CHAPTER 3

資訊安全與保護

資訊安全是維護電腦系統，使其正常運作的管理程序或安全防護技術。維護資訊安全不僅是企業及政府資訊部門的重要工作，也是每個電腦使用者所應重視的事項。

影響資訊安全的因素有很多，常見的有「天災與人為疏失的問題」、「散播惡意軟體的問題」、「駭客入侵的問題」等，本章將逐一說明，並介紹其防範措施。

3-1 天災與人為疏失的問題

數年前的「怪颱」納莉颱風造成全台各地大淹水，許多企業機關的電腦設備及資料檔案受到嚴重損害，這就是一個天然災害影響資訊安全的實際案例。以下將介紹影響資訊安全常見的天災、人為因素，及其防範對策。

3-1.1 影響資安的天災及人為因素

影響資訊安全的天災及人為因素有很多，這些因素可歸類為意外災害、人為疏失、軟硬體設備故障等3大類（圖3-1）。

- **意外災害**：風災、水災、火災、地震、雷擊等天然災害，常會造成電腦設備損毀或資料遺失。
- **人為疏失**：人為作業的疏失，可能造成電腦硬體設備的損壞，或資料的遺失。
- **軟硬體設備故障**：軟硬體設備的故障，可能導致電腦系統無法正常運作，或資料毀損。

圖3-1 影響資安的天災及人為因素

檢定這樣考～電腦軟體應用試題

(C)10.下列何者不屬於資訊安全的威脅？ (A)天然災害 (B)人為過失 (C)存取控制 (D)機件故障。 [工作項目04]

(D)40.確保電腦電源穩定的裝置是？ (A)保護設備 (B)網路系統 (C)空調系統 (D)不斷電系統。 [工作項目04]

(C)58.在電腦術語中常用的「UPS」，其主要功能為何？ (A)消除靜電 (B)傳送資料 (C)防止電源中斷 (D)備份資料。 [工作項目04]

3-1.2 天災及人為因素造成資安問題的防範

為了防範以上3種天災及人為因素所造成的資安問題，我們必須規劃對應的措施，以加強資訊安全的防護。

意外災害的防範措施

- 電腦主機避免設置在低窪地區或地下室，以免水災發生時設備損壞。
- 定期檢查防火設備，以便在火警發生時可迅速通報或撲滅。
- 電腦的電源設備應有適當的接地措施，以免電腦因雷擊而損壞。
- 定期備份資料，並存放在不同場所，以便在意外發生時，可將資料回復。

防震不斷電系統 (1:45)

小辭典－不斷電系統

當電腦出現電壓不穩定或電源不正常中斷的情況時，不斷電系統可以正常供電，讓電腦保持正常運作。

人為疏失的防範措施

- 制定電腦系統的管理制度，並由專人負責系統的維修及管理。
- 加強人員對於電腦的操作訓練，使其熟練正確的操作方法，以免因操作錯誤而造成資料遺失或設備損毀。

軟硬體設備故障的防範措施

- 電腦機房應設置空調及除濕設備，以維持電腦系統正常運作。
- 電腦機房應備有穩壓器及**不斷電系統**（**Uninterruptible Power System, UPS**），避免因電壓不穩而損壞電腦設備，或造成資料流失。
- 定期維護硬體設備，延長設備的使用壽命。

節練習

(?) 1. 美國911事件中，許多金融機構中的電腦損毀，但是在短期間內即恢復運作，是因為他們落實了下列哪一項資訊安全措施？　(A)備份資料異地儲存　(B)遠端監視　(C)遠端遙控　(D)遠端安裝。

* (?) 2. 下列資訊安全的防護措施中，何者不適當？　(A)將檔案備份多份，並分地存放　(B)電腦機房設置在地下室，較隱密安全　(C)電腦損壞交給專人維修　(D)加裝穩壓器及不斷電系統（UPS）。2. 若將電腦機房設置在地下室，易因環境潮濕或水災，使得設備損壞

3. 為避免電腦因停電或電壓不穩而當機，應加裝 (?) 設備。

檢定這樣考　電腦軟體應用試題

(B) 7.下列那一種程式具有自行複製繁殖能力，能破壞資料檔案及干擾個人電腦系統的運作？ (A)電腦遊戲 (B)電腦病毒 (C)電腦程式設計 (D)電腦複製程式。 [工作項目04]

(D) 61.所謂的「電腦病毒」其實是一種？ (A)資料 (B)黴菌 (C)毒藥 (D)程式。 [工作項目04]

3-2 散播惡意軟體的問題

我們經常透過電腦來瀏覽網頁、接收信件、下載檔案，你知道這些動作，都可能使你的電腦遭到「惡意軟體」的侵害嗎？爲了保護資料的安全，我們應學會如何防範惡意軟體的入侵。

統測這樣考
(A)16. 下列哪一種病毒，主要會寄生在磁碟的啟動磁區裡？
(A)開機型病毒 (B)檔案型病毒
(C)巨集型病毒 (D)千面人病毒。 [100]
(A)9. 下列何種病毒程式，會依附在副檔名為.EXE、.COM等的可執行檔中？
(A)檔案型 (B)巨集型 (C)隨機型 (D)動畫型。 [99]

3-2.1 認識惡意軟體

惡意軟體（Malicious software, Malware）是泛指會造成電腦系統或網路無法正常運作的軟體，它通常透過各種網路服務及儲存媒體進行傳播，例如檔案下載、電子郵件、即時通訊軟體（如：LINE）、隨身碟……等。**電腦病毒**、**特洛伊木馬程式**、**電腦蠕蟲**等，都屬於惡意軟體。

