

博士論文

*PROPOSALS OF THE IOT DEVICE
SECURITY QUALITY METRICS METHOD
(IoT-SQMM)*

Kosuke ITO

Graduate School of Information Security

Institute of Information Security

伊藤 公祐

情報セキュリティ大学院大学

情報セキュリティ研究科

情報セキュリティ専攻

March 2022

*PROPOSALS OF THE IOT DEVICE
SECURITY QUALITY METRICS METHOD
(IoT-SQMM)*

Kosuke ITO

Graduate School of Information Security

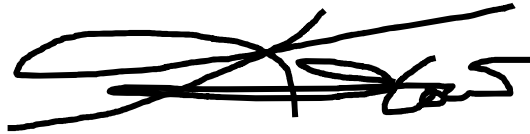
Institute of Information Security

March 2022

DECLARATION

This dissertation is the result of my own work and includes no outcome resulting from collaboration except where specifically indicated in the text. It has not been previously submitted, in part or whole, to any university or institution for any degree, diploma, or other qualification.

Signed: _____



Date: _____

March 1, 2022

Kosuke ITO

ABSTRACT

This paper proposes a method for setting up metrics that reveal security quality as part of quality control throughout the product lifecycle of Internet of Things (IoT) devices, noting that quality control efforts have traditionally been established by IoT device vendors to promote security measures for IoT devices. The study identifies the quality of the security aspects of IoT devices and verifies the method for setting metrics. This work also reveals the security response efforts from the development phase to the evaluation, production, and post-shipment maintenance phases of IoT devices as well as the feasibility and evaluability of the method. For this paper, “security” will be interpreted as mean cybersecurity, unless the term is used in the name or otherwise.

Security incidents caused by IoT devices have recently become evident; consequently, IoT security measures have become indispensable. In particular, the growing number of attack packets to IoT devices has been observed so far. Traditionally, security attacks have mainly targeted information systems in corporate networks and websites providing online services. Based on this experience, information systems on networks have been designed with security measures to prevent security incidents due to a certain level of attacks. For protecting system development, secure coding rules, for example, have been set up to avoid the inclusion of vulnerable codes into source codes. In contrast, with the widespread use of wireless networks and the improving performance of network-enabled devices, establishing various systems online through the IoT mechanism has become possible. As a result, the number of security incidents involving IoT devices has rapidly increased. This can be attributed to the fact that, unlike information system vendors, IoT device vendors did not have sufficient experience to cope with security attacks on the Internet and therefore did not consider sufficient security when designing IoT devices.

The IoT security concerns have activated various IoT security discussions in 2015–2016, mainly in the US, Europe, and Japan. Moreover, many IoT security guidelines were released by government agencies and private organizations. Some government legislatures have also started to legislate security requirements for IoT devices. However, such guidelines have not been able to advance the security commitment of IoT vendors.

Accordingly, the author conceived the idea of defining metrics to evaluate the security quality of IoT devices as a means to promote the protection support of IoT devices. By considering security as one of the quality factors in addition to the conventional quality control metrics for developing devices, the security provided by IoT device vendors may encompass a wide scope.

The IoT mainly consists of the service functions on the network, the network connecting the IoT devices and services, and the IoT devices installed in the physical space. All of these require security measures; however, in this study, the author opted to focus on the scope of security on IoT devices for the following reasons. 1) The attacks on IoT devices are rapidly increasing, and 2) IoT devices are mainly developed by electronics vendors. 3) Furthermore, IoT devices are in a position to connect physical space and cyberspace as well as influence users in the physical space by abnormal conditions in cyberspace.

To date, security capabilities could only be assessed via professional evaluation reports or certifications, such as the Common Criteria of ISO 15408 and the EDSA (Embedded Device Security Assurance) certification of IEC 62443. The concept of security as a quality factor was embodied in the ISO 25000 series for software but was not applied to IoT devices. Because software vulnerability is not the responsibility of IoT vendors as product liability, most IoT vendors do not consider the security capability of products as part of their product quality management. Furthermore, an appropriate IoT security quality metric that IoT vendors can refer to does not exist; instead, companies have to set their own security standards, which may lack consistency and are difficult to justify.

To resolve this problem, the author, inspired by the goal-question-metric (GQM) method that permeates the field of quality control, proposes a universal method for specifying IoT Device Security Quality Metrics Method (IoT-SQMM) on a globally accepted scale. This method enables vendors to verify whether their products are developed under the requirements of existing baselines and certification programs. Moreover, it can help vendors in customizing their quality requirements to satisfy the specified security requirements.

As an approach to proceed with this study, the author adopted the research methodology consisting of five main steps used by the European Union Agency for Cybersecurity and others. These steps include the 1) definition of scope, 2) literature

review, 3) preparation of draft metrics, 4) collection and review of expert opinions, and 5) analysis of review results and measurement of the effectiveness of revised metrics.

The definition of scope in the first step was IoT devices because, as mentioned earlier, they have been the focus of attacks among IoT as a whole. The literature review in the second step was conducted using a systematic method, which is a snowballing approach to research. In the course of the review, the author gained insight on the GQM approach, which is a common evaluation method in the quality industry. The literature review results led to the first draft of the metrics formulated with the GQM approach.

In general, many of the departments managed by a vendor share in the responsibility of fabricating a product at each process from design to after-sales support, throughout the product lifecycle. Therefore, to provide a secure product, the expected level of security initiatives at each process must be clarified for each department to understand their security efforts to implement. Then, the author devised a framework called the transparency model of IoT device security quality to formulate the metrics to encompass the entire product lifecycle. This model is constructed in six areas: security by design A, security by design B, security assurance assessment, security production, security operation, and compliance with law, regulation, and international standard. For each area, security quality goals were defined, and questions were posed for checking these goals; the means for answering the questions was set in the metrics. Accordingly, this enabled the author to develop the metrics necessary to comprehensively check the security implemented throughout the entire product lifecycle. A group of security experts and another group of quality experts reviewed the first draft of the metrics, which were subsequently modified based on the comments raised. The revised set of metrics was examined as the sample of IoT device security quality metrics by the proposed method for effectiveness verifications.

Although the metrics presented in this paper are high-level, they are general perspectives that are independent of the product field. In addition, the author aimed to render the metrics understandable to anyone involved in product development. The metrics require a minimum understanding of security terminology, but do not require technical expertise in security. The author considered that IoT vendors should implement all applicable metrics. However, the degree of implementation and countermeasures may vary depending on the assumed use case of the IoT device depending on the security threats to the device. Therefore, the metrics must be tailored to flexibly implement them

without deviating from the goal of why they have been formulated. Accordingly, the metrics are set as customizable samples available as basis for tailoring.

The verification of metric effectiveness (Step 5 of the research method) can be best implemented if the difference in the security levels between products developed with and without the implementation of the metrics can be verified. However, developing a product in two different ways with the same specifications is extremely difficult in terms of resources and time. Therefore, the effectiveness and validity of the proposed method were examined in three ways.

First, the feasibility of whether the metrics methodology could be adopted by IoT vendors was verified. The author presented the metrics to two companies: one is a large company with a well-known international brand, and the other is a mid-small size IoT startup; interviews were conducted respectively. The results showed that both companies considered the metrics adoptable. In particular, the company with the international brand had limited knowledge of security, however they could start security response efforts with the proposed method and metrics.

Second, the metrics were applied to evaluate the differences in the characteristics of the requirements between existing IoT regulations, baseline requirements, and the certification programs for IoT security. The author confirmed that the metrics were effective for characterizing each set of requirements and balancing the security efforts in each area when developing IoT devices to conform to a set of requirements.

The third verification of the effectiveness of the metrics was to check the security quality by evaluating two commercial dashboard cameras offered as Original Design Manufacturing (ODM) products with similar functional specifications. The metrics could illustrate the differences in security efforts made by each ODM. The metrics could help users to know the security quality of IoT devices behind the product specifications.

Based on these verifications, the author could confirm the applicability of this method to companies and its effectiveness in evaluating existing requirements and assessing the security quality of products. By incorporating metrics into the existing quality control process, it is possible to visualize the efforts to ensure the security quality of IoT devices developed by the company is possible. Furthermore, it is feasible to check whether the product satisfies the requirements of the market and users.

The author also discussed the social contribution of the proposed method. As confirmed that IoT vendors can start security efforts even without specialized knowledge

in security, the proposed method is anticipated to contribute to the development of secure IoT devices by many IoT vendors. In addition, if secure IoT devices become widespread, then more options can become available for users who prefer to utilize the secure one. As security responses for IoT devices become a legal requirement, the security measures become a manufacturing responsibility that is a product liability for IoT vendors. In the future, insurance to cover the cost of security incidents of IoT devices may become more common. In this case, the proposed metrics can contribute to assess the security quality of IoT devices in the security insurance as a reference material.

Therefore, the author proposes the IoT-SQMM as an effective method for IoT vendors to implement security measures in developing a secure IoT device. This method can aid vendors in tailoring their quality metrics to satisfy security requirements. In turn, IoT users can use these metrics to verify the security quality of IoT devices.

The author expects that the results of this research will contribute to improving the efforts of many IoT vendors, who are likely to neglect to consider security as a quality requirement when simply referring to general ideas of initiatives in security guidelines. The author strongly believes that they will be able to incorporate security initiatives into their product development processes.

Keywords: Internet of Things, Information security, Quality management, Software metrics, Security Quality management

論文要旨

本論は、IoT 機器のセキュリティ対策を推進するために、従来から電子機器ベンダによる品質管理の取り組みが確立されていることに着目し、IoT 機器の製品ライフサイクルを通じた品質管理の一環として、セキュリティ品質を明らかにするメトリクスを設定する方法を提案する。本研究では、IoT 機器のセキュリティ面の品質を明らかにし、指標の設定方法を検証する。また、IoT 機器の開発段階から評価、生産、出荷後の保守段階に至るまでのセキュリティ対応の取り組みを明らかにするとともに、本手法の導入可能性、評価可能性を明らかにするものである。本論では、名称などに使われる用語を除き、「セキュリティ」はサイバーセキュリティのことを意味する。

IoT は、ネットワーク上のサービス機能から IoT 機器とサービスをつなぐネットワーク、そして物理空間に設置される IoT 機器から主に構成される。近年、IoT 機器に起因するセキュリティ事故が顕在化しており、IoT 機器のセキュリティ対策が求められている。特に IoT 機器への攻撃パケットは年々増加していることが観測されている。

従来、セキュリティ攻撃の対象は企業ネットワークやオンラインサービスを提供するウェブサイトの情報システムが中心だった。この経験からネットワーク上の情報システムは一定の攻撃を受けても問題が起きないように、セキュリティ対策設計を行い、ソースコードに脆弱性のあるコードが含まれない様にセキュアコーディングルールを設定するなどをして、セキュアなシステム開発を行ってきた。一方、無線ネットワークの普及やネットワーク接続可能な機器の高性能化などにより、様々なシステムが IoT と呼ばれる仕組みによりオンライン化することが可能となった。IoT 機器のベンダは、製品の付加価値を高めるため、機器にネットワーク接続機能を追加する形で積極的に機器の IoT 化を進めた。その結果、IoT 機器のセキュリティ事故が急増してしまった。

この原因として、情報システムのベンダと異なり、IoT 機器ベンダはインターネット上のセキュリティ攻撃については多くの経験がないため、IoT 機器の設計にセキュリティへの配慮が足りなかったことが考えられる。

IoT 機器に起因するセキュリティ問題が顕在化したことを受けて、2015～2016 年頃、主に日米欧では様々な IoT セキュリティの議論が活発化した。そして多くの IoT セキュリティガイドラインが政府関連だけでなく民間団体からリリースされた。一部の政府機関では、IoT 機器に対するセキュリティ要件を法制化する動きも始まった。しかし、ガイドラインは IoT ベンダのセキュリティ対策の取組みをなかなか推し進めるに至らなかった。

そこで本研究では、IoT 機器のセキュリティ対策を促進させるため、IoT 機器の製品ライフサイクル全般にわたる IoT ベンダの取組みのセキュリティ品質を明らかにするメトリクスを設定方法を提案する。一般的に、機器ベンダには品質管理の取組みが定着している。IoT 機器のベンダは、従来と同じ製品開発プロセスに従って開発を続けている。したがって、IoT 機器ベンダにセキュリティを浸透させるためには、従来の製品開発における品質管理の取組みにセキュリティ対策のための検討事項を組み込む方法が必要と考えた。

IoT を構成するすべての要素に対してセキュリティ対策は必要となる。しかし、本研究では、以下の理由で IoT 機器にスコープを置いた。1) IoT 機器への攻撃が急増していること、2) IoT 機器は主に電子機器ベンダが開発するものであること、そして3) IoT 機器は、物理空間とサイバー空間をつなぎ、サイバー空間の異常な状態を物理空間にいるユーザに影響を及ぼすポジションにあること。

これまでの情報技術やシステムのセキュリティの評価は、ISO 15408 の Common Criteria (CC) や IEC 62443 の Embedded Device Security Assurance (EDSA) 認証など、セキュリティ専門家による評価レポートや認証によってのみ行われてきた。一方、品質要素としてのセキュリティの考え方は、ソフトウェアでは ISO25000 シリーズで具現化されていたが、IoT 機器には適用されていなかった。ソフトウェアの脆弱性はハードウェアの製造物責任の範囲外であったため、ほとんどの IoT ベンダは製品のセキュリティ能力を品質管理の一環として考慮していなかった。さらに、IoT ベンダにとって適切な IoT セキュリティ品質の一般的なメトリクスは存在しておらず、各ベンダが独自にセキュリティ品質のメトリクスを設定しなければならない状況であった。その独自のメ

トリクスはベンダごとに違うため一貫性を欠き、各ベンダは自ら設定したメトリクスを対外的に正当化することは困難であった。

この問題を解決するために、筆者は、品質管理の分野に浸透する GQM (Goal-Question-Metric) 手法にヒントを得て、IoT機器のセキュリティ品質メトリクスを世界的に理解される尺度で規定する普遍的な手法、IoT-SQMM を提案する。この手法により、ベンダは自社製品が既存のベースラインや認証プログラムの要件に沿って開発されているかどうかを検証することができ、また、与えられたセキュリティ要件を満たす様にベンダが品質要件を調整することができる。

本研究を進める方法として、ENISA などが用いている主に5つのステップからなる調査手法を採用した。1) スコープの定義、2) 文献調査、3) メトリクスの下案の作成、4) 専門家によるレビューと意見収集、5) レビュー結果の分析と修正したメトリクスの効果測定という5つのステップである。

スコープの定義では、前述の通り、IoT 全般の中でも攻撃対象として注目されている IoT 機器とした。文献調査は、雪だるま式に調査を進めていくシステマティック文献調査方法で実施した。文献調査を進める中で、品質業界では一般的な GQM approach による評価方法があることを知った。文献調査の結果を総括し、GQM 手法の考え方でメトリクスの一次ドラフトを作成した。

一般に、製品ライフサイクル全体の中、企画から販売後のサポートまでの各フェーズの責任を多くの部門が分担して、製品開発を進めていく。したがって、セキュアな製品を提供するためには、各フェーズでのセキュリティの取組みを明確にして、責任を持つ部門が実行すべきセキュリティの取組みを理解できるようにする必要がある。そのように筆者は考えた。

そこで、製品ライフサイクルのすべてを網羅するようにメトリクスを設定するために、筆者は the Transparency Model of IoT Device Security Quality というフレームワークを考案した。そのモデルを、Security by Design A, Security by Design B, Security Assurance Assessment, Security Production, Security Operation, Compliance with Law, Regulation, International Standard の6つのエリアで構成した。各エリアに品質ゴールを定め、ゴールのために確認すべきことを質問事項とし

て掲げ、その質問への答え方をメトリクスとして設定した。それにより、製品ライフサイクル全体にわたるセキュリティの取組みを網羅的に確認するメトリクスを策定できた。

このメトリクス一次ドラフトを、セキュリティと品質の専門家グループにレビューしてもらい、挙げられた意見を基にメトリクスを修正した。この修正版を IoT 機器のセキュリティ品質メトリクスとした。

本研究で紹介するメトリクスは、製品分野に依存しない、ハイレベルの一般的な視点で策定した。また、筆者は、セキュリティ用語の理解はある程度必要だが技術的な専門知識は必要としない、製品開発に携わるすべての人に理解できるメトリクスを目指した。

筆者は、IoT ベンダは IoT 機器に実施するすべての取組みをメトリクスとして設定すべきであると考え。しかし、IoT 機器に対するセキュリティ脅威を踏まえた上で、想定する IoT 機器のユースケースに応じて、セキュリティ対策方法やリスク低減のレベルは異なる。そのため、IoT ベンダは、メトリクスの設定目的から逸脱しない範囲で、設定するメトリクスを柔軟に調整する必要がある。したがって、ここで設定したメトリクスは、テーラリングの基として利用可能なサンプルメトリクスと位置付けている。

ステップ5の効果測定として、実際にメトリクスに沿って開発した製品と、メトリクスのない製品とのセキュリティ対策レベルの違いを評価できればよいが、2つの異なる方法で同じ仕様の製品を開発することはリソース面でも時間的にも現実的に困難である。そこで、筆者は次の3つの評価をもって本手法の有効性を評価した。

1 つは、本研究で策定した本手法が、IoT 機器ベンダで採用可能かの実現可能性を確認した。国際的に著名なブランドを持つ企業と中小企業の IoT スタートアップの 2 社にメトリクスを紹介し、採用できるかをヒアリング調査した。結果としていずれの企業も採用できると評価した。特に国際的なブランドを持つ企業では、これまでセキュリティ対策の実施の経験はなかったが、サンプルメトリクスを参考に本手法で調整したメトリクスを製品設計標準プロセスに導入し、セキュリティ対策の取組みを開始した。このことから、本研究は、

企業の大小にかかわらず，本手法により企業でのセキュリティ対策の取組みの導入を加速することに貢献するものとする。

2つ目は，既存の IoT に関する法規制，ベースライン要件，および IoT セキュリティの特徴の違いをメトリクスによって評価した．メトリクスによって各要件群の特徴がわかることを確認できた．本研究では，IoT 機器を開発する際，各エリアにおけるセキュリティの取組みのバランスを確認することを示し，既存の要件を評価し，可視化するツールとしての有効性を確認した．

3つ目の効果測定は，機能仕様が似ている ODM 製品として市販されている2つのドライブレコーダを評価し，セキュリティ品質を確認した．同じような機能の製品でも，メトリクスによってセキュリティ品質の違いを明らかにすることができた．このメトリクスにより，IoT 機器のセキュリティ品質を確認できることが示された．検証の結果，本研究では，製品のセキュリティ品質を評価する手法としての有効性を確認できた．

本研究の貢献は，セキュリティの専門的知識がなくてもセキュリティの取組みを開始できることが確認できたことから，多くの IoT ベンダによるセキュアな IoT 機器の開発と普及につながることを考える．その結果，セキュアな IoT 機器が普及すれば，セキュアな製品を望むユーザにとって選択肢は広がる．既存の品質管理プロセスにメトリクスを組み込むことで，自社で開発した IoT 機器のセキュリティ品質確保の取り組みを可視化することができる．そして，その製品が市場やユーザの要求を満たしているかどうかを確認することも可能となる．IoT 機器ベンダとユーザの間における，IoT 機器のセキュリティ品質に関するコミュニケーションツールとしても貢献すると考える．

さらに，IoT 機器のセキュリティ対策が法規制化されることにより，IoT ベンダにとってセキュリティ対策は製造責任の範囲となってくるだろう．万が一のセキュリティ事故となった場合に備えて，インシデント対応費用をカバーするための保険を掛けておくことも将来一般化するかもしれない．その場合，保険料率の評価にも本メトリクスは貢献できると考える．

改めて，筆者は，IoT 機器ベンダのセキュリティ対策に有効な手法として，IoT 機器のセキュリティ品質メトリクス手法「IoT-SQMM」を提案する．この方

法は，IoT ベンダがこれらのセキュリティ要件を満たすために品質要件を調整するのに役立つと考えられる．また，IoT ユーザは，IoT 機器のセキュリティ品質を検証する方法に，このメトリクスを使用することができるだろう．

筆者は，本研究成果が，ガイドライン等で一般的なセキュリティ対策の考え方を示しただけでは具体的なセキュリティ対策の取組みにつなげられない IoT ベンダにとって，従来の品質管理の考え方に基づき，IoT 機器のセキュリティ対策を実行する手段として取組み易くすることに貢献し，脆弱な IoT 機器が市場にまん延している現状の改善と安全な IoT 市場の形成に寄与するものと考えている．

キーワード：Internet of Things（モノのインターネット），情報セキュリティ，品質管理，ソフトウェアメトリクス，セキュリティ品質マネジメント

ACKNOWLEDGEMENTS

I wish to express my utmost gratitude to my supervisor, Prof. Atsuhiko Goto, who read my numerous revisions, aided in organizing the disarray, and provided advice. Moreover, thanks to the thesis review committee members at IISEC, Prof. Masayo Fujimoto, Prof. Takao Okubo, and Prof. Toshihiro Matsui for their support and advice. Further, many thanks to Ms. Miwako Yamaguchi of the President's Office, IISEC, for reviewing the English grammar in this work. I must also thank my seminar mates at the Goto Laboratory, IISEC, who gave me numerous advice.

I wish to express my special thanks to Dr. Shuji Morisaki (Associate Professor, Nagoya University) for his valuable inputs and suggestions throughout my study.

I am grateful to my colleagues at the IoT security working group of the Japan Network Security Association (JNSA) for their advice and for providing the opportunity to exchange opinion.

Most importantly, I am grateful to my family for the unconditional, unequivocal, and loving support.

CONTENTS

1 INTRODUCTION.....	1
1.1 BACKGROUND	1
1.2 RISE IN DEMANDS FOR PRODUCT SECURITY RESPONSES.....	2
1.3 WHAT IS IoT AND POSITION OF IoT DEVICES?.....	2
1.4 BURDEN OF SECURITY RESPONSES BY IoT VENDORS	6
1.5 SCOPE OF THIS STUDY	8
1.6 PURPOSE OF THIS STUDY.....	9
1.7 CONTRIBUTION OF THIS STUDY.....	10
1.8 STRUCTURE OF THIS PAPER.....	11
2 NECESSITY OF THIS STUDY	15
2.1 MOTIVATION OF THIS STUDY	15
2.2 QUESTION 1: DOES ANY EXISTING LITERATURE OR STANDARD COVERING SECURITY QUALITY CONTROL MEASURES FOR IoT THROUGHOUT THE PRODUCT LIFECYCLE EXIST?	16
2.3 QUESTION 2: DOES ANY REASON FOR VISUALIZING THE SECURITY CONTROL MEASURES EXIST?	18
2.4 SUMMARY OF THIS SECTION	19
3 RESEARCH ON IOT DEVICE SECURITY QUALITY	21
3.1 RESEARCH METHOD.....	21
3.2 DEFINITION OF SCOPE (STEP 1)	22
3.3 LITERATURE SURVEY (STEP 2).....	23
3.3.1 <i>Current Situation of IoT Security Awareness of Vendors</i>	24
3.3.2 <i>Security Attacks on IoT</i>	25
3.3.3 <i>Notable Security Incidents on IoT</i>	27
3.3.4 <i>Product Quality Management</i>	32
3.3.5 <i>Product Liability</i>	33
3.3.6 <i>Quality Metrics of Software</i>	34
3.3.7 <i>Security Evaluation Method</i>	38
3.3.8 <i>Security Maturity Model</i>	41
3.3.9 <i>Applicability of existing methods to IoT devices</i>	45
3.3.10 <i>Security Guidelines</i>	47
3.3.11 <i>Summary of Literature Review</i>	49

4 ITEMIZING IOT DEVICE SECURITY QUALITY METRICS	53
4.1 DEFINITION OF IOT DEVICE SECURITY QUALITY.....	53
4.2 REQUIREMENTS OF IOT DEVICE SECURITY QUALITY	54
4.3 TRANSPARENCY MODEL OF IOT DEVICE SECURITY QUALITY.....	55
4.4 PROPOSAL DEVELOPMENT OF IOT DEVICE SECURITY QUALITY METRICS (STEP 3).....	57
4.4.1 <i>Extraction of candidate items from literature Surveyed</i>	57
4.4.2 <i>GQM Method</i>	58
4.4.3 <i>Setting Goals for Each Area</i>	60
4.4.4 <i>Setting Sample Questions and Metrics for Each Goals (Step 3 – 4)</i>	62
4.5 EXPERT REVIEW AND OPINION GATHERING (STEP 4).....	79
4.6 EXPERT OPINION ANALYSIS (A PART OF STEP 5)	81
4.7 DISCUSSION OF SETTING IOT DEVICE SECURITY QUALITY METRICS	81
5 EFFECTIVENESS OF THE PROPOSED METHOD (STEP 5)	85
5.1 FEASIBILITY OF IMPLEMENTATION OF THIS METHOD TO IOT VENDORS	85
5.1.1 <i>Subject Selection and Criteria Setting</i>	86
5.1.2 <i>Results of Examination</i>	86
5.1.3 <i>Discussion of the Results</i>	87
5.2 EVALUATION OF EFFECTIVENESS AS A TOOL FOR IDENTIFY THE CHARACTERISTICS OF THE REQUIREMENTS OF IOT-RELATED REGULATIONS, GUIDELINES, AND CERTIFICATION PROGRAMS	88
5.2.1 <i>IoT Regulations</i>	89
5.2.2 <i>IoT Security Baseline Guidance</i>	90
5.2.3 <i>IoT Security Certification Program</i>	91
5.2.4 <i>Discussion of the Results</i>	92
6 EVALUATION OF IOT DEVICES WITH THE PROPOSED METHOD	95
6.1 TARGET IOT DEVICES	95
6.2 EVALUATION WITH THE PROPOSED METHOD	96
6.3 EVALUATION RESULTS	96
6.4 DISCUSSION OF THE RESULTS	97
7 CONSIDERATIONS ON SOCIAL CONTRIBUTIONS.....	101
7.1 CONTRIBUTION TO THE SPREAD OF SECURE IOT DEVICES	101
7.2 CONTRIBUTION AS A SELECTION INDICATOR FOR SECURE IOT DEVICES	102
7.3 CONTRIBUTION TO CREATE SUPPORTING ENVIRONMENT FOR IOT VENDORS BY SECURITY INSURANCE	102

7.3.1 Product Liability Insurance	102
7.3.2 Creating a New Market for IoT Security Insurance	103
8 FUTURE DIRECTION	105
9 CONCLUSION.....	107
10 REFERENCES.....	111
11 APPENDICES	126
APPENDIX 1: RESULT OF A COMPARATIVE STUDY OF THE REQUIREMENTS LISTED IN THE LITERATURE.....	127
APPENDIX 2: THE DRAFT QUESTIONS AND METRICS FOR THE EXPERT REVIEW	129
APPENDIX 3: CANDIDATES OF OPTIONAL QUESTION AND METRICS..	132
CANDIDATES FOR AREA 1-A	132
CANDIDATES FOR AREA 1-B	132
CANDIDATES FOR AREA 2	135
CANDIDATES FOR AREA 3	136
CANDIDATES FOR AREA 4	136
CANDIDATES FOR AREA 5	136
APPENDIX 4: THE RESULTS OF IOT DEVICE EVALUATION WITH THE PROPOSED METHOD.....	137
AREA 1-A: SECURITY BY DESIGN	137
AREA 1-B: SECURITY BY DESIGN (SECURITY MEASURES, SECURE DEVELOPMENT)	137
AREA 2: SECURITY ASSURANCE ASSESSMENT	139
AREA 3: SECURITY PRODUCTION	141
AREA 4: SECURITY OPERATION.....	142
AREA 5: COMPLIANCE WITH LAW, REGULATION, AND INTERNATIONAL STANDARD	143
RESEARCH ACHIEVEMENTS.....	144
JOURNALS WITH PEER REVIEW	144
INTERNATIONAL CONFERENCES WITH PEER REVIEW	144
OTHER ACHIEVEMENTS.....	144

LIST OF TABLES

TABLE 3.1 TYPE OF ATTACK VECTORS ON IoT DEVICES	31
TABLE 3.2 COMPARISON OF THE QUALITY REQUIREMENTS [71] (MODIFIED BY AUTHOR).....	36
TABLE 3.3 SEVEN LEVELS OF EAL.....	39
TABLE 3.4 COMPARISON OF SECURITY MATURITY MODELS.....	44
TABLE 4.1 REQUIREMENTS OF IoT DEVICE SECURITY QUALITY	54
TABLE 4.2 GOALS FOR EACH AREA OF TRANSPARENCY MODEL	60
TABLE 4.3 QUESTION AND METRICS FOR AREA 1-A	64
TABLE 4.4 QUESTION AND METRICS FOR AREA 1-B	65
TABLE 4.5 QUESTION AND METRICS FOR AREA 2	70
TABLE 4.6 QUESTION AND METRICS FOR AREA 3	74
TABLE 4.7 QUESTION AND METRICS FOR AREA 4	77
TABLE 4.8 QUESTION AND METRICS FOR AREA 5	79
TABLE 5.1 LIST OF DOCUMENTS FOR EVALUATION OF EFFECTIVENESS	88
TABLE 6.1 SUMMARY OF THE EVALUATION RESULTS	96

LIST OF FIGURES

FIGURE 1.1: IoT ARCHITECTURE [13]	4
FIGURE 1.2: DOMAIN BASED REFERENCE MODEL (AUTHOR BASED ON ISO/IEC 30141 [15]).....	5
FIGURE 3.1: RESEARCH METHOD (AUTHOR BASED ON ENISA [31])	21
FIGURE 3.2: STATUS OF IoT VENDORS CONSIDERING SECURITY.....	25
FIGURE 3.3: STATUS OF IoT VENDORS HAVING THE SECURITY POLICY BY SECTORS.	25
FIGURE 3.4: ATTACKS OBSERVED IN 2019 (AUTHOR BASED ON NICT [50])	26
FIGURE 3.5: IMAGE OF THE ATTACK USING THE USB DRIVES (AUTHOR BASED ON [53])	28
FIGURE 3.6: INSECAM WEB SITE [54] (AS OF DEC 2020).....	28
FIGURE 3.7: IMAGE OF THE BOTNET	30
FIGURE 3.8: IMAGE OF PACEMAKER ATTACK	30
FIGURE 3.9: SOFTWARE PRODUCT QUALITY MODEL IN ISO/IEC 25010	35
FIGURE 4.1: TRANSPARENCY MODEL OF IoT DEVICE SECURITY QUALITY	55
FIGURE 5.1: BAR CHART OF REQUIREMENTS DISTRIBUTION OF IoT SECURITY REGULATIONS	89
FIGURE 5.2: BAR CHART OF REQUIREMENTS DISTRIBUTION OF IoT SECURITY BASELINE GUIDANCE.....	90
FIGURE 5.3: BAR CHART OF REQUIREMENTS DISTRIBUTION OF IoT SECURITY CERTIFICATION	92
FIGURE 6.1: BAR CHART OF RESULTS OF EVALUATION	97

LIST OF ABBREVIATIONS AND ACRONYMS

3G:	the 3rd Generation
AI:	Artificial Intelligence
B2B:	Business to Business
B2C:	Business to Consumer
BITAG:	Broadband Internet Technical Advisory Group
BSIMM:	Building Security in Maturity Model
CC:	Common Criteria
CCDS:	Connected Consumer Device Security council of Japan
CCRA:	Common Criteria Recognition Arrangement
CFW:	Cybersecurity Framework
CSA:	The Cloud Security Alliance
Dash-cam:	Dashboard Camera
DAST:	Dynamic Application Security Testing
DevOps:	Development-Operations
DDoS:	Distributed Denial of Service
DHS:	Department of Homeland Security
EAL:	Evaluation Assurance Level
EDSA:	Embedded Device Security Assurance
ENISA:	The European Union Agency for Cybersecurity
ETSI:	European Telecommunications Standards Institute
EUCC:	European Cybersecurity Certification
FDA:	Food and Drug Administration
FTC:	Federal Trade Commission
GPS:	Global Positioning System
GQM:	Goal-Question-Metric(s)

GSM: Global System for Mobile communications

GSMA: GSM Association

HSM: Hardware Security Module

IACS: Industrial Automation and Control Systems

ICT: Information and Communication Technology

ID: Identification

IDE: Integrated Development Environment

IEC: International Electrotechnical Commission

IIC: Industrial Internet Consortium

IoT: Internet of Things

IoT SMM: IoT Security Maturity Model

IP: Internet Protocol

IPA: Information-technology Promotion Agency of Japan

ISO: International Organization for Standardization

JTAG: Joint Test Action Group

METI: Ministry of Economy, Trade, and Industry of Japan

MIC: Ministry of Internal Affairs and Communications of Japan

NICT: National Institute of Information and Communication of Japan

NISC: National center of Incident readiness and Strategy for Cybersecurity of Japan

NIST: National Institute of Standards and Technology

ODM: Original Design Manufacturing

OSS: Open Source Software

OWASP: Open Web Application Security Project

PL: Product Liability

PSIRT: Product Security Incident Response Team

QoE: Quality of Experience

SAST: Static Application Security Testing

SLR: Systematic Literature Review

SOC: Security Operation Center

SSDL: Secure Software Development Lifecycle

SSE-CMM: Systems Security Engineering – Capability Maturity Model

TARA: Threat Analysis and Risk Assessment

UART: Universal Asynchronous Receiver/Transmitter

UL: Underwriters Laboratories Limited Liability Company

USB: Universal Serial Bus

vBSIMM: Vendor Building Security in Maturity Model

1 INTRODUCTION

This section discusses the background, motivation, purpose, the reasons for placing the scope of this research on IoT devices, and overview of this study pertaining to a proposed IoT device security quality metrics method.

1.1 Background

With the proliferation of IoT (Internet of Things) devices, security has become more important. Many security breaches of IoT devices have already been reported; hence, the necessity of IoT security has increased [1]–[4]. IoT security is a considerably active problem that has become a topic area at Black Hat, the world’s leading conference on security concerns.

However, even before the term “IoT” became popular, security problems involving consumer electronics with Internet connectivity have already been experienced. The attack target was the recording reservation function of video recorders at home via the Internet. At the time of shipment, the factory security settings of these devices were disabled (no password). As a result, in 2004, Linux-based video recorders became a springboard and source of spam mail. Such breaches are still existing, such as the malware called *Mirai* and its subspecies. They spread across cyberspace, targeting IoT devices, including IP/web/network cameras, digital video recorders, home routers, smart speakers, and network printers [5], [6].

In addition, the array of devices connecting to the network to expand services is becoming increasingly diverse. Automobiles and medical equipment are also evolving into network-connected devices in a form known as “smart.” Because the safety of these

devices is directly related to the lives of their users, security measures must be carefully implemented. The vendors of these devices have been developing their products with adequate safety considerations. However, thus far, safety design has been limited to a certain level based on indicators, such as the ratio of manufacturing defects in the internal components of the equipment to the failure rate. Malfunctions caused by malicious attacks through the network were not envisioned in the design.

1.2 Rise in Demands for Product Security Responses

During security conferences, announcements regarding new vulnerabilities of IoT devices receive considerable attention. This is probably because IoT devices are more accessible and new to the security community and hence more interesting than the vulnerabilities in servers and online service software. Moreover, many security experts are beginning to resolve the security problems of IoT devices, which are a mass of embedded technology. To resolve these problems, many organizations that promote security measures have published guidelines and guidance on managing the security of IoT devices. Nevertheless, progress on the security measures for IoT devices remains lacking. The author was extremely curious regarding the reason for this situation.

Researchers on IoT security have made significant progress on mitigating security threats and vulnerabilities, such as remote attacks via wireless connectivity (e.g., Wi-Fi, Bluetooth, or ZigBee) [7]–[9], and protecting architecture to satisfy security requirements [4], [10]. These countermeasure functions and mitigation technologies are frequently not self-developed by IoT vendors but externally procured. Consequently, IoT vendors are inherently required to assess the security quality of the communication components they employ. However, in reality, IoT security researchers have not yet clarified the standard initiatives that IoT vendors can easily adopt to ensure the development of secure IoT devices. Different from legislation on safety and environmental concerns, the laws, regulations, and international standards for IoT security have not been established thus far. The guidelines on IoT security and privacy, i.e., ISO 27400 [11], continue to undergo development.

1.3 What is IoT and Position of IoT Devices?

“The internet of things” was first mentioned in 1999 by Kevin Ashton, co-founder of the Auto-ID Center at MIT, at his presentation to Procter & Gamble [12]. According to Ashton, “The Internet of Things, or IoT, is a system of interrelated computing devices,

mechanical and digital machines, objects, animals or people that are provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.”

