パブリックコメントで寄せられたご意見に対する考え方（案）

【資料４】

ID	No	提出者	該当箇所	御意見の概要	御意見に対する考え方
1	1	匿名	-	世界的なIoTの普及に伴い、我が国でもSociety 5.0やConnected Industriesへの取り組みが急務と思われる時代になりつつあると感じています。 とは言いますものの、CPSF３層モデルを実現・実装しようとした場合に「統一電子認証基盤がない」と感じる事が多くございます。 この問題を掘り下げますと、サーバ認証であればセコム社・シマンテック社になりますし、e-Govでは電子認証登記所さまや日本電子認証株式会社さまが紹介されているため、用途に応じた個別契約が必須と言える現状はとても効率が悪いと感じますし、CPSF第三層における「データの信頼性（両開き青矢印）」に疑問符がつく原因ではないかと思います。 デジサート・ジャパン合同会社によるホワイトペーパー「Global State of Online Digital Trust」によれば、オンラインの信頼性と収益低下の直接的な関係性が指摘されています。 国外でも例のない話であるため実現の可能性は低いと感じますが、株式会社ではない、政府機関（または公益機関）による統一電子認証基盤の整備も重要ではないでしょうか？	いただいた御意見は、今後、サイバーセキュリティ政策を進める上で参考にさせていただきます。
2	1	個人	-	フィジカル空間とサイバー空間の境界である第２層において、流れる情報のフィルターまたは関門の機能の検討を提唱します。 目指しているSociety 5.0は、近い将来確立するであろう超高速大量情報通信システムを礎に、現実社会(フィジカル空間)に生きる人々の営みや人々が使用する機器・システム等から産み出されるデータ等情報をサイバー空間に送り、そこで形成されるビッグデータを基に、そこでの分析や計算、シミュレーションから産み出される価値や知恵を現実社会に還元し、現実社会に生きる人々の福祉に寄与する社会、とイメージしております。 その境界である第２層には、サイバー空間に向かう上りの情報(データ等)と、フィジカル空間(現実社会)に向かう下りの情報(演算結果等)の二方向の情報の流れがあると思います。この流れについて、間違いなく通す(セキュリティ・セーフティ)機能に加えて、問題のある情報をブロックする機能が必要と考えるわけです。 フィジカル空間に存在する大量で様々な機器のアクチュエータが受けるまたセンサが発する信号、人々の行動の軌跡、撮影・認証・解析された映像等のデータ、商品流通・企業活動等が産み出す諸情報、等々、そのようなものが上りの情報として第２層を通ってサイバー空間のビッグデータに挿入されていくと思います。しかしながら一旦ビッグデータに取り込まれてしまったものはもはや人の力では簡単には修正できないものになっているはずです。そうであるからこそ、第２層において、誤った情報や問題のある情報を的確に識別してそれを排除する機構が必要と考えるわけです。 考えられるものとして、部品の故障による誤信号、輻輳等によるデータの不達や入れ替わり、人的ミス(思い込み、誤解、操作ミス等)、バグ、悪意(フェイク、サイバー攻撃等)、その他いろいろな要因が想定されます。例えばもしある人のデータが誤って別の人のデータとすり替わってビッグデータに取り込まれたとたならば、後々取り返しのつかない事態を産むこともあるでしょう。 それとともに、人々にはプライバシーがあり、他人に知られたくないことは誰にもあると思います。家庭での夫婦生活とか、私的な時間において自分所有のＩＴ機器を通してある種のサイトを閲覧したとか、ある店に寄った姿を街頭カメラに撮影され顔認証されたとか、そのような人に知られることを望まない情報についてはビッグデータに取り込まれないようにする配慮は不可欠かと思います。しかしながら、これについての削除の判断基準は、ある種の価値観、コンセンサスに基づくものになると思うので、これはとても難しい作業になると思われます。下手をすると例えば犯罪の未然防止に役立つ情報等をカットしてしまうことにもなるかもです。 下りの情報の制限が必要と思うのは、ビッグデータのそのままの活用やコンピュータがはじき出す結果の盲信というのは危険と思うからです。蓄積されたビッグデータを基にコンピュータがはじき出す演算結果が、社会をどこに牽引、誘導してしまうのかが気になります。皆が幸せになる社会を期待してこのシステムを構築したのに、コンピュータはそれと違う結果をはじき出すかもしれません。これを人間という尺度で取捨選択をする機能が必要と思います。しかしこれも価値観やコンセンサスをもとに設定しなければならないので、難しいところと思います。政治やイデオロギー等の介入の条件ともなるかもです。 さて、第２層はどこに存在することになるでしょうか。今日的な雰囲気からすれば、ＧＡＦＡをはじめ、一定の電気通信事業者等に集中すると予測されます。利益を追求する私企業です。そこに存在する倫理は、はたして社会一般のそれと一致するでしょうか。各企業の戦略に作用され、倫理が歪曲される可能性もあります。これらの倫理を形成する基本的な力は、人間性なのか、欲望なのか、競争なのか、イデオロギーなのか、そのあたりのことを丁寧に見極める必要性を感じます。それをコントロールするために、国(民主勢力)の介入等も考慮する必要性を感じます。	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。
3	1	団体	-	第2層を対策の決めてとし「転写機能の正確性」に絞り込んでいるが、その後関する記述がない。 後半部分に「本フレームワークを利用することで転写機能の正確性」が担保できる理由を説明すべきである。	ご指摘の通り、CPSFにおける第2層は「転写機能の正確性」を信頼性の基点としています。一方で本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有するためのものであり、本フレームワークによって必ずしも転写機能の正確性が担保されるものではありません。転写機能の正確性をどのように担保するかについては、「『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース」での議論を踏まえた上で、引き続き検討してまいります。
3	2	団体	-	セーフティまで踏み込んだ、検討のためのフレームワークとするなら、業界の「セーフティ」面への取り組みへの繋がりが必須と思われる。 製造系ではまさに「確率的定義」を含めたIEC 61508に規定されるSILやISO26262のASILなどでレベルを規定し、開発するのが標準として必須になっている。それとは別の定性的レベルを提示するならば、少なくともSIL/ASILへのマップの仕方へのガイドを、今の時点で無いのであればせめて今後の更新版で追加するなど謳うことが望ましい。	本フレームワークでは、様々な人命/身体、プライバシー/名誉、資産、生活環境、経済活動への影響、風評等の影響を受ける様々な事象を「発生したインシデントの影響の回復困難性の度合い」及び「発生したインシデントの経済的影響の度合い（金銭的価値への換算）」の軸で整理し、リスクのカテゴライズを行っておりますが、いただいた御意見も参考に、本文「3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理」を以下のとおり修正いたします。 ・「なお、本フレームワークに基づき、産業界での議論等を踏まえた上で具体的な要求を整理する際には、起こりやすさについても考慮することが適切であることに留意されたい。」を追記 また、本文「3-3 求められるセキュリティ・セーフティ要求の整理」を以下のとおり修正いたします。 ・「なお、対策の実施はコストに直結することから、求められるセキュリティ・セーフティ要求に対しどのような対策を取るかは、インシデントの起こりやすさ等も踏まえた上で決定されることが適当である。」を追記 今後、セキュリティ・セーフティ要求を検討する際、一般的には起こりやすさの議論も必要であるところ、国際標準等も参照しながら、各産業界や機器の性質等を踏まえて検討してまいります。
3	3	団体	-	おおよそ殆どの国際規格やガイドラインでは、「リスク」という用語を「起こり易さ（発生確率）」との関係で定義しており、算出が難しいという理由によって「起こり易さ」を排除した時点で、本フレームワークで「リスク」という用語を使うことは混乱を生じさせるものと思われる。 拠って、本ガイドラインの用途において、リスクの整理に「起こり易さ（発生確率）」を除外しても差し支えが無いという根拠を明示するか、もしくは、「本フレームワークでは、（便宜上）全てのインシデントにおいての「起こり易さ」を一定と考える」とか、「ユースケースとしてリスクと対策を整理する際には、別途、「起こり易さ」への考慮を必要とする」などの注記が必要ではないか。	本フレームワークでは、様々な人命/身体、プライバシー/名誉、資産、生活環境、経済活動への影響、風評等の影響を受ける様々な事象を「発生したインシデントの影響の回復困難性の度合い」及び「発生したインシデントの経済的影響の度合い（金銭的価値への換算）」の軸で整理し、リスクのカテゴライズを行っておりますが、いただいた御意見も参考に、本文「3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理」を以下のとおり修正いたします。 ・「なお、本フレームワークに基づき、産業界での議論等を踏まえた上で具体的な要求を整理する際には、起こりやすさについても考慮することが適切であることに留意されたい。」を追記 また、本文「3-3 求められるセキュリティ・セーフティ要求の整理」を以下のとおり修正いたします。 ・「なお、対策の実施はコストに直結することから、求められるセキュリティ・セーフティ要求に対しどのような対策を取るかは、インシデントの起こりやすさ等も踏まえた上で決定されることが適当である。」を追記 今後、セキュリティ・セーフティ要求を検討する際、一般的には起こりやすさの議論も必要であるところ、国際標準等も参照しながら、各産業界や機器の性質等を踏まえて検討してまいります。
3	4	団体	3-3　求められるセキュリティ・セーフティ要求の整理	第１軸＆第２軸は、「問題領域に内在する要件（本質的な要件）」としてのレベルわけ。一方第３軸は、本質的な要求ではなく「手法の分類」に過ぎず、またこの分類は強弱というレベルわけではない。 したがって、この３軸を図６のように直行させるのは違和感が大きい。	「第1軸：発生したインシデントの影響の回復困難性の度合い」及び「第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）」は機器・システムのカテゴライズに用いるものであるのに対し、第3軸である「求められるセキュリティ・セーフティ要求の観点」はカテゴライズされた機器・システムにおいてどのような観点でセキュリティ・セーフティ要求を検討すべきか示すものです。なお、いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
3	5	団体	3-3　求められるセキュリティ・セーフティ要求の整理	第３軸として上げられている4つの観点が、これら自体に順序関係や包含関係があるのか否かが分かり難い。 順序関係がある、即ち、第3軸が「確認要求の強度」という概念で、例えば、第2の観点が要求される場合、必然として第1の観点も要求される（もしくは、第2の観点が要求される場合は、第1の観点は不要）というのであれば、その様な順序カテゴリであることが判るように書くべき。 他方、これらが順序性の無い独立した4つの観点である場合は、第3軸自体が4つの要素（観点）を持つベクトルになるので、図6のような立方体の表現は誤解を招くので改めるべきである。（この場合、図中の肌色のプレートは、必ずしも、最低面から始まり連続して上に延びる単一のものにはならないこともあり得る。）	いただいた御意見を踏まえ、本文「3-3 求められるセキュリティ・セーフティ要求の整理」を修正いたします。 ・図6「カテゴリに応じて求められるセキュリティ・セーフティ要求の観点のイメージ」における青矢印を削除し、第1の観点～第4の観点という文字に修正 ・「第3軸における4つの観点は、それぞれが必ずしも完全に独立したものではない。」を追記 ・「また、必ずしも全ての観点での要求が求められるものではなく、例えば第2の観点に係る要求が無くとも、第1や第3の観点に係る要求により対策を構成することも考え得る。」を追記
3	6	団体	3-1　基本構成の背景にある考え方	求められるセキュリティ・セーフティは多様性を考慮する必要があると「基本構成の背景にある考え方」に記載されているが、要求がカテゴライズされているだけで、「回復困難性が高いシステムはここまで要求する必要がある」ということが分からない。高中低などである程度要求事項を整理しないと活用できるフレームワークにならないのではないか。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的な要求事項は、IoT機器の多様性等を考慮し、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
4	1	個人	-	日本国政府がメーカーに日本独自のスーパーコンピューター(以下電脳太郎)を受注し開発を助成する。電脳は2重構造に成って居て民間のコンピューターネットワークからは完全に自由に切り離す事が出来る(信号機の管理と同じ様に民間のコンピューターはアクセスできない)太郎の心臓部(絶対に正常状態だけを保存する機能)と太郎の神経系(心臓より先にプログラムを実行して見る機能)。そして太郎の周辺機器として太郎と類似する機能を十分に兼ね備えたシミュレーター(以下電脳花子)に民間のネットワークを接続し花子に一度アクセスしプログラムを一定期間実行させる。花子は事前に制限が掛けられて居てサイバー攻撃性や事故被害性を検知し除外するプログラムを拡充しながら実行して居る。高精細シミュレーターで異常が発見されなければ太郎に花子を通してアクセス可能とする。民間のアクセスにより花子が破損した場合は太郎との正常な関係性以前の状態に問題性をピックアップし一時停止しながらも強制的に元に戻す事が出来る事にする。太郎と花子は日本独自の暗号化された日本語版のコンピューター言語で繋がり絶えず正常を保つように扶助し合って居る。太郎の権限も多重化しない様に分権化され各権限が隔絶されながらも確立しなければならない。花子には民間のコンピュータとやり取りできる一般的なコンピューター言語も兼ね備えて居る。逆説的にパニックを引き起こさない様に被害に繋がるプログラムを理解する事が初めから出来ない様にProgramする。花子に認証され政府が許可したProgramだけを太郎に落とし込むプロセスを創り上げる事で1度認証されたシステムは完全に守られる。 余談ですがポイント経済政策を日本で実施しませんか？ポイントとは一般的に販売者が購入後に付与するポイント還元ではなく。日本政府が購入直前に購入予定額に対してポイントを発行する経済システムです。ポイントは大蔵省の認証IDが当てられ偽造できない様な仕組みの電子ポイントです。ポイントを消費税よりも高い割合で発行すれば日本の消費社会が活発に成るでしょう。勿論国民すべてにお財布端末を開発して無料で配布する事にします。現金経済、電子マネー経済、電子ポイント経済の3本柱です。ポイントは購入予定のサービス限定の購入(1次利用)にしか利用できずに、購入されない場合は直ぐに消失します。販売者はポイントを回収で通貨として日本国内で利用できます。間接的なポイントの2次利用の比率を決めて置き、2次利用されたポイントは販売者によって流通貨幣の様に扱われますが、インフレ防止を兼ねて2次利用の後の利用時に半額ずつ政府が回収(シャボン効果＝ポイント販売税)します。回収した政府はポイントを全額通貨と同様に利用できる様にします。又、政府の社会保障システムを大幅に拡充して置き、広く国民に活用して貰える様にする為には、消費販売とは区別して2次利用の際と同様にそれ以後の利用時にも全額利用出来て国にポイントで社会保障(失業保険等、あらゆる社会保障)に加入し其れを利用できるようにします。社会保障費用は一般的な税金からポイント回収した相当額に当てて行き、ポイントは消失させます。 此のポイント経済システムの導入により更に抵抗感なくスムーズに売り買いが成され、企業で働く者の社会保険等の負担の軽減をしながらも消費税自体は増収し2次利用以降の回収できる半額ポイントも国庫として考えられる。	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	御意見の概要	御意見に対する考え方
