



核能研究所網路現況報告

單位：核能研究所

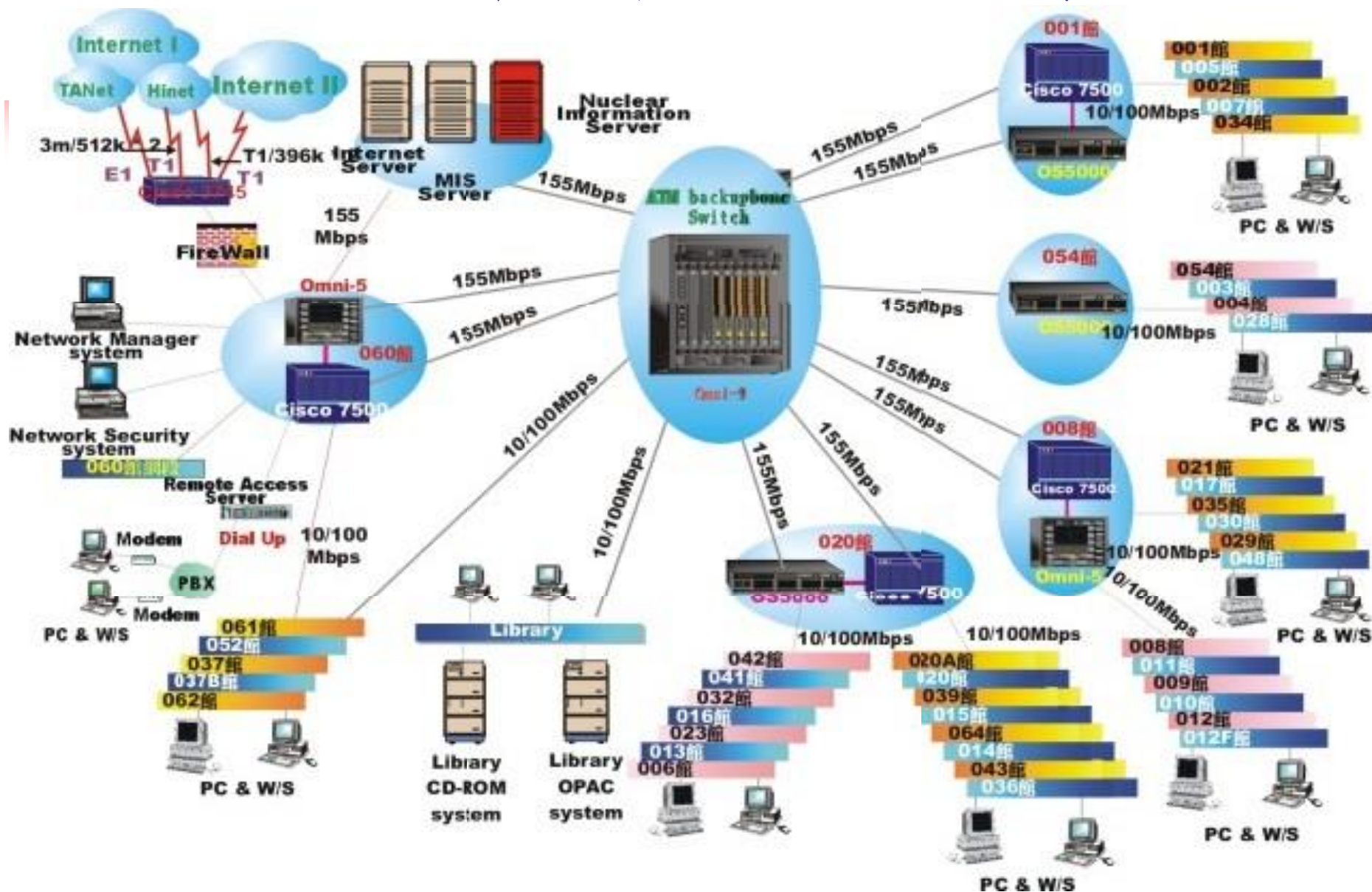
日期：民國九十二年十二月十一日



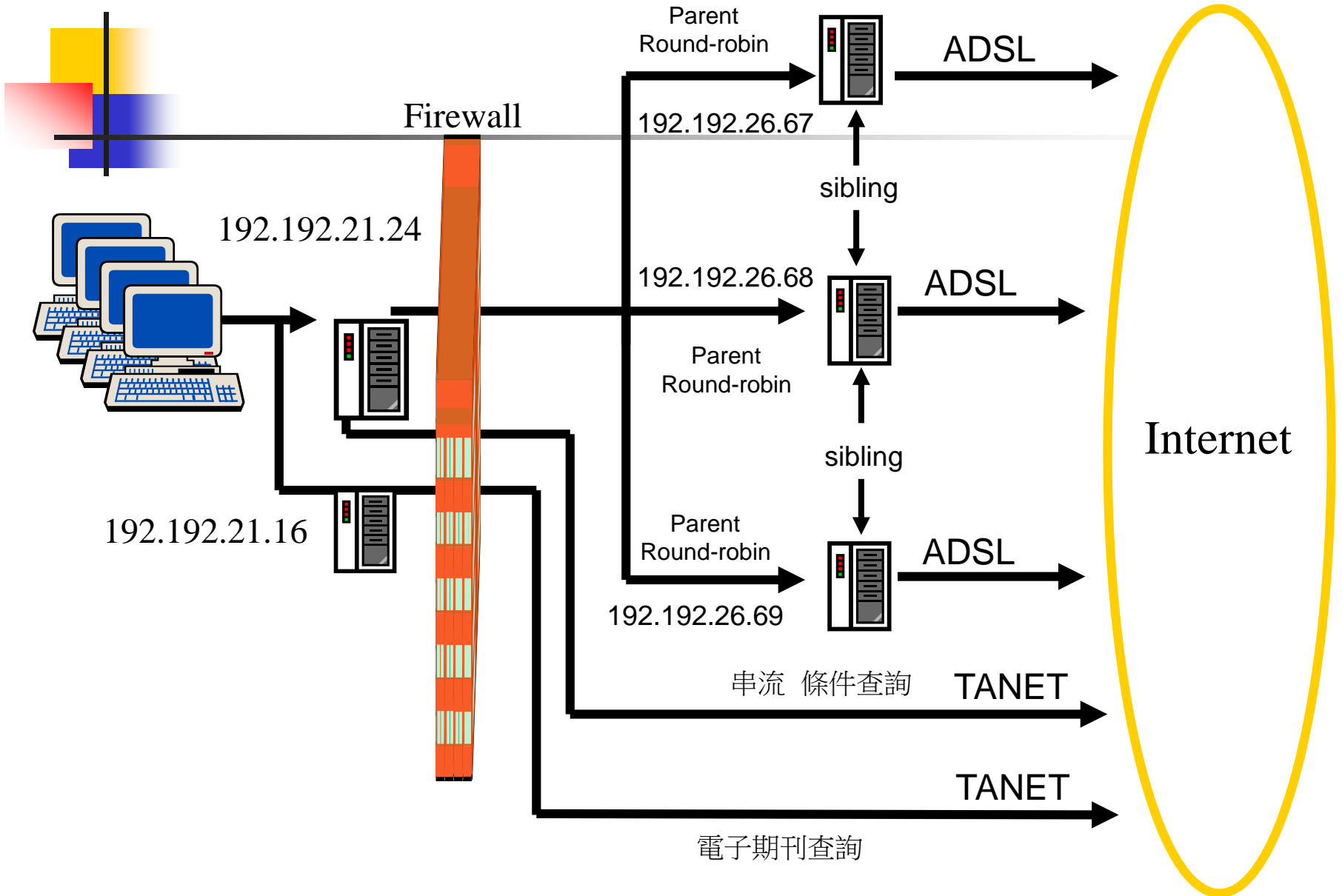
簡報大綱

- 本所網路架構
- Proxy Server
- 流量統計圖
- 電腦病毒防治
- 入侵偵測系統
- 未來展望

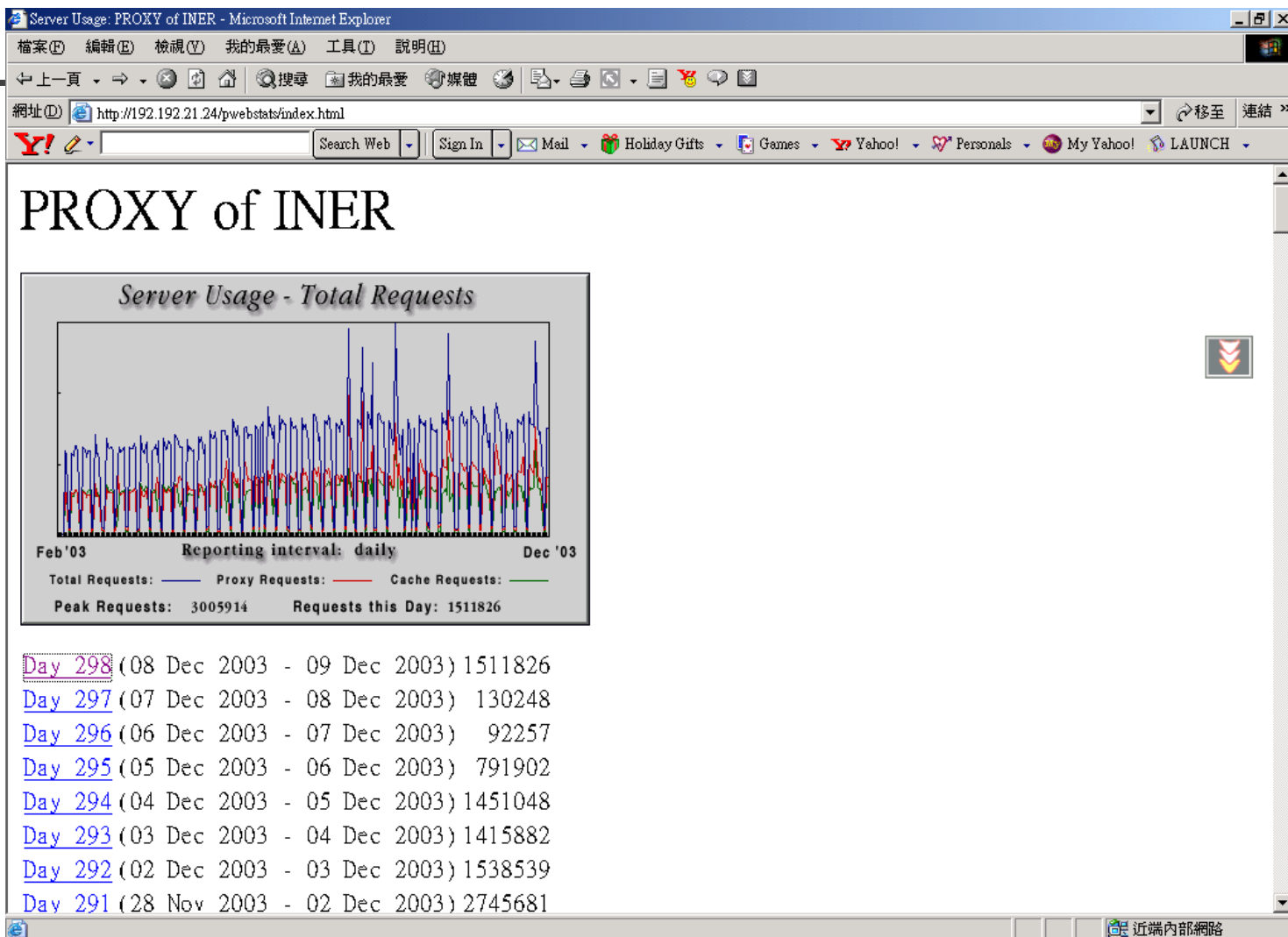
核能研究所區域網路架構



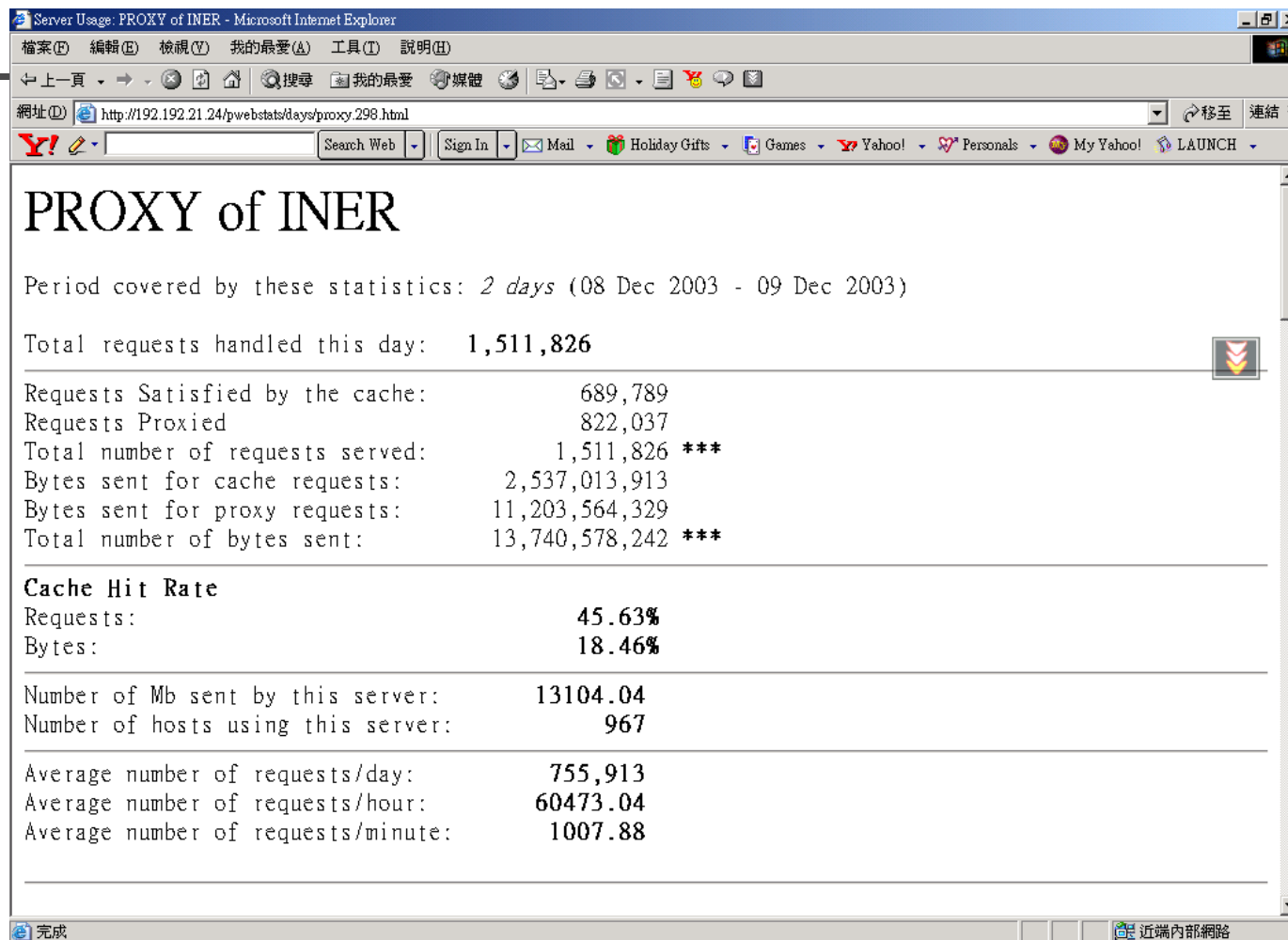
WWW Proxy 系統示意圖



代理伺服器Log分析(一)



代理伺服器Log分析(二)



網路連通狀況

