第3回テクノロジーベースの規制改革推進委員会資料

IoTセキュリティ対策への新たな取り組みのご紹介と一提案

～認証製品へのラベリング（マーク制度）始まってます！～

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

CCDSの概要

- 名称：一般社団法人 重要生活機器連携セキュリティ協議会
  - 英名：Connected Consumer Device Security council (CCDS)
- 設立：2014年10月6日
- 会長：徳田英幸（情報通信研究機構　理事長、慶応大学 名誉教授）
- 代表理事：荻野 司（情報セキュリティ大学院大学　客員教授）
- 理事：後藤厚宏（情報セキュリティ大学院大学 学長、SIP：PD）
  松本 勉（横浜国立大学先端科学高等研究院 教授）

- 会員数：216（正会員以上：58、一般会員：122、学術系：19、協賛:17）(2022年1月)

- 主な事業：
  1. 生活機器の各分野におけるセキュリティに関する国内外の動向調査、内外諸団体との交流・協力
  2. 生活機器の安全と安心を両立するセキュリティ技術の開発
  3. セキュリティ設計プロセスの開発や検証方法のガイドラインの開発、策定および国際標準化の推進
  4. 生活機器の検証環境の整備・運用管理及び検証事業、セキュリティに関する人材育成や広報・普及啓発活動等

第三者認証制度に求められる条件の比較

■ 第三者認証制度に求められる４条件の比較

No.	条　件	ISO15408	CCDSｻｰﾃｨﾌｨｹｰｼｮﾝﾌﾟﾛｸﾞﾗﾑ
条件１	分かりやすい	△ ・難解なセキュリティ設計仕様書の理解が必要	○ ・対策レベル絶対的基準の導入 ・一目で識別できるマーク制度
条件２	信頼できる	○～△ ・セキュリティ設計仕様書に依存	○ ・対策エビデンスの追跡可能性 ・外部有識者による要件レビュー ・指定検査資格制度とサイバー保険付帯
条件３	普及しやすい(低コスト)	× ・認証費用が数千万円～1億円超	○ ・自主検査と第三者検証の組合せ ・低コスト認証費用 (45万円～※)
条件４	新攻撃に追従しやすい	× ・認証更新費用が高額	○ ・セキュリティ要件の毎年見直し

※ CCDS幹事会員・正会員以外の申請者に初年度掛かる費用

国内外におけるIoTセキュリティの標準化動向

■2019年以降、日米欧において規格、標準化が加速

法制化関連施策　標準やガイドライン

日本

2017年
- 改正個人保護法施行
- 医療情報システムの安全管理に関するガイドライン第5版

2018年
- 電気通信事業法の技術基準適合認定にセキュリティ要件追加の提案

2019年
- パブコメ募集
- サイバー・フィジカル・セキュリティ対策フレームワーク

2020年
- 技適適合基準施行
  - ４つのセキュリティ要件義務化

2021年

2022年
- 5G促進法成立

米国

2017年
- IoT Cybersecurity Act 2017法案提出
  - 政府調達条件を規定

2018年
- NIST IR8200 (草稿)
  - 目的、リスク、脅威の分析、国際標準化状況
- カリフォルニア州 IoTセキュリティ法 成立

2019年
- IoT Cybersecurity Improvement Act 2019法案

2020年
- NIST IR 8259 (最終版)
  - 政府調達に適切な管理推奨事項
- カリフォルニア州 SB327 施行
  - 共通の初期パスワード禁止等

2021年
- IoT Cybersecurity Act 2020法
  - 政府調達機器セキュリティ規制強化
- Executive Order 14028
  - サイバーセキュリティ大統領令(コンシューマ機器)

2022年
- 消費者向けIoT製品のサイバーセキュリティラベリング推奨基準
- 消費者向けソフトウェアサイバーセキュリティラベリング推奨基準
  - ラベリング推奨(認証) 基準
- NIST IR8425 (最終版)
  - 消費者向けIoT機器最低限要件

