2019 年 7 月 30 日
独立行政法人情報処理推進機構（IPA）

欧州ネットワーク情報セキュリティ機関（ENISA）
「IoT のセキュリティ標準のギャップ分析」
IoT 分野のセキュリティ/プライバシー要件に対する既存標準のマッピング

This is a translation undertaken by IPA and therefore is not official translation of ENISA.
The official version is in English and on the ENISA site
http://www.enisa.europa.eu/

本文書は、ENISA の文書“IoT Security Standards Gap Analysis”を独立行政法人 情報処理推進機構（IPA）が翻訳したものであり、ENISA による公式の翻訳ではありません。日本語へ翻訳した本文書の著作権は、IPA に帰属します。
本文書は、原文にできるだけ忠実に翻訳するよう努めていますが、完全性、正確性を保証するものではありません。翻訳監修主体である IPA は、本翻訳文書に記載されている情報より生じる損失または損害に対して、いかなる人物あるいは団体にも責任を負うものではありません。原文のありのままの内容を理解する必要のある場合は、ENISA ウェブサイトに掲載されている原文をお読み下さい。

IoT Security Standards Gap Analysis
https://www.enisa.europa.eu/publications/iot-security-standards-gap-analysis

【訳注】
2019 年 6 月 27 日、ENISA の名称が European Union Agency for Network and Information Security（European Network and Information Security Agency）から European Union Agency for Cybersecurity に変更されましたが、*IoT Security Standards Gap Analysis* は名称変更以前に発行された文書であるため、本文書における ENISA の名称の記載は旧名称にて記載しています。

ENISA について

欧州ネットワーク情報セキュリティ機関（European Network and Information Security Agency：ENISA）は、欧州連合（EU）、その加盟国、民間部門およびヨーロッパ市民のためのネットワークおよび情報セキュリティの専門知識を集約している機関である。ENISA はこれらのグループと協力して、情報セキュリティにおけるグッドプラクティスに関するアドバイスや提言を提供している。これは、EU 加盟国が関連する EU 法の実施を支援し、ヨーロッパの重要な情報インフラおよびネットワークのレジリエンスの向上に役立っている。ENISA は、EU 全体のネットワークおよび情報セキュリティの向上に取り組む、国境を越えたコミュニティの発展を支援することによって、EU 加盟国における既存の専門知識の強化を促進している。
ENISA の詳細については、下記ウェブサイトを参照。
www.enisa.europa.eu

連絡先

本文書に関する問い合わせ先：isdp@enisa.europa.eu
本文書に関するメディアからの問い合わせ先：press@enisa.europa.eu

著者

Elżbieta Andrukiewicz
Scott Cadzow
Sławomir Górniak

ISBN: 978-92-9204-275-2, DOI: 10.2824/713380

目次

概要

ENISA は IoT 関連の標準類の状況について予備的な分析を実施しており、その分析結果は、セキュアな IoT を市場に投入するための各標準間には大きなギャップはないことを示している。しかしこれは、IoT エコシステム全体のセキュリティが、これらの標準によってカバーされているということではない。一連の標準には IoT セキュリティに対する全体論的なアプローチの要素は見受けられるが、IoT エコシステム全体を保護する包括的なアプローチを実現するためには、更なる作業が必要とされる。したがって、IoT エコシステムの特殊性（たとえば、非常に高いスケーラビリティ、利用形態、短期間での市場投入、コストの影響など）を考慮して、この調査では IoT 全体に対する特定の解決策を奨励するつもりはない。逆にこの調査では、IoT セキュリティのための既存の標準の状況を明らかにし、マッピングすることによって、IoT をセキュアにするための望ましい改善領域と、更なる追加の取り組みを明確にすることを目的としている。

一般的に、ベンダーが自らの IoT 製品やサービスがセキュアであると主張するためのプロセスには識別可能なギャップがある。標準は相互運用を可能にする、という主張において、セキュアな IoT のための標準の使用・適用に一体性がないという事実は、たとえすべての機器がセキュリティ機能を有効にして市場に投入されたとしても、相互運用性は保証されないということを意味している。

この文書の最も重要な要旨は、「標準は不可欠ではあるが、市場へのオープンアクセスを確保するには十分ではない」、ということである。セキュリティの特定のケースにおいて、市販される機器が確実にセキュアであるということを保証するためには、膨大なプロセスと技術標準を整備する必要がある。この点に関して、本文書では付録 B において、機器認証、サービス認証およびプロセス認証を通じた市場アクセスを可能にするための先駆けとして、何が十分なのかを把握するための認証、保証および検証スキームに向けた理論的アプローチを提案している。標準適用の実行可能性に影響を与える経済的問題などの関連する懸念を考慮に入れていないため、このアプローチは本質的に理論的なものであることに注意していただきたい。

本文書で推奨されるプロセスは、「セキュアな IoT」を市場に投入するための唯一の形態とし、認証、保証テスト、検証、市場調査を通じて市場に信頼を与えることによって、機器のセキュリティに対する態度の変化を生み出すことを目的としている。

本文書の資料の大部分は、既存の標準と要件をマッピングした「付録 A」、および市場認証の技術的基盤を提案した「付録 B」に含まれている。

１．概説

1.1 調査の背景と目的

ENISA は 2017 年に「IoT のベースラインセキュリティに関する提言」を公開した。この提言の目的は、IoT のセキュリティ要件への洞察、重要な資産と関連する脅威のマッピング、起こり得る攻撃の評価、および IoT システム保護のために適用される可能性のあるグッドプラクティスとセキュリティ対策を明らかにすること、であった。

この提言の第 4 節「セキュリティ対策／グッドプラクティス」および付録 A「セキュリティ対策／グッドプラクティス詳細」は、セキュリティとプライバシーに関する要件を定義している。これらの要件は、セキュリティ項目ごとに参照可能な標準でグループ化、分析され、その結果としてマッピングを提供した。

2017 年に、ENISA は https://www.enisa.europa.eu/publications/gaps-eu-standardisation で入手可能なレポート「NIS*標準化におけるギャップ- EU 標準化ポリシーにおける NIS の改善のための勧告」を公開した。同レポートの構造は、このプロジェクトの基礎として考えられている。
*訳注：Directive on security of network and information systems（通称 NIS）

この調査の全体的な目標は、IoT の分野におけるセキュリティとプライバシーに関する要件を既存の標準にマッピングし、ギャップを特定することである。

1.2 調査の範囲

この調査は、ギャップを分析し、標準の採用および NIS 分野における EU 標準化のガバナンスを促進するべく、特に標準の開発や整理に関するガイドラインを提供する。ENISA はこの関係に、利害関係者にとってより適切であるように、また一般的な規制の枠組みへの準拠性をさらに高めるために、NIS の技術的および組織的なノウハウを取り入れている。

欧州のサイバーセキュリティ認証の枠組みの下で運用される新しいサイバーセキュリティ認証スキームに関連する EU のニーズには特別な注意が払われている。このフレームワークはまだ採用されていない[1]が、2018 年末に完成予定である。標準を含む、または要件を含む他の広く採用されている技術仕様が、あらゆる認証活動の基盤となっている。IoT の世界で採用されているセキュリティ評価モデル、方法、手法、およびツールの欧州規格が、IoT セキュリティに関する既存のイニシアチブ、グッドプラクティス、および業界のガイドラインを補完するために早急に必

1 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”)
ENISA（EU サイバーセキュリティ機関」に関する規制の提案（EU 規制 526/2013 の廃止を含む）、および情報通信技術（ICT）のサイバーセキュリティ認証（サイバーセキュリティ法）に関する規制の提案

要とされている。

1.3 関連文書

この調査は以下の文書に基づいている。

[1] ROLLING PLAN FOR ICT STANDARDISATION 2018
https://ec.europa.eu/growth/content/2018-rolling-plan-ict-standardisation-released_en

[2] Baseline Security Recommendations for IoT, Nov 20, 2017
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

