経済産業省

資料４

サプライチェーンサイバーセキュリティ等に関する海外の動き

経済産業省　商務情報政策局

サイバーセキュリティ課

1. 米国の直近の動向

- NISTIR 8200 (Draft)
- 電力業界におけるサプライチェーンマネジメント強化
- ボットネット及びその他の自動化・分散化した脅威に対する対策

2. 欧州の直近の動向

- ESTI WORKSHOP : Cybersecurity Act - Establishing the link between Standardization and Certification
- Conference : Towards the EU Cybersecurity Certification Framework

1. 米国の直近の動向

- NISTIR 8200 (Draft)
- 電力業界におけるサプライチェーンマネジメント強化
- ボットネット及びその他の自動化・分散化した脅威に対する対策

NISTIR8200(Draft)の概要

- **2018年2月、NIST（アメリカ国立標準技術研究所）よりNISTIR8200のDraft版が公表された。**
- **5つのアプリケーション（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、脅威の分析及び国際標準化状況を整理したもの。**

ドキュメント名	Interagency Report on Status of International Cybersecurity Standardization for the Internet of Things (IoT)
発行元	IICS WG：The Interagency International Cybersecurity Standardization Working Group （WGはアメリカ国家安全保障会議のCyber Interagency Policy Committee (NSC Cyber IPC)に2015年12月に設置）
目的	IoTの概念を抽象化し、個人の安全とプライバシーを担保することを目的としている
IoTの構成要素	①ネットワーク接続されたデバイス、②システム、③これらにより構成されたサービスの3から構成されると定義

IoT 5つのアプリケーション（ユースケース）を定義

I. **コネクティッドカー（CV:Connected Vehicle）**：車両、道路、交通インフラが交通データを共有するサービス

II. **カスタマーIoT**：屋内のIoTアプリケーションと、ウェアラブル端末によるサービス

III. **ヘルスIoT・メディカルデバイス**：電子化された診察記録や患者から取得されたヘルスケアデータを共有するサービス

IV. **スマートビルディング**：エネルギー使用量監視システム、制御セキュリティシステム、照明制御システム等のサービス

V. **スマート製造**：データ、テクノロジー、高度な生産能力、クラウド、その他のサービスを統合するサービス

NISTIR8200(Draft)の目次

1. NISTIR 8200の目的と5つのアプリケーション(ユースケース)
   「NISTIR 8200　1、2章」

2. IoTの構成要素
   「NISTIR 8200　4章」

3. IoTアプリケーションの例
   「NISTIR 8200　5章」

4. IoTサイバーセキュリティの目的及びリスク・脅威
   「NISTIR 8200　7章」

5. アプリケーションごとの国際標準化状況
   「NISTIR 8200　9章」

6. サイバーセキュリティとIoTの11の視点
   「NISTIR 8200　6章」

NISTIR8200(Draft)のIoTの構成要素

環境	ネットワーク化され、システムに組み込まれるコンポーネントのセットとサポート技術。
システム	何らかの目標を達成するために、相互に作用するコンポーネントのセット。
コンポーネント	他のシステムのコンポーネントと連携して目標を達成できるシステムを形成する構成要素。

コンポーネントの機能性に着目した5つの能力

動作系	物理的な世界を変化させる能力を提供する。内部センサ、アクチュエータ、およびプロセッサを使用して物理的な世界で動作する。
データの保存	データおよび情報を記憶する能力を提供する。データ記憶能力のいくつかの例には、コンポーネント入力データの記憶およびコンポーネント生成データの記憶が含まれる。
ネットワーキング	ネットワーク機能は、物理的または論理的に別の場所にデータを移動する機能を提供する。イーサネット、米国電気電子学会（IEEE）802.11、RS-422等が関連する。
処理	アルゴリズムに基づいてデータを変換する能力を提供する。
センシング	物理的または論理的に感知する能力を提供する。検出能力を有する構成要素は、アナログ、デジタル形式の両方でデータを取得することができる。

コンポーネントの協調に着目した3つの能力

ヒューマン・ユーザ・インタフェース	コンポーネントが人と直接対話する能力を提供する。
ネットワークインターフェース	データを通信するために必要な通信ネットワーク構成要素間のインタフェースを提供する。すべてのコンポーネントには少なくとも1つのネットワークインターフェイス機能が必要である。
サポート機能	機能をサポートする。サポート能力のいくつかの例には、暗号化能力および認証能力等が挙げられる。

電力業界におけるサプライチェーンマネジメント強化

- **2018年1月18日に、米国連邦エネルギー規制委員会（FERC）は、電力業界に対して、強化されたサプライチェーンリスクマネジメント信頼性標準を採用することを提案した。**

