ご案内資料

IoT機器向け　サーティフィケーションプログラム キックオフイベントのご案内

2019年10月30日

一般社団法人　重要生活機器連携セキュリティ協議会（ＣＣＤＳ）

キックオフイベント　開催概要

開催日時：2019年10月30日（水）11時―12時30分
実施場所：フクラシア丸の内オアゾ　15階　I会議室

プログラム：
11:00-11:30　サーティフィケーションプログラム説明
　　（サーティフィケーションプログラム）
　　（サーティフィケーションマーク取得製品紹介）
　　（自動付帯されるIoTサイバー保険）

11:30-11:45　Q&A

11:45-11:50　フォトセッション
　　（認証を取得した企業の担当者、CCDSメンバー）

11:50-12:30　フォトセッション
　　（認証を取得したIoT機器の撮影）

趣旨

重要生活機器連携セキュリティ協議会（以降、CCDS)は、民生機器を中心としたIoT機器やサービスにおけるセキュリティ向上を目指した産学連携の協議会です。

このたび、IoTセキュリティ要件を定め、サーティフィケーションプログラムを開始いたしました。

本キックオフイベントでは、プログラム概要、**サーティフィケーションマークを付与された機器のご紹介**、並びに**自動付帯されるIoTサイバー保険**についてご紹介いたします。

CCDSは、産業界自らがセキュリティ対策を投資として位置付け、消費者に安全・安心なIoT機器・サービス提供に貢献できる活動を引き続き目指してまいります。

登壇者紹介

・（一社）重要生活機器連携セキュリティ協議会/情報セキュリティ大学院大学　代表理事/客員教授
荻野司（おぎの　つかさ）

・株式会社JVCケンウッド　取締役　執行役員 最高技術責任者（CTO）オートモーティブ分野 技術本部長
／事業企画本部長　技術開発部担当、知的財産部担当
園田 剛男（そのだ　よしお）

