Introduction of Anti-malware Measures using Whitelisting based on Behavioral Detection

October , 2015
Yasuhiro Otsuka
Information Technology Group

九州電力
ずっと先まで、明るくしたい。

Table of Contents

➢ Recent years have seen changes in malware types from those that target multiple unspecified users, producing flamboyant effects and exhibiting destructive behavior that make users aware of the malware infection, to those with the characteristics listed below, continually heightening the risk of intrusion and infection.

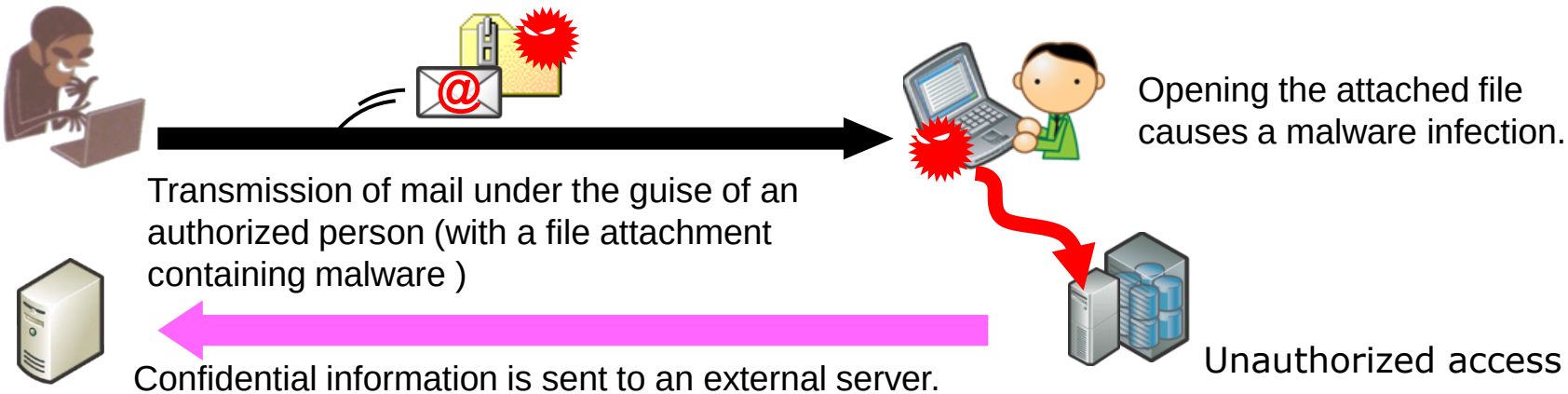
- Rather than reusing the types of malware that have been used in the past, new types of malware designed for specific targets or goals are created.
- New types of malware are used after verifying that they cannot be detected by general anti-malware software.
- New types of malware are created with restrictions on the environment in which they can be executed such as the inability to run anywhere but on the target computers, making them difficult to detect by third parties.

It is necessary to prepare for attacks by new types of malware that target specific organizations or companies.

