Guide for <Avoidance of Risks> When You Use the Internet

Malicious Intent lurking in the Internet
Do not fall for such deception!!

IPA 独立行政法人情報処理推進機構
セキュリティセンター

http://www.ipa.go.jp/security/

June 8, 2012 4th Edition
1. Malicious Intent on the Internet

2. Trend of Malicious Intent

3. Changes in Attackers

4. Malicious Intent via E-mail and Instant Messaging Service
   (1) An E-mail Carrying a Virus
   (2) A Spam E-mail or Message for Unwanted Advertisements and Inducement
   (3) An E-mail or Message that Lures Recipients to a Website that Causes the Downloading of a Malicious Program
   (4) An E-mail or Message whose Purpose is to Carry Out Phishing
   (5) A Demagogic E-mail or Message that Makes Recipients Feel Uneasy

5. Malicious Intent via a Website
   (1) By Visiting a Tampered Website ...
   (2) A Website that Deceives Visitors
   (3) SEO Poisoning
   (4) A Website having Vulnerabilities

6. Countermeasures Currently Taken by Users

7. Glossary

8. Reference Information
1. Malicious Intent on the Internet

Using the Internet, we can do various things. However, there is a variety of malicious intent on the Internet. Malicious intent that general users encounter includes e-mail-based one (e.g., virus e-mail\(^1\), spam e-mail\(^2\)), acts to defraud people (e.g., phishing\(^3\)); a Website with malicious intent that is prepared to embed a malicious program; and viruses that carry out infection activities or attacks via a network (e.g., bot\(^4\), worm\(^5\)). It is hard to enumerate all here.

Therefore, we summarize acts with malicious intent for general users.

2. Trend of Malicious Intent

A decade ago, malicious intent on the Internet was mainly obstructive behavior by a computer virus against users. However, recent malicious intent is for the purpose of defrauding people of money. So, the majority of such acts are undertaken in a way that users do not notice them.

As for viruses, the occurrence frequency of subspecies is on the increase and some have the nature of regionality (i.e., infection to a limited extent) and in some situations, even antivirus software\(^6\) fails to detect them.

Furthermore, acts with malicious intent tend to be compounded and antivirus software alone cannot provide sufficient security measures.
3. Changes in Attackers

People called "script kitty" who were unable to become a cracker due to their skill shortage have been in existence since olden days. Those people create malicious programs or carry out unauthorized computer access by using information released by crackers or security researchers. They would engage in such dishonest acts out of curiosity or to play tricks.

However, recently, an environment is available in which even people with little knowledge and skill can create a sophisticated virus by using programs called virus creation tool or root-kit. In stead of pursuing technologies, an increasing number of wicked people are making use of existing viruses. In short, wicked people in the real world have been making their way into the Internet.

Consequently, attackers' objectives have shifted from self-display to defrauding the victim of money.

In the underground community of the Internet, virus creation tool and root-kit are organically created, and unreleased vulnerability information and environments for carrying out dishonest acts (e.g., managed bot network) are trafficked.

Without your noticing, your money could be taken away!?

De-visualization of viruses is in progress
4. Malicious Intent via E-mail and Instant Messaging Service

Typical examples of malicious intent via e-mail or Instant Messaging (IM) service\(^\text{10}\) are as follows:

* An e-mail carrying a virus
* A Spam E-mail or Message for Unwanted Advertisements and Inducement
* An E-mail or Message that Lures Recipients to a Website that Causes the Downloading of a Malicious Program
* An E-mail or Message whose Purpose is to Carry Out Phishing
* A Demagogic E-mail or Message that Makes Recipients Feel Uneasy

(1) An E-mail Carrying a Virus

An e-mail carrying a virus is generally sent to unspecified number of users. A virus itself may be sent as an e-mail attachment and there is also a virus e-mail that exploits vulnerabilities in mailer\(^\text{11}\) that handles e-mails.

For example, such e-mail attempts to make you open it, saying:
- This is a photo of myself;
- This is a patch for your OS;
- This is a present;
- This is important notice;
- This is secret information;
- This is leaked information;

To counter virus e-mails like these, it is effective to use antivirus software or a virus check service provided by your Internet service provider.

But you should not place too much trust in these software/services. These are mainly signature\(^\text{12}\)-based countermeasures, which are effective only against known viruses and may not work for the latest viruses.

