國中小資通安全稽核標準規範
教育訓練

Time:09:00~17:30

Date:2013年03月26日(二)

Out Line

- 國中小資通安全稽核標準規範與實行作法
- 網站弱點檢測修補
- 殭屍病毒防治
- 國中小資通安全稽核重點與技巧
- 結語

- 國中小資通安全稽核標準規範與實行作法
- 網站弱點檢測修補
- 殭屍病毒防治
- 國中小資通安全稽核重點與技巧
- 結語

- 背景說明
- 教育體系資通安全管理規範介紹
- 國中、小學資通安全管理系統實施原則
  - 文件目標
  - 適用範圍
  - 實施原則
    - 網路安全
    - 系統安全
    - 實體安全
    - 人員安全
    - 法令遵循
- 結語

- 背景説明

背景說明

- 行政院成立「國家資通安全會報」以協助建立政府機關及重要民間業者建立安全之資通訊及網路系統。
- 政府為了滿足各行政單位之需求，民國88年制定了「行政院及所屬各機關資訊安全管理規範」。

背景說明(續)

行政院國家資通安全會報資通安全責任分級

作業名稱 / 等級	防護縱深	ISMS推動作業(註一)	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(註二))	專業證照(註四)	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(註三)	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(註三)	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1次

背景說明(續)

- 由於學術單位與政府機關的屬性不同，雖然行政院已有頒布可依循之規範，但無法適用於教育體系，因此有必要研擬一套專屬的資通安全管理規範。
- 教育部於 96 年 6 月 11 日發函各機關學校公布推動「教育體系資通安全管理規範」及「國中小學資通安全管理系統實施原則」為教育體系 ISMS 建置參考。

背景說明(續)

校園資訊安全服務網

http://cissnet.edu.tw/index.aspx

背景說明(續)

資訊安全管理制度

http://cissnet.edu.tw/rule.aspx

背景說明(續)

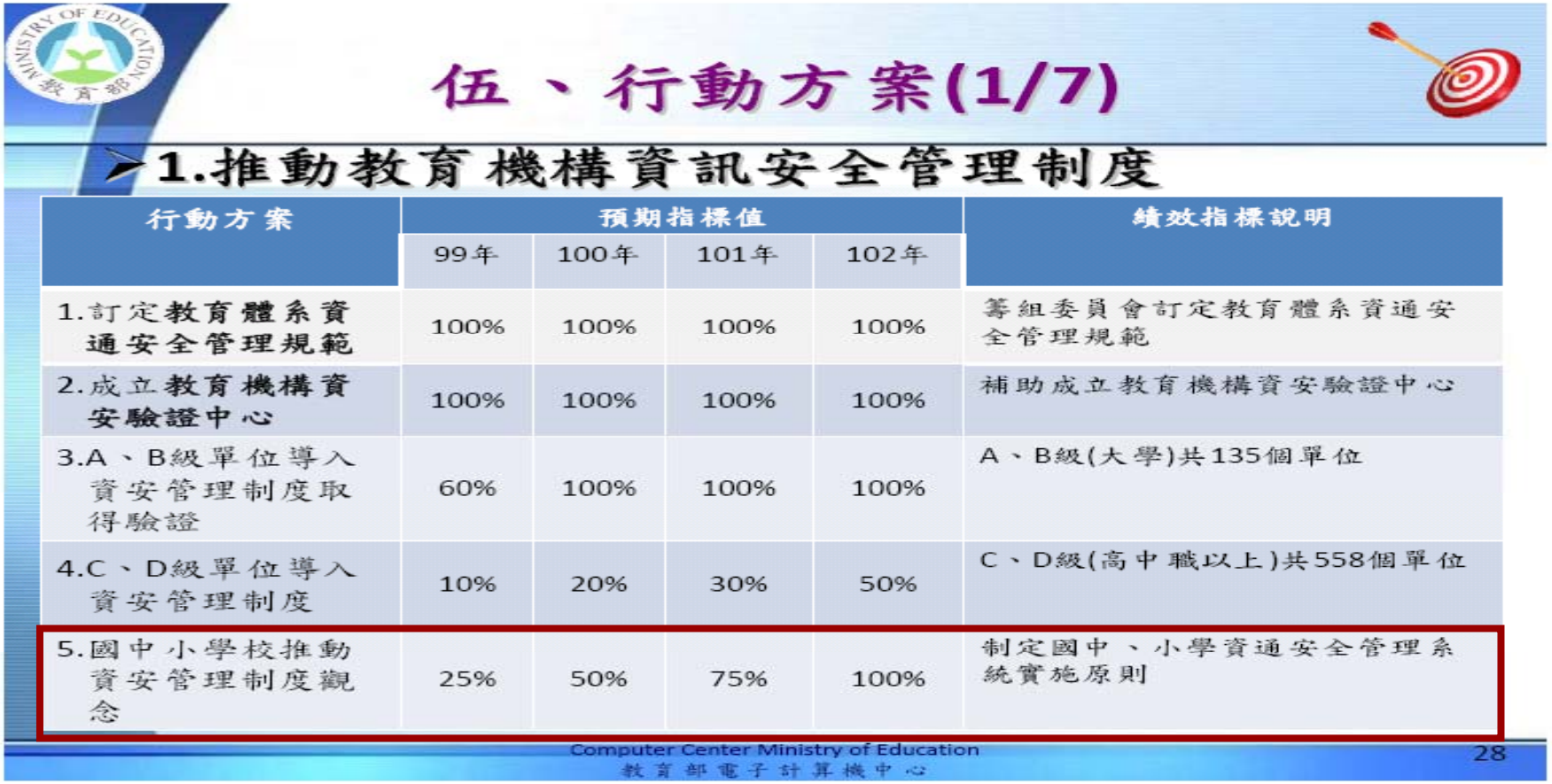
- 教育部針對資訊安全責任分級，規劃教育體系機關學校共分為A、B、C、D四級。

背景說明(續)

學研機關（構）資安等級區分表

類別	內容
A 級 重要核心	● 教育政策主管機關（教育部） ● 教學醫院（台大醫院、成大醫院）
B 級 核心	● 5 所入學考試常設機構 ● 102 所大學 ● 12 個 TANet 區網中心 ● 25 個縣/市網中心 ● 陽明大學附設醫院 【註：承辦入學考試業務機關學校比照 B 級單位】
C 級 重要	● 49 所技術學院及 15 所專科學校 ● 24 個部屬館所
D 級 一般	● 503 所高中職學校 ● 3,412 所國中小學

背景說明(續)



伍、行動方案(1/7)

1.推動教育機構資訊安全管理制度

行動方案	預期指標值				績效指標說明
	99年	100年	101年	102年	
1.訂定教育體系資通安全管理規範	100%	100%	100%	100%	籌組委員會訂定教育體系資通安全管理規範
2.成立教育機構資安驗證中心	100%	100%	100%	100%	補助成立教育機構資安驗證中心
3.A、B級單位導入資安管理制度取得驗證	60%	100%	100%	100%	A、B級(大學)共135個單位
4.C、D級單位導入資安管理制度	10%	20%	30%	50%	C、D級(高中職以上)共558個單位
5.國中小學校推動資安管理制度觀念	25%	50%	75%	100%	制定國中、小學資通安全管理系統實施原則

Computer Center Ministry of Education
教育部電子計算機中心
28

資料來源：

教育部民國99~102年教育體系資通安全發展策略及行動方案

- 教育體系資通安全管理規範介紹

教育體系資通安全管理規範發展背景

- 為協助教育體系各級單位，以有限的成本與時間，達到資訊安全之目標，95年度由成功大學賴溪松教授、NII團隊共同草擬，並邀請產官學研界專家共同檢視與修正。
  - 參考 CNS_ISO 27001、CNS_ISO 27002與我國政府規範等法令標準，訂定出適用於教育體系之資訊安全管理規範。
  - 使各級學校與教育網路中心能以最低成本與時間，建構嚴謹且合適之資訊安全管理系統。
  - 配合教育部規劃之「**教育體系資訊安全管理驗證機制**」，建構國內專屬之第三方驗證標準。

規範設計之準則

- 將CNS_ISO 27001中不適用各連線單位之項目予以調整；並將語義不清或不適用之文字進行修改。
- 參酌CNS_ISO 27002控制措施之最佳實務說明進行實作建議。
- 參酌行政院及所屬各機關資訊安全管理規範為稽核項目範本，並刪除其中不適用之項目。

規範刪除(合併)項目

- 附錄B刪除之規範與控制項(部分刪除項)

A.10.9	電子商務服務	確保電子商務服務的安全，以及被安全的使用。	由於 10.9.1 和 10.9.2 予以刪除，而 10.9.3 內容可與 10.8 合併，因此將 10.9 刪除。
A.10.9.1	電子商務	制定包括電子資料交換、電子郵件和線上交易等電子商務行為之控管措施。	由應用系統的角度來看，電子商務可歸屬於此範圍中，另外連線單位尤其學校鮮少有類似的業務發生，因此予以刪除。
A.10.9.2	線上交易	線上交易資訊應保護防止不完全的傳送、誤傳、未授權的資訊變更、洩露、複製及重傳。	線上交易亦屬於電子商務的一環，因此依據上一條款之理由，予以刪除。

規範刪除(合併)項目(續)

- 附錄B刪除之規範與控制項(部分合併項)

A.13.1.1	通報安全事件	安全事件應循適當管理途徑儘快通報。	由於安全事件或安全弱點皆需盡速進行通報程序，所以將兩項予以整合。
A.13.1.2	通報安全弱點	應要求資訊服務之使用者在注意到系統(服務)有任何明顯(可疑)安全弱點(威脅)時逕行通報。	

適用範圍

- 本標準適用於教育部電算中心、部屬館所、縣市網中心、大專院校以及高中職資訊管理單位等資訊業務相關單位（或其他管理單位認為應加入ISMS規範範圍之部門）。
- 依單位層級區分二群
- 第一群：教育部電算中心、部屬館所、縣市網中心、公私立大專院校（計網中心及校務行政）等。
- 第二群：公私立高中職學校為主要。
- 依業務分為「學術網路系統」與「行政資訊系統」。

ISO 27001與教育體系資通安全管理規範

規範名稱	章節數	控制目標	控制項
ISO 27001:2005	11	39	133項

規範名稱	章節數	控制目標	控制項
教育體系資通安全管理規範	11	36	適用大專院校 100項 適用高中職以下 69項

Information Security Management System (ISMS)

規範內容 – 整體架構

- 資訊安全管理制度建置步驟
  - ISMS之建立(Plan)
  - ISMS之實施與操作(Do)
  - ISMS之監控及審查(Check)
  - ISMS之維持及改進(Act)
- 資訊安全管理系統 (ISMS)建置需求
  - 文件要求
  - 管理階層責任
  - 管理階層審查
  - ISMS之改進

規範內容 – 整體架構(續)

- 控制項 - 共11個領域(1/2)
  - 資訊安全政策訂定與評估 (A.5)
  - 資訊安全組織 (A.6)
  - 資訊資產分類與管制 (A.7)
  - 人員安全管理與教育訓練 (A.8)
  - 實體與環境安全 (A.9)
  - 通訊與作業安全管理 (A.10)

規範內容 – 整體架構(續)

- 控制項 - 共11個領域(2/2)
  - 存取控制安全 (A.11)
  - 系統開發與維護之安全 (A.12)
  - 資訊安全事件之反應及處理(A.13)
  - 業務永續運作管理 (A.14)
  - 相關法規與施行單位政策之符合性 (A.15)

