Design and Operational Guide to Protect against "Advanced Persistent Threats"

Revised 2nd edition

A Approach to improve security measures against new cyber security threats



Information-technology Promotion Agency, Japan

 \mathbf{P}

November 2011

This document is available for download at:

Design and Operational Guide to Protect Against "Advanced Persistent Threats"

http://www.ipa.go.jp/security/vuln/documents/eg_newattack.pdf

Table of Contents

Table of Contents
Introduction
Contents and Positioning of this Document
Target Audience
1. Executive Summary
1.1 Impact on Organizations
1.2 Concept of Our Measures
2. Issues and Background of "Advanced Persistent Threats"
2.1 About "Advanced Persistent Threats"
2.2 Definition and Methods of Targeted Attacks
2.2.1 Types of targeted attacks
2.2.2 Overview and characteristics of APTs
2.2.3 Overview and characteristics of indiscriminate attacks
2.2.4 Spheres of information security and relevant security measures
2.3 Behavior of "Advanced Persistent Threats"11
2.4 What cannot be done with "Inbound Measures" 12
2.5 Summarizing the Concept of Our Measures
3. Sorting out Behavior and Issues of "Advanced Persistent Threats" 15
3.1 Flow of "Advanced Persistent Threats"
3.2 Analyzing and Summarizing the Attack Specifications
3.3 Types of backdoor communication (according to research in 2011)
4. Points to Counter New Threats
4.1 Considering with Fresh Measure Concept
4.2 Inbound and Outbound Measures
4.3 How to Realize "Outbound Measures"
4.4 Effectiveness of Backdoor Countermeasures, Issues for Consideration
4.5 Eight Measures to Prevent Critical Information from Being Stolen by Cyber Attacks 34
Appendix1: Results from Testing Implementation Items
Appendix2: Measure Requirement Definition Templates
Appendix3: Summarizing Information Security Measures

Introduction

In recent years, there have been cases in which organizations' intellectual property information and personal information are stolen in an attack via e-mail or an attack via external media such as USB stick. The stolen information (a manufacture's design information, etc.) was critical information for those organizations and was stored in a location deemed unreachable by outsiders in general. But in the case of recent attacks like these, critical information is stolen from inner systems deemed unreachable by outsiders in the past.

These attacks have successfully been carried out not because of absence of considerations for security managements on the part of organizations but because they take subtle approaches to cause damages even to organizations that have certain level of security managements in place. Internationally, some of these attacks are known as *Advanced Persistent Threats* (APTs). IPA also calls it "Advanced Persistent Threats" in this document.¹

When it comes to defending against attacks via the Internet, organizations tend to focus on blocking the invasion of such attacks into their systems at the inbound by using firewall, antivirus software, etc. But these "Inbound Measures" do not work for the case where systems within the organization have already been infected with a virus and another attack to exfiltrate more information is carried out.

To prevent critical information from exfiltration the data, which would cause losses, organizations need to establish measures on the premise of possible virus infection. Information transferred from viruses to attackers passes through the organization's network, heading for the outbound. So it is important to have "Outbound Measures" in place to prevent the information from going out of the organization's network. Designing and operating networks in consideration of defense is critical for "Outbound Measures". Organizations need to properly design what attacks need to be prevented at the inbound and what at the outbound.

This document explains what "Advanced Persistent Threats" really is and how to design and operate networks and systems to counter it.

We hope this document will be of help in solving security issues associated with "Advanced Persistent Threats".

Contents and Positioning of this Document

In December 2010, IPA's working group for threats and measures released Technical Watch Vol1² "Advanced Persistent Threats" and since then, has been examining effective measures against such attack. This document presents recommended measures for network systems that were derived from the views exchanged between "those engaged in computer virus analysis" and "those engaged in network system design" in this WG about effective measures for organizations.

What is described in this document is just one example of solutions. It is not a requirement that all the measures presented be implemented. We just hope this document will serve as a reference material for solving security issues associated with "Advanced Persistent Threats".

Target Audience

Target audience of this document is classified by chapter as follows:

Chapter 1:Corporate managers and other people who want to know the threats of "Advanced Persistent Threats" and make investment decisions from the management aspect.

Chapter 2:Project administrators who provide suggestions and instructions about measures against "Advanced Persistent Threats"

Chapter 3 and later part of this document:

Those who actually implement measures against "Advanced Persistent Threats"

¹ In Japan, since the definition of APT is ambiguous, it is calling by another peculiar Japanese name as a confusion preventive measure. IPA named this "Attacks of new type".

² http://www.ipa.go.jp/about/technicalwatch/20101217.html

1. Executive Summary

When establishing information security measures, it is important to make clear what needs to be protected from what attack. This document presents approaches to devising measures against "Advanced Persistent Threats" that steals information located deep within an organization.

1.1 Impact on Organizations

Targeted attacks are evolving daily. Cyber attacks became prominent around the year 2000. At that time, easy-to-attack publicly-accessible servers were targeted for such attacks. As a result, damages such as site compromise and proliferation of viruses were caused. This type of attack was carried out by a single attacker for such purposes indiscrimination. To counter these attacks, organizations installed firewall and antivirus software and implementing measures against vulnerabilities, trying to block their Intrusion at the inbound (i.e., "Inbound Measures").

However, attackers in recent years carry out cyber attacks for their business, in the form of coordinated attacks, social engineering³, exploitation of zero-day vulnerabilities⁴, etc. and with such dexterity that the victim does not realize that the attack is being carried out. As a result, organization's critical information such as intellectual property information and personally identifiable information might be stolen, or organization's critical systems might be cracked. Furthermore, there have been cases where critical information that was located deep within an organization was stolen, which was thought to be impossible in the past.

1.2 Concept of Our Measures

At the meetings of IPA's working group for threats and measures, professionals mainly engaged in computer virus analysis and professionals mainly engaged in system and network design and operation shared information closely and in collaboration, analyzed how "Advanced Persistent Threats" works on actual systems and networks within an organization and examined effective measures for organizations.

Collaboration between professionals analyzing attacks (hereinafter referred to as "attack analysts") and professionals designing and operating an entire system (hereinafter referred to as "system designer/operator") facilitates detailed examination of how organizations can effectively protect their systems and networks against "Advanced Persistent Threats".

Neither of those two professional groups is expected to have a full picture of both the attack and systems. For example, attack analysts conduct their analysis from the aspect of how the attack is carried out and what methods are available to prevent the attack; but they may fall short of analyzing "to what extent each method is effective and practical in protecting the entire system" and "what would happen if their measures were circumvent". In short, attack analysts may fall short of having a full picture of a system within an organization. On the other hand, system designers/operators tend to accept without questioning measures proposed by attack analysts, which may result in implementing costly measures that are not commensurate with the full picture of the system.

The way of devising measures presented here is effective not only against "Advanced Persistent Threats". Should more elaborate attacks be carried out in the future, collaboration between professional groups would facilitate the establishment of effective measures.

³ General term for an act of exploiting gaps in human psychology and behavior and obtaining information fraudulently from the victim by means of narrative skill, eavesdropping, or peeping, etc.

⁴ Unknown vulnerabilities for which no measures are released.



Figure 1-2: Image of Effectiveness of Bridging

On the basis of this concept, IPA's working group for threats and measures examined measures against "Advanced Persistent Threats". Then it found that "Advanced Persistent Threats" has common attack techniques, including virus-attacker communication. It also learned that organizations need to have "Inbound Measures" to defend against conventional attacks and "Outbound Measures" to prevent information from being passed to an attacker outside in case part of an attack gets into the organization, by blocking the common attack technique section. It is important that "Outbound Measures" be penetrated to organizations.



Figure 1-1: Image of "Inbound Measures" and "Outbound Measures"

2. Issues and Background of "Advanced Persistent Threats"

2.1 About "Advanced Persistent Threats"

On the Internet, a variety of attacks are carried out almost every day. They include SQL injection attack that steals Personal information from servers by exploiting vulnerabilities in Web applications or software running on them; phishing scam that induces computer users to click a malicious link to obtain money by fraud; and an attack that compels computer users to install fake antivirus software on their computers.

One elaborate attack being carried out in recent years uses e-mails or external media to break into computers of staff and executives within an organization, as typified by targeted attack. After the Intrusion, it gets further into the organization and eventually steals critical information for the organization (i.e., intellectual property information and personally identifiable information) covertly.

In the past, it was thought that if an organization had certain level of security controls in place, its inside would not be intruded. But this is not true for attacks like targeted attack. Because these attacks are carried out persistently, adapting to the measure situation at each occasion and approaching the target information little by little, they can circumvent conventional measures. This was evidenced by the cases where organizations' critical information such as intellectual property information was stolen or organizations' critical systems were cracked. This type of attack is called "Advanced Persistent Threats (APT)" in abroad. IPA calls it "Advanced Persistent Threats". This "Advanced Persistent Threats" consists of <u>common attack techniques</u> for which conventional measures do not work and <u>individual attack techniques</u> that are tailored for a specific organization. Among them, "common attack techniques" become a keyword for measures against "Advanced Persistent Threats".





2.2 Definition and Methods of Targeted Attacks

Some APTs are targeted attacks, but keep in mind that targeted attacks fall into a few patterns, depending on the attackers' intent and methods. Thus, in considering your security options in system design, you should sort out which type of targeted attack may apply to your organization and determine relevant measures. Misinterpreting the attackers' intent may lead to meaningless measures that are costly and ineffective, and your security issues will remain unresolved. This section therefore categorizes targeted attacks and concludes by indicating the corresponding sphere of information security activities for your measures.

Specifically, targeted attacks are positioned and classified within the sphere of cyber security. This understanding should be fundamental in your discussions and implementation of measures. Among other benefits, it will help you establish a common awareness by clarifying the nature of issues under discussion, which can support measures with substantive results and provide more robust defense against attacks.

Accordingly, this guide distinguishes between two types of targeted attacks, based on various characteristics.

2.2.1 Types of targeted attacks

Looking beyond the aspect of targeted e-mail attacks to consider the overall behavior and intent of attackers, we can classify targeted attacks into the following two types. To distinguish between them, we must consider not only differences in the message body of targeted e-mails but also differences in the attackers' intent, behavior, and overall attack activities.

Advanced persistent threats (APTs)

In the context of spying on or exfiltration organizational information that affects national economies or security, APTs are persistently cyber espionage targeting specific organizations. The term *APTs* as used in the United States and elsewhere indicates this type of attack.

Indiscriminate attacks

These attacks, which steal personal information mainly for financial gain, do not target specific victims.

Of these, APTs can be further classified by level of attack as either general/exploratory information reconnaissance (cyber espionage) or targeted attacks for specific purposes, which are more sophisticated and hard to detect. Be aware that the targeted e-mail used in cyber espionage may contain "single-use" viruses that the attacker intends antivirus software to detect and remove.





2.2.2 Overview and characteristics of APTs

In Advanced Persistent Threats, attackers conduct careful preliminary information reconnaissance on affiliated organizations and others as the basis to select their ultimate targets and plan attacks. At this stage, attackers gather e-mail messages, addresses, and similar information for attacks, after which they prepare targeted e-mail and viruses to use against targeted organizations.

Using the targeted e-mail to Infilitrate the system, attackers then establish a backdoor, which they use for ongoing intelligence-gathering from the organization via remote control. Characteristics of this pattern of attack include having a specific intent and conducting a gradual series of attacks (for intelligence gathering) against the same target. Attackers also target information in closed systems, by means of virus infection via USB.

