資訊管理

# 網路安全管理與SSL加解密機制技術研究

副教授　吳嘉龍


## 提要

有了網際網路之後，無論是個人、家庭、組織、政府單位在電腦的使用上，都陸續面臨各種網路惡意程式威脅，其中包括了網路詐騙、瀏覽程式漏洞攻擊、網路釣魚程式攻擊、外掛程式、間諜程式入侵、殭屍網路、網路釣魚、身分竊盜、網路病毒感染等。美國《華盛頓時報(Washington Times)》2010年3月18日報導，美國五角大廈遍佈全球的龐大電腦網路，在2008年遭遇一個經由隨身碟進入電腦的惡意程式攻擊，這場電子攻擊促使美國改善網路安全系統。由於Internet的普及和發展，作業系統與軟體上相繼發現的許多安全弱點，使駭客更容易入侵電腦。通過安全聯接層虛擬專網(IPSec VPN)技術實現大量數據的遠程訪問為人們提供了一種低運行成本、高生產效率的遠程訪問方式，SSL VPN技術幫助網路使用者通過標準的Web瀏覽器進行網站資料存取與應用，提高了工作效率也同時解決了全性問題。針對網路安全管理層面分析，當我們開啟瀏覽器上網時所可能面臨的威脅，則除了可能造成網路與電腦本身的破壞之外，最重要的是還可能造成私密的資訊外洩、財物的損失，因此如何落實資訊安全風險管理顯得格外重要與迫切，有鑑於此，本論文針對SSL加解密機制、安全協定與網路安全技術與資安風險管理加以研究探討，以期建立正確資安觀念，並加強落實資訊安全管理與防護作為。

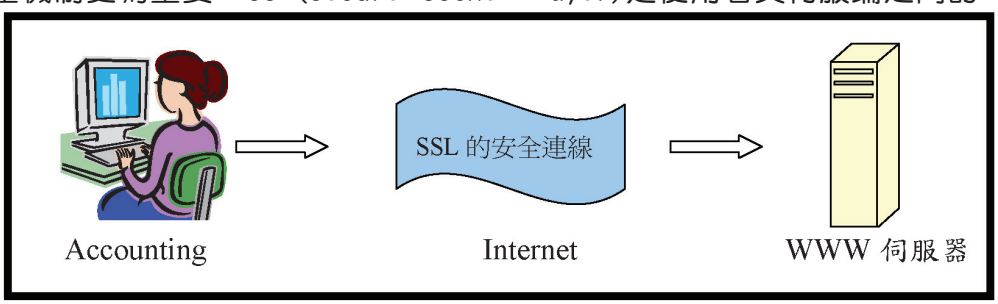

關鍵字：SSL加解密機制技術、資安管理、SSL憑證、網路協定、通訊安全協定

## 壹、前言

隨著電子商務發展、自動化與網際網路的蓬勃發展，整個社會的資訊化程度不斷提高，透過網路進行電子交易的人日趨熱絡，網路電子交易正扮演著與生活緊密不分的重要角色。資訊安全防護已成為國家安全工作首要採取的作為，運用風險管理機制及各種管控手段，落實備援措施、緊急應變及協調回報等管理程序，已是刻不容緩的重要議題。除了建立相關資安及獎懲規範、落實資訊安全制度、實施實體隔離等措施，還需要建立多層防護還有管控的資安防護能量。網路安全不管是在人員上的管理還是在設備上的精進改良都是需要相當的完善的作為，除應加強對資料的加密技術、防火牆控制功能等相關認知，並應了解駭客的惡意程式破壞作法加以防範以確保網路安全[1]。國防部通資次長室資通安全處於去年二月已完成資訊安全政策的修訂及頒布，結合「風險管理」的作為確保資訊安全，使國軍官兵善用先進的資訊通信科技，從服務、管理與使用等三個面向，打造更安全、更有保障的資訊環境。針對資訊安全議題探討，在運用電腦化作業時，要時時警惕對資訊安全的維護，因為資訊安全攸關國家安全，對於相關規定必須確實遵守，並採取風險管理積極作為來加以防範。為提昇部隊訓練成效，發揮國防應有戰力，落實風險管理乃必然趨勢，風險管理不僅是先進國家政府施政趨勢，亦為行政院積極推動的政策之一。而資訊安全風險管理是一套持續改善的反覆過程，建立早期預警機制，落實有效控管，進而降低風險與危機肇生之可能性與衝擊程度，使網路管理者對於資訊安全危安因子能夠早期預警，並採取必要管控措施，有效降低風險肇生和衝擊[2]。

