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

平成31年4月4日

経済産業省　商務情報政策局

サイバーセキュリティ課

１．米国の最近の動き

（１）サプライチェーン及びIoT機器等

（２）重要インフラ（電力分野の例）

２．欧州の最近の動き

1．米国の最近の動き（サプライチェーン及びIoT機器等）

時期	サプライチェーン, フレームワーク	IoT機器
2018年4月 5月	**NIST Cybersecurity Framework version 1.1** • 「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	**ボットネット対策等に関する報告書（5月）** • 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靭性強化に関して5つの目標を設定
6月 9月	**NIST SP800-171 Rev.1 の更新** • 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。	**Draft NISTIR 8228（9月）** • 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
		カリフォルニア州のIoTセキュリティ法（9月） • 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
10月 11月	**ICT Supply Chain Risk Management Task Force** • 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	**NIST Cybersecurity Whitepaper（10月）** • 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
		対ボットネット強靭化ロードマップ（11月） • 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
		NISTIR 8200（11月） • 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
2019年2月	**NIST Privacy Framework のドラフト公表** • NISTで開発中のプライバシーフレームワーク（企業リスクマネジメントツール）のアウトラインを公表	**Core IoT Cybersecurity Capabilities Baseline（2月）** • サイバーセキュリティ機能のベースライン候補を公表
		Security for IoT Sensor Networks（2月） • センサネットワークのセキュリティ要件、脅威を整理

NIST Cybersecurity Framework の改定

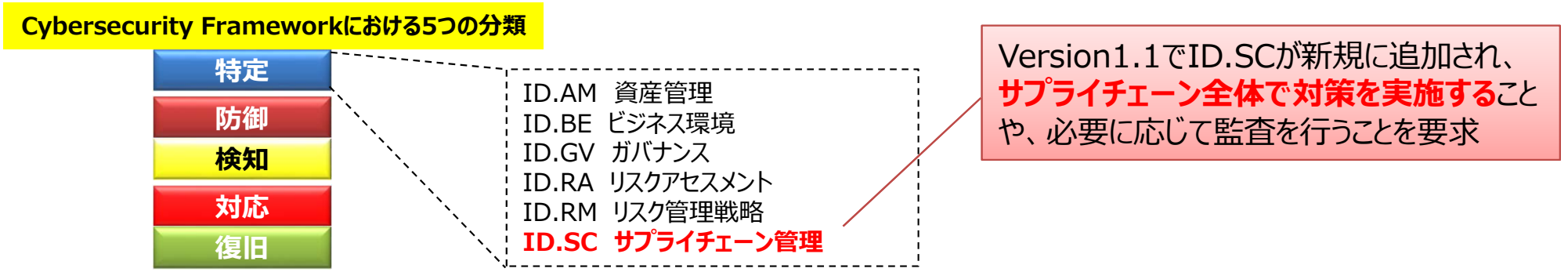
- 2度の意見募集を踏まえた修正を行った上で、**2018年4月**、米国国立標準技術研究所（NIST）が**「Cybersecurity Framework Version 1.1」を決定**。
- 国際標準化に向けた活動も開始。