電腦病毒

「CIH病毒」曾在1998~2004年間造成全球6000萬台電腦癱瘓，損失超過十億美金。這支程式是台灣學生為了證明防毒軟體並非百分之百防毒所設計出，沒想到釀成大禍。這起事件發生後，我國增訂了妨害電腦使用罪。

電腦病毒（virus）是指具有破壞性或惡作劇性質的電腦程式。它多半會隱藏在檔案或磁碟中的特定磁區，藉由自我複製或感染電腦中的其它正常程式，來達到破壞電腦系統的目的，例如早期專門寄生在Office文件中的「巨集型病毒」、專門寄生在執行檔（即副檔名爲COM或EXE）中的「檔案型病毒」、專門寄生在啓動磁區[註]的「開機型病毒」等。

特洛伊木馬程式

十萬手機個資遭竊 (1:42)

特洛伊木馬程式（Trojan horse）是一種「依附」在電腦檔案中的惡意軟體，使用者開啓檔案時，這種軟體就會被啓動（圖3-2）。特洛伊木馬程式通常是以竊取他人私密資料爲目的，大多不會破壞電腦系統，也不會影響電腦的正常運作。

圖3-2 特洛伊木馬程式

註 啓動磁區（boot sector）是指電腦硬碟中的一塊磁區，用來存放開機所需的資料。

統測這樣考 (B)10. 下列何種惡意程式，會耗用掉大量的電腦主記憶體儲存空間或網路頻寬？
(A)電腦搜尋程式　(B)電腦蠕蟲程式
(C)電腦怪蟲程式　(D)電腦編輯程式。　[99]

電腦蠕蟲

電腦蠕蟲（worm）會不斷地大量自我複製，並藉由網際網路的管道來散播，一旦發作，常會造成電腦、網路及郵件伺服器無法正常運作（圖3-3）。

圖3-3　電腦蠕蟲

惡意軟體有很多，有些惡意軟體刻意設計在特定時間或條件下才會發作，這類惡意軟體俗稱爲**邏輯炸彈**（logic bomb）。表3-1是惡意軟體的特性比較。值得注意的是，目前所流行的惡意軟體大多同時結合了電腦病毒、特洛伊木馬程式、電腦蠕蟲的特性，因此感染速度及破壞力越來越強大。

表3-1　惡意軟體比較表

惡意軟體 / 特性比較	電腦病毒	特洛伊木馬程式	電腦蠕蟲
是否會感染其他檔案	✓		
是否需寄生在別的檔案或程式	✓	✓	
主要目的	惡作劇或破壞電腦系統正常運作	入侵他人電腦窺視或竊取資料	耗用電腦資源，使電腦無法正常提供服務

參考案例

「百毒不侵」破功！蘋果金招牌「掉漆」

➕此病毒名為WireLurker，其作者已於2014年底落網。

蘋果公司的作業系統一向給人安全性較高的印象，但2014年，出現一種針對蘋果作業系統的「超級病毒」，只要設備下載了非官方版的App程式，即可能感染病毒，且會將病毒傳染給以USB相連接的設備，造成一傳十、十傳百的效果。目前已有數十萬台蘋果設備染毒，官方呼籲民眾切勿使用未通過審核的程式。

3-2.2 惡意軟體的防範

常言道：「預防勝於治療」，要預防惡意軟體，我們可以從**安裝防毒軟體**及**養成良好的電腦使用習慣**著手。

安裝防毒軟體

主動防毒小技巧 (2:26)

防毒軟體是一種可以偵測與刪除惡意軟體的軟體，它所使用的防毒技術有很多種，目前較常見的是將電腦檔案與防毒軟體公司所蒐集到的**病毒碼**進行比對，以判別檔案是否已遭到惡意軟體感染。

小辭典－病毒碼

病毒碼是從惡意軟體中所擷取出來的一段程式碼。

由於惡意軟體不斷的變種與翻新，因此在安裝防毒軟體之後，還必須定期更新防毒軟體的**病毒碼**，才能有效防範惡意軟體的入侵。表3-2為常見的防毒軟體。

防毒軟體排名(網頁)

表3-2 常見的防毒軟體

防毒軟體	免費中文版	下載網址
Avira AntiVir（小紅傘）	✓	http://www.avira.com/zh-tw/
avast!	✓	http://www.avast.com/
AVGAnti-Virus	✓	http://www.avgtaiwan.com/
Norton（諾頓）	30天試用	http://tw.norton.com/
PC-cillin	30天試用	http://www.pccillin.com.tw/
Kaspersky（卡巴斯基）	30天試用	http://www.kaspersky.com.tw/

請注意！一台電腦不宜安裝多套防毒軟體，否則可能會因為軟體相互衝突，導致電腦或軟體無法正常運作。

http://www.kaspersky.com/virusscanner 卡巴斯基線上掃毒
http://housecall.trendmicro.com/apac/ 趨勢科技線上掃毒

養成良好的電腦使用習慣

要防範惡意軟體的入侵，除了可以安裝防毒軟體之外，還必須養成良好的電腦使用習慣，才能減少電腦感染惡意軟體的機會。

- **開啟軟體自動更新**：作業系統或應用軟體的開發廠商常會不定期提供軟體更新的資訊，以修補程式的錯誤或漏洞；下載並安裝這些修補程式，可防止惡意軟體入侵。
- **不使用來路不明的軟體**：來路不明的軟體（如網路流傳的盜版軟體）可能含有惡意軟體。如果要下載軟體，應到軟體的官方網站或有公信力的網站下載。
- **不任意開啟來源不明的檔案**：網路上流傳的檔案可能含有惡意軟體，我們應避免開啟來源不明的檔案。
- **避免瀏覽高危險群的網站**：色情網站及提供非法資源的網站（如盜版音樂交流網站）經常藏有惡意軟體，我們應避免瀏覽這類高危險群的網站。
- **定期備份資料**：定期將資料備份在DVD、外接式硬碟、隨身碟等儲存媒體中，一旦電腦不幸遭惡意軟體入侵，有助於重新找回遭破壞的資料。