As effective countermeasures:
Use your antivirus software with the following in mind:
- Keep its virus definition files\(^\text{13}\) up-to-date;
- Perform virus scan regularly;
In addition,
- Eliminate vulnerabilities in your mailer and operating system;
- Use the e-mail filtering service*14 provided by your e-mail server;
Lastly, as the most important countermeasures,
- Do not easily open an e-mail or an attachment from a stranger;
- Do not open an e-mail that appears to be damaged;
- Be careful with an e-mail disguising as an unknown receiver error mail.

(2) A Spam E-mail or Message for Unwanted Advertisements and Inducement

Spam e-mails or spam messages from Internet Messaging (IM) that are sent for unwanted advertisements and inducement may increase rapidly for various reasons. Some people have never received such e-mail or message, and others received them all of a sudden. There are also people who have already received a pile of them. A possible cause for receiving a pile of such e-mails or messages is that, the victims' e-mail address or registered designation for IM has been disclosed on the Internet.

As for these e-mails and messages, just opening or reading them would not cause any particular problem, but if the recipient fell victim to their allurement, he or she might get caught in the crossfire. So care should be taken. In particular, money-making or dating service-related talk may involve you in cybercrimes. For more details, please visit the website below.

- Cybercrime Countermeasures by National Police Agency
(3) An E-mail or Message that Lures Recipients to a Website that Causes the Downloading of a Malicious Program

You should be careful with a link (URL) in an e-mail/IM message that lures the recipient to a sexually explicit site (including dating site), or in an e-mail/message that introduces how to make money.

Majority of one-click billing fraud sites (described later) are using this technique and if you fall victim, you may suffer from an unreasonable billing statement being displayed, spyware\textsuperscript{*15} downloaded, or even your personal information stolen.

Effective countermeasures are:
\begin{itemize}
  \item Do not easily open an e-mail or an attachment file from a stranger;
  \item Be careful with honeyed words;
  \item Set your web browser’s security level to as high as possible;
  \item Pay attention to warning messages issued by the operating system on your PC.
\end{itemize}
(4) An E-mail or Message whose Purpose is to Carry Out Phishing

We need to watch out for an e-mail disguising as a bank or a credit loan company that lures the recipient to a phishing site, or an e-mail /message that lures the recipient to a phony Internet shopping site or a prize-wining site.

By clicking a link (URL) in such e-mail/message, the recipient may be redirected to a phony site (e.g., phishing site). If the recipient easily trusts in such e-mail/message or the contents of the linked website, he may have his personal information stolen.

Personal information that was stolen might be abused to withdraw the victim's money from his bank account or to bill him for a commercial product he hadn't received. This is the case caused by so called "spoofing".

Recommended countermeasures are:

- Do not easily trust in an e-mail from a bank or a credit loan company;
- Without relying on the link, make direct contact with the bank or the credit loan company or visit their website for verification;
- Check for the address of the web page that the link represents;
- Make sure that cryptographic communication (SSL)*16 is adopted in the entry screen for personal information.

[Method of confirmation] For financial institutions' Websites where personal information and other critical information is input, communication is encrypted by using SSL in general.

If the user is connected with that Website by SSL, "https://" is displayed in the address field and a locked-key is displayed on the web browser, so check it.

Thay say, it is difficult for even experts to see through a phishing site. An increasing number of latest web browsers have a built-in anti-phishing feature. Use of such latest web browsers is also effective but the best way is, to implement the second countermeasure in the above list. In short, it is important to verify the authenticity of information by yourself.
Furthermore, in addition to the leak of personal information by a phishing site, use of an easy-to-guess user ID/password, or the entry of personal information at a Net cafe where unspecified number of people may visit might also allow for spoofing by wicked people. So care should be taken.

The figure below shows a phishing e-mail disguising as VISA and detected in November 2004.

1. A spoofed e-mail whose sender is update@visa.co.jp
2. The link in the text (i.e., https://www.visa.co.jp/verified/) looks like the legitimate URL of VISA, but in the HTTP source code, the link represents http://xxx.196.163.74/verified/. If the recipient clicks it, he is redirected to a phishing site where he is prompted to enter his card number and ID number.
(5) A Demagogic E-mail or Message that Makes Recipients Feel Uneasy

There is a case where phony information is sent by e-mail or as a pop-up message in order to make the recipients feel uneasy.

