Establishment and Development of Cybersecurity Technologies to Solve Problem of Increasing Operation Costs and to Minimize Damage

Yuzo Koga, Yoshiaki Nakajima, Naoko Chiba, Jun Miyoshi, Takaaki Koyama, Hidehiro Shito, and Asami Miyajima

Abstract

While responding to new cybersecurity threats such as cyber attacks, we will radically improve the efficiency of security operations by developing technologies for autonomous and automated security measures. Such technologies will enable operators to concentrate on countermeasures against advanced threats that cannot be handled mechanically and enhance overall security-response capabilities.

Keywords: cybersecurity, security operation, security measures

1. Background

Cyber attacks are increasing yearly and becoming more complicated and sophisticated. In particular, there has been a significant increase in cyber attacks that directly target humans, which has dramatically increased the cost of cybersecurity measures for enterprises.

When users have diverse requirements and enterprises need to cope with long tail customers, a variety of applications should be provided through a combination of servers and software on ultrahigh-speed optical communication networks connecting various communication equipment, terminals, and devices. In such a situation, the efficiency of security measures to handle each cyber attack is too low, which can be a factor hindering the digital transformation and business-value creation of enterprises.

2. Goal of our research and development

We are conducting research and development (R&D) on technologies for automatically and proactively implementing security measures against cyber attacks and various vulnerabilities that are targets of them.

Through such technologies, we will provide an information and communication technology (ICT) environment capable of preventing damage caused by cyber attacks and resolving the shortage of human resources in security operations that restrict enterprise management, enabling users to use services with peace of mind. This environment eliminates the need for enterprises to respond to security vulnerabilities each time (whack-a-mole game), after an incident (cat-and-mouse game), or respond to business loss due to damage (**Fig. 1**).

By reducing the total cost of security operations, we will enable enterprises to focus on development and operations and support them in creating business values in short cycles in a Smart World of smart factories, buildings, mobility, etc. (**Fig. 2**).

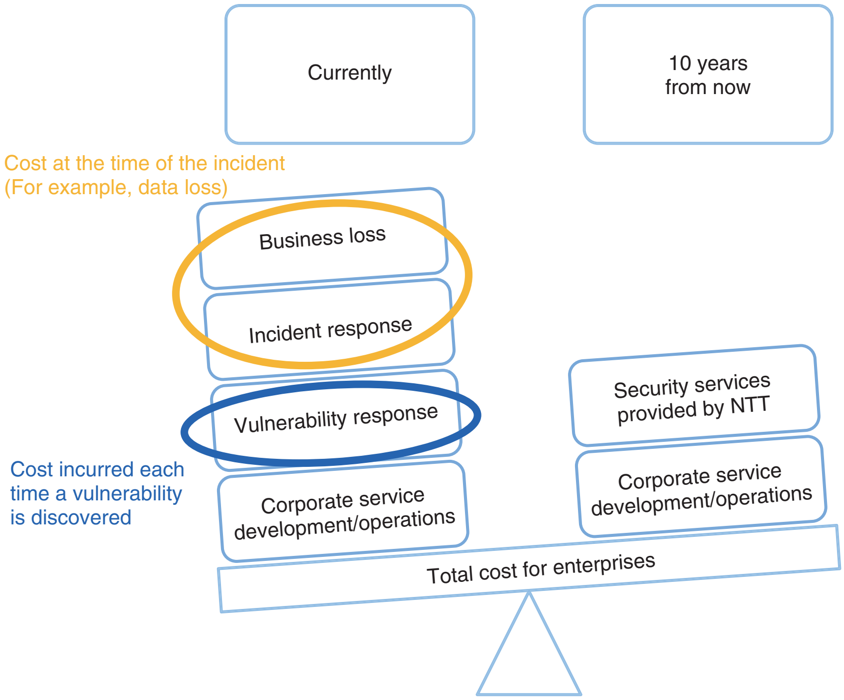

Currently
10 years from now
Cost at the time of the incident (For example, data loss)
Business loss
Incident response
Vulnerability response
Cost incurred each time a vulnerability is discovered
Corporate service development/operations
Security services provided by NTT
Corporate service development/operations
Total cost for enterprises

Fig. 1. Total cost reduction of security operations.

