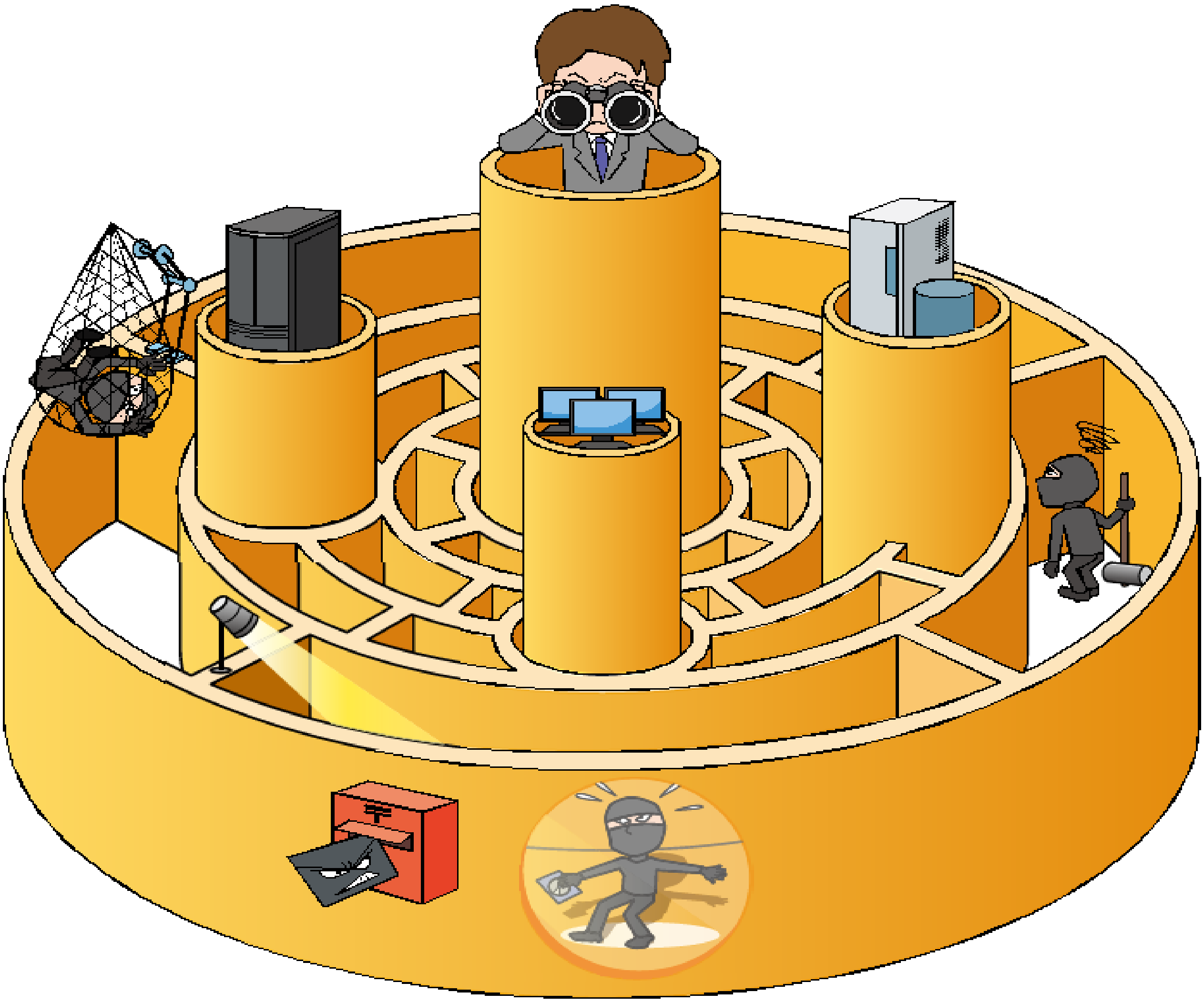
System Design Guide for Thwarting Targeted Email Attacks

~Make Your System Difficult for Attackers to Operate Inside~



IPA IT SECURITY CENTER (ISEC)
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

December 2013

This document is available for download at the following URL:

System Design Guide for Thwarting Targeted Email Attacks

http://www.ipa.go.jp/security/english/newattack_en.html

Contents

Introduction

Over the past few years, sensitive information that could affect the national interests or businesses have been stolen from government agencies and companies through targeted email attacks, and that is posing a serious problem. The data like the sender, message and file name of the attachment of targeted emails are so masterfully faked that it is quite difficult to notice and stop them at the so-to-speak “entry point” when their recipient receives them.

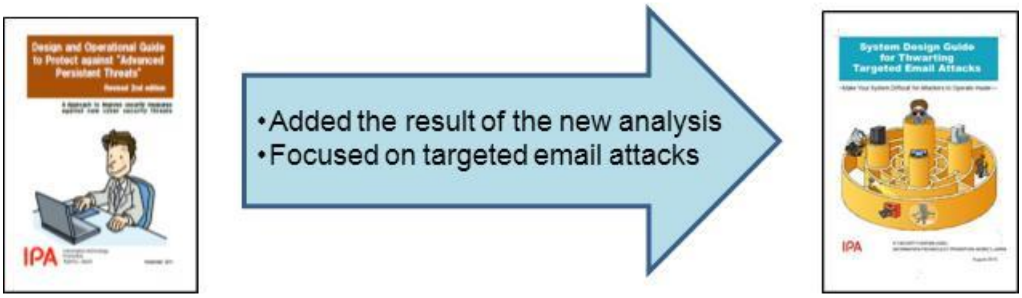
On the premises that some targeted emails will manage to infiltrate the internal system of targeted organizations, IPA has analyzed a full picture of and techniques used by targeted email attacks after their successful infiltration and formulated the defense measures against the attacks at the system design level.

Based on the result of the aforementioned analysis, this guide breaks down a targeted attack into seven phases and explains an attacker’s objective and characteristics/patterns of the attack at each phase. The guise also introduces the system design measures focusing on hacking and information theft that occur deep inside the internal system, which the traditional security measures have failed to cover. The system design measures introduced in this guide are independent of specific technologies or solutions. Instead, they aim to make the internal system difficult for the attacker to infiltrate and operate inside, meaning “move around and do things freely”, by revising the current system design and settings.

IPA hopes this guide will help government agencies and companies understand targeted emails attacks better and improve their system design and operation to prevent the damage that can be caused by the attacks.

Document Series

This guide is a sequel to the Design and Operational Guide to Protect against "Advanced Persistent Threats” released in November 2011, and focuses on the measures against targeted email attacks based on the analysis of the newly found facts and actual incidents. IPA used to collectively refer these attacks as advanced persistent attacks but decided to change them to “targeted email attacks” for their characteristic of being very target-specific.


Design and Operational Guide to Protect against "Advanced Persistent Threats"
IPA
•Added the result of the new analysis
•Focused on targeted email attacks
System Design Guide for Thwarting Targeted Email Attacks
IPA

Note that the measures introduced in this guide are examples of some possible solutions and not all of them are necessarily required to implement.

Intended Readers and How to Utilize This Guide

This guide is expected to be used by those responsible for the following roles at each standpoint, as a guidance to design their internal system with a comprehensive and panoramic view.

- Network administrators/operators
- Business system and server administrators/operators
- System integrators (system developers)
- System design staff and procurement staff

Characteristics of Targeted Email Attacks

Targeted email attacks are recognized as **an exceptional problem** different from the traditional information security issues due to **their specific intentionality, purposefulness**, consistency and that the targeted (stolen) information could affect **the national interests and intellectual property**. At the same time, targeted email attacks are an **important political issue many governments have positioned as a “cyberspace issue”**. It helps **to understand that the true nature of the issue** by reviewing the meaning and difference between the traditional concept of “information security, management or cyber security” and “cyberspace” from the standpoint of all relevant fields.

The “cyberspace issue” is different from the rest in a way that it is not simply a technical aspect but also involves with **other aspects, such as international politics, market interests (international public goods), intellectual property, national security, military operations and national crisis management.**

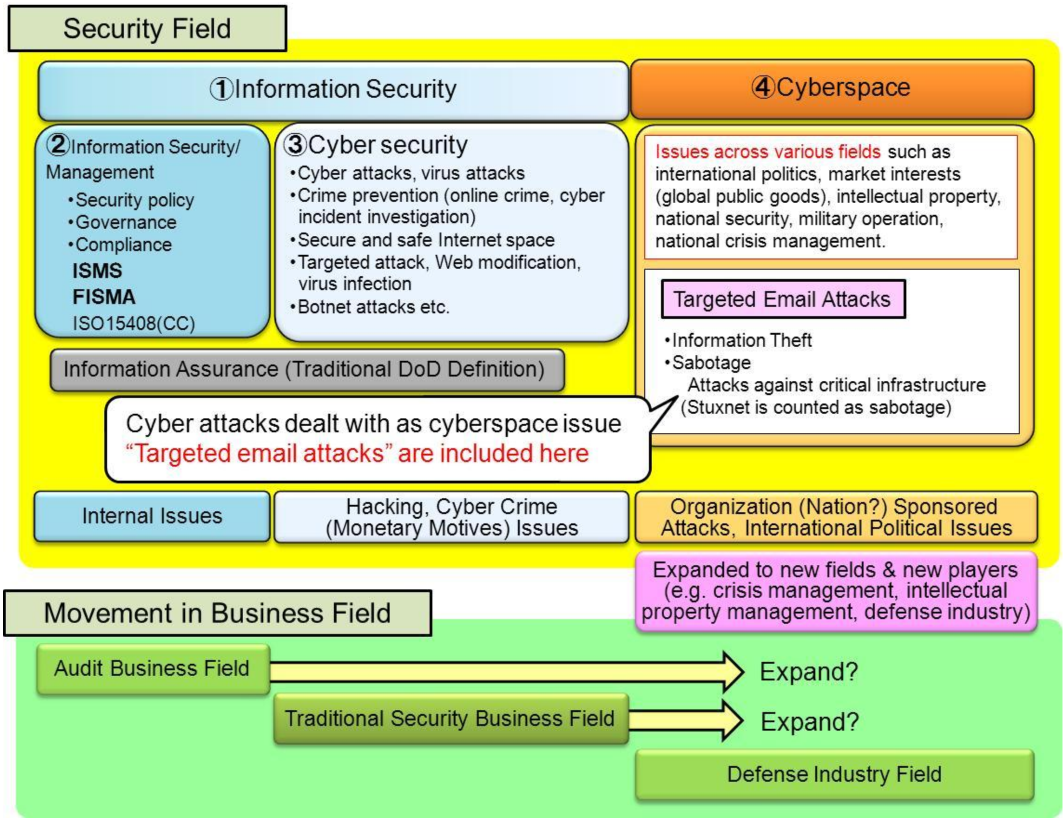

Security Field
①Information Security
④Cyberspace
②Information Security/ Management
•Security policy
•Governance
•Compliance
ISMS
FISMA
ISO15408(CC)
③Cyber security
•Cyber attacks, virus attacks
•Crime prevention (online crime, cyber incident investigation)
•Secure and safe Internet space
•Targeted attack, Web modification, virus infection
•Botnet attacks etc.
Issues across various fields such as international politics, market interests (global public goods), intellectual property, national security, military operation, national crisis management.
Targeted Email Attacks
•Information Theft
•Sabotage
Attacks against critical infrastructure
(Stuxnet is counted as sabotage)
Information Assurance (Traditional DoD Definition)
Cyber attacks dealt with as cyberspace issue
“Targeted email attacks” are included here
Internal Issues
Hacking, Cyber Crime (Monetary Motives) Issues
Organization (Nation?) Sponsored Attacks, International Political Issues
Expanded to new fields & new players (e.g. crisis management, intellectual property management, defense industry)
Movement in Business Field
Audit Business Field
Expand?
Traditional Security Business Field
Expand?
Defense Industry Field

Figure 1. Cyberspace and Information Security

1. Executive Summary

Beyond the concept of the word "cyber security" that has been traditionally used, t**he concept of "cyberspace"** that is often seen these days has an extensive scope of the coverage including **the field of international politics,** which alone includes various aspects. This guide emphasizes the explanation for the stuff, such as deciphering the problem structure and organizing the points of those aspects, **to zero in on what the true nature of the issue is.**

This guide has been developed to provide the necessary security measures to the organization that are a target of targeted email attacks executed under the scope of cyberspace and **have decided they must defend their confidential information that could impact not only the organizations themselves but also national interests.**

The system design measures introduced in this guide were narrowed down to the measures that were effective in response to the attack techniques used in targeted email attacks. They were developed with one thing in mind: that the organizations can understand a full picture of the targeted email attack and what the real issue is, and select the measures well balanced in need, cost-performance and priority accordingly to each organization.

1．1 Overall Structure of Cyberspace Issue

The concept of "cyberspace" was first introduced by the U.S. government (the Department of State and Department of Defense) in January 2010. After that, in May 2011, the White House released the "International Strategy for Cyberspace[1]".

It showed that the U.S. now recognized and "added cyberspace, which is one of the international public goods, as a fifth domain[2]" to air, land, sea and space, and **did not focused just on cyber attacks anymore**.

After that, since 2013, international talks on the establishment of international rules regarding cyberspace have been started, for example, through the U.S.-Japan Cyber Dialogue[3] and U.S.-China Summit.

The themes of the issue and supposed threats in this movement are "destruction of critical infrastructures and theft of confidential information (e.g. defense secrets and intellectual property)" as well as **interstate matters** (economy, intellectual property, diplomacy, national security, and national crisis management).

It is a different dimension from the traditional, simple cyberattack (cybersecurity) issue.

[1] Ministry of Internal Affairs and Communications "Trend in International Argument on Cyberspace": http://www.soumu.go.jp/menu_seisaku/ictseisaku/cyberspace_rule/index.html (in Japanese)

[2] US Embassy website in Japan: The Release of President Obama Administration's International Strategy for Cyberspace http://japanese.japan.usembassy.gov/j/p/tpj-20110517a.html (in Japanese)

[3] Japan-U.S. Cyber Dialogue Joint Statement http://www.mofa.go.jp/mofaj/area/page24_000009.html (in Japanese)

Unlike the cybersecurity issue, because the cyberspace issue is extended to such a wide scope of areas, non-traditional areas such as **the field of international politics, economics, diplomacy, and military, are becoming involved**.

Understanding the difference in the implication and background of the concept presented by the word “cyberspace” and traditional “cyber security” becomes important when considering **the true nature of the issue and an organization’s position in the situation, or the impact on the organization**.

Becoming aware that it is not just the word “cyber security” has been replaced by the word “cyberspace” can be all it is required to gain insight into the true nature of the issue.

1．2 Impact and Issue of Targeted Email Attacks

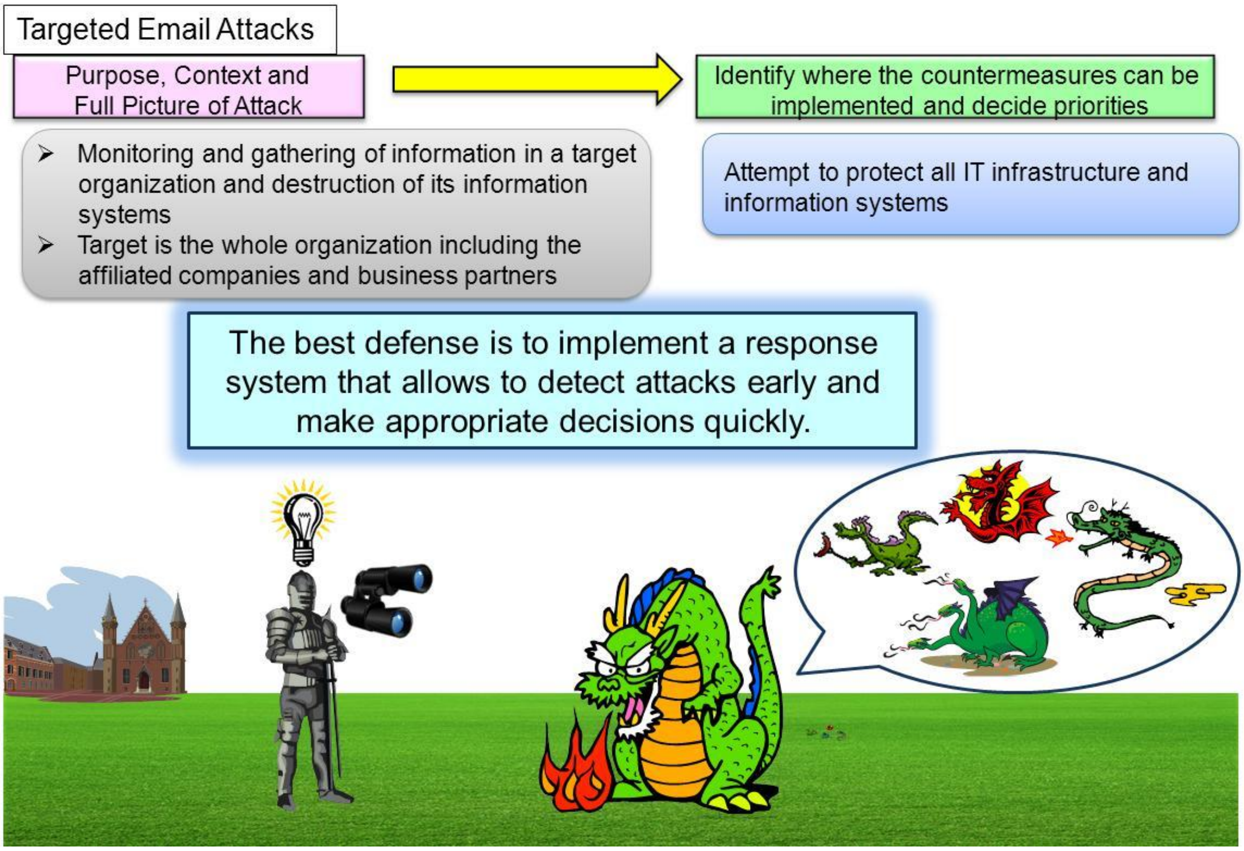
Based on the background mentioned in 1.1, **one of the themes that has an important role and need to be addressed is targeted email attacks**. The question of “who are doing them for what purpose” has remained unsolved for a long time. Even though targeted email attacks have been around since 2003 (see 2.1.2 Column: HIstory of Targeted Email Attacks）, no one could answer who and why for all these years. Things changed in 2011 **after the U.S. government began to handle targeted email attacks as a “cyberspace issue”** and the pieces of the answer for “who and why” have started to become open to the public.

While targeted email attacks have been known for ten years, the analysis of their full scope and concrete countermeasures (periodically-issued security alerts) were not sufficiently done or given.

This guide’s **first principle was to shed light on a full picture of the targeted email attacks** instead of part of them we were able to get a glimpse of until now. Because if we know the purpose, context and full picture of the attacks, it **becomes possible to identify where the countermeasures can be implemented and decide priorities;** in other words, can consider the necessary and appropriate countermeasures.

As seen in the actual incidents at home and abroad, the purpose and context behind the targeted email attacks are assumed to be **the monitoring and gathering of information in a target organization and/or destruction of its information systems**. Thus, organizations **need to be aware that a target is not the individuals within an organization but the whole organization including its affiliated companies and business partners**. For this, this guide tries to provide the security measures **in an attempt to protect an organization’s all IT infrastructure and information systems.**

The true nature of targeted email attacks is not in the targeted emails or malware attached to them. **The core of the attack is to infiltrate the internal systems deeper**. Knowing that, the best defense is to organize and implement the response system **that allows the organization to detect an attack as early as possible and make appropriate decisions as quickly as possible.** With such response system in operation, collaboration and information sharing with other organization becomes also valuable.



Targeted Email Attacks

Purpose, Context and Full Picture of Attack

- Monitoring and gathering of information in a target organization and destruction of its information systems
- Target is the whole organization including the affiliated companies and business partners

Identify where the countermeasures can be implemented and decide priorities

Attempt to protect all IT infrastructure and information systems

The best defense is to implement a response system that allows to detect attacks early and make appropriate decisions quickly.

Figure 1.2-1 Awareness of Real Issue of Targeted Email Attacks

1．3 Set of System Design Measures

When the Design and Operational Guide to Protect against “Advanced Persistent Treats[4]”, which is a prequel to this guide, was developed, the areas of the expertise from which people participated in the study were system development (system integrators) and cyber security (virus analysts, SOC operators, academic researchers). The experts from each area sat around the same table and through the exchange of information and insight, discussions and multi-field correlations, we could understand and establish the images of how an targeted email attack would take place at the first phase of the attack (the initial compromise phase where malware attached to a targeted email does its work).

For this guide, in addition to the same areas of the expertise as in the previous study, the experts from the field of attack analysis (forensics), penetration testing, operations management, crisis management and public administration have participated, and **through the same roundtable study as before, uncovered the full scope of an targeted email attack at the deep infiltration phases, which were the core of the attack**.

We assume a reason why it has been said that targeted email attacks are difficult to understand is due to **a limitation imposed by the way that the past studies were conducted from a single point of view (area of expertise)**. Through **the multi-field study scheme** like one we used to develop this guide, it is possible to notice the things one have missed before. The set of the system design measures has been developed through such scheme and reflects the expertise from each field extensively throughout the guide.

Based on a similar perspective, we tried to **make the set of the system design measures play a role of the interface between relevant parties**, such as a contractor and contractee, field management unit and budget management unit, business management unit and development unit, and user and vendor (supplier). When considering the measures and response actions, the most important thing is for the relevant parties to **have the same understanding, goal and perception of the issue**.

Figure 1.3-1 Collaboration among Experts

[4] http://www.ipa.go.jp/security/vuln/newattack.html (in Japanese)

2. Overview of System Design Measures

This chapter explains a full picture of the attack operation of a targeted email attack and how to design the internal system to defend against the targeted email attacks. In addition, the approaches taken by IPA Security Threat and Countermeasure Study Group to derive the countermeasures are also introduced.

2．1 Full Picture of Attack and Approach for Deriving Countermeasures

The set of the system design measures was developed as a “**system design specification**” to detect and block the attacks at each phase by analyzing the complete process of targeted email attacks (a full picture of “**the attack operations conducted by the attacker**” on the targeted system) in detail.

Based on the analysis of the attacker’s operations on the targeted system (indicated by the red arrow → in the figure below) and the attacker’s state of mind, the measures focus on **making the system difficult for the attacker to operate inside, inducing the attacker to make mistakes and detecting the presence of the attacks that are trying to infiltrate deeper into the system as early as possible**.

Note that there exist various definitions for what a targeted email attack is and that has been a cause of confusion. In this guide, we call an attack operation that follows a certain series of actions – send a fraud email and gain a foothold into the internal system, infiltrate the system deeper and stole the targeted information - as a targeted email attack, and distinguish it from other targeted attacks.

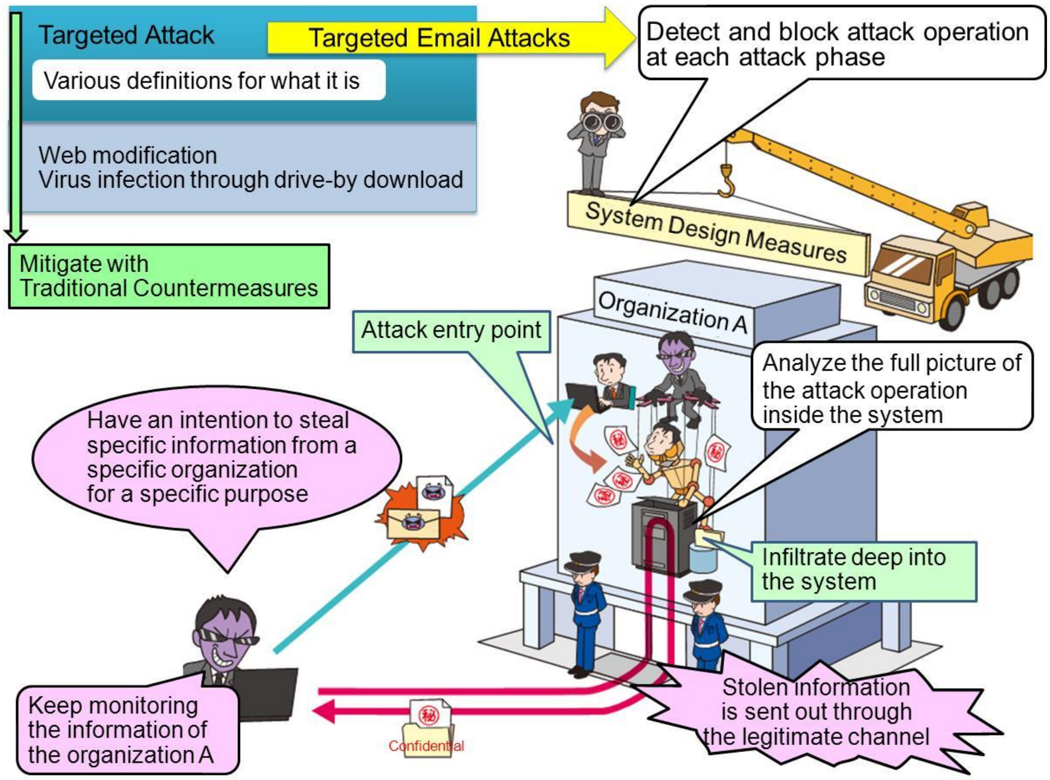

Targeted Attack
Targeted Email Attacks
Various definitions for what it is
Detect and block attack operation at each attack phase
Web modification
Virus infection through drive-by download
Mitigate with Traditional Countermeasures
System Design Measures
Organization A
Attack entry point
Analyze the full picture of the attack operation inside the system
Have an intention to steal specific information from a specific organization for a specific purpose
Infiltrate deep into the system
Keep monitoring the information of the organization A
Confidential
Stolen information is sent out through the legitimate channel

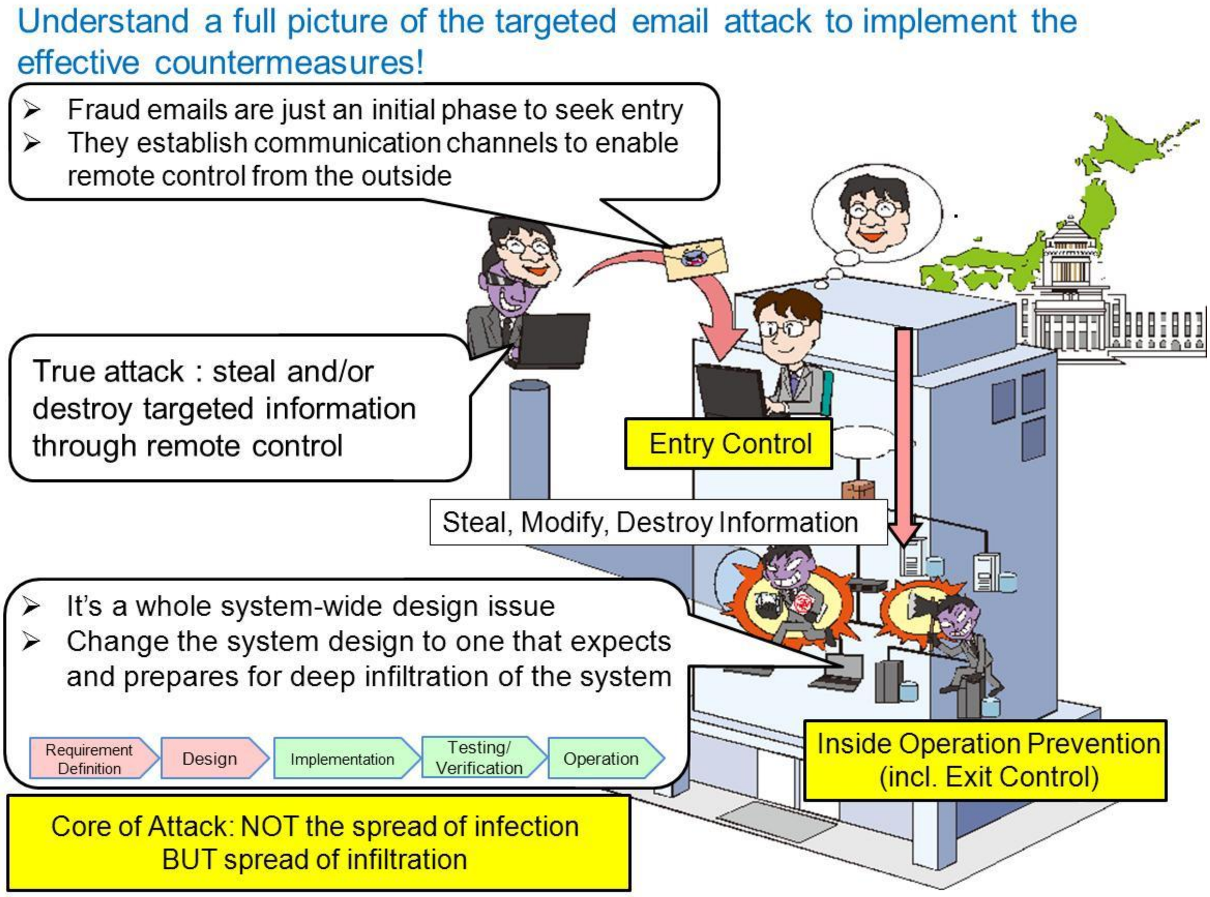
Figure 2.1-1 Overview of Targeted Email Attack

2．1．1 Need and Background of System Design Measures

(1) Nature of Attack

From an image the word “targeted email attacks” may provoke, they are often recognized as a problem of fraud emails and malware infection. However, the research conducted by IPA Security Threat and Countermeasure Study Group shows that fraud emails and malware infection are just a very initial phase of a grand scheme for the attacker to gain a foothold into the internal system to establish communication paths to enable remote control from the outside, and the true attack takes place later, in which the **remote attacker infiltrates the internal system deeper to steal and/or destroy the targeted information**. Thus, it can be said that **the nature of the targeted email attacks is** “**not the spread of infection but spread of infiltration**”.

