

Rebalancing convenience and security to contend with 2025

[Summary]

- Due to the unexpected advent of COVID-19, many companies and organizations **had their workers begin working remotely. They had never expected to have to work in such a way. As a result, the balance between convenience and security was lost.**
- To promote the sustained growth of companies and to encourage flexible ways of working, in anticipation of the approaching contactless society, the current state of the balance between convenience and security must be reviewed (hereinafter referred to as “rebalancing”). **If this rebalancing is not done, businesses may be significantly affected by reduced productivity, the occurrence of cyber risk events, and other matters.**
- In 2025 we will face major technological challenges, including the “2025 Digital Cliff”¹ for IT systems and the end of support for Windows 10 Pro. In addition, in 2025 a new age will begin, in which stakeholders will say that one cannot manage a company if one does not understand digitalization and security. Consequently, “plus (+) security human resources” will be sought by executives. As such, **if we do not urgently begin the rebalancing of convenience and security, it may become too late for us.**²
- When JCIC conducted interviews and literature surveys to investigate company trends, it discovered great variation in the ways companies thought about convenience and security control. If we analyze their principles and philosophies on digitalization, **each company can be classified as one of four types** (Fig. 1). Each division and department of a company can also be classified as a type in the “Model of the balances between convenience and security.”
- IT security managers and others can use the “Model of the balances between convenience and security” to understand their company’s current situation, and then take the necessary measures to ensure consistency with their company’s future management strategy. If this step is taken, it should be easier for everyone at a company to agree which type their company will aim to become in the medium to long term. As a result, such aims as “productivity improvement” or “customer satisfaction improvement” will be achieved under the work-from-home environment. **The objective of this report is to support you to formulate strategies such as working style changes, digital transformation (DX), and security management for the future.**

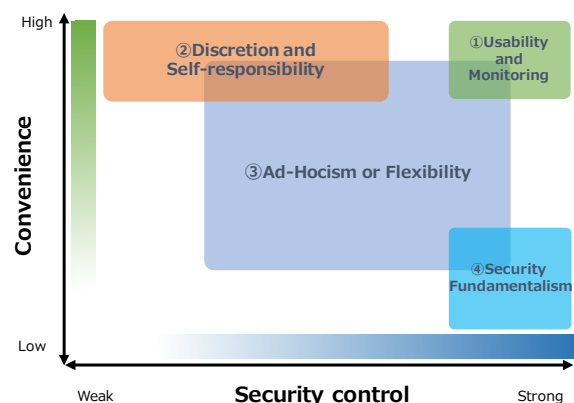


Figure 1: Model of the balances between convenience and security

¹ The Ministry of Economy, Trade and Industry’s “Report on Digital Transformation (DX)” states that existing systems are aging, becoming overly complex, and becoming “black boxes,” and that if these matters are allowed to continue until 2025 without our intervention, they will hinder DX and risk incidents such as information leaks, besides magnifying economic losses. The report states that we must begin intensively updating systems if we want to overcome the “2025 Digital Cliff.”

² From JCIC reports *Corporate Cybersecurity Disclosure Report*, *Shortfall of Human Resources and its Solutions: Plus (+) Security Human Resources*, and *Offensive Plus Security Human Resources*.

1. Introduction

In the midst of COVID-19, many companies and organizations had their workers begin working remotely. They had never expected to have to work in such a way. As a result, the balance between convenience and security was lost. As companies rapidly implemented remote working, those that prioritized convenience faced higher risks of becoming targets of cyber attacks and internal crimes. Conversely, companies that implemented excessively robust security measures must deal with the “backdoor” use of IT systems. It may become routine for employees to work from a personal computer at home, from necessity, using an unauthorized cloud service. If there is no rebalancing of convenience and security, businesses may be significantly affected. This report sets out an idea for rebalancing convenience and security, with the period after the COVID-19 pandemic in mind.

The intended readers of this report are mainly IT security managers (CISO, department heads, etc.). But everyone involved in the management of their company is encouraged to read it: directors, corporate auditors, the management team, and staff in corporate planning, risk management, information systems, human resources, general affairs, and finance. We hope it will be helpful as you prepare your strategies for such projects as changes to working style, digital transformation (DX), and security management, in preparation for the future.

2. When the balance between convenience and security is lost, businesses are significantly affected

The Japan Smartphone Security Association (JSSEC) conducted a survey.³ When asked whether the promotion of remote working to prevent coronavirus infections had changed the way in which remote workers handle confidential information, more than half of the respondents answered “There is no change from before” (the gray area in Fig. 2). Another 14% of respondents answered that “There is now a stricter handling of confidential information” because of the promotion of remote working (the light blue area in Fig. 2). Another 24% of the respondents answered that “There is now a more relaxed handling of confidential information” (the orange area in Fig. 2). In other words, as increasing numbers of general affairs departments and temporary workers begin to work remotely, some companies have chosen to prioritize security and others to prioritize convenience.

