待ったなし！IoT機器のサイバーセキュリティ対策を解説
～JC-STARラベリング制度、欧州CRA適合に向けた製品設計、開発、運用に向けて～

・セキュリティクリアランス制度の動向
・各国のラベリング制度
・JC-STARとCRA

公開

会社概要／サイバートラスト 株式会社

商号
サイバートラスト株式会社

本社
〒106-0032
東京都港区赤坂 1 丁目 12 番 32 号
アーク森ビル 31 階

設立
2000年6月1日

資本金
806,465,000 円 （2023年3月31日現在）

主な株主
大日本印刷株式会社
SBテクノロジー株式会社
株式会社オービックビジネスコンサルタント
みずほ証券株式会社
株式会社エヌ・ティ・ティ・データ
セコム株式会社
株式会社日立製作所
THE BANK OF NEWYORK 133595
（2023年3月31日現在）

日本初の商用電子認証局として、多くのWebサイトにご採用いただいております。
20年以上にわたり電子認証サービスを提供しているセキュリティ企業です。
「信頼とともに」。サイバートラストは、IT インフラに関わる、
専門性・中立性の高い技術で、安心・安全な社会を実現します。

安心・安全なデジタル社会を実現する トラストサービス を提供

公開

講師紹介

松本 義和（まつもと よしかず）

1975年9月　静岡県静岡市生まれ。
電子認証分野の大手であるサイバートラスト社の Principal Security Architect として、
医療・通信・金融といった重要インフラの情報セキュリティ対策をメインに、
暗号と認証の技術を背景に幅広い分野に従事。
大小を問わず、広く企業や行政の情報セキュリティ施策の策定に参画している。

■サイバートラスト株式会社
プリンシパル セキュリティ アーキテクト

■日本RA株式会社
業務執行役員
最高技術責任者CTO

■中央大学研究開発機構／横浜市立大学 医学部
客員研究員：量子暗号分野

■専門分野
・情報セキュリティコンサルタント
・PKIコンサルタント
・セキュアIoTプラットフォーム協議会　標準化部会　副座長
・金融／医療分野セキュリティトレーナー
・医療情報セキュリティアドバイザ
・放射線部門医療情報システムアドバイザ
・ISO/TS 11633 （RemoteServiceSecurity）策定主査
・MEDIS-DC 監査証跡検討委員会代表委員
・医療情報ネットワーク基盤検討会　認証サブWGメンバ

公開

セキュリティクリアランス：米国の政府と民間

米国の民間事業者等に対するセキュリティクリアランス制度の概要

【米国　民間企業のセキュリティクリアランス制度】

・国家の防衛、重要インフラの防護及びその他の国家安全保障に関する事業の実施には、**民間企業の協力が欠かせない**

・防衛装備にしろ、サイバー関連設備にしろ、これらの全てを国営企業が製造・運営することはできない。このため、これらの装備等の製造等などあたっては、**国の機密情報を民間企業と共有して業務を遂行してもらう必要がある**

・民間企業は、国とは別個の法人であり、また、通常は株式会社制度等により運営されており、国が支配しているわけではない

・このため、政府とは別のセキュリティクリアランス制度が設けられている

【民生品に対してはCUIとUIを分けて管理監督を実施】

・**SP800-171**と**53**とを区別し、製品やサービスで取り扱う情報の機密度により要件を整理している

・**国内（米国）CMMC2.0基準への準拠が調達要件**。**国外輸入製品についても同様の審査基準を設ける方向**。

※CMMC2.0：サイバーセキュリティ成熟度モデル認証（Cybersecurity Maturity Model Certification、以下CMMC）は、米国国防総省（Department of Defense）が開発したサイバーセキュリティの認証フレームワーク。この認証制度は、防衛産業基盤を担う企業の連邦契約情報やCUI※をサイバー攻撃や盗用から保護することを目的としている。

取り扱う情報のレベルに応じ、製造業への展開を図っています

公開

セキュリティクリアランス：日本政府の動き①

民生品におけるCMMC2.0への準拠

【防衛装備庁の動き】

・防衛産業サイバーセキュリティ基準と同じく**NIST SP800-171に基づいて**おり、サプライチェーン全体におけるサイバーセキュリティ確保のための最新基準のCMMCへの準拠性を求める　※輸入品について言及

・2025年に予定されている本格的な実装が開始されれば、日本企業からの防衛品の調達も対象

・最新のCMMC2.0は3段階のレベル評価となっている

【認証取得の条件】（レベル2とレベル3）

・**CMMC2.0の認証取得には適切な文書作成が必要**

・準拠に必要なポリシー、手順、リスク管理計画を作成し、審査プロセスをスムーズに進めるための準備が重要。

→SP800-171の審査項目が適応される。

製造業を通じ、米国との連携を図っています

公開

セキュリティクリアランス：日本政府の動き②

「重要経済安全情報保護活用法」の成立　※令和６年５月10日に成立し、同月17日に公布

【日本におけるセキュリティクリアランスの考え方】

・**政府が保有する安全保障上重要な情報**として指定された情報に対し、**アクセスする必要がある者**のうち、**情報を漏らすおそれがないという信頼性を確認した者**の中で取り扱うとする制度