※ NIST: 米国標準技術研究所
※ IR: Internal Report

欧州

2017年
- サイバーセキュリティ認証フレームワーク導入検討を公表
- ENISA IoTベースラインセキュリティ推奨事項を発表

2018年
- EU一般データ保護規則(GDPR)施行

2019年
- 英政府コンシューマIoT向けセキュリティ行動規範13箇条
  - コンシューマ機器の最低限のセキュリティ要件

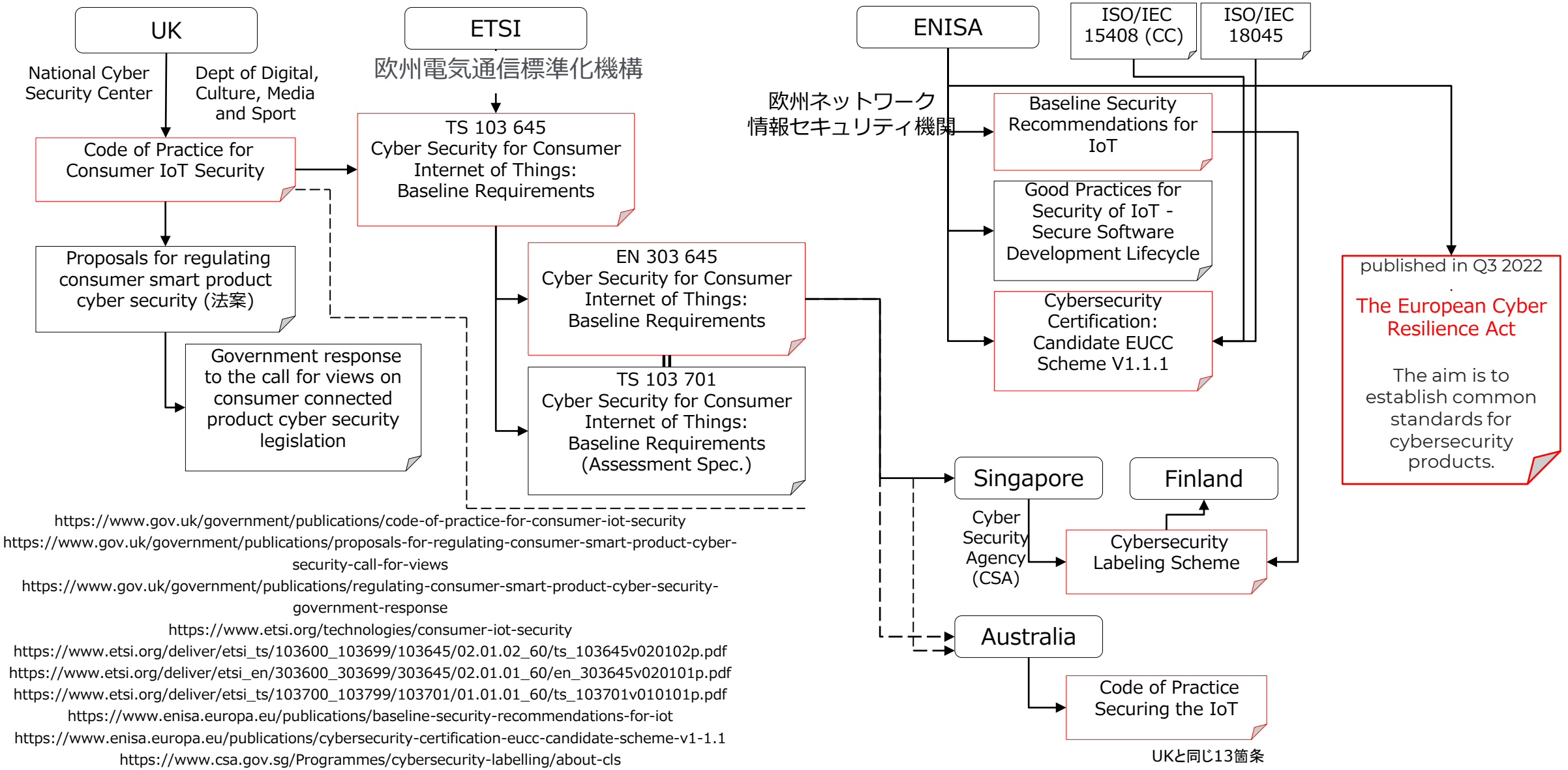
2020年
- ETSI EN 303 645 Cyber Security for Consumer IoT
  - 英政府行動規範のEU版

2021年
- ETSI TS 103 701
  - EN303 645のテストシナリオ
- ENISA Guidelines for Securing the Internet of Things
  - IoT製品サプライチェーン保護のためのガイドライン

