政府資通安全政策推動及重點工作

行政院資通安全辦公室

103年12月

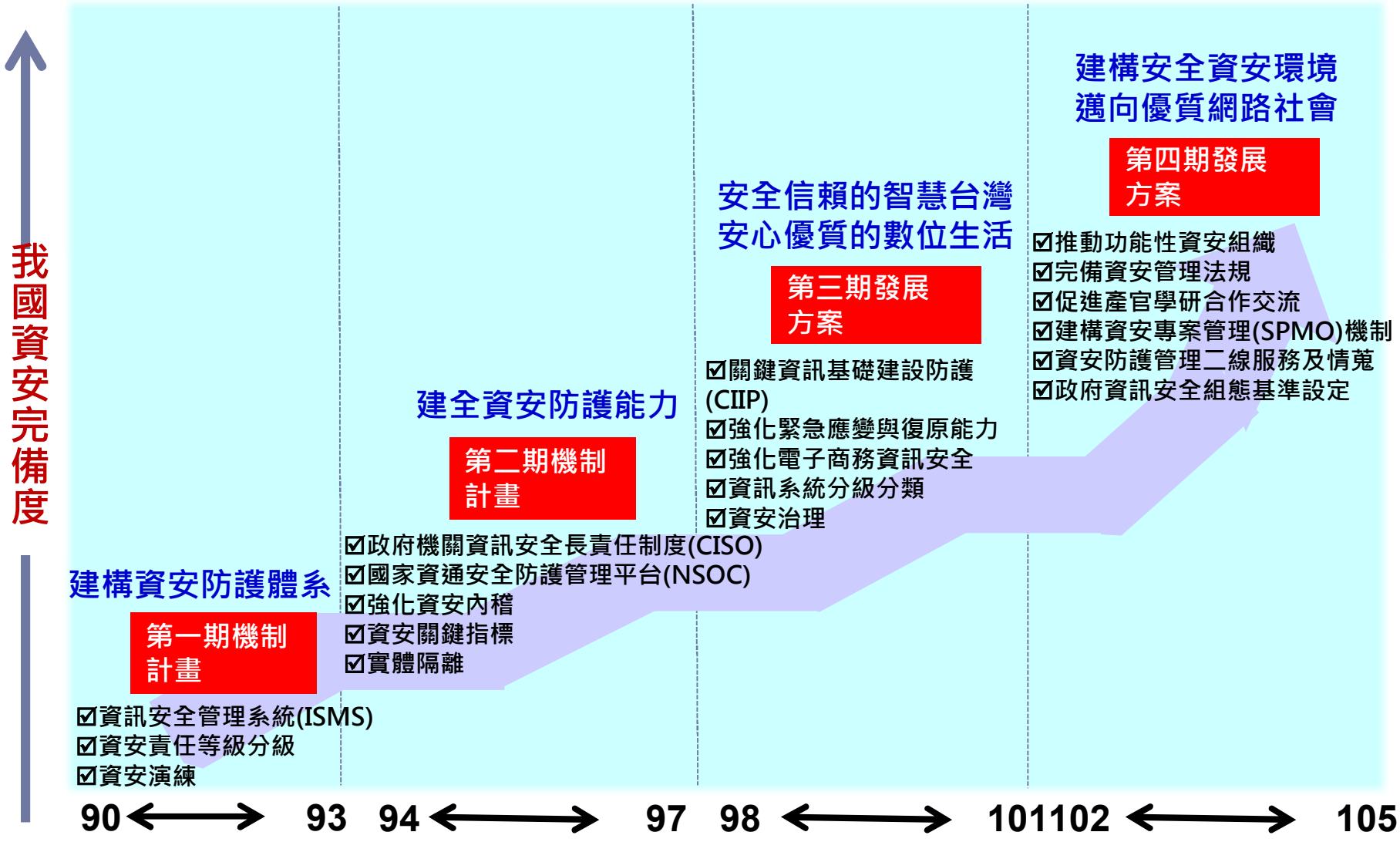
大綱

- ❖政策推動
  - 國家資通訊安全發展方案
  - 資通安全責任等級及應辦事項
- ❖重點工作
  - 資通安全稽核
  - 網路攻防演練
  - 政府組態基準
  - 共同供應契約資安服務品項
  - 行動裝置資安強化措施
- ❖結語