資訊安全管理系統(ISMS)建置步驟

- ISMS之建立(捌、三)
  - 依據該單位之類型、規模、資源、業務特性，定義 ISMS 範圍；考慮相關法律、法規，以及合約之要求，於適度評估風險及應對措施後，訂出經由管理階層核准之ISMS政策，並擬定一份適用性聲明書文件。

ISO
本文4.2.1

- ISMS之實施與操作(捌、四)
  - 施行單位應確實實施控制措施，以符合控管的目標，並執行訓練與認知計畫，確保偵測安全事件的能力，以及迅速回應和應對處理的時效。

ISO
本文4.2.2

資訊安全管理制度建置步驟（續）

- ISMS之監控及審查(捌、五)
  - 施行單位應針對ISMS進行監控程序與其他控制措施，即時鑑別資安事件的發生、處理順序與解決方法；定期審查ISMS有效性（建議一學年至少一次），並將相關有顯著影響之活動與事件記錄下來。

ISO 本文4.2.3

- ISMS之維持及改進(捌、六)
  - 施行單位應定期實行改進活動，採取適當的矯正與預防措施，並得到管理階層之同意，並確保各項措施達到預期目標。

ISO 本文4.2.4

資訊安全管理制度建置需求

- 文件要求(玖、七)
  - 關於ISMS文件化（電子檔案或紙本），必須包含[illegible]、安全目標、ISMS範圍、適用性聲明、資安事件紀錄，以及其他有助於提升ISMS成效之文件；上述之文件需接受保護與管制，並定期的審查及更新，確保文件之最新版本；任何過期文件需保留或銷毀，應予以適當的鑑別。

ISO
本文4.3

- 管理階層責任(玖、八)
  - 管理階層最為重要的是給予承諾及實際的支持，並適度的提供資源以助ISMS程序進行，必要時審查 ISMS 的控制措施與有效性；另外，確保於ISMS範圍內之員工具備足夠之能力及認知，並定期進行教育訓練。

ISO
本文5

資訊安全管理制度建置需求（續）

- 管理階層審查(玖、九)
  - 管理階層應在規劃期間內，審查該單位的[illegible]適用範圍，確保其持續的適用性、適切性及有效性；其中應審查包含變更需求與改進時機，並將其結果確實文件化。

ISO
本文7

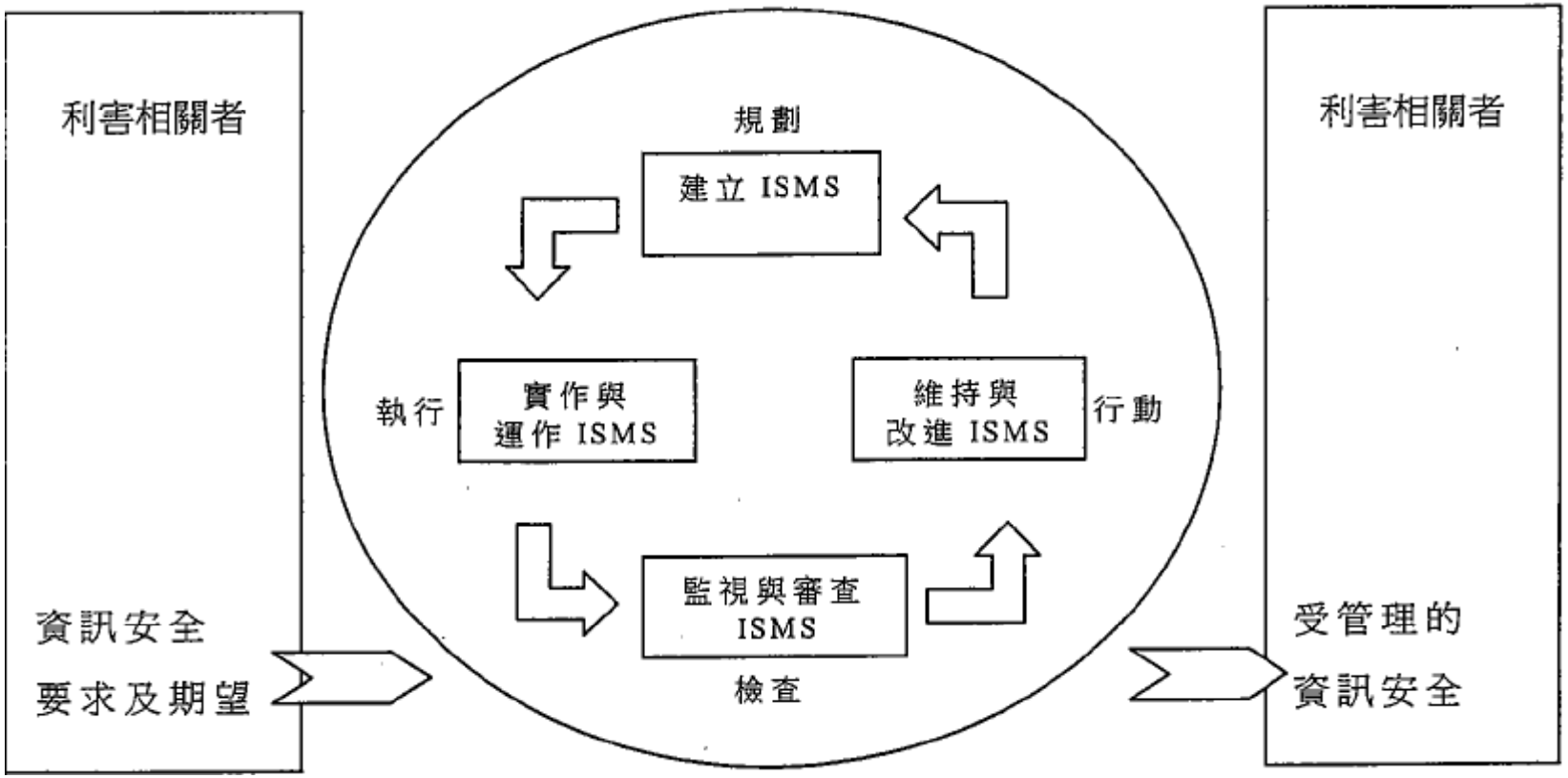
- ISMS之改進(玖、十)
  - ISMS的改進是持續的，必須藉由各資安事件與審查結果，做出適度的反應與改進，持續系統之有效性；另外，對應的矯正措施以及防範未然的預防措施，亦須予以制定並文件化。

ISO
本文8

教育體系資通安全管理規範要求事項

- 上述捌、玖兩節的規範，施行單位必須確實執行，不得因任合因素而有所簡化，甚至避免。
- 將其中過程適度文件化，留存紀錄待查，如此才得由教育部宣告該施行單位之ISMS符合本標準規範。

ISMS(PDCA模型)



- 國中、小學資通安全管理系統實施原則

國中、小學資通安全管理系統實施原則

- 您可以從校園資訊安全服務網站，下載國中、小學資通安全管理系統實施原則。

https://cissnet.edu.tw/images/archive/eduisms-j-960530v1.doc(版本960530版)

國中、小學資通安全管理系統實施原則

- **97年的校園資安計畫，NII已協助修訂國中、小學資通安全管理系統實施原則。**

- 國中、小學資通安全管理系統實施原則
  - 文件目標

文件目標

- 提供國中、小學資通安全管理實施原則指引。

- 國中、小學資通安全管理系統實施原則
  - 適用範圍

適用範圍

- 國中、小學資訊系統及其相關處理設施之管理。

- 國中、小學資通安全管理系統實施原則

  - 實施原則
    - 網路安全

實施原則 – 網路安全

- 網路控制措施
  - 學校與外界連線，宜僅經由縣網中心，以符合一致性與單一性之安全控管要求。
  - 學校內特殊系統（例如會計系統、學生學籍、成績原始資料系統等）宜區隔於網路之外；當有必要透過網路傳輸資料時，應有安全的控管機制如（加密、VPN、SSL 等）。
  - 禁止以電話線連結至電腦主機或網路設備。

實施原則 – 網路安全(續)

- 網路安全管理服務委外廠商合約之安全要求
  - 委外開發或維護廠商必須簽訂安全保密切結書。

保密切結書範本

- 國中、小學資通安全管理系統實施原則

  - 實施原則

    - 系統安全

實施原則- 系統安全

- 集中式管理
  - 學校的行政系統主機（例如財務、人事、公文系統等）電腦，建議由各個縣（市）教育網路中心或教育局等單位**統籌管理**。

實施原則- 系統安全(續)

- 對抗惡意軟體、隱密通道及特洛依木馬程式
  - 學校內的個人電腦應：
    - 安裝防毒軟體，並定期更新病毒碼。
    - 定期（至少每個月）進行如「Windows Update」之程式更新作業，以防範作業系統之漏洞。
- 不得使用非法軟體。
- 新系統啟用前，應經過掃毒與更新系統密碼，以防範可能隱藏的病毒或後門程式。
- 學校對外提供之網頁服務應防範資料庫隱碼(SQL-injection)問題，針對存取資料庫程式碼之輸入欄位進行字元合理性檢查。

實施原則- 系統安全(續)

- 資料備份
  - 學校重要系統（例如系統檔案、應用系統、資料庫等）應定期進行資料備份；建議週期為每週進行一次。

實施原則- 系統安全(續)

- 操作員日誌
  - 敏感度高、或包含特殊資訊的電腦系統應進行檢查、維護、更新等活動，並將這些活動填寫日誌予以記錄，以供查考。
  - 日誌內容應包含以下各項：
    - 系統例行檢查、維護、更新活動的起始時間。
    - 系統錯誤內容和採取的改正措施。
    - 操作人員簽名。

操作員日誌範本

實施原則- 系統安全(續)

- 資訊存取限制
  - 學校宜針對個人隱私資料相關資訊之使用、傳輸與管理，訂定安全的管理規定。
  - 學校內之多人共用的電腦應以特定功能為目的，並設定安全管控機制（例如限制從網路非法下載檔案行為、限制自行安裝軟體行為、限制特定資料的存取等）。

實施原則- 系統安全(續)

- 使用者註冊
  - 學校應制定電腦系統使用者註冊及註銷程序，並透過該註冊及註銷程序來管理使用者存取權限，該作業應包括以下內容：
    - 每位使用者皆有各自的識別碼（ID）。
    - 保存一份包含所有識別碼註冊的紀錄。
    - 使用者調職或離職(留職停薪)後，應調整或移除其存取權限。
    - 定期（建議每學期1 次）檢查使用者之帳號及權限，若有未經授權的帳號產生或不適當之權限設定，應立即調整或取消帳號權限。帳號檢查活動應留存紀錄。
    - 若上述帳號異常狀況研判為駭客入侵應依通報程序處理（參照本文件2.10 段落）。

實施原則- 系統安全(續)

- 特權管理
  - 學校的電腦與網路系統具有最高權限之帳號應建立使用人員清單。
  - 應開啟電腦系統稽核紀錄功能，留存最高權限的使用活動電腦稽核紀錄(log)。 。

實施原則- 系統安全(續)

