HITACHI
Inspire the Next

24th Annual FIRST Conference

Feasibility study of scenario based self training material for incident response

June 21, 2012

Hitachi Incident Response Team
Chief Technology and Coordination Designer
Masato Terada
http://www.hitachi.com/hirt/

HITACHI
Inspire the Next

Opening

The transition of incidents over several years is concerned, a new type of security breach arises in a short cycle time, and remains constant once established. This situation leads many users and engineers to these incidents. Also, it is difficult to acquire and share incident cases among some organizations by the targeted attacks for incident readiness.

This presentation shows the concept of "scenario based self training material for incident response" to solve above problems.

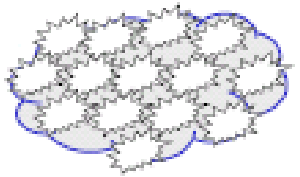
HITACHI
Inspire the Next

Contents

1. Introduction
2. Related works
3. Our proposal for "scenario based self training material for incident response"
4. Example of material
5. Conclusions

HIRT Hitachi Incident Response Team

Transitions of incidents

Period	Features	Impact model
2000 -2001	Single occurrences of homogeneous impact over a wide area Website defacement	
2000 -2005	Chain reaction of homogeneous impact over wide area. Dissemination of mails with viruses attached Spread of network worms	
2005-	Local impact of a similar kind Web site attacks through SQL injection Phishing, Spyware, Bot viruses, etc.	
2006-	Local impact of various kinds Targeted attacks Web malware, USB malware, etc.	

HIRT Hitachi Incident Response Team

Research motivation

- **How we can provide a training resource for the general users and new comer engineers that helps their understanding for incident response of old and new type ?**

Old type (2001-2004)
(ex. network worm infection etc.)

New type (2008-)
(ex. Targeted Attack such
as Advanced Persistent Threat etc.)

HIRT Hitachi Incident Response Team

Virtual Training Environment (VTE)

- VTE provides e-learning delivered right to Web browser.
  - On-demand lecture in the form of video, audio presentations, and demonstrations
  - Hands-on lab environments
  - A learning management system to manage enrollments and track progress

- VTE provides the following contents.
  - Malware Analysis Apprenticeship
  - Fundamentals of Incident Handling
  - Advanced Incident Handling etc.

Virtual Training Environment (VTE)
https://www.vte.cert.org/vteWeb/

2. Related works

KYT (Kiken Yochi Training in Japanese)

- **KYT is popular in real field of manufactures in Japan, for realizing zero disaster.**
- **KY is a ability to anticipate risks, while working in the field.**
- **KYK is a typical training to discover direct causes for dangerous areas and actions about intended tasks visually and consider measures against them, based on the utilization of illustrations and scene photographs.**

Manabu Sawaguchi: A Study of Effective Risk Management Approach for "ICT-Based Risks“
ICBI 2011

HIRT Hitachi Incident Response Team

Basic steps of KYT

- Step1: Comprehension of facts at intended tasks
- Step2: Investigation into essential cause of intended tasks
- Step3: Considering the proposed measures
- Step4: Decision of activity plan about proposed measures

What kind of risks in this situation ? (Step1)

Step1:What kind of risks in this situation?

Please point out many risks in this illustration.

You are cleaning the door at the emergency stair step of the outside.

Japan Industrial Safety & Health Association
http://www.jisha.or.jp/zerosai/kyt/index.html

HIRT Hitachi Incident Response Team

Basic steps of KYT

Step1:What kind of risks in this situation?

Please point out many risks in this illustration.

You are cleaning the door at the emergency stair step of the outside.

He puts a hand in the door gap.

He falls from the stair.

Japan Industrial Safety & Health Association
http://www.jisha.or.jp/zerosai/kyt/index.html

HIRT Hitachi Incident Response Team

Basic steps of KYT

Step2:Point out essential cause of risks

The footstool is high.
He falls from the stair

Step3:Considering the measures

Move footstool to wall side.

Use safety belt.

Step4:Decision of action plan

Use safety belt.

Japan Industrial Safety & Health Association
http://www.jisha.or.jp/zerosai/kyt/index.html

HIRT Hitachi Incident Response Team

Let's try a KYT of information security !

Step1:What kind of risks in this situation?

HIRT Hitachi Incident Response Team

Let's try a KYT of information security ! (cont.)

Step2:Point out essential cause of risks

PC may infect by conficker.

Step3:Considering the measures

Update virus definition.

Don’t use personal USB.

Step4:Decision of action plan

Disable autorun

Japan Industrial Safety & Health Association
http://www.jisha.or.jp/zerosai/kyt/index.html

HIRT Hitachi Incident Response Team

Let's try a KYT of information security ! (cont.)

Step2:Point out essential cause of risks

Prediction of the threats and that flows by imagination

sures

Step4:Decision of action p

Japan Industrial Safety & Health Association
http://www.jisha.or.jp/zerosai/kyt/index.html

HIRT Hitachi Incident Response Team

Research motivation (again)

- **How we can provide a training resource for the general users and new comer engineers that helps their understanding for incident response of old and new type ?**

Keywords for the solution are "scenario based" and "self training".

Old type (2001-2004)
(ex. network worm infection etc.)

New type (2008-)
(ex. Targeted Attack such as Advanced Persistent Threat etc.)

3. Our proposal

scenario based self training material

- Many incidents disclose some snapshot information (ex. privacy information disclosure, SQL injection and etc.), but we can't acquire incident details such as response scenario. In other words, we can't publish our incident details in many cases, too.

- Therefore, we propose the concept of "scenario based self training material for incident response" that makes new incident scenario by selecting and combining parts from many facts.

3. Our proposal

(1) fact based

- Use of the story (scenario based) which describes incident response activities by timeline based.
  - The story is composed by the facts.
  - The facts are customized (or anonymized) in that story.

