「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

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
1	1	個人		「経済産業省商務情報政策局サイバーセキュリティ課」が提唱している内容では、「日本語及び英語」での提案を明記していますが、日本国の問題なので、外国語における英語等の提案は、不要と私は考えます。具体的には、英文の「Invitation for public comments及びThe Cyber/Physical Security Framework(Draft)」等の英語バージョンは、不要と考えます。要約すると、何の目的に対し、外国語の公文章を導入したのかを、明記するべきです。	セキュリティ対策は我が国だけの取組だけでは不十分であり、海外の制度等とも十分に調和を取りながら検討を進める必要があります。そのため、国内だけでなく国外からの意見を求めるために英語でのパブリックコメントを実施しました。
1	2	個人		経済産業省が明記している「Invitation（インビテェーション）」とは、能動的な概念での「招待する事、訪れる事」等と言う意味で有り、公募と言う概念では、受動的な別の意味に成り、英語の出来ない日本人が、創作した和製英語です。例えばですが、意見の提案を公募と言う意味の事を明記したいので在れば、「Suggestion（意見）」等が、妥当と考えます。「Comments（意見）」という概念も、「Suggestion（意見）」等という意味に対し、同類の概念と考えます。要するに、「Suggestion for public comments」等が、的確と考えます。	いただいた御意見は、今後、パブリックコメントを実施する上で参考にさせていただきます。
1	3	個人		「Society6.0（ソシエティー6.0）」の構造では、「宇宙居住（スペースコロニー）」の導入と考えますので、「5G（第5世代）」での導入における「サイバーフィジカルシステム（CPS）」から成る「センサー技術、ネットワーク技術、デバイス技術」とに対し、IoT機器に接続した場合での「ストレージ（記憶容量）」の通信における「フリーズ（動作停止）」での問題と、私は考えます。具体的には、「情報技術（IT）」の分野におけるクラウドコンピューティングから成る「ビックデーター（BD）」でのインターネット回線での「ISPサーバー（インターネットサービスプロバイダー）」及び電話回線での「SIPサーバー（セッションインテーションプロトコル）」が、融合する事と、考えます。「人工知能（AI）」の分野におけるエッジコンピューティングから成る「API（アプリケーションプログラミングインターフェイス）」での「HTTP（ハイパーテキストトランスファープロトコル）」が、融合する事と、考えます。要約すると、「HGW（ホームゲートウェイ）」に対し、有線LANでの「FTTH（光ファイバー）」及び「CATV（ケーブルテレビ）」が、「GPS（グローバルポジショニングシステム）」の機能における「衛星通信（サテライトシステム）」に対応が、出来る事で、3GPPから成る「GSM方式及びW-CDMA方式」に対し、無線LANでの「Wi-Fi（ワイアーレスローカルエリアネットワーク）」に、融合されると、アンテナチューナの場合では、「エリア（セクター）」の構造におけるアンテナの設置が、必要と考えます。要するに、「ゼネコン（土木及び建築）、船舶、航空機、鉄道、自動車、産業機器、家電」等の分野における構造の概念を描く事が、必要と思います。例えば、「5G（第5世代）」では、「衛星通信回線（サテライトシステム）、電話回線、（テレコミュニケーション）、インターネット回線（ブロードバンド）」での「NR（New Radio）」と考えます。「6G（第6世代）」では、「衛星通信回線（サテライトシステム）、電話回線（テレコミュニケーション）、インターネット回線（ブロードバンド）、テレビ回線（ブロードキャスト）」での「NA（New Audio）」と考えます。	今後の政策を検討する上での御意見として承ります。
1	4	個人		「フレームワーク（骨格）」の部分では、「サイバーフィジカルシステム（CPS）」での「情報技術（IT）」の分野におけるITネットワークでのクラウドコンピューティングに対して、サイバーセキュリティー対策が、必要と考えます。「人工知能（AI）」の分野におけるAIネットワークでのエッジコンピューティングに対して、サイバーセキュリティー対策が、必要と考えます。具体的には、「センサー、ネットワーク、デバイス」が、融合されて来ると考えますので、AIネットワークに対しては、Web上に対しての「HTTP（ハイパーテキストトランスファープロトコル）」通信における「API（アプリケーションプログラミングインターフェイス）」が、基準に成ると考えます。ソフトウェアーには、「アプリケーション、ファームウェアー、データーベース」等に対し、対応が出来るサイバーセキュリティー対策が、必要と考えます。要約すると、ネットワークとは、「データーベース（DB）」における「ビックデーター（BD）」から成る構造と考えます。	今後の政策を検討する上での御意見として承ります。
1	5	個人		「人工知能（AI）」の分野では、約1パーセントの「天才（ジェニー）」と約99パーセントの「凡人（オーディナリー）」の「区別（セパレーション）」が、付いて来ると、私は考えます。植物及び生物における知能の定義とは、「学習能力、認識能力、判断能力」と、私は考えます。人間における知性の定義とは、「言語性、創造性、判断性」と、私は考えます。具体的には、AIにおける「回答（アンサー）」での「データー（数値）」の「メカニズム（仕組）」での構造では、「統計学習（プロバビィリティーラーニング）」と「機械学習（マシーンラーニング）」の構造から成る事と、私は思います。（ア）統計学習における、統計の構造では、人間が、AIに対して、目的を導入する事で、過去のデーターから現在のデーターを、「ベイズ理論（ゲーム理論）」での「統計解析（アナライザー）」を導入したデーターを、人間が使用する構造の事と考えます。AIが、目的に対し、導き出した解答では、「根拠（ベイシス）」等は、無い構造です。（イ）機械学習における「ニューラルネットワーク（パーセプトロン）」の構造では、ソフトウェアーの「アルゴリズム（情報処理手順）」での「ディープラーニング（深層学習）」から成ります。ハードウェアーでは、「入力層、隠れ層、出力層」での「ノード（トランジスター回路）及びエッジ（バス配線）」の構造です。例えば、教師有り学習での「畳み込みニューラルネットワーク（CNN）」、教師有り学習での「再帰型ニューラルネットワーク（RNN）」、教師無し学習での「敵対的生成ネットワーク（GAN）」等の事です。チューニングテストにコストが、掛かる為の構造の事と考えます。AIが、目的に対し、導き出した解答では、「根拠（ベイシス）」等は、無い構造です。要約すると、人間が、約1パーセントの天才における様な高度に成らなければ、AIも高度化に対し、対応が、出来ない構造です。約1パーセントの天才が、高度にした構造では、約99パーセントの凡人を上回るAIの構造を、創作が、出来ても、約1パーセントの天才を、上回る構造のAIは、創作が、出来ないと、私は考えます。要するに、人間が中心と提唱しても、約99パーセントの凡人は、AIの構造における場合では、生物進化論の「遺伝と環境」で、自然淘汰されて行くと思います。	今後の政策を検討する上での御意見として承ります。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
2	1	企業	CPS.DS-5	「サービス活動を停止させないリソースの十分な(＝完全な)確保」は現実的には不可能なことであり、「サービス拒否攻撃等のサイバー攻撃を受けた場合でも、『保護あるいは影響を最小限とするリソース(ヒト、モノ、システム)を確保する】』とする。 【理由】 (D)DoS攻撃に対する完全な防御策は無いと考えているので、「リソースの十分な確保」はあり得ない。 また、監視・調整で「ヒト」の確保も必要。 （参考1) DDoS攻撃を完全になくすのは実質的に困難 https://japanese.engadget.com/2016/10/22/dns-ddos-twitter-spotify-psn/ （参考2) Akamaiが手を引いた事例 https://japanese.engadget.com/2016/09/26/620gbps-ddos/ （参考3) ボットネットだった場合、防御できたか不明。 https://japanese.engadget.com/2016/02/25/ddos-project-shield-google/	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.9 データセキュリティ CPS.DS-5
2	2	企業	CPS.DS-8	「ファイル閲覧停止」は一次的な拡大防止対策だと思われ、「適切な対応」の代表項目に適さないと考える。 ⇒ 自組織の保護すべきデータが不適切なエンティティに渡ったことを検知した場合、『影響の把握や拡大防止及び再発防止策』等の適切な対応を実施する。 【理由】 最初は「不適切に渡ったでデータ」を「ファイル閲覧停止」すると読んでしまった。 「適切な対応」の記述としては、一次的な拡大防止対策である「ファイル閲覧停止」ではなく、添付C(P.14/27)にある『影響の把握や拡大防止及び再発防止策』の方が重要かと考える。	元の記載、ご指摘の内容を含め、情報漏えい検知後の対応は、対策要件カテゴリーのCPS.RP以降で記載することが適切と考えますので、当該対策についてはCPS.RP-1、CPS.AN-1等を参照することとしたく存じます。
2	3	企業	CPS.PT-2	不要な各種ポートは「物理的に閉鎖」ではなく「物理的または論理的に閉鎖」とする。 【理由】 OSのポートを含んでいるため。また、物理的な閉鎖は、市販の専用器具であれば、誰でも購入できる価格帯のものもあり、ポート制御は可能であれば「論理的(ソフトウェア的対策)と物理的」の両方の対策の検討が必要と考える。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.12 保護技術 CPS.PT-2
3	1	個人		最終的な決定における参考とかいって、やることはもう決定してる前提で意見します こんな意見集めても時間の無駄だとおもいます、意見が通ったところで。 厚生労働省の不正のように、中の人間が不正しても責任を誰も取らないから何をやっても無駄だとおもいます。	パブリックコメントとして国内外の皆様からお寄せいただいた御意見を参考に、本フレームワークを修正しています。
4	1	個人	表2.1-4	第1層において想定されるセキュリティインシデント(1)(d)の以下は誤記と思われます。 誤）「・・・、危機の破損等・・・」 正）「・・・、機器の破損等・・・」	いただいた御意見のとおり、修正いたします。 修正箇所：（日本語版）表2.1-4
5	1	企業	CPS.AC-8	CPS.AC-8に『IoT 機器、サーバ等がサイバー空間で得られた分析結果を受信する際、及び IoT 機器、サーバ等が生成した情報(データ)をサイバー空間へ送信する際、双方がそれぞれ接続相手の ID(識別子)を利用して、接続相手を識別し、認証する』とあります。 これは情報の送信先、もしくは送信元を偽装することによる、情報の漏洩や偽の情報が混入するリスクに対する対策要件であると読み取りました。 一方、本フレームワークが対象としているネットワークにつながる「モノ」を考えた場合、用途によっては容易に悪意を持った人物に入手される可能性があります。 モノが自らを認証してもらうためには、内部のどこかに識別情報／認証情報を置く必要があり、これらの情報の実装方式によっては、ROMからの直接吸出しなどShack attack的な手法で入手される可能性があります。 識別情報／認証情報自体が不正入手されてしまえば、CPS.AC-8の対策要件は無効化されてしまいます。 こちらの観点からの対策要件として『識別情報／認証情報の安全な格納』の追加を提案いたします。	ご指摘いただいた通り、認証に用いるクレデンシャルのような重要情報は、物理的に十分な強度が確保されたハードウェアに格納することが望ましいと考えます。本フレームワークでは、ハードウェアに対する物理的な攻撃を想定し、CPS.DS-4、CPS.DS-7、CPS.DS-11等の対策要件を記載しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
6	1	個人	CPS.RM-2	CPS.RMの内容に関しては、 3.5.CPS.RMリスク管理戦略 自組織の優先順位、制約、リスク許容度、想定を定め、運用リスクの判断に利用する。 特に CPS.RM-2 ・リスクアセスメント結果およびサプライチェーンにおける自組織の役割から自組織におけるリスク許容度を決定する について、次項の 3.6.CPS.SC サプライチェーンリスク管理 企業等の優先順位、制約、リスク許容値、および想定が、サプライチェーンリスク管理に関連するリスクの決定を支援するために確立され、利用される。企業等は、サプライチェーンのリスクを特定、評価、管理するプロセスを確立し、実施する。 と比較すると、整合性の観点から 「自組織の役割から自組織におけるリスク許容度を決定する」 としてしまうことは、矛盾があるように感じる。	CPS.SCの説明文にもありますように、CPS.RMにおいて「サプライチェーンにおける自組織の役割から」決定される「自組織のリスク許容度」は、サプライチェーンリスク管理プロセス確立のための重要なインプットとなると考えられますので、いただいた御意見については、原案のとおりとさせていただきます。
7	1	個人	p.3 等	国民一般が分かるように、一般的でない用語については意味等を明記すること、また、カタカナ用語は極力使用を控えるようにすべき。 「バリュークリエイションプロセス」⇒「価値創造過程」　（初出P3） P3では、価値創造過程（バリュークリエイションプロセス）」と定義されているが、以降は「バリュークリエイションプロセス」が用いられている。これをすべて「価値創造過程」とすべき。	いただいた御意見も参考に、バリュークリエイションプロセスが価値創造過程を言い換えた表現であることが明確になるよう修正いたします。 修正箇所：はじめに 1.
7	2	個人	p.11 等	「プロシージャ」　用語解説を分かりやすく表示　（初出P11） P11 では注釈をつける：「プロシージャについては、表1.2.1（P16)を参照のこと） P16　表１.2.１の「定義された目的を達成するために一連の活動を定めたもの」の表現が曖昧。⇒ 「定義された目的を達成するための手続の体系」	いただいた御意見も参考に、プロシージャの定義を修正いたします。 修正箇所：第Ⅰ部2. 及び 表1.2-1
7	3	個人	p.14	「転写機能」は分かりにくいので「情報の転写機能」または「情報転写機能」とする。	いただいた御意見について、前後の文章から転写機能の対象は明らかと考えるため、原案のとおりとさせていただきます。
7	4	個人	p.30	「ハザード」は、用語解説に追加すべき。 ハザード：危害要因。事故や災害を引き起こす原因。ハザードに遭遇する確率に事故や災害の影響を乗じたものがリスクでもある。	いただいた御意見も参考に、修正いたします。 修正箇所：添付E (数字を挿入する)
7	5	個人	全体	生活者がステークホルダーとして重要な役割を果たすのがSociety5.0の世界であると考える。生活者に配慮した表記とすべきである。 具体的な個所と修正提案は以下の通り。 ア　図i-2（P2）　最下部に「生活者（Consumer）」を加える。 イ　図1.3-1（P19）　右端に「生活者（Consumer）」を加える。 ウ　図2.1-5（P28）　右端に「生活者（Consumer）」を加える。 エ　添付A　ユースケース１　右端に「生活者（Consumer）」を加える。	Society5.0の社会においては、生活者もステークホルダーとして重要な役割を果たすものと認識しています。いただいた御意見も参考に、図の一部を修正いたします。 修正箇所：図i-2, 添付Aユースケース 1
7	6	個人	p.13	第１層の説明、第二段落「企業のマネジメント」は「企業の情報セキュリティマネジメント」の方が表現の的確さや分かりやすさが高まる。	第1層の信頼性の基点である企業のマネジメントは、情報セキュリティマネジメントのみに限らず、企業のガバナンス等も含む広い概念であるから、原案のとおりとさせていただきます。
7	7	個人		リスクとリスク源の関係について説明がないため、ISO31000 をよく理解しないと、分からない。 P24　箇条書きの後あたりに、リスクとリスク源の関係について解説を付けてはどうか？（イメージとしては、「ISO/IEC27017　クラウドサービスのための情報セキュリティ管理策の実践の規範解説と活用ガイド」：日本規格協会：2017年10月10日、のP251の記述である。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第II部

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
7	8	個人	p.29	②の第二段落「フィジカル空間の動態を計測し、サイバー空間へデータとして伝送する機能を果たす機器」が具体的に何を指すか不明。 例示を加えるべき。「センサー」？	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第II部 1.1. 分析対象の明確化(三層構造モデルへの落とし込み) (2)
7	9	個人	図2.1-6	「ハザード要因」の意味が不明。「ハザード」は「危害要因」を意味するので危害要因要因となり意味が分からない。注釈等を削除するか、「リスク」または「リスク源」に置き換える。	いただいた御意見については、引用している他の文書(IoTセキュリティガイドライン等)との整合性確保のため原案のとおりとさせていただきます。
7	10	個人	p.30	③の第三段落「自組織のアクションにおける重要度」を簡潔な表現とすべき。文の初めの方に「自組織」とあるので、「組織」で意味が通じる。 また、組織は目的をもつ集団であり、組織目的に照らした重要度という概念がマネジメント上一般的である。 修正案：「組織自らが定めた重要度」	いただいた御意見のとおり、修正いたします。 修正箇所：本文第II部 1.1. 分析対象の明確化(三層構造モデルへの落とし込み) (2)
7	11	個人	図2.1-6	三層構造との関係が不明確なので、記述を変更すべき。 「攻撃は第三層から行われる。第二層のコントローラのぜい弱性を突かれ、不正な指令が生成され機器に送られる。機器における異常作動防止装置が不備な場合、災害が生じる。」というシナリオを図にしてほしい。 この場合、「攻撃」、「コントローラのぜい弱性」及び「機器の異常作動防止装置不備」がリスク源となる。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第II部 本文第II部 1.1. 分析対象の明確化(三層構造モデルへの落とし込み) (2)
7	12	個人	p.25, 48	IoTなどに係る処理はクラウドサービスを用いることが一般的である。クラウドサービスは第三層に位置するが、管理は第一層の物理的機器と同様に行う必要がある。この点について、補足することが望ましい。 ア　P25　最終段落の次に以下の文を挿入：なお、クラウドサービスを利用する場合、仮想マシン（仮想サーバ、仮想ネットワーク、仮想スイッチ、仮想ストレージ等）は第三層に位置するが、第一層の機器としてもリスク分析を行う。 イ　P48　文献リストの末尾に、クラウドサービスに係る注記を記載。 （注）クラウドサービスの利用にあたっては、ISO/IEC27001のAnnex Aの項番に従ったISO/IEC27017の項目も参照することが望ましい。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第II部 1.1. 分析対象の明確化(三層構造モデルへの落とし込み) (1) 本文第III部 3．対策要件 （2） 国内外主要規格との対応
7	13	個人		意見記載において本文参照がおこないにくいので、報告書はeGavの文字コードで作成すべき。	いただいた御意見は、今後、パブリックコメントを実施する上で参考の１つにさせていただきます。
8	1	団体	p.14 脚注3	現行記載では“インターネット接続を想定”とされているが、本フレームワークの内容を見る限りは、インターネットを使用しないＩｏＴ（例えば組織内の閉じた環境で使用するＩｏＴ）も多用されていると思われることから、記載の見直しが望ましいのではないか。 なお、「添付Ａ ユースケース」では、インターネット接続ではない事例が多数ある。また、「添付Ｅ 用語集」でも「ＩｏＴ機器＝汎用的な通信手段によりネットワーク接続して動作する機器」とされており、インターネットを想定した記載とはなっていない。	いただいた御意見を踏まえ、修正いたします。 修正箇所：第Ｉ部2.1.
8	2	団体	図1.2-4	「図1.2-4」は、それ以前の頁で文書にて述べられてきたコンセプトが初めて図で示されたものであるが、本フレームワークを先頭から読み進めてきた読者にとっては、何のケースを記載したものか分からず、また要素や層の重なりが多く理解が難しいことから、解説を付けるなどの充実を図ってははどうか。 一案として、「表2.1-1」（25頁）の整理区分を用いて、この「図1.2-4」を解説するなどが考えられる。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ｉ部2.2.
8	3	団体	表2.1-1	「第３層 - サイバー空間におけるつながり」の「分析対象」に関して、 第３層については、現行では“組織を越えたつながり”にフォーカスされたような記載となっているが、本フレームワークの内容を踏まえると“組織内におけるデータ流通（つながり）”についてもこの層に該当するものと考えられる。 しかしながら、“組織内でのデータの流通”については、現在、同表の第１層として整理されていることから、全体的な整合性を確認するとともに、誤解の無いように記載を見直す必要があるのではないか。 一案として、「組織内および、組織を越えて・・・」等とすることが考えられる。	いただいた御意見も参考に、修正いたします。 修正箇所：表2.1-1
8	4	団体	添付A	他分野のユースケースや本文中「図2.1-5」の抽象モデルと見比べた際、ビル分野については、 ・［ユースケース8頁］ 構成要素の配置の考え方が他分野と異なる ・［ユースケース9頁］ 分類のイメージが8頁の図と異なる （例えば、9頁ではサーバ類・統合ネットワークは3層に整理されているが、8頁の図では主に2層に配置されている） ように見受けられる。 本フレームワークでは、構成要素は複数層の機能を併せ持つこととされているため、各々分野における視点の置き方によって、他分野と異なるケースが作成されることは理解できるものの、多くの読者はユースケースを参照して本フレームワークの具体的なイメージを掴もうとするであろうことから、ケースの特徴やポイントを記載するなど、充実を図ってはどうか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付Aユースケース5

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
9	1	個人	p.19	各層の役割や守るべき機能について、層間のつながりをより重視して追加を行った方がよいように感じました。 具体的には、1層では各ソシキ自体の信頼性を確保することは従来からでも必要なことですが、これに加えて転写元となるデータを生成することも機能に加えるということはどうでしょうか。また、2層においても機能としてはデータを転写するだけでなく、1層のソシキと3層のデータが同一のものを指し示すことを証明・担保することも機能になるのではないでしょうか。 3層ではセキュリティ事象やリスク減にはなりすましや不正な相手が考慮されているため、機能においても通信先を認証する、あるいは通信元として自身を証明するということも機能として考慮されるのではないでしょうか。	いただいた御意見も参考に、修正いたします。 修正箇所：図1.3-1
10	1	企業	添付C	サプライチェーンの委託先選定および評価にセキュリティ・アクション宣言を加えていただきたく。 ・理由 各種認証は中小企業には負担が大きい場合があり、ＣＰＳにおいてもセキュリティ・アクションを活用していただきたい。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.SC-3 Basic
10	2	企業		サイバー・フィジカル・セキュリティ対策フレームワーク（以下「ＣＰＳ」）のサプライチェーンの委託先選定および評価へ対応できるよう、セキュリティ・アクション「付録6　情報セキュリティ関連規程（サンプル）」にＣＰＳの対策事例（ＢＡＳＩＣ）を加味すべきと思われます。 「付録６　情報セキュリティ関連規程（サンプル）」の対策例のうち、加味すべきと思われる対策要件ＩＤは以下のとおりです。 ＣＰＳ．ＢＥ－１（Ｂａｓｉｃ） ＣＰＳ．ＳＣ－５（Ｂａｓｉｃ）評価基準に「セキュリティ・アクション宣言をおこなっていること」を追加 また、ＩｏＴを利用する事業者は、上記に加え、セキュリティ・アクション宣言において以下の対策を規定すべきと思われます。 （１）ＩｏＴ機器への要求事項　ＣＰＳ．ＡＣ－８ （２）ＩｏＴ機器のライフサクル管理　ＣＰＳ．ＲＡ－４、ＲＡ－６、ＲＰ－１、ＳＣ－２、ＤＳ－１２ ・理由 発注者ごとの委託先への要求事項や評価項目に対応することは委託先の中小企業には負担となります。また、発注者にも評価項目がある程度標準化されていることはメリットがあると考えるため。	いただいた御意見は、今後、セキュリティ・アクションの検討を進める上で参考にさせていただきます。
11	1	団体	添付Ａ	現状の「ユースケース」には自動車、スマートホーム、ビル、電力の例示があるが、流通業界の事例がない。サプラーチェーンは流通までを含めた対応が必要であるため、「ユースケース」および「対策要件に応じたセキュリティ対策事例集」に流通の領域で特にインターネットに依存する割合の高い通信販売（主にＥコマース）分野の例示を追加してほしい。	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、ユースケース図は、本フレームワークのイメージを容易に把握できるようにするために添付した例であります。よって、具体的なユースケースやセキュリティ対策要件については、産業分野や企業ごとに、本フレームワークを活用し、検討いただきたいと考えております。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
11	2	団体		以下に例示する様に通信販売を取り巻く環境はダイナミックであり、サイバーセキュリティと密接に関連し複雑化している。 ・オムニチャネルの進展によるサイバー・フィジカル双方向からの情報発信と利用 ・ＩｏＴを利用したＥコマースの自動化 ・第三者由来の情報をサイバー空間に提供する場合 ・物流等のフルフィルメントにおけるＩｏＴ利用 ・越境ＥＣの拡大とＥＵ一般データ保護規則への対応 ・仮想通貨による取引 ・ブロックチェーンによる認証 ・プラットフォーマーの台頭と規制 当会では弁護士、コンサルタント等の専門家と実務者の共同により、オムニチャネルの研究、（２０１４～１５）、表示リスクマネジメントの研究（２０１６～１７）などに継続的取り組んできた。通販業界にも影響が大きいと思われる「サイバー・フィジカル・セキュリティ対策フレームワーク（案）」について情報交換を御願いしたい。 ・理由 「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）」はセキュリティフレームワークの範囲を越えて、サイバー空間に提供される情報や、事業者間取引で提供および共同利用される情報そのものの信頼性およびサプライチェーンの信頼性も対象としている。そのため、今後のサイバー・フィジカル空間のコミュニケーションや取引への様々な施策のベースとなる基本概念を提供するものであると考える。 情報セキュリティマネジメントをプライバシーマークやＩＳＯ２７０００ファミリを参照している通販事業者は多いが、「サイバー・フィジカル・セキュリティ対策フレームワーク（案）」ではさらに広汎な事項への対応が必要となることが予想される。 中小を含め、多数の通販事業者が「サイバー・フィジカル・セキュリティ対策フレームワーク（案）」を容易に活用するためには、ガイダンス類が必要であると考えるため、ガイダンスの作成を検討いただきたいことと、その作成につき情報交換を御願いしたい。	産業分野での具体的なユースケースやセキュリティ対策要件を検討していく上で、様々な関係者と情報交換をさせていただければと考えております。
12	1	個人		3層構造モデル 3層全体で見ると矛盾がある。第1層は企業などの組織のISMSによってセキュリティが確保される層としているが、第3層のサイバー空間においても組織が管理する領域はあるので、第3層は第1層を包含しなければならない。すなわち、第1層と第3層は分離していない。第2層はフィジカル空間とサイバー空間をつなげる転写機能の層なので、第1層はフィジカル空間であると言っているに等しい。第2層と第3層は変えずに、第1層をフィジカル空間と定義するのが妥当であろう。その場合でも、各層に組織の管理の及ぶ領域と外の領域があるので、本書の第1層の考え方は活用できる。すなわち、第1層の定義を変更し、加えて、各層で組織内のセキュリティ管理と組織のセキュリティ管理の及ばない領域への対応に、再構成すれば良いと思う。 p.10等の「第1層　企業間のつながり」についても「フィジカル空間のつながり」にする。	三層構造モデルは、Societyt5.0 の実現に向けて新たな産業社会を捉えるモデルであり、それぞれの層に含まれる対象を明確に分離するモデルではありません。その中で、社会全体のサイバーセキュリティ対策を考えた場合の信頼性の基点として、企業間のつながりで求められる、企業（組織）のマネジメントの信頼性の確保を求めるものです。そういう意味で、いただいた御意見のとおり、サイバー空間の事物であっても、企業（組織）マネジメントの対象となる領域はございますので、第1層の定義は、原案のとおりとさせていただきます。三層構造モデルは、フレームワークのコンセプトとなる考え方ですので、引き続き丁寧に説明して参ります。
12	2	個人	p.3	バリュークリエイションプロセスは長いし、意味を取り難い。 変更案：「価値創造プロセス」に変更する（「プロセス」は、ITでは一般的であり、「過程」よりも適切である。このように変更すれば、タイトルに複数現れる「価値創造過程（バリュークリエイションプロセス）」も「価値創造プロセス」だけにすることができる）。	いただいた御意見も参考に、バリュークリエイションプロセスが価値創造過程を言い換えた表現であることが明確になるよう修正いたします。 修正箇所：はじめに 1.
12	3	個人	p.5, p.22, p.44	コンセプト、ポリシー、メソッドと並び、その中の「コンセプト」の指す意味は概ね理解できる。しかし、ポリシー、メソッドが何を指しているのか、本文を読んでも理解できない。上記３つの用語を除けば、第I部から第III部までのタイトルは理解できる。 第II部のタイトルにある「ポリシー」の意味がわからない。対策要件はポリシーと言えると思うが、「リスク源の洗い出しと対策要件の特定」がポリシーなのではない。 第II部を含めてメソッドでもあり、「メソッド」が何を指しているか不明確である。 変更案：第I部から第III部までのタイトルから、コンセプト、ポリシー、メソッドを削除する。	いただいた御意見も参考に、それぞれが指す事項を冒頭部の本部構成で明確になるよう修正いたします。 修正箇所：はじめに 5.