“A thing” on the IoT can be similar to a person with a heart monitor implant, a farm animal with a biochip transponder, an automobile with built-in sensors to alert the driver when tire pressure is low. Also, it is similar to any other natural or man-made object that can be assigned an IP address and transfers data over a network. This implies that IoT is cyber-physical and action in cyberspace is affecting a physical phenomenon. The risk in our physical life is directly affected by security in cyberspace.

Many published reports in literature explain the characteristics of IoT; however, Patel et al. [13] describe the characteristics of IoT as follows:

- 1) Interconnectivity
- 2) Things-related services
- 3) Heterogeneity
- 4) Dynamic changes
- 5) Enormous scale
- 6) Safety
- 7) Connectivity.

IoT Acceleration Consortium of Japan [14] explains that there are six characteristics of IoT as follows:

- Characteristic 1: Large influence on a wide range in case of a cyberattack
- Characteristic 2: Long lifecycle of IoT
- Characteristic 3: Difficulty in monitoring IoT
- Characteristic 4: Insufficient mutual understanding between stakeholders on the IoT device side and the network side
- Characteristic 5: Limited functions and computing performance of IoT
- Characteristic 6: Unintended network connections of IoT even for the manufacturers.

Patel et al. seem to view the characteristics of the IoT from the perspective of the IoT services as a whole, while the IoT of the IoT Promotion Consortium is viewed from the perspective of the IoT devices. There are lots of definition and explanation of IoT, but

others said similarly. This implies that the IoT is connecting online on a large scale for the various kinds of services dynamically connected across the industry sectors.

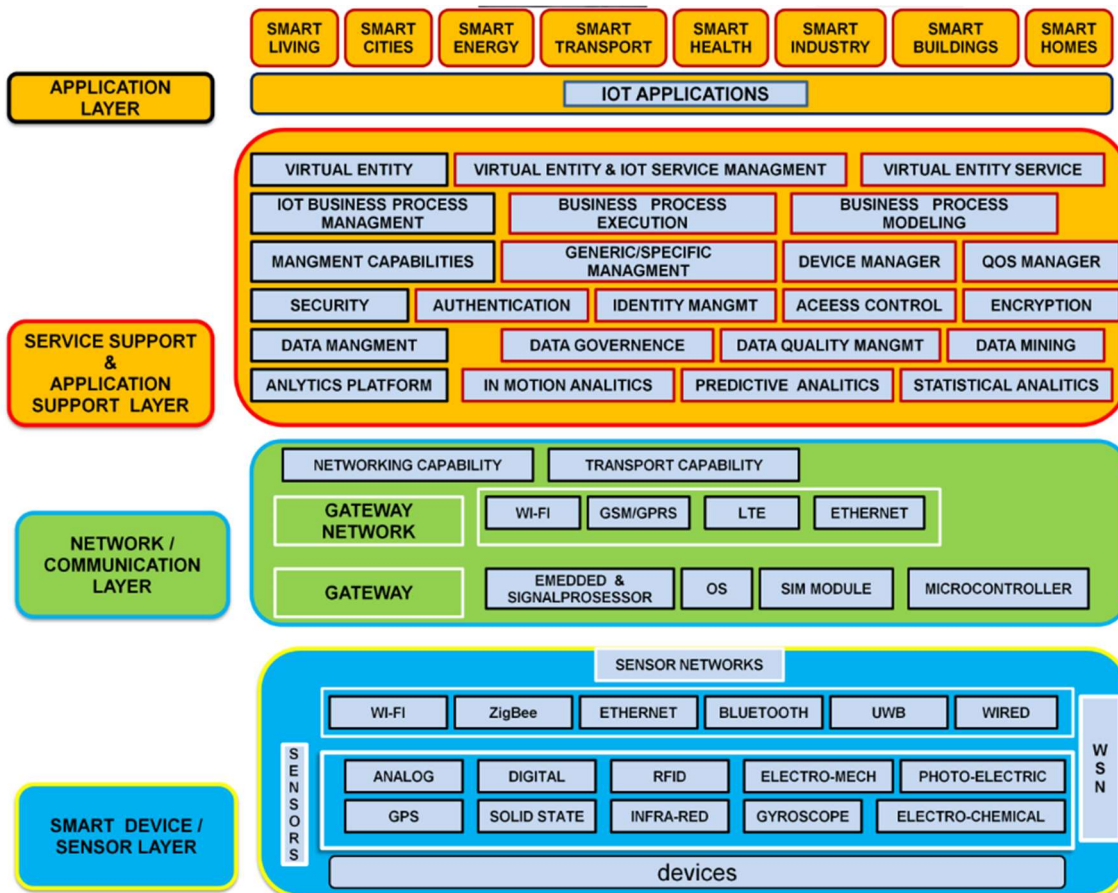


Figure 1.1: IoT Architecture [13]

The IoT architecture consists of four layers, as shown in Fig. 1.1.

- **Application Layer:** applications for “smart” environments/spaces in domains such as Transportation, Building, City, Lifestyle, Retail, Agriculture, Factory, Supply chain, Emergency, Healthcare, User interaction, Culture and tourism, Environment and Energy
- **Service and Application Support Layer:** the processing of information possible through analytics, security controls, process modeling and management of devices
- **Network/Communication Layer:** a robust and high performance wired or wireless network infrastructure as a transport medium and gateway networks such as Ethernet, Wi-Fi, and Global System for Mobile communications (GSM), etc.
- **Smart device / Sensor Layer:** smart objects integrated with sensors

The reference architecture is defined in ISO/IEC 30141 [15]. Franberg et al. [16] explained that the reference architecture consisted of the following:

- 1) User domain of user interface
- 2) Operation and management domain
- 3) Application and service domain
- 4) Access and communication domain
- 5) Sensing and controlling domain
- 6) Physical entity domain

as in the domain-based functional view as shown in Fig. 1.2.

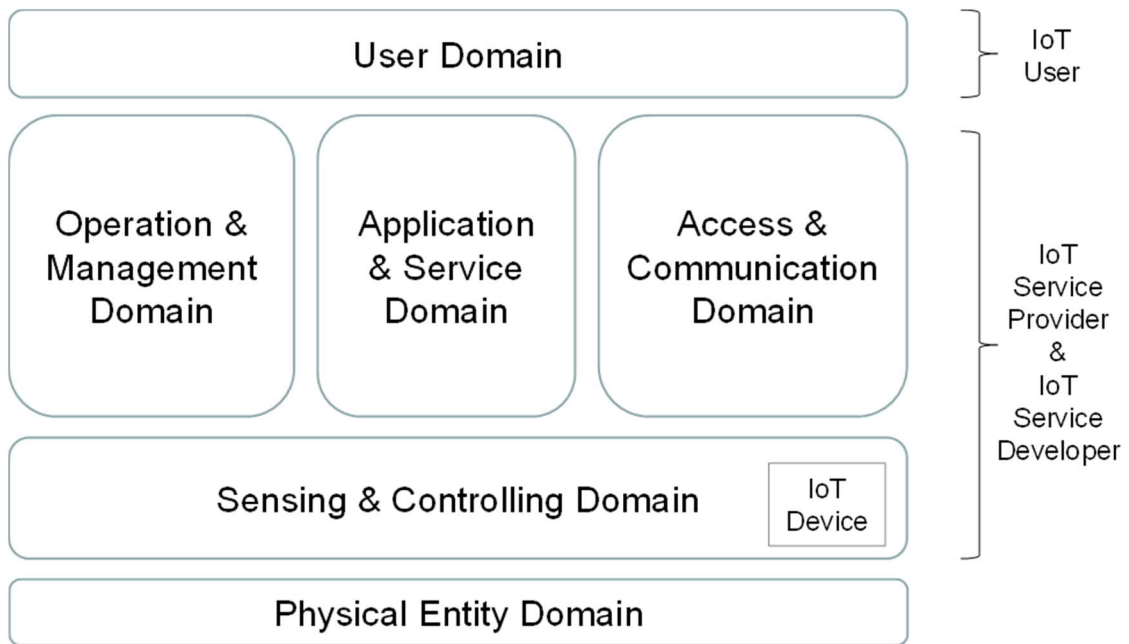


Figure 1.2: Domain Based Reference Model (Author based on ISO/IEC 30141 [15])

The sensing and control domain consists of IoT devices and sensors for detecting the state or characteristics of physical objects and regulating physical objects. This domain is essential to an IoT system by providing critical information to all other domains regarding the given environment. The discussion presented in this paper focuses on the security quality of IoT devices.

ISO/IEC 30147 [17] provides efforts to ensure the trustworthiness of IoT systems as a system lifecycle process and is applicable and complementary to the general system lifecycle process ISO/IEC/IEEE 15288:2015. This international standard was initially proposed from Japan based on the IoT security guidelines in Japan. And this standard is to provide a unified international approach to the trustworthiness of IoT services that will expand globally in the future in order to avoid the imposition of disparate requirements

in different countries. This standard explains that the concept of IoT trustworthiness is similar to that of dependability, which covers reliability, availability, maintainability and supportability and other related attributes such as durability, integrity, recoverability and robustness. This document also defines integrity and availability as constituents of security. Maintainability, supportability, durability, recoverability, and robustness themselves do not appear in the definition of IoT trustworthiness. However, they are attributes to achieve resilience and reliability of IoT trustworthiness. Therefore, the security of the IoT system is an essential element of the other trustworthiness elements, and the security of the IoT devices constituting the IoT system is also the essential element.

IoT devices are important entities that directly affect users as a position of contact with the physical space in the overall IoT system. Among the aforementioned characteristics, the relevant ones to IoT devices are the followings:

- Safety
- Long product lifecycle after placement
- Limited functional and computational capabilities
- Unintended network connectivity

It will be important to have the capability to design and develop IoT devices as securely as possible before shipment and to maintain them to update to evolving service operation environments and security threat situations after shipment.

1.4 Burden of Security Responses by IoT Vendors

Ten years after the video recorder problem, why do security problems, such as the use of weak passwords, remain unresolved? The author surmises the following as the main reason. For video recorder users, there was no disadvantage for them in user, and they did not recognize the security springboard problem because the device normally functioned. Consequently, the vendor did not perceive the issue as a product quality problem because user complaints might not exist. Moreover, IoT vendors consider improving user convenience such as the plug-and-play design concept may have been prioritized rather than security. Because IoT vendors must consider that a fewer number of user support cases is better for the product quality.

At present, security problems, such as the breaching and hijacking of remote connection authentication, persist. However, the author presumes that IoT vendors have

not recognized a security issue as a quality control target. This also may be attributed to the culture wherein the development of IoT devices was initiated by electronics vendors.

The characteristics of IoT vendors are likely to be the followings:

- Compliant to laws such as consumer product safety, electrical safety, product liability (PL), environmental load reduction (recycling)
- Compliant to intellectual property rights such as open-source software (OSS)
- Design the device with fewer hardware resources (small foot-print of silicon)
- Quality basics of ISO 9001
- Quality base culture with reduction of cost and defect rate (yield)
- Sharing quality control responsibilities among departments throughout the product lifecycle

There is no “security” context in this.

Many developers and researchers have adequately resolved information security problems via ISO 27001 [18] or discussed a new cybersecurity certification method [19]. Many IoT vendors recognize the importance of information security. However, they consider the issues to be handled by the information system department. Although ISO 27001 outlines the management and protection of information assets [20], [21], security quality management for the development of IoT devices is necessary throughout the product lifecycle and has to be defined similarly to the case of developing secure software [22].

In software development, the consideration of security as a quality factor is common to the extent that it has become an international standard. However, mechatronics development is the focus of electronics vendors. Although electrical and functional safety are both required to comply with the Product Liability Law, there is no law for IoT vendors who develops their hardware requiring security. Hence, the culture of incorporating security as a requirement into specifications does not exist. Therefore, in general, the quality assurance department is unfamiliar with security and may not even consider security as an evaluation target.

Thus far, IoT devices remain immature in terms of security and can be exclusively attacked by security hackers. In the past, IoT devices were few and might not have

been regarded as a target of attack. The author believes that this situation has not fostered a culture in which IoT vendors consider security as a quality factor.

Because the necessity of security only becomes evident when malicious activities occur on IoT devices by hackers, the conventional approach of ensuring the quality of products based on a certain probability of occurrence of problems undesirable to users cannot be applied for security assurance. On the other hand, from a technical standpoint, product development engineers have difficulty determining the weaknesses of that security attacker's target. Moreover, engineers occupied with product development do not have sufficient time to understand the numerous technical terms in security. Although they consider security necessary, they may not want to consider themselves in charge of providing or ensuring security. Generally, IoT vendors may think the consideration of countermeasures to reduce weaknesses and to ensure safety according to the appropriate perspective must be considered by security experts.

Pino et al. explained that the software development process is a critical factor for delivering quality software systems [23]. This implies that software quality is influenced by the nature of the development process. This strategy is similar to those implemented in other branches of engineering and industries [24]. Jones reported that most successful projects utilize similar patterns of planning, estimation, and quality control technologies [25]. A paradigm similar to software product quality must be observed for IoT devices because these products are controlled by the software.

Quality management in general ensures consistency in the promised features of the product or service offered to the customer and its performance. It has four main components: quality planning, quality assurance, quality control, and quality improvement. Quality management focuses not only on the quality of products and services but also on the means to achieve them.

Therefore, security measures are necessary; however, to guarantee the quality, it is necessary to define initiatives and visualize them as processes throughout the development cycle.

1.5 Scope of This Study

The author focused on IoT devices. This is for the following reasons. 1) Attacks on IoT devices are rapidly increasing. 2) These devices are mainly developed by electronics vendors unfamiliar with security initiatives. 3) The IoT devices are in the position of connecting to physical space and cyberspace; hence, they can affect users in the physical

space with abnormal conditions in cyberspace. As described in ISO 30141:2018 on the IoT reference architecture [15], [26], [27], IoT devices create an important connection between cyberspace and real physical space. Consequently, when IoT devices are under attack, both cyberspace and real physical space are confronted with security risks.

Security measures have been implemented for devices in information systems because security problems have been emphasized for years. In contrast, IoT devices with few security measures have spread across the market with limited defense against security risks in cyberspace. In addition, electronics vendors, who have no experience with IoT security and risks, have been developing IoT devices. For attackers, targeting IoT devices is easy through the wireless communication route, such as Wi-Fi or Bluetooth, or via the firmware update function. Because IoT devices are widely available in the market, the attackers can investigate their weaknesses in their hands, it is easier for them to identify the vulnerabilities compared to identifying those for information system devices. Thus, ensuring the security quality of IoT devices requires a standardized development process for IoT vendors to encounter security. Those processes must be defined throughout the product lifecycle, and they are understandable by IoT consumers.

The metrics presented in this paper are high-level; however, they are general perspectives that are independent of the product field. In addition, the author endeavored to render the metrics easy to understand for anyone involved in product development. It requires sufficient knowledge of security terminology but not technical security expertise..

1.6 Purpose of This Study

The goal of this study is to improve the ability of device vendors to develop secure IoT devices with a certain security quality. This will help for enabling users to become aware and informed of security quality when purchasing IoT devices. The IoT device security quality metrics are developed as a methodology for this purpose. To gain the trust and confidence of users, defining and implementing initiatives are necessary. With these, the initiatives and measures considered to ensure the security quality of IoT devices can be transparently explained to users.

Many electronics vendors are familiar with quality assurance for user safety but not with security. They typically conduct a hazard analysis to ensure the safety of their products. The process of identifying hazards, which are assumed to cause health and other problems, involves the study of countermeasures to prevent the occurrence of events. Subsequently, the results are reflected in the formulated design, clearly identifying what

to do and when to do it. To ensure security, it is basically the same as ensuring safety to assume the threats on devices and its results of risks.

The author surmised that the security efforts of IoT vendors could be promoted if some form of manual was available to check the security quality that anyone can implement to ensure a certain level of security quality without special expert knowledge. The author also conceived that it was important to structure the manual in such a way that departments (e.g., product planning, design, quality control, and market support) taking the initiatives in the phases of the product development lifecycle can comprehend their area of responsibility. For this purpose, the author deemed it necessary for the objective and reason of the initiative to be understood.

The IoT device security quality transparency model with six areas of the product lifecycle is devised for developing and supporting secure IoT products. Additionally, the IoT device security quality metrics are compiled for each area of the model using the Goal-Question-Metric (GQM) approach by referencing the requirements of various IoT security regulations and guidelines and the opinions of security experts. This model is a tool to aid each department members who are proactively working on each phase of the product development lifecycle to understand their own scope of responsibility. Security is generally considered to be a vague task for non-security experts. However, by identifying the goal and the initiatives to be accomplished in each area, the author presumes that the members involved in all the phases of product development can realize that they are all responsible for ensuring security quality.

1.7 Contribution of This Study

The primary contribution of the proposed methodology is to promote the ability of IoT vendors to set security quality metrics and to improve the security quality and security-aware capabilities of IoT devices. As security-secure IoT devices become more widespread, users' demands for the security quality of IoT devices will become louder. If such demands become louder, IoT vendors will also focus on security quality to improve the competitiveness of IoT devices. In this way, the increase in the number of IoT devices with high-security quality will contribute to broadening the choices of secure IoT devices for users.

The proposed approach will also help IoT vendors to understand the characteristics of IoT security regulations, guidelines, and certification program requirements. IoT vendors will be able to predict the nature of the regulatory and certification program

requirements that need to be met and will be able to allocate man-hours appropriately to ensure security quality. Furthermore, they can use this method to validate their own adjusted IoT security metrics against IoT security requirements from customers and regulations.

The author anticipates this study to contribute to the improvement of the situation in which many IoT vendors are unable to consider security as a quality requirement. The study can also aid these vendors to incorporate security into specific product development processes through its simple presentation of general ideas in the guidelines.

1.8 Structure of This Paper

This paper consists of nine sections. Section 1 discussed the background of this study, the definition of IoT devices, and the reason for setting the scope of this study to IoT devices. The remainder of this paper is organized as follows.

Section 2 explains the motivation and necessity of this study by describing the absence of previous work on IoT security from the perspective of quality. The necessity of this study is stated as follows: IoT vendors have not considered the security capabilities of their products as part of their quality control; there is no general metric for IoT security quality that is appropriate for IoT vendors; each vendor has to set their proprietary security quality metrics.

It also discusses the lack of appeal of security initiatives to IoT vendors based on IoT security guidelines and related literature. The section presents the hypothesis of the author regarding the root cause and six reasons for the vulnerability of IoT devices. Then, the literature survey conducted by the author to identify prior studies relevant to this research is elaborated. Finally, the section reviews the reasons for visualizing security initiatives.

Section 3 outlines the research approach on the IoT device security quality. First, the research method of the five-step approach adopted for this research is presented. This study adopts the five-step research methodology used by ENISA and other organizations (1. definition of scope, 2. literature review, 3. drafting of metrics, 4. review and collection of opinions by experts, 5. analysis of the review results and measurement of the effectiveness of the revised metrics). This section describes the research methods: 1. definition of scope, 2. literature survey. The author defines the scope of this study as step 1 to set the IoT devices. The main content of this section is the literature survey results (Step 2). In the literature survey, the systematic literature survey method is used to

conduct the survey in a snowballing fashion. An overview of the main topics of the survey results is provided in terms of the perspectives to consider when studying security quality metrics for IoT devices. The main perspectives are the current situation of IoT security, security attacks on IoT, notable IoT security incidents, product quality management, product liability, software quality metrics, security evaluation methods, and security guidelines. The author also discusses the fact that the security in the software quality model must be considered as a quality factor of IoT devices controlled by software. The author further discusses the rationale for using the GQM concept in the quality evaluation method.

Section 4 describes the development of IoT device security quality metrics. This section summarizes the results of the literature review and presents the first draft of metrics based on the concept of the GQM Method (Step 3). The author defined a framework, named the Transparency Model of IoT Device Security Quality, to set up metrics to cover the entire product lifecycle. And the first draft of metrics was revised to the sample set of metrics through the reviews by both security and quality expert groups. The model, which consists of six areas, enables a clear understanding of the efforts expended for the overall product lifecycle. The 37 references shown in Appendix 1 have been reviewed to identify the candidates enumerated in Appendix 2. An overview of the GQM methodology used as a reference for constructing individual metrics is presented. The specific goals, the questions to ask regarding these goals, and the metrics are set. The next part summarizes the discussion on the results of the security and quality review conducted by experts (Step 4) on the candidates; then, the analysis of the opinions of experts follows. In the last part of this section after the expert review and their opinion analysis, the author summarizes the proposed security quality metrics method for IoT devices.

Section 5 explains a part of Step 5 of the proposed method. In this section, the effectiveness of the proposed method is evaluated through interviews with two companies and a comparison of requirements with existing regulations and guidelines. The author examined the feasibility of the proposed method for IoT vendors. The author selected two IoT vendors and requested them to consider the use of the proposed method to incorporate product security initiatives into their existing product development process. Two evaluation criteria are defined, and the evaluation results of each criterion are discussed in this section. Next, the author evaluated the applicability of the method as a tool for assessing the characteristics of a set of existing security requirements. The author divided

the existing set of security requirements into three categories to evaluate IoT security: regulatory requirements, baseline requirements, and IoT certification requirements. The results showed that the proposed method is applicable as a tool to visualize the characteristics of each category of requirements.

Section 6 also considers Step 5. The author demonstrates the effectiveness of the sample metrics to illustrate the characteristic differences in the security quality of IoT devices through sample evaluation. The author selected two IoT dashboard cameras with similar functional specifications for evaluation. This section discusses the assessment results of the two IoT devices and the variations in security quality revealed by the method.

Section 7 discusses the social contribution of the results of this research. The contribution of this research is that it will lead to the development and diffusion of secure IoT devices by many IoT vendors by presenting a method for setting quality metrics that allows users to start security efforts without security expertise. In addition, as a social effect of this research, in addition to providing users who want secured IoT devices with options, this research will also contribute as a communication tool between IoT device vendors and users regarding the security quality of IoT devices. Three main contributions are identified. First, the proposed method is useful for improving the security quality of IoT devices. Second, it may be utilized as a security quality indicator in the selection of secure IoT devices. Third, when ensuring security quality is imposed as a product liability in the future, the results of the proposed metrics may be reference material encouraging the creation of a new market of cyber PL insurance to cover the cost of handling security issues in case of emergency.

Section 8 discusses future directions. Two main areas are presented for further studies. The first is the classification of metrics and evaluation axes for either product quality or process quality. The second is about how to display the evaluation results. The second is how to indicate the evaluation results. In this study, it was limited to bar graphs only. The second is the method of displaying the evaluation results. In addition, the application to development processes such as Agile and Development-Operations (DevOps) other than the conventional V-shaped development process is also mentioned.

Finally, Section 9 summarizes the conclusions of this study, and Sections 10 and 11 present the References and Appendices, respectively.

2 NECESSITY OF THIS STUDY

Security incidents and accidents on IoT devices such as the connected car hacking namely the “JEEP” incident leading to recall and the botnet “Mirai” malware to cause a large-scale distributed denial of service (DDoS) attack has become apparent. The spread of IoT increases cyber-attack risk in various industries sectors.

To encounter these issues, in the latter half of the 2010s, the public and private sectors in Europe, the US, and Japan stepped up efforts to develop guidelines, international standards, and laws and regulations to address this IoT security issue. In the US, California and Oregon have established state laws [28], [29] on security response to IoT, which have been in effect in 2020. Ministry of Internal Affairs and Communications of Japan (MIC) also released the regulation for IoT to default setting password [30]. The European Union Agency for Cybersecurity (ENISA) has also published some guidelines to promote IoT security in the industry [31]. And there have been several cases of lawsuits against IoT vendors regarding lack of security response. This is in the direction of requiring IoT vendors to be accountable for the security capability of their products.

Thus, IoT security response has become required in the market. IoT vendors need to communicate to users that they are security-ready and gain trust in the IoT systems they provide. Many of these guidelines and regulations had the goal of securing IoT devices since both problems of the Mirai and Jeep cases were security issues on connected devices.

2.1 Motivation of This Study

For the IoT era, the author foresees that not only functions and safety capability but also security capability should be one of the selection factors by users. Users will buy a better product with not only the functionality and safety but also with security, even if it is a little more expensive. For the security quality of IoT devices, users will surely be

willing to pay some extra. However, many IoT vendors have not been able to bring their attention to security quality.

For responding to those needs, IoT vendors should be able to explain the quality of their products to users. Due to cost issues, IoT vendors sometimes compromise the quality, not in line with the user's ideal. If the case, IoT vendors need to be able to explain what kind of quality they are offering, including compromises made due to cost and usage conditions. The same is for security quality.

If there is a method for users to know the security capability of IoT devices, it is beneficial for both purchasers and IoT vendors. And it is also beneficial for purchasers to select the IoT devices with the appropriate security level. For the establishment of such a market, a method to evaluate the security quality of IoT devices is necessary.

The author hypothesized the following reasons for the failure of many IoT vendors to initiate security measures.

- 1) Unlike product safety, responsibility for security is not regulated or required by law, with a few exceptions
- 2) The idea of how much security response is required is not yet generally accepted.
- 3) Excessive security response makes IoT devices expensive and hinders the development of IoT devices and services.
- 4) The security requirements of users are unclear.
- 5) It is a lack of incentives for IoT vendors to match security response costs
- 6) Lack of standardized methods for communicating security measures to users

The author thought that a method for confirming the security quality of IoT devices provided by the vendor is necessary to comprehensively and accurately communicate the security quality of the IoT devices to the users or the purchasers to resolve the issues above. The issues about IoT security can be categorized into the two questions as follows.

2.2 Question 1: Does any Existing Literature or Standard Covering Security Quality Control Measures for IoT throughout the Product Lifecycle Exist?

Many security experts have addressed the guidelines for IoT security management from the viewpoint of the basic principles, approaches, threats, and countermeasures. Security management is the identification of assets to be protected, followed by the development, documentation, and implementation of policies and procedures to protect those assets. Organizations use these security management procedures for information

classification, threat analysis, risk assessment, and risk analysis to identify threats, classify assets, and assess the vulnerability of systems.

To assess the security of systems, researchers have developed methods such as the Evaluation Assurance Level with Common Criteria certification based on ISO 15408 [32] and EDSA (Embedded Device Security Assurance) certification based on IEC 62443 [33]. However, these certifications are extremely professional for those in charge of designing and evaluating the quality of their products to understand the requirements and require the third-party assessment which makes the assessment costly. ISO 15408 focuses on quality assurance and assesses the level of validity and rigor of the assessment, and does not specify what initiatives to take, whereas IEC 62443 is specialized for critical infrastructure with the industrial control system, which mainly assesses the validity of threat analysis and communication protocol vulnerabilities and does not apply to general IoT. If an IoT device is for critical infrastructure that requires strict security standards and management, a certain amount of evaluation cost can be spent. But if you want to widely promote IoT devices for cost-sensitive general consumer applications, in-house security quality evaluation is appropriate, unless a third-party assessment is required as a particular requirement, just like for the general product development. Furthermore, both approaches do not present a simple way of describing the quality of security in IoT devices (for vendors and/or general consumers with no knowledge of security). If a general IoT device can be modeled, it may be possible to create a protection profile for that model. However, it is questionable whether it is feasible to create protection profiles for general IoT devices, which have been created for each product field.

There are benchmarks and assessment methods for information security that have been proposed [34], [35]. However, both fall short from a web-specific and a lifecycle perspective when utilized for product security in IoT. There is a template proposed to consistently describe the service level of a cloud service [36]; it is, however, specific to cloud services rather than IoT. Similarly, Baldini et al pointed out the importance of IoT security [19]; however, the article only mentions the certification scheme and does not cover the entire product lifecycle. IoT security has also been previously discussed [37], [38]; unfortunately, the discussions are limited to the security of communication protocols.

The more literature includes high-level guidelines and baseline requirements for IoT security for IoT vendors in 2020, discussion of security for IoT with AI (artificial intelligence) [39], [40] or with the cloud [41], and the user's quality of experience (QoE) [42], [43] in 2021. The extensive literature search failed to produce any literature

concerned with benchmarks or suggestions for secure development for IoT vendors. Thus, the author could find no simple, standard way of describing the status of security readiness from the perspective of product security in terms of the quality of IoT devices.

2.3 Question 2: Does Any Reason for Visualizing the Security Control Measures Exist?

Most electronics vendors producing IoT devices are familiar with ISO 9001, the international quality assurance standard that clarifies the process of product development to standardize the quality throughout the life of a product. Vendors predominantly follow the defined production process and do not perform anything outside the process for cost-efficiency. To prevent non-compliance, it is common to define (and visualize) processes for designing safe products and selecting components with a low impact on the environment.

Similarly, the modalities for product security should be defined in existing processes. In addition, the Information-technology Promotion Agency of Japan (IPA) reported that approximately half of the IoT vendors have specific policies; however, over 70% of them have no concrete standards for their security responses in product development [44]. This implies that the reason behind the lack of concrete action might be that IoT vendors have no clear understanding of who would be responsible for the security; moreover, they do not recognize security measures as their responsibility even if they knew the significance thereof. Because it is difficult to add security countermeasures at the implementation stage of the development process, engineers need to devise and apply effective countermeasures at inception. The confirmation of the effective functioning of the countermeasures at the verification stage is essential. If a new vulnerability emerges even after the product release, it must be fixed.

Therefore, the author affirmed the significance of standardized documentation according to ISO 9001 for quality control efforts and the results of these efforts. It is necessary to define actions to be carried out in each phase of the product lifecycle. The author considered the need for a methodology that would allow IoT vendors to tailor security quality metrics in addition to existing quality metrics for their products. This would, in turn, indicate to consumers the level of security quality of the IoT devices they develop. The author attempted to derive quality metrics for IoT devices based on the literature and perspectives reviewed by the experts.

2.4 Summary of This Section

In this section, the necessity of this paper was discussed in terms of the author's motivation, the presence of previous studies and literature, and the reasons for clarifying the metrics. First, the author hypothesized that the root cause of the security issues by vulnerabilities in IoT devices is the lack of security consideration as a quality issue by IoT vendors. After assuming six reasons for this as in 2.1, the author decided to examine how to construct the security quality metrics with consideration of those causes. Therefore, the author thought that it would be worthwhile to propose a security quality metrics method for IoT devices using a quality control approach and that it would make a new contribution to the industry.

The author surveyed existing research and literature to see if such a method had been proposed in the past. And the author confirmed that it did not exist. However, no literature clarifies who should consider what and when for the security in the development process of IoT devices. And there is no literature on quality control approaches as well.

The author also reviewed the reasons for visualizing security initiatives. Most vendors are familiar with ISO 9001 and have a culture of developing products according to a defined quality control process and quality checks. Without defining security initiatives in the product development process there, no matter how important they were, IoT vendors would not implement them. In reality, the IPA survey showed that 70% of the companies were not taking security measures. Therefore, the author thought that it would be easier for IoT vendors to take security initiatives by defining the security measures in their process.

3 RESEARCH ON IOT DEVICE SECURITY QUALITY

3.1 Research Method

A systematic literature review (SLR) [45] was conducted using a combination of keywords such as IoT, security, and quality metrics to find related work. The SLR with the snowballing way by the Wohlin guidelines consists of three steps: 1) Planning the literature review; 2) Conducting the review; 3) Reporting the review. In addition, the survey methodology adopted by ENISA [31] was adopted as the reference model of this research. This research method starts with a literature survey. The proposal then follows and is succeeded by proof of the effectiveness of the proposal, as in Fig. 3.1.

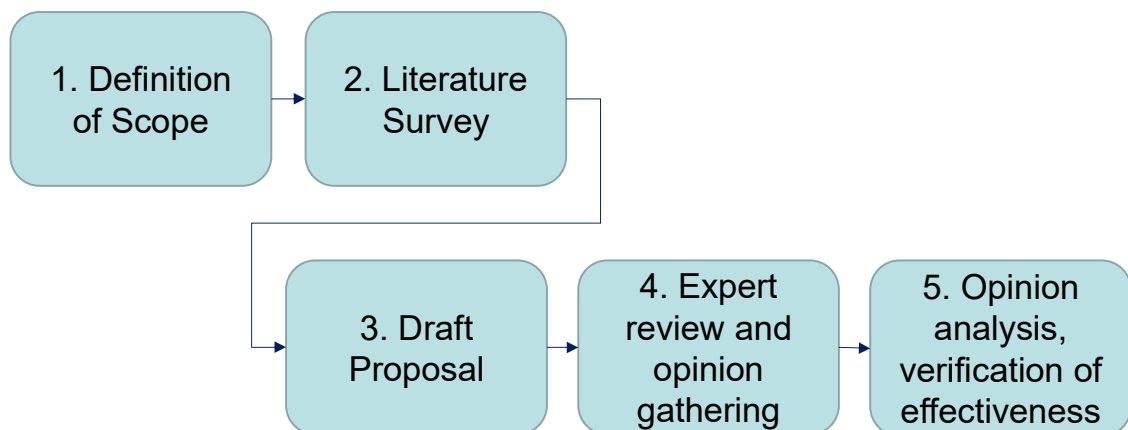


Figure 3.1: Research Method (Author based on ENISA [31])

Many security guidelines are formulated on the basis of similar sequences: screening the literature in the relevant fields, selecting items that fulfil the objectives of the guideline(s) to be developed, and reviewing the draft(s)—by experts and the public—before finalizing the guideline/s. In fact, ENISA's Baseline Security Recommendation for IoT includes items from the National Institute of Standards and Technology (NIST)

Cybersecurity Framework v1.1 [46] and the GSMA IoT Security Guidelines [47]. For example, there is a section about threat analysis that is cited in many studies. Therefore, this research method involving a literature survey is well-suited to this study.

3.2 Definition of Scope (Step 1)

To commence the research, the author defined the scope of this study as illustrated in Step 1 in Fig. 3.1 of the research method. An IoT system is complex and comprises many IoT devices, a network to connect IoT devices, and cloud services. Therefore, to simplify the discussion and the reasons discussed in section 1.5, the author focused on IoT devices primarily intended for consumer usage. The security of cloud services is covered under the information and communication technology (ICT) and software industry; there is no such culture as far as hardware is concerned. Historically, most electronics vendors are familiar with the physical or electrical safety aspects of quality, but few have ever faced a device connecting to the Internet under cyberspace fraught with malicious attacks. Most IoT devices are in the sensing and control domain, which are positioned to connect between cyberspace and physical real space.

What security attackers would want most would be identifications (IDs) and passwords for access authentication that could hijack IoT devices. Remote attacks are defined as the highest threat level to be avoided. If they can identify ID and passwords over the network, it will be simpler for the attacker and easier to attack. The Insecam and Mirai incidents reveal that many IoT devices are in operation with weak IDs and passwords, and packets searching for IoT devices with these weak IDs and passwords are constantly flowing on the Internet, and the number of packets is increasing every year.

On the other hand, since IoT devices are relatively inexpensive, there are many attempts to purchase them, physically disassemble them, and analyze the electronic circuit boards to steal the credentials stored inside. Black Hat, a famous security conference, provides hands-on training on this physical analysis method. Side-channel attacks are a well-known form of advanced hardware analysis. But they require advanced techniques and specialized analysis equipment, and the number of attackers who can perform them is limited.

In terms of the level of technical knowledge required for an attack, the easiest would be a port scan or Wi-Fi connection protocol scan over a network that requires the knowledge of the use of tools and PCs. The next most advanced would be an analysis of the electronic circuit boards of IoT devices that requires the knowledge and environment

of developing embedded devices. And the most advanced would be a side-channel attack that requires the knowledge of advanced cryptography and special equipment analyzing the leaked signals.

In this study, the author focused on IoT devices, and the process taken by the IoT vendors, because the behavior of IoT devices may directly threaten users' lives and their environment in daily life. Among the major attacks on IoT devices, the author will focus on online attacks, which have already become commonplace, and electronic circuit board attacks, which are becoming more widely known through hands-on seminars. Specifically, measures such as blocking Joint Test Action Group (JTAG) and Universal Asynchronous Receiver/Transmitter (UART) from the circuit board for mass production, and changing the initial settings of ID and password to device-unique settings at the time of shipment will be the scope. Advanced and/or expensive measures, such as secure elements that store credentials such as certificates for legitimate firmware activation and keys for encryption are not the main scope, and they are listed in Appendix 3 as optional candidates. In addition, the impact on safety caused by security issues in IoT devices is not in the scope of this study, as it will be discussed in the context of safety-related legal responses.

3.3 Literature Survey (Step 2)

In order to identify the appropriate items to express the security quality of an IoT device, the SLR has been conducted in the following field of documents.

