IoT

MDPI

Article

IoT Security-Quality-Metrics Method and Its Conformity with Emerging Guidelines

Kosuke Ito [1,*], Shuji Morisaki [2] and Atsuhiro Goto [1]

[1] Institute of Information Security, Yokohama 221-0835, Japan; goto@iisec.ac.jp
[2] Graduate School of Informatics, Nagoya University, Nagoya 464-8601, Japan; s.morisaki.jp@ieee.org
* Correspondence: k-ito@iisec.ac.jp

Abstract: This study proposes a security-quality-metrics method tailored for the Internet of things (IoT) and evaluates conformity of the proposed approach with pertinent cybersecurity regulations and guidelines for IoT. Cybersecurity incidents involving IoT devices have recently come to light; consequently, IoT security correspondence has become a necessity. The ISO 25000 series is used for software; however, the concept of security as a quality factor has not been applied to IoT devices. Because software vulnerabilities were not the device vendors' responsibility as product liability, most vendors did not consider the security capability of IoT devices as part of their quality control. Furthermore, an appropriate IoT security-quality metric for vendors does not exist; instead, vendors have to set their security standards, which lack consistency and are difficult to justify by themselves. To address this problem, the authors propose a universal method for specifying IoT security-quality metrics on a globally accepted scale, inspired by the goal/question/metric (GQM) method. The method enables vendors to verify their products to conform to the requirements of existing baselines and certification programs and to help vendors to tailor their quality requirements to meet the given security requirements. The IoT users would also be able to use these metrics to verify the security quality of IoT devices.

Keywords: Internet of Things; information security; quality management; security management; software metrics

Citation: Ito, K.; Morisaki, S.; Goto, A. IoT Security-Quality-Metrics Method and Its Conformity with Emerging Guidelines. *IoT* **2021**, *2*, 761–785. https://doi.org/10.3390/iot2040038

Academic Editor: Francesco Bergadano

Received: 19 October 2021
Accepted: 11 December 2021
Published: 15 December 2021

1. Introduction

Security becomes more important with the proliferation of Internet of Things (IoT) devices. In fact, many security breaches on IoT devices have already been reported, hence the increased need for IoT security [1–4]. Such breaches involve, for example, the "Mirai" malware and its subspecies spreading across cyberspace targeting IoT devices, including IP/web/network cameras, digital video recorders, home routers, smart speakers, and network printers [5,6].

Researchers of IoT security have made significant progress in mitigating security threats and vulnerabilities, such as remote attacks via wireless connectivity such as Wi-Fi, Bluetooth, or Zigbee [7–9], and securing an architecture to meet security requirements [4,10]. However, because these functions and mitigation technologies are not self-developed by IoT vendors in most cases, but are externally procured components, IoT vendors are required to assess the security quality of the communication components they adopt. Having said that, in reality, IoT security researchers have not yet clarified standard initiatives that IoT vendors easily adopt to ensure the development of secured IoT devices.

Unlike legislation on safety and environmental issues, laws, regulations, and international standards for IoT security have not been established yet. ISO 27400 (guidelines on IoT security and privacy) [11] is still under development.

Many developers and researchers have duly addressed information security issues via ISO 27001 [12] or have discussed a new cybersecurity certification method [13]. Although ISO 27001 outlines the management and protection of information assets [14,15],

security-quality management for the development of IoT products is necessary throughout the product lifecycle and needs to be defined, as is the case with secure software development [16].

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

Pino et al. explained that the software development process is a critical factor for delivering quality software systems [17]. This implies that the quality of the software is influenced by the quality of the development process. This strategy is equivalent to those being implemented in other branches of engineering and industries [18]. Jones reported that most successful projects utilize similar patterns of planning, estimation, and quality-control technologies [19].

A similar paradigm must be followed for IoT devices controlled by the software. As described in ISO 30141:2018, the Internet of Things (IoT)—Reference Architecture [20,21], IoT devices are in an important position to connect cyberspace with the real physical space. Consequently, when IoT devices are exposed to attacks, both cyberspace and real physical space face security risks.

Security measures have been implemented for devices for information systems since security issues have been pointed out for years. In contrast, IoT devices, for which there have been few indications of security issues, have spread across the market with few defenses against security risks in cyberspace. In addition, electronics vendors, which have no experience with IoT security risks, have been developing IoT devices without awareness of security risks. For attackers, it is easy to target IoT devices through the wireless communication route such as Wi-Fi or Bluetooth, or the firmware update function. The IoT devices are easily available, and the weaknesses are easier to find, as compared with the information system devices protected. Thus, ensuring the quality in security of IoT products is important and requires a clear standardized development process for IoT vendors. Moreover, the processes must be defined for implementation throughout the product lifecycle and need to be understood by the IoT consumers.

The IoT security-quality transparency model with six areas of the product lifecycle is devised for developing and supporting secure IoT products. Additionally, the IoT security-quality metrics are compiled for each area using the GQM approach, by referencing the requirements of various IoT security regulations and guidelines, and the opinions of security experts.

A primary contribution of the proposed method is for IoT vendors to understand the characteristics of the requirements of IoT security regulations and guidelines. Additionally, the validity of the proposed metrics against the publicly released IoT security requirements from the market and regulations can also be verified.

Thus, we consider this paper to contribute to the improvement of the situation in which many IoT vendors are unable to consider security as a quality requirement and incorporate it into specific secure product development processes simply by presenting the ideas in the guidelines.

The remainder of this paper is organized as follows: Section 2 summarizes the background and necessity of this research by describing no prior work of IoT security from the quality perspective. Section 3 outlines the authors' previous work on IoT security quality. Section 4 describes the authors' proposed universal method for IoT security-quality metrics and items that the IoT vendors will be able to design. In Section 5, the authors apply the proposed method to the requirements of emerging IoT security regulations and guidelines and confirm the possibility of evaluating the validity of the proposed metrics. Section 6 demonstrates the sample evaluation results of applying the proposed method to IoT devices. Finally, Section 7 discusses the results of this study, Section 8 provides the future directions, and Section 9 summarizes the conclusion.

2. Background and Necessity for This Study

From the discussion above, the issues with regard to IoT security can be categorized into the following two questions.

2.1. Question 1: Does Any Existing Literature or Standard Covering Cybersecurity-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.

To assess the cybersecurity of systems, researchers have developed methods such as the Evaluation Assurance Level with Common Criteria certification based on ISO 15408 [22] and EDSA (Embedded Device Security Assurance) certification based on IEC 62443 [23]. However, these certifications are extremely professional: ISO 15408 focuses on quality assurance and does not specify what initiatives to take, whereas IEC 62443 is specific to critical infrastructure in the industrial control system, which generally does not apply to IoT. Furthermore, both approaches do not present a simple way of describing the quality of cybersecurity in IoT products (for vendors and/or general consumers with no knowledge of security).

Although benchmarks and assessment methods for information security have been proposed [24,25], both fall short from a web-specific and a lifecycle perspective when utilized for product security in IoT.

A template to consistently describe the service level of a cloud service has also been proposed [26]; it is, however, specific to cloud services rather than IoT.

Similarly, the importance of IoT security has been pointed out [14]; however, the article only mentions the certification scheme and does not cover the entire lifecycle, service, or system. IoT security has also been previously discussed [27,28]; unfortunately, the discussions are limited to the security of communication protocols.

The majority of the 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) [29,30], or with the cloud [31], and the user's quality of experience (QoE) [32,33] in 2021. Our extensive literature search failed to produce any literature concerned with benchmarks or suggestions for secure development for IoT vendors.

Thus, no simple, standard way of describing the status of cybersecurity readiness from the perspective of product security in terms of the quality of IoT devices was found.