・日本では、セキュリティクリアランス制度を規定している法律として、**特定秘密保護法**と**重要経済安保情報保護活用法**がある

・民間事業者に対しては、**施設・組織の信頼性**をセキュリティクリアランスの項目として考える

【重要経済安保情報 ∩ 重要経済基盤保護情報】

・重要経済基盤とは、**公共サービスの提供体制または重要な物資**の供給網を指す

・国民の生存に必要不可欠である重要な物資（プログラムを含む）、広くわが国の国民生活・経済活動が依拠し、または依拠することが見込まれる**重要な物資（プログラムを含む）**の供給網

【解釈】

・セキュリティ・クリアランス制度の対象企業は、重要経済安保情報にアクセスする必要がある民間企業。具体的には、電力、通信、鉄道、金融などの重要インフラ事業者や、半導体、AI、量子、バイオテクノロジーなどの重要物資・先端技術を扱う企業、そしてそれらを取り扱うサプライチェーン関連企業が想定される

・適合事業者の認定では、当該企業の**意思決定に外国の所有・支配・影響がないか**を確認される。

・**重要経済安全情報を取り扱うためには、厳格な情報セキュリティマネジメントが不可欠であり、CSFや各種SP800ｓが参考となる**。

公開

【参照】セキュリティクリアランスと製造業について

https://www.cybertrust.co.jp/blog/security/icam-security-clearance.html

公開

攻撃主体者は誰か？

脅威主体（攻撃者）は単なる愉快犯ではなく、金銭・政治・テロ目的が中心になってきています。

<サイバー攻撃者の例>

- **金銭目的の犯罪者、愉快犯**
- **ハクティビスト集団**
- **国家が関与・支援するサイバー攻撃集団（APTグループ）**

APTグループの特徴：

政治的・軍事的な国家目標を達成するため、軍や情報機関の作戦として攻撃を実行

- **▶重要インフラの破壊、情報操作、諜報活動など、**
- **▶任務達成のため、コスト度外視で執ような攻撃を継続**
- **▶犯罪者や民間のハッカーを外部の協力者・代理人として使う場合もある**

欧米政府によって特定･公表されたAPT集団と国家機関のつながり

APTの識別名（カッコは別名の例）	関連する国家機関 ※欧米政府の公表に準拠	関与したサイバー攻撃事案、標的の例
APT1（Comment Panda）	中国人民解放軍	● 原子力メーカーなど在米６組織からの情報窃取（2006～2014年）
APT41（Wicked Panda）	中国国家安全部	● オンラインゲーム会社を狙った金銭目的の攻撃（2009～2015年頃） ● 化学・ハイテク産業を狙った技術情報の窃取（2015年頃～）
APT28（Fancy Bear）	ロシア連邦軍参謀本部情報総局（GRU）	● ドイツ連邦議会を狙った情報窃取（2015年） ● 米国大統領選挙を狙った情報窃取・暴露（2016年） ● 反ドーピング機関を狙った情報窃取・暴露（2016年）
Sandworm（BlackEnergy）	ロシア連邦軍参謀本部情報総局（GRU）	● ウクライナ大規模停電（2015、2016年） ● 韓国・平昌冬季大会の妨害（2018年）
Lazarus（APT38）	北朝鮮偵察総局	● ソニーピクチャーズのシステム破壊・情報窃取（2014年） ● バングラデシュ銀行からの約8,100万ドル窃取（2016年） ● ランサムウェア「WannaCry」（2017年）

