ISOC-JPセミナー

CCDSの取組み状況

重要生活機器連携セキュリティ協議会（CCDS）ストラテジックアドバイザ
情報セキュリティ大学院大学 セキュアシステム研究所 客員研究員
JVCケンウッド 技術開発部　技術企画グループ長／PSIRTリーダ
伊藤 公祐

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、慶應大学 名誉教授）
- 代表理事：荻野 司（京都大学 特任教授）
- 理事：後藤厚宏（情報セキュリティ大学院大学 教授、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：182（正会員以上：50、一般会員：102、学術系：16、協賛:14）
  (2018年末)

- 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 Members

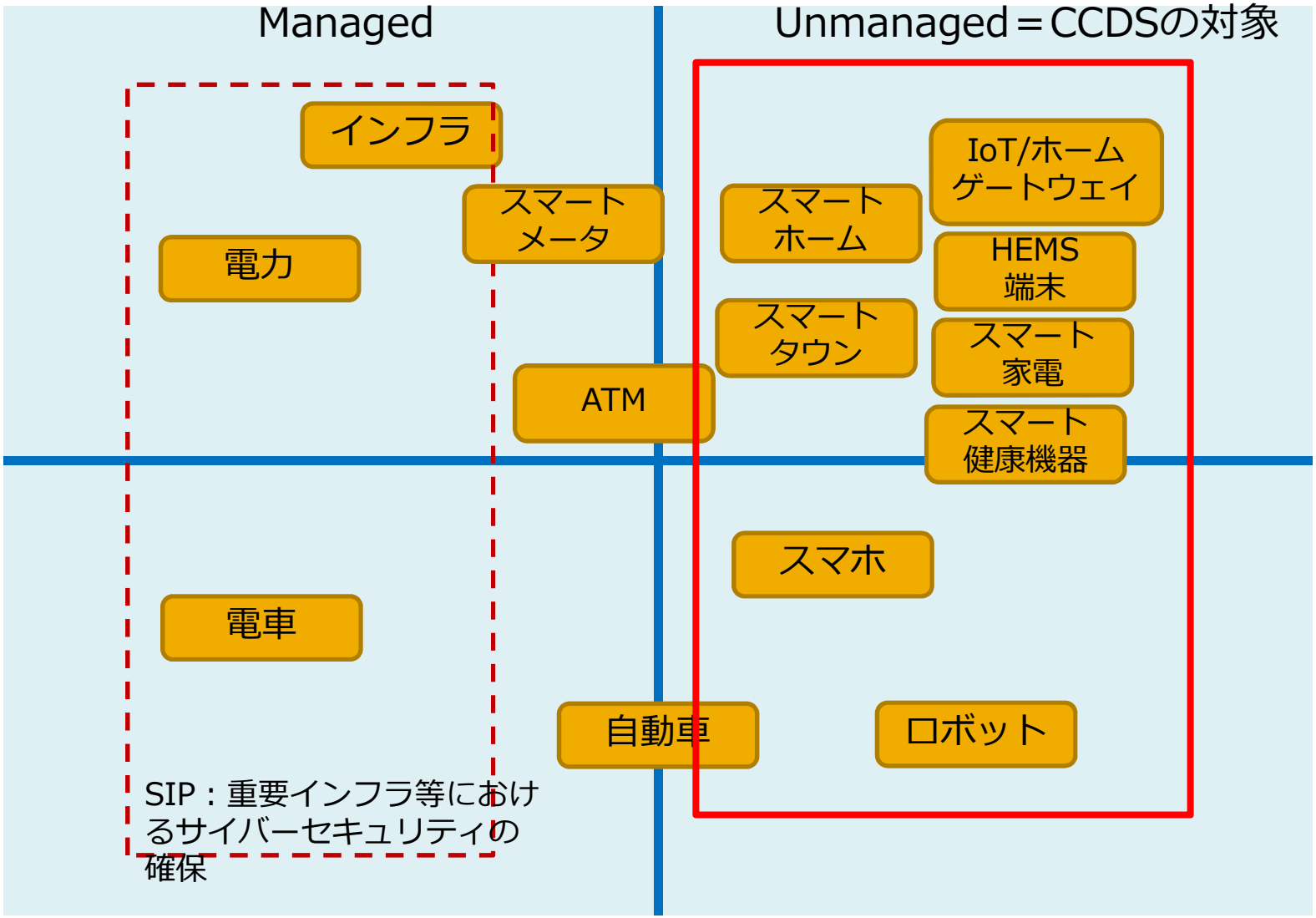
- Total number of members: 182 (as of Dec., 2018) *not all appeared
  - Executive Members: 22 such as;

