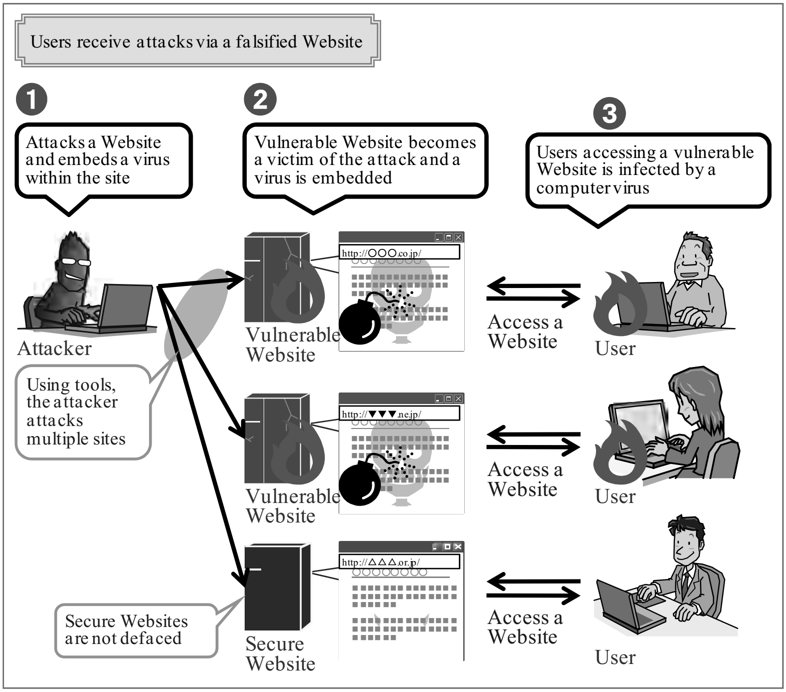
Threats to System Administrators/Developers

【1st】 Threats of Attacks via a Legitimate Website [2nd Overall]


Users receive attacks via a falsified Website
1
Attacks a Website and embeds a virus within the site
2
Vulnerable Website becomes a victim of the attack and a virus is embedded
3
Users accessing a vulnerable Website is infected by a computer virus
Attacker
Using tools, the attacker attacks multiple sites
Secure Websites are not defaced
http://○○○.co.jp/
Vulnerable Website
Access a Website
User
http://▼▼▼.ne.jp/
Vulnerable Website
Access a Website
User
http://△△△.or.jp/
Secure Website
Access a Website
User

As in the previous year, we also saw the spread of "Attacks via a Legitimate Website" in 2008, in which a legitimate Website is defaced and users accessing it suffer from certain damages.

<Outline of the Problem>

For an attack aimed at those visiting a legitimate Website, the first objective of an attacker is to attempt to deface the Website. While various methods can be used for Website forgery, SQL Injection Attacks that exploit SQL Injection Vulnerability in web applications were most commonly seen in 2008. SQL Injection Attacks are designed to attack databases used for Websites (e.g., compromising, falsifying or deleting the information contained in the database). In some cases, defaced Websites are used as the source of subsequent attacks. Attackers are said to be using a tool that automatically carries out those attacks.

<Progress of the Problem>

In Japan, SQL-Injection-driven information leakage incidents occurred in 2005 caused the issue of SQL Injection Attacks to appear frequently on the news. Originally, this attack was designed to steal the information on databases used for Websites but, around 2007, it began to change its form and, nowadays, it is designed to embed a computer virus into a legitimate Website so that the Website visitors would catch that virus. This sort of attack method has become prominent, producing further damages (For details, please refer to "[1st] Diversified Infection Routes for Computer Viruses and Bots" in "Threats to Users").

According to the observation by security vendors in Japan, the number of SQL-Injection-driven incidents in 2007 was higher than the previous year and the number increased at an accelerating pace in 2008. Moreover, cases surfaced in which user IDs and passwords that were stolen on a Website were used illicitly to use other site's services, as the users had been using the same User ID and password for multiple Websites (For details, please refer to "[4th] Threats Arising from Using the Same User ID and Password" in "Threats to Users").

<How to Address This Problem>

One of the reasons why SQL Injection attacks are on the rise is, while a Website that interacts with a database has become common, there still are many sites whose countermeasures against SQL Injection attacks are insufficient.