・日立オムロンターミナルソリューションズ株式会社　取締役常務執行役員
濱崎 敏也（はまさき　としや）

・オムロンソーシアルソリューションズ株式会社　事業開発統轄本部　生活ソリューション事業本部　事業本部長
山崎宏司（やまさき　こうじ）

・文化シヤッター株式会社　執行役員　商品開発部長
石倉 則夫（いしくら　のりお）

・リンナイ株式会社　執行役員　開発本部　技術開発部長
清水正則（しみず　まさのり）

・三井住友海上火災保険株式会社　常務執行役員　金融公務営業推進本部長
大内 章生（おおうち　あきお）

・スマートホームWG主査/積水ハウス株式会社 技術業務部 課長
南　裕介（みなみ　ゆうすけ）

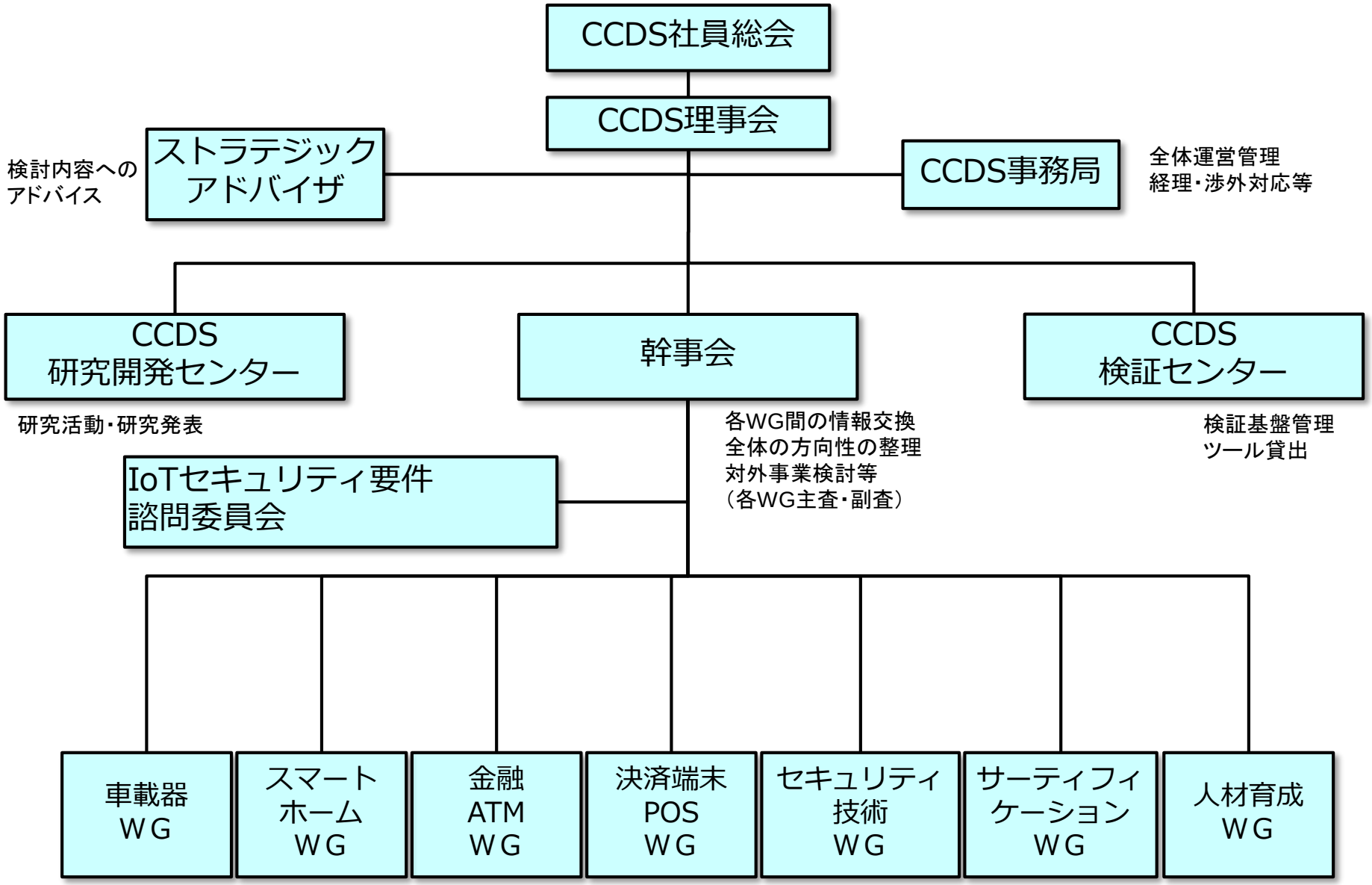
CCDSの概要

- 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：195（正会員以上：47、一般会員：116、学術系：17、協賛:15）(2019年９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

