第二十一章

數位社會檔案管理目錄服務初探

A Preliminary Study on the Directory Service in Digital Records Management

樊國楨

Kwo-Jean Farn

鈺松國際資訊股份有限公司 副總經理

Vice President , Internet Security Solutions International Co.

壹、前言

檔案爲各級機關依法行使公務，於工作進行中所產生之各項紀錄，具有行政稽憑、法律信證與績效展現等重要功能，亦爲學術研究資料最佳之史料來源。鑑於我國政府部門檔案管理原無統一之立法，全國各機關管理檔案業務之法令，僅有行政院所訂的「事務管理規則」中設有檔案管理一章，致各機關檔案之蒐集、整理與借調管理標準寬嚴不一，亦未定有開放使用之辦法，以供應用[1]。然檔案管理機制之建構攸關知識經濟之發展與人民知的權利，先進國家均設有職司檔案管理之運作及其應用(Use)等事宜的專責機構；同時，頒佈相關之法律作爲檔案管理之依據[2]。

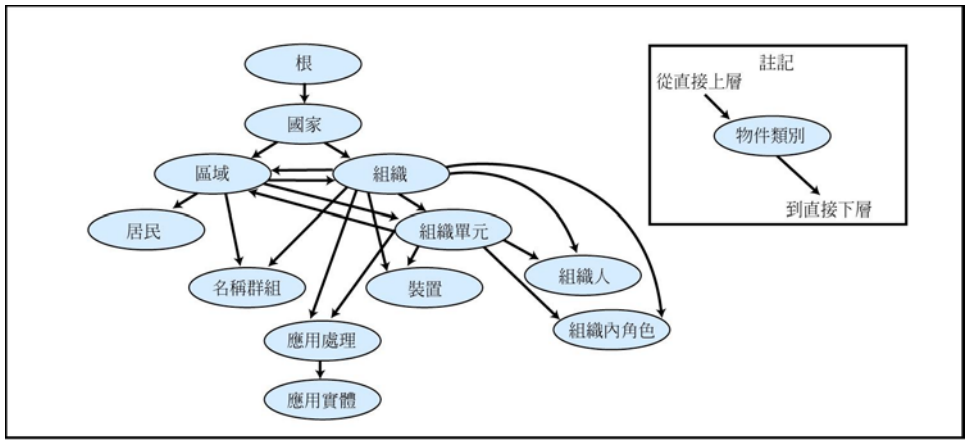
爲健全我國檔案管理制度，「檔案法」之研訂可上溯至 1986 年全國行政會議之決議；之後，國史館於 1989 年 2 月 23 日以(78)台國料字第 0268 號函送「中華民國檔案法」草案請行政院參處，經行政院交行政院研究發展考核委員會組織專案小組審慎研議，歷經 19 次會議，反覆討論，完成初稿，復徵詢五院暨各部會、學會等相關機構意見後，於 1992 年 1 月 20 日以(81)會書字第 00410 號函將「檔案

法草案」函報行政院，經行政院 1992 年 5 月 7 日第 2278 次院會修正通過；2002 年 5 月 22 日行政院以台(81)研書字第 02471 號函送「檔案法草案」，請立法院審議；經立法院三讀通過後，於 1999 年 12 月 15 日以華總一義字第 8800297480 號總統令頒佈，寫下我國檔案管理的新頁。

檔案管理之最終目的是爲提供使用，檔案大都均採閉架式管理，一般讀者無法透過直接瀏覽的方式找到所需要的檔案，需要依靠查檢工具，檢案的查檢工具經透過各種不同形式的目錄，建立檔案的實體與知識管理[3]。由於電子科技的一日千里，檔案資訊化已是潮流之所趨，如何使用線上查詢與閱讀並就其應用加以存取控制(Access Control)已是數位社會中目錄管理的發展方向。根基於此，本文分於第二節與第三節簡要研析物件識別符(Object Identifier，簡稱 OID)、目錄服務(Directory Service)之標準與角色基存取控制（Role Based Access Control，簡稱 RBAC）及其在檔案管理上之可能應用；第四節，我們探討數位檔案管理目錄服務之保護剖繪；最後，在第五節提出本文的結論。