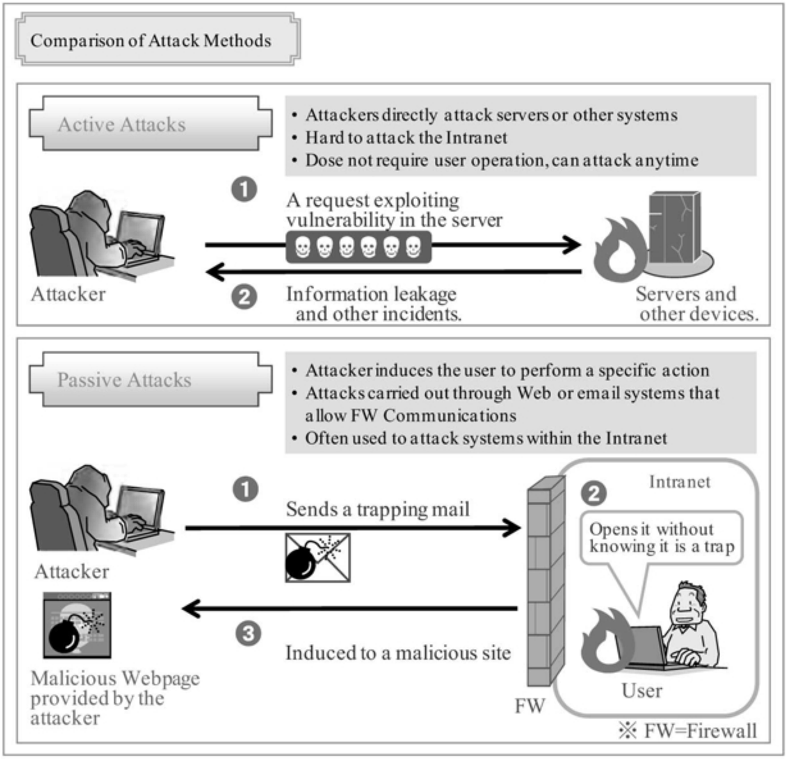
When using a database for the Website, system administrators and Web application developers should incorporate SQL Injection countermeasures into their programs during the design and development phase. Developers should strive to improve Website security by referring to document such as "How to Secure Your Website", published by IPA. They also need to consider Website vulnerability scan and system renovation programs.

References

ラック:改ざんされたWebサイト閲覧による組織内へのボット潜入被害について
http://www.lac.co.jp/news/press20081222.html (in Japanese)
NRI Secure Technologies: セキュリティ診断結果の傾向分析レポート2008年版を公開
http://www.nri-secure.co.jp/news/2008/0728.html (in Japanese)
IPA: Security Alert for SQL Injection Attacks
http://www.ipa.go.jp/security/english/vuln/200805_SQLinjection_en.html
IPA: How to Secure Your Web Site 3rd Edition Released
http://www.ipa.go.jp/security/english/vuln/200806_websecurity_en.html

Threats to System Administrators/Developers

【2nd】Actualized Passive Attacks [7th Overall]


Comparison of Attack Methods
Active Attacks
• Attackers directly attack servers or other systems
• Hard to attack the Intranet
• Dose not require user operation, can attack anytime
❶ A request exploiting vulnerability in the server
Attacker
❷ Information leakage and other incidents.
Servers and other devices.
Passive Attacks
• Attacker induces the user to perform a specific action
• Attacks carried out through Web or email systems that allow FW Communications
• Often used to attack systems within the Intranet
❶ Sends a trapping mail
Attacker
Intranet
❷ Opens it without knowing it is a trap
❸ Induced to a malicious site
Malicious Webpage provided by the attacker
FW
User
※ FW=Firewall

There have been an increasing number of incidents caused by "Passive Attack"[1] - an attack in which users are induced or directed to the phony Website containing false information that is created by an attacker exploiting a vulnerable legitimate Web server.

<Outline of the Problem>

"Passive Attack" is attacks where the attacker induces the user to view a vulnerable Website or a trapping-mail. Examples of passive attack are: "Targeted Attack" and an attack that exploits cross-site scripting Vulnerability or other vulnerabilities in Web browsers (For details, please refer to "[2nd] Increasingly-Sophisticated Targeted Attacks" in "Threats to Organizations").

[1] Passive Attacks: Attacks where the attacker induces or directs the user to perform a specific action.

Cross-site scripting is an attack method that exploits vulnerability in web applications to attack Website users. In this attack, a malicious script is executed on users' browsers when they visited a vulnerable Website, causing damages such as phishing scam or information leakage. There are many Websites whose countermeasures against cross-site scripting are insufficient, and many reports on vulnerable Websites are submitted to IPA.

In a passive attack that exploits vulnerability in browsers, the user's PC might be infected with a computer virus by just accessing a malicious Website.

The characteristic of passive attack is that, it exploits a network available for general use within the organization. This is because there aren't many networks attackers can directly attack. Nowadays, it has become common for enterprises to install firewall. Meanwhile, for software products that were vulnerable to active attacks, source programs were modified to reduce the vulnerabilities that can be exploited for active attacks. This may account for the decrease in active attacks and the increase in passive attacks.