CCDSの実施体制

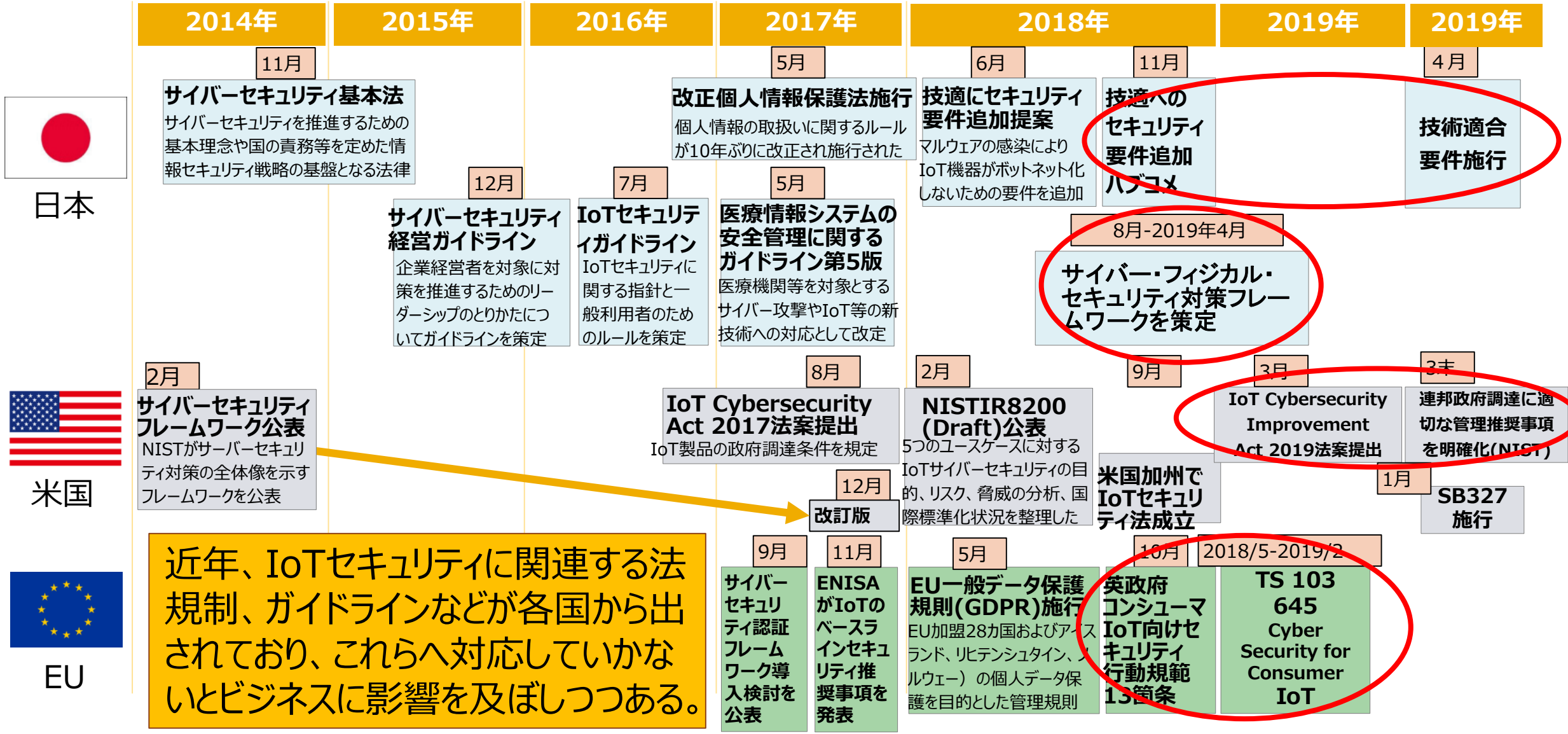

CCDS社員総会
CCDS理事会
検討内容への
アドバイス
ストラテジック
アドバイザ
CCDS事務局
全体運営管理
経理・渉外対応等
CCDS
研究開発センター
研究活動・研究発表
幹事会
各WG間の情報交換
全体の方向性の整理
対外事業検討等
（各WG主査・副査）
CCDS
検証センター
検証基盤管理
ツール貸出
IoTセキュリティ要件
諮問委員会
車載器
WG
スマート
ホーム
WG
金融
ATM
WG
決済端末
POS
WG
セキュリティ
技術
WG
サーティフィ
ケーション
WG
人材育成
WG

サーティフィケーションプログラム

2019年10月30日

一般社団法人　重要生活機器連携セキュリティ協議会

IoTセキュリティを取り巻く各国の動向



サーティフィケーションプログラム

1　背景

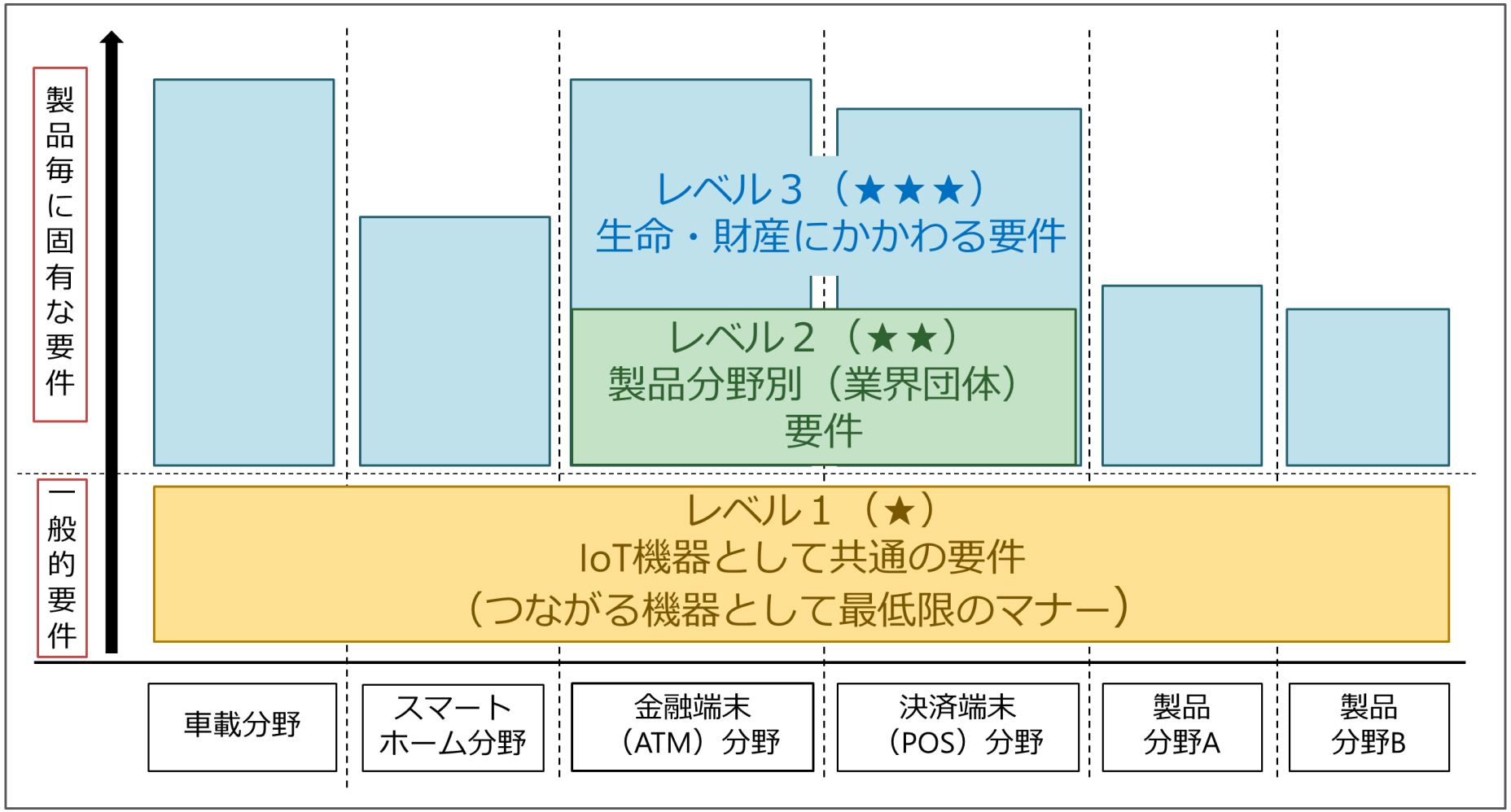
■サーティフィケーションプログラムの目的

・これからの IoT 社会では、安心して使用できる製品のセキュリティ基準や、製品がそのセキュリティ基準を満たすことを検証するスキームが重要になります。本協議会では、日常生活で利用する様々な機器が横断的につながる世界において、あるべきセキュリティ対策について検討を重ね、この度、IoT 機器共通の要件に対するサーティフィケーションプログラムを開始いたします。

