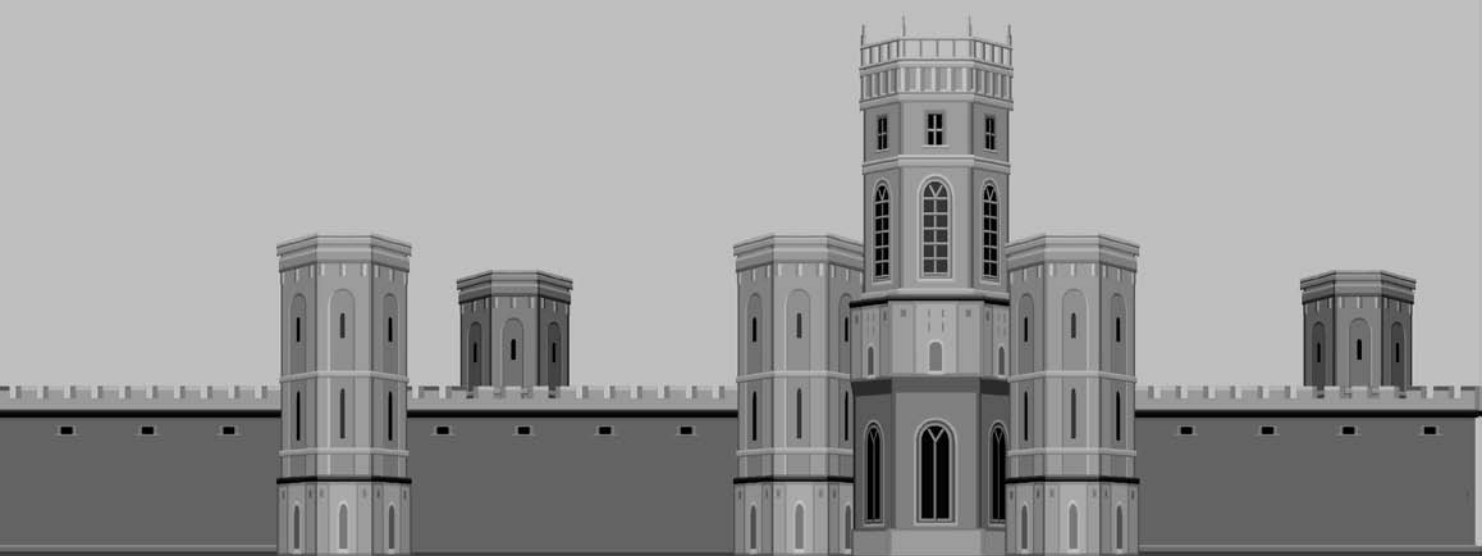
CHAPTER 01

資訊安全概論

本章概要



這一章的目的在協助讀者建立正確的資訊安全概念，同時希望藉由對存取控制與網路安全這兩項核心議題的討論，讓大家認知到資訊安全需要「技術」與「管理」兩個層面的充分配合。本章內容涵蓋很廣，但多為概論性說明，會在往後章節再做比較深入的討論。

1.1 資訊安全問題的演進

隨著人們對資訊科技的依賴與日俱增，歹徒有更大的動機利用資訊進行破壞，而這種破壞對每個人的工作與生活就產生更大的衝擊。因此，資訊安全問題隨著資訊科技的不斷創新而越趨複雜。

資訊科技是個新領域，從 1960 年代電腦才開始市場化，直到 1980 年代初期，電腦還在比較封閉的環境中由少數人操作，安全風險不高。在大型電腦主機（mainframe）的時代，資訊安全事件大多是人為操作錯誤所造成的資料遺失，或是內部人員操守問題所造成的洩密。

隨著個人電腦從 1980 年代逐漸普及化，影響眾人的資訊安全事件開始浮現。早期個人電腦的設計並未考慮存取控制（access control），因此無法保護資訊的保密性與完整性。除此之外，交換使用軟碟（floppy disks）讓電腦病毒（computer viruses）開始出現。Elk Cloner 被視為最早的電腦病毒，在 1982 年由一位十五歲的美國學生 Rich Skrenta 寫在 Apple II 電腦上。感染媒介是軟碟，使用受感染的軟碟開機五十次，螢幕上就會出現一首打油詩。

網際網路（Internet）在 1990 年代以驚人的速度成長，由於大家的電腦都連結在一起，使病毒散播與駭客攻擊更加方便有效。Melissa 是 1999 年由電子郵件傳播的 Word 巨集（macro）病毒，它利用受感染電腦的電子郵件通訊錄，再發出五十封病毒郵件，因此數小時內就可以傳遍全球。另外，像 Code Red 蠕蟲（worm）利用當時作業系統的瑕疵，在 2001 年七月十九日一天內感染全球 359,000 台電腦。該蠕蟲的攻擊速度與範圍皆駭人聽聞。

