資料８

IoT製品に対するセキュリティ適合性評価制度の構築について

事務局説明資料

三菱総合研究所

デジタル・イノベーション本部

2022年 11月 1日

目次

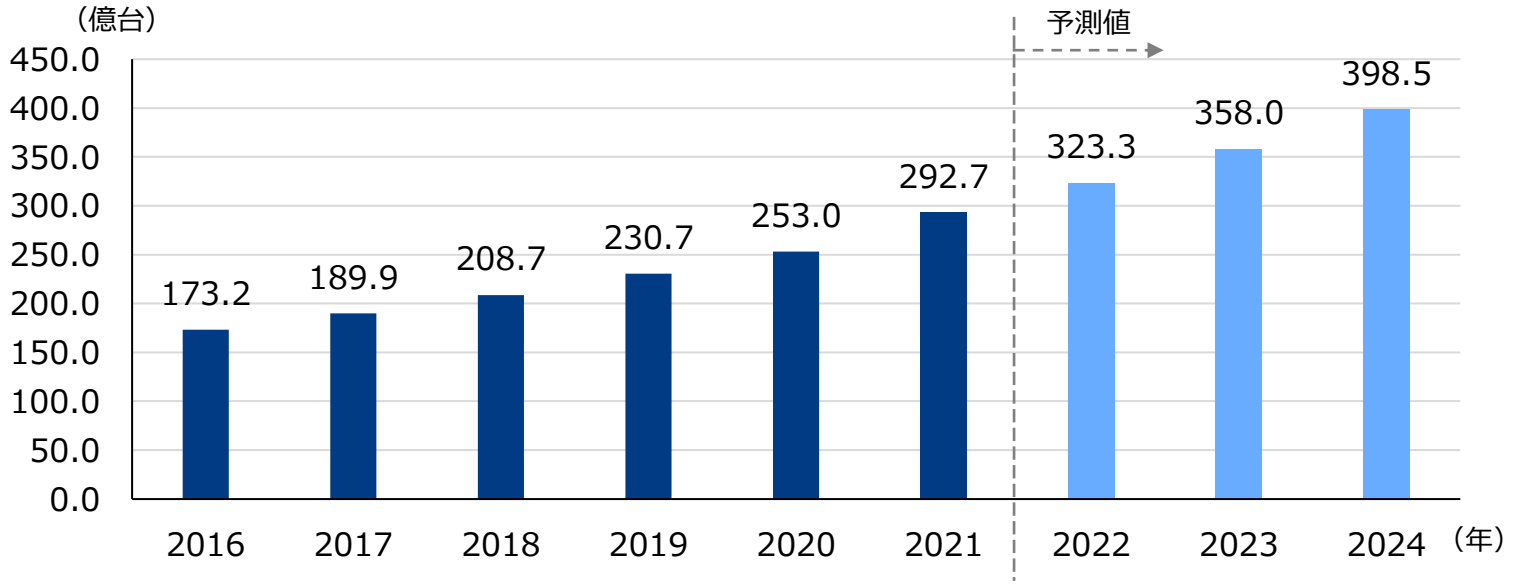
- 1. 背景
- 2. 現行でカバーできていない課題・求められる取組
- 3. 本日の討議事項
- 4. 今後の検討会における報告内容・討議事項案
- 参考資料

Copyright © Mitsubishi Research Institute

近年、IoT機器の台数は急速に増加しており、今後も増加の一途を辿ることが予想されている。

- 近年、インターネットに接続される**IoT機器の数は急速に増加**している。
- 世界のIoT機器数について、2021年には292億台程度であるが、2023年には323億台、2023年には358億台、2024年には400億台程度と、**今後も増加の一途を辿ることが予想されている**。

世界のIoT機器数の推移及び予測



※ ここでのIoT機器とは、固有のIPアドレスを持ちインターネットに接続が可能な機器及びセンサーネットワークの末端として使われる端末等を指す。

出所）総務省、令和4年度情報通信白書 https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/r04/html/nb000000.html

Copyright © Mitsubishi Research Institute

IoT機器数の急激な増加に伴い、IoT機器の脆弱性を狙ったサイバー脅威も増加傾向にある。脅威の高まりを受け、各国はIoT機器の安全性確保に向けた取組に力を入れている。

- IoT機器数の急激な増加に伴い、IoT機器の脆弱性を狙ったサイバー脅威も増加傾向にある。
- Kasperskyの調査によれば、**2021年上半期だけで、2020年の2倍以上のIoT機器に対するサイバー攻撃が発生**した。
- また、IBM Security X-Forceの調査によれば、2019年第3四半期から2020年第4四半期にかけて、**IoT機器を対象としたマルウェアの活動が3,000%増加**した。
- 同調査によれば、2020年から2021年にかけて脆弱性全体の増加率は0.4%の増加に留まった一方で、**IoT機器関連の脆弱性の件数は16%も増加**した。
- 加えて、Checkpointの研究者は、IoT機器に対するサイバー攻撃は日々増加するだけでなく、**洗練かつ広範で破壊的になりつつある**ことを指摘している。
- IoT機器に対する脅威の高まりを受け、各国はIoT機器の安全性確保に向けた取組に力を入れている。

IoT機器を対象としたサイバー脅威に関する動向

IoT機器を対象としたサイバー攻撃の増加率	200% （2020年一年間→2021年上半期）
IoT機器を対象としたマルウェア活動の増加率	3,000% （2019年第3四半期→2020年第4四半期）
IoT機器に関係する脆弱性件数の増加率	16% （2020年→2021年）

出所）Threatpost, IoT Attacks Skyrocket, Doubling in 6 Months https://threatpost.com/iot-attacks-doubling/169224/
IBM Security X-Force, X-Force 脅威インテリジェンス・インデックス 2022 https://www.ibm.com/security/jp-ja/data-breach/threat-intelligence/, https://www.ibm.com/downloads/cas/QA59ZP3P
Checkpoint, Protecting IoT Devices from Within – Why IoT Devices Need A Different Security Approach? https://blog.checkpoint.com/2022/07/25/protecting-iot-devices-from-within-why-iot-devices-need-a-different-security-approach/

Copyright © Mitsubishi Research Institute

米国では、IoT機器のセキュリティに関する複数のガイドラインが発表されているほか、セキュリティラベリング制度の検討がなされている。また、一部の州では対策が義務化されている。

- 米国政府におけるIoT機器の安全性確保に向けた近年の代表的な取組として、2020年に「IoT Cybersecurity Improvement Act of 2020」が成立し、**連邦政府がIoT機器を調達する際のガイドライン（NIST SP 800-213）が策定**された。
- また、2021年に署名されたサイバーセキュリティを強化する大統領令（Executive Order on Improving the Nation's Cybersecurity）に基づき**消費者向けIoT製品に対するセキュリティラベリング制度の構築が検討されている**。
- そのほか、州の取組として、**カリフォルニア州やオレゴン州ではIoT機器に対するセキュリティ対策が義務化**されている。

IoT Cybersecurity Improvement Act of 2020（2020年12月）

- NISTに対して、**政府機関が所有・管理する情報システムに接続されたIoT機器を、適切に使用・管理するための標準やガイドラインの作成を指示**した。
- 本法律の制定を受け、2021年11月、NISTより、連邦政府がIoT機器を調達する際のガイドラインであるNIST SP 800-213及びNIST SP 800-213Aが公表された。これらのガイドラインでは、具体的なセキュリティ対策内容について、NISTIR 8259シリーズが引用されている。

Executive Order on Improving the Nation's Cybersecurity（2021年5月）

- NISTに対して消費者向けIoT製品のラベリング制度の検討を指示。
- 2022年2月、NISTは消費者向けIoT製品に対するラベリング制度に関する考慮事項を示した文書を発表し、ラベリングのためのベースライン基準として、NISTIR 8259に基づく基準を推奨した。ただし、具体的な制度オーナー、評価方法、ラベルの種類等は定められておらず、今後の検討事項に位置づけられている。
- 2022年10月、**ホワイトハウスは、消費者向けIoT製品のラベリング制度の構築に向け、企業、団体及び政府機関のステークホルダー間で議論を実施。**ラベル付与の方法については、米国政府の基準に基づき、審査・承認された機関によってテストする方針を示しつつ、まずルーター及びホームカメラ※から着手して、**2023年春の制度展開を目指すと発表**した。

SB-327 Information privacy: connected devices（カリフォルニア州、2020年1月）

HB-2395 Oregon Cybersecurity Bill（オレゴン州、2020年1月）

- IoT機器（インターネットに接続するコネクテッドデバイス）に対するセキュリティ強化を目的とした法律で、**それぞれの州で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求めた**。
- 対象となる機器について、インターネットに直接的・間接的に接続される機器が対象となるが、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（産業用IoT製品、PC、サーバー、モバイル端末等のIT製品等）は対象外である。

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

※ この2機器の選定理由として、最も一般的かつリスクが高い機器であることを挙げている。

Copyright © Mitsubishi Research Institute

英国では、2018年に消費者向けIoT製品のセキュリティに関する行動規範が発表されたほか、消費者向けIoT製品に対する対策の義務化を求める法律の検討が進められている。

- 英国政府におけるIoT機器の安全性確保に向けた近年の代表的な取組として、2018年にDCMS（デジタル・文化・メディア・スポーツ省）が、**消費者向けIoT製品のセキュリティに関する13の行動規範である「Code of Practice for Consumer IoT Security」を公開**した。
- DCMSは本規範をEU全体に普及させるべく技術仕様の国際標準化をETSIに提案し、**本規範に基づく欧州規格であるEN 303 645が2019年11月に発表**された。
- また、**消費者向けIoT製品に対してセキュリティ対策の義務化を求める法律（Product Security and Telecommunications Infrastructure）の検討が現在進められている**。

