"Research and Development on IP packet traceback technology"
National Institute of Information and Communications Technology(NICT) sponsored

ISP field test plan of IP packet traceback prior experiments in 2008

- Summary
- Network Environment
- Management system
- Legal issues
- Experiment summary

Ken. Wakasa

Summary： Purpose

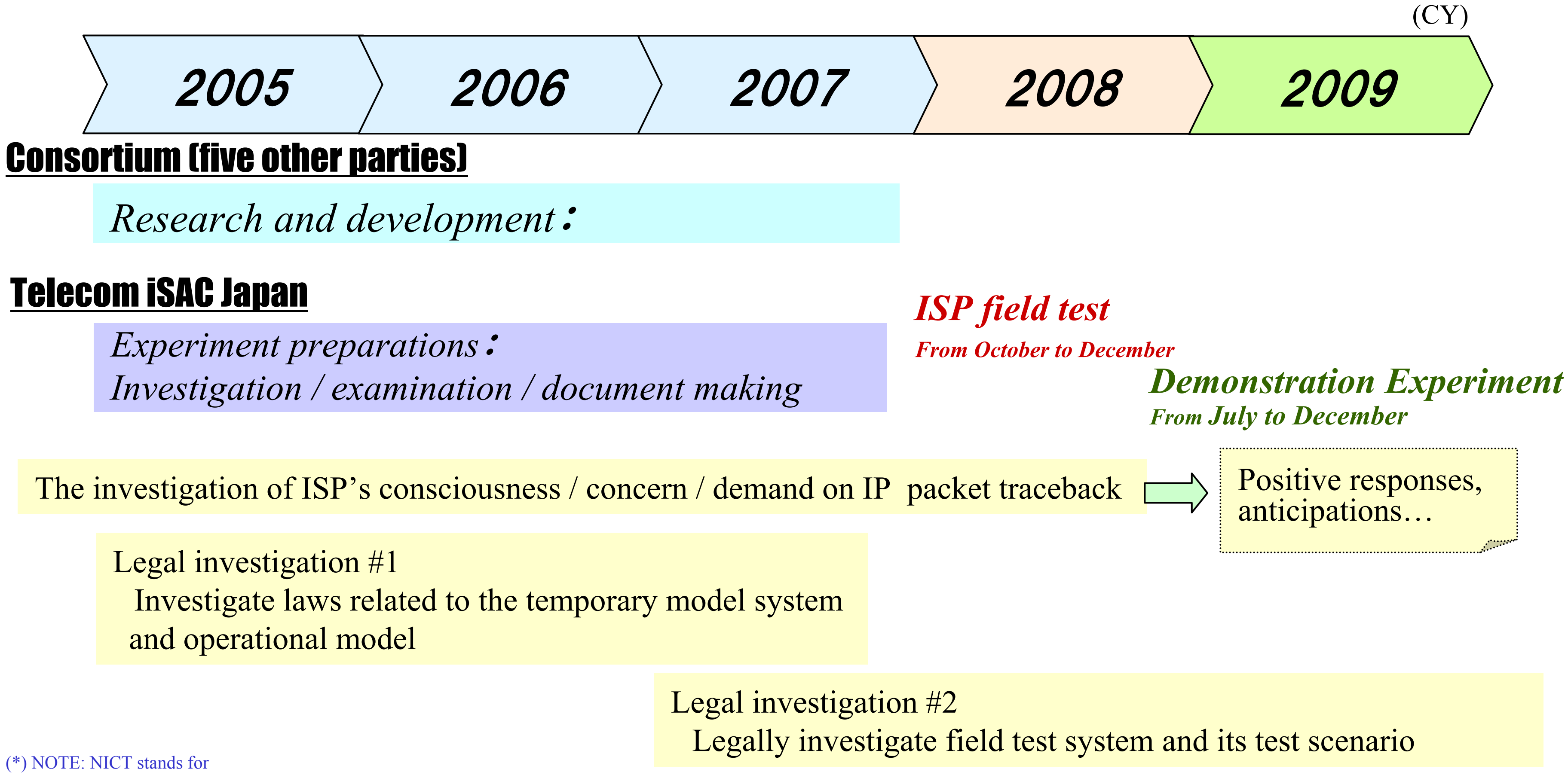
- The preparations for demonstration experiment in 2009
  - Collect information necessary for demonstration experiment
    - Data, problems, know-how to be collected with a long-time consecutive operation
    - Set up real machine at ISP environment
    - Data, problems, know-how to be collected at ISP field trial
  - Investigate risks from the information collected and formulate measures to realize the demonstration experiment.
    - Review outstanding issues
    - Define any function to be added or corrected