By understanding this nature correctly, we can formulate effective countermeasures. Misunderstanding the full picture of the targeted email attacks is one of the reasons why the current countermeasures fail to show real effectiveness.



Understand a full picture of the targeted email attack to implement the effective countermeasures!

- Fraud emails are just an initial phase to seek entry
- They establish communication channels to enable remote control from the outside

True attack : steal and/or destroy targeted information through remote control

- It’s a whole system-wide design issue
- Change the system design to one that expects and prepares for deep infiltration of the system

Core of Attack: NOT the spread of infection BUT spread of infiltration

Figure 2.1.1-1Truth of Attack

(2) Need for System Design Measures

Because the goal of the targeted email attacks is to steal the information and/or disrupt the business, and **the attacker tries to infiltrate as deeper as possible (to hack the internal system),** the subjects of the security measures are not the individual PCs and servers but **need to be the whole system-wide design.**

The traditional system design intended to **prevent the attacker's initial hacking attempts (the entry control measures)**. Because targeted email attacks will get them through and infiltrate deep into the internal system, the **system design needs to be changed to one that aims to prevent the spread of infiltration and enhance monitoring (the inside operation prevention measures) on the premises that the attacks will manage to infiltrate deep into the system**.

The set of the system design measures has been developed **as a new system design method** from the above perspective based on the analysis of the attack techniques used in the actual attacks.

In this guide, the exit control measures introduced in the prequel, the Design and Operational Guide to Protect against "Advanced Persistent Threats", are included in the inside operation prevention measures.

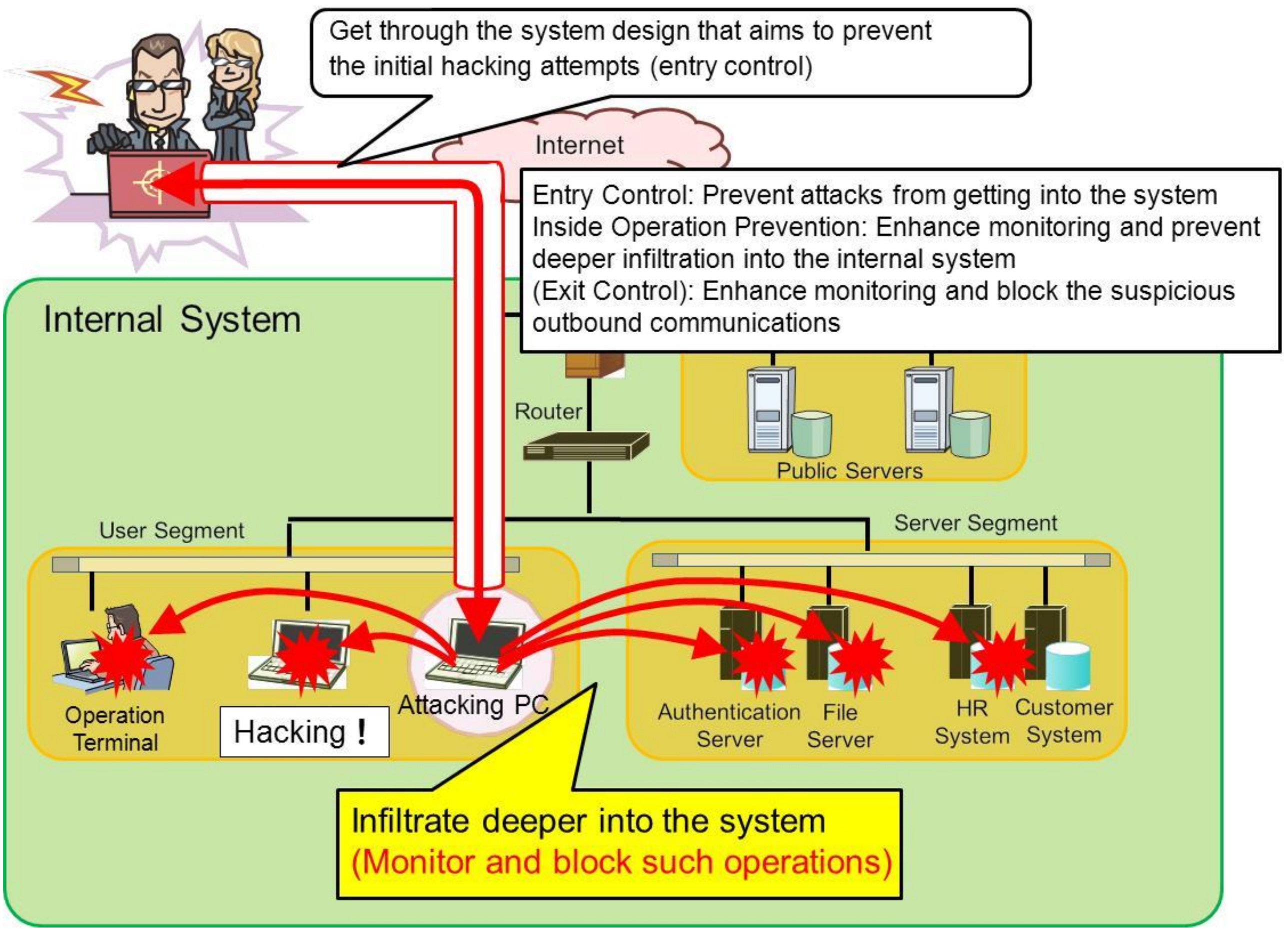

Get through the system design that aims to prevent the initial hacking attempts (entry control)
Internet
Entry Control: Prevent attacks from getting into the system
Inside Operation Prevention: Enhance monitoring and prevent deeper infiltration into the internal system
(Exit Control): Enhance monitoring and block the suspicious outbound communications
Internal System
Router
Public Servers
User Segment
Server Segment
Operation Terminal
Hacking !
Attacking PC
Authentication Server
File Server
HR System
Customer System
Infiltrate deeper into the system
(Monitor and block such operations)

Figure 2.1.1-2 Attacker's Activities to Be Stopped

The set of the system design measures focuses on preventing the deep infiltration into the internal system and its key points can be summarized below:

- Make the system difficult for the attacker to operate inside
- Set up the traps to detect the attacker's operation inside the system
- Enable the system administrators to become aware of the attempts of deeper infiltration (the presence of the attack operations inside the system) as early as possible (THAT leads to blocking and preventing the attacks!!)

Note that the Study Group on the Protection against Advanced Persistent Threats (APTs) at National Information Security Center (NISC) and IPA Security Threat and Countermeasure Study Group have been collaborating and the set of the system design measures is to be used as a guideline in a cybersecurity initiative for the government agencies. Also, part of the outcome of the Study Group on the Protection against APTs, NISC, will be reflected in this guide.

The Study Group on the Protection against APTs, NISC, has been formed by a policy implemented by the government to deal with the attacks that target the nation's important information and some members of IPA Security Threat and Countermeasure Study Group participate in it as well.

The activities of the Study Group on the Protection against APTs, NISC, can be read in the article, the "Initiative to Strengthen the Protection against APTs on the Basis of Risk Assessment", in the page eighteen of the "Annual Report on Information Security of the Government Agencies[5]".

[5] http://www.nisc.go.jp/conference/seisaku/dai36/pdf/36shiryou0402.pdf (in Japanese)

2. 1. 2 Full Picture of Attack (Attack Scenario)

A targeted email attack has seven phases. With the intention to accomplish a specific mission like stealing information, the whole attack is planned in advance and executed as planned.

It is difficult to find out a full picture of the attack and formulate the effective measures by just investigating part of the attack, such as the analysis of fraud emails or malware. Every single targeted email attack is a customized, manual attack. We can understand the full picture and formulate the workable measures only by deciphering what the attacker's mission is and **investigating and analyzing the complete picture of the attack plan** comprehensively through a multidimensional perspective.

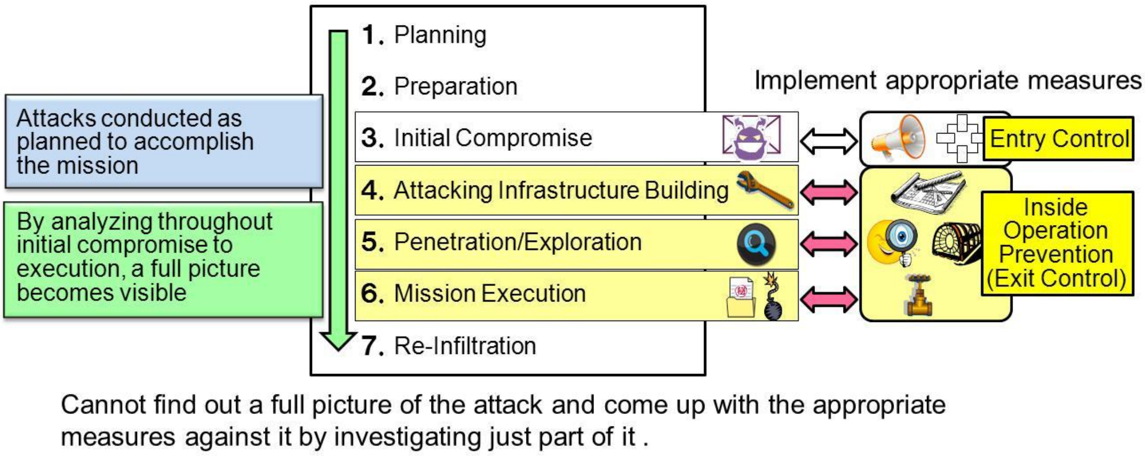

1. Planning
2. Preparation
3. Initial Compromise
4. Attacking Infrastructure Building
5. Penetration/Exploration
6. Mission Execution
7. Re-Infiltration
Attacks conducted as planned to accomplish the mission
By analyzing throughout initial compromise to execution, a full picture becomes visible
Implement appropriate measures
Entry Control
Inside Operation Prevention (Exit Control)
Cannot find out a full picture of the attack and come up with the appropriate measures against it by investigating just part of it .

Figure 2.1.2-1 Targeted Email Attack - Attack Scenario

(1) Attack Scenario: Overall Flow

Below is a basic pattern of the targeted email attacks derived from the analysis (for more details, see 3.1 Targeted Email Attack Scenario in Detail. The scope of this guide is **from ④ Attacking Infrastructure Building to ⑥Mission Execution.**

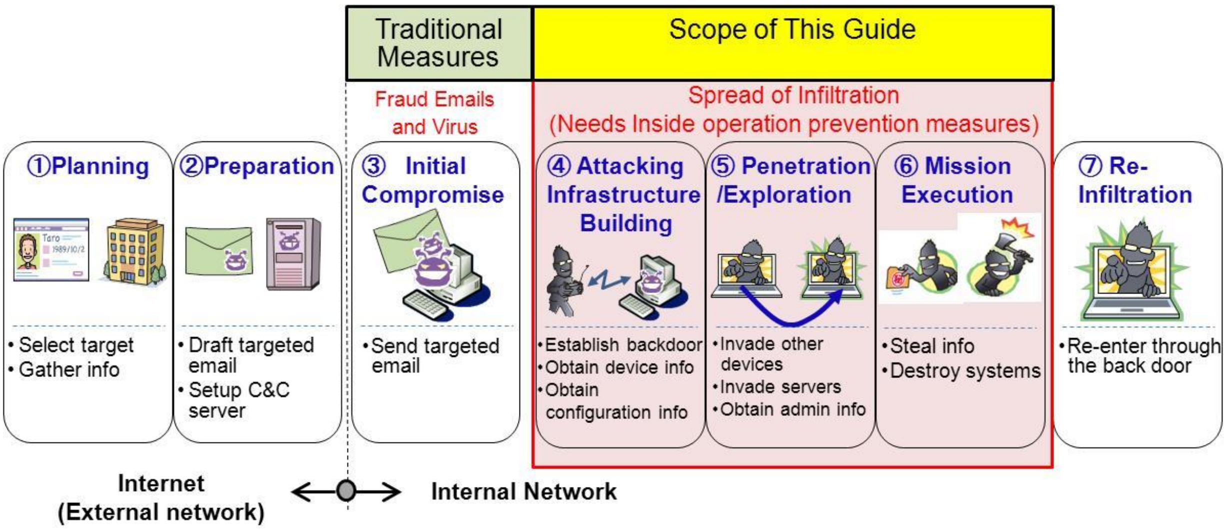


Figure 2.1.2-2 Targeted Email Attack – Attack Phases

The following summarizes the attacking operation at each phase.

a. ① Planning Phase and ② Preparation Phase

These phases are for reconnaissance and attack planning. The actions taken by the attacker at these phases include, but not limited to, selecting a target, obtaining the email address that belong to the target, email correspondences between the target and organizations involved with the target that can be exploited to draft targeted emails, clarifying the criteria of success at these phases, preparing targeted emails attached with malware, and setting up an environment to remotely control the compromised devices.

b. ③ Initial Compromise Phase

At this phase, malware-ridden targeted emails are sent to the target (and/or related organizations) simultaneously.

The goal is to infiltrate the internal system of the target and establish a "communication channel for remote control (connect-back channel)" with some devices on the internal system. Prevention of attacks at this phase is within the scope of the entry control measures (e.g. sharing information about fraud emails, monitoring and detecting malware, patching vulnerabilities, blocking access to malicious websites). In the actual incidents, it is difficult to prevent targeted email attacks at this phase and the attacks often **succeed in moving into the next phase of the attack process**.

c. ④ Attacking Infrastructure Building Phase

From this phase, the attack is transformed into an "**infiltration into the internal system by the remote attacker**" via one or more connect-back channels. The attacker **attacks the internal system manually by trial and error** using various tools. Once the attack reaches this phase, the defenders need to **"change their mindset and think how they can detect the presence of the attack and deter the deeper infiltration"**. The attack process at ④ Attacking Infrastructure Building phase is the following:

Goal: To gather information about networks and servers from the compromised user PC

- Record success and failure of the infiltration attempts and **keep tabs on the targets ("target management")** to exploit them on a continuous basis.
- Steal the ID/password hash from the compromised user PC and prepare to exploit other devices.
- After this phase, **it isn't about malware infection anymore and becomes a careful, manual hacking conducted by the attacker**, and moves to ⑤ Penetration/Exploration Phase.

【Characteristics of Attack】

- Because communications via connect-back channels are established as legitimate ones that use and follow the protocols and network design rules defined by the system, **it is difficult to detect in most cases.**

- After establishing a connect-back channel between the compromised user PC and the C&C server, the attacker downloads the tools to be used in the further attack. (For more details, see 3.3 Tools Used for Infiltration).

d. ⑤ Penetration/Exploration Phase

This phase is **the core of the targeted email attacks** and the reason why we express our image of the targeted email attacks as NOT the "spread of infection" BUT "spread of infiltration". The attack process at ⑤ Penetration/Exploration phase is the following.

Goal: To infiltrate the internal system deeper while stealing account information on the way

- Using the administrative account information obtained from the user PCs, **hijack the key devices** such as file servers, authorization servers (e.g. Active Directory), operation terminals and operations management servers.
- Ensure multiple PCs that are remotely controllable and set up an **attacking infrastructure that consists of the compromised PCs with different roles** – one to command the attack inside, one to compromise others, one to lie hidden, one to explore and gather information and one to send out stolen information.
- **Infiltrate deeper** into other segments and connected systems.

【Characteristics of Attack】

- The compromise spreads to the devices on the same segment → the authentication servers (Active Directory) → network devices → operations management servers.
- Because the attacking infrastructure is decentralized based on the role each compromised device plays, **it is difficult to see through a full picture of the attack.**

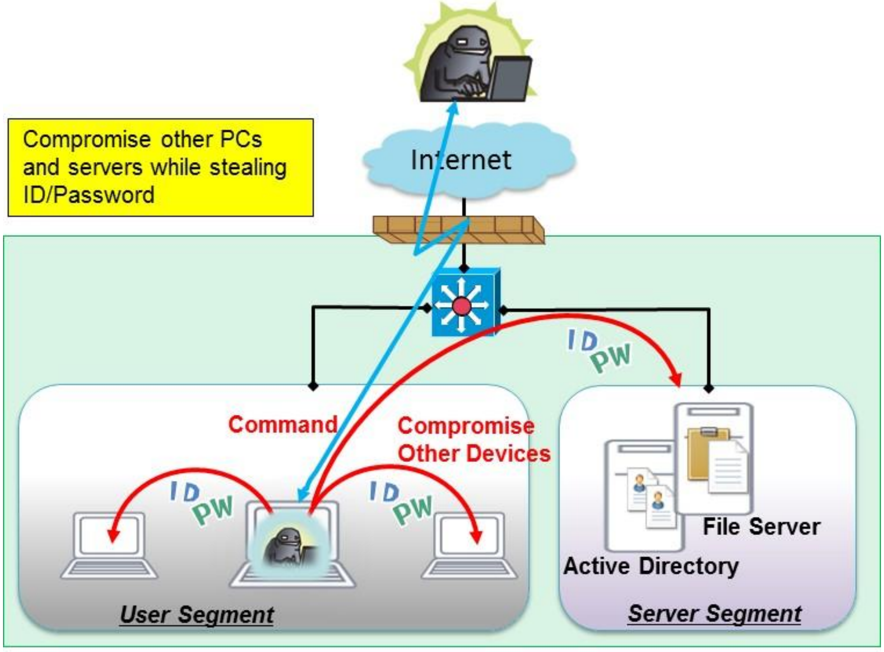


Figure 2.1.2-3 Image of System Compromise

e. ⑥ Mission Execution Phase

At this phase, the attacker transmits the target information stolen from the hijacked devices under the control of the attacker with the administrator privileges to the outside in bits and pieces through the multiple data send-out PCs. For this, if the defender looks for the stolen information “in one piece”, it will be difficult to detect. The stolen information is sent out through the connect-back channels, which makes it more difficult to detect.

Goal: To steal confidential information from the hijacked servers and/or destroy critical systems

So far, only the attacks that aim to steal confidential information have been confirmed in Japan, but from the incidents observed in other countries, it has been confirmed **the attacks that aim to destroy the system follow the same steps up to ⑤ Penetration/Exploration phase as well**.

Which means since the information system is under the control of the attacker at this phase, what will happen and how the consequence will impact the organization depend on the attacker’s intention.

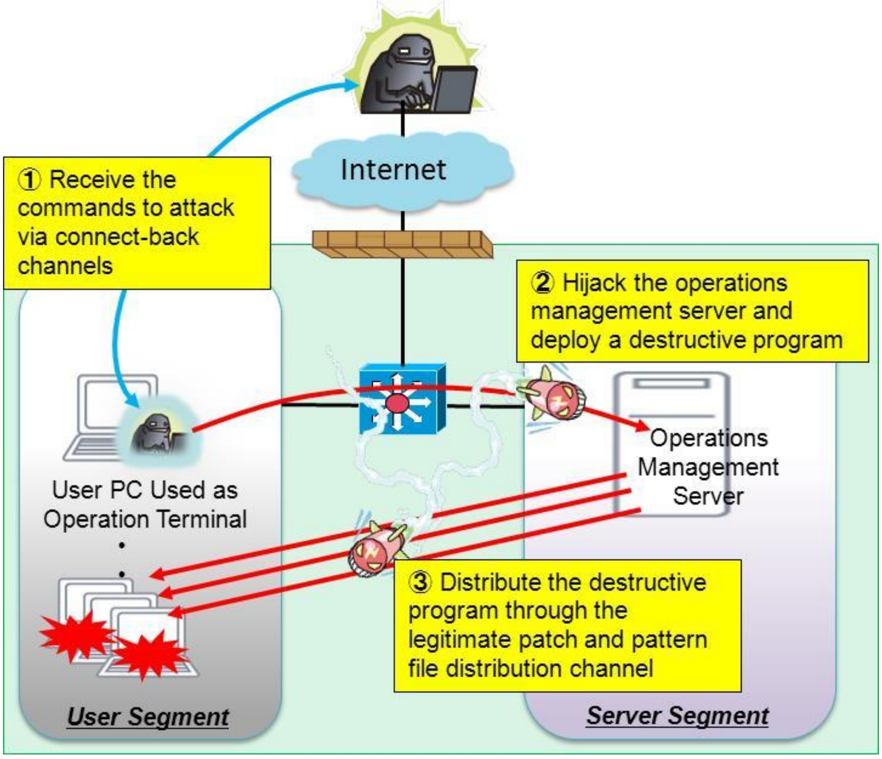

Internet
① Receive the commands to attack via connect-back channels
② Hijack the operations management server and deploy a destructive program
User PC Used as Operation Terminal
Operations Management Server
③ Distribute the destructive program through the legitimate patch and pattern file distribution channel
User Segment
Server Segment

Figure 2.1.2-4 Image of Destruction of the System

f. ⑦ Re-Infiltration

At this phase, the attacker **continuously infiltrates** and explores the target system through the existing connect-back channels. At the same time, **to set up yet another attacking PC and establish a new connect-back channel**, the attacker often keeps sending targeted emails attached with malware to the same organization.

For this reason, it is sometimes difficult to determine whether the attack was over or not. **Once targeted**, it is important to assume that the attacker will be coming back and to **continuously monitor** if connect-back channels exist.

(2) Details of the Attack Scenario

Overview of the core of the attack - ④ Attack Infrastructure Building, ⑤Penetration/Exploration and ⑥Mission Execution phase - and the details of the attack techniques at each phase are described in 3.1 Targeted Email Attack Scenario in Detail. They are **for those who define the system requirements, system designers and system operators to refer to** when designing a system based on the set of the system design measures.

Based on the set of the system design measures, those involved should **consider which system design measures to employ while balancing with the overall system design** which depends on the characteristics of the system and the environment in which it operates.

Column

Relation between Email, Vulnerability and Residual Risk

Even if it's just one person, if someone within the organization opens a malware link or file attached to a fraud email, a remote control path (connect-back channel) for the attacker is established and the targeted email **attack succeeds to infiltrate the system**.

For the organizations that have a large number of staff, have offices in dispersed locations, or have departments that require active contact with the outside organizations, **it is very hard to completely stop the fraud emails**.

In addition, because of the recent increase in the targeted email attacks that try to establish a benign email correspondence with the target first[6], which makes the receiver open the attachment more easily, the infiltration rate seems to be getting higher every year.

A traditional approach of "**the higher the patching rate, the lower the risk**", taken as a measure against malware and vulnerability, will not apply here. In fact, **what makes the targeted email attacks atypical** can be its characteristic that **even if the patching rate is 99%, the residual risk is still 100%.**

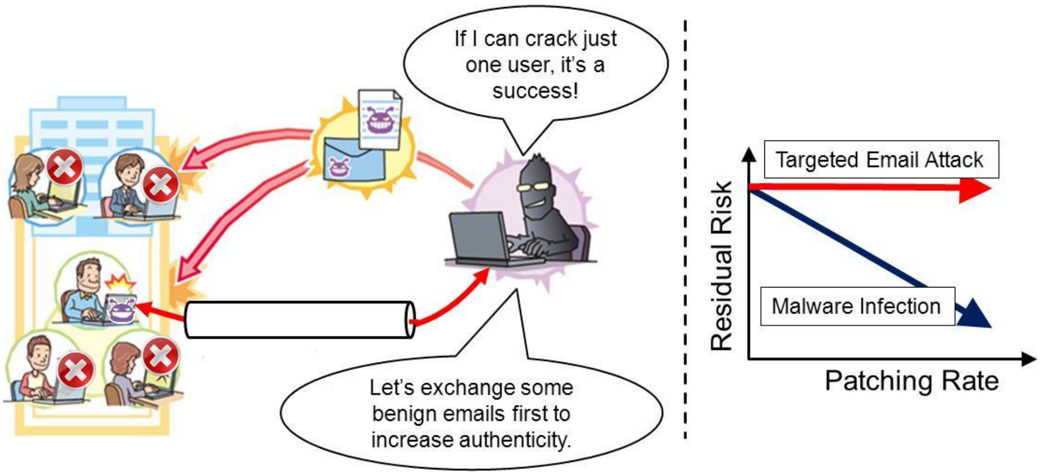

If I can crack just one user, it's a success!
Let's exchange some benign emails first to increase authenticity.
Residual Risk
Targeted Email Attack
Malware Infection
Patching Rate

Figure 2.1.2-5 Relation between Email Opening Rate and Residual Risk

[6] http://www.npa.go.jp/keibi/biki3/250822kouhou.pdf (in Japanese)

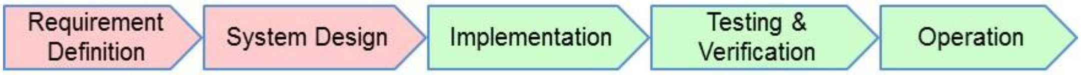
Column

Challenge at Requirement Definition and System Design

At the phase of requirement definition and system design, **first the possible threats that will be the premises of the system design are analyzed** and then design the system (e.g. network topology, security features, product selection).