Code of Practice for Consumer IoT Security（2018年10月）

- **消費者向けIoT製品のセキュリティに関する13の行動規範**で、消費者向けIoT製品の設計段階で安全性が確保されるよう、また利用者がデジタルの世界を安心して楽しめるようにガイドラインを設けることで、IoT製品の開発、製造、販売に携わる利害関係者を支援することを目的としている。
- 対象製品について、インターネットやホームネットワーク（両方又はその一方）と関連サービスに接続する消費者向けIoT製品を対象としている。
- 英国DCMSは**本行動規範をEU全体に普及させるべく、技術仕様の国際標準化をETSIに提案**した。ETSIはこの提案に基づき、EU加盟各国のステークホルダーによる討議を実施し、2019年2月にTS（技術仕様）であるETSI TS 103 645を公表、2019年11月には、**EN 303 645として欧州規格化**された。なお、ETSI EN 303 645はフィンランド、ドイツ、シンガポールのラベリング制度のベースとなっているほか、右記PSTI法案のベースにもなっている。

Product Security and Telecommunications Infrastructure （検討中）

- 2021年11月24日に**庶民院（下院）に提出された法案で、インターネットに接続するスマートフォン、スマートTV、スマートスピーカー等の機器に対して、セキュリティ対策を義務化**する内容が含まれている。2022年10月27日時点で、**庶民院・貴族院（上院）の両方を通過し、国王の裁可に向けた最終修正段階**である。
- 具体的な対策として、デフォルトパスワードの禁止、脆弱性開示ポリシーの開示、セキュリティアップデートを受ける期間に関する情報の開示の3点が含まれ、自己適合宣言又は第三者評価による適合性評価が必要となる。
- 現状の法案では、法案には遵守しない企業に対する罰金に関する条項も含まれており、最高1,000万ポンド又は当該企業の全世界売上高の4%以内の罰金が科せられる内容となっている。
- 対象となる企業について、機器のメーカーだけでなく、輸入業者や販売業者も含まれる。
- なお、法案が可決された後、完全に施行される前に少なくとも12ヶ月の準備期間を設ける予定であることが示されている。

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

Copyright © Mitsubishi Research Institute

メーカーによる任意対策に関する取組（ガイドライン、任意認証制度・ラベリング制度 等）

メーカーによる対策義務に関する取組（法規制）

欧州では、IoT機器を含む製品の認証スキームが検討されているほか、無線機器に対するセキュリティ対策が2024年8月から義務化される予定である。

- 欧州全体のIoT機器の安全性確保に向けた近年の代表的な取組として、2019年に「EUサイバーセキュリティ法」が施行され、欧州での**IoT機器を含む製品の認証スキームであるEUCC（Common Criteria based European Candidate Cybersecurity Certification Scheme）が検討されている**。
- 2022年9月に**EU市場に投入されるデジタル製品のセキュリティ対応を義務付ける「EUサイバーレジリエンス法」の草案を発表**。2025年後半の施行を予定しており、**対象製品の上市にあたってはセキュリティ要件への適合性証明（自己適合宣言もしくは第三者認証）が求められる**。
- 加えて、**無線機器に関する「EU無線機器指令（RED）（2014/53/EU）」にセキュリティに関する要件が追加**され、**2024年8月から欧州で販売する無線機器に対するセキュリティ対策が義務化**される。

EUサイバーセキュリティ法（2019年6月）

- 2004年に設立されたENISAの役割を強化するとともに、**EUにおけるデジタル関連製品・サービス・プロセスのサイバーセキュリティ認証制度（EUCC）の枠組みを設置**した。
- EUCCはサイバーセキュリティ法に基づく任意の認証制度で、その枠組みも同法に定められており、既存のCC（Common Criteria）のスキームの後継として機能させることを目的としている。
- 2021年5月には、EUCCのスキーム候補に関する報告書（Ver 1.1.1）を公表し、ISO/IEC 15408とISO/IEC 18045に基づいて、ICT製品のサイバーセキュリティの認証を検討していることを発表した。

EUサイバーレジリエンス法（2022年9月草案発表、2025年後半施行予定）

- 2022年9月15日、欧州委員会は、**EU市場に投入されるデジタル製品のセキュリティ対応を義務付けるEU Cyber Resilience Actの草案を発表**した。
- ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆるデジタル製品が対象となるが、既存の規則で対象となる製品は対象外である。
- 求められる対策として、リスクに応じた適切なレベルのサイバーセキュリティを確保するように設計、開発、生産することのほか、悪用可能な既知の脆弱性がない状態とすること、製品のSBOMを作成すること等、多岐にわたる対策が求められる。
- 対象製品の上市に当たって、当該製品に対するセキュリティ要件への適合性証明（自己適合宣言もしくは第三者認証）が求められる。

EU無線機器指令（RED）（2014/53/EU）（2022年2月発行、2024年8月より義務化予定）

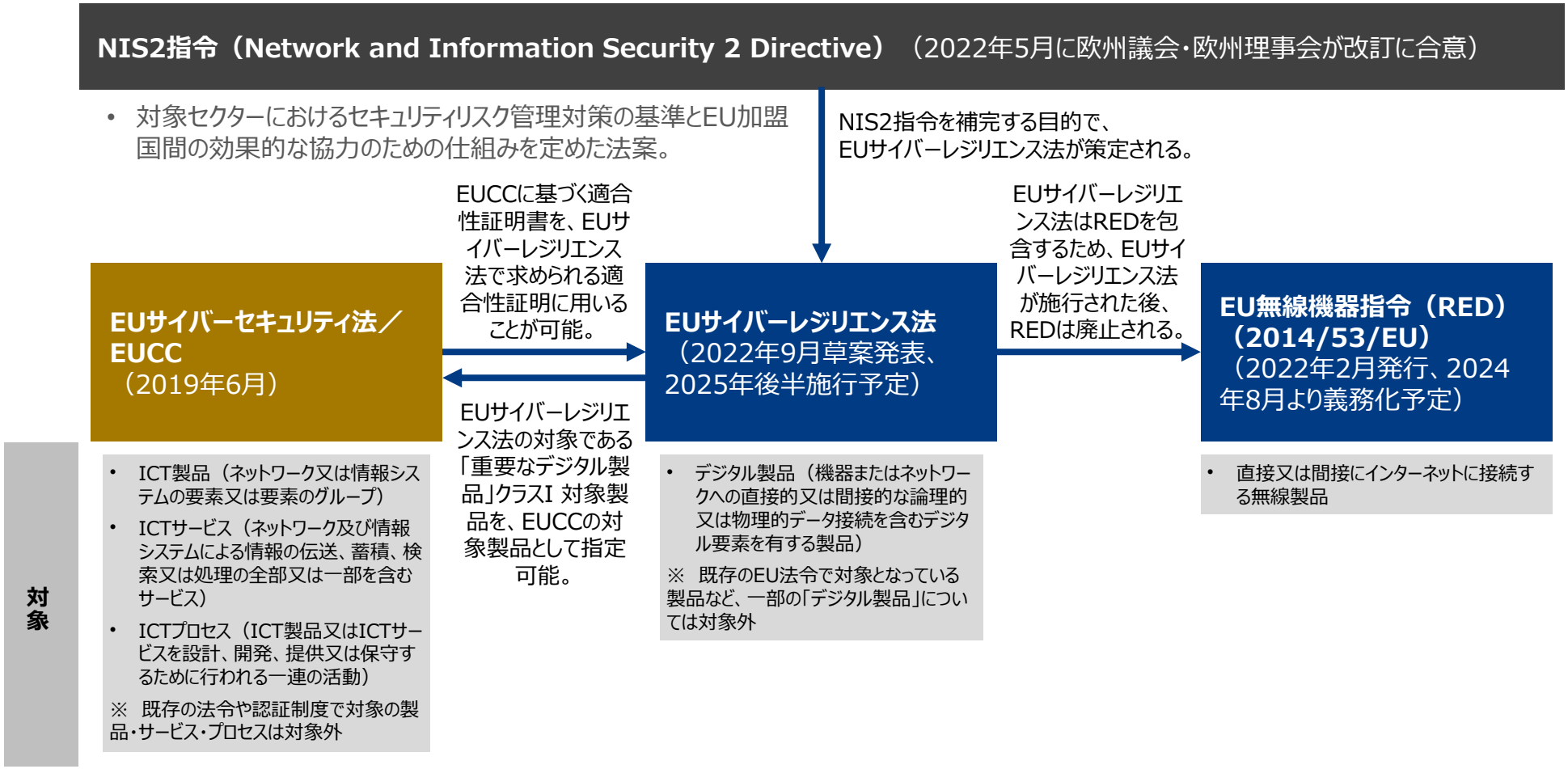
- 2022年1月12日、欧州委員会は、**Radio Equipment Directive（欧州無線機器指令）のサイバーセキュリティ関連条項の施行に関する委任規則（EU）2022/30が発行**し、EU市場に投入される無線機器に対してセキュリティの強化を求めた。
- 具体的な規則は2024年8月1日より義務化。
- 対象機器について、直接・間接問わずインターネットに接続される無線機器が対象となる。
- 求められる対策として、許容できないサービスの低下を引き起こさないこと、個人データ及びプライバシーを保護するための手段を組み込んでいること、不正行為から保護するための一定の機能をサポートすることの3点が求められているが、具体的な規格要件は2023年10月までに準備される予定である。