2　サーティフィケーションプログラムのレベル構成

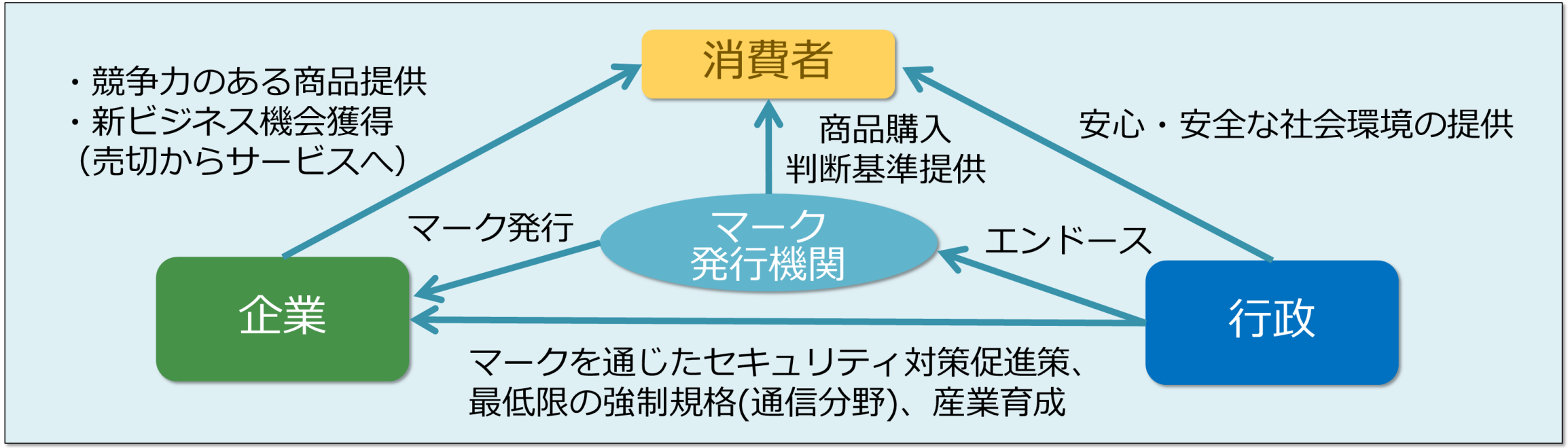
・消費者にも分かりやすいよう、★の数でセキュリティ対策のレベルを示す３階層のモデルを提示

・まずはレベル１の共通要件から、サーティフィケーションプログラムをスタートします



サーティフィケーションプログラム

3　CCDSサーティフィケーションのスキーム



ポイント

1.任意マーク（罰則なし）
2.自主評価と第三者評価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

CCDSサーティフィケーションマーク

2019年10月
開始！

2020年4月開始を目指して
活動中！

登壇者のご紹介

マーク付与機器のご紹介

■ 株式会社JVCケンウッド

HDメモリーカードカメラレコーダー「GY-HC900CH」

CONNECTED CAM™

IPを介してさまざまな周辺機器と連携できる“CONNECTED CAM™”第一弾として市場投入したJVCブランドのHDメモリーカードカメラレコーダー「GY-HC900」。

安定したIP伝送を可能とし、遠隔地からの映像転送やカメラ制御など、ユーザーニーズに合わせたワークフローの構築を可能とするIoTに対応した業務用カメラレコーダーです。

マーク付与機器のご紹介

■ 日立オムロンターミナルソリューションズ株式会社

国内向けATM「AKe-S」（サーティフィケーションマークオプション設定）

「AKe-S」は利用者の使いやすさに配慮したデザインを採用し、紙幣等のハンドリング技術を結集して高い信頼性を実現、消費電力の低減などで環境にも配慮してきましたが、従来のセキュリティ対策に加えて、新たにCCDSセキュリティ要件にも準拠可能となります。

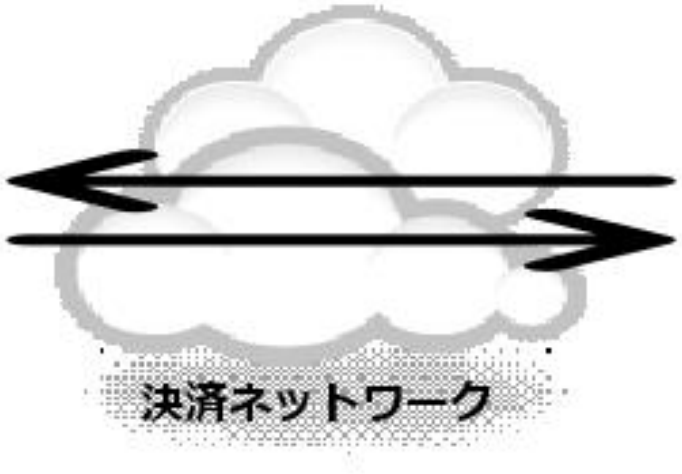
マーク付与機器のご紹介

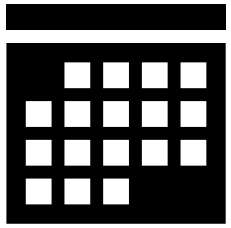
■ オムロンソーシアルソリューションズ株式会社

決済端末：CATS300/900シリーズ
マルチ決済端末として、クレジット、電子マネー、コード決済、ポイントカードなど各種決済に対応した決済端末として、2015年リリースから数万台を市場展開している。

