Traceback Research & Experiments Against Source Address Attacks

APRICOT2010

Japan Data Communications Association
Telecom-ISAC Division
Ken Wakasa

JADAC

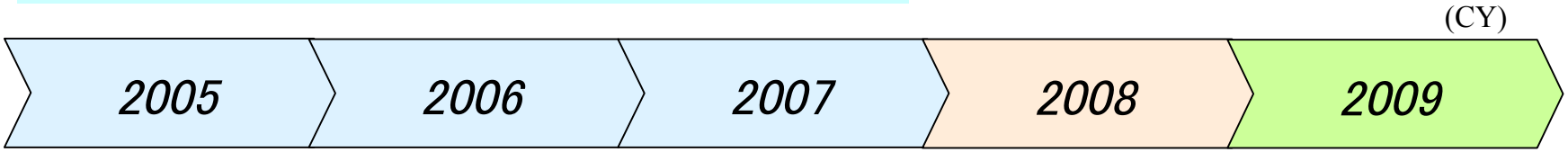
Traceback Research project

(*) NICT stands for National Institute of Information and Communications Technology.

* A research project offered by NICT(*), started 2005 by the Consortium of six parties
* Goal of the project is Demonstration Experiment of traceback

Consortium (five other parties)

Research and development :



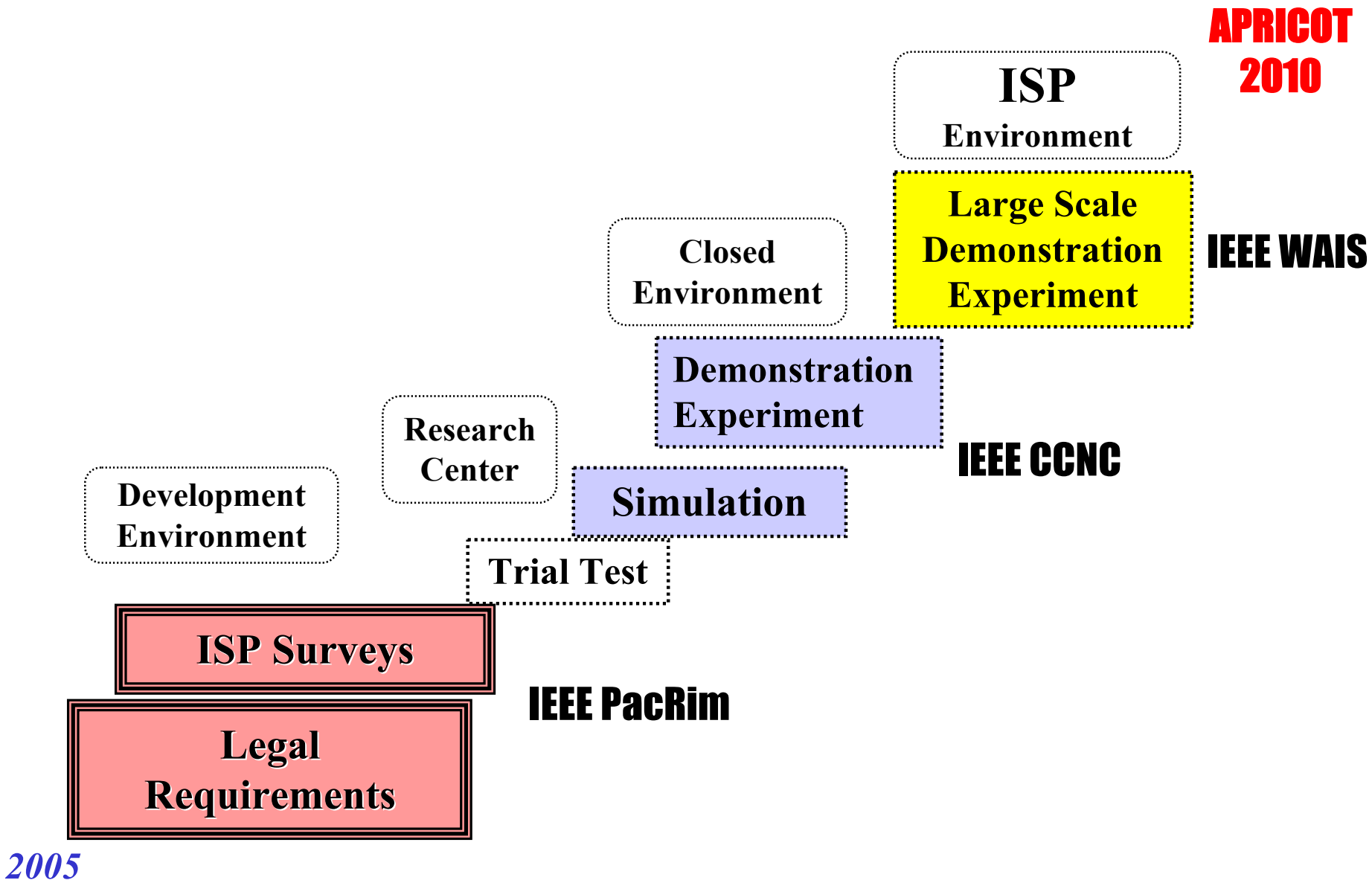
JADAC

Experiment preparations :
Investigation / examination / document making

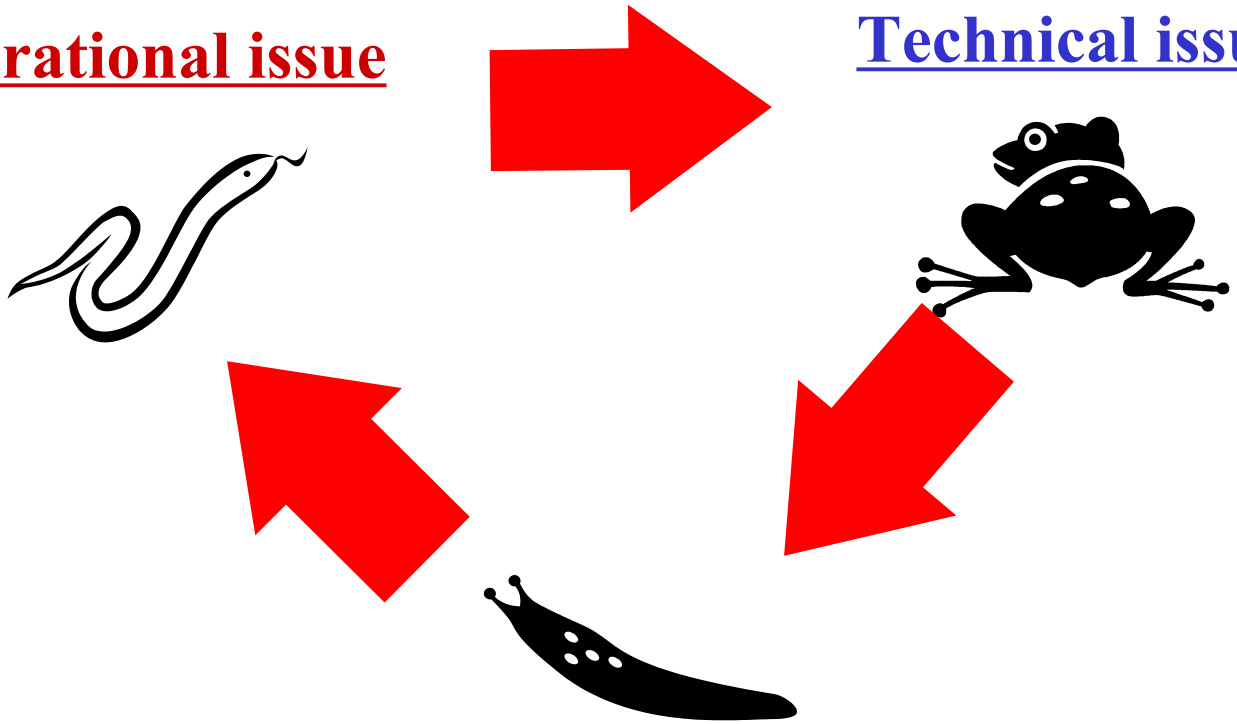
Demonstration Experiment

Large Scale Demonstration Experiment

Schedule



Three fundamental issues greatly influence one another.

