IoT Security Safety Framework

-Ensuring the reliability of the connection between physical space and cyber space-

Version 1.0

Cyber Security Division, Commerce and Information Policy

Bureau, Ministry of Economy, Trade and Industry

Reiwa 2nd November 5th

table of contents

1. 1. The need for this framework

1-1 Layer 2 in CPSF (connection between physical space and cyber space)

1-1-1 CPSF Introduction

In an industrial society where cyberspace and physical space are highly integrated, it is called products and services.

The process of creating value (supply chain) has changed from the conventional standard and linear process to various connections.

It has changed to an atypical one. Such a new value creation process (value creation)

By organizing the security issues and countermeasures for the process, a new industrial society will be created.

A cyber physical security measure frame that summarizes the idea of securing utility

Work (CPSF). At CPSF, "In ensuring the security of the value creation process

For the connection between reliable management companies that is assumed in the conventional supply chain.

Therefore, beyond the area where added value is created, information in physical space is digitized by IoT.

It is taken into cyberspace as data, and such data is freely distributed in cyberspace.

As a result, various data can create new data to create added value, or can be newly created.

Creating new products and services by feeding back the collected data to the physical space by IoT

It is necessary to take into consideration a series of new activities to create new added value, which is to put out.

The first layer, physical space and cyber space, which places the basis of reliability in the connection between companies.

The second layer that puts the base point of reliability in the flow, the first layer that puts the base point of reliability in the connection in cyberspace

We set three different reliability base points, three layers, and secure the entire economy and society around these base points.

It summarizes the identification of issues related to qualities and their countermeasures.

1-1-2 Positioning of the second layer

The second layer is the boundary between cyberspace and physical space, and information changes accurately at that boundary.

Being converted, that is, ensuring the accuracy of the transfer function, is the starting point of reliability in the second layer.

There is. In general, the boundary between cyberspace and physical space is, for example, the sensor responsible for the above-mentioned transfer function.

It is made up of so-called IoT systems that consist of actuators. Like IoT

The equipment and systems that connect physical space and cyber space are the corporate activities of humans and humans who use them.

While it benefits dynamic and economic activities, when an incident occurs, people and people who use it

Ki will be liable for loss and liability. Therefore, to ensure the security of IoT device / system 1

Is the core of security measures in the second layer. In this framework, only the equipment

The reason why the system is also targeted is that the device / system is targeted when considering security measures.

Equipped with sensors and actuators where it is important to focus on the added value provided to users

While there are cases where the equipment to be used alone provides added value, it is the first time that the equipment has been incorporated into the system.

This is because it may provide added value.

On the other hand, the security issues in the second layer are not uniform. Also in CPSF, as follows

Multiple cases are shown in.

ÿ As a result of a cyber attack on the sensor function, the data in the physical space cannot be transferred correctly.

Incorrect data is provided to cyberspace, and operations are carried out by utilizing the data.

Lost trust in

ÿ **Machines** in physical space due to incorrect instructions from cyberspace or attacks on IoT devices

Safety due to incorrect control of the equipment, physical harm to employees, damage to equipment, etc.

The above problem occurs

ÿ The functions of IoT devices and systems stop due to cyber attacks, etc.

In addition, we will discuss issues related to the management of IoT devices and systems that connect cyberspace and physical space.

But it touches as follows.

ÿ Installation area management and monitoring according to the importance of the role played by IoT devices in organizations, etc.

It is necessary to consider multi-layered measures such as implementation.

ÿ It is difficult for organizations to manage IoT devices installed in homes by individuals.

Therefore, it is necessary to take measures considering the risk of theft, loss, etc.

In this way, security measures in the second layer have many issues related to IoT devices and systems.

It is necessary to take measures not only based on the characteristics but also on the diversity of the environment in which they are used. To this diversity

On the other hand, CPSF organizes risk sources and countermeasure requirements through a three-layer structure approach and responds to countermeasure requirements.

An example of security measures is shown. In that case, functional safety is a major premise for ensuring safety.

In this framework, regarding IoT, with reference to ISO / IEC 20924: 2018, the infrastructure of entities, people, systems and information resources that are interconnected with services that process and react to information from physical space and cyber space. We defined it as a structure, and defined a system that provides such a function as an IoT system, and an entity that interacts with and communicates with the physical space through sensing or actuation in that system as an IoT device. In this framework, it is important to focus on the added value provided to users using IoT, so it does not distinguish between IoT devices and IoT systems, and refers to the unit that provides added value. It is expressed as "equipment / system".

As it is necessary to respond by combining measures from the viewpoint and cyber security measures

There is.