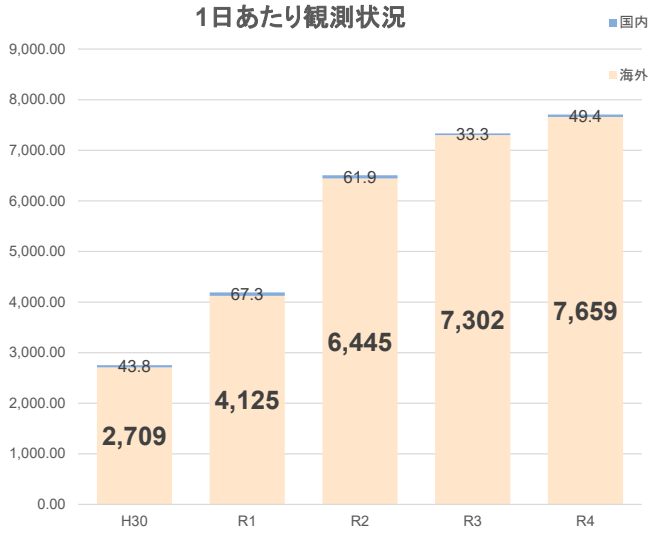
出典：サイバー空間における脅威の概況：公安調査庁

公開

ますます活発になる日本国内における偵察行動

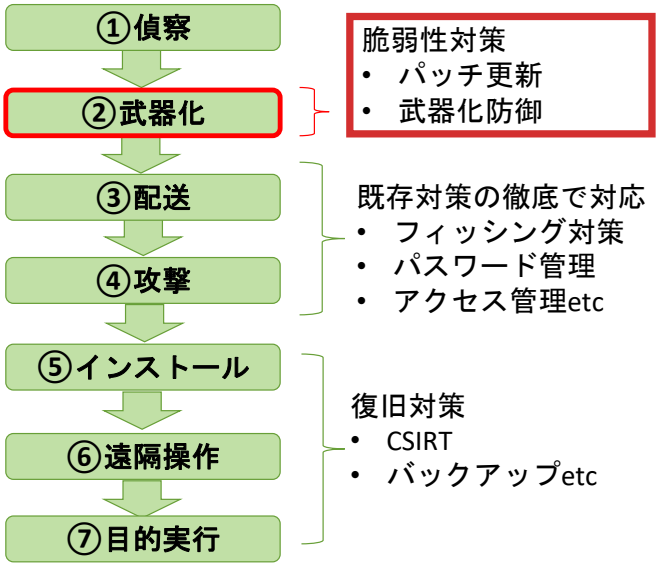
cybertrust

サイバー空間におけるぜい弱性探索行為等の
1日あたり観測状況



令和４年におけるサイバー空間をめぐる脅威の情勢等について

サイバー攻撃プロセス（キル・チェーン）



脆弱性対策が最も有効な水際対策

公開

欧米英における主なセキュリティ標準／規制（2025年11月時点）

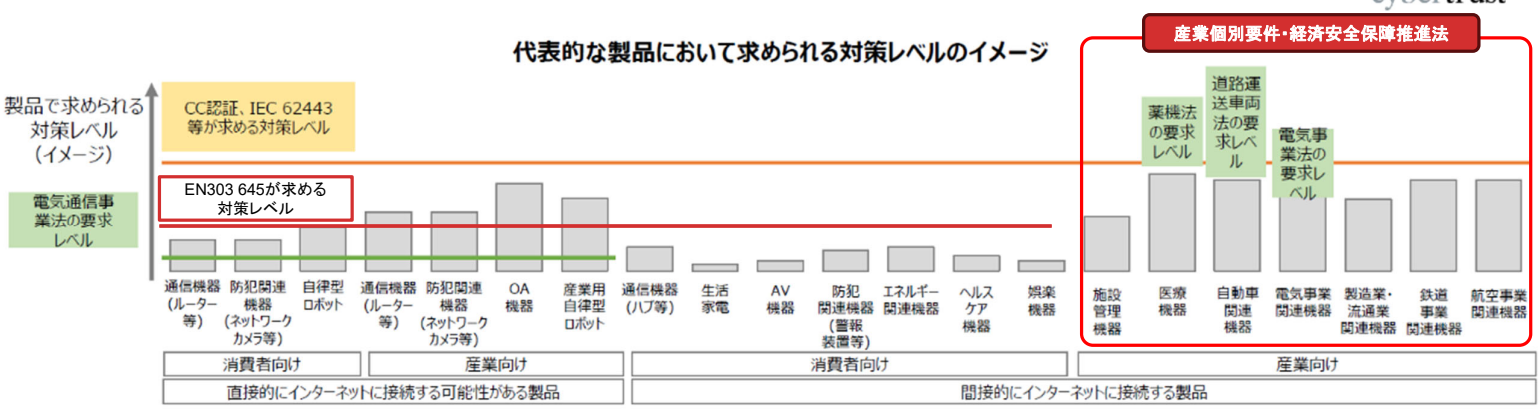
cybertrust

主要各国にてサイバーセキュリティ標準／規制が策定され、相互承認する方向（各国共通規定）

国、地域	標準／規制	主な対象	運用開始	備考
	PSTI 法	消費者向け、且つ インターネット接続可能な （有線/無線）製品	2024年4月29日	ETSI EN 303 645
	サイバーレジリエンス法 （CRA）	デジタル要素を含む ソフトウェア、ハードウェア製品	2027年12月全面施行	ETSI EN303 645 IEC62443
	NIST SP800s	デジタル要素を含む ソフトウェア、ハードウェア製品	-	NIST SP800-171 NIST SP800-53 NIST SP800-207
	JC-STAR	消費者機器向け☆1から重要インフラ☆4まで 4段階に分けて制度設計	2025年3月～☆1開始 2025年内～☆2以上順次開始	英PSTIと相互承認 2025年11月

公開

民生品・産業製品それぞれのセキュリティ標準規格の対策レベル



国際協調で進むサイバーセキュリティ規制規制（各国のラベリング制度）

- **日本：JC-STAR（EN303 645相当）★１が運用スタート**
- **米国： NIST SP800-171･53 、**Cyber Trust Mark（NIST SP800-213 / NIST IR 8259）
- **欧州：CRA（EN303 645 / IEC 62443） ※罰則規定あり**

