FUJITSU Security Initiative

● Taishu Ohta

We are now 15 years into the 21st century and entering an age of uncertainty that was unthinkable in the past. As information and communications technology (ICT) is utilized as social infrastructure and use of the Internet is increasingly widespread, safe and secure operation of ICT is strongly desired. Security has conventionally been seen mostly from the perspective of accidental leakage of personal information and preventive measures. However, the growing frequency of cyber attacks means that ICT-related organizations must now embrace the fact that security incidents are bound to occur. This paper presents the FUJITSU Security Initiative, which systematizes this new concept of security. It also describes three technical requirements in particular that need strengthening and Fujitsu's approach to doing this. We intend to establish safe and secure operation of ICT by working with organizations to ensure that they understand these requirements and take steps to meet them. In addition, as we are now in an age in which the Internet of Things (IoT) is quickly being implemented and data is becoming even more valuable, we also aim to help realize a society in which both safe and secure operation of ICT is ensured.

1. Introduction

Japan's Personal Information Protection Act, enacted in April 2005, was intended to provide society with an optimal solution that struck a balance among confidentiality, convenience, and productivity in information and communications technology (ICT), but this came at the expense of convenience and productivity for many organizations. In addition, the internal controls and disclosure system for financial products transactions established in 2008 by the Financial Instruments and Exchange Act of 2006 (commonly referred to as J-SOX), which established countermeasures against corporate fraud, further diminished the positive effects of ICT while promoting standard management practices.

However, security-related incidents such as the accidental leakage of personal information have continued unabated, and since 2011 targeted cyber attacks have become particularly problematic. Society has come to realize that information security cannot be preemptively established and that security-related incidents are bound to occur. This will affect the optimization of ICT operations and the formation of an infrastructure that ensures service continuation.

This paper introduces Fujitsu's approach to security. It describes three requirements for strengthening system security—security intelligence, privacy protection, and full authentication—and presents new ideas on supporting operations toward business continuity.

2. Current state of cyber attacks

At the beginning of the 21st century, the dissemination of information had become extraordinarily easy thanks to the spread of the Internet and the proliferation of personal computers. Indeed, the use and application of information had evolved far beyond what was capable in the past. At that time, security measures centered about annoying attacks called "viruses," and investments in anti-virus countermeasures were made in an ad hoc manner when and where needed.

Japan's Personal Information Protection Act of 2005 compelled companies to implement a variety of preventive measures, but information leaks nevertheless continued to occur, giving senior management a

cause for concern. Then, on the basis of analyzing new cases of information leakage, companies were asked to construct internal control systems from the viewpoint of compliance. Since many mechanisms underlying corporate governance had much in common with security management, awareness of the costs involved in implementing security measures took root.

In terms of internal risks, many organizations have held the assumption that "employees and people are basically good" and that they would be protected from external threats by the law. However, the rapid development and expansion of ICT in recent years has brought changes to internal risks and made it difficult to respond effectively to external attacks. In addition, the failure to prevent internal corporate fraud and the escalating amounts of damage caused by cyber attacks has revealed the limits of conventional countermeasures.

The Stuxnet malware discovered in June 2010 was a turning point in attitudes toward cyber attacks as they finally came to be viewed as a new type of threat to the Internet society. Since then, cyber attacks between nations as well as those mounted by organized crime for monetary profit have escalated, and many incidents have occurred in Japan as well as a result of cyber attacks from outside Japan. Still, there are many managers who optimistically think that everything is fine in their organization despite the daily occurrence of security-related incidents and the fact that there is no technology that can completely block cyber attacks. These are the challenges facing ICT today.

It is vitally important that everyone concerned is aware that ICT-related risks need to be handled as an element of corporate governance and that strict security-related operations need to be implemented as part of an appropriate investment strategy.

3. New approaches

Company managers have come to depend on ICT to achieve business continuity and to create new value. This dependency on ICT means that companies will never be free of security problems that can change from day to day. Consequently, management must recognize that security is not a short-term investment in countermeasures against cyber attacks but something that must be continuously implemented and adjusted to match the risks currently faced by the organization.

The approach to cyber attacks from the viewpoint of business continuity is shown in **Figure 1**. This diagram shows the need for a prior response (preparations) to bring the business restoration curve after a crisis occurrence to a minimum business level and the need for crisis management to bring the curve back to the standard business level at an early stage compared with no countermeasures for cyber attacks. This type of response is similar to risk response in the case of natural disasters and equipment failure. However, opportunities exist for sensing the risk of a cyber attack before a crisis occurs, so it is possible to prevent the crisis from occurring in the first place by responding appropriately to the signs of an impending incident. Sensing these signs is a challenge, and this is where innovation can play a role.