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
12	4	個人	p.6	(3)グローバルハーモナイゼーションを実現する 書いてある内容は、グローバルハーモナイゼーション実現の一歩手前である。 変更案：「国外標準との整合性を確保する」が妥当である。	いただいた御意見も参考に、修正いたします。 修正箇所：はじめに 6.
12	5	個人	7.(1)	「信頼性の基点」の用語集での定義は、エンティティの信頼性が確保されていることを確認するための確立された信頼点であるが、「確立」と「信頼点」の意味が明確でない。本文では、マネジメント、機能、データが、信頼性の基点として挙げられている。また、信頼性はエンティティに限定して良いのか。例えば、処理の信頼性は、本文書の対象になり得ると考えるが、エンティティの定義にソフトウェアが含まれているから良いのか。定義では、ソフトウェアも含め、モノとして捉えているが、上記の「処理」は行為の意味であるので、不足があると考える。しかし、処理自体の信頼性は問わず、処理の信頼性も含めて処理を実施する主体の信頼性で捉えるのであれば、エンティティの信頼性に限定することも可能である。 変更案：エンティティや処理の信頼性を判定するための基準となるプロシージャやデータ、またはそれらの集まり	いただいた御意見も参考に、修正いたします。 修正箇所：添付E
12	6	個人	7.(3)	この部分は、「７．フレームワークの使い方」の他の部分の記述とは異なり、使い方ではなく、今後の活動になっている。 変更案：「８．フレームワークに基づく今後の活動」を新設するか、７の中での注にする。または、(3)のタイトルの最後に「（今後の活動）」と追記する。	いただいた御意見も参考に、修正いたします。 修正箇所：はじめに 7.(3)
12	7	個人	第Ⅰ部1.	「直線的」の意味が明確でない。 変更案：削除する。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ⅰ部1.
12	8	個人	第Ⅰ部1.	従来のサプライチェーンの信頼性は、セキュリティのマネジメントもある程度は考慮されていたが（例えば、クラウドやデータセンターの利用、ソフトウェア開発委託などの場合）、よりISO 9000の方が重視されていたと思う。「従来のサプライチェーン」が指す範囲が明確ではないが、単にデータを交換するだけの場合に相手企業がISMS認証を取得しているかを問題にすることはなかった。 変更案：第1段落を以下のように変更する。 従来のサプライチェーンでは、参加主体の組織ガバナンス、マネジメントが信頼できるものであれば、サプライチェーンの信頼性も確保されるという考え方に基づいていた。サプライチェーンにおける情報処理の一部がデータセンターやクラウドに委託される場合は、ISMSなどのセキュリティ対応をしっかりと行い認証を取得した委託先企業であれば、そのプロセス全体のセキュリティが確保される、したがって、セキュリティを確保するための基点は、組織のマネジメントの信頼性に基礎が置かれることになる。なお、上記の情報処理も、後述のようなものではなく、定型的なものに限定されていた。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ⅰ部1.
12	9	個人	第Ⅰ部2.	「ビジネス資産を固定的に把握してリスク源に対応していくのでは、それぞれのバリュークリエイションプロセスで防御しなければならない本質を見逃す恐れがある」において、「資産を固定的に把握」と「防御しなければならない本質」がわかり難い。 変更案：ビジネス資産を固定した組織に属することを前提とするのでは、リスク源に適切に対応できず、それぞれのバリュークリエイションプロセスで本質的な防御を見逃す恐れがある。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ⅰ部2.
12	10	個人	第Ⅰ部 2.1	「２．１．三層構造アプローチ」について、アプローチが述べられておらず、意義が記述されていない。三層構造モデルとその構成要素が紹介されているだけである。また、第1段落の最後に「ここで示している三層構造アプローチは、信頼性の基点を的確に設定するためのモデルである」と言っているが、アプローチとモデルは異なる。アプローチは三層構造モデルに基づいてセキュリティ対策をするということであろうが、そのような記述を見つけられなかった。 変更案：2.1のタイトルを「三層構造モデルと構成要素」に変更する。「三層構造アプローチ」を使うなら、内容を明確に記述する。文書全体で対応を検討していただきたい。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ⅰ部2.1.
12	11	個人	第Ⅰ部 2.1	「両空間の境界において行われる情報の変換は高い正確性を求められ、いわば、転写・翻訳というべき正確性が確保されなければ」において、「転写」はさておき、「翻訳」は必ずしも「正確性」を具備しない。よって、文意が不明確である。 変更案：「両空間の境界において行われる情報の変換（以下では「転写」と表現する）の正確性が確保されなければ」にする。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ⅰ部2.1.

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
12	12	個人	第Ⅰ部 2.2	「資産を固定的に捉える」がわかり難い。資産と構成要素の関係が不明確である。 変更案：「資産が固定した組織に属することを前提とする」に変更する。資産が構成要素のどれに当たるのかを追記する。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ⅰ部2.2.
12	13	個人	表1.2-1	企業や団体内で異なるセキュリティポリシーを持つ組織は「ソシキ」として扱わなくて良いのか。「プロシージャ」は、システムが実施するものとヒトが実施するものが考えられる。範囲が明確でない。 変更案：定義を明確にする。「ソシキ」については、上記のような組織も含める必要があれば、「バリュークリエイションプロセスに参加する企業・団体における同一のセキュリティポリシーを共有する範囲」とする。	いただいた御意見も参考に、修正いたします。 修正箇所：表1.2-1
12	14	個人	第Ⅰ部 2.2	「本フレームワークで示した三層構造を踏まえると、図1.2-4 のとおり表現できる」とあるが、何が表現されているのかわからない。 変更案：表現対象を記述する。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第I部 2.2. 6 つの構成要素
12	15	個人	第Ⅰ部3.	タイトルに「整理」とあるが、リスク源は整理するものかも知れないが、対応方針は整理するものではなく作成するものである（本文書では「整理」という言葉が多用されているが、多様な意味を持っていると思う）。 変更案：「リスク源の整理と対応方針の作成」にする。	本フレームワークでは、第Ⅱ部及び添付Ｂにてリスク源に基づく対応方針を網羅的に取りまとめており、各産業界や企業における対応方針の作成に活用いただきたいと考えておりますので、いただいた御意見については、原案のとおりとさせていただきます。
12	16	個人	第Ⅰ部3.	「三層構造アプローチと6つの構成要素によって」の意味がわかり辛い。「整理していく」までがアプローチなのではないか。 変更案：「三層構造モデルと6つの構成要素に基づいて」に変更する。	いただいた御意見のとおり、修正いたします。 修正箇所：第Ⅰ部3.
12	17	個人	第Ⅰ部3.	マルチステークホルダーアプローチの意味が不明確である。 変更案：「いくこととなり、マルチステークホルダーによるセキュリティ対策の取組が必要になる」を「いくことになる。直接・間接の関与者全体としてのセキュリティ対策への取組を、本書ではマルチステークホルダーアプローチと呼ぶ」とする。	いただいた御意見を踏まえ、修正いたします。 修正箇所：第Ⅰ部 3.
12	18	個人	第Ⅰ部4.	「４．フレームワークにおける信頼性の確保の考え方」とあるが、４に書かれている内容はフレームワークに含まれていない。 変更案：「フレームワークに基づく信頼性の確保のあり方」または「今後の取組み」とする。	いただいた御意見を踏まえ、修正いたします。 修正箇所：第Ⅰ部 4.
12	19	個人	第Ⅰ部4.	Ex. は別の表現にする。	いただいた御意見も参考に、修正いたします。 修正箇所：（日本語版）第Ⅰ部 4.
12	20	個人	図1.4-1	図の右と左の関係がわからない。 変更案：説明を追記する。	いただいた御意見を踏まえ、修正いたします。 修正箇所：図1.4-1
12	21	個人	第Ⅱ部	第1段落の2行目の「整理」は、ここでは「決定」なのではないか。	いただいた御意見については、原案のとおりとさせていただきますが、信頼性の基点の整理は三層構造モデルにて行っていることが明確になるよう記載を修正いたします。 修正箇所：第Ⅱ部
12	22	個人	第Ⅱ部 1. ②	「及び、」は一般的でない。「及び」の前後に読点を打たないか、打つ場合は前の方がより一般的である。 変更案：読点を取る。	いただいた御意見のとおり、修正いたします。 修正箇所：（日本語版）第Ⅱ部1.②
12	23	個人	第Ⅱ部 1.	第2段落で（１）①から④を留意点とする根拠が書かれていない。第3段落に「観点の捉え方」とあるが、それは根拠とは異なると思う。29ページ以降に書かれていると思うので、それを記述すべきである。 変更案：第1段落の最後に、「以下の4点を考慮すべき根拠は、１．１（2）に記述する」と加える。	いただいた御意見を踏まえ、修正いたします。 修正箇所：第Ⅱ部1.
12	24	個人	第Ⅱ部 1. 1.(1)	「各層の特性及び機能・役割」の「機能」の意味が、一般的な意味での機能とは異なるのだと思う。そのために、文意が取り辛い。各層の特性のために果たすべき機能であろう。「分析範囲及び資産の整理」の「整理」の意味が不明確である。 変更案：「各層の特性及び機能・役割」を「各層の特性及びその特性のために果たすべき機能・役割」にする。「分析範囲及び資産の整理を行う」を「分析範囲を決定し、資産を分類する」にする。	いただいた御意見を踏まえ、修正いたします。 修正箇所：第Ⅱ部1.1.(1)

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
12	25	個人	第Ⅱ部 1. 1.(1)	「管理対象となるモノはすべて第１層に含まれるものの」の「管理対象」という表現は、ここまでに現れない。「分析対象」ではないか。「場所」という表現があるが、特別な意味を持っていないようである。最後の「適当である」も要否を明確に表現すべきである。 変更案：次のように変更する。 分析対象となるモノはすべて第１層に含まれる。しかし、第２層、第３層の機能を備えるモノについては、その層に含まれるモノとして分析する必要がある。また、第２層の機能と第３層の機能を併せ持つモノについては、両方の層での分析が必要であることに留意する。その際、機能を踏まえてモノやシステムが設置される場所、ヒトに対して特定のプロシージャを 要求する場所も、リスクアセスメントにおいて検討が必要である。	いただいた御意見を踏まえ、修正いたします。 修正箇所：第Ⅱ部1.1.(1)
12	26	個人	表2.1-1	(1)カラム「対象の具体的イメージ」の「対象」は分析対象である。特性カラムで右にインデントされた記述はサブ特性の記述と思うが、第1層のサブ特性はひとつなので細分化されているわけでなく、サブ特性の記述内容も特性の記述内容とほぼ同じである。(2)「分析対象」カラムにある「転写する機能」の定義があることが望ましい。(3)「サイバー空間から受け取ったデータに基づいて、一定のルールに基づいて、モノを制御したり、データを可視化したりするように表示したりする機能」は転写機能の逆変換を意図していると思うが、逆変換の出力の方が転写機能の入力となる領域（フィジカル空間）より大きく、対応が取れていない（データを可視化するのは、第1層に閉じた処理と考える）。また、この逆変換は、名称に転写機能を使うべきではなく、別の名称が必要である。(4)「対象の具体的イメージ」に、転写機能と逆変換機能の両方のイメージが混在している。3Dプリンタは、逆変換機能だけしか持たない。 変更案：(1)「対象の具体的イメージ」を「分析対象の具体的イメージ」にする。第1層のサブ特性を削除する。(2)第2層の「機能・役割」カラムのひとつめの「変換」を「変換（転写機能）」にして、「分析対象」カラムの「転写する機能」を「転写機能」にする。(3)「データを可視化したり」の部分をフィジカル空間への出力になる例に置き換える。逆変換に名称を付けるとしたら、「実化機能」は候補になるであろう。名称追加に伴い、「分析対象」カラムに必要な変更を施す（現在は「転写機能」に関する記述だけ）。(4) 転写機能と逆変換機能のイメージを分ける。	(1), (2)に関しましては、いただいた御意見も参考に、修正いたします。 修正箇所：表2.1-1 (3), (4)に関しましては、御意見の趣旨は理解いたしますが、サイバー空間からフィジカル空間への転写とフィジカル空間からサイバー空間への転写を分けると煩雑になるため、原案のとおりとさせていただきます。
12	27	個人	図2.1-3	「第１層の分析範囲及び資産の関係を示す」とあるが、どう表現されているのかがわからない。	図2.1-3は、表2.1-1の整理に基づく分析対象とその具体的イメージを表現したものですので、いただいた御意見も参考に、修正いたします。 修正箇所：図2.1-3, 図2.1-4, 図2.1-5
12	28	個人	第Ⅱ部 1. 4.	IEC TR 63074とIEC TR 63069が並記されているが、39ページの解説を読むと、セキュリティ対策が安全に影響を与えることもあり得るので、後者が妥当である。 変更案：不要。	セーフティとセキュリティの統合に関する検討状況を紹介するための図であるため、いただいた御意見については、原案のとおりとさせていただきます。
12	29	個人	表2.2-1	脆弱性がなければ脅威はなく、脅威が現実となってインシデントがある。 変更案：表の並びを、脆弱性、脅威、想定されるセキュリティインシデント、の順にする。	本フレームワークでは、リスクシナリオベースにより各層で想定し得るセキュリティインシデントから、リスク源（脅威・脆弱性）を洗い出し、対応する対策要件を網羅的に取りまとめておりますので、いただいた御意見については、原案のとおりとさせていただきます。
12	30	個人	第Ⅲ部 1.(1)	「①に関しては、～」は文が長く、わかり難い。 変更案：以下を提案する。 （１）①に関しては、各組織で実装すべきセキュリティ対策のレベル選択の一助とすることを目的にして、添付C にまとめた。国内外の様々なガイドライン等を参照した上で、参照した文書による分類をベースに、対象とするスコープ(例：自組織内のみの適用か、関連する他組織を巻き込んだ適用か)、対策を導入・運用する際の相対的コスト等の観点を考慮してセキュリティ対策を選択できるように、セキュリティ対策例をHigh Advanced、Advanced、Basic の三段階のレベルに分けて示している。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 1. 対策要件及び対策例集を活用したリスク対応（1） 自組織のセキュリティマネジメント強化

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
12	31	個人	表3.3-1	カテゴリーの名称に改善の余地があり、また、カテゴリーの並びにライフサイクルが考慮されていない。その結果として、「リスク管理戦略」と「サプライチェーンリスク管理」の関係がわからない。「保護技術」の指す内容が不明確であり、その結果として、「認証及びアクセス制御」や「データセキュリティ」との重複があるように見える。「伝達」と「低減」は、何に関するものかがわからず、漠然としている。 また、後掲の各カテゴリーの対策要件も、一部はライフサイクルを考慮した並びになっておらず、読者にわかり辛い部分がある。 変更案：以下を提案する。 「資産管理」「ビジネス環境」「ガバナンス」「リスク管理戦略」「リスク評価」「サプライチェーンリスク管理」「意識向上及びトレーニング」「アイデンティティ管理、認証及びアクセス制御」「データセキュリティ」「保護技術」「保守」「情報を保護するためのプロセスおよび手順」「セキュリティの継続的なモニタリング」「検知プロセス」「異常とイベント」「対応計画」「伝達」「分析」「低減」「改善」 各カテゴリーの対策要件を、ライフサイクルを考慮して並べる。	カテゴリーの並び順については、参考としたNIST "Framework for Improving Critical Infrastructure Cybersecurity"とのハーモナイズの観点を考慮したものとなっております。そのため、カテゴリーの並び順についていただいた御意見については、原案のとおりとさせていただきます。また、カテゴリー内の対策要件の並び順につきましては、いただいた御意見も参考に、修正いたします。
12	32	個人	CPS.AM-6	関係者とは誰か。ステークホルダーとは異なるのか。また、何故伝達が必要なのか。関係者によっては、内容が詳細過ぎる。共有だけで十分ではないか（共有は所在を知らせるだけ、伝達は内容も含めて知らせる、と考えて）。 変更案：上記に基づき、変更して下さい。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-6
12	33	個人	CPS.RM-1	「関係者」を「ステークホルダー」または「関係する他システム」にする。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.5 リスク管理戦略 CPS.RM-1
12	34	個人	CPS.AT-2	「関係組織」によっては過大な要求である。 変更案：過大な要求にならないように修正する。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.8 意識向上及びトレーニング CPS.AT-2
12	35	個人	CPS.IP-3	本対策要件はメタレベルな対策要件であり、他の対策要件とレベルが異なる。これ自体が対策要件全体に対応する。 変更案：削除する。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.10 情報を保護するためのプロセス及び手順
12	36	個人	CPS.IP-4 CPS.IP-7 CPS.IP-9 CPS.AE-4	CPS.IP-4, CPS.IP-7, CPS.AE-4の「している」は記述方法と他と異なるため、「する」に変更する。 同様に、CPS.IP-9の「含めている」は「含める」に変更する。	いただいた御意見のとおり、修正いたします。 修正箇所：本文第III部 3.10 情報を保護するためのプロセス及び手順
12	37	個人	CPS.IP-10	「脆弱性管理計画」とは何か。 変更案：説明を追記する。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.10 情報を保護するためのプロセス及び手順、添付E
12	38	個人	CPS.MA-2	誰の「承認」かが不明である。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.11 保守
13	1	企業	添付B	「3_3 データを送受信する機能」について、 L3_3_a_SYS の対策要件に、CPS.MA-1が２回登場しています。 最初のMA-1は不要ではないでしょうか（後にMA-1、MA-2が並んで登場しています）	いただいた御意見のとおり、修正いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
14	1	個人	CPS.SC-7	「自組織が関係する他組織との(後略)」を「自組織が関係する他組織および個人との」のように変えるなど、対個人への情報開示の必要性を明記する。その他、企業と個人のデータの転送に関する箇所に対個人の場合を明記する。 ・理由 添付Ａ．ユースケース４：スマートホームの例のように組織対個人のデータの転送も当フレームワークの対象に含まれているため。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.6 サプライチェーンリスク管理 CPS.SC-7
14	2	個人	CPS.RP	事業継続が不可能になったときに自組織が持つデータの処分についての計画しておくことを追加する。 ・理由 事業継続が不可能な事態に陥った場合その後の分析・改善が不可能になり、組織解散後はデータの管理者が不在になるなど組織が存続する場合と異なる点が多く、また、混乱が生じやすく漏洩等のリスクも高まる状態であるため。	対策を実施する主体である組織が存在しないケースにおける情報保護については、検討の対象範囲外とさせていただきたいと考えております。一方、製品・サービスの提供終了時の対応についてはCPS.SC-10をご参照ください。いただいた御意見については、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
15	1	企業		映像や音声などの情報は、今やその形がデジタルデータになっただけではなく、その流通方法はインターネットなどのネットワークを経由して行われている。 通常、商用の映像や音声などのメディアデータ(例 映画、音楽)はその著作権者がおり、その著作権を保護するためにDRM(Digital Rights Management)のような技術が暗号技術や認証技術を利用し、メディアデータが著作権者により許可をした特定の消費者にだけ視聴を可能にすることで保護を実現してきた。 しかしながら、AIなどの技術の発達により全く異なる形の攻撃が増えてきている。その一つが情報の改ざんであり、一部ではDeepfakeと言われている。 （参考ニュース）：http://www.niemanlab.org/2018/11/how-the-wall-street-journal-is-preparing-its-journalists-to-detect-deepfakes/ このようなDeepfakeの利用が広まると、メディアデータに対して真贋を問うことが非常に困難になる。例えば、身近なところでは、現在は写真や監視カメラによる映像データが犯罪などの証拠になり得るが、このようなDeepfakeの発達により映像や音声の真贋の評価が難しくなり、そのようなデータの証拠としての価値を判断がAIの進化とともに困難になる。またこのような技術により、一国の首相や大統領の映像を利用したフェイクニュースにより情報操作も増えることが容易に想像される。以前であればニュースの情報源がTVなどの放送波だったが、今日はでネットワークを介して発信される情報が非常に多岐にわたるため、情報のソースの特定が一層難しくなり、それはこのようなフェイクニュースの流布を容易にする結果になる。 Deepfakeを可能にしているのがAIであれば、それを検知するAIもあるので、それを利用することが対策にもなるが、それには幾つかの課題もある。第１に、新型のDeepfakeのAIアルゴリズムが出るたびに、検知AIもそれに順応する必要があるため、その順応までの間にタイムラグが生じ、いわゆるゼロディ攻撃を防ぐことができない。第２に様々なインターネットのソースからDeepfakeによるデータが発信されるとき、それをいかにも視聴者が見る前に全てAIにより検閲をするかである。これはインターネット中をクローリングして見つけられるメディアデータを片っ端からAIにて検閲すれば可能かもしれないが、インターネットの規模を考えると現実的ではないだろう。 そこで考え得る別の角度からの対策としては、情報の真贋性をデータベース化して、視聴者がメディアデータを視聴する際には、そのデータベースに問い合わせを行うことにより、視聴者自身がそのメディアデータの真贋性を判断する手段を提供する方法である。その際にはメディアデータが経由する様々な処理プロセスの段階で、メディアデータの処理者、処理方法、出力メディアの情報を、安全な方法でデータベースに登録することで、視聴者がメディアデータを利用する際に、そのメディアデータが、例えばどのカメラで撮影され、その後どのような画像処理ソフトで変更されたかを明確に確認することにより、メディアデータの真贋性を判断することができる。 このようなデータベースを構築するには、上記の例の場合だと、カメラならびに画像処理ソフトから安全にデータを受け取り、尚且つその情報の受け取り日時の情報を含めた上でデータベースにて安全に保存し、もし視聴者からの問い合わせがあれば、その問い合わせに直ちに応じて情報を安全に提供することが必要になる。このようなシステムを大規模で構築するには非常に複雑な設計や、システムの拡張性が必要になるように見えるが、実際にはBlockchainの仕組みがここで利用することができる。つまりは、上記のデータベースに当たる部分をBlockchainで実現することにより、そこへの入力情報を安全に保存することができまた過去の情報の改ざんもBlockchainの性質上、暗号的に非常に堅牢に防ぐことができる。またBlockchainは仮想通貨などの発展を支えるべく拡張性についても優れているため、その仕組みを流用することができる。 このような仮想通貨という一つのブームを背景に様々な研究や開発が行われて発展し利用されているBlockchainという仕組みは、ディープフェイクのようなメディアデータの真贋性が問われるような環境においても非常に優れた機能を提供することが可能である。	データそのものの信頼性確保は「Society5.0」の実現に向けて重要な課題と認識しており、フレームワークでも対策要件（CPS.GV-3, CPS.SC-7, CPS.CM-4 等）として言及しています。 その上で、実際の産業活動への実装を進めるにあたっては、取り扱うデータの区分に応じたセキュリティ対策や、データの完全性、真正性等の確認手法等も必要です。いただいた御意見も踏まえ、引き続き、検討を進めてまいります。
16	1	個人	3.	Stuxnetを念頭にした記述と思われるため、制御系システムの部品や通信が汎用化・標準化していったことも要因のひとつである記述にしたほうが良い。この場合、チャールス・ペロー氏の「ノーマル・アクシデント」の概念に近い。 【原文】また、「ネットワーク化されず、インターネットにも接続されない」システムと認識していても、IT 機器の小型化・高機能化に伴い、電子機器を含むすべてのシステム等が重要性を増し、フィジカル空間を通じたサイバー攻撃を受けるなどの懸念も増大しており、所有する電子機器及びシステムが本フレームワークの適用範囲に含まれ得るという認識に立ち、必要なセキュリティ対策を講じる必要がある。 【改定案】また、「ネットワーク化されず、インターネットにも接続されない」システムと認識していても、システムで使用している独自仕様の電子機器や通信プロトコルが汎用化・標準化されることに伴い、機器間の連携がシームレスになり利便性向上につながる一方で、小さなインシデントの影響が容易にシステム全体へ波及する可能性が高まり、フィジカル空間を通じたサイバー攻撃を受けるなどの懸念も増大しており、所有する電子機器及びシステムが本フレームワークの適用範囲に含まれ得るという認識に立ち、必要なセキュリティ対策を講じる必要がある。	いただいた御意見を踏まえ、修正いたします。 修正箇所：3. フレームワークを策定する目的と適用範囲

