参考資料

IoT機器・システムのセキュリティに関する認証制度について

一般社団重要生活機器連携セキュリティ協議会

CCDSでの議論（まとめ）

認証マーク　［必要］

★消費者保護の視点　（参考：米国FTCとASUS訴訟事案）

－セキュリティ対策レベルの見える化

★セキュリティ対策　コストから投資へ

－投資・差別化要素とする。

認証マークスキーム：

★検証：セルフチェック（第三者による検証スキームも用意）

★認証：最低限守るべき要件と製品分野毎に各々で用意

① つながる機器としての最低限のセキュリティ要件

⇒　第三者認証（行政がエンドース）

② 分野毎に異なる機能に対するセキュリティ要件

⇒　業界認証（２者認証方式）

検証方法： IoT機器（規模）にあったLight weightな基準

★プロセスチェック：

セキュリティを考慮したという証跡の有無を示すプロセスを提示

★レベルチェック：

ガイドラインに明示された検証手法と結果に到達の有無のみ提示

CCDS 製品分野別WG

車載機WG	主査：JVCケンウッド
スマートホームWG	主査：積水ハウス 副査：LIXIL
金融ATMWG	主査：日立オムロンターミナルソリューションズ
決済端末POSWG	主査：オムロンソーシアルソリューションズ
セキュリティ技術WG	主査：セルテック 副査：大日本印刷
ユーザビリティWG	主査：SDテック 副査：Ueye’sデザイン
人材育成WG	主査：デロイト トーマツ リスクサービス 副査：トレンドマイクロ

論点１　IoT機器の対象範囲

- IoT機器の対象範囲
  - ネットと繋がった機器（単独）
    - 外部から攻撃を受ける、自身が攻撃者になる
  - ネットが繋がった機器と繋がったシステム（複数機器連携）
    - 繋がる機器から攻撃を受ける、自身が攻撃者になる

- IoT機器の守るべきセキュリティが必要な範囲
  - 外部ネットワーク（キャリア網経由）：WANに接続
    - 他機器、システムへのエントリーポイントとなりうる。
      - 従って、最低限の守るべきセキュリティは必要
  - 内部ネットワーク：LAN
    - LAN内に外部と繋がる機器がある場合
      - WAN用機器として扱う必要
    - 無い場合
      - WANへの転用が可能な場合には、WAN機器として扱う必要

論点２　守るべきセキュリティ

1. セキュリティ要件は、製品分野毎に異なる
   - 製品分野毎に異なるセキュリティ要件（対策コスト、被害コスト）
     - 必要機能：ex.表示、蓄積
     - 構成要素：ex.OS,入出力

   従って、製品分野毎にセキュリティ要件を設定する必要がある。

2. 繋がる製品機器（システム）間で異なるセキュリティレベルが存在すると、低いところがエントリーポイントとなる。
3. WANに繋がるIoT機器には、最低限必要なセキュリティ要件が必要

   従って、共通の最低限守るべきセキュリティ要件を設定する必要がある。

論点３　セキュリティレベルの見える化

- IoT機器、IoT機器を使ったサービスにおけるセキュリティ状況の開示：消費者保護
  - 使用者、購買者（企業調達者）への情報開示
  - 品質管理（体制、基準、実施、結果,etc）の見える化が必要

  ー＞基準、結果の見える化（情報の公開）

- 製品分野毎に異なるセキュリティ要件をどのように公開、周知させるか？他製品分野と繋がった場合？
  - 業界団体毎で認証（自主認証含む）
    - 実施基準、実施手法、実施結果の体制構築と公開（見える化等）基準の策定
    - 既存基準との整合性、海外基準との整合性
  - 業界団体毎のセキュリティ要件との整合、調整
    - サプライチェーン