5	1	企業	3-2-3　フィジカル・サイバー間をつなげる機器・システムのカテゴライズ	P9 223行目 3-2-3節「フィジカル・サイバー間をつなげる機器・システムのカテゴライズ」について 機器をマッピングするのではなく、機器の機能・リスクをマッピングするべきと考えます。 ■根拠 P9 223行目 3-2-3節において、「フィジカル・サイバー間をつなげる機器・システムのカテゴライズ」という説明がございますが、3-2節冒頭におきまして、「フィジカル・サイバー間をつなぐ機器システムに潜むリスクのカテゴライズ」（P7 180行目）と記載しております。 つまり、「発生したインシデントの影響の回復困難性」と「発生したインシデントの経済的影響の度合い」の2軸で整理されるのは「リスク」であり、「機器・システム」とは異なります。 上記により、P9 223行目 3-2-3節で説明する機器・システムを前述の2軸で整理するのは不適切と考えます。 ■対案 IoTシステムの一例として、以下のような空調のIoTシステムを考えます。 ・クラウドを介して複数の端末（スマホ、PC、など）から遠隔で冷暖房機能を操作（温度設定、冷暖房切替、など）を行うシステム 上記IoTシステムの冷暖房機能において、以下のようなリスクが挙げられます。 （1）DoS攻撃により停止する （2）不正ログインされて意図しない設定変更される （3）クラウドが不正アクセスで顧客情報を取得される （4）不正ログインされて設定情報が漏えいする これらのリスクを経済的影響の度合い（以下、経済的影響）と発生したインシデントの影響の回復困難性の度合い（以下、回復困難性）の2軸を小/中/大の3段階で整理しますと、以下のように整理できると考えます。 （1）経済的影響：中　回復困難性：小 理由：冷暖房機能が停止すると人命/設備に一定の影響が存在するため、経済的影響があると考えます（病院、データセンタ、など）。 一方、SWアップデートなどで回復は可能なため、回復は可能と考えます。 （2）経済的影響：中　回復困難性：小 理由：冷暖房機能の設定変更により空調制御が変わると、人命/設備に一定の影響が存在するため、経済的影響（病院、データセンタ、など）があると考えます。 一方、SWアップデートなどで回復は可能なため、回復は可能と考えます。 （3）経済的影響：中　回復困難性：中 理由：顧客情報に個人情報を含むなど、賠償などリスクあり、経済的影響が存在すると考えます。 また、一度流出した顧客情報は時間遡及とため、回復困難性は比較的高いと考えます。 （4）経済的影響：小　回復困難性：小 理由：設定情報が漏えいしても直接は経済（企業経営など）に影響は小さいと考えます。 また、SWアップデートなどでホリスクは回復可能と考えます。 上記のようにリスクを経済的影響と回復困難性の観点でマッピングする方法が適切と考えます。	セキュリティ対策を検討する際には、機器・システムが利用者に提供する付加価値に着目することが重要であり、機器単独で付加価値を提供する場合と、当該機器がシステムに組み込まれて初めて付加価値を提供する場合があると考えています。また、同じIoT機器であったとしても、どのようなシステムで使われるか、システムにおいてどのような役割を持つのか、どのようなスキルを持つ者が使うのか等、その使われる環境等により、課題やインシデントによる影響等が大きく異なることを示すため、本文「3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ」において、機器・システムをマッピングしました。 なお、いただいた御意見も参考に、本文「1-1-2　第2層の位置づけ」を以下のとおり修正いたします。 ・「なお、本フレームワークにおいて機器だけでなくシステムも対象としているのは、セキュリティ対策を検討する際には当該機器・システムが利用者に提供する付加価値に着目することが重要であるところ、センサやアクチュエータを搭載する機器単独で付加価値を提供する場合もある一方、当該機器がシステムに組み込まれて初めて付加価値を提供する場合があるためである。」を追記。 また、本文「3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理」を以下のとおり修正いたします。 修正前「フィジカル・サイバー間をつなぐ機器・システムに潜むリスクのカテゴライズを行う2つの軸として設定することとした。」 修正後「フィジカル・サイバー間をつなぐ機器・システムを当該機器・システムに潜むリスクに基づいてカテゴライズし、マッピングする2つの軸として設定することとした。」
6	1	企業	-	管理者Ａの範囲だけでも、管理者Ｂの範囲だけでも見えない正帰還ループが、管理範囲にまたがって存在することがある。この問題がＩｏＴでは、あらゆる分野に発生するので、正帰還ループ検出、暴走検知、暴走停止の対策機能が必要。	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。
6	2	企業	-	同じ仕組みの多数のＡＩに、ネットワーク経由で同じデータが同時に与えられますと、全部のＡＩが同じタイミングで同じ反応をします。 同じ反応をするＡＩに制御された活動が社会の多くの場所や分野で一斉に同じタイミングで発生しますと、「過負荷によるシステムの停止や破壊」や「バランスの崩壊」が発生します。これは、社会に大混乱や大損失を与えます。したがって、ＡＩに多様性を確保して、ＡＩの一斉動作による破壊やバランス崩壊を防がねばならないということになります。	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。
6	3	企業	-	ＡＩ多様性の確保のためには、同じアルゴリズムや同じ知識を持つＡＩは、分野別に存在できる個数および比率の上限値を設けるという規制が必要でしょう。	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。
7	1	個人	-	「サイバーセキュリティー対策」が重要な構造と、私し個人は思います。例えばですが、「センサー技術、 ネットワーク技術、デバイス技術」から成る「CPS（サイバーフィジカルシステム）」の導入により、「ゼネコン（土木及び建築）、船舶、鉄道、航空機、自動車、産業機器、家電」等が融合される構造と、私は考えます。具体的には、「電波規格（エレクトロリカルウェーブスペック）」及び「通信規格（トランスミッションスペック）」での「回線（サーキット）」の事例が有ります。（ア）「通信衛星回線（サテライトシステム）」における「トランスポンダー（中継器）」から成る「ファンクションコード（チャンネルコード及びソースコード）」のポート通信での「DFS（ダイナミックフレカンシーセレクション）」の構造。（イ）「電話回線（テレコミュニケーション）」における基地局制御サーバーから成る「SIP サーバー（セッションイニテーションプロトコル）」の構造。（ウ）「インターネット回線（ブロードバンド）」におけるISPサーバーから成る「DNSサーバー（ドメインネイムシステム）」の構造。（エ）「テレビ回線（ブロードキャスト）」における「通信衛星回線、電話回線、インターネット回線」の構造。具体的には、「方式（システムスペック）」での「回線（サーキット）」の事例が有ります。（ア）「3G（第3世代）」における「GPS（グローバルポジショニングシステム）」から成る「3GPP方式（GSM方式及びW-CDMA方式）」の構造。（イ）「4G（第4世代）」における「LTE方式（ロングタームエボリューション）」から成る「Wi-Fi（ワイアーレスローカルエリアネットワーキング）」の構造。（ウ）「5G（第5世代）」での「NR（New Radio）」における「MCA方式（マルチチャンネルアクセス）」から成る「DFS（ダイナミックフレカンシーセレクション）」の構造。具体的には、「情報技術（IT）」及び「人工知能（AI）」での「回線（サーキット）」の事例が有ります。（ア）クラウドコンピューティングでは、「ビッグデータ（BD）」から成る「データーベース（DB）」の導入により、ITネットワークの構造。例えばですが、ファイアーウォールにおける強化では、ルーターとスイッチを挟み込む様に導入する事で、「クラウド側（プロバイダー側）←ルーター⇔ファイアーウォール⇔スイッチ→エッジ側（ユーザー側）」を融合する事で、ハードウェアーの強化の構造。（イ）エッジコンピューティングでは、Web上における「URL（ユニフォームリソースロケーター）」での「HTML（ハイパーテキストマークアップランゲエッジ）」から成る「API（アプリケーションプログラミングインタフェース）」に導入により、「HTTP通信（ハイパーテキストトランスファープロトコル）」における暗号化によるソフトウェアーでの「HTTPS（HTTP over SSL/TLS）」の融合により、AIネットワークの構造。具体的には、「サイバー空間（情報空間）」及び「フィジカル空間（物理空間）」での「回線（サーキット）」の事例が有ります。（ア）「サイバー空間（情報空間）」では、「SDN/NFV」における「仮想化サーバー（メールサーバー、Web サーバー、FTP サーバー、ファイルサーバー）」から成る「リレーポイント（中継点）」での「VPN（バーチャルプライベートネットワーク）」が主流な構造。（イ）「フィジカル空間（物理空間）」では、「AP（アクセスポイント）」が主流な構造。要約すると、「ボット（機械における自動的に実行する状態）」による「DoS攻撃」及び「DDoS攻撃」でのマルウェアーにおける「C&Cサーバー（コマンド及びコントロール）」では、「LG-WAN（ローカルガーブメントワイドエリアネットワーク）」を導入した「EC（電子商取引）」の場合では、クラウドコンピューティング及びエッジコンピーティングにおける「NTP（ネットワークタイムプロトコル）」の場合では、「検知（ディテクション）⇒分析（アナライズ）⇒対処（リアクションメソッド）」での「サイバーセキュリティー対策」が重要と、私は考えます。	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。
8	1	団体	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求 3-3-2 第2の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求	サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされるリスクに着目し、これらリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示する取組みに、我々、制御機器業界も賛同します。 ■該当箇所 3-3-1 第1の観点：運用前におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求 3-3-2 第2の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求 〈意見内容〉 制御機器製造メーカである当業界にとって、関連のある観点であり、今後の取組みの中で、国際標準（IEC62443シリーズなど）の要求を包含する、日本発のフレームワークとなる事を期待	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。 なお、いただいた御意見も参考に、「5. リファレンス」を追加し、本フレームワーク作成にあたり参照した規格等の文書を記載いたします。
8	2	団体	3-3　求められるセキュリティ・セーフティ要求の整理 3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ	サイバー空間とフィジカル空間をつなぐ新たな仕組みによってもたらされるリスクに着目し、これらリスクに対応するセキュリティ・セーフティ対策の類型化の手法を提示する取組みに、我々、制御機器業界も賛同します。 ■該当箇所 3-2-3 フィジカル・サイバー間をつなげる機器・システムのカテゴライズ 3-3 求められるセキュリティ・セーフティ要求の整理 〈意見内容〉 回復困難性と経済的影響の度合いとで機器・システムをカテゴライズし、そのカテゴリに応じて求められるセキュリティ・セーフティ要求の観点（セキュリティ・セーフティを確保するための手法）を整理されていますが、同じ機器でも使用形態や用途によってマッピング先が異なるとの記載がある通り、今後のユースケースの整理を通して、マッピングやカテゴライズ手法の指針やガイドラインなどの整備が必要	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等での議論を踏まえた上で、引き続き検討してまいります。
9	1	団体	-	全体的な印象として、セーフティ観点(安全性)に対する分析方法や基準などが抜けている印象である。また、第1層と第3層との関連性が見えないため、第2層のセキュリティ・セーフティの定義に漏れがあるように思える。フィジカル・サイバー空間を正確に転写する機能の信頼性だけをフォーカスするだけでなく、対象機器のとなるサプライチェーンや安全性の要求、セキュリティゴールを明確にできるフレームワークにならないと全体的なフレームワークとして成り立たないように思える。 リファレンスとするアーキテクチャの定義が明確にないため、IoTのリファレンスアーキテクチャを明確にすることが必要と考える。NISTのベースラインを参考としていると考えるが、目的、目標とする部分を明確にする必要があると考える。 抽象度の高いフレームワークであり、中身についてはこれからユースケースを集めて有用性を高めていくとのことであるが、ユースケースの具体的な記述方法が提案されていないので、活用可能性が見こない。ユースケースの共有はどのようにしてすすめるかなど、各企業や各団体との連携方法なども定義が必要に思える。 第1軸にて「回復困難性の度合い」の概念が抽象化し過ぎているため、フィジカル空間に対することと、サイバー空間に対することとが一まとめにされており、各々の空間で軸を分けた軸の定義を行い、安全性の要求とセキュリティゴールについての定義を細分化することが必要と考える。この部分は、フィジカル空間を生み出すための第1層との関係性が重要な要素と思える。 「経済的影響の度合い」においては、モノを作る部分、モノを動かす部分、モノを運用する部分の３つの視点でサプライチェーンを見える化し、サプライチェーンにおけるリスク分析を実施するべきと考える。金銭的換算においては、事例が必要となるが事例や定義をどのように定義していくのか？の指針の定義が欲しいと考える。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的な活用方法については、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。なお、ご指摘いただいている第1層から第3層の関連性や対象機器となるサプライチェーン等は「サイバー・フィジカル・セキュリティ対策フレームワーク」にて整理を行っております。加えて、サプライチェーンにおけるリスク分析についても「サイバー・フィジカル・セキュリティ対策フレームワーク」に記載しておりますので併せてご確認ください。