參考案例

簡訊也有毒！「快遞通知」讓你帳單多千元

2014年，一位曾先生收到知名宅急便公司的「包裹簽收電子憑證」簡訊，他點按簡訊中的連結後，沒多久竟收到多封小額付款成功的簡訊，總額近4,000元，這才驚覺被詐騙。警方表示，近來簡訊詐騙層出不窮，民眾千萬不可點按不明連結，以免被騙。

3-2.3 電腦感染惡意軟體的徵兆與補救

電腦若感染了惡意軟體，通常會出現一些不尋常的徵兆。以下介紹電腦感染惡意軟體常見的徵兆及補救措施。

電腦感染惡意軟體的徵兆

電腦感染惡意軟體後，可能會出現以下的症狀：

- 電腦執行速度變慢、程式無法正常執行。
- 網路連線速度變慢，或無故斷線。
- 無法存取磁碟、光碟機、資料夾或檔案。
- 瀏覽器的首頁被惡意軟體鎖定爲某個網頁，且無法變更（俗稱爲首頁綁架），或不時自動開啓廣告視窗。

如何移除被綁架的網頁 (網頁)

- 電腦經常無故當機，或重新啓動。
- 螢幕顯示奇怪訊息。
- 可用硬碟空間無故變小。
- 檔案大小或修改時間無故改變。

值得注意的是，現今的惡意軟體通常不以破壞電腦系統爲目的，因此不一定會出現明顯的症狀。比較保險的做法是，定期利用防毒軟體掃毒，以檢查電腦是否遭到感染。

電腦感染惡意軟體的補救

如果電腦不幸遭到病毒、蠕蟲、特洛伊木馬等惡意軟體的感染，可參照下列步驟來進行補救處理：

1. 使用防毒軟體進行電腦硬碟掃毒及解毒的工作。
2. 若防毒軟體無法解毒，應立刻關閉感染病毒的電腦，避免病毒感染其它檔案或造成更大的損害。若感染的病毒是透過網路傳播，應先拔除網路線，暫時阻斷電腦與外界的連結。
3. 利用未受到病毒感染的電腦，上網查詢病毒相關資訊，並下載解毒程式。
4. 重新開啓感染病毒的電腦，開機時按 F8 鍵，以安全模式[註]進入Windows作業系統。
5. 使用解毒程式進行解毒的工作。

若進行以上所述的補救處理之後，電腦仍無法回復正常運作，便需請專業人員來協助處理。

節練習

(?) 1. 網路中流傳的「遊戲自動練功程式」經常含有惡意軟體；這種軟體會伺機竊取玩家的帳號密碼，但不會影響電腦的正常運作。請問上述惡意軟體最可能是屬於下列哪一種類型？ (A)特洛伊木馬程式 (B)巨集病毒 (C)電腦蠕蟲 (D)USB病毒。

(?) 2. 電腦病毒通常會透過下列哪些管道來傳播？①電子郵件 ②即時通訊軟體 ③螢幕 ④隨身碟 (A)①②③ (B)①②④ (C)①②③④ (D)②③。

3. 請問下列哪些作法有助於防範電腦病毒的入侵？（請勾選）

(?) (1) 經常清理磁碟
(?) (2) 不瀏覽色情網站
(?) (3) 安裝防毒軟體，並定期更新病毒碼
(?) (4) 購買最新機型的電腦
(?) (5) 不定期更換密碼
(?) (6) 不任意開啓電子郵件的附加檔案

註 有關「安全模式」的使用時機及進入方法，可參考微軟網站的說明（http://windows.microsoft.com/zh-TW/windows7/what-is-safe-mode）。

3-3 駭客入侵的問題

智慧汽車也會被駭 (2:01)

「駭客」是什麼人？他們可不是電影「駭客任務」中的人物，而是現實世界中的電腦犯罪者。根據美國FBI估計[註]，全球每年因駭客攻擊所造成的損失，高達數千億美金；更令人憂心的是，駭客的犯罪率正逐年上升。以下將介紹駭客常用的攻擊手法，以及防範駭客入侵的措施。

3-3.1 駭客攻擊的手法

⊕智慧家電也可能被入侵，曾經有駭客讓智慧馬桶不斷沖水。

駭客（hacker）一詞原來是指**熱衷鑽研電腦或網路破解技術的人士**，並不一定有惡意破壞他人電腦的意圖。但因現今報章雜誌、電影等都習慣以「駭客」代表電腦犯罪者，因此與蓄意破壞或犯罪的**怪客**（cracker）已有混用的情形。

駭客通常具有相當豐富的電腦知識，犯罪者動機很多，如挾怨報復、爲了獲取不法利益，或是爲了證明自己的功力等。以下介紹幾種駭客常用的攻擊手法：

- **散布惡意程式**：製作並散布惡意軟體（如特洛伊木馬程式），以炫耀自己的電腦能力，或竊取他人的私密資料，以獲取不法的利益。
- **入侵網站**：透過網際網路入侵他人網站，竊取資料或篡改網站的內容。
- **網路釣魚**（Phishing）：駭客建立與合法網站極爲相似的網頁畫面，誘騙使用者在網站中輸入自己的帳號、密碼、信用卡卡號，以取得使用者的私密資料。

美國中情局主管也被騙 (1:32)

