

# 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

平成30年12月25日

経済産業省 商務情報政策局

# サプライチェーンサイバーセキュリティ及びIoT機器のサイバーセキュリティに係る米国における最近の動き

時期	報告書等
2018年4月	<b>NIST Cybersecurity Framework version 1.1</b> <ul style="list-style-type: none"> <li>「サプライチェーンのリスク管理」「サイバーセキュリティリスクの自己評価」を追記</li> </ul>
2018年5月	<b>ボットネット対策等に関する報告書</b> <ul style="list-style-type: none"> <li>ボットネット等の脅威に対するネットワークのエコシステムの強靱性強化に関して5つの目標を設定</li> </ul>
2018年6月	<b>SP800-171 Rev.1 の更新</b> <ul style="list-style-type: none"> <li>セキュリティ要件を満たすために必要な具体的事項の記載を追加。</li> </ul>
2018年9月	<b>Draft NISTIR 8228</b> <ul style="list-style-type: none"> <li>IoT機器により生じる、サイバーセキュリティとプライバシーリスクを軽減するための対策例を整理</li> </ul>
2018年9月	<b>カリフォルニア州のIoTセキュリティ法</b> <ul style="list-style-type: none"> <li>インターネットに接続する機器に合理的なセキュリティ機能を備えることを製造者に求める法律</li> </ul>
2018年10月	<b>NIST Cybersecurity Whitepaper (元NISTIR 8222)</b> <ul style="list-style-type: none"> <li>IoT製品・サービスの信頼に影響を及ぼす17の技術的な懸念事項を整理</li> </ul>
2018年10月	<b>ICT Supply Chain Risk Management Task Force</b> <ul style="list-style-type: none"> <li>ICTサプライチェーンのリスクを特定、管理するために形成された官民パートナーシップ</li> </ul>
2018年11月	<b>対ボットネット強靱化ロードマップ</b> <ul style="list-style-type: none"> <li>5月の報告書で示した個々のボットネット対策のステークホルダー、実施スケジュールを整理</li> </ul>
2018年11月	<b>NISTIR 8200</b> <ul style="list-style-type: none"> <li>IoTの5つのユースケースに対するリスク、脅威分析及び国際標準化状況を整理</li> </ul>

# NIST Cybersecurity Framework の改定

- 2度の意見募集を踏まえた修正を行った上で、**2018年4月**、米国国立標準技術研究所（NIST）が「**Cybersecurity Framework Version 1.1**」を決定。
- 国際標準化に向けた活動も開始。

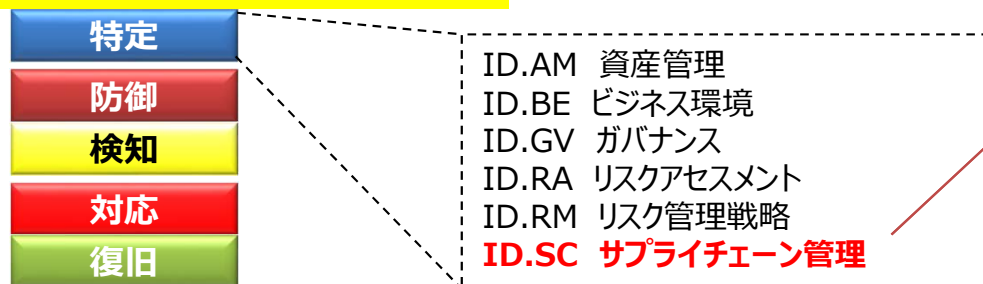
## NIST「Cybersecurity Framework」の経緯

- 2014年2月、サイバーセキュリティ対策の全体像を示し、「特定」、「防御」、「検知」、「対応」、「復旧」に分類して対策を記載した「Cybersecurity Framework Version 1.0」を策定。
- 2017年1月、「Cybersecurity Framework Version1.1 draft1」を公表。
- 2017年12月、「Cybersecurity Framework Version1.1 draft2」を公表。
- 2018年4月、「Cybersecurity Framework Version1.1」を決定。

## NIST「Cybersecurity Framework Version1.1」の特徴

- Version1.1は、Version1.0より特に以下の点が追記され、その重要性が説かれている。
  - サプライチェーンのリスク管理（**Supply Chain Risk Management**）
  - サイバーセキュリティリスクの自己評価（**Self-Assessing Cybersecurity Risk**）