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。

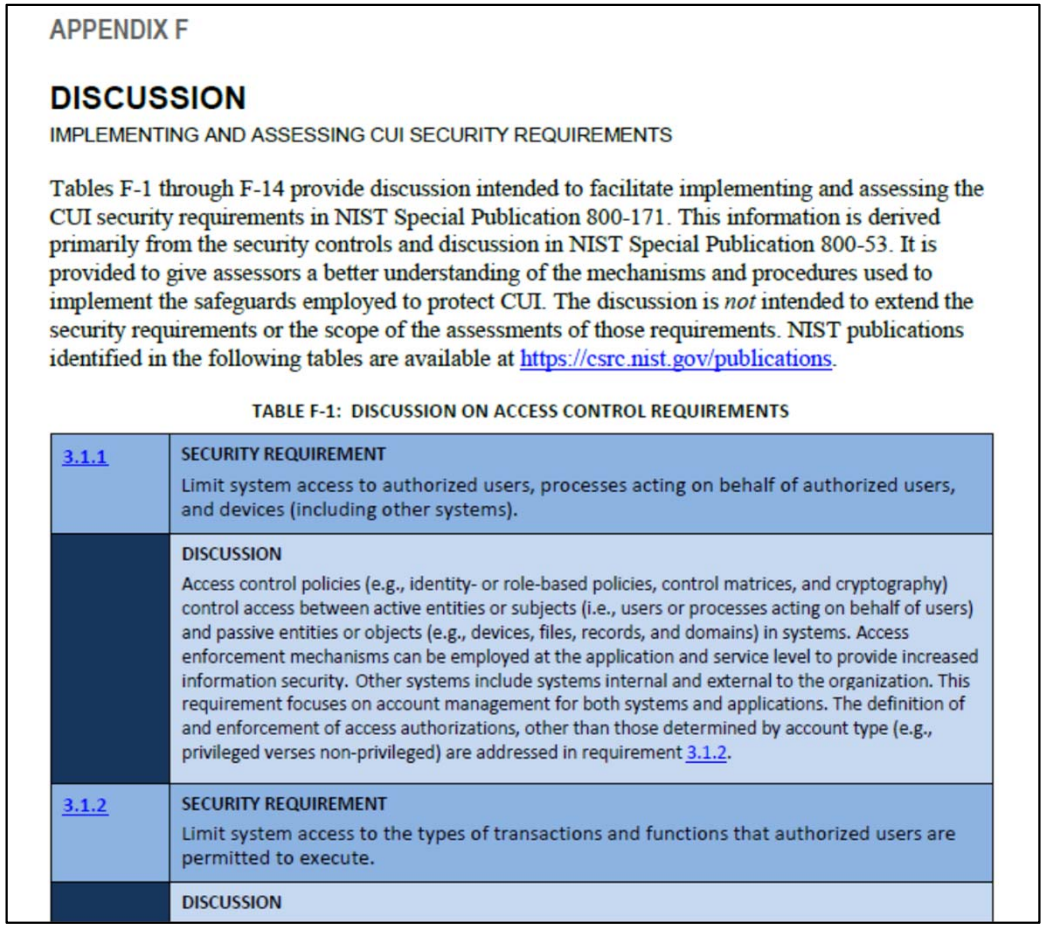
NIST「Cybersecurity Framework Version1.1」の特徴

- 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）



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

3.1.1	SECURITY REQUIREMENT Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems).
	DISCUSSION 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 verses non-privileged) are addressed in requirement 3.1.2.
3.1.2	SECURITY REQUIREMENT Limit system access to the types of transactions and functions that authorized users are permitted to execute.
	DISCUSSION

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。

※ Controlled Unclassified Information: 管理対象となるが秘密指定されていない情報

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。
- 2019年2月18日、25日にタスクフォースは会合を行い、**５つの優先事項のために活動する５つのワーキンググループが設置**した。ワーキンググループは３月中旬に初会合を開き、2019年の夏を目途に、一連の活動のとりまとめの公表を目指している。

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。

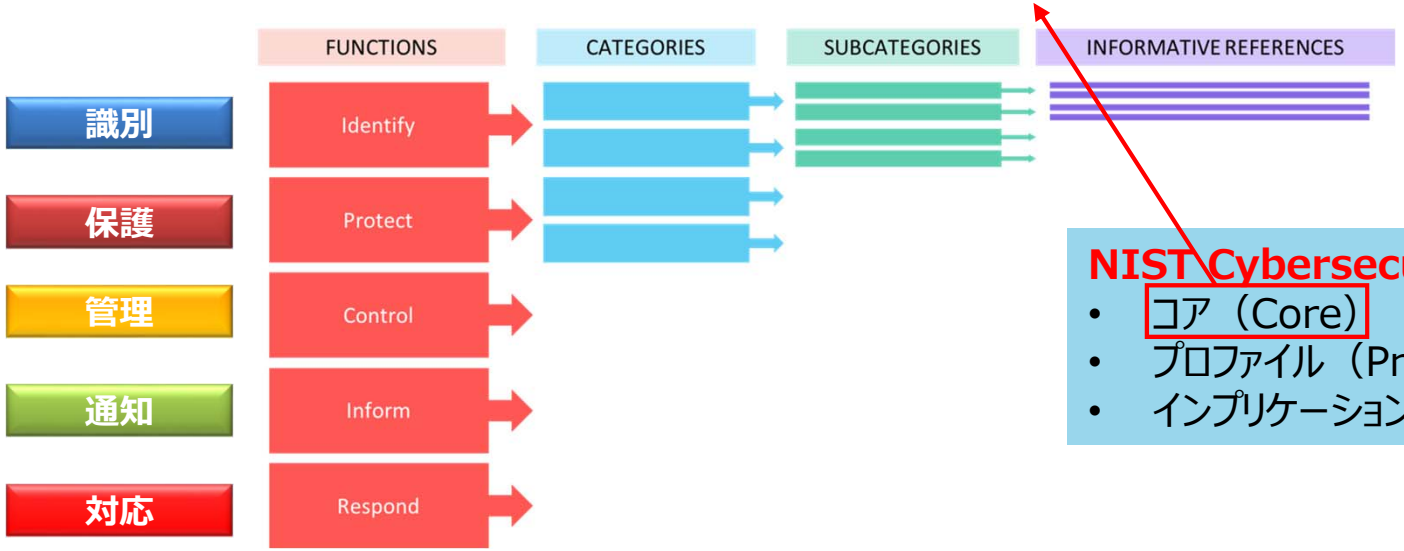
■ ５つの優先事項

・政府と産業全体にわたる既存のサプライチェーンのリスク管理に関するとりまとめの作成
・政府と民間部門との間の双方向の脅威情報共有の改善
・ICT製品及びサービスの脅威に基づく評価のためのプロセスと基準の策定
・資格のある入札者および製造元リストに関する推奨ポリシーの作成
・OEM及び正規販売代理店に関する調達規則の設定方法の作成