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
16	2	個人	p.22	あえてJIS Q 31000:2010を使うと宣言しているので問題はないが、最新のリスクマネジメント規格はJIS Q 31000:2019（ISO 31000:2018）であり、プロセス図では「企業等の状況の確定」が「適用範囲、状況、基準」に変わり、「記録作成及び報告」が新たに追加された。現在JIS Q 31000:2019が発行されているにも関わらず9年前の規格を参照するのは古すぎる。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第II部 1. 三層構造アプローチと６つの構成要素を活用したリスクマネジメントの進め方 図2.1-1
16	3	個人	p.22~23	リスクマネジメントのプロセスとステップのずれが大きい。できるだけあわせる書き方にする。またIPA「制御システムのセキュリティリスク分析ガイド 第2 版では「想定される攻撃シナリオ」（事業被害ベースのリスク分析のこと？）だけでなく「資産ベースのリスク分析」も記述されており不十分に見える。もちろんここで全てを記述する必要はなく、「想定される攻撃シナリオ」を（できればFault TreeとAttack Treeを組合せたリスク特定、分析、評価を意識した）一例とした記述にすることで改善できる。 【改定案】 セキュリティリスクマネジメントにおけるプロセスの一例を下記に示す。 ■「企業等の状況の確定」（または「範囲、状況、基準」） １分析対象の明確化（１．１） ～原文そのまま～ ２想定されるセキュリティインシデント及び事業被害レベルの設定（１．２） ～原文そのまま～ ■リスクアセスメント[リスク特定、リスク分析、リスク評価] ３リスク分析の実施（１．３） ～原文そのまま～ ■リスク対応 ４リスク対応の実施（１．４） ～原文そのまま～	図2.1-2 でも記載している通り、本フレームワーク第II部では、あくまで、一例として事業被害ベースのリスク分析を想定して記載しております。一方で、資産ベースでの手法につきましても、モノやシステムが柔軟につながるSociety5.0における分析のあり方を今後検討していく必要があるかと考えております。一方、ISO31000のステップとの対応については、いただいた御意見を踏まえ、修正いたします。
16	4	個人	p.36	「１．４．リスク対応の実施」の中の「回避、低減、移転、保有」はJISQ2001:2001の概念であり18年前の概念は古すぎる。JIS Q31000:2019でのリスク対応の選択肢は下記7つである。「７つを４つにまとめると回避、低減、移転、保有になる」など記述を変えて古い概念をそのまま使っているわけではないことを示すか、最新の７つの記述に変えたほうが良い。 ・リスクを生じさせる活動を、開始又は継続しないと決定することによって、リスクを回避する。 ・ある機会を追及するために、リスクをとる又は増加させる。 ・リスク源を除去する。 ・起こりやすさを変える。 ・結果を変える。 ・（例えば，契約，保険購入によって）リスクを共有する。 ・情報に基づいた意思決定によって、リスクを保有する。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第II部 1. 三層構造アプローチと６つの構成要素を活用したリスクマネジメントの進め方 1.4. リスク対応の実施
16	5	個人	p.39	機械安全（IEC側）を扱うIEC/TC44の「IEC TR 63074（既存安全制御システムのためのセキュリティ対策）」、制御系安全を扱うIEC/TC65の「IEC TR63069（一般的制御システムにおける安全とセキュリティの分析・対応）」はまだ発行前であるが、既に発行済みの機械安全（ISO側）を扱うISO/TC199の「ISO TR22100-4:2018（セキュリティ面のガイド及び考慮）」にも言及が必要ではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第II部 1. 三層構造アプローチと６つの構成要素を活用したリスクマネジメントの進め方 1.4. リスク対応の実施 図2.1-9
17	1	政府機関	p.1-4	翻訳）セキュリティを確保するための総合的な対策の必要性は非常によく強調されている。	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。
17	2	政府機関	Part I: 2.	翻訳）自動化された分析によって生成されたデータを使用してプロセスを最適化することもできる。	様々なデータを自動分析し、その結果に基づいてプロセスを最適化を実現することはSociety5.0 が目指す超スマート社会における産業活動の１つの姿です。
17	3	政府機関	Part I: 2.	翻訳）動的で柔軟なバリュークリエイションプロセスによって、重要なポイントを見逃しがちなのはなぜか。	バリュークリエイションプロセスが動的・柔軟であることによって、バリュークリエイションプロセスに関与する構成要素がその時点の活動の目的や必要性に応じて変化し、構成要素を固定的に捉えたセキュリティ対策が困難であるためです。
17	4	政府機関	Figure 1.3-1	翻訳）リスク源の特定に、この全体像がどのように適用されるのか？	図1.3-1は各層におけるセキュリティ対策の概要を示す図であり、リスク源の特定については、第2部に記載しております。
17	5	政府機関	Figure 1.4-1	翻訳）モノに関する信頼の創出は、何らかの形でセキュアな製品開発プロセスの方針に関連しているのか？	本文第II部 1.4. リスク対応の実施でも記載しているように、モノの信頼を創出し、維持するためには、設計、調達から運用、廃棄に至るまでのモノのライフサイクルを通じたセキュリティ対策が重要と記載しております。ご指摘いただいているセキュアな製品開発プロセスは、その中の重要な部分を占めていると認識しております。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
17	6	政府機関	Part II	翻訳）分析の範囲に関して、環境へのインターフェースも含まれているか？	分析の範囲に含まれていると認識しております。ご指摘の内容も踏まえ、よりわかりやすい内容となるよう、記載を修正いたします。
17	7	政府機関	Figure 2.1-9	翻訳）セキュリティには関連するがセーフティには関連しない資産があるかもしれない。	ご指摘いただいている通り、セーフティの問題との関わりが薄い資産も存在すると考えられます。そのため、機器やシステムの企画時、調達時等からリスクアセスメントを実施し、その結果を踏まえ、セーフティに係る対策を実装することが必要になると考えております。
17	8	政府機関	Part III	翻訳）第III部は、対策の実施に非常に役立つ。	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。
18	1	企業	4.	翻訳）製造された（スマート）製品は、エンドユーザーのヒトによって使用されることになる。 彼らの利益集団の代表も想定読者として加えた方がよい。	エンドユーザーもバリュークリエイションプロセスを構成する一員であると考えており、想定読者に含まれるよう、いただいた御意見も参考に修正いたします。 修正箇所：はじめに. 4 .
18	2	企業	Part I	翻訳）このフレームワークは組織間の関係を網羅している。 しかしながら、データは組織間で共有されるだけでなく、顧客施設に設置された消費者向け機器とも交換される。この課題は、部分的にしか言及/対処されていない。	いただいた御意見のとおり、Society5.0においては、様々な組織やヒトの間でのデータ流通が増大することから、第3層では信頼性の基点をデータと定義し、組織に属さないヒトもスコープに入れ、セキュリティ要件等を記載しております。
18	3	企業	Figure 1.4-2	翻訳）この図では「ユーザー」となっているが、これは消費者を意味しているか？消費者がマネージドセキュリティサービスを導入し、それを頼りにすることが要求されているのか？	いただいた御意見を踏まえ、修正いたします。 修正箇所：図1.4-2
18	4	企業	Appndix. A #1	翻訳）この図は「モノのつながり」を表しており、少なくとも「スマートホーム」アプリケーションではエンドユーザーの機器に対応するように見える。 これらのIoT機器はフレームワークでどのように対処されているか？	転写機能を有する機器として捉えると第2層となり、エンドユーザーが管理する機器としてみると第1層となります。各層で想定されるセキュリティインシデントから対処すべき事項を決定します。
18	5	企業	Appndix. A #4	翻訳）エンドユーザーの施設(住まい手)が示されている。エンドユーザー/消費者施設でのセキュリティ管理にはどのような概念が適用されるのか？	エンドユーザーは、本フレームワークにおいても重要なステークホルダーと認識しております。しかし、エンドユーザーに十分なセキュリティ対策を求めることは難しいことから、エンドユーザーにモノやサービスを提供するステークホルダーがしっかりセキュリティ対策を実施することが重要と考えております。
19	1	企業	Part I: 2.1	翻訳）[変更した方がよい記述] "...it is necessary to introduce other types of the basis of trustworthiness and to secure the basises." [変更案] "…it is necessary to introduce additional types of bases for trustworthiness and to secure them."	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part I: 2.1.
19	2	企業	Part I: 2.1	翻訳）[変更したほうがよい記述] "In other words, the trustworthiness of the value creation process is not ensured unless ensureing the accuracy of transcription and translation." [変更案] "In other words, the trustworthiness of the value creation process is not ensured unless the accuracy of transcription and translation is confirmed."	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part I: 2.1.
19	3	企業	Part I: 2.1	翻訳）"thedata" の間にスペースを挿入した方がよい。	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part I: 2.1.
19	4	企業	Part I: 2.1	翻訳）[変更したほうがよい記述] "…where cyber space and physical space become integrated one, security measures…" [変更案] "…where cyber space and physical space are highly integrated, security measures…" [示唆] 文全体を次のように言い換えることができる。サイバー空間とフィジカル空間が高度に統合された産業社会のバリュークリエイションプロセスでは、3つの各層に対応するセキュリティ対策が考慮されなければならない。	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part I: 2.1.
19	5	企業	Table 1.2-1	翻訳）コメント：「消費者」あるいは「最終消費者」も付加価値連鎖の一部と見なされているか。その場合は、「消費者」と「最終消費者」を含めたほうがよい。	バリュークリエイションプロセスには、「消費者」あるいは「最終消費者」も含まれています。
19	6	企業	Table 1.2-1	翻訳）1. モノの説明から"those"を削除 2. プロシージャの説明の中で、"archive"は"achieve"に置き換えたほうがよい。	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Table 1.2-1
19	7	企業	Part I: 2.2	翻訳）1. タイピングのエラー：‘physcal machines’ → ‘physical machines’ 2. "… complexly related each other." を"… complexly related to each other." とした方がよい。	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part I: 2.2.
19	8	企業	Part I : 3	翻訳）タイピングのエラー：‘developped’ → ‘developed’	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part I: 3.
19	9	企業	Figure 1.3-1	翻訳）以下の点が理解できない：第2層のセキュリティインシデントには、「安全面に支障をきたす動作」とある。加えて、「データの利用不可」もセキュリティ上の問題となる可能性がある。 たとえば、物理システムからサイバー空間への測定値の送信をブロックするサービス拒否攻撃が考えられる。	ご指摘いただいているインシデントは、「第2層において想定されるセキュリティインシデント」の(1)(d)にて言及しているものと認識しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
19	10	企業	Part I: 4	翻訳）信頼の創出、信頼の証明および信頼チェーンの構築と維持という概念は非常に明確に考案されている。	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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
19	11	企業	Part I: 4	翻訳）[変更したほうがよいポイント] '…to preserve above records' [変更案] ' …to preserve previous records' or 'preserve historical data'. コメント：信頼の創出のこの部分はどのようなものか？	いただいた御意見も参考に、修正いたします。 修正箇所：（英語版）Part I: 4
19	12	企業	Part I: 4	翻訳）[変更したほうがよいポイント] "To create and managethe list for…" [変更案] "To create and manage the list for…"	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part I: 4 . (2)
19	13	企業	Part I: 4	翻訳）[変更したほうがよいポイント] 'To confirm of the trust of components/data by inquiring to the list for trustworthiness.' [変更案] 'To confirm the trust of components/data by inquiring to the list of trustworthy entities/assets.' 質問：これは、構成要素の信頼性を証明する認証機関が常に存在することを意味するのか？これは、信頼性の要素としてデータの完全性が要求される第3層でどのように実現されるのか。	いただいた御意見も参考に、修正いたします。 修正箇所：（英語版）Part I: 4
19	14	企業	Figure 2.1-2	翻訳）最初のブロックにおいて、'clarifying' を'identifying' あるいは'determining' に置き換えた方がよい。	いただいた御意見を踏まえ、修正いたします。 修正箇所：（英語版）Figure.2.1-2
19	15	企業	Part II: 1.1	翻訳）タイピングのエラー：'implementin' → 'implementing' 'Tagets of analysis' → 'Targets of analysis'	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）PartII: 1.1.
19	16	企業	Part II	翻訳）タイピングのエラー：'exxchange' → 'exchange'	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part II
19	17	企業	Figure 2.1-6	翻訳）この図には安全性に対するセキュリティ侵害の影響が、非常によく示されている。 図のタイトルから'problems'を取り除くことを勧める。	いただいた御意見については、原案のとおりとさせていただきます。
19	18	企業	Part II	翻訳）'inappropriate data'とは何のことを言っているのか？不法な情報漏えいのことを言っているのか？あるいは、例えば、中間者攻撃を受けたことにより、不正確になったデータのことを言っているのか？ 示唆："unauthorized data"に置き換えたほうがよい。	'inappropriate data' とは、マルウェアに感染しているファイル、ネットワーク上で改ざんされたデータ、偽装されたIPアドレスから送信されたデータ等のセキュリティ事象により悪影響を受けたデータを指すと認識しております。これは、権限の有無というよりも、データ自体の真正性に関わる事項と考えておりますので、いただいた御意見については、原案のとおりとさせていただきます。
19	19	企業	Table 2.1-6	翻訳）表は各層のセキュリティインシデントの非常に包括的なコレクションを表している。第2層では、不正な組織へのデータの漏洩について追加することを提案したい。例えば、IoT機器が悪意のあるサーバーにデータを送信するために改造されているか、CPSシステムのバックドアが機密情報を攻撃者に送信したりするケースがある。	ご指摘いただいた種の事象については、添付BのL1_1_dにて取り扱っております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
19	20	企業	Part II	翻訳）第2層において、機器の調達およびテストフェーズにおけるセキュリティ・バイ・デザインについて言及しているのは素晴らしい。	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	21	企業	Part II	翻訳）タイピングのエラー：'tsecurity' → 'security'	いただいた御意見のとおり、修正いたします。 修正箇所：（英語版）Part II
19	22	企業	Part III	翻訳）"advanced, medium and basic"ではなく、"high advanced, advanced and basic"という分類を用いたのに何か理由はあるか？	いただいた御意見については、原案のとおりとさせていただきます。
19	23	企業	Part III	翻訳）[変更したほうがよいポイント] 'When the organization implements security measures classified as High Advanced, it should also implement the security measures classifed as Advanced and Basic.' 文章のメッセージがあまり明確でない。これは、組織がHigh Advancedと並行してBasicやAdvancedのセキュリティ対策を講じなければならないことを意味しているのか？1つのセキュリティリスクに対して複数のセキュリティ対策をとるということか？ [変更案] 組織が、"High Advanced"に分類されるセキュリティ対策を実装する際、"Advanced"と"Basic"に分類されたセキュリティレベルをカバーすべきである。 [示唆] おそらくここも"Advanced, Medium and Basic"に置き換えた方がよいだろう。	ご指摘の内容も踏まえ、よりわかりやすい表現となるよう、記載を修正いたします。
19	24	企業	Annex A Use case #2	翻訳）", and supplier pays products…"という表現を理解できない。	いただいた御意見も参考に、修正いたします。 修正箇所：Annex A
19	25	企業	Annex A Use case #3	翻訳）ユースケース#3は非常によい。バリュークリエイションプロセスとしての将来のコネクテッドカーの描写は非常に印象的である。	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。
19	26	企業	Annex D	翻訳）適用される箇所にはIEC 62443を含めることを推奨する。	いただいた御意見も参考に、IEC 62443 との対応関係についても追記します。 修正箇所：添付 C
20	1	企業	Figure.i-1	翻訳）図i.1において生み出された概念であるSociety5.0はまさに人間のユーザの利益を示しています。しかしながら、それは私達に、Connected IndustriesがどのようにSociety5.0に新しい付加価値を生み出すかを教えてくれるだろう。	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。
20	2	企業	Introduction	翻訳）Society5.0の所与の定義と、CEN/CLC JTC13 WP2019における"Digital Society"の定義を比較した方がよい。	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。
20	3	企業	Figure.i-2	翻訳）Society5.0における新しい価値を創出するためには、サプライチェーン構造にどのような変化が必要になるか？	第1部1.に新たな時代におけるサプライチェーンの考え方について記載しております。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
20	4	企業	Table i.1	翻訳）表i.1のIoT保護対策を、NIST CRITISのサイバーセキュリティ対策を超える水準であるIEC 62443シリーズの対策に関連付けたほうがよい。(CPS FWがISA 62443と整合するように計画されていることに留意した方がよい)	いただいた御意見も参考に、IEC 62443 との対応関係についても追記します。 修正箇所：添付C
20	5	企業		翻訳）グローバルデジタル社会のためのサプライチェーンリスクマネジメントがISO 27036-3に定義されているため、留意したほうがよい。	本フレームワークは、主要な国際規格等も参照し策定にしております。一方、新たな国際規格等も常に策定されることから、いただいた御意見も参考に、本フレームワーク策定後においても、様々な国際規格等も参照し、適正に改訂して参ります。
20	6	企業	Annex A	翻訳）Society5.0のユースケースが、CPSフレームワークのメイン部分でより中心的に考慮されている方がよい。	いただいた御意見のとおり、「Society5.0」を中心的に考慮するという意味で、ユースケースの初めに記載させていただいております。
20	7	企業	Annex D.1	翻訳）CPS FWにおけるサイバーセキュリティ管理策のマッピングは、NISTサイバーセキュリティフレームワークのサブカテゴリに言及するだけでなく、CEN/CLC、ISO/IEC 270xxなどのEU標準化団体が焦点を当てているデジタルソサエティ標準にも言及するほうがよい。	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。
20	8	企業	Annex E	翻訳）用語集における定義をクラウドコンピューティング、ビッグデータ、AI、IoT、IACS等に関するISO/IECの語彙とハーモナイズしたほうがよい。	いただいた御意見も参考に、修正いたします。
21	1	団体		翻訳）全体として、我々は、自主的なリスク管理に基づく枠組みを確立するための経済産業省の努力を支持する。そしてドラフト作成の過程を通して産業界と協議する日本政府の意欲を非常に高く評価する。 これまでのコメントで述べたように、セキュリティを確保しながら経済活動を促進するには、マルチステークホルダーによるアプローチが最も効果的な方法であり、効果的なサイバーセキュリティはデジタルインフラストラクチャ、デジタルトレード、およびグローバルなバリューチェーンのレジリエンスにとって不可欠だと考えている。	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。
21	2	団体		翻訳）提案されているフレームワークは、セキュアなIoTまたはサイバー/物理ソリューションを作成する際の開発者に対する技術的考慮事項に対する包括的な見解を提供している。しかしながら、リスク管理は効果的なサイバーセキュリティにとって根本的であると強く信じているため、リスクベースのアプローチを反映し、リスク管理プロセスの実装を優先するためのポリシーが必要とされている。つまり、合意ベースの基準とサイバーセキュリティ事象を検知し、対応し、復旧するために、サイバーセキュリティリスクを識別、防御するリスク管理のベストプラクティスに依拠したリスクベースのアプローチを企業が採用および奨励することを推奨する。これを達成するために、我々は、フレームワークがリスクの評価と特定、それを最小化する方法、そして国際的なベストプラクティスを実行する際の企業の成熟度に焦点を合わせるべきであると信じている。	いただいた御意見のとおり、リスクベースアプローチは重要であると認識しており、本フレームワークに採用しております。
21	3	団体		翻訳）また、我々は、消費者がIoTおよびサイバーフィジカルシステムを使用、展開する際に、プライバシー認証スキームが消費者との信頼関係を築く上で重要な役割を果たすと考えている。この目的のために、我々は、フレームワークが安全で技術的な解決策と並んで、データを保護するという強い文化をよりよく促進していくことを望んでいる。	Soeicty5.0 において、データ保護の重要度は高まっており、第3層の信頼性の基点をデータと定義し、その対策要件及びセキュリティ対策例を示しております。
21	4	団体		翻訳）業界では、マルチステークホルダーの枠組みが、国際的な分野を含む、企業のサイバープラクティスのための健全なベースラインであるという幅広いコンセンサスがある。 商工会議所はこれを歴代の米国政権に伝えてきた。そして我々はそのようなアプローチがグローバルに企業のサイバーセキュリティリスクと脅威を管理するための礎石になると主張する。相互運用性が貿易の観点からもたらす利点を超えて、マルチステークホルダーアプローチは、企業が国境を越えてクラス最高のサイバーセキュリティプラクティスを拡大し、サイバーセキュリティの全体的なレベルを上げることを確実にする。 我々は、ドラフト中での国際ハーモナイゼーションに関する議論を称賛する一方、経済産業省がサイバー規制間の相互運用性を促進するために、同省が国際的な相手方及び業界とどのように協力するかについてより詳細な戦略を策定することを奨励する。	いただいた御意見のとおり、マルチステークホルダーアプローチは重要であると認識しており、本フレームワークに採用しております。 国際ハーモナイゼーションに関する御意見は、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	5	団体		翻訳）我々は、フレームワークに関する日本政府内の調整が優先されることを求める。 国内のさまざまな機関がサイバーセキュリティとデジタル経済に関連する競合するフレームワークまたは規制スキームを確立すると、企業は世界中で規制の不確実性に直面することが多くなる。企業がそのような不確実性に直面しないことを確実にするという点で日本は世界的なリーダーであったが、経済産業省、総務省、NISCのサイバーセキュリティ戦略における産業サイバーセキュリティへのアプローチが少々異なるものであることに気づいた。日本政府がこれらのアプローチにおいて調整されることを確実にすることで、ICTおよびサイバーセキュリティ業界の成長に対するリスクや課題がより軽減され、日本全体のサイバーレジリエンスがより強化されるだろう。	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。
22	1	企業		分割定義された階層の概念が読む人によって理解が異なる可能性があり、どのレイヤにも属さない隙間が発生する懸念がある。階層定義に対する十分な解説書またはガイドラインの整備が望まれる。	本フレームワークで提示した三層構造モデルは、Societyt5.0 の実現に向けて新たな産業社会を捉えるモデルであり、それぞれの層に含まれる対象を明確に分割するものではありません。それぞれの層に何が含まれるかは、産業分野やビジネス活動の特性に基づいて検討される事項と考えております。このような考え方について、引き続き丁寧な説明に努めるとともに、本フレームワークの策定に関わった方々などによる解説など、様々な活動が広がることを期待しています。
22	2	企業		フレームワークが定義した要求事項や、参照する各種標準の要求事項の比較は整理され対応関係が良く理解できるものになっている。可能であれば、各要求事項の差異ポイントの整理ができれば、本フレームワークを一層適用しやすくなる。	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。
22	3	企業		フレームワークの内容は多少、難解ではあるが、米国の標準との整合性をもちながら、三層構造の導入により新たな視点を加えられている。 産業界全体に、このフレームワークに基づき、実際の運用や導入展開をどのように行うかが重要かと考える。	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。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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
23	1	団体		翻訳）我々は、日本全体のサイバーセキュリティと物理セキュリティの向上、および、サプライチェーンや、雇用の創出、社会一般において重要な役割を果たす中小企業（SME）を含む、あらゆる産業の啓発のために社会全体を推進する経済産業省の取り組みを高く評価する。私たちは、本事業が信頼性の高い"Society5.0"と"Connected Industries"に対する日本のビジョンを実現するための基礎になるものと理解している。世界中のポリシーメーカーの注目が高まっているポイントである、産業分野のサプライチェーンが直面しているセキュリティ課題に対処しようとする経済産業省のリーダーシップに感謝する。	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。
23	2	団体		翻訳）2019年に新たに更新されたフレームワーク第2原案は大幅に改善されており、私たちは以前のコメントの多くが考慮されていることを感謝する。一般に、最新のドラフトは、業界の利害関係者が管理するシステムやネットワーク、および彼等が維持するサプライチェーンを横断して存在するリスクの評価、管理、および対応のための重要なツールを提供している。我々は、経済産業省が採用したリスク管理アプローチを歓迎する。このアプローチは、規制によるアプローチよりも効果的であると考えられる。また、重要なISO標準など、国際的に認められた既存のベストプラクティスと意識的に整合していることに、より大きく感謝したい。前回のコメントでは、経済産業省に対し、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NISTサイバーセキュリティフレームワークと整合させることを勧めたが、第2原案において、これらのフレームワークをハーモナイズすることに対して大幅に注意が払われていることに感謝する。この調整により、開発者は、一国の市場を超えてセキュリティの問題にアプローチし、国境を越えた新たなセキュリティ脅威に協力して対処し、共通のコンセプトを持ってトレーニングされたグローバルな主体を構築することができる。	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。
23	3	団体		翻訳）サイバー・フィジカル・セキュリティに日本固有のフレームワークを採用することには慎重な姿勢を続けたい。私たちは、経済産業省が、IoTとクラウドコンピューティングの融合にフォーカスすることで、現在の国際的に認められたフレームワークを超えたガイダンスを開発していると認識している。ISO/IEC 30141:2018 及び ISO/IEC 17789:2014 等の既存のフレームワークでは、IoTおよびクラウドコンピューティングの領域への既存のISO標準の適用可能性をマッピングするための参照アーキテクチャを確立しているが、実装ガイダンスにはまだ大いにギャップがある。 このように日本政府がフレームワークの開発と適用を進める一方、我々は、産業界に不注意による混乱を生じさせ、他の試み(例：米国、EU、その他の地域における試み)との相互運用性による利益を損なうことを避けるため、国際的に認められた規格と最大限の整合を確保するために継続的に文書を見直すことを経済産業省に求めたい。	本フレームワークは、主要な国際規格等も参照し策定にしております。なお、新たな国際規格等も常に策定されることから、いただいた御意見も参考に、本フレームワーク策定後においても、様々な国際規格等も参照し、適切に対応して参ります。
23	4	団体		翻訳）フレームワーク原案にて提唱されているモデルは、三層（「企業間のつながり」、「フィジカル空間とサイバー空間のつながり」、「サイバー空間におけるつながり」）と6つの構成要素（ヒト、ソシキ、システム、モノ、データ、プロシージャ）を特定しているが、デジタル産業エコシステムにおける主要な関係者や関係性を理解するための有用な概念を提供している。責任とセキュリティの考慮事項が重なる可能性がある場所、およびそれらが分岐する可能性がある場所をうまく示している。さらに、それは現代のデジタル産業サプライチェーンの複雑なエコシステムにおいて、明白ではない可能性があるセキュリティ計画に関わる資源または関係性を考慮することをサイバーセキュリティ担当者に促している。 原案の添付Aに示されているように、三層構造は、リスク管理活動を導くための分析ツールに有用に変換される。 一方、6つの構成要素は、分析ツールとしてではなく、例示のための概念として最も役立つ。私たちは、多くのサイバーセキュリティ専門家による適用に当たって、分析ツールとして、6つの構成要素が多くの複雑性と曖昧性をもたらす可能性を気にしている。第II部では、特に、サイバーセキュリティの専門家が組織のサイバーセキュリティ計画およびポリシーを策定する際に、限られたリソースの割り当てに役立つようにモデルを簡略化できるかどうかを検討する価値があると考えている。	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。
23	5	団体	Part III	翻訳）フレームワークは、国際的によく知られたベストプラクティスとよく整合しており、デジタル産業のエコシステム及びサプライチェーンを保護するに当たり重要と考えられる広範囲にわたる考慮事項を提示している。	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。
23	6	団体	CPS.AM	翻訳）資産管理に関する第2原案のカテゴリには、すべてのハードウェアとソフトウェアの一覧を管理し、製造日や製造条件などの記録を作成するためのガイダンスが含まれている。また、ソフトウェアが一覧化されるだけでなく、適切にライセンスされ、最新化されているかどうかも確認するため、透明性の高い検証可能なソフトウェア資産管理(SAM)のプラクティスを採用するためのガイダンスも含むべきである。ライセンスされていないソフトウェアは、マルウェアの発生に関連するリスクを軽減するような重要なセキュリティ更新プログラムを受け取る可能性が低いため、その使用により有害なサイバーセキュリティインシデントのリスクが高まる。信頼できないソースからのライセンスされていない技術には、悪意のあるアクターによって挿入された埋込み型のマルウェアが含まれる可能性がある。現在のCPS.AM-4の後に、新しい対策要件を追加することを推奨する。 “ CPS.AM-X. ソフトウェアが適切にライセンスされ、最新のものであることを保証するために、透明性の高い検証可能なソフトウェア資産管理プラクティスを適用する。」 国際的に認められている関連規格はISO 19770-1である。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-1

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
23	7	団体	CPS.AM-5	翻訳）「クラウドセキュリティガイドライン活用ガイドブック」(経済産業省, 2013)は、特にクラウドサービスを利用する観点から、ユーザーの役割と責任に関して契約事項を明記する際、考慮するポイントを参照するのに役立つ。また、以下の国際標準がこの目的に対して有用である： ・ISO/IEC 17789：2014(情報技術) — クラウド・コンピューティング — 参照アーキテクチャー ・ISO/IEC 19086-1：2016、ISO/IEC 19086-1：2016 (情報技術) — クラウド・コンピューティング — サービス・レベルの契約(SLA)フレームワーク — パート1：概要と概念 ・ISO/IEC 19086-4：2019、ISO/IEC 19086-4：2019 (クラウド・コンピューティング) — サービス・レベルの契約(SLA)フレームワーク — パート4：保安の、そして、PIIの保護の構成要素	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.AM-7
23	8	団体	CPS.AM-6	翻訳）機能、重要性、およびビジネス上の価値に従って資産を分類することは、効果的な資産管理にとって重要だが、それに基づいてヒトを分類するのにはそれほど意味がない。組織内の個人は、ビジネス上の価値の重要性に関係なく、同様のセキュリティ上の課題(例：芳しくないサイバー衛生、内部不正)を示す可能性がある。本対策要件から「ヒト」を削除することを勧める。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-6
23	9	団体	CPS.BE-3	翻訳）この対策要件は、CPS.AM-2といくらか重複しているように見える。CPS.AM-2を削除することを勧める。	ご指摘いただいた2つの管理策は、関連するものではあるものの、内容が重複するものではないと認識しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
23	10	団体	CPS.GV	翻訳）強力なサイバーセキュリティガバナンスを実現するための基本的な方法は、サイバーセキュリティに関する情報が、必要に応じて、執行役員や取締役会を含む組織の上級管理職に伝達されるのを確実にすることである。CPS.GV-4に続いて、新しい対策要件を追加することを推奨する。 「サイバーセキュリティリスク管理ポリシーおよび重大なサイバーセキュリティインシデントに関する重要な情報を組織の上級管理職に伝達するためのプロセスを確立する」	ご指摘の通り、サイバーセキュリティに対する上級管理職のコミットは非常に重要と考えます。既存の対策要件であるCPS.GV-1、CPS.RM-1等について、いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.GV-1、CPS.RM-1、CPS.RP-1
23	11	団体	CPS.RA-1	翻訳）本対策要件が総合的な脆弱性と組織の資産の簡単な評価と文書化を要求しているのか、それとも個々の脆弱性の評価と文書化を要求しているのか明確でない。要件が後者に対するものであること、つまり、組織がその資産の個々の脆弱性を識別し文書化すべきであることが重要である。	対策要件の含意についてはご指摘いただいている通りと考えます。いただいた御意見については、原案のとおりとさせていただきます。
23	12	団体	CPS.SC-2	翻訳）明確さと使いやすさを確保するため、対策要件はいくつかの別々の記述に分割したほうがよい。さらに、第2原案は現在、第三者あるいは自己証明によってセキュアで安全であると認証されたIoT機器を使用するためのガイダンスを提供している。しかしながら、IoT機器を評価するための標準やベンチマークとはリンクしていない。基準となる標準やベンチマーク、認証、または自己証明がなければ、IoT機器の安全性とセキュリティに関するさまざまに異なる情報が伝達される可能性がある。認証されたIoT機器の使用に関する原案の記載を将来のバージョンまで延期することを勧める(たとえば、より広く検証されたIoTセキュリティ標準が存在するタイミングで追記する)。対策要件を次のように再編成することを推奨する。 "CPS.SC-2. 組織の運営を維持するために不可欠な関係者を特定し、優先順位を付け、評価する。" “ CPS.SC-X. サービスおよびシステム運用において、サービスを効率的かつ効果的に運用および管理するサービス提供者を選択する。" “ CPS.SC-X. 機器を調達する際に、マネジメントシステムが適切に確立、運用され、ヘルプデスクとサポートシステムが適切に準備されているIoT機器のサプライヤを選択する。"	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.6 サプライチェーンリスク管理 CPS.SC-2 添付C CPS.SC-2
23	13	団体	CPS.AC-6	翻訳）ネットワークやその他の機密資産へのアクセスを保護するための多要素認証の使用を強く支持する。 最近の技術開発により、認証に対する追加のリスクベースのアプローチ(地理位置情報、機器認識、パターン分析などのコンテキスト情報の使用等)が可能となった。これは、多要素または生体情報による識別と組み合わせて使用できることが多い。したがって、対策要件を次のように変更することを推奨する。 「ネットワークを介して特権ユーザーとしてシステムにログインする際に、2種類以上の認証および/またはその他のリスクベースの認証技術を組み合わせた多要素認証を採用する。」	ご指摘いただいた追加のリスクベースのアプローチは、多要素認証の枠組みの中で利用されるものと認識しておりますので、本対策要件に対していただいた御意見については、原案のとおりとさせていただきます。
23	14	団体	CPS.DS-6	翻訳）バージョンアップとセキュリティパッチを適用してソフトウェアを保守することは、ネットワークとIoTの両方のセキュリティにとって重要である。 そのため、次のように、この重要なセキュリティ対策に個別の対策要件を割り当てることを推奨する。 "CPS.DS-6：IoT機器、通信機器、回路などに対する、定期的な品質チェック、スタンバイデバイスと無停電電源装置の準備、冗長性の提供、障害の検出、交換作業を実施する。" "CPS.DS-X：IoT機器を含むソフトウェア資産が、すべての最新のアップグレードとセキュリティパッチで維持されることを確実にする。"	保守については特にCPS.MAにて記載しておりますので、御意見については、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
23	15	団体	Annex E	翻訳）フレームワークが関連するISO国際規格に見られる次の用語の定義と用法を参照することは有用かもしれない。 (1) 「アクチュエータ」[SOURCE：ISO / IEC 20924：2018、3.2.2] (23) 「ハッシュ値」[SOURCE：ISO / IEC 27037：2012、3.11] (24) 「識別子」[SOURCE：ISO / IEC 20924：2018、3.1.21] (28) 「IoT」[SOURCE：ISO / IEC 20924：2018、3.2.1] (29) 「IoT装置」[SOURCE：ISO / IEC 20924：2018、3.2.4] (56) 「センサー」[SOURCE：ISO / IEC 20924：2018、3.2.9] (57) 「サービス」[SOURCE：ISO / IEC TR 17028：2017、3.1] (64) 「タイムスタンプ」[SOURCE：ISO / IEC 18014-1：2008、3.12] (65) 「信頼性」[SOURCE：ISO / IEC 20924：2018、3.1.32] また、[IoTの信頼性]について[SOURCE：ISO / IEC 20924：2018、3.2.10]にチェックしたほうがよい。	いただいた御意見も参考に、修正いたします。 修正箇所：添付E 該当部分
24	1	団体		翻訳）IoTは、世界の経済や社会を変革する態勢を整えており、日本のSociety5.0の重要な構成要素でもある。IoTが提示する課題は、コラボレーティブなセキュリティアプローチをこれまで以上に重要にしており、世界中の政府は、IoTセキュリティの将来を形成するための重要な選択をしている。経済産業省がこの問題の重要性を認識し、マルチステークホルダーのアプローチを用いてこの問題に取り組むための行動を起こしていることを嬉しく思う。 具体的には、企業がIoTエコシステムへの信頼を強化するため、方針を策定し、施策を実行する際の指針として、「セキュリティ・バイ・デザイン」を基本原則として採用したことを賞賛したい。	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。
24	2	団体	CPS.AC-1 CPS.AC-4 CPS.AC-6 CPS.AC-8	翻訳）デバイスソフトウェアの更新を認証する：METIフレームワークはユーザー認証には対応していますが、機器の「自動的な」ソフトウェアアップデートの認証を要求するようには見えない。これがないと、攻撃者は接続をハイジャックし、悪意のあるソフトウェアをIoT機器にダウンロードする可能性がある。(OTA原則1、6)	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.MA-2
24	3	団体	CPS.AC-1 CPS.AC-4 CPS.AC-6 CPS.AC-8	翻訳）機器間通信を認証する：ユーザーと機器の間、または機器とサーバー間の通信だけでなく、機器間の通信も認証する必要がある。(OTA原則13)	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.7 アイデンティティ管理、認証及びアクセス制御 CPS.AC-8
24	4	団体	CPS.DS-1 CPS.DS-2 CPS.DS-3 CPS.DS-4 CPS.DS-6 CPS.DS-9 CPS.DS-12 CPS.DS-13 CPS.MA-1	翻訳）制御ソフトウェアが安全でアップデートされており、暗号化されていることを確認する：METIフレームワークは、機器、サーバー、およびそれらの通信のためのソフトウェアアップデート、監査、暗号化を明示的に要求していますが、モバイルデバイスやワークステーション上で、あるいは、Webブラウザ経由で実行されるアプリケーションである可能性のある機器制御ソフトウェアについては触れていない。システムは最も弱いノードと同程度の強度しか持たないため、すべてのシナリオでこれらの制御アプリケーションを検討することが重要である。これらの推奨事項を制御ソフトウェアに適用することは既に暗に示されている可能性があるが、明示的にすることを推奨する。(OTA原則1、2、3、6、7、8、13)	いただいた御意見については、既存の記載でカバーされているものと認識しておりますので、原案のとおりとさせていただきます。
24	5	団体	CPS.IP-1	翻訳）強力でユニークなパスワードのための特定の要件：METIフレームワークでは、デフォルト設定を変更する初期プロセスについて言及しているが、さらに一歩進んで、各機器またはサービスに強力で一意のパスワードを設定することが重要ではないかと考えている。このような場合、資格情報が開示されても、影響範囲は限定される。フレームワークは、適用可能な場合は多要素認証を要求しており、これも推奨するベストプラクティスであることに同意する。(OTA原則13)	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.AC-4、CPS.IP-1
24	6	団体	CPS.IP-1	翻訳）パスワード変更の通知：これは非常に具体的な問題だが、機器、サービス、またはアプリケーションを乗っ取る攻撃の検知に役立つ。パスワードが変更されると、ユーザー(または管理者)に通知される。(OTA原則16)	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.IP-1
24	7	団体	CPS.IP-1	翻訳）パスワードの安全な回復：パスワードを忘れた場合、サプライヤはパスワードをリセットするための安全な回復メカニズムを提供する必要がある。これにより、攻撃者はパスワードの変更を強制できず、その結果生じる対話を傍受できない。(OTA原則14)	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.IP-1