The story is virtual story and is not fact.
But it is based on fact.

3. Our proposal

(1) fact based - timeline

- **Timeline based story provides overview of incident flow and time span (for prediction of the threats and that flows by imagination).**

  - **DAY1 (April 20, 20XX)**
    We built a conference web server with the database on the cloud environments.
  - **DAY2 (May 29, 20XX)**
    An external organization notified us. "Unauthorized access to SSH from conference web server".
  - **DAY3 (May 30, 20XX)**
    We began to examine the logs of the firewall and web server.

3. Our proposal

(1) fact based - timeline

- **June 21, 2012: Plenary session … Good example**
  - **April 11, 20XX (9AM)**
  - **9:30AM Laptop Retrieved from Guards**
  - **9:45AM Blade host - Host Forensics**
  - **10AM - Kickoff "Prior24" Network Forensics**
  - **11AM - Beacons, Beacons Everywhere**
  - **11:10AM - All Hands on Deck !!!!**
  - **11:15 AM - War Room**
  - **11:30AM Realization that our laptops are also owned**
    Owned Systems List Grows
    Further Analysis = Full Domain Compromise
  - **1:44 PM - Extortion Email Arrives**
  - **April 22, 20XX (9AM) - Time to Eradicate and rebuild**

3. Our proposal

(1) fact based - customized

- **Customized story provides virtual story which is not fact and is the based on fact (for prediction of the threats and that flows by imagination).**
  - **Facts**
    - ✓ **DAY1 (April 11, 2012): Post #Operation FIRST 2012**
      DDoS attack to www.first.org on June 21, 2012
    - ✓ **DAY2 (June 11, 2012): Detection of DDoS attack**
      DDoS Attacks Exceed 1 Gbps

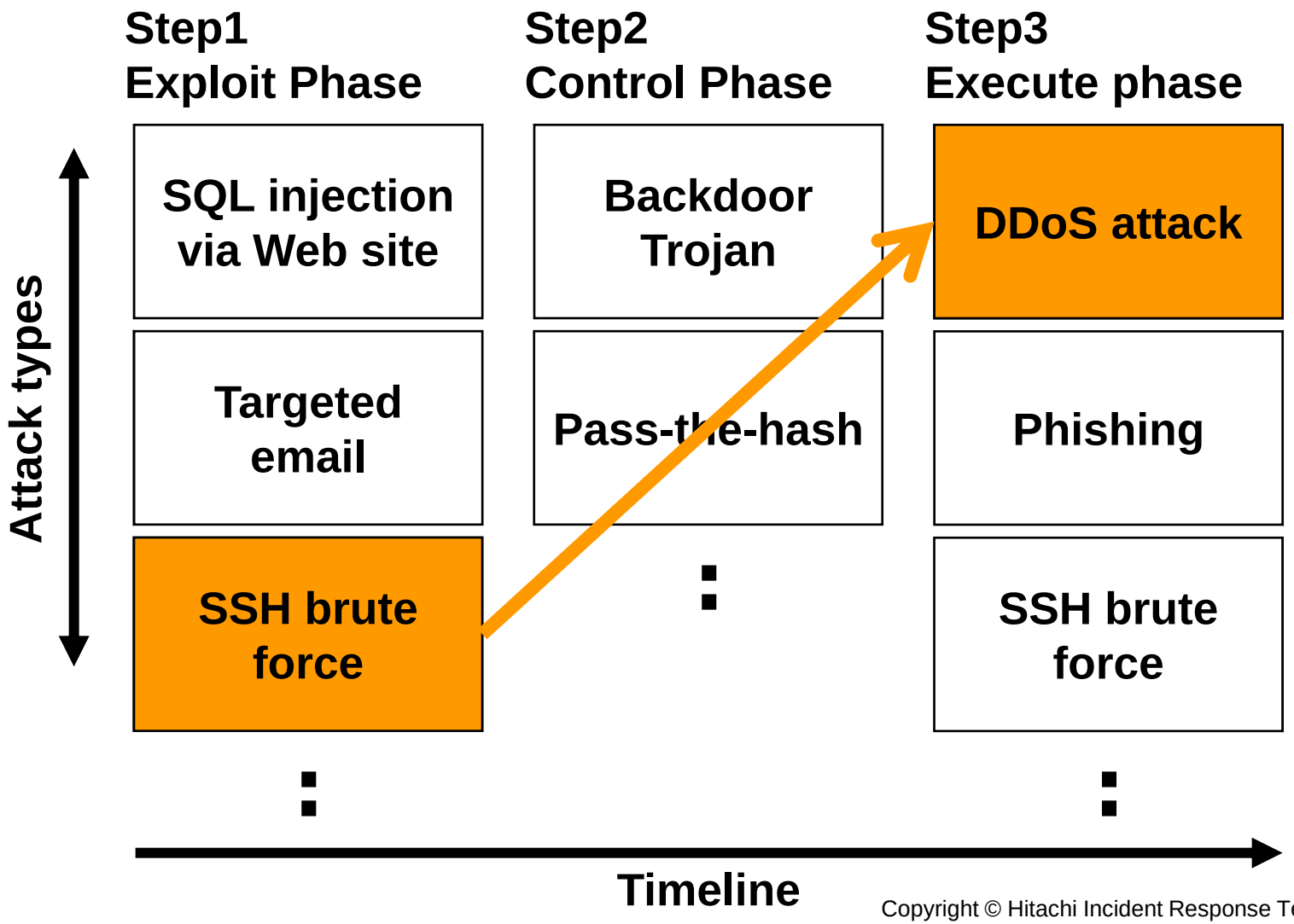
  - **Customized (or anonymized) in our story**
    - ✓ **DAY1 (April 22, 20XX): Post #Operation SECOND 20XX**
      DDoS attack to www.second.org on June 21, 20XX
    - ✓ **DAY2 (June 22, 20XX): Detection of DDoS attack**
      DDoS Attacks Exceed 100 Mbps

(2) selected and combined by parts

- Making of new story (incident scenario) by selecting and combining parts from many facts.
  - We split an incident into some blocks. For example, Step1: Exploit Phase, Step2: Control Phase and Step3: Execute phase.
  - We make new story by selecting and combining parts from customized blocks.