If the targeted email attack is picked up as a possible threat, **the system design needs to premise that the attacker will infiltrate deep into the internal system**, but most system design case studies show **there is little information available to have such premises** and that makes it difficult for organizations to design the system to prevent deeper infiltration or monitor the system.

The set of the system design measures was developed to "**provide the system designers and operators the information" about the "premises (possible threats) and the system design measures based on them"**.

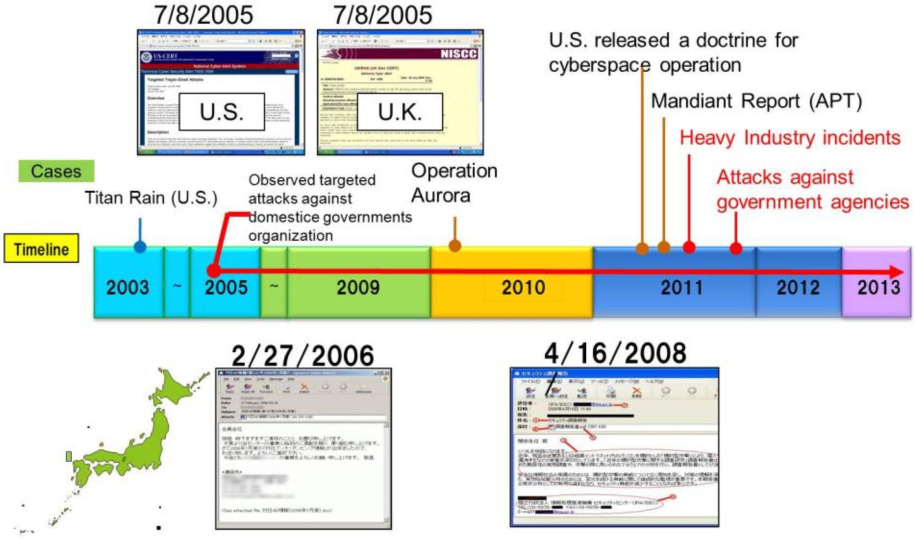


Column

History of Targeted Email Attacks

Targeted email attacks are an attack technique that has emerged all over the world since about 2003. They have been around for a quite long time, yet their full picture or intention is still poorly understood.

After the U.S. government released the doctrine for a "cyberspace operation" in 2011, **cyberspy operations** through targeted email attacks become an international political issue.



- The same attacks have been around for 10 years. Yet, haven't been able to prevent the damages and victims.
- After the attacks that targeted the heavy industry in Japan, the problem has become visible and active.
- We need to recognize that they are different from ordinary cyber attacks and special attention is required.

Figure 2.1.2-6 History of Targeted Email Attacks

2. 1. 3 Approach for Deriving Countermeasures

In this section, an approach taken by the IPA Threat and Countermeasure Study Group to derive the system design measures is introduced.

(1) Procedure Used to Derive System Design Measures

The Study Group's consideration of the system design measures followed the approach below.

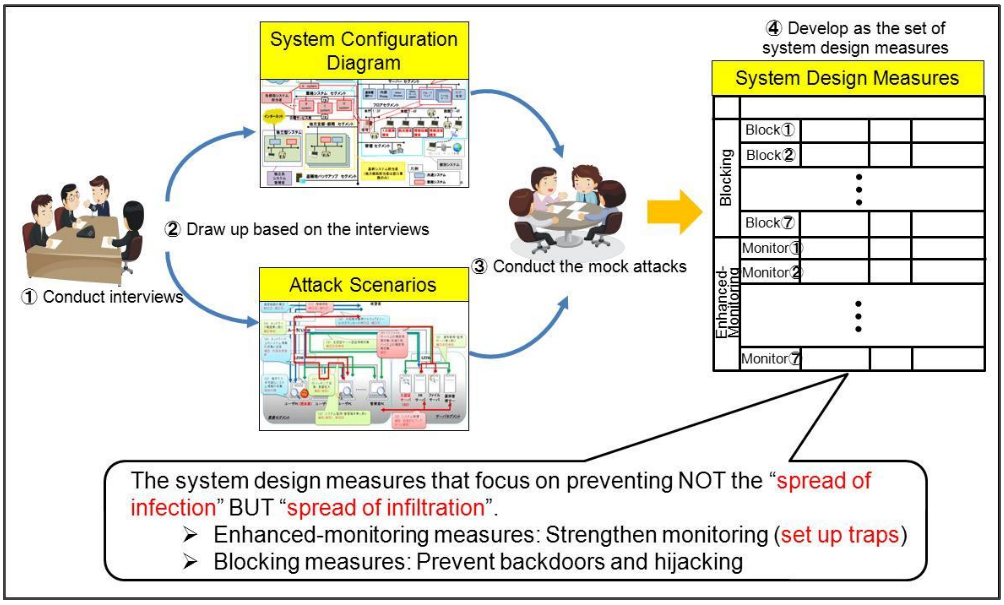
① **Analyze the attack procedure at each phase in detail and develop an attack scenario** based on the analysis of the attack techniques used in target email attacks（through case study research) and system-compromise detection techniques.

② Draw up a system design model (system configuration diagram) of a target system.

③ Based on the attack procedure at each phase in the attack scenario, conduct the mock attacks on the system design model (system configuration diagram) and **see if the attacks succeed or fail**. (Done focusing on ④ Attacking Infrastructure Building, ⑤ Penetration/Exploration and ⑥ Mission Execution)

④ Using the result, discuss the system design measures that would detect and prevent those attacks, categorize them into the "enhanced-monitoring measures" and "blocking measures" for further analysis and developed the set of the system design measures.

The set of the system design measures has been **developed through the mock attacks** using the real attack scenarios on the realistic system configuration drawn up based on the information obtained through the interviews to the companies. **They are concrete, implementable measures to prevent attacks from infiltrating deeper into the internal system**. The figure below shows the approach in a glance.


System Configuration Diagram
④ Develop as the set of system design measures
System Design Measures
Blocking
Block①
Block②
Block⑦
Enhanced-Monitoring
Monitor①
Monitor②
Monitor⑦
② Draw up based on the interviews
① Conduct interviews
③ Conduct the mock attacks
Attack Scenarios

The system design measures that focus on preventing NOT the "spread of infection" BUT "spread of infiltration".

- Enhanced-monitoring measures: Strengthen monitoring (set up traps)
- Blocking measures: Prevent backdoors and hijacking

Figure 2.1.3-1 Approach for Deriving System Design Measures

(2) Key Points of System Design Measures

With targeted email attacks, not depending solely on the automatic defense enabled by the blocking measures but **knowing a full picture of the attack as early as possible**, such as knowing the answer to the questions like “at which phase the attack stealthily compromising the internal system is right now?” or “is it already at the final phase of sending out the stolen information or destroying the system?”, **will help the organization avoid the worst case scenario**. The “enhanced-monitoring measures” would enable that. The key points we focused when formulated the measures are the following. (For more details, see 3.2 System Design Measures Based on System Design Model).

- Conduct the mock attacks based on the attack objective (criteria of success) and techniques at each phase of the attack scenario, adding the psychological elements that could possibly affect the attacker (Identify where the attacker may likely make a mistake)
- If the attack succeeds, formulate the design measures that can prevent the attack, verify its behavior and shape the measures.
- Conduct the mock attacks **to verify the effectiveness of the measures again**.

(3) Organization of the Set of the System Design Measures

The set of the system design measures **consists of the “list of technical design measures (system design outline)” and “implementation guide (how to use the technical design measures in combination and operational issues)”**.

In addition, some support information which will help the reader understand the goal of this guide and possible threats, customize the design measures and implement them into the reader’s system accordingly to its environment and characteristics is provided in the later chapter. Also, some other helpful information, such as about the organizational approach toward the incidents (a response system to escalate the information within the organization when a critical attack happens), and the relationship between the design measures and corresponding emergency mitigation measures, is provided in 3.2 System Design Meausres Based on System Design Model. Below is an image of the organization of the set of the system design measures.

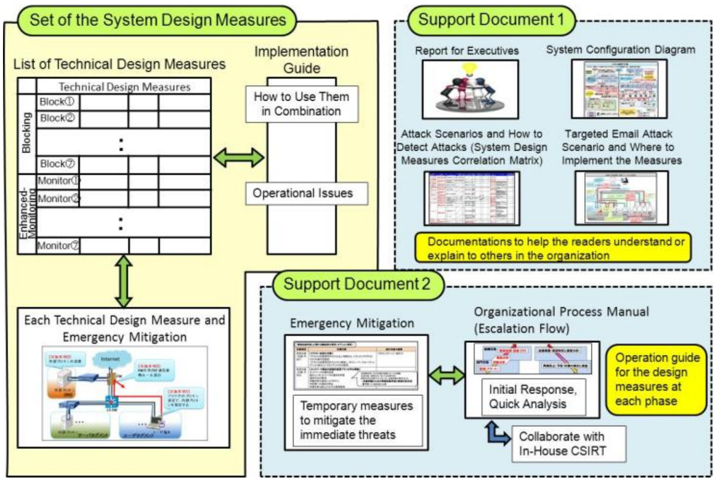

Set of the System Design Measures
List of Technical Design Measures
Technical Design Measures
Blocking
Block①
Block②
:
Block⑦
Enhanced-Monitoring
Monitor①
Monitor②
:
Monitor⑦
Implementation Guide
How to Use Them in Combination
Operational Issues
Each Technical Design Measure and Emergency Mitigation
Support Document 1
Report for Executives
System Configuration Diagram
Attack Scenarios and How to Detect Attacks (System Design Measures Correlation Matrix)
Targeted Email Attack Scenario and Where to Implement the Measures
Documentations to help the readers understand or explain to others in the organization
Support Document 2
Emergency Mitigation
Temporary measures to mitigate the immediate threats
Organizational Process Manual (Escalation Flow)
Initial Response, Quick Analysis
Operation guide for the design measures at each phase
Collaborate with In-House CSIRT

Figure 2.1.3-2 Image of the Set of the System Design Measures

2. 2 Set of System Design Measures

This chapter introduces the contents of the set of the system design measures. The IPA Threat and Countermeasure Study Group has derived the “enhanced-monitoring measures” from the intrusion-detection perspective and “blocking measures” from the intrusion-prevention perspective.

The “**enhanced-monitoring measures**” are the design measures **focused on letting the system defender and operators detect the attacker’s attacking infrastructure building and inside operations within the system as early as possible** by setting up the traps and enhancing monitoring.

The “**blocking measures**” are the design measures focused on enabling to avoid the attacks such as establishing connect-back channels, hacking/hijacking servers and stealing passwords by designing the system to expect and prepare for the attacks predicted in the attack scenarios.

In some cases, the venders may differ for the system design/development and operation/maintenance. Even so, as a contractor, the organization should check with the contractee (respective vendors) to see if the measures work for the organization and consider the deployment of the enhanced-monitoring and blocking measures. The set of the system design measures is intended to be used as an interface in such contract negotiations between the parties. In the following, the system design measures at the attacking infrastructure building phase and penetration/exploration phase - the core of the targeted email attack – are explained.

(1) Attacking Infrastructure Building Phase

The goals of the measures at the attacking infrastructure building phase are below:

① To detect and block the connect-back traffic

② To detect and block the attacker’s penetration/exploration operation

Table 2.2-1 System Design Measures at the Attacking Infrastructure Building Phase (1/2)

	No.	Measures	Description	Device
Blocking Measures	B①	Block connect-back traffic with Firewall (FW) (See 2.2.1)	Block connect-back traffic at firewall based on the design of network communication paths	･FW ･Proxy Server
	B②	Block connect-back traffic with access control at proxy server (See 2.2.2)	Block connect-back traffic with access control at the proxy server	･Proxy Server
	B③	Block connect-back traffic with proxy authentication (See 2.2)	Block illegitimate communications with proxy authentication	･Proxy Server
Enhanced Monitoring Measures	EM①	Monitor and analyze the proxy authentication log (See 2.2.4)	Analyze the proxy server’s authentication log and look for connect-back traffic	･Proxy Server
	EM②	Uncover connect-back traffic through forced-disconnection (See 2.2.5)	Disconnect all communications that go through the proxy server and uncover connect-back traffic that try to reconnect with the C&C server by checking the logs recorded after the event of forced disconnection.	･Proxy Server
	EM③	Detect http communications that mimic browser communications	Using the proxy server, monitor the difference in the characteristics between the browser’s HTTP communications and HTTP communications mimicked by malware. **【Work In Progress】**	･Proxy Server

B: Blocking Measures EM: Enhanced-Monitoring Measures

Table 2.2-1 System Design Measures at the Attacking Infrastructure Building Phase (2/2)

	No.	Measures	Description	Device
Enhanced-Monitoring	EM④	Monitor the specific services using the unused IP addresses	Set up monitoring devices (e.g. decoy server[7]) with the unused IP addresses and monitor the indicators that might suggest the penetration/exploration operation by the attacker **【Work In Progress】**	･Network

(2) Penetration/Exploration Phase

The goals of the measures at the penetration/exploration phase are below:

① To prevent the attack from infiltrating the internal system deeper

② To Prevent the attack from stealing the account information from the user PCs

Table 2.2-2 System Design Measures at the Penetration/Exploration Phase

	No.	Measures	Description	Devices
Blocking Measures	B④	Segment network for operation terminals and user PCs (See 2.2.6)	Segment the network for the user PCs and operation terminals and make sure that the user PCs cannot access the operation terminals.	･User PC ･Operation Terminal
	B⑤	Implement network segmentation and access control (See 2.2.7)	Implement proper network segmentation and access control between network segments	･Network Devices
	B⑥	Ban to cache highly-privileged admin account (See 2.2.8)	Do not cache the highly-privileged administrative account information (e.g. Domain Admins)	･User PCs
	B⑦	Ban to share files among user PCs (See 2.2.9)	Prohibit (disable) file sharing among the user PCs and allow to share with only minimally necessary devices such as file servers.	･User PCs
Enhanced-Monitoring	EM⑤	Monitor and analyze access log for trap accounts (See 2.2.10)	Set up the trap accounts on the user PCs and detect the login attempts using the trap accounts by the attacker.	･User PCs ･Authentication Server (AD)
	EM⑥	Monitor the listening ports newly opened	Monitor the listening ports newly opened for connect-back channels **【Work In Progress】**	･Server
	EM⑦	Monitor hacking commands	Monitor the use of the commands that are unlikely used for operation/maintenance but often used for hacking **【Work In Progress】**	･Server

B: Blocking Measures　EM: Enhanced-Monitoring Measures

In the following sections, each system design measure is further explained. For those marked【Work In Progress】, we are still working to verify the technical issues and effect on operation/maintenance. They will be updated upon completion.

[7] A server that acts as a decoy to be attacked on behalf of the target and records the detail of the attacks.

【Blocking Measure ①】

2. 2. 1 Block Connect-Back Traffic with Firewall

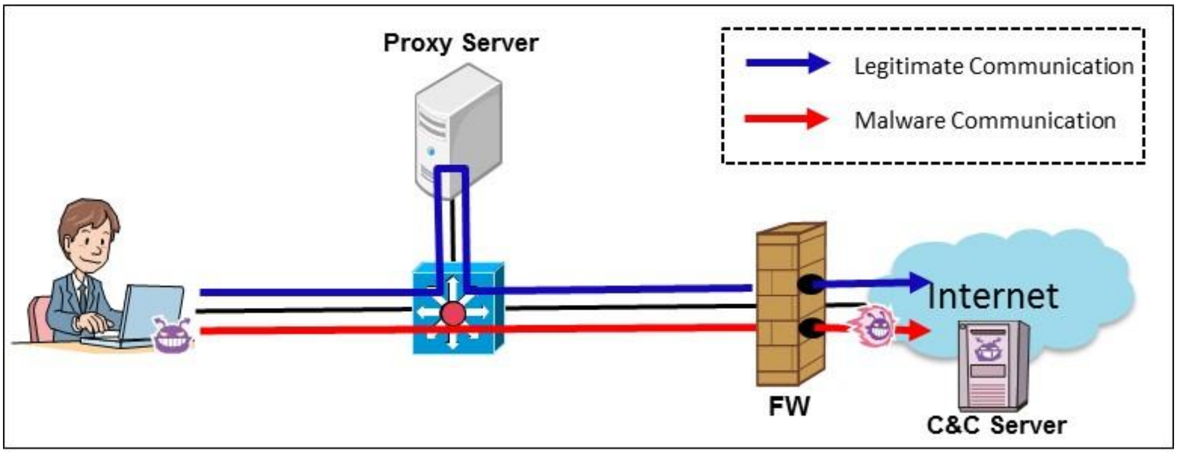


Figure 2.2.1-1 Attacking Image: Before Implementing the Measure

There are a certain number of malware that do not support the proxy settings. This measure sets a rule that a program must use the proxy server to access the external network, aiming to block the malware's connect-back traffic that does not follow the rules at the firewall (FW).

(1) System Design Overview

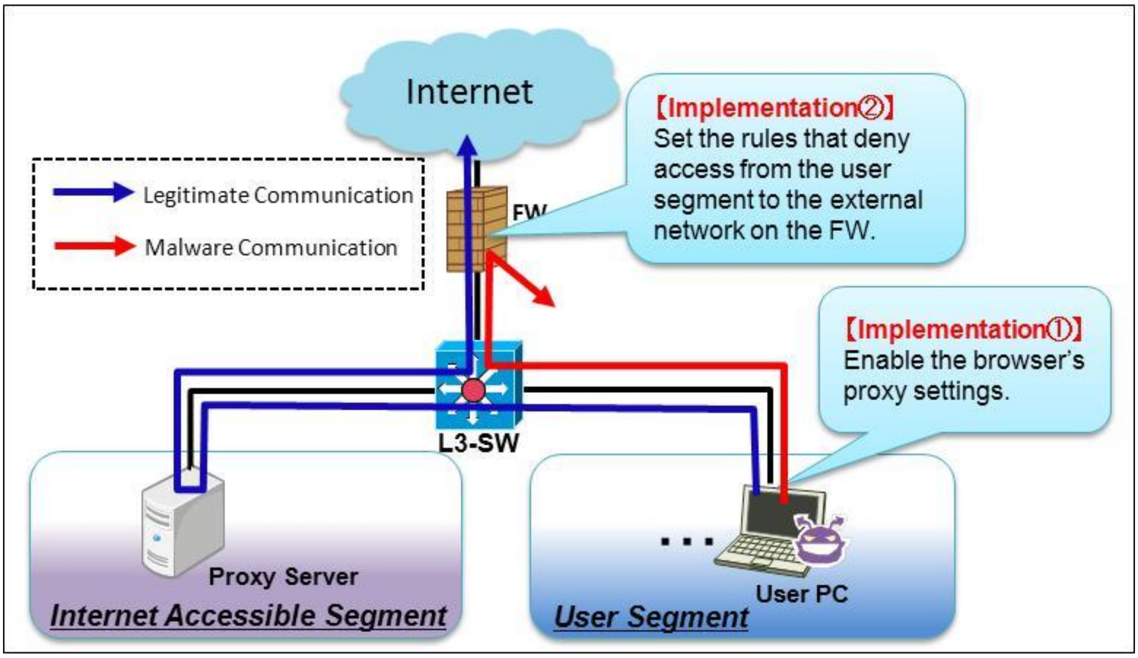

Internet
Legitimate Communication
Malware Communication
FW
【Implementation②】
Set the rules that deny access from the user segment to the external network on the FW.
【Implementation①】
Enable the browser's proxy settings.
L3-SW
Proxy Server
Internet Accessible Segment
・・・
User PC
User Segment

Figure 2.2.1-2 Image of the System Design Measure

Configure the FW to permit the legitimate services that follow the browser's proxy server settings to pass the FW. On the other hand, block the malware's attempts to access the external server that do not go through the proxy server at the FW. By configuring the FW this way, it makes it possible to block the malware's connect-back traffic that does not support the proxy settings.

【Implementation①: Enable the browser's proxy settings】

For the user PCs that access the Internet, mandate the use of the organization's proxy server in the browsers. In combination with the implementation ②, deny the user PCs on which the proxy settings in the browser are disabled access to the Internet directly.

【Implementation②: Set the rules on FW that deny access from the user segments to the outside】

Set and apply the following rules to block the outbound traffic on the FW.

- Permit the outbound traffic via the proxy server only and block the outbound traffic from the devices that attempt to access the Internet directly without using the proxy server
- Block the outbound port 80 and 443 traffic that have not gone through the proxy server for they can be a connect-back traffic to the C&C server
- Design the services that need to access the outside network over the port 80 and 443 to use the proxy server (except the special devices deployed in the DMZ)

Table 2.2.1-1 Examples of the Services That Should Use the Proxy Server

Services	Applied For
Windows Server Update Services (WSUS)	Communicate with the Windows Update Server (80,443)
System Center Configuration Manager (SCCM)	E.g. Update non-Microsoft products, asset management
Anti-virus software	Update virus pattern files
Security patch management software	Obtain things like the latest patch and virus pattern files
Others	E.g. License verification

【NOTE】

If software uses the online update feature and does not support the proxy settings, consider alternative way, such as offline update via the file server.

(2) Operational Issues

【Operation①: Check the FW access log (block entries) periodically】

Periodically monitor the access log (block entries) of the FW and see if there is connect-back traffic attempted by the user PCs. If there are access log entries (block entries) that suggest a user PC has attempted to connect the Internet directly over the port 80 or 443 but was blocked and failed, investigate the user PC, for it may be infected with malware.

【Operation②: Review the FW access control rules】

Periodically review the FW access control rules and see if there are still necessary.

【Blocking Measure ②】

2．2．2 Block Connect-Back Traffic with Access Control at Proxy Server

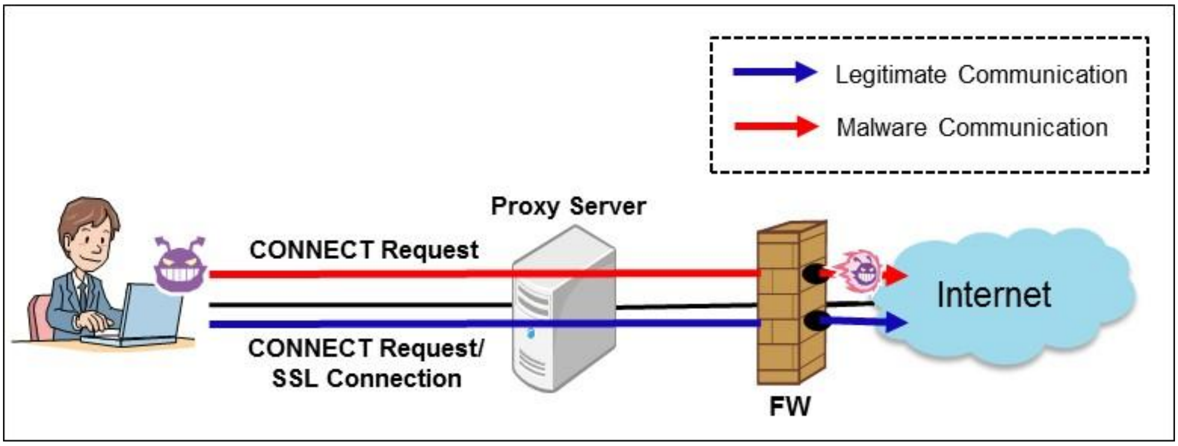


Figure 2.2.2-1 Attacking Image: Before Implementing the Measure

The CONNECT method is a feature of HTTP1.1 to request a proxy server for a tunnel connection. In general, it is used to tunnel the data encrypted by the protocols such as SSL/TLS. Some malware are known to exploit this feature and issue a CONNECT request to the proxy server to connect the Internet.

This measure aims to permit only the CONNECT requests issued by the programs that do need to access external servers over the HTTPS port (typically TCP/443 is used) to pass, and block all other traffic.

(1) System Design Overview

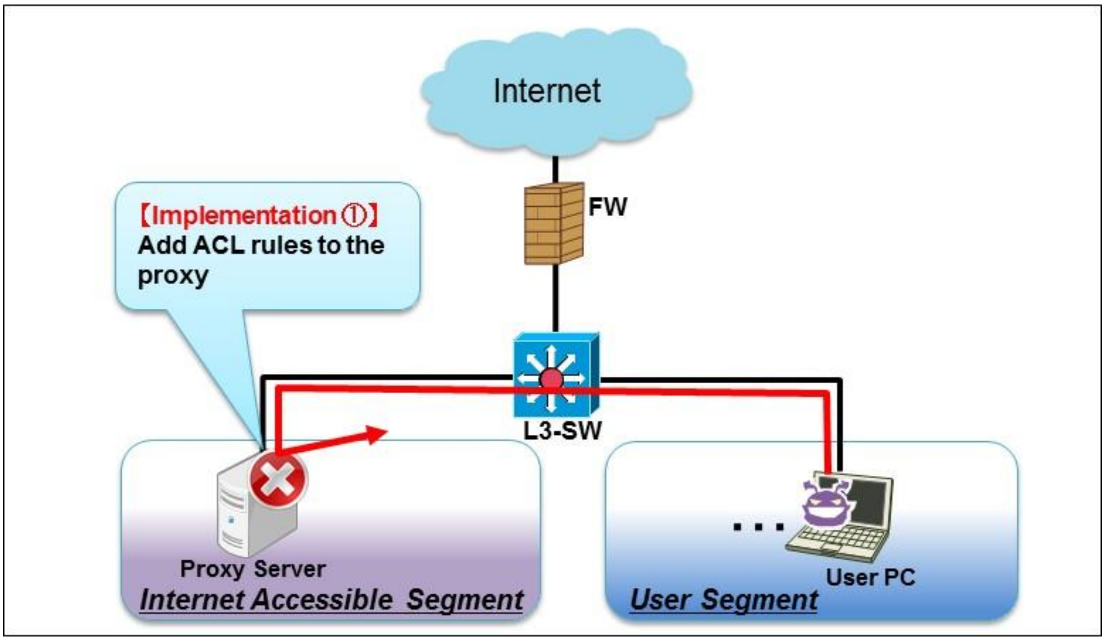


Figure 2.2.2-2 Image of the System Design Measure

For the outbound traffic from the user PCs to the Internet through the proxy server, configure the proxy server to limit the ports that can be used to the minimum (e.g. HTTP and HTTS only), and block all traffic that use the ports other than the permitted, legitimate ones at the proxy server. By designing this way, it makes it possible to detect and block the malware's connect-back traffic that uses the ports the organization does not normally use.