## 貳、SSL加解密機制技術

所謂『網路協定』就是網路中，兩個通訊體之間有關通訊如何進行的協議方式。而在網路通訊時，往往需要安全性的保護，尤其在網路金流日益頻繁之際，這樣的安全機制更為重要。SSL(Secure Socket Layer)是使用者與伺服端之間的一種加




圖一　網際網路中SSL的網路連線示意圖(自行整理)

密通訊協定，主要的設計目標就在於確保網際網路流通的訊息，能在安全無慮的情況下，使得以主從式為架構的應用程式，如瀏覽器及Web伺服器，在不被網路駭客惡意的偽造、竄改的情況下，將訊息完整地送至該目的端，在SSL的安全保護下，將會為通訊雙方，建立起一個專屬安全通道如圖一，雙方均可透過這一安全通道傳送私有的秘密，而不必擔心此一私有秘密為另一第三者所知道[3]。

表一　SSL的演進(自行整理)

| 版本 | SSL演進內容 |
|---|---|
| SSL v1.0 | 這個版本一開始只能在Netscape公司內部使用。 |
| SSL v2.0 | 這個版本對於之前只能在公司內部使用的情況已經有所改善。 |
| SSL v3.0 | 對於安全因素又加以更新，是目前廣為使用的版本。 |

網路保密原則以安全為最優先考量，針對電腦設備與資訊媒體之管制及安全防護，須有更多的管制與規範，SSL加密通訊協定是Secure Socket Layer的英文縮寫，是目前在網際網路中，線上夠物網站最常使用的一種安全協定，這一安全協定的提出，歷史緣由最早是在1994年7月由網景公司(Netscape Communication)所設計研發而成的。SSL是網景公司特為其產品Netscape Navigator所設計出來的資料傳輸標準，此標準可作為在Internet上傳送加密訊息的通訊安全協定，表一是SSL版本的演進[3]。

網路的安全管理是必需的，組織必須先評估現有網路的安全狀況，才能充分了解自身網路的安全防禦能力，並擬定妥善的網路安全政策，配合適當的防護設備、定期的稽核以及持之以恆的系統管理制度配合，才能在利用網路的高效率的同時，也能保護網路及資源不致於被破壞或竊取。微軟公司(Microsoft Corp.)針對SSLv2.0所出現的一些漏洞，做出適當的修正成為PCT協定。一個Internet技術標準組織IETF(Internet Engineer Task Force)，也以SSLv3.0為基礎，設計出TLSv1.0(或SSLv3.1)[3]。IETF(www.ietf.org)將SSL作了標準化，即SSL/TLS(transport layer security)的加密協定-RFC2246，常見的應用是在瀏覽器下方狀態列上鎖的圖示，用來保護當使用連線時不被竊聽[6]。

網路安全在過去一直傾向採取被動式管理的防護策略，被動式防護所使用的設備及工具也是最直接有效的，如防火牆、入侵偵測、虛擬私人網路(Virtual Private Network；VPN)等。在此針對SSL的安全交易協定層主要的組成及其功用加以說明，事實上，IPSec VPN缺點是使用十分複雜，使用時須安裝和維護客戶端軟體[3]。另外，從遠程通過IPSec通道連接到組織內部網絡可能會增加局域網路受


圖二　TCP/IP Layer與SSL Layer之關係(自行整理)

到攻擊或被病毒感染的可能。然而在複合式病毒出現後，被動式的防護策略已顯得防禦力不足。SSL是介於TCP/IP協定和應用程式(如HTTP、FTP、E-Mail)中間的一個層級，如圖二所示。在TCP/IP的協定層級上，主要任務在於負責二台電腦間傳送無錯誤的匿名資料串流(data stream)[4]。