9	2	団体	3-3　求められるセキュリティ・セーフティ要求の整理	「セキュリティ・セーフティ要求の観点」では、4層に分けられている。その他、社会的なサポート等については、「セキュリティ・セーフティ要求の観点」を包括するような位置づけと考えられ、何故この部分が必要になるのかを説明するべきと考える。もしくは、層の構成上、認定レベルなどを設けて、コスト試算した後に対応する位置づけにする必要があるように思える。	「第4の観点：その他、社会的なサポート等の仕組みの要求」は例えば法制度のような、製造者やユーザだけでは設定できないものや、製造時や運用時全体に影響を与えるものを包含していると考えております。 本フレームワークでは上記の様な制度設計を行う者も対象読者になり得ると考えており、「第4の観点：その他、社会的なサポート等の仕組みの要求」を設定したため、原案のとおりとさせていただきます。
9	3	団体	3-3　求められるセキュリティ・セーフティ要求の整理	「セキュリティ・セーフティ要求の観点」においては、運用前の部分と運用中の部分の関係性の明確化が必要に思える。通常、機能安全においても、セキュリティ設計においても、リスク分析を行う場合に想定されるユースケースから、被害や事故、損失を分析した上で、事象に対する対策を想定し、検討する事が一般的である。運用するシステムの想定が曖昧であり、利用・運用のユースケースの洗い出しがあって、運用前の確認要求となるような層の定義が必要に思える。セキュリティの場合、悪意ある第三者からの攻撃によって新たなインシデントが発生することも考えられ、運用時の対応に関しての定義が必要に思える。	運用前、運用中など、ライフサイクルのステージの整理の仕方は、業界や対象とする機器・システムによって異なると考えられ、各産業界や機器・システムの性質等を踏まえて、ステージを整理し、各ステージで求められるセキュリティ・セーフティ要求を検討していただくことになると考えております。

ID	No	提出者	該当箇所	御意見の概要	御意見に対する考え方
9	4	団体	3-3-4　第4の観点：その他、社会的なサポート等の仕組みの要求	運用者に対する確認要求については、サービスを提供する人なのか？オペレータなのか？どちらを想定しているのかが明確に見えない。また、運用中の部分から運用者を特に外している理由が明確でないため、定義が曖昧なように見える。 305-308に記載された部分として、使用者の定義があるが、使用者と想定しているのは、サービス利用者なのか？サービス提供者なのか？が明確になっていないと思われる。	本フレームワークでは、運用者とは主にオペレータを、IoT機器・システムを使用する者とは利用者を想定しておりますが、例えば、システムを所有している者が、システムの運用を他の者に委託しているケースなど、様々なケースが考えられます。ステークホルダーの関係が整理されることが重要と考えております。 なお、いただいた御意見も参考に、本文「3-3-3 第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求」を以下のとおり修正いたします。 ・「なお、ここでいう運用者には、サービス提供者のようなシステムを直接操作するわけではないものも含みうる。」を追記 ・「使用方法等の情報を提供する際には、どのようにしてその情報へのアクセシビリティを向上させるかも検討する必要がある。」を追記 ・「この例のように、複数のステークホルダーが関係するリスクへの対処は、複数の観点から行えることから、関係するステークホルダーにおける負担について、各ステークホルダーが機器・システムのリスクに関連する情報を可視化・共有する等の方法を通じて、総合的に検討し、ステークホルダー間で合意する必要がある。したがって、単独のステークホルダーが全ての要求に対処する必要はなく、また、ある観点内であらゆるケースで必須に求められる具体的な要求の規定を一律に求めることは困難である。」を追記
9	5	団体	3-3-4　第4の観点：その他、社会的なサポート等の仕組みの要求	「セキュリティ・セーフティ要求の観点」部分で最も抽象的となっている部分として、想定ユーザや想定ケースが抜けている点である。運用前の部分については、製造メーカーを想定していると思われるが、運用中の部分は、製造メーカーでないケースが想定されるため、運用中の部分がどのようなサプライチェーンであるかを明確にし、運用ケースの定義が必要と考える。	いただいた御意見については、ユースケースの策定も含め、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
9	6	団体	3-3　求められるセキュリティ・セーフティ要求の整理	誤解を避けるために“セーフティの確保”の“セーフティ”が“セキュリティ・セーフティ”の意味であれば“セキュリティ・セーフティ”にしてほしい。 （工場、社会インフラ等の安全の意味であれば“安全”とすべきと考える。）	本フレームワークでは「安全性」を「セーフティ」という用語で統一しております。パブリックコメントを募集した時点での107行目は、セーフティとセキュリティの組み合わせが重要である旨を本文中で初めて述べている箇所であることから「セーフティ」を単独で用いているため、原案のとおりとさせていただきます。
9	7	団体	3-2-3　フィジカル・サイバー間をつなげる機器・システムのカテゴライズ	"フィジカル・サイバー間をつなげる機器・システムのカテゴライズ"とありますが、機器、システムの粒度を明確にしないとカテゴライズを明確にするべきだと考える。	どのような機器・システムを想定し、どのようにカテゴライズを行うかはIoT機器の多様性等によって異なるものであり、産業界等での議論を踏まえた上で、引き続き検討してまいります。
10	1	企業	-	アセスメントスケール（評価尺度）には、セキュリティ視点のものはあるが、そこにセーフティ視点を取り入れなさい、という考え方指針を示したものだと理解。本案は、コンセプトや課題の提案にとどまっているように思われ、具体的な対策をまとめている部分が読み取れませんでした。このフレームワークの発行後、なんらか具体的なメソッド、基準などを出していただけると開発者は助かる。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
10	2	企業	-	セーフティとセキュリティの規格・ガイドラインをサーベイして、特徴比較していただければ、さらに参考になります。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
10	3	企業	3-2-3　フィジカル・サイバー間をつなげる機器・システムのカテゴライズ	3-2-3「フィジカル・サイバー間をつなげる機器・システムのカテゴライズ」 「同じ機器でも利用形態などによりマッピング先が異なりえることに留意する必要がある。」とあるのですが、マッピング先が異なったら何を考慮しないければならないのか、についても示唆いただきたい。	一般的に、マッピング先により必要なセキュリティ・セーフティ要求が異なり得ると考えられますが、具体的にどのような要求が必要かについては、産業分野等により異なるものであり、産業界等での議論を踏まえた上で、引き続き検討してまいります。
10	4	企業	3-3　求められるセキュリティ・セーフティ要求の整理	「3-3 求められるセキュリティ・セーフティ要求の整理」 第1の観点～第４の観点までが記載されています。そのほかに、システムの利用者・選定者はどのような観点で何が必要なのかを検討するポイントを記載いただきたい。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのようなステークホルダーが関連するかについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。 なお、いただいた御意見も参考に、本文「3-3-3 第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求」を以下のとおり修正いたします。 ・「なお、ここでいう運用者には、サービス提供者のようなシステムを直接操作するわけではないものも含みうる。」を追記 ・「使用方法等の情報を提供する際には、どのようにしてその情報へのアクセシビリティを向上させるかも検討する必要がある。」を追記 ・「この例のように、複数のステークホルダーが関係するリスクへの対処は、複数の観点から行えることから、関係するステークホルダーにおける負担について、各ステークホルダーが機器・システムのリスクに関連する情報を可視化・共有する等の方法を通じて、総合的に検討し、ステークホルダー間で合意する必要がある。したがって、単独のステークホルダーが全ての要求に対処する必要はなく、また、ある観点内であらゆるケースで必須に求められる具体的な要求の規定を一律に求めることは困難である。」を追記
11	1	企業	1-1-2　第2層の位置づけ	従前の詳細な制御マッピングではなく、IoT システムの非技術的リスクを評価するための仕組みに焦点を移したフレームワークへの変更は、IoT アプリケーションの設計者および運用者にとって有用な参照モデルになると考えられます。 「1-1-2：第2 層の位置づけ」（100-101 行目） 一般的に、物理的分離は、組織の負担を増加させ、機器の有用性を制限する規範的な制御方法であり、セキュリティ設計上の利点とのバランスを考慮する必要があります。 100～101 行目の事例で触れられている「設置区域管理」について、物理的分離を指すものと混同されないようにする必要があります。本事例においては、重要なIoT 機器を保護するため、組織内のIoT システムの設計者と運用者が、当該機器が設置されている環境条件に基づいて追加の物理的セキュリティ制御対策を検討する必要がある旨を記述すべきです。物理的分離のみに焦点を当てたコントロール策は、63 行目から65 行目で強調されているIoT 環境条件の動的かつ多面的な性質を考慮すると、必ずしも効果的または効率的なアプローチとはなりません。 さらに、この事例には、データの整合性を確保するための仕組みをプロセスに含める際に考慮すべき事項も加えるべきです。許容可能なパラメーター内でデータの整合性を確保するための動的、効果的かつ効率的なメカニズムは、データを収集・処理するアプリケーション内の第3 層に実装されるのが最適と思われます。フィジカル空間でIoT 機器により収集され、アナログからデジタルへ転写されたデータの正確性を保証することはできないからです。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。なお、ご指摘の通りパブリックコメントを募集した時点での100行目より101行目にて言及されている設置区域管理については、CPSF内のIoT機器の重要性等に応じて追加の物理的セキュリティ制御対策等を検討する必要があることを紹介するものです。また、データの整合性が重要であることはご指摘の通りですが、データの整合性を確保するための検討は、『『第3層：サイバー空間におけるつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース」にて引き続き検討を行う予定です。
11	2	企業	1-2　本フレームワークの目的	「1-2：本フレームワークの目的」（121-122 行目） 本フレームワークにおいて、アプローチの一貫性がソリューションを拡大する上で重要な要素である一方で、データを収集、使用、または処理しているアプリケーションの実際のセキュリティ要件を著しく改善しない可能性があることが認識されるべきです。我々は、複数の実装にわたって行われる対策の一貫性よりも、懸念される脅威に対処するアプリケーション固有のセキュリティ要件の特定を優先すべきと考えます。	本フレームワークは、画一的なセキュリティ対策を求めるためのものではなく、各産業分野において別々のプロセスを経て設定された対策がフラグメンテーションを起こさないことを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
11	3	企業	3-2-2　第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）	「3-2-2 第2 軸：発生したインシデントの経済的影響の度合い」（213-221 行目） 本フレームワークにおいて、「人命/安全」より広範な社会的行動への影響を考慮すること、IoT システムの設計と使用が個人やグループの行動をどのように変化させるかについて考慮することが重要と考えられます。例えば、攻撃者は、ユーザーがフィッシングまたは悪質なWeb サイトにアクセスするQR コードをスキャンするよう誘導し、定期的にユーザーから情報を取得したり取引を実行させたりします。この例が示すように、ユーザーの身体に危害を及ぶことはないにしても、生命と安全にリスクをもたらす行動につながる場合があります。機器がどのように人の行動を変え、人命と安全へのリスクを増大させるかを認識し、そうした考えをセキュリティモデル組み込むことができなければ、システムの悪用が可能になります。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。なお、本フレームワークでは人命/安全を「第1軸：発生したインシデントの影響の回復困難性の度合い」にカテゴライズしました。また、プライバシーを例示したように、「第1軸：発生したインシデントの影響の回復困難性の度合い」及び「第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）」のどちらにもカテゴライズされるものもあると考えられます。具体的にリスクに基づいて機器・システムがどのようにマッピングされるかについては、検討される必要があると考えています。
11	4	企業	3-3-4　第4の観点：その他、社会的なサポート等の仕組みの要求	「3-3-4 第4 の観点：その他、社会的なサポート等の仕組みの要求」（296-303 行目） 本フレームワークにおいて、既知及び新たに発生するインシデントの両方を把握して対応できるよう、対応と回復の仕組みを準備する必要がある旨を規定すべきです。 本セクションにおける議論の焦点を、極端な大規模インシデントから様々なインシデントシナリオを検証する仕組みに拡大することで、本フレームワークによって、組織、ユーザー、および運用者が適切に準備を進めることが可能になると考えられます。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。ご指摘のとおり、対応と回復の仕組みは重要であり、それらの仕組みが第3軸における「第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求」より「第4の観点：その他、社会的なサポート等の仕組みの要求」までの観点に含まれれる必要があると考えています。なお、具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。

ID	No	提出者	該当箇所	御意見の概要	御意見に対する考え方
