経済産業省

IoT製品に対するセキュリティ適合性評価制度構築に向けた検討状況

2023年12月14日

商務情報政策局 サイバーセキュリティ課

課長補佐　木本 達也

1. IoTセキュリティの重要性

2. IoTセキュリティに関する各国動向と国内検討会立ち上げ

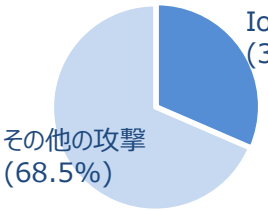
3. IoT製品に対するセキュリティ適合性評価制度の検討状況

IoT機器の利用拡大に伴い増加するリスク･経営への影響

ネットワークに接続される機器(IoT機器)は増加傾向、IoT機器を狙った攻撃は多い

IoT機器の
利用数は増加

世界のIoT機器数の推移及び予測(※1)



不審な通信のうち
約1/3はIoT機器を狙った攻撃

ダークネットにおける年間観測パケット数の割合(※2)

[※1] 出所:総務省「情報通信白書令和4年版 データ集」(3章関連データ)
[※2] 出所:NICT「NICTER観測レポート2022」調査を除く攻撃パケットのうち、23/TCP、22/TCP、5555/TCP、81/TCPへのパケットを集計。

IoTにおけるセキュリティインシデントが経営に大きな影響を及ぼす可能性が高まっている

操業停止や逸失利益の発生を含む事業への直接的な影響

半導体製造工場の制御装置に対する攻撃によって、**3日間の操業停止、営業機会損失が発生(売上高(四半期)の3%損失)**[台湾:2018]

石油化学工場の安全計装システムを対象とした攻撃による**操業停止。プラント爆発のおそれ**[サウジアラビア:2017]

脆弱性対応や損害賠償を含む追加費用の発生

脆弱性発見による自動車140万台のリコールの発生。脆弱性等の対応で、**2億9900万ユーロ(約394億円)の赤字を計上**(四半期の最終損益) [米国:2015]

評判の低下等より生じる競合優位性の低下

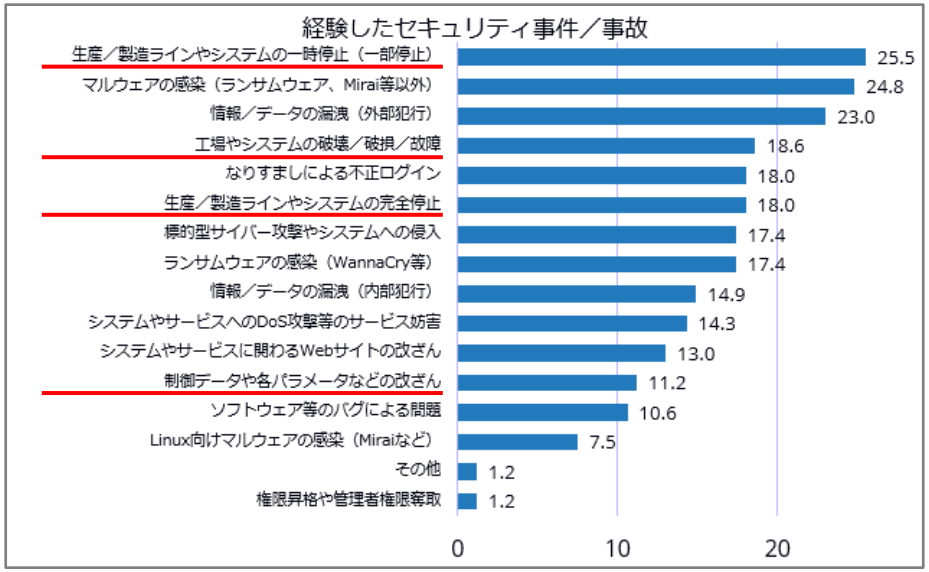
高級ホテルで客室のカードキー発行システムがランサムウェアに感染し、一切のシステム操作が不可能となった。客室扉の施錠、開錠が不可能となり、宿泊客が閉め出される事態が発生。**サービスの品質が著しく低下** [オーストリア: 2017]

[参考] 各公開情報を基に作成

IoT機器に対するセキュリティ対策の必要性

- DXの進展により、インターネットとIoT機器が繋がり始めたところであるものの、**セキュリティ事件/事故によるIoT機器やOTシステムの一時停止を約25%の企業が経験**。**こうした機器やシステムでセキュリティ対策を多くの者が導入しているとは言い難い**状況。
- 機器に対する十分なセキュリティ対策が実施されず、脆弱性が残存した場合、悪意ある攻撃者によって不正操作や誤作動が実行され、**機器の利用者へ影響を及ぼす恐れ**。
- また、**開発企業は脆弱性の対応に追われる**こととなる。過去には、**脆弱性によりリコールや利用者による訴訟に発展した事例**もあり、最悪の場合、**開発企業の経営に対して影響を与える可能性**もある。
- 今後さらなる脅威の増加・高度化が想定されるところ、**機器に対するセキュリティ対策の具備が不可欠**。

2021年 国内企業のIoT/OTセキュリティ対策実態調査結果



セキュリティ対策の不備により開発企業に影響を及ぼした事例

自動車における脆弱性の検出による140万台のリコール

販売中の自動車に対して外部から不正アクセス可能な脆弱性が公開。**顧客からの問い合わせが殺到し、開発企業は140万台のリコール**。**リコールの対応には1,000万ドル以上の費用**を要した。

心臓ペースメーカーにおける脆弱性の検出による46.5万台のリコール

販売中の心臓ペースメーカーに対して心拍リズムを外部から制御可能な脆弱性が公。**開発企業は市場に流通している46.5万台を対象にリコール**。

脆弱な家庭用ネットワークカメラのメーカに対する訴訟

家庭用ネットワークカメラにおいて、認証不備に関する脆弱性が内在し、脆弱性を悪用した不正アクセスが行われた。不正アクセスの被害を受けた複数の利用者により、**開発企業に対して500万ドルを求める集団訴訟**が提起。

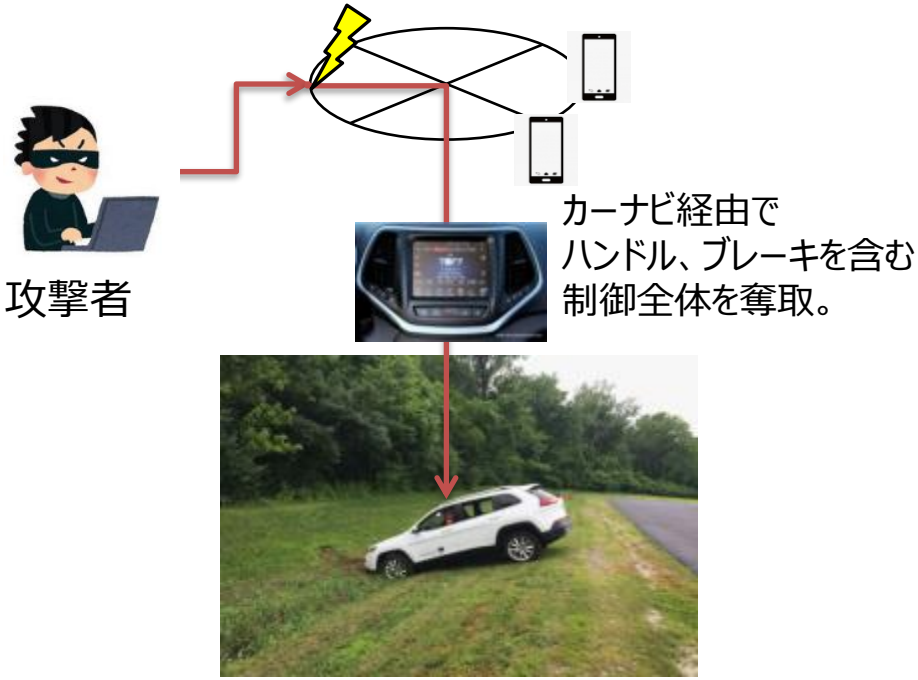
IDC「2021年 国内企業のIoT/OTセキュリティ対策実態調査」https://www.idc.com/getdoc.jsp?containerId=prJPJ47631521
※ 調査実施：2021年2月、調査対象：国内企業443社

＜事例＞ IoTの進展に伴う新たな脅威：新たにつながるデバイスの不正操作

- これまでネットワークに接続されていなかった自動車やカメラなどの機器が、Wi-Fiや携帯電話網などを介してインターネットに接続されることによってサイバー攻撃の新たな対象に。
- **不正操作による誤作動、不適正作動**などのリスクが顕在化。