Creation of new story is easier.
Also new story is virtual story, too.

(2) selected and combined by parts



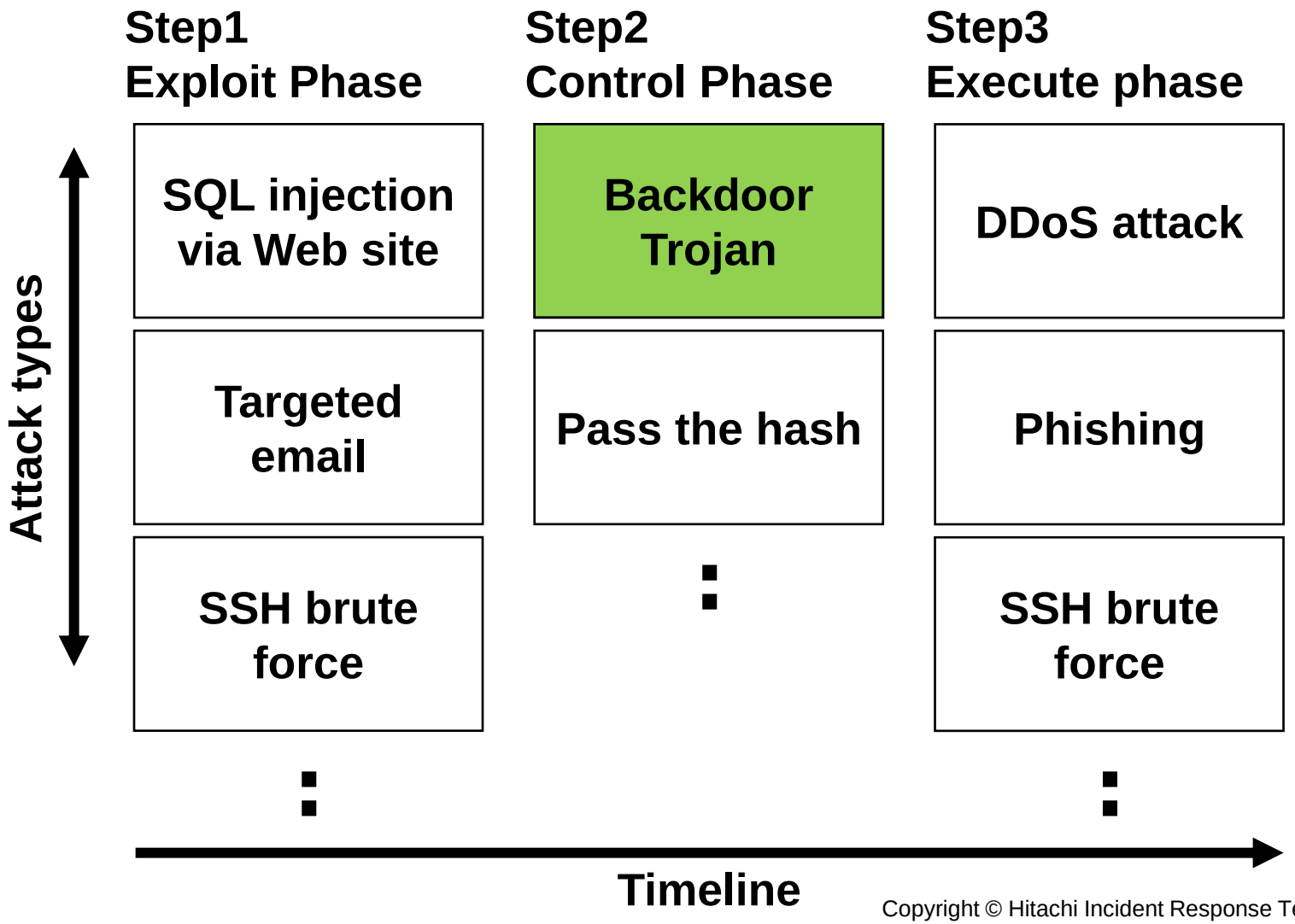
Hitachi Incident Response Team

(3) review points provided

- To present the review or discussion points to consider measure of incident readiness or incident response process (for prediction of the threats and that flows by imagination).
  - Questions (ex.)
    - In build steps of a Web server, what's missing in security measures ?
    - In build steps of a Web site, what's missing except Web serever in security measures ?