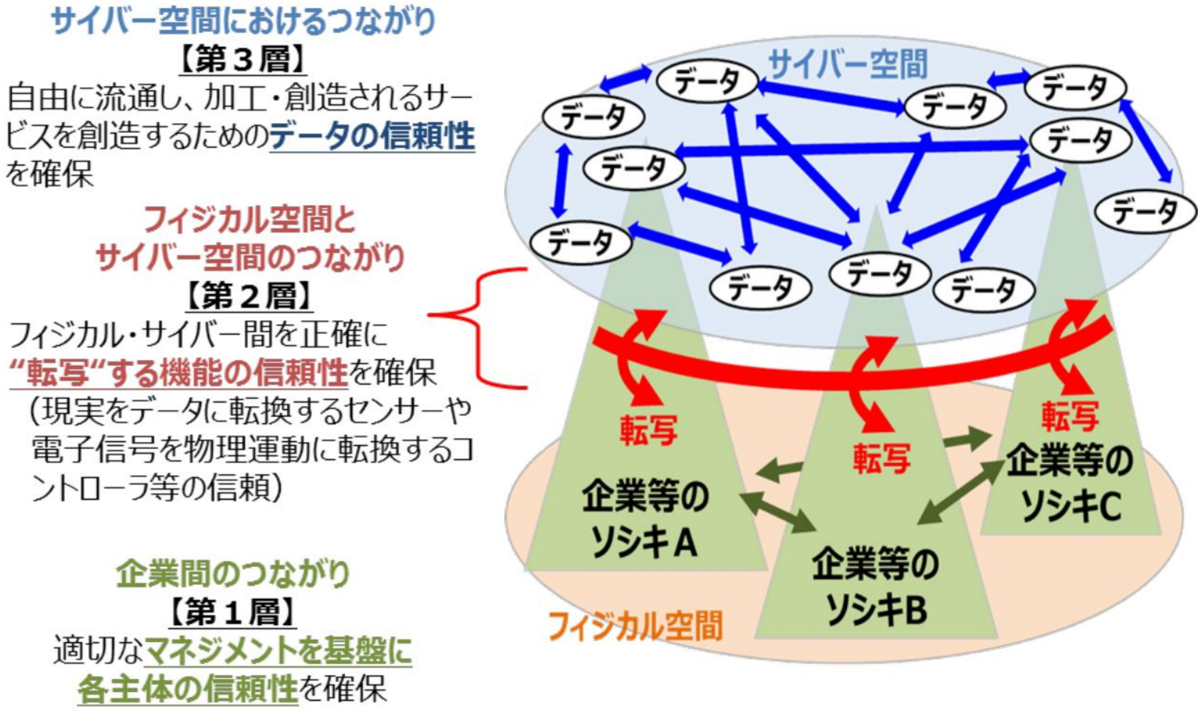
サイバー空間におけるつながり
【第３層】
自由に流通し、加工・創造されるサービスを創造するためのデータの信頼性を確保
フィジカル空間とサイバー空間のつながり
【第２層】
フィジカル・サイバー間を正確に“転写“する機能の信頼性を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）
企業間のつながり
【第１層】
適切なマネジメントを基盤に各主体の信頼性を確保
サイバー空間
データ
転写
企業等のソシキA
企業等のソシキB
企業等のソシキC
フィジカル空間

Figure 1 Three-layer structure model in CPSF and reliability in each layer

1-2 Purpose of this framework

As mentioned in IoT Security Guideline 2 , it is used in the field of simple information services.

IoT devices and IoT devices used in fields related to safety such as factories and social infrastructure systems

Are different in required security level, purpose of security measures, and priority. Utilization of IoT in the future

With the expansion of, individual and specific for each field of use, based on the peculiarity and diversity of each field

It is expected that actual security measures will be advanced for IoT devices and systems. That too

Regarding the security and safety of devices and systems that connect cyberspace and physical space

And because there is a lack of a unified approach to comprehensively grasping issues, in each field / industry

There is concern that unique security and safety measures will be set through separate examination processes.

To. If inconsistencies arise in each countermeasure, society will accept and manage new mechanisms.

The cost may increase.

[2] IoT Promotion Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy, Trade and Industry, formulated in July 2016

This framework connects cyberspace and physical space to avoid the above situation.

Focus on the new risks posed by the new mechanism and respond to risk types and such risks.

It presents a method for categorizing security and safety measures. That is, different fields / businesses

Devices / systems in which players in the world connect cyberspace and physical space, that is, IoT devices / systems

A "basic common foundation" for sharing a framework that contributes to the examination of security and safety in

The purpose is to provide it and enable the society to effectively accept the new mechanism of IoT. IoT

It is not intended to create regulations that have a uniform enforcement force on equipment and systems.

In this framework, it is a representative example of equipment and systems that connect cyberspace and physical space.

