資料安全儲存技術發展之研究

作者/王岳吉 技士

提要

一、隨著儲存技術成熟發展，越來越多的可攜式週邊設備(如隨身碟及燒錄器等)都能夠提供數位檔案儲存能力，且能夠輕易地與現有的電腦系統透過如USB、FireWire(1394)、紅外線等連接埠進行資料存取，對個人而言，這些設備確實提供了方便性，但是對企業而言，卻可能是病毒感染及機密資訊外洩的新管道。

二、根據 2005 年 iThome 電腦報專刊[1]轉載美國 FBI 的調查發現，企業所發生的資料外洩事件中，有 50~80%是從防火牆內部的區域網路流出去的，真正被駭客利用網際網路攻破，進而竊取資料的比例其實相當低，也就是說，企業資訊安全最大的威脅往往是來自於「自己人」。

三、國軍除持續加強資訊安全以防止外部駭客的入侵外，如何防範內部的使用者在有意或無意情況下，透過實體儲存媒體將資料夾帶出去，是刻不容緩的資安議題。

前言

「資料」是當前商業運作的基本要素，而資料運作方式可概分為傳輸中的資料(Data-In-Flight, DIF)及儲存中的資料(Data-At-Rest, DAR)，為保護資料，許多企業所投入資訊安全預算，都是著重於防止外部駭客入侵及以保護傳輸中的資料為主，殊不知這些資安事件很高的比列來自於內部的使用者，且資安風險最大的是儲存中的資料。

援引 2004 年 McData 的調查顯示，有高達 84%~91%的企業用戶，並無任何關於儲存安全的政策，其中有 53%的受訪者表示沒有編列相關預算以進行儲存安全措施，因此，在 iThome 電腦報[2]針對企業資訊安全廣泛調查結果發現，2005 年企業資訊安全十大威脅項目即包括有「員工資安觀念薄弱」、「可攜式設備的管理漏洞」及「身分與重要資料被竊取」等項目，顯示除資訊用戶的人為問題外，端點(End point)安全已成為不可忽視之資安重點，從端點資料之個人儲存設備(如隨身碟及硬碟等)，延伸至區域網路或廣域網路之儲存系統，均存在著資料儲存安全(Storage Security)風險。

隨著 IT 儲存架構由 1980 年代以伺服器主機為中心(Server-centric)、到 1990

年代以網路為中心(Network-centric)，發展至今以資料為中心(Data-centric)，企業在運用資料時，除著眼於資訊生命週期管理(Information Lifecycle Management, ILM)及資料分類管理(Information Classification Management, ICM)外，如何兼顧資料保全(Data Security)與儲存資源管理(Storage Resource Management, SRM)，以共創雙贏局面，應加以審慎評估。

以安全為首重之國軍網路環境，資料運用是戰備整備任務的基本，資料儲存是備援與復原的工具，資料傳輸是 C4ISR 的手段，資料安全是克敵制敵的最高指導原則，唯有掌握及管理所有資料，以達成資訊安全(Information Security)目標。

以下分別就儲存技術與系統發展、儲存安全弱點與威脅、儲存安全策略與實現、儲存安全標準規範、國軍安全部署建議及結論等章節逐一介紹。

儲存技術與系統發展

隨著企業資訊化與電子化的日益普及，企業資源規劃(Enterprise Resource Plan, ERP)、客戶關係管理(Customer Relationship Management, CRM)、電子商務(Electronic Commerce, EC)、知識管理(Knowledge Management, KM)等營運所需的整合應用系統被廣泛建置，其所衍生的資料成為企業營運與發展的核心資產，加上網際網路化與數位多媒體化的快速發展，加快資料容量的增長速度及增加資料倉儲(Data Warehousing)的應用需求，相對地，也造就儲存技術與系統的發展，以下就其發展作一簡介：

一、儲存技術發展

資料儲存需有容器(Container)，一般為硬碟(Hard Driver, HD)，隨著硬碟介面技術逐漸提升，除容量持續增大外，硬碟機的轉速將只維持在每分鐘 7200 轉到 15000 轉之間，尺寸將往 2.5 吋方向發展，而影響其效能的關鍵因素為轉速、單片碟片的容量密度、碟片的直徑大小、單顆硬碟內的碟片數量與磁頭數量及振動等項目。

(一)硬碟介面技術

硬碟傳輸介面類型可分為平行式的，如 SCSI(Small Computer System Interface)和 PATA(Parallel AT Attachment) (Integrated Drive Electronics, IDE 屬 PATA)，另一種是序列式的，如 FC(Fiber Channel)、SATA(Serial ATA)和 SAS(Serial Attached SCSI)，其技術發展，如表一。

表一 硬碟傳輸介面發展(資料來源：本研究整理)

	SCSI	PATA	FC	SATA	SAS
	平行式	平行式	序列式	序列式	序列式
使用對象	伺服器	個人	伺服器	個人	企業
介面傳輸速度	160MB/s 320MB/s	100MB/s 133MB/s	1Gbps 2Gbps 4Gbps	1.5Gbps 3.0Gbps	3.0Gbps 6.0Gbps
轉速(RPM)	10,000 15,000	5,400 7,200	10,000 15,000	7,200 10,000	10,000 15,000
容量	36GB 73GB 147GB	250GB 320GB 400GB	36GB 73GB 147GB 300GB *450GB*	250GB 300GB 400GB 500GB *640GB* *750GB* *1TB* *1.5TB*	*73GB* *147GB* *300GB* *450GB*

