Japan Computer Emergency Response Team Coordination Center

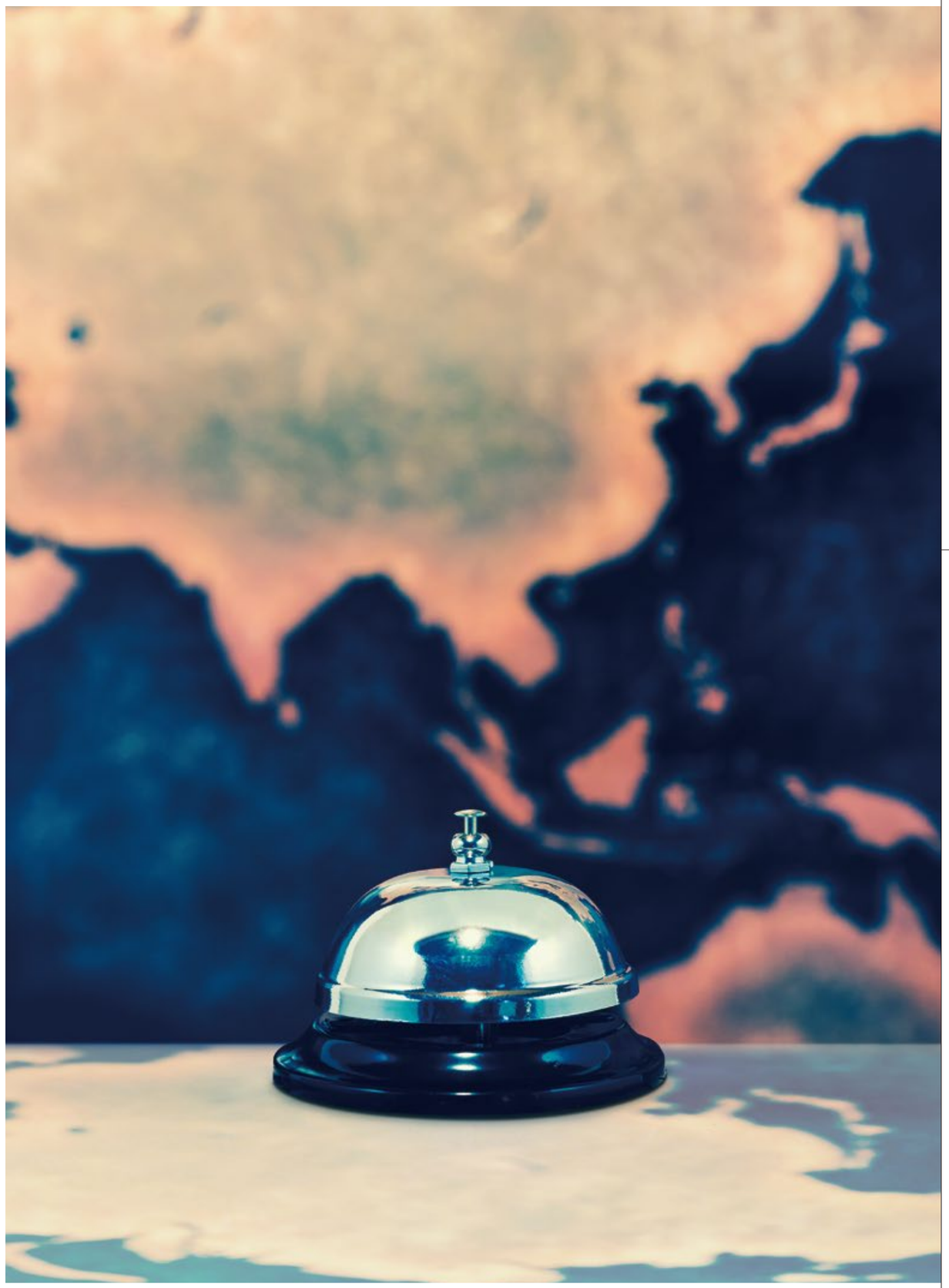
https://www.jpcert.or.jp/

JPCERT CC®

Japan Computer Emergency Response Team Coordination Center

Activity Outline

JPCERT Coordination Center



Coordination Center for Cyber Incidents

Towards a safer cyber space without incidents[*1]

Various causes lie behind incidents.
To respond to incidents and minimize damage,
knowledge and technology accumulated over many years are essential, and so is coordination with partners.
As Japan's point of contact for incident coordination,
JPCERT/CC is uniquely positioned to provide that function.

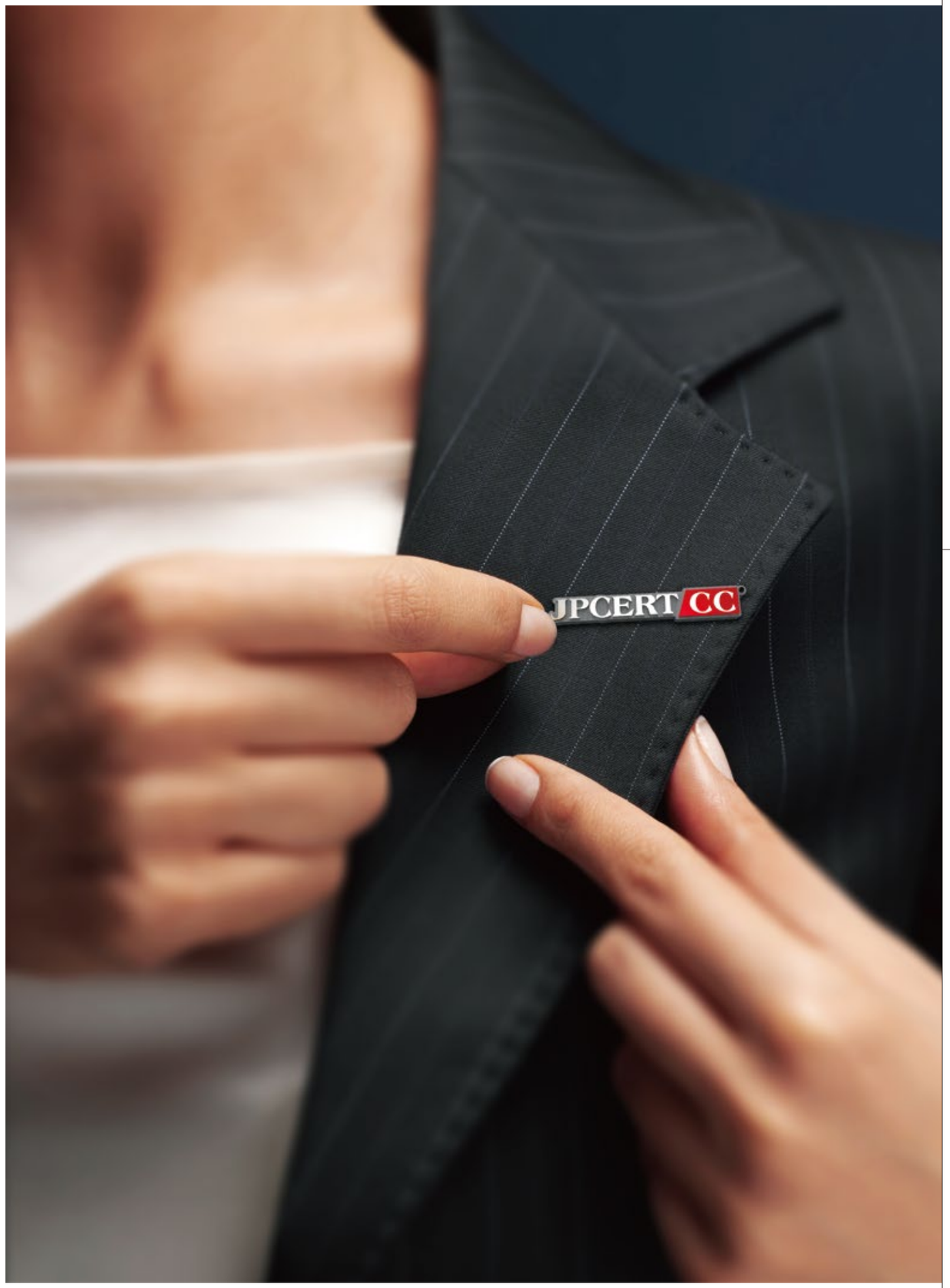
As a coordination center, we aggregate and coordinate information.