利用軟體漏洞進行攻擊的病毒總是造成大量損失，SSL提供了相關資訊傳輸的安全防護，所以將在資訊傳輸的接口上，以相關密碼技術，完成資料的保密性、認證性、整體性以及不可否認性，這一資料串流將加入許多的額外的資訊及特徵說明如表二[3]。

表二　密碼資訊及特徵(自行整理)

| 方式 | 內容 |
|---|---|
| 密碼學上的加密技術(encryption technology) | 來確保資料保密性(confidentiality)，保障在資料傳輸時的隱密性。 |
| 密碼學上數位簽章(digital signature)技術 | 來達到伺服器端(server)以及客戶端(client)的身份認證(authentication)和不可否認性(non-repudiation)。 |
| 密碼學上的訊息認證碼(message authentication code；MAC) | 運用訊息認證碼來滿足資料的完整特性(integrity)。 |
| 密碼學理論安全性(theoretical security) | 資訊無絕對永久的安全，基於數論(number theory)運算不可行的特性(computation infeasible)以保障資料安全。 |

表三　SSL Layer之組成(自行整理)

| 層級 | 內容 |
|---|---|
| 底層—SSL記錄層(SSL record layer) | SSL的底層為記錄層，其主要功能為接收來自較高層級所傳來未被解釋(un-interpreted)的資料訊息，由於這些資料區塊是以任意長度傳送的，透過記錄層將可對這些資料封包作一處理。 |
| 上層—SSL訊息層(SSL message layer) | SSL協定層中的上層為訊息層，主要是作為訊息傳遞的功用，內容包含了用戶端的相關資訊及一些在作為用戶端和伺服端彼此所傳遞的對話狀態訊息。 |

表四　SSL的通訊協定(自行整理)

| 協定 | 定義 |
|---|---|
| 加密演算轉換協定(Alter cipher spec protocol) | 加密演算轉換協定(cipher spec protocol)是指在密碼的策略中的訊號改變，這協定為所採用密碼演算法定義(cipher spec)下被加密壓縮的單一訊息。當SSL的通訊過程中，用戶端想要以另一種加密演算法取代目前和(伺服端)遠端之前所以協定好的加密演算法，用戶端便可利用此協定來達成其所需的要求。 |
| 警告協定(alert protocol) | SSL的警告協定，主要是來自於在當連線雙方無法取得適度的資訊或是達到彼此互相的協調時，透過SSL記錄層來傳送相關警告的訊息給對方(用戶端或伺服端)，來告知連線雙方在訊息傳送的過程中出了什麼狀況，提供處理的依據。 |
| 交握式協定(handshake protocol) | Record Layer上面操作用來產生連線雙方(用戶端與伺服端)交談狀態下的密碼學參數即是交握式協定，用戶端將根據這些交握過的資料，建立起一個Premaster secret供交談使用。 |

雲端運算資訊科技帶來具備可擴充性、成本效益與彈性的便利性，然而有賴於雲端運算服務安全性、措施與流程，才能確保網路服務的安全。針對網路安全特性，SSLv3.0的通訊協定層大致可分成兩個部份，其上層為訊息層，下層為記錄層如表三，訊息層的資料主要是為相關訊息的集合，而記錄層的工作則是接收此記錄封包，SSLv3.0的通訊協定就是透過此一記錄層來通知連線雙方資料傳輸時彼此必須遵守的規定，此SSLv3.0所

制定的通訊協定有三種，分別為警訊(alert)協定、加密演算法修正協定及交握協定，SSL訊息層內容包括用戶資料、交握式通訊協定資料、警告資料與相關密碼資料[3]。

## 參、SSL的主要協定及交握(Handshake)方式

SSL的通訊協定，簡單的來說，就是用戶端為傳送某些特殊敏感的訊息，透過SSL的記錄層來通知其欲連線的伺服端，彼此在傳輸過程中所應遵守的協定，這些協定含了彼此用來加密的演算法及將採行的網路連線模式[3]，SSL的通訊協定主要可分為三個主要的協定描述如表四，SSL運作原理說明如表五[7]。

SSL VPN技術運用瀏覽器與VPN閘道器建立SSL連線並將資料加密，讓使用者可以透過此SSL通道存取一些受保護的資料。針對最新相關資訊科技發展趨勢分析，盛達電業BILLION針對中小組織推出的多功能安全閘道器發展出BiGuard SSL VPN系列工具，該系列工具將SSL VPN、防火牆及