NIST プライバシーフレームワーク ワーキングドラフト公表

- NISTは、任意の（voluntary）**プライバシーフレームワーク（Privacy Framework）を開発中。**
- プライバシーフレームワークの目的は、以下のとおり。
  - **プライバシーリスク**のより適切な識別、評価、管理、及び伝達
  - 個人のプライバシーを保護するための**革新的なアプローチの開発**を促進
  - **製品やサービスの信頼**を高める
- 2018年11月、**プライバシーフレームワークの開発に関するパブリックコメント（RFI）を実施。**
- 2019年2月、RFIの意見を踏まえ、**プライバシーフレームワーク ワーキングドラフトを公表。**

プライバシーフレームワークのコア構造



NIST Cybersecurity Frameworkの構造を採用。
- コア（Core）
- プロファイル（Profile）
- インプリケーションティア（Implementation Tiers）

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靭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。政府による規制的アプローチに対して懸念を表明するとともに、官民の強いパートナーシップを求めている。

International Anti-Botnet Guide

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うる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機器ためのサイバーセキュリティ機能、プライバイシー機能の可用性、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

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月にドラフト版を公開後、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。
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	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はなく、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・インターフェイ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）。

Considerations for a Core IoT Cybersecurity Capabilities Baseline

- ボットネット報告書及びNISTIR 8228を踏まえて、NISTは、2019年2月にIoT機器のサイバーセキュリティ機能のコアとなる、12のベースライン候補を公表。現在、パブリックコメントを実施中。

12のベースライン候補

○ 全て又はほとんどのIoT機器に適用されるベースライン候補

1．論理的かつ物理的に識別できる。
2．ソフトウェア及びファームウェアは、安全で制御された設定可能な機構を用いてアップデートできる。
3．許可されたユーザーは、安全な「デフォルト」状態への復元を含めて、機器の設定を安全に変更できる。機器設定に対する許可されていない変更を防ぐことができる。
4．機器及び機器インターフェースへのローカル及びリモートのアクセスを制御できる。
5．保存及び送受信されたデータを保護するための暗号を使用できる。
6．機器通信のすべての層に、業界が承認した標準化されたプロトコルを使用できる。
7．サイバーセキュリティイベントの詳細をログに記録し、許可されたユーザー及びシステムがそれらにアクセスできる。
8．機器上の全ての保存データは、許可されたユーザーによってリセットでき、全ての内部データストレージから安全に削除される。

○全てのIoT機器に要求するには適さない可能性があるベースライン候補

9．ソフトウェア、ファームウェア、ハードウェア及びサービスの全ての取得元を確認するための情報が開示され、アクセスできる。
10．バージョンやパッチの状態を含む、現在の機器内部のソフトウェア及びファームウェアの一覧が開示され、アクセスできる。
11．機器の設計や設定を通じて、機能を最小限とする指針を実施できる。
12．物理的なアクセスを制御できるように設計される。

Security for IoT Sensor Networks

- 無線センサの市場は2016年時点で573百万ドル、2023年には少なくとも1.2兆ドルに成長する見込みであり、安価なIoTセンサのセキュリティ対策が求められている。
- NIST内のNCCoEは、**ビル管理システムのIoTセンサネットワーク**防御をユースケースとして、**センサネットワークに求められるセキュリティ要件、脅威等**を整理し、2019年2月にドラフト版を公表。
- センサネットワークを構成するコンポーネント毎に、セキュリティ要件、脅威、具体的なセキュリティ技術、NIST Cybersecurity Framework サブカテゴリとの対応関係を整理

【センサネットワークを構成するコンポーネント】

- **センサ（温度、湿度、動作センサ等）**
  - マイクロコントローラとセンサにより構成
  - 運用は無線だが、設定は有線の場合もある
- **ベースステーション／アグリゲータ**
  - 無線等を介してセンサから受信・集約したデータをコントローラへ送付
  - コントローラからの指示をセンサに送信
- **コントローラ**
  - センサのデータを処理し、センサに指示する
  - ソフトウェアの他に Rasberry Pi 等でも実装可能
- **通信路**
  - センサデータ、制御信号の伝送路

