IoTセキュリティの国際動向
～法規制やサーティフィケーションはどうなる？～

2019年12月20日

CCDS ストラテジックアドバイザ
サーティフィケーションWG　主査
ＪＶＣケンウッド PSIRTリーダ　伊藤公祐

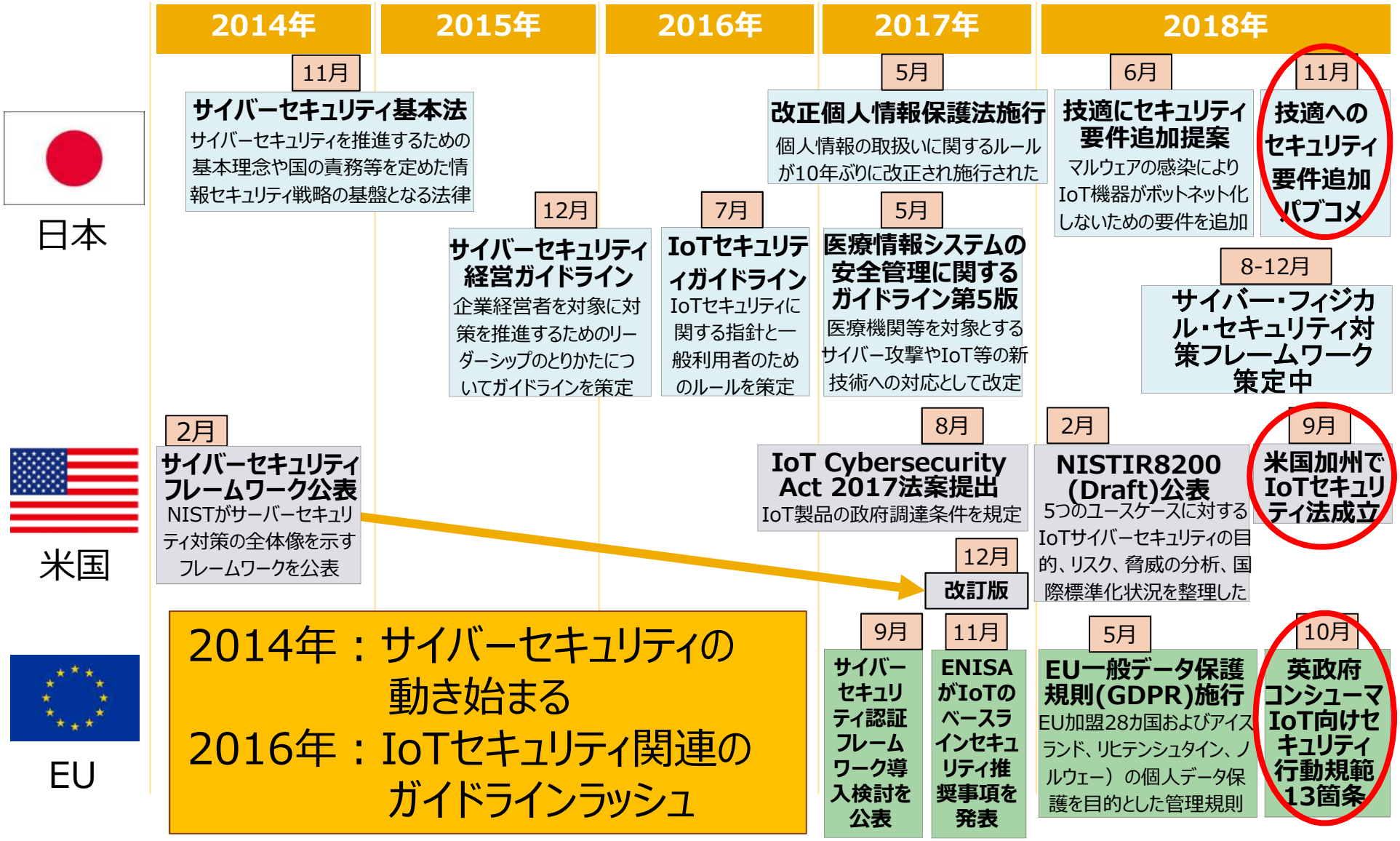
Copyright 2019 Connected Consumer Device Security Council Proprietary