表五　SSL通訊協定運作原理過程(自行整理)

| 步驟 | 內容 |
|---|---|
| 步驟一 | 用戶端(client)透過HTTPS連到伺服端(server) |
| 步驟二 | Server傳送伺服端Public Key給client |
| 步驟三 | 用戶端產生後續傳輸資料需要用來加密/解密用的Session Key，並以伺服端傳過來的公鑰Public Key加密(encrypted)後回傳給伺服端 |
| 步驟四 | 伺服端用個人私密金鑰Private Key解開用戶端以Public Key加密(encrypted)回傳的資料，以取得Session Key[ |
| 步驟五 | 用戶端與伺服端間傳送資料就以此Session Key來做資料加密與解密的處理 |

表六　交握式的通訊協定過程(自行整理)

| 步驟 | 內容 |
|---|---|
| 步驟一 | Client hello message和server hello message主要為在建立安全通道時所必需要的屬性資料，具有SSL程式的用戶端(client)與伺服端(server)，由用戶端開啟連線接口送出client hello給伺服端，伺服端也將在接到來自用戶端的client hello message後，送出server hello message給用戶端。 |
| 步驟二 | 伺服端被認證(authenticated)成功後，在hello message傳送時，將送出本身的憑證(certificate)資料，以便讓用戶端確認自己的身份，當伺服端沒有任何憑證資料，或是其憑證資料只能用作簽章(signature)使用時，伺服器將會送伺服端金鑰交換(server key exchange)的訊息給用戶端。 |
| 步驟三 | 伺服器端被認證(authenticated)時，用戶端將根據這些交握過的資料，建立起一個Premaster secret供交談使用，並利用伺服器端的公鑰進行加密(encrypted)的動作，而將此加密後的Premaster secret資料送至伺服端。 |
| 步驟四 | 當伺服端作用戶端進行身份確認(identification)時，可傳送certificate request訊息給用戶端使其傳送其本身的憑證資料。如果用戶端本身沒有憑證，伺服端可能基於安全的考量，就此中斷SSL的連線，用戶端也可傳送client key exchange，只是其訊息內容必須根據之前server hello和client hello所選定的公鑰演算法(public-key cryptographic algorithm)。 |
| 步驟五 | 當用戶端確定送出certificate verify訊息後，若用戶端是可以被認證成功的，伺服器將會利用自己的私密金鑰(secret key)對先前用戶端所加密Premaster secret進行解密(decrypted)動作，得到Premaster secret後，經過一連串模算術運算(modular arithmetic)，計算產生Master secret。 |
| 步驟六 | 到此，伺服器和用戶端兩者均可利用其Master secret來進行建立交談金鑰Session Keys，如果認為所選用是有安全的顧慮時，可利用送出change cipher spec訊息，重新選擇加密演算法(encryption algorithm)，並開始使用經過協商過的加密演算法及壓縮方式來進行一連串傳輸資料的加密及壓縮。 |

路由器功能整合於一機，使用一般瀏覽器即可上網，不必購買其他設備便能管理所有連線與遠端存取分享，解決資料遭到竊取的問題，並大幅提高網路效率[9]。目前90%的IPSec VPN應用都可以被SSL VPN來實現，而SSL VPN更加容易配置和管理，實現成本要比IPSec VPN低很多[8]，有鑑於此，包括思科(Cisco)、諾基亞、Cyberoam、Juniper Networks、Array Networks也積極研究發展SSL VPN技術。交握式(handshake)的通訊協定中完成SSL程序的建立，表六是交握式的通訊協定過程敘述[3]，最後用戶端和伺服端將會收到來自對方的finished訊息，如此便完成所有步驟的交握式通訊協定。

## 肆、SSL安全協定特性與優點

SSL安全協定是一種安全技術，提供了加密、驗證及數位簽章等功能，以保護機密資料，因此SSL VPN具有防止資訊洩漏、拒絕非法訪問、保護資訊完整、防止用戶假冒、保證系統的可用性的特點。SSL協定為網路連

