 ・具体的には、モノ・データ等が、正しく生成され、かつ、すり替えられない、あるいは改ざんされないことよう、適切に管理することが必要である。 ・この適切な管理に際しては、モノ・データ等が本物であることの問い合わせ先としての信頼できるリスト（トラストリスト）が必要となる。 ・当然のことながら、このトラスト自体の信頼（トラスト）の確保が不可欠である。 ・ちなみに、デジタルデータの真正性の確保のための電子署名やタイムスタンプの電子証明書等の有効性確認も、ある種の信頼できるリストへのインターネットトラストセンターを通じての参照行為で言える。信頼できるリストを運営する認証局やタイムスタンプ局は、信頼できる認証機関による監査を受けている。 ・このようにトラストリスト自体の信頼（トラスト）の確保（トラストアンカー）が重要である。 ・とりわけ、グローバルな価値創造過程におけるトラストリストの管理の主体は、公平・中立な機関であるべきである。同時に、事業継続の観点から、経済的な自立を含めて、適切な官民の役割分担を踏まえた制度設計を検討する必要がある。 【原文92ページに対する修正・追記案　2】 1. 信頼（トラスト）の創出 ●セキュリティ要件を満たすモノ・データ等の生成 ●対象のモノ・データ等が要件を満たした形で生成されたことの確認 2. 信頼（トラスト）の証明 ●対象のモノ・データ等が正常に生成されたものであることを確認できるリスト(トラストリスト)の作成と管理 ●トラストリストを参照することで対象のモノ・データ等が信頼できるものであることの確認 ●公平・中立な機関がトラストリストを管理することにより、国内外での信用を維持 3. 信頼（トラスト）のチェーンの構築と維持 ●信頼（トラスト）の創出と証明を繰り返すことで信頼のチェーンの構築(トレーサビリティの確保) ●信頼のチェーンに対する外部からの攻撃等の検知・防御 ●攻撃に対するレジリエンスの強化	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	14-5	法人	第3章 L3.001	P60■構成要素毎の対策例の〇組織の例 （例: ITSMS認証(ISO/IEC 20000)） ・意見内容:変更案 （例: ITSMS認証(ISO/IEC 20000-1)） 【理由】 要求事項のため、正式な規格番号を記した方がよいと思われます。	いただいた御意見を踏まえ、修正いたします。

NO		提出者 （種別）	該当箇所	御意見	御意見に対する考え方
	14-6	法人	付録A	P93 ISO/IEC 27002:2013の説明 ISO/IEC 27002:2013（ISO/IEC） （情報マネジメントシステムの仕様を定めた国際標準規格であり、情報セキュリティ管理のベストプラクティスを提供。） ・意見内容:変更案 ISO/IEC 27002:2013（ISO/IEC） （情報セキュリティ管理策の実践のための規範を定めた国際規格であり、情報セキュリティ対策のベストプラクティスを提供。） 【理由】 ISO/IEC 27002は、マネジメントシステムについての規格ではなく、情報セキュリティ管理策を解説した規格のため、表現を上記の通り変更した方がよいと思われます。 （この文書では、全体的に「国際規格」を用いているようでしたので、上記案では「国際規格」としました。）	いただいた御意見を踏まえ、修正いたします。
	14-7	法人	付録A	○ ITSMS適合性評価制度（JIPDEC） （国際的に整合性のとれたITサービスマネジメントに対する第三者適合性評価制度。） https://isms.jp/isms.html ・意見内容：変更案 ○ ITSMS適合性評価制度（JIPDEC） （ITサービスマネジメントに対する、認定に基づく認証のための国際的に整合性のとれた第三者評価制度。認証基準は、国際規格ISO/IEC 20000-1である。） https://isms.jp/itsms.html 【理由】 この制度の認証基準を明確にした方が、国際整合性がより明確になると思われます。ISTMS制度のURLを示した方がわかりやすいと思います（ISMS制度のURLになっているようです）。	いただいた御意見を踏まえ、修正いたします。
	14-8	法人	付録A	P95の○５つめ ○サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度（JIPDEC） （産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムにおける国際標準規格IEC62443-2に基づいて第三者認証を行う制度。） https://isms.jp/csms.html ・意見内容：変更案 ○サイバーセキュリティマネジメントシステム（CSMS）適合性評価制度（JIPDEC） （産業用オートメーション及び制御システムを対象としたサイバーセキュリティマネジメントシステムに対する、認定に基づく認証のための国際的に整合性のとれた第三者評価制度。認証基準は、国際規格IEC62443-2に基づいて作成されたCSMS認証基準(IEC 62443-2-1:2010)である。） https://isms.jp/csms.html 【理由】 認定に基づく認証のための第三者評価制度ということを明記した方が、国際整合性を示すためにもより適切と思われます。認証基準名を明記した方がわかりやすいように思われます。	いただいた御意見を踏まえ、修正いたします。

NO		提出者 （種別）	該当箇所	御意見	御意見に対する考え方
	14-9	法人	付録A	P95の〇7つめ 〇情報セキュリティマネジメントシステム（ISMS）適合性評価制度（JIPDEC） （情報セキュリティマネジメントシステムにおける国際標準規格ISO/IEC27001に基づいて第三者認証を行う制度。） https://isms.jp/isms.html ・意見内容：変更案 〇情報セキュリティマネジメントシステム（ISMS）適合性評価制度（JIPDEC） （情報セキュリティマネジメントシステムに対する、認定に基づく認証のための国際的に整合性のとれた第三者評価制度。認証基準は、国際規格ISO/IEC 27001である。） https://isms.jp/isms.html 【理由】 認定に基づく認証のための第三者評価制度ということを明記した方が、国際整合性を示すためにもより適切と思われます。	いただいた御意見を踏まえ、修正いたします。
	14-10	法人	付録C	P110の（８） （8） ITSMS(IT Service Management System) ITサービス提供者が、提供するITサービスをPDCAサイクルに基づいて管理することで、品質の維持管理及び改善を行っていくための仕組み。国際規格ISO/IEC 20000に満たすべき要求事項が定められている。 ・意見内容：変更案 （8） ITSMS(IT Service Management System) ITサービス提供者が、提供するITサービスをPDCAサイクルに基づいて管理することで、品質の維持管理及び改善を行っていくための仕組み。国際規格ISO/IEC 20000-1に満たすべき要求事項が定められている。 【理由】 要求事項のため、正式な規格番号を記した方がよいと思われます。	いただいた御意見を踏まえ、修正いたします。
	14-11	法人	第3章 L1.012	「OECD8原則」に則り文書化することが良いが、「OECD8原則」は基本原則であるため対策ポイント及び対策例としては具体性に欠ける。対策ポイント及び対策例として国際規格である「ISO/IEC 29100（JIS X 9250）」を取り入れることが良いと考える。更に、安全管理措置の要件を定めるためには、対策としてPIA（Privacy impact assessment）の実施などを追加することが良いと考える。 【理由】 ISO/IEC 29100で示すプライバシー原則は、OECD8原則を含む既存の原則に由来しており、11のプライバシー原則を示すとともに、原則を遵守するための方法について記載されているため。	いただいた御意見を踏まえ、指定の規格等の参照などについて記載内容の修正を検討いたします。
	14-12	法人	第3章 L2.005	パスワードの「定期的な変更」の記載は、外した方がよいと考える。また、IoT機器の初期設定において、手順を定めるだけではなく、初期パスワードは必ず変更することを要件として定めることが良いと考える。 【理由】 IoT機器への適切なセキュリティ設定ということで、前提が不明瞭ではありますが、機器の制約により1つのアカウントを複数人で利用する場合には、パスワードを定期的に変更することで、リスクを低減させることが可能である。しかし、個別のアカウントを用いることが可能な場合には、パスワードの使いまわしや安全でない方法によるパスワードの保管等のリスクが考えられるため、定期的なパスワード変更を求めないことが望ましい。また、初期パスワードを変更せずそのまま使用することにより、IoT機器の乗っ取り等の問題が起きていることから、初期パスワードは必ず変更するように要件として定めるべきである。	いただいた御意見を踏まえ、修正いたします。
15	15-1	個人	第1章	・１ページの１行目「はじめに」と、２ページの最下行から上に３行目「始めに」とは、文言の統一が必要と思います。	いただいた御意見のとおり、修正いたします。
	15-2	個人	付録A	・９４ページの脚注は、８９ページの脚注と記載内容が重複しているので、８９ページでの再記載は不要と思います。	いただいた御意見を踏まえ、修正いたします。
	15-3	個人	付録C	・１１０ページの（1）、１１２ページの（１６）： 用語が本文に記載されていないのでは？	いただいた御意見を踏まえ、付録Cを修正いたします。
	15-4	個人	付録C	・１１１ページの（１０）に、１１０ページの（８）の「PDCAサイクル」についての説明の記載も必要と思います。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
16	16-1	法人	全体	Society 5.0, Connected Industriesが実現する社会において、サイバー攻撃、物理攻撃の多様化、高度化に対応すべくセキュリティフレームワークを構築することは非常に重要な施策と考えます。 第一層、第二層、第三層に分類して検討することにより、うまく整理できているのではないかと思います。 その一方で、各項目の粒度が異なるため、個々の問題が扱う対象が大まかすぎたり、細かすぎたりと曖昧なため、全体として散漫な印象があり、網羅性にも懸念があります。具体的には　brute force attack への対応、無線LAN機器のセキュリティの対応、TV会議システムが例外であるなど、選定基準が不明な個別の問題に踏み込みすぎているところがあり、この文章で扱うべき範囲を超え、結果的にページ数が増えすぎています。 また、第一層においてはISMSやCSMSの構築・運用が有効と記載されていますが、既存のガイドラインや規格、制度が色々あるなかで、今回のフレームワークは何が違うのか、どこは同じでどこが新しいのかなど、既存制度との比較、位置づけを示すと、分かりやすいと思いました。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	17-1	法人	第2章	「各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる」と記載がありますので、後述に記載の各対策において、提示されている対策だけでなく、その対策にて防ぐことができる具体的な脅威事例を示しておく必要があろうかと思います。是非、各対策に紐づいた具体的な脅威も示して頂き、利用者が活用する上で有益な参考資料にして頂ければと思います。 【理由】 提示されている対策と関係する具体的な脅威事例が提示されていないので、対策実施における具体的効果を実感できず、対策の必要性や深刻度が判断できないと思われる。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-2	法人	第2章	「セキュリティ対策の必要性とコストの関係を把握」については、サプライチェーン全体を構成する中小企業を含めた事業者が、実際に対策を行えるよう、想定されるリスクと必要な対策のコストのバランスをイメージできるような内容にすべきかと思います。 ［意見17-1］と同様に、フレームワーク内に想定されるリスクと実際に生じた脆弱性の事例（例えば、ＪＶＮ，ＣＶＥに記載されている事例）を提示する必要があろうかと思います。また、対策には攻撃される強度に応じた複数の対策が存在します。例えば、自己の機器が乗っ取られないための対策や、他のIoT機器に悪影響を及ぼさない対策など、種々の対策においても、最低限守るべき対策、より安全に防御するための再対策があります。従って、後述の各対策においても、対策できるレベル毎にフレームワークを分類しておけば費用対効果をイメージしやすいと考えます。 【理由】 現状の想定リスクだけでは、実際の被害状況を想定することは困難です。 コストの関係を把握するには、示された対策で守れる攻撃のレベルを示す必要があります。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	17-3	法人	第2章	「セキュリティレベルを保ったままでコストを圧縮できるような内容にする」とありますが、後述のフレームワーク内容では、一定のセキュリティレベルを維持しつつ、コストを低減できるような対策の提示がなされていません。例えば、一つの対策が複数の脆弱性リスクの防止につながるケースなど、コスト面を意識した整理が必要です。 【理由】 本フレームワークで示されている対策は、一定のセキュリティレベルを維持しつつコストを圧縮可能な手法が示されていない。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	17-4	法人	第2章	実際に脆弱性リスクの影響を把握するには、本対策を示すために使用したリスクシナリオを提示する必要があります。想定されるリスクの網羅性を把握し、リスクシナリオベースの対策検討という考え方が、実施できるような内容にすべきかと思われます。 【理由】 実際に脆弱性リスクの影響を把握するためあには、具体的なリスクシナリオを知る必要がある。	いただいた御意見を踏まえ、リスクシナリオも考慮して全体構成などの見直しも含めて記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	17-5	法人	第2章	フレームワークの図7には、対策の前段に「守るべきもの」「セキュリティリスクの洗い出しという脅威分析を考慮した記載がありますが、3章では、対策のみ列挙される形式となっており、本フレームワークの利用方法がイメージできません。P.11記載の「守るべきもの」の洗い出し、「セキュリティリスクの洗い出し」は個社で別途実施した上で、対策を検討する段階でのみ使用されることを想定しているのでしょうか。 【理由】 3章では対策のみが列挙される形式であり、フレームワーク図７の構成図と不整合があることから本フレームワークの利用方法がイメージできないため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、具体的な活用については、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、検討してまいります。
	17-6	法人	第3章	3章全体に言えることですが、IoT推進コンソーシアムで策定された「IoTセキュリティガイドライン」との対応付けが明示されておりません。ガイドラインで提示されている項目（指針や要点）と、本フレームにおける対策との対応関係をあわせて示すことが必要と思われます。 【理由】 「IoTセキュリティガイドライン」の方針に沿った具体的な対策案として、リファレンス資料として活用できるものになる。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	17-7	法人	第3章	参考文献に記載されている各ガイドラインから想定されるリスク、対策を抽出したでしょうか？本フレームワークにて提示された対策の選定理由を記載していただきたいと思います（例えば，社会的影響度の高い被害を防ぐという観点にて抽出した。など、本フレームワークでの対策を挙げた理由を明示。） 【理由】 設計から廃棄に至るライフサイクルにおいて、必要なセキュリティ対策が、どの程度網羅性があるのかを示す必要がある。その対策が最低限の内容なのか、必要条件であるのか、十分条件であるのかを明示する必要がある。	本フレームワーク作成にあたり、様々なガイドライン等を参照しており、ISO/IEC27001、NIST CSF、NIST SP800-171はその比較をお示ししてます。その他のガイドライン等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。 また、いただいた御意見を踏まえ、ライフサイクルの観点も含めて記載内容の修正を検討いたします。
	17-8	法人	第3章	3書の構成として、対策ごとに「リスク要因」と「リスク影響」が記載されておりますが、具体的にどのような脅威を防ぐための対策であるかを記載すべきかと思われます。例えば、JVNやCVE等のデータベースで公開されている実際に発生したインシデントを示しておくことが望ましいと思われます（類似意見［意見17-1］［意見17-2］） 【理由】 各項目がIoT機器への具体的な脅威と紐付けられ、対策の費用効果を見積もる上で有益な情報とするため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-9	法人	第3章 L2.001	対策ポイントについては「第三者機関による評価」のみが記載されていますが、「自己適合確認により安全性を評価したIoT機器」も追記すべきかと思われます。 また、中古市場で流通されたIoT機器に対する対策観点を盛りこみ、購買者が購入したIoT機器に不正改造がないことを、何らかの形で検証できる仕組みについても記載が必要と思われます。 【理由】 「対策の概要」の記載との整合性がとれていないため。	いただいた御意見を踏まえ、認証に関する記載内容の修正を検討いたします。