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
24	8	団体	CPS.RA-1 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.DS-5	翻訳）接続が失われたときの動作を理解する：METIフレームワークは、複数の箇所でDDoS攻撃に対するレジリエンスに対処しているが、単純な接続の喪失(意図的かどうかにかかわらず)も、これらのシステムとサイバーフィジカルの相互作用に大きな影響を与える可能性がある。これらのシステムの所有者は、接続性が失われた際の機器、サーバー、および制御アプリケーションの動作を理解し、それをリスク評価に組み込む必要がある。(OTA原則21)	ご指摘いただいたポイントは、サイバー・フィジカル・システムにおけるリスクとして非常に重要なものかと認識しておりますが、必ずしもセキュリティ事象に起因するものでないと考えられます。そのため、いただいた御意見については、原案のとおりとさせていただきます。
24	9	団体	CPS.RA-1 CPS.RA-4 CPS.RA-5 CPS.RA-6 CPS.DS-5	翻訳）ソフトウェア更新中の動作：ソフトウェアアップデート中の機器の動作を理解することがこの問題と関係する。アップデートがインストールされている間、一部の機器は通常どおりに動作し続けるが、他の機器は動作に大きな影響を与える可能性がある、長い「一時停止」を経る。これはデータの収集と整合性に影響を及ぼし、攻撃者に潜在的な攻撃対象を提供する可能性があるため、動作をリスク評価に織り込む必要がある。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.MA-1
24	10	団体	CPS.AM-1 CPS.CM-6 CPS.SC-2 CPS.DS-4	翻訳）購入前のライフサイクルの問題：これは、フレームワークで既に暗に示されている可能性があるもう1つの問題だが、機器またはサービスの購入前に明示的に考慮する必要があるライフサイクルの問題がいくつかある。 [例] ・サプライヤは、セキュリティのパッチ適用とサポートのために一定の期間を約束したか？ ・その時間が経過すると、機器やサービスはどのように動作するか。(つまり、すべて同じ機能がまだ利用できるのか、それとも制限されるのか) (OTA原則1、6、8、19、21)	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.SC-2, CPS.SC-4
24	11	団体	CPS.DS-5 CPS.AN-1 CPS.MI-1	翻訳）電子メールのやり取りを保護する：電子メールは主要な攻撃経路であり、攻撃者が偽の電子メールを送信して悪意のある機器ソフトウェアをダウンロードするようにユーザーを誘導するケースが報告されてる。これを防ぐための方法のひとつは、Eメール認証技術(SPF、DKIM、DMARC)および、サーバー間でEメールを暗号化するTLSの使用である。これは通常の機器、サーバー、アプリケーションのやり取りの「帯域外」だが、この脆弱性は大きなリスクをもたらす可能性がある。(OTA原則34、35、36)	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C
24	12	団体		翻訳）セキュリティは継続的なプロセスであり、サプライチェーンマネジメントによるIoTおよび産業用制御システムの保護に向けたこの包括的な取り組み、および主要な国際規格との整合性を確保することの重要性の認識に対して、経済産業省を賞賛したい。エコシステムのすべての層において信頼が不可欠であり、このフレームワークは、インターネット全体、特に、IoTと産業用制御システムのセキュリティを向上させるという共通の目標に取り組むステークホルダーにとって優れたリソースとなる。	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。
24	13	団体		翻訳）この分野のいくつかの重要な文書を参照いただきたい。それは、セキュリティ・バイ・デザインを改善するような類似または補足的な取り組みの基礎、あるいはモデルとして役立つ。 1. インターネット・ソサエティ・オンライン・トラスト・アライアンス(OTA) IoTトラストフレームワーク：セキュリティ、プライバシー、そして長期的な持続可能性(ライフサイクル)の問題に対処する40の原則を導入している。開発には、業界、政府、および消費者を代表する100人以上の利害関係者が関係し、推奨される一連のコアアクションに貢献した。フレームワークは日本語で利用可能である： https://www.internetsociety.org/iot/trust-framework/ 2. インターネット・ソサエティは、IoTセキュリティを世界規模で強化するために多数のマルチステークホルダープロセスに取り組んでいる。カナダでは、カナダ政府(イノベーション、科学と経済開発、ISED)、カナダ・インターネット政策・公益相談所、CANARIE、およびカナダ・インターネット登録局（CIRA）と提携して、消費者教育、ネットワークのレジリエンス、およびIoT機器のラベリングのための推奨事項とフレームワークを用意している。このイニシアチブの成果の中には、IoT機器の課題を念頭に置いて設計された、オープンソースのセキュア・ホーム・ゲートウェイのプロトタイプを作成するためのCIRAの取り組み支援がある。https://iotsecurity2018.ca/	いただいた御意見は、今後、IoT機器に関する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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
				フレームワークのさらなる発展に関連する可能性がある他のリソースには以下が含まれます。 1. 英国で「消費者向けIoTセキュリティのための行動規範」と併せて開発された「IoTにおけるセキュリティとプライバシーのマッピング」： https://iotsecuritymapping.uk/ 2. ENISAの「重要情報インフラにおけるIoTに対するベースラインセキュリティの推奨事項」： https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot 3. 昨年11月にバンコクで開催された最新のIETF会議のIETF IoTラフガイド - インターネット技術標準化委員会(IETF)での関連標準作業のスナップショット：IoTに関連するIETFの成果をより簡単に閲覧するためのリソースとして、これらをすべてのIETF会議の前に公開している。 https://www.internetsociety.org/blog/2018/10/rough-guide-to-ietf-103-internet-ofのこと/ 4. IoT機器をプロビジョニングし、ネットワークアクセス制御設定を自動化するのに役立つ「製造元使用説明仕様」(MUD)が、2018年に提案された標準としてインターネット・エンジニアリング・ステアリング・グループ(IESG)によって承認された。https：// datatracker .ietf.org / doc / draft-ietf-opsawg-mud /	
25	1	個人	脚注3	脚注の「米国国立標技術研究所」は、「米国国立標準技術研究所」の誤記です。	いただいた御意見のとおり、修正いたします。 修正箇所：脚注３
25	2	個人	第Ⅲ部3.	表のタイトルの行にも縦罫線があったほうが読みやすいと思います。（添付Ｃの表のように）	いただいた御意見のとおり、修正いたします。 修正箇所：本文第III部 3. 対策要件 (1) 対策要件のカテゴリー
25	3	個人	第Ⅲ部3.	１８行目「ver1.1」、同頁の表のタイトルの「v1.1」、４８頁の表の「関連標準等」欄の「Ver.1.1」は、記載の統一が必要です。	いただいた御意見のとおり、修正いたします。 修正箇所：第III部 3.
25	4	個人	添付C	表のタイトルの「rev.4」は、本文と同様に「Rev.4」のほうが適当です。	いただいた御意見のとおり、修正いたします。 修正箇所：添付C
26	1	企業	添付C CPS.IP-2	対策例<High Advanced>の記載において、ソフトウェアの制限とソフトウェアのインストールの不可を、「ともに」で繋ぎ両方実施するような対策例としているが、2つの対策をどちらも実施することは現実的でないため、どちらかの対策を実施するような記述とすべきである。 ■ 理由 マルウェアの多くはファイルを配置しただけで実行可能なソフトウェアであり、ホワイトリスト及びブラックリスト対策はソフトウェア配置後、ソフトウェアが実際に実行される際に制御が行われることが多いという点。 また、ファイルを配置しただけで実行可能な場合等において、ソフトウェアのインストール（ファイルの配置）を不可とする要件の実現性は乏しいという点から、インストールを不可とする要件を「又は」等でつなぎ両対策のどちらかの実施を促すように修正することが望ましい。	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.IP-2
26	2	企業	添付C CPS.CM-3	ホワイトリスト型マルウェア対策も有効であるため、対策例<High Advanced>に併記すべきである。 ■ 理由 振る舞い検知型に対策を限定しているが、振る舞い検知型も振る舞いの定義を更新することがあり、大量に配布するようなIoT機器の場合に必ずしも最適ではない。 機能が限定できるIoT機器の場合には、ホワイトリスト型の対策も併記すべきである。	下の御意見の内容も踏まえ、修正を検討いたします。 修正箇所：添付C CPS.CM-3
26	3	企業	添付C CPS.CM-3	ホワイトリスト型マルウェア対策も有効であるため、対策例<Advanced>に併記するべきである。 ■ 理由 パターンファイル型の検出・修復ソフトウェア導入と限定しているが、ＩｏＴ機器の機能が限定されていること、線が細いネットーク環境での利用等を考慮してホワイトリスト型の対策を併記すべきである。	上の御意見の内容も踏まえ、修正を検討いたします。 修正箇所：添付C CPS.CM-3
26	4	企業	添付C CPS.AM-1	対策要件としては、資産管理が基本ではあるが、<High Advanced>な対策例としては、資産管理上で発見された異常な資産についての対処も同時に実施するメカニズムが良いです。従って、<High Advanced> の対策例に”許可されていない資産を自動的に検出するメカニズムを導入”との表記があるが、”許可されていない資産を自動的に検出し、管理情報から外す・システムから切り離す等を実行するメカニズムを導入”としたほうが良いと考えます。	上の御意見の内容も踏まえ、修正いたします。 修正箇所：添付C CPS.AM-1

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
26	5	企業	添付C CPS.AM-5	外部システム上に自組織のポータブルストレージを接続して、自組織から利用する場合を示しているのか、自組織のポータブルストレージを外部システムから利用する場合を示しているのか、それとも両方であるのか表現がわかりません。どちらかまたは両方なのかにより、使用制限を実施する主体組織が変わります。従って、<Advanced>の対策例について「外部のシステム上での自組織のポータブルストレージの使用を制限する。」の補記が必要です。 また、ポータブルストレージとは何を示しているのか？持ち運び可能なストレージ装置を指していると想定した場合、本対策は、ポータブルストレージに限らず、すべてのストレージ（データ保存装置）に共通するべきと考えます。従って、<Advanced>の対策例として、"ポータブルストレージ"の表記は、単純にストレージ　（データ保存装置）のほうがふさわしく思います。	本対策例は、ご指摘いただいてる内の前者を意図したものでございます。いただいた御意見の内容を踏まえ、その点がよりわかりやすい表現となるよう修正いたします。また、ポータブルストレージとは、持ち運び可能なストレージデバイスを指しておりますが、ご指摘を受けて、ストレージデバイス全般を対象とした記載に変更いたします。 修正箇所：添付C CPS.AM-5
26	6	企業	添付C CPS.RA-3	一般に公開されている脅威情報以外を利用した犯罪・問題が多く発生しているため、情報入手の方法のレベルを上げる必要があると考えます。そのため、本対策要件の＜High Advanced＞対策例においては、一般的に更改されている情報のみを利用するのではなく、専門家によって調査分析された、ダークウェブ上の情報も視野に入れるべきであり、以下の対策例を追記すべきです。 ・組織は必要に応じて、専門家が提供するサービス等を活用し、一部の専門家しか知りえない情報を入手しそれをもとに、脅威を特定する。	いただいた御意見の内容を踏まえ、修正いたします。 修正箇所：添付C CPS.RA-3
26	7	企業	添付C CPS.SC-5	取引先等の他組織においても、CSFにおける特定(Identify)機能も強化することが望ましく、ダークウェブ調査等により自社のセキュリティリスクが低いことを委託元に定期的に提示することで、双方のセキュリティ対策への意識を高めることに繋がると考えます。 また、信頼できるサービスをリスト化することで、使用するサービスのレベル差を少なくすることができると考えます。従って、<High Advanced>の対策例に以下を追加して頂きたいです。 ・重要な取引先およびその再委託先以降の組織は、ダークウェブ調査等による攻撃の予兆、情報流出の事実がないかを調査し、組織に対して結果を定期的に報告する。 ・使用する調査サービスは、リストに掲載されたサービスを利用する。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.SC-5
26	8	企業	添付C CPS.AC-5	システム管理者であっても、セキュリティ事故による被害を最小化するため、システム管理者の権限を最小化できること、重要なサービスや保護されたプロセスは停止不可とできることが必要と考えます。そのため、<High Advanced>の対策例に以下を追加して頂きたいです。 ・組織は、セキュリティ事故による被害を最小化するため、システム管理者の権限を最少化させることができる。 ・組織は、セキュリティ事故による被害を最小化するため、システム管理者であっても、サーバの重要なサービスや保護されたプロセスは停止不可とすることができること。	下の御意見の内容も踏まえ、修正を検討いたします。 修正箇所：添付C CPS.AC-5
26	9	企業	添付C CPS.AT-2	対策要件には、"割り当てられた役割を遂行するための適切な訓練"とあるが、対策例でも同じ言葉を繰り返してるため、アクションを取るには不親切と考えます。そのため、"割り当てられた役割を遂行するための適切な訓練"について、訓練の例を示したほうが、対策が取りやすいと考えます。 よって、"実際のインシデント発生時を想定した、シミュレーション"等具体的に記したほうが良いです。	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.AT-2
26	10	企業	添付C CPS.DS-3	政府統一のセキュリティ基準の2018年度改定において、外部と送受信するすべてのデータについての暗号化を基準としています。対策要件にも同様な事が示されているにも関わらず、対策例において検討範囲を狭めるのは適切ではありません。そのため、本対策要件の＜High Advanced＞対策例においては、すべての送受信データを暗号化するべきであり、重要度の高い・低いに限らず、すべての通信データを適切な強度で暗号化するべきです。なお、"重要度の高い機器からの"の部分は削除して問題ないと思います。	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.DS-3
26	11	企業	添付C CPS.DS-9	対策要件内に"不正なソフトウェアの起動を防止する"とあるが、対策例には通知・検知についての触れているのみであり、対策要件の起動防止について明確となっていません。 より明確に不正なソフトウェア（業務に無関係のソフトウェア）の起動防止を記載するべきであるため、<High Advanced>の対策例に以下を追加して頂きたいです。 ・組織は、不正なソフトウェアが検知された場合に、対象ソフトウェアの起動を防止するツールを使用する。 また、不正ソフトウェアの起動を防止する考え方に加えて、起動するソフトウェアを限定する対策も併記すべきと考えるため、<Advanced>の対策例に以下を追加して頂きたいです。 ・システムは、起動するソフトウェアを登録（特定）することで、登録されていないソフトウェアの起動を停止する	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.DS-9

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
26	12	企業	添付C CPS.IP-7	外部からの攻撃に関する評価の一つとして、ダークウェブ調査を追加すべきと考えます。従って、<Basic>の対策例に以下を追加して頂きたいです。 ・組織は、攻撃対象となっていないことを定期的な評価を実施し、管理責任者へ報告する。	ご指摘の点は、添付C CPS.RA-3のHigh-Advancedにおいて、「組織は、必要に応じて、専門家が提供するサービス等を活用し、一部の専門家しか知りえない情報を入手しそれをもとに、脅威を特定する」と記載しておりますので、そちらをご参照いただきたく存じます。
26	13	企業	添付C CPS.PT-1	OS機能のログだけでは、様々な場面におけるニーズに対応できないことを考慮し併記すべきと考えます。従って、<High Advanced>の対策例に以下を追加して頂きたいです。 ・収集するログは、セキュリティインシデントの検知に加え、セキュリティ事故及び不正の原因を事後に追跡することに有効であるため、OS機能では残らない詳細ログ(OSコマンドレベル)も収集する。	下の御意見の内容も踏まえ、修正を検討いたします。 修正箇所：添付C CPS.PT-1
27	1	団体		個々に示されている対応指針について、確かにやるべきこととしてみることができるが、文書全体を通じ（特に「理由」での指摘のとおり）、「本フレームワーク」の説明がブレており、結局、何を「フレームワーク」として構造的に示したいのか、判然としない。 本フレームワークとは、 ・新たな産業社会の構造＝３層構造と６つの構成要素のことか？ ・この文書の構成（第I 部、第II 部、第III 部）のことか？ ・セキュリティ対応指針の集合体のことか？ ・共通対策の集合体のことか？ ・分析対象を明確化するアプローチ方法の集合体か？ また、NIST Cybersecurity Framework v1.1 と対比させて、「ハーモナイズ」としているが、現状では、3 層構造における検討指針の提案をNISTのフレームワークに沿って分類しているにすぎず、新たなフレームワークの考え方が示されていると理解し難い。 ■理由 「本フレームワーク」としての表現が下記の通り多様なため。 ①(P.Ⅰ)エグゼクティブサマリ 24 行目(５つ目の○) 「本フレームワークは、…付加価値を創造する活動が直面する新たなリスクに対応していくための指針」 ②(P.4) 3．フレームワークを策定する目的と適用範囲 「本フレームワークは新たな産業社会の全体像」 ④(P.7) 7．フレームワークの使い方 「本フレームワークは、…全体を以下のように構成する （1） 第Ⅰ部（コンセプト）・・・ （2） 第Ⅱ部（ポリシー）・・・ （3） 第Ⅲ部（メソッド）・・・ ： このように、本フレームワークは…状況の変化に応じて進化していくものである」 ④(P.7) 7．フレームワークの使い方 「本フレームワークで示す三層構造モデルを参考にして」 ⑤(P.9)10 行目～ 「本フレームワークでは、…サプライチェーンの概念に求められるセキュリティへの対応指針を示すことを目指す」 ⑥(P.10)3 行目～ 「本フレームワークの第Ⅰ部では、…各構成要素が各リスク源に対応する方針を整理するためのコンセプトを明らかにする」 ⑦(P.11)8 行目～ 「３つの層でバリュークリエイションプロセスにおけるリスク源を洗い出し、６つの構成要素について各リスク源に対するセキュリティ対策の方針と具体的な対策事例を示すのが、本フレームワークの基本構成である」 ⑧(P.21)5 行目～ 「本フレームワークは、…全産業に共通的なセキュリティ対策を示している」 ⑨(P.24)第Ⅱ部 ポリシー：リスク源の洗い出しと… 「本フレームワークでは、第Ⅰ部第２節にて提示した三層構造アプローチに基づいて分析対象を明確にする方法を提供する」	本フレームワークは、「Society5.0」の社会に求められるセキュリティ対策の全体像を提示するもので、①三層構造・６つの構成要素を活用した産業社会の捉え方、②三層構造・６つの構成要素に基づいたセキュリティリスクの洗い出し、③ 特定したセキュリティリスクに対応するための対策要件・対策例集から構成されるものです。いずれも本フレームワークを構成するものでありますが、いただいた御意見の内容を参考に、丁寧な説明となるよう修正を検討いたします。 また、本フレームワークでは、NISTのCSFの区分を参考に対策要件を整理していますが、CSF, SP800-171, ISO/IEC 27001 との対応関係を添付Ｄで示しており、海外主要規格と整合性にも配慮しています。 修正箇所：はじめに等

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
27	2	団体		第1 層はシステムや製品のライフサイクルの中で議論した方が表現しやすいので、ライフサイクルを軸にして構成を見直した方が良いと思う。 ■理由 人や組織の観点から見て、第1 層と第2、3 層を分けて論じるのには限界があると思う。 サプライチェーンや、システムの上位から下位まで、全てに人や組織が関わるので、それだけを切り出して階層を分けて論じるのは難しいと感じる。 例えば、物理的なアクセスによるセキュリティリスクは内部犯罪にも関わるため、内部犯罪向けの対策も必要となる。スマートホームでは居住者や来訪者もシステムを攻撃してくることもあり、階層を分けて議論するのはそぐわないと感じる。 このように第2 層や第3 層でも運用やメンテナンスで人の関わりが出てきて、それを意識したセキュリティ対策が必要となる。それが表現できていないように感じる。	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ます。ライフサイクルを考慮したセキュリティ対策例は、産業分野や個社ごとに異なるものであり、産業サイバーセキュリティ研究会ＷＧ１分野別サブワーキンググループ等において、いただいた御意見も踏まえ、引き続き、最適なセキュリティ対策例を検討いたします。
27	3	団体	6. (2) ③	国外の規格との関係を整理した対比表について、具体的な解説を記載してほしい。 ■理由 ここで記載されている対比表は添付Ｄのことであると考えるが、添付Ｄについての解説（対比した規格、対比方法など）を記載があると、添付資料が有効に活用されると思う。	いただいた御意見の内容を参考に、修正を検討いたします。 修正箇所：第Ⅲ部1.(1)
27	4	団体	6. (2) ③	日欧のトラストサービスに関する制度比較を行い、欧州との相互運用性を実現するため、制度の補完と欧州との話し合いを元に実施するような内容に方針を立てるべきと考える。 ■理由 時刻を証明するタイムスタンプ局、本人を証明する電子署名に関して、日本では欧州同様のトラストフレームワークとしての法的根拠がない。また、モノ(IoT)や企業・組織などのソシキを証明する根拠となるべき証明書は、欧州のe-Seal に相当するものが国内に法整備がされていない。 比較資料として、総務省の調査研究の一環として開催されたワークショップである、以下の資料の参照をおすすめする。 (http://www.soumu.go.jp/main_content/000597573.pdf) 日・EU のトラストサービスに関する制度比較： (https://nosurrender.jp/trust_ws/docs/download/s05.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。
27	5	団体	第Ⅰ部 2.1 4.	① 欧州e-Seal と相互運用性を持つ日本版e-Seal を法制化し、企業に対して個人同様の証明書を発行して相互に信頼できるトラストフレームワークの構築を求める。 ② ６つの構成要素の中のソシキ、ヒト、モノそれぞれに対して証明書を発行し、ID をもとに相手を信頼してやりとり出来る仕組みの構築を提案する。欧州の仕組みそのものになる。 ③ ６つの構成要素の中のソシキ、ヒト、モノそれぞれに、信頼できる期間からの証明書を付与し、それぞれの構成要素の情報に対して証明書を発行する仕組みにすることを意見する。また、欧州のeIDAS との相互運用性を持たせることを意見する。 ④ ６つの構成要素の中のプロシージャとして、証明書を発行する機関に対して、監査する仕組みを提案する。また、欧州のeIDAS の監査の仕組みと、監査の信頼を担保できる相互運用性を実現することを意見する。	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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
				■理由 P.11 にある６つに整理された対象の中のソシキ、ヒト、モノそれぞれに対してID や証明書を付与し、それぞれの間が信頼できるトラストフレームワークの構築によって、目的の信頼するつながりが実現される。 日本国内だけで企業のつながりを持たせて、欧州、米国と信頼性の相互運用性が持てないことは、国家戦略として完全に主導権を欧州、米国に奪われている。e-Seal の定義やその先の企画の提議で進んでいる欧州の規格に積極的に提案することで主導権を持った企業間のつながりの仕組みを定義すべきである。 エストニアがソシキ・ヒトに対して証明書を付与してやりとりする環境をX-Road という情報交換基盤と国民ID で実現し、多くのサービスを実現している事例として有名である。 総務省 プラットフォームサービスに関する研究会 トラストサービス検討ワーキング グループ（第1 回）平成31 年1 月31 日の柴田構成員の資料のP.14 にX-Road の実態 （2019 年1 月時点：参照 https://www.x-tee.ee/factsheets/EE/#eng ） (http://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/02cyber01_04000001_00016.html) ＊ 接続サービス：2,691 ＊ クエリ：100,231,584/月 ＊ 接続事業者：民間651、公的機関504 とあり、そのサービス普及具合がわかる。 モノに対してのID 割当に関するEU・米国での検討状況は不勉強のため、わからない。 日本から発信すべき内容なのかもしれない。	
27	6	団体	p.19	６つの構成要素の中のデータの信頼性に対して、事前に定義が必要と考える。過度にデータへの信頼を担保した仕組みをターゲットしない仕組み作りになると予想する。 ■理由 データの信頼性は、あくまでデータ提供者の証明書を元にした、データソースの信頼の証明までしか出来ないのではないかと予想している。内容が事実か否かの証明は問わないことを割り切った仕組みになる。例えばA 新聞が発行したニュースは、発行元の信頼性までは担保できても、ニュースの中身までは信頼できないからである（フェイクニュース）。また、善意の誤報も部分切り取りニュースもあり得る。	データそのものの信頼性確保は「Society5.0」の実現に向けて重要な課題と認識しており、フレームワークでも対策要件（CPS.GV-3, CPS.SC-7, CPS.CM-4 等）として言及しています。 その上で、実際の産業活動への実装を進めるにあたっては、取り扱うデータの区分に応じたセキュリティ対策や、データの完全性、真正性等の確認手法も必要です。いただいた御意見も踏まえ、引き続き、検討を進めてまいります。
27	7	団体	p.21	“実態に則したセキュリティ対策の項目を列挙したプロファイルの作成に…"とあるが、プロファイルの例を提示してほしい（この後にこの種のプロファイルに関する記述がない） ■理由 通常、設計時に脅威分析や過去のインシデント分析から対策（セキュリティ機能）を設計しますが、このフレームワークはサプライチェーンの各プロセスを含んだ広範囲のモノなのでわかりやすい例があると活用しやすくなると思う。	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ます。一方、プロファイルに関しては、産業分野や個社ごとに異なるものであり、産業サイバーセキュリティ研究会WG1の下の分野別サブワーキンググループ等において、いただいた御意見も踏まえ、引き続き検討いたします。
27	8	団体	表2.1-1	フィジカル空間の物理現象を例示とともに定義すべきと考える。 ■理由 フィジカル空間の物理現象はヒトの行動だけ考えても、食事からトイレやまばたきまで数多あり、また、瞑想しているのか、考えているのか、寝ているのか、本人しか判断できないようなものも有り、すべての物理現象をデジタル情報へ変換することは困難と予想される。	本フレームワークは、すべての物理現象をデジタル情報に変換することを想定しているものではありませんが、いただいた御意見も参考に、新たな付加価値の創造に活用できる物理現象をイメージしやすいように修正いたします。 修正箇所：第Ⅰ部1.
27	9	団体	p.29	IoT の定義を、外部と通信を行う単位、など、定義すべきと考える。 ■理由 IoT 機器も複数のIoT 機器の組み合わせからできあがっている。HEMS の単位から車、電車、飛行機などの単位までも大きなIoT 機器になると思う。外部にデータ通信を行う際に、その機器からの情報である証明が証明書を元にやりとりできることが大事と考える。ただし、機器の内部へのハッキングを防ぐためにはより小さな機器への証明書の準備も必要になってくるとは思うので、最低限で用意すべき単位と、将来より詳細に用意された方が良い望ましい単位は別に追加で定義されていくと予想する。	いただいた御意見については、添付Eで定義しているとおりのため原案のとおりとさせていただきます。
27	10	団体	図2.1-8	(図2.1-8 中の)Acquirer は日本語がよい Acquirer＝調達側 ■理由 別の個所で"Acquirer"を利用していないし、図中の文章もあえて"Acquirer"としなければならない理由はないと思う。	いただいた御意見のとおり、修正いたします。 修正箇所：本文第II部 1.4 リスク対応の実施 図2.1-8