表七　基本連線的特性(自行整理)

| 特性 | 內容 |
|---|---|
| 連線隱私性 | 為了達到對資訊的保密，在交握協定時產生交談金鑰，並利用此交談金鑰應用對稱式密碼器對傳輸資訊加密，以確保資料之隱私性。 |
| 身份認證 | 採用點對點之間的身份認證，以非對稱式密碼器之公鑰(含憑證)之認證來確認連線雙方的身分。 |
| 訊息可靠性 | 連線傳送訊息具有可靠性，在訊息的傳送，使用MAC (Message Authentication Code)來確保傳送資訊的完整性。 |

表八　SSL VPN技術的優點(自行整理)

| 優點 | 內容 |
|---|---|
| 密碼的安全性 | SSL加密金鑰能在Client與Server連線時，憑證內的公開金鑰確認身分且資料傳輸的過程都在加密機制中運作，若以信用卡交易就回歸到國際交易的標準機制，而PayPal機制就是建構在第三方付款的概念下，付款閘道安控主機有防木馬程式入侵防火牆與SSL加密金鑰來確保授權資料傳遞的安全，在管理資料庫是採分層檔案加密，個資與卡號資料是分開，駭客即使取得任一部分資料也難以重組。 |
| 相容性的操作 | 伴隨組織資訊化程度的加深，遠程安全訪問、協同工作的需求增加，針對於相互的關連性分析，資訊管理員與程式員可利用SSL 3.0自行研發其他應用程式，此應用程式可避開NAT相容性問題，也將可以成功的交換密碼學的參數(parameter)，而無須任何額外的轉換。 |
| 降低使用成本 | SSL VPN部署成本低廉，在應用性方面，SSL VPN不需要安裝客戶端軟體，目前主流的商業瀏覽器都集成了SSL，實施SSL VPN不需要再安裝額外的軟體。遠程用戶可標準的瀏覽器連接Internet，即可訪問組織的網絡資源，實現遠程安全訪問Web應用。 |
| 具較高穩定性 | 在管理維護和操作性方面，SSL VPN可完成基於應用的控制，SSL VPN還提高了平台的靈活性，方便擴展應用和增強性能，因為IPSec VPN是網絡層連接，SSL VPN連接比IPSec VPN更穩定而不易中斷。 |
| 具有伸展性 | 雲端運算的崛起也將會引領雲端服務的共同協定、網路架構與安全標準，由於資訊安全密碼Security演算法和協定(protocol)都有不可預知的弱點(unpredictable weaknesses)，SSL架構可視環境需求，加入新的演算法(algorithm)，可針對密碼元件研究發展出新的協定。 |
| 相對效率高 | 基於SSL協定無需安裝客戶端軟體，使用一般瀏覽器即可上網，並且能透過SSL VPN網路加密技術遠端存取內部網路，提供了一個可供選擇的快取方案(optional caching scheme)來減少需要被建立的連線數目，減少在網路時的活動上，基於運算複雜度而言，不必重覆對每筆的通訊資料做複雜之模乘法、模指數法等公鑰運算，即可進行安全的通訊，因此相對而言，網路應用的效率增加。 |

線中加解密的動作機制，除了在傳送訊息時，能防止惡意竊聽(eavesdropping)、竄改及偽造(forgery)外，更可因此對於傳送方進行身份的確認[6-8]。加密演算修正協定和交握式通訊協定為連繫雙方訂定連繫的準則規範，警告協定則為這兩個通訊協定，作出雙方反應的訊息轉送；透過上述的三種協定後在雙方(用戶端及伺服端)獲取同步之時，便可以進行應用程式的資料傳輸了[3]。針對於SSL VPN的優點分析，多種認證和授權方式的使用可授權用戶訪問內部網絡，從而保護了組織內部網絡的安全性。因此，SSL協定將能確保網路通訊雙方的隱私(privacy)以及資料傳輸的可靠性(reliability)，SSL的協定基本連線的特性分析如表七[13]。