【Implementation①: Add the ACL rules to the proxy server】

Add the ACL rules that block all traffic "that use the CONNECT method but do not use 443/TCP".

```
# Deny all CONNECT requests that do not use the SSL-designated port
acl SSL_ports port 443
acl CONNECT method CONNECT
http_access deny CONNECT ! SSL_ports
[ snip ]
# Modify the log format, for example, to log the time in a format that is easy to understand
logformat combined %>a %ui %un [%tl] "%rm %ru HTTP/%rv" %>Hs %<st "%{Referer}>h"
"%{User-Agent}>h" %Ss:%Sh
access_log /var/log/squid/access.log combined
```

Figure 2.2.2-3 Example of ACL rules on Squid

【NOTE】

If the business systems are using the CONNECT method for something other than SSL communications, allocate the port numbers for those use and add them to the ACL rule as well.

(2) Operational Issues

【Operation①: Check the proxy server's access log (block entries) periodically】

Periodically monitor the access log (block entries) of the proxy server and see if there are connect-back traffic attempted by the user PCs. If there are access log entries (block entries) that suggest a user PC used the CONNECT method and attempted to connect the Internet via the unpermitted ports, investigate the user PC, for it may be infected with malware.

(See:3.4 Analysis Rusult of Proxy Server Log)

When a CONNECT request is made via the unpermitted port, a log entry like below will be recorded.

```
(src IP address) - - [30/Jul/2013:20:52:11 +0900] "CONNECT (dst IP Address):(port number) HTTP/1.1" 403
3355 (referrer) (user agent) TCP_DENIED:NONE
```

Figure 2.2.2-4 Example of access.log Output

【Operation②: Review the proxy server's access control rules】

Periodically monitor the access log. See if the traffic related to the business (legitimate traffic) is not blocked and review the proxy server's access control list (ACL) accordingly.

【Blocking Measure ③】

2．2．3 Block Connect-Back Traffic with Proxy Authentication

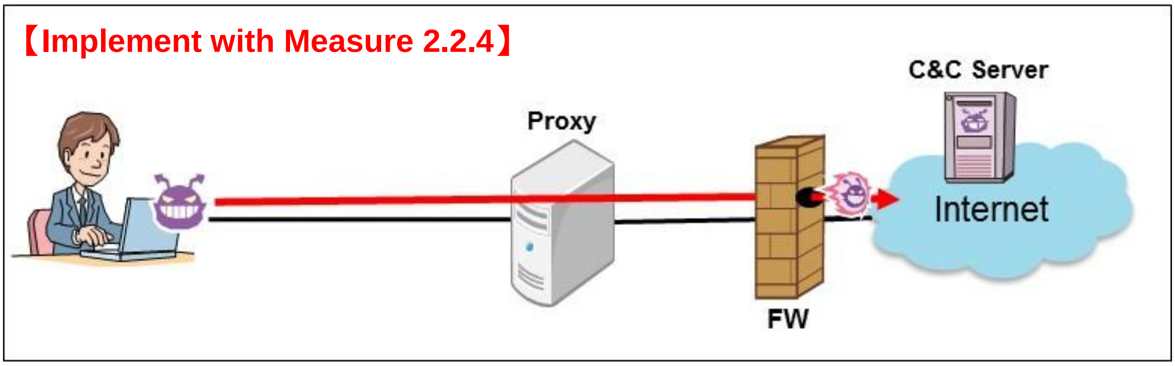


Figure 2.2.3-1 Attacking Image: Before Implementing the Measure

There are a certain number of malware programs that do not support the proxy authentication. This measure aims to block the connect-back traffic using the proxy authentication when a malware that does not support the proxy authentication tries to connect the external network through the proxy server.

In addition, by using it in combination with 2.2.4 Monitor and Analyze Proxy Authentication Log, we can expect a synergistic effect.

(1) System Design Overview

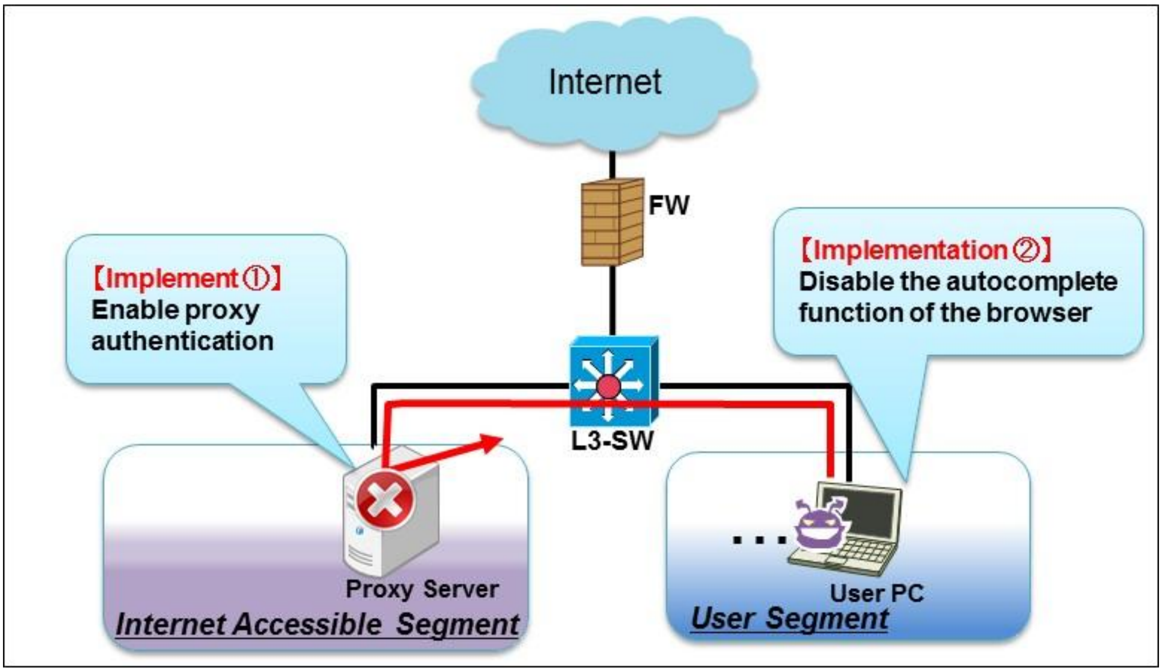

Internet
FW
【Implement①】
Enable proxy authentication
【Implementation②】
Disable the autocomplete function of the browser
L3-SW
Proxy Server
Internet Accessible Segment
User PC
User Segment

Figure 2.2.3-2 Image of the System Design Measure

Implement user authentication for the traffic that goes through the proxy server and permit only those successfully authenticated to pass it through. By designing this way, it makes it possible to block the malware’s connect-back traffic that does not support the proxy authentication at the proxy server.

【Implementation①：Enable Proxy Authentication】

It is recommended that a proxy server satisfy the following requirements.

- ➢ Have a user management functionality or is able to use a directory service
- ➢ Can authenticate by user
- ➢ Can use a safer authentication method such as the Digest or NTLM authentication

【NOTE】
It is not recommended to use the Basic authentication since it sends the ID/PW in plain text into the network.

【Implementation②：Disable the browser’s autocomplete function】

If the browser’s autocomplete function[8] is enabled and used, the ID/PW is stored on the user PC, which allows the attacker to steal the user credential. Make sure that the users cannot use the autocomplete function through some means, such as a group policy, and have them enter the ID/PW each time they open a browser.

(2) Operational Issues

【Operation①：Manage user accounts properly】

Manage the user accounts used for the proxy authentication properly. To make sure that unnecessary accounts are all deleted, a periodic review is needed as people’s duty and department change within the organization. By linking and using an authentication server (e.g. Active Directory or LDAP server), a total user management can be achieved.

【Operation②：Monitor and analyze the authentication log of the proxy server】

Monitor and analyze the authentication log of the proxy server, look for indicators of unauthorized access. (For more details, see 2.2.4 Monitor and Analyze Proxy Authentication Log).

[8] A browser function that presents possible word entries the user may be about to enter based on the past input history when the user inputs data.

2. 2. 4 Monitor and Analyze Proxy Authentication Log

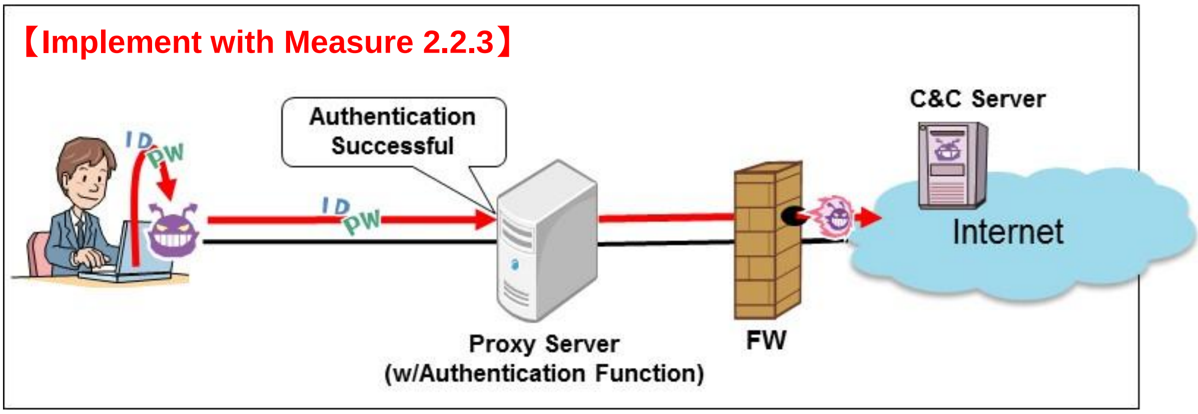

【Implement with Measure 2.2.3】
ID
PW
Authentication Successful
ID
PW
C&C Server
Internet
Proxy Server
(w/Authentication Function)
FW

Figure 2.2.4-1 Attacking Image: Before Implementing the Measure

There are malware programs that obtain user credentials stored in the user PCs through some means, such as through the autocomplete function, and get by proxy authentication. This measure aims to improve the capability to conduct further investigation into the malware and attacker utilizing the authentication log recorded by the proxy server.

In addition, by implementing this in combination with 2.2.3 Block Connect-Back Traffic with Proxy Authentication, we can expect a higher effect.

(1) System Design Overview

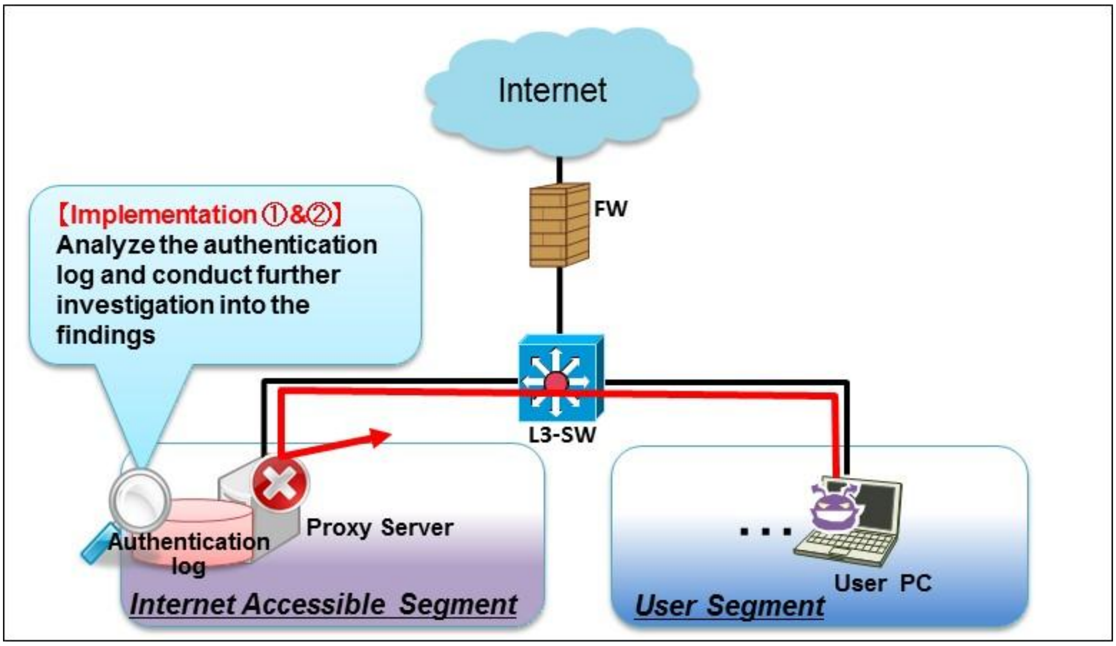

Internet
FW
【Implementation ①&②】
Analyze the authentication log and conduct further investigation into the findings
L3-SW
Proxy Server
Authentication log
Internet Accessible Segment
・・・
User PC
User Segment

Figure 2.2.4-2 Image of the System Design Measure

Enable proxy authentication and configure it to log the results of user authentication (success/failure). By designing this way, it is expected to detect possible connect-back channels from the authentication log and deal with them early.

【Implementation①: Enable proxy authentication】

Employ the implementation requirements suggested in 2.2.3 Block Connect-Back Traffic with Proxy Authentication. It is recommended that the ID/PW used for authentication be not shared among the users and be issued to each user.

(2) Operational Issues

【Operation①: Analyze authentication log of the proxy server】

Monitor the entries about the success and failure logged in the proxy server's authentication log periodically and see if malicious acts like the following have been attempted.

- Brute force attacks[9] against a specific user ID

  If a specific user ID is targeted by brute force attack, a huge volume of failure entries for the specific user ID will be logged within a short period of time. Thus, if a more than certain amount of failure entries is logged within a certain period of time, the user PC with that problematic user ID should be checked out.

- Different IDs being tried for a specific PW

  If the attacker attempts to find the correct ID that matches a specific password by trying different IDs against the specific password, the authentication log will show a failure entry for the different user IDs sent from a specific user PC. Look through the log to check that such events have not taken place for the user PCs per IP address.

- User ID reuse

  If the attacker tries to exploit the user ID/PW reuse and it works, the authentication log will show success entries for the same user ID from the different user PCs. Look through the log to check that such events have not taken place for the user PCs per IP address. Note that an IP address may be assigned by DHCP. In that case, check must take into account the expiration date of the IP address.

【Operation② : Conduct further investigation into the findings from the log analysis】

Based on the findings from the authentication log analysis done in operation①, identify and investigate the user PCs that are possibly being exploited for unauthorized communication. Since the user IDs used in the suspicious success entries are most likely compromised, change their password and conduct investigation into the user PC used by the owner of the compromised user ID.

[9] An attack technique to check all possible combination of keys and strings to crack a password.

【Enhanced-Monitoring Measure ②】

2．2．5 Uncover Connect-Back Traffic through Forced-Disconnection

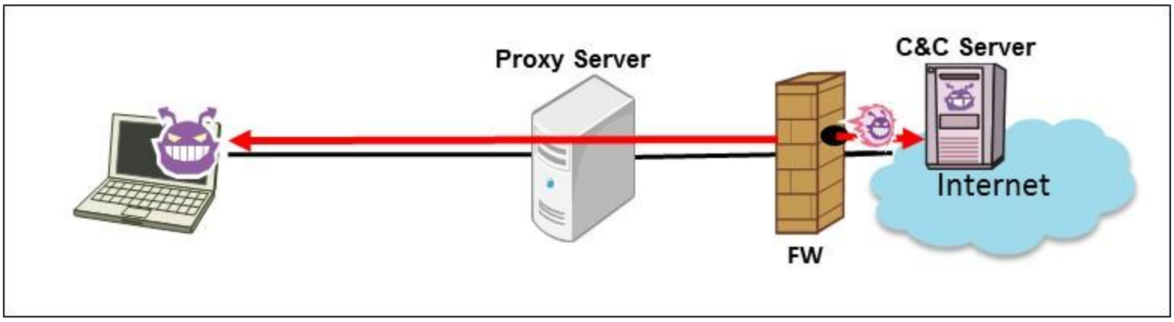


Figure 2.2.5-1 Attacking Image: Before Implementing the Measure

To receive the instructions from the C&C server, malware tries to maintain the connection with it. This measure aims to uncover connect-back traffic that automatically tries to reconnect to the C&C server by periodically forcibly disconnecting all the outbound connections through the proxy server.

(1) System Design Overview

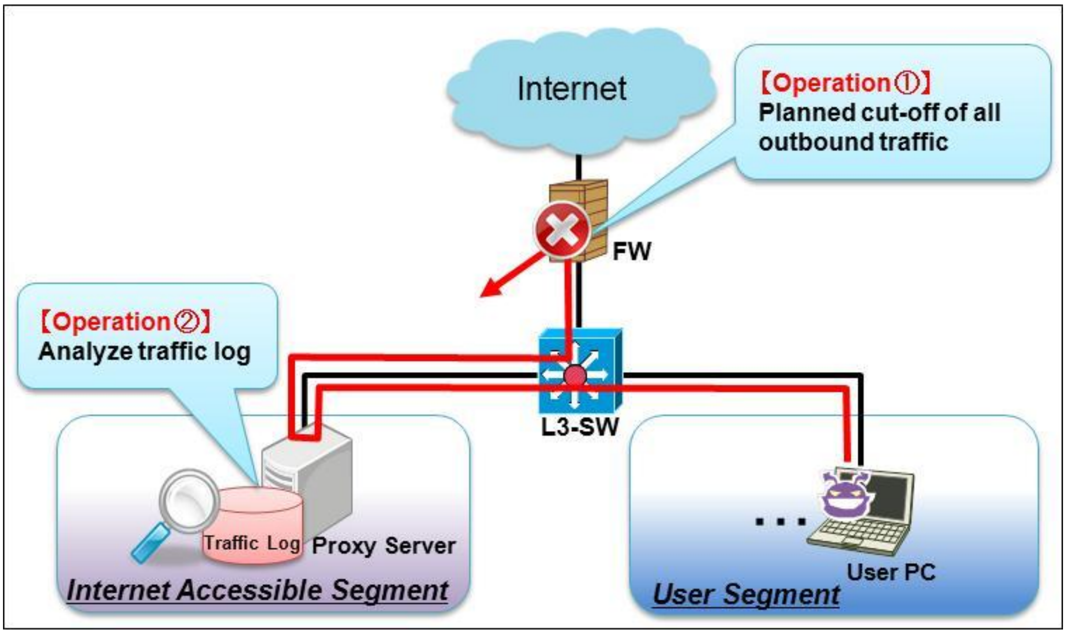


Figure 2.2.5-2 Image of the System Design Measure

Block all outbound communications that go through the proxy server mandatorily at the FW. This will prompt the malware to try to reconnect the C&C server to recover its connect-back channel. The measure makes it possible to discover unauthorized communications early by logging such traffic on the proxy server.

【Implementation①: Enable the browser’s proxy settings】

【Implementation②: Set the rules that deny outbound traffic on the FW】

Employ the implementation requirements suggested in 2.2.1 Block Connect-Back Traffic with Firewall and configure to make all business traffic go through the proxy server to access the external network.

(2) Operational Issues

【Operation①：Planned forced-disconnection of outbound traffic】

By mandatorily cutting off all communications that go through the proxy server using the filtering feature of the FW or server in the off-peak business hours like at night, uncover the malware's connect-back channels that regularly try to reconnect to the C&C server. To check the regularity, it is effective to perform mandatory disconnection at least twice.

In addition, if the business traffic is present in the proxy server's traffic log, it makes harder to distinguish the malware traffic from business traffic. Thus, **it is recommended to notify the employees and staff of keeping their PC power-on but unused during the mandatory disconnection in advance.**

【NOTE】
The business servers are assumed to obtain data like the pattern files and update information from the outside. Therefore, it is recommended that the servers' access to the Internet be permitted.

【Operational Issue②：Analyze traffic logs】

Check the traffic logs after the forced disconnection and see if there are any attempts that try to regularly reconnect to the outside. Track down the user PCs responsible for the detected connect-back traffic based on the source and destination IP.

【Blocking Measure ④】

2. 2. 6 Segment Network for Operation Terminals and User PCs

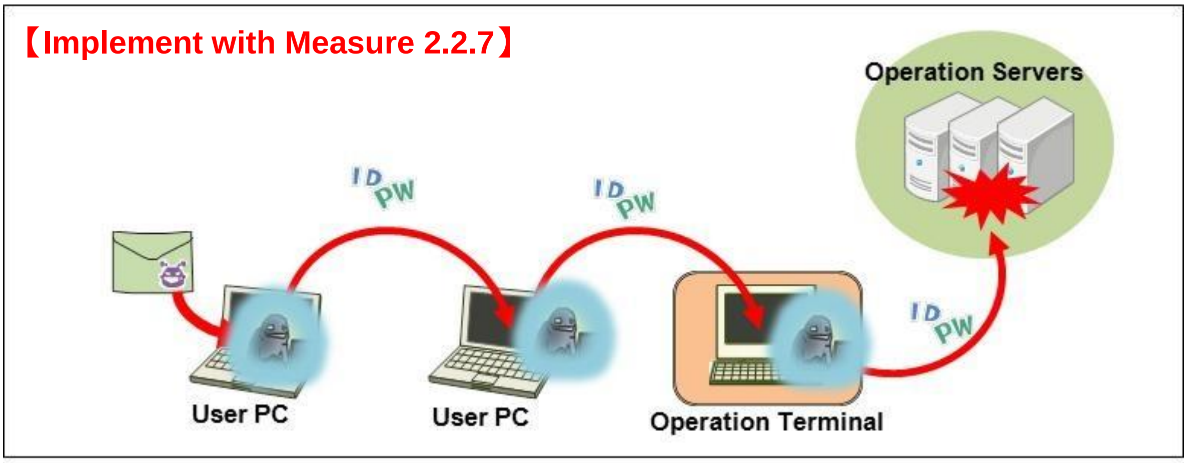


Figure 2.2.6-1 Attacking Image: Before Implementing the Measure

At the penetration/exploration phase, the attacks have been observed where the ID/PW required for operation and maintenance was stolen and exploited. This measure aims to prevent the operational information from being stolen by the attacker who has infiltrated into the system, and stop unauthorized access to the operation servers by applying network segmentation for the operation terminals and user PCs.

In addition, by implementing this in combination with 2.2.7 Implement Network Segmentation and Accesss Control, we can expect a highly positive effect.

(1) System Design Overview

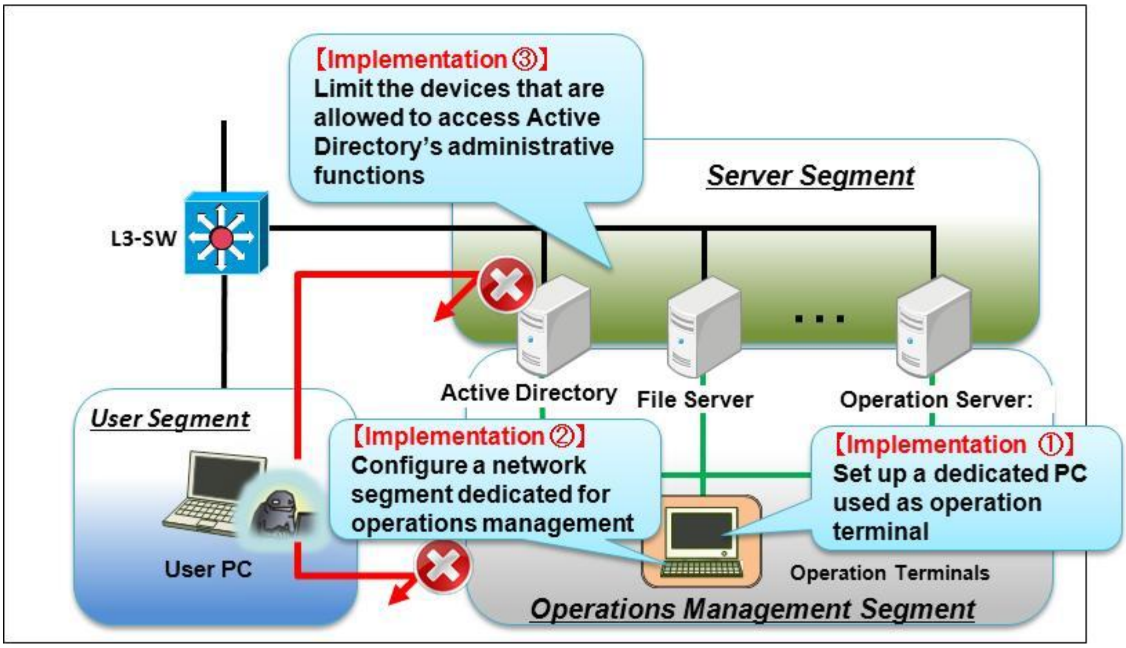

【Implementation ③】
Limit the devices that are allowed to access Active Directory's administrative functions
Server Segment
L3-SW
Active Directory
File Server
Operation Server:
User Segment
User PC
【Implementation ②】
Configure a network segment dedicated for operations management
【Implementation ①】
Set up a dedicated PC used as operation terminal
Operation Terminals
Operations Management Segment

Figure 2.2.6-2 Image of the System Design Measure

Configure the network in such a way that even if the user PCs are infected with malicious programs, the operation terminals are unreachable and cannot be hijacked by segmenting their network. Also, as for the critical servers such as the Active Directory, mitigate the risk of unauthorized access by limiting the devices that are allowed to access Active Directory's management features to the specific terminals. By designing this way, it makes it possible to prevent the attacker who has managed to hijack a user PC from gaining a direct access to the operation servers.

【Implementation①：Set up a dedicated PC as operation terminal】

Prepare operation terminals that meet the following requirements and permit management and maintenance operation of servers and network devices only from those operation terminals.

- ➢ No Internet connection (services) allowed, such as emailing and browsing (it is recommended to use an operations management server located within the internal network for security patch deployment and pattern file update)
- ➢ Do not store credential information for servers and network devices in the operation terminals in any way

In the case where some business departments run their own system individually, they tend not to have a dedicated operation terminal separately due to their small system size. Even so, the organization should have those business departments set up a dedicated operation terminal and maintain the segmentation as an organization-wide effort.

