「IoTセキュリティにおける守るべき要件について」
～国際動向について解説する～

情報セキュリティ大学院大学
一般社団法人　重要生活機器連携セキュリティ協議会
客員教授/代表理事　荻野　司

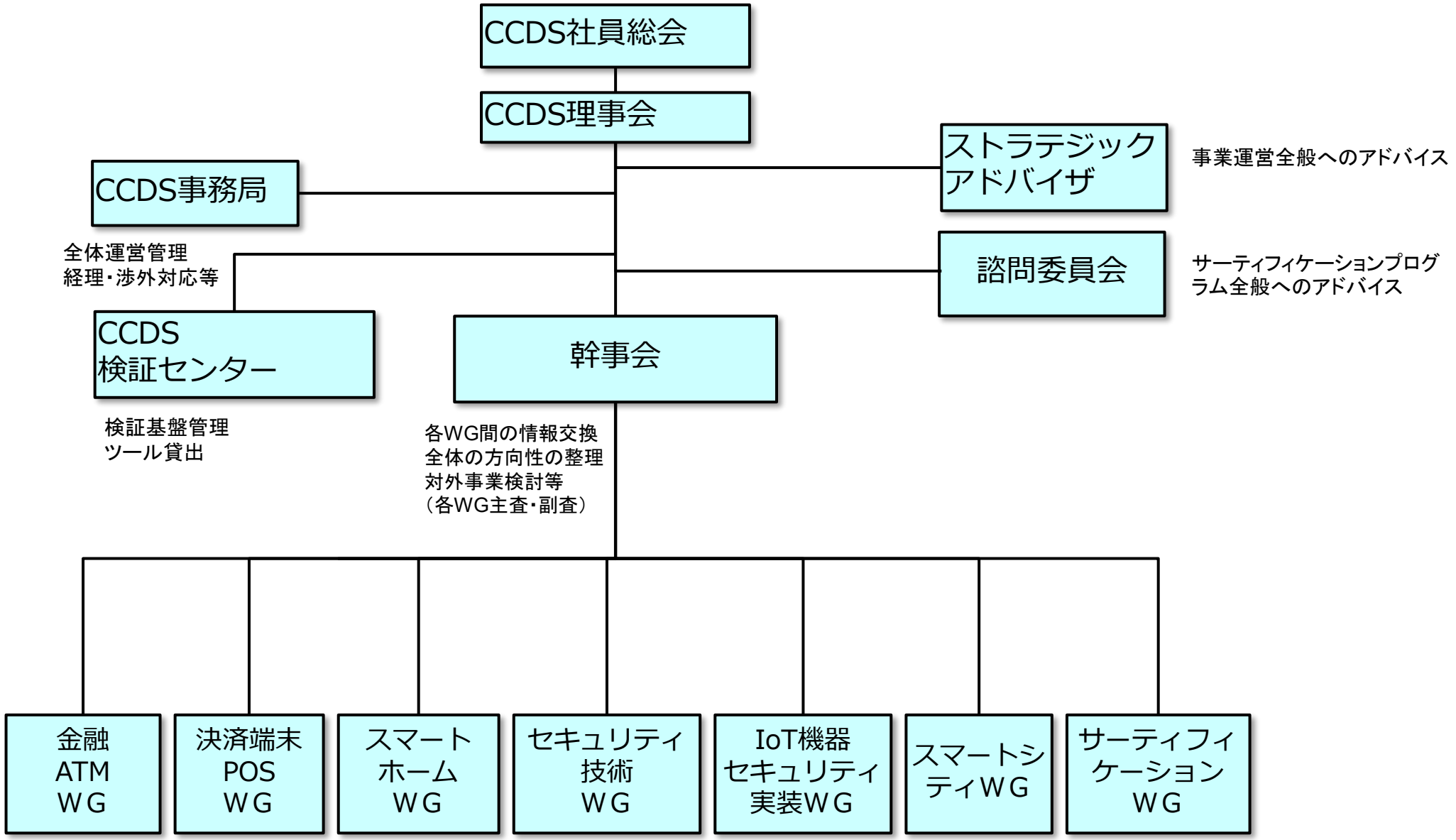
CCDSの概要

- 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）(2021年11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