1. Increased Security Threats caused by New Types of Malware
~ Examples of Damage at Home and Abroad ~

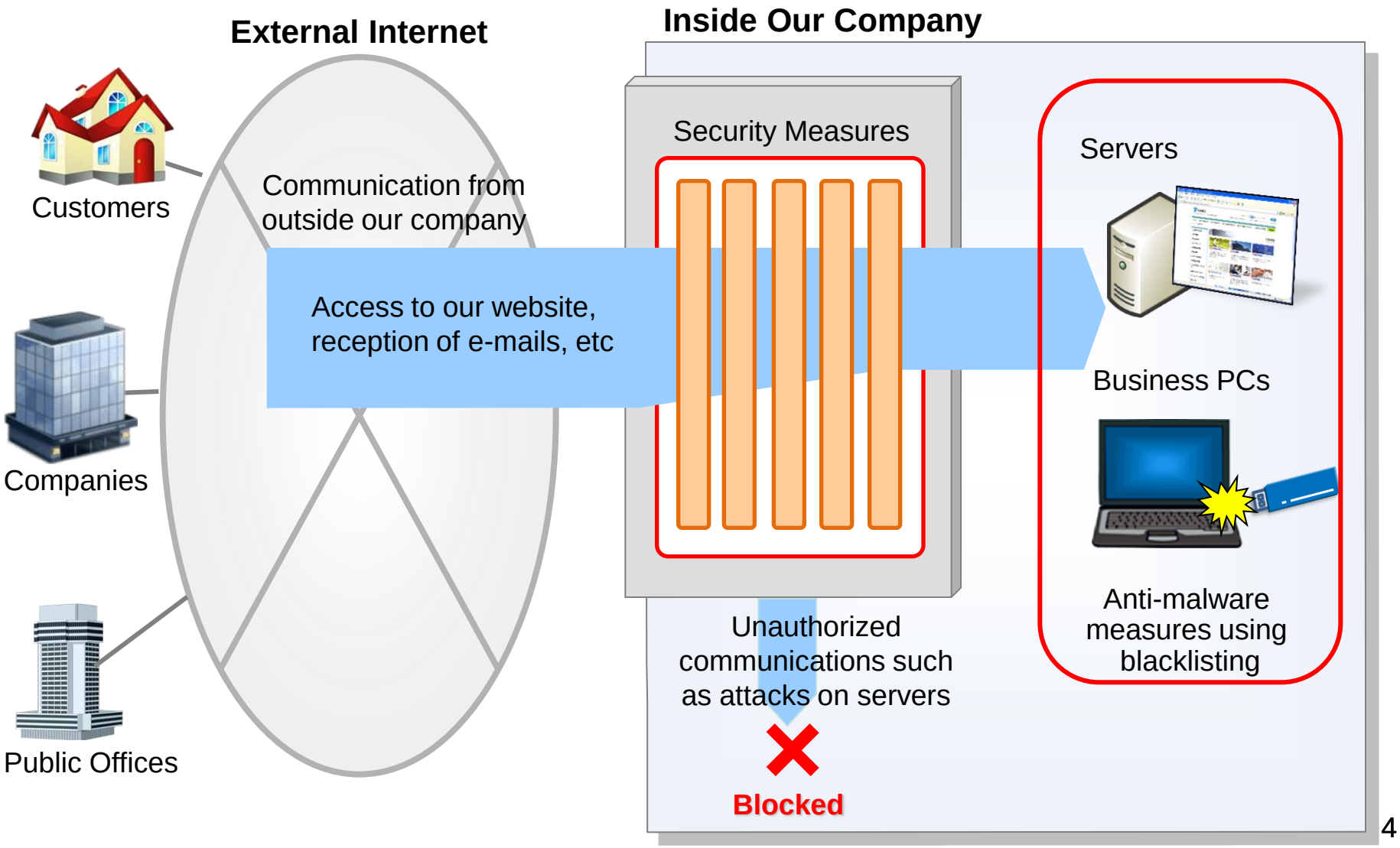
- Announcement by Sony Pictures Entertainment in November 2014
  Sony Pictures Entertainment was subjected to a cyber attack that caused damage such as the leakage of data on movies that have not yet been released and information contained in in-house mails as well as the destruction of data on in-house PCs.

  Although it was later discovered that devices such as PCs had been infected with multiple types of malware, they were new types of malware that were undetectable by anti-malware software available at the time.
- Announcement by Japan Pension Service in June 2015
  The terminals of employees were infected with malware contained in an e-mail originating outside the company, resulting in unauthorized access and leakage of some personal information held by Japan Pension Service. Information including as many as 1.25 million basic pension numbers, names, dates of birth and addresses was leaked.

