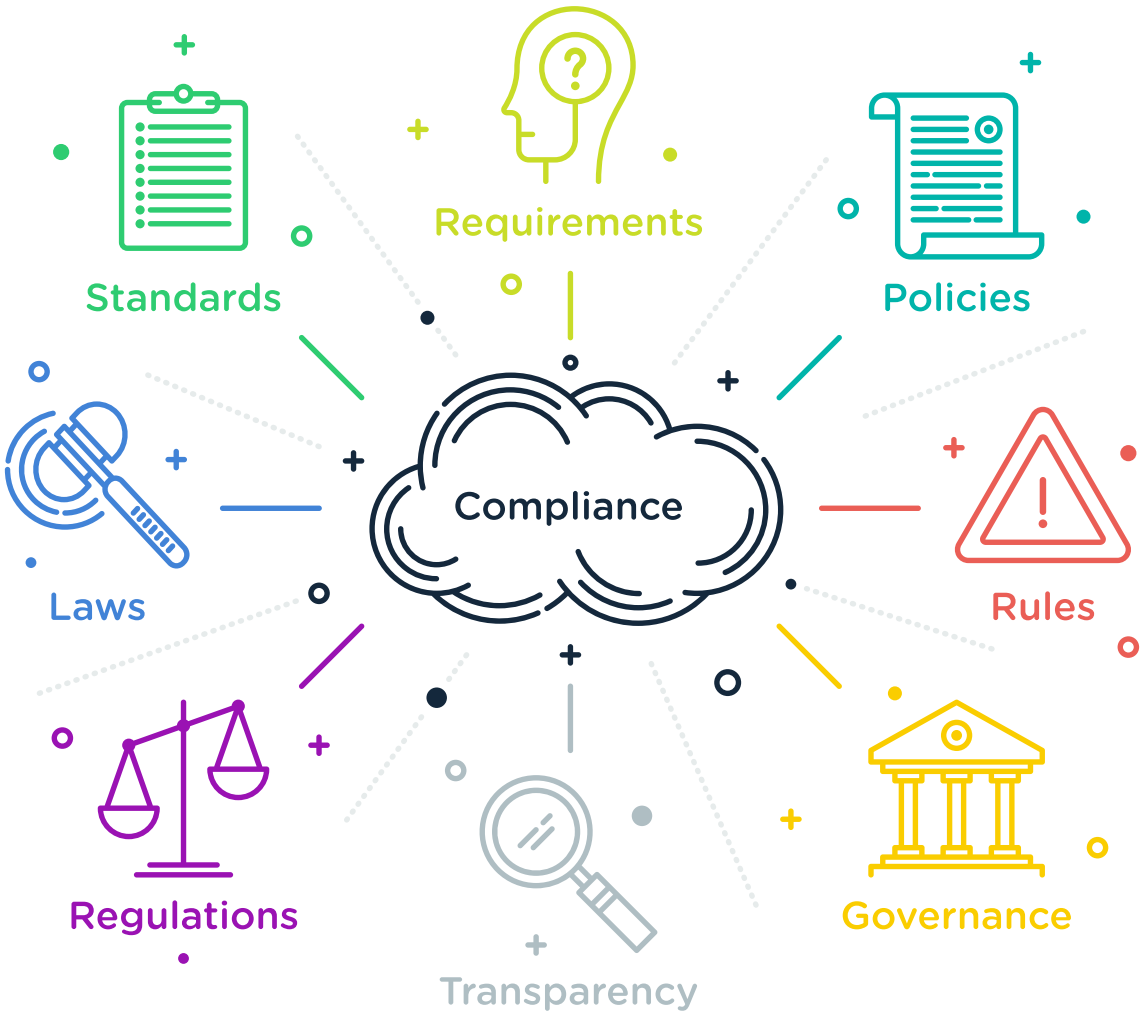


EUサイバーレジリエンス法 準拠に向けた取り組みガイド

～本質的なゴールを達成するためのステップとは～

本資料では、多くの製造事業者の方々が準拠へ向けた検討・準備・取り組みを進められているであろう EU サイバーレリジリエンス法（Cyber Resilience Act）・無線機器指令（Radio Equipment Directive）に関しての概要解説、潜在課題の提言、推奨される取り組みをお伝えします。

これらの全体像に関する情報はインターネット上でも多く見受けられ充足してきている様に感じます。しかし、準拠に向けた本質的なゴールを見据えたセキュリティ技術領域の理解と指標となる考え方、要件適用における潜在的な検討要素や課題に対する言及はまだ少ないのではないでしょうか。

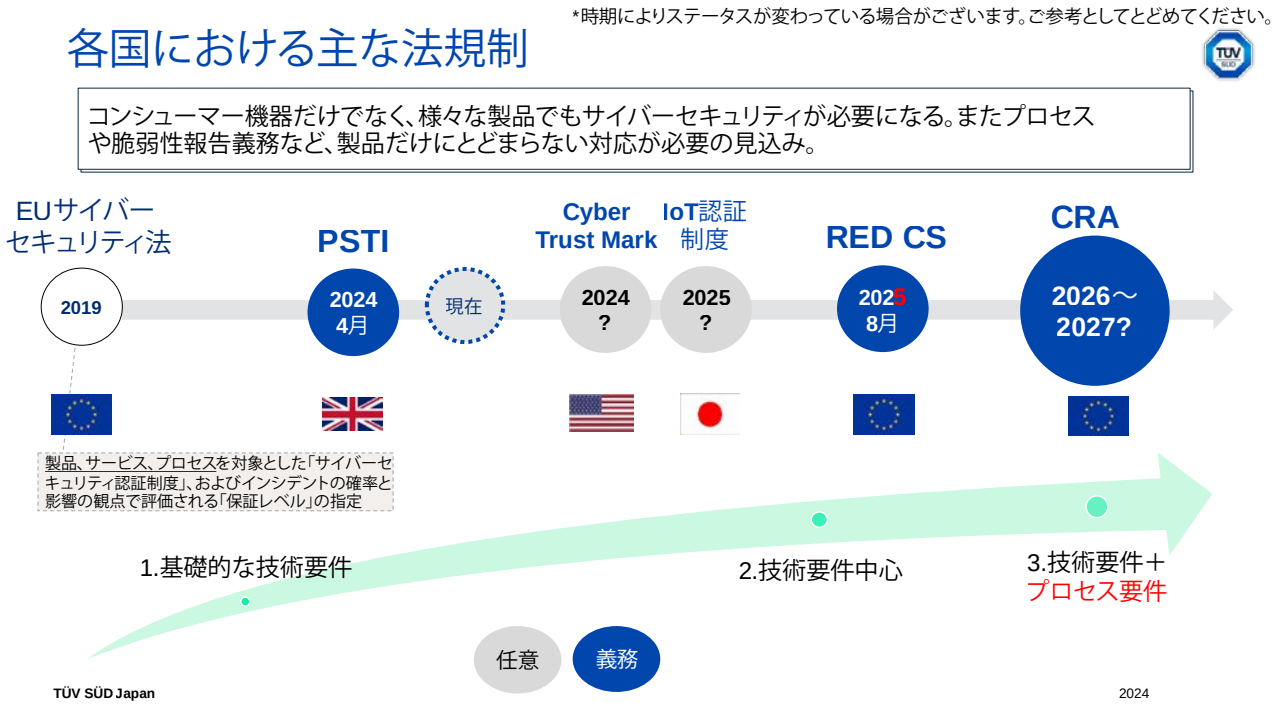
本資料では、これらの前述の部分に焦点を当てた内容を記載しています。

最初のコンテンツとして、テュフズードジャパンから現在の法規制動向概説を示します。

目次

IoT 機器における
製品サイバーセキュリティの文脈と各国法規制

IoT 機器に対するサイバー脅威の増加により、英国、米国、日本、欧州において規制が始まっています。



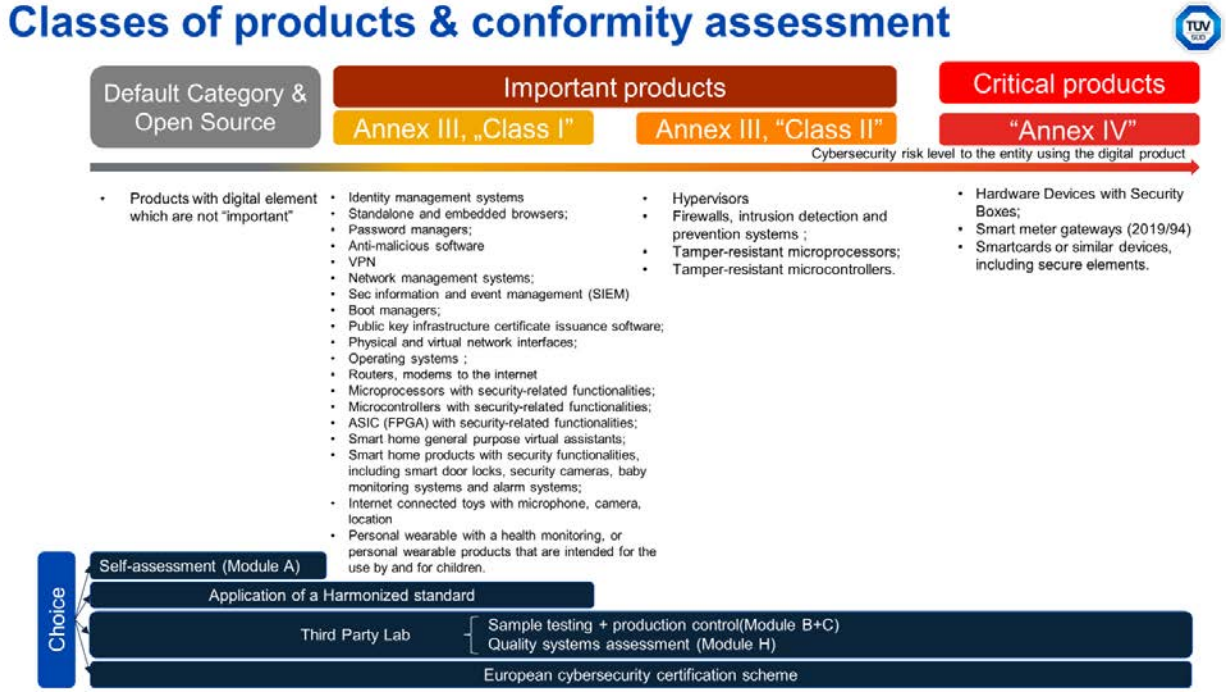
2024 年 4 月末から義務化された英国の PSTI は 1 つの技術要件（ユニバーサルデフォルトパスワードの禁止）と、2 つのプロセス要件（脆弱性に関する公開ポリシー、セキュリティアップデート期間の公開）が定義されていますが、義務化の前後において、この基本的な 3 つの要件においても苦労された製造業者様が多くいらっしゃいました。技術要件においては条文や要件の解釈、またプロセス要件においては、社内関係各所との整合を取ることに多くの時間を費やすケースが見受けられました。