【コンポーネント毎の整理】

公開されるインターフェイス
想定される攻撃ベクトル
セキュリティ要件
具体的なセキュリティ技術
NIST Cybersecurity Framwork との対応関係

１．米国の最近の動き
（１）サプライチェーン及びIoT機器等
（２）重要インフラ（電力分野の例）

２．欧州の最近の動き

米国の電力業界におけるサイバー攻撃の懸念を踏まえた動向①

- 2018年7月31日、米国連邦エネルギー規制委員会(FERC)※1 は北米電力信頼度評議会(NERC)※2 に対し、インシデント報告に係る要求基準の強化を指示。NERCは10月1日にまでに基準を改定。
- 2018年8月16日、NERCは大規模電力システム※3 制御センター間の通信の保護に係る新基準を決定。

※1 FERC：米国エネルギー省（DoE）の管轄下の機関。
※2 NERC：FERCが電力信頼度機関（ERO）として認定。FERCの監督の下、NERCは電力セクターのセキュリティ基準の作成・監査を実施。違反には罰金。
※3 大規模電力システム：BES（Bulk Electronics System）。大規模発電設備、送電・配電設備のうち大きな停電につながる可能性がある設備の総称（NERCが定義）

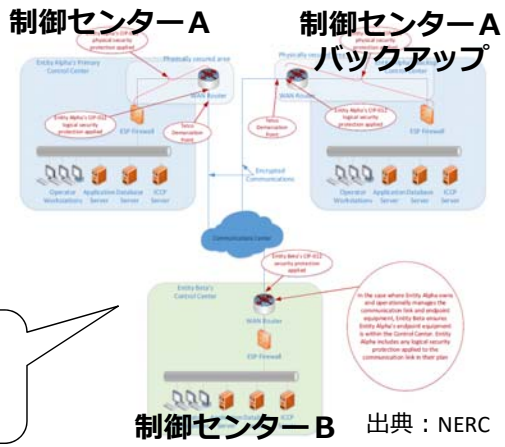
インシデント報告に係る要求基準強化の指示（7/31 FERC）

- 2015-2016年にインシデント報告が無かったことを踏まえ、攻撃が失敗（attempt to achieve）した場合のインシデント報告も義務化（※ 現行のNERC基準CIP-008-5では、被害があった場合のみ報告を義務化）
- インシデント報告に求められる最低限の情報を標準化（※ 機能的影響（示せる場合）、攻撃経路、侵入のレベルを報告に含める。）
- インシデントの深刻度に応じた報告タイムラインを設定（※ 重大事象ほど迅速な報告が求められる。）
- E-ISACに加え、DHSのNCCIC ICSに対してもインシデント報告を義務化

大規模電力システム制御センター間の通信の保護に関する基準（8/16 NERC）

- 新たなCIP（Critical Infrastructure Protection）標準であるCIP-012-1を策定。（※ NERCはこれまでセキュリティ関連の主なもので約10の基準を策定。）
- 電力システムのリアルタイム監視データ等を大規模電力システム制御センター間で通信する際に必要となるセキュリティ対策の策定・実施や役割分担の明確化を求めている。

CIP-012-1基準の履行ガイドラインの草案では、制御センター間で通信をする際に必要となる対策の例として、拠点間の通信の暗号化や通信機器の物理セキュリティ対策など、具体的に記述。



出典：NERC

米国の電力業界におけるサイバー攻撃の懸念を踏まえた動向②

- 2018年10月31日、米国連邦エネルギー規制委員会(FERC)は、**新たなサプライチェーンリスク対策**として、北米電力信頼度評議会(NERC)が新たに作成・更新したCIP-013-1,CIP-005-6,CIP-010-3を承認。
- さらにFERCは、**NERCに対するOrder 850を発行**。

CIP-005-6（Cyber Security - Electronic Security Perimeters）

影響度「中」又は「大」の大規模電力システムにおいて、ベンダーからのリモートアクセスのセッションを把握する手段を１つ以上持つこと（Requirement 2.4）及び無効化する手段を１つ以上持つこと（Requirement 2.5）という要求事項が追加。

CIP-010-3（Cyber Security - Configuration Change Management and Vulnerability Assessments）

影響度「中」又は「大」の大規模電力システムにおいて、ソフトウェアのソースのidentityとintegrityを検証することという要求事項が追加。

CIP-013-01（Cyber Security - Supply Chain Risk Management（新規））

影響度「中」又は「大」の大規模電力システムにおいて、サプライチェーン・サイバーセキュリティ・リスクマネジメント計画として、ベンダーのサイバーインシデントの報告、ベンダーの脆弱性公表、ソフトウェア検証等に関するプロセスの策定等を要求。

