Here, where the Land Ends and Space Begins

Creating a Safe and Secure Cyberspace

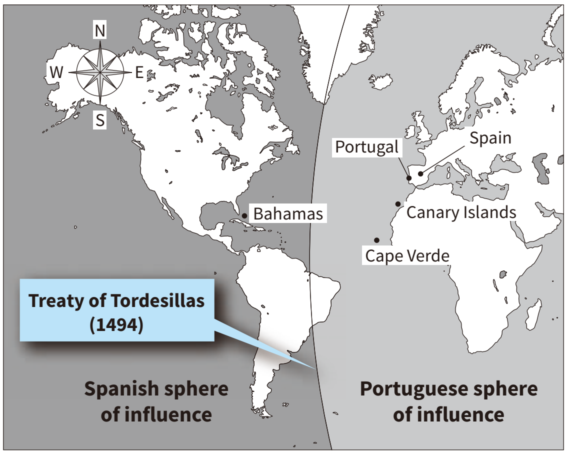
The Age of Exploration and the Law of the Sea

"*Onde a terra se acaba e o mar começa* (Here, where the land ends and the sea begins)." These words are inscribed on a stone monument that looks out over the expanse of the Atlantic Ocean from Cabo da Roca, Portugal, on the westernmost edge of the Eurasian continent. The passage was written by the famous Portuguese poet Luís de Camões and comes from a poem about his country's great achievements in the Age of Exploration. It was Portugal and Spain that lifted the curtain on that period of history.

Both countries were looking not to the Mediterranean Sea, which was under the control of Islamic forces, but rather to the Atlantic Ocean. The Portuguese explorer Bartolomeu Dias reached the Cape of Good Hope in 1488 and, sponsored by Spain, Christopher Columbus opened up passage to the West Indies in 1492.

To avoid competition between the two nations, they signed the 1494 Treaty of Tordesillas agreeing to split rights to the world's great oceans between them [1]. The challengers to these great powers were the emerging nations of England and the Netherlands. England began to amass wealth through a class of pirate ships known as privateers[*1] that were authorized by Queen Elizabeth I and plundered South American gold, silver, and other valuables from Spanish ships. While Spain tried to keep its sea routes secret, the information was acquired by a network run by Sir Francis Walsingham, principal secretary to Queen Elizabeth I and the man who came to be seen as the original English spymaster.

[1] Treaty of Tordesillas


N
W
E
S
Portugal
Spain
Bahamas
Canary Islands
Cape Verde
Treaty of Tordesillas (1494)
Spanish sphere of influence
Portuguese sphere of influence

Prepared with reference to "The Geopolitics of the Seas – A 400-year History of Hegemony" by Isami Takeda

The desire by the Dutch to open up routes to the Indian Ocean led to Hugo Grotius proposing the notion of "the free seas" in 1609. This was in opposition to Portugal, which held a monopoly on trade with the region, and marked the beginning of international law. Growing rich on the success of its privateers, England started resorting to the law when they came into conflict with the Dutch. England opposed the idea of the free seas with the idea of maritime jurisdictions, which introduced the concept of territorial waters, and passed the Navigation Act in 1651. While control of the seas was largely based on the rules of war up until the 18th century, there was a gradual transition toward laws aimed at boosting confidence in maritime travel and making it safer.

In 1945, President Truman of the USA published the Truman Proclamation covering such matters as rights to the continental shelf and was devised with offshore oilfields and fisheries in mind. The proclamation had a major impact worldwide and led to an international treaty (the Convention on the Continental Shelf) as well as the concept of exclusive economic zones. The United Nations Conference on the Law of the Sea was held in 1958 and the United Nations Convention on the Law of the Sea came into force in 1994, the latter being known as a "constitution for the oceans." Five hundred years after the Treaty of Tordesillas, international laws governing safety and security on the oceans were finally in place.