  - Regular Members: 28 such as;

  - General members: 102 such as;

  - Academic members: 16
    - Hiroshima City Univ., Keio Univ., Nagoya Univ., Univ. of the Ryukyus, Yokohama Nat'l Univ., Inst. of Information Security (IISEC), Japan Adv. Inst. of Science and Technology (JAIST), Nat'l Inst. of Adv. Industrial Science and Technoloty (AIST), Nat'l Inst. of Information and Communications Technology (NICT), Nat'l Inst. of Informatics (NII), etc.
  - Liaison members: 14
    - Computer Software Assoc. of Japan, Internet Assoc. of Japan , Japan Network Security Assoc., Japan Cloud Security Alliance, etc.

IoT環境で対象とするシステム



慶應義塾大学教授/CCDS会長 徳田英幸氏「IoTセキュリティの課題」
CCDSにて修正（ATM、スマートメータ部）

CCDSが取り組む事業分野

検証基盤構築

・検証業務をサポートする共通基盤開発
－組込み機器評価・検証基盤システム

・セキュリティ検証ツール開発
－車載、IoT-GW、ATM、POS分野

・テストベット検討

標準化推進

・セキュリティガイドライン策定
－セキュリティガイドラインWG
（車載、IoT-GW、ATM、POS-SWG）

・IoTセキュリティ対策技術の体系化
－デバイスセキュリティ技術SWG
