T6-3

Creating and Operating a CSIRT (Incident Handling Team) within the Enterprise.

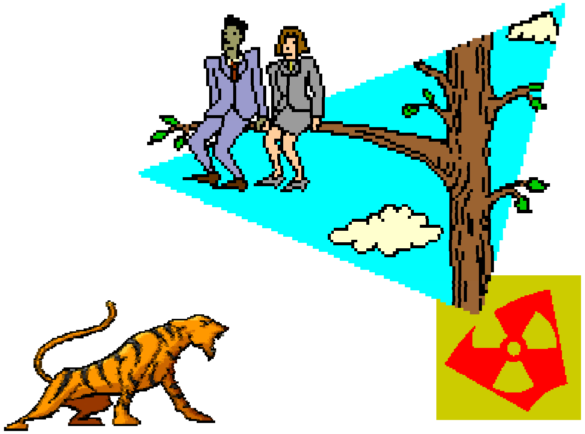
NISHIMOTO Itsuro
JSOC Chief Director
Little eArth Corporation Co., Ltd. (LAC)
itsuro@lac.co.jp
http://www.lac.co.jp/security/

APRICOT
2005 KYOTO

Contents

1. Back ground
2. CSIRT (Incident Handling Team) within the Enterprise
3. PSOC (Private Security Operation Center)
4. Security Management
5. Security Maintenance
6. Security Monitoring
7. Incident Response
8. Practice Leval

1. Back ground



1. Back ground

Rapid development of information technology (IT)

- Progress of computer & network technology
  - ⇒ the high speed, large capacity circuit (ADSL, CATV connection)
  - ⇒ High speed processing ability, large capacity
- hard disk, memory
  - ⇒ Decline of a/the price
- Change of an/the application structure
  - ⇒ Twenty-four hours constantly connection
- Systematization, network -ization of the social life base

New life and communication style

Rapid formation/settlement/growth of the new society

1. Back ground

The situation of critical incidents number of cases in JSOC （The urgent incident in security surveillance of JSOC）

Year 2003: 1 occurrence/m/org. (65%: intranet)
Year 2004: 3～4 occurrences/m/org. (90%: intranet)

The incident number of cases in intranet relatively increase

Client who considers intranet surveillance has increased

Trend of the threat in JSOC

1．Internet

1）Exploit、、 ↘

2）Brute force attack ↗

3）DoS ↗

Spam、click＆reload（Program）、syn flood 、、

4）Web application ↗

2．Intranet

1）Virus/Worm ↗

2）BOT ↗

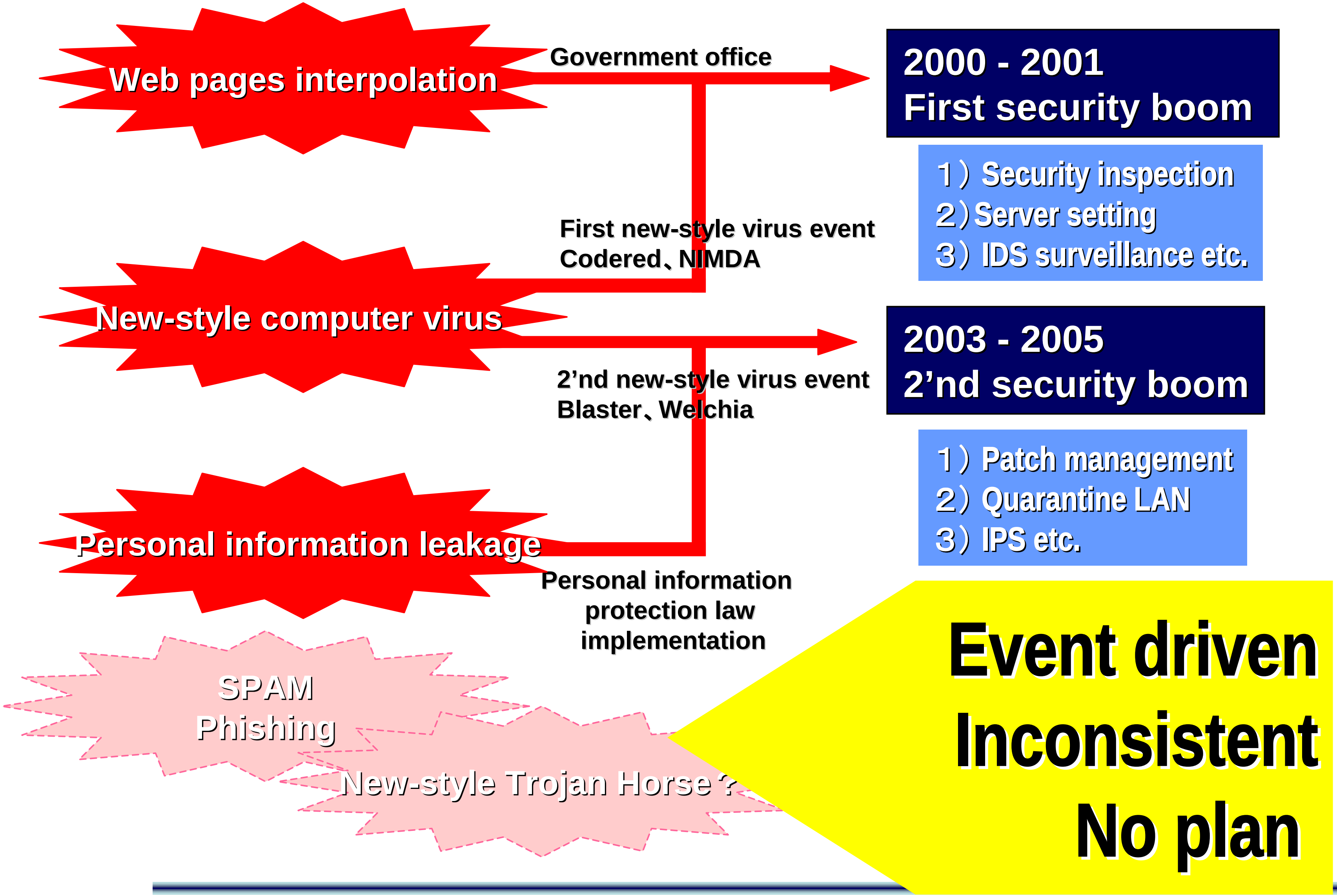
3）P2P/Tunneling ↗

4）exploit →

5）Abuse of Right ↗

1. Back ground

■Movement in the past in case of Japan



Web pages interpolation

Government office

New-style computer virus

First new-style virus event
Codered、NIMDA

2’nd new-style virus event
Blaster、Welchia

Personal information leakage

Personal information protection law implementation

SPAM
Phishing

New-style Trojan Horse？

2000 - 2001
First security boom

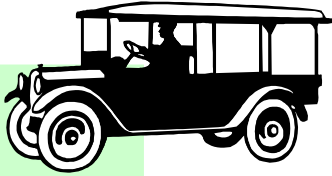
1）Security inspection
2）Server setting
3）IDS surveillance etc.

2003 - 2005
2’nd security boom

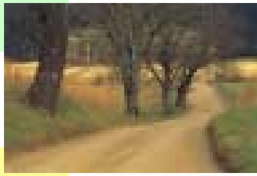
1）Patch management
2）Quarantine LAN
3）IPS etc.

