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

「IoT 製品に対するセキュリティ適合性評価制度構築方針案」に対する意見

［氏　名］	（企業・団体の場合は、企業・団体名、部署名及び担当者名） 一般社団法人 重要生活機器連携セキュリティ協議会(CCDS) 事務局　事務局長　田久保 順
［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
［電子メールアドレス］	takubo@ccds.or.jp

［意見］全１３件

■意見１）

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

［対象となる資料］

IoT 製品に対するセキュリティ適合性評価制度構築方針案

［項目］

3.7. ラベルの信頼性確保のための仕組み

・意見内容

［指摘内容］

「有資格者が評価したと掲載するための条件として、指定資格の保有者（情報処理安全確保支援士等）が、IoT セキュリティ評価に関する研修受講完了又は評価ガイドを理解していることを宣誓したうえで、評価又は評価結果の確認を実施することを求める。」とあるが、「研修」がここにしか言及されない。

［修正案］

まだ未確定であっても「IoT セキュリティ評価に関する研修については今後、本制度の技術審議委員会で検討する」などの補足が必要。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

「研修」に関する情報がないため読者の混乱を招く。

■意見２）

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

［対象となる資料］

『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』

［項目番号］

＃２　NA となるための条件、基準の補足説明

・意見内容

［指摘内容］

適合基準にて「パスワードやパスコードを使用する製品において」と対象を限定している。
このため、認証に「パスワードやパスコードを使用しない（パスワードやパスコード以外の仕組みを使用する）製品」は対象外となるのではないか。

[修正案（青字箇所）]
NA となるための条件、基準の補足説明
以下のいずれかの条件に該当する。(OR 条件)
・ネットワークを介したユーザ認証の仕組みがない（「NA であることの理由」に、脅威に対抗するためにユーザ認証が必要ない根拠を記載すること）
・認証の仕組みにパスワードやパスコードを使用しない（「NA であることの理由」に、使用している認証の仕組みを記載すること）

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
＃３の☆１適合基準において、認証の種類として「パスワード、トークン、指紋等」と記載しており、パスワード/パスコード以外の認証を示唆している。＃３と整合を取るとともに、そのような製品をカバーする必要がある。

■意見３）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
[対象となる資料]
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目番号]
＃４　NA となるための条件、基準の補足説明

・意見内容
[指摘内容]
「機器に対するネットワークを介したユーザアクセスの仕組みがない」とあるが、ユーザアクセスはあるがユーザ認証がない場合も NA になると思われる。

[修正案（青字箇所）]
NA となるための条件、基準の補足説明
・機器に対するネットワークを介したユーザ認証の仕組みがない（「NA であることの理由」に、外部からの不正アクセスに対抗するためにユーザ認証が必要ない根拠を記載すること）

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
＃２、＃３の「NA となるための条件、基準の補足説明」の記載〔ネットワークを介したユーザ認証の仕組みがない〕と整合させる必要がある。
もし、当該要件において意図的に違う用語を使っているのであれば、その意図を明確にしないと、読者の混乱を招く恐れがある。

■意見４）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目番号]

＃６　NA となるための条件、基準の補足説明

・意見内容
[指摘内容]
対象機器によっては、消防法などの適用により、ソフトウェアコンポーネントの更新に制約が生じる製品が存在する。正当な理由がある製品については、理由及び代替手段を示すことで、NA とすることを許容すべきと考える。

[修正案（青字箇所）]
NA となるための条件、基準の補足説明（以下の文章を追記）
ソフトウェアコンポーネントの更新に制限がある製品
（「NA であることの理由」にソフトウェアコンポーネントの更新ができない理由と共に、ハードウェアの交換などの代替手段及び、対応期限（期間）を記載すること）

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
消防法（昭和二十三年法律第百八十六号）に関連し、火災報知設備又はガス漏れ火災警報設備に使用する受信機は、下記の省令によりソフトウェアのアップデートに制約がある。

昭和五十六年自治省令第十九号受信機に係る技術上の規格を定める省令
第五条他
https://elaws.e-gov.go.jp/document?lawid=356M50000008019

■意見５）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
[対象となる資料]
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目番号]
＃１２　☆１適合基準

・意見内容
[指摘内容]
適合基準①は、「情報の盗聴」に対する保護対策であることが明示されているが、②では同様の記載がないため、対策すべきリスクが、曖昧であるように読めてしまう。
冒頭に「情報の盗聴に対する以下のいずれかの保護対策を行うこと」と、対策するリスクが明示されているので、①の「情報の盗聴に対する」の記述は削除する。

[修正案（青字箇所）]
☆1 適合基準
ネットワーク経由で伝送される守るべき情報資産について、情報の盗聴に対する以下のいずれかの保護対策が行われていること。

① 他の IoT 機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、~~情報の盗聴に対する~~保護対策を機器自らが行う。
② 他の IoT 機器やサーバ（クラウド上のサーバを含む）へネットワークを介して伝送される守るべき情報資産について、保護された通信環境（VPN 環境や専用線を経由した接続環境

）においてのみ伝送される。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

■意見６）

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

[対象となる資料]

『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』

[項目番号]

＃１３　☆１適合基準、NA となるための条件、基準の補足説明

・意見内容

[指摘内容]

適合基準②には、「脆弱性スキャンツールによる既知の脆弱性検査を実施」とあるが、評価ガイドでは「B）Bluetooth」、「C）USB」は検査対象外となる。公開文書では、評価ガイドが対象外となるため、誤解を避ける上で、「B）Bluetooth」、「C）USB」については脆弱性スキャンの対象外となる旨を、追記した方が良い。