自動車へのハッキングよる遠隔操作

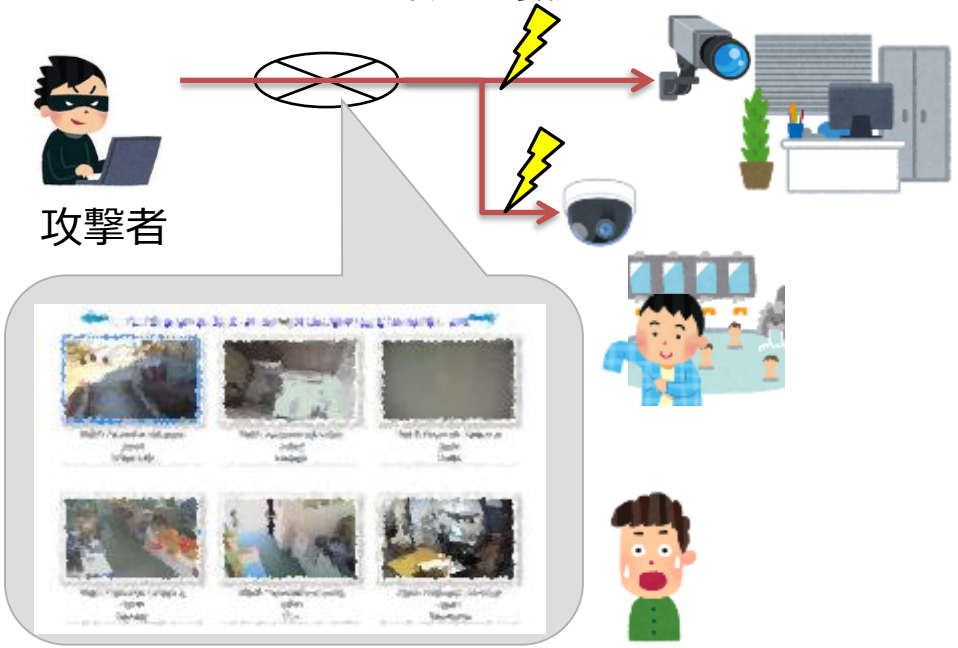
携帯電話網経由で遠隔地からハッキング



人命にも関わる事故が起こせることが証明され、
自動車会社は**140万台にも及ぶリコール**を実施。

監視カメラの映像がインターネット上に公開

利用者が気づかないまま、ID/パスワードを
デフォルトのままインターネットに接続

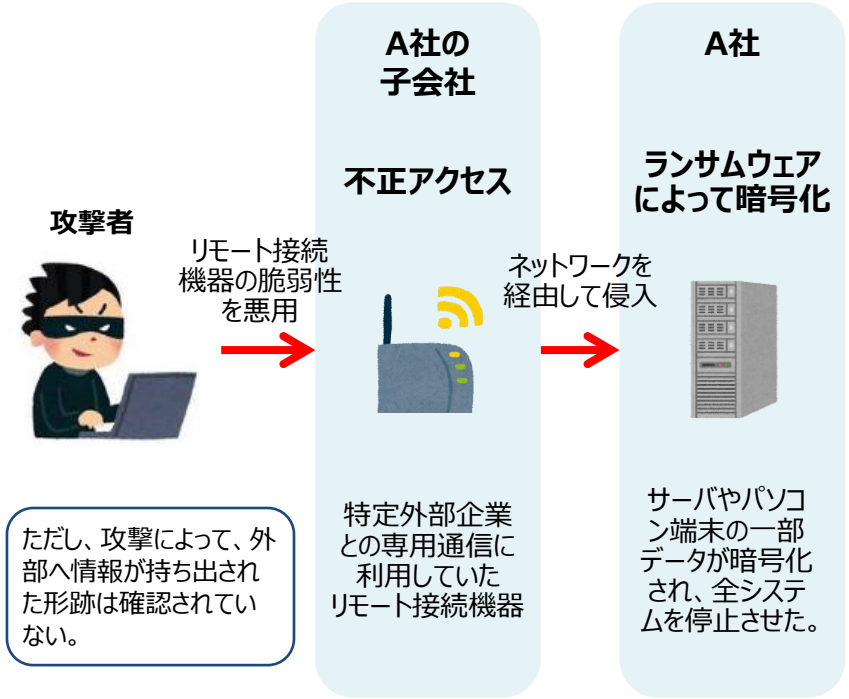


セキュリティ対策が不十分な**日本国内の多数の監視カメラの映像が海外のインターネット上に公開**。

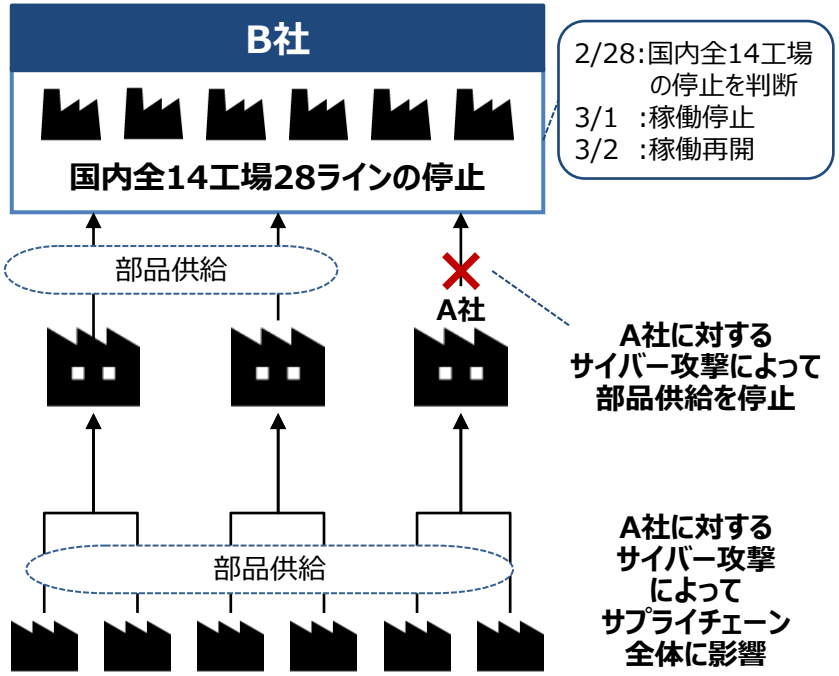
＜事例＞ 自動車部品メーカーに対するランサムウェア攻撃事案

- 2022年2月、B社に自動車部品を納入しているA社は、子会社のネットワークを経由して不正アクセスを受けたことで、サーバやパソコン端末の一部データがランサムウェアによって暗号化され、被害拡大防止のために全システムを停止させた。
- A社へのサイバー攻撃によって、 2022年3月にB社は国内全14工場28ラインの停止を判断。

子会社を通じた不正アクセスの概要



サプライチェーン全体への波及



[参考] 各公開情報を基に作成

1. IoTセキュリティの重要性

2. IoTセキュリティに関する各国動向と国内検討会立ち上げ

3. IoT製品に対するセキュリティ適合性評価制度の検討状況

IoT製品適合性評価に関する各国動向

法規制

米国

【カリフォルニア州】**SB-327 Information privacy: connected devices**
【オレゴン州】**HB-2395 (2019) Oregon Cybersecurity Bill**

- 他の法令やガイダンスに基づくセキュリティ要件の対象となっている製品を除く**インターネットに接続される機器**が対象
- **IoT機器を販売するメーカーに対し**、パスワードの管理等を含む**合理的なセキュリティ機能を具備することを要求**
- 【オレゴン州のみ】セキュリティ対策違反を起こした場合、調査措置や差止命令が行われる可能性があるほか、故意に違反していると判断された場合には、最高25,000ドルの罰金の支払いが命じられる可能性がある

日本

端末設備等規則（総務省令）

- **電気通信事業者のネットワーク（インターネット等）に直接接続するIoT製品**。
- **間接的にネットワークに接続するIoT機器**（ホームネットワークのみに繋がるスマートホーム機器、等）**は対象外。**

EU

Cyber Resilience Act（CRA）（草案提出中）

- 一部例外を除き**デジタル要素を備えた全ての製品に対して、EU全域に水平的なサイバーセキュリティ要件**を課す内容（罰則あり）
- **製造業者への①上市前の設計製造に関する義務、②上市後の報告等義務**等。

Radio Equipment Directive（RED）（2025年8月1日から）

- **直接又は間接にインターネットに接続する無線製品**が対象
- ①ネットワーク・機能の損害/ネットワーク・リソース悪用/許容できないサービス低下の防止、②個人データ・プライバシー保護、③不正行為からの保護サポートを要求予定

英国

Product Security and Telecommunications Infrastructure (PSTI) Act 2022（2024年4月開始予定）

- **インターネットもしくはネットワークにつながる製品**に対して、セキュリティ対策を義務化する内容（罰則あり）
- 今後、下位法令にて具体的な内容が規定される。

任意制度（認証、ラベリング）

米国

U.S. Cyber Trust Mark Program（検討中）

- **消費者向けIoT機器**に対する任意の認証制度を2024年内に開始予定。
- 中でも消費者向けルーターは個別に要件策定がなされている。

EU

EU Cybersecurity Certification (EUCC)（検討中）

- ICT製品を対象とするCommon Criteria（ISO/IEC 15408）及び関連する共通評価方法（ISO/IEC 18045）に基づく認証スキーム

ドイツ

IT-Sicherheitskennzeichen (IT Security Label)（導入済）

- **ブロードバンドルーター、電子メールサービス、スマートテレビ、スマートスピーカー等の消費者向けIoT製品**を対象
- 2022年8月22日時点（制度開始後8ヶ月）で34製品・サービスがラベルを取得