1.4 適用される方法論

[2]の付録 A に示す要件と関連標準を組み合わせたマトリクスを作成するために、広く認められているいくつかの標準化団体を調査した。

[1]で得られた IoT の分野における主要な標準化活動の分析に基づいて、マトリクスには以下からのインプットを含めている。
・3 つの欧州標準化機構（ESO）－CEN、CENELEC、特に ETSI TC Cyber
・SC27（IT セキュリティ技術）および SC41（IoT と関連技術）を含む ISO/IEC JTC1 傘下の各 SC（subcommittee）
・ITU-T Y シリーズ勧告：グローバル情報通信インフラストラクチャー（GII）及びインターネットプロトコル側面および次世代ネットワーク

結果は「付録 B：IoT 分野のセキュリティ標準の進化の提案」に示す。

2. 標準規格のギャップ分析

ENISA レポート「IoT のベースラインセキュリティに関する提言」に記載されている要件は、それらの要件を満たすことができる既存の標準にマッピングされている。要件ごとの詳細なマッピングは付録 A に示す。

簡素化された分析によって、すべての要件が既存の標準によって満たすことが可能で、標準間に大きなギャップはないことが判明した。問題は、これが正しい答えでも期待された答えでもないことである。標準は、機器またはサービスを構成する様々な要素のために存在する。ただし IoT に関しては、機器とサービスだけでなく、エコシステムも関係する。さらに IoT の利用形態、高いスケーラビリティおよびその他の特殊性により、その領域はさらに複雑になり、より一般的で柔軟なアプローチが要求される。したがって、セキュリティに関する各 IoT 機器標準間のギャップを例にとると、ユーザを認証し、送信データを暗号化し、受信データを復号でき、完全性の証明を提供または検証できる機器を市場に投入できたとしても、各標準が総体的に扱われていないため、その機器はセキュアではないだろう。同様に、IoT 製品またはサービスを開発している組織は、ISO/IEC 27000 シリーズなどの管理ガイドラインで定義されている開発プロセスを規定しているかもしれないが、それでもセキュアでない製品を提供している。

規制当局およびサプライヤにとっての課題は、セキュアな IoT 機器のみを市場に投入することであり、これには動的な IoT エコシステムの性質に十分対応できる柔軟性を持ったアプローチが必要である。そして、憶測となるかもしれないが、これから数年で社会がどのようになるかを想像し、その時の社会への脅威を考慮するという挑戦が必要となる。ICT はより多くの接続性、ICT を利用した日常生活のさらなる増大を伴って社会の中に益々浸透すると見込まれており、これには ICT とサイバーセキュリティの対応が求められる。しかしながら、今後数年の間に想定される懸念は、セキュリティ技術だけの範疇をはるかに超えて広がっており、本文書における多くの提言は、ICT、特にサイバーセキュリティを組み込んだ ICT が日常生活に与える影響についての社会的理解を深めることにまで及んでいる。

本書の IoT セキュリティのセキュリティ要件のチェックリストと特定の標準へのマッピングは、総合的で効果的な IoT セキュリティへの出発点として役立つが、IoT エコシステムの複雑さには、より柔軟なアプローチが求められることに注意してほしい。競争力やイノベーションを妨げないように、順応性のある、コンテキストベース／リスクベースのソリューションを要する根本的な技術的課題だけでなく、IoT 市場の制約も考慮する必要がある。

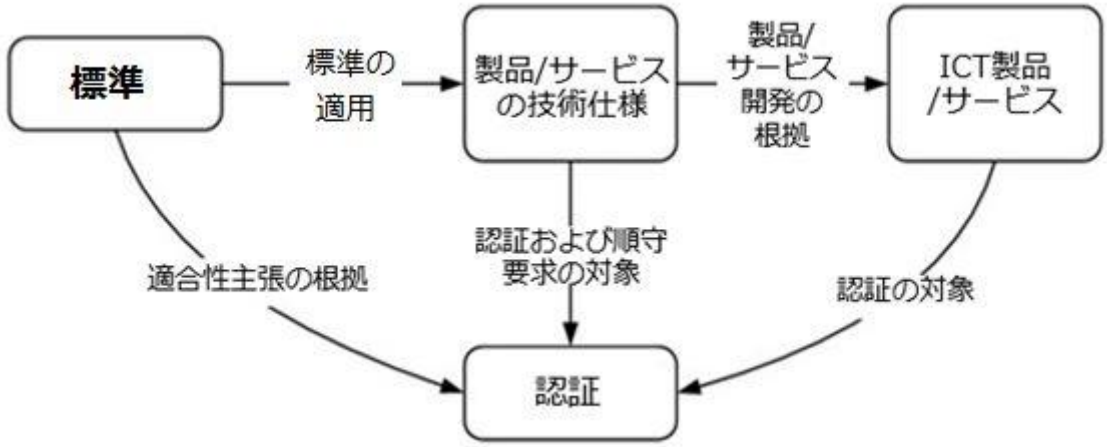
3. 認証の機会

市場の観点から見た標準の全体的な目的は、それが何を達成しようとしているのかによって 2 つの要素、（1）相互運用性、および（2）信頼性から成る。

相互運用性を達成する上での標準の従来の役割は付録 A である程度議論されており、ここでは繰り返さない。

「信頼」の領域における標準の役割はあまり明確に定義されておらず、セキュリティの文脈において簡単な言葉で述べるのは困難である。IoT に関しては、個々の機器だけを考慮すべきではなく、IoT が内在的に持つ機器、サービス、人、プロセス、およびデータの固有の接続性と相互依存性により、全体的なアプローチが求められる。したがってこれは、暗号化のように、機器がどの標準に準拠しているかについての比較的クローズドな見解とは対照的に、機器の役割に関するより包括的な見解を要することを意味する。

標準は、ある種類の製品の特定のコンテキストでの技術仕様を開発するために使用でき、製品のセキュリティ評価のためのフレームワークを提供する。このような一般的な概念を下図に示す。



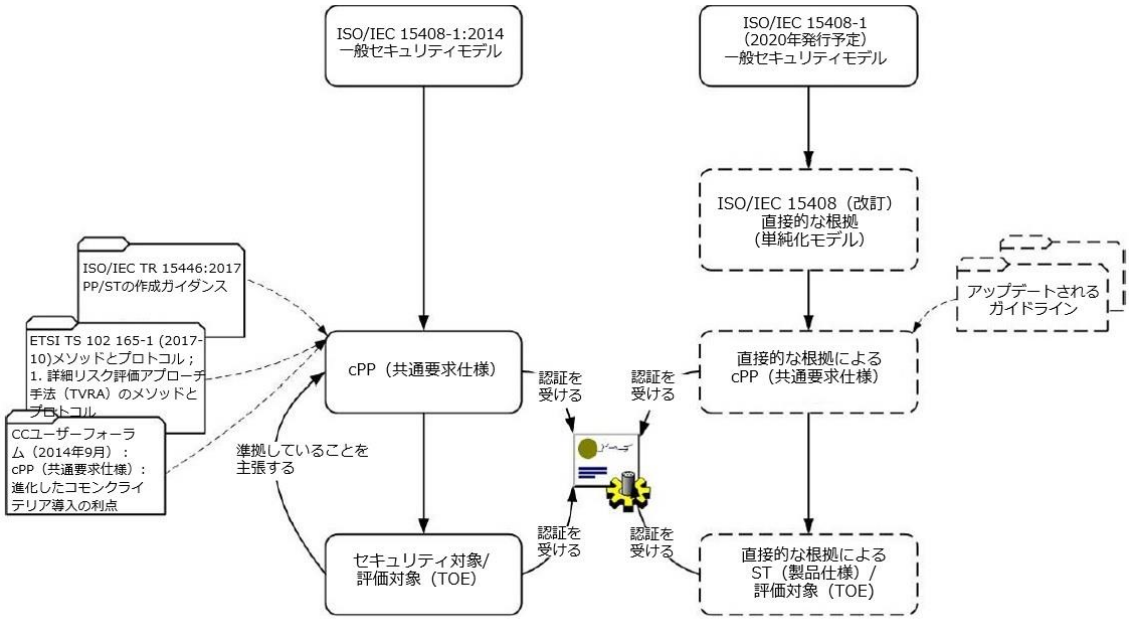
代表的なユースケースの例として、ここでは「コモンクライテリア」（CC）として広く知られている、国際標準 ISO/IEC 15408 IT セキュリティの評価標準について説明する[2]。CC は次の 3 つの部分から構成されている。