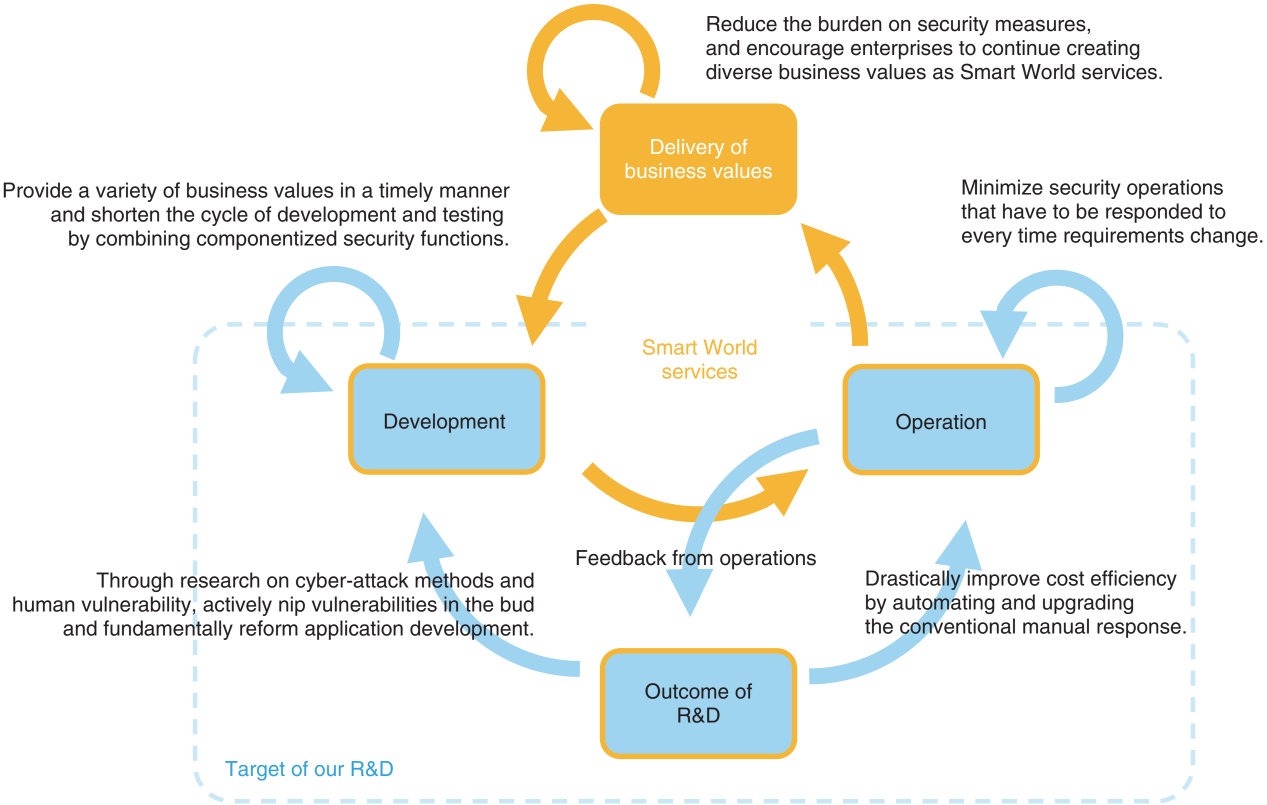

Reduce the burden on security measures, and encourage enterprises to continue creating diverse business values as Smart World services.
Delivery of business values
Provide a variety of business values in a timely manner and shorten the cycle of development and testing by combining componentized security functions.
Minimize security operations that have to be responded to every time requirements change.
Smart World services
Development
Operation
Feedback from operations
Through research on cyber-attack methods and human vulnerability, actively nip vulnerabilities in the bud and fundamentally reform application development.
Drastically improve cost efficiency by automating and upgrading the conventional manual response.
Outcome of R&D
Target of our R&D

Fig. 2. Purpose of our R&D.