Hackers, Pirates in the Great Era of Cyberspace

The Portuguese Man of War is a marine organism named for its resemblance to the caravels that sailed the oceans in the Age of Exploration. In Japan, however, the species (scientific name *physalia physalis*) is commonly known as the electric jellyfish. A movie was released in Japan last year that played on this common name for these poisonous creatures: *Denki Kurage no Inshidento* (The Electric Jellyfish Incident). Set in Fukuoka, it is about the conflict between a hacker who deliberately spreads malware for stealing personal information from mobile phones and a "white hat" hacker who is giving chase.

Malware is the general term for malicious programs such as computer viruses. They come in a variety of forms, including

[*1] A ship that has been granted a "letter of marque," meaning a license from the government of one nation to attack and plunder the ships of enemy nations.

Kenji Kato
Industrial Policy Division,
Government and External Relations Group,
Hitachi, Ltd.

viruses that spread by infecting files or programs, worms that spread as standalone programs, and trojans that appear to be legitimate software but conceal malicious purposes. Once used as a term of respect for people proficient in skills like programming, "hacker" has now come to mean the pirates of cyberspace, namely people who attempt to gain unauthorized access to networks (hacking). The term "white hat" hacker, meanwhile, refers to computer security personnel who try to stop these malicious hackers. Similarly, an "incident" is something that threatens the security of a network, such as hacking or the destruction of data. While the movie was a work of fiction, there have been actual incidents significant enough to warrant a place in a novel or film. Though born in Japan, Tsutomu Shimomura has since his teenage years been active as a computer security specialist at places such as the Los Alamos National Laboratory. In 1995, he worked as a white hat hacker assisting in the arrest of a notorious hacker wanted by the US Federal Bureau of Investigation (FBI), helping trace where this person lived. Coming at a time when use of the Internet was just starting to become mainstream, the incident attracted widespread attention, including the publication of a book about what happened, "Takedown," which was also made into the movie "Takedown" ("Track Down" in some markets).

The world's first hacker appeared in 1903 before the Internet and computers even existed. In that year, Guglielmo Marconi, inventor of the radio telegraph, conducted an experiment in which he sent a cleartext transmission from Cornwall in the far west coast of England to London, 300 miles away. Unfortunately, someone managed to hack into this experiment and send a message of their own that insulted Marconi. While the identity of this first-ever hacker remains unknown, the magician Nevil Maskelyne coined the term hacking to express the vulnerability of radio telegraphy, a very open form of infrastructure.

As the nation that conquered the world's oceans, Britain recognized the importance of information networks. With the telegraph established as a practical technology, the laying of undersea cables got underway in the 1850s, resulting in a telegraph network that spanned Europe and America in particular as well as many of Britain's overseas colonies. UK intelligence agencies used the network during World War I to hack an encrypted telegraph message that Arthur Zimmermann, the German State Secretary for Foreign Affairs, sent to the Mexican government encouraging it to join the war against the USA. The UK passed the message on to the USA while keeping its origins secret. The term "attribution" is used to indicate identification of the individual or organization responsible for a hack or other cyberattack. This attribution is not easy and is further complicated by the fact that, depending on the amount of damage done or whether in fact there was any damage at all, the victim of the attack may not even be aware that it has happened.

Recent Olympic Games have also experienced large-scale cyberattacks, including those hosted by London and Rio de Janeiro. London alone was said to have been the target of 200 million such attacks. Although its postponement has been announced, the Olympic Games planned for Tokyo in 2020 also brought a gradual heightening of public awareness of cyberattacks and security, as exemplified by the new movie release discussed above.

Cyberspace Offence and Defense

Jasper Maskelyne, son of Nevil and like his father a famous magician, joined the British Army during World War II and teased the German Afrika Korps of General Rommel with clever schemes that ranged from using magic tricks to camouflage tanks to moving the port of Alexandria and making the Suez Canal disappear. Jasper spoke of magic as being an application of science and knowledge of human behavior. This way of thinking is also called social engineering, with applications in cyberspace that include both offence and defense.