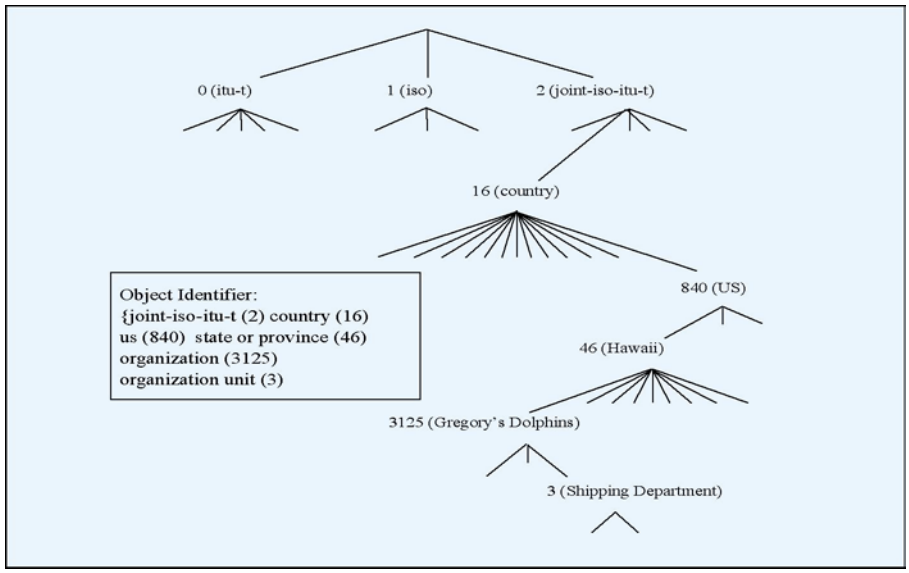
貳、目錄服務與物件識別符

現今資訊科技的快速發展與散佈，已經爲商務運作、社會互動與政府行政的本質帶來了重大的改變，全國檔案管理的資訊化與標準化已在進行中[4~6]，由於目錄服務的整體價值正隨著數位社會的日益普及而逐漸提高，一個良好的目錄服務會幫助我們建立儲存、發展、傳播、擴散知識的基石，進而達到資源共享之檔案管理應用之目的。廣義而言，目錄服務是一種資料儲存的結構與檢索之協定，國際標準組織早在 80 年代就開始制定數位世界目錄服務的標準，提供如圖一與圖二所示之資訊社會的目錄服務，自 1986 年起在分散式網路上提供目錄服務的商品開始陸續問市；目前，在分散式網路環境下提供資料儲存與檢索的系統，無論是在效能、安全與強健方面，目錄服務系統的表現均優於資料庫管理系統[7]。



圖一 目錄資訊基底(Directory Information Tree，簡稱 DIT)架構示意

(說明：參考 ISO/IEC 9594-7：1990 (E)標準)



圖二 物件識別符(Object Identifier，簡稱 OID)結構示意

在國際標準組織(the International Organization for Standardization，簡稱 ISO)頒佈之目錄服務標準中[8]，目錄服務內部所儲存的資料均有一清楚的命名與定址機制，這個機制稱之爲名稱空間(Namespace)，名稱空間所對應的資訊儲存空間稱爲目錄資訊基底(Directory Information Tree，簡稱 DIT)。ISO 同時規範了 DIT 之註冊程序[9]，提供 DIT 註冊機構以及想要在註冊簿上登錄項目的機構或人使用。在 DIT 中的每一個節點(Node)被稱做物件(Object)，每一物件均有自己隸屬的物件類別(Object Class)，每個物件是由一些屬性(Attribute)所構成，而每個屬性均有自己