較早的電腦或網路破壞者大多以炫耀技術或惡作劇為主，但在電子商務蓬勃發展的二十一世紀，他們的目的已逐漸轉變為獲取非法利益。例如，有位十九歲

的俄國駭客在 1999 年侵入 CD Universe 公司的網路，盜取三十萬筆信用卡資料。在勒索十萬美元贖金未遂後，就報復性地將其中數千筆資料公布在網際網路上。2000 年九月，全球首屈一指的金融服務機構 Western Union 關閉網站五天，因為它遭到駭客入侵並盜走一萬五千筆信用卡資料。經追查，駭客是利用系統維修時沒有防火牆的十五分鐘空檔入侵。一個較新的案例是美國花旗銀行在 7-11 便利店的自動提款機 PIN 碼被竊賊破解，2007 年十月後的半年間至少 200 萬美元被盜領。據調查，由於銀行新安裝的系統允許透過網際網路的維修方式，一向受慎密保護的 PIN 碼資料，疑似就是操作人員未按照正常加密規定動作，在傳輸過程中洩漏。

近年情況頗為失控的木馬程式、間諜軟體、釣魚網站、垃圾郵件等，大多以商業利益為攻擊目的。它們也許不像蠕蟲那麼轟動地登上新聞頭版頭條，但卻造成更大的整體經濟損失，也更難使用單一技術來防禦它們。

1.2 推動資訊安全應有的觀念

大家都知道資訊安全很重要，但有些似是而非的說法常造成資訊安全推動的困難。最常聽到的是：「推動資訊安全會增加工作負擔，並影響組織的正常作業。」因此，企業主或資訊管理人員常存僥倖之心，以為資訊安全事件不會那麼巧地發生在自己身上，因此降低它的優先順位，等到事件發生就後悔莫及了。其次，許多人誤以為資訊安全問題可以「一次」解決，只要建立起完美無缺的防禦體系，就可以高枕無憂。事實並非如此，今天安全的東西可能明天就被破解了，資訊安全是永不停止的攻防過程。另一個常聽到的謬誤是認為資訊安全單靠產品，只要有功能強大的防火牆（firewall）與防毒軟體（anti-virus）就夠了。事實上，單靠產品的效果有限，必須結合相關人員的資訊安全認知與訓練。

資訊安全是一種取捨

推動資訊安全需要投入人力、物力，同時可能犧牲部分人的方便、自由、甚至工作效率，所以主其事者應該採取比較務實的做法來化解組織的反彈與阻力。

天下沒有絕對完美的防禦，因此資訊安全是一種「取捨（tradeoff）」。應在有限的條件下，將資源投資在最容易受到攻擊或是對組織衝擊最大的安全弱點上。例如，一家五位員工的小企業可能最該做的是為每台電腦安裝防毒軟體，而不是花幾千萬元建構一個安全營運中心（Security Operation Center, SOC）。

另外，防禦措施需要在「安全」與「便利」之間做合理的取捨。過度防禦會造成使用者的不便，反而違背資訊科技帶給人便利的初衷。有一家企業安裝了安全性極高的門禁管制系統，員工進出任何門都需要刷卡並輸入 PIN 碼。公司追求高安全性的立意甚佳，但由於操作不方便，員工乾脆不關門，反而形成始料未及的安全漏洞。

資訊安全是管理議題

許多人以為資訊安全是個「技術」議題，但事實上它是一個需要技術輔助的「管理」議題。2004 年 Wells Fargo 銀行員工的筆記型電腦在公司外遭竊，最敏感的客戶交易紀錄及二十萬筆信用卡資料洩漏，造成公司嚴重的財務與形象損失。若要防止這一類的資訊安全事件，技術固然重要，例如筆記型電腦應該設定很強的登入密碼，同時重要資料必須加密。但更重要的是管理，例如員工是否確實地執行加密要求？是否有必要將這麼多機密資料存放在可以攜出的筆記型電腦？一旦筆記型電腦遭竊，是否有一套標準作業流程來處理這種緊急狀況，以降低客戶與組織的損失？

如圖 1-1 所示，完整的資訊安全應該同時建設三個 P：它們是「人員（people）」、「程序（process）」、與「產品（product）」。我們可以用一句話來整合三者的關係：**人員都遵守資訊安全程序，產品才能發揮功效**。延續前面的例子：公司規定筆記型電腦要設定很強的登入密碼，同時重要資料必須加密，這就是一種程序規範。公司必須對員工進行宣導與獎懲，使所有員工都正確地執行這個程序。唯有如此，公司所購買的作業系統、加解密產品、甚至單點登錄（single sign-on）系統才能發揮保護資訊的功效。