Incident response involves quickly responding to incidents that occur beyond national, regional, and industrial boundaries and preventing damage from spreading. For example, we receive information about incidents and malware from around the world and conduct technical and threat analyses. We promptly take appropriate steps to provide information to those who need it, and coordinate with partners in Japan and abroad and other national CSIRTs to solve the situation. To prevent damage from vulnerabilities in software, etc., we also study measures to reduce the impact of the vulnerabilities and help product developers address them. All our efforts are made with one aim: to continue to be a bulwark against cyber attacks that keep growing and transforming.

Connecting Japan and the world as Japan's point of contact for incident coordination.

Cyber security experts around the world advocate establishing Computer Security Incident Response Teams (CSIRTs) to be able to appropriately handle incidents that are becoming increasingly diversified. Many companies and organizations in Japan are heeding this advice and creating their own CSIRTs. CSIRTs enhance their ability to respond to incidents by sharing information, knowledge, and technology among the CSIRT community. JPCERT/CC is a neutral organization independent of any specific government agency or company, and coordinates with CSIRTs at home and abroad as Japan's point of contact for incident coordination. By supporting the establishment of overseas CSIRTs, we also develop contact points around the world and serve as a bridge that connect them.

*1 A cyber incident is "an event that may occur in the management of information and industrial control systems, and that may be considered a security issue."
In this document, cyber incidents are referred to as incidents unless otherwise noted.



Spirit

Facing cyber security with a spirit of coordination

Speed. Accuracy. Tenacity.
The essence of coordination lies in striking a balance between these seemingly contradictory elements.

Just after 5 a.m. Japan time, an incident is identified in Washington D.C. At JPCERT/CC, we immediately start collecting information, find the software exploit code suspected to be the cause, and get to work on analysis. Five hours later at 10 a.m., we have already grasped the situation, and we start coordinating with relevant parties to prepare to release information. It is around noon when we release a security alert to the Japanese public. This whole process is conducted in about half a day. It is said that malicious attacks are carried out in a matter of days after a vulnerability is published. In other words, speed is of the essence in thwarting attacks.

Delivering the right information to those who need it, in a world overflowing with information.

News reported by the media have a major social impact. When information is disseminated before it has been confirmed, that information takes on a life of its own, creates confusion, and often leads to a situation that works in favor of attackers. At JPCERT/CC, we release appropriate information such as Early Warnings and Security Alerts on a timely basis. On CISTA*1, a portal site run by JPCERT/CC to enable registered organizations to access and exchange security-related information, we emphasize information exchange between related parties, instead of simply providing information. JPCERT/CC aims to strengthen the defense capabilities of the community as a whole by serving as a hub and sharing analysis results.

Connecting researchers, vendors, and users through the power of coordination.

Vulnerabilities are security weaknesses that lie hidden in software and hardware systems. Cyber attacks are carried out by exploiting undiscovered and unaddressed vulnerabilities. Herein lies the meaning of coordination that mediates between those who discover vulnerabilities and product vendors. JPCERT/CC follows the spirit of researchers working on this problem, and notifies product vendors of reported vulnerability and negotiates with them. Then the product vendors deliberate countermeasures based on that information and release vulnerability information to the users. Vulnerability information is published on the product vendors' websites and on a website jointly run by JPCERT/CC and IPA*2 called JVN*3.*4

*1 Collective Intelligence Station for Trusted Advocates *2 Information-technology Promotion Agency, Japan *3 JVN: Japan Vulnerability Notes (https://jvn.jp/en)
*4 JPCERT/CC is a vulnerability coordinating body prescribed in the "Standards for Handling Vulnerability-related Information of Software Products and Others " (the Ministry of Economy, Trade and Industry's Public Notice No.19 of 2017) and the "Public Notice to Designate Receiving Bodies and Coordinating Bodies" (the Ministry of Economy, Trade and Industry's Public Notice No.20 of 2017).

History

A history of advancing coordination

In November 1988, an American graduate student created a program that infected numerous hosts on the Internet. Computers of universities and research institutions around the world were affected. This was the world's first Internet worm incident.

In 1992, in the early days of the Internet, it all began with a mailing list.

"Before another major incident takes place, we need to have a contact point for receiving information from overseas and for coordination." So in 1992, an organization that later became JPCERT/CC set up a contact point and started operation. In 1996, JPCERT/CC started providing information related to cyber incidents. In 1998, we became the first Japanese CSIRT to join the Forum of Incident Response and Security Teams (FIRST), an international forum of CSIRTs. We advocated the need for a CSIRT within Japanese companies and organizations, and started providing support for its establishment.

In 2000, websites of the central government were hacked, and many new threats emerged.