論点４　認証主体（自主認証、業界認証、行政認証）

- 自主認証(ex.Appleアプリ)
  - メーカ側の品質基準による。日本国内のIoT機器セキュリティの向上は市場原則に依存する。
- 業界認証（ex.EchonetLite)
  - 製品特有の守るべきセキュリティ要件を設定する。
  - 個社でなく、業界として一定の要件を定めるため、自主認証に比べて、周知をしやすいい。一方、品質基準は、メーカ側依存。
    - 大会社だけなく中小会社も含めた要件にできるか？
    - 認証が製品のブランドとして意味付け（価格反映）できるか？
    - 業界毎の認証マークの違いの周知？
- 行政認証(ex.IEC62443(EDSA),ISO/IEC15408(CC))
  - 最低限守るべきセキュリティ要件を設定する。
  - 業界認証に比べて、周知をしやすく、ブランドとしての意味付けの効果に期待はできる。
    - 基準を明確にし、運用も透明化する必要がある。
    - 認証スキームの簡素化が必須（認証コストの低廉化）

論点５　検証主体（自主検証、第三者検証）

- 自主検証
  - 製品に適切なセキュリティ要件を、開発時から実施可能なので、
    - 企画・設計段階からSecurity byDesignを実施することが可能
    - 第三者検証に比べれば検証にかかるコストは安価となる
  - 考慮点
    - メーカ側の品質体制に依存
    - 中小メーカ等の自主的に実施できない場合への対策
    - 輸入販売代理店等の自主的に実施できない場合への対策
- 第三者検証
  - 検証機能を開発要件から切り離し独立性を担保する
    - セキュリティ要件に従って、厳格な検証結果が得られる
    - 自社に検証体制を持てないメーカにアウトソースが可能
  - 考慮点
    - メーカ側と第三者検証側で煩雑な手続きのが懸念（簡素化）
    - 製品情報の開示、実施結果情報、対策手法の開示などへの懸念

参考資料

総務省
「一定のセキュリティを確保したIoT機器の認証のための仕組みの構築に向けた調査結果」より

調査会社：株式会社マストトップ社
監修：（一社）重要生活機器連携セキュリティ協議会

報告書　目次内容

機器認証に対するIoT機器製造事業者のニーズの調査
(１)各企業に対するヒアリング調査

下記のIoT機器製造事業者に対してニーズ調査を実施

種別	選定理由
住宅設備機器メーカ	ガス調理機器、ガス温水機器等の製造。ネットワークに接続可能な先端的設備機器を開発。
ホームネットワーク関係機器メーカ	広範なIoT家電製品の製造を行う国内最大手企業であり、製品セキュリティ行政部、品質・環境保証部の担当者へヒアリングを行う。
通信機器メーカ	重電製品からIoT家電製品にいたる広範な機器の製造業者であり、CCDS製品分野別セキュリティガイドラインのIoT-GW編の策定WG座長
車載器メーカ	インフォテイメント車載機器の製造を行う大手企業であり、CCDS製品分野別セキュリティガイドラインの車載編の策定WG座長

機器認証に対するIoT機器製造事業者のニーズの調査
(２) ヒアリング結果の分析・考察①

１）認証マークの要否

・ヒアリングの結果、認証マークは不要という回答はなし

・認証マークによる利用者へのセキュリティ認知度の向上とセキュリティ対策済み製品として訴求できる価値を理解する声が多かった。

２）認証マークの仕組み

・認証スキームは、基本的に二者認証(自主検証、第三者検証併用)とする要望が高かった。

・取得にあたり、あまり多くの費用が掛かっては、その費用回収に必要な売上げも多大となってしまう。一定のセキュリティ安全性が確保できるレベルを維持しつつ、簡易な手続きや評価方法により誰でも認証マーク取得を検討できるバランスのある制度が求められている。