Of all cyber attacks, this attack pattern is the most dangerous and difficult to defend against. Attackers take this approach against specific industries or fields. Examples include cyber attacks targeting governments and national or international defense. As mentioned, the general term for these serial attacks is *Advanced Persistent Threats* (APTs).

It must be noted that unlike occasional, suspicious e-mail or virus infections, these attacks involve ongoing hacking of targeted systems. They should be perceived as attacks meant to destroy from the foundation the balance of the personnel, systems and work flows of an organization. Additionally, because perfect implementation of conventional inbound measures to detect and prevent incursion is difficult against APTs, outbound measures must also be implemented to block excursion and prevent information leaks.

To evaluate the priority of measures against APTs, consider the context, intent, general characteristics, potential organizational or social impact, and estimated costs. Toward this end, also review relevant measures taken by computer security incident response teams (CSIRTs), which use mainly conventional methods.



Figure 2-2-2-1: Overview and characteristics of APTs

Details of the overall attack sequence of APTs are shown below. More of these attacks have emerged since around 2005, and although they have been observed around the world, the attackers' intent and motives—who is conducting the attacks, and why—remain largely unclear. As for characteristics of recent incidents, attackers first obtained e-mail messages, addresses, and similar information in preliminary cyber espionage on affiliated organizations or local authorities. This information served as the basis to break through inbound system defenses using targeted e-mail containing remote control tools—specifically, RATs⁵. Via off-site remote control, the attackers then spied on information of interest on computers at the organization (in e-mail and elsewhere) or in their storage systems.

⁵ RATs:remote access trojans/remote administration tools

In other cases, as a conventional means of attack, organizations were infected with a virus through targeted e-mail, which opened a backdoor through which the attacker spied on information of interest, updated the spyware, and so on. Either method of attack is a way to conduct ongoing intelligence-gathering within an organization.



Figure 2-2-2-2: Details of overall APTs attack sequence

2.2.3 Overview and characteristics of indiscriminate attacks

This type of attack may be easily confused with APTs, because victims receive suspicious e-mail. What distinguishes indiscriminate attacks is that they target random victims (that is, an unspecified large number of people) and are conducted to obtain personal or financial information, so the attack itself is a singular event. Although random attacks ultimately reach corporate or governmental addresses, the attacks should be considered distinct from attacks on these organizations.

Judging by suspicious e-mail messages alone, it may be difficult to differentiate indiscriminate attacks from APTs. In determining effective design-based defensive measures against indiscriminate attacks, consider the overall attack behavior to distinguish these attacks from APTs.

Indiscriminate attacks are clearly different from APTs in terms of the severity of impact and organizational problems they pose. They are not intended as acts of espionage with serious consequences in matters of national defense or the economy. Moreover, conventional inbound measures are often effective against indiscriminate attacks. Examples of attack vectors include e-mail with malicious attachments (such as SpyEye) that add infected computers to a botnet, phishing e-mail that steals bank PINs, e-mail with links to phishing sites, and websites compromised by SQL injection.



Figure 2-2-3-1: Overview and characteristics of indiscriminate attacks

2.2.4 Spheres of information security and relevant security measures

The positioning of APTs in the context of information security in general is illustrated below. Because cyber attack issues differ from information management issues (such as leaks) both qualitatively and in defensive measures, these spheres of information security must be considered separately. Moreover, because cyber attacks may involve a variety of incidents, before considering viable security measures, clarify which attack pattern the measures are for, and what information must be protected. For example, different measures are taken for security threats faced by an organization (or specifically, the organization's information systems) than for threats faced by home computer users.

In particular, APTs as discussed here are persistent, involving ongoing information espionage and other activities that pose serious consequences to organizations. Moreover, security measures are difficult to take against these attacks, and incursions are hard to detect. For organizations, APTs must therefore be addressed as a significant threat.

Keep in mind that defensive measures against indiscriminate attacks will not protect against APTs. When planning measures against APTs, evaluate the potential impact of APTs on your organization. Keep the practicalities (including cost) in mind when deciding your approach and how thorough your protection should be. Most important, do not to treat measures against APTs as merely another facet of general defense against cyber attacks. Instead, effective security calls for an approach highly tailored to your organization. In this regard, any lapses in your judgment will only drive up costs without benefit.

Although conventional inbound measures are more or less effective against many cyber attacks (and indiscriminate, non-targeted attacks), the fact that APTs are especially serious, measures are difficult to take, and incursions are hard to detect makes it imperative to establish outbound measures to detect and prevent espionage.

In this guide, APTs and corresponding design-based security measures are discussed in a way that encourages security against APTs on the level of system design. Because indiscriminate attacks share many characteristics of APTs, measures derived from this guide will also be useful against indiscriminate attacks.



Figure 2-2-4-1: Spheres of information security and relevant security measures

2.3 Behavior of "Advanced Persistent Threats"

Damages caused by "Advanced Persistent Threats" include internal important documents or data being stolen covertly. In 2011, targeted attack e-mails taking advantage of the Great East Japan Earthquake were confirmed. Typical flow of this attack is as follows:

- (i) <u>Preparing for the attack</u> In preparation for espionage to obtain the desired information, attackers conduct attacks on organizations affiliated with the targeted organization. E-mail and similar information gained at this stage are used in later stages.
- (ii) Initial infiltration

An e-mail posing as the one from a concerned party is sent to a specific e-mail address within an organization. A file attached to this e-mail is an unknown virus that is not detected with antivirus software. Virus infection at this stage allows the attack to move on to the next stage.

(iii) Building an attack infrastructure

The virus downloads another virus and communication path between the attacker and the former virus is established. Specifically, communications are done by modeling on the HTTP communication used in the organization's business operation (i.e., HTTP backdoor communication).

(iv) Probing the target system

At this stage, the virus searches for the target information within the internal system. This may take several weeks to several months, requiring frequent interactions with the attacker. Other tasks such as virus updates that are tailored for each organization are also carried out.

(v) Pursuing the final goal of the attack

Organizations' critical information such as intellectual property information is stolen and transferred to the attacker. Further attacks can be carried out by using the internal information obtained from the organization (e.g., the organization's account information).

In this flow, the attacker tries to steal useful documents, which is the final goal of this attack. To this end, the attacker frequently communicates with the virus and attempt to obtain critical information specific to the organization. For the targeted attack e-mails that took advantage of the Great East Japan Earthquake, as of the creation of this guide, no report has been submitted to IPA about critical information being stolen by an outsider; in abroad, however, such cases did occur, including the theft of a security product's critical information and a government's critical information.

This type of attack is not limited to e-mails. USB sticks and other external media have also been used as an inbound for such attack. In the case of an attack that uses a USB stick or other external media (hereinafter referred to as "attack-via-media"), even a computer that is not connected to the Internet and thus has no risk of receiving an attack from outside is compromised. Examples of attack-via-media include Conficker and Stuxnet.

In the case of targeted attacks or attack-via-media, even if the organization has security controls in place, they may be circumvented. This is because recipients generally have no idea whether the e-mail or USB stick they received is harmful.

As a result, an enterprise's classified documents (such as on an anchor product) might be stolen and abused without it noticing the attack, leading to the losses such as the deterioration of competitiveness.

2.4 What cannot be done with "Inbound Measures"

Nowadays, it is natural for organizations to have security controls in place. However, despite such security controls being implemented, they may not work effectively against "Advanced Persistent Threats". This is because most of them are focused on preventing attacks from outside at the inbound. Since these controls are intended to detect and prevent attacks at the inbound, we shall call them "Inbound Measures" throughout this document.

While Web and e-mails are frequently used within an organization, they are also used by "Advanced Persistent Threats" to get inside an organization. Needless to say, organizations have been implementing "Inbound Measures" to tackle such attack, including installing firewall, intrusion detection system (IDS) and antivirus software, and applying security patches to remedy vulnerabilities.

But these "Inbound Measures" alone are not sufficient, because some attacks cannot be prevented at the inbound only. For example, let's think about a targeted attack e-mail that exploits zero-day vulnerability. If the e-mail's attached file is a virus and antivirus software fails to detect it, the PC is infected with the virus by opening it. Furthermore, not all viruses are detected with antivirus software. This is because attackers first check the detection status and then create a file that they think would not be detected and launch an attack. Even if the organization applies security patches as part of vulnerability measures, it does not work for the case where zero-day vulnerabilities in a variety of organization-used software are being targeted by attackers. So it is becoming more or more difficult for organizations to address all software vulnerabilities. Furthermore, communication feature of the virus uses a communication used by Web, so it is difficult to detect abnormalities from such communication.

For this reason, if all measures were circumvented, the attack would end up in success. Of course, by installing these software products and implementing measures at the inbound, organizations can significantly reduce the success rate of an attack. If these "Inbound Measures" are not implemented, even a known virus or a virus that exploits a known vulnerability may succeed in an attack. While "Inbound Measures" are essential, some attacks can circumvent them. As a result, organizations may suffer from damages such as their critical information being stolen.

Item	Limits of Inbound Measures		
Diversification of virus types	As there are a large number of viruses, not all the viruses are detected with antivirus software.		
Exploitation of zero-day vulnerabilities	Even if patch management is in place, an attack may be carried out successfully.		
Exploitation of vulnerabilities in a variety of software	In some cases, there are so many types of patches to apply that organizations cannot manage them properly.		
Attacker-virus communications following a successful attack	Because a communication path used in the organization's business operation is used, it is difficult to distinguish malicious communications from normal ones.		

Table 2-3: Limits of "Inbound Measures"

2.5 Summarizing the Concept of Our Measures

As discussed in Section 2.3, there are limitations to "Inbound Measures". So, organizations need to have extra measures in place.

When establishing measures, organizations should take into account possible losses caused by the attack. When we think about what kind of incidents would cause losses to an organization, we would come up with the leaks of the organization's classified information to an outside party or the stoppage of critical systems (as described in Section 2.2).

A key point for measures against "Advanced Persistent Threats" is: "not allowing classified information to be passed to attackers" and "not giving attackers a chance to operate critical systems". To this end, we need to understand how a virus works after getting into an organization.

After getting into an organization, the virus sends some sort of information to the attacker. Apparently, this communication is done to notify the attacker of its successful infiltration into the organization, what information is stored, and to what virus it needs to be updated to make an attack more effective.

One of the measures to avert negative impacts on the organizations is to block outbound communications so that information is not passed to the attacker and the attack ends up in failure. So it is important for organizations to have "Outbound Measures" in place with which they can block attacker-intended communications and avert negative impacts on them. Specific measures are described in Section 4-1 through Section 4-3.



Figure 2-4: Image of "Outbound Measures"

For "Advanced Persistent Threats" described in this document and other evolving attacks, a department that sees to the organization's entire systems and a department that knows the real threats of the attack need to collaborate and analyze the impacts on organizations. Based on the assessment results, organizations need to implement required measures. The most important point is, those measures needs to be interoperable to be effective. So, let's think about interoperable measures.

When establishing measures, project managers need to assess their organization's system's capacity to respond to "Advanced Persistent Threats". For this, they need to check whether persons in charge have an understanding of the threats of this attack and if not, to make them understand the contents of Chapter 3 and later part of this document. The next step is to instruct them to examine whether the specific threats can be prevented. Based on the examination results, project administrators analyze impacts on their organization and determine whether or not to implement measures.