4. Example of material

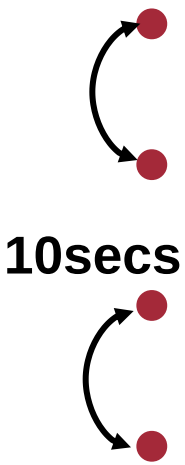
Example of block part … Poison Ivy



4. (1) Example of block part

DAY1(20XX-10-23) Detection of malicious proxy log

- **We detect a following repeated events in user authenticated proxy log.**

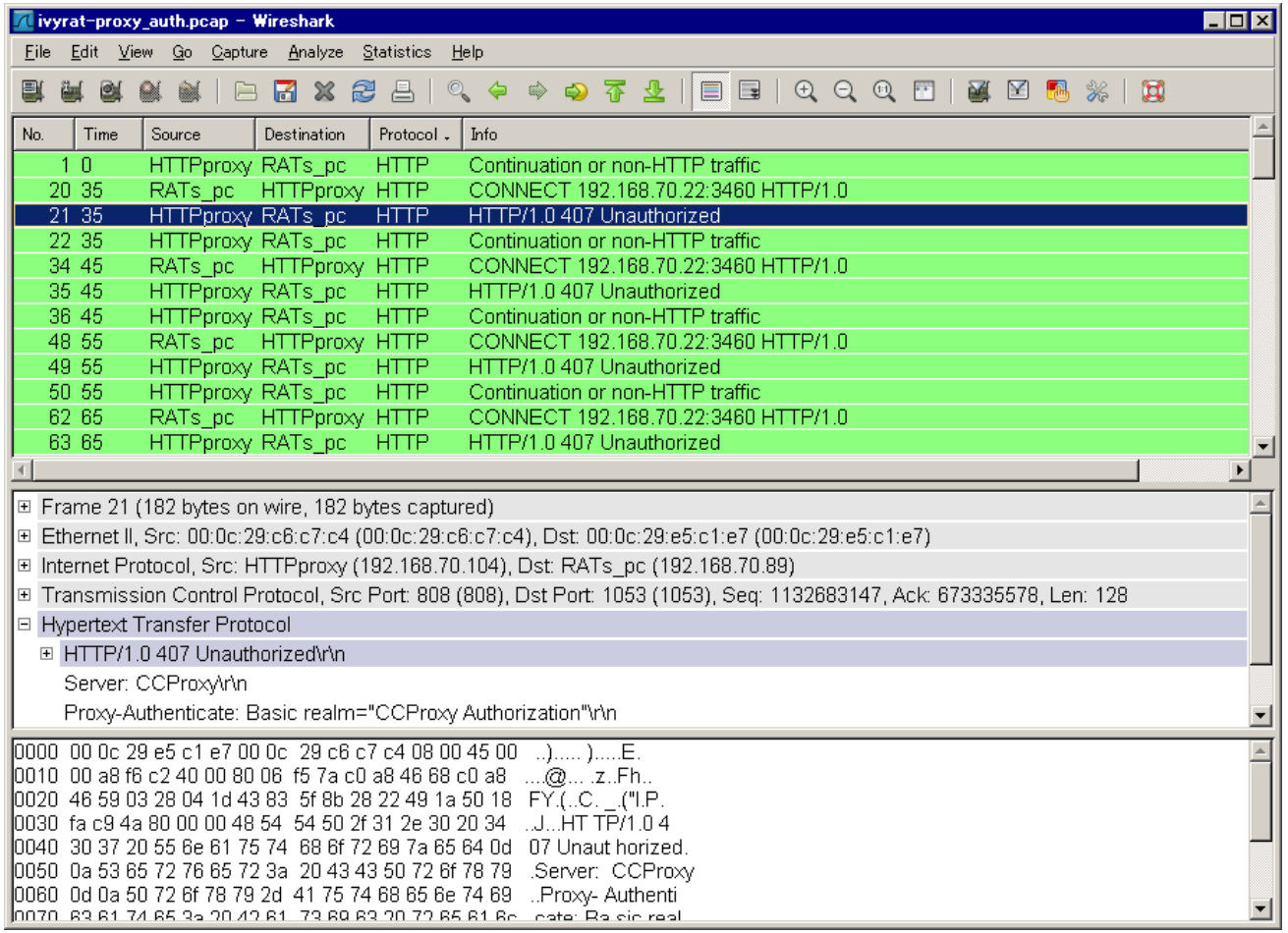



```
1319379001.773 0 192.168.70.89 TCP_DENIED/407 2117
CONNECT 192.168.70.22:3460 - NONE/- text/html
1319379011.796 0 192.168.70.89 TCP_DENIED/407 2117
CONNECT 192.168.70.22:3460 - NONE/- text/html
1319379021.814 0 192.168.70.89 TCP_DENIED/407 2117
CONNECT 192.168.70.22:3460 - NONE/- text/html
1319379031.949 0 192.168.70.89 TCP_DENIED/407 2117
CONNECT 192.168.70.22:3460 - NONE/- text/html
1319379041.964 0 192.168.70.89 TCP_DENIED/407 2117
CONNECT 192.168.70.22:3460 - NONE/- text/html
```