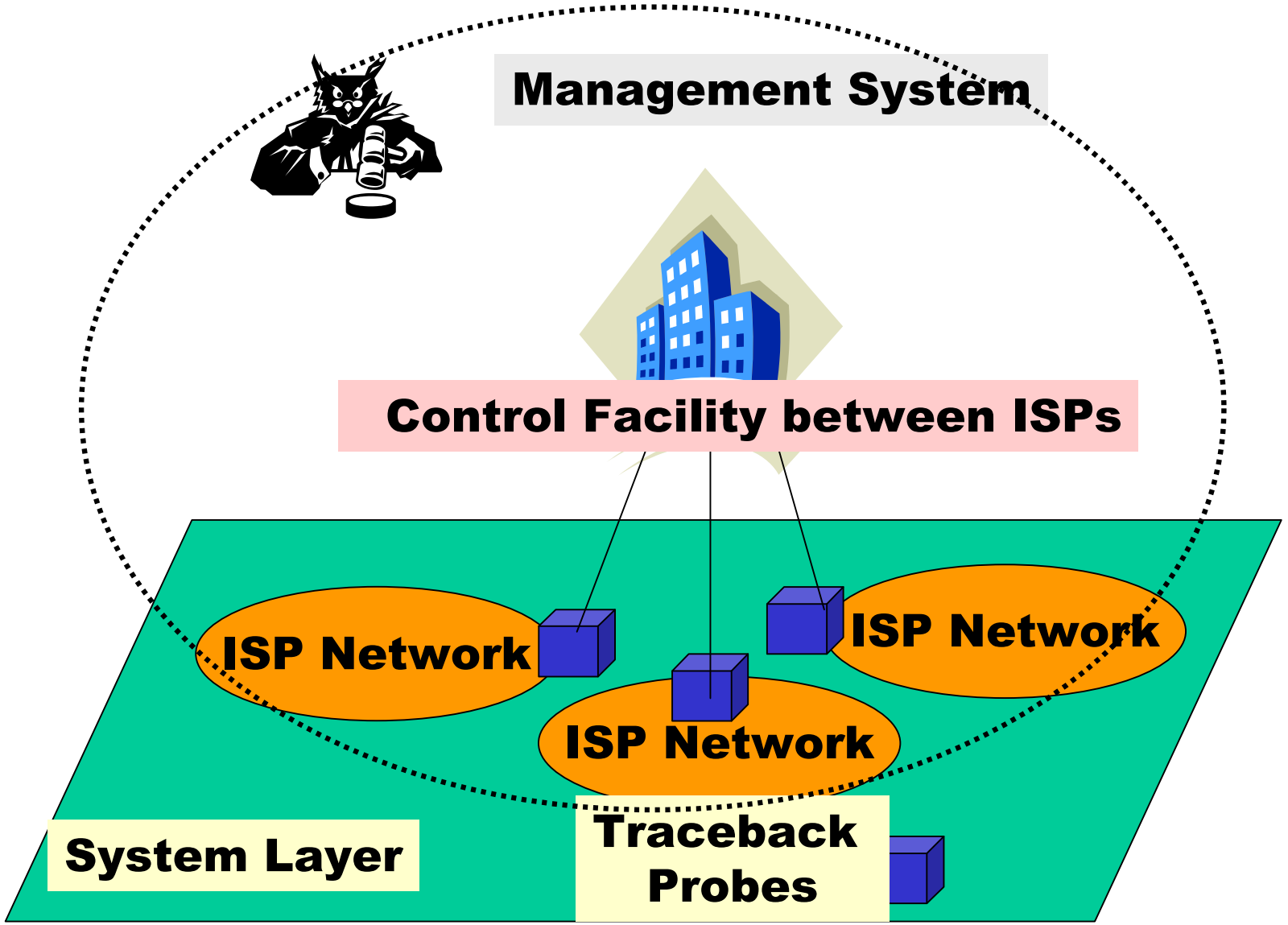


Privacy of Communications

Measures of Satisfy Requirements

Legal Requirements	Measures to Satisfy Requirements
(1) Mitigating the Impact on Equipment	Use of TAPs/mirrors
(2) Guranteering Privacy of Communications	Adoption of Hash Method
(3) Tracking Personal Authentication	Access Control
(4) Incident Response	Policies
(5) Protecting of Data to Outbreak	Policies
(6) Obligation of Confidentiality in Data Sharing	Agreements
(7) Information Disclosure	Policy Disclosure
(8) Obligation of Confidentiality	Agreements
(9) Appropriate Security Policies and Privacy Policies	ISMS