<Progress of the Problem>

Passive attack has been known since a long time ago. Cross-site scripting Vulnerability became widely known to the public through the information provided by CERT/CC and Microsoft in February 2000. Meanwhile, a number of vulnerabilities in Web browser were detected and some of those vulnerabilities were exploited for malicious purposes. At that time, however, only active attacks were emphasized while passive attack was barely grasped. But the threat of passive attack was gradually recognized by the public as "Targeted Attack" appeared and an attack that exploits vulnerability in Web browsers was carried out. Nowadays, passive attack is acknowledged as one of the most serious problems.

<Situation of Countermeasure>

By the end of 2008, the number of reports on cross-site scripting Vulnerability that had been submitted to IPA based on "Early Warning Partnership" had reached 1,024. Of those cases, only 314 cases had been solved by the end of January (such as by applying patches), leaving 710 cases unsolved.

<How to Address This Problem>

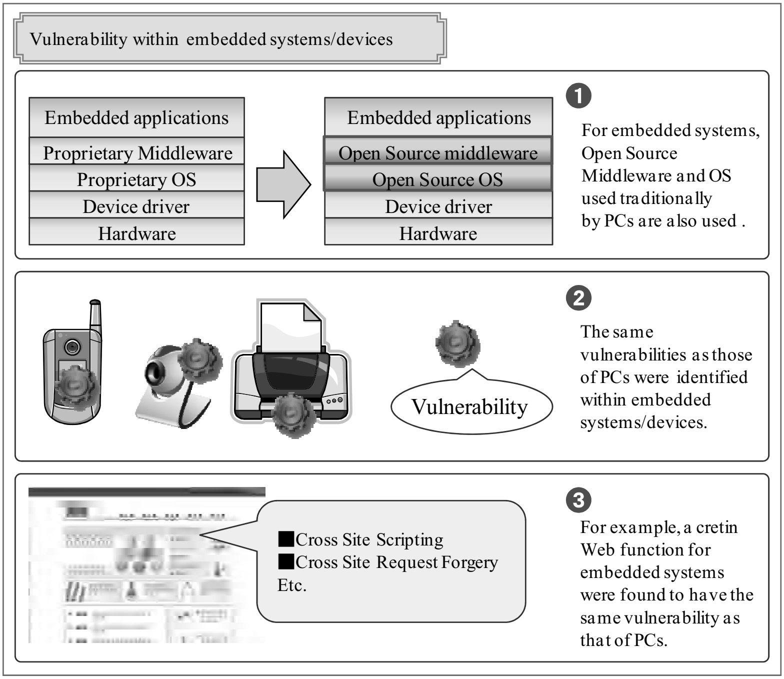
System administrators and web application developers should take note of cross-site scripting Vulnerability and other vulnerabilities that may become the cause of passive attack. This is an issue developers should take care of as users can do nothing about it. Developers should incorporate countermeasures into their systems from the design phase, making sure that no security hole is introduced. They should take necessary steps by referring document such as "How to Secure Your Website", published by IPA.

References

IPA: Reporting Status of vulnerability-related information
http://www.ipa.go.jp/security/english/quarterlyrep_vuln.html

Threats to System Administrators/Developers

【3rd】Potential Vulnerability in Embedded Systems/Devices [9th Overall]



For embedded systems, Open Source Middleware and OS used traditionally by PCs are also used .

The same vulnerabilities as those of PCs were identified within embedded systems/devices.

For example, a cretin Web function for embedded systems were found to have the same vulnerability as that of PCs.

Network environment for embedded systems/devices are improving and an increasing number of embedded systems/devices are using open source operating systems and middleware. This means that, any vulnerability in embedded system/device, as in other systems, could be exploited for an attack.

<Outline of the Problem>

Development of information and communication technology made it easy to add a communication feature to embedded systems/devices, enabling the use of network anywhere at any time.

When exploited, vulnerability in embedded systems/devices could allow attackers to steal information as they would on computers connected to the Internet or to perform operation on those systems/devices in an unauthorized manner. In recent years, we saw an increasing number of embedded systems/devices using open source operating systems and middleware and having the Internet connection capability. For this reason, the same problem arose as that for computers connected to the Internet.

In 2008, vulnerability was detected in popular mobile phones in Japan and security alert was issued on an attack in which silent phone calls are made to IP telephones. Furthermore, JVN (Japan Vulnerability Notes) released information about vulnerabilities in the mobile phones, portable music players and small terminals that were used widely in Japan. Some of Internet-capable embedded-systems/devices have Web Interface functions. These functions might also have Web application vulnerability. Among eight embedded-system-related vulnerabilities reported on JVN in 2008, four cases were related to Web Interface functions. As with web applications, we need to promote security measures for embedded devices' Web interfaces.

<Progress of the Problem>

Up until a few years ago, there had been only a few embedded systems/devices with the Internet connection capability, so for most embedded systems/devices, update feature was unavailable. But now, embedded systems/devices, in particular, those having the Internet connection capability are equipped with update capability, enabling users to update systems to overcome the vulnerability detected.

