



大專校院校務資訊技術與經驗交流

資安業務

林瑞龍
教育部
106年6月23日

簡報綱要



政策目標及推動策略

技術防護及管理作業

臺灣學術網路資安事件統計

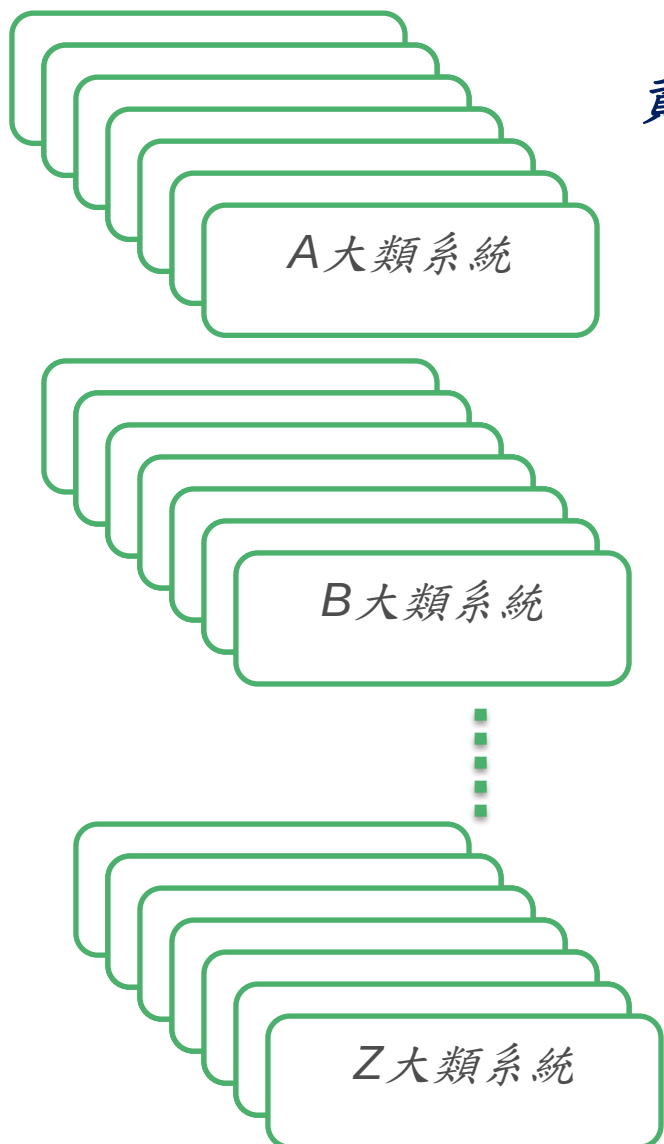
資安事件威脅分析

臺灣學術網路資安防護團隊

政策目標及推動策略(1/3)



資訊系統分類分級



政策目標及推動策略(2/3)



陽光普照，灑滿片地

重要服務
核心系統

部門參與度

資安人員認知

管理作業落實

技術防護完整

資
安
政
策

政策目標及推動策略(3/4)