アジェンダ

- IoTセキュリティガイドラインの歴史
- 近年のＩｏＴセキュリティ要件
- CCDSサーティフィケーション 2020要件策定に向けて

Copyright 2019 Connected Consumer Device Security Council Proprietary

IoTセキュリティを取り巻く各国の動向



Copyright 2019 Connected Consumer Device Security Council Proprietary

IoTセキュリティガイドラインの例（海外）

- Dept. of Homeland Security
  - STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)
- oneM2M:
  - Security Solutions v2.4.1 (TTCより日本語版あり)
  - Security v2.0 (TR analysis)
  - End-to-End Security and Group Authentication v2.0
- CSA:
  - Security Guidance for Early Adopters of the Internet of Things (IoT)
  - Identity and Access Management for the Internet of Things – Summary Guidance
  - Security Guidance for Smart Health, for Smart Cities, for Smart Retails
  - Analysis of Hardware Security Options for the IoT
  - Checklist for Secure IoT Device Development
  - Internet of Things (IoT)インシデントの影響評価に関する考察 (CSAジャパンより日本語版あり)
  - Future-proofing the Connected World: 13 Steps to Developing Secure IoT Products（同上）
- OWASP
  - IoT Security Guidance (Draft)
    - https://www.owasp.org/index.php/IoT_Security_Guidance
- GSMA:
  - IoT Security Guidelines (Overview, for Service Eco-Systems, for End Point Eco-Systems, and for Network Operators)
  - IoT Security Self-Assessment
- SAE:
  - J3061（Cybersecurity Guidebook for Cyber-Physical Vehicle)
- Continua Health Alliance
  - End-to-End Security for Personal Telehealth