2025 年 8 月からは、この PSTI の要件を大きく上回る数の要件への対応が必要な欧州無線機器指令（以下、RED）の委任規則 3（3）（d）（e）（f）の義務化がスタートします。
RED サイバーセキュリティにおいては、製品に関する要件（いわゆる技術要件）がほとんどですが、規制に対する適合性の確認に最も有効である整合規格が、3（3）（d）（e）（f）それぞれに対して発行される予定です。製品が 3（3）（d）（e）（f）すべてに該当する場合には、3 つの整合規格への適合性を確認、宣言しなければなりません。

英国を含む欧州だけでなく、米国や日本においても IoT 製品に対するセキュリティ規格への適合を促す仕組みの導入が始まりつつあります。これらの規格や規制は、現在のところ欧州と比較すると任意の規格であるため、適合していなくても販売を継続することが可能ですが、各国において IoT 機器におけるサイバーセキュリティがいかに重要視されている状況であるかご理解いただけるものと思います。

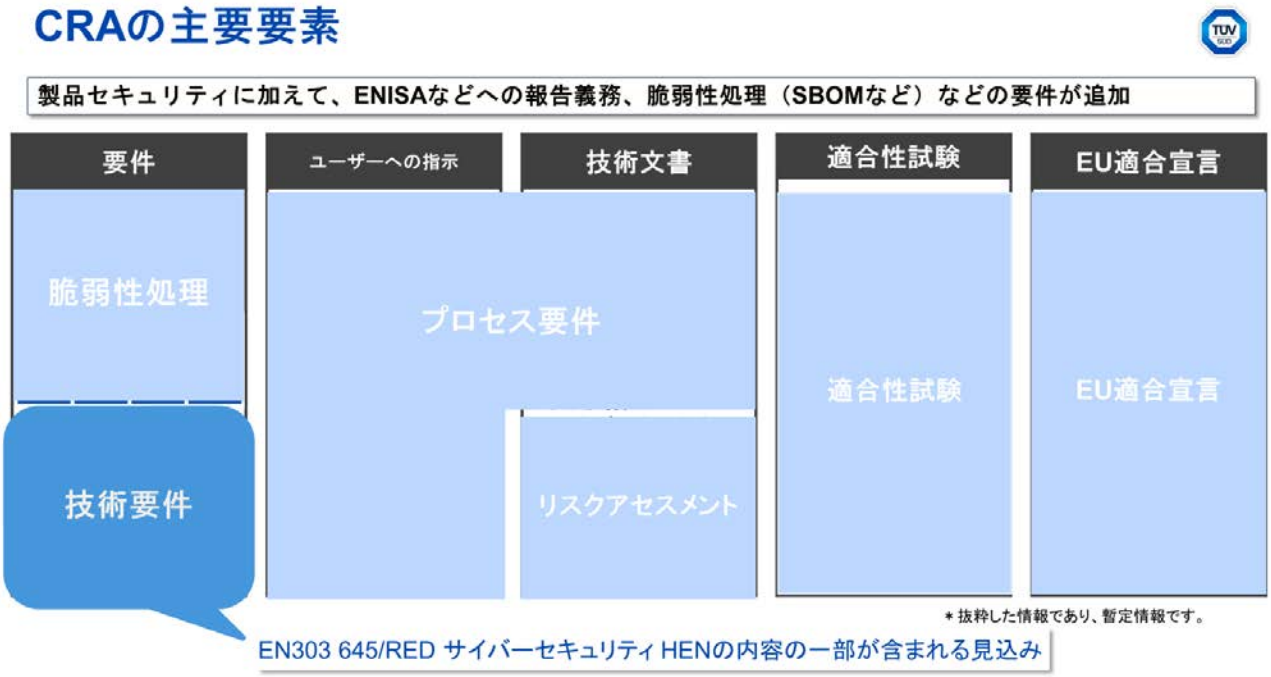
RED から CRA に至る流れ、
時間軸と主なリードタイム（標準）

RED 委任規則（サイバーセキュリティ）においては、無線機能を搭載したインターネット接続を行う機器が対象となっていたため、対象製品の範囲はおのずと限られています。
しかしながら 2024 年秋ごろに採決が予定されている EU サイバーレジリエンス法（以下、CRA）においては、デジタル要素を含み、かつデータ接続があるハードウェア、ソフトウェアも製品の対象範囲となるため、大幅に増加する見込みです。多くの製品（約 90%）は通常の製品として扱われますが、重要な製品として 3 つのクラスが存在します。



その重要度に応じて自己適合、整合規格準拠、第三者認証機関による認証と、適合性確認のレベルも変化します。

これら製品要件に加えて、サプライチェーンのデューデリジェンスや、脆弱性処理要件（SBOM 含む）など、企業として取り組むべきもの（プロセス要件）が多く含まれているのが特徴です。



CRA においては、RED サイバーセキュリティの対象製品も対象範囲のため、将来的には統合が検討されています。そこで、RED サイバーセキュリティにおける製品セキュリティ試験のリードタイムを参考として見ていきたいと思います。
本稿執筆時点では、RED サイバーセキュリティに対する製品適合試験はグレイボックス試験という方式が採られています。これは、任意のサイバーセキュリティ規格である EN303 645 と同じアプローチになります。

グレイボックス試験においては、申請者には対象機器のサイバーセキュリティ リスクアセスメントや対象機器が有するセキュリティ機能の説明を、テクニカルドキュメントとして提出いただきます。一方、試験ラボでは「記入頂いた内容が整合規格に適合しているか？」さらには「対象機器に記載された内容の通りに導入されているか？」を検証します。そのため、テクニカルドキュメントへ記載いただく内容の正確さが試験結果に影響します。この方式に不慣れな場合には、テクニカルドキュメントの準備に大幅に時間を取られることになります。

テュフズードでは、EN303 645 のギャップ分析を多く手掛けていますが、通常、初めてのお客様においてはこの記入作業に対して統計的に 3−7 カ月程度を要しています。さらには、この製品セキュリティ適合試験に加えてプロセス要件があるため、関係各所を含めた企業全体での取り組みが必要です。

影響を受ける関係者、ステークホルダー

RED と CRA においては、その対象範囲が異なるため、影響を受ける関係者、ステークホルダーは変わってきます。

- RED サイバーセキュリティは製品での対応となるため、製品開発担当者、中でも**ソフトウェア開発者**が中心となります。通常の開発業務に加えて、規格への適合が必要です。
- CRA では、上記に加えて各製品フェーズのセキュリティ要件を満たすための全体的なプロセスの導入、脆弱性処理要件を満たすための PSIRT のような全社的な組織、サプライチェーンのデューデリジェンス、セキュリティ期間の定めなどの業務が多岐にわたります。また、ステークホルダーも**製品開発者、品質保証、法務部門、購買部門、また部門間をつなぐ PSIRT、企画部門**など幅が広いことが特徴です。これらに加えて、ハードウェア、ソフトウェアのコンポーネント供給者においても対応が必要な場合があるため、その範囲は格段に広がります。

多くの関係者が存在することになる CRA においては、早期の対応開始が求められます。社内にない知識、ノウハウは外部のサービスを検討する必要があります。

重要な位置づけとなるリスクアセスメントの目的

RED、CRA のどちらでも言われていることですが、リスクアセスメントが必要です。
リスクアセスメントではその製品が持つアセット（資産）を定義し、その資産に対するリスクを特定し、リスクに対抗するセキュリティ目的、セキュリティ要件、セキュリティ機能を決める必要があります。そしてそのアセットを守るセキュリティ機能が適切であるかどうかを判定することが適合性評価の一部に含まれています。

RED サイバーセキュリティを例に取ると、整合規格のドラフトには、リスクアセスメントの方式、規格に関しての指針は出ていないため、サイバーセキュリティの考慮がなされているリスクアセスメントの方式、規格をご自身で選択する必要があります。（下図は手法の一例として、IPA ウェブサイトに掲載されている制御システムのセキュリティリスク分析 37 ページより）