- 密碼之使用
  - 管制使用者第一次登入系統時，必須立即更改預設密碼。
  - 資訊系統與服務應避免多人使用共同帳號及密碼。
  - 學校應制定及發佈密碼（Password）使用規則[參考優質密碼設定原則與使用原則，附件A-3]，內容應包含以下各項：
    - 使用者應該對其個人所持有密碼盡保密責任
    - 要求使用者的密碼設定，避免使用易於猜測之數字或文字，例如生日、名字、鍵盤上聯繫的字母與數字（如12345678 或 asdfghjk），以及過多的重複字元等。或建議密碼應該包含英文字大小寫、數字、特殊符號等四種設定中的三種。

實施原則- 系統安全(續)

密碼設定原則與使用原則

實施原則- 系統安全(續)

- 原始程式庫之存取控制
  - 應用程式之原始碼存取行為應加以控管。

實施原則- 系統安全(續)

- 通報安全事件與處理：
  - 資訊安全事件包括：任何來自網路的駭客攻擊、病毒感染、資料或網頁遭竄改、以及通訊中斷等。
  - 學校應建立資訊安全事件通報程序，其程序應包括學校內部通報，以及學校與所屬縣市教育網路中心的通報。
  - 當遭遇重大或學校內部無法處理之資通安全事件，應通報其所屬縣市網路中心。
  - 所訂出之資訊安全事件通報程序應公佈於校園內使用電腦與網路之場所，提供使用者瞭解。原始程式庫之存取控制。

實施原則- 系統安全(續)

資安事件通報程序(範本)

資通安全事件通報單(範本)

資通安全事件解除單(範本)

– 實施原則

- 實體安全

實施原則- 實體安全

- 設備安置及保護
  - 學校重要的資訊設備應置於安全地點（如主機機房）並設有空調設施。
  - 學校設置大量資訊設備之地點，如：主機機房、電腦教室區域，應設置滅火設備，並避免堆積易燃物或在區域內飲食。
  - 學校設置大量資訊設備之地點：如主機機房、電腦教室區域內的電源線插頭應有接地的連結或有避雷針等裝置，避免如雷擊事件造成損害情況。
  - 學校設置大量資訊設備之地點，如：主機機房、電腦教室區域，應於入出口處加裝門鎖或其他安全措施。

實施原則- 實體安全(續)

- 電源供應
  - 學校重要的資訊設備應有適當的電力支援設施，例如UPS、電源保護措施，以免斷電或超過負載而造成損失。
- 纜線安全
  - 學校主機機房、電腦教室區域內應使用符合安全要求之纜線並綑綁整齊，必要時以管線包覆。
- 設備與儲存媒體之安全報廢或再使用
  - 所有包括儲存媒體的設備，在報廢或再使用前應先確保已將任何敏感資料和授權軟體刪除或覆寫。設備安置及保護。

實施原則- 實體安全(續)

- 設備維護
  - 設備委託廠商維護時應與廠商建立維護合約，並將安全條款納於合約中。
  - 廠商受託維護設備或執行任務而接觸學校重要或敏感資訊時，須先請其簽訂全保密切結書。
- 財產攜出
  - 財產之攜出應依教育部或學校既有之相關規定處理。包含：
    - 未經授權不得將學校的資訊設備、資訊/資料或軟體攜出校園以外。
    - 財產攜出應予登記並追蹤歸還情形。

實施原則- 實體安全(續)

- 桌面淨空與螢幕淨空政策
  - 學校教職員工於工作結束時，應將其所經辦或使用具有機密或敏感特性的資料（例如公文、學籍資料等）及資料的儲存媒體（如USB 隨身碟、磁碟片、光碟等），妥善存放。
  - 學校提供教職員工或學生使用的電腦應採取適當的安全措施，如鎖匙、登入密碼驗證及設定螢幕保護程式。

- 人員安全

實施原則- 人員安全

- 將安全列入工作執掌中
  - 應將資訊安全要求納入教職員手冊說明中，以強化工作上之資訊安全意識。
- 資訊安全教育與訓練
  - 學校資訊系統管理人員應定期參與資訊安全專業訓練，確保有足夠能力執行任務。
  - 學校應安排全體教職員參與資訊安全教育訓練或宣導活動，以提昇資訊安全認知。

– 實施原則

- 法令遵循

實施原則- 法令遵循

- 法規之遵守：
  - 學校全體教職員應對以下法令有基礎認知，以免誤觸法令。
- 智慧財產權：
  - 應實作適當程序，以確保所使用的資料可能涉及智慧財產權與所使用的專屬軟體產品，可遵循法律、法規及契約的要求。
  - 個人資訊的資料保護及隱私：應如同相關法令，法規及若適用的契約條文所要求的，確保資料保護與隱私。

資訊安全組織(補充)

- 資訊安全長：由校長擔任，負責綜理資訊安全管理作業協調與督導工作。
- 資訊安全執行秘書：由圖書與教學資源中心主任擔任，負責規劃及管理資訊安全管理作業相關事宜。
- 執行小組：由系統管理師擔任，負責執行資訊安全管理作業相關事宜。
- 稽核小組：由人事單位擔任，負責規劃及執行資訊安全管理作業稽核工作。
- 全體人員（含委外廠商）：配合及遵守資訊安全各項要求及規定。

- 國中小資通安全稽核標準規範與實行作法
- 網站弱點檢測修補
- 殭屍病毒防治
- 國中小資通安全稽核重點與技巧
- 結語

網站安全性技術評估

- 為降低弱點存在以及被利用的潛在風險，必須實施有效的資訊環境安全性評估。

- 常見之安全性評估技術：
- 弱點掃瞄(Vulnerability Scan)
- 滲透測試(Penetration Test)

弱點掃描 vs. 滲透測試

- 弱點掃描使用自動化的掃描工具檢查伺服器上的安全弱點
- 不真正執行弱點攻擊程式
- 測試已知的系統安全弱點
- 只是滲透測試的一個步驟
- 滲透測試不只是掃描，同時亦試驗攻擊程式以取得遠端伺服器的控制
- 真正執行弱點攻擊程式
- 包含完整的入侵及試探可能之系統存在的弱點

資料來源: 網頁的危機與防禦 賴溪松 教授

何謂弱點掃描？

- 弱點掃瞄是一種防範未然的資安技術，用來找出資訊環境下的安全性弱點。
- 弱點掃描也可說是通訊埠掃描的進階，通常檢查提供服務的伺服器端程式(Server program)是否具有安全上的漏洞。
- 這種掃描通常都是將一些較簡單的滲透測試的方法加以自動化，以非惡意的方式模擬入侵的行為，當受測的伺服器端程式有某些形式的回應時，就代表這個程式有安全上的漏洞。

為何要弱點掃瞄？

- 以風險角度：
  組織單位環境若存在越多弱點就越容易遭受攻擊

- 既定之事實：
  99% 的駭客利用已知的漏洞入侵

- 組織之策略：
  定期的弱點評估有助於掌握及降低遭受攻擊入侵的風險

弱點掃瞄可以幫助我們什麼?

- 檢測組織單位的安全性政策是否有效及落實
- 檢測防火牆、過濾路由器、入侵偵測等既有安全性機制的運作是否正確無誤且發揮預期效果
- 測試資安防禦系統的保護強度
- 驗證採用安全防禦前後之差異及效果

弱點在哪裡?

- 系統、軟體漏洞
- 作業系統
- Windows / Linux / Unix ……
- 應用軟體
- IIS / Apache / SQL Server ……
- 軟體開發套件
- JAVA / ASP.NET ……

弱點更新來源

- 系統、軟體更新來源
- Microsoft Windows Update、Linux Update……
- 商業化作業系統供應商
- Sun / Apple / HP / IBM / ……
- 軟體開發廠商(Oracle / Adobe / McAfee……)
- 技術開發人員(Java / .NET……)
- 軟體協力開發商(SAP /……)

弱點掃瞄工具

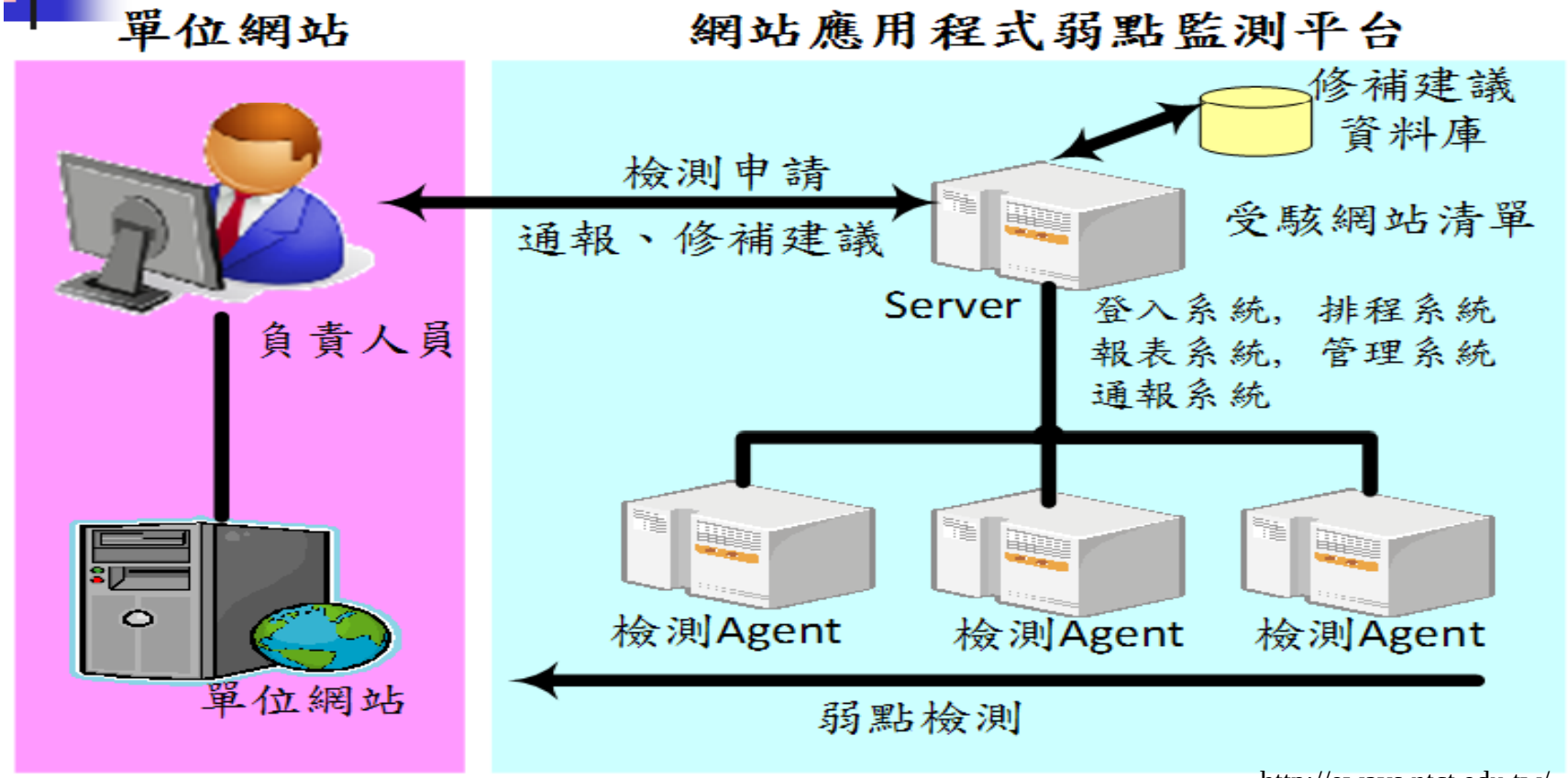
- MBSA, by Microsoft
- Nessus, by the Tenable Network Security
- SARA, by Advanced Research Organization
- VLAD the Scanner, by Razor
- DragonSoft Security Complete Solution 中華龍網