### Cybersecurity Frameworkにおける5つの分類



Version1.1でID.SCが新規に追加され、**サプライチェーン全体で対策を実施すること**や、必要に応じて監査を行うことを要求

# NIST SP800-171 Rev.1 の更新

- CUI ※の保護を目的に14カテゴリ、110項目のセキュリティ要件から構成。
- NISTはSP800-171の定期的なメンテナンスを実施し、2018年6月7日にアップデート版を公表。

## APPENDIX F

### DISCUSSION

#### IMPLEMENTING AND ASSESSING CUI SECURITY REQUIREMENTS

Tables F-1 through F-14 provide discussion intended to facilitate implementing and assessing the CUI security requirements in NIST Special Publication 800-171. This information is derived primarily from the security controls and discussion in NIST Special Publication 800-53. It is provided to give assessors a better understanding of the mechanisms and procedures used to implement the safeguards employed to protect CUI. The discussion is *not* intended to extend the security requirements or the scope of the assessments of those requirements. NIST publications identified in the following tables are available at <https://csrc.nist.gov/publications>.

TABLE F-1: DISCUSSION ON ACCESS CONTROL REQUIREMENTS

<a href="#">3.1.1</a>	<b>SECURITY REQUIREMENT</b> Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	<b>DISCUSSION</b> Access control policies (e.g., identity- or role-based policies, control matrices, and cryptography) control access between active entities or subjects (i.e., users or processes acting on behalf of users) and passive entities or objects (e.g., devices, files, records, and domains) in systems. Access enforcement mechanisms can be employed at the application and service level to provide increased information security. Other systems include systems internal and external to the organization. This requirement focuses on account management for both systems and applications. The definition of and enforcement of access authorizations, other than those determined by account type (e.g., privileged versus non-privileged) are addressed in requirement <a href="#">3.1.2</a> .
<a href="#">3.1.2</a>	<b>SECURITY REQUIREMENT</b> Limit system access to the types of transactions and functions that authorized users are permitted to execute.
	<b>DISCUSSION</b>

2018年6月7日に公表されたアップデート版では、セキュリティ要件を満たすために必要な具体的な事項を記載した「APPENDIX F : DISCUSSION」が追加された。

例

3.1.13

**SECURITY REQUIREMENT**

リモートアクセスセッションの機密性を保護するために暗号メカニズムを採用する。

**DISCUSSION**

一般に適用される暗号標準には、FIPSで検証された暗号とNSAで承認された暗号が含まれる。

# 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 インターネット・通信のエコシステムの強靱性の強化に関する報告書

- 2017年5月の「サイバーセキュリティ強化のための大統領令」の署名を受けて、2018年5月30日に商務省（DoC）及び国土安全保障省（DHS）が、**ボットネット対策等のために官民が取るべき対策**を報告書として公表。
- 連邦政府が取り組むべき事項に力点を置き、関係者による様々な取組の調整・協働をサポートするための道筋を提示。
- DoC及びDHSに対して、**本報告書承認後120日以内に、産業界・社会・国際パートナーと協議し、初期ロードマップ策定を要請。**

## 報告で設定された5つの目標

- 適応可能、持続可能かつ安全な技術市場環境の実現に向けた明確な道筋の特定
- 進化する脅威に動的に対応するためのインフラのイノベーションの促進
- ネットワークのエッジにおけるイノベーションの促進による、自動化・分散化した脅威の防止、検出、影響の緩和
- 国内外のセキュリティ、インフラ、運用技術の各コミュニティ間の連携の促進と支援
- エコシステム全体にわたる啓発・教育の強化

# 報告書を受けた官民の取組

- 2018年5月の報告書を受けて、DoC及びDHSは同年11月、「**対ボットネット強靱化ロードマップ**」を公開。報告書で示している24のボットネット撲滅活動を5つの取組に分類した上で、**官民が行うべき個別のWorkstream（タスク）として、実施スケジュールと共に整理。**
- ロードマップの公表に合わせ、米国電気通信協会（USTelecom）、情報技術産業協議会（ITI）、全米家電協会（CTA）からなる The Council to Secure the Digital Economy（CSDE）が「**国際アンチボットネットガイド**」を公表し、政府による規制的アプローチに対して懸念を表明する一方、官民の強いパートナーシップを求めている。

## ロードマップにおける5つの取組・タスク

### 1. IoT機器のセキュリティ向上

- 信頼性の高いIoT機器の強固な市場の開拓
- エコシステム全体にわたるIoTセキュリティの持続的な適用

### 2. 企業のサイバーセキュリティリスクマネジメント

- NIST CSF を用いたプロファイル作成
- ネットワークアーキテクチャの高度化
- 企業のベストプラクティスの連邦政府への適用
- OTのサイバーセキュリティ対策