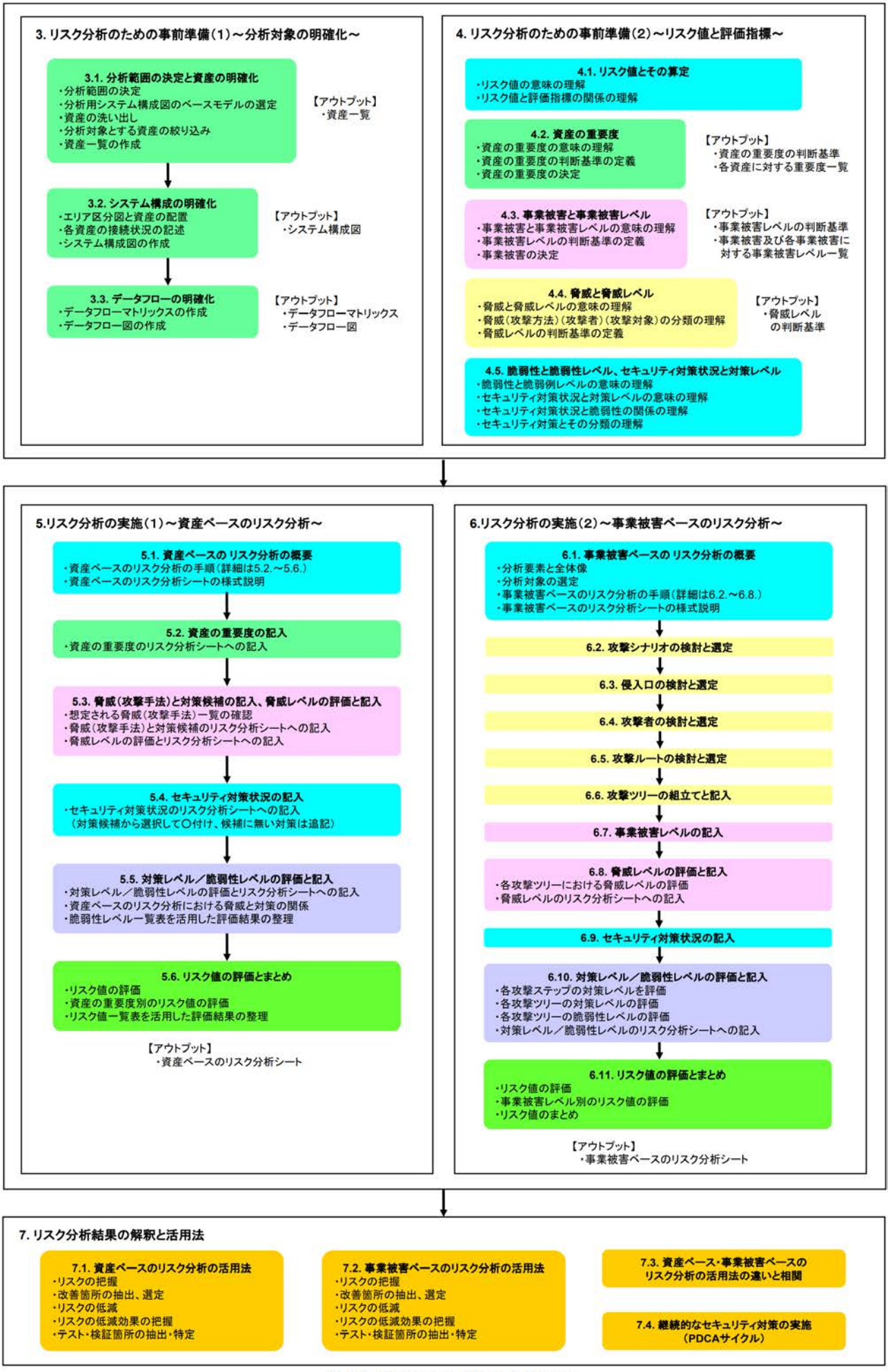


図 2-2 制御システムのリスク分析の流れ

また、整合規格は、様々な無線機器を対象とした水平的な整合規格（多くのアプリケーションに対応しうる汎用的な規格）であるため、リスクアセスメントにおいて、それぞれの機器における各セキュリティ機能の“適切さ“を導き出す必要があります。そして、適切であれば整合規格に適合したこととなる項目が多く存在しています。（将来的には、主要なアプリケーションに特化した垂直的規格がリリースされる可能性があります。）

本来、リスクアセスメントは開発初期段階から行われるべき内容となりますが、今回の法規制に併せて、改めて取り組まれることをお勧めいたします。

使用目的、ユーザーの重要性

リスクアセスメントの中で考慮しなければならない項目の一つに使用目的（Intended Use）や使用環境（Operational Environment）、ユーザーの想定があります。これらの想定される状況により、必要とされるセキュリティ機能が変わってくる点に注意が必要です。
例えば、スマートロックのような製品で、同じ製品が家庭で使われる場合と、軍事施設に使用される場合では、そのアセット（守るべき資産）が変わってきます。軍事施設では、より重要なアセットを手に入れるべく、高度なスキルセットを持った攻撃者プロファイルが想定されるため、それに対応しうる高度なセキュリティ機能が必要になってきます。
つまり、同じ製品においても使用目的やユーザーにより、必要なセキュリティ機能が変わってくることになります。

日本の製造業者様におかれましては、サイバーセキュリティに関するリスクアセスメントについてあまりご経験がないケースが多く見受けられます。テュフズードでは初学者に向けたコンシューマ IoT 製品を中心としたリスクアセスメント（脅威分析モデル）の TR64 という規格に基づいたトレーニング、ワークショップをご用意しています。

免責事項と独立性に関する注意書き

テュフズードは第三者認証機関として、独立性、公平性に重きをおき企業活動を行っております。共同で開催、参加する展示会、セミナー、ウェビナーなどのイベントや共著において、主催、共催、参加されるいかなる企業様との関連は無く、それらの企業様の製品、サービスなどを利用することは、当社の本質的な業務である認証や試験に影響を与えるものではありません。

ここまでがテュフズードジャパンからの法規制動向と概説となります。
ここからは、前述項内にも挙げられているリスク評価に関する重要性を少し深堀し解説します。

リスク評価・分析の重要性

製品製造事業者には適用対象製品に対するリスク評価が義務化されています。

Article 13

Obligations of manufacturers

1. When placing a product with digital elements on the market, manufacturers shall ensure that *that product* has been designed, developed and produced in accordance with the essential requirements set out in Annex I, *Part I*.

2. For the purpose of complying with the obligation laid down in paragraph 1, manufacturers shall undertake an assessment of the cybersecurity risks associated with a product with digital elements and take the outcome of that assessment into account during the planning, design, development, production, delivery and maintenance phases of the product with digital elements with a view to minimising cybersecurity risks, preventing incidents and minimising the impacts of such incidents, including in relation to the health and safety of users.

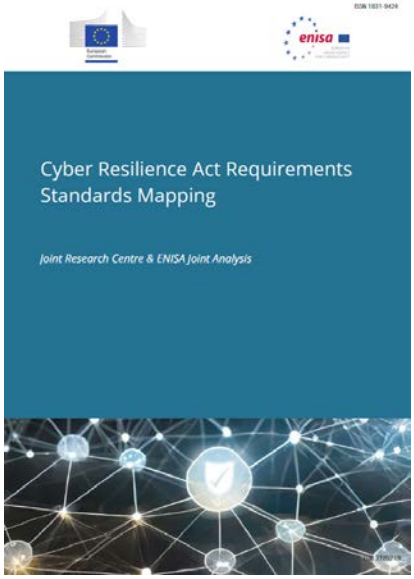
3. *The cybersecurity risk assessment shall be documented and updated as appropriate during a support period to be determined in accordance with paragraph 8 of this Article. That cybersecurity risk assessment shall comprise at least an analysis of cybersecurity risks based on the intended purpose and reasonably foreseeable use, as well as the conditions of use, of the product with digital elements, such as the operational environment or the assets to be protected, taking into account the length of time the product is expected to be in use. The cybersecurity risk assessment shall indicate whether and, if so in what manner, the security requirements set out in Annex I, Part I, point (2), are applicable to the relevant product with digital elements and how those requirements are implemented as informed by the cybersecurity risk assessment. It shall also indicate how the manufacturer is to apply Annex I, Part I, point (1), and the vulnerability handling requirements set out in Annex I, Part II.*

出展：Cyber Resilience Act 製造業者義務より抜粋

これは CRA の目的にも通じる“リスク管理を持続的に行えること”が求められていると認識しています。昨今の整合規格に対する評価の傾向として、なぜ実装したセキュリティ機能が必須要件を満たしているか・最適であるとしたのかを論理的な説明とエビデンスが求められることと無関係ではなく、より厳格性の高い評価基準になったと考える方がよいでしょう。

製品製造事業者は対象製品内で組み込まれている 2nd party・3rd party 製 SW/HW に対するリスクも把握することが必要な場合があります。これはブラックボックス化された要素が製品へ組み込まれることを防止しますが、セキュリティ要件に対するセキュリティ機能の透明性のある説明ができることでリスク管理が行われていることを意味していると考えます。製造サプライチェーン上の部品 / モジュール供給事業者もリスク評価・管理ができていることは、今後の市場を考えるうえで重要な取り組みになるといえます。

より詳細な要件記載粒度である整合規格を基にした取り組みを早急に実施したい一方、現在（※2024 年 6 月時点）のところ、整合規格や Notified Body と呼ばれる委任団体は決まっていません。代用価値のある標準規格はいくつか存在していますが、企業毎の事業分野よって選択する規格に違いはあります。その際には、ENISA 発行の Standards Mapping 資料が役立つでしょう。



4 Summary of the identified standards and overall remarks

Here the overall list of identified standards is summarised with the respective mapping, grouping them according to the two groups of CRA essential requirements.