2.2. Question 2: Does Any Reason for Visualizing the Cybersecurity Control Measures Exist?

Most electronic-device 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 noncompliance, 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; moreover, over 70% of them have no concrete standards for their security responses in product development [34]. 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 know 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. Therefore, the confirmation of 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, it is necessary to define actions to be carried out at each phase of the product lifecycle. Thus, it would not be possible to develop a secure IoT

product unless the relevant processes and practices are clearly defined in the corresponding development process.

In this regard, this paper is a continuation of our previous study [35] in which we reviewed the relevant literature and clarified prospective items in the development of the security-quality metrics discussed herein.

We 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. We attempted to derive quality metrics for IoT devices based on the literature and perspectives reviewed in our previous work. We referenced the goal/question/metric (GQM) methodology commonly used in the quality field.

The following section is an overview of the previous study [35].

3. Past Research on IoT Security Quality

This section summarizes our previous study conducted, in which we reviewed the relevant literature and clarified prospective items that could be used in the development of the security-quality metrics. We conducted the works in Steps 1 and 2 using the research method described in Figure 1; the results of the research on developing prospective items are discussed in our paper [36].

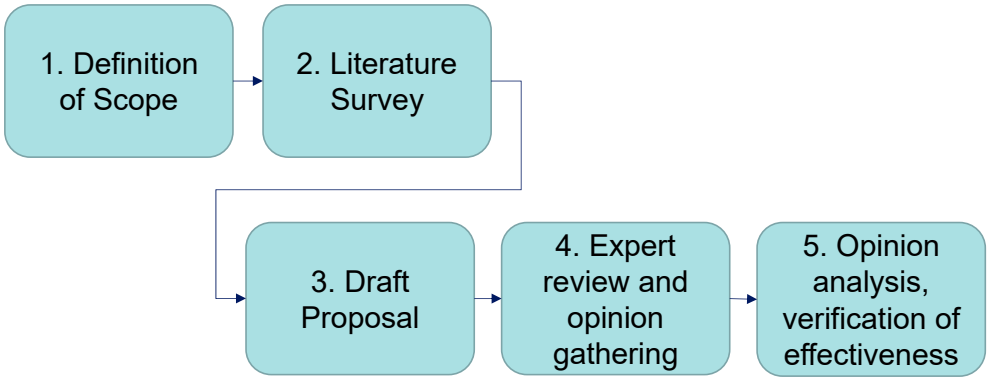

Figure 1. Research method.

3.1. Research Method

We conducted a systematic literature review [36] using a combination of keywords such as "IoT", "security", and "quality metrics" to find related work. The systematic literature review, with respect to the Wohlin guidelines, was conducted in three steps: (1) Planning the literature review; (2) Conducting the review; and (3) Reporting the review.

In addition, the survey methodology adopted by The European Union Agency for Cybersecurity (ENISA) was adopted as the reference model [37]. This research method starts with a literature survey. The proposal then follows and is succeeded by proof of the effectiveness of the proposal, as shown in Figure 1.

Many security guidelines are formulated on the basis of similar sequences: screening the literature in the relevant fields, selecting items that fulfill 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 [37] includes items from the National Institute of Standards and Technology (NIST) Cybersecurity Framework v1.1 [38] and the GSMA IoT Security Guidelines [39]. 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, we defined the scope, as illustrated in Step 1 in Figure 1 of the research method. An IoT system is complex and comprises many IoT devices and cloud services. Therefore, to simplify the discussion, we focused on IoT devices that are primarily intended for consumer usage. The cybersecurity of cloud services is handled in the ICT (software) industry; there is no such culture as far as hardware is concerned. Historically, most electronic-device vendors are familiar with the physical or electrical safety aspects of quality, but few have ever connected a device to the Internet, a cyberspace fraught with malicious attacks. Consequently, the cybersecurity of IoT devices requires urgent attention.

3.3. Results of Literature Review (Step 2)

As mentioned earlier, we conducted a systematic literature review, as described Step2 in Figure 1, to screen for other researchers with similar research interests. However, we could not find any studies or standards from the systematic review.

The International Standard for Software Quality (SQuaRE, ISO/IEC 25000 series) places "security" (one of the subcategories of functionality) as a quality category for system software. SQuaRE lists "security" as a major nonfunctional requirement in terms of system safety. 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 clearly elaborated.

In the security evaluation based on GQM, Abdulrazig et al. [40] 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. [41] discussed the security assessment of cloud storage. Thus, it is worthwhile to define IoT security-quality metrics based on GQM that IoT vendors could use.

In this study, 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 Security-Quality Metrics

Our literature review found no specific work on IoT quality from a security perspective. Therefore, before discussing IoT security-quality metrics, in Step 3 in Figure 1, it is necessary to define the IoT security quality.

4.1. Definition of IoT Security

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 performance 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 that all of the predefined development and production processes conform to the required standards; thus, an assessment of the performance of samples alone is sufficient. Essentially, the collective quality should comprise both process and product quality.

Thus, the quality of cybersecurity of an IoT device may be defined as a combination of the quality of the product-development process and that of the cybersecurity performance of the product.

To outline the security development process, items indicating how to design, build, and support the product should be listed. These items include the results of the process review and the maintenance program based on the development lifecycle. Further, to outline the cybersecurity performance of the product, the results of the security assessment should be listed. To demonstrate IoT cybersecurity performance (mostly in software), the said items should reflect the static and/or dynamic security testing of IoT devices.

4.2. Requirements of IoT Security Quality

Before defining the aforementioned items, it is necessary to clarify the goals and the aspects to screen for.

First, the items must describe the development process in security transparently (for instance, 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 should be listed. Importantly, the items should include those responding to market needs as well as those complying with international standards and guidelines.

A crucial source of consumer feedback is aftersales support. The security support program should partly comprise product cybersecurity quality. Activities such as security monitoring, receiving vulnerability feedback, and rolling out updates should be listed as items.

Furthermore, items should be easily comprehensible from the consumer's perspective; this is important for gaining the user's trust.

Thus, the requirements of IoT security quality are summarized in Table 1.

Table 1. Requirements of IoT 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 cybersecurity capability properly	Quality of product cybersecurity performance
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's trust	-

4.3. Transparency Model of IoT Security Quality

To comprehensively identify items of IoT security quality, we defined a transparency model of IoT security quality that describes the nature of items as presented in Figure 2—prior to Step 3—by integrating the definition of IoT security quality and its requirements. This definition of IoT security quality would satisfy the requirement R1, which ensures transparency of the entire product development process.

This model provides a framework for the IoT security-quality metrics. The model is derived by mapping the security development lifecycle, which was released by many organizations such as NIST [42], Microsoft [43], Synopsys [44], and PwC [45], 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 product development will know which security-quality metrics they should be responsible for.

When considering IoT 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 efficient to implement in the future as new requirements emerge.

The "transparent" model for IoT security quality is as follows:

1. The "security by design" area comprises two parts, namely, the process quality and corresponding product quality [46]. Those in charge of product 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 product security incident response team (PSIRT) 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.

Based on this model, perspectives that should be regarded as the state of IoT security—frequently alluded to in the literature survey—are listed.