1. 導入資訊安全管理
系統範圍適切性

新增：
資安治理

2. 機關首長對
資安業務支持度

新增：利害關係人管理

3. 資源投入
資安業務狀況

4. 資安業務運作
規劃與落實

策略
面

管理
面

技術面

5. 個人資料保護
與管理

6. 資訊資產管理
與風險評鑑

7. 人力資源管理

8. 資訊委外安全管理

9. 通訊與作業管理適切性與落
實執行狀況

新增：網路即時通訊安全、電子郵件安全

10. 資安事件通報
與管理

11. 資訊系統開發
與維護安全管理

資安治理架構流程構面

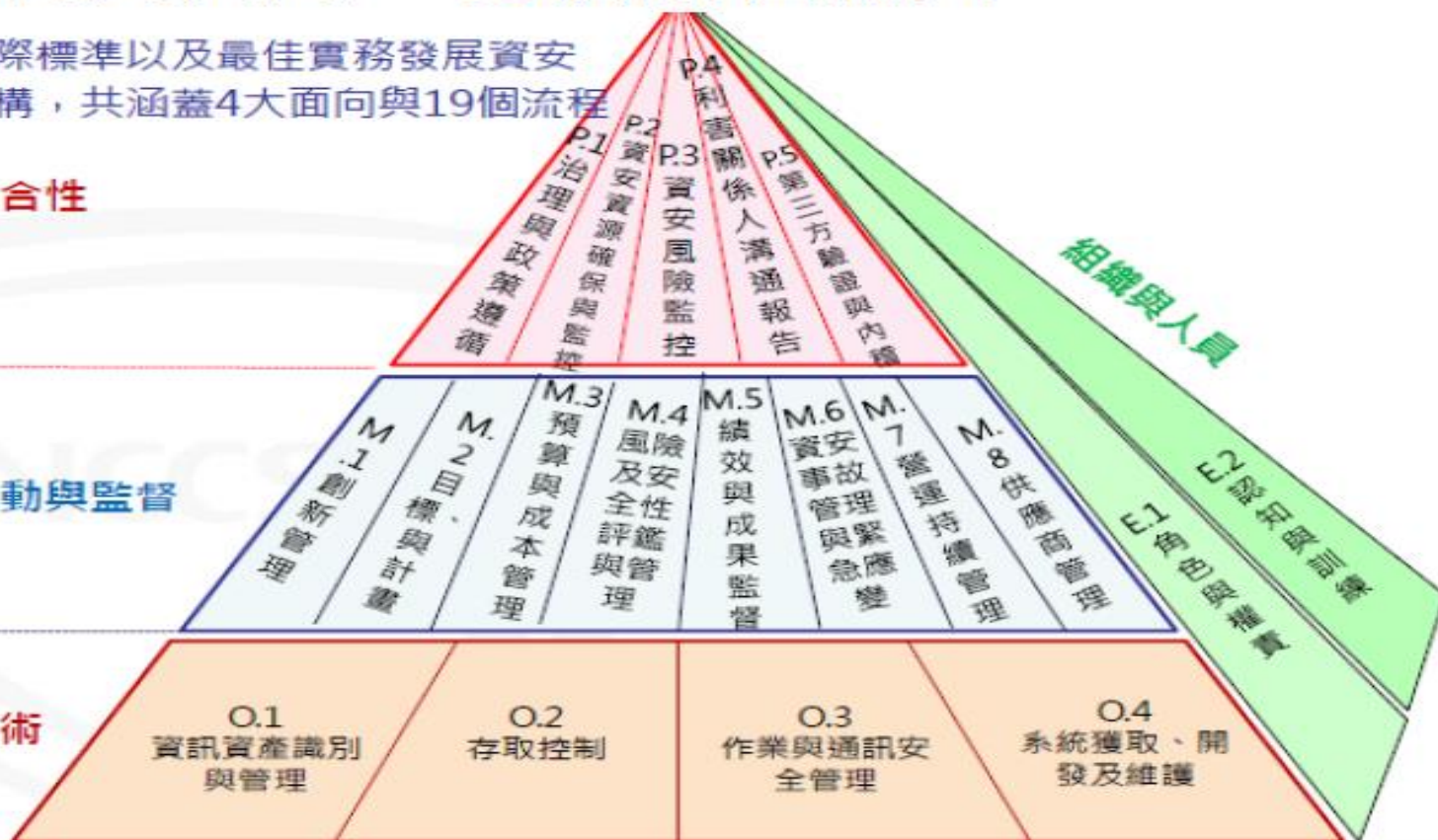
共涵蓋4大面向、**19**個流程構面

- 基於國際標準以及最佳實務發展資安治理架構，共涵蓋4大面向與19個流程構面

政策與符合性

規劃、推動與監督

作業與技術



技術防護及管理作業(1/3)



檢測作法



1.使用者電腦安全檢測

- 使用者電腦弱點掃描
- 使用者電腦安全防護檢測
- 組態設定安全防護檢測

針對**全機關進行PortScan**，挑選**50台使用者電腦**進行使用者電腦安全檢測，並挑選10台高風險之使用者電腦進行深度檢測



2.惡意中繼站連線阻擋檢測

- 一般機關使用者網段
- 核心系統管理員網段

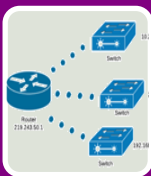
針對機關**使用者網段**及**核心系統管理員網段**之關鍵200筆名單進行檢測



3.核心資訊系統安全檢測

- 核心資訊系統內網滲透測試
- 系統防護檢測

針對機關核心資訊系統進行內網滲透測試，並針對**核心資訊系統之系統防護項目**進行檢測



4.網路架構檢測

- 網路與系統之管理控制措施
- 網路與系統之安全控制措施
- 網路與系統架構之備援機制
- 防火牆規則及存取控制

除透過訪談與實際檢視方式確認管理與防護情形之外，亦新增**網路設備SNMP設定**與**網路設備校時設定**等兩項檢測項目



5.AD主機安全防護檢測

- 防毒軟體
- 安全性修補程式更新檢視
- 組態設定項目

透過實際檢視方式，針對機關之AD主機進行防毒軟體、安全性修補程式更新及安全設定項目進行檢視

資料來源:行政院資通安全處

技術防護及管理作業(2/3)