弱點掃瞄作業流程

確認測試主機	前端入口網站、後端資料庫、防火牆
作業平台確認	Windows、Unix、Linux……
選取掃瞄模組	Backdoors、Remote File Access
執行弱點掃瞄	針對已確認之資訊系統進行弱點掃瞄
產出分析報告	針對弱點進行分析、確認高、中、低風險、產出弱點掃瞄報告

教育機構弱點監測掃描平台

網站應用程式弱點監測平台架構圖



http://ewavs.ntct.edu.tw/

資料來源：南投縣教育網路中心營運點

網站應用程式弱點監測平台特色

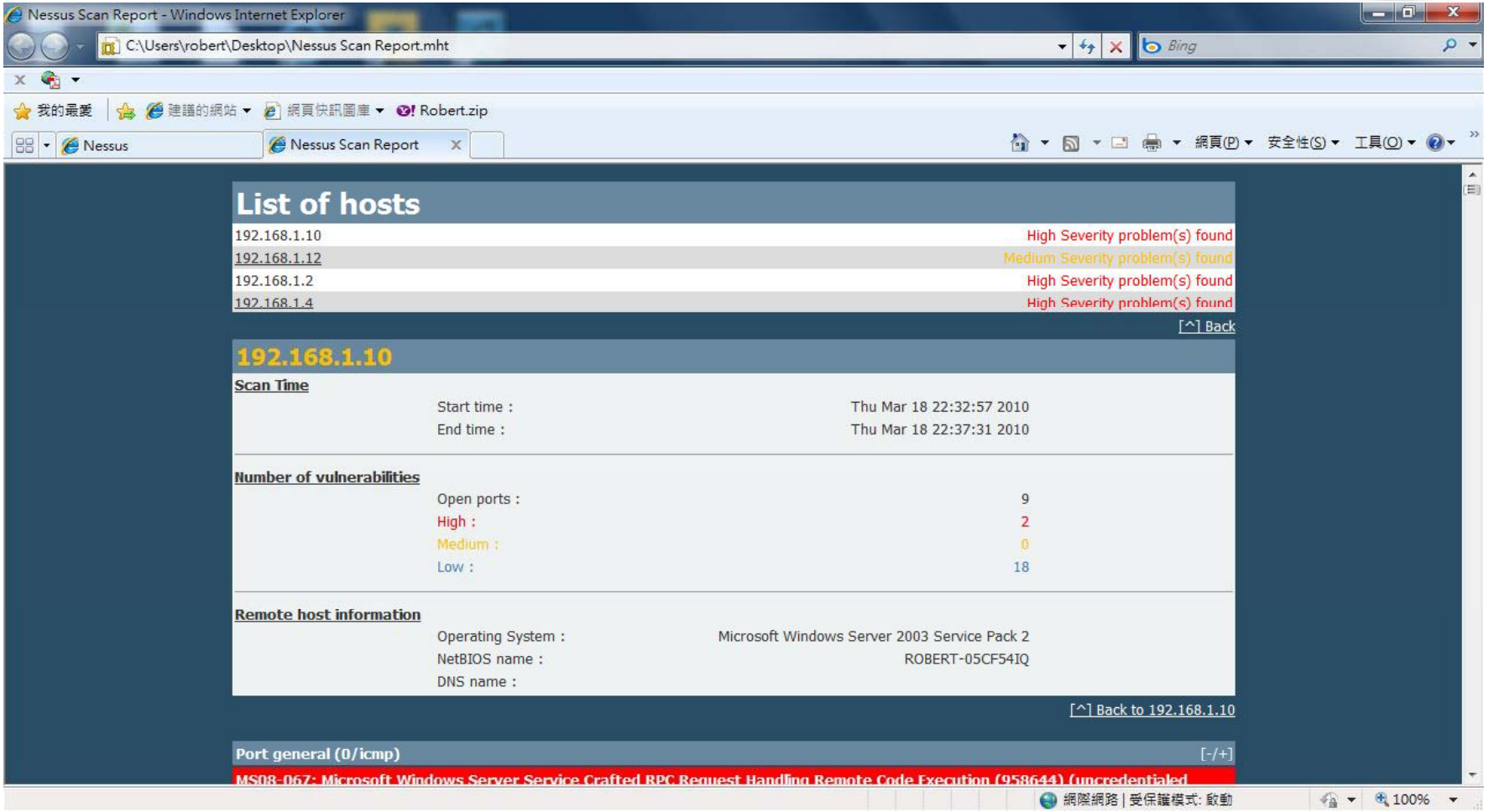
- 智慧型網站搜尋系統
- 多樣化檢測模組
- 人性化排程模組
- 專案式檢測管理
- 完整的報表支援

網站應用程式弱點監測平台流程圖

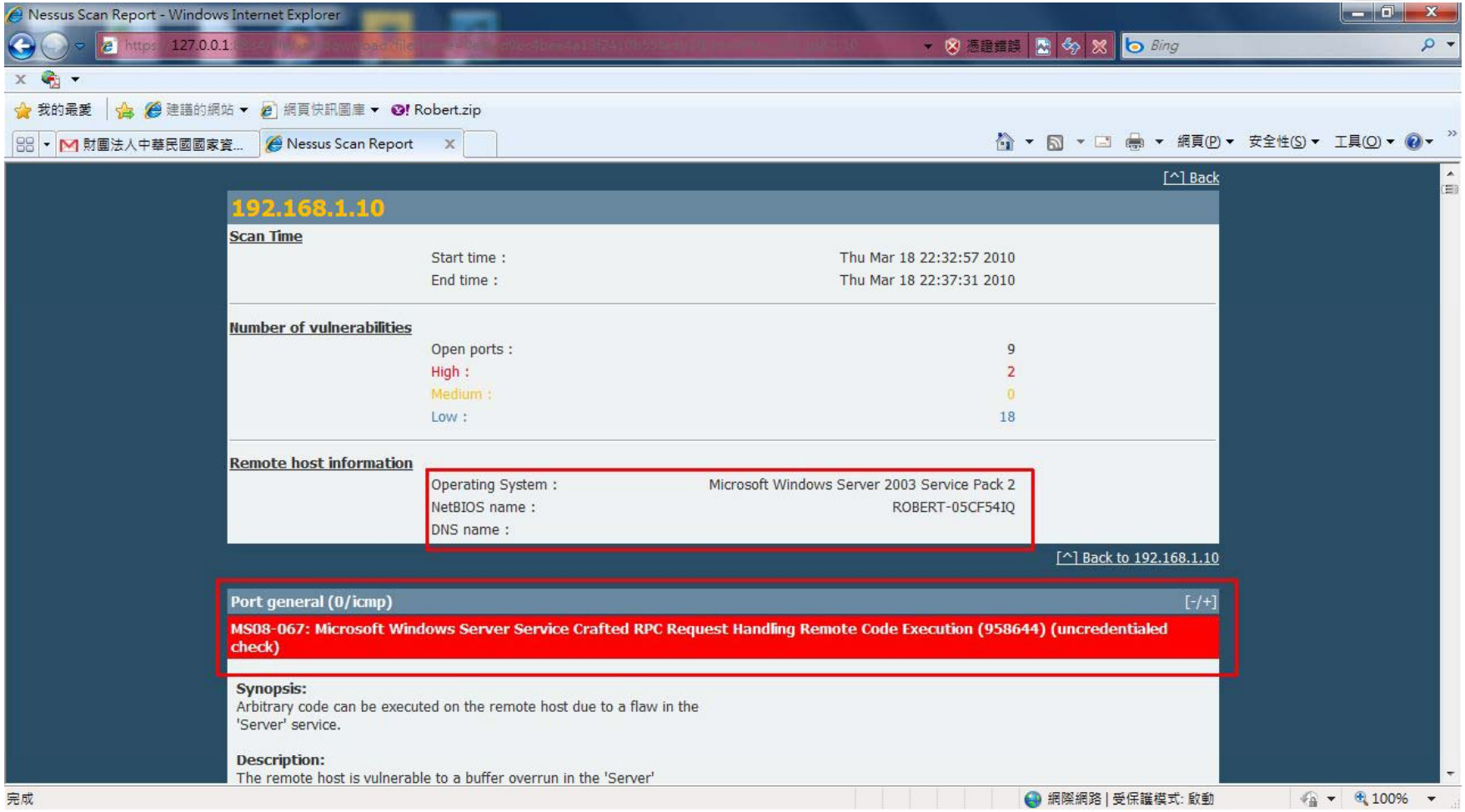
- 1-1.檢測申請 - 使用者帳號申請流程圖
- 1-2.檢測申請 - 網站檢測申請流程圖
- 檢測申請流程說明
- 2.　系統檢測流程圖
- 3-1.　異動流程 - 單位使用者資料修改流程圖
- 3-2.　異動流程 - 檢測網站新增流程圖
- 3-3.　異動流程 - 檢測網站刪除流程圖
- 3-4.　異動流程 – 平台中斷機制
- 3-5.　異動流程 – 取消排程