1. Current situation of IoT security awareness of vendors
2. Notable security Incidents on IoT
3. Product Quality Management
4. Product liability on products
5. Quality metrics of software
6. Security Evaluation Method
7. IoT security guidelines

The SLR was conducted by setting the following start set keywords to snowballing search for public information.

- what is internet of things, IoT
- IoT, security, incident
- IoT, vulnerability, threat analysis, risk assessment

- security, certification, maturity model
- product quality, liability, lifecycle, recall
- quality assurance, indication, labeling
- software, quality, metrics
- product safety, accident report

The author conducted iterations of forward and backward snowballing SLRs.

3.3.1 Current Situation of IoT Security Awareness of Vendors

To understand the current situation of IoT device security, the study was conducted from two viewpoints; one is the survey of IoT vendor awareness; another is the security threat cases on IoT. First, the research on the security awareness of IoT vendors is discussed.

The IPA conducted a survey and issued reports [48], [49] on the current status and awareness of security measures in IoT devices and service developers. The IPA reported that vendors considering security and conducting vulnerability assessment was 70%, hence only about 40% of vendors perform secure programming or code-review at the design phase as shown in Fig. 3.2. The survey results revealed that only about 30% of all vendors have internal rules and processes for product security, and 0% of IoT device vendors. In fact, in the results of asking IoT vendors whether they had a policy for security standards and responses during product development, 35% of the respondents said they had a policy.

By product category, as shown in Fig. 3.3, awareness is relatively high in the network equipment category, with about 60% of vendors responding that they have a policy, while there were no vendors with a policy in the consumer IoT equipment category. Compared to the network equipment sector, awareness of supporting security for the sectors of the industrial IoT devices and the consumer IoT devices are low in the rate of having the security policy. The reasons given for the lack of security support for IoT devices included limited resources for IoT devices, difficulty in passing on the cost of security support to the price, and lack of personnel with knowledge of security measures.

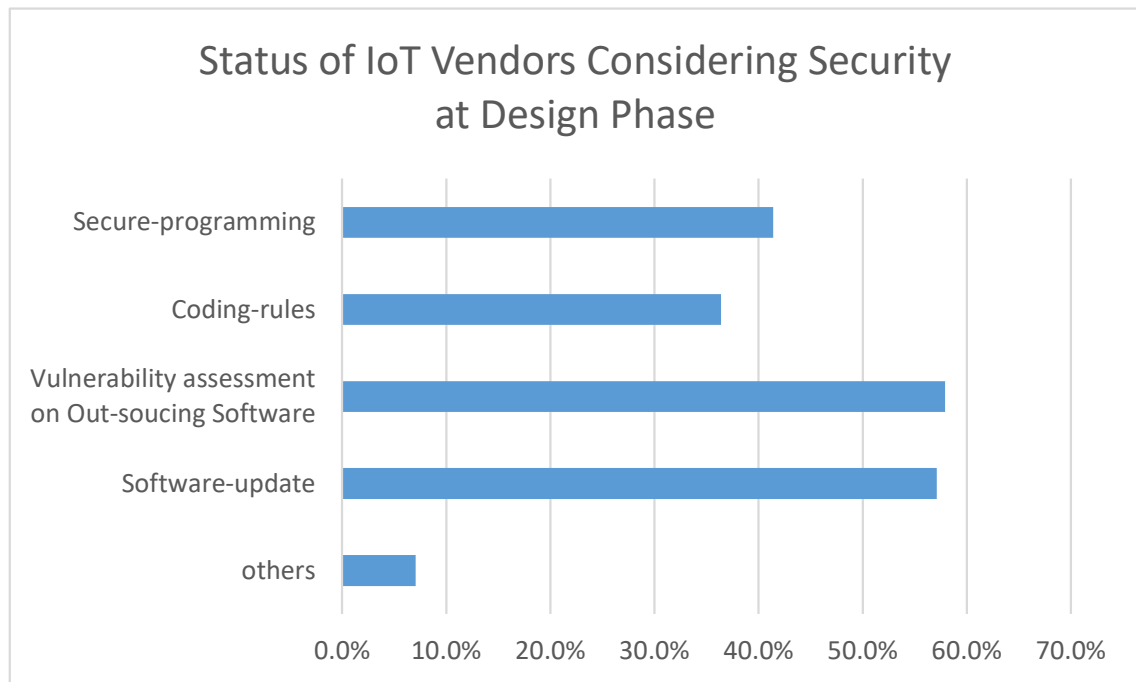


Figure 3.2: Status of IoT vendors considering security (Author based on IPA [47])

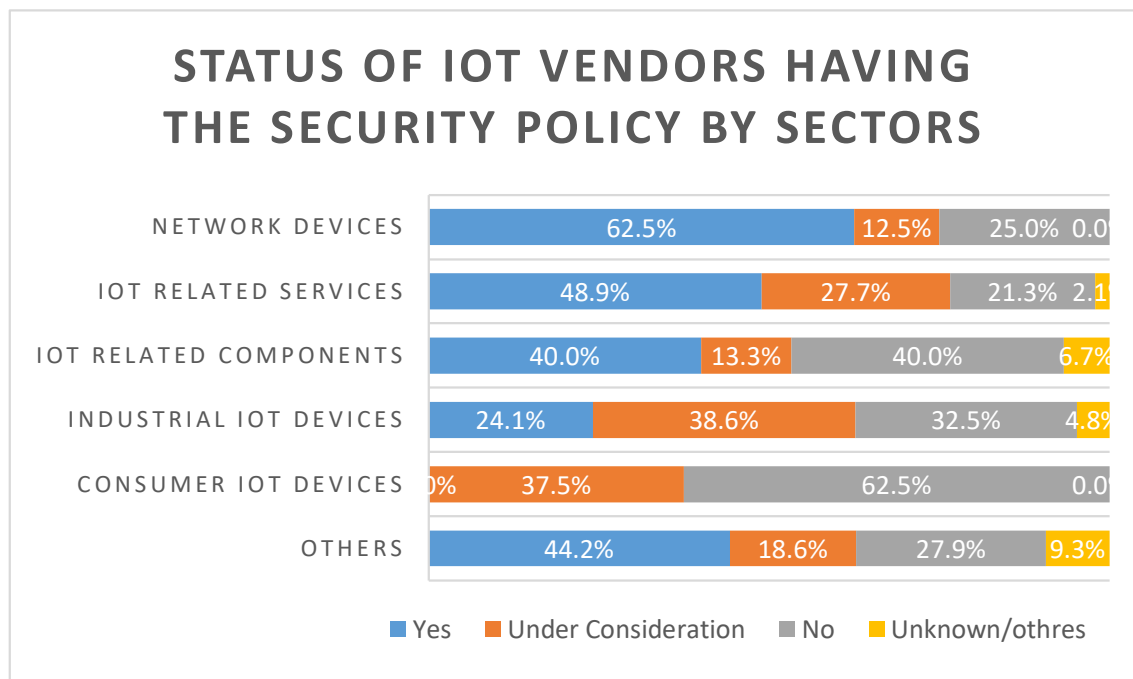


Figure 3.3: Status of IoT vendors having the security policy by sectors (Author based on IPA [47])

3.3.2 Security Attacks on IoT

In this part, the research on the security threat situation on IoT is discussed. National Institute of Information and Communication of Japan (NICT) reported the observation

results and analysis of communications relevant to a cyberattack in 2019 [50]. According to them, they observed communications relevant to a cyberattack in 2019 were about 1.5 times higher than in 2018, an increasing trend over the last years as shown in Fig. 3.4. And there was a significant increase in the number of scans from overseas organizations, accounting for 53% of the total packets observed; the trend in communications targeting IoT devices was similar to 2018, with Telnet (23/TCP) attacks, the most common, accounting for a slight increase. There was a slight increase in the number of attack packets targeting Telnet (23/TCP) from 29.4 billion to 36.4 billion packets. Other Ports accounted for a noticeable half of the total but included many ports used by IoT devices, such as ports for device web management interfaces, UPnP-related ports, and ports for device-specific services.

These results show that attacks on IoT devices are commonplace at a high rate. IoT vendors should be aware that IoT devices are under a storm of attack packets. If the security quality of IoT devices is not improved, they will soon fall into the hands of attackers.

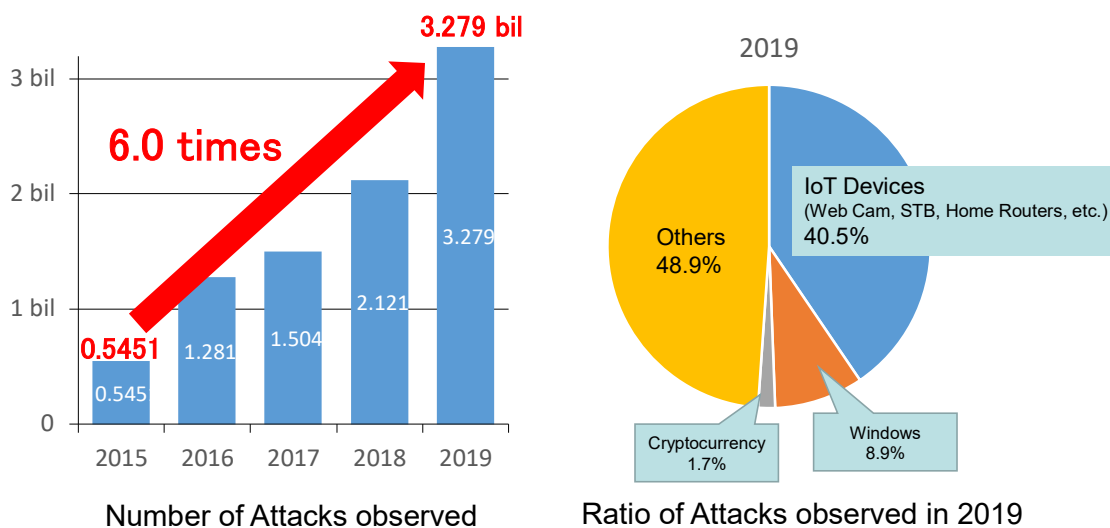


Figure 3.4: Attacks observed in 2019 (Author based on NICT [50])

Security attacks on IoT devices are varied; the main ones raised in several studies [51], [52] and the author's experiences on IoT security attacks are as follows.

- Attacks remotely via network (on-line)
 - TCP/IP port scanning targeting weak access authentication (ID/password) settings (spoofing for malware infection)

- Communications sniffing (especially attacks on Wi-Fi and/or Bluetooth connection procedures)
- Firmware updates (forcing users to update to malicious firmware on an attacker site)
- DoS attacks
- Attacks physically on IoT devices
 - Extraction of credentials through internal analysis using debugging ports left on electronic circuit boards such as JTAG and UART during product development
 - Firmware binary analysis (to identify adopted Open Source Software (OSS) components possibly vulnerable)
 - Firmware update via Universal Serial Bus (USB) (to update to malicious firmware)
 - Side-channel attacks (targeting sensitive information inside the device (cryptanalysis) by observing the operation of the cryptographic device through various physical means)

Not limited to these, there are many other vulnerabilities inherent to IoT devices.

3.3.3 Notable Security Incidents on IoT

There were lots of IoT security incidents in the past. The followings are well-known and notable examples of IoT.

3.3.3.1 Stuxnet, Iran 2010

The malware made the nuclear facility operation system down even the system was isolated from the outer network. Social engineering attacks with USB flash drives enabled this attack in a non-connected environment [53]. Fig. 3.5 illustrated this incident. Before this incident, it was taken for granted that the isolated area with firewalls or physically separated networks would be perceived as a secured environment with security measures in place. This lesson was the collapse of the myth that the isolated network is safe.

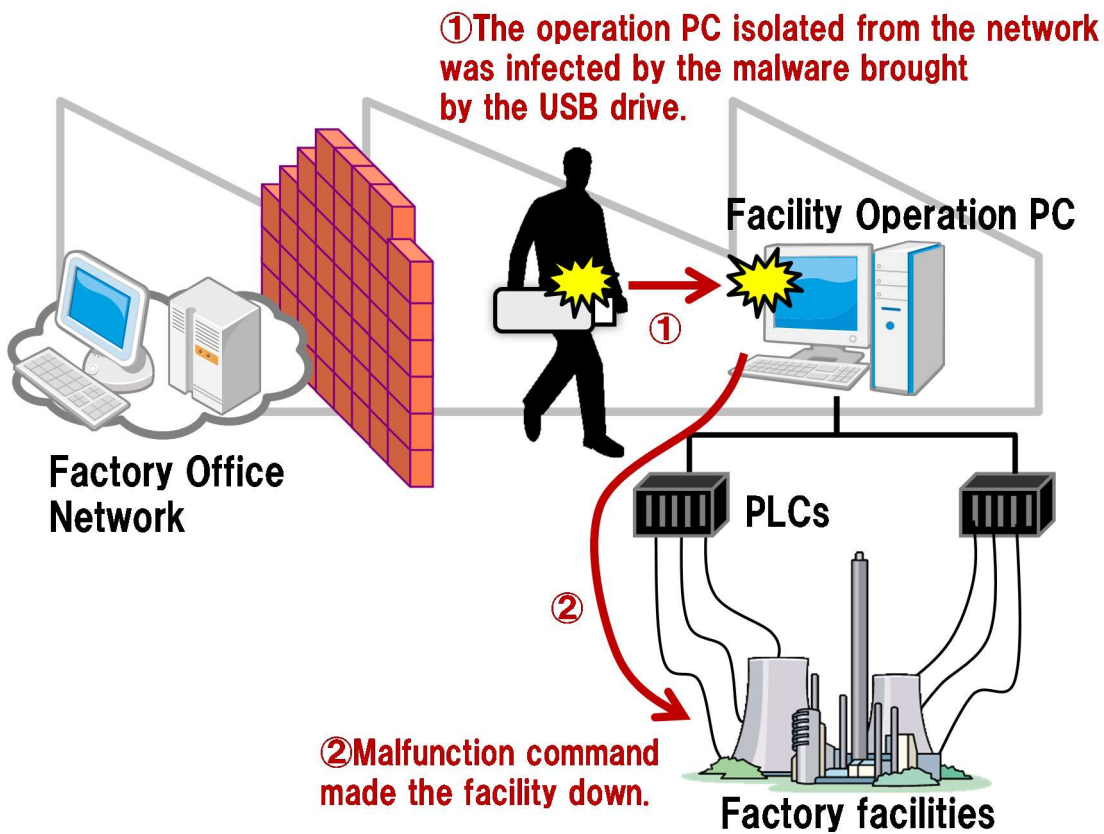


Figure 3.5: Image of the Attack using the USB drives (Author based on [53])

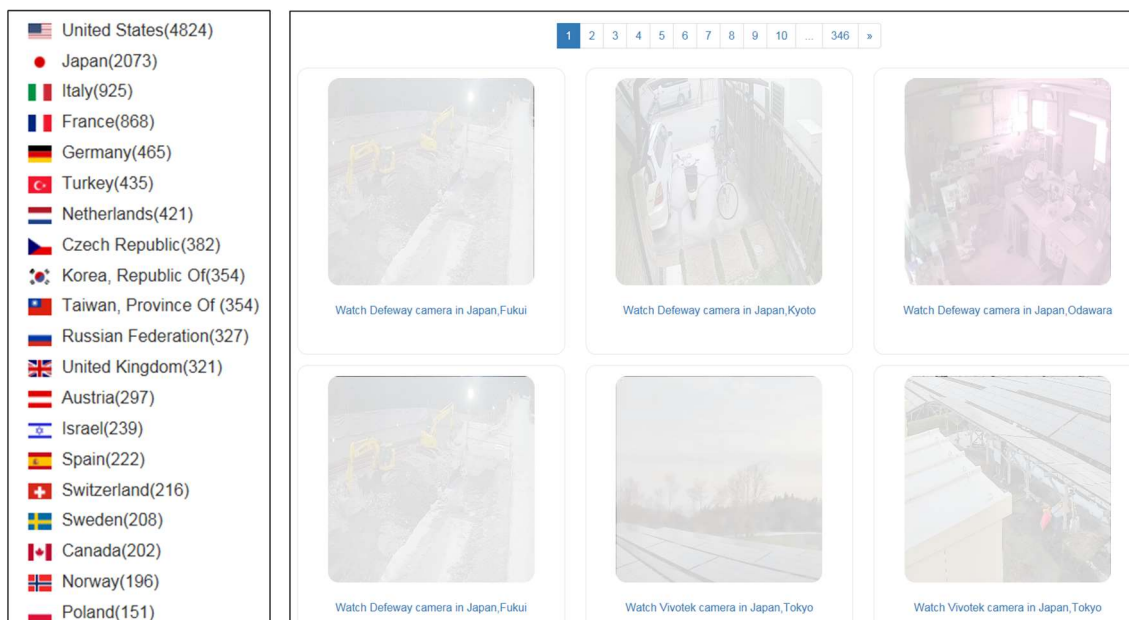


Figure 3.6: Insecam Web Site [54] (as of Dec 2020)

3.3.3.2 Insecam, Russia

The Insecam [54] is a collection site of network cameras that are in use with the factory default ID and password. Fig. 3.6 is the front page of the site. The site provides a selection of network cameras by country and city. The purpose of the site is not intended to attack network cameras, but it presents the reality of the current situation of network camera usage that anyone can access remotely. This is caused because a factory pre-set (default) password was all the same and those are publicly available via the user's manual. The lesson was that most users use the device as they use the device with a factory pre-set. The market and IoT vendors should learn the reality of how many IoT devices have been used without changing the default common ID and password.

3.3.3.3 Jeep Connected Car, Black Hat USA 2015

Miller and Valasek reported their demonstration of realizing the remote-hacking without any physical alteration in Black Hat USA 2015 [55]. They have demonstrated that it is possible to remotely interfere with the operation of air conditioners, wipers, brakes, gear shifting, steering, and engine on/off of a car in operation, and also possible to obtain information about the car at all times. The cause was a lack of confidentiality of the IP address of the head-mounted display through the Wi-Fi connectivity, the 3rd generation (3G) carrier network security for an emergency call service, and no authentication in the execution process of firmware update on the head unit. The impact of this report leads to the recall of 1.4 million cars of Jeep.

This event was a catalyst for the entire automotive industry to focus on security for the future era of automated driving. And the event was also a learning experience for Car manufacturers to clarify the roles of carriers and suppliers of head units regarding security in ensuring the security of the entire IoT system.

3.3.3.4 Mirai, 2016

This was a characteristic incident of the IoT era that the Botnet malware called “Mirai” was to execute a large-scale (1Tbps-class) DDoS attack on a target site [5], [56]. Mirai infected vulnerable network-connected devices such as routers, surveillance cameras, recording devices, and so on. This attack was a similar vulnerability of Insecam, caused by the default password not being changed from the factory pre-set or well-known password popularly used. Fig. 3.7 illustrates the botnet. The passwords publicly known by shown on the user manual or service manual were collected as a dictionary to attack IoT devices of telnet 23 port.

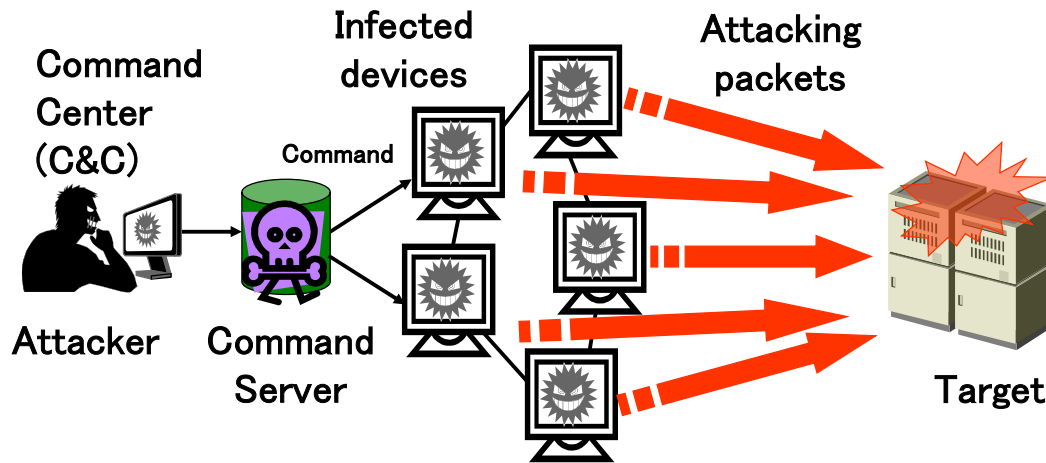


Figure 3.7: Image of the Botnet

Since the main attack vector for IoT devices is the point of connection to the network where the attacker may reside, the most basic access defense to control IoT devices is access authentication using ID and password. If the combination of ID and password is easy to guess, it is easy to impersonate someone else and gain access to the device, so it is important to make the combination difficult to guess. However, in general, people tend to prioritize convenience and use IDs and passwords that are easy for anyone to remember, and this situation has been exposed.

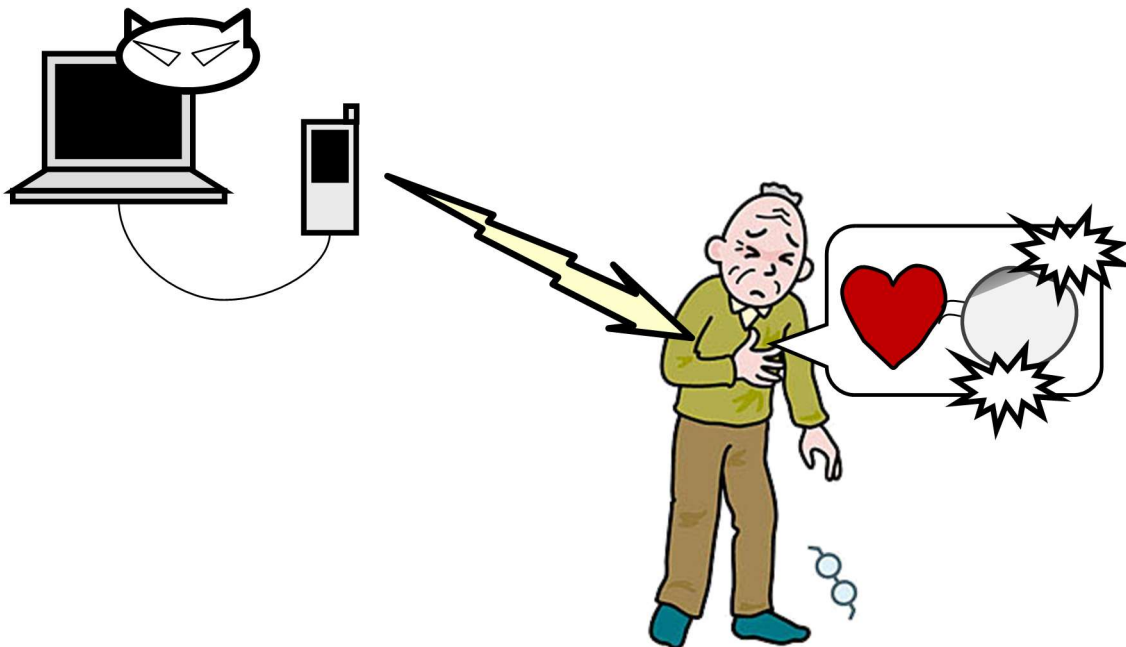


Figure 3.8: Image of Pacemaker Attack

3.3.3.5 FDA Alert on Cardiac Pacemaker, 2017

This incident was also led to the recall of 465 thousand devices because Food and Drug Administration (FDA) in the US made an alert [57]. The attack target was the vulnerable wireless setting function and no authentication of control commands. Fig. 3.8 illustrates the incident.

There was a similar vulnerability was seen at the Jeep incident said above, which was no authentication of control commands for replacing the firmware of the device. It is important to learn the lesson from the past incidents not to repeat the same in the future. Also, it would be important to share the lessons across the industry sectors.

3.3.3.6 Attack vectors on IoT Devices

From the above four cases, the target in all cases was weak IDs/passwords for remote access. These are problems before the level of technical issues requiring security expertise. In addition, the Jeep and FDA warning cases were recall cases that resulted in the vendor being held responsible for the response, suggesting that security issues are becoming a quality issue for vendors.

Attack vectors to search a vulnerability of IoT devices include not only online attacks via networks, but also physical attacks on the circuit board. The physical attack takes advantage of the situation where the actual IoT devices can be obtained without incurring significant costs because of the availability of the used and junk market. The Jeep case was an attack that skillfully used both online and physical attacks. Table 3.1 summarizes the characteristic attack paths of IoT devices.

Table 3.1 Type of Attack Vectors on IoT Devices

Type of Attack	Online Attack	Physical Attack
Interfaces used for development and debugging	Communication port search	Analysis from JTAG and UART port on the board
External connection interface	Exploiting Wi-Fi/Bluetooth Specification Vulnerabilities Internal Structure Search	Internal structure search via USB connection
Chip on circuit board	-	Credential information fraud (side-channel attack)

3.3.4 Product Quality Management

IoT devices are one of the electronic devices that have been used in the past, and like electronic devices, users require product quality. In this section, quality will be reviewed.

3.3.4.1 What is Quality?

“Quality” is defined in ISO 9000:2015 [58], [59]. According to ISO 9000, quality is "the degree to which a set of inherent characteristics of an object fulfills requirements. Since there is no set measurement method for quality, there is no clear unit of measurement. Criteria are defined by requirements, and the degree of achievement of the requirements is evaluated by the standards.” Moreover, the quality requirements change over time. For example, food quality was mainly about safety in the past, but nowadays, nutritional value, taste, and appearance are also important factors.

Quality control efforts began on the manufacturing group of people, and most of the elements derived from hardware meant physical elements that could be manageable numerically. Later, as the term "quality" became more common and widely demanded by society (the market), the scope of interpretation and application of the term became much broader. This phenomenon indicates that customers' attitude towards the quality of products is expanding beyond the functions of products described in the catalogs. Moreover, the fact that a product functions according to specifications and can be safely used is also considered.

Two aspects are needed to ensure the quality of products. One is the product quality, and another is the process quality [60]. The product quality is the result of the development. The process quality is the sufficiency of the work performed in development and quality checks. To verify the quality of each of these, metrics and targets are established.

3.3.4.2 ISO 9000

ISO 9000 [58] is the major international standard for a quality management system. It is based on the PDCA cycle to make improvements. ISO 9000 has enhanced the risk base management in 2015. The risk in quality management is different from the risk of security, but the risk-based approach should be an important factor. Many manufacturers comply with this international standard to demonstrate to their partners and users that they are committed to quality control of their products.

3.3.4.3 Law of Food Labeling (in Japan)

The purpose of the Food Label Act is, because the labeling of food plays an important role in ensuring safety when consuming food and in ensuring opportunities for voluntary and rational selection of food, to ensure the appropriateness of labeling of food offered for sale by establishing standards and providing other necessary matters, and thereby to promote the interests of general consumers [61].

The content of food labels has historically changed. In the beginning, it was just the manufacturer, date of manufacture, storage method, and additives; since 1970, ingredients, country of origin, and content have been added. Later, expiration dates, country of origin, presence of allergic substances, genetically modified materials, etc. were added [62]. This is another result of the change in the content of information necessary to ensure the safety of consumers' health and their choice of foods over time.

3.3.4.4 Consumer Product Safety Act (in Japan)

The purpose of this Act is to protect the interests of general consumers by regulating the manufacture and sale of specified products, promoting the proper maintenance of specified maintenance products, and taking measures such as collecting and providing information on product accidents, in order to prevent danger to the lives or bodies of general consumers caused by consumer products [63].

This law set the following rules:

- Product accident information report and publication rule
- Long-term product safety inspection and indication rule

To protect consumers, product safety has been highly emphasized and laws and regulations have been imposed. When cyberspace has become a social infrastructure and IoT devices support consumers' lives, it is natural to consider the security aspect as one of the safety factors to be covered.

3.3.5 Product Liability

Economic Planning Agency in Japan expressed their understanding of “Product Liability” and said, “The software itself is immaterial and is not subject to product liability. However, the product in which the software is embedded may be covered by this law. In the case of an accident caused by a product incorporating software due to a defect in the software, the defect in the software may be interpreted as a defect in the product itself, and in this case, if a causal relationship is recognized between the defect and the damage,

the manufacturer of the product will be liable for damages under this law. In this case, if a causal relationship is found between the defect and the damage, the manufacturer of the product shall be liable for damages under this law.” [64]

In addition, the agency also said that the manufacturer of the product will be liable for damages if the vulnerability itself is considered to be a defect and other requirements are met. By the cyber-physical nature of IoT, it is considered that certain security measures will be indispensable as the manufacturer's responsibility. The case where the vulnerability is considered to be "defective" is, for example, the situation where the software does not have the "security" that is normally provided at the time of provision.

The efforts to ensure security in software and system development are becoming more common to gain trust as a secure service [65]. This trend is expected to apply to IoT systems as well.

3.3.6 Quality Metrics of Software

Software quality control has traditionally been a challenge because an established method for assessing software quality did not exist. In the past, attempts such as visualization by using a bug curve and the number of defects identified have been tried as a method for quantifying software quality. On the other hand, in terms of software reliability, some studies observed that consistency, availability, and maintainability (less downtime) resulted in improved quality. However, when the security perspective is considered, the quality of the product appears to depend on transparency. Before getting into a discussion about security quality, the discussions about software quality were reviewed.

3.3.6.1 Quantification of Quality

If there is any good example of describing the quality of software-driven products, the quality indication of IoT devices should be the same or similar. Then, the research was conducted on the past challenges to quantifying the quality of software.

Around 2010, the quantitative quality control method for software became popular in Japan. There were two guidelines found: one by the Ministry of Economy, Trade, and Industry (METI) [66] and the other one by the IPA of Japan [67]. The challenge was to quantify the number of defects pointed out. Then, it is visualized as “the bug curve” with review effort density/review point-out density. This could be used for the improvement of the security capability of IoT devices when the number of detected vulnerabilities is used as bugs.

ISO/IEC 25010:2011 [68] has been revised in 2011, the 25010 defined software quality as the ability of a software product to meet an explicit or implied need when used under specified specific conditions. The quality model determines which quality characteristics as shown in Fig. 3.9 will be considered when evaluating the properties of a software product. There are eight quality characteristics and five sub-characteristics for security: 1) security (confidentiality), 2) integrity, 3) non-repudiation, 4) accountability and 5) authenticity.

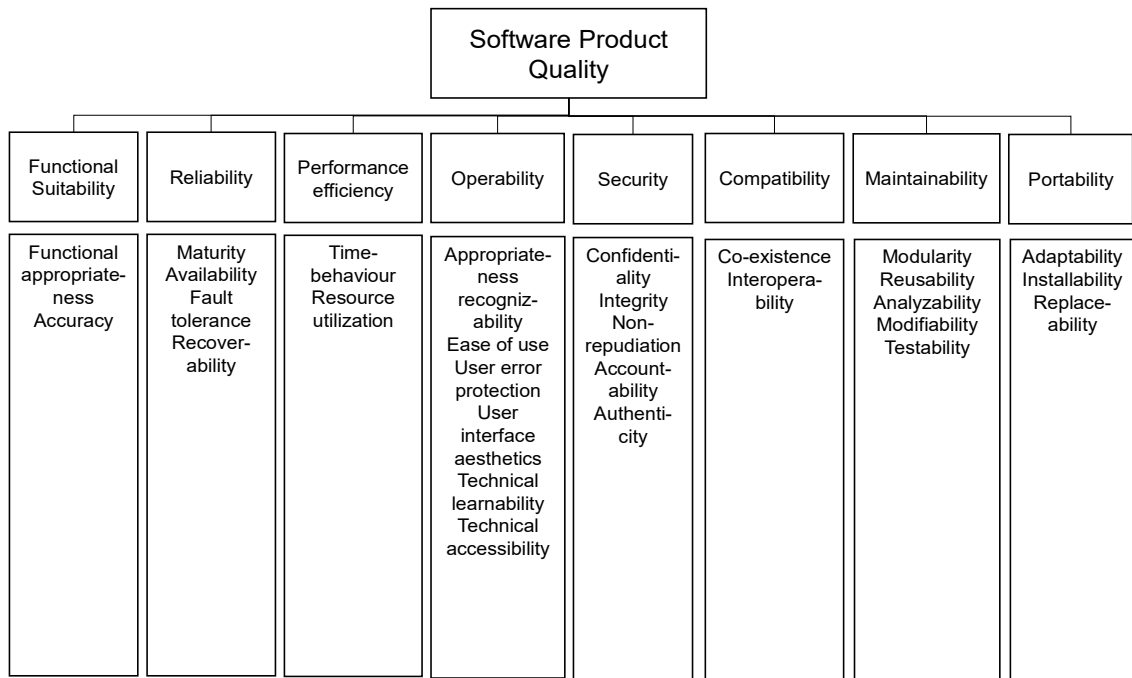


Figure 3.9: Software Product Quality Model in ISO/IEC 25010

IPA and the Union of Japanese Scientists and Engineers also pointed out the need for a quality definition from the customer point of view [69], [70]. They said that the quality was determined by the customer's evaluation (satisfaction). There is some variation in quality. The level of quality is that increasing the value does not satisfy customers psychologically, but lowering the value makes them unhappy, which is the basic quality that the customers demand. The other level of quality is that customers are not dissatisfied if certain features are absent but are psychologically satisfied when those features are present.

3.3.6.2 Reliability in Quality

Another research was conducted on the software quality aspect in reliability. Yamamoto compared five approaches [71]. The comparison results was shown in Table 3.2.

Table 3.2 Comparison of the Quality Requirements [71] (modified by Author)

	Davis	Gilb	ISO	KS	P
Development Condition					
Failure rate during development	O		O		
Terms of Use	O	O		O	O
Fail-safe			O		
Failure rate during operation	O		O	O	O
Resiliency/Failure Lifetime	O	O	O	O	O
Impact	O				
Suitability			O		

- 1) Alan Davis 1990 : The ability of the software to behave consistently in a manner that is acceptable to the user in the environment intended to be used.
- 2) Tom Gilb 2005 : Low-level concept of availability among performance requirements (same level as maintainability, integrity).
- 3) ISO 9126 2003 : the property of maintaining a specified level of achievement (including maturity, Fault tolerance, Recoverability, Compatibility).
- 4) Kotonya, Sonnmerville 2002 : constraints on the run-time behavior of the system, and two aspects of availability and failure rate.
- 5) Pfleeger 1998 : The probability of the system operation without failure under the given conditions in the given time interval.

Davis insisted the value of behavior consistency is reliability. Tom insisted on the availability. ISO9126 focused on maintainability as the key to reliability. ISO9126 also sorted out the software quality properties as Functionality, Reliability, Usability, Efficiency, Maintainability, and Portability. Kotonya insisted on two of availability and failure rate, and Pfleeger insisted on the operation without failure. One thing to say, all of them are paying attention to the system running in a normal manner without irregular action. The author could not find any basic understanding or consensus reached in the software quality community.

3.3.6.3 Transparency for Trust Building

Transparency in the process of delivering products is important to gain trust in product quality. Many organizations emphasize transparency for quality credibility. Regarding security, some approaches are made to gain public trust by increasing the

transparency of corporate efforts on security activities. This could be one measure to indicate the vendor's quality of security.

Microsoft demonstrated their transparency by three activities in 2009 [72] as follows:

1. Acknowledgement: publicly acknowledged the vulnerability
2. Workaround: reduce the immediate risk to affected users by supplying a workaround
3. Communication: actively participated in a public dialog about the vulnerability, continued to update the security advisory with new information, speak with the press.

Traditionally, security efforts are presumed to have been done privately, but Microsoft has made a major policy change. They have taken a policy of gaining the trust of their users by revealing their progress and the systems in place to properly deal with any security issues that may be discovered.

Kaspersky is another example. To recover the trust from the US, United Kingdom (UK), and the Netherlands who decided to prohibit the use of Kaspersky's products, Kaspersky shifted to the open strategy that demonstrates their transparency program with four activities as follows called "Global Transparency Initiative" [73].

1. Auditing and accreditation of technical processes by a 3rd party organization
2. Starting and expanding the bug-bounty program
3. Reviewing the source code and updates by a 3rd party organization
4. Restructuring R&D infrastructure

There is no single way to describe the software quality and reliability. But, ensuring transparency by engagement and communication with other organizations to reveal their insight of security activities should be important to indicate their security quality to gain the trust of users.

3.3.6.4 Quality Management over the Supply Chain

It is important to manage the security throughout the supply chain for IoT since the IoT device is a system that integrated and assembled the components developed by multiple vendors. ISO 27036: 2016 - Information security for supplier relationships [74] is the guideline for managing the ICT supply chain security. Various security controls are included based on the system lifecycle stages (ISO15288: 2015). The goal of this

guideline is to present how to build an “extending trust environment with shared responsibility for security” through the supply chain.

