Updated Comparison of Japanese Guidelines with Those of the GSMA on Security for the Internet of Things (IoT)

Overview of Updates:

- Version 2 of the IoT Security Guidelines, published on 28 September 2017 by the Information-Technology Protection Agency (IPA) of Japan's Ministry of Economy, Trade and Industry (METI), has streamlined the previous 21 guidelines of Version 1 from July 2016 into 17 revised guidelines, grouped, as before, under five categories, but with simpler headings of Policy, Analysis, Design, Maintenance, and Operation. The new IPA guidelines are also available in English at https://www.ipa.go.jp/english/sec/reports/20160729-02.html, rather than previously only in Japanese. The 106-page Version 2 of the IPA's IoT Security Guidelines provides descriptions and examples, with images of each guideline.

- GSMA updated its four papers of IoT Security Guidelines totalling 217 pages, first as Version 1.1 in November 2016, and then as a Version 2, a day after the IPA's Version 2 on 29 September 2017. The updates of GSMA's Version 1 from February 2016 consist mainly of adding references to GSMA IoT security (in November 2016), references to the global-standards initiative for machine-to-machine communications, oneM2M, and to low-power, wide-area (LPWA networks) in September 2017. In October 2017, the GSMA also published a 39-page IoT Security Checklist Assessment (CLP.17) and an accompanying 6-page explanatory process (CLP.17) for the Checklist Assessment. The four GSMA IoT security papers consist of an Overview of IoT Security Guidelines (CLP.11), a Guideline for Service Ecosystems (CLP.12), a Guideline for Endpoint Ecosystems (CLP.13), and a Guideline for Network Operators (CLP.14).

- Version 2 of the IPA Guidelines removes and does not replace previous Guideline 7 (on learning from the past), previous Guideline 14 (on establishing appropriate network connections according to functions and applications), previous Guideline 15 (on awareness of initial settings), previous Guideline 16 (on introducing an authentication function), previous Guideline 17 (on maintaining safety and security of devices after shipment and release), previous Guideline 20 (on understanding the roles of stakeholders in IoT systems), and previous Guideline 21 (on identifying the vulnerability of devices and raising users' attention).

- Version 2 of the IPA Guidelines adds new Guideline 2 (on reviewing systems and human resources for Safety/Security), new Guideline 14 (on implementing the functions to maintain Safety/Security even after the passage of time), and new Guideline 16 (on informing relevant business operators of the procedures to be followed after market release).

- The GSMA's Version 1 guidelines lacked only one comparable guideline to those from IPA's Version 1—specifically an equivalent to IPA's previous Guideline 15 on awareness of initial IoT settings, but the new IPA guidelines, Version 2, have removed that previous Guideline 15.

- The text below has two parts:
  (1) a summary of the IPA guidelines, Version 2; and
  (2) a comparison table of IPA's and GSMA's Version 2 guidelines, colour coded according to a traffic light system of green as concurrence, yellow as some differences, and red as nothing comparable.

Summary of IPA's IoT Security Guidelines, Version 2:

Part 1: Policy

Guideline 1: Formulating the basic policies for Safety/Security

(i) Managers shall formulate the basic policies for the Safety/Security of the Smart-society, make them known within the company, continuously evaluate their achievement status, and review them as required.

Guideline 2: Reviewing systems and human resources for Safety/Security

(i) Establish systems and environments for discussing the Safety/Security issues of the Smart society in an integrated manner.

(ii) Secure/develop human resources (developers and maintenance staff) for that purpose.

Guideline 3: Identify essential functions and information to be protected

(i) Recognize the possible existence of internal fraud that can be a threat to the Safety/Security of the Smart-society, and discuss the measures to guard against it.

(ii) Discuss the measures to prevent mistakes by relevant parties and to protect Safety/Security even when mistakes are made.

Part 2: Analysis

Guideline 4: Identifying objects to be protected

(i) Identify the intrinsic functions, information, etc. to be protected from the point of view of the Safety/Security of the Smart-society.

(ii) The functions for connections (IoT functions) should also be identified to be protected for the Safety/Security of the intrinsic functions and information.

Guideline 5: Assuming the risks caused by connections

(i) Even for devices and systems intended for closed networks, assume the risks on the basis that they are used as IoT components.

(ii) The risks that the connected entity is fake or hijacked should be assumed.

(iii) The risks during maintenance and risks due to the illegal use of maintenance tools should also be assumed.