相互運用を実施

シンガポール

Cybersecurity Labelling Scheme (CLS)（導入済）

- **すべての消費者向けIoT製品を対象とする任意の認証制度。**4段階の認証。
- 2022年8月22日時点（制度開始後22ヶ月）で206製品がラベルを取得

オーストラリア

Labelling for Smart Devices（検討中）

- インターネットやホームネットワークに接続される前提で開発された**すべての消費者向けのスマートデバイスを対象**として検討中

フィンランド

Finnish Cybersecurity Label（導入済）

- **インターネットに接続され、デジタル形式でデータを処理・伝送する製品・サービスを対象**
- 2022年8月22日時点（制度開始後33ヶ月）で14製品がラベルを取得

相互運用を実施

【欧州】サイバーレジリエンス法案　（審議中）

- **2022年9月**に欧州委員会が欧州議会・理事会に**草案提出**。**EU全域に水平的なサイバーセキュリティ要件**を課し、製品ライフサイクル全体を通じたセキュリティ向上を目指すもの。
- 一部例外を除き、**デジタル要素を備えた全ての製品**が対象。高リスクの「重要なデジタル製品」、低リスクの「重要なデジタル製品」、「その他」に**製品を３分類し、それぞれの分類に応じた適合性評価**を求める。
- 草案は**主として、製造業者への①上市前の設計製造等に関する義務、②上市後の報告等義務**に代別される。
- **罰則あり**。（最高1,500万ユーロ又は当該企業の全世界売上高の2.5%以内）
- **現在委員会・議会・理事会間で最終調整中**。

欧州委員会草案の主な義務

- **製造業者**

上市前の設計製造等に関する義務

- 付属書Iの1に記載の「セキュリティ特性要件」に従って、製品を設計/開発/製造する。
- 技術文書を作成する。
- 適合性評価手続きを行い、付属書Iとの適合性が実証された場合はCEマーキングを貼付する。

上市後の報告等に関する義務

- 積極的に悪用された脆弱性を発見した場合やインシデントを認識した場合、24時間以内にENISAに報告する。また、インシデントについては直ちにユーザーに報告し、必要に応じてその影響を緩和するための是正措置に関する情報を提供する。
- 上市後5年間または製品寿命のうち短い期間の間、付属書Iに記載の「セキュリティ特性要件」が満たされない場合は必要な是正措置を講じる、または製品の撤回・リコールを行う等適切に対処する。
- 上市後10年間、技術文書と（該当する場合）EU適合性証明書を保管する。

- **輸入者**

- 製造業者が、CE マーキング添付を含めた技術要求を満たしていることを確認する。

- **流通業者**

- 製造業者及び輸入者が、CE マーキング添付を含めた適切な手段を講じているかを確認する。

（参考）「重要なデジタル製品」

以下の各クラスに規定された要素を主に有するデジタル製品

クラスI(低リスク)第三者認証(EUCC,EN規格以外)

1. ID管理システム、アクセス管理ソフト
2. スタンドアロン型/組込み型ブラウザ
3. パスワードマネジャー
4. マルウェア検知・削除・隔離ソフトウエア
5. VPN機能を持つ製品
6. ネットワーク管理システム
7. ネットワーク・コンフィグレーション管理ツール
8. ネットワーク・モニタリングシステム
9. ネットワーク・リソース管理
10. SEIM（セキュリティ情報イベント管理）
11. ブートマネジャーを含む更新・パッチ管理
12. アプリケーション構成管理システム
13. リモートアクセス/共有ソフトウェア
14. モバイル機器管理ソフトウェア
15. 物理ネットワークインターフェイス
16. OS（クラスII製品以外）
17. ファイアウォール、侵入検知・防止システム（産業用以外）
18. ルータ、モデム、スイッチ（産業用以外）
19. マイクロプロセッサ（クラスII製品以外）
20. マイクロコントローラ
21. NIS 2 指令の別添Iに示される目的でのASIC、FPGA
22. PLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）（クラスII製品以外）
23. 産業用IoT（クラスII製品以外）

クラスII(高リスク) 第三者認証

1. OSであってサーバ、デスクトップ、モバイル機器用のもの
2. OSや同様の環境の仮想化を実施するためのハイパバイザー及びコンテナー・ランタイム・システム
3. 公開鍵インフラ及びデジタル証明書発行
4. 産業用のファイアウォール、侵入検知・防止システム
5. 汎用マイクロプロセッサ
6. PLCやセキュアエレメントへの統合を目的としたマイクロプロセッサ
7. 産業用のルータ、モデム、スイッチ
8. セキュアエレメント
9. ハードウェア・セキュリティ・モジュール（HSMs）
10. セキュア暗号プロセッサ
11. スマートカード、スマートカードリーダー、トークン
12. 産業用のPLC、DCS、CNC、SCADAなどの産業用自動化制御システム（IACS）
13. NIS 2 指令の別添Iに記載された重要エンティティが使用する産業用IoT機器
14. ロボットセンシング/アクチュエーターコンポーネント及びロボットコントローラー
15. スマートメーター

【米国】U.S. Cyber Trust Mark（検討中）

- **FCC（米連邦通信委員会）**が2023年8月にNPRM（立法案公告）を公表した、**任意のラベリング制度**。米時間10月6日までパブコメを実施。
- **想定対象は「消費者用IoT機器」**（詳細は下記）。ラベリングを得た機器とその機器に関する情報を全国登録簿に掲載し、ラベルに付随するQRコードを通じて全国登録簿が参照できるような仕組みを想定。
- 今まで**NIST(米国立標準技術研究所）が公表してきた基準に基づく見込み**。なお、**消費者向けルーター、スマートメーターについては、別途セキュリティ要件を定義する**予定。
- **2024後半の運用開始を目指す。**

米FCC　NPRM（立法案公告）の主な内容

● **対象について**

以下２つを満たすものを提案。

(1) 物理的世界と直接相互作用するための、1つ以上のトランスデューサー（センサーまたはアクチュエーター）を備え、意図的にラジオ周波数を放出することができる（※intentional radiatorに限定）インターネット接続デバイス

(2) デジタル世界と相互作用するための、1つ以上のネットワークインターフェース（Wi-Fi、Bluetoothなど）

※ただし、FCCのCovered listや、米商務省のEntity List、米国防総省のList of Chinese Military Companiesの機器、またはその企業が生産する機器は対象外とする。

➢ 対象をIoT「機器」とするべきか、NIST定義に基づくIoT「製品」とするべきか（IoT機器＋バックエンド、ゲートウエイ等必要な追加部品）

➢ 「消費者」IoTに限定するべきか、「商業用」目的のものも含むべきか、対象は「使用方法」で判断するべきか。

● **スキーム・体制について**

第三者機関としてCyber LABs（Cybersecurity Labeling Authorization Bodies）を設置することを提案。

● **基準策定について**

➢ NIST基準をどのように活用できるか。その他考慮するべき基準はあるか。

➢ よりリスクが高いIoT機器・機器の分類には、別途基準を策定するべきか。

経済産業省においてIoTセキュリティ適合性評価制度の検討会を立ち上げ

- **IoT機器の急増に伴い、IoT機器の脆弱性を狙ったサイバー脅威が高まってきた**ことから、**IoT製品のセキュリティ対策を適切に評価し、適切な対策が講じられているIoT製品が広まる仕組みの構築が必要**。また、我が国のIoT製品がグローバルマーケットから弾き出されないよう、諸外国の取組を考慮することが必要。
- こうした観点で制度の検討を行うため、2022年11月より「**IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会**」を３回開催し、2023年5月に**中間報告をとりまとめた**。委員は、学術界、法曹界、業界団体、企業、消費者団体から構成。オブザーバとして、関係省庁、研究機関、認証機関が参画。 2023年度中の最終報告に向け議論を継続中。
- 国内での議論と並行して、米EU等の諸外国との制度調和を図るための国際的な対話も実施中。

中間報告（概要）

検討会において議論した事項

● **課題**

ベンダ、利用者、国民の三者において、以下の課題が存在。

✓ **ベンダ**： **対策が評価されず製品価値に繋がらない**。諸外国の制度対応負担が増加。
✓ **利用者**： **適切な対策の製品が可視化されていないため、適切な製品を選べない**。
✓ **国民**： 適切でない製品が多く流通した場合、IoTがボット化するなどして、**国内のシステムや国民生活に悪影響を及ぼす**。

● **構築すべき適合性評価制度**

✓ ベンダによる能動的なセキュリティ向上を促す観点や、特に中小企業の負担の観点から、**まずは任意制度として制度を運用することが適当**。**ただし、制度の浸透具合や、諸外国の動向によっては、法令に基づく義務化の検討も必要になり得る**。