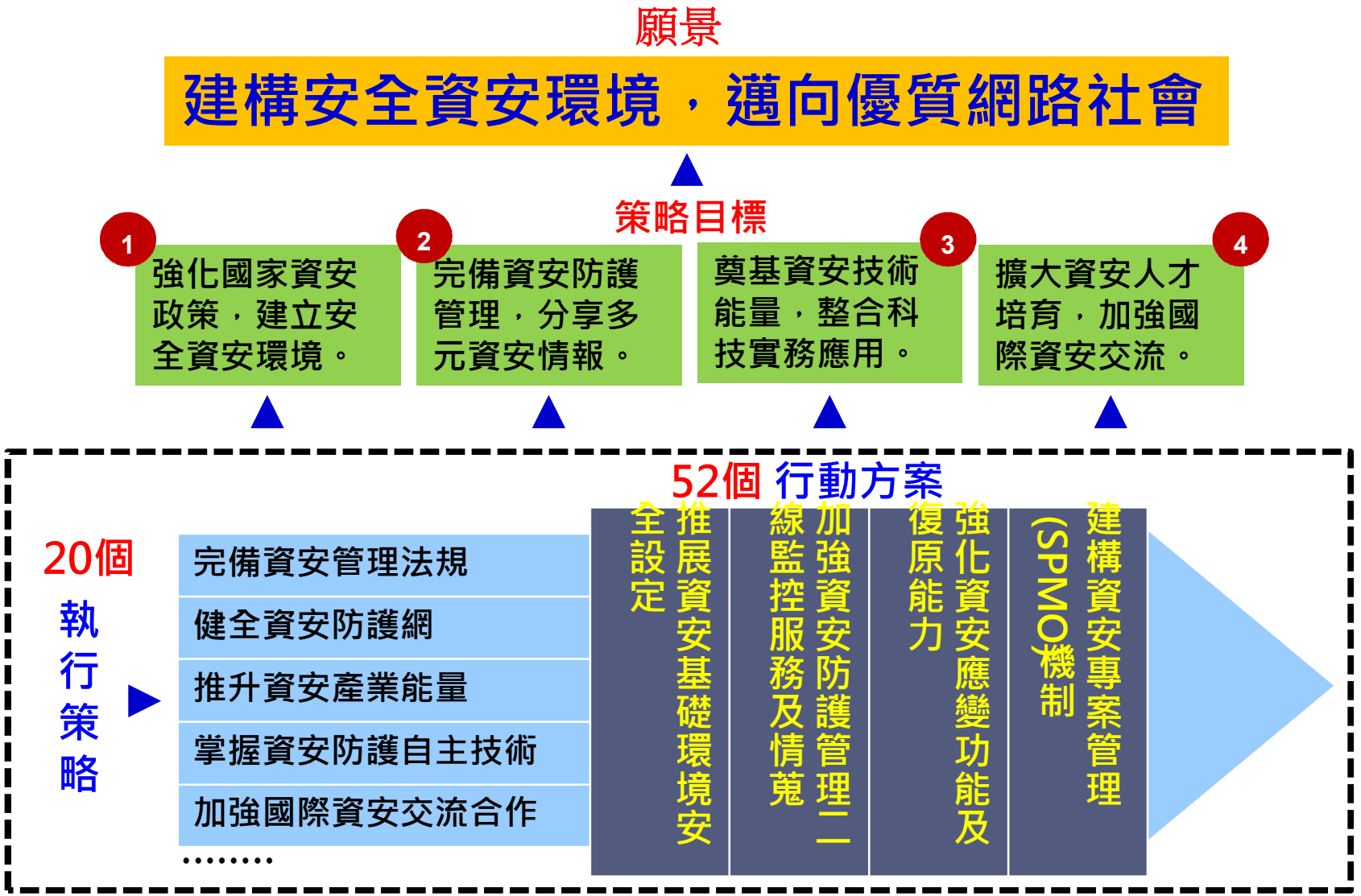
政策推動

- ❖國家資通訊安全發展方案
- ❖資通安全責任等級及應辦事項

國家資通訊安全發展方案 - 推動歷程



國家資通訊安全發展方案（102年至105年）(1/2)
- 願景與策略目標、執行策略與行動方案



國家資通訊安全發展方案（102年至105年）(2/2) - 執行重點

- 國家資通訊安全發展方案（ 102年至105年）已於102年12月25日函分行行政院所屬各部會行總處署、各省（市）政府及縣（市）政府，就該管部分積極推動辦理。
- 發展方案之願景旨在達成「建構安全資安環境，邁向優質網路社會」，期經由前瞻政策引導，在政府與民間通力合作之下，透過國家整體資源力量，逐步推動並落實優質網路社會。
- 發展方案定位為推動我國未來四年資安防護計畫發展之依據，做為貫通政府、產業與民眾資安防護之價值樞紐，透過宏觀環境的科技趨勢發展進行資安整體性規劃。
- 行政院資通安全辦公室現正依據國家發展需要及切合資安實務需求，每年視需要滾動式檢討發展方案及相關推動計畫。

資通安全責任等級及應辦事項(1/3)

❖93年

國家資通安全會報制訂「政府機關(構)資訊安全責任等級分級作業施行計畫」，主要針對重要政府機關（構）建立完整的資通安全整體防護體系。

❖94年

增訂各政府機關資安等級應執行工作事項。

❖98年

精進各政府機關資安等級應辦事項。

❖103年

因應資訊科技發展及資通安全威脅趨勢，檢討修訂政府機關資安責任等級及應辦事項，完善國家整體資安防護體系，預計103年底將完成研修作業。

資通安全責任等級及應辦事項(2/3)

作業名稱 / 等級	防護縱深	ISMS推動作業	稽核方式	資安教育訓練(一般主管、資訊人員、資安人員、一般使用者)	專業證照	檢測機關網站安全弱點
A級	NSOC直接防護/SOC自建或委外、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少2次內稽	1. 每年至少(3、6、18、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定	維持至少2張資安專業證照	每年2次
B級	SOC(選項)、IDS、防火牆、防毒、郵件過濾裝置	通過第三者驗証	每年至少1次內稽	1. 每年至少(3、6、16、3小時) 2. 資訊人員、資安人員需通過資安職能鑑定	維持至少1張資安專業證照	每年1次
C級	防火牆、防毒、郵件過濾裝置	自行成立推動小組規劃作業	自我檢視	每年至少(2、6、12、3小時)	資安專業訓練	每年1次
D級	防火牆、防毒、郵件過濾裝置	推動ISMS觀念宣導	自我檢視	每年至少(1、4、8、2小時)	資安專業訓練	每年

有關政府機關資安應辦事項，行政院資通安全辦公室已配合政府組改、資訊系統向上提升及雲端環境發展等因素進行精進，將建構完整之政府機關資安防護基準，預計103年底前可完成修訂作業。

資通安全責任等級及應辦事項(3/3) - 研修草案

1.擴充資通安全責任等級施行對象，增加政府機構、行政法人及由政府委託民間興建營運後轉移(Build-Operate-Transfer, BOT)之關鍵資訊基礎設施營運單位。

2.簡化責任等級，因應資安威脅情勢，簡化層級以加強資安防護將原A、B、C、D 4個等級，調整為A、B、C 3個等級。

3.明定CII責任等級，凡涉及關鍵資訊基礎設施(Critical Information Infrastructure, CII)之機關(構)，其資安責任等級列為A級。

4. 各機關責任等級核定權責調整，原政府機關資安責任等級，由各該機關核定後，報資安會報備查，將調整為經行政院資安辦複核後，提請資安會報核定（備）資安責任等級。

5.擴增應辦事項，原計畫定義6類應執行之工作事項，經參考102~103年網路攻防演練及政府機關（構）資安健診、稽核結果後，即進行資安責任等級應辦事項之檢討，將以政策、管理、技術及認知與訓練等4個面向、10個類別，強化應辦事項內容。