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
27	11	団体	第Ⅱ部 1.4.	具体的には、設計、調達時におけるセキュリティ・バイ・デザインの… ⇒「設計」「調達時」だけでなく「企画」も必要 ■理由 何を守るべきかを「企画」の段階で考える必要がある。	いただいた御意見のとおり、修正いたします。 修正箇所：本文第II部 1.4 リスク対応の実施
27	12	団体	第Ⅱ部 1.4.	「望ましい」ではなく「必要である」とすべき。 ■理由 「望ましい」では決して実行されない。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第II部 1.4 リスク対応の実施
27	13	団体	第Ⅱ部 1.4.	以下の内容についての修正案 実行される製造、輸送等の… ⇒実行されるソフトウェアの設計、実装を含んだ製造、輸送等の… ■理由 「委託先のソフトウェアの設計、実装」のプロセスとプロダクト品質が重要なため	いただいた御意見のとおり、修正いたします。 修正箇所：本文第II部 1.4 リスク対応の実施
27	14	団体	p.41	以下の内容についての修正案 具体的には、データが改ざんされたものでないか… ⇒具体的には、正しい機器と接続されているか、データが改ざんされたものでないか… ■理由 そもそも正しい機器が繋がれているかの確認が必要	いただいた御意見については、既に記載している内容(不正な構成要素(ソシキ、ヒト、モノ等)から生成・送信されたものでないか)と重複している内容と考えられるため、原案のとおりとさせていただきます。
27	15	団体	第Ⅲ部	High Advanced ⇒ Highly Advanced ■理由 文法的に正しく修正。またはVery Advanced。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 添付C
27	16	団体	CPS.RA-4	IoT セキュリティガイドライン 要点10, 要点12 に加え要件4 と思われる。 ■理由 IoT セキュリティガイドラインで企画からリスク分析に言及しているのは要点4 と思われる。	いただいた御意見のとおり、修正いたします。 修正箇所：本文第III部 3.4 リスク評価 CPS.RA-4
27	17	団体	CPS.RA-5	IoT セキュリティガイドライン 要点 4 、要点 7 を追記 ■理由 IoT セキュリティガイドラインの要点 4 と 7 がリスク判断の助けになると考えられる。	いただいた御意見のとおり、修正いたします。 修正箇所：本文第III部 3.4 リスク評価 CPS.RA-5
27	18	団体	添付D.3 A.12.1.1	(要求事項)記載の「利用可能にしなければならない。」を実現するために、Human Centered Design の取り組み（ISO9241-210 等のHCD プロセス）を実施することをお勧めしたい。 ■理由 利用可能にする操作手順書は、ISO9241-210 のHCD プロセスを導入することで成立、構築されるため。	いただいた御意見については、原案のとおりとさせていただきます。
27	19	団体	添付D.3 A.12.2.1	(要求事項)に記載の「利用者に適切に認識させること」を実現するために、Human Centered Design の取り組み（ISO9241-210 等のHCD プロセスに加え、ISO25010 の製品品質「使用性」および、「利用時の品質」の管理）を実施することをお勧めしたい。 ■理由 認識しやすいユーザインタフェースは、ISO9241-210 のHCD プロセスの導入、および、ISO 25010 の各品質を高めることで成立、構築されるため。	いただいた御意見については、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
28	1	企業	添付D.2	添付資料D.2において、NIST SP 800-171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」との対応表が示されています。 この対応表において、フレームワーク側の対策例が、"Basic", "Advanced", "High Advanced"三段階のレベルに分かれていますが、レベル別にどの対策例を実施すべきか集約し、レベル別逆引きができる表があると活用し易いと考えます。 ■理由 各業界及び各企業において、当フレームワークを参照しセキュリティ対策プロファイルを作成するにあたり、適用する分野、製品にマッチしたプロファイルとするには、上記対応が有益と考えられるため。	いただいた御意見については、原案のとおりとさせていただきます。
28	2	企業	第III部 3.9 3.11	以下の対策要件IDの「関連標準等」欄に、NIST SP 800-193, Platform Firmware Resiliency Guidelinesを追加されてはいかがでしょうか。 ：CPS.DS-11, CPS DS-12, CPS MA-1, CPS MA-2 ■理由 IoT機器のファームウェア改竄等の脅威対策に関する仕様の為、当該箇所での参照が有益と考えられるため。	第III部 対策要件の「関連標準等」においては、ISO/IEC 27001やIEC 62443、NIST Cybersecurity Framework等のセキュリティ対策全般について扱った文書をリファーしておりますので、いただいた御意見については、原案のとおりとさせていただきます。
29	1	団体	p.4-5	第四次産業革命と位置づけられている「Connected Industries」の成否が日本の将来に大きな影響を与えると考えている。この実現のためには、サイバー空間とフィジカル空間の融合と共に、企業間の協調の必要性とセキュリティの重要性は、報告書と同意見です。本フレームワークを活用し、自らが所属する企業等の実態に合わせて、必要となるセキュリティ対策を実施するに当たっては、当協会利用部会より2019/2/28発行した「IoTセキュリティチェックシート」も貢献できるものと考えており、こういった民間の活動との連携も推進いただけますと幸いです。	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。
29	2	団体	p.7	一般企業からみると、コアテクノロジーとなるIoT の活用を先ずは進め、理解と知恵を深め「Connected Industries」に向かうことが現実的であると考えており、IoTが企業に普及するかは「安全・安心にIoT 活用する知恵」つまりセキュリティがカギとなると考えております。 この部分で当協会利用部会より2019/2/28発行した「IoTセキュリティチェックシート」は、企業における具体的な活動に貢献できるもと考えており、こういった民間の活動との連携も推進いただけますと幸いです。	いただいた御意見は、サイバーセキュリティ政策を官民連携して進める上で参考にさせていただきます。
29	3	団体	4.	実務的には、ベンダーや部材選定において、今回策定されるフレームワークで言及されている観点も踏まえて購買意思決定が行われるべきことから、想定読者として、サプライチェーンでの購買意思決定にかかわる部門の追加が望ましいと考えます。	いただいた御意見については、フレームワークの想定読者として「サプライチェーンマネジメントに関わる戦略・企画部門の担当者」を記載しており、購買意思決定者も含まれると考えられるため、原案のとおりとさせていただきます。
29	4	団体	第Ⅰ部	「バリュークリエーションプロセスの中でフィジカル分野にとどまっていた情報がデジタル化され、データとしてサイバー空間に大量に移転」とありますが、このフレームワークにおけるコンテクスにおいて、具体的にどのようなフィジカル情報が対象になるかの例示があると読者が理解しやすいと考えます。 添付A.ユースケースに記載されている第2層にある内容を集約したものでよいと考えます。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ⅰ部1.
29	5	団体	表2.1-4	第1層(1)Cにおいて、サービス拒否攻撃に加えて、Wannacry等破壊型マルウェア・ランサムウェアによる組織内の情報機器の破壊が発生している状況を考慮し、ランサムウェアによる破壊が併記されることが望ましいと考えます。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第II部 1. 三層構造アプローチと 6 つの構成要素を活用したリスクマネジメントの進め方 1.2. 想定されるセキュリティインシデント及び事業被害レベルの設定 表2.1-4
30	1	企業		Society5.0 の描くような複雑システム社会では、すべての構成要素の信頼性(trustworthiness)を確立するのは非常に困難です。それよりも、必要な「信頼の輪」を形成する外部要因を制限し、信頼に値しないコンポーネントが重大事象を引き起こさない様にコントロールすることが重要です。 そのコンセプトの体現として、主に 2 つの手法が実践されています。 一つは多層防御構造です。システム上の重要なエンティティのみを信頼できるものと限定し、故意にシステムの多くの部分を信頼できない領域と定義します。例えば、多層に保護された領域にある計測機器から信頼性の低い上層とつなぐモデムへの通信は、認証・値を暗号化することができます。これによって、モデムが攻撃を受けた場合に、受信したメッセージを取りこぼすことがあっても、メッセージを改変することはできなくなり、信頼を保つことができます。計測機器とモデム間のコミュニケーションがデータダイオードで保護されていれば、モデムを足がかりに計測機器が攻撃を受けることはなくなります。 徹底したシステマティックな構造分析は、エンドデバイスのセキュリティを担保できない現状の制御システムでは困難です。適切なセキュリティレベルを満たすことができない箇所を早急に特定し、ネットワークから切り離すことができない場合にはネットワークの大部分から専用のセキュリティゲートウェイ、検知能力の高い強力な監視を導入して独立したゾーンを形成することが望まれます。 二つ目の手法に信頼の分配があります。例えば、ネットワークを形成するノードそれぞれに要求される信頼性を限定するブロックチェーンなどの技術、またはセンサーの読み取り値が他の値と比較して意味を成す値かどうかを確認するインテリジェントなシステムがあります。 以上から、制御システムの現状とブロックチェーンをはじめとするセキュリティ技術動向を踏まえ、すべての要素の信頼性を担保できないことを前提としたフレームワーク設計を推奨します。	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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
30	2	企業	第1部 4.	「信頼(trust)」と、「信頼性(trustworthiness)」を区別することが重要です。信頼は、本質的には心理状態の表現です。例えば、たとえそれが愚かな判断であったとしても、「自分の９歳の子供がこっそりお菓子を食べることはないと"信頼する(trust)"」ことができます。一方で、信頼性(trustworthiness)はセキュアな状態を担保する方策を指します。（この例においては、菓子棚に鍵をかける、など。）本フレームワーク文中においては「信頼」と「信頼性」というキーワードを明確に定義し、適切に使い分けることを推奨します。	本フレームワークでは「信頼」と「信頼性」というキーワードを使い分けていますが、いただいた御意見を参考に、用語集を修正します。 修正箇所：添付E
30	3	企業	Part I:4.(2)	このパラグラフの英語版は特に意図が汲み取りにくいため、英訳の再検討を強く推奨します。	いただいた御意見も参考に、修正いたします。 修正箇所：（英語版）Part I: 4.(2)
30	4	企業	第Ⅰ部 4.(3)	先述の通り、日本語版では「信頼性のチェーン」、英語では「Chain of trustworthiness」または「the trustworthiness chain」と表現することを推奨します。 信頼性のチェーンにおいては、構成要素の担保できる信頼性の想定と期待をコントロールする必要があります。 例えば、ある通信システムでデータが暗号化されていなくても、そのシステムを利用するアプリケーション全てがその事実を認識し、必要に応じて各自で暗号化を行うなどの対処を行えば信頼性は担保されます。よって、信頼性のチェーンを担保するには、「システム同士が対話する箇所において、対話する相手のシステムにおいてどのようなセキュリティレベルが想定されるか、そして期待される要件が実装されていることを裏付ける方策のドキュメンテーションとその管理」が必須であると考えます。	いただいた御意見も参考に、修正いたします。 修正箇所：（英語版）Part I: 4.(3)
30	5	企業		リスクベースの考え方に加え、リスク想定に起因しないセキュリティ衛生(security hygiene)対策レベルも必要です。セキュリティ衛生は、一般の衛生管理においてどのバクテリアに対して効果的であるかという理由にこだわらず、一定数の菌類に対処するために手洗いを実施します。同様にして、セキュリティ衛生としてグッドプラクティスがすべてのコンポーネントとサブシステムにおいて必須であるべきです。（例えば、データが暗号化されている場合、それが自作ではなくAES(Advanced Encryption Standard)など政府公認の暗号法であること、など。（スマートメータセキュリティ要求仕様カタログ[http://www.gridsec.org/docs/20150614%20E2E-Sicherheit-Anforderungskatalog-EN.PDF]を参照ください。） また、要求仕様はその要求事項が検証可能であることを明示するために、検証方法の仕様も付帯することを推奨します。要求事項が検証できない場合、その要件が信頼性チェーンにおいて破綻する可能性が高くなります。	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。
30	6	企業		ISO 27000 のようにビジネスリスクとITリスクの分析を中心としたリスク分析手法は、Society5.0 の描くスマート社会においては、不十分であると考えます。組織間の繋がりが複雑化した社会では、社会全体の抱えるリスクが単体組織の抱えるリスクを大幅に超過します。例えば、オリンピックゲームに脆弱なコンポーネントを提供してしまった組織においての最悪のケースは破産に止まりますが、オリンピックでサイバーインシデントが発生したことに対して、開催国全体が抱える障害はそれを大幅に超えます。 例えば、OpenSSL のHeartbleed(ハートブリード)バグは、オープンソースであったため、その脆弱性を生み出してしまった人々にとってのビジネスインパクトはほぼ皆無でした。しかし、多数のシステムで起きた損害は合わせて何百万ドルにも及びます。同様に、サプライチェーン上でサプライヤーが共通の下位サプライヤーを利用しているかどうかを管理することは困難であり、下位サプライヤーで起きたインシデントがサプライチェーン上で広域に影響を与えた場合の損害も大きくなる可能性があります。 合わせて、ISO 27000 に基づく情報セキュリティリスク管理は、物理的リスクを見逃しがちです。再度オリンピックの例を挙げると、スタジアムの消灯、ドーピング検査局の保冷庫の停止、またはスタジアムの防火シャッターの一斉閉鎖など、物理的ダメージを目的とする攻撃者による攻撃が情報システムをターゲットにした攻撃よりも大きな影響と損害を与えることができます。 したがって、ISO27000 を前提としたリスクアセスメントは情報セキュリティを対象とした標準であるため Society5.0 を前提とした本フレームワークにおいてはリスク分析範囲において誤解を招く恐れがあると考えます。本フレームワークではSTAMP や、ISA/IEC 62443 などプロセスシステムを対象に含む標準やフレームワークに焦点を当てることを推奨します。以上を踏まえ、本フレームワークの策定により多くのICS/SCADA分野の専門家が関わることを強く勧めます。また、官学民それぞれから様々な産業分野の専門家がバランスよく参加することも重要です。	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。
30	7	企業		リスクアセスメントの項において、プライバシーに関する観点が欠如しているように見受けられます。消費者によって豊富なデータが生み出されることを踏まえ、消費者に与えうるリスクについて分析することを推奨します。特に、欧州の取引先をもつグローバルサプライチェーンにおいては、流動性の高いデータを持つチェーン構成者すべてにGDPR(General Data Protection Regulation)ガイドラインに準拠することが求められます。	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。
30	8	企業	第Ⅱ部 1.1.(2) ③	すべてのデータの取得元と信頼レベルをラベリングすることは、一部の組織のシステム構成においてのみ実現が可能であり、すべての組織に当てはめることは難しいと考えます。加えて、AI システムによって生成されたデータの管理が困難です。AI システムは、インプットデータがアウトプットデータに与える影響を特定することが難しく、またインプットデータの信頼性レベルにばらつきがあったかどうか、最終結果の信頼性を確実に特定することができません。	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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
30	9	企業	全体	本フレームワークで参照される国際スタンダードは米国標準に偏りがみられます。グローバルサプライチェーンに在欧企業が含まれる可能性を踏まえ、GDPR やNIS directive をはじめとする欧州標準やガイドラインを参照に含むことを推奨します。	本フレームワークは、主要な国際規格等も参照し策定にしております。なお、新たな国際規格等も常に策定されることから、いただいた御意見も参考に、本フレームワーク策定後においても、様々な国際規格等も参照し、必要に応じて改訂して参ります。
30	10	企業	添付E	（55）ハッシュ値：ハッシュ値の特色の説明に不足が見られます。例えば、ハッシュ値のみから元の値に関する情報を導き出すことができない、２つのインプットが同じハッシュ値を持つ可能性が低い、インプットした値に詳細な変更をしたら、ハッシュ値は全く異なるものであるべき、など。	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	11	企業	添付E	（59）プロセス：産業制御システムなどサイバーフィジカルシステムにおいては、プロセスが物理プロセスを指すことがあります。本フレームワークの用語集においてISO2700 の定義を参照するのは誤解を招く恐れがあるため、制御システムを踏まえた定義を参照されることを推奨します。	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	12	企業	添付E	(20)公開鍵：公開鍵は、認証（例 ：デジタル署名）、鍵確立や他の機能に利用することも可能です。本用語集で提示された定義は暗号方式にのみ触れており、不十分であると考えます。	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	13	企業	添付E	(32)信頼性(Trustworthiness)：信頼性については定義されていますが、信頼(trust)の定義がされていません。信頼(trust)を一般に知られるように「信頼されたシステムは、そのシステム障害がセキュリティポリシーを破る可能性のあるシステム」と定義することを推奨します。	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	14	企業	添付E	(30)冗長化：電源供給や人員など、コンピュータ以外のシステムでも冗長化は可能です。そのため、本定義を見直すことを推奨します。	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	15	企業	添付E	(37)セーフティ(安全性)：セーフティにおいてはこれまで偶発的なリスクに焦点を当てていたのに対して、セキュリティは故意の、悪意を持った行為に焦点を当てます。セーフティとセキュリティを同時に扱う本フレームワークにおいて、「許容できないリスク」だけでは定義が不十分であり、定義を見直すことを推奨します。	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	16	企業	添付E	(43)セキュリティ・バイ・デザイン：セキュリティバイデザインは、ユースケース分析、リスク分析、脅威分析、資産の棚卸し、セキュリティアーキテクチャ、外部要求仕様分析、プライバシー影響アセスメントなどのステップを含みます。	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	17	企業	添付E	(41)セキュリティ事象：サイバーフィジカルシステムにおいては、セキュリティ事象は物理的・またはプロセスのセキュリティに影響を及ぼす可能性があります。	物理的・またはプロセスへの影響は、セキュリティ事象の結果と考えられますので、いただいた御意見については、原案のとおりとさせていただきます。
30	18	企業	添付E	(44)セキュリティポリシー：セキュリティポリシーは、トップマネジメントによって優先順位づけされたものに限りません。ポリシーはヒエラルキー状に構成され、より詳細なポリシーも下位に含みます。 （例えば、金庫は、侵入者の行動を最低５時間遅らせる施策が必要、というセキュリティポリシーなどは、ポリシーですがトップマネジメントの判断ではありません）。	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	19	企業	添付E	(45)セキュリティリスク：Society5.0 においては、自組織に与える影響だけに限らず、社会全体や他組織への影響も含めるべきです。また、経営に対するリスクのみ焦点を当てている意図が不明瞭です。（例えば、病院のセキュリティ欠陥が理由で患者が死亡した場合、その影響は組織の経営によりも患者自身にとって大きなリスクです。）	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
30	20	企業	添付E	(46)セキュリティルール：セキュリティコントロール(security control)の方がより一般的な表現であると考えます。	「セキュリティ管理策」は、ルールの中に記載された対策そのものを指すと考えられますので、いただいた御意見については、原案のとおりとさせていただきます。
30	21	企業		広く国内外のコミュニティからのアクセスを可能にする英語版ドキュメントの作成に感謝します。一方で、専門文書の翻訳は難度の高い作業であり、同じ表現であっても言語によっては意味合いが微かに異なる、またはコンテクストが全く異なる場合があります。（例えば、安全とセキュリティを区別できない言語もあります。）今回、英語版と日本語版の照合を行いながらグループとしてレビューをした結果、日本語版からは理解できても、英語版のみのレビューでは曖昧、不明瞭、または不十分な箇所が本意見に記述した他に多数ありました。本フレームワークの次回改定の際には、日本語版のコンテクストが英語版でも正しく伝わっていることを保障するために、英語版ドキュメントの翻訳品質を(理想的には日英それぞれの言語を母国語とする複数の)バイリンガルの分野専門家と国外の分野専門家らによって管理することを推奨します。	いただいた御意見も踏まえ、留意して翻訳作業をいたします。
31	1	団体		・比喩やアナロジーを使った説明 フレームワークへの理解を深めるために、「例えば食品であればこういうこと」といったアナロジーを用いた説明資料を用意いただけると良いと考えます。当団体としても説明会を開催いただき、理解が深まったところもありますが、直接の説明がなくとも理解が浸透するような仕掛けとしてレトリックの活用があると思います。	いただいた御意見は、今後、フレームワークの活用を推進する上で参考にさせていただきます。
31	2	団体		・「3層」の層という表現を他のものに変更する 「層」という言葉を使っているために理解のための説明が１つ必要になってしまっています。 また、解説にある図も階層をイメージさせるものであり、日本語の意味として「上下に次第にかさなる」ものと解釈されます。 一方、今回の3層構造は、各々の定義軸が異なるため、お互いの定義が排他的でなく、 画一的に分類できるものではないため、読む側、活用する側のことを考えると、 「3つの視点」、「3つの観点」、「3側面」などに変えた方が、理解されやすいと考えます。	いただいた御指摘については、分野横断SWGの議論の中でも検討をしましたが、『層』という言葉には、重なりがあってはならないものではなく、意味としては間違いではないのではないかという指摘をいただいており、また、英語で「layer」といったときには、このフレームワークの3層のアプローチを表現するものとして適切ではないかという意見もいただいております。このため、原案のとおりとさせていただきますが、いただいた御指摘を真摯に受け止め、丁寧にフレームワークの説明を行ってまいります。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
31	3	団体		・添付B/C/D/Eについて 添付B・C・Dで、JNSAの下部組織であるISOG-Jが作成・公開しているいくつかの文書が参照されています。また、「添付E 用語集」では、「SOC」「CSIRT」「セキュリティ対応組織」に対するそれぞれの用語解説がなされています。 ISOG-Jとしては、「SOC」「CSIRT」を包含する形で「セキュリティ対応組織」と位置付けていますので、用語集の「セキュリティ対応組織」にも、例えば以下のような解説を追加いただきたいと考えます。 例）セキュリティ対応組織は、SOC, CSIRTといった組織や機能を包含する。 [セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v1.0 (ISOG-J, 2017年)、 セキュリティ対応組織の教科書 v2.1 (ISOG-J, 2018年)、セキュリティ対応組織の教科書 ハンドブック v1.0 (ISOG-J, 2018年)、 セキュリティ対応組織の教科書 成熟度セルフチェックシート v2.2 (ISOG-J, 2019年)]	いただいた御意見の内容も踏まえ、記載を修正いたします。 修正箇所：添付E
32	1	個人		悪意を持った人物が起こしたリスク対応として別紙Bに具体的対応例が示されています。現行の法令下で関係者がやれそうなことは書いています。ただ現状の個人情報保護法や公正競争規約あるいは機密保護法はサイバー犯罪に対応しきれないので、現状(将来も見据えて)に即した新法(民間情報もカバーするスパイ防止法など)の制定が必要ではないでしょうか？さもないと小手先の対応だけではサイバー犯罪等に太刀打ちできないと思われます。是非とも貴省が中心となって法制化に進んで頂きたく存じます。	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。
33	1	企業		翻訳）我々は、グローバルなICTサプライチェーンに関連したリスクの特定と管理に対する重要な戦略的課題に取り組むための、経済産業省によるリスクの明確化および対策実施への取り組みを支援したい。政府と産業界の双方が、自組織の関係する製品やシステムのセキュリティ体制を強化するために必要な措置を講じていることを実証することが重要である。METIによるフレームワークの第2原案をサポートするため、我々は以下を推奨する。 (1) サイバーセキュリティの教訓とベストプラクティスの共有を促進するために、業界と政府の連携および関係者の学習環境を支援する。 (2) ICT製品サプライチェーンに関連するセキュリティリスクに対処し、それを軽減する。 a. サプライヤーに、社会に対する信頼、信頼性および価値を構築するための適合性評価プログラムを実施する可能性を提供する。 b. 最も効果的で費用対効果の高いメソドロジーを活用して、製品やシステムのセキュリティ体制を改善する。 i. サプライチェーンの関係者がコンプライアンスを示す場合、評価、認証、検証などの適合性評価プラクティスを利用してこれを達成できる。 (3) ICT製品、およびそれを支えるITインフラストラクチャのサイバーセキュリティ保証のための適切な測定基準および評価手法を開発し利用する。 a. 産業界と政府は、リスクベースのアプローチで、サイバーセキュリティに関する国際的に認められ調和された基準を確立する必要がある。	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。
33	2	企業		翻訳）コネクテッド技術に対する製品レベルのサプライチェーンリスクを製品のライフサイクルを通じて軽減し、機器、サービス、システム、および企業のセキュリティに関する信頼を回復するために、サプライチェーンリスク管理ポリシーには次の要素を含める必要がある。 •リスクの特定、サードパーティ製のソフトウェアと機器の調達、役割と責任、潜在的な脆弱性の調整された開示など、サプライチェーンの効果的なセキュリティ対策への認識を高め、維持するための実践的かつ継続的な従業員訓練を実施する。 •プロセスの完全性検証をともなうサプライチェーン全体のデューデリジェンス評価を実施して、ソフトウェアまたは機器の使用に関連するサイバーセキュリティリスクを最小限に抑えるための適切な保護策が実施されているかどうかを定期的なフォローアップ監査により判断する。 •ICT製品のライフサイクルを通して使用されるすべてのサードパーティ製ソフトウェア製品およびコンポーネントに対する、法的要件または禁止事項を含んだ明確な技術基準および要件を設定する。 •すべてのソフトウェアアプリケーションをセキュリティ上の欠陥および脆弱性から十分に保護することにより、侵害の可能性がある潜在的な脆弱性を特定する。 •ICT製品に関連する情報セキュリティに対するリスクを含む、定期的なリスク評価を検討する。 •サードパーティソフトウェアのセキュリティを検証するためにとられた手順を独立で検証する。 •新たに特定される脅威に対して継続的な保護を確実なものとするために、ソフトウェアアプリケーションを特定して定期的に更新し、必要に応じてパッチを適用するための正式なプロセスを定める。 •ソフトウェアのアップデートやセキュリティパッチへの効率的なアクセスを容易にし、従来の製品に対する継続的なサポートを確保するために、すべてのソフトウェア、機器、およびコードのソースを確立し、モニタリングするための「追跡および取引」プログラムを実装する。	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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
33	3	企業		翻訳）スマートカーを含む自動車、ソフトウェアおよびワイヤレスデジタルシステムを含むコネクテッドカーや電気自動車、自律走行車は、セキュリティの脅威に対して非常に脆弱である。これは、自動車の免許、自動車の登録、交通管理、法執行機関などの政府機関にとって重要な関心事である。私たちは自律走行車のニーズと安全運転者による高度に自動化された車をテストしたいという期待に対処するための安全基準を開発している。新しいプログラムと認証の取り組みにより、市場は消費者へのリスクや、地方自治体や連邦政府機関の懸念を軽減しながら、新しい革新的な技術を開発することができる。私たちは現在、米国運輸省をサポートして、ヨーロッパにおけるUNECE型の承認と同様に、現在の自動車サイバーセキュリティリスクを実証している。その結果、リスクを軽減し、自動車業界がコンプライアンスや規制の問題から貿易の課題や市場へのアクセスに至るまで、サプライチェーン全体の複雑さを乗り越えられるよう支援することができる。	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。
33	4	企業		翻訳）私たちは、サイバーセキュリティを強化するための、経済産業省のリーダーシップ、民間部門との調整、および協調を称賛する。サイバーセキュリティは、強力な官民パートナーシップに理想的な機会を提供する。公共部門と民間部門の双方と協力し、私たちは自主的で市場主導のメカニズムを信頼して、リスク管理ベースで国際的に整合したソリューションを開発することによって、重要インフラ防護とサイバーセキュリティリスクに対処するための複数のサイバーセキュリティ/リスク管理標準とプログラムを開発した。私たちは、サイバーサプライチェーンリスク管理の目標を支援するために経済産業省がさらに関与することを楽しみにしている。	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。
34	1	団体	添付B L1_1_a_PEO	［ヒト］自身が関わりうるセキュリティリスクに対して十分な認識を有していない ・訓練・教育を実施するだけでなく、対応マニュアル、連絡先、フロー、公衆Wi-Fiに接続して良いのかなども検討すべき（IoT機器が増えるのであれば置き忘れなどの確率も高いため、その際はどこに連携すれば良いか、他、不審メールを開いたときの連絡先など）	ご指摘いただいている「対応マニュアル、連絡先、フロー、公衆WiFiに接続してよいか」等の事項は、他の対策要件(例えば、CPS.AC-3, CPS.DS-3, CPS.RP-1)をご参照いただきたいと考えております。上記の事項は本対策要件で扱う教育・訓練のコンテンツになると考えられますので、いただいた御意見も参考に、対策例の記載を修正いたします。 修正箇所：添付C CPS.AT-1
34	2	団体	添付B L1_1_a_SYS	［システム］早期にセキュリティ上の異常を素早く検知し、対処す るような仕組みがシステムに実装されていない ・ログの確保が入っていない（内部犯の想定、重要データ・ファイルに対する操作履歴など） ・通信の遮断・ホワイトリストの適用準備、可用性を考慮するとどこまでの通信を遮断許容かの定義 ・マルウェアは削除せずに隔離する（後の解析でマルウェアの機能・通信先が把握できない） ・論理的な侵入・侵害範囲拡大は含まれない？	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件 L1_1_a_SYS
34	3	団体	添付B 第一層	想定されるセキュリティインシデント「自組織で管理している領域から保護すべきデータが漏洩する」に対応する脅威として以下を追加すべきではないか。 ・外部攻撃によるWEBページの改ざん（不正なファイルのアップロード、XSS） ・内部不正によるデータ改ざん（Write権限を保有する従業員による犯行） ・センサー情報の改ざん（物理破壊やジャミングによる攻撃） ・マルウェア感染によるデータ改ざん	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	4	団体	添付B 第一層	想定されるセキュリティインシデント「自組織のセキュリティインシデントにより自組織が適切に事業継続できない」において、［データ］の脆弱性に対する考慮がなされていない。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	5	団体	添付B 第一層	想定されるセキュリティインシデント「製品・サービスの提供チャネルでセキュリティ事象が発生し、危機の破損等の意図しない品質劣化が生じる」への対応において、自組織と外部関係会社が ISO/IEC 27001などの認証を取得しているかの確認も行なった方がいいと思います。	いただいた御意見については、同箇所に参照されているCPS.SC-3をご参照いただきたく、原案のとおりとさせていただきます。
34	6	団体	添付B 第二層	脅威 ・盗難等により不正な改造を施されたIoT機器 によるネットワーク接続 ・悪意を持った自組織内外のヒトによる不正改 ざん への対策として、ネットワークを監視するスイッチ機器による対策がない。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	7	団体	添付B L2_3_c_SYS	［システム］による対策が無線だけにとどまっている。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件 L2_3_c_SYS
34	8	団体	添付B L3_4_b_DAT	「データが分散している」という脆弱性に対して、リスクマネジメントをして判断というのは難しい。おそらくデータを分散していない会社は無く、非現実的。	例えば、データを取り扱う業務を外部に委託する際、受け渡すデータの重要性にも応じて、委託可否の判断において当該事業者で十分なセキュリティマネジメントが実施されているかどうかを考慮することは、サプライチェーン全体におけるセキュリティを確保する上で重要であると考えられます。そのため、いただいた御意見については、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	9	団体	添付B 第三層	想定されるセキュリティインシデント「不正な組織/ヒト/モノ/システムによる正規エンティティへのなりすまし」において、不正なモノが接続される脅威が記載されていない。	ご指摘の事項は「不正な組織/ヒト/モノ/システムによる正規エンティティへのなりすまし」に含まれていると認識しておりますので、いただいた御意見については、原案のとおりとさせていただきます。
34	10	団体	添付B 第三層	想定されるセキュリティインシデント「（なりすまし等をした）ソシキ/ヒト/ モノ等から不適切なデータを受信する」において、サイバー空間での認証・識別の仕組みがIDのみとなっており、認証強度が弱い。（リプライ攻撃の可能性がある）	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	11	団体	添付B 第三層	想定されるセキュリティインシデント「（なりすまし等をした）ソシキ/ヒト/ モノ等から不適切なデータを受信する」において、無線接続先（ユーザやIoT機器、サーバ等）の認証について中間者攻撃に対する対応が不足している。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	12	団体	添付C CPS.BE-1	サプライチェーンの定義（どの範囲までがサプライチェーンに含まれるのか。例えば、電力や水は含まれるのか）があれば良いかと思います。	いただいた御意見については、添付Eにおける「サプライチェーン」の定義をご参照いただきたく、原案のとおりとさせていただきます。
34	13	団体	添付C CPS.BE-1	<Advanced>と<Basic>の内容が似ているのでマージしたほうが良いかと思います。	直接の取引先との取引関係か、再委託先以降も踏まえたさらに広範な取引関係も含めたスコープかという点で実施上の負荷も異なることが想定されるため、いただいた御意見については、原案のとおりとさせていただきます。
34	14	団体	添付C CPS.BE-2 CPS.AM-6	CPS-AM-6 とCPS-BE-2 の内容が似ているのでマージしたほうが良いかと思います。	CPS.AM-6は資産というレベルで、CPS.BE-2は事業や業務というレベルで重要度等による分類をすることを記載しており、記載の重複はないと考えておりますので、いただいた御意見については、原案のとおりとさせていただきます。
34	15	団体	添付C	対策例の実施タイミングを明確にしていただきたいです（年一回なのか、内容に変更があった時点なのか）	対策例の実施タイミングは、法的規定事項、業種、業務等の様々な要因により変化することが想定されますので、本フレームワークにおいては一般的な記載に留めております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	16	団体		三層構造においては重複しているものがあり、自分で考える際どちらに分類すれば良いのか不明なものが多々ある。例えば、第１層は物理的な要素に言及しており、そこに合致するのは「ヒト」「ソシキ」などで、第３層では「データ」「プロシージャ」などが合致すると納得できる。しかし、付録Bなどを見ると、全ての階層に全ての構成要素が関係しており、理解が及ばない部分が多い。	三層構造モデルは、Societyt5.0 の実現に向けて新たな産業社会を捉えるモデルであり、それぞれの層に含まれる対象を明確に分離するモデルではありません。企業（組織）のマネジメントの信頼性の確保を求める上で、企業（組織）の管理するサイバー空間の事物やIoT機器の転写機能の信頼性の確保が求められます。この三層構造モデルは、フレームワークのコンセプトとなる考え方ですので、引き続き丁寧に説明して参ります。
34	17	団体		各階層で同じようなリスク源の記載があるが、階層によりリスク源は全く異なるのではないか。リスク分析には、既存のフレームワークを活用する方が分かりやすいのではないか。（例えば、アタックツリーなど）	三層構造モデルに基づいてバリュークリエイションプロセスを捉えたときに、いずれの層においても6つの構成要素が含まれるため、リスク源が各層でまったく異なるということはないと考えております。
34	18	団体	添付Ｂ 第３層	機能には「データを処理する機能」といった分類が必要ではないか。そして、それに対して「改ざん」などのリスクが存在する。	データを処理する機能は、「データを加工・分析する機能」、「データを送受信する機能」に含まれているものと想定しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	19	団体	添付Ｂ 第３層	「サービス拒否攻撃」とはDoS攻撃だと思うのですが、第１層、第２層ではDoSという表記がありました。用語が統一されないと混乱してしまいます。	いただいた御意見のとおり、記載を統一いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	20	団体	添付Ｂ 第３層	想定されるセキュリティインシデント「サービス拒否攻撃により、関係する他組織における自組織のデータを取り扱うシステムが停止する」において、DoS攻撃が「ソシキ」に割り当てられているが、「システム」で対応するのでは？	自組織のシステムに対して対応する場合、ご指摘いただいた通り「システム」で対応することが必要ですが、自組織の直接的なガバナンスが利かない他組織には自組織から「組織」的な対応を通じて「システム」による対応を間接的に実施してもらうことになると想定しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	21	団体	添付Ｂ 第３層	無線や電波の観点が見当たらない。 例：無線により物理的に距離のあるところから、機器の不正操作などにより被害を被るケース 例：よそから電波妨害されてサービス影響など	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件 添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	22	団体	添付B 第３層	想定されるセキュリティインシデント「関係する他組織で管理している（データ保管）領域から自組織の保護すべきデータが漏洩する」の［ヒト］［データ］において、データ持ち出しに対するリスク、対応が記載されていない。	自組織のシステムに対して対応する場合、ご指摘いただいた通り対応することが必要ですが、自組織の直接的なガバナンスが利かない他組織には、主に自組織から「組織」的な対応を通じて「ヒト」や「データ」による対応を間接的に実施してもらうことになると想定しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	23	団体		三層構造アプローチでリスク源の網羅性を体系的に担保しようとしていると感じたが、実際に本ガイドラインでセキュリティチェックを実施する際に、Society5.0がまだ進んでいない企業は自企業用に落とし込む必要がある。そのため、業界ごとのセキュリティガイドラインがとても重要になってくると感じた。	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ますが、具体的なセキュリティ対策例は、産業分野や個社ごとに異なるものであり、産業サイバーセキュリティ研究会ＷＧ１分野別サブワーキンググループ等において、引き続き、各産業分野の実態に即したセキュリティ対策例を検討いたします。
34	24	団体		わかりづらい記載や曖昧な表現が多いため、現時点でこのフレームワークを利用し各企業が評価・対策を行うのは困難であると感じました。引き続き、経済産業省や各企業と調整・検討いただき、利用価値のあるフレームワークを作成いただくようお願いします。	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ますが、具体的なセキュリティ対策例は、産業分野や個社ごとに異なるものであり、産業サイバーセキュリティ研究会ＷＧ１分野別サブワーキンググループ等において、引き続き、各産業分野の実態に即したセキュリティ対策例を検討いたします。
34	25	団体		別紙が読む人によって解釈が異なったり、似た文面の項目が多くチェックする負荷が高いと感じた。負荷を軽減するために、SEが記載する部分・マネジメント層が記載する部分を分けたり、構成図と項目を関連づける工夫があれば、良いと感じた。	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。
34	26	団体		「安全」「ハザード」「適切」といった曖昧な表現が多々があるため、業界分野毎で齟齬が発生しない様に定義を明確化する必要がある。IT系のCIAに寄った記述に見える。OT系のSAIC（安全性、可用性、完全性、機密性）といった観点（場合により切断し、現場運用）で記載してはどうか。	いただいた御意見を参考に、用語の定義を明確化いたします。 修正箇所：添付E
34	27	団体		NISTのフレームワーク等の国際規格に準じる資料と対比しており、網羅性を確保する点でとても良いと思う。	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。
34	28	団体	添付B	機能・セキュリティインシデントの抽出に網羅性が十分でない様に見えます。(CIA, STRIDE等のフレームワークを活用してはどうか)	セキュリティインシデントの抽出に当たっては、ISO/IEC 27001におけるCIA(機密性、完全性、可用性)の観点や、IEC 62443におけるHSE(健康、安全、環境)の観点等も踏まえ、網羅的な検討を意図して実施しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	29	団体	L1_1_a_COM	「モノのセキュリティ状況やネットワーク接続状況が適切に管理されていない」とあるが、資産の棚卸しができていないとそもそも第１層のチェックができないのではないか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	30	団体	添付B 第１層	想定されるセキュリティインシデント「自組織で管理している領域において保護すべきデータが改ざんされる」において、物理的な侵入や保護の観点が言及されていない。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	31	団体	添付B 第１層	想定されるセキュリティインシデント「サービス拒否攻撃ににより、自組織のデータを取り扱うシステムが停止する」のいて、可用性を損なう攻撃やインシデントがサービス拒否攻撃だけに限定されていることに違和感がある。他にもあるのではないか？（zero-dayなど）	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	32	団体	添付B 第１層	想定されるセキュリティインシデント「法制度等で規定されている水準のセキュリティ対策を実装できない」について、法制度等で規定されている水準のセキュリティ対策を実装できないことはセキュリティインシデントではなく、書くとしたら脆弱性ではないか。各産業界で定められた法規制を遵守することは対策要件ではなく罰則ありのルール。ここに出てくるのは違和感がある。	セキュリティに係る法制度の不遵守はセキュリティに関わる事象であって事業の運営を危うくする確率が高く、ビジネスモデルの変革、事業のグローバル化の進展等を踏まえると、リスクは高まっていると考えられますので、十分注意を払うべきセキュリティインシデントであると考えております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	33	団体	添付B 1_3	「危機」は「機器」の誤字である。	いただいた御意見のとおり、修正いたします。 修正箇所：添付Ｂ 1_3
34	34	団体	添付B 第２層	転写機能がおかしくなったときの方針として、 「データ転写のみ安全に停止する or 切り離す」という観点が盛り込まれていない。 　第3層：データはおかしくなくて、 　第1層：企業、サプライチェーンおよび物理に問題はない ため。転写のみ想定されていない動作をしたときに、物理機能（人とか）で代替えするような観点も必要ではないか？復旧だけではなく。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	35	団体	CPS.IP-8	0　「適切なパートナー」の基準が曖昧。政府認定などの具体性が必要ではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	36	団体	CPS.MA-1	「可能であれば」の言葉は不要ではないか。やるのかやらないのかや粒度は添付Cで規定すれば良い。	数が多い、様々な場所に設置されている等のIoT機器に想定される性質を勘案すると、リモートメンテナンスの必要性は非常に高いと考えられますので対策要件にて記載しておりますが、現実的にはそのような仕組みを導入することが困難なケースもあるため、「可能であれば」と付言しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	37	団体	添付B L2_1_a_PRO	「調達時に、適切なレベルのセキュリティ機能が実施されているかを確認するプロシージャがない」とあるが、調達時だけではなく運用時におけるチェックも必要ではないか。	運用時においては同箇所に参照されている他の対策要件を実装することで対応するものと認識しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	38	団体	添付B 第２層	想定されるセキュリティインシデント「正規のユーザになりすましてIoT機器内部に不正アクセスされ事前に想定されていない動作をする」のシステムの脆弱性に「脆弱なプロトコルを使っている」が無く、これに対する対策要件が欠落している。また、ヒトの脆弱性として、ID・パスワードの使い周りがあるのではないか。	いただいた御意見については、モノの脆弱性に記載されている「セキュリティの観点において強度が十分でない設定(パスワード、ポート等)がなされている」に包含されていると考えられるため原案のとおりとさせていただきます。
34	39	団体	添付B 第２層	想定されるセキュリティインシデント「正常動作・異常動作に関わらず、安全に支障をきたすような動作をする」において、システムとして、安全計装の観点が欠落している。ビルだと、火災報知器系ネットワークの分離やエレベーターの非常停止が想定される。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	40	団体	添付B 第２層	想定されるセキュリティインシデント「（MAC等の改ざん検知機能に対応していない機器から生成された）データがIoT機器・サイバー空間間の通信路上で改ざんされる」において、MACアドレス改ざん検知機能は対策要件の1つであるし、payloadの一部を改ざんする攻撃も存在するから、（MAC等の～）は不要である。	いただいた御意見のとおり、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	41	団体	添付B 第２層	想定されるセキュリティインシデント「計測機能に対する物理的な不正行為により、正確でないデータの送信等が発生する」は、脅威と脆弱性・対策要件が紐づいていない。人の不正行為を取り締まることが対策ではないか。第１層のセンター部分に対するインシデントや脅威として記載した方が腑に落ちる。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	42	団体	添付B 第３層	想定されるセキュリティインシデント「一部の関係者だけで共有する秘匿性の高いデータのセキュリティ要求が設定・対応されていない」は、システムの観点で分割するという項目がない。ビルで活用するなら、秘匿性高いデータをセグメント分割することなどが考えられる。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	43	団体	添付C CPS.AM-2	<High Advanced>記載の「共通ナンバリングルール」について、異業種間で通用するナンバリングルールはやりすぎな気もするが、そのような産業はあるのでしょうか。 （参考：同じ意見） <High Advanced>に記載されている「異業種間でも通用するよう業種横断的な共通ナンバリングルール等に基づいていることが望ましい。」は現実的に可能なのか。既に導入している事例はあるのか。これを導入すると取引先変更などによりサプライチェーンに変更が加わった時の影響が大きくなる。	現在確立している施策は管見の限り存在しないものと認識しておりますが、将来的に既存の業種を超えたコラボレーションが活発する場合におけるトレーサビリティの確保には有効と考えられます。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	44	団体	添付C CPS.AM-3	<High Advanced>に、検索の利便性を付け加えるべきではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.AM-3
34	45	団体	添付C CPS.GV-1	<High Advanced>と<Advanced>の対策例の違いがわかりにくい。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.GV-1
34	46	団体	添付C CPS.RA-4	「ハザード」の定義が曖昧である。	いただいた御意見を踏まえ、定義を追記いたします。 修正箇所：添付E
34	47	団体		IoTをセンサとして捉えている箇所がある一方で、IoTで制御するという記述があり、違和感がある。	本フレームワークにおいては、IoT機器を、センサーやアクチュエータ等の機能を有する可能性のある機器と捉えております(センサーやアクチュエータの定義は添付Eをご参照ください)。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	48	団体	添付B 第１層	資料構成とて重要なもの「可用性」「完全性」「機密性」の順番に記載すべきではないか。 （例） １．設備、機能の停止、制御不能 ２．制御データ、製品情報の改ざん ３．認証情報の漏えい	利用者の客観的状況によって、機密性、完全性、可用性のいずれを重視するかが変化することが想定されます。例えば、産業用制御システム(IACS)をサイトとして想定すると、ご指摘の順序となるかと認識しておりますが、本フレームワークとしては、カテゴリー内のインシデントの並びに特段の意図をこめておらず、利用者が必要に応じてどの要素が重要であるかを判断してご利用いただければと考えております。そのため、いただいた御意見については、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	49	団体	添付B 第１層	OT環境設備すべてに関する資産管理が必要では無いか。PCにフォーカスしすぎている。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.AM-1
34	50	団体	添付B 第１層	「人」の価値について、IT目線で記載されている。IT→いくらでも代替できる。OT→安全面の観点が高い、というギャップを認識した上での記載が必要。省人、省力、自動化の観点を盛り込むべき。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	51	団体	添付B 第２層	不正コマンドの送信やサービス不能(DOS)が含まれていない。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	52	団体	添付B 第２層	想定していない通信先へのデータ送信（例：Ｃ２サーバ）へのリスクについて触れていない	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	53	団体	添付B 第２層 第３層	内部犯行やヒューマンエラーなど、内部からの脅威について考慮していない。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件、第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	54	団体	添付B 第２層 第３層	CPS.IP-5のようにセキュリティと関係のない対策が含まれている。	ご指摘いただいているCPS.IP-5は、物理的セキュリティの確保に寄与する対策と認識しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	55	団体	添付B 第３層	関係する他組織との連携については、SLOないしSLAの締結が必要ではないか。	取引先とのSLA、SLOの締結は、特に、添付Bで参照しているCPS.SC-4で求めている製品・サービスにおける要求事項の対応手段のひとつと認識しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	56	団体	添付B 第３層	データ保護については、管理責任の所在（部署単位）を明確化すべきではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	57	団体	添付B 第３層	データの暗号化については、暗号の強度レベル以前に機密レベルの定義が必要ではないか	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	58	団体	添付B 第３層	OSやソフトウェアのアップデートについての制限が必要ではないか。	CPS.MA-2では、自組織の資産に対する保守を、「不正アクセスを妨げる形」で、かつ、(特に資産のオーナーによる)「承認を得て」から実施するよう記載しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	59	団体	添付C	<High Advanced>, <Advanced>, <Basic>の判断基準を明確にした方が良いのではないか。例えば、<Basic>はドキュメント化、<Advanced>が運用が確実になされていること、<High Advanced>は自動化が進んでいることや定期的な監査と改善が行われているなど。	対策例のレベル分けについては、ご指摘いただいたようなポイントに加え、対策の適用範囲、他のガイドライン等におけるレベル分けの参照等を通じて総合的に判断しているものになっております。その旨がわかるよう、いただいた御意見も参考に、修正いたします。 修正箇所：添付C
34	60	団体	添付C CPS.BE-3 CPS.BE-4	CPS.BE-3とCPS.BE-4の違いがわかりません。3の対策が高度化すると4の対策のようにポリシーとして明文化されるのではないでしょうか。	CPS.BE-4は存在しないため、誤記と思われます。(対応なし)
34	61	団体	添付C CPS.GV-2	対策要件を「法・ガイドラインなどに合わせた社内ルールを策定している」にして、「継続的かつ速やかにルールを見直す」などは<High Advanced> の対策例にするとスッキリすると思います。	いただいた御意見のとおり、修正いたします。 修正箇所：本文第III部 CPS.GV-2 添付C CPS.GV-2
34	62	団体	添付C CPS.RA-6	CPS.RA-6の<High Advanced>と<Advanced>の対策例の繋がりがよくわかりません。	＜High Advanced＞では、＜Advanced＞と異なり、セーフティに関わるリスクアセスメントとセキュリティに関わるリスクアセスメントを統合して実施する旨を記載しております。
34	63	団体	添付C CPS.RM-1	経営層は何をレビューするのかわかりません。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.RM-1