And IoT, that is, "Internet of Things", but this framework is cyberspace and fi.

This applies to all devices and systems that connect the physical space.

2. Assumed readers of this framework

We will build a mechanism that connects cyberspace and physical space, and realize new mechanisms and services.

For those who are trying to do so, the mechanism and services will be realized in various forms, and the security will be improved.

Recognizing that the challenges of

I must take measures. The higher the innovation of new mechanisms and services, the more

In order to be accepted by society, it is necessary to take comprehensive measures to deal with various expected issues.

It will be struck.

Therefore, in this framework, the entity that realizes a new mechanism / service becomes a new risk.

When trying to take security measures against, and the entity that uses such a mechanism / service

Will take advantage of such mechanisms and services after recognizing the risks themselves through the understanding of this framework.

It is assumed that they will be referred to when they are used. For example, the following persons are used as readers.

I'm assuming.

ÿ Let's realize a new mechanism / service that connects cyber space and physical space by utilizing IoT

Who

ÿ **Those** who develop IoT devices and systems that will be used in such new mechanisms and services.

ÿ **Try** to realize a system / environment that appropriately manages such new mechanisms / services

person

ÿ **Those** who receive such new mechanisms and services

3. 3. Basic configuration of this framework

3-1 The idea behind the basic configuration

There are various forms of new mechanisms that connect cyberspace and physical space, and the security that accompanies them. In addition to the above issues, the form of damage in the event of an actual incident is extremely diverse. If uniform security requirements are set for the devices and systems that make up such a mechanism, provisional Even if that requirement is met, it is not enough to meet various security challenges. Can not. That is, it cannot be said that the situation is such that the users and the like are properly protected.

The key to considering second-tier security measures is how to approach this diversity. Is it done?

In this framework, "diversity" of new mechanisms and services that connect cyber space and physical space. As a means to approach the issue of "sex", the equipment and systems that make up this mechanism (and beyond) Furi It is called "devices / systems that connect physical and cyber".), How to understand the risk and its pair Utilizing the three axes that summarize the basic ideas related to response, categorize them, and take appropriate measures. We are proposing to organize the contents so that they can be compared and examined.

3-2 Sorting out risks hidden in devices and systems that connect physical and cyber

The security issues of devices and systems that connect physical and cyber are actually incidents. In some cases, the events that affect the outbreak of sickness may be life-threatening. There are a wide variety of cases, including cases related to sea, cases related to asset damage, and cases related to the living environment. be. In other words, there are various risks lurking in the devices and systems that connect physical and cyber.

However, it is physically difficult to sort out the events affected by the occurrence of an incident. When considering security measures for devices and systems that connect cybers, the idea is rather complicated. It will be something like that. Therefore, to extract some common terms from the affected events. By narrowing down to a small number of standards abstracted by, we will create devices and systems that connect physical and cyber. It is necessary to be able to organize the hidden risks in a simple form.

Therefore, in this framework, various human life / body, privacy / honor, assets, living environment, and economics Various events affected by activities, rumors, etc. are abstracted and organized according to the following two criteria. Categorize devices / systems that connect physical and cyber based on the risks hidden in the devices / systems. I decided to go and set it as two axes to map.

3-2-1 Axis 1: Degree of difficulty in recovering the impact of the incident that occurred

This first axis captures risk from the difficulty of recovering from the effects of an incident. Trouble with recovery

Regarding difficulty, it is necessary to first consider the effects on human life / body. Until you say

No, but if human life is lost, it will not be restored. Also, as a result of the occurrence of an incident,

When severe disability occurs, it is often not possible to completely recover. Recovery

Even if it can be done, there are cases where it can be recovered early, and there are cases where it takes time to recover.

be. Whether or not the effects of the incident can be recovered, and what can be recovered

In that case, the first axis was set as the axis of judgment as to whether or not early recovery could be achieved.

This first axis is the safety required by the legal system in fields such as product safety and occupational safety.

It stands in the same position as the basic idea of the regulatory system that sets measures and prohibited acts, and is an existing one.

Consistency with the institutional system is ensured.

On the first axis, as mentioned above, the issue is to avoid the irreparable situation of human life / body first.

However, some of the information related to personal privacy / honor was revealed once.

If it becomes, it also contains sensitive information that causes irreparable damage to the person.

In the first axis, there are also events related to the protection of information that causes irreparable damage to the person.

It can be organized into issues that can be grasped.

Here, regarding "risk", the degree of impact of the incident and the likelihood of the incident.

In this framework, devices and systems that connect physical and cyber are used.

It is relatively difficult to calculate so that it can be easily categorized based on the diversity of the system.

Do not consider, and take an approach to categorize based on the degree of impact when an incident occurs.