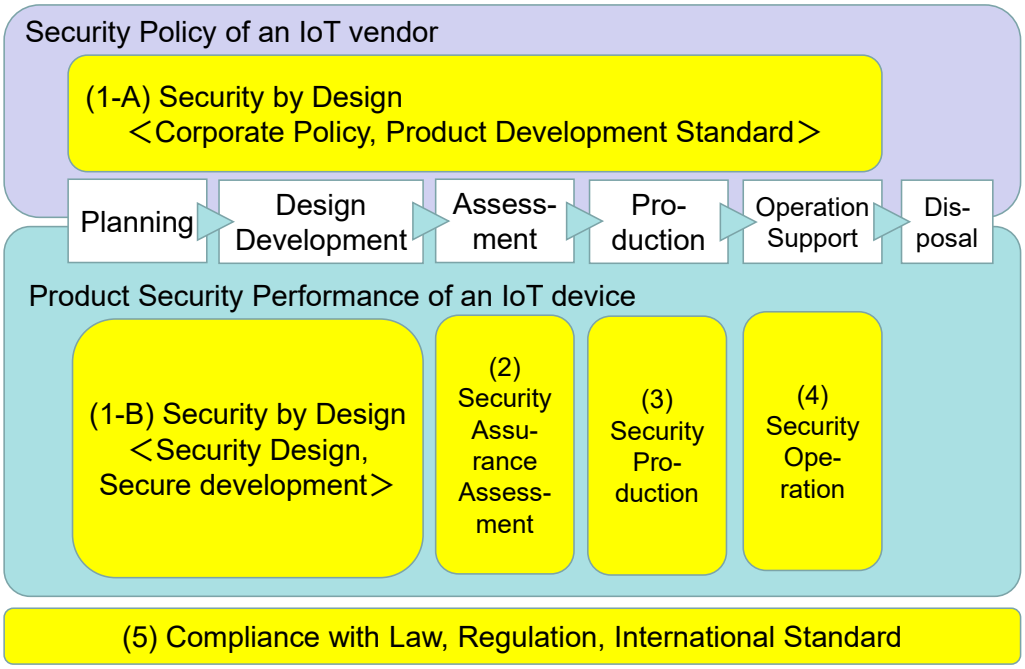

Figure 2. Transparency model of IoT security quality.

4.4. Draft Proposal Development of Security-Quality Metrics

Based on the transparency model (Figure 2), IoT security-quality metrics items were examined, and a draft proposal was subsequently developed (Step 3 in the research method).

4.4.1. Software Quality

Because the functionality and security are controlled by software, perspectives of the software quality were referenced [42–45].

Software-quality control has traditionally been a challenge because an established method for assessing software quality did not exist. Previously, 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.

4.4.2. GQM Method

The GQM paradigm [47] is a three-tier measurement framework and modeling method in software engineering; the first, second, and third tiers represent the goal, question, and metric, respectively.

Metrics are constructed with reference to the "GQM" method in terms of what to achieve (goal), what to evaluate to achieve the goal (question), and what to use as the evaluation method (metric).

4.4.3. Setting Goals for Each Area

Based on the IoT security-quality requirements discussed in Section 4.2, the goals for each area of the transparency model were set, as listed in Table 2.

Table 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 lifecycle.
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 lifecycle.
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.

We set high-level goals for each area/phase. Furthermore, we excluded product-specific indicators from the goals because these would vary for each product and industry.

The Security by Design area under Area 1 is subdivided into two main areas. 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 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 in accordance with the basic 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.

Area 3 is a perspective specific to 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 such actions 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 procured externally and assembled manually. Thus, during production, after verifying the

security of the product, supplementary actions are taken to finalize the product prior to shipping to the market. There are security risks involved in this process, and the goal is to eliminate or reduce those risks in this area. Each of G1B, G2, G3-1, and G3-2 correspond to the requirement of R2.

The objective of Area 4 is to provide a unique security response that is different from traditional quality assurance. Traditional 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 are 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 nonconventional 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; they are required as industry standards to comply. Although this objective should 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. G5 corresponds to the requirements 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 on the aspects of “What do you want to know about IoT security quality?” and “How do you want to make sure?”.

From the perspective of IoT consumers, the questions are intended to reveal what security measures are being taken and how secure the products being made are.

From the perspective of the IoT vendors, identifying what to do and when to do it in the development process is necessary.

The metrics were devised with the following points in mind:

(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 makes it easy to understand. 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 used 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 documentation and whether assessments were performed.

The reason for a simple evaluation is that a clear basis or objective indicator to classify the content of each response does not exist. When the organization is sufficiently mature to implement advanced initiatives, these questions and metrics sets are likely to evolve

into an advanced form of evaluation by establishing complex questions and metrics with approximately three levels, such as well done, partially done, and nothing done.

The 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 details of the approach to set the IoT security-quality metrics and the results of the examination of the questions and metrics for each area are presented in Appendix A. However, 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. 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.

5. Evaluation of Various IoT Security Guidelines with the Sample Metrics

In this section, the characteristics of the requirements presented in IoT security regulations, guidelines, and certification programs are examined. This examination is based on the common security-quality metrics for IoT products reviewed by the quality and security experts as a part of Step 5 in the research method to examine the effectiveness of the metrics. The results are presented in the form of bar charts, respectively. Table A7 in Appendix B shows the source of references examined for evaluating the effectiveness of the IoT security-quality metrics of this study.

5.1. Regulations

The following four regulations are compared with the IoT security-quality metrics: Terminal Conformity Regulation under Telecommunications Business Law by Ministry of Internal Affairs and Communications of Japan [48], California Senate Bill No. 327 [49], Oregon House Bill 2395 [50], and the consultation on regulatory proposals on consumer IoT security of the UK [51].

Figure 3 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 that correspond with the IoT security-quality metrics items and the total number of IoT security-quality metrics items in each area. The number on the horizontal axis is the total number of metrics set for each area. Thus, the percentage for each area is the ratio of the number of metrics matched to the total number of metrics. The same is the case for Figures 4 and 5, shown below.

The requirements of these regulations are minimal, as can be observed in Figure 3. It is also clear that Area 1-A of vendor attitude (such as security policy) or Area 3 of assessment (such as vulnerability assessment) are not required. Therefore, the IoT security-quality metrics cover the range of regulatory requirements sufficiently well to ensure compliance.

As observed in Figure 3, all these regulations focus on Area 1-B and Area 3. The UK regulation requires a security operation after product sales.

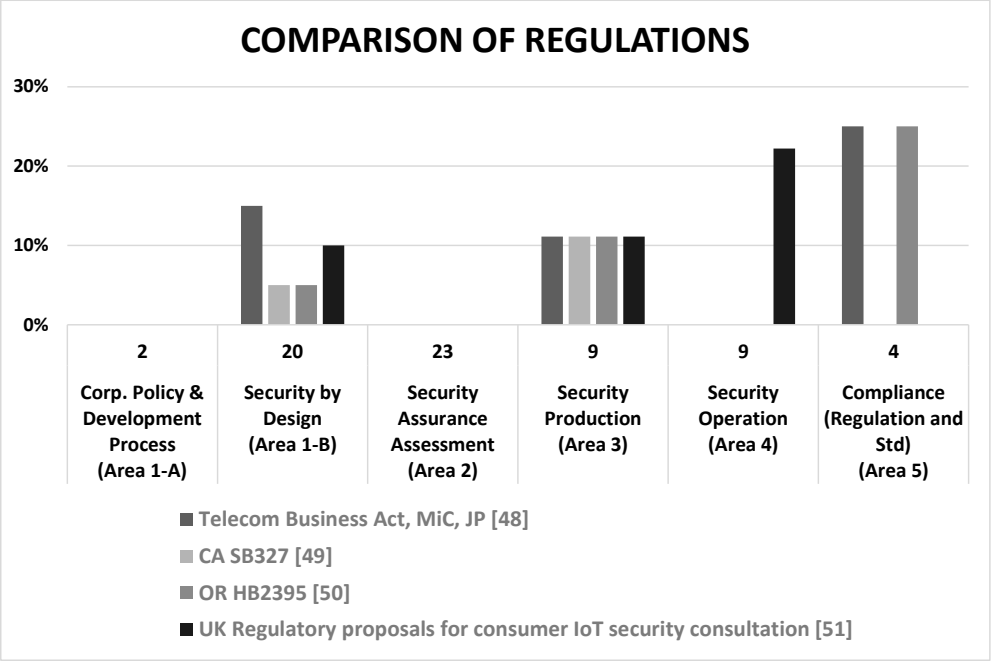

Figure 3. Bar chart of requirements distribution of IoT security regulations.