One example is: phony information about the spread of a virus (i.e., virus demagogic e-mail) is sent to users; and users who follow its instruction and delete a specified file suffer from the deletion of an actually legitimate file.

Recently, there was a case where a virus e-mail whose subject could draw people's attention (e.g., "the war has broken out" or "the President of the United States has died") was sent to people in an attempt to make them open its attachment. An e-mail that is used for so called one-click billing fraud is also considered a type of demagogic e-mail.

The figure below shows a virus demagogic e-mail, although it is a bit old example.
Should you receive this type of e-mail, don't panic! The e-mail says, "The file 'jdbgmgr.exe' is a virus, so delete it," but this file name refers to the name of Microsoft's legitimate Java debug program and it is not necessarily the virus-infected file. If no virus is detected by your antivirus software, do not delete this.

Countermeasures include:

- If you sense anything odd, in order to verify its authenticity by yourself, perform Internet search with the keyword contained in that e-mail ("jdbgmgr.exe" in the above example);
- "Please forward it to other people" is a risky keyword. To avoid causing a chain mail, do not forward such e-mail to other people;
- As for the possibility of virus infection, perform virus scan by using your antivirus software;
- If you have no antivirus software, perform a free online virus scan provided by any one of antivirus vendors.

Information about demagogic e-mails is also available on the Websites below. So use them as a reference.

- Information about a Demagogic E-mail about VirusHoaxes (Fake Virus)  
  [http://www.ipa.go.jp/security/topics/virus_hoax.html](http://www.ipa.go.jp/security/topics/virus_hoax.html)  
  (in Japanese)

- Information about a Demagogic E-mail Related to "jdbgmgr.exe"  
  (in Japanese)

- Information about virus hoax (Trendmicro)  
  [https://imperia.trendmicro-europe.com/jp/threat/threats-knowledge/non-virus/](https://imperia.trendmicro-europe.com/jp/threat/threats-knowledge/non-virus/)  
  (in Japanese)
5. Malicious Attack via a Website

(1) By Visiting a Tampered Website …

From the latter half of 2007, the number of Websites tampered through unauthorized access has rapidly been increasing. Appearances of these Websites were unchanged, but due to the malicious code being embedded in a part that is out of sight, visitors could be redirected to a malicious Website and consequently, a malicious program (e.g., a virus) installed on their PC.

[Example of How a Tampered Website causes damages to a User]

Launches an attack against a Website having a certain vulnerability

Tampers a Web page within the site by adding the following imperative statement

For example …

A legitimate Website

Tampers a Web page within the site by adding the following imperative statement

An imperative statement to have the PC access the Web page "*****.htm" in the site "*****.com".

(iii) If the user accesses the tampered Website

While a legitimate Website's page is displayed, the user is redirected to the malicious Website's page (However, the malicious Website's page is crafted so that it cannot be seen).

The Web page in which a virus that exploits the vulnerability is embedded (i.e., *****.htm)

The malicious Website (http://*****.com)

Then, the PC is infected with the virus!!
Until now, when browsing websites, people are encouraged to set their web browser's security settings to a higher level and to ensure secure site access by distinguishing between unreliable sites and reliable ones. But nowadays, even a site which used to be thought reliable could be dangerous.

For example, Microsoft's Internet Explorer allows users to make individual security settings for the Internet, Intranet, reliable sites and restricted sites, based on the concept of security zone*17.

Precondition for settings like this to be effective is that, reliable sites "should not allow for tampering"; however, a problem might occur behind the user’s back, which is considered a threat posed by recent Websites.

This is a downright uncomfortable situation. Under this situation, there are two countermeasures that general users can take:

- Eliminate vulnerabilities in the operating system and applications on your PC (Bring them up-to-date)
  - When your PC’s operating system is Windows PC, perform Windows Update or Microsoft Update;
  - Bring your web browser up-to-date (Furthermore, check the update status)

- Strengthen the security settings of the web browser that you use for Web reference
  - Select one of the latest web browsers with enhanced security settings;
  - Deactivate ActiveX and JavaScript.

