104年網路攻防演練辦理情形

行政院資通安全辦公室
周智禾 諮議

中華民國104年12月21日

大綱

壹、104年網路攻防演練作業

貳、104年網路攻防演練綜合評估

　一、情境演練

　二、實兵演練

　三、電子郵件社交工程演練

參、結論與建議

壹、104年網路攻防演練作業

104年網路攻防演練

❖104年網路攻防演練：

- **情境演練**
  - **期間：9月24日至12月17日**
  - **對象 (能源與交通)：**
    - 臺灣港務股份有限公司花蓮港務分公司 (演練日期：9月24日)
    - 台灣電力股份有限公司第二核能發電廠 (演練日期：11月24日)
    - 台灣中油股份有限公司大林煉油廠 (演練日期：12月4日)
    - 交通部民用航空局松山機場 (演練日期：12月17日)
- **實兵演練(含電子郵件社交工程)**
  - **期間：10月12日至11月20日**
  - **對象：**
    - 行政院所屬二級機關(含**三、四級機關共用資訊系統)**

貳、104年網路攻防演練綜合評估

一、情境演練

- 情境演練主要目的係檢視標準作業程序是否規劃得宜，情境與演練腳本設計應務求逼真以反映真實狀況
- 104年情境演練主要針對花蓮港務分公司、第二核能發電廠、大林煉油廠、松山機場的關鍵基礎設施系統進行演練
- 演練機關需視情境內容所描述之不同狀況即席回答應變處置作為，再由學者專家提供改善建議

第二核能發電廠
ERF、RFC暨DEH系統情境演練

發布時間	演練程序	演練時間
	演練狀況： 核二廠目前是台灣電力供應系統中裝置容量最大的發電機組。但隨著反核民意的升高，數名內部人員因不滿核電廠，想利用本身的專業知識進行一連串的干擾行為，欲使得一般民眾不信任核電廠安全。	
14:15	狀況(一) DEH自動控制器處理模組故障，人機介面操作電腦遭植入病毒	15分鐘
14:30	狀況(二) RFC Foxboro軟體參數遭內部人員蓄意竄改，以致再循環流量產生異常	15分鐘
14:45	狀況(三) ERF系統的Windows Server在安裝修補程式過程中不慎感染病毒	15分鐘
15:00	狀況(四) 已被病毒感染的DEH人機介面操作電腦，因運轉員執行測試指令而觸發惡意程式	15分鐘
15:50	綜合討論	40分鐘
16:30	情境演練會議結束	

102至104年情境演練比較

	102年	103年	104年
演練對象	行政院所屬33個二級部會行總處署	關鍵資訊基礎設施(交通與通訊傳播)： ① 新北市政府交通局之都會交通控制系統 ② TWNIC之網域名稱管理系統	關鍵資訊基礎設施(能源與交通)： ① 第二核能發電廠 ② 大林煉油廠 ③ 花蓮港務分公司 ④ 松山機場
演練方式	模擬演練，輔以視訊會議瞭解各機關即時應處情形	模擬演練，即席回答應處作為	模擬演練，即席回答應處作為
演練時間	全日 (共6個子情境)	半日 (共3個子情境)	半日 (共3個子狀況及1個特別狀況)

- ✓辦理SCADA安全教育訓練
- ✓與演練機關進行多次訪談
- ✓設計3套劇本，每套劇本含3個子狀況及1個特別狀況(由專家學者設計)
- ✓演練當天現場抽選演練劇本

二、實兵演練

- 於10月12日至11月20日期間，由攻擊手對32個機關(共1,322個系統)，以不影響演練機關系統正常業務運作為原則，採遠端弱點掃描、滲透測試及社交工程攻擊等方式，實際攻擊入侵機關系統與網路，並由裁判組負責記錄與監控攻擊組之攻擊過程
- 2013年OWASP十大弱點測試手法，並增加系統弱點、弱密碼、應用程式弱點及新型態弱點等檢測，共計16類檢測項目