マーク付与はCATS300/900の「BASEユニット」にて取得しています。
BASEユニットは、伝票印刷、情報センタ接続（LANインターフェース）、POS連動、各種ペリフェラル接続を実現するユニット。別途「操作ユニット」にてキー入力、表示、カード入力等を行いますが、このユニットはクレジットの国際ブランドのセキュリティ認定を別途受けています。

CATS300/900
BASEユニット





カード会社等

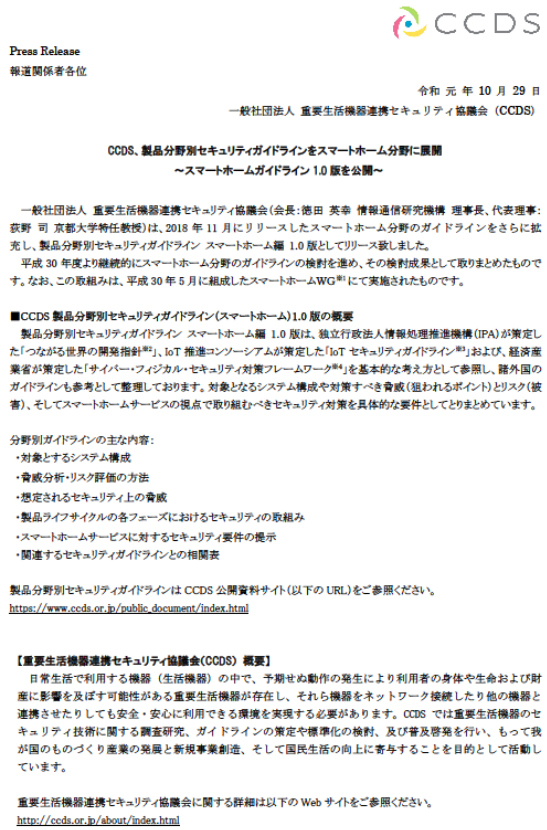
スマートホームＷＧについて

■ 2019年10月29日　**スマートホームガイドラインV1.0　リリース**

製品分野別セキュリティガイドライン スマートホーム編 1.0版は、独立行政法人情報処理推進機構（IPA）が策定した**「つながる世界の開発指針※2」**、IoT推進コンソーシアムが策定した**「IoTセキュリティガイドライン※3」**および、経済産業省が策定した**「サイバー・フィジカル・セキュリティ対策フレームワーク※4」**を基本的な考え方として参照し、諸外国のガイドラインも参考として整理しております。

分野別ガイドラインの主な内容：
- **対象とするシステム構成**
- **脅威分析・リスク評価の方法**
- **想定されるセキュリティ上の脅威**
- **製品ライフサイクルの各フェーズにおけるセキュリティの取組み**
- **スマートホームサービスに対するセキュリティ要件の提示**
- **関連するセキュリティガイドラインとの相関表**

https://www.ccds.or.jp/public_document/index.html



CCDS

Press Release
報道関係者各位

令和 元 年 10 月 29 日
一般社団法人 重要生活機器連携セキュリティ協議会（CCDS）

CCDS、製品分野別セキュリティガイドラインをスマートホーム分野に展開
～スマートホームガイドライン 1.0 版を公開～

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 情報通信研究機構 理事長、代表理事：荻野 司 京都大学特任教授）は、2018 年 11 月にリリースしたスマートホーム分野のガイドラインをさらに拡充し、製品分野別セキュリティガイドライン スマートホーム編 1.0 版としてリリース致しました。
平成 30 年度より継続的にスマートホーム分野のガイドラインの検討を進め、その検討成果として取りまとめたものです。なお、この取組みは、平成 30 年 5 月に組成したスマートホームWG※1 にて実施されたものです。

■CCDS 製品分野別セキュリティガイドライン（スマートホーム）1.0 版の概要
製品分野別セキュリティガイドライン スマートホーム編 1.0 版は、独立行政法人情報処理推進機構（IPA）が策定した「つながる世界の開発指針※2」、IoT 推進コンソーシアムが策定した「IoT セキュリティガイドライン※3」および、経済産業省が策定した「サイバー・フィジカル・セキュリティ対策フレームワーク※4」を基本的な考え方として参照し、諸外国のガイドラインも参考として整理しております。対象となるシステム構成や対策すべき脅威（狙われるポイント）とリスク（被害）、そしてスマートホームサービスの視点で取り組むべきセキュリティ対策を具体的な要件としてとりまとめています。

分野別ガイドラインの主な内容：
・対象とするシステム構成
・脅威分析・リスク評価の方法
・想定されるセキュリティ上の脅威
・製品ライフサイクルの各フェーズにおけるセキュリティの取組み
・スマートホームサービスに対するセキュリティ要件の提示
・関連するセキュリティガイドラインとの相関表

