My Vision No.57
2021.12

Considering the Responsibilities of the Public and Private Sectors in the Face of the Increasing Incidence of Cyberattacks

With a rapid shift towards the greater use of IT in our daily lives (telework, online services, etc.) amid the COVID-19 pandemic, threats in cyberspace are becoming increasingly serious.
What is the current situation in this respect?

About This Issue

Urgent Countermeasures Required Against Cyberattacks in the Era of DX

- Fears of Catastrophic Impacts on Our Economy and Society -

Noriyuki Yanagawa
Executive Vice President, NIRA／Professor, Graduate School of Economics, The University of Tokyo

Against the background of a rapid shift towards the greater use of IT in our daily lives (telework, online services, etc.) generated by the COVID-19 pandemic, threats in cyberspace are becoming extremely serious. Not only are both the public and private sectors exposed to cyberattacks, but the level of threat is considered to differ from what we have experienced up to the present. What types of threat are we facing in cyberspace? What measures should we consider taking in response to these threats? In this issue of *My Vision*, we ask the opinions of experts at the front lines of cybersecurity.

Keywords…Digital transformation (DX), Practical measures, Development of professional human resources

Expert Opinions

Considering the Responsibilities of the Public and Private Sectors in the Face of the Increasing Incidence of Cyberattacks

What types of threat are we facing in cyberspace?
What measures should we consider taking in response to these threats?

Do Not Neglect Preparations for IoT Devices That Might Become the Starting Point for Attacks

Masahiro Murashima
Pen Tester, Ierae Security, Inc.

Keywords…Starting points for infiltration, Basic security measures, Certificate-based authentication

A Clear and Present Danger of Ransomware Attacks

Mihoko Matsubara
Chief Cybersecurity Strategist, NTT Corporation

Keywords…Ransomware, Colonial Pipeline, JBS, CISO

As Cyber Attacks Intensify, Japan’s Debate on Active Defense Must Accelerate

Ken Jimbo
Professor, Faculty of Policy Management, Keio University

Keywords…National Security, Loss of Life, Tallinn Manual, Active Defense

There Is an Urgent Need to Adopt Effective Measures in Anticipation of Organized Crime and Conflicts Between Nations

Motoki Nishio
Visiting Professor, Center for Rule-making Strategies, Tama University

Keywords…Organized crime attacks, Economic statecraft, State-backed attacks, Duty of care

Balancing DX and Cybersecurity

Akira Saka
Chief Information Security Officer (CISO), Digital Agency Japan

Keywords…Online activity during COVID-19 pandemic, Effect on decision-making processes, Cooperation between government agencies

Interview period：October, 2021
Interviewer：Sosuke Suzuki（NIRA Research Coordinator & Research Fellow）

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese. NIRA bears full responsibility for the translation presented here. Translated by Michael Faul.

Copyright © 2021 by Nippon Institute for Research Advancement

My Vision No.57
2021.12

About This Issue

Urgent Countermeasures Required Against Cyberattacks in the Era of DX

– Fears of Catastrophic Impacts on Our Economy and Society

Noriyuki Yanagawa
Executive Vice President, NIRA／
Professor, Graduate School of Economics, The University of Tokyo

The importance of cyberspace security has been pointed out for a considerable length of time. However, a variety of problems have arisen in this area of a quite different level to those encountered previously. Nevertheless, it seems that awareness of these problems is not yet sufficiently widespread in our society. In this issue of *My Vision*, we therefore asked experts to discuss the problems that cybersecurity is currently facing, and what they consider to be the important points.

Unprotected IoT Devices Amid Rapid Digitalization

Today, with the importance of digitalization (irrespective of whether in the public or private sector) being widely bruited and the term digital transformation (DX) coming to be frequently heard, the importance of safely managing digital data no doubt goes without saying. In particular, improving the security of data that is indispensable for business and data that is related to the safety of people's lives are urgent tasks. To take an example, if medical data was to be stolen or tampered with in a cyberattack, it could lead to serious situations that put lives in danger. In the future, as the networking of many pieces of equipment becomes more realistic with the IoT, it is easy to imagine the possibility that data tampering could cause catastrophic problems for companies and for society.