・リリース日程の長期化を懸念する声に対して、申請から認証判定に要する期間は、できるだけ人手をかけずに短くできる工夫が求められる。

３）認証マークの活用、取得情報の開示方法等

・認証マーク表示の要望は高かったが、表示方法は事業判断とする声が多い。認証マークの乱用を避ける意味でも、表示ガイドを提示し、事業者が選択できる形がよいと考える。

・認証マークを取得したメーカ（フロントランナー）からフィードバックされた情報として、認証マーク取得時の参考となる、開発時や評価時に留意すべきことなどの情報提供サービスがあれば、IoT機器メーカでのセキュリティ対応も向上し、認証マークを取得する動きも加速すると考えられる。

IoT機器の脆弱性についての調査
(１)統計的アプローチによる調査結果①

過去の脆弱性DB(NVD)より、リスク分析による深刻度の高い脆弱性Top20を抽出する調査結果を活用し、123のCWEそれぞれについて、CVSSv3の結果が「High」と「Critical」となるインシデント数の多いCWEを特定した

	ID	Vulnerability	総数	Critical	High	合計(C+H)
1	CWE-119	Buffer Errors	3,352	867	1,988	2,855
2	CWE-264	Permissions, Privileges, and Access Control	1,667	151	1,204	1,355
3	CWE-284	Improper Access Control	1,693	161	773	934
4	CWE-20	Improper Input Validation	1,319	156	589	745
5	CWE-200	Information Exposure	1,877	51	388	439
6	CWE-89	SQL Injection	397	208	157	365
7	CWE-352	Cross-Site Request Forgery (CSRF)	347	3	306	309
8	CWE-399	Resource Management Errors	547	6	260	266
9	CWE-416	Use After Free	298	115	139	254
10	CWE-125	Out-of-bounds Read	422	32	180	212
11	CWE-22	Path Traversal	295	29	161	190
12	CWE-190	Integer Overflow or Wraparound	225	59	124	183
13	CWE-254	Security Features	370	43	129	172
14	CWE-476	NULL Pointer Dereference	348	31	134	165
15	CWE-287	Improper Authentication	193	90	67	157
16	CWE-77	Command Injection	162	64	88	152
17	CWE-787	Out-of-bounds Write	173	54	93	147
18	CWE-426	Untrusted Search Path	118	2	114	116
19	CWE-255	Credentials Management	148	57	56	113
20	CWE-19	Data Processing Errors	150	15	82	97

IoT機器の脆弱性についての調査
(２)既存のセキュリティ要件、有識者へのヒアリングによる調査結果

１）有識者へのヒアリングによる調査結果

追加の指摘があった基礎的な脆弱性
①不要な待ち受けポートがないか
②Wi-Fi/BTの通信方式の確認
③外部とのI/Fにおいて既知の脆弱性が対策されているか
④廃棄やリユース時の考慮

２）海外におけるIoTセキュリティに関する認証要件や調達要件の調査結果

EDSA認証とUL2900は、セキュリティ機能の妥当性(開発プロセス、静的ソースコード解析)と脆弱性の残存確認(ツールによる評価)を行うもの
UL2900は、IoT Cybersecurity Improvement ACT 2017にある下記の要件を満たせるように設計されているよう見受けられた ・既知の脆弱性の排除 ・認証ID・パスワードの不適切（ハードコーディング、変更不可等）な実装 ・アップデートできない（セキュアにアップデートできない）
ISO15408は、評価の観点は参考になるが、定義したPPに対する設計・開発・実装の妥当性の観点のみのため、今回検討している認証とは性格が異なる
調達要件には、納品前にセキュリティの問題がないこと、アップデート修正可能なこと、認証機能のハードコードの回避を確認することのみ要求されており、評価手法に言及しているものはなかった

(３)IoT機器が満たすべきセキュリティ要件の案

統計的に重要と思われる脆弱性と、有識者ヒアリングにおいて指摘のあった脆弱性および海外の認証制度の要件や調達要件を調査し、総合的にIoTセキュリティ要件を検討した。

○統計的に影響度が高く重要と考えられる脆弱性

- 「3.1.2　IoT機器の脆弱性についての調査」より統計的に重要な脆弱性Top20の抽出を行った。
- CWE Top20のうち5つ（#264, #399, #254, #255, #19）は、複数のCWEをまとめたCWEとなるためリストから除外している。