❖ 總分 = 技術檢測 (30%) + 實地稽核 (70%)

項次	技術檢測項目	檢測子項	配分
1	使用者電腦安全檢測	使用者電腦弱點掃描	10
		使用者電腦安全防護檢測	20
		組態設定安全防護檢測	5
2	惡意中繼站連線阻擋檢測	惡意中繼站連線阻擋檢測	5
3	核心資訊系統安全檢測	核心資訊系統內網滲透測試	30
		系統防護檢測	10
4	網路架構檢測	網路架構檢測	10
5	AD主機安全防護檢測	AD主機安全防護檢測	10
合計			100

構面	實地稽核項目	配分
策略面 30	1.導入資訊安全管理系統範圍適切性	5
	2.機關首長對資安業務支持度	5
	3.資源投入資安業務狀況	5
	4.資安業務運作規劃與落實	15
管理面 30	5.個人資料保護與管理	10
	6.資訊資產管理與風險評鑑	8
	7.人力資源管理	5
	8.資訊委外安全管理	7
技術面 40	9.通訊與作業管理適切性與落實執行狀況	20
	10.資安事件通報與管理	10
	11.資訊系統開發與維護安全管理	10
合計		100

技術防護及管理作業(3/3)



//建設下世代智慧學習環境//



本部技術檢測結果

項次	技術檢測項目	檢測子項	配分
1	使用者電腦安全檢測	使用者電腦弱點掃描	10
		使用者電腦安全防護檢測	20
		組態設定安全防護檢測	5
2	惡意中繼站連線阻擋檢測	惡意中繼站連線阻擋檢測	5
3	核心資訊系統安全檢測	核心資訊系統內網滲透測試	30
		系統防護檢測	10
4	網路架構檢測	網路架構檢測	10
5	AD主機安全防護檢測	AD主機安全防護檢測	10
合計			100

沒發現問題

1000多台中1台更新漏3筆

沒發現問題

沒發現問題

1個高風險8個中風險1個低風險

圖形驗證碼無效

3最底層SWITCH密碼未設

1000多台中100項1筆未符

事件 來源 月份	self-report	告知通報										總計
		ABUSE	miniSOC	N-ASOC	S-ASOC	TACERT	Web-P	MJIB	NCCST	TW CERT	TW CSIRT	
105/05	39	4	44	1,087	1,557	10	0	37	9	10	0	2,797
105/06	45	7	73	1,729	988	10	0	12	2	11	0	2,877
105/07	36	2	69	939	533	3	2	21	2	9	0	1,616
105/08	22	3	70	1,071	723	17	0	31	4	17	0	1,958
105/09	27	1	45	2,323	1,324	3	0	65	1	10	0	3,799
105/10	14	0	86	2,531	1,255	8	0	26	0	9	0	3,929
105/11	36	0	125	1,912	1,204	18	0	20	0	13	0	3,328
105/12	26	0	65	1,741	1,179	8	0	8	0	5	0	3,032
106/01	10	3	39	409	613	5	7	32	5	6	0	1,129
106/02	22	1	30	453	786	5	7	46	0	2	0	1,352
106/03	40	0	128	1,860	1121	5	3	73	1	4	0	3,235
106/04	78	0	83	1,144	596	1	6	68	0	10	0	1,986
106/05	43	0	63	1,874	889	7	0	43	0	24	1	2,944
總計	438	21	920	19,073	12,768	100	25	482	24	130	1	33,982