Guideline 6: Assuming the risks spread through connections

(i) Assume the risks of spreading security threats and the impacts of device failures due to connections with other devices.

(ii) Assume in particular that the risks of spreading the impacts increase when devices and systems with low level of Safety/Security measures are connected.

Guideline 7: Understanding physical security risks

(i) Assume the risks of unauthorized operations of stolen or lost devices, and physical attacks at locations where no administrator is present.

(ii) Assume the risks of information retrieval, software alternation, and resale of second-hand or disposed devices.

Part 3: Design

Guideline 8: Designing to enable both individual and total protection

(i) Discuss the measures to be taken at individual IoT components against the risks via external interfaces, internally contained risks, and physical security risks.

(ii) If the risks cannot be handled by individual IoT components, discuss the measures to be taken at upper-layer IoT components that include them.

Guideline 9: Designing so as not to cause trouble in other connected entities

(i) Discuss the designs to enable the detection of abnormalities of IoT components.

(ii) Discuss suitable behaviors when abnormalities are detected.

Guideline 10: Ensuring consistency between the designs of Safety/Security

(i) Visualize the designs of Safety/Security.

(ii) Verify the mutual impacts of the designs of Safety/Security.

Guideline 11: Designing to ensure Safety/Security even when connected to unspecified entities

(i) Discuss the designs to enable IoT components to determine the connection methods according to the entities to be connected to and conditions of the connections.

(ii) Consider the design to prevent IoT components and users from a connection which may result in a hazard.

Guideline 12: Verifying/validating the designs of Safety/Security

(i) Verify and validate the Safety/Security design of devices and systems to be connected, with consideration given to the risks unique to the IoT.

Part 4: Maintenance

Guideline 13: Implementing the functions to identify and record own status

(i) Discuss the functions to identify and record the component's own status and the status of communications with other devices.

(ii) Discuss the functions to disallow unauthorized deletion/manipulation of records.

Guideline 14: Implementing the functions to maintain Safety/Security even after the passage of time

(i) Discuss the functions to maintain Safety/Security by updates against increased risks due to aging or changes of usages and environments.

Part 5: Operation

Guideline 15: Identifying IoT risks and providing information after the market release

(i) Collect/analyze the latest information on defects, vulnerabilities, accidents, and incidents at all times.

(ii) Provide risk information within the company, to relevant business operators, and oninformation provision sites as required.

Guideline 16: Informing relevant business operators of the procedures to be followed after-market release

(i) Inform the procedures that need to be followed in deployment, operation, maintenance, and disposal to the staff and external business operators directly involved in them.

Guideline 17: Making the risks caused by connections known to general users

(i) Notify general users that careless connections and unauthorized use not only affect the individual but also damage others or cause adverse impacts on environments.

(ii) Notify general users of the requirements to be followed for maintaining Safety/Security.

Comparison of METI and GSMA Guidelines:

- The GSMA's IoT security Guidelines include four sets of documents (http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/)
  - CLP.11: IoT Security Guidelines Overview Document
  - CLP.12: IoT Security Guidelines for IoT Service Ecosystem
  - CLP.13: IoT Security Guidelines Endpoint Ecosystem
  - CLP.14: IoT Security Guidelines for Network Operators

The following traffic-light system of colour coding displays the degree of alignment in detail and substance between the GSMA and METI guidelines, with green optimal, yellow of possible concern, and red a warning of significant divergence.

- Green: the IPA and GSMA guidelines are aligned in detail and substance.
- Yellow: GSMA's guidelines share similar messages, but provide more (or less) detail than those of the IPA
- Red: the IPA or GSMA does not provide a comparable guideline to that of the other.

Japan’s IPA IoT Security Guidelines, version 2.0 (issued on 28 Sept. 2017)			GSMA IoT Security Guidelines, version 2.0 (issued on 29 Sept. 2017)	Remarks
Policy: Making corporate efforts for the Safety/Security of the Smart-society	**Guideline 1**	Formulating the basic policies for Safety/Security (~ previous Guideline 1)	Throughout CLP.11 – CLP.14: Overview (CLP.11) and Guideline for Service Ecosystems (CLP.12), Guideline for Endpoint Ecosystems (CLP.13), and Guideline for Network Operators (CLP.14)	The IPA guideline, at pp. 33-34 provides a high-level list of example matters to consider in formulating the policies.
	Guideline 2	Reviewing systems and human resources for Safety/Security	CLP.11, Chapter 6 on Privacy Considerations with examples in Chapters 8-10 of wearables, drones, and vehicle sensor networks, respectively, and in Annex A, considerations for IoT Service Providers. Also in the Checklist Assessment	The IPA guideline provides a list of example measures, at pg 35, and sources of info pertaining to HR, at pp 36-37.
	Guideline 3	Preparing for internal fraud and mistakes (previous Guideline 2)	CLP.12, Chapter 6.12: “the user, administration, and partner authorization technologies must be configured separately … their actions and identities must be authenticated using a separate system.” “ensures that each action is traceable to an authenticated user and an authorization. These metrics can be stored and later reviewed in the event that a compromise is suspected”	Both recognize the potential of internal fraud. GSMA also introduces methods to prevent, detect and minimize these internal risks.