- パート 1：概説と一般モデル
- パート 2：セキュリティ機能要件
- パート 3：セキュリティ保証要件

2 これは例示的なものであることを強調しておく必要がある。したがって、CC の使用に対して、または IoT ドメインでの他の標準の使用に対しての優先を意味するものではない。これには、経済に関するものも含め、すべての関連する側面および詳細を考慮に入れた、さらに徹底的な分析が必要である。

パート 1 で説明されるセキュリティモデルに基づいて、CC で言うところの、製品の種類に応じたセキュリティ要求仕様（PP：プロテクションプロファイル）、または特定の製品のセキュリティ仕様（ST：セキュリティターゲット）と呼ばれる技術仕様を開発できる。それらの仕様は、CC のパート 2 で規定された正式な分類法によるセキュリティ要件を含み、同時に CC のパート 3 で規定されたセキュリティ保証コンポーネントを使用することによって評価要件を作成する。

PP/ST から cPP（国際的なプロテクションプロファイル）へ、そして Common Criteria グループから提案された「直接的な根拠（Direct Rationale)」アプローチへの CC の進化は、セキュリティ、すなわち信頼性についてのより広範囲で全体的な見方の枠組みを提供する。「直接的な根拠」アプローチは、従来のものよりも単純な、製品のための包括的なセキュリティ仕様を作成する方法を提供しており、IoT 分野における優れた技術仕様の整備に用いることができる、また同時に、製品がセキュリティ要件を満たしているという、確かで裏付けされた自信に根拠を与える。



IoT のセキュリティに対する市場の信頼を高める機会は、ICT セキュリティを開発するすべての標準化団体に提案するためにコモンクライテリアの進化の中で行われてきた取り組み（付録 B を参照)、cPP への取組みや、直接的な根拠に基づく cPP 開発への取り組み、等から生じ得る。

明らかに IoT に関しては、CC のユースケースの例を検討するこができる。前述のように、IoT 環境では柔軟で適応性のあるソリューションへの要求が高まっている。しかし、完全な分析はこのレポートの範囲外とする。

現在、テスト可能で、セキュリティ保証の証明として認証チェーンで利用されるような標準を開発する機会がある。控えめな主旨は、標準に準拠し、その標準が適切に維持されていれば、適合性は十分であるということである。分かり難いのは、セキュリティ保証を証明するには多くの標準に準拠する必要があるということである。

付録 A　要件と標準のマッピング

A.1 標準化の役割

A.1.1 一般的な概要

IoT 機器に関して標準の役割を広く一般化すると、それは「モノ」の相互運用性を提供すること、ということである。また、標準は満たすべき要件を提示するが、要件を実装する方法についての指示を提示しない。これらは、広義の解釈としてセキュリティ標準に適用されるが、この解釈は、多くのセキュリティ標準、またはより多くの場合標準で定義されたセキュリティ機能は、敵対する当事者による攻撃を受けたときの「モノ」の相互運用性の保証を与える、という若干の修正と共に適用される。したがって標準は、機能（例えば暗号化アルゴリズム）、その機能の適用（例えば特定の暗号化モードの使用（カウンタモード等））、およびその機能を使用する状況（例えば機密保護サービスの提供への暗号化の適用）に対処している。

相互運用のために暗号技術を用いたセキュリティを用いる事業者は、鍵とアルゴリズムを含む知識と機能を共有することも求められる。したがってセキュリティ標準は、適切な方法でセキュリティ侵害に対応するために、シンプルな機械的相互接続、意味上・構文上の共通の意味、および属性と組織の管理について取り上げていなければならない。

A.1.2 組織の相互運用性

セキュリティにおける組織管理の標準には「Need to Know」(情報は知る必要がある者にのみ与える)を強化しようとする組織内の役割を定義するクラスがある。セキュリティの観点からは、2 つの組織が共通の Communications Security（ComSec）フレームワークを使用してデータを安全に転送する場合、ComSec 交換では転送前または転送後にデータがどう扱われるのか推測できない。したがって、送信側組織と受信側組織のローカル IT セキュリティポリシーは同レベルのものだと信頼され、この信頼は外的手段によって強化できる。

A.1.3 構文上の相互運用性

構文（syntax）という言葉は、順序付けと配列を意味するギリシャ語の単語に由来する。主語－述語－目的語（SVO）の英語の文構造は構文の単純な例であり、一般に構文は形式言語において、基本的な記号の集合から成る適格な表現を可能にする規則の集合である。コンピュータ・サイエンスにおいて、構文はデータの標準的な構造を指す。構文上の相互運用性を実現するためには、記号のセットと記号の順序についての共通の理解が必要となる。どの言語でも記号には制約があるので、一般に動詞は、例えば名詞として間違って解釈されてはならない。（とはいえ通常使用になった誤用の例もある。例えば、従来の「He won a medal」という文意において動詞としての「medal」の使用は現在「He medalled」というように誤用されている。）

A.1.4 セマンティック相互運用性

構文は意味を伝えることができないため、セマンティック（意味論）が導入される。セマンティックは、構文的に正しい文から意味を導き出す。セマンティックの理解自体は語用論と文脈の両方に依存している。セマンティックコンテンツの可用性と文脈上の知識の伝達の最適化を成功させることは、データの構造化にかかっているが、セマンティック情報を交換する方法はいくつかある（語用論の伝達はあまり明確ではない）。構文的に正しい情報に意味を持たせる仕組みの最も明白な例は、例えば認証プロトコルのような、メッセージセットにコンテキストを与えるプロトコルである。プロトコルは、コンテキストを識別する手段として共有の状態の概念を使用してさらに拡張することができ、このような拡張はしばしばプロトコルに埋め込まれる（例えば、認証プロトコルは、「認証済み」状態になる前に「識別」、「チャレンジ発行」、およびの「応答保留」を含む状態を通過する可能性がある）。

A.1.5 電気的および機械的相互運用性

例えば、IEC 60906-2 規格の電源コネクターを持つ装置は、IEC 60906-2 規格のコネクターからのみ電力を受け入れる。同様に、たとえば、USB-Type-A に準拠したシリアルポートは、USB-Type-C のリード線に接続できない。単純な機械的適合性に加えて、電気的相互運用性を保証するための、電圧レベル、アンペア数レベル、DC または AC、AC の場合の周波数、変動レベルなどの要件がある。

A.1.6 無線通信の相互運用性

無線通信は、周波数帯域、変調方式、符号レート、電力などについての共通の知識を必要とする。一般に、無線通信はブロードキャストで信頼性が低いと見なすことができる。物理メディアの性質上、無線プロトコルではリンクの信頼性を最大限高めるための対策が必要である。ほとんどの場合、リンク層（OSI スタックのレイヤー2）でさまざまな形式の前方誤り訂正（FEC）を使用して達成される。

A.2 標準化のギャップ

標準を策定する機関は非常に多いが、ほとんどのサービスプロバイダ、製造業者、および政府がそれらのかなりの数に関与していることも認識されている。残念ながら、これはまた、各標準化団体が互いに競合しているため、内容に重複があることを意味し、それ自体がセキュリティに対するリスクとなる。

主旨:各標準間のギャップは、更なる標準化活動によって軽減できる可能性があるリスクを示す。

しかし、標準化活動の重複は、更なる標準化活動では軽減できないが、合意による整理または既存の標準の改訂によって軽減できる可能性があるリスクを示している。

表 A.1：要件と現行標準のマッピング

要件 ID	内容	要件をサポートする標準
セキュリティ・バイ・デザイン		
GP-PS-01	機器/アプリケーションの設計と開発のすべてのレベルにわたるライフサイクル全体を通して、開発、製造、および展開全般にわたるセキュリティを統合し、一貫した総合的なアプローチで IoT システム全体のセキュリティを検討する。	ISO/IEC 30141 11.3.3 ITU-T Y.4806 モノのインターネットの安全を支えるセキュリティ機能
GP-PS-02	様々なセキュリティポリシーと技術を統合できる能力を確保する。	ISO/IEC 30141 11.3.2
GP-PS-03	セキュリティは人間の安全に対するリスクを考慮しなければならない。	ISO/IEC 30141 11.2
GP-PS-04	省電力のための設計によって、セキュリティが侵害されてならない。	該当なし
GP-PS-05	区画を分けたアーキテクチャを設計し、攻撃に備えて、要素をカプセル化する。	ISO/IEC 30141 11.3.2
GP-PS-06	IoT ハードウェアメーカーと IoT ソフトウェア開発者は、製品が期待どおりに機能するかどうかを検証するためのテスト計画を実施する必要がある。 侵入テストは、不正な形式の入力処理、認証回避の試み、および全体的なセキュリティ対応の特定に役立つ。	ISO/IEC 15408-3（ATE および AVA クラスの説明） 文書化されたセキュリティ要求に対する自律保証テストによって部分的に対応でき得る。 侵入テストの役割は、法律で禁止されている、または制限されていることがよくある（例：コンピューター悪用法）。