4. (1) Example of block part

DAY1(20XX-10-23) Detection of malicious proxy log

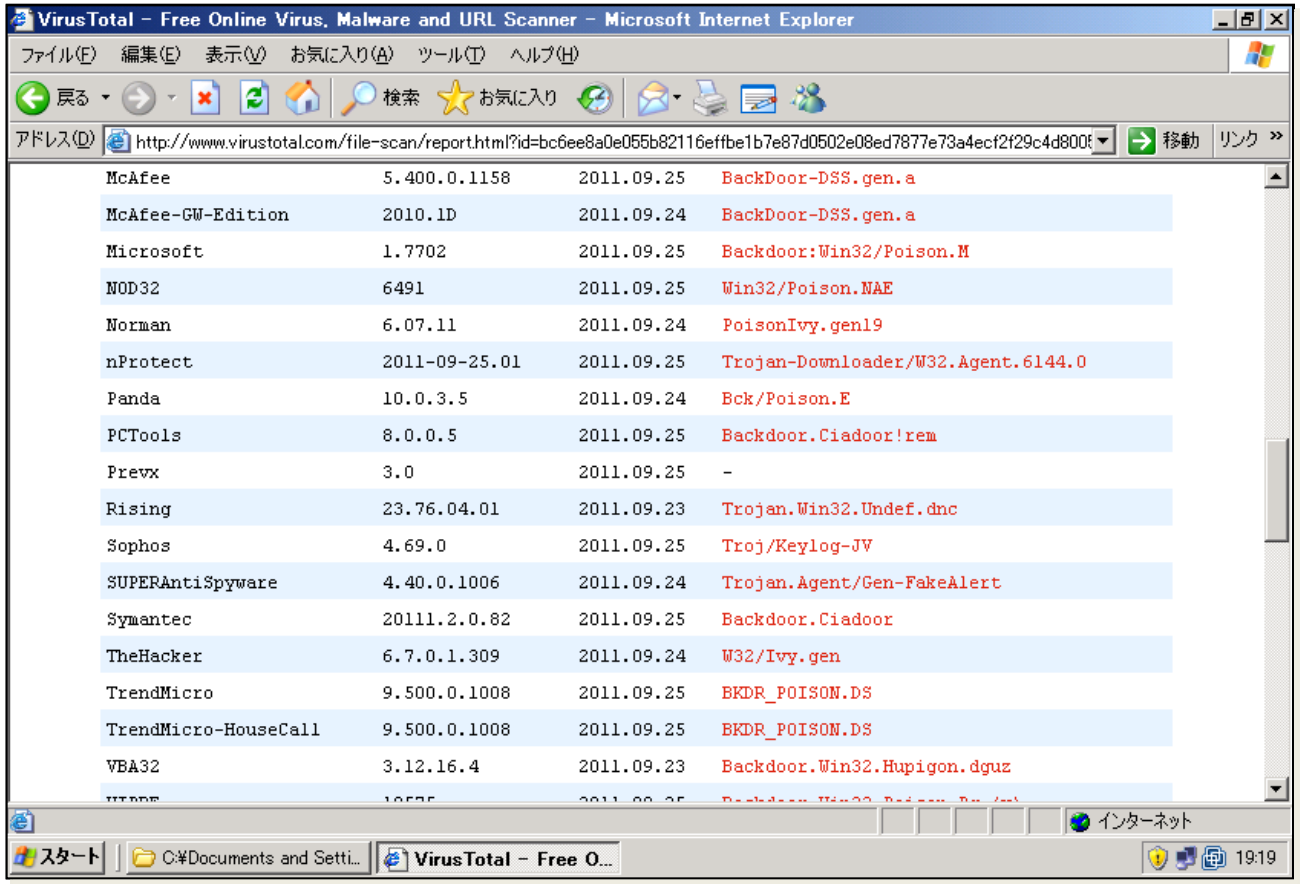
- **Also, the repeated network events exist in captured traffic.**



4. (1) Example of block part

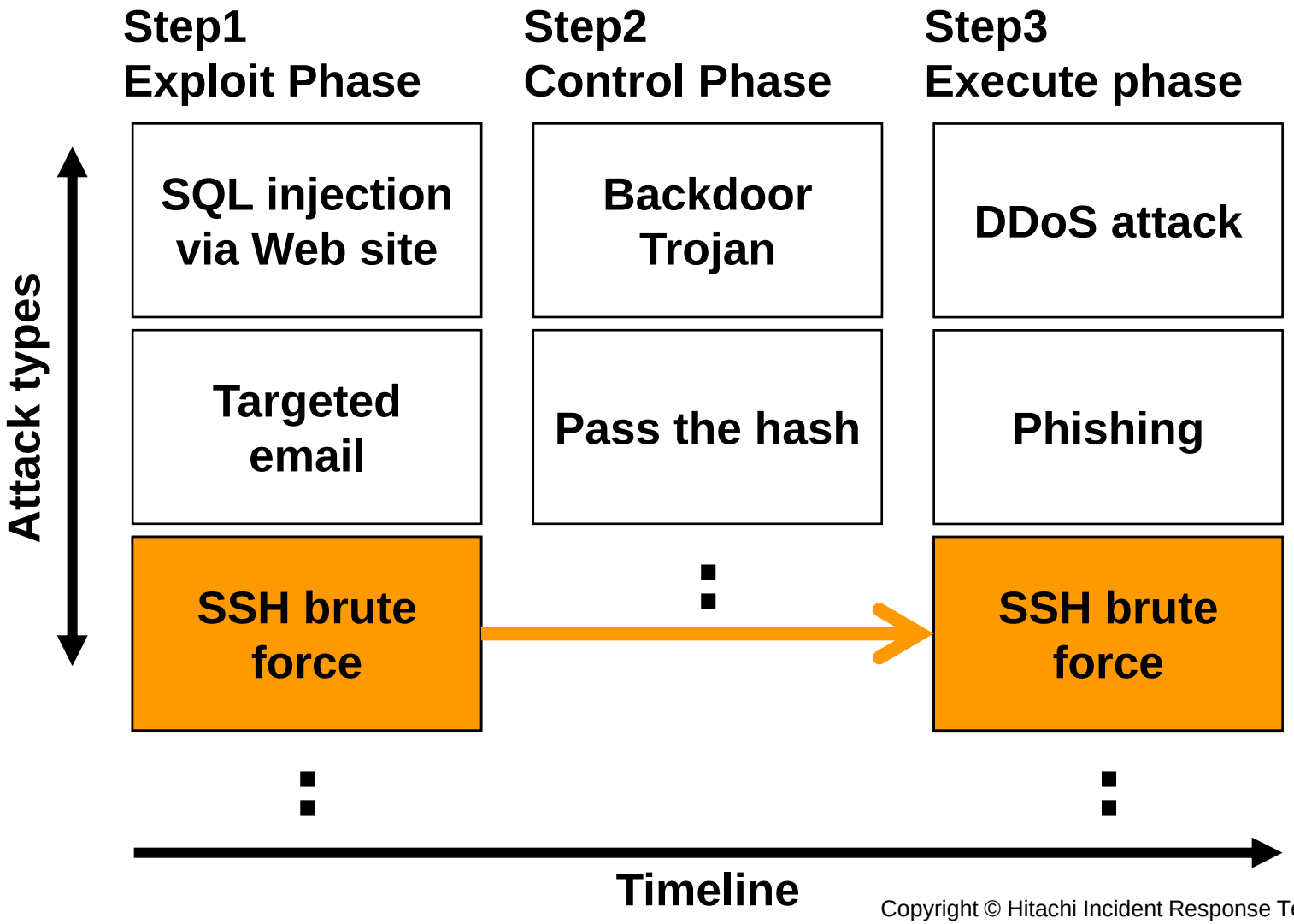
DAY2(20XX-10-24) Identification of infected PC