Analysis: Understanding the risks of the Smart-society	**Guideline 4**	Identifying objects to be protected (previous Guideline 3)	CLP.11, Chapter 5: “While every organization should create a granular perspective of technological risk, there are high level questions that function as starting points for the risk assessment process: What assets (digital or physical) need to be protected?”	Both recognize the importance of risk assessment and identification of objects in need of protection.
	Guideline 5	Assuming the risks caused by connections (previous Guideline 4)	CLP.13, Chapter 3.4: “IoT Endpoints, by nature, participate in a network of other Endpoints.” “With this perspective in mind, it is clear that even the easiest to develop type of Endpoint device must behave in a reliable, high quality, and secure manner because it is expected to participate in a network that could eventually span up to millions of devices in size.”	Both recognize that any threat from a single device will have an effect on its entire IoT ecosystem since the risk may spread through connection.
	Guideline 6	Assuming the risks spread through connections (previous Guideline 5)		

	Guideline 7	Understanding physical security risks (previous Guideline 6)	CLP.13, Chapter 2.4: "Many IoT Endpoints are physically accessible to the Attacker. All hardware components and interfaces on these Endpoints are therefore potentially subject to attack and must be secured by the developer." Chapter 6.9.1: "The ability for stolen devices to be subverted through brute-force password guessing" could be prevented by implementation of Endpoint Password Management. Chapter 9.7: "IoT Service Providers who are conscious about security must take into account the source of their components, their assembly, and the fulfilment process used to ship the assembled technology."	Both recognize the physical-security risks of IoT devices.
<u>Design</u>: Considering the designs to protect the objects to be protected	**Guideline 8**	Designing to enable both individual and total protection (previous Guideline 8)	CLP.12, Chapter 3: "Security in Service Endpoint environments can be designed using common pieces of infrastructure, strategies, and policies…these components must be secured individually, but using similar methodologies."	GSMA's document introduces how to enable protection without going into specifics.
	Guideline 9	Designing so as not to cause trouble in other connected entities (previous Guideline 9)	CLP.12, Chapter 5.7: "Each system must be monitored to allow administrators and Information Technology (IT) works to detect and diagnose anomalies." "Monitoring must be performed at multiple dimensions." Chapter 5.8.1:	Both recognize the importance to prepare, detect, and respond to an anomaly.

			"Organizations should be prepared to respond to an incident almost immediately…" CLP.13, Chapter 7.2: "Anomalous behaviour emanating from an Endpoint may include: • Erratic reboots or device resets • Leaving or joining a communications network at erratic intervals • Connecting to abnormal service Endpoints, or connecting to service Endpoints at inappropriate times • A significantly different network traffic fingerprint than normal • Multiple poorly-formed messages sent from the Endpoint to server Endpoints … By setting a baseline of behaviour, then continually monitoring for potential outliers, the organization can more quickly diagnose both security and performance problems in production environments."	
	Guideline 10	Ensuring consistency between the designs of safety and security (previous Guideline 10)	CLP.13, Chapter 5.14: "The architectural model may need to be shifted in order to maintain both safety and security. Where possible, security should not be discarded in favour of safety."	Both agree that the design of IoT systems and devices should maintain both security and safety.