要件 ID	内容	要件をサポートする標準
GP-PS-07	IoT ソフトウェア開発者は、製品の最終バージョンのバグを減らすのに役立つので、開発中にコードレビューを行うことが重要である。	ISO/IEC 15408-3（ATE クラスの説明） これは標準に直接マップされていないが、コードレビューを強制する可能性のある品質保証がある。さらに、多くのコーディング実施ガイドラインでは、コードレビューを実施する手段を明確に取り上げており、多くのフレームワークでは、コードレビューを実施する時期を明確に特定している。 Apple secure development guidelines *https://developer.apple.com/library/content/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html* Microsoft Security Development Lifecycle (SDL) *https://www.microsoft.com/enus/sdl* Open Software Assurance Maturity Model (SAMM) *http://www.opensamm.org* Building Security in Maturity Model (BSIMM), incorporating the SSDL method *https://www.bsimm.com*
注意： 上記のそれぞれ、特に GP-PS-05 と GP-PS-07 には、特定の開発者環境向けのベストプラクティスガイドラインがいくつかある。		
プライバシー・バイ・デザイン		
GP-PS-08	プライバシーをシステムの不可欠な部分とする。	ISO 29550
注：プライバシーの侵害は、その侵害を実行する少なくとも 1 人の行為者を必要とすることに注意。適用時にデータ保護影響評価（DPIA）を実施するという GDPR（EU 一般データ保護規則）の勧告は、侵害を、適用されたあらゆる措置の明示的な破綻、またはシステムの末端にいる行為者による特定の行動に限定する。		
GP-PS-09	新しいアプリケーションを公開する前にプライバシー影響評価を実施する。	ISO/IEC 27005、ISO/IEC 29134 ISO/IEC 27005 は、プライバシー影響評価（PIA）を実施する方法を定義。GDPR は DPIA / PIA の実施を求めていることに注意。
GP-PS-10	主要なネットワークおよび情報システムの資産管理手順および構成管理を確立し維持する。	ETSI TS 103 305（CIS からの制御による） ISO/IEC 27002 の 8.1 は、ISO/IEC 27002 の他の部分を含む管理の選択に適用することができる。 ISO 55000 アセットマネジメント

要件 ID	内容	要件をサポートする標準
GP-PS-11	多層防御アプローチを使用した重大なリスクを特定する。	以下のような軍事規格が適用できる。一般に、セキュリティの専門家の間で受け入れられているベストプラクティスだが、多層防御アプローチを定義している標準はない。
https://www.iad.gov/iad/customcf/openAttachment.cfm?FilePath=/iad/library/iaguidance/archive/assets/public/upload/Defense-in-Depth.pdf&WpKes=aF6woL7fQp3dJiLgJBSABf7qwgxHD5mzFWdTgW		
GP-PS-12	既定の IoT 機器の使用目的と環境を明確にする。	セキュリティ評価の範囲を定義する際のリスク分析の策定に必要（ISO/IEC 15408-1 および ISO/IEC 15408-2 の ToE）。 （近日公開される）ETSI TS 103 645 を含むいくつかの IoT ベストプラクティスに記載。
組織的、人的、運用的対策		
GP-OP-01	IoT 製品の寿命末期に関する戦略を策定する。	ISO/IEC 30141 の 11.3.3（IoT システムおよび製品のセキュリティライフサイクル参照モデル）TS 103 645 および ETSI TR 103 533 で記載。
GP-OP-02	（製品の保証を超えた）セキュリティおよびパッチサポートの実施期間および終了時期を開示する。	ISO/IEC 30141 の 11.3.3（IoT システムおよび製品のセキュリティライフサイクル参照モデル）TS 103 645 および ETSI TR 103 533 で記載。
GP-OP-03	パフォーマンスと既知の脆弱性のパッチを、製品ライフサイクルの「サポート終了」期間まで監視する。	ISO/IEC 30141 の 11.3.3（IoT システムおよび製品のセキュリティライフサイクル参照モデル）TS 103 645 および ETSI TR 103 533 で記載。
GP-OP-04	科学団体などで認められている実績のあるソリューション、すなわちよく知られている通信プロトコルおよび暗号アルゴリズムを使用する。カスタム暗号アルゴリズムなどの特定の独自の解決策は避けるべきである。	ISO/IEC 27002 10 ISO/IEC 11770（かぎ（鍵）管理） 一連の標準 ISO/IEC 29192（軽量暗号化 - 全 7 部、アルゴリズムとプロトコルをカバー） 標準では特に取り上げられていない。その理由は、設計上の標準は実証済みのソリューションに基づいて構築されており、標準への準拠がこれに対処していることになるため。
GP-OP-05	セキュリティインシデントを分析および対処するための手順を確立する。	ISO 27002 16 TS 103 645 および ETSI TR 103 533 に記載。

要件 ID	内容	要件をサポートする標準
GP-OP-06	脆弱性の組織な開示。	ISO/IEC 30111（TS 103 645 および ETSI TR 103 533 で対応） さらに、Common Vulnerability Handling Process の使用および開示（ISO/IEC 29147（脆弱性の開示））が該当。
GP-OP-07	情報共有プラットフォームに参加して、脆弱性を報告し、パブリックおよびプライベートパートナーから現在のサイバー脅威および脆弱性に関するタイムリーかつ重要な情報を入手する。	ISO/IEC 27002 6.1.3 ISO/IEC 27002 6.1.4 TS 103 645 および ETSI TR 103 533 で記載。 さらに、Common Vulnerability Disclosure（ISO/IEC 29147）の使用が該当。 また多くの CERT フレームワークの一般的な使用が期待される規制文書（GDPR、NIS、…）に記載。
GP-OP-08	脆弱性報告のための公開されたメカニズムをつくる。(例) バグバウンティ<tba>プログラム	ISO/IEC 30111（脆弱性処理プロセス）および ISO/IEC 29147（脆弱性の開示）TS 103 645 および ETSI TR 103 533 に記載。 一部のベンダーは金銭的インセンティブを提供しており、これは考慮すべき（金銭的インセンティブが提供されるならば、バグハンターはそのようなインセンティブが適用されない場合よりももっと動機づけられるかもしれない）。
GP-OP-09	プライバシーとセキュリティを促進する従業員の活動を実施する - プライバシーとセキュリティのグッドプラクティスについて従業員を訓練する。	ISO/IEC 27002 の 7.2
GP-OP-10	プライバシーとセキュリティのトレーニングを文書化し監視する。	活動 ISO/IEC 27002 の 7.2.2
GP-OP-11	すべての従業員に対するサイバーセキュリティの役割と責任が確立されていることを確認し、プロジェクトの特性とセキュリティエンジニアリングのニーズに応じた人員配置を実施する。	ISO/IEC 27002 の 7.2.1
GP-OP-12	第三者によって処理されたデータは、データ処理契約によって保護されている必要がある。	ISO/IEC 27002 の 13.2.4、15

