Information Security Laboratory
ISL

SADFE 2016
Keynote Presentation

SEP. 23 , 2016

Digital Forensics Trends in Japan

Professor, Tokyo Denki University
Ryoichi Sasaki
sasaki@im.dendai.ac.jp

Table of contents

My Profile (1)

Dr. Sasaki received his B.S. Degree in health science and Ph.D Degree in system engineering from the University of Tokyo in 1971 and 1981, respectively.

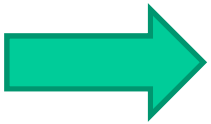
From April of 1971 to March of 2001, he was engaged in the research and research management related to systems safety, network management and information security at Systems Development Laboratory of Hitachi Ltd.

HITACHI
Inspire the Next

My Profile (2)

Dr. Sasaki started the study of information security in 1984. He is a co-inventors of the cipher named MULTI, which is the Japanese Digital Satellite Broadcast System standard.

In 2001, he moved from Hitachi ltd. to Tokyo Denki University



Profile of Dr. Ryoichi Sasaki

(1) Professor, Tokyo Denki University(TDU)

(2) Director of Cyber Security Institute of TDU

(3) Cyber Security Advisor, NISC (National Center of Incident readiness and Strategies for Cyber Security Information Center, Cabinet Office, Government of Japan)

(4) Visiting Professor, National Institute of Informatics

(5) Former General Chair, Japan Society of Security Management

(6) General Chair of Institute of Digital Forensics

University Overview

- Tokyo Denki University is a private university for future engineers located in Adachi, Tokyo, Japan.
- Our founding spirit is “Respect for Practical Studies” .
- The predecessor of the school was founded in 1907. It was chartered as a university in 1949.

TDU

First President of our University

Dr. Niwa and Origin of FAX

Dr. Niwa, the first president of our university, invented an original means of transmitting information, which later became known as “facsimile” or “Fax”.

Profile of Dr. Ryoichi Sasaki

(1) Professor, Tokyo Denki University(TDU)

(2) Director of Cyber Security Institute of TDU

(3) Cyber Security Advisor, NISC (National center of Incident readiness and Strategies for Cyber Security Information Center, Cabinet Office, Government of Japan)

(4) Visiting Professor, National Institute of Informatics

(5) Former General Chair, Japan Society of Security Management

(6) General Chair, Institute of Digital Forensics(IDF)

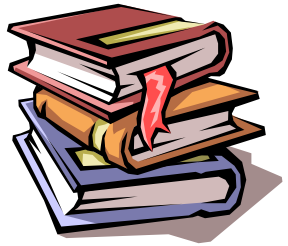
Table of contents

Early History on Digital Forensics in Japan

In 1996: The Japan National Police Agency (NPA) set up a section tasked with the mission of dealing with digital forensic issues triggered by the Subway Sarin Incident.

In 2003 : The first company formed to deal exclusively with digital forensics was established in Japan.

In 2004 : The institute of Digital Forensics (IDF) was established.



Background

On March 20, 1995, Aum Shimrikyo cult members released sarin gas in Tokyo's subway trains, killing 13 passengers and station workers, and injuring some 6,000.

Background

In Aum Shirikyo, there were many educated members who have high level knowledge with regards to information technologies.

They used cryptography including public key cipher to protect their data files.

=> Japanese National Police Agency set up the section having the mission to handle the digital forensic issue.

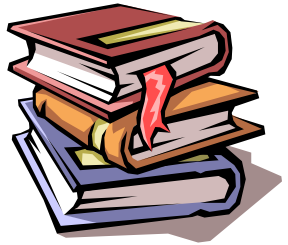
Shokou Asahara
Aum Shinrikyo founder

Early History on Digital Forensics in Japan

In 1996, The NPA began efforts to deal with the digital forensic issues related to the Subway Sarin Incident.

In 2003 : The first company formed to deal exclusively with digital forensics was established in Japan.

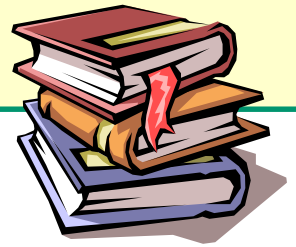
In 2004 : The Institute of Digital Forensics(IDF) was established.



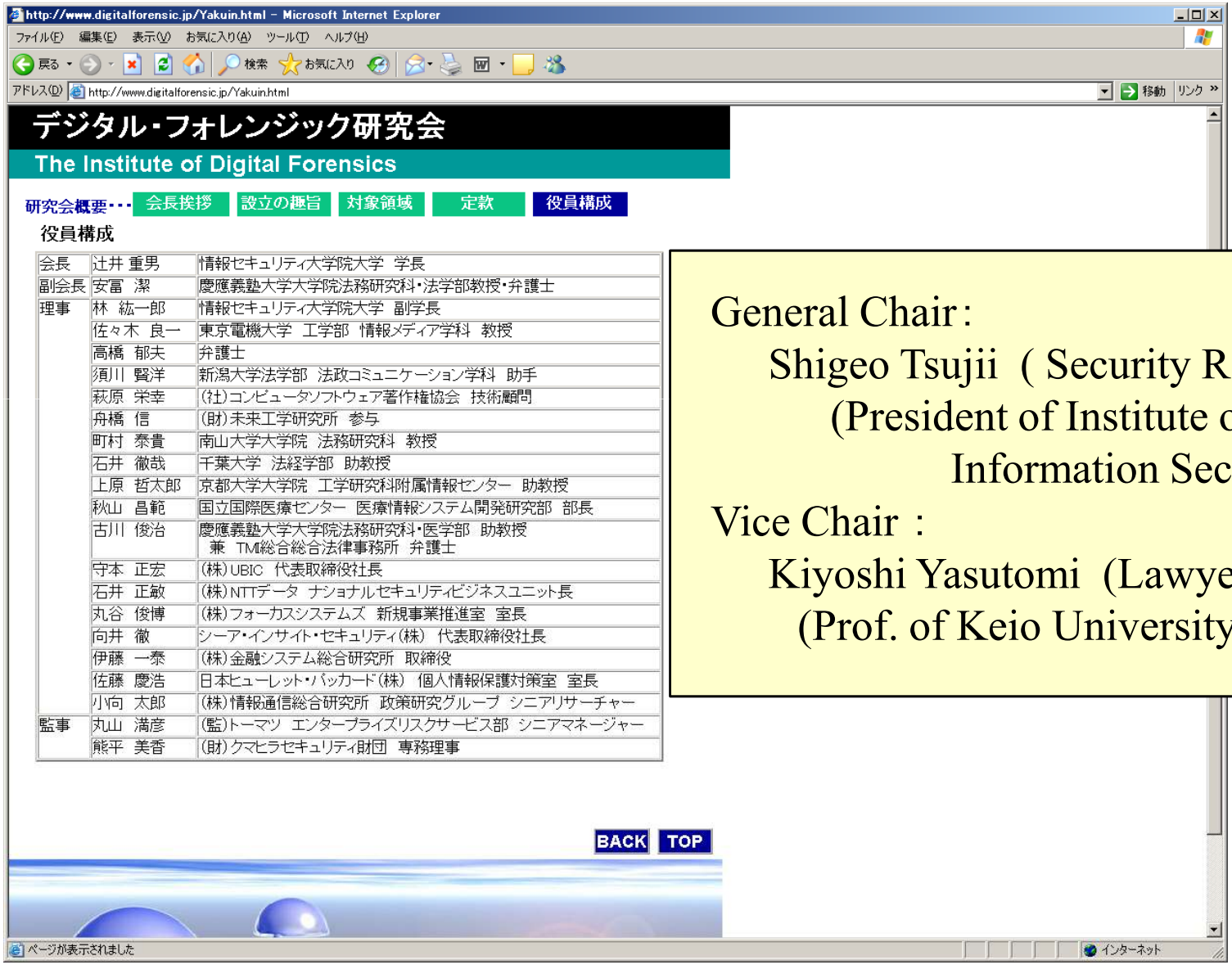
Institute of digital forensics(IDF)

The IDF is a non-profit organization (NPO) dedicated to spreading and promoting digital forensics, as well as contributing to the realization of a healthy information technology (IT) society.

IDF membership includes security researchers, digital forensic engineers, people concerned with digital forensic law and law enforcement, as well as digital
forensic users.



Main Member of IDF at Formation



General Chair:
Shigeo Tsujii (Security Researcher)
(President of Institute of Information Security)

Vice Chair :
Kiyoshi Yasutomi (Lawyer)
(Prof. of Keio University)

Table of contents

Main IDF Activities

In 2004: The IDF was established. The first digital forensic conference, which was called the Digital Forensic Community, was held in December of this year.

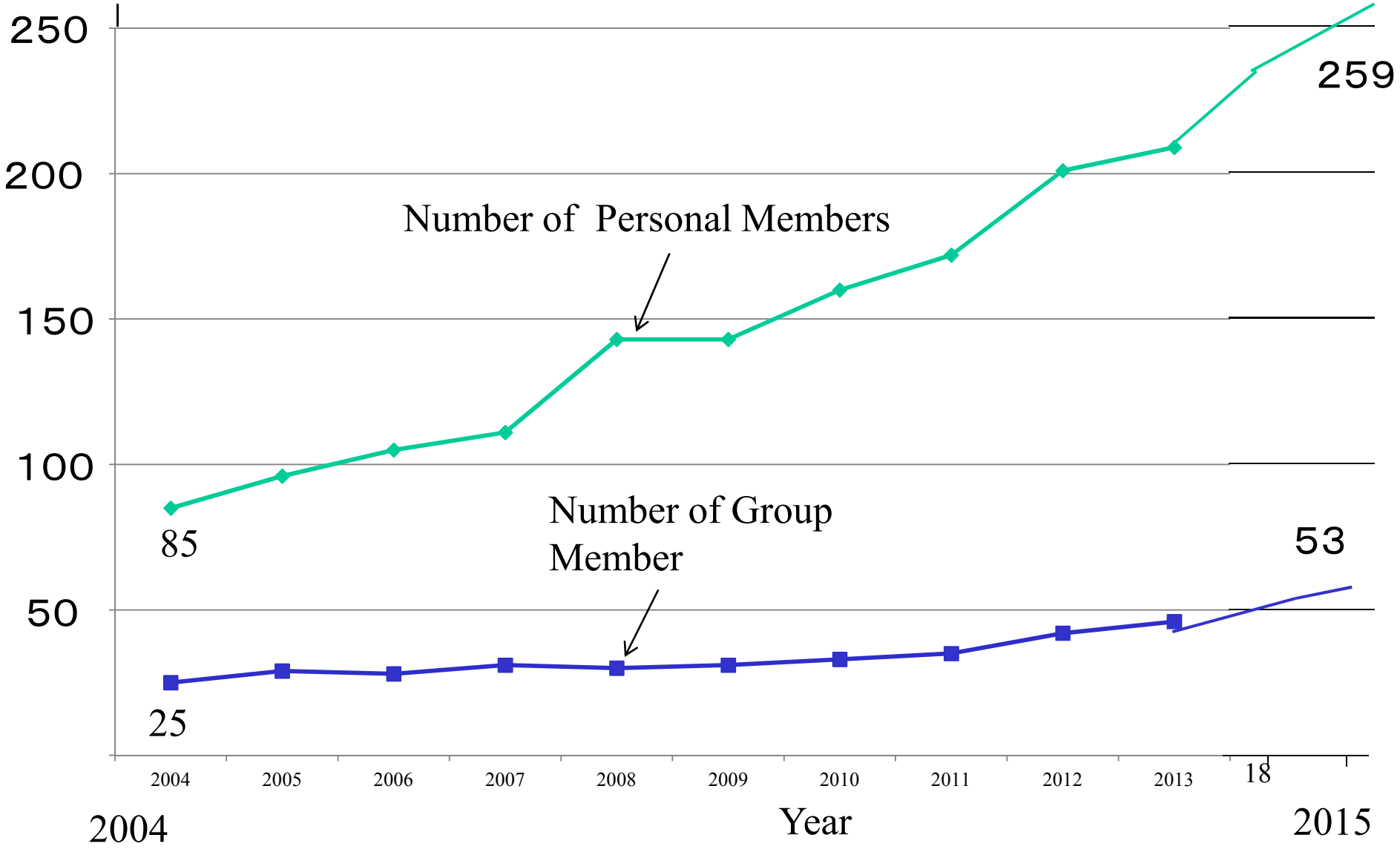
In 2006: The Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of the IDF.

In 2011: The first Digital Forensic Introductory Training hosted by IDF was conducted.

In 2012: The Guideline for Maintaining Evidence (Version 2) was released by the IDF.

In 2015: The Revised Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of the IDF.

IDF Membership Growth



Main IDF Activities

In 2004: The IDF was established. The first digital forensic conference, which was called the Digital Forensic Community, was held in December of this year.

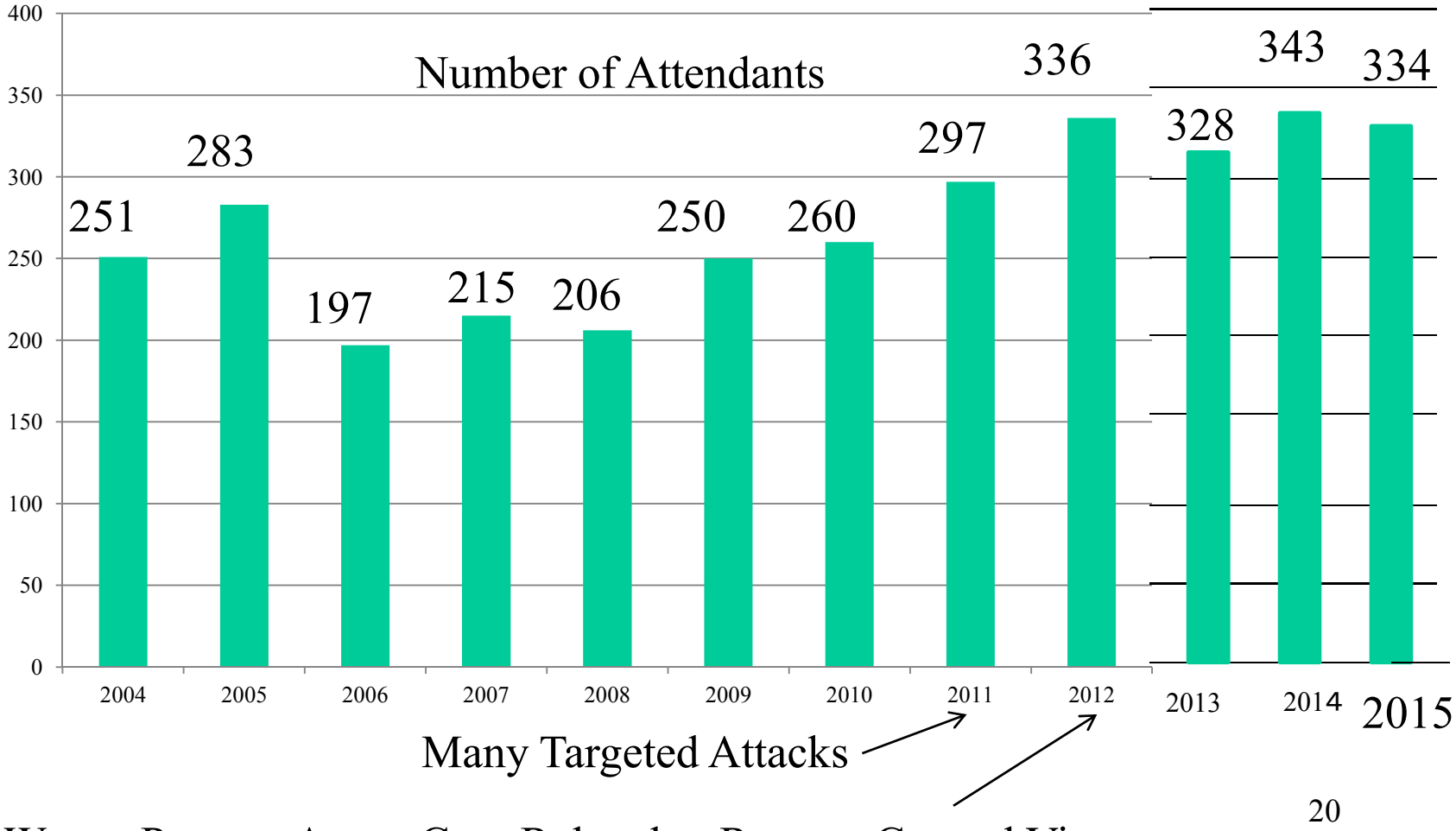
In 2006: The Encyclopedia of Digital Forensics was published from Nikka Giren publisher with the supervision of IDF.

In 2011: The first Digital Forensic Introductory Training hosted by IDF was held.

In 2012: The Guideline for Maintaining Evidence (Version 2) was released by the IDF.

In 2015: The Revised Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of the IDF.

Number of Attendants to the IDF Sponsored Conference



Main IDF Activities

In 2004: The IDF was established. The first Digital Forensic conference, which is called the Digital Forensic Community was held in December of this year.

In 2006: The Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of IDF.

In 2011: The first Digital Forensic Introductory Training hosted by IDF was held.

In 2012: The Guideline for Maintaining Evidence (Version 2) was released by the IDF.

In 2015: The Revised Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of the IDF.

Encyclopedia of Digital Forensics

Edited by IDF

【Contents】

496pages , 21,000Yen, 2006

Main IDF Activities

In 2004: The IDF was established. The first Digital Forensic conference, which is called the Digital Forensic Community was held in December of this year.

In 2006: The Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of IDF.

In 2011: The first Digital Forensic Introductory Training hosted by IDF was held.

In 2012: The Guideline for Maintaining Evidence (Version 2) was released by the IDF.

In 2015: The Revised Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of the IDF.

Digital Forensic Introductory Training

	Year	No. of Attendees*	No. that attended Special Courses **
First	2011	215	—
Second	2012	370	—
Third	2013	436	—
Fourth	2014	250	20
Fifth	2015	252	42
Sixth	2016	326	56

* Two-hour courses

** One-day courses

Main IDF Activities

In 2004: The IDF was established. The first Digital Forensic conference, which is called the Digital Forensic Community was held in December of this year.

In 2006: The Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of IDF.

In 2011: The first Digital Forensic Introductory Training hosted by IDF was held.

In 2012: The Guideline for Maintaining Evidence (Version 2) was released by the IDF.

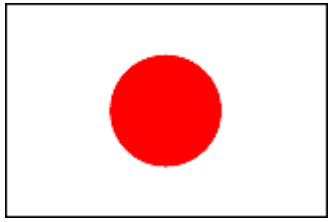
In 2015: The Revised Encyclopedia of Digital Forensics was published by Nikka Giren under the supervision of the IDF.

Digital forensics related events in Japan

Beginning in 2004, Japan-U.S. collaborative investigations on Digital forensic matters started between Tokyo Denki University etc. and Mississippi State University.

In 2005: Digital Forensics was selected as one of the most important 11 security technologies in a report published by the Secretary of Cabinet in Japan.

In 2008: The Fourth Digital Forensic International Conference, which is hosted by the International Federation for Information Processing, Technical Committee 11 (IFIP TC11), was held in Japan.



Digital forensics related events in Japan

Beginning in 2004, Japan-U.S. collaborative investigations on Digital forensic matters started between Tokyo Denki University etc. and Mississippi State University.

In 2005: Digital Forensics was selected as one of the most important 11 security technologies in a report published by the Secretary of Cabinet in Japan.

In 2008: The Fourth Digital Forensic International Conference, which is hosted by the International Federation for Information Processing, Technical Committee 11 (IFIP TC11), was held in Japan.

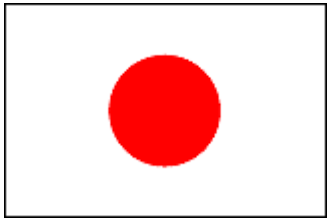
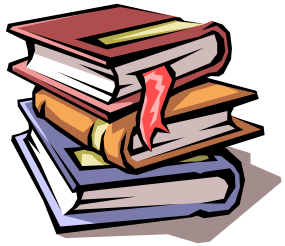


Table of contents

Articles Related to DF in Japan

- We searched CiNii to find the articles in Japan related to “Digital Forensics”.

CiNii is a searchable database service containing academic information on articles, books, etc in Japan.



Number of Articles According to Year

Year	Number of Articles
2006	4
2007	6
2008	11
2009	13
2010	2
2011	7
2012	4
2013	11
2014	7
2015	12
Total	78

Total Number of Articles: 78

Average Number of Articles: ~8

Japanese papers presented in other countries are not included in these figures.

Map of Our Main Studies

Managemental

Technical

④ Guide System for DF using Android Terminal

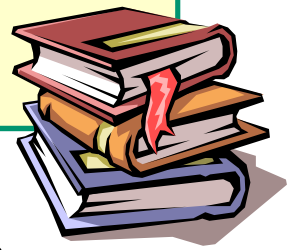
⑥ DF in Japan

⑤ Fog Forensic

③ LIFT System

② Onmitsu

① Signature scheme for Maintaining Evidence



Element  System

LIFT: Live and Intelligent Network Forensic Technologies

Map of Our Main Studies

Managemental

Technical

Guide System for DF
using Android Terminal

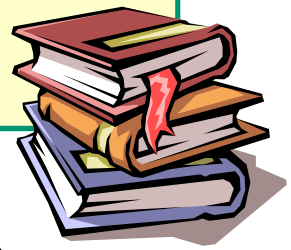
⑥ DF in Japan

⑤ Fog Forensic

③ LIFT System

② Onmitsu

① Signature scheme for Maintaining Evidence



Element  System

LIFT: Live and Intelligent Network Forensic Technologies

Proposal and evaluation of safe and efficient log signature scheme for the preservation of evidence

Naoki Kobayashi
Dep. of Information Systems and Multimedia Design
Tokyo Denki University, 5 Senju-Asahi-cho,
Adachi-Ku, Tokyo 120-8551, Japan

Ryoichi Sasaki
Dep. of Information Systems and Multimedia Design
Tokyo Denki University, 5 Senju-Asahi-cho,
Adachi-Ku, Tokyo 120-8551, Japan

Abstract— **In recent years, the requirements for the preservation of evidence have increased for important log data, such as the data in the planned common number identification system in Japan. One of the proposed evidence preservation methods, the hysteresis signature scheme, reflects previously summarized data with a new digital signature of the log data. However, it takes a long time for this scheme to verify signatures. Therefore, we propose a new hybrid signature scheme that is based on the existing united signature scheme and the hysteresis signature scheme. In evaluations under various conditions, we** ineffective when the numbers of generations and verifications of signatures are the same.

We propose the hybrid signature scheme and compare it with conventional schemes, including the hysteresis signature scheme.

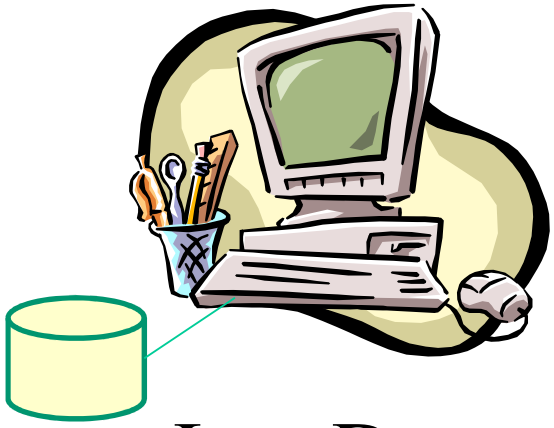
As a result, we show that our proposed scheme is the most effective among them. In a survey of related papers, such as [7][8][9][10][11], a method having the same function as our hybrid signature scheme has not yet been proposed.

CFSE2014 held in Conjunction with COMPSAC 2014

CFSE: Computer Forensics in Software Engineering
COMPSAC 2014: The 38th IEEE Computer Society International Conference on Computers, Software & Applications

Background

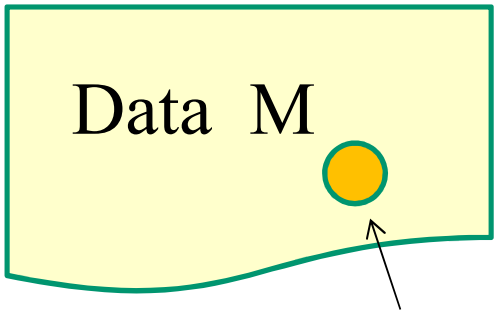
- In recent years, the requirements for preserving important log data as evidence have increased.



Log Data

Basic Scheme and Its Issue

- As a scheme to detect the tampering of digital data, a digital signature scheme is generally used.
- This mechanism is a combination of the public key cipher and the hash function.

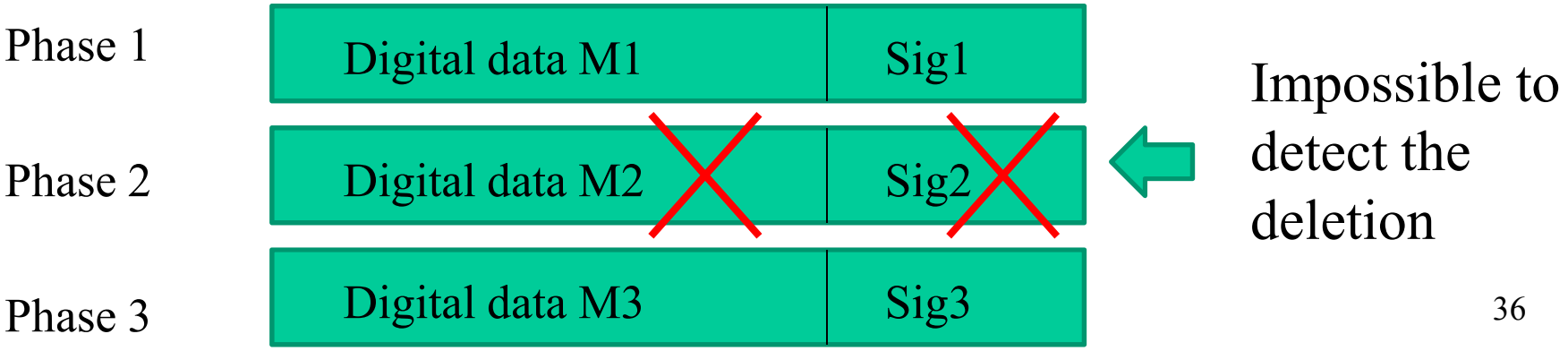


Digital Signature

Sig = S(h(M))
where
Sig: Digital Signature
h:Hash function
S: Public key encryption using a secret key

Basic Scheme and Its Issue

- However, it is impossible to detect log data tampering using a normal digital signature scheme because log data appears intermittently.
- If both the digital data and its related digital signature are deleted together, the deletion cannot be detected in the digital forensics verification phase.



Proposed Scheme

We will now propose a hybrid signature scheme and compare it with two conventional methods.