http://ewavs.ntct.edu.tw/about_content4.html

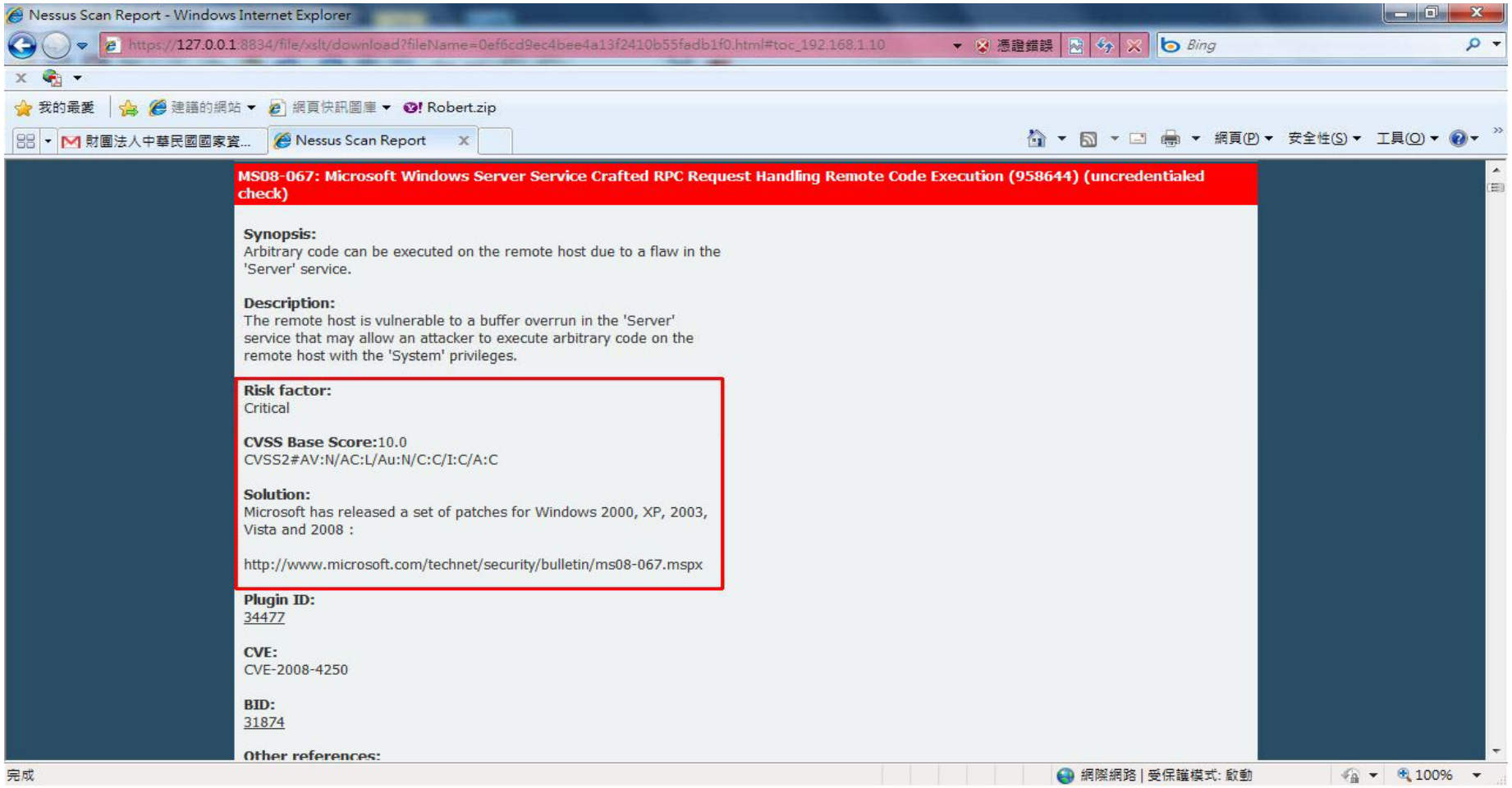
弱點檢測結果分析



弱點檢測結果分析(續)



弱點檢測結果分析(續)



弱點掃描複測

- 完成弱點修補後，需再進行一次弱點掃瞄作業，其目的在於確認弱點已經被正確的修正
- 如複測未通過，可能是下述原因：
- 未確實或正確的執行修正方法或步驟
- 掃瞄工具誤認(false positive)

弱點修補原則

- 優先處理緊急、有立即危害、重要與影響程度高的安全漏洞；其餘輕微甚至毫無影響的漏洞，則視時間、資源與預算考量。

漏洞存在之嚴重性

- 增加駭客攻擊之機會。
- 被當成跳板，攻擊其他單位。
- 資料外洩之風險(隱碼攻擊)。
- 增加病毒感染之機會。

弱點掃瞄注意事項

- 利用非線上時間執行弱點掃瞄
- 事先協調相關單位及人員配合辦理(如：網路或系統廠商、系統負責人)
- 進行掃瞄前，先執行重要系統組態及資料備份
- 注意掃瞄標的
- 掃瞄時可能會造成網路設備異常或當機，如：網路印表機
- 避免進行 DoS等危險的掃瞄模組

弱點掃瞄重要性

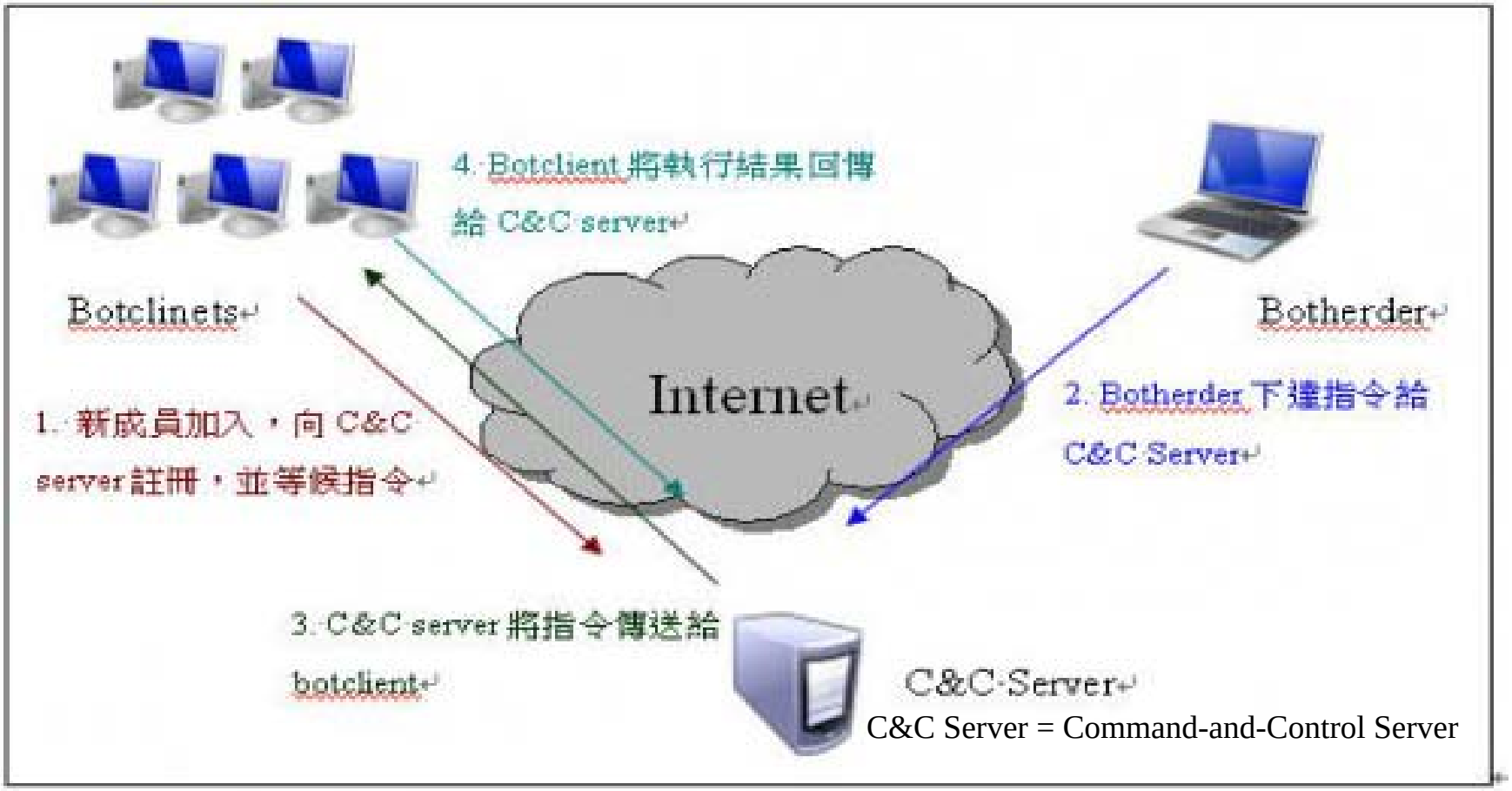
- 弱點掃瞄是不間斷的工作
- 定期弱點掃瞄為必要的資安工作
- 系統通過弱點掃瞄只不過說明已知弱點可能不存在，並不保證系統絕對安全
- 由於漏洞每天都不斷地在被找出來，且駭客的攻擊技術日新月益，所以弱點掃瞄只能當作是一個提升系統安全及降低入侵風險的技術與工作之一

- 國中小資通安全稽核標準規範與實行作法
- 網站弱點檢測修補
- 殭屍病毒防治
- 國中小資通安全稽核重點與技巧
- 結語

殭屍病毒

- 殭屍網路（Zombie Network），又稱BotNet，俗稱「機器人網路」（Robot Network），病毒通常會隨著e-mail、即時通訊軟體（例如，MSN或IRC：Internet relay chat）或電腦系統漏洞，侵入電腦，再藏身於任何一個程式裡。
- BotNet的特性就是，統一發布或執行命令。例如，公司的伺服器管200台電腦，把伺服器關掉，BotNet找不到命令，就無法運作，無法對外發動攻擊。但前提是，要先找到它。

殭屍病毒攻擊示意圖



資料來源：http://domynews.blog.ithome.com.tw/resource/1252/19064#album

殭屍網路造成之威脅

- 擴張地盤
- DDoS攻擊
- 安裝廣告軟體
- 散佈垃圾郵寄及釣魚郵件
- 非法儲存或偷取智慧財產
- 破解密碼
- 點擊詐欺

資料來源：http://domynews.blog.ithome.com.tw/post/1252/36516

殭屍病毒造成之風險

駭客假冒臉書寄通知　網友當心

中央社

2011-05-10 06:25 PM

Fonts Size

Printer-Friendly

讚 成為你朋友中第一個說這讚的人。

Taiwan News (漢文) 的 Facebook

讚 490

（中央社記者吳佳穎台北10日電）臉書（Facebook）用戶小心！資安廠商表示，國外發現針對臉書用戶的惡意程式，會以電子郵件通知用戶密碼更換，要求用戶點擊附件下載密碼，使電腦感染中毒，網友切勿上當。

Facebook變粉紅超可愛？　小心變惡意程式幫手

湯蕙如

2012年1月13日 13:17

333 333 2 +1

記者湯蕙如／綜合報導

看膩 Facebook 呆板的藍色介面，想換個粉紅裝飾一下？小心被惡意程式纏上身！最近有個標榜可以幫 Facebook 換張「臉」的應用程式「Switch To Pink Facebook」（或紅、藍、黑色），看起來好像超級貼心，只要點幾個按鈕，就能擁有自己風格，但真相卻是惡意程式悄悄入侵臉書！

Switch To Pink Facebook (Limited Time!)

t.co

Say Good Bye to your boring old Blue Theme!

Like · Comment · Share

號稱可以幫Facebook介面換顏色的「Switch To Pink Facebook（Limited Time）」，但他實際是個惡意程式。（圖／擷取自Facebook）

駭客開始以臉書等受歡迎的社群網路服務為誘餌，假冒客服人員或製作假程式吸引網友上鉤。

(上圖)資料來源: 中央通訊社
http://www.cna.com.tw
(下圖) 資料來源: 今日新聞網
http://news.cts.com.tw/

殭屍病毒造成之風險

瘋啥？下載中國版《憤怒鳥》 恐中毒

2012年04月16日 讚 479 +1 9

有毒的《憤怒鳥》安裝後看起來與正版一樣，但已被植入木馬程式。翻攝網路

你是對岸「免費」Android軟體的愛用者嗎？如果你的hTC、三星或SONY手機最近曾安裝中國網站上的《憤怒鳥太空版》（Angry Birds Space）遊戲，小心已經中毒了。

「太空版」有木馬

網路資安公司Sophos警告，這款《憤怒鳥》系列最新一代遊戲，已發現暗藏木馬程式的版本，遊戲可以正常運作，但手機會被駭客操縱，帳號隱私全都露。

《憤怒鳥太空版》在iPhone、iPad以及Android手機平台都有推出，iPhone版售價約30元台幣，iPad版售價約90元台幣，Android的版本則是免費，但會有廣告。中毒的都是Android版本。

