August 1, 2016
1st Edition

Concept for security

~ What is needed when considering the security of the Internet ~

1. Introduction

The Internet is now critical, indispensable and basic global platform to distribute and share any digital information for all social and private activities. In business operation and in a variety of communication in business, the consideration and implementation of the best use of the Internet is critical and fatal for any single company to continue and to growth in their business.

On the other hand, leakage of customer information, management of company's business information, management of privacy information or fraud by malicious third party attacks is getting of large social interest. Therefore, the recognition of the importance of appropriate design and its implementation of security measures in every single organization has been increased. This is especially important and critical for the organization such as a private company and the sufficient security implementation is their mandatory corporate governance and management.

Security is likely to have the image of "a difficult one", but the most important point and action for the security implementation is to keep thinking "how effectively we use the Internet infrastructure, safely". Keep thinking in our/your mind about "how to implement safer environment" is the important action in order to approach to the essence of "Internet" security and to implement it.

We must remember and realize that security problem is not resolved by someone, security problem is resolved by the cooperation and collaboration among all the related stakeholders[1]. Also, "self-help is the first, mutual assistance is the second, and public assistance is the last" is most important concept and practice for us. As for "mutual assistance", the practical implementation of the vertical collaboration and cooperation among equipment and software vendors, service providers and

[1] This is called as "Collaborative Security" defined by ISOC (Internet Society): http://www.internetsociety.org/collaborativesecurity

users and the horizontal collaboration and cooperation among vendors, providers and users is important.

The purpose of this document is stimulating and encouraging the discussion about the guideline to use the Internet safely by anyone. We believe that when all the stakeholders related to the Internet improve the quality of security and trust of their own system and collaborate/cooperate with all the operators related with their system, the quality of service and trust provided by “you” is improved and it leads to the improvement of “your” market competitiveness. In the following sections, we discuss “idea of the underlying concepts in considering the Internet security”, step-by-step.

2. Background and object of this document

Since the Internet is universally popular and deployed, ensuring the Internet security has become a major and critical issue in order to protect the day-to-day of our lives. However, the followings are the reality of and frequent implementation of practical situation in many companies and organizations.

- ✓ Too rigid and strict security policy is applied to and implemented, then the activities of people is sadly inhibited
- ✓ Simply think that "disconnecting from the Internet provides safety", and neglecting mandatory measures of security

These approaches are very dangerous idea in today and in future, for the society which is premising on the provision of connectivity to the Internet and for the organizations which has a risk of information theft by insiders. This trend seems to be frequent and be typical in the industries, which start to use and start to be connected to the Internet significantly, such as the IoT (Internet of Things).

We have to improve “withdrawal type of society and organizations”, and hope that the Internet will continue to contribute to the sustainable innovation of society. In this document, we show the basic idea for the Internet security, and we would like to support your practical implementation. We may think the followings would be examples how to use this document by some organization.

- ✓ Distribute the document to organization members, so as to share the basic idea and direction for the improvement of security
- ✓ Deliver a guideline, which is adequate to your organization, with detailed

and concrete description focusing in your organization, after the consideration and modification on this document

The Internet has been widely adopted and used in our social and industrial activities, and has created “global digital economy”. There has been a lot of cyber security discussion and has been delivered some guidelines. However, since the region and area where the Internet technology is adopted and used is significantly expanded by the accelerated digitization and globalization of our social and industrial infrastructure, a lot of new security issues come out in front of us.

The object of this document is stimulating and encouraging the discussion about the adequate common security guideline to preserve the design, the implementation and the operation of our future global social platform, as a referenced and discussion document. We do not think all the discussion or contexts described in this document are fit with your organization or with your community. Using this document, we hope you may find the contexts, which fit with your organization/community, or you may initiate concrete and detailed discussion and contexts for your organization/community, or may deliver new discussion item(s) and idea(s). Also, we hope, after the discussion triggered by this document, some documents, which is useful and valuable for each organization or each community, would be delivered.

- Assumed reader of this document

  All of Internet user

- Structure of following sections

In this document, at first, we describe the essence of security in the Internet. Then, we show it by the 10 of key points to be referred to, when you design and implement appropriate security measures in your organization.

3. Basic when you consider the Internet security

In considering the Internet security, the followings are important; to maintain the nature and characteristics of the Internet, to protect the confidentiality, integrity and availability of information, and to contribute to the sustainable and continuous innovations and development of the society.