The incident in which the web pages of central government ministries and agencies were hacked and defaced shocked the public and alerted people to the importance of security. At the end of February 2000, the Government established the IT Security Office under the Cabinet Secretariat, which later became the National center of Incident readiness and Strategy for Cybersecurity. Around this time, new threats such as the Code Red worm and Nimda virus inflicted major damage. This was followed by the advent of botnets, and financially motivated phishing scams began. Under these circumstances, JPCERT/CC started Internet threat monitoring, fact-finding surveys of botnets, and handling of phishing scam reports. In 2004, JPCERT/CC was designated as a coordinating body for vulnerability information in a public notice issued by the Ministry of Economy, Trade and Industry, and further expanded its range of activities.

1992 Started handling computer security incident reports

1996 Launched the Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)

1998 Joined FIRST, an international forum of CSIRTs

2002 Hosted the Asia Pacific Security Incident Response Coordination Conference (APSIRC) forum

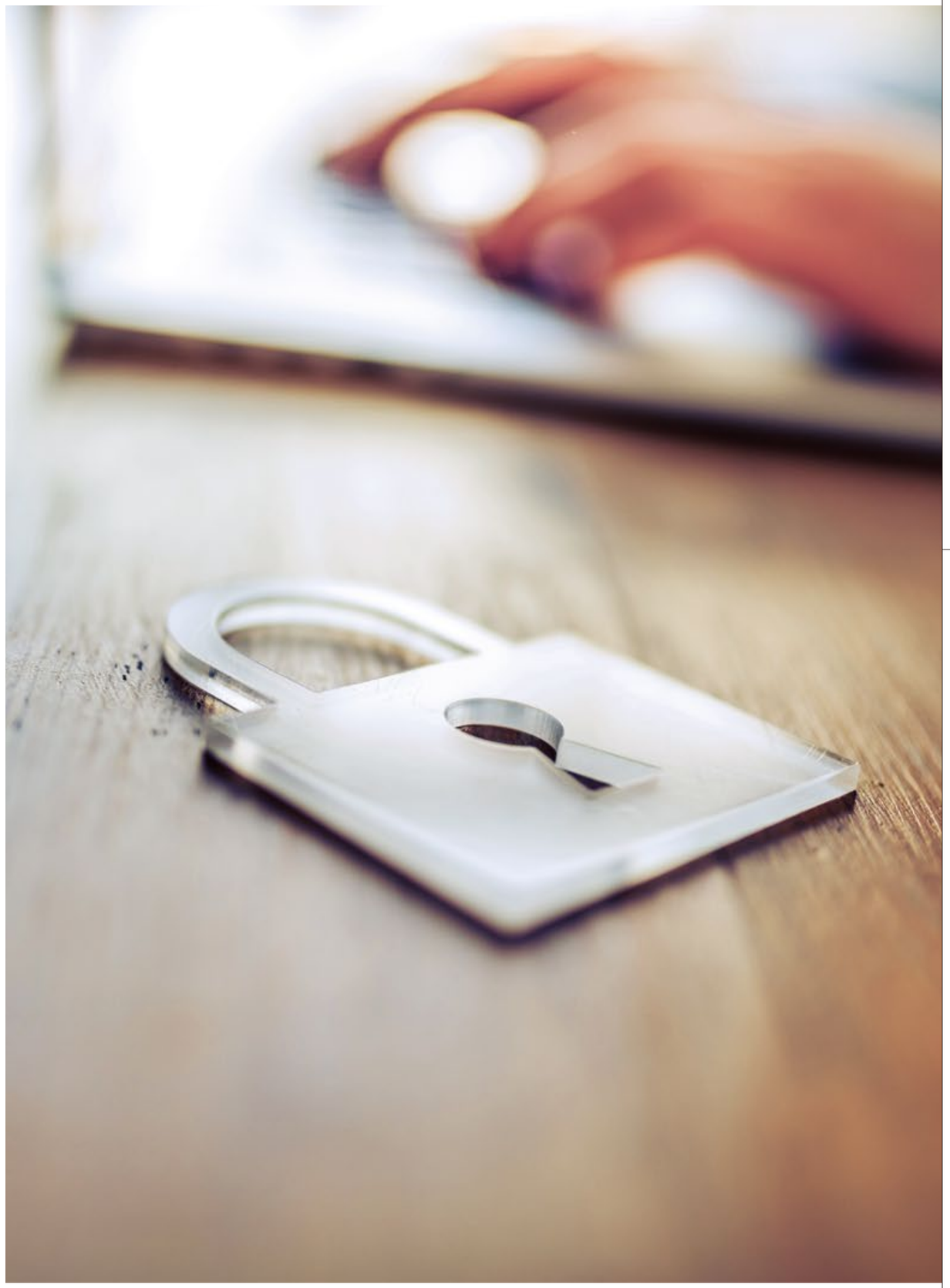
2003 Launched the Internet threat monitoring system

2004 Started providing vulnerability-related information

2005 Started early warning services

2006 Started Bot Program Analysis Group activities in connection with the bot countermeasure project jointly funded by the Ministry of Internal Affairs and Communication and Ministry of Economy, Trade and Industry

2007 Jointly established the Nippon CSIRT Association (NCA)



Technology

Technology cultivated for coordination

Our work is built on hard and steady application, and may be unglamorous. But the technology we develop thwarts Internet threats and crimes each day, and occasionally even prevents attacks that could rock the economy.

Responding to huge numbers of incidents with equal care

On the Incident Handling Status page*1 of the JPCERT/CC website, we provide daily updates on the numbers and types of incidents and phishing sites that are being handled. Highly sophisticated attacks are hidden among numerous and diverse attacks. Our job is to identify them by examining every single attack with thorough attention, and responding to them with the technology we have developed over the years. These efforts lead to coordination and further accumulation of knowledge.

Investigating incidents onsite, and analyzing them in the lab.

When it is found that an organization's server is being exploited as a command&control server for malware, we notify the organization of the situation, and in some cases we even visit them to investigate and analyze from every angle the artifacts that provide evidence related to the incident. In the case of malware, we run the program to examine its actual behavior. The binary program is deciphered directly through reverse engineering. It is an exploratory process that takes hard, steady work, but it allows us to directly examine the incident and find out how it works.

Highlighting attacker profiles through open source intelligence.

Open source intelligence is a profiling method that uses publicly available information. Experts can reveal a whole range of information about the attacker, including when he goes to bed, that attacks are carried out at roughly the same time of day, that attacks are triggered by commands, that the attacker may have few friends, and that the attacker is about the age of a junior or senior high school student. Needless to say, the more detailed the profile, the easier it is to plan a suitable defense strategy.