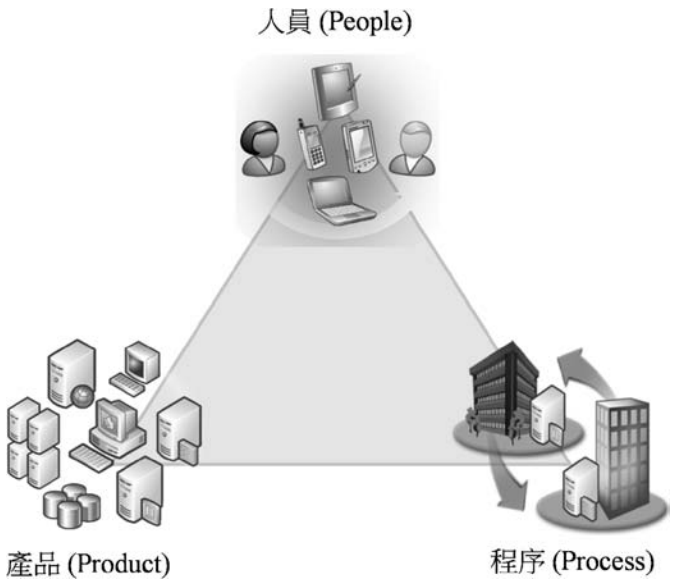


圖 1-1　資訊安全的三個 P

有一家公司購買並安裝了很強的登錄系統，並且規定所有員工必須設定至少八個字元的通關密碼（password），同時密碼必須每月更換，而且相同密碼在一年之內不得重複使用。員工雖然都照做了，但有些人因為記不得經常更換的密碼，就把它寫成小紙條貼在螢幕上。這家公司有安全的產品，也訂定了安全的操作程序，但因為人員欠缺資訊安全意識而功虧一簣。可見三個 P，缺一不可。

1.3 資訊安全的範圍與目標

如果有人為了防小偷在家門上裝了十道鎖，但卻不關窗戶，是不是很荒謬？相同的，維護資訊安全也要顧及全面性。如果有一個領域的防禦不佳，其它領域做得再多也是枉然，因為資訊安全事件會發生在最脆弱的環節。

甚具公信力的「資訊系統安全專家認證（Certified Information Systems Security Professionals, CISSP）」涵蓋以下十個領域：

- 資訊安全與風險管理（Information Security and Risk Management）
- 存取控制（Access Control）

- 應用程式安全（Application Security）
- 密碼學（Cryptography）
- 通訊與網路安全（Telecommunications and Network Security）
- 實體安全（Physical Security）
- 營運安全（Operations Security）
- 安全架構與設計（Security Architecture and Design）
- 業務持續與災害復原計畫（Business Continuity and Disaster Recovery Planning）
- 法律、規章、遵循性與調查（Law, Regulations, Compliance, and Investigations）

這些領域的內容留待以後章節討論，在這裡單從十個領域的名稱就可以看出資訊安全的範圍極廣，包括數學、科技、管理、法律等各個層面。

資訊安全的三元素

我們也可以從資訊安全的三元素（security triad）來討論它的範圍，這三元素是「實體安全（physical security）」，「營運安全（operational security）」，以及「管理與政策（management and policies）」。

實體安全保護你的資產與資訊，讓未經授權的人無法做實體接觸。所保護的是看得見、摸得著、並能被偷的東西。維護實體安全有以下三個重點：

- 讓你所保護的實體位置不要成為受攻擊的目標。
- 即時地偵測到侵入或竊盜的發生。
- 當被盜取或損失重要資訊或系統後，能夠快速復原。

研究資訊安全的人常因為資訊沒有實體，而忽略了實體安全的重要性。事實上，無形的資訊仍然需要有形的載具，例如伺服器、磁碟機、電纜線等，如果惡意攻擊者能夠接觸到這些載具，他們就有更高的機會竊取或破壞其上的資訊。

營運安全在確保組織能經常地正確運作，尤其應注意以下工作重點：

- 電腦、網路及有線與無線通訊系統的運作。
- 資訊與檔案管理。
- 存取控制、身分認證及網路的安全結構設計。
- 經常性的網路維運、與其它網路的連結、備份計畫與復原計畫等。