重點工作

- 資通安全稽核
- 網路攻防演練
- 政府組態基準
- 共同供應契約資安服務品項
- 行動裝置資安強化措施

資通安全稽核(1/8)

- 行政院國家資通安全會報為「協助各機關強化資安防護工作之完整性及有效性，並透過持續改善以降低資安風險」，於網際防護體系下設「稽核服務組」，由行政院資通安全辦公室主辦（103年3月3日生效）。

- 「國家資通安全發展方案（102年至105年）」行動方案2.3.3落實資安稽核作業「每年至少選定20個重要機關辦理資安外部稽核」。

- 103年1月10日「國家資通訊安全策進專報會議」指裁示事項，本年度受稽對象以負責財政和經濟機關(構)為主。

資通安全稽核(2/8)

類別	主管機關	受稽機關
財經相關(15個)	中央銀行(1個)	
	財政部(4個)	關務署、國有財產署、高雄國稅局、北區國稅局
	經濟部(5個)	工業局、投資審議委員會、中小企業處、能源局、智慧財產局
	金管會(4個)	臺灣土地銀行、財團法人聯合信用卡處理中心、臺灣證券交易所股份有限公司、臺灣集中保管結算所股份有限公司
	新北市政府(1個)	新北市政府稅捐稽徵處
民生相關(2個)	經濟部(1個)	台電（總管理處）
	交通部(1個)	臺灣區國道高速公路局（含遠通電收公司）
大量個資(2個)	衛福部(1個)	國民健康署
	交通部(1個)	公路總局（含第3代公路監理資訊系統專案辦公室及台北市監理所）
其他(1個)	勞動部(1個)	

資通安全稽核(3/8)

面向（總分）	項目	配分
策略面(31)	導入資訊安全管理系統範圍適切性	7
	機關首長對資安業務支持度	7
	資源投入資安業務狀況	7
	業務運作規劃與落實	10
管理面(31)	個人資料保護與管理	15
	風險評鑑、資訊資產清查與管理	8
	人力資源管理	8
技術面(38) （含技術檢測）	通訊與作業管理適切性與落實執行狀況	20
	資安事件通報與管理	9
	應用系統開發及維護安全管理	9
總分：100		

資通安全稽核(4/8)
- 共同發現與建議（策略面）

共同發現	建議
部分機關資安長與資訊長未能明確設置	建議依行政院相關規定設立資安長（由副首長擔任）督導與規劃資安業務及個資保護工作
部分機關資安推動組織成員大多為資訊部門，業務部門較少參與，難以反映相關資安控制措施是否有效（102年亦有類似發現）	建議各機關資安推動組織，宜整體考量資安業務之推動，由各業務部門主管組成，訂定適當之資安管理指標，制定有效量測方式，透過定期召開推動會議，追蹤與檢討相關資控措施的適切性及有效性
部分機關對內稽缺失所提之矯正/改善/預防措施，後續追蹤改善情形落實度不足（102年亦有類似發現）	建議各機關應定期召開資安管理/審查會議，列管與追蹤矯正/改善/預防措施執行情形
部分機關資訊（安）人員遇缺不補，造成人力不足，對一般人員風險亦缺乏有效管理	建議各機關應妥適編列資訊（安）人力，或將業務集中向上管理，因應人員不足現象。並依照員工及業務屬性辨識其可能資安風險，透由內、外部稽核及教育訓練等，妥適控管風險
部分機關對Windows XP EOS尚未完全汰換，恐仍存有資安風險	建議各機關確實評估WindowsXP電腦，妥適因應WindowsXP終止支援服務之衝擊，配合整體資訊業務調整，積極進行汰換作業

資通安全稽核(5/8)
- 共同發現與建議（管理面）

共同發現	建議
部分機關對委外廠商管理較少進行資安稽核，大都以委外合約進行約束，缺少對資安要求的有效性管理	各機關應規劃與落實對委外廠商進行資安稽核，建議委外契約本文增加對共通之資訊安全條款及個資保護條款要求之引用，以避免資料外洩，訂定委外廠商銷毀因執行委外案所擁有之機敏資料
部分機關對於委託廠商進行應用軟體開發，缺乏軟體安全監督能力	建議增加對應用系統委外廠商之資安管理能力要求及稽核，除開發能量及品質能力外，須特別注意原始碼來源安全、保存、使用與傳輸之管理
部分機關過度倚賴委外廠商，對駐點人員亦較少約束	各機關應對委外廠商駐點人員進行工作劃分，機關同仁負責管理與稽核，廠商駐點人員負責執行，加強查核委外廠商，具重要資訊系統管理權限之存取紀錄
部分機關對個人資料盤點內容較不周延（102年亦有類似發現）	建議個人資料以作業流程面向進行盤點，考量採流程圖方式繪製出個資生命週期，並呈現出相關利害關係者
部分機關執行業務所蒐集之個人資料，若提供再利用時，較少評估個資內容提供的妥適性	各機關執行業務所蒐集之個人資料，若與其他機關（構）介接或提供再利用，宜審慎評估適法性（個資法之特定使用目的要求），並應妥適規劃後續之供應鏈（第二者稽核）管理機制，確保再利用機關之資料使用符合安控與個資法要求
部分機關已展開ISMS改版作業，風險評鑑方法與人員訓練略顯不足	建議各機關對於風險評鑑之風險評估方法論，應適時加以檢討，以符合機關實際需求。對於ISMS改版作業，建議人員應進行主任稽核員之改版訓練，提升資安管理能量