最新連通測試 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 下一頁 搜尋 我的最愛 媒體 列印 複製 貼上 取消 確定

網址(1) http://192.168.60.5/hello/result.html 移至 連結 >>

Y! Search Web Sign In Mail Holiday Gifts Games Yahoo! Personals My Yahoo! LAUNCH

各館網路最新連通狀況

 目前每小時0,15,30,45分，自動進行全所各館連通測試!

 [依日期查看連通記錄](#)

• 起: Wed Dec 10 08:15:00 2003 • 迄: Wed Dec 10 08:18:17 2003

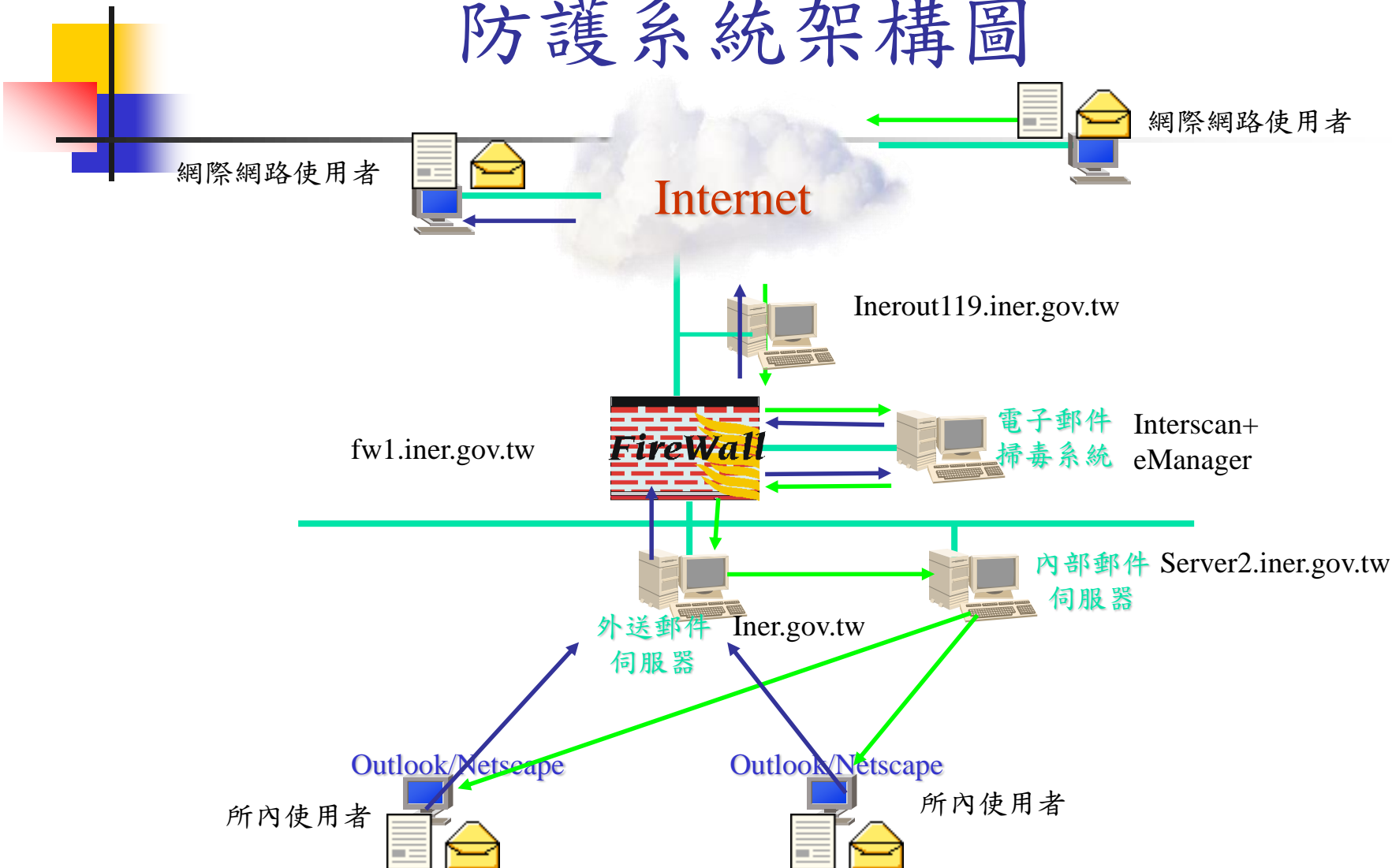
正常	001館(核儀組)	192.168.1.254 (5)
正常	002館(化學組)	192.168.2.254 (5)
正常	007館(化學組)	192.168.7.254 (5)
正常	016館(化學組)	192.168.16.254 (5)
正常	023館(化學組)	192.168.23.254 (5)
正常	003館(物理組)	192.168.3.254 (5)
正常	054館(物理組)	192.168.54.254 (5)
正常	027館1F(核工組)	192.168.27.254 (5)
正常	027館2F(核工組、技轉中心、核安會)	192.168.127.254 (5)
正常	027館3F(核工組、TDR IT)	192.168.227.254 (5)