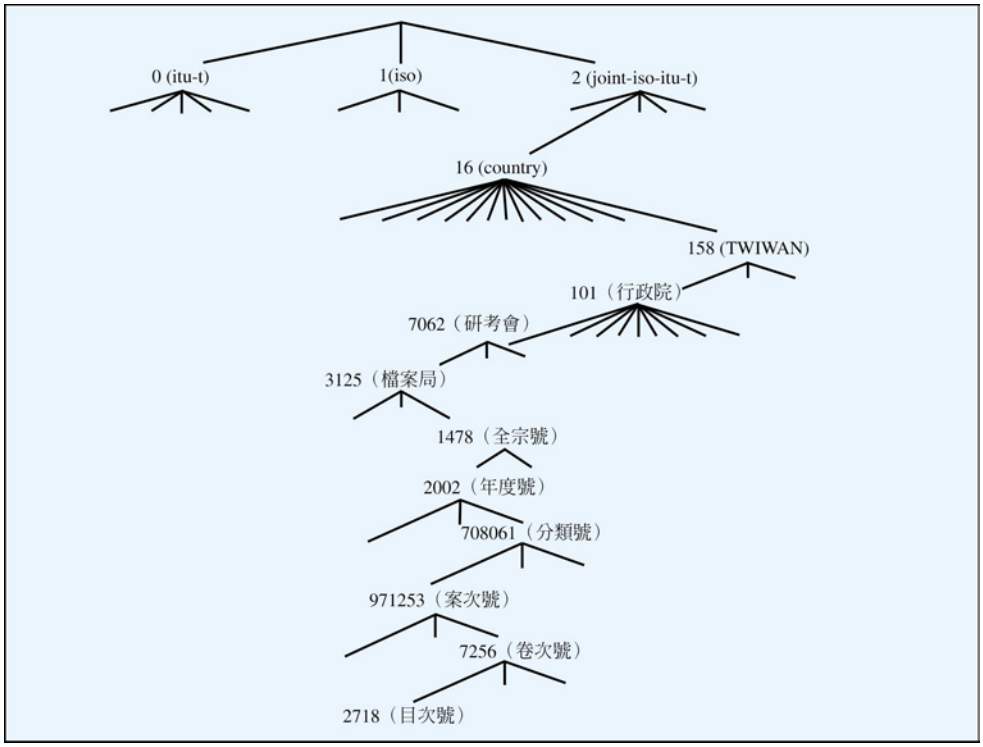
隸屬的屬性種類(Attribute Type)。

在物件類別方面，ISO/IEC 9594 定義了 17 個基本物件類別，並允許使用者自行增加與擴充物件類別；在屬性種類方面，ISO/IEC(International Electrotechnical Commission) 9594[9] 定義了 40 個基本屬性，亦允許使用者自行增加與擴充屬性種類。換言之，OID 的註冊簿是一個共同參考點(Common Reference Point)，透過唯一的識別符(Identifier) 註冊在其上的資訊物件(Information Object)，OID 可以是團體組織(例如：國家、院轄市、部會、機構、公司、……)、典藏單位(Repository)、全宗及副全宗(Record Group and Subgroup)、文件系列(Series)、案卷(File Unit)及案件(Item)、……；因此，這個註冊簿也可視爲用以確立註冊項目之基本屬性的儲存庫(Repository)，其主要目的是要讓數位世界的個體(Entity)能夠識別並且協定一個已經達成協議的 OID。依據 ISO 對 OID 結構之定義，OID 是一樹狀結構，其根是在 ISO 或 ITU-T(International Telecommunication Union － Telecommunication Standardization Sector)組織，而每一節點代表一行政管理單位，負責該節點之下分支(Arc)的配置與管理[10]。

綜上所述，數位世界的目錄服務與物件識別符應可適用於檔案管理之檔號編訂與編案編目[11]之上，圖三是其可能的使用示意說明。

參、目錄服務與檔案管理

檔案管理之目的在於將實際作業文獻彙集的紀錄(檔案)典藏並應用，前述紀錄一經編案後檔案管理人員應確立該案件於卷首之位置，編訂檔號，依「檔案分類編案規範」規定，機關檔案檔號結構(指每一案件而言)包括年度號、分類號、案次號、卷次號及目次號；國家檔案號結構則區分爲上下兩排，上排爲國家檔案全宗號，下排爲原機關(構)、團體或個人之檔號，以遵循檔案整理之原則。期使檔號成爲檔案管理之唯一識別鍵值，在檢索上具唯一及不可重覆性[11]。