2021年度　運営体制


CCDS社員総会
CCDS理事会
CCDS事務局
全体運営管理
経理・渉外対応等
ストラテジック
アドバイザ
事業運営全般へのアドバイス
諮問委員会
サーティフィケーションプログラム全般へのアドバイス
CCDS
検証センター
検証基盤管理
ツール貸出
幹事会
各WG間の情報交換
全体の方向性の整理
対外事業検討等
（各WG主査・副査）
金融
ATM
WG
決済端末
POS
WG
スマート
ホーム
WG
セキュリティ
技術
WG
IoT機器
セキュリティ
実装WG
スマートシ
ティWG
サーティフィ
ケーション
WG

IoTセキュリティを取り巻く各国の動向

ガイドライン提案加速

法規制に向けて

	2014年	2015年	2016年	2017年	2018年	2019年	2020年
日本	11月 サイバーセキュリティ基本法 サイバーセキュリティを推進するための基本理念や国の責務等を定めた情報セキュリティ戦略の基盤となる法律	12月 サイバーセキュリティ経営ガイドライン 企業経営者を対象に対策を推進するためのリーダーシップのとりかたについてガイドラインを策定	7月 IoTセキュリティガイドライン IoTセキュリティに関する指針と一般利用者のためのルールを策定	5月 改正個人情報保護法施行 個人情報の取扱いに関するルールが10年ぶりに改正され施行された 5月 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 医療機関等を対象とするサイバー攻撃やIoT等の新技術への対応として改定	6月 技適にセキュリティ要件追加提案 マルウェアの感染によりIoT機器がボットネット化しないための要件を追加 11月 技適へのセキュリティ要件追加パブコメ	8月-2019年4月 サイバー・フィジカル・セキュリティ対策フレームワークを策定	4月 技術適合要件施行
米国	2月 サイバーセキュリティフレームワーク公表 NISTがサーバーセキュリティ対策の全体像を示すフレームワークを公表			8月 IoT Cybersecurity Act 2017法案提出 IoT製品の政府調達条件を規定 12月 改訂版	2月 NISTIR8200 (Draft)公表 5つのユースケースに対するIoTサイバーセキュリティの目的、リスク、脅威の分析、国際標準化状況を整理した 9月 米国加州でIoTセキュリティ法成立	5月 IoT Cybersecurity Improvement Act 2019法案提出 1月 加州SB327施行	3末 連邦政府調達に適切な管理推奨事項を明確化(NIST) NISTIR 8259DRAFT
EU	9月 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 11月 ENISAがIoTのベースラインセキュリティ推奨事項を発表				5月 EU一般データ保護規則(GDPR)施行 EU加盟28カ国およびアイスランド、リヒテンシュタイン、ノルウェー）の個人データ保護を目的とした管理規則 10月 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	2018/5-2019/2 ETSI TS 103 645 Cyber Security for Consumer IoT	

ISO/IEC 27400,27402

近年、IoTセキュリティに関連する法規制、ガイドラインなどが各国から出されており、これらへ対応していかないとビジネスに影響を及ぼしつつある。

国内外のセキュリティ動向

日本

2019年10月、JTC1/SC27、SC41において原案（CD化）※継続中
ISO/IEC 27030 Information technology — Security techniques — Guidelines for security and privacy in Internet of Things(IoT) [DRAFT]

※2016年7月 IoT推進コンソーシアムの「IoTセキュリティガイドライン」をベースに、ISO/IEC JTC1/SC27の規格(27030)として、国際標準化のトラックにて進行中。

2018年7月策定
NISC 政府機関等の対策基準策定のためのガイドライン（平成30年度版）

※政府機関等の情報セキュリティ対策の統一基準
※第６部には、情報システムのセキュリティ要件を記載（調達要件）

2016年10月公開
NISC 外部委託等における情報セキュリティ上のサプライチェーン・リスク対応のための仕様書策定手引書

※CCDSを含め、多くのIoT関連ガイドラインの基本指針

国際標準化文書

2013年8月公開
ISO/IEC 27001:2013 情報セキュリティマネジメントシステムー要求事項

2015年12月公開
ISO/IEC 27017:2015
ISO/IEC 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践と規範

米国

2020年12月 法制度として成立（法案提出：2019年3月）
The IoT Cybersecurity Improvement Act

※①NISTがIoTデバイスの安全な開発、ID管理、パッチ適用、および構成管理などのガイドラインを発行
※②アメリカ合衆国行政管理予算局（OMB)がガイドラインに基づく活動を行っているかをチェック

詳細定義

2020年5月公開（Final版）
NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufactures

