

Case Studies on Cyber Incidents

2016. 2. 21





Contents

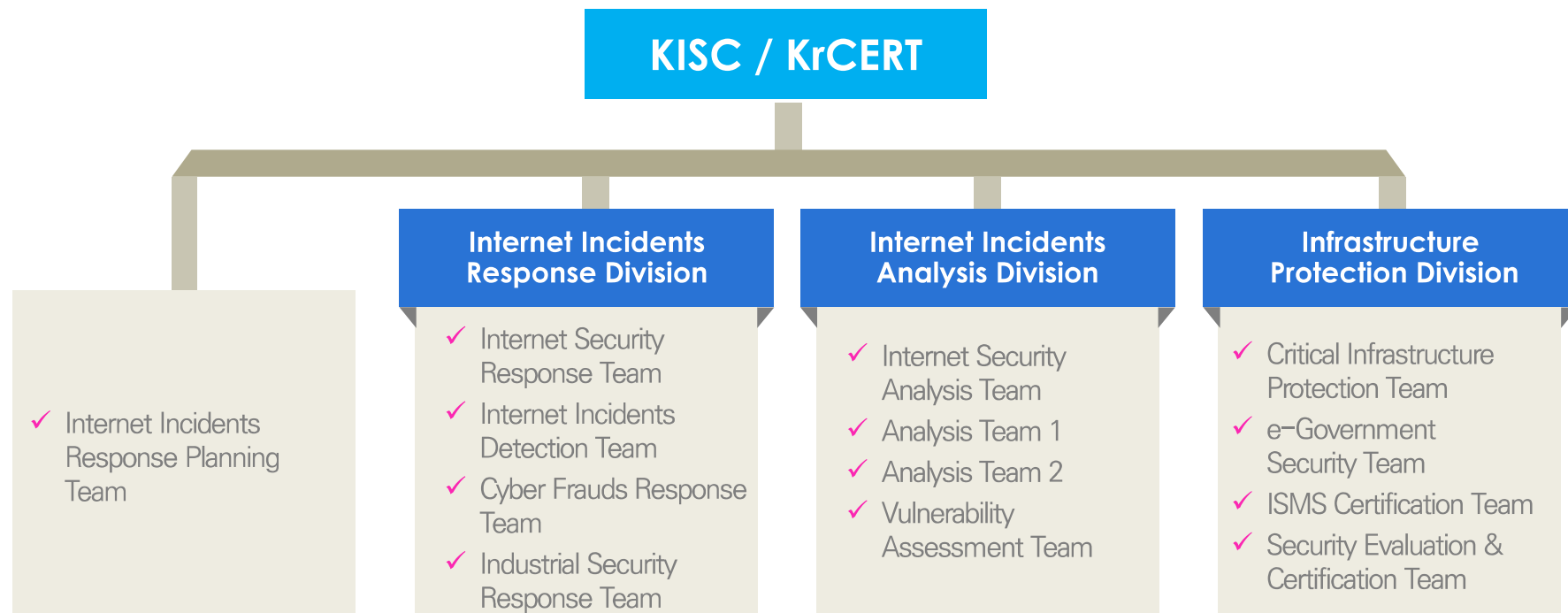
- 1** Introduction of KrCERT/CC
- 2** Case Studies



Introduction of KrCERT/CC

1. Organization of KISC

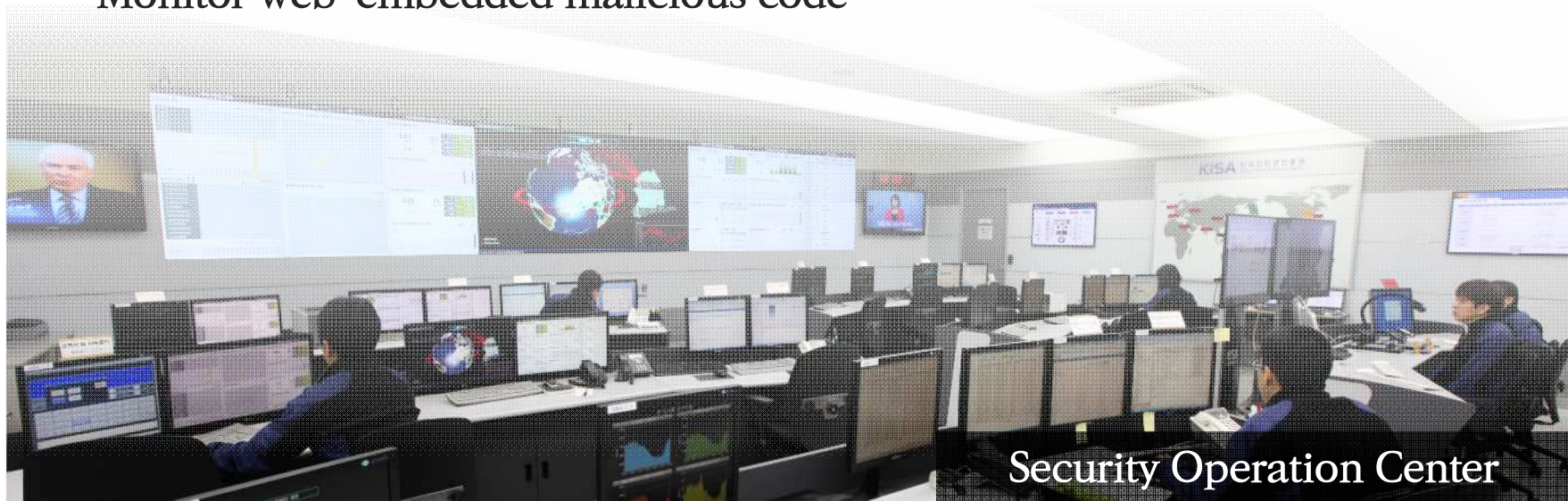
- **KISC** (Korea Internet Security Center) is a **Part of KISA** (Korea Internet & Security Agency)
- **Mission** : Rapid Detection / Response for Cyber Incidents in **Private sector**