The nature and characteristics of the Internet is listed, below:

- ✓ It is global and unique network on the earth
- ✓ There is alternatives and there are possible to be selected and be used
- ✓ Opportunity of challenges is preserved and encouraged
- ✓ Sustainable operation is mandatory and respected
- ✓ Everything, such as technology or operation, is transparent and open

The confidentiality, the integrity and the availability of the information are of the three major requirements for information security[2], and is intended to protect the information assets, such as companies and organizations from a variety of threats.

- ✓ Confidentiality: to be able to access to the information by only authorized persons
- ✓ Integrity: information held is accurate, keeping the state is complete
- ✓ Availability: to be able to access the information at any time when the authorized person is required

When there is a security implementation that meets the above requirements, everyone will be able to connect any device to the Internet with confidence.

4. The 10 basic key idea

In this document, we show the following 10 basic key ideas for the Internet security:

1. Thinking globally, implementing local measures
2. Respecting “practice principle”, than “fundamentalism”
3. Instead of restriction or enforcement , supporting the improvement activities
4. “Overprotection” causes rather the increase of risk

[2] For more information, refer to as “the concept of information security” by the Ministry of Internal Affairs and Communications (In Japanese):
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/executive/02.html

5. Instead of “to be enforced by someone” , aiming “want to do”
6. Security measures is the investment to quality improvement {and future}
7. Sharing of experience and knowledge of everyone
8. Protecting and supporting the person, who experiences cyber security incident, as a “victim” rather than “bad guy”
9. Preservation of “anonymity” and protection of “privacy”
10. Firstly self-help, next mutual assistance, finally public assistance

(1) Thinking globally, implementing local measures

Some of the security measures, to companies and individuals, are mandated by law, regulation or institutions defined by governments. The rules defined by government or delivered from culture are not the same, but can be different for each country. The computer networks of many organizations exchange the digital information across the national border over the globe by using the Internet or their private networks, and they must implement optimized security measures and systems across the country, where different rules are carried out. This means that the security measures must be designed and implemented, while having a global perspective and taking into account the constraints of each local region, with locally optimized solution.

(2) Respecting “practice principle”, than “fundamentalism”

The Internet, while always running, in response to a request from a user that changes from moment to moment, is an open system that is formed by the continuously evolving/innovating technology. From the beginning (even before the present), it is realized that the determination or the definition of the detailed and whole of technical specifications is impossible and irrational. This is the idea of the Internet, i.e., we should start from the implementable system based on rough consensus; rule of thumb in the Internet (This is called as BCP, Best Current Practice). In the Internet, with the intentional non-optimization, respecting the actually running system in the field with rough consensus architecture, we must continue the modifications, changes and innovations.

So as to understand this principle in the field of cyber security, we may suggest to capture this (Internet Security) as a process. It is not good idea aiming 100% of safety from the beginning. Individuals, organizations and society should constantly reviewing their security measures, and it can be said that it is

important to realize the continuous change of the IT system and of the Internet. .

(3) Instead of restriction or enforcement, supporting the improvement activities

Not good security will head in the direction of "patience, perseverance and productivity decrease". In contrast, the correct or good security head in the direction of "carefree, efficiency, productivity improvement" and provided "the possibility of innovation."

Even in the same security measures, if well utilized in positive thinking, it can be transformed into a growth strategy. Specific means (weapons) is also the same, different "strategy", it will spawn a different effect.

Internet security is required "for innovation", it must be designed and implemented to provide an environment that can accept atypical activity. In its implementation, "enforcing" or "restricting" something should be avoided as much as possible. It is the most important thing to cheer and to encourage the vitality improvement of activity.

(4) "Overprotection" causes rather the increase of risk

Too strict regulations lead to not only its high implementation cost, but also may conduct the formation of the back door(s) and the black market, and also will increase the risk against the change of environment. Thus, the regulation of appropriate security should be appropriate severity and should intentionally have a kind of "play-room" in the system.

In other words, too strict regulations will provide a "too safe" environment to the people who live and the activities in this inappropriate environment[3]. Then, it leads to end up of undermining respect to a change of the environment. For example, in an office which is of completely isolated environment from the outside, people may have misconception that security measures is unnecessary, and it will take away the opportunity to learn how to protect themselves from the employees. Therefore, in order that we are surviving species, the following conclusion is derived, i.e., there is a need to create a "not too safe" environment,

---

[3] In a factory, which is isolated from the Internet, the whole of the operation in the factory had been halt / suspended, due to a computer virus during the scheduled software maintenance procedure in the factory.

intentionally. This is one of the important features of the Internet, i.e., “ensuring and preservation of diversity by ensuring the alternatives and selectivity”.

