10 Major Security Threats and Current Status of Japan
Have you already updated?

HIDEAKI KOBAYASHI
IT Security Center
Information-technology Promotion Agency (IPA), Japan
November 5, 2009

Copyright © 2009, IPA all right reserved.
発表内容

・IPA?
・Security Activities in Japan  日本でのセキュリティ活動
・10 Major Security Threats and Case study of Attacks targeting Vulnerabilities 10大脅威と脆弱性を突く攻撃の例
・Countermeasures 対策は
・Continuous Improvement in security 日本のセキュリティレベル向上に向けて
Government Organisation under the Ministry of Economy, Trade and Industry (METI)
Chairman : Mr. Koji Nishigaki

Invigorating Japan through IT

Organisation Structure

IT Security Center (ISEC) <Security>
Software Engineering Center (SEC) <Reliability>
Open Software Center (OSC)
IT Human Resources Development HQ
   IT Skill Standards Center (ITSSC)
Japan IT Engineer Examination Center (JITEC)
The IT Security Center (ISEC) is the core and leading unit for promoting Japanese IT security countermeasures, including diffusing and enlightening security awareness to the Japanese citizens, providing alert information on latest security vulnerabilities and publishing security guidelines for enterprises and personal computer users.
発表内容

• IPA？
• Security Activities in Japan  日本でのセキュリティ活動
• 10 Major Security Threats and Case study of Attacks targeting Vulnerabilities 10大脅威と脆弱性を突く攻撃の例
• Countermeasures 対策は
• Continuous Improvement in security 日本のセキュリティレベル向上に向けて
Security Countermeasures in Japan is perfect? How to continue this status?
日本のセキュリティへの対応は十分か？今後も維持するためには。

Distribution Map of the Number of PCs Infected by Malware per 1000 PCs
2008年下半期の国/地域ごとの感染率

Computers Cleaned per Mil (CCM) と呼ばれる測定基準を使用して表しています。
MSRT（Malicious Software Removal Tool: 悪意のあるソフトウェアの削除ツール）

国内BOT感染率は
感染率は最低レベル

出典: マイクロソフト セキュリティ インテリジェンス レポート
（最終更新日: 2009年4月9日）

Copyright © 2009, IPA all right reserved.
Activity 1: Cyber Clean Center
Cooperation with public and private

Cyber Clean Center

- succeeded in reducing the number of computers infected by botnet malware to 1 percent in June 2008, from 2.5 percent in April 2005

- contributed to improving the detection rate of malware on users’ computers by providing security vendors with samples collected by honey pots

2006. 12.12 Open
2006年12月12日開設

Copyright © 2009, IPA all right reserved.

https://www.ccc.go.jp/
https://www.ccc.go.jp/en_index.html
Main activities
主な活動内容

- Alert promotion with ISP
ISPと連携した注意喚起活動

- CCC Cleaner supply
ボットの駆除ツール提供

- Information for preventing infection
感染防止のための対策情報提供

For your safety net life
BOT is a type of computer malware and a program that is frequently uploaded with malicious intent to control your computer externally. Any computer could be infected by BOT once connected to the Internet. This site is to provide you information on how to clean BOT as well as how to protect your computer from BOT.

Information
Activity Report 2006-07
Fiscal Year 2006 Activity Report on Cyber Clean Center 2007/05/25
This is the FY 2006 activity report on "anti-bots measures project," jointly conducted by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry. NETS since March 2006, the government has been targeting infected computers and infected POS in Japan through collaborative efforts by public and private sectors.

What is BOT?
What is Cyber Clean Center?
Procedure of BOT cleaning
Some hints to prevent BOT infection
FAQ
Links

Click here to see Bot-infection Check procedures.

Copyright © 2009, IPA all right reserved.
Critical Information Infrastructures Protection (CIIP) in Japan

Activities 2: National Strategy on Information Security

The First National Strategy on Information Security
- Aiming to make Japan an Information Security Advanced Nation through Establishment of a New Public-Private Partnership Model – First Step toward a Trustworthy Society -

The Second National Strategy on Information Security
- Aiming for Strong "Individual" and "Society" in IT Age – "Accident Assumed Society"

NISC: National Information Security Center

10 sectors are identified:
- "Telecommunications",
- "Finance",
- "Civil aviation",
- "Railways",
- "Electricity",
- "Gas",
- "Governmental/ Administrative services (including local governments)",
- "Medical services",
- "Water works" and
- "Logistics"

Preparedness and enhancement of security measures against the incidents.

Preparedness and enhancement of security measures against the incidents.

NISC has been established since April 25, 2005 in the Cabinet Secretariat.

Copyright © 2009, IPA all right reserved.
Information Sharing / Analysis Framework among CEPTOAR, NISC and IPA, etc.

Cabinet Secretariat
National Information Security Center (NISC)

Incident response relevant agencies
Central government agencies concerning information security

Related organizations

CEPTOAR-Council

Information Sharing/Analysis function (CEPTOAR)
Information Sharing/Analysis function (CEPTOAR)

Information for IT-malfunctions

Ministries and Agencies of the relevant critical infrastructure

Analysis of Interdependency

Early-warning Information, etc.
Various related information Recovery method information, etc.
Various related information Recovery method information, etc.