As an ICT vendor, Fujitsu is committed to solving this security problem by demonstrating the benefits of optimizing operations through techniques that can be used as reference and by recommending processes for developing technologies essential to those operations.

The concept of the FUJITSU Security Initiative is shown in **Figure 2**. This is an ongoing initiative for achieving safe and secure ICT from the customer's perspective to promote innovation in the customer's business and for co-creating with customers a secure intelligent society through three key elements. Specifically, this concept is centered about "operations," which reflects the need to build up optimal operations in an organization. An important part of this concept is the idea that "products and services" needed to

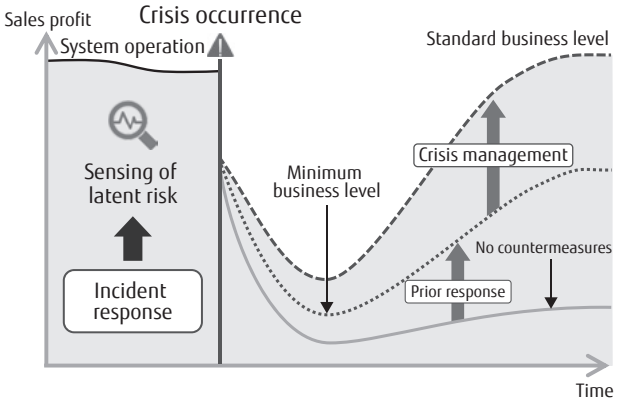

Figure 1
Approach to cyber attacks from viewpoint of business continuity.

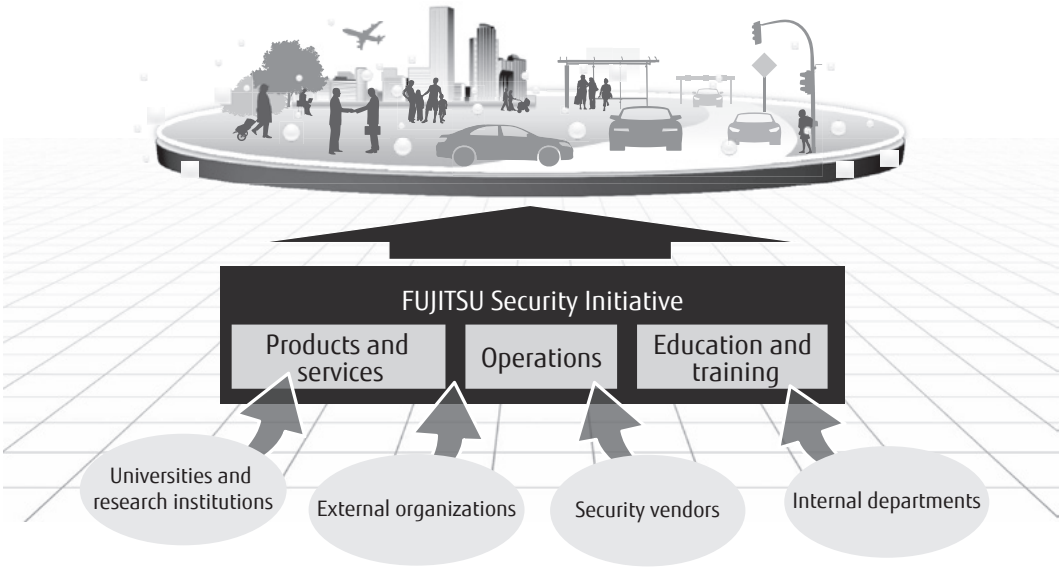

Figure 2
Concept of FUJITSU Security Initiative.

achieve these operations be selected appropriately and that the requirements of safety, confidentiality, and availability be met. However, simply introducing products and services will not in itself achieve satisfactory risk management and emergency response capabilities. Personnel with at least a minimal amount of knowledge and experience are needed for achieving appropriate operations. Ongoing "education and training" for developing human resources and improving competence in crisis management are therefore considered to be another important part of this concept. Fujitsu is continuously striving to develop innovative operations based on this concept. Several of the efforts being made in this regard are described in other papers in this issue.

4. Technology strategy

The Internet of Things (IoT), which will enable ICT to be used in an "anytime, anywhere, anyone, and anything" manner, continues to evolve. By 2020, we will be in an era in which more than 50 billion devices are connected to the Internet and mutually accessible. Amid this interconnection of diverse devices and sensors and the creation of value by utilizing the data that is generated, effective handling of cyber attacks will be needed to enable ICT to be used in a safe and secure manner.