Traceback Platform outline

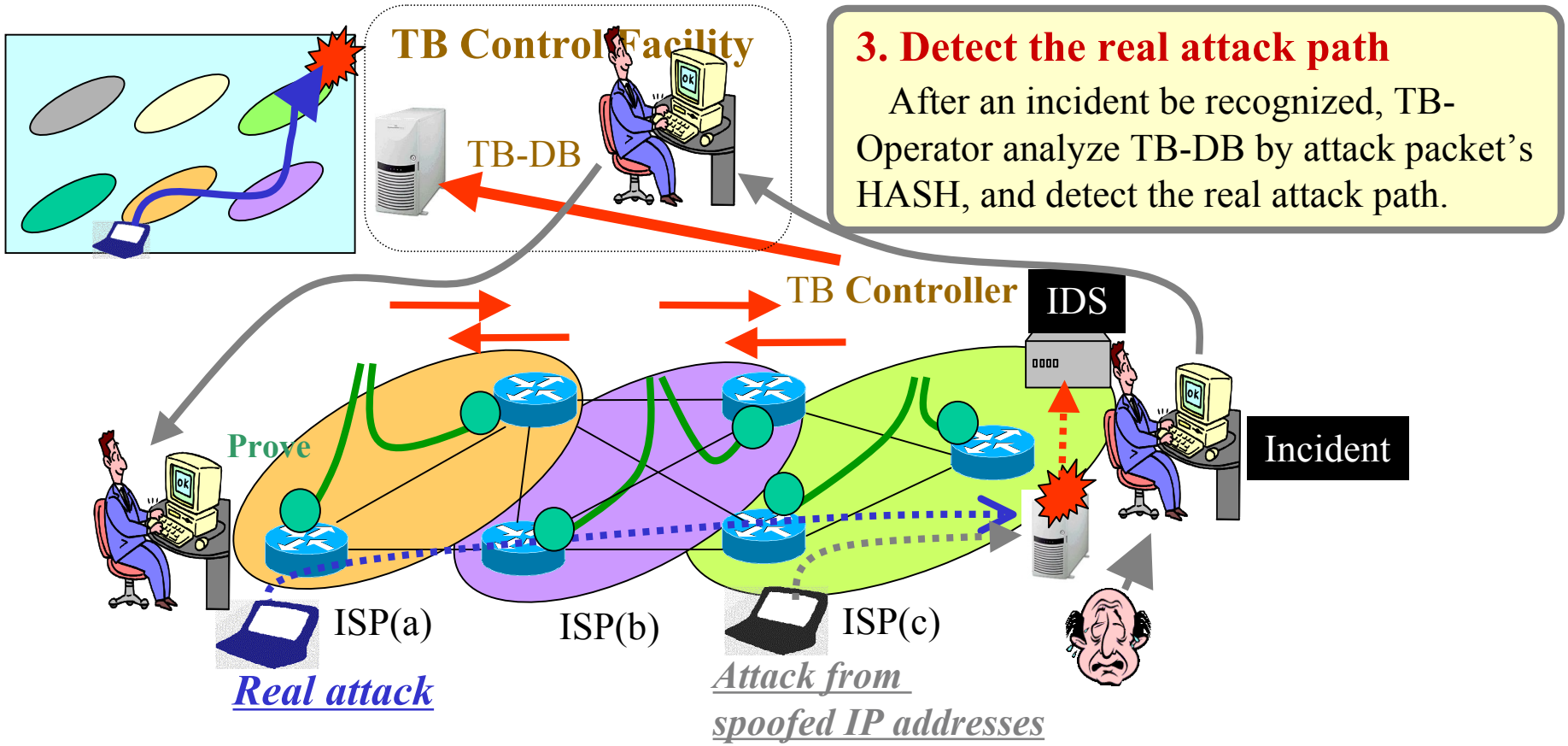


Traceback System outline

JADAC

2. Store suspicious information.

Whenever IDS notify suspicious attacks, TB controller calculates the attack packet's HASH, and automatically recursive analyze its AS map with neighbor AS's TB manager, and store it to TB-DB.