✓ 対象製品範囲については、「**間接的又は直接的にインターネットに接続する製品**」とすることが適当。その上で、具体的な対象製品については今後要検討。

✓ 適合性評価基準については、国際的な標準を参照の上、**国際的な標準と整合的な形で構築していくことが適当**。その上で、具体的にいかなる製品にどのような基準を適用するかは今後要検討。

✓ 運用については、**既存の評価スキームを活用**した制度とすることが適当。その上で、具体的にどのようなスキームを活用すべきかは今後要検討。

今後議論が必要な事項

上記に加え、政府の関与や検討体制のあり方、IoT製品ベンダーの能動的な制度活用を促す仕掛け、適合性評価済製品におけるセキュリティ事案への対応。

【IoT機器に対するセキュリティ適合性評価制度構築に向けた検討会】会議資料
ワーキンググループ3（IoT製品に対するセキュリティ適合性評価制度構築に向けた検討会） （METI/経済産業省）
https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html

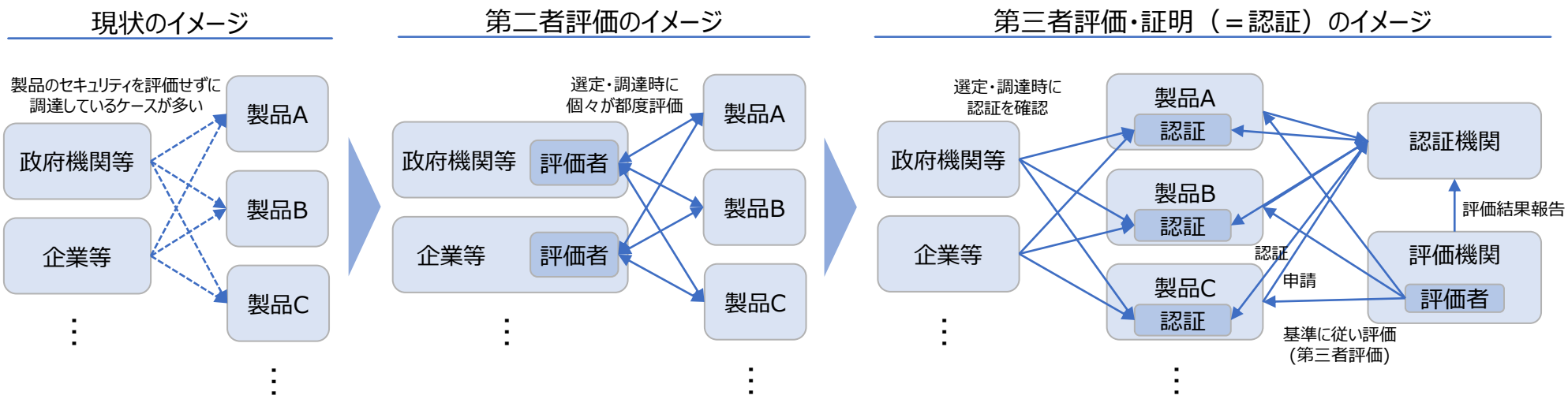
1. IoTセキュリティの重要性

2. IoTセキュリティに関する各国動向と国内検討会立ち上げ

3. IoT製品に対するセキュリティ適合性評価制度の検討状況

【目的①】政府機関等・企業等のIoT製品調達ニーズへの対応

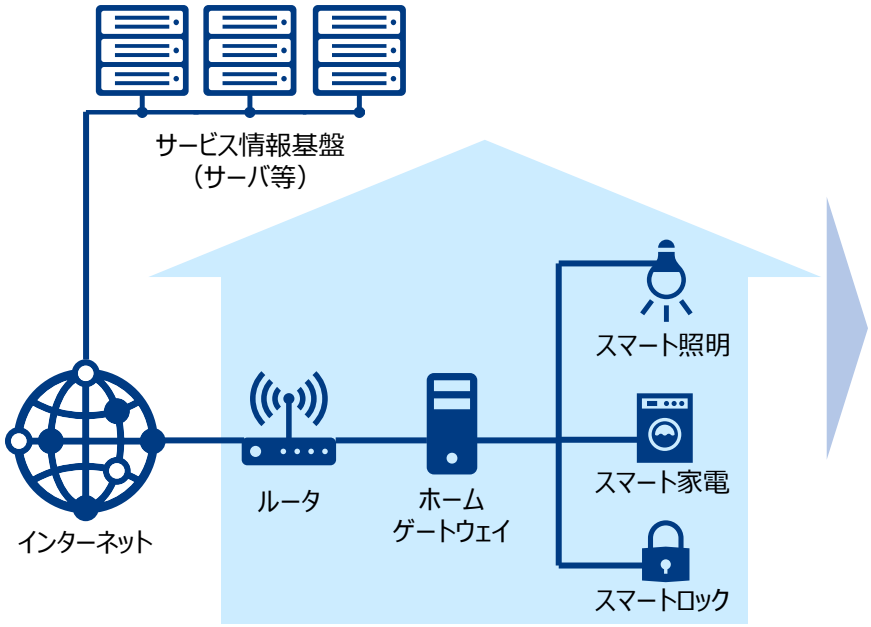
- 政府機関等・企業等のセキュリティ対策において、**調達する製品や製品ベンダーのセキュリティも含めた広義なサプライチェーンリスク管理の取り組みが広がっている**。
- その際、IoT製品のセキュリティに関して、選定時や調達時に、その**セキュリティ機能や対策状況を自組織で確認すること（第二者評価）が本来必要であるが、そのための確認プロセスを整備できている政府機関等・企業等は少ないのが現状**である。一方、仮に政府機関等・企業等がそのプロセスを整備する場合、調達を行う各組織においてその**確認のための知識と工数が必要**となり、またIoT製品ベンダーは各者から**異なる要件に対して繰り返し回答・対応が求められ**、双方対応しきれなくなる。
- そこで、第二者評価を代替する仕組みとして、**共通的な物差しでIoT製品のセキュリティを第三者が評価し、その結果に対して認証を付与する制度**を整備する。政府機関等・企業等は**認証取得の確認をベースとして活用**しながら、必要な場合に追加的な確認を実施することで、各組織の求めるセキュリティ水準のIoT製品を選定・調達することが可能となる。
- **政府機関等の第二者評価の代替として公平・中立な認証を行うためには公的機関（IPA）が認証機関**となり、制度を維持・運営していくことが望ましい。



【目的②】特定分野で使用されるIoT機器の最低限のセキュリティ確保

- IoT製品は、単体で比較・検討されて調達されるだけではなく、**特定分野のシステムに組み込まれて調達され、利用される**ケースもある。そのようなケースでは、最終調達者（ユーザー）がセキュリティを考慮したIoT製品を直接選定するのではなく、システムに組み込まれる段階で選定・調達される。（例）**スマートホーム、工場システム、ビルシステム**など
- **特定分野のシステムそれぞれの想定するユースケース、守るべき資産、脅威、リスクを定義**し、実施すべき対策のひとつとして、**組み込まれるIoT製品に求めるセキュリティ要件を定める**必要がある。当該要件で、IoT製品類型共通の☆1以上が必要となる場合に、**☆2以上の整備を本制度で検討**する。
- 各業界団体等では、特定分野のシステムのセキュリティに対して、**それぞれの用途や機能を考慮し、組み込むIoT製品のセキュリティ要件として必要な認証・ラベルを指定**する。その他のセキュリティ要件も含めたセキュリティガイドラインの作成や、システム全体としての認証制度等の整備を行い、**その準拠を業界標準とする**ことで、**当該特定分野のシステムにおいて、最低限のセキュリティが確保されたIoT機器のみが採用される**ことを目指す。