### 3. インフラ

- ルーティングのセキュリティ向上

- 実践的な情報共有の推進
- 情報共有プロトコルの開発
- インフラセキュリティ向上のための研究開発

### 4. セキュリティ技術の開発・移り変わり

- セキュアなソフトウェア市場の構築
- 国際協調
- 革新的な技術開発

### 5. 啓発と教育

- IoT機器のセキュリティに対する消費者の信頼を促進
- IoT機器のサイバーセキュリティの脅威に対する労働者の教育

# カリフォルニア州のIoTセキュリティ法

- インターネットに接続する機器に合理的なセキュリティ機能（例：機器固有のデフォルトパスワード設定、パスワードの初回起動時の変更等）を備えることを製造者に求める法律にカリフォルニア州知事が署名（2020年1月1日施行予定）

## 接続される機器（コネクティッド・デバイス）のセキュリティ法

- インターネットに接続する機器の製造者は、当該機器に合理的なセキュリティ機能または以下のすべてを備えたものとする。
  1. デバイスの性質と機能に適し、
  2. 収集、保管、または送信できる情報に適し、
  3. 不正なアクセス、破壊、使用、変更、または開示から、機器および機器に含まれるすべての情報を保護する設計
- ローカルエリアの外で認証を実施する機器は、以下のいずれかを満たす場合に、合理的なセキュリティ機能を備えているとみなす。
  1. あらかじめプログラムされたパスワードは、製造された各機器に固有のものであること
  2. 当該機器は、初回アクセスが許可される前にユーザーが新しい認証手段を生成しなければならないセキュリティ機能を備えていること

# NIST Cybersecurity Whitepaper – IoT Trust Concerns

- IoT製品やサービスが所望の動作を提供できるかどうかを判断する上では、利用者が使用するIoT、サービス、データを**信頼**できるかという観点が必要。
- IoT製品やサービスの信頼に悪影響を及ぼす可能性のある17の技術的な懸念事項について、一般的なIT技術者に広く理解を促すためのホワイトペーパー。

## 17の技術的懸念事項

1. 圧倒的なスケーラビリティ
2. 異種性
3. 所有者と管理の喪失
4. 合成性、相互運用性、統合性、互換性
5. 豊富な機能
6. 同期
7. 測定の欠如
8. 予測可能性
9. テストと保証
10. IoT認証基準の欠如
11. セキュリティ
12. 信頼性
13. データの整合性
14. 過剰なデータ
15. スピードとパフォーマンス
16. ユーザビリティ
17. 可視性と発見可能性



# Draft NISTIR 8228 – Consideration for Managing IoT Cybersecurity and Privacy Risks

- IoT機器の導入に伴い生じる、**サイバーセキュリティとプライバシーのリスクを軽減するための対策例**を整理。
- IoT機器の機能の多様性を踏まえ、機器のセキュリティ、データのセキュリティ、個人のプライバシー情報という3つの観点から対策例を提示した上で、NIST Cybersecurity Framework、SP 800-53 Rev.5 (Draft)、その他のIoTセキュリティ関連文書との対応関係を整理。

## IT機器と比較して、IoT機器がサイバーセキュリティリスク、プライバシーリスクに影響を与える3つの懸念

物理世界とデバイスとの相互作用	IoT機器の多くは、従来のIT機器では通常行わない方法で物理世界とのやりとりを行う。
デバイスアクセス、管理、モニタリング機能	IoT機器の多くは、従来のIT機器と同じ方法でアクセス、管理、監視することができない。
サイバーセキュリティ機能、プライバシー機能の可用性、効率、有効性	IoT機器のためのサイバーセキュリティ機能、プライバシー機能の可用性、効率、有効性は、従来のIT機器とは異なる。

## IoT機器のサイバーセキュリティリスク、プライバシーリスクを軽減する対処領域

機器のセキュリティを守る	• アセットの管理、脆弱性管理、アクセス管理、機器のセキュリティインシデント検知
データのセキュリティを守る	• データ保護、データのセキュリティインシデント検知
個人のプライバシー情報を守る	• 情報フローの管理、特定個人情報の処理権限の管理、特定個人情報の提供に際する意思決定、データ管理との分離、プライバシー違反の検知

# ICT Supply Chain Risk Management Task Force の発足と重要インフラのセキュリティ対策に係る新たな政府機関設置の設置について

- 2018年10月30日、国土安全保障省（DHS）は**国家保護・プログラム局（NPPD）のサイバーサプライチェーンリスクマネジメント（C-SCRM）プログラム**の一つとして、**ICT Supply Chain Risk Management Task Force** を設置した。
- また、同年11月16日、NPPDを格上げする形で、DHS内部の独立機関として**サイバーセキュリティ・インフラストラクチャー・セキュリティ庁（CISA）** が設立された。