Masahiro Murashima, a pen tester for Ierae Security Inc., indicates that IoT devices will be important to the convenience of our lives and new services provided by companies, but warns that they may also be the starting point for cyberattacks. According to Mr. Murashima, the problem with IoT devices is that there are numerous cases in which even basic security measures have not been put into effect. The importance of such security measures is currently being pointed out.

Cyberattacks May Shake Our National Security and Economy

All the experts interviewed in this issue emphasize the fact that cyberattacks are now a threat that goes beyond causing damage to a single individual or organization.

Akira Saka, CISO of Japan's Digital Agency, points out that in addition to direct cyberattacks on organizations, individuals, and infrastructure, attacks that affect individual and national decision-making are becoming increasingly serious. He informs us of US government initiatives to build a system to protect elections, involving cooperation between federal agencies, state and local governments, and even the military. The Tokyo Olympics and Paralympics also faced threats such as attacks on the Games management system and the Games website, counterfeit tickets, etc., and Mr. Saka makes clear that a variety of measures were adopted in

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese. NIRA bears full responsibility for the translation presented here. Translated by Michael Faul.
Copyright © 2021 by Nippon Institute for Research Advancement

response, such as strengthening the management system. He also indicates the determination of the Digital Agency to manage policies aimed at balancing DX and cybersecurity into the future.

Mihoko Matsubara, NTT Corporation's Chief Cybersecurity Strategist, stresses that far from being "someone else's problem," the threat of ransomware represents a real issue for Japanese companies. In addition, given that it has been shown that even an attack on a single company can have a major impact on a nation's economy and national security, she believes that this is a golden opportunity for Japan's government and industry to enhance their cybersecurity and also national security.

It Is Time for Japan Also to Consider Measures That Go a Step Further

What measures should we consider taking against the rapidly increasing threat of cyberattacks?

Mr. Motoki Nishio, a Visiting Professor at Tama University's Center for Rule-making Strategies, takes the discussion further and stresses that while the entity that has been attacked is uniformly treated as a victim in Japan, we should amend this thinking, and consider them responsible for not taking measures against cyberattacks. In addition, touching on the global trend of possessing the capability of attack as a deterrent, Mr. Nishio indicates the importance of more practical countermeasures, pointing out that whether or not Japan is able to legally obtain viable cyberattack capabilities will be a significant issue in the area of national interest.

Professor Ken Jimbo of Keio University's Faculty of Policy Management indicates that it will be necessary for Japan to develop an "active defense" system that imposes legal sanctions and allows physical response by the Self-Defense Forces in the event of a cyberattack, as the possibility of conflicts involving armed forces will increase if lives are lost to cyberattacks. He goes on to say that the government should, at the least, work to establish a unified view regarding the requirements for exercising Japan's right of self-defense against cyberattacks.

The sense of crisis shared by experts on this subject – that the possibility of terrorism and attacks in cyberspace might precipitate the entire economy or nation into a major crisis – perhaps because it emerges from a specialized area that is unfamiliar to many people, tends not to be widely shared. However, in the future, it will be necessary for the public to gain a wider recognition of the importance of the field of cybersecurity, and to consider relevant measures.

Focus On the Development of Human Resources

The points that have been made here seem not only to indicate a sense of crisis, but also a direction for the development of human resources. At present, the need to develop specialized human resources in areas such as AI and programming is strongly emphasized. Human resources of this type are of course indispensable, but in addition to this, human resources responsible for cybersecurity will become even more important in the future. Without such human resources, we will be unable to meet the challenges indicated by the experts interviewed in this issue. And if anything, in the sense of generating minutely detailed solutions to problems, the field of cybersecurity should not be a field in which the Japanese are at a disadvantage, and there is every possibility that Japan can play a leading global role in this area. Given this, I believe that we should focus more of our efforts on developing human resources to oversee cybersecurity in the future.

