新生醫專
2018 網路資訊安全

簡報人員：忠明

簡報單位：精誠軟體服務

技術協助單位：三勝資訊

精誠軟體服務
SYSTEX Software & Service

Agenda

- 網路資訊安全-資訊分級作業
- 網路資訊防護
- 網路資訊通報
- 影片觀賞
- QA

精誠軟體服務
SYSTEX Software & Service

網路資訊安全-分級作業

精誠軟體服務
SYSTEX Software & Service

網路資訊安全－資訊分級作業

面向 / 作業名稱 / 等級	技術面		
	縱深防護	監控管理	安全性檢測
A	一、防毒、防火牆、郵件過濾裝置 二、IDS/IPS、Web應用程式防火牆 三、APT攻擊防禦設備或系統	SOC監控(104年底前) 結合臺灣學術網路或教育部資安監控系統機制	一、每年至少辦理2次網站安全弱點檢測 二、每年至少辦理1次系統滲透測試 三、每年至少辦理1次資安健診
B	一、防毒、防火牆、郵件過濾裝置 二、IDS/IPS 三、Web應用程式防火牆(機關具有對外服務之核心資訊系統或網站)	SOC監控(105年底前) 結合臺灣學術網路或教育部資安監控系統機制	一、每年至少辦理1次網站安全弱點檢測 二、每2年至少辦理1次系統滲透測試 三、每2年至少辦理1次資安健診
C	一、防毒 二、防火牆 三、郵件過濾裝置(機關具有郵件伺服器)	結合臺灣學術網路或教育部資安監控系統機制	核心業務如有運用資訊系統(或網站)，於系統建置或更新時，或每年至少辦理一次資安弱點檢測作業，並對弱點進行修復作業