12	1	個人	-	私たちはサーバに依存した考え方を根本的に見直し、物理的なネットワーク分離環境を構築するのではなく、現在のインターネット環境で企業間または企業とユーザー間を安心してご利用可能とする技術を提供します。 現状の通信は秘匿化でSSL/TLSを使用し、提供側(サーバ側)を証明書で安全を担保をしており、利用者特定では多要素認証と多段階認証を組合せた運用です。しかし、この様な秘匿化の実装では、フィッシングサイト等ではDNSの乗っ取りやニセURLに誘導して、実際のIDやパスワードを入力させ、偽サイト経由で実サイトに値を入力する仕組みが行われます。 そのため、多段階認証をしていても、正しい値を利用者本人が偽サイト経由で実サイトに入力してしまうので、防ぐのが非常に困難です。 弊社は、インターネット上で複数の経路を持ち通信経路が断たれても自律的に新しい通信経路を開き、常に複数の通信経路保持を実現する「HYDRA」と命名した技術を保有します。 このHYDRAは、複数の通信経路上で電子副符により分散配置したデータをハッシュグラフで管理します。 HYDRAの要素技術 ■多重因子三点ルーティングテクノロジー ・インターネット上で用意されたHYDRAのノード間の通信は多重因子による経路の多重化により、理論的な経路が拡散されます。 そのため、通信障害などで経路が塞がれても自律的に最適な経路のノードで通信経路を確保し、強靭な高速通信を実現します。 ・HYDRAのノードは1親等以上のつながりを持たず探索は１親等を超えて直接探索が行えません。 従って、遡りが行えない仕組みの為、なりすましを防ぎます。 ・ハッシュグラフ技術の利用 インターネットが誕生した当時から使われているピア・ツウ・ピア通信の仕組みをハッシュグラフの技術を使い膨大な量のデバイスやそれを操作するユーザーを前提に高速に且つ高いセキュリティーとプライバシーを実現するようにアップデートしました。 ハッシュグラフは分散型台帳テクノロジー（DLT）で、ビットコインのブロックチェーン上に記帳していく手法と異なり、高速、セキュリティ、公平性といった特徴を持つアルゴリズムです。 ・電子副符の採用 秘密分散法を応用した暗号技術の一種です。 一般的な暗号化はパスワードを破られると強力な暗号も破られますが、秘密分散は破られない暗号化と言えます。 例えば、6754という数字を分散する場合、足し算を使い7293と9461（=16754）に分割し、下四桁のみが暗号化された数字とします。 実際には排他的論理和を使用します。 HYDRAは、理論的に多重化された経路の上で、データの電子副符に基づいた秘密分散処理が行われ、強靭な高速ネットワーク上で秘匿性の高い通信を実現します。 弊社は従来のセキュリティシステムまたは専用回線、VPNと異なり、インターネットでセキュア通信を可能にする技術です。 昨今のサイバーセキュリティ対策では、複数の要素が必要と思われますが、弊社は、その中の一部としてお役に立てられると考えております。	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。
13	1	企業	-	セキュリティ・セーフティに於いて、現行のサービス提供形態(中央集権型)から自律分散型サービスへの遷化にも対応するセキュリティ対策を検討すべきと考えます。その為には、今までのセキュリティ対策だけでなく新たな技術の参画も可能とするフレームワークとして頂きたいと思います。 そこで、弊社が開発したセキュリティ対策について簡単に記載いたします。 従来のセキュリティ技術ではサイバー攻撃を防ぐ事が困難でしたが、弊社のセキュリティ保護機構はOSより前に立ち上がり、OSの背後であらゆるサイバー攻撃からコンピュータをリアルタイムで保護を行うという、まったく新しい仕組みを実現した技術です。 この技術により、古い資産で運用を行っている企業様のシステム環境でもサイバー攻撃を防ぐ事が可能です。 弊社の様なセキュリティに特化した会社でなければ大手企業様では開発が困難な技術であり、海外製品ではなく弊社が独自で開発した日本の技術です。 是非、紹介を行う機会を頂きたいと存じます。 【株式会社ETRON INT-Rの紹介】 ■不可能を可能にした技術 OSの機構をOSの外部から保護し、全ての動きを監視・保護する。 発想自体はシンプルですが、実際にはCPUやOSの仕様を非常に深いレベルで理解し、実装する技術が必要となります。 実は、これまで多くの技術者・研究者が挑戦してきたと言われていますが、世界で初めて、ETRON社が実用化に成功しました。 全く新しいセキュリティ保護機構、「INT-R」の特徴を、大きく三つご紹介します。 まず、INT-Rはコンピュータの起動直後、OSよりも先に動作を開始します。そして、OSからは見えないメモリ領域を確保して、自らの動作環境を構築します。その上で、残りのメモリ領域をOSに割り当てて、起動シーケンスを実行していきます。 不正プログラムはOS上で動きますので、INT-Rが攻撃されることは絶対にありません。 INT-RはOSの起動からシャットダウンまで監視を続け、コンピュータを確実に保護します。 このようにして、INT-RはOSの外部から保護機構を提供するのです。 次に、INT-Rは、コンピュータ上の全ての処理を、CPUに対する命令単位で把握し制御します。 この処理は、Intelのvt-xx環境を使って行われ、ハードウェアのエミュレーション等もありませんので、非常に高速に行われます。監視対象はOS・アプリケーションによる処理、CPUによる処理、そしてOSやCPUの環境設定値に対する書き込みや読み込みなどです。 最後に、INT-Rは、CPUの処理命令について、インテリジェンスを提供します。実行されているカーネルの処理、プロセス、デバイスのI/O、通信などをモニタリングしながら、ユーザーによる正規の処理なのか、第三者による不正な処理なのかを判別し、不正なものだけを確実に止めることができるのです。 INT-Rの保護ポリシーは、攻撃者の視点から見たコンピュータの不正な侵入経路を、全てブロックしています。これにより、たとえ未知の不正なプログラムであっても、確実に止めることができるのです。 ■INT-R [INT-R保護モデル] あらゆるサイバー攻撃からコンピュータをリアルタイムで保護します。不正なプログラムは、自身が実行可能な環境を作る過程で必ずCPUやOSを不正に操作したり、管理者権限を奪ったり、新しいプロセスを起動して外部のサーバと通信したりします。 これは、プログラムが既知であるか未知であるかに関わらず、すべてに共通しています。 「INT-R保護モデル」は、プログラムからの処理要求をCPUの命令レベルで監視し、不正な処理の要求があったときのみ、その処理を実行することなく、該当するプロセスを停止します。 [INT-R監視モデル] 保護モデルと同じように動作しますが、プログラムを停止させることなく、ログを出力します。このモデルを使えば、保護モデルの導入に先立って、お使いの業務用アプリケーションがETRONの設定したルールに抵触しないかどうかを調べることができます。 [INT-R解析モデル] 保護モデルよりもさらに詳細なログを出力します。このモデルを使えば、特定の不正なプログラムの挙動や、コンピュータの動作状況を非常に深いレベルで解析することができます。	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。なお、本フレームワークは新たなセキュリティ対策技術を排除するものではありません。
14	1	企業	3-2　フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理	○P7 168～181行目 サイバー間をつなげる機器・システムのセキュリティ対策を検討する上で、共通項を抽出することによって抽象化した2軸でシンプルに整理するアプローチは、とっかかり易さや汎用性のメリットがある半面、曖昧過ぎてどの業種にとっても使い難く活用されない可能性も併せ持つと思います。そこで、従来の安全施策を講じてなお伴う脅威を、読者が適切かつ「基本的共通基盤」として認識できる指標、あるいは手引きがあると理解が進むと思います。 ・理由 インシデントが発生した際の回復困難性や経済的影響の度合い、特に重要インフラは社会的責任を、工場などでは人命を最優先で保護すべきことなどを考慮した上で、管理すべき機器、マニュアル策定を日常的に行っていると思います。他方、回復困難性や経済的影響度合いの低い機器・システムは組織から見落とされがちで、それに伴い脆弱性を多く保有している可能性があり、これら脆弱な部分を攻撃者が標的として組織内部へと侵入することを考慮すると、むしろ、P10 図5の左下に位置する機器・システムに対し重厚な対策が必要になるケースも想定されると思います。 IoTの普及により懸念点となることは、従来の安全対策を講じたうえでなおサイバー攻撃の脅威に晒され、何重にも行っているはずの安全対策が機能しない可能性が生じることであり、これをもって重点的な対策を施すべき機器・システムを考慮してカテゴライズする観点も必要になると思います。特に想定読者が、IoTを活用して新たな仕組み・サービスを実現・開発・管理・享受する者ならば、その多様的な脅威を体系的に把握可能な指標をフレームワークとして提示することで、脅威に対する認識の足並みを揃えることも一案と思います。そのため、第２層におけるセキュリティ上の課題は一様ではないことは前提としつつも、P4で述べられているような複数の事例から見て取れる脅威における共通項を抽出・抽象化し、カテゴライズの指標として採り入れる要素があっても良いと思います。（例：外的接点の増加度（完全なクローズド環境からつながることのリスク）、機器間の連鎖・依存度合い（第2層における改ざん・完全性喪失や、一つの機器・システムに依存することによる信頼性欠如のリスク）、メンテナンスの困難性（脆弱性を解消できないリスク）など）	本フレームワークを有効に活用していくためには、ユースケースの整理が必要と認識しております。今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理してまいります。
14	2	企業	3-2-3　フィジカル・サイバー間をつなげる機器・システムのカテゴライズ	○p9 223～247行目 2軸マッピングでの分析について3段階の区分をより明確に読者につたえるため、事例の提示があると理解しやすいと考えます。 ・理由 システムにおける経済的影響の度合いが低く、発生したインシデントの影響の回復困難性が高い事象としては、運用中に発生した低価格なIoT機器の破損による一部機能の毀損などが考えられる。軸の提示に加えて、他のそれぞれの象限について該当する事例を記載いただけるとカテゴライズによる整理の助けになると考えます。	本フレームワークを有効に活用していくためには、ユースケースの整理が必要と認識しております。今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理してまいります。
14	3	企業	4.　本フレームワークの活用方法	○P14 334～337行目 ユースケースの整理・蓄積において、手法や内容のブラッシュアップのみではなく、人・組織間における連携・統制・体制などにも着目頂ければ、主に新たな仕組み・サービスを実現・管理する読者にとって参考になると思います。 ・理由 現状、ユースケースの整理・蓄積にあたっては、カテゴライズ手法の洗練やセキュリティ・セーフティ要求の観点・内容を比較できる環境整備について述べられていますが、多くの工場ではこれらIoTの活用における運用・対策検討・責任範囲について、所謂、IT（情報技術）部門、とOT（運用技術）部門どちらに比重をおくのか、または協業することが効率的かつ望ましいのか、という点も悩ましいと思います。第1・2軸によるカテゴライズも、第3軸のセキュリティ・セーフティ要求の達成も組織の一部門だけ関われば良いわけでは無く、さらに利用の停止やや廃棄の際の留意事項まで含めて、組織内における部門間連携例などについてもユースケースとして整理・蓄積された情報として可能な限り提示頂ければ、そこから学べる点・参考にできる点が多くあると思います。	本フレームワークを有効に活用していくためには、ユースケースの整理が必要と認識しております。今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理してまいります。

ID	No	提出者	該当箇所	御意見の概要	御意見に対する考え方
15	1	個人	-	不適切に観念的であると思われた。 モデル化に失敗しているのではないかと思われる。 なお、通常、第3層にサイバー空間におけるつながり、第2層にフィジカル空間とサイバー空間のつながり、を取るのであれば、第1層にはフィジカル空間での出来事、のようなものを取るのが通常と思われるが、ここで企業間のつながり、を取ってきているのは、どうも理系ならざる者による発想が強いものと疑われたが、そこに企業間のつながりを置くのは不適切であるように思われる。（全体的に） なお、11頁目の図6について、どうも上位層に「その他、社会的なサポート等（保険加入義務等）」「運用者に対する確認要求（ライセンス等）」があるのが問題と思われる。機器・システムが適切である事こそが重要であるはずであるが、上位層に置かれたそれらはシステムの適切性に全く関係が無いからである。 また、途中で出てくる図のように、1次元、2次元、3次元の図上のマッピング、を行っていくのではなく、要件からの求められる対応の組み合わせ、によっての考慮を行っていくべきであると考える。そしてその様な考え方の推奨を行っていく方が望ましいと考える。（要するに、要件・要求・要素の分析であるが。）（要するに、ライセンスの有用性が高い事務であればライセンスについて重要視し、運用するCDNシステムについて高い可用性が必要とされる場合は高可用性とその保証がなされたシステムを注文し、社内恥にすべきシステムかつ保険の設定出来ないものについては自前でシステムに冗長性を持たせるようにする等、そしてそれらにおける使用技術・製品・方式のメリット・デメリットについての分析をする等、であるが。） 1次元、2次元、3次元の図、ではそのどこかにマッピングされる、という事すなわちそれら全ての軸のどこかにマッピングされる、という事から逃れられず（そして11頁目の図6の様な図は不適切である。保険やライセンスを求めるのはこの図6に示されるようになっていない（この図は費用についてもリスク分析についても捨象しているものと認識される。）。）、また3次元より高い次元にするのは困難性がともなうのであるが（3次元でも既に困難であるが。）、要件からの求められる対応の組み合わせであれば、何次元（何要件）でも可能だからである。 まぁちょっと、当方としては、今回の提示のあったフレームワークは、検討の際に用いたくないものと思われたが（意見を行う事にも難がある様な不適切に観念的なものに思われた。）、ゼロベースでの再考を行っていただきたいと考える。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
16	1	政府機関	-	本フレームワークは、IoT関連リスクを分析するための統合的なアプローチを効果的に促進するものである。サイバーセキュリティと物理セキュリティを別個に検討するのではなく、複数のドメインにまたがる複数のリスクを分析することを通じて、本来なら見逃されていたであろう問題を特定できる（行番号100-103及び350-354）。同一の機器であっても、利用方法が異なっている場合や、適用される物理セキュリティ上の考慮事項が異なる環境に展開される場合には、リスクは明らかに変化する。 我々は、「第2層」と呼ばれるフィジカル空間とサイバー空間の交差点に特別な注意を払う必要がある点に賛同する。 消費者IoTセキュリティでは、機器がセーフティ関連機能（例：煙探知、ドアロック）を実行する場合に、「第2層」の観点が特に重要となる。 これは、英DCMS(デジタル・文化・メディア・スポーツ省)によるCode of Practice for Consumer IoT Security のガイドライン 9（"Make Systems Resilient to Outages"）およびETSI TS 103 645/EN 303 645の関連セクションにも反映されている。	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。