5.2. 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 [52] and 8259A [53] and C2 Consensus on IoT Device Security Baseline Capabilities [54] of the US, and Baseline by ENISA [37] and ETSI EN 303 645: Cyber Security for Consumer Internet of Things: Baseline Requirements [55].

Figure 4 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 Figure 3. Values over 100% indicate that there are a greater number of requirements than the total number of IoT 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.

The approaches taken by the two European guidelines differ from that of the "baseline". The ENISA baseline offers broad coverage, and many requirements appeared in all areas. In particular, the security function requirements in the area of security-by-design are very extensive, and hence incomparable to the sample metrics. On the other hand, the distribution of ETSI requirements resembles that of the two from the US, and the approach to baselines is also considered close.

5.3. Certifications

Several private IoT security certification programs have been released in the market. We examined the following four sets of requirements. The first is from the certification program of CCDS [56] in Japan, and the second is from the ioXt alliance [57] in the US. Finally, we analyzed the two different grades (Bronze and Diamond) of the IoT Security Rating of UL [58], also in the US.

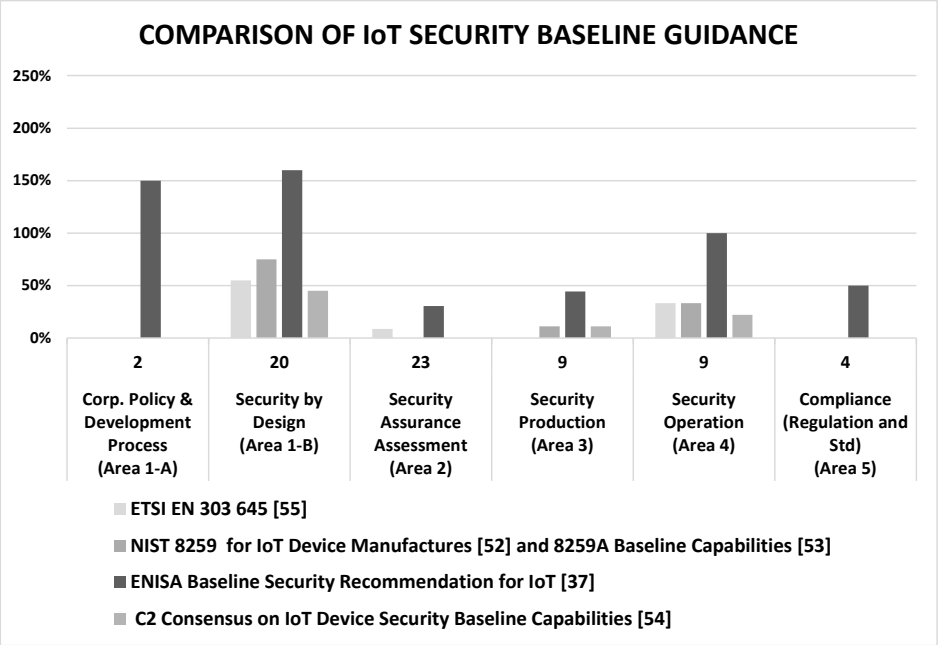

Figure 4. Bar chart of requirements distribution of IoT security baseline guidance.

The result for the area of the transparency model to which each certification requirement belongs is described in Figure 5. The vertical scale represents similar concepts as those in Figures 3 and 4, and the meaning of the values that are greater 100% is also the same.

Except for the requirements of UL Diamond, the other programs have a similar number of requirements, and these are covered (i.e., they are below the 100% line) by the metrics.

We also found that the requirements in the security functions of Area 1-B of UL Diamond are quite strict compared to the same level of ENISA baseline requirements. This implies that the ENISA baseline requirements are a very high-level set of requirements, despite being baselines.

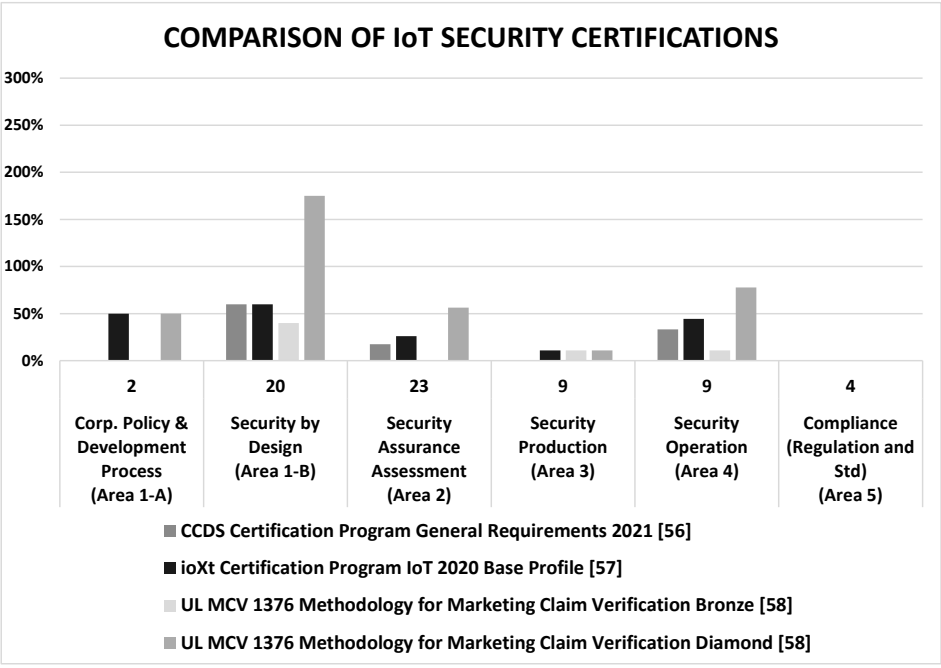

Figure 5. Bar chart of requirements distribution of IoT security certifications.

6. Evaluation of IoT Devices with the Proposed Method

We evaluated the IoT devices by the proposed method. We selected two commercial dashcam recorders (Product A and B) with almost the same functional product specifications as IoT devices. These are products provided by Original Design Manufacturing (ODM) vendors.

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.
- GPS location recording.
- Wi-Fi (wireless) connectivity with a smartphone.
- 16 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 dashcam.

As mentioned above, the two dashcams 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, as they are almost the same in terms of functionality, most users will choose Product A because of the price difference, unless they prefer the design of Product B 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

As far as we were able to confirm through interviews with ODMs, we evaluated and compared the security perspective with the metrics of the proposed method.

The results of the evaluation are shown in Figure 6.

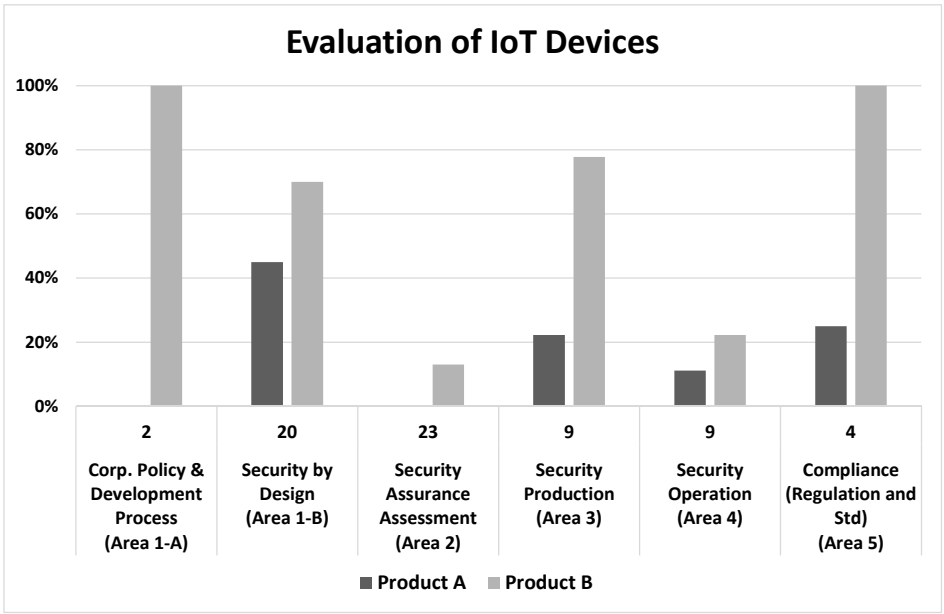

Figure 6. The evaluation results of IoT devices.