	17-10	法人	第3章 L2.004	本項目の記載については、オープンソースのソフトウェア等を利用した場合の考え方についても考慮すべきかと思われます。 【理由】 オープンソースを使用する場合、正規品かどうかの正当性基準が不明確であり、また、サプライヤーの識別や認証も行われていない可能性が存在するため。	いただいた御意見を踏まえ、ソフトウェアの信頼性も考慮して記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
17	17-11	法人	第3章 L2.005	本項目に記載されている「IoT機器の初期設定手順（パスワード等）」や「不要なサービスの停止」については、一様に守るべき事項ですが、製品分野毎には、本例以外にも守るべき初期設定（が）必要です。従って、一様に守るべき事例に加えて、製品分野毎に異なる初期設定方法・手法についても事例として示しておく必要があります。 【理由】 本ポイントの事例は、つながるIoT機器に必要な最低限のマナーとしての要件ですが、製品分野毎には、本例に加えて守るべき初期設定がありますので、その事例も記載が必要なため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-12	法人	第3章 L2.006 L2.007	［意見17-11］と同様に、本項目に記載されている対策は、一様にまもるべき要件に対する対策ですが、実際のIoT機器に適用するには、製品分野毎に本例に加えて守るべき初期設定がある点を追記する必要があります。具体的な事例として、製品分野毎に異なる方法を示しておくと必要があります。 【理由】 本項目に記載されている対策は、つながるIoT機器に必要な最低限のマナーであり、製品分野毎に本例に加えて守るべき初期設定があるため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-13	法人	第3章 L2.008	本項目に記載されている対策を、実際のIoT機器に適用するには、製品分野毎に本例に加えて守るべき要件を追記する必要があると思われます。具体的な事例として、製品分野毎に異なる方法を示しておく必要があります。 また、具体的な対策の一例として、デバッグポートを論理的に閉鎖する点も追加が必要であると思われます。 【理由】 本項目に記載されている対策は、つながるIoT機器に必要な最低限のマナーであり、製品分野毎に本例に加えて守るべき初期設定があるため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-14	法人	第3章 L2.009	本項目に記載の対策としては、サービス活動を一部あるいは全停止するという対策の追加が必要と思われます。 【理由】 サービス活動を一部あるいは全停止することで、システムやサービスに波及する影響を最小限に抑え、長期的視野に立った可用性を担保するという選択肢も考えられるため。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	17-15	法人	第3章 L2.011 L2.012 L2.013	本項目に記載の対策を適用する上で、対象となるIoT機器の規模や機能により制限を受けるため、前項のL2.001~L2.009とは区別し、製品分野毎に異なる要件として明示しておく方が良いと思われます。 【理由】 例えば、マルウェア対策についても、製品毎に具体的な対策内容が異なることが想定されるため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-16	法人	第3章 L2.013	本項目に記載の対策ポイントには、セキュリティパッチの正当性が確認できる手段や手続きを設ける旨を追加する必要があると思われます。 【理由】 情報セキュリティにおいては標準的な考え方であり、対策として追加が必要なため。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	17-17	法人	第3章 L2.014	本項目については、リモートアップデートサーバに対する攻撃も想定し、サーバ側のセキュリティ対策を示しておく事が必要と思われます。 【理由】 サーバ側の攻撃についても、実際のインシデント事例としており、対策の必要があるため。	サーバを含むサイバー空間のセキュリティ対策については、第3層で記載しています。
	17-18	法人	第3章 L2.014	本項目については、リモートアップデートの実装が困難な場合の更新方法や対策についても、示しておく必要があると思われます。 【理由】 全てのIoT機器にリモートアップデート機能の実装が可能とは限らないため。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	17-19	法人	第3章 L2.015	本項目に記載の対策を適用する上で、対象となるIoT機器の規模や機能により制限を受けるためあ、前項のL2.001～L.009とは区別し、製品分野毎に異なる要件として明示しておく方が良いと思われます。 【理由】 例えば、マルウェア対策についても、製品毎に具体的な対策内容が異なることが想定されるため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-20	法人	第3章 L2.018	本項目の対策ポイントに記載の内容は「L2.006」、「L2.008」、「L2.012」に記載されているホワイトリストによる対策と同様なものであり、IoT機器に共通して適用可能な対策と、製品分野毎に必要な対策を区別して記述する方が、理解しやすいのではないかと思われます。 【理由】 本項目の「対策の概要」に記載されている内容は、実際には対象となるIoT機器によって対策が異なることが想定されますが、最低限守るべき要件としては非常に重要なポイントであり、上記のように明確な対象の区別と対策の説明が必要なため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-21	法人	第3章 L2.019	本項目に記載されている対策は、実際のIoT機器に適用するためには製品分野毎に、本例に加えて守るべき要件がある点を追記する必要があると思われます。具体的な事例として、製品分野毎に異なる方法を示しておく必要があります。 【理由】 本項目に記載されている対策は、つながるIoT機器に必要な最低限のマナーであり、製品分野毎に本例に加えて守るべき要件があるため。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	17-22	法人	第3章 L2.020	本項目に記載されている対策ポイントについては、IoT機器からの異常通知が妨害されるリスクを考慮した対策についても、追加する必要があると思われます。 【理由】 情報セキュリティにおいては標準的な考え方であり、対策として追加が必要なため。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	17-23	法人	第3章 L3.001	本項目に記載されている対策の概要については、自己適合確認により安全性を確認したサービスサプライヤーの選択についても、追加すべきであると思われます。 【理由】 IoT機器を用いたサービス事業は多種多様であり、今後も多くのサービスサプライヤーが登場し、評価要件についても随時アップデートが必要が必要なため、既存の認証制度は不向きであると想定されます。従って、例えば、製品毎、業界毎に柔軟にサービサーの安全確認ができる仕組みが必要であると考えます。また、第三者機関による評価は、コスト的、時間的に事業への足かせになることも想定されるため、「IoT機器の導入での対策」と同様に自己適合確認により、サービスサプライヤー側での評価を促進することが肝要であります。	いただいた御意見を踏まえ、自己適合確認の利用に関して記載内容の修正を検討いたします。
	17-24	法人	第3章 L3.001	対策ポイントについては「第三者機関による評価を経て安全性を確認された製品・サービスを提供しているサプライヤー」のみが記載されていますが、対策ポイントに「自己適合確認により安全性を確認されたIoT機器やサービスを提供しているサプライヤー」も追記すべきかと思われます。 【理由】 「L2.001 セキュリティ対策が施されたIoT機器の導入」の記載との整合性がとれておらず、また、L3.001の［意見17-22］で記載した理由からも、追加が必要と考えられるため。	いただいた御意見を踏まえ、自己適合確認の利用に関して記載内容の修正を検討いたします。
	17-25	法人	第3章 L3.001	対策ポイントについては「企画・設計段階において実施する要件定義・設計の結果を第三者機関がセキュリティの観点から評価」と記載されていますが、対策ポイントに「自己適合確認により安全性を確認する」を追記すべきかと思われます。 【理由】 「L2.001 セキュリティ対策が施されたIoT機器の導入」の記載との整合性がとれておらず、また、L3.001の［意見17-22］で記載した理由からも、追加が必要と考えられるため。	いただいた御意見を踏まえ、自己適合確認の利用に関して記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	17-26	法人	第3章 L3.010	本項目に記載されている対策ポイントについては、IoT機器からの異常通知が妨害されるリスクを考慮した対策についても、追加する必要があると思われます。 【理由】 情報セキュリティにおいては標準的な考え方であり、対策として追加が必要なため。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	18-1	法人	全体	サイバー×フィジカルという名称にするのであれば、 IoT 以外のフィジカル環境における対策への言及も必要ではないか。 【理由】 本フレームワークの趣旨には賛同するが、グローバルでの活用を前提とするのであれば、physical という単語の意味を日本独自定義で進めるべきではない。サイバーと対をなす単語、例えば現実空間を意図するのであれば、RealSpace が妥当な単語ではないか。	フィジカル環境に対する対策は、第一層で記載しています。 また、NISTでもphysicalを使って使用しており、本フレームワークでも同様にphysicalを使用しています。
	18-2	法人	全体	海外の既存フレームワーク（例：NIST のFramework for Cyber- Physical Systems）との対応関係を明示すべき。 【理由】 フレームワークの策定意図に照らして、既存のフレームワークとの対応関係を明示しない内容では意味が無いと思われる。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、その他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	18-3	法人	全体	本文書の形式は「フレームワーク」と呼ぶには不適切ではないか。 【理由】 第２章だけがフレームワーク的な内容となっているが、わずか6 ページでその概念や価値を伝えることに無理があり、わかりにくい。セキュリティフレームワークと言えば、NIST のサイバーセキュリティフレームワーク、ISMS、METI/IPA のサイバーセキュリティ経営ガイドラインなどがあるが、それらと比較しても内容が薄く、フレームワークと呼ぶのであれば、条件に応じて共通して使えるような考え方を明示し、内容をわかりやすくして充実すべきである。	本フレームワークは、NIST CSF等との比較も行いながら、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示する目的で策定しております。
	18-4	法人	全体	本文書全体を通じて、「データ」と「情報」の２つの用語の使い分けが不適切である。また、データの定義が「フィジカル空間にて収集された情報、及び共有・分析・シミュレーションを通じて加工された情報」とされていることに違和感がある。 【理由】 本フレームワークが社会全体を対象に適用することを意図していることを踏まえると、こうした用語の使い方は不適切ではないか。本来「データ」と「情報」は異なるものである。例えば、個人情報保護法では個人情報と個人データは区別されているし、IoT ではセンサーからの生データとそれらを分析等して価値のあるものとして加工された情報は、それぞれリスクが異なるはずで、それを全て「データ」として扱うことに違和感がある。	いただいた御意見を踏まえ、「データ」と「情報」の使い分けも考慮し記載内容の修正を検討いたします。
	18-5	法人	第2章	記載されているフレームワークを活用することで、競争力の強化につながるという主張を行うのであれば、その根拠を示して欲しい。 【理由】 フレームワーク案から競争力の強化につながることが読み取れない。	P.7に示すように、本フレームワークでは、「Society 5.0」型サプライチェーン（価値創造過程）における新たな付加価値を創造する活動領域のセキュリティ上のリスクを洗い出し、対処方針を提示しています。本フレームワークを活用することで、「Society 5.0」型サプライチェーンで創出される新たなサービス・製品の提供を各事業者が適切なセキュリティ水準を持った適正な水準の投資によって実施でき、競争力の強化につながると考えています。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	18-6	法人	第2章	各対策の中にある、「構成要素毎の対策例」からオペレーションレベルで活用できることを理解できない。どのようなオペレーションを対象としたものかを網羅的かつ具体的に説明すべきである。 【理由】 各対策の中にある、「構成要素毎の対策例」はあくまで例でしかなく網羅性も具体性も満足しておらず、オペレーションレベルでの活用をイメージできない。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	18-7	法人	第2章	フレームワーク案の内容ではコストをイメージできることを理解できない。 【理由】 記載の中ではコストをイメージできる表現は一切ない。また、セキュリティレベルを保ったままでコストを圧縮できる記載も一切ない。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	18-8	法人	第2章	３層構造で整理する理由、根拠、メリット等をわかりやすく説明すべき。 【理由】 これからの産業が、フィジカル空間とサイバー空間の境目をいかに見えなくするかという方向に進むことが明らかである中で、フレームワークとして、各々を分割して枠にはめることは設計上の柔軟性を制約するなどのデメリットを産むことも考慮する必要がある。セキュリティ上の必然性があるのであれば、それをきちんと説明し、納得してもらわなければフレームワークを活用してもらえないのではないか。 フレーム案の内容では、１．企業間のつながりと２．フィジカル空間と３．サイバー空間という事業と物理を対比した定義の意味がまったく分からない。さらに、従来型サプライチェーンという表現があるが、従来型ではないサプライチェーンが２層、３層の事を言っているわけではないため、３層の対比自体に意味がないように思える。	いただいた御意見を踏まえ、三層構造に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	18-9	法人	第2章	６つの構成要素で整理する理由、根拠、メリット等をわかりやすく説明すべき。 【理由】 フレームワーク案からは、付加価値の創造に関与するものが、この６つである根拠が理解できない。 「付加価値の創造に関与する物が明確になれば、オペレーションで活用される」という根拠も不明である。また、付加価値の創造に関与するもの毎に、セキュリティ対策を行う事の蓋然性も不明である。６つの構成要素の定義がないため、対策例の説明の粒度がバラバラである。また、図６で何を説明したいのかも分からない。	いただいた御意見を踏まえ、6つの構成要素に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	18-10	法人	第2章	「指針を示す」のであれば、指針に相当する内容を記載すべき。 【理由】 対策の中では「例」となっており、サンプルレベルに過ぎず、指針として利用することは困難である。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。

NO		提出者 （種別）	該当箇所	御意見	御意見に対する考え方