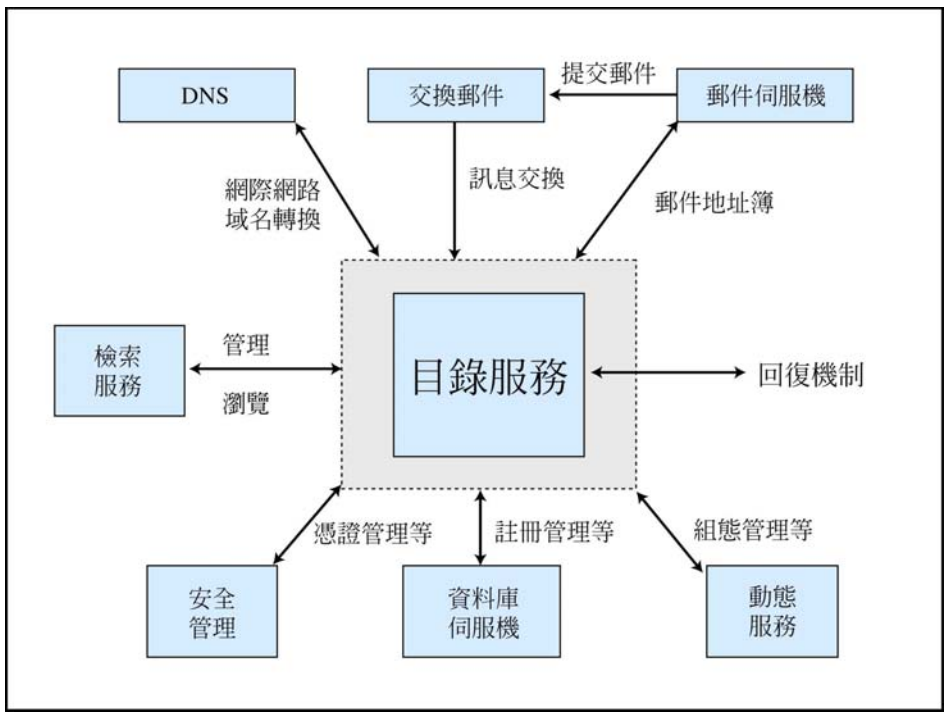


圖三 檔案立案編目物件識別符示意說明

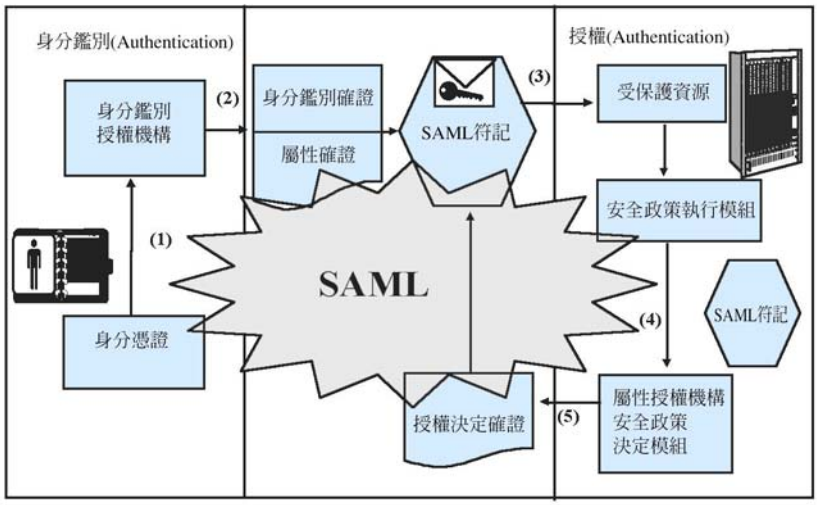
電子化政府的檔案管理系統必須面對全國各地甚至國外使用者的檢索，其目錄所支持的協議與物件格式是對目錄的開放性(Openness)程度之測量；然而，理想的開放性也給檔案管理人員帶來更多的挑戰。如果電子化政府的網路對企業、學校、個人等用戶開放檔案檢索，那麼，其安全問題將更加嚴峻。一個良好的目錄服務系統已將網際網路之域名系統(Domain Name System，簡稱 DNS)與作業系統之目錄服務整合在一起，提供如圖 3.1 之命名、檢索、登錄、管理、答詢等目錄管理以外的功能。在安全性方面，目錄服務提供存取控制表列(Access Control List，簡稱 ACL)[12]，將不同之目錄基底 (例：圖二與圖三) 間依存取政策，建立不同物件間之存取權利，而不同物件間之身分鑑別可以透過電子化政府中已建置使用三年之公開金鑰基礎建設(Public Key Infrastructure，簡稱 PKI)的現有機制[13]，實作如聯合國 UN/CEFACT(The United Nations Center for Trade Facilitation and Electronic Business)組織與 OASIS(The Organization for Advancement of Structured Information Standards)組織合作於 1999 年 11 月共同成立 eb XML (e-Business XML)成爲產業標準之國際計畫，所訂定如圖四、圖五與圖六所示，具開放性之電子化