精誠軟體服務
SYSTEX Software & Service

網路資訊安全－資訊分級作業

政府機關（構）資安責任等級

(一) 政府機關

1. A 級：總統府、國安會、立法院、司法院、考試院、監察院、行政院及直轄市政府。

2. B 級：縣（市）政府機關。

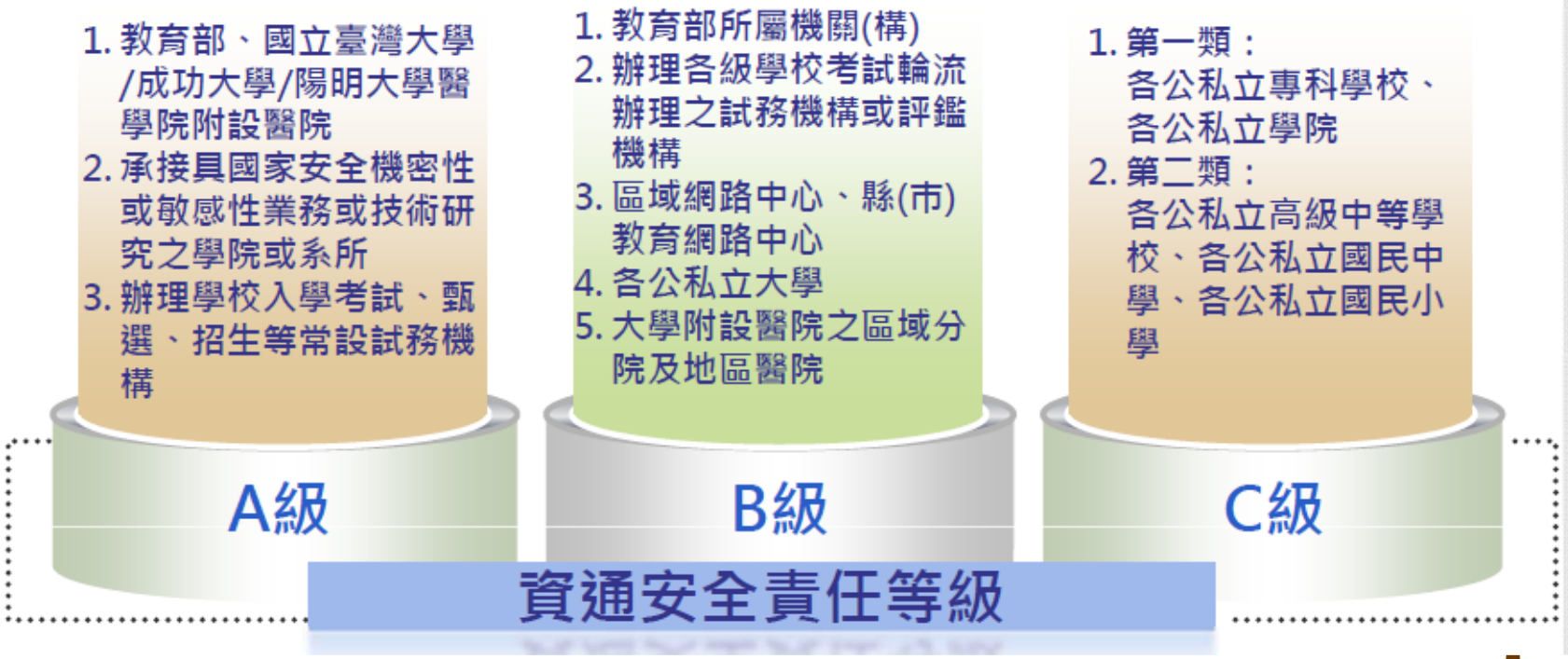
3. C 級：其他政府機關及地方政府民意機關。

精誠軟體服務
SYSTEX Software & Service

網路資訊安全－資訊分級作業

教育機關（構）資安責任等級

依行政院函頒之政府機關(構)資通安全責任等級分級作業規定，資通安全責任等級區分為A級、B級、C級等三級。



網路資訊安全－資訊分級作業

C 級網路分類職責				
項目	等　級	綜　深　防　護	數量	說明
1	C	資安負責人力 (兼任)	1	
2	C	ISMS 稽核方式	0	C 級網路，僅需辦理安全性自我檢查
3	C	安全性自我檢查： a. 網站弱點掃描 b. 資安健檢 (自我檢查)	1	a-b / 1次 / 年
4	C	資安教育訓練： a. 一般使用者與主管	3hrs	a / 1次3HRS / 年
5	C	防護縱深： a. 防火、毒牆 (AV、URL Filter、DLP、IPS) b. 垃圾信防護 (Spam Mail System)	1	具備防毒、火、IPS 等功能之防護設備
6	C	資安通報： a. 查詢並回應教育部、上層網路站(中央大學) 資安弱點通報及改善	1	

網路資訊安全防護

精誠軟體服務
SYSTEX Software & Service

網路資訊安全－基本防護

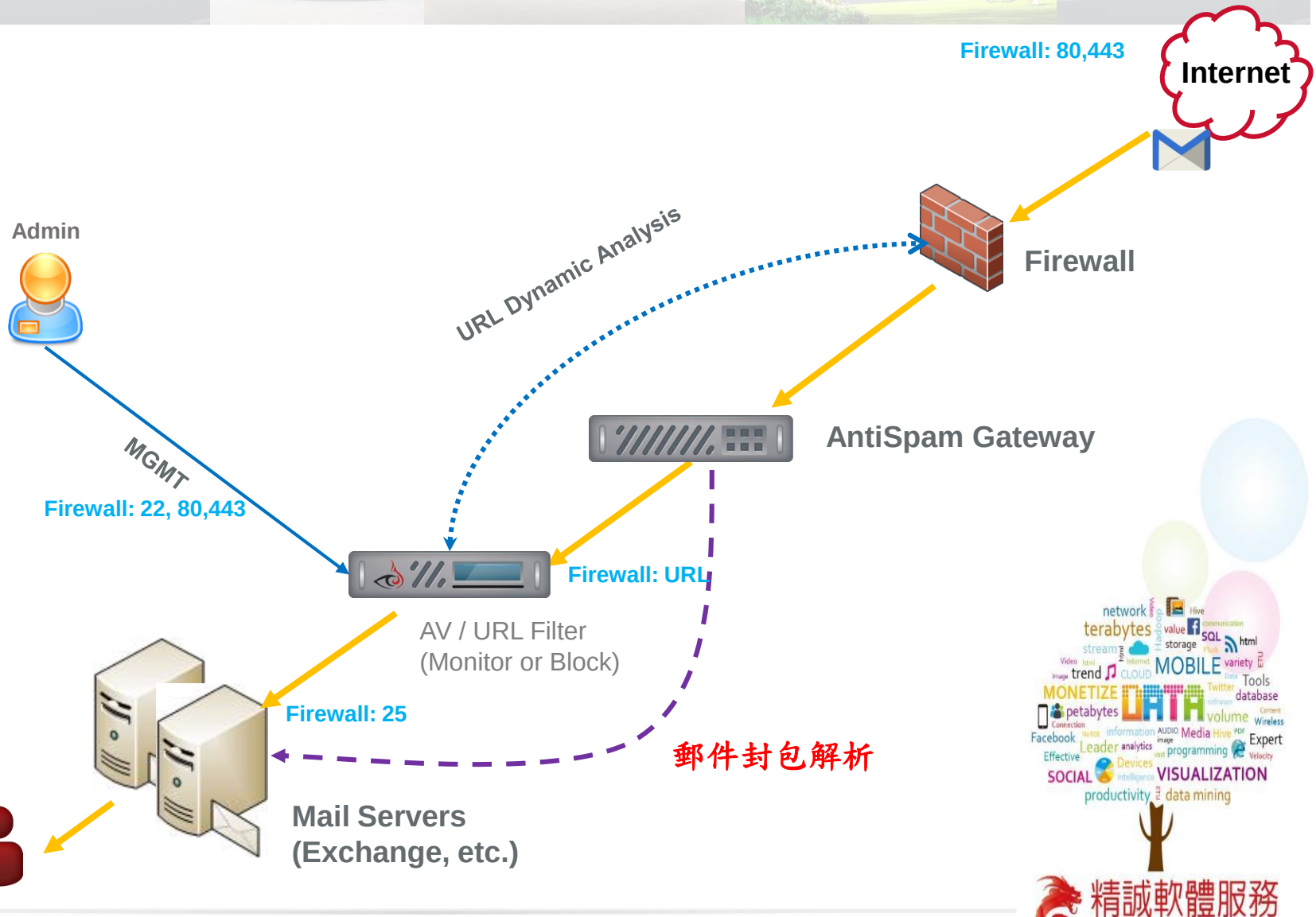

71
種
電腦操作行為全記錄
文件移動
遠端中斷
文件刪除
Exchange郵件
文件修改
文件下載
QQ
文件連接
軟體派送
使用者登入
設備控制策略
文件上傳
安全更新管理
遠端連接
使用者登出
POPO
共享文件刪除
Skype
共享印表機列印
Baidu Hi
UC
系統啟動
RTX
TM
共享文件新增
共享文件修改
文件重新命名
撥號
遠端控制策略
虛擬印表機列印
共享文件重新命名
日誌記錄策略
使用者登出
使用
文件新增
文件回復
網頁瀏覽
FETION
應用程式
止
隨身碟移除
螢幕記錄策略
基本策略
FeiQ
Yahoo
列印控制策略
LSC
文件複製
資產增加
文件連接
ALI
文件移動
文件移動
263EM
網頁郵件
一般郵件
ICQ
系統關閉
設備控制策略
資產變化
隨身碟移除
應用程式啟動
軟體派送
文件刪除
MSN
資產刪除
虛擬印表機列印
Lotus郵件
遠端連接
文件回復
共享印表機列印
日誌記錄策略
設備控制策略
文件連接
應用程式控制策略
Google Talk
撥號
體服務
SYSTEX Software & Service