2. Monitoring

Monitor internet network in Korea

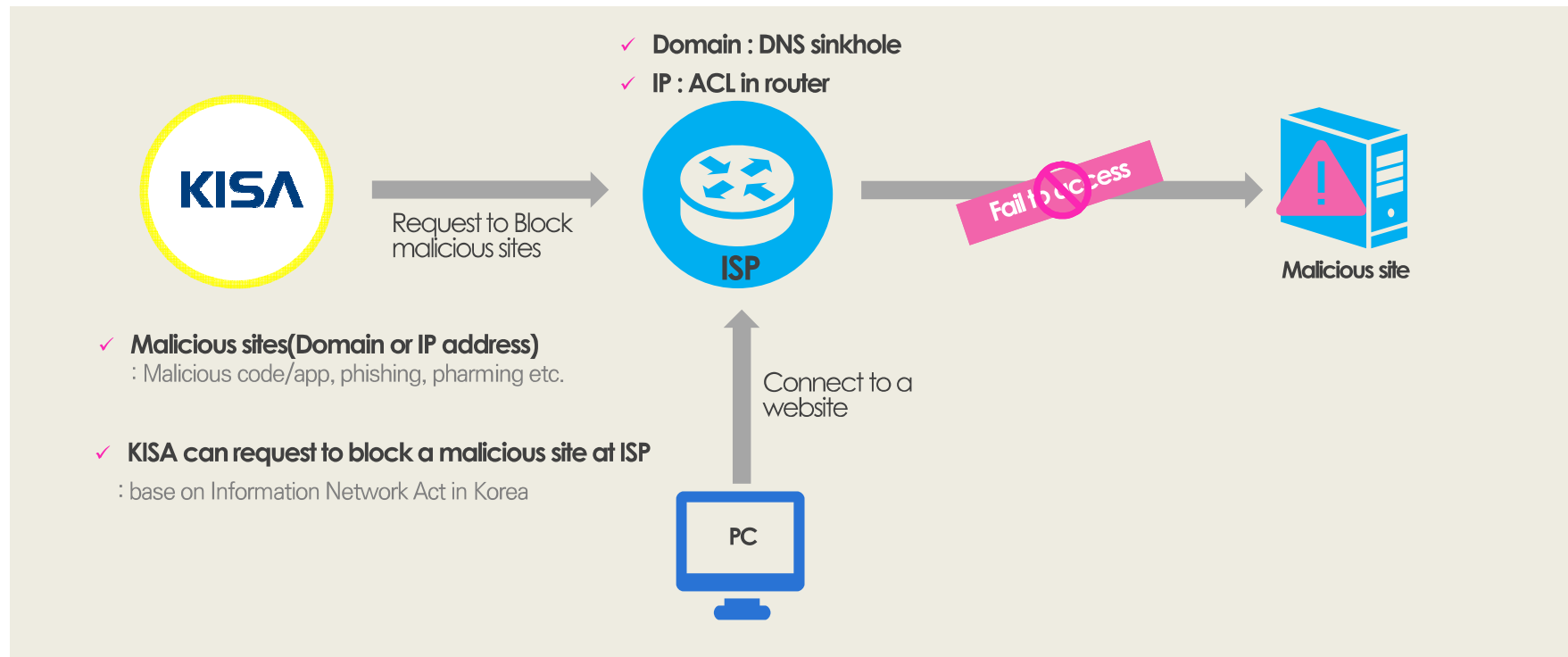
- **Traffic** : local Internet Service Provider Traffic, Ports, Protocols, Attacks
- **Web Servers** : 900+ Major Domestic Web servers
- **DNS** : 13 Root DNS, 6 KR DNS, 12 Major Domestic ISP DNS
- **Security Information** : Major Anti-Virus, System/Software/Security Company sites
- **Monitor web-embedded malicious code**