2022年
- 欧州連合官報RED委任規制
  - 無線機器にセキュリティ要件追加
- サイバー・レジリエンス法案
  - ネットワーク接続機器にサイバー攻撃対策を義務化

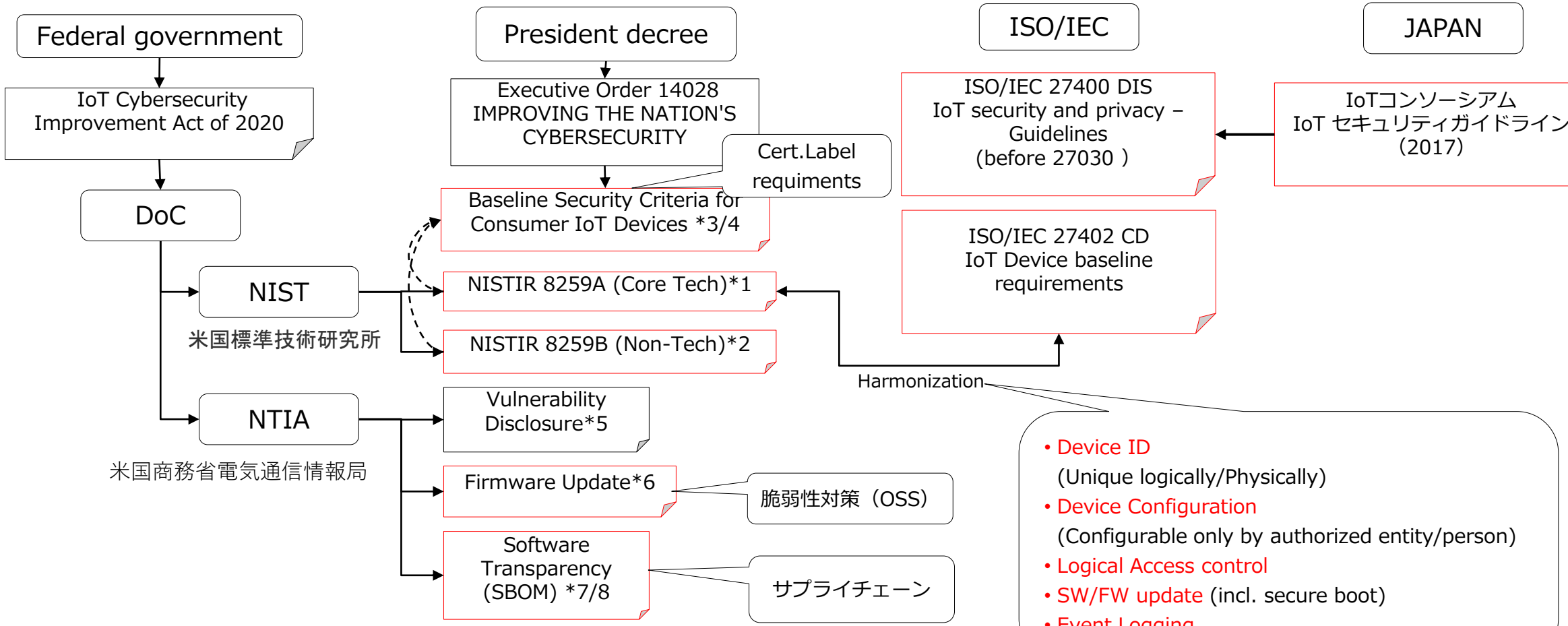
※ ENISA: 欧州ネットワーク情報セキュリティ庁
※ ETSI:　欧州電気通信標準化機構

EURO overview,etc



https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security
https://www.gov.uk/government/publications/proposals-for-regulating-consumer-smart-product-cyber-security-call-for-views
https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response
https://www.etsi.org/technologies/consumer-iot-security
https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf
https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
https://www.etsi.org/deliver/etsi_ts/103700_103799/103701/01.01.01_60/ts_103701v010101p.pdf
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot
https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1
https://www.csa.gov.sg/Programmes/cybersecurity-labelling/about-cls
https://www.homeaffairs.gov.au/reports-and-pubs/files/code-of-practice.pdf