網路資訊安全－資安防護

- 安全防護
- 應用程式
- 網頁瀏覽
- 稽核紀錄
- 文件操作
- 弱點修補
- 螢幕保護
- 遠端維護
- 郵件管控
- 移動儲存
- 網路管控
- 即時通訊

精誠軟體服務
SYSTEX Software & Service

網路資訊安全 –安全防護



精誠軟體服務
SYSTEX Software & Service

- **駭客首先入侵的是個人電腦**

萬惡根源-個人端點設備

從APT（進階持續性威脅），駭客有可能透過魚叉式釣魚郵件的方式，騙取點選連結下載木馬軟體，或破解系統密碼入侵並控制個人電腦後取得進入內網的能力。

網路資訊安全 –安全防護

FortiGate 800D HSC_FG800 admin

root

- Favorites
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report
  - Forward Traffic
  - Local Traffic
  - System Events
  - User Events
  - Web Filter
  - Learning Report
  - Local Reports

Add Filter | Log location: Disk | Details

#	Date/Time	Source	Destination	Application	Security Events	Result	Policy
1	10:41:37	213.202.225.59	163.25.34.15	SSH		Deny: policy violation	0 (Implicit Deny)
2	10:41:37	213.202.225.59	163.25.34.19 (edoc.hsc.edu.tw)	SSH		Deny: policy violation	0 (Implicit Deny)
3	10:41:37	46.17.102.130	163.25.34.151 (multiwork.hsc.edu.tw)	TCP/8536		Deny: policy violation	0 (Implicit Deny)
4	10:41:37	213.202.225.59	163.25.34.7	SSH		Deny: policy violation	0 (Implicit Deny)
5	10:41:37	46.17.102.130	163.25.34.244	TCP/4317		Deny: policy violation	0 (Implicit Deny)
6	10:41:37	213.202.225.59	163.25.34.25	SSH		Deny: policy violation	0 (Implicit Deny)
7	10:41:37	46.17.102.130	163.25.34.42	TCP/9501		Deny: policy violation	0 (Implicit Deny)
8	10:41:37	46.17.102.130	163.25.34.169	TCP/9666		Deny: policy violation	0 (Implicit Deny)
9	10:41:37	180.177.164.226	163.25.34.21 (elearning.hsc.edu.tw)	HTTP		907 B / 756 B	12
10	10:41:37	46.17.102.130	163.25.34.2 (www.hsc.edu.tw)	TCP/7760		Deny: policy violation	0 (Implicit Deny)
11	10:41:37	46.17.102.130	163.25.34.151 (multiwork.hsc.edu.tw)	TCP/7043		Deny: policy violation	0 (Implicit Deny)
12	10:41:37	46.229.168.70	163.25.34.91 (fms.hsc.edu.tw)	HTTP		1.07 kB / 15.83 kB	12
13	10:41:37	46.17.102.130	163.25.34.24	TCP/3427		Deny: policy violation	0 (Implicit Deny)
14	10:41:37	77.72.82.94	163.25.34.21 (elearning.hsc.edu.tw)	TCP/8823		Deny: policy violation	0 (Implicit Deny)
15	10:41:37	46.17.102.130	163.25.34.81 (ebook.hsc.edu.tw)	TCP/9076		Deny: policy violation	0 (Implicit Deny)
16	10:41:37	46.17.102.130	163.25.34.42	TCP/5894		Deny: policy violation	0 (Implicit Deny)
17	10:41:37	46.17.102.130	163.25.34.39	TCP/3541		Deny: policy violation	0 (Implicit Deny)
18	10:41:37	177.95.44.206	163.25.34.45	SCCP		Deny: policy violation	0 (Implicit Deny)

IP 213.202.225.59
Port 56011
Country Germany
Interface wan1 (External)

« ‹ 0 /0 › » [Total: 0]

網路資訊安全－資訊安全小提醒

- **系統設備 (Network Equipment)**
  - 採用較複雜 密碼，夾雜大小寫英文、數字及特殊符號
  - 密碼數不低於 8 碼
  - 不使用Browser Cache 記住密碼
  - 不使用生日、車牌等好記簡單密碼
  - 不使用 E-mail 傳送密碼

- **遠端維護 (Maintain from Remote)**
  - 進行遠端設備維護，禁用加密性低的程式 Telnet
  - 使用 Third Party 遠端連線軟體，使用完畢後，要立即關閉程式

精誠軟體服務
SYSTEX Software & Service

網路資訊安全－基本防護

郵件伺服器

- **散佈型病毒 ：**
  - 大量散佈惡意附檔
  - exe、scr、bat 等執行檔案
  - 帶有惡意、木馬、蠕蟲等
  - word、excel、pdf等文件檔案
  - 將上述病毒檔案壓縮，常見如zip、rar