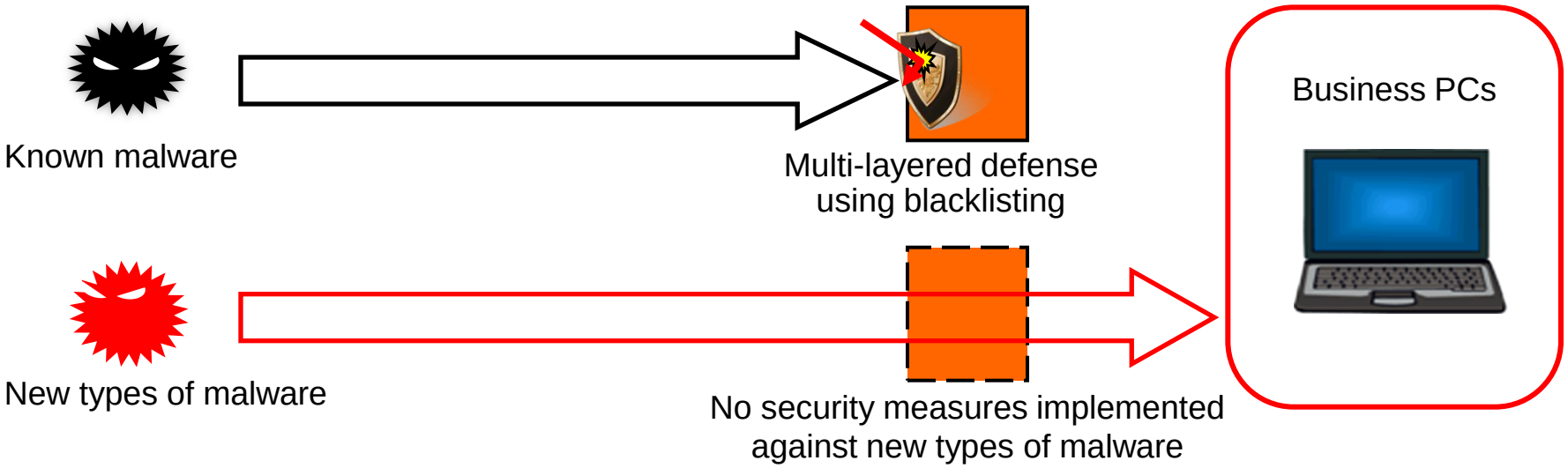


2. Current Status of Security Measures implemented by Our Company

- In-house servers and PCs are protected from malware infection mainly by security measures in place at external Internet connection points.



2. Current Status of Security Measures implemented by Our Company

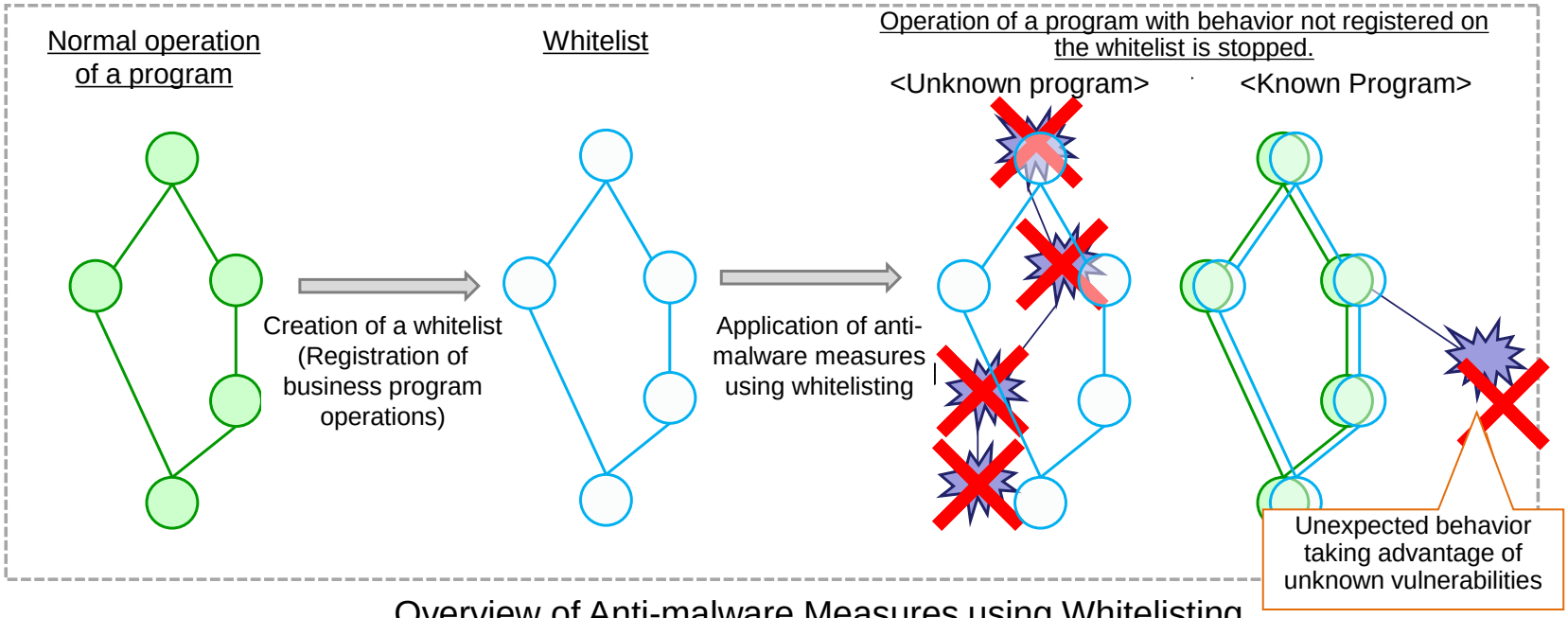


- Although our company has implemented multiple information security measures to protect business PCs from the threat of cyber attacks, these measures use the blacklisting approach and this has presented the problem of being unable to provide protection from zero-day attacks by new types of malware.