Event driven
Inconsistent
No plan

1. Back ground



IT that is said with revolutionary over Motorization

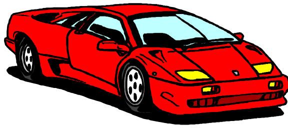


How much is the infrastructure arranged?
IT society vs Automobile society

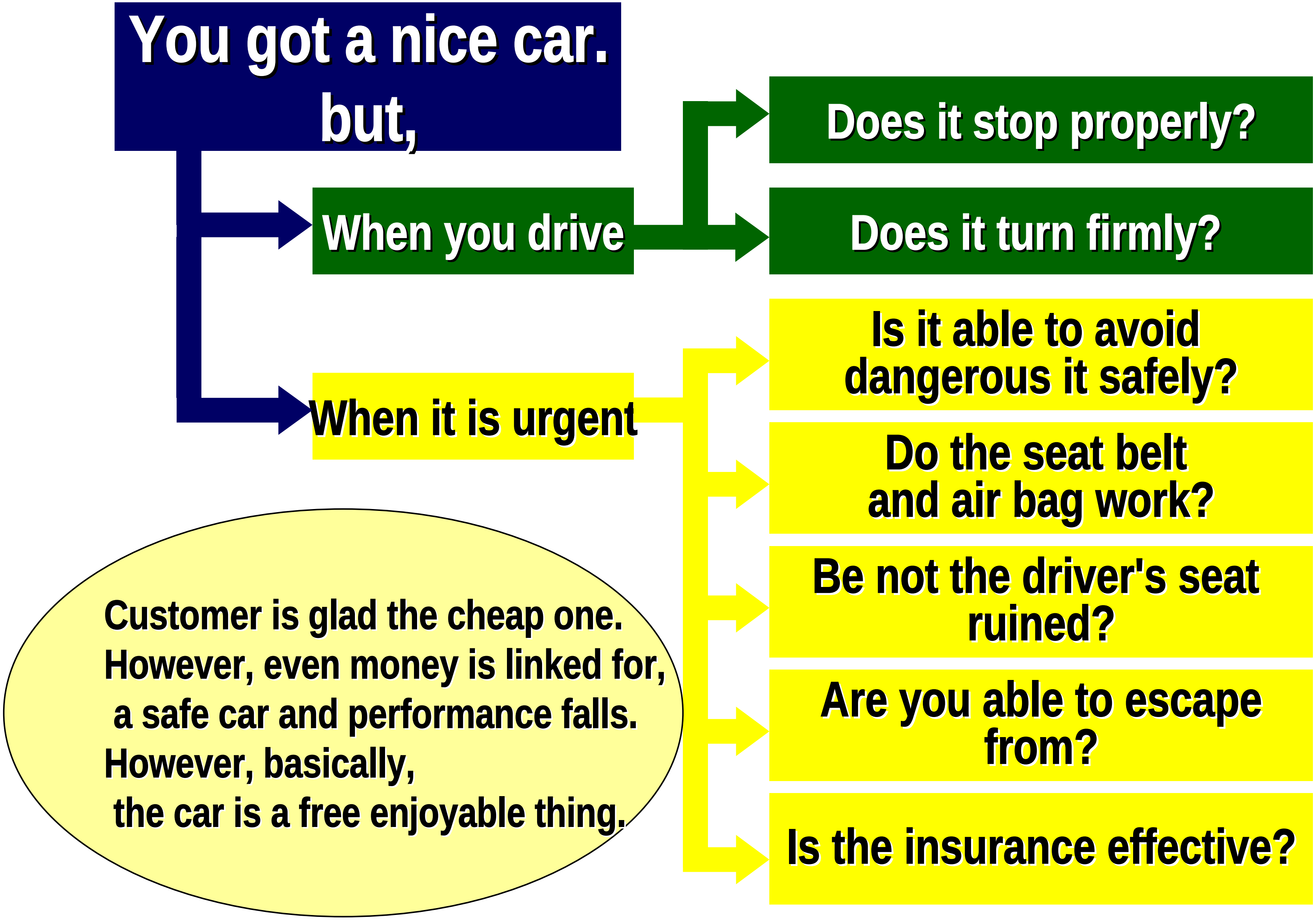
Situation

Highspeed/high function of PC	Engine became highly efficient
Penetration of broadband	Highway/road was arranged
Fusion of network and system	Generalization of automobile

Automobile came up to here in this 100 years



1. Back ground



You got a nice car.
but,

When you drive

Does it stop properly?

Does it turn firmly?

When it is urgent

Is it able to avoid dangerous it safely?

Do the seat belt and air bag work?

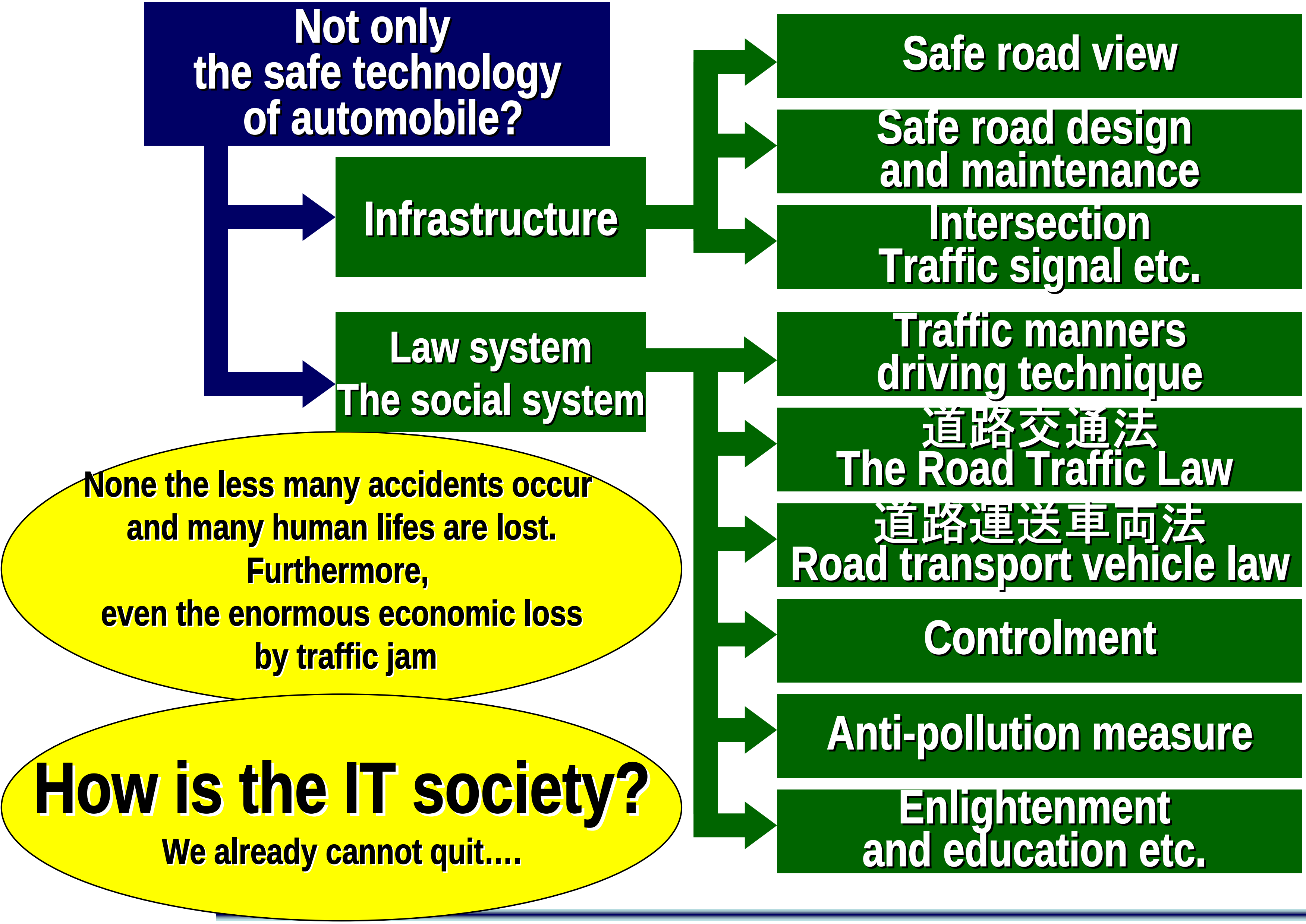
Be not the driver's seat ruined?

Are you able to escape from?

Is the insurance effective?

Customer is glad the cheap one.
However, even money is linked for,
a safe car and performance falls.
However, basically,
the car is a free enjoyable thing.

1. Back ground



Not only
the safe technology
of automobile?

Infrastructure

Safe road view

Safe road design
and maintenance

Intersection
Traffic signal etc.

Law system
The social system

Traffic manners
driving technique

道路交通法
The Road Traffic Law

道路運送車両法
Road transport vehicle law

Controlment

Anti-pollution measure

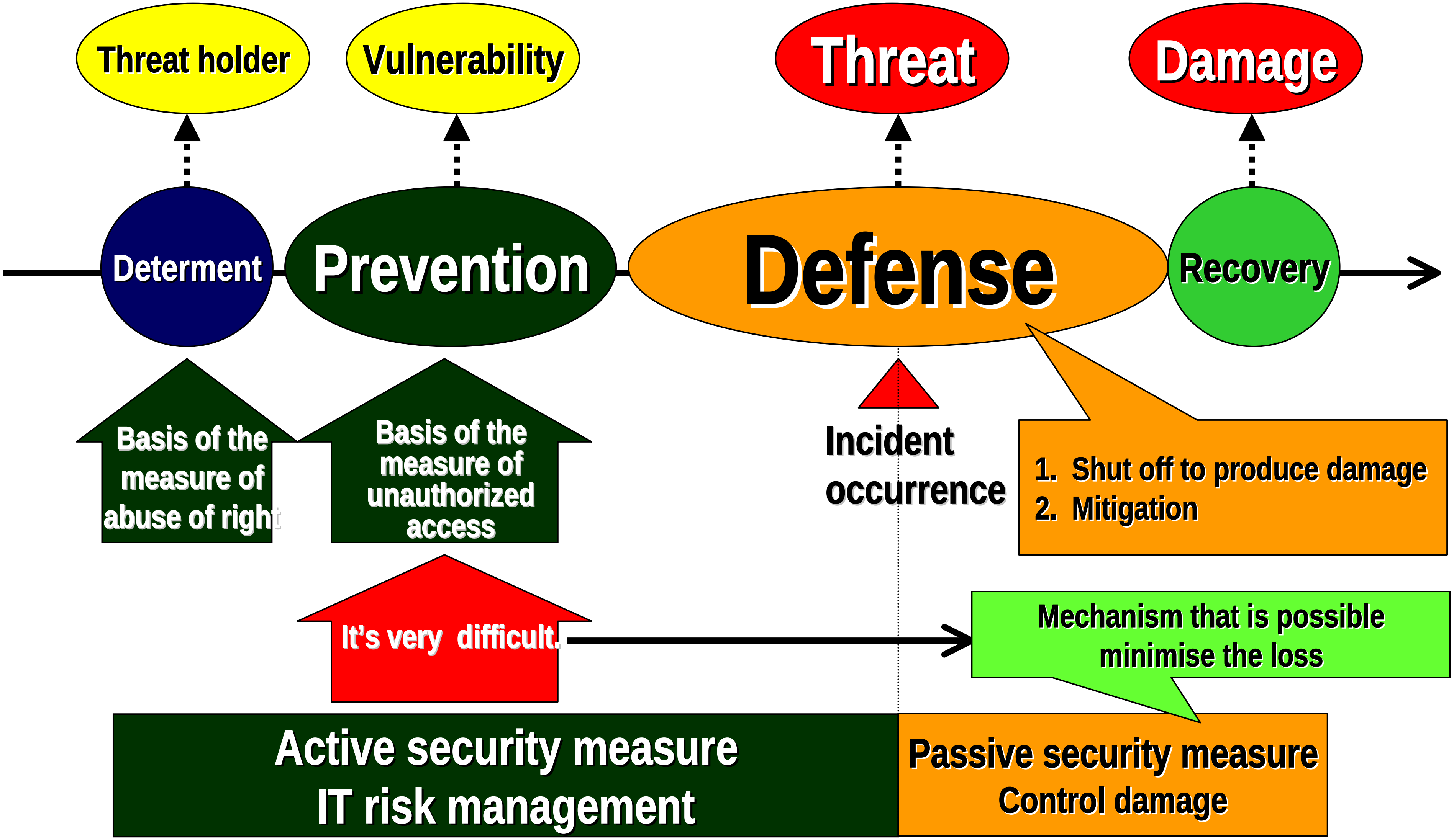
Enlightenment
and education etc.