I'm taking it. In addition, based on this framework, specific requirements based on discussions in the industrial world, etc.

It should be noted that it is appropriate to consider the likelihood of occurrence when organizing.

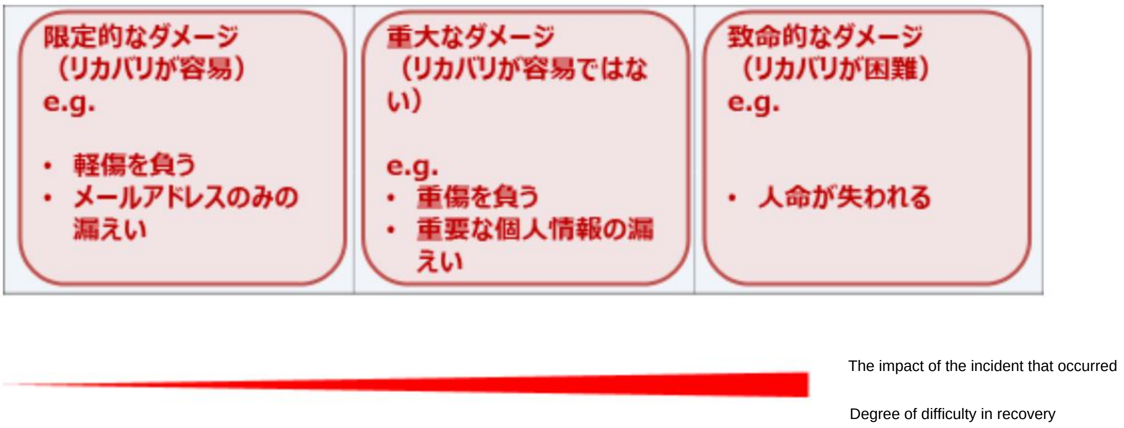
限定的なダメージ（リカバリが容易）
e.g.
• 軽傷を負う
• メールアドレスのみの漏えい
重大なダメージ（リカバリが容易ではない）
e.g.
• 重傷を負う
• 重要な個人情報の漏えい
致命的なダメージ（リカバリが困難）
e.g.
• 人命が失われる
The impact of the incident that occurred
Degree of difficulty in recovery

Figure 2 Image of the degree of difficulty in recovering the effects of an incident that occurred

3-2-2 Axis 2: Degree of economic impact of the incident that occurred (conversion to monetary value)

The second axis is for incidents, except for the possibility / difficulty of recovery from the effects of the incident.

It is based on the magnitude and degree of the impact of the conversion into monetary value.

This standard is related to the life / body and serious privacy / honor discussed in 3-2-1.

It does not take into account the difficulty of recovering the effects of the incident in

Assuming that it can be converted into monetary value, it will damage assets, economic activities and society.

It was decided to map and capture events such as the effects of.

The 2nd axis is a standard that should be considered independently of the 1st axis, and it is difficult to recover in the arrangement in the 1st axis.

It is a device / system that connects physical and cyber, which is regarded as having a low degree of difficulty.

However, it is sufficient that the second axis is organized as having a very high degree of economic impact.

On the other hand, Fiji was perceived as having a high degree of difficulty in recovery in the arrangement on the first axis.

Devices and systems that connect Cal and Cyber are actually converted into monetary value in the form of compensation, etc.

There is a high possibility that it will fall under a reasonable level.