－ユーザビリティWG

・ガイドライン国際標準化検討

人材育成

・オープンセミナーの開催
－セキュリティシンポジウム
－検証技術セミナー
－CCDSガイドライン勉強会　.etc

・ワークショップの開催
－検証ツールハンズオン講習会
－IoTセキュリティ評価検証
技術講習会

CCDS

動向調査・研究

・国内外のガイドライン、標準化動向

・検証手法、検証ツールの調査・研究

・脅威事例の収集、ハッキング技術調査

・認証制度の実現に向けた調査

普及啓発

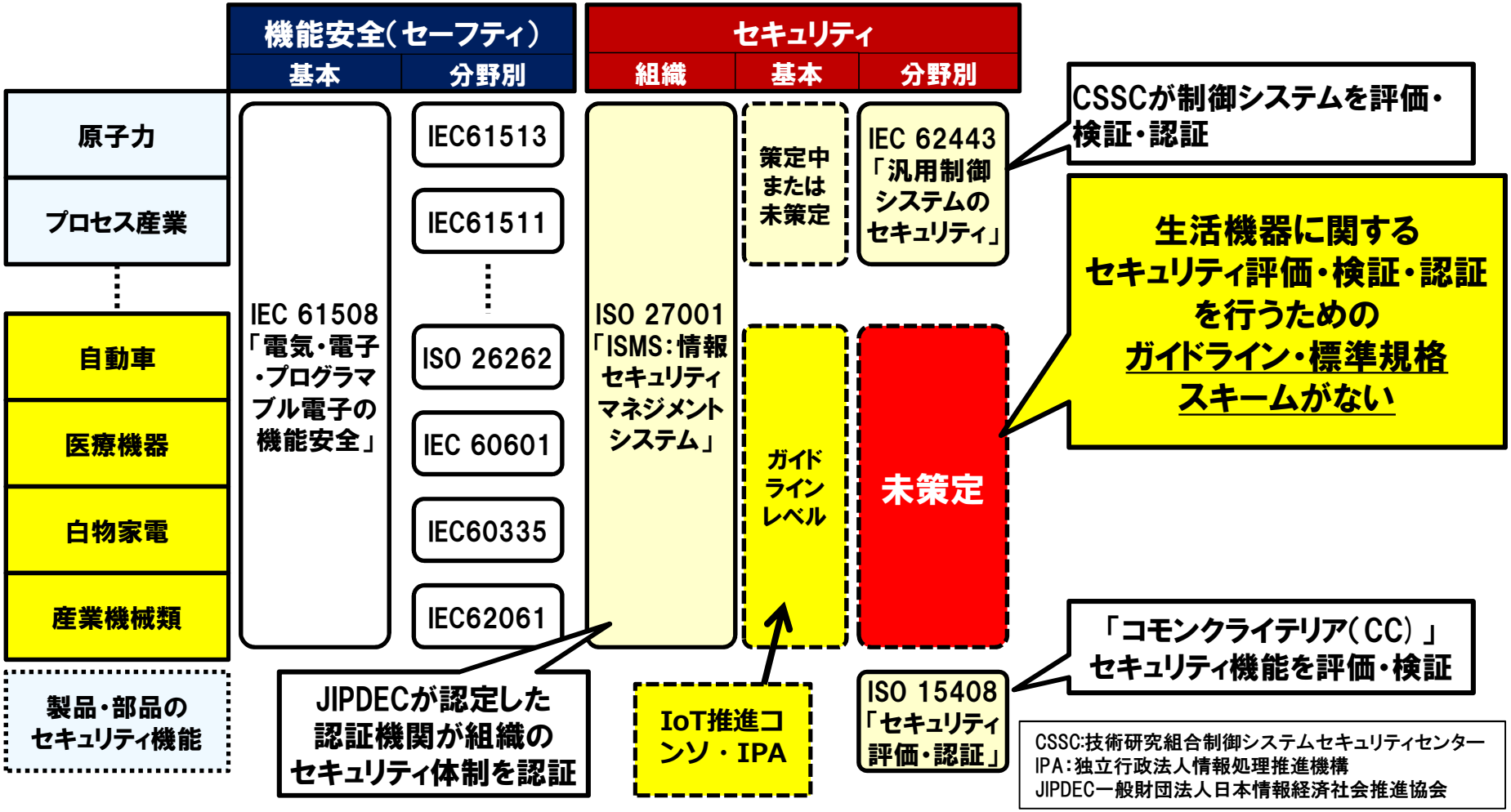
・シンポジウム、セミナーの主催

・調査資料、ガイドラインの公開

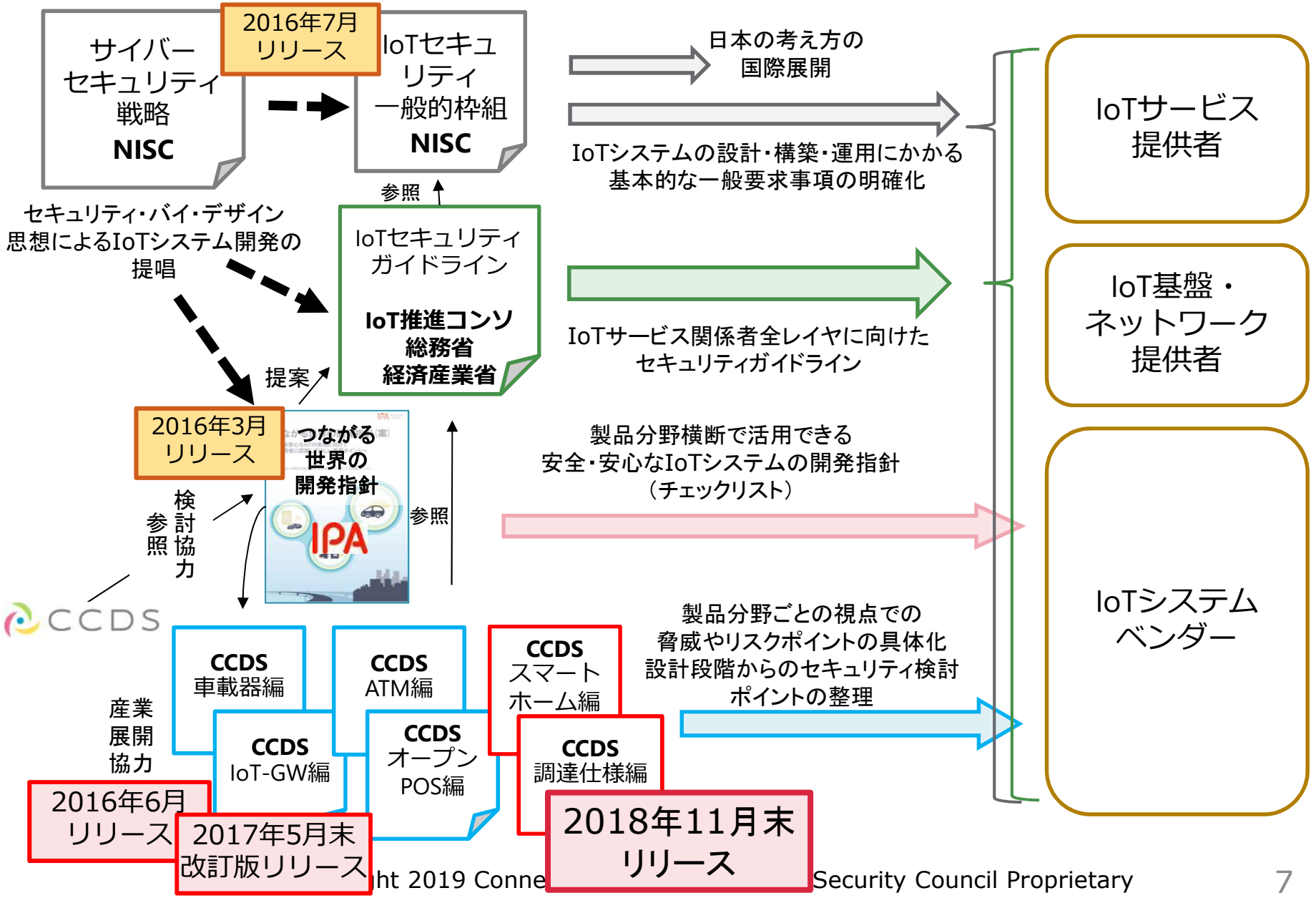
・提携団体での講演活動

CCDS発足当初の状況

- IoT普及において、セキュリティ懸念が増しているが、IoT向け生活機器のセキュリティ標準が未整備。