	Guideline 11	Designing to ensure Safety/Security even when connected to unspecified entities (previous Guideline 11)	CLP.12, Chapter 5.4: "For publicly accessible services, several pieces of security and reliability technology are required to maintain the availability, confidentiality, and integrity of the service: • DDoS-resistant infrastructure • Load-Balancing infrastructure • Redundancy systems • Web Application Firewalls (optional) • Traditional Firewalls …" "Front-end security should be applied to all protocols implemented by the service, if the service is available over IPv4 and IPv6, the same security constraints should be applied to the service over both protocols. If a service is accessible over TCP as well as Stream Control Transmission Protocol (SCTP), the security constraints should be applied to both of those protocols as well. Ports that do not offer public services pinned to the IoT product or service should not be accessible." Chapter 7.3: "By restricting access to the Access Point Name (APN), an organization can ensure that only authenticated endpoints are allowed to connect to the service infrastructure made available through the APN." Chapter 7.3.1 Risk: "It is much more valuable to the business and to the	Both agree on the importance of ensuring safety in public access to IoT devices.

			security of the entire IoT ecosystem when Endpoints are forced to connect only to approved services.”	
	Guideline 12	Verifying/validating the designs of safety and security (previous Guideline 12)	CLP.13, Chapter 1.2 Document Purpose: “All technologies used to drive the physical device shall be evaluated for security risks.” The entire document discusses how to verify and evaluate IoT designs.	Both agree on the importance of evaluating the safety and security of IoT. However, the GSMA guidelines do not include examples of international IoT standards.
Maintenance: Considering the designs to ensure protection even after market release	**Guideline 13**	Implementing the functions to identify and record own status (previous Guideline 13)	CLP.13, Chapter 6.13 Logging and Diagnostics: “[T]he IoT Service Provider should constantly evaluate the behaviour of the Endpoint and determine whether the Endpoint is functioning within the set of approved behaviours. To accomplish this, three strategies should be used: 1. Anomaly detection (Chapter 7.2) 2. Endpoint logging (Chapter 6.13) 3. Endpoint diagnostics (Chapter 6.13)”	Both recognize the importance of recording the status of IoT devices and system.
	Guideline 14	Implementing the functions to maintain Safety/Security even after the passage of time	CLP.14, Chapter 3 Network Security Principles: “Proper and reliable security mechanisms must be implemented by Network Operators in their networks.” The entire CLP.14 addresses the issues related to network connection and provides plenty of guidelines.	Both agree on the need to discuss and properly construct the method of network connection.
Operation:	**Guideline 15**	Identifying IoT risks and providing information	CLP.12, Chapter 6.6 Define an Update Model: “Updating an execution environment, application image, or TCB is a challenging process. Consider the following example model that simplifies the overall process:	Both recognize the importance of building a set of procedures and updated model for collecting risk information and protection.

Protecting with relevant parties		after the market release (previous Guideline 18)	• For each layer of the execution platform, define a network resource such as a unique URL for the new application image • Generate a signing key for each specific layer • For all new, authorized versions of each layer, generate an image of that layer • Include metadata describing the image (version, timestamp, identity, etc.) in the layer image • Sign the layer image with the signing key • Make the image, the signature, and the public key available, possibly via the unique network resource, or through a update service …” “This recommendation implies that a patch management process should be used to maintain services and technologies within the infrastructure.”	
	Guideline 16	Informing relevant business operators of the procedures to be followed after market release	CLP.11, Chapter 7.5 Ongoing Lifecycle: “The security life cycle does not stop at this juncture. Rather, security is an inherent part of the overall engineering of a process. Endpoints and IoT Services have a lifetime, and must be continually serviced throughout that lifetime… Cryptographic algorithms become dated or deprecated. New protocols and radio technologies	Both recognise the need for ongoing monitoring after initial deployment. The IPA guidelines, at pp 79-81, provides detailed examples.

			must interoperate with the product or service. This ever changing ecosystem our embedded products are deployed in must be constantly reviewed to ensure that confidentiality, integrity, availability, and authenticity are maintained. Managing the ongoing security lifecycle corresponds with the Monitor and Frame components of the NIST Risk Management Framework [5], and steps one, four, and five of the CERT OCTAVE model [6].” CLP.12, Chapter 5.10 Define a Sunsetting Model: “Every system that is deployed by an organization, and every tier used, has a lifetime. Even if the same product or service is deployed by the organization for decades, the technologies used to drive that product or service will change. Thus, there must not only be a plan for designing and implementing the product or service, there must be a plan to sunset that product or service.”	
	Guideline 17	Making the risks caused by connections known to general users (previous Guideline 19)	CLP.13, Chapter 8.4 User Interface Security: “When an anomaly has occurred, such as … the user should receive a visible alert. Alternatively, the user should be able to review alerts from the system from within the User Interface.” “[T]he user should be prompted to confirm action and validate that the action performed is desirable. The user should be given the option to cancel the action.”	Both agree that users should receive alerts when they undertake any actions that may lead to undesirable effects.