○既存のセキュリティ要件、有識者によるヒアリング調査にもとづく脆弱性

- 統計的には少数だが、有識者より指摘されるIoTの分野共通的な脆弱性
- 海外の認証要件や調達要件となっている要件、脆弱性
- 上記の脆弱性について、検証ツールによる評価で脆弱性を発見でき、解決を確認できるものと、開発プロセスでの設計やコーディングレベルのレビューを要するもの

IoT機器の脆弱性についての調査
(３)調査結果にもとづくIoTセキュリティ要件の整理②

・統計的アプローチや、有識者へのヒアリング、海外の認証プログラムの調査結果をもとに、IoTセキュリティ要件の候補を以下のように整理。

最低限対策すべき脆弱性（４象限の分類）　　**太字：IPA10大脅威にある重要度の高いもの**

	統計的見地から対策が必要な脆弱性				統計には表れない対策が必要な脆弱性（海外の要件例、有識者ヒアリングでの指摘）	
	No.	順位	CWE-ID	脆弱性の内容	No.	脆弱性の内容
ツール検証が可能（Webアプリ検証ツール、データベース検証ツール等）	A-1	1	CWE-119	Buffer Errors（バッファオーバーフロー）	B-1	車載：不要サービスポートの解放(BOT対策)
	A-3	**4**	**CWE-20**	**Input Validation（不適切な入力検証）**	B-2	車載：オープンサービスポートの不適切なアクセス権限（BOT対策）
	A-4	**5**	**CWE-200**	**Information Leak / Disclosure（情報暴露/開示）**	B-3	EDSA/UL：ゼロデイ脆弱性の排除（ファジング、推奨は高価なツール：Synopsys Protocode）
	A-5	6	CWE-89	SQL Injection（SQLインジェクション）	B-4	UL/US法案：既知の脆弱性の排除（高度・高価なツールが必要：Synopsys Codenom icon）
	A-6	7	CWE-352	Cross-Site Request Forgery (CSRF)（クロスサイトリクエストフォージェリ）		
	A-7	**11**	**CWE-22**	**Path Traversal（パストラバーサル）**		
	A-8	**15**	**CWE-287**	**Authentication Issues（認証に関する脆弱性）**		
	A-9	16	CWE-77	Command Injection（コマンドインジェクション）		
開発プロセス検証（仕様確認）が必要	No.	順位	CWE-ID	脆弱性の内容	No.	脆弱性の内容
	C-1	**3**	**CWE-284**	**Improper Access Control（不適切なアクセス権限）**	D-1	車載/US法案：認証ID/PWDの不適切な実装（ハードコーディング、変更不可等）
	C-2	9	CWE-416	Use After Free　（不適切なメモリ管理、解放後のメモリ参照による脆弱性）	D-2	車載：廃棄やリユースを想定したセキュリティ情報、プライバシー情報の一括削除機能が実装されていない
	C-3	10	CWE-125	Out-of-bounds Read（メモリ領域外のデータ読み取り）	D-3	車載：WiFiの通信方式において、最新の方式が適用されていない（WEP、WPA）
	C-4	12	CWE-190	Integer Overflow or Wraparound（整数オーバーフローとラップアラウンド）	D-4	車載：Bluetoothのペアリング方式において、最新の方式が適用されていない（PIN）
	C-5	14	CWE-476	NULL Pointer Dereference（NULLポインタの参照解除）	D-5	車載：外部I/Fの既知の脆弱性が対策されていない（既知の脆弱性に対して、最新パッチが適用されていない）
	C-6	17	CWE-787	Out-of-bounds Write（バッファ境界外への書き込み）	D-6	車載：USBの不要なクラスの利用
	C-7	**18**	**CWE-426**	**Untrusted Search Path（信頼できない検索パス）**	D-7	車載：USBの使用クラスに対する不適切なアクセス権限
					D-8	US法案：アップデートできない（セキュアにアップデートできない）