[An approach to closed-system security]

In industries such as manufacturing and finance, we can classify information systems as open or closed depending on whether they are directly connected to the Internet. Even for closed, isolated system, administrators must consider the impact of APTs. Although closed systems are not directly connected to the Internet, data can be exchanged with them via USB sticks or other removable media. Attackers are likely to focus on this vector.

Initially attackers may target open systems for virus infection, which they hope to spread via USB sticks or similar means. When members of the organization insert an infected USB stick in a closed system computer, the closed system may also become infected. The virus will then extract confidential information, and when a USB stick is returned to an open-system computer again, the information will be sent to the attackers. Thinking a system is safe merely because it is closed is therefore a mistake.

At the same time, as long as USB sticks or similar devices are used in business, it would be impractical to prohibit their use. For this reason, to protect information in closed systems, consider the same kinds of measures taken against espionage in open systems.

The espionage is ultimately conducted through an open system. Outbound measures in relevant open systems will prevent attackers from obtaining information from the closed system. This approach can help your organization avoid the consequences of incursion.

[Budgetary considerations for security measures]

New cyber attacks seem to emerge every day. Unfortunately, introducing inbound measures for them increases security deployment and administration costs. Even if many layers of similar measures are introduced, their potential effectiveness is limited, and the ultimate goals of attacks—espionage or destruction of information—will not change. In addition, as of 2011, we have seen no major changes in one common attack method, which is that in order to steal information, communication between the attack server and the attack infrastructure buried deeply inside the system is essential.

For this reason, establishing outbound measures to avoid real harm entails considering these measures on the level of system design. The required approach involves keeping system costs balanced while determining and selecting essential and effective security measures that will be practical.

3. Sorting out Behavior and Issues of "Advanced Persistent Threats"

This Chapter provides concrete description of characteristics and attack pattern of "Advanced Persistent Threats".

When it comes to cyber security (attack), organizations would focus on individual cases (incidents), checking what attack was carried out against which organization to steal such information. In this chapter, we look at common behaviors of "Advanced Persistent Threats", rather than examining each case. This approach would be helpful in devising measures in Chapter 4.

3.1 Flow of "Advanced Persistent Threats"

Let's take a look at the flow of infiltration by "Advanced Persistent Threats". Infiltration into an organization is carried out in planned four stages. Such infiltration is intended to steal information from the organization and targeted at information systems within the organization.

Preliminary stage: Preparing for attack

In preparation for espionage on desired information, attackers study the targeted organization and obtain relevant information in advance. Toward this end, they attack affiliates or related organizations to gather information such as e-mail correspondence with the organization that will serve as the basis for initial infiltration. This information is used in attacks with a better chance of helping attackers infiltrate the organization.

First stage: Initial infiltration

At initial infiltration stage, a variety of attack techniques are used. Suspicious (targeted) e-mail is one example. This technique is used by attackers to send a virus into the deep part of an organization and if such e-mail is opened by anyone within the organization, its objective is achieved. At initial infiltration stage, there is no need to infect multiple systems. Attack techniques applied at this stage are single-use techniques and designed on the assumption of possible detection and disinfection.

Second stage: Building an attack infrastructure

After a successful infiltration into the system, the virus quickly establishes backdoor communication path with a sever (C&C⁶) provided by the attacker. Unlike conventional backdoor, this backdoor uses a HTTP communication or other communications that are used in the organization's business operation and thus are not blocked by the organization's firewall. Using this backdoor, the virus adds required functions for probing the target system and builds an attack infrastructure.

Third stage: Probing the system

Using this attack infrastructure, the virus probes the system for the target information. In this occasion too, backdoor is used to communicate. It continues its probe while checking the system information.

Fourth stage: Pursuing the final goal of the attack

The virus obtains the target information through the backdoor. Based on the information obtained, it may carry out an attack again. While leaving the established attack infrastructure within the organization, it repeats infiltration and obtains more information. This is a persistent attack.

⁶ Command and Control: An external command and control server prepared by an attacker.

Table3-2: Description of Attacks at each Stage	e of "Advanced Persistent Threats"
--	------------------------------------

Stage	Description of Attack	Characteristics
Preparing for attack	 (1) Attacks organizations affiliated with the targeted organization • E-mail espionage and so on 	Gathers e-mail messages and recipient addresses to use in social engineering, to improve chances of success in initial infiltration.
Initial infiltration	 (1) Initial attacks Sends a targeted attack e-mail with a virus attached Guides (the victim) to a download server via a defaced Website Virus infection via external media (such as USB stick) 	Circumvents "Inbound Measures" and gets deeper into the system; Quickly moves on to the next stage; Uses single-use attack techniques.
Building an attack infrastructure	 (1) Builds an attack infrastructure by using backdoor Downloads another virus and gives it instructions. Adds advanced features to the virus Builds an attack infrastructure within the system 	The established attack infrastructure is not detected. The established attack infrastructure is reused.
Probing the system	 Obtains information from the system within the organization Identifies the location of the target information 	Repeatedly carries out the attack over time.
Pursuing the final goal of the attack	 Steals the organization's critical information Based on the organization's information (such as account information), sets the target again 	Steals information through the repeated attack. Steals information that affects the organization.

[Example of Initial Infiltration]

Here we describe an example of how a virus circumvents the detection and gets deeper into the target system (organization) at the initial infiltration stage. The following is an example of a targeted attack e-mail related to a nuclear accident at the Fukushima nuclear power plant. The figure below shows an image of HispaSec Sistemas "VIrus Total⁷" that fails to detect a virus attached to an e-mail. In this way, no antivirus software can detect such virus upon receiving "Advanced Persistent Threats.

Apparently, attackers send such virus after confirming that it is not detected by the antivirus software installed on the target computer. Similarly, a virus that is extended through the later-established backdoor is not detected, either. By using this technique, the attack can break through the measures provided by the system.



Figure3-1-1: Image of a Scan Result; As You can See, the Virus is not Detected at the Initial Stage

[Example of Building an Attack Infrastructure]

The goal of this stage is to enable communications between the virus that infected the organization and the attacker's server, and this is done as follows:

(1) Establishes a communication path with C&C server

After breaking through the organization's measures at initial infiltration stage, the virus establishes a communication path with the attacker's C&C server. This communication path is called backdoor and it uses HTTP communication. Because this uses the same communication as the one used by the company staff's PC to access the Internet, it is less likely to be detected and blocked with the organization's measures.

(2) Downloads advanced features

Advanced features appropriate for attacking the target organization are downloaded through this backdoor.

Through these steps, an attack infrastructure is established in the deep part of the organization.

⁷ https://www.virustotal.com/

Attack infrastructure refers to the establishment of backdoor and a virus that evolved enough to receive instructions from the attacker's C&C server. Once this attack infrastructure has been established, the attacker preserves it for later use, including probing the system and obtaining the target information through persistent, repeated infiltrations.





(i.e., Building an Attack Infrastructure)

[Actions taken after the establishment of an attack Infrastructure: Proving the System;

Pursing the Final Goal of the Attack]

The communication diagram below shows the flow of communications between the attack infrastructure established in the deep part of the organization (system) and the C&C server. As shown in this diagram, the virus continues to send a "Keep alive" signal to the C&C server through the established backdoor and based on the instruction given, it downloads advanced features. This type of communication is carried out persistently over time and as a result, the virus expands its features and gets deeper into the target organization.

While lurking, the virus continues to send the "Keep alive" signal until it receives an instruction. This is a persistent attack in which the virus repeats act-rest cycle based on the instructions given											
Unnatural "Keep alive" communication											
Date	Date SA DA Proto. Size IDS/AV										
2011/*/** **:**	win-xp-sp2: 1865	*.com.br: 80	tcp	178							
2011/*/** **:** <u>*.com.br: 80 [BR]</u>		<u>*.com.br: 80 [BR]</u> win-xp-sp2: 1865		tcp 161600 (SF)Portable Execut	(SF)Portable Executable binary file transfer						
	(AV)V adup-107										
In response to the "Keep alive" signal, an executable binary file is downloaded											

Figure3-1-3: Flow of Downloading and Executing a New Virus

Target of "Advanced Persistent Threats" is organizations' systems. So we need to view this "Advanced Persistent Threats" as a threat to organizations systems. As for organizations' system, the larger its scale, the more complex it is, and if this is the case, we cannot view this "Advanced Persistent Threats" mealy as a problem for a single PC or a Web server.

To facilitate the examination of issues and measures associated with system design structure, it is a good idea to identify certain patterns in the cyber attack cases that have actually occurred. National Information Security Center (NISC) presents six "behavioral patterns" of cyber attack in a report by a working group for risk requirement reference model. The patterns presented below are based on the above-mentioned patterns.

[Five Types of Advanced Persistent Threats]

Type 1: Infected with a virus by browsing a legitimate website (information being stolen)

A user of the system brows a defaced, legitimate website and was guided to a virus distribution site and virus infection takes place. As a result, authentication information and other information are stolen and a backdoor is established. Furthermore, attempts are made to expand the attack infrastructure through the use of the authentication information obtained.

Type 2: Targeted e-mail attack (information being stolen)

A deceiving e-mail containing a virus is sent to a computer and if opened, a backdoor to a C&C server is established. As a result, information stored in the information system is leaked. Since an e-mail targeting at a specific organization is sent, this is called "targeted attack".

Type 3: Induction via a defaced, legitimate website

Site visitors are directed to a site where a virus is distributed, prepared by attackers who hack a legitimate website to redirect visitors to a site that infects them with a virus. In this way, targeted organizations become both victims and victimizer of an attack.

Type 4: Infected with a virus via a medium (theft of information), attack against control systems

A virus that got into a USB stick or other media in a variety of contexts enters into an information system. After the interfusion, the virus spreads its infection to the system's network and a backdoor to a C&C server is established. As a result, network and server failures occur and information stored in the system is stolen. One facet of this attack was that it exploited information exchanged via USB between the victim's open, core system and their closed control system.

Information collected by a virus that infected the closed system was saved to a USB stick and uploaded to a C&C server when the USB stick was switched to the open system. As a result, through the backdoor communication established in the in-house mission-critical system, the virus receives instructions from the C&C server and performs tasks such as stealing information and adding features to a program designed to attack the closed system.

Type 5: Attack infrastructure using combined DDoS attacks

Unlike general DDoS attack, combined DDoS attack uses functionally-distributed multiple viruses that work in a coordinated manner. Here, note the attack infrastructure, instead of the DDoS attack itself. The attack infrastructure obtains information from infected computers.

[Common Behavioral Features of "Advanced Persistent Threats"]

And now, based on these attack patterns, we examine the impacts on information system and measures. We also derive common behavioral features from these patterns in order to help organizations design measures for their information systems. The following are four common behavioral features of "Advanced Persistent Threats", which enable a "hard-to-detect, silent attack". As you can see, any attacks involving stealing information and destroying information have common behavioral features, which are linked with the measures for systems that are described in Chapter 4. Any of these are hard to cope with conventional measures.

- (1) Http backdoor communication
- (2) Spread of infection within the compromised system
- (3) Simultaneous updates (e.g., P2P)
- (4) Information gathering via USB



Common Attack Technique Section

Figure 3-2-1: Four Common Behavioral Features

In order to devise system measures against these common behavioral features, we need to analyze the specific flow of the attack against a system within an organization. By understanding how this attack flow is related to the system's network, system designers can design a system taking into account its impacts and measures.

Table 3-2 shows common behavioral feature's roles and how they work on a system within an organization.