3. Blocking

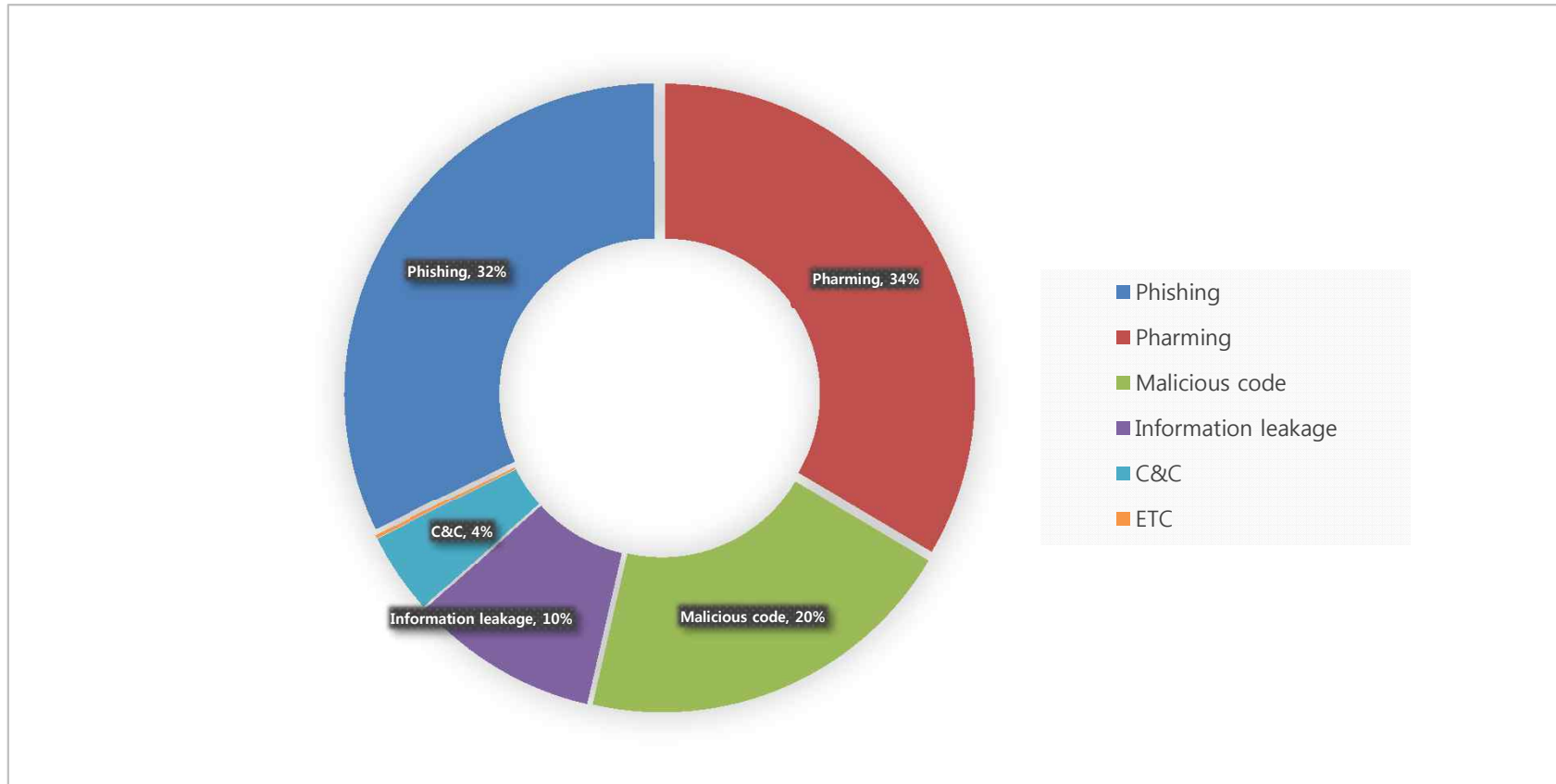
Block access to malicious sites

- Collaboration with ISPs to prevent damage by blocking malicious sites



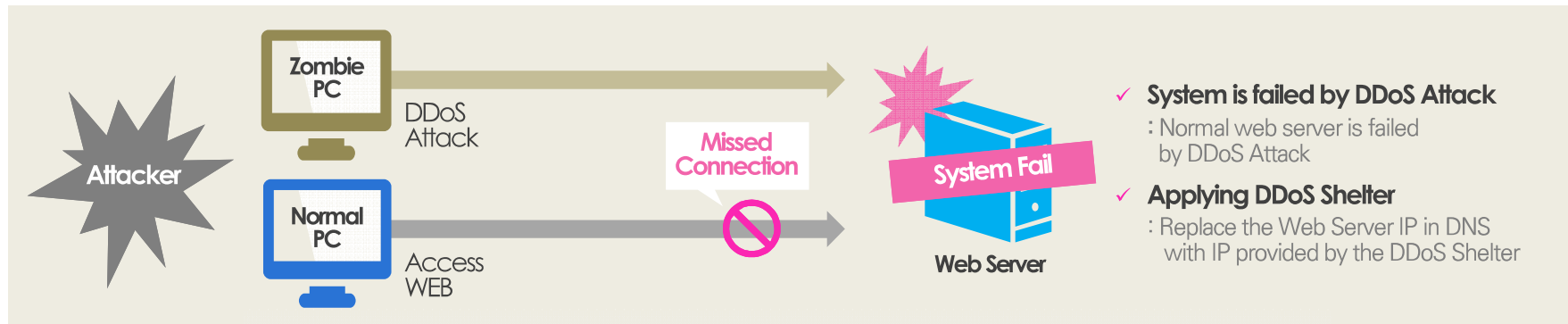
3. Blocking(cont.)