製品分野別セキュリティガイドラインは CCDS 公開資料サイト（以下の URL）をご参照ください。
https://www.ccds.or.jp/public_document/index.html

【重要生活機器連携セキュリティ協議会（CCDS）概要】
日常生活で利用する機器（生活機器）の中で、予期せぬ動作の発生により利用者の身体や生命および財産に影響を及ぼす可能性がある重要生活機器が存在し、それら機器をネットワーク接続したり他の機器と連携させたりしても安全・安心に利用できる環境を実現する必要があります。CCDS では重要生活機器の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活動しています。

重要生活機器連携セキュリティ協議会に関する詳細は以下の Web サイトをご参照ください。
http://ccds.or.jp/about/index.html

マーク付与機器のご紹介

■ 文化シヤッター株式会社

住宅用窓シャッター　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 文化シヤッター

ワイヤレス通信機２
型式：SCX1801

（マーク取得対象機器）

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

マーク付与機器のご紹介

■ 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

お風呂の自動運転　おいだき　お風呂の予約　床暖房　スマートスピーカーでの操作

IoTサイバー保険　概要

ＣＣＤＳは、三井住友海上火災保険株式会社、損害保険ジャパン日本興亜株式会社と連携し国内初となる「ＩｏＴ機器保険付認証制度」を構築。ＣＣＤＳがマーク付与した製品に対してサイバー保険を自動付帯します。