*1 https://www.jpcert.or.jp/english/ir/status.html

Human Resource

Human resources underpinning coordination

The unique role played by JPCERT/CC is
supported by its diverse human resources.
Its potential grows through engagement with various people.

A diversity of skills defines who we are.

Each day, we respond to incidents and vulnerabilities and complete coordination by email, by phone, or onsite. To help establish CSIRTs, we visit countries with different cultures and security situations and start by building personal relationships to serve as a foundation. We lock ourselves in the lab and study samples day after day to identify the hidden problem. We collect information related to various incidents, interact with parties in Japan and Asia to handle a range of secretariat duties, and call for security countermeasures through events and lectures. Yes, our work covers a lot of ground. That is why we have such a diverse range of human resources, each with different skills and backgrounds. We have them, because we need them.

One group. Two sets of thinking skills.

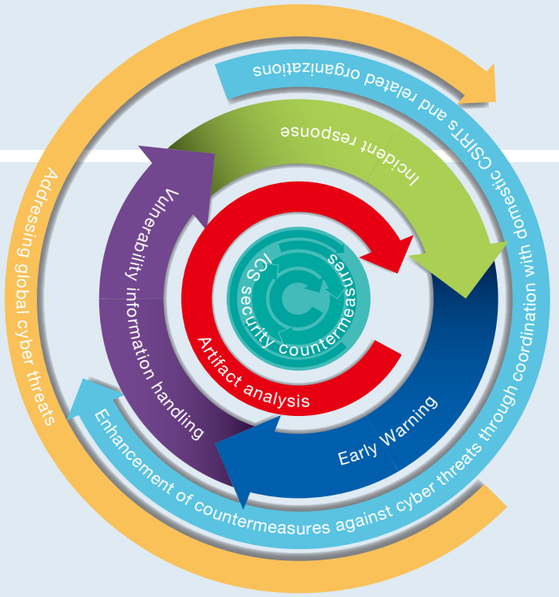
In "early warning" (p.15), for example, there is a duty that we refer to as open source intelligence, in which our staff unravel incidents using only publicly available information. The group tasked with this duty needs two sets of thinking skills. One is the capacity for accurate and meticulous thinking, the ability to examine a vast amount of information and extract and associate meaningful information. The other is the capacity for inspiration, the flashes of genius that find the most unexpected path leading to a single correct answer. Our daily early warning missions are operated based on these innate gifts and capacity for thinking that are refined through day-to-day operations and that compensate each other.

Connections with people and trust from organizations in Asia and the rest of the world.

By assisting the establishment of CSIRTs in countries and regions where they do not exist, we can help increase the security level across the world. We visit regions as far as Africa to offer support in creating CSIRTs. Over many years, we have continued these activities worldwide and cultivated relationships of mutual trust through personal interactions, so that we may help each other in times of need. For these reasons, we are recognized as a CSIRT representing Asia, and one of the leading CSIRTs in the world. Our human resources are rooted not just in Japan but across the world. JPCERT/CC and the window it opens to the world have a depth defined by its spirit, history, technology, and people. Through a combination of these elements, we continue our activities with the aim of creating a world where people can live with peace of mind.

Formation of JPCERT/CC

Incident control cycle for cyber security



The services provided by JPCERT/CC form a cycle comprising "prevention," "detection," and "response," which are elements of coordination activities aimed at controlling incidents and achieving cyber security.

"Incident response" (p.14) consists of support services designed to expedite handling of incidents.

It would be even better if incidents could be detected quickly. That is what we are aiming for with our "early warning" (p.15) services.

"Vulnerability information handling" (p.16) is a series of services such as identifying and removing system vulnerabilities at an early stage to minimize the occurrence or spread of incidents.

In the event of a serious incident, "artifact analysis" (p.17) is conducted to study related malware, etc. The analysis results are used to help respond to incidents and incorporated into our knowledge base to help prevent future incidents.

To operate this cycle effectively, we work on "enhancement of countermeasures against cyber threats through coordination with domestic CSIRTs and related organizations" (p.20). Through these activities, we create an environment that facilitates interaction between companies and JPCERT/CC.

We also engage in activities including overseas support, building relationships, and international coordination as part of "addressing global cyber threats" (p.19).

While past incidents primarily involved information systems, industrial control systems (ICS) that support the functions of critical infrastructure are also subjected to the threat of cyber attacks. In this area, we provide services in the form of "ICS security countermeasures" (p.18).

Responding to ongoing events that threaten security

Incident response

Incident response is at the core of CSIRT activities, and supporting incident response is the starting point of our activities. At JPCERT/CC, we study and analyze incident reports and other information provided from around the world each day, mainly to assess incidents related to stakeholders in Japan. We also provide technical assistance and conduct coordination necessary for incident response, with the aim of containing the damage caused by an incident and preventing its recurrence.

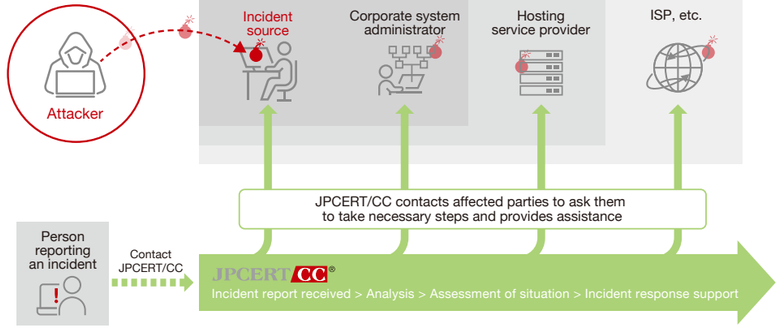


Figure 1: We coordinate between stakeholders in an incident and take measures to thwart attacks and prevent recurrence.

What is incident response?

Incident response refers to activities aimed at responding to incidents overall. More specifically, it consists of a diverse range of activities including identifying incidents, collecting necessary information and data, handling emergency situations, determining the extent of impact and cause, coordinating with relevant parties, and recovery.
Incidents we are called on to address also come in many types. From phishing and website defacement to malware infection, DDoS attacks, and targeted attacks, we need to prioritize and respond to various incidents that occur on a daily basis.
For instance, different approaches are required in responding to malware infections in which online banking account information is stolen and in which the malware is specially designed to carry out a targeted attack to steal critical information unique to a specific organization. Similarly, responses vary in dealing with phishing cases in which an organization's brand is misused, in which a phishing site is created on a website administered by an organization, and in which an organization's user is redirected to a phishing site.
Of course, there are no national boundaries in Internet-based incidents, and incident response is rarely completed within a single organization. Accordingly, setting up a point of contact for external communication is also an important point in incident response.