各国とも同等のサイバーセキュリティ規制を準備中
欧州のCRAが最も厳しい規制になると考えられる。

公開

日本国内の動向

公開

IoTサイバーセキュリティ規制とその影響

日本経済新聞

トップ　朝刊・夕刊　LIVE　My二ユース

IoTのサイバー対策、経産省が認定制度　公共調達の要件

経済　＋フォローする

2024年3月12日 17:04 [有料会員限定記事]

Think!　佐藤一郎さんの投稿

産業ロボットなどネットにつながっているIoTのサイバー対策が急務になっている

経済産業省は家電などあらゆるモノがネットにつながる「IoT」機器のサイバー対策を認定する新たな制度を2024年度から始める。国内のサイバー被害の4割を占める

日本経済新聞

トップ　朝刊・夕刊　LIVE　My二ユース

企業のサイバー対策、5段階で格付け　経産省25年度にも

情報通信・ネット　＋フォローする

2024年4月4日 5:00 (2024年4月4日 19:19更新) [会員限定記事]

経済産業省は企業格付け制度を通じ、サイバー攻撃の対応力を高める

経済産業省は企業のサイバー攻撃対策を格付けする制度を2025年度にも始める。各社の対策を5段階で評価し、取引先がどこまで対策をとれているかが分かるようにす

公開

政府統一基準群のガイドラインへの反映

- 2024年7月に公開された政府統一基準群のガイドラインに、今後の本制度活用を反映した。

「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）の一部改定（令和６年７月）」（抜粋）

4.3　機器等の調達

4.3.1　機器等の調達

（解説）

- **基本対策事項** 4.3.1(1)-2「必要なセキュリティ機能が適切に実装されていること」について

必要なセキュリティ対策を実施するためには、機器等に必要なセキュリティ機能が適切に実装されていることが求められる。例えば、IoT 機器等に必要なセキュリティ機能の具体例としては、少なくとも以下の内容が考えられる。

- 容易に推測可能な初期パスワードの設定禁止
- 主体認証のネットワークを介した総当たり攻撃対策
- 容易に行えるソフトウェアの脆弱性対策（アップデート等）
- 機器内のセキュリティパラメータの保護
- 安全な通信の確保
- 利用者が作成したデータの容易な消去
- 利用しない機能や通信ポートの無効化

機器等に必要な情報セキュリティ対策が適切に実装されていることを確認するには、機器等の仕様書の確認、製造者へのヒアリングの実施のほか、次の「IoT 製品のセキュリティ適合性評価制度」の活用が考えられる。

本制度☆１適合基準相当の内容

IoT 機器等に対する要求すべきセキュリティ要件に関連して、2024 年度中（2025 年３月頃）に「IoT 製品に対するセキュリティ適合性評価制度」の☆１のラベル付与が開始される予定であり、今後の調達における活用が考えられる。☆１は機器等共通の最低限満たすべきセキュリティ項目を満たしていることを製造業者が自己で評価し、その適合性を宣言することで取得可能となるものである。☆１の取得を確認することで、上記に記載しているセキュリティ機能の実装状況の確認の代用とすることができる。

また同制度では、製品種別毎により高度なセキュリティ適合基準に対する評価を行う☆２（自己適合宣言）、☆３以上（第三者認証）が順次整備される予定である。制度整備の状況を踏まえつつ、2025 年度中に同制度の☆１以上を取得していることを機器等の選定基準に含めるとともに、以降も、☆２、☆３以上の対象機器の拡充に応じて選定基準への反映を順次行っていく予定である。

本制度の活用方針

情報システムの重要度に応じて「重要度：低」は☆１以上、「重要度：高～中」は少なくとも☆３以上の IoT 機器等を各機関等の選定基準に含めることの追加を検討している。なお、ラベル付与製品が普及する時期をめどに、政府機関等では求めるセキュリティ水準に応じたラベル付与製品の調達を必須化する方針である。

参考：経済産業省「IoT 製品のセキュリティ適合性評価制度構築方針」
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/index.html）

重要インフラ役務事業社から一般民間企業まで広く反映される

公開

経産省　IPA　JC-STAR

経済産業省が運用を開始したJC-STARは、共通的な物差しでIoT製品に具備されているセキュリティ機能を評価・可視化し、政府機関、民間企業から一般消費者まで、IoT製品の購入者・調達者が、本制度のラベルを確認することで、**自らが求めるセキュリティ水準の製品を容易に選択できるようにすること**を目的としています。現時点では★１が開始され、年内に★２以降が順次公開される予定です。