【特定分野のシステムのイメージ（スマートホームの例）】



【各IoT製品に求める認証・ラベル指定のイメージ】

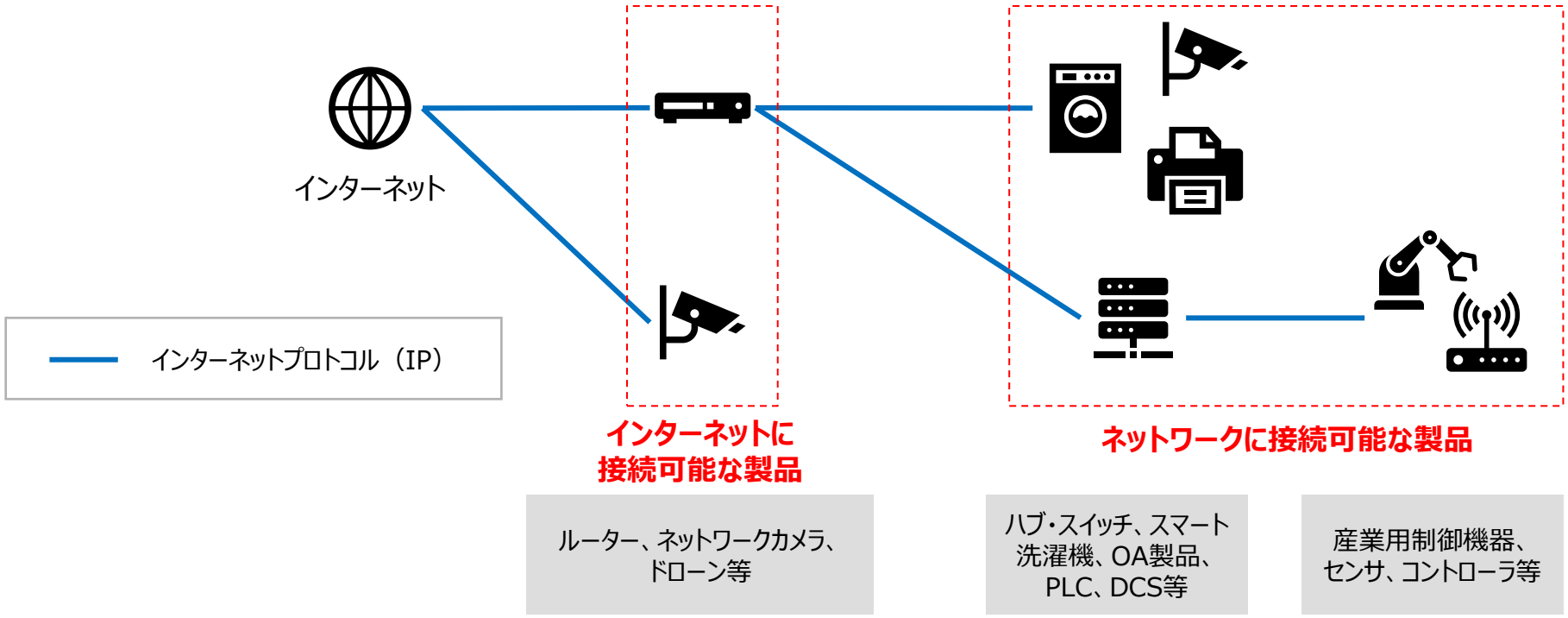
IoT製品	認証・ラベル	指定理由（例）
ルータ	☆2以上	• 外部からの侵入ルートになる可能性があるため
ホームゲートウェイ	☆2以上	• 外部からの侵入ルートになる可能性があるため
スマート照明	☆1以上	• 機器単体が侵害を受けても被害は限定的であるため
スマート家電	☆1以上	• 機器単体が侵害を受けても被害は限定的であるため
スマートロック	☆2以上	• 侵害が受けた場合、人的資産や物理的資産の損害に繋がる恐れがあるため

※ システムの重要度・規模やIoT製品の用途で指定する認証・ラベルを分けることもある。

本制度における対象製品の定義

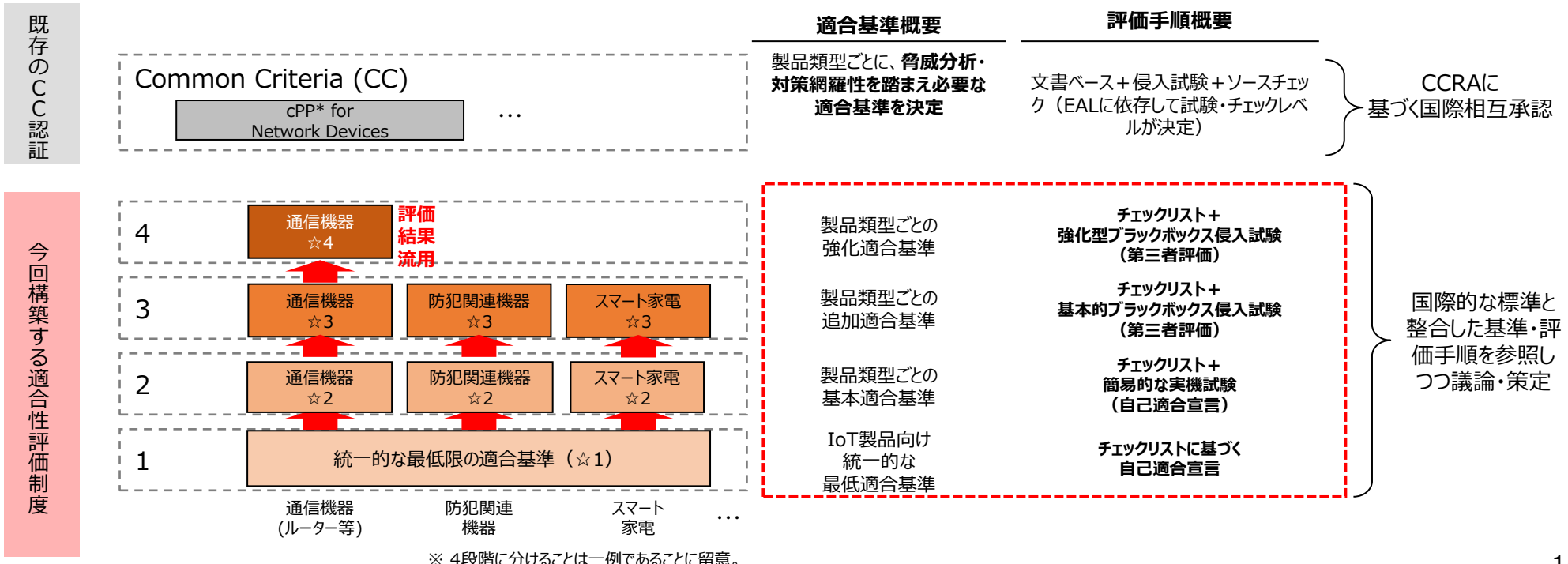
- 本制度では、**インターネットプロトコル（IP）を使用してデータを送受信する機能を持つ以下のIoT製品**(※1)を対象とする。
  - **インターネットに接続可能な製品**：IPを使用してインターネット上でデータを送受信する機能を持つ製品
  - **ネットワークに接続可能な製品**：IPを使用して、他の「インターネットに接続可能な製品」又は「ネットワークに接続可能な製品」に接続し、データを送受信する機能を持つ製品
- ただし、広くITシステムで利用されており、利用者が任意のソフトウェアにより随時かつ容易にセキュリティ機能を変更することができる汎用的なIT製品（PC、タブレット端末等）は対象外(※2)とする。

※1：ETSI EN 303 645の定義を参照し、「IoT製品（IoT product）」には、IoT機器（IoT device）とその関連サービスを含む。
※2：英国PSTI法、総務省端末設備等規則等の国内外制度も同様の理由で対象外としている。



制度概要

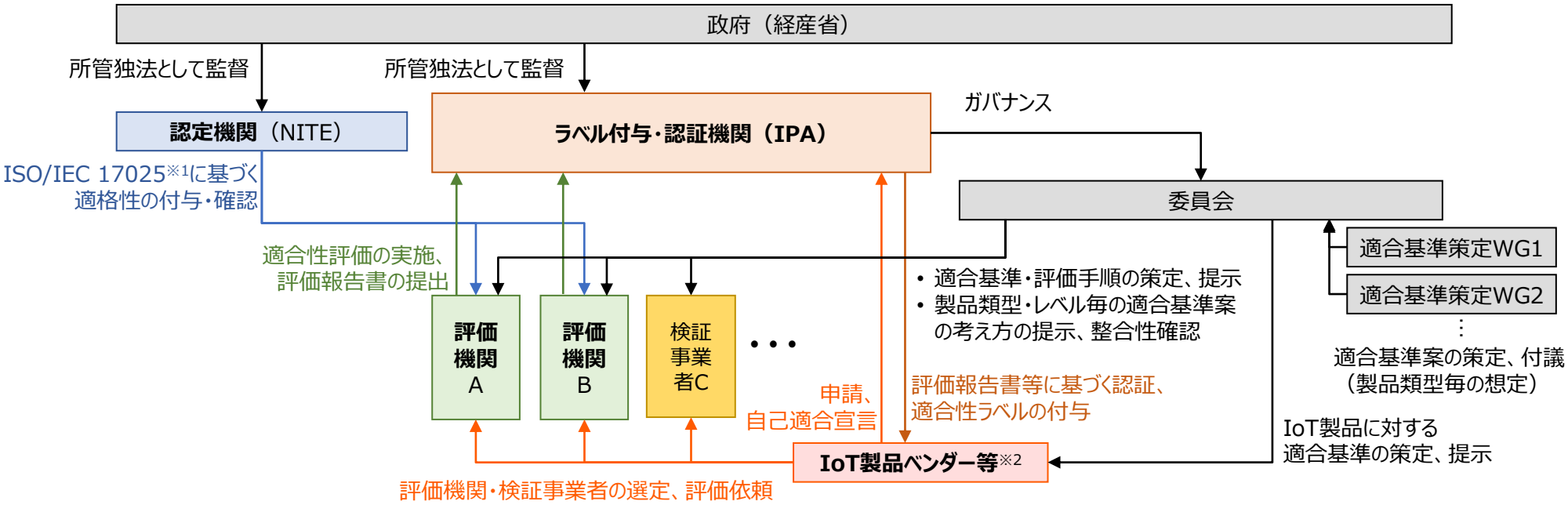
- 幅広いIoT製品を対象としつつ、製品ごとの特性に応じた基準を既存の制度を活かしながら設けられるよう、**複数のレベル（☆）を用いた制度を想定。**
- **☆1は、幅広いIoT製品を対象に、統一的な最低限の適合基準**を想定。**評価方法は**、チェックリストに基づく**自己適合宣言**を想定。
- **☆2以上は、製品類型ごとに適合基準を策定**することを想定。評価方法は、チェックリストに基づく**自己適合宣言及び実機試験・侵入試験等の第三者評価**を想定。なお、どの程度の第三者評価をどのレベルで求めるかは今後製品類型ごとに要検討。