<How to Address This Problem>

When developing an embedded system/device to be connected to a network, developers should take precaution so as not to create security holes in their systems/devices from the design phase. It's best to provide a mechanism for users to update programs in an easy-and-secure manner should any vulnerability be detected. As with other systems, embedded systems/devices should be developed with information security in mind. Developers should strive to improve Website security by referring to document such as "How to Secure Your Website", published by IPA.

References

IPA: 複数の組込み機器の組み合わせに関するセキュリティ調査報告書
http://www.ipa.go.jp/security/fy19/reports/embedded/ (in Japanese)

IPA: Security Alert for Vulnerability in Multiple YAMAHA Routers
http://www.ipa.go.jp/security/english/vuln/200801_Yamaha_press_en.html

IPA: Security Alert for Vulnerability in Multiple I-O DATA Wireless LAN Routers
http://www.ipa.go.jp/security/english/vuln/200803_iodata_press_en.html

IPA: Security Alert for I-O DATA DEVICE HDL-F Series Vulnerability
http://www.ipa.go.jp/security/english/vuln/200811_iodata_en.html

IPA: Security Alert for Vulnerability in Sony SNC Series Network Camera
http://www.ipa.go.jp/security/english/vuln/200902_sonysnc_en.html

【Appendix A】Relations among 10 Major Security Threats

Appendix Table 1. 10 Major Security Threats

Overall Rankings and Those who Need to Take Measures

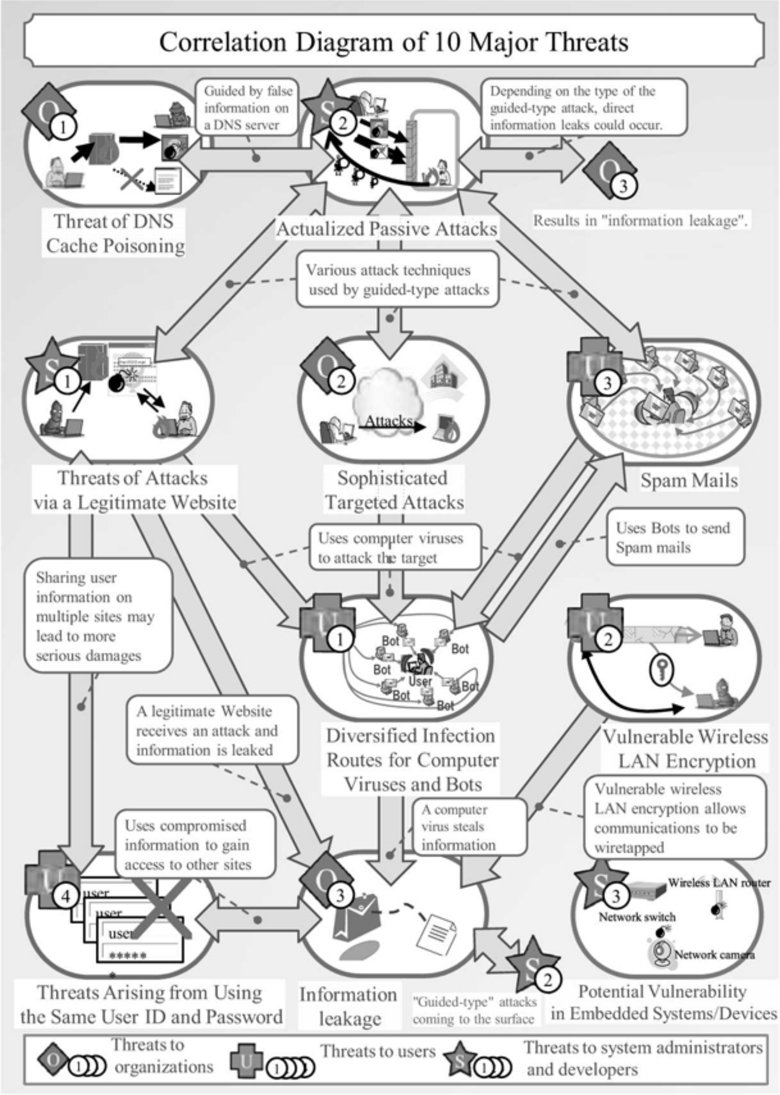
10 Major Security Threats		Those who Need to Take Measures				Ranking [2009]	Previous Ranking [2008]
		Management	Users	System administrators	Developers		
Threats to Organizations							
1st	Threat of DNS Cache Poisoning			◎		1st (Up)	－
2nd	Sophisticated Targeted Attacks	◎		◎		3rd (Up)	4th
3rd	Information Leakage Occurring on a Daily Basis	◎		○		5th	3rd
Threats to Users							
1st	Diversified Infection Routes for Computer Viruses and Bots		◎	○		4th (Up)	6th
2nd	Threats Arising from Vulnerable Wireless LAN Encryption		◎	○	○	6th (Up)	－
3rd	Never Decreasing Spam Mails		◎	○		8th (Up)	9th
4th	Threats Arising from Using the Same User ID and Password	○	◎	○		10th (Up)	－
Threats to System Administrators/Developers							
1st	Threats of Attacks via a Legitimate Website	○		◎	○	2nd	2nd
2nd	Actualized Passive Attacks			○	◎	7th	1st
3rd	Potential Vulnerability in Embedded Systems/Devices				◎	9th (Up)	10th