	Security requirements relating to the properties of products with digital elements											
Standard	1	2	3 a	3 b	3 c	3 d	3 e	3 f	3 g	3 h	3 j	3 k
I N ISO/IEC 27002:2022	x		x					x			x	x
I N ISO/IEC 27005:2022	x											
I N IEC 62443-3-2:2020	x									x		
I N IEC 62443-4-1:2018	x	x										
ISO/IEC 18045:2022		x								x		
ITU-T X.1214 (03/2019)		x										
ETSI I N 303 645 V2.1.1 (2020-06)	x	x	x	x	x	x	x	x	x	x	x	x
ISO/IEC 18031:2011			x									
ISO/IEC 9798, Parts 1 to 6				x								
ISO/IEC 24760, Parts 1 to 3				x								
ISO/IEC 29146:2016				x								
ITU-T X.1253 (09/2011)				x								
ITU-T X.812 (11/1995)				x								
I N IEC 62443-4-2:2019				x	x	x		x		x		x
ITU-T X.805 (10/2003)					x			x				
ISO/IEC 18033, Parts 1 to 7					x							
ITU-T X.814 (11/1995)					x							
ISO/IEC 9796, Parts 2 and 3						x						
ISO/IEC 9797, Parts 1 to 3						x						
ISO/IEC 14888, Parts 1 to 3						x						

51

[引用：ENISA, Cyber Resilience Act Requirements Standard Mapping]

しかし、CRA 準拠を目指される方々にとって最初からすべての要件を満たしていくことは非常に時間と労力がかかるのも悩みどころです。民生機器メーカーであれば、まずは整合規格のリリースが近く、セキュリティ必須要件としても CRA へ取り組まれる RED の整合規格（※2024 年 6 月時点では未リリース）が有益であろうと考えます。最初にリスク評価を行うことが重要であることに変わりはありませんが、アプローチとして推奨したいのはコンプラアインスチェック（体制・プロセス構築）と事実ベースの確認（ギャップ分析）のハイブリット方式です。

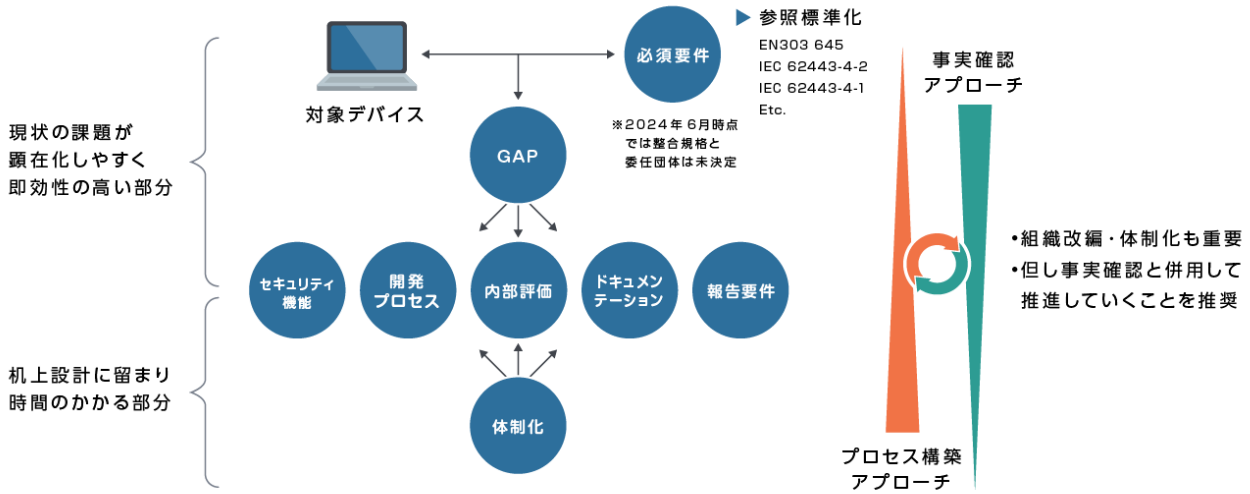
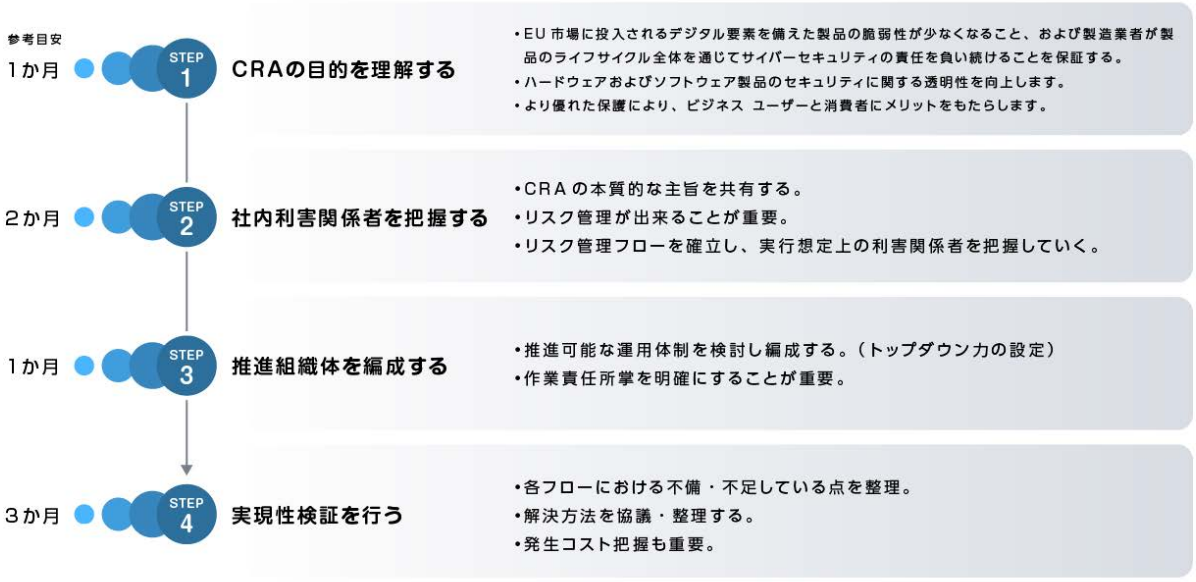


図 . 推奨アプローチ概念図

体制・プロセス構築も重要ですが、この取り組みへの比重が大きい傾向にある場合には組織内での議論・協議に多くの時間と労力を使ってしまい、結果的にセキュリティ要件へ適用する時期が遅れる可能性があります。そこで推奨されるのが、事実確認の両面から行うことです。これにより、現状の実態とのギャップを把握しやすくなり、どういうプロセスをどんな体制で運営していくのが自社にとって最適かが分かります。組織内で時間のかかる要因のひとつには、別部署間での情報整理・統制の難しさがあるのではないかと考えています。その際、外部の中立的な第三者の支援を受けることも選択肢の 1 つです。

図 . リスクとプロセス・組織化相関

また、これから取り組みを始める方々には、ぜひ CRA の目指している目的理解の共有と共に社内推進体制の構築を推奨します。



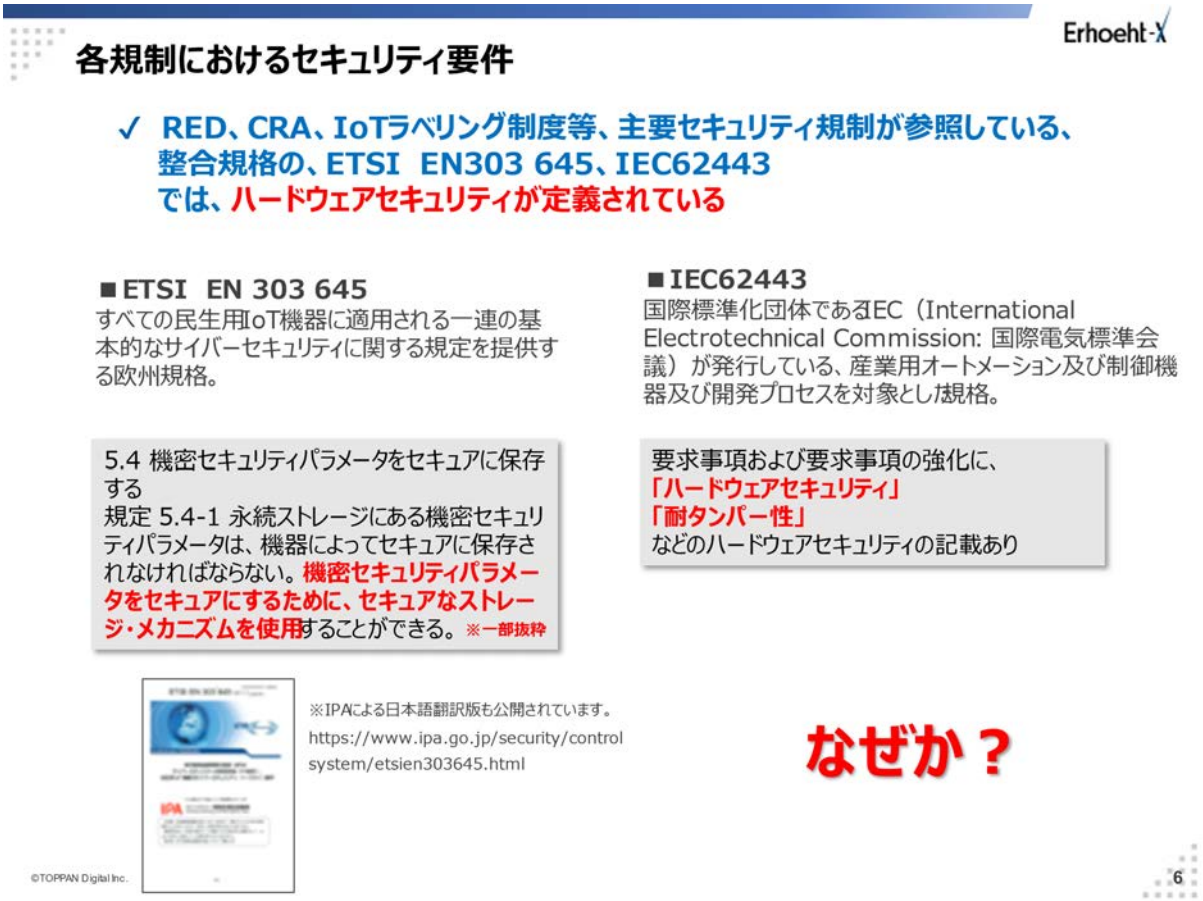
ここからは具体的な要件レベルでの課題に関して掘り下げていきます。
リスク評価結果に応じセキュリティ施策を採用していくことになりますが、特に悩ましい要素としてセキュリティレベルの向上のための専用セキュリティハードウェアの検討があると考えます。