※ 4段階に分けることは一例であることに留意。

適合性評価制度の想定スキーム

- これまでの議論を踏まえ、本制度の各主体の適格性について、政府のガバナンスが効く構造が重要。係る観点から**CC認証の知見があるIPAのJISEC認証制度**（ITセキュリティ評価及び認証制度）**を拡張する形の制度**を構築予定。
- プレ委員会を設置し、**2023年度末までに製品類型共通で最低限必要となる☆1の要求基準・適合基準の検討**および**ルーター、スマート家電等を対象とした評価検証**を実施中。

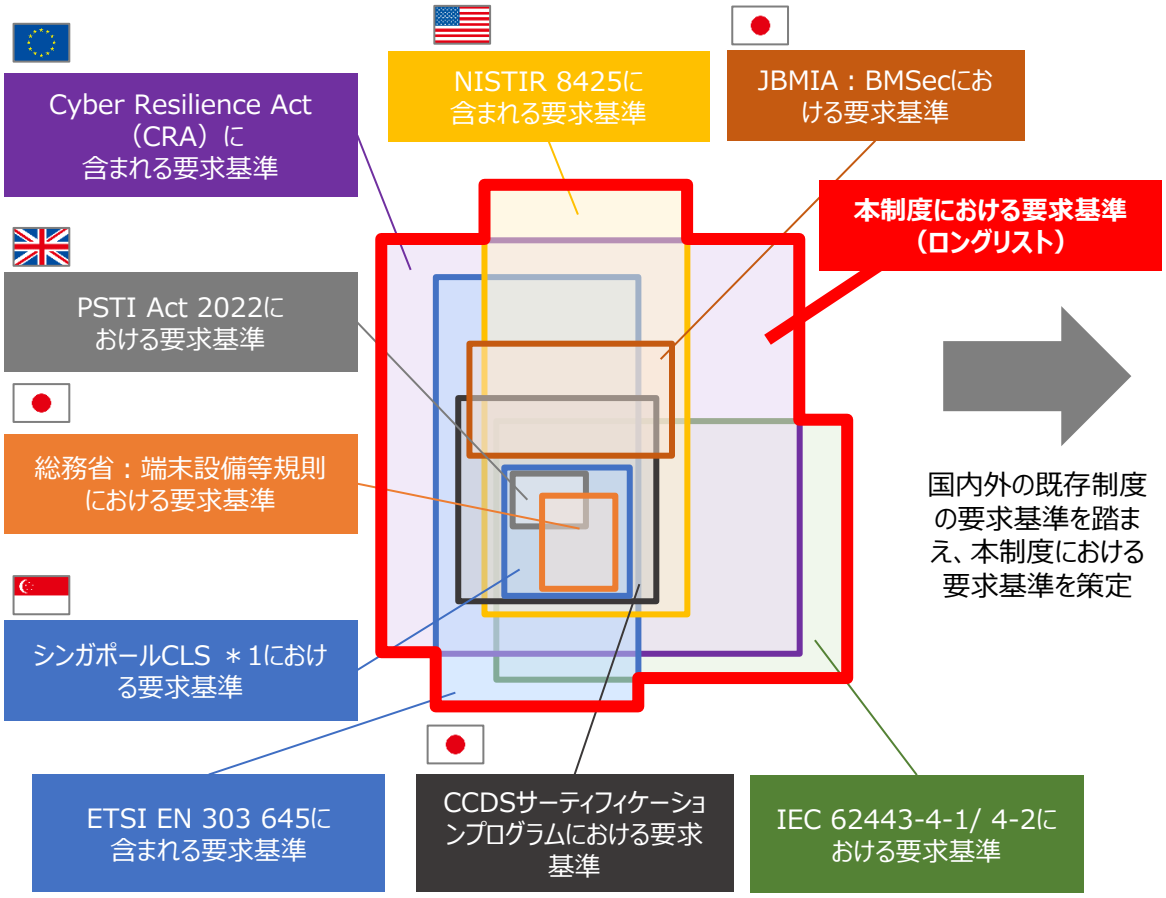


※1：ISO/IEC 17025（JIS Q 17025）は、試験所及び校正機関の試験・校正能力に関する一般要求事項を規定した国際標準であり、JISEC認証制度に基づくIT製品及びシステムのセキュリティ評価を行う試験事業者に求められる。なお、ISO/IEC 17065（JIS Q 17065）は、製品認証機関の認証能力に関する一般要求事項を規定した国際標準である。
※2：IoT製品を製造するベンダーだけでなく、海外からIoT製品を輸入・販売する輸入業者も含まれる。

国際基準を踏まえた要求基準案

- 要求基準は、本制度で対象となるIoT製品において求められうるセキュリティの要求の全体（ロングリスト）であるため、ETSI EN 303 645、NISTIR 8425、EU-CRA等の国内外の要求基準の集合関係を踏まえ、**重ね合わせの関係（∪（カップ））にある要求事項のロングリストを整理**。

諸外国制度において求められる要求基準の関係性イメージ

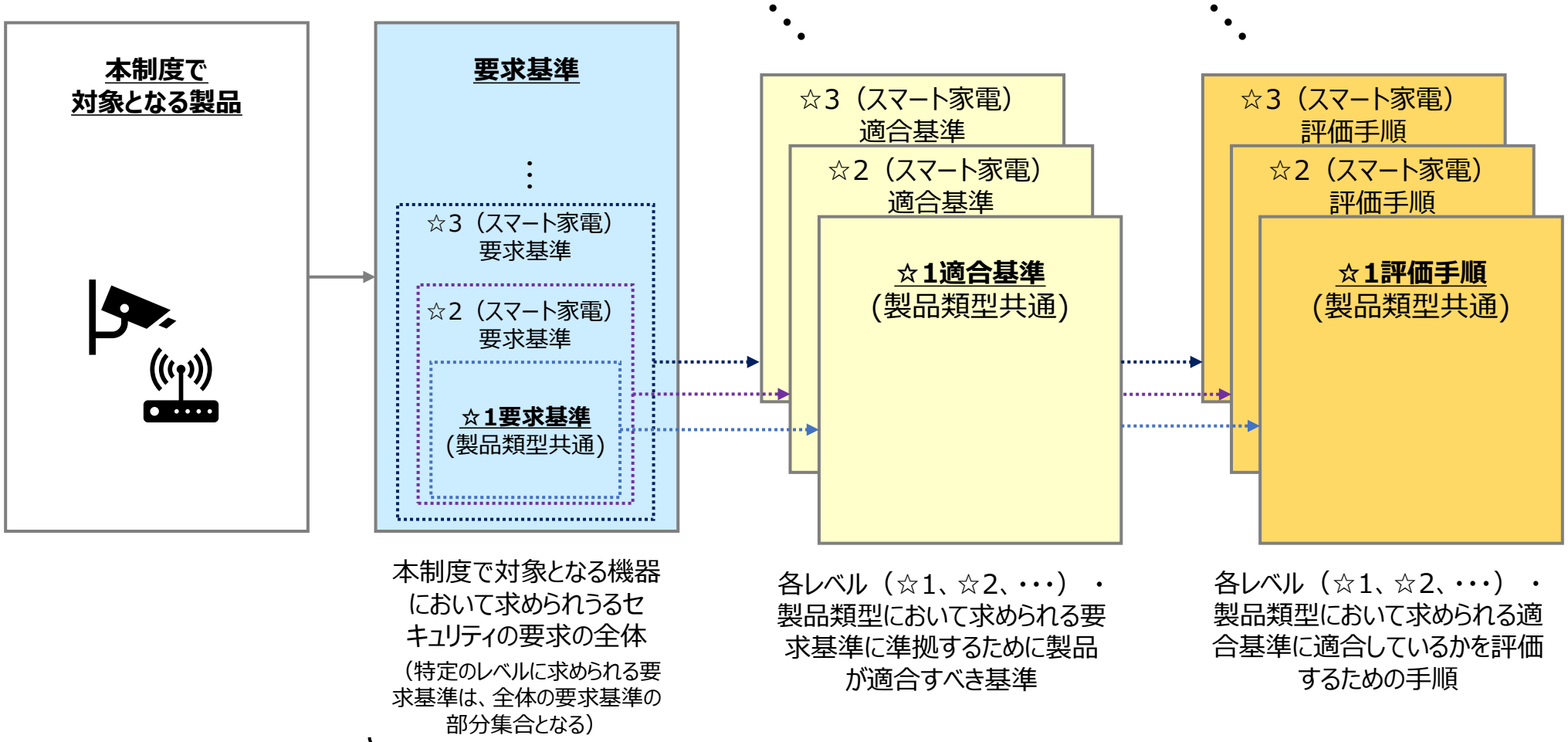


本制度における要求基準（ロングリスト）のイメージ

要求基準案	
1. 汎用のデフォルトパスワードを使用しない	1-1. パスワードが使用され、工場出荷時のデフォルト以外の状態にある製品において、すべてのパスワードは、製品ごとに固有であるか、又は利用者によって定義されるものでなければならない。
	1-2. プリインストールされた固有のパスワードを使用する場合、自動化された攻撃への耐性をもつために、パスワードは十分なランダム性を保有しなければならない。
	1-3. 製品に対して利用者を認証するために使用される認証メカニズムは、製品用途の特性等に適した想定するリスクを低減できる暗号技術を使用していなければならない。
	…
2. 脆弱性の報告を管理するための手段を導入する	2-1. 製造業者は、脆弱性開示ポリシーを公開しなければならない。このポリシーには、少なくとも以下が含まれていなければならない： • 問題を報告するための連絡先情報； • 以下のタイムラインに関する情報： 1) 最初の受領確認； 2) 報告された問題が解決されるまでの状況の更新。
	…
…	…