Order 850

監視制御システム（EACMS：Electronics Access Control or Monitoring Systems。FW、認証サーバ、IDS、SIEM等。）についてもNERCのサプライチェーン対策のスコープに含むよう指示。

出典ITTA

いずれも米国の電力業界（The Edison Electric Institute, Electronic Power Supply Association, the Electricity Consumers Resource Council）から反論を受けている模様

米国の電力業界におけるサイバー攻撃の懸念を踏まえた動向③

- 2019年2月6日、北米電力信頼度評議会（NERC）は、大規模電力システム※1に係るサプライチェーンリスクへの対応策を提言した報告書『**サプライチェーンのサイバーセキュリティ・リスク（Cybersecurity Supply Chain Risks）**』のドラフトを発表。
- 本報告書は、**米国連邦エネルギー規制委員会（FERC）によるOrder 850※2に応えたもの**となっている。

※1　大規模電力システム：BES（Bulk Electronics System）。大規模発電設備、送電・配電設備のうち大きな停電につながる可能性がある設備の総称（NERCが定義）
※2　Oder 850：FERCからNERCへの指示であり、現状NERCのサプライチェーン対策の対象に含まれていない監視制御システム（EACMS）についても対象とせよ、との提示。

背景・特徴

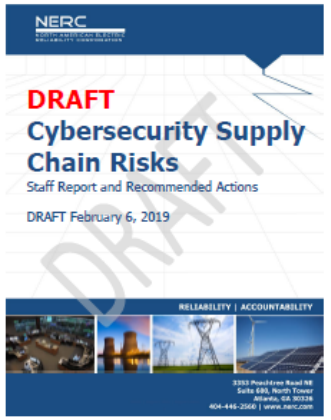
- FERC は2018年10月にサプライチェーン基準（NERC CIP-013-01等）を承認した際、現状対象外である**監視制御システム（EACMS）**及び**物理的アクセス制御システム（PACS）**について、サプライチェーン対策の新たな対象とすべく検討するよう指示（Oder 850）しており、NERCは本報告書によりこの指示に応えたもの。
- 本報告書の特徴は、制御システム（EACMS及びPACS）を対象としたことで、構成部品の確認、供給業者の特定、当該装置に係る特定リスクの評価等、**製品レベルでの具体的な対応策を盛り込んでいる**点が挙げられる。

➡ 将来的に、基準・標準・認証につなげていく可能性を注視

内容（項目）

- 監視制御システム（EACMS）及び物理的アクセス制御システム（PACS）を、**新たなサプライチェーン基準として組み込む**こと
- 大規模電力システム（BES）に係る調達プロセスを策定する際、①第三者によるプロセスの認証、②物資の安全な配送、③セキュリティ仕様の環境に応じた調整、④オープンソース等サポートされていないツールを利用する際のリスクの軽減、⑤影響度の低いリスクへの対策の自主的な適用、といった観点から、**業界ガイドライン及びプラクティスを参照**すること

等を提言している。



NERC : Cybersecurity supply Chain Risks(DRAFT)
(Member Representatives Committee | Feb 6,2019)

米国大手電力会社Duke Energy社におけるCIP基準違反

- 2019年1月25日、**北米電力信頼度評議会(NERC)**※が**米国大手電力会社Duke Energy社**に対して127の**CIP基準違反**（多くは自己申告）のため**1,000万ドルの罰金**を科す。
- さらに、Duke Energy社は、和解契約（Settlement Agreement）により**改善措置を講じる必要**がある。

※ **北米電力信頼度評議会（NERC）**
米国連邦エネルギー規制委員会(FERC)が電力信頼度機関（ERO）として認定。
FERCの監督の下、NERCは電力セクターの**セキュリティ基準（CIP）**の作成・監査を実施。違反には罰金。

CIP基準違反の例

- **ファイアウォールの不適切な設定**。
- 重要なサイバー資産に関する**機密情報の保護不全**。
- 適切な許可を得ずに従業員が**機密情報へのアクセスが可能**。
- 多要素認証なしで**機密システムへのリモートアクセスを許可**。

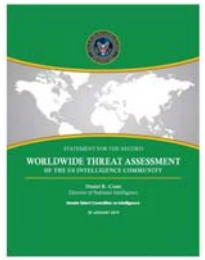
改善措置の例

- **上位管理職による関与と監督**の強化。
- **統一的なCIP監視部門**の設置。
- 資産と構成の管理、訪問者のログ記録、アクセス管理、及び構成の監視と脆弱性評価に関連する**全社規模のツールへの投資**。
- コンプライアンスとセキュリティの取り組みを管理及び実施するための**リソースの追加**。
- **コンプライアンス訓練**の実施