Table3-2: Roles of Common Behavioral Features

Common Feature	How it Works on a System within an Organization	Roles
	Using http or other communication protocols or ports that are used by the target organization, it performs backdoor communications.	Establishes a communication between the virus and the attacker's C&S server
Http backdoor communication	 There are four major patterns of communication: HTTP protocol or similar protocols that use a proxy Proprietary protocols that use a proxy HTTP protocol or similar protocols that do not use a proxy Proprietary protocols that do not use a proxy Proprietary protocols that do not use a proxy 	
Spread of infection within the compromised system	Infects a network within an organization and then spreads infection to systems by exploiting vulnerabilities.	Infects many more computers so that it can more efficiently steal the information stored in the system
Simultaneous updates (e.g., P2P)	Updates spread viruses in chores with the extended capability module downloaded from the C&C server.	Equips the viruses spread in the system with capability of carrying out an effective attack.
Information gathering via USB	Spreads to a closed system via a USB stick and collects information stored in the closed system. When the USB stick is switched to the open system, the collected information is uploaded to the C&C server. Instructions and additional features from the C&C server are passed to the closed system via the USB stick.	In order to carry out an attack such as collecting information from the closed system, a virus is embedded into the USB stick.

[Example of how http backdoor communication takes place]

Figure 3-2-2 shows an example of "http backdoor communication" on a system.

Http backdoor refers to backdoor communication by a virus that uses a protocol and an access route that are used by system terminals to access websites on the Internet. Since this communication looks the same as the one used for accessing a legitimate website, it is not detected by IDS. Thought this backdoor, the virus receives instructions and downloads advanced features from the C&C server, and transfers obtained information to the C&C server.

On this occasion, the access route actually taken is the same as the one for accessing websites in business operation. If the organization can block the http backdoor communication by the virus at any point on the route, it can prevent "the organization's information from being stolen".

Measures described in Chapter 4 are based on the concept of "not allowing the virus to steal the organization's information" even if it gets into the organization. For this, we look at design-based measure approaches, including designing an access route on the system based on the characteristics of http backdoor communication.



Figure 3-2-2: Access Flow of Http Backdoor Communication (in case of HTTP Protocol or Similar Protocols that uses a Proxy)

3.3 Types of backdoor communication (according to research in 2011)

One technical aspect in common to attacks is the use of backdoor communication. Here, we introduce some modes of backdoor communication employed. Although you may intend to take measures against backdoor communication, your approach will vary depending on the mode of communication used. The following statistics are from 50 samples of viruses in e-mail attachments assumed to be part of targeted attacks, as collected by Trend Micro between April and October 2011.



Figure 3-3-1: Types of communication by viruses

No single means of defense can guard against each mode of communication. Measures for each mode are introduced in sections 4.4 and 4.5.

4. Points to Counter New Threats

4.1 Considering with Fresh Measure Concept

For an attack that cannot be prevented with conventional measure approaches (as discussed in Chapter 3), how should organizations be prepared for? Organizations will need to change their way of thinking about measures.

Key points for new measure concept to counter new threats are as follows:

Point 1: Mull Measures to Avoid Serious Damage to the Organization Point 2: Mull Measures that Place an Emphasis on the "Exit" Point 3: System Designer and Person(s) in Charge of Security should Collaborate in Mulling those Measures

Details of each point are as follows:

[Point 1: Mull Measures to Avoid Serious Damage to the Organization]

True nature of damage to an organization would be "critical information being stolen" or "availability of a critical system being hampered" and not just the invasion of a virus, so the most important issue is whether the organization can avoid a conclusive damage.

If the organization could block the flow which would otherwise lead to a conclusive damage, it should be able to avoid such conclusive damage. In other words, by choking off the flow of this attack, beginning with the entry of a virus and followed by the spread of infection, communications with an external party through a backdoor, enhancement or transformation of the virus, invasion to the deep part of the system, and information-stealing and system destruction, organization can minimize damage. To realize this, organizations need to defend as much as possible against direct attacks from outside and should they fail to defend, to block communications with outsiders (i.e., "Outbound Measures"). Figure 4-1-1 shows the overall concept.



Figure 4-1-1: Measures to Avoid Serious Damages to an Organization

[Point 2: Mull Measures that Place an Emphasis on the "Exist"]

Given that this type of attack cannot be prevented with conventional measures that focus on "inbound" (i.e., not allowing threats to get into the organization), let's think about how organizations can "prevent their information from being stolen at the outbound in case a threat gets in."

Figure 4-1-2 shows the model of "Advanced Persistent Threats". After circumventing conventional measures and getting into the system, the virus establishes a backdoor, performs communications with an outside party through the backdoor, gets deeper into the system via the internal network, all of which are primary functions of "common attack specifications". Devising "Outbound Measures" to block outbound communications should lead to the establishment of common measures that are applied to individual cases involving "Advanced Persistent Threats".



Figure 4-1-2: Model of "Advanced Persistent Threats" and Concept of Measures

[Point 3: System Designer and Person(s) in Charge of Security Should Collaborate in Mulling those Measures]

In system development, project managers (PMs) are responsible for designing and building the system. They are required to consider in a comprehensive manner the balance of overall features (including security feature and service feature), user needs and required costs, and then proceed with the project. As shown in Figure 4-1-3, during the system development, persons in charge of cyber security (e.g., threat analyst) and persons in charge of the product are placed under a PM.

In the conventional security measures, organizations would just deploy a vendor product within their systems, so PMs often had no clear idea about cyber security. On the other hand, threat analysts who were in charge of cyber security had no full picture of the systems that needed to be protected from attacks like "Advanced Persistent Threats" that target the core of the system.

By mutually understanding their missing points, PMs and threat analysts would be able to devise measures with fresh idea against an attack deemed un-defendable in the past. An effective way to cope with "Advanced Persistent Threats" is to design systems and networks with such attack in mind, rather than just deploying a security product.

Organic collaboration among PMS, threat analysts and vendors should facilitate the finding of the optimum solution to avoid a conclusive damage to the organization.



Figure 4-1-3: System-Wide Security Measure System

Measures taken in the past were based on the design concept of "not allowing a threat to get in (defense at the border)"; emphasis was placed on "Inbound Measures". Despite these measures being taken adequately, "Advanced Persistent Threats" is able to circumvent such measures and get into the depth of a system. Figure 4-2-1 shows a conceptual diagram that covers this issue.

There are several reasons for "Advanced Persistent Threats" to be able to circumvent conventional measures, including exploiting vulnerabilities for which no patch is available; using a seemingly-normal communication so that it is not detected with conventional detection techniques and that no trace is left in logs; and getting into a system after confirming that it is not detected with the antivirus software installed.

To address issues like these, what approaches should be taken by those responsible for information systems' design and development or operation and maintenance.

Even if a threat gets into the depth of a system, organizations need to thwart its objective (information leeks or destruction) and avoid a conclusive damage. This means, devising measures based on the concept of "preventing damages even if a threat gets in" and the measures derived from this concept are "Outbound Measures". To realize this, organizations need to prevent the virus that succeeded in incursion from increasing its activities and to block backdoor communication instructing the virus to advance to the depth of the system, so that they can avoid a conclusive damage (their information being stolen or destroyed).

When establishing "Outbound Measures" like these, organizations need to consider them from the aspect of system network flow design. So the concept of "Outbound Measures" is, defending with design-based measure approaches.



Figure 4-2-1: Limits of Conventional Design-Based Measures and Positioning of "Outbound Measures"

Figure 4-2-2 shows a full picture of "Inbound Measures" and "Outbound Measures". "Advanced Persistent Threats" circumvents "Inbound Measures" and gets inside the system. Subsequent activities include instructing the virus, through the backdoor communication, to enhance its capability, access the target server and steal the target information, or destroy the system. So

"Outbound Measures" are what blocks this backdoor communication which is the core of those activities. In Section 4.3, we delve into "Outbound Measures".



_Figure 4-2-2: Category List for "Inbound Measures (Conventional Measures)" and "Outbound Measures"

This section shows how to realize "Outbound Measures" derived from the approaches described in the previous sections. With effectiveness and feasibility in mind, we set the following design requirements for "Outbound Measures".

- •From the analysis results of the attack flow, select and use necessary information for the system's measure design.
- •Design in a way that emphasis is placed on "Outbound Measures" to prevent conclusive damages
- •Based on the behavioral flow of the common attack techniques applied, adopt measures proven to be effective as "Outbound Measures"
- Design network topology based on the communication character of the attack

(1) Approaches for establishing "Outbound Measures"

In creating this guide, IPA's working group for threats and measures took the approach below. Figure 4-3-1 shows a full picture of that approach. In this approach, the WG analyzed real cases (incidents) and came up with five types of threats and five common threat patterns. The identified five common threat patterns are what need to be addressed. These points are outlined below.

- Real attack cases analyzed The WG collected data on "Advanced Persistent Threats" that circumvented conventional "Inbound Measures" and got into the system and analyzed it.
- (2) Threats categorized Through the analysis of real attack cases, the WG identified five types of threats.
- (3) Five common threat patterns identified
- Based on the virus analysis information, the WG analyzed common attack behavior specification, extracted five common behavioral patterns and defined them as the threats to be addressed.
- (4) "Outbound Measures" established

The WG established measures against the five common threat patterns. Considerations taken at this stage were as follows:

•Examining required design-based measures based on the network flow in the system design drawing

• Adopting substantial, low-cost measures, ideally realized by just changing the settings of existing network-related equipment.

(5) Test phase

The WG used the five common threat patterns, which are addressed in the system design, as confirmation items for the examination. During the examination, designed measures against the five common threat patterns were confirmed.

WG analysis of what common behavioral features of APTs can be addressed in system design led to the identification of the following six common threat patterns.

Common threat pattern 1: Using an HTTP backdoor (protocol: HTTP; no proxy used) Common threat pattern 2: Using an HTTP backdoor (protocol: original; no proxy used) Common threat pattern 3: Using an HTTP backdoor (protocol: HTTP; proxy used) Common threat pattern 4: RAT communication (RAT backdoor communication using CONNECT commands to an internal proxy) Common threat pattern 5: Probing in the system Common threat pattern 6: Spread of infection in the system, updating functions

These six common threat patterns from a design perspective form the basis for recommended outbound measures. Taking this approach in system design offers the following benefits. Although analyzing each incident to determine relevant measures in system design would require significant work, design and testing can be incorporated into routine production workflows by defining the common behavioral features of APTs (derived from common technical aspects of attacks) as threats subject to security measures. In the testing phase, these common behavioral features of APTs (which were defined as threats to address in system design) are used to test the effectiveness of corresponding security measures taken in system design.



Figure 4-3-1: Full Picture of Approach for Establishing "Outbound Measures"

(2) Eight "Outbound Measures"

Based on the approaches described in the previous section, the WG traced the six common threat patterns on a standard system's design drawing and derived eight "Outbound Measures". Figure 4-3-2 shows common behavioral features of APTs and eight corresponding outbound measures. The eight outbound measures are listed below. Implementing these eight security measures in system design will help ensure that even if threats infiltrate deep into the system, your organization can block communication with the remote attack server to avoid substantial damage.

Measure 1 and 2: Detect and block http backdoor Measure 3: Detect and block CONNECT method through proxy by RAT Measure 4: Prevent the establishment of http backdoor in the server segment Measure 5: Protect servers that may be subject to serious attacks Measure 6: Prevent the internal diffusion of the virus, Measure 7: Monitor the internal diffusion Measure 8: Prevent the functional update via P2P after the internal diffusion within a local segment When planning system design based on this guide, take into account your network structure and your communication equipment.