Against the above background, Fujitsu considers that three technology areas need to be strengthened while fostering innovation in ICT operations with an eye to the future (**Figure 3**).

1) Security intelligence

This is a new technology area that has arisen to deal with the threat of cyber attacks, which have become a major security problem. The aim is to respond rapidly to an attack through the consolidation and application of knowledge and through security operations that change in response to changes in threat conditions.

2) Privacy protection

This area makes use of anonymization and encryption technologies to minimize or eliminate damage at the time of an information leak. In contrast to neutralizing the behavior of cyber criminals, privacy protection aims to nullify the effects of an attack while facilitating the effective use of information.

3) Full-range authentication platform

The construction of a reliable authentication and permission platform that connects the real world and cyberspace will enable accurate access control, optimization at the service provision level, and early discovery and blocking of unauthorized use. This, in turn, will help to prevent internal corporate fraud, facilitate the discovery of cyber attacks, and enable the effective use of forensic information (evidence). In short, a full-range authentication platform will enable an accurate

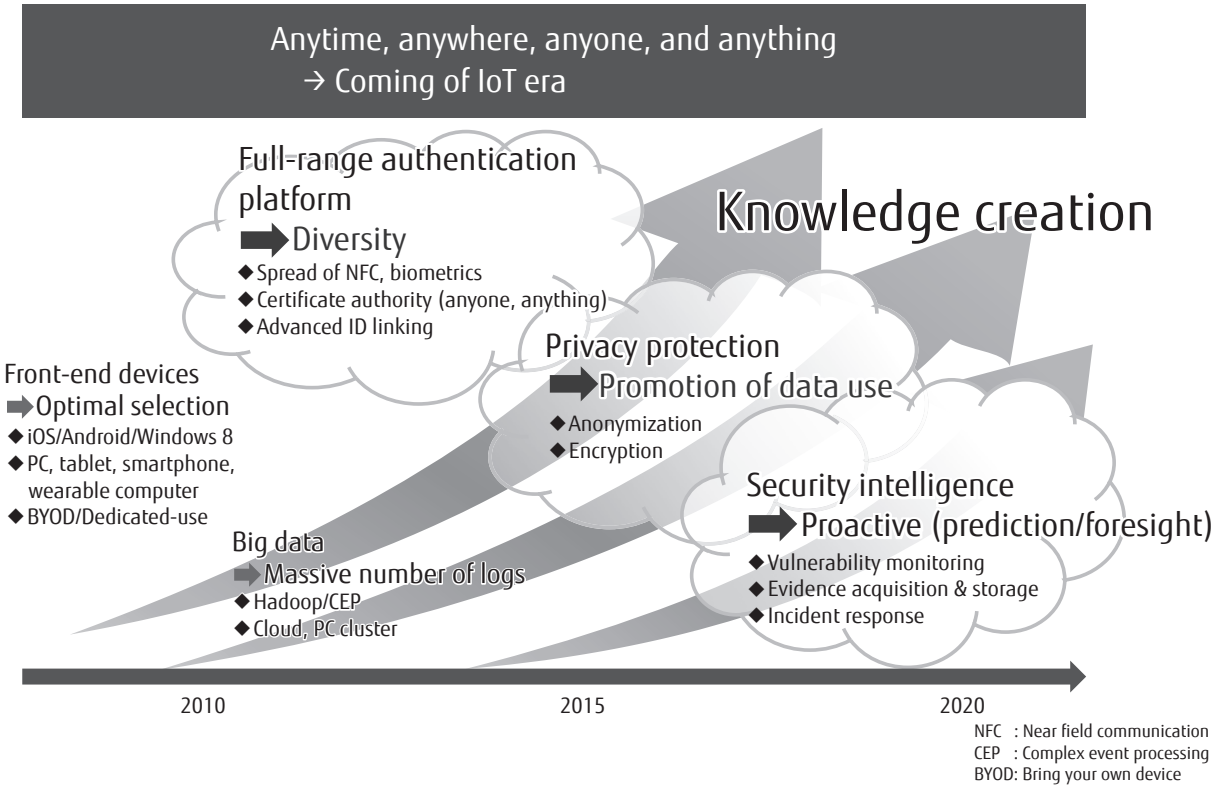

Figure 3
Strengthening of security toward the future.

assessment of current conditions and an appropriate crisis response.