	18-11	法人	第2章	次のように修正すべきと考える（第3 層は変更なし）。 ［第1 層］ 現行 企業間のつながり（従来型サプライチェーン） 修正 フィジカル空間（現実社会）におけるつながり ［第2 層］ 現行 フィジカル空間とサイバー空間のつながり 修正 フィジカル空間とサイバー空間との結節点（チャネル） 【理由】 本文書における三層は、記載内容から次の内容を表象していると解釈できる： （第1 層：フィジカル空間） 実体：現実社会 セキュリティ対策：これまでのIT セキュリティにおける管理的対策（ルール、契約、運用時の対策等）、物理的対策 （第3 層：サイバー空間） 実体：コンピュータシステムやネットワークの中に広がる仮想空間 セキュリティ対策：これまでのIT セキュリティにおける論理的対策、技術的対策 （第2 層：第１層と第３層の結節点（チャネル）、情報の変換装置） 実体：サイバー空間から見たフィジカル空間（現実社会）への入力（センサー（観測装置）、ICT 入力装置、受信機）、出力（作用器（アクチュエーター）、制御装置、ICT 出力装置、発信器） セキュリティ対策：いわゆるIoT セキュリティ（これのみで網羅できるわけではない） 上記と照らして第2 章の記載内容を見ると、第１層のフィジカル空間と第３層のサイバー空間はイメージしやすいが、第２層の捉え方（フィジカル空間とサイバー空間のつながり）が分かり難いように思える。第２層を第１層や第３層と同じような独立の空間として記述するのではなく、第１層と第３層の結節点（チャネル）であることが判るような表現が良いのではないか。 また、第１層のフィジカル空間と第３層のサイバー空間には、それぞれにその層内での横の「つながり」（connected）が示されているが、第２層の定義も同じように「フィジカル空間とサイバー空間のつながり」と書いてしまうと、何か第２層内での横の「つながり」あるように感じられ、違和感がある。さらに、第１層を「企業間のつながり」としているが、「Society5.0」を企業に限定する必要はない。B とC とP（Public）がその区別も曖昧にネットワーク状につながると考えられるので、「サプライチェーン」という用語も限定的であり、第１層の定義としては不要ではないか。	いただいた御意見を踏まえ、三層構造に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	18-12	法人	第2章	「三層構造アプローチの意義」における第2 層にある6 個のループ状の矢印（図4、図7 も同様） 読者の誤解を招きやすいので、↑↓のように上下間を直線状の矢印で結ぶように表現すべき。 【理由】 図5 の第２層において、「転写」と書かれたループ状の赤い矢は、上下間の「転写」を表現するものと 理解するが、何か層内でデータの授受が行われているように見える。	いただいた御意見を踏まえ、三層構造に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	18-13	法人	第3章 L1.001 L1.002 L1.003 L1.009 L1.010 L1.012 L3.022 L3.023	現状の定義では、ポリシーや体制は層に関わらず全てに関係するはずであり、第１層に割り当てるのは不適切ではないか。 【理由】 ルールに関する定義、運用に関する定義、技術対策に関する定義などオペレーションで活用されるものを目指すのであれば、人間の理解、動きに即した分類、並べ方とすべき。	いただいた御意見を踏まえ、セキュリティ対策の分類に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
18	18-14	法人	第3章 L1.001 L1.006	「統一的なセキュリティ対策」とあるが、組織内で統一されるべきなのは方針ではないか。 【理由】 組織で扱う情報やその利用環境は多様であり、対策はそれぞれの条件に応じて異なるのが一般的である。 同様の条件にも関わらず対策がバラバラになってしまうことを問題としているのであれば、その旨言葉を補うべきである。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-15	法人	第3章 L1.001	「事業におけるミッション、目標、活動に関して優先順位を確立し、共有した上で」とあるのを「事業におけるミッション、目標を共有し、活動に関する優先順位を確立した上で」に修正すべき。 【理由】 一般にミッションや目標には優先順位を付けない。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-16	法人	第3章 L1.001	「コンプライアンスを示す」とあるのを「コンプライアンスのための対策を示す」あるいは「コンプライアンスに関する姿勢を示す」などに修正すべき。 【理由】 「コンプライアンスを示す」では意味が通じない。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-17	法人	第3章 L1.001	「特に特権を持つ管理者は、」とあるのを「特にセキュリティ対策の責任者、特権を持つ管理者等は、」に修正すべき。 【理由】 「名ばかり責任者」が引き起こすガバナンス上の問題も重大であるため。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-18	法人	第3章 L1.002	他項目と同じ内容が示されているが、本項に相応しいのは「脅威に対する識別漏れやリスクに関する認識不足」等ではないか。 【理由】 他と同じ内容では読者に不親切であり、項目を分ける必然性を示すべきである。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-19	法人	第3章 L1.002	5 行目に「責任のある者が帯同し、部外者の行動を監視」とあるが、「適切な者が帯同し、部外者による不正な行動を牽制」くらいの表現に修正すべきではないか。 【理由】 「責任のある者」が意味するところが曖昧である。重要施設への入館権限を有する者はその時点で全員何らかの責任を負っており限定になっていないほか、責任者と解釈するのも無理がある。また、「行動を監視」という表現はやや過剰な印象を与える。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-20	法人	第3章 L1.002	19 行目の「サイバー保険活用」は「サイバー保険を活用」に修正すべき。 【理由】 脱字のため。	いただいた御意見のとおり、修正いたします。
	18-21	法人	第3章 L1.004 L2.001 L2.004 L3.001	サプライヤーの選定や機器の導入契約は、層ごとに分けられるものではないことを考慮した内容とすべきである。 【理由】 契約対象は機器、サービス（ネットワーク、ソフト等）それぞれ多様であり、契約形態も同様に購入、リース等多様であり、記載されているサンプルの内容で実用レベルの対策に活用するのは困難である。	セキュリティ対策は、三層構造の定義に基づき、分類していますが、いただいた御意見を踏まえ、サプライヤーの選定や機器の導入契約に関するセキュリティ対策の分類分けに関して、記載内容の修正を検討いたします。
	18-22	法人	第3章 L1.004	他項目と同じ内容が示されているが、本項に相応しいのは「保守契約を締結しなかったり、保守契約に適切なセキュリティ対策が盛り込まれなかったりすることで、対策漏れが生ずる」といった内容なのではないか。 【理由】 他と同じ内容では読者に不親切であり、項目を分ける必然性を示すべきである。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	18-23	法人	第3章 L1.004	「機器のサプライヤーとの保守契約手続き」とあるのを「機器のサプライヤーとの間で、適切なセキュリティ対策の実施が含まれた保守契約を締結する」に修正すべき。 【理由】 保守契約を締結しさえすればよいとの誤解を与える。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-24	法人	第3章 L1.005	「新たに発生したセキュリティインシデント」を「既存のルールで想定されていないような、新たな脅威に適切」のような内容に修正すべき。 【理由】 PDCA が回っていない組織でも、インシデントが発生すれば相応に対応するのではないか。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-25	法人	第3章 L1.005	2 行目「セキュリティインシデント」を「セキュリティ上の脅威」などに修正すべき。 【理由】 単に「新たなセキュリティインシデント」のみであれば対応は可能と見込まれる。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-26	法人	第3章 L1.005	2 行目の「必要に応じてセキュリティポリシーを見直す」を「新たな脅威への対策方針をセキュリティポリシーに反映させる」などの内容に修正すべき。 【理由】 必要に応じてセキュリティポリシーを見直すのは当然であり、例示になっていない。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-27	法人	第3章 L1.005	13 行目の「サプライヤーの行動を監視する」を「サプライヤーとの通信内容を監視する」に修正すべき。 【理由】 サプライヤーの行動を終始監視することは現実的ではない上に、サプライヤーに不快感を与える表現ではないか。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-28	法人	第3章 L1.007	「対策漏れを引き起こす機器」とあるのは「機器の対策漏れ」に修正すべきではないか。 【理由】 「対策漏れを引き起こす機器」という表現は、機器が自ら対策漏れを生じさせるわけではないので不適切である。	いただいた御意見を踏まえ、修正いたします。
	18-29	法人	第3章 L1.011	「生産活動に内部規則を整備」は意味がわからないので、「生産活動の記録に関する内部規則を整備」などに修正すべき。 【理由】 脱文ではないか。	いただいた御意見を踏まえ、修正いたします。
	18-30	法人	第3章 L1.012	多様な情報があるなかで、プライバシーに関する情報のみを外出しする趣旨が理解できない。 【理由】 産業を対象とするのであれば、営業機密、インサイダー等他にも考慮すべき多くの情報種類があり、プライバシー情報のみを保護すればよいという誤解を読者に与えかねない。	本年5月のGDPR施行に代表されるように、プライバシー保護に係る法規制等は、今後ともグローバルなレベルで強化されることが予想されるため、重要な項目として記載しています。
	18-31	法人	第3章 L1.013	他項目と同じ内容が示されているが、本項に相応しいのは「セキュリティ対策に関する情報共有が日ごろからなされていないことで、セキュリティインシデント発生等の際に必要な情報が不足する」等ではないか。 【理由】 他と同じ内容では読者に不親切であり、項目を分ける必然性を示すべきである。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者 （種別）	該当箇所	御意見	御意見に対する考え方
	18-32	法人	第3章 L2.001 L2.002 L2.003 L2.004	機能安全の定義がないため、何が言いたいのか分からない。また、導入関係の対策すべてで、開発ライフサイクルとしているが対策が同じであれば、分ける意味がない。 【理由】 機能安全を扱うのであれば、その要件についてあらかじめ定義する必要がある。対策についても条件に応じて変わってくるが、フレームワーク案では同様の記述に終始しており、読者に誤解を与える恐れがある	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-33	法人	第3章 L2.005	パスワードの定期的な変更に関する内容は削除すべきではないか。 【理由】 フレームワークやガイドライン毎にパスワードの定期変更に関する要件が異なるのは混乱を招くので、NISC の方針に合致させるべきである。	いただいた御意見を踏まえ、修正いたします。
	18-34	法人	第3章 L2.008	IoT 機器に関する対策として、「IoT 機器の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の対策を実施する」という内容は不適切である。 削除するか、他の内容に置換すべき。 【理由】 「施錠、入退室管理、生体認証等の導入」は限られた利用者による操作を前提とした業務用端末機器等を保護するための対策、「持ち物や体重検査等の対策」は操作者による物理的な持ち出し等への対策であり、いずれも操作者による操作を前提とせずに連続的に動作することも多いIoT 機器のセキュリティ対策としては不適切と考えられる。	「IoT 機器の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の対策」は、不正アクセス防止やIoT機器の持ち出し防止に対する対策として有効と考えています。
	18-35	法人	第3章 L2.009	ここでリスクとすべきは「サイバー攻撃等でIoT 機器及びその通信に障害が発生する」ことなのではないか。 【理由】 「故障や不具合が生じる」ことは機器として避けられないものであり、リスク要因として扱うのは不適切である。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-36	法人	第3章 L2.010	「IoT 機器を悪用され、不正IoT 機器が作成される」を「IoT 機器を不正目的で悪用される」などに修正すべき。 【理由】 「機器が作成される」というのはこの文脈ではおかしい。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-37	法人	第3章 L2.011	「遠隔からも確認できる必要がある」とあるが、「遠隔からも確認できることが望ましい」と緩めるべき。 【理由】 すべてのIoT 機器に対して遠隔からの確認機能を必須とするのは現実的ではない上に、目的や環境によっては不要な場合も想定される。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-38	法人	第3章 L2.012 L2.014 L2.015 L2.016 L2.017 L2.020	文末に「（可能な場合）」を補ってはどうか。 【理由】 すべてのIoT 機器において、こうした機能や対策が適用可能とは限らないため。	いただいた御意見を踏まえ、実施が望ましいけれども対策の実施が可能ではない場合があるものについては、「可能な場合」あるいは「することが望ましい」と追記するなど記載内容の修正を検討いたします。
	18-39	法人	第3章 L2.013	「必要に応じてIoT 機器に適用する」とあるのを「必要に応じて検証の上IoT 機器に適用する」に修正してはどうか。 【理由】 自らの環境にパッチを適用しても問題が生じないかの検証プロセスは、IoT 機器においてもきわめて重要である。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者 （種別）	該当箇所	御意見	御意見に対する考え方
	18-40	法人	第3章 L2.021	「IoT 機器が故障等により不正に動作し、作業員に危害が及ぶ、又はIoT 機器の破損が発生する」とあるのを「IoT 機器が本来担うべき機能を果たさなくなったり、定められた動作以外の動作を行ったりするようになる。」などに修正すべき。 【理由】 ここに示されているような影響（作業員への危害、機器の破損）は、いずれも大半のIoT 機器においては想定しにくいため。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-41	法人	第3章 L3.002 L3.006	第３層にある理由が不明。 【理由】 耐タンパー性とは物理特性であり、各層の定義と矛盾がある。	セキュリティ対策は、三層構造の定義に基づき、分類していますが、いただいた御意見を踏まえ、セキュリティ対策の分類分けに関して記載内容の修正を検討いたします。
	18-42	法人	第3章 L3.003	「特権を持つユーザーのシステムへのログイン」とあるのを、「特権を持つユーザーのシステムへのネットワーク経由でのログイン」に修正する。 【理由】 最近はクラウド利用が一般的であるので考慮する必要は少なくなっているが、サーバに直結されたコンソール端末で管理者がログインする場合は、二要素認証が利用可能とは限らないため。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-43	法人	第3章 L3.004 L3.005	識別と認証を分けて対策とする必要はない。また、認証と識別は第３層においてのみ求められるものではなく、全ての層で必要である。 【理由】 オペレーションを考えた場合、識別と認証はセットで対策を考えるべきものであり論理的な正確性よりも、実用を重視すべき	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-44	法人	第3章 L3.006	「IoT 機器、サーバ等の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の対策を実施する」という記載内容を見直すべき。 【理由】 p43 L2.008 についてコメントしたように、IoT 機器に対してはこうした対策は不適切と考えられる。サーバについては適切な場合もあり得るが、ポイントとして書くべき内容とは考えにくく、例示にとどめるべきである。また、マイクロSD カードの重量やサイズを考えると、持ち物検査や体重検査はもはや情報漏えいの防止手段として意味が無く、外部デバイスに書き出しを不可能とすることを主眼に置いた対策が必要である。	「IoT 機器の設置エリアの施錠、入退室管理、生体認証等の導入、監視カメラの設置、持ち物や体重検査等の対策」は、不正アクセス防止やIoT機器の持ち出し防止に対する対策として有効と考えています。