適合基準案・評価手順の策定と評価検証

- 今年度、実際の製品に対する適合性評価の評価検証を行い、関係者にどの程度のコストが発生しうるかを検証する。
- プレ委員会を設置し、☆１（最も低レベルの評価基準）の要求基準案・適合基準案・評価手順案を議論・策定し、これらに基づき、実際のIoT製品に対する適合性評価の評価検証を行う。



プレ委員会を通じて、☆1の要求基準案・適合基準案・評価手順案を作成、実際の製品に対する評価検証を実施

諸外国の適合性評価制度との国際連携に向けて

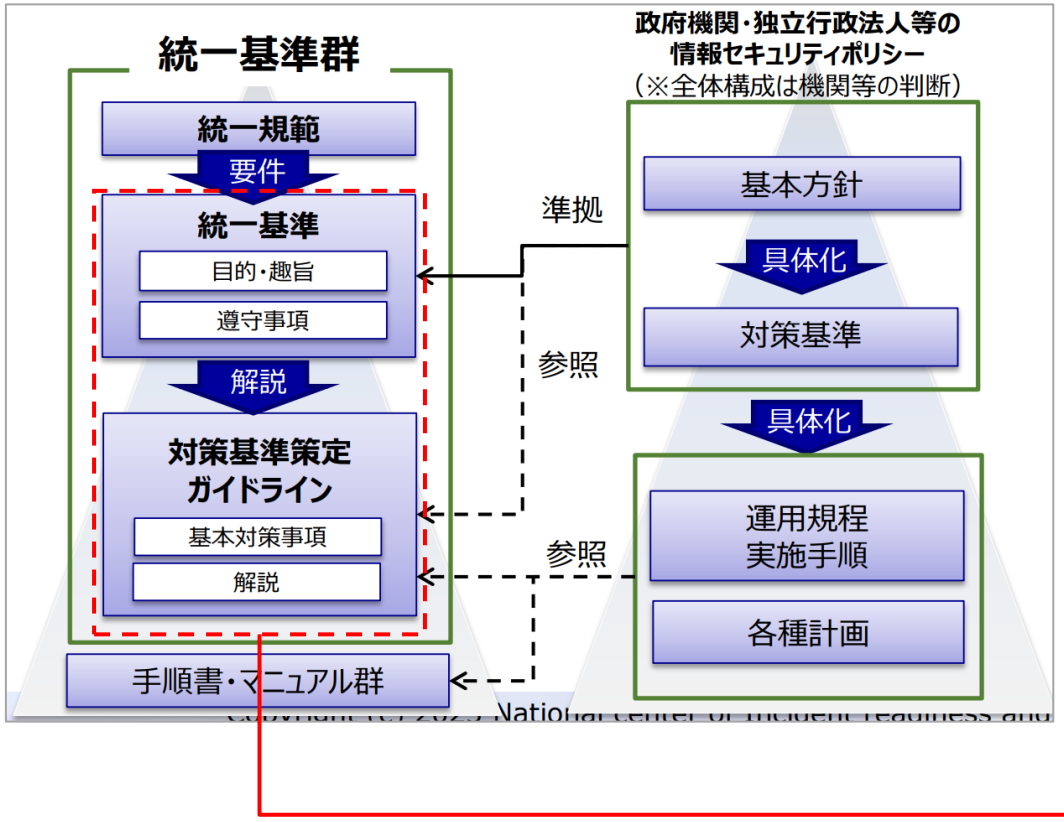
- **☆１開始時に導入されている、シンガポールCLS（の＊１）と英PSTI法を内包**するべく基準を設計する。
- ☆１開始時に制度設計途中の見込みである**欧CRA及び米Cyber Trust Markについては、差分を確認し、国内基準（☆１更新時又は来年度以降に検討をする☆２以上）で包含又は追加対応を要する差分の公表等で対応**する。
- 国内制度設計と並行して、☆１相互承認に向けて諸外国と調整を行う。
- 同時に、国際標準化に向けてISO/IEC 27404等の動きと連携をする。

国・地域					
制度名	発展JISEC制度	Cybersecurity Labelling Scheme（CLS）	Product Security and Telecommunication Infrastructure Act（PSTI法）	U.S. Cyber Trust Mark（仮）	Cyber Resilience Act（CRA）
開始時期	☆1：2024年度下期開始予定 ☆2以上：2025年度以降開始予定	2020年10月制度開始	2024年4月施行	2024年中に開始予定	未定（2027年開始想定）
任意/義務	任意	任意	義務	任意	義務
対象	IoT製品	消費者向けIoT機器	消費者向けIoT製品	消費者向けIoT機器（想定）	デジタル製品
適合基準	☆1：ETSI EN 303 645及びCLSの記載内容を中心に検討中（ただし、一部の記載については、総務省技適の要件、CCDSの要件の参照のほか、事務局にて記載内容を検討）	• ＊：ETSI EN 303 645の基準の一部※1 • ＊＊：＊の基準に加え、ETSI EN 303 645の基準の一部※2 • ＊＊＊及び＊＊＊＊：＊＊の基準に加え、IMDA「IoT Cyber Security Guide」の9つのライフサイクル基準	ETSI EN 303 645の基準の一部（5.1-1、5.1-2、5.2-1、5.3-13）	NISTIR 8425をベースとした基準となる見込み	• 基本的な対策基準のほか、SBOM等に基づく脆弱性管理、脆弱性報告等、広範な基準が求められる予定 • 法案の内容について（欧州委員会・議会・理事会間で）政治合意がなされた後、法案に伴う基準がETSI EN 303 645等を参照して設定される予定
評価方法	☆1：自己適合宣言 ☆2：自己適合宣言（ただし、一定のスキル要件を満たした評価者による評価を求める） ☆3以上：第三者認証を求める方針	• ＊及び＊＊：自己適合宣言 • ＊＊＊及び＊＊＊＊：自己適合宣言及び評価機関による試験	自己適合宣言	検討中	• 「重要なデジタル製品」以外の製品：自己適合宣言 • 「重要なデジタル製品」のクラスⅠ（リスクが低い製品）でEUCCやEN規格の対象外の製品及びクラスⅡ（リスクが高い製品）の製品：第三者認証

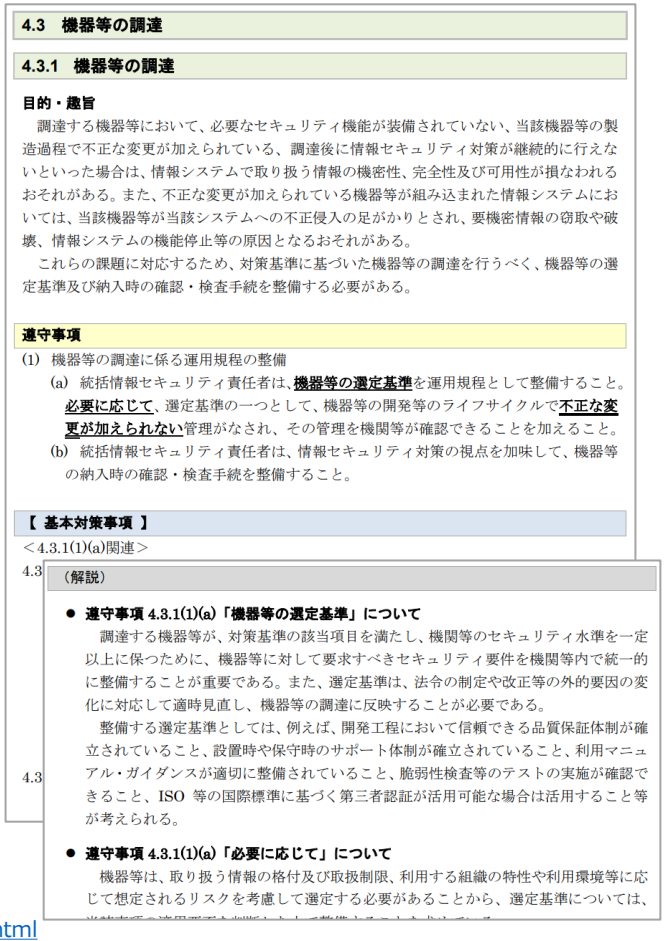
政府機関等の調達における本制度活用の検討

- 政府機関等が遵守すべき事項を定めた「政府機関等のサイバーセキュリティ対策のための統一基準」およびそのガイドラインに、情報システムの重要度に応じ、**「重要度：低」は☆1以上**、**「重要度：高～中」は少なくとも☆3以上のIoT製品を各機関等の選定基準に含める**ことの追加をNISCと検討している。
- ラベル取得済み製品が普及する時期をめどに、政府機関等では**ラベル取得済みIoT製品の調達を必須化する方針**。