USA/ISO/IEC/日本　overview



[1] https://csrc.nist.gov/publications/detail/nistir/8259a/final
[2] https://csrc.nist.gov/publications/detail/nistir/8259b/final
[3] https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-device-criteria
[4] https://www.ntia.gov/IoTSecurity
[5] https://www.ntia.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities
[6] https://www.ntia.doc.gov/files/ntia/publications/ntia_iot_security_update_framework.pdf
[7] https://www.ntia.doc.gov/files/ntia/publications/standards_and_formats_june_27_update.pdf
[8] https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf

IoT機器のセキュリティ機能やソフトウェア開発手法について、一般の人々を教育するためのパイロットプログラムを開始することになった

IoT機器セキュリティ認証スキームのポイント

ポイント１：つまるところベースライン要件は、ほぼ変わらい。
ー＞日本案は、日本のメーカや消費者にとって最適に設定すべきであろう
（ETSI,NIST,あまり変わらない）

ポイント２：経年変化するセキュリティなので、要件・適合基準は鮮度が重要。
ー＞柔軟に要件・適合基準をアップデートできる仕組み
（非営利組織で柔軟に動ける体制が寛容）

ポイント３：標準化は、たいていはプロセスチェック重視なのでドキュメント
チェックが多く認証にかかるコストが増大する（重くなる）
ー＞軽い検査プロセスが重要。
適合基準を我が国として作成することが重要。（経済安全保障）

ポイント４：社会実装：使われることに意味がある。メーカー賛同し消費者が受け入れる
ー＞双方にインセンティブが必要
メーカ：認証にかかるコストを安価に！そして購買意欲につながる！
ユーザー：安心・安全の視覚化、加えて分かるメリットetc.(ex.サイバー保険とか)

CCDS　IoTセキュリティガイドライン整備状況　～社会実装～

CCDS外の動きや国際標準化の動き

提案 → **ISO/IEC 27400提案** IoT security and privacy – Guidelines → 標準化 → **ISO/IEC 27400** IoT security and privacy – Guidelines

IoTセキュリティ一般的枠組 **NISC** → 各種ガイドライン（文書）発行

参照

提案 → IoTセキュリティガイドラインV1.0 **IoT推進コンソ 総務省 経済産業省**

医療情報システムの安全管理に関するガイドライン第5版 **厚生労働省**

サイバー・フィジカルセキュリティ対策フレームワーク **経済産業省**

提案 → **ISO/IEC 30147** Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes

協力 つながる世界の開発指針 IPA

CCDS認証マーク例

CCDS内の動きや文書発行

2016年
- 車載機編ガイドライン V1.0
- IoT-GW編ガイドライン V1.0
- ATM編ガイドライン V1.0
- オープンPOS編ガイドライン V1.0
- 分野別ガイドライン V1.0

2017年
- 分野別ガイドライン V2.0
- 分野別ガイドライン V2.0別冊
- 分野別ガイドライン V1.0英語版
- 分野別ガイドライン V2.0英語版
- 評価検証ガイド v1.0

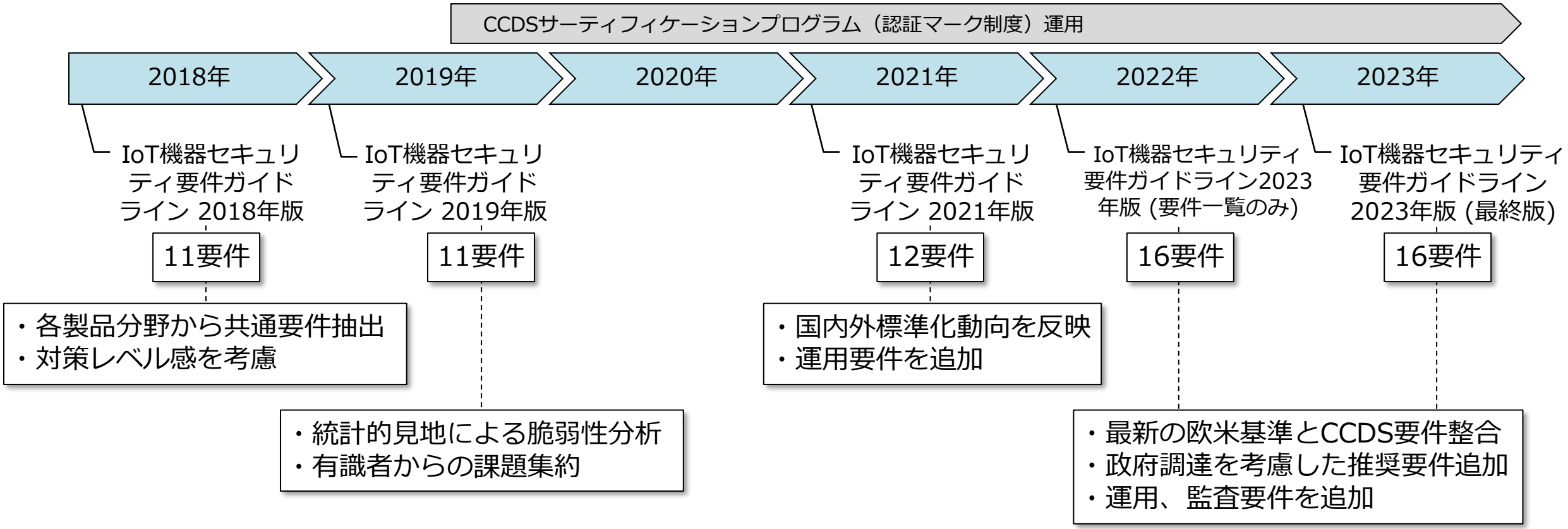
2018年
- IoT分野共通セキュリティ要件ガイドライン_2018年版
- CCDS 調達仕様編 草稿