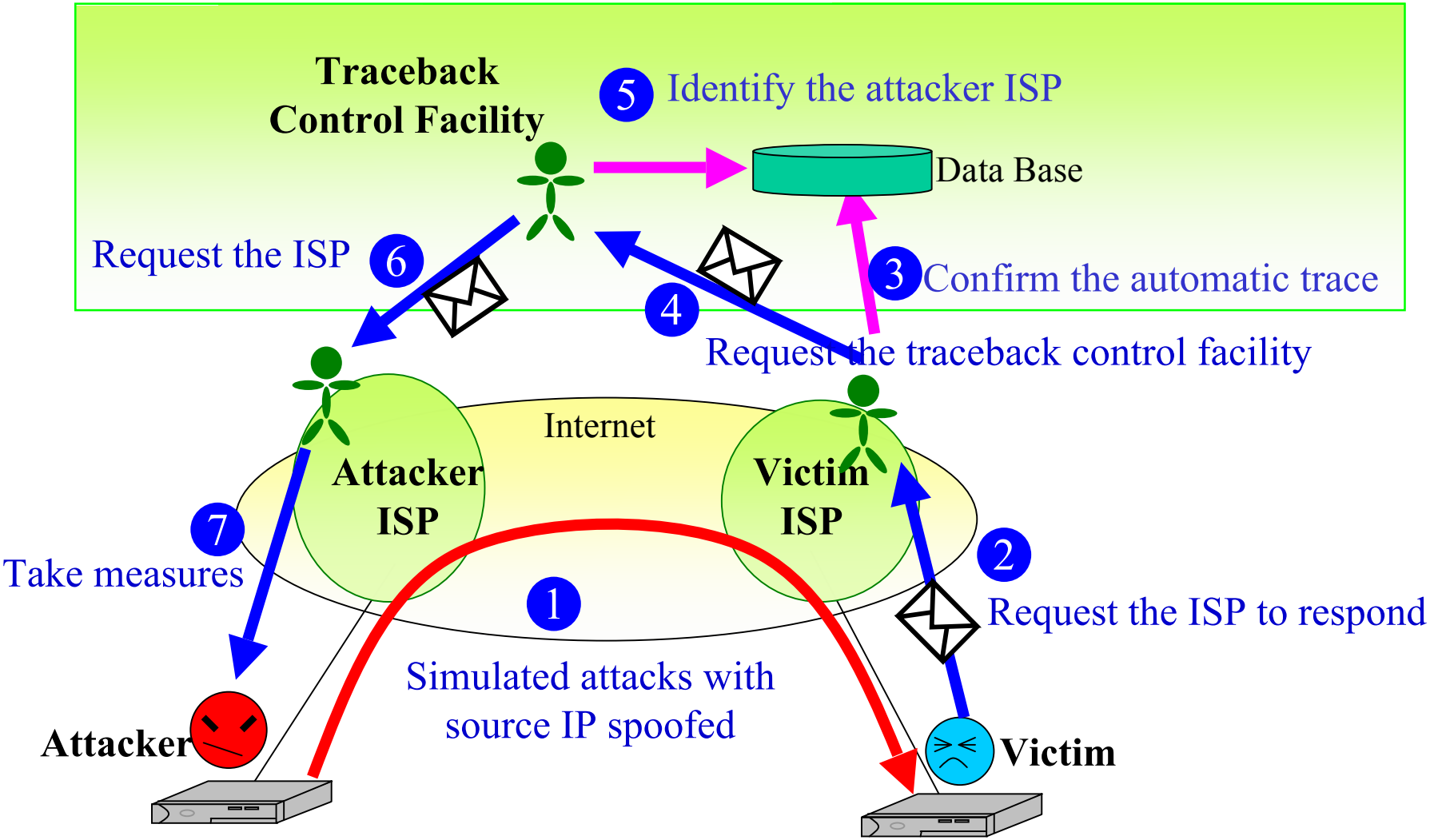
3. Detect the real attack path

After an incident be recognized, TB-Operator analyze TB-DB by attack packet's HASH, and detect the real attack path.