註：斜體字為未上市

(二)磁碟陣列(RAID)技術

磁碟陣列(Redundant Arrays of Inexpensive Drivers, RAID)係透過多顆硬碟所組成一個陣列系統，主要為加速與容錯備援運用，以保障資料的安全及提高資料可用度(Availability)，各種 RAID 模式比較，如表二。

表二 RAID 模式比較表(資料來源：本研究整理)

RAID 等級	0	1	0+1 1+0	3	4	5
種類(Mode)	Stripe		Mirror		Parity	
空間利用率	-		低		高	
最少組成硬碟數量(顆)	2	2	4	3	3	3
適合多人環境使用	V	V	V	-	V	V
具資料保護功能	-	V	V	V	V	V
支援動態擴增硬碟	-	-	-	V	V	-

註：

1. Stripe：將一筆資料的寫入分成數個區段，分別寫入不同的磁碟機。
2. Mirror：將一顆硬碟機當中的所有資料，如同照鏡子般，原封不動地存到另一顆硬碟。
3. Parity：當某顆硬碟故障時，藉由其他硬碟中的資料以同位元檢查原理來重新運算重建損壞硬碟當中的資料。

二、儲存系統發展

依資料運用需求及資料容量多寡而言，儲存系統可概分為個人與企業型儲存系統，前者以個人電腦(PC)及筆記型電腦(NB)為主，後者儲存架構不光只有硬碟及光碟機問題，企業儲存從員工電腦中的單機資料、到多台伺服器、網路交換器，再到後端儲存設備，都有密切關聯，分述如后：

(一)個人型儲存系統

除 PC 內嵌固定型硬碟機、光碟燒錄機(DVD-R/RW)及攜帶型硬碟外接盒外，隨著通用序列匯流排(Universal Serial Bus, USB)技術發展，其隨插即用(Plug and Play)及高速傳輸(Max. 480Mbps)的功能，不須經過繁瑣的安裝程序便可任意與電腦連結、配置及移除，滿足彈性與容易使用需求及實現行動生活目標。因此，運用此種連接介面的週邊儲存設備孕育而生，以下列舉三種常用可攜式(或可移除式)儲存設備。

1.USB 隨身碟

隨著快閃記憶體技術發展，隨身碟如雨後春筍般地產出，而隨身碟除資料備份用外，市場上陸續將應用程式或安裝精靈放入隨身碟，如 MP3 隨身聽、個人文件管理、Outlook 帳號管理及系統開機(Disk on Key, DoK)等功能，發揮隨身碟之跨平台使用便利性及應用性。

2.磁光碟機(Megneto Optical,MO)

MO 光碟機屬「抽取式」儲存設備，其存取資料的原理與軟碟機相仿，係利用雷射光學作讀寫時的定位，定位準確度比軟碟機高非常多，MO 片可拿來當作開機片或當硬碟使用，最大特色在於操作穩定度高、保存期限較長、可移動性及容量大等。

3.記憶卡

以 NAND 快閃記憶體做成的記憶卡，亦屬「抽取式」儲存設備，可隨處抽取、存取資料。記憶卡目前有 CF(Compact Flash)及 SM(Smart Media)介面兩種，均具存取速率高、保存容易、省電持久、高相容性及使用年限長等特色，隨著大容量記憶卡誕生，預判未來快閃記憶體將取代硬碟機，成為電腦及消費電子的主要儲存設備。

(二)企業型儲存系統

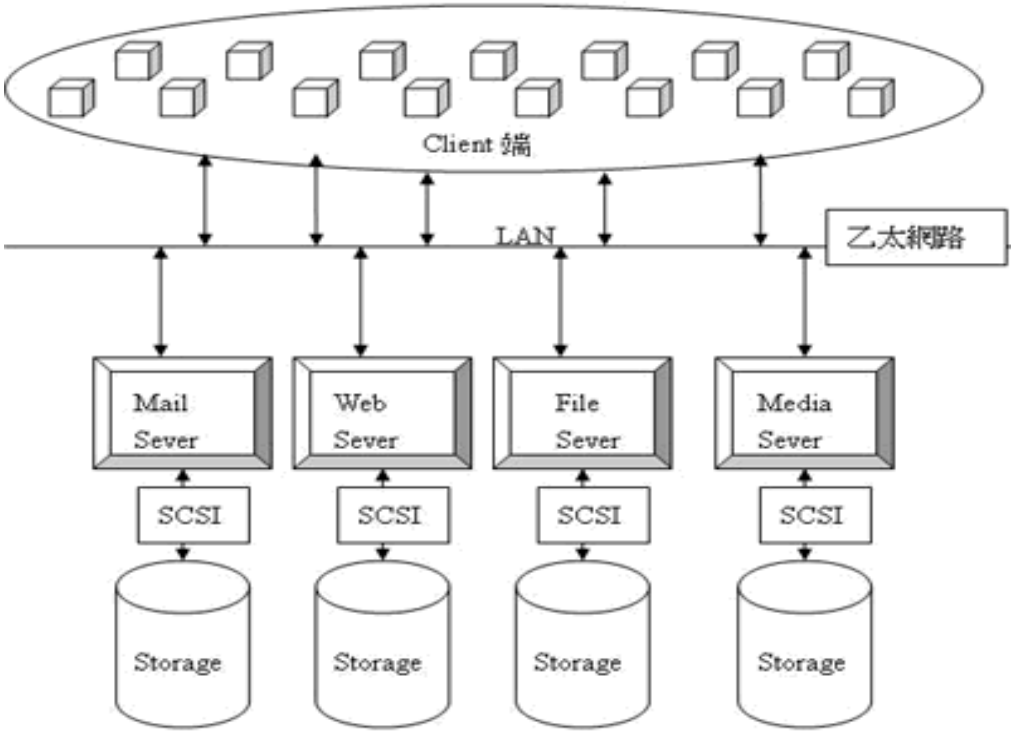
依企業儲存系統之伺服器與儲存設備間的資料存取通道來做分類，可分為直接附加儲存(Direct Attached Storage, DAS)、網路附加儲存(Network Attached Storage, NAS)及儲存區域網路(Storage Area Network, SAN)等三種架構，其架構圖(如圖一至三)及說明比較(如表三)如后：