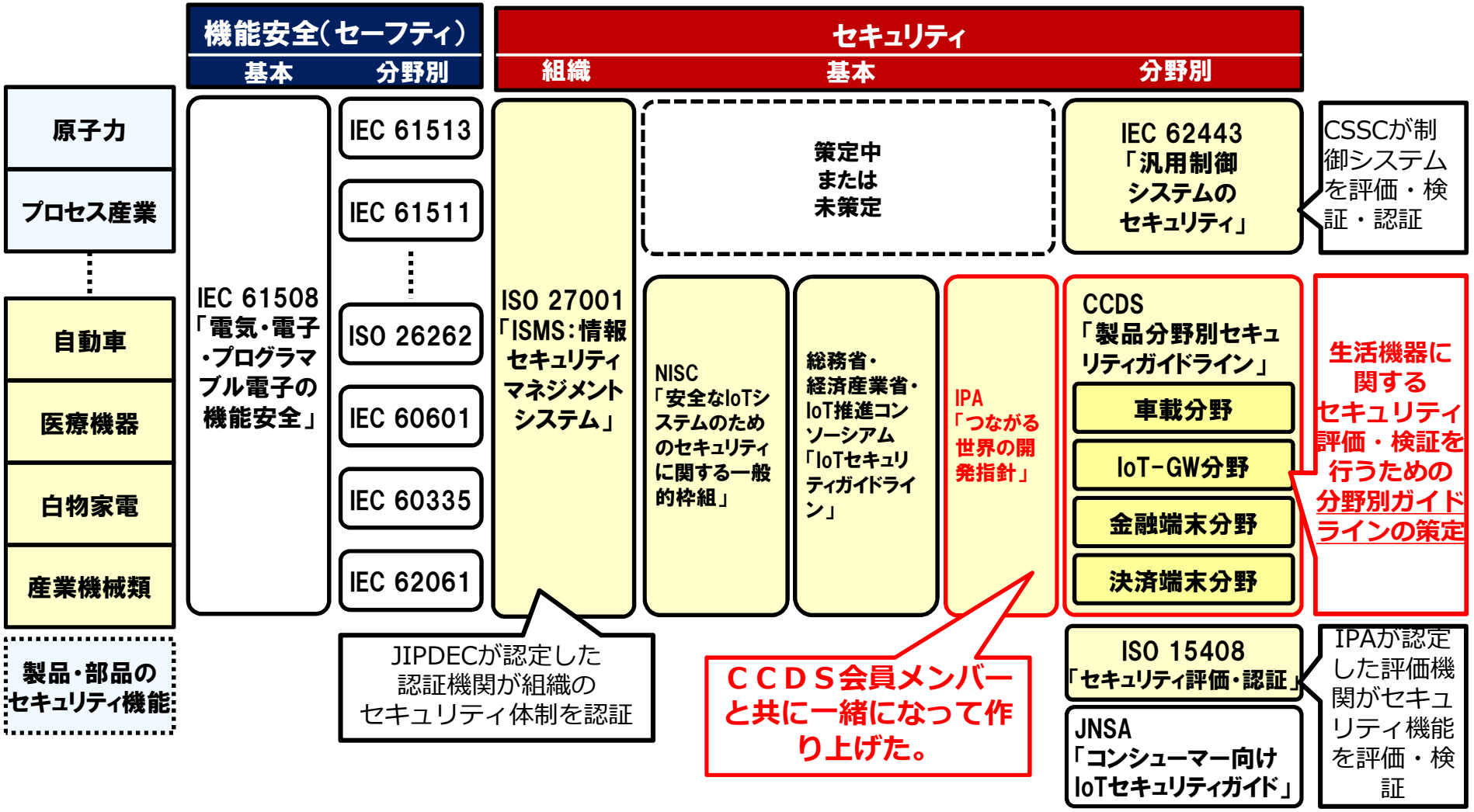
IoTセキュリティガイドラインの整備状況



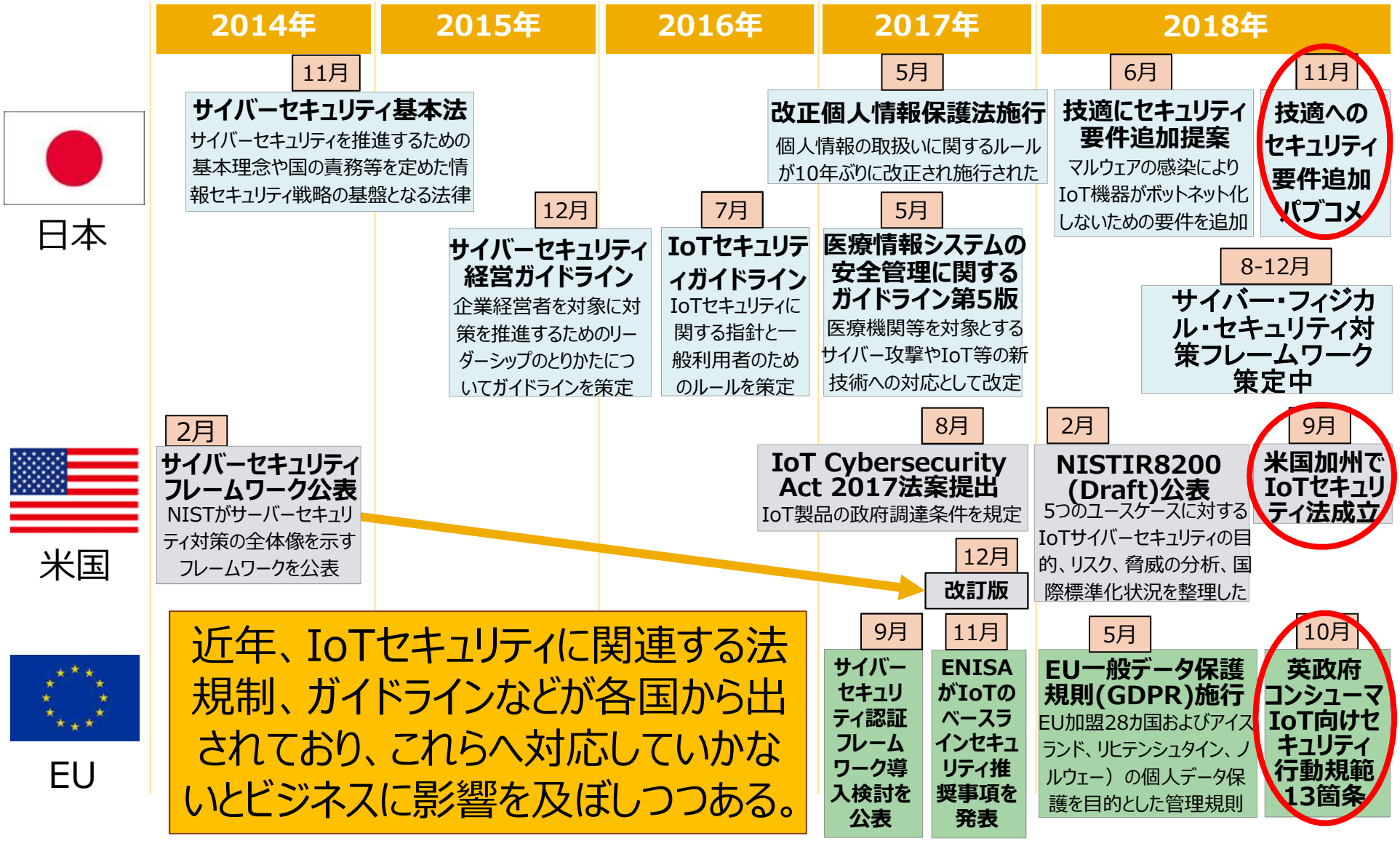
規格策定への取り組み（2016年度）

＜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セキュリティを取り巻く各国の動向



NIST Cybersecurity Framework v1.1

- NIST（National Institute of Standard and Technology)の発行した、セキュリティ対応のための基本項目をフェーズごとに整理したフレームワーク。
  - Identify：（脅威・攻撃手法）特定
  - Protect：防御
  - Detect：（攻撃）検知
  - Respond：対応
  - Recover：復旧

- 様々なガイドラインや標準で参照されている世界標準的考え方
- 2018年4月にv1.1がリリース
  - **サプライチェーン**全体でのセキュリティ管理が追加された
    - 中国製スマホバックドア問題、クローンルータ問題
    - 脆弱性の残る古いチップ（参考：Broadcom, MarvellのWiFiチップ）

次は施策は、認証マーク

まず、呼び方は。。。

「CCDS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プログラムの目的

- 世の中のIoT機器をセキュアにする方法としての**提案**
  ⇒ 様々な方法論はあるが、議論のスタートポイントとして。

- IoT機器をセキュアにするための努力の結果を**見える化**する
  ⇒ Security By Designの取組みへのインセンティブの提供
  それによって、ベンダの積極的な「セキュリティ投資」を促す
  ⇒ ユーザの必要とするセキュリティ品質を持つIoT機器を選択できる
  健全な市場形成に貢献する