1. Store HASH data temporary.

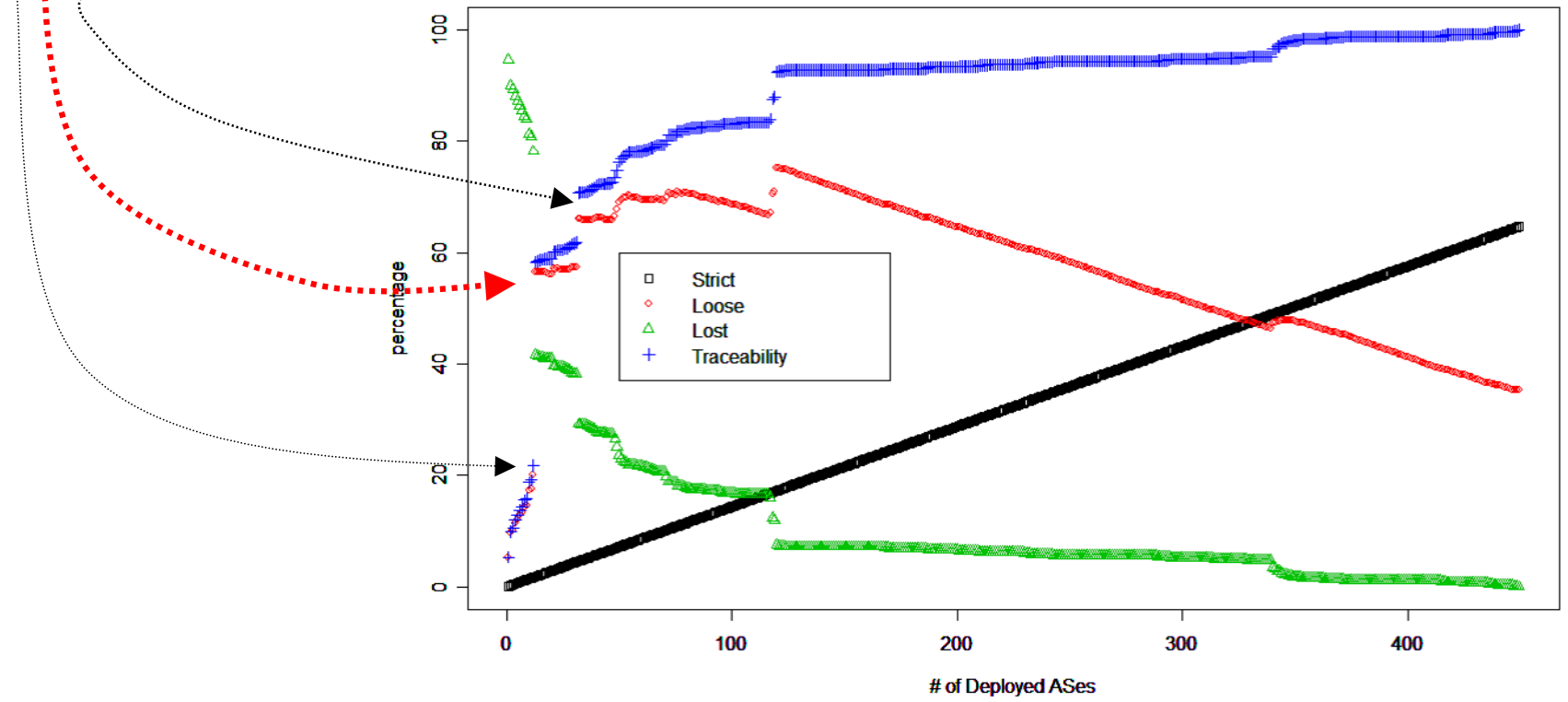
Each probe convert packet to HASH, and store own cache automatically.