SSL VPN技術為SSL採用經過嚴格檢核的密碼學協定標準以確保建立安全的雙向通道[3]，SSL VPN基於用戶和組賦予不同的應用訪問權限，並對相關訪問進行審計，SSL VPN技術可對128位數據加密，讓數據在傳輸過程中不被竊取，並可以確保數據傳輸的安全性，**SSL優點整理如表八[4]，SSL VPN技術最新發展趨勢分析為Cyberoam科技公司積極研究虛擬化SSL VPN解決方案[7]。**

## 伍、網路安全技術與資安風險管理

針對惡意程式攻擊網路安全管理技術與資訊風險管理分析，資安工作就是防患於未然的工作，多做一分預防工作，就可以強化一分資安的戰力，軟體的弱點存在於作業系統和應用程式軟體中的錯誤，駭客就經由這些弱點對電腦進行入侵，取得、更改、破壞電腦中的資料或造成當機，而它所造成的損失，常常是無法估算的管理弱點，由於管理上的疏失，因而導致被入侵，如系統設置不當或是帳號密碼過度於簡單而容易猜測組織中有許多的資安事件，都是來自於用戶端電腦的使用不當所導致的，而其中絕大多數發生的原因都與使用者的上網與Email的使用有關，因此資訊安全教育與網路管理都必須確實落實與嚴格把關才可以有效防範，弱點風險管理第一步是瞭解網路環境找到資訊系統特性以及弱點，因為對於資管人員，充分瞭解資訊系統整體弱點存在狀況，才可以正確做好弱點風險管理，表九為資訊系統弱點分佈狀況表[8]。

評估每一個弱點的風險等級，計算整體的風險狀況，運用整體風險狀況瞭解網路弱點各種風險分佈實際狀況，評估如何將風險維持到一定的安全範圍內。找到資安弱點(information security vulnerability)是落實資訊安全根本的問題所在，而且網路安全根本解決之道，就是徹底瞭解網路環境中，找出弱點並進行弱點風險評估。例如，做好管理與修補而當開啟瀏覽器上網時所可能面臨的威脅，則除了可能造成網路系統與電腦本身的破壞之外，最重要的是還可能造成個資等私密資訊的外

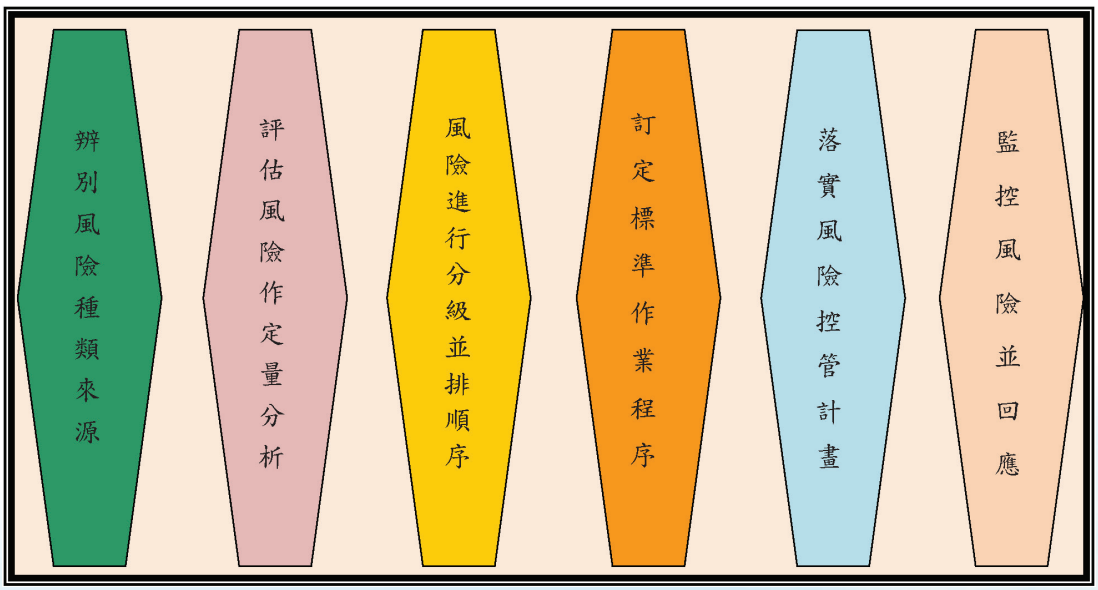
洩、財物的損失[3]。

資訊安全風險管理過程中的資訊安全工作是一項防患於未然的風險管理過程，藉辨識、評估、處理及監測等機制有效管理以降低資訊危安事件發生，多數專案失敗的最大原因，往往因為在執行的過程中，沒有事先預防、做好處理，所以產生失敗及錯誤。解決之道就是要能夠提升專案人員主動的來處理風險的能力，要能夠辨別風險、建置風險管理資料庫與善用使用定性定量分析的工具，風險管理正確的流程說明如圖三。