## ICT Supply Chain Risk Management Task Force について

- グローバルICTサプライチェーンのリスクを特定し管理するための共通の提案を検討し、展開するために形成された官民パートナーシップ。11月15日に初会合が行われた（共同議長：ITI, CTIA）。
- 民間企業からは、Verizon や AT&T のような主要ISP、Cisco、Palo Alto Networks 等のネットワーク機器会社、Samsung、Intel、FireEye、Microsoft 等が参加している。政府機関からは、DHS、国防総省（DoD）、商務省（DoC）、共通役務庁（GSA）等が参加している。

## CISAについて

- CISAの役割は米国の重要インフラに対する物理的脅威及びサイバー攻撃の脅威から守ること。
- <CISAの取組>
- 国家リスク管理センター（National Risk Management Center）による重要インフラに対するあらゆる危機に対するリスク分析を提供する。
  - 緊急通信に関して、あらゆる政府レベルでの公共安全のための相互運用可能な通信の向上に取り組む。
  - 自然災害、テロ、その他の人災に際して、緊急対応者及び関連する政府関係者の通信が継続できる能力の維持及び促進のために全土での連携に取り組む。

# NISTIR 8200 – Status of International Cybersecurity Standardization for the IoT

- IoTの概念を抽象化することで、IoTコンポーネント、システム、アプリケーションの共通理解を図る。
- 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。
- 2018年2月にDraft公開後、2018年11月末に正式版が公表。

## NISTIR 8200 における IoT の基礎概念

IoTは、以下の2つの基礎概念から構成：

- ① N対Nの関係を提供するネットワークによって、コンポーネント間が接続される
- ② 一部のコンポーネントは、フィジカル空間からデータを収集するセンサや、フィジカル空間に影響を及ぼすアクチュエータを備える。

## IoTの5つのアプリケーション（ユースケース）

1. **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
2. **消費者向け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
3. **ヘルスケア・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
4. **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
5. **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

# NISTIR 8200 における 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及びサポート技術。
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。
<b>コンポーネント</b>	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	コンポーネントに与えられる入力情報に基づいて物理的な世界を変化させる能力を提供する（例：ヒータ、電子錠、モータ制御、ロボットアーム）。
センシング	フィジカル世界を論理的に感知する能力を提供する（例：温度センサ、CTスキャナ、カメラ、マイク）。
データの転送	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（例：イーサネット、IEEE 802.11 無線通信プロトコル）。
データの処理	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。
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。コンポーネントへの入力データだけでなく、コンポーネントが生成データの記憶も含む。

## コンポーネントの協調に着目した3つの能力

アプリケーション・インターフェース	アプリケーションを介してコンポーネントが他のコンピューティングデバイスと対話する能力を提供する。
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ーフェースを提供する。すべてのコンポーネントは少なくとも1つのネットワーク・インターフェース機能を備える必要がある。

## その他の能力

サポート機能	システムをサポートするための追加機能（例：協調動作、遠隔管理、認証）。
隠れている機能	外部からのアクセスにより有効化される機能（例：コンポーネントの機能を拡張させるUSBポート）。

# サプライチェーンサイバーセキュリティ及びIoT機器のサイバーセキュリティに係る欧州における最近の動き

時期	報告書等
2017年9月	<b>サイバーセキュリティ認証フレームワーク</b> <ul style="list-style-type: none"> <li>ネットワークにつながる機器を対象とした認証フレームワークの導入に向けた議論</li> </ul>
2017年11月	<b>Baseline Security Recommendations for IoT</b> <ul style="list-style-type: none"> <li>IoTセキュリティに関する課題を抽出し、解決に有用な考え方を念頭にベストプラクティスを整理</li> </ul>
2018年9月	<b>European Cybersecurity Centres of Expertise Map ~Definition and Taxonomy~</b> <ul style="list-style-type: none"> <li>サイバーセキュリティに関する活動を、①研究領域、②セクター、③適用・技術、の3次元で分類</li> </ul>
2018年9月	<b>Towards secure convergence of Cloud and IoT</b> <ul style="list-style-type: none"> <li>IoTとクラウドのセキュリティを「接続性」「分析」「統合」の3カテゴリに分類、セキュリティ課題を特定</li> </ul>
2018年10月	<b>消費者向けIoT製品のセキュリティに関する行動規範（英国）</b> <ul style="list-style-type: none"> <li>IoT製品の製造メーカー等が実践すべき対策を13項目のガイドラインにまとめたもの</li> </ul>
2018年11月	<b>Good Practice for Security of IoT in the context of Smart Manufacturing</b> <ul style="list-style-type: none"> <li>産業IoTのセキュリティ確保に求められる対策指針をポリシー・組織・技術という3つの側面で整理</li> </ul>
2018年11月	<b>セキュアルータの技術ガイドライン（ドイツ）</b> <ul style="list-style-type: none"> <li>“Mirai”の事例を受けて作成された、ルータのセキュリティ要件を定めた技術ガイドライン</li> </ul>