- **We identify the infected PC and find out the execution files which includes Poison Ivy.**



4. Example of material

Example of material … SSH brute force



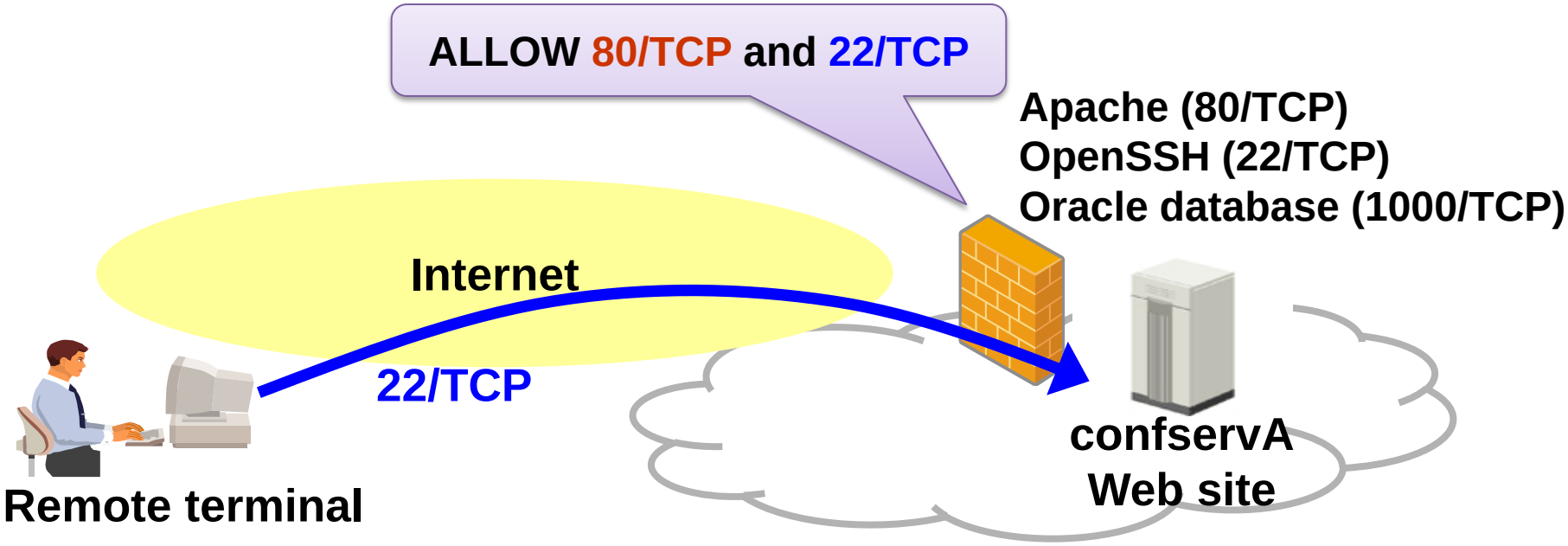
4. (2) Example of material

DAY1(20XX-04-20) Construction of a conference web site

- **We built a conference web site with the database on the cloud environments.**
  - **Web site (confservA)**
    - **Apache (80/TCP)**
    - **OpenSSH (22/TCP)**
    - **Oracle database (1000/TCP)**
  - **Firewall rules**
    - **HTTP access (80/TCP) of Internet and confservA: ALLOW**
    - **SSH access (22/TCP) of Internet and confservA：ALLOW**

DAY1(20XX-04-20) Construction of a conference web site

- We built a conference web site with the database on the cloud environments.