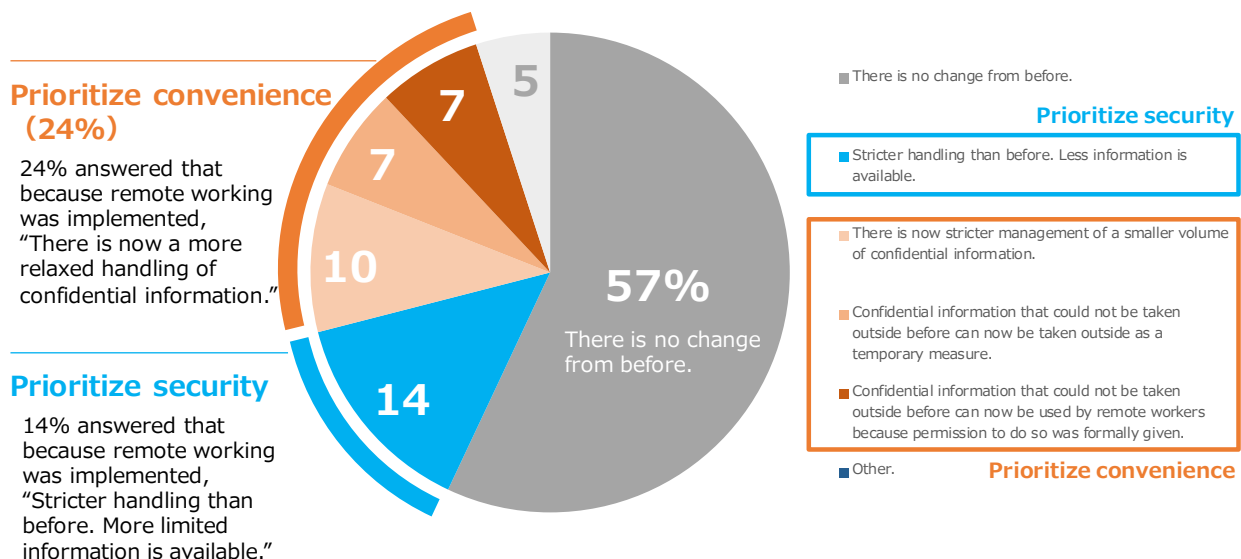


Figure 2: Changes in handling of confidential information, prompted by remote working

³ Japan Smartphone Security Association (JSSEC), *A report on the survey on the situation of remote working and security (n = 432 persons)* (July 2020), <https://www.jssec.org/report/20200722.html>

3. The “Model of the balances between convenience and security”

How should companies assess the balance between convenience and security? Seeking an answer, JCIC conducted company interviews and literature surveys. We found great variation in the ways companies thought about convenience and security control. When we analyzed each company’s principles and philosophy on digitalization, we learned that companies can be classified into four types. The model thus created is called the “Model of the balances between convenience and security.” Each division and department of a company can also be classified as a type in this model.

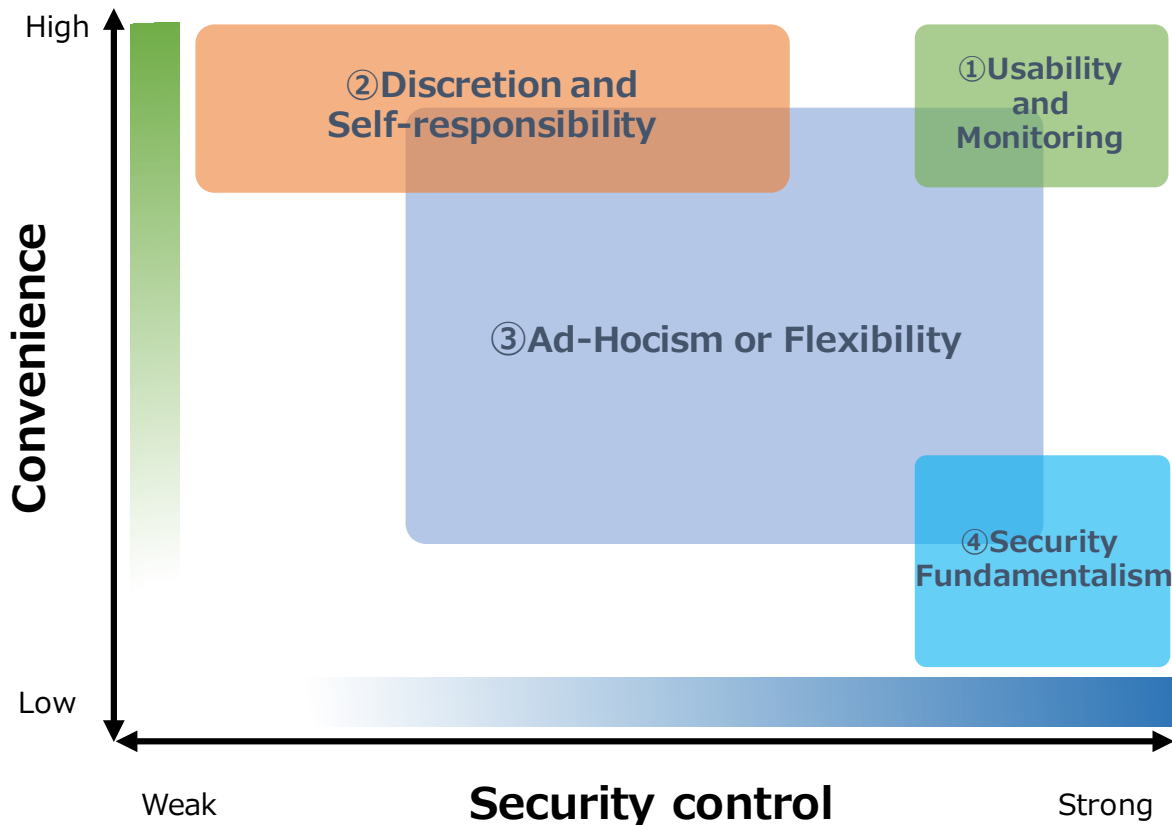


Figure 1: Model of the balances between convenience and security (reposted)

The horizontal axis in Fig. 1 indicates security control. The further to the right a company is located, the more its management prefers stronger security. The vertical axis indicates convenience. The higher on the vertical axis a company is positioned, the more convenience it prefers to give its employees. For example, companies of the Discretion and Self-responsibility type (2) prefer high convenience and tend not to make security management too robust. Type (4) Security Fundamentalism companies prefer robust security management and are somewhat tolerant of low convenience.

