経済産業省商務情報政策局サイバーセキュリティ課　パブリックコメント担当 御中

「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）」に対する意見

一般社団法人重要生活機器連携セキュリティ協議会（会長：徳田英幸、代表理事：荻野　司）は、日常生活で利用する機器（生活機器）の安全・安心に利用できる環境を実現するため、セキュリティ技術に関する調査研究、ガイドラインの策定や標準化の検討、及び普及啓発を行い、もって我が国のものづくり産業の発展と新規事業創造、そして国民生活の向上に寄与することを目的としている団体で御座います。

当協議会として、この度の「情報セキュリティサービス基準（案）」に対するパブリックコメント募集に際して、下記の２６点の意見を述べさせて頂きます。

氏　名	一般社団法人　重要生活機器連携セキュリティ協議会 代表理事　荻野　司
住　所	〒141-0021 東京都品川区上大崎 2-12-1　野田ビル 3F
電話番号	03-6455-7193
FAX 番号	03-6455-7194
電子メールアドレス	ccds-sec@ccds.or.jp

意　見
【意見１】 ■該当箇所 **P.6　２．サイバー・フィジカル・セキュリティ対策フレームワークの考え方** **２．１．フレームワークを策定する目的** **（2）　フレームワークの特徴** **① 各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる** ■意見内容 「各事業者が実施するセキュリティ対策のオペレーションレベルで活用できる」と記載がありますので、後述に記載の各対策において、提示されている対策だけでなく、その対策にて防ぐことができる具体的な脅威事例を示しておく必要があろうかと思います。是非、各対策に紐づいた具体的な脅威も示して頂き、利用者が活用する上で有益な参考資料にして頂ければと思います。

■理由

提示されている対策と関係する具体的な脅威事例が提示されていないので、対策実施における具体的な効果を実感できず、対策の必要性や深刻度が判断できないと思われる。

【意見２】

■該当箇所

P.6　② セキュリティ対策の必要性とコストの関係を把握できる

■意見内容

「セキュリティ対策の必要性とコストの関係を把握」については、サプライチェーン全体を構成する中小企業を含めた事業者が、実際に対策を行えるよう、想定されるリスクと必要な対策のコストのバランスをイメージできるような内容にすべきかと思います。

【意見１】と同様に、フレームワーク内に想定されるリスクと実際に生じた脆弱性の事例（例えば、JVN，CVE に記載されている事例）を提示する必要があろうかと思います。また、対策には、攻撃される強度に応じた複数の対策が存在します。例えば、自己の機器が乗っ取られないための対策や、他の IoT 機器に悪影響を及ぼさない対策など、種々の対策においても、最低限守るべき対策、より安全に防御するための再対策があります。従って、後述の各対策においても、対策できるレベル毎にフレームワークを分類しておけば費用対効果をイメージしやすいと考えます。

■理由

現状の想定リスクだけでは、実際の被害状況を想定することは困難です。

コストの関係を把握するには、示された対策で守れる攻撃のレベルを示す必要があります。

【意見３】

■該当箇所

P.6　② セキュリティ対策の必要性とコストの関係を把握できる

■意見内容

「セキュリティレベルを保ったままでコストを圧縮できるような内容にする」とありますが、後述のフレームワーク内容では、一定のセキュリティレベルを維持しつつ、コストを低減できるような対策の提示がなされていません。例えば、一つの対策が複数の脆弱性リスクの防止につながるケースなど、コスト面を意識した整理が必要です。

■理由

本フレームワークで示されている対策は、一定のセキュリティレベルを維持しつつコストを圧縮可能な手法が示されていない。

【意見４】

■該当箇所

P.6　② セキュリティ対策の必要性とコストの関係を把握できる

■意見内容

実際に脆弱性リスクの影響を把握するには、本対策を示すために使用したリスクシナリオを提示する必要があります。想定されるリスクの網羅性を把握し、リスクシナリオベースの対策検討という考え方が、実施できるような内容にすべきかと思われます。