政府檔案管理角色基存取控制系統[14~15]，應是可行方案。

僅使用 PKI 技術無法達成一個使用者簽入(Login)一次，跨多個檔案管理資訊系統存取控制的問題，植基於 PKI 與傳輸層安全(Transport Layer Security，簡稱 TLS)協定技術可以解決上述問題。一般而言，使用目錄伺服器（Directory Server，簡稱 DS）與 TLS 即可建置伺服器端主催（Server-Pull）架構之 RBAC 系統，提供跨越多個網域，存取異類網路資源與服務的網格(Grid)化[16]，具備安全保證(Information Assurance)之分散式的、開放性之動態的電子化政府檔案管理角色基存取控制系統。

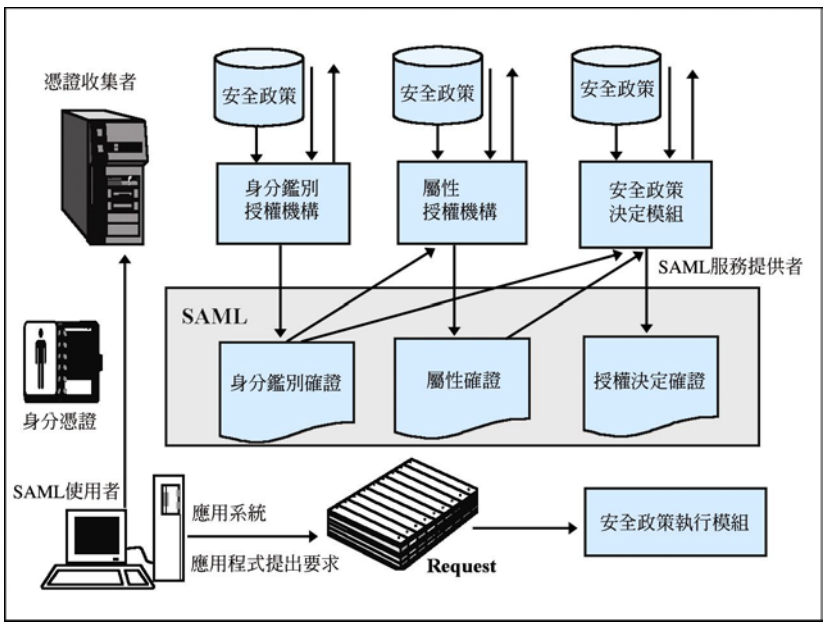


圖四 目錄服務功能機制示意說明



說明：1. PKI：Public Key Infrastructure
2. SAML：Security Assertion Markup Language

圖五 植基於 PKI 之存取控制步驟示意說明之一



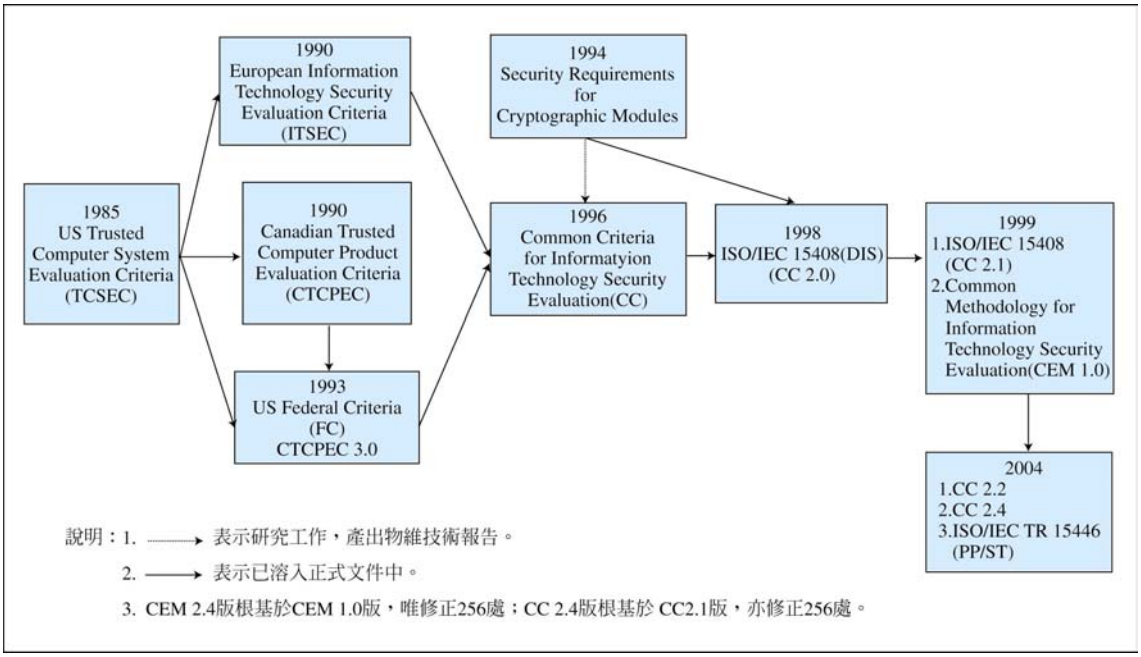
圖六 植基於 PKI 之存取控制步驟示意說明之二

肆、目錄服務安全初探

由於電子科技的一日千里，電腦與網路的結合，已在二十世紀的末期發出了令人眩目的光環，對人類社會文明所產生的擊與影響，顯示了今日資訊安全技術的發展路途，在資訊安全工程與管理的研究中，「跨領域」的整合不再僅是「研究與瞭解」而已，已經更直接地進入「建置與執行」的階段。