IoT機器認証の制度構築に向けた検討

IoT機器認証業務

（１）既存のセキュリティ認証プロセスの調査結果①

IoT機器認証業務のプロセス設計にあたり、既存の認証プロセスの調査を行った。対象とした認証プロセスを以下となる。

■第三者認証の事例として調査

１)IEC62443(EDSA)認証プロセス

２）Common Criteria(ISO/IEC 15408)認証プロセス

■第二者認証の事例として調査

３)ECHONET Lite認証プロセス

４)IPv6 Ready Logo認証プロセス

IoT機器認証業務

（１）既存のセキュリティ認証プロセスの調査結果②

第三者認証・代人者のメリット・デメリットの整理

認証形態	メリット	デメリット
第三者認証	・申請元のIoT製造企業が検証用の技術、知識、人員、環境を用意する必要がない。 ・より客観性の高い検証結果を得られる。	・外部検証機関との契約プロセスが必要となる（与信や口座開設などの対応の手間） ・検証に掛かる費用や期間をコントロールしにくい。 ・検証結果に問題が発生した場合、再度検証が必要となり、コストが見積りにくい
第二者認証	・認証の申請から付与までの期間やコストをコントロールしやすい。 ・問題が発生した場合にトライ＆エラーがしやすい。	・社内で検証用の技術や知識、人員、環境を用意する必要がある。 ・検証結果の客観性に乏しい。

IoT機器認証業務

（１）既存のセキュリティ認証プロセスの調査結果③

既存の認証プロセスの課題・改善点の整理

認証の名称	課題・改善点	
EDSA	認証プロセス	・SDSAはV字モデルの全工程にセキュリティの考え方を導入するためコスト負担が大きい
	認証レベル	※評価の要求事項数に応じたレベル設定は、対費用効果の点からも参考になる
Common Criteria	認証プロセス	・開発者の想定が及ばない範囲で脆弱性を作りこむケースは対象範囲外となる ・STの記述には、CC認証のプロセスや記載方法に関する専門的な知識が必要
	認証レベル	対策すべきセキュリティ要件から認証レベル設定をする考え方とは設計理念が異なる
ECHONET Lite	認証プロセス	・規格への適合性を証明するための申請文書が多く、必要な事項の絞り込みが必要。
	認証レベル	・対象外（認証レベルは設定されていない）
IPv6 Ready Logo	認証プロセス	・IoTセキュリティの認証を想定した場合、開発プロセスの対応事項のチェックが必要
	認証レベル	・対象外（認証レベルは設定されていない）