厳格化が進む IoT デバイスのセキュリティ規制における ハードウェアセキュリティ対策の有用性

＜市場動向＞

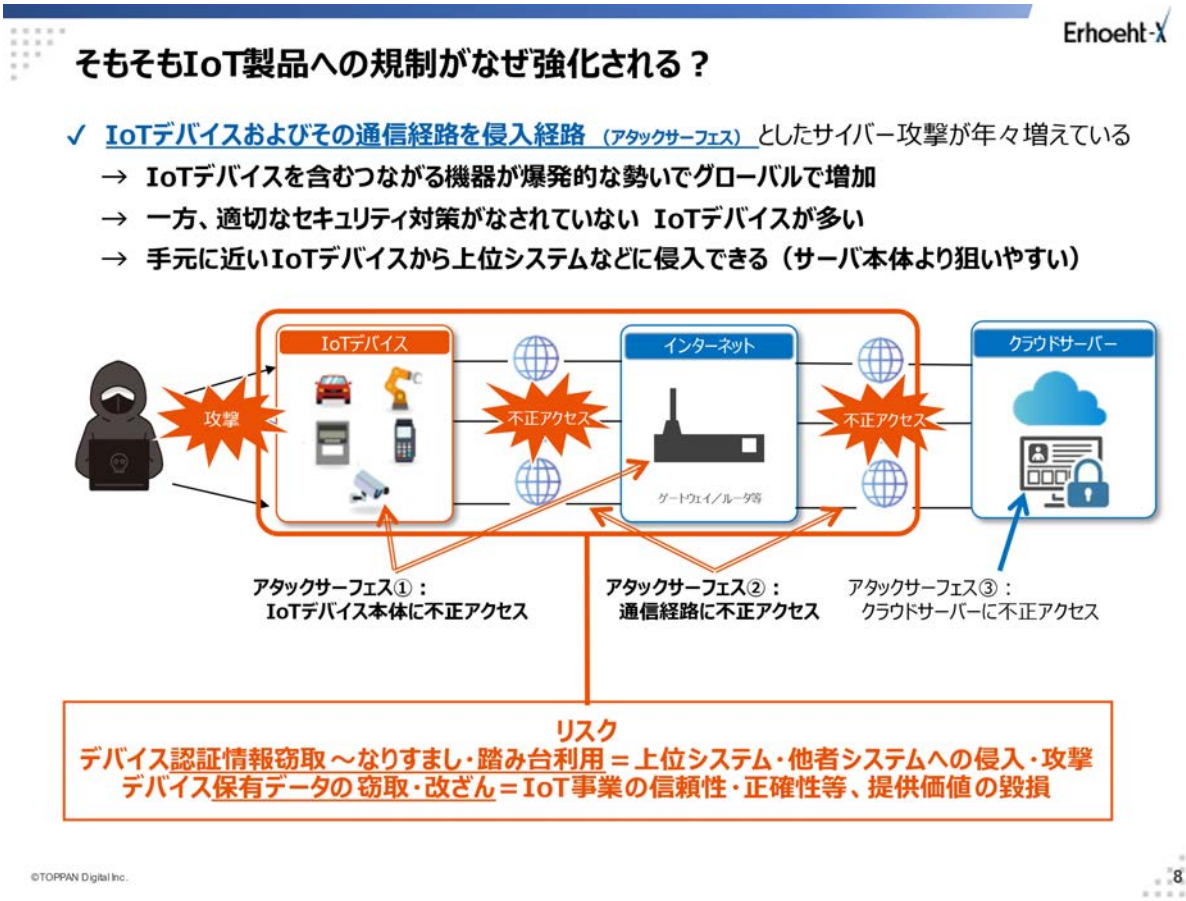
はじめに、市場の動向についてです。IoT デバイスのセキュリティに対する規制がグローバルで強化されています。欧州での無線機器司令やサイバーレジリエンス法などはもちろんのこと、日本でも IoT 製品セキュリティ評価制度の導入が発表され、各社セキュリティ対策の必要性が高まっています。

各規制が参照しているのが、欧州の整合規格である、ETSI EN 303 645 と IEC62443 です。これらにはセキュリティ要件が記載されていますが、両規格とも信頼・保護の強化として、ハードウェアに関しての記載があります。なぜハードウェアへの言及がなされているのでしょうか？



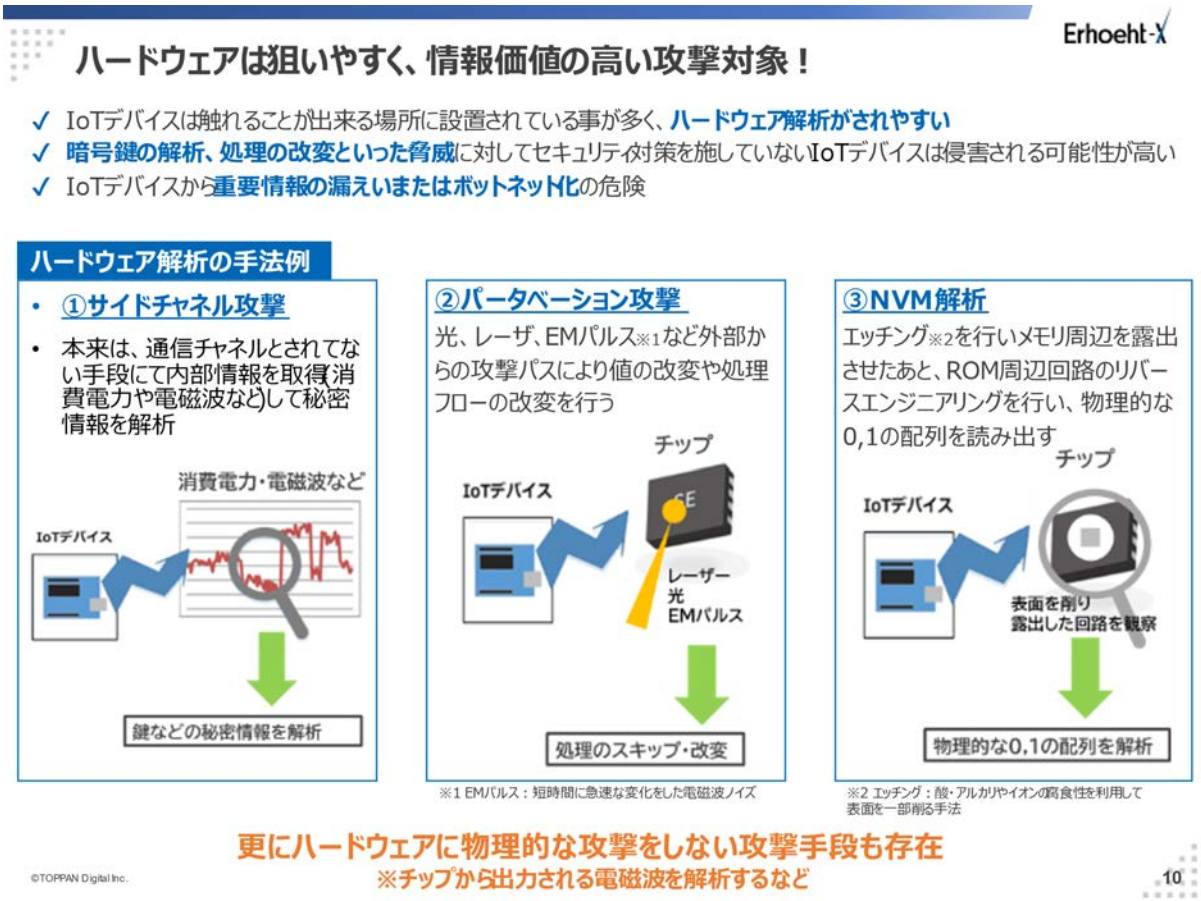
＜狙われやすい IoT デバイス＞

ここで、IoT デバイスにおけるセキュリティ規制が強化される背景をおさらいしておきたいと思います。図のように、IoT のシステムには多様な攻撃の入り口があるため、IoT 機器の爆発的な増加に比例して、サイバー攻撃も年々増加しています。このような状況がある一方で、適切なセキュリティ対策が施されていない IoT デバイスは数多く存在し、手に触れやすい IoT デバイスがハッカーの格好の餌食となっています。単純に IoT デバイスの停止だけでなく、上位のシステムに侵入されることで、被害規模は計り知れないほど大きいものになってしまう可能性も秘めています。



IoT デバイス起点でのインシデントも多発しております。実際に、IoT デバイス起点でのインシデントも多発しております。防犯カメラや車を狙ったハッキング事例や IoT デバイスのソフトウェアの脆弱性を狙ったもの、電子証明書の管理不徹底によるインシデントなど、多様な攻撃手段での事例が発生している状況です。

そんな IoT デバイスですが、ソフトウェアのみでなく、ハードウェアへの攻撃により、ハードウェアに格納されている重要データを搾取し、結果的にシステムに侵入する攻撃手段があることをご存知でしょうか？　ハードウェアの攻撃手段には図のようにさまざまなものがあり、攻撃者はあらゆる手法を駆使して侵入を試みます。物理的な直接攻撃だけでなく、ハードウェアから発せられる電磁波などを離れたところから観測・解析して重要な情報を抜き取る手段もあります。そのため、単にハードウェア的に開封できないような構造だからというような理由だけでは、ハードウェア対策は不十分です。