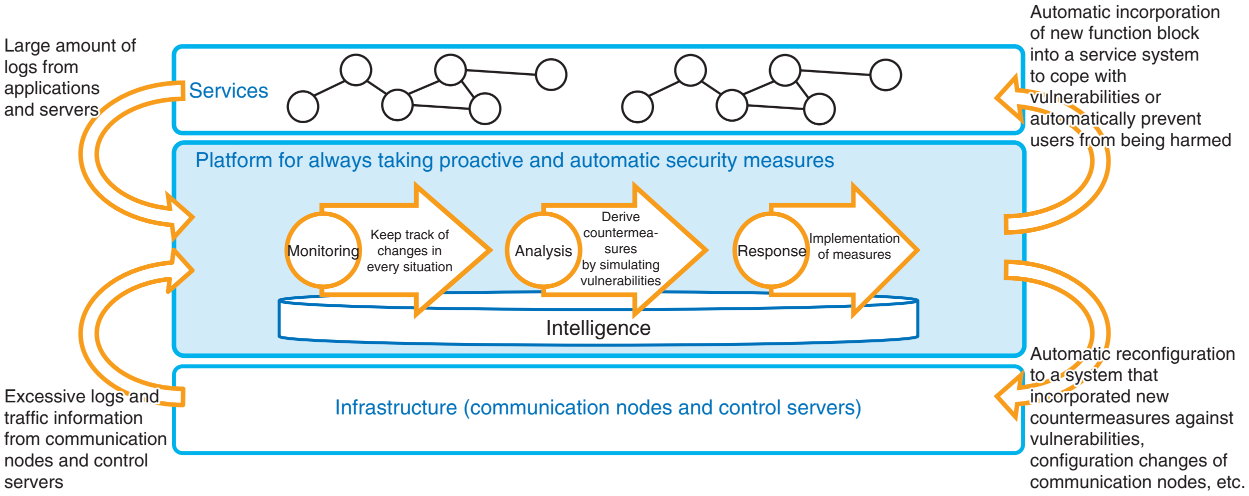

Large amount of logs from applications and servers
Services
Automatic incorporation of new function block into a service system to cope with vulnerabilities or automatically prevent users from being harmed
Platform for always taking proactive and automatic security measures
Monitoring
Keep track of changes in every situation
Analysis
Derive countermea-sures by simulating vulnerabilities
Response
Implementation of measures
Intelligence
Excessive logs and traffic information from communication nodes and control servers
Infrastructure (communication nodes and control servers)
Automatic reconfiguration to a system that incorporated new countermeasures against vulnerabilities, configuration changes of communication nodes, etc.

Fig. 3. Platform as a result of our R&D.

3. Platform as a result of our R&D

In security operations, many security measures, such as monitoring, analysis, and response, are implemented manually, so the ability to carry them out depends heavily on human skills.

By implmenting a platform with our technologies, we will constantly monitor the status of devices and applications that make up infrastructure and services and automatically execute security measures on systems in advance as soon as a vulnerable situation is found. The platform provides an environment to conduct stable, effective, and efficient security measures (**Fig. 3**).

4. Challenges in implementing the platform

To automatically and proactively implement security measures, we will conduct R&D on the following three technologies (**Fig. 4**) and create intelligence, as shown in **Fig. 5**.

(1) Technologies for actively visualizing and minimizing vulnerabilities, and implementing automatic correction cycles

To provide robust security, we will conduct R&D on visualizing and minimizing vulnerabilities, and also on implementing automatic correction cycles to enable shift-left security measures that can nip vulnerabilities in the bud and drastically improve efficiency of security operations.

(2) Technologies for generating and using intelligence that follows environmental changes

Security measures are continuously and autonomously implemented in a wide variety of ICT environments through technologies for automatically generating intelligence unique to telecommunication carriers and automatically using intelligence that does not require awareness.

(3) Technologies for countering human-induced risks

We will conduct R&D on security technologies that can respond to risks arising from humans and drastically reduce risks related to human errors, fraudulent attacks targeting humans, internal fraud by employees, etc., which can lead to security damage.

In the following section, we introduce our major R&D efforts.