Summary： Schedule

IP packet traceback R&D project

* A research project offered by NICT(*), started 2005 by the Consortium of six parties

* Goal of the project is Demonstration Experiment of IP packet traceback



(CY)

2005

2006

2007

2008

2009

Consortium (five other parties)

Research and development：

Telecom iSAC Japan

Experiment preparations：
Investigation / examination / document making

ISP field test
From October to December

Demonstration Experiment
From July to December

The investigation of ISP’s consciousness / concern / demand on IP packet traceback

Positive responses,
anticipations…

Legal investigation #1
Investigate laws related to the temporary model system and operational model

Legal investigation #2
Legally investigate field test system and its test scenario

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

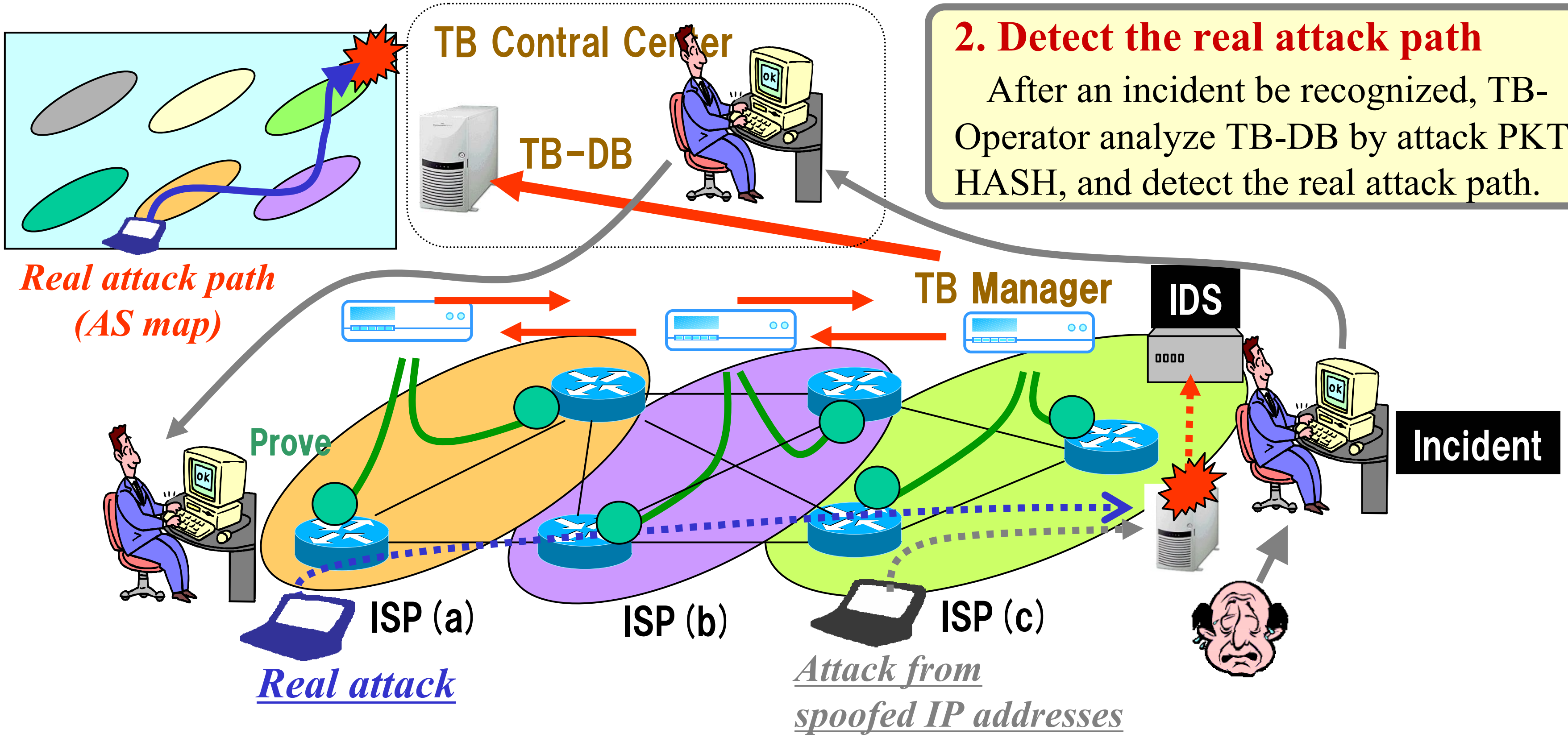
Summery:Outline of Traceback system

1. Store suspicious information.

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

2. Detect the real attack path

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



0. Store HASH data temporary.

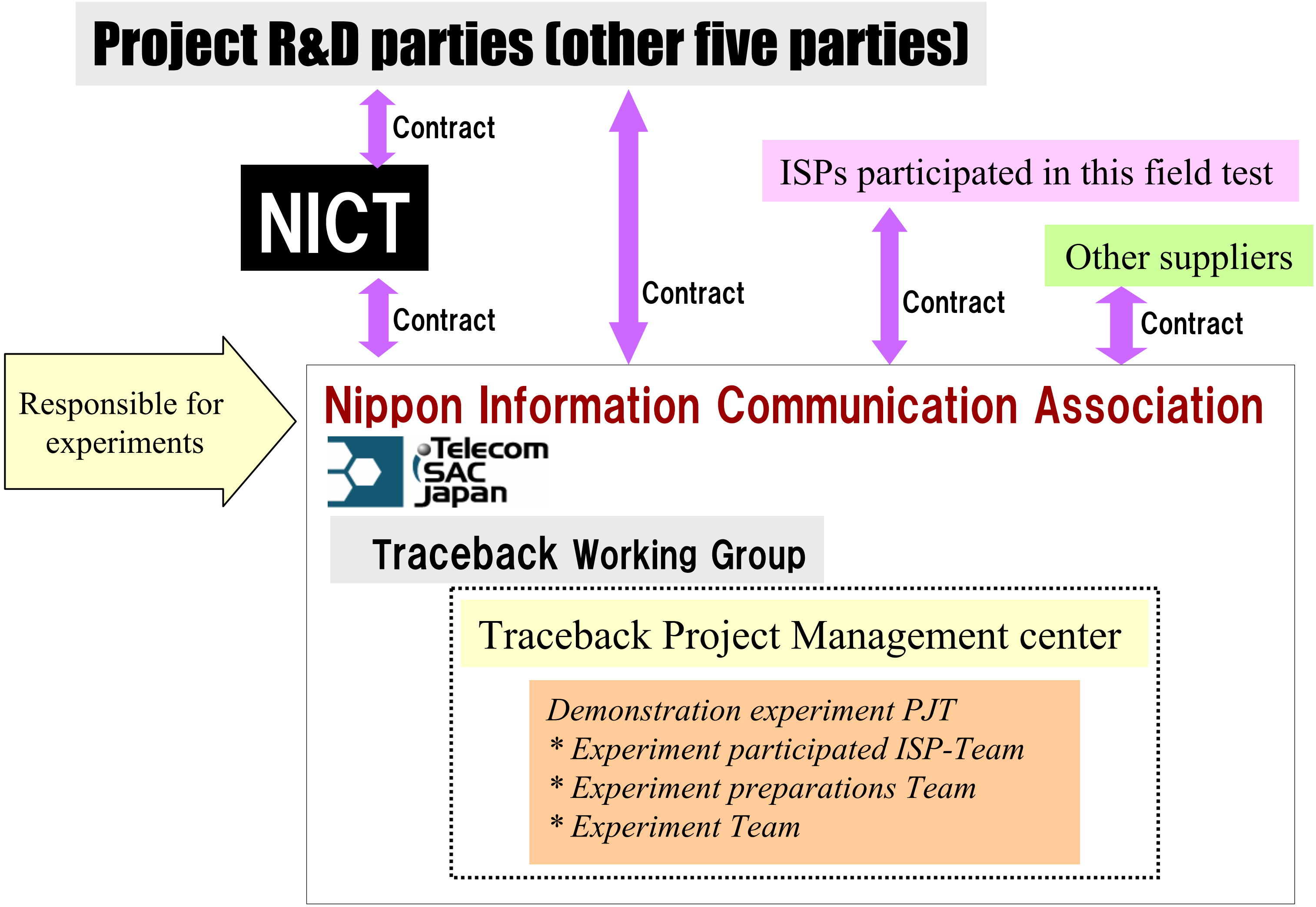
Each probe convert PKT to HASH, and store own cache automatically.