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.

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 postshipment support.

6.3. Evaluation Result

The proposed method demonstrated that it could illustrate the differences in the security quality of IoT devices. In addition, it could increase the transparency of the security quality of IoT devices.

It is not easy for general users at present 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.

7. Discussion of Findings

As described in Section 3, the IoT 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 industry, and the metrics that were reviewed by quality and security experts are produced.

Originally, this methodology was designed to help IoT vendors to produce their own IoT security-quality metrics. However, it has also proved to be a useful tool for developing categories of guidelines and certification programs to understand which requirements are lacking or missing from the product lifecycle. In practice, international standards by themselves are insufficient for practical implementation; hence, it is necessary to tailor the contents of international standards to suit the development target, development process, organization, and environment. As discussed previously [59], GQM is used for this tailoring. In the future, as IoT vendors' product security efforts advance, improvements will be required; the validating GQM (V-GQM) is proposed as a method for reviewing or improving each element of GQM [60]. The review or improvement should occur as soon as the values of the metrics are collected. The use of such a method is expected to make it easier to implement 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 on 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.

This approach was also useful in helping IoT vendors to understand how regulatory requirements, guidelines, and certification program requirements are distributed across the product lifecycle and where they are focused. The results of Section 5 reveal that not all sets of requirements are the same and that there are differences in requirements. This may help IoT vendors tailor their IoT security-quality metrics according to the particular

requirements specified by consumers. If any deficiencies are found, IoT vendors can make improvements by eliminating them from the quality metrics to meet the security-quality objectives early in the lifecycle of the product being developed, thereby saving time and effort.

In addition, we believe 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 in the difference in product features in functional specifications. To date, a way to communicate the quality of IoT security has not existed. Nevertheless, we foresee that this novel approach will become a quality communication tool between product vendors and consumers.

A limitation of the proposed method is that it is conceived from a framework that assumes a conventional V-shaped development model. Therefore, we have not been able to evaluate its applicability to recent development methods such as an agile development [61,62] and DevOps [63,64].

8. Future Directions

There are three related areas that we would like to pursue in future work. The first possibility is to categorize the metrics that show the countermeasure capabilities of IoT products and those that demonstrate the efforts of IoT vendors. The current metrics belong to either or both of these areas. We plan to examine how to categorize metrics to easily distinguish between the quality of security in IoT products 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 authors selected the bar chart for this purpose; however, comparatively simple methods for visualizing the coverage may be available. Thirdly, although we believe that IoT vendors can adopt this proposed method because of their knowledge of the product manufacturing culture of electronic-device vendors, we also consider it necessary to ask several IoT vendors to adopt this method to verify whether their IoT products are developed securely. In addition, when security support by IoT vendors becomes common practice, and security threats are evolving day by day, we will need to add and refine the basic set of metrics in detail and would need to consider its refinement cycle in the future.

9. Conclusions

This study proposes a method for tailoring security-quality metrics for IoT devices to ensure the quality of IoT security, 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. In addition, the proposed method demonstrates its capability to reveal the difference of security quality behind the product functional specification of IoT devices.

The authors developed the six areas of the transparency model of IoT security quality to outline the entire product lifecycle with reference to the GQM methodology. The draft was reviewed by quality and security experts who reflected upon the findings and incorporated them into the final set of metrics.

To validate the metrics, they were analyzed against the requirements of various IoT security regulations, guidelines, and certification programs. Most of the regulations, guidelines, and certification programs only describe what needs to be actioned 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. Thus, it is easier for the entity or IoT vendors to self-assess the security-quality metrics items needed for their security goal.

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. The presentation of the metrics for each area as a framework enables IoT vendors to easily incorporate security initiatives into their existing processes.

The proposed method and the metric for IoT security quality were examined and found to be useful for (1) developing categories of guidelines and a set of requirements to review the balance of items throughout the product lifecycle, (2) enabling IoT vendors to determine the focal areas of guidelines and a set of requirements to meet, and (3) enabling consumers to use these IoT product security-quality metrics to communicate the security risks to the product vendors.

Author Contributions: Conceptualization, K.I., methodology, K.I. and S.M.; validation, K.I.; writing—original draft preparation, K.I.; writing—review and editing, S.M. and A.G.; visualization, K.I.; supervision, A.G.; project administration, A.G.; funding acquisition, A.G. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by JST CREST Grant Number JPMJCR1503, Japan.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: The authors would like to thank Miwako Yamaguchi, President Office of IISEC.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Appendix A

The process of how the IoT security-quality metrics were set and the results of the examination of questions and metrics for each area are described.

Appendix A.1 Area 1: Security by Design

To satisfy the goals of Area 1, we consider what to clarify, and how to clarify it. Area 1 covers the product lifecycle from policy to development.

To achieve the goal of Area 1-A in Table 2, the questions for Area 1-A were set as basics to assess whether the IoT vendors consider security support important [38,65].

We set two secondary questions to make the question more specific. The first inquired whether there is a policy in place stating that the management's commitment to security response is considered important. Because security responses require monetary investments, many guidelines recommend that security responses should be publicly stated as a management policy. The other question 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 as opposed to an ill-conceived security response. The questions and metrics for Area 1-A are listed in Table A1.

Table A1. Questions and metrics for Area 1-A.

Question	Sub-Question	Metrics
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
	Is the product-security-development process defined?	It is documented. = 1 There is no process defined. = 0

Neither the quality experts nor the security experts raised any specific objections for these two questions and metrics. The quality experts stated that the same was true for clarifying the product security response as well, because it was important for the management to present the policy to make it an enterprise-wide effort in promoting product safety response.

In Area 1-B, the questions and sub-questions were set up to check whether the basic actions to be performed in the security development process were included [39,66,67].

The questions and metrics are set up to check which security response items should be performed at the appropriate timing. With respect to these items, it should be clear what to do, when to do it, and under what conditions.

For example, if engineers design a security countermeasure without conducting a threat analysis, they end up having to perform threat analysis to justify the developed countermeasure in terms of need and priority, which results in unnecessary work. A set of questions relates to the threats that IoT products may face and the risks that may arise from those threats. As a basic security response, it is necessary to recognize what threats exist to the target to be protected and the risks that may arise from those threats. In many cases, IoT device vendors consider that they implement security measures by setting IDs and passwords without recognizing these threats. It is then necessary to check whether appropriate security measures are selected to eliminate the threats that cause risks that should not occur. It is also important to identify the list of threats not to take into account, as it is impossible to prevent all threats within the limited development time and cost. In addition, the policy and protection measures for the acquisition and use of personal information, which is of great interest to the general public, are also important aspects. The questions and evaluation criteria included clarifying the software configuration of the IoT product in preparation for postlaunch security monitoring.

Neither the quality nor the security experts expressed any specific objection to these questions and metrics. However, the 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 questions and metrics for Area 1-B are listed in Table A2.

Table A2. Questions and metrics for Area 1-B.

