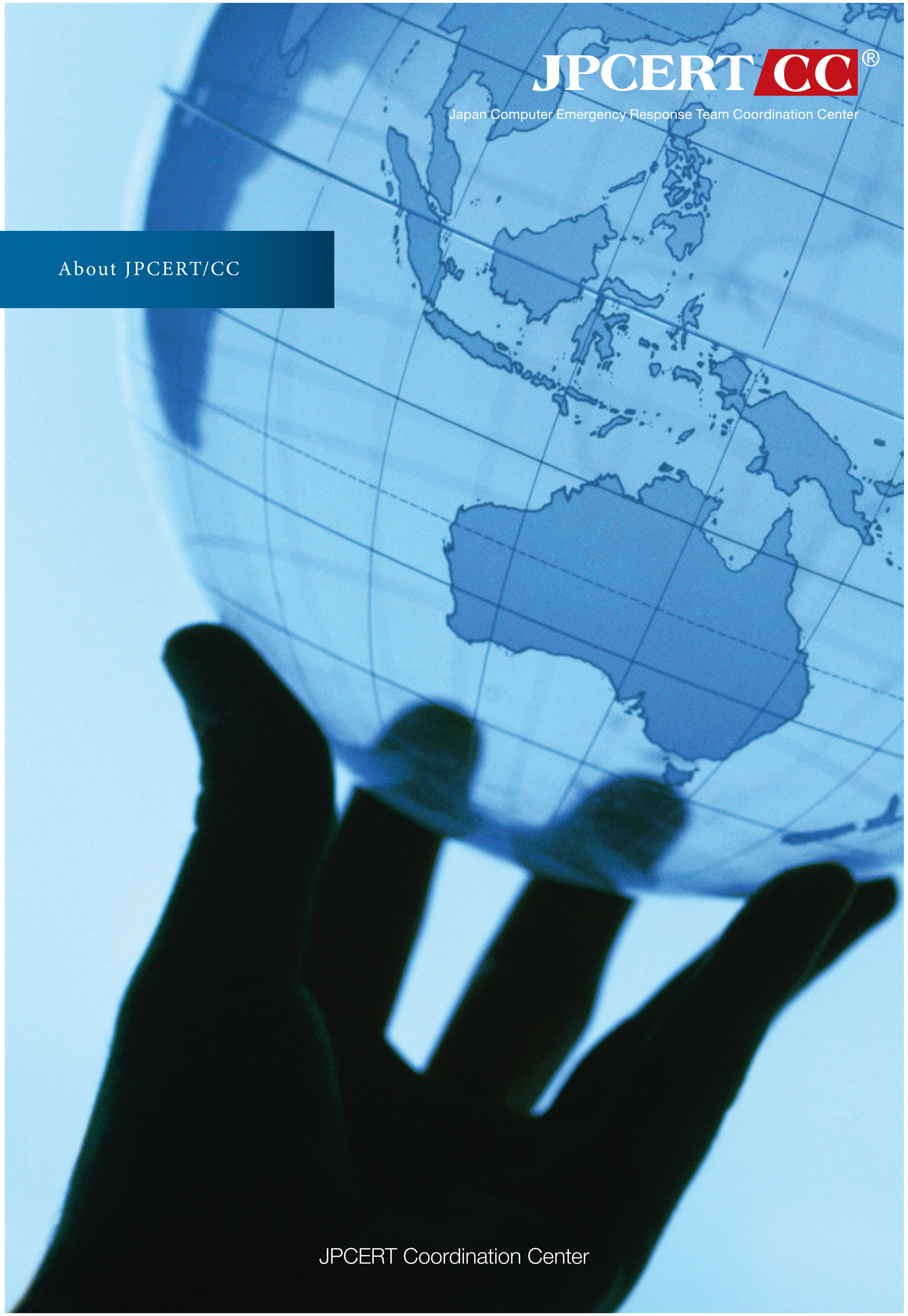
JPCERT/CC®

JPCERT Coordination Center
Hirose Building Floor 11, 3-17 Kandanishiki-cho, Chiyoda-ku, Tokyo, 101-0054
TEL : +81-3-3518-4600　FAX : +81-3-3518-4602　http://www.jpcert.or.jp/

GREEN PRINTING JFPI
P-B10054
This document was printed on environment-friendly material manufactured at a plant with a green printing certification, with print materials compliant with green criteria.