A Scenario for the Simulated attack experiments



Evaluation of Equipment Adoption rates and Tracing Success Rates

- Best Deployment Scenario
  - First introduce to small/mid-size ASs rather than starting with larger-scale ASs.
- Result of a simulation with .JP domain model
  - Twelve small-/middle-scale ASs **21.75%**
  - 1st ranked AS **58.35%**
  - Eighteen small-/middle-scale ASs and 2nd ranked AS **70.74%**



Large Scale Demonstration Experiments

JADAC

With Fifteen ISPs and Three research centers

From Apr to Sep in 2009

Good **1. Measurement System Performance**

2. Simulated Attack Outcomes

Good a) DDoS simulated attack

Good b) Multiple simultaneous DDoS simulated attacks

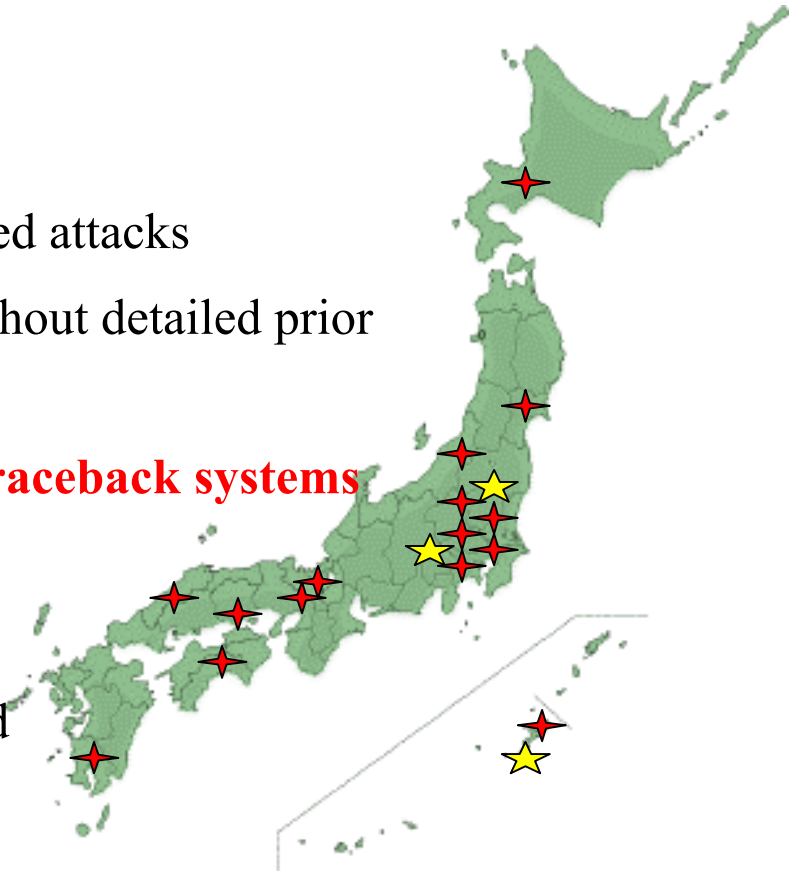
Good c) DDoS simulated attack conducted without detailed prior information

Not good d) DDoS simulated attack **among two traceback systems**

Good e) DDoS simulated attack experiments conducted while system performance was reduced and problems introduced

Good f) DNS reflection simulated attack

Not good **3. Real Attacks**



Measurement of System Performance

- Measured the traceback processing time
  - Pattern one
    - Connected to one another.
    - Request to all ISPs.
    - Less than 1.0 second.
  - Pattern two
    - Connected in series.
    - Request only to the next ISP.
    - Average 3.0 seconds, the worst 4.0 second.

- Most suitable value of hash table refresh time is 4.0 second.