【Implementation②：Configure a network segment dedicated for operations management】

Configure a network segment dedicated for operations management that cannot be accessed from other segments, and put the operation terminals there. In addition, make sure access from the user segments to operations management segment is prohibited.

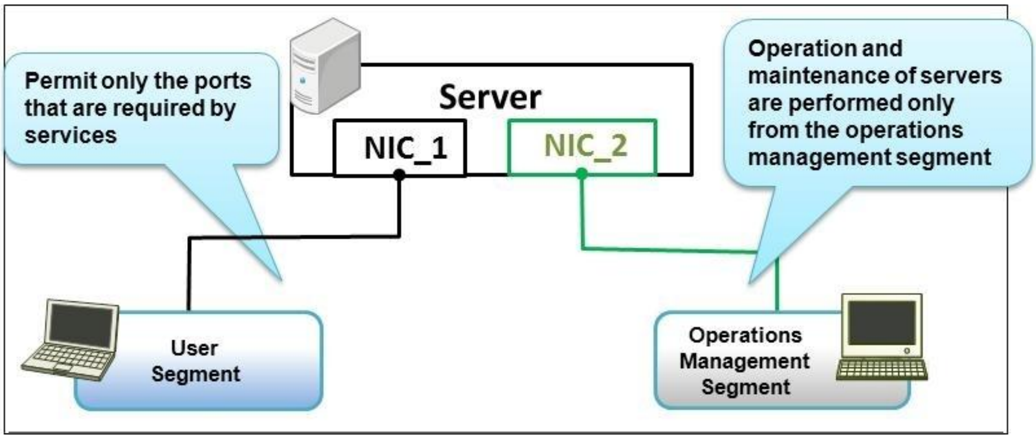

Permit only the ports that are required by services
Server
NIC_1
NIC_2
Operation and maintenance of servers are performed only from the operations management segment
User Segment
Operations Management Segment

Figure 2.2.6-3 Image of Operations Management Segment

An operations management segment can be configured by creating a LAN using a different LAN port that is connected to the server segment, or using a special LAN port that is dedicated for the operation terminal.

Also, make sure that the operation servers are not accessible from the user segments via the SSH port or other ports that the operation terminals use for the operations management, such as the port used by web client GUI. Moreover, make the operations management segment a dedicated segment available only for the system administrators and closed to the general users.

When performing remote maintenance, design the network to do it via a transit server[10] by setting up the transit server that provides the authentication, user management and log management function in front of the operation servers. By designing this way, it makes unauthorized access to the operation servers difficult and makes it easier to find indicators of unauthorized access from authentication logs,

【Implementation ③: Limit the devices allowed to access Active Directory's administrative functions】

Because Active Directory holds the credentials for all users in its administration domain, it tends to be targeted for infiltration. Thus, access to Active Directory's administrative functions should be treated with special caution and it is important to implement access control through a policy to allow only the specific devices to access with the administrative privilege.

(2) Operation Issues

【Operation ①: Use and manage administrator accounts properly】

Manage the operation terminals properly to make sure that unauthorized users cannot use them.

【Operation ②: Ensure security of the operation terminals】

Implement anti-virus measures and software vulnerability countermeasures to leave the operation terminals vulnerable.

(3) Emergency Mitigation

If configuring a network segment dedicated for operations management or having NIC for an operation terminal is infeasible, consider taking the following emergency mitigation measures to reduce the risk of hijacking of operation terminals.

- ➢ Connect an operation terminal to a user segment but do not keep it connected all the time. When system management is required, connect the operation terminal to the user segment and after operation is done, disconnect it from the user segment.
- ➢ Connect the operation terminal to a user segment but make sure it is dedicated for management works only and separated from the PCs that use the Internet and emails for work.
- ➢ Filter access to the operation server through IP address or such to make sure it is accessible only from the operations management terminal.

[10] A relay server between networks to be used when performing maintenance works on servers or network devices. We had been calling it a "stteping stone" server, but since the name also means a vulnerable server in the context of the attacking methods, this guide calls it a "transit server" to avoid confusion.

This page is intentionally left blank.

【Blocking Measure ⑤】

2. 2. 7 Implement Network Segmentation and Access Control

【Implement with 2.2.6】

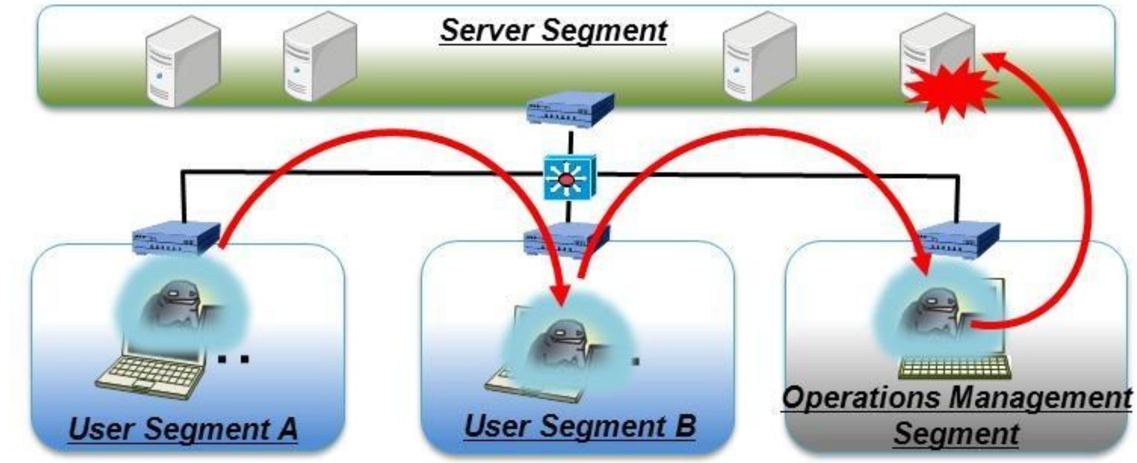


Figure 2.2.7-1 Attacking Image: Before Implementing the Measure

Occasionally, the cases are observed where the attacker exploits a flat network topology and breach all parts of the system at the Penetration/Exploration phase.

This measure aims to confine the breach and prevent the attacker from infiltrating deeper into the servers.

In addition, by implementing this in combination with 2.2.6 Segment Network for Operation Terminals and User PCs, we can expect a higher effect.

(1) System Design Overview

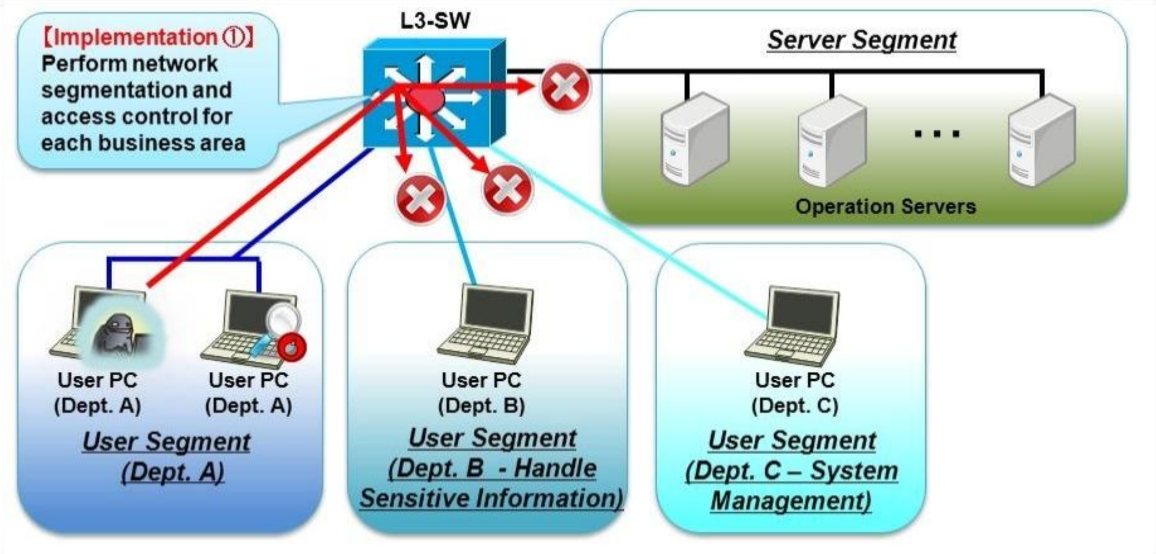

【Implementation①】
Perform network segmentation and access control for each business area
L3-SW
Server Segment
Operation Servers
User PC (Dept. A)
User PC (Dept. A)
User Segment (Dept. A)
User PC (Dept. B)
User Segment (Dept. B - Handle Sensitive Information)
User PC (Dept. C)
User Segment (Dept. C – System Management)

Figure 2.2.7-2 Image of the System Design Measure

It is important to design and implement appropriate network segmentation of the internal network in terms of the role and access requirements of each network, such as server segment, user segments and operations management segment, and minimize the communications between the segments. By implementing the proper network segmentation and access control, it will make the attacker's penetration attempt more difficult.

【Implementation ①: Implement network segmentation for business networks and access control】

Prevent the deeper infiltration by dividing the internal network into segments with network devices and minimizing the communications between them.

It is recommended that access control lists (ACL) be designed based on the matrix like the following - whether to permit the communications between two segments or which port to use for permitted communications. Table below is a sample model of segmentation and the real segmentation must be more detailed. The permit/denied notation in the table is just an example.

Table.2.2.7-1 Example: Access Control Design

		Destination Segment					
		Internet	DMZ	Server	User (Gen.)	User (Device)	Operation Management
Source Segment	Internet		○	×	×	×	×
	DMZ	○		○	×	×	×
	Server	○※1	○		××	×	×
	User (Gen.)	×	×	○		×	×
	User (Devices)	×	×	○	×		×
	Operations Management	×	×	○※2	×	×	

Legend: ○:Permitted, ×: Denied

※1 Assume the traffic from the proxy server or operations management server

※2 Include the communications required for patch management for the operation terminals and/or other necessary operation

(2) Operational Issues

【Operation ①: Revise ACL Periodically】

In time with the changes in the operational needs or system needs (modification or disposal), revise the ACLs between each segment to prevent an access control mechanism from falling into a mere façade.

【Blocking Measure ⑥】

2. 2. 8 Ban to Cache Highly-Privileged Admin Account

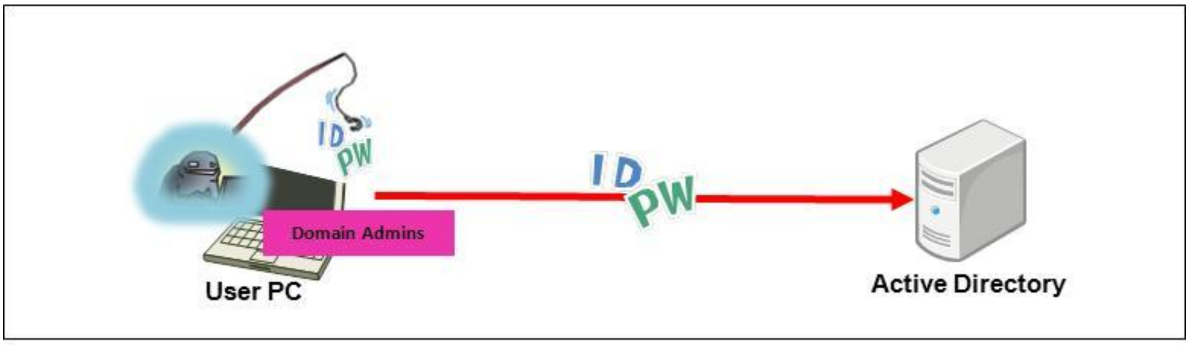


Figure 2.2.8-1 Attacking Image: Before Implementing the Measure

The attacker who has succeeded at infiltrating the internal system tries to steal the account information from the compromised user PC. If the information on a highly-privileged admin account, such as a Domain Admins group account, is stored in cache on the compromised user PC, the theft of that account information will greatly increase the risk of unauthorized access to the authentication servers (e.g. Active Directory). Nevertheless, the admin privileges may be required for operations like software autoupdate or remote maintenance and which left us few options: we just need to store the highly-privileged account information securely.

This measure aims to manage user accounts in a way that does not affect the authentication servers (Active Directory) or operation servers while allowing the necessary operations that require the admin privileges like remote patch distribution.

(1) System Design Overview

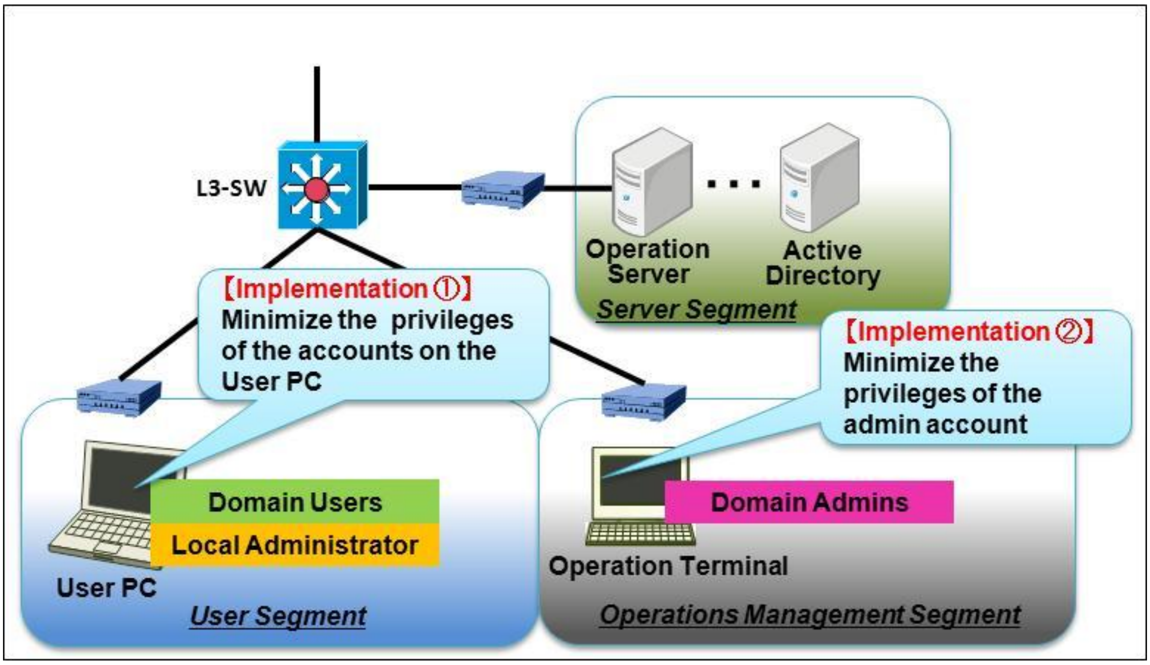


Figure 2.2.8-2 Image of the System Design Measure

Use a highly-privileged account like a domain administrator only on the specific operation terminal and do not use it for the normal activity such as emailing and browsing. As for the operations with which the admin privileges are required on a user PC, such as for remote help desk support, design the system to execute the necessary operations with the local admin privileges only. By allowing the users the least privileges necessary for their work, even if the attacker manages to steal the user account information stored in the compromised user PC, it makes it possible to prevent the attacker from hijacking other devices (user PCs or servers) except the primarily-compromised one because the user account privileges for other PCs or servers are independent of those for the compromised user PC and the stolen user account privileges do not work on them.

【Implementation ①：Allow the least user account privileges for the accounts on the user PC】

Design the accounts on the user PCs in the following way to allow the least privileges.

- Domain user：the Standard privileges on the user PC
- Local user：the Administrator privileges on the user PC

Do not use the Domain Admins group lightly and design the user accounts following the least-privilege principle, for example, by having the user execute the programs with local administrator privileges. For the services and scheduled tasks on the user PC, avoid executing them with a highly-privileged account, such as a Domain Users group account, to the extent possible.

【Implementation ②：Use the Administrator account at a minimum】

By assigning an administrator account that is just for performing the activities that require the administrator privileges and using it only on a specific operation terminal, it makes it possible to prevent the administrator account information from carelessly being stolen and widely used.

(2) Operational Issues

【Operation ①：Do not log on to the user PC with a Domain Admins group account】

Do not allow to log on to the user PC with a highly-privileged account, such as a Domain Users group account. Moreover, check the authentication server’s (Active Directory’s) log regularly to see if someone is logged on to the user PCs with a Domain Admins group account.

【Blocking Measure ⑦】

2. 2. 9 Ban to Share Files Among User PCs

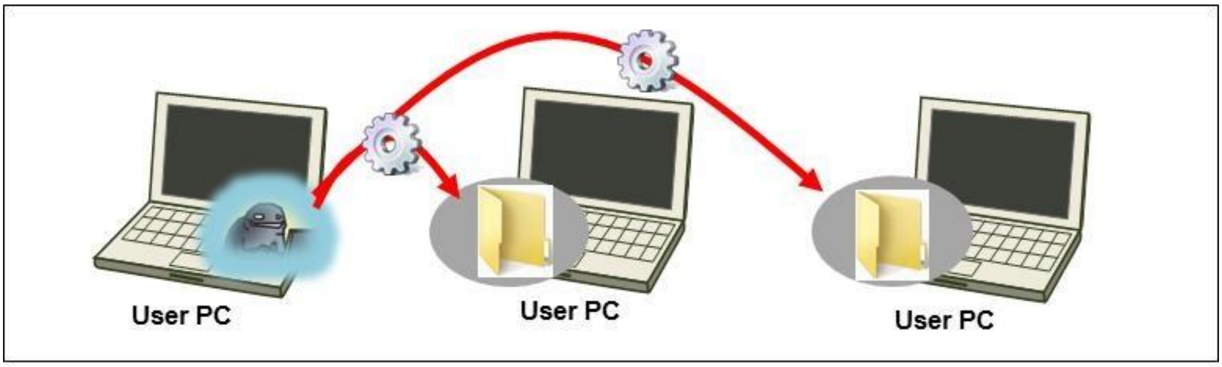


Figure 2.2.9-1 Attacking Image: Before Implementing the Measure

Occasionally, the cases are observed where the attacker exploits a file sharing feature on the user PC and infiltrate further into the network at the Penetration/Exploration phase. Nevertheless, banning file sharing completely can be difficult since it is used for operation as well, such as communication with an authentication server (Active Directory).

This measure aims to prevent deeper infiltration by limiting with whom the user PCs can share files to the devices that are absolutely necessary to share.

(1) System Design Overview

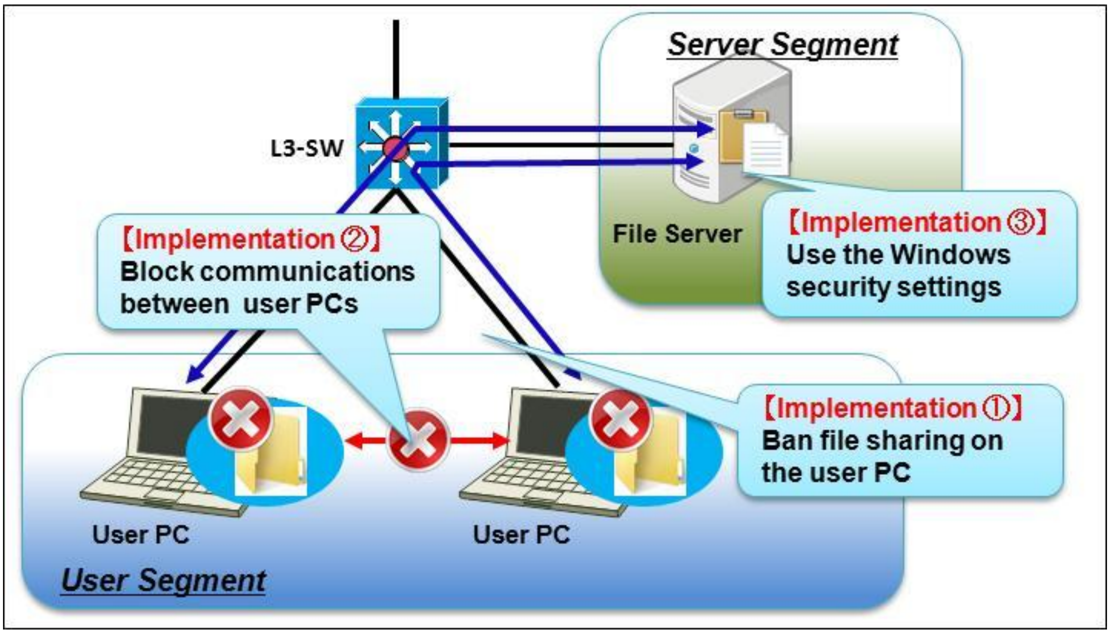


Figure 2.2.9-2 Image of the System Design Measure

Ban file sharing among the user PCs by disabling file sharing on the user PCs or blocking file sharing communications between the user PCs. By designing this way, it makes it possible to prevent the attacker from invading other user PCs via file sharing.

【Implementation ①: Disable the file sharing feature on the user PCs】

Disable the file sharing feature on the user PCs. Consider an option like banning new file sharing on a mandatory basis through an Active Directory group policy[11].

【Implementation ②: Block communications between user PCs】

If employing the Implementation ① is difficult, block communications between the user PCs using the access control feature that comes with a personal firewall, and permit to accept only the communications required for operation, such as auto-distribution of virus pattern files and security patches.

【Implementation ③: Utilize Windows Security Settings】

Microsoft Windows offers a remote maintenance tool for the servers and PCs called PsExec[12]. The attacker sometimes tries unauthorized access by exploiting PsExec, sending specific commands remotely and executing .exe files on the server. With the server operating systems including and later than Windows Server 2008, the User Account Control (UAC) feature is enabled by default, making PsExec unusable. Thus, if using Windows Server 2008 or later as an Active Directory or file server, keep the UAC feature enabled as it comes.

(2) Operation Issues

【Operation ①: Monitor suspicious processes】

If using Active Directory or file servers that run on a Windows OS, do not use PsECE for remote maintenance as an operational rule. In addition, monitor if a ”PsExecsvr” process is invoked not to miss an indicator of attacks.

[11] Enable or Disable File Sharing with Group Policy
http://technet.microsoft.com/en-us//library/cc754359%28v=ws.10%29.aspx

[12] Microsoft Technet　Windows Sysinternals　PsExec v2.0
http://technet.microsoft.com/en-us/sysinternals/bb897553.aspx

【Enhanced-Monitoring Measure ⑤】

2. 2. 10 Monitor and Analyze Access Log for Trap Accounts

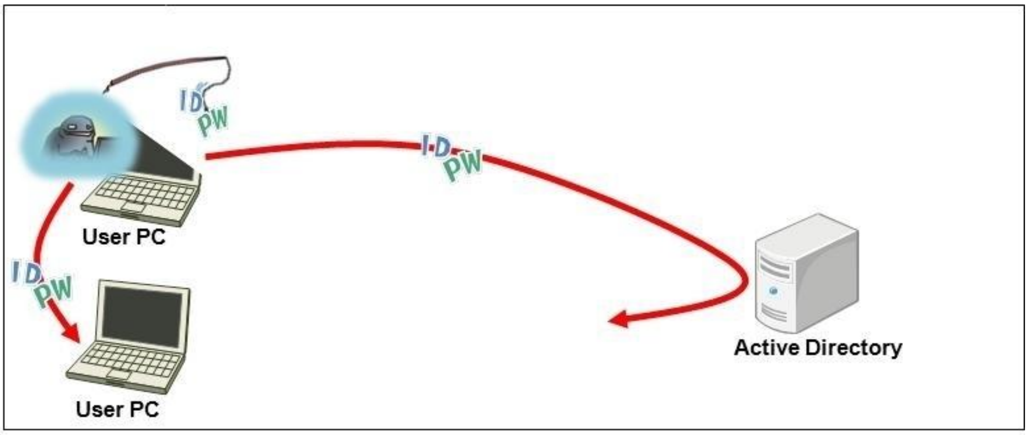


Figure 2.2.10-1 Attacking Image: Before Implementing the Measure

By exploiting the account information (ID/PW) stolen from the user PCs and servers the attacker succeeded in infiltrating, the attacker tries unauthorized access to more high-value servers (authentications servers (Active Directory) and operations management servers). To distinguish such unauthorized access from legitimate access is quite difficult because it is done with the legitimate user accounts.

This measure aims to distinguish between unauthorized access from truly legitimate access by setting up a trap account that is not used for work on the user PCs and monitoring intensively.

(1) System Design Overview

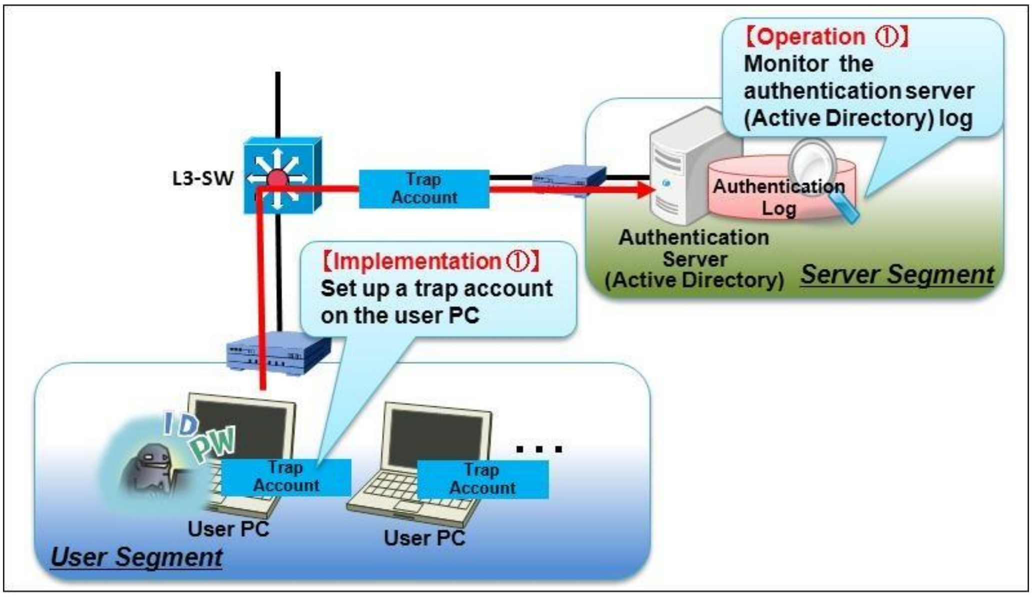


Figure 2.2.10-2 Image of System Design Measure

Set up and cache a fake user account that is not used for work on the user PC as a trap account to detect unauthorized access by monitoring the authentication server (Active Directory) log for the authentication entries recorded by that shouldn't-be-used trap account.

【Implementation ①: Set up a trap account on the user PC】

Set up and cache a trap account with a user name that intentionally suggests that the user must have high privileges (e.g. clientadmin01) on the user PCs used in the departments that handle confidential information or those that work with external entities a lot. To cache the trap account information on the user PC, log in to the user PC with that account.