App藏病毒 「食人魚」吞2.3億 百款惡意程式多扣話費 「比賣毒還好賺」

綜合報導

中國近來出現手機惡意軟體，中毒的手機會每月自動多扣用戶話費，至上月中國已有超過21萬支手機中毒，估不法份子一年可獲利逾2.3億元台幣。

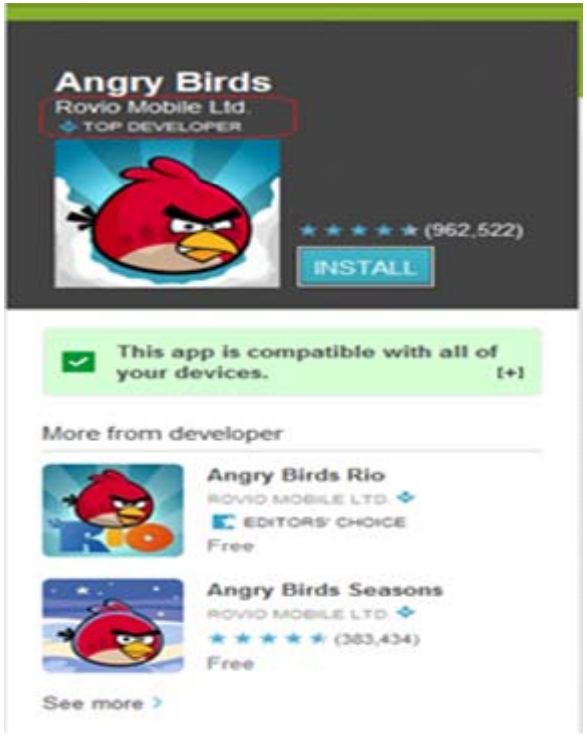
河北的趙小姐平常手機話費每月約230元台幣，但從去年12月開始，月租費突暴漲1倍以上；北京的李先生為手機儲值460元後，3天就用完了，兩人分別將手機送檢查，才發現是他們所下載的應用軟體中藏有病毒。

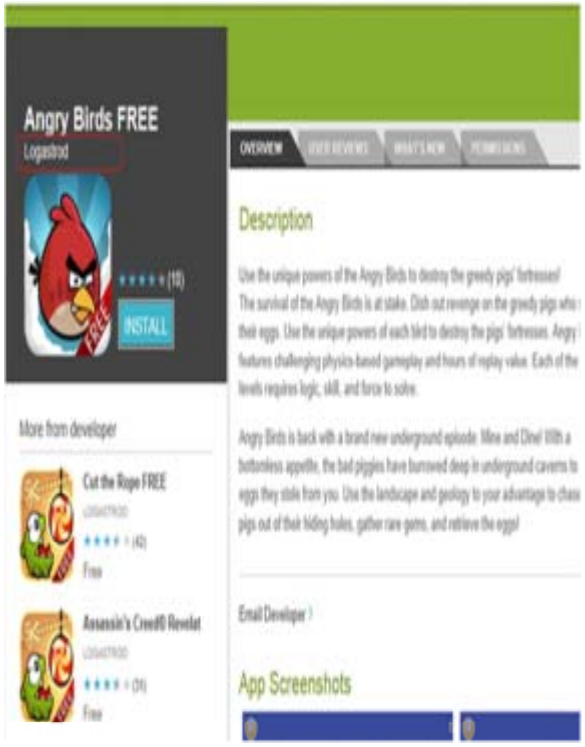
不少惡意程式直接偽裝成一般App內容並在線上商店提供下載安裝，一旦使用者安裝，駭客可能會因此竊取個資，或能夠控制被害者的手機。

(上圖)資料來源: 蘋果日報
www.appledaily.com.tw/
(下圖) 資料來源: 爽報
www.sharpdaily.com.tw

殭屍病毒攻擊手法

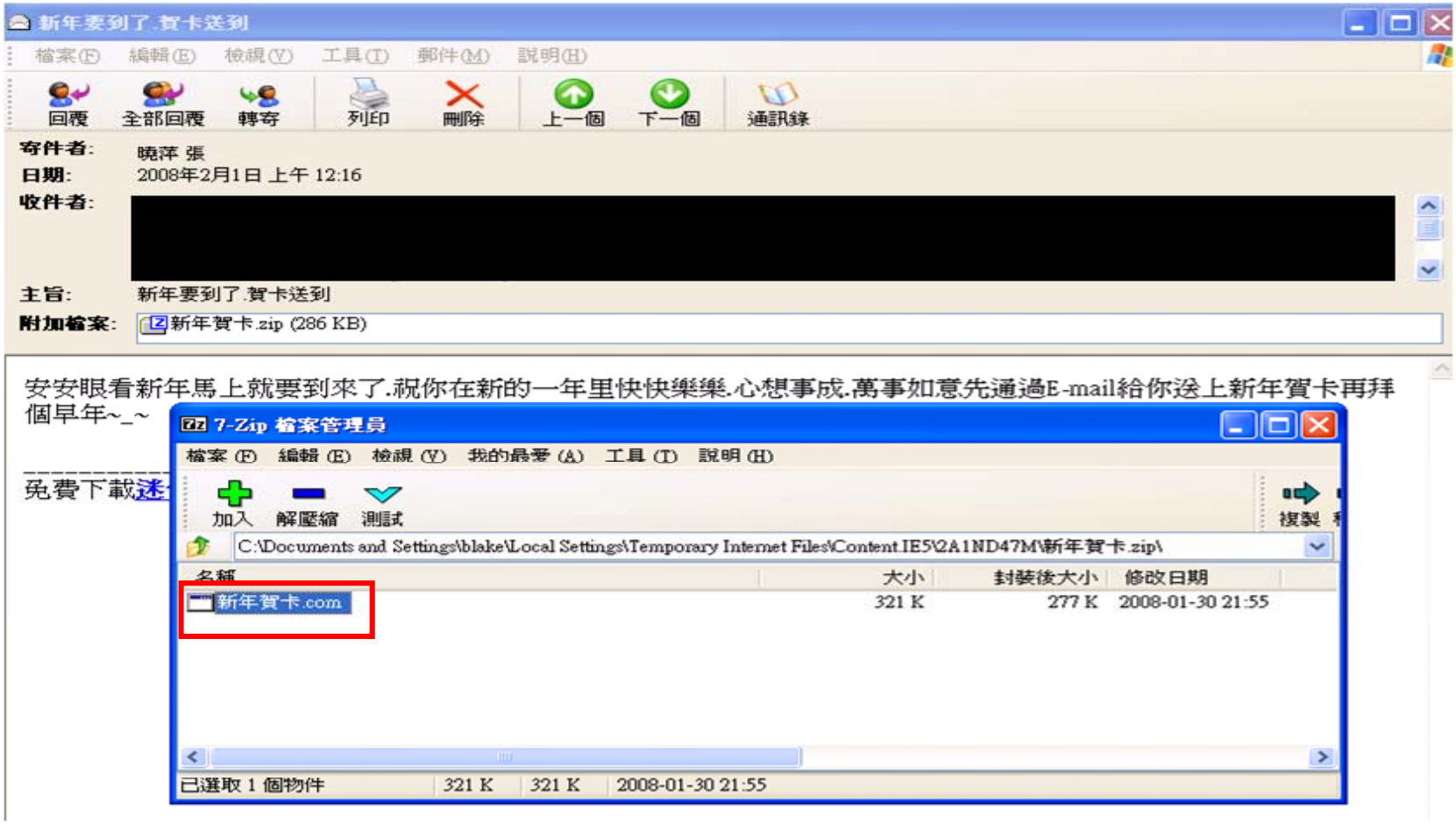
- 網路犯罪分子經常會利用某些應用程式的流行而去偽裝成它們。但是，因為它們不能以原始開發者的名義發佈，所以開發商的名稱可以說是合法軟體的好指標。**比方說，真正的憤怒鳥在*Android Market*網頁上顯示是由Rovio Mobile所開發的，但是惡意程式版本的開發者是*Logastrod*：**





原文出處：[Checking the Legitimacy of Android Apps]

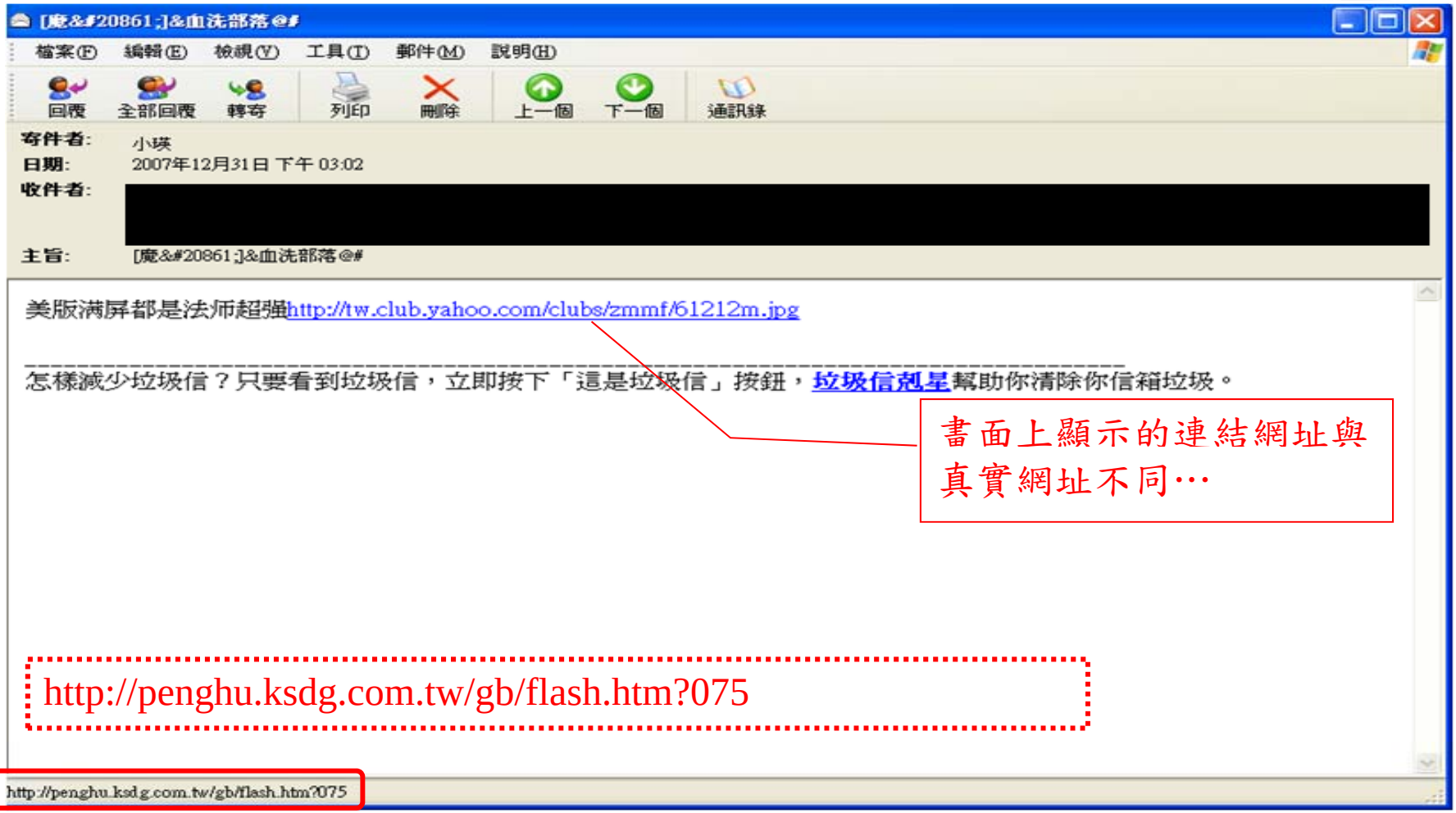
殭屍病毒攻擊手法(續)