JPCERT/CC's incident response support services

JPCERT/CC serves as a point of contact for incident reports concerning organizations within Japan. In this function, we support incident response work, assess the situation, analyze methods used, and consider and propose recurrence prevention measures.
Based on analysis of incoming incident reports and other matters, if there is a concern that the same types of incidents may occur across a wide area, we issue security alerts and other information to call for action.
When people identify an incident that concerns their own organization or organizations within Japan, they can file an incident report with JPCERT/CC to receive consultation on how to handle the incident or request coordination for solving the problem. At JPCERT/CC, we coordinate not only with related organizations in Japan but also with overseas organizations through our international CSIRT partnerships to help solve problems. We sometimes coordinate with domestic organizations and provide technical assistance based on requests from overseas.
Incidents related to organizations are often recognized only after being contacted by us.

Detecting incidents and quickly providing appropriate information

Early Warning

Based on our own unique information network and knowledge accumulated over the years, we provide early warning information about anticipated incidents and information about incidents that might occur and have growing impact. We make sure the information reaches stakeholders quickly and after undergoing thorough scrutiny. Whether in normal or emergency situations, we contact the right person in an organization and provide reliable information on a timely basis.

Information from around the world examined to detect signs of attack

Each day, new causes of incidents that exploit vulnerabilities arise somewhere in the world. The Early Warning group investigates various sources of information, and looks for patterns in the information to detect "signs" of attack activities. In this effort, they scour message boards, malware information, incident reports, and elsewhere. Publicly available information sources may also contain critical information. In some cases, an analysis conducted in response to a report of damage may lead to the knowledge that another organization is being used as a springboard for attacks, or to the identification of the malware used to carry out attacks or the platform used by the attacker.

Information processed into five types and distributed according to content

The results of information collection and analysis are summarized in an easy-to-understand notification and provided using one of five types of distribution channels, including "early warning information" directed toward specific industries, etc., and "security alerts" made available to the general public on our web page. The most suitable distribution channel is chosen in light of the nature of the case at hand. [Table 1]

From providing information to sharing information, and to reducing risks

For example, in our early warning information, we provide incident and vulnerability information, attack warning, information related to advanced cyber attacks, and so on to organizations registered as users, through CISTA*1 and email. We assume this information will be used by personnel responsible for security countermeasures within the organizations.
The users who receive the information will feed back new information, further enhancing the quality of the information. [Figure 1]
By moving from one-way information provision to two-way information sharing, we will be able to reduce overall risks.

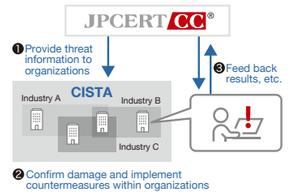


Figure 1: Accuracy of information is increased through information sharing, reducing risks to companies, industries, and communities.

*1 A portal site for limited users where important threat information can be obtained. Collective Intelligence Station for Trusted Advocates

Table 1: Speed, volume, or accuracy. Five media for providing information are used as appropriate according to the nature of information.

	Name	Description	Interval	Target	Distribution method
Alert	Early Warning (Japanese Only)	Information that mainly provides an overview of vulnerabilities and threats that are believed to have a major impact within the country or an impact on critical infrastructure operators, along with countermeasures. Unlike security alerts, this information is focused on immediacy.	As needed	Critical infrastructure, etc.	CISTA + email
Alert	Security Alerts	Information that mainly provides an overview of vulnerabilities and threats that are considered to have a major impact within the country, along with countermeasures that should be taken.	As needed	Companies, general users	Website + Mailing list
Reference	Analyst Notes	Important information selected from the vulnerability information, threat information, and security-related information collected daily, and edited along with analyst comments. Reference information positioned as "analyst notes."	Every day	Overseas CSIRTs, critical infrastructure, etc.	CISTA + email
Reference	Weekly Reports (Japanese Only)	Important vulnerability information released in the past one or two weeks, along with summaries of each information, targeted to system administrators of companies and organizations.	Every week	Companies, general users	Website + Mailing list
Reference	Cyber News Flash (Japanese Only)	Information summarizing matters with an ongoing or future impact within the country, along with an overview of the situation, not amounting to a security alert.	As needed	Companies, general users	Website

Supporting awareness and defense by providing timely information

Security countermeasures are a race against time. In some cases, attacks begin within days after vulnerability information is released. Early awareness and defense are key to minimizing damage. Timely information provision that makes it possible is also essential. Incidents related to organizations are often recognized only after being contacted by us.

For preventing security-related damage

Vulnerability information handling

Vulnerabilities are security weaknesses hidden in the operating systems, software, and embedded devices of smartphones, computers, home appliances, and so on. Attackers target those vulnerabilities. In vulnerability information handling, we relay information about vulnerabilities identified to product vendors to support their countermeasures, including creating patches and updates. Once the countermeasures are ready, we collaborate with the vendors to communicate countermeasure information to the product users through publication activities. This helps minimize the exploitation of vulnerabilities by the attackers and prevent the occurrence of incidents.

Delivering information about vulnerabilities and countermeasures to the right people

If vulnerability information is disseminated without any information about how to counter it, that information may be used to carry out attacks. To prevent that from happening, it is necessary to limit the sharing of vulnerability information to relevant parties until countermeasures are ready. It is also important to urge product users to quickly apply the countermeasures once they are ready. At JPCERT/CC, we strictly manage reported information concerning vulnerabilities and delivery it to product vendors, while communicating information about countermeasures to product users in an understandable language.

Serving as a linchpin of vulnerability information in Japan and the world

In Japan, the Ministry of Economy, Trade and Industry has issued a public notice prescribing "Standards for Handling Vulnerability-related Information of Software Products and Others" which calls on those who have identified vulnerabilities and product vendors to take appropriate steps. In response to this public notice, industry groups such as JEITA, JISA, CSAJ, and JNSA, IPA*1, and JPCERT/CC have jointly established "Guidelines for Information Security Early Warning Partnership," and are conducting vulnerability handling activities based on the guidelines. In addition, JPCERT/CC also collaborates with overseas CSIRTs and researchers to disseminate vulnerability information globally.