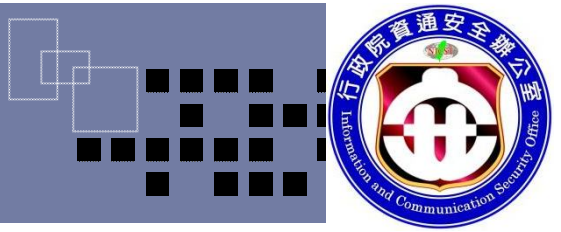
資通安全稽核(6/8)
- 共同發現與建議（技術面）

共同發現	建議
部分機關網路服務安全控制措施之適切性及落實度較不足	建議應強化網路服務設定之安全設定強度，檢討外部遠端連線內部系統之必要性，訂定安控設定的檢視週期，落實執行相關必要檢視
部分機關應用系統開發上線，未進行弱點掃描等必要性之安全檢查，應用系統疑遭駭客入侵之風險	建議委外維護之應用系統開發或變更上線前，應進行版本控管，對於系統或軟體進行弱點掃描，且定期辦理滲透測試，降低系統遭駭客入侵之風險
對於行動裝置較缺乏有效管理方式	各機關如因業務需要開放使用行動裝置，建議應在需求面及安全性同時兼顧下啟用，妥善管理行動裝置存取權限，以確保資訊安全
各機關對於網路或系統存取系統日誌應妥善保管	建議各機關對於軌跡紀錄的保存、管理與分析，宜考量數位鑑識需求，依系統容量及日誌之屬性，規劃適度日誌管理方式

資通安全稽核(7/8)
- 共同發現與建議（技術檢測）

共同發現	建議
使用者電腦安全防護： 12機關安全性更新未符合機關規定，3機關未建立Java更新政策，6機關未建立更新檢視機制	各機關應建立使用者電腦軟體安裝、盤點與控管機制。建立各項軟體（含Java與Adobe）更新之檢視週期與更新政策，並留存相關檢查紀錄
組態設定安全防護： 5個機關存在組態設定與機關規定不符合之情形	各機關應建立群組原則定期檢視機制，確認群組原則已成功派送並落實機關規定。針對AD相關管理人員進行教育訓練，提升技術能量，避免因人為疏失或不熟悉操作造成資安漏洞
惡意中繼站連線阻擋： 10個機關存在未完全阻擋惡意中繼站之情形	機關應訂定惡意中繼站名單部署政策，依循政策進行惡意中繼站連線防護，定期抽測惡意中繼站連線防護狀況，才能有效阻擋惡意中繼站連線行為
內網主機滲透測試： 11個機關存在高風險弱點，10個機關存在中風險弱點，13個機關存在低風險弱點	機關宜建立複測機制，針對初測結果進行追蹤與修補。網頁服務過濾SQL語法與特殊字元，以避免SQL Injection與XSS弱點，更新服務主機上相關程式如：Apache等，以避免因版本過舊產生資安漏洞

資通安全稽核(8/8)
- 104年重點工作



- ❖受稽機關（構）
  - 102年為業務機敏及保有大量個資之機關（構）
  - 103年為財經重點及保有大量個資之機關（構）
  - 104年選取原則預計於104年3月底前公布，以利各政府機關(構)事前先辦理資安健診等準備工作
- ❖稽核時間
  - 104年7月-10月
- ❖稽核重點
  - 策略面、管理面、技術面及精進之技術檢測

網路攻防演練(1/11)

- 為提升我政府機關資安防禦及應變能力，資安會報於102年首次辦理國內大規模網路攻防演練，以行政院所屬二級部會行總處署為對象。
- 經提報演練結果後，奉總統指裁示略以：嗣後應每年辦理，並逐步將關鍵基礎設施及其他重點防護對象納入演練中。
- 103年網路攻防演練：
  - 演練期間：10月16日至11月7日
  - 演練對象：
    - 情境演練：都會交通控制系統與網域名稱管理系統
    - 實兵演練（含電子郵件社交工程）：總統府、五院、直轄市政府及各縣(市)政府

網路攻防演練(2/11)

❖情境演練作業

- 情境演練共分**都會交通控制系統**與**網域名稱管理系統**，**各有3個子情境**。演練機關需視情境內容即席回答應變處置作為，並由學者專家提供改善建議

網路攻防演練(3/11)

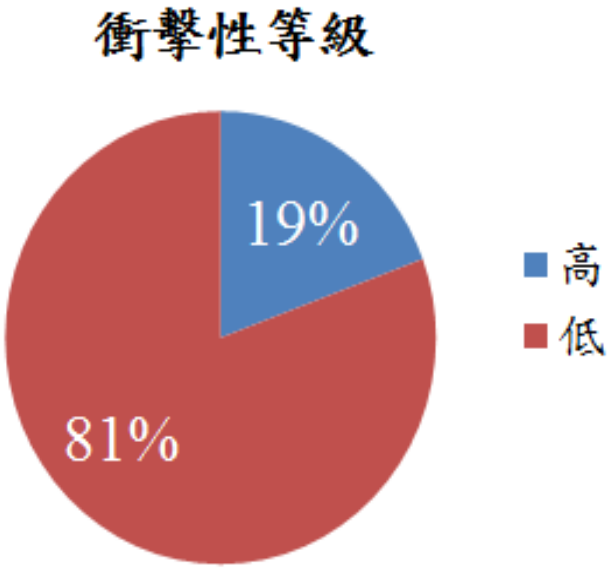
❖ 實兵演練作業

- 以遠端弱點掃描、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
- 2013年OWASP十大弱點測試手法，並增加系統弱點、弱密碼及應用程式弱點等檢測，共計15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)			

網路攻防演練(4/11)