1.DAS：類似 PC 內配置的硬碟，儲存設備直接連接至伺服器，透過伺服器

經由 Ethernet 區域網路提供網路上資料存取服務。

2.NAS：由專屬的檔案伺服器與儲存設備組合而成，其檔案伺服器經過特殊設計，把和檔案分享無關的軟硬體元件移除，並提供乙太網路介面連接至區域網路。

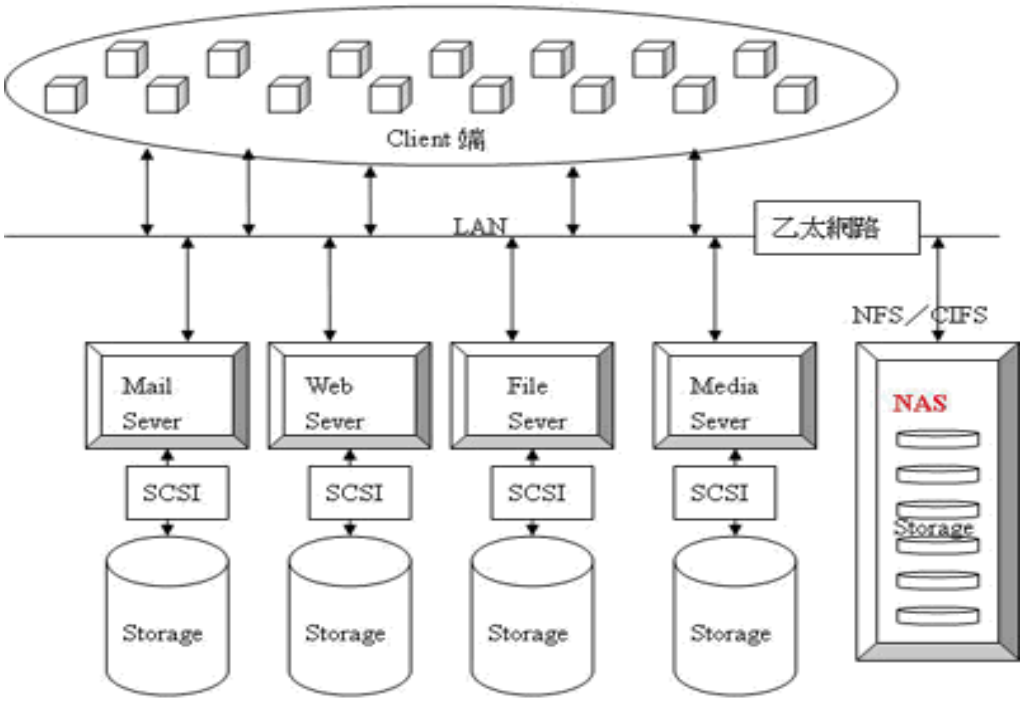
3.SAN：主流傳輸介面為光纖通道(Fibre Channel, FC)，其網路架構由 FC 交換器連接儲存設備和伺服器所構成，獨立於企業內既有的區域網路外；為達成普及化，市場陸續推出 IP SAN 儲存產品，以運用於 TCP/IP 網路環境。