*1 IPA: Information-technology Promotion Agency, Japan

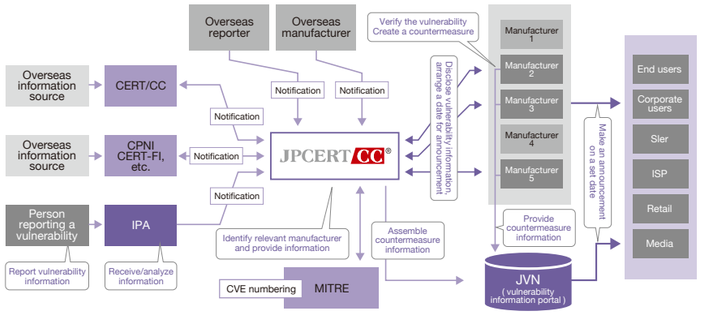
JVN portal site as a one-stop source for vulnerability countermeasure information

Primary information about vulnerability countermeasures is released by the vendors concerned, but countermeasure information about vulnerabilities handled by JPCERT/CC is also posted on the Japan Vulnerability Notes (JVN) portal site with the cooperation of product vendors. [Figure 1]
https://jvn.jp/en

Activities to promote and raise awareness of secure coding

Secure coding is gaining attention as a way to reduce vulnerabilities by taking security into consideration when developing software. This is an indispensable technique particularly in industries that provide products requiring high reliability, such as automobiles, medical devices, and control systems. At JPCERT/CC, we create and provide various materials for learning secure coding, including a Japanese version of the "CERT C Coding Standard," which was developed at the Software Engineering Institute at Carnegie Mellon University. We also hold various seminars and events both in Japan and abroad targeting product vendors and students.
https://www.jpcert.or.jp/sc-rules/

Figure 1: Vulnerability information is disseminated by JPCERT/CC and IPA and through the JVN portal site



CVE numbering:
JPCERT/CC has been certified by MITRE, a U.S. company managing and operating Common Vulnerabilities and Exposures (CVE), as a CVE Numbering Authority (CNA), and assigns CVE numbers.

Analyzing attack methods

Artifact analysis

"Artifacts" are traces left behind when an incident occurs. For example, malware, tools, and logs obtained from network devices are also artifacts. At JPCERT/CC, we investigate and analyze artifacts that provide evidence of an attack to study incidents including their cause [Figure 1]. Our analysis results are used to help support incident response and also provided as technical information to be widely used by companies and organizations.

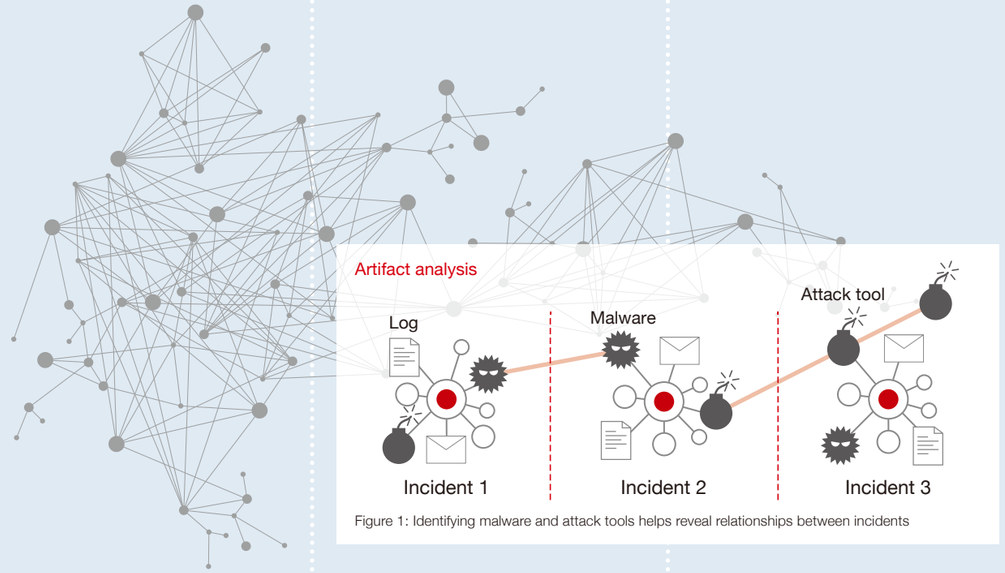


Figure 1: Identifying malware and attack tools helps reveal relationships between incidents

Incidents and artifact analysis

Some artifacts are commonly found in various places, while others are seen only in specific attacks. Analyzing artifacts requires accuracy and caution, and what approaches to use, how detailed an analysis should be, and so on need to be strictly decided, in light of the purpose of analysis, envisioned use of analysis results, and time and other constraints. In this effort, we need to coordinate people and technology, increase efficiency, and engage in analysis day after day. At JPCERT/CC, we have a system in place to allow us to prepare and establish an analysis environment and perform reviews at any time, so that we can respond and conduct analysis flexibly according to each artifact.

Artifact analysis is a means to link threats and incidents

When an incident occurs, various artifacts may be left behind, such as malware, logs, and attack tools. It is necessary to piece together the overall picture of the incident as accurately as possible by analyzing these artifacts as a composite whole. For example, in the analysis of malware, its functions and command&control servers can be clarified, but the infection route is rarely identified. Artifact analysis is conducted from various perspectives instead of being bound by a single piece of information, in an attempt to obtain information that will help measure the scope of impact and severity of the incident. [Figure 1]
At JPCERT/CC, we gather and analyze threat information including provided artifacts so that it can be used appropriately to respond to incidents, and we support incident response and provide information based on the analysis results.

Providing technical information and creating a community of analyzers

To help combat growing cyber attacks, JPCERT/CC makes technical knowledge obtained from artifact analysis available to the public, either summarized in the form of reports or incorporated into tools that can be used to counter cyber attacks.
We also maintain technical interchanges through conferences with artifact analysts from around the world and other channels.

Protecting the critical infrastructures of companies and society

ICS security countermeasures

Experts point out that industrial control systems (ICS) generally lag behind information systems in terms of security countermeasures, and security concerns surrounding ICS have been heightening in recent years. To help ensure that industrial plants, power plants, factory production lines, and so on do not come under cyber attacks and grind to a halt, JPCERT/CC collects and disseminates information that can be used to enhance ICS security, as well as responding to incidents and raising awareness.

Threat of cyber attacks is becoming a reality

In the end of 2015, a coordinated cyber attack was carried out against power facilities in Ukraine. In this incident, the attackers first intruded into an information system to find out the access route to an ICS, from which they entered a power transmission system and caused a major power outage affecting tens of thousands of households.
It used to be understood that an ICS is secure if it is cut off from other systems, or if external contact points are kept to a minimum. Recently, however, entry points for cyber attacks have increased due to linkage with ERP systems and other external systems, and more frequent use of temporary external connections with engineering PCs, USB devices, and so forth. In fact, cases of malware infection via such access routes are growing, infecting the universal operating system and other components of ICS.
Today, ICS is as much a target of cyber attacks as information systems, and if a security incident were to occur, the resulting damage can be enormous, including property damage and threats to human life.