米国政府の重要インフラ（電力業界含む）に対するサイバー攻撃の懸念

- Duke Energy社は、米国電力業界において、セキュリティ対策が進んでいる会社と考えられており、**Duke Energy社への罰金は、米国政府による他の電力会社に対しての警告**との意見がある。
- 米国政府の**重要インフラ（電力業界含む）に対する中国やロシアのサイバー脅威の高まりが背景**にあると考えられる。

1/29発表　米国世界脅威評価報告書（US World Wide Threat Assessment）



- **中国**は、米国の軍事及び**重要インフラシステム**に対して、**持続的なサイバースパイと攻撃の脅威**を有する。

China

China presents a persistent cyber espionage threat and a growing attack threat to our core military and critical infrastructure systems. China remains the most active strategic competitor responsible for

- **ロシア**は、2015年と2016年にウクライナで実証されたものと同様に、**配電網**を少なくとも数時間破壊するなど、**重要インフラに局所的で一時的な破壊的影響を与えるサイバー攻撃能力**を有する。

Russia has the ability to execute cyber attacks in the United States that generate localized, temporary disruptive effects on critical infrastructure—such as disrupting an electrical distribution network for at least a few hours—similar to those demonstrated in Ukraine in 2015 and 2016. Moscow is mapping our critical infrastructure with the long-term goal of being able

１．米国の最近の動き
（１）サプライチェーン及びIoT機器等
（２）重要インフラ（電力分野の例）

２．欧州の最近の動き

２．欧州の最近の動き

時期	報告書等
2017年9月	**サイバーセキュリティ認証フレームワーク** • 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
2017年11月	**Baseline Security Recommendations for IoT** • 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
2018年9月	**European Cybersecurity Centres of Expertise Map ~Definition and Taxonomy~** • 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
2018年9月	**Towards secure convergence of Cloud and IoT** • 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
2018年10月	**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）** • 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
2018年11月	**Good Practice for Security of IoT in the context of Smart Manufacturing** • 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
2018年11月	**セキュアルータの技術ガイドライン（ドイツ）** • “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
2018年12月	**サイバーセキュリティ認証フレームワーク** • 欧州議会、欧州連合理事会、欧州委員会が「Cybersecurity Act」を政治合意
2019年2月	**Cyber Security for Consumer Internet of Things （ETSI）** • 英国「消費者向けIoT製品のセキュリテイに関する行動規範」に基づく欧州標準

欧州サイバーセキュリティ認証フレームワーク

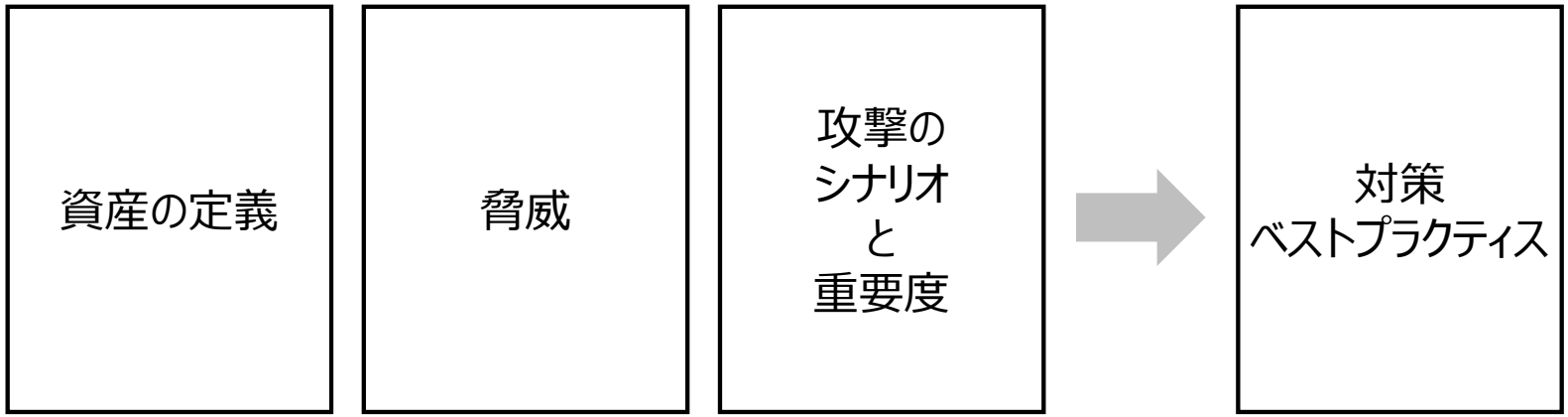
- 2018年12月、「Cybersecurity Certification Framework」の創設を含む「Cybersecurity Act」の内容について、欧州議会、欧州連合理事会、欧州委員会が政治合意。
- 今後、欧州議会と欧州連合理事会で正式に承認をされたのち、ルータ等の具体的な製品・カテゴリ毎に基準が順次策定されていく予定。