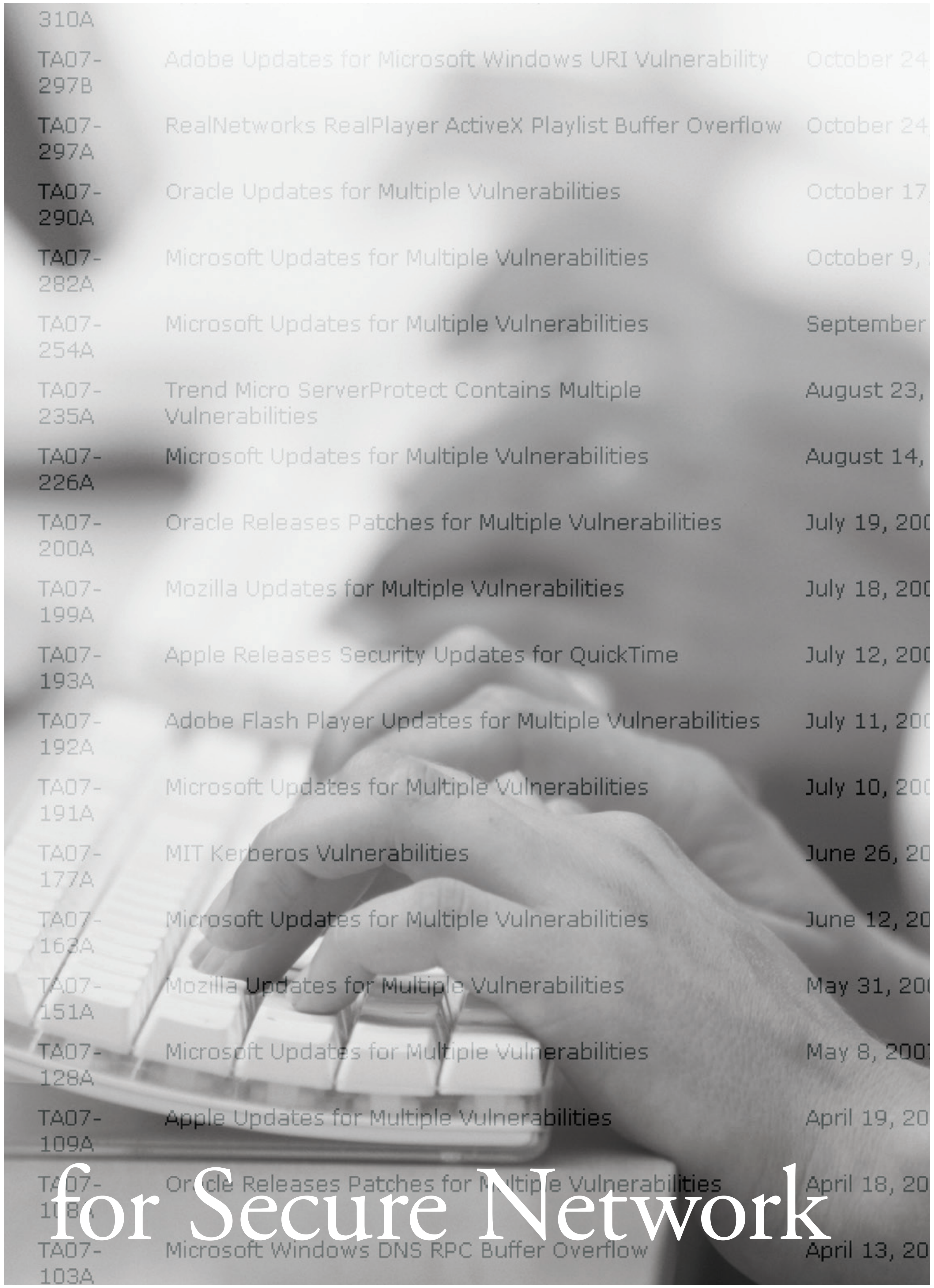


JPCERT/CC®

Japan Computer Emergency Response Team Coordination Center

About JPCERT/CC

JPCERT Coordination Center


310A
TA07-297B Adobe Updates for Microsoft Windows URI Vulnerability October 24
TA07-297A RealNetworks RealPlayer ActiveX Playlist Buffer Overflow October 24
TA07-290A Oracle Updates for Multiple Vulnerabilities October 17
TA07-282A Microsoft Updates for Multiple Vulnerabilities October 9,
TA07-254A Microsoft Updates for Multiple Vulnerabilities September
TA07-235A Trend Micro ServerProtect Contains Multiple Vulnerabilities August 23,
TA07-226A Microsoft Updates for Multiple Vulnerabilities August 14,
TA07-200A Oracle Releases Patches for Multiple Vulnerabilities July 19, 200
TA07-199A Mozilla Updates for Multiple Vulnerabilities July 18, 200
TA07-193A Apple Releases Security Updates for QuickTime July 12, 200
TA07-192A Adobe Flash Player Updates for Multiple Vulnerabilities July 11, 200
TA07-191A Microsoft Updates for Multiple Vulnerabilities July 10, 200
TA07-177A MIT Kerberos Vulnerabilities June 26, 20
TA07-163A Microsoft Updates for Multiple Vulnerabilities June 12, 20
TA07-151A Mozilla Updates for Multiple Vulnerabilities May 31, 20
TA07-128A Microsoft Updates for Multiple Vulnerabilities May 8, 200
TA07-109A Apple Updates for Multiple Vulnerabilities April 19, 20
TA07-108A Oracle Releases Patches for Multiple Vulnerabilities April 18, 20
TA07-103A Microsoft Windows DNS RPC Buffer Overflow April 13, 20
for Secure Network

JPCERT CC®

Expansion of threats following the development of network technology. Security measures becoming crucial for all network users.

Today, the Internet is a part of daily life for people of all ages. Inter-business communications, various administrative services, and individual financial transactions have become more and more dependent on e-mail, the web, and social media, while new uses for the web have begun to take hold.

At the same time, the expansion of such network use has created various security issues. One of the main causes is that users who are not as computer literate have increased and thus are more likely to be victims of misconduct using computers. As a result, they can be unwittingly involved in attacks on others. A second cause is that the systems that support these increasingly sophisticated networks are becoming more and more complex, making it difficult to construct and operate systems free of vulnerabilities or other security issues. Compounding this, knowledge regarding methods of attacking such vulnerable networks as well as tools that exploit vulnerabilities are being freely exchanged or bought and sold in public and private forums and markets. If broad, effective countermeasures are not adopted, society may suffer considerable consequences as a result of the continuing weakness of these vulnerable networks.

For everyone who uses networks to continue to seek greater efficiency and create new value, comprehensive security measures would need to be implemented to contain threats that keep growing on networks. The implementation of security measures will require cooperation both in and between organizations as well as countries.

Incident Handling

Our mission is to assist people dealing with security issues at the front. JPCERT/CC responds to a rapidly changing world.