2013年OWASP十大Web資安弱點			
A1	注入攻擊(Injection)	A6	敏感資訊暴露(Sensitive Data Exposure)
A2	遭破壞的認證與連線管理 (Broken Authentication and Session Management)	A7	缺乏功能性的存取控管 (Missing Function Level Access Control)
A3	跨網站腳本攻擊(Cross Site Scripting)	A8	跨網站的偽造要求(Cross Site Request Forgery)
A4	不安全的物件參考 (Insecure Direct Object References)	A9	使用具有已知弱點的元件(Using Components with Known Vulnerabilities)
A5	錯誤的安全性設定 (Security Misconfiguration)	A10	未驗證的重導與轉出(Unvalidated Redirects and Forwards)

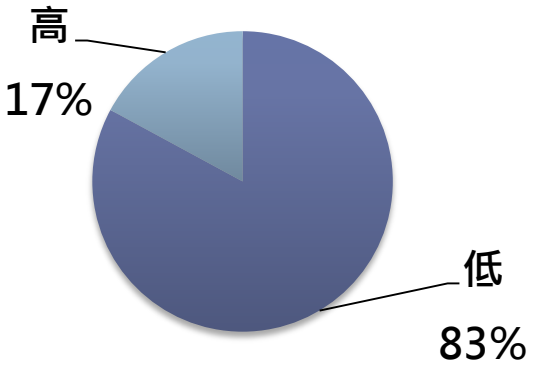
資料來源：OWASP (http://www.owasp.org.tw)

弱點分布 – 整體

排名	弱點類型	比例
1	敏感資訊暴露	40.7%
2	跨網站腳本攻擊	25.1%
3	不當的安全組態設定	8.6%
4	注入攻擊	8.3%
5	弱密碼	7.4%
6	不安全的物件參考	4.4%
7	未經驗證的重新導向與轉送	3.5%
8	缺少功能級別的存取控制	2.1%
總計		100%

本年共發現339個弱點：

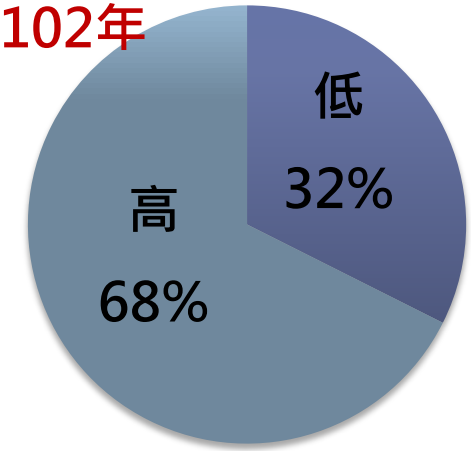
- 58 個高衝擊性弱點（佔17%）
- 281個低衝擊性弱點（佔83%）



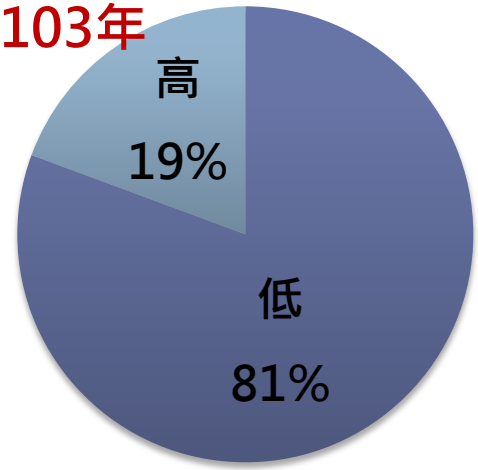
判斷原則	高衝擊性	低衝擊性
機密性：取得屬於未公開或需經授權的資料或文件內容	重要帳號密碼(具管理權限)、密級以上資料、機敏網頁程式碼、民眾個資等	一般使用者帳號密碼、測試帳號密碼、非密級資料等
完整性：未經認證或授權即可修改內部資料或文件	插入攻擊語法(XSS等)、修改機敏資料等	置入圖片、修改一般資料等