16	2	政府機関	-	我々は本フレームワークの目的を理解したい。例えば、貴省が進めたいと考えている政策的な介入に関する情報提供を意図しているのか。あるいは、産業界がリスク管理に役立てるために利用することを意図しているのか。	本フレームワークの目的は、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することで、産業界での議論を促進することです。 いただいた御意見も参考に、本文 1-2「本フレームワークの目的」を修正いたします。 ・「IoT機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。」を追記
16	3	政府機関	-	貴省は、ETSI規格やISOのIoTセキュリティ規格（27402）等の他の国際規格やガイドラインに、本フレームワークがどのように適合していると考えていますか？	既存のIoTセキュリティに関する標準は、主に機器・システムに対して、具体的な要求を求めるものと認識しています。しかし、本フレームワークの目的は、具体的な要求を定めるためではなく、セキュリティとセーフティを併せて考えるべきこと、また、機器だけでなく運用者や社会制度についても合わせて検討する必要があるのではないか、という議論のための問題提起にあります。 なお、いただいた御意見も参考に、「5. リファレンス」を追加し、本フレームワーク作成にあたり参照した規格等の文書を記載いたします。
16	4	政府機関	-	本フレームワークの実際の適用方法（例：消費者向けIoT分野）に関するケーススタディを共有できないか。	本フレームワークを有効に活用していくためには、ユースケースの整理が必要と認識しております。今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理してまいります。
16	5	政府機関	3-3　求められるセキュリティ・セーフティ要求の整理	第3軸（セキュリティ・セーフティ要求の観点）を「製品ライフサイクル段階のためのリスク低減」に改名できないか。	いただいた御意見について、製品のライフサイクルの各ステージにおけるリスク軽減は重要であり、「第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求」や「第2の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求」に包含されると考えています。しかし、第3軸における「第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求」及び「第4の観点：その他、社会的なサポート等の仕組みの要求」では、運用者の適格性や、その業界における社会制度等についても対象としており、製品のみを対象としていないため、原案のとおりとさせていただきます。
17	1	企業	1-1-2　第2層の位置づけ	103行目：…盗難、紛失のリスクを考慮した対策の実施が必要。 ＞盗難、紛失、複製（clonig）等のリスク	いただいた御意見を踏まえ、本文「1-1-2 第2層の位置づけ」を以下のとおり修正いたします。 修正前「盗難、紛失のリスクを考慮した対策」 修正後「盗難、紛失等のリスクを考慮した対策」
17	2	企業	1-1-2　第2層の位置づけ	103行目：…盗難、紛失のリスクを考慮した対策の実施が必要。 ＞そのため、各IoT機器にセキュリティ/セーフティアンカーを追加して、体系的な認証メカニズムを考慮することが重要である。これが、セキュリティ・バイ・デザインによる相互接続性を提供する唯一の方法である。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような方法で信頼性を確保するかについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
17	3	企業	1-2　本フレームワークの目的	115-117行目：今後、IoTの活用の拡大に伴い、それぞれの分野の特殊性・多様性を踏まえて、使用分野ごとに個別・具体的なIoT機器・システムに対して実際のセキュリティ対応が進んでいくことになると考えられる。 ＞適用可能なセキュリティ基準（存在する場合）もまた様々である。例えば、工場の場合はIEC 62443、一般的なセキュリティの場合はFIPS 140-2/3、コモンクライテリアなどを適用可能である。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
17	4	企業	1-2　本フレームワークの目的	117-121行目：その過程において、サイバー空間とフィジカル空間をつなぐ機器・システムのセキュリティ・セーフティに関して、包括的に課題を捉える統一的な手法が欠如しているため、それぞれの分野/業界において別々の検討プロセスを経て、独自のセキュリティ・セーフティ対策等が設定されることが懸念される。それぞれの対応策に不整合が生じれば、社会として新たな仕組みを受容・管理していくためのコストが増大する恐れがある。 ＞したがって、産業向けと消費者向けの世界では異なる機能を具備し、信頼性の高いセキュリティ/セーフティアンカーを備えた機器レベルから始めるセキュリティ/セーフティの共同アプローチが必要である。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような方法で信頼性を確保するかについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
17	5	企業	2.　本フレームワークの想定読者	146-147行目：IoTを活用してサイバー空間とフィジカル空間をつなぐ新たな仕組み・サービスを実現しようとする者 ＞購買戦略とサプライヤー評価を適合させることが目的となる。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
17	6	企業	2.　本フレームワークの想定読者	148行目：そのような新たな仕組み・サービスで活用されるIoT機器・システムの開発を行う者 ＞機器設計に適切な方法を実装すること（セキュリティバイデザイン）が目的となる。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
17	7	企業	2.　本フレームワークの想定読者	151行目：そのような新たな仕組み・サービスを受ける者 ＞適切なセキュリティレベルが実装されているか、適切なセキュリティ認証/保証が含まれているかどうかを検証することが目的となる。	いただいた御意見は、記載内容の修正に当たって参考にさせていただきます。
17	8	企業	3-2-3　フィジカル・サイバー間をつなげる機器・システムのカテゴライズ	246-247行目：同じ機器でも使用形態などによってマッピング先が異なり得る。例えば、機器 g と機器 h が同じ機器で異なる使用形態である場合などがあり得る。 ＞ここで説明されるように、正式な文書において明確にこの分析に言及する必要がある。これらの問題を特徴づけるような関連する保護プロファイル（PP）が必要である。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのようなケースでどのような保護が必要か等については、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
17	9	企業	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	265-268行目：フィジカル・サイバー間をつなぐ機器・システムが製造され、実際に利用に供される前の段階で、機器・システムそのものが必要なセキュリティ・セーフティ対策を講じられていること、又は当該機器等の生産者や供給者、検査者、場合によっては生産設備・工場等が必要な能力条件等を満たしていることなどを確認することを求めるものである。 ＞適切なセキュリティを確保するために、セキュリティとセーフティ機能/対策を設計段階という早い段階で実装する必要がある。	いただいた御意見を参考に、本文「3-3-1 第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求」及び図6を修正いたします。 修正前「製造段階等」 修正後「設計・製造段階等」
17	10	企業	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	270-272行目：また、その内容が満たされていることを確認する方法についても、自己適合宣言や第三者による認証など様々な形態があり、求められる確認レベルの専門性や客観性などを踏まえて実際の確認方法が設定されることになる。 ＞セキュリティを保証するために、関連する認証スキーム/標準の使用を一般化する必要がある。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
17	11	企業	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	277-279行目：そのような問題が発生していないかを確認するために、運用開始後に、ライフサイクルやサービス期間も考慮しながら機器・システムを確認することを求めるものである。 ＞したがって、ライフサイクルのすべての段階でセキュリティを適応および管理するメカニズム（セキュリティパラメータのプロビジョニング、更新など）が必要である。最新の攻撃は常に変化しているため、実装されたセキュリティ機能の妥当性を定期的に監視する必要があることに注意すべきである。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。

ID	No	提出者	該当箇所	御意見の概要	御意見に対する考え方
17	12	企業	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	277-279行目：そのような問題が発生していないかを確認するために、運用開始後に、ライフサイクルやサービス期間も考慮しながら機器・システムを確認することを求めるものである。 ＞セキュリティ機能自体が攻撃されたり、誤動作したりする可能性があることを認識し、考慮することも重要である。したがって、ライフサイクルに沿ってセキュリティ機能を更新/管理するメカニズムの実装は必須である。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
17	13	企業	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	291-294行目：例えば、自動車の場合、運転をする者には一定の技術及び知識を持つことを証明する運転免許の取得を求めており、インシデントが発生した場合の影響が大きいものの、社会的に大きな便益をもたらす技術を社会として受容する社会的な仕組みを構築している。 ＞したがって、使用するセキュリティ機能により、ビジネス/運用の改善と説明責任のため、セキュリティ問題のアラームとログを送信できるようにすることが重要である。トレーサビリティが鍵となる。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
17	14	企業	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	337-340行目：したがって、今後、本フレームワークに基づいて、具体的な仕組み・サービスをユースケースとして整理していくことで、IoTが広く活用されるサイバー空間とフィジカル空間が高度に融合した社会におけるセキュリティ・セーフティ対策を適切に実施していく制度的対応の整備を進めていくための基礎的条件を整えて行く必要がある。 ＞セキュリティ対応チームのスコープは、ハードウェア関連のセキュリティ課題にまで拡大する必要があり、特にOTの課題を考慮に入れる必要がある。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。なお、ご指摘の通り、セキュリティ・セーフティ対策を適切に実施するにあたりOTの観点は重要であるため、「『第2層：フィジカル空間とサイバー空間のつながり』の信頼性確保に向けたセキュリティ対策検討タスクフォース」においてはセキュリティ及びセーフティの両面から議論を行っております。
18	1	企業	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	製造段階と運用段階の間にある統合という中間のステージも考慮する必要がある。特に、組込み機器に運用前からインストールされるファームウェアやソフトウェアにはサプライチェーンセキュリティの側面が関連している。多くのIoT機器は、運用前にFPGAなどのプログラム可能なハードウェアから構成されており、運用前の設定やインストールが必要である。これはオンプレミスまたはリモートでベンダによって行われるが、その間、セキュアでないソフトウェアやFWの設定等のセキュリティ上の問題を引き起こす可能性がある。	いただいた御意見を参考に、本文「3-3-1 第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求」図6を修正いたします。 修正前「製造段階等」 修正後「設計・製造段階等」
18	2	企業	3-3-3　第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求	本フレームワーク内における「運用者」という用語のスコープを明確にする必要がある。5Gの登場および公衆回線、プライベート(産業用)回線における差し迫った採用により、消費者IoTと産業用IoTのギャップは小さくなる。これはロジスティクス、輸送、製造等の特定のセクターで特に当てはまる。さらに、クラウドでホストされるIoTアプリケーションの管理フレームワークにAIが導入されることで、ライセンスされた運用者とサービスプロバイダーの明確な定義が必要となる。	本フレームワークでは、運用者とは主にオペレータを、IoT機器・システムを使用する者とは利用者を想定しておりますが、例えば、システムを所有している者が、システムの運用を他の者に委託しているケースなど、様々なケースが考えられます。ステークホルダーの関係が整理されることが重要と考えております。 なお、いただいた御意見も参考に、本文「3-3-3 第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求」を以下のとおり修正いたします。 ・「なお、ここでいう運用者には、サービス提供者のようなシステムを直接操作するわけではないものも含みうる。」を追記 ・「使用方法等の情報を提供する際には、どのようにしてその情報へのアクセシビリティを向上させるかも検討する必要がある。」を追記 ・「この例のように、複数のステークホルダーが関係するリスクへの対処は、複数の観点から行えることから、関係するステークホルダーにおける負担について、各ステークホルダーが機器・システムのリスクに関連する情報を可視化・共有する等の方法を通じて、総合的に検討し、ステークホルダー間で合意する必要がある。したがって、単独のステークホルダーが全ての要求に対処する必要はなく、また、ある観点内であらゆるケースで必須に求められる具体的な要求の規定を一律に求めることは困難である。」を追記