【NOTE】

To make sure to prevent the attacker from exploiting the trap accounts, change the password for the cached trap accounts to a different one on the authentication server (Active Directory) to make the attacker's login attempts fail.

(2) Operational Issues

【Operation ①: Monitor the authentication server (Active Directory) log】

Monitor the authentication log for the trap accounts in the Active Directory's security event log. If there are the entries for the trap accounts, investigate the source user PCs in detail because it is likely that the attacker has attempted unauthorized access.

2．3 Organizational Approach

To avoid the damage from targeted email attacks, it is critical to implement the system design measures introduced in Section 2.2 to enable the organization's system to monitor and block attacks. Also, not to aggravate the damage, it is necessary to have an organizational structure and approach to properly handle the situation when an attack indicator is detected.

The way the targeted email attacks are used suggests that resulting disclosure of the confidential information through the attacks **may not be confined as an internal problem within an organization or department, but could become an organization-wide or even political, diplomatic issue.**

This section addresses the things to consider about **how to establish an organizational structure to prepare for such a worst case scenario**. **It is not for all organizations** but provided for those that feel a necessity.

Below are the examples of the issues to think about. Especially an idea shown in ⑥, which is expanding the role of a computer security incident response team (CSIRT) and utilizing it to improve the security measures to prevent recurrence, has not been strongly supported and the work of the CSIRT has been focused on analysis - independent of the effort by a security team. (E.g. Too much focus is placed on analysis and no collaboration with other relevant people/organizations is contemplated.)

The role and model of CSIRT vary depending on the organizations and it is important to **establish an organizational structure that is beyond the concept of just an "incident response"**.

Issues to Consider:

①What measures are used how at which step to lead it to an overall organizational response.

- What decisions should be made at each step and what information is necessary to make those decisions.
- What trigger should determine that it is the time to escalate to the next step.

②How to decide which decisions have more priority than others.

③How to decide which measures should be more appropriate and used at each step.

④What emergency avoidance (recovery) measures are available at the initial response.

- Formulate risk mitigation measures to enable information gathering to understand a full picture of the attack

⑤What role the CSIRT should play in the organization-wide response process.

- Redefine the role of the CSIRT in the organization and make it participate throughout the response process including the discussion on recurrence prevention measures.

⑥How to establish a mechanism to connect the incident response with recurrence prevention.

- Consider a mechanism that allows to utilize the result of monitoring and analysis into system design and operations management to help prevent recurrence.

Incidents vary and they may be confined at a department level or involve the entire organization and/or external entities, but in all incidents, **decision making of whether or not to escalate to the next step,** is required at each step from the initiation to closing of an incident response process.

The key points are how to gather necessary information to help make decisions and how to make decisions. The information that can be obtained by each function of the set of system design measures **are selected to help those decisions.**

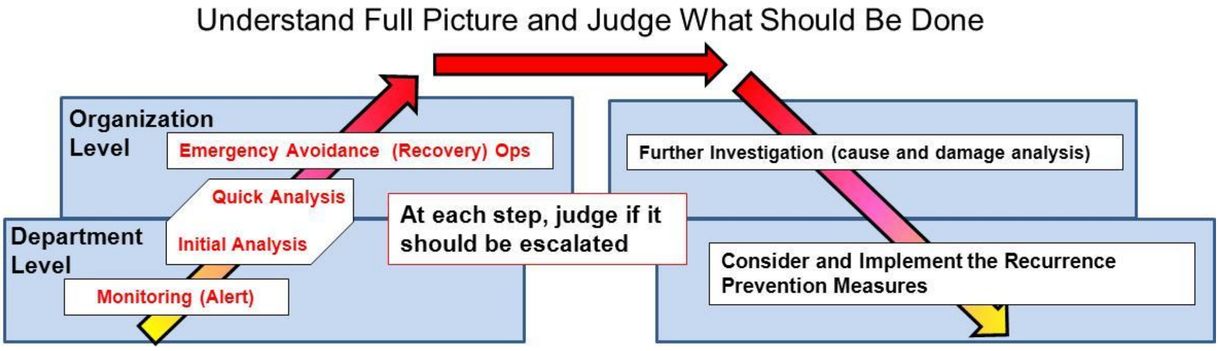

Understand Full Picture and Judge What Should Be Done
Organization Level
Emergency Avoidance (Recovery) Ops
Quick Analysis
Department Level
Initial Analysis
Monitoring (Alert)
At each step, judge if it should be escalated
Further Investigation (cause and damage analysis)
Consider and Implement the Recurrence Prevention Measures

Figure 2.3-1 Image: Escalation and Response in time of incident

The table below shows examples of the risk mitigation measures that should be taken until an emergency response decision is made to ensure the ways to gather necessary information to understand a full picture of the attack.

What is most important is to gather the information needed for the organization to make decisions, but it is also necessary to plan emergency avoidance (recovery) measures **in case the efforts to gather the information fail**.

Table 2.3-1 Example of Emergency Recovery Measures.

Contingency Avoidance Actions (Sample)	Measure (Sample)
Contingency Avoidance (Recovery) Plan ①	【Cloud Computing/Virtual Environment】 ・Move a guest OS onto the supervisory host operating system, and monitor traffic and operations on the guest OS systems ・Copy a guest OS onto the supervisory host OS and monitor only suspicious clients with policy-based routing.
Contingency Avoidance (Recovery) Plan ②	【Network Configuration Gradual-Change Plan (Prepare in Advance)】 ・Change network configuration in time of emergency ・Restrict suspicious network traffic ・Strengthen Monitoring of traffic ・Do not allow to initiate a communication with other departments ・Tighten monitoring of traffic that attempts to bypass the restricton

3 Support Documentation

This chapter provides the supplemental information for the measures and contents discussed in Chapter 2.

It will help when applying the set of system design measures discussed in this guide to an organization’s information system design and operations management.

3. 1 Targeted Email Attack Scenario in Detail

In this section, the system design measures addressed in this guide are mapped to a detailed attack flow model of each attack phase. This can be used to improve understanding of the attack flows, goals of the attacker, and system design measures against the attack.

(1) Targeted Email Attack Flow at Each Phase

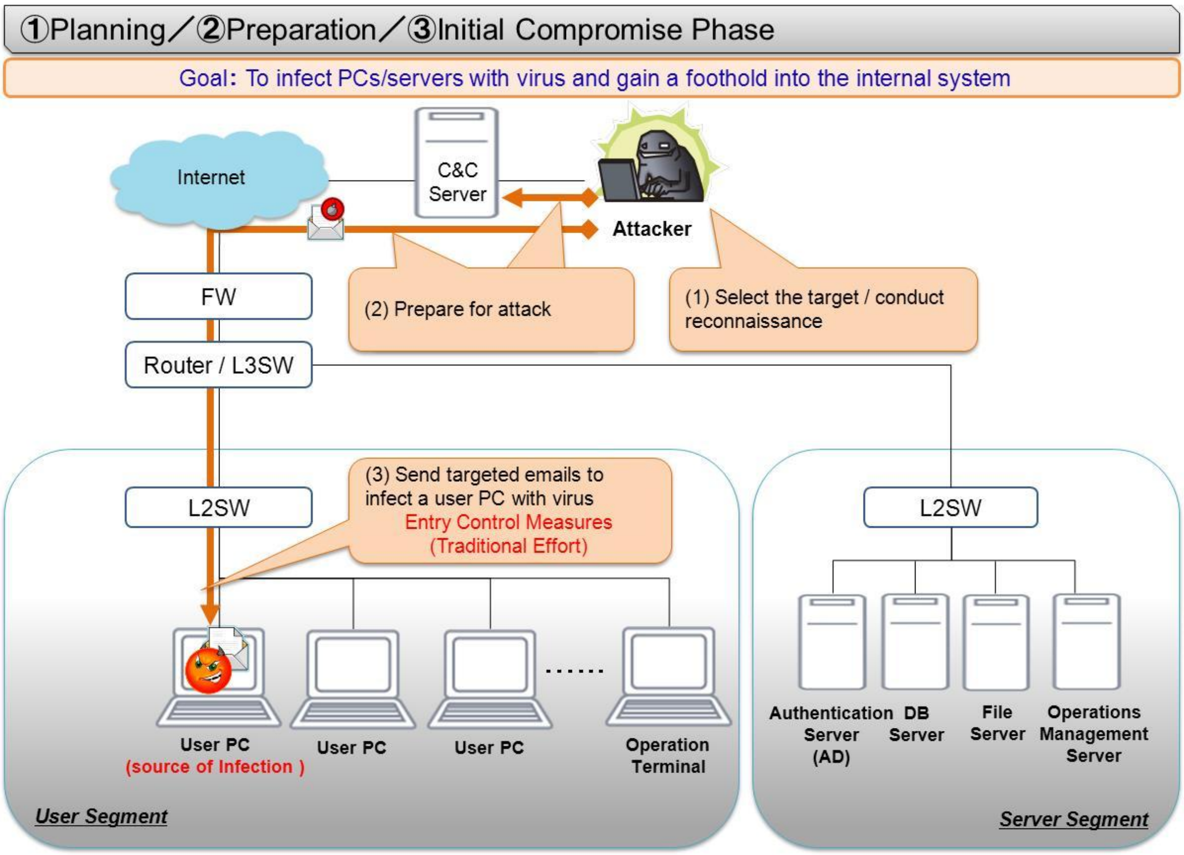
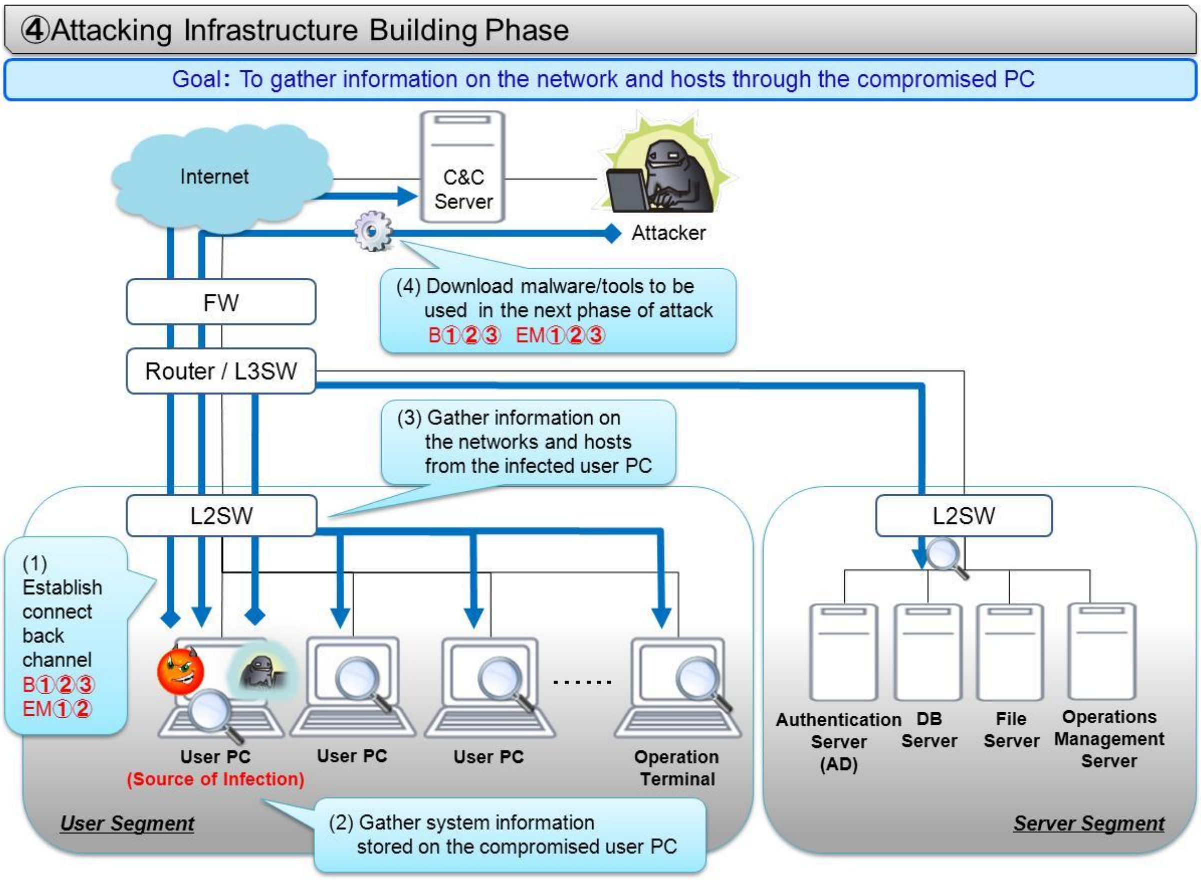

①Planning／②Preparation／③Initial Compromise Phase
Goal: To infect PCs/servers with virus and gain a foothold into the internal system
Internet
C&C Server
Attacker
FW
Router / L3SW
(2) Prepare for attack
(1) Select the target / conduct reconnaissance
L2SW
(3) Send targeted emails to infect a user PC with virus
Entry Control Measures (Traditional Effort)
L2SW
User PC
(source of Infection)
User PC
User PC
……
Operation Terminal
Authentication Server (AD)
DB Server
File Server
Operations Management Server
User Segment
Server Segment

Figure 3.1-1

Attack Flow and Key Points of System Design: from Planning Phase to Initial Compromise Phase



④Attacking Infrastructure Building Phase

Goal: To gather information on the network and hosts through the compromised PC

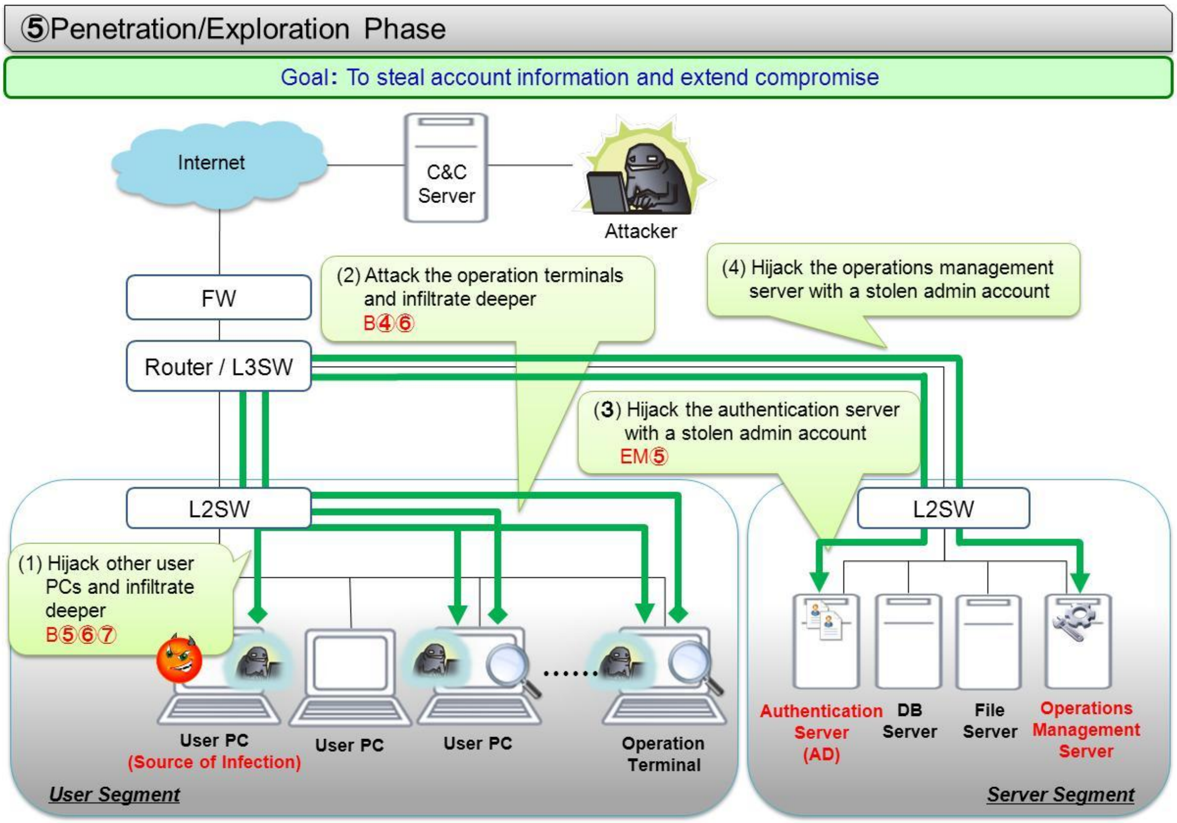
(1) Establish connect back channel B①②③ EM①②

(2) Gather system information stored on the compromised user PC

(3) Gather information on the networks and hosts from the infected user PC

(4) Download malware/tools to be used in the next phase of attack B①②③ EM①②③

Figure 3.1-2 Attack Flow and Key Points of System Design: Attacking Infrastructure Building Phase



⑤Penetration/Exploration Phase

Goal: To steal account information and extend compromise

(1) Hijack other user PCs and infiltrate deeper B⑤⑥⑦

(2) Attack the operation terminals and infiltrate deeper B④⑥

(3) Hijack the authentication server with a stolen admin account EM⑤

(4) Hijack the operations management server with a stolen admin account

Figure 3.1-3 Attack Flow and Key Points of System Design: Penetration/Exploration Phase

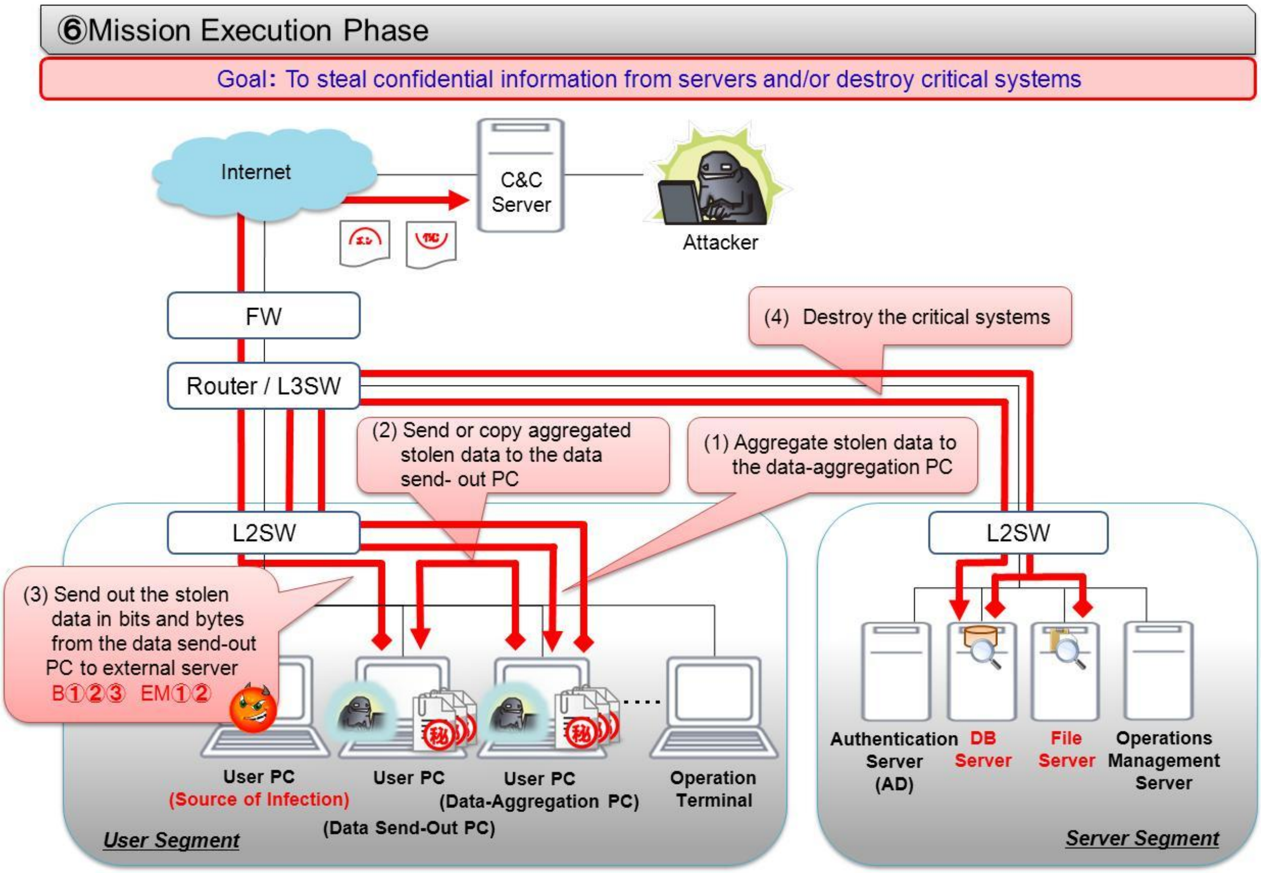
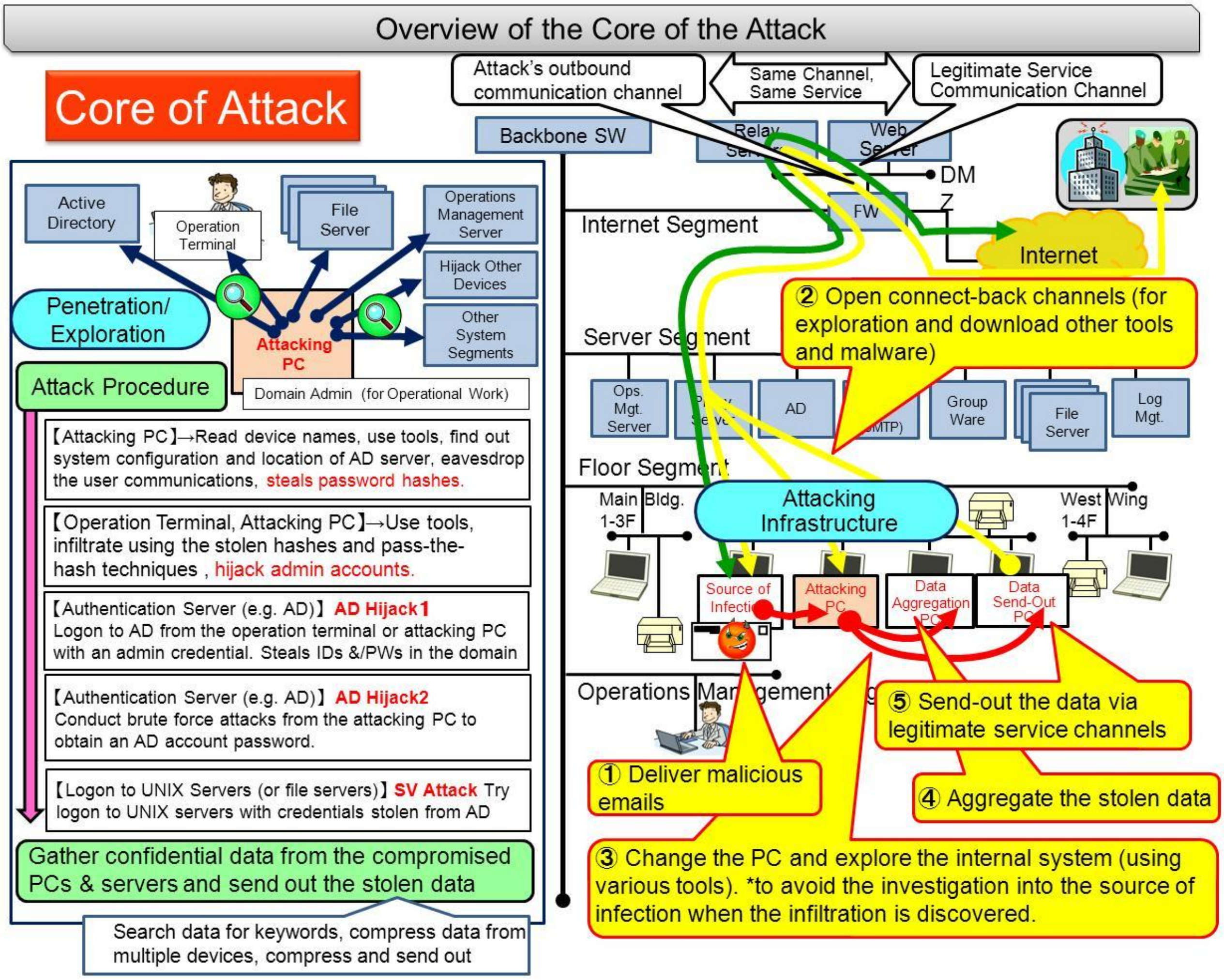

⑥Mission Execution Phase
Goal: To steal confidential information from servers and/or destroy critical systems
Internet
C&C Server
Attacker
FW
Router / L3SW
(4) Destroy the critical systems
(2) Send or copy aggregated stolen data to the data send- out PC
(1) Aggregate stolen data to the data-aggregation PC
L2SW
L2SW
(3) Send out the stolen data in bits and bytes from the data send-out PC to external server
B①②③ EM①②
User PC
(Source of Infection)
User PC
(Data Send-Out PC)
User PC
(Data-Aggregation PC)
Operation Terminal
User Segment
Authentication Server (AD)
DB Server
File Server
Operations Management Server
Server Segment

Figure 3.1-4 Attack Flow and Key Points of System Design: Mission Execution Phase

（2）Overview of the Core of the Attack

The figure below is the overview of the core of the attack: ④Attacking Infrastructure Building, ⑤Penetration/Exploration and ⑥Mission Execution phase. It shows things like how the compromise spreads or how to hijack accounts in detail.



Overview of the Core of the Attack

【Attacking PC】→Read device names, use tools, find out system configuration and location of AD server, eavesdrop the user communications, steals password hashes.

【Operation Terminal, Attacking PC】→Use tools, infiltrate using the stolen hashes and pass-the-hash techniques , hijack admin accounts.

【Authentication Server (e.g. AD)】 AD Hijack1 Logon to AD from the operation terminal or attacking PC with an admin credential. Steals IDs &/PWs in the domain

【Authentication Server (e.g. AD)】 AD Hijack2 Conduct brute force attacks from the attacking PC to obtain an AD account password.

【Logon to UNIX Servers (or file servers)】 SV Attack Try logon to UNIX servers with credentials stolen from AD

Gather confidential data from the compromised PCs & servers and send out the stolen data

Search data for keywords, compress data from multiple devices, compress and send out

② Open connect-back channels (for exploration and download other tools and malware)

① Deliver malicious emails

⑤ Send-out the data via legitimate service channels

④ Aggregate the stolen data

③ Change the PC and explore the internal system (using various tools). *to avoid the investigation into the source of infection when the infiltration is discovered.