營運安全是大多數資訊安全人員的主要工作範圍，也佔據了本書最多的篇幅，然而大家不可以忽略它和另外兩個元素之間的依存性。

一個組織的資訊安全管理政策直接領導了它的管理方向，若要發揮作用，需要組織高層的絕對支持。訂定資訊安全政策時應該考慮以下項目：

- **行政管理政策**（administrative policies）：為系統及網路管理員制定標準作業流程，如升級、監控、備份及稽核等。
- **軟體設計要求**（software design requirements）：制定組織採購、外包、或自行開發軟體之相關安全要求。
- **災害復原計畫**（disaster recovery plans, DRP）
- **資訊政策**（information policies）：包括資訊存取、機密等級、標示、儲存、以及機密資訊的傳遞與銷毀。
- **安全政策**（security policies）
- **使用政策**（usage policies）：說明資訊與資源該如何被使用，應包括隱私權、所有人制度，與不當行為之處分。
- **使用者管理政策**（user management policies）：員工在受雇期間的資訊安全相關管理制度，包括新人訓練、存取權限的設定與取消等。

資訊安全的目標

組織或個人推動資訊安全所要達到的目標（goals）有三項：一是預防（prevention），事先預防比事後處理容易，不論是人員訓練、程序制定、或防火牆之類產品的建置都可以預防電腦或資訊被違規使用。二是偵測（detection），

要能即時地偵測到事件的發生。除了人員的資訊安全警覺性之外，入侵偵測系統（intrusion detection systems, IDS）與防毒軟體等產品也能達到偵測目的。三是反應（response），在平時就要發展策略與技巧來因應遭受的攻擊或造成的損失，並且要廣為宣導、經常演練。而資料備份（backup）與資訊系統冗餘（redundancy）設計也都有助於資訊安全事件發生後的反應與復原。

1.4 基本的存取控制

存取控制（access control）是資訊安全的核心項目之一，它特別重要一方面因為它是大多數資訊系統的入口，將入口顧好，就能解決大半的安全問題。另一方面因為它定義了每位使用者的身分，在見不到實體的資訊與網路時代，電子身分就代表個人，若被冒用，很容易造成名譽與財產的損失。

存取控制決定使用者與系統之間的溝通，防止系統資源或資料被未經授權地存取。存取控制在組織中有以下三種操作模式：

- 強制存取控制（mandatory access control, MAC）是一種比較嚴格卻沒有彈性的存取控制模式，由系統管理員（administrator）統一規定組織中的哪些人能夠存取哪些系統、檔案或資料。
- 任意存取控制（discretionary access control, DAC）是比較有彈性的一種模式，它讓每位系統、檔案或資料的所有人（owner）決定組織內使用者對它們的存取權限。
- 角色基準存取控制（role-based access control, RBAC）是一種 DAC，但它不針對使用者訂定存取權限，而用他在組織中的角色（如職務）。

身分認證的方法

身分認證（authentication）是存取控制裡的重要環節，它讓使用者或要求存取的系統能夠證明自己的身分。認證有以下三種要素（factors）：

- 「所知之事（something you know）」是利用正確的使用者才知道的事情進行認證，例如通關密碼或 PIN。
- 「所持之物（something you have）」是利用正確的使用者才會持有的東西進行認證，例如智慧卡。
- 「所具之形（something you are）」是利用正確使用者本身的生物特徵進行認證，例如指紋或視網膜比對。

以上三者各有優缺點，同時使用多種要素的認證方法（multi-factor authentication）比較安全。例如同時使用智慧卡與通關密碼，可以降低智慧卡失竊或密碼遭窺視等單一事件所造成的傷害。

「所知之事」是最常用的認證方法，大部分作業系統都以「使用者名稱」和「通關密碼」做為登入時的身分證明。一種簡單的方法是以 Password Authentication Protocol（PAP）將使用者名稱與密碼送到伺服器上進行比對，但由於 PAP 傳輸並未加密，這種簡單的認證方法並不安全。

安全代符（security tokens）憑「所持之物」做身分認證。這種隨身攜帶的元件上儲存著比人腦記憶的通關密碼複雜的認證資訊，使身分認證程序更加安全。安全代符的種類很多，較常見的有：

- **一次性密碼代符**（one-time password tokens）：元件上所顯示的數字與遠端伺服器上的數字同步變化，因此在每次登入時都可以驗證代符的真實性。
- **智慧卡**（smart cards）：本身具有運算功能的晶片卡，可以讓元件與系統進行互相認證。
- **記憶卡**（memory cards）：只儲存金鑰而不做複雜運算的晶片卡。
- **無線射頻身分證明**（RFID）：非接觸式晶片卡。

生物特徵（biometrics）藉由使用者「所具之形」做身分認證。主要的方式包括手的比對（指紋、掌紋、手掌尺寸），臉部特徵，視網膜（retina）與虹膜（iris）掃描等。DNA 比對技術若進入實用階段，可以有效降低生物特徵的誤判率。