The national center of Incident readiness and Strategy for Cybersecurity (NISC) of Japan released a guideline for formulating specifications for supply chain risk management on information security in outsourcing [75]. This guideline is describing “how-to” for the procurement side such as government officials to implement compliance matters properly regarding supply-chain risk in information security in case of entrusting a system development to a 3rd party or purchasing ICT devices. This could be an item for assessment in-process quality to see the level of care of the supply chain risk.

3.3.7 Security Evaluation Method

There are several ways to evaluate the security in technical about products and maturity of organization activities. This section describes the several ways of security evaluation available in the market. There is a presentation that discusses what can be measured about security in the past. Abbadi discussed what metrics are, the need for metrics, examples of security metrics in the past, types of security metrics, etc. He concluded by saying that what users want in the end is something like a Food Label [76]. I concluded. However, there were no concrete recommendations on what kind of metrics would be good for the end-user.

3.3.7.1 ISO/IEC 15408

ISO/IEC 15408 [77] is the international standard for information technology product security certification and is known as “Common Criteria (CC) [78].” ISO/IEC 15408 provides the framework for evaluating that products and systems related to information technology have been properly designed and that the design has been correctly implemented from the perspective of information technology security and for determining the security level of confidence, the Evaluation Assurance Level (EAL). According to CC [32], there is an international agreement through the Common Criteria Recognition Arrangement (CCRA) to recognize the certification issued at one of the CCRA member countries.

In order to investigate and evaluate the security of IT systems and products, experts from accredited partner labs must first define the target of evaluation (TOE) and conduct further evaluation of current and applicable documentation. The targets defined earlier are then evaluated in detail. The CC evaluation verifies the claims made about the safety target and confirms the security function of the target by examining the following points:

- Security Target (ST), a document that identifies the security properties of a target
- Protection Profile (PP), a document that identifies the security requirements for a class of security equipment
- Security Functional Requirements (SFRs), documents that specify the individual security functions that a product may provide

To determine the level of confidence in a product's security features, a thorough CC evaluation by a contracted third-party laboratory includes the following quality assurance processes:

- The Evaluation Assurance Level (EAL) corresponds to a package of security requirements and assesses the depth and severity of the CC evaluation.
- Security assurance requirements (SARs) describe the measures taken during the development and evaluation of safety products to ensure compliance with claimed security features.

Table 3.3 Seven levels of EAL

EAL Level	Description
1	Evaluators analyze manuals and functional specifications and conduct independent testing.
2	Developers test functional specifications (external interfaces) and analyze for obvious vulnerabilities. The evaluator verifies the program structure using high-level design documents, sampling tests, and penetration tests for obvious vulnerabilities.
3	Developers conduct testing and misuse analysis up to the higher level (subsystem level). Evaluators assess the development security and configuration management status of development artifacts and conduct their vulnerability analysis.
4	Developers automate configuration management. Evaluators use lower-level design documents to verify the process. Source code is also verified for important parts.
5	Developers create a high-level design document using anti-formal description reduction. Evaluators analyzed all source code and hidden information leakage routes.
6	Developers create a lower-level design document using a semi-formal description language.
7	Developers design and test based on a verification method using a semi-formal description language.

There are seven levels of EAL as described in Table 3.3. The EAL is selected based on the value of the protected assets in the TOE and the level of confidence required in the security function. The EAL is a measure of how well the evaluation target has been verified. The EAL 4 is generally considered to be the highest level for commercial use.

Since the U.S. government requires digital MFPs to be certified in order to prevent document data leaks, CC certification has become widespread in the digital MFP field. In addition, IC chips installed in credit cards are also targeted to prevent financial damage. ENISA is considering a certification scheme based on the concepts of ISO/IEC 15408 and ISO/IEC 18045 as the European Union's Cybersecurity Certification scheme (EUCC). A strict evaluation like the CC is necessary on the 18045-based for the IoT service and the 15408-based for IoT devices. Because the third-party evaluation work leads to rigorous evaluation is costly, it is unlikely that consumer IoT devices will be voluntarily certified, as CC is generally not obtained unless requested by the customer, and the cost is a barrier.

3.3.7.2 IEC 62443-4: EDSA Certification

International Electrotechnical Commission (IEC) explains that The IEC 62443 series was developed to secure industrial automation and control systems (IACS) throughout their lifecycle [79]. IEC also addresses that IT standards are not appropriate for IACS and other OT (operational technology) environments, because they have different requirements on capability and availability, and equipment lifetime. In addition, IEC emphasizes that cyber-attacks on IT systems have are essentially economic consequences, while cyber-attacks on critical infrastructure can also be heavily environmental or even threaten public health and lives.

IEC 62443 covers not only the technology that comprises a control system, but also the work processes, countermeasures, and employees, and takes a risk-based approach to security, which is based on the concept that it is neither efficient nor sustainable to try to protect all assets in equal measure.

The IEC 62443 series consist of four parts:

- Part 1. General contents covering terminology, concepts, and models
- Part 2. Policies and procedures covering methods and processes associated with IACS security

- Part 3. System part covering Security technologies for IACS, Security risk assessment for system design, System security requirements, and Security levels at the system level
- Part 4. Component part covering secure product development lifecycle requirements and Technical security requirements for IACS components

A program that certifies conformity to the requirements of Part 4 is Component Security Assurance (CSA) by ISASecure [33]. The Embedded Device Security Assurance (EDSA), the first ISASecure certification, focuses on the security of embedded devices and addresses device characteristics and supplier development practices for those devices and is designed to certify to international standard IEC 62443-4-1 Security for industrial automation and control systems Part 4-1: Secure product development requirements and to the international standard of IEC 62443-4-2, Security for industrial automation and control systems Part 4-2: Technical security requirements for IACS components. This certification program offers four certification levels for a device. The increasing levels of device security assurance are from Level 1 to Level 4.

There are three aspects of assessments in this program as follows.

- Security development assessment
- Functional security assessment
- Robustness testing on the device

The robustness testing consists of two kinds of testing: 1) scanning the presence of known vulnerabilities and 2) examining the capability of the device to adequately maintain essential functions while being subjected to normal and erroneous network protocol traffic at normal to extremely high traffic rates (flood conditions). The main focus is to check for known vulnerabilities in the software installed on the device and its robustness for network attacks, and the requirements do not include aspects of countermeasure functions such as factory settings and configuration rights.

3.3.8 Security Maturity Model

The security maturity model is the mean of describing the organizational capability on security. The idea of the maturity model was investigated as a reference for a method of checking process quality in IoT vendors. There are lots of security maturity models of various kinds, but the following two of them are close to the IoT industry.

3.3.8.1 IIC IoT Security Maturity Model

The IoT Security Maturity Model (IoT SMM) is released in 2018 from Industrial Internet Consortium (IIC) to support sharing the common understanding of security requirements and the goal of maturity level on providing IoT services among the service partners [80]. The objective of IIC is to present a new model of IoT SMM, one model that is suitable for all, regardless of industry (Home, Office, Plant, for individuals and implementers, etc.). And this model helps the executive level balance business and security when they are asked to explain not only the profitability of the service but also whether the IoT implementation is secure.

The maturity is measured in three dimensions and two levels.

Three Dimensions:

- 1) Governance; Strategy, management, and execution (threat models, risk analysis, and assessment)
- 2) Enablement: Security measures (identity/connection management, data protection, asset management, physical security)
- 3) Hardening: Vulnerability and patch management, incident response, audits, etc.

Each dimension consists of three domains and six practices, and each dimension is evaluated from two perspectives.

Two Perspectives:

- 1) Comprehensiveness: the degree of depth and consistency of security measures applied
- 2) Scope: the degree of fit to the industry or system needs

This model provides an external account of the security readiness of the services provided by the organization that is the IoT service operator. While the focus is on service operations and does not indicate the security quality of the IoT services themselves, it does describe initiatives that may be helpful to IoT vendors.

3.3.8.2 BSIMM

Building Security in Maturity Model (BSIMM) is a software security framework to support understanding of the position (maturity level) of its enterprise objectively about the security efforts measured in four domains and 121 activities grouped into 12 practice areas by comparing with other program participants (128 members in 2021) [81]. It is not a pass/fails assessment. BSIMM was initiated by Gary McGraw, Ph.D., Brian Chess,

Ph.D., and Sammy Migue in 2008 with BSIMM1, and the current version is BSIMM12 in 2021. Knowing the position in the industry enables a company to assess the current state of their software security controls, identify shortfalls, prioritize changes, and determine where and how to allocate resources to achieve immediate improvements.

BSIMM consists of four domains with twelve practices. Each domain has three practices. The structure of the domains and practices in BSIMM is as follows.

- 1) Governance domain: the core of software security activities that covers the practices of 1. Strategy & Metrics, 2. Compliance & Policy, and 3. Training.
- 2) Intelligence domain: a collection of organizational knowledge that drives software security activities across the organization that covers the practices of 4. Attack Models, 5. Security Features & Design, and 6. Standards & Requirements.
- 3) Secure Software Development Lifecycle (SSDL) Touchpoints: evaluation and analysis in software development, including security measures that cover the practices of 7. Architecture Analysis, 8. Code Review, and 9. Security Testing.
- 4) Deployment: Activities that directly affect Software Security, such as software configuration, maintenance, and environment-related to network security and software maintenance departments that cover the practices of 10. Penetration Testing, 11. Software Environment, and 12. Configuration Management & Vulnerability Management.

The BSIMM is a self-assessment of the level of security management in companies that develop, operate, and maintain their own corporate systems, and an understanding of the level of maturity by comparing them to other companies, which is difficult for IoT vendors to refer to directly. However, BSIMM has a subset of its kind called “vBSIMM (vendor BSIMM).” The vBSIMM focuses especially on vendors to minimize the scope of measurements in two domains such as SSDL touchpoints and Deployment with seven practices.

These models are good examples to assess the corporate level of security capability. Some practices are good to refer to, but both models are not for the security capability of IoT devices themselves. Table 3.4 compares the two Maturity Models. BSIMM is an evaluation method to assess the maturity of security support in the corporate's information system by comparing it with other companies using certain indicators, while IoT SMM is an evaluation method to clarify the security maturity of the business service system operated by the company. On the other hand, IoT SMM differs in that it is an evaluation

method for clarifying the maturity level of security for business service systems operated by the company.

Table 3.4 Comparison of Security Maturity Models

IIC IoT SMM		BSIMM
Understand the security requirements of your own business (enhance existing security frameworks)	Objective	Objective evaluation of one's own position by comparing one's own security maturity level with that of others.
Main target: Business operation systems		Main target: Corporate systems
Goal setting from a management perspective and understanding of the current situation by the security team, comparison of the two, and plans to achieve them	Characteristics	Assessment of the current status of security measures for the company's operational systems, identification of shortcomings based on comparisons with other companies, and resource allocation planning to achieve improvements
Formulated by service and system stakeholders		Self-assessment
Governance: Strategy, management and execution (threat model, risk analysis and assessment)	Evaluation Perspective	Governance: strategy and indicators, compliance policy, training
Enablement: Security measures (ID/connection management, data protection, asset management, physical security)		Intelligence: attack models, security functions and design, standards and requirements
Hardening: vulnerability and patch management, incident response, auditing, etc.		SSDL Touch Pt: Architecture analysis, code review, security assessment
		Deployment: penetration testing, SW environment, configuration management, vulnerability management
Relationship with BSIMM is unknown		Historical activities since 2006
Led by Ron Zahavi (Microsoft)	Others	Software Security led by author Gary McGraw

3.3.8.3 ISO 21827

ISO 21827:2008 [82] is called SSE-CMM (registered); Systems security engineering – Capability maturity model. ISO21827 is related to ISO 15504-2: 2003, Information technology - Process assessment - Part 2: Performing an assessment and maintained by the International Systems Security Engineering Association (ISSEA). SSE-CMM is a process reference model that focuses on the requirements of the security implementation

of an information system (or its related systems) and a mechanism to improve security engineering work for the quality requirements. SSE-CMM is also a methodology that aims to reduce costs and improve the quality of high availability and secure systems, reliable products, and security engineering services.

There are four aspects of the quality standard required for the development and operation of secure systems and trusted products.

- 1) Continuity: knowledge based on experience
- 2) Repeatability: how to repeat the experience of success
- 3) Efficiency: How developers and evaluators can work more efficiently
- 4) Assurance: a degree of confidence

SSE-CMM defines the base practices as 129 practices in a total of 22 areas. And the generic practices specified in ISO/IEC 15504-2 that indicate higher levels of process capability are located at the top of the capability dimension. The lowest common feature is the base practices. The base practices are simply checked whether an organization performs all the base practices in a process area. The level of capability is evaluated in five levels:

- Capability Level 1 - Performed Informally
- Capability Level 2 - Planned and Tracked
- Capability Level 3 - Well Defined
- Capability Level 4 - Quantitatively Controlled
- Capability Level 5 - Continuously Improving

While this level of indicator is very straightforward to see the status of the initiative, the author sees that the final step in confirming the status of the IoT device's security response is to check the evidence of whether the initiative has been taken place or not.

3.3.9 Applicability of existing methods to IoT devices

The CC assesses the appropriateness of a product's security design and its implementation. It is out of scope neither the product strength of security protection capability nor the security operation capability of the product vendors. For IoT users, the existence of a security maintenance program in the use of IoT devices is an important perspective. This part is lacking in the CC evaluation.

The Smart Communication Alliance is releasing a protection profile of secure elements for IoT [83] in 2019 for CC as the German Standard of BSI-CC-PP-0109-2020. However, the TOE is limited to the secure elements that perform the storage part of the cryptographic key, the function to access the cryptographic key, and the random number generation function, which are necessary for modules and applications to perform secure communication. Protection against physical destruction is also an evaluation target, but still, the scope is limited to the secure element.

Greater confidence in the validity and certainty of the security function can be obtained by inspection of a wider range of more rigorous evidentiary material. However, problem evaluation methodology and evaluation process is a time-consuming process, so it eventually makes the process a costly one. Assessing that the assurance requirements of the more rigorous assurance components (e.g., full quasi-formal functional specifications with additional formal specifications) are met for all assurance families of all assurance classes would require a corresponding cost and time frame. Because of this costly and time-consuming certification, there are not many cases of vendors including IoT vendors voluntarily obtaining CC certification, except when certification is mandatory as a procurement requirement. Many vendors use the ISO/IEC 17050 Supplier Declaration of Conformity for self-certification, unless third-party certification is required.

To obtain the EAL2 level, the application fee is about US\$7,000, but an additional evaluation fee is required; according to the IPA, the evaluation period takes at least four to six months on average. The cost for a security expert is much higher than the cost for a regular software engineer. That is likely around US\$30,000 to US\$50,000. So if one security expert is assigned to the evaluation for six months, that alone will cost at least \$180,000 to \$300,000. For consumer products evaluation, this high cost is not likely to incur just for security unless there is a customer requirement.

On the other hand, EDSA certification under IEC 62443 also requires third-party assessment because it was originally intended for embedded devices for critical infrastructure and objectivity is important. Therefore, like CC, it is time-consuming and costly and is not suitable for general IoT devices. In addition, the evaluation perspective is limited to the design artifacts of communication robustness, security design assessment in software development, and functional security assessment. From the cost point of view, EDSA certification requires about \$30,000 for applying the Communication Robustness Test assurance and about \$50,000 for the Functional Security assurance. In addition to

this, a third-party evaluation is necessary to check the status of functional implementation from the design stage. As with the CC certification, the resulting cost is going to be about \$300,000 per product.

The IoT security certification program offered by the Connected Consumer Device Security council (CCDS) allows for a single-party certification (self-certification) that requires a minimum expenditure of about \$2,000 for registration management fee and 2-3 months of in-house evaluation time. As compared to the CC and the EDSA, this certification program is more IoT vendor-friendly from the cost point of view.

Consumer IoT devices are generally produced in large numbers, so they may absorb the cost, but the two barriers of time and cost are not suitable for the IoT field where time-to-market is crucial. It may be appropriate for highly critical IoT devices. But if general consumer IoT devices want to increase their security level, they need a different method than the CC and EDSA certification schemes.

The three maturity models already introduced, BSIMM, IoT SMM, and SSE-CMM are evaluation systems for building and operating secure systems and are evaluation systems from the operator's perspective. Therefore, the evaluation items do not fit IoT vendors who develop and provide secure products. However, the basic process of threat analysis, risk assessment, and clarification of security requirements will be helpful for IoT vendors to develop their development process.

3.3.10 Security Guidelines

There are a lot of kinds of security guidelines worldwide. Some of them are not specifically for IoT but are useful for IoT. In this study, the documents in a total of thirty-seven were examined; twenty-four were from the US, three from the EU, five from Japan, and five of international standards, as listed below to find candidate items for metrics effective in describing security quality. The results of the comparison of requirements are shown in Appendix 1.

From the US:

- NIST, Cybersecurity Framework v1.1 [45]
- NIST, SP800-64 v2 Security Consideration in System Development Life Cycle [84]
- NIST, SP800-183 Network of Things [85]
- NIST, SP800-193 Platform Firmware Resiliency Guidelines [86]

- NIST, Cybersecurity White paper IoT Trust Concern [87]
- NIST, SP800-160 System Security Engineering [88]
- Online Trust Alliance, IoT Security & Privacy Trust Framework v2.5 [89]
- US Department of Homeland Security (DHS), Strategic Principles for Securing IoT [90]
- Federal Trade Commission (FTC), Internet of Things Privacy & Security in a Connected World [91]
- FDA, Content of Premarket Submissions for Management of Cybersecurity in Medical Devices [92]
- FDA, Postmarket Management of Cybersecurity in Medical Devices [93]
- The Internet Engineering Task Force (IETF), Best Current Practices for Securing IoT devices [94]
- IIC, IIoT Security Framework (Securing the Internet of Things) [95]
- IIC, IoT Security Maturity Model [80]
- BSIMM [81]
- vBSIMM [96]
- UL (Universal Asynchronous Receiver/Transmitter) 2900 [97]
- R.J. Anderson, Security Engineering [98]
- Hewlett Packard Inc., 9 ways to improve IoT device security [99]
- Information System Audit and Control Association (ISACA), Managing the Risk of IoT, INTERNET OF THINGS: RISK AND VALUE CONSIDERATIONS [100]
- BITAG (Broadband Internet Technical Advisory Group), IoT Security and Privacy Recommendations [101]
- CSA, Future-proofing the Connected World: 13 steps to develop secure IoT Products [102]
- Open Web Application Security Project (OWASP), IoT Security Guidance – Manufacturer [103]
- GSMA, IoT Security Guidelines for Endpoint Ecosystem [47]

From the EU:

- UK, Code of Practices for consumer IoT Security [104]
- European Telecommunication Standards Institute (ETSI), TS 103 645 [105]
- ENISA, Baseline Security Recommendation for IoT [31]

From Japan:

- NISC, General Framework for Secure IoT Systems [106]
- IoT Acceleration Consortium, IoT Security Guideline v1.0 [14]
- IPA, Guide to develop IoT Devices Safe and Secure (High-Reliability Edition) [107]
- IPA, Guide to secure the Quality of IoT Devices and Systems [108]
- CCDS, Certification Program General Requirements 2021 [109]

From International standard:

- ISO/IEC/IEEE 15288, Systems and software engineering - System life cycle processes [110]
- ISO 21827, System Security Engineering - Capability Maturity Model [82]
- IEC 62443, ISASecure EDSA Certification [33]
- International Telecommunication Union Telecommunication Standardization Sector (ITU-T), Y.4806: Security capabilities supporting safety of the Internet of things [111]
- oneM2M, TR-0008-v2.0 Security [112]

3.3.11 Summary of Literature Review

As described in Step 2 in Fig. 3.1, a SLR is conducted to identify other researchers with similar research interests. However, the author could not find studies or standards defining the security quality metrics for IoT devices. The International Standard for Software Quality (SQuaRE, ISO/IEC 25000 series) places “security” (one of the sub-categories of functionality) as a quality category for system software. SQuaRE listed “security” as a major non-functional requirement in terms of system safety. There is a rationale for treating security as a quality. However, these standards only highlight ideas at the conceptual level together with examples to be considered. Although some ideas and

items can be used as references, none of the security quality control items are elaborated. In the security evaluation based on GQM, Abdulrazig et al. [113] discussed the misuse of Web applications. However, this should not be misconstrued as a discussion on the security of IoT devices. Further, Yahya et al. [114] discussed the security assessment of cloud storage. Thus, it is worthwhile to define IoT device security quality metrics based on GQM that IoT vendors could use.

There was a lot of discussion on how to measure and indicate quality, but in the end, it became clear that the only basic principle is for manufacturers to consider and implement the necessary measures to ensure user safety ahead of time and that the content of these measures varies depending on the industrial field and usage environment of the product and cannot be determined in general. It was also clarified that quality can be ensured by two types of quality: process quality, which defines the processes to be implemented to maintain a certain level of quality and evaluates the sufficiency of the implementation status, and product quality, which evaluates whether the deliverables of each process are made according to the design. Therefore, it is necessary for quality metrics methods to be structured in such a way that they can be evaluated from both aspects.

In the literature related to laws, regulations, and guidelines that show requirements for IoT security, initially, most of the literature showed requirements for security countermeasure functions and many examples of how to achieve them, but gradually many of them also show requirements for logical procedures and processes that should be performed to design and develop secure products. However, gradually more and more requirements are indicating logical procedures and processes that should be followed to design and develop secure products. Ultimately, it is important for a product to be secure, but the importance of confirming the company's attitude toward product design, such as how the security function of the product was designed, how it was evaluated, and what kind of support is provided, is considered to have begun to be recognized. Existing security certifications, such as CC and EDSA, are biased towards technical evaluations of security design and implementation status and are in the form of third-party certifications. While this approach is acceptable for evaluating IoT devices installed in mission-critical critical infrastructure systems, it is not appropriate for the scope of consumer-oriented IoT devices. The first step is to check the very basics, such as default settings of ID and password for remote access and the availability of update functions, which are prominent security issues in IoT devices. The author believes that a rigorous

evaluation of security should be added when the use case of the IoT device requires advanced security measures.

Thus, the potential security-quality metrics for IoT devices were selected from the literature for each phase of the previously studied product lifecycles. Quality-control practices were then defined to reflect the opinions of security and quality experts on the parameters that should be considered from the perspective of IoT device users.

4 ITEMIZING IOT DEVICE SECURITY QUALITY METRICS

The formulation of the proposed evaluation items based on required initiatives or the recommendations of many documents is discussed in this section.

4.1 Definition of IoT Device Security Quality

The literature survey found no specific work on IoT quality from the perspective of security. Therefore, before the IoT security quality metrics in Step 3 in Fig. 3.1 are discussed, defining the IoT device security quality is necessary. Because the IoT system consists of electronic devices, it is composed of a hardware device consisting of electronic circuits, sensors, and occasionally actuators, as well as software that controls the functions of the electronic device. Consequently, the capability of every product to verify the quality cannot be comprehensively evaluated. Therefore, it is common practice to guarantee the quality of all products by ensuring all of the pre-defined development and production processes conform to the required standards; thus, an assessment of the capability of samples alone is sufficient. Essentially, the collective quality should comprise both process and product quality. Thus, the quality of security of an IoT device may be defined as a combination of the quality of the product development process and that of the security capability of the product.

To outline the security development process, items indicating how to design, build, and support the product must be identified based on the product lifecycle. These include the results of the process review and the maintenance program. Further, to outline the cybersecurity performance of the product, the results of the security assessment must be

listed. To demonstrate the IoT cybersecurity performance, these items must reflect the static and/or dynamic security testing of IoT devices.

4.2 Requirements of IoT Device Security Quality

Before defining the aforementioned items, clarifying the goals and aspects to screen is necessary. First, the items must transparently describe the development process in security (e.g., the security policy of an IoT vendor and the organization's standardized security development process).

To accurately describe the product quality, items properly describing the cybersecurity capability are also required. The results of the product security evaluation must be listed. More importantly, the items must include those responding to market demands as well as those complying with international standards and guidelines. A crucial source of consumer feedback is aftersales support. The security support program must partly comprise product cybersecurity quality. Activities, such as security monitoring, receiving vulnerability feedback, and issuing updates, must be listed as items. Furthermore, the items must be easily comprehensible from the consumer's perspective; this is important to gain the trust of users. The requisites of IoT device security quality are summarized in Table 4.1.

Table 4.1 Requirements of IoT Device Security Quality

Requirements	Aspect
R1: Describing the development process transparently	1: Security policy of an IoT vendor
	2: Quality of Security Development Process
R2: Describing the security capability properly	Quality of Product security Capability
R3: Responding to the market needs and/or requirements	1: Covering the requirements by law or regulation
	2: Following the recommendations of international standards and guidelines
R4: Security support program (post-market)	Security monitoring, receiving the vulnerability input, update, etc.
R5: Any items gaining the user trust	

4.3 Transparency Model of IoT Device Security Quality

To consistently deliver products with a certain level of quality, vendors define and iteratively execute processes throughout the product lifecycle. In contrast, the proactive players in the product lifecycle can change in each phase. For example, in the development phase, the design department mainly initiates the development work. When the development progresses to a certain extent, the quality assurance department evaluates the implementation status. Once the implementation is confirmed, the manufacturing department takes over and starts manufacturing. Thus, to produce a product, many departments of a vendor share the responsibility at each phase from the design to the support after-sale in the whole product lifecycle. Therefore, to provide a secure product, it is necessary to clarify the security efforts in each phase so that the responsible department can understand the security efforts to implement. The author considered this as such.

To comprehensively identify items of IoT device security quality, the author defined a transparency model of IoT device security quality that describes the nature of items as presented in Fig. 4.1—before Step 3—by integrating the definition of IoT device security quality and its requirements. This definition of IoT device security quality would satisfy the requirement R1, which ensures transparency of the entire product development process.

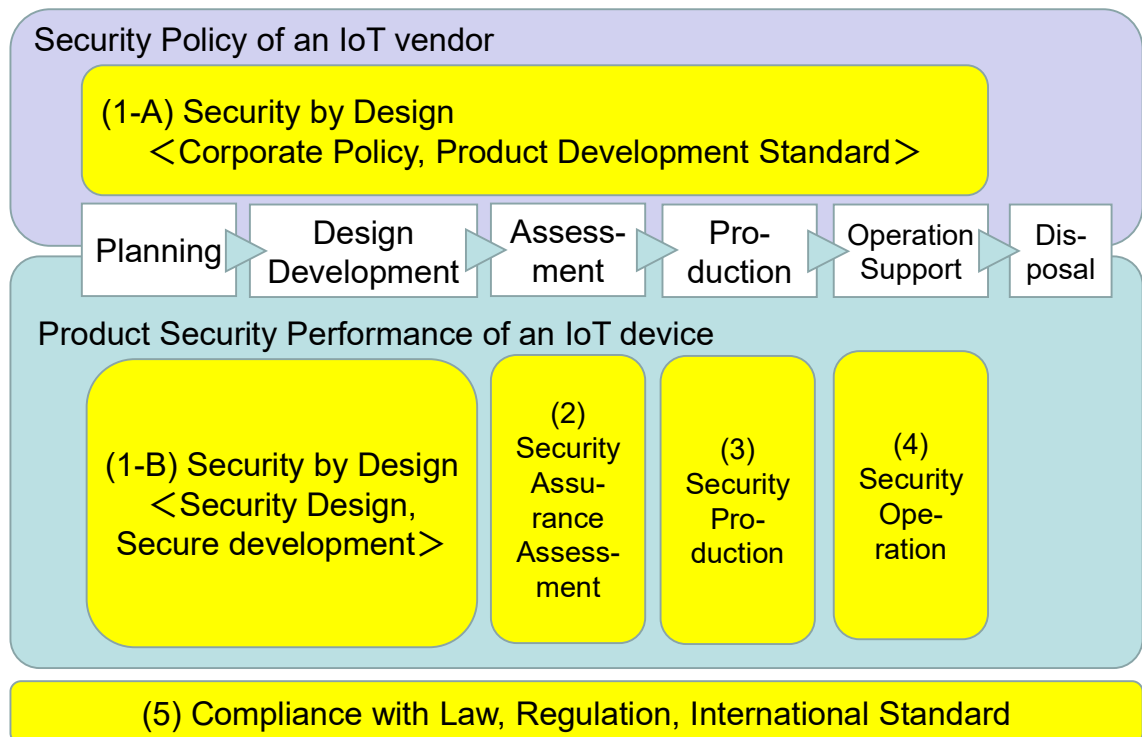


Figure 4.1: Transparency Model of IoT Device Security Quality

This model provides a framework for the IoT device security quality metrics. The model is derived by mapping the security development lifecycle, which was released by many organizations such as NIST [115], Microsoft [116], Synopsys [117], and PwC [118], onto the V-shaped product development process that many IoT vendors follow. Nevertheless, by clarifying the relationship between the V-shaped product development process and the security development lifecycle, each of the members involved in IoT device development will know which security quality metrics they should be responsible for. The “transparent” model for IoT device security quality is structured as follows.

- 1) The “Security by Design” area comprises two parts, namely the process quality of performance and capability by an IoT vendor and corresponding product quality of an IoT device [119]. The Security by Design area under Area 1 is subdivided into two main areas. Especially in Area 1-A, the involvement of business managers is important as the level of commitment to producing secure IoT devices as a corporate policy. Area 1-B is the area where the security aspects of the IoT device specifications are determined and implemented. Those in charge of product business planning and those in charge of determining basic specifications are mainly responsible for this area.
- 2) The “Security Assurance Assessment” area involves the evaluation results. Those in charge of product development and those in charge of quality assurance are responsible for this area.
- 3) The “Security Production” phase entails the items of security management during production. Those in charge of manufacturing the product are responsible for this area.
- 4) The “Security Operation” phase encompasses aftersales security monitoring and response to incidents. Those in charge of customer support, maintenance and PSIRT (product security incident response team) are responsible for this area.
- 5) The “Compliance with Law, Regulation, International standard” area implies that the public or industry requirements have been fulfilled. Compliance with industry standards and regulations is relevant to all areas. All members, not just the product manager, are responsible for this area.

When considering IoT device security quality metric items, this novel model not only allows each metric to be assigned to the appropriate area of responsibility but also makes it easier to determine the areas efficiently to implement in the future as new requirements emerge.

Based on this model, perspectives that should be regarded as the state of IoT security—frequently alluded to in the literature survey—are listed. Security initiatives are necessary throughout the product lifecycle. And those initiatives are not able to carry by a few departments; it would be nice if IoT devices were security-perfect, but achieving sufficient security is not easily achieved. There is the case of Kaspersky [73], which lost the trust of its users due to its opaque approach to security and worked to increase transparency to regain that trust.

There are some things not preferably to expose by increasing transparency. However, losing the users' trust and not selling products is not the end of the world. To prepare for transparent explanations, it is necessary to set metrics so that the efforts in each area can be understood and to keep a trail of evaluation results. Regardless of whether or not to disclose the information, it is necessary to leave a trace of evidence of the adequacy of security measures and the results of security assessments in a form to explain in case a problem occurs later.

4.4 Proposal Development of IoT Device Security Quality Metrics (Step 3)

Based on the transparency model (Fig. 4.1), the items to be the IoT device security quality metrics were selected from the literature relating to IoT security. And a proposal was subsequently drafted (Step 3 in the research method) by compiling those items. The key point is that security quality metrics are not simply a checklist of security measures that are considered necessary; instead, they are items that clarify the quality goals behind the quality metrics and why they must be checked.

4.4.1 Extraction of candidate items from literature Surveyed

The items of candidates were selected from the literature surveyed in section 3 said above, and especially from the IoT Security Guideline documents in section 3.3.8. The author selected items that fit into each area of the transparency model and that were implementable by IoT device vendors as listed in many of the documents.

Across the literature surveyed, several characteristics below were observed. And the result of a comparative study of the requirements listed in the literature is Appendix 1. “Threat Analysis and Risk Assessments” are the items most of the documents (more than 22 out of 37) recommend.

In addition, many documents recommend the following items:

- Mitigation of risk (11 docs)
- Handling of Personal Information (10 docs)
- Security Assessments (Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST)), Security Patch assurance (14 docs)
- Closing unnecessary port or proper authentication (12 docs)
- Security Operations such as Security Operation Center (SOC)/PSIRT, Vulnerability information reception (14 docs)
- Security countermeasures: Update (15 docs), Encryption (19 docs), Access authentication (18 docs)

The following items, though less recommended, are considered important to show the security readiness based on the experience.

- Accepted threat list and workaround (2 docs)
- Clarify the outsourced components (8 docs)
- Personal information handling (8 docs)
- Law/regulation compliance (4 docs)
- Security maintenance period and disclaimer (2 docs)

Based on this research, the author developed a set of candidate items for describing the IoT device security quality. Because the functionality and security measures are controlled by software, perspectives of the software quality were referenced [115], [116], [117], [118].

4.4.2 GQM Method

The GQM paradigm [120] is a three-tier measurement framework and modeling method in software engineering in which the first, second, and third tiers represent the goal, question, and metric, respectively.

Metrics are constructed by referencing the GQM method in terms of what to achieve (goal), what to evaluate to achieve the goal (question), and what to employ as an evaluation method (metric). By defining the goals to achieve, all parties involved in product development can view the set goal. Then, by measuring the degree attained to reach the goal, the alignment of the product with the original aim is confirmed.

Metrics are the methods and scales of measurement of targets.

- Method: mapping of attributes (measurable features) to values or categories on a scale
- Scale: a set of values or categories
- Target: Product, process, resource (raw material, material)

Clarification of the object to be measured is the priority because it affects the measurement method. The advantages of having metrics will be as follows.

- As this method is prevalent in the quality community, it is easy to gain the understanding of the quality department.
- To prevent the quality standard from being influenced by the individual designer's way of thinking
- If left to individuals, unevenness and oversights will occur and quality will not be stable.
- Sharing the same quality goals and rationale helps all members involved in product development to have a common understanding of the risks that need to be addressed.

An example of a typical GQM configuration for a software product is described below. Assuming that the goal is to eliminate defects, two questions can be set up: one is how many defects are detected? The other question is: What are the causes of defects? The next step is to consider how to evaluate each question. Question 1 can be evaluated using two indicators: the number of defects and the impact of those defects. Question 2 is to list the causes of defects. This is how the GQM can be set up. Translating this into a security problem, it would be as follows in concrete terms. The goal is to eliminate known vulnerabilities. To achieve this goal, two questions should be posed: one is how many known vulnerabilities are detected? The second question is what are the causes of known vulnerabilities? For question 1, the number of known vulnerabilities detected and their impact (severity) can be evaluated as in the previous example. For question 2, the cause of the detected vulnerabilities can be listed. In this way, various metrics for security quality can be set up using the GQM method.

Based on the perspective that procurers or users want to know the product quality, formulate a question to understand the type of security measures that must be

implemented from their perspective. If the question involves several elements, create a sub-question to make it more specific.

4.4.3 Setting Goals for Each Area

Based on the IoT device security quality requirements discussed in Section 4.2, the goals for each area of the transparency model are listed in Table 4.2. The author has set high-level goals for each area/phase. Furthermore, product-specific indicators are excluded from the goals because these can vary according to each product use case and industry.

In setting the goal, the goals must be agreeable to all stakeholders involved in the development, quality assurance, production, sales, and support departments related to the IoT devices to be developed, including the business manager. The ultimate goal is to make sure that the IoT devices provided to customers will be safe for users, and the goals should be clearly defined for this purpose.

Table 4.2 Goals for Each Area of Transparency Model

Area	Goals
1-A. Security by Design (Corporate Policy & Development Process Standard)	G1A-1: To provide secure products which gain the trust of customers
	G1A-2: To define the corporate standard of secure development processes so that all products provided can be manufactured with security throughout the product life cycle
1-B. Security by Design (Security measures, Secure Development)	G1B: To develop secure products based on the defined development standard from the planning stage of the product life cycle
2. Security Assurance Assessment	G2: To evaluate and confirm that secure products are developed as designed
3. Security Production	G3-1: To carry out production with a secure production operating system to avoid containing security risks
	G3-2: To secure the supply continuity
4. Security Operation	G4: To take prompt actions to minimize the damage to customers, when a security risk becomes apparent in the provided product
5. Compliance with Law, Regulation, and International Standard	G5: To provide products complying with laws, regulations, and international standards of the destination market

The author suggests setting goals with the following perspectives in mind.