2019年
認証マーク制度運用開始
- IoT分野共通セキュリティ要件ガイドライン_2019年版
- IoT分野共通セキュリティ要件ガイドライン_2019年_別冊～解説編
- CCDS スマートホーム編 V1.0

2020年
認証マーク**制度のサービスへの適用開始**
- IoT機器セキュリティ要件ガイドライン_2021年版
- IoT機器セキュリティ要件ガイドライン_2021年版_別冊～解説編
- IoT機器セキュリティ要件_2021年版_対策方針チェックリスト_v1.0
- CCDS アップデート機能編
- CCDS ATM勉強会報告書

CCDS IoT機器セキュリティ要件の変遷　～社会実装～

・世界動向より先行し、 CCDSは2018年よりIoTセキュリティ要件の策定に着手すると共に、
世界の規格・標準化動向や、サイバー攻撃の傾向を踏まえて継続的に要件更新。



コンシューマ機器のセキュリティ対策に関する欧米動向

▲ 英国 コンシューマIoTセキュリティ行動規範

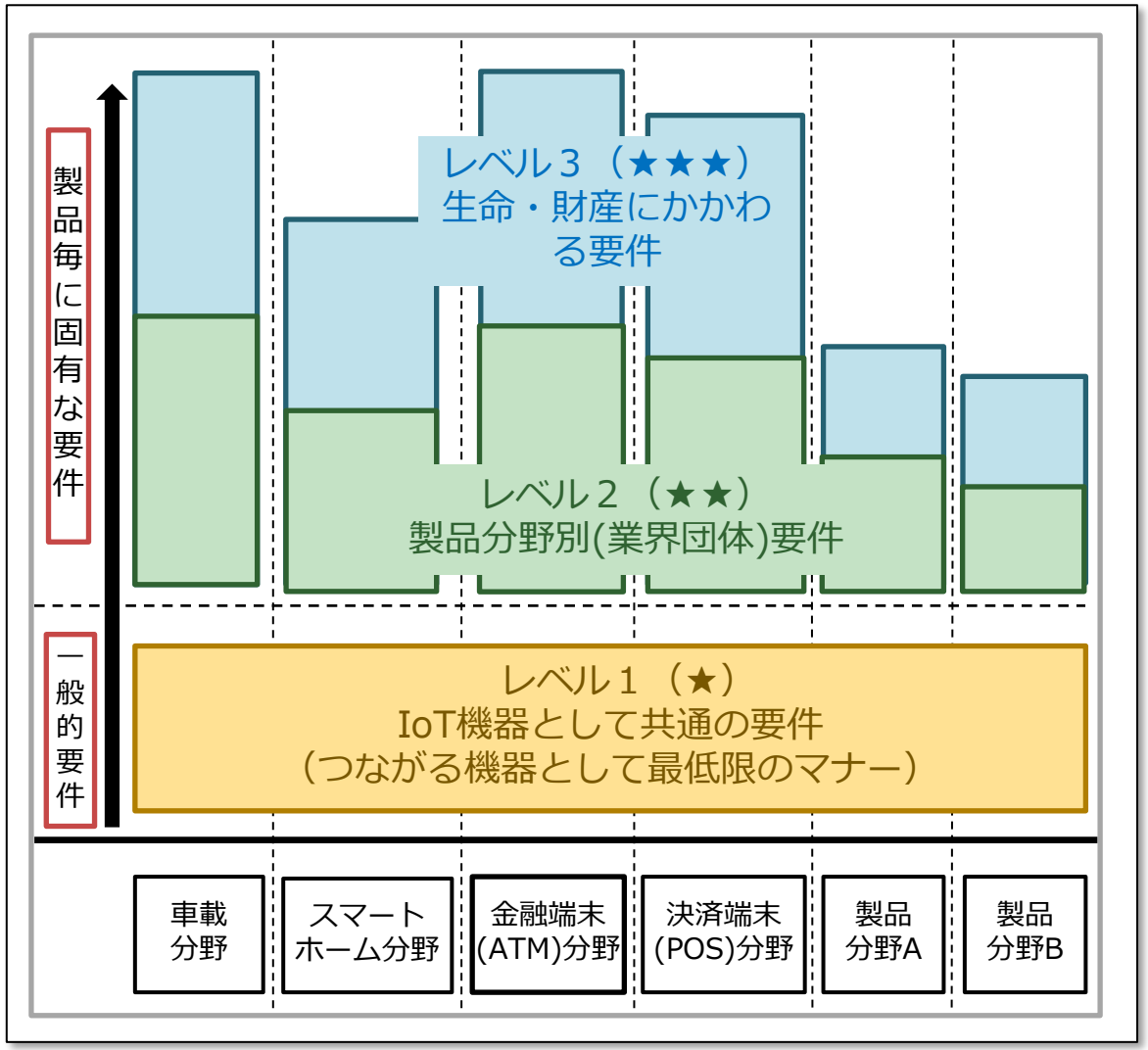
▲ 欧州 ETSI EN 303 645

▲米国 NIST IR8425
(IoT機器の認証要件)

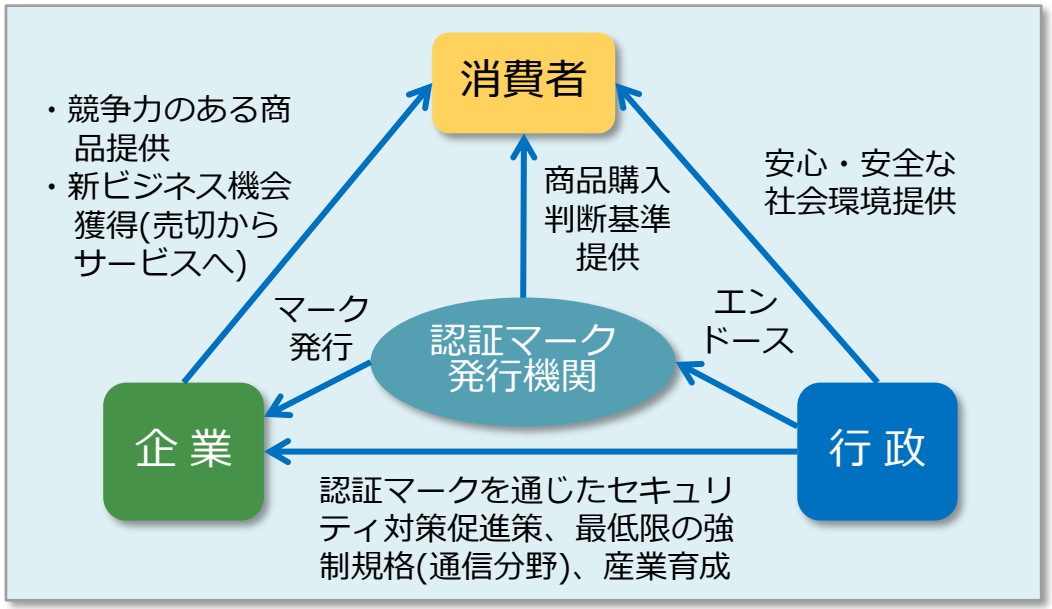
※ NIST: 米国標準技術研究所
※ IR: Internal Report
※ ETSI: 欧州電気通信標準化機構