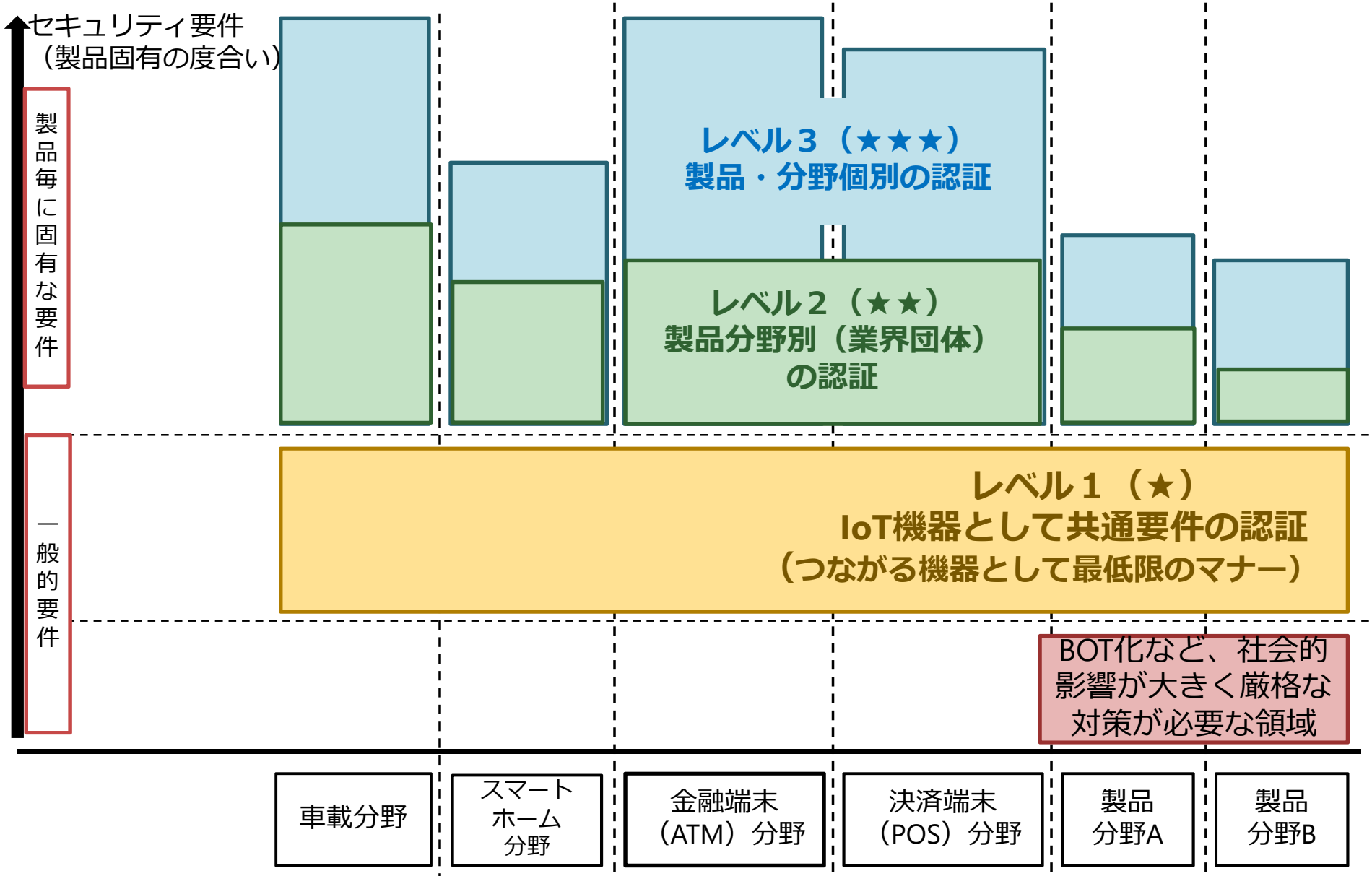
- 「つながる世界（IoT時代）」に向けて、IoT機器全体が
  一定水準のセキュリティを確保した社会にする
  ⇒ 分野間連携する際、相互にセキュリティレベルが理解できる
  共通言語を提供する

- IoT機器の「セキュリティ品質」を確認するための
  エビデンスとトラッキングの仕組みとする
  ⇒ 一定のセキュリティ品質を確保していたIoT機器へのインシデント
  から、教訓と改善を行うナレッジを蓄積し、ベンダ間で共有する

- 広くセキュリティ対応を普及させるため、要件のハードルは高くせず、でも、低すぎず
  - 「脆弱性を排除（ゼロ）にしろ」という無茶な要件にしない
    - 少し頑張れば手の届く（超えられる）ハードル
  - 「接続認証パスワードは個々にユニークに」くらいの最低レベルから始めて、徐々に上げていく
    - まずは「Better than Nothing」から
    - 総務省技適、加州SB327、UK Code of Practicesを参照

- 広くセキュリティ対応を普及させるため、低廉に取得できる
  - 第三者評価を必須にしない（自己評価を許容する）⇒二者認証方式
  - ベンダの「やる気」を喚起し、IoT機器の普及を阻害しない