# サイバーセキュリティ認証フレームワーク

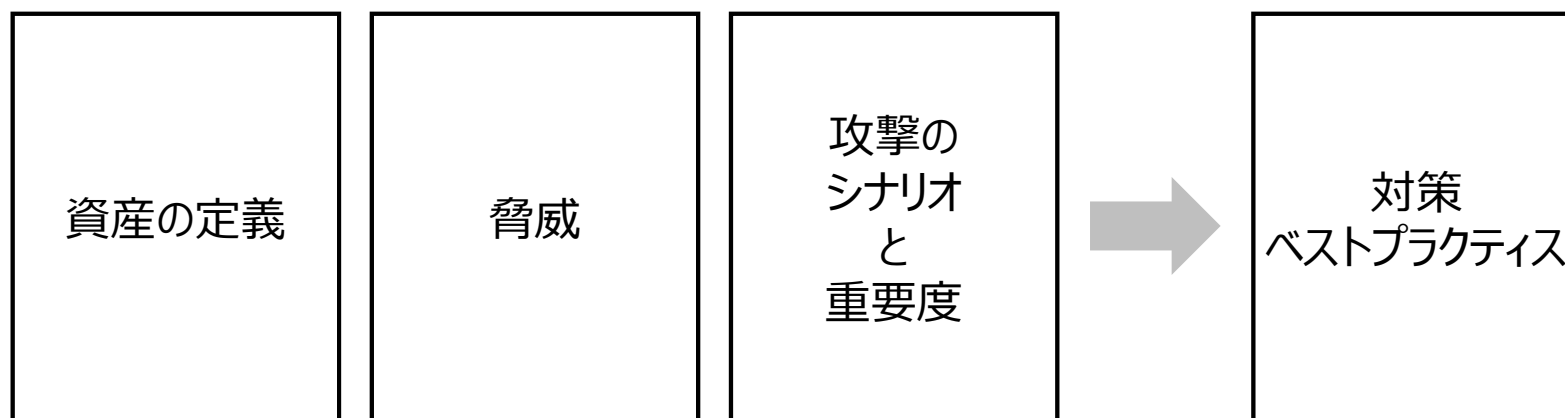
- 欧州では、「**Cybersecurity Certification Framework**」の導入に向けた議論が継続。欧州各国及び欧州議会で合意が取れば、ルータ等の具体的な製品・カテゴリ毎に基準が順次策定されていく予定。
- 一部で義務化を求める声もあり、11月末時点で合意は形成されていない模様。

## 欧州委員会、ENISAの動向

- 2017年9月、ユンカー欧州委員会委員長の施政方針演説で、EUにおけるサイバーセキュリティ政策（**Cybersecurity Act**）が発表され、新たなサイバーセキュリティ認証フレームワーク（**Cybersecurity Certification Framework**）の導入について言及。
- 2017年11月、ENISAが「**Baseline Security Recommendations for IoT**」（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、EU標準化団体とENISAにより「**Cybersecurity Act**」に関する会議開催
- 2018年3月、欧州委員会とENISAにより「**Cybersecurity Certification Framework**」に関する会議開催（2018年11月にも開催）
- 2018年9月、ENISAが「**Towards secure convergence of Cloud and IoT**」を発表
- 2018年9月、欧州委員会が「**European Cybersecurity Centre of Expertise ~Taxonomy and Definitions~**」を発表
- 2018年11月、ENISAが「**Good Practices for Security of Internet of Things in the context of Smart Manufacturing**」を公表
- 2019年5月、**Cybersecurity Act** の施行予定

# Baseline Security Recommendations for IoT (ENISA)

- IoTのセキュリティに関する一般的な課題を抽出し、関係者が解決するために有用となる考え方やツール（既存の規格、ガイドライン、研究資料等）、具体的な産業分野（スマートホーム、スマートカー等）を念頭においたベストプラクティスを紹介。