Summary： Prior Experiments

- Closed network test
  - Use machines at Data Center (closed network environment)
  - Collect data with consecutive long-term operation
  - Verify operations and functions, not available at ISP field test because of the legal issues

- ISP field test
  - Integrating machines at Data Center and ISP site networking “The Internet”
  - Verify primitive act and operations

Summary： Project formation


Project R&D parties (other five parties)

Contract

NICT

Contract

Contract

ISPs participated in this field test

Contract

Other suppliers

Contract

Responsible for experiments

Nippon Information Communication Association

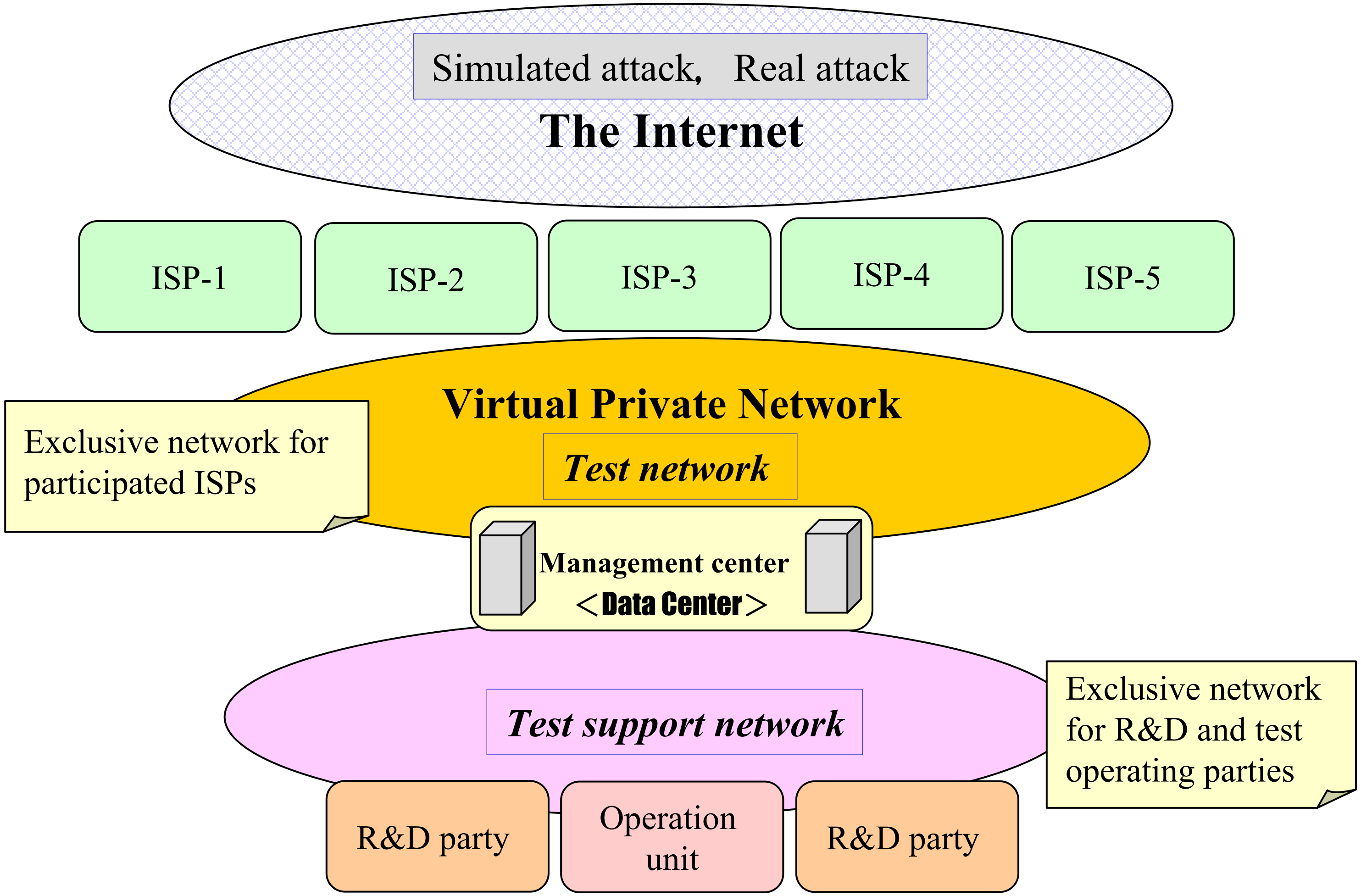
Telecom ISAC Japan

Traceback Working Group

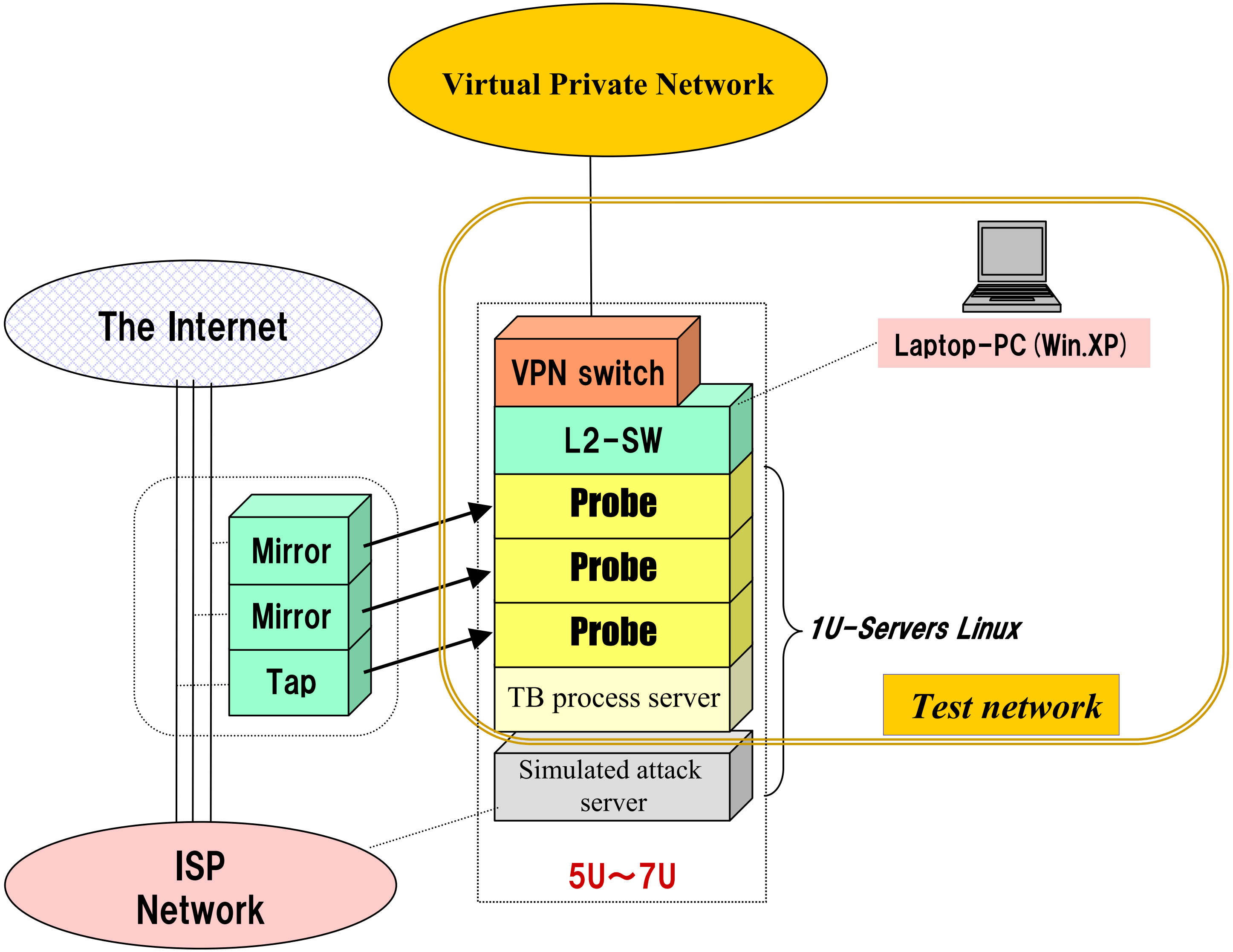
Traceback Project Management center

Demonstration experiment PJT
** Experiment participated ISP-Team*
** Experiment preparations Team*
** Experiment Team*