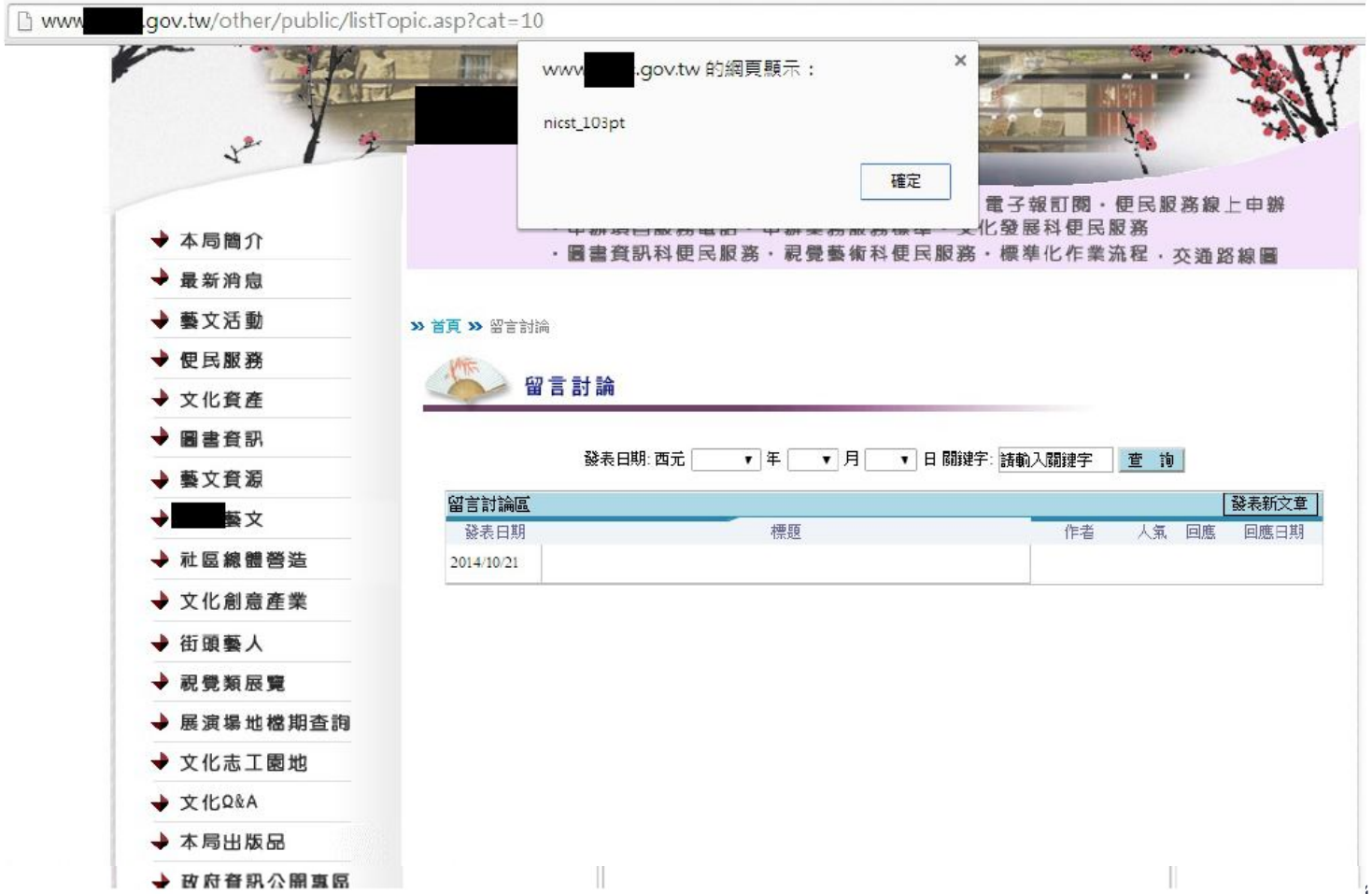
名次	弱點類型	比例
1	跨網站腳本攻擊	41.9%
2	敏感資訊暴露	21.7%
3	不當的安全組態設定	14.7%
4	注入攻擊	12.4%
5	弱密碼	8.8%
6	缺少功能級別的存取控制	0.5%
總計		100%



	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(如XSS)、修改機敏資料等	置入圖片、修改一般資料等
可用性：導致受測目標無法正常運作且該攻擊流程、步驟與結果可重製	受測目標系統或服務停頓	受測目標遭暫時性影響(如網路連線變慢)

網路攻防演練(5/11)
- 常見弱點範例（跨網站腳本攻擊）

❖ **公開討論區可任意留言，嘗試輸入XSS語法，成功寫入資料庫，將影響瀏覽此網頁之民眾**



網路攻防演練(6/11)
- 常見弱點範例（敏感資訊洩漏）

❖ 搜尋機關含有txt的頁面，**發現姓名、性別、年齡及電話等敏感資訊**

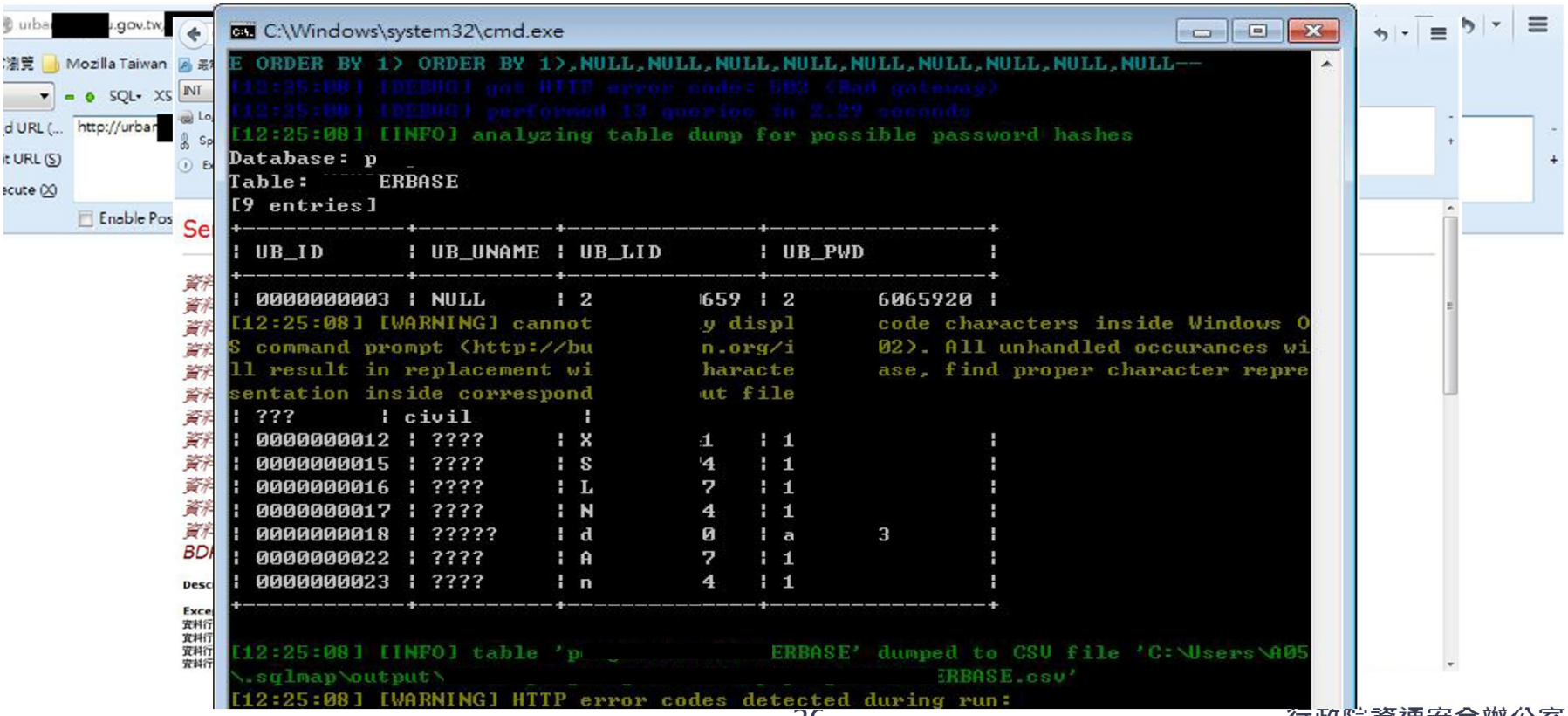
http://histor[redacted]gov.tw/public/OnlineOrder/04151154571.txt
連結下載後檢查確定包含使用者個資