19	1	団体	-	●イノベーションを促進するリスクベースアプローチを続けるべきである リスク管理が効率的なIoTセキュリティの基盤であると考える。本フレームワークで開発しているように、ベストプラクティスに依るリスクベースアプローチを継続し、IoTセキュリティに対する脅威を特定して防御することを推奨する。このため、本フレームワークはリスクの評価と特定、リスクを最小化する手法に焦点を当てるべきと考える。本フレームワークは新技術に適応することができるため、そのようなアプローチを通じて、イノベーションを促進し、セキュリティとイノベーションに報いるだろう。	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。なお、ご指摘の通り、本フレームワークにおいても、CPSFにおいてもリスクベースアプローチに基づいており、今後もリスクベースアプローチに基づき、IoTセキュリティを検討すべきと考えております。
19	2	団体	-	●既存の国際的なベストプラクティスと整合させるべきである 本フレームワークが、産業主導の国際標準やフレームワークに基づくことを推奨する。政府機関が既存の外国のサイバーセキュリティフレームワーク(例：NISTサイバーセキュリティフレームワーク、ISO/IEC 27001:2013)を将来的な政策執行に取り入れる場合、民間産業は大きく利益を得られる。こうしたフレームワークは、組織がサイバーセキュリティプログラムを開始したり既存のプログラムを改善したりするのに役立つプロセスだが、IoTセキュリティにも適用することができ、企業が長期的にセキュリティの状態を評価し、強化するために取ることができる、多くの業種別の行動を特徴としている。加えて、NISTは、"IoT機器製造者向けの推奨事項"を開発しており、最新ドラフトはリスクベースの測定アプローチに沿ったものとなっている。既存のサイバーセキュリティフレームワークやベストプラクティスのその他の例として、Framework for Improving Critical Infrastructure Cybersecurity、Council to Securing the Digital Economy C2 Consensus on IoT security core capabilities baseline、NISTIR 8259を挙げることができる。	本フレームワーク策定にあたっては、主要な国際規格等も参照しております。本フレームワークはIoTセキュリティ・セーフティを社会としてどう捉えるべきかについて考え方を示すものであり、例えば製造者に対する考え方を示したNISTIR8259等とは、補完的な役割を担うことができると考えています。 なお、いただいた御意見も参考に、「5. リファレンス」を追加し、本フレームワーク作成にあたり参照した規格等の文書を記載いたします。
19	3	団体	-	●キャパシティビルディングと情報共有に重点を置くべきである 公共部門と民間部門の間におけるキャパシティビルディングと情報共有を奨励している。情報共有により、政府や企業が強力になり、敵対者やサイバー攻撃者を弱体化させることができる。我々は、IoT機器関係者が脅威インテリジェンスや既知の脆弱性を報告し共有することを奨励するセクションを将来のドラフトに設けることを推奨する。それにより攻撃者に対するエコシステムの防御を強化することができる。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。なお、経済産業省としては、CPSFや本フレームワークとは別の枠組みにて、サイバーセキュリティ経営ガイドラインの策定など情報教育やセキュリティ教育にも注力を行っております。
19	4	団体	-	●本フレームワークの次のステップを明確にすべきである 本フレームワークは自発的なガイダンスと理解した。本フレームワークに関連する法律を検討している場合など、フレームワークの次のステップが明確になれば、企業が次のステップを検討する際に役立つだろう。	いただいた御意見も参考に、本文 1-2「本フレームワークの目的」を修正いたします。 ・「IoT機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。」を追記
20	1	企業	-	connectivityレベル（「サイバー空間とフィジカル空間の間」）のセキュリティに焦点を当てることを求める、IoTセキュリティに対する包括的で成果ベースのアプローチの本フレームワークを支持する。	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。
20	2	企業	-	多くのステークホルダーが機器レベルのセキュリティ（認証含む）に焦点を当てる中、それだけでは十分なポリシーアプローチではないとする経済産業省のメッセージに賛同する。	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。
20	3	企業	-	第1軸、第2軸について、私たちは、これらの2つの重要なレンズを介して、組織があらゆるサイバーセキュリティリスクを見て、管理すべきであることに同意する。	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。
20	4	企業	-	第3軸について、運用前と運用中の要件を含め、様々な観点から望ましいIoTセキュリティ・セーフティ要求を見ることを提案しており、両フェーズにおけるセキュリティ要求が重要であることに同意する。	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。
20	5	企業	-	国際的に出張して立場を議論したり（Covid19以前）、本フレームワークを英語に翻訳したり、英語でのコメントを許可したりすることなど、国境を越えてアプローチを理解してもらうための経済産業省の努力に感謝する。	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。
20	6	企業	-	IoTネットワークをどのように保護するか（secureにするか）について、本フレームワークに以下のようなreferences（言及）を含めることを提案する。 ○全機器とその動作を常に完全に可視化すること IoT 機器やシステムを利用する組織は、ネットワークを通過するトラフィックを常にリアルタイムで可視化し、きめ細かく制御する必要がある。その時にのみ、IoTベースのボットネットなど、ネットワークを通過する悪意のある脅威やアクティビティを検出し、止めることができる。経済産業省は、組織がネットワークを完全に可視化し、接続された IoT 機器の発見、識別、安全性の確保、最適化を彼ら自身でできるようにする技術を活用することを奨励すべきである。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
20	7	企業	-	IoTネットワークをどのように保護するか（secureにするか）について、本フレームワークに以下のようなreferences（言及）を含めることを提案する。 ○IoT機器が展開されているネットワークの分離 機器のリスクプロファイルに基づいて IoT 機器の設置区域管理を行う組織は、IT と IoT システム間の相互感染（cross-infections）を回避する可能性が高くなる。レガシーでパッチが少なく（low-patched）、一般的にリスクの高いIoT機器が他のIT資産と通信する能力を分離して制限することで、組織はネットワーク全体に広がる脅威を回避することができる。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。

ID	No	提出者	該当箇所	御意見の概要	御意見に対する考え方
21	1	団体	-	●国際相互運用性 政府の IoT セキュリティ政策は、世界中の他の同様の取り組みを参考にし、可能な限りそれに沿ったものとすべき。国際的に認められた標準があればそれに基づくべき。以下の取り組みについて経済産業省のレビューを推奨する。 - The US National Institute for Standards and Technology (NIST) Recommendations for IoT Device Manufacturers: Foundational Activities and Core Device Cybersecurity Capability Baseline (2nd Draft)　https://csrc.nist.gov/publications/detail/nistir/8259/draft - The C2 Consensus on IoT Device Security Baseline Capabilities (in revision) https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf - ISO/IEC 27402 (in process) (IoT security and privacy – Device baseline requirements)	本フレームワーク策定にあたっては、主要な国際規格等も参照しております。本フレームワークはIoTセキュリティ・セーフティを社会としてどう捉えるべきかについて考え方を示すものであり、例えば製造者に対する考え方を示したNISTIR8259等とは、補完的な役割を担うことができると考えています。 なお、いただいた御意見も参考に、「5. リファレンス」を追加し、本フレームワーク作成にあたり参照した規格等の文書を記載いたします。
21	2	団体	-	●一貫性のある定義 IoT セキュリティポリシーが、どの機器が対象となるかを可能な限り具体的かつ明確に定義することを推奨する。一般的に、IoT セキュリティポリシーは、国際的に認知された標準（※）に基づいた「IoT 機器」と「IoT システム」の定義を使用すべき。 - ネットワークに接続するように設計され、データの収集、送信、受信に必要なコンピュータ処理能力を含む機器を指す。 - 他の製品に組み込まれたり統合されたりすることなく、コンポーネントではない、意図された目的に使用可能であり、エンドユーザーが利用可能な完成品を指す。 - IoT 機器は、他のコンポーネント、機器、およびシステムを含むより広範なエコシステムに接続されるように設計されていることを認めること。そして、 - パーソナルコンピューティングシステム、スマートモバイル機器、メインフレームコンピューティングシステムを含む一般的なコンピューティング機器は含まれない。 （※）e.g.： ISO/IEC 17788:2014 Information technology - Cloud computing - Overview and vocabulary; ISO/IEC 20924:2018 Information technology - Internet of Things (IoT) – Vocabulary; ISO/IEC TR 23188:2020 Information technology - Cloud computing - Edge computing landscape	本フレームワークでは、ISO/IEC 20924:2018におけるIoT機器、システムの定義を準用しております。いただいた御意見も参考に、本文「1-1-2第2層の位置づけ」を以下のとおり修正いたします。 ・脚注に「本フレームワークでは、IoTについて、ISO/IEC 20924:2018も参考に、フィジカル空間とサイバー空間からの情報を処理し、反応するサービスと相互接続されたエンティティ、ヒト、システムおよび情報資源のインフラストラクチャであると定義し、そのような機能を提供するシステムをIoTシステム、そのシステムにおいてセンシング、あるいはアクチュエーティングを通じてフィジカル空間と相互作用し、通信するエンティティをIoT機器であるとした。本フレームワークにおいては、IoTを用いて利用者に提供する付加価値に着目することが重要であることから、IoT機器とIoTシステムを区別せず、付加価値を提供する単位を指して「IoT機器・システム」と表現している。」を追記
21	3	団体	1-1-2　第2層の位置づけ	●1-1-2 第2層の位置づけ　94-98行目 本節の例で、IoTシステムの設計者や実装者が重要なIoT機器を保護するため、IoT機器の環境条件に基づき追加の物理的なセキュリティ制御手段を検討する必要性を強調することを推奨する。 提案されている物理的分離を必要な制御として使用することは、55行目から57行目で強調されているIoT環境の動的で多面的な性質を考慮すると、規定的（prescriptive）なものであり、効果的または効率的なアプローチとは言えない。 さらに、物理的なネットワーク分離は、物理層でIoT機器によって収集され、アナログ信号からデジタルドメインに変換されたデータの精度が保証されないため、データを収集、処理、または処理しているアプリケーション内に最適に実装された許容可能なパラメータ内でデータの完全性を確保するための動的、効果的、かつ効率的なメカニズムを妨げる可能性がある。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
21	4	団体	1-1-2　第2層の位置づけ 3-2-1 第1軸：発生したインシデントの影響の回復困難性の度合い	●1-1-2 第2層の位置づけ　94-98行目 　3-2-1 第1軸：発生したインシデントの影響の回復困難性の度合い 本フレームワークで採用されている結果/影響アセスメントプロセスを補完するリスク管理への追加のアプローチを検討することを提案する。 最近の取り組みの参考文献には、IoTにおけるリスク分析のための追加的なアプローチについての有益な情報が含まれている。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
21	5	団体	3-3-1　第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	●3-3-1から3-3-3まで:求められるセキュリティ・セーフティ要求の整理 本節では、セキュリティのための様々な確認要求（自己適合宣言、認証、ライセンスなど）の利用を提案する。これらの要求の多くは、特にリスクの高いアプリケーションのセキュリティにとって有益だが、標準の国際相互運用性を確保し、セキュリティプロトコルを世界的に向上させるための規格を確立するために、国際的な調整を活用すべきである。我々は、経済産業省が確認要求の条件をさらに明確にすることを推奨する。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