Figure 3.1-5 Overview of the Core of the Attack

3. 2 System Design Measures Based On System Design Model

Based on the “targeted email attack scenario in detail” described in 3.1, IPA Security Threat and Countermeasure Study Group conducted the mock attacks which executed the attack procedures on the “basic system configuration” shown below and checked out the weaknesses of the system design and discussed the countermeasures.

This section introduces the approaches IPA Security Threat and Countermeasure Study Group took to formulate the system design measures. This technique will help the organizations when they consider the system design measures for their own system. We hope the organizations will make a good use of this guide.

(1) Draft Basic System Configuration

As a first step to consider system design measures, we drafted a basic system configuration shown below based on the interviews and the expertise of operations management staff. The point here is to clarify where the devices and equipment that involve in the communication with external services are deployed in the network to become capable to monitor a full picture of the attack. The following basic design system is a design model of a common information system and not a real one.

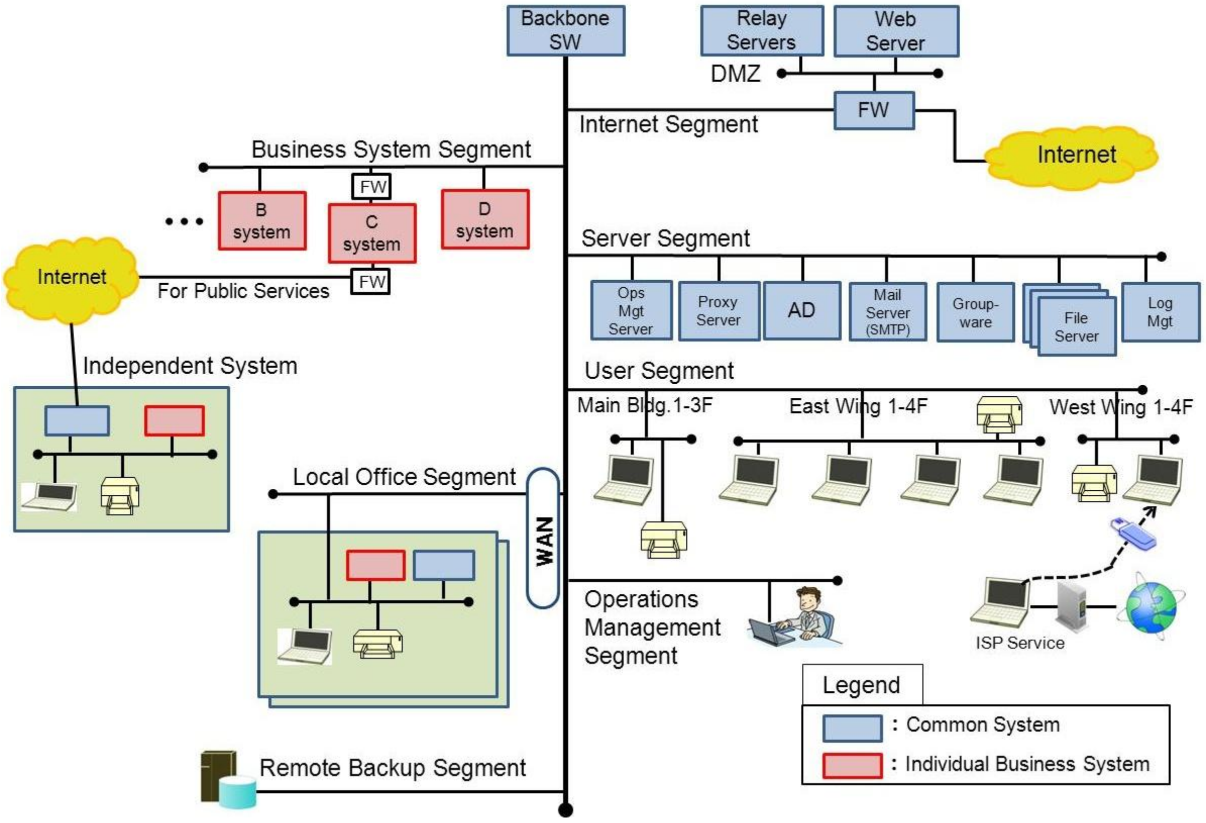


Figure 3.2-1 Basic System Design Overview ①

(2) Clarify Segregation of Management

For the targeted email attacks, as mentioned before, the whole system can be their attacking field. A system that is above a certain size would be running on a complicated segregation of operations (privilege control on each system and network segment) and collaboration between the relevant departments and people is mandatory to enable an organization-wide incident response. Thus, we clarified who operated and managed what system to list up the stakeholders necessary to formulate and consider possible system design measures. By doing so, we were able to know who should take actions at a given moment and with whom they should coordinate their actions and ask for cooperation. That makes the consideration proceed smoothly.

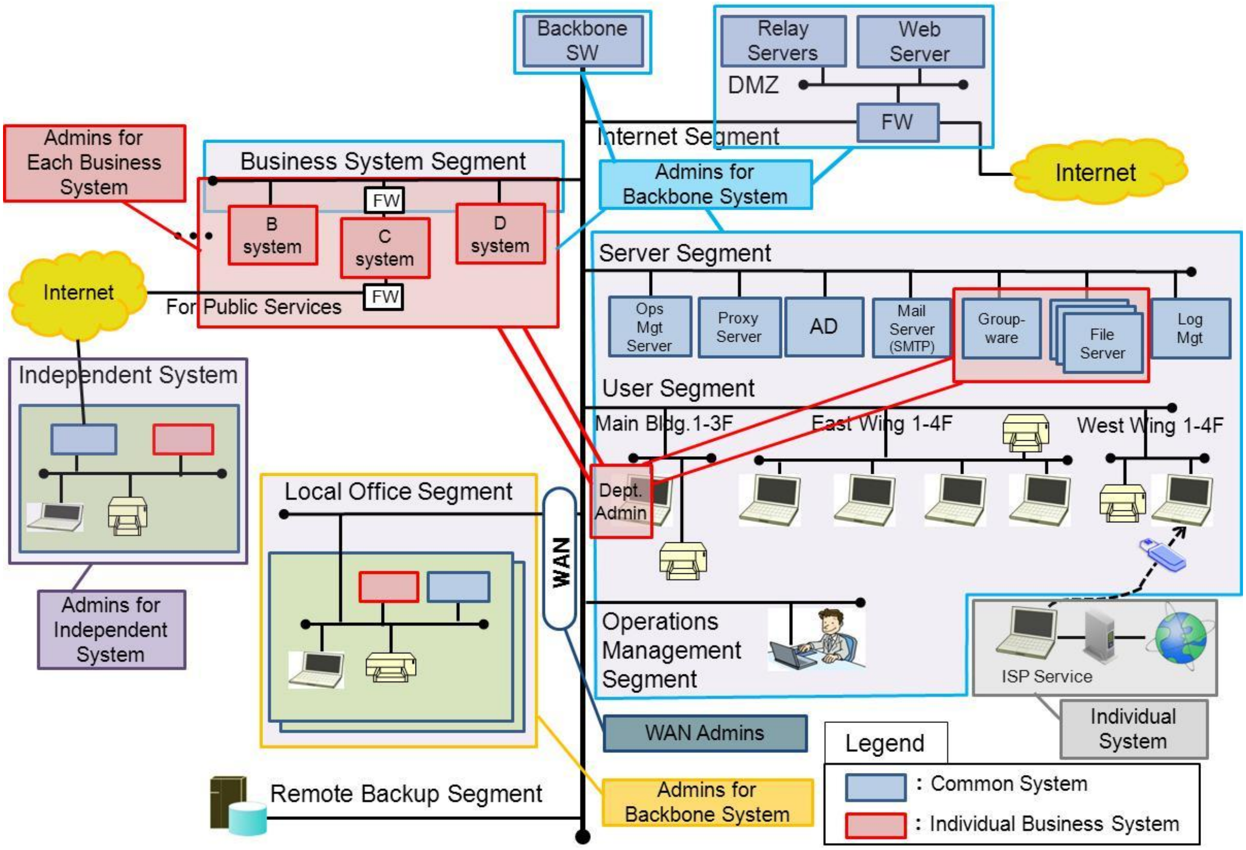


Figure 3.2-2 Basic System Configuration ②

(3) Conduct Mock Attacks

Following 3.1 Targeted Email Attack Scenario in Detail, we conducted the mock attacks on the basic system configuration and identified the devices and equipment that the security measures need to be implemented. Here, based on the premises that the attacker will manage to infiltrate the internal system, we clarified the steps the attacker would take in accordance with the attack scenario.

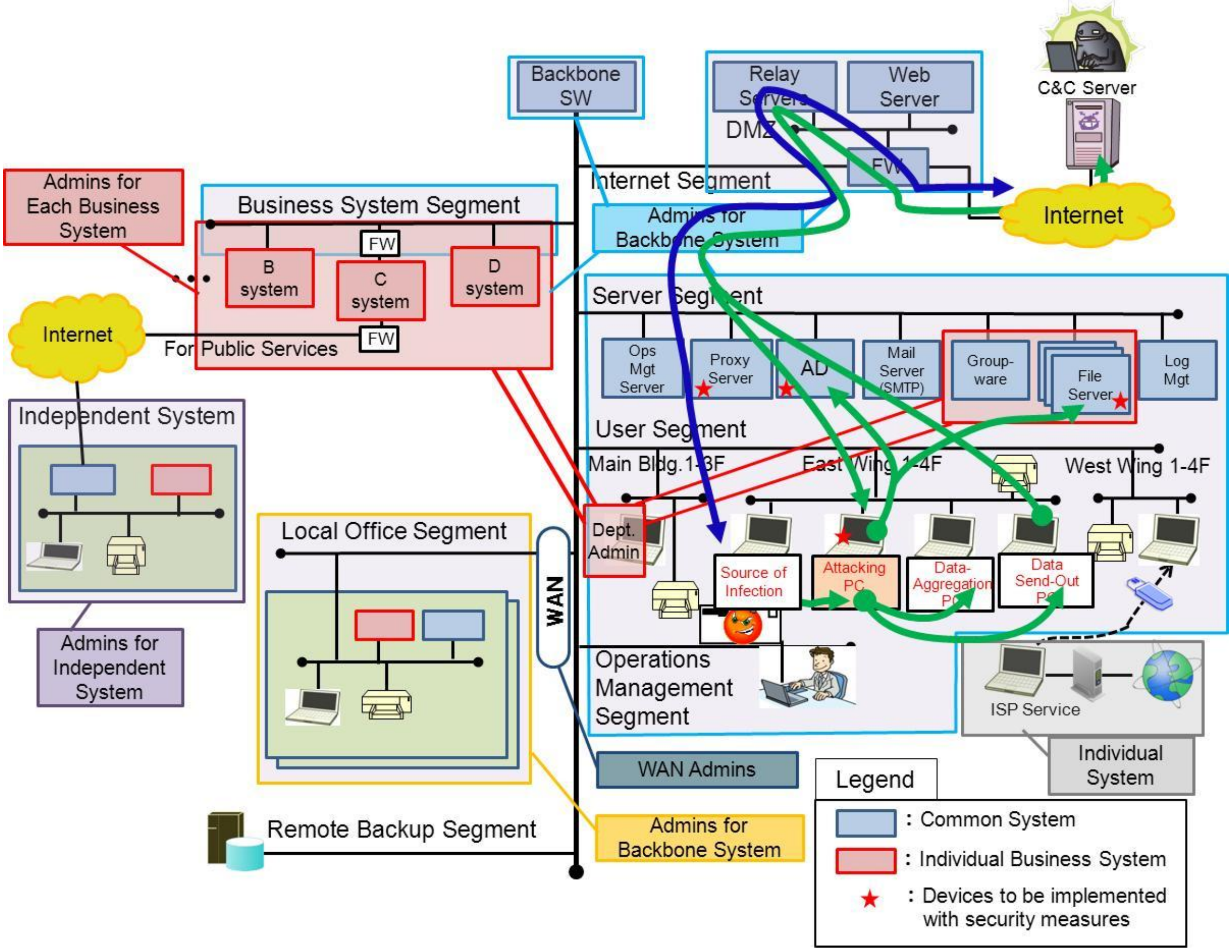


Figure 3.2-3 Basic System Design ③

(4) Develop System Design Measure Matrix

The analysis result of the mock attacks was divided into the measures to enhance monitoring and those to block malicious communication traffic, and organized into a matrix as the system design measures at each phase. The table below is part of the matrix.

The point here is to consider the enhanced-monitoring measures and blocking measures after clarifying the threat scenarios and the objective of the measures at each phase. Also it is important to discuss the matters not only among the people with specific expertise but also with those with different and multiple perspectives such as network configuration, server operation and virus analysis. By having multiple experts with different fields of expertise, such as administrators from each system segment and infrastructure/system development vendors, more effective solutions can be inspired.

Threat Scenarios		Objectivel of Measure	No	Measures			
				Blocking Measures (Prevention)		Enhanced-Monitoring Measures (Detection)	
	Scenario Scenarios derived from the interviews	Measures against derived threat		Description Design measures to block attacks	Subject Devices	Description Triggers to detect the Indicators	Subject Devices
Attacking Infrastructure Building Phase	(1) Establish connect-back channels						
	【Malware Communication Protocol 】 - Other than: Authentication Proxy Supported/Port:443/TCP, CONNECT	Block connect-back communications (Detect and block the communications that use RAT)	B②	①Design the proxy server to block the traffic other than "CONNECT/TCP443" ②Monitor the proxy server log for RAT CONNECT communications	Proxy Server		
	【Malware Communication Protocol 】 - Authentication Proxy Supported/Port:443/TCP, CONNECT	Detect connect-back communications (Detect RAT and unauthorized communications by malware)	EM①			①Periodical forced-disconnection of all communications via the proxy server ②Look for Keep-Alive probes in the communications that attempt to reconnect	Proxy Server
	(2) Gather system information available on the user PCs	Prevent the attacker from gathering system information available on the user PCs	Existing Measures				
Penetration/Exploration Phase	(1) Hijack the current user PC, other user PCs/Servers and compromise the internal system further	Prevent the attacker from stealing the domain account information from the user PCs	B⑥	Ban to cache highly-privileged admin account information	User PC Operation Server		
	(2) Attack an operation terminal and compromise the internal system further	Prevent the attacker from hijacking the admin privileges by blocking the access from the user PCs to the servers	B④	①Perform network segmentation for the user PCs and operation terminals ②Filter the source IP addresses on the servers ③Design the network in a way that the maintenance port of each server is invisible and inaccessible from the business segments (user segments) and accessible from the operations management segment only	User PC Operation Server		
			B⑤	①Perform network segmentation for the user segment and operation server segments ②Traffic between the segments are permitted only on the ports that are absolutely necessary for the business operations	Network Devices		

Figure 3.2-4 Attack-Measure Matrix

◆Process of Deriving System Design Measure

Below are sample images of system design measure formulation. Map attack patterns to an organization’s supposed system configuration and formulate and consider the design measures against the problems found in the current state (with the current design).

By using the analysis result of the real incidents and the organization’s real system configuration, effectiveness of the measures will be improved.

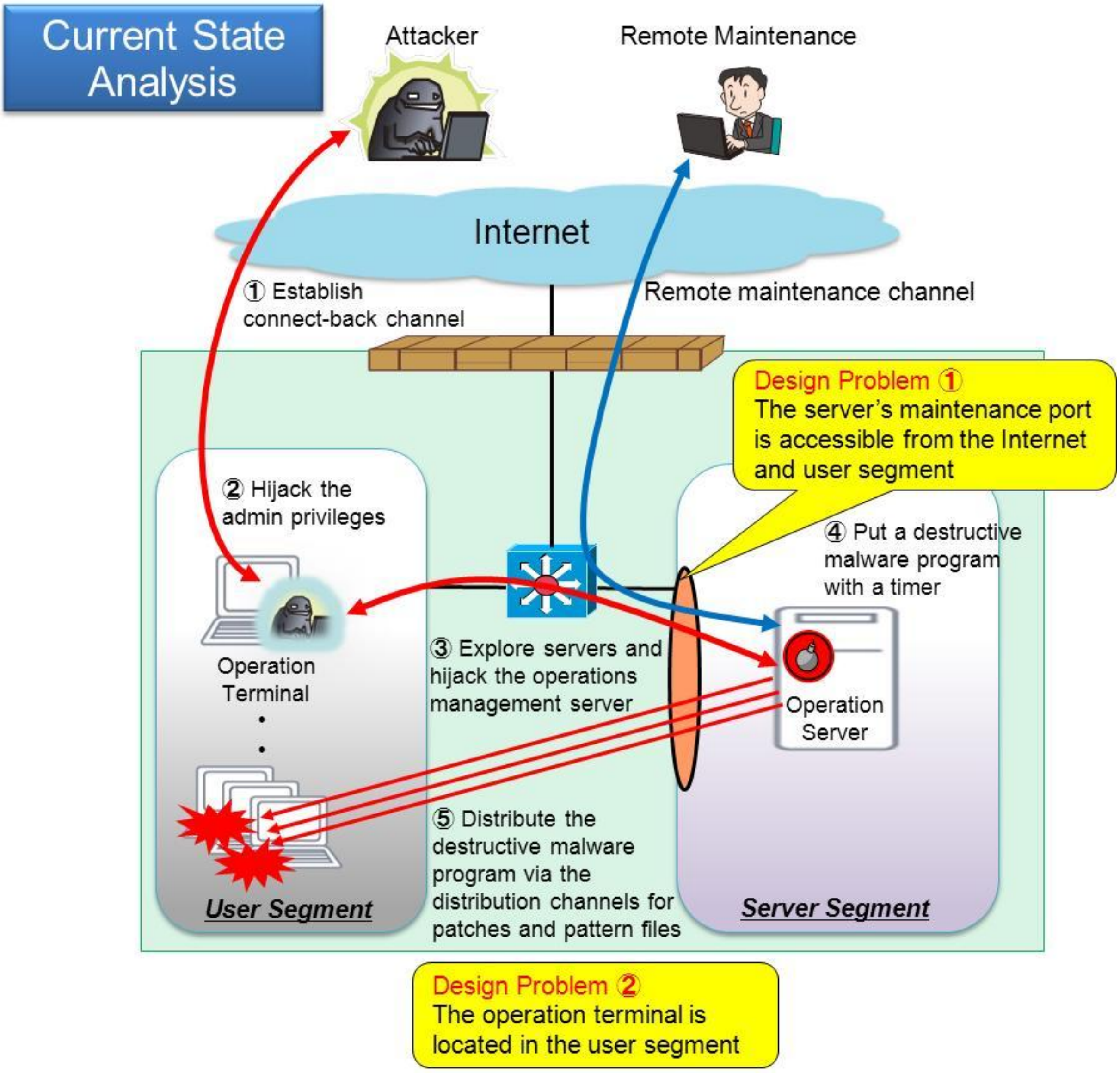
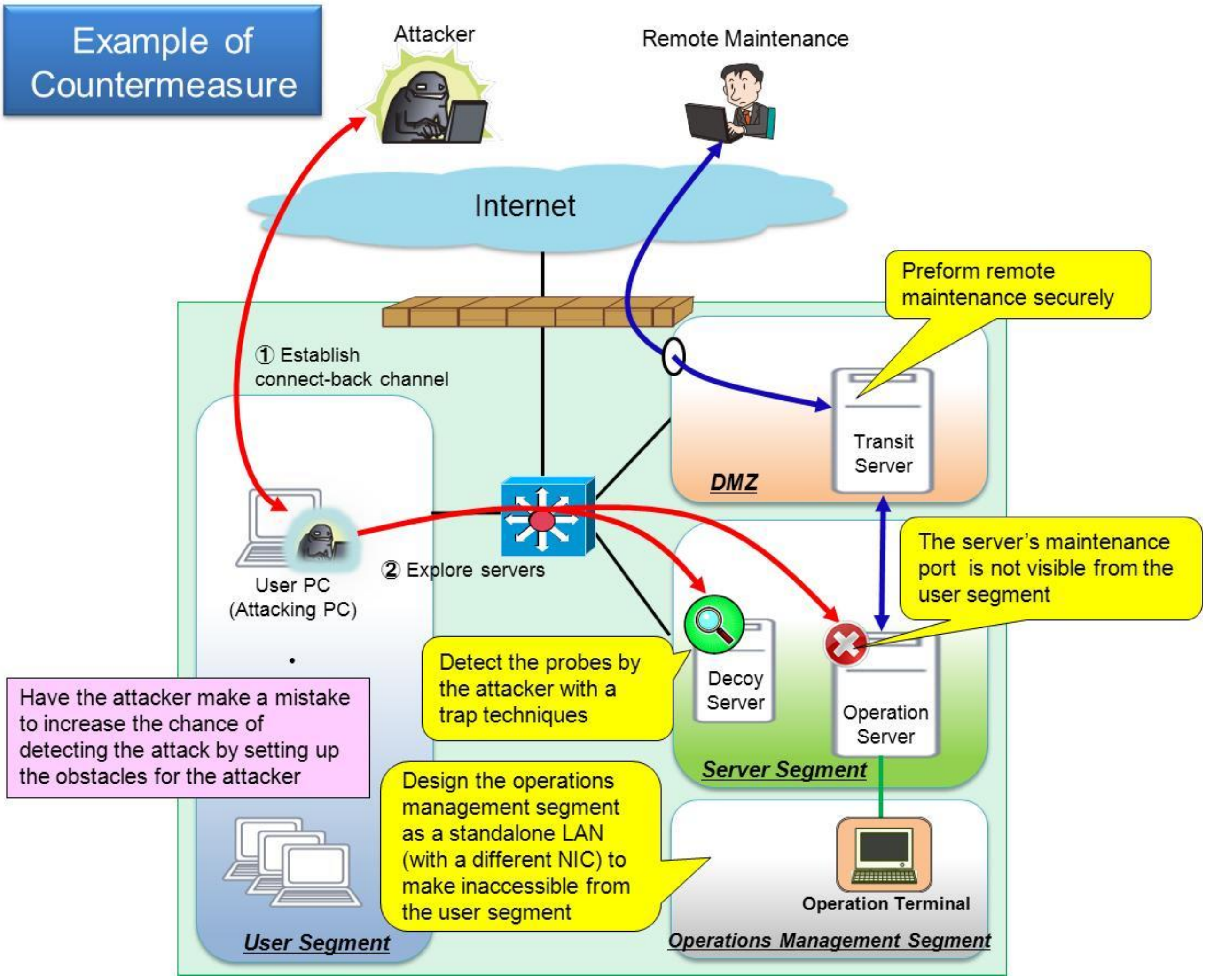

Current State Analysis
Attacker
Remote Maintenance
Internet
① Establish connect-back channel
Remote maintenance channel
Design Problem ①
The server’s maintenance port is accessible from the Internet and user segment
② Hijack the admin privileges
④ Put a destructive malware program with a timer
Operation Terminal
③ Explore servers and hijack the operations management server
Operation Server
⑤ Distribute the destructive malware program via the distribution channels for patches and pattern files
User Segment
Server Segment
Design Problem ②
The operation terminal is located in the user segment

Figure 3.2-5 Example of Current State Analysis



Example of Countermeasure
Attacker
Remote Maintenance
Internet
Preform remote maintenance securely
① Establish connect-back channel
Transit Server
DMZ
User PC (Attacking PC)
② Explore servers
The server's maintenance port is not visible from the user segment
Detect the probes by the attacker with a trap techniques
Decoy Server
Operation Server
Have the attacker make a mistake to increase the chance of detecting the attack by setting up the obstacles for the attacker
Server Segment
Design the operations management segment as a standalone LAN (with a different NIC) to make inaccessible from the user segment
Operation Terminal
User Segment
Operations Management Segment

Figure 3.2-6 Example of Current State Analysis

◆Basic Concept of System Design Measures

The basic concept of the system design measures is to prevent deeper infiltration by the attacker who has managed to gain a foothold into the system by properly segmenting the network and permitting only the traffic that is absolutely necessary for the business operations (see examples of the access control rules below). The key points of the basic system configuration recommended by this guide are summarized below.

① Design the network to make the outbound traffic from the user segment go through the proxy server

② Do not allow the maintenance operations through the access via the user segment

③ Set up a network segment dedicated to operations management and allow only the specific administrators to perform maintenance operations on the servers

Table 3.2-1 Examples of Access Control Rules

Access Control Rules (Example)		Access Segment <Destination>						
		Internet	DMZ	Business System	Intranet Server	Internet Connection	User	Operations Management
Access Segment <Source>	Internet		○	×	×	×	×	×
	DMZ	△		×	○	○	×	×
	Business System	×	×		△	○	×	×
	Intranet Server	×	×	×		×	×	×
	Internet Connection	×	○	×	○		×	×
	User	×	○	○	○			×
	Operations Management	×	○	×	○	○	×	

Legend ○: Permitted, △: Partially Permitted, ×: Denied

3. 3 Tools Used For Infiltration

As a valuable information that can reveal what kind of tools attackers are using, Trend Micro released a report on the tools often used in sophisticated unauthorized access attacks, such as targeted email attacks, on March 7, 2013[13].

Based on the report, this section has organized the tools used after establishing connect-back channels, namely at the “Attacking Infrastructure Building” and “Penetration/Exploration” phase in the attack flows.

These tools may be detected by anti-virus software.

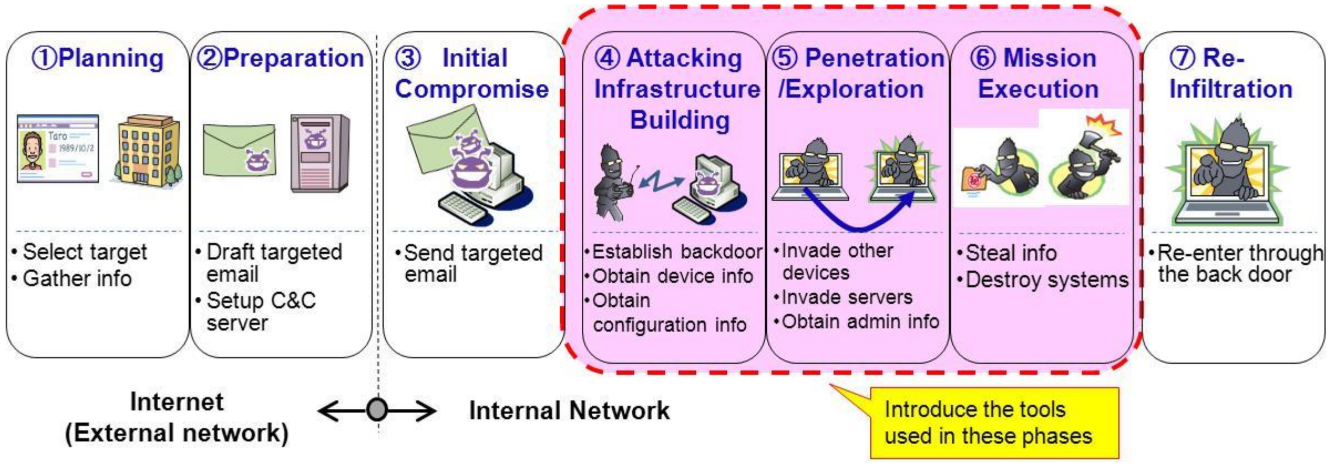


Figure 3.3-1 Attack Phases

(1) Example of the Tools Used in Attacks

Below is a list of tools used in attacks after connect-back channels are established. Notes were added by IPA Security Threat and Countermeasure Study Group to the original information released by Trend Micro.