Cyberattacks can be broadly divided into those that are indiscriminate and those that are targeted. Example techniques used for indiscriminate cyberattacks include attaching malware to a file and spreading it by electronic mail or embedding malware in a website. Indiscriminate methods of cyberattack are a common feature in ransomware incidents, in which malware first locks an infected computer or encrypts all of its data, then demands a ransom to undo the damage. Social engineering is used to cleverly exploit users' psychological weaknesses to trick them into opening an attached file.

Targeted cyberattacks, meanwhile, tend to go after government agencies or companies, especially those organizations such as hotels, airlines, and hospitals that hold large amounts of important personal information. Even in these cases, however, attacks are frequently perpetrated by first using a fake e-mail message to infiltrate malware and then going through the victim's data.

Jasper Maskelyne used a fake port and dummy submarines to protect important infrastructure from enemy attack, an approach that also works in cyber-defense. A "sandbox" is a safe virtual environment on a computer that can be used to determine whether a program contained in an attached file is malware. Similarly, a "honeypot" is a way of detecting cyberattacks by, for example, deliberately leaving a system open to attack by choosing not to fix vulnerabilities in its operating system (OS).

Examples of targeted attacks on critical infrastructure are too many to count. In 2012, 3,000 PCs used in control systems at an oil plant in the Middle East became infected by malware. In 2016, the electricity systems in the USA and Canada came under attack after the US presidential election. Among notable examples of attacks on government agencies was a 2007 distributed denial-of-service (DDoS) attack against Estonia, a nation with well-established IT infrastructure. DDoS attacks typically involve forcing the targeted service to shut down through such methods as flooding its servers or other systems with data from a large number of different addresses. As these cyberattacks are sometimes state-sponsored, just like the privateers in the Age of Exploration, or may be covert actions by mysterious international terrorist organizations, as in a James Bond movie, identifying the perpetrators is difficult, as is maintaining a perfect defense against such attacks.

Awareness of Cybersecurity among Senior Management

Speaking of James Bond movies, they have included a number of instances in which M, the head of the British intelligence service, played by famous actress Judi Dench, had her own PC hacked by Bond or one of the villains. While one may wonder how low the security awareness of someone who leads an intelligence agency might really be, one of the incidents in which M was hacked led to an entire movie's worth of strife. Don't be too quick to laugh this off as being just a movie: in real life a business e-mail fraud was detected in 2016 that involved fake e-mails purporting to be from the chief executive officer (CEO) of a European aerospace component manufacturer. In accordance with instructions received, accounting staff were duped into making an emergency transfer of 42 million euros to fund a corporate acquisition. Of this sum, the company only succeeded in recovering 10.9 million euros. Whereas M got the job done without succumbing to hacking, the long-serving CEO of the component manufacturer lost his job for dereliction of duty.

The villain in the movie fought on. In the final climactic confrontation when Bond and the villain face off at the latter's secret hideout, Bond at first finds it very easy to get inside. When the facility then somehow gets set alight, the fire spreads throughout its large area in just a few cuts, setting off a huge site-wide explosion and revealing that, for all its apparent splendor, the hideout was in fact very cheaply put together. Whereas the villain had spent heavily on the attack, he had not invested properly in security, as if he saw the hideout as merely a cost center. As a result his plans were foiled.

Here again, a similar incident happened in real life (although it involved a cyberattack rather than a physical one). A North American IT equipment manufacturer that went out of business in 2009 turned out to have been under cyberattack since around 2000. It was discovered in 2004 that the accounts of the CEO and other top management had been hijacked. Security personnel urged management to take countermeasures, but the advice was ignored, thereby allowing the attacks to continue for the next few years. This resulted in the theft of important documents, including research and development material and business plans, and was believed to have contributed to the company's collapse.