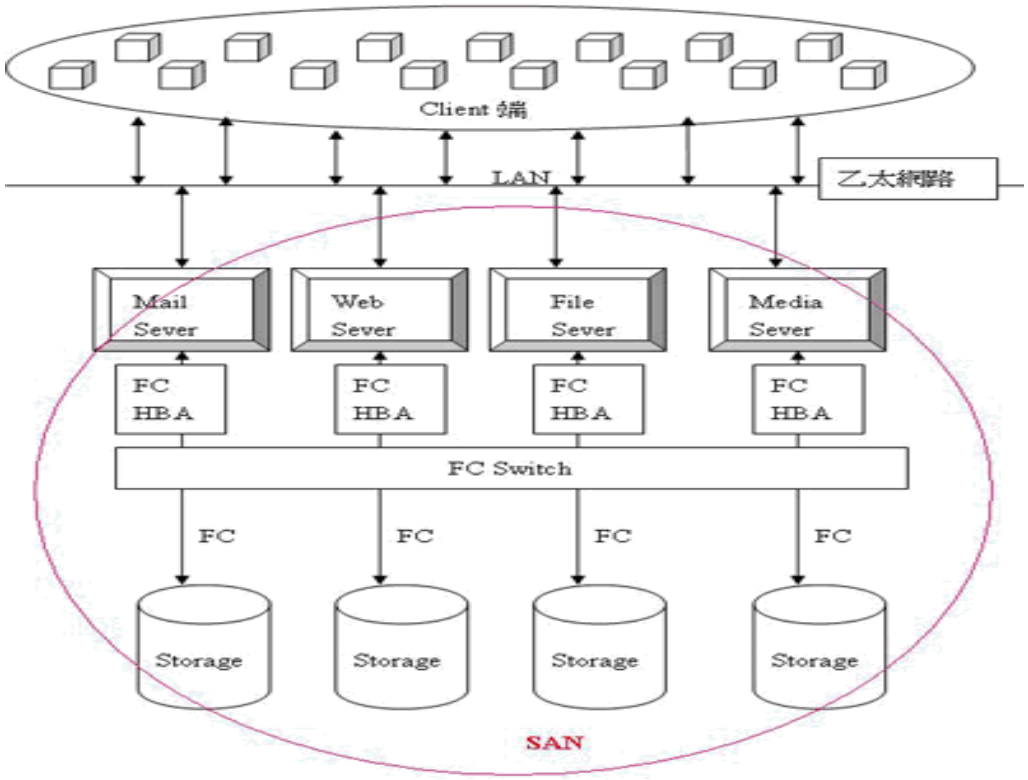
圖一 DAS 架構圖(資料來源：2005 年薛怡青[3])

表三 DAS、NAS 與 SAN 比較(資料來源：本研究整理)

架構	優點	缺點
DAS	1.建置成本較低 2.存取速度最快	1.擴充性差及無法資源共享 2.資料備份時，消耗伺服器運算能力及網路傳輸頻寬
NAS	1.系統建置容易 2.具多重協定檔案存取能力 3.Web 化管理介面 4.適用檔案層級(File I/O)存取	1.資料備份時，佔用網路傳輸頻寬 2.不支援區塊存取方式
SAN	1.簡化儲存程序，增強管理能力 2.獨立網路系統，無頻寬壅塞問題 3.儲存擴充性高 4.適用區塊層級(Block I/O)存取	1.FC 傳輸技術為主，建置成本較高 2.光纖線路佈建與距離限制



圖二 NAS 架構圖(資料來源：2005 年薛怡青[3])



圖三 SAN 架構圖(資料來源：2005 年薛怡青[3])

儲存安全弱點與威脅

儲存安全技術包含儲存、網路及安全等範疇，而儲存安全基本對象則包含有儲存系統安全、儲存資源管理(SRM)、儲存中的資料(DAR)及儲存網路內的傳輸資料(DIF)等項目，在對於儲存安全技術與基本對象有所掌握後，須評估可能存在的儲存安全弱點與威脅等風險，方可研擬因應的對抗措施，以建立有效的防禦縱深(Defense-in-depth)，以下分就安全弱點與威脅敘述：

一、安全弱點

(一)個人型儲存系統

2005 年林皇興[4]指出，Windows 作業系統的判別存取控制清單(Discretionary Access Control List, DACL)標準，尚無法支援對可攜式儲存設備進行各種適當的權限設定與使用稽核，然而將檔案加密或賦予數位憑證的方法，在現階段還不夠成熟或未加以落實而無法普及，截至目前，對於 USB 及 FireWire(1394)等連接埠，在電腦預設是開放的，任何人都可將 USB 隨身碟、硬碟外接盒等可攜式儲存設備連接到電腦，輕易地將數百 MB 到 GB 資料複製到設備夾帶出去。

(二)企業型儲存系統

除 DAS 屬獨立儲存設備，其安全弱點較偏重於環境安全保護探討外，其餘 NAS 及 SAN 均屬網路型儲存設備，其安全弱點多源自網路環境原有可能存在的弱點。2005 年 Dwivedi[5]分析 NAS 及 SAN 儲存安全，其可能存在的安全弱點，表述如下：

表四 儲存安全弱點(資料來源：本研究整理)

儲存方式	安全弱點	描述
NAS(以 Common Internet File System, CIFS 為例)	列舉 (enumeration)	CIFS Enumeration 將使用者名字、群組、分享、密碼認證方法、服務等訊息列舉，使攻擊者有機會獲得此類資訊。
	分享層級密碼 (share-level passwords)	NAS 使用單一密碼(明文)來進行網路用戶間之存取分享，造成攻擊者以暴力攻擊或竊聽方法取得密碼。
	Kerberos Ticket	Kerberos Ticket 及微軟 Active Directory 等密碼可能被洩露及允許未被授權的存取之安全弱點。
SAN	全球名稱 (Worldwide Name, WWN)	SAN 係基於節點之 WWN 以配置資料資源(data resource)，忽略 WWN 授權方法，以改變 WWN 至另一個 HBA 是非常容易的。

	E-port 複製	FC 交換器轉換至另一個交換器時，將所有名字伺服器、路由等訊息，在無須任何形式授權程序即可將兩個 E-port 連接在一起並加以複製。
	交換器管理介面	SAN 交換機之網頁 Web(HTTP)管理介面易遭受暴力攻擊法取得足夠的訊息。