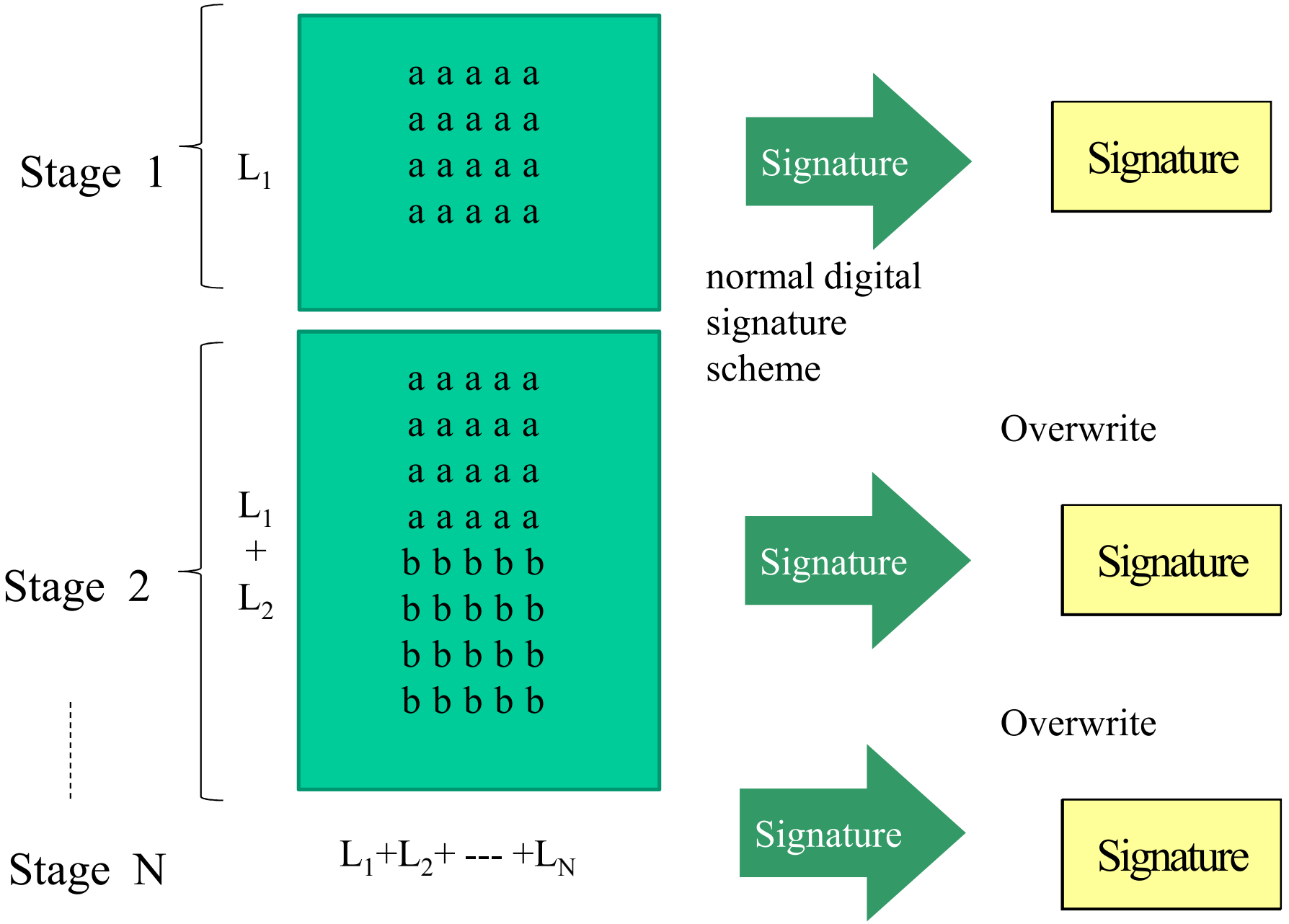
(1) United Signature Scheme

(Conventional Method)

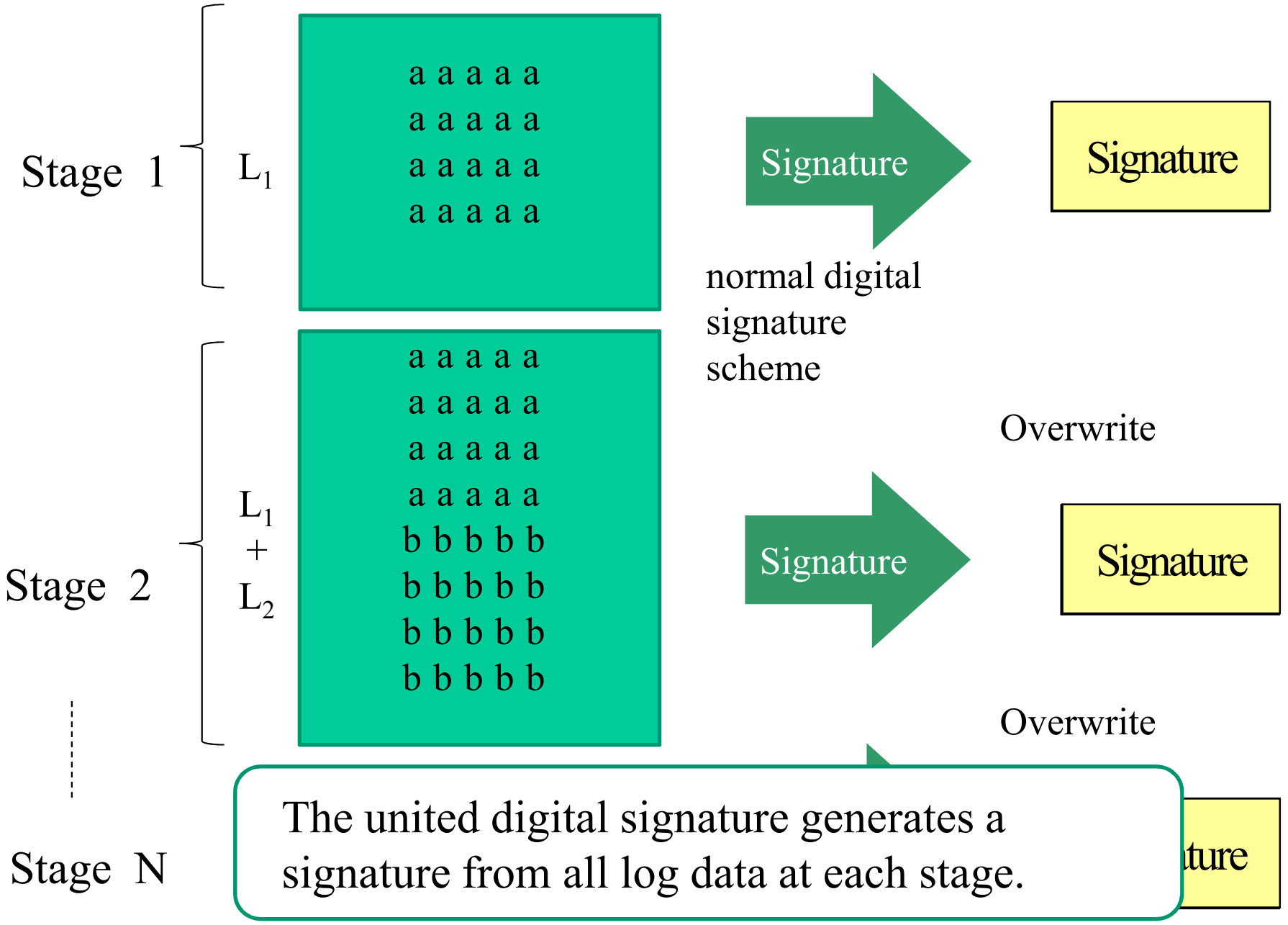
(2) Hysteresis Signature Scheme

(Conventional Method)

United Signature Scheme Generation Phase

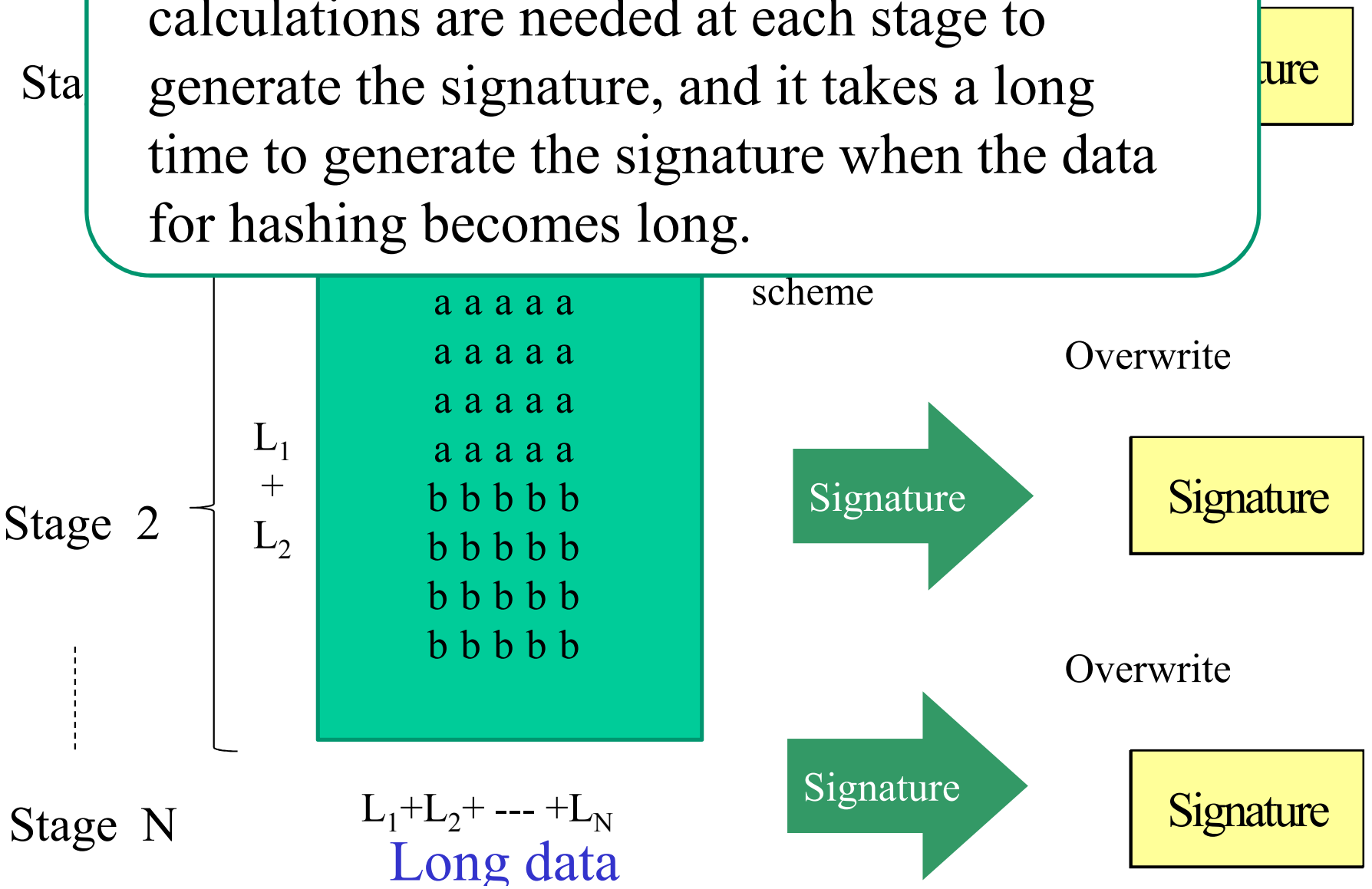


United Signature Scheme Generation Phase

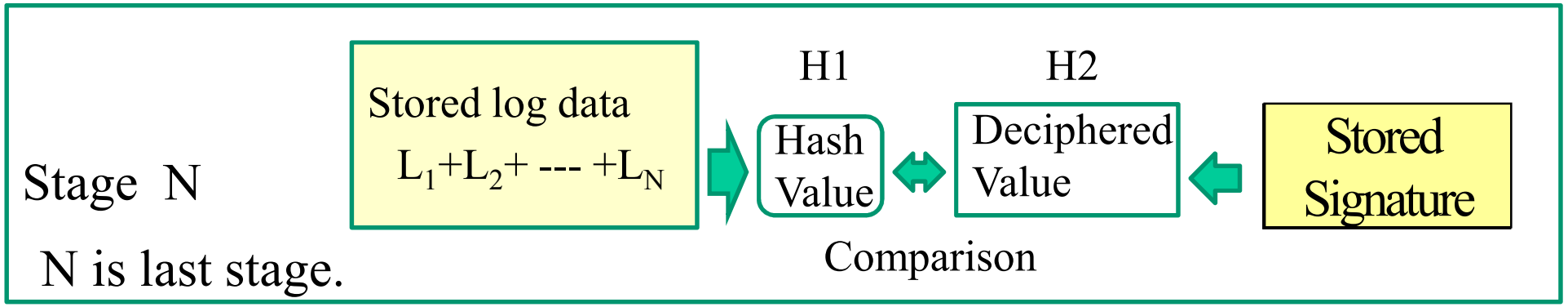


Generation Phase of United Signature Scheme

The disadvantages of this scheme are that calculations are needed at each stage to generate the signature, and it takes a long time to generate the signature when the data for hashing becomes long.



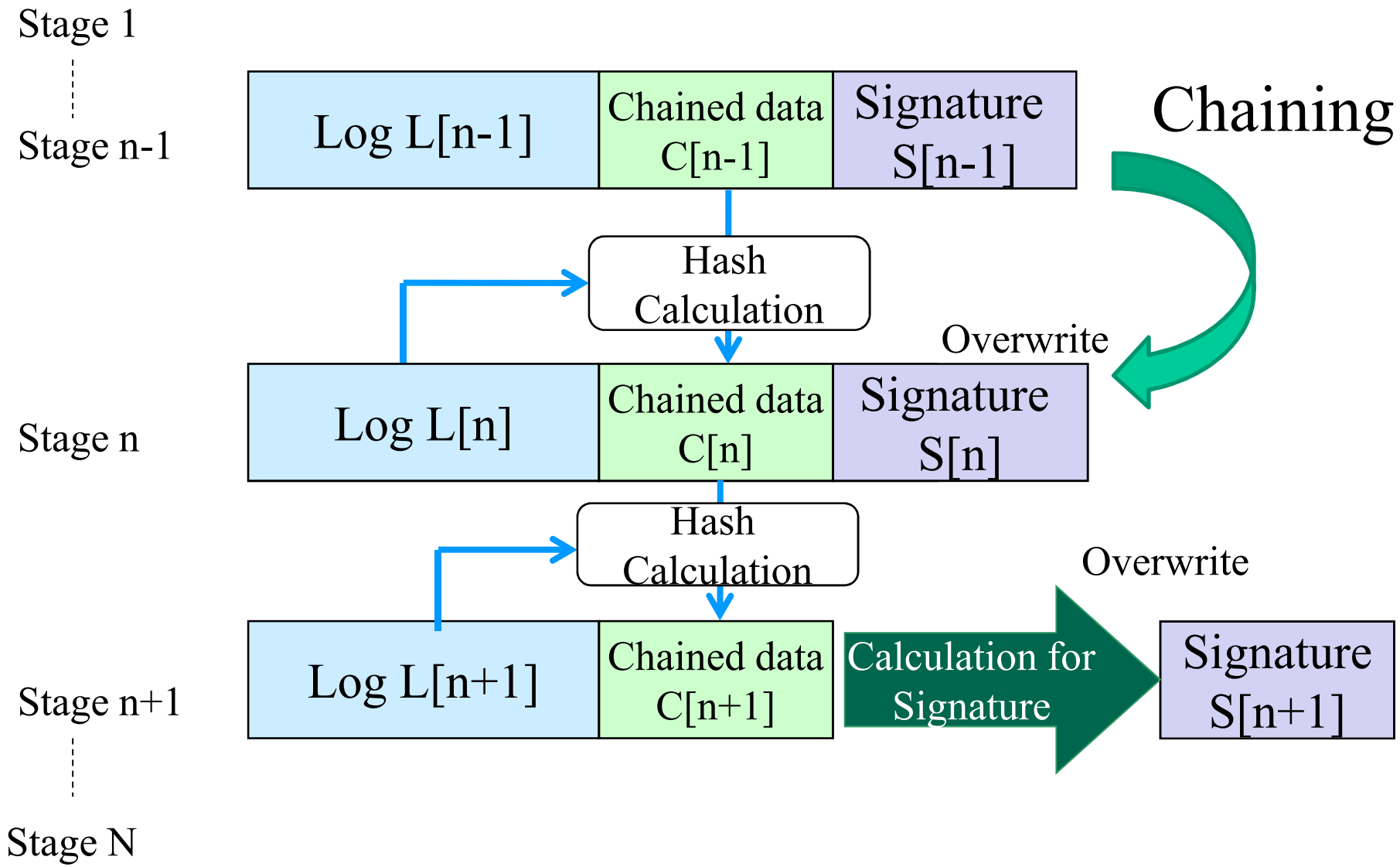
United Signature Scheme Verification Phase



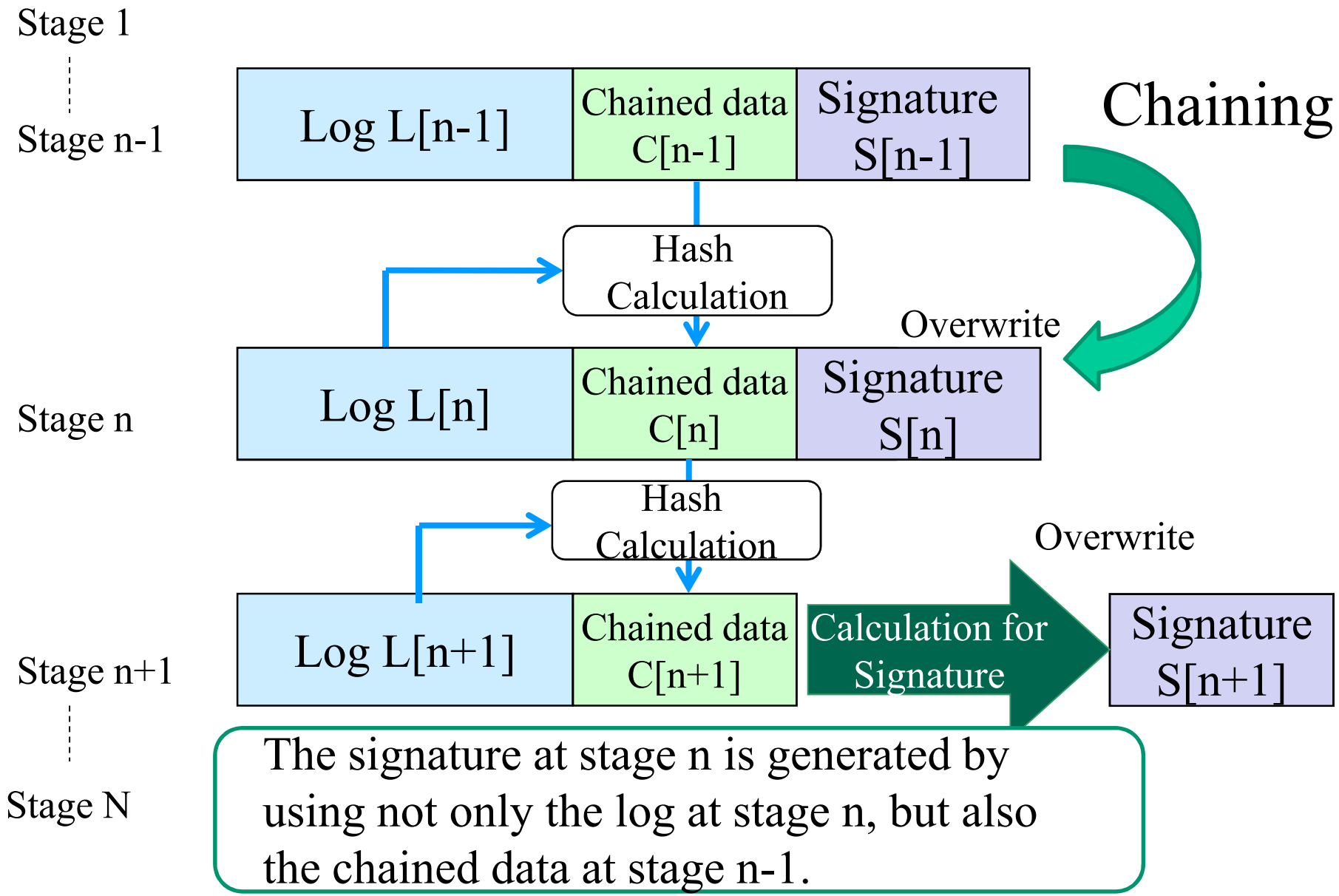
For united signature scheme verification, it is only necessary to check the last stage.

Therefore, reductions in the computation time required for verification can be expected.

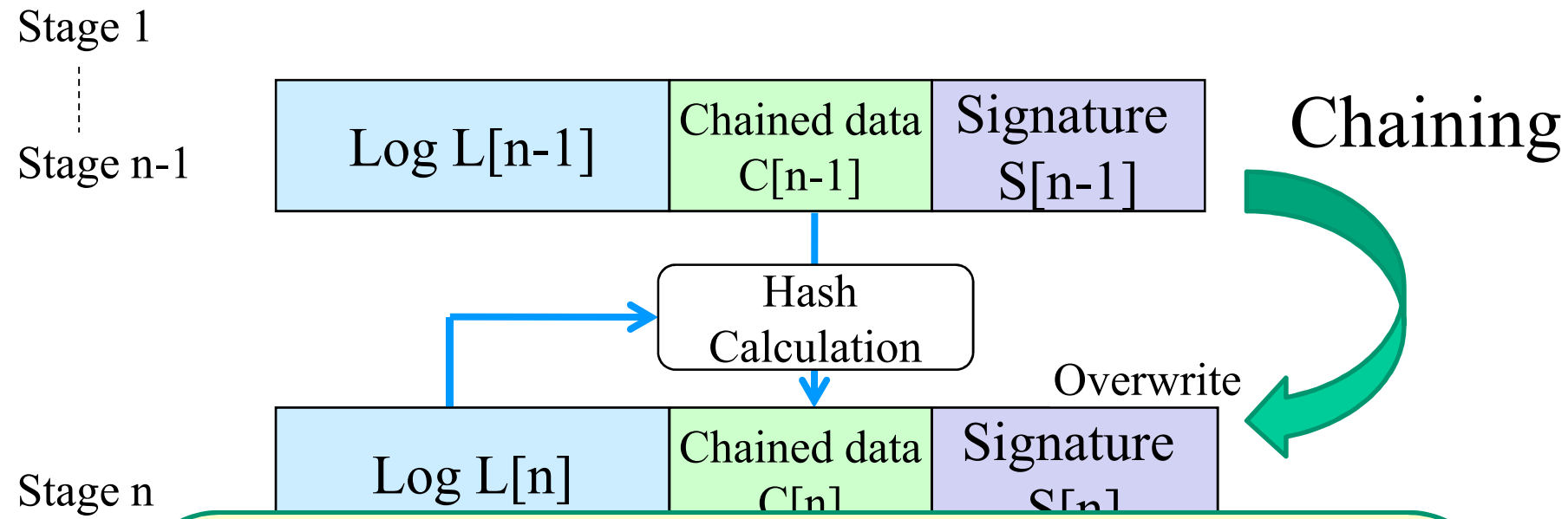
Hysteresis Signature Scheme Generation Phase



Hysteresis Signature Scheme Generation Phase



Hysteresis Signature Scheme Generation Phase

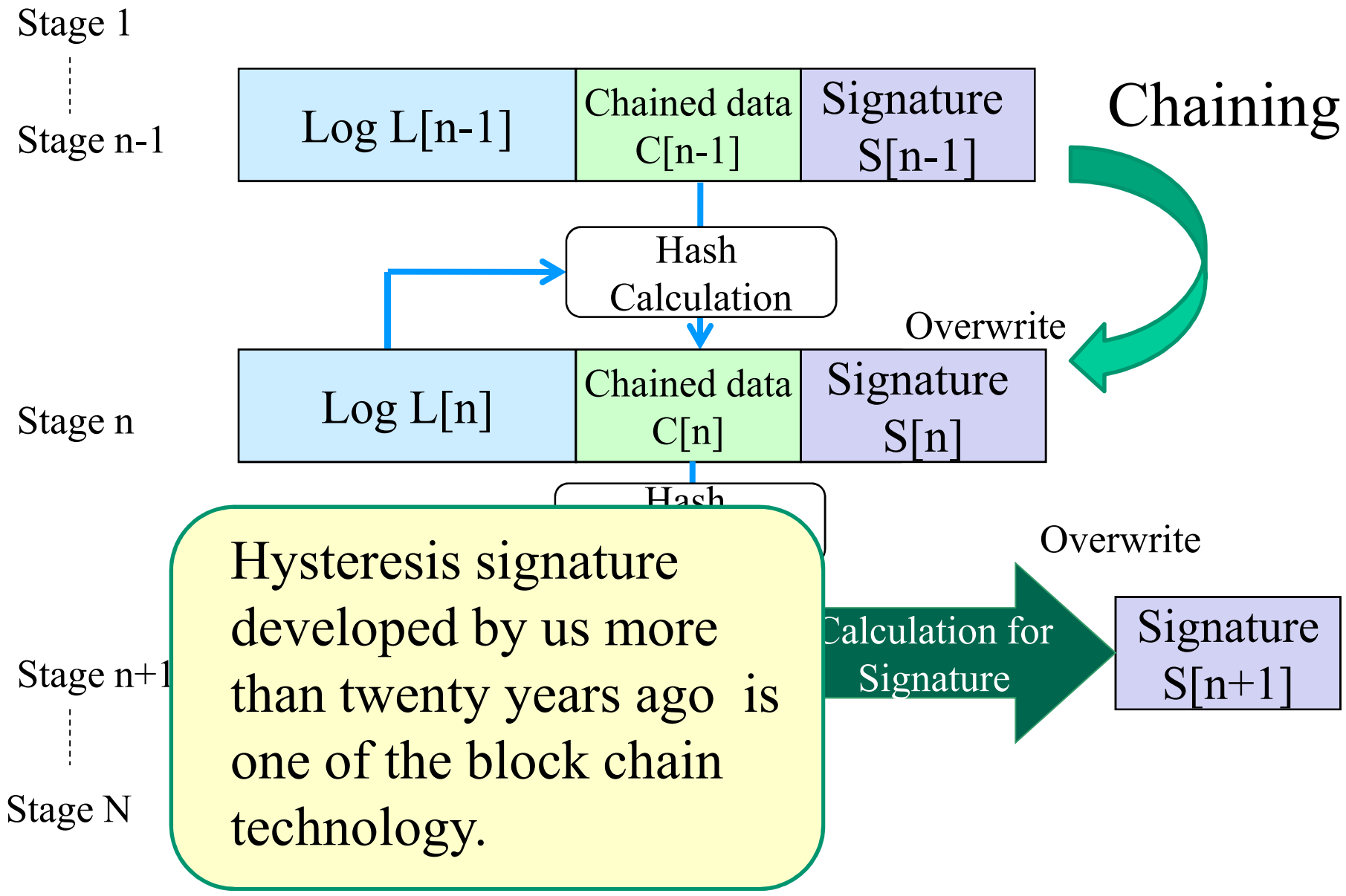


The hysteresis signature advantages are as follows:

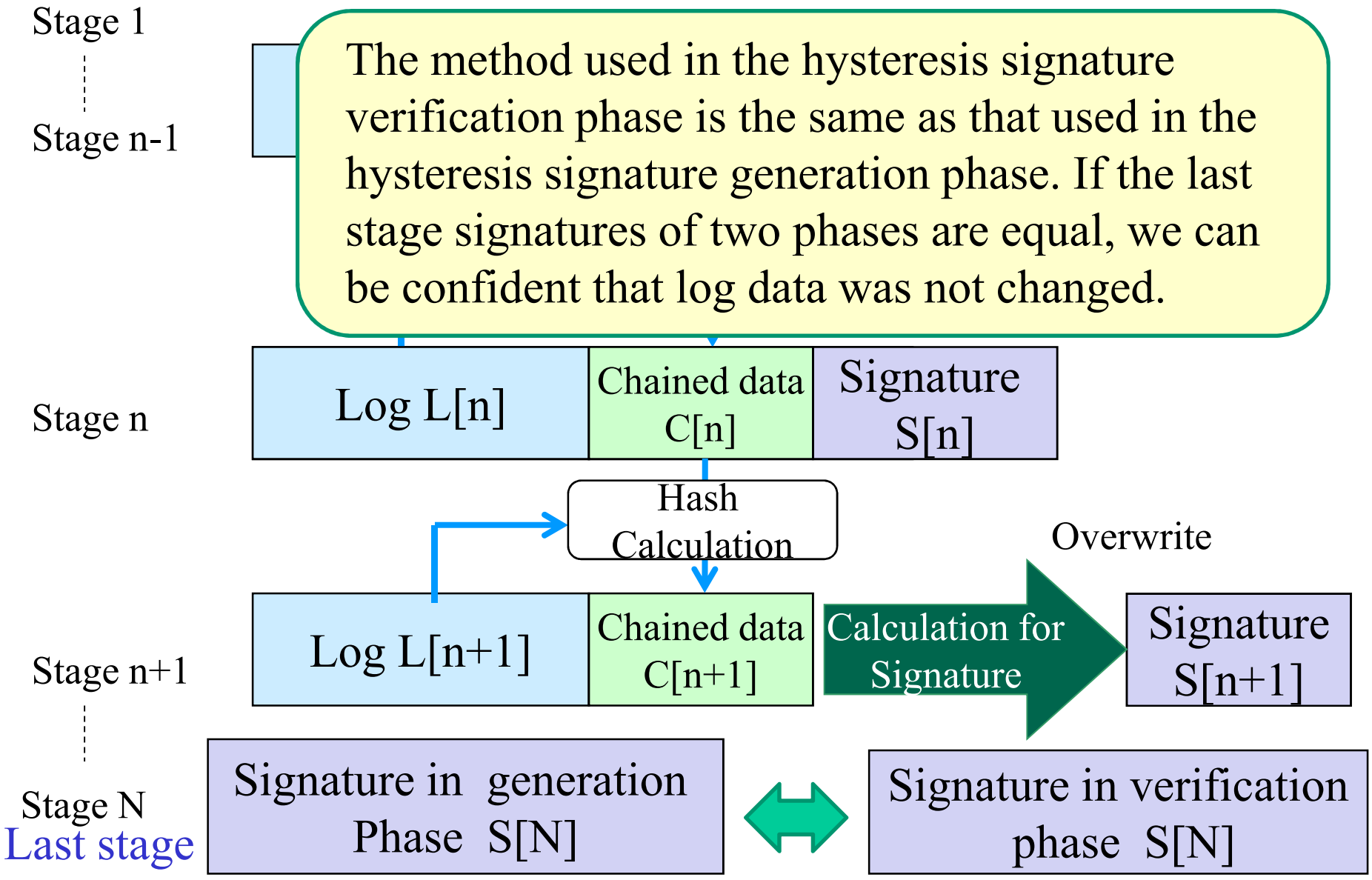
(1) Log data deletion can be detected because the hysteresis signature constructs a chain structure between signatures.