小辭典-社交工程

是指利用社交手段（如套關係）來降低他人戒心、博取信任，再趁機騙取機密資料的手法，網路釣魚即是社交工程的一種。

參考案例

facebook 送 LINE 貼圖？是釣魚啦！

2014年又有新詐騙！如果收到朋友用LINE傳訊告知：「FB送LINE貼圖，登入即可領取」，千萬不要上當！一旦點開訊息中的連結，並在假的FB登入畫面輸入帳密，你的帳號即會遭到詐騙集團惡用。警方呼籲，現在有許多利用貪小便宜心態的網路釣魚詐騙，民眾務必提高警覺。

⊕**勒索軟體**（Ransomware）：駭客利用引人注意的標題郵件，誘騙使用者點開郵件，進而入侵電腦，將受害者電腦中的所有檔案加密，並威脅受害者於期限內交付贖金才解密，否則電腦中的所有檔案將全數被刪除。

註 資料來源：商業周刊930期。

補充資料：

●惡意程式防不勝防，Melissa、I LOVE YOU、Sasser等惡名昭彰的病毒，就是這些重大病毒要犯撰寫出來的

● 手機遭駭案例（http://www.youtube.com/watch?v=T0BqYgFYnQw）

- **網頁掛馬攻擊**：是指駭客在網頁中植入惡意軟體，使用者只要連上這些網頁，電腦就可能感染惡意軟體。

參考案例 Yahoo！奇摩被「掛馬」，一點就中招

2014年，Yahoo！奇摩首頁的廣告被植入惡意軟體，瀏覽者只要點擊廣告，電腦就可能感染病毒，造成約上萬台電腦「中箭落馬」。Yahoo公司表示已刪除暗藏病毒的廣告，並加強資訊安全保護，以避免類似事件再發生。

惡意軟體防不勝防，同學應養成安裝防毒軟體並定期更新病毒碼的良好習慣，以保護自己的電腦。

- **字典攻擊法**：駭客蒐集常用來作爲密碼的字串，做成「字典」檔，再利用程式依序地從「字典」檔中讀取這些字串，並透過一一嘗試的破解方式來找出正確的密碼。取得密碼後，駭客會進行不法行爲，例如竊取個人資料、冒用身分……等。許多網站要求登入帳號密碼時，還需輸入如圖3-4所示的圖形驗證碼，即是爲了防範字典攻擊法。

圖3-4 圖形驗證碼

- **鍵盤側錄**：駭客在使用者電腦中植入「鍵盤側錄程式」，記錄使用者所輸入的帳號、密碼，再利用竊得的帳號密碼來進行不法行爲。因此部分網站爲了防止這類鍵盤側錄程式，會使用「螢幕虛擬鍵盤」，讓使用者以滑鼠點按的方式來輸入密碼（圖3-5）。

圖3-5 螢幕虛擬鍵盤

- **阻斷服務（Denial of Service, DoS）攻擊**：藉由不斷地發送大量訊息，使被攻擊的網站癱瘓，而無法提供服務（圖3-6）。

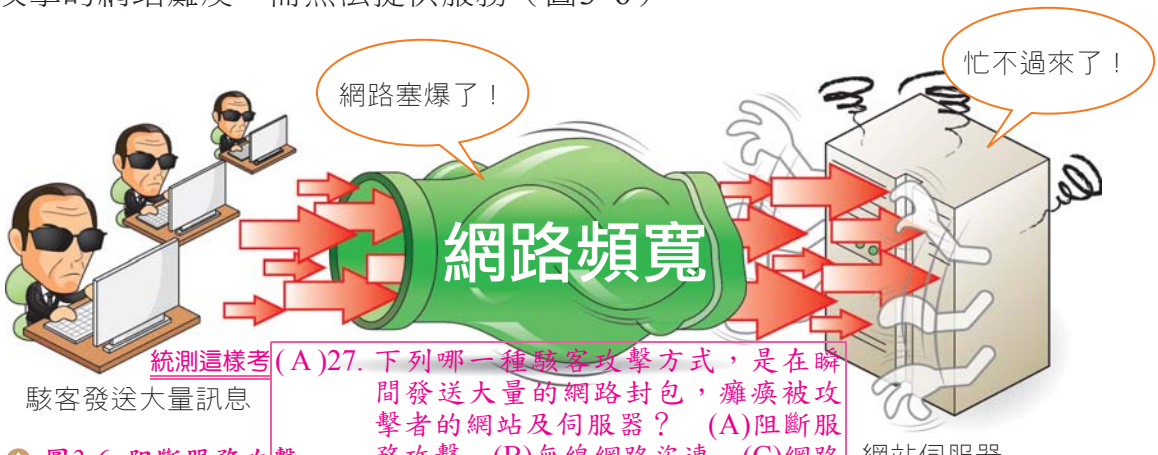


圖3-6 阻斷服務攻擊

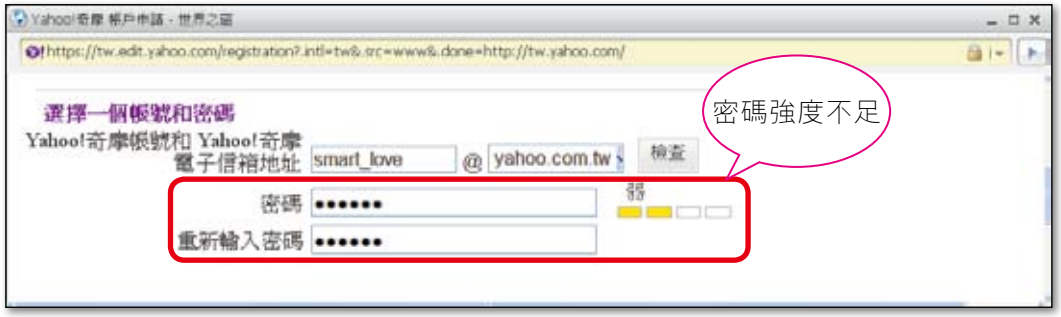
統測這樣考 (A)27. 下列哪一種駭客攻擊方式，是在瞬間發送大量的網路封包，癱瘓被攻擊者的網站及伺服器？ (A)阻斷服務攻擊 (B)無線網路盜連 (C)網路釣魚 (D)電腦蠕蟲攻擊。 [104]