Statistics on 2015

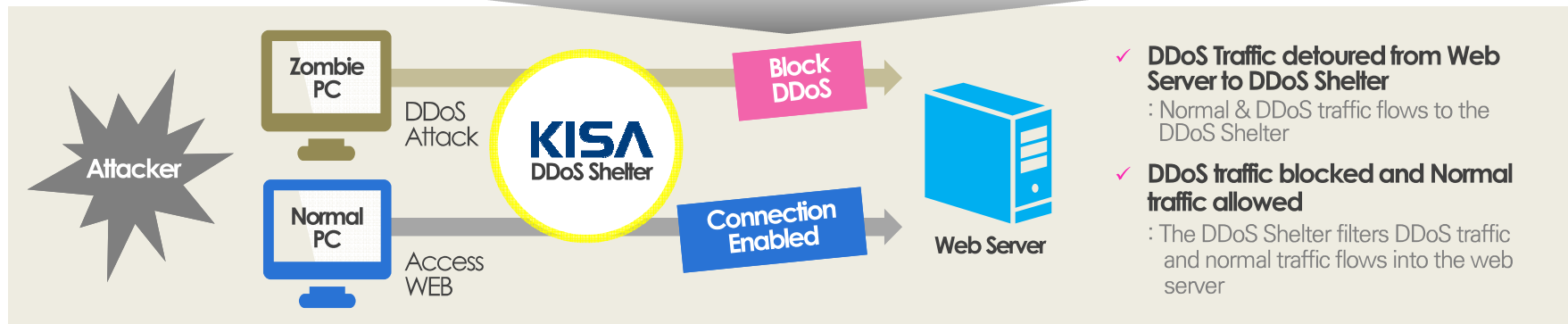


4. DDoS Shelter System

- DDoS defense service at the government level for SMEs
: It's blocking DDoS attack and supporting normal web service of SMEs