Network : overview



Network： ISP network configuration



Management system： Documents

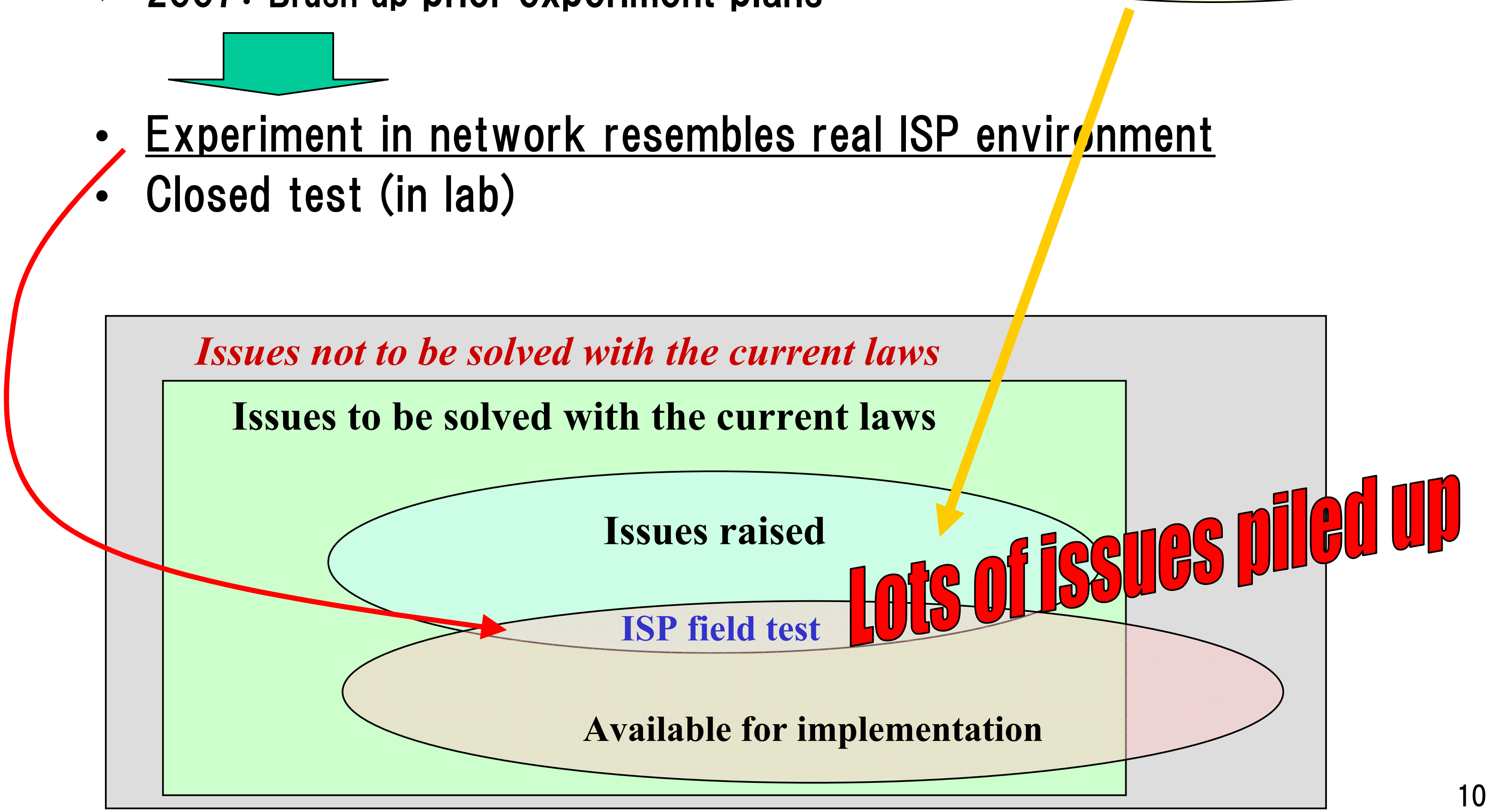
- Operation policy
- Operation basic regulations
  - Safety measures rule, Information system management / instruction manual, media handling manuals
  - TB Management center operative unit criteria of selection (test facilities/operation)
- Operation procedure book
  - Setting/removal manuals, Operation manual, Simulation test manual, Incident test manual
- Testing unit organizing regulations
  - Working Group/TB Management center administration rule, preparations / implementation / Participated ISP-team administration rule,
- Contract model
- Test plan (for prior experiment / demonstration experiment)
  - Scenario
- Risk analysis
  - Questionnaires, list of information system, management, countermeasures
- Criteria of selection on ISPs (field test participants)