補充資料：

密碼強度檢測

有些人怕忘記密碼，會使用如 "1111"、"1234"、"abc123"、"password"……等簡單好記的「懶人密碼」，但這種密碼很容易被別人猜到，或是被駭客用字典攻擊法破解並盜用。

爲了提醒網友不使用懶人密碼，有些網站會設計「密碼強度檢測」機制，當使用者輸入密碼時，即會自動檢測並顯示密碼強度，若密碼強度不夠，最好更換密碼，直到密碼的強度符合「強度」爲止。



(https://tw.edit.yahoo.com/)

密碼強度檢測機制

參考案例「監視攝影機也淪為駭客DoS攻擊工具」
駭客不僅會入侵他人電腦、手機，當作DoS攻擊的犯案媒介，就連監視攝影機也遭殃。資安業者發現有駭客遠端操控由900台監視攝影機系統所組成的殭屍網路，來攻擊雲端服務，影響全球數百萬名用戶的權益。
專家提醒，只要是有連網的3C產品，都應設定密碼，以免成為駭客為惡的工具。

BotNet攻擊：駭客透過網路散布具有遠端遙控功能的惡意軟體，電腦遭到感染後，就會成爲駭客手下的**殭屍電腦**。駭客常集結大量的殭屍電腦，來構成**殭屍網路**（BotNet），以進行濫發垃圾郵件、竊取他人個人資料等不法行爲（圖3-7）。

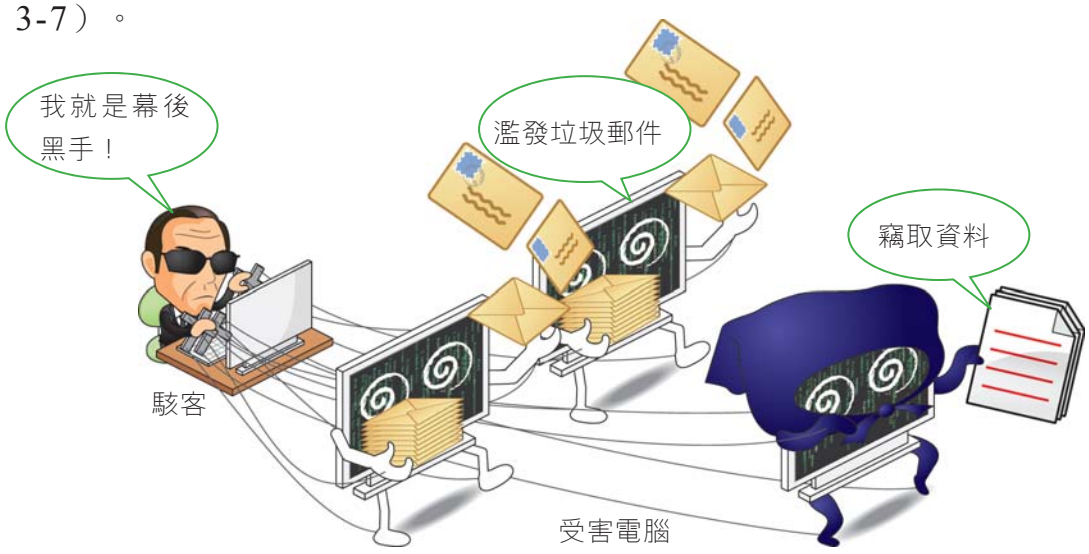


圖3-7 BotNet攻擊

參考案例 10萬殭屍電腦，攻擊網路公投系統

2014年香港民衆爲爭取普選權，由民間發起全民公投活動，但期間內，公投網站卻遭到來自駭客的DoS攻擊，在攻擊高峰期，一度有10萬台殭屍電腦同時攻擊公投系統。

警方提醒民衆平日應做好防毒防駭的工作，以免成爲駭客發動阻斷服務攻擊的幫凶。

零時差攻擊：利用軟體本身的安全漏洞進行竊取資料、植入病毒等不法行爲。因爲這種手法通常是駭客在發現軟體的安全漏洞後，立即發動攻擊，所以又被稱爲「零時差攻擊」（Zero-day Attack）。

參考案例 微軟軟體屢遭零時差攻擊，警報響不停

微軟公司的軟體使用者衆多，因此常成爲駭客的攻擊目標。2014年，接連爆出Windows、Office、IE等多項產品的設計有漏洞，遭到駭客以零時差攻擊，迫使微軟公司緊急發布修補程式。

資安專家呼籲民衆應配合廠商的訊息即時更新軟體，以免成爲「受害者」。

課外閱讀

間諜軟體

間諜軟體（spyware）通常被設計成一個有用的小程式（如產生密碼的程式），但卻會在暗地裡竊取使用者的個人資料（如帳號、密碼），或是做出讓使用者困擾的動作，例如不斷彈出廣告視窗、更換瀏覽器首頁……等。

爲了保護個人的隱私資料，我們應養成不安裝來路不明軟體的習慣。此外，我們也可安裝專業的反間諜軟體程式，如Spyware Doctor（圖3-8），來避免電腦遭到間諜軟體的入侵。