None the less many accidents occur
and many human lifes are lost.
Furthermore,
even the enormous economic loss
by traffic jam

How is the IT society?

We already cannot quit....

1. Back ground



Threat holder

Vulnerability

Threat

Damage

Determent

Prevention

Defense

Recovery

Basis of the measure of abuse of right

Basis of the measure of unauthorized access

Incident occurrence

1. Shut off to produce damage
2. Mitigation

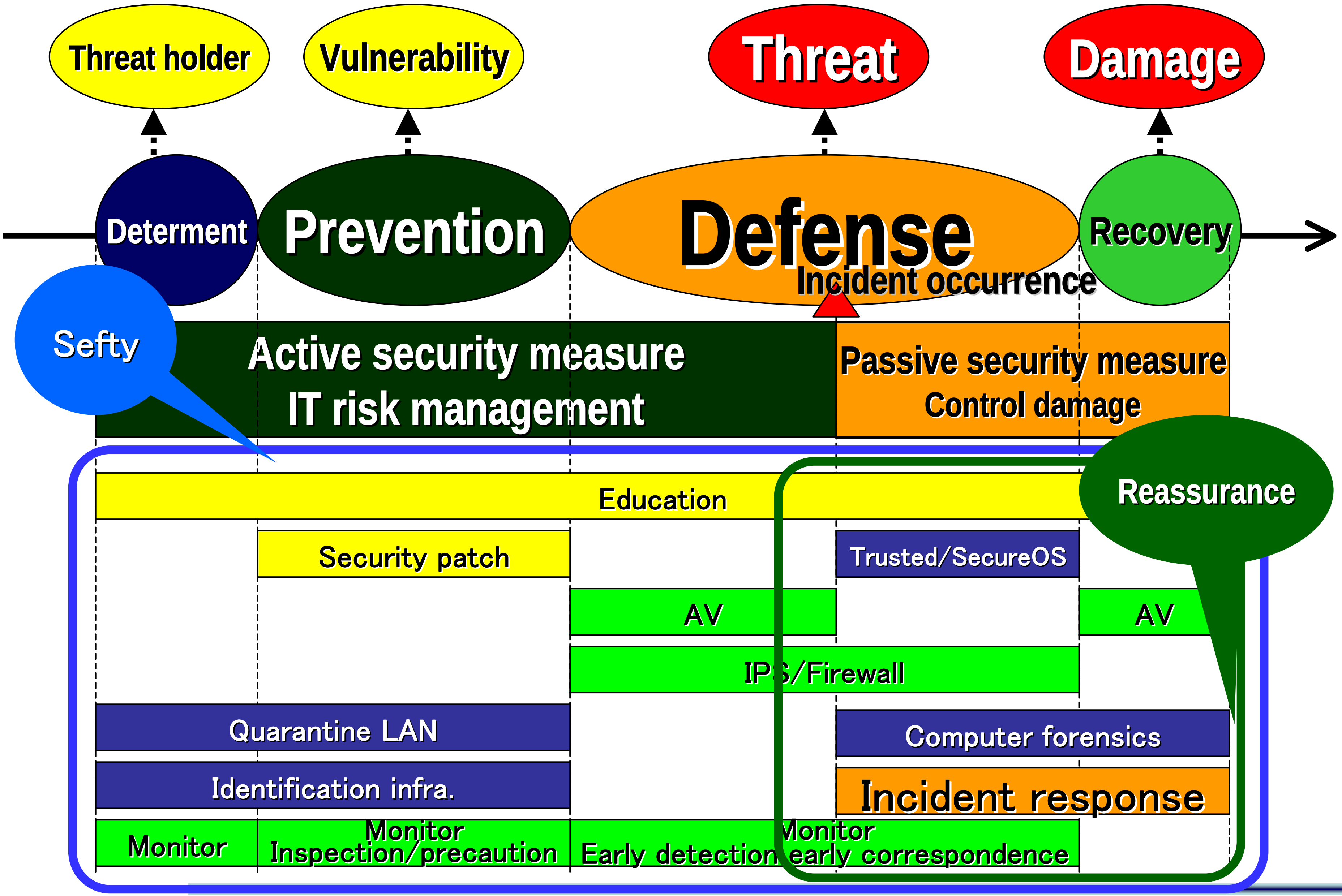
It's very difficult.

Mechanism that is possible minimise the loss

Active security measure
IT risk management

Passive security measure
Control damage

1. Back ground



Threat holder

Vulnerability

Threat

Damage

Determent

Prevention

Defense

Recovery

Incident occurrence

Sefty

Active security measure
IT risk management

Passive security measure
Control damage

Reassurance

Education

Security patch

Trusted/SecureOS

AV

AV

IPS/Firewall

Quarantine LAN

Computer forensics

Identification infra.

Incident response

Monitor

Monitor
Inspection/precaution

Monitor
Early detection, early correspondence

1. Back ground

Reference

NPO-JNSA
http://www.jnsa.org/english/e_index.html
Security incidents Survey Report
http://www.jnsa.org/english/e_active2003_1.html

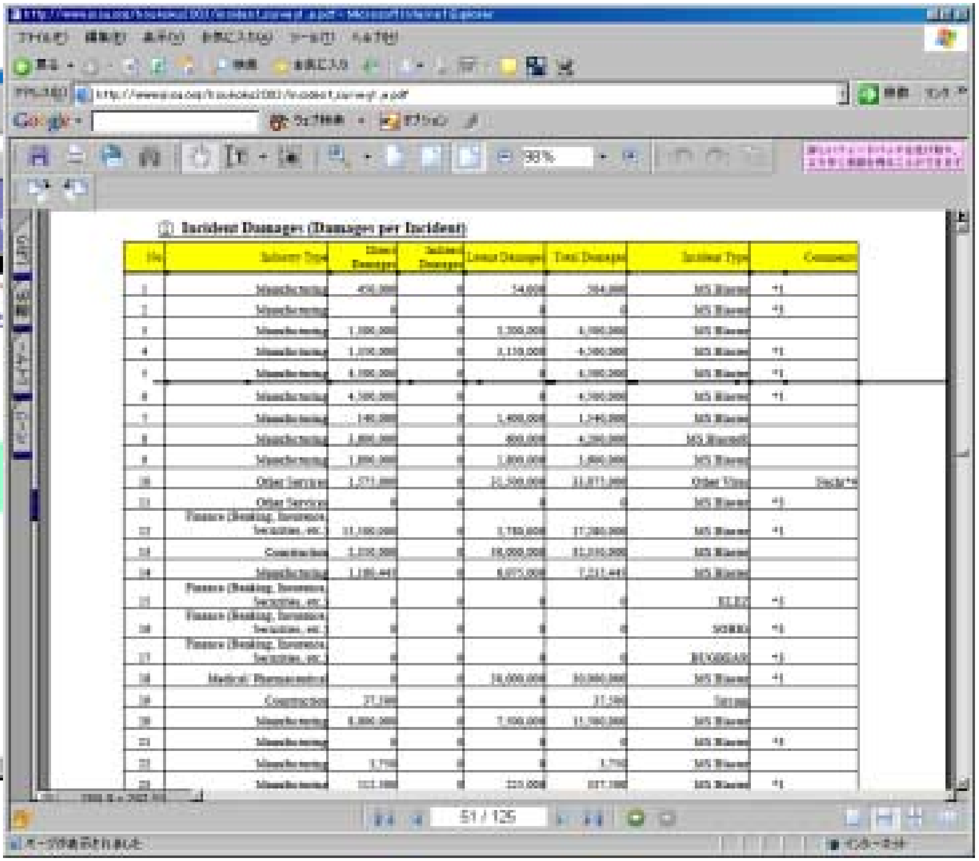
JNSA

NPO Japan Network Security Association

Seisaku Committee

[Security Incidents Survey WG (Security Incidents Survey Project)]

1 The Activity Purpose



① Incident Damages (Damages per Incident)

51 / 125

2. CSIRT (Incident Handling Team) within the Enterprise

2. CSIRT (Incident Handling Team) within the Enterprise

1）Positioning of incident handling

Security measure			Automatic	Man	System
Determent	Monitoring Security policy / penalty			◎	◎
Prevention	Vulnerability management Inspection/precaution		◎	◎	◎
Defense-1	Shut off to produce damage		◎	○	
Defense-2	A	Mitigation(Automatic)	◎		
	B	Incident Handling		◎	○

2）Every day of the incident handling team?

As for the incident handling team an incident takes an active part at the time of occurrence.

（1）Every day enforcement of training in preparation for incident occurrence.

（2）Security operation, so called

⇒ Incident handling is one of security operation.

⇒ Consideration of SOC within the organization. (Private SOC)

3. PSOC (Private Security Operation Center)

3. PSOC(Private Security Operation Center)

1）Purpose of PSOC

Case 1

To improve the IT utilization technology (the IT literacy) of the employee and raise enterprise power

Case 2

Because thorough safe control is demanded

Case 3

To publicize externally

etc.