5. Current activities

(1) Configuration and status analysis technology (**Fig. 6**)

We are currently conducting R&D on software agents and communication-analysis engines that analyze the configuration and status of Internet of Things devices for people and things as a security technology to protect complex cyber-physical systems composed of various elements such as smart cities. We will conduct R&D on crossing-analysis technology for multiple domains to detect signs of security anomalies and estimate probable causes and measures, which have been difficult in the past, by analyzing the correlation between elements across systems and services in addition to configuration and status.

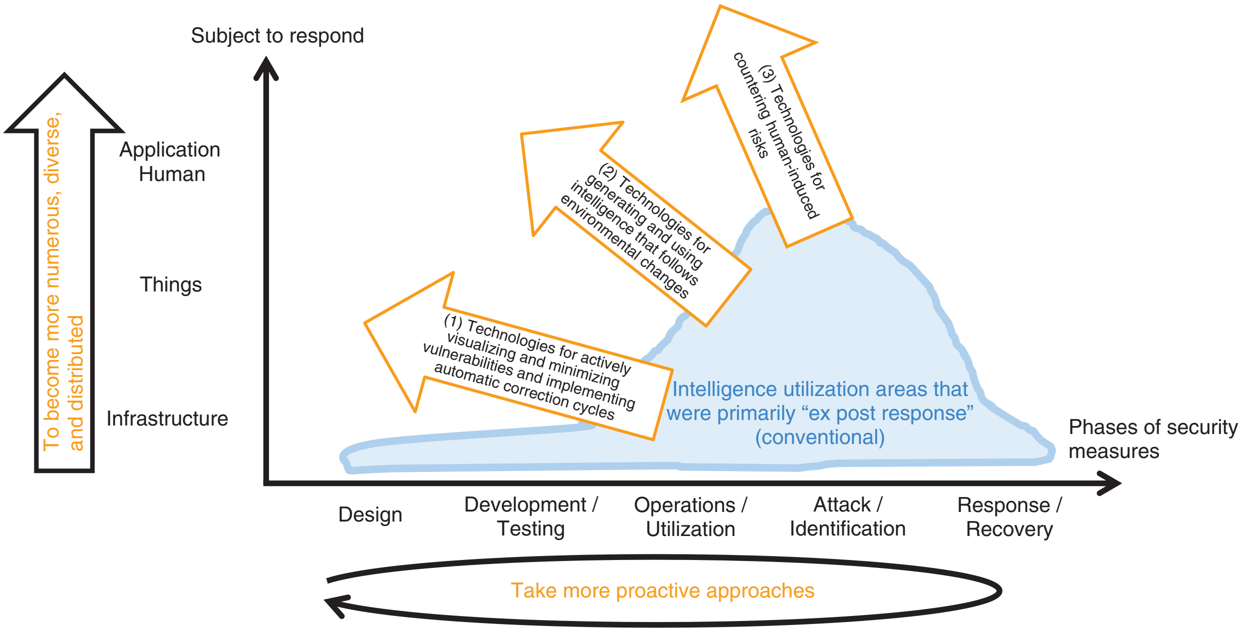
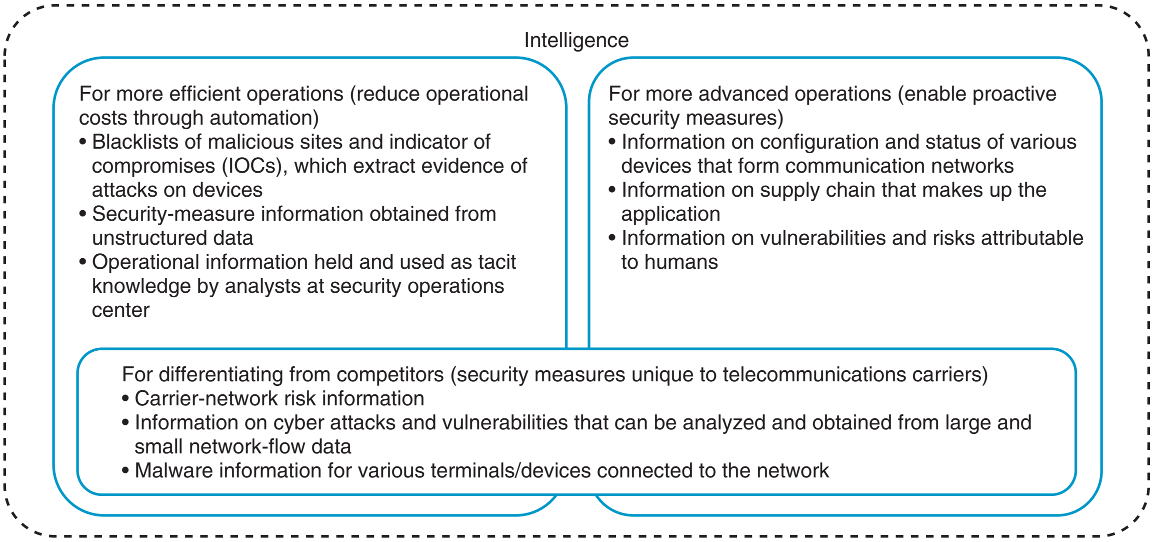