*G-ISAC改名為「國家資通安全科技中心」，縮寫為NCCST

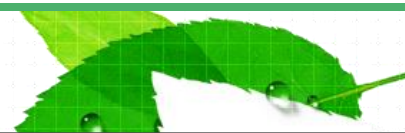
*106/5新增派單來源單位「臺灣電腦安全事件應變中心」，縮寫TWCSIRT



資安事件等級統計

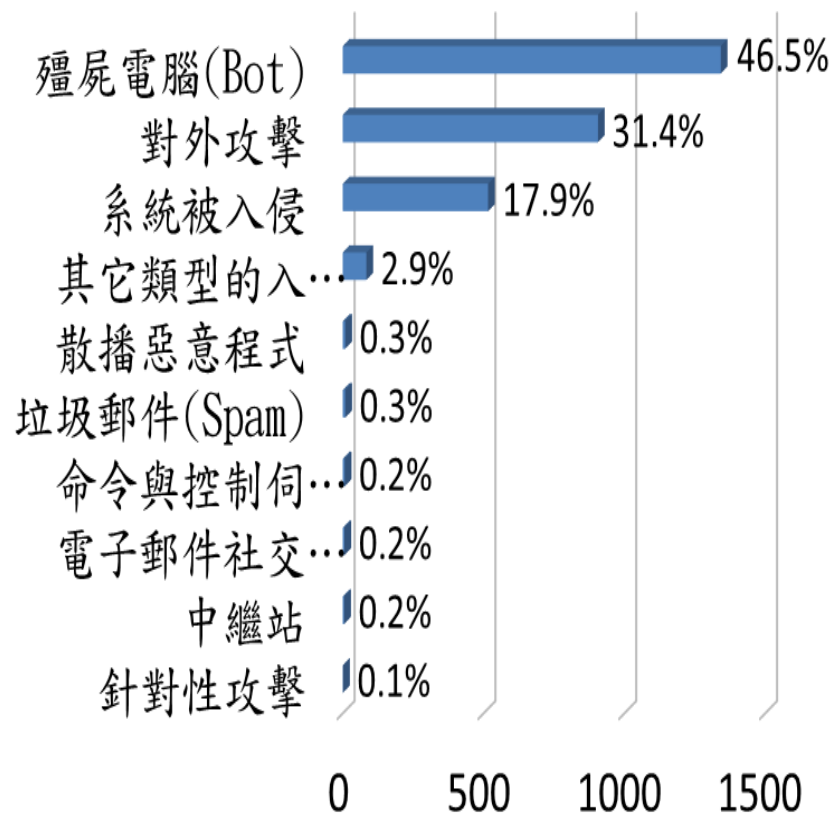
時間 / 通報來源 \ 事件類型		High		Medium	Low
		4級資安事件	3級資安事件	2級資安事件	1級資安事件
106年5月	self-report	0	1	1	41
	ABUSE	0	0	0	0
	miniSOC	0	0	0	63
	N-ASOC	0	0	0	1,874
	S-ASOC	0	0	1	888
	TACERT	0	0	0	7
	Web-P	0	0	0	0
	MJIB	0	0	0	43
	NCCST	0	0	0	0
	TWCERT/C C	0	0	0	24
	TWCSIRT	0	0	0	1

資安事件類型統計(INT)



事件類型	子類別	數量
入侵攻擊(INT)	殭屍電腦(Bot)	1342
	對外攻擊	906
	系統被入侵	516
	其它類型的入侵攻擊	84
	垃圾郵件(Spam)	9
	散播惡意程式	9
	命令與控制伺服器(C&C)	7
	電子郵件社交工程攻擊	6
	中繼站	5
	針對性攻擊	1
	總計	2,885