表九　資訊系統弱點分佈狀況表(自行整理)

| 分部項目 | 弱點分佈狀況 |
|---|---|
| IP位址分佈 | 確實掌握IP位址相關資訊，瞭解系統環境的使用與實際分佈狀況。 |
| 主機作業系統 | 瞭解所屬IP位址的使用人以及網路環境中所使用的作業系統。 |
| 通訊埠 | 瞭解每個主機所開啟的通訊埠數量，開啟的數量越多，風險也越高。 |
| 弱點係數 | 瞭解每個主機中，所存在的弱點數，數量越多，風險也越高。 |
| 風險係數 | 瞭解每個主機整體風險高低，分析哪些主機是整體環境中，存在較高風險，做一個整體的分析與瞭解。 |

國軍基於對資訊安全的重視，因應各層級組織規劃、單位任務需求及環境特性導入的「ISMS資安管理制度」，係依據CNS27001國家標準所制定，行政院研考會已明確指導政府各機關，必須依照標準推行建立相關資安管理制度[11]。資訊風險管理可定義為對資訊安全持續改善的反覆過程，藉辨識、評估、處理及監測等機制，使資訊管理者對於資訊系統各項危安因子能夠早期預警與先期教育訓練，並採取必要管控措施，有效降低資安風險肇生和衝擊。資訊戰首重安全，國軍當前戰略構想考量資訊安全作為應置網路防護為優先，而資安風險是指威脅利用弱點對資產造成




圖三　風險管理的流程(自行整理)

衝擊的可能性，其中包括威脅、弱點、資產、衝擊程度及發生機率等五大風險因子[12]。要因應資安風險首先應確實掌握異動狀態，保持即時且正確的資訊資產相關資料，除建立「風險辨識」、「風險評估」及「風險處理監控」等預防機制，並隨時應變處置的作為，訂定每一個弱點的風險等級，計算整體的風險狀況，期能運用整體風險狀況瞭解網路弱點各種風險分佈實際狀況，評估如何將風險維持到一定的安全範圍內，從資訊服務提供、管理與使用三個面向，建立安全有保障的資訊環境，表十為妥善管理資產重點整理[11]。

表十　妥善管理資產重點(自繪表格)

| 重點項目 | 妥善管理資產內容 |
|---|---|
| 追蹤資產異動狀態 | 從資訊資產清查做起，對資產實施風險評鑑，建立單位資訊安全所應防護管控之對應政策，制定應遵循的規範與原則。 |
| 控管資產生命周期 | 要做好管理資產生命周期，掌握資產的狀態，避免資源閒置，在降低資安風險的作為中，建立單位安全適用的使用環境。 |
| 監控資產設備維運 | 操作電腦需要有制度，因為不正確操作會造成資訊風險，故而需要有完整的資產管理計畫(property management plan)。 |
| 制定災難復原計劃 | 善用服務預維管理與做好問題的統計，充分掌握處理狀態，並將資料作有效保存，妥善完整備份資料和演練復原計畫。 |
| 訂定標準作業程序 | 建立資產預維機制，針對規範文件的製作及管理作為的執行訂出SOP程序，將人為與作業疏失所帶來的危害降到最低。 |
| 預防資產資料外洩 | 禁用等外接式儲存媒體避免因資料外洩所帶來的安全危害，利用遠端控制與資訊管理技術，來降底時間和成本的浪費。 |
| 善用資安防護工具 | 目前工具可分為四大類，分別是周邊控管與資料內容過濾、檔案和磁碟加密、數位版權加密(DRM)與周邊控管四大類型。 |