※ IoTデバイス製造者向けの活動指針

2020年5月公開
NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline

※IoTデバイスのセキュリティ要求事項

欧州

2016年6月発行
Cybersecurity Act 欧州サイバーセキュリティ認証フレームワーク

※ICT製品、サービス等を対象にサイバーセキュリティ認証スキームを検討中
（ENISAよりCCを参照した候補スキームのDRAFTが提示）

2019年7月法制度として成立、2020年12月NIS指定2として法案提出
Network and Information Systems Directive（NIS指令）

※①国家レベルでのサイバーセキュリティ能力向上。
※②EUレベルの協力強化。
※③重要インフラ事業者やデジタルサービス提供者等に対するリスクマネジメントやインシデント報告義務化
（2020年12月発表）

2020年6月公開（Final版）
ETSI EN 303 645 Cyber Security for Consumer Internet of Things

※IoTコンシューマ向けのグローバルIoTセキュリティ標準として公開

ISO/IEC 27400　DIS（Draft International Standard）ファイナルの一歩手前

- タイトル：IoT security and privacy – Guidelines
- 概要：IoTソリューションのセキュリティとプライバシーに関するリスク、原則、コントロール（対策）に関するガイドラインを提供
- 対象：IoTサービスプロバイダ、IoTサービス開発者、IoTユーザ
- トピック
  - 2017年：総務省・経産省のIoTセキュリティガイドラインv1.0を提案
  - 上記をベースにドラフト案では、プライバシー要件が追加されて標準化を進めている

ISO/IEC 27402CD（Committee Draft）

- タイトル： IoT security and privacy –Device baseline requirements
- 概要：IoT機器とその製造者の情報セキュリティとプライバシーに関するコントロール（対策）をサポートするためのベースライン要件を提供するもの
- 対象： IoT機器とその製造者
- トピック
  - 2019年：米国発案

つながる世界の開発指針（ISO/IEC 30147 として発効）

■ 2021年5月

ISO/IEC 30147：2021 Internet of Things (IoT) –

Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes

IoT製品・サービスにセーフティ・セキュリティ等を実装するプロセスが国際標準として出版

～日本提案の規格が国際標準化団体ISO/IECにて出版～
IPA 独立行政法人 情報処理推進機構

https://www.ipa.go.jp/ikc/info/20210621.html

「つながる世界の開発指針」の特徴

■安全・安心なIoTを実現するために、IoT製品やシステムの開発者が開発時に考慮すべきリスクや対策を17の指針として明確化

■IoTに関連する様々な製品分野・業界において分野横断的に活用されることを想定

■IoT製品・システムの安全性・セキュリティに関して分野横断的に活用可能な国内初の開発指針

※本開発指針は、2016年3月24日に公開（PDF版）
http://www.ipa.go.jp/sec/reports/20160324.html

米国IoTセキュリティの動向

米連邦政府

2020.12.4
The IoT Cybersecurity Improvement Act 2020
米国連邦法「IoTサイバーセキュリティ改善法」成立（法案提出：2019年3月）

文書整備

NIST

2020.05.29 FINAL
NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufactures
「IoTデバイス製造事業者向け 基本的なサイバーセキュリティ活動」

2020.5.29 FINAL
NISTIR 8259A IoT Device Cybersecurity Capability Core Baseline
「IoTデバイスのサイバーセキュリティ機能のコアベースライン」

2021.8.25 FINAL
NISTIR 8259B IoT Non-Technical Supporting Capability Core Baseline
「IoT非技術的サポート機能のコアベースライン」

2020.12.15 DRAFT
NISTIR 8259C (Draft) Creating a Profile Using the IoT Core Baseline and Non-Technical Baseline
「IoTコアベースラインと非技術ベースラインを使用したプロファイルの作成」

2020.12.15 DRAFT
NISTIR 8259D (Draft) Profile Using the IoT Core Baseline and Non-Technical Baseline for the Federal Government
「連邦政府向け IoTコアベースラインと非技術ベースラインを使用したプロファイル」

2020.12.15 DRAFT
SP 800-213 (Draft) IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements
「連邦政府向けのIoTデバイスサイバーセキュリティガイダンス」