入侵攻擊(INT)子類型比率圖



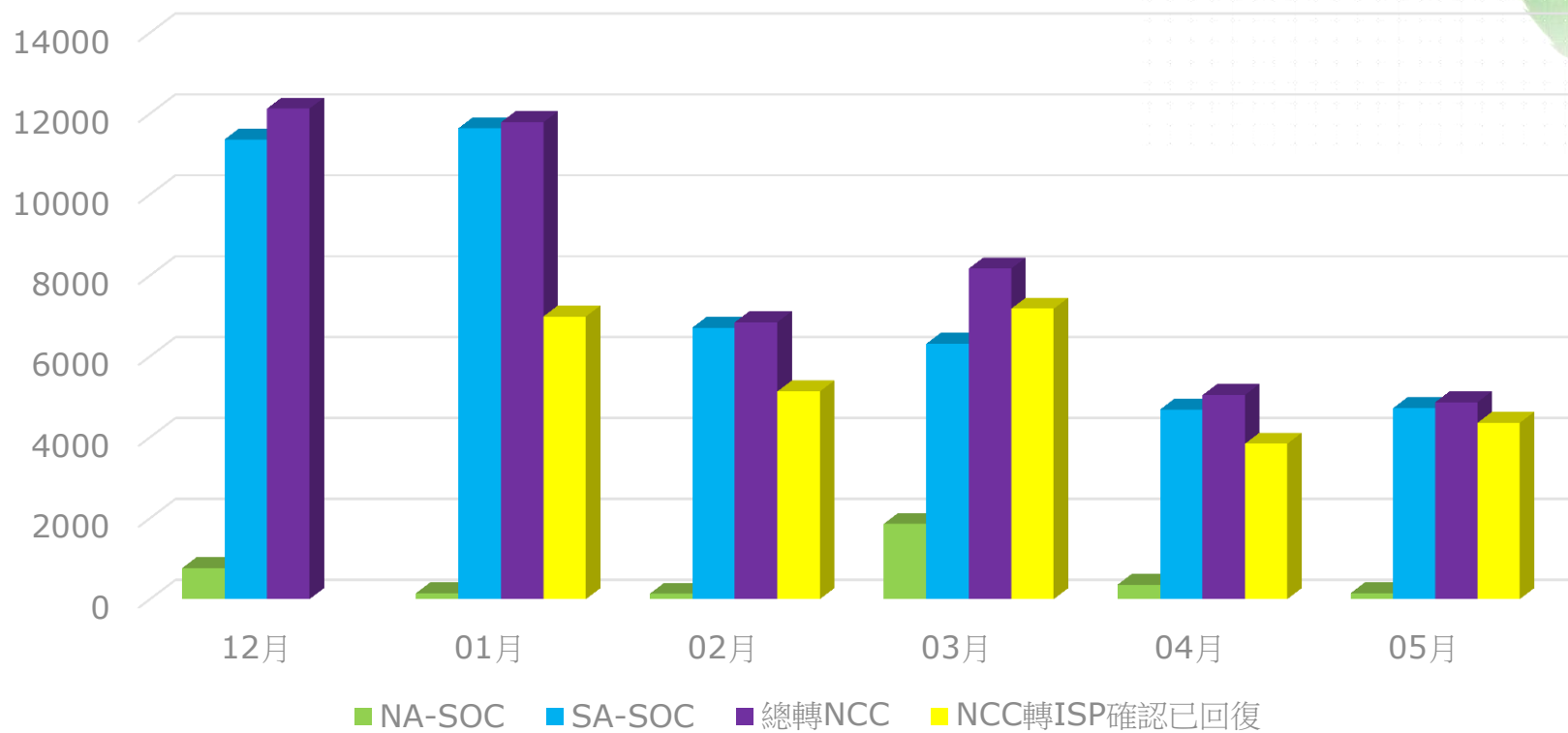
臺灣學術網路資安事件統計(4/4)							資安事件子類型統計						
事件 類型	子類別	來源											
		self-report	ABUSE	Mini SOC	N-ASOC	S-ASOC	TACERT	Web-P	MJIB	NCCST	TW CERT	TW CSIRT	總計
入侵 攻擊 (INT)	殭屍電腦	17	0	4	1,299	22	0	0	0	0	0	0	1,342
	對外攻擊	3	0	5	222	668	0	0	0	0	8	0	906
	系統被入侵	10	0	28	305	172	0	0	0	0	1	0	516
	其它	10	0	21	35	17	0	0	1	0	0	0	84
	垃圾郵件	0	0	0	0	2	4	0	0	0	3	0	9
	散播 惡意程式	0	0	3	5	1	0	0	0	0	0	0	9
	命令與控制 伺服器	0	0	0	2	5	0	0	0	0	0	0	7
	電子郵件社 交工程攻擊	0	0	0	0	0	3	0	0	0	3	0	6
	中繼站	0	0	0	5	0	0	0	0	0	0	0	5
	針對性攻擊	0	0	1	0	0	0	0	0	0	0	0	1
網頁 攻擊 (DEF)	惡意網頁	2	0	1	0	1	0	0	17	0	5	1	27
	網頁置換	0	0	0	0	0	0	0	21	0	4	0	25
	其它	0	0	0	0	1	0	0	4	0	0	0	5
	個資外洩	1	0	0	0	0	0	0	0	0	0	0	1
	釣魚網頁	0	0	0	1	0	0	0	0	0	0	0	1
總計		43	0	63	1,874	889	7	0	43	0	24	1	2,944

學術網路遭受勒索軟體WannaCry損害調查

- 統計自**106/5/12~106/6/7**為止，受害單位共計**14**間，受害主機數量共計**133**臺
- 受害單位類型以「大專院校」佔**86%**為大宗，其次為「國民中小學」佔**14%**
- 受害主機大都為電腦教室或學生的個人電腦，尚無公務電腦受害

列標籤	受害主機數	受害的單位類型數量				
		大專院校	高中職	國民中小學	其他單位	小計
中央研究院	61	2	0	0	0	2
雲嘉區域網路中心	19	1	0	0	0	1
高屏澎區域網路中心	15	2	0	0	0	2
臺中區域網路中心	12	2	0	0	0	2
臺北區域網路中心(1)	10	1	0	0	0	1
桃園區域網路中心	5	1	0	0	0	1
嘉義市教育網路中心	4	0	0	2	0	2
新竹區域網路中心	3	1	0	0	0	1
臺南區域網路中心	2	1	0	0	0	1
花蓮區域網路中心	2	1	0	0	0	1
總計	133	12	0	2	0	14