Question	Sub-Question	Metrics
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
	Is risk assessment based on threat analysis performed?	There is an assessment result. = 1 It is not performed, or no result. = 0
	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
		There is a security countermeasure design document. = 1 There is no countermeasure design. = 0
	Is the threat excluded from countermeasures clear?	There is a list of accepted threats. = 1 There is no list of accepted threats. = 0
	Are the methods for reducing threats excluded from countermeasures and alerts described in manuals, etc.?	There is a document for users. = 1 There is no document. = 0
	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
Are secure development methods adopted?	Are secure coding rules applied?	Secure coding rules are applied. = 1 There is no rule applied. = 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
	Is the adopted open-source software clear?	All of the open-source software names and versions are clear. = 1 Some or none of OSS is clear. = 0

Table A2. *Cont.*

Question	Sub-Question	Metrics
	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
	Is the self-designed software clear?	The software name and version are confirmed. = 1 It is not clear. = 0
		Outsourcing vendor, component name, and version are confirmed. = 1 It is not clear = 0
Is there a security maintenance feature for the IoT product?	Is there software update capability?	The product is capable of updating software. = 2 (automatic), = 1 (manual) There is no update capability. = 0
	Is there a software configuration self-verification function? (For automatic updates)	There is a function. = 1 There is no function. = 0
	Is there an access control feature?	There is a function. = 1 There is no function. = 0
	Is there an encryption feature?	There is a function. = 1 There is no function. = 0
	Is there a logging function?	There is a function. = 1 There is no function. = 0
	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
Is the IoT product 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

Appendix A.2 Area 2: Security Assurance Assessment

In this area, the questions and sub-questions were set to ensure that the development process was implemented properly. For example, the questions sought to establish whether the software on the IoT devices was free of vulnerabilities, whether communication ports and connectors that are not normally used for development had been removed, whether software developed outside the company had been inspected prior to acceptance, and to determine the security level of cloud services with which the IoT products are connected [68,69].

One security expert pointed out that recent attack methods tended to find vulnerabilities through hardware analysis; the JTAG and UART, which are connection ports left on boards by vendors for flaw analysis, are commonly targeted. Therefore, it is important to verify that these ports are eliminated during production. Even the 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.

The questions and metrics for Area 2 are listed in Table A3. As in Area 1-A, because various evaluation methods are available, the methods suited to individual IoT products are different. Therefore, it is not meaningful to include specific methods in the question list until a common understanding in the industry is fostered.

Table A3. Questions and metrics for Area 2.

Question	Sub-Question	Metrics
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
		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
	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
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It cannot be confirmed. = 0
	Has the software no known vulnerabilities?	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 cannot be confirmed. = 0
	Have the latest security patches applied on the OS/OSS been confirmed?	There is a confirmation result. = 1 It is not confirmed. = 0
		The version of the applied patch is confirmed. = 1 There is no confirmation. = 0
		The name of the evaluator is verified. = 1 It cannot be confirmed. = 0
	Has the implementation of preventive measures for HW analysis been confirmed?	There is confirmation of the blockade of JTAG, UART, etc. = 1 There is no confirmation. = 0
	Are unnecessary communication ports 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
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It cannot be confirmed. = 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
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It cannot be confirmed. = 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
		Assessment tool name and version are confirmed. = 1 Those are not confirmed. = 0
		The name of the evaluator is verified. = 1 It cannot be confirmed. = 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

Appendix A.3 Area 3: Security Production

Area 3 is part of the production-process check that is specific to IoT products. The peculiarity of this part of the IoT production process is that the responsibility for this part exists not with the development or quality assurance department, but with the factory. There is no appropriate reference found regarding this aspect.

Even if it is confirmed that the IoT product has been developed into a secure product through Area 1-B and Area 2, it will not ultimately become a secure product unless proper production controls are established during the production phase. For example, if you were to set different passwords for individual IoT devices but accidentally ship them with the same password, even if only one of the devices is attacked, the other devices will still be affected; but the attack on the other devices can be prevented. Therefore, even if the product is designed to be secure, it will not be produced as a secure product unless proper controls are applied.

In addition, factory production systems have been under attack recently. In many cases, the systems that manage and control production lines were attacked and forced to shut down the lines. 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, and therefore the questions and metrics on the factory system management are unique. However, consumers' trust in the vendors of IoT products would certainly increase if the products are produced in factories that are safe from cyberattacks.

There was no specific objection or concern raised by either the quality or security experts against the questions and metrics. The questions and metrics for Area 3 are listed in Table A4.

Table A4. Questions and metrics for Area 3.

Question	Sub-Question	Metrics
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
		There is a record of the access control to the production site. = 1 There is no record of access control. = 0
	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
		The results of the production process audit are confirmed. = 1 There is no confirmation. = 0
	Is production under control to be produced with genuine parts?	Certificates of authorized parts are verified. = 1 There is no confirmation, = 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
Is there security measure in place for the production system?	Is it possible to detect cyberattacks such as malware infiltration, virus infections and others on production systems?	It is capable of attack detection. = 1 It is not capable. = 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
	Is coordination in place with CSIRT for incident response?	CSIRT is cooperating for factory incident. = 1 There is no incident response readiness. = 0

Appendix A.4 Area 4: Security Operation

The questions and metrics pertaining to Areas 1–3 relate to confirmation of the effort involved before launching IoT products into the market. On the other hand, those of Area 4 relate to the postmarketing stage. These questions and metrics are intended to ensure that a system is in place to provide security support for the IoT products 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 products, 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 carry out when security support ends. The confirmation of the implementation of functions that enable the security support required for IoT products was also included in this area.

In response to the draft questions and metrics, one security expert pointed out the following issue. When a security issue is uncovered, a thorough investigation into what happened needs to be conducted. Logging is an important part of the investigation, and the need to maintain a log of connections and an activity history was pointed out. There was also a suggestion that the IoT devices themselves need to be able to self-verify the need for software updates; this functionality was added to the pertinent items. The questions and metrics for Area 4 are listed in Table A5.

Table A5. Questions and metrics for Area 4.

Question	Sub-Question	Metrics
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
	Is there an incident response system for products?	PSIRT (product security incident response team) is in place. = 1 There is no response system. = 0
	Is the incident response process defined?	The incident response process is documented. = 1 There is no process defined. = 0
	Is there a contact point for receiving vulnerability information?	The contact information is publicly available. = 1 There is no contact information. = 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
Is there a system for the stable operation of IoT products?	Is there a system monitoring the operational status of the cloud services which IoT products works with?	The cloud operator's contact information is clarified. = 1 There is no means to check the cloud operation. = 0
		It is capable of checking the status of cloud operation. = 1 It is not capable of checking the cloud operation. = 0
	Is it capable of managing customer information for service in use?	It is capable of managing customer information 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

Appendix A.5 Area 5: Law Regulation and International Standard

Area 5 essentially needs to be considered at the product planning stage, as discussed in the goals section. However, according to the literature review, it emerged that the regulations and/or guidelines that need to be complied with may relate to the entire lifecycle of the product. Therefore, Area 5 is set as a separate area.

Depending on the industry sector and destination of the IoT product, the laws and regulations that need to be addressed and the international standards and guidelines that need to be ratified are different; hence, they need to be checked carefully. In particular, laws, regulations, and guidelines for IoT security are still evolving and changing in terms of their content. Thus, it is necessary to stay updated to ensure compliance.

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. The questions and metrics for Area 5 are listed in Table A6.

Table A6. Questions and metrics for Area 5.

Question	Sub-Question	Metrics
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
	Does the product have the required certifications or conformity statements, if necessary?	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
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 can be confirmed. = 1 The need for a certification/conformity certificate has not been confirmed. = 0
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

Appendix B

The sources of references examined for evaluating the effectiveness of the IoT security-quality metrics of this study are shown in Table A7.