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	64	団体	添付C CPS.RM-2	「重要な取引先」について、何をもって重要とするのか。また、インタビューの頻度や質問の内容をどうすべきか。インタビューではなくリスクの認識・許容・共有が目的なのではないか。	「重要な取引先」の重要度を決める際の細かな観点は業種や企業により様々に異なることが考えられますが、一般的に、当該取引先において供給の途絶、あるいは適切でない供給(例えば、品質基準に満たない製品の出荷)が発生した際の自組織の事業への影響の大きさ、加えて、そのような事象の発生しやすさが挙げられるかと認識しております。また、インタビューの頻度や内容等につきましてはいただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.RM-2
34	65	団体	添付C CPS.SC-1	「サプライチェーンに係るセキュリティ対策基準」が何かわからない。	取引先のセキュリティマネジメント、あるいは提供される製品・サービスに対して適用するセキュリティ対策基準のことを指しております。
34	66	団体	添付C CPS.SC-2	<High Advanced>に記載の２つの対策例の内容の方向性が一貫していない。	1つ目の対策例は、自組織の事業、リソースの優先順位付けを実施するものであり、2つ目の対策例は、取引先におけるセキュリティインシデントが1つ目の対策例で議論している事業やリソースにどれだけ影響するか、どの程度の起こりやすさかを見積もるものになります。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	67	団体	添付C CPS.SC-2	<Basic>に記載の対策例の実施に際して、具体的な基準が必要と考えます。	具体的な基準や尺度については、各組織の状況や調達する製品・サービスの性質等に依存するものと考えられますが、いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C CPS.SC-2
34	68	団体	添付C CPS.SC-2	以下の対策例は、文章が長すぎてよくわからない。 「組織は、取引先(サービスプロバイダー)の選定に当たり、JIS Q 20000に基づくITSMS認証等を取得するか、あるいは自己適合確認により認証取得相当の対策の実装を確認しており、提供するITサービスのマネジメントを効率的、効果的に運営管理するサービスプロバイダーを選定することが望ましい。」	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.SC-2
34	69	団体	添付C CPS.AC-1	自組織のシステムアカウント管理の自動化なんて存在するのでしょうか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.SC-2
34	70	団体	添付C CPS.DS-14	対策例「物理的な攻撃に対して耐性を有しているか」は <Basic> に移動したほうが良いのではないか。	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.DS-14
34	71	団体	添付C CPS.AE-1	OT領域ではメカニズム以外の方法でのモニタリング、あるいはモニタリングを代替する方策の適用が必要ではないか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.AE-1
34	72	団体	添付C CPS.AE-2	<Advanced> の対策例として、組織内だけでなく組織間のデータ連係部分を含めることを注記した方がよい。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.AE-2
34	73	団体	添付C CPS.AE-3	ここでの「センサー機器」は、IoTのそれではなくセキュリティ対策でのIDS, IPS, SIEMなどのそれ（前項）であることを（念のため）注記した方がよいのではないか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.AE-3
34	74	団体	添付C CPS.AE-3	<Advanced>の対策例として、IoTなどのエッジデバイスのログへの言及すべきではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.AE-3
34	75	団体	添付C CPS.AE-4	誤字：「仮設」ではなく「仮説」	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.AE-4
34	76	団体	添付C CPS.CM-1	VoIPのみ特別扱いなのはなぜでしょうか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.CM-1
34	77	団体	添付C CPS.CM-1	複合機へのファックス回線経由での攻撃のようにネットワークがコンピュータに限定されないことについて注記した方が良いのではないか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.CM-1
34	78	団体	添付C CPS.CM-2	物理的アクセスの制御を設定することは自明だから記載されていないのでしょうか。	CPS.AC-2において、物理的なアクセス制御の実施を要求しておりますので、そちらをご参照ください。
34	79	団体	添付C CPS.CM-3	「外部情報源からのファイルのリアルタイムスキャン」は意味が不明確に思います。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.CM-3
34	80	団体	添付C CPS.RP-1	<High Advanced>記載の異常発生時の緊急停止対応などは、<Basic>で実施すべき内容ではないか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.RP-1
34	81	団体	添付C CPS.RP-1	<Basic>に記載の対策例について、対処が必要かどうかの判断は、<Advance>に記載のある判断基準が必要になるのではないか。<Basic> だけの対応ができず、破綻している。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.RP-1

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	82	団体	添付C CPS.CO-2	「肯定的な側面の認識」のが意味がよくわからない。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.CO-2
34	83	団体	添付B L1_1_b_DAT	脆弱性として、中間者攻撃を検知するセキュリティ機器を導入していない点の考慮と、その対策要件として、通信ネットワークに中間者攻撃を検知できるセキュリティ機器の実装が必要ではないか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B L1_1_b_DAT
34	84	団体	添付B L1_1_c_SYS	通信途絶時のフィジカル機器の対応を定めておく必要があるのではないか。	L1_3_a「自組織のセキュリティインシデントにより自組織が適切に事業継続できない」における記載をご参照ください。
34	85	団体	CPS.GV-4	サイバー空間でのリスクだけではなく、フィジカル空間でのリスクも考慮する必要があるのではないか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本分第III部 3.3 ガバナンス CPS.GV-4
34	86	団体	添付B 第１層	想定されるセキュリティインシデント「法制度等で規定されている水準のセキュリティ対策を実装できない」について、METI、IPAが様々なガイドラインを出しているのだから、関連ガイドラインの参照くらい入れてはどうか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.GV-2
34	87	団体	添付B L1_3_a_SYS	IIoT機器は自組織のネットワークをバイパスできるから、監視不十分となるのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件 L1_3_a_SYS
34	88	団体	添付B L1_3_c_PEO	セキュリティ事象による被害を受けたモノ（製品）・サービスが生じることも脆弱性ではないか。 また、対策要件として、セキュリティインシデント発生時に被害を受けた設備にて精算される等して、何らかの品質上の欠落が生じていることが予想されるモノ（製品）に対して、回収などの適切な対応をおこなうことが必要ではないか。	ご指摘のポイントについては、L1_3_c_PEOにて記載していると認識しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	89	団体	添付B L2_3_a_ORG	改ざん検知の機能の実施の確認を導入者側に実施させるのは無理。品質などと同様に外部専門組織にて認証などのお墨付きをくれたものから導入判断するようにしなければ成立しない。	ご指摘のポイントは、CPS.SC-4を実装する際の一つの手段として考えられます。ご指摘いただいている通り、実際には、調達側のケイパビリティ等も勘案して手段を選択いただく形になると認識しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	90	団体	添付B 第３層	想定されるセキュリティインシデントについて「データの送受信不可」、リスク源として「機器の乗っ取りによるデータの送受信停止」「妨害電波発信」が必要ではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	91	団体	添付C CPS.AM-2	<Advanced><Basic>に記載されている「組織は、製造およびサービス提供の全過程において、監視および測定の要求事項に関連してアウトプットの状態を識別する。」の意味がわからない。もう少し詳しい説明がほしい。	本対策例は、製品・サービスのライフサイクルを通じて、契約等を通じた購買側からの要求あるいは業法等により規定された要求事項が遵守されているかを識別することを求めているものになります。なお、記載の意味が不明瞭になっている箇所につきましては、いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.AM-2
34	92	団体	添付C CPS.BE-1	<Basic>に記載されている対策例について、取引関係を認識しておくことは重要であるが、共有を義務付けると、取引先などの更新があった時に混乱する、もしくは更新漏れが頻発するのではないか。	本対策例の記載は、取引関係の報告を義務化するということは意図しておらず、あくまである時点における概要を把握するものと認識しております。可能であれば、個々の取引まで把握して継続的に変更にも対応しておくことが望ましいですが、ご指摘の通り、管理も煩雑化しますので、潜在的なリスクの大きさに即した対応(例えば、供給の停止等が事業に与える影響が大きいサプライヤーのみ、より深い階層まで概要を把握しておく等)を実施すべきと考えます。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	93	団体	添付C CPS.GV-4	<Advanced>に記載されている「組織は、すべての資本計画および投資管理プロセスに、セキュリティに関わるリスクマネジメントの実施に必要なリソースが含まれるようにして、この要件に対する例外を文書化する。」について、すべてに対して行うことは現実的ではないのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.GV-4
34	94	団体	添付C CPS.RA-1	<High Advanced><Advanced>に記載されている対策例について、制御システムについては脆弱性テストを実施することが難しい企業がほとんどないのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.RA-1
34	95	団体	CPS.RA-2	制御システムについては、SOC/CSIRTの対応範囲外となっている企業がほとんどである。情報システムについてSOC/CSIRTがあるため、この項目を満たしていると判断する企業が多いのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.RA-2
34	96	団体	CPS.RA-4	対策要件の記載では、対象のシステムが情報システムだけなのか、IoTを含むシステムだけなのか、または制御システムまで含むのかが明確でない。	対策要件においては各種システムに共通した原則を記載しているため対象システムを記載していませんが、実際には、対象システムの性質により実施上の困難の度合いが異なると考えられます。いただいた御意見も参考に、対策例において可能な限り対象システムが明確になるように修正いたします。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	97	団体	添付C CPS.RA-4	リスクアセスメントの範囲はどこまでか（制御システム～情報システムのすべてを含むのか）。すべてに対して、「制御システムのセキュリティリスク分析ガイド」を適用するのであれば、年に1回でもかなりの企業の負担になると考えられる。レベル感を示して欲しい。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.RA-4
34	98	団体	CPS.RA-5	CPS.RA-4との項目の違いがよくわからない。	CPS.RA-4は単にリスクアセスメントを実施することを求めており、CPS.RA-5はアセスメントの中で実際にリスクを評価する際に、脅威、脆弱性、可能性、影響を考慮することを求めています。
34	99	団体	添付C CPS.RM-1	<Basic>の対策例に、「組織が、サイバーセキュリティリスクの責任範囲や責任者を明確にする」ことが含まれるのではないか。	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.RM-1
34	100	団体	添付C CPS.SC-6	<Basic>の対策例に、「組織は、取引先の監査あるいはテストの不適合が発見された場合、発生した不具合による自組織へのリスクを認識できている」ことが含まれるのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.SC-6
34	101	団体	添付C CPS.SC-9	<Basic>の対策例に、「組織は、組織は自組織で起こり得るインシデントを認識できている」ことが含まれるのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.SC-9
34	102	団体	添付C CPS.SC-10	<Basic>の対策例に、「組織は、取引先などの関係する他組織との契約の終了を常に認識できている」ことが含まれるのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.SC-10
34	103	団体	添付C CPS.AC-5	<Basic>に「人的リソース等の関係で、職務の分離が困難な場合、」と記載されているが、場合分けせずに最低限のレベルとして記述してはどうか。	あくまで実施すべきは職務の適切な分離であり、現在＜Basic＞に記載されている対策はそれに直接的な実装ではないため、「人的リソース等の関係で、職務の分離が困難な場合、」という付記をしております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	104	団体	添付C CPS.AC-7	<Basic>の対策例に「データフロー制御ポリシーを定め」とあるが、データフロー制御ポリシーのような決まりごとは、概要レベルで本文に記載すべきではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部
34	105	団体	添付C CPS.RA-1 CPS.DS-9 CPS.DS-10	CPS.RA-1の対策例に記載された「脆弱性診断ツール」や「侵入テスト」は、OT現場への導入が困難である。 CPS.DS-9の<High Advanced>の対策例に記載された「自動化されたツール」や、CPS.DS-10の<Advanced>の対策例に記載された「完全性検証ツール」についても同様に、OT現場への導入が困難である。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C
34	106	団体	添付C CPS.DS-12	機器のシリアル番号やハッシュ値等を利用して、定期的にIoT機器および搭載されているソフトウェアが正規品であることを確認するために、資産管理ツールの導入を提案するのはどうか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：CPS.DS-12
34	107	団体	添付C CPS.IP-9	<High Advanced＞に記載の対策例は、<Advanced>レベルではないか。 また、<Basic>に記載の「要員」の審査は、審査の内容によっては <Advanced><High Advanced>レベルではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.IP-9
34	108	団体	添付C CPS.IP-10	<Basic>に記載の参考について、IoT機器よりも制御機器の方がさらにパッチ適用が困難である。	いただいた御意見を踏まえ、修正いたします。 修正箇所：CPS.IP-10
34	109	団体	添付C CPS.MA-1	<High Advanced>に記載の対策例「組織は、自組織のIoT機器、サーバ等のアップデート等を実施する要員が持ち込むメンテナンスに必要な機器やツールを検査し、不適切な変更または不正な変更がない」は、検査の内容によっては<Advanced>でよいかと考えます。	いただいた御意見については、本項目では検査の内容は問わず、一般的な記載を試みているため、原案のとおりとさせていただきます。
34	110	団体	添付C CPS.MA-2	<High Advanced>に記載の対策例は <Advanced> でいいかと考えます。 <Advanced>に記載の対策例は <Basic>でいいかと考えます。	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.MA-1
34	111	団体	添付C CPS.PT-3	<High Advanced>の対策例に「本質安全設計」と記載されていますが、そもそもコネインやSmart Factoryの取り組みと本質安全設計とは全く別の議論かと思います。本質安全設計は、プラントの新設または全面に更新時において考慮すべきであって、IIoTやデータ利活用に伴い本質安全設計を見直すものではないと考えます。 セキュリティインシデントに伴う不安全状態の発生頻度、発生時の影響度を下げる議論は大いにするべきだと思いますが、本質安全設計は論点が異なると考えます。	『つながる世界のセーフティ＆セキュリティ設計入門』(IPA ソフトウェア高信頼化センター(当時), 2016年) 4.2.3 セーフティ設計の手法 にも記載されているように、セーフティに関わる対策として、本質的安全設計によるリスクの除去や軽減は有効と考えられます。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	112	団体	添付B	リスク分析の結果、リスクを許容するプロセスの記載がない。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第II部
34	113	団体	添付B 第１層	データ漏えいのリスク源として盗聴（中間者攻撃）に関する記載がない。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第II部
34	114	団体	添付B 第２層	保守員への帯同義務を課すべきではないか。	ご指摘の点は、CPS.AC-2, CPS.CM-2において＜Basic＞で記載されております。優先度の高い対策かと思われますが、実施に際しては、事業者のリスク分析等に基づいた判断に依拠するものとしたく存じます。そのため、いただいた御意見については、原案のとおりとさせていただきます。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	115	団体	添付B L2_3_b_ORG	機器の状態を把握できていない脆弱性に対応する対策要件として、「システムを構成する一覧を文書化、保存」とあるが、定期的な棚卸、最新化をする必要があるのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：本文 第III部 3.1 資産管理 CPS.AM-1 添付C CPS.AM-1
34	116	団体	添付B 第３層	脅威として「DoS」のみが記載されているが、他にも攻撃手法・脅威があるのではないか。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	117	団体	添付B 第３層	機密情報へのセキュリティ要求→攻撃に対する対策は記載されているが、ヒューマンエラー（設定ミス等）に関する記載がない。	設定ミス等のヒューマンエラーは、本フレームワークで想定しているセキュリティインシデントに対する脆弱性となると考えられます。いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付B 第3層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	118	団体	添付C	具体的な施策例であったり「これをやれば大丈夫！」といった お墨付き（ユーザーの期待値）を得られるようなものではないが、セキュリティ対策の検討のキッカケを与えてくれるツールとしては有効。	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。
34	119	団体		リスク源、対応要件の網羅性が高く、幅広い業界で有効なものが揃っているように見受けられた。セキュリティ対策検討のためのチェックリストとして活用するにはとても有効。何かの拠りどころとなるようなものが用意されているという事は企業にとってはとてもありがたい事。他方、網羅性が高すぎるが故に、どの部分を参考に見ていけば良いのかが分かりづらいという印象は抱いた。	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す。具体的なセキュリティ対策例は、産業分野や個社ごとに異なるものであり、産業サイバーセキュリティ研究会ＷＧ１分野別サブワーキンググループ等において、いただいた御意見も踏まえ、引き続き最適なセキュリティ対策例を検討いたします。
34	120	団体		効果が高い対応策（添付Bで対策要件が重複しているもの）が分かるようになっていれば尚良いフレームワークになるのでは。	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す。具体的なセキュリティ対策例は、産業分野や個社ごとに異なるものであり、産業サイバーセキュリティ研究会ＷＧ１分野別サブワーキンググループ等において、いただいた御意見も踏まえ、引き続き最適なセキュリティ対策例を検討いたします。
34	121	団体	添付C	対策例の<Basic>, <Advanced>, <High Advanced> の振り分け基準が曖昧で、自組織で運用する場合、どこまでやるべきなのか判断しづらいと思われる。また、対策例の<Basic>, <Advanced>, <High Advanced>の順番が、難易度順になっているのではないか。本来は優先度順にしていくべきではないか。	対策例のレベル分けについては、対策のオペレーションの高度さ、対策の適用範囲、優先度、他のガイドライン等におけるレベル分けの参照等を通じて総合的に判断しているものになっております。対策の振分けについては、いただいた御意見も参考に、今後継続的に検討したいと考えております。 修正箇所：添付C
34	122	団体		甲乙の力関係から、このフレームワークを運用するのは、難しいのではないか。	いただいた御意見を踏まえ、企業・組織の関係性に関係なくフレームワークを社会実装するための取組を検討して参ります。
34	123	団体	添付B 第１層	想定脅威として侵入は想定されているが物理破壊が存在しない。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付B 第1層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	124	団体	添付B 第１層	IoTは始まりだした分野であるため、そもそも対応するデバイスを供給する会社の健全性を把握するプロセスが必要ではないか。	実際には、特に新規の取引先の場合は当該企業の財務状況や反社会的組織との関係等、一般的に調達プロセスにおいて確認すべき点を確認することが想定されますが、そのようなアクションはセキュリティに係る特定のインシデントや脆弱性に紐づくわけではないと認識しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	125	団体	添付B 第２層	製品そのものに対する規格の概念を定めたほうがいいのではないか？　粗悪な製品を阻害するために、基準を満たした製品を導入すべきであれば、そのような記述がなければ、配下のガイドでサポートされない。	特定のセキュリティ機能を実装している製品に対する認証については、CPS.SC-4＜Advanced＞において例を挙げておりますので、そちらをご参照ください。
34	126	団体	添付C	読む順番と実施順序から勘案しても、Basic→Advanced→High Advancedの順序で記載した方がわかりやすい。Advancedを実施する人はBasicを実施してからその対策に臨むため。	いただいた御意見については、原案のとおりとさせていただきます。
34	127	団体	添付C CPS.AM-1	文書化が主目的ではなく、管理こそが主目的ではないか。また、管理システムの導入についてもう少し着目しても良いのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：本文 第III部 3.1 資産管理 CPS.AM-1 添付C CPS.AM-1
34	128	団体	CPS.AM-2	製造物のトレーサビリティ確保が主目的と思われるが、対策要件からはそれが読み取りにくい。また、「識別」「特定」などの言葉の使い分け基準が不明確。	いただいた御意見を踏まえ、記載の統一、適切な使い分けを実施いたします。 修正箇所：CPS.AM-2
34	129	団体	添付C CPS.AM-5	対策要件と <Advanced> 以降の対策例が合致していない。利用する外部情報システムの管理が必要であれば、その旨対策要件に記載すべき。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS,AM-5