較先進的身分認證協定

前述 PAP 是一種簡單卻不安全的協定，只在沒有其它選擇的情況下使用。Challenge Handshake Authentication Protocol（CHAP）是一種握手協定（handshake protocol），提供比較好的安全性。CHAP 的運作方法可見圖 1-2，客戶端（client）送一個登入要求（logon request）給伺服器；伺服器回應一個挑戰（challenge）給客戶端，挑戰通常是一串隨機數。客戶端以金鑰（key）將挑戰加密後做成回應（response）送給伺服器，伺服器再以對應的金鑰驗證回應之正確性，來決定是否授權客戶端開始使用伺服器的資源。

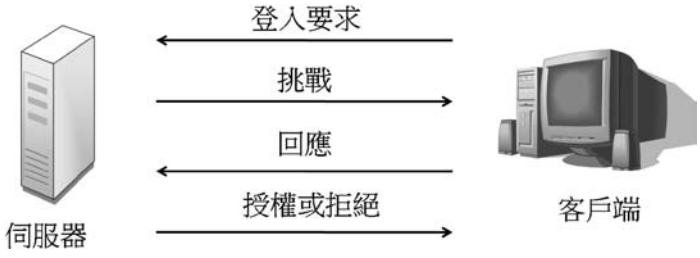


圖 1-2 CHAP 認證方法

憑證（certificates）是另一種常用的身分認證方法。如圖 1-3 的右圖所示，客戶端要使用應用伺服器的資源，它先與安全伺服器完成認證（例如使用 CHAP）之後取得一張憑證，客戶端以憑證就可以存取應用伺服器。憑證可能是一串很長的數字，或一張儲存著很長數字的智慧卡。

圖 1-3 的左圖是 Kerberos，一種常用的單點登錄（single sign-on, SSO）技術。電腦設備（例如客戶端與應用伺服器）之間的對話都以較有效率的對稱式（symmetric）加解密來完成，而密鑰則由密鑰分派中心（key distribution center, KDC）掌控。相較之下，憑證系統因為使用非對稱式（asymmetric）加解密，故較 Kerberos 複雜。以上這些身分認證方法將在以後的章節做更多介紹。

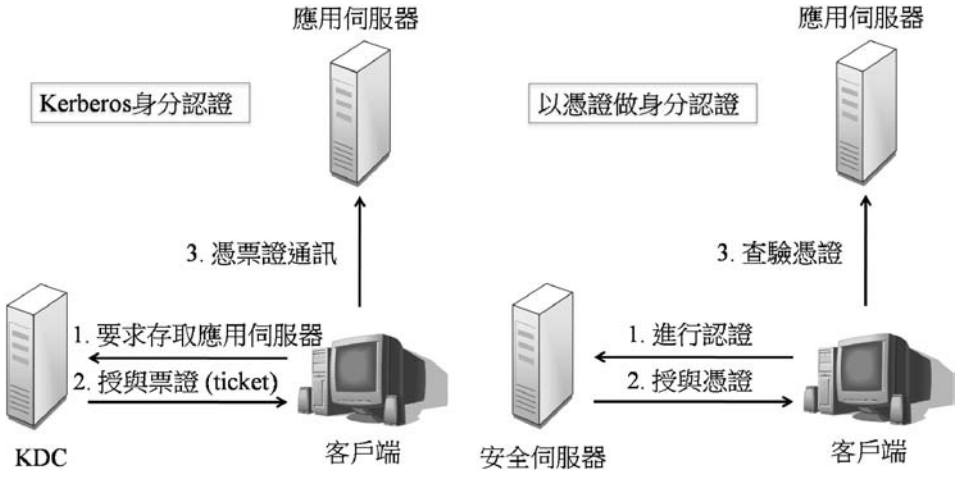


圖 1-3　憑證與 Kerberos 認證方法

1.5 基本的網路安全

我們平常使用的網路是由許多網路服務所組成，以下是常見的例子。各種通訊都有潛在的安全風險，因此網路安全也是資訊安全的一個核心項目。

- Mail：幾乎所有網路使用者都需要電子郵件服務，所以資訊安全計畫必須包括傳送及接收郵件的部分。
- Web：相關的安全考量應包含網頁伺服器（web server）及客戶端的網路瀏覽器（web browser）。
- **即時通訊**（instant messaging, IM）：IM 像是兩者或多者之間的即時電子郵件，它有時會受到下載惡意碼攻擊，許多欺騙行為也藉由 IM 遂行。
- Telnet：Telnet 允許遠端使用者以模擬終端機的方式連上系統，這種舊式的協定沒有安全防護，應該改採用較安全的協定，如 SSH 等。
- File Transfer Protocol (FTP)：FTP 在網際網路常被使用，但經由 FTP 傳輸的資訊沒有加密，登入的通關密碼也多以明碼傳送，應小心使用。
- Domain Name Service (DNS)：DNS 可以將網路位址如 www.abc.net 翻譯為 TCP/IP 位址如 192.168.0.110。