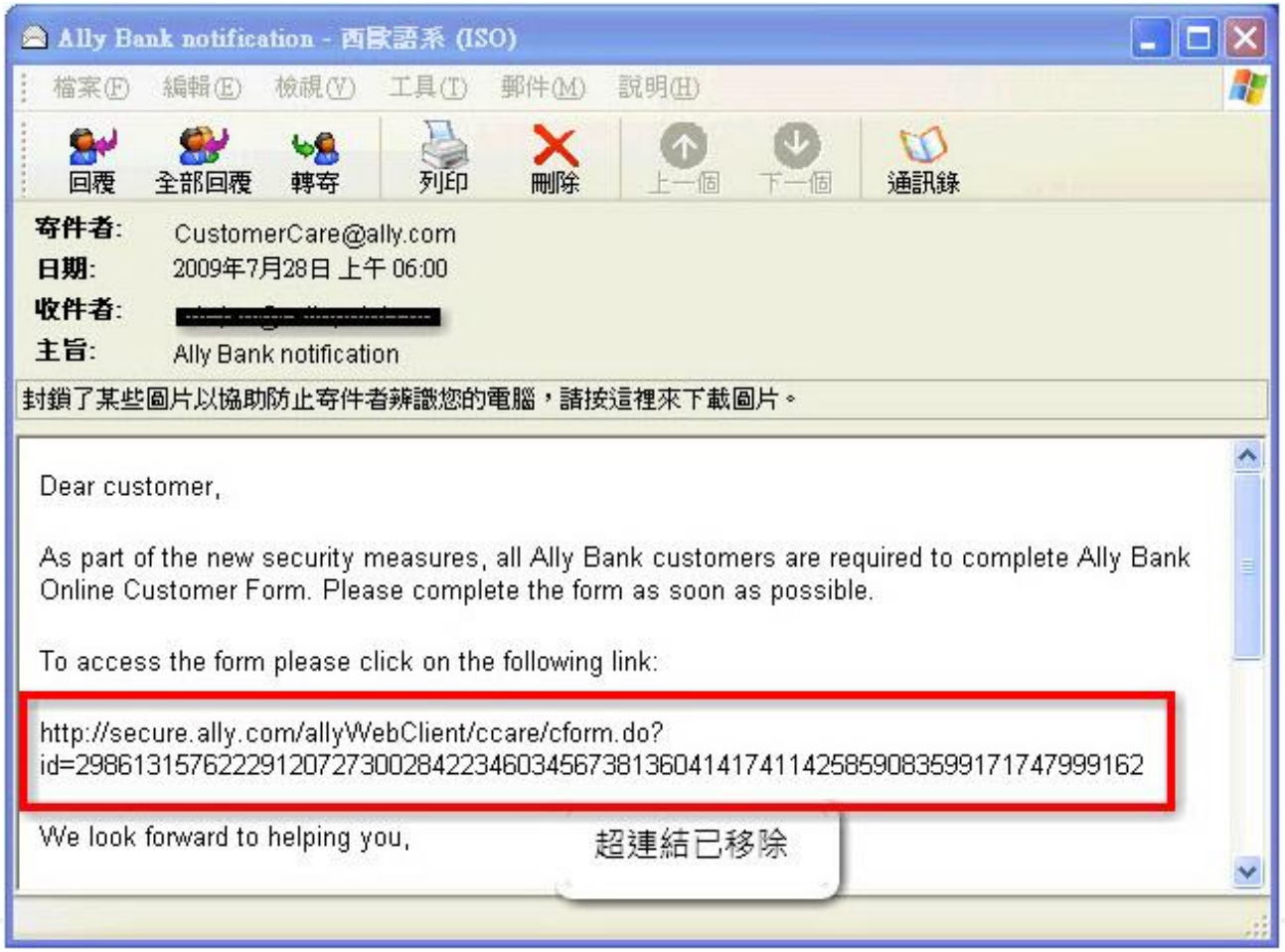
警報視窗
通知管理員

- **惡意連結：**
  - 連結隱含惡意行為
    - 連結下載惡意程式或檔案
    - 隱藏詐騙內容誘使點擊
    - 連結已被掛馬的正常網站

精誠軟體服務
SYSTEX Software & Service

網路資訊安全 –安全防護

- 駭客預先埋入 病毒 or 後門 URL 連結



精誠軟體服務
SYSTEX Software & Service

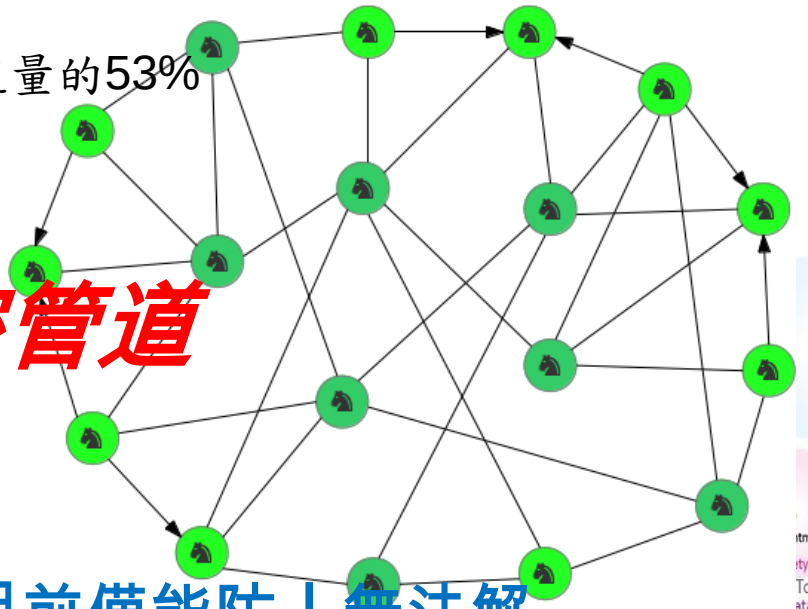
網路資訊安全－應用程式

- **惡意連結附件：**
  - 內含附件的連結惡意行為
  - 來路不明的郵件請勿開啟附件或觀看信件內容

P2P是駭客與病毒的溫床

佔據頻寬

據CNN報導，BT已經佔據了網路上所有P2P流量的53%



駭客入侵與洩密管道

資訊安全無法百分百解決！P2P目前僅能防！無法解

檔案分享：目前使用最多的應用，包括BT、eMule、eDonkey等。

精誠軟體服務