The real risk is that, even the vulnerable status continues, the status without having a way to defend them even with the imminent danger continues.

(5) Instead of “to be enforced by someone”, aiming “want to do”

Even with the same technology or even with the same security measures, it can be transformed into a growth strategy (as we mentioned in item 2), if well utilized it with the positive thinking.

The achievement by us (i.e., human-beings) with enforced activities will be in general small. However, in the case where their specific activities will contribute to the improvement of the value and activities of the quality of their organization, community or society, their activities goes to of autonomous and enthusiastic.

Even though it is difficult to generate profits in normal circumstances, we need to implement the necessary security measures in order to make sustainable our activities even in an emergency or even in a new environment.

(6) Security measures is the investment to quality improvement {and future}

Security measures should be defined as the collaborative improvement of the quality to ensure safety and security, by all the stakeholder of the Internet. By carrying out any kind of “security QC activities” in their respective positions, such as the Internet infrastructure, various services offered on the Internet, or the products and devices connected to the Internet and by the collaborative involvement of all people involved in the Internet business/operation, the improvement of quality of the Internet is achieved and can build a safe and secure Internet.

In addition, if it is possible to consider the security and quality by us, you and we can build the insurance and compensation system even in the case of damage caused by the failure of the product, which is beyond its capability. Some legal treatment could be applied to against the services or products with poor quality. In order to build such a society, the establishment of practice and concept for the security with the collaborative security concept for all the people must be premised.

In other words, the promotion of security measures in the companies and organizations is not by moral and by social responsibility, but it should be achieved by the incentive of the improvement of the quality of services. And, it should be regarded as the important investment for the expansion and of their current and future business.

(7) Sharing of experience and knowledge of everyone

Experience and knowledge of the incidents should be shared with the outside of people and in its organization. By sharing those information, we can generate the opportunities among all stakeholders, including the Internet security experts, to share the latest security incidents. It is very important to provide and to share a chance, so as to prevent and mitigate the damage caused by the similar or the same security incident.

In other words, we want encourage to all of you "to raise your voice to share your experiences", since it shall contribute to the society so as to improve our security measures against the security risk. Yes, we must respect and encourage the braveness of people who put their unhappy experience to be shared in the public domain. .

(8) Protecting and supporting the person, who experiences cyber security incident, as a "victim" rather than "bad guy"

One of the reasons, why the incident victims may want to hesitate to share their experience and knowledge, would be because that the public opinion tends to chase or criticize their responsibility or their potentially inappropriate counter measure against the incident(s).

Arts and behavior of the attackers in cyber space are changing every day. Therefore, it is almost impossible to achieve a zero possibility, in general, even when the victim may take the possible security measures that are likely to be sufficient. We are, with the exception of the cases, such as that incident of the victim had intentionally failed to sufficient security measures, should them to "protect and support", also respects them is the act of sharing a third party and experience you should.

There is no sense to blame them, since they are the victim. Rather, the degradation of their incentive to share and to implement their security measure is a loss and a risk of our society. As we widely shared, in case of the accident

investigation of aircraft, it is well recognized and is well performed the disclosure and the sharing of any information to prevent next/future accidents. We should pour our force and power so as to prevent a recurrence by them, rather than punish them. .

(9) Preservation of "anonymity" and protection of "privacy"

In many basic disciplines such as constitution, in many countries, the protection of "privacy/secrecy of communication/correspondence" and "freedom of expression" is defined as basic right and thing we must preserve. The information, that we must protect, is contents of communication and identification of communicator. In order to protect these information, we should aggressively adopt available new technologies, such as encryption technologies, and rules.

It is commonly recognized that we need user authentication for cyber security. However, from the point of view of a broad sense of security, "anonymity", which does not recognize a user, is necessary and play an important role. Then, as an example, for telecom operators, even if the contents of the user communication are visible, making use of its contents is strictly prohibited. Even the contents are related with terrorism and crime, the protection of the confidentiality for these communications must be mandatory.