Subject to respond
To become more numerous, diverse, and distributed
Application
Human
Things
Infrastructure
(3) Technologies for countering human-induced risks
(2) Technologies for generating and using intelligence that follows environmental changes
(1) Technologies for actively visualizing and minimizing vulnerabilities and implementing automatic correction cycles
Intelligence utilization areas that were primarily “ex post response” (conventional)
Phases of security measures
Design
Development / Testing
Operations / Utilization
Attack / Identification
Response / Recovery
Take more proactive approaches

Fig. 4. Three technical issues.


Intelligence

For more efficient operations (reduce operational costs through automation)
- Blacklists of malicious sites and indicator of compromises (IOCs), which extract evidence of attacks on devices
- Security-measure information obtained from unstructured data
- Operational information held and used as tacit knowledge by analysts at security operations center

For more advanced operations (enable proactive security measures)
- Information on configuration and status of various devices that form communication networks
- Information on supply chain that makes up the application
- Information on vulnerabilities and risks attributable to humans

For differentiating from competitors (security measures unique to telecommunications carriers)
- Carrier-network risk information
- Information on cyber attacks and vulnerabilities that can be analyzed and obtained from large and small network-flow data
- Malware information for various terminals/devices connected to the network

Fig. 5. Intelligence created from our R&D.

(2) Initial-forensic-investigation technology (**Fig. 7**)

In cyber forensic investigation, a terminal that is suspected of being attacked is preserved, and a security analyst extracts evidence of an attack. While detailed analysis is possible from investigation by humans, it depends on the analyst’s experience and can take several days. In the initial investigation phase, therefore, its accuracy and speed remain issues for early clarification of the entire damage. Therefore, we are developing a technology for preserving only important logs and automatically extracting traces of attacks. The goal with this technology is to create an intelligence database of attack procedures that are often used by attackers and processing them