As a matter of course, even for aforementioned reliable sites, it is recommended that you use a security-enhanced web browser to access them. Although the use of various useful functions and information might be hindered …
If the users are personnel within a company (organization), the company (organization) can place a proxy server in the gateway between its Intranet and the Internet, so that it can negate a malicious code that is embedded in a tampered Website (esp., a code to redirect site visitors to a malicious Website), such as by requiring users to have access authority to access non-registered Websites. Recently, a Web (URL) filtering service in which information on acknowledged malicious Websites is shared and such sites are filtered out is also provided.

For general users, it would be difficult to build the above-mentioned system. So alternatively, they can use integrated security software provided by some security vendors or a security-enhanced web browser to filter out acknowledged malicious Websites.

Currently, from the security aspect, it is the best to use the web browser Firefox plus the add-on NoScript and to set NoScript options to prohibit <IFRAME>.

Note, however, that some Websites can only be displayed (and function) correctly by Microsoft IE. You may opt to install multiple web browsers and use appropriate one for a specific Website, or to use an add-on for the combined use of Firefox and IE engine.

In either case, users need to determine whether the site they visit is safe or not (e.g., whether it allows for scripts or not).

For the administrators of the Websites that transmit information to general users, it is expected that they will eliminate vulnerabilities in their Website and ensure secure operation so as not to allow this type of problem to occur and their Website to be tampered.

(2) A Website that Deceives Visitors

Apart from the Websites tampered through unauthorized access, there are other types of malicious Websites. For example, there are one-click billing fraud (unfair billings) site, fishing site, a site that provides fake security software, an annoying blog site that intrigues users and rope users into a malicious site, the one that charges a hefty usage fee, or steals personal information, or hits on useless software, etc. Malicious Websites come and go, and have been deceiving computer users by using similar methods.
(a) One-Click Billing Fraud (Unfair Billings) Site

- Hazardous Sites Include, But are Not Limited to Sexually Explicit Sites -

One-click billing fraud (unfair billings) cases occur mainly on sexually explicit sites. Clicking the "Display image" button etc. on a Website results in the display of an unfair billing statement in stead of an image: Such case is not rare and there is also an instance in which a virus called one-click ware\(^\text{20}\) is installed and an unfair billing statement begin to appear ceaselessly on a person's PC.

But in fact, a similar technique is used also in Websites other than sexually explicit sites. The (investment-related) site in the above instance claims that it provides profitable stocks information and urges visitors to apply for membership. If the item "Click here for membership registration" is clicked, a malicious program such as virus is downloaded.

To avoid falling victim, take care not to access unreliable sites and should you access such sites, avoid careless downloading. If the security alert screen is displayed by Windows (as shown in the above instance), never click "Run"; click "Cancel" instead to avoid proceeding further.

---

\(^{20}\) one-click ware: A type of software that, when clicked, automatically downloads and installs malicious programs onto a user's computer without the user's consent or awareness.

---
For more detail on one-click billing fraud (unfair billings), visit the Website below.
- To avoid suffering from unfair billing

(b) Phishing Site

A phony e-mail containing attractive messages such as "speedy examination for quickie loan up to three million yen" and urging recipients to access the URL in its body text; then, the recipients who click on the link are redirected to a phony page and prompted to enter their personal information such as address and name.

[Example of Phishing Site: March 2007]

The site, to which the user was redirected by the phishing e-mail, was designed to trick the user into entering his personal information etc. The information entered here was to be leaked to the operator of that phishing site.

If such personal information is leaked to such malicious entity, further phishing attacks might be carried out based on that information.

Apart from the instances we have introduced, malicious entities may provide a phishing site that resembles a variety of Internet services (e.g., banks, ISPs) in an attempt to get site visitors to enter their user ID and password. If a legitimate user's user ID and password are stolen, his password and contract detail may be changed by the malicious entity, which may lead to an irrevocable consequence.

Nowadays, if you replace your web browser for Internet connection with the latest one, that browser may be equipped with a function to see through phishing sites to some extent and issue alerts. But basically, it is important to be cautious about an e-mail that contains alluring words and not to easily click any link in that e-mail.
For more detail on one-click billing fraud (unfair billings), visit the Website below.

- **Anti-Phishing Measures**
- **AntiPhishingJapan (Council for Anti-Phishing Measures)**

(c) **Website that Provides Fake Security Software**

There is a case where while a person is using the Internet, all of a sudden, a message box appears, saying "**A virus has been detected in your PC**" or "**An error has occurred in your PC**", and he is recommended to buy the "security software" displayed on the screen to solve those problems. In reality, in most cases, such messages are fake and even though there is no problem, it makes the user believe that there is a problem and attempts to have him pay for the security software. Even if he pays for it, as there is no problem from the beginning, nothing is solved.