完成 近端內部網路

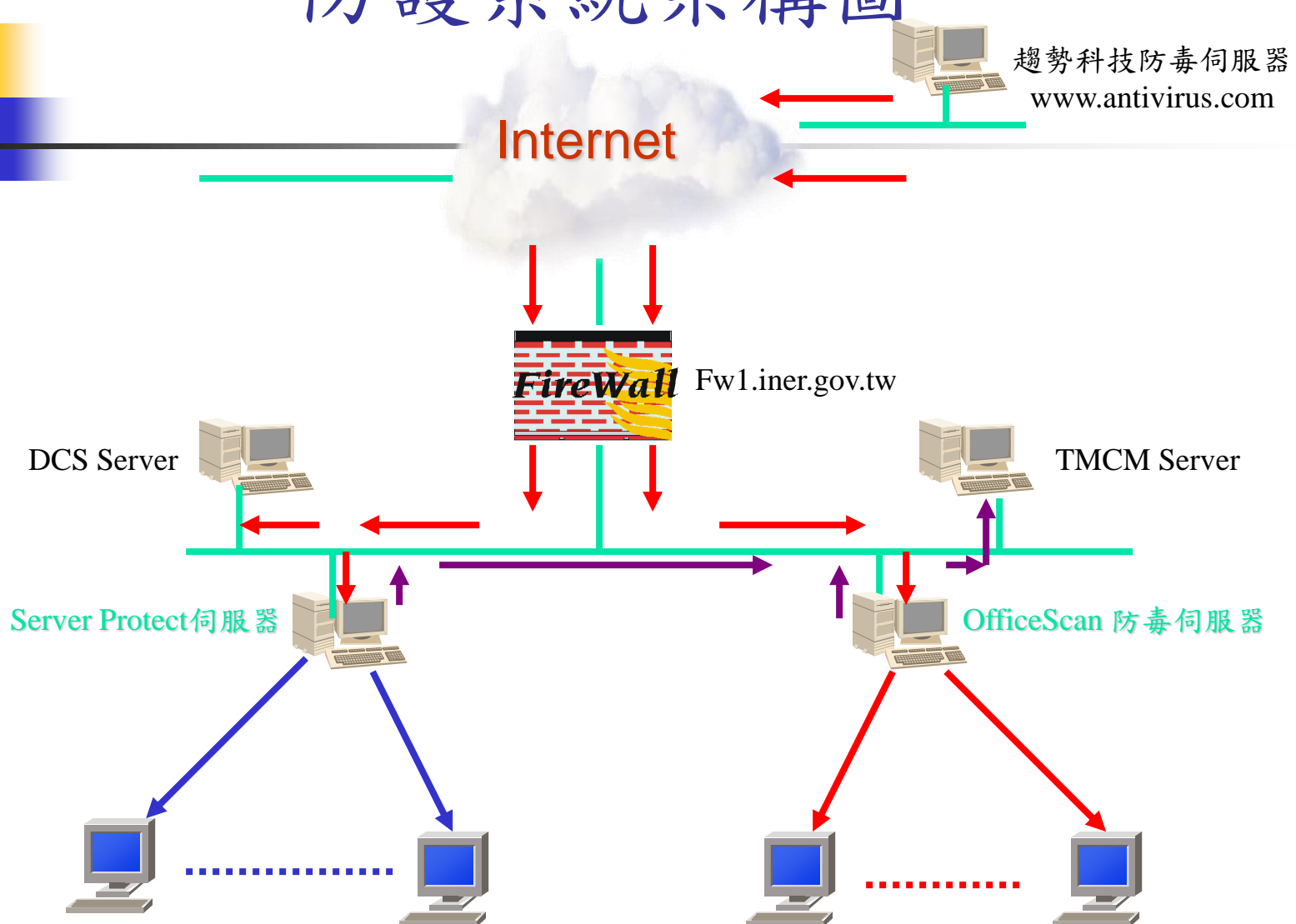
即時流量統計



核能研究所電子郵件安全防護系統架構圖



核能研究所中央控管安全 防護系統架構圖



TMCM監控畫面

Trend Micro Control Manager 2.5 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

↔ 上一頁 → 下一頁 ↻ 搜尋 我的最愛 媒體

網址(UD) http://192.192.21.70/controlmanager/cgi-bin/dm_htmlpage.cgi.exe?pageid=1&mrf_ip=localhost&mrf_inner_port=10198&mrf_outer_port=10319&security_level=2&random=8! 移至 連結 >>

Y! Search Web Sign In Mail Holiday Gifts Games Yahoo! Personals My Yahoo! LAUNCH

TREND MICRO Control Manager Outbreak Alert Help | Support | Security Info | About

Home | Outbreak Commander | Products | Computers | Reports | Administration

Signed in as: i0334 | [Sign Out](#)

Home

Welcome i0334

The last time you logged on was 2003/12/10 上午 11:30:36.

[View my account](#)

Security Information and News
[Virus Information Center](#)
[Knowledge Base](#)

Status Summary **Outbreak Alert** **Reports**

Change summary to

Summary from 2003-12-10 00:00:00 to 2003-12-10 11:33:01

Antivirus Summary

Action	Cleaned	Deleted	Quarantined	Passed	Renamed	Other	Failed	Total
Virus count	0	5	0	0	0	0	6	11

Content Security Summary

Action	Deleted Attachment Stripped	Forwarded	Delivered	Postponed	Quarantined	Other	Total
Violation count	0	0	0	0	0	0	0

Web Security Summary

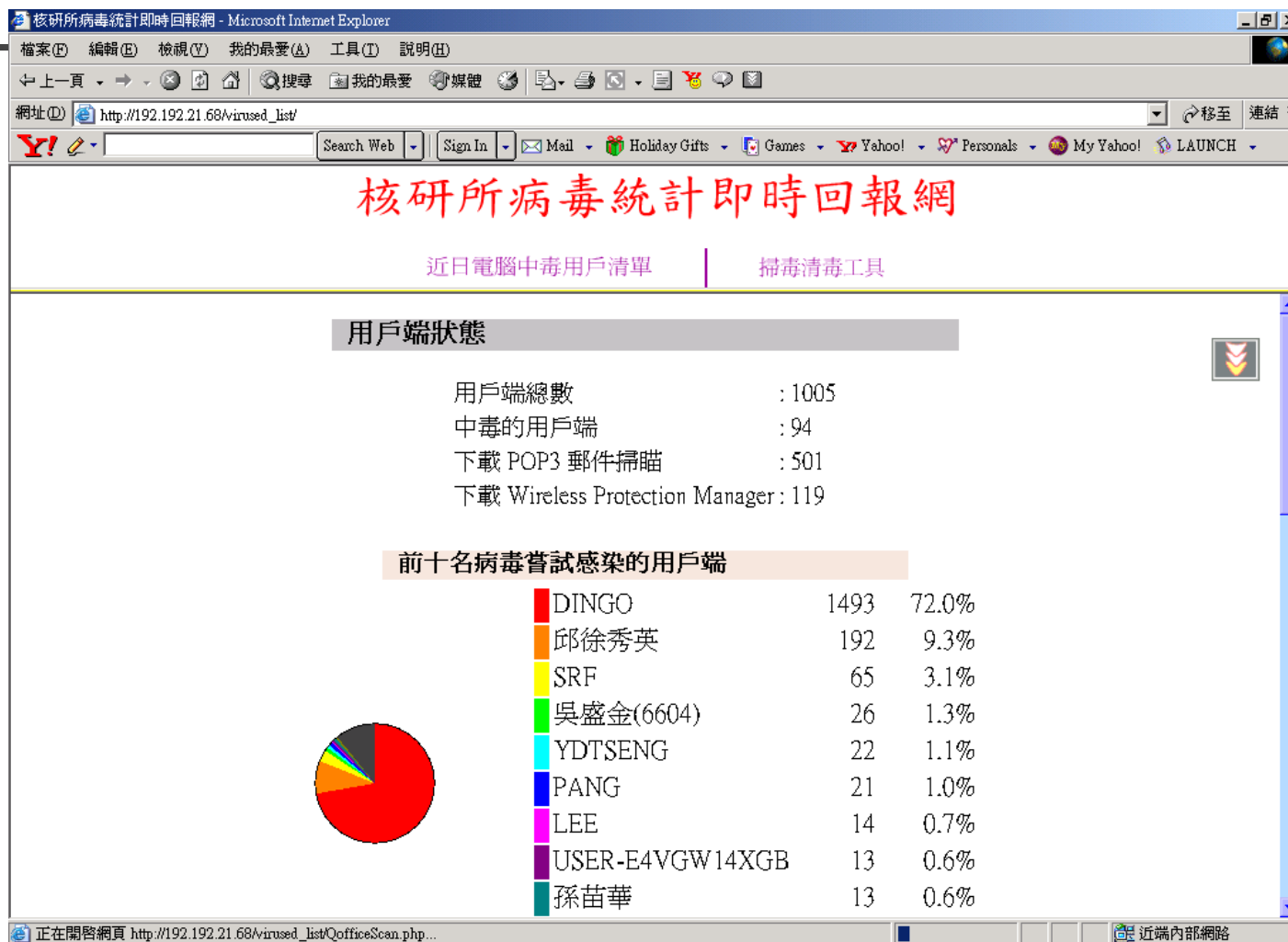
Action	File Name	Web Mail Site	Web Server	URL Pattern	Java/VB Script	True File Type	User Defined	Other	Total
Violation count	0	0	0	0	0	0	0	0	0