(2) The time required for signature generation is short, because the hashing data is short.

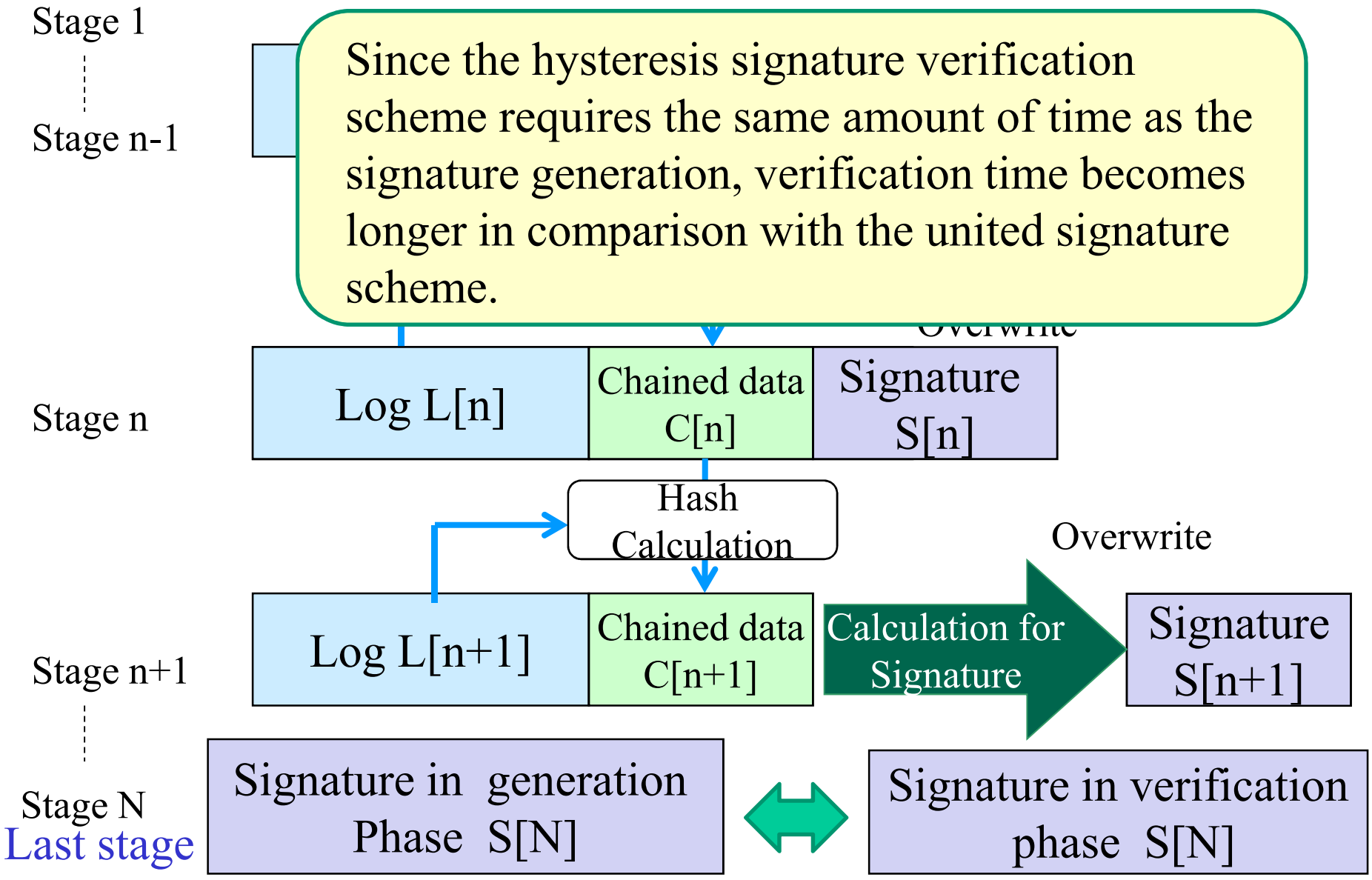
Hysteresis Signature Scheme Generation Phase



Hysteresis Signature Scheme Verification Phase



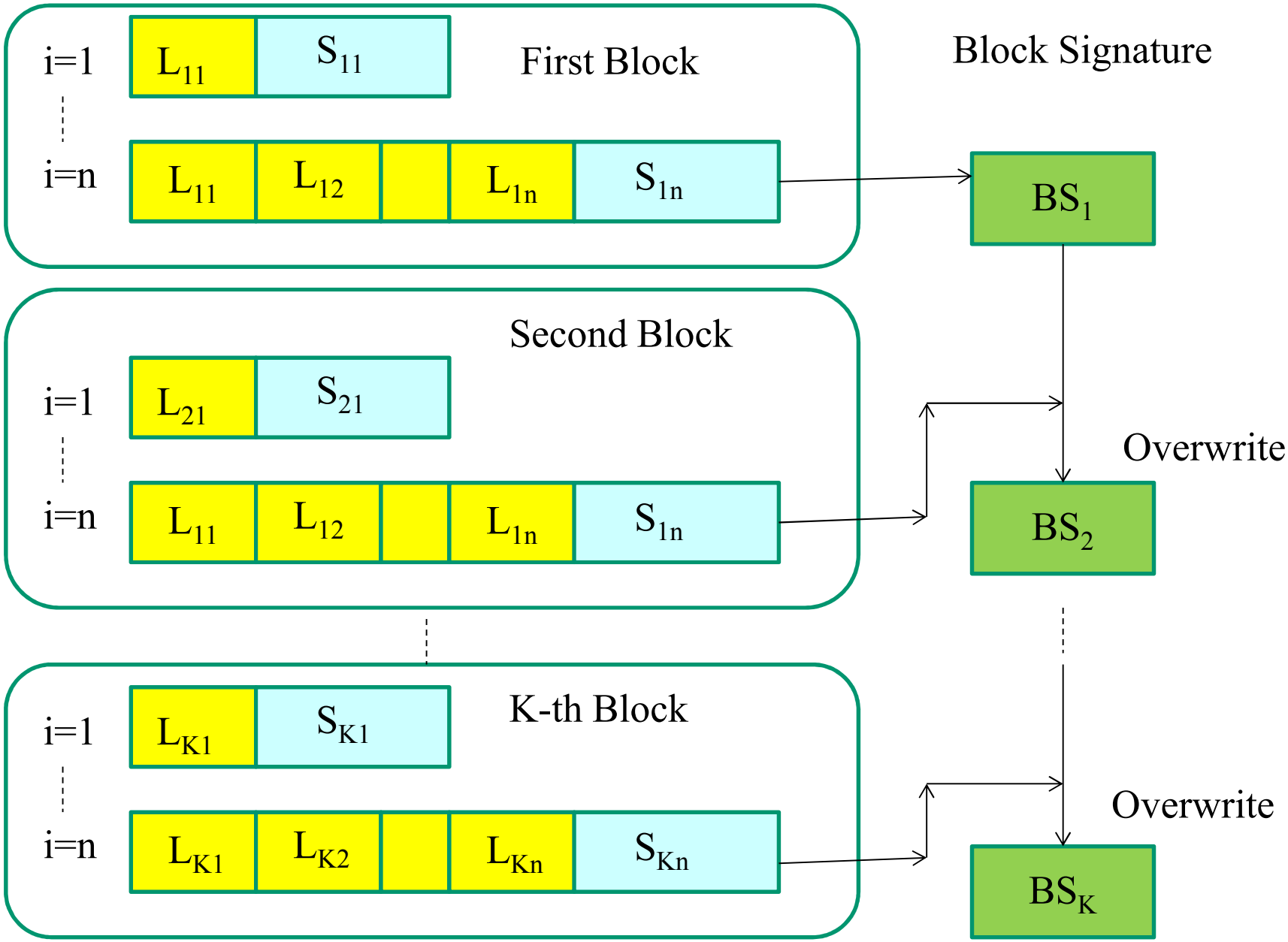
Hysteresis Signature Scheme Verification Phase



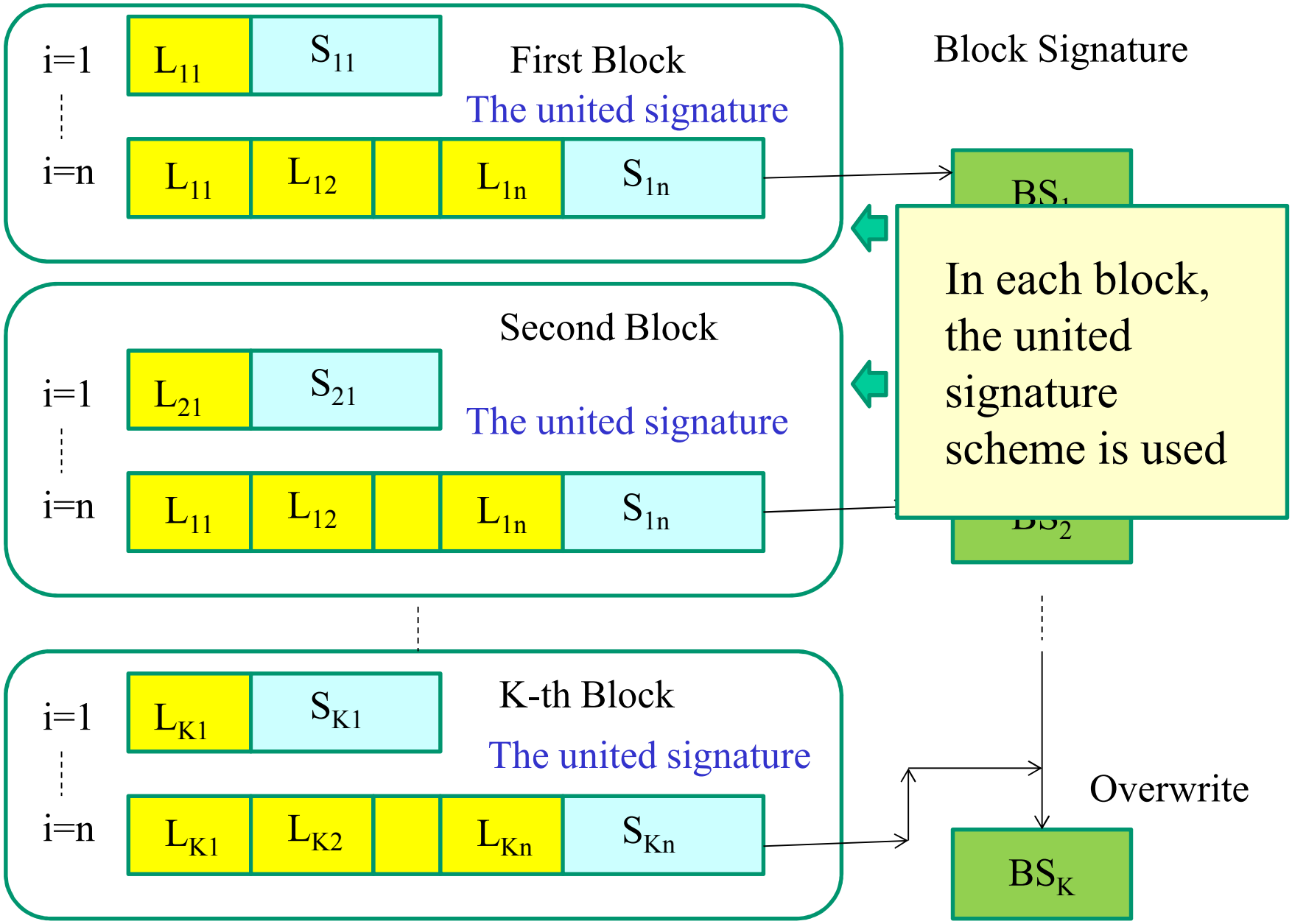
Requirements for the proposed scheme

- **Requirement 1**: The verifier can detect tampering to any part of the log data.
- **Requirement 2**: The verifier can detect log data deletions even if part of the log data and the related digital signature are deleted together.
- **Requirement 3**: The total calculation time for signature generation and log data verification is the shortest among all schemes.

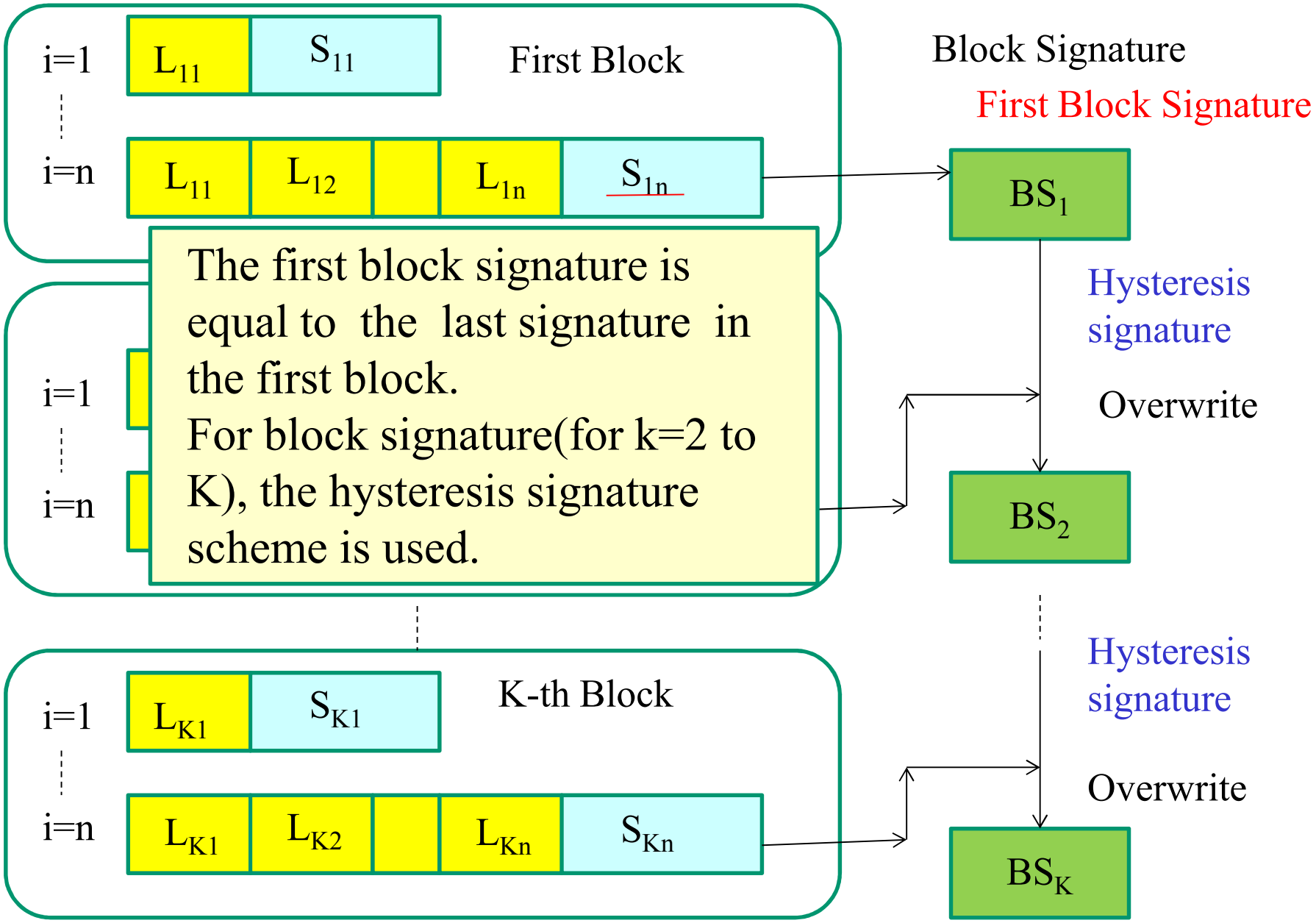
Hybrid Signature Scheme Generation Phase



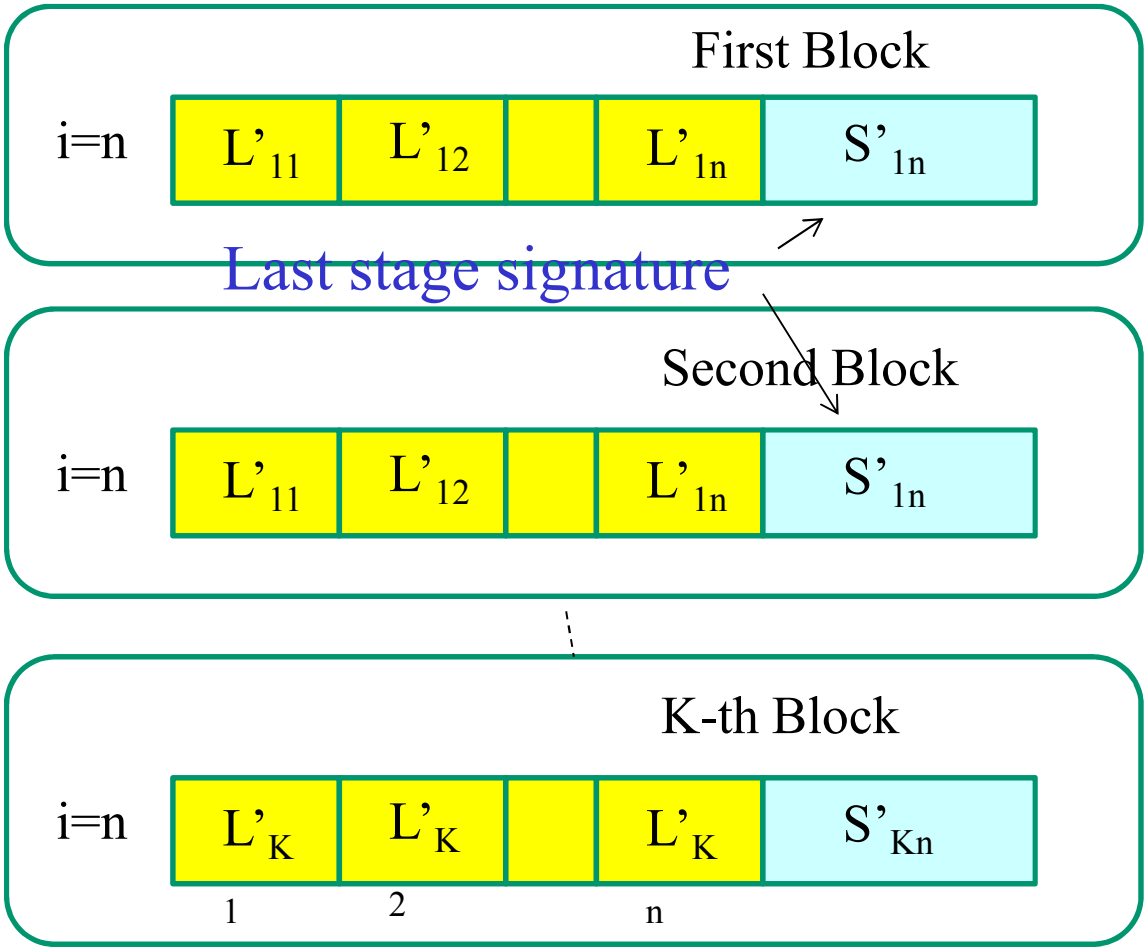
Hybrid Signature Scheme Generation Phase



Hybrid Signature Scheme Generation Phase



Hybrid Signature Scheme Verification Phase

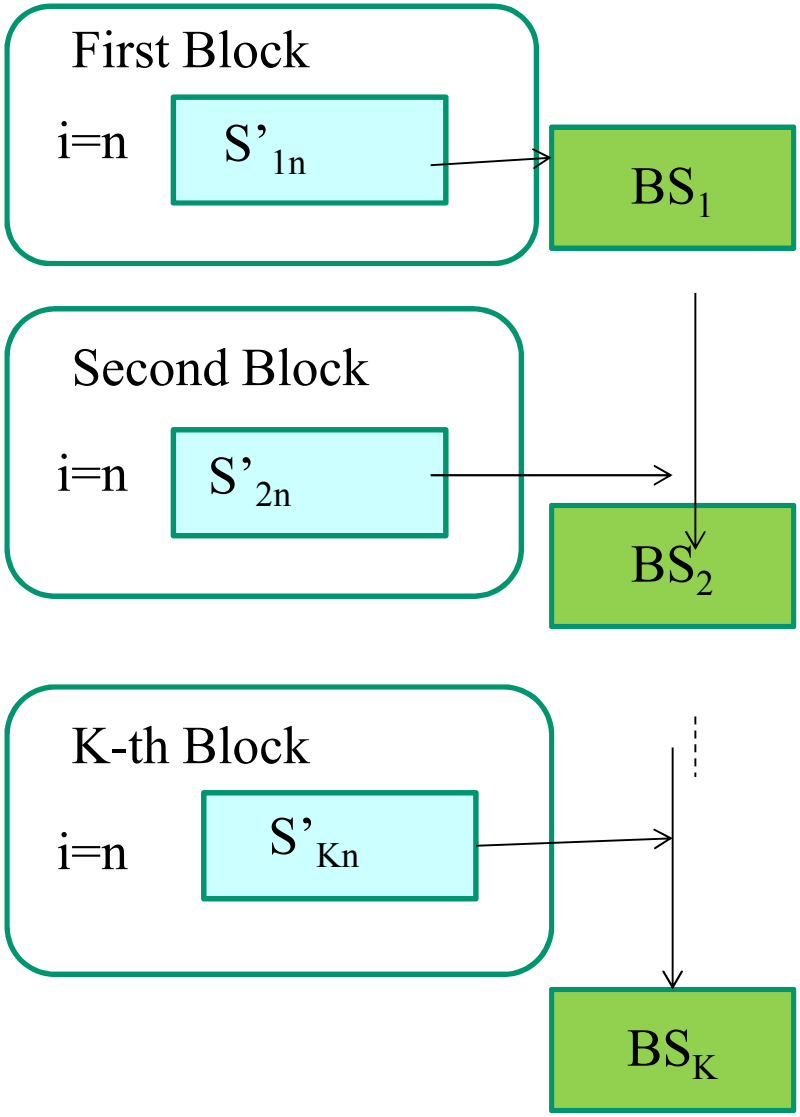


STEP 1:
In each block, the last stage signature is verified in the same manner as a normal digital signature.

$H1=Kp(S'_{kn})$, where Kp( ) represents the decryption function using the public key cipher and the public key Kp.

$H2=h(L'_{k1}, L'_{k2}, ..., L'_{kn})$

Hybrid Signature Scheme Verification Phase



STEP 2:

Step 2-1: For first block,

The value of S'_{1n} is given to BS_1

Step 2-2: For k=2, ..., K

Calculate BS_k using hysteresis scheme.

STEP3:

If BS_K=BS'_K, it can be confirmed that no data tampering has occurred and no part of the log data or the related signature has been deleted.

Experimental Environment

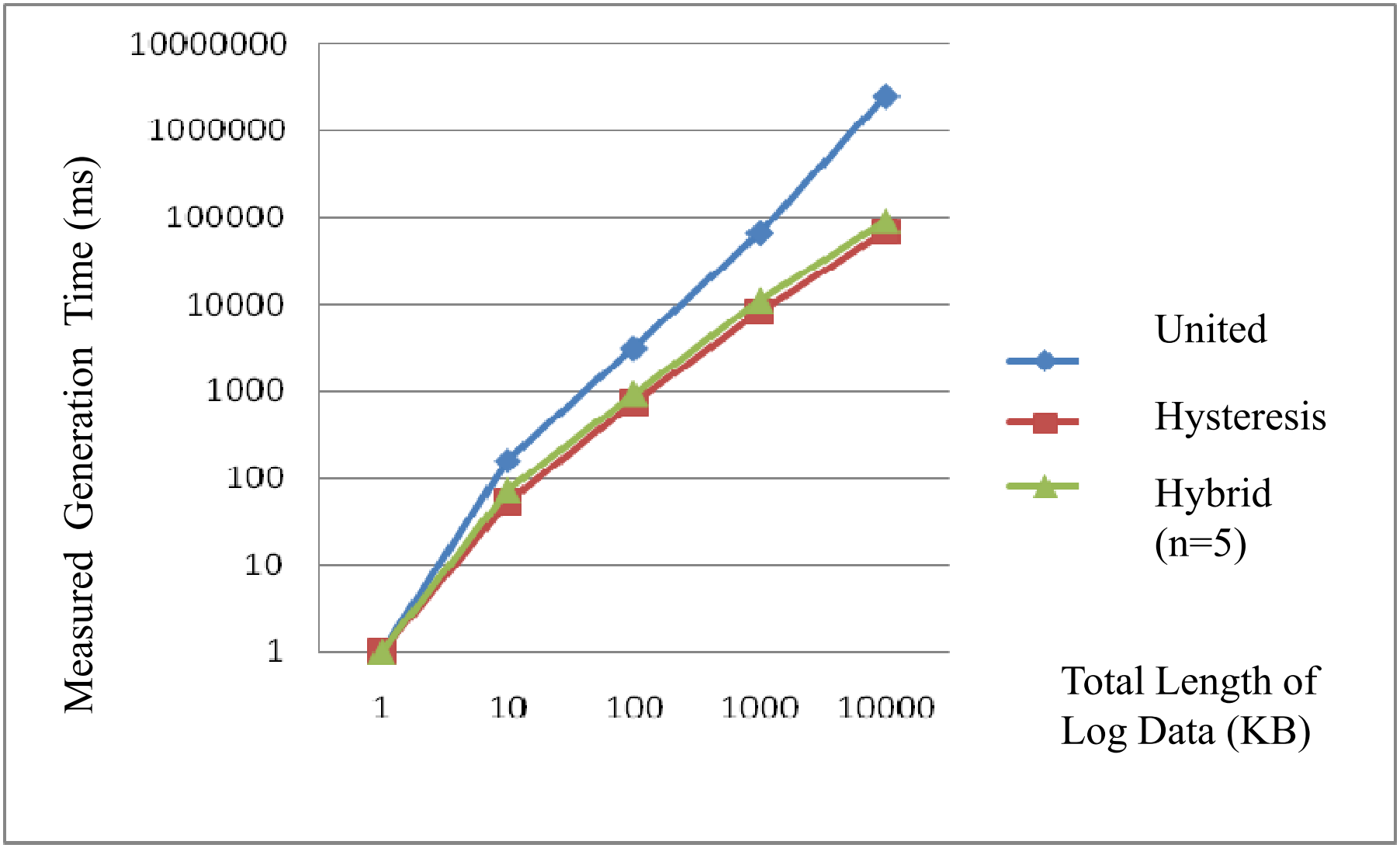
To verify that the proposed scheme is the most effective among the three schemes, we measured the generation times and verification times.