殭屍病毒攻擊手法(續)

寄件者	主旨	收到日期
vsfzijkmwm@pcho...	酒店妹'為一千塊被玩爽的真不...	1/28 (五) 6:21 PM
全台獨家無碼棒.真...	每日新片.隨插即看 全台獨家...	1/21 (五) 11:21 PM
Lucien Jacobson	GUCCI名牌包包`通通2990元	1/20 (四) 3:33 PM
◆■◆◆■••◆...	大批女明星"不雅照再現網路...	1/19 (三) 3:38 AM
專辦銀行企業放款...	信保基金到單代償,臨時營運週...	1/18 (二) 9:01 AM
qzfegn gvq	強站阮體中心一定有你要得物品	1/17 (一) 2:15 PM
您多久沒替自己買...	Yahoo!奇摩拍賣 問題：dqcw...	1/17 (一) 1:57 PM
3w5tr	遊戲 電影 音樂 情色更新速度...	1/17 (一) 12:29 PM
qzfegn gvq	最多得超級專家盒即~持續發...	1/17 (一) 10:10 AM
3w5tr	產品最低75元8fY8Sq0e 0c2y27	1/17 (一) 9:34 AM
資訊人員培訓機構	ＩＴ能力職場生存問券(sam99...	1/17 (一) 9:31 AM
qzfegn gvq	強檔超促銷狂賣中	1/17 (一) 8:30 AM
5R3W	3天內送達ocHaPVE	1/17 (一) 8:13 AM
5R3W	採用sony品質最好的遊戲片jc...	1/17 (一) 7:54 AM
5R3W	遊戲 電影 音樂 情色更新速度...	1/17 (一) 7:05 AM
3w5tr	3天內送達lfapj	1/17 (一) 6:37 AM
qzfegn gvq	本次都有最新、最炫、最棒得...	1/17 (一) 4:36 AM

殭屍病毒攻擊手法(續)



殭屍病毒攻擊手法(續)

- 利用偽造的網頁作為誘餌，詐騙使用者洩漏如帳戶密碼等個人機密資料
- 釣魚網頁畫面與官方網站相同 ，但其實這個網址並非官方網站
- 以相似的字元來偽裝網址，
  例如：以數字來替換英文

殭屍病毒攻擊手法(續)

- 安裝免費軟體時，有可能同時間被植入病毒。

資料來源：http://richardfx.blogspot.tw/2009/08/opencandy.html

殭屍病毒攻擊手法(續)

- 間諜流氓軟體(opencandy)安裝進你的電腦，有洩漏個人私穩及電腦資料的風險。
- opencandy它是經營軟體廣告的中介人公司。
- Opencandy是未經許可便安裝到電腦中。
- 程式會偷偷地連結至網上該公司伺服器(收集有關被推薦軟體安裝與反裝的資訊以供統計分析使用的)。
- 無法透過「正途」把它移除，這是嚴重侵害電腦用家對電腦使用及控制的應有權利。

資料來源：http://richardfx.blogspot.tw/2009/08/opencandy.html

殭屍病毒攻擊手法(續)

- Opencandy在安裝進你的電腦前，應先告知相關資訊，例如：尊重安裝及使用者的「自由權益」、「知情權益」及「私隱權益」。
- 廣告程式不應在無聲無色的情況下，以欺騙/強逼的方式安裝到使用者電腦中。

資料來源：http://richardfx.blogspot.tw/2009/08/opencandy.html

殭屍病毒攻擊手法(續)

- 如何清除Opencandy，步驟如下：
  - 開始→執行→輸入(regedit)。
  - 進入「登錄編輯程式」後，順序找尋：「HKEY_LOCAL_MACHINE > SOFTWARE > OpenCandy」的位置。
  - 在Opencandy資料夾上按右鍵，選擇「刪除」(Vista會多一些確認提示，全都選是就對了)，之後重新開機就行。
  - 最後，最好用「編輯」>「尋找」，輸入opencandy作搜查，找到刪除後再選「找下一個」，直到不再發現任何opencandy的資料為止，務求徹底清理)。

資料來源：http://richardfx.blogspot.tw/2009/08/opencandy.html

殭屍病毒造成之危害

- 使電腦或手機無法運作
  - 最常見的病毒危害
- 導致電腦或手機中儲存的個資遭竊
  - 駭客可能將竊取得個人資料用於詐騙或冒用身分等不法行為
- 傳播非法訊息
  - 以被害人的名義透過簡訊或電子郵件，大量對外散布色情、非法圖片等訊息
- 手機電話帳單金額莫名其妙地暴增
  - 惡意程式會自動傳送簡訊或撥打付費電話

殭屍病毒防範

- 安裝防毒閘道器
- 進行系統更新
- 良好的網路使用習慣
  - 不連結不明網站
  - 下載免費軟體應至官網下載
  - 不在網路上洩漏敏感性個資(社群網站)
- 安裝防毒軟體
- 後門程式檢測

- 國中小資通安全稽核標準規範與實行作法
- 網站弱點檢測修補
- 殭屍病毒防治
- 國中小資通安全稽核重點與技巧
- 結語

稽核基本觀念

- 資訊安全管理系統要求事項
  - 組織應規劃稽核計畫，界定稽核範圍、頻率及方法
  - 依規劃的期間施行資訊安全管理系統內部稽核
  - 稽核人員應遵守稽核準則，不應稽核本身的工作...等規範

•符合「教育體系資通安全管理規範」及相關標準、法律或法規的要求
•符合所識別的資訊安全要求
•有效的實作與維持

稽核基本觀念(何謂稽核)

- 稽核是由有能力且獨立之人員客觀取得與評估證據，以支持其聲明是否符合之報告的系統化過程。

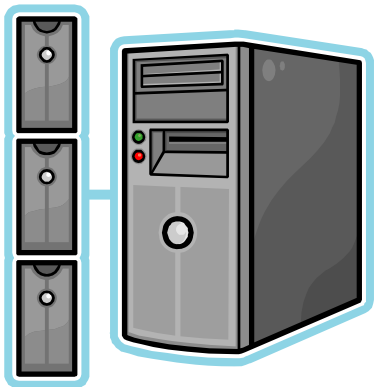
- ISO 19011**定義
  - 透過系統化、獨立性及文件化的流程取得稽核證據，並透過客觀地評估，以鑑別其稽核準則所涵蓋的範圍是否達成。

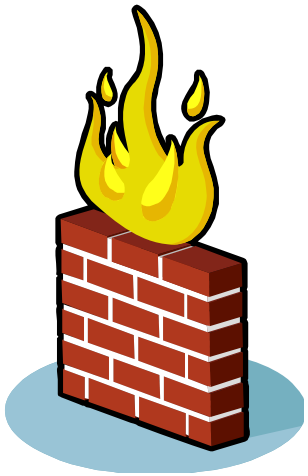
** ISO 19011 「品質與/或環境管理系統稽核指導綱要」

稽核基本觀念(關鍵字Key Words)

稽核基本觀念(定義)

- 資安稽核之定義為
  - 對資訊及其處理設施或系統(含相關聯之非自動化處理部分，及其間之介面)各方面或各部分之查核評估。





稽核基本觀念(符合目標)

- 資訊安全稽核的目標
  - 確保單位遵循資訊安全政策及標準程序、衡量資訊安全管理制度之有效性
  - 例如：
    - 控管程序是否落實
    - 檢查與評估資安控制措施之缺失
    - 評估管理成效...

稽核基本觀念(稽核人員的素養)

- 熟悉欲驗證之標準或規範
- 具備正確的資安認知
- 瞭解職業道德規範
- 稽核技巧熟練
- 正確的心態
- 開放的心胸

稽核基本觀念(稽核測試的方式)

- 遵循測試
  - 測試是否遵循其要求執行
    - 法令、法規、契約要求
    - 驗證標準
    - 制度、規範、程序
- 證實測試
  - 測試其執行結果與要求或預期相符合
    - 系統功能
    - 公式、計算結果

稽核基本觀念(問題思考)

- 請問以下案例屬「遵循測試」或「證實測試」？

案例1
稽核人員發現作業人員確實依規定於每週一上班前檢查並維護機器。

遵循測試

證實測試

案例2
稽核人員發現資訊資產清冊所列設備清單有所遺漏。

證實測試

案例3
稽核人員發現系統未能依組織政策在帳號輸入密碼錯誤達5次以上時，自動鎖定帳號。

稽核基本觀念(稽核技巧)

- 說(訪談)、寫(文件)、做(實地)是否一致。
- 聆聽受稽單位的執行說明，思考可能遺漏的環節。
- 善用執行程序的連貫性來稽查是否確實落實。
- 使用客觀、顯著、可驗證性的證據來判別與撰寫稽核發現結果。

稽核基本觀念(稽核查檢表)

南投縣國民中、小學資訊安全與個資管理內部稽核表					
文件編號		機密等級	敏感	版本	1.0

填表日期：　　年　　月　　日

稽核單位：	
稽核地點：	
參考條款：	國中小資通安全管理系統實施原則（中華民國96年5月30日版）、教育機構個人資料保護工作事項（教育部 100年度提升校園資訊安全服務計畫）
稽核日期：	
稽核範圍：	國中、小學內電腦、資訊與網路服務相關的系統、設備、程序、及人員。

適用對象：
本稽核表之設計主要參照「國中小資通安全管理系統實施原則」及「教育機構個人資料保護工作事項」（以下簡稱規範）之內涵，並沿用規範所定義之適用範圍與對象。本表適用對象爲南投縣國民中、小學。

評分標準說明：
A：相關資訊安全與個資管理制度規範已建立，且落實執行
B：相關資訊安全與個資管理制度規範未建立，但已實施替代性資安控管措施
C：相關資訊安全與個資管理制度規範已建立，但未落實執行
D：相關資訊安全與個資管理制度規範未建立，且未實施替代性資安控管措施
E：不適用

稽核基本觀念(稽核查檢表填寫標準)

- A：相關資訊安全與個資管理制度規範已建立，且落實執行

你可以這樣判斷

單位已制定相關管理規範，且已落實執行。

例如：單位已依照程序要求，每年進行帳號權限清查，並留存帳號權限清查紀錄，留存被查。

稽核基本觀念(稽核查檢表填寫標準)

- B：相關資訊安全與個資管理制度規範未建立，但已實施替代性資安控管措施

你可以這樣判斷

單位未制定相關管理規範，但已有相關執行方式落實進行。

例如：單位已要求每6個月定期變更密碼，但未明確規範於程序文件中。

稽核基本觀念(稽核查檢表填寫標準)

- C：相關資訊安全與個資管理制度規範已建立，但未落實執行

你可以這樣判斷

單位已制定相關管理規範，但未落實執行。

例如：單位已要求個人電腦應設定螢幕保護程式，15分鐘無動作時，自動鎖定電腦，但單位未落實執行。

稽核基本觀念(稽核查檢表填寫標準)

- D：相關資訊安全與個資管理制度規範未建立，且未實施替代性資安控管措施

  你可以這樣判斷

  單位未制定相關管理規範，且未落實執行。

  例如：單位未規範重要電腦資料應定期備份，備份執行週期，由系統管理人員自行決定。

- E：不適用

  單位內無此項業務。

稽核實務與施行

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
1.2	網路安全管理服務委外廠商合約之安全要求				
1.2.1	保密條款之簽訂	委外開發或維護廠商必須簽訂安全保密切結書，確保其了解應有之資安責任與相關限制[參考文件編號A-01]。	□ □ □ □ □	□ □ □ □ □	