2）Pattern of PSOC

(1) Operation method

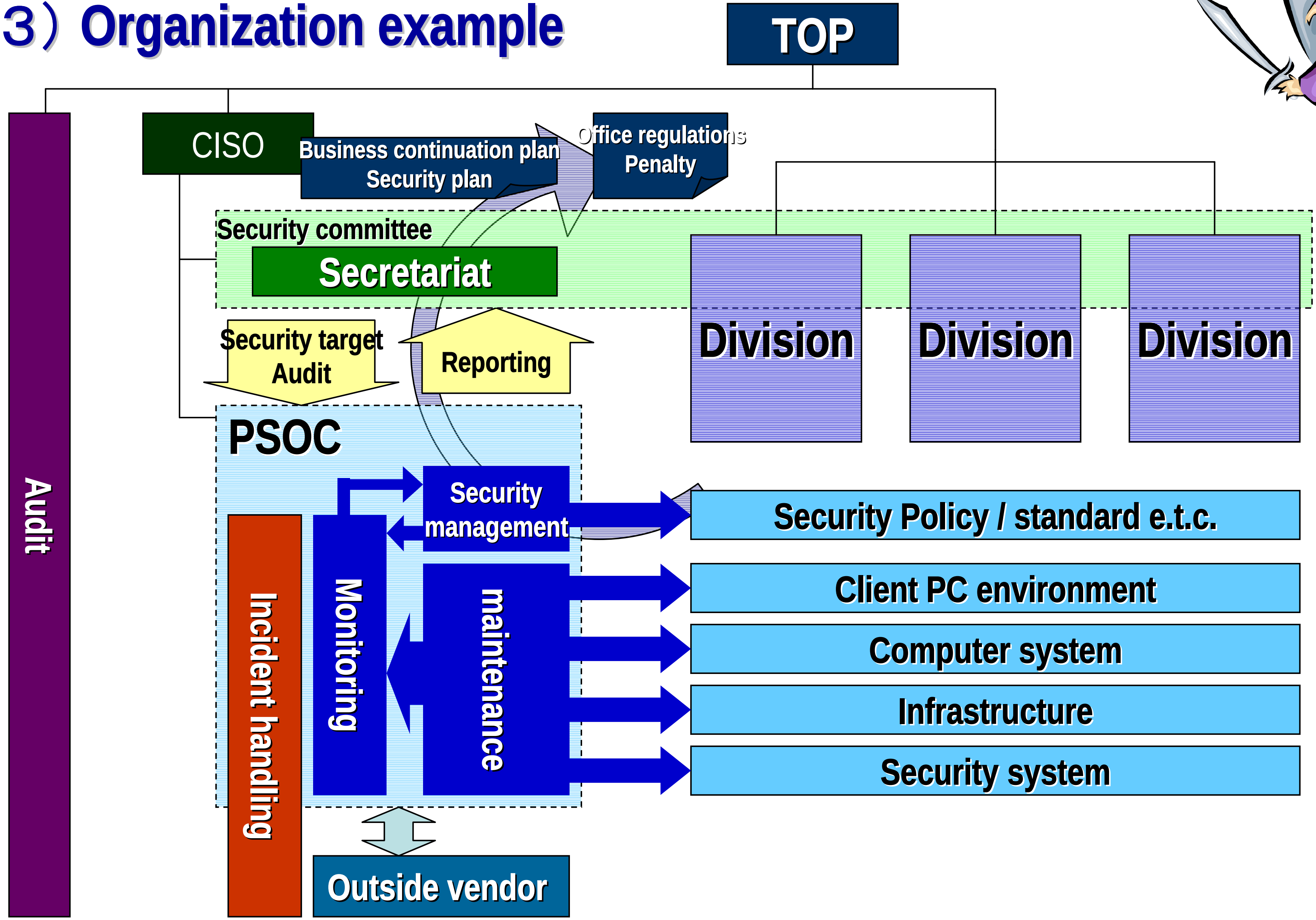
1) Management and inside interfacing, with the self, others are out sauce
2) Almost, with the self, special field are out sauce
3) All, with the self

(2) Scope

1) Company inside
2) Company group

3. PSOC(Private Security Operation Center)

3）Organization example



3. PSOC(Private Security Operation Center)

4) Thought of PSOC function division

(1) Lawmaking

→ Security committee

→ Operation : PSOC

To be able to defend without fail

(2) Administration

→ Each division

→ Operation : PSOC

To defend without fail

(3) Justice & investigation(Police)

→ Legal department/Personnel affairs division

→ Operation : PSOC

Action that discerned target

4. Security management

4. Security management

1）PSOC settlement

The demand and the inspection from the security committee are accepted on behalf of PSOC. Also, Reporting etc.

It is also possible to concurrently hold the post of the security committee secretariat.

4. Security management

2）Incident management

(1) Breakdown to the enforcement policy from the business demand, security demand (the goal)

(2) Vulnerability/threat/besides with the information collection and own threat analysis and also measure plan of event etc.

(3) Feed back from security monitoring
Unauthorized access/ security policy violations/ suspicious access and also neglect of vulnerability e.t.c.

(4) Discovery and analysis of the standard and the procedure that they are not able to apply

⇒ Preparation/revision of the standard and the procedure
Completeness/education/training enforcement such as the policy.
A necessary security function plan.
(Determent/Prevention/Defense/Detection/Recovery).
Maintenance of an appropriate precaution level.

4. Security management

3）Security policy standard/procedure control

(1) Although the procedure is a basis to set in each division operation and maintenance (the work flow & record such as a application) in a bundle control rational by PSOC.

(2) Operation and maintenance of the policy

1) Policy document revision and common knowledge completeness and record.

2) Rationalization and record of policy operation. Usually gearing work flow (common knowledge completeness and approval/application)

3) Education and training and record

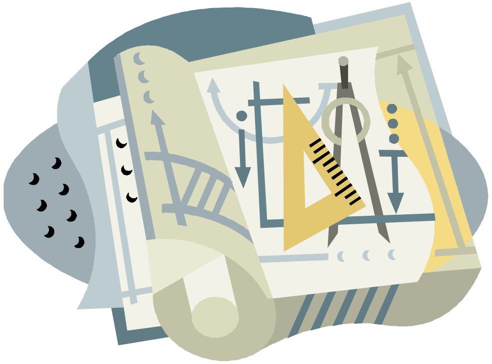
4. Security management

4）Implementation management of security function

(1) Middle period planning of implementation.
⇒ Planning of next few years under risk prediction on the basis of incident management.

(2) Prediction/survey/evaluation of the measure technology and product and also out sauce service etc. of the present condition in accordance with a/the middle period plan.

(3) Enforcement control of the short term plan.
⇒ Expectation effect/budget/application cost.



5）PDCA

Generally,

Plan⇒Do⇒Check⇒Action

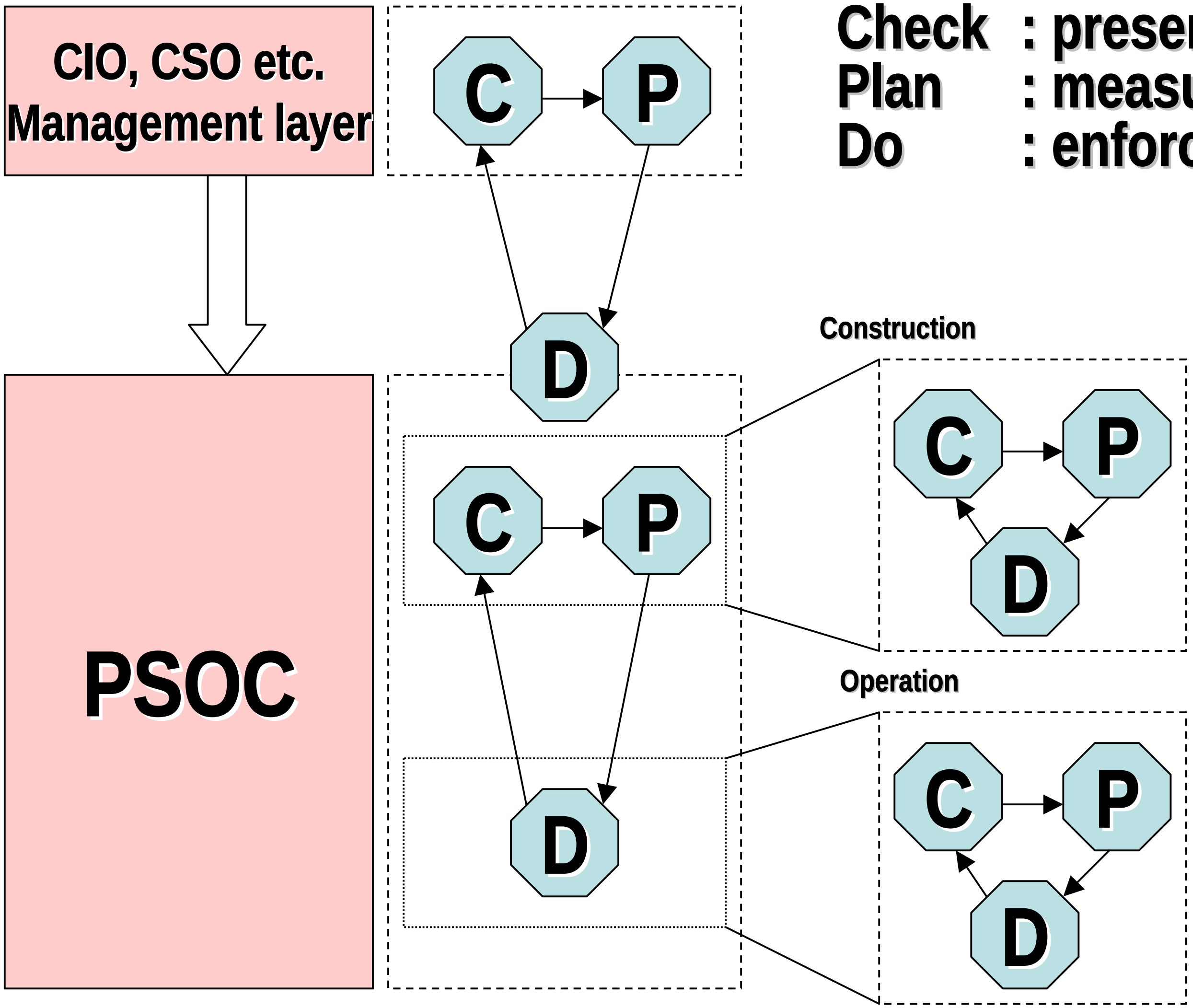
However, the security is not the leading part.
Because we want do something security becomes necessary.
Therefore,