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese. NIRA bears full responsibility for the translation presented here. Translated by Michael Faul.
Copyright © 2021 by Nippon Institute for Research Advancement

Do Not Neglect Preparations for IoT Devices That Might Become the Starting Point for Attacks

Masahiro Murashima
Pen Tester, Ierae Security, Inc

The rapidly increasing number of IoT devices will improve the convenience of our lives, but will also be the starting point for cyberattacks. If products are recalled due to an attack, stock prices will fall and companies will suffer damage. There are cases in which large amounts of data have been encrypted by ransomware attacks, forcing companies to postpone announcement of their financial results. In addition to attackers exploiting vulnerabilities in Windows in order to gain access to terminals and file servers, it is possible that in the future network attached storage (NAS), the data storage location for IoT devices, will become a target for ransomware, and there will be cases in which companies will be forced to deal with attackers.

Attackers spend an enormous amount of time conducting attacks, and it is difficult to move beyond the current situation in which attackers are seen to be in the superior position. However, this is not to say that the attacker has the advantage and therefore no measures need be taken. It will be necessary for manufacturers to anticipate risks in advance and to implement countermeasures on that basis. From the perspective of IoT device security, the first points to check are hardware implementation, firmware, protocols for communicating with devices and the cloud, etc., but there is a limit to the development budget and security budget that can be invested in a single IoT device, and it is impossible to defend against all eventualities. In many cases, cyberattacks target the intellectual property of a specific company. Other than botnet attacks, there is little to be gained from attacking individual domestic IoT devices such as home appliances, but if in the future sensed data collected via IoT devices increases value in the market, it is possible that this data may also be targeted.

The issue with regard to IoT devices is that there are many cases in which even basic security measures have not been put in place. For example, a vulnerability that I have often encountered in the past is the use of the same certificate (either a client certificate or a private key) for authentication of multiple IoT devices when connecting to the cloud. There are even instances in which the same authentication certificate is used across the brands of multiple companies in the case of OEM products (products that are manufactured under the brand names of multiple companies). If a criminal was to obtain an authentication certificate for one of these devices, depending on the specific implementation of the IoT device, it might be possible for them to attack all the other connected devices, resulting in serious damage. For example, if such a vulnerability was to exist in a part related to the control of a vehicle, it might be possible to shut down the systems of all vehicles then in operation.

However, as the reader will have realized, prevention is possible even when attacked. Changing certificates for each device will make it possible to prevent the most serious threat – attacks on other devices. With regard to security measures, it will be essential to conduct investments based on projections of precisely where attackers will attack.

Following a period working as a security engineer for Kobe Digital Labo, Mr. Murashima is now a pen tester for Ierae Security. At the request of clients, he conducts extremely realistic mock attacks from a hacker's perspective. He has also served as a core member of the community "IoTSecJP," which shares knowledge regarding IoT security. He writes the “Hacker’s Handbook” series (published by Data House), which explains approaches to hacking for engineers and beginner hackers. Mr. Murashima gives numerous lectures at events conducted by groups seeking to increase awareness of cybersecurity.

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese. NIRA bears full responsibility for the translation presented here. Translated by Michael Faul.

Copyright © 2021 by Nippon Institute for Research Advancement

NIRA
NIPPON INSTITUTE FOR RESEARCH ADVANCEMENT

Expert Opinions

There Is an Urgent Need to Adopt Effective Measures in Anticipation of Organized Crime and Conflicts Between Nations

Motoki Nishio
Visiting Professor, Center for Rule-making Strategies, Tama University

I would like to point out the three most recent changes that we should be aware of with regard to threats in cyberspace. The first is the entry of organized crime groups into the area of cyberattacks. While attacks were formerly mounted from political motives or the desire for hackers to demonstrate their skills, we are now seeing attacks by organized criminal groups seeking money. Platform services that allow ransomware attacks to be conducted even if the attacker has no technical skills are becoming widely used, and do not require any advance capital. There are also services that allow black money to be laundered. As long as money can be obtained, any company might be the target of an attack, regardless of its size.