- Reducing the level of risk for users of the service/product

- Increasing the transparency within the market
- Increasing awareness within the market
- Reducing the level of uncertainty by the implementer
- Establishing a baseline level of security per product /service /process /organization type

The goal of 1-A is to establish a basic policy for providing a secure product that would earn the trust of consumers and define a basic process for implementing the policy. This allows users to trust in management's commitment to developing secure products. G1A-1 corresponds to the first aspect of R1 and R5 of Table 4.1. G1A-2 corresponds to the second aspect of R1. The goal of 1-B, G1B, is to develop a product that considers security throughout the lifecycle of the product following the corporate policy and process in 1-A.

The goal of Area 2, G2, is to ensure that the product developed in Area 1-B is secure as designed. The goal is to provide IoT devices to users as secure products by confirming the security countermeasure functions to meet the security goals set at the specification review stage and no fatal vulnerabilities inherent in the devices.

Area 3 is a perspective specific to the IoT and is absent from general software development. Because IoT products consist of both software and hardware, they are assembly-processed similar to software products. The production process entails actions, such as physical assembly, serial number labeling, and the setting of device-specific IDs and passwords for security. In certain cases, the hardware components required for production may be externally procured and manually assembled. Thus, during production, after verifying the product security, supplementary actions are implemented to finalize the product before it is shipped to the market. Security risks are involved in this process, and the goal is to eliminate or reduce those risks in this area. Goals G1B, G2, G3-1, and G3-2 correspond to the requirement of R2.

Area 4 is the area of providing a unique security response that is different from traditional quality assurance. Traditionally, quality assurance operates such that if a product performs to a certain standard, it is shipped. However, unless a product that does not meet the standard is found in the marketplace (i.e., unless the personnel is notified of a problem by users), the quality assurance personnel do not check and monitor the status of the products in the market themselves. On the other hand, in the world of security, even with the best efforts to develop a secure product, the level of security perceived to be

secure is changing every day as attack techniques constantly evolve. Security risks will gradually increase from the time the product is shipped. It is, therefore, necessary to monitor changes in the circumstances surrounding the product even after it is shipped. Accordingly, the goal, G4, is to have a response system in place to check and correct any product-related security issues discovered and be ready to respond at any time. G4 corresponds to the requirement of R4. In the traditional approach, if a quality issue occurs after shipment, the cause of the problem may be identified and addressed. In contemporary scenarios, however, a security problem is different from traditional quality assurance because these problems are manifested by a malicious attack and must be dealt with via non-conventional means.

The goal of Area 5, G5, is to comply with the IoT security laws and regulations with which increasing numbers of countries and regions have been demanding conformity in recent years. In some cases, product sector-specific guidelines are provided in some markets and required as industry standards. Although this objective must naturally be considered at the design stage, its content is subdivided into different areas. This is because security-related laws and regulations have recently come into force, and the requirements are related to the entire product lifecycle. Significant regional differences also exist. Goal G5 corresponds to the requirement of R3-1 and R3-2.

4.4.4 Setting Sample Questions and Metrics for Each Goals (Step 3 – 4)

Based on the GQM method mentioned above, the questions and metrics were formulated for each area from the perspectives clarified in the previous research to answer the following questions. “What do you want to know about IoT device security quality?” and “What do you require to be sure?”

From the standpoint of the IoT consumer, the question is to clarify what security measures are being taken and how secure the supplied products are. On the other hand. From the standpoint of IoT vendors, it is necessary to clarify what needs to be done and when in the development process.

The metrics were devised considering the following.

- a) Do the metrics make sense to IoT vendors?
- b) What are the criteria for the metrics?
- c) Will they interfere with the existing development process?

For a), clarifying the reason for performing metrics make it easy to understand. When setting metrics, clarifying the reason for measuring the metrics will increase the conviction of the development engineers when measuring them. For b), the metrics are formulated based on “what and when,” whereas for c), the metrics are clear and can be incorporated into existing design processes.

First, the primary questions were listed. The secondary questions were then added to set up a more specific perspective and provide supplementary confirmation. The metrics at this stage are set as simple assessments, such as the presence or absence of documented evidence and whether assessments are performed. The reason for employing a simple evaluation is that a clear basis or objective indicator for classifying the content of each response does not exist. When an organization is sufficiently mature to implement advanced initiatives, these questions and metric sets can evolve into an advanced form of evaluation. This involves establishing complex questions and metrics with approximately three to five levels, such as well done, partially accomplished, and nothing done, or similar to the SSE–CMM approach.

The results of this study are based on the elimination of field-specific product perspectives as much as possible. As such, these results should be considered an example of questions and metrics for IoT in general. This is because there is no one-size-fits-all definition of security quality metrics common to all IoT vendors. If there is a field-specific item necessary to assess, it can be modified to be field-specific by adding such field-specific questions and metrics. Tailoring of questions and metrics is necessary because there are different risks, business practices, and requirements based on the prerequisites of the environment in which IoT devices operate. This study proposes a method for deriving metrics, and the proposed metrics here are items that are generally considered necessary.

Quality and security experts then review and evaluate the validity of the draft questions and metrics in Step 4 of the research method to refine the list of questions and metrics. The reviewed draft questions and metrics are listed in Appendix 2. The process of setting the IoT device security quality metrics and the results of the examination of questions and metrics for each area are described hereafter.

4.4.4.1 Area 1: Security by Design

To satisfy the goals of Area 1, the author considers what and how to clarify. Area 1 covers the product lifecycle from the policy level to the product support after-sales. To achieve the goal of Area 1-A in Table 4.2, the questions for Area 1-A as shown in Table

4.3 were set as basics to assess whether the IoT vendors consider security quality and support important [46], [106]. The reason for this question is that whether or not there is a commitment to security quality at the management level of a company or business unit is a major factor for users in determining the safety of a product.

Table 4.3 Question and Metrics for Area 1-A

Question	Sub-question	Metrics
Q1A-1: Does the company recognize the importance of handling product security?	Q1A-11: Does the company have a product-security policy?	M1A-11: It is documented. = 1 There is no policy defined. = 0
	Q1A-12: Is the product-security-development process defined?	M1A-12: It is documented. = 1 There is no process defined. = 0

Then, the author formulates two secondary questions to render the question more specific. The first, Q1A-11, inquires whether a policy stating that the management's commitment to security response is considered important is in place. Because security responses require monetary investments, many guidelines recommend that such responses must be publicly stated as a management policy. The other question, Q1A-12, sought to confirm whether a secure development process was defined, and the environment was ready for all products to be secured using the same process in contrast to the ill-conceived security response. Then, the metrics are simply set to confirm the presence of documents for those aspects. Moreover, this area may include checking the handling policy of personal information in the case of IoT devices that deal with personal information.

Neither the quality experts nor security experts raised any specific objections to these two questions and metrics. The quality experts stated that the same was true for clarifying the product security response because it was important for the management to present the policy as an enterprise-wide effort that promotes product safety response. Thus, the questions and metrics for Area 1-A are listed in Table 4.3.

In Area 1-B, the questions and sub-questions were formulated to check whether the fundamental actions to perform in the security development process were included [47], [101], [121]. The questions and metrics are formulated to identify the security response items that must be implemented at the appropriate time. Concerning these items, what to

do, when to do it, and under what conditions must be clear. The questions and metrics for Area 1-B are listed in Table 4.4.

The formulated questions include the threats that the IoT device will confront, the risks that may arise from those threats, and whether security countermeasures are properly selected to safeguard against these threats. For example, even if an engineer implements a security measure designed without threat analysis, there will be rework that will eventually require threat analysis to justify the need and priority of the measure in the end.

In the planning stage of IoT devices, determining the level of security measures by assuming the threats that may confront the IoT devices and the user risks at the stage of assuming the use cases is necessary. This is confirmed by Q1B-11, Q1B-12, and Q1B-13. Appendix 1 clearly shows that threat analysis and risk assessment are required in many documents; hence, these items must be mandatory.

Table 4.4 Question and Metrics for Area 1-B

Question	sub-question	Metrics
Q1B-1: Is security considered from the planning/design stage?	Q1B-11: Is threat analysis performed?	M1B-11: There is an analysis result. = 1 It is not performed, or no result. = 0
	Q1B-12: Is risk assessment based on threat analysis performed?	M1B-12: There is an assessment result. = 1 It is not performed, or no result. = 0
	Q1B-13: Are threats selected for countermeasures based on risk assessment and risk mitigation countermeasure design implemented?	M1B-13-1: There is a list of threats to be protected. = 1 There is no list of threats to be treated. = 0
		M1B-13-2: There is a security countermeasure design document. = 1 There is no countermeasure design. = 0
	Q1B-14: Is the threat excluded from countermeasures clear?	M1B-14: There is a list of accepted threats. = 1 There is no list of accepted threats. = 0
	Q1B-15: Are the methods for reducing threats excluded from countermeasures and alerts described in manuals, etc.?	M1B-15: There is a document for users. = 1 There is no document. = 0
	Q1B-16: Is the handling of personal information taken into consideration?	M1B-16: There is a personal information list to handle. =1 There is no list or care. = 0

Q1B-2: Are secure development methods adopted?	Q1B-21: Are secure coding rules applied?	M1B-21: Secure coding rules are applied. = 1 There is no rule applied. = 0
Q1B-3: Are all the software components composing the product listed?	Q1B-31: Is the adopted OS clear?	M1B-31: The OS name and version are clear. = 1 It is not clear. = 0
	Q1B-32: Is the adopted open source software clear?	M1B-32: All of the open source software name and version are clear. = 1 Some or none of OSS is clear. = 0
	Q1B-33: Is the adopted outsourced software clear?	M1B-33: Vendor name, component name, version and country of origin of the outsourced software can be confirmed. = 1 It is not clear. = 0
	Q1B-34: Is the self-designed software clear?	M1B-34-1: The software name and version are confirmed. = 1 It is not clear. = 0
		M1B-34-2: Outsourcing vendor, component name and version are confirmed. = 1 It is not clear = 0
Q1B-4: Is there a security maintenance feature for the IoT device?	Q1B-41: Is there software update capability?	M1B-41: The product is capable of updating software. = 2 (automatic), = 1 (manual) There is no update capability. = 0
	Q1B-42: Is there a software configuration self-verification function? (For automatic updates)	M1B-42: There is a function. = 1 There is no function. = 0
	Q1B-43: Is there an access control feature?	M1B-43: There is a function. = 1 There is no function. = 0
	Q1B-44: Is there an encryption feature?	M1B-44: There is a function. = 1 There is no function. = 0
	Q1B-45: Is there a logging function?	M1B-45: There is a function. = 1 There is no function. = 0
	Q1B-46: Is there a deactivation function or a fallback operation function when the security maintenance service ends?	M1B-46: There is a function. = 1 There is no function. = 0
Q1B-5: Is the IoT device designed with consideration of disposal?	Q1B-51: Is there a function to delete user data for disposal?	M1B-51: There is a function. = 1 There is no function. = 0

The common IoT threats to consider should be based on the experience of security incidents. The threat by Botnet malware infection targeting the weak access authentication configuration such as Mirai is one of the threats to IoT devices. This threat is the denial-of-service (DoS) attack using Internet connection routes as attack vectors, intrusions, and malware infections using commonly used ID and password dictionary attacks. The physical attacks on JTAG or UART pins intended to debug IoT devices and on the sensors of IoT devices are other threats uniquely to IoT devices. And malware loading by exploiting software update procedures is another threat to consider because this attack vector is a great opportunity for attackers to modify IoT devices as they wish. In particular, it is necessary to analyze threats based on the premise that the management state of IoT devices installed by general users is almost unmanaged, with no firewall in the operating environment, unlike industrial IoT devices that are watched over by professional maintenance managers. Moreover, since it is the boundary between the physical environment where IoT devices are placed and cyberspace, it is necessary to be especially aware of threats that can lead to physical damage and the risk of compromising the safety of users.

Some IoT devices operate autonomously without a user interface, and some IoT devices cooperate machine-to-machine (M2M) without the user's intervention. Many of these IoT devices become invisible from the user except when they are installed, and it is difficult to visually confirm the abnormal status of the IoT device. As mentioned above, it is important to assume the risk that remote or physical attacks may cause an abnormal state. If this state is left unattended for a long time, the IoT devices may be operated with inaccurate data emitted from them, resulting in unexpected outcomes. A question comes up what kind of risk to assume is based on the use cases of the IoT device in planning. And it is up to imagine an undesirable situation from those risks.

Many types of threats for IoT devices can be assumed. Attackers may even exceed expectations. Hence, the implementation of measures against all threats is not unreasonable. Questions Q1B-14 and Q1B-15 identify the threats excluded from the countermeasures and communicate to users that certain risks exist as a precaution. In the use of IoT devices, there may be use cases where the personal information of users is entered and recorded. Clarifying the personal information that is to be handled in the planning stage of IoT devices is important because the protection of such information is legislated in some cases, as confirmed by Q1B-16.

After the security requirements to implement as countermeasures are determined in Q1B-1, Q1B-2 is to check the development methods for securing IoT devices. In this question, the selection of secure-coding rule is covered specifically as a sub-question of Q1B-21. Since the development methods taken are vary depending on the development environment, development methods other than secure-coding rules may be selected or added. As a metric, it checks whether the secure-coding rule is applied or not. In addition to this, the specific secure-coding rule should be clarified, as some product sectors may define the secure-coding rule to be adopted.

The vulnerabilities of IoT devices stem from the implemented software or firmware. At the time of development, clarifying the software components to be implemented is necessary for pre-shipment inspection and post-shipment vulnerability monitoring; Q1B-3 confirms this point of view. The use of open-source software (OSS) is also essential for the development of IoT devices. The selection of vulnerable OSS must be avoided because of supply chain risks; NIST CFW, IoT-SMM, and BSIMM add this requirement. In addition to the operating system (OS) and OSS, there are cases where artifacts from other companies, such as communication modules, drivers, and user interface functions, have been implemented; Q1B-33 checks all of these. As for component granularity, the sub-questions of Q1B-31 and Q1B-32 are set to check the OS and OSS to be selected. This is because these questions have not been formulated for in-house use but general application.

The selection of security measures should be derived from the results of threat analysis and risk assessment. The security solutions that security guidelines often recommend are various. For example, hardware security modules (HSMs) that securely store security elements with tamper resistance as a trust anchor, encryption functions that protect data during communication and storage, secure boot functions that prevent tampered software from starting, and malware detection functions. The selection decision is made based on the balance between the threats assumed from the use case of the IoT device, the need for countermeasures, and the return on investment. Therefore, individual security solutions are not mentioned here as metrics. It is recommended that the selection of countermeasures be made by referring to the protection profile for IoT [80] and guidelines for the development of secure IoT devices such as GSMA [47], HP [99], CSA [102], OWASP [103], and IPA [107].

Security measures need to include not only countermeasures against threats but also functions to respond to security problems that may occur during the use of IoT devices.

Q1B-4 asks about these security maintenance functions. The major requirements in the Appendix 1 survey were the ability to update to fix problems, encryption, and logging, so these were set as sub-questions Q1B-41, 44, and 45. In addition, weak access control settings, which have been the cause of malware infections in many IoT devices, were set as Q1B-43.

Product lifecycle has to be considered up to the disposal phase; user-specific information for IoT devices and data recorded during use is information related to the privacy of users that must be deleted. Question Q1B-5 is set for this aspect. In the past, personal information on the IoT device has been leaked to other users; Q1B-51 checks whether an information leakage countermeasure function to erase such information before disposal or reuse is implemented.

Neither the quality nor the security experts expressed any specific objection to these questions and metrics. Q1B-42 was added because security experts pointed out in the review that it is a necessary function to avoid contradiction by updating with contents inconsistent with the contents of linked services if the automatic update function does not check its status before updating. However, quality experts had certain concerns regarding the challenges in designing the software coding protocols and integrating the components included in the software into the metrics, given that this is a novel undertaking. The experts suggested that not limited to these questions and metrics, depending on the characteristics of the IoT devices to be developed, other questions and metrics may be added, referring to the requirements pointed out in the literature in Appendix 1.

4.4.4.2 Area 2: Security Assurance / Assessment

In this area, the questions and sub-questions were set to ensure that the development process was properly implemented. The questions were also formulated to determine the security level of cloud services with which the IoT products were connected [122], [123]. The questions and metrics for Area 2 are listed in Table 4.5. Similar to Area 1-A, because various evaluation methods are available, the techniques suitable to individual IoT products differ. Therefore, the inclusion of specific methods in the question list is not meaningful until a common understanding in the industry is fostered.

Table 4.5 Question and Metrics for Area 2

Question	sub-question	Metrics
Q2-1: Is the IoT device evaluated to ensure it is secure as designed?	Q2-11: Does the source code violate secure coding rules?	M2-11-1: There are assessment results that comply with the rules. = 1 There is no result. = 0
		M2-11-2: Assessment tool name and Version are confirmed. = 1 Those are not confirmed. = 0
		M2-11-3: The name of the evaluator is verified. = 1 It is not confirmed. = 0
	Q2-12: Has static analysis of the source code confirmed that there are no vulnerabilities in the source code?	M2-12-1: There are the results of the static analysis. = 1 There is no result. = 0
		M2-12-2: Assessment tool name and version can be confirmed. = 1 It cannot be confirmed. = 0
		M2-12-3: The name of the evaluator can be verified. = 1 It cannot be confirmed. = 0
	Q2-13: Has the software no known vulnerabilities?	M2-13-1: There are the evaluation results with the date. = 1 There is no result. = 0
		M2-13-2: Assessment tool name and version can be confirmed. = 1 It cannot be confirmed. = 0
		M2-13-3: The name of the evaluator can be verified. = 1 It cannot be confirmed. = 0
	Q2-14: Have the latest security patches applied on the OS/OSS been confirmed?	M2-14-1: There is a confirmation result. = 1 It is not confirmed. = 0
		M2-14-2: The version of the applied patch is confirmed. = 1 There is no confirmation. = 0
		M2-14-3: The name of the evaluator can be verified. = 1 It cannot be confirmed. = 0
	Q2-15: Has the implementation of preventive measures for HW analysis been confirmed?	M2-15: There is confirmation of the blockade of JTAG, UART, etc.. = 1 There is no confirmation. = 0

Q2-16: Are unnecessary communication ports open and is it verified that the open ports are not vulnerable?	M2-16-1: There are the evaluation results with the date. = 1 There is no result. = 0
	M2-16-2: Assessment tool name and version can be confirmed. = 1 It cannot be confirmed. = 0
	M2-16-3: The name of the evaluator can be verified. = 1 It cannot be confirmed. = 0
Q2-17: Is it verified that there are no zero-day vulnerabilities? (Has a fuzzing assessment been performed?)	M2-17-1: There are the evaluation results with the date. = 1 There is no result. = 0
	M2-17-2: Assessment tool name and version can be confirmed. = 1 It cannot be confirmed. = 0
	M2-17-3: The name of the evaluator can be verified. = 1 It cannot be confirmed. = 0
Q2-18: Have the security features and vulnerabilities of the outsourced software been evaluated? (Has the acceptance assessment been conducted?)	M2-18-1: There are the evaluation results with the date. = 1 There is no result. = 0
	M2-18-2: Assessment tool name and version can be confirmed. = 1 It cannot be confirmed. = 0
	M2-18-3: The name of the evaluator can be verified. = 1 It cannot be confirmed. = 0
Q2-19: Has the security service level of the cloud services been verified?	M2-19: There is a contract (SLA clause) in place and confirmed. = 1 There is no confirmation. = 0

The main question, Q2-1, was formulated to confirm the evaluation and verify that the implementation followed the design specifications. The sub-question, Q2-11, is a conformity check for Q1B-21. As metrics, not only the evaluation result of M2-11-1 but also the evaluation tool, M2-11-2, and its operating evaluator, M2-11-3, must be recorded to supplement the certainty of the evaluation result. In case the evaluation result there is doubted, the cause of the doubt can be traced.

Question Q2-12 checks whether the software or firmware implemented in the IoT device contains known vulnerabilities. Although this is not a security assessment specific to IoT devices, the presumption is that finding known vulnerabilities at the

implementation stage results in lower costs even if some man-hours may be consumed, considering the cost of corrective actions after shipment. Although eliminating all known vulnerabilities is difficult, those detected by the tools must be eliminated before the production phase to the extent possible. As in Q2-11, the metrics are set in the same manner to record the evaluation tool, evaluator, and evaluation results.

Q2-13 is also a check for known vulnerabilities. While Q2-12 is based on static analysis of the source code, other security assessments, such as dynamic analysis and penetration testing under the operating environment, should be used to leave a trail of the results, the tools used, and the evaluators. Problems that cannot be detected in the source code level, such as problems caused by compilation settings or response problems when connecting requests, can be evaluated.

There are many vulnerabilities found in OS and OSS, and patches to fix them are released daily. It is desirable to configure software for IoT devices with the OS and OSS having the latest patches applied whenever possible. Q2-14 checks whether the patch is applied. Unlike software products, in the development of IoT devices, it is common to decide on the version of the patch to be applied long before the final product is available. Therefore, it is difficult to apply the latest patches when the IoT device is released. However, the author considers metrics setting based on the idea that the application of the latest patches should be considered as possible.

One security expert pointed out in the review that attack methods tended to find vulnerabilities through hardware analysis; the JTAG and UART, which are connection ports for debugging during the development phase left on boards by vendors for flaw analysis, are commonly targeted. This aspect is unique to IoT devices. Therefore, Q2-B15 is to verify that these ports are eliminated for the production version. Even quality experts understood the reason for the removal, however, they were hesitant to make the removal mandatory because these connection ports were necessary for error analysis. Eventually, we decided to establish a blockade that requires connection authentication instead of eliminating these ports.

Q2-16 is to check whether the external listening ports unnecessary for the application of IoT devices are closed off. The security design principle has the idea of minimizing the number of objects to be protected. The aforementioned IoT problem of Mirai was caused because the telnet access port, used during development but not necessary for users, was exposed to the internet world in a listening state. In addition to unnecessary ports, the removal of unnecessary functions included in open source packages should also

be considered. This aspect may be added to the metrics. However, careful consideration should be given to removing the functions, because using an open-source package that is said to work, with its self-modifications, involves detailed operation verification work and sacrifices the original benefit of short-term development.

Q2-17 is another security assessment, along with static and dynamic assessments. It is an evaluation in which various unexpected data is input to check if it does not lead to abnormal behavior. For IoT devices with limited resources, abnormal data input often causes the device to suspend, behave abnormally, fall into safe mode, operate in administrator privilege mode, or fail to operate according to specifications. However, the possibilities of the fuzz data to be input are infinite, and the time involved in the test could be enormous. Also, even if the evaluation results found no particular problem, the test cannot guarantee that it is safe. To make the test effective and efficient, it is better to define the range of fuzz data to be tested and the duration of the test before testing, and then check if there were any problems within that range.

IoT vendors develop IoT devices by aggregating the deliverables of suppliers, contract developers, and external resources. From this perspective, Q2B-18 is a delivery acceptance check to ensure that the outsourced resources do not contain any security issues before the IoT vendor manufactures the IoT device. Instead of conducting the acceptance verification themselves, IoT vendors may require their contractors to submit the results of the specified security evaluation.

Q2-19 is formulated to check the security service level of the cloud, which is the operating environment for the service site that IoT devices connect to. The IoT vendors generally rely on the security management system of cloud vendors who are knowledgeable about security but neglect the security measures that they must implement. However, the scope of security management services provided by cloud vendors is limited; hence, they must clearly understand that scope.

4.4.4.3 Area 3: Security Production

Area 3 is part of the production-process check that is specific to IoT devices. The peculiarity of this part of the IoT production process is that the responsibility for this part is not with the development or quality assurance department but with the factory. There is no appropriate reference found in this aspect. The questions and metrics for Area 3 are listed in Table 4.6.

Table 4.6 Question and Metrics for Area 3

Question	sub-question	Metrics
Q3-1: Is the product produced in a secure manufacturing process?	Q3-11: Is the identity of the line manager verified for in-house production?	M3-11-1: All employees are identified. = 1 Not all of the person in the factory are identified. = 0
		M3-11-2: There is a record of the access control to the production site. = 1 There is no record of access control. = 0
	Q3-12: Has the ODM (Original Design Manufacturing) manufacturing process been verified?	M3-12-1: Company name and country of production are confirmed. = 1 It is hard to confirm who manufactures. = 0
		M3-12-2: The results of the production process audit are confirmed. = 1 There is no confirmation. = 0
	Q3-13: Is production under control to be produced with genuine parts?	M3-13: Certificates of authorized parts are verified. = 1 There is no confirmation, = 0
	Q3-14: Is the production process capable of setting each device with unique IDs and passwords?	M3-14: It is capable of setting unique IDs and passwords to each device. = 1 It is not capable. = 0
Q3-2: Is there security measure in place for the production system?	Q3-21: Is it possible to detect cyber-attacks such as malware infiltration, virus infections and others on production systems?	M3-21: It is capable of attack detection. = 1 It is not capable. = 0
	Q3-22: Are security measures in place for production systems?	M3-22: Security measures to the production system are in place. = 1 There is no security countermeasure on the production system. = 0
	Q3-23: Is coordination in place with CSIRT for incident response?	M3-23: CSIRT is cooperating for factory incident. = 1 There is no incident response readiness. = 0

Although an IoT product has been developed into a secure product through Areas 1-B and 2, it cannot become fully secure unless proper production controls are in place during the production phase. For example, the requirement is setting different passwords for individual IoT devices is necessary during the production process; however, if they

are accidentally shipped with the same password, then all the IoT devices can be affected if one of them is attacked. However, if individually different passwords are set at the time of shipment, only the attacked IoT device can be affected; hence, attacks on other devices can be prevented. Therefore, even if a product is designed with safety in mind, it can never be produced as a secure product unless the proper production controls are in place; Q3-1 confirms this secure production process perspective.

Factory production systems have recently been under attack. In many cases, the systems that manage and control production lines were attacked and forced to shut down. From the perspective of product supply continuity, factory production systems were also included in the scope of the study. The security of a production system of a factory is not the IoT product itself; therefore, the questions and metrics on the factory system management are unique. However, the trust of consumers in vendors of IoT products can certainly increase if the products are produced in factories that are safe from cyberattacks.

As sub-questions, Q3-11 confirms the legitimacy of the person in charge of the production line, and Q3-12 checks the management system of the production line in the case of outsourced production. Q3-13 also confirms the legitimacy of the parts or the genuine parts put into the production line. In production sites, there are cases, not limited to security, replacing parts without the approval of the ordering party to alternative parts that are not following the original specifications of the contract, or where counterfeit parts with functions not specified in the specifications are delivered. These are confirmations to dispel such concerns. Q3-14 checks the possibility to produce IoT devices that allow the setting of IDs and passwords unique to the individual device as mentioned above.

There was no specific objection or concern raised by either quality or security experts against the questions and metrics in this area. Questions and metrics in this area may include confirming that the master software is free from infection by malware, or that imitation parts are not installed, by the lesson of the past experiences that have occurred in manufacturing.

4.4.4.4 Area 4: Security Operation

The questions and metrics on Area 1 to 3 relate to confirmation of the effort involved before launching IoT devices into the market. On the other hand, those of Area 4 relate to the post-marketing stage. These questions and metrics are intended to ensure that a system is in place to provide security support for the IoT devices being utilized in the market. For example, the questions and metrics sought to establish whether the company monitors vulnerability information about software components in IoT devices, whether it

has a defined process and members to respond to security incidents upon discovery, whether it has an in-house information management system, and the procedure to do when security support ends. At the beginning of the study, the implementation and confirmation of functions to maintain security during the use of IoT devices was included in this area. However, since the functions necessary to ensure security need to be considered and implemented at the design stage, they were moved to Area 1-B. The questions and metrics for Area 4 are listed in Table 4.7.

Many electronics manufacturers have developed a customer service system to answer any questions or problems with their products. However, they did not have a system to monitor the operational status of the products they sold. Because the ownership of the sold product is transferred to the customer, the vendor has no right to monitor the equipment unless requested to do so. The following four sub-questions were set.

Security is different from the quality that naturally degrades because the situation changes day by day. And there is no way to predict when a security problem will be discovered in the IoT devices provided. Q4-1 confirms this point of view. Question Q4-11 confirms the existence of a system for monitoring security issues in the security operations center (SOC). Questions Q4-12 and Q4-13 verify the existence of a system and process for dealing with the discovered security problems of IoT devices. Question Q4-14 confirms the presence of a contact point for external security issues.

The management of personal information is a concern for users. An appropriate policy and management system in place is important to gain the trust of users; Q4-2 confirms this perspective.

Q4-3 is also a question from the perspective of gaining users' trust. Stable operation of IoT devices and their linked services will lead users' trust in IoT vendors. Cloud services are also a target of security attacks. Therefore, it is necessary to confirm the system to constantly check the status of the connecting cloud services. And the system should manage customer information on the services to minimize downtime and reduce the risk of personal information leakage. Sub-questions Q4-31-1, Q4-31-2, and Q4-32 confirm this perspective.

Table 4.7 Question and Metrics for Area 4

Question	sub-question	Metrics
Q4-1: Is there a product security response team for the products in the market?	Q4-11: Is there an operating system to monitor vulnerability information for products?	M4-11: SOC (security operation center) is in place. = 1 There is no system to monitor vulnerability. = 0
	Q4-12: Is there an incident response system for products?	M4-12: PSIRT (product security incident response team) is in place. = 1 There is no response system. = 0
	Q4-13: Is the incident response process defined?	M4-13: The incident response process is documented. = 1 There is no process defined. = 0
	Q4-14: Is there a contact point for receiving vulnerability information?	M4-14: The contact information is publicly available. = 1 There is no contact information. = 0
Q4-2: Is there a personal information handling policy and management system in place?		M4-2: There are a policy and a management system. = 1 There is no policy and management system. = 0
Q4-3: Is there a system for the stable operation of IoT devices?	Q4-31: Is there a system monitoring the operational status of the cloud services which IoT devices works with?	M4-31-1: The cloud operator's contact information is clarified. = 1 There is no means to check the cloud operation. = 0
		M4-31-2: It is capable of checking the status of cloud operation. = 1 It is not capable of checking the cloud operation. = 0
	Q4-32: Is it capable of managing customer information for service in use?	M4-32: It is capable of managing customer information based on the management rules documented. = 1 It is not capable. = 0
Q4-4: Are restrictions on product security support clearly stated?	Q4-41: Is the warranty period and exemption for security service/maintenance provided?	M4-41: Security service/maintenance that the company provide is clarified. = 1 It is not clarified. = 0

Users trust IoT vendors and their products, especially without paying much attention to security. In order to manage to provide IoT devices with high cost-performance, it may

be possible to compromise security capability to some extent. Q4-4 confirms this point. Additional maintenance service for security may be provided, separated from the general product warranty.

In response to the draft questions and metrics for this area, one of the security experts pointed out one issue. Once a security problem is discovered, an investigation of the cause of this problem should be conducted. Checking the logging records will be the first step of the investigation. Thus, the function for logging the activity history and the connections to the external entities was emphasized. There was also a suggestion that the IoT devices themselves should self-verify the necessity of software updates; hence, this functionality was added to the pertinent items.

4.4.4.5 Area 5: Law, Regulation, International Standard

Area 5 must be fundamentally considered at the product planning stage, as discussed in the goals section. However, according to the literature review, the regulations and/or guidelines requiring compliance may relate to the entire lifecycle of the product. Accordingly, Area 5 is defined as an independent area from the others.

Depending on the industry sector and the IoT product destination on the globe, the laws and regulations that must be adhered to and the international standards and guidelines that must be ratified differ; hence, they have to be carefully checked. In particular, laws, regulations, and guidelines for IoT security are still evolving and changing in terms of content. Thus, staying updated is necessary to ensure compliance. The questions and metrics for Area 5 are listed in Table 4.8.

In this area, three general questions were established: Q5-1 simply ascertains whether the IoT device conforms to the laws and regulations enforced in the country or region where it will be sold; Q5-2 ascertains whether it conforms to specified international standards; Q5-3 ascertains whether it conforms to certification program requirements for IoT security carried out in the private or other sectors.

The metrics are simply proof of compliance with the required regulations, international standards, and certifications. For users, a declaration of compliance is easier to understand than a detailed specification, and for companies, it is easier to explain to the public.

Table 4.8 Question and Metrics for Area 5

Question	sub-question	Metrics
Q5-1: Does the product comply with the laws and regulations about the product security of the region to be sold?	Q5-11: Does the product meet legal and regulatory requirements?	M5-11: There are the evaluation results that meet the requirements. = 1 There is no evaluation result. = 0
	Q5-12: Does the product have the required certifications or conformity statements, if necessary?	M5-12: After confirming the necessity of certification/conformity certificate, the acquisition result can be confirmed. = 1 The need for a certification/conformity certificate has not been confirmed. = 0
Q5-2: Does the product comply with the required international standards?	Q5-21: Does the product have the required certifications or conformity statements, if necessary?	M5-21: After confirming the necessity of certification/conformity certificate, the acquisition result can be confirmed. = 1 The need for a certification/conformity certificate has not been confirmed. = 0
Q5-3: Does the product comply with private security certification?	Q5-31: Has the product acquired the certification of conformity with the standard that is decided to be required or voluntarily acquired?	M5-31: After confirming the necessity or voluntary acquiring of certification/conformity certificate, the acquisition result can be confirmed. = 1 The need for a certification/conformity certificate has not been decided. = 0

The quality or security experts did not have any specific objection or concern about the questions and metrics. However, the quality experts suggested that it would be easier to convince company management of security initiatives if these were generally accepted by third parties in the form of certification.

4.5 Expert Review and Opinion Gathering (Step 4)

The draft items for the security quality metrics for IoT devices were reviewed by a group of eight quality control experts and a group of six security experts who are not familiar with security. The following points were raised as common comments from both groups. There is nothing to disagree with within the proposal.

- In general, how rigorously quality evaluation is performed and the man-hours required to perform it are directly related to the cost of the product. Therefore, in order to make products as low cost as possible, the cost of quality assurance is limited to the bare minimum, such as complying with laws and regulations, or ensuring quality such as safety, which is considered essential by users. However,

if there are many things that are not done, it will give a negative impression to the procurement side, so it is difficult to find a balance between the procurement side that wants to know and the vendor side that does not want to inform too much. It is also important to consider whether all of the items listed must be addressed or not.

- In the case of B2B (Business to Business), the procuring side wants to know everything, so the more the better in some cases. In B2B, the more the better because the procurer wants to know everything.
- On the other hand, in the case of B2C (Business to Consumer), users generally do not care much about the details (or do not understand them). It is important to display the information in a simple and easy-to-understand manner with such a certification mark. However, since they are sensitive to their personal information or privacy, it is necessary to include a section on the handling of personal information.

A group of quality experts pointed out the possibility that vendors may want to refrain from (or may not want to present) the detailed security status of their products, even if they are treated as confidential in B2B because the level of countermeasures can be conveyed to attackers if they are presented as quality in too much detail. Therefore, it is necessary to carefully consider what should be disclosed externally in the metrics to satisfy customers.

The group of security experts made the following additional points.

- It would be better to divide the items into mandatory and recommended items, rather than all being uniform.
- Forensics is important as a security measure. The existence of a log function is very important.
- It is important to check whether the product has a function to check its own status (self-scan) during automatic updates.
- Procurers want to check the development environment (framework or integrated development environment (IDE)) that automatically generates code since vulnerabilities can be built in due to problems with the development environment.
- Hardware analysis has been pointed out as a problem specific to IoT devices. Procurers want to check the sealing status of UART and JTAG on the circuit.

- Concerning personal information, users want to check the vendor's "information security management policy," the system for handling personal information, and the existence of a system for responding to problems when they occur.
- Procurers or users would also like to check the scope of the service level guarantee and disclaimer after shipment.

These opinions were reflected in the draft to complete the aforementioned quality metrics items.

4.6 Expert Opinion Analysis (A Part of Step 5)

The method of placing quality metrics throughout the product lifecycle to increase the transparency of the security quality of IoT devices through both process quality items that measure the efforts made in the design process of IoT devices and product quality items that confirm the security measure functions of the products was found to be appropriate and gained a certain level of understanding by experts.

The experts' opinions on the items in each area are as described in Sections 4.4.4 and 4.5. What was impressive was that the security experts tended to want to check the points of concern in detail, while the quality experts tended to have a strong customer-request-based approach to check in the form that the customer wants to know. In particular, the quality experts told us that for consumer products, most customers are more willing to believe a product as long as it meets a certain standard and shows that it is OK with something like a certification mark, rather than detailed information.

4.7 Discussion of Setting IoT Device Security Quality Metrics

In this chapter, the flow of deriving metrics was explained. The author established the draft questions and metrics as in Appendix 2 from the literature review. And the security and quality experts reviewed them. The author received their input on items to be added, resulting in the metrics shown in Table 4.3-4.8.