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

メーカーに過失が発生する場合、賠償金をお支払いいたします。

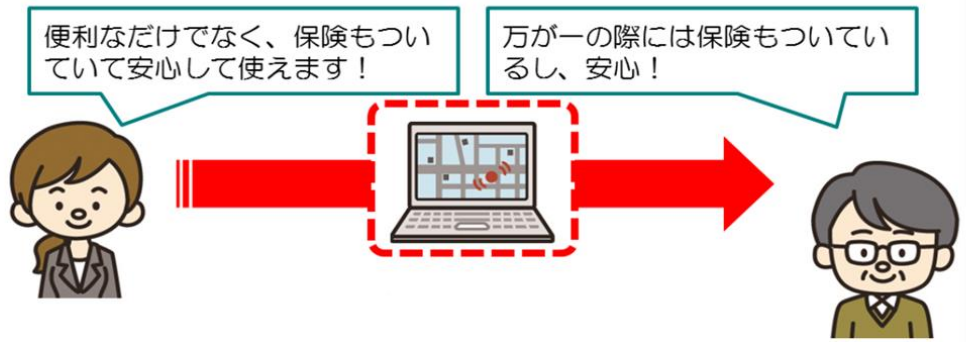
その他費用損害

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。

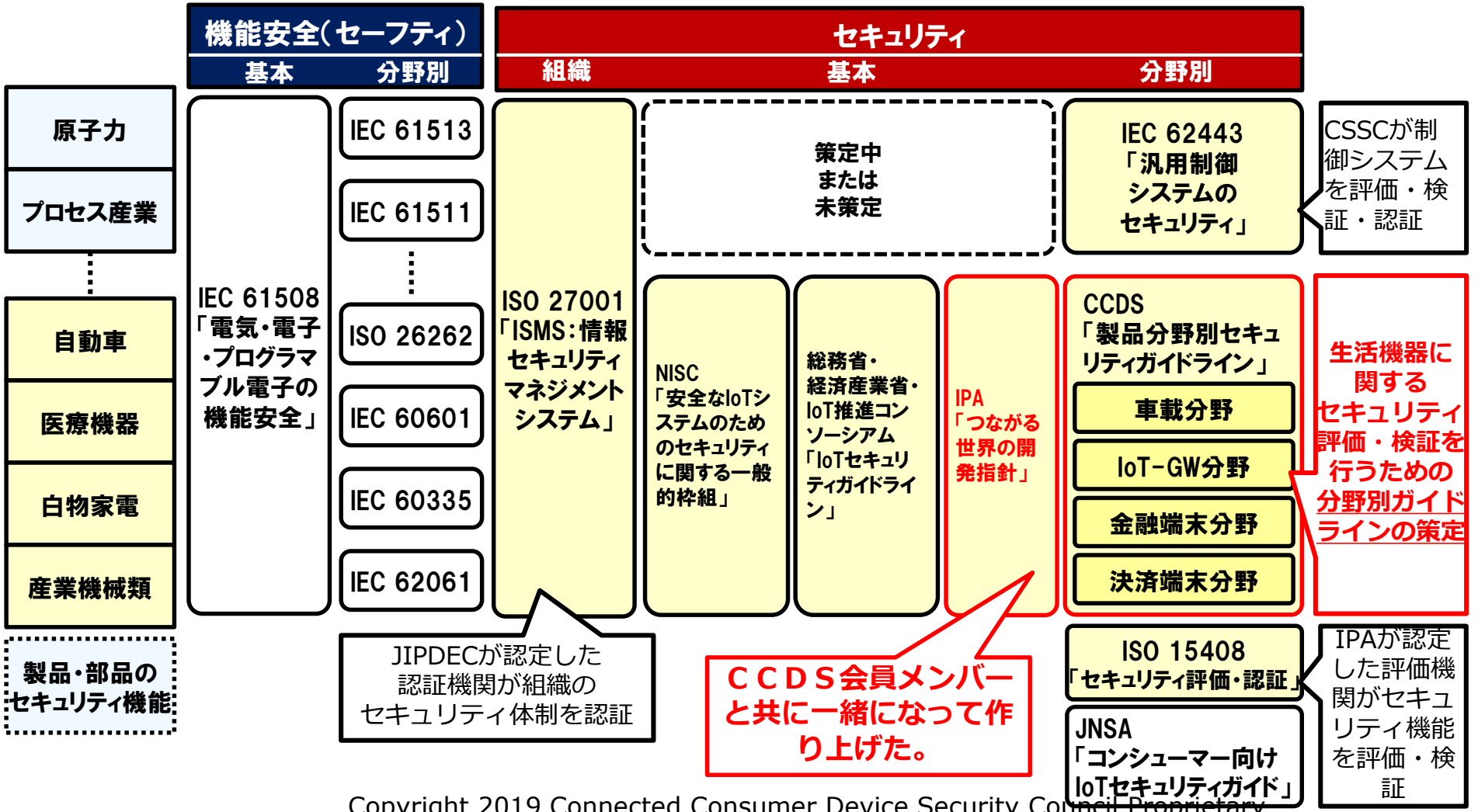


参考資料

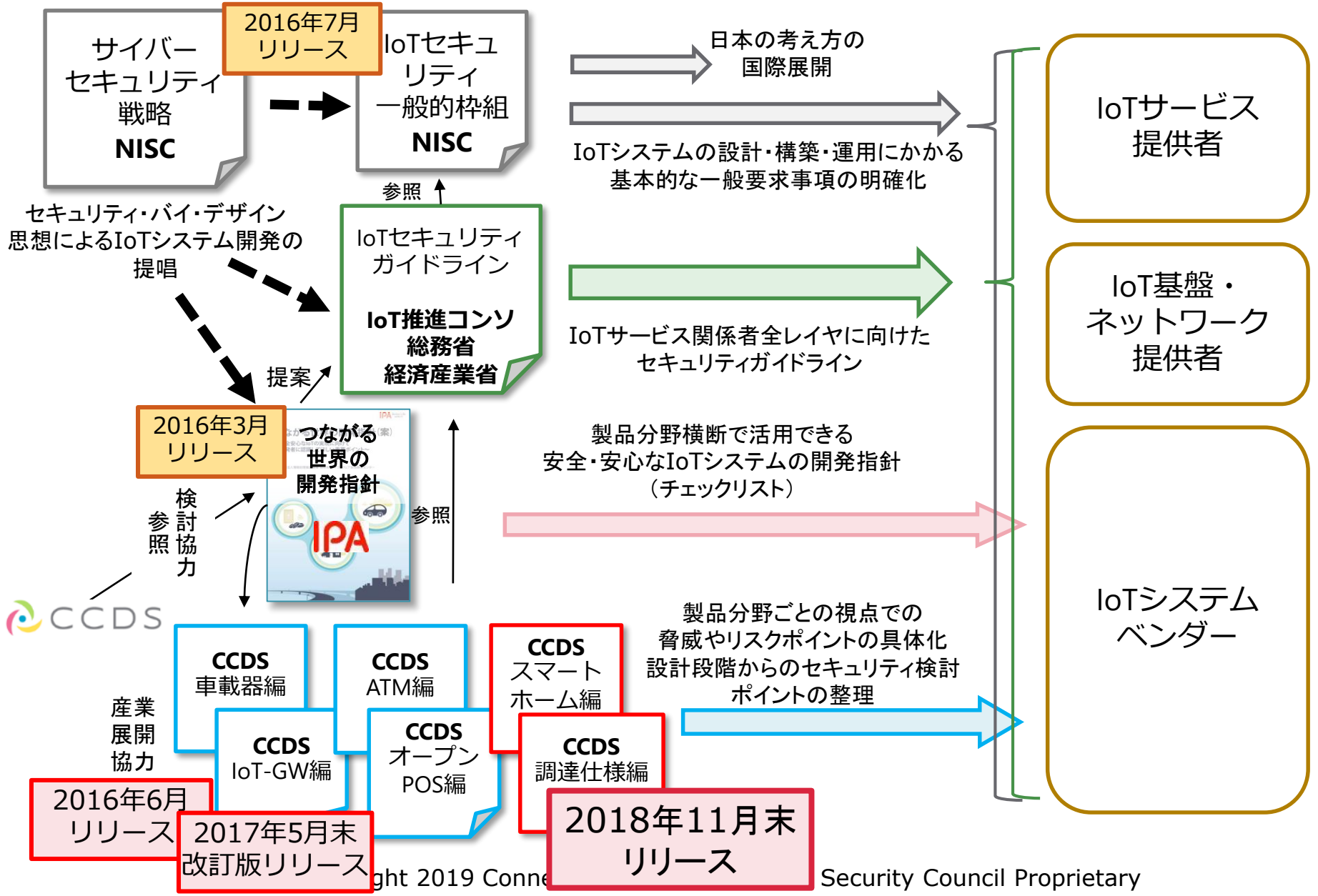
規格策定状況：2018年度

＜セーフティとセキュリティの国際規格の策定状況＞

NISC：内閣サイバーセキュリティセンター
CSSC:技術研究組合制御システムセキュリティセンター
IPA：独立行政法人情報処理推進機構
JIPDEC一般財団法人日本情報経済社会推進協会
JNSA：特定非営利活動法人 日本ネットワークセキュリティ協会