The sizes of rectangles (1) to (4) indicate each type’s range of tolerance of convenience and security control. The overlapping parts denote a type with a preference somewhere between the preferences of the two distinct types; there are such companies. The white spaces indicate areas preferred by very few companies.

The characteristics of and points about the four types are summarized in Fig. 3. All four types have pros and cons, and the most suitable choice differs from company to company. It is the thinking of the company’s management that will determine which type a company should aim to become, and the direction it should take. However, one effective method is for the IT security manager to approach management and seek its involvement in discussions about which type the company should become. We encourage IT security managers to use this model of the balances when formulating medium- to long-term policies.

	Characteristics	Points to be aware of
① Usability and Monitoring	<ul style="list-style-type: none"> Although employees are comfortable, their activities are monitored. Internet businesses and IT companies are of this type. 	<ul style="list-style-type: none"> Because this type must constantly respond to the newest trends, it must possess considerable resources (i.e., people and money).
② Discretion and Self-responsibility	<ul style="list-style-type: none"> Although the company establishes minimum standards of conduct, employees are given a high degree of freedom. Companies with creative cultures. 	<ul style="list-style-type: none"> The risk of insider crime is high. The risk of becoming a victim of an internal crime is high.
③ Ad-Hocism or Flexibility	<ul style="list-style-type: none"> Can flexibly deal with matters not covered by its security policy. Many companies are of this type. 	<ul style="list-style-type: none"> In matters not covered by its security policy, it tends to be slow to make a decision. Tends to act on a case-by-case basis.
④ Security Fundamentalism	<ul style="list-style-type: none"> Closed IT network and system Companies of highly-regulated industries and many critical infrastructure businesses. 	<ul style="list-style-type: none"> Has difficulty carrying out DX and working style reform. Has difficulties when responding to a crisis, such as an occurrence of infections.

Figure 3: Characteristics of each balance type, and points to be aware of

- Usability and Monitoring type companies attempt to achieve high degrees of both convenience and security management. IT companies are examples of this type. Although employees can work comfortably and freely anytime, anywhere, using any device, their activities are continuously monitored by the company. Such companies must constantly respond to new technologies and changing trends. They must therefore possess vast resources (i.e., people and money). If a company decides to become this type, it must strongly commit itself to that policy. Changing policies midway will reduce either the degree of convenience or the degree of security management.
- Discretion and Self-responsibility type companies prefer high convenience and tend not to make their security management too robust. This type of company establishes minimum requirements for employee conduct but allows high flexibility. Companies with creative corporate cultures tend to be of this type. In other words, they rely on the judgements of their employees, who are the parties concerned. They face a higher risk of an information leak due to a cyber attack, and of an internal crime where an employee intentionally takes information outside the company.
- Ad-Hocism or Flexibility types are companies that have no consistent policy for convenience and security management, or companies that balance them depending on the situation as a result of trial and error. Many Japanese companies are of this type, but they tend to make case-by-case judgments and so tend to take longer to make decisions. Companies wishing to become this type must make themselves aware of the disadvantages.
- Security Fundamentalism type companies prefer robust security management and are somewhat tolerant of low convenience. They do not provide laptop computers and work smartphones to all employees, but allow only some employees to work remotely. Many public organizations and important infrastructure businesses, which are heavily regulated, are of this type. This type has difficulty in carrying out DX and working style reform, and in responding to a crisis, such as the occurrence of infections.

4. Examples of efforts at balancing convenience and security

This section introduces some examples of efforts to balance convenience and security. Note that it describes in part the efforts that companies are making, and does not classify entire companies into the four types.

Example 1: The efforts of Nihon Unisys to rebalance business continuity and security⁴

Nihon Unisys is a system integrator. It builds systems that Japan's information society and industries rely on. The company was already in the process of creating an environment in which all group employees can safely use its internal system from outside the company. Responding to the spreading coronavirus, from February 2020 Nihon Unisys encouraged remote working and staggered work hours. From April 2020 it made remote working the normal arrangement for all group employees, and allowed only those employees who had permission to work at the office.

By advancing digitalization, the company made remote workers able to do work safely that previously could not be done by them. Nearly 90% of all employees were set to work remotely. The company first assessed the various risks, such as employees carrying around personal computers, working at home, and using their home networks. It assessed the risks of remote working by employees of cooperating companies, and the increased need of cloud services. It then took the necessary measures before implementing remote working.

Currently, Nihon Unisys is creating and implementing a platform for cybersecurity measures that is based on the concept of zero trust, which it had been working on in accordance with its cybersecurity strategy, and it is doing so at a greater speed than before. The company has positioned this platform for cybersecurity measures as the security measure necessary for the new working styles brought about by the coronavirus catastrophe.