	18-45	法人	第3章 L3.007	提示されている内容は、現実でオペレーション可能な対策ではない。 【理由】 対策のポイントとして、動作前の検証や異常の事前定義をあげているが、現実にはこうした対応を事前に行うことは不可能である。	いただいた御意見を踏まえ、実施が望ましいけれども対策の実施が可能ではない場合があるものについては、「可能な場合」あるいは「することが望ましい」と追記するなど記載内容の修正を検討いたします。
	18-46	法人	第3章 L3.009 L3.010 L3.012 L3.016 L3.017	第３層で再掲する必要が理解できない。 【理由】 第２層で提示された内容を、第３層で再掲する意図がわからない。読者を混乱させる恐れがある。	セキュリティ対策は、三層構造の定義に基づき、分類していますが、いただいた御意見を踏まえ、セキュリティ対策の分類分けに関して記載内容の修正を検討いたします。
	18-47	法人	第3章 L3.010	「必要に応じてIoT 機器、サーバ等に適用する」とあるのを「必要に応じて検証の上IoT 機器、サーバ等に適用する」に修正してはどうか。 【理由】 自らの環境にパッチを適用しても問題が生じないかの検証プロセスは、IoT 機器やサーバ等においてもきわめて重要である。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-48	法人	第3章 L3.011 L3.017 L3.018 L3.019	自らの環境にパッチを適用しても問題が生じないかの検証プロセスは、IoT 機器やサーバ等においてもきわめて重要である。 【理由】 適切な鍵管理がなされなければ、暗号化の有効性が損なわれてしまうことを考慮した内容とすべきである	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	18-49	法人	第3章 L3.013	機能の分離ではなく、権限の分離を行うべきである。また、当該内容は第三層に限らず全ての層において必要である。 【理由】 内容が不適切ないし説明不十分と思われる。	L3.023において、サイバー空間における権限の分離については、記載していますが、いただいた御意見を踏まえ、その他のセキュリティ対策についても記載内容の修正を検討いたします。
	18-50	法人	第3章 L3.014	「組織内の」である必要性はない。また、何を目的に分離するのか記載がないと意味不明ではないか。 【理由】 組織内に限定する意図が理解できない。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	18-51	法人	第3章 L3.020	改ざん対策の対象を通信路上のみとするのは不適切ではないか。 【理由】 改ざんは、通信上だけではなく、あらゆる個所で起こりうる。	L3.020においては、いただいた御意見のとおり、通信経路上での改ざん防止について記載していますが、保管時についてはL3.002やL3.011、保守作業時についてはL2.014等、通信経路以外の改ざん防止についても記載しています。
	18-52	法人	第3章 L3.021	第２層で扱うべき内容ではないか。 【理由】 第３層で扱う意図が読み取れない。	セキュリティ対策は、三層構造の定義に基づき、分類していますが、いただいた御意見を踏まえ、セキュリティ対策の分類分けに関して記載内容の修正を検討いたします。
19	19-1	法人	全体	来るべき超スマート社内に向けて、このようなフレームワークは社会の安全性を高める上で非常に有用と考えており、本活動に賛同いたします。	本フレームワークに対する肯定的な御意見として承ります。
	19-2	法人	第3章	L1に示されるような情報管理体制の監査・認定制度の創設と、ベンチャーや中小企業も考慮し、より現実性を高めるため、評価を受けた第三者へ情報管理を委託することも対策例に盛り込むべきです。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	19-3	法人	第3章 L2.002	対策ポイントおよび対策例中のシステム開発ライフサイクルに、IoT機器の「製造」、「配布・設置」、「運用」および「廃棄」を含めるべきです。 （L2.005やL2.010の通り、IoT機器のセキュリティは機器単独の機能で保護できるものではなく、適切な製造、配布・設置、運用、廃棄が大前提となるため。）	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	19-4	法人	第3章 L2.010	遠隔地に設置されたIoT機器の場合、ネットワークなどを通じて、遠隔から安全に停止（廃棄）する方法が必要となります。対策例に例示するべきです。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	19-5	法人	第3章 L2.010	廃棄すべき情報をIoT機器中の着脱可能な耐タンパデバイス(L3.002参照)に格納し、廃棄時は同デバイスのみを破棄することで、必要なセキュリティを担保するといった方法も有効です。対策例に例示するべきです。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	19-6	法人	第3章 L2.011	ソフトウェアの起動順序確認機能や不正なソフトウェアの起動防止機能を、IoT機器中の耐タンパデバイス(L3.002参照)と連携させることで、安全性をより高めることが可能です。対策例中に例示するべきです。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	19-7	法人	第3章 L2.013	将来的な暗号アルゴリズムの危殆化に備えて、暗号アルゴリズムの移行が可能な機能を持つIoT機器の導入を推奨するべきです。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	19-8	法人	第3章 L2.013	NIST勧告にもある通り、安全性が確認された暗号アルゴリズムの選択と、暗号鍵の定期的な更新を推奨するべきです。（NIST SP800-57、CRYPTREC参照）	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	19-9	法人	第3章 L3.002	リスク要因として、盗難に加えて、悪意のある利用者、保守員、管理者による不正も加えるべきです。そのような不正に対しても、耐タンパーデバイスは有効に作用します。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	19-10	法人	第3章 L3.004	様々なシステムが有機的に連携して動作するため、様々な体系のID（識別子）が混在することになります。システム間でのIDの相互連携が必要となることを明示するべきです。 なお、現在はIDの相互連携の仕組みが十分に練られていません。Society 5.0としてID付与またはその連携のルールが必要です。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	19-11	法人	第3章 L3.005	Society 5.0の世界では多数のIoT機器が連携するため、PKIベースの認証システムが効果的です（共通鍵ベースの場合、鍵配布が複雑かつ高トラフィックとなるため）。PKIの利用を、対策例または対策ポイントで例示するべきです。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	19-12	法人	第3章 L3.010	セキュリティパッチの更新は、盗聴・改ざんに十分な配慮が必要であることを明示するべきです（L2.014参照）。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	19-13	法人	第3章 L3.019	L3.018は通信経路の暗号化、L3.019は通信経路上を流れるデータそのもの暗号化を要求しているものと理解しておりますが、その趣旨が伝わりづらいです。対策例に例示するか、または、対策の概要を「通信経路との暗号化とは別に、情報（データ）そのものも暗号化して送受信する」などとするべきです。 ※IoT分野のセキュリティにおいて重要なのは、L3.018の経路暗号ではなく、L3.019の情報（データ）暗号化です。特に、本フレームワークが対象とするサプライチェーンが複雑に連携した社会では、通信経路全体の安全性を確認することが現実的に難しく、情報（データ）の暗号化が必須と考えます。	L3.018は通信経路の暗号化、L3.019は情報（データ）自体の暗号化と分けて記載していますが、いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	19-14	法人	第3章 L3.019	ここで利用する暗号鍵を、IoT機器またはサーバに接続された耐タンパーデバイス(L3.002参照)に格納することで安全性をより高めることが可能です。対策ポイントまたは対策例に明示するべきです。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	19-15	法人	第3章 L1.012	OECD8原則の内容に包含されているのかとは思いますが、包括同意、トレーサビリティ、オプトアウトといった機能面について盛り込むべきです。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	19-16	法人	第3章 L1.012	OECD8原則の原則3にて、「個人データを収集する目的を明確にし」とありますが、センサーデータを常時取得～流通するケースを検討した場合、フローデータのため、データ取得時点では目的が明確化されていないケースも考えられますので、包括同意に関する規定も検討してみる必要があります。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
20	20-1	法人	第3章 L2.001	１．L2.001に記載されているとおり、第三者機関による評価を取得することは、IoT機器にとって重要と認識しております。電気用品安全法でも製造輸入事業者は技術上の基準を満たし、PSEマークを表示したうえで販売しなければならないとしており、サイバーセキュリティにおいても基準を満たすことが重要であると考えます。加えて、第三者機関が評価および認証することは、セキュリティの高い製品を実現する上で有効であると考えます。 ２．さらに、評価・認証を取得したことをPSEマークのように表示することで、ユーザーがセキュリティ対策が施された製品であることを識別することができるようになると考えます。 ３．規格の例として、EDSEおよびIEC62443-4-2が記載されておりますが、ご承知かとは存じますが、アメリカではANSI/UL 2900 も作成・運用されておりますので、ご参考までに連絡させていただきます。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	20-2	法人	第3章 L2.004	４．L2.004にご提案されているとおり、模造品対策も非常に重要であると認識しております。評価・認証制度ならびに認証マークの表示が、模造品対策にも貢献することを期待します。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	21-1	法人	第3章 L1.011	対策ポイントとして、「ナンバーを付与する等」ではなく、「一意であることを示すためのID(識別子)や重要情報(秘密鍵、電子証明書等)を付与する等」とするほうが望ましい。 【理由】 モノの生産記録を管理し特定する上の前提となる「モノの識別」に関する記載がない。 特定の際には一意性が必要。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	21-2	法人	第3章 L2.005	対策ポイントとして、 「IoT機器に対し、強固なパスワードの設定、機器やサービスの間で使い回しのないパスワードへの定期的な変更」ではなく、「IoT機器に対し、証明書認証等や多要素認証等の高度な認証方式の設定、強固なパスワードの設定、機器やサービスの間で使い回しのないパスワードへの定期的な変更」とするほうが望ましい。 【理由】 以下に強固なものにしようとパスワードという仕組み上、脆弱な部分が存在するため、より高度な認証方式が設定できるのであれば望ましいため。 「L3.003 サイバー空間への不正ログイン対策」等では高度な認証に関しての記載がある。認証はヒトだけではくモノにも適用されるべき。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	21-3	法人	第3章 L2.006	「L2.006 IoT機器へのアクセス制限」ではなく、「L2.006 IoT機器へのアクセス制御」とするほうが望ましい。 【理由】 本文の内容には、本来アクセスすべきものではないアクセス元からの制限だけではなく、本来アクセスすべきアクセス元からのアクセスの許可（識別、認証、認可）も含まれため。より意味が広いアクセス制御とするほうがよい。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
21	21-4	法人	第3章 L2.011	「起動するソフトウェアの完全性を確認した」ではなく、「コードサイニングを利用し起動するソフトウェアの完全性を確認したり」とするほうが望ましい。 【理由】 完全性の確認の方法としては、https://www.ipa.go.jp/security/pki/075.html　にあるようにコードサイニングが有効であるため。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	21-5	法人	第3章 L2.014	「ソフトウェアの更新作業は、盗聴・改ざんに十分に配慮する」ではなく、「ソフトウェアの更新作業は、改ざん（コードサイニングによる完全性の確保）に十分に配慮する」とするほうが望ましい。 【理由】 一般的にセキュリティパッチは公開されているものである。（WindowsやOffice、各種アプリ等に対するパッチは誰でも入手可能である。したがって盗聴を考慮する必要はない（っというよりできない）。　改ざんに関しては、https://www.ipa.go.jp/security/pki/075.html　にあるようにコードサイニングが有効であるため。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	21-6	法人	第3章 L2.015	「搭載されているソフトウェアを確認する」ではなく、「搭載されているソフトウェアの完全性の確認や配布元の認証を実施する」とするほうが望ましい。 【理由】 「確認する」では具体性にかける。ここでの「確認する」は完全性や配布元の認証を意図していると考えられる。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	21-7	法人	第3章 L3.003	「二つの認証機能」ではなく、「二つ以上の認証機能」とするほうが望ましい。 【理由】 二要素に限定する意味はあまりない。参考　https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html 　　https://pages.nist.gov/800-63-3/sp800-63b.html　等の認証に関する標準ににおいても二要素よりは多要素と用いられていることが多い。	いただいた御意見を踏まえ、修正いたします。
	21-8	法人	第3章 L3.003	「二要素認証の１つは、耐タンパーデバイスを用いた認証を採用する」ではなく「二要素認証の１つは、耐タンパーデバイスを用いた認証を採用する。（なお耐タンパーデバイスは1つ目の認証を実施するデバイスとは別のデバイスであることとする。）」とするほうが望ましい。 【理由】 変更内容ができるだけすくないように意見内容を記載しているが、要はPC上の耐タンパーデバイスに証明書を保持している場合などはマルウェア感染によるPC乗っ取りに対しては無力であり、認証強度が高いとはいえないので、別のデバイスであるという記載があったほうが望ましい。（多デバイスや多経路などによる認証強化策全体に関する記載がされていれば望ましい。） 参考　https://openid-foundation-japan.github.io/800-63-3-final/sp800-63b.ja.html 　　https://pages.nist.gov/800-63-3/sp800-63b.html	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
22	22-1	個人	第3章 L1.002	＞重要施設への入館は、責任のある者が帯同し、部外者の行動を監視する。 については、増加・増大する内部の者の犯行及びその協力について把握・抑制するために、「また、内部者の特定エリア立ち入りについても監視・記録する。」とすべきであると考える。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	22-2	個人	第3章 L1.002	「組織」において、電磁波漏洩（第1層第2層両方に関係する問題と思われる。）についても考慮した機器を組織的に導入していく事について明記していただきたい。考えてみればすぐに分かる事であるが、構内全てをUTPケーブルを使いケーブルが目に見える・手でケーブルに触れる事も出来る様な形で構築した物理環境よりも、通信関係機器が全メタル筐体化されており光ケーブルLANや処理が適切にされたSTPケーブルを用いている方がテンペスト技術にはずっと耐性が高いはずである。その様な耐性を持つ体制が構築出来るかどうかは組織による決定如何にかかっているのであるが、明らかに政府はテンペスト技術対策を官民その両方に対して注意・指導すべきであるので、この様なサイバー・フィジカル両方の記述がなされるガイドライン的文書においては必ず電磁波対策についての記述を行っていただきたいと考える。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