制定安全設計目標

我們為什麼要設計安全的網路？目的當然是要保護組織的利益，降低資訊風險。以下幾項安全組件（security components）可以做為安全設計的目標：

- **保密性**（confidentiality）：保密性的目的在防止未經授權的人或系統存取資料或訊息。法律或規範經常要求特定資訊應予保密，例如身分證字號、員工薪資、個人資料、醫療紀錄等。過去有許多銀行和公司曾因信用卡資料及銀行帳號洩漏，導致重大的金錢及商譽損失。
- **完整性**（integrity）：完整性在於確保被使用的為正確資料，若資料不確實或遭未經授權之人的竄改，例如駭客入侵銀行資料庫竄改存款金額，組織將蒙受巨大損失。
- **可用性**（availability）：可用性在確保資訊服務隨時可用，無法使用資訊等於沒有資訊。如果網路或資料庫不能運作，不論是受攻擊或只是意外，全組織的資訊都無法正常存取，業務也將停擺。
- **責任性**（accountability）：組織內有許多部門與個人，當事件發生時該由誰負責處理必須明確規定。資料或系統的負責人應該在平時對所負責之事、物持續地監看與紀錄。

以下介紹的各種防禦措施都為了保護以上的安全組件；相對的，駭客或其它惡意攻擊者所亟欲破壞的也是這些安全組件。

切割安全區域

網路環境非常複雜，應該將網路切割成安全區域，以便管理區域之間的通訊權限。網際網路（Internet）是最開放的全球公用網路，幾乎所有的區域網路和電腦都經由它彼此連結。內部網路（Intranet）是指公司或組織內的私人網路（private network），或稱為區域網路（local area network, LAN）。開放的網際網路充滿資訊安全威脅，所以必須與區域網路切割，以免私密的資訊遭到破壞。

企業外部網路（Extranet）包含組織的內部網路與外部夥伴組織之間的連結，夥伴可能是供應商或承包商等。它是兩個可以互相信任的組織之間的連線。這種

連線可以用專線或經由網際網路上架設虛擬私有網路（Virtual Private Network, VPN）來完成，如圖 1-4 所示。

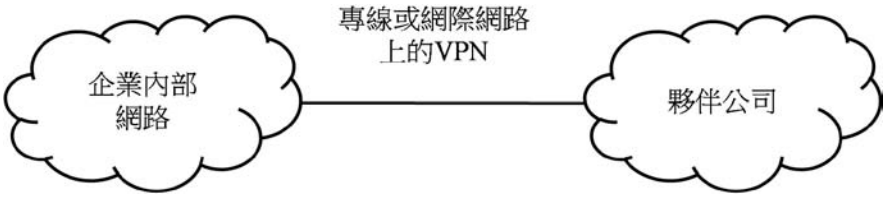


圖 1-4　VPN 示意圖

Demilitarization Zone（DMZ）被譯為非軍事區或安全區，它是指在組織內部放置公開資訊（如網站）的區域。如圖 1-5 所示，防火牆能將網際網路、內部網路與 DMZ 區域分隔開。透過網際網路進入的使用者，只要沒有惡意，都能任意瀏覽網頁伺服器的資訊，但卻不得進入內部網路。

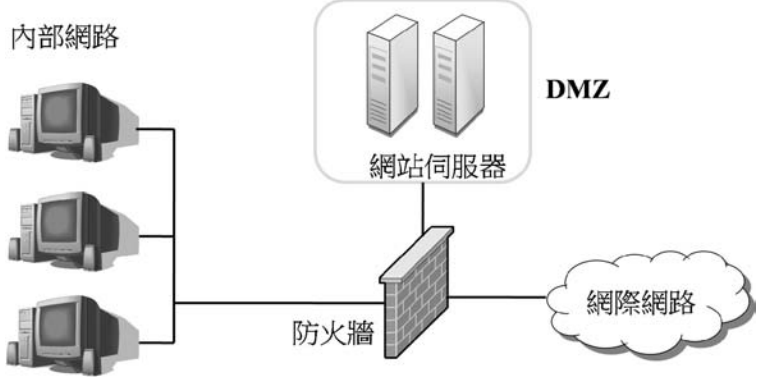


圖 1-5　DMZ 示意圖

融入新科技

近年來網路才逐漸發展為眾人所使用的技術，不容諱言的，像 TCP/IP 這類網路設計並未將網路安全列為重要考量。因此我們應該融入較新的技術，來補強傳統網路的弱點。

企業或機構的組織龐大，內部網路也日趨複雜。如果將組織內的區域網路切割為數段虛擬區域網路（Virtual Local Area Networks, VLAN），如圖 1-6 所示。這種做法可以得到以下好處：