JPCERT/CC's origins in Incident Response Support

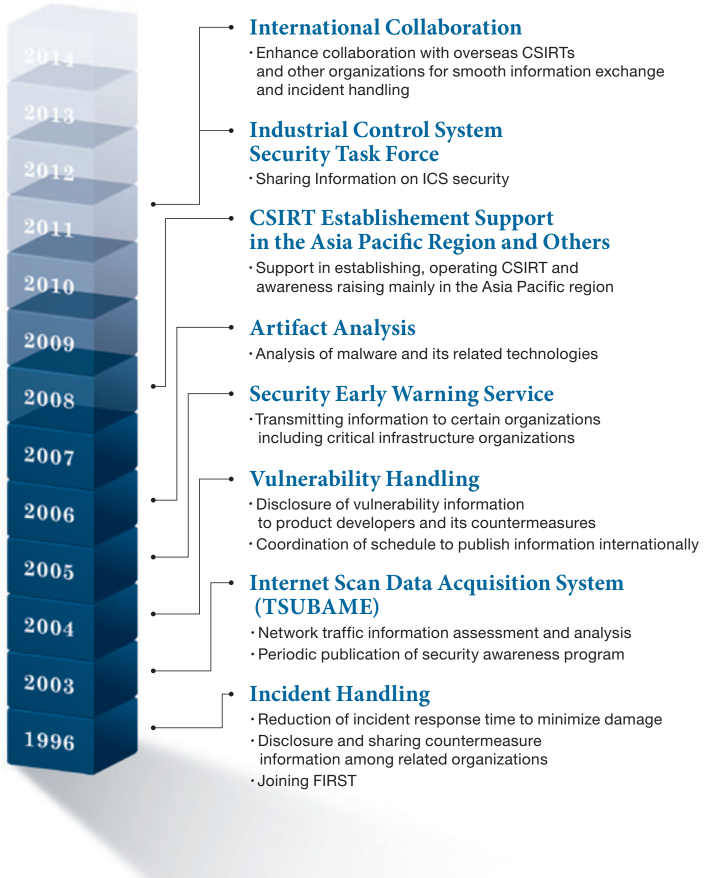
In 1992, JPCERT Coordination Center (known as "JPCERT/CC") initiated its incident response operations for system security incident reports. It was founded by volunteers with the common belief that Japanese computer security must be protected. In 1998, JPCERT/CC became the first Japanese member of FIRST (Forum of Incident Response and Security Teams), the international forum of CSIRTs *1 (Computer Security Incident Response Teams), and has continued to expand its global incident response activities since. Moreover, in 2004, JPCERT/CC was designated by the Ministry of Economy, Trade and Industry to act as the coordination institution to publicly disclose software and other vulnerability-related information. Through these activities, JPCERT/CC has accumulated significant experience in coordinating response operations among domestic and international organizations.

Receiving Incident Reports and Taking Preventative Action

Monitoring incidents in real time and minimizing their impact is important in addition to adopting countermeasures against incidents that have occurred. JPCERT/CC has deployed sensors to capture incident occurrences to collect, analyze and publish information on security threats, malware and its related technologies (artifact) which can be used for cyber attacks. The focal point of JPCERT/CC is to provide timely and practical countermeasure information for organizations supporting IT infrastructure. This includes companies supporting critical infrastructure such as water supply, electricity, ISPs, etc., where the existence of a security incident or vulnerability can have a major impact on society.

Taking Security Activities to the Next Level

The mission of JPCERT/CC is to support the activities of those who are in the field of information security by monitoring security threats. JPCERT/CC continues to utilize its expertise in incident response support, network observation, coordination of software and other vulnerability related information, artifact analysis, and related international cooperation and information gathering.



International Collaboration
- Enhance collaboration with overseas CSIRTs and other organizations for smooth information exchange and incident handling

Industrial Control System Security Task Force
- Sharing Information on ICS security

CSIRT Establishement Support in the Asia Pacific Region and Others
- Support in establishing, operating CSIRT and awareness raising mainly in the Asia Pacific region

Artifact Analysis
- Analysis of malware and its related technologies

Security Early Warning Service
- Transmitting information to certain organizations including critical infrastructure organizations

Vulnerability Handling
- Disclosure of vulnerability information to product developers and its countermeasures
- Coordination of schedule to publish information internationally

Internet Scan Data Acquisition System (TSUBAME)
- Network traffic information assessment and analysis
- Periodic publication of security awareness program

Incident Handling
- Reduction of incident response time to minimize damage
- Disclosure and sharing countermeasure information among related organizations
- Joining FIRST

*1 A CSIRT is an organization that provides countermeasure information to relevant organizations through the collection of various incident reports and security related information as well as assessment and analysis of the situation.

CSIRT @ Japan

JPCERT/CC®

JPCERT/CC is a coordination center for incident response. Collaborative activities are performed domestically as well as internationally.