Component Status

Component	Latest Version	Out-of-date	Current	Total
Virus pattern	698	8	23	31
Spam Rule	225	0	0	0
Scan engine	VxD 6.810	0	1	1
	32 bit DLL(NT/2000) 6.810	0	0	0

近端內部網路

病毒即時回報



疑似中毒機器名單

核研所病毒統計即時回報網 - Microsoft Internet Explorer

檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)

← 上一頁 → 搜尋 我的最愛 媒體

網址(1) http://192.192.21.68/virusd_list/ 移至 連結 ×

Y! Search Web Sign In Mail Holiday Gifts Games Yahoo! Personals My Yahoo! LAUNCH

核研所病毒統計即時回報網

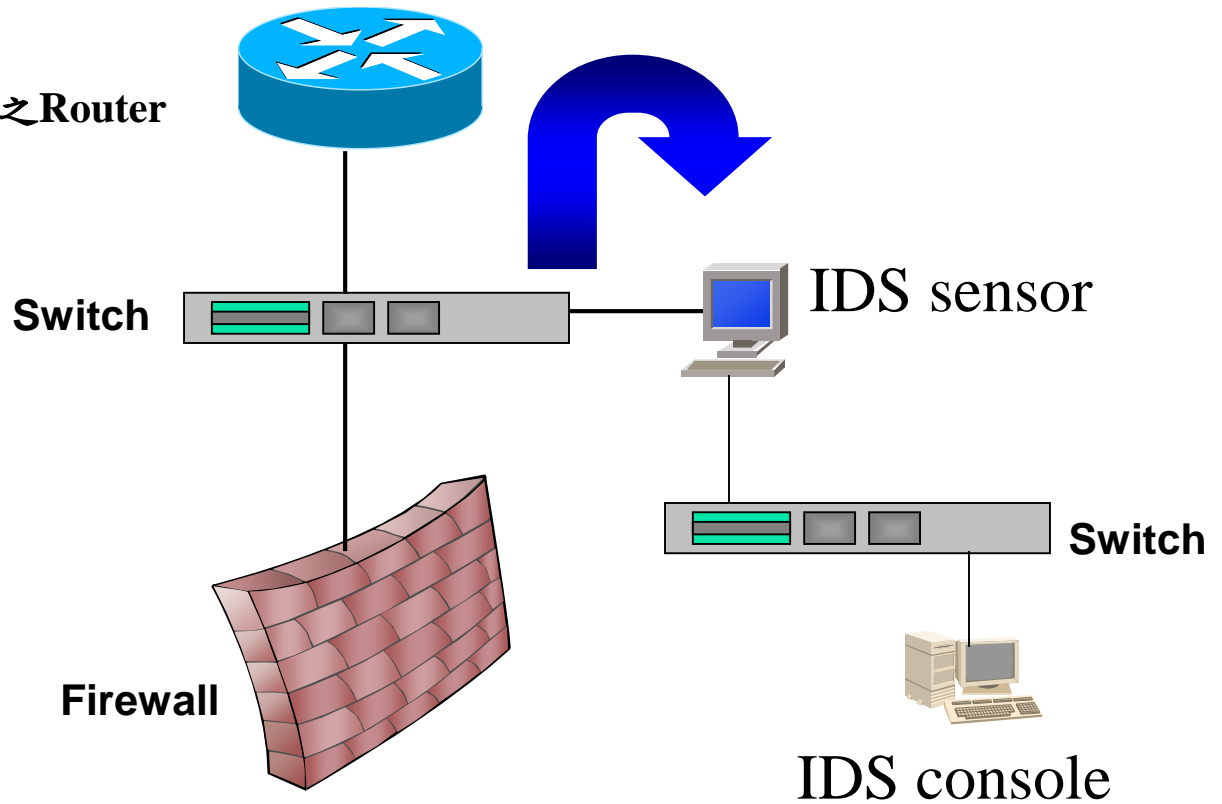
近日電腦中毒用戶清單 | 掃毒清毒工具

用戶端	平台	網域	程式	病毒碼檔案	掃描引擎	通訊協定	允許掃描設定	允
027ZTB5LP4PJ4P7(192.168.37.9)	Windows NT 5.1.2600	Workgroup	5.5	694	6.81 HTTP-based	否		否
ABC-SWFMCO84DHE(192.168.5.140)	Windows NT 5.1.2600	Workgroup	5.5	694	6.81 HTTP-based	否		否
ADMINIST-8B619C(192.168.1.72)	Windows NT 5.0.2195	D-sdg_1	5.5	694	6.81 HTTP-based	否		否
ASUS(192.168.5.141)	Windows NT 5.1.2600	Workgroup	5.5	694	6.81 HTTP-based	否		否
CHAOHO-LEE(192.168.1.68)	Windows NT 5.1.2600	Vnv	5.5	690	6.81 HTTP-based	否		否
CHEN(192.168.28.62)	Windows NT 5.0.2195	燃材組(028)	5.5	694	6.81 HTTP-based	否		否
CHING-LUNHUANG(192.168.42.8)	Windows NT 5.1.2600	Workgroup	5.5	694	6.81 HTTP-based	否		否
COLINV(192.168.62.43)	Windows NT 5.1.2600	Mshome	5.5	694	6.81 HTTP-based	否		否
CORNUCOPIA(192.168.1.79)	Windows NT 5.1.2600	D-sdg	5.5	694	6.81 HTTP-based	否		否
CPQ32548872431(192.168.35.18)	Windows NT 5.1.2600	Mshome	5.5	694	6.81 HTTP-based	否		否
DILEE(192.168.5.53)	Windows NT 5.1.2600	工程組	5.5	694	6.81 HTTP-based	否		否
ECS-8VX6AD2WZPK(192.168.62.23)	Windows NT 5.1.2600	Workgroup	5.5	690	6.81 HTTP-based	否		否
F18(192.168.52.57)	Windows NT 5.1.2600	Workgroup	5.5	694	6.81 HTTP-based	否		否
F1T5Z8(192.168.227.51)	Windows NT 5.0.2195	保物環境分組	5.5	694	6.81 HTTP-based	否		否
FCLIN1(192.168.54.22)	Windows NT 5.0.2195	Uhv	5.5	694	6.81 HTTP-based	否		否
HHH24G(192.168.8.123)	Windows NT 5.1.2600	Diydiy	5.5	694	6.81 HTTP-based	否		否
HPIC(192.168.8.241)	Windows NT 5.0.2195	保物環境分組	5.5	694	6.81 HTTP-based	否		否
HPWORKSTATION(192.168.227.30)	Windows NT 5.1.2600	工程力學	5.5	694	6.81 HTTP-based	否		否
HUCC1231(192.168.10.30)	Windows NT 5.1.2600	工程組	5.5	690	6.81 HTTP-based	否		否
I-EKSTTNERYN1QF(192.168.42.155)	Windows NT 5.0.2195	Workgroup	5.5	690	6.81 HTTP-based	否		否

完成 近端內部網路