統一基準群（令和５年度版）文書体系



対策基準策定ガイドラインの「4.3.1 機器等の調達」の記載



4.3 機器等の調達

4.3.1 機器等の調達

目的・趣旨

調達する機器等において、必要なセキュリティ機能が装備されていない、当該機器等の製造過程で不正な変更が加えられている、調達後に情報セキュリティ対策が継続的に行えないといった場合は、情報システムで取り扱う情報の機密性、完全性及び可用性が損なわれるおそれがある。また、不正な変更が加えられている機器等が組み込まれた情報システムにおいては、当該機器等が当該システムへの不正侵入の足がかりとされ、要機密情報の窃取や破壊、情報システムの機能停止等の原因となるおそれがある。

これらの課題に対応するため、対策基準に基づいた機器等の調達を行うべく、機器等の選定基準及び納入時の確認・検査手続を整備する必要がある。

遵守事項

(1) 機器等の調達に係る運用規程の整備

(a) 統括情報セキュリティ責任者は、**機器等の選定基準**を運用規程として整備すること。**必要に応じて**、選定基準の一つとして、機器等の開発等のライフサイクルで**不正な変更が加えられない**管理がなされ、その管理を機関等が確認できることを加えること。

(b) 統括情報セキュリティ責任者は、情報セキュリティ対策の視点を加味して、機器等の納入時の確認・検査手続を整備すること。

【 基本対策事項 】

＜4.3.1(1)(a)関連＞

4.3

（解説）

- **遵守事項 4.3.1(1)(a)「機器等の選定基準」について**

  調達する機器等が、対策基準の該当項目を満たし、機関等のセキュリティ水準を一定以上に保つために、機器等に対して要求すべきセキュリティ要件を機関等内で統一的に整備することが重要である。また、選定基準は、法令の制定や改正等の外的要因の変化に対応して適時見直し、機器等の調達に反映することが必要である。

  整備する選定基準としては、例えば、開発工程において信頼できる品質保証体制が確立されていること、設置時や保守時のサポート体制が確立されていること、利用マニュアル・ガイダンスが適切に整備されていること、脆弱性検査等のテストの実施が確認できること、ISO 等の国際標準に基づく第三者認証が活用可能な場合は活用すること等が考えられる。

- **遵守事項 4.3.1(1)(a)「必要に応じて」について**

  機器等は、取り扱う情報の格付及び取扱制限、利用する組織の特性や利用環境等に応じて想定されるリスクを考慮して選定する必要があることから、選定基準については、

統一基準の記載内容

上記遵守事項に対する基本対策事項と解説をガイドラインに記載

出所）NISC「統一基準群改定のポイント（令和５年度版）」https://www.nisc.go.jp/policy/group/general/kijun.html
NISC「政府機関等の対策基準策定のためのガイドライン（令和5年度版）」https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

【参考】IoT製品の類型・既存の文書、認証制度等

【凡例】
- 製品個別のセキュリティ対策に関するガイドライン
- 製品個別のセキュリティ対策基準を定めた文書等（下線は義務）
- 製品個別のセキュリティ対策要件を含む認証制度
- システム全体のセキュリティ対策に関する文書等

赤字：Sマークによる認証が行われている製品

注）各製品類型に対するセキュリティ対策要件を定めたガイドラインや認証制度のうち、代表的なガイドライン、制度等をマッピングしている。ただし、CC（ISO/IEC 15408）に基づく認証制度については、グローバルで認証付与されている代表的な製品類型又はcPP(Collaborative Protection Profile)が用意されている製品類型に対してマッピングをしている。また、IEC 62443-4に基づく認証について、IEC 62443-4の対象である通信機能を有する産業用自動制御システムのコンポーネントに対してマッピングしている。

		製品類型	製品個別の対策に関するガイドライン、基準を定めた文書、認証制度等	高いレベルの基準に基づく認証制度	システム全体の対策に関する文書等
直接的又は間接的にインターネットに接続する製品	直接的にインターネットに接続する可能性がある製品	消費者向け	通信機器（ブロードバンドルーター、Wi-Fiルーターなど）	総務省：技術基準適合認定及び設計についての認証 CCDS：分野別ガイドライン（IoT-GW編） CCDS：CCDSサーティフィケーションプログラム（現状で取得実績は無いが、対象製品範囲に含まれる）		経産省：スマートホームセキュリティガイド CCDS：分野別ガイドライン（スマートホーム編）
			防犯関連機器（ネットワークカメラなど）	日本防犯設備協会：RBSS（監視カメラ、デジタルレコーダー）		
			自律型ロボット（ドローンなど）	NEDO：無人航空機分野 サイバーセキュリティガイドライン		
		産業向け	通信機器（ルーター、アクセスポイント、ファイアウォール、UTMなど）		CC認証 IEC 62443-4に基づく認証	
			防犯関連機器（ネットワークカメラなど）	日本防犯設備協会：RBSS CCDSサーティフィケーションプログラム（カメラで実績あり） IPA：情報セキュリティ対策要件チェックリスト（ネットワークカメラ）		
			産業用自律型ロボット（産業用ドローン、AGVなど）	NEDO：無人航空機分野 サイバーセキュリティガイドライン 国交省：機体認証制度		
	間接的にインターネットに接続する製品	消費者向け	通信機器（ハブ・スイッチなど）			経産省：スマートホームセキュリティガイド CCDS：分野別ガイドライン（スマートホーム編）
			生活家電（掃除機、洗濯機、冷蔵庫、レンジ、エアコンなど）			
			AV機器（スマートTV、レコーダー、スマートスピーカーなど）			
			防犯関連機器（警報装置、電気錠システムなど）	日本防犯設備協会：RBSS CCDS：CCDSサーティフィケーションプログラム（電気錠操作盤、電子シャッターで取得実績あり）		
			エネルギー関連機器（エネファーム、PCS、ガス給湯器など）	JET：系統連系保護装置等認証制度（PCSのみ） CCDSサーティフィケーションプログラム（ガス給湯器リモコンで実績あり） 各一般送配電事業者：系統連系技術要件		
			ヘルスケア機器（ウェアラブル端末、電動トレーニングマシンなど）			
			娯楽機器（ゲーム機、スマート玩具など）			
		産業向け	通信機器（ハブ・スイッチなど）	CCDS：CCDSサーティフィケーションプログラム（現状で取得実績は無いが、対象製品範囲に含まれる）	CC認証 IEC 62443-4に基づく認証	※
			産業用コントローラー（PLC、DCSコントローラーなど）			※
			産業用センサー（温度センサー、圧力センサー、変位センサーなど）			※
			OA機器（複合機など）	JBMIA：BMsec	CC認証	
			金融関係機器（決済端末、POS端末など）	CCDS：分野別ガイドライン（ATM編、オープンPOS編）→ CCDS：CCDSサーティフィケーションプログラム（ATM、決済端末で取得実績あり）		FISC：安全対策基準
			施設管理機器（入退室機器、受変電設備、照明、昇降機など）	IPA：情報セキュリティ対策要件チェックリスト（入退室管理）		経産省：ビルガイドライン
			医療機器（人工呼吸器、人工心臓弁、輸液ポンプなど）	厚労省：医療機器のサイバーセキュリティの確保及び徹底に係る手引書 → 厚労省：医療機器の薬事承認等		厚労省：医療情報ガイドライン
			自動車関連機器（ECU、IVI、TCUなど）	国交省：道路運送車両の保安基準 CCDS：分野別ガイドライン（車載器編）	CC認証	
			電気事業関連機器（スマートメーター、発電設備、PCSなど）	JESC：スマートメーターシステムセキュリティガイドライン		JESC：電制ガイドライン
			製造業・流通業関連機器（生産設備、自動倉庫など）			経産省：工場ガイド 国交省：物流ガイド
			鉄道事業関連機器（CTC装置、PRC装置など）			国交省：鉄道ガイドライン
			航空事業関連機器（IMS、iDMUなど）			国交省：航空ガイドライン

※ 各産業分野に設置される機器については、各ガイドラインにおいて、システム全体に求められるセキュリティ対策が示されている。

METI
Ministry of Economy, Trade and Industry

経済産業省のサイバーセキュリティ政策ウェブページはこちら⇒
https://www.meti.go.jp/policy/netsecurity/index.html