整理番号	RM17-13-000
タイトル	Supply Chain Risk Management Reliability Standards サプライチェーンリスクマネジメント信頼性標準
概要	米国連邦エネルギー規制委員会（FERC）は、電力システムのサプライチェーンリスク管理保護を強化するために、新たに必須の信頼性基準を承認することを提案。 提案された基準は、グリッド関連のサイバーシステムのサプライチェーンに関連するサイバーセキュリティリスクを軽減するために、現在の重要インフラ保護基準を強化することを目的としている。 FERC指令No.829（2016年）は、産業用制御システムのハードウェア、ソフトウェア、コンピューティング及びネットワーキングサービスのサプライチェーンリスク管理に対処する基準を開発するよう指示しており、これを受け、北米電力信頼度協議会（NERC）は、FERC指令No.829に対応した標準を提案していた。

ボットネット及びその他の自動化・分散化した脅威に対する対策

- **2017年5月、トランプ大統領が「サイバーセキュリティ強化のための大統領令」に署名。**
- **2018年１月、大統領令を踏まえた報告書案を公表（セキュリティ確保のためのエコシステムの形成を強調）。**
- **2018年2月28日~3月1日、NIST、NTIA、DHSによるワークショップ開催。**
- **2018年５月、本報告書を大統領に報告予定。**

2017年5月大統領令

Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure（連邦ネットワーク及び重要なインフラストラクチャに対するサイバーセキュリティの強化に関する大統領令）　2017年5月11日
①連邦政府のネットワーク　②重要インフラ　③国家／国民のためのサイバーセキュリティ(ボットネット対策含む)に関して各連邦政府機関の長に対し、期限以内に大統領に報告書を提出するよう指示

2018年1月報告書案

A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats（ボットネットおよびその他の自動化・分散化した脅威に対するインターネット・通信のエコシステムの強靭性の強化に関する報告書）　2018年1月5日

ボットネット及びその他の自動化・分散化した脅威に対する対策

2018年2月ワークショップの主なプログラムと議論の内容

1. **Incentivizing Security**
   - DDoS対策について、乗っ取られている人自体にインセンティブが働かないので、どのように対応すべきか
   - 政府調達でセキュアな製品を大量に買うことで、セキュアな製品の価格を下げ、セキュアな製品の流通を促すようなインセンティブ策
   - 国際協調の重要性

2. **The Financial Community Perspective**
   - 金融業界のボットネット対策でFSISACが活躍した事例

3. **DDoS CSF Peofile and IoT functional profile**
   - CSFに沿った形で整理した企業のDDoS対策のプロファイル
   - IoT機器の対策に関するプロファイル

4. **Assessment, Certification, Evaluation?**
   - IoT機器のある程度のレベルの認証は前提としたうえで、C&C, Cloud, Device全体を含むエコシステムで考える重要性
   - 海外のIoT機器からのDDoS攻撃

2. 欧州の直近の動向

- **ESTI WORKSHOP : Cybersecurity Act - Establishing the link between Standardization and Certification**

- **Conference : Towards the EU Cybersecurity Certification Framework**

欧州における近年の動き

- 2016年、ＥＵ各国の重要インフラ事業者（エネルギー、交通、銀行、金融等）に対して、セキュリティ対策を義務化。その際セキュリティ関連国際標準を考慮することを指示。（NIS 指令）
- 2017年9月13日、ユンカー欧州委員会委員長の施政方針演説でサイバーセキュリティに関する言及があり、これを受けたデジタル単一市場の施策の一環として、新たにサイバーセキュリティ認証フレームワーク（EU Cybersecurity Certification Framework）の導入を検討していく旨公表。
- 2017年11月20日、ENISAが「IoTのベースラインセキュリティの推奨事項」を発表。
- 2018年2月13日、Cybersecurity Actに関する会議開催。（詳細、別スライド）
- 2018年3月1日、EU Cybersecurity Certification Frameworkに関する会議開催。（詳細、別スライド）
- 2018年5月から、EUの顧客データを扱う企業に対して、データ処理制限、流出などの際の通知義務などをEU域外においても義務化。（EU一般データ保護規則：GDPR）

Cybersecurity Act - Establishing the link between Standardization and Certification

- **2018年2月13日に、EU標準化団体(CEN、CENELEC及びETSI)とEUサイバーセキュリティ局(ENISA)による会議が開催された。**

1．欧州Cybersecurity Act:

- Cybersecurity Actの適用に向けたタイムラインは、2019年5月。
- 標準化ステークホルダーは、欧州委員会と協力して将来のスキームを準備し、2019年春までに用意。国の規制機関はセクターの標準化スキームの実装を開始。