23	23-1	法人	全体	和訳）IoT(Internet of Things)やCPS(Cyber Physical Systems)を現実世界に当てはめて運用するためには，プロセスの一部として現実世界のヒトを含んだ構造を考えなければならない(HITLCPS: Human-in-The-Loop CPS)．提案されている３層構造のフレームワークは「企業」までを含むもので、ビジネス・イノベーションの視点では満足できるものである。しかしながら、そのビジネスに巻き込まれ制御プロセスの要素となるヒト（HiTLCPSにおけるヒトの役割はセンサから集まるデータをシステムを用いて解析した結果に基づいて，制御対象の挙動を決定するインテリジェントコントローラであり、製品生産ライン労働者や製品利用者やその利用に関わる人々が対象）に関しての言及はなされていない。したがって、「サイバー・フィジカル・セキュリティ」がダイナミックに運用される場の議論を惹起するためのフレームワークを用意すべきである。 　また、現実世界の「ヒト」をシステムのプロセスの一部として含むには、システムが正常に動き続ける安全なシステム構造をも訴求するフレームワークであるべきであり、外乱（サイバー攻撃も含む）が発生しても安全なシステム構造を維持し続けるレジリエントなシステム構造を対策とするフレームワークであるべきである。 　更に、EUで制定されたEU一般データ保護規則（GDPR）を考えると、国際的なサプライチェーン構築にたいする「ヒト」の組み込まれ方を考慮し、「ヒト」のデータ保護（データ独禁法）の境界を設定することで対策範囲を確定できるフレームワークであるべきである。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	24-1	法人	全体	和訳）1.リスクに応じて権限を定める オーストラリア国内におけるサイバーセキュリティ政策で最も議論となるテーマのひとつが、権限である。CISOは特定の管理策を実装する決定をする際、しばしば困難に直面する。特定のカテゴリーに対するリスクを解釈し、指定する権限を誰が有するのかを定めること。日本の政府機関や民間事業者においても、将来的にこの議論が繰り返し実施されるだろう。我々はリスクをカテゴライズする権限を有する意思決定者や実行者にガイダンスを提供することが非常に有効だと考えている。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	24-2	法人	全体	和訳）2.リスクに関する共通見解の特定 オーストラリア政府のProtective Security Policy Frameworkでは、対象となるリスクのカテゴリーが、全政府機関に対して明確に定義されている。民間事業者が自身でリスクの閾値を定めている一方、政府の方針は部局に対してリスクの閾値を定義している。これにより、リスクに対する管理策のカテゴライズ方法について、全ての政府機関に対して有意な見込みを定めている。ドラフト版のフレームワークがセキュリティを確立し、管理する方法について重要で意味のある対策を示す一方で、政府のリスクマトリックスは、対策が実装に向かう際に、一貫性を持って定められることを確実にする(https://www.protectivesecurity.gov.au/governance/security-risk-management/Documents/Business-impact-levels.pdf)．。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	24-3	法人	全体	和訳）3.重要インフラ オーストラリアでは、最近になって、重要インフラを安全なものとする方法について、国家的な議論を開始したところである。オーストラリア政府は、国内の政府機関におけるリスクを定義する権限を持っているものの、政府内部の重要インフラの全てに対する権限を有しているわけではない。結果として、我々の議論は、民間事業者とのパートナーシップを利用して重要インフラを守るという方向に強く傾いている。今回のドラフト版のセキュリティフレームワークは、IoTと国家とのつながりの重要性を喚起すると同時に、多くの面でオーストラリアの先を行っている。しかしながら、フレームワークの核にあるサプライチェーンとIoTとの関係性は、重要インフラとの関連において、文脈により強く結びつく可能性がある。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	24-4	法人	全体	和訳）4.認定 本文書において詳細化されている対策は強く言及されており、セキュリティにおける真の変革を促す可能性があるが、一方で、追加のサポートを利用することができる。オーストラリアでは、誰が政府機関のシステムを監査する権限を有するのかという点について議論がなされてきた。オーストラリア政府では、監査を実施し、システムがセキュリティ基準に見合うものかを判定する権限を持つような個人を認定している。これにより、監査人が、質についての政府の期待を満たすことが確固たるものになる。また、政府が、トレーニングや、監査で用いられる基準を定義することができる。監査人もまた、政府に定期的に情報を共有し、主題の専門家(SMEs)として行動することができる。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	24-5	法人	全体	和訳）5.官民連携(PPP) 日本の政府機関のシステムについて私が最も賞賛していることのひとつとして、民間事業者との強力なつながりがある。本文書は、サイバーセキュリティに関して、国家全体によるアプローチを採っている点で野心的である一方、民間事業者へのてこ入れとなる可能性もある。私は、日本が共同サイバーセキュリティセンター(JCSC)を創設することを提案したい。オーストラリア国内では、民間事業者は政府と提携することが可能であり、これにより、より素晴らしい協働と情報共有が可能となる。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	24-6	法人	全体	和訳）6.行動計画 本文書は、日本のサイバーセキュリティの将来像について強力な見解を提供している。しかしながら、我々は、見解の確立に向けた重要なステップを定義することには非常に価値があると知っている。本文書は大胆だが、時系列に設定された日本政府の優先事項、将来像の実現に向けた重要なステップを見える化することで、国際的なパートナーにとってより有益なものとなるだろう。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。

NO		提出者 (種別)	該当箇所	御意見	御意見に対する考え方
	24-7	法人	全体	和訳）7.国際的なエンゲージメント 本文書は素晴らしいことに、国際的なサイバーセキュリティ規格の現実にフィットしている。しかしながら、私は、経済産業省が国際的なサイバーエンゲージメント戦略の策定にコミットすることを勧めたい。 上で議論した幅広いテーマがサイバーセキュリティの戦略的な問題に言及している一方で、より小さな内容を以下にリスト化する。 * 特定のサイバーセキュリティ規格の選択を考慮すること * 管理策の解釈的な力を定義すること(例えば、何が義務で、何が推奨事項なのかを明確にすること) * フレームワークの実現を可能にする立法権の概略を説明すること * 民間におけるセキュリティクリアランスについて考慮すること * サイバーインシデントの開示について特定すること * 非公開のドアセッションやブリーフィングが非公式に提供される様々な産業向けの委員会を設立すること * 戦略実施に責任を有する政府全体のCISOを任命すること * サイバーセキュリティに関する研究・イノベーションセンターを創設すること * 公共サービス分野において、サイバーセキュリティ人財の技術的なキャリアトラックを確立すること * サイバーセキュリティ分野において女性人財を活用すること * 成功を判定するためのメトリクスを確立すること * サイバー攻撃の中心的な報告システムを確立すること * 重要な用語を定義すること(「サイバーセキュリティ」とは何か？)	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	25-1	法人	全体	和訳）「対策(measure)」という用語は、下記のように、使用する場面により非常に様々な意味を持つ。 - 戦略(strategy) - プロセス(processes) - 対抗策(countermeasure) そのため、本文書が、特にこの分野の初心者にとって読みにくいものとなっている。 代わりに、戦略(strategy)、プロセス(processes)、対抗策(countermeasure)という用語を、文脈により使い分けることを推奨する。	いただいた御意見を踏まえ、用語の使い分けに関して記載内容の修正を検討いたします。
	25-2	法人	全体	和訳）オペレーショナルな対策と、技術的な対策が文書を通じて混在している。文書中で双方を明確に区別していただきたい。	いただいた御意見を踏まえ、運用的対策と技術的対策の区分に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	25-3	法人	全体	和訳）各対策について、誰が対策の責任を有するのか、誰が対策を実施するのかを示していただきたい。例えば、L3.010はパッチが存在する場合のみ実施が可能である。そのため、下記の通り対応することが求められる。 - 資産所有者は、パッチを適用する必要がある。 - 製品サプライヤーは、各層の対策において、タグによって可視化可能なパッチを開発、適用、配布する必要がある。	いただいた御意見を踏まえ、対策の実施者に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。なお、実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	25-4	法人	全体	和訳）推奨事項：各対策に、対策を適用する対象(資産所有者、製品サプライヤー、サービスプロバイダー等)に関する記載を追加していただきたい。	いただいた御意見を踏まえ、対策の実施者に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。なお、実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	25-5	法人	全体	和訳）国際規格ではあるけれども、IEC 62443が本文書では目立っていない。NIST文書等と同様に言及すべきである。Topic 3を参照のこと。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、IEC 62443などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	25-6	法人	第4章	和訳）相互信頼の創出が本文書の最終目的である。この目的が、本文書の冒頭でより目立つべきである。読者は文書を読み進める中で、上記の目的を知ることになる。そのため、4章を文書の冒頭に移動することを検討いただきたい。	いただいた御意見を踏まえ、「信頼の確保」に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
25	25-7	法人	全体	和訳）下記の内容に関する対策が重要であるものの、本文書においてはほとんど言及されていない。 - 信頼できるクラウド事業者の選定方法 - クラウド事業者の脅威、リスクの評価方法 - クラウドサービスを含んだセキュアなシステムの設計方法 上記に関して、より多くのアイディアを求めたい。	政府において、クラウドサービスの安全性評価について本年度から検討を開始する予定であり、その検討内容やいただいた御意見も踏まえて、本フレームワークの記載内容についても検討いたします。
	25-8	法人	第2章	和訳）主体間の信頼の創出が本文書の中心的な要素である。従って、2章の記述や、図5において、「信頼」がより目立つべきである。	いただいた御意見を踏まえ、「信頼」に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	25-9	法人	全体	和訳）「組織」には、製品製造者、システムインテグレーター、サービスプロバイダー、装置のユーザー等の様々な役割がある。これらの役割は、どの対策を適用すべきかを考える上で重要である。残念ながら、本文書では、上記に関して詳しく掘り下げられていない。	いただいた御意見を踏まえ、対策の実施者に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。なお、実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	25-10	法人	第2章	和訳）図6が何を意味するのか明確でない。	いただいた御意見を踏まえ、図6の記載内容の修正を検討いたします。
	25-11	法人	第3章 L1.001	和訳）「対策」という用語を、戦略(strategy)、プロセス(processes)に置き換えた方がよい。	いただいた御意見を踏まえ、用語の使い分けに関して記載内容の修正を検討いたします。
	25-12	法人	第3章 L1.001	和訳）事業者の対策状況を測定するために、KPIを定義することが重要であるが、どういうわけか、KPI開発の重要性が見落とされている。担当者が対策の進捗状況を計測可能である必要がある。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	25-13	法人	第3章 L1.002	和訳）組織的な対策と、技術的な対策を明確に区別する必要がある。	いただいた御意見を踏まえ、組織的対策と技術的対策の区分に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	25-14	法人	第3章 L1.011	和訳）非常に不明確な内容となっている。よりセキュリティに特化した内容とすべきではないか。この対策を扱うのは誰か。製品製造者か、あるいは製品のエンドユーザーだろうか。	いただいた御意見を踏まえ、対策の実施者に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。なお、実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	25-15	法人	第3章 L1.012	和訳）情報の正確な分類は重要である。従って、各ステークホルダーは最初に情報資産の分類を行うべきである。その上で、分類に従って正しい対策を適用すればよい。	情報資産の分類については、L1.002において、適切な区分を踏まえたデータの管理については、L3.022に記載しています。
	25-16	法人	第3章 L1.012	和訳）GDPRのような政府の法規制が既に存在しているため、「OECD8原則」では不十分かもしれない。既存法規制の遵守の確認が不可欠である。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。また、GDPRとの関係に関しては、その内容を確認しつつ適切な対応を検討いたします。
	25-17	法人	第3章 L1.013	和訳）擬似的なインシデントハンドリングを実施するような訓練が重要であると強調したほうがよい。	定期的な教育・訓練は、L1.006で記載しています。
	25-18	法人	第3章 L2.001	和訳）記載された対策のどちらを選択するかにより、全く異なるセキュリティレベルに至りうる。我々は、CEマーク等において、自己適合確認が広く濫用されていると考えている。自己適合確認は注意をもって扱わねばならず、有効性を維持するには、強い市場の監視が必要となる。よって、よい対策とは言えない。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	25-19	法人	第3章 L2.002	和訳）第三者がどのプロセスを遵守しているかを確認することは困難である。単体のIoT製品について、詳細かつ徹底した形でセキュリティの文書化を求めるほうが、より現実的な要件となるだろう。	いただいた御意見を踏まえ、実施が望ましいけれども対策の実施が可能ではない場合があるものについては、「可能な場合」あるいは「することが望ましい」と追記するなど記載内容の修正を検討いたします。
	25-20	法人	第3章 L2.003	和訳）セキュリティとは関係がありません。安全機能のない製品を安全性が要求される用途に用いるのは、一般的な法規制に違反しており、不可能である。この要件を省略することを推奨する。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	25-21	法人	第3章 L2.004	和訳）実施する対策は実施主体の役割によって異なるため、本要求事項を以下の2つに分割することを推奨する。 - 製品製造者を対象としたもの - 製品の顧客を対象としたもの	いただいた御意見を踏まえ、対策の実施者に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。なお、実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	25-22	法人	第3章 L2.012	和訳）IoT機器に対してウイルスチェックを実施することは可能だろうか。多くの機器では全く確認できないだろう。	いただいた御意見を踏まえ、実施が望ましいけれども対策の実施が可能ではない場合があるものについては、「可能な場合」あるいは「することが望ましい」と追記するなど記載内容の修正を検討いたします。