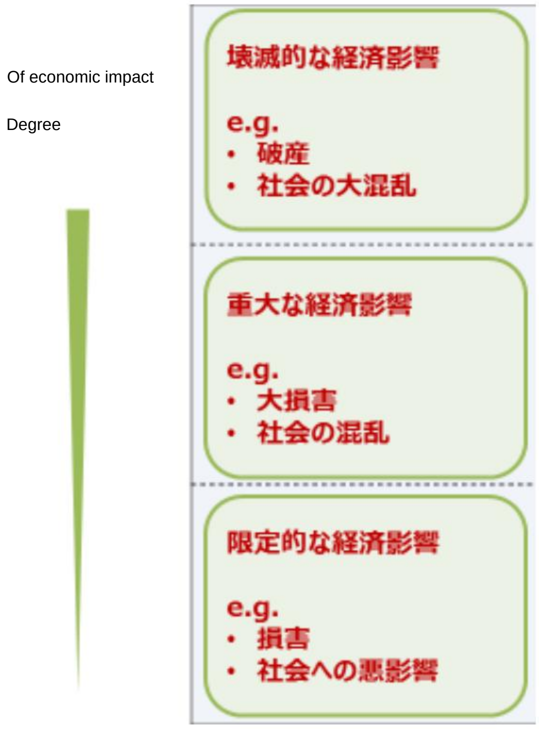

Figure 3 Image of the degree of economic impact of an incident that has occurred

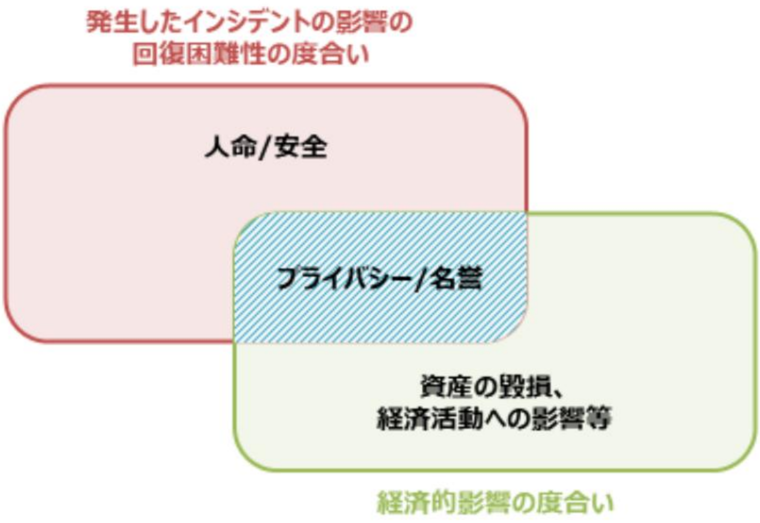

Figure 4 Privacy / Honor Arrangement that Can Be Organized on Axis 1

3-2-3 Categorization of devices and systems that connect physical and cyber

Based on the above two axes, the equipment / system that connects physical / cyber is the equipment / system. It can be mapped based on the risks lurking in the stem.

For example, on the 1st axis, from the viewpoint of difficulty in recovery, limited damage (easy to recover) and serious uselessness. Organize in the form of ji (not easy to recover) and fatal damage (difficult to recover), and on the second axis, From the perspective of economic impact, limited economic impact, significant economic impact, and catastrophic economic impact. By organizing in a shape, it is possible to categorize into 9 quadrants (categories) according to the risk. Become.

Use this category when considering appropriate measures for each device / system. Can be done. As mentioned above, in terms of security of devices and systems that connect physical and cyber Since the issues are diverse, appropriate measures for each device / system are not uniform. However However, by considering based on this category, the ones that are generally categorized in the upper right are better. Since the impact of incidents tends to be large, it is considered that more profound measures are required. On the other hand, it is possible to sort out that the ones categorized in the lower left have the possibility that minor measures are sufficient. It becomes Noh. Details will be described in 3-3.

Here, as an example, equipment / system mapping is performed, but the equipment / systems that make up the service are used. It is also conceivable to focus on the functions provided by the stem for mapping. For each device / system However, it can be set arbitrarily when mapping. Also, if it was the same device / system But what kind of environment is it used in, what kind of role it has in that environment, and what kind of skis Depending on the purpose, such as whether it is used by a person who has a problem, its importance, issues, and the impact of an incident are large. It's very different. Therefore, even with the same device / system, the mapping destination may differ depending on the usage pattern, etc. It should be noted that.