CCDSサーティフィケーションプログラムの概要

プログラムのレベル構成



プログラムのスキーム



プログラムのポイント

1. 任意マーク（罰則なし）
2. 自主検査と第三者検査のいずれか選択可能
3. 第三者機関によるマーク付与の意味（検証結果保持と追跡可能）
4. マークの毎年更新（新規攻撃への対応）
5. セキュリティ対策の普及促進策　⇒　例えば税制優遇、助成金

マークに自動付帯するIoTサイバー保険の概要

・マーク取得機器を対象に、IoTサイバー保険が自動付帯される
（保険契約はCCDSが行い、マーク取得者による契約や保険費用負担は不要）

・インシデント発生時に、マーク取得者（ベンダ）の原因調査費用、損害賠償費用、その他費用を補償する。（間接的に機器利用者を保護する）

安心・安全なIoT機器を選択するための指標

マークによって、分野を問わず最低限守るべき要件を満たしていることが確認できるため、ユーザーがIoT機器を購入する際に選択の指標となります。

フォレンジック調査等、様々な費用・損害を保険で補償します。

原因調査

インシデントの発生またはそのおそれがある場合、迅速に調査を実施します。

損害賠償金

メーカーに損失が発生する場合、賠償金をお支払いします。

その他費用損害

損害拡大防止・再発防止費用等、インシデントに起因する費用を幅広く補償します。

＋

事故時専門業者紹介サービス

サイバーセキュリティに関する事故が発生した際、CCDS・三井住友海上が迅速に専門業者を紹介いたします。

認証スキーム（CCDS版）

- **民間による認証スキームオーナ：経年劣化するセキュリティ対策への対応**
  - セキュリティ要件（認証要件）：ほぼ欧米と同基準で実施可能までコンセンサスはとれてきている
  - 適合基準（検査手法、基準）：日本にあった適切な基準作りを目指している
- **ラベル効果**
  - 消費者への購入時支援、メーカへのインセンティブ
- **サイバー保険適用：社会的なセーフティネット**
  - インシデント時への迅速な対応を支援（消費者支援、メーカ支援）
- **第三者認証＆（自己検査or第三者検査）**
  - メーカ内の品質保証部門の教育もかねて、教育＆資格認定プログラムを策定
  - 第三者検証事業者が育ってくれば自己検査から第三者検査にアウトソースする流れになるであろう

適合基準（試験仕様書、試験シナリオ）を策定・提供
・柔軟に改定できるように毎月WGを開催し検討をしている。
試験ツールの提供（OSSベース）：各種フリーソフトを統合化した検査ツールによる自動試験

参考として：IPv6 Ready Logo Program（IPv6 forum:議長　東京大学　江崎浩　教授）
・IPv6 認定対象機器:ルータをはじめとした通信機器や、パソコン・IP 電話機等の通信端末、組み込みソフト（プロトコルスタック）、OS（Windows Vista）等がある。
・適合性および相互運用性テストのテスト仕様を定義、セルフテスト ツールの提供、IPv6 Ready Logo を提供。
（仕様適合性検査：試験仕様書、相互接続性検査：試験シナリオ）
https://www.ipv6ready.org/index.html

サーティフィケーションの取得実績・予定　～社会実装～

■現在までの取得実績

レベル	企業名	製品・サービス名称	型式番号	製品URL	登録日
Lv.1（★）	株式会社JVCケンウッド	CONNECTED CAM	GY-HC900CH	製品HP	2020/4/1
Lv.1（★）	オムロンソーシアルソリューションズ株式会社	CATS300/900 Base ユニット	3M8CR-Base	製品HP	2020/5/11
Lv.1（★）	文化シヤッター株式会社	ワイヤレス通信機２	SCX1801	製品HP	2020/5/15
Lv.1（★）	リンナイ株式会社	無線LAN 対応リモコン	MC-301Vシリーズ/MC-302Vシリーズ	製品HP	2021/1/22
Lv.1（★）	株式会社アルファ	電気錠操作盤	WS800-W-SH-PFH（Cn-83）	製品HP	2021/1/22
Lv.1（★）	日立チャネルソリューションズ株式会社	自動受付精算機	–	製品HP	2021/1/22
Lv.2（★★）	積水ハウス株式会社	PLATFORM HOUSE touch	–	サービスHP	2021/8/2