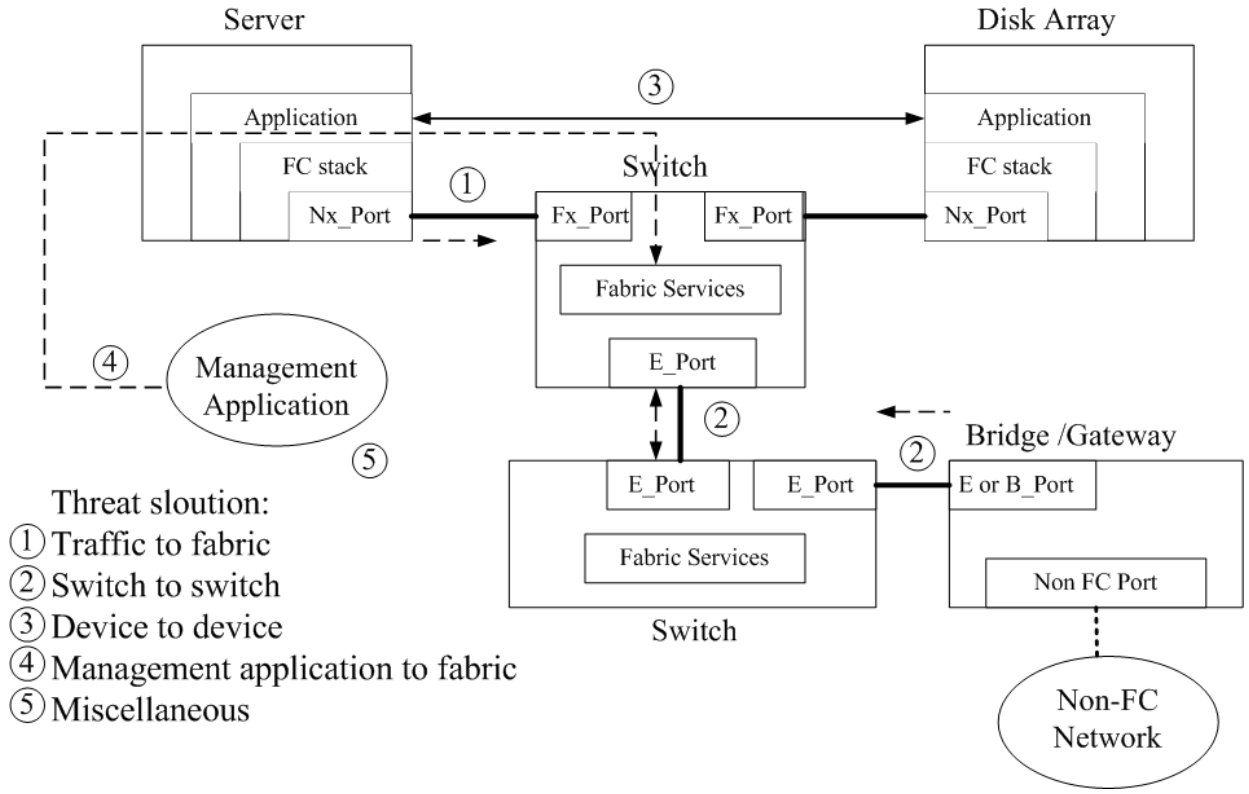
二、安全威脅

2003 年 451 小組(451 Group)[6]分析企業儲存安全威脅項目(如表五)，表述如下：

表五 儲存安全威脅(資料來源：本研究整理)

威脅項目	描述
竊取特權存取	存取根目錄(roots)或管理者帳號
更改事件	非惡意的更改資料、儲存或網路資源
特權存取的濫用	授權使用者做未被授權的事
竄改資料	藉由外部或內部偷聽者進行惡意資料竄改
竄改應用程式	更改軟體，如錯誤的升級版本(Patch)管理等
竊取硬體	竊取儲存硬體，如硬碟、伺服器等
竊取媒體	竊取實體儲存媒體，如磁帶

2004 年 Brandon[7]轉載美國國家標準協會(America National Standard Institute, ANSI)T11 專案的研究指出，FC 計有五種安全威脅模式(如圖四)，分別為 1.流量(Traffic)到 FC 交換器、2.交換器(SW)到交換器(SW)、3.設備(Device)到設備、4.管理應用程式(API)到交換器及 5.各式各樣的威脅模式，前四種屬連接埠間之威脅，係因連接埠間之存取控制權限不周延而產生安全威脅，後一項屬管理應用程式內之威脅，係因應用程式之封包流量未加密而遭竊聽。



圖四 安全威脅模式(資料來源：ANSI T11[7])

儲存安全策略及實現

儲存安全並非僅為安全概念，如何建置一個安全的儲存系統，如同產品的開發過程，須經由初期評估、可行方案、建置執行至定期稽核等工作，方可確保儲存安全。2005年Jon[8]提出儲存安全生命週期，計分為四個階段，說明如后：

(一)評估階段：評估資產儲存技術與程序及搜尋安全弱點。

(二)實踐階段:列舉創造商業的重要價值清單項目，以作為儲存安全實踐對象。

(三)建置階段：進行建置的控制及加強儲存設定，同時發展儲存安全工具。

(四)監視階段：定期稽核結果。

除依循上述儲存安全生命週期來規劃儲存安全建置工作外，制定儲存安全的策略作為目標方針亦是必要的，以下分就儲存安全策略及安全實現作一說明：

一、儲存安全策略

2005 年 Brandon[9]提出 FC 儲存安全策略，其建置步驟說明如下：

(一)使用管理標準(如 SMI-S)集中管理儲存網路和藉由標準認證機制來管制對管理網路與介面的存取。

(二)對所有光纖設備使用共通的認證標準，以統一設備間的認證作業，如挑戰交握認證協定(Challenge Handshake Authentication Protocol, CHAP)。