The second change is the connection with the economic security of major nations – economic statecraft. The Trump administration barred products manufactured by China's Huawei from the United States. In addition to such economic sanctions, the United States is making cybersecurity a strategy to enable expansion of its economic sphere. What this means is that foreign companies doing business with US companies are also obliged to comply with cybersecurity standards established by the United States when handling security-related products, equipment, and information. Companies that are not able to comply with these standards will not be able to do business with the United States.

The third change is the occurrence of what are termed "state-backed" cyberattacks, in which a nation lies behind the attack. In these cases nations launch attacks for the purpose of reducing the power of another nation. Because it is difficult to identify and prove the source of a cyberattack, attacks by nations on other nations are actually carried out as much as an attacking nation wishes. The US, Chinese, and Russian governments have tolerated attacks by organized crime groups in cyberspace to the extent that their own country is not attacked, and have also acquired human resources to engage in cyber activities by allowing plea bargaining by cyber criminals. The world trend is to retain the ability to attack as a deterrent. How Japan can legally learn to mount practical cyberattacks is developing into a serious issue related to the national interest.

Unless companies and society as a whole are obliged to respond to cyberattacks, the risk of which is increasing, Japan's power as a nation will eventually decline. Until now, Japan has treated the attacked entity uniformly as a victim, but we should change this approach and question their culpability in not taking measures against cyberattacks. For that purpose, it will be necessary to define standards for responsibility as a "duty of care," and to clarify their scope. It would be best for the government to first establish such standards for each ministry and agency, and following this to spread them to the private sector. Once the scope is clear, it can provide a yardstick for the amount of funds to be invested in cybersecurity.

Mr. Nishio is self-taught in the area of cybersecurity technology, having undertaken mock battles with famous white hat hackers throughout the world. Other than those in the student category, he was the youngest participant in the international information security conference "CODE BLUE 2015," a meeting of the world's leading experts in the field. Since 2016, he has been a Visiting Professor in Tama University's Center for Rule-making Strategies, overseeing research on international standardization in the area of cybersecurity. Taking a cybersecurity perspective, Mr. Nishio analyzes international trends, and promotes rule-making activities from the point of view of security, and the strengthening of industry capacity on this basis.

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese. NIRA bears full responsibility for the translation presented here. Translated by Michael Faul.

Copyright © 2021 by Nippon Institute for Research Advancement

My Vision No.57
2021.12

Expert Opinions

A Clear and Present Danger of Ransomware Attacks

Mihoko Matsubara
Chief Cybersecurity Strategist,
NTT Corporation

The number of ransomware attacks has been increasing during the pandemic. While ransomware attacks used to be considered a financially-motivated crime, the world is now convinced that ransomware could lead to a national security crisis. A game-changer incident was the ransomware attack on Colonial Pipeline, which accounts for 45% of the fuel supply on the U.S. East Coast, in May 2021. The pipeline shutdown caused severe turmoil centering on the East Coast, such as the rerouting of flights by American Airlines and incidents of violence over gasoline shortages. At the end of the same month, another ransomware attack hit meat giant JBS, and temporarily shut down slaughterhouses in North America and Australia. Both of these cases have highlighted the fact that a ransomware attack on even one company could have a devastating impact on a country's economy and national security.

The U.S. government has therefore begun to fundamentally enhance its cybersecurity and review its response to ransomware attacks. Following the JBS incident, Deputy National Security Adviser for Cyber and Emerging Technology Anne Neuberger sent an open letter to corporate executives and business leaders in early June 2021 to ask them to take specific actions to protect against ransomware attacks. Her list included crafting an incident response plan and using multifactor authentication, both of which Colonial had neglected. The unprecedented letter urged business leaders to consult with their Chief Information Security Officer (CISO) in order to determine which measures had been taken or needed to be supplemented. Since global supply chains require U.S. industries to enhance cyber resiliency in collaboration with their business partners and subsidiaries in other countries, this initiative will contribute to the security of the entire supply chain.