網路攻防演練(7/11)
- 常見弱點範例（不當的安全組態設定）

❖ 測試機關**網頁「忘記密碼」功能**，發現可直接對使用者進行密碼重設，且密碼明文顯示

網路攻防演練(8/11)
- 常見弱點範例（注入攻擊）

❖針對參數進行SQL Injection語法測試，**發現目標網站把所有Table欄位全部列出**，利用sqlmap.py工具列舉資料庫登入表單帳號密碼，**取得帳號密碼**



網路攻防演練(9/11)
- 常見弱點範例（弱密碼）

❖常見<u>弱密碼(admin/admin)或是透露密碼規則</u>

網路攻防演練(10/11)

- 電子郵件社交工程演練：
  - 針對28個機關，共838個郵件帳號，寄發4封測試郵件至受測者
  - 隨機寄發社交工程郵件，並記錄使用者「開啟郵件」及「點閱連結/附件」等行為
  - 設計類社交工程郵件類型(共12種信件)
    - 惡意網頁轉址/惡意word檔：心靈、保健
    - 惡意網頁轉址/惡意rtf檔：八卦、新奇
- 開啟郵件機關數或開啟附件機關數高達60%以上，並有少數機關開啟率超過20%、點閱率超過10%，顯示機關人員資安意識仍需強化。

網路攻防演練(11/11)
- 104年重點工作

- 104年度網路攻防演練將邀請國際專家參與，以相互交流學習彼此經驗。
- 規劃於年中召開網路攻防資安技術研討會，與各機關資訊（安）人員分享常見網站（系統）弱點，以強化機關防禦能量。
- 演練進行方式分：
  - 情境演練：逐步將關鍵基礎設施及其他重點防護對象納入演練。
  - 實兵演練：由攻擊手實際入侵網站（系統），亦包含電子郵件社交工程演練。

政府組態基準(1/2)

- 政府組態基準（Government Configuration Baseline ， GCB)目的在於**規範資通訊設備**（如：個人電腦）的**一致性安全設定**（如：密碼長度、更新期限等），以降低成為駭客入侵管道，進而引發資安事件之疑慮。
- 現行規範
  - Windows 7、IE 8
- 103年重點工作
  - 辦理北、中、南、東16場實機教育訓練
  - 提供電話諮詢服務，協助機關執行部署作業

政府組態基準(2/2)

- ❖ 發展組態基準設定
  - 因應機關使用需求，以及微軟於105年1月終止支援舊版IE瀏覽器，規劃發展Windows 8.1與IE11組態基準
  - 擴展GCB應用範圍，規劃發展無線網路組態設定基準
- ❖ 辦理教育訓練
  - 數位化103年授課內容，提供線上學習
  - 辦理實體授課，推廣Windows Server 2008 R2與Red Hat Enterprise Linux 5等伺服器主機作業系統組態基準

共同供應契約資安服務品項(1/5)

- 行政院資通安全辦公室於102年推動資安服務納入共同供應契約，旨在：
  - 協助機關即時取得服務
  - 訂定資安服務合理價格

- 重要作業包括：
  - 研議資安服務納入共同供應契約之可行性
  - 瞭解政府機關整體資安現況及需求
  - 資安服務之品項規劃及規格確認
  - 協調委辦機關辦理招標相關事宜

共同供應契約資安服務品項(2/5)

❖ 推動過程

102年1~5月	• 與廠商召開14次會議研議資安服務品項 • 邀政府機關召開2次會議研議資安服務規格
102年6月~	• 協調法務部擔任委辦機關，協助辦理招標程序，包括預估採購數量、確認品項規格、協助訂定底價、檢附招標文件函請台銀辦理共同供應契約採購招標作業等
102年10月	• 計價方式採人天費率方式計價 • 共契採購系統介面修改
102年10~11月	• 歷經5次開(跟)標會議，在102年11月14日公告於「政府電子採購網」(LP5-102060)，期限至103年9月30日止
103年6~9月	• 協調法務部協助再次辦理103年資安服務納入共契招標事宜，並於103年10月1日正式上架(LP5-103036)

共同供應契約資安服務品項(3/5)