In some cases, the installed software may be a virus and various types of malicious traps may be embedded in that PC.

Recently, some people call this type of software "scareware (threatening software)" and we can say that this is the same problem as one-click billing fraud.
fraud (unfair billings), as both of them threaten computer users without any ground and extort money.

(d) An annoying blog site or an annoying blog comment/track back

We see an annoying blog site that attempts to have visitors click a link to a malicious Website by providing attractive information for them, or an act of posting an annoying comment or an annoying track back on a general blog site so that readers who are interested in it would be redirected to a malicious Website.

Unlike unwanted e-mails (spam e-mails), they are not active, but we need to watch out for a malicious intent that sets the hook and waits for a prey.

It’s very difficult to determine whether certain piece of information is ill-willed one or not. So, be sure to implement countermeasures for users that are described in (1).

(3) SEO Poisoning

SEO (Search Engine Optimization) is, an act of: making a malicious site appear on the top of a search result by exploiting the search engine optimization feature of that search engine. A case in which search engines such as Google and Yahoo were used to manipulate a search result with a popular keyword and users were lured into a malicious site: Such case was reported in large numbers to some search engine providers.

Some users easily trust in the information that appears on the top of a search result by a search engine, but there is no guarantee that sites appearing in a search result are reliable.

In the worst case, a Website that causes the downloading of a computer virus called "spyware" or "bot" may be displayed on the top, so it is recommended to strengthen the security settings of your web browser and to use a variety of security software. Furthermore, vulnerabilities in users’ PC might be exploited, so be sure to perform security update on your PC.
There are a number of Websites that have a cross-site scripting vulnerability, which is a threat to computer users. This vulnerability is often found in bulletin board sites where many people post information, Websites that require membership registration, and shopping sites, etc.

If a malicious attacker successfully guided computer users to a malicious Website by using phishing or other techniques, had users enter information in the input regions that resemble those on a vulnerable Website, embedded a malicious script in the input information, and lured the users into another vulnerable Website, the attacker would be able to execute the malicious script on the user's web browser.

In the worst case, his browser might be taken over completely, false information displayed, personal information leaked, sessions hijacked, or malicious code downloaded. Unlike the tampered Website shown in (1), these become a very dangerous (uncontrolled) existence when even the administrator of that Website is unaware of. To prevent the occurrence of problems like these, Website administrators are expected to understand their Website vulnerabilities and strive for eliminating such problems and ensuring secure operation.

[Cross-Site Scripting (XSS) – Extracted from "How to Secure Your Web Site"]
6. Countermeasures Currently Taken by Users

Some of recent web browsers have a function to issue alerts, prior to displaying any malicious sites, about the execution of any script that could put users at a disadvantage or the display of such malicious sites. With this function, users are alerted to a certain level of threats, but it does not provide complete protection. Remember that users need to understand the threats they may face and protect themselves against such threats.

In your daily life, implement the following minimum-required countermeasures:

- Eliminate vulnerabilities in the operating system and applications (including web browser and mailer) on your PC (bring them up-to-date) and strengthen the security settings (e.g., Deactivate ActiveX and JavaScript);
- Regularly perform virus scan by using your antivirus software;
- Do not easily open an e-mail or an attachment from a stranger;
- Do not easily trust in an e-mail from a bank or a credit loan company;
- If an alert message is displayed by your OS, without panic, cancel the download which is against your will.
(1) Virus e-mail  
An e-mail whose attachment carries a computer virus. If the user carelessly opens such attachment, his PC is infected with the virus.

(2) Spam e-mail  
An e-mail containing advertisements or harassing messages (e.g., for specific individuals, for religious acts) that is sent to unspecified number of people. It may be for commercial purposes or other purposes. In general, this is also called "unwanted mail".

(3) Phishing  
An act of sending an e-mail disguising as a financial institution (e.g., bank, credit-card company) or other organizations to the target, with the goal of fraudulently obtaining his/her personal information (e.g., address, name, bank account number, credit-card number).