Information security measures have been reinforced by introducing “anti-malware measures using whitelisting” into our business PCs to protect against zero-day attacks.

3. Overview of Anti-malware Measures using Whitelisting

- Anti-malware measures using whitelisting represent a system that allows preregistration of normal program operations and stops the operation of any non-registered programs if detected.



Overview of Anti-malware Measures using Whitelisting

Detection mode: Setting in which the details and history of unauthorized behavior of programs not registered on the whitelist are acquired as detection logs

Block mode : Setting in which unauthorized behavior is blocked if detected in addition to detection-mode operation

4. Implementation of Pre-verification to achieve Introduction

- In preparation for the introduction of anti-malware measures using whitelisting, pre-verification was performed to verify detection performance and identify and sort operational issues.

Verification Environment

Terminals verified: Information Systems Dept. (Approximately 100 units)
Other operating depts. (Approximately 40 units in 11 depts.)

Terminal environment: Windows OS
Conventional anti-malware measures using blacklisting were also used.

Verification period: April to December 2012 (9 months)

Operation mode: Detection mode

- During verification, the standard whitelist attached to the whitelist-based defense against malware was utilized, but so many program operations were listed in detection logs as to interfere with the operation of the systems.

This problem made it necessary to carefully examine detection logs and efficiently register normal program operations on the whitelist to reduce the number recorded in the detection logs.

4. Implementation of Pre-verification to achieve Introduction

- Analysis of the detection logs with the aim of reducing the number of program operations recorded in the logs revealed the characteristics shown below.

(1)The program operations of standard OA applications such as Office and Adobe Reader were also detected.

(2)Operations of programs involving communication with business servers were detected.

(3)Operations such as Cookie information uploads to advertizing sites when browsing the Internet were detected.

(4)Free software operations were detected.

4. Implementation of Pre-verification to achieve Introduction

Based on the results of the analysis, the measures listed below were implemented to resolve the problem.

(1) Quality improvements to the software were urged to improve detection accuracy.
(2) & (3) The scope of defense provided by the anti-malware measures using whitelisting was limited to the threat of “information theft” (so that communications completed in-house would not be detected).
(4) A software installation prevention function was mounted in tandem with PC replacements to limit the installation of applications unrelated to business.

With exception of (1) to (4) above, approximately 280 operations (approximately 1% of the whole) were detected and, after careful scrutiny, it was expected that making additional registrations on the whitelist would resolve the problem.

5. Introduction into Our Company's Environment

- Based on the anticipated reduction of the number of program operations recorded in detection logs, the anti-malware software using whitelisting was installed in all in-house business PCs.

  Target terminals: 13,600 units (All business PCs)

  Terminal environment: Windows OS

  Conventional anti-malware measures using blacklisting were also used.