- 可以降低區域網路的廣播（broadcast）流量。
- 可以提高網路效能，並且方便管理。
- 可以降低對網路實體連結的依賴。
- 可以強化資訊安全管理，例如將權限相當的使用者劃分在同一段 VLAN 區域內。

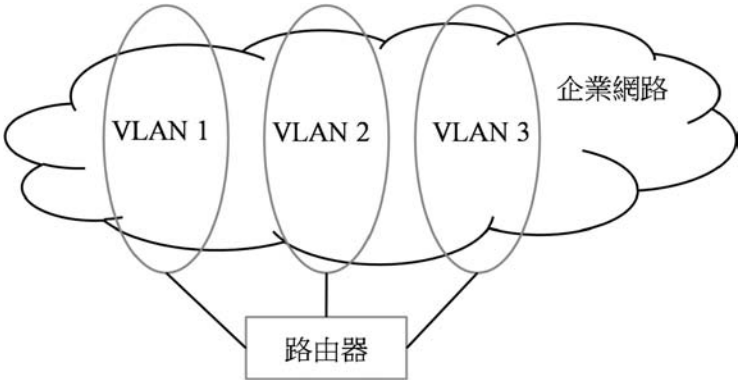


圖 1-6 VLAN 示意圖

電腦在網際網路上通訊時使用 IP 位址，但 IP 位址有被用罄之虞，因此部分 IP 位址被保留給內部網路使用，讓內部的所有電腦在公開網路上共用一個外部 IP 位址。這個技術稱為 Network Address Translation（NAT），如圖 1-7 所示。

內部網路使用的 IP 包括：

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

圖 1-7 NAT 示意圖

NAT 除了提供內、外部網路位址翻譯外，對網路安全也有很大助益。使用 NAT 的組織與外部網路只有一個接點，因此可有效隱藏內部網路不為外部知曉；此外 NAT 伺服器可以監控進出組織的資料，兼具部分的防火牆過濾功能。

安全通道（tunneling）是另一項有用的網路安全技術，它在兩個系統或網路間建立一條虛擬的專屬通道，如圖 1-8 所示。資訊雖然還是在公開網路上傳輸，但通道兩端使用彼此同意的方法來封裝訊息，使中途攔截者無法讀取，這種協定包括 IPSec 和 L2TP 等。而以安全通道協定所建立的網路就是前述的虛擬私有網路（VPN），在不安全的公開網路上建立私有的安全通道。

圖 1-8　安全通道示意圖

管理資訊風險

各種安全的設計與努力，其目的不外乎保護組織的利益，降低資訊風險。資訊安全管理包括以下四個重點：

- **資產識別**（asset identification）：公司或組織將資訊及系統條列出來，並標示其價值。資訊資產的價值若無法純粹以金錢價格標示，可以用權值來表達失去該資產對組織的衝擊。
- **威脅識別**（threat identification）：威脅包括內部威脅，例如內部竊盜、系統失敗、惡意破壞、間諜活動、不遵守資訊安全準則、使用非法軟體等，與外部威脅，包括自然災害如火災與地震，和惡意攻擊如盜賊、駭客、網路病毒等。
- **弱點識別**（vulnerability identification）：資訊弱點可能發生在作業系統、TCP/IP 網路、電子郵件系統等。過去產品供應商經常隱瞞安全弱點，現在則較願意公布弱點，並且快速提供補救，例如微軟公司經常下載安全補丁（security patch）。

- **風險評鑑**（risk assessment）：風險可以被定義為：「威脅」利用「弱點」對「資產」造成「衝擊」的「可能性」。五個項目都可以用量化方式表達，因此企業或組織的資訊風險可以被數字化地計算與考核。藉由修補弱點與控制威脅的成功機率，我們就可以有效地降低資訊風險。

建立多層次防禦

網路環境越來越複雜，每一層環節都可能有弱點，引來內部或外部的威脅。因此需要建立「多層次防禦（layered defense）」。例如，只在個人電腦上安裝防毒軟體不算多層次防禦；應該在每台個人電腦、檔案伺服器、郵件伺服器上都裝防毒軟體，並在代理伺服器（proxy server）上執行內容篩檢，才算多層次防禦。又例如，僅只設定使用者與檔案的存取權限不算多層次防禦；對重要檔案實施多層次防禦至少應該做到：