■今後、製造業者に求められること
- 自社製品の適用吟味
  →通信機能の有無
  →組み込み資材としての判断
  →消費者への対応
- 適合レベルの判断
- 認証取得に関するコスト算出　等

https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/20240823.html

公開

対象製品と適合性評価レベル

■対象製品

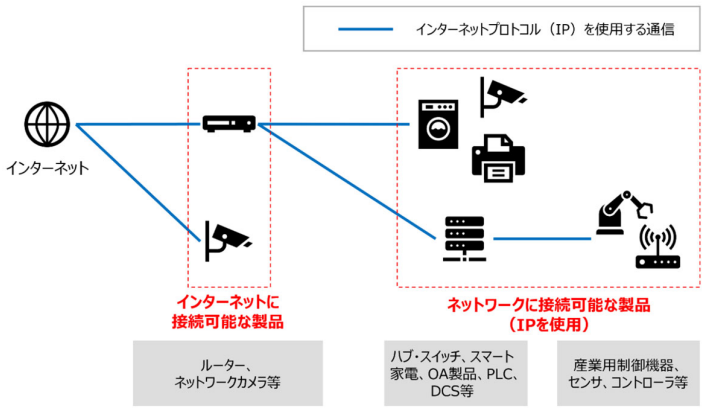


図 3.2-1　本制度の対象とする製品のイメージ

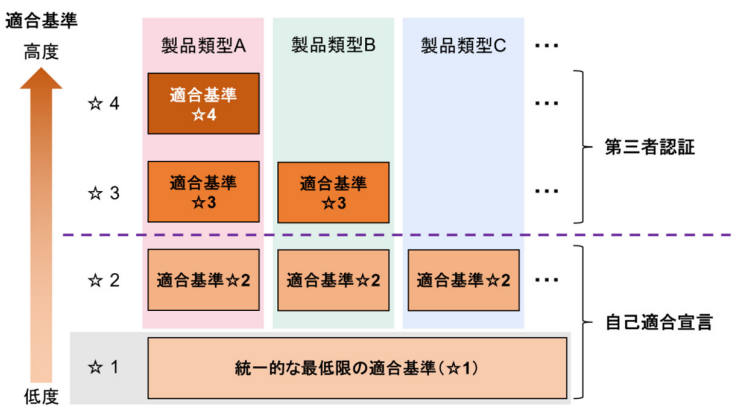


図 3.3-1　適合性評価レベルのイメージ図

出典: https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_cybersecurity/iot_security/pdf/20240315_1.pdf の P. 14,