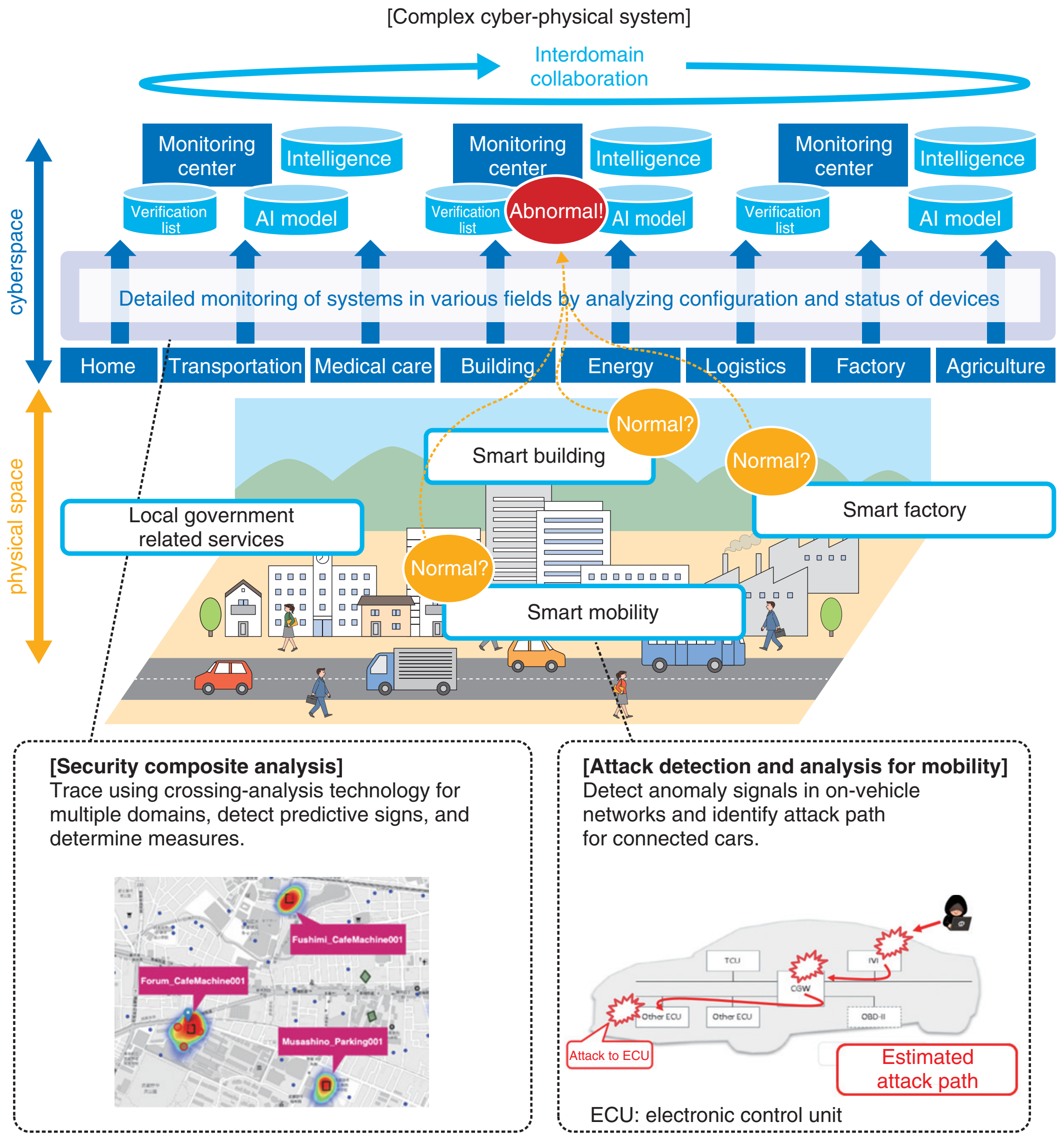

[Complex cyber-physical system]
Interdomain collaboration
cyberspace
physical space
Monitoring center
Intelligence
Verification list
AI model
Monitoring center
Intelligence
Verification list
Abnormal!
AI model
Monitoring center
Intelligence
Verification list
AI model
Detailed monitoring of systems in various fields by analyzing configuration and status of devices
Home
Transportation
Medical care
Building
Energy
Logistics
Factory
Agriculture
Normal?
Smart building
Normal?
Smart factory
Local government related services
Normal?
Smart mobility
[Security composite analysis]
Trace using crossing-analysis technology for multiple domains, detect predictive signs, and determine measures.
Fushimi_CafeMachine001
Forum_CafeMachine001
Musashino_Parking001
[Attack detection and analysis for mobility]
Detect anomaly signals in on-vehicle networks and identify attack path for connected cars.
TCU
IVI
CGW
Other ECU
Other ECU
OBD-II
Attack to ECU
Estimated attack path
ECU: electronic control unit

Fig. 6. Configuration and status analysis technology.

automatically. Initial investigations can be conducted in a few hours, regardless of the skill levels of analysts.

(3) Technology for detecting web-based social-engineering attacks that exploit human psychological vulnerabilities (**Fig. 8**)

Attackers use opportunities such as international sporting events and the spread of COVID-19 infection to attract people's interests and carry out cyber attacks that deceive users. Attackers can trick users into visiting a malicious site with interesting content or fake warning messages, causing malware infections and theft of money and personal information. We are conducting R&D on technology that can emulate the browser operations of deceived people, automatically crawl and collect webpages, and detect malicious sites with high accuracy and speed based on the image, language, and feature amount of the arrival path with the aim of reducing fraud damage targeting such people.