圖3-8 Spyware Doctor

統測這樣考 （B）43. 在網路系統中，當企業內部網路（Intranet）與網際網路（Internet）相連時，其架構上最主要用來防止駭客入侵的設備為何？
(A)閘道器 (B)防火牆
(C)集線器 (D)防毒軟體。 [101]

3-3.2 駭客入侵的防範措施

你知道一台沒有防護的電腦，在駭客眼中就像一頭肥羊嗎？如果同學以爲自己的電腦不會被駭客「看上」，那可就太過樂觀了。要防範駭客的入侵，我們可以從**安裝防火牆**及**養成良好的電腦使用習慣**等方面來著手。

安裝防火牆

防火牆（firewall）是一種可以用來過濾資料來源，以維護內部網路安全的軟體或硬體設備；它的運作原理[註]類似於在使用者的電腦與網際網路之間建立一道防衛的城牆，讓駭客無法直接存取使用者電腦中的資料（圖3-9）。

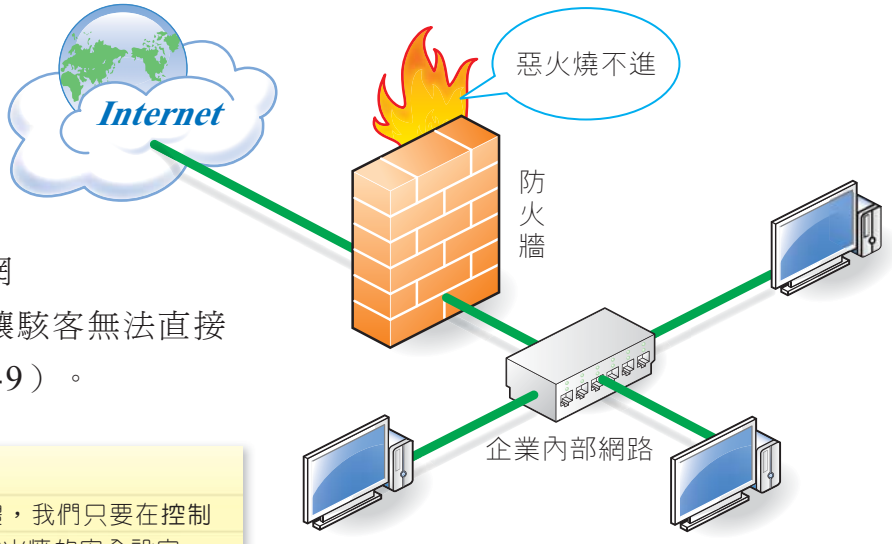


圖3-9 防火牆的運作示意圖

Tip
Windows作業系統即內建有防火牆軟體，我們只要在控制台中雙按Windows防火牆，即可進行防火牆的安全設定。

註 有關防火牆的運作原理，在本書第II冊-「計算機概論II」第3章將會詳細介紹。

檢定這樣考　電腦軟體應用試題

(B)112.過濾、監視網路上的封包與通聯狀況，達到保護電腦的軟體為何？ (A)防毒軟體 (B)防火牆 (C)瀏覽器 (D)即時通。 [工作項目04]

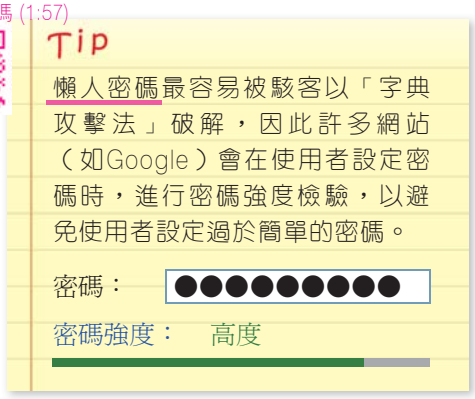
統測這樣考 (B)23. 使用者瀏覽網站時，網站在使用者電腦儲存使用者瀏覽相關資訊的檔案稱之為？
(A)blog　(B)cookie　(C)intranet　(D)ssl。[101]

養成良好的電腦使用習慣

爲避免駭客入侵，除了安裝防火牆之外，還須養成下列良好的電腦使用習慣：

- 配合軟體公司所發佈的更新訊息，下載並安裝修補程式。
- 有些網站爲了提供更多元的服務，會自動儲存一份記錄使用者所登入的帳號、瀏覽記錄等資料的檔案在使用者電腦中，這種檔案稱爲**cookie**。在瀏覽網站後，我們可刪除cookie檔案，以保護自己的隱私。
- 遵照以下原則，設定及管理密碼。
  - 密碼至少8個字元以上。
  - 密碼宜混合使用英文大小寫、數字、符號，避免使用例如 "1111"、"1234"、"abc123"、"password"……等簡單好記的**懶人密碼**。
  - 避免使用個人相關的資料（如生日）作爲密碼。
  - 不定期更換密碼，且勿隨意透露自己的密碼。

如何設定好密碼 (1:57)