Various related information Recovery method information, etc.

Note: This diagram shows the future flow of information required for service maintenance or recovery of critical infrastructures, which is based on an appropriate system of providing for/sharing with business entities engaged in critical infrastructures. The arrow (→) basically indicates a range not covered in this diagram. However, it is shown for reference, to clarify meaning of other arrows.
Activity 3: Protect IT Systems from Vulnerability

Vulnerability Information Handling Framework

“Information Security Early Warning Partnership” (From July 8, 2004)

Security researchers, engineers, etc.
Total number of reports exceeded 5,800 in about 5 years (3Q2004–3Q2009)
- Software Product 994, Website 4,832
- Increased about 3,000 in a recent year (4Q2008 – 3Q2009)
- On average, 4.56 reports a day
JVN（Japan Vulnerability Notes） & JVN iPedia
IPAとJPCERT/ CCの共同運営

http://jvndb.jvn.jp/en

Copyright © 2009, IPA all right reserved.
Vulnerability Countermeasure Information Portal Site and Database (Continued)

- **JVN (Vulnerability Handling Coordination DB)**
  Providing vulnerability countermeasure information and Japanese vendor status for reported vulnerabilities by “Information Security Early Warning Partnership”

- **JVN iPedia (Vulnerability Archiving DB)**
  Providing countermeasure information database for covering overall vulnerabilities

- **MyJVN**
  Providing vulnerability countermeasure information via machine readable interface such as Web APIs and Version Checker.

**CVE Compatible**
IPA’s Security Guidelines and Mitigation/Prevention Tools for Vulnerability countermeasures

1. How to Secure Your Web Site

2. Secure Programming

3. 10 Major Security Threats

4. Secure Critical Infrastructure
   - Information Security Forum
     - Check tool for attack-evidence of SQL Injection, XSS, ...
     - (Japanese only)

5. iLogScanner
   - Report and Inspection tester for known Vulnerabilities of TCP/IP
   - (Japanese only)

6. Vulnerability Countermeasure Information Portal Site and Database
   - MyJVN - Version Checker
     - Improvement of the keeping up-to-date environment
   - Copyright © 2009, IPA all right reserved.

Note: All links are in English, except for the last two, which are in Japanese.

Copyright © 2009, IPA all right reserved.
Analyzing Tool sets for Malware targeting Vulnerabilities

脆弱性を突くマルウエア解析ツール

脆弱性を突くマルウエアは、ますます複雑・巧妙になってきている。対策のための分析を困難にしている。このためマルウエア解析ツールを開発した。

Analyzing Tool sets

- Core Engine
  - Instruction Tracer
  - Disassembler
  - PE Builder
- Shellcode Extractor
- Anti-Obsfuscation
  - Section Packing
  - Data Packing
  - Shellcode Decoder
- Code Injection Tracer
  - User-mode injection tracer
  - Kernel-mode injection tracer
- API Tracer
  - API call tracing
  - Handle tracing
  - Memory tracing
- API Name Resolver
- IAT Rebuilder
- undo & Back trace
- Report Engine
  - XML report generator
  - HTML forms
- Malware Server Emulator
- Per-process Packet monitor

Copyright © 2009, IPA all right reserved.
発表内容

• IPA？
• Security Activities in Japan 日本でのセキュリティ活動
• 10 Major Security Threats and Case study of Attacks targeting Vulnerabilities 10大脅威と脆弱性を突く攻撃の例
• Countermeasures 対策は
• Continuous Improvement in security 日本のセキュリティレベル向上に向けて
10 Major Security Threats
Trend of Information Security Threats in Japan

Outline of the Problem

Major case of the 2008 virus infection is “Virus-infection via PDF, Flash or Microsoft Office files (such as Word, Excel or Powerpoint) that are in electronic document file format”.

- Threats to Organizations
  - [1st] Threat of DNS Cache Poisoning
  - [2nd] Sophisticated Targeted Attacks
  - [3rd] Information Leakage Occurring on a Daily Basis

- Threats to Users
  - [1st] Diversified Infection Routes for Computer Viruses and Bots
  - [2nd] Threats Arising from Vulnerable Wireless LAN Encryption
  - [3rd] Never Decreasing Spam Mails
  - [4th] Threats Arising from Using the Same User ID and Password

- Threats to System Administrators/Developers
  - [1st] Threats of Attacks via a Legitimate Website
  - [2nd] Actualized Passive Attacks
  - [3rd] Potential Vulnerability in Embedded Systems/Devices
Targeted Attack is an attack whose target is limited to a specific organization or person. In 2008, a sophisticated attack method appeared that distributes a computer virus through the exploitation of vulnerability in software products, such as by using "Social Engineering - a technique to illicitly obtain people's personal information by exploiting an off-guard state in their mind and behavior."
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.

PDFやMSオフィスのファイルの脆弱性が狙われる

Copyright © 2009, IPA all right reserved.
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.