102至104年實兵演練比較

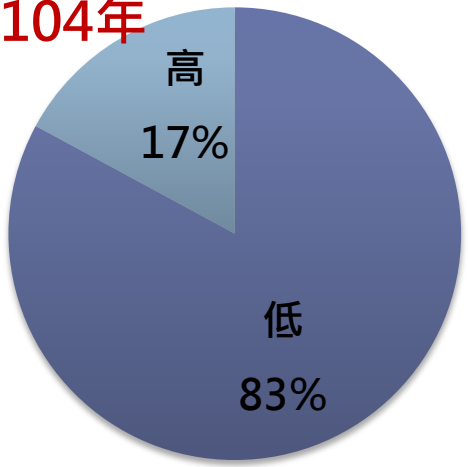
102年



103年



104年



	102年	103年	104年
演練對象	行政院所屬33個二級部會行總處署	府、五院、各直轄市及縣(市)政府(計28個機關)	行政院所屬32個二級部會行總處署(含三、四級機關共用資訊系統)
演練期間	32個日曆天	23個日曆天	40個日曆天
攻擊手	30位	21位	20位
系統數	482	1,267	1,322
系統平均弱點數	0.224	0.171	0.256

三、電子郵件社交工程演練

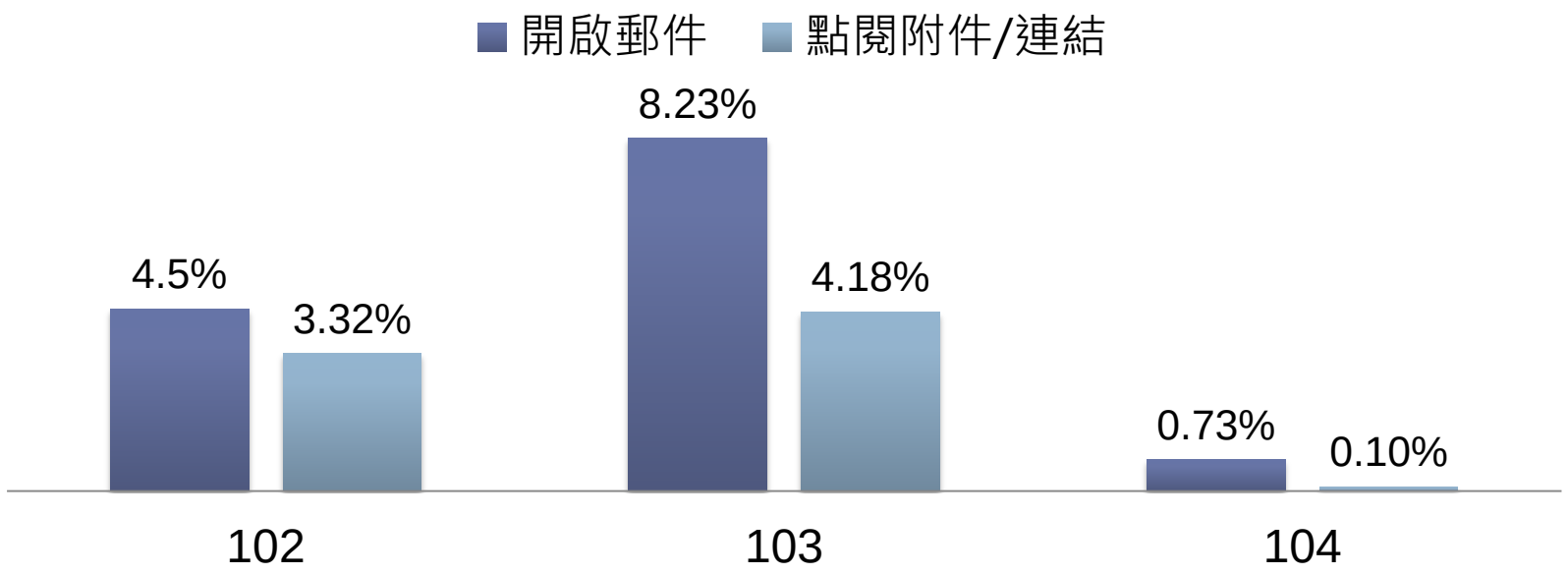
於網路上尋找32個機關可取得之所屬人員電子郵件帳號(共960個郵件帳號)