(1) CPU: Intel Core i5
(2) OS: Windows 7 Enterprise 64-bit
(3) RAM: 2 [GB]
(4) SSD: 120 [GB]
(5) Development language of the computer program for the experiment: C#

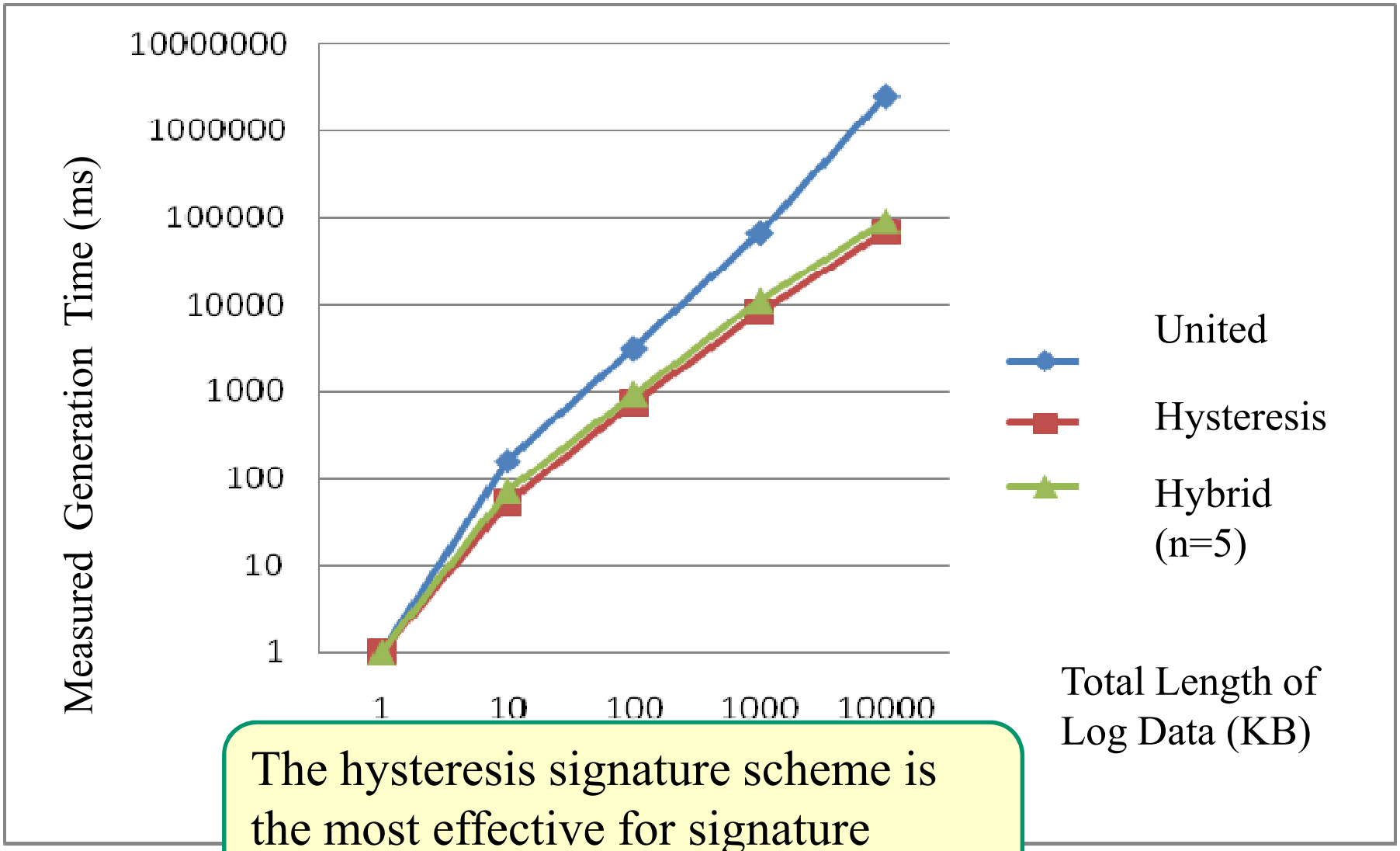
Parameter values

1	K: Number of blocks	200
2	n: Number of log data in each block	5
3	L: Length of each log data	1 KB
4	N: Number of log data	1000
5	L*N	1 MB

Measured times for generating signatures with the three schemes

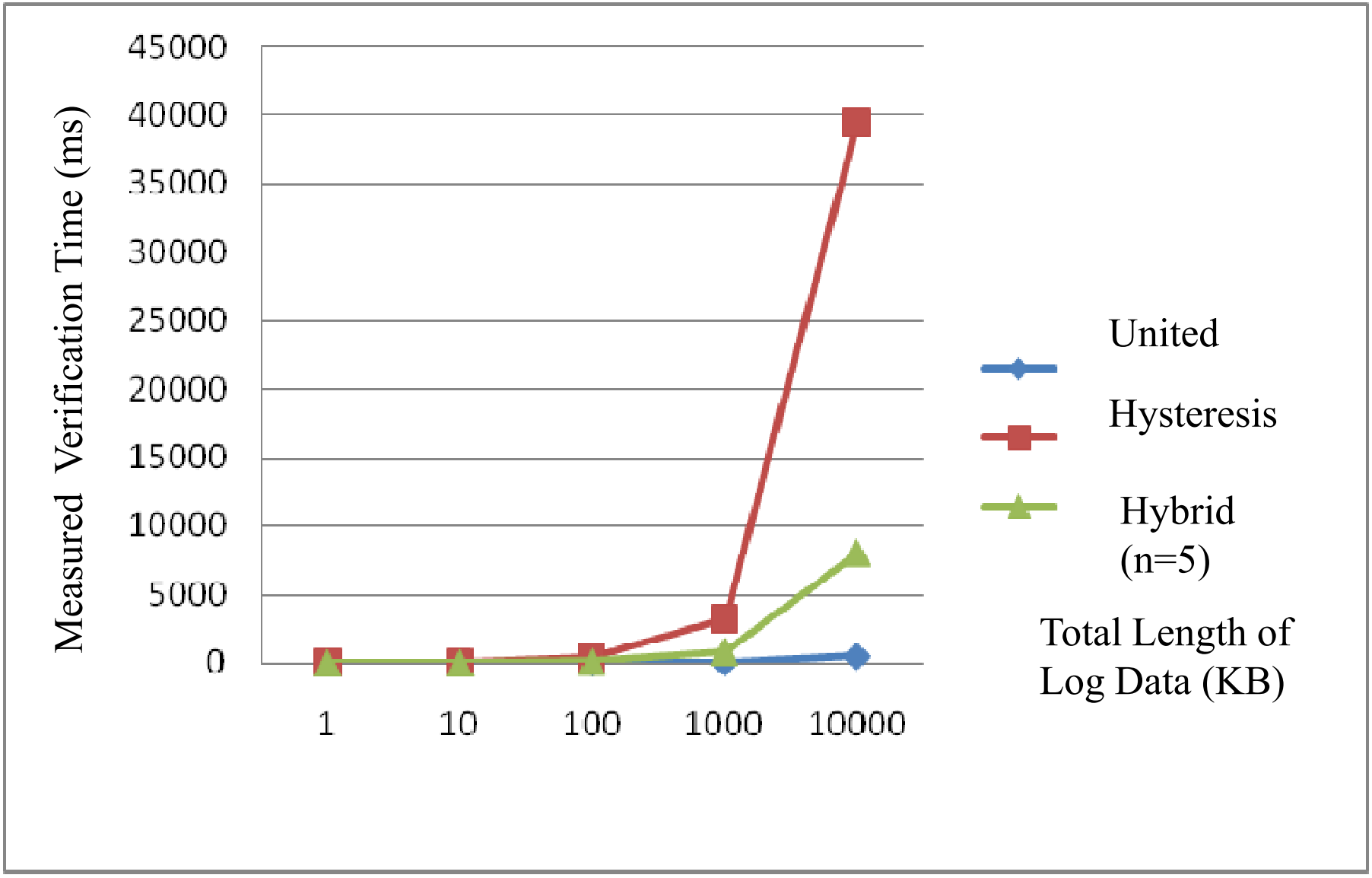


Measured times for generating signatures with the three schemes

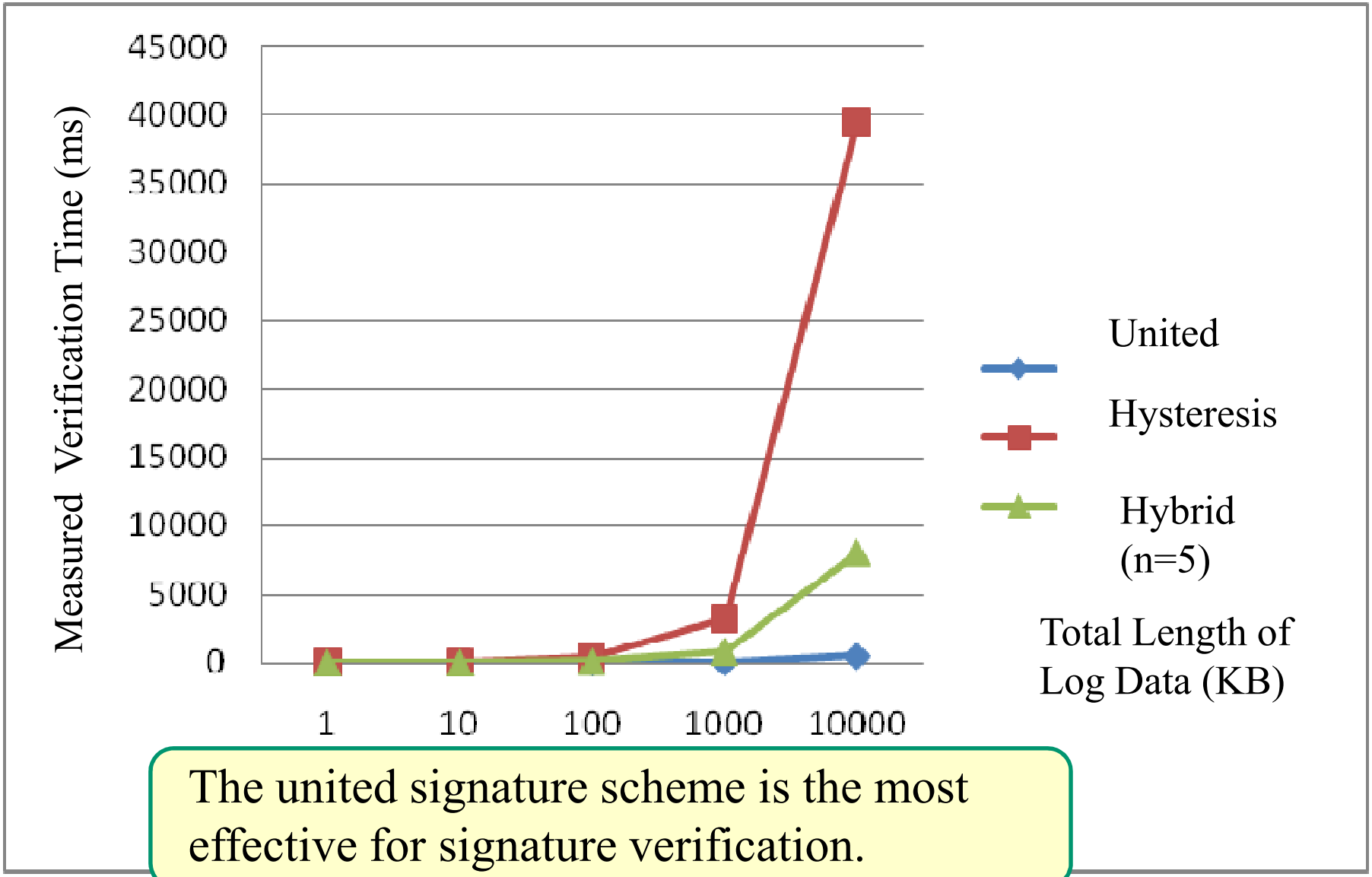


The hysteresis signature scheme is the most effective for signature generation.

Measured times for verifying signatures with the three schemes

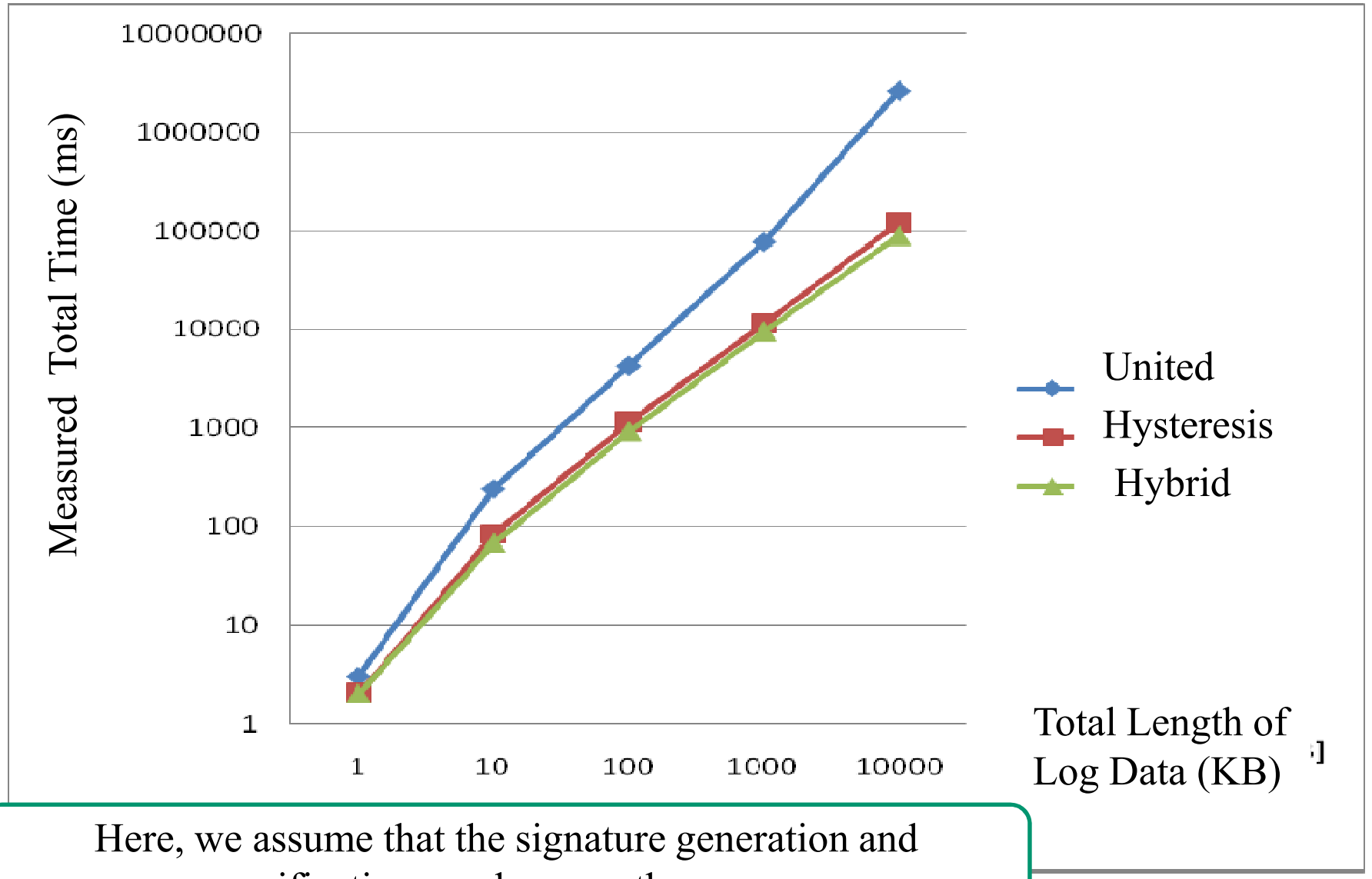


Measured times for verifying signatures with the three schemes



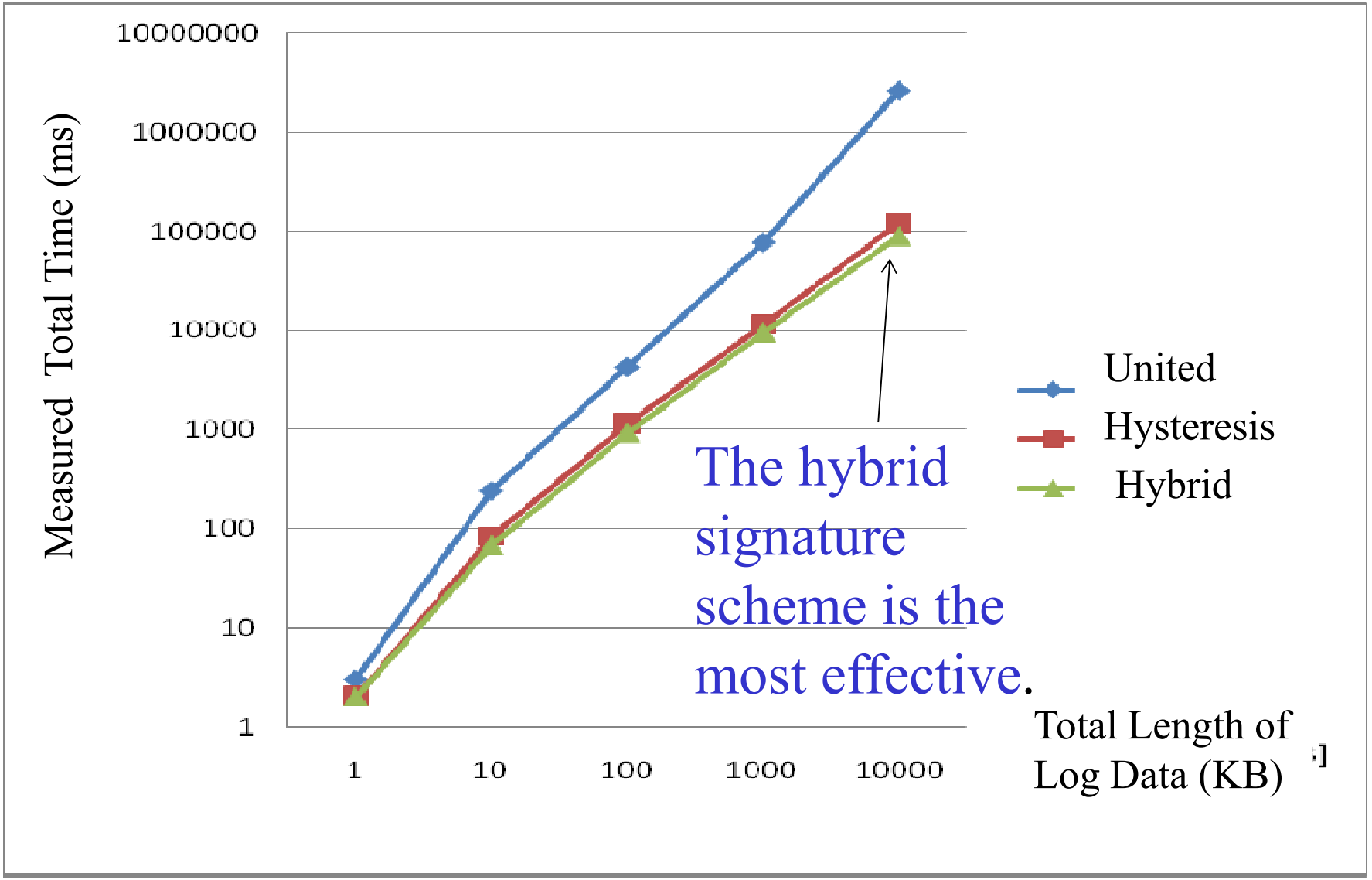
The united signature scheme is the most effective for signature verification.

Measured total computation times with the three schemes



Here, we assume that the signature generation and verification numbers are the same.

Measured total computation times



Evaluation Results

The proposed scheme satisfies the three requirements shown below:

Requirement 1: As described in the hybrid signature scheme verification phase, the verifier is able to detect any log data tampering.

Requirement 2: As described in the hybrid signature scheme verification phase, the verifier can also detect any log data deletions, even if a part of the log data and its related digital signature are deleted together.

Requirement 3: As described in the evaluation results, the total calculation time of the hybrid scheme for log data signature generation and verification is generally the shortest among all three schemes.

Map of Our Main Studies

Managemental

Technical

④ Guide System for DF using Android Terminal

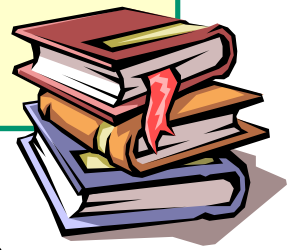
⑥ DF in Japan

⑤ Fog Forensic

③ LIFT System

② Onmitsu

①Signature scheme for keeping Evidence



Element  System

LIFT: Live and Intelligent Network Forensic Technologies

TITLE: METHOD FOR ESTIMATING UNJUST COMMUNICATION CAUSES USING NETWORK PACKETS ASSOCIATED WITH PROCESS INFORMATION

Download Here

Year of Publication: 2014

Page Numbers: 44-49

Authors: Satoshi Mimura, Ryoichi Sasaki

Conference Name: The International Conference on Information Security and Cyber Forensics (InfoSec2014) - Malaysia

Abstract:

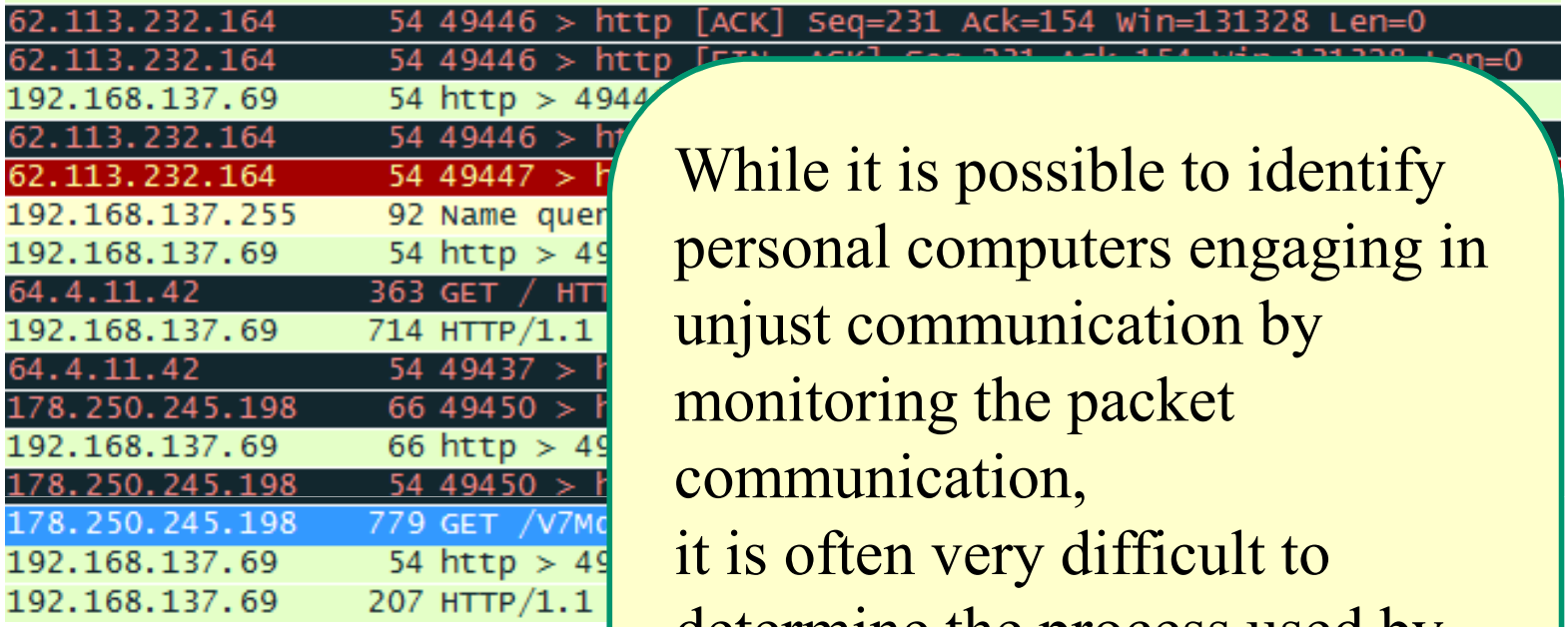
The number of attacks based on advanced persistent threat (APT), which is a set of stealthy and continuous computer hacking processes, has been increasing around the world. To cope with such attacks, a management system that stores and analyses log information in order to identify unjust packet network communications has come to be used for threat detection in equipment equipped with functions such as security information and event management (SIEM). However, while it is possible to identify personal computers (PCs) engaging in unjust communication using this system,

Study Background

- In recent years, attacks have become increasingly advanced.
- It becomes important to identify a cause of unjust communication.

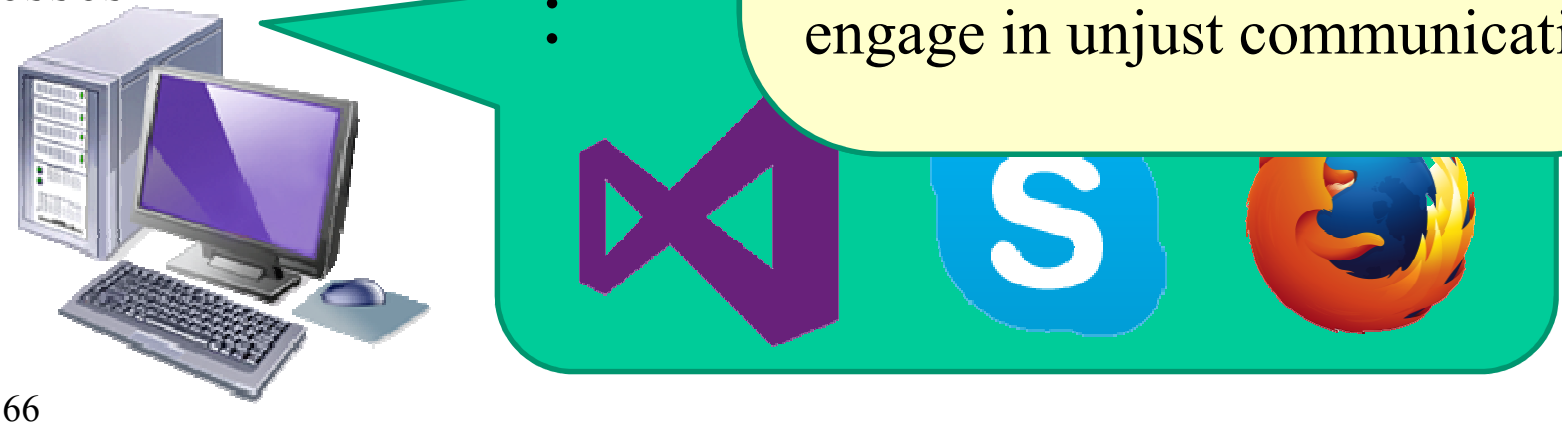
Study Objective

Packet Status



While it is possible to identify personal computers engaging in unjust communication by monitoring the packet communication,
it is often very difficult to determine the process used by the malware to cause the PC to engage in unjust communication.