Example 2: Yahoo! Japan establishes an unrestricted remote working system allowing 10,000 people to work remotely⁵

On October 1, 2020, Yahoo! Japan introduced an "unrestricted remote working system." It does not limit how often an employee can work remotely and has no flextime-based core period. The company had already implemented remote working in 2014. However, due to the effects of COVID-19, it made remote working a general rule. This new system was established as a result of the company formally adopting the emergency system to deal with the coronavirus catastrophe as its new working style. About 10,000 employees, of whom several thousand are employees of subcontractors and temporary workers, will work remotely.

In starting its unrestricted remote working system, Yahoo! Japan strengthened the recording of the operation log for each device. The company had been recording operation logs, but less strictly than it is doing now. Strict recording was implemented because once remote working is implemented, the risk of internal crimes increases, where employees intentionally take information out of the company. Operation logs can also be used to prove the innocence of an employee accused of doing something. The company does not allow privately-owned personal computers to be used ("bring your own device"; BYOD). Only personal computers that the company has lent to employees are able to access the company's internal system. An ID, a password, and another element are required to log in to its internal system.

Through unrestricted remote working, the recording of operation logs, and strong authentication, Yahoo! Japan is seeking a good degree of both convenience and security management. It is doing so because it thinks that certain information must be protected to the maximum degree, but for other types of information, the risks caused by convenience of working should be accepted to a certain level.

Example 3: LISA, Netflix's unique security approach⁶

Netflix provides video streaming services, such as of movies and dramas. It owns no servers and relies 100% on the cloud. Its guiding principle is LISA, its unique location-independent security approach. LISA requires the company to stop believing it is safe inside the boundaries of the office network, and to check every time the reliability of the user authentication and the device, so that resources can be safely used from anywhere. In short, LISA is the Netflix version of zero-trust

⁴ From *Nihon Unisys Group Integrated Report 2020*, <https://www.unisys.co.jp/invest-j/ir/pdf/ir2020.pdf> and interviews

⁵ ITmedia; "Yahoo! Japan built an unrestricted remote working system", <https://www.itmedia.co.jp/news/articles/2010/03/news019.html>

⁶ <https://www.usenix.org/conference/enigma2018/presentation/zimmer>

architecture.⁷ Netflix has developed its own software and released it free of charge to implement its approach to security. The company has made public its Netflix Content Security Best Practices⁸, which it recommends its content partners adopt. The best practices include the principle of minimum authority (example: zero trust) and multi-factor authentication (MFA).

The CEO of Netflix believes that its growth is underpinned by the “no-rules management of it that gives freedom and responsibility to the employees.”⁹ In accordance with his management philosophy, he has made Netflix 100% reliant on the cloud, has established LISA, and has given security recommendations to content partners.

Due to security concerns, local governments have implemented only limited remote working¹⁰

According to a survey on local governments’ introduction of remote working, conducted by the Ministry of Internal Affairs and Communications in March 2020, only 51 (3%) of Japan’s 1721 local government bodies had introduced remote working. The other 97% (1670 organizations) had not introduced it, and only 139 (8%) of them were considering doing so.

The most common reasons for local governments not to introduce remote working were: “Worried about how to ensure information security” at 80.6%; “Creating rules for labor management is difficult” at 78.8%; and “The cost of introduction is a burden” at 62.8%. In other words, three factors—fear of information leaks, not wanting to spend time and effort devising rules, and having no budget—are preventing local governments from adopting remote working. Further, in the local governments that have introduced remote working, three out of four part-time employees are not considered eligible for remote working. Thus, these local governments are not experiencing the full benefits of remote working.

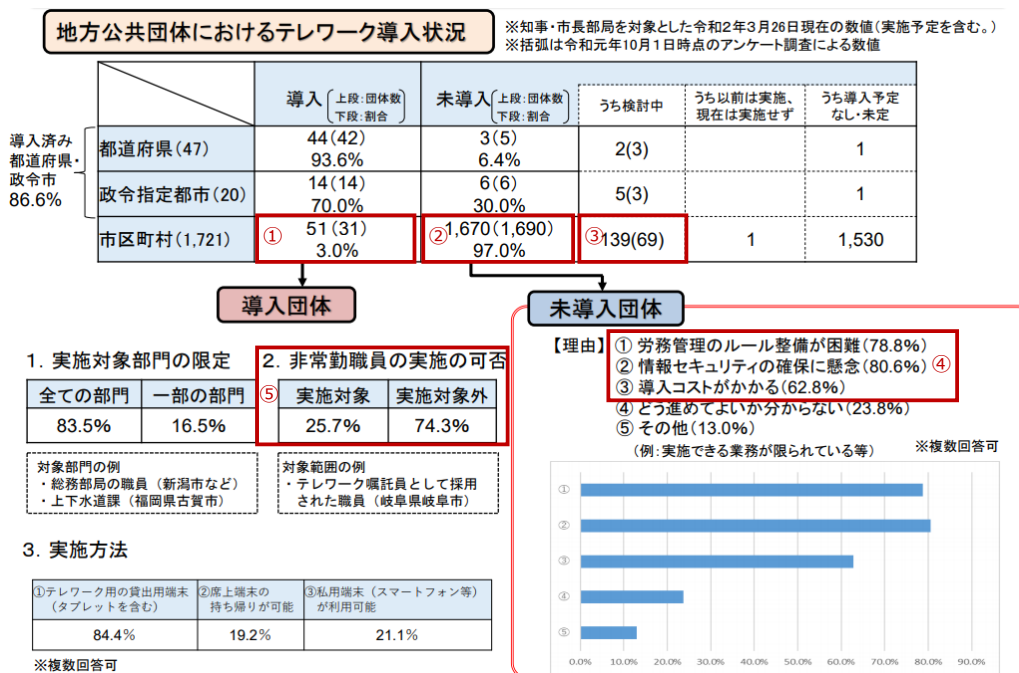


Figure 4: Status of the efforts for remote working local governments are making

⁷ A concept denoting taking security measures under the assumption that nothing can be trusted. This method never trusts users’ requests, performs verifications each time, and provides minimum access to corporate resources after granting access. The National Institute of Standards and Technology (NIST) released its definition in August 2020.