Check⇒Plan⇒Do

Check : present condition grasp
Plan : measure plan
Do : enforcement

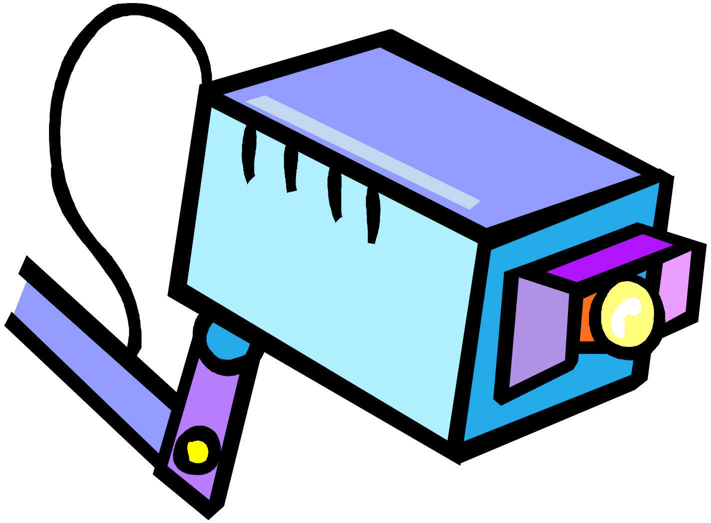
4. Security management

5）PDCA



Check : present condition grasp
Plan : measure plan
Do : enforcement

5. Maintenance(Security system)



5. Maintenance

1）Compliance operation and maintenance

(1) Security documents disclosure and confirmation.
(2) Work flow such as application.
(3) Instructions and confirmation such as measure/precaution.

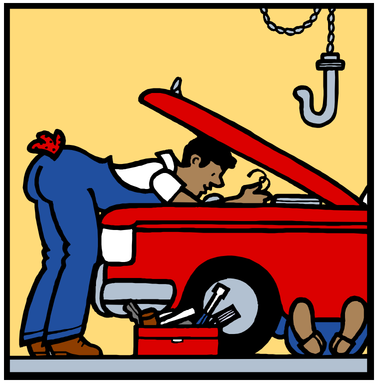
⇒ Important viewpoint even operation record

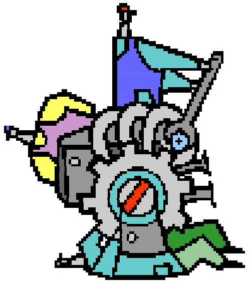
5. Maintenance

2）Security device operation and maintenance

⇒ Firewall, Anti Virus, Quarantine LAN, Patch management system
Monitoring system Etc.

(1) Operation surveillance.
(2) Definition file renewal and optimization.
(3) Patch management of device itself.   etc.





5. Maintenance

3）Security help desk

(1) User support

1) Virus etc.

2) Security setting support

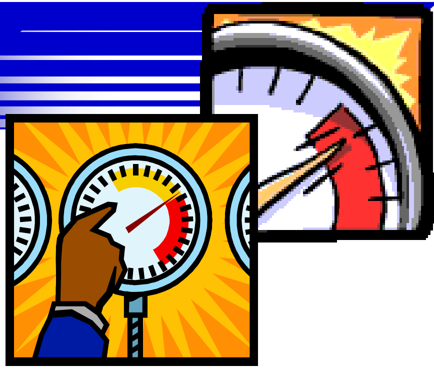
(2) System manager support

1) Vulnerability information and avoidance plan etc. to server systems.

2) Precaution method etc.

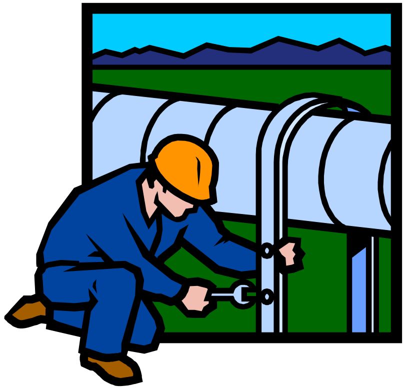
(3) Accept urgent correspondence
(perhaps additional post with correspondence)

5. Maintenance



4）System healthy management

① Operation situation of each system, network
PING (IP layer), service port (service AP layer)
In addition AP, DB etc.



② Property control of each system and client PCs.
(The setting contents, implemented AP etc.)

⇒It makes NOC and system application over lap.
Mechanism that is able to grasp abnormal and irregularity condition with the viewpoint of availability, especially is important

（1）Trouble or accident?

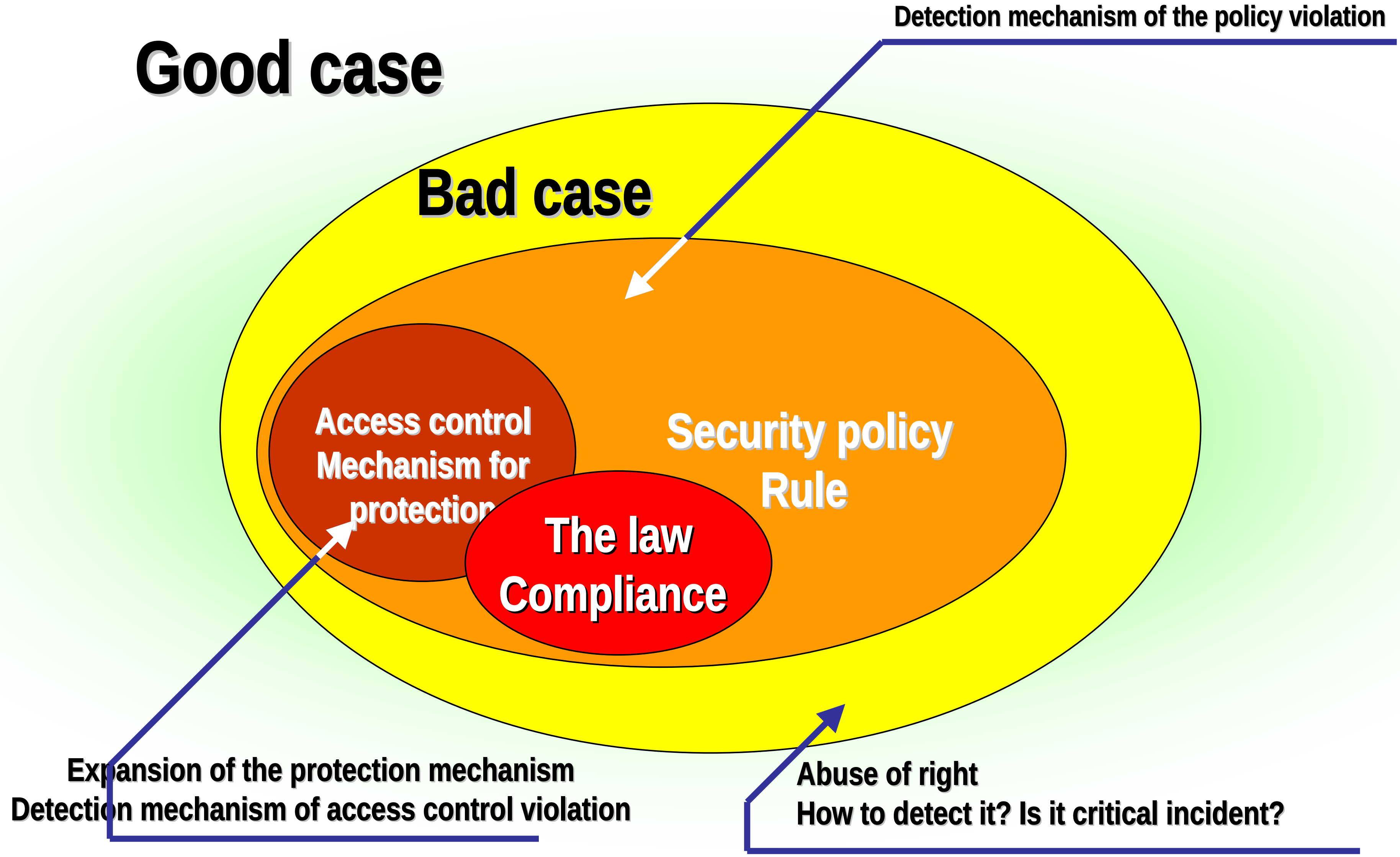
（2）Security incidents?

⇒ It had better do a consideration well to live together with inside security surveillance.

6. Security Monitoring

6. Security Monitoring

1) Category of security monitoring


Detection mechanism of the policy violation
Good case
Bad case
Access control Mechanism for protection
Security policy Rule
The law Compliance
Expansion of the protection mechanism
Detection mechanism of access control violation
Abuse of right
How to detect it? Is it critical incident?