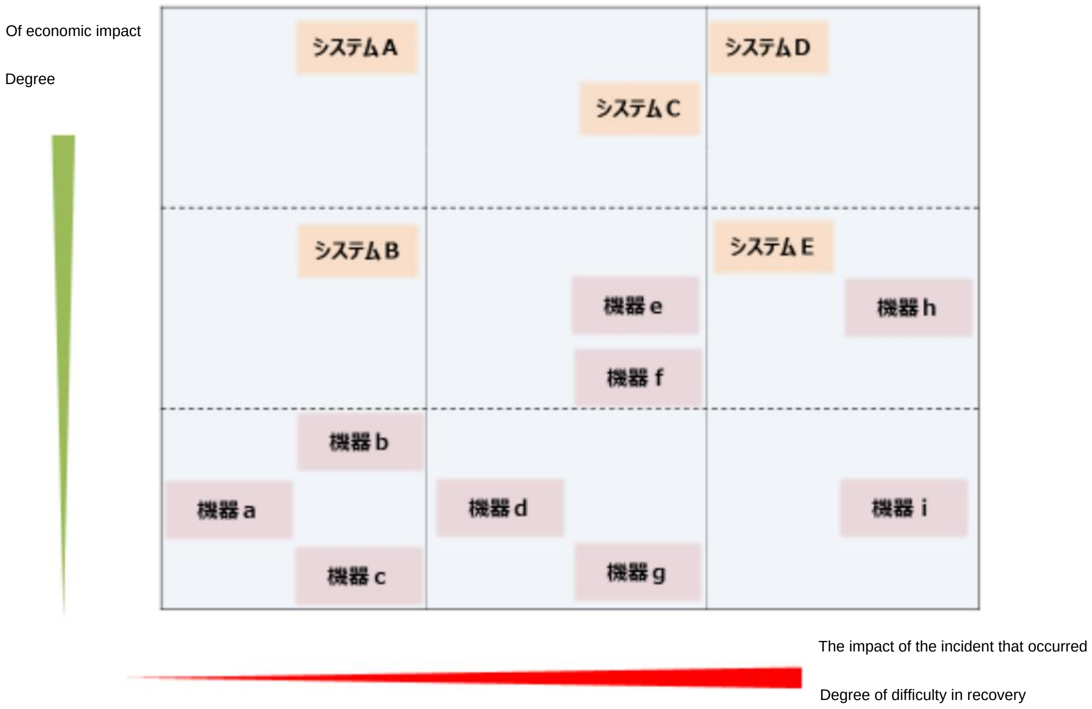

Figure 5 Image of categorization of devices and systems that connect physical and cyber

(* The mapping destination may differ depending on the usage pattern, etc., even for the same device / system. For example, there may be a case where the device g and the device h are the same device but have different usage patterns.)

3-3 Arrangement of required security and safety requirements

As described in 3-2-3 above, devices and systems that connect physical and cyber by utilizing the 1st and 2nd axes. Can be categorized based on the risk, but this alone is a new mechanism. It is difficult to consider specific measures for accepting services as a society. Therefore, this frame At MWORK, we comprehensively organize security measures for devices and systems that connect physical and cyber systems. To make sense, we set the third axis from the perspective of required security and safety requirements.

The third axis is orthogonal to the plane formed by the first axis and the second axis, and constitutes a so-called three-dimensional structure. And the viewpoint of security and safety requirements for each category organized by the second axis It plays a role of showing.

The third axis organizes the methods for ensuring security and safety from the following four perspectives. To.

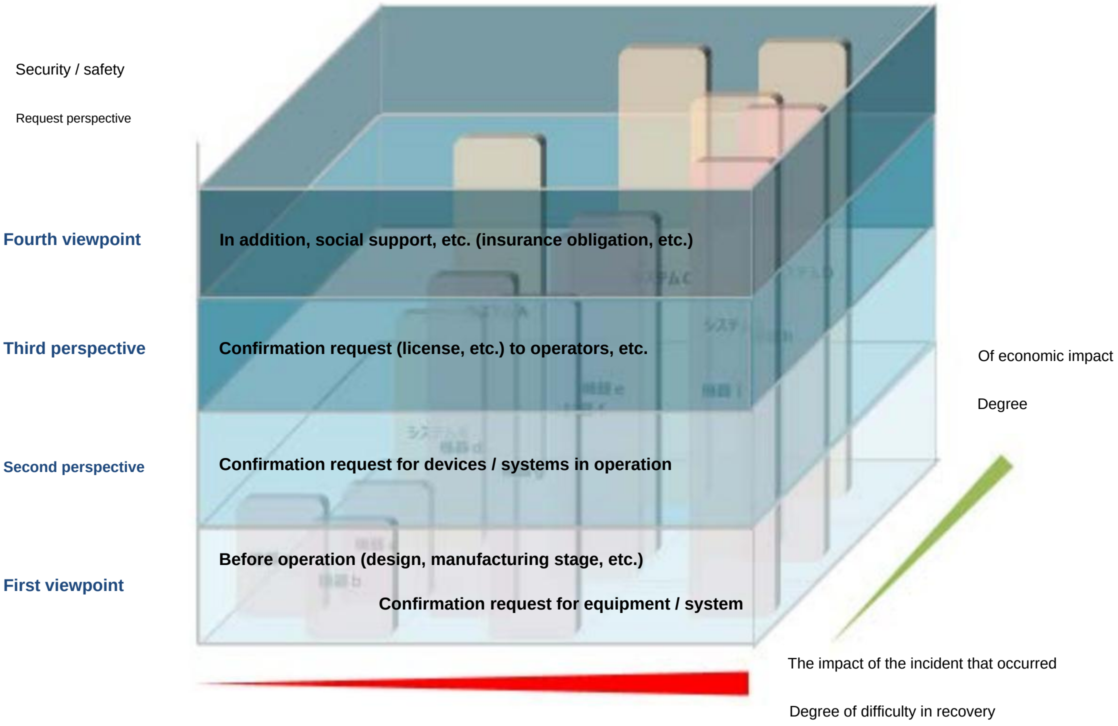
Security / safety
Request perspective
Fourth viewpoint
In addition, social support, etc. (insurance obligation, etc.)
Third perspective
Confirmation request (license, etc.) to operators, etc.
Second perspective
Confirmation request for devices / systems in operation
First viewpoint
Before operation (design, manufacturing stage, etc.)
Confirmation request for equipment / system
Of economic impact
Degree
The impact of the incident that occurred
Degree of difficulty in recovery