IoTセキュリティガイドラインの整備状況



IoT セキュリティ要件1/2（★）

No	認証要件	脆弱性の種類	脅威の背景	事例
1	**Web入力経由**によるSQLインジェクションの不具合がないこと	SQLインジェクション	ユーザからの入力に含まれた SQL構文の排他が不十分であり、セキュリティチェックの回避や、ステートメントの挿入によりバックエンドのデータベースを改ざんやシステムコマンドの実行に利用される可能性がある。（CWE-TOP6）	・Wi-Fi 無線ルータ（CVE-2015-6319）
2	**Web入力経由**によるクロスサイトサイトリクエストフォージェリの不具合がないこと	クロスサイトリクエストフォージェリ	ユーザからのリクエストが、適切な フォーマットであるかを検証しない ことで発生する脆弱性。攻撃者がク ライアントを騙し、意図しないリク エストを Web サーバに送信させる 可能性がある。（CWE-TOP7）	・Wi-Fi 無線ルータ（CVE-2014- 7270）
3	**Web入力経由**によるパストラバーサルの不具合がないこと	パストラバーサル	外部入力からパス名を作成し、制限 されているディレクトリへのアクセ スを許してしまう脆弱性。（CWETOP11）	・IP カメラ（CVE-2017-7461）
4	**未使用ポートを外部より使用されないこと**	不要サービスポートの解放	機能やサービス上必要のないサービスポートを解放しておくことで、サ イバー攻撃に悪用される恐れのある 通信が可能となる。	・Wi-Fi 無線ルータ、IP カメラ等
5	システム運用上、必要なポートには、適切なアクセス認証方法（**機器毎にユニークなID/パスワード、もしくは外部公開の恐れのない管理されたID/パスワード**）で管理されていること	オープンサービスポートの不適切なアクセス管理	解放されたサービスポートに対し て、適切なアクセス管理が行われて おらず、機器内のデータの情報漏洩 や、権限昇格（管理機能の掌握）等 の問題を生じる可能性がある。	・Wi-Fi 無線ルータ、IP カメラ等
6	・認証情報の設定変更が可能なこと ・**初めて利用する際、設定変更を促す**こと ・ID/パスワードは**ハードコーディングをしない**こと（初期パスワードは共通でも可とする） ※Web管理画面アクセス時のID/パスワードを対象とし、認証鍵は対象外とする	アクセスコードの不適切な実装（ハードコーディング、変更不可等）	機器やアプリケーションにアクセス用の ID/パスワード情報などを、ハ ードコーディングしているケース や、設定変更ができない実装により、 ID/パスワードが危殆化してしまっ た場合の対応ができず、脆弱性につ ながる。	・医療機関システム

IoT セキュリティ要件2/2（★）

No	認証要件	脆弱性の種類	脅威の背景	事例
7	・利用者の設定した情報、および機器が利用中に取得した情報は、容易に消去する機能を有すること＊ただし、更新されたシステムソフトウェアは維持されること	**廃棄やリユースを想定した機能実装**不備	機器やアプリケーションが保持する セキュリティ上の設定値、機密情報、プライバシー情報等の削除機能を実 装しておらず、廃棄時やリユース時に機密情報やセキュリティ設定値、 プライバシー情報などが漏洩する可能性がある。	・PC、USB メモリ、スマートフォン
8	・Wi-Fiアライアンス推奨の**最新の認証方式**が装備されていること	Wi-Fiの通信方式が最新の方式ではない	Wi-Fi 機器において使用される通信 暗号化の方式が最新のものではなく脆弱な暗号化プロトコルや、暗号化 アルゴリズムが使用されている。	・Wi-Fi 無線ルータ
9	・BluetoothSIG推奨の**最新のペアリング方式**が装備されていること	Bluetoothのペアリング方式が最新の方式ではない	Bluetooth 2.0+EDR 以前の仕様で は、ペアリングする機器同士が、共通の“PIN コード”と呼ばれる数字 を入力する方式となっている。一般 的には“0000”など、4 桁の数字を 入力による実装で多く、決め打ち攻 撃で容易に破れてしまう。	・Bluetooth 2.0+EDR 以前の機器
10	システム運用上、**不要なクラス**を認識できないこと	USBの不要なクラスの利用	不要なデバイスクラスの実装によ り、BadUSB による攻撃を受ける可 能性がある。	・USB 実装機器全般
11	・**ソフトウェア更新**が可能なこと ・ソフトウェア更新された状態が電源OFF後も維持できること	ソフトウェアアップデートできない	ソフトウェアやファームウェアに脆 弱性が見つかった場合に、更新を行う機能が実装されていない事で、セ キュリティホールを突かれた攻撃を受ける可能性がある。	・Wi-Fi 無線ルータ、IP カメラ等