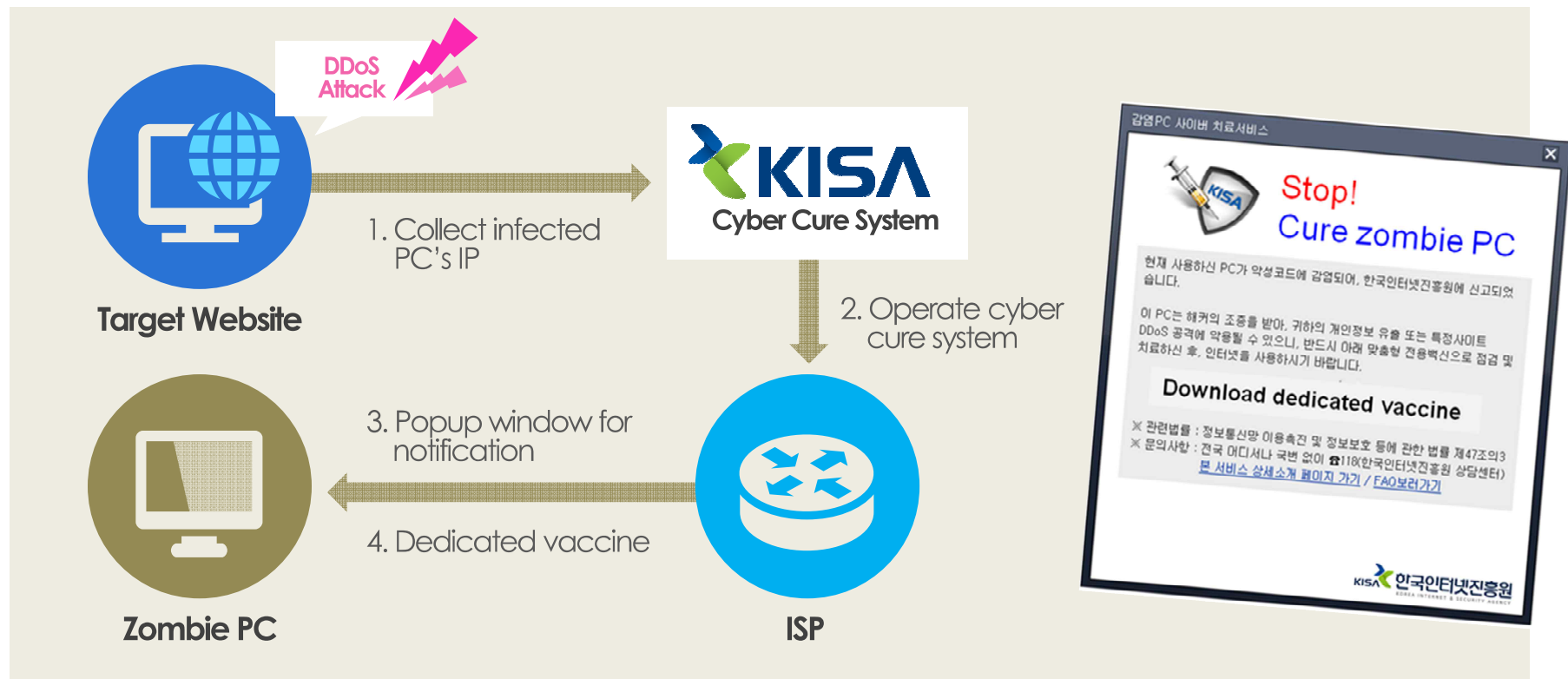


After applying DDoS Shelter



5. Cyber Curing System

- Provide a notification of malware infection and removal method using popup window
- Effective measure against large-scale DDoS attack





2 Case Studies

Case 1 : Personal Information leakage


- Data breach(2015.9)
 - Hacked a famous community site and a demand for an apology
 - Threats to disclose around 1.9 million sets information
 - Disclosed some customer's information(ID, Password, e-mail, etc.)



A	B	C	D	E	F	G	H	I	J	K
2015-09-11	HNJ0200	50	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	vovddlibb	5	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	kangdha	5	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	titleguy	69	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	nawkddlek		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	oassao	76	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	kymksm525		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	ucs2001	8	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	dongukm	9	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	sjsj444	9	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	foto413	9	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	lgctax	a13	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	chaniblo		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	cjsdnxhddns	7870	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	chlvhdgur7	806	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	cleoohc		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	mike5820		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	dena	ader	시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	otlyang		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	sado1star		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	kimjv0507		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?
2015-09-11	wizard1187		시작?	시작?	시작?	시작?	시작?	시작?	시작?	시작?

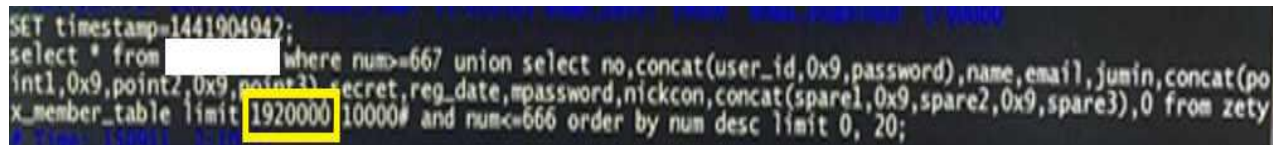
Case 1 : Personal Information leakage

- Analysis & Response
 - Korea IP(X.X.161.67) in web log.



```
webadmin@web11/home/logs
161.67 - [11/Sep/2015:00:23:39 +0900] "GET /...php HTTP/1.1" 200 758
161.67 - [11/Sep/2015:00:37:13 +0900] "GET /...php HTTP/1.1" 200 9010
161.67 - [11/Sep/2015:01:13:53 +0900] "POST /...sis2.php HTTP/1.1" 200 15165
161.67 - [11/Sep/2015:01:20:19 +0900] "POST /...sis2.php HTTP/1.1" 200 895492
161.67 - [11/Sep/2015:01:20:59 +0900] "POST /...sis2.php HTTP/1.1" 200 866301
161.67 - [11/Sep/2015:01:21:02 +0900] "POST /...sis2.php HTTP/1.1" 200 889871
161.67 - [11/Sep/2015:01:21:15 +0900] "POST /...sis2.php HTTP/1.1" 200 875067
161.67 - [11/Sep/2015:01:21:39 +0900] "POST /...sis2.php HTTP/1.1" 200 875067
```

- SQL-injection attack and 1920,000 information leakage



```
SET timestamp=1441904942;
select * from [redacted] where num=667 union select no,concat(user_id,0x9,password),name,email,jumin,concat(po
int1,0x9,point2,0x9,point3),secret,reg_date,mpassword,nickcon,concat(spare1,0x9,spare2,0x9,spare3),0 from zety
x_member_table limit 1920000 10000# and num<=666 order by num desc limit 0, 20;
```