Figure 6 Image of security and safety requirements required according to category

3-3-1 First viewpoint: Equipment that connects physical and cyber before operation (design, manufacturing stage, etc.) System confirmation request

The stage before the equipment and systems that connect physical and cyber are manufactured and actually used. Therefore, the equipment / system itself must have necessary security / safety measures, or this Capabilities required by producers, suppliers, inspectors, and in some cases production equipment / factories of the equipment / systems, etc. It is required to confirm that the force conditions are satisfied.

Regarding security and safety measures, when the supplier sets the contents by himself / herself and in laws and regulations, etc. Therefore, it may be forcibly set. Also, those who confirm that the contents are satisfied There are various forms of law, such as self-declaration of conformity and certification by a third party, and the required confirmation level is required. The actual confirmation method will be set based on the expertise and objectivity of Le.

3-3-2 Second viewpoint: Request for confirmation of devices / systems connecting physical and cyber in operation

Even if you check the implementation status of security and safety measures before operating the equipment / system, it will be issued during operation.

Unexpected questions due to breakdowns that occur, software updates and maintenance that are carried out, etc.

The subject may occur. Started operation to check if such a problem has occurred

Later, it is required to check the equipment / system while considering the life cycle and service period.

Is.

A higher level of security and safety as it is a security and safety measure during operation.

It will be possible to secure it. On the other hand, whether the owner / operator of the equipment / system is involved, or the equipment / system

It is necessary to meet the conditions such as the ownership and control right of the system remaining on the supplier side, and it is a certain fact.

In order to request the treatment, each stakeholder should clarify the role and the demarcation point of responsibility.

It is necessary to prepare a social mechanism. The inspection here is also a voluntary inspection.

It can take various forms such as inspection by a third party.

3-3-3 Third viewpoint: Request for confirmation regarding the ability of the person who operates and manages equipment and systems

The impact of incidents caused by misuse or misoperation of equipment / systems is the security factor.

-A person who operates and manages equipment and systems when the level is not acceptable only with measures against footage.

Make sure that the equipment / system has the necessary capabilities to operate and manage it properly.

Will be required. For example, in the case of a car, the driver has a certain level of skill and knowledge.

We are seeking a driver's license to prove that we are doing so, and if an incident occurs, it will have a large impact.

However, we are building a social system that accepts technology that brings great social benefits as a society.

To.

The operator here does not directly operate the system like the service provider.

Can also include things.

3-3-4 Fourth viewpoint: Requests for other mechanisms such as social support

If an incident occurs, the impact will be very large, and the owner of the mechanism, etc. will be individually compensated.

If it is not easy to deal with the above, do not require insurance in advance.

Which social safety net is required.

For example, in the case of a car, ask the person who owns and drives the car to obtain a driver's license.

In addition, it is obligatory to take out automobile liability insurance, which is compulsory insurance. to this

Even if the driver who caused the accident does not have enough resources, the minimum amount for the victim

We are building a social safety net so that compensation can be made.

The four viewpoints on the third axis are not necessarily completely independent. example For example, in order to avoid the occurrence of incidents due to misuse or misoperation by the user, from the third viewpoint Is it appropriate to realize it by confirming the ability of the person who operates and manages it, or use it before sales from the first viewpoint Is it appropriate to oblige users to provide information such as how to use the equipment / system? It is necessary to consider based on the characteristics of. How to provide information such as usage It is also necessary to consider improving accessibility to that information. Also, not all The requirements from the viewpoint are not required, for example, even if there is no requirement from the second viewpoint, the first and third viewpoints are not required. It is also conceivable to configure countermeasures according to the requirements related to the above viewpoint. In addition, it takes time to take measures from a certain point of view. If so, it can be assumed that it will be temporarily supplemented from another point of view. Multiple stakeholders, as in this example -Because it is possible to deal with related risks from multiple perspectives, it is possible for related stakeholders to deal with them. Each stakeholder visualizes and shares information related to the risks of equipment and systems. It is necessary to comprehensively consider and agree among stakeholders through methods such as. Followed Of course, direct measures for equipment and systems are important, but all single stakeholders are involved. There is no need to deal with all the requirements, and within a certain point of view, the specific requirements that are essential in all cases. It is difficult to uniformly seek the provisions of various requirements.