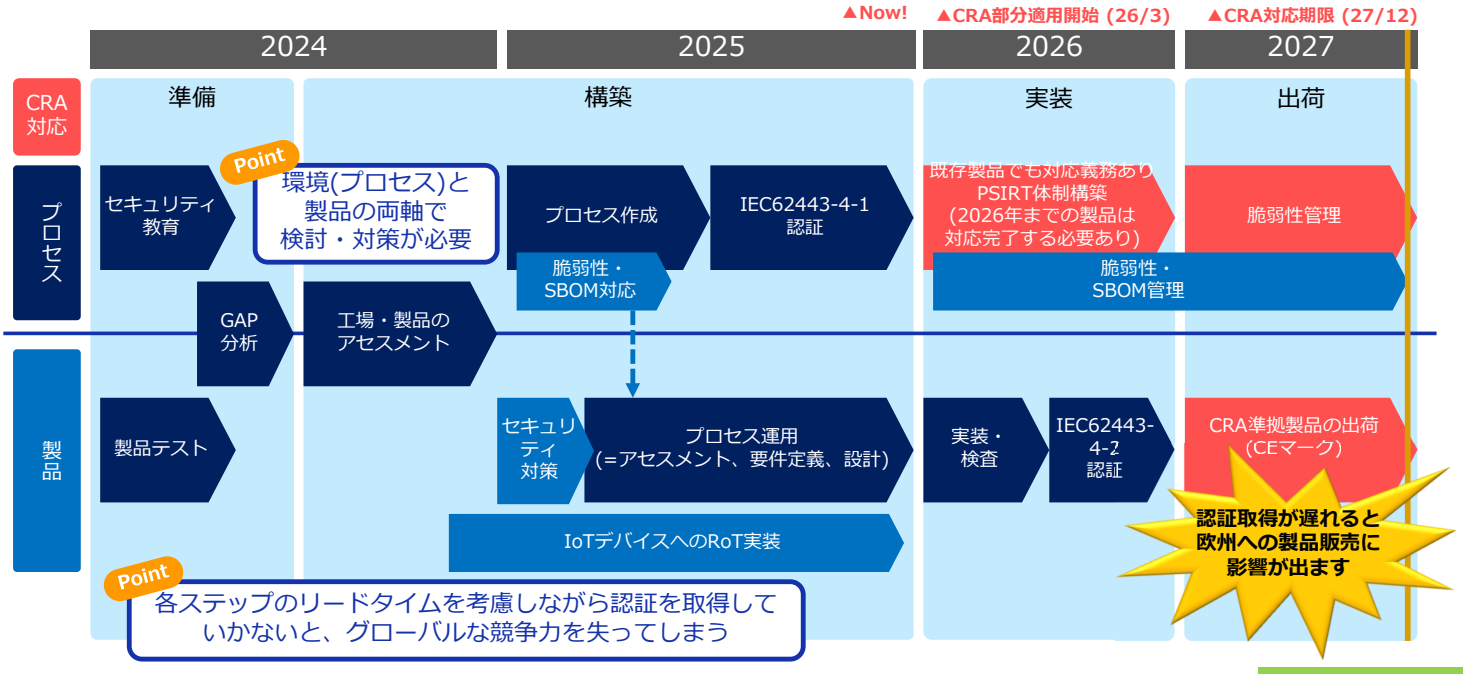
公開

サイバーレジリエンス法（CRA）による影響

公開

EUサイバーレジリエンス法による影響

EU CRA対応に要する工程と平均対応時間



公開

【参考】欧州CRA第13条　製造業者の義務

1. デジタル製品を市場に出す際、附属書Iの 1「セキュリティ特性要件」を遵守して設計・開発・製造 されていることを確認する。
2. サイバーセキュリティ上の**リスクアセスメントを実施**し、その結果を設計・開発・製造・配送・メンテナ ンスの際の考慮に入れる。
3. デジタル製品を市場に出す際、上記の**リスクアセスメントの結果を技術文書に含める**。
4. 第31条および付属書VIIに従って要求される技術文書には、本条第3項で言及されるサイバーセキュリティリスク評価を含める。
5. 第三者から提供された部品を使用する際は、その部品により製品のセキュリティリスクを高めないことを保証する。
6. 特定した脆弱性を報告・対処・修復する。対処のための変更は機械可読形式でコンポーネントの製造または保守を行う個人または団体と共有する。
7. デジタル製品に関する**サイバーセキュリティ観点の情報を体系的に文書化**する。
8. **サポート期間は5年間と製品の使用期限のうち短い方とし、期間内は製造業者は脆弱性に効果的に対処する**。製造業者は脆弱性開等に適切なポリシーや手続きを有する。
9. **製品の上市から10年間、またはサポート期間のいずれか長い方の期間、セキュリティアップデートを利用可能とする**。
10. 大幅な変更バージョンは付属書 I、パート II、ポイント (2) の必須要件に準拠すればよい。最新バージョンへは無料でアクセスでき、旧バージョンユーザーが環境調整コストなしで適用できること。
11. ユーザーが過去のバージョンおよびサポート外ソフトウェアの使用に伴うリスク情報にアクセスできるようにする。
12. 上市前に製造業者は技術文書を作成する。対応する適合性評価手続きを行い、適合性が実証された場合はCEマーキングを貼付する。
13. 上市後10年間、技術文書と（該当する場合は）EU適合性証明書を市場監視当局が自由に使えるように保管する。
14. 一連の製造の中で、適合性を維持するための手順が整備されていることを確認する。
15. 製品の個体識別のため型番、バッチ番号、シリアル番号などを付記する。
16. 製品に製造業者の名前、商標、郵便住所、電子メールアドレスなどのデジタル連絡先、ウェブサイトなどを表示する。
17. 脆弱性報告ための単一の連絡先を附属書 II に記載されているユーザーへの情報および指示に記載する。連絡先はユーザーが通信手段を選択できるようにし、手段を自動化ツールに限定してはならない。
18. 附属書 II に定めるユーザーへの情報および説明書を**紙または電子形式で添付**する。情報および説明書は10年間とサポート期間の長い方の期間保持し、オンライン提供の場合はアクセス可能とする。
19. 購入時に、第8項のサポート期間の終了日へアクセスできるようにする。可能であれば、製造業者はサポート期間の終了をユーザーに通知する。
20. **EU適合性証明書か簡易EU手企業宣言を提供する**。簡易宣言の場合は完全なEU適合宣言へのURLを提供する。
21. **上市後5年間と製品寿命の短い方の期間で附属書Iの 1「セキュリティ特性要件」を遵守しない場合、直ちに必要な是正措置を講じ製品の撤回またはリコールを行う**。
22. 市場監視当局からの要求に応じて製品の適合性を証明する情報・文書を提出する。
23. 操業を停止し義務を遵守できなくなる場合、操業停止前に市場監視当局やユーザに通知する。
24. 欧州委員会は実施法の中で、SBOMの形式と要素を指定することができる。
25. ADCO は製品のフリーソフトウェアおよびオープンソースソフトウェアへの依存度評価の実施を決定できる。市場監視当局は附属書I第II部ポイント(1)の SBOM 提供を要求できる。

設計前のリスクアセスメントの実施及び設計書への反映を文書化する必要がある。
製品寿命もしくは5年間は脆弱性処理要件を満たす必要がある。（PSIRT相当の対応が必須）