[修正案（青字箇所）]

NA となるための条件、基準の補足説明（以下の文章を追記）

適合基準②の「脆弱性スキャンツールによる既知の脆弱性検査」は、「A）TCP/UDP ポート」のみを対象とし、「B）Bluetooth」、「C）USB」については対象外とする。
※ただし物理的なインターフェースにかかわらず、上位レイヤーで TCP/UDP ポートを利用する場合は対象とする。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

■意見７）

・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）

[対象となる資料]

『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』

[項目番号]

＃１５　☆１適合基準

・意見内容

[指摘内容]

適合基準①記載の「C）ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名」について、「暗号鍵やデジタル署名」は削除すべき対象データの解釈が、読み手によって齟齬を生じやすく、対策のハードルが高い情報が含まれる。例えば電子証明書については、製造段階で IC チップのセキュリティ秘匿領域に格納されており、データ消去が困難なケースが想定される。
また、「ユーザが設定した認証値」については、「Ｂ）のユーザ設定値」に含まれるものと解釈可能である。
従って、「C）ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名」に

ついては、記述を削除することが望ましい。

[修正案（青字箇所）]
☆1 適合基準
① ユーザによって、製品本体や関連サービス（モバイルアプリケーション等）を介して、ユーザに関する少なくとも以下の情報を削除できること。
A) 機器利用中に取得した情報資産（個人情報含む）
B) ユーザ設定値
~~C) ユーザが設定した認証値、製品利用中に取得した暗号鍵やデジタル署名~~

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

■意見８）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
[対象となる資料]
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目番号]
＃１５　セキュリティ要件

・意見内容
[指摘内容]
「ユーザは、簡単な方法で製品からユーザデータを消去できるような機能を提供されなければならない。」とあるが、日本語としては主語がユーザとなっているため、ユーザの義務のように誤解を与える。

[修正案（青字箇所）]
☆1 適合基準
製造業者は、ユーザが簡単な方法で製品からユーザデータを消去できるような機能を提供しなければならない。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

■意見９）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
[対象となる資料]
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目番号]
＃１６　☆１適合基準

・意見内容
[指摘内容]
適合基準「④対象製品やサービスのサポート期限又はサポート終了時の方針を周知すること」について、製造メーカとしては、「サポート期限」を明確化することが難しいという意見も出ている。また「方針」という記述は、曖昧な点があるため、文章の変更を提案する

。
[修正案（青字箇所）]
☆1 適合基準
④セキュリティに関するサポートを終了する場合、終了となるサポート内容の詳細を、サポート期限が満了する前に利用者へ周知すること。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）

■意見１０）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
[対象となる資料]
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目番号]
＃１７下の脚注表記

・意見内容
[指摘内容]
「The Security Requirements and ☆1 Conformance Criteria (1-1 to 17-3, 17-8) within this document are extracted from the ETSI EN 303 645 ©European Telecommunications Standards Institute 2020.」とあるが、「Conformance Criteria」は ETSI EN 303 645 から抽出したものではないと思われる。

[修正案]
脚注
「The Security Requirements (1-1 to 17-3, 17-8) within this document are extracted from the ETSI EN 303 645 ©European Telecommunications Standards Institute 2020.」
・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
ETSI EN 303 645 には「Conformance Criteria」の記載は該当しないため。

■意見１１）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
[対象となる資料]
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目]
【参考資料】セキュリティ要件・適合基準に関する用語集

・意見内容
[指摘内容]
「【別添】☆1 セキュリティ要件・適合基準」の中に出てこない用語がある。
例： 「外部感知機能」

[修正案]
「【別添】☆1 セキュリティ要件・適合基準」の中に出てこない用語を削除する。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
読者の混乱を招く可能性があるため。

■意見１２）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
[対象となる資料]
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目]
【参考資料】セキュリティ要件・適合基準に関する用語集
「機密セキュリティパラメータ」

・意見内容
[指摘内容]
「機密セキュリティパラメータ」を「重要なセキュリティパラメータ及び公開セキュリティパラメータ。」と説明されているが、機密情報でありがら、公開パラメータを含んでいることは、矛盾する記述のように受け取れる。

[修正案]
「慎重に取り扱うべき」「重要な」「センシティブ」等と記載したほうがよい。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
ETSI EN 303 645 で定義されている「sensitive security parameters」のことだと思われるが、定義上明確に公開情報（公開セキュリティパラメータ）を含むのであれば「sensitive」の訳語として「機密」は避けたほうがよいと思われる。

■意見１３）
・該当箇所（どの部分についての意見か、該当箇所が分かるように明記して下さい。）
[対象となる資料]
『IoT 製品に対するセキュリティ適合性評価制度構築方針案
別添 ☆1 セキュリティ要件・適合基準.pdf』
[項目]
【参考資料】セキュリティ要件・適合基準に関する用語集
「重要なセキュリティパラメータ」

・意見内容
[指摘内容]
「機密セキュリティパラメータ」での指摘通り、「機密セキュリティパラメータ」の「機密」を「重要な」と変更した場合に訳語が重なる。

[修正案]
「機密の」「非常に重要な」「クリティカル」などとしたほうがよい。

・理由（可能であれば、根拠となる出典等を添付又は併記して下さい。）
ETSI EN 303 645 で定義されている「critical security parameters」のことだと思われるが、

定義上明確に秘密情報となっており、「sensitive security parameters」ではなく、こちらを「機密」としたほうがよいと思われる。また、「critical」なので、「非常に重要な」「クリティカル」なども候補に挙がると思われる。