In fact, the U.S. government has already asked for international cooperation to deal with the growing ransomware threat. The White House hosted the Virtual Counter-Ransomware Initiative Meeting for two days in mid-October 2021, attended by ministers and representatives from over 30 countries including Japan and the European Union. The holding of a conference at this level reflects the strong will of the U.S. government to counter the cyber threat and make their critical infrastructure more resilient.

The U.S. government’s firm resolve to enhance cybersecurity is also attested to by personnel numbers and the size of budgets. Secretary of Homeland Security Alejandro Mayorkas announced in July 2021 that his department had hired almost 300 cybersecurity professionals and extended 500 tentative job offers, for a total of 800 new employees. In addition, the U.S. government's cybersecurity budget for 2022 amounts to 9.8 billion dollars, or one trillion yen. This is two orders of magnitude higher than the Japanese government's budget request of 91.9 billion yen for the same year.

Japanese companies have also been suffering from ransomware attacks in a variety of industrial sectors, including at overseas bases in Asia, Europe, and North America. Thus, it makes even more sense for Japan to work closely with other countries, by sharing information on the techniques employed in ransomware attacks as well as cybersecurity best practices with the public and private sectors of the United States and other nations. This is a golden opportunity for Japan’s government and industry to enhance their cybersecurity and also national security.

Mihoko Matsubara is Chief Cybersecurity Strategist at NTT Corporation, Tokyo, and is responsible for cybersecurity thought leadership. Upon graduation from Waseda University, Tokyo, she worked at the Japanese Ministry of Defense for nine years before receiving a Fulbright Scholarship to pursue an MA at the Johns Hopkins School of Advanced International Studies in Washington DC. Afterward, she accepted a fellowship at Pacific Forum CSIS (now Pacific Forum) in Honolulu to research Japan-U.S. cybersecurity cooperation. She then joined Hitachi Systems as cybersecurity analyst, and next took a position at Intel K.K., Tokyo, as Cybersecurity Policy Director. Her most recent experience includes serving as VP and Public Sector Chief Security Officer (CSO) for Asia-Pacific at Palo Alto Networks in Singapore. Ms. Matsubara’s book on cybersecurity, cyber threat intelligence, and talent development (Shinchosha Publishing Co., Ltd, 2019; in Japanese) won the 29th Okawa Publications Prize in JFY 2020.

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese.
NIRA bears full responsibility for the translation presented here. Translated by Michael Faul.
Copyright © 2021 by Nippon Institute for Research Advancement

Expert Opinions

Balancing DX and Cybersecurity

Akira Saka
Chief Information Security Officer (CISO), Digital Agency Japan

Together with the progress of the digitalization of society, the threat of cyberattacks is again coming into focus with the sudden increase in online activity during the COVID-19 pandemic. The Information-technology Promotion Agency (IPA), which works to strengthen information security in Japan, has cited ransomware attacks as the main threat for organizations and unauthorized use of smartphone payments as the main threat for individuals. While the number of criminal offenses and the like is decreasing in the real world, cybercrime is increasing; threats are shifting from the real world to cyberspace. Attackers are constantly attacking all levels, fields, and targets, and the forces of the attacking side and the defending side are constantly in conflict.

The thing that I see as a particularly significant problem is the fact that in addition to direct cyberattacks on organizations, individuals, and infrastructure, attacks that affect personal and national decision-making are becoming more serious. For example, during the US presidential election, in addition to attacks on the electoral system itself, there were attempts to manipulate public opinion using cyber tools such as fake news and fake videos. The US government is establishing a system to protect elections in collaboration with federal agencies such as the Department of Homeland Security and the Treasury Department, state and local governments, and even the military. In Japan also, cooperation between government agencies will be an ongoing issue.