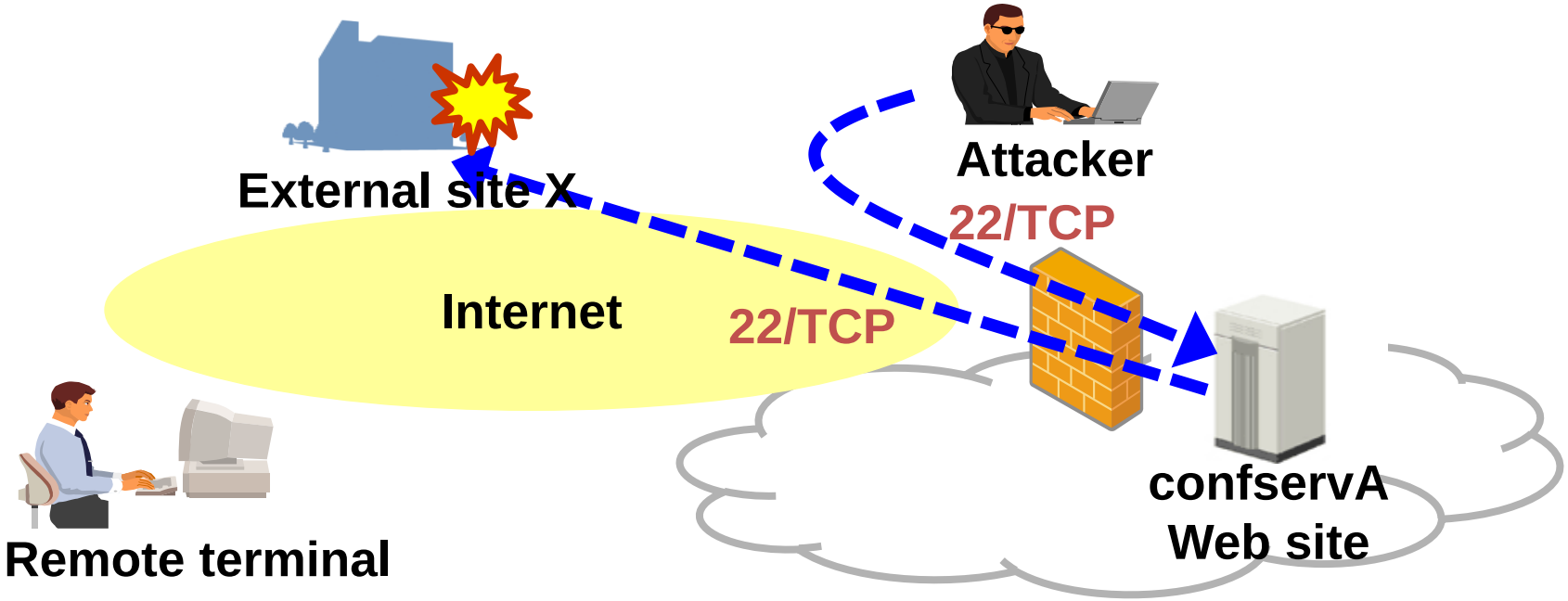
4. (2) Example of material

DAY2(20XX-05-29)：Receive a notification

- **An external site X notified us. "Unauthorized access to SSH from confservA". We examined the logs of the firewall. There is an enormous amount for the Internet access via SSH from confservA.**
  - **Investigation summary of firewall logs**
    - **At least 7 days before, a lot of SSH access to the Internet from confservA.**
    - **Over 30,000 records of SSH access to the external site X.**

DAY2(20XX-05-29):Receive a notification

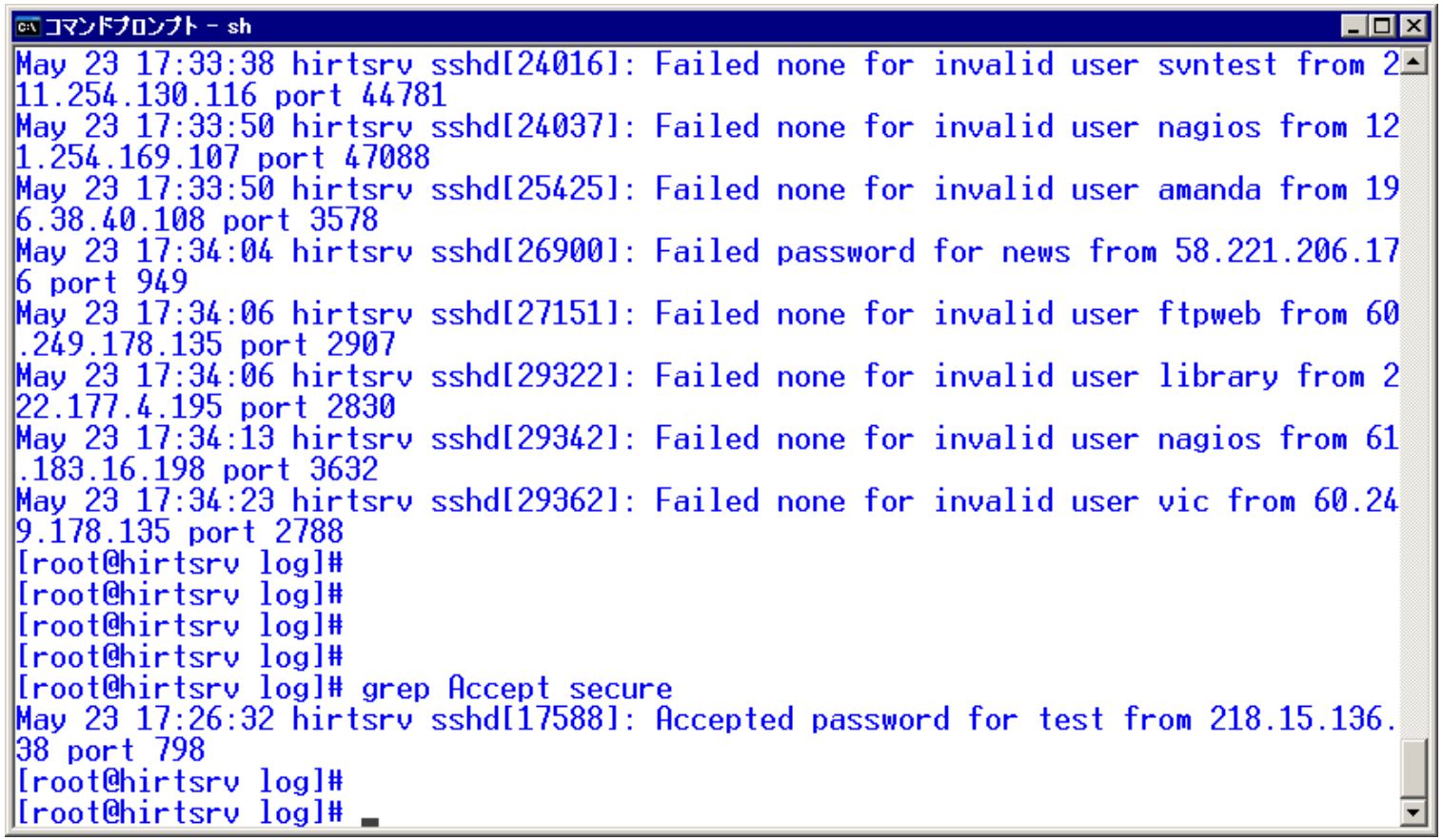
- An external site X notified us. "Unauthorized access to SSH from confservA". We examined the logs of the firewall. There is an enormous amount for the Internet access via SSH from confservA.



4. (2) Example of material

DAY3(20XX-05-30):Start of investigation of the incident

- **We investigated logs of confservA (/var/log/secure.log). There was a lot of failed evidence for log in SSH.**



4. (2) Example of material

DAY3(20XX-05-30):Detailed investigation (cont.)