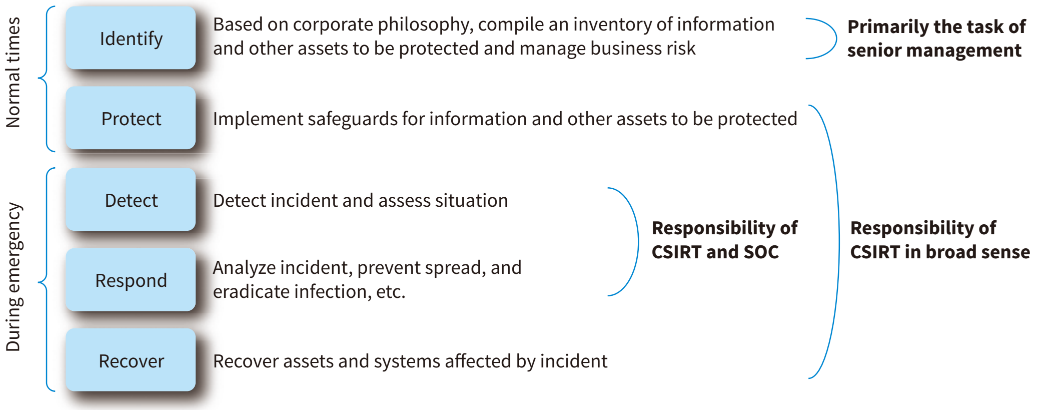
Treating cybersecurity as a management problem and raising awareness of security among senior executives is currently a worldwide challenge. This led the Japan Business Federation (Keidanren) to announce its Declaration of Cybersecurity Management in 2018, followed by publication of the Cyber Risk Handbook for company directors in 2019.

Framework for Cybersecurity

Having a cybersecurity framework helps companies and their managers gain an understanding of security. One well-known example is the framework first published by the US National Institute of Standards and Technology (NIST) in February 2014 [2]. President Obama spoke about the risk of cyberattack on critical infrastructure in his 2013 State of the Union address and issued Executive Order 13636 (Improving Critical Infrastructure Cybersecurity) in February of the same year. It was in response to this that NIST produced its cybersecurity framework.

The framework defines five core functions: (1) Identify, (2) Protect, (3) Detect, (4) Respond, and (5) Recover. "Identify" means to identify which information and other assets are to be protected from cyberattack. This is an exercise that involves determining, from a management perspective, the organization's core competencies and what underpins its competitive advantage, getting a sense of risks to the business should

[2] NIST cybersecurity framework


Normal times
During emergency
Identify
Based on corporate philosophy, compile an inventory of information and other assets to be protected and manage business risk
Primarily the task of senior management
Protect
Implement safeguards for information and other assets to be protected
Detect
Detect incident and assess situation
Respond
Analyze incident, prevent spread, and eradicate infection, etc.
Responsibility of CSIRT and SOC
Responsibility of CSIRT in broad sense
Recover
Recover assets and systems affected by incident

Prepared with reference to "Introduction to Cybersecurity Management" by Keisuke Kamata, and other material.

CSIRT: computer security incident response team SOC: security operation center

these be infringed or destroyed, and making an inventory of the information and other assets to be protected. While the second function, "protect," means to deploy practical countermeasures, given that no defense will ever be 100% effective, the functions of "detect," "respond," and "recover" are also essential.

Management plays a central role in the "identify" function, taking account of considerations such as the corporate philosophy, while the other functions are handled by specialist groups known as computer security incident response teams (CSIRTs) or security operation centers (SOCs). CSIRTs arose out of a recognition of the need for a team that can provide the entire organization with timely updates on incidents and other relevant information, something that was highlighted by the extensive damage done on the Internet by the first worm infection in 1988. CSIRTs serve as a command center for incident response, with a scope of responsibility that varies widely between organizations. Similarly, an SOC is a team dedicated to incident detection and response.

Hitachi established an incident response project in 1998 that was subsequently formalized as the Hitachi Incident Response Team (HIRT) in 2004. Along with incident response, HIRT supports Hitachi's cybersecurity work by patching system vulnerabilities and dealing with in-house information security, and also through its work on customer information and control systems to ensure the security of Hitachi products and services. The SOC has been providing 24-hour-365-day monitoring of cyberattacks since October 2017. Hitachi's activities also include the supply of managed security services (MSSs) for customers across more than 50 different countries and in four different languages (English, French, Spanish, and Japanese) from four sites around the world.