22	1	団体	-	●基本的な共通インフラストラクチャ 本フレームワークが、サイバーセキュリティ業界内の様々な主体に適用できる「基本的共通基盤」を確立していることを評価する。 IoT機器やシステムの文脈でサイバーリスクについて共通の理解と考え方を作ることは、これらの問題について考え、アプローチする方法に大いに必要な構造を提供する。 機器レベルのセキュリティだけではなく、connectivityレベル（「サイバー空間とフィジカル空間の間」）のセキュリティに焦点を当てることを求める、IoT セキュリティに対する包括的な成果ベースのアプローチという経済産業省の本フレームワークを支持する。	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。
22	2	団体	-	●リスクマネジメントフレームワーク IoT分野でのステークホルダーの多様性を考えると、IoTのセキュリティがリスクマネジメントアプローチを採用することは重要であり、経済産業省が本フレームワークでそのようなアプローチを採用していることは心強い。そのために、本フレームワークのドラフトは、コンプライアンス要求を強制するのではなく、自主的な遵守を前提としていると推測している。次のドラフトでフレームワークへの準拠が実際には自主的なものであることを明確にしてくれると助かる。	いただいた御意見も参考に、本文 1-2「本フレームワークの目的」を修正いたします。 ・「IoT機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。」を追記
22	3	団体	-	●フレームワークのスコープの明確化 本フレームワークのスコープとそれが適用される主体に関する議論を明確にすることを推奨する。 現在のドラフトでは、本フレームワークは、IoT機器やシステムの商業用・運用アプリケーションと同様に、消費者や家庭用製品も対象としていると理解している。我々は本フレームワークが、両方の分野に適用されるかどうか、及びどのように適用されるかをより明確にし、これらの分野がドラフトに記載されている様々な軸にどのような影響を与えるかを記述することを助言する。	パブリックコメントを募集した時点での本文「1-2 本フレームワークの目的」113行目に、「簡易な情報サービスの分野に使用されるIoT機器と、工場や社会インフラシステム等の安全に関わる分野で使用されるIoT機器では、求められるセキュリティレベル、セキュリティ対策の目的、優先度が異なる。」と記載されているように、本フレームワークは様々な分野におけるIoT機器を想定しています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります
22	4	団体	-	さらに、フレームワークは、 “Device”, “IoT Device” (e.g. lines 60-61) や “IoT device Manufacturer” (e.g. line 283)などの主要な用語の定義を、国際標準やフレームワーク（※）で使用されているものと調和させ、IoT機器をパーソナル・コンピューティング・システムやスマート・モバイルなどの汎用コンピューティング・デバイスと明確に区別すべきである。 （※）e.g. NISTIR 8259, Draft 2nd (referenced above), lines 288–289.	本フレームワークでは、ISO/IEC 20924:2018におけるIoT機器、システムの定義を準用しております。いただいた御意見も参考に、本文「1-1-2第2層の位置づけ」を以下のとおり修正いたします。 ・脚注に「本フレームワークでは、IoTについて、ISO/IEC 20924:2018も参考に、フィジカル空間とサイバー空間からの情報を処理し、反応するサービスと相互接続されたエンティティ、ヒト、システムおよび情報資源のインフラストラクチャであると定義し、そのような機能を提供するシステムをIoTシステム、そのシステムにおいてセンシング、あるいはアクチュエーティングを通じてフィジカル空間と相互作用し、通信するエンティティをIoT機器であるとした。本フレームワークにおいては、IoTを用いて利用者に提供する付加価値に着目することが重要であることから、IoT機器とIoTシステムを区別せず、付加価値を提供する単位を指して「IoT機器・システム」と表現している。」を追記
22	5	団体	-	●国際協力 国際協力に対する経済産業省の揺るぎないコミットメントを評価する。 もし、本フレームワークのドラフトがIoT機器やシステムのセキュリティに対処する他の国に影響を与え、同様のアプローチと整合性が取ることに役立つならば、最も影響力のあるものとなるだろう。 我々は特に、本フレームワークの立場を議論するために国際的に出張したり、本フレームワークを英語に翻訳したり、英語でのコメントを許可したり、コメントのための期間を延長したりするなど、フレームワークの提案を国境を越えて理解してもらうために行った経済産業省の努力に感謝している。また、世界の多くの政府をはじめとするステークホルダーは、IoTセキュリティに深い関心を持っており、日本のような先進国とアイデアを共有することで恩恵を受けることができる。本フレームワークが今後もこのような取り組みを継続していくことを期待する。	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。
22	6	団体	3-2-1　第1軸：発生したインシデントの影響の回復困難性の度合い	●リスクの解釈 3-2-1において、本フレームワークのドラフトは発生確率を考慮せず、インパクトの度合いでリスクをカテゴライズするアプローチをとっている。 このアプローチについて質問がある。この状況において、企業は、edge case や　tail riskをどう扱えば良いか？ リソースをどこにどのように割り当てる必要があるかを評価するときに、重要性と確率の両方を検討することが、経済産業省も推進するリスクベースアプローチにおける基本的な前提である。加えて実際には、すべてのシナリオを想定できるわけではないし、そうしようとすることが賢明なリソースの使い方でもない。デミニマシナリオ（de minimis scenarios）、すなわち、影響や確率が一定の閾値を下回っている場合には、それ以上の行動をとる必要がないシナリオのガイドラインを作成することが有用である可能性がある	本フレームワークでは、フィジカル・サイバー間をつなぐIoT機器・システムの多様性を踏まえたカテゴライズが容易に行えるように、算出が比較的難しいインシデントの起こりやすさは考慮せず、インシデントが発生した場合の影響の度合いからカテゴライズを行うアプローチを採用していますが、いただいた御意見も参考に、本文「3-2 フィジカル・サイバー間をつなげる機器・システムに潜むリスクの整理」を以下のとおり修正いたします。 ・「なお、本フレームワークに基づき、産業界での議論等を踏まえた上で具体的な要求を整理する際には、起こりやすさについても考慮することが適切であることに留意されたい。」を追記 また、本文「3-3 求められるセキュリティ・セーフティ要求の整理」を以下のとおり修正いたします。 ・「なお、対策の実施はコストに直結することから、求められるセキュリティ・セーフティ要求に対しどのような対策を取るかは、インシデントの起こりやすさ等も踏まえた上で決定されることが適当である。」を追記 今後、セキュリティ・セーフティ要求を検討する際、一般的には起こりやすさの議論も必要であるところ、国際標準等も参照しながら、各産業界や機器の性質等を踏まえて検討してまいります。

ID	No	提出者	該当箇所	御意見の概要	御意見に対する考え方
22	7	団体	3-2-2　第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）	●経済的影響の度合い Section 3-2-2では、第2軸として、インシデントの経済的影響の度合いを説明している。 ここでは、インシデントが発生した場合の経済的影響について、損失や社会への悪影響などの限定的な経済的影響から、倒産や社会の大混乱などの壊滅的な経済的影響まで、さまざまな範囲を示している。 倒産などの直接的な経済的影響については、企業は試算が可能なはずだが、（社会や経済が）大混乱した場合には、社会への経済的影響の程度を評価できる情報が十分に得られない可能性がある。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
22	8	団体	3-2-2　第2軸：発生したインシデントの経済的影響の度合い（金銭的価値への換算）	●経済的影響の度合い IoT機器の展開やユースケースは多岐にわたるため、この分野におけるコンセンサスとして、メーカーが、ユースケースやIoTデバイスの展開環境、エンドユーザによるセキュリティ機能の提供・有効化の方法など、入手可能な情報をすべて把握しているわけではないことを認識しておくべき。 経済産業省が認識しているように、使用方法、展開先、および使用環境を予測する上でのこのような制限は、潜在的な攻撃の影響を予測することを非常に困難にする。 したがって、経済産業省は、企業に追加のガイダンスを提供することを含め、フレームワークで採用されるアプローチを定義する際に、これらの原則と制限を考慮すべき。	いただいた御意見は、フレークワークの更なる検討を進めていくに当たって参考にさせていただきます。
22	9	団体	3-2-3　フィジカル・サイバー間をつなげる機器・システムのカテゴライズ	●デバイスとシステムの利用形態に基づく分類 Section 3-2-3のシステムにおける機器の分類に関する議論の中で、同じ機器であっても、利用形態などによってマッピング先が異なる場合があることに重要な注意が払われている。 経済産業省が機器自体の特性だけではなく、ユースケースやデバイスが動作する環境にフォーカスしていることを評価している。 このアプローチは、インシデントの影響をより包括的に見ることができる。	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。
22	10	団体	3-3-3　第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求	●確認要求 Section 3-3-3では、IoT機器やシステムの運用・管理を行う個人が適切にIoT機器やシステムを運用・管理する能力を有していることを確認するための確認要求の必要性が強調されており、例として自動車の場合は運転免許証の要件が挙げられている。 IoT機器やシステムの運用・管理に一定の前提条件を設けることが重要であり、関連性のある状況であることは間違いないが、実際には、ライセンスや認証制度は、開発と施行の両方が過度に煩雑である。このようなライセンス・認証制度が国際的に調整されていない場合、貿易や専門知識の国境を越えた流れに負の影響を与え、最終的には認識された利益を上回る可能性がある。 このことを念頭に、本フレームワークのドラフトの次回改訂では、文書全体で明確に強調されている国際的な整合性を確保することを目的に、確認要求が必要とされるのか、あるいは奨励されるのかの文脈について、より明確にすることを提言する。	いただいた御意見も参考に、本文 1-2「本フレームワークの目的」を修正いたします。 ・「IoT機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。」を追記
23	1	団体	-	●基本的な共通インフラストラクチャ 本フレームワークが、サイバーセキュリティ業界内の様々な主体に適用できる「基本的な共通基盤」を確立することを奨励している。 IoT機器やシステムの文脈でサイバーリスクについて共通の理解と考え方を作ることは、これらの問題について考え、アプローチする方法に大いに必要な構造を提供する。	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	-	●リスクマネジメントフレームワーク 我々は、IoTセキュリティに関連して出現するあらゆる標準は、チェックボックスのコンプライアンスアプローチではなく、リスクマネジメントフレームワークを採用すべきであるとの立場をとっている。 経済産業省が本フレームワークのドラフトをリスクマネジメントアプローチに基づいて作成したことは喜ばしく、本フレームワークは既存の国際的なセキュリティ基準とうまく調和するものと確信している。 そのために、本フレームワークのドラフトは、リスクマネジメントのアプローチと緊張関係にあるコンプライアンス要求を義務付けるのではなく、自主的な遵守を前提としていると考えている。次のドラフトでは、本フレームワークへの準拠が実際には自主的なものであることを明確にすることが有用であろう。	いただいた御意見も参考に、本文 1-2「本フレームワークの目的」を修正いたします。 ・「IoT機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。」を追記
23	3	団体	3-3-3　第3の観点：機器・システムの運用・管理を行う者の能力に関する確認要求	●確認要求 Section 3-3-3では、IoT機器やシステムの運用・管理を行う個人が、IoT機器やシステムを適切に運用・管理する能力を有していることを確認するために、機器やシステムの運用・管理を行う個人に対する確認要求の必要性が強調されており、例として自動車の運転免許証の要件が挙げられている。IoT機器やシステムの運用・管理に一定の前提条件を設けることが重要であり、関連性のある状況であることは間違いないが、実際には、ライセンスや認証制度は開発だけでなく、施行するのも非常に面倒である。 このようなライセンス・認証制度が国際的に調整されていない場合、貿易や専門知識の国境を越えた流れに負の影響を与え、最終的には認識された利益を上回る可能性がある。 このことを念頭に置き、我々は、本フレームワークの次回の改訂では、確認要求が必要とされるのか、あるいは推奨されるのかの文脈について、より明確にすることを提言する。	いただいた御意見も参考に、本文 1-2「本フレームワークの目的」を修正いたします。 ・「IoT機器・システムに対する具体的な要求の一律の規定を目的に定めるものではない。」を追記
23	4	団体	-	●国際協力 国際協力に関する経済産業省の計画についての更なる明確化を歓迎する。本フレームワークは、IoT機器やシステムのセキュリティに対処するための素晴らしい出発点を提示している。しかし、その有用性は最終的には国際的な整合性に依存し、その整合性がなければ貿易とセキュリティの障壁が本フレームワークのドラフト案の提示する多くの利点に勝ってしまう可能性がある。	本フレームワーク策定にあたっては、主要な国際規格等も参照しております。本フレームワークはIoTセキュリティ・セーフティを社会としてどう捉えるべきかについて考え方を示すものであり、例えば製造者に対する考え方を示したNISTIR8259等とは、補完的な役割を担うことができると考えています。 なお、いただいた御意見も参考に、「5.　リファレンス」を追加し、本フレームワーク作成にあたり参照した規格等の文書を記載いたします。