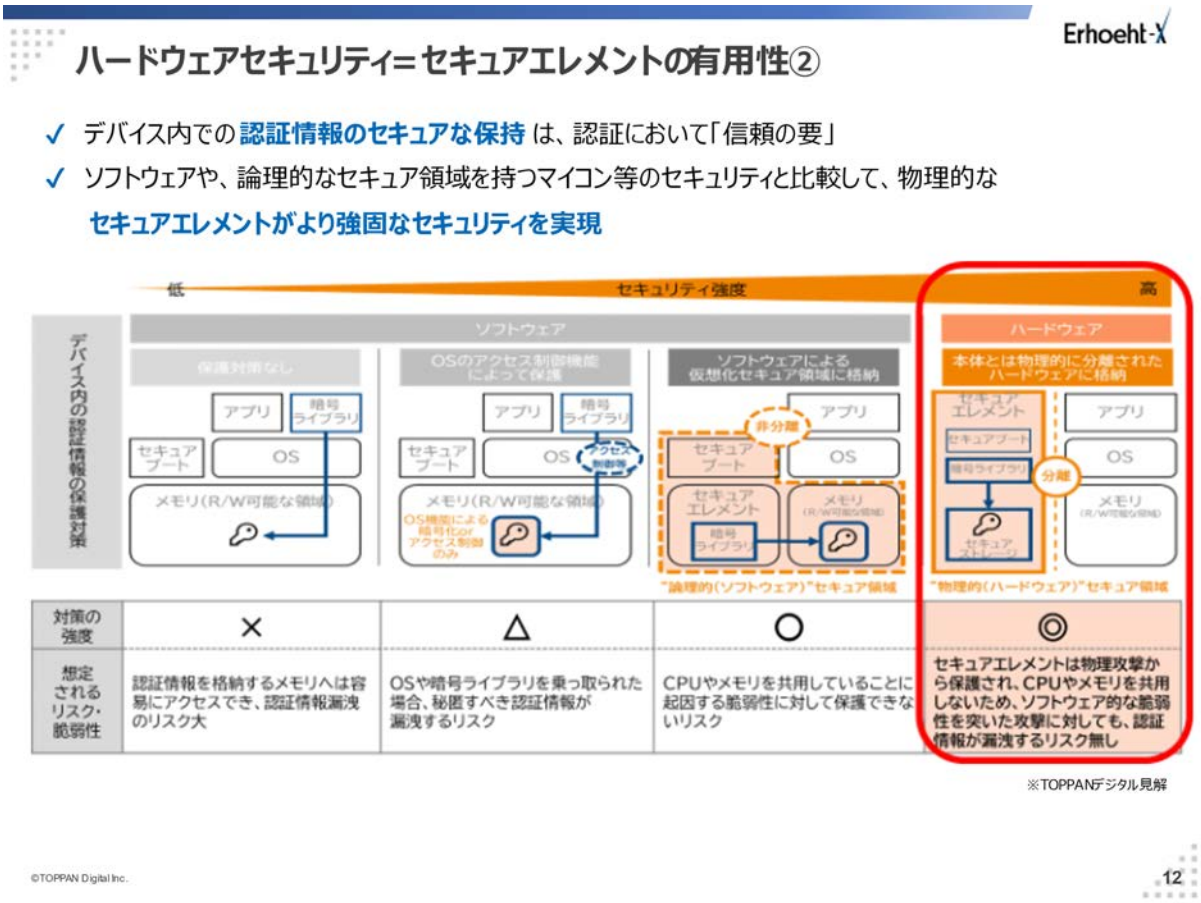
実例としては、テレビの認証カードの改造により暗号が書き換えられ、有料チャンネルを登録なしで見られるようになってしまった事例や、サイドチャネル攻撃によって、Google の「Titan セキュリティキー」の二段階認証の暗号が解読され突破されてしまった事例などがあります。

＜ハードウェアのセキュリティ対策の有用性＞

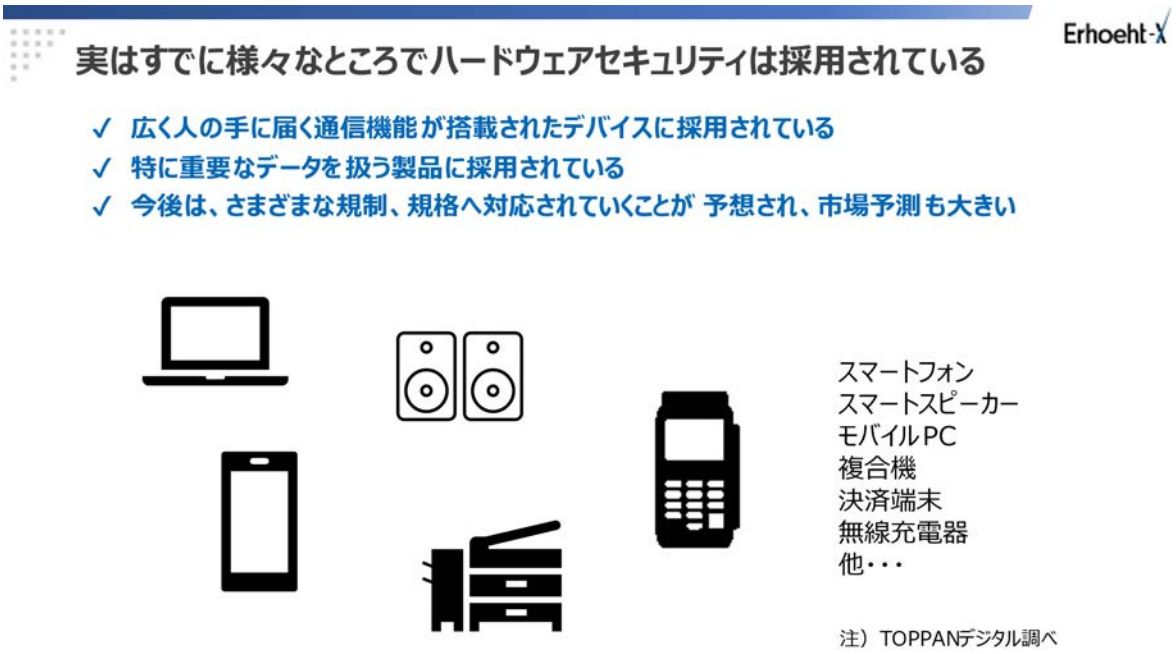
　ハードウェアのセキュリティ対策として有用な手段の一つに、セキュアエレメントがあります。これは特殊な構造をしたチップで、外部からの攻撃があっても電力解析ができないようになっています。また、過度な攻撃があった場合にはサービスを停止する機能が搭載されているため、外部からの攻撃を無効化できます。

図：セキュアエレメント（例）

認証のための情報や機密性の高い情報は、ハードウェアに格納された状態で機能しています。情報の保護の方法としては、ソフトウェア保護がありますが、それでは物理的攻撃に弱いため、物理的攻撃に強いハードウェア保護を採用することで、より強固なセキュリティを実現できます。また、ハードウェアを分離することで、サービス本来の機能とセキュリティ機能を分離することになり、責任分界点が明確になります。

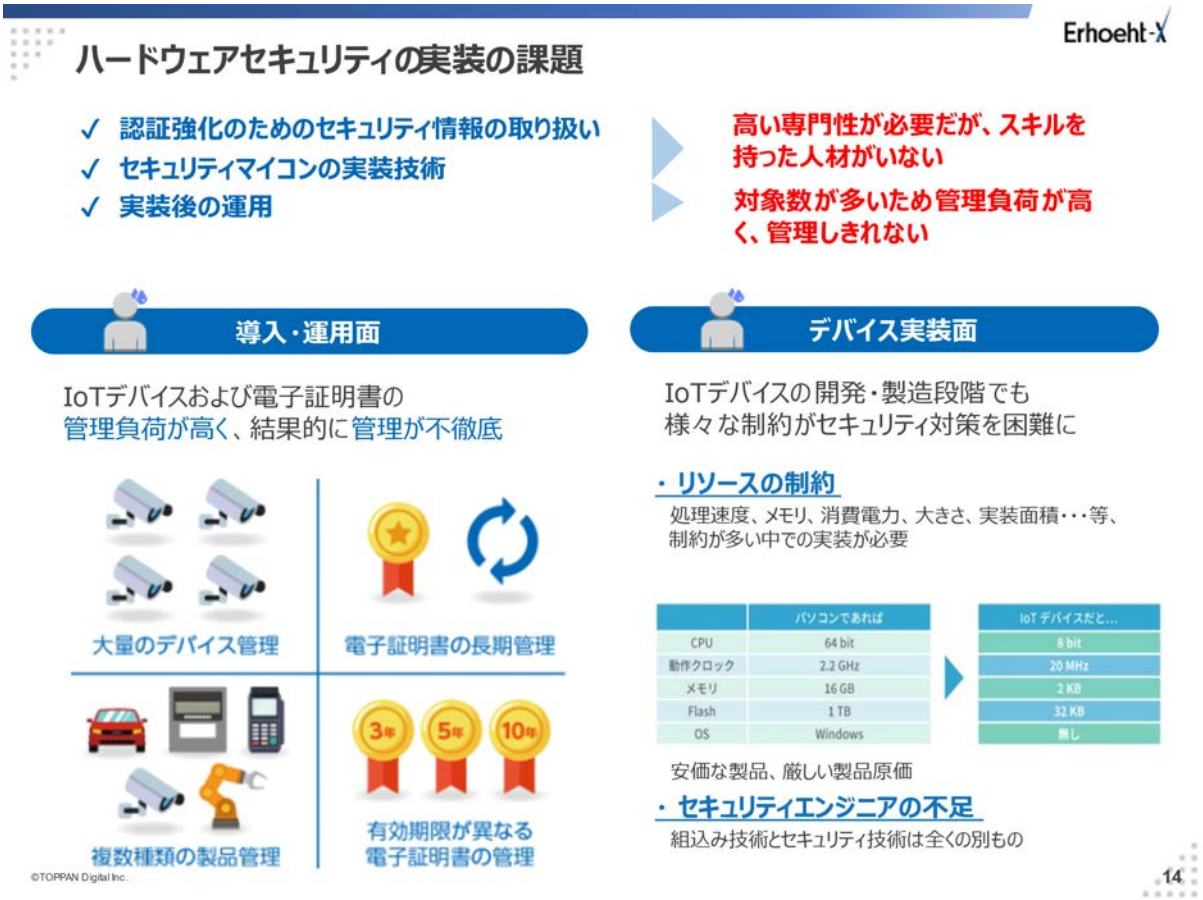


世の中にはすでに、ハードウェアセキュリティ（セキュアエレメント）を搭載した機器が多数存在しています。特に、広く人の手にわたりやすいデバイスや重要データを扱うデバイスなどに搭載されており、新しい規制や規格などでは、セキュリティ強化の文言が追加されてきていることもあります。そのため、今後の市場動向の予測値でも大きな成長が見込まれる市場となっています。