◎：Those who should take measures　　○：Those who should take measures on an as-needed basis

(Up)：Those ranked higher than the previous year level

Appendix Table 1 shows overall rankings of 10 major security threats and who needs to take measures. Among the new threats ranked in Top 10 in this year are: "Threat of DNS Cache Poisoning" and "Threats Arising from Vulnerable Wireless LAN Encryption." Among the threats ranked higher than the previous year level are: "Diversified Infection Routes for Computer Viruses and Bots" and "Increasingly-Sophisticated Targeted Attacks."

【Appendix B】Correlation Diagram of 10 Major Security Threats


Correlation Diagram of 10 Major Threats
O 1
Guided by false information on a DNS server
S 2
Depending on the type of the guided-type attack, direct information leaks could occur.
O 3
Threat of DNS Cache Poisoning
Actualized Passive Attacks
Results in "information leakage".
Various attack techniques used by guided-type attacks
S 1
O 2
Attacks
U 3
Threats of Attacks via a Legitimate Website
Sophisticated Targeted Attacks
Spam Mails
Uses computer viruses to attack the target
Uses Bots to send Spam mails
Sharing user information on multiple sites may lead to more serious damages
U 1
Bot
Bot
Bot
User
Bot
Bot
Bot
U 2
A legitimate Website receives an attack and information is leaked
Diversified Infection Routes for Computer Viruses and Bots
Vulnerable Wireless LAN Encryption
A computer virus steals information
Vulnerable wireless LAN encryption allows communications to be wiretapped
Uses compromised information to gain access to other sites
U 4
user
user
user
*****
O 3
S 3
Wireless LAN router
Network switch
Network camera
S 2
Threats Arising from Using the Same User ID and Password
Information leakage
"Guided-type" attacks coming to the surface
Potential Vulnerability in Embedded Systems/Devices
O 1 Threats to organizations
U 1 Threats to users
S 1 Threats to system administrators and developers

Appendix Table 2. Relations among 10 Major Security Threats

【Appendix C】References

[For Organizations]

（1）ソーシャル・エンジニアリングを巧みに利用した攻撃の分析と対策, Feb. 2009
http://www.ipa.go.jp/security/vuln/report/newthreat200902.html (in Japanese)

（2）近年の標的型攻撃に関する調査研究－調査報告書－, Mar. 2008
http://www.ipa.go.jp/security/fy19/reports/sequential/ (in Japanese)

（3）知っていますか？脆弱性（ぜいじゃくせい）, Jul. 2007
http://www.ipa.go.jp/security/vuln/vuln_contents/ (in Japanese)

（4）情報漏えい発生時の対応ポイント集, Sep. 2007
http://www.ipa.go.jp/security/awareness/johorouei/ (in Japanese)

[For System Administrators]

（5）安全なウェブサイト運営入門, Jun. 2008
http://www.ipa.go.jp/security/vuln/7incidents/ (in Japanese)

（6）ウェブサイト運営者のための脆弱性対応ガイド, Feb. 2008
http://www.ipa.go.jp/security/fy19/reports/vuln_handling/ (in Japanese)

（7）Vulnerability Information Portal Site JVN
http://jvn.jp/en/

（8）Vulnerability Countermeasure Information Database JVN iPedia
http://jvndb.jvn.jp/en/

（9）Filtered Vulnerability Countermeasure Information Tool MyJVN
http://jvndb.jvn.jp/en/apis/myjvn/

（10）SQL インジェクション検出ツール　iLogScanner, Apr. 2008
http://www.ipa.go.jp/security/vuln/iLogScanner/ (in Japanese)

（11）DNS キャッシュポイズニング対策, Jan. 2009
http://www.ipa.go.jp/security/vuln/DNS_security.html (in Japanese)

[For Developers]

（12）セキュアプログラミング講座
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/ (in Japanese)

（13）How to Secure Your Web Site 3rd Edition Released, Jun. 2008
http://www.ipa.go.jp/security/english/vuln/200806_websecurity_en.html

（14）TCP/IP に係る既知の脆弱性に関する検証ツール, Jan. 2009
http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html (in Japanese)

（15）SIP に係る既知の脆弱性に関する検証ツール, Apr. 2009
http://www.ipa.go.jp/security/vuln/vuln_SIP_Check.html (in Japanese)

（16）Vulnerability Disclosure Guideline for Software Developers Released, Jul. 2007
http://www.ipa.go.jp/security/english/vuln/200807_announce_manual_en.html

（17）自動車と情報家電の組込みシステムのセキュリティに関する調査報告書, Mar. 2009
http://www.ipa.go.jp/security/fy20/reports/embedded/index.html (in Japanese)

【 Appendix D 】 Information Security Overview for FY 2008（10 Topics）

In this section, we outline 10 topics selected from what happened in the field of information security in the fiscal year ending in March 2008.