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

Copyright © Mitsubishi Research Institute

【参考】EUサイバーレジリエンス法と他のEU法令との関係

- EUサイバーレジリエンス法は、2022年5月に欧州議会・欧州理事会が改訂に合意したNIS2指令を補完する目的で策定された。
- EUサイバーレジリエンス法はREDを包含するため、EUサイバーレジリエンス法が施行された後、REDは廃止される。
- EUサイバーセキュリティ法との関係について、EUCCに基づく適合性証明書をEUサイバーレジリエンス法で求められる適合性証明に用いることが可能である。対象について、ICTサービスやプロセスも対象としているEUCCの方が対象範囲が広いが、製品自体の定義に大きな差異はない。



出所）各種動向に関する公開情報に基づき三菱総合研究所作成

Copyright © Mitsubishi Research Institute

【参考】EUサイバーレジリエンス法の対象製品／対象外製品

- 対象となる「デジタル製品」のうち、重要な「デジタル製品」のうちリスクが低い製品をクラスⅠ、リスクが高い製品をクラスⅡとして詳細に定義しており、クラスに応じて、選択できる適合性証明の方法が異なる。
- 既存のEU法令で対象となっている製品など、一部の「デジタル製品」については、今回の法案の対象外として明記されている。

サイバーレジリエンス法の対象となる「デジタル製品」
デジタル要素を備えた全てのソフトウェア製品・ハードウェア製品で、
デバイスやネットワークに直接的/間接的に接続されるコンポーネントも含む。

重要な「デジタル製品」（クラスⅠ）
重要な「デジタル製品」であるが、リスクが低い製品。

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. SIEM（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、IDS/IPS（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. NIS2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）

重要な「デジタル製品」（クラスⅡ）
重要な「デジタル製品」のうち、リスクが高い製品。

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. NIS2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
15. コントローラー

▶ **自己適合宣言もしくは第三者認証を選択**　▶ **EUCCやEN規格の対象外の製品は第三者認証が必要**　▶ **第三者認証が必要**

出所）EU, Cyber Resilience Actに基づき三菱総合研究所作成 https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

対象外の製品・理由、関連する日本国内法令

対象外製品	対象外の理由	関連する日本国内法令
• **医療機器** • **体外診断用医療機器**	既存のEU法（Regulation (EU) 2017/745、Regulation (EU) 2017/746）の対象であるため。	2023年を目処に、IMDRFガイダンス※を薬機法の医療機器規制に取り入れる方針が示されている。
• **自動車**	既存のEU法（Regulation (EU) 2019/2144）の対象であるため。	道路運送車両の保安基準（道路運送車両法）
• **航空機関連のデジタル製品**	既存のEU法（Regulation (EU) 2018/1139）の対象であるため。	航空法
• **SaaSなどのソフトウェアサービス**	今後策定されるNIS2指令の対象であるため。	-
• **国家安全保障または軍事目的にのみ開発されたデジタル製品** • **機密情報を処理するために特別に設計された製品**	特に理由は明記されていない。	-

※国際医療機器規制当局フォーラム（IMDRF）が発表した医療機器に関するサイバーセキュリティ対策のガイダンスのこと。

Copyright © Mitsubishi Research Institute

メーカーによる任意対策に関する取組（ガイドライン、任意認証制度・ラベリング制度 等）

メーカーによる対策義務に関する取組（法規制）

MRI

ドイツ、シンガポール、フィンランドでは消費者向けIoT製品に対するセキュリティラベリング制度を既に運用開始しているほか、オーストラリアでは当該制度の運用に向けた検討を進めている。

- その他諸外国政府におけるIoT機器の安全性確保に向けた近年の代表的な取組として、**ドイツ、シンガポール、フィンランドでは、消費者向けIoT製品に対するセキュリティラベリング制度が既に開始している**ほか、**オーストラリアでも同様のラベリング制度の構築に向けた検討がなされている**。

IT-Sicherheitskennzeichen (IT Security Label)（2021年12月～）

- 対象製品について、現状では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製品のみを対象としているが、今後対象製品を拡大する方針を示している。
- ラベル付与のためには、**ETSI EN 303 645の要件に加え、各製品分野のセキュリティ要件（BSI及びETSIが作成）を満たしていることを、認定を受けたセキュリティ機関によって評価されることが必要**となる。
- 2022年10月27日時点（制度開始後11ヶ月）で34製品・サービスがラベルを取得している。

Finnish Cybersecurity Label（2020年1月～）

- 対象製品について、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・サービスを対象としている。
- ラベル付与のためには、**ETSI EN 303 645をベースに作成された情報セキュリティ要件を満たしていることを、認定を受けたセキュリティ機関によって評価されることが必要**となる。
- 2022年10月27日時点（制度開始後36ヶ月）で17製品がラベルを取得している。
- シンガポールのCLSとの相互運用を行っており、本制度でラベルが付与された製品は、シンガポールのCLSでレベル3を満たしていると認められる。

相互運用実施

Cybersecurity Labelling Scheme (CLS)（2020年10月～）

- すべての消費者向けIoT製品がラベリングの対象である。
- ラベルは4段階に分かれ、**レベル1・2は開発者の自己適合宣言で取得可能、レベル3・4では第三者機関による検証が必要**となる。ラベル付与のためにはETSI EN 303 645の要件に加え、レベル3では、第三者機関によるバイナリ解析、レベル4では機器に対するペネトレーションテストにクリアする必要がある。
- 2022年10月27日時点（制度開始後22ヶ月）で222製品がラベルを取得しているほか、本制度の要件はISO/IEC 27404として、国際標準化に向けた提案がなされている。

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、**あらゆる消費者向けのスマートデバイスを対象としたセキュリティラベリング制度の検討が進められている**。
- ラベル付与のための基準として、ETSI EN 303 645を採用する方針が示されている。
- なお、2021年にはBETA（豪州政府行動経済学チーム）がIoT製品のセキュリティラベルの有効性に関する調査を実施し、セキュリティラベルが付与されることで、IoT製品に対する消費者の支払意思額が増加することを示した。

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

Copyright © Mitsubishi Research Institute

我が国においてもIoT機器の安全性確保に向けた取組を推進してきており、代表的な取組として、IoT製品メーカーの対策を支援するガイドラインを複数発表している。

- 我が国においてもIoT機器の安全性確保に向けた取組を推進してきた。
- 代表的な取組として、経済産業省、IPA、総務省等は**メーカーのセキュリティ対策を支援するガイドラインを複数発表**している。

#	文書タイトル	発行時期	発行者	文書概要
1	サイバー・フィジカル・セキュリティ対策フレームワーク（CPSF）	2019年4月	経済産業省	新たなサプライチェーン構造において求められるセキュリティ対策の全体像を整理し、セキュリティ対策例をまとめた文書
2	IoTセキュリティ・セーフティ・フレームワーク（IoT-SSF）	2020年11月	経済産業省	IoT機器・システムをリスクに応じてカテゴライズし、各カテゴリに対するセキュリティ・セーフティ要求の検討の考え方を示した文書
3	機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き	2021年4月	経済産業省	機器のセキュリティ検証において検証サービス事業者や検証依頼者が実施すべき事項等について整理した文書
4	電気用品、ガス用品等製品のIoT化等による安全確保の在り方に関するガイドライン	2021年4月	経済産業省	家電製品などがインターネット環境で使われることで想定されるリスクに対し、安全確保の在り方を示した文書
5	IoTセキュリティ・セーフティ・フレームワーク Version 1.0 実践に向けたユースケース集	2022年4月	経済産業省	一連のIoT-SSFの適用の流れを、複数のユースケースを用いて例示した文書
6	IoTセキュリティガイドライン ver 1.0	2016年7月	IoT推進コンソーシアム、総務省、経済産業省	リスクに応じた適切なサイバーセキュリティ対策を検討するための考え方を、分野を特定せずまとめた文書
7	つながる世界のセーフティ&セキュリティ設計入門	2015年10月	IPA	IoT製品のセーフティ設計・セキュリティ設計の手法の用い方について解説した文書
8	つながる世界の開発指針	2016年3月	IPA	IoT製品の開発時に考慮すべき安全安心に関わる事項を指針としてとりまとめた文書
9	IoT開発におけるセキュリティ設計の手引き	2016年5月	IPA	IoT製品のセキュリティ設計を担当する開発者に向けた手引きとして、参考となる情報をまとめた文書
10	つながる世界の品質確保に向けた手引き	2018年6月	IPA	IoT製品やシステムの品質をライフサイクルにわたり確保・維持するために注意が必要となるポイントをまとめた文書
11	脆弱性対処に向けた製品開発者向けガイド	2020年8月	IPA	製品開発者において実施すべき脆弱性対処と、その開示方法を掲載した文書
12	IoT機器等を開発する中小企業向けのセキュリティ対策に関するガイドライン（仮称）	作成中	経済産業省（予定）	中小のIoT機器メーカーが現実的に対応可能な範囲で実施が求められる対策を示した文書（予定）