For the design and implementation of six design-based measures, in general, multiple work teams collaborate and proceed with design under the direction of project manager. Concerned teams may need to meet regularly to ensure appropriate implementation of those measures. It is important that concerned teams have the same design cognition and work with design. Concerned teams include, for example:

Network design team	Designs topology and line performance, etc.			
Security design team	Designs firewall rules and ACL (Access Control List), etc.			
Business flow design	Designs business applications and business data flow, etc.			
team				
Operational	Takes care of operation and maintenance COTS (Commercial off			
infrastructure design	the Shelf), designs operation logs, etc.			
team				
Operational design	Designs successive/daily/monthly operation (how and what to			
team	audit), etc.			

This section and "Appendix 2: Measure Requirement Definition Templates" are also intended as a tool for ensuring a shared awareness of system design among various teams.



Figure 4-3-2: Association Chart for Six Common Threat Patterns and Eight "Outbound Measures"

This section explores how effective the recommended measures may be against backdoor communication as discussed in Section 3.3. Figure 4-4-1 shows the modes of communication used by viruses described in Section 3.3.



Figure 4-4-1: Types of communication by viruses

Of these, virus communication via an original TCP-based protocol or HTTP (incompatible with proxies) can be blocked by measures in **Implementation Item 1 in Section 4.5 below, which can prevent some 46% of attacks**. Moreover, implementing this measure is **also effective in alerting you in case your organization is attacked.** Because measures for Implementation Item 1 do not require extensive revision of network design, they can be implemented immediately.

On the other hand, blocking virus communication via HTTP (compatible with proxies) and HTTPS does present some issues. Measures against HTTP (compatible with proxies) are described in Section 4.5, Implementation Item 2, and measures against RAT communication (defined later in Section 4.5, Implementation Item 3) are described in Implementation Item 3. Effectiveness of these approaches will depend on your verification and testing. Meanwhile, a growing proportion of virus communication is conducted via HTTPS, and effective measures against these methods of backdoor communication must be found. Ongoing study is underway by the IPA's working group for threats and measures.

4.5 Eight Measures to Prevent Critical Information from Being Stolen by Cyber Attacks

This section describes how to implement security measures that address the six common threat patterns discussed up to Section 4.4, beginning with an overview of measures against backdoor communication and continuing with descriptions of each implementation item.

[Interrelationship of implementation items 1–3, against backdoor communication]

Implementation Items 1–3 are measures against of backdoor virus communication 1-4, in the context of the six common threat patterns. These measures against backdoor communication are illustrated in Figures 4-5-1 and 4-5-2.

Implementation Item 1 blocks communication that uses an original protocol and, of the various types of HTTP traffic, communication that does not pass through an internal proxy. Consider using Implementation Item 2 to block HTTP-based communication via an internal proxy, and Implementation Item 3 to block RAT communication.



Figure 4-5-1: Measures against backdoor virus communication (overview)

Types of Backdoor Virus Communication Specifications				System de communic	sign-based measur ations	es Me	leasures against HTTP backdoor				
Threat	Has a proven	Internal proxy	Type of communication Protocol		Type of communication Protocol			Block	point		Measure (1) Design service communication path
pattern	track record?	used/unused	Port	Protocol		A	B	Log	Measure (2)		
Pattern 1	Yes	Unused	8080tcp	HTTP (GET,POST) Proprietary protocol HTTP (GET,POST)		Nopass	FW rule	FW	Design a function to detect a HTTP communication that models on		
Pattern 2	Yes	Unused	8080tcp			No pass	FW rule	FW	browser communication patters		
Pattern 3	Yes	Used	8080tcp			Pass	Pass	?	HTTP backdoor block feature		
Pattern 4	Yes	Used 8080tcp Proprietary RAT protocol (CONNECT)				Some pass	Pass	?	RAT communication blocking		
Measure (3) Detect and block RAT communication with an internal proxy (CONNECT connection)											
"Advanced Persistent Threats (APTs)" backdoor virus communication types and system design-based measure Information being stolen											

Figure 4-5-2: Measures against backdoor virus communication (details)



Figure 4-5-1-1: Example using Implementation Item 1: Design service communication paths

This measure is intended to block backdoor communication with remote C&C servers, based on characteristics of viruses that do not follow design rules for communication paths.

Of the six common threat patterns, the measure targets both communication based on original protocols that does not pass through an intermediate proxy and HTTP communication without an intermediate proxy.

Measures to implement for the communication path

1-1 م

Design firewall blocking rules for outgoing traffic (to be implemented with guideline 1-2)

Apply the following rules, accounting for characteristics of virus communication (that is, communication using an original protocol without an intermediate proxy and HTTP communication without an intermediate proxy).

(1) Configure firewall to permit only outbound communication via an internal proxy (application G/W) and block any direct communications from a computer that does not use proxy.

Design in a way that the services in the table below that use 80,443 are routed through an internal proxy (except functional units deployed on DMZ).

Example of feature	Communication application			
Windows Server Update Services	Communicates with the Windows Update Server (80,443)			
(WSUS)				
System Center Configuration	Updates non-MS products, performs resource			
Manager(SCCM)	management			
IDS/IPS	Updates signatures			
Antivirus software-related	Updates pattern files			
Quarantine-related	Obtains up-to-date patches and pattern file information			
Spam mail filter	Updates blacklist			
Others	License authentication			

[Precaution]

For software programs whose online updates are not possible via proxy, arrange a shared file server so that updates are performed via this server. Secure updating must be investigated. For example, on a secure computer, system administrators can use a network connection separate from the internal network to obtain the files to upload for software updates, and then upload the files to a shared file server.

(2) Treat any external communication received from computers on port 80 that does not pass through an internal proxy as potential backdoor communication with a C&C server.

1-2 — A second state of the secon

Analyze firewall blocking log, check for backdoor communication by the virus, and identify infected computers. Log retention period should be estimated based on the timing of backdoor communication activities (sleep or keep alive) by the virus.

■ Flow of communication after communication path design measures are taken (example)



Figure 4-5-1-2: Flow of communication following "Measure 1: Design service communication paths"

The blocked communication is logged as follows. In this way, monitoring logs enables organizations to determine if computers are infected with a virus.



Figure 4-5-1-3: Flow of communication following "Measure 1: Design service communication paths"

[Implementation item 2: Design a function to detect a HTTP communication that models on browser communication patters]

Example of Communication Path Design



This measure is intended to block backdoor communication with remote C&C servers by viruses adapted to the organization's communication path design that communicate as browsers do (by using HTTP methods such as GET, POST, and CONNECT).

Of the six common threat patterns, the measure targets HTTP communication via a proxy.

Measures to implement for the communication path



This measure draws on the ability of browsers to react to HTTP responses in ways that viruses cannot. Prepare the system proxy to redirect other parties using JavaScript or META tags, and use the other party's reaction to distinguish between backdoor virus communication and browser communication. This measure must be implemented on the system proxy.

The measure is focused on the following characteristics of backdoor virus communication.

✓ Virus response to communication is not for the sake of webpage display.

2-2 -

- ✓ Viruses cannot follow redirection implemented with JavaScript or META tags.
- ✓ By preparing the system proxy to redirect other parties using JavaScript or META tags, you can use the other party's reaction to distinguish between backdoor virus communication and browser communication.

Browser communication when this approach is taken is shown in the communication flow of Figure 4-4-3. Because viruses cannot follow the redirect request in step (2), virus communication is blocked.

• Based on the communication character, including the HTTP header specific to the virus, identify backdoor communications *[Note] After the completion of examination and verifications of these technologies, revisions will be made to the description here with additional information.

This is a design-based security measure that draws on differences between backdoor communication via HTTP and legitimate browser communication. For example, because browser header information differs from that of viruses, the difference can be used in defense.

The measure is focused on the following characteristics of backdoor virus communication.

- ✓ Structurally, headers in virus backdoor communication are sometimes simpler than browser headers.
- ✓ Virus headers are not browser-dependent. Instead, they rely on virus communication specifications.
- ✓ Some patterns of communication exist between viruses and C&C servers, such as cyclical communication involving keep-alive commands and executable downloading.
- ✓ The User-Agent in virus HTTP header extensions often differs from that of browsers.

The simplicity of headers in virus backdoor communication is shown in the following example. In contrast, Figure 4-5-2-2 shows header information in communication with Internet Explorer 8.

GET
/CIS/55/000/000/016/481.swf?fd=jp.msn.com&clickTAG=http%3A//g.msn.com/2AD0004N/130000000044826.1%3F%3FPID%3D8722904
%26amp%3BUIT%3DM%26amp%3BTargetID%3D10666778%26amp%3BAN%3D52560302%26amp%3BPG%3DJHP201%26amp%3BASID%3
D2e312bb00ae2479da4bc97db458b894a&clickTag=http%3A//g.msn.com/2AD0004N/1300000000044826.1%3F%3FPID%3D8722904%26amp
% 3BUIT% 3DM% 26 amp% 3BTargetID% 3D10666778% 26 amp% 3BAN% 3D52560302% 26 amp% 3BPG% 3DJHP 201% 26 amp% 3BASID% 3D 22 amp% 3D 22 amp% 3BASID% 3D 22 amp% 3D 22 amp% 3BASID% 3D 22 amp% 3D 22 amp% 3BASID% 3D 22 amp% 3D 22 amp% 3BASID% 3D 22 amp% 3D 22 amp% 3BASID% 3D 22 amp% 3D 3D 22 amp% 3D 22
b00ae2479da4bc97db458b894a HTTP/1.1
Accept: */*
Accept-Language: ja-JP
Referer: http://jp.msn.com/?ocid=iefvrtx-flash-version: 10,3,181,14
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; .NET4.0C; .NET4.0E; .NET CLR 1.1.4322; .NET CLR
2.0.50727; .NET CLR 3.0.04506.30; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: a.ads2.msads.net
Connection: Keep-Alive

Figure 4-5-2-2: Example of Internet Explorer 8 request header information

Headers in browser communication contain multiple items of information. On the other hand, headers in virus communication are simple, as shown in Figure 4-5-2-3.

Virus	s example 1
GET http:// OsJh¥ Host: Pragr	/login.51edm.net/getconf.php?m=f9c46f1f7ed5073091dd2a196cde7761&q=FamWNHTEDv¥dSvfKy=8qRnyry9fqylyqyv0qlwZqc9uqCv0a8aT ⁄eywfaFXQvsJha8p4MsJfaDelHsJZKyxtWlvfOSXIOyO55 HTTP/1.1 login.51edm.net <mark>na</mark> : no-cache
Virus	s example 2
GET http:// Host:	/pds.adncommerce.com/jmoy.php?npic= HTTP/1.1 pds.adncommerce.com

Figure 4-5-2-3: Example of the request header information of a virus

As a way to enact measures based on these characteristics, the following techniques are under review.

- White-list HTTP header's legitimate User-Agent
- Register the character of keep-alive communications between the backdoor virus and the C&C server
- Check for an unnatural HTTP response data size
- Identify dynamical characteristic (e.g., the C&C server having multiple access points)
- Check the length of HTTP headers for abnormality

[Implementation Item 3: Design a means to detect and block communication between RATs and internal proxies (CONNECT connections)]

Example of Communication Path Design



Figure 4-5-3-1: Example of monitoring for CONNECT communication via an internal proxy

Measures to implement for the communication path

This measure is intended as a means of detection and blocking that draws on characteristics of RAT communication, which is established by sending a CONNECT method to an internal proxy, enabling remote communication that follows network design rules and bypasses the firewall via the internal proxy on port 8080, forming a TCP connection tunnel.