轉NCC事件單量圖



圖片來源：A-ISAC

總體資安威脅分析-資安事件類型 Top10

資安事件威脅分析(3/6)

* Top10資安事件類型-攻擊來自國外

排行	類型	攻擊數量	開單類型
1	MS.RDP.Connection.Brute.Force	1,390,562,570	INT
2	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	713,312,762	EWA
3	Telnet.Login.Brute.Force	427,943,702	INT
4	SSH.Connection.Brute.Force	241,978,401	INT
5	Worm.Slammer	50,948,687	INT
6	VxWorks.WDB.Agent.Debug.Service.Code.Execution	15,136,855	EWA
7	ASUS.Router.infosvr.UDP.Broadcast.Command.Execution	10,331,335	觀察中
8	NTP.Monlist.Command.DoS	6,758,552	INT
9	POP3.Login.Brute.Force	6,464,110	INT
10	MS.DCERPC.NETAPI32.Buffer.Overflow	4,740,884	INT

- **MS.RDP**帳號密碼暴力破解攻擊，如成功利用將可以連入未經授權的系統，進行非法的存取。
- **中國製網路路由器Netis**的密碼繞道攻擊，攻擊者可任意上傳、下載執行檔案，也可修改路由器設定進行中間人攻擊。
- **Telnet**帳號密碼暴力破解攻擊，如攻擊成功將可以連入未經授權的系統，進行非法的存取。

總體資安威脅分析-資安事件類型Top10

資安事件威脅分析(4/6)

* Top10 資安事件類型- 攻擊來自學術網路內部

排行	類型	攻擊數量	開單類型
1	MS.RDP.Connection.Brute.Force	105,144,319	INT
2	Telnet.Login.Brute.Force	47,713,776	INT
3	WordPress.xmlrpc.php.wp.getUsersBlogs.Brute.Force	7,056,538	EWA
4	FTP.USER.Command.Overflow	1,954,164	EWA
5	MS.SMB.Server.Trans.Peeking.Data.Information.Disclosure	1,352,218	EWA
6	Backdoor.DoublePulsar	938,183	EWA
7	SSH.Connection.Brute.Force	761,788	INT
8	POP3.Login.Brute.Force	732,703	INT
9	NTP.Monlist.Command.DoS	357,429	INT
10	FTP.Text.Line.Too.Long	202,315	不開單

- **MS.RDP** 帳號密碼暴力破解攻擊，如成功利用將可以連入未經授權的系統，進行非法的存取。
- **Telnet** 帳號密碼暴力破解攻擊，如攻擊成功將可以連入未經授權的系統，進行非法的存取。
- **WordPress** 帳號密碼暴力破解攻擊，如攻擊成功將可以連入未經授權的系統，進行非法的存取。

圖片來源：S-ASOC

總體資安威脅分析-資安事件類型Top10

資安事件威脅分析(5/6)

* Top10資安事件類型-攻擊來自國內其他ISP業者

排行	類型	攻擊數量	開單類型
1	MS.RDP.Connection.Brute.Force	5,896,046	INT
2	Telnet.Login.Brute.Force	384,293	INT
3	SSH.Connection.Brute.Force	314,851	INT
4	Netcore.Netis.Devices.Hardcoded.Password.Security.Bypass	111,179	EWA
5	NTP.Monlist.Command.DoS	88,670	INT
6	HTTP.URI.SQL.Injection	55,389	不開單
7	China.Chopper.Webshell.Client.Connection	9,905	INT
8	Linux.LCDproc.Parse.Code.Execution	9,058	EWA
9	Multiple.Vendor.ICMP.Remote.DoS	4,804	INT
10	Commandline.Overflow	2,602	EWA

- **MS.RDP**帳號密碼暴力破解攻擊，如成功利用將可以連入未經授權的系統，進行非法的存取。
- **Telnet**帳號密碼暴力破解攻擊，如攻擊成功將可以連入未經授權的系統，進行非法的存取。
- **SSH** 帳號密碼暴力破解攻擊，如成功利用將可以連入未經授權的系統，進行非法的存取。

圖片來源：S-ASOC

Botnet分析-受害主機統計

資安事件威脅分析(6/6)