Running processes



Study Objective

62.113.232.164	54	49446 > http [ACK] Seq=231 Ack=154 Win=131328 Len=0
62.113.232.164	54	49446 > http [FIN, ACK] Seq=231 Ack=154 Win=131328 Len=0
192.168.137.69	54	http > 49446 [FIN, ACK] Seq=154 Ack=231 Win=15680 Len=0
62.113.232.164	54	49446 > http [ACK] Seq=232 Ack=155 Win=131328 Len=0
62.113.232.164	54	49447 > http [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.137.255	92	Name query NB WPAD<00>
192.168.137.69	54	http > 49446 [ACK] Seq=155 Ack=232 Win=15680 Len=0
64.4.11.42	363	GET / HTTP/1.1
192.168.137.69	714	HTTP/1.1 302 Found (text/html)
64.4.11.42	54	49437 > http [ACK] Seq=1255 Ack=41924 Win=65280 Len=0

We would like to identify the running process in the PC connected to packet .

Running processes:

STUDY OBJECTIVE

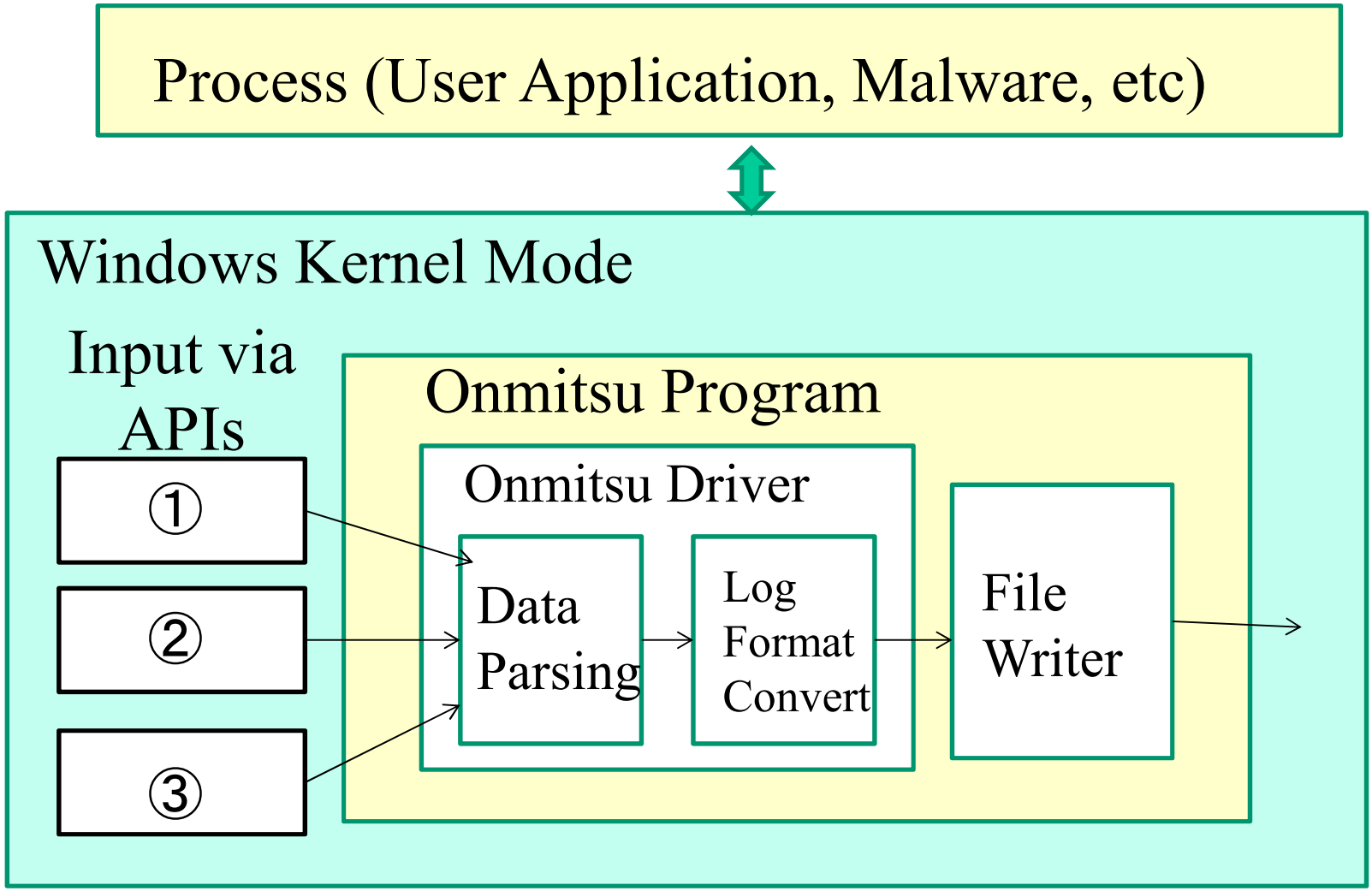
To answer the requirement,

IN 2014, WE DEVELOPED THE LOGGER DRIVER PROGRAM NAMED "ONMITSU" .

Onmitsu?

- Have you heard of “Ninja?”
- Ninja were covert agents in feudal Japan.
- A Ninja who engaged in an intelligence activity was called an **“Onmitsu”**.

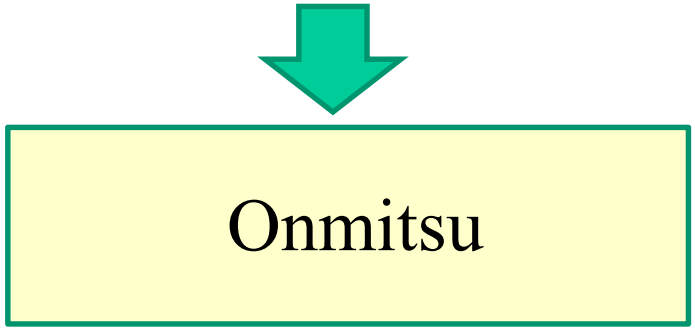
Onmitsu Structure



This program was written by C++, and the total program length is approximately 1K steps.

APIs for Input to Onmitsu

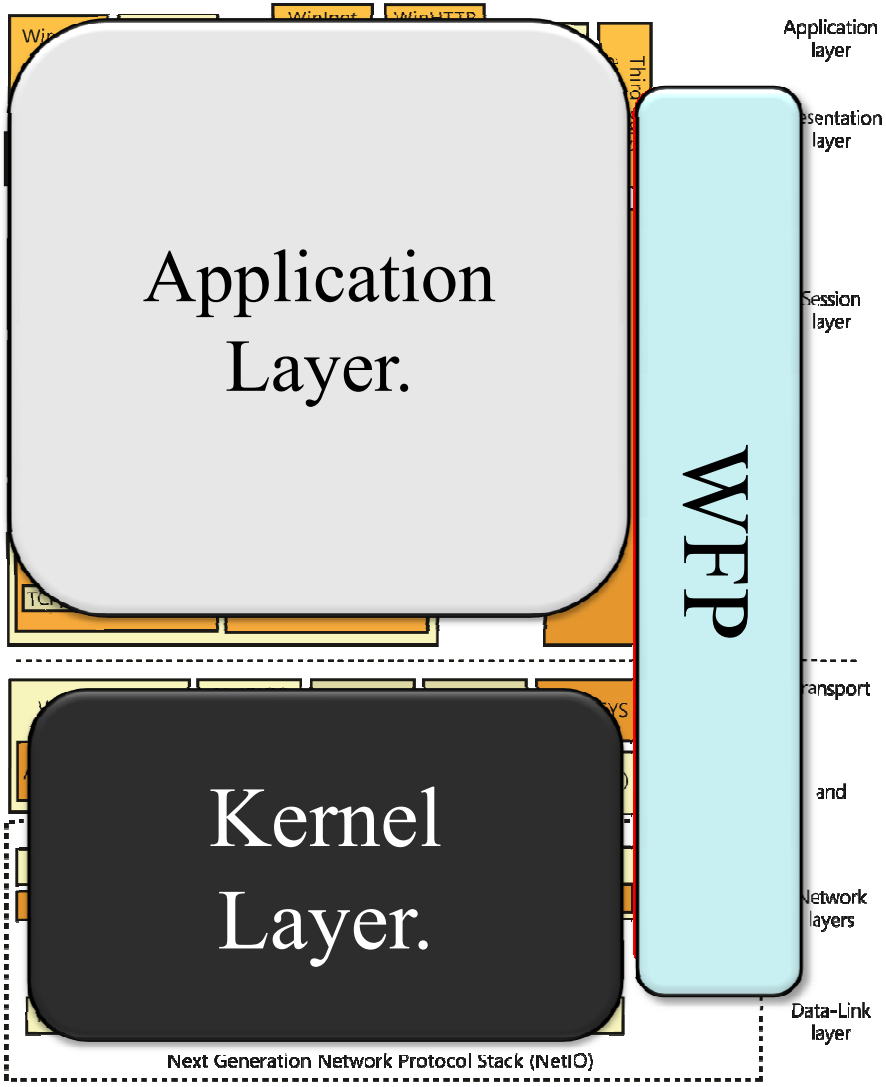
- APIs for Input.
  - Windows Filtering Platform(WFP) - ①
  - PsSetCreateProcessNotifyRoutineEx - ②
  - PsSetLoadImageNotifyRoutine - ③



Onmitsu Logic

To obtain network information

- Windows Filtering Platform (WFP)
  - It is generally used to create a firewall.
  - The Onmitsu driver gets Network Information when the connection status is "ESTABLISHED".



From, Windows Internals 6th P.586

Onmitsu Logic

- Can retrieve these data from WFP.
  - Source IP address and port number.
  - Destination IP address and port number.
  - Communication data.

Onmitsu Logic

To obtain process information

- PsSetCreateProcessNotifyEx
- PsSetLoadImageNotifyRoutine

These APIs, which are Windows kernel mode functions, are used by Onmitsu to register the callback functions that detect process loading, exiting, or module loading.

Onmitsu Recordable Items

Actions	Data
Launch of Process	Time
	Process ID
	Parent Process ID
	Executable Image file path.
	Command Line
End of Process	Time
Load a module.	Time
	Process ID
	Module Image file path.
Established a connection.	Time
	Process ID (Ordered the operation.)
	Source IP Address.
	Source Port Number.
	Destination IP Address.
	Destination Port Number.
	Protocol ID (Transport layer.)

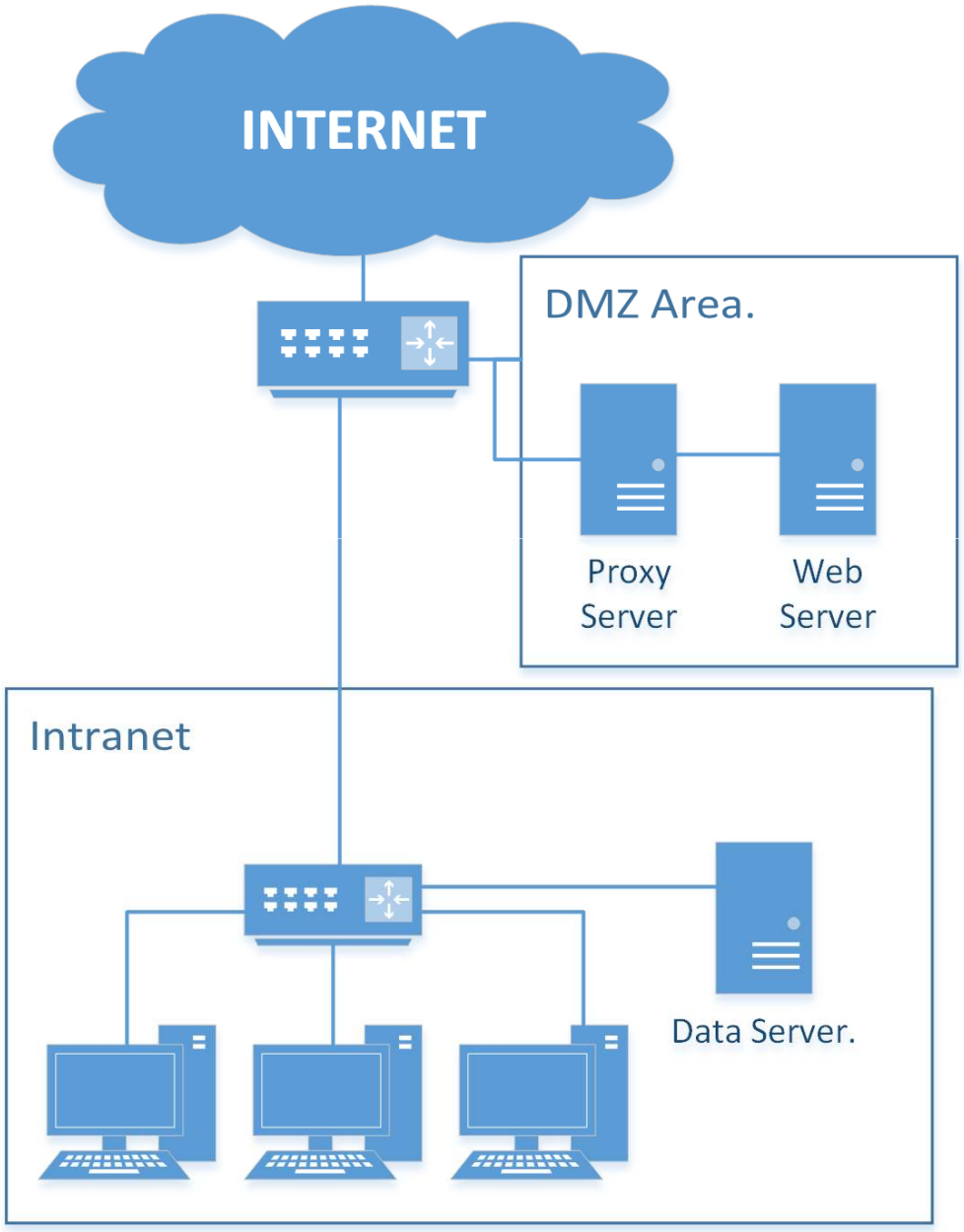
Onmitsu Logic

- Format of log :
  - Process Launch
    PROCESS_LAUNCH,(PID),(P_PID),(PATH),(CMDLINE)
  - Loading a module:
    PROCESS_MODLOAD,(PID),(MODULE_PATH)
  - IPv4 communicate:
    NETWORKV4,(PID),(L_ADR),(L_PORT),(R_ADR),(R_PORT),(PROTO)
  - IPv6 communicate:
    NETWORKV6,(PID),(L_ADR),(L_PORT),(R_ADR),(R_PORT),(PROTO)
  - Process Exit:
    PROCESS_QUIT,(PID)

Evaluation Items

① Log accuracy
② Log usefulness
③ Log volume
④ System load

Network environment



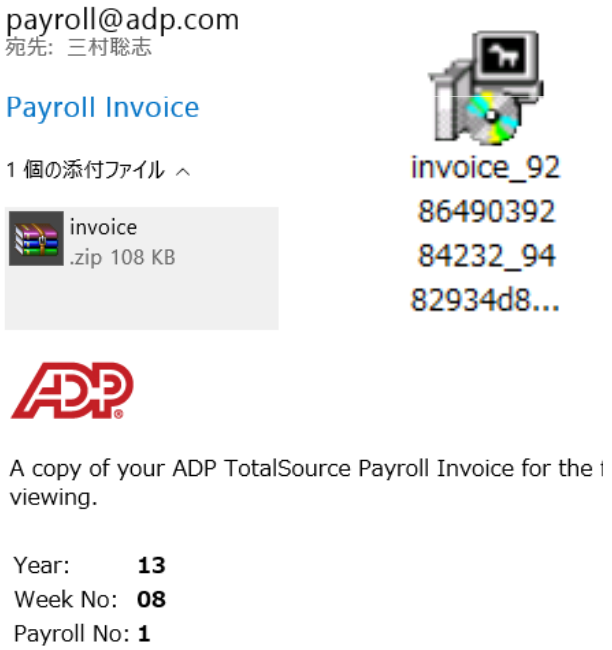
Microsoft Windows Vista or later is required for the client PC as for the OS version.

Evaluation Results ①

- Log accuracy evaluation method.
  - Compare the results of Onmitsu and Dumpcap.

There were no differences between the results obtained from Onmitsu and that obtained from Dumpcap

Log accuracy is enough.



Example of Logs from Onmitsu

TYPE	PID	PARENT	CMDLINE	SRCPORT	DSTIP	DSTPORT
PROCESS_LAUNCH	1832	1848	C:¥Users¥TESTUSER¥Desktop¥SHARE¥invoice_928649039284232_9482934d88.pdf.exe			
PROCESS_LAUNCH	2068	1832	C:¥Users¥TESTUSER¥AppData¥Local¥Temp¥zdttuqbg.exe			
PROCESS_LAUNCH	1896	2068	C:¥Users¥TESTUSER¥AppData¥Local¥Temp¥zdttuqbg.exe			
PROCESS_LAUNCH	2716	752	C:¥Program Files¥Internet Explorer¥iexplore.exe -Embedding			
NETWORKV4	2716			49446	62.113.232.164	80
NETWORKV4	2716			49447	62.113.232.164	80
PROCESS_QUIT	2716					
NETWORKV4	1896			49450	178.250.245.198	80

PID 2716

PID 1896

```
62.113.232.164      54 49446 > http [ACK] Seq=231 Ack=154 Win=131328 Len=0
62.113.232.164      54 49446 > http [FIN, ACK] Seq=231 Ack=154 Win=131328 Len=0
192.168.137.69      54 http > 49446 [FIN, ACK] Seq=154 Ack=231 Win=15680 Len=0
62.113.232.164      54 49446 > http [ACK] Seq=232 Ack=155 Win=131328 Len=0
62.113.232.164      54 49447 > http [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
192.168.137.255     92 Name query NB WPAD<00>
192.168.137.69      54 http > 49446 [ACK] Seq=155 Ack=232 Win=15680 Len=0
64.4.11.42         363 GET / HTTP/1.1
192.168.137.69     714 HTTP/1.1 302 Found  (text/html)
64.4.11.42          54 49437 > http [ACK] Seq=1255 Ack=41924 Win=65280 Len=0
178.250.245.198     66 49450 > http [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SA
192.168.137.69      66 http > 49450 [SYN, ACK] Seq=0 Ack=1 Win=12600 Len=0 MSS=12
178.250.245.198     54 49450 > http [ACK] Seq=1 Ack=1 Win=132096 Len=0
178.250.245.198    779 GET /V7MqD64K7VJOOHWZvlU7oe4s%2feLsgFA%2foi1kOacN4SOtN1RtS
192.168.137.69      54 http > 49450 [ACK] Seq=1 Ack=726 Win=14080 Len=0
192.168.137.69     207 HTTP/1.1 503 Service Unavailable  (text/html)
```

Evaluation Result ②

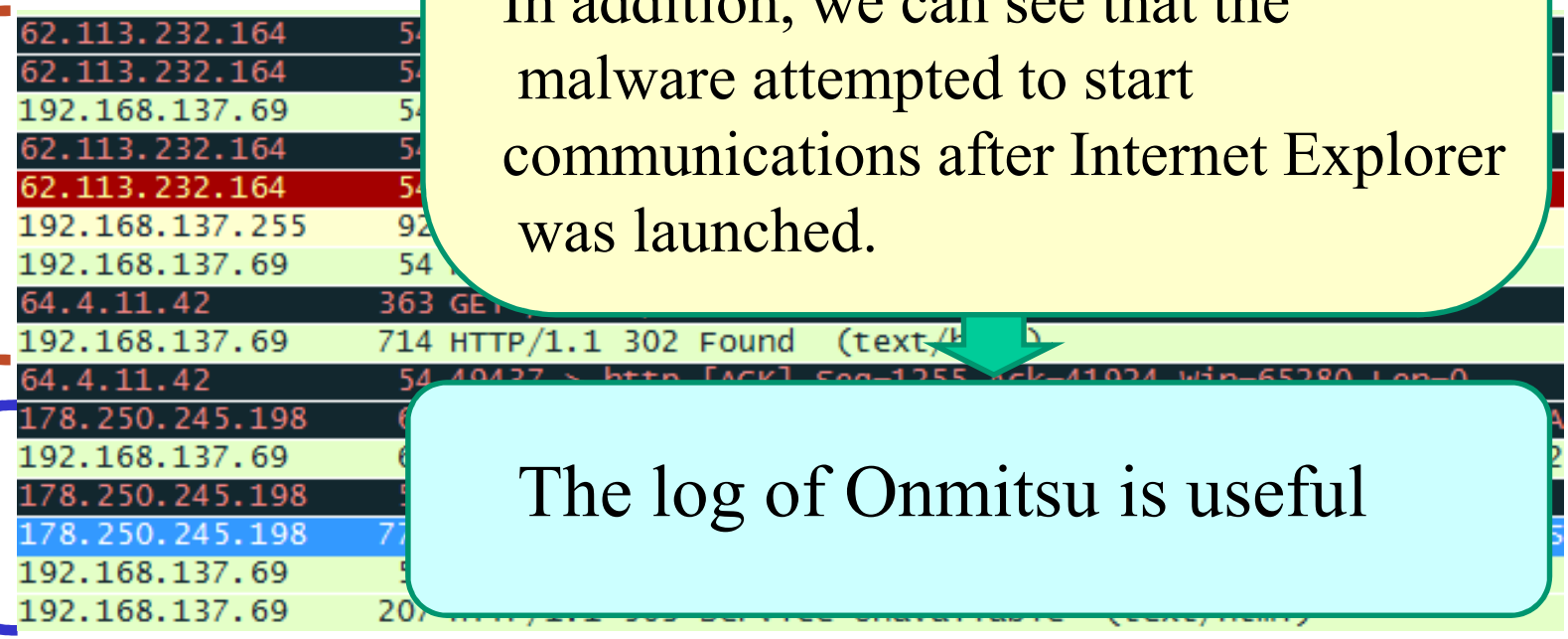
TYPE	PID	PARENT	CMD
PROCESS_LAUNCH	1832	1848	C
PROCESS_LAUNCH	2068	1832	C
PROCESS_LAUNCH	1896	2068	C
PROCESS_LAUNCH	2716	752	C
NETWORKV4	2716		
NETWORKV4	2716		
PROCESS_QUIT	2716		
NETWORKV4	1896		

From this log data, we can see that the malware started and activated other programs in the temporary folder.

In addition, we can see that the malware attempted to start communications after Internet Explorer was launched.

PID 2716

PID 1896



The log of Onmitsu is useful

Evaluation Results ③

- Log file size.
  - Test duration using Onmitsu: 3 hours.
  - File size of Onmitsu log: 10,868,492 (10.36 MB)
    - With “zip” compression : 755,732 bytes (738.01 KB / 6.95%)
  - Estimated volumes for one year by simple calculation.
    - 2,205,651,767 bytes (2.05 GB)

➡ Within acceptable volume size, because the volume of recent PC is around 1TB.

Evaluation Results ④

- System load.
  - Futuremark PCMark 8 score:
  - Result:
    - Without Onmitsu: 4319 (101%)
    - With Onmits : 4264 (100%)

The system loading imposed by the Onmitsu driver is close to negligible.

Result

- We measured the log file obtained by Onmitsu and verified its usability.
- The log from Onmitsu is useful and there are no problems with regards to system load and log volume.

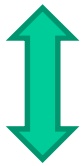
*CSV : comma-separated values

Resent Status

1. Onmitsu has been introduced to the Caplogger software product manufactured by DIT company and is in actual field usage.
2. A study aimed at using Onmitsu for identifying the network PC that originated the intrusion has started.

Map of Our Main Studies

Managemental



Technical

④ Guide System for DF using Android Terminal

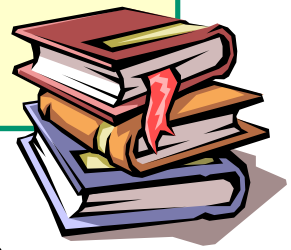
⑥ DF in Japan

⑤ Fog Forensic

③ LIFT System

② Onmitsu

①Signature scheme for keeping Evidence



Element  System

LIFT: Live and Intelligent Network Forensic Technologies

Development of intellectual network forensic system LIFT against targeted attacks

Kazuki Hashimoto,Hiroyuki Hiruma, Takashi Matsumoto, Kosetus Kayama, Yoshio Kaikizaki, Hiroshi Yamaki, Ryoichi Sasaki
Tokyo Denki University
5 Senju Asahi-cho, Adachi-ku, Tokyo, JAPAN
hashimoto@isl.im.dendai.ac.jp,
hiruma@isl.im.dendai.ac.jp,
sasaki@im.dendai.ac.jp

Tetsutaro Uehara

Ritsumeikan University
1 Nojihigashi, Kusatsu, Shiga, JAPAN
Uehara@cs.ritsumei.ac.jp

***Abstract*—Recently, the number of targeted attacks to specific organizations, such as companies or governments, has been increasing. Although such organizations are required to conduct to protect against the attack or mitigate the effect of the targeted attack, it is very difficult to perform the proper operation without the assistance of a support system. Therefore, the authors developed the Live and Intelligent Network Forensic Technologies (LIFT) system to guide the proper operation and/or conduct an automatic operation using artificial intelligence. The LIFT system collects the logs from servers, PCs, and communication equipment such as routers and detects abnormal signs from the collected logs. Next, the**

to perform the proper operation without the assistance of a support system.

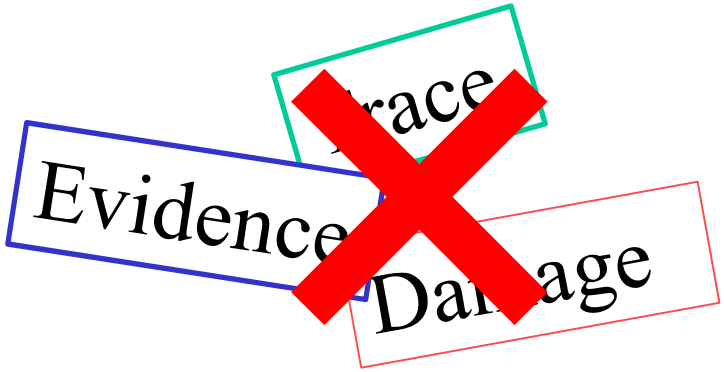
The Security Information and Event Management (SIEM) system has been attracting attention as a support system against targeted attacks [3]. The SIEM system gives real-time security threat detection capabilities to the log management system. Because it performs network forensics in real time, SIEM can be called a live network forensics system. Network forensics secures the evidence of saved collections for an analysis of a log in real time.

However, it is difficult to protect against an attack or mitigate the effect of the attack by using only the SIEM

Cybersec 2015 held in Indonesia

Background

- Targeted attacks have been increasing year by year



  - It is difficult to perform proper countermeasures against targeted attacks without the assistance of a support system.