- 爲避免駭客入侵竊取硬碟中的資料，機密資料最好儲存在隨身碟或光碟中。
- 公用電腦容易遭受電腦病毒感染，我們應避免使用公用電腦進行線上交易，以免私密資料外洩。
- 若需要在網站中登入帳號、密碼等私密資料，應確認網址是否正確，例如政府網站的網址類別應爲gov，教育單位應爲edu，公司行號應爲com，以避免落入網路釣魚的陷阱。
- 若有郵件、手機簡訊、LINE或Facebook訊息要求你登入某個網站，可能是網路釣魚的手法，請勿直接點按訊息中的連結來登入網站，建議同學自己輸入正確網址，或利用值得信賴的搜尋引擎（如Google）來連結至該網站。

http://www.takka.com.hk/jstutor/ch17/ch17.htm　瀏覽cookie檔案的內容

做了就會 1 刪除cookie與帳號密碼記錄

使用公用電腦後，爲了避免帳號密碼遭到有心人士盜用，應刪除cookie與帳號密碼記錄。

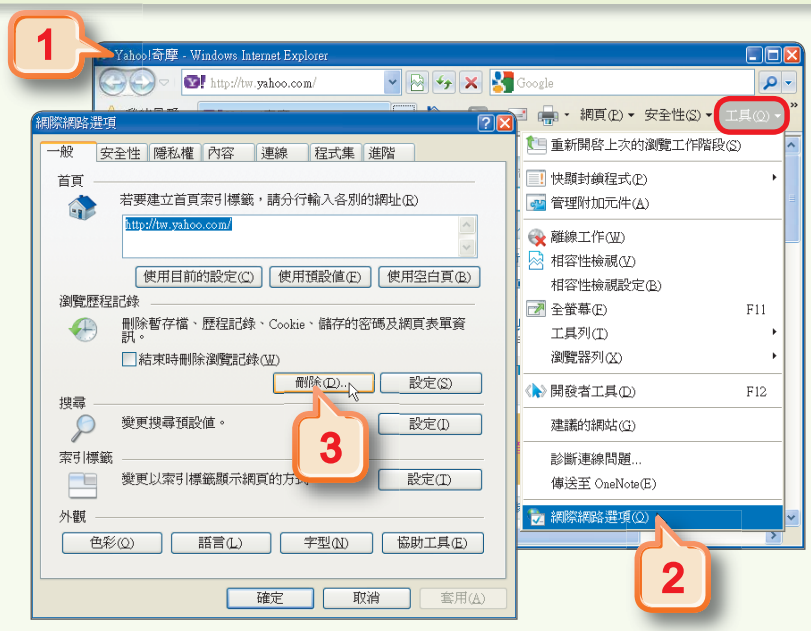
詳細步驟參考

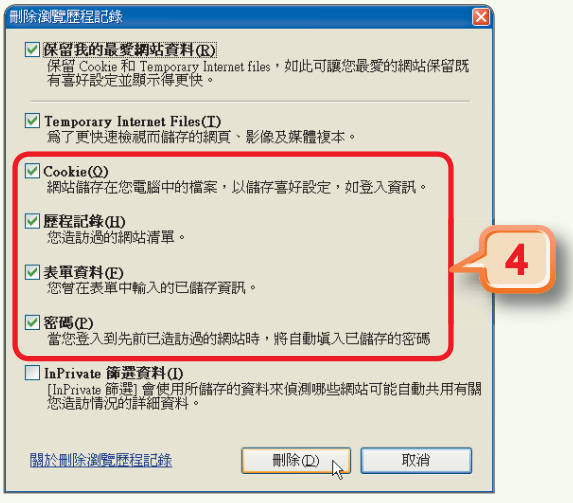
1. 開啓IE瀏覽器

2. 選按『工具/網際網路選項』，開啓網際網路選項交談窗

3. 按刪除鈕，以開啓刪除瀏覽歷程記錄交談窗

4. 勾選Cookie、歷程記錄、表單資料、密碼核取方塊，並按刪除鈕，待回至網際網路選項交談窗，再按確定鈕，關閉交談窗





節練習

1. (　?　) 所謂的「駭客」是指？ (A)奇裝異服的電腦從業人員 (B)電腦犯罪者 (C)網拍賣家 (D)線上遊戲玩家。

2. (　?　) 下列哪些是常見的駭客攻擊手法？①入侵他人網站 ②零時差攻擊 ③阻斷服務攻擊 (A)①② (B)①③ (C)②③ (D)①②③。

3. (　?　) 可用來過濾資料來源，以維護內部網路的安全，達到防範駭客入侵的效果。

本章習題

選擇題

3-1 1. 電力公司的電纜故障造成無預警停電，導致公司內部許多同仁，來不及將電腦中的作業存檔，而遺失資料，請問這是屬於下列哪一種影響資訊安全的因素？ (A)蓄意破壞 (B)意外災害 (C)人為疏失 (D)駭客入侵。

2. 為避免因電力公司突然電力中斷，造成電腦硬體的損壞以及未儲存檔案資料的流失，我們可以使用何種裝置？ (A)全球定位系統（GPS） (B)突波保護器 (C)不斷電系統（UPS） (D)充電器。

3-2 3. 阿德覺得電腦變慢了，他關閉所有程式後，CPU的使用率仍居高不下（如95%），請問這種情形最可能的原因為何？ (A)電腦感染了惡意軟體 (B)電腦螢幕快壞了 (C)電壓不足 (D)硬碟空間不足。

* 4. 電腦病毒的傳播途徑不包含下列何者？ (A)電子郵件 (B)唯讀記憶體（ROM） (C)隨身碟 (D)即時通訊軟體。4. ROM是一種只能讀取而不能寫入資料的記憶體，除非在製作ROM時就寫入含有電腦病毒的資料，否則此種記憶體不會是電腦病毒傳播的途徑