## 陸、未來因應與心得結論

近年來，資訊便利性與網路科技的蓬勃發展，讓現代生活對網路的應用無所不在，並與網路的關係已密不可分，電子商務帶動出共同存取協定、網路架構與共同遵循標準。然而，在享受方便之餘的我們卻也面臨許多安全的威脅，像是駭客透過各種方式入侵電腦系統，竊取重要的資料，破壞檔案與設備，甚至傳送電腦病毒，透過網頁瀏覽器的弱點，可以快速不費力地入侵至組織的內部網路，因此經由網路擴散，對我們造成極大的傷害等許多因素。針對網路戰爭而言，它是一個沒有砲火的戰爭模式，所以資訊戰也被稱之為「無形的戰爭」，資訊的使用與安全防護同等重要，身為國軍的一份子，應當瞭解「網路即戰場」，要確保立於不敗之地，就必須強化資安作為。國防部正加強推動風險管理政策，要求單位與個人應建立風險辨識確認、風險評估、風險處理監控及風險溝通的觀念。事實上，不管防毒防駭工具如何先進、防火牆再怎麼堅固，絕對無法達到百分之百的安全防護；要做好資安防護應加強資訊設施與資料內容保全與管理，以了解所存在的安全風險與安全需求。

針對如何落實資訊安全危機管理作為，應確實遵守資安政策，一方面積極推動資訊安全風險管理機制，以期將資安風險加以評估與計算，排除資訊危安的因子，改善作業模式，以降低危安因素，另一方面針對資訊風險危安控管工作應落實，恪遵各項安全規定，確依「遵程序」、「按步驟」、「循要領」原則。總而言之，要重視「資訊安全保密工作人人有責」觀念，也唯有建立正確資安危機管理意識，強化網路管理能量，嚴密資訊防護與危機處理作為，才是堅實國防安全穩固的磐石。

## 柒、參考文獻

[1] 顧武雄，Windows用戶端上網安全管理指引，RUN！PC雜誌，193期，58-59頁，2010年02月。
[2] 王明達，國軍新修頒資安政策、落實風險管理，國防部青年日報社軍事新聞網，2010年3月18日。
[3] 賴溪松、葉育斌，資訊安全入門，全華科技圖書股份有限公司，74-83頁，2006年01月。
[4] 魏紜鈴，電子商務刷卡安全嗎？，資安人，68期，60-65頁，2010年03月。
[5] VeriSign認證銷售部亞太區總監Armando Dacal，通往雲端的信任守門機制，網路資訊，223期，65-67頁，2010年06月
[6] Icepeer，SSL工作原理，ChinaITLab，2005年03月22日，http://icepeer.itpub.net/ post/3982/23123，存取日期2010年12月18日
[7] Luckyhoo，認識SSL，2007年09月07日，http://forum.liferec.com/viewtopic.php，存取日期2010年12月18日
[8] NeoEase，SSL VPN技術原理及其應用，2009年6月19日，http://blog.smarthei.com/，存取日期2010年12月18日
[9] Biguard，「MPLS + SSL VPN應用系列研討會」組織逆境求生致勝關鍵，2009年05月08日，http://forum.icst.org.tw/phpbb/viewtopic.php。
[10] Biguard，「遠端存取新主張，安全連線有保障」-盛達電業BILLION推出SSL VPN閘道器促銷方，2009年07月02日，http://forum.icst.org.tw/phpbb/viewtopic.php，存取日期2010年12月18日。
[11] 國防部通資次長室，遵守管理規範 降低資安風險，國防部青年日報社軍事新聞網，2010年11月10日。
[12] 吳建德，專論：落實風險管理 確維部隊戰力，黃一翔記錄整理，國防部青年日報社軍事新聞網，2010年12月22日。
[13] 蔡志展，可疑的中國互聯網絡資訊中心SSL憑證，網管人，51期，117-118頁，2010年04月。

## 作者簡介

空軍中校教授　吳嘉龍

學歷：國防大學中正理工學院48期電機系電子組、美國空軍理工學院電腦工程研究所、國防大學中正理工學院國防科學研究所電子工程組。經歷：電子官，區隊長，教官、講師，助理教授，校教評秘書，科主任，系主任，副教授。現職：航空技術學院一般學科部航空通電系中校教授。