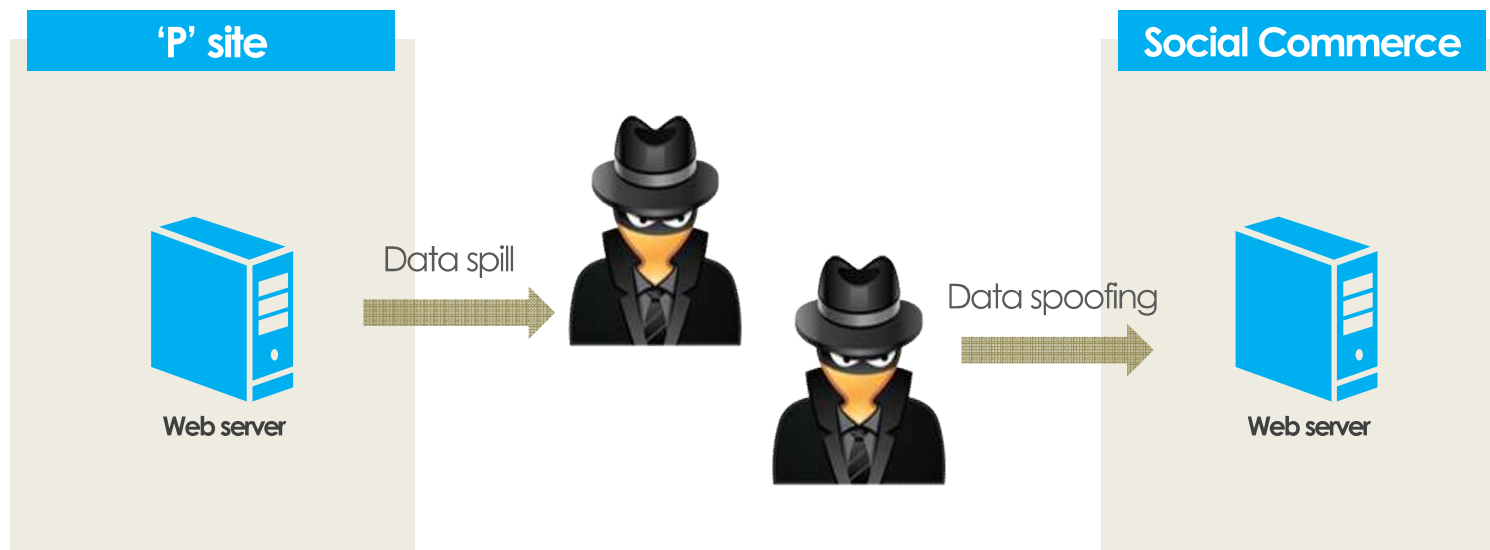
- Additional attack using CMS vulnerability
- Noticed a guideline for prevention of further hacking

Case 1 : Personal Information leakage

- **Violation(According to Information Network Act in Korea)**
 - §28-①-2(Access Control) : must have access control devices.
 - §28-①-3(Access Log) : must have a web log over 6 months
 - §28-①-4(Encryption) : must use a proper encryption algorithm
- **Fine(According to Information Network Act in Korea)**
 - Below 3% of the total sales & Below 30 Million won
 - 120 Million won(≙ 110 thousand dollars)