要件 ID	内容	要件をサポートする標準
GP-OP-13	製品機能の使用またはサービス運用が特に要求されている、または制限されていない場合に限り、消費者の明確な同意を得て消費者の個人データを第三者と共有すること。	ISO/IEC 27002 の 18.1.4 これは GDPR の重要な制約であり、データの合法的な処理に関する第 6 条に具体的に記載されている。
GP-OP-14	IoT ハードウェアメーカーおよび IoT ソフトウェア開発者は、サイバーサプライチェーンのリスク管理ポリシーを採用し、サイバーセキュリティ要件をサプライヤおよびパートナーに伝達することが必要である。	ISO/IEC 27002 の 15
技術的対策		
GP-TM-01	ハードウェアベースの変更不可能な信頼の基点（root of trust）を採用する	TCG からの TPM（ISO/IEC 11889 として公開） ETSI SCP の SIM
GP-TM-02	機器の防御と完全性を強化するために、セキュリティ機能を組み込んだハードウェアを使用する。たとえば、トランジスタレベルでセキュリティを統合したセキュリティチップ/コプロセッサを組み込んだプロセッサを用いて、信頼できるストレージを提供するなどして、機器 ID と認証手段、保管時および使用中の鍵の保護、および特権のない者によるセキュリティ上重要なコードへのアクセスの防止などを保証する。 ローカルおよび物理的な攻撃は、機能的なセキュリティによって防御されている。	TCG からの TPM（ISO/IEC 11889 として公開）
GP-TM-03	他のソフトウェアまたは実行可能プログラムへの信頼を保証するには、その前にブート環境で信頼を確立する必要がある。	セキュアブート、TCG で定義（ISO/IEC 11889 として公開）
GP-TM-04	機器にとって安全なものとして署名した後に改ざんされていないことを保証するために、暗号技術を用いて署名する。コードが読み込まれた後に悪意のある攻撃によって上書きされないように、ランタイム保護と安全な実行監視を実装する。	一連の標準 ISO/IEC 29192-5 および-6（軽量暗号 - 第 5 部：ハッシュ関数、第 6 部：メッセージ認証コード（MAC）、ITU-T X.1362 IoT 環境用の簡単な暗号化手順

要件 ID	内容	要件をサポートする標準
GP-TM-05	認証されていないソフトウェアやファイルがオペレーティングシステムにロードされるのを防ぐために、ソフトウェアのインストールを制御する。	ISO/IEC 27002 の 12.6.2。 これは、ロード時の検証、ブート時の検証、および実行時の検証を含む手法でカバーされています。これらの技術の多くは TPM（ISO/IEC 11889 として公開）に基づく。 さらに、ETSI GR NFV-SEC-007 はこのトピックに関する幅広いガイダンスを提供。
GP-TM-06	セキュリティ侵害が発生した後、またはアップグレードが成功しなかった場合に、システムをセキュアな状態に戻すことができるようにする。	ISO/IEC 27002 の 12.3
GP-TM-07	信頼および信頼関係を表現し管理することができるプロトコルとメカニズムを使用する。	一般的に暗号技術を用いた信頼には、X.509 で定義されたメカニズムを、TLS のような X.509 証明書を転送する追加のプロトコルメカニズムと共に適用する。
GP-TM-08	適用可能なセキュリティ機能はすべてデフォルトで有効とし、未使用または安全でない機能はデフォルトで無効にする必要がある。	ISO/IEC 15408-1 および-2 TS 103 645 および ETSI TR 103 533 で記載。 デフォルトでセキュアなアプローチが選択されている場合、安全でない機能は存在しないため無効にする必要はない。
GP-TM-09	解読しにくい、機器固有のデフォルトパスワードを設定する。	ISO/IEC 27002 の 9.2.4。デフォルトのパスワードの使用は避けなければならないため、これは推奨される方法ではない。 TS 103 645 および ETSI で対処 TR 103 533
GP-TM-10	個人データは、公正かつ合法的に収集および処理される必要がある。データ対象者の同意なしに収集および処理されてはならない。	ISO/IEC 27002 18.1.4 ISO/IEC 29100 ISO/IEC 29184 オンラインのプライバシーに関する通知と同意 ISO/IEC 30141 の 11.4（プライバシーと PII 保護）。これは GDPR の前提条件（第 6 条が適用される）。 同意に関しては、第 6 条のすべての部分が適用されるわけではない（同意が合法的な処理を可能にする唯一の道ではない）。

要件 ID	内容	要件をサポートする標準
GP-TM-11	個人データを収集時に明示した目的に使用していること、今後も収集時に明示した目的以外に使用しないこと、およびデータ対象者に十分な情報を提供していることを確認する。	これは GDPR の前提条件。 ISO/IEC 29100
GP-TM-12	収集して保持するデータを最小限にする。	これは GDPR の前提条件。 ISO/IEC 29100
GP-TM-13	IoT の利害関係者は EU の一般データ保護規則（GDPR）に準拠している必要がある。	標準化は適用されない。
GP-TM-14	IoT 製品およびサービスのユーザは、情報への各種権利、アクセス、消去、修正、データの移植性、処理の制限、処理への異議を行使でき、それらの権利は自動処理よって判断されてはならない。	GDPR ISO/IEC 29100 ISO/IEC 30141 11.4 （ea：特定されるべき他の PII [個人識別情報] 規格） 特定の標準規格は適用されない。これに対処する GDPR からの義務があり、いくつかの ETSI ベストプラクティスが策定されている。
GP-TM-15	システムと運用上の停止を念頭に置いて設計し、システムが容認できないほどの損傷のリスクや物的損害の危険を引き起こさないようにする。	ISO/IEC 27002 17.1.1
GP-TM-16	自己診断のメカニズム、および故障、機能不全、または侵害された状態から自己回復/回復するためのメカニズム。	ISO/IEC 27031（事業継続のための情報通信技術の準備に関するガイドライン）
GP-TM-17	スタンドアロン操作を保証する - 重要な機能は、通信が喪失しても、また侵害された機器やクラウドベースのシステムからの悪影響を受けながらも引き続き機能するべきである。	ISO/IEC 27031（事業継続のための情報通信技術の準備に関するガイドライン） デフォルトでは、IoT 機器はスタンドアロンモードでは動作できず、インターネットに接続されるように設計されている。これにより、IoT 機器に新しいモードが導入された。

要件 ID	内容	要件をサポートする標準
GP-TM-18	機器ソフトウェア/ファームウェア、それらの設定およびアプリケーションが、無線（OTA）でアップデートできる機能を保証する。即ち、アップデートサーバがセキュアであること、アップデートファイルがセキュアな接続を介して送信されること、機密データ（例えば、ハードコードされた資格情報）が含まれていないこと、承認された信頼できる機関によって署名され、容認された暗号化方法を使用して暗号化されていること、またアップデートパッケージがデジタル署名されていること、署名用証明書およびその証明書チェーンなどが、アップデート・プロセスが実行される前に機器によって検証されること。	TS 103 645 および ETSI TR 103 533 で記載。
GP-TM-19	自動ファームウェアアップデートメカニズムを提供する。	ETSI などからのベストプラクティスガイダンスに記載
GP-TM-20	ファームウェアアップデートの下位互換性。自動ファームウェアアップデートでは、ユーザに通知することなく、ユーザ固有の設定、セキュリティ設定やプライバシー設定を変更しないことが望ましい。	ETSI などからのベストプラクティスガイダンスに記載。
GP-TM-21	システムレベルの脅威モデルに基づいて、（機器ごとに固有の）認証および承認スキームを設計する。	ISO/IEC 29192 CD 軽量暗号化 - パート 7：ブロードキャスト システム全体の脅威分析が必要。そのような脅威分析へのアプローチは ETSI TS 102 165-1、ISO27000 シリーズ、ISO15408 シリーズ、そして特定のセクターのための他のものを含む。 認証プロトコルおよび認証方式のフレームワークは、ETSI TS 102 165-2 および ISO/IEC 29115 に記載。
GP-TM-22	デフォルトのパスワード、さらにデフォルトのユーザ名も初期セットアップ中に変更させること。また、弱いパスワード、null パスワード、または空白のパスワードを許可しないこと。	ISO/IEC 27002 9.2.4、 ISO/IEC 27002 9.4.2 ISO/IEC 27002 9.4.3 TS 103 645 および ETSI TR 103 533 で記載。