SYSTEX Software & Service

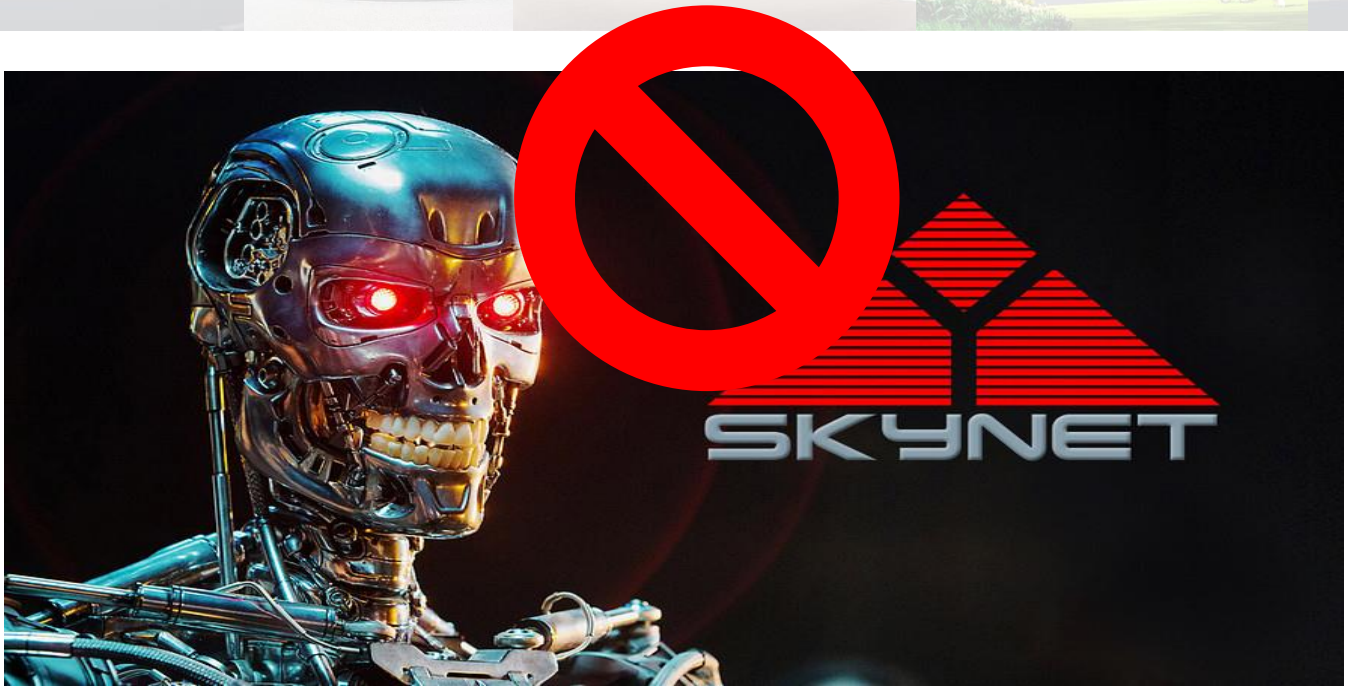
網路資訊安全 – 資訊通報

BT(BitTorrent)	找資源檔 (種子)
eMule:eMule： 中文叫騾子，是 eDonkey(驢子)的改良 eMule 可以設定下載上傳速率	找伺服器
Foxy 簡單易用，只要將主程式下載回硬碟，然後進行安裝後就可下載東西， 整個流程快速，比起 BT 要去找資源檔、eMule 要找伺服器，FOXY 不需任何設 定單靠一條搜尋列，就能輕鬆找到自己要的東西，方便程度可想而知	單-搜尋分享 / 也容易分享本地的檔案出去

大多數的P2P在散播過程中，並不需要規範 P2P檔案分享通訊協定埠
大都以自動化搜尋目前網路中，可使用之正常通訊協定，如 HTTP、HTTPS
P2P 程式，僅須提供一分享目錄，種子目錄、路徑等資訊即可上線

精誠軟體服務
SYSTEX Software & Service

網路資訊安全 – 資訊通報



GSN / 軍網 / 企業網路 @ 各為封閉網路
P2P 如何運作 ?!