IoT機器のセキュリティ評価検証ガイドラインのあり方

セキュリティ要件の分析から分類（4象限）

※赤字は重要度が高い要件（ IPAの2017年10大脅威にあてはまる数が多い要件）
※赤枠内は、BOT化対策として対応が必要な要件

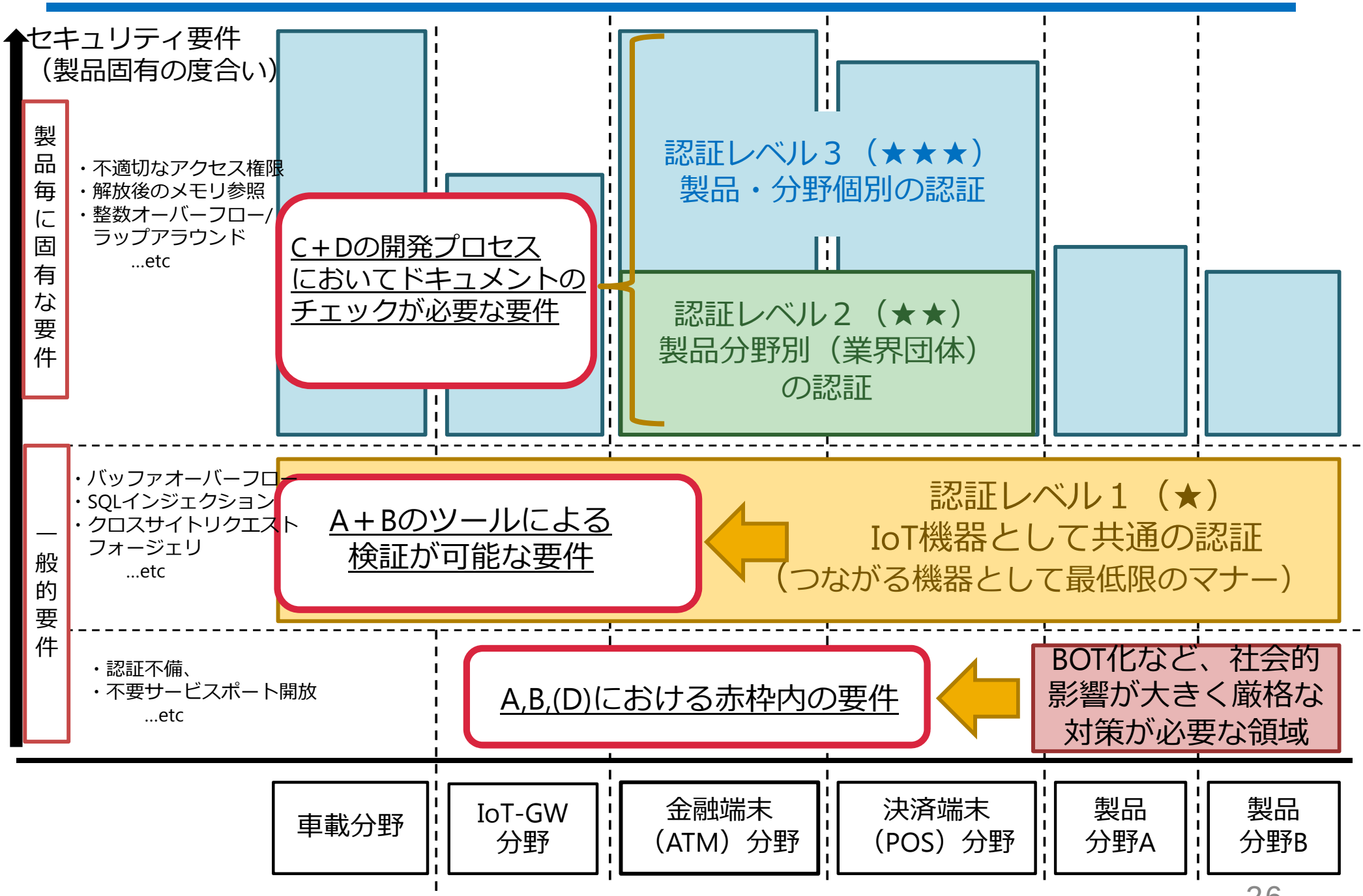
	統計的見地から対策が必要な脆弱性				統計には表れない対策が必要な脆弱性（海外の要件例、有識者ヒアリングでの指摘）	
	No.	順位	CWE-ID	脆弱性の内容	No.	脆弱性の内容
ツール検証が可能	A-1	1	CWE-119	バッファオーバーフロー	B-1	不要サービスポートの解放
	A-3	**4**	**CWE-20**	**不適切な入力検証**	B-2	オープンサービスポートに対する不適切なアクセス権限
	A-4	**5**	**CWE-200**	**情報暴露/開示**	B-3	EDSA/UL：I/Fゼロディ攻撃対策
	A-5	6	CWE-89	SQLインジェクション	B-4	UL/US法案：既知の脆弱性の排除
	A-6	7	CWE-352	クロスサイトリクエストフォージェリ		
	A-7	**11**	**CWE-22**	**パストラバーサル**		
	A-8	**15**	**CWE-287**	**認証に関する脆弱性**		
	A-9	16	CWE-77	コマンドインジェクション		
開発プロセス検証（仕様確認）が必要	No.	順位	CWE-ID	脆弱性の内容	No.	脆弱性の内容
	C-1	**3**	**CWE-284**	**不適切なアクセス権限**	D-1	アクセスコードや認証鍵の不適切な実装（ハードコーディング、変更不可等）
	C-2	9	CWE-416	解放後のメモリ参照による脆弱性	D-2	廃棄やリユースを想定したセキュリティ情報、プライバシー情報の一括削除機能が実装されていない
	C-3	10	CWE-125	メモリ領域外のデータ読み取り	D-3	WiFiの通信方式において、最新の方式ではない（WEP、WPA）
	C-4	12	CWE-190	整数オーバーフローとラップアラウンド	D-4	Bluetoothのペアリング方式が最新の方式ではない（PIN）
	C-5	14	CWE-476	NULLポインタの参照解除	D-5	外部とのI/Fにおいて既知の脆弱性が対策されていない（既知の脆弱性に対して、最新パッチが適用されていない）
	C-6	17	CWE-787	バッファ境界外への書き込み	D-6	USBの不要なクラスの利用
	C-7	**18**	**CWE-426**	**信頼できない検索パス**	D-7	USBの使用クラスに対する不適切なアクセス権限
					D-8	US法案：アップデートできない（セキュアにアップデートできない）