出所）各種ガイドラインや検討に基づき三菱総合研究所作成

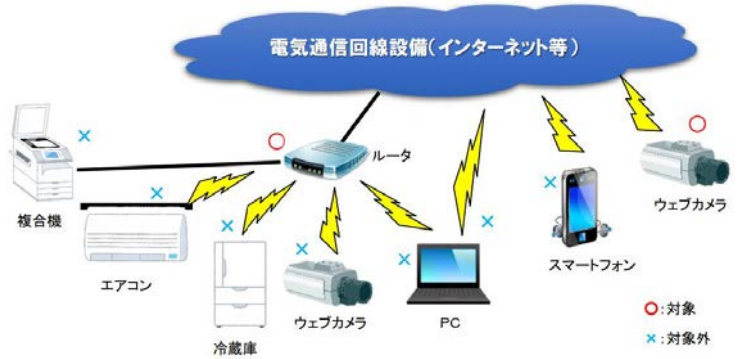
Copyright © Mitsubishi Research Institute

総務省の端末設備等規則の一部改正により、インターネットに直接接続するIoT機器におけるセキュリティ対策の実装が義務化されている。

- 総務省は端末設備等規則（省令）（第34条の10）を2020年4月に一部改正し、**電気通信業者のネットワークに直接接続する同規則の施行後に販売されたIoT機器においてアクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の実装を原則義務化**した。
- また、総務省及びNICTは、**サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起の取組であるNOTICE（National Operation Towards IoT Clean Environment）を2019年2月から開始**している。

端末設備等規則（省令）（第34条の10）（2020年4月より原則義務化）

- 端末設備等規則の一部改正が施行され、**電気通信業者のネットワークに直接接続するIoT機器においてアクセス制御機能、初期パスワードの変更機能、ソフトウェアの更新機能の実装が原則義務化**された。
- 対象となる設備のイメージは以下のとおりであり、例えば、ルータやインターネットに直接接続するウェブカメラ等は該当するが、電気通信回線設備（インターネット等）に直接接続して使用されない機器、PC・スマートフォン、専用線のみにつながる機器等は対象外である。



NOTICE（National Operation Towards IoT Clean Environment）（2019年2月～）

- インターネットサービスプロバイダー（ISP）と連携した、**サイバー攻撃に悪用されるおそれのあるIoT機器の調査及び当該機器の利用者への注意喚起を行う取組**である。
- NICTがインターネット上のIoT機器に容易に推測されるパスワードの入力等を行うことで、サイバー攻撃に悪用されるおそれのある機器を調査し、当該機器の情報をISPに通知する。
- ISPは、NICTから受け取った情報を元に当該機器の利用者を特定し、電子メールや郵送などにより注意喚起を行う。
- 2022年8月時点で73社のISPと連携し、当該ISPの約1.12億のIPアドレスに対して調査を実施した。
- 調査の結果、ログインが可能であり、注意喚起対象としてISPに通知されたIoT機器の件数は2022年8月分で4,381件であった。

出所）総務省、電気通信事業法に基づく端末機器の基準認証に関するガイドライン(第２版) https://www.soumu.go.jp/main_content/000744264.pdf
NOTICEホームページ https://notice.go.jp/

Copyright © Mitsubishi Research Institute

IoT機器を対象に含む国内の認証制度として、IPAによるCC認証、ISASecureによるCSA認証のほか、CCDSによるCCDSサーティフィケーションプログラムが存在する。

- IoT機器を対象に含む認証制度として、**IPAによるCC（Common Criteria）認証が存在**するほか、**産業用IoT機器に対する認証制度としては、IEC 62443-4-2に基づくCSA（Component Security Assurance）認証制度が存在**する。
- 加えて、**CCDSが運用するIoT製品の認証プログラムであるCCDSサーティフィケーションプログラムが存在**する。

IPA：Common Criteria（CC）認証制度

- **IT関連製品のセキュリティ機能の適切性・確実性をISO/IEC 15408に基づき適合性評価機関が評価し、その評価結果を認証機関が認証する制度**である。
- IT関連製品のCC認証取得のためには、認定機関によって認定された適合性評価機関（試験機関）によって検証・評価が実施される必要がある。
- 適合性評価機関によって作成された検証・評価結果レポートは認証機関（各国のセキュリティ機関）に報告され、検証・評価の結果に基づき、製品が認証を受ける。
- 認証機関は、評価結果を確認した後、その製品に対する認証書を発行する。なお、認証は国際的承認アレンジメント加盟国（CCRA加盟国）でも通用する。

ISASecure： CSA（Component Security Assurance）認証制度

- **産業用コンポーネント製品に対するセキュリティ認証制度**であり、従来のEDSA認証制度を拡張する形で2019年8月から開始している。
- CSA認証は、IEC 62443-4-2に基づき、ソフトウェア開発プロセスのセキュリティ評価、機能的セキュリティ評価、脆弱性テストの3つの観点から評価される。
- 対象機器について、ソフトウェアアプリケーション、組込み機器、ホストデバイス、ネットワークデバイス等を含む産業用コンポーネント機器が対象となる。
- 認証機関として、国内では技術研究組合制御システムセキュリティセンター CSSC認証ラボラトリーがある。

CCDS：CCDSサーティフィケーションプログラム

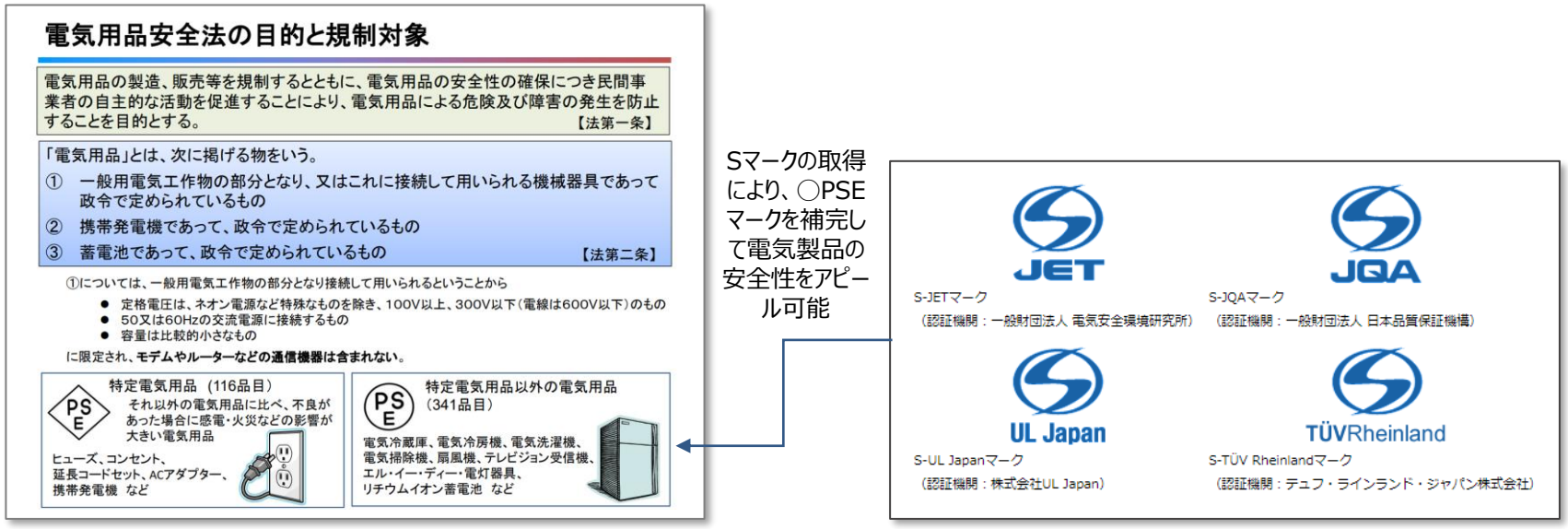
- **一定のセキュリティ確保のための要件を満たしたIoT機器に対する認証サービス**で、2019年10月より開始している。
- 認証は3段階のレベルに分かれ、レベル1はIoT機器として共通する一般的要件、レベル2以上は製品分野別に設定された要件への遵守が必要となる。
- 対象機器について、インターネットにつながるIoT機器全般が現状の対象であるが、今後IoT機器を利用したサービスも範囲に含むことが検討されている。
- 認証は、CCDSが独自で策定した「IoT 機器セキュリティ要件ガイドライン」の要件に基づく。
- 認証が付与された製品に対しては、賠償損害や費用損害に対する保険が付与される。

出所）各種動向に関する公開情報に基づき三菱総合研究所作成

Copyright © Mitsubishi Research Institute

【参考】電気用品安全法（PSEマーク／Sマーク）の概要

- 電気用品安全法（電安法）とは、電気用品の製造・輸入・販売を事業として行う場合の手続きや罰則を定めた法律であり、危害発生のおそれがある製品を電気用品として指定し（457品目）、国が定めた技術基準の遵守を義務付けている。
- PSEマークは、◇PSEマークと○PSEマークの二種類が存在する。
- 危害発生のおそれが高い特定電気用品（116品目）については、自主検査に加え、第三者検査機関による適合性検査が必要であり、この検査に合格した製品において◇PSEマークが表示される。他方で、○PSEマークは自主検査にて表示できる。
- PSEマークとは異なり、法律で義務付けられた認証制度ではないが、○PSEマークを補完する目的等で電気製品の安全性をアピールするSマークが存在する。店頭で販売されている主な電気製品の7割程度にSマークが表示されている。
- Sマークの対象製品について、電安法の対象製品457品目（特定電気用品116品目、特定電気用品以外の電気用品341品目）のほか、あらゆる電気製品が対象となるが、現状では電安法の規制対象品目において多く活用されている。
- Sマークの認証基準について、電安法の技術基準の解釈をベースにした認証基準としている。電安法の規制外の製品については、Sマーク認証機関が定める又は認めるJISやIEC等の基準に基づく。