⁸ Netflix Content Security Best Practices: <https://partnerhelp.netflixstudios.com/hc/ja/articles/360001937528>

⁹ The 22nd Nikkei Global Management Forum: <https://www.nikkei.com/article/DGXMZO66027930Q0A111C2000000/>

¹⁰ Ministry of Internal Affairs and Communications, “Efforts for remote working made by local governments”, https://www.fdma.go.jp/laws/tutatsu/items/200630_syoukyu_188.pdf, and the Nikkei, “Local government employees are remote working refugees”, <https://www.nikkei.com/article/DGXMZO64142990T20C20A9000000/>

Fig. 5 shows some other samples found by JCIC’s research. There are companies that can be simultaneously classified as being of two types, and they are comparable to companies located in the overlapping parts in Fig. 1.

- When implementing remote working, with the exception of type (4), Security Fundamentalism, all types, all employees, and all temporary workers are eligible for remote working, as a general rule.
- Companies classified as type (1), Usability and Monitoring, and type (2), Discretion and Self-responsibility, allow the use of BYODs. The former type requires employees to install a dedicated app that does not allow sensitive information to be left on privately-owned devices, but the latter type does not require employees to install such an app.
- As for the use of web conferencing systems such as Teams, Zoom, and WebEx, type (4) Security Fundamentalism companies require employees to obtain permission each time they hold a remote meeting, if they are using a system other than that specified by the company. All the other types place no restrictions on the web conferencing system, as long as it is done via browsers.
- In monitoring employees, type (1), Usability and Monitoring, and type (3), Ad-Hocism or Flexibility companies tend to rigorously record operation logs (event logs) of personal computers and mobile devices, and security logs. They tend to monitor constantly. Type (2), Discretion and Self-responsibility, and type (4), Security Fundamentalism companies generally record logs but tend not to be rigorous about continuous monitoring. The former type likely behaves in this way because it lacks resources, and the latter type because it does not consider the monitoring of logs to be important, already having strong security.
- If a decision must be made on a matter not covered by the security policy (for example, the temporary unauthorized use of cloud storage), type (2) Discretion and Self-responsibility companies tend to leave the decision-making to the concerned party’s manager. Type (4) Security Fundamentalism companies in principle do not permit decisions to be made about matters not covered by their security policy.

Type	Efforts for remote working	Use of privately-owned devices for work (BYOD)	Web conferencing types	Employee monitoring	Decisions about matters not covered by security policy
①Usability and Monitoring	All employees and all temporary workers can work remotely, in general	Permitted (must install dedicated app)	No restrictions as long as web conferencing is done via browsers	By recording device operation logs and other logs, have strengthened monitoring	Consult with the IT security department
②Discretion and Self-responsibility	All employees and all temporary workers can work remotely, in general	Permitted (no restrictions)	No restrictions as long as web conferencing is done via browsers	Logs are recorded but constant monitoring is not done	Establishes a minimum standard of conduct at the beginning
③Ad-Hocism or Flexibility	All employees and all temporary workers can work remotely, in general	Not permitted	No restrictions as long as web conferencing is done via browsers	By recording device operation logs and other logs, have strengthened monitoring	Consult with the IT security department
④Security Fundamentalism	Has not introduced remote working, or only some employees can work remotely	Not permitted	Must obtain permission each time if using a tool other than that specified by the company	Logs are recorded but constant monitoring is not done	Not permitted in principle

Figure 5: Typical efforts made by companies of each balance type

5. How to use the Balance Model

A questionnaire to determine a company’s type is shown in Fig. 6. First answer the four questions about convenience and count the number of “yes” answers (A). For a question that applies only to a part of a company, a “yes” answer is counted as 0.5. Then answer the four security control questions and count the number of “yes” answers (B). Place the number of “yes” answers to convenience questions on vertical line (A), and to security questions on horizontal line (B). In addition, Ad-Hocism or Flexibility can be determined by question (C).