要件 ID	内容	要件をサポートする標準
GP-TM-23	認証メカニズムでは、強力なパスワードまたは個人識別番号（PIN）を使用しなければならない。また、証明書に加えて、スマートフォン、バイオメトリクスなどの二要素認証（2FA）または多要素認証（MFA）の使用を検討することが望ましい。	ISO/IEC 19790 暗号モジュールのセキュリティ要件
GP-TM-24	認証用証明書は、ソルトを用い、ハッシュ化と暗号化の両方またはいずれかを行わなければならない。	ISO/IEC 19790 暗号モジュールのセキュリティ要件
GP-TM-25	「ブルートフォース（総当たり攻撃）」やその他の悪意のあるログイン攻撃から保護する。この保護では、機器に格納されている暗号鍵も考慮することが望ましい。	ISO/IEC 19790 暗号モジュールのセキュリティ要件
GP-TM-26	パスワードの回復またはリセットメカニズムが堅牢であり、有効なアカウントを示す情報を攻撃者に提供しないこと。これらは、鍵更新メカニズムおよび鍵回復メカニズムにも当てはまる。	ISO/IEC 19790 暗号モジュールのセキュリティ要件
GP-TM-27	きめ細かい認可メカニズムを実装し、最小特権の原則（POLP）を使用して、特定のシステムに許可されるアクションを制限する。アプリケーションは可能な限り低い特権レベルで動作しなければならない。	標準なし。ベストプラクティスの要件
GP-TM-28	機器ファームウェアは、特権コード、プロセス、およびデータを、それらにアクセスする必要がないファームウェアの部分から分離するように設計することが望ましい。機器ハードウェアは、特権のないユーザがセキュリティ上重要なコードにアクセスするのを防ぐための分離の概念を提供することが望ましい。	標準なし。ベストプラクティスの要件
GP-TM-29	データの完全性と機密性は、アクセス制御によって実施しなければならない。アクセスを要求している対象者が特定のプロセスへのアクセスを許可されている場合、定義されたセキュリティポリシーを実施する必要がある。	ISO/IEC 27002 9
GP-TM-30	さまざまなレベルの重要性を反映したコンテキストベースのセキュリティとプライバシーを確保する。	ISO/IEC 27002 8.2

要件 ID	内容	要件をサポートする標準
GP-TM-31	タンパーに対する保護および検出手段。ネットワーク接続性に依存せずに、ハードウェアタンパーの検出とリアクションができることが望ましい	ISO/IEC 19790 暗号モジュールのセキュリティ要件
GP-TM-32	機器を容易に分解できないこと、およびデータ記憶媒体が保管時に暗号化されており、容易に取り外すことができないこと。	ISO/IEC 19790 暗号モジュールのセキュリティ要件、ITU-T Y.4415 参照 IoT 機器機能公開のためのアーキテクチャ
GP-TM-33	機器が機能するために必要な重要な物理的外部ポート（USB など）のみを備えていること。また、テスト/デバッグモードが安全であること。それによって、機器に悪意のあるアクセスができないようにする。一般的には、信頼できる接続だけが物理ポートに接続できるようにする。	ISO/IEC 15408-2（さらに詳細調査要）
GP-TM-34	転送中および保管中のデータおよび情報（制御メッセージを含む）の機密性、信頼性、および/または完全性を保護するために、暗号技術を適切かつ効果的に使用する。標準かつ安全な暗号化アルゴリズムと安全な鍵を適切に選択し、セキュアでないプロトコルを無効化する。実装の堅牢性を検証する。	ISO/IEC 27002 10
GP-TM-35	暗号鍵はセキュアに管理しなければならない。	GP-Op-04 を参照
GP-TM-36	軽量暗号化およびセキュリティ技術と互換性があるように機器を構築する。	GP-Op-04 を参照
GP-TM-37	スケーラブルな鍵管理スキームをサポートする。	対応する標準なし。ベストプラクティス要件。
GP-TM-38	ネットワーク上で転送される情報、または IoT アプリケーションやクラウドに保存される情報のさまざまなセキュリティ側面（機密性 [プライバシー]、完全性、可用性、および信頼性）を保証する。	ISO/IEC 27002 5 ISO/IEC 27034（アプリケーションセキュリティ） ISO/IEC 27033（ネットワークセキュリティ） ISO/IEC 27040（ストレージセキュリティ） ISO/IEC 27017（クラウドサービス用 27002）
GP-TM-39	暗号化用の TLS など、最新の標準化されたセキュリティプロトコルを使用して、通信セキュリティを提供する。	対応する標準なし。ベストプラクティス要件。

要件 ID	内容	要件をサポートする標準
GP-TM-40	認証情報が内部または外部ネットワークトラフィックに公開されていないこと。	ISO/IEC 15408-2 （さらに詳細調査要）
GP-TM-41	データ送信からデータ受信までの信頼できる交換を可能にするためにデータの信頼性を保証する。データをキャプチャして保存する場合は、いつでもどこでも、常に署名することが望ましい。	ISO/IEC 15408-2（さらに詳細調査要）
GP-TM-42	受信したデータを信頼せず、常に相互接続を検証する。信頼を確立する前に、ネットワークに接続されている機器を発見、識別、検証/認証し、信頼性の高いソリューションとサービスのためにそれらの完全性を維持する。	ISO/IEC 15408-2（さらに詳細調査要）
GP-TM-43	IoT 機器は、通信を許容するのではなく、制限することが望ましい。	ベストプラクティスの要件
GP-TM-44	必要な接続のみ確立する。プロトコルのすべてのレベルにおいて、製品または製品が接続されている他の機器への不正な接続を防止する。	ISO/IEC 15408-2（さらに詳細調査要）
GP-TM-45	接続を制限するために、特定のポートやネットワーク接続を無効にする。	ISO/IEC 15408-2（さらに詳細調査要）
GP-TM-46	レート制限。自動化された攻撃のリスクを低減するためにネットワークを経由で送受信されるトラフィックを制御する。	対応する標準なし。ベストプラクティス要件。
GP-TM-47	リスクセグメンテーション。セキュリティ侵害を隔離し、全体的なリスクを最小限に抑えるために、ネットワーク要素を個別のコンポーネントに分割する。	ISO/IEC 27033 ネットワークセキュリティ（6 部）
GP-TM-48	プロトコルは、単一の機器が侵害されても、それがセット全体に影響を及ぼさないように設計することが望ましい。	対応する標準なし。ベストプラクティス要件。
GP-TM-49	単一の機器の侵害が他の製品ファミリを危険にさらすことにつながるため、製品ファミリ全体で同じ秘密鍵を導入しないこと。	ISO/IEC 15408-2（さらに詳細調査要）
GP-TM-50	必要なポートだけが公開されて使用可能になっていること。	対応する標準なし。ベストプラクティス要件。
GP-TM-51	DDoS 耐性および負荷分散インフラストラクチャを実装する。	対応する標準なし。ベストプラクティス要件。

要件 ID	内容	要件をサポートする標準
GP-TM-52	Web インターフェースが機器からバックエンドサービスまでのユーザセッションを完全に暗号化し、XSS、CSRF、SQL インジェクションなどの影響を受けないようにする。	対応する標準なし。ベストプラクティス要件。
GP-TM-53	エラーメッセージを設計するときは、セキュリティ問題が発生しないようにする。	ISO/IEC 15408-22（さらに詳細調査要）
GP-TM-54	データ入力検証（使用前にデータが安全であることの確認）および出力フィルタリング。	ISO/IEC 15408-22（さらに詳細調査要）
GP-TM-55	ユーザ認証、アカウントとアクセス権の管理、セキュリティ規則の変更、およびシステムの機能に関連するイベントを記録するログシステムを実装する。ログは永続的なストレージに保存され、認証された接続を介して取得可能でなければならない。	ISO/IEC 15408-2（さらに詳細調査要）
GP-TM-56	定期的な監視を実施して、機器の動作を検証し、マルウェアを検出し、完全性エラーを発見する。	対応する標準なし。ベストプラクティス要件。
GP-TM-57	セキュリティ制御の有効性を確認するために、定期的な監査とレビューを実施する。少なくとも 2 年に 1 回はペネトレーションテスト（侵入テスト）を実行する。	ISO/IEC 27002 12

付録 B　IoT 分野のセキュリティ標準の進化の提案

B.1 導入

本文書の本文で示唆されているように、製品、サービスまたはシステムに標準が適用される際に、どの標準の組み合わせがセキュアな IoT をもたらすかが明確でない限り、各標準間にはギャップが存在する。以下に提示する提案は、IoT 製品・サービスに認定マークを付けるプロセスの開発についてである。これは、IoT 製品が合理的に期待される程度にセキュアであることを市場に保証するものである。このプロセスがどのように機能するかの例として、コモンクライテリア（ISO/IEC 15408 で標準化されている）の場合を考える。この例は、CC が IoT の文脈において最適または好ましい手法であることを意味するのではなく、一般的なプロセスを説明するための例としてのみ役立つことに留意されたい。