出所）経済産業省、電気用品安全法の目的と規制対象 https://www.meti.go.jp/policy/consumer/seian/denan/topics/mlb/outline_of_law.pdf
電気製品認証協議会（SCEA） http://www.s-ninsho.com/s_attestation.html

Copyright © Mitsubishi Research Institute

【参考】国内外における任意認証制度・ラベリング制度の概要

政府機関におけるIoT製品等に対する任意認証制度・ラベリング制度の概要（灰色塗りは、現在検討中の制度を意味する）

国	制度名	制度分類	制度オーナー	認証取得・ラベル取得に要する費用	基準	製品数※1
米国、英国、日本など※2	Common Criteria	認証	各国セキュリティ関係機関	EAL2で1,000万～2,000万円、EAL3で1,600万～2,700万円、EAL4で4,000万～1億円程度。	ISO/IEC 15408	1,652
米国、日本など	Component Security Assurance (CSA)	認証	ISASecure	約1,000万円	IEC 62443-4-1, IEC 62443-4-2	58
	EUCC	認証	ENISA	-	ISO/IEC 15408に基づく基準が検討中	–
	Certification de Sécurité de Premier Niveau（CSPN）	認証	ANSSI※3	約300万円～600万円	ISO/IEC 15408を一部抜粋した基準	53
	Commercial Product Assurance (CPA)	認証	NCSC※4	約2,000万円	The CPA Build Standard	39
	Cybersecurity Labeling for Consumer IoT Product	ラベリング	未定	-	NISTIR 8259に基づく基準でほぼ確定	–
	IT-Sicherheitskennzeichen (IT Security Label)	ラベリング	BSI※5	約1万円～50万円＋検証費用	ETSI EN 303 645やBSIの技術ガイドライに基づく基準	34
	Labelling for Smart Devices	ラベリング	未定	-	ETSI EN 303 645の予定	–
相互運用を実施	Cybersecurity Labelling Scheme (CLS)	ラベリング	CSA※6	約5,000円～35万円＋検証費用	ETSI EN 303 645やIMDAガイドラインに基づく基準	222
	Finnish Cybersecurity Label	ラベリング	TRAFICOM※7	約10万円＋検証費用	ETSI EN 303 645に基づく基準	17

※1: 2022年10月27日時点。
※2: CCRAにより、認証国17カ国でCC認証を受けた製品は、CCRC加盟国において、CC認証製品として相互に承認される。
※3: Agence nationale de la sécurité des systèmes d'information。フランス国家情報システムセキュリティ庁のこと。
※4: National Cyber Security Centre。英国国家サイバーセキュリティセンターのこと。
※5: Bundesamt für Sicherheit in der Informationstechnik。ドイツ連邦政府情報セキュリティ庁のこと。
※6: Cyber Security Agency of Singapore。シンガポールサイバーセキュリティ庁のこと。
※7: Finnish Transport and Communications Agency。フィンランド運輸通信庁のこと。

出所）各国関連制度に関する公開情報に基づき三菱総合研究所作成

Copyright © Mitsubishi Research Institute

【参考】国内外における法規制（対策義務）の概要

- 以下に示す法規制はIoT製品全般を対象とした法規制であり、スマートメーターや医療機器等、産業分野別のセキュリティ規制は別途存在することに留意。

国内外におけるIoT製品のセキュリティ対策に関する法規制（灰色塗りは、現在検討中・準備中の法規制を意味する）

国	法規制名称	所管組織	対象製品
	端末設備等規則（省令）（第34条の10）	総務省	電気通信回線設備（インターネット等）に直接接続する製品。
	SB-327 Information privacy: connected devices（カリフォルニア州）	カリフォルニア州	直接又は間接にインターネットに接続するIoT製品。
	HB-2395 (2019) Oregon Cybersecurity Bill（オレゴン州）	オレゴン州	直接又は間接にインターネットに接続する消費者向けIoT製品。
	EUサイバーレジリエンス法	欧州委員会	ソフトウェアやハードウェアを含む、他の製品やネットワークへの直接的・間接的な接続が存在するあらゆるデジタル製品。
	EU無線機器指令（RED）【2024年8月より義務化】	欧州委員会	直接又は間接にインターネットに接続する無線製品。
	Product Security and Telecommunications Infrastructure (PSTI) Bill	DCMS※1	直接又は間接にインターネットに接続する消費者向けIoT製品。（予定）