Top10_受殭屍網路控制之受害主機

IP	來源	名稱	攻擊數量	備註
66.240.205.34	美國	Zeroaccess.Botnet	1,436,698	
163.23.102.116	彰化縣立大城國民中學	Mirai.Botnet	304,598	
210.240.125.227	臺東縣教育網路中心	Nitol.Botnet	118,113	
66.240.205.34	美國	Gh0st.Rat.Botnet	92,737	
140.134.208.25	私立逢甲大學	Ganiw.Botnet	85,594	
163.172.191.95	法國	Hajime.Botnet	60,478	
120.113.167.92	雲林縣斗六市公誠國民小學	Nitol.Botnet	36,889	
45.32.1.44	美國	Hajime.Botnet	28,788	
163.24.82.212	屏東縣牡丹鄉牡丹國民小學	Salinity.Botnet	28,465	
140.120.75.139	國立中興大學	Mirai.Botnet	26,955	

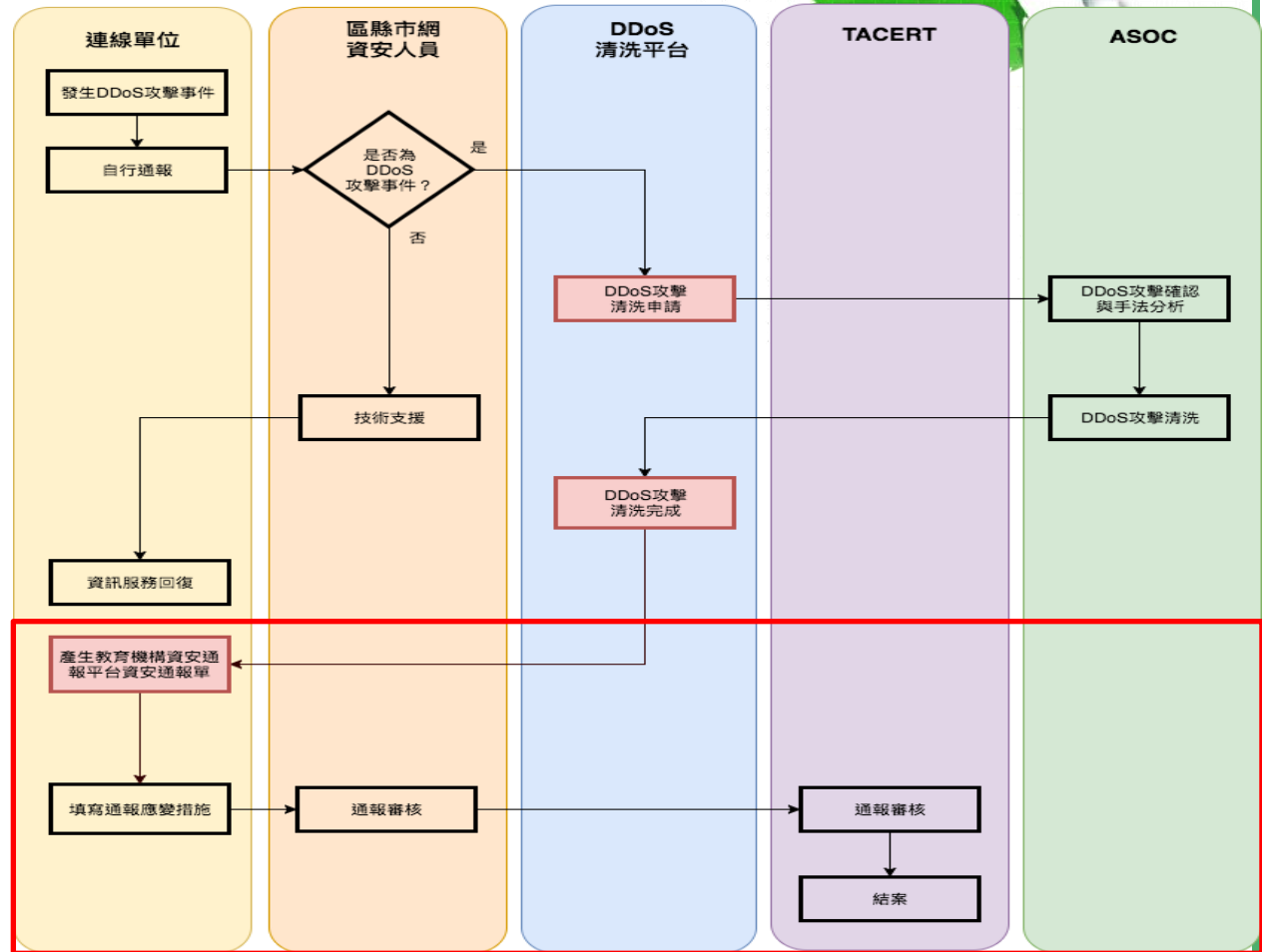


DDoS清洗申請系統說明

- 教育體系DDoS攻擊清洗申請流程
需新增自動產生資安事件單，通知第一線人員填寫通報應變措施

教育體系DDoS攻擊清洗申請流程

2017.05.09



新增流程

圖片來源：S-ASOC

臺灣學術網路資安防護團隊



行政院國家資通安全
會報技術服務中心
NCCST
G-ISAC



A-ISAC
(逢甲大學)



TA-CERT
(中山大學)



資安訓
練、救援
(交通大
學)
全國校園



Web-P
(成功大
學)
全國校園



NASOC
(臺灣大
學)
北區網路



SASOC
(國網中
心)
南區網路



**MINI-
SOC** (逢
甲大學)
縣市資安



接軌國際達成業界標準



業界

2005

2013

ISO 27001
2005年版

ISO 27001
2013年版

教育體系資通安全暨個人資料

2007/6

2015/4 2015/6

2016/12

2017/8

教版

教育體系資
通安全管理
規範96年版