Measurement of System Performance

JADAC

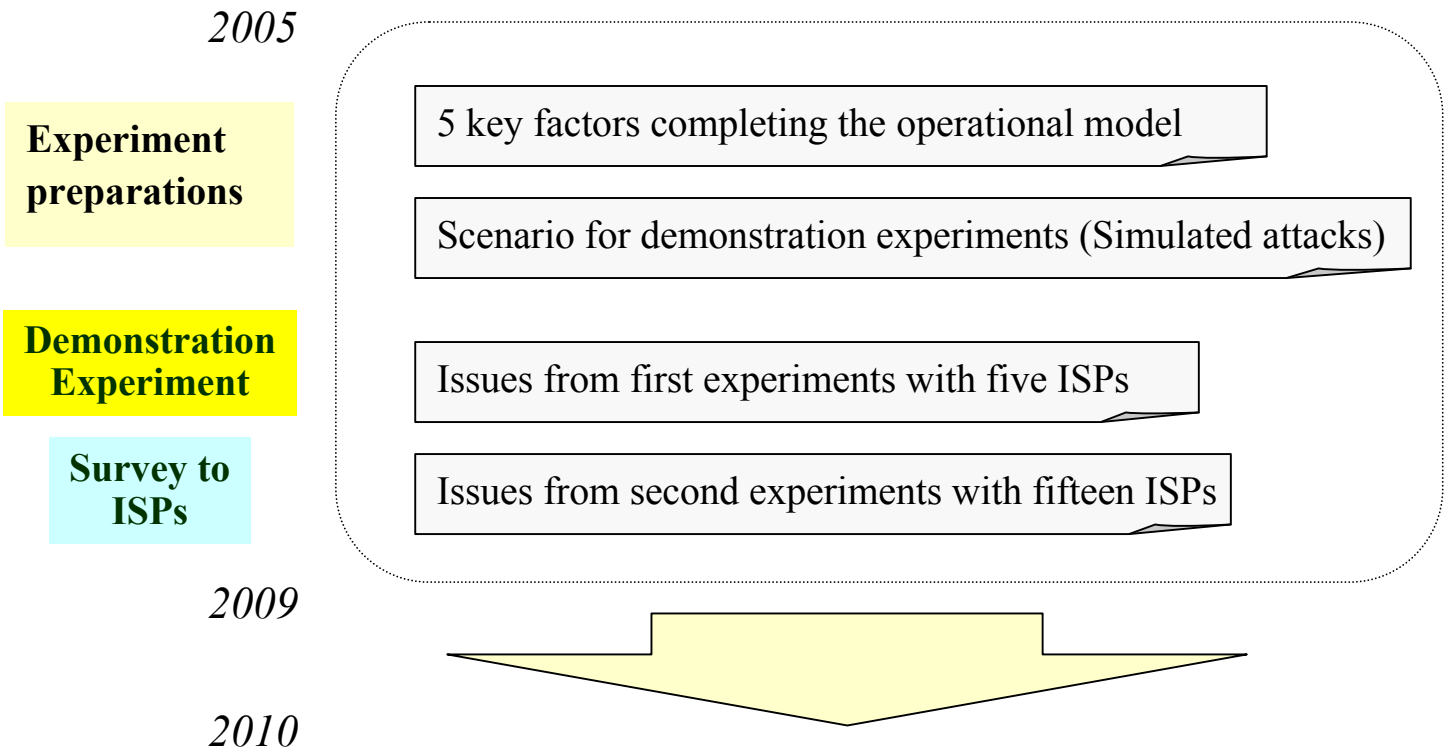
b) False Detection rate of each Probe

Probe	Traffic	Bit	False Detection rate	
			Mesured	Logical
A	445Mbps	26bit	5.78_10^{-6}	3.65_10^{-6}
B	440Mbps		3.46_10^{-6}	3.57_10^{-6}
C	320Mbps		3.07_10^{-6}	1.89_10^{-6}
D	180Mbps		0.40_10^{-6}	0.60_10^{-6}
E	105Mbps		0.31_10^{-6}	0.20_10^{-6}
F	105Mbps		0.25_10^{-6}	0.20_10^{-6}

c) Losing Rate * Reduced 50% by sampling

Probe	Traffic	Type	Hit / Query	Losing rate
_	* 445Mbps	Soft	653 / 2040	0.68
_	440Mbps		1635 / 2040	0.198
_	320Mbps		1799 / 1800	0.001
_	180Mbps		1800 / 1800	0
_	105Mbps		1860 / 1860	0
_	105Mbps		2220 / 2220	0
_	890Mbps	Hard	2040 / 2040	0

Future issues to widespread adoption



Future issues to be addressed to enable widespread adoption

1. Traceback operational processes should be designed to adapt to the real world.
2. Traceback success rates should be more than 50%.
3. Hash data should be calculated by standard ISP network equipment.
4. Traceback software and operations must be highly secure.

We need next traceback project to resolve and validate these issues.

Any Questions ?

- Please send me any questions by e-mail.

secretariat@telecom-isac.jp