本所IDS 部署架構(Mirror Port)

連接中央大學之Router



入侵偵測系統監控畫面

RealSecure Console - INER.rse

File View Activity Window Help

Active Events (31 events)

- HTTP_Code_Red_II (5 events)
 - 24.214.126.87 (1 event)
 - 193.159.185.2 (1 event)
 - 211.93.160.210 (1 event)
 - 218.108.44.90 (1 event)
 - 219.95.194.7 (1 event)
- EventCollector_Error (1 event)
 - 192.168.61.59 (1 event)
- HTTP_POST_repeated_char (1 event)
 - 212.242.117.112 (1 event)
- Ping_Sweep (15 events)
 - 0.0.0.0 (1 event)
 - 24.123.116.77 (1 event)
 - 61.158.73.8 (1 event)
 - 61.223.159.128 (1 event)
 - 63.231.132.97 (1 event)
 - 192.192.6.8 (1 event)
 - 192.192.164.166 (1 event)
 - 192.192.167.108 (1 event)
 - 192.192.230.71 (1 event)
 - 192.192.237.79 (1 event)
 - 192.192.237.80 (1 event)
 - 192.192.237.189 (1 event)
 - 192.192.237.191 (1 event)
 - 192.192.237.226 (1 event)
 - 218.102.118.102 (1 event)
- Fragment_Differential_Size (2 events)

Source Destination Events

High Priority

Sensor	Event	From	To	Info
network_sensor_1@192.168.61.60	HTTP_Code_Red_II	193.159.185.2	192.192.21.1	URL - /de
event_collector_1@127.0.0.1	EventCollector_Error	192.168.61.59	192.168.61.59	Message -
event_collector_1@127.0.0.1	EventCollector_Error	192.168.61.59	192.168.61.59	Message -
event_collector_1@127.0.0.1	EventCollector_Error	192.168.61.59	192.168.61.59	Message -

Medium Priority

Sensor	Event	From	To	Info
network_sensor_1@192.168.61.60	Ping_Sweep	192.192.164.1...	192.192.0.0	victim-ip-addr - 192.192.0
network_sensor_1@192.168.61.60	Ping_Sweep	24.123.116.77	192.192.0.0	victim-ip-addr - 192.192.0
network_sensor_1@192.168.61.60	Ping_Sweep	192.192.6.8	192.192.0.0	victim-ip-addr - 192.192.0
network_sensor_1@192.168.61.60	Ping_Sweep	192.192.6.8	192.192.0.0	victim-ip-addr - 192.192.0

Low Priority

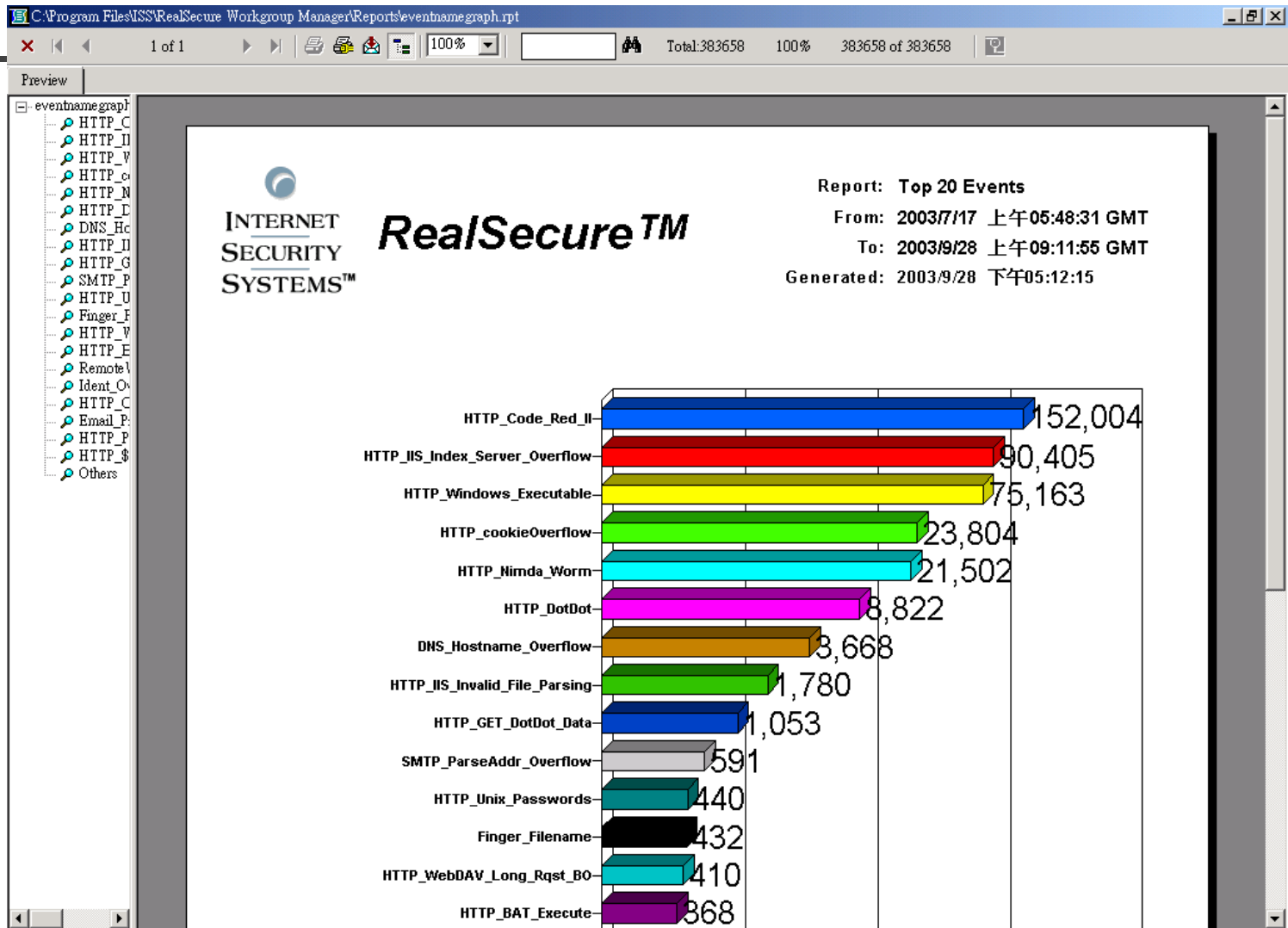
Sensor	Event	From	To	Info	Date
network_sensor_1@192.168.61.60	Fragment_Differential...	80.11.164.107	192.192.24.216	was - 16404	2003/09/28
network_sensor_1@192.168.61.60	TCP_Service_Sweep	192.192.26.110	207.115.0.0	port - 25	2003/09/28
network_sensor_1@192.168.61.60	DNS_Malformed	61.218.112.138	192.192.21.1	victim-ip-ad...	2003/09/28
network_sensor_1@192.168.61.60	DNS_Malformed	61.218.112.138	192.192.21.1	victim-ip-ad...	2003/09/28