他にもいっぱいあると思います…

Copyright 2019 Connected Consumer Device Security Council Proprietary

IoTセキュリティガイドラインの例（国内）

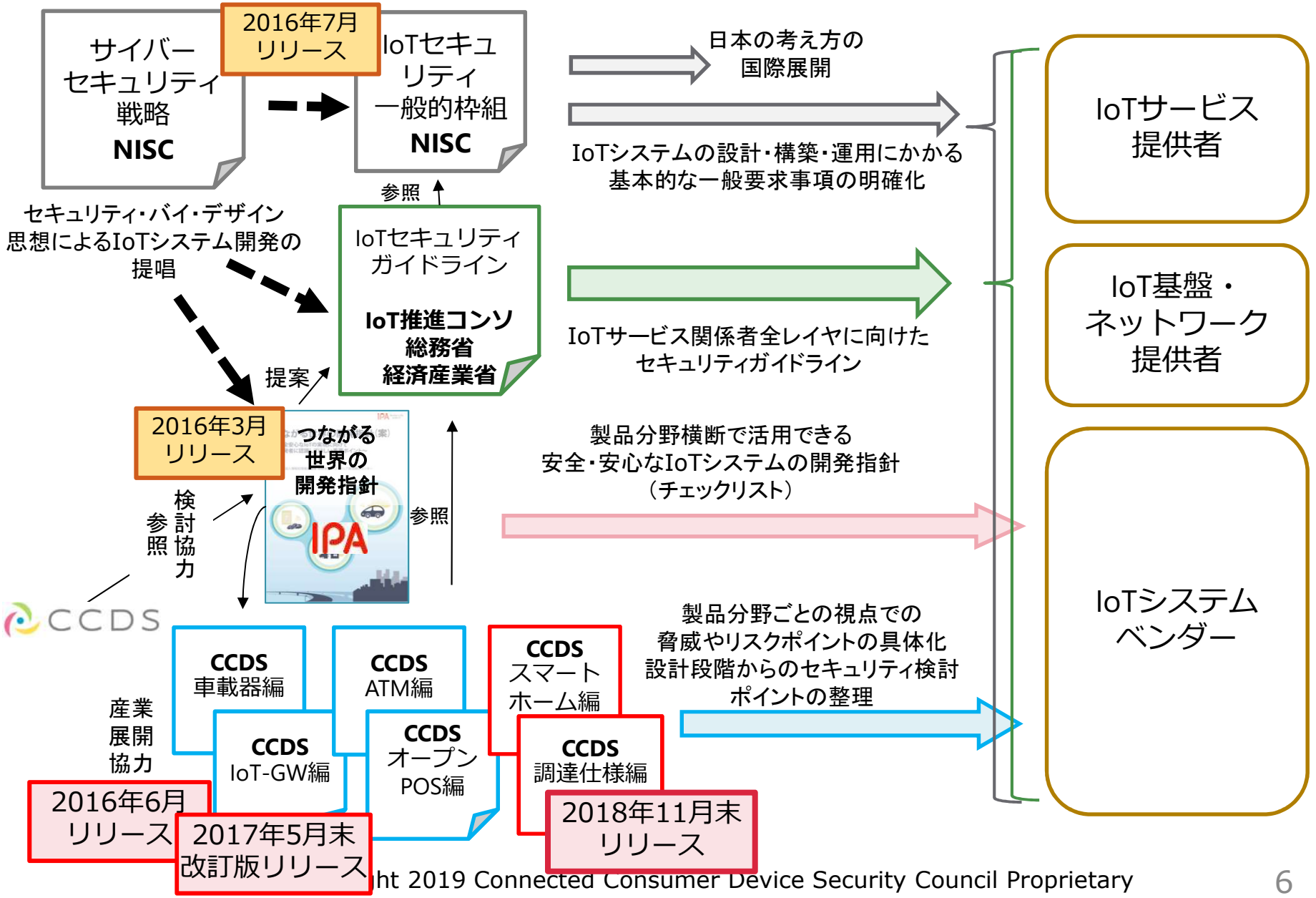
- NISC（内閣サイバーセキュリティセンター）
  - 「IoTセキュリティ一般的枠組み」
    - http://www.nisc.go.jp/active/kihon/pdf/iot_framework2016.pdf
- IoT推進コンソーシアム（IoTセキュリティWG）・総務省・経済産業省
  - 「IoTセキュリティガイドライン」
    - http://www.iotac.jp/wg/security/
- IPA
  - 「つながる世界の開発指針」
    - https://www.ipa.go.jp/files/000051411.pdf
  - 「つながる世界の開発指針の実践に向けた手引き＜高信頼化機能編＞
    - https://www.ipa.go.jp/files/000059278.pdf
- JNSA（IoTセキュリティWG）
  - 「コンシューマー向けIoTセキュリティガイド」
    - http://www.jnsa.org/result/iot/data/IoTSecurityWG_Report_Ver1.pdf
- CCDS
  - 「分野別セキュリティガイドライン」
    車載器編、IoT-GW編、オープンPOS編、ATM編
    - CCDSホームページ「公開資料」コーナーで一般公開中！
    - https://www.ccds.or.jp/public_document/