Background

- SIEM attracts the attention
  - The system combines the functions of security event management and log analysis to provide real-time network forensics.
- However
  - It is difficult to protect attack by using only the SIEM system, because operators need enough knowledge and skill to use the system appropriately.

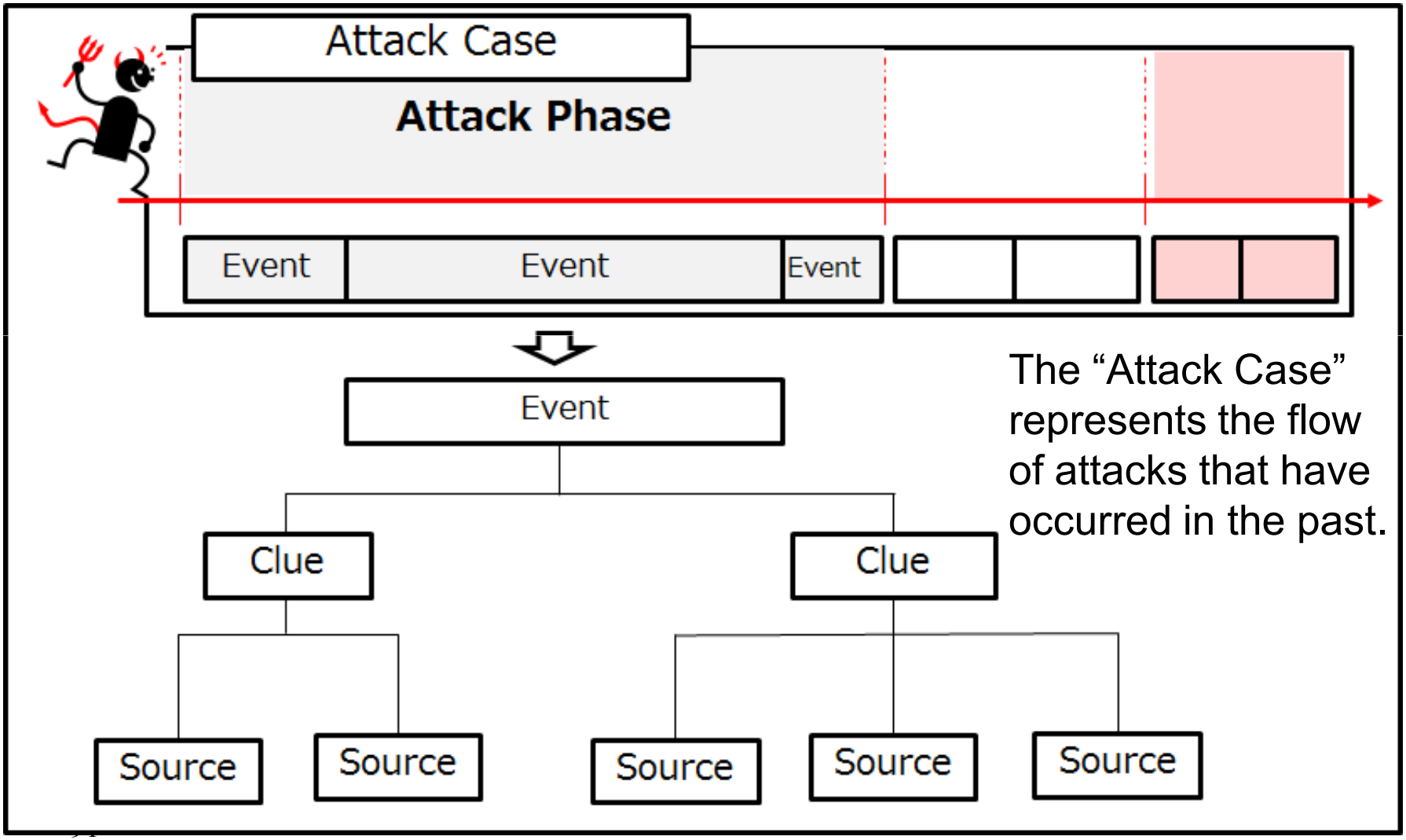
Overview of LIFT Project and System

- To cope with the issue, the LIFT project began at the Cyber Security Research Institute of Tokyo Denki University in 2013.
- In the project, we developed the LIFT system having the function of automatic operation using artificial intelligence(AI) and providing appropriate actions response guidance during incidents

LIFT: Live and Intelligent Network Forensic Technologies

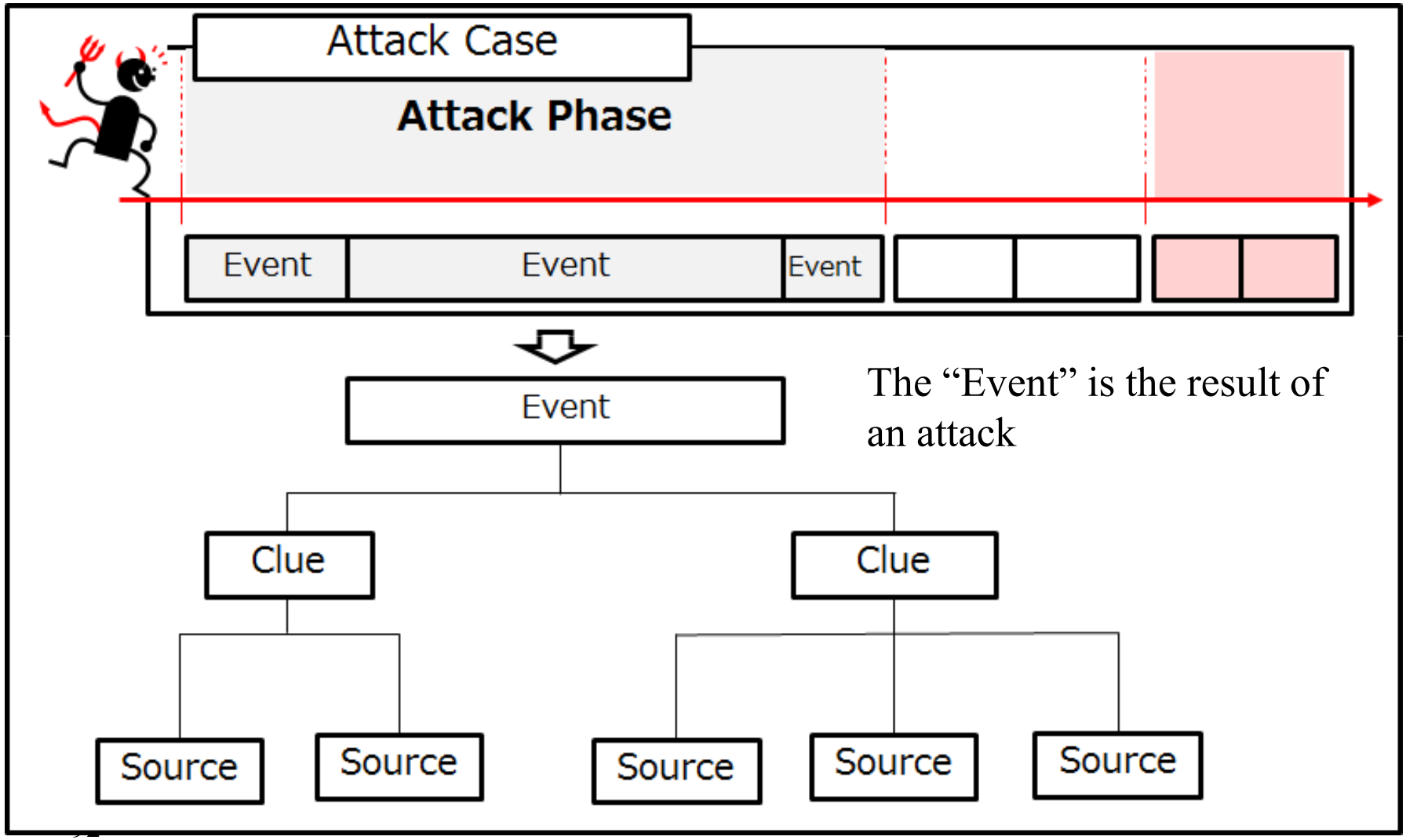
LIFT Project & LIFT System

- Attack Structure and LIFT System Terms Used



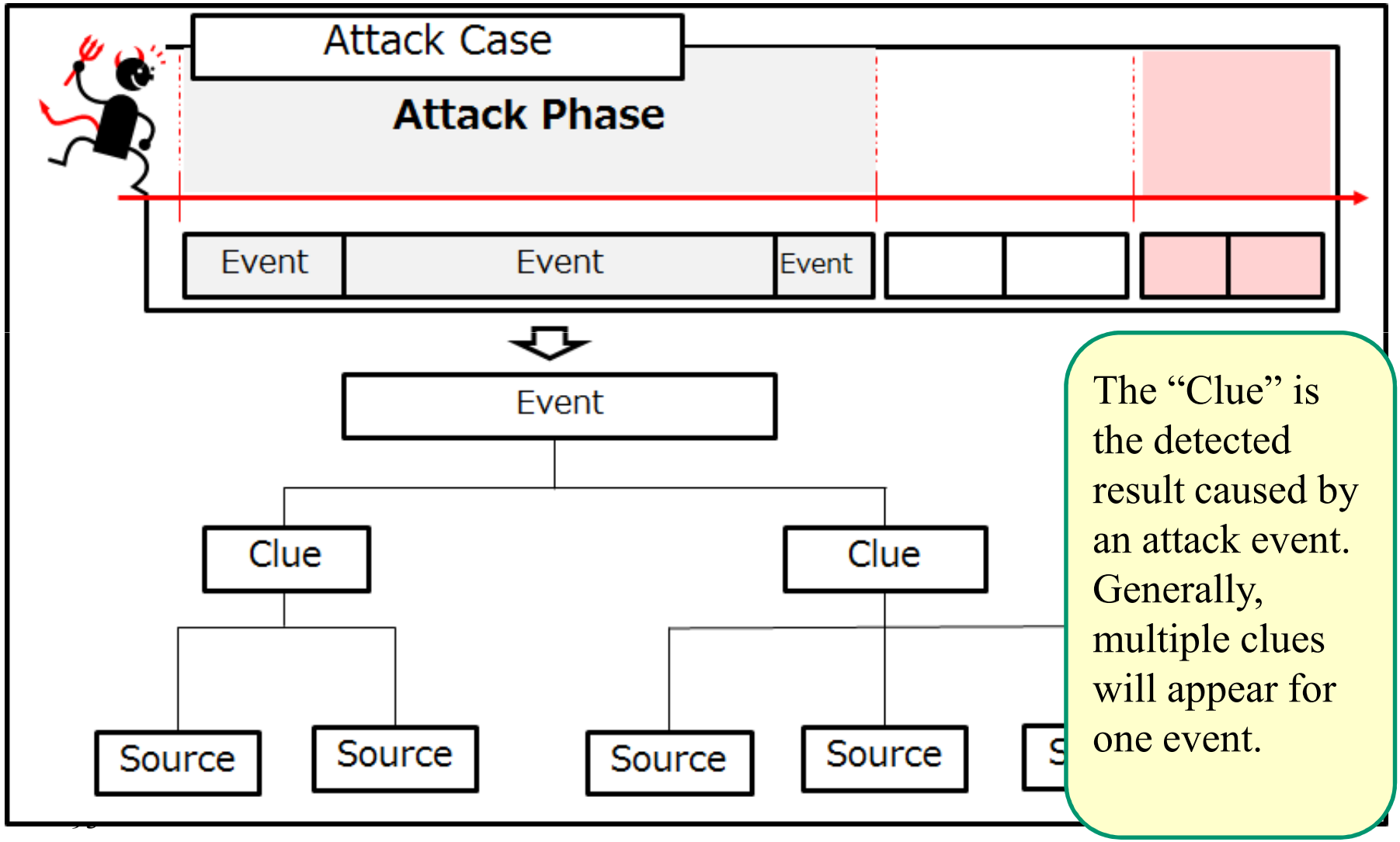
LIFT Project & LIFT System

- The structure of attack and terms used



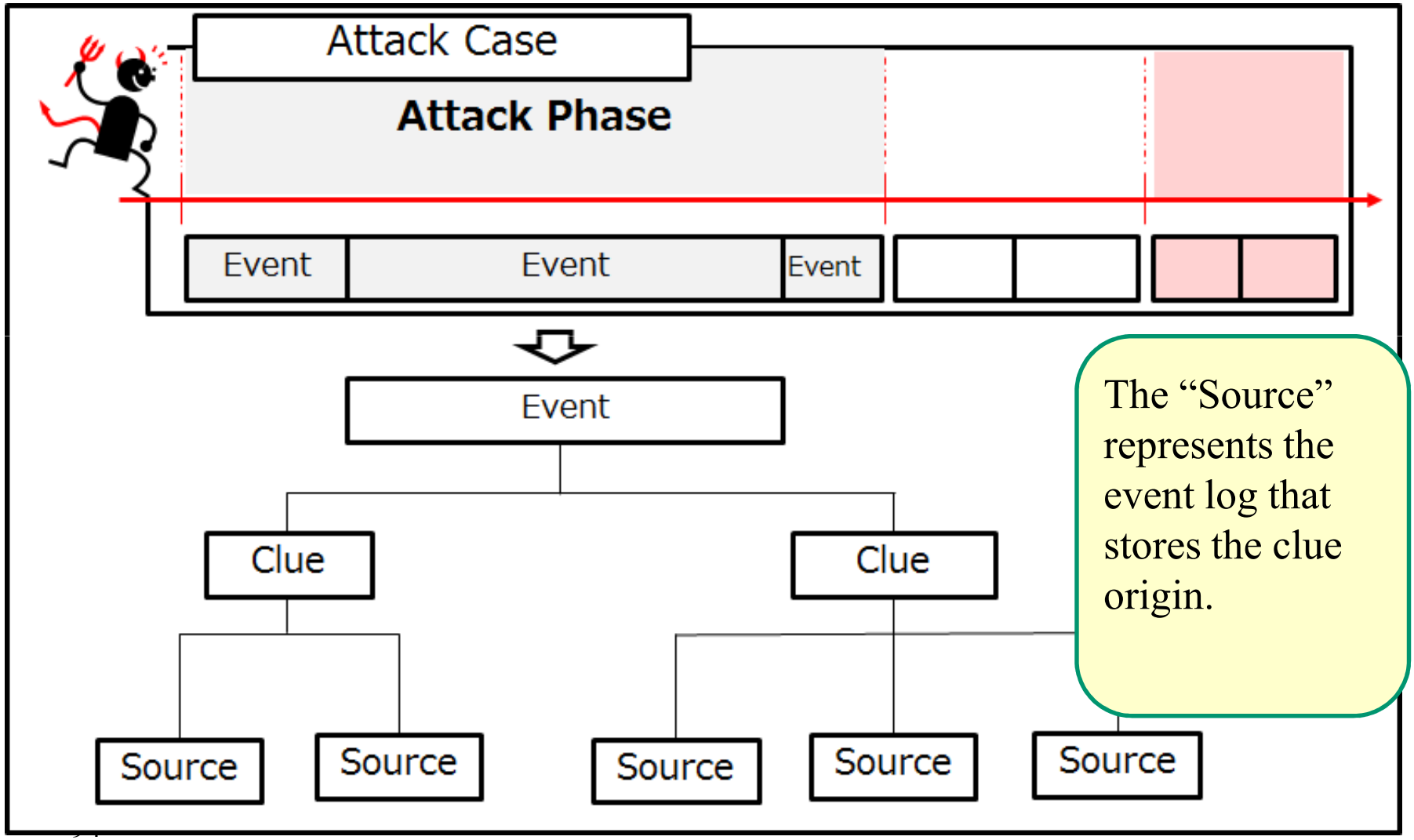
LIFT Project & LIFT System

- The structure of attack and terms used



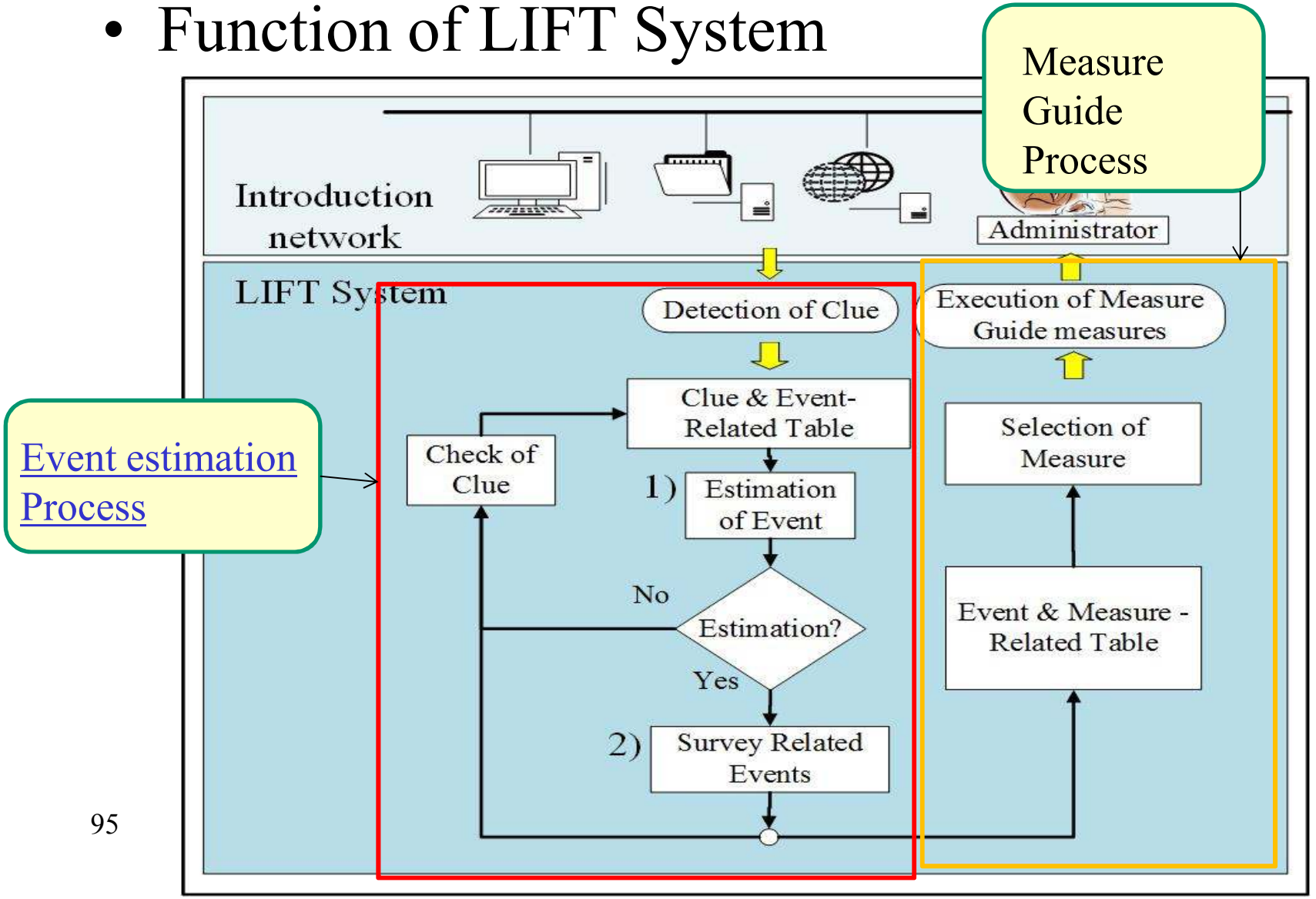
LIFT Project & LIFT System

- The structure of attack and terms used



Overview of LIFT System

- Function of LIFT System



Example of Event and Clue Related Table

	Event \ Clue		Proxy Server			
		The execution of the suspicious process	Communication without passing proxy	Using the CONNECT method other than port 443	Long session	Unnecessary commands to business
Attack Infrastructure Construction	Malware execution	0.3				
	Communication to C&C		0.6	0.6	0.4	
	Download of necessary function for attack	0.4	0.4		0.3	
	Malware collects information of the terminal	0.5			0.2	0.4

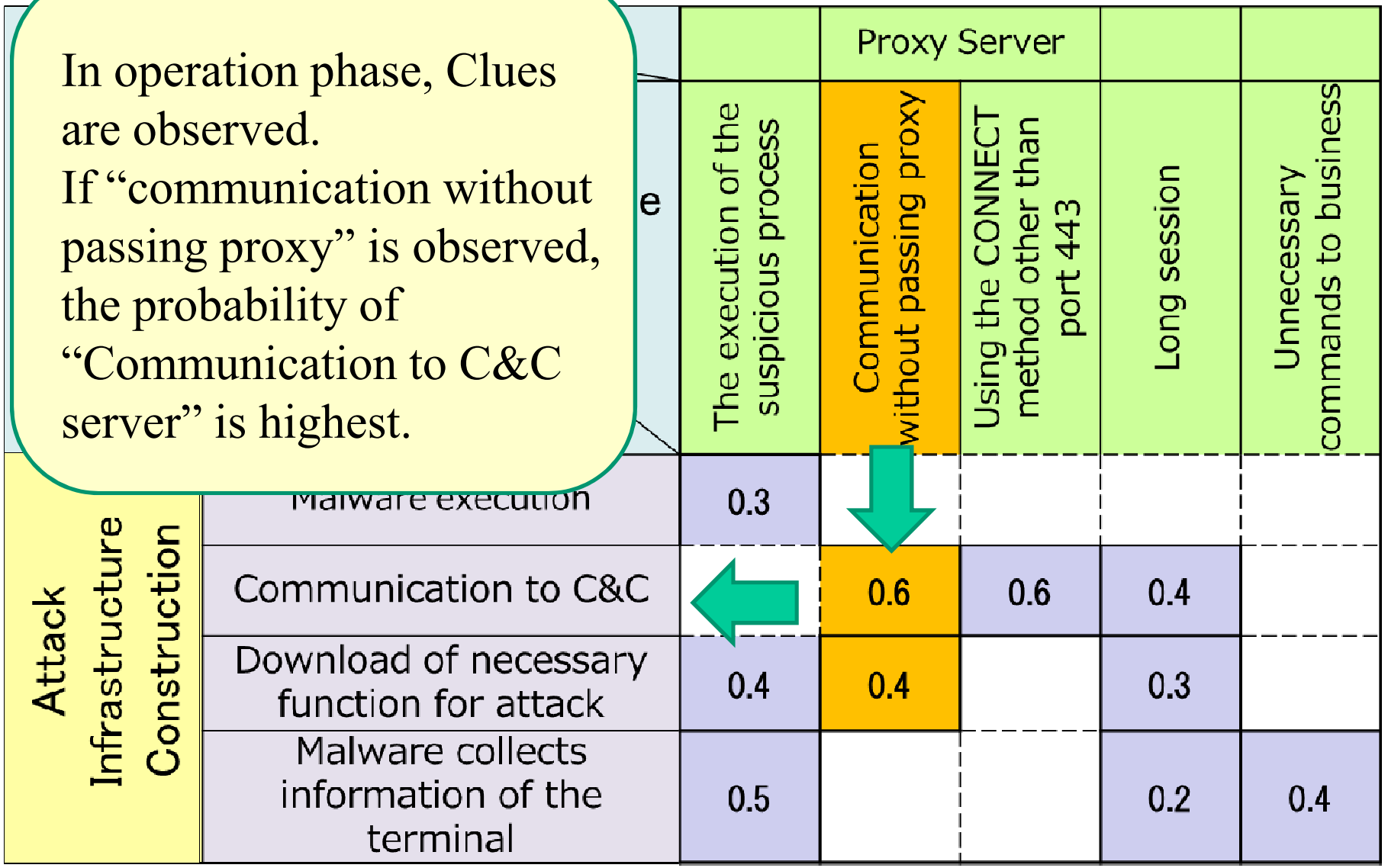
Example of Event and Clue Related Table

This table is constructed by experts considering what clues appear, when the event has occurred.

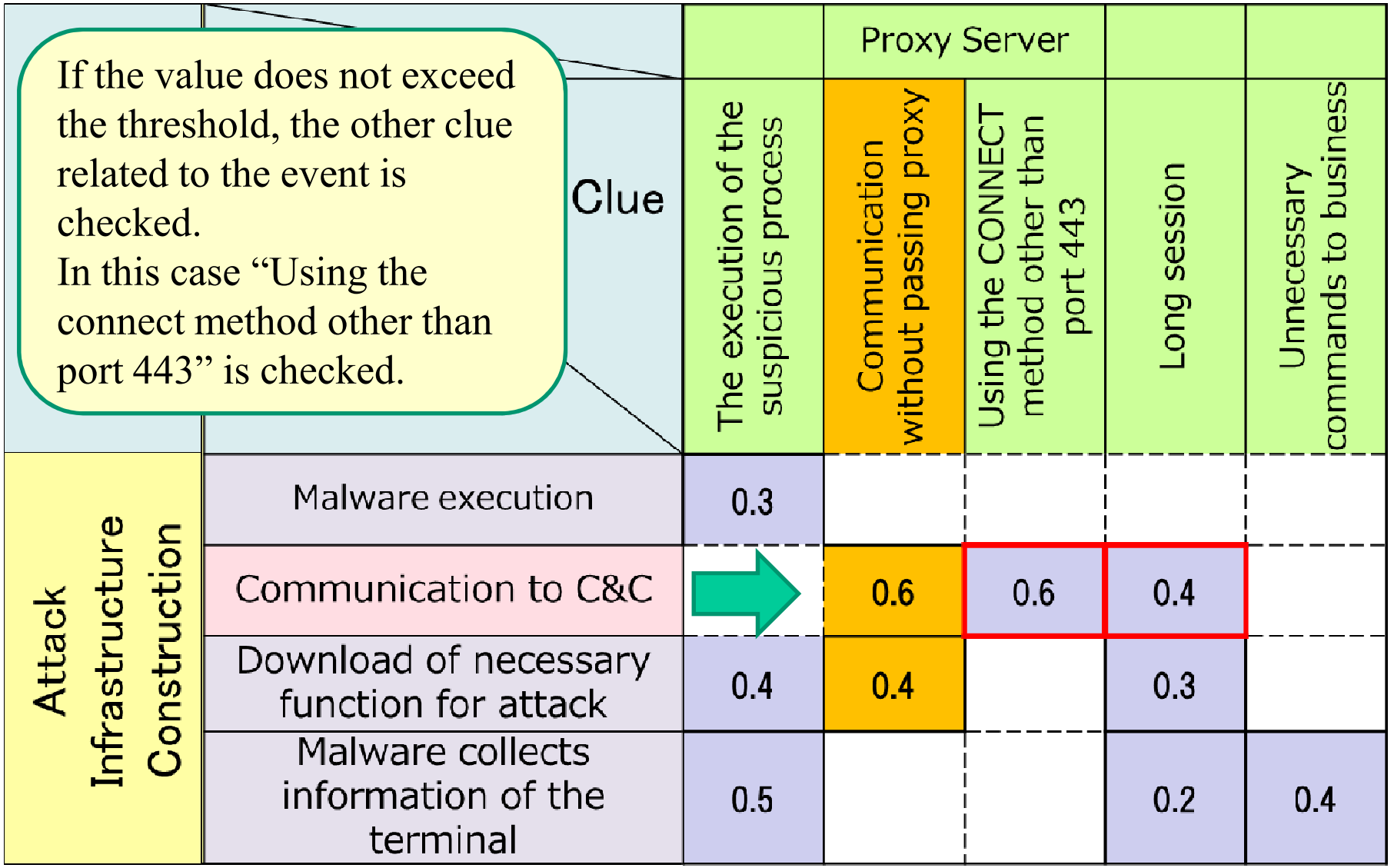
	Event \ Clue		Proxy Server			
		The execution of the suspicious process	Communication without passing proxy	Using the CONNECT method other than port 443	Long session	Unnecessary commands to business
Attack Infrastructure Construction	Malware execution	0.3				
	Communication to C&C		0.6	0.6	0.4	
	Download of necessary function for attack	0.4	0.4		0.3	
	Malware collects information of the terminal	0.5			0.2	0.4

LIFT Project & LIFT System

In operation phase, Clues are observed.
If “communication without passing proxy” is observed, the probability of “Communication to C&C server” is highest.