In the case of the 2020 Tokyo Olympics and Paralympics, amid threats such as attacks on the Games management system and the Games website, counterfeit tickets, etc., initiatives including strengthening the management system, creating infrastructure for the sharing of information with the government's response system and related parties, and international cooperation, we were able to finish the Games without any effect on Games management. Issues that can be pointed to were ensuring the security of relevant personnel to enable the building and operation of systems together with numerous companies and organizations in Japan and overseas, and, in the case of Games venues, the necessity to protect not only the systems set up by the Organizing Committee but also the legacy systems in the existing facilities. Experience of this type will be a legacy of the Olympics, and will serve as a future reference.

The people in charge at the front line of cybersecurity are in a situation in which the opponent is constantly attacking; they are fighting as if on a battlefield. The Digital Agency, which was established in September 2021, states its mission in the slogan "No-one left behind," and seeks to create a society in which everyone can use digital technologies with peace of mind. In addition, based on a security perspective and the concept of ensuring the safety and security of cyberspace – which has become a public space – in order to protect every citizen, the new "Cyber Security Strategy" decided on by the Cabinet in September 2021 aims to balance DX with cybersecurity for the entire nation.

Mr. Saka joined the National Police Agency in 1981, and was involved in cybercrime countermeasures as the Chief of the Security System Planning Office of the Community Safety Bureau and the Director of the Cybercirme Division. In 2002, he studied cyberterrorism as a visiting researcher at Harvard's Weatherhead Center for International Affairs (WCFIA). For two years from 2008, he was a professor in the Keio University Graduate School of Media and Governance. In 2021, Mr. Saka served as the CISO of the Organizing Committee of the Tokyo Olympic and Paralympic Games. Currently, he is also a Director of the Japan Cybercrime Control Center (JC3) and Managing Director of the Council for Public Policy, (CPP).

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese. NIRA bears full responsibility for the translation presented here. Translated by Michael Faul.
Copyright © 2021 by Nippon Institute for Research Advancement

NIRA
NIPPON INSTITUTE FOR RESEARCH ADVANCEMENT

Expert Opinions

As Cyber Attacks Intensify, Japan's Debate on Active Defense Must Accelerate

Ken Jimbo
Professor, Faculty of Policy Management, Keio University

Over the past decade, with the rapid increase in the sophistication of cyberattacks,　it is now only a matter of time until such attacks lead to the loss of life, making them increasingly relevant to national security. The digital transformation has led to rapid growth in the number of networked systems that can be accessed remotely, from factories across the industrial spectrum to infrastructure, and this has created increasing vulnerability to the hijacking of control systems, attacks on critical infrastructure, and the obstruction of military operations. Such attacks have already occurred against gas pipelines and water bureaus in the United States, and the control systems for the power grid in Ukraine. If the integrity of a water system were to be compromised and drinking water contaminated, or a large-scale blackout to occur, many lives could be lost. With very little notice, cyberattacks have come to possess a destructive potential nearly equivalent to that of conventional military operations.

Such attacks could easily provoke a military response, bringing with it the potential for catastrophic escalation and war. It is thus becoming increasingly important to understand how each country's national security apparatus perceives the level of threat from cyber operations. To clarify the threshold past which a cyberattack may become the catalyst for the use of military force in response and establish an international consensus around such "red lines" that must not be crossed. Such actions would hopefully deter the increasingly escalatory nature of cyberattacks. The Tallinn Manual on the International Law Applicable to Cyber Warfare regards scenarios such as causing a nuclear meltdown or the destruction of a dam as a "red line," but any standards formulated in the Manual will necessarily have to be reviewed to consider more recent cases of cyberattacks.

In the case of Japan also, I believe that it has become necessary to establish an "active defense" system that would impose legal sanctions and allow physical responses by the Self-Defense Forces in the event of a cyberattack. Such an active defense system would first need to demonstrate to its antagonist that it knows the perpetrator of the cyberattack and understands the nature of the attack, thus preventing or deterring further attacks. Japan demonstrated competency in this regard with the hosting of the 2020 Tokyo Olympic and Paralympic Games. The next step in the development of Japan's cyber capability is recovering assets stolen in an attack and removing the attacker's method of attack. While the United States and other countries have already demonstrated such capabilities, Japan still struggles to do so. At the very least, it will be necessary for the government to work to establish a unified view about the conditions which must be fulfilled for Japan to exercise its right of self-defense against a cyberattack.