1. Information leakage in FY 2008:

"File-Sharing Software" was ranked 1st. "Unauthorized Access" was also notable

As the major cause of information leakage, "（anonymous）File Sharing Software" was ranked 1st in FY 2008, in comparison to "Loss/Theft" in FY 2007. As a result, an unreasonable situation arose, in which second-leakers received no punishment, while users who fell victim of information leakage incident by disclosure viruses in their computers were slapped by social sanction (in some cases, legislative measure such as copyright law was enforced). “Second-leakers” intentionally upload the leaked information in a file-sharing network, after the initial information leakage incident has quieted down. Concerned bodies submitted a petition to the government calling for legislation on this issue. The Japanese society is now being asked: " Which is more important, the privacy of the second-leaker's communications or the privacy of the owner of the leaked information?"（Figure 1）

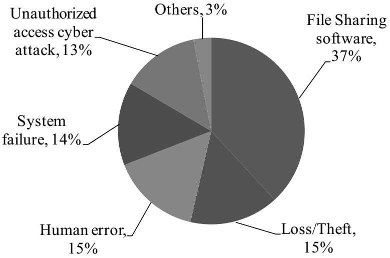
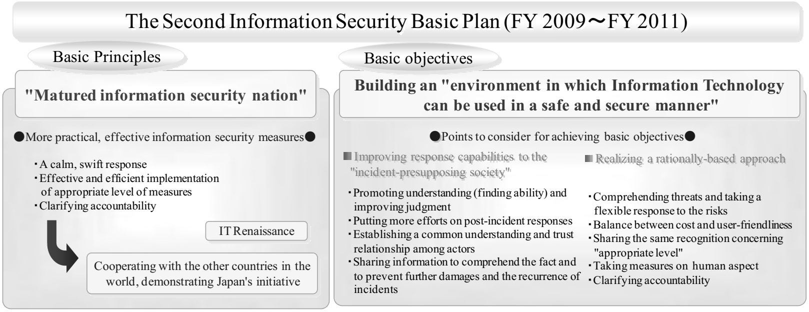


Figure 1. Cause of Information Leakage

2. The Second Stage of Japan's overall plan:

Making a new Information Security Basic Plan



The Second Information Security Basic Plan (FY 2009〜FY 2011)

Basic Principles

"Matured information security nation"

●More practical, effective information security measures●

- A calm, swift response
- Effective and efficient implementation of appropriate level of measures
- Clarifying accountability

IT Renaissance

Cooperating with the other countries in the world, demonstrating Japan's initiative

Basic objectives

Building an "environment in which Information Technology can be used in a safe and secure manner"

●Points to consider for achieving basic objectives●

■ Improving response capabilities to the "incident-presupposing society"

- Promoting understanding (finding ability) and improving judgment
- Putting more efforts on post-incident responses
- Establishing a common understanding and trust relationship among actors
- Sharing information to comprehend the fact and to prevent further damages and the recurrence of incidents

■ Realizing a rationally-based approach

- Comprehending threats and taking a flexible response to the risks
- Balance between cost and user-friendliness
- Sharing the same recognition concerning "appropriate level"
- Taking measures on human aspect
- Clarifying accountability

Figure 2. Basic Principles and Objectives of the Second Information Security Basic Plan

Japan's information security policy has been implemented based on "The First Information Security Basic Plan (Target period: FY 2006 to FY 2008)", but on February 3, 2009, the government formulated "The Second Information Security Basic Plan"(Target period: FY 2009 to FY 2011), as the next stage in the national plan. In addition to "Proactive Defense" and "Protection" addressed in the prior plan, the Second Basic Plan covers issues such as improving response capabilities to the "incident-presupposing society", balancing cost and user-friendliness, and realizing a rationally-based approach (e.g., clarifying accountability.) (Figure 2)

3. Vulnerability in Domain Name Servers: Cache Poisoning has become a topic of global interest

Information on a vulnerability named "Cache Poisoning", along with patch programs to remedy it, was released by experts around the world in July 2008.