6. For the future

Cybersecurity risks can now threaten countries and are one of the most serious social problems. As the situation continues to be dominated by attackers, we

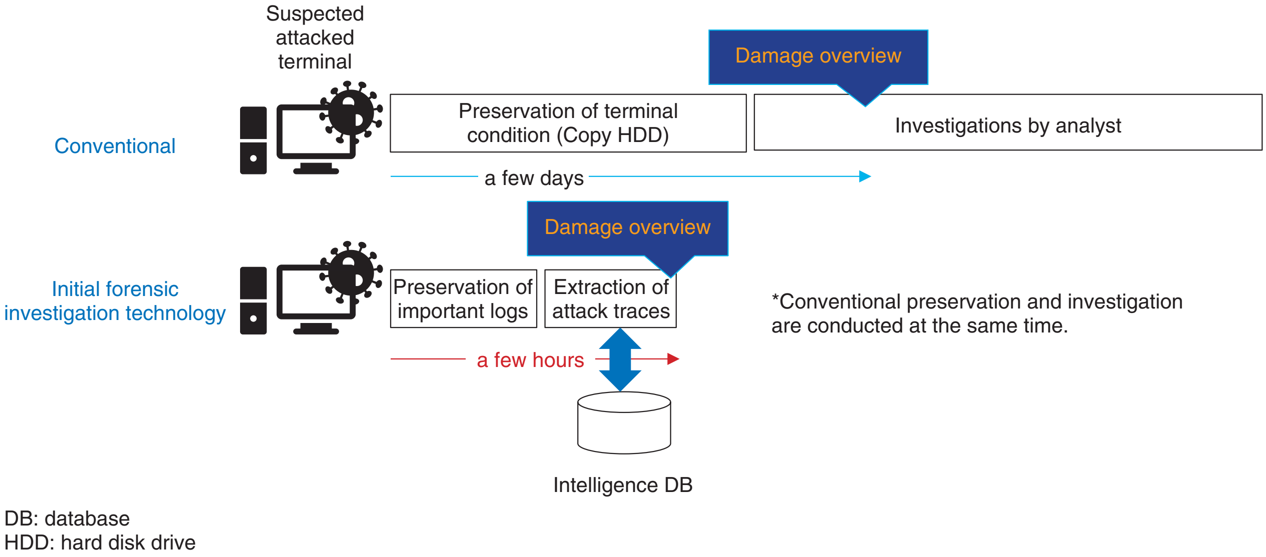

Suspected attacked terminal
Conventional
Damage overview
Preservation of terminal condition (Copy HDD)
Investigations by analyst
a few days
Initial forensic investigation technology
Damage overview
Preservation of important logs
Extraction of attack traces
*Conventional preservation and investigation are conducted at the same time.
a few hours
Intelligence DB
DB: database
HDD: hard disk drive

Fig. 7. Initial forensic investigation technology.