6. Security Monitoring

2）Example of the category as view point of the occurrence phenomenon

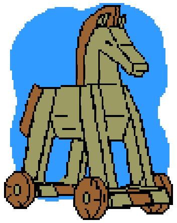
(1) Unauthorized access

1) Cracker attack and BOT

2) Worm（Active Attack、Remote Exploit）

3) Malware such as computer virus and Trojan Horse
（Passive Attack、Contents Exploit）

4) Access control violation

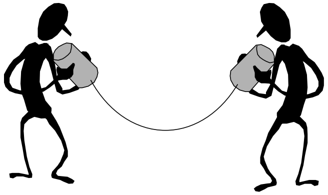


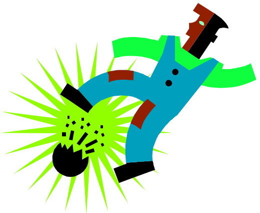
(2) Security policy violation

1) Account management violation

2) Action of authority outside

3) Dangerous action etc.





(3) Devices trouble and disasters

(4) Operation accident and setting mistake

(5) Suspicious access

1) Anomaly behavior

2) Others（Investigation necessary）

6. Security Monitoring

３）Example of incident category as view point of the threat

(1) Business stoppage

With which system or which segment?

(2) Information leakage

With which information?

(3) Morals collapse

With which level?（Viciousness degree ）

There is the method that binds the alert as above.

6. Security Monitoring

4）Example of the determination of level of importance

It has occurred
when,where,which etc.

Occurrence phenomenon	Threat category			Level of importance			
	Business stoppag	Information leaka	Morals collaps	RED	Orange	Yellow	Green
(1) Unauthorized acces	◎	◎	◎				
(2) Security policy violation	△	◎	◎				
(3) Devices trouble and disasters	◎	△	△				
(4) Operation accident and setting mistake	◎	○	○				

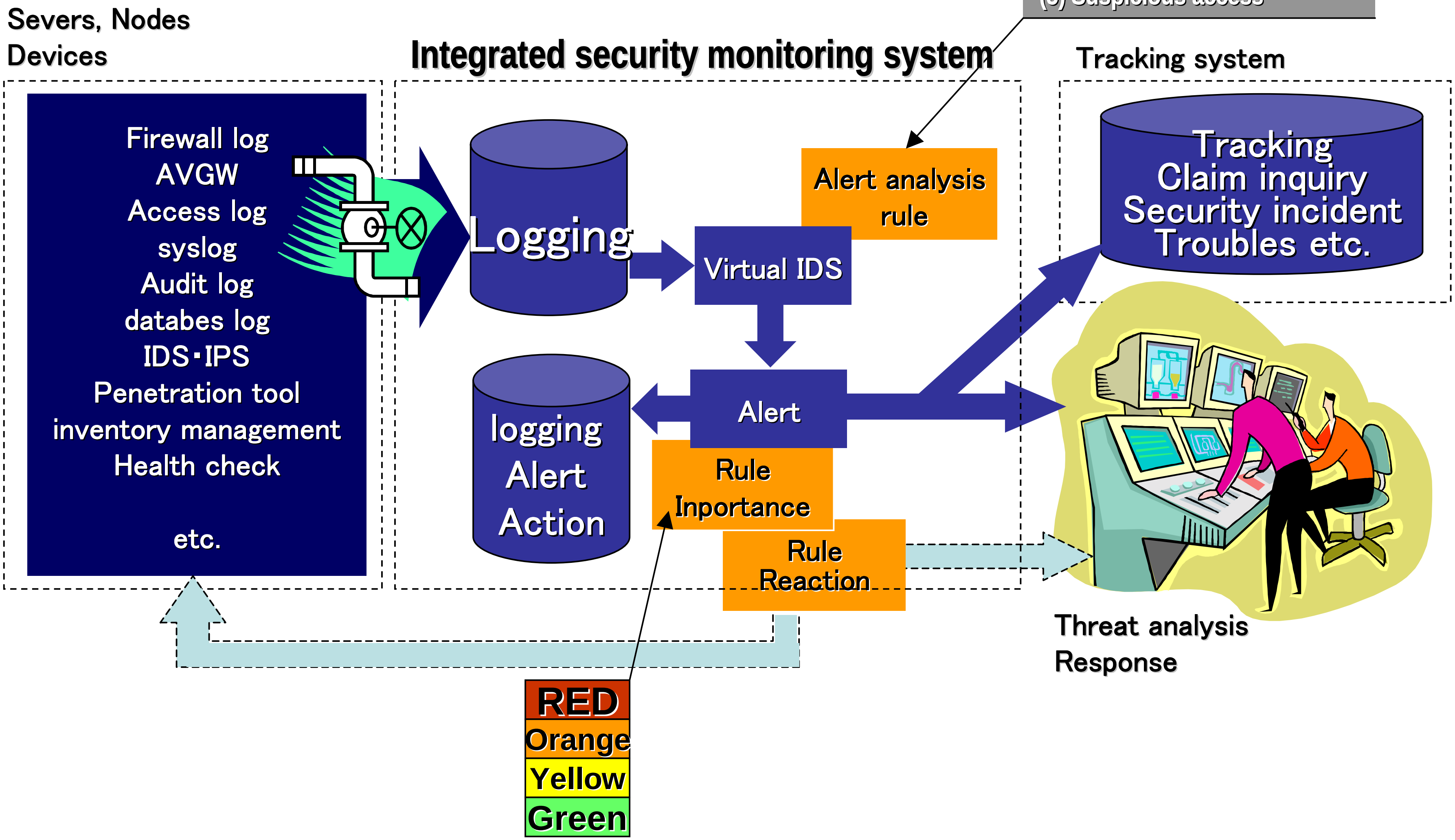
(5) Suspicious access	To above which does it correspond? Confirmation to the scene of the fact…

※	
RED	Prompt correspondence
Orange	Precaution/urgently correspondence
Yellow	Attention /weekly/monthly
Green	Information/statistics

Thought in each organization

5）Concept of Integrated security monitoring

(1) Unauthorized access
(2) Security policy violation
(3) Devices trouble / disasters
(4) Accident and mistakes
(5) Suspicious access



Severs, Nodes
Devices

Firewall log
AVGW
Access log
syslog
Audit log
databes log
IDS･IPS
Penetration tool
inventory management
Health check

etc.

Integrated security monitoring system

Logging

Alert analysis rule

Virtual IDS

Alert

logging
Alert
Action

Rule
Inportance

Rule
Reaction

RED
Orange
Yellow
Green

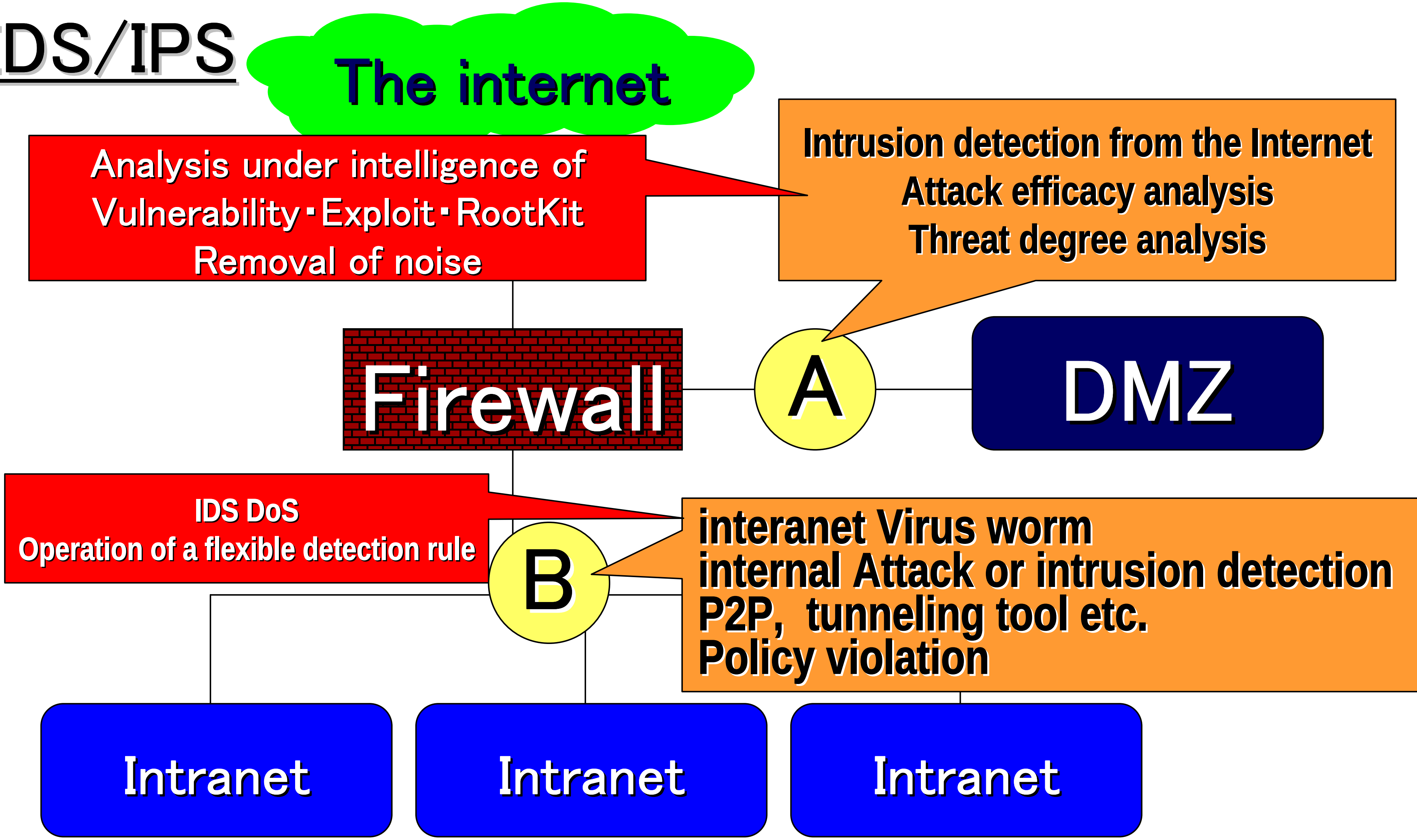
Tracking system

Tracking
Claim inquiry
Security incident
Troubles etc.