Convenience questions (vertical line)	Answer
Management is committed to maximizing employee productivity and provides sufficient resources.	Yes / No
Allowed to access critical data by BYOD (Bring Your Own Device) as long as the rules are followed.	Yes / No
When a matter not covered by your organization’s security policy is encountered, a decision is made in a short period of time.	Yes / No
Remote working is permitted in many departments, and in the remote working environment, employees can work the same way they did at the office.	Yes / No
The number of yeses (If applied to only a part of the company, counted as 0.5)	# of Yeses A

Security control questions (horizontal line)	Answer
Has established a guiding principle of convenience and security, and is willing to devote considerable resources to implement the guiding principle.	Yes / No
Critical data is strictly controlled and cannot be technically taken out.	Yes / No
Centralized management of operation logs and security logs for devices accessing the internal system, with immediate alerts for unauthorized accesses.	Yes / No
A security policy has been established and reviewed based on the results of regular risk assessments.	Yes / No
The number of yeses (If applied to only a part of the company, counted as 0.5)	# of Yeses B

Determination of Ad-Hocism or Flexibility	Answer
For new needs or changes, follow established rules to determine acceptable risks and get an approval of revised policy by management.	Yes / No C

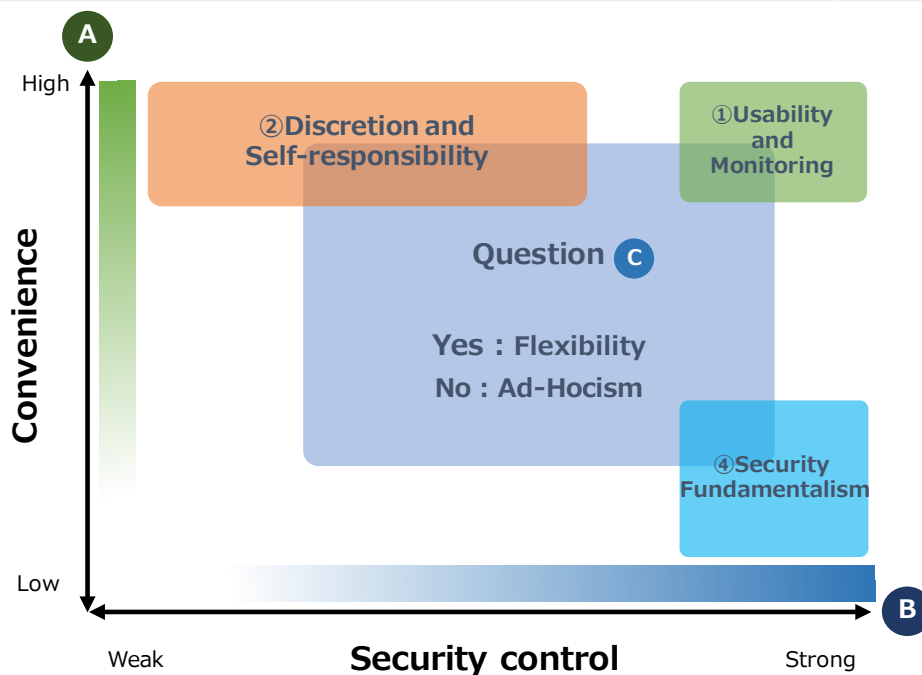


Figure 6: Determining balance type

After identifying which type your organization is, follow the instructions below to use the balance model.

1. Understand how your company's strategy will change.
2. Follow Figure 6 to identify your organization's type.
3. Decide on the balance type that your company prefers for the medium to long term, and obtain the agreement of those inside your company. (Examples are shown in Fig. 7.)

In particular, when deciding on the balance type you prefer for the medium to long term, it is important that your choice is consistent with your future management strategy. Each type has its pros and cons, and there is no best type in common, so it is the thinking of your company's management that will determine your company's type. However, one effective method is for the IT security manager to approach management and seek its involvement in discussions about which type the company should become. A company may choose to become one that can be classified as being in two balance types simultaneously. Besides considering which type a company should seek to become, considering which type each division and each department of a company should aim to become is also possible.

When agreement is reached within a company on the balance type it should be in the medium to long term, it becomes easier to make necessary provisions. For example, you can settle upon specific themes, such as rebuilding internal systems and networks, revising the security policy and rules, and reviewing internal processes. A plan for each theme can then be prepared and implemented.

The balance types that types (2)–(4) will most likely aim to become are as follows.

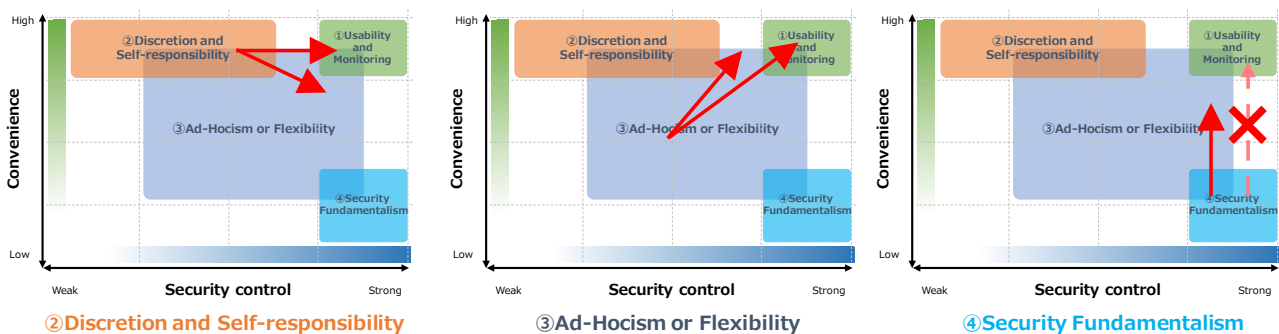


Figure 7: Types that each balance type typically aims to become

- There are two main types that a type (2), Discretion and Self-responsibility company will seek to become. It may choose to move closer to type (1), Usability and Monitoring, by strengthening security management while maintaining convenience. Or it may aim to become a type (3), Ad-Hocism or Flexibility company by partially restricting convenience and strengthening security management after an event such as becoming publicly listed.
- Type (3) Ad-Hocism or Flexibility companies will likely either opt to stay the same, and strengthen both convenience and security control, or seek to become type (1), Usability and Monitoring.
- Due to the corporate cultures of type (4) Security Fundamentalism companies and their stakeholders, such as their business partners, it is difficult for them to directly become type (1), Usability and Monitoring companies. The more realistic course for them is to seek to become type (3), Ad-Hocism or Flexibility, while maintaining strong security management.
- Although it is possible for type (1), Usability and Monitoring companies to relax either convenience or security management and seek to become another type, because very few are likely to do so, type (1) is omitted in Fig. 7.