精誠軟體服務
SYSTEX Software & Service

網路資訊安全 – 資訊通報

From: 桃園區網公告 [mailto:tanet_ncu@ncu.edu.tw]
Sent: Wednesday, March 22, 2017 4:37 PM
To: XXXX
Subject: [通知] [重要通知] CVE-2017-3881 - Cisco IOS and IOS XE Software Cluster Management Protocol Remote Code Execution Vulnerability

根據思科2017/03/17發佈的 CVE-2017-3881的訊息，攻擊者能夠透過這個漏洞經由Telnet來取得設備控制，執行惡意程式，或是刻意造成設備Reload

受影響之設備範圍非常廣 (Catalyst 2960, 3750, 3560等等)，其嚴重程度為 Critical

思科目前正在修正IOS/IOS XE並提供更新軟體版本來解決這個問題

針對這個漏洞，思科建議Disable Telnet及使用SSH，如無法關閉，建議採用ACL去限制設備存取

電話服務：週一至週五 08：00-17：00 03-4227151# 57555, 57566
網路電話(VoIP)：97820055、97820066
週一至週五 17：00-23：00　03-4227151# 57511
週六、日　9：00-16：00　03-4227151# 57511
Email 服務： tanet_ncu@ncu.edu.tw
桃園區網網址： http://www.tyrc.edu.tw

精誠軟體服務
SYSTEX Software & Service

網路資訊安全－資訊通報

以下何者屬於資安事件？(可複選)

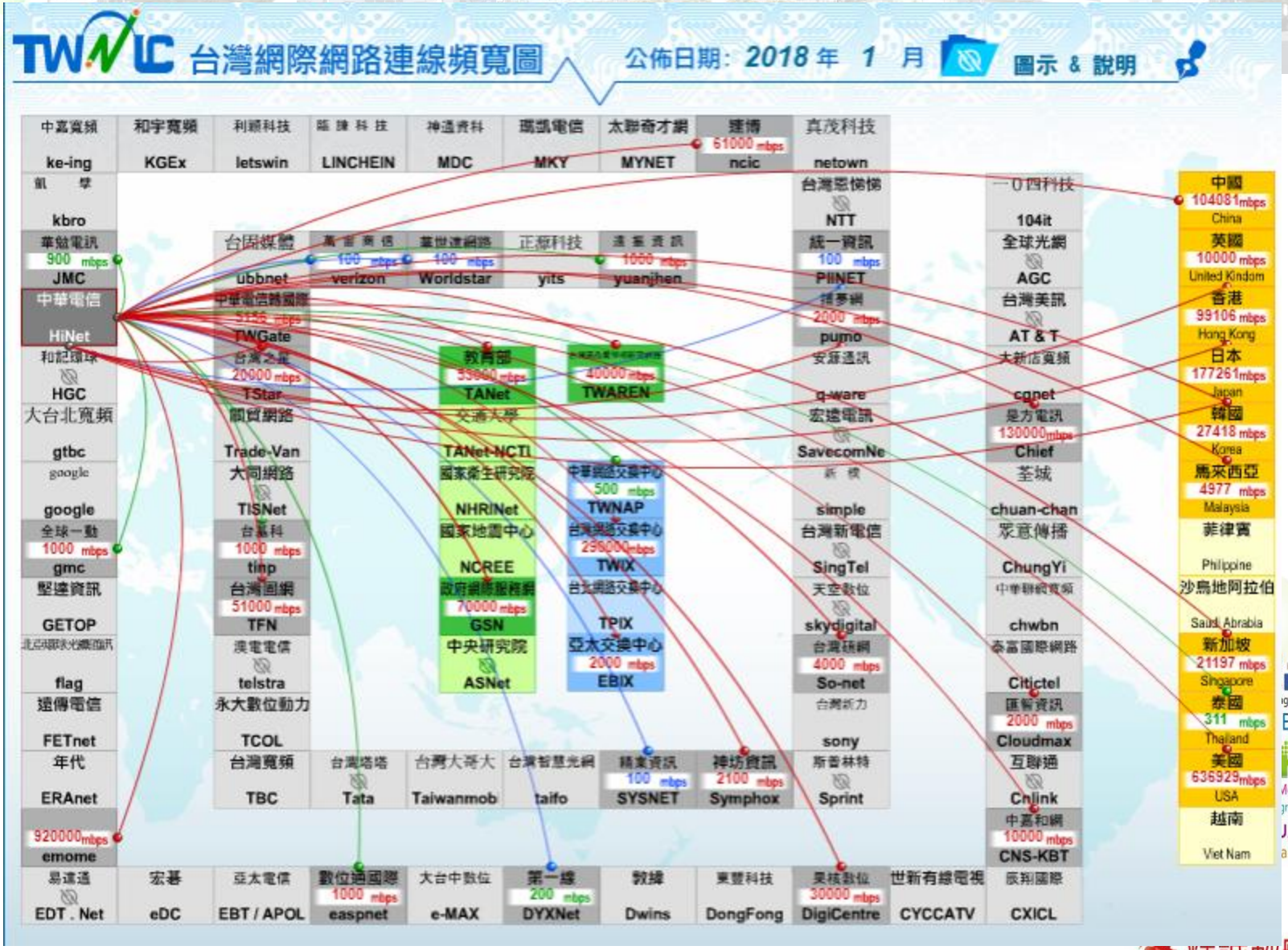
A. 資料詐欺或盜竊
B. 網路攻擊
C. 恐怖攻擊

正解：A、B

- Google公布Android 2017安全報告(March 23, 2018)
- 英國政府公布物聯網安全準則(March 20, 2018)
- 4G LTE協定存在多個漏洞(March 15, 2018)
- GitHub遭史上最大DDoS攻擊(March 12, 2018)
- 專家警告AI可能帶來的負面影響(March 8, 2018)
- 澳洲正式實施資料洩漏通知計畫(March 2, 2018)
- 美國情報機構公開不推薦民眾使用華為產品(February 23, 2018)
- 數以千計網站被植入挖礦軟體(February 21, 2018)
- 2017年醫療保健業遭勒索軟體攻擊之比例最高(February 13, 2018)
- Malwarebytes發布2017年資安報告(February 8, 2018)
- 美國參議院通過修正版FISA(February 5, 2018)