Fujitsu has accumulated experiences and knowledge through ongoing security-related improvements using its own ICT security operations as reference and has decided to return this valuable knowledge to society. It also aims to play a leading role in ICT operations in the IoT era by making even more improvements in these three technology areas through ongoing technology development and provision of products.

5. Technology challenges

This section introduces techniques for solving the problems discussed in "Current state of cyber attacks" above and new technologies for achieving these techniques in the order that they appear in this issue.

1) Authentication technology

The use of ICT by the end user has quickly shifted from personal computers to smartphones and tablets. However, security in the use of ICT is still weak at the ID and password level. With this in mind, organizations and service areas that incorporate at least two-factor authentication or biometric authentication have started to emerge. Fujitsu has taken up the challenge of constructing an economical and safe authentication platform that combines a variety of constraints (time, place, device, organization role) as needed. The plan is to adopt palm vein authentication as a platform that will enable anyone to access all sorts of services at any time with accurate authentication while satisfying the need for both convenience and safety.

Furthermore, in conjunction with the distribution of ID cards for Japan's "My Number (Individual Number)" social security and tax number system that began in January 2016, Fujitsu is completing preparations toward the spread of an identity authentication platform that will be tied to public identity documents that serve as a basis for various types of authentication platforms.

2) Privacy protection, encryption technology

Data plays a major role in ICT through cloud computing. There is a need, however, for new technologies that can support privacy protection and the safekeeping of confidential information. In response to the My Number system, Japan's Personal Information

Protection Act, and the EU General Data Protection Regulation, Fujitsu has established technologies such as *k*-anonymization and homomorphic encryption to enable the safe use of personal data, which represents personal information (name, address, age, etc.) and private information (location information, route information, purchase history, etc.) and has begun to provide solutions incorporating these technologies. In addition, its achievements in leading-edge encryption technologies that make it extremely costly for cyber thieves to convert data stolen in a cyber attack into useful information are introduced in the paper "Leading-edge Cryptography" in this issue.

3) Security intelligence

Cyber attackers, who have an overwhelming advantage, use technical advances for criminal or antisocial behavior. It is therefore important that much information on threats be collected from all sectors of society and that preparations be made to counter new threats. An effective solution is to implement a system that can handle anticipated future risks and attacks. This means that management must stay on top of the latest developments in the ICT being used and continuously test the appropriateness of its responses to threats.

A commonly used mechanism that reflects current ideas on information collection is to detect attacks and incursions at gateways in and out of the Internet. At the same time, security intelligence, which identifies threats by performing correlation analysis on a large quantity of ICT operation logs and then mounts an effective response to those threats, is coming into use. This approach facilitates the analysis of attack patterns and incursion techniques and enhances technologies for determining well-defended conditions and vulnerabilities to incursion. It provides, in short, effective intelligence to counter cyber attacks. While cyber attacks cannot be completely prevented, it has become possible to discover internal incursions after an attack and to thwart their expansion. We can expect the application of such capabilities to many ICT operations in the future, thus providing even more advanced intelligence.

In addition to tackling the challenges in the three technology areas described above, Fujitsu has begun to address the need for training personnel in security-related development and operations. The Ministry of Economy, Trade and Industry predicts a shortage of about 80,000 security engineers in 2020, which reflects the increasing importance of developing and training security personnel in the development and operation of ICT. How to discover and secure new personnel in this field is a major problem facing society, and in response to this dire situation, Fujitsu launched a Security Meister Certification System in fiscal year 2014 to support the training of its engineers. There are many ways of finding new personnel such as by offering financial incentives or hiring new graduates, but at Fujitsu, we have placed more importance on recruiting and training personnel from within the company. This, we believe, is the optimal solution for achieving ongoing cooperation with customers in dealing with the threat of cyber attacks and associated operation problems that will continue as long as ICT exists. In this regard, we would like to provide our education and training know-how to our customers and contribute to personnel development throughout society.

6. Conclusion

To enable the safe and secure use of ICT in an age of uncertainty, Fujitsu has completed preparations to enable its customers to use in diverse ways the technologies and know-how it has accumulated through in-house practices. At present, however, it is expected that cyber attacks will be more sophisticated in the future, so there is a need for security-related technologies to evolve even further.

Fujitsu places importance on operation practices and technology research through the co-creation and sharing with customers of intelligence pertaining to security operations and the formation of an efficient system throughout society. I would like to close this paper by promising to promote innovation in our customers' security environments, including the training of next-generation security engineers.

Taishu Ohta
Fujitsu Ltd.
Mr. Ota is currently engaged as a security evangelist in promoting the value of security to customers and managing in-house feedback related to social issues.