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

There is an increasing number of vulnerabilities in PDF and MS Office files that are being exploited.
Increase of vulnerability for Application software

Increase annually for application software
desktop applications such as Internet Explorer, Firefox, Microsoft Office,
middleware products such as web servers, application servers, databases,
development/management platforms such as PHP, Java, and GNU libraries.

Each year, many new applications are developed and, since they are accompanied by new vulnerabilities, improving security measures concerning application software should be of especially high priority.

Copyright © 2009, IPA all right reserved.
発表内容

・IPA？
・Security Activities in Japan
・10 Major Security Threats and Case study of Attacks targeting Vulnerabilities
・Countermeasures
・Continuous Improvement in security
How to Address This Problem

For these threats, we can apply traditional measures such as keeping up-to-date operating systems, applications, plug-ins (such as ActiveX) and virus definition files of antivirus software.

It's simple solution, but it's difficult to keep the latest environment.

Keeping up-to-date operating systems: Easy ... Microsoft Update
applications: Poor ... Each products provide individual method
plug-ins (such as ActiveX) : Poor ... Each products provide individual method

Our motivation ... 最新の環境を保つ方法の改善が目標
Improvement of the keeping up-to-date environment.
Improvement of the keeping up-to-date environment

Splitting the keeping up-to-date steps into two phase.

- Step 1: Check phase
  Is your PC keeping the latest version?

- Step 2: Remedy phase
  Let's update the applications and the plug-ins on your PC.

MyJVN - Version Checker supports the check phase.

Simple and easy operation.

Copyright © 2009, IPA all right reserved.
Simple and easy operation

Step 1: Check phase - 2 clicks

Click the Select ALL and the Start buttons.

(1) Click the Select ALL button. 「すべてを選択」ボタンを押す
Simple and easy operation

- **Step 1: Check phase - 2 clicks**
  - Click the Select ALL and the Start buttons.
  - (2) Click the Start button.

Keeping the latest version or not

「最新のバージョンです」、「最新のバージョンではありません」、「インストールされていません」の3つのチェック結果が得られます。最新のバージョンでない製品のアップデートが促されます。
Simple and easy operation

- **Step 2: Remedy phase - 2 clicks**  
  Navigation to the application update Website

  アプリケーションアップデートのウェブサイトへ誘導

(1) Click the details  
(1) チェック結果詳細の「表示」をクリックすると

(2) Jump to the application update Web site  
(2) アプリケーションアップデートのウェブサイトへジャンプの2クリック
Keep the latest version on your PC
MyJVN - Version Checker

Microsoft Update (Windows Update)

マイクロソフトの製品は、マイクロソフトアップデートを使用してアップデートできます。パッチの自動更新もできます。

しかし、マイクロソフト以外のベンダの製品の対策は、ばらばらの状況。
JRE, pdf, 解凍ソフト等のアップデートを単純・簡単化し機械化するのがMyJVNバージョンチェッカです。

Update JRE, pdf etc.

MyJVN - Version Checker

We need to develop Standards
各種の標準化が必要
発表内容

- IPA ?
- Security Activities in Japan 日本でのセキュリティ活動
- 10 Major Security Threats and Case study of Attacks targeting Vulnerabilities 10大脅威と脆弱性を突く攻撃の例
- Countermeasures 対策は
- Continuous Improvement in security 日本のセキュリティレベル向上に向けて
日本のセキュリティへの対応は十分か？今後も維持するためには。

Distribution Map of the Number of PCs Infected by Malware per 1000 PCs
2008年下半期の国/地域ごとの感染率

今後も維持するためには。
How to continue this status?
Embedded systems and Control systems

Information systems

Control systems

Internet

E-marketplace, Social system, etc.

At home

Internet of Things

Internet of Energy

Today's systems and control systems

今後も維持するためには？
組み込みシステムと制御システムのセキュリティ対策は？

Copyright © 2009, IPA all right reserved.
Around the year 2005, vulnerabilities have slowly proceeded to become published concerning embedded software products in intelligent home appliances such as network devices, mobile phones, and DVD recorders.

2005年以降、家庭内のネットワーク機器（ルータ・スイッチ）、携帯電話、DVDレコーダ等の情報家電に組み込まれるソフト製品の脆弱性が少しずつ増加してきている。

the type of products registered to JVN iPedia
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.
To Know the Current Level of your Organization: you can compare your organization’s “approach for IT security” with the 4 security levels defined in this approach and check for the current level of your organization.

Set your Sight on a Higher Security Level: you may set your sight on a higher security level than you are at now. The higher the level, the more proactively the organization is addressing IT security.

More Secure Products: As the organization’s IT security level increase, so does the security level of embedded systems developed by the organization, which would result in more secure products.
Thank You!

IT Security Center
Information-technology Promotion Agency, Japan
http://www.ipa.go.jp/index-e.html

2-28-8 Honkomagome
Bunkyo, Tokyo 113-6591, Japan
Tel: +81-3-5878-7501
Fax: +81-3-5978-7510