The metrics presented here are the result of the author's discussions from the perspective of confirming what IoT vendors are doing as security measures in developing and providing IoT devices, independent of the industry sector, and are not final and complete. And again, because there is no one-size-fits-all definition of security quality metrics common to all IoT vendors, the metrics should be tailored by IoT vendors for designing their IoT devices.

Most regulations, guidelines, and certification programs only describe what needs to be done without designating an entity to put into practice and without clarifying the purpose of action to perform; this results in ambiguity over the extent of duty and may lead to nothing being accomplished. With this metric, however, the rationale is clear from the GQM.

In the case of examining security robustness, more metrics, such as the presence or absence of security features, can be introduced. As for the reliability of data outputted by IoT devices, metrics can be added for it from the perspective of integrity to confirm that IoT devices have not been tampered with. Moreover, confirming whether the appropriate design and implementation are accomplished is necessary. When adding these metrics, confirming the existence of specifications and functionality evaluation is necessary. In any case, if something needs to check, it is important to clarify the purpose (goal) of the check and the reason for setting the metrics to be checked. There is no single set of metrics universally applicable to all IoT devices. Thus, the author proposed this as a method to tailor referencing the sample metrics presented here, depending on the characteristics of the IoT device.

IoT vendors need to make IoT devices secure through a certain approach and consider how to claim the security capabilities of IoT devices separately. However, IoT vendors who have no experience in quality assessment in the security aspect do not understand what to assess. The design and development department takes the lead in the design and development of software and systems, and the corporate culture in which the design and development department has also been responsible for the functional evaluation of the software and systems has permeated the electronics vendors. Therefore, there is an implicit understanding that the design and development department is also responsible for software security. However, the members of the quality control department have experience in identifying hazards in product safety, taking measures to reduce the risks caused by those hazards, and evaluating the implementation of those measures. Once they understand the same concept of quality assessment for product security and the purpose and reason for the assessment, they will be able to tailor the necessary metrics.

By setting up metrics and keeping the evaluation results, evidence that security measures are being implemented can be provided. This evidence can be used to hold the security response accountable. Considering security as a part of IoT product quality, the

ability of vendors to explain their product security efforts to users can generate competition among companies in providing IoT devices that gain the trust of users.

5 EFFECTIVENESS OF THE PROPOSED METHOD (STEP 5)

As discussed in Section 4, the draft proposal of IoT device security quality items was clarified (step 3) and reviewed by the experts (step4). Then, the effectiveness of this proposal was examined as Step 5. In this section, the author describes the verification of the effectiveness of the IoT quality metrics method devised in this study from two perspectives.

The first is the possibility of implementation by IoT device vendors and the effect of presenting quality metrics in a transparency model as compared to mere existing guidelines. The other is the effectiveness of this quality metrics section as a tool to identify the features of the requirements of IoT-related regulations, guidelines, and certification programs.

5.1 Feasibility of Implementation of This Method to IoT vendors

Many IoT vendors are aware of the need for security. However, they are not able to take action for it, because the author suspects that not only they do not know what to do, but they also don't have a clear picture of when to place to do in their existing processes they should be doing it. The author hypothesized that providing information on "what to do," "who and when to do it," and "how to check within existing processes" would lower the bar for product security measures and make it easier for IoT vendors to begin their efforts. On the other hand, if the security response process is set up independently from the existing product development process, the person in charge of the actual product

development and the person in charge of quality evaluation will have to carry out the two separate processes in parallel, which will place a heavy burden on them.

In this chapter, the effectiveness of the metrics created by this method is examined. The metrics should be comprehensive to IoT vendors. Therefore, it is important that the effectiveness of this approach is consistent with existing product development processes and that the security response efforts can be embedded in existing processes.

5.1.1 Subject Selection and Criteria Setting

The two IoT vendors are selected, and the examination asking to consider using this approach to incorporate product security initiatives into their existing product development process is conducted. One of the vendors is a company with internationally well-known brands offering products internationally in several industries including Automotive, Medical, and Audio Visual. Among the six business units, two business units involved in industrial sectors with high-security response needs were considered for implementation. The other one is a start-up company, with a size of about 100 employees, who are developing their own IoT services with IoT devices under their own development process standard. The reason why the author chose IoT start-ups as an evaluation target is that the author wanted to make sure that the proposed method is understandable and adaptable not only by large enterprises but also by a wide range of IoT start-ups.

The following criteria were set for evaluating effectiveness.

- a) No items that contradict the existing development process
- b) No items that are inconsistent with market requirements for IoT devices

5.1.2 Results of Examination

5.1.2.1 Results in the Criterion a)

Neither of these companies expressed uncomfortable with these proposed metrics because they understood why they were implementing them. In the course of the implementation study of this method in the two business units at the vendor with International brands, they raised some questions. One question is about the meaning of the individual metrics, and the other is about whether or not to set priorities based on the requirements of the marketplace (i.e., 4 items out of 67 (6.0%): two in Area 2, one in Area 3 and one in Area 4). Those questions were clarified through the discussion. Both companies judged the metrics to be able to introduce their existing development process.

Their responses indicated that there were no items that could not be implemented due to inconsistencies in their existing process.

Moreover, the need for additional items for the industry-specific requirements was pointed out; however, there was no problem with this methodology since the sample in this study dared to use metrics that excluded industry-specific requirements. One of the two business units of the International brands has completed implementing the proposed security metrics to their development process, which will be applied to the next phase of product development.

This result showed another effect such that the business unit is able to clarify what the industry-specific metrics are necessary and also able to improve the metrics by adding industry-specific ones based on the reasons why the industry and/or users want to require them. At the start-up vendor, their response is also in favor of the metrics proposed since all of the items are understandable with reasons why to check. The results of the examinations also confirmed that the three points (a, b, and c) raised above in Section 4.4.4 are satisfied.

5.1.2.2 Results in the Criterion b)

Both vendors expressed that they can assume the security risks if they do not use the metrics. Furthermore, no inconsistencies were found in checking the coverage against regulations or guidelines. However, one question was raised on whether everything should be clear (or satisfied) as quality checkpoints. This question was raised because it might cause a situation where the product could not be released at the quality assurance check if all the metrics need to be cleared or satisfied. The response to this question was no. It is key to know the status of the security quality of the IoT devices. However, this issue should be clarified using the metrics.

5.1.3 Discussion of the Results

The proposed metrics have been validated and proven to be implementable by the IoT vendors in practice. External validity was validated not only in specific areas of a large company but also in the development of IoT systems in small and medium-sized start-up enterprises. There was no issue observed in the examination based on the premise of real deployment, not just for a trial.

5.2 Evaluation of Effectiveness as a Tool for Identify the Characteristics of the Requirements of IoT-related Regulations, Guidelines, and Certification Programs

In this section, the characteristics of the requirements presented in IoT security regulations, guidelines, and certification programs are examined by the sample metrics.

Table 5.1 List of Documents for Evaluation of Effectiveness

Name of Source	Doc Type	Year	Country	Issued by	Org Type
Telecom Business Act	Law /Regulation	2020	Japan	MIC (Japan)	Gov
State Bill 327	Law /Regulation	2020	USA	State of California	Gov
House Bill 2395	Law /Regulation	2020	USA	State of Oregon	Gov
Consumer IoT Security Consultation	Law /Regulation	2020	UK	Department for Digital, Culture, Media & Sport	Gov
EN 303 645 v2.1	Baseline Standard	2020	EU	ETSI	SDO
NISTIR 8259	Baseline Standard	2020	USA	NIST	SDO
Baseline Security Recommendations for IoT	Baseline Standard	2017	EU	ENISA	Gov
The C2 Consensus on IoT Device Security Baseline Capabilities	Baseline Standard	2019	USA	Council to Secure the Digital Economy (CSDE)	Industry
IoT Common Security Requirements Guidelines 2021	Certification	2020	Japan	CCDS	Industry
ioXt 2020 Base Profile ver.1.0	Certification	2020	USA	ioXt Alliance, Inc.	Industry
Methodology for Marketing Claim Verification: Security Capabilities Verified to level Bronze/Silver/Gold/Platinum/Diamond, UL MCV 1376	Certification	2019	USA	UL LLC	Industry

This examination is conducted based on the security-quality metrics for IoT devices reviewed by the quality and security experts as a part of Step5 in the research method to examine the effectiveness of the metrics. The regulations, guidance, and certification programs evaluated are listed in Table 5.1. The results are presented in the form of bar charts respectively in the following sections.

5.2.1 IoT Regulations

The following four regulations are compared with the IoT security-quality metrics: California Senate Bill No. 327 [28], Oregon House Bill 2395 [29], Terminal Conformity Regulation under Telecommunications Business Law by Ministry of Internal Affairs and Communications of Japan [30], and the consultation on regulatory proposals on consumer IoT security of the UK [124].

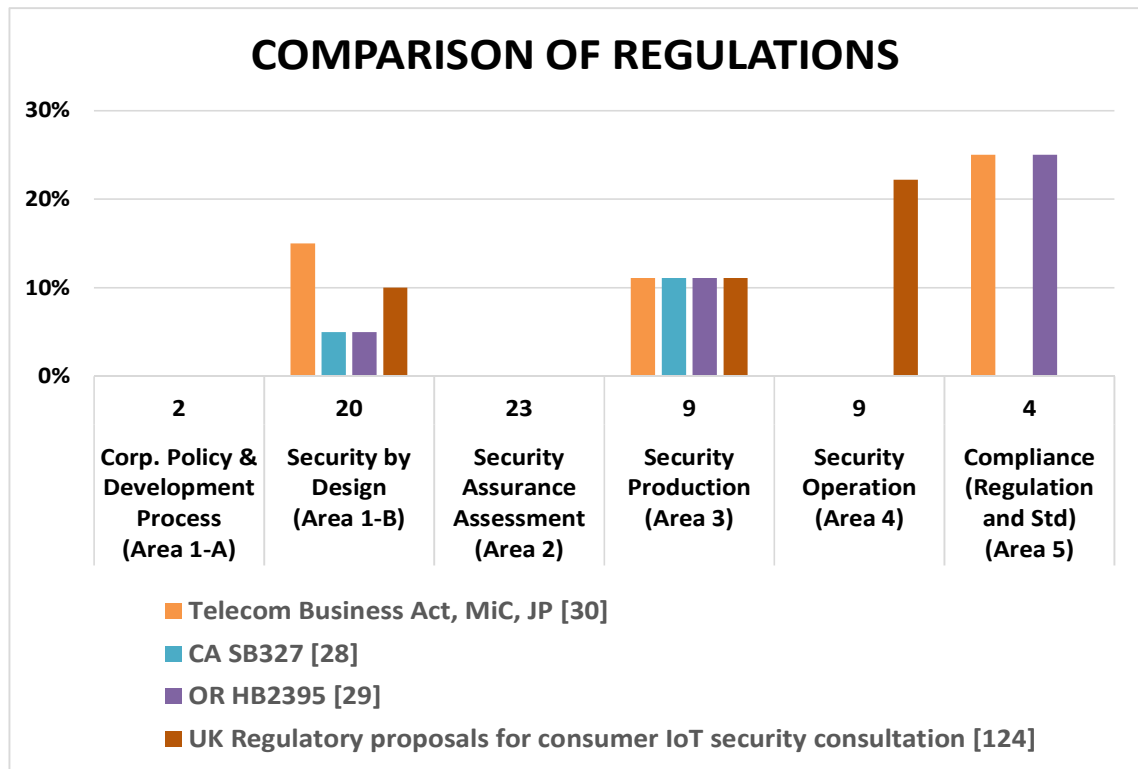


Figure 5.1: Bar Chart of Requirements Distribution of IoT Security Regulations

Fig. 5.1 illustrates the area of the transparency model under which each regulatory requirement falls. The percentages on the vertical scale indicate the ratio between the number of requirements of each regulation, corresponding with the items of the IoT device security quality metrics, and the total number of items of these metrics in each area. The number on the horizontal axis indicates the total number of metrics set for each area. Thus, the percentage for each area is the ratio of the number of metrics matched and

the total number of metrics. This relationship is the same for the bar charts shown in Fig. 5.2 and 5.3.

That the requirements of these regulations are minimal, as can be observed in Fig. 5.1. It is obvious from the figure that Area 1-A of vendor attitude (e.g., security policy) or Area 2 of assessment (e.g., vulnerability assessment) are not required. Moreover, all regulations focus on areas 1-B and 3 (unique device ID/PWD settings). Only the U.K. requires a maintenance system after product sales. Therefore, the IoT device security quality metrics sufficiently cover the range of regulatory requirements well to ensure compliance. From this observation, the UK legislation imposes requirements that are not found in Japanese or US laws and regulations.

5.2.2 IoT Security Baseline Guidance

The following four standards and guidelines from the United States and Europe that are presented as baselines are examined here. These are NISTIR 8259 [125] and 8259A [126] and C2 Consensus on IoT Device Security Baseline Capabilities [127] of the US, and Baseline by ENISA [31] and ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements [128].

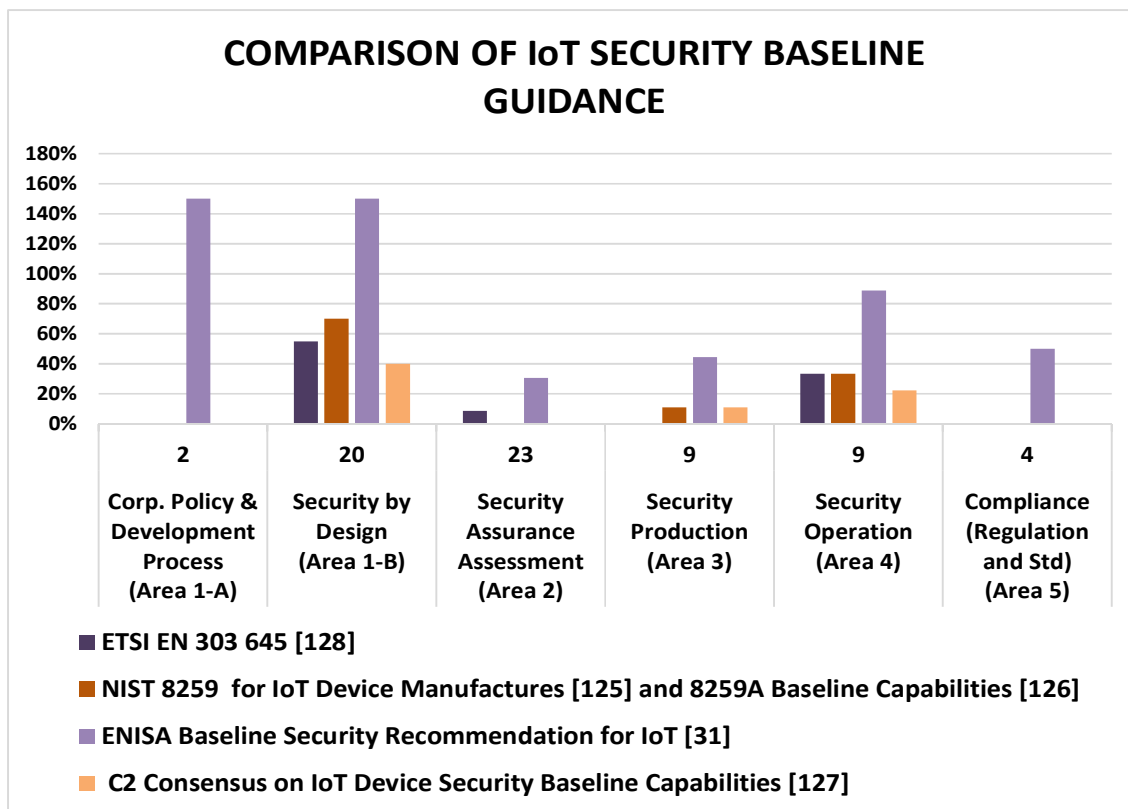


Figure 5.2: Bar Chart of Requirements Distribution of IoT Security Baseline Guidance

Fig. 5.2 describes the results of the area of the Transparency Model that each baseline requirement fits into. The vertical scale indicates the same units as that in Fig. 5.1. Values over 100% indicate that there are a greater number of requirements than the total number of IoT device security quality metrics items in each area.

The distributions of the two standards from the US are similar, and the trend of the requirements can be considered to follow the same direction. Certain functional requirements for devices that were not set in the IoT security-quality metrics were found in these two US standards. In contrast, the two European distributions are very different, showing the different approaches of the two. ENISA has a lot of requirements in all areas. In particular, the security function requirements by ENISA in Area 1-B of Security by Design are very extensive and hence incomparable to the proposed metrics. Contrarily, ETSI has a similar distribution to the US one. The approach of those to baselines is considered close.

5.2.3 IoT Security Certification Program

Several private IoT security certification programs have been released on the market. The following four sets of requirements were examined. The first is from the certification program of CCDS [109] in Japan, and the second is from the ioXt alliance [129] in the US. Finally, we analyzed the two different grades (Bronze and Diamond) of the IoT Security Rating of UL [130], also in the US.

The result for the area of the Transparency Model to which each certification requirement belongs is described in Fig. 5.3. The vertical scale represents similar concepts as those in Fig. 5.1 and Fig. 5.2, and the meaning of the values that are greater than 100% is also the same. Except for the requirements of UL Diamond, the rest of the programs have a similar number of requirements, and these are covered (i.e., they are below 100% line) by the metrics.

The author also observed that the requirements in the security functions of UL Diamond in Area 1-B are strict as the same level of ENISA baseline requirements [31]. This implies that the ENISA baseline requirements are a very high-level set of requirements, despite being baselines.

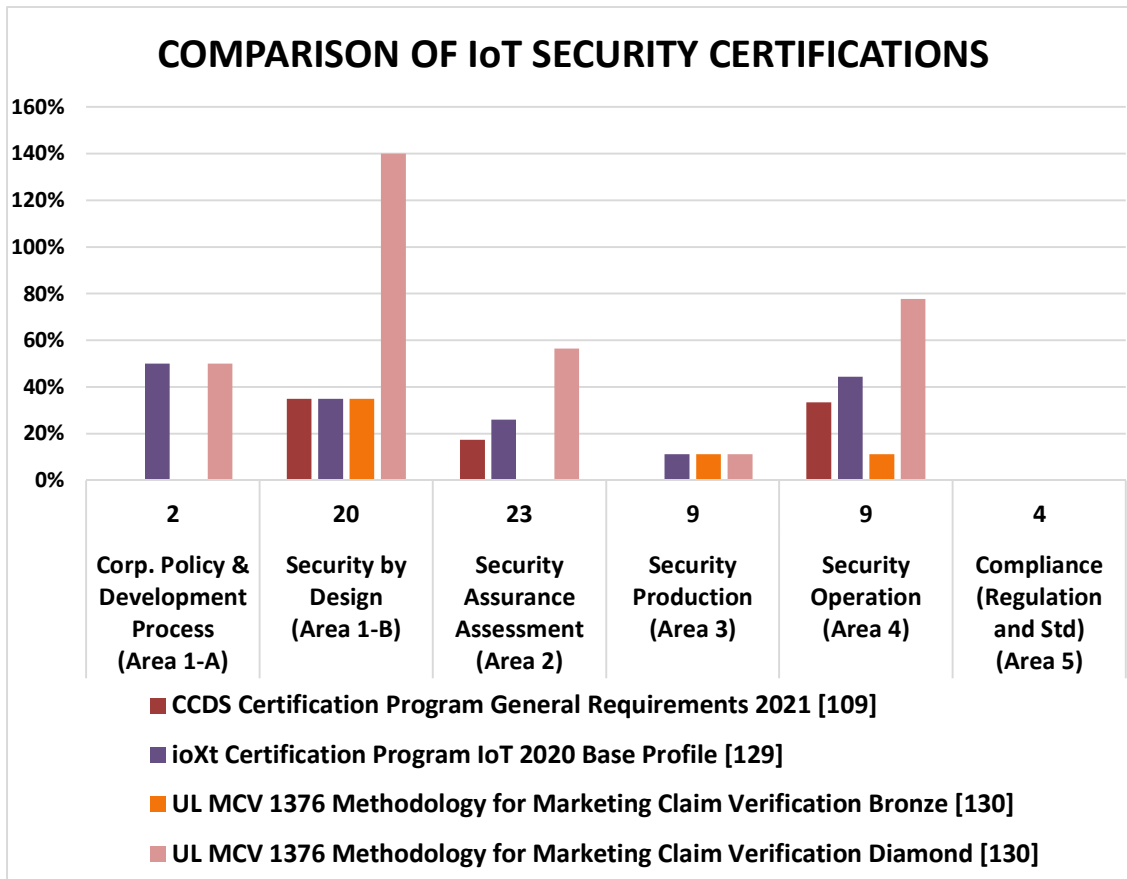


Figure 5.3: Bar Chart of Requirements Distribution of IoT Security Certification

5.2.4 Discussion of the Results

As described in Section 3, the IoT device security quality metrics are examined from a product lifecycle perspective; quality items are articulated in a manner inspired by GQM methods common in the quality community. And the metrics that were reviewed by quality and security experts are produced.

Originally, the proposed method was designed to help IoT vendors to produce their own IoT security-quality metrics. However, the metrics also confirmed its effectiveness as a tool for understanding which requirements are missing or deficient in the product life cycle. It proved to be a useful tool for grasping the characteristics of the requirements of guidelines and certification programs, and for planning the allocation of man-hours when developing products. Because the metrics show the characteristics of each requirement group, the effectiveness of using them to adjust the balance of the security effort focused on each area is also confirmed. In practice, the international standards by themselves are insufficient for practical implementation; hence, customizing the contents of international standards to suit the development target, development process, organization, and environment is necessary. Botella et al. discussed [131] that the GQM could be employed

for this customization. Furthermore, its refinement is required. In the future, as the product security efforts of IoT vendors advance, improvements are required. The validating GQM is proposed as a method for reviewing or improving each GQM element [132]. The review or improvement must be implemented as soon as the values of the metrics are collected. The use of such a method is expected to facilitate the implementation of reviews and improvements.

As mentioned in Section 4, all requirements are not distributed evenly throughout the product lifecycle. All regulations are focused on Areas 1-B and 3, whereas only the UK focuses on the maintenance phase of Area 4. Additionally, ENISA suggests incorporating the items in all areas (especially items in high demand) into the policy, process, and security functions at the design phase. Other baselines focus on security functions and operations rather than the level of ENISA. Most certifications focus not only on security functions but also on security assurances.

A group of quality experts shared their experience that there would be cases where there would be resistance to providing all the detailed information of quality assessment to the procuring party, even if it is for the sake of transparency. As a countermeasure to this issue, the method of showing the coverage rate of the requirements indicated by the procuring party in the form of a bar chart may be effective as a way to show that the requirements are being met without exposing everything in detail.

6 EVALUATION OF IOT DEVICES WITH THE PROPOSED METHOD

The author evaluated the IoT devices by the proposed method. This evaluation is also part of the verification of the effectiveness of Step 5. The author selected two commercial dashboard camera (dash-cam) recorders (Product A and B) with almost the same functional product specifications as the sample IoT devices. Both were products provided by ODM (Original Design Manufacturing) vendors. The author will refer to them as Product A and Product B so as not to identify two products.

6.1 Target IoT Devices

The two products are similar in the following aspects.

- They are consumer products that can be purchased online and in stores.
- A full-HD high-definition recording is the main selling point
- Global Positioning System (GPS) location recording
- Wi-Fi (wireless) connectivity with a smartphone
- 16 Giga-byte (GB) storage space
- Easy to install and start using by powering from a cigar socket
- Downloadable applications for smartphones and PCs that can be connected to and functionally linked with a dash-cam

As mentioned above, the two dash-cams are very similar in terms of functionality. The only differences observed from the specification are the following points.

- Product design: shape and color
- Price: Product A is cheaper than Product B.

Simply speaking, since they are almost the same in terms of functionality, most users will choose Product A because of the price difference, unless they like the design too much. However, as a user, the following points not readily apparent from the functional specifications are of concern. The points are the policy for handling personal information such as recorded image information, GPS information, information about the user, and the access restriction function for connection functions.

6.2 Evaluation with the Proposed Method

Based on what the author was able to confirm through interviews with ODMs, the security perspective is evaluated and compared with the metrics of the proposed method. The evaluation results of all metrics are described in Appendix 4; Table 6.1 summarizes the results.

Table 6.1 Summary of the Evaluation Results

	# of Metrics	Product A	Product B
Corp. Policy & Development Process (Area 1-A)	2	0%	100%
Security by Design (Area 1-B)	20	45%	70%
Security Assurance Assessment (Area 2)	23	0%	13%
Security Production (Area 3)	9	22%	78%
Security Operation (Area 4)	9	11%	22%
Compliance (Regulation and Standard) (Area 5)	4	25%	100%

6.3 Evaluation Results

The results of the evaluation in a bar-chart format are shown in Figure 6.1. The comparison results show that Product B has more product security measures in all areas than Product A, and we can infer that the security quality of Product B is better. This difference is probably reflected in the price difference.

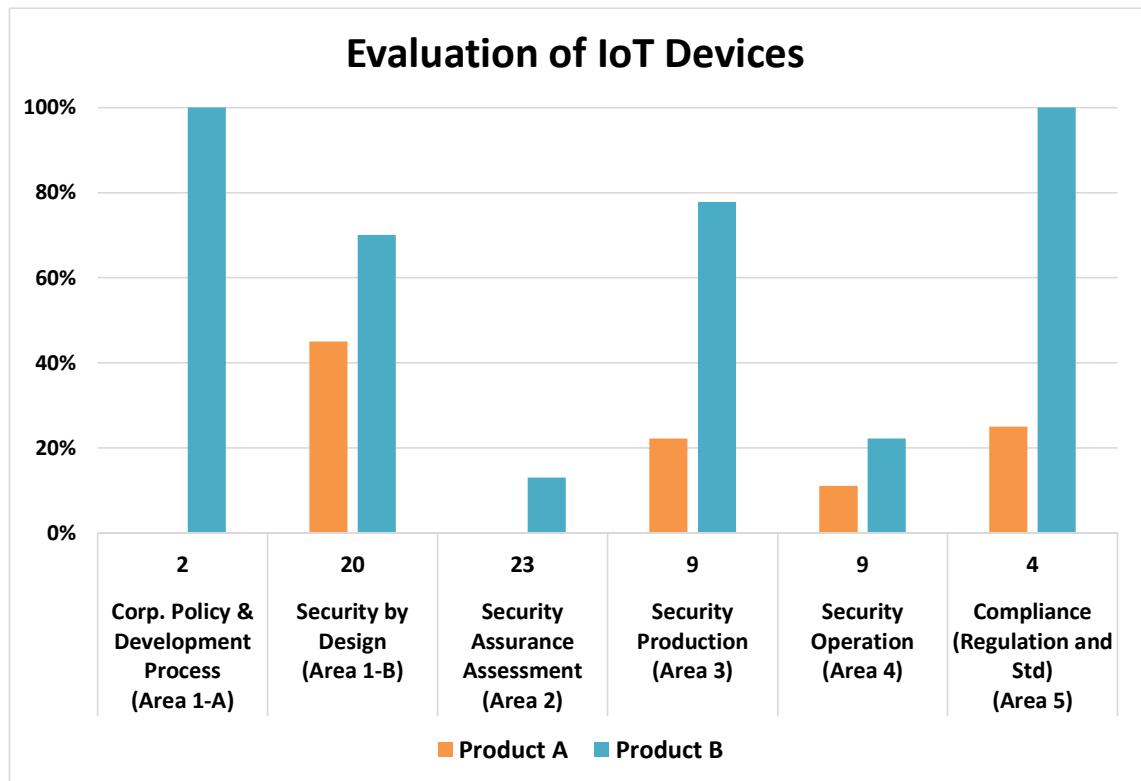


Figure 6.1: Bar Chart of Results of Evaluation

Both companies had policies for handling personal information. However, there was a difference in the authentication of the Wi-Fi connection: Product A had the factory default access point name as the product name and no password (blank). Product B, on the other hand, had the same factory setting with the product name as the access point name, but the password was set to be unique for each device. This perspective is critical as the requirements affect compliance with California law. Although the specification that anyone can use the device immediately without a password is appealing, the default setting that only the purchaser of the device can access is safer. Even in Product B, we found that there are few efforts in Area 2 and Area 4. The security-conscious IoT vendor of Product B has yet to demonstrate security verification or post-shipment support.

6.4 Discussion of the Results

The proposed method demonstrated that it could illustrate the differences in the security quality of IoT devices. Overlooking the five areas, the security efforts in each area in Product B are higher than those in Product A. At a glance, it is clear to understand that Product B is a more security-conscious product. In other words, it could increase the transparency of the security quality of IoT devices. A closer look at the metrics evaluation results in Appendix 4 also reveals the following points.

First of all, the author noticed in Area 1-A that the vendor of Product A does not have a product security policy nor a product security development process, while Product B does. For users, a company's commitment to product security is a high priority in product selection.

Next, in Area 1-B, the author noted that Product A does not have Threat Analysis and Risk Assessment (TARA), but still designs security measures. The effectiveness of Product A's security measures designed without identifying possible threats and risks that should be reduced or eliminated is questionable. On the other hand, Product B has conducted TARA and designed security measures, so the effectiveness of the security measures in Product B is trustworthy. The content and source of the software configuration for both Product A and B are clear, and the author can assume that both can handle the security issues in the supply chain.

In Area 2, neither of the two products did much security assessment, with Product B only performing static analysis of the source code on the development tool. Even if the design of security measures is good, it would be a problem if the source code is vulnerable. But the value of the metrics is that these metrics illustrated the weakness of the security assessment phase.

In the production phase Area 3, the author focused on the capability to set a unique ID and password for each device. Setting unique IDs and passwords for each device at the time of shipment is becoming a legal requirement in California, Japan, and the UK. Since a dash-cam is a consumer product, this is an important assessment item. Another noteworthy item was the security measures for Product B production systems. In recent years, there have been several problems involving the shutdown of factories due to ransomware attacks, and this is an important initiative in terms of business continuity.

In area 4, there were no major differences between the two products, and both vendors had privacy policies in place. The visualization from this evaluation revealed that there was little to no security support system after the shipment of the products, thus revealing the need to determine the support details through contracts. Regarding the response in area 5, Product A pays a minimum amount of attention to laws and regulations but shows little awareness of certifications. The result of Product B, on the other hand, shows that efforts in this area are being emphasized.

Although Product A's functional specifications and capabilities were not inferior to those of Product B, the metrics revealed a significant difference in security, which is a

non-functional specification. If both products were priced the same, people would naturally choose Product B. However, the price of Product B is actually higher than that of Product A. The price might reflect the efforts made not only for security but also for other non-functional specifications. Therefore, this method has the potential to contribute to IoT vendors as a tool to appeal the security quality to users.

At present, it is not easy for general users to make this kind of comparative evaluation since they have only the product specifications released by IoT vendors to judge. However, IoT vendors will want to appeal to users the security measures they have invested in during the development and maintenance of IoT devices. At that time, this method can be a tool to support improvement and raise the level of security measures, since it visualizes areas where security measures are lacking.

The final selection of a product is a comprehensive decision based on information such as product functions, performance, non-functional specifications, and price. The clarification of the security quality will increase the decision-making resources and lead to more appropriate product selection.

7 CONSIDERATIONS ON SOCIAL CONTRIBUTIONS

7.1 Contribution to the spread of secure IoT devices

The proposed method can help many IoT vendors without security knowledge who have started to develop and offer new IoT devices to incorporate security support into their existing development process and contribute to secure product development. In this section, the possible contributions of this proposal to society are discussed.

If IoT device vendors themselves come to understand the security quality of the IoT devices they provide, they are expected to actively promote security quality to users as well. Some IoT vendors will obtain security certifications for their IoT devices and label their products; others will clearly state the security maintenance period for their IoT devices and promote their support system. On the other hand, users will also demand to know the security capabilities of IoT devices, and IoT vendors will evolve their appeals methods to meet such demands. When this movement emerges in the market, this proposed method should contribute to IoT vendors not only for their own internal security quality management but also to be used as a communication tool with users on security quality.

In productizing IoT devices, the in-house development of everything from scratch is not practical. For example, open-source software is being utilized and wireless communication modules are externally procured to reduce the development period and improve efficiency. In this way, multiple parties are building a supply chain to develop a single IoT device. However, the agreement on the security quality of IoT devices among these parties is not yet thorough. The author believes that information sharing on security quality metrics among the parties involved in the supply chain indicates the level of the

security quality of included components and may be effective in managing the security quality of IoT devices.

In addition, product development costs can inevitably increase because security requires an approach that differs from the previous techniques. To ensure the security quality of IoT devices, it may be necessary to invest in development environment facilities and human capacity building. As a policy to realize a secure society, tax incentives for investment by IoT vendors to expand security initiatives may be an expecting option. At that time, security quality metrics are evidence of secure product development.

7.2 Contribution as a Selection Indicator for Secure IoT Devices

The proposed method will also make it easier for all users, including general consumers as well as businesses, municipalities, and government agencies, to understand how secure the IoT devices are by assessing the results of the metrics from IoT-SQMM. As a result, the author believes that this method can contribute to the creation of a market where users will be able to consider not only the cost performance of functionality and price but also the cost performance including the security capability of the IoT devices. Moreover, the users will be able to choose secure IoT devices even if they cost more.

7.3 Contribution to Create Supporting Environment for IoT Vendors by Security Insurance

7.3.1 Product Liability Insurance

Cornell states the following [133]: “product liability refers to the liability of any or all parties along the chain of manufacture of any product for damage caused by that product. This includes the manufacturer of components (at the top of the chain), an assembling manufacturer, the wholesaler, and the retail store owner (at the bottom of the chain). Products containing inherent defects that cause harm to a consumer (or someone to whom the product was loaned, given, etc.) of the product would be the subjects of products liability suits. While products are generally thought of as tangible personal property, products liability has stretched that definition to include intangibles (e.g., gas), naturals (e.g., pets), real estate (e.g., house), and writings (e.g., navigational charts). Products liability is derived mainly from torts law. The primary aims of tort law are to provide relief to injured parties for harms caused by others, to impose liability on parties responsible for the harm, and to deter others from committing harmful acts.”

In the US, the Product Liability Act regulates the liability of a manufacturer for defective products [134]. This law covers all tangible personal properties, even if they have been incorporated into another movable property or forms of immovable property, as well as electricity. There are three types of product defects: 1) design defect that is inherent before manufacturing the product; 2) manufacturing defect that occurs during the construction or production of the item; and 3) defect in marketing, that is, improper instructions or failure to warn consumers of latent dangers in the product. Since IoT devices and systems are cyber-physical, IoT devices may harm users if IoT devices are controlled by their controlling systems to move their arms or close their doors without any safety protecting mechanisms. The new potential issues of product safety and liability are pointed out [135].

In the field of product safety, there are product liability insurance schemes in place in the unlikely event that a product defect is discovered, resulting in a recall that requires corrective measures or a recall. On the other hand, in the field of information security, cyber insurance schemes that protect against problems caused by operational cyberattacks, such as customer information leaks due to attacks on corporate information systems and outages due to attacks on operations management systems at critical infrastructure facilities and factories, are beginning to spread. Then, the new need for cyber-insurance on IoT should increase as IoT becomes spread.

7.3.2 Creating a New Market for IoT Security Insurance

Currently, IoT vendors have no choice for transferring the risk of IoT devices to insurance. The only options left are to take implement countermeasures to reduce the risk or to accept the risk. When the author interviewed the insurance industry, there are three major requirements necessary for an insurance program to be established;

- 1) Insurability to be established by the law of large numbers
- 2) Availability that can cover wide-range of individuals even the one with high risk, and
- 3) Affordability is a reasonable range of premium payments.

According to the insurance industry, there is still very little data available for cyber insurance underwriting, making it very difficult to set premiums, even some insurance programs have started. It is said to take ten to fifteen years to collect sufficient data to calculate the cyber risk of a company. When an IoT device is attacked by a cyber-attack, the level of resistance of the IoT device to the attack can be estimated by the IoT device

vendor's design and evaluation efforts before shipping. It will also be possible to estimate the cost and time required to repair the equipment depending on the presence or absence of a system to deal with the incident problem.

If the case, the proposed quality metrics method for IoT device security could be a useful and helpful reference to consider new cyber insurance for IoT devices or IoT vendors. And, if the results of the proposed metrics and the relevance of secure IoT devices are converted to data, it could contribute as reference material to plan new cyber insurance for IoT vendors, in near future. If such an insurance mechanism is established, there will be more options for IoT device vendors to choose from when considering security measures, such as transferring the risks to insurance or implementing technical measures, which will further promote the development of cost-effective, secure IoT devices.