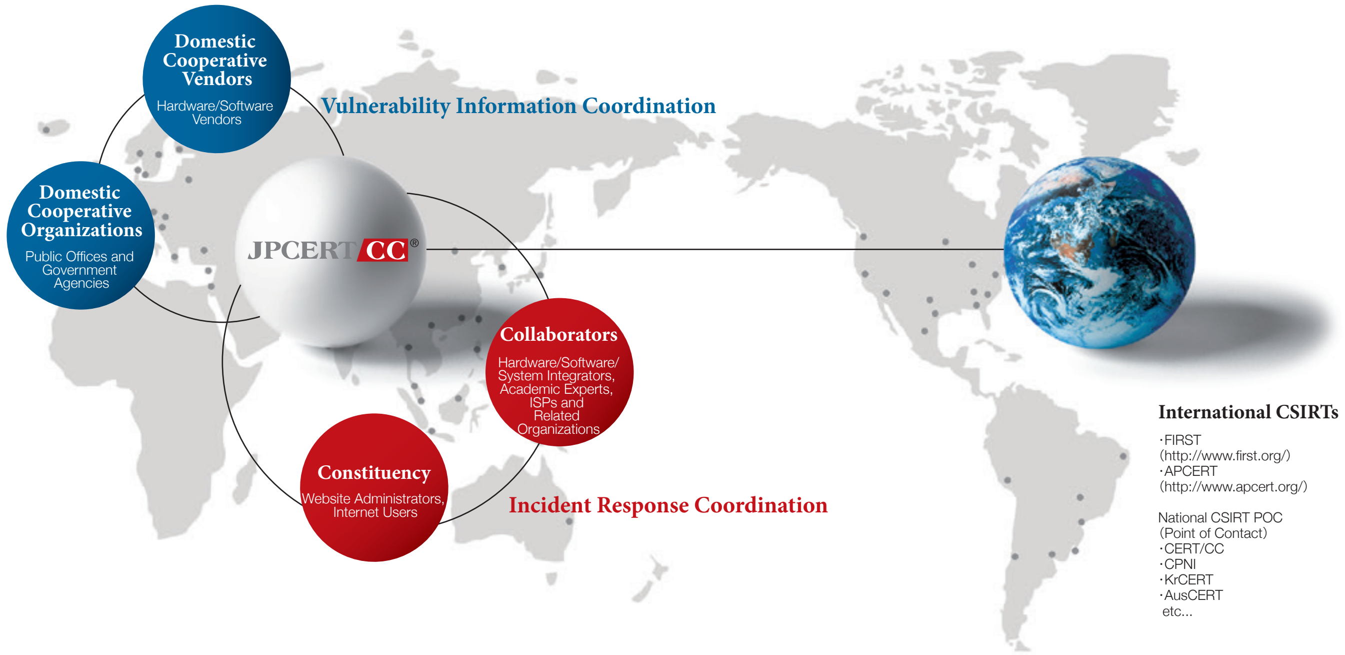
Activity as a CSIRT within Japan

JPCERT/CC is an organization that coordinates the activities of CSIRTs and other related organizations to report computer security incidents and vulnerability related information. Acting as the national CSIRT of Japan, JPCERT/CC coordinates between domestic and international CSIRTs and related organizations to manage incidents that require international coordination.

To improve the level of computer security domestically, JPCERT/CC collects incident reports from various sources such as product developers, vendors, and users; assesses and analyzes how incidents occurred; and provides support for incident response including attacker profiling. The results from the assessment and analysis are published as countermeasures. The goal of these activities is for the user to implement these countermeasures and prevent cyber attacks by making it increasingly difficult for attackers.

Your Security is our Security: Security Enhancement across National Borders

With respect to security, a global perspective is required as the entire world is highly interconnected via the Internet. JPCERT/CC has been involved in the administration of FIRST, the international forum of CSIRTs, as a core member, exchanging information with about 309 CSIRTs in 67 countries. (as of December 1,2014) In addition, thanks to partnerships with the United States' CERT/CC and the United Kingdom's CPNI for vulnerability related information coordination, as well as collaboration with China's CNCERT/CC, Korea's KrCERT/CC and CSIRTs of other countries, JPCERT/CC has strengthened its relationships with those organizations.


Domestic Cooperative Vendors
Hardware/Software Vendors
Domestic Cooperative Organizations
Public Offices and Government Agencies
JPCERT/CC®
Vulnerability Information Coordination
Collaborators
Hardware/Software/ System Integrators, Academic Experts, ISPs and Related Organizations
Constituency
Website Administrators, Internet Users
Incident Response Coordination

International CSIRTs

- ·FIRST (http://www.first.org/)
- ·APCERT (http://www.apcert.org/)

National CSIRT POC (Point of Contact)

- ·CERT/CC
- ·CPNI
- ·KrCERT
- ·AusCERT

etc...