At the Security Conference

Security awareness and countermeasures are especially required for mission critical systems

A wide range of critical infrastructures, including public utilities, railroads, aviation, logistics, and manufacturing, use ICS. At JPCERT/CC, we conduct awareness-raising activities targeting industries that use ICS, including the ICS Security Conference held each year in February, as well as lectures, surveys, research, and presentations. Since this is a relatively new field with limited case examples, learning from incidents abroad and the latest security countermeasures discussed at overseas conferences is essential.

Seven services provided by JPCERT/CC for ICS

At JPCERT/CC, we provide various service options tailored for ICS, based on services designed for information systems. The setup can be characterized as a smaller version of JPCERT/CC for ICS.

1. ICS incident response support
2. Collection, analysis, and dissemination of threat and reference information
3. Vulnerability information handling
4. Provision of self-assessment tools
5. ICS assessment services
6. Awareness-raising activities and external coordination
7. Surveys and research

Prevention activities are key to nipping critical incidents in the bud. It is important to ensure that no ICS is connected to the Internet without protection. We search for any Internet-reachable ICS. If there is, we contact and alert the company or organization concerned. We also gather and analyze information about ICS security from websites and mailing lists around the world, overseas CSIRTs, and other sources. We then compile this information into security alerts, reference information, newsletters, news clips, and so on, and provide them through our mailing lists and ConPas [Figure 1], a special portal site for ICS security information.
As a first step in implementing security countermeasures, we provide J-CLICS [Figure 2], a simple self-assessment tool that visualizes the status of ICS security countermeasures. For a more in-depth assessment, we provide the Japanese version of SCADA Self-Assessment Tool (SSAT), both available for free.

Figure1: ConPas screen

Figure2: J-CLICS simple self-assessment tool

Establishing and leading global CSIRT networks to address growing cyber threats

Addressing global cyber threats

As Japan's point of contact for incident coordination, JPCERT/CC has a structure in place for international collaboration with overseas CSIRTs, companies, research institutions, and other parties. For regions where CSIRTs do not exist, we provide training sessions on creating CSIRTs. We continue to demonstrate leadership in the global CSIRT community by building trust among CSIRTs through joint international projects and other efforts.

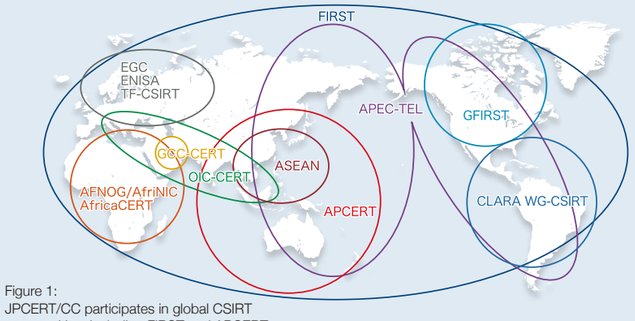


Figure 1:
JPCERT/CC participates in global CSIRT communities, including FIRST and APCERT

Building an international community founded on trust

CSIRT communities are formed on a regional basis and also to serve specific purposes. Among existing CSIRT communities, FIRST*1 stands out for its membership size and extensive track record of activities.
Ever since JPCERT/CC became the first Japanese organization to join FIRST, we have been supporting other CSIRTs in Japan and abroad seeking to join FIRST. We have also been deeply involved with APCERT*2, a CSIRT community in the Asia Pacific region, as a founding member, having served as its Secretariat and Steering Committee member to date. Through such activities, we have acquired trust in the international community, and we maintain cooperative relationships with the CSIRTs of other countries so that we may support each other in the event of an incident. [Figure 1]
While it is said that the Internet has no borders, differences in the culture, language, and legal system of each country pose difficulties in handling incidents. Collaboration based on trust among frontline engineers is indispensable to overcoming this challenge.

*1 Forum of Incident Response and Security Teams
*2 Asia Pacific Computer Emergency Response Team

Support for the establishment of overseas CSIRTs

We visit regions where CSIRTs are not fully established, and we help increase the incident response capabilities of those regions by holding training sessions to provide the know-how necessary for creating and running CSIRTs. To date, we have provided support primarily in the Asia Pacific region and Africa. Our wide range of support covers everything from technical matters directly connected with practical operations, including malware analysis and network forensics, to matters for organization managers, such as how a CSIRT organization should be run.

Working to support the establishment of CSIRTs

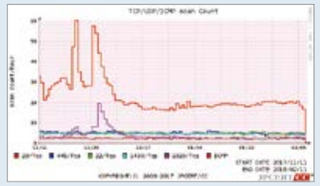


Figure 2: TSUBAME, a system that monitors Internet traffic for security threats

Operating TSUBAME and providing quantitative data on threat information

TSUBAME is a joint Internet threat monitoring system run by JPCERT/CC. [Figure 2]
It uses sensors deployed in Japan and abroad for monitoring threats and visualizes monitoring results. The data obtained by TSUBAME is shared mainly with the CSIRTs in regions that participate in the TSUBAME project*3.
We also support the activities of CSIRTs in each country by sharing signs of incidents based on data and providing training on analysis methods. In Mejiro, an Internet risk visualization service, we collect data on various risk factors on the Internet, calculate risk factor indicators for each country and region, and visualize the results.
By collaborating with organizations such as CyberGreen Institute, an NPO established following a demonstration experiment conducted by JPCERT/CC from 2014 to 2015, we are working to gather more useful monitoring data and improve the calculation formula for risk factor indicators.

*3 A project that deploys Internet threat monitoring sensors in national CSIRTs in the Asia Pacific region and others

Connecting domestic organizations and building on a foundation of trust

Enhancement of countermeasures against cyber threats through coordination with domestic CSIRTs and related organizations

At JPCERT/CC, we have a structure in place to coordinate with domestic companies and organizations with aim of sharing technical information related to incidents and facilitating incident response and countermeasures. Our contact point is kept available at all times so that necessary support and information can be provided to the right people and organizations at the optimal timing. We also engage in community activities to provide opportunities for the CSIRTs and security-related departments of various organizations to promote interaction and share knowledge about security countermeasures and other matters.