## 章の構成

- ・ スコープ【1.2】
- ・ 対象読者【1.4】
- ・ セキュリティ上の課題【2.2】
- ・ アーキテクチャ【2.4】
- ・ IoT 資産の分類【2.5】
- ・ IoT に対する脅威とリスクの分類【3.2】
- ・ 攻撃シナリオ【3.3】
- ・ セキュリティ対策／ベストプラクティス【4.1、4.2、4.3】
- ・ ギャップ分析【5】
- ・ 提言【6】

# European Cybersecurity Centres of Expertise Map

## ~Definition and Taxonomy~

- 欧州共同研究センター（JRC）がDG-CONNECTの協力を得て、国際標準規格等を参照しつつ、様々なサイバーセキュリティに関する活動を、①研究領域、②セクター、③適用・技術、の3つの次元で分類する方式を策定。
- これに基づき、各国における研究所等の専門領域を特定し、ネットワーキング等を促進。

### ①研究領域

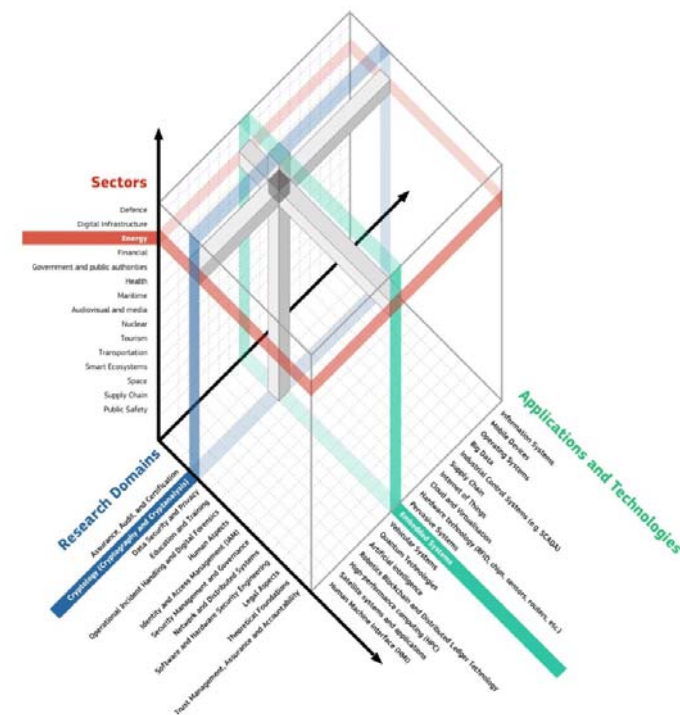
- 保証・監査・認証
- 暗号
- データセキュリティ・プライバシー
- 教育・訓練
- インシデントハンドリング・デジタルフォレンジック
- ヒューマンファクター
- ID・アクセス管理
- セキュリティ管理・統治
- ネットワーク・分散システム
- セキュリティエンジニアリング
- セキュリティ測量
- 法的観点
- 基礎的理論
- 信用の管理・保証・説明責任

### ②セクター

- 防衛
- デジタルインフラ
- エネルギー
- 金融
- 政府・公共機関
- ヘルスケア
- 海洋
- メディア
- 原子力
- 観光
- 運輸
- スマートエコシステム
- 宇宙
- サプライチェーン
- 公衆安全

### ③適用・技術

- AI
- ビッグデータ
- ブロックチェーン
- クラウド・仮想化
- 組込みシステム
- ハードウェア技術
- 高性能計算（HPC）
- HMI
- 制御システム
- 情報システム
- IoT
- モバイル端末
- OS
- 分散システム
- 量子技術
- 衛星システム
- サプライチェーン
- 車両システム