CSIRT Community

JPCERT/CC promotes CSIRT establishment and operational support in Japan and the Asia-Pacific region.

APCERT Enables and Promotes Information Exchange

In the Asia-Pacific region, cultures, legal systems, economic levels and Internet adoption rates vary greatly from one country to another, in spite of their geographical relationship. Some countries do not have their own national CSIRT, where concerns in the computer security field vary depending on the country. APCERT (Asia Pacific Computer Emergency Response Team) is an organization that supports those countries and promotes efficient information coordination in the Asia-Pacific region. 27 teams in 20 countries (as of December 1,2014) including China, Korea are members of APCERT.

JPCERT/CC joined APCERT as a governing board member and has been serving as its secretariat.

National CSIRT Establishment Support in the Asia-Pacific Region

In countries where Internet use is expanding, but there is no national CSIRT facility available and information security related literacy is insufficient, coordination can be difficult in the event of a security incident. As a result, this makes it difficult to minimize possible damages. Furthermore, multinational corporations conducting business activities in those regions may be concerned about the risk of security incidents.

For such regions, JPCERT/CC provides expertise to establish and operate national CSIRT support services including training to perform incident response operations.

CSIRT Establishment Support for Domestic Organizations

JPCERT/CC has assisted domestic companies in establishing their own CSIRT facilities, providing expertise and technical support. JPCERT/CC has participated in the building of a framework so that Japanese CSIRTs can closely work together.