Furthermore, each viewpoint is set based on the difference in the way of thinking about security and safety requirements. There is only one individual security and safety measure that is specifically required even from the same point of view. Not like. Therefore, if the viewpoint and contents of security / safety requirements are converted into costs, Categories where only security and safety requirements up to the second perspective are required, and up to the fourth perspective When comparing costs with all the categories for which security and safety requirements are required, the former It should be noted that the strike is not always low. In addition, the implementation of measures is directly related to the cost. Therefore, what kind of measures should be taken to meet the required security and safety requirements is determined. It is appropriate to make a decision after considering the likelihood of dents.

Organize specific security and safety requirements from each perspective in detail in each field By doing so, it is possible to make this framework more elaborate.

Four. How to use this framework

Various new mechanisms and services will be created by connecting cyberspace and physical space in the future. It is expected that it will be created in various ways. The entity trying to realize the service makes use of this framework

By using it, the equipment / systems are based on the risks hidden in the equipment / systems that connect the physical and cyber systems.

Categorize the system and grasp the viewpoint of security and safety requirements required for each category.

It will be possible to grasp and compare between categories. This makes it possible to consider it in a separate process.

However, the security and safety required for each device / system that supports new mechanisms / services

It is possible to ensure the consistency of the viewpoints and contents of tee measures to a certain extent.

At that time, it is important to note that incidents occur depending on the application of IoT devices and systems.

It means that the content and magnitude of the effect of doing so are different.

In other words, this framework is uniquely security and safe for a specific device / system.

It does not determine the viewpoint of the tee request, but it is an insi from the user side of the mechanism / service to be realized.

Appropriately analyze the effects of dents, categorize them according to the 1st and 2nd axes, and then categorize them.

Appropriately consider the viewpoints and contents of security and safety requirements by utilizing the third axis according to the category.

It is a framework for this.

In order to make effective use of this framework, we will continue to organize use cases and use it as the first axis.

While refining the categorization method based on the 2nd axis, the 3rd axis will be accumulated by accumulating use cases.

It is required to create an environment where the viewpoints and contents of security and safety requirements can be compared.

To. Therefore, in the future, based on this framework, specific mechanisms and services will be used as use cases.

A company that highly integrates cyberspace and physical space where IoT is widely used.

We will promote the development of institutional measures to appropriately implement security and safety measures at the association.

It is necessary to prepare the basic conditions for this.

Five. reference

This framework is taken in Part I and Part II of the Cyber Physical Security Measures Framework.

Based on the summarized three-layer structure, it was created with reference to documents such as the following standards.

• Cyber Physical Security Framework (CPSF) Ver1.0

Cyber Security Division, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry April 2019

• Cyber Physical Security Measures Guidelines for Building Systems 1st Edition

Industrial Cyber Security Study Group Working Group 1 (Institution / Technology / Standardization) Building Subworking Group June 2019

- IoT Security Guidelines Ver1.0

  IoT Promotion Consortium, Ministry of Internal Affairs and Communications, Ministry of Economy,

  Trade and Industry July 2016

- ISO / IEC 20924: 2018

  "Information technology — Internet of Things (IoT) — Vocabulary"
  December 2018

- ISO / IEC 27001: 2013

  "Information technology — Security techniques — Information security management systems — Requirements
  "October 2013

- IEC 61508: 2010

  "Functional safety of electrical / electronic / programmable electronic safety-related systems" April 2010

- IEC 62443-2-1: 2010

  "Industrial communication networks --Network and system security --Part 2-1: Establishing an industrial automation and control system security program" November 2010

- IEC 62443-3-3: 2013

  "Industrial communication networks --Network and system security --Part 3-3: System security requirements and security levels" August 2013

- ETSI EN 303 645 V 2.1.1

  "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements"
  ETSI
  June 2020

· REGULATION (EU) 2019/881 (Cybersecurity Act)
European Parliament and Council April 2019

- SB-327 "Information privacy: connected devices"
  California

September 2018

-Cybersecurity Framework Version1.1
NIST
April 2018

- NISTIR 8200
"Interagency Report on the Status of International Cybersecurity Standardization for the Internet of Things (IoT) "
NIST
November 2018

- NISTIR 8228
"Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks"
NIST
June 2019

- NISTIR 8259
"Foundal Cybersecurity Activities for IoT Device Manufacturers"
NIST
May 2020

- NISTIR 8267 (Draft)
"Security Review of Consumer Home Internet of Things (IoT) Products"
NIST
October 2019

- NISTIR 8276 (Draft)
"Key Practices in Cyber Supply Chain Risk Management: Observations from Industry"
NIST
February 2020

- White Paper "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF) "
NIST
April 2020

- Code of Practice for Consumer IoT Security

UK Department for Digital, Culture, Media & Sport
October 2018

- Internet of Things (IoT) Security Policy Platform Statement
  Internet Society (ISOC) IoT Security Policy Platform
  November 2019