❖資安服務品項

	品項		說　明	共契案
1	資安健診服務		網路架構檢視、有線網路惡意活動檢視、使用者端電腦檢視、伺服器主機檢視，安全設定檢視	1件
2	SOC監控服務 低流量/ 中流量/ 高流量	SOC監控環境部署	部署監控必要之偵測器與遠端收集設備，並配合安全防護需求，負責監控環境之軟硬體維護升級、調整變更設定及安全架構設計	3件
		監控服務	提供7*24全天候即時遠端資安事件監控服務，包括日誌(Log)分析、警訊判讀、事件通報及處理建議等	
		資安事件(故)處理	監控人員發現並確認為可疑的網路活動或異常資安事件時，須依資安事故處理之標準作業程序進行通報與應變	
		資安威脅預警	國內外資訊安全威脅發表後，提供資訊安全警訊通報服務	
3	弱點掃描服務		針對Web主機或電腦系統進行安全弱點掃描，提供掃描結果分析暨修正建議報告之諮詢服務	1件
4	滲透測試服務		透過模擬駭客的攻擊方式，對目標主機或網路服務進行安全強度的測試，以找出可能的資安漏洞，並提出改善建議	1件
5	社交工程郵件測試服務		提供電子郵件警覺性測試，根據測試結果瞭解可能發生的安全缺口	1件

共同供應契約資安服務品項(4/5)

❖資安服務廠商(藍色字體表示103年10月1日各品項新增之廠商)

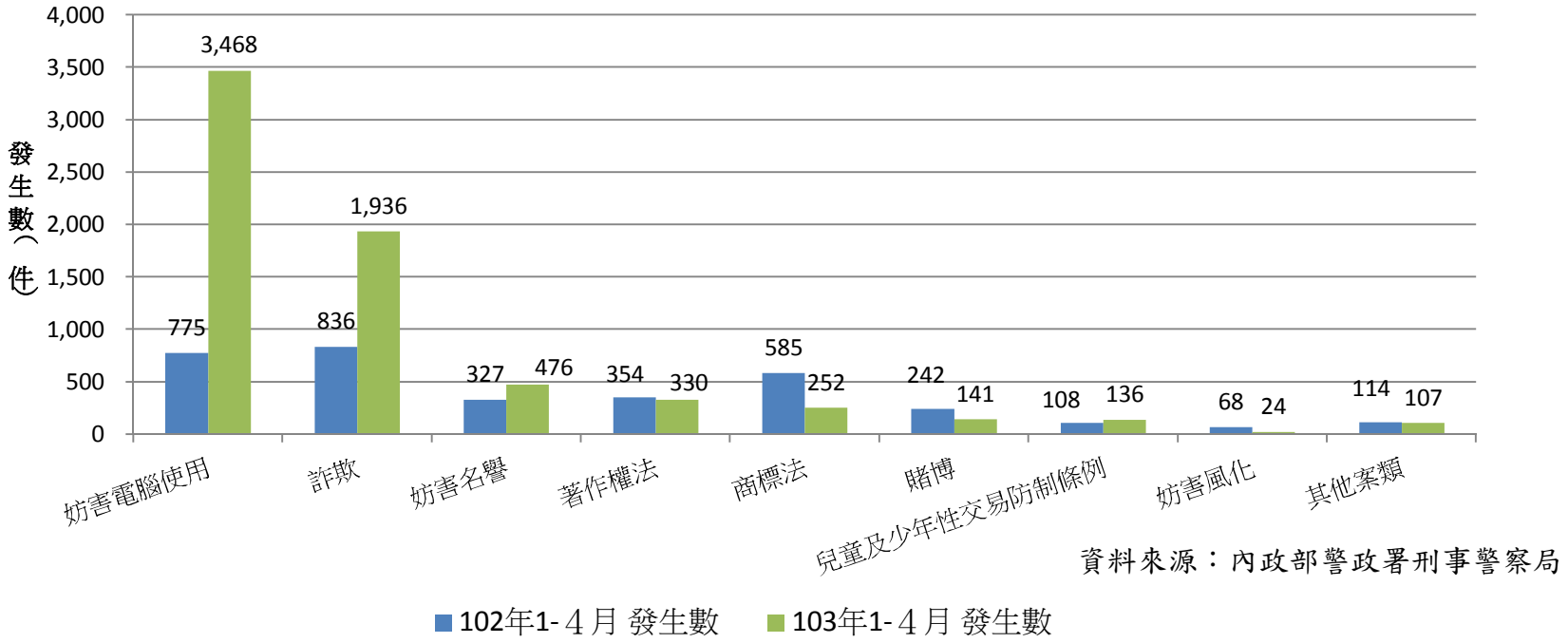
服務品項		服務廠商(按筆畫排序)
資安健診服務		光盾/安碁/果核數位/漢昕/德欣寰宇/數聯/優易/關貿
SOC監控服務	低流量	中華/安碁/果核數位/漢昕/數聯/關貿
	中流量	中華/安碁/果核數位/漢昕/數聯/關貿
	高流量	中華/安碁/果核數位/漢昕/數聯/關貿
弱點掃描服務		中華/光盾/安碁/果核數位/漢昕/德欣寰宇/數聯/優易/關貿
滲透測試服務		中華/光盾/安碁/果核數位/漢昕/德欣寰宇/數聯/優易/關貿
社交工程郵件測試服務		中華/光盾/安碁/果核數位/漢昕/德欣寰宇/數聯/優易/關貿

共同供應契約資安服務品項(5/5)

- 資安會報為建立產官學研資通安全技術交流平台，掌握資通安全技術發展趨勢，充實資通安全作業能量，於101年8月成立「資通安全技術交流小組」。
- 該小組任務之一係「評估資通安全服務供應商能量及專長優劣，提供政府機關選擇委外合作廠商之參考」。
- 103年針對共同供應契約提供資安服務品項之廠商進行評鑑作業。