■理由

実際に脆弱性リスクの影響を把握するためには、具体的なリスクシナリオ知る必要がある。

【意見５】

■該当箇所

P.11　２．３．フレームワークの構成

図 7 各層におけるセキュリティ対策の概要

■意見内容

フレームワークの図７には、対策の前段に「守るべきもの」「セキュリティリスクの洗い出しという脅威分析を考慮した記載がありますが、３章では、対策のみが列挙される形式となっており、本フレームワークの利用方法がイメージできません。P.11 記載の「守るべきもの」の洗い出し、「セキュリティリスクの洗い出し」は個社で別途実施した上で、対策を検討する段階でのみ使用されることを想定しているのでしょうか。

■理由

３章では対策のみが列挙される形式であり、フレームワーク図７の構成図と不整合があることから、本フレームワークの利用方法がイメージできないため。

【意見６】

■該当箇所

P.12～P.91　３．必要なサイバー・フィジカル・セキュリティ対策

※３章全体に関する意見

■意見内容

３章全体に言えることですが、IoT 推進コンソーシアムで策定された「IoT セキュリティガイドライン」との対応付けが明示されておりません。ガイドラインで提示されている項目（指針や要点）と、本フレームワークにおける対策との対応関係をあわせて示すことが必要と思われます。

■理由

「IoT セキュリティガイドライン」の方針に沿った具体的な対策案として、リファレンス資料として活用できるものになる。

【意見７】

■該当箇所

P.12～P.91　３．必要なサイバー・フィジカル・セキュリティ対策

※３章全体に関する意見

■意見内容

参考文献に記載されている各ガイドラインから想定されるリスク、対策を抽出したのでしょうか？本フレームワークにて提示された対策の選定理由を記載していただきたいと思います。（例えば、社会的影響度の高い被害を防ぐという観点にて抽出した。など、本フレームワークでの対策を挙げた理由を明示）

■理由

設計から廃棄にいたるライフサイクルにおいて、必要なセキュリティ対策が、どの程度網羅性があるのかを示し必要がある。それ対策が最低限の内容なのか、必要条件であるのか、十分条件であるのかを明示する必要がある。

【意見８】

■該当箇所

P.12～P.91　３．必要なサイバー・フィジカル・セキュリティ対策

※３章全体に関する意見

■意見内容

３章の構成として、対策ごとに「リスク要因」と「リスク影響」が記載されておりますが、具体的にどのような脅威を防ぐための対策であるかを記載すべきかと思われます。例えば、JVN や CVE 等のデータベースで公開されている実際に発生したインシデントを示しておくことが望ましいと思われます。類似意見【意見１】【意見２】

■理由

各項目が IoT 機器への具体的な脅威と紐づけられ、対策の費用効果を見積もる上で有益な情報とするため。

【意見９】

■該当箇所

P.33　３．２.【第 2 層】フィジカル空間とサイバー空間のつながりに係るセキュリティ対策

L2.001 セキュリティ対策が施された IoT 機器の導入

対策ポイント

■意見内容

対策ポイントについては「第三者機関による評価」のみが記載されていますが、「自己

適合確認により安全性を評価したIoT機器」も追記すべきかと思われます。
　また、中古市場で流通されたIoT機器に対する対策観点を盛り込み、購買者が購入したIoT機器に不正改造がないことを、何らかの形で検証できる仕組みについても記載が必要と思われます。
■理由
「対策の概要」記載との整合性が取れていないため。

【意見１０】
■該当箇所
P.37　L2.004 IoT機器における正規品の導入
■意見内容
　本項目の記載については、オープンソースのソフトウェア等を利用した場合の考え方についても考慮すべきかと思われます。
■理由
　オープンソースを使用する場合、正規品かどうかの正当性基準が不明確であり、また、サプライヤーの識別や認証も行われていない可能性が存在するため。

【意見１１】
■該当箇所
P.39　L2.005 IoT機器への適切なセキュリティ設定
■意見内容
　本項目に記載されている「IoT機器の初期設定手順(パスワード等)」や「不要なサービスの停止」については、一様に守るべき事項ですが、製品分野毎には、本例以外にも守るべき初期設定必要です。従って、一様に守るべき事例に加えて、製品分野毎に異なる初期設定方法・手法についても事例として示しておく必要があります。
■理由
　本ポイントでの事例は、つながるIoT機器に必要な最低限のマナーとしての要件ですが、製品分野毎には、本例に加えて守るべき初期設定がありますので、その事例も記載が必要なため。