※1: Department for Digital, Culture, Media & Sport。英国デジタル・文化・メディア・スポーツ省のこと。

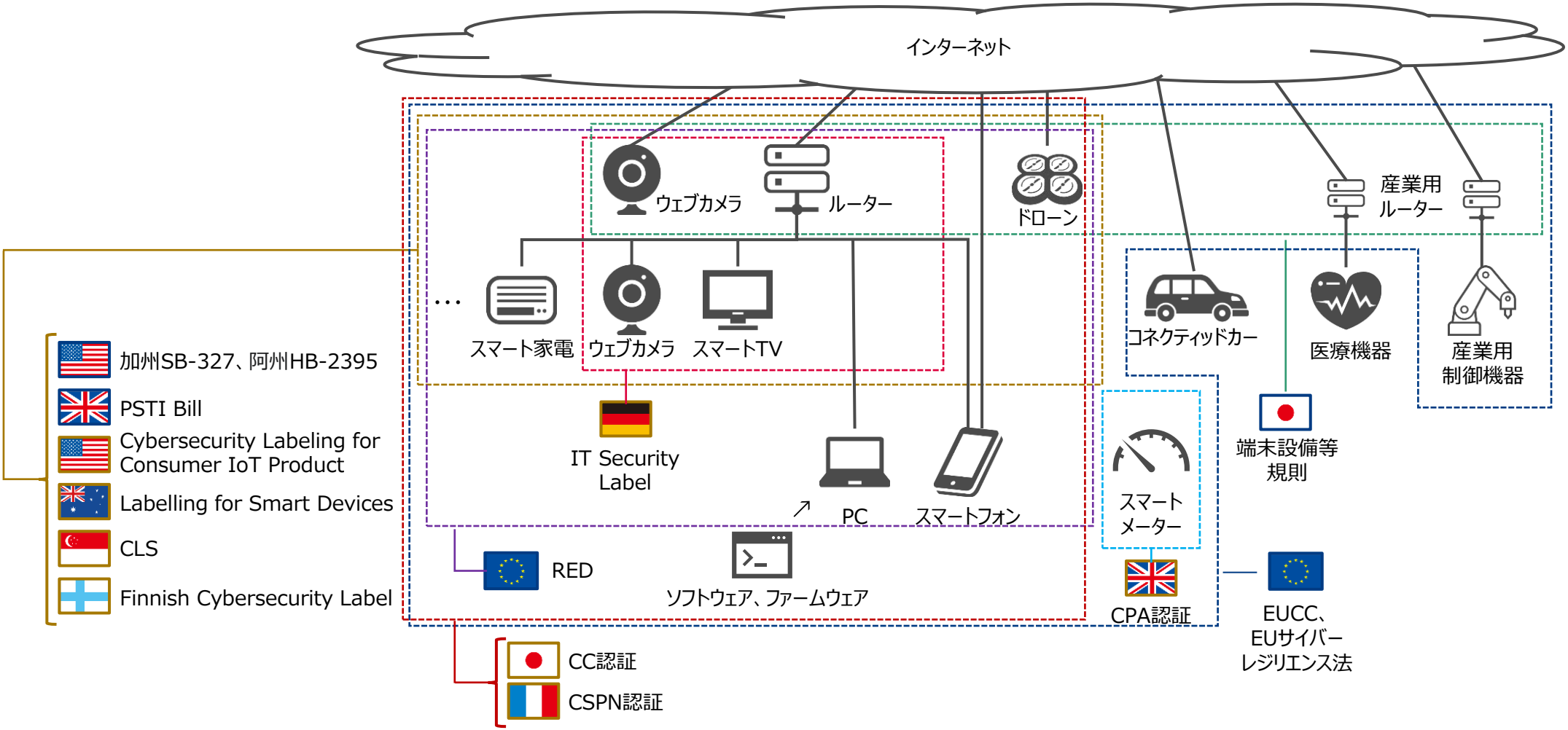
出所）各国関連法規制に関する公開情報に基づき三菱総合研究所作成

Copyright © Mitsubishi Research Institute

【参考】国内外の任意対策・対策義務に関する取組の対象製品

- IoT製品等に対する任意認証制度・ラベリング制度及び法規制の対象範囲イメージは以下のとおり。

IoT製品等に対する任意認証制度・ラベリング制度及び法規制における対象製品範囲イメージ



出所）各国関連制度に関する公開情報に基づき三菱総合研究所作成

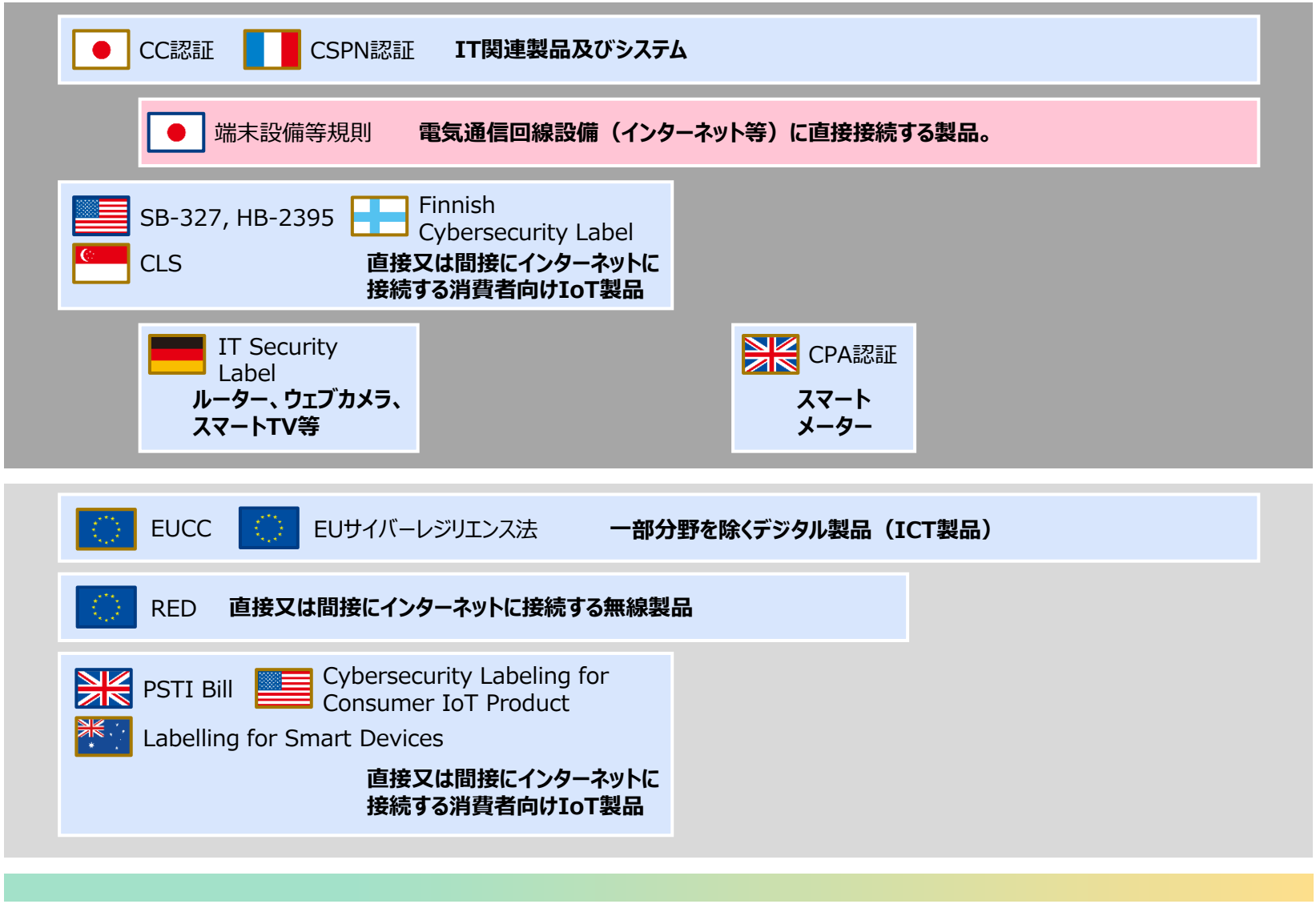
Copyright © Mitsubishi Research Institute

メーカーによる任意対策に関する取組（ガイドライン、任意認証制度・ラベリング制度 等）

メーカーによる対策義務に関する取組（法規制）

【参考】国内外の任意対策・対策義務に関する取組のポジショニングマップ

- IoT製品等に対する任意認証制度・ラベリング制度及び法規制の対象範囲と取組状況のポジショニングマップイメージは以下のとおり。



出所）各国関連制度に関する公開情報に基づき三菱総合研究所作成

※ 各枠は、各取組の対象製品範囲のイメージを示す。青塗枠は直接的・間接的にインターネットに接続する製品を対象としている取組、赤塗枠は直接的のみインターネットに接続する製品を対象としている取組を意味する。

Copyright © Mitsubishi Research Institute

既存制度ではカバーできていないと考えられる課題や、それを踏まえた方向性は以下のとおり。

- ✓ **IoT機器メーカー視点の課題**として、**メーカーにおけるセキュリティ対策の取組を利用者にアピールすることができず、対策に要するコストを製品の販売価格に反映しづらい**。また、既存制度の認証取得による明確なインセンティブが存在していない。
- ✓ **IoT機器利用者視点**では、**適切なセキュリティ対策が施された製品がわかりづらいため、適切な対策が施されていない製品を購入してしまう**ことに繋がり、結果として、**セキュリティ対策が担保されているかが不透明なIoT製品が国内に多く導入されてしまうおそれ**。
- ✓ **対象範囲に関する課題**として、例えば総務省規則の対象外である**スマートロックにおいて十分なセキュリティ対策が施されていない場合、利用者の財産に影響を及ぼすインシデントにつながるおそれ**。このような製品においては、製品安全に関する「電気用品安全法」の技術基準の解釈において、通信機能途絶時の対応や操作端末の識別管理に関する要件が含まれているものの、一般的なセキュリティ対策についてはカバーできていない。
- ✓ **国際競争力に関する課題**として、現行の取組は諸外国と相互認証を行える領域も限定的であることから、**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るおそれ**。

- **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。**
- その際には、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**。

Copyright © Mitsubishi Research Institute

本日の検討会では、次頁の仮説を踏まえつつ、以下の点についてご議論いただきたい。

1. どのようなIoT製品を対象とすべきか。

- ✓ 諸外国制度と同様の対象範囲とする
- ✓ 直接的／間接的にインターネットに接続するIoT製品を対象とする
- ✓ 消費者向けIoT／産業用IoTのいずれか／いずれも対象とする　等

2. どのような適合性評価基準を採用すべきか。

- ✓ ドイツ、シンガポール、フィンランドのラベリング制度と同様にETSI EN 303 645をベースとする
- ✓ Common Criteriaと同様にISO/IEC 15408をベースとする
- ✓ 新たな基準を開発する　等

3. どのようなスキームで適合性評価を行うべきか。

- ✓ 政府が制度のスキームオーナーとなりつつ、適合性評価は民間の適合性評価機関が実施する
- ✓ シンガポールのラベリング制度のように自己適合宣言（第一者評価）を認める／ドイツ・フィンランドのラベリング制度のように適合性評価機関による評価（第三者評価）を必須とする
- ✓ 諸外国との相互承認を認める／相互認証の形式を取らずとも、各国の制度において外国の適合性評価機関を認める　等

4. 諸外国とはどのような国々と、どのような共通認識を醸成していくべきか。

- ✓ 二国間対話（日米、日EU、日英、日シンガポール等）やQUAD間での議論を実施し、相互承認スキームの構築を目指す／相互承認に形式は取らずとも適合性評価基準を一致させる　等

5. その他、上記の討議事項のほか、今後制度の骨格を検討するにあたり、大きく議論すべき論点はあるか。

- ✓ 適合性評価にかかる費用・期間のあるべき姿、評価後にセキュリティの懸念が発覚した場合の扱い（市場監査、罰則）、制度の広報 等

Copyright © Mitsubishi Research Institute

構築する仕組みの考え方の仮説は以下のとおり。
（今後の議論を通じ、方向性を取りまとめる。）

	①消費者向けIoT製品を対象とした簡易的な適合性評価	②Common Criteria認証・CSA認証等(IoT関連製品を対象とした既存の適合性評価)	③高リスクな産業用IoT製品を対象としたハイレベルな適合性評価
対象製品案 (討議事項1. どのようなIoT製品を対象とすべきか。)	直接又は間接にインターネットに接続する消費者向けのIoT製品 （例）  スマート家電　ウェブカメラ　ブロードバンドルーター	CC認証・CSA認証等における既存対象製品 （例）  PC　MFP（複合機）　産業用ルーター	高リスクな産業用IoT製品 （例）  重要インフラに用いられる産業用ルーター　重要インフラに用いられる産業用制御機器
適合性評価基準案 (討議事項2. どのような適合性評価基準を採用すべきか。)	ETSI EN 303 645	ISO/IEC 15408、IEC 62443等 （既存制度の適合性評価基準）	諸外国と連携可能な基準とするか、国内独自基準とするかは要検討
適合性評価スキーム案 (討議事項3. どのようなスキームで適合性評価を行うべきか。)	IoT製品メーカーによる自己適合宣言か、第三者評価を選択可能な形式とする	ISO/IEC 17025に基づき認定機関により認定された適合性評価機関による第三者評価を必須とする （既存制度の適合性評価スキーム）	認定機関により認定された適合性評価機関による第三者評価を必須とする （認定基準は別途検討）
諸外国との共通認識案 (討議事項4. 諸外国とはどのような国々と、どのような共通認識を醸成していくべきか。)	消費者向けIoT製品を対象とした適合性評価制度が存在する又は検討中である米国、EU、英国、シンガポール、豪州等と日本との間で、ハーモナイズすべき範囲を調整※1する	既存認証制度における国際相互承認を継続して実施する	国際ハーモナイゼーションの可能性を考慮し、ハーモナイズすべき範囲を調整※1しつつ、国内で整備すべき事項を見極める