行動裝置資安強化措施(1/4)
- 網路犯罪現況分析

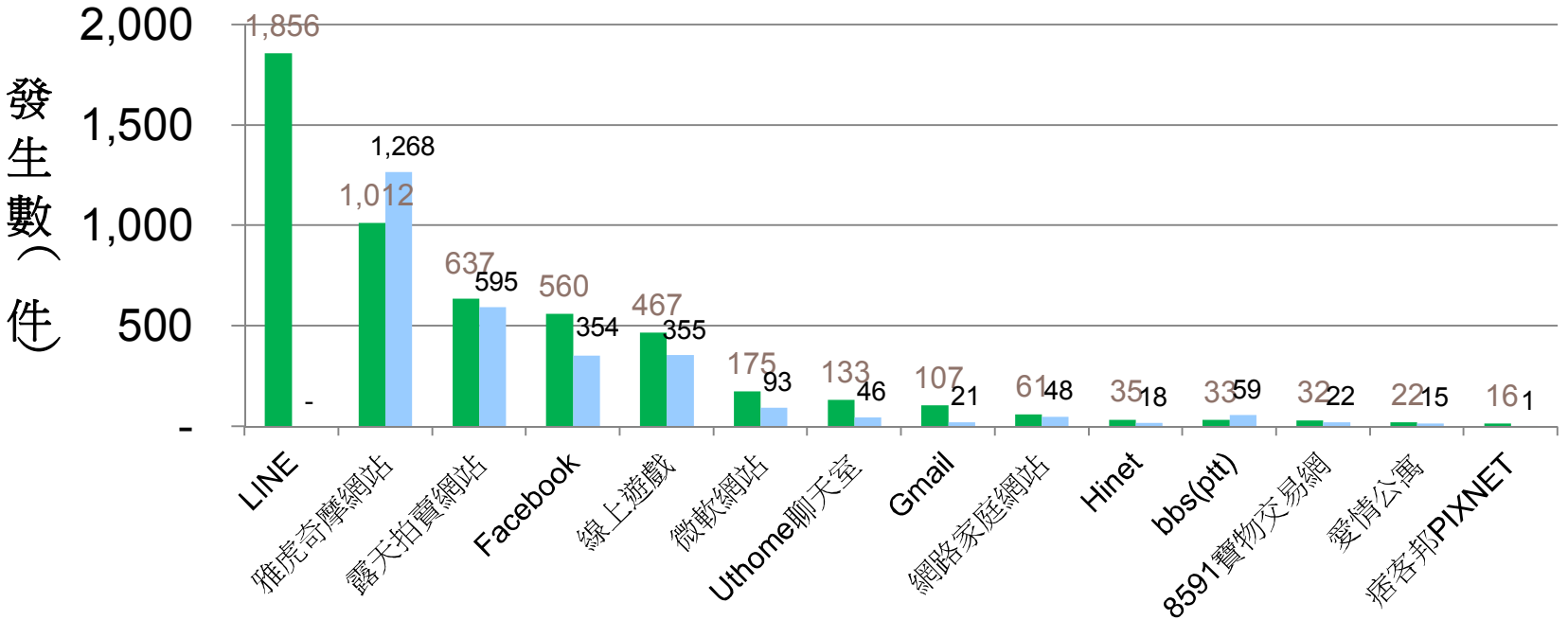
❖103年1至4月與102年同期各類網路犯罪發生數比較



經分析以**妨害電腦使用罪**發生3,468件，增加2,693件(347.48%)最高，**詐欺罪**發生1,936件，增加1,100件(131.58%)次之，近期網路犯罪增長以上述兩種案類為主。

行動裝置資安強化措施(2/4)
- 網路犯罪現況分析

❖103年1至4月與102年同期網路犯罪場所分析



資料來源：內政部警政署刑事警察局

經分析網路犯罪發生場所以「LINE」發生數最多，其中妨害電腦使用罪與詐欺罪總數1,856件最高，顯然網路犯罪已由電腦轉向至智慧型手機，並藉由網路通信便利與匿名特性，造成新型態的犯罪趨勢。

行動裝置資安強化措施(3/4)

❖行動裝置主要資安議題：

- 網路即時通訊軟體(LINE)網路詐騙問題層出不窮。
- 為維護消費者權益，行政院消費者保護處於102年10月針對HTC New One、Samsung Note 3、Sony Xperia Z等三款暢銷智慧型手機進行資安測試，測試結果發現其內建軟體均有資安缺失。
- 日前經媒體檢測，發現大陸手機「小米機」自動回傳使用者個資至中國大陸之伺服器，小米公司回應該連線行為僅在確認手機是否為正版商品等。
- 網路犯罪手法不斷翻新，且往往涉及多個目的事業主管機關，應加強跨部會合作共同防制網路犯罪。

行動裝置資安強化措施(4/4)

- 103年6月24日資安會報第26次委員會議重要決議：
  - 手機與電腦之應用軟體（包含LINE）基本資安規範由經濟部主管，惟手機屬電信法第42條規定之電信終端設備，其出廠時已內建之軟體仍併同硬體由通傳會主管；請前揭二部會依此分工原則積極研議相關管理作為，並規劃制訂資安檢測標準及鼓勵廠商自主驗證等業務。
  - 鑒於網路犯罪問題往往涉及多個目的事業主管機關，且犯罪手法不斷翻新，請內政部定期（每季）召開會議作為溝通協調平臺，並由內政部次長擔任召集人，邀集法務部、通傳會、經濟部、金管會及科技部等相關部會共同研商網路犯罪偵防相關政策與重要業務之推動，期新型態網路犯罪事件發生時，政府機關能儘速提出突破性的作法及有效的管理措施。
  - 為避免公務及機敏資料被不當竊取，各機關應落實辦理公務機關個人電腦非經核准，不可安裝非公務用軟體，包括即時通訊軟體。

結語

- 網路攻擊已成為全球首要安全威脅，而我國面對的是有規模、有組織的網軍，必須從制度、組織及環境等面向，不斷強化資安防禦縱深、健全資安聯防體系及提升資安應變效率，才能因應網軍的挑戰。

- 政府資安防禦亟待補強，落實資安防護措施，提高所屬對資安之警覺，為當前第一要務，敬請全力配合辦理。


行政院資通安全辦公室
Information and Communication Security Office

報　告　完　畢