公開

【参考】欧州CRA第14条　製造業者の報告義務

1. **悪用されている脆弱性を認識した場合は第7項に従い CSIRT と ENISA に同時に通知する。**
2. **第1項の通知では以下を提出する。**
   (a) 脆弱性を認識してから24時間以内に早期警告通知
   (b) 脆弱性を認識してから72時間以内に、製品の一般情報、悪用の性質、講じられた・またはユーザーが講じられる是正・緩和措置を含む脆弱性通知
   (c) 是正措置または緩和措置が利用可能になってから14日以内に以下を含む最終報告書
      (i) 脆弱性の説明（その深刻度および影響を含む）
      (ii) 入手可能な場合、脆弱性を悪用した悪意のある行為者に関する情報
      (iii) 脆弱性修正のためのセキュリティアップデートまたはその他の是正措置に関する詳細
3. **製品のセキュリティに影響を与える重大なインシデントを認識した場合は第7項に従い CSIRT と ENISA に同時に通知する**
4. **第3項の通知では以下を提出する。**
   (a) インシデントを認識してから24時間以内に早期警告通知。違法または悪意のある行為により比企侵された疑いがあるかを含む
   (b) インシデントを認識してから72時間以内に、インシデントに関する一般情報と初期評価、講じられた・またはユーザーが講じられる是正・緩和措置を含むインシデント通知
5. **以下の場合インシデントは重大とみなす。**
   (a) 機密性の高いまたは重要なデータや機能の可用性、真正性、完全性、または機密性を保護する能力に悪影響を及ぼす可能性がある
   (b) ユーザーのネットワークおよび情報システムにおいて悪意のあるコードの導入または実行につながる可能性がある
6. **CSIRT は現在悪用されている脆弱性や重大なインシデントに関する中間レポートの提供を製造元に要求する場合がある。**
7. **第1項と第3項の通知は、第16条で規定する単一の報告プラットフォームを介して提出される。**
8. **積極的に悪用されている脆弱性または重大なインシデントを認識した場合、これらについてユーザーに通知する。**
9. **本法案発効日から12ヶ月以内に欧州委員会は第61条に委任行為を採択する。**
10. **欧州委員会は、通知された情報の種類、形式、手順を更に指定することができる。**

自社製品に対するサイバーセキュリティ・インシデントへの報告・対応・連絡を行う組織が求められる
（PSIRT相当の対応が必須）

公開

【参考】CRAで求められる要件と該当規格のマッピング

cybertrust

附属書Iの 1「セキュリティ特性要件」

1. リスクに基づいて適切なサイバーセキュリティを確保するよう設計・開発・生産されていること。
2. リスクベースアセスメントに基づいて、以下を満たすこと。
   - (a) 悪用可能な脆弱性が含まれないこと。
   - (b) 製品を元の状態にリセット可能である等、デフォルトで安全な設定となっていること。
   - (c) セキュリティアップデートにより脆弱性に対処できること。
   - (d) 適切な制御メカニズムにより不正アクセスからの保護が確保されていること。
   - (e) 最先端の暗号化などにより個人データ・その他のデータの機密性を保護すること。
   - (f) データやプログラムなどの完全性を許可されていない操作から保護し、破損についても報告すること。
   - (g) 必要なデータに限定して処理を行うこと。（データの最小化）
   - (h) DoS攻撃からの回復・緩和などの重要な可用性の機能を保護すること。
   - (i) 他の機器やネットワークからのサービスの可用性について自身への悪影響を最小化すること。
   - (j) 外部インターフェース等の攻撃対象領域を制限して設計・開発・製造されていること。
   - (k) インシデントの影響を軽減するように設計・開発・製造されているころ。
   - (l) アクセス、データ修正、サービス、機能などの内部活動を記録・監視し、セキュリティ情報を提供すること。
   - (m) ユーザーが全てのデータと設定を簡単に永久に削除できること。それら情報が転送可能な場合は安全に転送できること。

附属書Iの 2「脆弱性処理要件」・・・製造業者が満たすべき要件

1. 製品に含まれる脆弱性とコンポーネントを特定し、文書化すること。
   - 機械可読形式で一般的に使用されるSBOM作成（少なくとも最上位レベルの依存関係含む）を行うこと。
2. セキュリティアップデートの提供など、遅滞なく脆弱性に対処・緩和すること。
3. 効果的かつ定期的なテストとレビューを行うこと。
4. 修正された脆弱性について、情報の公開を行うこと。
5. 脆弱性開示ポリシーを導入し、実施すること。
6. 製品やサードパーティコンポーネントの潜在的な脆弱性に関する情報共有を行い、連絡先を提供すること。
7. 悪用可能な脆弱性が適時に修正・緩和されるように安全にアップデートを配布するメカニズムを提供すること。
8. セキュリティパッチや更新プログラムが遅滞なく無料で配布され、ユーザーへの助言メッセージも添付すること。

公開

CRAが及ぼす影響（セキュリティ特性要件/脆弱性処理要件）

cybertrust

出荷前技術開発 → 出荷後技術対応 → 出荷後運用プロセス

CRA処理要件

セキュリティ特性要件	脆弱性対応	脆弱性管理
リスクアセスメントに基づいて適切なサイバーセキュリティを確保する設計・開発・生産・検査	脆弱性脅威度に基づき、セキュリティパッチの開発と製品への対応	SBOMと脆弱性対応プロセスの整備 ・脆弱性情報の公開及び修正を行う脆弱性開示ポリシーを導入し実施 ・製品やサードパーティコンポーネントの潜在的脆弱性に関する情報共有

対象部門

- 運用部門：PSIRT（メーカ側）/CSIRT（ユーザ側）部門
- 技術開発部門

SBOM 共通言語

CRAが要件とする範囲：EN303 645（カテゴリにより項目異なる見込み）SBOM生成管理、脆弱性対応

CRAでは出荷前の設計開発から販売終了まで一貫した対応が求められる
開発部門のみならず全社的な対応が必要

公開

SIOTP協議会：「セキュアIoT認定プログラム」について

IoTの脆弱性に起因するセキュリティ事故を未然に防ぐために、大企業から中堅・中小企業にいたるまで、IoTシステムの製造事業者、運営事業者に対する脆弱性検査の普及促進が重要だと考えます。