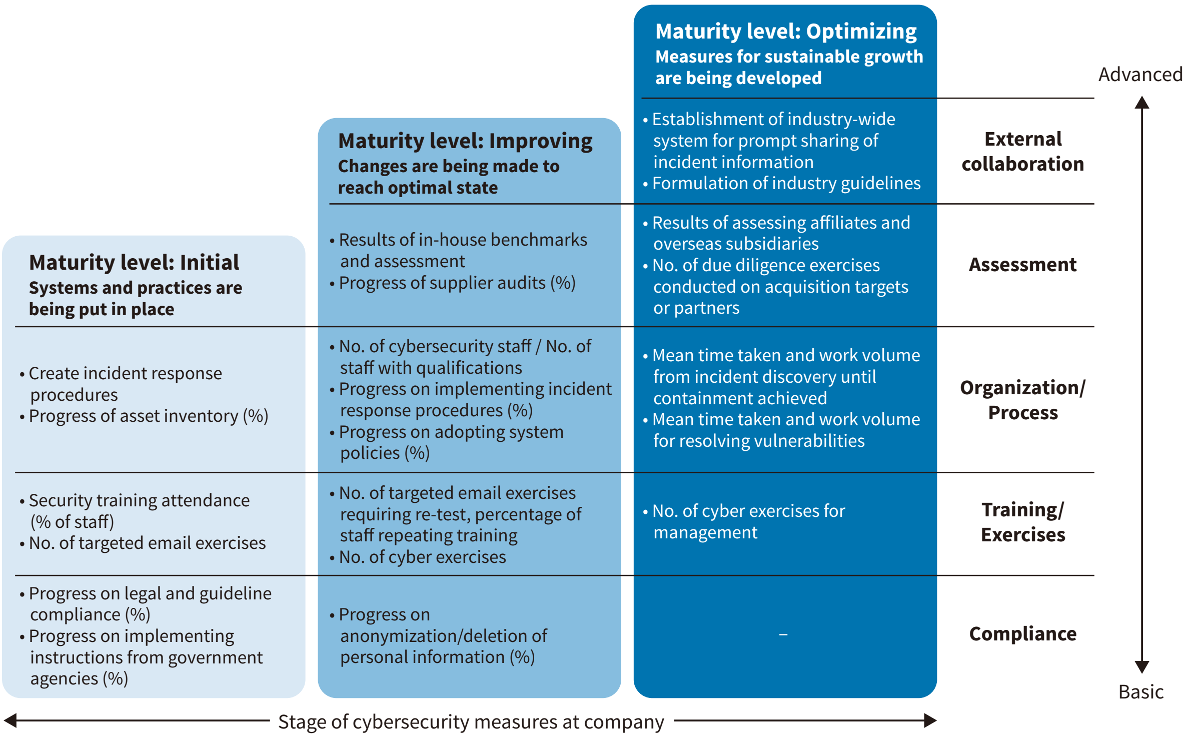
Making Security Transparent

Dr. Osamu Shimomura, father of the white hat hacker Tsutomu Shimomura, was awarded the Nobel Prize in Chemistry in 2008 for his research into the green fluorescent protein (GFP) responsible for the bioluminescence of crystal jellyfish (*aequorea victoria*). When incorporated into the proteins of a cell, the green bioluminescence of GFP makes it easier to see what is happening internally.

One of the challenges currently facing attempts to improve awareness of security among senior managers is how to improve transparency by making it easier to see the level of maturity of cybersecurity at their companies. To reiterate, security is not so much a technological problem as it is an issue of management. In this regard, the Japan Cybersecurity Innovation Committee (JCIC), a thinktank dedicated to cybersecurity, has proposed a key performance indicator (KPI) model that makes use of monetary sums (financial losses) in order to help people appreciate that security is a management issue [3]. The JCIC KPI model classifies the maturity of security at an organization into the three levels of "Initial," "Improving," or "Optimizing," and uses the categories of "Compliance," "Training/exercises," "Organization/procedure," "Assessment," and "External collaboration" to group the different security measures. The model then combines these in the form of a matrix to express the company's situation.