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
- 2018年12月、欧州議会、欧州連合理事会、欧州委員会が「Cybersecurity Act」を政治合意。
- 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

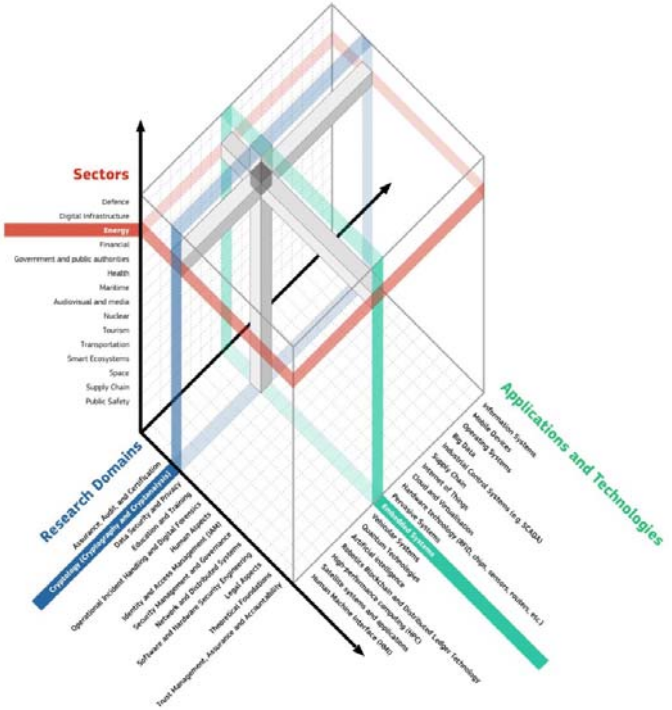
- 保証・監査・認証
- 暗号
- データセキュリティ・プライバシー
- 教育・訓練
- インシデントハンドリング・デジタルフォレンジック
- ヒューマンファクター
- ID・アクセス管理
- セキュリティ管理・統治
- ネットワーク・分散システム
- セキュリティエンジニアリング
- セキュリティ測量
- 法的観点
- 基礎的理論
- 信用の管理・保証・説明責任

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

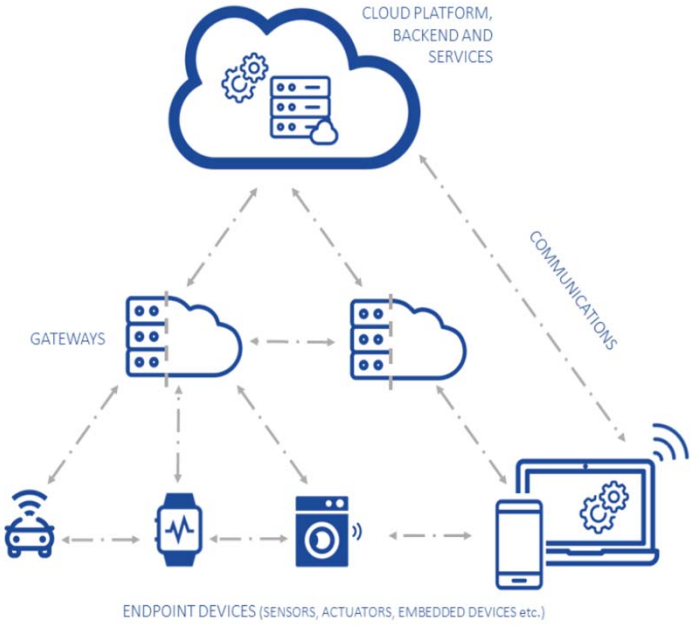
- AI
- ビッグデータ
- ブロックチェーン
- クラウド・仮想化
- 組込みシステム
- ハードウェア技術
- 高性能計算（HPC)
- HMI
- 制御システム
- 情報システム
- IoT
- モバイル端末
- OS
- 分散システム
- 量子技術
- 衛星システム
- サプライチェーン
- 車両システム