Point of connection for the information and people of companies and organizations

Incidents are often noticed only after receiving notification from the outside. For this reason, it is important to have a point of contact, make the point of contact known to external parties, and build relationships of trust as a basis for mutual communication in an emergency. These preparations must be made before an incident occurs.
JPCERT/CC serves as a contact point for consultations and inquiries from domestic companies and organizations in the event of an incident. We also maintain and regularly update a list of contacts (i.e., security departments and personnel) to enable smooth mutual communication at all times, direct contacts to the appropriate department or person in JPCERT/CC or a related organization according to the nature of the communication, and support the early resolution of problems and establishment of a cooperative framework.

Delivering threat information securely to the right people

Whether in normal or emergency situations, collecting, analyzing, and sharing information is important for incident response and countermeasures. We share information through our CISTA portal site with a wide range of parties, including government organizations, public institutions, operators of critical infrastructure such as railroads and public utilities, leading operators of SNS and other businesses directly connected to people's lives, manufacturers, trading companies, and organizations with an internal CSIRT. [Figure 1]

Aiming to create a framework for close collaboration among teams to resolve incidents quickly

As the Secretariat of the Nippon CSIRT Association

Organizations are advised to establish an internal CSIRT as a measure to reduce damage and regain control more quickly when a computer security incident occurs. The Nippon CSIRT Association was founded to enable CSIRTs within organizations to collaborate and share information including early signs of attacks and how to deal with incidents.

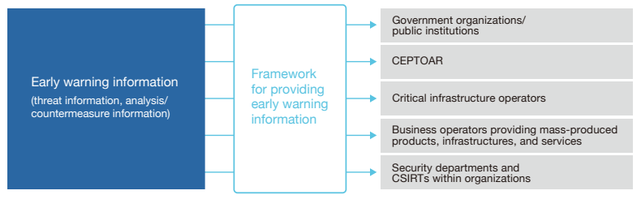


Figure 1: Early warning information provided to registered business operators.

JPCERT/CC is one of the founding members and also serves as its secretariat to help facilitate operations.
https://www.nca.gr.jp/en

To reduce damage from phishing scams within Japan

As the Secretariat of the Council of Anti-Phishing Japan

The Council of Anti-Phishing Japan was established by organizations working to address phishing, a fraudulent act in which the victim is lured into visiting a fake web page to steal IDs, passwords, and other personal information, with the aim of raising the awareness of general users and business operators by providing information and organizing events. The Council receives reports concerning phishing and provides security alerts and materials on responding to and taking measures against phishing attacks.
JPCERT/CC supports its activities as its secretariat, as well as handling coordination for the closure of phishing sites, creating documents for publication, and operating the Council's website.
https://www.antiphishing.jp/

Providing accumulated knowledge and a foundation of trust to facilitate activities

We leverage the foundation of trust built over the years and our wealth of knowledge to support operations and facilitate activities.

JPCERT/CC information portal sites

In addition to our official website, we run original portal sites targeting specific audiences with clear objectives.
On JVN, we provide information related to vulnerabilities and their countermeasures. CISTA serves as a forum for sharing information about incidents.
ConPas is an information portal site that deals specifically with ICS security. Here we provide an overview of each site, along with their characteristics.

JVN Japan Vulnerability Notes

JVN : Japan Vulnerability Notes

This portal site provides and archives information about vulnerabilities in software and other products used in Japan, along with countermeasure information. It was launched in response to the "Rules for Handling Information Related to Vulnerabilities in Software Products, etc.," a public notice issued by the Ministry of Economy, Trade and Industry, and it has been jointly operated by JPCERT/CC and the Information-technology Promotion Agency, Japan (IPA) since July 2004. The website is intended to help system administrators, system integrators, product vendors, and others to assess the threat of a vulnerability and take appropriate countermeasures. On JVN, we provide information about vulnerabilities reported and coordinated in accordance with the Information Security Early Warning Partnership scheme, and vulnerability information coordinated with CERT/CC and other overseas coordinating bodies.
It can be used without any procedures.

https://jvn.jp/en

CISTA

CISTA : Collective Intelligence Station for Trusted Advocates

This portal site provides and shares threat information as well as analysis and countermeasure information on a timely basis. Specific users such as information security-related departments and internal CSIRTs of organizations that provide infrastructures, services, or products that have a major impact on people's social activities are able to receive security alerts and early warning information from JPCERT/CC, and also use the website as a platform for sharing information among companies and industries. By sharing information about damage within organizations, countermeasures taken, and so on, users are able to grasp the status and overall picture of incidents and reduce the risk of threats.

(Japanese Only)

ConPaS Control System Security Partner's Site

ConPas : Control System Security Partner's Site

This portal site specializes in ICS security information. It provides materials including security alerts and reference information, newsletters, and security information distributed via mailing lists for sharing ICS information, guides to enhancing ICS security (documents related to ICS security, international standards, etc.), and survey and research reports. It can also be used as an archive of newsletters and reference information issued in the past.

(Japanese Only)

Sending inquiries and requests to JPCERT/CC

The following is a list of contacts for JPCERT/CC's services introduced in this document.
Please contact us at the addresses shown below.
If you wish to request incident response or ICS incident response services, please be sure to review the information posted on our website before doing so.
Please note that it may take a few days for us to respond to inquiries.

https://www.jpcert.or.jp/english/

Subject of inquiry		Contact
Security alerts / Weekly Report		ew-info@jpcert.or.jp
Early Warning information	Inquiries regarding administrative procedures	cista-sec@jpcert.or.jp
	Inquiries about the contents	cista-info@jpcert.or.jp
Vulnerability countermeasure information		vultures@jpcert.or.jp
Documents, lecture requests, citations		pr@jpcert.or.jp
Internet threat monitoring, other		office@jpcert.or.jp
International operations		global-cc@jpcert.or.jp

If you wish to request incident response or ICS incident response services,
please be sure to review the information posted on our website before doing so.

https://www.jpcert.or.jp/english/ir/form.html

Incident handling	info@jpcert.or.jp

https://www.jpcert.or.jp/english/cs/how_to_report_an_ics_incident.html

ICS incident handling	icsr-ir@jpcert.or.jp

* Personal information contained in inquiry emails will be handled according to JPCERT/CC's privacy policy.
  Personal information will be used for the sole purpose of responding to inquiries.
  https://www.jpcert.or.jp/english/privacy.html
* Please note that it may take a few days for us to respond to inquiries.

JPCERT Coordination Center
Tozan Bldg. 8F, 4-4-2 Nihonbashi-honcho, Chuo-ku, Tokyo 103-0023, Japan
TEL: +81-3-6271-8901 FAX:+81-3-6271-8908 https://www.jpcert.or.jp/