諸外国とのハーモナイゼーションを見据えた検討を進める

ハーモナイゼーションの可能性を考慮しつつ、諸外国動向を踏まえ、国内で整備すべき事項を見極める

Copyright © Mitsubishi Research Institute

※1: QUAD、日EUデジタルパートナーシップ、日英デジタルパートナーシップ等の座組を活用

今後の進め方は以下を想定している。

- 今年度内に3回の検討会を開催し、**我が国におけるIoT製品の適合性評価制度構築に向けた中間報告案を取りまとめる**。
- このために、次回の検討会では、本日の議論結果を踏まえて整理・検討した対象製品、運用主体、適合性評価方法の案についてご報告させていただくとともに、適合性評価基準や適合性評価を受けた製品の可視化方法についてご議論いただく予定である。

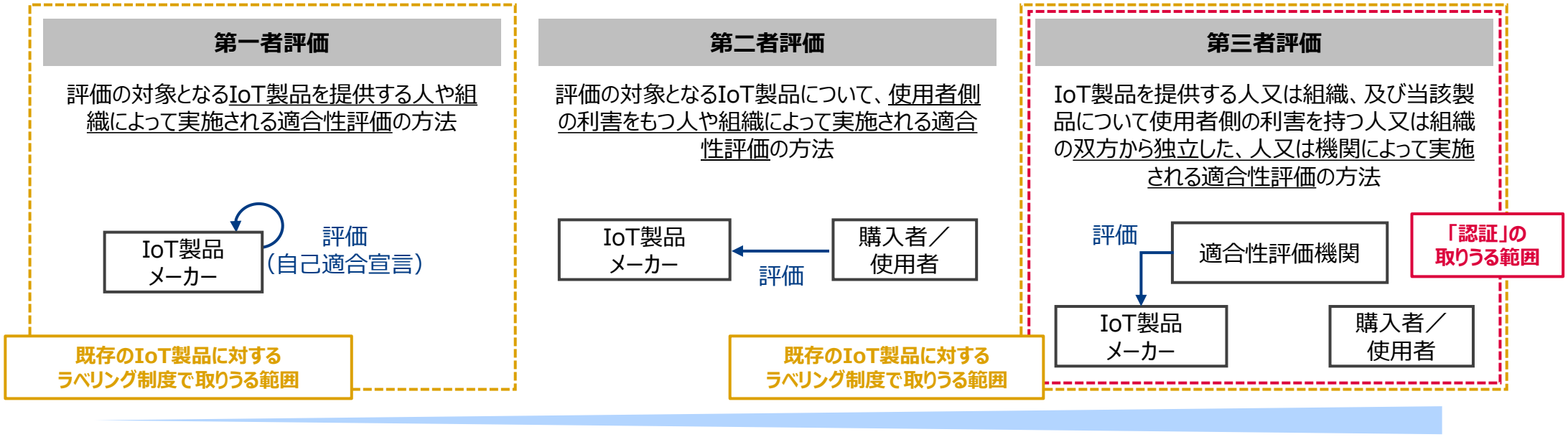
回	報告内容案	討議事項案
有識者検討会①（本日）	【有識者によるプレゼン】 • IoT製品のセキュリティ対策に関する諸外国の規制・取組（NICT中尾委員） • パナソニックホールディングスにおける製品セキュリティの取組み（パナソニック中野委員） • CCDSサーティフィケーションプログラムの概要・国際的な動向（CCDS荻野様） • 適合性評価制度の概要（JQA大塚様） 【事務局資料】 • IoT製品のセキュリティ対策に関する背景 • IoT製品のセキュリティ対策に関する諸外国の取組 • IoT製品のセキュリティ対策に関する国内の取組の課題 • 討議事項	• どのようなIoT製品を対象とすべきか。 • どのような適合性評価基準を採用すべきか。 • どのようなスキームで適合性評価を行うべきか。 • 諸外国とはどのような国々と、どのような共通認識を醸成していくべきか。
有識者検討会②（2022年12月～2023年1月頃）	【事務局資料】 • 第一回検討会を踏まえた対象製品の考え方 • 第一回検討会を踏まえた運用主体の考え方 • 第一回検討会を踏まえた評価基準・適合性評価方法の考え方 • 第一回検討会を踏まえた諸外国との連携の考え方 • 討議事項	• 適合性評価を受けた製品をどのように可視化すべきか。 • 適合性評価機関をどのように認定すべきか。
有識者検討会③（2023年2月頃）	【事務局資料】 • 第一回検討会・第二回検討会を踏まえた適合性評価制度構築に関する中間報告案	• 国内におけるIoT製品に対するセキュリティ適合性評価をどのように位置づけ、制度化すべきか。（義務化/任意）

Copyright © Mitsubishi Research Institute

【参考】適合性評価方法の区分

- ISO/IEC 17000:2004 [JIS Q 17000:2005] の定義に拠れば、「適合性評価（Conformity Assessment）」とは、製品、プロセス、システム、要員又は機関に関する規定要求事項が満たされていることの実証を意味する。
  - 適合性評価活動は、第一者評価・第二者評価・第三者評価の3つの評価方法に区分され、規定要求事項の充足が実証されたという表明の発行を「証明（Attestation）」という。
  - 「認証 (Certification) 」とは、製品、プロセス、システム又は要員に関する第三者証明を意味する。また、「認定 (Accreditation)」とは、適合性評価機関に関し、特定の適合性評価実務を行う能力を公式に実証したことを伝える第三者証明を意味する。
- 諸外国で開始しているIoT製品に対するセキュリティラベリングは適合性評価の一つであり、NISTの文書に拠れば、製品に対する技術要件に適合していることを単独もしくは複数の方法で評価し、何らかのラベルを付与することをいう。

適合性評価方法の3つの区分



出所） ISO/IEC 17000:2004 [JIS Q 17000:2005] https://www.jisc.go.jp/app/jis/general/GnrJISSearch.html
NIST, Recommended Criteria for Cybersecurity Labeling for Consumer Internet of Things (IoT) Products
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02042022-2.pdf

Copyright © Mitsubishi Research Institute

参考資料

- A. IoT製品に対するセキュリティラベルが消費者に与える影響に関する調査結果
- B. 国内企業におけるセキュリティラベリング制度のニーズに関する調査結果

Copyright © Mitsubishi Research Institute

豪州BETAの調査結果によれば、セキュリティラベルが付与されたIoT製品は、付与されていない製品よりも13～19%多く選定された。

- 2021年、BETA（豪州政府行動経済学チーム）はオーストラリア国民6,000人を対象に、オンラインショッピングにおけるIoT製品のセキュリティラベルの有効性に関する調査を実施した。
- 調査では、3種類のセキュリティラベル（有効期限のテキスト、有効期限のテキスト＋アイコン、レベル分けされた盾アイコン）を対象に、**種類ごと効果の差異、セキュリティレベルごとの効果の差異、ラベル付与によるWTP（支払意思額）への影響等が分析**された。
- 調査の結果、ラベルが付与されたIoT製品は、付与されていない製品よりも、**製品選定率が13～19%増加した**。
- 種類別の比較結果について、**3種類のラベルの中で最も高い選定率となったのは人目につきやすい盾アイコンのラベル**であった。

調査で使用した3種類のセキュリティラベル及び製品選定増加率

	①有効期限のテキストのみ	②有効期限のテキスト＋アイコン	③レベル分けされた盾アイコン
ラベル無しと比較した場合の製品選定の増加率	13.4%	13.9%	**18.8%**

レベル分けされた盾アイコンが、消費者に最も選定された

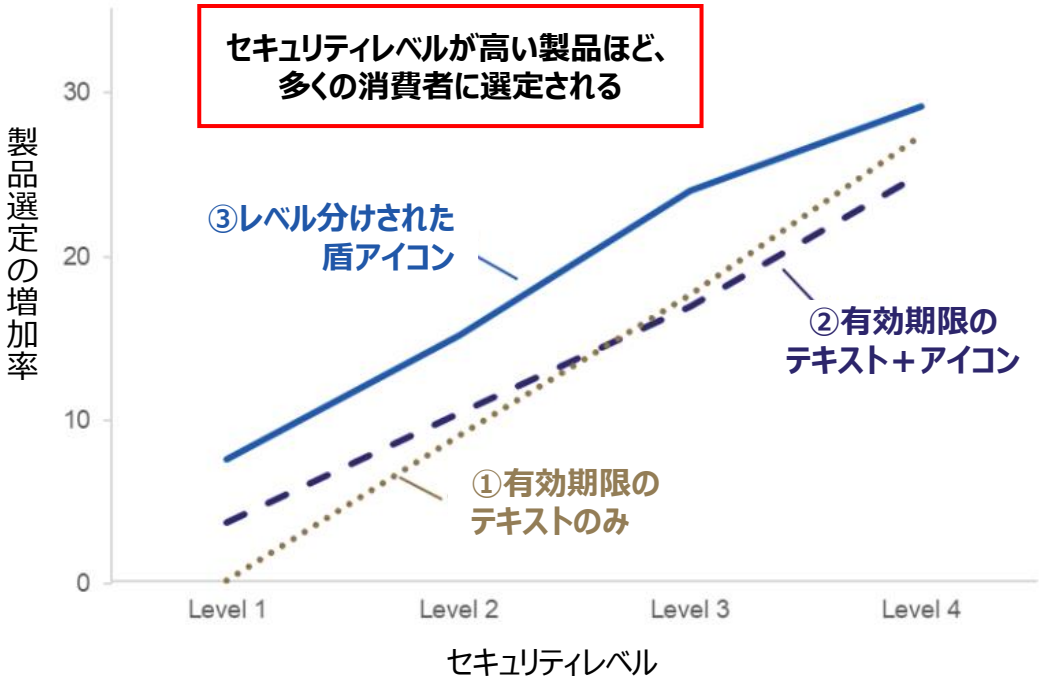
出所）BETA、Helping consumers choose cyber secure smart devices（March 2022）に基づき三菱総合研究所作成
https://behavioraleconomics.pmc.gov.au/sites/default/files/projects/beta-report-cyber-security-labels.pdf