今日有關資訊安全可信賴性的策略，都是在不完整的資訊內容下做決定的，標準可以減輕因不完整資訊所引發的困難，因爲標準可以減少選擇的範圍而簡化可信賴性供給與需求決策制定的過程。標準的發展與改革會仔細研討以減少現有設計的缺點並且因而提昇可信賴性。同時，標準的存在會提昇關於一個評估脆弱性存在與否的基礎。

自關稅暨貿易總協定(General Agreement on Tariff and Trade，簡稱 GATT)體系之技術性貿易障礙協定(Agreement on Technical Barrier to Trade，簡稱 TBT)中要求各國爲安全、衛生、環保或保護消費者等因素，而訂定之技術法規或標準，以及證明相關產品符合這些技術法規或標準之符合性評鑑程序(Conformity Assessment Procedure，簡稱 CAP)，不應對國際貿易造成沒有必要的障礙後。鑑於沒有真確性(Integrity)等安全可靠性質的資訊，電子商務與電子化/網路化政府等均將遙不可及，虛擬世界仍將跳不出文娛和廣告的格局；1999 年 12 月 1 日，自 1990 年開始製訂之全球資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation，簡稱 CC)CC2.1 版正式成爲 ISO/IEC 15408 號標準[17]，圖七與表一分別是其發展簡史之示意與說明。換言之，在電子化/網路化的社會中，資訊系統的安全性產品、系統及服務標準將有調和一致的國際規範。