＜IoT デバイスのハードウェアセキュリティ対策の課題＞

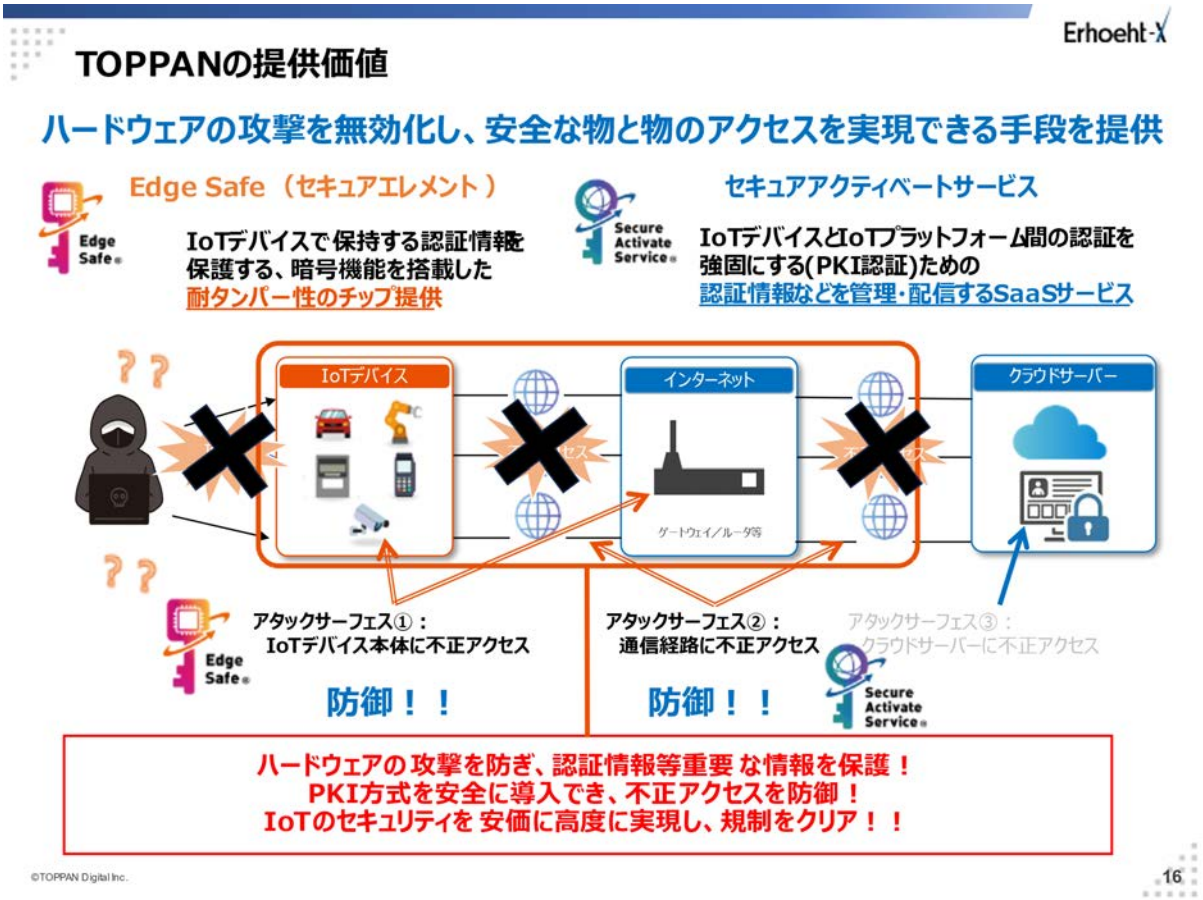
ただし、IoT デバイスならではの実装の課題があり、なかなか普及にはいたらない実情もあります。そもそも、セキュリティの実装は、高度な専門性や実装スキルがなければ実装が難しい機能であるため、セキュリティ開発が可能な人材の確保が必要になり、スキルを持った人材がいなければ実装ができません。また、実装後であっても数量が多く、さまざまなところに設置される IoT デバイスを管理しきれない状況になれば、セキュリティ観点でも管理の課題がでてきてしまいます。こうした課題を解決しない限り、安全な IoT デバイスの普及は難しいです。



＜TOPPAN の IoT デバイス向けセキュリティサービス＞

TOPPAN の IoT デバイス向けセキュリティサービスでは、それらの課題を解決できるソリューションを提供しています。ハードウェアセキュリティを実現できる Edge Safe では、物理攻撃に強い耐タンパー性のチップで、機密情報を安全に保持し、暗号復号の作業も一手に引き受けられるアプリケーションを搭載しているため、ハードウェアセキュリティを高い専門知識がなくとも実装が可能なものになっています。セキュアアクティベートサービスでは、格納する機密情報を安全に配信することができ、情報の有効期限なども外部からコントロール、管理することが可能になるため、市場に出た IoT デバイスのセキュリティ管理が容易かつ、安全に実現できる手段となっております。

両方をあわせることで、非常に強力で、セキュリティ規制をクリアできるセキュリティ機能の実装が可能になります。ここでは詳しい内容は述べませんが、ご興味ある方は、ぜひ下記画像や web サイトもご参照ください。https://solution.toppan.co.jp/toppan-digital/service/secureactivate.html



ここからはもう１つ別の具体的な課題としてデジタル証明書の利活用に関して記述します。

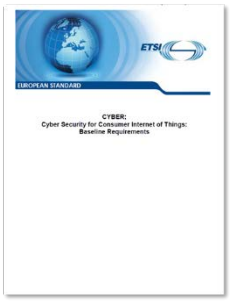
PKI 技術に関する留意点

ここからは、デジタル証明書を活用した技術に関しての内容をお伝えします。まず、多くの方が最初に悩まれるのが、デジタル証明書ひいては認証局の活用に関する知見や情報の不足です。しかし、これはある意味では正しい状態ではないかと考えられます。

インターネットの世界で多く使われるサーバー証明書、社内 IT 環境で従業員向けに使われるユーザー証明書は、専門ベンダーへ社内IT部門の方々が問い合わせし購入･実装されていることが多いのではないでしょうか。その際、インターネットのブラウザとウェブサイト間の暗号化された接続を支えている標準化団体や認証局企業の取り組みに関する背景、詳しい認証概念の基本設計や証明書の記載内容について議論することは少ないはずです。そのため、IoT 機器への導入が必要になった際に社内知見を転用するような仕組みや分野知見の蓄積がされづらい分野であるともいえます。

IoT 機器へのデジタル証明書の導入が難しいと考えられるもうひとつの側面に、その製品が置かれているビジネスモデル、業界規格 / 標準化の理解、技術的概念、を正しく理解する必要があることが挙げられます。デジタル証明書活用における理解を進めたうえで初めて認証局ベンダーの選定（選定基準・コスト）を実施・判断してくことが可能になります。また、選定時は複数選択肢をもちながら選定することを推奨します。

次に、具体例を用いて解説していきたいと思います。現在の必須要件記載粒度でも、実際にどうすればよいのか判断しづらい表現は多く見受けられます。



1. 普遍的なデフォルトパスワードは使用しない
2. 脆弱性の管理報告手段を実装する
3. ソフトウェアのアップデートをし続ける
4. 機密性の高いセキュリティパラメータは安全に保存する
5. 安全に通信する
6. アッタックサーフェースの最小化
7. ソフトウェアの整合性を確保する
8. 個人データを確実に安全にする
9. 停止から回復力のあるシステムにする
10. 通信データの検査をすること
11. ユーザが簡単にユーザのデータ消去が行える
12. 機器へのインストールとメンテナンスが容易であること
13. 入力データは検証すること

図 .RED/303645 要件で PKI 利活用推測領域

A. Authentication

There are generally two types of authentication controls—information and entities—and a properly-secured system is able to prove the existence of both.

Authentication of *information*[69] exists where the device and the system in which it operates are able to prove that information originated at a known and trusted source, and that the information has not been altered in transit between the original source and the point at which authenticity is verified. It is important to note that while authenticity implies that data is accurate and has been safeguarded from unauthorized user modification (i.e., integrity), integrity alone does not provide assurance that the data is real and came from a trusted source. Therefore, for the purposes of this guidance, authentication is discussed as a larger security objective over integrity.

Authentication of *entities* exists where a device and the system in which it operates is able to prove the identity of an endpoint (whether hardware and/or software) from which it is sending and/or receiving information, or authorized user/operator at that endpoint.

図 .FDA の PKI 利活用推測領域。

(d) ensure protection from unauthorised access by appropriate control mechanisms, including but not limited to authentication, identity or access management systems, and report on possible unauthorised access;

(e) protect the confidentiality of stored, transmitted or otherwise processed data, personal or other, such as by encrypting relevant data at rest or in transit by state of the art mechanisms, and by using other technical means;

(f) protect the integrity of stored, transmitted or otherwise processed data, personal or other, commands, programs and configuration against any manipulation or modification not authorised by the user, and report on corruptions;

図 .CRA の存在証明部分の原文抜粋

CRA・RED/EN303645・FDA でも類似性のある「認証 /Authentication」という言葉が含まれる要件に注目してみます。これは、通信相手（クラウドサービスや他社製デバイス）に対して自らの存在証明 /ID を提示すること、相手の存在証明を検証することを求めています。このような機器間の相互認証を実現するには、単一事業者だけの製品環境であれば、その事業者で全てを取り決めることが可能です。

しかし、他社製機器同士の相互利用の場合は「誰かが主体となり認証をするのか」という概念設計が必要であり、信頼できる第三者が信頼の基点となること（各事業者 / 信頼する側からの信頼対象としての存在）が重要な考え方になります。相互認証・相互利用においては、このような信頼の基点を取り込んだ標準化が重要な要素となってきます。

スマート家電分野ではすでに CSA（Connectivity Standard Alliance）が策定した操作性統一規格である Matter 規格において相互認証を PKI/ デジタル証明書で実現しており、CSA が承認した認証局を信頼する構造が策定されています。これは、今後他分野への進展が期待される良い事例といえます。実装レベルにおいては、デジタル証明書を利用したセキュリティ機能が組み込まれた汎用プロトコルへの難易度はさほど高くはないと考えられます。

難易度の高い課題は、専門性のある本領域を要件適合へ向けて基本設計にどう取り組んでいくかです。デジタル証明書の利活用は開発部以外の複数部署と連携することが必要になるため、手戻りが発生した際の影響は大きくなってしまいます。これは、デジタル証明書におけるライフサイクルの構築を意味しており、鍵データ生成を「いつ」「どこで」「誰が」行い、「いつ」「誰が」「どのように」デジタル照明書を発行し、デバイスへ書き込むのかという業務フローを構築しなくてはならないからです。