Of the six common threat patterns, the measure targets RAT communication.

• Block Ivy connection attempts by designing the network to accept only certain port numbers [**] in CONNECT 172.16.0.210[**] commands for internal proxies

This measure blocks communication straying from a rule that would violate rules when the RAT attempts to access other computers. For example, security design measures allowing only TCP traffic on port 443 will block communication attempts using CONNECT 172.16.0.210:3460, as used by the default setting of Poison Ivy.

3-2 —

Because Ivy communication leaves the log record described below, monitor the proxy log for lines that include the string CONNECT in communication other than TCP traffic on port 443. (Specifically: grep CONNECT access_log | grep -v :443.)

As for other measures against RAT communication, study is underway by the IPA's working group for threats and measures that focuses both on the persistent nature of RAT (Poison Ivy) sessions and system design details that include dedicated equipment, for example.

Technical features of RATs and characteristics of communication (example: Poison lvy)

· RATs (remote access trojans/remote administration tools) defined

- RATs may give attackers tools with the following functions and characteristics.
- ✓ Remote control of compromised systems. Used for covert activities and espionage.
- ✓ Establishing a communication environment for remote connections that bypass firewalls.
- ✓ Original protocol, enabling communication over HTTP proxy (using CONNECT methods) and over SOCKS (v4).
- ✓ Common RATs: Poison Ivy, Gh0st RAT, and so on. Some of these tools are now widely available.
- Increasingly, in targeted attacks (Advanced Persistent Threats), these tools are disguised as regular e-mail attachments.
- ✓ RATs enable attackers to do the following remotely. As a result, infected computers can be used to search and attack the system.

File and folder operations, process operations, command execution, screen capture, relaying/updating, and so on

· RAT intrusion methods

Attackers break through inbound security measures by using targeted e-mail with virus attachments, for incursion to the computers of general users inside the system, which are targeted by the attack.



Figure 4-5-3-2: RAT (Poison Ivy) intrusion

■ Testing detection and blocking of RAT communication with an internal proxy (CONNECT connection)

Test Details

In an environment simulating the network topology of an information system, a test of detection and blocking was conducted to verify Poison Ivy (RAT) capabilities and TCP tunneling using the CONNECT method with the RAT. Communication data and communication logs of the internal proxy were obtained.



Figure 4-5-3-3: Environment to test detection and blocking of RAT-based internal proxy communication

(CONNECT connection)

Characteristics of Poison Ivy communication

① Any original protocol can be used as the Poison Ivy protocol. (Default: A CONNECT method is sent via proxy over TCP on port 3460 to open a tunnel.)



- ② Once the Ivy host has been created, the following settings and operation are possible:
 - Explicit designation of the proxy
 - Spying on proxy setting values configured in the system (here, proxy setting values configured in IE are used)
 - Although by default, the listener port on the administrative host is for TCP traffic on port 3460, any listener port can be designated when preparing the lvy virus.
- ③ Ivy does not use SSL (measures against HTTPS backdoor communication (CONNECT connections) must be investigated separately from this test)
 - Ivy: An original protocol is used over TCP connections established with a CONNECT method
 - HTTPS: SSL + HTTP protocols are used over TCP connections established with a CONNECT method
- ④ Ivy communication is encrypted, using shared-key encryption

Results of detection and blocking test

Conclusions from the test of detection and blocking are as follows.

- ① Because Ivy opens a tunnel with the internal proxy using a CONNECT method and communication follows network design rules, a perfect way to block it is difficult using proxy and firewall rule settings alone. However, the virus may be discovered due to characteristics of Ivy communication.
- (2) Ivy sessions are persistent, and proxy log records are only produced after the CONNECT session is terminated.
- ③ Proxy logs are only recorded for CONNECT sessions (as long as header logging is not specified).

172.16.0.35 - - [17/Nov/2011:16:22:52 +0900] "CONNECT 172.16.0.210:3460 HTTP/1.0" 200

④ In the case of Ivy, for CONNECT methods, no HTTP header (for example, User-Agent) whatsoever is included. Thus, communication requests established with CONNECT consist only of the CONNECT line. (This characteristic only applies to Ivy.)

Ivy: CONNECT 172.16.0.210: 3460 HTTP/1.0 IE or other browsers: CONNECT 172.16.0.210: 3460 HTTP/1.0 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1 Proxy-Connection: proxy-keeepalive

(5) When the default Ivy port (TCP traffic on port 3460) is used, network design can be adopted that restricts the port number [**] designated in CONNECT 172.16.0.210[**] commands for the proxy to block attacks.

All CONNECT attempts to ports other than 443 are denied. Measures involving a change of the listener port for administrative hosts from the default port of 3460 are also possible.

Example with default Squid settings

[All CONNECT methods for ports other than 443 (specified in SSL_ports) are denied] acl SSL_ports port 443 acl CONNECT method CONNECT http_access deny CONNECT!SSL_ports

(6) Proxy logs can be analyzed to monitor for Ivy communication. Because Ivy communication leaves the log record described below, monitor the proxy log for lines that include the string CONNECT in communication other than TCP traffic on port 443.

CONNECT 172.16.0.210:3460 J (grep CONNECT access_log | grep -v :443)

[Implementation item 4: Avoid a direct internet connection from the most important section]

Example of Communication Path Design



Figure 4-5-4-1: Design measures to ensure separation and avoid direct Internet connections from critical servers

This measure is intended to prevent backdoors in critical network areas. Of the six common threat patterns, the measure targets searching for information stored in the system. Implement this measure in conjunction with "Implementation Item 8: Limit the range of access by P2P."

Measures to implement for the communication path

Separate critical servers from direct Internet access by using a VLAN

Avoid direct Internet connections from the most important areas of the network (critical servers) for ordinary services (HTTP, SSL, and so on) by routing these services through a VLAN, for example, to maintain separation, as protection against control sequences from remote attack servers.

For example, besides implementing the separate structure mentioned, consider the following approaches in system design.

- ✓ Use a VLAN or other means to separate network segments, to prevent direct Internet access from critical servers.
- ✓ Limit information retrieval from critical servers to users in the administrative segment.
- ✓ Use the administrative segment for Internet access.

[Implementation Item 5: Protect servers that may be subject to serious attacks]

This measure is intended to protect critical servers that may be targeted in attacks. Of the six common threat patterns, the measure is focused on searching for information stored in the system. Often in Advanced Persistent Threats, computers for general use or administration are attacked, after which espionage is conducted on information at the organization to determine what to target next. Thus, central authentication servers that store information at the organization (such as all internal e-mail addresses, authentication information, and so on) may be targeted in attacks. These servers should therefore be positioned as critical equipment, and protective design measures taken. The same measures should be taken for any replica servers for the authentication servers.

Implement this measure in conjunction with Implementation Items 4 and 8 ("Avoid a direct internet connection from the most important section" and "Limit the range of access by P2P," respectively).

Measures to implement for the communication path







administrative segment

This measure can be implemented immediately. However, the measure is of limited effectiveness against authentication server access via backdoor remote control from computers for general use and administration.

a. Protection of the administrative segment, used to manage authentication servers (servers for Active Directory, Notes, and so on)

Take the following kinds of measures for the segment used to manage authentication servers.

- (a) Do not open ports to segments other than the administrative segment. (Allow communication from the administrative segment.)
- (b) Treat vulnerability patching of administrative computers as a priority.
- **b.** Protection of authentication servers (servers for Active Directory, Notes, and so on) Take the following kinds of measures for the authentication server segment.
 - (a) Design access control to restrict authentication server login to users on administrative computers.
 - (b) Take measures to prevent attacks from computers of general users to crack administrative passwords for authentication servers (such as dictionary attacks).

Ex: Set a retry limit for consecutive attempts to log in to authentication servers.

Reference: Recommended Microsoft settings for an Active Directory account lockout policy# Setting values should be adjusted to suit overall system design and your business.• Lockout period15 minutes• Account lockout threshold10 failed logon attempts

Lockout count reset
 15 minutes

5-2·

(c) Treat vulnerability patching of authentication servers that provide services to computers of general users as a priority.

Measures to consider when replacing equipment, or at similar junctures



Figure 4-5-5-2: Design measures to protect the authentication server segment and authentication server

administrative segment

a. Consider requiring authentication for LDAP access from the user segment (general users).

(However, some business adjustments would be required.)

b. Deploy smart cards for PKI authentication between administrator computers and critical servers (including Active Directory servers), and have administrators only insert the smart cards during access.

(This measure prevents Active Directory login caused by viruses.)

■ Reference: Other approaches to design (requires investigation)

Position a reference LDAP server that replicates only the required information of authentication servers (in the critical segment) in the business server segment accessible to general users. This

system design blocks access from general users to critical segments, as an approach that denies general access to critical segments. However, relevant considerations include authentication server functionality other than LDAP functions (that is, user authentication) and determination of non-essential user information. Thus, careful verification is required if this approach is investigated, keeping in mind consistency with overall system design.

Although it would not be effective in preventing attackers from spying on organization information and e-mail addresses, this approach would help restrict access to critical server segments from general user segments, which are relatively easier to infiltrate in targeted attacks.



Figure 4-5-5-3: Design measures to deny access to critical segments from general computers

Reference: Considerations in network topology design where Active Directory is

used

In Active Directory network design, currently the following issues should be considered.

- ① Because critical servers require access to Active Directory data, Active Directory must be located in the critical server segment.
- (2) Because Active Directory provides services directly to users, designing access for general users via the business server segment would be difficult.
- ③ For optimal security, it would be desirable to deny all access from general user segments to critical server segments. However, because the Active Directory must be located in the critical server segment, access from the general user segment cannot be denied. This poses a risk to other critical servers.
- When restricting the ports allowing access to critical server segments from general user segments, you must know all the ports used for business applications and for Active Directory services, but there may be many "black boxes" with an unknown purpose.
- (5) Regarding access control design that routes access from general user segments to Active Directory (in the critical server segment) via Exchange or other business servers (or segments), this design must be reviewed for feasibility and in view of overall system design.

Main Active Directory services

- Directory services (LDAP)
- Client management (SMB file sharing)
- User authentication (Kerberos)
- MAPI (messaging API, using RPC over TCP (when Exchange Server is used))



Figure 4-5-6-1: Design measures to separate administrative from general LANs

This measure is intended to minimize the spread of viruses and enable detection. Of the six common threat patterns, the measure supports virus containment in compromised systems.

Measures to implement for the communication path

, 6-1

Separate network segments to restrict access from general LANs to administrative LANs, and incorporate features to detect the spread of infection (to be implemented with guideline 6-2)

Taking this measure can help avoid backdoors and prevent infection from spreading from general to administrative LANs. Specifically, a log of any violations of rules designed to separate administrative from the general LANs (by means of a VLAN) is monitored using a Layer 3 Switch, to detect any actual spreading of a virus.

6-2

Design segments and routing to eliminate any unnecessary routing (to be implemented with guideline 6-1)

Required for monitoring with the Layer 3 Switch, as deployed in measures for Implementation Item 6-1. After determining requirements in each segment, eliminate any truly unnecessary routing. Consider each of the following points for the segments when adopting a separate system design.