参照・詳細定義

大統領

2021.05.12
Executive Order 14028
Improving the Nation's Cybersecurity

文書整備

2021.08.31 DRAFT
DRAFT Baseline Security Criteria for Consumer IoT Devices

2021.12.3 DRAFT
Consumer Cybersecurity Labeling for IoT Products:
Discussion Draft on the Path Forward

2022.2.4 FINAL
Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products

2022.2.4 FINAL
Recommended Criteria for Cybersecurity Labeling of Consumer Software

IoTセキュリティを取り巻く各国の動向

ガイドライン提案加速

法規制に向けて

	2014年	2015年	2016年	2017年	2018年	2019年	2020年
日本	11月 サイバーセキュリティ基本法 サイバーセキュリティを推進するための基本理念や国の責務等を定めた情報セキュリティ戦略の基盤となる法律	12月 サイバーセキュリティ経営ガイドライン 企業経営者を対象に対策を推進するためのリーダーシップのとりかたについてガイドラインを策定	7月 IoTセキュリティガイドライン IoTセキュリティに関する指針と一般利用者のためのルールを策定	5月 改正個人情報保護法施行 個人情報の取扱いに関するルールが10年ぶりに改正され施行された 5月 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 医療機関等を対象とするサイバー攻撃やIoT等の新技術への対応として改定	6月 技適にセキュリティ要件追加提案 マルウェアの感染によりIoT機器がボットネット化しないための要件を追加 11月 技適へのセキュリティ要件追加パブコメ	8月-2019年4月 サイバー・フィジカル・セキュリティ対策フレームワークを策定	4月 技術適合要件施行
米国	2月 サイバーセキュリティフレームワーク公表 NISTがサーバーセキュリティ対策の全体像を示すフレームワークを公表			8月 IoT Cybersecurity Act 2017法案提出 IoT製品の政府調達条件を規定 12月 改訂版	2月 NISTIR8200 (Draft)公表 5つのユースケースに対するIoTサイバーセキュリティの目的、リスク、脅威の分析、国際標準化状況を整理した 9月 米国加州でIoTセキュリティ法成立	5月 IoT Cybersecurity Improvement Act 2019法案提出 1月 加州SB327施行	3末 連邦政府調達に適切な管理推奨事項を明確化(NIST) NISTIR 8259DRAFT
EU				9月 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 11月 ENISAがIoTのベースラインセキュリティ推奨事項を発表	5月 EU一般データ保護規則(GDPR)施行 EU加盟28カ国およびアイスランド、リヒテンシュタイン、ノルウェー）の個人データ保護を目的とした管理規則 10月 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	2018/5-2019/2 ETSI TS 103 645 Cyber Security for Consumer IoT	

ISO/IEC 27400,27402

近年、IoTセキュリティに関連する法規制、ガイドラインなどが各国から出されており、これらへ対応していかないとビジネスに影響を及ぼしつつある。

NISTからの新たなIoTセキュリティ関連ドキュメント公開

■NIST公開文書　「 IoT Device Criteria」について

■ NISTは、サイバーセキュリティに関する大統領令（2021/5/21発行の14028）を受けて、IoTデバイスに関するラベリングプログラムの基準案を記載したホワイトペーパーを2021/8/31にリリースした。

■ IoT Device Criteriaは、下記３つの表にて、対応基準を記載。

表１）IR8259Aを詳細化したIoT製品のサイバーセキュリティ機能：７項目

表２） IR8259Bを詳細化した組織、運用に関する非技術的項目：４項目

表３）複数のIoT製品で補い合うことのできる追加機能：７項目（表１の各項目へ追加）

・参考）NISTのHP URL：

https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-device-criteria

■CCDSの対応

■ NISTでは、ホワイトペーパーの草案に関するパブリックコメントを10/17まで募集している。CCDSは日本における取組の事例として、「IoT機器セキュリティ要件ガイドライン（2021年版）」の英訳版をインプットする。

NIST公開文書「IoT Product Criteria」の概要について①

・NISTは、サイバーセキュリティに関する大統領令（2021/5/21発行の14028）を受けて
NIST発行された「IoT Device Criteria」に関する続報となる。

① 2021/8/31リリース：「 IoT Device Criteria」
→IoTデバイスに関するラベリングプログラムの基準案のDRAFT文書
※第3回幹事会にてご報告

②【NEW】2021/12/3リリース：「 IoT Product Criteria」
「 **Consumer Cybersecurity Labeling for IoT Products:　Discussion Draft on the Path Forward** 」
（IoT製品の消費者サイバーセキュリティラベリング：今後のディスカッションドラフト）

2022.2.4 FINAL
Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products

2022.2.4 FINAL
Recommended Criteria for Cybersecurity Labeling of Consumer Software

■概要

・「IoT Device Criteria」のFinal版文書として発行。
・Final版では、IoT製品の「消費者向け」サイバーセキュリティラベリングの基準である事を明確化し、
名称を「**IoT Product Criteria**」へと変更
・Draft版の「IoT Device Criteria」では別表として分割していた表１（8259Aを参照したデバイスのサイバーセキュリティ機能）と表２（8259Bを参照した非技術的なサポート機能）が、統合されている。
・デバイスのサイバーセキュリティ機能より「製品のセキュリティ」の項目が削除。
・その他の基本構成に大きな差異はないが、一部クライテリア（基準）が緩和、抽象化されている。
・新たに章が追加され、ラベリング基準の目指す方向性や目的（消費者の購入決定を支援など）のDRAFT案が記載されている。