Threat analysis
Response

6. 1 Characteristic and usage of monitoring sensor

IDS/IPS



Analysis under intelligence of
Vulnerability･Exploit･RootKit
Removal of noise

Intrusion detection from the Internet
Attack efficacy analysis
Threat degree analysis

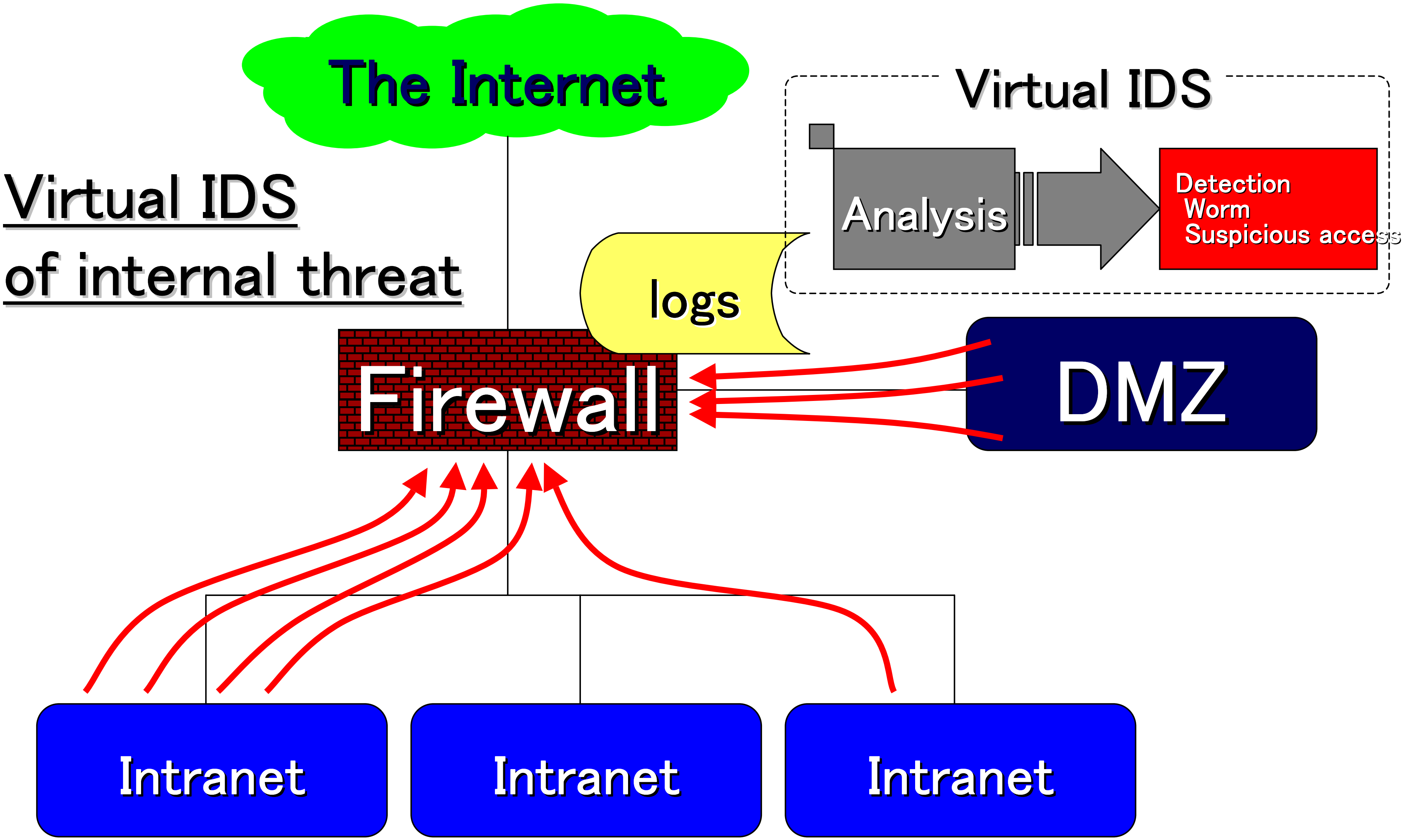
IDS DoS
Operation of a flexible detection rule

interanet Virus worm
internal Attack or intrusion detection
P2P, tunneling tool etc.
Policy violation

6．1 Characteristic and usage of monitoring sensor

Virtual IDS

of internal threat



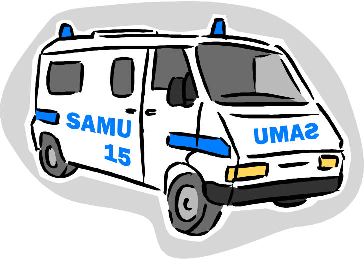
6．1 Characteristic and usage of monitoring sensor

DoS

There may not be malice.

Layer image		Threat or Method	Damage
7	DB	Dead lock Exclusion control Successive clicks user	Processing impossible/delay
6	AP	Thread and Queue Exclusion control Successive clicks user	Resources waste by the minority user and general user processing impossible
5	Service AP	Request number Low speed circuit user Successive clicks user	Rejection of new sessions
4	TCP	Syn Flood Session number etc.	Protocol stack Session control such as Firewall Rejection of new sessions
3	IP	UDP, ICMP Flood Smarf etc.	Node down Overflow of the network

7. Incident Response



Is it just accident?

Trouble?

Recovery,,

Mistake/Ignorant?

Morals collapse / Broken window theory

Not make the enemy

Intentional?

Sensitive operation / Thoroughly

7. Incident Response

Where is the enemy?

Outside :

Normal operation

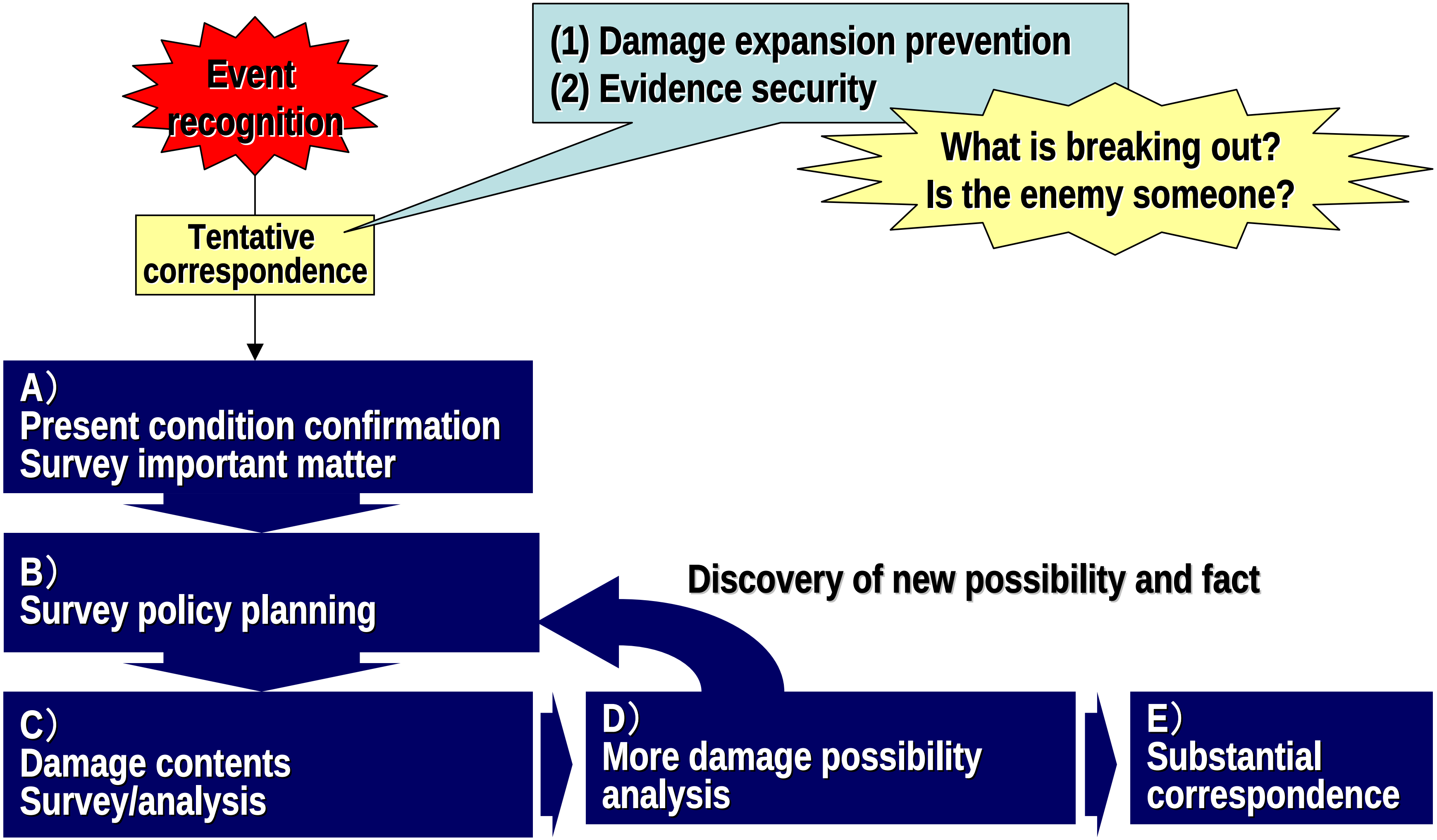
Inside :

Sensitive operation

The way of response differs largely.