Managed Assets

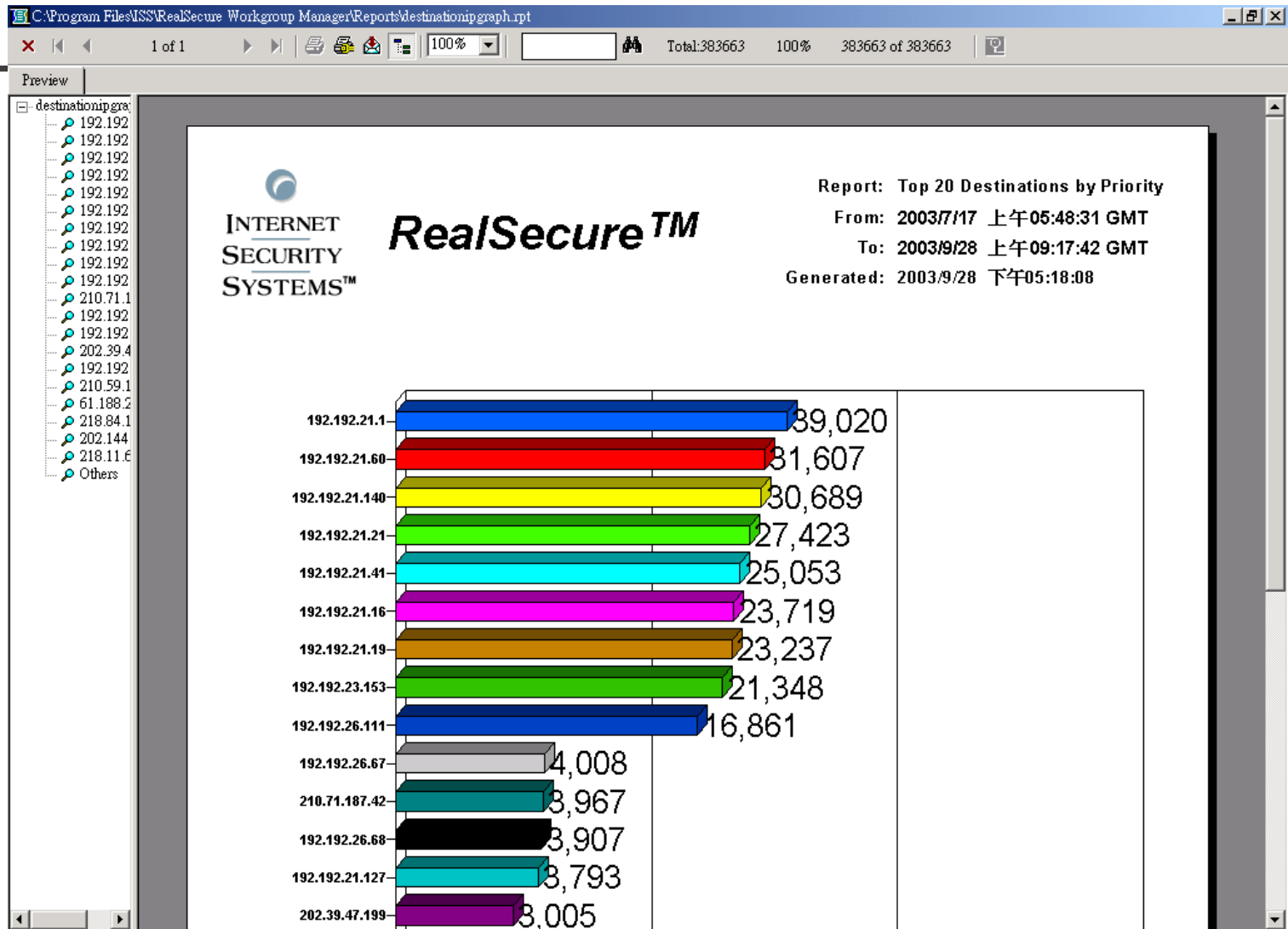
Asset	Event Collector
Component St...	Event Status
Location	Version
Policy	Master
Database	
127.0.0.1	6.5.2003.34 (SR 1.5)
192.168.61.60	7.0.2002.155 (MU 21.2)
192.168.61.60	7.0.2002.155 (MU 21.2)
192.168.61.60	7.0.2002.155 (MU 21.2)