LIFT Project & LIFT System

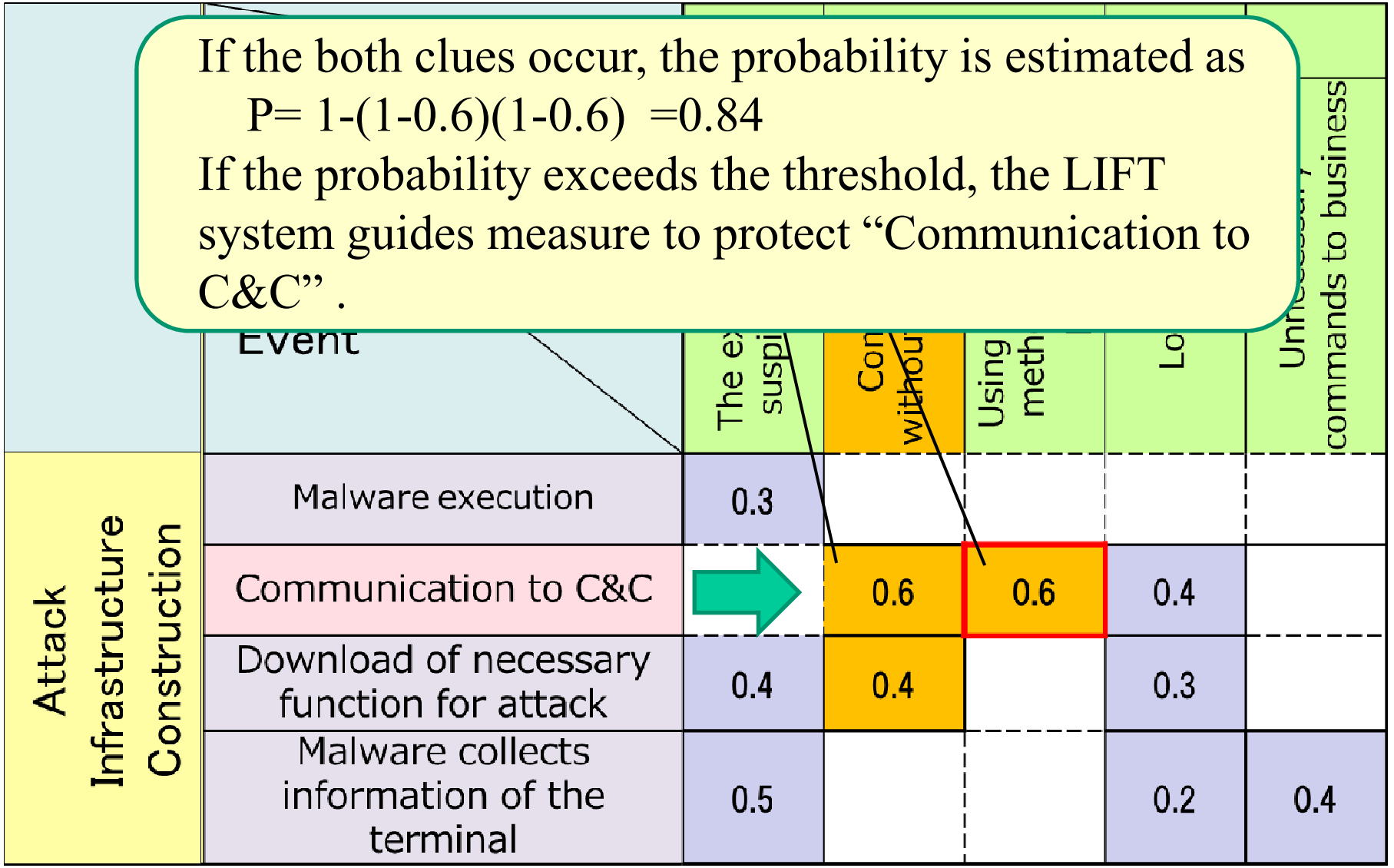


LIFT Project & LIFT System

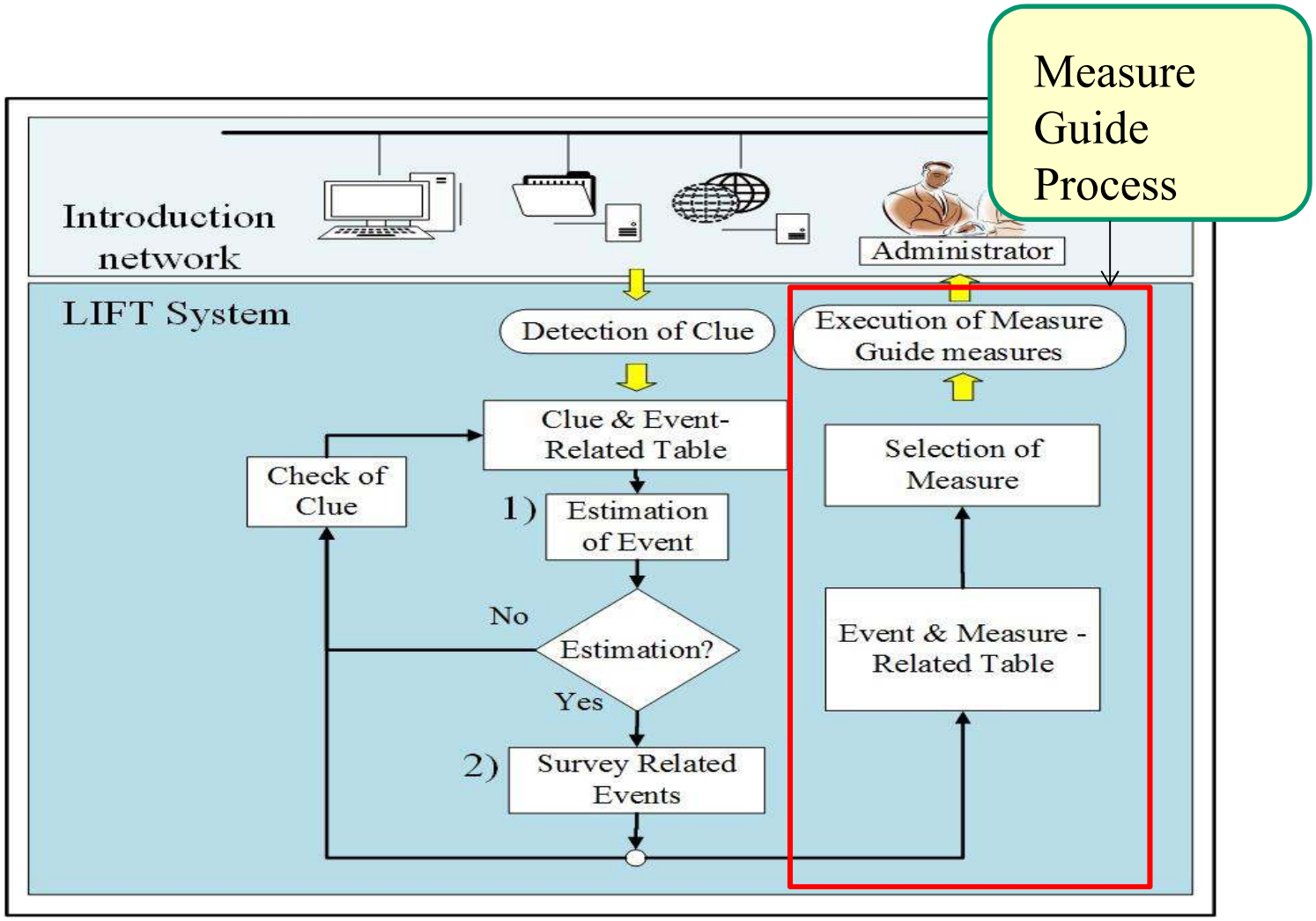
If the both clues occur, the probability is estimated as

P= 1-(1-0.6)(1-0.6) =0.84

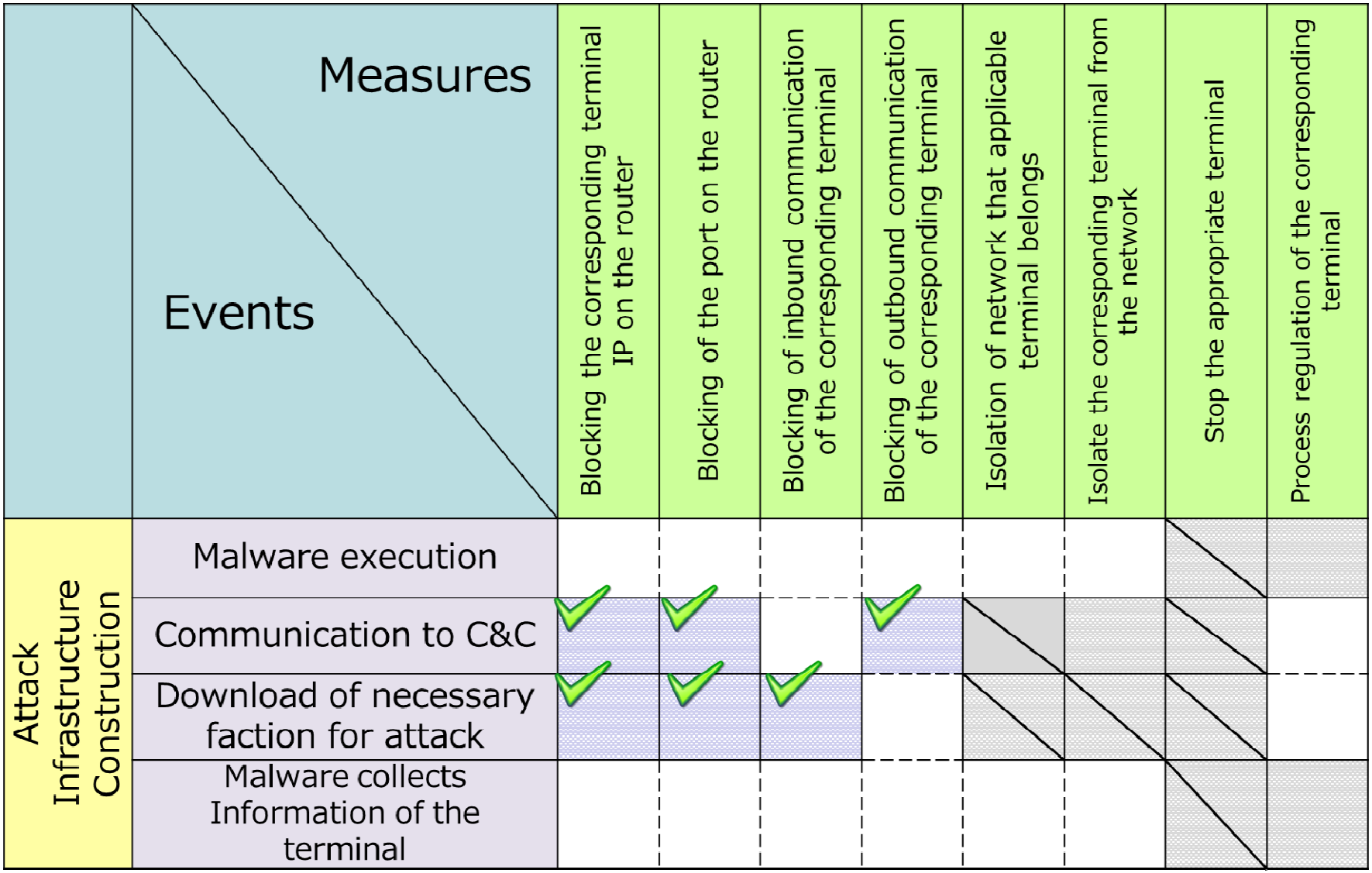
If the probability exceeds the threshold, the LIFT system guides measure to protect “Communication to C&C” .



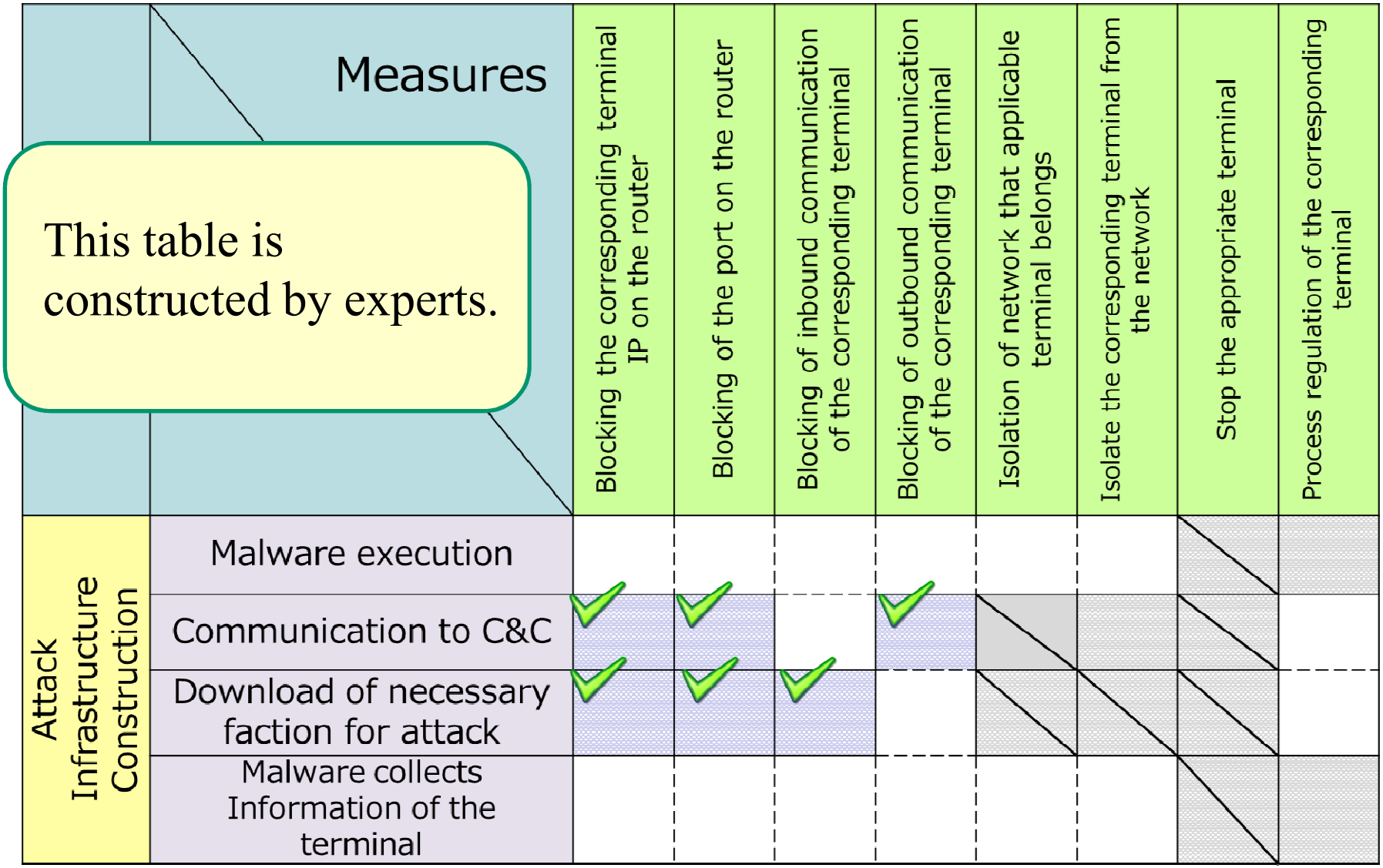
LIFT Project & LIFT System



Example of Event Measures Related Table

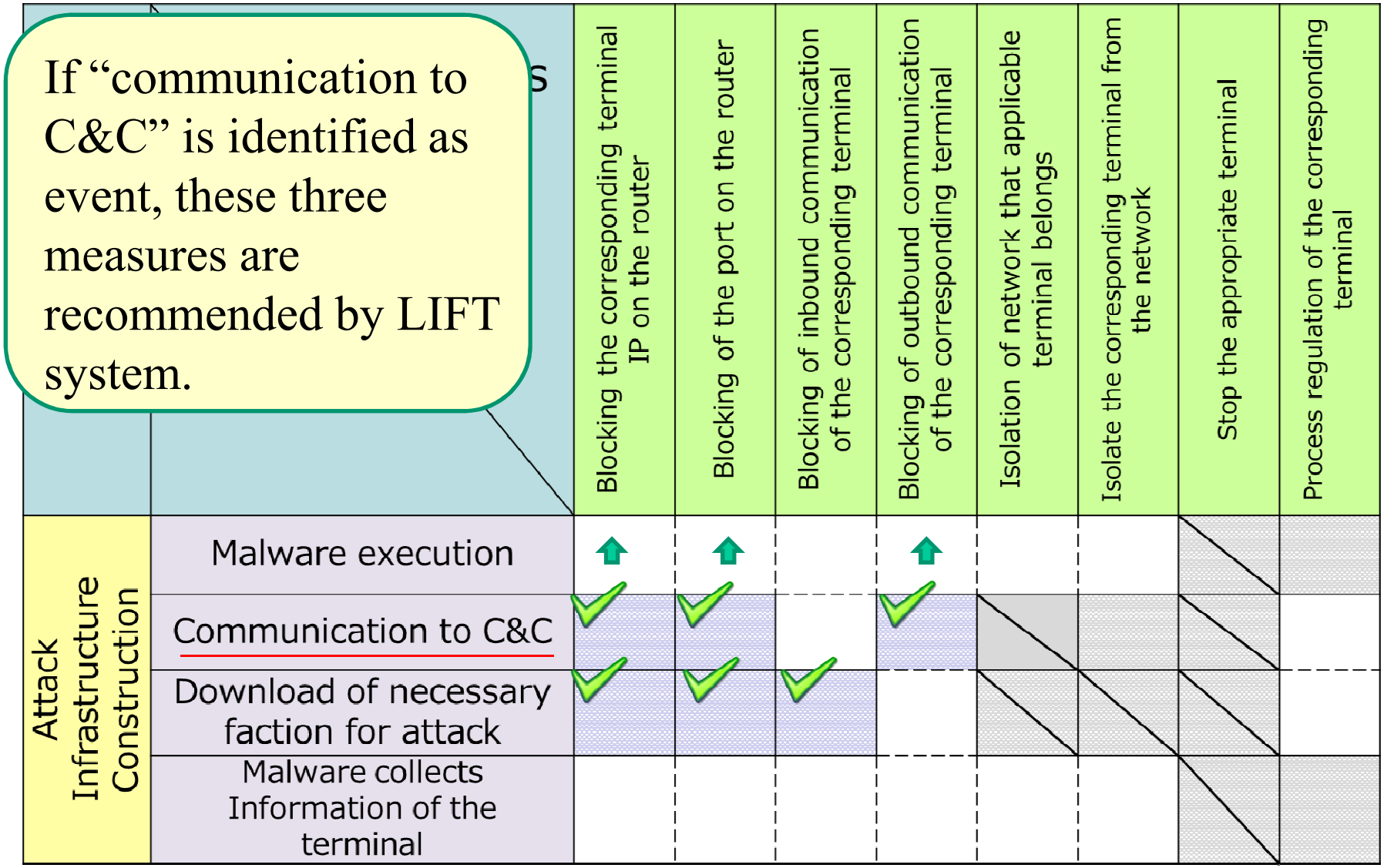


Example of Event Measures Related Table



Example of Event Measures Related Table

If “communication to C&C” is identified as event, these three measures are recommended by LIFT system.

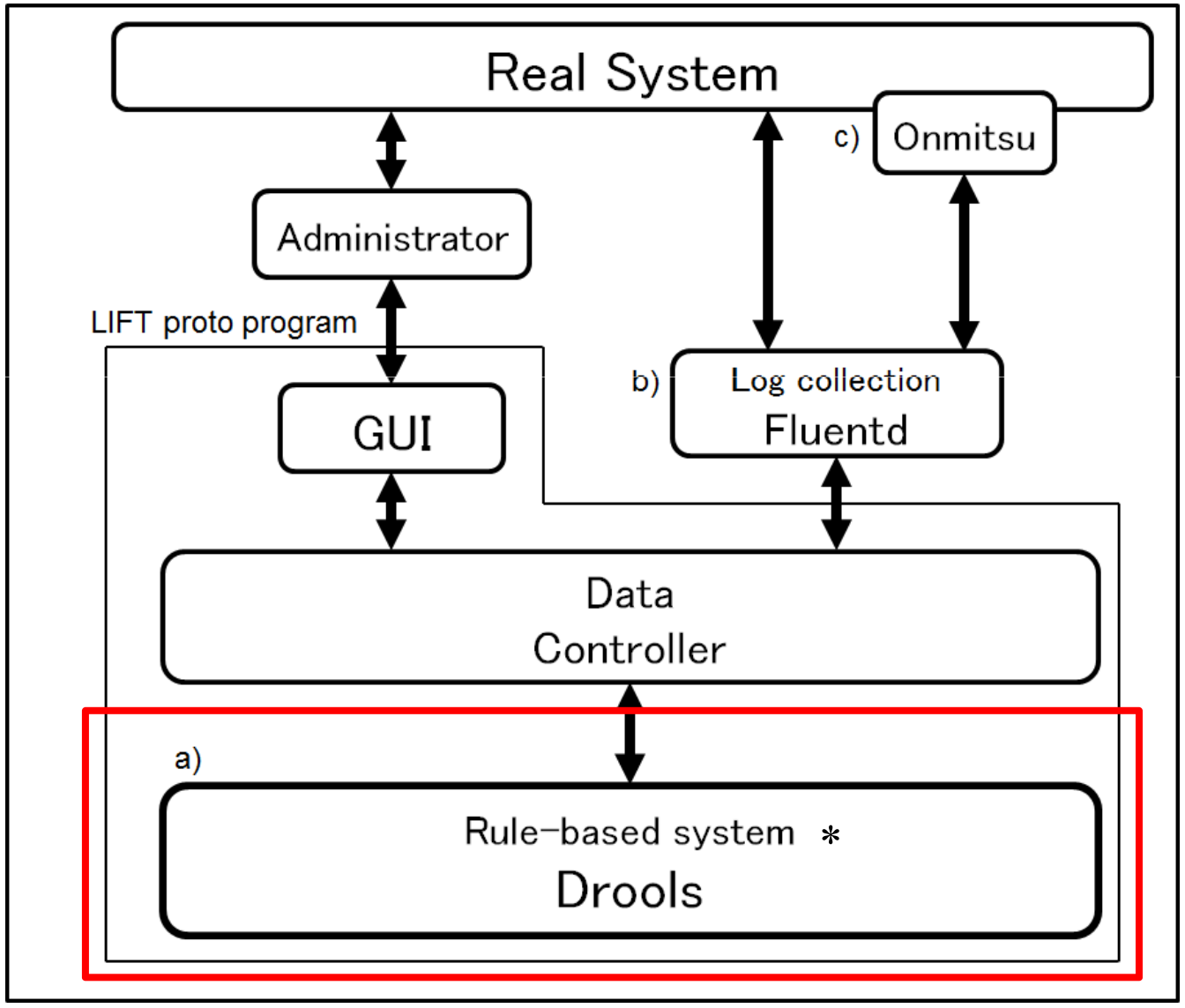


LIFT System Development

- LIFT proto program was developed under the environments.

Development Element	software
Development software	Eclipse
OS	Ubuntu 14.04
Development language	Java 8 Domain Specific Language

LIFT System Development



*One of AI technologies

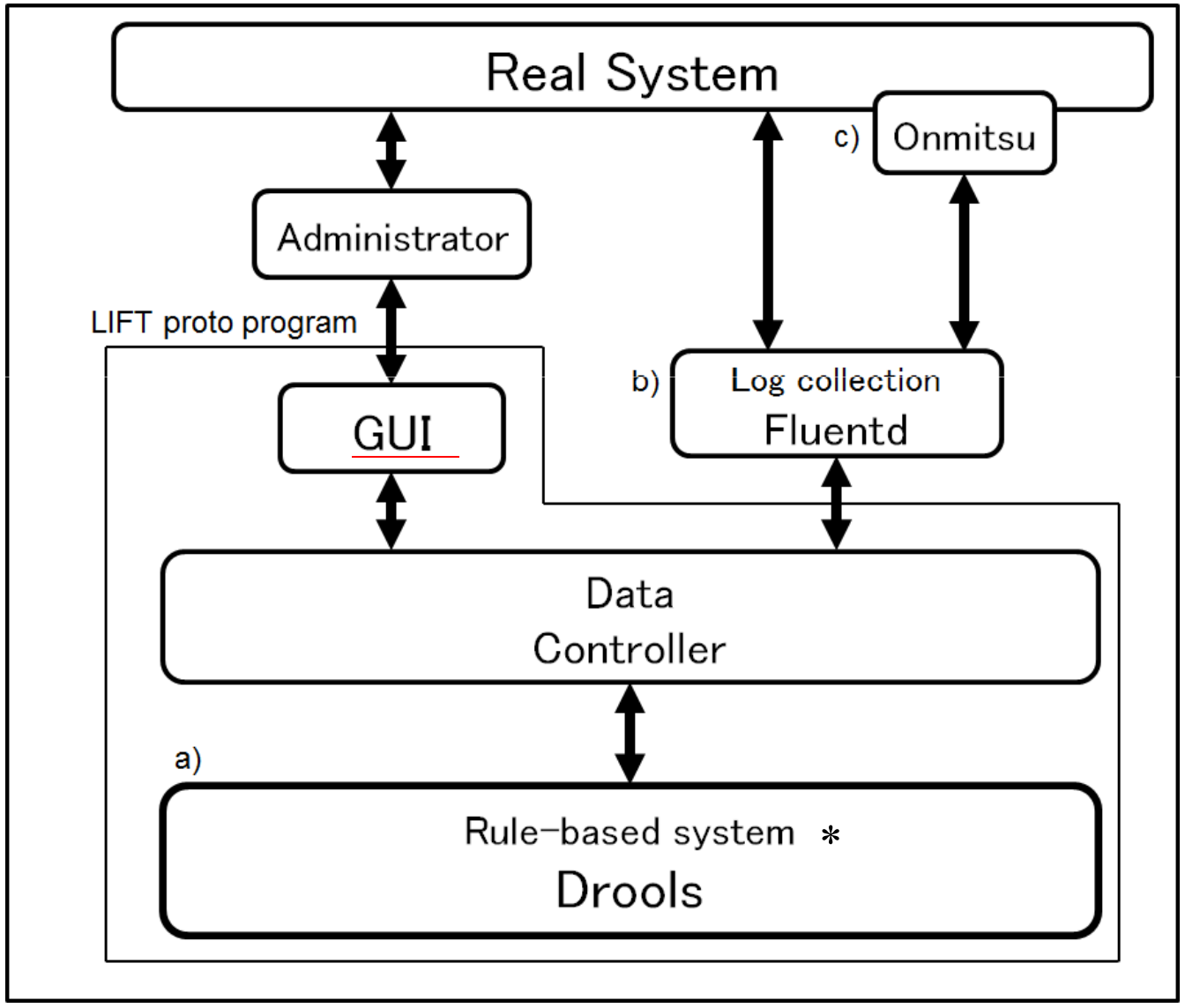
Tables are represented as rules in this system.