5. Summary

In this report we explained an idea for rebalancing convenience and security, with the post-coronavirus era in mind. IT security managers and others can use the “Model of the balances between convenience and security” to understand the current situation of their company, and then take steps to ensure consistency with their company’s future management strategies. Afterwards, after proposing the desired type for the medium to long term, it should be easier to reach agreement on it inside the company.

We must undertake the rebalancing and begin operating under the revised balance by 2025, due to the “2025 Digital Cliff.” In 2025 the risks of information leaks will increase, and new personal computers will replace the old ones due to the ending of support for Windows 10 Pro. Thus, 2025 prompts rebalancing. As stated in JCIC’s Corporate Cybersecurity Disclosure Report, 2025 will be the start of an age when stakeholders will say one cannot manage a company if one does not have “an understanding of the benefits of digitalization for businesses” and “an understanding of the importance of security.” In other words, company managers must by then be “plus (+) security human resources.” To rebuild systems and networks on a company-wide scale will take at least two years; that is, to create a plan, secure a budget, and implement the project. For this reason, if we do not begin the rebalancing of convenience and security now, it will become too late.

Finally, we want to say that undertaking the rebalancing of convenience and security is a means and not the objective. Remember that the final goal is to realize the company’s vision, increasing sales and profits, improving productivity and customer satisfaction. In the post-coronavirus era, a rebalancing of convenience and security is necessary to achieve this goal.

Reference material 1: “Odds of survival” checklist

The following checklist will help you to determine whether you and your company or organization can survive in the post-coronavirus era. When JCIC asked its member companies, 83% fell into the category of “Have adapted to the New Normal” while 17% were in the category of “Needs review.” None answered that it “Needs immediate attention.” (36 respondents)

For each question, please choose the answer that is closest to how you and your company or organization think.

#	Category	Question	Answer
1	Management strategy	Your company’s management strategy and employees’ way of working has changed dramatically as a result of the coronavirus crisis	Y / N / Unknown
2		You can explain and provide to others an overview of your company’s management strategy	Y / N / Unknown
3	Business continuity plan	Even if another state of emergency is declared, because your company has further digitalized its processes and implemented remote working, its business will be less affected	Y / N / Unknown
4		Large-scale system shutdowns due to cyber attacks, etc., are included in your business continuity plan (BCP)	Y / N / Unknown
5	Customer value	You are digitizing your products and services so that they need not be provided face-to-face	Y / N / Unknown
6		Your products and services are digitized and are online, and your management understands the balance between convenience and risk	Y / N / Unknown
7	Employee value	Working is possible outside the office or not on-site, and start/closing time can be chosen to some extent	Y / N / Unknown
8		As a result of the promotion of remote working through the coronavirus crisis, the security policy and measures for management were reviewed	Y / N / Unknown
9	Information system	Your <u>information system</u> takes into account the balance between employee productivity and security	Y / N / Unknown
10	Products and services	Your <u>products and services</u> are balanced in terms of user convenience and security	Y / N / Unknown







Number of yeses	Odds of survival
0–3	Needs immediate attention 
4–6	Needs review 
7 or more	Have adapted to the New Normal 

Figure 8: “Odds of survival” checklist

Reference material 2: Convenience and security decision-making tool

Many IT security managers are probably troubled daily by having to make decisions about matters not covered by their company's security policy. The following table is a tool for making decisions about convenience and security.

This example considers the choosing of a user authentication method for a digital service of a company (such as a website for members). A particularly important point is that the effects and likelihood of security risks and user convenience are evaluated in a single table. You can use this decision-making tool to help stakeholders understand.

Matter to be considered		Choosing a user authentication method for a digital service of a company				
#	Choices	User convenience		Security risk		Notes
		Benefits	Convenience	Impact	Possibility	
1-1	Only ID and PW	Because this is a familiar method used by many websites, user convenience is high	○ Users can work without instructions		✗ Two or more incidents per year	To strengthen the authentication process, strict password policies are needed
1-2	ID and PW plus authentication by email 	Because two-factor authentication by email is gradually becoming common, many users have no trouble using it	△ Users must read instructions	△ Unauthorized access may cause customer information or sensitive information to leak	△ About one incident per year	If users are not allowed to use free email services, "Possibility of incidents occurring" is changed to "○"
1-3	ID and PW plus authentication by SMS 	Because two-factor authentication by SMS is gradually becoming common, many users have no trouble using it	△ Users must read instructions		○ Less than one incident per several years	Authentication by SMS is not strong, so users must be limited to have one account per user
1-4	ID and PW plus authentication by OTP 	Because OTP (one-time password) apps and devices are needed, user convenience is not high	✗ Users must be assisted by someone		○ Less than one incident per several years	Users must install dedicated apps or use dedicated devices