【意見１２】
■該当箇所
P.40　L2.006 IoT機器へのアクセス制限
P.42　L2.007 IoT機器への不正ログイン対策
■意見内容
　【意見１１】と同様に、本項目に記載されている対策は、一様にまもるべき要件に対す

る対策ですが、実際の IoT 機器に適用するには、製品分野毎に本例に加えて守るべき初期設定がある点を追記する必要があります。具体的な事例として、製品分野毎に異なる方法を示しておくと必要があります。

■理由

本項目に記載されている対策は、つながる IoT 機器に必要な最低限のマナーであり、製品分野毎に本例に加えて守るべき初期設定があるため。

【意見１３】

■該当箇所

P.43　L2.008 IoT 機器への物理的なセキュリティ対策

■意見内容

本項目に記載されている対策を、実際の IoT 機器に適用するには、製品分野毎に本例に加えて守るべき要件を追記する必要があると思われます。具体的な事例として、製品分野毎に異なる方法を示しておく必要があります。

また、具体的な対策の一例として、デバッグポートを論理的に閉鎖する点も追加が必要であると思われます。

■理由

本項目に記載されている対策は、つながる IoT 機器に必要な最低限のマナーであり、製品分野毎に本例に加えて守るべき初期設定があるため。

【意見１４】

■該当箇所

P.44　L2.009 IoT 機器の可用性維持

■意見内容

本項目に記載の対策としては、サービス活動を一部あるいは全停止するという対策の追加が必要と思われます。

■理由

サービス活動を一部あるいは全停止することで、システムやサービスに波及する影響を最小限に抑え、長期的視野に立った可用性を担保するという選択肢も考えられるため。

【意見１５】

■該当箇所

P.48　L2.011 IoT 機器における不正なソフトウェアへの対策

P.49　L2.012 IoT 機器のマルウェアへの感染防止

P.50　L2.013 IoT 機器の継続的な脆弱性対策

■意見内容

本項目に記載の対策を適用する上で、対象となる IoT 機器の規模や機能により制限を受けるため、前項の L2.001～L2.009 とは区別し、製品分野毎に異なる要件として明示しておく方が良いと思われます。

■理由

例えば、マルウェア対策についても、製品毎に具体的な対策内容が異なることが想定されるため。

【意見１６】

■該当箇所

P.50　L2.013 IoT 機器の継続的な脆弱性対策

■意見内容

本項目に記載の対策ポイントには、セキュリティパッチの正当性が確認できる手段や手続きを設ける旨を追加する必要があると思われます。

■理由

情報セキュリティにおいては標準的な考え方であり、対策として追加が必要なため。

【意見１７】

■該当箇所

P.51　L2.014 IoT 機器のリモートアップデート

■意見内容

本項目については、リモートアップデートサーバに対する攻撃も想定し、サーバ側のセキュリティ対策を示しておく事が必要と思われます。

■理由

サーバ側の攻撃についても、実際のインシデント事例としており、対策の必要があるため。

【意見１８】

■該当箇所

P.51　L2.014 IoT 機器のリモートアップデート

■意見内容

本項目については、リモートアップデートの実装が困難な場合の更新方法や対策についても、示しておく必要があると思われます。

■理由

全ての IoT 機器にリモートアップデート機能の実装が可能とは限らないため。

【意見１９】

■該当箇所

P.52　L2.015 IoT 機器に導入するソフトウェアの管理

■意見内容

本項目に記載の対策を適用する上で、対象となる IoT 機器の規模や機能により制限を受けるため、前項の L2.001～L2.009 とは区別し、製品分野毎に異なる要件として明示しておく方が良いと思われます。

■理由

例えば、マルウェア対策についても、製品毎に具体的な対策内容が異なることが想定されるため。

【意見２０】

■該当箇所

P.55　L2.018 IoT 機器への広域ネットワークからの不正侵入対策

対策ポイント

・IoT 機器での通信は、通信を拒否することをデフォルトとし、例外として利用するプロトコルを許可する

■意見内容

本項目の対策ポイントに記載の内容は、「L2.006」,「L2.008」,「L2.012」に記載されているホワイトリストによる対策と同様なものであり、IoT 機器に共通して適用可能な対策と、製品分野毎に必要な対策を区別して記述する方が、理解しやすいのではないかと思われます。