Currently, responsibility for responding to cyberattacks is divided amongst the Cabinet's National Center of Incident Readiness and Strategy for Cybersecurity (NISC), the National Police, the Ministry of Internal Affairs and Communications, and the Cyber Security Division of the Ministry of Economy, Trade and Industry, and there is an urgent need to unify these disparate approaches under one umbrella. There is also a need for a dedicated ministerial level representation in cybersecurity to serve as a counterpart to the institutions existing in other countries, enabling the creation of a cooperative framework to respond to cyberattacks with nations throughout the world.

Dr. Ken Jimbo specializes in national security, the security of the Asia Pacific region, and Japanese Defense and Foreign Policy. He has previously worked in various capacities at institutions such as the Japanese Ministry of Defense, the Cyber Defense Council (CDC), and the National center of Incident readiness and Strategy for Cybersecurity (NISC). He warns of the risks engendered by the rapid development of cyber technologies from the perspective of international politics. He has been an influential voice on the national security risks of emerging technologies in the cyber domain. He is the author of "Security Architecture in the Asia-Pacific: The Three-Layered Structure of Regional Security" (editor and editor, Nippon-Hyoronsha, 2011; in Japanese) and the co-author of "Ask Demography! A Map of the World in 2050" (Chuokoron, 2020; in Japanese).

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese. NIRA bears full responsibility for the translation presented here. Translated by Jonathan Webb.

Copyright Ⓒ 2021 by Nippon Institute for Research Advancement

Glossary

Botnet	A "bot" is a computer virus that externally remotely controls a computer. A "botnet" is a network of computers infected with bots. When an attacker gives instructions via the Internet, the computers connected to the botnet perform actions such as delivering junk mail or attacking other computers and stealing data.
Client certificate	An electronic certificate issued to authenticate an individual or organization. When a client uses a system, service, email, etc., the certificate proves to the server that the client is a legitimate user.
Firmware	Software embedded in devices such as computers for basic hardware control.
Network Attached Storage (NAS)	An external storage device that can be utilized via a network.
Multifactor authentication	A method of combining at least two of the three elements represented by the user's memory, something in the user's possession, and the user's biometric data ("knowledge, possession, inherence") when authenticating a user. This method further enhances security.
Private key	A key that is possessed without being shown to others when encrypting using public key encryption or when using a digital signature. The person who receives the encrypted communication decrypts the data using the private key.
Protocol	An international standardized rule such as a data format or a transmission and reception procedure that is established to enable computers to exchange data via a network.
Ransomware	A malicious program that, when it infects a terminal, etc., encrypts the stored data and makes it impossible to use. The criminals using the program demand money (a ransom) in return for decrypting the data.
Sensed data	Data collected using sensing devices (sensors), etc. IoT devices equipped with sensors collect a variety of data, such as temperature, humidity, light, movement, sound, smell, and taste data.
Tallinn Manual	A guide to the application of international law in cyberspace. Under international law, there is no established opinion regarding the definition of "armed attack" in cyber warfare. The Tallinn Manual is an attempt to provide examples of the interpretation of "armed attack." Published by NATO's Cooperative Cyber Defence Center of Excellence in 2013.

Source) Formulated based on materials published by the Police Agency, the Ministry of Internal Affairs and Communications, the Ministry of Foreign Affairs, the Prime Minister's Office, GMO GlobalSign Holdings K.K., DigiCert Inc., etc., and Imidas, NTTIT trend terms, etc.

Editor: Reiko Kanda, Maiko Sakaki and Tatsuya Yamaji. This is a translation of a paper originally published in Japanese. NIRA bears full responsibility for the translation presented here. Translated by Michael Faul.

Copyright © 2021 by Nippon Institute for Research Advancement