	25-23	法人	第3章 L2.014	和訳）主体によって実施すべき内容が異なるため、本要求事項を複数の要求事項に分割した方がよい。 - 製品サプライヤー - 製品インテグレーター - エンドユーザー 実装例：リモートアップデートを開始することは、アプリケーションによっては危険になり得る。最大限の注意をもって利用されねばならない。よって、一般性のある推奨事項ではない。	いただいた御意見を踏まえ、対策の実施者に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。なお、実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
26	26-1	業界団体	全体	和訳）全体を通して、我々は自主的なリスクマネジメントベースのフレームワークを確立しようとする経済産業省の試みを支持する。我々は、サイバーセキュリティに対するマルチステークホルダーアプローチこそが、セキュリティを確立しつつ経済活動を促進する最も効率的な手段であると強く信じている。当団体は、フレームワーク案を広く支持するが、フレームワークをより強化し、明確化の恩恵を受けられるよう、以下に示す特定の方法を提案する。	本フレームワークに対する肯定的な御意見として承ります。
	26-2	業界団体	全体	和訳）ひとつめの提案は、中小企業がどのようにフレームワークを活用するのかという点に関するものだ。提案されている草案における詳細な管理策のレベルが高いため、内部に高度なサイバーセキュリティの能力がない組織の利用可能性を下げている。中小企業の多くはサードパーティにセキュリティマネジメント業務を外注するだろう。我々は、貴省が、中小企業にもより利用しやすいガイダンスを開発し、サイバーセキュリティ機能をサードパーティに外注する場合における責任関係をより明確なものとすることを推奨する。	本フレームワークは、セキュリティ対策のポイントを整理し、セキュリティ対策の全体的な枠組を提示するものであり、具体的なセキュリティの要求水準を定めたものではございませんが、本フレームワークが実際にセキュリティ対策を実施するうえで活用できるものになるよう、いただいた御意見も踏まえ、具体的な対策例について、対策による効果やコスト等も考慮しつつお示しできるよう修正してまいります。 セキュリティ対策に関する具体的な要求水準等については、産業分野別の具体的な検討を踏まえつつ、分野横断的課題を相互にフィードバックし、分野に共通する対策を洗い出す等の取組を進めてまいります。
	26-3	業界団体	全体	和訳）第二に、産業界には、マルチステークホルダーフレームワークがビジネス上の実践として優れたベースラインであるという広い合意がある。当団体は、この点を継続的に米国政権に伝えてきた。我々はそのようなアプローチこそが、企業のサイバーセキュリティリスクおよび脅威をグローバルに管理するための礎となると訴えている。相互運用性が通商の観点からもたらす利益を超えて、サイバーセキュリティに対するマルチステークホルダーアプローチにより、国境を越えて最高レベルのサイバーセキュリティ対策を拡大し、全体的なサイバーセキュリティレベルを向上することができると確信している。我々は、本フレームワーク案についての国際連携の議論を賞賛する。その一方で、各種サイバー規制間の相互運用を促進するために、どのように政府が海外政府および産業界と協働するのかという点に対して、貴省がより詳細な戦略を策定することを推奨する。	いただいた御意見を踏まえ、マルチステークホルダーに関して全体構成などの見直しも含めて記載内容の修正を検討いたします。
	26-4	業界団体	全体	和訳）最後に、本フレームワーク案に関する日本政府内の調整が優先して実施されることを望んでいる。国内の異なる機関がサイバーセキュリティやデジタルエコノミーに関する競合するフレームワーク、乃至は規制スキームを策定する際、企業側は世界中で規制の不確実性に非常に頻繁に直面する。日本は、企業がそのような不確実性に直面することがほとんどないという点において世界的なリーダーである一方、我々は、経済産業省と総務省の間で、産業界のサイバーセキュリティへのアプローチ方法が少々異なっているということに気がついた。両者がアプローチについて歩調を合わせることで、日本におけるICT産業、サイバーセキュリティ産業の発展に対するリスクが緩和される助けとなるものと確信している。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
27	27-1	法人	全体	和訳）防衛・航空産業における日本の中小企業の一部は、OEMとの直接的な連携によりNISTの規制を回避して事業を実施できると考え、サイバーセキュリティ規制の回避方法の調査のため、複数のOEMとやりとりをしていると言われている(彼等は経済産業省やNISTの規制が日本国内からのみ課されるものと間違った理解をしている。)。しかし、日本国内外のOEMは、米国政府に関係する調達について、NISTの規制を遵守せずに事業を行うことが不可能だと認識している。NISTの要求事項に対する知識の有無に関わらず、一部の日本の中小企業は防衛・航空産業から脱落し、多くの中小企業はサイバーセキュリティに関するガイダンスに対応することで市場に留まるものと予想される。 サイバー/IT規制を回避するため動向を注視している中小企業にまつわる、現在と同様の状況が2008年頃、日本の銀行業界において発生している。当時、日本の投資銀行は、規制当局を米国連邦準備制度理事会(FRB)に切替え、その結果、FRBセキュリティ要求事項の対象となった。日本のメガバンクは、データセンターを含む重要なIT機能の多くを外注していたため、大きな関心が寄せられた。2010年までに、サプライヤーおよびベンダーに由来するITリスクに対処するため、FRBは全銀行がサプライヤーに関するリスクマネジメントプログラムを有することを義務化した。NIST SP800-171と同様、ベンダーは法令順守に関する自己適合証明が可能であった。しかし、自己評価は72頁にも渡り、英語のみ可能であった。この評価はFRBによって開発され、FRB監査・検査プログラムに組み込まれた。 当時800以上あった銀行向けサプライヤーの中で、中小企業は、自身がどの銀行のシステムにも接続しておらず、FRBのIT規制を遵守する必要がないと主張した。この議論は2008年から2010年のおよそ2年間続き、多くの事業ユニットおよびバックオフィスは、自己評価実施への経営資源の配分をサプライヤーに強制することを渋っていた。最終的に、FRBは、米国で事業を行う日本の銀行および日本で事業を行う米国の銀行を含む、全銀行が規制の対象となる旨を通知した。そこに例外規定はなく、全銀行に法令遵守証明の責任が課された。一部のサプライヤーは、セキュリティ要求事項に対応しなかったことを理由に銀行のサプライチェーンから外されることとなった。 NIST SP800-171の導入が、日本の防衛・航空産業において中小企業をめぐる同様の潮流となりつつある。規格は英語で公開され、最終的に、国防総省がOEMを通じて遵守を要求することになるだろう。追加の教育および支援がなければ、多くの中小企業がNIST SP800-171の110項目に対応することは至難の業となる。しかし、これこそが、中小企業が米国政府および、(米国政府と契約合意を得ている)OEMと契約合意を得られるかどうかを決める課題となる。）	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
28	28-1	法人	全体	和訳）フレームワークのエリアは、少なくとも説明では、広げられたのは、第2層（コンポーネントは、IoTデバイスであるサイバーフィジカルシステム）である。この層は、非常に複雑である。例えば、このフレームワークは、IoTデバイスを認証するか、IoTデバイスを（例えば公式に）分類することを望んでいる。集中化した認証はサイバーセキュリティのために必要であるが、どうやって取り掛かるか、IoTデバイス（例えば、とても単純なデバイス、スマートフォンのモーションセンサー）に幅広い範囲の機能性と性能を持たせることを理解することは難しい。もう一つの広範囲に起因する例は、元々IoTデバイスはユビキタスであるために生じるフィジカル・アクセスのブロックが難しいことである。したがって、おそらく、この節は、少なくとも特定の産業（例えば自動車）が、異なる面をもって対処すべきと言わなければならない。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	28-2	法人	全体	和訳）（産業の中でさえ存在する）非常に異なるIoTデバイスによって生じる困難のもう一つの例は、脆弱性の継続的な修正である。また、これは、手段がないか、倒産した企業によって製造された非常に単純なIoTデバイスに対して実用的であろうか？これはNISTの主要な懸念である。そして、我々は十分に古くて更新する気持ちはないが、現用のデバイスの例をすでに目にしている。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	28-3	法人	全体	和訳）信頼を確立するために：信頼できるサプライチェーンは、重要で日常茶飯的であるが、いくつかの点で防御的で、後ろ向きに見ている。我々は、「チェーン」のセキュリティが強くイノベーションに依存しているのを感じている－つまり、悪いアクターの前向きのイノベーション、これが、信頼できるチェーンの上で取り組むことに加えて、進出で攻撃的な面を与える。おそらく、このフレームワークは、これへの言及をすることができた。	本フレームワークに対する肯定的な御意見として承ります。
	28-4	法人	全体	和訳）最後に、このフレームワークは印象的な成果である、そして、これが詳述したものを見て新たな気持ちになった。技術的で、よくよく考えられている。標準、認証などが個別の産業でセットされるならば、それらの産業に「実施要請」するのは良いだろう。	本フレームワークに対する肯定的な御意見として承ります。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	29-1	業界団体	全体	和訳）当団体は、国家のサイバーセキュリティ政策および法制の発展に関連して、世界中の政府と密に協働している。その際、我々は、当該政策および法制が、サイバーセキュリティ脅威を効果的に抑制、管理し、市民のプライバシーおよび自由を保護する可能性を目撃してきた。 このような経験の結果として、当団体は" International Cybersecurity Policy Framework(国際サイバーセキュリティ政策フレームワーク)"を開発し、一貫性のあるサイバーセキュリティ政策のための推奨モデルを設定した。当団体のInternational Framework を本コメントに同封している。 要約すると、当団体のInternational Frameworkは、国家のサイバーセキュリティ政策を成功に導くような6つの最重要な原則を推奨している。政策は下記のようになされるべきである。 1. 国際的に認知された標準と整合すること 2. リスクベースで、結果に照準を合わせ、技術中立的であること 3. 可能であれば、市場駆動型のメカニズムを信頼していること 4. 柔軟で、イノベーションを促進すること 5. 官民連携に基づくこと 6. プライバシー保護を志向していること これらの原則による枠組みは、国家の包括的なサイバーセキュリティ政策をガイドするものであるが、我々は、当団体による枠組みがサイバー・フィジカル・セキュリティ対策フレームワークと非常に深い関係を有しており、我々のアプローチが共有すべきものだと信じている。 当団体は、サイバーセキュリティ、フィジカルセキュリティ両面からの社会全体としての対応改善、日本におけるあらゆる産業(サプライチェーン、雇用創出、社会において重要な役割を担っている中小企業を含む)の啓発を促すものと、経済産業省の試みを評価している。我々は、そのような試みが、信頼性のあるSociety 5.0およびコネクテッド・インダストリーズに対する日本のビジョンを実現するための基礎となると理解している。 我々は、フレームワークが、例えばサプライチェーン・セキュリティの重要性のような、重要かつ最新なセキュリティの話題にアプローチしている点、セキュリティ・バイ・デザインの概念および、そのIoTとの関連性を議論している点で、経済産業省に特に感謝している。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	29-2	業界団体	全体	和訳）フレームワーク案を改善するため、当団体は経済産業省が、サイバーセキュリティに関わる既存の国際規格および民間事業者の試みを、より強調することを推奨する。グローバルなサプライチェーンは数多くの国の事業者からなっており、国際的に標準化された政策およびプラクティスは、グローバルな事業者が国際的に最も優れたセキュリティソリューションを供給乃至は調達する上で、非常に有効である。民間事業者は、自発的に最善の対策を共有し、サプライチェーンおよび顧客基盤を通じたサイバーセキュリティを強化するために、コラボレーションする。フレームワーク案は、これら民間事業者による試みを、産業、社会を通貫したサイバー・フィジカル・セキュリティ強化の手段として利用することになる。 我々は、特定のセキュリティ上の考慮事項を議論する間に、フレームワーク案において複数の国際的に認知された技術標準を引用したことを賞賛したい。 しかし、フレームワーク案は、製品、プロセス、ビジネスプラクティスを、国際的に認知された関連基準と概念的に整合させる重要性をより明確かつ強く強調することにより、より改善されるだろう。更に、我々は、ISMS(ISO/IEC 27001)、CSMS(IEC 62443-2-1)、EDSA(IEC 62443-4-2)、ITSMS(ISO/IEC 20000)に関して、特定の記載場所の対策の例として、フレームワーク案によるリファレンスがあるとメモしている。しかし、フレームワーク案は、ISO/IEC 27103(NISTサイバーセキュリティフレームワークと整合した重要インフラのサイバーセキュリティに関するISO/IECにより最近リリースされたテクニカルレポート)、ISO/IEC 27034(セキュアな開発ライフサイクルに関する標準)のような他の重要な国際的認知のある標準への言及をオミットしている。 フレームワーク案が、国際的に認知された標準やベストプラクティスと矛盾している可能性のある、ローカルなサイバーセキュリティ要求事項の開発と実装を主張しているものとして解釈されないようにすることが重要である。既存標準への対応の不備により、追加の法令遵守のためのコストが生じるだけでなく、グローバルにシームレスかつ相互運用可能な標準規格のレジームにおける日本のリーダーシップを損なうリスクもある。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO/IEC 27103やISO/IEC 27034などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
29	29-3	業界団体	全体	和訳）我々には、フレームワーク案において推奨されている対策が、サプライヤー(製品の生産・製造者)や、コンシューマー(製品の購入者)のような異なる対象をターゲットとしているように見える。そのように、推奨対策が所与のシナリオで適用可能かどうかという点において曖昧さがある。例えば、L1.008とL1.009は、ユーザー側の組織が、インシデントを検知し、事業継続計画を実行するための仕組みを構築することに言及しているため、よりコンシューマー向けだろう。しかし、L2.006は、主としてサプライヤーにより実施され、コンシューマーは資格を確認する立場にいないような、アクセス制御による不正なログインの防止に言及しているため、よりサプライヤー向けだろう。L2.011は、よりサプライヤー向けの推奨策の例である。偽造ソフトウェアに対する対抗策は、コンシューマーではなくサプライヤーにより確立、実施される必要がある。	いただいた御意見を踏まえ、対策の実施者に関して全体構成などの見直しも含めて記載内容の修正を検討いたします。なお、実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	29-4	業界団体	全体	和訳）要求事項は、異なるIoT機器が異なる能力を有しており、すべてのIoT機器が要求事項に示される範囲の特徴および能力を実装できるわけではないという可能性を考慮に入れていない。この点と関係して、フレームワーク案にて提案されている様々な製品の特徴(例えば、L2.011における偽造ソフトウェアの識別、L2.013における脆弱性対策、様々なユーザーによりアクセス可能な機能群の搭載)は、どれだけの計算リソースが機器内に搭載されているかに依存する。能力の低いIoT機器では、これらの機能はハンドリングできない。	いただいた御意見を踏まえ、実施が望ましいけれども対策の実施が可能ではない場合があるものについては、「可能な場合」あるいは「することが望ましい」と追記するなど記載内容の修正を検討いたします。
	29-5	業界団体	全体	和訳）速いペースの技術的進歩、対応するサイバー脅威環境の進化を鑑みると、我々は、ロバストかつ自発的な、国際的に認知された技術標準にも通じたフレームワーク案を開発したという点で、経済産業省を賞賛したい。加えて、更なるフレームワーク案の強化、利活用の促進のため、経済産業省と協働することを楽しみにしている。我々は、フレームワーク案が厳格な処方箋として課されることが、逆効果になると信じているが、フレームワーク案は、ベストプラクティスの一環として大いに価値がある。ここで我々が提供した推奨により、フレームワーク案のインパクトを強化し、幅広い採用を促進することを意図している。	本フレームワークに対する肯定的な御意見として承ります。