Table A7. Sources of references examined.

Name of Source	Doc Type	Year	Country	Issued by	Org Type
Telecom Business Act [48]	Law/Regulation	2020	Japan	Ministry of Internal Affairs and Communications	Government
State Bill 327 [49]	Law/Regulation	2020	USA	State of California	Government
House Bill 2395 [50]	Law/Regulation	2020	USA	State of Oregon	Government
Consumer IoT Security Consultation [51]	Law/Regulation	2020	UK	Department for Digital, Culture, Media & Sport	Government

Table A7. *Cont.*

Name of Source	Doc Type	Year	Country	Issued by	Org Type
EN 303 645 v2.1 [55]	Baseline Standard	2020	EU	European Communications Standards Institute (ETSI)	SDO
NISTIR 8259 [52], 8259A [53]	Baseline Standard	2020	USA	National Institute of Standards and Technology (NIST)	SDO
Baseline Security Recommendations for IoT [37]	Baseline Standard	2017	EU	ENISA (European Union Agency for Cybersecurity)	Government
The C2 Consensus on IoT Device Security Baseline Capabilities [54]	Baseline Standard	2019	USA	Council to Secure the Digital Economy (CSDE)	Industry
IoT Common Security Requirements Guidelines 2021 [56]	Certification	2020	Japan	Consumer Connected Device Security Council (CCDS)	Industry
ioXt 2020 Base Profile ver.1.0 [57]	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 [58]	Certification	2019	USA	UL LLC	Industry

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. [CrossRef]
2. Oh, S.; Kim, Y.-G. *Security Requirements Analysis for the IoT*; Platcon: Busan, Korea, 2017. [CrossRef]
3. Alaba, F.A.; Othman, M.; Abaker, I.; Hashem, T.; Alotaibi, F. Internet of Things security: A survey. *J. Netw. Comput. Appl.* **2017**, *88*, 10–28. [CrossRef]
4. Mahmoud, R.; Yousuf, T.; Aloul, F.; Zualkernan, I. Internet of things (IoT) security: Current status, challenges and prospective measures. In Proceedings of the 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 14–16 December 2015. [CrossRef]
5. Kolias, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and Other Botnets. *Computer* **2017**, *50*, 80–84. [CrossRef]
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 BIAS to Sweyntooth: Eight Bluetooth Threats to Network Security*; Bastille Networks: San Francisco, CA, USA, December 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.* **2017**, *2017*, 1723658. [CrossRef]
10. Vallois, V.; Guenane, F.; Mehaoua, A. Reference Architectures for Security-by-Design IoT: Comparative Study. In Proceedings of the 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2–3 March 2019. [CrossRef]
11. ISO/IEC DIS 27400. *Cybersecurity: IoT Security and Privacy—Guidelines*; ISO: Geneva, Switzerland, 2021; Available online: https://www.iso.org/standard/44373.html (accessed on 13 December 2021).
12. Gillies, A. Improving the quality of information security management systems with ISO 27000. *TQM J.* **2011**, *23*, 367–376. [CrossRef]
13. Baldini, G.; Skarmeta, A.; Fourneret, E.; Neisse, R.; Legeard, B.; Gall, F.L. Security certification and labelling in Internet of Things. In Proceedings of the 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), Reston, VA, USA, 12–14 December 2016. [CrossRef]
14. Costa, D.M.; Eixeira, E.N.; Werner, C.M.L. Software Process Definition using Process Lines: A Systematic Literature Review. In Proceedings of the XLIV Latin American Computer Conference (CLEI), Sao Paulo, Brazil, 1–5 October 2018. [CrossRef]
15. Haufe, K.; Brandis, K.; Colomo-Palacios, R.; Stantchev, V.; Dzombeta, S. A process framework for information security management. *Int. J. Inf. Syst. Proj. Manag.* **2016**, *4*, 27–47. [CrossRef]
16. Siddiqui, S.T. Significance of Security Metrics in Secure Software Development. *Int. J. Appl. Inf. Syst.* **2017**, *12*, 10–15. [CrossRef]
17. Pino, F.J.; García, F.; Piattini, M. Software process improvement in small and medium software enterprises: A systematic review. *Softw. Qual. J.* **2008**, *16*, 237–261. [CrossRef]
18. Humphrey, W.S. *Managing the Software Process*; Addison-Wesley: Boston, MA, USA, 1989; pp. 247–286. ISBN 978-0-201-18095-4.

19. Jones, C. Patterns of large software systems, Failure and success. *Computer* **1995**, *28*, 86–87. [CrossRef]
20. ISO/IEC 30141. *Internet of Things (IoT)—Reference Architecture*; ISO: Geneva, Switzerland, 2018; Available online: https://www.iso.org/standard/65695.html (accessed on 18 October 2021).
21. 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*; Research for Development; Springer: Berlin, Germany, December 2019; pp. 267–278. [CrossRef]
22. 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; p. 2. Available online: https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf (accessed on 15 September 2021).
23. ISASecure. IEC 62443—EDSA Certification. Available online: https://www.isasecure.org/en-US/Certification/IEC-62443-EDSA-Certification-(In-Japanese) (accessed on 15 September 2021). (In Japanese).
24. Mendes, N.; Madeira, H.; Durães, J. Security Benchmarks for Web Serving Systems. In Proceedings of the 2014 IEEE 25th International Symposium on Software Reliability Engineering (ISSRE), Naples, Italy, 3–6 November 2014. [CrossRef]
25. Oliveira, R.; Raga, M.; Laranjeiro, N.; Vieira, M. An approach for benchmarking the security of web service frameworks. *Future* **2020**, *110*, 833–848. [CrossRef]
26. Bernsmed, K.; Jaatun, M.G.; Undheim, A. Security in service level agreements for cloud computing. In Proceedings of the 1st International Conference on Cloud Computing and Services Science (CLOSER 2011), Noordwijkerhout, The Netherlands, 7–9 May 2011; Available online: https://jaatun.no/papers/2011/CloudSecuritySLA-Closer.pdf (accessed on 15 September 2021).
27. Keoh, S.L.; Kumar, S.S. Securing the Internet of Things: A Standardization Perspective. *IEEE Internet Things J.* **2014**, *1*, 265–275. [CrossRef]
28. Granjal, J.; Monteiro, E.; Silva, J.S. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. *IEEE Commun. Surv. Tutor.* **2015**, *17*, 1294–1312. [CrossRef]
29. Aversano, L.; Bernardi, M.L.; Cimitile, M.; Pecori, R. A systematic review on Deep Learning approaches for IoT security. *Comput. Sci. Rev.* **2021**, *40*, 100389. [CrossRef]
30. Ahmad, R.; Alsmadi, I. Machine learning approaches to IoT security: A systematic literature review. *Internet Things* **2021**, *14*, 100365. [CrossRef]
31. Samann, F.E.F.; Zeebaree, S.R.; Askar, S. IoT Provisioning QoS based on Cloud and Fog Computing. *J. Appl. Sci. Technol. Trends* **2021**, *2*, 29–40. [CrossRef]
32. Zikria, Y.B.; Ali, R.; Afzai, M. Next-Generation Internet of Things (IoT): Opportunities, Challenges, and Solutions. *Sensors* **2021**, *21*, 1174. [CrossRef] [PubMed]
33. Fizza, K.; Barnerjee, A.; Mitra, K.; Jayaraman, P.P.; Ranjan, R.; Patel, P.; Georgakopoulos, D. QoE in IoT: A vision, survey and future directions. *Discov. Internet Things* **2021**, *1*, 4. [CrossRef]
34. *Report on the Current Status and Awareness of Security Measures among IoT Product and Service Developers*; Information-Technology Promotion Agency: Tokyo, Japan, March 2018; Available online: https://www.ipa.go.jp/files/000065094.pdf (accessed on 15 September 2021).
35. Ito, K.; Morisaki, S.; Goto, A. *A Study toward Quality Metrics for IoT Device Cybersecurity Capability*; International Studies Association (ISA) Asia-Pacific: Singapore, July 2019; p. 22. Available online: https://pure.bond.edu.au/ws/portalfiles/portal/34024127/ISA_AP_Singapore_2019_Full_Program.pdf (accessed on 15 September 2021).
36. Wohlin, C. Guidelines for Snowballing in Systematic Literature Studies and a Replication in Software Engineering. In Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering (EASE '14), London, UK, 13–14 May 2014; Article No. 38. pp. 1–10.
37. *Baseline Security Recommendations for IoT*; European Union Agency for Cybersecurity (ENISA): Attiki, Greece, 2017; ISBN 978-92-9204-236-3. [CrossRef]
38. *Framework for Improving Critical Infrastructure Cybersecurity v1.1*; National Institute of Standards and Technology (NIST): Gaithersburg, MD, USA, April 2018. [CrossRef]
39. *IoT Security Guidelines for Endpoint Ecosystem, Ver. 2.2*; The GSM Association (GSMA): Atlanta, GA, USA, February 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).
40. Abdulrazig, A.; Norwawi, N.; Basir, N. Security measurement based on GQM to improve application security during requirements stage. *Int. J. Cyber-Secur. Digit. Forensics (IJCSDF)* **2012**, *1*, 211–220. Available online: http://oaji.net/articles/2014/541-1394063127.pdf (accessed on 15 September 2021).
41. Yahya, F.; Walters, R.J.; Wills, G. Using Goal-Question-Metric (GQM) Approach to Assess Security in Cloud Storage. *Lect. Notes Comput. Sci.* **2017**, *10131*, 223–240. [CrossRef]
42. Dodson, D.; Souppaya, M.; Scarfone, K. *Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)*; NIST: Gaithersburg, MD, USA, April 2020. [CrossRef]
43. Security Development Lifecycle (SDL). Microsoft. 2008. Available online: https://www.microsoft.com/en-us/securityengineering/sdl/ (accessed on 15 September 2021).
44. Secure SDLC (Software Development Life Cycle). Synopsys. Available online: https://www.synopsys.com/blogs/software-security/secure-sdlc/ (accessed on 15 September 2021).