したがって全体的な概念は、コモンクライテリアから派生するセキュリティ要求の評価におけるベストプラクティスから構築し、セキュリティ要求がプロの評価者と市場からどのように評価されるかについて開発者が確実に取り組むことを目的としている。ETSI は 2010 年頃から、開発者がリスク分析を行い、製品またはサービス用に標準化されたすべてのセキュリティメカニズムの理論的根拠を提供することを保証するために、この開発形態を考慮した「保証設計」のパラダイムを推進し、さらにプロトコルのセキュリティ要求も明確にしてきた。

B.2 ST と PP の従来の開発

ISO/IEC 15408-1 には、セキュリティ要求仕様（PP ： プロテクションプロファイル）と呼ばれる製品タイプの一般的な説明形式と、セキュリティ仕様（ST ： セキュリティターゲット）と呼ばれる専用の技術仕様の策定に関する詳細なガイダンスが含まれている。製品はその後、評価対象（ToE：Target of Evaluation）と見なされ、ST または PP のいずれかの内容に従って開発された製品は、さらなるセキュリティ評価の対象となり得る。評価者が、ToE（対象製品）が ST/PP で行われた主張に準拠していることに同意する場合、ToE（対象製品）が ST/PP で説明されている制約の範囲内においてはセキュアであると主張するのが合理的である。ST/PP に対するセキュリティ要件を策定するプロセスは、図 B.1 に示されているいくつかのステップを含む（数字は仕様を作成するプロセス中のステップを示す）。

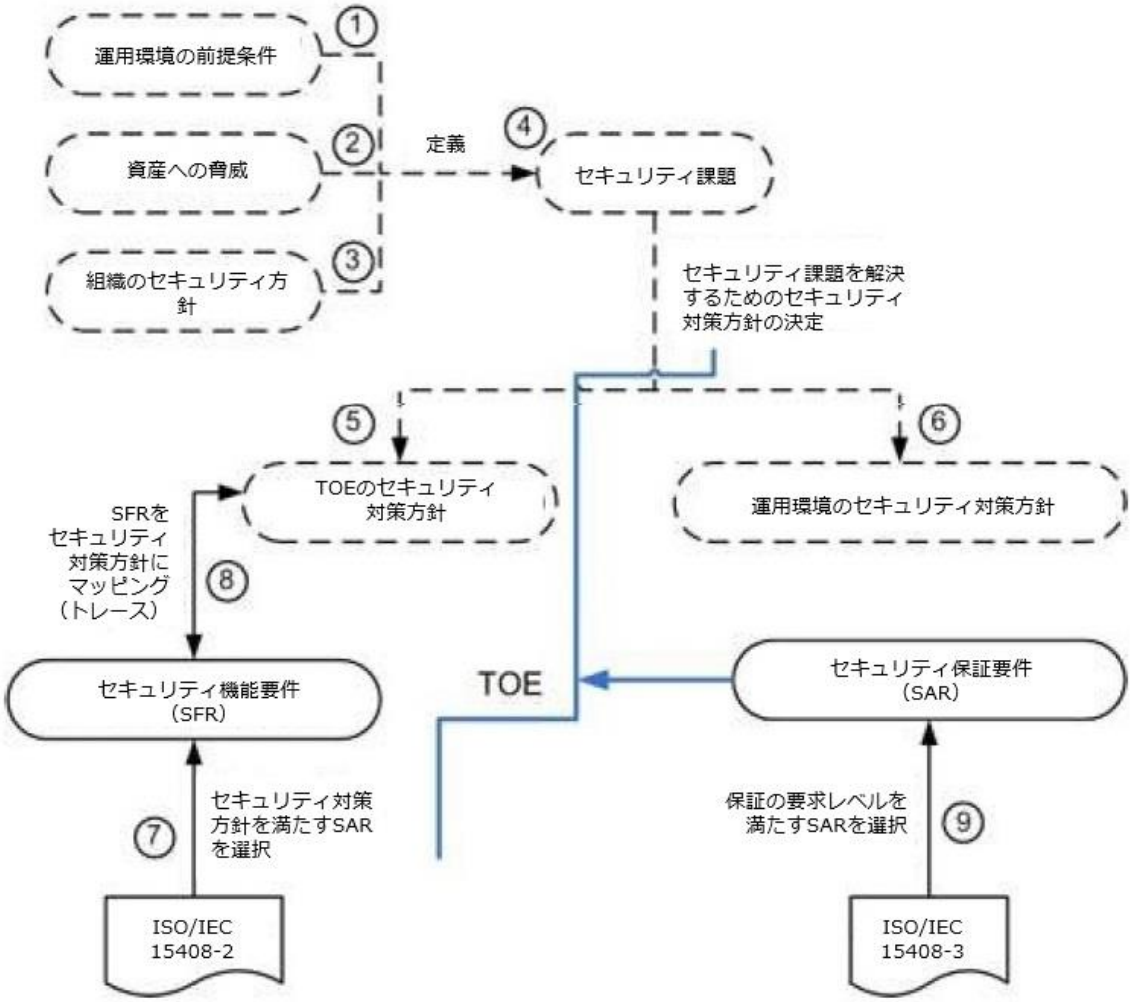


図 B.1：技術仕様（PP や ST）を策定するための通常のアプローチ

このプロセスの結果、通常、熟練していないユーザにとっては理解するのが難しい長い技術仕様が作成される。

この時間とリソースを消費するプロセスの単純化のアイディアは、ISO/IEC 15408-1 の現在のバージョンに「低保証」ST/PP という名前で存在している。しかし、その使用は最低レベルの保証、すなわち EAL1 に制限されており、標準では簡単に説明されているだけである。

ISO / IEC 15408-1 の改定版では、「低保証」の概念が「直接的な論理的根拠」の概念に置き換えられている。しかし、それは名前を変えるだけでなく、アプローチも変えている。直接的な論理的根拠は、仕様を作成する方法を単純化した PP/ST のタイプの 1 つである。さらに、低保証のパッケージに限定されず、より高いレベルの保証を要求できる。

B.3 より簡単で早い仕様策定のための「直接的な根拠」によるアプローチ

定義上、「直接的な根拠」とは、セキュリティ課題定義（SPD：Security Problem Definition）要素（すなわち、前提条件、脅威および組織のセキュリティ方針）がセキュリティ機能要件（SFR：Security Functional Require）に直接マッピングされている要求仕様（PP）または製品仕様（ST）の種類、もしくは運用環境に対するセキュリティ対策方針、という意味である。（図 B.2 参照）。