■2022年以降の取得候補

マーク発行累積は2019年以降増大しており、
2021年後半からスマートホーム関連機器が増大

発行数量も数千台～数万台へと拡大中

レベル	対象製品	予定されている製品数
Lv.1（★）	ATM端末	3製品
Lv.1（★）	情報ネットワーク機器	1製品
Lv.1（★）	スマートホーム関連機器	3製品
Lv.1（★）	POS端末	2製品
Lv.2（★★）	ATM端末	3製品
Lv.2（★★）	POS端末	2製品
Lv.3（★★★）	スマートホームサービス	1サービス

ブランディング戦略として活用　コストから投資へ

プラットフォームハウス　タッチ

「PLATFORM HOUSE touch」

SH02-2021 CCDS 2021 ★★ Security Certification

PFHデータベース

住環境

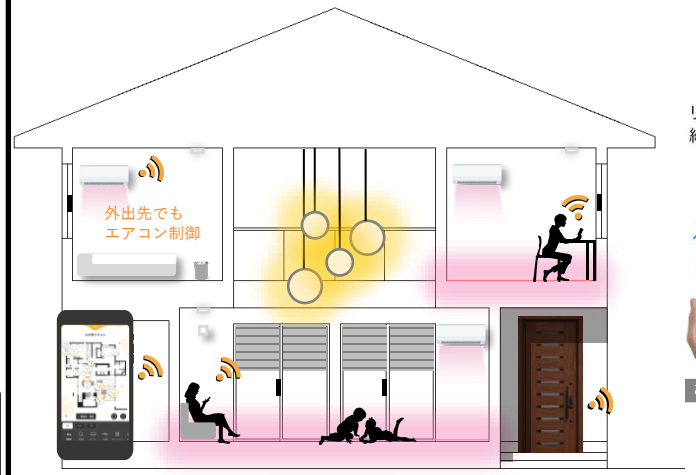
ライフスタイル

＋

企業・自治体と
アライアンス

Benefit　住まい手ひとりひとりに

スマートハウス（積水ハウス）＋住設メーカ（文化シャッター、リンナイ、アルファーなど）



リンナイ株式会社
給湯リモコン　MC-301VC(A)/302VC(A)・・・どこでもリンナイアプリ

Rinnai

シャッター株式会社
用窓シャッター　マドマスター・スマートタイプ

スマートフォンで窓シャッターの操作や状態確認ができます。
HEMSやスマートスピーカーとも連携が可能です。

BX 文化シャッター

ヤレス通信機２
式：SCX1801
ーク取得対象機器）

個別操作・一斉操作　状態通知機能
半開操作　お好みタイマー・おひさまタイマー
HEMS連携　スマートスピーカー連携

まとめ

ポイント１：セキュリティ要件の整理・情報提供

ー＞国際的な協調をとりながら、日本のメーカや消費者にとって最適な要件を策定する。

認証・検証スキームのベストプラクティスを公開し日本が積極的に世界へ貢献（できるハズ）

ポイント２：運用経験の共有：社会実装：使われることに意味がある。

ー＞メーカと消費者の双方にインセンティブが必要

メーカ：認証・検証にかかるコストを安価に！そして購買意欲につながる！

ユーザー：安心・安全の視覚化、加えて分かるメリットetc.(ex.サイバー保険とか)

ラベリング（マーク）付与ー＞技術マップへの認証・検証マークの掲載を提案！

ポイント３：検証体制：経年変化するセキュリティなので、要件・適合基準は鮮度が重要。

ー＞柔軟に要件・適合基準をアップデートできる仕組み。

（民主導で柔軟に動ける体制　IPv6redylogo、CCDS 認証マーク）

ポイント４：KPIからKGIへ（経済安全保障、カーボンニュートラル）

ー＞技術適合基準を我が国として作成することが重要（経済安全保障）

ex. ZEH net Zero Energy House スマートハウスとしてエコで安全ー＞ブランディング

お知らせ

■IoT 機器セキュリティ要件ガイドライン （2023）
ーー守るべき要件とその背景（脅威、事例）ーー
■IoT 機器セキュリティ適合基準ガイドライン（2023）
ーー合格基準、検査方法ーー

■適合基準ガイドライン2023年版_ANNEX1_海外セキュリティ要件との対応資料
（https://www.ccds.or.jp/public_document/index.html#GR01-2023）