Under such circumstances, there is an example in Japan of an insurance policy attached to the certification of IoT devices that covers the cost of investigating the cause of security incidents. The CCDS [136] has started its private certification program [109], [137] for IoT devices with liability insurance. According to CCDS, the certification criteria are limited, and the coverage of insurance is also limited to the cost of initial investigation and the treatment for affected customers. This case might be the starting point, and if the need for IoT security insurance arises, there will be a need to use a broader range of metrics to calculate premium rates. The proposed metrics should contribute as reference materials for establishing security insurance for future.

8 FUTURE DIRECTION

In this section, future issues and research directions, and the limitation of this study will be discussed. There are two areas that the author would like to pursue in this study.

The first possibility would be to categorize the metrics that show the countermeasure capabilities of IoT devices and those that demonstrate the efforts of IoT vendors. The current metrics belong to either or both of these areas. The author plans to examine how to categorize metrics to easily distinguish between the quality of security in IoT devices and the quality of the IoT management process at a glance. The second area that may warrant further research involves investigating methods to visualize the coverage of metrics. Herein, the author selected the bar chart for this purpose; however, comparatively simple methods for visualizing the coverage such as radar charts may be available.

In addition, when the security support after-sales by IoT vendors becomes common practice and the security threats are evolving day by day, the author would need to add and refine the basic set of metrics in detail and need to consider its proper refinement cycle in the future. Furthermore, the author would like to develop this IoT security quality metrics methodology so that it can be applied from the scope of IoT devices to the entire IoT system.

A limitation of the proposed method is that it has been conceived from a framework that assumes a conventional V-shaped development model. Therefore, the author has not been able to evaluate its applicability to recent development methods such as agile development [138], [139] and DevOps [140], [141]. The author would also like to consider evaluating the applicability of the proposed method from this perspective of the recent development practices.

9 CONCLUSION

This study proposes a method for tailoring security quality metrics for IoT devices to ensure the security quality of IoT devices, named IoT Device Security Quality Metrics Method, IoT-SQMM. And the method demonstrates the validity to evaluate the characteristics of the emerging requirements and suggestions of relevant laws, regulations, guidelines, and certification programs in IoT security based on the produced metrics. Also, the proposed method demonstrates its capability to reveal the difference in security quality behind the product functional specification of IoT devices. This proposed method has the following three features.

- Frameworks the placement of metrics in the "IoT Device Security Quality Transparency Model," which clarifies the main department in charge of quality control within the IoT vendor during the product lifecycle of IoT devices.
- A method for self-setting and adjustment of metrics inspired by the GQM method, a quality metrics setting method that permeates the field of software quality.
- Covers both the security capabilities of IoT devices as well as the processes to be followed by IoT vendors

Although many guidelines are available for the development of secure software, no practical framework follows the lifecycle of a hardware-oriented product that is easy for device vendors to understand. Then, the author developed the six areas of the Transparency Model of IoT Device Security Quality to ensure the coverage of the entire hardware product lifecycle. Through the literature survey, the author set a draft set of metrics by selecting the popular items pointed out by the literature. And for each of those areas of the model, the draft set of metrics are settled based on the GQM approach. Then,

the draft set of metrics was reviewed by quality and security experts who reflected the findings and had incorporated them into the sample set of metrics.

IoT devices will have various specifications depending on their use cases. For those use cases, there are also various risks to be eliminated and threats to be assumed, so the sample metrics presented here are designed to eliminate perspectives specific to various fields. There will be no one-fits-all metrics able to apply to all IoT devices. The IoT-SQMM proposed in this paper shows the method of developing the confirming points against the goals in the form of questions and setting the way of answering the questions as metrics. Therefore, based on the sample metrics presented here, if more detailed confirmation is necessary, IoT vendors can tailor the questions and metrics to be added. If they have set up a new security goal, they can add questions and metrics for that goal. IoT device security quality metrics are not just a checklist of items to confirm in terms of thought-out security, but rather an evaluation perspective set up to make sure the security quality goals to achieved.

To validate the sample metrics by the proposed method, the metrics analyzed the requirements of various IoT security regulations, guidelines, and certification programs. This validation confirmed the applicability of the metrics to serve as a tool for clarifying the differences and characteristics of the requirements of various IoT security documents. The sample metrics demonstrate the capability to illustrate the difference in the security quality behind the functional specifications of commercial IoT devices in the market. Thus, it is easier for the entity or IoT vendors to self-assess the security quality metrics items necessary for their security goal. The presentation of the metrics for each area as a framework enables IoT vendors to easily incorporate security initiatives into their existing development processes. In examining the adaptability of the proposed method by a large company with an international brand and an IoT startup, both expressed that the method is adaptable. This method has contributed to large companies that validated this set of sample metrics to start adding security quality items to their business unit's product development standards.

The effectiveness evaluation of this approach demonstrated useful in helping IoT vendors to understand how the requirements of the regulation, guidelines, and certification program distribute across the product lifecycle and which phase they focus on. The results of Section 5 reveal that all requirements are not the same and that there are differences in approach to the security requirements. This method may help IoT vendors tailor their IoT device security quality metrics according to the requirements

specified by consumers. If deficiencies are found, IoT vendors can make improvements and save time and effort by eliminating the deficiencies to achieve security quality goals early in the lifecycle of the product under development.

In addition, the author believes that this method will also serve as an indicator of the product security standard for consumers. From the results of Section 6, we also verified that this method could illustrate that there is a clear difference in security quality, which is difficult to indicate the difference in product features in functional specifications. To date, a way to communicate the quality of IoT security has not existed. Nevertheless, the author foresees this novel approach will become a quality communication tool between product vendors and consumers.

In conclusion, the author hopes that the IoT-SQMM will help IoT vendors to incorporate the development and support of secure and reliable IoT devices as part of their conventional quality control.

10 REFERENCES

- [1] Xu, T.; Wendt, J.B.; Potkonjak, M. *Security of IoT Systems: Design Challenges and Opportunities*; IEEE/ACM ICCAD: San Jose, CA, USA, November 2014. <https://doi.org/10.1109/ICCAD.2014.7001385>.
- [2] Oh, S.; Kim, Y-G. *Security requirements analysis for the IoT*; Platcon, 2017, Busan, Korea. DOI: 10.1109/PlatCon.2017.7883727.
- [3] Alaba, F.A.; Othman, M.; Abaker, I.; Hashem, T.; Alotaibi, F. Internet of things security: A survey. *J. Netw. Comput. Appl.*, Jun. 2017, vol. 88, pp. 10-28. DOI: 10.1016/j.jnca.2017.04.002.
- [4] Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and pro-spective measures. 10th ICITST, Dec. 2015, London, UK. DOI: 10.1109/ICITST.2015.7412116.
- [5] Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer*, Jul. 2017, vol. 50, pp. 80-84, DOI: 10.1109/MC.2017.201.
- [6] Krebs, B. Who Makes the IoT Things Under Attack? Krebs on Security, Oct. 3, 2016, Virginia, USA. Available online: <https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/> (accessed on 15 September 2021).
- [7] The Hong Kong Computer Emergency Response Team Coordination Centre (HKCERT) and the Hong Kong Productivity Council (HKPC). Device (Wi-Fi) Security Study. Mar. 2020, Hong Kong, China. Available online: <https://www.hkcert.org/f/blog/263544/95140340-8c09-4c9a-8c32-cedb3eb26056-DLFE-14407.pdf> (accessed on 15 September 2021)
- [8] Baxley, B. *From BLAS to Sweyntooth: Eight Bluetooth Threats to Network Security*; Bastille Networks, San Francisco, CA, USA, Dec. 2020. Available

- online: <https://www.infosecurity-magazine.com/opinions/bluetooth-threats-network/> (accessed on 15 September 2021)
- [9] Vaccari, I.; Cambiaso, E.; Aiello, M. Remotely Exploiting AT Command Attacks on ZigBee Networks. *Secur Commun Netw*, Oct. 2017, vol. 2017, 1723658, pp. 1-9. DOI; 10.1155/2017/1723658.
- [10] Vallois, V.; Guenane, F.; Mehaoua, A. Reference architectures for security-by-design IoT: Comparative study. Fifth Conference on Mobile and Secure Services (*MobiSecServ*), Mar. 2019, Miami Beach, FL, USA. DOI: 10.1109/MOBISECSERV.2019.8686650.
- [11] Cybersecurity: IoT security and privacy – Guidelines, *ISO/IEC DIS 27400*, 2021. Available online: <https://www.iso.org/standard/44373.html> (Accessed on 13 December 2021)
- [12] Ashton K.; That 'Internet of Things' Thing; *RFID J.*, Jun. 2009; Available online: <http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf> (Accessed on 15 September 2021)
- [13] K. K. Patel, S. M. Patel, “Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges,” *IJSEC*, vol. 6, no. 5, May 2016, DOI 10.4010/2016.1482
- [14] *IoT Security Guidelines ver. 1.0*, IoT Acceleration Consortium, Ministry of Internal Affairs and Communications Ministry of Economy, Trade and Industry, Japan, Jul. 2016. Available online: http://www.iotac.jp/wp-content/uploads/2016/01/IoT-Security-Guidelines_ver.1.0.pdf (Accessed on 8 Feb. 2019).
- [15] *ISO/IEC 30141:2018*, Internet of Things (IoT) — Reference Architecture, August 2018. Available online: <https://www.iso.org/standard/65695.html> (accessed on 18 October 2021).
- [16] O. Franberg, A. Kung, “Preparing the ISO/IEC 30141 IoT reference architecture edition 2 through a mindshare,” presented in *IoT Week*, Aarhus, Denmark, Jun. 2019. Available online: <https://iotweek.blob.core.windows.net/slides2019/4.%20THURSDAY%2020/IoT%20Systems%20Architectures%20Models%20Guidelines/20190620%20IoT%20Week%20session%20architecture%20SC41%20OstenFramberg%20-%20AK%20v2.pdf> (Accessed on 15 September 2021).

- [17] *ISO/IEC 30147:2021*, Internet of Things (IoT) - Integration of IoT trustworthiness activities in ISO/IEC/IEEE 15288 system engineering processes, Available online: <https://webstore.iec.ch/publication/62644> (accessed on 7 February 2022)
- [18] Gillies, A. Improving the quality of information security management systems with ISO 27000. *The TQM Journal*, Jun. 2011, vol. 23 no. 4, pp. 367-376. DOI: 10.1108/17542731111139455.
- [19] Baldini, G.; Skarmeta, A.; Fournieret, E.; Neisse, R.; Legeard, B.; Gall, F.L. Security certification and labelling in Internet of Things. *IEEE 3rd World Forum on IoT (WF-IoT)*, Dec. 2016, Reston, VA, USA. DOI: 10.1109/WF-IoT.2016.7845514.
- [20] Costa, D.M.; Eixeira, E.N.; Werner, C.M.L. Software process definition using process lines: A systematic literature review. *XLIV Latin American Computer Conf. (CLEI)*, Oct. 2018, Sao Paulo, Brazil. DOI: 10.1109/CLEI.2018.00022.
- [21] Haufe, K.; Brandis, K.; Colomo-Palacios, R.; Stantchev, V.; Dzombeta, S. A process framework for information security management. *Int. J. Information Syst. Project Management*, Oct. 2016, vol. 4, no. 4, pp. 27-47. DOI: 10.12821/ijispm040402.
- [22] Siddiqui, S.T. Significance of security metrics in secure software development. *Int. J. Appl. Inf. Syst.*, Aug. 2017, vol.12, no. 6, pp. 10-15. DOI: 10.5120/ijais2017451710.
- [23] Pino, F.J.; Garcia, F.; Piattini, M. Software process improvement in small and medium software enterprises: A systematic review. *Software Qual J*, Nov. 2007, vol. 16, pp. 237-261. DOI: 10.1007/s11219-007-9038-z.
- [24] Humphrey, W.S. Defining the Software Process. In *Managing the software process*, 1989, Boston, MA, USA, Addison-Wesley, ch. 13, pp. 247-286, ISBN:978-0-201-18095-4.
- [25] Jones, C. Patterns of large software systems, Failure and success. *Computer*, Mar 1995, vol. 28, no. 3, pp. 86 – 87. DOI: 10.1109/2.366170.
- [26] *ISO/IEC 30141:2018*, Internet of Things (IoT) — Reference Architecture, August 2018.
- [27] Atta, N.; Talamo, C. Digital Transformation in Facility Management (FM). IoT and Big Data for Service Innovation. In *Digital Transformation of the Design, Construction and Management Processes of the Built Environment*, Springer, Dec. 2019, pp. 267-278. DOI: 10.1007/978-3-030-33570-0_24.

- [28] *California Senate Bill No. 327*. Sep. 2018, CA, USA. Available online: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB327 (accessed on 15 September 2021).
- [29] *Oregon House Bill 2395*. July 2019, OR, USA. [Online]. Available: <https://legiscan.com/OR/text/HB2395/id/2025565/Oregon-2019-HB2395-Enrolled.pdf> (accessed on 15 September 2021).
- [30] *Terminal Conformity Regulation of Telecommunications Business Law*, Part 10 of Section 34 (in Japanese). Ministry of Internal Affairs and Communications, Tokyo, Japan. January 2020. Available online: <https://elaws.e-gov.go.jp/document?lawid=360M50001000031> (accessed on 15 September 2021).
- [31] *Baseline security recommendations for IoT*; The European Union Agency for Cybersecurity (ENISA). Nov. 2017. ISBN: 978-92-9204-236-3, DOI: 10.2824/03228.
- [32] *CCMB-2017-04-001*; Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model Ver. 3.1, Rev. 5, The Common Criteria, April 2017, pp. 2. Available online: <https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf> (accessed on 15 September 2021).
- [33] *IEC 62443 - EDSA Certification*; ISASecure. Available online: <https://www.isasecure.org/en-US/Certification/IEC-62443-CSA-Certification> (accessed on 15 September 2021).
- [34] Mendes, N.; Madeira, H.; Duraes, J. *Security benchmarks for web serving systems*. IEEE 25th Int. Symposium on Software Reliability Engineering (ISSRE), Nov. 3-6, 2014, Naples, Italy. DOI: 10.1109/ISSRE.2014.38.
- [35] Oliveira, R.; Raga, M.; Laranjeiro, N.; Vieira, M. An approach for benchmarking the security of web service frameworks. *Future*, Sep. 2020, vol. 110, pp. 833-848. DOI: 10.1016/j.future.2019.10.027.
- [36] Bernsmed, K.; Jaatun, M.G.; Undheim, A. Security in service level agreements for cloud computing. 1st Int. Conf. on Cloud Comput. and Services Science (CLOSER 2011), May 7-9, 2011, Noordwijkerhout, Netherlands. Available online: <https://jaatun.no/papers/2011/CloudSecuritySLA-Closer.pdf> (accessed on 15 September 2021).

- [37]Keoh, S.L.; Kumar, S.S. Securing the Internet of things: A standardization perspective. *IEEE Internet Things J.*, Jun. 2014, vol. 1, no. 3, pp. 265-275. DOI: 10.1109/JIOT.2014.2323395.
- [38]Granjal, J.; Monteiro, E.; Sa Silva, J. Security for the Internet of things: A survey of existing protocols and open research issues. *IEEE Commun. Surveys Tuts.*, Jan. 2015, vol. 7, no. 3, pp. 1294 – 1312. DOI: 10.1109/COMST.2015.2388550.
- [39]Aversano, L.; Bernardi, M.L.; Cimitile, M.; Pecori, R. A systematic review on Deep Learning approaches for IoT security. *Comp. Sci. Rev.*, May 2021, vol. 40, pp. 100389. DOI: 10.1016/j.cosrev.2021.100389
- [40]Ahmad R.; Alsmadi, I. Machine learning approaches to IoT security: A systematic literature review. *Internet Things*, Jun. 2021, vol. 14, pp. 100365. DOI: 10.1016/j.iot.2021.100365.
- [41]Samann, F.E.F.; Zeebaree, S.R.; Askar, S. IoT Provisioning QoS based on Cloud and Fog Computing. *J. Appl. Sci. Technol. Trends*, Mar. 2021, vol. 02, no. 01, pp. 29 – 40. DOI: 10.38094/jastt20190.
- [42]Zikria, Y.B.; Ali, R.; Afzai, M. Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions. *Sensors*, Feb. 2021, vol. 21, no. 4, 1174. DOI: 10.3390/s21041174.
- [43]Fizza, K.; Barnerjee, A.; Mitra, K.; Jayaraman, P.P.; Ranjan, R.; Patel, P.; Georgakopoulos, D. QoE in IoT: a vision, survey and future directions. *Discover Internet Things*, Feb. 2021, vol. 1, no 1, article no. 4. DOI: 10.1007/s43926-021-00006-7.
- [44]*Report on the current status and awareness of security measures among IoT product and service developers*, Information-technology Promotion Agency (IPA), Tokyo, Japan, Mar. 2018. Available online: <https://www.ipa.go.jp/files/000065094.pdf> (accessed on 15 September 2021).
- [45]Wohlin, C. Guidelines for snowballing in systematic literature studies and a replication in software engineering. *Proc. 18th Int. Conf. Evaluation and Assessment in Software Engineering (EASE '14)*, May 2014, Article No. 38, pp. 1-10. DOI: 10.1145/2601248.2601268.
- [46]*Framework for Improving Critical Infrastructure Cybersecurity v1.1*. National Institute of Standards and Technology (NIST). April 2018. DOI: 10.6028/NIST.CSWP.04162018.
- [47]*IoT Security Guidelines for Endpoint Ecosystem, Ver. 2.2*. The GSM Association (GSMA). Feb. 2020. Available online:

- <https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.13-v2.2-GSMA-IoT-Security-Guidelines-for-Endpoint-Ecosystems.pdf> (accessed on 15 September 2021).
- [48] *IoT Product and Service Vulnerability Response Guide* (in Japanese). Information technology Promotion Agency of Japan (IPA), 2018, pp 6. Available online: <https://www.ipa.go.jp/files/000065095.pdf> (Accessed on 15 September 2021)
- [49] *Survey report on the current status and awareness of security measures in IoT product and service developers* (in Japanese). IPA, 2018. Available online: <https://www.ipa.go.jp/files/000065094.pdf> (Accessed on 15 September 2021).
- [50] *NICTER Observation Report 2019* (in Japanese). NICT, 2020. Available online: <https://www.nict.go.jp/press/2020/02/10-1.html> (Accessed on 15 September 2021)
- [51] M. Capellupo, J. Liranzo, M. Z. Alam Bhuiyan, T. Hayajneh, G. Wang; Security and Attack Vector Analysis of IoT Devices, in *the conference proceeding of SpaCCS 2017*, pp 593-606, Guangzhou, China, December 12-15, 2017. DOI: 10.1007/978-3-319-72395-2_54
- [52] Rachit, S. Bhatt, P. R. Ragiri; Security trends in Internet of Things: a survey, *SN Applied Sciences*, Vol 3, Article number: 121, Jan 2021. Available online: https://www.researchgate.net/publication/348429338_Security_trends_in_Internet_of_Things_a_survey
- [53] P. Mueller, B. Yadegari; The Stuxnet Worm, *Teaching*, pp 466-566, 212, The Univ. of Arizona. Available online: <https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/topic9-final/report.pdf> (Accessed on September 15 2021)
- [54] Insecam, Available online: <https://www.insecam.org/> (Accessed on 15 September 2021).
- [55] C. Miller, C. Valasek, Remote Exploitation of an Unaltered Passenger Vehicle, Aug. 2015, Available online: <http://illmatics.com/Remote%20Car%20Hacking.pdf> (Accessed on 15 September 2021).
- [56] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J.A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, Y. Zhou,

- Understanding the Mirai Botnet, in *the Proceedings of the 26th USENIX Security Symposium*, pp 1093-1110, Aug. 2017, Vancouver, BC, Canada, ISBN 978-1-931971-40-9. Available online: <https://www.usenix.org/system/files/conference/usenixsecurity17/sec17-antonakakis.pdf> (Accessed on 15 September 2021).
- [57] L.C. Williams, FDA alerts on pacemaker recall for cyber flaw. *The Business of Federal Technology*, FCW, Aug. 2017. Available online: <https://fcw.com/articles/2017/08/29/fda-pacemaker-cyber-recall.aspx> (Accessed on 15 September 2021).
- [58] *ISO 9000:2015*, Quality management systems — Fundamentals and vocabulary, Sep 2015.
- [59] *ISO 9000:2015(en)* Quality management systems — Fundamentals and vocabulary, ISO Online Browsing Platform, Available online: <https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en> (Accessed on 15 September 2021).
- [60] P.N. Golder, D. Mitra, C. Moorman, What is Quality? An Integrative Framework of Processes and States, *J. Marketing*, 2012, DOI:10.1509/jm.09.0416
- [61] *Law of Food Labeling* (in Japan), Available online: <https://elaws.e-gov.go.jp/document?lawid=425AC0000000070> (Accessed on 15 September 2021).
- [62] *Main reason for food labeling Background* (in Japanese), Food Labeling Division, Consumer Affairs Agency, Dec. 2011, Available online: https://www.caa.go.jp/policies/policy/food_labeling/other/review_meeting_002/pdf/111219sankou-a.pdf
- [63] *Consumer Product Safety Act*, Ministry of Economy, Trade and Industry, Tokyo, Japan, 1973. Available online: <http://www.japaneselawtranslation.go.jp/law/detail/?id=1838&vm=04&re=01>
- [64] *Explanation of Article by Article Product Liability Law* (in Japanese), First Consumer Affairs Division, National Consumer Affairs Bureau, Economic Planning Agency, Shojihomu Kenkyukai, Jan 1995. ISBN-10: 4785706988.
- [65] L. Prates, J. Faustino, M. Silva, R. Pereira, DevSecOps Metrics, SIGSAND/PLAIS 2019, pp 77-90, Aug. 2019. DOI: 10.1007/978-3-030-29608-7_7

- [66] *A Guide to Using Public Data for Quantitative Management* (in Japanese), Software Metrics Advancement Project, Ministry of Economy, Trade and Industry. Mar. 2010. Available online: https://www.meti.go.jp/policy/it_policy/softseibi/metrics/process_metrics.pdf (Accessed on 15 September 2021)
- [67] Y. Miyazaki, Approach to Software Quality Description (in Japanese), Jul. 2014, IPA. Available online: <https://www.ipa.go.jp/files/000040880.pdf> (Accessed on 15 September 2021)
- [68] *ISO/IEC 25010:2011*, Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models, Mar. 2011.
- [69] Y. Miyazaki, Do you think that bugs are the only quality? (in Japanese), IPA, May 2015. Available online: <https://www.ipa.go.jp/files/000045962.pdf>
- [70] *The Tips of Product Planning* (in Japanese). The Union of Japanese Scientists and Engineers, Tokyo, Japan. Available online: <https://www.juse.or.jp/departamental/point02/08.html>
- [71] S. Yamamoto, Reliability Requirements, *Series Requirements Engineering, Business Communication*, vol. 24, NTT Data, Oct. 2006. Available online: <https://www.bcm.co.jp/site/youkyu/youkyu24.html>
- [72] R. Naraine, What is security transparency?; ZDNet, Mar. 2009. Available online: <https://www.zdnet.com/article/what-is-security-transparency/> (Accessed on 15 September 2021).
- [73] *Kaspersky Lab strengthens its commitment to transparency* (in Japanese); Kaspersky, Oct. 2017. Available online: https://www.kaspersky.co.jp/about/press-releases/2017_bus24102017 (Accessed on 15 September 2021).
- [74] *ISO/IEC 27036:2013+*, Information technology — Security techniques — Information security for supplier relationships. Available online: <https://www.iso27001security.com/html/27036.html> (Accessed on 15 September 2021).
- [75] *Guideline for formulating specifications for supply chain risk management on information security in outsourcing* (in Japanese), National center of Incident readiness and Strategy for Cybersecurity (NISC), May 2015. Available online: <https://www.nisc.go.jp/conference/cs/taisaku/ciso/dai02/pdf/02shiryou0303.pdf> (Accessed on 15 September 2021).

- [76]Z. Abbadi, Security Metrics What Can We Measure?; Available online: https://owasp.org/www-pdf-archive/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf (Accessed on 8 Feb. 2019).
- [77]*ISO/IEC 15408-1:2009*; Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model.
- [78]*Common Criteria Services – ISO 15408*, TUV Rheinland. Available online: <https://www.tuv.com/world/en/common-criteria-services-%E2%80%93-iso-15408.html> (Accessed on 15 September 2021).
- [79]*Understanding IEC 62443*, International Electrotechnical Commission, Feb. 2021. Available online: <https://www.iec.ch/blog/understanding-iec-62443> (Accessed on 15 September 2021).
- [80]*IIC IoT Security Maturity Model: Description and Intended Use*, Industrial Internet Consortium, Apr. 2018. IIC:PUB:IN15:V1.0:PB:20180409. Available online: https://www.iiconsortium.org/pdf/SMM_Description_and_Intended_Use_2018-04-09.pdf (Accessed on 15 September 2021).
- [81]*BSIMM*, Available online: <https://www.bsimm.com/> (Accessed on 15 September 2021)
- [82]*ISO/IEC 21827:2008*; Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model (R) (SSE-CMM (R)).
- [83]*IoT Secure Element Protection Profile (IoT-SE-PP) Version 1.0.0*, Secure Communications Alliance, Dec. 2019. Available online: https://www.commoncriteriaportal.org/files/ppfiles/pp0109b_pdf.pdf (Accessed on 15 September 2021)
- [84]*Security Considerations in the System Development Life Cycle*, SP 800-64 Rev. 2, NIST, Oct. 2008. Available online: <https://csrc.nist.gov/publications/detail/sp/800-64/rev-2/archive/2008-10-16> (Accessed on 8 Feb. 2019).
- [85]J. Voas, Network of Things, NIST Special Publication 800-183, NIST, Jul. 2016. DOI:10.6028/NIST.SP.800-183.
- [86]A. Regenscheid, Platform Firmware Resiliency Guidelines, NIST SP800-193, NIST, May 2018, DOI:10.6028/NIST.SP.800-193
- [87]J. Voas, R. Kuhn, P. Laplane, S. Applebaum, Internet of Things (IoT) Trust Concern, NIST Cybersecurity White paper, Oct. 2018. Available online:

- <https://csrc.nist.gov/CSRC/media/Publications/white-paper/2018/10/17/iot-trust-concerns/draft/documents/iot-trust-concerns-draft.pdf> (Accessed on 8 Feb. 2019)
- [88] R. Ross, M. McEvelley, J.C. Oren, System Security Engineering, NIST SP800-160, NIST, Nov. 2016. DOI:10.6028/NIST.SP.800-160.
- [89] *IoT Security & Privacy Trust Framework v2.5*, Online Trust Alliance, Apr. 2019. Available online: https://www.internetsociety.org/wp-content/uploads/2019/04/iot_security-and-privacy-trust-framework-v2.5.pdf (Accessed on 8 Feb. 2019).
- [90] *Strategic Principles for Securing IoT*, U.S. Department of Homeland Security, Nov. 2016. Available online: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf (Accessed on 8 Feb. 2019).
- [91] *Internet of Things Privacy & Security in a Connected World*, U.S. Federal Trade Commission (FTC), Jan. 2015. Available online: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf> (Accessed on 8 Feb. 2019).
- [92] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices*, Food and Drug Administration (FDA), Oct. 2018, FDA-2018-D-3443. Available online: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/content-premarket-submissions-management-cybersecurity-medical-devices> (Accessed on 8 Feb. 2019).
- [93] *Postmarket Management of Cybersecurity in Medical Devices*, FDA, Dec. 2016, FDA-2015-D-5105. Available online: <https://www.fda.gov/regulatory-information/search-fda-guidance-documents/postmarket-management-cybersecurity-medical-devices> (Accessed on 8 Feb. 2019).
- [94] K. Moore, R. Barnes, H. Tschofenig, Best Current Practices for Securing IoT devices, *Internet-Draft*, Jul. 2017. Available online: <https://tools.ietf.org/html/draft-moore-iot-security-bcp-01> (Accessed on 8 Feb. 2019).
- [95] S. Rizvi, J. Pfeffer, A. Kurtz, M. Rizvi, Securing the Internet of Things (IoT): A Security Taxonomy for IoT, in the conference *IEEE TrustCom 2018*, Aug. 2018, New York, USA. DOI 10.1109/TrustCom/BigDataSE.2018.00034.

- [96] *vBSIMM Vendor Analysis*, Synopsys, Aug. 2017. Available online: <https://community.synopsys.com/s/article/vBSIMM-Vendor-Analysis> (Accessed on 8 Feb. 2019).
- [97] J. Heyl, *Overview of UL2900, Medical Device Cybersecurity*, 2017. Available online: <https://cybersecuritysummit.org/wp-content/uploads/2017/10/4.00-Justin-Heyl.pdf> (Accessed on 8 Feb. 2019).
- [98] R.J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd Ed. New York, NY, USA: John Wiley & Sons. 2008. ISBN-13: 978-0470068526.
- [99] *9 ways to improve IoT device security*, Hewlett Packard Enterprise, Jan. 2017. Available online: <https://www.hpe.com/us/en/insights/articles/9-ways-to-make-iot-devices-more-secure-1701.html> (Accessed on 8 Feb. 2019).
- [100] *Managing the Risk of IoT*, ISACA J., vol. 3, pp 19-26, 2017. Available online: <https://www.isaca.org/-/media/files/isacadp/project/isaca/articles/journal/2017/volume-3/journal-volume-3-2017> (Accessed on 8 Feb. 2019).
- [101] *IoT Security and Privacy Recommendations*, A Uniform Agreement Report, A BROADBAND INTERNET TECHNICAL ADVISORY GROUP (BITAG), Nov. 2016. Available online: [https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_\(IoT\)_Security_and_Privacy_Recommendations.pdf](https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf) (Accessed on 8 Feb. 2019).
- [102] *Future-proofing the Connected World: 13 steps to develop secure IoT Products*, IoT Working Group, Cloud Security Alliance (CSA), 2016. Available online: <https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf> (Accessed on 8 Feb. 2019).
- [103] *IoT Security Guidance – Manufacturer*, Open Web Application Security Project (OWASP), Available online: https://www.owasp.org/index.php/IoT_Security_Guidance#Manufacturer_IoT_Security_Guidance (Accessed on 8 Feb. 2019).
- [104] *Code of Practices for consumer IoT security*, Department for Digital, Culture, Media & Sport, United Kingdom, Oct. 2018. Available online: <https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/code-of-practice-for-consumer-iot-security> (Accessed on 8 Feb. 2019).

- [105] *ETSI TS 103 645*, CYBER; Cyber Security for Consumer Internet of Things, ETSI, Feb. 2019. Available online: https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf (Accessed on 8 Feb. 2019).
- [106] *General Framework for Secure IoT Systems*, NISC, Japan, Aug. 2016. Available online: https://www.nisc.go.jp/eng/pdf/iot_framework2016_eng.pdf (Accessed on 8 Feb. 2019).
- [107] *Guide to develop IoT Devices Safe and Secure (High-Reliability Edition)* (in Japanese), SEC Books, IPA, Japan, Jun. 2017. ISBN 978-4-905318-52-1. Available online: <https://www.ipa.go.jp/files/000059278.pdf> (Accessed on 8 Feb. 2019).
- [108] *Guide to secure the Quality of IoT Devices and Systems* (in Japanese), SEC Books, IPA, Jun. 2018. ISBN 978-4-905318-59-0. Available online: <https://www.ipa.go.jp/files/000064877.pdf> (Accessed on 8 Feb. 2019).
- [109] *Certification Program General Requirements 2021*, Connected Consumer Device Security Council, CCDS-GR01-2021, Nov. 2020. Available online: https://www.ccds.or.jp/english/contents/CCDS_SecGuide-IoTCommonReq_2021_v1.0_eng.pdf (Accessed on 15 September 2021).
- [110] *ISO/IEC/IEEE 15288*; Systems and software engineering - System life cycle processes, May 2015.
- [111] *Y.4806*: Security capabilities supporting safety of the Internet of things, ITU-T, Nov. 2017. Available online: <https://www.itu.int/rec/T-REC-Y.4806-201711-I/en> (Accessed on 8 Feb. 2019).
- [112] *TR-0008-v2.0.0 Security, Technical Report*, oneM2M, Aug. 2016. Available online: http://www.onem2m.org/images/files/deliverables/Release2/TR-0008-Security-V2_0_0.pdf (Accessed on 8 Feb. 2019).
- [113] A. Abdulrazig, N. Norwawi, and N. Basir, Security measurement based on GQM to improve application security during requirements stage, *Int. J. Cyber-Security and Digital Forensics (IJCSDF)*, vol. 1, no. 3, pp. 211-220, Jul. 2012, ISSN: 2305-0012, Available online: <http://oaji.net/articles/2014/541-1394063127.pdf> (Accessed on 15 September 2021).
- [114] F. Yahya, R. J. Walters, and G. Wills, Using goal-question-metric (GQM) approach to access security in cloud storage, *Enterprise Security*, LNCS 10131, pp. 223–240, 2017, DOI: 10.1007/978-3-319-54380-2_10.

- [115] D. Dodson, M. Souppaya, and K. Scarfone, Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF), April 2020, DOI: 10.6028/NIST.CSWP.04232020.
- [116] *Security Development Lifecycle* (SDL), Microsoft, 2008. Available online: <https://www.microsoft.com/en-us/securityengineering/sdl/> (Accessed on 15 September 2021).
- [117] *Secure SDLC* (software development life cycle), Synopsys. Available online: <https://www.synopsys.com/blogs/software-security/secure-sdlc/> (Accessed on 15 September 2021).
- [118] *SDLC* (Secure Development Life Cycle) (in Japanese), PwC, Tokyo, Japan, 2019. Available online: <https://www.pwc.com/jp/ja/services/digital-trust/cyber-security-consulting/product-cs/sdlc.html> (Accessed on 15 September 2021).
- [119] *Cybersecurity Strategy* (in Japanese), National center of Incident readiness and Strategy of Cybersecurity (NISC), Japan, September 2015. Available online: <https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf> (Accessed on 15 September 2021).
- [120] V. Basili, C. Caldiera, and D. Rombach, Goal, question, metric paradigm, *Encyclopedia of Software Engineering*, vol. 1, pp. 528-532, Wiley, 1994.
- [121] *Security guidelines for product categories – Automotive on-board devices – Ver. 2.0*, CCDS, Tokyo, Japan, May 2017. Available online: http://ccds.or.jp/english/contents/CCDS_SecGuide-Automotive_On-board_Devices_v2.0_eng.pdf (Accessed on 8 Feb. 2019).
- [122] *IoT security assessment checklist Ver. 3*, the GSM Association (GSMA), Sep. 2018. Available online: <https://www.gsma.com/security/resources/clp-17-gsma-iot-security-assessment-checklist-v3-0/> (Accessed on 8 Feb. 2019).
- [123] *IoT security evaluation and assessment guideline* (in Japanese), CCDS, Tokyo, Japan, June 2017, Available online: http://ccds.or.jp/public/document/other/guidelines/CCDS_IoT%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E8%A9%95%E4%BE%A1%E6%A4%9C%E8%A8%BC%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_rev1.0.pdf (Accessed on 8 Feb. 2019).
- [124] *Consultation on regulatory proposal on consumer IoT security*, Department for Digital, Culture, Media & Sport, UK, 2020. Available online:

- <https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security> (Accessed on 15 September 2021).
- [125] Foundational cybersecurity activities for IoT device manufacturers, NISTIR 8259, NIST, USA, 2020, DOI: 10.6028/NIST.IR.8259.
- [126] *IoT device cybersecurity capability core baseline*, NISTIR 8259A, NIST, USA, 2020, DOI: 10.6028/NIST.IR.8259A.
- [127] *The C2 consensus on IoT device security baseline capabilities*, Council to Secure the Digital Economy, USA, 2019. Available online: https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf (Accessed on 15 September 2021).
- [128] *EN 303 645 V2.1.1*; Cybersecurity for consumer Internet of things: Baseline requirements. ETSI, Sophia Antipolis, France, June 2020. Available online: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (Accessed on 15 September 2021).
- [129] *ioXt 2020 Base Profile Ver. 1.00*, ioXt alliance, USA, April 2020. Available online: https://static1.squarespace.com/static/5c6dbac1f8135a29c7fbb621/t/5ede6a88e6a927219ee86bb2/1591634577949/ioXt_2020_Base_Profile_1.00_C-03-29-01.pdf (Accessed on 15 September 2021).
- [130] UL MCV 1376, Methodology for Marketing Claim Verification: Security Capabilities Verified to level Bronze/Silver/Gold/Platinum/Diamond (IoT security rating), Underwriter Laboratories LLC., Northbrook, IL, USA, June 2019. Available online: <https://www.shopulstandards.com/PurchaseProduct.aspx?UniqueKey=40671> (accessed on 13 December 2021).
- [131] P. Botella, X. Burgues, J. P. Carvallo, and X. Franch, ISO/IEC 9126 in practice: what do we need to know?, in *Proc. 1st Software Measurement European Forum (SMEF)*, Rome, Italy, Jan. 2004, DOI: 10.1.1.295.5269.
- [132] T. Olsson, and P. Runeson, “V-GQM: A feed-back approach to validation of a GQM study, in *7th METRIC*, London, UK, April 2001, DOI: 10.1109/METRIC.2001.915532.
- [133] *Products liability*, Legal Information Institute, Cornell Law School. Available online: https://www.law.cornell.edu/wex/products_liability (Accessed on 15 September 2021).