你可以這麼做

請委外廠商簽署保密切結書。

於稽核時提供資訊服務委外保密切結書，供稽核人員抽查，確認該控制點，已被有效落實。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
2.6.1	記錄日誌內容	日誌內容可包含以下各項： 系統（例行檢查、維護、更新）活動的起始時間、系統錯誤內容和採取的改正措施[參考文件編號A-02] 紀錄日誌項目人員姓名與簽名欄	□□□□□	□□□□□	

你可以這麼做

將每日資訊設備狀態紀錄於電腦系統操作日誌表。

於稽核時提供電腦系統操作日誌表，確認資訊設備之維護，已被有效落實。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
2.6	使用者註冊				
	使用者註冊之管理	學校應制定行政系統（如公文管理系統、勞健保）使用的使用者註冊及註銷程序[參考文件編號A-03、A-04]，透過該程序來控制使用者資訊服務的存取，該作業應包括以下內容： 使用唯一的使用者識別碼（ID）。 檢查使用者是否經過系統管理單位之授權使用資訊系統或服務。 保存一份包含所有識別碼註冊的記錄。 使用者調職或離職後，應移除其識別碼的存取權限。	□ □ □ □ □	□ □ □ □ □	

稽核實務與施行(續)

你可以這麼做
落實使用者註冊、變更及註銷程序。
於帳號新增、異動時，填寫行政系統帳號申請表。
人員職務異動時，填寫異動移交流程表。
於稽核時提供行政系統帳號申請表、異動移交流程表，確認使用者帳號，依職務確實被有效(或)停用權限。

稽核實務與施行(續)

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.6.3	人員異動	處理個人資料檔案之人員，其職務如有異動，應將所保管之儲存媒體及有關資料列冊移交 [參考文件編號A-05] 接辦人員除應於相關系統重置通行碼外，應視需要更換使用者識別帳號。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

你可以這麼做

人員職務異動時，填寫異動移交流程表。

於稽核時提供異動移交流程表，確認人員職務異動已按照流程進行職務交接與物品歸還等。

稽核實務與施行(續)

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.6.4	離職註銷	處理個人資料檔案之人員，應簽訂保密切結書[參考文件編號A-06]，並確認於離職時或合約終止時取消或停用其使用者識別帳號，且收繳其通行證及相關證件。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

你可以這麼做

人員到職時，應請人員簽署個人保密切結書。

人員離職時，應填寫異動移交流程表，確認人員離職已按照流程進行職務交接與物品歸還等。

於稽核時提供行個人保密切結書，確認人員已簽署完成。

稽核實務與施行(續)

2.8	通行碼之使用				
2.8.2	通行碼之設定原則	由學校發佈通行碼（Password）制定與使用規則給使用者，參考優質通行碼設定原則與使用原則[參考文件編號A-07]，應包含以下各項：1.使用者應對其個人所持有通行碼盡保密責任。2.要求使用者的通行碼設定，避免使用易於猜測之數字或文字，及過多的重複字元等	□□□□□	□□□□□	
條款章節	依據條文		自評 A B C D E	稽核評分 A B C D E	稽核發現與說明
2.8.3	多帳號通行碼	因特殊需要擁有多個帳號時，可考慮使用一組複雜但相同的通行碼。	□□□□□	□□□□□	
2.8.4	通行碼設置	處理個人資料檔案之資訊設備，需設置使用者代碼及通行碼。	□□□□□	□□□□□	
2.8.5	通行碼變更	通行碼至少每六個月更換一次，通行碼長度應至少，且包含英文數字	□□□□□	□□□□□	

稽核實務與施行(續)

你可以這麼做
從資訊系統管理人員開始，進行優質密碼設定。
密碼設定，應設8碼以上，以英數字、大小寫、特殊符號組成。
設定密碼變更週期設定(如每半年變更一次)。
稽核抽查時，確認密碼設定已符合程序要求。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
	內外之通報	學校應建立資訊安全事件通報程序[參考文件編號A-08]以及安全事件通報單；資安事件應即刻進行通報，通報程序應包括學校內部通報，以及通報本縣教育網路中心	□ □ □ □ □	□ □ □ □ □	

你可以這麼做

發生資安事件時，應依資訊安全事件通報程序進行。

資訊管理人員應透過教育部提供之資安事件通報平台進行通報。

進行資安事件處理。

於稽核時提供資安事件處理之紀錄，確認資安事件已被有效控管。

稽核實務與施行(續)

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
3.1.5	儲存媒體管控	儲存個人資料檔案之相關儲存媒體，應指定專人管理，並置於實體保護之環境（如上鎖之防潮箱、書櫃），必要時應建立備援機制，以防止資料損壞、遺失或遭竊取相關儲存媒體非經權責單位同意並留存紀錄[參考文件編號A-09]，不得任意攜出或拷貝複製。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

你可以這麼做

存有敏感性資訊之儲存媒體，應有專人管理。

儲存媒體若需備份或複製時，應填寫儲存媒體管控記錄單，有效控管儲存媒體之使用。

於稽核時提供儲存媒體管控記錄單，確認儲存媒體已被有效控管。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
3.6.1	攜出授權與登記	當有必要將設備或授權軟體攜出，應檢視相關授權，並實施登記與歸還記錄[參考文件編號A-10]。	□ □ □ □ □	□ □ □ □ □	

你可以這麼做
資訊設備攜出、攜入時，應填寫資訊設備移出記錄表。
稽核時提供資訊設備移出記錄表之紀錄，確認資訊設備攜出、攜入時，已被有效控管。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
5.1.1	適用法規之宣導	蒐集相關法律條文(智慧財產權、個人資料保護法、個人資料保護法施行細則、資料隱私保護及其他相關法規[參考文件編號A-11]、了解與資訊處理設施、軟體系統的關係，並予以書面或公開場合做宣導。	□ □ □ □ □	□ □ □ □ □	

你可以這麼做

應識別符合單位之資訊安全相關法規列表。

確認資訊安全相關法令、法規，保持於最新版本(如：法令法規名稱之正確性)

稽核時，提供資訊安全相關法規列表之紀錄，確認已正確識別出資訊安全相關法規。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
2.2	對抗惡意軟體、隱密通道及特洛依木馬程式				
2.2.1	防毒軟體更新	學校內的個人電腦應：裝置防毒軟體，將軟體設定為自動定期更新病毒碼；或由伺服器端進行病毒碼更新的管理，並應每週執行排程掃瞄定期（至少每個月）進行系統程式更新作業，以防範作業系統及應用程式之漏洞。	□ □ □ □ □	□ □ □ □ □	

你可以這麼做

個人電腦應安裝有版權之防毒軟體。

防毒軟體應朝向中央控管方式。

應於防毒伺服器上設定排程，定期掃描與病毒碼更新。

稽核時，開啟防毒伺服器，確認相關設定，已符合資安管理要求。

稽核實務與施行(續)

條款章節	依據條文		自評					稽核評分					稽核發現與說明
			A	B	C	D	E	A	B	C	D	E	
2.2.4	弱點掃描	各相關網站每年至少進行一次網站弱點監測平台掃描，並完成弱點修補。	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

你可以這麼做

透過教育機構弱點監測掃描平台進行弱點監測。

高風險之弱點應進行修補。

完成修補後，應進行弱點複測，確認弱點以正確修補。

稽核時，提供弱點掃描監測報告，確認已符合資安管理要求。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
2.3	備份作業之控管				
2.3.2	異機備份	資料檔如有異動，至少每月異機備份。	□□□□□	□□□□□	

你可以這麼做

進行重要系統備份工作。

定義備份週期(如：每週完整備份、每日差異備份)。

將備份結果進行紀錄(如：系統、紙本)。

稽核時，提供備份結果，確認已符合資安管理要求。

稽核實務與施行(續)

條款章節		依據條文	自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
3	實體安全				
3.1	設備安置及保護				
3.1.1	實體環境安全	學校重要的資訊設備（如主機機房）應置於設有空調空間或通風良好之空間。學校資訊設備主機機房、電腦教室區域，應設置滅火設備，並禁止擺放易燃物、或飲食	□□□□□	□□□□□	

你可以這麼做

重要資訊設備應存放於機房。

機房內應有滅火器(如：滅火系統、手持式滅火器)。

機房內應禁止堆放雜物、易燃物、食物等。

稽核時，以實地訪查方式，確認已符合資安管理要求。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
3	實體安全				
3.1	設備安置及保護				
3.1.3	設備安置地點之保護措施	學校資訊設備主機機房、電腦教室區域內的電源線插頭應有接地的連結、或有避雷針、穩壓器、不斷電等裝置避免如雷擊事件所造成之損害情況。	□□□□□	□□□□□	

你可以這麼做

機房內應有不斷電系統，保護資訊設備。

機房內之不斷電系統，應注意負載狀態，避免負載過高。

稽核時，以實地訪查方式，確認已符合資安管理要求。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
3.3	纜線安全				
3.3.1	佈纜的安全	學校資訊設備主機機房、電腦教室區域內地板上應盡可能避免佈明線。	□ □ □ □ □	□ □ □ □ □	

你可以這麼做
機房內之佈纜應朝向電源與通訊線路分離。
機房內之纜線應整束與標示。
稽核時，以實地訪查方式，確認已符合資安管理要求。

稽核實務與施行(續)

條款章節	依據條文		自評	稽核評分	稽核發現與說明
			A B C D E	A B C D E	
3.7	桌面淨空與螢幕淨空政策				
3.7.1	桌面淨空安全管理	應考量採用辦公桌面的淨空政策，以減少具有機密或敏感特性的資料及儲存媒體等在正常的辦公時間之外遭未被授權的人員取用、遺失、竄改或是被破壞的機會。	□ □ □ □ □	□ □ □ □ □	
3.7.2	電腦保護裝置	學校提供教職員工或學生使用的個人電腦應設定保護裝置，如個人鑰匙、個人密碼以及螢幕保護，並將螢幕保護啟動時間設定為 15 分鐘以內。	□ □ □ □ □	□ □ □ □ □	

稽核實務與施行(續)

4	人員安全				
4.1	資訊安全職責				
條款章節	依據條文		自評 A B C D E	稽核評分 A B C D E	稽核發現與說明
4.1.1	加強宣導	於學校重要會議上宣導相關資安知識，以強化工作上之資訊安全意識。	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	

稽核實務與施行(續)

你可以這麼做

應請同仁於離開辦公室時，將敏感性資料存放於儲存櫃中，並上鎖。

個人電腦應設定螢幕保護程式，於一定時間之內，自動進入螢幕保護程式(如：15分鐘)。

透過學校重要會議上宣導，請同仁養成操作電腦之良好習慣予資安意識宣導。

稽核時，以實地訪查方式，確認已符合資安管理要求。抽查教育訓練紀錄，確認已進行資安相關教育訓練。

稽核實務與施行(續)

稽核實務與施行Q&A

- 國中小資通安全稽核標準規範與實行作法
- 網站弱點檢測修補
- 殭屍病毒防治
- 國中小資通安全稽核重點與技巧
- 結語

結語

- 資訊安全是不間斷的工作，應落實執行。
- 時時提高警覺，有效降低資安事件發生。
- 每個同仁皆應遵守組織資訊安全規定。

資訊安全
人人有責