■理由

本項目の「対策の概要」に記載されている内容は、実際には対象となる IoT 機器によって対策が異なることが想定されますが、最低限守るべき要件としては非常に重要なポイントであり、上記のように明確な対象の区別と対策の説明が必要なため。

【意見２１】

■該当箇所

P.57　L2.019 IoT 機器における不正な無線接続への対応

■意見内容

本項目に記載されている対策は、実際の IoT 機器に適用するためには製品分野毎に、本例に加えて守るべき要件がある点を追記する必要があると思われます。具体的な事例として、製品分野毎に異なる方法を示しておく必要があります。

■理由

本項目に記載されている対策は、つながる IoT 機器に必要な最低限のマナーであり、製品分野毎に本例に加えて守るべき要件があるため。

【意見２２】
■該当箇所
P.58　L2.020 IoT 機器の集中管理
対策ポイント
■意見内容
　本項目に記載されている対策ポイントについては、IoT 機器からの異常通知が妨害されるリスクを考慮した対策についても、追加する必要があると思われます。
■理由
　情報セキュリティにおいては標準的な考え方であり、対策として追加が必要なため。

【意見２３】
■該当箇所
P.60　３．３.【第 3 層】サイバー空間におけるつながりに係るセキュリティ対策
L3.001 信頼できるサービスサプライヤーの選定
対策の概要
・第三者機関による評価(ITSMS 認証等)を取得したサービスサプライヤーの選択
■意見内容
　本項目に記載されている対策の概要については、自己適合確認により安全性を確認したサービスサプライヤーの選択についても、追加すべきであると思われます。
■理由
　IoT 機器を用いたサービス事業は多種多様であり、今後も多くのサービスサプライヤーが登場し、評価要件についても随時アップデートが必要なため、既存の認証制度は不向きであると想定されます。従って、例えば、製品毎、業界毎に柔軟にサービスサーの要件をアップデートし、その最新の要件に従って、サービサーの安全確認ができる仕組みが必要であると考えれます。また、第三者機関による評価は、コスト的、時間的に事業への足かせになることも想定されるため、「IoT 機器の導入での対策」と同様に自己適合確認により、サービスサプライヤー側での評価を促進することが肝要であります。

【意見２４】
■該当箇所
P.60　L3.001 信頼できるサービスサプライヤーの選定
対策のポイント
・第三者機関によるセキュリティ評価を経て安全性を確認された製品・サービスを提供しているサプライヤーを選定する

■意見内容

対策ポイントについては「第三者機関による評価を経て安全性を確認された製品・サービスを提供しているサプライヤー」のみが記載されていますが、対策ポイントに「自己適合確認により安全性を確認された IoT 機器やサービスを提供しているサプライヤー」を追記すべきかと思われます。

■理由

「L2.001 セキュリティ対策が施された IoT 機器の導入」の記載との整合性が取れておらず、また L3.001 の「意見２２」で記載した理由からも、追加が必要と考えられるため。

【意見２５】

■該当箇所

P.60　L3.001 信頼できるサービスサプライヤーの選定

対策ポイント

・企画・設計段階において実施する要件定義・設計の結果を第三者機関がセキュリティの観点から評価する

■意見内容

対策ポイントについては「企画・設計段階において実施する要件定義・設計の結果を第三者機関がセキュリティの観点から評価」と記載されていますが、対策ポイントに「自己適合確認により安全性を確認する」を追記すべきかと思われます。

■理由

「L2.001 セキュリティ対策が施された IoT 機器の導入」の記載との整合性が取れておらず、また L3.001 の「意見２２」で記載した理由からも、追加が必要と考えられるため。

【意見２６】

■該当箇所

P.75　L3.010 IoT 機器、サーバ等の継続的な脆弱性対策

■意見内容

本項目に記載されている対策ポイントについては、IoT 機器からの異常通知が妨害されるリスクを考慮した対策についても、追加する必要があると思われます。

■理由

情報セキュリティにおいては標準的な考え方であり、対策として追加が必要なため。

以上