“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。



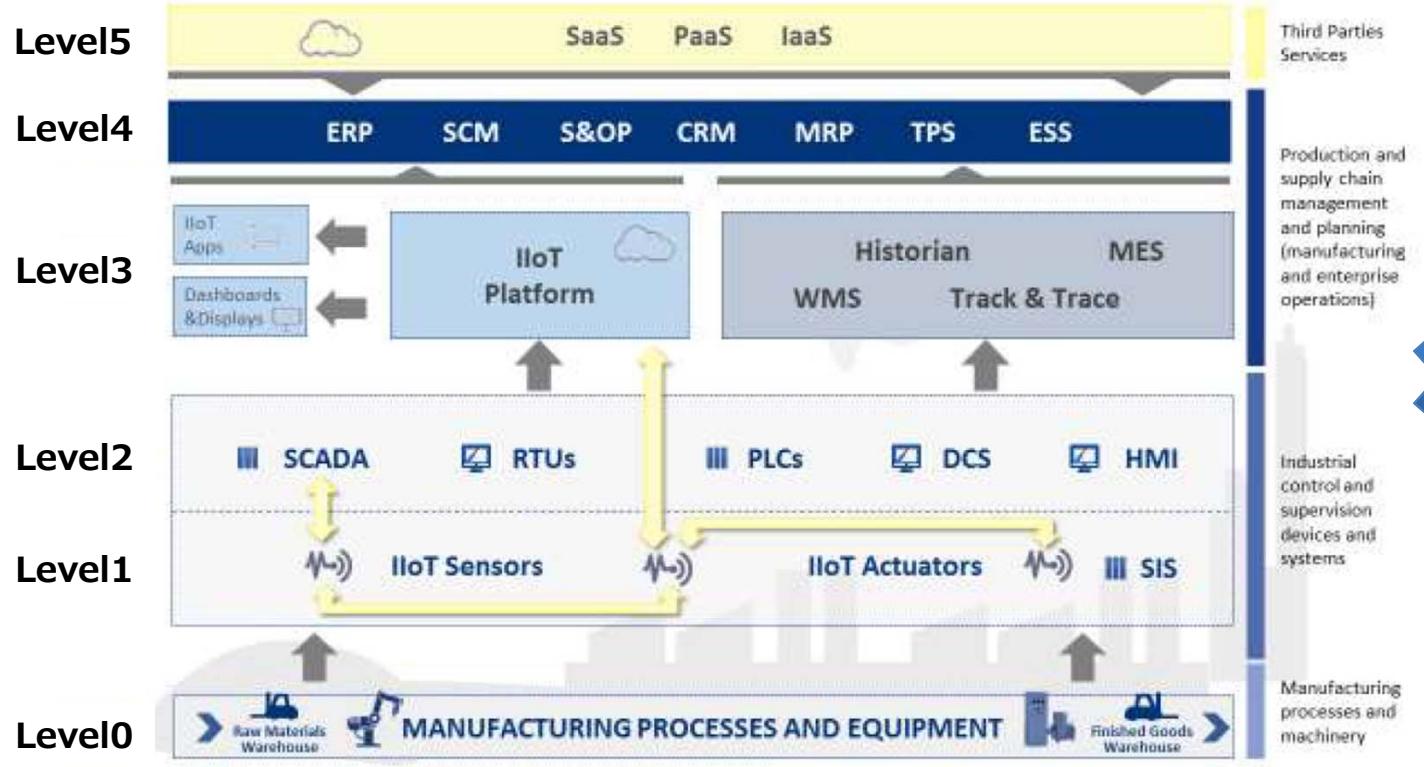
IoT Cloud を使用した IoTエコシステムのアーキテクチャ

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
接続性 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	• 通信のための異種プロトコル • エッジからクラウドへの安全でないデータ フロー	• デバイスの仮想化による均質性の実現 • 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
分析 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	• 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 • クラウドの分散化によるセキュリティへの影響	• 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
統合 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	• 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 • セキュリティはIoT開発者の実装に大きく依存する • 古いデバイス	• IoT環境へのセキュリティ要素の追加 • ベースラインセキュリティ対策の採用 • 自動化された安全なソフトウェアアップデート • 環境全体を通したエンドツーエンドのセキュリティ対策

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



セキュリティ対策指針 × 関連する脅威 × 既存のセキュリティ関連文書との対応関係

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（欧州電気通信標準化機構）を通じた国際基準の策定にも関与しつつ、一部の事項については規制に向けた検討も進めている。**

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

Cyber Security for Consumer Internet of Things (ETSI)

- 2019年2月に公表された、英国で策定された「消費者向けIoT製品のセキュリティに関する行動規範」に基づく欧州標準。**将来の欧州サイバーセキュリティ認証フレームワークの実装を助けるもの**であることが明示。
- **消費者向けIoT製品のセキュリティを確保するための開発・製造者向けガイダンス**であり、セキュリティ課題の網羅的な対策ではなく、重要なセキュリティ課題を解消する技術上の対策、組織上の対策に焦点。
- 規定の13項目は英国の行動規範と実質的に同じだが、それぞれ細分化がなされており、必須要件（M）と推奨要件（R）、条件付き必須要件(MC)、条件付き推奨要件(RC)に整理。

消費者IoTのためのサイバーセキュリティ規定（13項目）

1. 単一のデフォルトパスワードを使用しない
2. 脆弱性の報告管理手段を実装する
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調査する
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