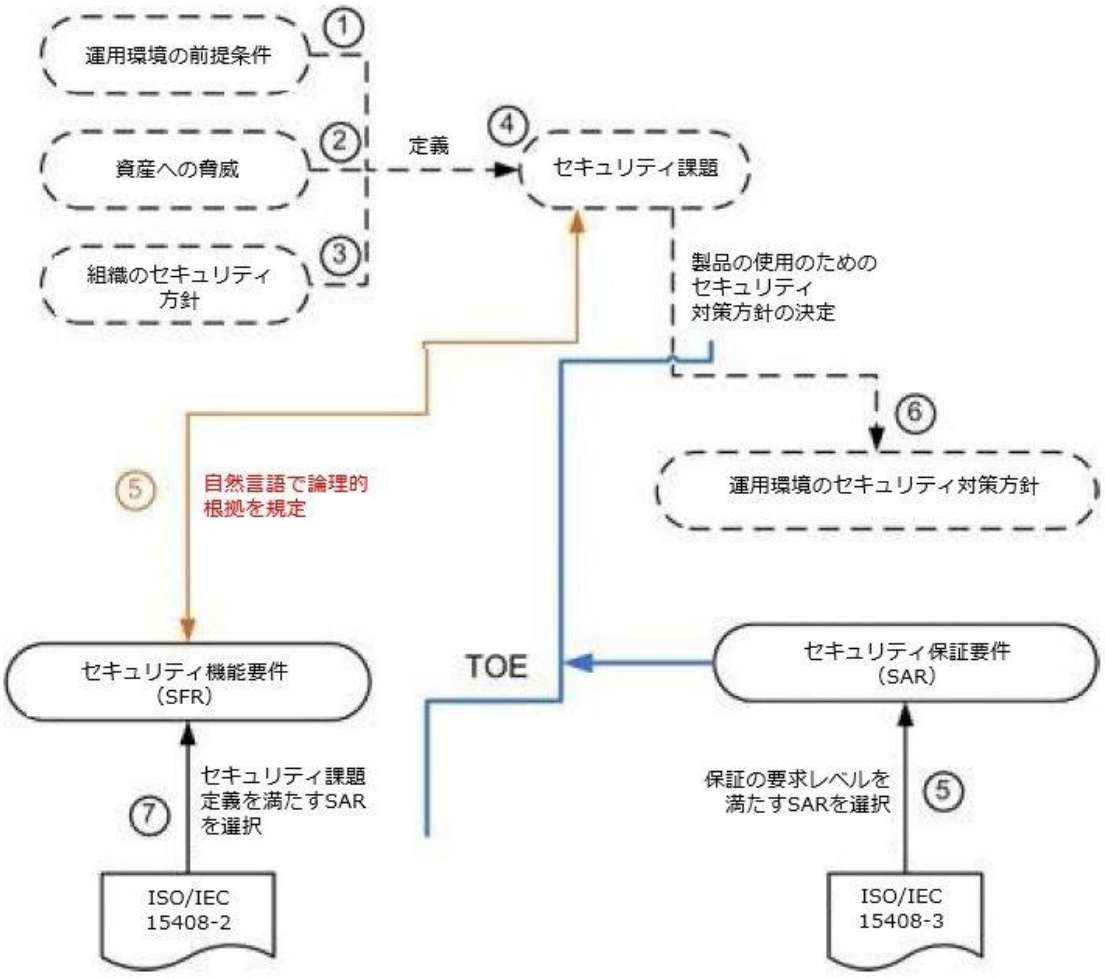


図 B.2：技術仕様を策定するための「直接的な根拠」によるアプローチ

直接根拠の ST には、通常の ST と比較して以下のすべての違いがある。

- TOE に対するセキュリティ対策方針は記述されていない。運用環境に対するセキュリティ対策方針は依然として記述されなければならない。
- ST には TOE セキュリティ対策方針がないため、セキュリティ対策方針根拠はない。
- 管理者や他のユーザに見えるアーキテクチャに関して、SFR の自然言語での説明、およびセキュリティ機能との関係を提供することが要求されている。
- セキュリティ要件の根拠は、SPD の要素を運用環境の SFR およびセキュリティ対策方針に直

接マッピングする。

直接的な根拠 PP は、直接的な根拠 ST から通常の ST のように、通常の PP と同様の単純化をしている。

いくつかの「直接的な根拠」PP が存在し[2]、直接的な根拠 ST の基盤として使用されている。

直接根拠 ST/PP の場合、セキュリティ保証要件（SAR）は通常、事前定義された評価保証レベル（EAL）とは無関係である。その代わりに、仕様に適した特定の保証コンポーネントのリストがある。TOE が評価されるとき、パッケージからすべての保証コンポーネントをチェックする必要はない。そのようなアプローチは、評価を従来のものよりも速くそしてより費用効率的にすることができる。

市場投入時間の短いパラメータを持つ単純な機器や製品に適用可能であるか、または大量生産を意図した特定の状況では、直接的な理論的アプローチが有用な解決策になる可能性がある。

B.4 IoT 機器に適したコンポジット評価

改定された ISO/IEC 15408 シリーズの規格は、評価に対する柔軟なアプローチも提供する。これは、IoT の世界に適していることが証明される可能性がある。このアプローチは「コンポジット評価」と呼ばれる。
コンポジット評価は、2 つの層、すなわち自律的基本構成要素の層および従属構成要素の層に編成することができる 2 つ以上の構成要素からなる製品を検討する場合に行われる。コンポジット評価は、段階的アプローチで、多成分/多層製品に必要なだけ何度でも適用することができる。

コンポジット製品評価は、さまざまな種類の目的を満たす。
- いくつかのアプリケーションおよび顧客に対応するために、プラットフォーム評価を一度独自に実行する。
- 1 つまたは複数の認定プラットフォームにロードするための 1 つまたは複数のアプリケーションを作成する。
- 1 つまたは複数のアプリケーションを 1 つの認証済みプラットフォームにインストールして、評価作業を減らし、高い信頼性を維持する。

図 B.3 に示すように、スマートカード向けのコンポジット評価が開発されており、それは CC 認

2 例：Collaborative Protection Profile for Full Drive 2 Encryption - Encryption Engine
(https://www.commoncriteriaportal.org/files/ppfiles/CPP_FDE_EE_V2.0.pdf),
Collaborative Protection Profile for Full Drive Encryption – Authorization Acquisition v2.0
(https://www.commoncriteriaportal.org/files/ppfiles/CPP_FDE_AA_V2.0.pdf)

証の最も成功した実装であると思われる。そのようなアプローチは、開発者と評価者が以前の評価結果を再利用することを可能にし、したがって既存の評価の時間とコストを削減する。

図 B.3 スマートカード環境におけるコンポジット製品評価

適合性に関して製品開発にはいくつかの制約を適用して再利用アプローチから恩恵を受けるべきだが、この問題に関する詳細な議論は範囲外である。

特定の IoT 機器の階層化アーキテクチャを考慮すると、ISO/IEC 15408-1 の改定版で導入されたコンポジット評価アプローチは、IoT の世界に適用できると考えられる状況下にある可能性がある。

コンポジット評価に関する IoT 機器の一般的なアーキテクチャを図 B.4[4] に示す。

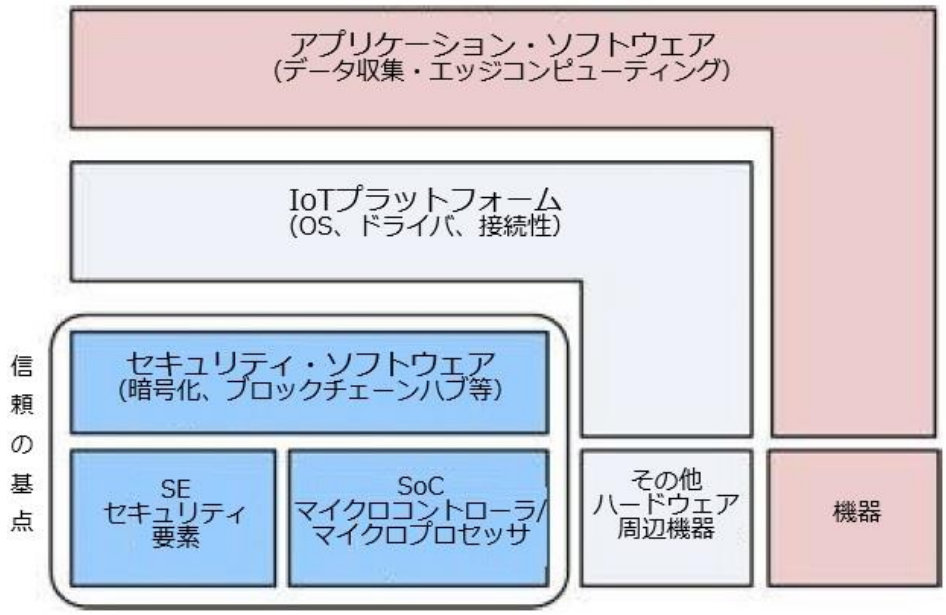


図 B.4 再利用された評価結果をコンセプトとした IoT 製品の階層化アーキテクチャ

「信頼の基点」の概念は、以前に認定された HW または HW-SW コンポーネントに基づいて費用対効果の高いセキュリティ評価の基盤を確立し、IoT 機器アーキテクチャの上位層を実行するための高度に制御された環境を作り出す。

4 この図は、E. Vetillard、G. Stütz、“Common Criteria as Backbone for IoT Security Certification”（第 17 回国際コモンクライテリア会議（ICCC）アムステルダム、2018 年 10 月 30 日－11 月 1 日）より採用。