社交工程郵件類型(共9種信件)
隨機寄發3種類型之社交工程郵件至每個電子郵件帳號

透過「社交工程演練系統」採隨機寄發社交工程郵件，並記錄使用者「開啟郵件」、「點閱連結」及「開啟附件」等行為

102至104年電子郵件社交工程演練比較

年度	受測人數	開啟郵件人數	開啟率	點閱附件/連結人數	點閱率
102	932	42	4.5%	31	3.32%
103	838	69	8.23%	35	4.18%
104	960	7	0.73%	1	0.1%



點閱率與開啟率均較102年與103年低。

研討會議及表揚

- 102年我國首次辦理網路攻防演練，期間邀外賓(4個國家計11位)進行相關經驗分享，各界對我演練籌劃及辦理成果多表示肯定
- 本年11月25日召開104年攻防演練研討會議，並邀請外賓(來自美國、歐盟、澳洲、日本、韓國、泰國共計16位)進行經驗交流

時間	議程內容	主講者
13:30-14:00	報到	
14:00-14:10	主席致詞	張召集人善政
14:10-14:40	資安趨勢與網路攻防演練簡介	技服中心
14:40-15:10	Enterprise Desktop Exercise Sharing	澳洲代表
15:10-15:40	Incident Exercises and Cyber threat situation in Thailand	泰國代表
15:40-16:00	中場休息	
16:00-16:20	104年網路攻防演練綜合評估	技服中心
16:20-17:10	綜合座談	主持人：張召集人善政 與談人： 演練團隊代表 外賓代表
17:10	賦歸	

- 對於表現績優機關，於12月21日資安會報第29次委員會議頒發獎座予以肯定；對於表現績優及良好機關，將函請各該機關給予參與人員適度行政獎勵

參、結論與建議

機關配合事項

- 關鍵資訊基礎設施(CII)營運機關：
  - 封閉或隔離之網路環境亦可能存在資安風險，應依需求檢視資訊與控制系統是否存在安全性風險，適時採取適當的防護作為
  - 情境演練劇本設計過程中，應廣泛設想及審慎辨識各種可能之資安威脅，並從系統失能之最壞狀況著手，嚴格檢視緊急應變時的縱向作業與橫向溝通SOP是否完善
  - 應持續關注CII資安威脅趨勢，定期檢視資安防護及應變能力，並依演練結果積極檢討強化防護措施
- 104年演練結果發現高衝擊性弱點主要為注入攻擊、弱密碼及敏感資訊暴露，應加強密碼管理、輸入驗證及系統安全設定等資安防護作業
- 機關應盤點所屬業務、資訊及測試等各項系統，若該系統已停止使用，應辦理下線程序，避免因疏於維運造成資安威脅
- 機關應依規定落實每年辦理1次通報演練及2次電子郵件社交工程演練，以有效確保機關人員之資安意識

資安會報後續辦理重點

- 持續將CII及相關重點防護對象納入演練範疇，並逐年強化演練腳本，確保標準作業程序更加完備
- 規劃於105年資安長及資訊主管會議，提報本次演練結果細部資料(各機關名稱以代碼方式呈現)；賡續於105年中召開網路攻防技術研討會，與各機關資訊(安)人員分享常見網站(系統)弱點及檢測防護措施，協助機關可自行檢測，以強化防禦能量
- 積極推動系統發展生命週期(SSDLC)，促請機關依「資訊系統分級與資安防護基準作業規定」，對高安全等級之系統(委外)開發時即要求導入，期有效從源頭強化整體資訊系統安全

報告完畢　敬請指教