DNS is an important server that provides the basis for the use of e-mail and Websites, and JPCERT/CC and relevant organizations in Japan were acting to keep the public informed about vulnerabilities identified. Among the vulnerability reports submitted to IPA in the second half of 2008, "DNS Cache Poisoning" accounted for a large proportion. Even now, no measures have been taken for most DNS Servers, and immediate action is strongly urged. (Figure 3)

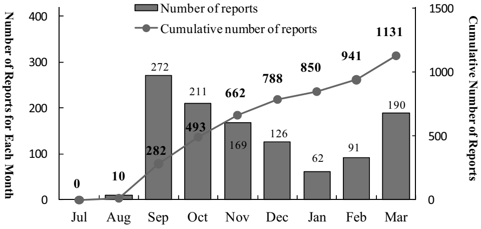


Figure 3. Changes in Number of Reported DNS Cash Poisoning Vulnerability

4. A study on cipher generation transition has started

In February 2009, a guideline was publicly released for soliciting cryptography, which is recommended for the e-Government systems that are expected to adopt new cryptography in 2013. Official public offering is scheduled in the autumn of 2009, following the security evaluation of the new cryptography proposed. The release of the guideline marked the start of new cryptography research by the related community in Japan. New cryptography that can be used worldwide is expected, rather than just adding it to the recommended cryptography list for e-Government.

5. IC Card security issue raised in Europe and the United States: Japan is also building a framework for security evaluations

IC cards are used for transportation cards, credit cards, electronic passports, etc., serving as a foundation for the lives of people around the world. In June 2008, university researchers in the Netherlands demonstrated that the "Oyster Card", which has 17 million issued copies in Europe, can be replicated by a special technique analyzing its electronic circuit, and used illegally in the London Underground. A similar demonstration was done with a pass-permit card used in the Boston subway. In Japan, there is increasing demand for information security measures that are applied for IC Card/Card Reader hardware and their operating systems. For this reason, the "IC Systems Security-Round Table", a private association to build a framework for IC Card security evaluation in Japan, was established in March 2009.

6. U.S. New President Obama's Information security policy: Given the first priority

On January 21, 2009, The Obama Administration announced the outline of a new strategy for cyber security, saying that cyber security is one of the first priorities for his administration. Since he made a campaign speech in the summer of 2008, President Obama has been addressing cyber security as the top priority of his Administration.

The new strategy consists of 6 pillars, including building a cyber infrastructure as the nation's strategic asset and reinforcing the U.S. government's leadership in the field, leading next generation of R&D, protecting IT infrastructure, preventing corporations from cyber-espionage, minimizing crime opportunity gain, protecting personal information and releasing information on incidents concerning information leakage.

Further, the position of "National Cyber Adviser," who reports directly to the President and is responsible for making federal policies regarding cyber security, will be established. (Figure 4)

The Cyber Security Social Contract
Policy Recommendations
for the
Obama Administration
and
111th Congress

INTERNET SECURITY ALLIANCE

A Twenty-First Century Model for Protecting and Defending Critical Technology Systems and Information

Figure 4. One of the Policy Proposals That Became the Basis for the President Obama's Information Security Policy

7. Enterprises' investment in information security: The impact of financial crisis has become visible, particularly in regional towns and cities

As the biggest challenge in implementing information security is "expenditures necessary for information security measures", the IPA’s surveys in many parts of Japan revealed that this tendency has become more prominent, particularly in regional nucleated cities. The next challenge is “expenditure to have staff with specialized expertise." Amid the global financial crisis that is also affecting Japan's economy, small and medium-sized enterprises in Japan are challenged to raise funds. This problem seems to affect enterprises' investment in information security measures.

Many large Japanese corporations had completed major information security-related investment by 2008 and such investment was reduced drastically in 2008, compared to 2007. Further support is required for small and medium-sized enterprises that have limitation on business resources.

8. E-government：
A study on how to improve services moved into high gear

A study on a mechanism which allows multiple administrative services to be completed at one site (e.g., next generation administrative services, social security cards, “electronic post-office box (tentative naming)”, etc.) moved into high gear in April, 2008. During the study session, system architecture is examined, taking into account information security and privacy, such as how to identify and authenticate users (citizens), and how to utilize and control information. It is important to build a social system, which is rational and convenient for people's living and economic activities. For this reason, the construction of common platforms and IDs is gathering momentum.

Private organizations also are making efforts to promote the shared use of IDs on multiple sites. Among them are "Open ID Foundation Japan", which was established in October 2008, and "Liberty Alliance".

9. Amendment of the Unsolicited Commercial E-mail Prevention Law, Opt-In system started in December 2008

In December 2008, the Unsolicited Commercial E-mail Prevention Law was amended to adopt an "Opt-In" system that prohibits sending commercial e-mail unless prior consent is obtained from recipients. Unsolicited commercial e-mail occupies a large portion of Internet bandwidth, slowing down transmission speed. Furthermore, they may allow computer viruses to be embedded in them and/or guide users to malicious websites containing computer viruses. Unsolicited commercial e-mail is often sent from abroad. Outside Japan, under the cooperation of concerned organizations, the network of a malicious ISP hosting the sending of unsolicited commercial e-mail was shut down in August 2008, proving to be an effective measure. Deeper international cooperation will be required in the future.