5. 如果電子郵件中含有附加檔案，下列哪一種類型的檔案最好不要隨意開啟，以免感染電腦病毒？ (A).bmp (B).txt (C).mid (D).exe。

6. 下列何者不是電腦病毒的特性？ (A)具有自我複製的能力 (B)具特殊之破壞技術 (C)關機再重新開機後會自動消失 (D)會常駐在主記憶體中。 乙

* 7. 下列敘述，何者不正確？ (A)使用防毒軟體，仍需經常更新病毒碼 (B)不可隨意開啟不明來源電子郵件附加檔案 (C)重要資料燒錄於光碟儲存，可避免受病毒感染及破壞 (D)重要資料備份於硬碟不同檔案夾內，可確保資料安全。7. 應將重要資料備份在不同儲存媒體中，如外接式硬碟、隨身碟、DVD等，才能避免資料遺失 統

* 8. 下列有關電腦病毒的敘述及處理，何者正確？ (A)將電腦電源關閉，即可消滅電腦病毒 (B)由於Word文件不是可執行檔，因此不會感染電腦病毒 (C)購買及安裝最新的防毒軟體，即可確保電腦不會中毒 (D)上網瀏覽網頁有可能會感染電腦病毒。 統

8. 文件檔也會感染電腦病毒；安裝防毒軟體後，必須定期更新病毒碼，才能有效防範電腦病毒

9. 下列何者不是預防電腦病毒的基本做法？ (A)將重要的資料隨時備份 (B)不開啟任何來路不明的電子郵件 (C)登入系統之密碼應不定期更換 (D)使用具有合法版權之軟體。 統

10. 下列哪一種做法與電腦病毒的防治最沒有關係？ (A)使用合法軟體 (B)定期備份資料 (C)定期作磁碟重組 (D)安裝防毒軟體。

3-3 * 11. 大雄要申請一個Facebook帳號，請問從安全的角度來看，使用下列哪一個密碼最恰當？ (A)1234 (B)aabbccdd (C)nobida_14d5l (D)password。11. 密碼應避免使用簡單好記的懶人密碼

12. 手機公司Hti的網址為http://www.Hti.com/，小明收到一封促銷新手機的電子郵件，郵件內的超連結是連結到相似但並不相同的網址http://www.Htl.com/，讓小明誤信這網址就是該手機公司Hti的網址，因而被誘騙在該網址的網頁填入個人身分及信用卡等資料。請問以上情境是哪一種網路攻擊手法？ (A)阻斷服務攻擊 (B)網路釣魚攻擊 (C)電腦蠕蟲攻擊 (D)網頁木馬攻擊。 統

13. 使用者瀏覽網站時，網站在使用者電腦儲存使用者瀏覽相關資訊的檔案稱之為？ (A)blog (B)cookie (C)intranet (D)ssl。 統

14. 曾有駭客要求遊戲網站刊登不法廣告不成，就挾怨報復，不斷對遊戲網站發送大量訊息，導致網站癱瘓無法運作。請問這種手法稱為 (A)網路釣魚 (B)阻斷服務攻擊 (C)設定程式炸彈 (D)植入特洛伊木馬。

本章習題

( ) 15. Facebook交友網站在全球已累積高達2億多的會員人數，許多駭客曾利用郵件寄發假網址誘使會員登入，並竊取這些會員的帳號、密碼等個人資料，請問這種犯罪手法稱之爲 (A)資料攔截 (B)電腦蠕蟲 (C)網路釣魚 (D)特洛伊木馬。

( ) 16. 下列何者爲架設防火牆的主要用途？ (A)防止駭客入侵電腦系統 (B)將重要檔案進行加密，避免他人窺視 (C)具有穩壓功能，避免硬體損壞 (D)避免電腦中毒。

( ) 17. 下列哪一項做法，最不可能防範駭客的入侵？ (A)定期備份 (B)定期修補程式漏洞 (C)妥善管理自己的帳號密碼 (D)安裝防火牆軟體。

( ) 18. 網際網路的應用普及之後，個人的網路行爲常有被窺探之虞。請問下列哪一種做法，可以有效避免上述的問題？ (A)定期進行磁碟重組 (B)上網後自行刪除cookie (C)定期進行資料備份 (D)定期進行磁碟清理。

( ) 19. 「網頁掛馬」是一種駭客的攻擊手法，駭客在正常的網頁中植入惡意軟體，使用者只要瀏覽網頁，電腦即可能感染病毒。請問我們可以透過下列哪種方法來防範這類攻擊？ (A)安裝防毒軟體 (B)使用外接式硬碟 (C)時常進行磁碟重組 (D)設定帳戶密碼。

* ( ) 20. 下列有關資訊安全的敘述，何者正確？ (A)Malware是一套免費的防毒軟體 (B)具有大量自我複製與散播特質的惡意軟體，稱爲特洛伊木馬程式 (C)駭客篡改網站首頁，稱爲「網路釣魚」 (D)懶人密碼易被駭客以「字典攻擊法」破解。

20.Malware是指惡意軟體；具有複製與散播特質的惡意軟體，稱為電腦蠕蟲；網路釣魚是指駭客建立與合法網站極為相似的網頁畫面，誘騙使用者在網站中輸入自己的帳號、密碼、信用卡卡號，以取得使用者的私密資料

多元練習題

1. 請連上『線上安全』網（http://aoema.azurewebsites.net/home.htm），點選「二分鐘測驗」超連結，進行安全等級測驗，以了解自己的電腦是否有足夠的安全防範措施，來防止駭客的入侵及電腦病毒的感染。

2. 請在下列資訊安全專有名詞前，填入正確的英文代號。

a. DoS　b. logic bomb　c. worm　d. Malware　e. virus
f. hacker　g. phishing　h. firewall　i. Trojan horse

( ) 網路釣魚　( ) 電腦病毒　( ) 電腦蠕蟲
( ) 惡意軟體　( ) 駭客　( ) 特洛伊木馬程式
( ) 阻斷服務　( ) 防火牆　( ) 邏輯炸彈