A　B　C　D

製品分野を加味した区分

認証レベル3 ：製品固有の認証	IoT機器において最低限守るべきセキュリティ要件を踏まえ、製品分野別に対策が必要な要件を抽出し、追加要件を設定する。 ↓ 評価・検証仕様書として、脅威分析～対策までを立案し、検証結果を報告する
認証レベル2 ：製品分野別の認証（業界団体等）	
認証レベル1 ：IoT機器共通の認証	IoT機器において最低限守るべきセキュリティ要件に基づく 検証結果の報告

セキュリティ要件と認証レベルの対応関係



認証マーク策定に向けた今後の課題

７．認証マーク策定に向けた今後の取り組み

- 本調査により、IoTセキュリティ認証マーク制度について検討し、制度の案がまとめられた。
- 認証マーク制度の本格運用を目指すためには、その準備が必要となる。認証制度を2019年度に試行する上で、事前に必要な取り組みを下記に示す。

1. 認証スキームの妥当性検証
   - 机上検討とシミュレーションで策定された認証マーク制度の案が、実環境で実施可能かを確認する必要がある
   - 一連の認証プロセスにかかる必要な費用と期間を確認する必要がある
   - 自主検証者および第三者検証者の認定要件を定義する必要がある

2. 対象とする製品機器を検討・選定
   - 今回の調査では限られたサンプルでのシミュレーションであったので、より多くのトライアル検証を実施し、幅広い分野のIoT機器に対する認証が可能か、認証対象として適正な製品範囲を確認する必要がある

⇒ **上記１．２を鑑みて認証スキーム実証実験の実施が必要と思われる**

７．認証マーク策定に向けた今後の取り組み（２）

3. 認証マーク取得要件を最終的に決定する中立的な有識者委員会の設置
   - 統計的な見地、有識者・業界からの意見を参考に策定した認証要件(案)を、今後のセキュリティ環境の変化や実証実験の結果から本格運用に入る際の認証要件として確定させる必要がある

4. 業界横断的な意見を集約する場の設置
   - 今回のヒアリング調査は４社と限定的であったので、広く業界の意見を集め、制度に反映させる必要がある

5. 認証マーク制度を普及させるための取り組み検討
   - IoT機器利用者やIoT調達機関への認証マーク取得認知度向上キャンペーン
   - 認証製品導入の税制優遇や政府調達要件への追加など、認証取得促進策
   - IoTセキュリティ評価業務増加に備えた検証エンジニアの人材育成など