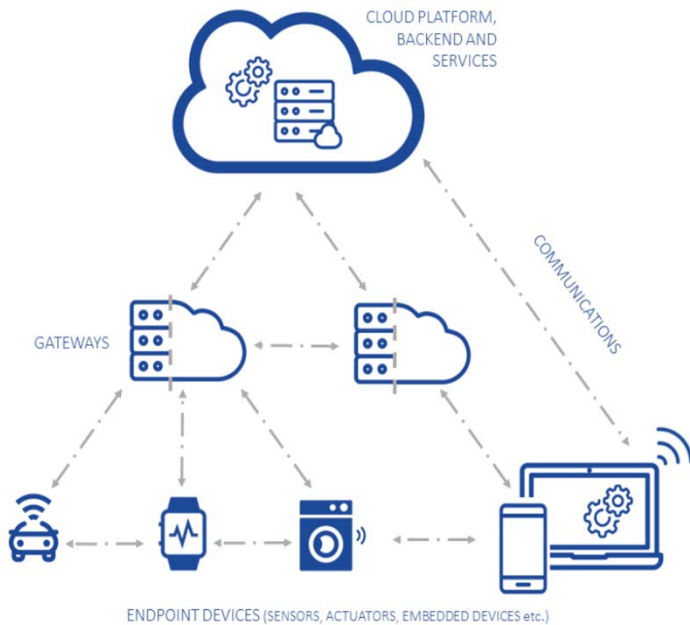


“European Cybersecurity Centres of Expertise Map - Definitions and Taxonomy” P26



# Towards Secure Convergence of Cloud and IoT (ENISA)

- IoTとクラウドを3つのカテゴリ（接続性、分析、統合）に分類し、セキュリティ課題を特定。
- IoTとクラウドの組み合わせに関する懸念に基づく攻撃シナリオを例示し、安全なソリューションを実現する方法を提示。