そこでセキュアIoT協議会では、検査を受ける動機づけとなる「認定」を付加価値要素とする、セキュリティ検査の仕組み「セキュアIoTプログラム」をリリースし、我が国における脆弱性検査の普及に貢献します。

今回のプログラムでは、IoTシステムの脆弱性の有無を確認する「脆弱性検査およびIoTセキュリティ検査」に加えて、その検査結果をもとに特に重要と考える以下の3項目において国際標準(IEC62443)への適合性を確認する「セキュアIoT認定」を組合わせて提供します。

【検査ポイント】

■ライフサイクル管理

- **真正性の担保と識別 (耐タンパ：鍵管理)**
- **認証と識別 (設計・製造、利用、廃棄、リサイクル)**
- **セキュアアップデート (OTA：Over The Air)**

セキュアIoT認定

本プログラムでは、産業用システムや業務システムを中心に、最終的なIoT機器だけではなく、IoT機器を構成する部品やソフトウェア、システムも認定対象とします。

公開

SIOTP協議会：「セキュアIoT認定プログラム」の構成

セキュアIoTプログラム

IoTセキュリティ検査

●検査項目：ライフサイクル管理
- 真正性の担保 (耐タンパ：鍵管理)
- 認証と識別
- セキュアアップデート (OTA)

✓ 対象となるIoTシステムに求められるセキュリティ強度によりclass1～4の基準を選択し、適合する検査を実施*

脆弱性検査

- ソースコード解析
- ファームウェア解析
- ネットワークスキャン
- 既知脆弱性診断　など

セキュアIoT認定

●認定基準

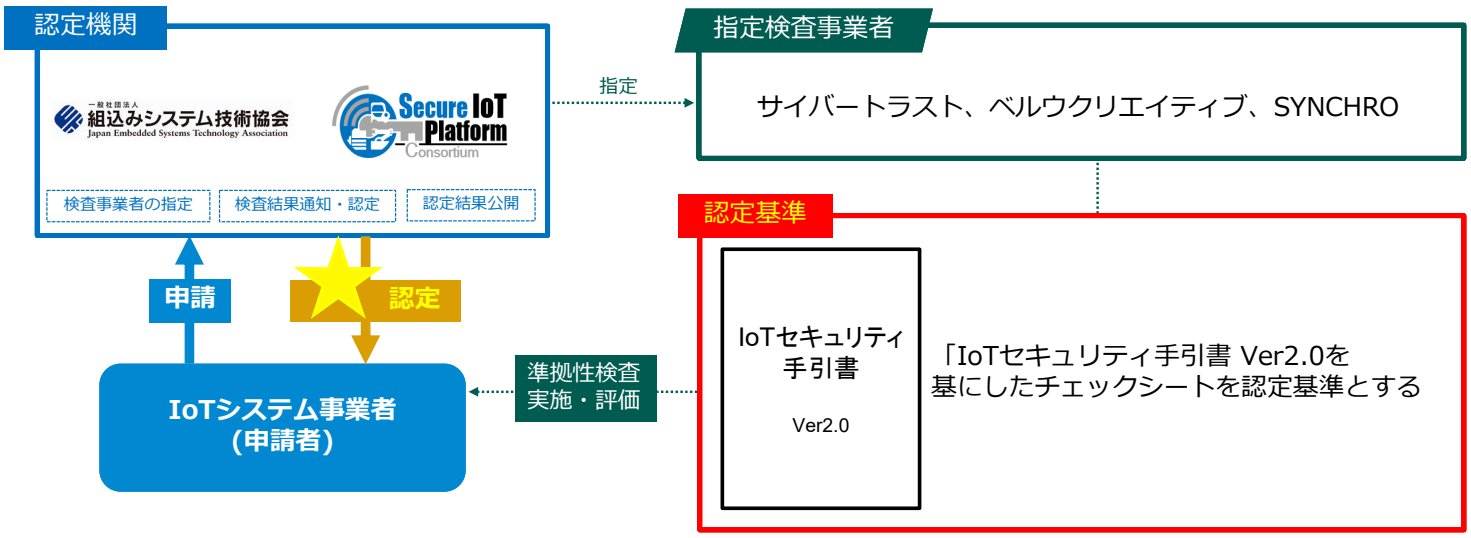
✓ 一定基準の「脆弱性検査」をクリア
- Bronze: 80%以上
- Silver: 90%以上
- Gold: 95%以上

✓ 加えてGoldの場合は、該当するclassの「IoTセキュリティ検査」要件クリア

＊ 認定対象の利用用途や目的によって適切なclassを認定機関が決定します。

公開

SIOTP協議会：「セキュアIoT認定プログラム」の認定スキーム



気軽にお問合せください。

公開

ご清聴ありがとうございます

公開