- Administrative server segment: Because a variety of work is conducted, there is a tendency to open many ports.
- Infrastructure server segment: Only specific ports are needed, and other ports should remain closed.
- Business server segment: Because many departments maintain servers in this segment, administrators may lose track of server usage.
- Load-balancing segment: Consider deploying a segment for this purpose if traffic becomes excessive.



Figure 4-5-7-1: Design measures to monitor traffic

This measure is intended to minimize the spread of viruses and enable detection. Of the six common threat patterns, the measure supports virus containment in compromised systems. Taking this measure will require coordination between a department in charge of network monitoring and a security department.

Measures to implement for the communication path

, 7-1

 Monitor file servers, switches, and similar nodes for unusual increases in traffic or logging

Viruses increase network traffic as packets are sent when they spread across an organization, which places an extra load on servers and routers and may cause increased logging. Network monitoring departments should identify any exceptional loads on servers or routers as a high-priority issue, and security departments should check for infected computers.



Figure 4-5-8-1: Design measures to monitor traffic

This measure is intended to prevent internal threats such as virus updating on infected computers.

Of the six common threat patterns, the measure supports virus containment in compromised systems. Implement this measure in conjunction with Implementation Items 4 and 6 ("Avoid a direct internet connection from the most important section" and "Separate a VLAN network by using switches etc.," respectively).

Measures to implement for the communication path

/ 8-	1					
٠	Network	design	that	removes	unnecessary	RPC
	communic	ations				

Communication by existing viruses in a compromised network may include update instructions. To reduce the threat of update instructions spreading across the system, you should understand the following characteristics of this communication.

Functions are updated and information is collected via P2P.

One example of this communication is the use of MS-RPC by Stuxnet.

P2P was chosen as the protocol to enable viruses on infected computers to update their functions and collect information even in segments that deny HTTP connections from inside the system.

Viruses updated this way in server segments are especially difficult to detect and remove.



Appendix 1: Results from Testing Implementation Items

This section of the appendix explores the technical feasibility of Implementation Item 2-2 ("Based on the communication character, including the HTTP header specific to the virus, identify the backdoor communications") in Section 4.5. The common threat pattern addressed by these measures cannot be addressed by measures for Implementation Item 1 ("Design service communication path"), because HTTP backdoor communication between the attack (C&C) server and virus follows communication path design and uses the same HTTP methods as browsers do.

Characteristics of virus communication were determined through virus analysis, and then techniques to detect and block HTTP backdoor communication as used by real viruses were investigated on computers. Additionally, methods of detecting RAT-based backdoor communication between an attack server and compromised system were also investigated.

These results were obtained using products of Trend Micro and IBM Japan. Three types of investigation were conducted.

No.	Details	Supported By
1	Detection of User-Agent in the virus HTTP header	Trend Micro
	(Tested by implementing rule-based detection)	
2	Detection of original virus HTTP header extensions (Tested by	-
	implementing IDS and IPS measures)	
3	Approach focusing on the length of HTTP headers sent by viruses	IBM Japan

Appended Table 1-1: Test details

Testing Example 1: Detection of User-Agent in the virus HTTP header (tested after implementing rule-based detection)

Detection is focused on the following characteristics: The User-Agent in virus HTTP header extensions often differs from that of browsers.

[Detection Technique]

User-Agent strings for legitimate communication (as used by browsers, for example) are whitelisted, forming the basis to compare other strings to detect "bad" User-Agent strings used by viruses.





Testing Example 2: Detection of original virus HTTP header extensions (tested after implementing IDS and IPS)

Detection is focused on the following characteristics: The User-Agent in virus HTTP header extensions often differs from that of browsers.

[Detection Technique]

HTTP header extensions of browsers or other HTTP applications are parsed to create a whitelist of legitimate headers. A list of HTTP header extensions used by viruses is also maintained. The HTTP header extensions in HTTP packets are examined to determine if they are on the lists. Although these lists are not provided as a standard feature of typical IDS or IPS solutions, custom signatures can be created to support detection. If real-time performance is not critical, logs can be analyzed using the sensor management console for detection.

HTTP Header

Summary of scanning process for HTTP header extensions



Testing Example 2:

Detection of original virus HTTP header extensions (tested after implementing IDS and IPS) - continued

[Test Results and Observations]

- (1) Preliminary Bayesian analysis of specified methods of browsers used in the system or HTTP-based applications may enable creation of whitelists that are very precise for the system involved. There is a need to study detection techniques utilizing IDS management consoles working with these whitelists.
- (2) Keep in mind that some applications use original HTTP header extensions. Analyzing applications used in your system beforehand can improve detection precision to a certain extent.
- (3) As mentioned, HTTP communication on port 80 for a variety of purposes is a requirement of many IT product specifications, some of which are undisclosed. This consideration, and the fact that User-Agent strings may change with each product update or security patch, makes it difficult to maintain whitelists.
- (4) The User-Agent whitelist technique should be viewed as an approach that limits the chance of APT attacks to some extent.
- (5) When you plan system design, investigating the ports, protocols, and other working details of applications used in the system will be an important step in understanding potential system vulnerabilities to cyber attacks.

Testing Example 3: Approach focusing on the length of HTTP headers sent by viruses

Detection is focused on the following characteristics: Structurally, headers in virus HTTP backdoor communication are sometimes designed for convenience and are simpler than Internet Explorer headers.
[Detection Technique] Drawing on the fact that HTTP headers in backdoor communication are generally short, set up an IDS to detect headers shorter than a threshold level.
العيار
Having the IDS detect this kind of communication simply because the headers are short may cause some concerns regarding false positives. Efficacy must be investigated.
 [Test Results and Observations] (1) Preliminary steps before testing Ensure that headers of an appropriate length can be detected using IDS custom signature. Investigate the header length of specific partians of headers used by common browsers and HTTP-based applications
Also investigate relevant HTTP header length of several dozen samples of backdoor viruses.
Determine a guideline threshold level that can be used to identify backdoor communication of viruses.
 Assuming browser use in a desktop environment, discriminating between lengths of specific portions of HTTP headers enables detection of backdoor communication.
(3) Issues determined from testing on computers
HTTP communication from user agents other than browsers may generate false positives.
 (4) For this technique to be effective in detecting backdoor communication, a whitelist based on IP addresses or URLs and HTTP headers must be prepared from a preliminary investigation of HTTP-based applications.
[Proceutions]
In principle, detection is not possible for backdoor communication in which the header is spoofed and appears to be an



Test results screen: detection of the length of an HTTP header sent by a virus

ordinary browser header. Thus, other measures must also be taken.

Appendix 2: Measure Requirement Definition Templates

This appendix provides points for tailoring implementation design items 1–8 that are described in Section 4.5 "Eight Measures to Prevent Critical Information from Being Stolen by Cyber Attacks'", based on the organization's system's network topology and communication devices and other environmental elements. This appendix is intended to serve as a guideline for incorporating tasks required for implementation design into each work item of Work Breakdown Structure (WBS).

This appendix assumes the following general work items that cover requirement definition to implementation design.

(1) Flow of Measure Requirement Definition

- (2) Considering Measures against Six Common Threat Patterns
- (3) Considerations in each phase
- (4) Consider work items for each phase (anti-threat measures WBS)

In addition, examples of work items and deliverables for each phase are included. By referring to them, proceed with implementation design based on the characteristics of your system and project. Phase definition varies depending on the type of contract and the development approach. Based on your own phase definition, tailor the examples given in this appendix.

These templates for defining the requirements of measures were prepared following guidelines in *SLCP-JCF2007* (*Common Framework for Software Lifecycle Process*) for development processes, activities, tasks, and so on. When using the templates, adapt them to your organization's own development standards.

[(1) Flow of Measure Requirement Definition]

In order to implement-design each of the implementation design items 1–8 that are described in this document, organizations need to define measure requirements at an early stage of the project. After defining measure requirements, incorporate them into and implement them for work items in each phase. (This appendix assumes standard development phase to be: [1] Measure requirement definition -> [2] Design -> [3] Manufacturing (implementation) -> [4] Test -> [5] Operation.)

[1] Measure requirement definition				
(A) Clarify the objectives	From a broad point of view, clarify the objectives.			
(B) Classify the types of threats	 By referring to the classified threat types, assess the impact on your organization. 			
(C) Defines common threat patterns	 Taking these six common threat patterns as candidates for consideration, define threat patterns to be addressed. 			
(D) Examine the design policies	Examine where the eight "Outbound Measures" need to be implemented and establish design policies for each location.			
(E) Decide on measure requirements	Based on the cost-effectiveness, make final judgments and decide on measure requirements.			



[3] Manufacturing (implementation) to [5] Operation

Appended Figure 2-1: Flow of Measure Requirement Definition

Appendix table 2-1 shows the flow of measure requirement definition.

Flow of Measure Requirement Definition	Outline of Work	References in this document
(A) Clarify the objectives Wants to prevent espionage Wants to prevent system from being crashed	 When deciding on measure requirements, organizations first need to clarify the objectives from a broad point of view. It is important not to lose sight of the objectives and proceed with implementation design. The figure on the left lists the following two points: Wants to prevent espionage Wants to prevent system from being crashed 	_
 (B) Classify the types of threats 1. Targeted e-mail 2. An attack via websites 3. An attack that destroys control systems 4. A virus that transmits via USB 5. Combined DDoS attack 	 The next step is to assess the impact of each threat type on your organization (Refer to threat type classification in "(2) Considering Measures against Six Common Threat Patterns"). IPA's working group for threats and measures plans to release a revisited edition when a new type of attack emerges. 	Association chart in Section 4.5, "Eight Measures to Prevent Critical Information from Being Stolen by Cyber Attacks"

Appendix table 2-1: Flow of Measure Requirement Definition



Flow of Measure Requirement Definition	Outline of Work	References in this document
Definition (D) Examine the design policies Measure (1) Design service communication paths Measure (2) Design a function to detect a HTTP communication that models on browser communication that models on browser communication patters	 Examine how to realize the defense design against the six common threat patterns. Verification by IPA's working group for threats and measures revealed that the eight "Outbound Measures" shown on the figure on the left are effective in disabling the virus's communication with remote attack server even if it gets into the deep part of the system. (See Section 4.5. "Implementation Items 1–8" in the guide.) Examine where the eight "Outbound Measures" need to be implemented and establish design policies for each location. 	document Details of eight design- based measures (Implementation Items 1–8 and "Example of Implementation of System Design with Design-Based Measures" in Section 4.5)
Measure (3) Plan for detection and blocking of RAT communication through an internal proxy (CONNECT connection) Measure (4) Avoid a direct internet connection from the most important section	 Considerations are as follows: (1) Have on your hand the entire network configuration diagram (outline drawing) that was created in the requirement definition phase. (2) Draw on the entire network configuration diagram the devices that are to be deployed between zones (network segments) (3) By referring to the business requirements created in 	
Measure (5) Protect servers that may be subject to serious attacks Measure (6) Separate a VLAN	 the requirement definition phase, draw the communication paths for the Internet commutation (such as HTTP) and business applications. (4) By referring to Implementation Items 1–8 in Section 4.5, consider how to implement-design "Outbound Measures" on your system 	
network by using switches etc. Measure (7) Monitor the volume overload to detect infections Measure (8) Limit the range of access by P2P	Write down the points on the system configuration diagram, establish shared awareness among development teams (for system infrastructure and business application, etc.), and have each team check for the impact on the section they are in charge of (e.g., business application and communication service)	

(E) Decide on measure requirements	 After going through (A) Clarify the objectives to (E) Prevention measures, estimate the cost for the entire process (i.e., design phase trough assurance test phase), and based on the cost-effectiveness, make final judgments and decide on measure requirements. The key point is to identify what threats exist against those objectives and establish shared awareness of measures between corporate users and Sler. Anti-threat measures are not just making settings and deploying a commercial product. How to monitor/operate in real operation should also be considered. Defending against and preventing the impact of threats depend on system design; do not forget to implement such design. 	Subsection in Section 2.5: "Budgetary considerations for security measures"
---------------------------------------	--	---

[(2) Considering Measures against Five Common Threat Patterns]

Appendix table 2-2 shows considered measures against five common threat patterns.