サーティフィケーション基本フレームワーク



2019年版一般的要件（★１）

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
2. Web入力経由によるクロスサイトリクエストフォージェリの不具合がないこと
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
4. 未使用のTCP/UDPポートを外部より使用されないこと
5. システム運用上、必要なTCP/UDP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とパスワード、もしくは外部公開の恐れのない管理されたIDとパスワード）で管理されていること
6. 認証情報の設定変更が可能なこと&初めて利用する際、設定変更を促す機能を有すること&IDと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）
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、容易に消去できる機能を有すること&情報消去後も、更新されたシステムソフトウェアは維持されること
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
9. Bluetooth SIG推奨の最新のペアリング方式が装備されていること
10. システム運用上、不要なクラスを認識できないこと
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

プログラム開始に向けた準備の状況

- 共通要件検討WG（メンバー限定クローズドWG）にて以下の取組みを実施中

１）分野をまたがる最低限の要件を定義する
  - 製品機能・脆弱性評価が中心（必要ならプロセス評価要件も含む）

２）必要要件を評価する手法を定義する
  - 製品評価では、各要件において○×で判定可能になるよう考慮する

３）認証マークの申請、判定、発行方法を定義する

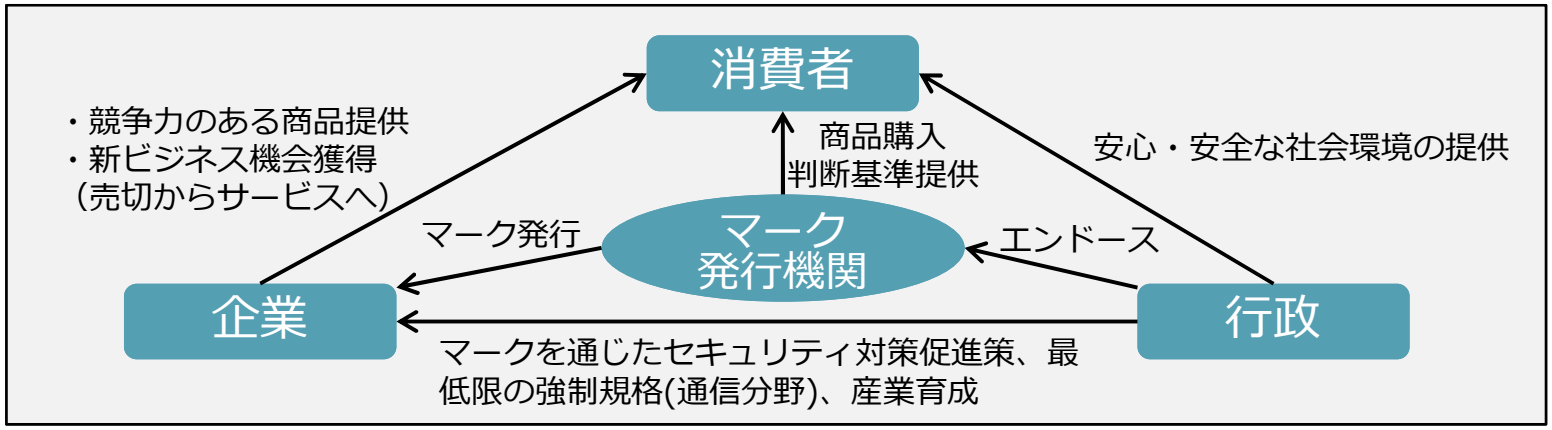
４）第三者検証手法、検証結果報告内容を定義する

プログラム開始に向けた準備の状況

- トライアル検証
  - 策定した検証ガイドライン・合格基準などの実効性評価作業
    - 検証ガイドラインに例示したツールでの評価の実効性
    - エビデンスとなる結果の提出方法
    - ドキュメント評価の確認事項
    - 課題があれば、上記ドキュメントに反映
  - WGメンバーのIoT機器をサンプルに検証実施中

プログラム運営スキーム

■ 関係者の位置付け



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も検討中

民間企業の自助努力を引き出しやすい仕組み

マーク
階層構成
（★★★）

業界マーク（個社横断）★★	金融端末	日本自動販売システム機械工業会で取組み中
共通要件マーク★	車載機、スマートホーム、金融端末、決済端末	**ＣＣＤＳマークとしてプレ実施**

分野別セキュリティガイドラインなど
CCDSホームページ「公開資料」コーナーで
無料公開中！
https://www.ccds.or.jp/public_document/

本日はご清聴ありがとうございました