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	130	団体	添付C CPS.AM-6	対策例 <High Advanced> に記載されている内容は、本来<Basic>で行うべきものではないか。<Basic>の対策例は情報系に偏っている。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.AM-6
34	131	団体	添付C CPS.AM-7	損害賠償や免責などの要素に偏っており、本来検討すべき、セキュリティの要求事項の取決めなどに関する記述が不足している。	セキュリティに関する要求事項の策定、適用については、CPS.SC-1, CPS.SC-3, CPS.SC-4に記載しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	132	団体	添付C CPS.BE-2	<High Advanced>と<Basic>の対策例は逆ではないか。自組織の優先順位付けは<Basic>でやるべきこと。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS,BE-2
34	133	団体	CPS.BE-3	CPS.BE-1, CPS.BE-2 と区別する理由が不明瞭。	CPS.BE-3自体は、直接的にはセキュリティ対策を想起しないものですが、セキュリティに関わる組織間の役割分担を明確化することを記載しているCPS.BE-1, CPS.BE-2へのインプットとなることを意図して、別の対策要件として記載しております。
34	134	団体	添付C	添付Cの対策において３段階あり、様々なセキュリティレベルの事業者が活用できるように工夫されていると感じるが、<Basic>は事業者が現実的に実行できる最低限の対策に妥協している気がしており、本当に効果的な対策であるか疑問に感じた。	いただいた御意見を参考に、今後内容を継続的に改善していきたく存じます。
34	135	団体		脅威と対策の対応が付いていない箇所や、重複している脅威や対策の記述が数多く存在する。また、全般的に記述内容がわかりにくく、解釈が難しい部分もあり、事業者が直接する利用するには利用イメージがわきにくい。	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す。具体的なセキュリティ対策例は、産業分野や個社ごとに異なるものであり、産業サイバーセキュリティ研究会ＷＧ１分野別サブワーキンググループ等において、いただいた御意見も踏まえ、引き続き最適なセキュリティ対策例を検討いたします。
34	136	団体	CPS.AM-2	「サプライチェーン上の重要性」とあるが、幅が広いのではないか。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.AM-2
34	137	団体	添付B L2_1_a_COM	［モノ］の脆弱性にある「機器」は「IoT機器」ではないか。	いただいた御意見のとおり、修正いたします。 修正箇所：添付B L2_1_a_COM
34	138	団体	添付B L2_1_b_SYS	［システム］の脆弱性として認証が足りていないのでは。	「アクセス制御」に「認証」の意味も含めて使用しております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	139	団体	添付B L2_1_b_COM	「強度が十分でない設定がなされている」ことに対して、物理的な閉塞を対策要件とすることに違和感を感じる。	いただいた御意見も参考に、対策要件の記載を修正いたします。 修正箇所：本文第III部 3.10 情報を保護するためのプロセス及び手順 CPS.IP-2
34	140	団体	CPS.AE-1	「ネットワーク運用のベースライン」と「ヒト、モノ、システム間の予測されるデータの流れを特定し、管理」は別の対策ではないのか。一緒に並べるとわかりにくい。	いただいた御意見については、関連する国際標準等とのハーモナイズのため、原案のとおりとさせていただきます。
34	141	団体	添付B L2_1_b_ORG	［ソシキ］ネットワークの適正利用を定期的に確認していない、という脆弱性に対してネットワーク監視・アクセス監視を実施するという常時監視の対策要件が記載されており、脆弱性と対策が一致していない。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付B L2_1_b_ORG
34	142	団体	添付B 第２層	想定されるセキュリティインシデント「遠隔からIoT機器を管理するシステムに不正アクセスされ、IoT機器に不正な入力をされる。」は、「遠隔からIoT機器を管理するシステムに不正アクセスされ、IoT機器に不正な入力をされ、事前に想定されていない動作をする。」ではないか。	いただいた御意見のとおり、修正いたします。 修正箇所：添付B 第2層における機能／想定されるセキュリティインシデント／リスク源／対策要件
34	143	団体	添付B 第２層	想定されるセキュリティインシデント「正常動作・異常動作に関わらず、安全に支障をきたすような動作をする」に対応する脅威として、「制御信号を改ざんするマルウェアに感染する」もあるのではないか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付B L2_2_a
34	144	団体	添付B L2_3_a_ORG	「改ざん検知機能」ではなく「改ざん検知機能及び改ざん防止機能」とすべきである。	いただいた御意見のとおり、修正いたします。 修正箇所：添付B L2_3_a_ORG
34	145	団体	添付B 第２層	想定されるセキュリティインシデント「（監視が行き届かない場所に設置された機器の運用中、あるいは廃棄後の盗聴等の後）改ざんされたIoT機器がネットワーク接続され、故障や正確でないデータの送信等が発生する」に対応する脅威として、「センサーの読み取り値が改ざんされる」もあるのではないか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付B L2_3_b
34	146	団体	添付B 第３層	想定されるセキュリティインシデントの「・・・データを受信する」と、リスク源の「・・・データの送受信」とで記載が一致していない。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.1 ビジネス環境 CPS,BE-2
34	147	団体	添付C 第３層	<High Advanced>の対策例に記載の「診断すべきシステムの脆弱性をすぐに更新できる脆弱性診断ツールを使用する」は、正しくは「診断すべきシステムの脆弱性データベースをすぐに更新できる脆弱性診断ツールを使用する」ではないか。	いただいた御意見のとおり、修正いたします。 修正箇所：添付C CPS.CM-7
34	148	団体	CPS.RM-1	関係者とは誰を指すのか。	いただいた御意見を踏まえ、「関係者」の指す内容が明確になるよう修正いたします。 修正箇所：本文第III部 3.1 リスク管理戦略 CPS,RM-1
34	149	団体	添付C CPS.RM-2	「CPS.BE-1にて実施している・・・」は<High Advanced>及び＜Advanced>双方に記載があるようだ。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文第III部 3.1 リスク管理戦略 CPS,RM-2

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	150	団体	添付C	リスクアセスメントやリスクマネジメントに関する記載が複数ページに渡り、過度に詳細に記載されている。	リスクアセスメントやリスクマネジメントはセキュリティ対策を実施する上で、非常に重要かつ基本的な対応と認識しておりますので、いただいた御意見については、原案のとおりとさせていただきます。
34	151	団体	添付C CPS.AC-9 CPS.DS	パスワードによる認証、暗号化に関してはIT寄りの対策が過度に詳細に記載されている。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C AC-9, CPS.DS
34	152	団体	添付C CPS.CM-2	入退管理について、<Advanced> に対策例が書きすぎており、<High Advanced>, <Basic> と粒度が異なる。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C CPS.CM-2
34	153	団体	添付C CPS.RA-2	外部情報源について、サイバーインテリジェンスに関する記載が不足している。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C CPS.RA-2
34	154	団体	添付C CPS.AC-3	OTでは、取り扱う情報がすべて機密性が高いと考えられる。	実際に情報を管理している事業者の判断により、機密性を含む、情報の重要度を規定することを想定しております。
34	155	団体	添付C CPS.AC-4	OTでは、一定期間再ログインできなくなると重要インフラサービスに影響が生じる。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C AC-4
34	156	団体	添付C CPS.AC-7	物理的なネットワーク分離について記載が無い。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.AC-7
34	157	団体	添付C CPS.DS-5	DoS攻撃等に対するリソース確保は記載があるが、検知について記載がない。	いただいた御意見を踏まえ、サービス拒否攻撃の検知に係る内容を追記いたします。 修正箇所：添付C CPS.CM-1
34	158	団体	添付C CPS.CM-3	IoT機器やサーバ機器が取り扱う情報が許容範囲内であることのチェックに関しては<Basic>に記載すべき。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付C CPS.CM-3
34	159	団体		情報漏えいやデータ改ざんに関する脅威や対策に重点が置かれている一方で、機器の不正動作などに関する記載粒度が荒すぎて、実際の脅威分析等に活用しにくい。	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す。具体的なセキュリティ対策例は、産業分野や個社ごとに異なるものであり、産業サイバーセキュリティ研究会ＷＧ１分野別サブワーキンググループ等において、いただいた御意見も踏まえ、引き続き最適なセキュリティ対策例を検討いたします。
34	160	団体	添付C	対策例で、下位レベルの記載が「○○すること」、上位レベルが「○○することの具体策」の記載は、分かりにくい。	該当する記載はありませんでした。
34	161	団体		本文の記載が先進的であるのと比較して、添付B以降の具体論が実質的にISMSベースになっていて、IoTや先進技術に対応できていない。	いただいた御意見を参考に、今後内容を継続的に改善していきたく存じます。
34	162	団体	添付B	語彙がIT技術者向けなので、平易な用語を使った方がよいのではないか。 例えば、CPS.IM-2の「コンティンジェンシープラン」は別単語に置き換えるべきではないか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付B
34	163	団体	添付C	対策例について、IT/OT/IoTが混在しているのでカテゴライズして欲しい。	いただいた御意見を踏まえ、記載を修正いたします。 修正箇所：添付C
34	164	団体	添付C	適用対象範囲によって難易度が異なるケースがあるので、対象範囲の列があってもいいのではないか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C
34	165	団体		編集して利用したいので、Excel形式でも公開してほしい。	いただいた御意見を踏まえ、より活用しやすい方法での公表方法について検討いたします。
34	166	団体	CPS.AM-1 CPS.RA-1	セキュリティ管理、脆弱性管理が必要な機器として、管理情報にIIoT機器を含むべきである。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-1 本文第III部 3.4 リスクアセスメント CPS.RA-1
34	167	団体	CPS.DS-8 CPS.SC-11	IT用語で「エンティティ」「プロシージャ」と書いているが、OT向けには単語を書き換えるべき。	いただいた御意見も参考に、用語の修正、定義の修正等を実施いたします。 修正箇所：添付E
34	168	団体	CPS.RA-1	脆弱性を特定し、許容する資産のリストを作成するものなのか記載から判別できない。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.4 リスクアセスメント CPS.RA-1

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	169	団体	添付C CPS.AM-1	<Basic> で実施すべき資産棚下ろしの範囲・粒度はどこまでか。また、<Basic>における重要度はどのように決めるのか。例えば、センサーやコントローラは、ベンダーしか分からない現実がある。また、センサーやコントローラは数が多いため、<Basic>レベルに位置づけるのは体力的に無理がある。重要度を決めるにも体力が必要。	資産棚卸しの範囲は、原則、自組織のシステムを構成するすべての資産(ハードウェア、ソフトウェア、情報)と考えております。実施の粒度については、「制御システムのセキュリティリスク分析ガイド 第2版」P.55 表3-7を参考に実施いただくことを想定しております。 重要度の決定は、CPS.AM-6＜Basic＞に記載しているように、機密性、完全性、可用性の観点(安全性についてはデータの完全性に関する要件と関連付けて整理を行うことが望ましい)や、発生しうる事業被害の大きさから検討するアプローチがあると認識しております。また、＜Basic＞の記載内容については、いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-1
34	170	団体	添付C	<Advance><Basic>共通で良いのか。 <Basic>「なし」と書かれている違いがわからない。記載方法の統一が必要ではないか。	いただいた御意見も参考に、表の読み方に関するガイダンスを追記するなど、記載を修正いたします。 修正箇所：添付C
34	171	団体	添付C CPS.AM-2	内容が漠然としすぎていて、何をすべきか分からない。 「全過程」を<Basic>の対策例でに求めるのは無理ではないか。適用範囲を狭める必要がある。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-2
34	172	団体	添付C CPS.AM-3	<Advance><Basic>共通の対策例は、対策要件を言い換えているだけに見え、対策例になっていない。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-3
34	173	団体	添付C CPS.AM-4	IoT機器、OT機器はファームウェアのロールバックが出来ないので、ロールバックの要件を満たすためには、コントローラやIoT機器そのものを予備で持つ必要が出てくるのではないか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-4
34	174	団体	添付C CPS.AM-4	<Basic>でシステム構成を洗い出す組織の単位とは。全社のシステム構成を洗い出すことは難しいと考える。	原則として、組織内におけるすべてのシステムを対象にすることが望ましいと考えますが、労力、予算等の問題により困難な場合、CPS.AM-5で定める重要度を参照して、一定以上の重要度のシステムの構成を優先的に明確化する等の対応が可能かと認識しております。いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.1 資産管理 CPS.AM-4
34	175	団体	添付C CPS.BE-1	サプライチェーンを考えるのは、発注元が考えることで、中小企業は発注元にしたがって出すだけで良いのではないか。	サプライチェーンの川上に位置する企業(中小企業を含む)は、ある業界内、あるいは業界横断的に複数の川下企業と取引していることが想定されるため、当該企業のインシデントの影響が広範囲に伝播する可能性があります。そのため、サプライチェーンを考慮した対策は発注元が考慮すればよいというではなく、川上の企業も含めてサプライチェーンリスク管理の観点から適切にマネジメントを実施ことが望ましいと考えます。
34	176	団体	添付C CPS.BE-2	<High Advanced>に記載された「組織は、自組織の事業活動の適切でない運用によりHSE(Health, Safety and Environment)への悪影響が発生するかも考慮してリソースの分類、優先順位付けを行う。」は、<Basic>相当ではないか。	いただいた御意見を踏まえ、記載を修正いたします。 修正箇所：本文第III部 3.2 ビジネス環境 CPS.BE-2
34	177	団体	添付C CPS.BE-3	<High Advanced>に記載された「組織は、自らの事業を継続する上で、重要な依存関係にあるサプライヤーを識別する。」は、事業計画上行うものであって、<Basic>なのではないか。 他の項目と重複している印象で、冒頭から順番に適用していった場合、二度手間になる可能性がある。	いただいた御意見を踏まえ、記載を修正いたします。 修正箇所：本文第III部 3.2 ビジネス環境 CPS.BE-3
34	178	団体	添付C CPS.GV-1	<Basic>, <Advanced> では、制御システムは対応しなくて良いという理解でOKか。	情報システムを主に想定して策定された、ある程度内容が詳細なセキュリティポリシーは、産業用制御システムに適用する際の齟齬が大きくなる部分があると考えられますが、より抽象的な記載のセキュリティ基本方針については可能な限り対応することが必要と考えます。
34	179	団体	添付C CPS.GV-2	<High Advanced>, <Advanced>, <Basic> まで同じ対策例でよいのか。	法令等の遵守は、ビジネスを行う上での前提となる基本的な要求と考えられますので、<High Advanced>, <Advanced>, <Basic>を共通して記載をしております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	180	団体	添付C CPS.GV-4	マネジメント戦略は、長期的な視点も含める旨を記載するべき。短期視点は<Advanced>ないし<Basic>扱い。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.3 ガバナンス CPS.GV-4
34	181	団体	添付C CPS.RA-2	OTの分野についても、セキュリティの最新情報を入手することを、<High Advanced>では要求したい。	いただいた御意見を踏まえ、記載を修正いたします。 修正箇所：本文第III部 3.4 リスクアセスメント CPS.RA-2

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
34	182	団体	添付C CPS.RA-4	<High Advanced>の対策例に記載されている「組織は、ハザードによって被害に至る状況を分析し、発生しやすさや被害の深刻度を明らかにすることで、生じるリスクを見積もる。その際、セキュリティの問題に起因するハザードの有無を確認することが望ましい。」は、<Basic>で行うべき。そうしないと、適用対象がわからなくなるはず。	製品におけるセーフティ設計やセキュリティ設計の必要は広く認められつつ、ルールの策定や実践は進んでいるとはいえない状況と認識しております(『セーフティ設計・セキュリティ設計に関する実態調査結果』(IPA, 2015年))。また、セーフティを踏まえたセキュリティ対策の実施につきましては、CPS.RA-6＜High-Advanced＞に記載しており、そちらのレベルとも平仄が取れております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
34	183	団体	添付C CPS.RA-5	リスクアセスメントを自動化し、サプライチェーンのステークスホルダーに脅威や脆弱性を共有することを<High Advanced>の対策例に入れても良いのではないか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.4 リスクアセスメント CPS.RA-5
34	184	団体	添付C CPS.RA-6	<Basic>の対策例に記載の「次の事項」とは何を指しているのか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.4 リスクアセスメント CPS.RA-6
34	185	団体	添付C CPS.SC-1	<High Advanced>の対策例に記載されている「組織は、取引先(外部情報システムサービスのプロバイダ)に対して、サービスの使用に必要な機能、ポート、プロトコル、および他のサービスを明確にする。」は、<Basic>ではないか。外部サービスを使うなら尚更。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.6 サプライチェーンリスク管理 CPS.SC-1
34	186	団体	添付C CPS.SC-3	<High Advanced>では、サプライチェーン上の全ての関係者で満たしていることを要求したほうがいいのではないか（下請け、孫請け・・・以下含む）。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.6 サプライチェーンリスク管理 CPS.SC-3
34	187	団体	添付C CPS.SC-3	「法令の相違によって生じる潜在的な法的規制リスク」とは何か。	一例として、クラウドサービスの利用において、データセンターの所在地により適用される法制度が異なるケースが考えられますが、諸般の事情により異なる法域の制度が適用される際に発生しうる認識不足等による未遵守リスクを指します。いただいた御意見も参考に、よりわかりやすい記載となるよう記載を修正いたします。 修正箇所：添付C CPS.SC-3
34	188	団体	添付C CPS.SC-3	ベンダーやSIerが超不利に見える。他の契約関係の法律と矛盾して、実効性が無いのではないか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.6 サプライチェーンリスク管理 CPS.SC-3
35	1	企業		翻訳）我々は、この最新の原案に対するレビュー期間の延長を含む経済産業省の公開協議プロセス、ならびに世界のステークホルダーからのコメントの受領および世界の利害関係者との関わりに対する関心を歓迎する。 私たちは、日本政府の「Society5.0」に対するビジョンと、そのビジョンをConnected Industriesプログラムを通じて支援するという経済産業省の意向に希望を得ている。フレームワーク原案の序文で説明したように、モノのインターネット（IoT）および人工知能（AI）テクノロジは、私たちの生活と社会を変革し、「人間中心の社会」に「新しい価値」を生み出す力を持っている。「AIによって、人間は膨大な量のデータを利用し、ヘルスケア、農業、教育、交通などの分野で飛躍的な進歩を遂げることができます。 AIが強化したコンピューティングが医師の医療ミスを減らし、農家が歩留まりを向上させ、教師が指導をカスタマイズし、研究者が私たちの惑星を守るためのソリューションを解き明かすのに役立つ方法をすでに見ています。」 しかしながら、経済産業省は「フレームワーク原案」の文脈を提供する際、「サイバー空間とフィジイカル空間」がより密接に統合されたよりデジタル的に関連を強めた社会が、サイバーセキュリティリスクへ影響を与えることを認識している。結果として、組織の運営と継続性を支援し、相互に関連するエコシステムを強化するために、サイバーセキュリティマネジメントへの効率的なアプローチの実装がますます重要になっている。基本的なサイバーセキュリティリスク管理の慣行が整っていなければ、組織はまた、Society5.0の実現に貢献するであろう先進技術を持続可能に統合することに苦労するかもしれない。さらに、セクターや地域を超えた基本的なサイバーセキュリティリスク管理アプローチの相互運用性がなければ、グローバルなバリューチェーンとよりダイナミックで直線性の低い「価値創造過程(バリュークリエイションプロセス)」による潜在的な利益が制限され、損なわれる可能性がある。	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。
35	2	企業		翻訳）フレームワーク原案に対する我々の見解は、私たちの企業のリスク管理の経験と、セクターや地域を越えて相互運用可能なサイバーセキュリティポリシーと要件の利点の認識に基づいている。原案の枠組みの中で、経済産業省は、ISO/IEC 27001:2013、ISA 62443、NIST Cybersecurity Framework 1.1を含む、提案されたセキュリティ対策と国際標準およびベストプラクティスで明確にされたものとの相互運用性にかなりの注意を払っている。特に、NIST Cybersecurity Framework のカテゴリを活用するための経済産業省の取り組みには、さまざまな組織に関連性のあるサイバーセキュリティリスク管理活動に役立つ枠組みを提供する価値がある。同様に、Cybersecurity Framework Subcategories 及び ISO/IEC 27001 管理策との整合性を示すための措置のマッピングを含むことで、より多くの組織にとってのフレームワーク原案の有用性が高まる。	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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
35	3	企業		翻訳）提案されているセキュリティ対策の、既存の国際標準やベストプラクティスとの相互運用可能性に対する組織の理解を確かなものにすることを目指してMETIが行った多くの投資をさらに進めるために、METIに第III部あるいは添付Dにて追加でISO/IEC 27103について検討することを勧める。ISO/IEC 27103は、ISO/IEC 27001やサイバーセキュリティフレームワークなど、すでにフレームワーク原案に組み込まれている多数の参考文献を、サイバーセキュリティリスク管理に関連する他のISOおよびIEC規格のいくつかと共にまとめたものである。（フレームワーク原案でも既に参照されているISO 31000を含む）。さらに、IEC規格へのマッピングを含めると、ISO/IEC 27103は、より広範な分野に特に関連し、さまざまな関連業界にわたるサイバーセキュリティリスク管理プラクティスの整合性を実証するのに役立つ。さらに、ISO/IEC 27103開発への重要な貢献者として、経済産業省は、そのガイダンスを追跡し活用することで、その価値を明確にし、国内および世界の両方の利害関係者に実証する立場にある。	本フレームワークは、主要な国際規格等を参照した上で策定しております。他方、新たな国際規格等も常に策定されることから、いただいた御意見も参考に、本フレームワーク策定後においても、様々な国際規格等を参照し、適正に改訂して参ります。
35	4	企業		翻訳）経営層、ERMの部門長、サプライチェーンのセキュリティやIoTの展開に重点を置いたグループのマネージャーなど、特定の利害関係者に合わせて簡素化されたガイダンスの提供によるフレームワーク原案の包括的なアプローチの補完 概念的な基盤だけでなく、リスク源の評価、一連のセキュリティ対策の提案、そして複数の国際標準とベストプラクティスへのマッピングについても記述した包括的な文書として、フレームワーク原案は重要な作業の集合となっている。一部の組織や利害関係者にとっては、そのすべてのコンテンツを1つのドキュメントにまとめることには価値があると思われるが、その他の者にとっては、フレームワーク原案のガイダンスを運用する役割と能力に基づいて、どのコンテンツが最も適しているかを認識するのは困難に思われる。 これらの利害関係者にとってフレームワーク原案の有用性を増すために、我々は、経済産業省がどの側面が異なる地域社会にとって最も有用であり得るかを検討し、適切かつその後のより合理化された自主的ガイダンスを開発するよう奨励する。たとえば、多くの経営幹部は、組織内で行われているサイバーセキュリティリスク管理活動のハイレベルの枠組みから利益を得て（たとえば、ISO/IEC 27103およびCybersecurity Frameworkの5つの特定、防御、検知、対応、および復旧の機能に似ている）、そのような枠組みがより単純化された方法で進捗状況や投資を追跡できるようにする。あるいは、企業リスク管理の担当幹部は、より広範な一連の活動を網羅し、それらをより詳細に評価するためのオプションを提供するフレームワークの恩恵を受ける可能性がある。さまざまな製品、サービス、または機能に関連する開発、配置、およびセキュリティまたはレジリエンスの問題。最後に、IoTの展開やサプライチェーンのセキュリティに焦点を当てたものなど、さまざまな製品、サービス、または機能に焦点を当てたグループの管理者は、より狭い一連の活動やプラクティスに関連するセキュリティ対策および標準に関する最も詳細なガイダンスから多くの恩恵を受ける。	本フレームワークは、サイバーセキュリティ対策の包括的な枠組を提示するものでありますが、いただいた御意見を踏まえ、産業活動の規模や利害関係者の立場に応じた、より効果的なサイバーセキュリティ対策へのアプローチについて検討いたします。
35	5	企業	添付C	翻訳）リスクに基づくアプローチと結果に焦点を当てたアプローチを通じた運用上の敏捷性と適切な焦点の育成 サイバーセキュリティリスク管理に対するリスクベースおよび成果重視のアプローチは、組織のミッションが変化し、テクノロジと脅威の展望が進化するにつれて、組織が優先的にリソースを適用し、十分な敏捷性と適応性を確保するのに役立ちます。リスクベースで成果重視のアプローチを採用していますが、両方の原則をさらに組み込む機会もあります。例えば、CPS.AC-6「特権ユーザーのためにネットワーク経由でシステムにログインするときに2種類以上の認証を組み合わせた多要素認証を採用する」は、重要なセキュリティ技術の使用を支持しているが、それは他の高度な技術や将来の発展の可能性（例えばバイオメトリクス）を説明するものではない。「アクセスの許可と承認は管理され、リスクに基づいて必要に応じて最低特権、義務の分離、および信頼性の高い認証方法を取り入れている」など、より成果重視でリスクベースの言葉を検討することをお勧めする。さらに、付録Cの中で、METIは、セキュリティ対策へのさまざまな投資レベルが必ずしも進歩のレベルと相関するのではなく、リスク評価とより広範な緩和戦略と同様に事業目的と優先順位に基づく適切な投資と相関するかもしれないことを反映するよう奨励する。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：本文第III部 3.7 アイデンティティ管理、認証及びアクセス制御 CPS.AC-6