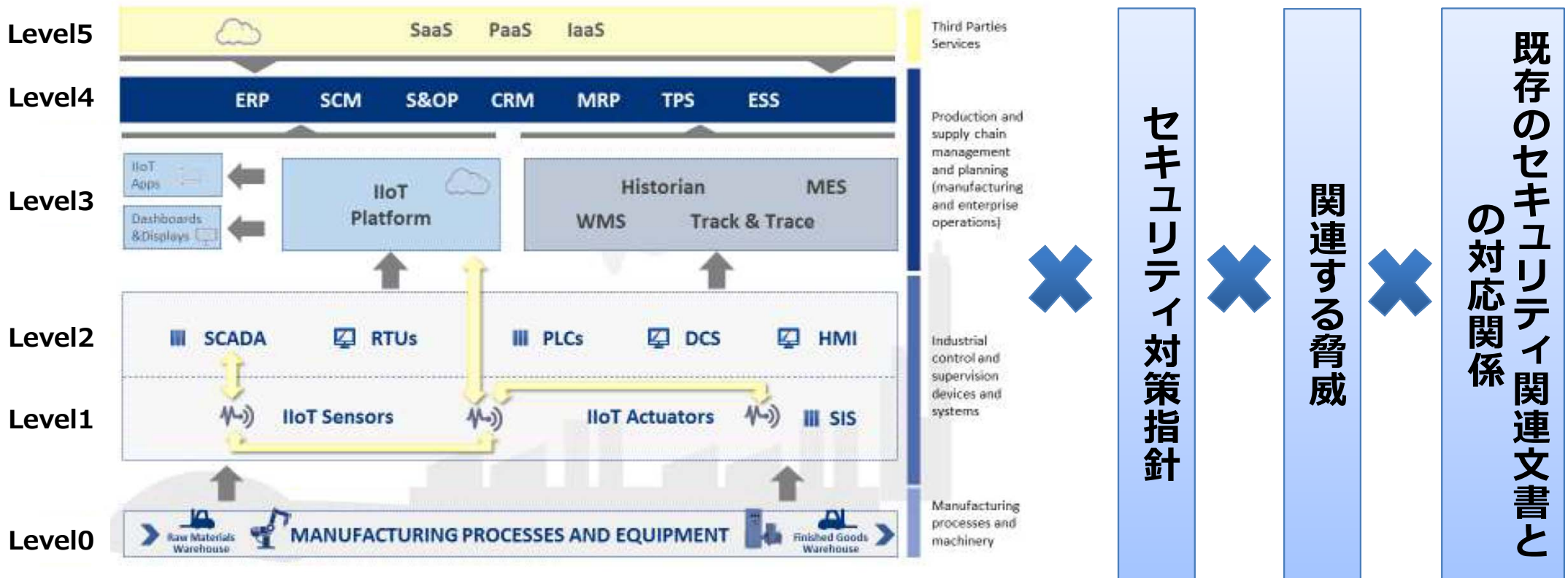
IoT Cloud を使用した IoTエコシステムのアーキテクチャ

カテゴリ	セキュリティ上の課題	セキュリティ上の脅威除去
<b>接続性</b> エンドポイント、ゲートウェイ及びおよびクラウド間の相互作用および通信	<ul style="list-style-type: none"> <li>• 通信のための異種プロトコル</li> <li>• エッジからクラウドへの安全でないデータフロー</li> </ul>	<ul style="list-style-type: none"> <li>• デバイスの仮想化による均質性の実現</li> <li>• セキュリティで保護された通信、セキュリティストリームの分析、※保存時のデータのセキュリティ対策</li> </ul>
<b>分析</b> IoTエコシステムの異なるレベルのIoTデバイスからのデータの処理、フィルタリングおよび集約	<ul style="list-style-type: none"> <li>• エッジでのリアルタイム処理がセキュリティを守らない</li> <li>• クラウドの分散化によるセキュリティへの影響</li> </ul>	<ul style="list-style-type: none"> <li>• エッジデバイスにおける物理的およびサイバーセキュリティ対策</li> </ul>
<b>統合</b> クラウドを介するIoTデバイスのクラウドAPIやリモートコマンド/コントロール (C&C) などによるデータのリアルタイム双方向フローを可能にする機能	<ul style="list-style-type: none"> <li>• セキュリティは、クラウドが提供している業種によって異なる</li> <li>• セキュリティはIoT開発者の実装に大きく依存する</li> <li>• 古いデバイス</li> </ul>	<ul style="list-style-type: none"> <li>• IoT環境へのセキュリティ要素の追加</li> <li>• ベースラインセキュリティ対策の採用</li> <li>• 自動化された安全なソフトウェアアップデート</li> <li>• 環境全体を通じたエンドツーエンドのセキュリティ対策</li> </ul>

# Good Practices for Security of Internet of Things in the context of Smart Manufacturing (ENISA)

- スマートマニュファクチャリングの観点から、産業IoTのセキュリティ確保に求められる対策指針をポリシー・組織・技術という三つの側面で整理。
- サイバーセキュリティの共通理解を促進するための用語定義、スマートマニュファクチャリングにおいて守るべき機器・サービス等の分類、産業IoTにおける脅威の分類を実施。
- セキュリティ対策ごとに既存のセキュリティ関連文書との対応関係も整理。

## 産業IoTにおける階層モデル



# 消費者向けIoT製品のセキュリティに関する行動規範（英国）

- 英国デジタル・文化・メディア・スポーツ省（DCMS）が、消費者向けIoT製品を利用するユーザのセキュリティに関する負担を軽減するために、IoT製品の開発、製造及び販売の段階で安全が確保されるよう、**製造メーカー等が実践すべき対策を13項目のガイドライン**にまとめ、2018年10月に公表。
- 記載されているガイドラインと、ENISAやIEEE等が公表している標準等との対応関係を表す「マッピング」文書も併せて公表。
- ETSIを通じた国際基準の策定にも関与しつつ、規制に向けた検討も今後行う予定。

## ベストプラクティス一覧（13項目）

1. デフォルトパスワードを使用しない
2. 脆弱性の情報公開ポリシーを策定する
3. ソフトウェアを定期的に更新する
4. 認証情報とセキュリティ上重要な情報を安全に保存する
5. 安全に通信する
6. 攻撃対象になる場所を最小限に抑える
7. ソフトウェアの整合性を確認する
8. 個人データの保護を徹底する
9. 機能停止時の復旧性を確保する
10. システムの遠隔データを監視する
11. 消費者が個人データを容易に削除できるように配慮する
12. デバイスの設置とメンテナンスを容易にできるように配慮する
13. 入力データを検証する

# セキュアルータの技術ガイドライン（ドイツ）

- 2016年にドイツ国内で発生したマルウェア“Mirai”の事案を受けて、情報セキュリティ庁（BSI）及び経済エネルギー省（BMWi）が**エンドユーザー向けルータのセキュリティ要件を定めた技術ガイドライン**を策定し、2018年11月に公表。
- 必須の要件（MUST）と推奨の要件（SHOULD）に整理。
- 規制ではなく自己宣言するものとして活用。当該要求事項を欧州のサイバーセキュリティ認証フレームワークの議論に持ち込み、欧州レベルでのルール化を目指す可能性。

## ガイドラインで求める必須要件の概要

- ルータが提供するすべてのサービスについて、使用するポートを含めて開示する
- 使用しないサービスのポートを閉じる
- ゲストモードで接続する機器について、他の機器やルータ設定へのアクセスを禁止
- 工場出荷時のパスワードは、ルータのモデル名やMACアドレスに関する情報から構成されないこと
- 工場出荷時のパスワードは、複数の機器で使い回してはならない
- パスワードは8字以上、英数字・記号の組み合わせでなければならない
- ファームウェアの更新機能を備える
- ファームウェア更新前にパッケージを検証する
- 製造メーカーは、重大な脆弱性に対するファームウェア更新の提供期間を情報開示し、サポート終了の際はその情報をルータ側でも確認できるようにする
- ファイアウォール機能を備える