10. Chinese Standard Expected to Harmonize with International Standard：
Concerns in the China Compulsory Certification system

The Chinese government has implemented the China Compulsory Certification system (CCC) since 2002, for the purpose of maintaining national security and ensuring the safety of products. In January 2008, the government announced that it would add 13 information security products to target products of CCC in May 2009. The Chinese government is purportedly planning to apply an ISO/IEC15408 (Common Criteria)-like standard for CCC. While major countries in the world join the international mutual recognition framework of Common Criteria, CCC is deemed to be a vehicle for China to not accept products certified in other countries, which became major concerns to the international community. For this reason, Japan, the U.S., European countries and South Korea are negotiating with China at WTO and other meetings. Continuous efforts should be made to come to an appropriate settlement.

(*) On April 29, 2009, the Chinese government announced that it would reschedule to May 1, 2010 and confine to products in government procurement. However, on May 4, 2009, the U.S. and Japan rendered a message requesting China to withdraw CCC.

Information Security White Paper 2009 Part 2

10 Major Security Threats

Attacking Techniques Become More and More Sophisticated

[Publication]	Mar. 24, 2009	First Printing
	May 25, 2009	Second Printing
	Jun. 25, 2009	English Translation First Printing

[Editor] Information Security Study Group,
IT Security Center,
Information-technology Promotion Agency, Japan

How to Report Information Security Issues to IPA

Designated by the Ministry of Economy, Trade and Industry, IPA IT Security Center collects information on the discovery of computer viruses and vulnerabilities, and the security incidents of virus infection and unauthorized access.

Make a report via web form or email. For more detail, please visit the web site:
URL: http://www.ipa.go.jp/security/todoke/ (Japanese only)

Computer Viruses

When you discover computer viruses or notice that your PC has been infected by viruses, please report to IPA.

Software Vulnerability and Related Information

When you discover vulnerabilities in client software (ex. OS and browser), server software (ex. web server) and hardware embedded software (ex. printer and IC card) , please report to IPA.

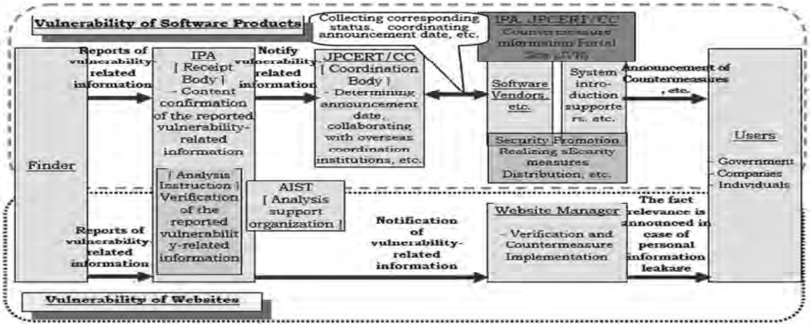
Unauthorized Access

When you detect unauthorized access to your network, such as intranets, LANs, WANs and PC communications, please report to IPA.

Web Application Vulnerability and Related Information

When you discover vulnerabilities in systems that provide their customized services to the public, such as web sites, please report to IPA.

Framework for Handling Vulnerability-Related Information
～ Information Security Early Warning Partnership ～


Vulnerability of Software Products
Collecting corresponding status, coordinating announcement date, etc.
IPA, JPCERT/CC Countermeasure Information Portal Site (JVN)
Reports of vulnerability-related information
IPA [Receipt Body] - Content confirmation of the reported vulnerability-related information
Notify vulnerability-related information
JPCERT/CC [Coordination Body] - Determining announcement date, collaborating with overseas coordination institutions, etc.
Software Vendors, etc.
System intro-duction supporters, etc.
Announcement of Countermeasures, etc.
Security Promotion Realizing sEcurity measures Distribution, etc.
Users
- Government
- Companies
- Individuals
Finder
[Analysis Instruction] Verification of the reported vulnerability-related information
AIST [Analysis support organization]
Reports of vulnerability-related information
Notification of vulnerability-related information
Website Manager
- Verification and Countermeasure Implementation
The fact relevance is announced in case of personal information leakage
Vulnerability of Websites

JPCERT/CC: Japan Computer Emergency Response Team Coordination Center, AIST: National Institute of Advanced Industrial Science and technology

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
2-28-8 Honkomagome, Bunkyo-ku, Tokyo 113-6591 JAPAN
http://www.ipa.go.jp/index-e.html

IT SECRITY CENTER
Tel: +81-3-5978-7527 FAX: +81-3-5978-7518
http://www.ipa.go.jp/security/english/