2

網路資訊安全－資訊通報



精誠軟體服務
SYSTEX Software & Service

網路資訊安全－資訊安全小提醒

Confidential Information Sharing

Chat Rooms

拒絕安裝P2P 軟體

File Transfer

IM Conversations

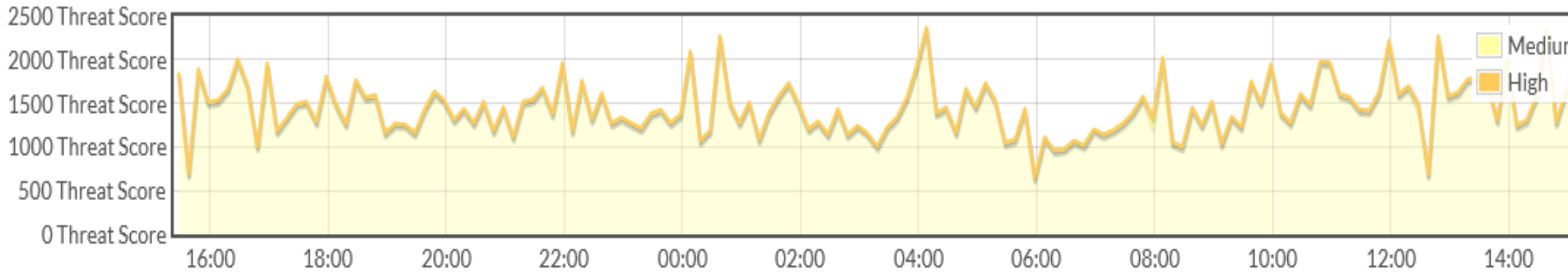
網路資訊安全－資訊通報

精誠軟體服務
SYSTEX Software & Service

網路資訊安全 – 資訊通報

Add Filter

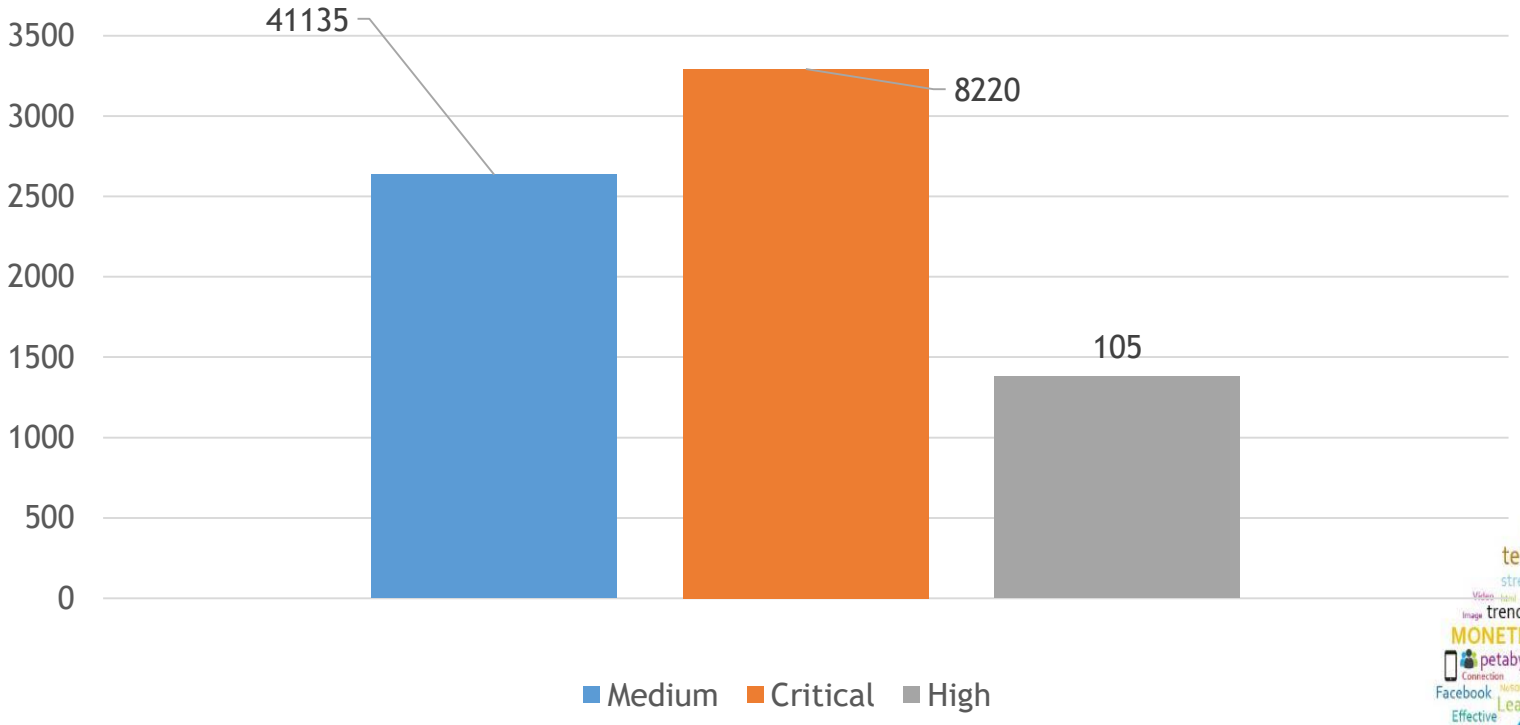
5 minutes | 1 hour | 24 hours



Threat	Category	Threat Level	Threat Score (Blocked/Allowed)	Sessions (Blocked/Allowed)
Failed Connection Attempts	Failed Connection Attempts	Medium	41135	8227
Blocked by Firewall Policy	Blocked by Firewall Policy	Critical	8220	274
payment.camerabay.tv	Pornography	High	105	3
kookporn.com	Pornography	High	70	2