	29-6	業界団体	第3章	和訳）当団体は、第1層にて、以下のポイントにアプローチすることを推奨する。 ・トレーサビリティ：サプライチェーンリスクマネジメントのベストプラクティスとして、事業者はすべての構成要素をパーツ単位で流通元へトレースすることができるということを確実にすべきである。 ・データセキュリティ：すべてのサプライチェーン上のデータおよびセンシティブな製品データは、格納時および移行時において暗号化その他の手法により保護されるべきである。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	29-7	業界団体	第3章 L2.002	和訳）当団体は、経済産業省が「セキュリティ・バイ・デザイン」をフレームワーク案に組み込んだことを賞賛する。ソフトウェアの世界にセキュリティ・バイ・デザインの原理を確立することで、より安全かつ脆弱性の少ない、よりよく機能するソフトウェアを生産することができる。また、ソフトウェアにおけるセキュリティ・バイ・デザインの採用を促進することで、どのような原則の業界全体での遵守を助けることができる。本セクションは、「セキュリティ・バイ・デザイン」の意味するところを、よりロバストに記載することで、強化することができる。その目的のために、本セクションは、ISO/IEC 27034(アプリケーションセキュリティ)を引用し、事業者がセキュリティをソフトウェアアプリケーション開発用、管理用のプロセスに統合する助けとなるガイダンスを提供すべきであろう。）	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO/IEC 27034などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	29-8	業界団体	第3章 L2.010	和訳）当団体は、本セクションにて、IoT機器の廃棄方法について議論するだけでなく、流通を維持する際、あるいは、製造者からサポートを得られなくなった際に必要となる、予防を目的としたIoT機器のリプレイスを実施するためのガイダンスも記載することを推奨する。）	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	29-9	業界団体	第3章 L2.013	和訳）当団体は、特殊な事情がない限り、機器が「パッチ対応可能」であるべきということを鑑みて、組織がIoT機器の調達検討において「パッチ対応可能性」について考慮すべきと特定することを推奨する。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	29-10	業界団体	第3章 L3.014	和訳）当団体は、ネットワークの物理的な分離は日本のビジョンであるSociety 5.0およびコネクテッド・インダストリーズを脅かし、しばしばセキュリティ強化とならないため、一般的に対策として勧めないことを経済産業省に推奨する。物理的に分離されたネットワークは、管理に非常に注意を要する情報のような特定のケースに限定されるべきである。加えて、物理的な分離に加え、物理的分離により生じるセキュリティリスクの緩和につながるような重要な機能が含まれるべきである。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	29-11	業界団体	全体	和訳）フレームワーク案が駆使し、言及すべき他の重要な国際標準がある。それゆえ、我々は、サイバーセキュリティリスクフレームワークを適用する際に既存標準の活用方法に関するガイダンスを提供するISO/IEC 27103や、ISO/IEC 27034のような、他の重要な国際規格を付録にリスト化することを推奨する。また、サプライチェーンリスクマネジメントに関する文書であるNIST IR 7622に言及することも助けとなるだろう。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO/IEC 27103やISO/IEC 27034などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	30-1	法人	全体	和訳）フレームワーク案に対する見方は、自身の製品・サービスおよび企業の環境に対して、直接的あるいはサードパーティ的なサイバーセキュリティリスクを管理してきた我々の経験に根ざしている。我々は、効率的なアプローチが、組織が優先順位化された手段でリソースを割り当てる助けとなるリスクベース・アプローチであることを学んでいる；脅威と技術が急速に高度化しているため、リスクベース・アプローチは、組織が機敏かつ適応的となることを可能にする；翻訳可能で、水平的、垂直的なリスクマネジメントに関する理解を架橋し、経営層の意味のあるコミットメントを促進する；国際標準に基づいており、ますます相互依存的なものとなるエコシステムにおいて、産業間、地域間の相互運用性をサポートする。全体として、効率的なアプローチは、持続的な評価や、関連する要求事項遵守に加えて、付加的な改善を促進するような総体的なプログラムの確立を助ける。 経済産業省のフレームワーク案は、リスクベース・アプローチを採用した多数のコンセプトと対策を含んでおり、代表的な国際標準およびベストプラクティスとの対策のマッピングを提供し、リスクベースで、柔軟かつ相互運用可能なアプローチを提唱している。加えて、フレームワーク案は、ICTサプライチェーン、あるいは「バリュークリエイションプロセス」が、より流動的より動的かつ非線形的になるSociety 5.0においてどのように変化しているのかを構造化し、記載している。	本フレームワークに対する肯定的な御意見として承ります。
	30-2	法人	全体	和訳）企業のリスクマネジメントプログラムの枠内でフレームワーク案を運用可能とすることに注力すること フレームワーク案がバリュークリエイションプロセスの複雑性およびダイナミズムを反映している一方で、経済産業省の目標は、フレームワークが、現在、ERM専門家により最適に実施されている運用レベルで利用されることにある。サイバー・フィジカル・セキュリティ対策フレームワークを、組織間を水平的にリスク管理し、垂直的に上級管理層へリスクの状況を報告するERMプログラム内部に統合することで、リスクベース・アプローチを確かなものとすることができるだけでなく、セキュリティに関する意思決定および投資への幹部層の意味のあるコミットメントを促進することもできるだろう。多くの組織において、ERMプログラムは少数の重要なステップを含んでいる：類似性、帰結、優先順位の考慮した上での資産の識別およびリスクの評価；リスク管理および資産の保護(例えば、回避、移転、緩和、受容)；持続的に進化する脅威に対する検知および対応；リスク管理プロセスの効率性のレビューおよび修正。これらのステップは、リスク管理のライフサイクル、すなわち、運用環境の変化と共に、ERMの専門家がリスクに対する姿勢を強化のために活用可能な一貫したプロセスに貢献する。例えば、サプライチェーンはますます複雑化しているが、これらのステップは、リスクの評価、管理、脅威への対応に関連し続ける。 サイバーセキュリティ・プログラムを枠組みとし、ERMプログラムに統合するために存在する複数のアプローチがある。当社は、伝統的に、「防御/検知/対応」フレームワークを利用してきた；ISO/IEC 27103およびNISTサイバーセキュリティフレームワークは、5つの「機能」(識別/防御/検知/対応/復旧)を使用している。両方のアプローチともに多くのERMプログラムで利用されているリスク管理のライフサイクルに対応しており、フレームワークをより直截に運用可能なものとしている。 経済産業省は、3層アプローチと組織がERMプログラムの中で利用するサイバーセキュリティフレームワークとを架橋するために、フレームワーク案をより発展させるべきである。特に、経済産業省は、国際標準やベストプラクティスにおける管理策への対策のマッピングを完遂するだけでなく、ERMプログラムというレベルでの相互運用性、統合性も考慮すべきである。ERM専門家は、Society 5.0のバリュークリエイションプロセスへの理解を改善するガイダンスから利益を得られる。しかし、セキュリティ対策は、自身を機能させることを促すような方法で枠づけられるべきである。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
30	30-3	法人	全体	和訳）フレームワーク案の成果重視のアプローチを強化すること サイバー・フィジカル・セキュリティ対策フレームワークに対する成果重視のアプローチは、最も効率的に今日の環境におけるリスク管理プロセスおよび技術を決定し、そのプロセスおよび技術を変化するエコシステムおよび脅威環境に沿って高度化させつつ、組織が十分な柔軟性を有することを確実なものとするため、重要である。経済産業省のフレームワーク案が柔軟なアプローチに根ざしている一方で、成果重視のアプローチを強化することで、フレームワークを更によりよいものとすることができるだろう。 例えば、L1.013 "セキュリティインシデントの適切な情報共有"では、組織がセキュリティインシデントに関する情報をJPCERT/CCと交換することを要求している。ある組織は、対策を履行することでリスクに対する姿勢を強化することができるかもしれないが、他の組織はより効率的に、the Industry Consortium for Advancement of Security on the Internet (ICASI) や the Cyber Threat Alliance、あるいは業界ISACのような代替的な情報共有フォーラムを活用するかもしれない。JPCERT/CCを活用するよう処方するよりも、むしろ、フレームワーク案は、組織が考慮する際に関連するかもしれない多様な情報共有フォーラムに光を当てるべきである。 同様に、第2層と第3層において、経済産業省は、IoT機器のライフサイクルに関連した多くのセキュリティ対策を概説している。これらの説明の多くを、当社が最近リリースした調査「高度な安全性を有する機器の7つの特性」に根ざしたアプローチにまとめることができる。以下の表は、IoTデバイスを設計、開発、および展開する際に、IoTステークホルダーが考慮すべき特性および問いを明確に示している。 繰り返しになるが、L2.001 "セキュリティ対策が施されたIoT機器の導入"では、組織による第三者認証を受けているか、あるいは自己適合確認により安全性を確認したIoT機器の選定を要求している。しかし、第三者認証の例はEDSA認証(IEC 62443-4-2)が示されているだけで、第三者認証の取得を促進するため、他にもこの文脈でリスト化されるべき標準がある。ここでは、以下に2つの例を挙げる。 OPC財団：製造業において、OPC財団は、自動化された工業用の設定におけるセキュアなデータ交換を可能とするために企業が従う、OPC標準を開発した。OPC統一アーキテクチャーセキュリティ機能群のチェックを実施した後、ドイツ情報セキュリティ庁が、セキュリティに留意して設計され、システム上の脆弱性がないことを確認する。 Trusted Computing Group(TCG)：相互運用可能で信頼できるコンピューティングプラットフォームのための標準策定に従事する組織であるTrusted Computing Group(TCG)は、機器の識別および認証のため、Device Identity Composition Engine (DICE)アーキテクチャーを開発している。これにより、製造者は、ハードウェアにおいて基礎づけられたデバイス識別実現のために、シリコンゲートを利用することが可能となる。これにより、セキュリティハードウェアをIoT機器の遺伝子の一部としている。 IoT向けのセキュリティ対策が、IoTエコシステムを強化するために活用される標準と同じように、我々の原理、製品、サービスに根を下ろし続けると考えているため、経済産業省のフレームワークがERMプログラムの文脈で考えられるべきであるというコメントと同様に、当社は、経済産業省および日本の産業界との更なる意見交換を歓迎している。最終的には、IoTがそれほど真新しくないか、あるいは真新しい技術となり、組織運営に組み込まれる。この進化に伴い、組織は、IoTを主たるERMプログラムの一部と捉えるようになっていく必要があるだろう。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	30-4	法人	全体	和訳）ISO/IEC 27103へセキュリティ対策を組み込み、マッピングすることで、グローバルな相互運用性を駆動すること グローバルに相互運用可能なフレームワークを開発するという経済産業省の意図は明確かつ素晴らしいものであるが、セキュリティ対策をISO/IEC 27103にマッピングすることで、より大きなグローバルでの相互運用可能性に向けた重要なステップを踏み出すことができるだろう。ISO/IEC 27103は、より広範なリスク管理ガイダンスを活用し、業界間の関連性をサポートした上で、JTC1 SC27で開発された標準だけでなく、他のISOおよびIECにおけるサブコミッティの成果をも統合している。更に、ISO/IEC 27103は、これらの標準により、NISTサイバーセキュリティフレームワークから導入された機能、カテゴリー、サブカテゴリーだけでなく、経済産業省のサイバーセキュリティ経営ガイドラインから導入される原則および重要事項の実装が、どのように可能になるのかという点も例示している。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO/IEC 27103などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	31-1	法人	全体	和訳）我々はITおよびIoTシステムのセキュリティの間での境界を認識している。過去に多くの問題がITからの要件をIoT上で使うことから起こっている。フレームワークはセイフティとセキュリティを調和させることための大きな第一歩で、ItとIoTの間の異なる操作上の条件であり、『Society 5.0』を達成しているためにセイフティを増加させることに大変役立っている。そのようなシステムを監査して、テストすることに接した我々の経験は、より多くのガイダンスを産業に提供する必要があることを示した。とても歓迎するべきステップである。	本フレームワークに対する肯定的な御意見として承ります。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
31	31-2	法人	全体	和訳）しかし、IoTの範囲にいくらかの注意を払うべきである。IoTデバイスの範囲は、かなり広く、たとえば家庭用娯楽機器、医療インプラント、パブッリクな照明からスマートグリッドと原子力プラントまで、カバーしている。これに、IoTデバイスのためのどんな一般的なガイドラインでも、むしろ広く必然的にとどまらなければならなくて、特定のセクターでベンダーとオペレーターに彼らが必要とするガイダンスの量を与えることができない。これに、我々は、テクノロジーの、そして、セクターに特有のセキュリティ必要条件に関する、より多くの詳細な関連文書を楽しみにしている。我々が役に立つことがありえるならば非常にうれしい。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	31-3	法人	全体	和訳）国際標準（NIST CSF、NIST SP 800- 171とISO27001）との調整は、よく意図されている。つまり、フレームワークのアイデアが、日本の産業の市場価格を上げること貢献することに役立っている。	本フレームワークに対する肯定的な御意見として承ります。