➔ The method that was chosen

Legend

Convenience

- ✗ Low: Users cannot work unless they are instructed by someone
- △ Medium: If users read and follow instructions, they can work
- High: In general, no instructions are needed and users can begin working right away
- ◎ Excellent: Because users can intuitively use it, work efficiency is maximized

Impact

- ✗ Large: The company suffers severe financial loss and loss of credibility
- △ Medium: Serious damage is suffered, and fines and financial losses may be incurred
- Small: Minor damage is suffered if it is revealed outside the company

Possibility of incidents occurring

- ✗✗ Extremely great: Two or more incidents per year, and perpetrators need no special technology
- ✗ Great: Two or more incidents per year; perpetrators must use special technology
- △ Moderate: About one incident per year
- Small: Less than one incident per several years

Figure 9: Convenience and Security decision-making tool

Reference material 3: Major events of 2025

Fig. 10 forecasts the major events of 2025 from four perspectives: politics, the economy, society, and technology.¹¹ In 2025 we will face an accelerated decreasing birthrate and aging population, which will affect workers' financial and labor burdens. To mitigate the impact, productivity must be improved through digitalization and automation, and the balance between convenience and security must be reviewed.

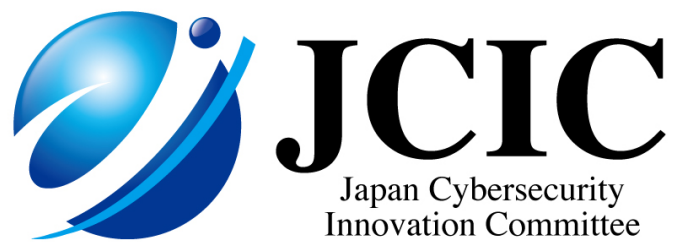
Politics	Economy	Society	Technology
The insurance premium per employee is about 30% of the annual salary	Cashless payments comprise 40% of all payments, which is double 2017 levels	Expo 2025 Osaka, Kansai	"2025 Digital Cliff" for IT systems
The age when men begin receiving employees' pension insurance benefits is raised to 65 years	Nationwide, more than 40 locations offer a service that provides automatic driving level 4 (unmanned autonomous driving)	One in four Japanese citizens is 75 or older (The 2025 Problem)	The end of the support lifecycles of Windows 10 (Home and Pro)
APEC in South Korea	Nationwide, around 320 commercial hydrogen stations exist	The world's population has increased to approximately eight billion	Problems occur in systems built during the Showa era; the "Showa 100 problem"
The EU accomplishes its Economic and Monetary Union (EMU)	NTT completes its transition to IP network from fixed-line network	In the EU and East Asia, populations tend to decrease	IoT devices reach 41.6 billion units and generate approximately 80 ZB of data

Figure 10: Major events of 2025

References

- Japan Smartphone Security Association (JSSEC) "Survey Report on Telework Status and Security" (July 2020), <https://www.jssec.org/report/20200722.html>
- Nihon Unisys Integrated Report 2020, <https://www.unisys.co.jp/invest-j/ir/pdf/ir2020.pdf>
- ITmedia, "How did you change Yahoo security measures that created an 'unlimited telework' system of 10000 people?" <https://www.itmedia.co.jp/news/articles/2010/03/news019.html>
- Netflix Content Security Best Practices, <https://partnerhelp.netflixstudios.com/hc/ja/articles/360001937528>
- 22nd Nikkei Forum, World Management Conference, <https://www.nikkei.com/article/DGXMZO66027930Q0A111C2000000/>
- "Telework Efforts by Local Governments" by MIC, https://www.fdma.go.jp/laws/tutatsu/items/200630_syoukyu_188.pdf and the Nihon Keizai Shimbun, "Local Officials of Telework Refugees", <https://www.nikkei.com/article/DGXMZO64142990T20C20A9000000/>
- NIST SP 800-207 Zero Trust Architecture, <https://csrc.nist.gov/publications/detail/sp/800-207/final>
- Social Premium, over 30% yearly in fiscal 25th, https://www.nikkei.com/article/DGXNASFS1602Z_W2A410C1MM8000/
- NRI-future tables 2020-2100, <https://www.nri.com/jp/knowledge/publication/cc/nenpyo/1st/2020/2020/2020>
- SMBC Nikko Securities 2025 Issue, <https://www.smbcnikko.co.jp/terms/other/N0003.html>
- IPSS United Nations World Population Estimate, <http://www.ipss.go.jp/publication/e/jinkomon/pdf/18557206.pdf>
- Windows 10 Home and Pro Support Lifecycle, <https://docs.microsoft.com/ja-jp/lifecycle/products/windows-10-home-and-pro> (See November 2020)
- IDC IoT Research (June 2019), <https://www.idc.com/getdoc.jsp?containerId=prUS45213219>

¹¹ PEST analysis is a method for understanding the trends of society from a macro perspective, viewed from these four perspectives.



[Inquiries about this study]
Kenji Uesugi, senior fellow: uesugi@j-cic.com

On using this material

- This material was prepared with the cooperation of JCIC members. Although this material was prepared based on the various data that was believed to be reliable at the time of preparation, JCIC does not guarantee its accuracy or completeness.
- This material is protected by copyright laws and all rights to it are the property of JCIC unless otherwise stated. When quoting, please clearly credit JCIC by including the following: "Source: Japan Cybersecurity Innovation Committee (JCIC)."
- [Contact us] info@j-cic.com