Legal issues : ISP field test scope

- Prepare for three years and confirm it in a permissible range.
  - ✓ 2005: Investigation on laws - domestic
  - ✓ 2006: Investigation on laws - global
  - ✓ 2007: Brush up prior experiment plans

Investigation on laws related to the temporary model system and operational model

- Experiment in network resembles real ISP environment
- Closed test (in lab)


Issues not to be solved with the current laws
Issues to be solved with the current laws
Issues raised
ISP field test
Lots of issues piled up
Available for implementation

ISP field test - outline -

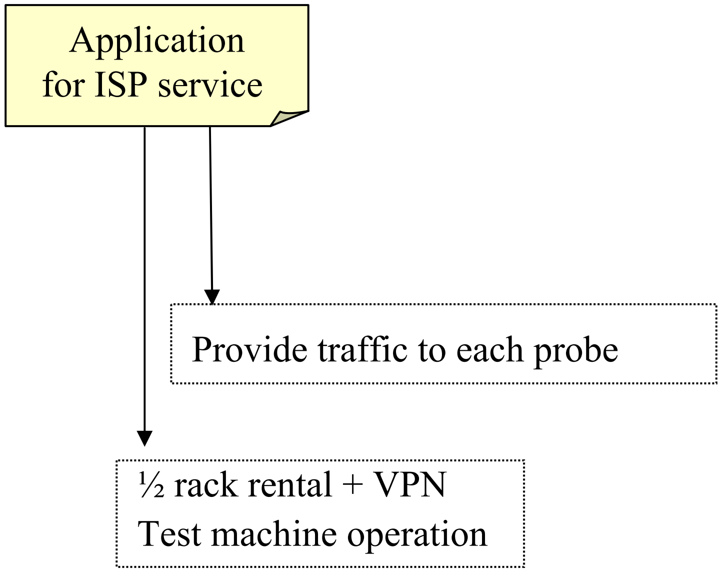
1. Setting
2. Verification on system
   - Automatic operation　simulated attack / real attack
3. Verification on operative plans for attacks
   - Simulated attack
     - Verification on operation against attacks along the scenario
     - Verification on operation against attacks without the scenario
   - Real attack (passive)
     - Verification on operation against attacks along the operation manual
     - Verification on operation against attacks beyond (above assumption) the operation manual
4. Removal