Case 1 : Personal Information leakage

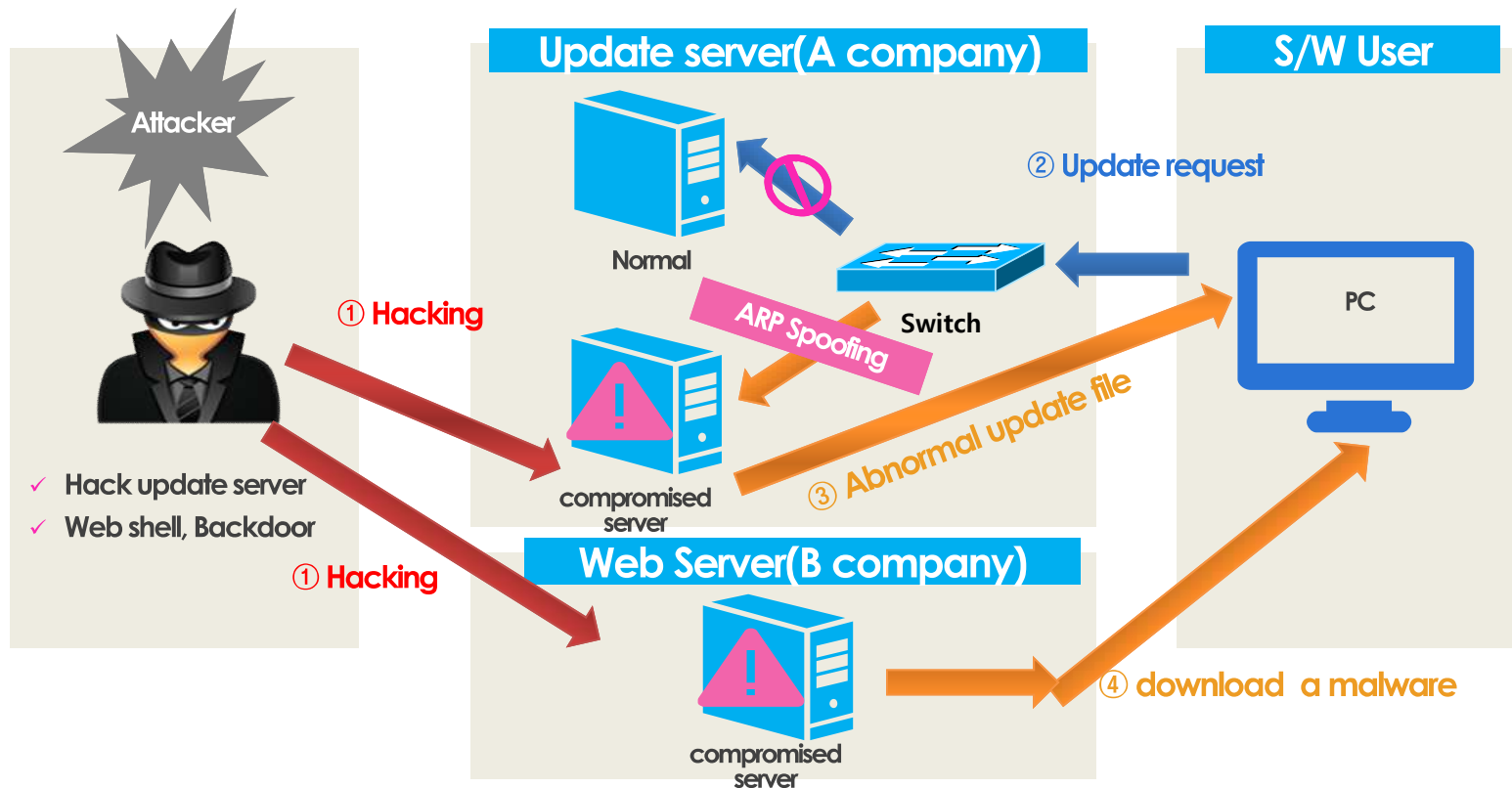
- Data spoofing(2015.12)
 - Customers' accumulated money is being paid without approval
 - Targeted users who used the same account information for both sites T and P



Case 2 : Update Server Hacking

- Summary

- Developing a fake update server and sending malicious update file
- Hacking a server for spread of malware



Case 2 : Update Server Hacking

- Analysis(A company)
 - Upload a webshell on web server
 - Acquisition of ROOT using the local privilege escalation vulnerability



The screenshot displays a webshell interface with a dark background and light text. At the top, it shows system information: 'uname: Linux', 'User: 99 (nobody) Group: ()', 'Php: 5.2.10 Safe mode: OFF [phpinfo] Datetime: 2015-11-02 21:33:34', 'Hdd: 7450.45 GB Free: 2847.78 GB (38%)', and 'Cwd: /home'. Below this is a navigation bar with buttons for '[Sec. Info]', '[Files]', '[Console]', '[Sql]', '[Php]', '[Safe mode]', '[String tools]', '[Bruteforce]', '[Network]', '[Logout]', and '[Self remove]'. The main content area is titled 'Server security information' and contains the following details: 'Server software: Apache/2.0.63 (Unix) mod_ssl/2.0.63 OpenSSL/0.9.8e-fips-rhel5 PHP/5.2.10', 'Disabled PHP Functions: none', 'cURL support: enabled', 'MySQL support: 5.0.84', 'MSSql support: no', 'Oracle support: no', 'PostgreSQL support: no', 'Readable /etc/passwd: yes [view]', 'Readable /etc/shadow: no', 'OS version: Linux version 2.6.18-92.el5PAE (root@sul2-build) (gcc version 4.1.2 20071124 (Red Hat 4.1.2-42)) #1 SMP Fri Feb 20 14:49:44 KST 2009', 'Distr name: SUIlinux release 2.0', 'Kernel \r on an \m', 'Useful: ld php python tar gzip bzip2 nc locate', 'Danger: iptables logwatch', and 'Downloaders: curl lwp-mirror'.

- Rerouting of the request traffic to the fake update server via ARP spoofing
- Transmission of malicious update file containing falsified field to user