45. *SDLC (Secure Development Life Cycle)*; 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). (In Japanese)
46. *Cybersecurity Strategy*; National Center of Incident Readiness and Strategy of Cybersecurity (NISC): Tokyo, Japan, September 2015. Available online: https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-kakugikettei.pdf (accessed on 15 September 2021). (In Japanese)
47. Basili, V.; Caldiera, C.; Rombach, D. Goal, question, metric paradigm. In *Encyclopedia of Software Engineering*; Wiley: Hoboken, NJ, USA, 1994; Volume 2, pp. 527–532. ISBN 1-54004-8. Available online: http://www.kiv.zcu.cz/~{}brada/files/aswi/cteni/basili92goal-question-metric.pdf (accessed on 15 September 2021).
48. *Terminal Conformity Regulation of Telecommunications Business Law*; Part 10 of Section 34; Ministry of Internal Affairs and Communications of Japan: Tokyo, Japan, January 2020. Available online: https://elaws.e-gov.go.jp/document?lawid=360M50001000031 (accessed on 15 September 2021). (In Japanese)
49. 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).
50. Oregon House Bill 2395. July 2019, OR, USA. Available online: https://legiscan.com/OR/text/HB2395/id/2025565/Oregon-2019-HB2395-Enrolled.pdf (accessed on 15 September 2021).
51. Department for Digital, Culture, Media & Sport, UK. Consultation on Regulatory Proposal on Consumer IoT Security. 2020. Available online: https://www.gov.uk/government/consultations/consultation-on-regulatory-proposals-on-consumer-iot-security (accessed on 15 September 2021).
52. *Foundational Cybersecurity Activities for IoT Device Manufacturers*; NISTIR 8259; NIST: Gaithersburg, MD, USA, 2020. [CrossRef]
53. *IoT Device Cybersecurity Capability Core Baseline*; NISTIR 8259A; NIST: Gaithersburg, MD, USA, 2020. [CrossRef]
54. Council to Secure the Digital Economy. The C2 Consensus on IoT Device Security Baseline Capabilities. 2019, USA. Available online: https://securingdigitaleconomy.org/wp-content/uploads/2019/09/CSDE_IoT-C2-Consensus-Report_FINAL.pdf (accessed on 15 September 2021).
55. *Cybersecurity for Consumer Internet of Things: Baseline Requirements, EN 303 645. V2.1.1*; ETSI: Sophia Antipolis, France, June 2020; Available online: //www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf (accessed on 15 September 2021).
56. *IoT Common Security Requirements Guidelines 2021*; Connected Consumer Device Security Council of Japan (CCDS): Tokyo, Japan, November 2020; Available online: https://www.ccds.or.jp/english/contents/CCDS_SecGuide-IoTCommonReq_2021_v1.0_eng.pdf (accessed on 15 September 2021).
57. *ioXt 2020 Base Profile Ver. 1.00*; ioXt Alliance, Inc.: Newport Beach, CA, 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).
58. *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).
59. Botella, P.; Burgues, X.; Carvallo, J.P.; Franch, X. ISO/IEC 9126 in practice: What do we need to know? In Proceedings of the 1st Software Measurement European Forum (SMEF), Rome, Italy, 28–30 January 2004.
60. Olsson, T.; Runeson, P. V-GQM: A feed-back approach to validation of a GQM study. In Proceedings of the Seventh International Software Metrics Symposium, London, UK, 4–6 April 2001. [CrossRef]
61. Othman, B.; Angin, L.; Weffers, P.; Bhargava, B. Extending the Agile Development Process to Develop Acceptably Secure Software. *IEEE Trans. Dependable Secur. Comput.* **2014**, *11*, 497–509. [CrossRef]
62. Oueslati, H.; Rahman, M.M.; Othmane, L.B. Literature Review of the Challenges of Developing Secure Software Using the Agile Approach. In Proceedings of the 2015 10th International Conference on Availability, Reliability and Security (ARES), Toulouse, France, 24–27 August 2015. [CrossRef]
63. Yasar, H.; Kontostathis, K. Where to Integrate Security Practices on DevOps Platform. *Int. J. Secur. Softw. Eng.* **2016**, *7*, 39–50. [CrossRef]
64. Constante, F.M.; Soares, R.; Pinto-Albuquerque, M.; Mendes, D.; Beckers, K. Integration of Security Standards in DevOps Pipelines: An Industry Case Study. In *Product-Focused Software Process Improvement (PROFES 2020)*; Springer: Turin, Italy, 2020; pp. 434–451. [CrossRef]
65. *Guide to Secure the Quality of IoT Devices and Systems*; Information Technology Promotion Agency of Japan (IPA): Tokyo, Japan, February 2019; Available online: https://www.ipa.go.jp/files/000064877.pdf (accessed on 15 September 2021). (In Japanese)
66. Jinesh, M.K.; Abhiraj, K.S.; Bolloiu, S.; Brukbacher, S. *Future-Proofing the Connected World: 13 Steps to Develop Secure Iot. Jan.*; CSA: Bellingham, WA, USA, 2016. [CrossRef]
67. *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 15 September 2021).
68. *IoT Security Assessment Checklist Ver. 3*; GSMA: Atlanta, GA, USA, September 2018; Available online: https://www.gsma.com/security/resources/clp-17-gsma-iot-security-assessment-checklist-v3-0/ (accessed on 15 September 2021).
69. *IoT Security Evaluation and Assessment Guideline*; 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 15 September 2021). (In Japanese)