In 2014, the UK government launched its Cyber Essentials certification scheme that stipulates core security activities for companies and other organizations. Having this certification was made a condition for tendering on government contracts

[3] JCIC's KPI Model of Cybersecurity



Maturity level: Initial Systems and practices are being put in place	Maturity level: Improving Changes are being made to reach optimal state	Maturity level: Optimizing Measures for sustainable growth are being developed	
		• Establishment of industry-wide system for prompt sharing of incident information • Formulation of industry guidelines	**External collaboration**
	• Results of in-house benchmarks and assessment • Progress of supplier audits (%)	• Results of assessing affiliates and overseas subsidiaries • No. of due diligence exercises conducted on acquisition targets or partners	**Assessment**
• Create incident response procedures • Progress of asset inventory (%)	• No. of cybersecurity staff / No. of staff with qualifications • Progress on implementing incident response procedures (%) • Progress on adopting system policies (%)	• Mean time taken and work volume from incident discovery until containment achieved • Mean time taken and work volume for resolving vulnerabilities	**Organization/ Process**
• Security training attendance (% of staff) • No. of targeted email exercises	• No. of targeted email exercises requiring re-test, percentage of staff repeating training • No. of cyber exercises	• No. of cyber exercises for management	**Training/ Exercises**
• Progress on legal and guideline compliance (%) • Progress on implementing instructions from government agencies (%)	• Progress on anonymization/deletion of personal information (%)	–	**Compliance**

Source: JCIC "Cybersecurity KPI Model"

KPI: key performance indicator JCIC: Japan Cybersecurity Innovation Committee

that involve confidential information. Meanwhile, a 2018 revision of the NIST cybersecurity framework added supply chain risk management as a core function. Given that they in turn interconnect with other companies, it is clearly not enough for customers and suppliers merely to improve the maturity level of their own security. Rather, as Society 5.0 is characterized by a high level of overlap between the cyber and physical realms, what is needed is to improve the maturity of cybersecurity across society as a whole.

In recognition of the way in which goods, people and organizations, and society are interconnected, Hitachi has adopted a new strategy of building security ecosystems. As it works toward achieving Society 5.0, Hitachi is taking steps to enhance cyber-resilience so that people will be able to enjoy greater safety and security, pursuing the establishment of a society-wide security ecosystem built through collaborative creation between industry, government, and academia along with its own in-house activities.

Aiming for Safer and More Secure Use of Cyberspace

At Davos 2019, Prime Minister Abe spoke about the importance of data governance ("data free flow with trust") in the coming data-driven society, proposing the "Osaka Track" for data governance. At the G20 summit of the same year he also urged the formulation of international rules, putting forward the idea of a zone within which free cross-border flows of data are permitted.

On the subject of the relationship between trust and "sincerity," one of the elements of the Hitachi Founding Spirit, Naosaburo Takao, a senior manager in Hitachi's early years, held that sincerity is a basic moral principle in human society that transcends time and place, while trust is paramount for critical infrastructure given how long it remains in use. Therefore, it is trust built up through the accumulation of sincere efforts that matters more than anything else. He went on to say that products made with sincerity are imbued with sincerity, that companies that use products imbued with sincerity are themselves imbued with sincerity, and that such companies will flourish. This chain of sincerity envisaged by Takao is both a force for overcoming malware and other forms of cyberattack made with malicious intent, and also the foundation for international rules on the safe and secure use of cyberspace based on trust.

We stand now on the brink of Society 5.0 and the great expanse of possibilities it offers, a sophisticated amalgam of the physical and cyber worlds. Hitachi is playing its part by

Stone monument inscribed with "*Onde a terra se acaba e o mar começa* (Here, where the land ends and the sea begins)" and the view out over the Atlantic Ocean from Cabo da Roca.

providing personnel and helping to raise the maturity level of security within the ecosystem, supplying security staff to fill roles such as head of the JCIC and chair of the operating committee of the Nippon CSIRT Association. The company is also engaged at a global level, participating in international standardization agencies (including ISO/IEC JTC 1/SC 27, OASIS CTI, and WG 10 and WG 20 of IEC TC 65*2), and its hope is to take every opportunity to spread this spirit of sincerity not only across the supply of products and services, but also to the entire ecosystem and society as a whole.