  Installation period: November 2014 to March 2015

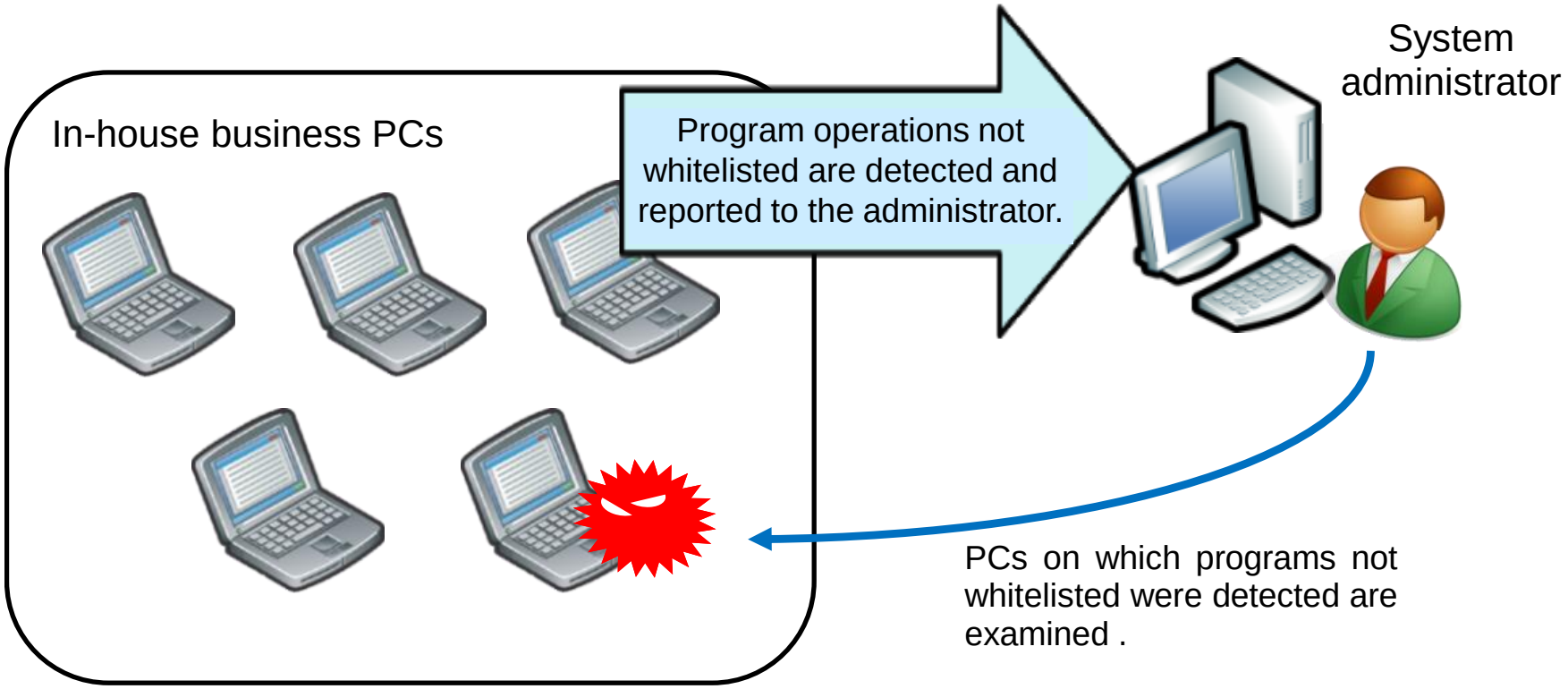
  Operation mode: Detection mode

- To prevent damage such as information leakage caused by intrusion by new types of malware, migration to block-mode operation needs to be implemented as soon as possible. However, program operations for systems commenced after pre-verification and operations of programs used by specific offices have not yet been registered on the whitelist, presenting the risk of interference with business operations.