Copyright © Mitsubishi Research Institute

消費者はセキュリティレベルが高いことを示すラベルが付与された製品を選ぶ傾向にある。また、ラベルが付与されている製品に多くの金額を支払う傾向にある。

- セキュリティレベルごと比較結果について、**セキュリティレベルが高いことを示すラベルの方が高い確率で選定された**。
- また、ラベルが付与されていることで消費者による製品に対するWTP（支払意思額）が増加することが確認され、**ラベルが付与されている製品に多くの金額を支払う傾向にある**ことが明らかとなった。
- なお、セキュリティラベルの意味を理解できていない消費者も確認されたため、**ラベルに関する解釈や使用方法に関する説明資料を準備**することが有効であることが示唆された。

各セキュリティレベルにおける製品選択の増加率（%）



ラベルが付与された製品に対する追加WTP（支払意思額）

製品類型	製品価格	追加WTP
スマートTV	$1,000 - $1,800	$322 - $377
スマートウォッチ	$420 - $720	$104 - $123
ホームハブ	$125 - $255	$53 - $60
スマート照明	$30 - $53	$8 - $10

消費者はラベルが付与された製品に対して、より多くの金額を支払う傾向にある

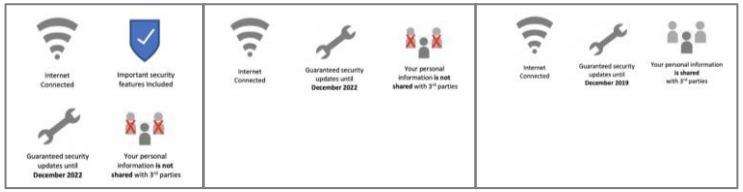
出所）BETA、Helping consumers choose cyber secure smart devices（March 2022）に基づき三菱総合研究所作成
https://behavioraleconomics.pmc.gov.au/sites/default/files/projects/beta-report-cyber-security-labels.pdf

Copyright © Mitsubishi Research Institute

UCLの調査結果によれば、セキュリティラベルが付与されたIoT製品のほとんどは、付与されていない製品よりも多く消費者によって選定された。

- 2019年、UCL（University College London）がイギリスの成人約3,000人を対象に、セキュリティラベルがIoT製品の購買意思にどのような影響を与えるかを調査した。
- 調査では、3種類のセキュリティラベル（情報ラベル、承認シール、等級付けラベル）を対象に、**種類ごと効果の差異、ラベル付与によるWTP（支払意思額）への影響、ラベル付与による消費者購買行動への定性的影響等が分析**された。
- 調査の結果、一部のラベルを除き、**ラベルが付与されたIoT製品は、付与されていない製品よりも製品選定率が増加**した。
- 種類別の比較結果について、**3種類のラベルの中で最も高い選定率となったのは最上位の情報ラベル**であった。

調査で使用した3種類のセキュリティラベル及び製品選定増加率

	情報ラベル（製品に関する情報＋アイコン）			承認シール	等級付けラベル		
							
	情報ラベル++ (製品が優れた機能とセキュリティ機能を有することの説明)	情報ラベル+ (製品が優れた機能を有することの説明)	情報ラベル- (製品が優れていない機能を有することの説明)		等級A (最もレベルが高い)	等級D (レベルが中程度)	等級G (最もレベルが低い)
ラベル無しと比較した場合の製品選定のオッズ比※	**5.46**	5.21	2.09	3.09	3.56	2.22	0.84

製品が優れた機能とセキュリティ機能を有することを説明する「情報ラベル++」が、消費者に最も選定された

出所）UCL、The impact of IoT security labelling on consumer product choice and willingness to payに基づき三菱総合研究所作成
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800

※:オッズ比が1以上の場合は消費者の選定率が高いこと、1以下の場合は選定率が低いことを意味する。

Copyright © Mitsubishi Research Institute

参加者は殆どのセキュリティラベルについて、付与された製品により多くの金額を支払う意思を持っており、さらに「製品の比較が容易になるため、購入の意思決定に役立つ」と考えていた。

- 等級Gラベルを除き、ラベルが付与されていることで、**製品に対するWTP（支払意思額）が増加する**ことが確認された。特に、**最上位の情報ラベルが付与された製品に対するWTPが最も高かった**。
- 製品区分別で比較すると、**多くの消費者がセキュリティ対策を懸念する防犯カメラにおけるWTPの増加率が最も高かった**。
- ラベルが付与されていることで、**消費者における製品購入時の意思決定が容易となり、また、製品の比較が容易となった**。この傾向は、**特に情報ラベルと等級付けラベルにおいて顕著**であった。
- また、ラベルの影響力を高めるために**デザインや配置箇所を検討する必要**があるほか、**ラベルが示す情報に関するマニュアルの必要性**も示唆された。

ラベルが付与された製品に対する追加WTP（支払意思額）

製品区分	製品価格	追加WTPの平均	情報ラベル++の追加WTP
防犯カメラ	£99.99	£33.60	£42.23
	-	33.6%	42.2%
スマートテレビ	£350.99	£65.71	£90.95
	-	18.7%	25.9%
ウェアラブル端末	£69.99	£19.03	£25.01
	-	27.2%	35.7%
サーモスタット	£159.99	£35.76	£48.91
	-	22.4%	30.6%

- **消費者はラベルが付与された製品に対して、より多くの金額を支払う傾向にある**
- **特に、情報ラベル++のWTPは他ラベルよりも高い**

ラベリングに関する参加者の嗜好平均点※

参加者への質問	情報ラベル			承認シールラベル	等級付けラベル		
	++	+	-		等級A	等級D	等級G
製品購入時にラベルは役立つか	5.90	5.74	5.65	5.09	5.60	5.21	5.43
ラベルにより製品比較が容易になるか	5.92	5.78	5.77	5.01	5.88	5.50	5.65

- **ラベルが付与されていることで、消費者における製品購入時の意思決定が容易となるほか、製品の比較が容易となる**
- **この傾向は情報ラベルと等級付けラベルにおいて顕著である。**

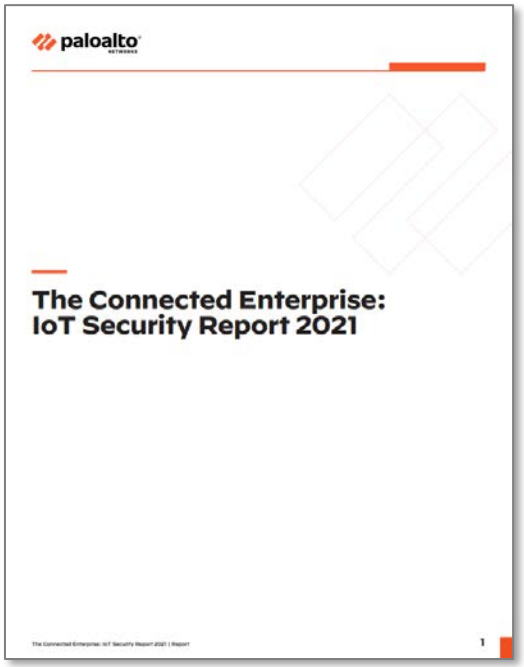
出所）UCL、The impact of IoT security labelling on consumer product choice and willingness to payに基づき三菱総合研究所作成
https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0227800

※：各質問にどの程度同意するかを、「1:強く同意しない」から「7:強く同意する」の7段階で評価。

Copyright © Mitsubishi Research Institute

パロアルトネットワーク株式会社の調査結果では、国内企業において、IoT製品に対するセキュリティラベルを求める回答が多く挙げられた。

- 2021年にパロアルトネットワーク株式会社がグローバルのIoTユーザー企業1,900社を対象に実施した調査において、「IoT製品の増加に対して、国や業界の規制が追いついていない」と回答した企業は7割を超えた。（日本：72%、グローバル：72%）
- この現状に対する具体的な方策に関して、グローバルの企業では、グローバルでのIoTセキュリティ基準の策定を求める企業が多く存在した一方で、**国内企業では、IoT製品のプライバシー・セキュリティに対する取組に関する情報を含むセキュリティラベルをメーカーに義務づけることを求める企業が最も多く、ラベリング制度に関する一定のニーズがある**ことが確認できる。



- 北米、EMEA（ヨーロッパ、中東、アフリカ）、JAPAC（日本、アジア太平洋地域）の19の国と地域における、従業員1,000人以上の企業に所属するIT部門の意思決定者1,900人に対する調査。
- ユーザー企業の7割以上が、IoT機器の増加に法・業界規制が追いついていないと回答。
- グローバルの企業では、グローバルでのIoTセキュリティ基準の策定を求める企業が多く存在した。
- 国内企業では、IoT製品のプライバシー・セキュリティに対する取組に関する情報を含むセキュリティラベルをメーカーに義務づけることを求める企業が最も多い。

出所）パロアルトネットワーク株式会社、日本を含むグローバルにおけるIoTセキュリティ実態調査を公開：7割以上がIoT機器の増加に法・業界規制が追いついていないと回答
https://www.paloaltonetworks.jp/company/press/2021/palo-alto-networks-releases-global-iot-security-survey

Copyright © Mitsubishi Research Institute