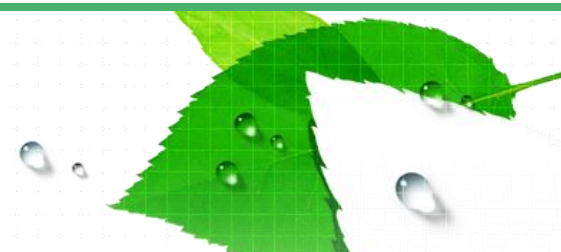
教育體系
新版規範
規畫啟動

聯合輔導
第一批採
新版驗證

新版規範
驗證正式
全面執行

轉由中興大學負責ISCB，所被賦予的主要任務就是要
參考業界新版標準制定新版規範並推動實施

新舊版之差異



新版資安規範(14控制領域)

原有資安規範(11控制領域)

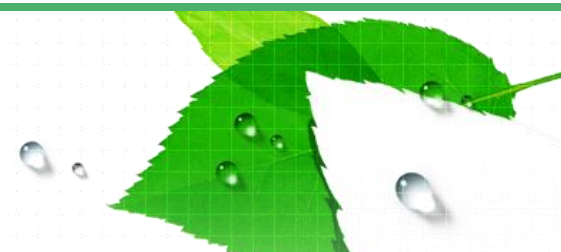
A.5	A.5 資訊安全政策訂定與評估
A.6	A.6 資訊安全組織
A.7	A.8 人員安全管理與教育訓練
A.8	A.7 資訊資產分類與管制
A.9	A.11 存儲
A.10	A.9 實體安全
A.11	A.10 通訊
A.12	A.10 通訊
A.13	A.10 通訊
A.14 系統獲取、開發及維護	A.12 系統
A.15 供應者關係	
A.16 資訊安全事故管理	A.13 資訊安全事件之反應及處理
A.17 業務永續運作管理	A.14 業務永續運作管理
A.18 遵循性	A.15 相關法規與施行單位政策之符合性

A15.1

應與供應者議定並文件化，降低與供應者存取施行單位資產關聯之風險的資訊安全要求事項。

基於目前各學校單位都有愈來愈多委外，必然是需要去考量檢視是否有相關資安措施

新舊版之差異



新版資安規範(14控制領域)	原有資安規範(11控制領域)
A.5 資訊安全政策訂定與評估	A.5 資訊安全政策訂定與評估
A.6 資訊安全組織	A.6 資訊安全組織
A.7 人力資源安全	A.8 人員安全管理與教育訓練
A.8 資訊資產分類與管制	7 資訊資產分類與管制
A.9 實體與環境安全	11 存取控制安全
A.10 通訊與作業系統管理	9 實體與環境安全
A.11 系統安全	10 通訊與作業系統管理
A.12 系統安全	10 通訊與作業系統管理
A.13 系統安全	A.12 系統安全
A.14 系統安全	A.12 系統安全
A.15 供應者關係	A.12 系統安全
A.16 資訊安全事故管理	A.12 系統安全
A.17 業務永續運作管理	A.14 系統安全
A.18 遵循性	A.15 系統安全

16.1.4

更具體要求落實資訊安全事件評估及決策的處理原則

16.1.5

對於資訊安全事故之回應要有文件化的程序



Thank You !