- [134] G-L. Garner, How the History of Product Liability Insurance Affects Business Today, *IAFNA*, Mar. 2018. Available online: <https://iafna.org/how-the-history-of-product-liability-insurance-affects-business-today/>
- [135] J.S. Marcus, Liability: When Things Go Wrong in an Increasingly Interconnected and Autonomous World: A European View, *IEEE IoT Magazine*, vol. 1, issue 2, pp 4-5, Dec. 2018. DOI: 10.1109/MIOT.2018.8717593.
- [136] Connected Consumer Device Security Council, CCDS. Available online: <http://ccds.or.jp/english/index.html> (Accessed on 15 September 2021).
- [137] Y. Takeuchi, Security Measures in IoT/5G Era, Tron Show, Dec. 2019. Available online: https://www.tronshow.org/2019-tron-symposium/sessions/data/pdf/1211T015_02.pdf (Accessed on 15 September 2021).
- [138] B. Othman, L. Angin, P. Weffers, and Bhargava, Extending the agile development process to develop acceptably secure software, *IEEE Trans. Dependable Secure Comput.*, vol. 11, no. 6, pp. 497-509, Nov-Dec. 2014, DOI: DOI: 10.1109/TDSC.2014.2298011.
- [139] H. Oueslati, M. M. Rahman, and L. B. Othmane, Literature Review of the Challenges of Developing Secure Software Using the Agile Approach, presented at *2015 10th Int. Conf. Availability, Reliability and Security (ARES)*, Toulouse, France, Aug. 2015, DOI: 10.1109/ARES.2015.69.
- [140] H. Yasar, and K. Kontostathis, Where to Integrate Security Practices on DevOps Platform, *Int. J. Secure Softw. Eng.*, vol. 7, no. 4, pp. 39-50, Oct. 2016, DOI: 10.4018/IJSSE.2016100103.
- [141] F. M. Constante, R. Soares, M. Pinto-Albuquerque, D. Mendes, and K. Beckers, Integration of Security Standards in DevOps Pipelines: An Industry Case Study, in *Product-Focused Software Process Improvement (PROFES 2020)*, Turin, Italy, pp. 434-451, DOI: 10.1007/978-3-030-64148-1_27.

11 APPENDICES

APPENDIX 1: RESULT OF A COMPARATIVE STUDY OF THE REQUIREMENTS LISTED IN THE LITERATURE	127
APPENDIX 2: THE DRAFT QUESTIONS AND METRICS FOR THE EXPERT REVIEW	129
APPENDIX 3: CANDIDATES OF OPTIONAL QUESTION AND METRICS.....	132
APPENDIX 4: THE RESULTS OF IoT DEVICE EVALUATION WITH THE PROPOSED METHOD	137
RESEARCH ACHIEVEMENTS	144

APPENDIX 1: RESULT OF A COMPARATIVE STUDY OF THE REQUIREMENTS LISTED IN THE LITERATURE

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37			
		NIST Cybersecurity FW v1.1	NIST SP800-64 v2 Sec Consideration in System DLS	NIST SP800-183 Network of Things	NIST SP800-193 Platform Firmware Resiliency Guidelines	NIST Cybersecurity White paper IoT Trust Concern	NIST SP800-180 System Security Engineering	Online Trust Alliance IoT Security & Privacy Trust Framework v2.5	US DoHS Strategic Principles for Securing IoT	FTC Internet of Things Privacy & Security in a Connected World	FDA Content of Premarket Submissions for Management of Cybersecurity in Medical Devices	FDA Postmarket Management of Cybersecurity in Medical Devices	IETF Best Current Practices for Securing IoT devices	IIC IloT Security FW	IIC IoT Security Maturity Model	BSIMM/ Synopsys	vBSIMM/ Synopsys	UL2900-1 (ANSI compliant)	Security Engineering/ Ross J. Anderson	HP 9 ways to improve IoT device security	ISACA INTERNET OF THINGS: RISK AND VALUE CONSIDERATIONS	BITAG IoT Security and Privacy Recommendations	CSA Future-proofing the Connected World: 13 steps to develop secure IoT	OWASP IoT Security Guidance - Manufacturer	GSMA IoT Security Guidelines for Endpoint Ecosystem	UK Code of Practices for consumer IoT Security ETSI EN303 645	Cybersecurity for Consumer IoT	ENISA Baseline Security Recommendations for IoT	NISC General Framework for Secure IoT Systems	IoT Acceleration Consortium IoT Security Guidelines v1.0	IPA Guide for Safe and Secure IoT Devices and Development (High Reliability)	IPA Guide to Ensuring the Quality of IoT Devices and Systems	CCDS Certification Program General Requirements 2021	ISO/IEC/IEEE 15288 Systems and software engineering -- System life cycle processes	ISO 21827 System Security Engineering - Capability Maturity Model	IEC62443 ISASecure EDSA Certification	ITU-T Y.4806 : Security capabilities supporting safety of the Internet of things	oneM2M TR-0008-v2.0 Security			
Product Security Policy (Documentation)	7	15	14	1	2	8	7	12	12	5	5	7	10	8	26	14	10	11	7	10	5	16	15	10	9	6	6	12	9	14	11	14	5	13	6	7	2	6			
Product Security Development Process Standard (Doc)	12		1					1							1	1		1		1			1					1													
Threat analysis result	23	1	1				1	1		1	1		1	1	1	1		1	1		1			1				1					1						1		
Risk Assessment result	24	1	1				1	1		1	1		1	1	1	1		1	1		1			1				1					1						1		
Corresponding threat selection/countermeasure design	11		1				1				1					1		1					1									1									
Result of the evaluation of the effectiveness of countermeasures Implemented	2						1				1							1					1									1									
Workaround/warning for the threats accepted in the user manuals?	2								1		1																														
Handling the personal data (vital data, action data, etc.)	11							1		1					1					1			1	1	1		1	1	1											1	
Secure-coding Rule(s) to apply	1																									1	1	1												1	
IOS (including library, driver)	6	1				1			1						1	1	1																							1	
IOSS (open source software) utilized	6	1				1			1						1	1	1																								
IProcured 3rd-party components	6	1				1			1						1	1	1																								
In-house coding component	4								1						1	1	1																								
ISecure coding rule conformance test	3																1																								
IStatic analysis	12		1				1					1	1		1			1													1				1					1	
IUnnecessary port scan	14		1				1					1	1		1	1	1	1				1	1	1							1				1						
IKnown vulnerability check , penetration testing	13		1				1		1					1	1	1	1				1	1	1	1							1				1						
IFuzzing (zero day) evaluation	12		1						1						1	1	1	1	1		1	1									1				1						
Applying Security patches to OS/OSS	8		1						1									1				1	1									1									
IEvaluation of acceptance for procured 3rd-party components	6								1							1	1					1	1			1															
Check cloud service level (SLA evaluation)	1																							1																	
nProduct Security Incident Response system (PSIRT)	15	1	1						1			1		1	1					1		1		1						1	1	1		1			1				
Incident response process (documentation)	14	1	1					1				1	1	1	1					1		1		1						1	1	1		1			1				
IVulnerability reporting contact	9	1						1				1		1	1															1	1			1							
IVulnerability disclosure	13	1						1				1	1	1	1					1		1					1	1		1	1	1	1								
Information control, personal information protection law compliance, system to comply with GDPR regulations	6						1			1					1							1	1	1			1	1		1	1	1	1								
IUpdate (repair) function	17	1			1	1			1			1	1		1						1	1			1		1	1	1	1		1			1	1					
IConfiguration scanning function (for automatic update)	3	1													1																										
IEncryption function	19	1				1		1	1				1	1	1			1		1	1	1		1	1	1	1	1	1		1										
ILog recording function	20	1		1		1		1					1	1	1			1	1	1	1	1		1	1	1	1	1	1												
IMalfunction detection	7				1															1			1	1	1				1			1									
IDegenerating function to terminate connectivity because of security maintenance	1																															1									
Easy deleting function of user setting data	7		1					1																			1	1					1		1						
Monitoring the corresponding cloud service level	7							1						1					1																						
nManagement of Customer Information in the services	2																					1																			
nIn-house manufacturing management, line-workers, parts and materials control	0																																								
nODM (manufacturing consignment), line audit	6	1													1							1			1				1							1					
Production with all genuine parts?	6	1													1							1			1				1							1					
nLaws and regulations complied	4									1					1					1						1															
International standard complied	5		1			1									1																								1		
nSecurity Certification granted	5		1			1												1		1																			1		
nSecurity maintenance period, guaranteed range of SLA/disclaimer	2																					1									1										

APPENDIX 2: THE DRAFT QUESTIONS AND METRICS FOR THE EXPERT REVIEW

1) Security by Design			Metrics	supplementary information if exists
	a	Product Security Policy (documented)	○ = Exist, × = No	
	b	Product Security Development Process (documented)	○ = Exist, × = No	
	b-1	Threat Analysis (results)	○ = Exist, × = No	
	b-2	Risk Assessment (results)	○ = Exist, × = No	
	b-3	Selection of threats and design of countermeasures	○ = Exist, × = No	
	b-4	Results of evaluation of effectiveness of countermeasure implemented	○ = Exist, × = No	
	c	Counter measured Threat List	○ = Exist, × = No	
	c-1	Accepted threats	○ = Exist, × = No	
	c-2	Security operation handling manual/warning	○ = Exist, × = No	
	d	Existence and identification of the handling of personal information	○ = Yes, × = No	
	e	Applying secure coding rules	○ = Yes, × = No	If yes, the name of the rule selected
	f	Software configuration list (Bill of Materials)	○ = Exist, × = No	
	f-1	OS (including libraries and drivers)	○ = Exist, × = No	
	f-2	OSS (Open Source Software)	○ = Exist, × = No	
	f-3	Development environment (framework, IDE)	○ = Exist, × = No	
	f-4	External Procurement Components	○ = Exist, × = No	
	f-5	In-house coding components	○ = Exist, × = No	
	f-7	In-house design components (outsourced)	○ = Exist, × = No	
2) Security assurance and evaluation				
	g	Performing a security assessment	○ = Yes, × = No	
	g-1	Secure Coding Rule Conformance Evaluation	◎3rd party test, ○ = Yes, × = No	
	g-2	Static coding analysis	◎3rd party test, ○ = Yes, × = No	

		g-3	Known Vulnerability Check	◎3rd party test, ○ = Yes, × = No	
		g-4	Dynamic testing (unwanted port scanning, penetration test)	◎3rd party test, ○ = Yes, × = No	
		g-5	Fuzzing test (zero-day test)	◎3rd party test, ○ = Yes, × = No	
		g-6	Confirmation of patch applied to OS/OSS	◎3rd party test, ○ = Yes, × = No	
		g-7	Evaluation of acceptance of externally procured components	◎3rd party test, ○ = Yes, × = No	
		g-8	Cloud service level (SLA) verification	○ = Yes, × = No	
		g-9	Blocking UART/JTAG ports	○ = Yes, × = No	
3) Security operations (security response system)					
	h	Information management, personal information protection law, and GDPR regulatory compliance system		○ = Exist, × = No	
	i	Vulnerability Monitoring System (SOC)		○ = Exist, × = No	
	j	Product incident response system (PSIRT)		○ = Exist, × = No	
	j-1	Incident response process (documented)		○ = Exist, × = No	
	j-2	Vulnerability Report Contact		○ = Exist, × = No	
	k	Cloud service level monitoring system		○ = Yes, × = No	
	m	Management of customer information		○ = Yes, × = No	related to item d
	n	Security maintenance function			
	n-1	Update (modification) function		○ = Yes, × = No	on-line (automatic/manual), off-line (w/ USB, PC)
	n-2	Self-configuration scan function (for automatic update)		○ = Yes, × = No	
	n-3	Access control		○ = Yes, × = No	Default setting: unique to the device / common to all
	n-4	Encryption function		○ = Yes, × = No	Supported standards (AES, etc.), protocols (TLS, etc.)
	n-5	Logging function		○ = Yes, × = No	
	n-6	Stop function by security maintenance deadline		○ = Yes, × = No	

		n-7	User personal data deletion function	○ = Yes, × = No	Measures to prevent personal information leakage
4) Secure Production					
	o		In-house manufacturing/entry control, parts inspection and management	○ = Exist, × = No	
	p		ODM (outsourced manufacturing)/line audit	○ = Yes, × = No	country of origin
5) Compliance with security standards and specifications					
	q		Laws and regulations	○ = Yes, × = No	Regulatory name/country
	r		International Standards	○ = Yes, × = No	ISO27001, IEC62443-2- 1, IEC62443-4, etc.
	s		Security Certification Programs	○ = Yes, × = No	Name of standard (CCDS certification, ISMS, EDSA certification, technical conformance standards, etc.)
6) Clarification of contractual (restrictions) matters					
	t		Reference to personal information handling system	○ = Yes, × = No	
	u		SLA Warranty Coverage (Disclaimer)	○ = Exist, × = No	

APPENDIX 3: CANDIDATES OF OPTIONAL QUESTION AND METRICS

Candidates for Area 1-A

Question	sub-Question	Metrics
Does the company recognize the importance of security capacity building?	Does the company have a human resource training program for security?	The company does have a program. = 1 There is no training program. = 0
Does the company recognize the importance of password to protect user data?	Does the company have a PWD policy for sensitive service?	The company does have a policy. = 1 There is no policy about PWD. = 0
Is the company trustworthy?	Does the company conduct periodic audit?	The company conduct the periodic audit. = 1 There is no audit conducted. = 0

Candidates for Area 1-B

Question	sub-Question	Metrics
Is the IoT device designed with the maintainability for keeping the security of the product?	Is maintainability assured?	Aspects of metrics: update function for repairing the vulnerable components, configuration function with authentication, data backup for log, configuration, data stored
	Is the credential recoverable?	There is a function. = 1 There is no function. = 0
	Is the self resource state monitoring available?	There is a function. = 1 There is no function. = 0
Is the IoT device designed with the consideration of secure use during its operation?	Is there ability to configure IoT device access control policies?	There is a function. = 1 There is no function. = 0
	Is there display information configuration?	There is a function. = 1 There is no function. = 0
	Is the operation mode switching function?	There is a function. = 1 There is no function. = 0
	Is the authorization designed as low privilege as possible?	There is a function. = 1 There is no function. = 0
Is the IoT device protecting data?	By means of Input data validation?	There is a countermeasure. = 1 There is no countermeasure. = 0
	is there Secured	There is a countermeasure. = 1

	communication?	There is no countermeasure. = 0
	Is information /data protected?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is data storage encrypted?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is there countermeasure anonymizing the user data?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is the IoT device able to store sensitive data separated from the logs and errors?	There is a function. = 1 There is no function. = 0
	Is there function erasing User data on request?	There is a function. = 1 There is no function. = 0
	Is 3rd party data protection utilized?	There is a function. = 1 There is no function. = 0
Is the IoT device equipped with enhanced authentication capabilities other than ID/PWD?	Is authentication using such as the 2 factor/Multi-factor, and biometrics?	There is an enhanced function. = 1 There is no function. = 0
	No PWD/credentials hard-coding	There is no hard-coded credential. = 1 No checking about code/ there is hard-coded credentials. = 0
	Is the design employs the best practice for key management?	The design takes the best practice. = 1 There is no consideration for key management. = 0
Does the IoT device ensure integrity?	Is an IoT device using a hardware incorporated security with integrity?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is there the hardware root of trust (Hardware Security Module) on an IoT device?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is there secure boot with trust?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is the signing code cryptographically used not to be overwritten the software/firmware?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is the design preventing from physical damage?	The design takes it into the consideration = 1 There is no consideration. = 0
Is there any conditional requirement to install the IoT	Is there any requirement for physical / environmental access control?	There is a requirement for users to protect IoT device physically. = 1 There is no access control to IoT devices. = 0

device?	Is there a requirement of security segmentation of network configuration for risk segmentation?	There is a requirement for users to protect IoT device on-line. = 1 There is no control for network to IoT devices. = 0
Does the IoT device have a design to resist from attacks?	Is there any measure to protect from brute-force?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is there any measure for DDoS-resistance?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is the secure pairing function of Bluetooth implemented?	There is a function. = 1 There is no function. = 0
Is the update function designed securely?	Does the IoT device require the authentication for update operation?	There is a function. = 1 There is no function. = 0
	Is there any measure for the update file inaccessible?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is there any measure for anti-rollback from the current status?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is there any measure for downgrade prevention?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is there any measure for the memory and compiler protection?	There is a countermeasure. = 1 There is no countermeasure. = 0
	Is there manual back-up or override operation for safety critical operation?	There is a function. = 1 There is no function. = 0
	Is there any direct execution of command / script for update?	There is no means of direct command or script for update. = 1 There is a direct command or script for update. = 0
Is the security development management carried out?	Are all protocols and services documented?	All of them are documented. = 2 Some of them are documented. = 1 There is no document retained. = 0
	Is the resource assignment for security sufficient?	Adequate security resources are assigned. = 1 Security resources are not sufficient. = 0
	Is the information shared with the 3rd party secured?	It is securely stored with access control. = 1 There is no access control. = 0

Candidates for Area 2

Question	sub-Question	Metrics
Is the IoT device free from the vulnerabilities?	Is the vulnerability check for the web function conducted?	There are the evaluation results with the date. = 1 There is no result. = 0
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It is not confirmed. = 0
	Is the unnecessary profile of Bluetooth disabled?	There are the evaluation results with the date. = 1 There is no result. = 0
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It is not confirmed. = 0
	Is the IoT device free from the known vulnerability of Bluetooth?	There are the evaluation results with the date. = 1 There is no result. = 0
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It is not confirmed. = 0
	Is the unnecessary class of USB disabled?	There are the evaluation results with the date. = 1 There is no result. = 0
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It is not confirmed. = 0
	Is the unnecessary functions for the IoT device removed?	There are the evaluation results with the date. = 1 There is no result. = 0
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It is not confirmed. = 0

Candidates for Area 3

Question	sub-Question	Metrics
Is the security by default setting at initial / at the factory?	Is all default setting securing the IoT device after installation by users?	It is set securing IoT devices at the factory production line = 1 There is no secure setting process in production phase = 0

Candidates for Area 4

Question	sub-Question	Metrics
Are there communication measures with users established?	Is there an user support site for providing security information?	There is an user support site providing security related information. = 1 There is no medium for user. = 0
	Does the service confirm opt in/out for data collection?	The service site conducts the opt in/out for data collection. = 1 The service site does not conduct it. = 0
	Is the notification sent to the users when the privacy policy changes?	The notice is sending on the event of policy change. = 1 There is no notice sent to the users. = 0
Is the operation securely?	Is the operation managing the sensitive service session under control?	There is a monitoring system to detect abnormal session. = 1 There is no security operation. = 0

Candidates for Area 5

Question	sub-Question	Metrics
Does the product comply with the industrial standards?	Does the product meet the Wi-Fi Alliance Security Std?	After confirming the necessity of certification/conformity certificate, the acquisition result is confirmed. = 1 The need for a certification/conformity certificate has not been confirmed. = 0
		Is proven solution for protocol, cryptography used? It is using the proven cryptography such as FIPS-140 = 2 It is using cryptography with no certification = 1 It is not using cryptography = 0

APPENDIX 4: THE RESULTS OF IOT DEVICE EVALUATION WITH THE PROPOSED METHOD

Area 1-A: Security by Design

(Corp. Policy & Development Process Std)			Product A	Product B
Question	sub-Question	Metrics	0	2
Does the company recognize the importance of handling product security?	Does the company have a product security policy?	It is documented. = 1 There is no policy defined. = 0	0	1
	Is the product security development process defined?	It is documented. = 1 There is no process defined. = 0	0	1

Area 1-B: Security by Design (Security measures, Secure Development)

(Security measures, Secure Development)			Product A	Product B
Question	sub-Question	Metrics	9	14
Is security considered from the planning/design stage?	Is threat analysis performed?	There is an analysis result. = 1 It is not performed, or no result = 0	0	1
	Is risk assessment based on threat analysis performed?	There is an assessment result = 1 It is not performed, or no result = 0	0	1
	Are threats selected for countermeasures based on risk assessment and risk mitigation countermeasure design implemented?	There is a list of threats to be protected. = 1 There is no list of threats to be treated. = 0	0	1
		There is a security countermeasure design document. = 1 There is no countermeasure design. = 0	1	1
	Is the threat excluded from countermeasures clear?	There is a list of accepted threats. = 1 There is no list of accepted threats. = 0	0	0
	Are the methods for reducing threats excluded	There is a document for users. = 1 There is no document. = 0	0	1

	from countermeasures and alerts described in manuals, etc.?			
	Is the handling of personal information taken into consideration?	There is a personal information list to handle. =1 There is no list or care. = 0	0	0
Are secure development methods adopted?	Are secure coding rules applied?	Secure coding rules are applied. = 1 There is no rule applied. = 0	0	0
Are all the software components composing the product listed?	Is the adopted OS clear?	The OS name and version are clear. = 1 It is not clear. = 0	1	1
	Is the adopted open source software clear?	All of the open source software name and version are clear. = 1 Some or none of OSS is clear. = 0	1	1
	Is the adopted outsourced software clear?	Vendor name, component name, version and country of origin of the outsourced software can be confirmed. = 1 It is not clear. = 0	1	1
	Is the self-designed software clear?	The software name and version are confirmed. = 1 It is not clear. = 0	1	1
		Outsourcing vendor, component name and version are confirmed. = 1 It is not clear = 0	1	1
Is there a security maintenance feature for the IoT devices?	Is there software update capability?	The product is capable of updating software. = 2 (automatic), = 1 (manual) There is no update capability. = 0	1	1
	Is there a software configuration self-verification function? (For automatic updates)	There is a function. = 1 There is no function. = 0	0	0
	Is there an access control feature?	There is a function. = 1 There is no function. = 0	1	1
	Is there an encryption	There is a function. = 1 There is no function. = 0	0	0

	feature?			
	Is there a logging function?	There is a function. = 1 There is no function. = 0	0	1
	Is there a deactivation function or a fallback operation function when the security maintenance service ends?	There is a function. = 1 There is no function. = 0	1	1
Is the IoT devices designed with consideration of disposal?	Is there a function to delete user data for disposal?	There is a function. = 1 There is no function. = 0	0	0

Area 2: Security Assurance Assessment

			Product A	Product B
Question	sub-Question	Metrics	0	3
Is the product evaluated to ensure it is secure as designed?	Does the source code violate secure coding rules?	There are assessment results that comply with the rules. = 1 There is no result. = 0	0	0
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0	0	0
		The name of the evaluator is verified. = 1 It is not confirmed. = 0	0	0
	Has static analysis of the source code confirmed that there are no vulnerabilities in the source code?	There are the results of the static analysis. = 1 There is no result. = 0	0	1
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0	0	1
		The name of the evaluator is verified. = 1 It is not confirmed. = 0	0	1
	Has the software no known vulnerabilities?	There are the evaluation results with the date. = 1 There is no result. = 0	0	0
		Assessment tool name and version are confirmed. = 1	0	0

	Those are not confirmed. = 0		
	The name of the evaluator is verified. = 1 It is not confirmed. = 0	0	0
Have the latest security patches applied on the OS/OSS been confirmed?	There is a confirmation result. = 1 It is not confirmed. = 0	0	0
	The version of the applied patch is confirmed. = 1 There is no confirmation. = 0	0	0
	The name of the evaluator is verified. = 1 It is not confirmed. = 0	0	0
Has the implementation of preventive measures for HW analysis been confirmed?	There is confirmation of the blockade of JTA, UART, etc.. = 1 There is no confirmation. = 0	0	0
Are unnecessary communication ports being open and is it verified that the open ports are not vulnerable?	There are the evaluation results with the date. = 1 There is no result. = 0	0	0
	Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0	0	0
	The name of the evaluator is verified. = 1 It is not confirmed. = 0	0	0
Is it verified that there are no zero-day vulnerabilities? (Has a fuzzing assessment been performed?)	There are the evaluation results with the date. = 1 There is no result. = 0	0	0
	Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0	0	0
	The name of the evaluator is verified. = 1 It is not confirmed. = 0	0	0
Have the security features and vulnerabilities of the outsourced software been evaluated? (Has the acceptance assessment been conducted?)	There are the evaluation results with the date. = 1 There is no result. = 0	0	0
	Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0	0	0
	The name of the evaluator is verified. = 1 It is not confirmed. = 0	0	0

	Has the security service level of the cloud services been verified?	There is a contract (SLA clause) in place and confirmed. = 1 There is no confirmation. = 0	0	0
--	---	---	---	---

Area 3: Security Production

			Product A	Product B
Question	sub-Question	Metrics	2	7
Is the product produced in a secure manufacturing process?	Is the identity of the line manager verified for in-house production?	All employees are identified. = 1 Not all of the person in the factory are identified. = 0	1	1
		There is a record of the access control to the production site. = 1 There is no record of access control. = 0	0	1
	Has the ODM producer's manufacturing process been verified?	Company name and country of production are confirmed. = 1 It is hard to confirm who manufactures. = 0	1	1
		The results of the production process audit are confirmed. = 1 There is no confirmation. = 0	0	1
	Is production under control to be produced with genuine parts?	Certificates of authorized parts are verified. = 1 There is no confirmation, = 0	0	0
	Is the production process capable of setting each device with unique IDs and passwords?	It is capable of setting unique IDs and passwords to each device. = 1 It is not capable. = 0	0	1
Is there security measure in place for the production system?	Is it possible to detect cyber-attacks such as malware infiltration, virus infections and others on production systems?	It is capable of attack detection. = 1 It is not capable. = 0	0	0
	Are security measures in place for production systems?	Security measures to the production system are in place. = 1 There is no security countermeasure on the production system. = 0	0	1

	Is coordination in place with CSIRT for incident response?	CSIRT is cooperating for factory incident. = 1 There is no incident response readiness. = 0	0	1
--	--	--	---	---

Area 4: Security Operation

			Product A	Product B
Question	sub-Question	Metrics	1	2
Is there a product security response team for the products in the market?	Is there an operating system to monitor vulnerability information for products?	SOC (security operation system) is in place. = 1 There is no system to monitor vulnerability. = 0	0	0
	Is there a incident response system for products?	PSIRT (product security incident response team) is in place. = 1 There is no response system. = 0	0	0
	Is the incident response process defined?	The incident response process is documented. = 1 There is no process defined. = 0	0	0
	Is there a contact point for receiving vulnerability information?	The contact information is publicly available. = 1 There is no contact information. = 0	0	0
Is there a personal information handling policy and management system in place?		There are a policy and a management system. = 1 There is no policy and management system. = 0	1	1
Is there a system for the stable operation of IoT devices?	Is there a system monitoring the operational status of the cloud services which IoT devices works with?	The cloud operator's contact information is clarified. = 1 There is no means to check the cloud operation. = 0	0	0
		It is capable of checking the status of cloud operation. = 1 It is not capable of checking the cloud operation. = 0	0	0
	Is it capable of managing customer	It is capable of managing customer information	0	0

	information for service in use?	based on the management rules documented. = 1 It is not capable. = 0		
Are restrictions on product security support clearly stated?	Is the warranty period and exemption for security service /maintenance provided?	Security service/maintenance that the company provide is clarified. = 1 It is not clarified. = 0	0	1

Area 5: Compliance with Law, Regulation, and International Standard

			Product A	Product B
Question	sub-Question	Metrics	1	4
Does the product comply with the laws and regulations about the product security of the region to be sold?	Does the product meet legal and regulatory requirements?	There are the evaluation results that meet the requirements. = 1 There is no evaluation result. = 0	1	1
	Does the product have the required certifications or conformity statements, if necessary?	After confirming the necessity of certification/conformity certificate, the acquisition result is confirmed. = 1 The need for a certification/conformity certificate has not been confirmed. = 0	0	1
Does the product comply with the required international standards?	Does the product have the required certifications or conformity statements, if necessary?	After confirming the necessity of certification/conformity certificate, the acquisition result is confirmed. = 1 The need for a certification/conformity certificate has not been confirmed. = 0	0	1
Does the product comply with private security certification?	Has the product acquired the certification of conformity with the standard that is decided to be required or voluntarily acquired?	After confirming the necessity or voluntary acquiring of certification/conformity certificate, the acquisition result can be confirmed. = 1 The need for a certification/conformity certificate has not been decided. = 0	0	1

RESEARCH ACHIEVEMENTS

Journals with Peer Review

Name of Journal: IoT (ISSN 2624-831X)

Publisher: Multidisciplinary Digital Publishing Institute (MDPI AG)

Published at: *IoT* 2021, 2(4), 761-785; <https://doi.org/10.3390/iot2040038>

Published Date: 15 December 2021

Title: IoT Security-Quality-Metrics Method and its Conformity with Emerging Guidelines

Author(s): Kosuke Ito, Shuji Morisaki, Atsuhiko Goto

International Conferences with Peer Review

Name of Conference: ISA Asia-Pacific Singapore 2019

Organizer(s): The International Studies Association

Conference Date: 4 – 6 July 2019

Presentation Date and Session: 4 July 2019 at TC08: Cybersecurity

Title: A Study Toward Quality Metrics for IoT Device Cybersecurity Capability

Author(s): Kosuke Ito, Shuji Morisaki, Atsuhiko Goto

Other Achievements

- Publication

- 機関誌「行政&情報システム」

- 出版元：（一社）行政情報システム研究所
 - 発行： 2018年12月号
 - タイトル：サイバーセキュリティの技術展望 ～セキュアなIoT社会に向けた取り組み～
 - 筆者： 伊藤公祐，後藤厚宏

- 主な内容：サイバーフィジカル融合の IoT 社会の脅威とリスクの拡がり，IoT 社会のセキュリティ対策，組織すべてによるセキュリティ総対応体制時代へ，セキュリティ対応の原則

○ 単行本：「企業リスクを避ける押さえておくべき IoT セキュリティ～脅威・規制・技術を読み解く！～」

- 出版元： 株式会社 インプレス
- 発行： 2018 年 12 月 14 日
- 筆者： 荻野 司，伊藤公祐，小野寺 正（編集：重要生活機器連携セキュリティ協議会）
- 主な内容： IoT セキュリティに関する最新の脅威トピックや事例、米国、EU、日本の政策動向の紹介、多様な IoT 機器を活用したサービスにおけるセキュリティの考え方やポイントを解説。

○ 機関誌：「クオリティ・クラブ」

- 連載：「情報セキュリティと品質」シリーズ（全 6 回）
- 出版元： 一般財団法人 日本科学技術連盟
- 筆者： 伊藤公祐
- 発行・タイトル：
- No.13 2019 年 3-4 月号「第 1 回 IoT に対する脅威事例と攻撃者とは」
 - 主な内容：情報セキュリティとは，IoT に対する脅威事例，攻撃者とは
- No.14 2019 年 5-6 月号「第 2 回 攻撃者が狙う脆弱性と想定されるリスク」

- 主な内容：脆弱性とは，脆弱性のタイプ，リスクの想定
- No.15 2019 年 7-8 月号「第 3 回 セキュリティ対応の基本的な考え方とプライバシー」
 - 主な内容：3つの特性 C, I, A, セキュリティ対応の基本的な手順，プライバシーとは
- No. 16 2019 年 9-10 月号「第 4 回 IoT セキュリティの特徴と安全性との関係」
 - 主な内容：IoT システムの特徴，IoT セキュリティの特徴，セキュリティによる安全性への影響
- No.17 2019 年 11-12 月号「第 5 回 IoT セキュリティに関する訴訟事例と法規制の動向」
 - 主な内容：IoT セキュリティに関する訴訟事例，IoT セキュリティの法規制の動向
- No.18 2020 年 1-2 月号「セキュリティを品質の要素に」
 - 主な内容：品質とは，セキュリティの特異点，IoT 機器の品質にセキュリティ
- Other Presentations
 - 出版物「IoT クライシスーサイバー攻撃があなたの暮らしを破壊する」
 - 著者/出版元：NHK スペシャル取材班
 - 発売日： 2018 年 7 月 25 日
 - 取材協力： 伊藤公祐、他 CCDS 関係者
 - 主な内容： 2017 年 11 月に放送された NHK スペシャル「あなたの家電が狙われている～インターネットの新たな脅威～」

○ カンファレンス「ソフトウェア品質シンポジウム 2018 (SQiP2018)」

- 主催者： 一般財団法人 日本科学技術連盟
- 開催日時： 2018 年 9 月 12 日（水）13:00～17:00
- タイトル： 併設チュートリアル「セキュリティ入門、品質としてのセキュリティ ～品質活動にセキュリティを取り込むには～」
- 講師： 伊藤公祐（情報セキュリティ大学院大学 客員研究員）
- 主な内容： 情報セキュリティ基礎（脅威事例，攻撃者とは，狙われる脆弱性，想定されるリスク），IoT セキュリティの特徴，プライバシー，セキュア開発ライフサイクル、セキュリティにまつわる法制度等

○ セミナー「ET&IoT Technology2018 CCDS IoT セキュリティセミナー」

- 主催者： 一般社団法人 組込みシステム技術協会
- 開催日時： 2018 年 11 月 16 日（金）10:30～13:00
- タイトル： 「IoT セキュリティ海外動向～規制の行方～」
- 講師： 伊藤公祐
- 主な内容： 2016 年 IoT セキュリティ関連のガイドラインラッシュから国際標準策定への動き、そして欧米日各国で施行が予定される IoT 機器を対象とする法規制の状況や業界ごとの動向を解説

○ カンファレンス「IoT Security Guideline & Certification Experience Exchange between JP & TW IoT Security in Smart Manufacturing」

- 主催者： 台湾工業技術研究院（ITRI）、Cloud Computing & IoT Association in Taiwan (CIAT)
- 開催日時： 2019 年 5 月 28 日（火）14:00-18:00

- タイトル： 「Introduction of CCDS Activities toward The Smart world with Safety and Security」
- 講師： 伊藤公祐（CCDS サーフイケーション WG 主査）
- 主な内容： CCDS の取り組み紹介、日本における IoT セキュリティに関するガイドライン策定の状況、法規制の状況、CCDS 認証マーク制度を紹介。

○ セミナー「IoT セキュリティシンポジウム 2019 by CCDS」

- 主催者： 一般社団法人 重要生活機器連携セキュリティ協議会
- 開催日時： 2019 年 6 月 17 日（金）13:00-18:00
- タイトル： 「CCDS サーフイケーションプログラムアップデート」
- 講師： 伊藤公祐（CCDS サーフイケーション WG 主査）
- 主な内容： CCDS サーフイケーションプログラム内容、分野共通要件の最新状況の紹介。

○ セミナー「JNSA IoT セキュリティセミナー」

- 主催者： 特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
- 開催日時： 2019 年 12 月 20 日（金）13:00-18:00
- タイトル： 「IoT セキュリティの国際動向～法規制やサーフイケーションはどうなる？～」
- 講師： 伊藤公祐（CCDS サーフイケーション WG 主査）

- 主な内容： IoT セキュリティガイドラインから法規制への歴史と近年の各国で示され始めた IoT セキュリティ要件の状況、および CCDS サーチフィケーションの 2020 年要件を検討するにあたり、参考になっている海外のベースライン要件を紹介。

○ セミナー「IPA ICSCoE 受講生向けセミナー」

- 主催者： 独立行政法人 情報処理推進機構（IPA）
- 開催日時： 2019 年 12 月 26 日（木）17:00-19:00
- タイトル： 「IoT 機器全般のセキュリティ向上に向けて」
- 講師： 伊藤公祐
- 主な内容： IPA 産業サイバーセキュリティセンター (ICSCoE) にて実施している人材育成プログラム受講生に対し、CCDS の取組み、日本における IoT セキュリティガイドライン類の系譜、PSIRT 活動の紹介。

EOF