また、IoT 機器で保持するデジタル証明書データに対するセキュリティ観点として HW セキュリティの採用可否についても検討は必要です。これはデジタル証明書という情報資産に対してのリスク・脅威を分析・検討し、施策を考えるべきであり、CRA や RED で提言されているリスク管理の実施にも繋がります。

ここからは要件レベルの課題ではなく、要件適合への実行環境である開発環境に関しての課題提起を記述していきます。

開発環境改善に関する留意点

ここまで、CRA や RED の概要と各セキュリティ要件に関する留意点を記載してきました。最後に、法規制等の対応により影響・変化が見込まれる開発業務の変化について想像してみてください。

業務種類と量は増える傾向にあるのは確かですが、その一方で、業務タスクの時間的短縮を迫られることは起こり得るのではないでしょうか。持続的なリスク管理を実現する新たなワークフローを構築したとしても、業務タスク時間が増加し、結果的に企業としての対応が遅れれば、信頼性や生産性を損なってしまうことになります。

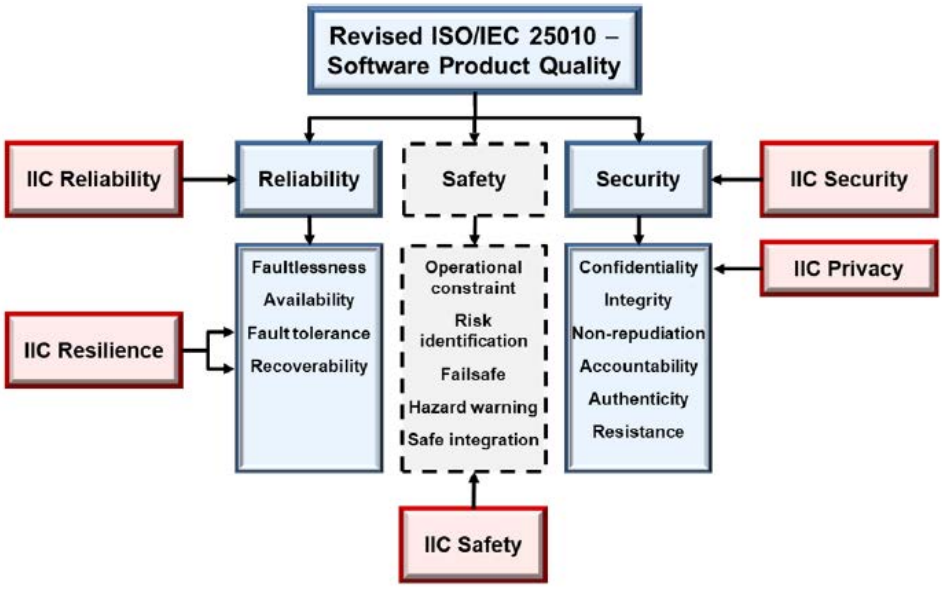


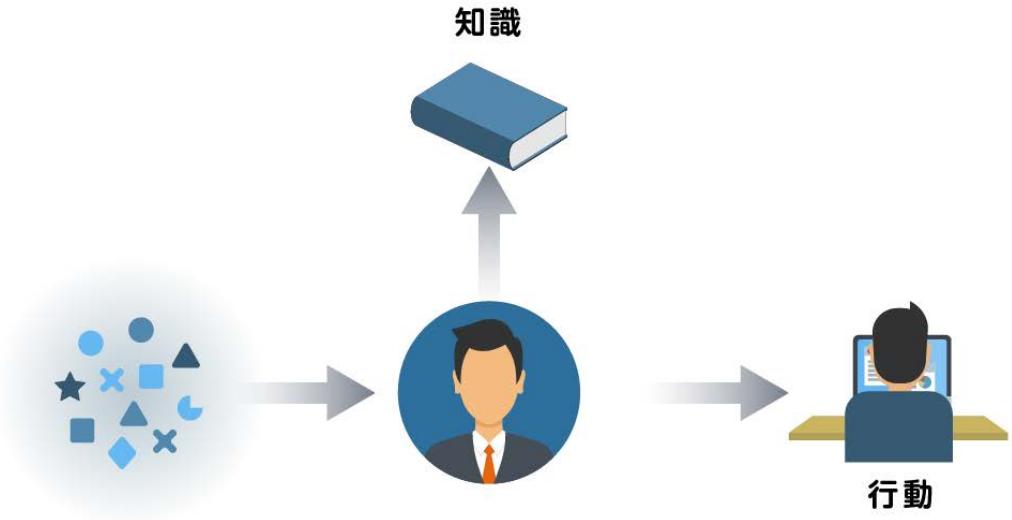
図 . Measuring the Trustworthiness of Software with ISO/IEC 5055

たとえば、なにか修正工程が発生したと想定した場合。セキュアコーディング規約の適用性確認、既存セキュリティ機能への影響、設計書とリスク評価結果との資料レベルでの突き合わせ確認、関係者とのレビューや打ち合わせ、テスト項目の変更、数多くのテスト項目のチェック実施と、今までよりも作業時間や打ち合わせが増える傾向にあると推察されます。こうした問題は、単にセキュリティ専門性の高い人材を確保すれば解消されるのでしょうか。確かにそれも解決策のひとつではありますが、属人性を高めた一時的な改善となる場合もあります。

業務整理・改善を行い、技術的な情報を共有できる仕組み作りまで担えるデジタル人材の獲得は容易ではありません。ここでお伝えしたいのは、業務・開発環境の改善に関する取り組み価値についてです。特に、ソフトウェア開発での概念で大きく５つの改善ポイントが存在します。

- コード負債
- デザイン負債
- テスト負債
- インフラ負債
- ドキュメンテーション負債

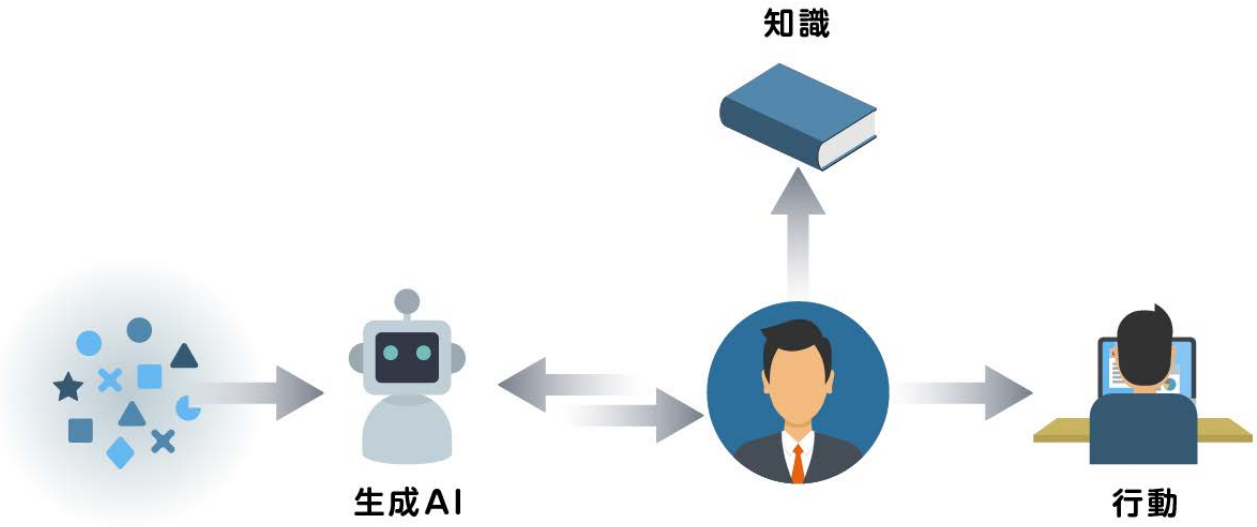
まずは、“どのような業務タスク”の“何の工程“に時間がかかるのか。整理してみることが重要です。



時間を要している工程がわかれば、改善施策の検討が可能です。たとえば、開発関連資料の記載内容や基準が揃っておらず、内容把握をするための時間がかかっているような場合には、ローコード・ノーコードアプリ開発ソリューションを活用すれば、一元的な管理・運用体制を築くための記載内容の基準をできます。これは、インフラ負債・ドキュメント負債の解消に寄与します。

また、公開された脆弱性の自社製品への影響を調べることに時間がかかっている場合は、脆弱性自体の理解（知識的な咀嚼）をし、発生実現性（咀嚼した原理を基にプログラムコードレベルで該当する箇所とセキュリティ機能の有効性）を調べ・改修検討することになります。このような情報収集・理解・論理的判断には、局所的なツールでは本質的な改善には不足しているため、昨今活用価値の期待が高まっている生成 AI/LLM を活用することで、作業コストの低減が可能になります。

ただし、生成 AI の利用においては AI の利用における理解が必要であり、秘匿性の高い開発資産情報を扱うことになるので、クラウドサービス型かオンプレ型の選択、利用価値・目的の設定、期待効果を通じた投資判断が必要になります。こちらはインフラ負債の解消に寄与します。



製造における開発環境の改善は潜在的な課題であり、非常に重要な取り組みになっていくと考えられます。この課題を解消し、改善・捻出されたコストを別事業への取り組みに投入することで、有益な効果が期待できるのではないでしょうか。

著者
3名共著として執筆。
黒澤 俊洋 / 株式会社マクニカ , DX コンサルティング推進室
齋藤 健一 / テュフズードジャパン株式会社 , ビジネスディベロップメントマネージャー
コンシューマープロダクトサービス（CPS）事業本部
下平 真武 / TOPPAN デジタル株式会社 , 事業開発センター カード・IoT ソリューション本部 IoT ソリューション部 セキュアエレメント販促チーム

お問い合わせ
https://www.macnica.co.jp/business/consulting/contact/

〒222-8563 横浜市港北区横浜1-5-5
TEL.045-476-2010 | FAX.045-476-2030

西日本オフィス 〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル14階
TEL.06-6227-6916 | FAX.06-6227-6917

株式会社マクニカ
©Macnica, Inc. ●本資料に掲載されております社名および製品名は、各社の商標および登録商標です。