(三)使用 WWN 授權技術管制設備連接至光纖交換器之存取控制權限。

(四)資料加密：在 IP SAN 網路可使用 IPSec(針對 iSCSI)及在 FC SAN 網路可

使用 IEEE 1619 或 ANSI T11 FC-SP 等安全標準來對資料加密。

(五)進行定期的稽核及紀錄。

除上述外，2005 年網路儲存工業協會(Storage Networking Industry Association, SNIA)之安全技術工作小組(Security Technical Work Group)[10]依據資訊技術安全評估共同準則(Common Criteria of Information Technology Evaluation, ISO15408)所定義，由擁有者、措施、弱點、風險、威脅至資產等關係來闡述資產保護之安全概念，以達成存取控制(包含辨認、認證、授權、執行等)、可信賴性(包含資料保護、資料隔離、流量保護等)、完整性、可用性及不可否認性等安全服務目標，提供儲存安全建議(如表六)。

表六 儲存安全建議(資料來源：本研究整理)

項目	說明
儲存管理安全化	安全化對象包含管理者的帳號、存取介面與控制台及管理應用程式與命令列公用工具等。
辨認與評估全部儲存介面	1.決定哪些伺服器可連接儲存設備、儲存設備附加於哪些網路等。 2.辨認管理介面(In-band,out-of-band)、所有儲存資源(如磁帶、使用權與使用者等)。
建立風險網域	1.隔離儲存流量與一般伺服器流量，如運用網路區段劃分(Zoning)或邏輯單元遮罩(LUN masking)等。 2.將管理流量獨立於其他流量。 3.謹慎地設定網路閘道器，特別是 FC-to-iSCSI。
監視與控制實體存取	限制資料中心/交換器的存取、實體隔離交換器、關閉未使用埠、監視可移除式媒體及熱插拔硬碟。
避免因共通錯誤所導致的失敗	使用合法版權軟體、在連接與登錄網路前設定適當存取控制、定期維護韌體、更改基本設定或開放存取埠等。
注重資料安全	1.以角色為對象建置適當認證、授權及存取控制。 2.確認外部稽核紀錄項目,如時間同步地記錄每筆企圖或成功管理事件與交易，並回傳到紀錄伺服器。 3.建置適當的資料 retention、完整性及信賴性測度。
保護外部資料	敏感性資料備援於離線(off-line)的磁帶應加以加密,且加密金鑰應與資料分開儲存，當被以網路傳送至遠端資料中心仍應加以加密，或是被傳送或儲存轉送於委外資料中心前均應以加密。
瞭解揭露的弱點	執行安全掃描、維護已知的弱點並安裝安全版本(Patch)、整合入侵偵測/防禦技術。
建置適當的服務連續性	1.建置營運持續(Business Continuity)及災難復原(DR)機制來處理因事件發生所造成的資料毀損。

	2.資料備援複製朝向自動化以減低重建時間與減少人員錯誤。
利用事件紀錄功能	1.建置中控式紀錄伺服器，以確實收集所有單一事件。 2.建置適當工具來保留紀錄完整性與預防非法毀損。 3.建置分析方法來 correlate 記錄檔,辨認重大顯著的安全事件並提供安全意外事件的指示。

註：iSCSI 是一項裝置互連，使用 IP 作為通訊機制，並將 SCSI 通訊協定放置在 IP 頂端。

二、儲存安全實現

為求高效能網路系統，美國國防部(Department of Defense, DoD)運用儲存區域網路(SAN)架構進行儲存設備與電腦系統間所需通訊傳輸，而大部分 SAN 使用光纖通道(FC)技術與交換器來建置，鑑此，2005 年國防部防衛資訊系統局(Defense Information System Agency, DISA)訂定「網路上共享週邊設備(SPAN)之安全技術設置準則(STIG)」[11]，作為各單位建置安全的 SAN 架構準則，以符合資訊確保政策之要求。以下摘述說明 SAN 安全架構要求：

(一)存取控制安全

1.網路區段劃分(Zoning)

如同 IP 網路的虛擬區域網路(Virtual LAN, VLAN)一般，SAN 架構係透過橋接器、交換器及集線器等來進行伺服器與儲存設備間的埠對埠連接，利用 Zoning 隔離 SAN 為數個子網路，可有效的管理、切割及控制介於儲存設備與光纖交換器間的路徑，來達成儲存資源最大化及資料完整性與資料安全的維護。

2.邏輯單元遮罩(LUN Masking)

在光纖通道領域中，LUN 是基於系統 WWN 實現的，LUN masking 係將 LUN 分配給主機伺服器，這些伺服器只能看到屬於它們的 LUN，同樣地，可對交換器、磁碟陣列(埠)或伺服器連接埠等進行遮罩的方法，以限制儲存設備的存取，進而保護 SAN。