7. Incident Response

1) Flow of urgent correspondence



7. Incident Response

A) Present condition confirmation/ Survey important matter

1) Present condition confirmation

(1) hearing

Detection method, Correspondence contents, Phenomenon

Network system configuration, Person concerned, Organization, software Version

2) Investigation requirement / Decision of the goal

(1) Investigation Target

1. Confirmation of the incident contents

2. Criminal investigation

3. Recovery

(2) Restriction time?

(3) Cost?

7. Incident Response

B）Survey policy planning

1) Are almost the contents able to conjecture? (from outside or inside?)

(1) From trace to survey

- **Detailed survey to cost, time, experience, advanced skill necessary**
- **Tools**
- **Issues**

  Volatility trace

  Trace that is not remaining to HDD (history)

(2) Survey with method of elimination

- **Pickup of possibility that under consideration of the intrusion route and method constitution of the present condition.**
- **And, enforcement with method of elimination from a/the log and trace**

In any case, you must decide the survey method in terms of settlement and, survey range.

7. Incident Response

C）Damage contents Survey/analysis

1) Survey from a/the disk image

2) Survey as it operated

Condition of the memory
Condition of the ports and process
Condition of the the screen
File such as temporary, program/script, setting, data, logs etc.

3) Analysis

The method, enforcement contents, timing etc.

Advance mechanism (record)

Good tools

7. Incident Response

D)More damage possibility analysis

Investigation result

In the case that the fact and possibility of the exception that are out in the table appeared

Many cases (hypothesize necessary)

7. Incident Response

E）Substantial correspondence

1) Institutional correspondence
   (1) Project organization
   (2) Public relations
   (3) Security policy etc.
   (4) Education/training

2) Technical correspondence
   (1) The countermeasure planning and enforcement
   (determent, prevention, defense, detection, recovery)
   (2) Inspection and Audit
   ※ Excessive/hypersensitive Too little/insensitive

Official recovery
Recurrence prevention

7）Example of emergency category

Category	Contents	Red	Orange	Yellow	Green
A	Related to the nucleus system	No prospect of recovery	Over 3 hours stoppage is expected	Less 3 hours stoppage is expected	
B	Related to client PC environment	No prospect of recovery and large-scale obstacle	Over 3 hours stoppage is expected	Less 3 hours stoppage is expected	
C	Security attack from the outside	Intruded	Intrusion is expected	Viciousness attack	
D	Security scandal	Disclosure information leakage	Disclosure information missing	Viciousness security policy violation Accident that is connected to information leakage or missing	

8. Practice level

8. Practice level

1) Outline of practice level

(1) Compliance

- Clarification of the management item

  Notice the policy such as security policy and rule etc.
- Proof of management enforcement

  Record a/the basis

  ⇒ Effective utilization of groupware

Minimum

(2) Passive security measure

- Traceability
- Security monitoring
- Fundamentally defense plan

Even if it occurs it is able to correspond

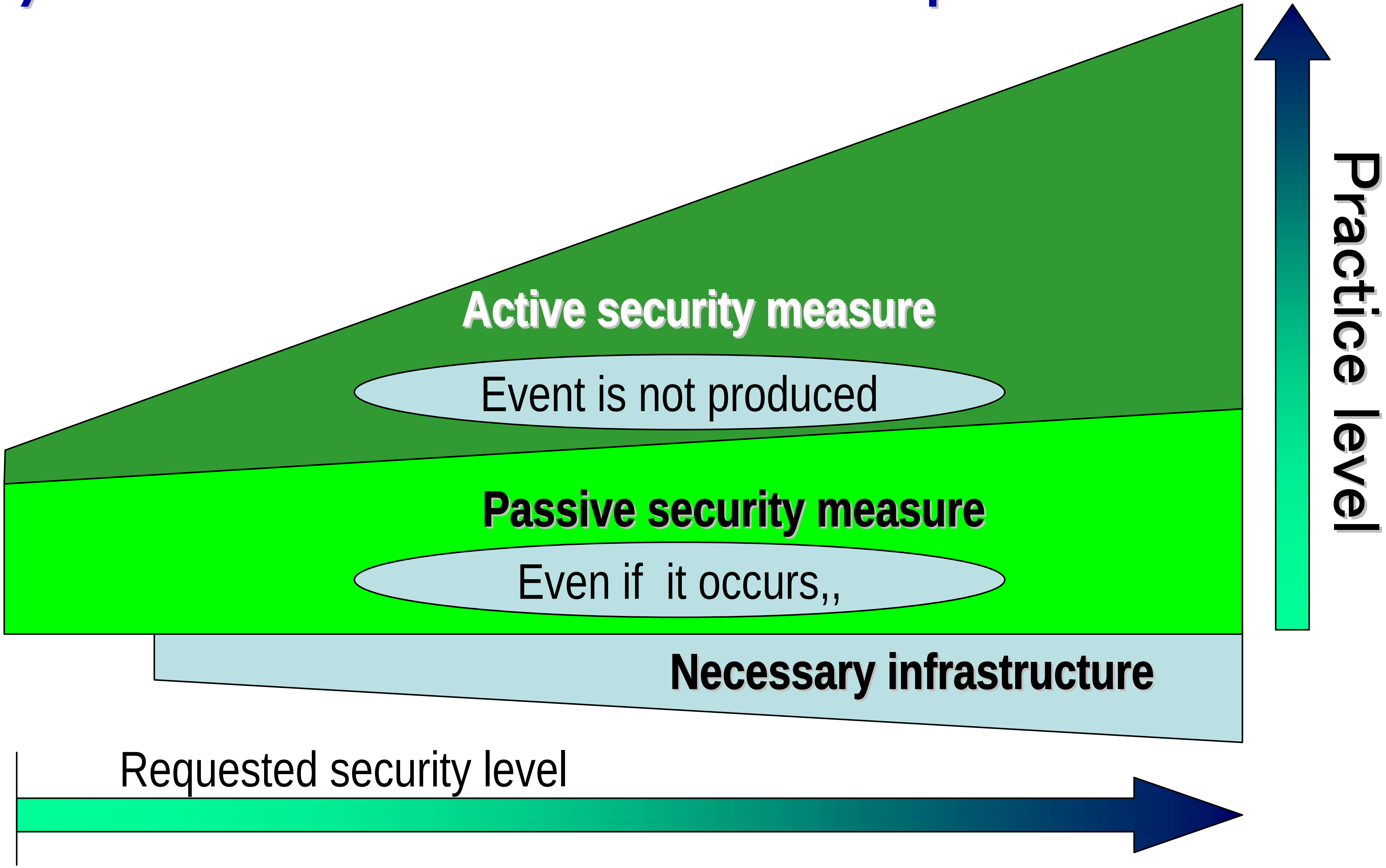
(3) Active security measure

- Prevention plan
- Determent plan

Event is not produced

8. Practice level

2) Level and measure method that are requested



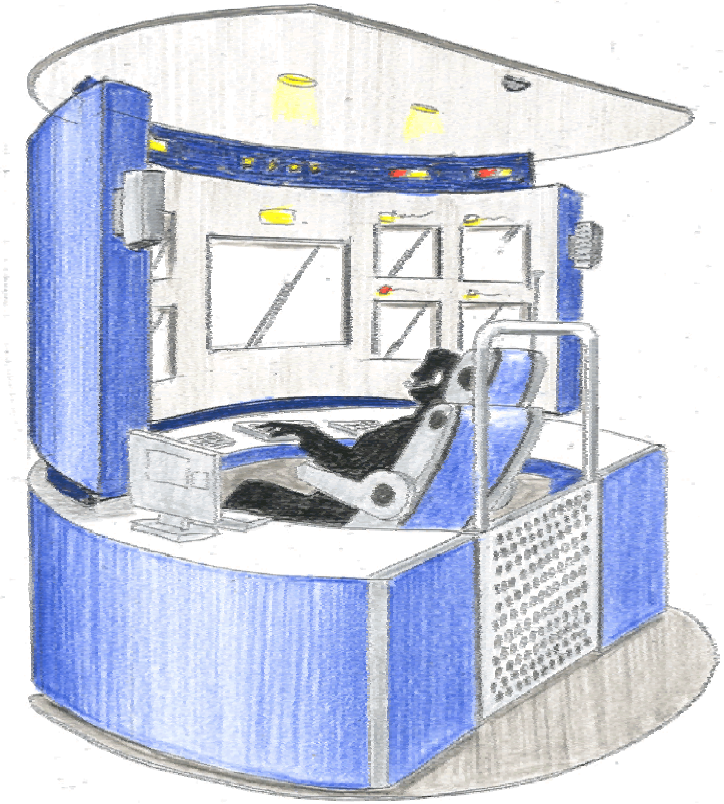
By the way

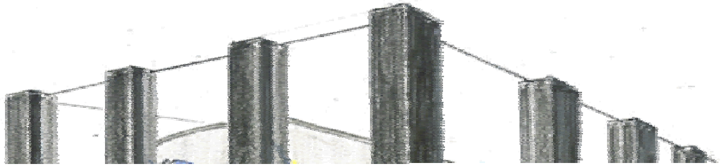
Problem on security must solve it without fail, because sometimes it should be happened.

And there is not causality in the importance of the result and its cause.

8. Practice level

3) Not only functions of PSOC but also visual effects might be more important.





Any questions?

itsuro@lac.co.jp