- **The investigation revealed matters are as follows.**
  - **confservA was hacked by SSH brute force attack.**
    There are over 30,000 logs of SSH Login failed. Login failed count list of each account is shown in the right table.
    - `sshd[25425]: Failed none for invalid user …`
    - `sshd[26900]: Failed password for …`
  - **The break-in at 17:26 on May 23.**
    - `May 23 17:26:32 shirt sshd[17588]: Accepted password for test from 218.15.136.38 port 798`

4. (2) Example of material

DAY3(20XX-05-30):Detailed investigation (cont.)

- **The investigation revealed matters are as follows.**
  - **The account "test" was used to intrusion. In addition, this account is the database account, too. When we install the program on the database server, the password for OS was added automatically.**

Login failed count

ID	Count
root	51048
test	2290
admin	1890
user	1220
oracle	1157
guest	934
nagios	900
info	588
web	544
Other	138117

HIRT Hitachi Incident Response Team

Questions

- In build step of a Web site, what's missing in security measures ?

- In build step of a Web site, what's missing except confservA in security measures ?

Now, Let's try it.

Please raise your hand if you have comments for security measures of this case.

5. Conclusions

We have presented:

- **We can’t response to all incidents and want no incidents. But, we (the general users, new comer engineers and CSIRTs) need to gain experience of old and new various incidents.**

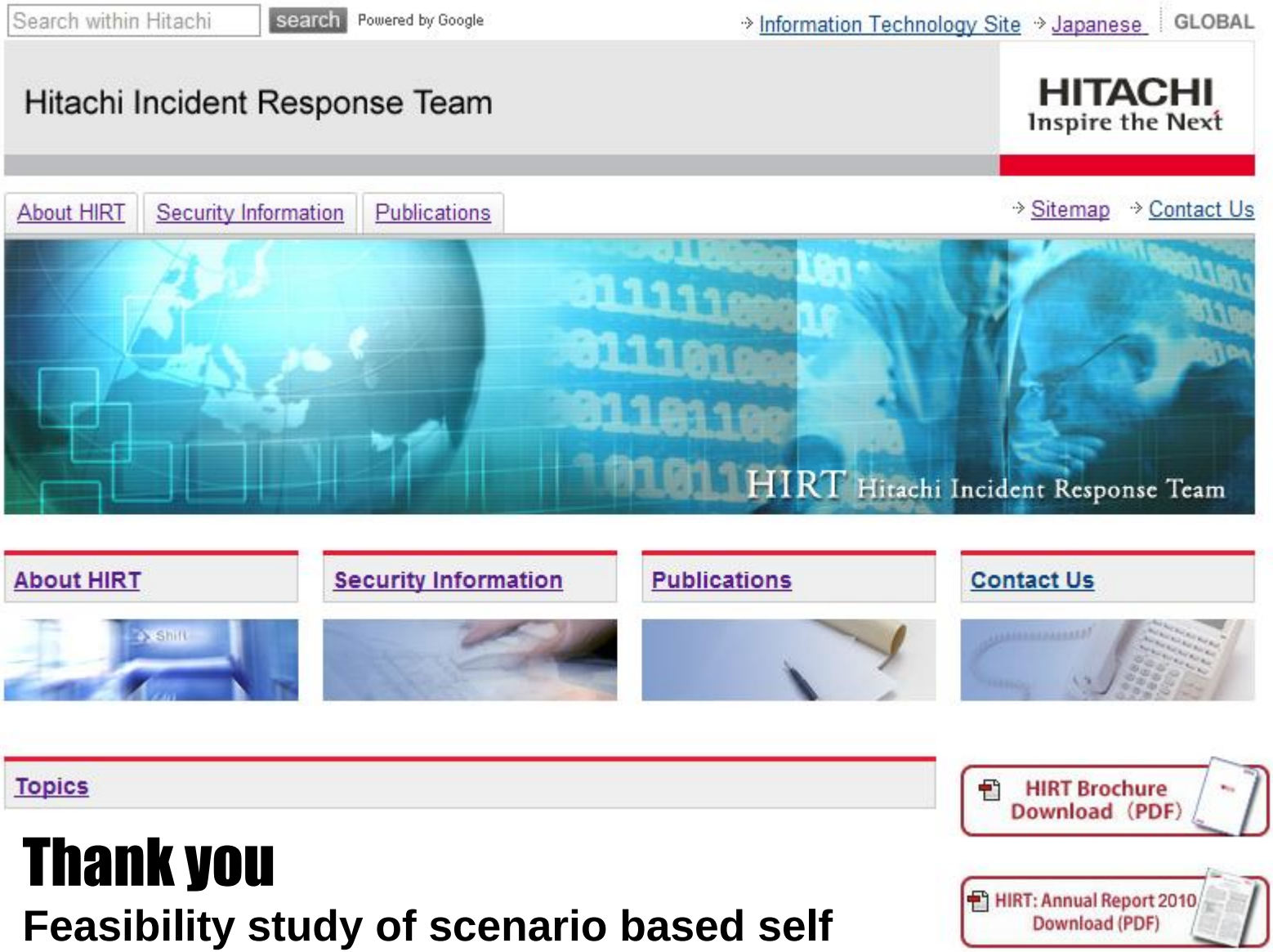
- **We have shown the concept of "scenario based self training material for incident response" in this presentation.**

5. Conclusions

Our future plans:

- Research of many incident (response) cases, especially targeted attack. Making several parts based on the above research, then making new virtual story from several parts.
- We will combine our approach with the following activities.
  NTT-CERT "A study for CSIRTs strengthening: From a Viewpoint of Interactive Srotytelling in an Organization".
- Also, we would like to propose our activities to FIRST Education Committee.

http://www.hitachi.com/hirt/



Thank you

Feasibility study of scenario based self training material for incident response


HITACHI
Inspire the Next