1． Setting

1） Pre-adjustment, Contract conclusion

Participation contract for field test

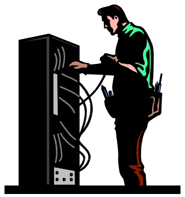
ISP field test plan



Application for ISP service

Provide traffic to each probe

½ rack rental + VPN
Test machine operation



2） System integration

ISP：Probe access
Trace Back：Machine setting,
Operational check

Test machine List

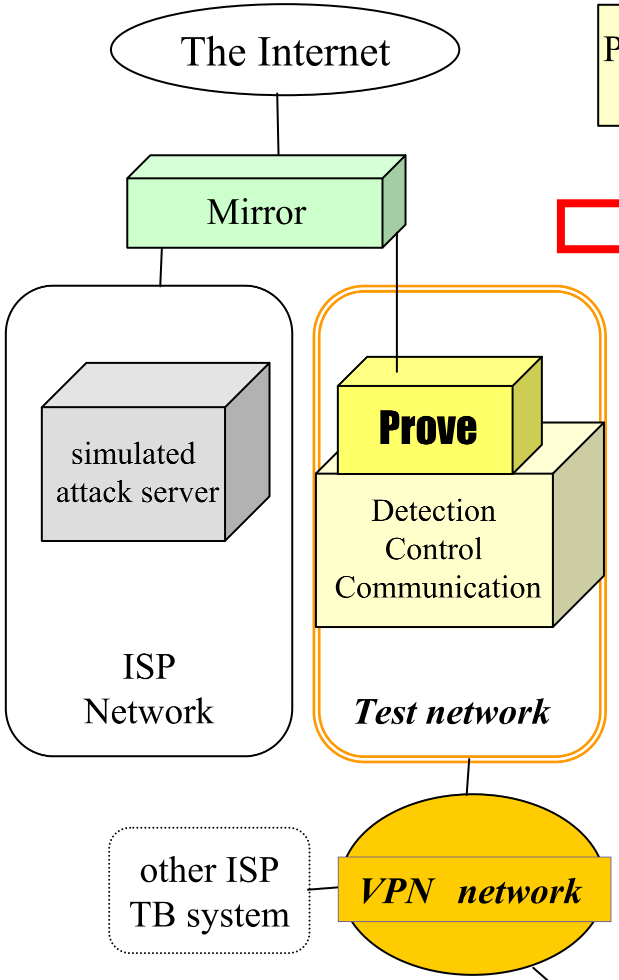
3） Operative explanation

From TB consortium to ISP
From ISP to TB consortium

Daily report

Report for incidents

2． Verification on system （Automatic operation）



Participation contract for field test

1）Attack detection

Simulated attack between simulated attack servers

Not decided :

Specific attack to the simulated attack server .

Specific attack to the specific server

2）Attack source tracing

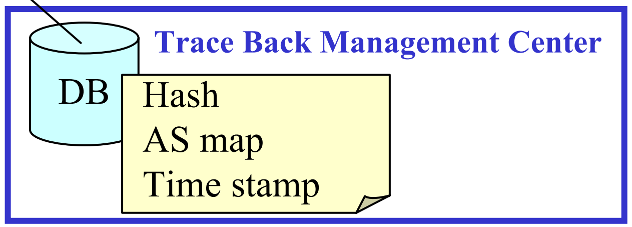
Ask attack source to other TB system referring hash value of attack IP packet ID.

Record source attack AS map by DB.

3）Operation verification

ISP：Confirm and send test logs

TB consortium：Verify test logs



3． Simulated attack scenario

- Leader： TB management center
- Roles
  - Assailant：Sender of simulated attack （TB management center）
  - Victim：Owner of the server that simulated attack took place （TB management center）
  - Damaged ISP：ISP which has the server that simulated attack took place
  - TB management center：Administration group of TB system.
  - Attack ISP：ISP which has the server that sends simulated attack
  - Pass-through ISP：ISP that simulated attack passes through (no role)
  - Participated ISP：All ISP participants on this field test
- Story
  - Scenario to continuous simulated attacks consecutive 2 to 3 hours.
  - TB management center prepares Server for attack, reputation trust Server and handles simulated attack enforcement, the collection of simulated attack packets.
  - In response to request from victim, damaged ISP / TB management center / attack ISP cope and handle the incident.

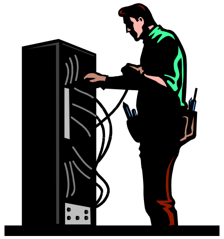
４．Removal

１）Conclusion (verification)

Third party interviews ISPs that the field test is carried out adequately

Daily report

Report for incidents



２）Data elimination

Eliminate all data created at the test

３）Removal of machines

Test machine list

More difficult issues piled up …

- **Operative issue**
  - The operative management that it is easy to introduce, Security of the reliability.
  - Cost, cost-benefit performance
- **Technical issue**
  - High speed, high-precision tracing
  - New technology besides packet capture, tap, mirror?
  - How the application traceback will work out……
  - Who confirms an incident, who starts traceback?
  - Hash retention time?
- **Legal issue**
  - Lots of issues piled up…