Even in an organizational management, anonymity is considered as something essential so as to ensure that the accused does not become impossible for inappropriate conduct and for other incidents. How to implement and operate "suggestion box" or "opinion box" is one of examples. We must avoid the case where the accused person is subject to retaliation and revenge by accusation. In other words, we must guarantee the accused person is not subject to retaliation and revenge from the people that make up the organization or from the organization the accused person belongs. In order to guarantee the above operation, we need "anonymity".

The protection of contents in communication and identification of communicator is mandatory from the view point of the protection of privacy, including the protection of individual information. Since the protection of privacy may lead to the inconvenience to use the Internet by every single individual or by organization, we have to have sustainable and continuous discussion and rule adaption, which appropriate to corresponding circumstance.

(10) Firstly self-help, next mutual assistance, finally public assistance

As well as natural disaster response, the idea of “self-help, mutual assistance, and public assistance” should be well recognized in the Internet security measures. The self-help is that each person, using the Internet, protects their own safety by himself/herself. Mutual assistance and is that protecting the safety by mutual help by every person in each region and in each business segments. Lastly, the public assistance is that the government or public institutions protect the safety of every citizen as a part of the public service.

As a matter of course, there is a limit to the user each person’s knowledge and time, only by the self-help security measures does not work well. The mutual assistance is necessary and needed to supplement the part of security that cannot be covered by self-help. And, even with the mutual assistance, we need a public assistant to fill the missing parts.

Taking the filtering (to restrict the access to harmful Web site) as an example, the responsibility to implement this should belong to the end user. However, a user can delegate the operation of content filtering to the trusted third party, that can be a kind of mutual assistance (and public assistance), by the user's responsibility.

This is exactly one of the basic principles of the Internet. This is the concept of “end-to-end”, leading to the transparent infrastructure, that end node can deliver advanced features without some inappropriate enforcement or restriction by organization or by government.

5. Summary

The Internet is now critical, indispensable and basic global platform for global digital economy and distribution and share of digital information for all social and private activities on the Earth. And, the Internet is recognized as the critical and mandatory resource to achieve our sustainable growth. According to the aggressive development of global digital economy premising the existence of the Internet, the framework and guideline of cyber security to achieve the safe use and operation of the Internet seems to be changing, significantly. For example, in some organizations, since they blindly adopt higher restricted rules to reach to higher security level and maintain this direction, the efficiency of organization is going to be degraded or new challenges are discouraged or inhibited. We may think we

should re-consider “what is the purpose of security?”, so that security acts should enable the introduction of new challenges, on technologies or on organization structures and operation, which contribute to the sustainable growth of organization, while considering “Security measures is the investment to quality improvement {and future}”.

In the Internet, the practical and transparent measures for local operation, while considering the global perspective and collaborating/cooperating with global system, shall be autonomously adopted in each organization or in each community. As for security measures, while premising “Firstly self-help, next mutual assistance, finally public assistance”, we think that the security measures, that aims the support and encouragement of the challenges for the growth and improvement of their activities, should be established and applied with the coordination/collaboration/cooperation by all the related stakeholders, while avoiding “overprotection” result to the increase of security risk and the “preservation of anonymity” and “protection of privacy” to achieve sharing of experience and knowledge.

We hope that this document contributes to the stimulation or encouragement of the discussion, which leads to the establishment of appropriate guideline and the implementation of security measures for the future global digital economy and society premising the existence of the Internet.

Authors

This document was developed by volunteer participants of Internet Governance Conference Japan (IGCJ) in the three face-to-face meetings and in the online discussions.

Participants (in alphabetical order):

Eiko Akashima
Kazuki Aranami
Hiroto Asaoka
Hiroshi Esaki
Tomohiro Fujisaki
Seiji Homma
Hirofumi Hotta
Yasuo Igano
Moto Kawasaki
Koichiro Komiyama
Akinori Maemura
Hiroyuki Minami
Osamu Nakamura
Tomoko Nezu
Tatsuya Osaki
Yuri Takamatsu
Toshio Watanabe
Shin Yamasaki
Makoto Yokozawa

Disclaimer

This document is a translation from the Japanese version of the document: セキュリティに対する考え方 (http://igcj.jp/meetings/concept-for-security.pdf). The translation is for informational purposes only, and is not a substitute for the original document. If a discrepancy is found between original and this translated document, the original document always supersedes.

Rights and Permissions