(4) Bot  
Bot is a type of computer virus and it infects PCs. It is designed to allow an external attacker to remotely operate the infected PCs via network (Internet). After the infection, it waits for commands from the external attacker and executes processing as instructed. Because its behavior is similar to that of "robot", it is called "bot".

(5) Worm  
General viruses require a program which is subject to infection, but worms do not require such program and they create copies of themselves for self-propagation. Because they look like an insect which worms within a network, they are given this name.

(6) Antivirus software  
Software that detects and cleans computer viruses. Note, however, that data damaged by a virus cannot be restored.

(7) Cracker  
A person who hacks into someone else's computer through a malicious act (e.g., unauthorized access) and eavesdrops or falsifies data.

(8) Virus creation tool  
A tool that allows users to easily create malicious programs.

(9) Root-kit  
A package of programs that carry out wrongful acts. It is used for unauthorized computer access and embedded into the hacked computer. It works in a manner that computer users do not recognize the acts of the malicious program.

(10) Instant-Messaging (IM) service  
Software that allows users whose PC is connected to the Internet to engage in chat or send/receive files. Those using this software can verify if the other side is connected to the Internet, and send messages in real
time. Among popular ones are AOL Instant Messaging and MSN Messenger.

(*11) Mailer
Software that allows users to create and send/receive e-mails and that saves and manages received e-mails.

(*12) Signature
Generally, it means an individual's signature, but in this guide, it refers to data that shows characteristics/patterns of viruses. A detection method that uses signature is called signature-based detection or detection through pattern matching. Virus definition files are a set of these signatures.

(*13) Virus definition files
Files that contain characteristics/patterns of viruses. These files are used by Antivirus Software to detect viruses. They are so called a set of arrest instructions.

(*14) E-mail filtering service
A function to filter out unwanted e-mails and spam e-mails, which is provided by an e-mail server (or service providers in the case of home users).

(*15) Spyware
A program that is installed on computers without their users/administrators' intent and that collects their users' personal information and access history, etc.

(*16) Cryptographic communication (SSL)
A protocol in which information exchanged over the Internet is encrypted and sent/received. It allows users to send/receive personal information and credit-card number, etc. in a secure manner and therefore, it is used for websites such as online banking.

(*17) Security zone
Detailed explanation is provided on the following site:

- Setting a Security Zone
  (in Japanese)

(*18) Proxy server
This server is placed at the boundary between the Internet and intranet and relays communications between networks. This is called "proxy server" and allows for virus countermeasures for e-mail servers and security measures such as web contents filtering.

(*19) Web (URL) filtering
This is a function to block access to Websites that have certain URL addresses. In this service, URL address information for phishing sites and malicious Websites that distribute viruses is shared to block access to such sites.

(*20) One-click ware
This is a program embedded in a Website whose purpose is to carry out one-click billing fraud. It disguises as an image or a video so that site visitors who are deceived by its appearance would download it. Once it infects a PC, it displays a billing message on the desk top. In most cases, such message is not easily deleted.
8. References

- Awareness Survey on Information Security Threats for FY 2011
- Information Security White Paper for FY 2011
- Reminder for this Month
- How to Secure your Website
- Information on Virus Hoaxes Demagogic E-mail
- Information on a Demagogic E-mail Concerning "jdbgmgr.exe"
- To prevent unfair billings
- Countermeasures against Phishing

IPA Countermeasures Guide Series
http://www.ipa.go.jp/security/antivirus/shiori.html
- IPA Countermeasures Guide Series (1) Countermeasures on Computer Virus
- IPA Countermeasures Guide Series (2) Countermeasures on Spyware
- IPA Countermeasures Guide Series (3) Countermeasures on Bots
- IPA Countermeasures Guide Series (4) Countermeasures on Unauthorized Access
- IPA Countermeasures Guide Series (5) Countermeasures on Information Leakage
- IPA Countermeasures Guide Series (10) Countermeasures against Targeted Attack Mail <Avoidance of Risks>
Bunkyo Green Court Center Office 16th Floors
2-28-8 Hon-Komagome, Bunkyo-ku, Tokyo, Japan 113-6591

URL http://www.ipa.go.jp/security/

[Worry-Free Information Security Consultation Service] (Computer Virus and Unauthorized Computer Access)

URL http://www.ipa.go.jp/security/anshin/
E-mail anshin@ipa.go.jp