Threat type classification	The six Common Threat Patterns (CTP)	Outline of measures
 Five types of threats in espionage or system destruction Type 1: Targeted e-mail Type 2: An attack via websites 	CTP 1: Backdoor communication - Backdoor communications that use HTTP protocol - Port80 and proxy not used	 Set firewall outbound communication blocking rules Permit only outbound communication via an internal proxy. Block any direct communications from a computer. Design monitoring/analysis timing and the manner of operation. Excidentials as Massure 1 in Section 4.5.
Type 3: An attack that destroys control systems Type 4: Virus that transmits via USB Type 5: Combined DDoS attack	CTP 2: Backdoor communication - Backdoor communications that use a proprietary communication protocol - Port80 and proxy not used	 Monitor firewall blocking log Analyze firewall blocking log and identify infected computers. Select a log retention device and estimate row data volume If the logs are to be archived and retained, select an appropriate device and check for its storage. Design monitoring/analysis timing and the manner of operation For details, see Measure 1 in Section 4.5.
	CTP 3: Backdoor communication - Backdoor communications that use HTTP method (GET, POST, CONNECT) - Port80 and proxy used	 Redirection by JavaScript or META tags Equip the system proxy with a redirect feature by JavaScript or META tags Based on the communication character, identify backdoor communications Monitor the log to detect unusual communications. Example: Despite the fact that our server is not on the Internet, outbound communications using POST method have been confirmed. Design monitoring/analysis timing and the manner of operation. For details, see Measure 2 in Section 4.5.
	CTP 4: RAT communication - RAT backdoor communications that use CONNECT commands to access an internal proxy - Port8080 and internal proxy used	 Block communication between RATs and internal proxies (CONNECT connections) Monitor proxy logs to detect RAT CONNECT traffic Also investigated dedicated equipment. For details, see Measure 3 in Section 4.5.
 Five types of threats in espionage or system destruction Type 1: Targeted e-mail Type 2: An attack via websites Type 3: An attack that destroys control systems Type 4: Virus that transmits via USB 	CTP 5: - Threat of intra-system information- seeking	 Prevent the establishment of a backdoor in the most important section. Implement zones design (separation by segment) for each sever usage, each user department and administrator. Do not provide direct internet connection environment to the most important server zone. Protect critical servers that may be targeted for searching. For details, see Measure 4 and 5 in Section 4.5. <make 3.="" adjustments="" commensurate="" final="" it="" measure="" so="" that="" with=""></make>
Type 5: Combined DDoS attack	CTP 6: - Threat of backdoor virus's internal diffusion within the system and functional update	 Separate a VLAN network by using switches etc. Implement zones design (separation by segment) for each sever usage, each user department and administrator. To minimize the impacts of backdoor virus's internal diffusion, separate potentially-impacted sections from other sections in the network design. For details, see Measure 6 in Section 4.5. Monitor the volume overload to detect infections Implement operation design in a way that log size/contents and communication volume are monitored for abnormality Implement operation design in a way that firewall blocking log and network equipment rule violation log are analyzed (e.g., frequent occurrence of "permission denied", Reject/Drop) For details, see Measure 7 in Section 4.5.

Appendix table 2-2: Considering measures against Six Common Threat Patterns

Threat type classification	The six Common Threat Patterns (CTP)	Outline of measures
Five types of threats in espionage or system destruction	CTP 6: - Threat of backdoor virus's internal diffusion within the system and	 Limit the range of access by P2P. Block unnecessary RPC with an internal firewall that is placed between an Internet enabled zone.
Type 1: Targeted e-mail	functional update	and a non-Internet-enabled zone.
Type 2: An attack via websites		(Same as 4, 5 and 6). For details, see Measure 8 in Section 4.5 (Same as
Type 3: An attack that destroys control systems		4, 5 and 6).
Type 4: Virus that transmits via USB		
Type 5: Combined DDoS attack		

[(3) Considerations in each phase]

Specific design-based measures against common threat patterns should be incorporated into each phase. Here, it is helpful to anticipate development teams keeping in touch and identifying any dependencies among tasks (when the deliverable of one task represents the input for another), among other coordination.

Appended Figure 2-2 shows an example of development teams organized for the projects discussed in this guide.

- Establish a team for non-functional requirements (security) within the general design team to implement outbound measures (Implementation Items 1–8) as security measures in system design.
- For security features corresponding to conventional inbound measures (such as access control, antivirus measures, and identity authentication), it is important to work with the general design team instead of working independently on design and implementation.



Appended Figure 2-2: Example of development team organization

		[1] Measure requirement definition	[2] Design		[3] Manufacturing (implementation)	[4] Test	[5] Operation
	Manage- ment	Keep cost-effective measures in mind Build relationships with stakeholders	Clarify roles, relative to stakeholders Approve hardware and software procurement	Approve completion of phases		-	
General Design Team	Business	Gather stakeholder feedback on current business and systems Prepare business requirements	•Conduct business design	• Draw up business test plans	•Organize business data	Conduct business tests	
	Non- functional Require-	 C1> Define overall system security requirements (A) Purpose of defensive measures (B) Types of threats (C) Compare threat a stronger 	 Create specifications for overall system security requirements (establish shared security policies) Design methods and implementation (consolidation) 	<3> Review non-topological security) Plan tests of the security of th	functional requirements overall system defense d adjust overall system risk	<4> • Test overall system defense	Conduct business with risk control measures in place (monitoring, analysis)
	ments (Security)	(b) Outbound measures (c) Design of defensive measures	of logging and monitoring; policies supporting network separation)	Outbound me overall system		asures: part of n design	
ent Team	Business application develop- ment	Determine the form of applications Investigate and select frameworks	Determine functions in general Determine function methods Design processes	Design program structures	Develop applications	Test operation of individual applications Test operation in business	Provide support in business use
ucture Developm	Infra- structure	Sort out infrastructure requirements - Define network segments - Define business whitelists	Determine infrastructure design in general Design infrastructure methods Network design Design hardware and software Log volume estimates	Conduct infrastructure environment design (prepare design sheets)	Construct the environment	Test infrastructure operation	Provide support for the infrastructure
System Infrastr	Security functions	Sort out requirements of security functions - Security function deployment	Design security function methods - Firewalls - Antivirus measures - Spam measures - Access control, etc.	Design security function details (prepare design sheets)	• Implement security functions Conventional element of inc	•Test individual security functions inbound measures: dividual system func	• Support security functions an ctions
Deliverables		Requirement definition document • Overall security requirements	General design specifications • Determine shared security policies Basic design document	etailed esign pecifications lesign neets, etc.)	Defense test scenario Operating procedures	Confirm defense test results	Operating procedures

Appended Figure 2-3: Considerations in each phase

Appendix 3: Summarizing Information Security Measures

Although "information security measures" are expressed in one word, each measure has different objectives. Objectives can be classified into the following two major types (Appended Figure 2-1):

- (1) To prevent company staff from taking out internal documents; to prevent noncompliance
- (2) To protect the organization against cyber attack from outside

When considering information security measures, organizations should take into account these two objectives and establish measures. That is to say, if the organization establish and implement measures without clearly understanding "what needs to be protected from what by that measure", it would become difficult to determine their effectiveness. In such cases, the organization would end up in squandering investment on those measures. When establishing security measures, it is important to determine whether they are intended to prevent information leakage from inside the organization or to preventing an attack from outside.

To prevent information leakage from inside the organization, organizations can apply various standards such as ISMS (Information Security Management System). These standards may include measures against an attack from outside. However, attacks evolve on a daily basis. So, just ensuring compliance with those standards does not mean that the organization is protected against an attack from outside. To protect your systems from an attack from outside, make clear "what needs to be protected from what" and then establish and implement security measures.



ISMS: Information Security Management System FISMA: Federal Information Security Management Act ISO15408: Information Technology Security Evaluation Criteria CC: Common Criteria

Appended Figure 3-1: Association Chart for Information Security

Literary work /Production Information-technology Promotion Agency (IPA), Japan

Hiroki	Nagoya University	Katsumi	NRI SecureTechnologies, Ltd.
Takakura		Kobayashi	
Mitsugu	National Information Security Center	Tetsuji	NEC Corporation
Okatani	(2011/05/16)	Tanigawa	-
Kousetsu	Fujitsu Limited	Norihiko	K.K. Kaspersky Labs Japan
Kayama		Maeda	
Yasuhiro	Fujitsu Limited	Suguru	K.K. Kaspersky Labs Japan
Fujiwara		Ishimaru	
Hiroshi	Kyushu Institute of Technology	Tomohiro	Trend Micro Inc.
Koide		Iida	
Masakazu	Microsoft Japan Co.,Ltd.	Bakuei	Trend Micro Inc.
Takahashi		Matsukawa	
Toshifumi	IBM Japan, Ltd.(2011/11)	Kunio	NTT DATA CORPORATION
Tokuda		Miyamoto	
Koichiro	IBM Japan, Ltd.	Kentaro	Hitachi Solutions, Ltd.
Watanabe		Nameki	
Eiichi	IBM Japan, Ltd.	Yuji	Hitachi Solutions, Ltd.
Moriya		Matsuura	
Hisao Nashiwa	IBM Japan, Ltd.	Koichi	Telecom-ISAC Japan(2011/11)
		Arimura	
Hidetoshi	IBM Japan, Ltd.	Ryuhei	Telecom-ISAC Japan
Ogura		Takahashi	
Yuji Motokawa	Hitachi Systems, Ltd.	Satoshi	Telecom-ISAC Japan
		Noritake	
Akira	Hitachi Systems, Ltd.	Masato	Hitachi, Ltd.
Orita		Terada	
Shinichi	Hitachi Systems, Ltd.	Yuji	Fourteenforty Reseach Institute Inc.
Tankyo		Ukai	
Akira	University of Tukuba	Ryoji Kanai	Fourteenforty Reseach Institute Inc.
Kanaoka			
Masahiko	Internet Initiative Japan Inc.	Junichi	Fourteenforty Reseach Institute Inc.
Kato		Murakami	

Author	IPA's working group	for threats an	d measures
--------	---------------------	----------------	------------

Information-technology Promotion Agency, Japan

Hideaki Kobayashi, Chisato Konno, Motokuni Souma, Masashi Ohmori, Yasunori Irisawa

Design and Operational Guide to Protect against

"Advanced Persistent Threats"

[Publication]	August 2011, the 1st edition, 1st printing
	November 2011, the 2nd edition, 1st printing
[Production]	IT Security Center, Technology Headquarters
	Information-technology Promotion Agency, Japan (IPA)
[Collaborator]	IPA's working group for threats and measures