- 為所有檔案建立較細節的存取控制單（access control list, ACL）。
- 以電腦系統來設定每位使用者對檔案的存取權限。
- 為存放資料的電腦規畫實體安全，避免資訊或系統遭到竊取。
- 建立使用者登入機制，確實認證使用者身分。
- 監控使用者對重要檔案之存取，並留下紀錄。

Open System Interconnection（OSI）網路模型將網路定義為七層，網路的多層次防禦可以沿著 OSI 模型來規劃。以下是一些例子：

- 防火牆要設定封包的篩檢功能，用以保護網路層（Network layer）。
- 在應用層（application layer）使用代理伺服器來保護組織免於未經授權的進入。
- 在網路層使用 NAT，可以隱藏內部網路的 IP 位址。
- 在實體層（physical layer）使用遮蔽式雙絞線（shielded twisted pair, STP）來降低遭受惡意掛線監聽的機會。
- 在網路層使用入侵偵測系統，監看進出網路的資料有無惡意攻擊的跡象。

- ✦ 使用 IPSec 等技術建立 VPN，在網路層防禦資料竄改等惡意攻擊。
- ✦ 在應用層妥善設定網頁伺服器，為公開與敏感的資訊建立不同的網站，以防禦未經授權的存取。
- ✦ 所有裝置都只打開必要的連接埠（port），可降低網路層與傳輸層（transport layer）受攻擊的風險。
- ✦ 在存取機密文件時，在傳輸層使用 Secure Socket Layer（SSL）協定。
- ✦ 在網路層，每週執行網路掃描，以尋找新弱點。

多層次防禦非常複雜，但最重要的第一步就是了解自己的環境，尤其是環境中的弱點，應該使用入侵偵測系統並且定時地進行弱點掃描。軟、硬體升級或者增加新設備造成系統或網路環境變更時，要特別注意是否出現新的弱點。防毒軟體的病毒碼應該按照規定更新並注意各種補丁下載的訊息。

我們未必需要最新或最貴的資訊安全產品；但我們要了解威脅會在哪裡發生，並將那些地方防禦好，這就是多層次防禦的精神。

自我評量

1. 以下哪一種方法以 KDC 對使用者、程式、或系統做身分認證？

A. PAP

B. CHAP

C. Kerberos

D. RFID

2. 以下哪一種存取控制模式是由組織制式規定，而資訊所有人（owner）沒有放寬的空間？

A. MAC

B. DAC

C. RBAC

D. CHAP

3. 為了安全考量，在開放的網路環境中，應該儘量避免使用以下哪一種服務或協定？

A. WWW

B. E-mail

C. NAT

D. Telnet

4. 以下哪一種身分認證方法主要是由伺服器給客戶端一個挑戰（challenge），客戶端做回應（response）送給伺服器？

A. PAP

B. CHAP

C. Kerberos

D. RFID

5. 以下哪一種協定可以讓組織在公開網路上共用一個外部 IP 位址，而在區域網路使用私人 IP？

A. VLAN

B. DMZ

C. VPN

D. NAT

6. 當組織的網路過大，我們將之切為數塊較小的私人網路的方法為何？

A. NAT

B. DMZ

C. VLAN

D. Extranet

7. 以下哪一種身分認證方法使用「something you have」的要素？

A. Smart cards

B. RFID

C. Onetime password token

D. 以上皆是

8. 在兩個系統或網路間建立一條虛擬的專屬通道，使用以下何種技術：

A. Tunneling

B. DMZ

C. NAT

D. VLAN

9. 當外部入侵資訊系統事件發生時，何者最能幫助了解入侵狀況？

A. Anti-virus software

B. Firewall

C. Kerberos

D. System logs

10. 您要為組織安裝一台伺服器，服務網際網路上的客戶。為免內部網路承受風險，應將該伺服器裝置於何處？

A. VLAN

B. Behind a main firewall

C. DMZ

D. Intranet

11. 組織推動資訊安全時，與以下何者會產生「取捨（tradeoff）」的考量？

A. 成本

B. 便利性

C. 系統效能

D. 以上皆是

12. 某公司的安全政策說明：「員工所保管的個人電腦必須依規定更新病毒碼。」請問是屬於資訊安全三個 P 的何者？

A. People

B. Products

C. Process

D. 以上皆是

13. 訂定組織的資訊安全政策（information security policy）是誰的責任？

A. 全體組織同仁

B. 組織的高層

C. 資訊部門經理

D. 品質經理

14. 組織要求重要資料必須備份，是為了資訊安全的哪一個目標？

A. Prevention

B. Detection

C. Response

D. All above

15. 期中考前一天，一位學生侵入老師的電子郵件系統竊取考試題目。請問這種行為破壞了哪一個安全組件？

A. Confidentiality

B. Integrity

C. Availability

D. Accountability