Ready NUM

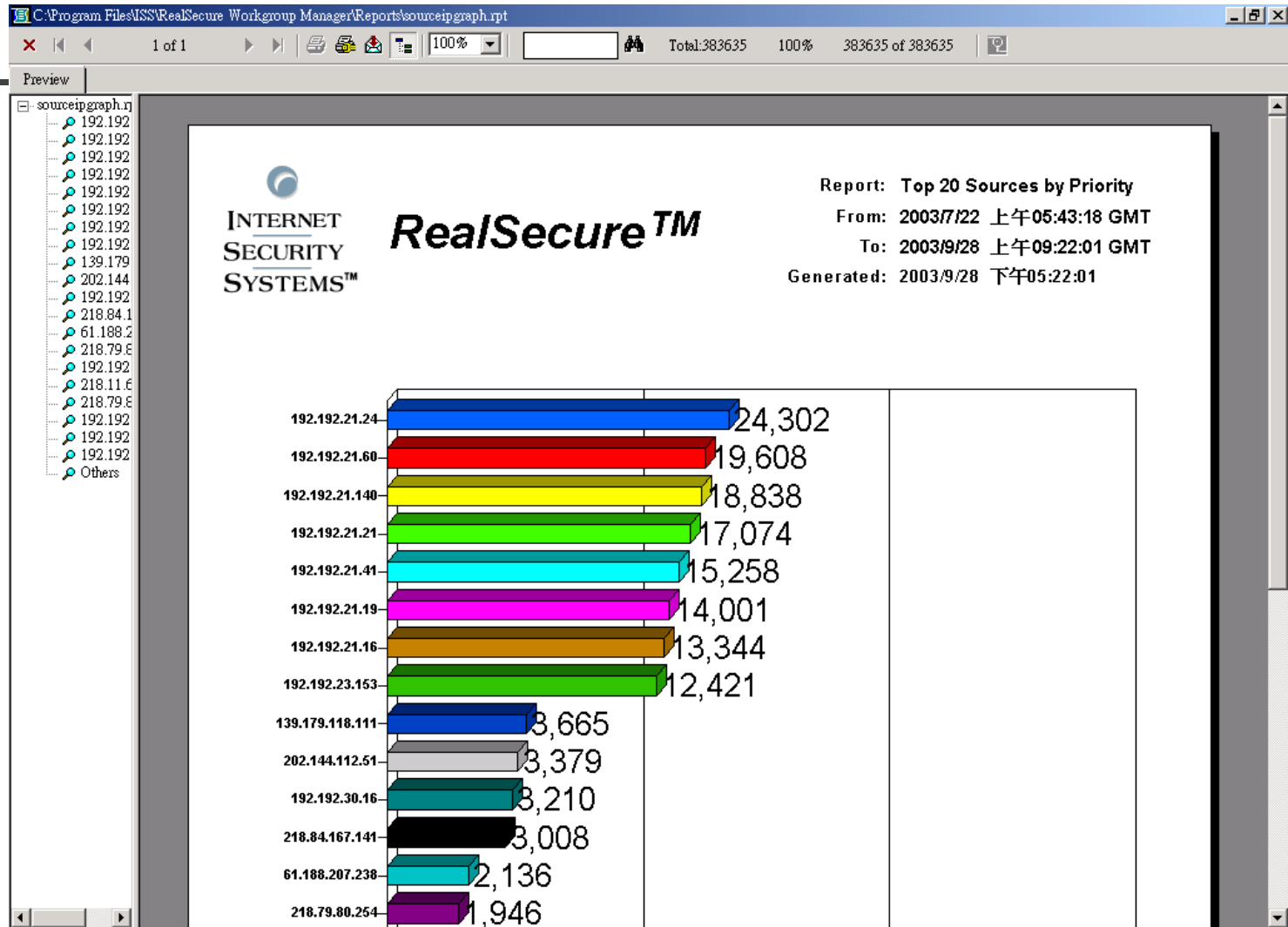
Top 20 Events Graph(7/17-9/28)



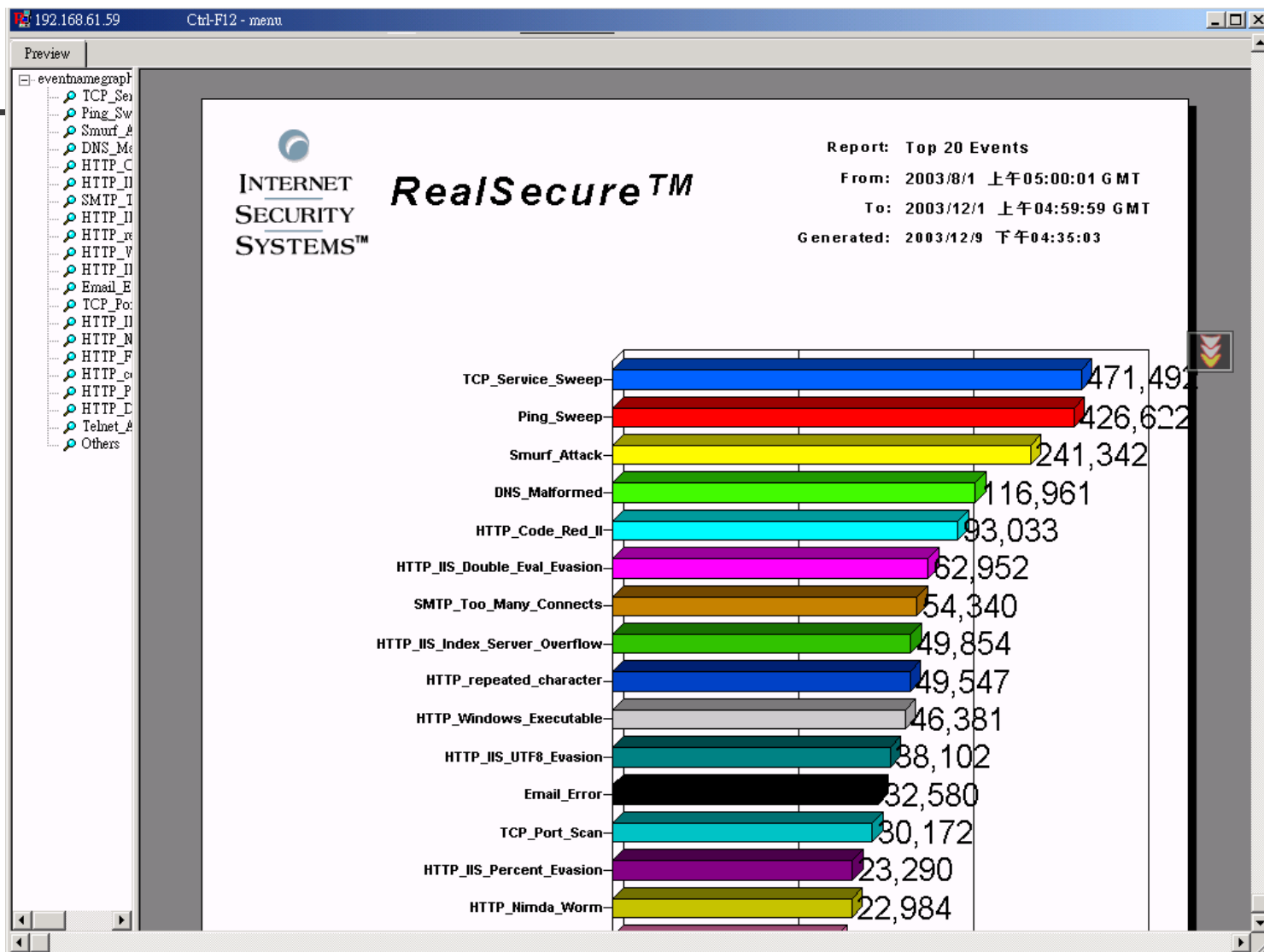
Top 20 Destinations Graph(7/17-9/28)



Top 20 Sources Graph(7/22-9/28)



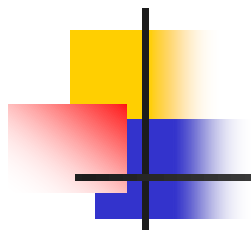
Top 20 事件(2003/08~11)





未來展望

- 強化不當資訊防治作為
- 杜絕可能的病毒來源(安裝SUS伺服器、IWSS及SPS)
- 導入頻寬管理系統
- 新一代所區網路架構設計



報告完畢
敬請指導