(二)網路與主機之間的安全

SAN 可視為獨立網路系統，同樣適用於一般網路安全政策要求，應運用公開金鑰基礎建設(Public Key Infrastructure, PKI)、加密技術及 Zoning 的存取控制清單(Access Control List, ACL)等，來建立光纖交換器彼此之間、主機到 FC 交換器之間的安全連接及安全的管理介面。

(三)資料備援(Data Backup)與災難重建(Disaster Recovery, DR)

備援與重建程序攸關 SAN 系統的安全與可用性，當系統發生當機，導致服務中

斷，而影響作戰時的資源可用性。當於主要站台存取重要資料檔(如磁碟或磁帶資料庫)時，一旦發生系統當機，光纖交換器應設定自動地接管(Fail over)到另一個不同的備援檔，即達成異地備援建置。

儲存安全標準規範

自從美國恩隆案爆發後，美國證期會通過 SEC 17a-3/4 法案，要求對交易資料讀寫正確及時間點都須予以證據保存；另通過沙賓法案(Sarbanes-Oxley Act)或新巴賽爾資本協定(New Basel Capital Accord)，對於財務會計資料的確保，不僅攸關儲存年限，與儲存資料的安全性有極大關係。

鑑此，陸續有許多單位分別訂定儲存安全標準，以明確規範建置儲存系統所需安全機制，以下作一簡介：

一、國際資訊技術標準委員會(InterNational Committee for Information Technology Standards, INCITS)

2005 年美國國家標準協會(ANSI)之技術委員會執行 T11 專案並制定光纖通道安全協定(FC- Security Protocol, FC-SP)[12](草案)，分別由安全基礎建設、可信賴性、完整性、授權與存取控制及認證等項目定義光纖通道內各設備間(如主機到 FC 交換器、FC 交換器到 FC 交換器及 FC 交換器到儲存設備等)彼此的安全協定作業規範，如表七。

表七 FC-SP 光纖通道安全架構(資料來源：本研究整理)

項目	運用說明
安全基礎建設	1.憑證：運用公開基礎建設(PKI)應用系統。 2.密碼管理：使用光纖通道密碼認證協定(FC Password AP, FCPAP)管理密碼。 3.共享密鑰管理(Shared-Secret Administration)：使用挑戰交握認證協定(Diffie-Hellman, DH-CHAP)或認證伺服器(RADIUS)進行AAA(Authentication Authority Account)管理。
可信賴性	1.使用安全連線管理協定(Security Association Management Protocol, SAMP)以進行SA連線。 2.使用ESP (Encapsulating Security Payload)封包格式。 3.使用網路密鑰交換(Internet Key Exchange, IKE)，進行密鑰管理。
完整性	結合ESP並使用數位簽章機制(Signatures / HMAC)。
授權(存取控制)	1.使用存取控制清單(ACL)來授權管制。 2.制定安全目標與政策，進行政策分配機制。
認證	1.光纖通道認證協定(FC Authentication Protocol, FCAP)：使用憑證

	系統。 2. 光纖通道密碼認證協定(FCPAP)：使用遠端安全密碼(Secure Remote Password, SRP)機制。 3.挑戰交握認證協定(DH-CHAP)：使用共享密鑰或導入DH交換機制。

二、電機電子工程學會(Institute of Electrical and Electronics Engineers)

2005 年 IEEE 安全儲存工作小組(Security in Storage Work Group, SISWG)[13]制定 IEEE 1619 標準(草案)，定義植基於磁區(sector-based)的儲存設備之加密演算法─LRW-AES，說明 其加密轉換(Encryption Transformation)及匯出/匯入加密金鑰方法(如表八)。

表八 LRW-AES 加密方法(資料來源：本研究整理)

演算法	操作模式	作者	特色
FIPS 197 AES	LRW	Liskov Rivest Wagner	1.可扭動的(Tweakable)區塊加密 2.防禦 copy-and -paste 攻擊 3.適用於光纖通道(FC) 4.適用於靜態資料(DAR)

國軍資訊儲存機制安全部署建議

目前針對國軍網路環境常見的USB隨身碟、PC硬碟、NAS及SAN等儲存系統安全，以下提供一些安全建議：

一、USB 隨身碟

(一)透過 BIOS 設定禁用 USB

除將所有電腦 USB 連接埠拔除、貼黏管制標籤，甚至焊死等作法外，於 BIOS 系統中設定禁用 USB(包含禁止於 BIOS 設定電腦允許被任何 USB 設備執行系統啟動)是最直接也是最簡單的方法，唯 BIOS 也須設定密碼。缺點是缺乏集中管理設定、存在 BIOS 密碼被破解疑慮及造成如 USB Token、IC 讀卡機等身分辨識機制無法透過 USB 來使用。

(二)導入軟體式集中管理機制

前述 BIOS 設定潛在人為因素，且無法集中管控，為兼具使用便利需求及安全存取管控，結合資產管理軟體或網域(Domain)伺服器導入軟體式集中管理軟、硬體設備，須可管理各種 USB 設備、軟碟機、光碟機、藍芽、FireWire、紅外線及串列埠等，不僅進行使用監視及稽核回報(如 Kerberos)，更落實全面性的使用管制及存取權控。