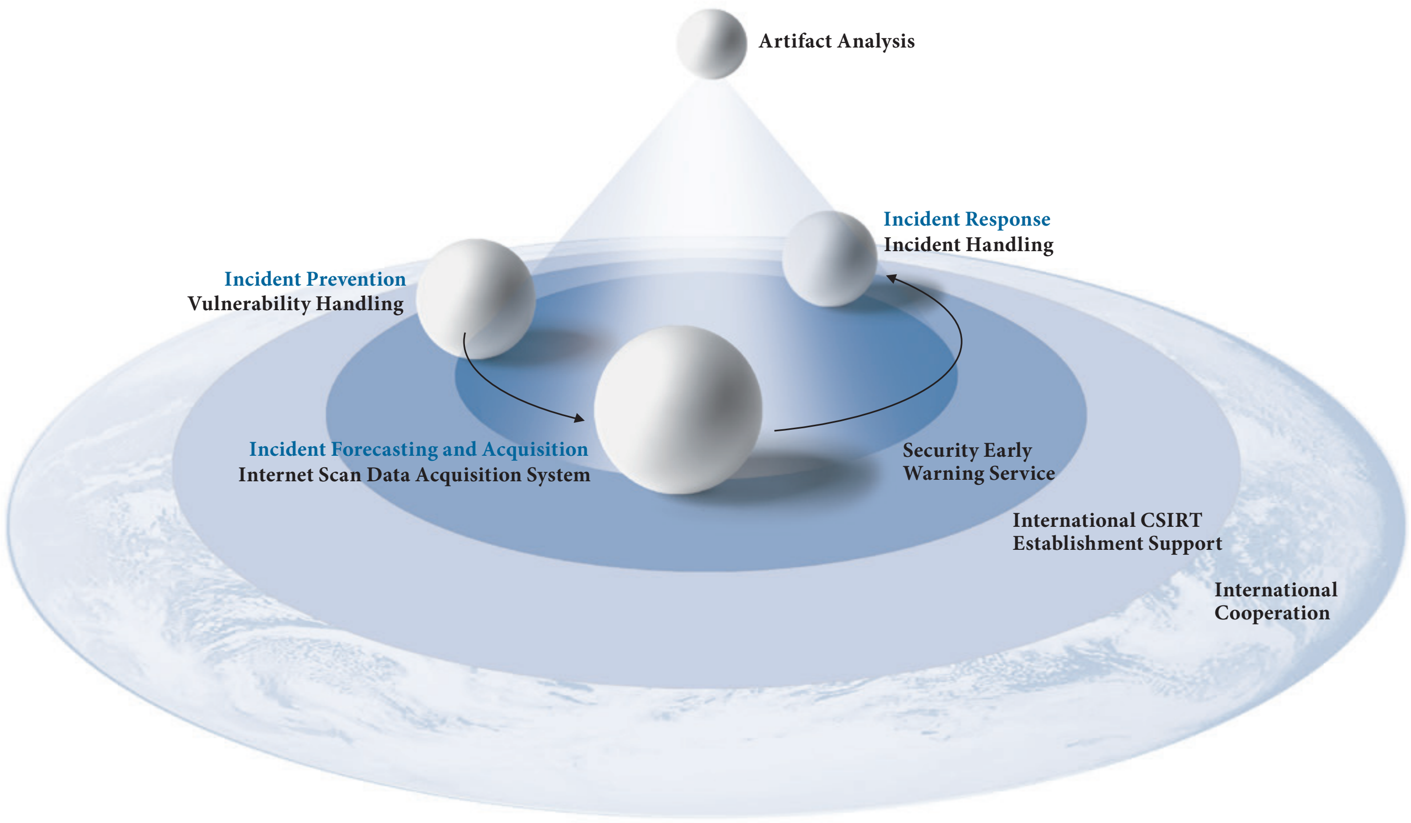
AfricaCERT

LaoCERT

ThaiCERT / ETDA

APCERT

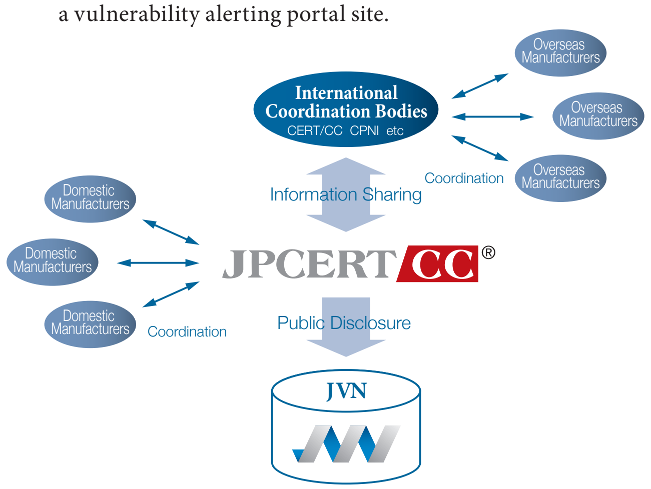
JPCERT/CC activities are aimed at providing practical measures for the prevention and resolution of security incidents.
This is achieved through the use of advanced analysis techniques to assist companies and other organizations in adopting countermeasures.



Vulnerability Handling

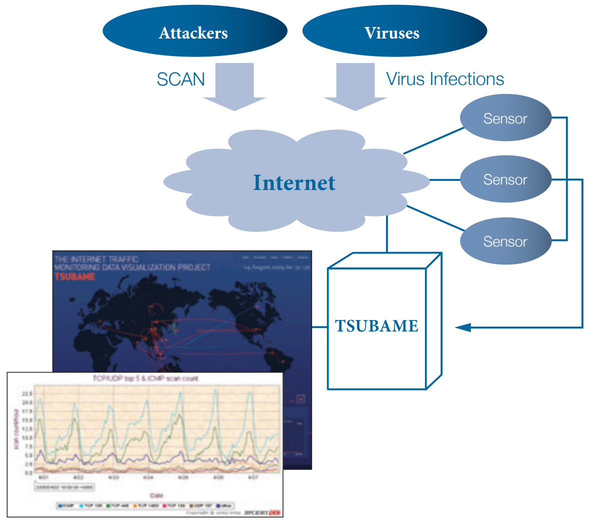
JVN Japan Vulnerability Notes

Vulnerability handling is a process to publish accurate vulnerability information in order to reduce the likelihood of possible incidents. JPCERT/CC provides vendors with information on detected vulnerabilities, requesting patches and workarounds. It manages advisory releases schedule with international CSIRTs and other related organizations so that vulnerability information can be published at the same time. JPCERT/CC publishes the information on JVN, a vulnerability alerting portal site.