Table 3.3-1 Examples of Tools Used in Attacks (1/3)

Tool	Description[14]	Note	References
Password Hash Theft			
Pwdump	Dumps password hashes from the Windows registry. Typically used to crack passwords for lateral movement throughout the victim environment. It can also be used in pass-the-hash attacks.	A tool used for password recovery. There are several versions, for example, pwdump and pwdump2 to 7. The latest version supports Windows 7.	http://www.openwall.com/passwords/microsoft-windows-nt-2000-xp-2003-vista-7
Cachedump	A program for extracting cached password hashes from a system’s registry. Typically used to crack passwords for lateral movement throughout the victim environment. It can also be used in pass-the-hash attacks.	It obtains domain hashes. It has been around since about 2003.	http://www.securiteam.com/tools/5JP0I2KFPA.html

[13] Trend Micro, TrendLabs Security Intelligence Blog: In-Depth Look: APT Attack Tools of the Trade http://blog.trendmicro.com/trendlabs-security-intelligence/in-depth-look-apt-attack-tools-of-the-trade/

Table 3.3-1 Examples of Tools Used in Attacks (2/3)

Tool	Description	Note	References
Password Hash Theft			
Lslsass	Dumps active login session password hashes from Windows processes. It is used to crack passwords for lateral movement throughout the victim environment. It can also be used in pass-the-hash attacks.	A tool to obtain password hashes in LSASS (Windows authentication process). Released in 2010.	http://www.truesec.se/sakerhet/verktyg/saakerhet/lslsass_v1.0_(x86)
Windows Credential Editor (WCE)	A security tool that allows to list logon sessions and add, change, list and delete associated credentials.	A tool to extract plaintext passwords in login session.	http://www.ampliasecurity.com/research.html
Gsecdump	Grabs SAM file, cached credentials, and LSA secrets (LSA-managed private data). It is used to crack passwords for lateral movement throughout the victim environment. It can also be used in pass-the-hash attacks.	A tool to obtain password hashes from SAM (a registry that stores Windows credentials). Released in 2010.	http://www.truesec.se/sakerhet/verktyg/saakerhet/gsecdump_v2.0b5
Communication Channel Securement			
HTRAN	It works as connection bouncer and redirects TCP traffic destined for one host to an alternate host. It is also used to help obfuscate source IP of an attacker. It allows the attacker to bounce through several connections in the victim country, confusing incident responders.	A tool to redirect packets. It can use a server or PC as a relay server. It is assumed that it was developed by Honke Union of China in about 2003.	http://blog.f-secure.jp/tag/HTran
ZXProxy (別名 AProxy)	It works as proxy functionality for traffic redirection. This helps redirect HTTP/HTTPS connections for source obfuscation. Trend Micro has confirmed it was used in data exfiltration.	A Proxy tool that supports Socks4/5. It can make a server or PC work as an internal proxy server.	
ZXPortMap	A tool to redirect traffic. It helps to obfuscate the source of connections.	A tool to redirect packets. It can use a server or PC as a relay server. Developed in about 2006.	
Web Server (Data Gathering and Distribution)			
Netbox	A hosting tool for drop servers and C2 servers. Commonly used as infrastructure on the backend to support operational tasks. (Netbox also has legitimate uses, and is not a direct indicator of compromise).	A very light, around 500KB, Web server program. It supports JavaScript, VBScript, Perl and more. Also supports SSL/TLS.	
ZXHttpServer	A small HTTP server that is deployable and extremely flexible. Trend Micro has confirmed it was used when attempting transfer of some files.	A very simple Web server. Developed in about 2006.	
Email Theft			
GETMAIL	Typically used to ascertain mail archives and mail out of those archives.	A tool to obtain emails that supports POP3.	http://www.interlog.com/~tcharron/getmail.html
mapiget	Used to collect emails directly from Outlook, prior to ever getting archived. It is then dumped to text files.	It looks like a tool that directly extracts emails but the details are unknown. mapi.exe is one of the same kind of tools.	

Table 3.3-1 Examples of Tools Used in Attacks (3/3)

Tool	Description	Note	References
File Compression			
Lz77.exe	Used as a compression application to help stealing information. Normally, this tool is seen in “Winrar”, “’zip” and “Winzip”.	It is assumed to suggest an archiver. Lz77 is a basic algorithm for data compression and freely available on the Internet.	
UPX Shell	Used to compress malicious program code used in APT campaigns. This tool prevents reverse engineering and code analysis.	An open-source, compression tool for executable files. UPX Shell is a Windows GUI tool but there is a command line version as well. It allows to evade pattern matching.	http://sourceforge.jp/projects/sfnet_upxshell/
Other Tools (Data Concealing, Secure Deletion, Information Theft)			
LSB-Steganography	Used to embed files into images using steganography techniques, which is a data-concealing technology. Mainly used at the initial compromise phase in the traditional APT attacks when stealing information.	It is assumed that the program code released for research purpose is diverted to malicious use. It is guessed that it is used to evade anti-virus GWs and proxy servers.	http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5328281&tag=1
Sdelete	A tool to securely delete files. Since it can delete the files securely, it makes forensic recovery hardship and incident response procedures complicated.	A secure file deletion tool offered by Microsoft Sysinternals. It is assumed that it is used to delete programs and stolen files.	http://technet.microsoft.com/ja-jp/sysinternals/bb897443.aspx
Dbgview	An application that allows to monitor debug output on a victim’s local computer or any computer on the network that the victim can access via TCP/IP.	A debug output tool offered by Microsoft Sysinternals. It can obtain debug information output by APIs and applications.	http://technet.microsoft.com/ja-jp/sysinternals/bb896647.aspx

（2）The Way Attack Tools Are Used

The aforementioned tools can be used in the following ways in attacks. They are not exhaustive but knowing what kinds of tools are out there that can be used by attackers and what functionality they have will provide valuable hints to guess what the attackers are going to do at each attack phase.

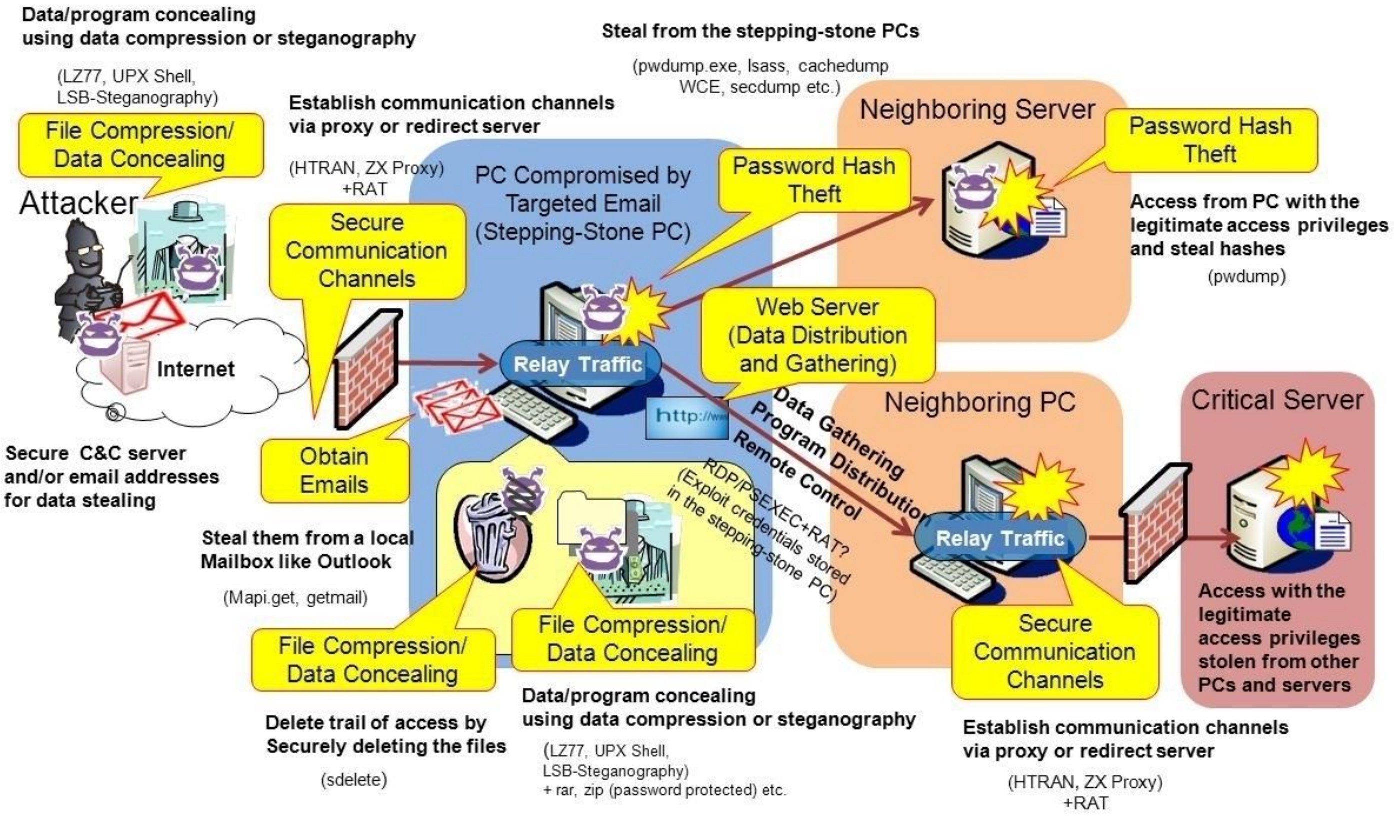


Figure 3.3-2 Attacking Image: Possible Ways the Tool Are Used

The attack techniques analyzed by the objective of attacks and the functionality of the tools at each attack phase are introduced at the following URL:

*Reference: Trend Micro “2013 First Half: Analysis of Persistent Targeted Attacks in Japan“
http://blog.trendmicro.co.jp/archives/7726 (in Japanese)

3. 4 Analysis Result of Proxy Server Log

When considering which security measures to adopt, it is important to do it based on the verification on the real implementation level. For that, this section provides the result of the verification of the log entries recorded by the proxy server during the attack using "PoisonIvy[15]", a malware used in some actual targeted email attacks.

The aim of this verification is to confirm objectively that **it is not enough to simply store log, but to specify what to log, adjusting accordingly to the real attacks, to put it in actual use**. We conducted verification to uncover the issues more concretely in terms of the feasibility of the measures in both implementation and operation. The verification was done in the following environment.

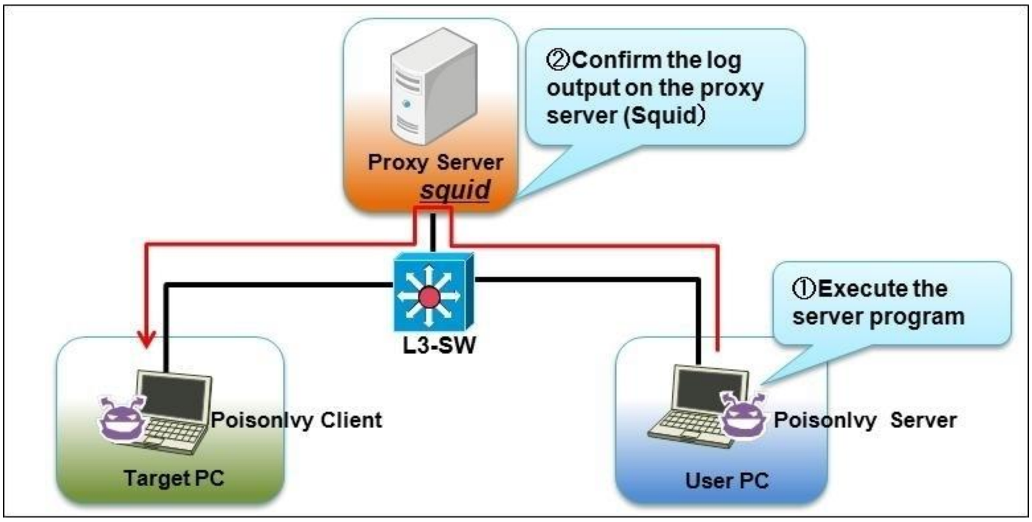

②Confirm the log output on the proxy server (Squid)
Proxy Server
squid
①Execute the server program
L3-SW
PoisonIvy Client
Target PC
PoisonIvy Server
User PC

Figure 3.4-1 Verification Environment

The verification was conducted in the following procedure.

A） Execute a traffic capture tool on the user PC

B） Execute the PoisonIvy server program

C） Confirm the establishment of a session in the PoisonIvy client program on the target PC

D） Check the various log entries recorded in the proxy server (Squid)

Squid provides a proxy server functionality and offers the following three types of log files. When installing Squid with the default settings, each log file is stored under the /var/log/squid/ directory.

1. access.log: A log file that records the requests (client address, request method, URL) from the client PC
2. cache.log: A log file that records the error and debug messages generated by the Squid services
3. store.log: A log file that records the objects recorded and deleted in cache

As the result of the analysis, we have found that PoisonIvy have the following characteristics.

・Unless the program is terminated, it keeps the session between the server and client.

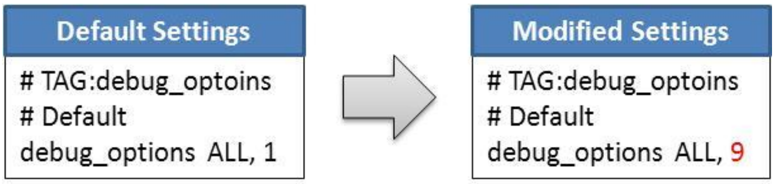
[15] A remote-access malware called "remote administration tool (RAT)"

・Squid’s access.log does not record a log when an access to the proxy server via the CONNECT method is made, but does record when a session is disconnected.

Based on the result that access to the proxy server via the CONNECT method was not recorded in the access.log file that was to be monitored in a typical proxy server operation, we changed the conditions and verified again. We changed the log level in the squid.conf file, a Squid configuration file, and analyzed the log entries recorded in the cache.log.

The cache.log is a log file that records the error and debug messages generated by the Squad services, thus normally the entries like requests for connection to the proxy server are not recorded. But as a result of the verification, we have found that it is possible to record the detailed log by changing the log level.

To change the log level of the cache.log file, change the value of the “debug_options” directive in the squid.conf file from “ALL,1” to “ALL,9”.



Default Settings

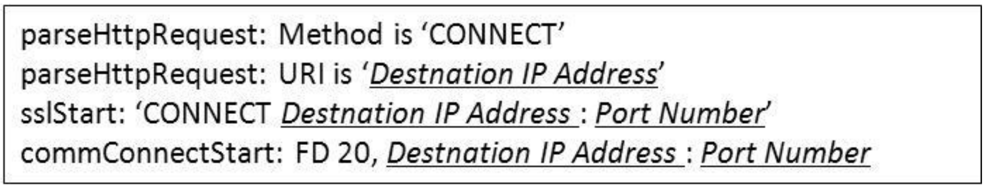
```
# TAG:debug_optoins
# Default
debug_options ALL, 1
```

Modified Settings

```
# TAG:debug_optoins
# Default
debug_options ALL, 9
```

Figure 3.4-2　Example of squid.conf Setting Modification

By changing the settings for the cache.log file, it is possible to record access to the proxy server via the CONNECT method that is not recorded in the access.log file.



```
parseHttpRequest: Method is ‘CONNECT’
parseHttpRequest: URI is ‘Destnation IP Address’
sslStart: ‘CONNECT Destnation IP Address : Port Number’
commConnectStart: FD 20, Destnation IP Address : Port Number
```

Figure 3.4-3　Example of access.log Output

By changing the settings like the above, it can be used as a trigger to detect a RAT tool’s connect-back channel to the C&C server on the proxy server. However, there are some critical problems to deploy this in the real operation.

【Issues Ascertained in the Verification】

- If the log level of the cache.log file is changed, the size of the log Squid outputs as a service becomes enormously large (about 10 MB per minute)
- It is not possible to configure to record logs that Squid outputs as a service and logs for the requests for connection to the proxy server separately.

Because of the above reason, we concluded that a measure that proposed to change the log level of the cache.log file to monitor the requests for connection to the proxy server had a low feasibility. The log level of the cache.log file is designed to use for trouble shooting and not for continual log monitoring. Due to this conclusion, we realized that we were in need to come up with a technique that could make use of the access.log file and came up with a method introduced in 2.2.5 Uncover Connect-Back Traffic through Forced-Disconnnection.

3. 5 Analysis of Statistics Data

From the analysis of the malware programs attached to targeted emails that are tasked with establishing a connect-back channel, it is possible to know the types of connect-back communications. The connect-back communications are used by the attacker to remotely control the target organization's system at each attack phase, thus they are major subjects of enhanced-monitoring and blocking suggested in the set of system design measures.

By implementing the following design measures, it is possible to monitor and block more than half of the connect-back communications.

- 2.2.1 Block Connect-Back Traffic with Firewall
- 2.2.2 Block Connect-Back Traffic with Access Control at Proxy Server
- 2.2.3 Block Connect-Back Traffic with Proxy Authentication
- 2.2.4 Monitor and Analyze Proxy Authentication Log
- 2.2.5 Uncover Connect-Back Traffic through Forced-Disconnection

Below are the comparison of the studies between one conducted in November 2008 and another in August 2013.

Source: Trend Micro, "2013 First Half: Analysis of Persistent Targeted Attacks in Japan"
http://blog.trendmicro.co.jp/archives/7726 (in Japanese)

- No change in trend since the last study
  (IPA Security Threat and Countermeasure Study Group had been concerned with a possible increase of the use of HTTPS, which is more difficult to deal with, and continued the analysis.)
- There are still many communications (about half) that do not use a proxy server and they are increasing: **46%→54%**
  - In the environment of the possible target organizations, many of them still allow the direct connection to the Internet.
  - Just forbidding the direct connection to the Internet will reduce the damage.
- The use of HTTPS is not increasing: **28%→14%**
  - It is possible that the attackers know that they do not have to use HTTPS to establish successful connections.
    (The use of an approach that detects suspicious communications based on the characteristics of the content of communications is not widespread)
  - Using an approach that detects suspicious communications based on the characteristics of the content of communications can reduce the damage.

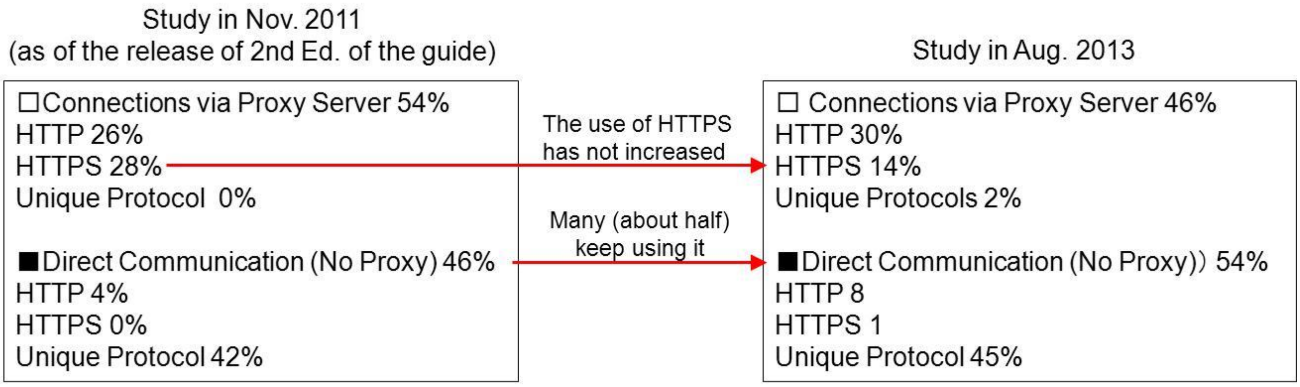

Study in Nov. 2011
(as of the release of 2nd Ed. of the guide)
Study in Aug. 2013
□Connections via Proxy Server 54%
HTTP 26%
HTTPS 28%
Unique Protocol 0%
■Direct Communication (No Proxy) 46%
HTTP 4%
HTTPS 0%
Unique Protocol 42%
The use of HTTPS has not increased
Many (about half) keep using it
□ Connections via Proxy Server 46%
HTTP 30%
HTTPS 14%
Unique Protocols 2%
■Direct Communication (No Proxy)) 54%
HTTP 8
HTTPS 1
Unique Protocol 45%

Figure 3.5-1 Transition of characteristics of malware communications

As the adoption of the approach that blocks and detects the malware’s C&C communications progresses, the attacker will increase the use of the legitimate services like HTTPS and cloud computing services as malware communication protocols, and it is assumed that the detection of connect-back traffic will be getting difficult.

Thus, IPA Security Threat and Countermeasure Study Group will continue to monitor and study the malware communications. In the meantime, by having a way of continuous monitoring and becoming capable of detecting the attacks, the organizations can catch the change in the attackers’ behavior early and contemplate what to do.

Terms

C&C Server

A command and control server. Used by an attacker to send commands to malware programs and control the behavior of the compromised computers.

Connect-Back Method

A method of communication used by a remote attacker to infiltrate a computer on the internal network. The internal computer requests a connection to the external computers (under the control of the attacker) and allows the attacker to gain access and infiltrate into the internal computer by responding to its initiation. Mainly used to bypass firewall security.

Entry Control Measures

A collective term for the security measures against targeted email attacks that focus on stopping the attacks at the entry point, such as fraud email detection, anti-virus software and vulnerability patching.

Inside Operation Prevention Measures

A collective term for the security measures against targeted email attacks that focus on blocking the malware programs' connect-back communication to the external computers and preventing the attacker who has managed to get into the internal system from infiltrating deeper.

Malware

A collective term for the computer programs that work against the user's interests. In this guide, a so-called viruses and Trojan horses are also called malware.

Inside Operation

Malicious actions, such as gathering information about the internal system to locate the attack targets or infiltrating deeper into the internal system, by the attacker who has successfully gained a foothold into the internal system through the connect-back method.

This page is intentionally left blank.

Collaborators

List of Collaborators (Job Title Omitted)

Name	Organization
Masahiko Kato	Internet Initiative Japan, Inc.
Katsumi Kobayashi	NRI Secure Technologies, Ltd.
Kunio Miyamoto	NTT Data Corp.
Nobuhiro Tsuji	NTT Data Intellilink Corp.
Norihiko Maeda	Kaspersky Labs Japan
Yuki Kanno	Simplex Consulting Inc.
Hiroki Iwai	Deloitte Tohmatsu Risk Services Co., Ltd.
Bakuei Matsukawa	Trend Micro Incorporated
Hiroki Takakura	Nagoya University
Koichiro Watanabe	IBM Japan, Ltd.
Yuji Motokawa	Hitachi Systems, Ltd.
Kentaro Nameki	Hitachi Solutions, Ltd.
Kousetsu Kayama	Fujitsu Ltd. (Fujitsu Cloud CERT)
Yasuhiro Fujiwara	Fujitsu Ltd.
Ryo Oba	Fujitsu Ltd
Hiroshi Kawarabayashi	Fujitsu FSAS Inc.
Tatsuya Kitao	Bank of Tokyo-Mitsubishi UFJ, Ltd.

System Design Guide for Thwarting Targeted Email Attacks

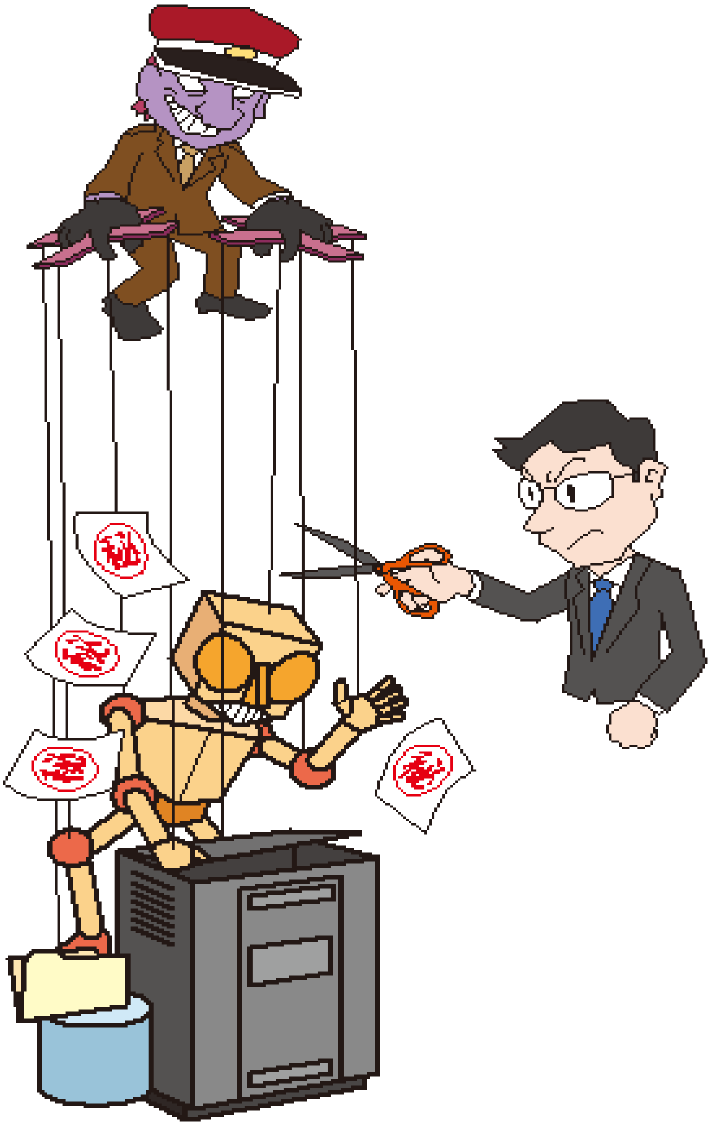
[Issued] December 2013

[Produced/Copyrighted By] IT Security Center, Information-technology Promotion Agency (IPA)

[Editor] Mitsugu Okatani, Masashi Ohmori

[Author] IPA Security Threat and Countermeasure Study Group

[Advisor] National Information Security Center



IPA

IT SECURITY CENTER (ISEC)
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Bunkyo Green Court Center Office
2-28-8 Honkomagome, Bunkyo-ku, Tokyo, 113-6591 Japan
TEL: 03-5978-7527 FAX: 03-5978-7518
http://www.ipa.go.jp/security/english/index.html