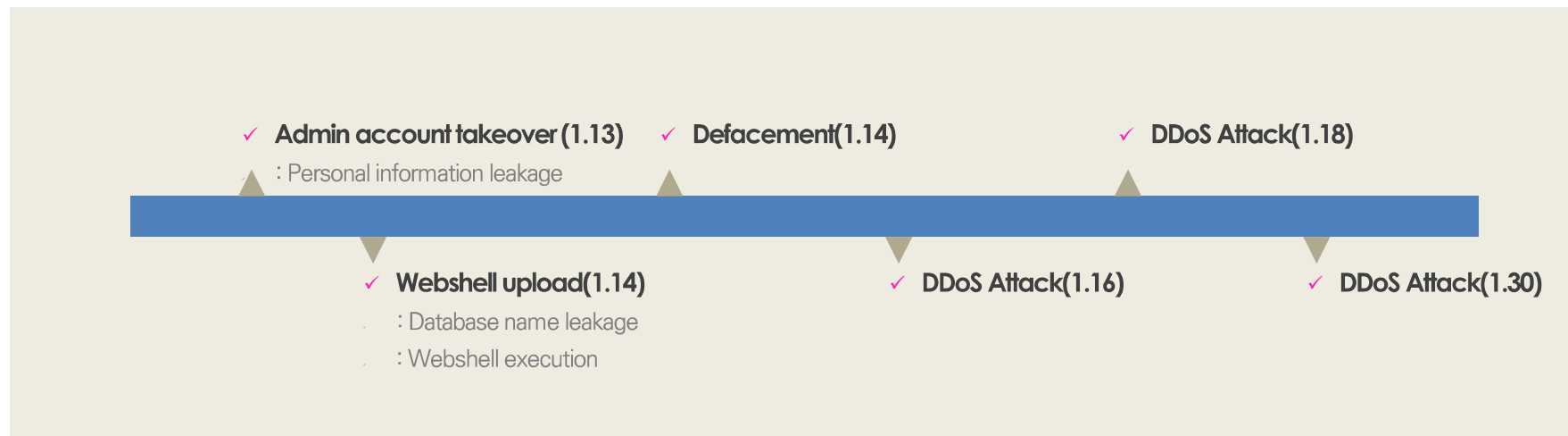
Case 2 : Update Server Hacking

- Analysis(B company)
 - Hijacking of user account through brute-force attack
 - Pharming type malware that leaks certificate and financial data
 - KISA, Blocking of information-leaking site, pharming and C&C IP access



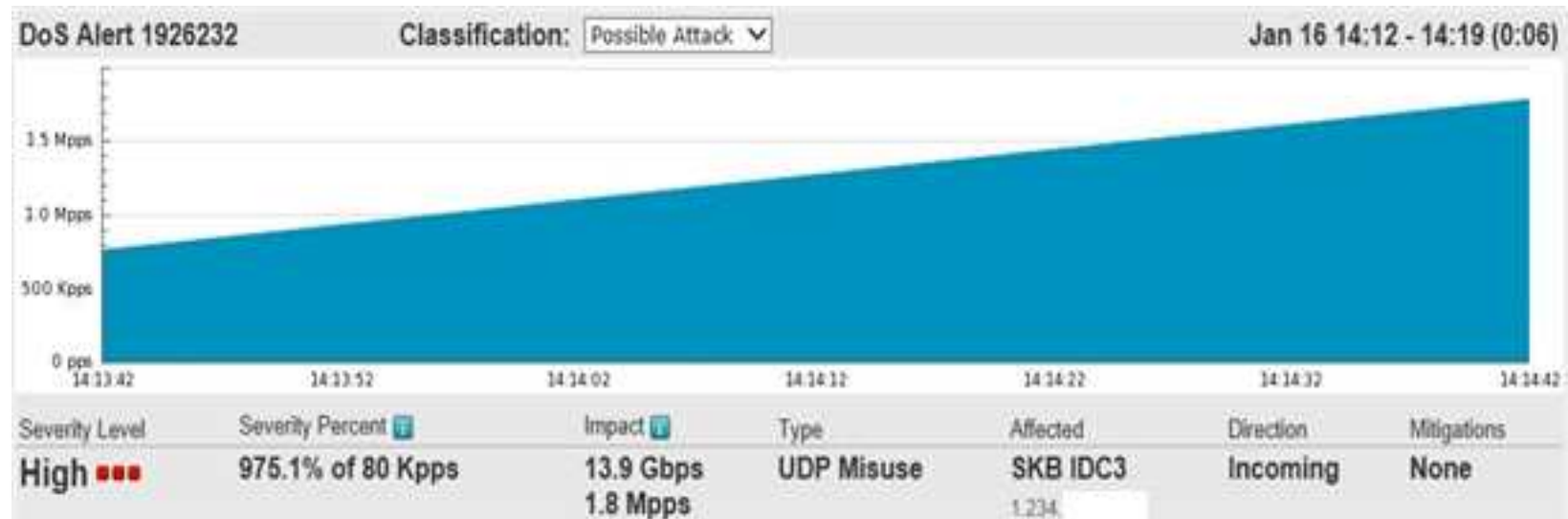
Case 3 : Anonymous

- Entertainment agency DDoS attack(2016. 1)
 - Cyber attack as the result of an international and political issue
 - Server hacking, Defacement, Information leakage, DDoS



Case 3 : Anonymous

- Analysis & Response(DDoS)
 - DNS DrDoS(Distributed Reflect Denial of Service)
 - Defense against DDoS attack by using the DDoS Shelter system



Thank you

lsw1@kisa.or.kr