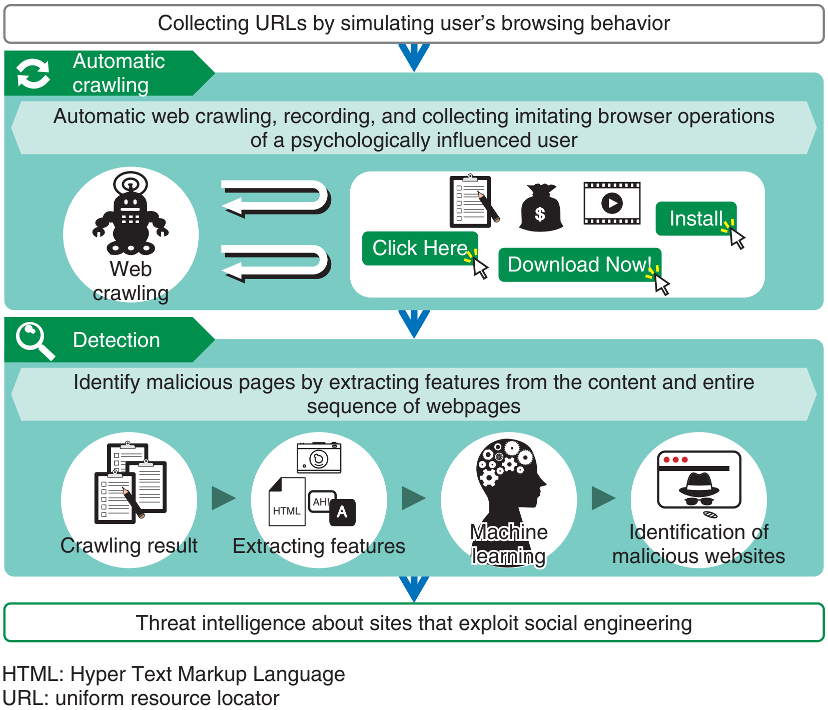

Collecting URLs by simulating user's browsing behavior
Automatic crawling
Automatic web crawling, recording, and collecting imitating browser operations of a psychologically influenced user
Web crawling
Click Here
Download Now!
Install
Detection
Identify malicious pages by extracting features from the content and entire sequence of webpages
Crawling result
HTML
Extracting features
Machine learning
Identification of malicious websites
Threat intelligence about sites that exploit social engineering
HTML: Hyper Text Markup Language
URL: uniform resource locator

Fig. 8. Technology for detecting web-based social-engineering attacks that exploit human psychological vulnerabilities.

will continue to contribute to the betterment of society by creating new security technologies that can overcome the current severe cybersecurity situation.

Yuzo Koga

Director, Head of Cyber Security Project, NTT Secure Platform Laboratories.

He received a B.E., M.E., and Ph.D. in instrumentation engineering from Keio University in 1996, 1998, and 2001. He joined NTT in 2001, and has had several years of experience in designing, building, and operating various communication services including identity management, cloud computing, the Internet exchange point, and the Internet access network. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Yoshiaki Nakajima

Director, Head of Security Operation Project, NTT Secure Platform Laboratories.

He received a B.S. in information science and an M.S. in mathematical and computing science from Tokyo Institute of Technology in 1995 and 1997. He joined NTT Information and Communication Systems Laboratories in 1997, where he worked on R&D of information security. From 2009 to 2013, he was with the Security Strategy Section of the Technology Planning Department. He has been involved in R&D of information and communication platforms, security platforms, and other areas. He is a Certified Information Systems Security Professional (CISSP) and Registered Information Security Specialist (RISS).

Naoko Chiba

Director, Cyber Security Project, NTT Secure Platform Laboratories.

She received a B.S. and M.S. from Tokyo Institute of Technology in 1998 and 2000. She joined NTT R&D in 2000 and has been working for more than 20 years in the information security field. Her research interest lies in high-quality and usable cybersecurity intelligence. She is a CISSP and a member of Information Processing Society of Japan (IPSJ).

Jun Miyoshi

Director, Cyber Security Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in system science from Kyoto University in 1993 and 1995. Since joining NTT in 1995, he has been researching and developing network security technologies. Prior to his current position, he was engaged in R&D strategy management of the Labs. from 2011 to 2015. He is a member of IEICE.

Takaaki Koyama

Director, Security Operation Project, NTT Secure Platform Laboratories.

He received an M.M.G. in media and governance from Keio University in 1996. He joined NTT in 1996 and has been studying several types of virtual private networks and software-defined networking as well as security operation systems for these network technologies. His research interests have recently extended to security analysis and operation technologies for smart cities. He is a member of IPSJ.

Hidehiro Shito

Director, Security Operation Project, NTT Secure Platform Laboratories.

He received a B.E. and M.E. in mechanical and system engineering from Yamanashi University in 1994 and 1996. He joined NTT in 1997. After several years of experience in R&D, operation, and construction of communications infrastructure, he started his career as a member of computer security incident response teams (CSIRTs) of organizations such as NTT EAST and NTT DATA. He joined NTT R&D in 2018, and his current position is a director of NTT-CERT (Computer Security Incident Response and Readiness Coordination Team), the representative CSIRT of the NTT Group.

Asami Miyajima

Director, Security Operation Project, NTT Secure Platform Laboratories.

She received a B.S. and M.S. in science and technology from Keio University in 1998 and 2000. She joined NTT R&D in 2000, and her research interests include cyber-physical systems security.