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
35	6	企業		IoTセキュリティに取り組むグローバルなコラボレーションに必要に応じて貢献し、その認識を高め、そしてそれらの成果の統合 フレームワーク原案は、ネットワーク接続された機器のリスクプロファイルがそれらのユースケースとそれぞれの実装に基づいてある程度変動することを有益に認めている。送電、ヘルスケア機器、輸送、および工場は、特定の機能と機器クラスを共有する場合があるが、それらのセキュリティプロファイルと適切な脅威防御機能は必ずしも同じではない。IoTのユースケースとリスクプロファイルの多様性は、この分野に焦点を当てている政策立案者にとってより複雑になる。それでも、IoTセキュリティ対策のベースラインとしての世界的なベストプラクティスは、サイバーセキュリティリスク管理の文脈のように明確に定義されていないか、または広く認識されていないかもしれません。一方で、一般的なユースケースとより具体的なユースケースの双方において、経済産業省が検討する可能性がある数多くの試みがある。 例えば、インダストリー4.0の文脈では、インダストリアルインターネットコンソーシアム（IIC）インダストリアルインターネットセキュリティフレームワークは、サイバー空間の文脈だけでなく物理的な領域（つまり、潜在的な問題を考慮するために必要なセキュリティメカニズム）においてもIoTを保護するために必要な対策を記述している。セーフティ、レジリエンス、および信頼性(Reliability)への影響さらに、IICのIoTセキュリティ成熟度モデルは、インターネットセキュリティフレームワークの概念に基づいて構築され、ビジネス目標と優先順位、そしてリスクに基づいて、組織が達成するさまざまなレベルのセキュリティ投資を定義する。これにより、特定のユースケースを満たすセキュリティメカニズムへの投資が可能になるだけでなく、リソースの制約に直面している組織が投資を評価し、必要に応じてサイバーフィジカルシステムの管理を継続的に改善できる方法のマッピングも提供される。 一般消費者向けIoT機器のセキュリティに対処するために、英国政府は一般消費者向けIoTセキュリティのための行動規範を公表している。これは、一般消費者向けIoT機器の製造業者が実装することを推奨する13のセキュリティガイドラインを示している。このプラクティスは、100近くの文書と50の組織から発行された標準、推奨事項、およびガイドラインに基づいてマッピングされている。このマッピングのおかげで、製造業者は、一般消費者向けIoTに焦点を当てた、行動規範と産業と政府の両方からの既存の資料との間の関係をよりよく理解することができる。これにより、開発者はさまざまなプラクティスを実装する際に既存のガイドラインおよび業界で認められているガイドラインを簡単に活用できる。さらに、規範的ではなく、これらの原則の結果に焦点を当てた性質は、現在のベストプラクティスに基づいてデバイスのセキュリティを向上させ、その後より良い方法が利用可能になるにつれて進化するための十分な柔軟性を製造業者に提供する。 IoT機器の製造元とそれを使用するお客様の両方が、おそらく国際的な環境で動作することになる。それを考慮に入れて、私たちは経済産業省がサイバーセキュリティリスク管理の文脈でそうであるように、市場内で認識が高まっている世界的な共同作業と国際標準の認識に貢献し、その認識を高めることを奨励する。さらに参考として、米国国立標準技術局（NIST）は、IoTサイバーセキュリティを標準化するための国際的な取り組みをまとめたレポート案も発行しています。暗号化、インシデント管理、物理的なセキュリティなど、これらを各分野の国際標準にマッピングしている。サイバーフィジカルシステムを保護するために国際標準を活用することは、組織がグローバルなランドスケープの中で活動するのを助け、業界がサポートするプラクティスと実装ガイドラインから利益を得るだろう。	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。いただいた御意見も参考に、本フレームワーク策定後においても、引き続き、サイバーセキュリティを巡る国際的な動向を注視しながら、新たに策定される国際規格等についても、改訂の際に必要に応じて本フレームワークに反映してまいります。
36	1	企業	全体	プラットフォーマー（による産業構造）が想定されていない。 【理由】 ・GAFAやBATに代表されるプラットフォーマが多くの企業・個人の経済活動（取引含む）の基盤となっているが、本フレームワークではそのような産業構造・ビジネス構造の場合のセキュリティリスク（+信用リスク）について考慮されていないのでは？ ・プラットフォーム上で展開されるエコシステムでは、さまざまな事業者（法人・個人）がプラットフォーム上で事業を行うが、旧来の、長期存続・規模集積を旨とする企業とは異質な事業を営むもの・・・アドホックな事業者、サイバー空間上の個人、データ販売の事業者、あるいはAIによる自動取引など・・・、従来の企業とは異なる事業主体がますます増えてくることが想定される。（すでに始まっている） ・この場合に、事実上の信頼の「根」となるプラットフォーマが具備すべきセキュリティ対策と、当該プラットフォーム上で事業者側が用意すべきセキュリティ対策のあり方を、描くべきではないか？ ・これは産業用データをやり取りする、企業間CPSの「場」での経済活動についても同様なことが必要になってくる。	いただいた御意見については、本フレームワークの第3層、サイバー空間におけるつながりに含まれる内容と理解しております。本フレームワークの第2部では、各層における守るべきもの、セキュリティインシデント、脅威、リスク源を分析することで対策を整理することができます。御指摘のような内容についても本フレームワークを活用して、セキュリティ対策を整理することができると考えています。 また、今後、分野別や分野横断で具体的な対策を検討していく際、いただいた御意見も参考にさせていただければと思います。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
36	2	企業	全体	新たな経済社会の枠組みにおけるセキュリティあるいは信用のあり方についての考慮が不足している。 【理由】 ・従来の貨幣経済では「国」による貨幣・銀行システム等の信用担保が、経済活動の一つの「根」だったが、いま起きている、分散化・シェアリング・バウンダリレスな経済活動では、ブロックチェーンに代表される、分散された基盤の上での相互信頼の枠組みが拡大している。 ・従来は、国・中央銀行・金融機関・企業・・・という比較的安定な枠組みでの信用に基づいた商取引が基盤となっていたが、それとは異なる新たな枠組みでの相互信頼が形成されつつある。 ・このような新たな信用・相互信頼の枠組み、分散化した・中央で規制されない・動的な枠組みにおけるセキュリティのあり方に対する考慮も求められる。	本フレームワークでは、新たな産業社会におけるサプライチェーンをバリュークリエーションプロセスと定義し、3層構造モデル、6つの構成要素で整理することで、まさに御指摘いただいた『新たな信用・相互信頼の枠組み、分散化した・中央で規制されない・動的な枠組み』におけるリスクの評価等を行うことができると考えています。
36	3	企業	第Ⅰ部2.1	企業間、サイバーフィジカル、サイバー間という区分けが根本的に妥当性に欠くと思われる。 【理由】 現状の企業間の連携はサイバー間連携の一部とみなすことができるからです。	いただいた御意見は、3層がそれぞれ重なる部分がある点について、妥当性を欠くという御指摘と理解しました。3層構造モデルについては、本フレームワークの第Ⅰ部２．１において整理させていただいたとおり、企業のマネジメントのみに信頼性の基点を置くことではバリュークリエーションプロセスのセキュリティを確保することが困難である現状に鑑み、他の観点から、信頼性の基点を的確に設置することで、プロセス全体の信頼性を確保することを目指しているものです。それぞれの層が独立しているものと考えているわけではなく、御指摘いただいた理由は当たらないと考えており、原案のとおりとさせていただきます。
36	4	企業	6.	グローバルハーモナイゼーションを定義してほしい。 【理由】 グローバルハーモナイゼーションという言葉の定義なしにフレームワークの特徴と提示するのは妥当ではない。	本フレームワークでは、国際的なセキュリティ対策の動向と調和をとっていくことを目的として、国際的な規格等との比較を行って関係性を整理しています。この点について、グローバルハーモナイゼーションの実現という特徴で記載させていただいているものです。該当箇所において、この趣旨は既に明示されておりますので、原案のとおりとさせていただきます。
36	5	企業	6.	セキュリティレベルの選択に対する指針を示していただきたい。 【理由】 （Sheet2に示したような考え方もあるため、参考になればと思います。） 例えば、生産設備のログや環境センサデータをクラウドに転写して生産性向上や工場間生産連携の分析に用いる場合、データ転送だけの場合はLevel1。クラウド（を介した外部システムを含む）から制御システムに対して制御を行う場合はLevel2など、同一システム内で複数のセキュリティレベルの対策を組み合わせて利用するという使い方も考えられると思います。	いただいた御意見も参考に、記載を追記いたします。 修正箇所：本文第III部 2. 対策例集の見方
36	6	企業	p.17	サイバーをひとつにまとめて記述しているのは違和感がある。 【理由】 サイバー空間は企業内にも存在し且つ企業外のクラウドのような空間においても複数のドメインがあるからです。	いただいた御意見については、個別ドメインを抽象化してサイバー空間の特徴として捉えるという該当部分の趣旨とは異なるため、原案のとおりとさせていただきます。今後、分野別の議論等を進めていく中で参考にさせていただきます。
36	7	企業	表1.2-1	"フィジカル空間にて収集された.."は不足があると考えられる。 【理由】 データは企業内にあるマスターデータ（IoS）や人から取得されるデータ（IoP）など数種類のデータソースがあるからです。	本記載の後に続く『共有・分析・シミュレーションを通じて加工された情報』の中でいただいた御意見で提示された情報が含まれると考えているため、原案のとおりとさせていただきます。
36	8	企業	添付C CPS.AC-4	<Basic>の対策例について、他のクレデンシャルについても含めるような文章とした方がよいのでは。 【理由】 クレデンシャルの有効期間について、パスワードのみに言及しているように見受けられるため。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C CPS.AC-4
36	9	企業	添付C CPS.AC-6	<Basic>の対策例について、共有アカウントに対する取扱いは特に言及しないのか？ 【理由】 アカウントに対する一意性のように見受けられるため。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C CPS.AC-6

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
36	10	企業	添付C CPS.AC-7	<Advanced>の対策例について、後者の場合、外部ネットワークの内部境界のモニタリング/制御はできないのでは。また、<Advanced>レベルで内部境界のモニタリング/制御まで求めるのか。 【理由】 文言的には、「自組織のシステムの繋がるネットワーク」が、システムが属するネットワークなのか、システムが属するネットワークに繋がるネットワーク（外部ネットワーク）なのかが、不明瞭にように思われるため。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C CPS.AC-7
36	11	企業	添付C CPS.DS-3	<Advanced>の対策例について、CPS.DS-2 で通信経路の暗号化を求めているが、さらにデータレベルでも暗号化することを求めるのは冗長ではないか。 【理由】 この要件は、元々通信エンティティとデータ処理エンティティが一致しないケースを想定していると考えられるが、通信エンティティとデータ処理エンティティが一致するケースでは冗長ではないか。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C CPS.DS-2
36	12	企業	添付C CPS.DS-9	<Advanced>の対策例について、対策要件の「起動時に」と対策例の「定期的に」は矛盾するのではないか。 【理由】 必ずしも起動が定期的に行われるとは限らないため。	いただいた御意見も参考に、記載を修正いたします。 修正箇所：添付C CPS.AC-6
37	1	企業		翻訳）私たちは、将来を見据えたリスクベースのフレームワークを確立するための経済産業省の努力を称賛します。これは、企業がセキュリティリスクを特定、評価、および管理するための重要なツールになると考えています。 私たちは、すべての人と物がモノのインターネット（「IoT」）を介して接続されている「Society5.0」にフレームワークの草案が焦点を当てていることを特に感謝します。 我々は、この新しい接続性が途方もない価値を生み出すことにMETIに同意し、付随するセキュリティリスクを慎重に検討する必要があることに同意します。	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。
37	2	企業		翻訳）5Gの開発は、サイバースペースと物理的なスペースのより大きな統合を可能にすることによって、フレームワーク原案が取り組もうとしている種類の深い変革を可能にするでしょう。 日本はこの種のイノベーションの恩恵を長い間認識してきました。 確かに、日本はすでに2020年の東京オリンピックのために計画されていた5Gの打ち上げを促進する過程にあります。 現在、5Gは今年日本でのプレコマーシャル発売に続いて2020年に完全な商用化が予定されています。フレームワーク原案は継続的なイノベーションへのこのコミットメントを強化します。	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。
37	3	企業		翻訳）私たちは、関連性の高い社会で企業がセキュリティリスクを特定、評価、および管理できるようにするための重要なメカニズムとして、フレームワーク原案をサポートしています。 IoTが低コストのセンサーとアクチュエーターで展開されるにつれて、バイオメトリックデータ、位置データ、インフラストラクチャ監視データなど、ますます機密性の高い情報がモバイルネットワーク上を流れます。 機密データのこのような広範なアクセスと使用にもかかわらず、セキュリティ機能は業界のエコシステムやモバイルプラットフォームを使用するIoTアプリケーション全体ではまだ利用されていません。 私たちは、コネクテッドカー、スマートホーム、ビル管理、電力システムに焦点を絞った将来のユースケースを含む、企業がこれらのセキュリティリスクに対処するのを支援するためのフレームワークの草案の取り組みに励まされています。	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。
37	4	企業		翻訳）特にサプライチェーンマネジメントに関して、フレームワーク原案の前向きなアプローチを継続する。 私たちは、デバイスがますます接続されるようになるにつれて、新しいサプライチェーンの問題が発生することになるとMETIに同意します。例えば、IoTデバイスを使用して新しいデータを作成し、標準のリニアサプライチェーン外の物理デバイスを制御することができます。同様に、消費者は人工知能を使用してデータに価値を付加することができ、それによって伝統的な供給者や製造業者に由来しないサプライチェーンを開始することができます。これらのダイナミックなサプライチェーンによってもたらされるセキュリティ問題に対処するために、我々は経済産業省が関連するすべての事業体にわたってセキュリティリスクの将来的な評価を継続することを奨励する。その際、サイバーセキュリティサプライチェーンにおける最初のリンクは、新しいテクノロジシステムの基盤を形成する長期的な研究への投資であると考えています。信頼された企業がそのような研究の最前線におらず、それを標準化したり、革新のための資金を持っていない場合、このリンクは進化しません。それが起こると、連鎖は壊れ、接続されているすべてのデバイスとネットワークのセキュリティが影響を受けます。経済産業省は、携帯電話インフラストラクチャにおける潜在的な攻撃面を評価することができる検証センターの設立を検討し、そのようなシステムを国内通信事業者に設定することについて勧告を行うことができます。イギリスは、National Cyber Security Centerでこのアプローチで良い結果を出しました。経済産業省は、特にセルラーインフラストラクチャコンポーネント間の通信に関して、ISO、IEC、およびNIST規格を含む関連する国際規格への企業のコンプライアンスの評価を奨励することを検討する可能性もあります。	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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
37	5	企業		翻訳）世界をリードする標準を活用し続けます。 私たちは、フレームワーク原案は米国およびヨーロッパの主要な基準と一致しているべきであるという経済産業省の認識を歓迎します。 例えば、パートIII、付録C及び付録Dにはすべて、フレームワーク原案と、ISO、IEC、およびNIST規格を含む主要な国際規格との整合点が含まれています。 これは、フレームワーク原案を遵守するための措置を採用する企業が他国のセキュリティ要件をも満たすことを保証するだけでなく、国境を越えた主要なサイバーセキュリティプラクティスの使用も促進します。 標準は、サイバーセキュリティと物理的セキュリティの重要な要素です。我々は、相互運用可能なサイバーセキュリティ標準の開発を支援するための他の方法を検討するために、国際的なカウンターパートと継続して取り組むことにより、METIがフレームワーク原案を構築することを奨励する。	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。
37	6	企業		翻訳）フレームワークが、セルラーインフラストラクチャ製造のローカルで新しいモデルの開発をサポートするようにします。 METIは、サイバーセキュリティのリスクだけでなく、機械学習、AI、及びSDNによってもたらされる機会にも注目することをお勧めします。例えば、携帯電話インフラストラクチャの提供が、ほんの一握りのベンダに絞られるのを見ています。 私たちは、インターネット会社やソフトウェア定義ネットワーキングと市販のハードウェアを利用している新しい小さなプレーヤーによる有望な仕事を見てきました、そしてこのアプローチがセルラーインフラ市場に新しいプレーヤーを引き付けるために有望であるかもしれないと信じます。 そのため、経済産業省は、フレームワークが日本の国内インフラ産業を刺激する可能性がある方法を検討する可能性があります。フレームワーク原案に定められた明確なセキュリティ基準とプロセスから恩恵を受けることができます。	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。
38	1	企業		本フレームワークは、グローバルスタンダードとの対比や多くのフレームワークに欠けがちな具体的な対策水準に言及している点で、活用する際の実効性を念頭に作られており有用な枠組みであると考える。今後はNISTがWebサイト※で提供しているような本フレームワークを活用した事例(Success Stories)などを普及の観点から内外に積極的に公表して頂くことを期待したい。　https://www.nist.gov/cyberframework/success-stories	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。今後、普及の観点から、各産業分野でのフレームワークを活用した取組の発信についても検討して参ります。
38	2	企業		翻訳）物理的なアクセス制御とメディア管理に関する項目があります。 ただし、物理的なセキュリティの意味を考えると、以下の項目を新たに追加することが理にかなっている可能性があります（これらの項目はKISA（韓国情報セキュリティ機関）のISMSの内容に基づいて書かれています）。 1. 保護区域の指定 1）目的 保護区域、制限区域、公共区域などの物理的な保護区域を指定し、各区域に対して保護対策を確立して実施する必要があります。 主な施設やシステムを無許可の物理的アクセスおよびさまざまな物理的および環境的災害から保護するため。 2）アイテム - 主な施設やシステムを保護するために、物理的保護区域は そしてゾーン保護対策が実施されている。 （例） 。 公共区域：外部エリア 。 制限区域：オフィスエリアなど 。 保護区域：重要な施設とシステム区域	いただいた御指摘については、AC-2やIP-5において、記載させていただいておりますので、原案のとおりとさせていただきます・

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
				2. 施設の保護 1）目的 各保護地域の重要性と特性によると、それは持っているべきです 温湿度管理、火災検知、火災などの十分な設備 消火装置、漏れ検知、UPS、非常用電子発電機 電力線が重複しています。また、アウトソーシングを通じて重要なシステムが運用されている場合 ベンダー、セキュリティ要件は契約に反映され、定期的に見直されるべきです。 2）アイテム - 運用手順は以下に従って確立され管理されているか。 火災、停電、その他の災害に備えて必要な設備を備えた各保護区域の重要性と特徴 - 保護区域内の主要システムおよび人員を火災から保護するための施設が設置され維持されているか。 - 非常ベル、非常灯、非常経路標識が設置されているか 火災やその他の災害が発生した場合に、要員が安全に避難することができますか？ - 施設内の主なシステムを確実にするために漏水を検知するための施設が設置されているか。 保護区域は洪水から保護されており、継続的に運営されているか 維持？ - 恒温恒湿設備は設置され維持されているか。 - 安定的に電力を供給する施設が設置され維持されているか。 - 重要なシステムがアウトソーシングベンダーを通じて運用されている場合、物理的保護のためのセキュリティ要件は契約に反映され、定期的に見直されていますか？	
38	3	企業		フレームワークを実行するにあたって求めている人材または人材像については記述がない。 確認したところ、２．２．６つの構成要素の「表１．２－１バリュークリエーションプロセスに関わる6つの構成要素」では、ヒトを定義している。また、CPS.RA-2,CPS.AE-3,CPS.AE-2,3ではSOC/CSIRTやインシデント対応の人材スキルを述べられている。 したがって、網羅的に対策要件と対策例集を述べているのにも関わらず、人材または人材象（スキル）はSOC/CSIRTやインシデント対応しか触れていない。網羅的に対策要件と対策例集を述べるのであれば対策毎に必要なスキルを追加するとよいと思う。	人材のスキルについては、産業サイバーセキュリティ研究会WG2（経営・人材・国際）の中で議論を進めているところであり、いただいた御意見も踏まえ、フレームワークを活用に求められる人材像についても引き続き検討してまいります。
38	4	企業	p.56, 80 etc	翻訳）「異常な活動」と「異常」という言葉は同じ意味で使われていますが、日本語版では同じ言葉が使われています。 2つの単語、異常と異常はどちらも正常ではないものを指します。 異常は、それらが集められたデータにもっと焦点を当てます。 異常はもっと悪い意味合いがあります。 それはほとんどいつも悪いことを指すのに使われますが、異常は悪いことも悪いこともありません。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.
38	5	企業	CPS.MA-1	翻訳）CPS.MA-1の対策要件がNIST Cybersecurity Framework Ver.1.1のPR.MA-1と一致しません サイバー/物理的セキュリティフレームワーク - 重要なセキュリティアップデートなどをIoTデバイスおよびサーバーで適切かつ適時に実施する方法について説明し、適用する。 - 必要に応じて、リモートコマンドを介してさまざまなソフトウェアプログラム（OS、ドライバ、およびアプリケーション）の一括アップデートを実行するためのリモートアップデートメカニズムを持つIoTデバイスを導入する NISTサイバーセキュリティフレームワークVer.1.1 組織資産の保守および修理は、承認され管理されたツールを使用して実行および記録されます	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.11 保守 CPS.MA-1
38	6	企業	CPS.PT-2	翻訳）CPS.PT-2 の対策要件は、NISTサイバーセキュリティフレームワークVer.1.1 PR.PT-2およびPR.PT-3をカバーするのに十分ではありません。 PR-PT-3に記載のとおり。 最小限の機能の原則は、必須の機能のみを提供するようにシステムを構成することによって組み込まれています サイバー/物理的セキュリティフレームワーク 不要なネットワークポート、USB、およびシリアルポートを物理的にブロックして、IoTデバイスとサーバーの本体に直接アクセスします。 --->内容は特定の部分に限定されています。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.12 保護技術 CPS.PT-3

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
38	7	企業	D-3-8 A.9.2.1	翻訳）A.9.1.1アクセス制御ポリシー/アクセス制御ポリシー A.9.2.1 A.9.2.1ユーザー登録と登録解除ユーザー登録と登録解除 重複する単語が使用されています。	いただいた御意見を踏まえ、修正いたします。 修正箇所：添付D-3
38	8	企業	第Ⅲ部 CPS.AC-4 CPS.DS-5	翻訳）CPS.AC-4 / CPS.DS-5 ロックアウトメカニズムがアクティブである場合、DoS状態は意図的にロックアウト攻撃をすることによって発生する可能性があります。 十分な処理能力と記憶容量があってもこの攻撃を防ぐことはできません。 行動検出など、DoSに対する別の対策を検討することが望ましいです。	いただいた御意見を踏まえ、修正いたします。 修正箇所：本文 第III部
38	9	企業	第Ⅲ部 CPS.SC-2 CPS.MA-1	翻訳）CPS.SC-2 / CPS.MA-1 使用前にサポートライフサイクルを確認することが望ましいです。 アップデートおよびパッチの提供のためのサポートライフサイクルが定義されている製品のみを使用する。 サポートライフサイクルが終了する前にシステムを破棄してください。 サポートライフサイクルが定義されていない製品を使用しないことが望ましいです。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.SC-2
38	10	企業	第Ⅲ部 CPS.CM-3	翻訳）CPS.CM-3がNIST DE.CM-4およびDE.CM-5と一致しません	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.14 セキュリティの継続的なモニタリング CPS.CM-3
38	11	企業	第Ⅲ部	翻訳）間違ったCIS参照 - ページ57> CPS.AM-4	CIS CSC 112 - > CIS CSC 11 - ページ70> CPS.AT-2	CIS CSC 917 - > CIS CSC 17 - ページ71> CPS.DS-1	CIS CSC 1713、14 - > CIS CSC 13、14 - ページ71> CPS.DS-2	CIS CSC 1713、14 - > CIS CSC 14 - ページ71> CPS.DS-3	CIS CSC 1713、14 - > CIS CSC 14	いただいた御意見のとおり、修正いたします。
38	12	企業		翻訳）文書全体に小さなスペルミスがあります。 例えば 7ページ、セクション（3）amaong - > among。 スペルチェックを実行してください。	いただいた御意見のとおり、修正いたします。 修正箇所：英語版 本文 7. (3)
38	13	企業	CPS.CO	翻訳）CPS.CO-2には「組織に対する社会的評価の回復に取り組む点を位置づける」とあるが、組織に対する社会的評価回復だけでなく、「インシデントが社会に与える影響を評価し、社会全体への混乱を防止するための伝達活動に取り組む」点をCPS.COに追記してはどうか。 【理由】 すべてがつながる社会(Society 5.0)は、インシデントが引き起こす社会全体への影響がこれまでよりも大きくなるだけでなく、ある1つのインシデントが他のインシデントを誘発するなどの事態も想定される。"3.17. CPS.CO – 伝達"に記載の「内外の利害関係者」の例には「地域や社会全体」が含まれていないが、近年においても一定のインシデントが発生した場合には、地域および社会全体がインシデントを起こした組織に対してコミュニケーション（情報発信）を求めるニーズは増していると思われ、"Connected Industries"がより浸透すれば、今後もそれらはさらに高まってくることも想定されるため。	いただいた御意見も参考に、修正いたします。 修正箇所：本文第III部 3.17 伝達 本文第III部 3.18 分析 CPS.AN-1
39	1	団体	エグゼクティブサマリー	「サプライチェーンの拡大は、攻撃側にとっては、ネットワーク化されたサプライチェーン上に攻撃起点が広く拡散していくことになり、～」の文章で、「攻撃者側にとっては」の述語が明確でなく、文章の意味が分かりにくいため、次のようにしてはいかがでしょうか。 代案） 「サプライチェーンの拡大は、ネットワーク化されたサプライチェーン上に攻撃起点が広く拡散していくことになり、攻撃側が攻撃起点を得る機会が増え、防御側が守るべき範囲が急激に拡大することを意味する。」	いただいた御意見のとおり、修正いたします。 修正箇所：エグゼクティブサマリー
39	2	団体	1.	「これまでの情報社会（Society 4.0）では、必要な知識や情報が共有されず、」とありますが、情報社会でも共有はされてきたと思います。そのため、ここでいう「共有」とはどういったものを指すのかの説明があった方が、読者に理解されやすいのではないでしょうか。	いただいた御意見については、十分には共有されないことが多く、そうした場合には、といった趣旨で記載させていただいていたものですが、御指摘を踏まえ、修正いたします。 修正箇所：はじめに 1.
39	3	団体	2.	「転換処理」とは具体的にはどういったことを指すのでしょうか？また、アナログからデジタルへの「変換」とも異なるのでしたら、「転換処理」がどういったことを指すのか説明が必要かと思います。可能であれば、例示があると読者も理解しやすいのではないでしょうか。	いただいた御意見も参考に、修正いたします。 修正箇所：はじめに 2.
39	4	団体	7.	「信頼性リストの策定」とありますが、初出であるP8の本文またはP8の脚注に説明（P20に記載している「信頼性リスト」の説明等）を入れた方が読者は理解しやすいのではないでしょうか。もしくは、P20を参照としてはいかがでしょうか。	いただいた御意見も参考に、修正いたします。 修正箇所：はじめに 7.
39	5	団体	第Ⅰ部1.	「組織の信頼という信頼点だけではなく」とありますが、「組織の信頼という観点だけではなく」の誤りではないでしょうか。	いただいた御意見のとおり、修正いたします。 修正箇所：第Ⅰ部1.

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
39	6	団体	図1.2-4	「第2層」の表記がどの部分を指しているか分からないので、「第2層」の範囲を何らかの色で囲ってはどうでしょうか？ もし、ピンク色の横軸全体を指すのでしたら、ピンク色の横軸内に配置した方が良いのではないでしょうか。青色の横軸とピンク色の横軸が接している横軸を指すのでしたら、その部分だけ、他の色で囲むなどの「第2層」の範囲を明示した方が良いのではないでしょうか。	いただいた御意見も参考に、修正いたします。 修正箇所：第Ⅰ部 図1.2-4
39	7	団体	図2.1-9	IEC TR 63069 の文言で「リスク分析結果に基づいて、安全機能仕様、セキュリティ仕様機能をそれぞれ設計する」とありますが、「セキュリティ仕様機能」は「セキュリティ機能仕様」の誤りではないでしょうか。	いただいた御意見も参考に、修正いたします。 修正箇所：第II部 図2.1-9
39	8	団体	第Ⅲ部3.8. CPS.AT	「自組織の職員およびパートナーに対して」とありますが、「自組織の要員」の誤りではないでしょうか。	組織は、必要に応じて外部委託先等のパートナーに対してもセキュリティに係る教育・訓練を実施することが必要と考えております。そのため、いただいた御意見については、原案のとおりとさせていただきます。
39	9	団体	第Ⅲ部3.9. CPS.DS	「データと記録をデータの機密性、完全性、可用性を保護するために定められた～」とありますが、ここでいう「記録」は何を指すのではないでしょうか。「データ」は表3.3-10 CPS.DS カテゴリーの対策要件において、「情報（データ）」とあるため、「情報」と受け取れますが、それに対して「記録」とは「（電子化されていない）情報」や「記録する」行為にも推察できるため、補足が必要ではないでしょうか。	いただいた御意見も参考に、修正いたします。 修正箇所：第III部 3.9 データセキュリティ
39	10	団体	第Ⅲ部3.17. CPS.CO	「例えば法執行機関のような組織からの支援を得られるように～」とありますが、冒頭の「例えば」は不要ではないでしょうか。	いただいた御意見のとおり、修正いたします。 修正箇所：第III部 3.17 伝達
39	11	団体	第Ⅲ部3.19. CPS.MI	「セキュリティインシデントを解消するための活動を実施する」とありますが、本章のタイトルからすると「セキュリティインシデントを解消する」ではなく、「セキュリティインシデントを低減する」ではないでしょうか。	いただいた御意見のとおり、修正いたします。 修正箇所：第III部 3.19 低減
40	1	企業		翻訳）産業の範囲 本稿は、さまざまな異種の産業データ間の関連性を構築することによって価値を生み出す、「Connected Industries」と呼ばれるプログラムに焦点を当てています。 「Society5.0」におけるプライバシーに関する市民の要件と懸念は時々まもなく言及されるが詳細には詳述されない。 それについての別の論文があるかもしれません。 もしそうなら、テュフラインランドもこの論文を喜んでコメントするでしょう。 そうでない場合は、開発してサポートを提供することをお勧めします。 我々は適切なレベルのデータ保護について相互承認を得て日欧間で適切な合意を結んでいるので、この追加の論文はGDPRに基づくことができる。	本フレームワークにおいては、取り扱うデータの内容については詳細について言及はしていません。いただいた御意見については、分野別の具体的な議論、例えばスマートホームの議論などを進めていく中で検討を深めていきたいと考えています。
40	2	企業		翻訳）ハッカーの標的 サイバーセキュリティは、Connected Industriesプログラムにとって非常に重要です。 攻撃者は、相互接続された新しいサプライチェーンにさらに多くのターゲットを見つけることができるため、サイバー防御を大幅に強化する必要があります。 業界のハッカーの目標は詳細に詳しく説明されています。 さらに消費者サイトにハッカーの標的がある エンドユーザーを相互接続サプライチェーンの一部と見なすことをお勧めします。 彼は、サイバーセキュリティのリスクとそのリスクを最小限に抑えるためにどのようにサポートできるかについて、透過的に知らされ、十分な教育を受けている必要があります。 これまでのところ、トレーニングと教育は、セキュリティインシデントの発生を防止することの発生と影響を抑制するために割り当てられた役割と責任を果たすことができるように、組織内のすべての個人に対してのみ考慮されます。 消費者もリスク源であり、強調されるべきです。	本フレームワークでは、エンドユーザーもサプライチェーンの一部と捉えた上で、主にサービス提供者側が実施すべきセキュリティ対策を取りまとめたものになっており、エンドユーザーもステークホルダーとして位置付けています。消費者の教育等に関する御意見は、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。
40	3	企業	Appendix A.	翻訳）スマートホーム Smart Homeは、102ページのユースケース＃4と見なされます。 スマートホームサプライチェーンについての私達の見解について、私たちは次の写真を共有したいと思います。 エンドユーザー/オペレータはその一部です。（図は省略）	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。本フレームワークのユースケースでは、エンドユーザーを「住まい手」として捉え、オペレータ含めてサプライチェーンの一部と認識しています。
40	4	企業		翻訳）人工知能 保護する必要がある膨大な量のデータを分析するためのツールとして、人工知能（AI）が挙げられています。 私たちはより広い範囲でAIを見ます： AIは、サイバー攻撃を防ぐためのツールとしても使用できます。 侵入やデータ侵害の可能性をより的確に特定し予測するための市販のAIプラットフォームがあります。 正反対のAIを使用して、サイバーセキュリティ攻撃を開発および実行できます。 AI自体は、人間に制御されたり理解されたりせずに他のシステムを攻撃することを決定することができます。 これまでのところ、これらは「将来の夢」ですが、AIはますます独立したものとなり、より高度な自律性をもって独立して決定するでしょう。 ドイツ政府はAIのセキュリティとプライバシーに関するいくつかの点を含むAI戦略を開発しました。 これはTÜVRheinlandによってコメントされており、ここから入手できます。https：//www.bmbf.de/files/Nationale_KI-Strategie.pdf（ドイツ語のみ）	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。

ID	No	提出者	該当箇所	御意見	御意見に対する考え方
40	5	企業		翻訳）暗号化 データの暗号化と通信チャネルの暗号化は、セキュリティにとって重要なポイントです。 これは、例えば、NIST Cybersecurity Frameworkおよび他の出版物で考慮されており、それらは論文で参照されている（例えば77ページ）。 また、「情報（データ）を適切なレベルのセキュリティ強度で暗号化して保存する」とも述べられています。L1_1_a_DAT。 108ページ。 IoTデバイスの内部メモリのデータ暗号化がどれほど重要かを指摘しておきます。 多くの場合、Wi-FiパスワードはIoTに暗号化されずに保存されます（例：https://limitedresults.com/2019/01/pwn-the-lifx-mini-white/）。 ユーザのWi-Fi認証情報が回復されました（プレーンテキストでフラッシュメモリに保存されています）。 より明確でより規範的な推奨事項を用いて、この点をより強く強調することを提案します。	いただいた御意見も参考に、修正いたします。 修正箇所：添付C CPS.DS-1
40	6	企業		翻訳）認証とサイバー保証 エコシステム内には、製造業者によって開発されているデバイスおよびIoTシステムの独立した検証、検証、および認証の役割があるはずです。 これにより、サプライチェーン全体に透明性とある程度の保証がもたらされます。	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。