2．欧州認証フレームワークの効果的な実装:

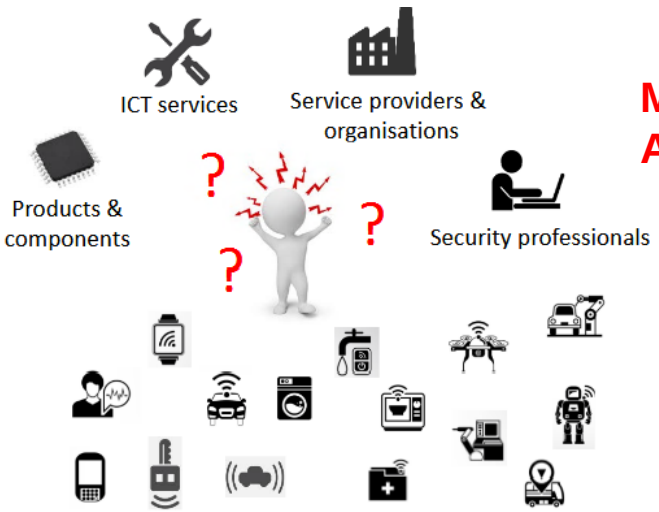
- ENISAは、欧州銀行連盟や保険分野と緊密に協力しながら、マルチステークホルダーアプローチを維持することが必要。
- 産業界は、Cybersecurity Actにおいて、セルフアセスメントによる対策により強調を置くことを要求。また、低、中、高の脅威レベルの閾値を策定する保証レベルの代わりに、企業がリスクを確認し、その対応を仕立てることを容易にするリスクベース分析を要求。

3．製品とサービスに関するサイバー分野標準化:

- 500を超える標準が存在しており、一から作り直す必要は無い。欧州委員会は、どの製品とサービスがターゲットとなっているのか明確にするために、ICT標準の優先リストの開発を維持。

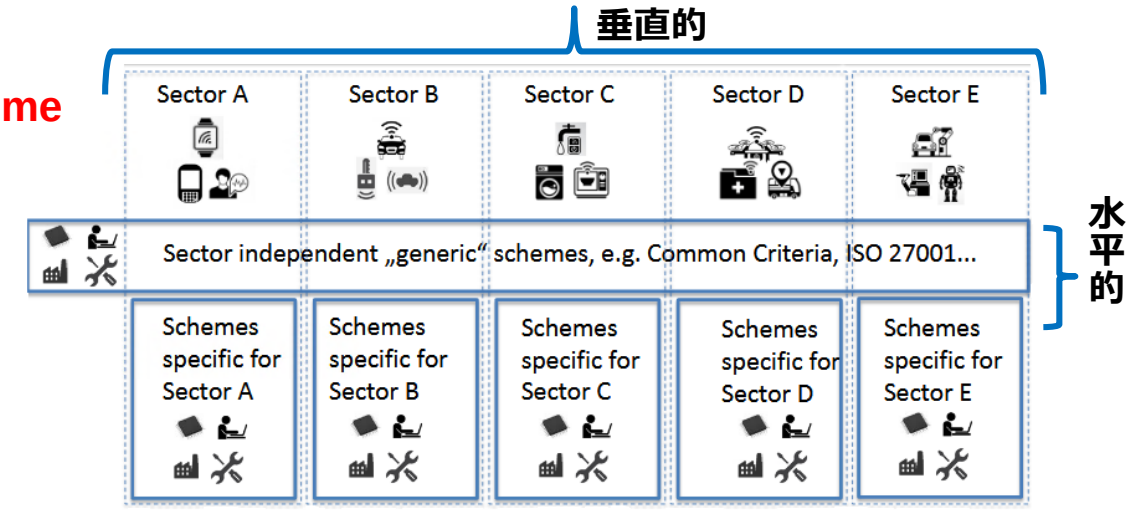
Conference: Towards the EU Cybersecurity Certification Framework

- **2018年３月1日に、欧州委員会とENISAによりEUのCybersecurity Certification Frameworkへ向けた会議が開催された。**



全ての要求を満たすスキームは存在せず、現時点で多くの標準とスキームが存在。

Meta-Scheme Approach



Meta-Scheme Idea

- **メタ言語を介した異なるスキーム横断の組み立て**
- **拡張可能な共通構造と再利用**
- **異なるスキームも定義可能**

欧州Cybersecurity Certification Frameworkの特徴

- 各国ICT認証の取り組みにより生じる断片化の回避
- 相互承認の推進
- 手続きの簡素化、IT製品とサービスの開発に掛かる期間とコストの低減
- 欧州の製品とサービスの競争力と品質の改善
- 一般消費者が購入するICT製品とサービスの信頼の確保