	32-1	業界団体	全体	和訳）スコープと実装 フレームワークは、企業がどのようにフレームワークを使うかについて、明らかに述べている;しかし、どんなタイプのエンティティがカバーされるか、特定のセクターだけがカバーされるかどうかが不明確である。フレームワークの意図が、セクターに特有であるならば、我々は各々のセクターの特定の要件を含め、それらが義務的になるかどうかについて述べることを推奨する。当団体は、METIがフレームワークならびにインプリメンテーションの採用のためのスケジュールを示すことも推奨する。 このフレームワークは、フレームワーク草案から、対策の3つのセクションの代わりに、ガイダンスとインプリメンテーションの既存の基準を参照することで、3層の各々に関しては鍵となる高水準の原理に集中することによって、より役に立つガイダンスを企業に提供することができるかもしれない。このやり方は、ユーザーと組織にとって、フレームワークで定められた対策に限られていることなく、柔軟に原理に従って彼らのニーズと調整することができる。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	32-2	業界団体	全体	和訳）国際標準との提携（アライメント） 当団体は、フレームワークの多数のサイバー・セキュリティの推奨策が、現在の国際標準と矛盾するか、重複である点に注目する。ローカルな基準と国際標準とが平行した状況は、各種セキュリティ、および相互運用性の問題、ならびに高い適合コストを招く可能性がある。産業は、ローカルな監査機関から個々の多数のフレームワークとの調停を受けなければならないという状況よりも、グローバル・スタンダードと統合から利益を得る。国際的フレームワークとローカル・フレームワーク間の潜在的な不一致は、グローバル・スタンダードを採用することによって、または、確実にローカル・フレームワークが国際標準に相互に完全に合わせることによって、解決することができる。 フレームワークの対策の多くは、IoTセキュリティとインシデント対応/管理の要求に集中している。当団体は、IoTセキュリティとインシデント対応/管理に関する特定のガイダンスが、それらの関心と要件に言及する国際標準から提供されるか、採用されるべき提案する。そして、関係する問題に関して、より集中し、より直接的なガイダンスを提供するべきである。フレームワークは、IoTシステムに集中しなければならないだけでなく、サイバースペースの一部と考えられるすべてのシステムをカバーしなければならなくなっており、間違った安心感を与えることになってしまっている。	グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、その他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	32-3	業界団体	全体	和訳）フレームワークを、企業のためにより役に立つようにするために、当団体は、METIがリスク、または3層（図4、8ページ）に対するセキュリティコンサーン（関心事）の登録簿を含むように提案する。このようなリスクの登録簿は、組織にとって彼らのリスクアセスメントとMETIのサイバーセキュリティフレームワークの調節(アライン)と、彼らが、セキュリティ・イノベーションを抑える慣例的なセキュリティ対策を必要とすることよりも、現存するプラクティスの一部として取り組むことを確実にすることに役立つ。ISMSのような既存の標準の管理策の実装と実行により、識別され評価されるリスクに従って、(フレームワーク案と)類似する対策を実装することになる。	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
	32-4	業界団体	第3章 L1.001 L1.002	和訳）L1.001「セキュリティ・ポリシーの策定、体制の準備」に関して、当団体は、リスク影響が指定されるリスク要因に必ずしも関連があるというわけではない点に着目している。たとえば、セキュリティ・インシデントに対する対策の遅れの理由は、準備不足、不十分な資源、予期しないインシデントなどであることがあり得る。同様に、L1.002のリスク要因は、異なる表現だが、L1.001で概説されることと類似している。また、この節のリスク要因の原因は、必ずしも、とられた/とられなかったリスク対策に起因しない。当団体は、METIがガイダンスのアライメントと明快さを確実にするためにISO 27001のような既存の標準を見直すのを奨励する。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	32-5	業界団体	第3章 L1.003	和訳）L1.003「セキュリティ・インシデントへの対応の明確化」に関して、セキュリティ・インシデント・レスポンスの効果は、単に同じ場所の関連ドキュメンテーションとセキュリティ対策を持つことだけに依存しない。当団体はそのMETIに、十分な準備を既知と今後出現するセキュリティ・インシデントに対する準備のためにISO 27031（ICT Readiness for Business Continuity）を、組織内の既知のリスク問題に対処することであるISMSを確実にするISO 27001の参照と採用を提案する。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。 また、グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO 27031などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
32	32-6	業界団体	第3章 L1.004	和訳）セキュリティ・リスク要因対弱点 L1.004「サプライヤーとの保守契約」に関して、このリスク要因とリスク影響は、一般的であり、契約者とサプライヤーに、この節で推薦されるセキュリティ対策の採用を動機づけすることに直接関係しない。関連した脅威を識別することなく、L1.004のリスク要因に記載されている事がらは、過度の少なくされており、そのようにリスク要因と分類されてはならない。ISO 27001は供給者セキュリティについて述べている。そして、ISO 27036シリーズは情報セキュリティ・サプライヤーに焦点を当てている。加えて、ISO 27017と27018は、クラウド・コンピューティングに要求される追加セキュリティとプライバシー・コントロールに取り組んでいる。これらの標準は組合せの、第三者プロバイダーを使うことに関係しているリスクに取り組んでいる。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。 また、グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO 27017や27018などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	32-7	業界団体	第3章 L1.005	和訳）L1.005「セキュリティ対策のPDCA実装等」に関して、PDCAは組織が使える多くの管理システムズアプローチの1つである。ISO/JTC1は、これを認めて、したがってISO 27001と9001を含むすべての管理システム標準の規定された管理システム・アプローチとして、PDCAを取り除いた。それぞれ、インシデント準備とレスポンス能力に対する懸念は、既存のISO規格27031と27035で取り組んでいる。この節の内容は、非常に一般的で、関連した標準を直接参照すべきである。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。 また、グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO 27031やISO 27035などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	32-8	業界団体	第3章 L1.007 L1.008	和訳）L1.007「モノ、システム等の資産管理」について、ITIは、資産管理はISO 27001 ISMSの一部である点に着目している。組織がISO 27001 ISMSを実装することであるならば、この例で引用されるリスク要因は、取り扱われるだろう。さらに、関連した脅威が識別されないならば、これらの要因はリスク要因でない、潜在的な脆弱性と分類されなければならない。記述されたリスク影響は、潜在的リスクである、しかし、管理されていない機器は、マルウェア感染の唯一のソースでない。 同様に、L1.008「セキュリティインソデントの適切な検知・分析機能、手順の実装」において、記述されたリスク要因は、所定の環境の潜在的な脆弱性である;しかし、関連した脅威を識別することなく、それはリスク要因と分類されてはならない。記述されたリスク影響は、セキュリティ・インシデントを発見することの遅れから潜在的に生じることがありえる。そして、それは正しくセキュリティ・インシデントを識別することができないことと同じでない。推薦策のタイトルが示唆しているように、効果的なインシデント検知とレスポンスシステムは、機能とプロシージャだけより、多くのものを含んでいる。要素毎の対処の例は、システム要素を含むが、コンポーネント、データ（例えば、イベント・ログ）、関係するプロシージャをカバーしていない。そして、それら全ては、セキュリティ・インシデントを識別する組織の能力に関する懸念に総合的に対処するために重要である。より効果的にこの問題に対処するために、ITIはインシデント管理と処理ガイダンスのための標準ISO 27035の採用を提案する。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。 また、グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO 27035などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	32-9	業界団体	第3章 L1.009	和訳）L1.009「事業継続計画又はコンティンジェンシープランへの反映」に関して、記述されたリスク要因は、他の弱点から生じる可能性がある不足または弱さである（すなわち、「事業継続判断が適切に行えない」）。－たとえば、事業継続計画（BCP）の不足、BCPの不十分なテスト、意思決定者の優柔不断または知識の不足。「組織は、セキュリティ・インシデント発生時において、その影響について適切な判断を行うことが出来ない」というシナリオで参照されるリスク影響は、リスク要因の参照において言及されていない。当団体は、このセクションで概説される懸念と対処が、ISO 27031「ビジネス連続性のためのICT用意」とISO 27035「情報セキュリティ・インシデント管理」の採用を通して概説にされるよう推奨する。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。 また、グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO 27031やISO 27035などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。
	32-10	業界団体	第3章 L1.011	和訳）L1.011「生産したモノの記録の管理」に関して、記述されるリスク要因は、たぶん他の問題の結果である。そして、多くの他の要因に関するものである。L1.011のリスク要因として表現されていることは、このようなリスク要因と分類されるには一般的過ぎる。この節で推薦される方法では、根本の原因が発見されて、確実にサプライチェーンの保証が改善されるということには、なりそうにない。代わりに、当団体は、保安が関するサプライチェーンのセキュリティ懸念を取り扱うISO 27036を参照することを提案する。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。 また、グローバルハーモナイゼーションを実現するためにも国際規格等との整合性を取ることは重要であり、既にお示ししているISO/IEC27001、NIST CSF、NIST SP800-171との比較に加え、NIST SP800-53との比較及び修正を実施いたします。また、ISO 27036などその他の国際規格等との比較に関しては、その内容を確認しつつ適切な対応を検討いたします。

NO		提出者（種別）	該当箇所	御意見	御意見に対する考え方
	32-11	業界団体	第3章 L1.013	和訳）情報共有 L1.013「セキュリティ・インシデントの適切な情報共有」のリスク要因は、記述されているタイトルとリスク影響につながっていない。記述されたリスク要因は、リスクとは考えられてはならない;むしろ、それは、特定の脅威状況の下でリスクに終わることがありえるシステムの不足である。効果的なサイバー・セキュリティの脅威情報の共有は、セキュリティ運用マニュアルの作成やJPCERT/CCとの共有以上のことを要求する。それは、活用できる脅威情報に従って行動する能力を備えたエンティティ（実体）の間で、共有を容易にする相互信頼、または信頼のエコシステムを確立することを必要とする。加えて、そのようなシステムは、どんな種類の情報を共有すべきか、共有された情報がシェアリング実体（例えば、個人情報）の機密データや所有権を損なうことなく、どのように使われるかの理解を含めて、共有情報の適切な保護を確実に行わなければならない。 当団体は、また、METIに日本を含む多くの国で政府と産業によって採用されているISO 27001認証と、Systems and Organizational Controls（SOC）の連続的保証スキーム（SOC ｌおよびII）のような、既存のトラスト組織（例えば独立した第三者の監査とattestation証明の使用）を見直すことを推奨する。市場アクセスのバリアを増やし、否定的にイノベーションとビジネス効率にネガティブな影響を与え、企業に追加費用を引き起こす新しい認証システムを作成する代わりに、既存のスキームを採用し、広められなければならない。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
	32-12	業界団体	第3章	和訳）第3.2節は、IoTセキュリティに焦点を当てている;しかし、それは異なるIoTシステム・モデルと、それらのモデルに特有の関連した保護アプローチの採用について完全には述べていない。たとえば、スマート・ホーム、スマート・オフィス、スマート・ビルディング、スマート自動車、産業制御システム（ICS）のためのIoTシステムは、すべて、異なるリスクシナリオ、IoTエンド・ポイントのコスト、データと関係するネットワーク方の下で、異なるセキュリティ・アプローチを必要とする。 一般的に、この節で提案される対処は、あまり狭く、高いレベルに見えるので、それらは実際のインプリメンテーションに役立たないかもしれない。たとえば、L2.008において、IoTデバイスのためのフィジカル・セキュリティー対策では、デバイスがインストールされる物理的環境とメンテナンス目的のためのフィジカル・アクセスを検討することなく、監視カメラとロックと入口/出口コントロールの利用だけを検討することだけを提案している。 L3.014（「ネットワークの分離」）に関して、当団体は、物理的な隔離は、システムが非常に機微でローカル目的のために使われるケースに限るよう推奨する。物理的な隔離の使用は、他系のネットワークからの切断になる。当団体は、METIに、現用のIoTセキュリティ基準を採用の検討、または、異なるIoTシステム・モデルのための適切なガイダンスの開発するためのISO標準委員会との共同作業の検討を提案する。	本フレームワークは、セキュリティ対策の全体的な枠組を提示するものであり、産業分野共通の考え方や対策について記載しています。実際に取り組むに当たっては、産業分野別に必要なセキュリティ対策の内容が異なることも想定されますので、今後、産業分野別の具体的なガイドラインを策定する取組等を踏まえつつ、具体的なものになるようにしていきたいと考えています。
	32-13	業界団体	第3章	和訳）第3.3節「サイバースペースでの接続のためのセキュリティ対策」は、「接続」に焦点を当てているが、対処は広大で高レベルであり、より多くをサプライチェーンとIoTセキュリティに当てている。また、推薦されている対処は、すべてのシステム、デバイスと人々にインパクトを与える、全てが異なる方法でつながり、より広くIoTシステムのセキュリティとサイバー・セキュリティに広大な影響を及ぼす総合的な接続よりも、IoTデバイスの接続関連の問題に集中している。さらに、当団体は、L3.006が、L2.008の物理的なセキュリティ対策と重なる点に着目している。加えて、L3.008「サイバー空間の可用性維持」は、また、「サイバースペース」がどのように定められるか次第であるが、幅広い要件を意味している。組織とユーザーにとって、ビジネス継続性とシステム可用性の問題は、第1層でカバーされており、対策は、また、ISO 27001とISO 27031でも提供されている。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
	32-14	業界団体	第3章 L1.010	和訳）各種法令の対応 L1.010に関して、当団体は、違反が一つ以上の不当活動の結果である点に着目している。そのように、それはリスク要因と分類されるべきではない。このフレームワークの文脈に関してだけでなく、法規の遵守は、すべての組織に期待される。我々は、この節を取り除くことを謹んで提案する。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
	32-15	業界団体	第3章 L1.012	和訳）プライバシー保護 L1.012のリスク要因は、個人のデータ収集と使用という狭い面に集中している。サイバースペースの文脈では、個人情報はデバイスだけではなく、他のオンライン・システム、社会的ネットワーク、その他から集められる可能性がある。OECD プライバシー原則をプライバシー保護のための対処方法と検討するのではなく、むしろ、フレームワークが進めなければならない一組の原理の一部としての検討することが、重要である。	いただいた御意見を踏まえ、記載内容の修正を検討いたします。
33	33-1	法人	まえがき	和訳）すべての種類の産業用IoTシステムへのセキュリティ機能の導入は、セキュリティが安全性、信頼性、レジリエンス、およびプライバシーに関して適切になるように注意深く集中する必要があると強く感じています。 私は、本フレームワークを「サイバー・フィジカル信頼性フレームワーク」として再考することを提案したいと考えています。 私が提案している例として、以下の本フレームワークの序文の改訂を試み、トラックチェンジ版も添付しました。 私はこの変更の範囲について議論する準備が整いましたが、それは良い変化であり、あなたのフレームワークをNISTのサイバー／フィジカルシステム同様、Industrial Internet Consortium、Industrie Platform 4.0、および作業ISOの新しいIoTワーキンググループの作業に近づけると信じています。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。