圖七　可信賴資訊系統安全評估準則簡史

表一　可信賴通資訊系統安全評估準則簡史示意說明

1	1985 年 12 月 26 日：美國公布俗稱橘皮書之可信賴電腦系統評估準則。
2	1987 年 7 月 31 日：美國公布俗稱紅皮書之可信賴電腦安全評估準則網路產品解釋。
3	1990 年： 3.1 歐洲之英國、法國、德國與荷蘭共同公布了資訊技術安全評估準則。 3.2 加拿大公布了可信賴電腦產品評估準則。 3.3 ISO 開始進行資訊技術安全評估標準制定之工作。
4	1991 年 4 月：美國公布了俗稱紫皮書之可信賴電腦安全評估準則資料庫管理系統產品解釋，成爲溯至 1967 年起，美國政府機關對資訊安全的可信賴研究中，陸續出版通稱彩虹系列之資訊安全評估相關報告之第 21 冊；彩虹系列至 1999 年 12 月 15 日，共有 33 冊，第 33 冊於 1993 年 11 月出版。
5	1993 年 1 月： 5.1 美國公布了融合歐洲與加拿大之資訊技術安全評估準則的可信賴電腦安全評估準則之聯邦準則。

5.2 加拿大公布了融合歐洲之資訊技術安全評估準則並包含密碼模組在內之可信賴電腦產品評估準則第 3 版。

6 1993 年 6 月：美國、加拿大、英國、法國、德國與荷蘭訂定可信賴資訊技術安全評估準則之 7 個機構(美國有國家安全局、國家標準與技術研究院(National Institute of Standard and Technology，簡稱 NIST) 2 個機構參加)，共同訂定資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation，簡稱 CC)，由 CCEB(Editorial Board)審核相關文件。

7 1994 年：

7.1 美國 NIST 公布了密碼模組安全需求 NIST FIPS PUB 140-1。

7.2 1994 年 11 月，ISO 開始進行資訊系統安全評鑑標準制定之工作。

8 1996 年 1 月：CCEB 公佈了 CC1.0 版。

9 1996 年 3 月 30 日：CCEB 公布了植基於 CC 之密碼模組評估準則草案 0.99b 版。

10 1996 年 4 月：CC1.0 成爲 ISO/IEC 15408 草案。

11 1997 年 10 月：ISO/IEC 15408 草案修正後之 CC2.0 版草案完成。

12 1998 年 5 月：CCEB 公布了 CC2.0 版。

13 1999 年 6 月 8 日:美國宣布 CC2.1 版已正式通過成爲 ISO/IEC 15408 之國際標準；1999 年 8 月，資訊技術安全評估共同方法(Common Methodology for Information Technology Security Evaluation，簡稱 CEM)第 1 版公佈。

14 1999 年 11 月 18 日：美國國家技術標準局公布了 NIST FIPS PUB 140-2 草案。

15 2000 年 8 月 30 日，NIST 公告 FIPS 140-2 將以符合 CC 之規範撰寫，並冀期成爲 CC 密碼模組保護剖繪。

16 2001 年 5 月 25 日，美國 NIST 公布了使用 CC 之 FIPS PUB 140-2。

17 2002 年 4 月 19 日，資訊技術安全評估共同方法第 1.1a 版公布；同年 4 月 25 日，ISO/IEC JTC1/SC27 將其做爲 ISO/IEC 18045 WD(Working Draft)第 1 版。

18 2003 年 6 月 30 日，ISO/IEC JTC1/SC27 公布根基於 FIPS PUB 140-2 之 ISO/IEC 19790 WD 第 1 版。

19 2003 年 9 月 30 日，ISO/IEC JTC1/SC27 公布根基於 ISO/IEC 15408、CEM 等之作業中系統安全評鑑（Security Assessment for Operational Systems）之 ISO/IEC TR