24	1	団体	-	●総論 機器を超えた範囲に焦点を当てたIoTセキュリティに対する貴省の包括的なアプローチを支持する。 機器レベルのセキュリティ(例：機器レベルのセキュリティに対する認証利用)に焦点を当てるだけではセキュアなIoTに向けた効果的な政策アプローチにはならないとする貴省の評価に賛同する。デフォルトパスワードの回避や適時のソフトウェア更新等、製造者が適用すべき特定のベースラインは既に存在する。一方で、IoT機器のセキュリティだけに焦点を当てるのは、効果的ではなく、多くの場合効率的なアプローチにもならない。残念ながら、多くの政策提案は、エコシステム全体ではなくエコシステム内の個々の構成要素に焦点を当てた狭小なものとなっている。例えば、単にインターネットサービス提供者(ISP)がすべてのボットネットを遮断すべき、数十億という数になる機器の製造者が例外なく製造する機器をセキュアにすべきという提案をしている政策が存在する。そのような過度に単純化された解決策では、持続的にエコシステムをセキュアにするための本質的なニーズに対処することができない。単体の機器、ネットワーク、ソフトウェアというレベルでどの対策が実施されるかにかかわらず、リスクは存在しており、現在進行で進化している。セキュリティは、エコシステム内のいかなる構成要素であっても単体では始まらず、完結することもない。 本フレームワークは、機器のセキュリティだけに焦点を当てたのでは、環境や経済活動等のいくつかの外部変数を考慮できないとも指摘している。同じ機器であっても常に同じように使用されるわけではないため、それにより様々なリスクプロファイルと潜在的な影響が生じることとなる。したがって、IoT機器が動作する複雑なエコシステムを考慮する重要性を認識し、ネットワークレベルを含めて、政策立案者に対してIoTセキュリティへの包括的なアプローチを奨励している本フレームワークのアプローチを我々は高く評価する。あらゆるIoT機器がネットワークを利用して通信するという事実を考慮すれば、ネットワークはIoTセキュリティの優先度の高い検知・対応ポイントになるだろう。国際的なパートナーに対してネットワークとエコシステムの重要性を強調することを通じて、貴省がIoTセキュリティのソートリーダーであり続けることを応援する。	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。
24	2	団体	3-3　求められるセキュリティ・セーフティ要求の整理	●IoTアプローチのグローバル・ベスト・プラクティスの参照を検討すべきである 「3-3 求められるセキュリティ・セーフティ要求の整理」の中で、以下の取り組みの参照を検討することを推奨する。 • 2nd draft of NIST 8259 IoT Device Manufacturers Foundational Activities and Core Baselines • C2 Consensus on IoT Device Security Baseline Capabilities • ISO/IEC 27402 IoT security and privacy – device baseline requirements (策定中) 特に、IoT ベースラインを開発するための NIST の継続的な取り組みは、IoT セキュリティに関する産官学間の協力関係を改善する上で不可欠なものとなっている。ITI は、Council to Secure the Digital Economy（CSDE）を共同設立し、ボットネットやその他の自動化された脅威に対抗するためのプラクティスと能力を特定するための「国際アンチボットネットガイド」（ボットネット・ロードマップ内で何度も引用されている文書）を発行した。我々は、他の約20の協会とともにCSDEが推進しているC2 consensusに参画し、IoT機器のセキュリティ・ベースラインに関する産業界の合意を構築した。我々は、貴省 が本フレームワークの中でこれらのセキュリティベースラインの参照を検討し、加えて、IoT アプローチを世界的に調和させる試みの中でもISO/IEC JTC1 SC27 の規格開発動向をフォローすることを推奨する。	本フレームワーク策定にあたっては、主要な国際規格等も参照しております。本フレームワークはIoTセキュリティ・セーフティを社会としてどう捉えるべきかについて考え方を示すものであり、例えば製造者に対する考え方を示したNISTIR8259等とは、補完的な役割を担うことができると考えています。 なお、いただいた御意見も参考に、「5.　リファレンス」を追加し、本フレームワーク作成にあたり参照した規格等の文書を記載いたします。

ID	No	提出者	該当箇所	御意見の概要	御意見に対する考え方
24	3	団体	-	●IoTの調和した定義を使用してキーコンセプトを定義すべきである 機器、IoT機器（英：60 行目）、IoT機器製造者（283 行目）等の IoTセキュリティに関連する定義を同期させておくと便利である。以下の既存定義の活用を推奨する。 ○「機器」(device)とは、他の製品に組込まれたり統合されたりすることなく、意図した機能のために使用可能な完成品であり、その構成要素ではない。 ○「IoT機器」(IoT device)は、物理世界と直接相互作用する少なくとも1つの変換器（センサまたはアクチュエータ）と、少なくとも1つのネットワークインターフェースを有し、サイバーセキュリティ機能の特定と実装が既存のフレームワークや構成要素の下で行われるスマートフォンやラップトップ等のような従来の情報技術（IT）デバイスではない。 ○「IoT機器製造者」(IoT manufacture)とは、組み立てられた最終的な IoT機器を作成するエンティティである。 したがって、構成要素（通常は単独では機能しないため、IoT機器の定義を満たせない）は、IoT機器の定義の範囲を超えている。IoT機器と汎用計算機器（PCやスマートフォンなど）を明確に区別して定義することを通じて、対象となるIoT機器の演算能力とセキュリティ機能をより良く扱うことが可能となり、本フレームワークが実用的で適用しやすいものとなることが確実となる。	本フレームワークでは、ISO/IEC 20924:2018におけるIoT機器、システムの定義を準用しております。いただいた御意見も参考に、本文「1-1-2第2層の位置づけ」を以下のとおり修正いたします。 ・脚注に「本フレームワークでは、IoTについて、ISO/IEC 20924:2018も参考に、フィジカル空間とサイバー空間からの情報を処理し、反応するサービスと相互接続されたエンティティ、ヒト、システムおよび情報資源のインフラストラクチャであると定義し、そのような機能を提供するシステムをIoTシステム、そのシステムにおいてセンシング、あるいはアクチュエーティングを通じてフィジカル空間と相互作用し、通信するエンティティをIoT機器であるとした。本フレームワークにおいては、IoTを用いて利用者に提供する付加価値に着目することが重要であることから、IoT機器とIoTシステムを区別せず、付加価値を提供する単位を指して「IoT機器・システム」と表現している。」を追記
24	4	団体	3. 本フレームワークの基本構成	● IoTネットワークのセキュリティを確保するための技術的対策を盛り込む（1/2） 「3. 本フレームワークの基本構成」で提供される視点は、IoTを含めたサイバーセキュリティリスクを組織がより効果的に管理するのに役立つ。 IoTセキュリティリスクを、発生したインシデントの影響の回復困難性の度合い、発生したインシデントの経済的影響の度合い、求められるセキュリティ・セーフティ要求の整理という3つの軸に整理することは、組織のリスクアセスメントを枠具けるのに役立つ方法である。特に、第3軸「求められるセキュリティ・セーフティ要求の整理」では、製造フェーズ（3-3-1）と運用フェーズ（3-3-2）の双方で望ましいIoTのセキュリティ・セーフティ要求を見ることが重要だと示唆している。製造段階では、セキュリティ要求事項は、ある時点で製品が要件を満たしていることを伝えるセキュリティ指標である。しかし、本フレームワーク（3-1）では、セキュリティ要求事項が一律に設定されていたとしても、そのような要求事項がすべてのセキュリティ課題に対応するのには十分と言えず、ユーザを常に保護できるとは限らないことも認識している。IoT機器は導入時には最も強固なセキュリティ基準に基づいて構築されているかもしれないが、一日の終わりには、予期せぬ技術的課題、人為的ミス、脆弱性の悪用、サイバー衛生の欠如等の問題が発生している可能性がある。つまり、成果に基づいた運用上のセキュリティ要求事項もまた不可欠である。	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。
24	5	団体	-	● IoTネットワークのセキュリティを確保するための技術的対策を盛り込む（2/2） 我々はまた、以下に示すIoTセキュリティを向上させるネットワークレベルでの技術的な推奨事項を、本フレームワークに含めることを推奨する。 ○あらゆる機器とその動作の常時監視を可能とする IoT機器やシステムを活用する組織は、自身のネットワークを通過するトラフィックをリアルタイムで可視化し、粒度の高い制御を行う必要がある。そうして初めて、IoTベースのボットネット等の悪意のある脅威や活動を検知し、阻止することができる。貴省は、ネットワークの完全かつ継続的な可視性を可能にし、接続されたIoT機器の発見、識別、セキュリティ、最適化を可能にする技術の活用を組織に奨励すべきである。 ○ゼロ・トラスト・アプローチを採用する ゼロ・トラストのコンセプト下では、組織は、自身のネットワーク境界の内外における認証されていない活動を自動的に信頼しない。そのかわりに、組織はIoT機器を含むシステムへのアクセスを許可する前に、システムに接続しようとするすべてのユーザや機器を認証しなければならない。重要インフラやデータをきめ細かく管理することで、サイバーセキュリティのリスク管理をより効果的に行うことができる。 ○ IoT機器が配置されているネットワークをセグメント化(セグメンテーション)する 機器のリスクプロファイルに基づいてIoT機器群にマイクロセグメンテーションを適用すると、ITシステムとIoTシステムの間での相互感染を回避できる可能性が高くなる。レガシーでパッチが少なく、一般的にリスクの高いIoT機器が他のIT資産と通信する能力を分離し、制限することで、組織は脅威がネットワーク全体に広がるのを防ぐことができる。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
25	1	企業	-	● 我々は、コメントのための本フレームワークの公開を歓迎し、この様な機会に感謝している。本フレームワークは、様々な関連するセキュリティ上の問題を理解するための概念的基盤を明確にし、なぜそれが重要なのかを明らかにするのに重要である。 特に開発中のIoT機器・システムに対して、本フレームワークを当てはめることに焦点を当てていることに歓迎している：IoT機器には最初からセキュリティが組み込まれていることが不可欠であり、製品の設計途中で追加されるものとは考えられない。我々の見解では、チップの設計段階において、セキュリティを第一に検討する必要がある。 これは、PSAアプローチの背後にある基本原則である。 「セキュリティ」と「セーフティ」を一緒に考えることが、貴省の提案をより詳細にするための最良の方法ではないかと考えている。最初にセキュリティがなければセーフティを確保することができないため、セキュリティフレームワークから始めた上で、次にセーフティを必要とする市場においてセーフティをさらに強化する方が簡単かもしれない。セキュリティとセーフティを分けることは必ずしも容易ではないと認識しているが、詳細に検討すると、セキュリティを向上させるために対応すべき問題と、セーフティに関連する問題があることに気付く。例えば、セーフティの重要な側面には、機器が故障したときに何が起こるか、つまり、「故障したとしても安全を保てるよう機器を設計できるか？」という点があるが、それはセキュリティの問題ではない。	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。
25	2	企業	3-3-1 第1の観点：運用前（製造段階等）におけるフィジカル・サイバー間をつなぐ機器・システムの確認要求	●我々が主に関心を持っているのは第1、第2層/観点である。 ●第1の観点：私たちのPSA認定プログラムの中核部分は運用前にセキュリティ要件が満たされているかどうかを確認することにある。 ベストプラクティスにおけるセキュリティ上の原則が適用されていることを示す方法が必要とされている。 PSA認定レベル1は、公開されているIoT機器の脅威モデルとセキュリティモデルの目標に基づいて、方法論的に開発されている。これは、NIST 8259A（NISTの助けを借りた）と欧州のEN 303 645（必須条件）との整合性が取れている。 我々は、貴省によるこの文書の参照が、貴省の政策である国際ハーモナイゼーションのニーズを満たすことになるので歓迎する。ルネサスはPSA認証に対応している主要なチップベンダーの一つであり、日本のサイバーセキュリティビジネスを支援し、海外市場を開拓するという政策にも合致する。 最低限、IoT機器やシステムについては、国際的に認知されたセキュリティのベストプラクティスが運用前に達成されていることを証明する文書が必要であると提案されている。 本フレームワークのドラフトは、機器やシステムのメーカーに対して、攻撃を受けた場合の経済的影響と回復困難性を考慮するよう求めている。 我々は、このガイダンスをより明確にし、機器メーカーが潜在的な経済的影響と回復困難性を考慮したセキュリティ要件を確立するために、セキュリティ脅威モデルの作成を要求されるよう提案する。経済的影響が大きい場合やインシデントからの復旧が困難な場合には、追加の脅威や緩和策を検討する必要があるかもしれない。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。
25	3	企業	3-3-2 第2の観点：運用中のフィジカル・サイバー間をつなぐ機器・システムの確認要求	●第2の観点では、運用中に（セキュリティ）要件が満たされていることを確認するメカニズムが必要となる。PSAには、チップや機器がEAT（Entity Attestation Tokens）を介して信頼できるclaimを行うための標準ベースのメカニズムを提供するマネージドオープンソースプロジェクトが付属している。EATは、Root of Trustによって署名され、証明書利用者によって検証可能なclaimのセットを提供する。 EATは、低コストのマイクロコントローラでも実行できる非常に小さなプログラム（チップの信頼されたファームウェアの一部）である。EATのclaimには、動作中の機器に関する検証可能な情報、例えば機器の完全性やステータスに関するレポートなどが含まれる。動作中に検証可能なclaimを作成するデバイスの例としてEATに関するホワイトペーパーを添付している。 我々は、信頼されたセキュリティデータを通信し、この目標を達成するために、IETFによって標準化され、オープンソースソフトウェアとして利用可能な方法として、EATを参照することを提案する。 我々は、これらの問題に対する最終的な答えを出すものとして、本フレームワークが意図されていないことを認識している。貴省が言うように、本フレームワークは、ある特定の機器に対して一義的にセキュリティ・セーフティ要求の観点を決定するものではなく、実現される仕組み・サービスの利用者側から見てインシデントが発生した場合の影響を適切に分析し、第1軸と第2軸に従ってカテゴライズを行い、そのカテゴリに従って第3軸を活用してセキュリティ・セーフティ要求の観点・内容を適切に検討するための枠組みとなるものである。本フレームワークを有効に活用していくためには、ユースケースの整理を進めていくことが求められる。 しかし、今後はIoT機器開発者を支援するためにも、より正確なものを提供する必要があると考える。この次の段階で、私たちのPSAアプローチが皆様の興味を引くことを願っている。	本フレームワークは、IoT機器・システムにおけるセキュリティ・セーフティの検討に資する枠組みを共有することを目的としています。具体的にどのような実装が必要かについては、産業分野等により異なるものであり、ユースケースの取組などによる具体化などについて、引き続き検討してまいります。