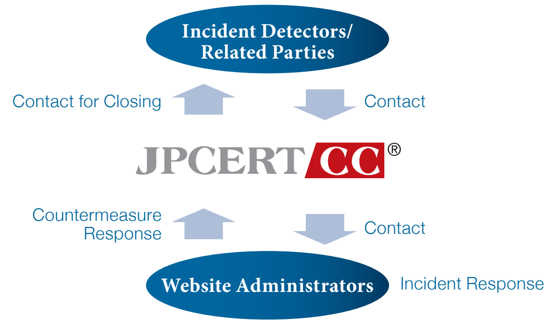
Internet Scan Data Acquisition System: TSUBAME

JPCERT/CC has deployed a system with sensors distributed throughout the Internet to observe various scanning activities such as worm infections and vulnerabilities. The observed data is analyzed and used for providing security awareness programs. This data is analyzed in cooperation with other observers and international CSIRTs.


Attackers
Viruses
SCAN
Virus Infections
Internet
Sensor
Sensor
Sensor
TSUBAME
THE INTERNET TRAFFIC MONITORING DATA VISUALIZATION PROJECT
TSUBAME
TCP/UDP top 5 & ICMP scan count
Date

Incident Handling

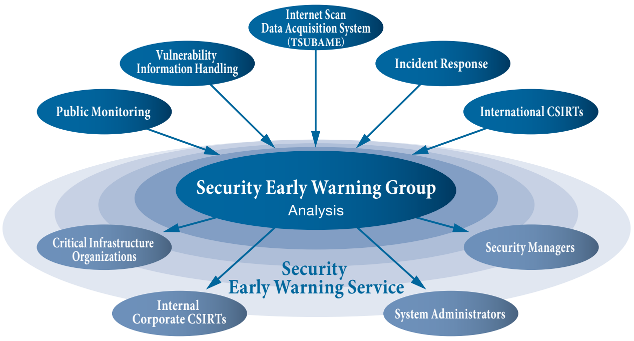
As a CSIRT working in cooperation with domestic and international CSIRTs, JPCERT/CC receives incident reports and provides support as necessary. For example, if it receives notification of a phishing site detected in a foreign country, it works in cooperation with that country's CSIRT and requests closure of the site. Information about the incident and countermeasures are exchanged and shared to minimize the damage and prevent future recurrence.



For incident related information please contact us as follows:
Email: info@jpcert.or.jp
Web: http://www.jpcert.or.jp/form/

Security Early Warning Service

JPCERT/CC has collected and analyzed various types of domestic and international threat information through vulnerability handling, TSUBAME, incident handling and published security alerts. Countermeasure information is provided to domestic critical infrastructure organizations including electric and gas companies, airlines, and railway companies. JPCERT/CC has provided support for establishing an internal CSIRT for organizations, while performing cyber security exercises to enable these organizations to conduct incident responses properly.



International CSIRT Establishment Support

JPCERT/CC has provided expertise and technical support for establishing national CSIRTs in the Asia-Pacific region. In addition, it provides periodic incident response training to strengthen cooperation among national CSIRTs and to better prepare for emergencies.

Artifact Analysis

JPCERT/CC analyzes malware and its related technologies (artifact) which can be used for cyber attacks and conducts research on countermeasure techniques. The findings are incorporated into the published information that forms the basis of JPCERT/CC activities. JPCERT/CC has made approaches to share analysis within the community.

Industrial Control System Security

To promote security measures for industrial control systems, we introduce guidelines and tools, as well as cases that illustrate advanced measures or otherwise merit attention, through security conferences, the portal site, and e-mail newsletters.

Portal Site for Safe and Secure Infrastructure

WAISE

This portal site provides security alerts and countermeasure information on a timely basis and is dedicated to particular users, including critical infrastructure organizations. This site is designed to assist the incident response activities of such organizations .

Vulnerability Decision Assistance

KENGINE

An assistance program that provides efficient countermeasure deployment methods for organizations based on decision making rules and threat analysis criteria created by each organization. It assists these organizations in conducting efficient vulnerability management.