精誠軟體服務
SYSTEX Software & Service

主機掃描結果風險統計



上網檢測分析說明

1. 利用 Threat 統計分析資料，Check 相關攻擊資訊

Summary of Blocked by Firewall Policy

Threat Score :	2925990
Sessions :	97,533
Time Period :	Last 24 Hours

來自外部攻擊

攻擊外部網站

Session Deny

Sources | Destinations | Countries | Sess...

Threat Type	Event	Date/Time	Source	Device	Destination	Application	Security Action	Sent / Received	Action
		15:38:54	191.101.167.235		163.25.34.85	TCP/8545		0 B / 0 B	deny
		15:38:54	181.214.87.88		163.25.34.171	TCP/433		0 B / 0 B	deny
		15:38:54	212.92.127.26		163.25.34.8 (mail.hsc.edu.tw)	TCP/42866		0 B / 0 B	deny
		15:38:54	181.214.87.89		163.25.34.188	TCP/1497		0 B / 0 B	deny
		15:38:52	123.152.104.159		163.25.34.85	TELNET		0 B / 0 B	deny
		15:38:51	77.72.82.92		163.25.34.11	TCP/22013		0 B / 0 B	deny
		15:38:51	46.17.102.130		163.25.34.154	TCP/451		0 B / 0 B	deny
		15:38:51	46.17.102.130		163.25.34.27 (od.epage.hsc.edu.tw)	TCP/8373		0 B / 0 B	deny
		15:38:51	198.20.70.114		163.25.34.33	X-WINDOWS		0 B / 0 B	deny
		15:38:50	89.248.172.16		163.25.34.10	TCP/17000		0 B / 0 B	deny

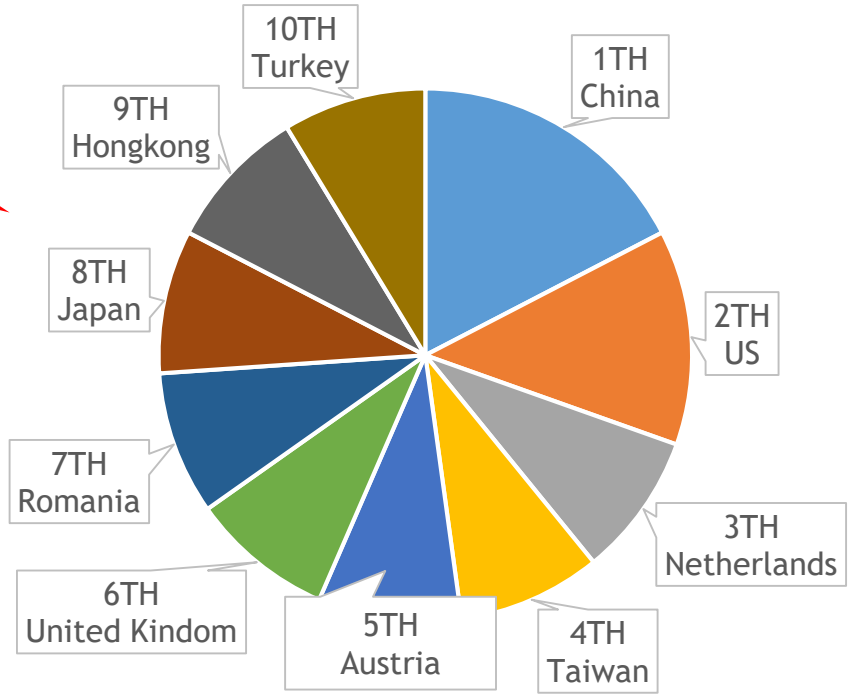
« ‹ 1 /7692 › » [Total: 384573]

防火牆

上網問題檢測分析說明

疑似駭客地理位址 TOP 10

TOP 10
疑似攻擊者果家



■ 1TH Random Port ■ 2TH Microsoft-ds ■ 3TH SSH/Telnet ■ 4TH Random Port

精誠軟體服務
SYSTEX Software & Service

網路資訊安全－資訊安全小提醒

- ✓ 儘可能關閉網路芳鄰服務
- ✓ 一段期間後更改網路、Server 密碼
- ✓ Server / Update Patch File
- ✓ 勿點選不明 URL 連結
- ✓ 儘量不使用無線網路分享
- ✓ 無線網路 AP 必須設定使用 WAP2 加密及密碼

精誠軟體服務
SYSTEX Software & Service

網路資訊安全 - 影片觀賞

Time 11:46
Artificial Intelligence
https://youtu.be/5J5bDQHQR1g

Time 11:56
The Dangers of Artificial Intelligence - Robot Sophia makes fun of Elon Musk - A.I. 2017
https://youtu.be/GzdY3gwE0WQ

Time 43:43
The World In 2050 [The Real Future Of Earth] - Full BBC Documentary HD(中文字幕)
https://youtu.be/f9d-5GnqEzs

精誠軟體服務
SYSTEX Software & Service

Thank You !

Q & A

精誠軟體服務
SYSTEX Software & Service