参考）NISTのHP URL：
https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/iot-product-criteria

CCDS　IoTセキュリティガイドライン整備状況

NISC

サイバーセキュリティ戦略
NISC

2016年８月
IoTセキュリティ一般的枠組
NISC

日本の考え方の国際展開

セキュリティ・バイ・デザイン思想によるIoTシステム開発の提唱

IoTシステムの設計・構築・運用にかかる基本的な一般要求事項の明確化

各種ガイドライン（文書）が発行

GR01-2021 CCDS 2021 ★ Security Certification

SH02-2021 CCDS 2021 ★★ Security Certification

SH03-2021 CCDS 2021 ★★★ Security Certification

IoT推進コンソーシアム

2016年3月
つながる世界の開発指針

2016年７月
IoTセキュリティガイドライン
IoT推進コンソ
総務省
経済産業省

参照

提案

IoTサービス関係者全レイヤに向けたセキュリティガイドライン

製品分野横断で活用できる安全・安心なIoTシステムの開発指針（チェックリスト）

IPA

検討協力

参照

産業分野へ展開

CCDS

2016年

6月
分野別v1.0版公開

CCDS 車載機編
CCDS IoT-GW編
CCDS ATM編
CCDS オープンPOS編

海外発信
バージョンアップ

2017年

4月
分野別v1.0版(英語)公開

5月
・分野別v2.0版公開
・別冊公開

6月
・分野別v2.0(英語)公開
・評価検証ガイドv1.0公開

CCDS 車載機編-別冊
CCDS IoT-GW編別冊
CCDS ATM編-別冊

海外発信
新規ガイド作成

CCDS 評価検証ガイド

2018年

11月
・共通要件2018公開
・調達編draft公開

CCDS 共通要件ガイドライン 2018年版
CCDS 調達仕様編 draft

2019年

10月
・マーク制度開始
・共通要件2019公開
・スマートホーム編V1.0公開

CCDS 共通要件ガイドライン 2019年版
CCDS スマートホーム編 V1.0

2020年

11月
・マーク制度拡張（サービスへ）
・共通要件2021公開
・アップデート機能編公開
・ＡTM勉強会報告書

CCDS 共通要件ガイドライン 2021年版
CCDS アップデート機能編
CCDS ATM勉強会報告書

ガイドランから基準作りへ！押さえておくべきポイント

1. ライフサイクル
   - ✓ 企画、開発、設計、製造、販売、保守、廃棄

2. アクター定義：「サプライヤー」・「メーカ」・「サービス事業者」・「顧客」・「保守事業者」
   - ✓ 役割分担
   - ✓ サプライチェーン

   ※弱い場所がアタックサーフェース

3. 「最低限守るべき要件（minimum equirements)」　と　「推奨要件」
   - ✓ つながる機器としの最低限守べき要件
   - ✓ 機器の種類（価格帯、使用環境）に応じて要件は異なってくる

   ※多段防御

4. 「達成して欲しい結果」　と　「結果を達成するための方法」
   - ✓ 脆弱性と対策技術は経年変化する
   - ✓ 業種毎に設定が必要

   ※柔軟なスキーム

5. サポート（保守）
   - ✓ メーカと顧客とのつながり強度がセキュリティ強度に影響する

   ※野良IoT問題

6. 「認証プログラム」・・・「自己宣言」「第三者認証」「自己検査」「第三者検査」
   - ✓ 認証コストと製品コスト
   - ✓ スキームオーナ

   ※エコシステム

CCDS IoTセキュリティ要件

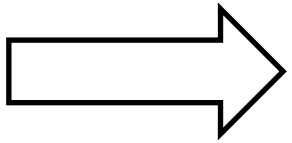
国内外のセキュリティガイドラインを踏まえ
2023年版策定に向けて活動中

2022年4月リリースを目指しております！

GR01-2021

SH02-2021

SH03-2021



GR01-2023

ご清聴ありがとう御座いました

【セッキュリティガイドライン】
https://www.ccds.or.jp/public_document/index.html

【サーティフィケーションプログラム】
https://www.ccds.or.jp/certification/index.html