(三)運用存取認證及加密機制

對於核准使用公發 USB 隨身碟用戶，囿於隨身碟的隨插即用及輕薄短小，在有意或無意情形下，將隨身碟的公務資料複製至非公發電腦或隨身碟遭竊、遺失而導致機密資料外洩，國軍應運用具存取認證(含指紋生物辨識功能)及加密機制之隨身碟，唯有在特定公務電腦方能進行檔案存取且存在於隨身碟的檔案生命週期應加以限定。

二、硬碟機

硬碟機(無論系統碟或資料碟)雖說大都是固定型且內嵌於電腦上，攜帶性及移動性不高，唯隨著硬碟技術突破，陸續有外接盒式之高容量硬碟產出，且尺寸越做越小，其存在的資安風險等同於隨身碟。

(一)運用系統及檔案加密機制

除環境實體安全(如門禁管制、監視系統等)考量外，特別在機敏作業區或演訓支援在外的 PC 或 NB，應運用軟、硬體加密及密鑰管理機制，將整顆硬碟(資料)加密，甚至從 BIOS 系統開機即以外接金鑰 Token 來管制存取權限，強化安全防禦縱深。

(二)導入數位版權管理(Digital Right Management , DRM)文件控管軟體

國軍資訊安全首重於機敏數位資料的保護，對於各種檔案格式的文件內容，為達成集中安全控存目標，運用中央控管軟體來進行個人端的文件編輯軟體(如微軟 Office 或 OpenOffice 等)之線上存取認證、加密存取及密鑰備援等工作，一旦複製資料至離線或未授權的電腦系統，即無法獲得認證與配賦金鑰進而讀取檔案。

三、NAS 與 SAN

(一)NAS

國軍內部區域網路環境內大都屬於 IP 網路，係使用 NAS 進行資料集中控管，區域網路之用戶對於 NAS 儲存設備之間應安裝網路儲存加密器，其需支援資料存取協定，如 NFS (Network File System)及 CIFS(Common Internet File System)，配合目錄管理伺服器管理存取權限帳號，所有存取於 NAS 儲存設備之檔案均以檔案層級(File-level)方式加密後儲存。

從遠端用戶之個人電腦端至網路儲存加密器之間可透過虛私有網路(VPN)方式建立安全通道(Tunnel)，以確保用戶端(Client)至網路儲存加密器間之傳輸安全。

(二)SAN

SAN 網路儲存設備多屬 FC 介面環境，隨著 Gigabit Ethernet 技術進步，SAN 朝向支援 TCP/IP，因此，如同 NAS 環境一般，對 SAN 儲存網路之間應安裝網

路儲存加密器，其需支援資料存取協定，如 FCP(FC over SCSI)或 iSCSI(SCSI over IP)，所有存取於 SAN 之檔案均以區塊層級(Block-level)方式加密後儲存，至於磁帶(Tape)備份儲存，亦可藉由網路儲存加密器加以壓縮、加密後再行儲存。

結論

當企業產出重要資料時，第一步就是要先加以保護，第二步則是進行管理，所謂「工欲善其事，必先利其器」，唯有全盤掌握資料安全儲存技術發展，方能找出儲存安全問題並加以對症下藥，而資訊技術環境瞬息萬變，當環境改變時，唯有像ISO 17799中不斷精進的規劃、執行、查核及改善(Plan,Do,Check,Active/PDCA)精神，才能確保資訊安全。

國軍規劃朝向資料網路中心(Internet Data Center, IDC)方向發展同時，對於建置安全無虞的儲存系統，應由儲存安全政策訂定、儲存安全稽核至定期檢討，並輔以人員的資安教育訓練及設備的存取管控軟體工具，以達成資訊安全目標，進而確保國軍在數位化戰場之資電優勢，實為刻不容緩的任務。

註釋

1.張智鴻，黃彥棻，「為資料買保險-儲存安全設備」，i Thome 電腦報專刊，第 13 期，頁 104-105，2005 年 5 月。

2.企業資安技術應用專刊，「2005 年十大資安威脅」，iThome 電腦報專刊，第 11 期，頁 28-35，2005 年 3 月。

3.蔣怡青，「儲存應用面面觀-深入剖析 NAS 系統」，DigiTimes 企業 IT，2005 年 7 月 19 日。

4.林皇興，「如何控管行動周邊裝置所帶來的資安風險」，iThome 電腦報專刊，第 11 期，頁 144-145，2005 年 3 月。

5.Himanshu Dwivedi “Securing Storage : a practical guide to SAN and NAS security ”, Addison-Wesley, 2005.

6.451 Group “Storage security market : emerging opportunities, unseen threats”, 451 Group,2003.

7.Brandon Hoff “Steps for ensuring storage network security”, InfoStor, Http:// is.pennnet.com,2004.

8.Jon Oltsik “Kasten Chase: Setting the standard for storage security”, Enterprise Strategy Group(ESG),2005.

9.Brandon Hoff “Steps for ensuring storage network security”, SC Magazine,2005.

10.Eric A. H., LeRoy B., Richard A. “Introduction to storage security”, Storage Networking Industry Association(SNIA),2005.
11.DISA “Sharing Peripherals Across the Network(SPAN)”, Version 1,Release 1, U.S Deportment of Defense(DoD) ,2005.
12.T11 Technical Committee “Fibre Channel – Security Protocol (FC-SP)”, ANSI, Rev 1.73, INCITS,2005.
13.Security in Storage Workgroup “Draft standard architecture for encrypted shared storage media”, IEEE P1619 D3, IEEE Computer Society,2005.