JBOSS Drools

- Rule-based system
- Event Estimation using reasoning
- Implements the rule engine based on the Rete algorithm corresponding to the Java Virtual Machine (JVM)

```
rule "Detect"
    salience 100
    //agenda-group "Fire"
    when
        $s : Core()
        $e : Assumption_Event(Accuracy >= Threequarters_Accuracy && Flag_Detect != 2)
    then
        $e.setFlag_Detect(2);
        $s.GUI_Notification(1,$e.getID(),2);
        update($e);
        update($s);
end
```

LIFT System Development



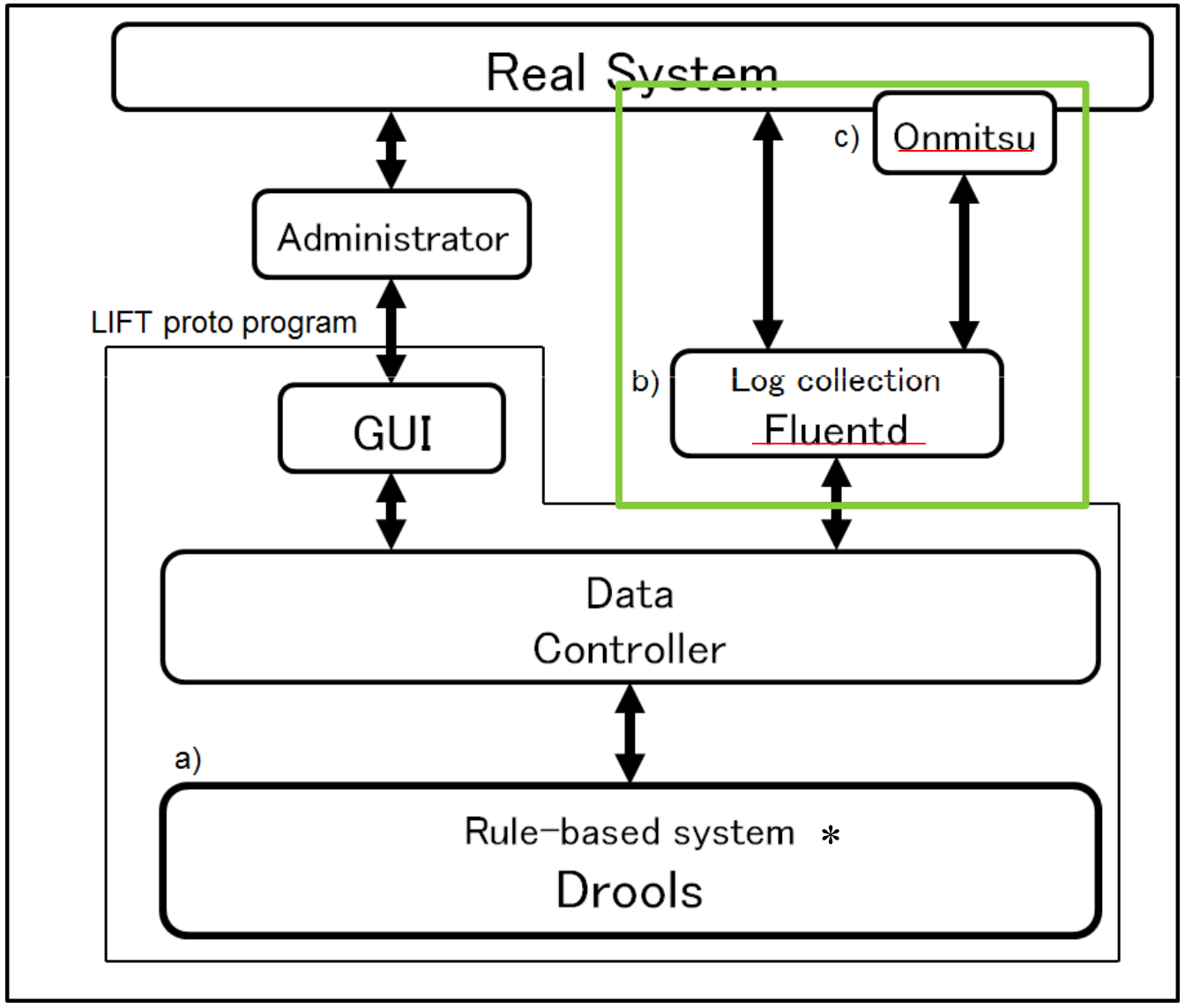
*One of AI technologies

Tables are represented as rules in this system.

Example of GUI

GUI in the case that a clue was observed.

LIFT System Development



*One of AI technologies

Tables are represented as rules in this system.

LIFT System Development

- Fluentd
  - Log collection software
    - Collection of various log
    - Structural log format
    - Input log in JavaScript Option Notation (JSON) format

- Onmitsu
  - Detection of the relationship between the network packets and process information in the computer

Application experiment

Purpose:

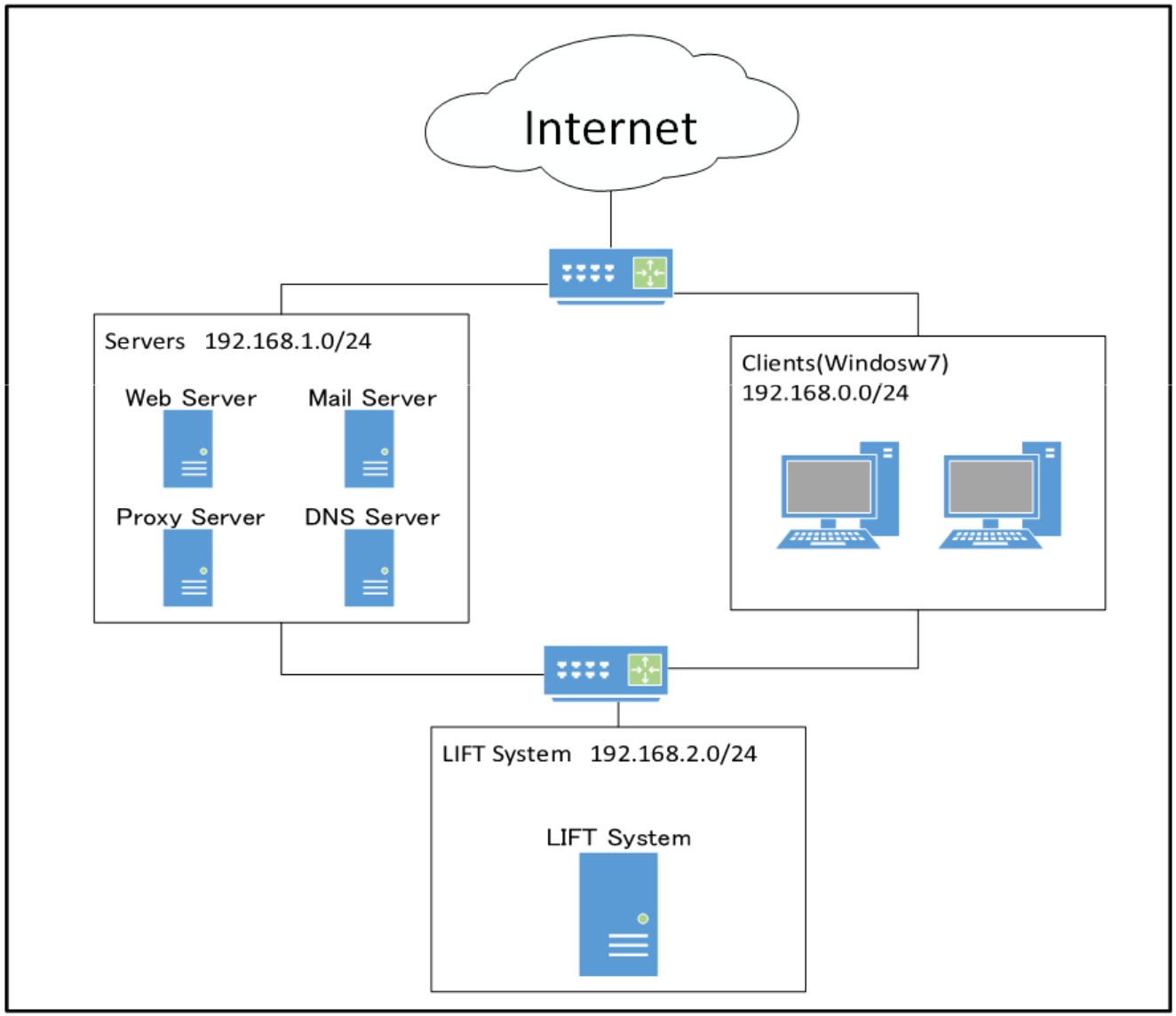
- Confirm the usefulness of the LIFT system
- Determine whether the LIFT proto program meets the LIFT system requirements.

Experiment

- We prepared six attack events
- Each pseudo attack was launched in the experimental environment 10 times
- The experimental results were compared against estimated attack results

Application experiment

- experimental environment



Application Experiment

- Experimental results ①

Event No.	Simulated attacks and events	Success or failure of estimated Event	Remarks
1	Employees launch malware contained in an email attachment	Success	Event 5 is also estimated
2	Malware communicates with the C&C server	Success	–
3	Malware extracts terminal information	Success	–

Application experiment

Event No.	Simulated attacks and events	Success or failure of estimated Event	Remarks
4	Malware explores the internal network	Success	–
5	Malware explores the internal network	Success	Event 1 is also estimated
6	Malware penetrates servers	Success	–

Application Experiment

Experimental results

- **LIFT proto program could estimate the events in all cases**
- **In two cases, the LIFT proto program estimated multiple events from the clue combinations**

To increase estimation accuracy

- **Introduce Bayesian network instead of Event – Clue related table**

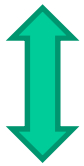
Recent Status

1. We introduced a Bayesian network instead of an Event - Clue related table and were able to identify all six events.

2. Although we were able to identify events that occurred in the past, it was difficult to identify new type events. To cope with this issue, a multi agent approach was introduced.

Map of Our Main Studies

Managemental



Technical

④ Guide System for DF Using Antroid Terminal

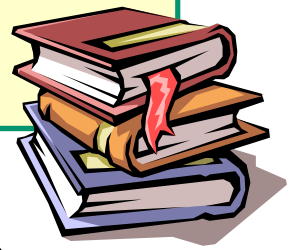
⑥ DF in Japan

⑤ Fog Forensic

③ LIFT System

② Onmitsu

①Signature scheme for keeping Evidence



Element  System

LIFT: Live and Intelligent Network Forensic Technologies

Extension and Evaluation of Guideline Total Support System for Digital Forensics

Takamichi Amano[1], Tetsutaro Uehara[2] and Ryoichi Sasaki[1]
[1]Tokyo Denki University
5 Senjuasahicho, Adachi-ku, Tokyo 120-8551, Japan
amano@isl.im.dendai.ac.jp and sasaki@im.dendai.ac.jp
[2]Ritsumeikan University, Japan

ABSTRACT

The recent rise in disputes relating to electromagnetic computer records has prompted the demand for digital forensic tools that can be used to preserve, investigate, and analyze digital evidence. Among the currently available digital forensic

1 INTRODUCTION

With the expansion of the information society, disputes related to computer electromagnetic records have been increasing. According to a 2013 white paper by the National Police

This study was presented at The International Conference on Information Security and Cyber Forensics (InfoSec2014) held in Malaysia.

Map of Our Main Studies

Managemental

Technical

④ Guide System for DF using Android Terminal

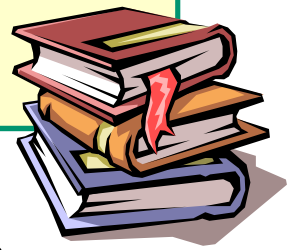
⑥ DF in Japan

⑤ Fog Forensic

③ LIFT System

② Onmitsu

①Signature scheme for keeping Evidence



Element  System

LIFT: Live and Intelligent Network Forensic Technologies

Paper related to Fog Forensics

Fog Computing:
Issues and Challenges in Security and Forensics

Yifan Wang, Tetsutaro Uehara
College of Information Science & Engineering
Ritsumeikan University
Kusatsu-shi, Shiga, Japan
wangyifian@cysec., uehara@{cs.ritsumei.ac.jp}

Ryoichi Sasaki
School of Science and Technology for Future Life
Tokyo Denki University
Adachi-ku, Tokyo, Japan
sasaki@im.dendai.ac.jp

***Abstract*—Although Fog Computing is defined as the extension of the Cloud Computing paradigm, its distinctive characteristics in the location sensitivity, wireless connectivity, and geographical accessibility create new security and forensics**

computing briefly. The following section takes a close look at Fog applications in different scenarios. In the fourth section we summarize different approaches to secure the cloud. In the fifth section, we discuss the Cloud forensics. Issues and

Presented at COMSAC2015

Map of Our Main Studies

Managemental

Technical

④ Guide System for DF

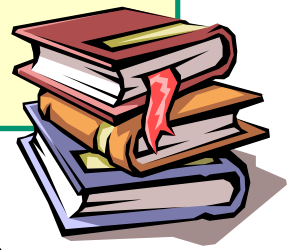
⑥ DF in Japan

⑤ Fog Forensic

③ LIFT System

② Onmitsu

①Signature scheme for keeping Evidence



Element  System

LIFT: Live and Intelligent Network Forensic Technologies

WIRELESS COMMUNICATIONS AND MOBILE COMPUTING
Wirel. Commun. Mob. Comput. (2010)
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/wcm.981

SPECIAL ISSUE PAPER

Development of digital forensics practice and research in Japan

Jigang Liu[1,2*], Tetsutaroh Uehara[1] and Ryoichi Sasaki[3]

[1] Kyoto University, Kyoto, Japan
[2] Metropolitan State University, St. Paul, MN, USA
[3] Tokyo Denki University, Tokyo, Japan

ABSTRACT

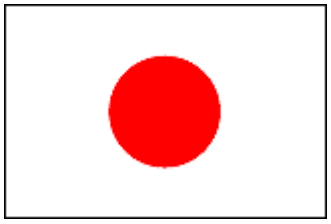
As a new frontier for fighting against cyber crime and cyber terrorism, digital forensics has experienced a rapid development in the last decade. Many countries have created new laws and legal procedures, developed new technologies, and enhanced education and research in this emerging field. Japan is no exception. In this paper, we first provide a nutshell of the Japanese

Paper in 2010

Table of contents

Background starting CySec

- The shortage of security experts is also a big issue in Japan.



Shortage of Security Field Workers in Japan

Number of Specialists Required（347,000）

Number of Current Security Field Workers（265,000）		Short-fall : (82,000)
Workers (Skilled) (106,000)	Workers (Unskilled) (159,000)	

http://www.ipa.go.jp/files/000040646.pdf July, 2014
IPA: INFORMATION-TECHNOLOGY PROMOTION AGENCY

Overview of CySec

- Tokyo Denki University launched a cyber-security education course named CySec in 2015.
- CySec is a course for Security workers and Master course students.
- It is supported by the Ministry of Education, Culture, Sports, Science and Technology (MEXT)

CySec Topics

1PF: Cyber Security Infrastructure

2CD: Cyber Defense Actual Exercise

3IN: Security Intelligence, Psychology, Ethics and Law

4DF: Digital Forensics

5MG: Information Security Management and Governance

6DD: Secure System Design and Development

CySEC

1PF: Cyber Security Infrastructure

2CD: Cyber Defense Actual Exercise

3IN: Security Intelligence, Psychology, Ethics and Law

4DF: Digital Forensics

5M

6D

It is a first regular course on digital forensics in a Japanese University.

Digital Forensics Curriculum in CySec①

1. Introduction of Digital Forensics
2. Hard disk structure, File system Technologies
3. OS for forensics
4. Forensic work basics
5. Forensic work, Data conservation
6. Forensic work, Data recovery
7. Forensic work, Data analysis①
8. Forensic work, Data analysis②

Digital Forensics Curriculum in CySec②

9. Forensic work exercise
10. Network forensic
11. Network forensic exercise
12. DF methods for typical targets①
13. DF methods for typical targets②
14. Law literacy and handling court
15. Future development of digital forensics

In course of 2016, mobile forensics was added instead of DF methods for typical targets②

Lecturers

(1) Prof. Sasaki (Tokyo Denki Univ.)

(2) Prof. Uehara (Ritsumei Univ.)

(3) Prof. Yamaki (Tokyo Denki Univ.)

(4) Mr. Sakuraba (Lawyer)

(5) Mr. Shirahama (Forensics Expert)

(6) Mr. Nozaki (Forensics Expert)

Education Status

1. In 2015, the course was attended by 54 security field workers and 16 Master course students.
2. Numerous security experts were among the students.
3. Security field workers were sent from police departments, financial services agencies, etc.
4. Based on post-course questionnaire results, students were highly satisfied with our lectures.

Future Directions

1. We will introduce an advanced course on digital forensics to Tokyo Denki University.

2. We will support the inauguration of digital forensic courses in other universities.

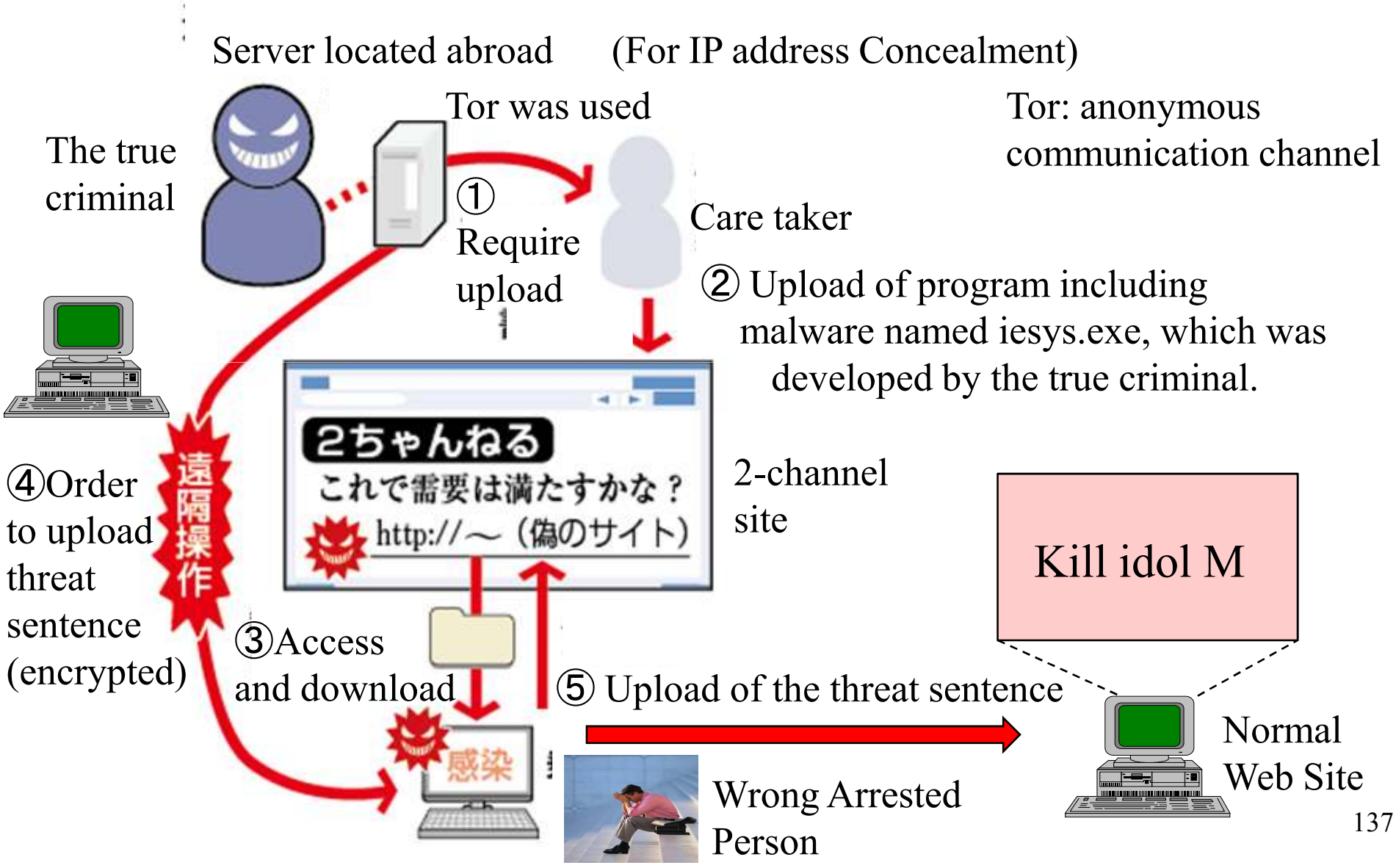
Table of contents

Improper Arrest Case Related to Remote Control Virus

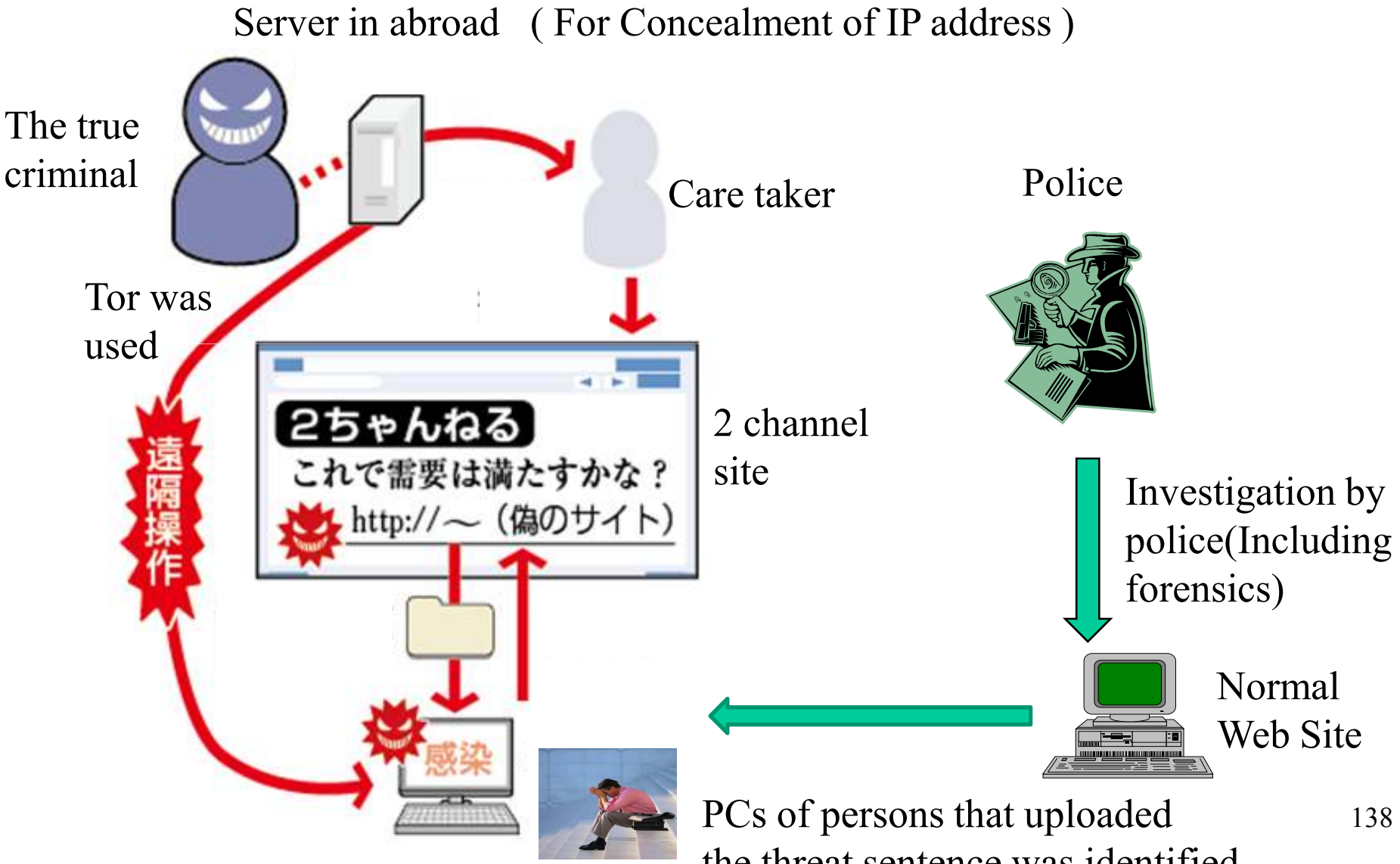
In 2012, four persons were arrested after being suspected of uploading threats to the Internet.

Later, it became clear that remote control viruses in the suspects' personal computers (PCs) were responsible for the uploading.

Attack Flow


Server located abroad
(For IP address Concealment)
Tor was used
Tor: anonymous communication channel
The true criminal
① Require upload
Care taker
② Upload of program including malware named iesys.exe, which was developed by the true criminal.
2ちゃんねる
これで需要は満たすかな？
http://～（偽のサイト）
2-channel site
遠隔操作
④Order to upload threat sentence (encrypted)
③Access and download
感染
⑤ Upload of the threat sentence
Kill idol M
Normal Web Site
Wrong Arrested Person

Flow of Investigation



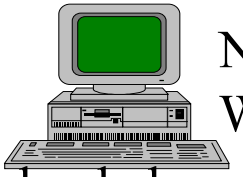
Flow of Investigation

Server in abroad (For Concealment of IP address)

(1) Four PC owners were arrested by mistake in 2012.
(2) One of them was charged with interference and prosecuted.
(3) However, malware named iesys.exe was founded in the PCs of the other arrested persons.
(4) Part of the same malware was also found in the PC of person prosecuted.
(5) The prosecuted person was released.
(6) The search to find the true criminal continued.

Police

Investigation by police(Including forensics)



Normal Web Site

PCs of persons that uploaded the threat sentence was identified

New Progress

(1) The following message was sent to mass media on Jan. 1, 2013: *"Happy new year. I am the real criminal. Can the police arrest me?"*

(2) The second message as follows was sent to mass media: *"I have attached a memory chip containing the iesys.exe source program and a text file describing the my objectives to a cat on Enoshima Island"*

Photograph of Enoshima

New Progress

(3) The cat with a memory chip attached to its neck was discovered by the police.

At the same time, the police examined Enoshima surveillance camera image data showing the memory chip being attached to the cat's neck.

New Progress

(4) A 30-year-old man, hereafter described as “X”, was arrested on Feb. 2, 2013.

(5) Police announced they had found evidence in the suspect’s company PC that showed “X” had accessed Tor around the same time when the malware was uploaded via Tor.

(6) “X” pleaded not guilty. In his appeal, he stated that he could not write the C# used for iesys.exe.

New Progress

(7) During the trial, the prosecution's digital forensic expert testified that a piece of the program remained in the slack space of the suspect's PC, thereby providing evidence.

This case marked that the first time deep discussions regarding digital forensics were held in a Japanese court.

Results

(1) After the suspect was released on bail, he held a press conference with his lawyers on May 16, 2014.

(2) Around the same time, mail from a person who claimed to be the real criminal was sent to mass media outlets. This convinced many people still that "X" was not the actual criminal.

Results

(3) However, a detective who tailed the suspect after his release witnessed him burying a mobile phone on a riverbank.

When the phone was examined, the police discovered an incriminating sentence, which the suspect had set to be sent out at the same time as the press conference.

Faced with this evidence, “X” confessed to the crime.

Results

(4)) In 2015, the Tokyo District Court has established penalties for 10 cyber-crimes, and announced penal servitude eight years.

Results

(4) In 2015, the Tokyo District Court has established penalties for 10 cyber-crimes, and announced penal servitude eight years.

Digital forensics has become a very important technology in Japan's courts.

Table of contents

Future Direction

1. The importance of digital forensics will increase year by year also in Japan.
2. We would like to increase the number of digital forensics experts, including researchers.
3. Personally, I would like to focus primarily on the following three targets:

   (1) Network Forensics

   (2) Live Forensics

   (3) Fog Forensics

Thank you for your attention