他にもあるかも…

2016年は国内外で
ガイドラインラッシュ

Copyright 2019 Connected Consumer Device Security Council Proprietary

IoTセキュリティガイドラインの整備状況

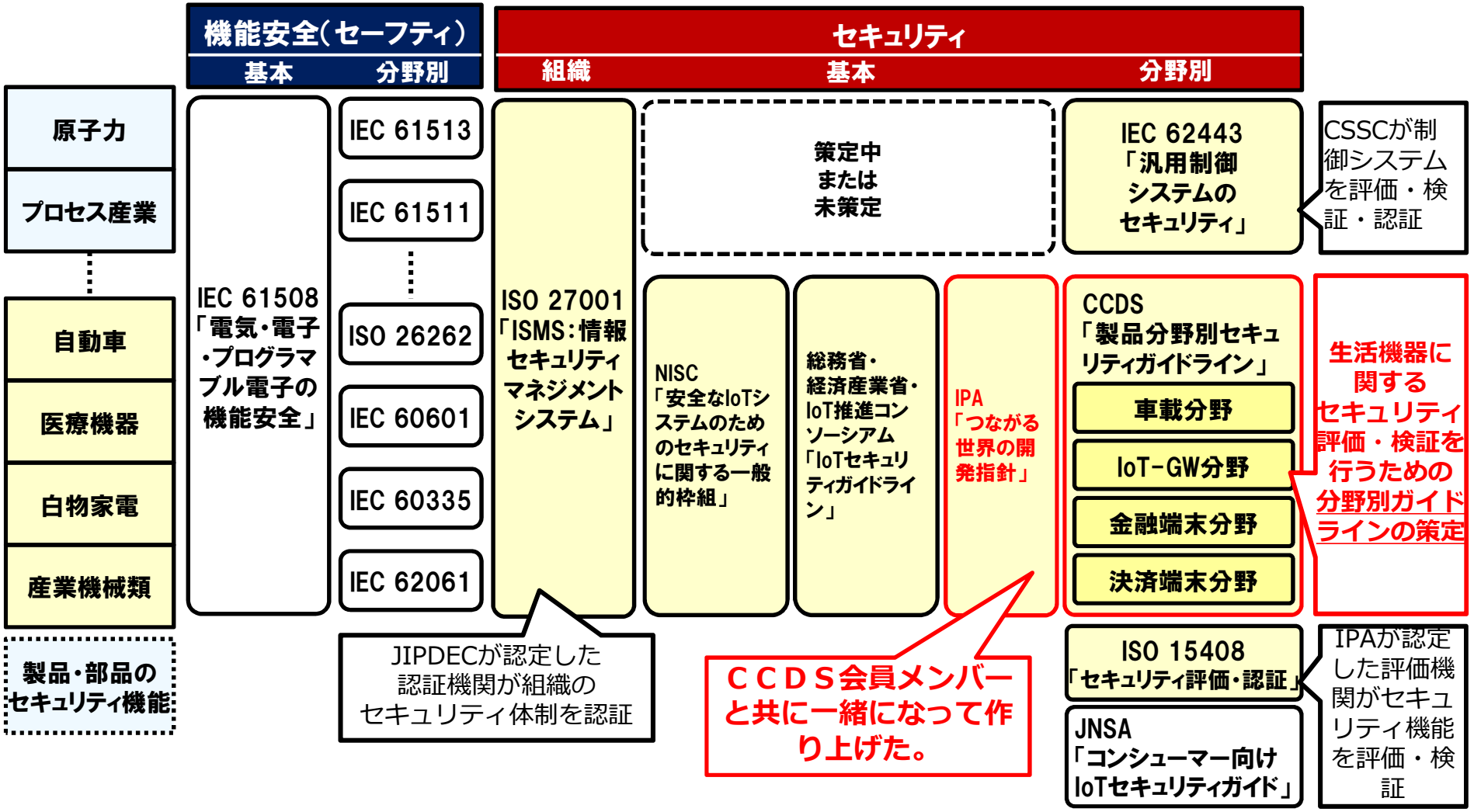


ht 2019 Connected Consumer Device Security Council Proprietary

規格策定への取り組み（2016-2018年度）

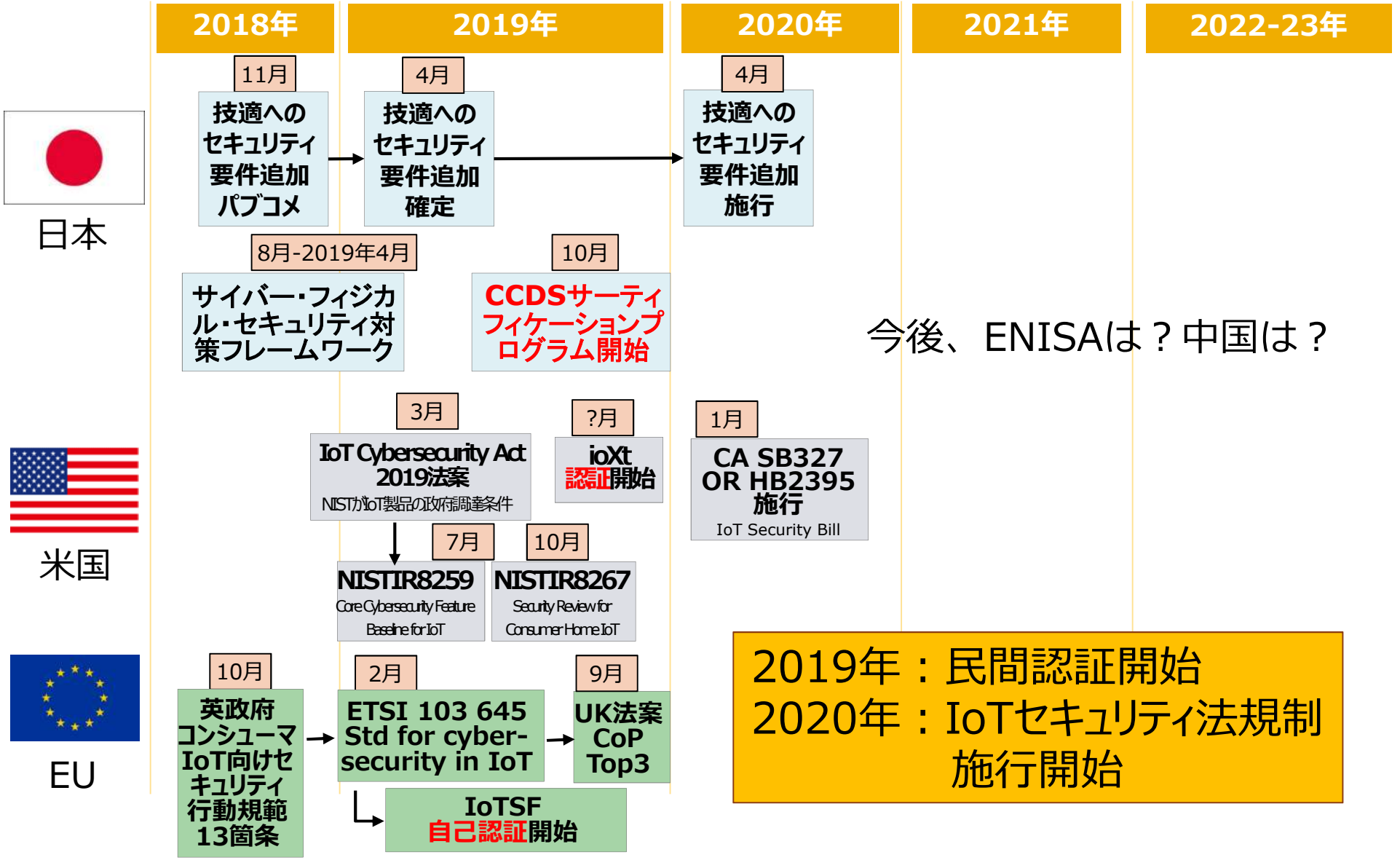
＜セーフティとセキュリティの国際規格の策定状況＞

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



Copyright 2019 Connected Consumer Device Security Council Proprietary

IoTセキュリティを取り巻く各国の動向



Copyright 2019 Connected Consumer Device Security Council Proprietary

CCDS 2019★1クラス要件

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
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
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
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. BluetoothSIG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、（USB）**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

Copyright 2019 Connected Consumer Device Security Council Proprietary

CCDSサーティフィケーションプログラム始動

- 11要件でスタート
- NHKニュース、日経、共同通信で配信
- マーク取得製品
  - 業務用カメラ
  - ATM
  - 決済端末
  - 給湯リモコン
  - 雨戸シャッター
- サイバー保険自動付帯

Copyright 2019 Connected Consumer Device Security Council Proprietary

参考：NISC

- サイバーセキュリティ関係法令の調査検討等を目的としたサブワーキンググループ

Copyright 2019 Connected Consumer Device Security Council Proprietary

AIとセキュリティ

- 技術の面
  - AI for Security（セキュリティ確保にAIを活用）
    - 予防－検知－対処
  - Security for AI（AIの信頼性確保のためのセキュリティ）
    - 教師データや遺伝的アルゴリズム操作対処

- 倫理の面
  - AIの振る舞い・結果に対する説明責任
  - 悪意あるAI vs 善意のAI
    - 裏側にいるエンジニアの倫理

Copyright 2019 Connected Consumer Device Security Council Proprietary

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

Copyright 2019 Connected Consumer Device Security Council Proprietary