Here, where the land ends and space begins. (*Onde a terra se acaba eo espaço começa.*)

*2 Abbreviations
ISO: International Organization for Standardization, IEC: International Electrotechnical Commission, ISO/IEC JTC 1/SC 27: A sub-committee (SC 27) of a joint technical committee (JCT 1) of the ISO and IEC, OASIS CTI: Cyber Threat Intelligence (CTI) technical committee of the Organization for the Advancement of Structured Information Standards (OASIS), TC 65: IEC technical committee on industrial-process measurement, control and automation, WG: working group

References

1) Industry Control Solution Laboratory Co., Ltd., "Collated Cybersecurity Incidents," (Feb. 2019) in Japanese.

2) "NTT Cybersecurity Laboratory: Cybersecurity as an Aspect of Management," Nikkei Business Publications, Inc., Tokyo (Oct. 2015) in Japanese.

3) T. Kaji, "R&D of Security Technologies for Secure and Trusted Social Infrastructures," Information Processing Society of Japan Magazine, Vol.55, No.7, National Institute of Informatics (Jul. 2014) in Japanese.

4) K. Kamata, "Introduction to Cybersecurity Management," Kinzai Corporation, Tokyo (Oct. 2017) in Japanese.

5) M. Koga, "The Rise of Modern Maritime Law: Historical Development of the Law of the Sea," Yushindo Kobunsha, Tokyo (Oct. 2004) in Japanese.

6) O. Shimomura, "Learning from Jellyfish: The Road to a Nobel Prize," Nagasaki Bunkensha Co., Ltd., Nagasaki (Oct. 2010) in Japanese.

7) T. Shimomura et al., "Takedown," Hyperion, New York (Jan. 1996)

8) N. Takao, "Hitachi Memoir," Hitachi Printing Co., Ltd., Tokyo (Feb. 1985) in Japanese.

9) I. Takeda, "The Geopolitics of the Seas – A 400-year History of Hegemony," Chuokoron-Shinsha, Inc., Tokyo (Nov. 2019) in Japanese.

10) I. Takeda, "Pirates Making World History," Chikumashobo Ltd., Tokyo (Feb. 2011) in Japanese.

11) M. Tsuchiya, "Geopolitics of Cybersecurity," ITU Journal, Vol. 47, No. 9, (Sept. 2017) in Japanese.

12) D. Fisher, "The War Magician: The Man Who Conjured Victory in the Desert," Weidenfeld & Nicolson, London (Oct. 2004)

13) K. Nakao, "Understanding History Through Security Technology: It's Present and Future," Information Processing Society of Japan, Digital Practice, Vol. 9, No. 3 (Jul. 2018) in Japanese.

14) JCIC, "Cybersecurity KPI Model" (Apr. 2019)

15) Hitachi, Ltd., "Information Security Report 2018" (Feb. 2019)

16) Hitachi. Ltd., "Hitachi Integrated Report 2019" (Year ended March 31, 2019)

17) Blue Planet Works, Inc., "Definitive Edition – Cybersecurity: New Threats and Defenses," Toyo Keizai Inc., Tokyo (Nov. 2018) in Japanese.

18) M. Matsubara, "Cybersecurity to Protect the Way of Our Digital Life," Shinchosha Publishing Co., Ltd., Tokyo (Nov. 2019) in Japanese.

19) T. Miyao, "Security Solutions Assisting Social Infrastructure Digitalization," Hitachi Review, 67, pp. 591–596 (Aug. 2018)

20) D. Gascueña, "Nevil Maskelyne vs Marconi: a hacker in 1903," https://www.bbvaopenmind.com/en/technology/visionaries/nevil-maskelyne-vs-marconi-a-hacker-in-1903/ (viewed in March 2020).