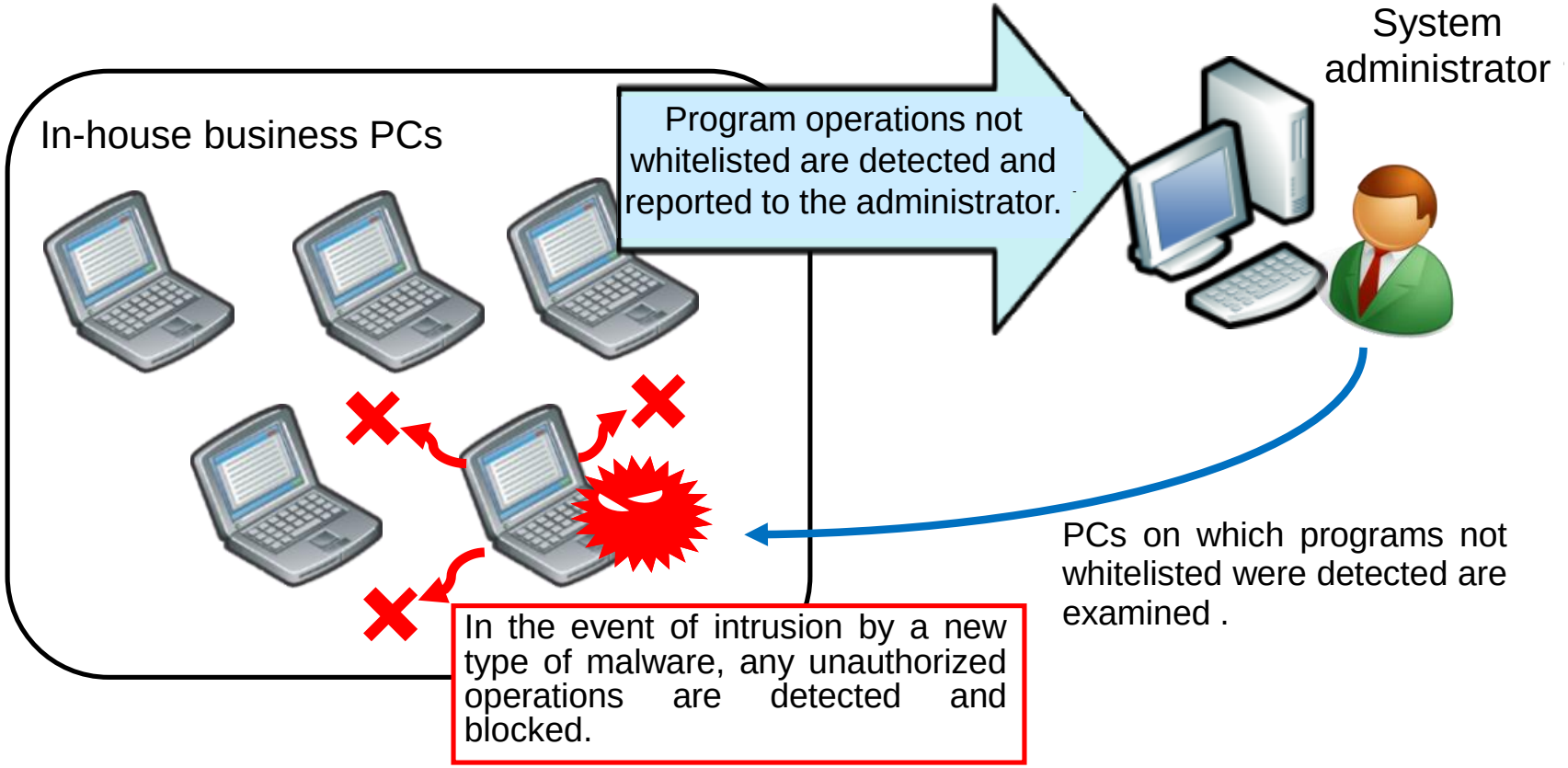
To address this situation, migration to block-mode operation in the following two stages has been planned.

Operation of the anti-malware measures using whitelisting is to be started in the detection mode and, after careful examination, additional registrations made on the whitelist to eliminate false detections.
=> Migration to block-mode operation

- A mechanism has been constructed to detect program operations that have not been whitelisted and report them to the system administrator, thereby enabling monitoring of intrusion by new types of malware.



➢ Migration to block-mode operation is planned as shown below.



6. Operational Status and Evaluation in Our Company

➢ The benefits of monitoring in the detection mode are as follows:

- Intrusion by new types of malware can be detected.
- Closer investigation can be carried out into factors such as damage status and routes of infection in the event of intrusion by a new type of malware.

➢ Incidents detected:

No incidents have been detected since introduction.

7. Current Issues and Future Measures

➢ Current Issues

The block mode cannot currently be applied for the reasons listed below:

- Improvement in detection accuracy through software modifications has not been adequately achieved.
- Since detection logs that could not be identified during the pre-verification are output from multiple business systems, whitelisting requires time. (Some detection logs need time to determine the risks of recorded program operations.)

➢ Future Measures

- Additional registrations on the whitelist need to be made in order to realize the early application of the block mode.
- The efficiency of whitelisting needs to be further improved to deal with constant changes in the system usage environment due to system modifications and the introduction of new systems.
  (e.g.: Accelerated determination of risk)

Special Report

Special Report①

Is it possible to describe how effective this solution is?
Are there any other experiences using White Listing within other EPUs?

Other Anti-malware Software of white list type are most products that prohibits the start of the program that are not allowed in the white list .

We use a variety of programs in our Office . If we use other Anti-malware Software of white list type , we need to register all of the software on the white list .
But it will not be able to operate . On the other hand , Anti-malware measure of whitelisting to block malware has been limited . In addition , we are able to specify the area to monitor (folder , IP address , other processes) .

Therefore , we do not need to register all of the programs to be used on business in the white list .

There are some other experiences using White Listing within other EPUs.

Special Report②
What are the possibilities to successfully implement this solution within other EPUs?

Although the number is not clear, there are some actual results of introduction in Japan.

Even the way of operation has few differences, the whitelisting acts as expected in other EPUs.

Thank you for your attention.