	19791 WD 第 1 版。
20	2003 年 12 月 31 日，CCEB 公布 CC2.1 之 138 項疑義之釋義，共 36 項修正之最終詮釋文件（Final Interpretation，簡稱 FI）。
21	2004 年 1 月，根基於 FI，CCEB 公布 CC2.2 版。
22	2004 年 3 月，根基於保證保護剖繪（Assurance Protection Profile Evaluation，簡稱 APE）與保證安全標的評估（Assurance Security Target Evaluation，簡稱 ASE）之修訂，CCEB 公布更動 256 處條文之 CC2.4 版。

CC 是結合 TCSEC、ITSEC 與 CTCPEC 的優點，做爲經由保護剖繪(Protection Profile，簡稱 PP)與安全標的(Security Target，簡稱 ST)讓資訊系統發展者與評估者遵循一致規範之描述資訊產品或系統安全性的共通結構與語言。在 CC 中，PP 包含許多和實作上無關的安全需求，可爲資訊技術安全需求的詞典；ST 則是進行資訊安全評估主體之評估標的(Target of Evaluation，簡稱 TOE)所需的許多安全需求與規格所形成的集合，是評估資訊產品或系統的基石。在 CC 中，功能組件(Component)是表示 PP 與 ST 中的各種安全需求；CC 同時包含評估其未列出之功能組件的安全評估保證需求的規範，在使用 CC 未列出之功能組件時，事先須經評估機關核准。爲落實 CC 之認證、驗證與檢測機制，自 1997 年 10 月 7 日起，美國就公告了其相關工作計畫，並於 1999 年 5 月 14 日起正式實施，其使用示意與簡史請分別參見表二與表三，表四是其保證評核等級檢測項目示意說明。

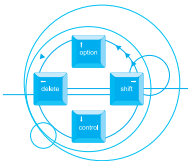
表二 資訊技術安全評估共同準則使用示意

共同準則典範(Paradigm)	系統取得典範(註：ISO/IEC 15408 亦即 CC)
保護剖繪(Protection Profile)	徵求建議書文件(Request for Proposals)
安全標的(Security Target)	建議書(Proposals)
評估標的(Target of Evaluation)	交付(Delivered)系統
系統評估結果	系統驗收與否依據

說明：共同準則－資訊技術安全評估共同準則(Common Criteria for Information Technology Security Evaluation，簡稱 CC)。

表三　ISO/IEC 15408 認證機制簡史

1	1997 年 10 月 7 日，美國公告了針對 ISO/IEC 15408(以下簡稱 CC)通過後認證機制所需之 TTAP(Trust Technology Assessment Program)Laboratories，接受植基於 CC 之測試與評估工作，做爲 NIAP (National Information Assurance Partnership) CCEVS(Common Criteria Evaluation and Validation Scheme)認證機制建立前之過渡期因應方案。
2	1997 年 11 月 8 日，TTAP 提出植基 CC 之認證、驗證檢測工作建議。
3	1999 年 4 月，美國、加拿大、德國、英國、法國共同簽署 CCMRA(Mutual Recognition Agreement)，預期歐洲、亞太其他各國將陸續加入。
4	1999 年 5 月 14 日，美國公告了 CC 認證計畫，同時宣布密碼模組認證計畫將併入此計畫。
5	1999 年 6 月 8 日，美國宣布 CC 2.1 版正式成爲 ISO/IEC 15408。
6	2000 年 5 月 23~25 日，在美國 Baltimore International Convention Center 舉辦第 1 次 CC 國際研討會。
7	2000 年 8 月 30 日，美國公告 Computer Science Corporation(CSC)，CygnaCom Solutions, Science Applications International Corporation (SAIC) 與 TUViT Incoporated 4 家民間實驗室已經通過 NIAP 的認可 CCTL$_S$(Common Criteria Testing Laboratories)。
8	2001 年 7 月 18~19 日，在英國 Brighton 舉辦第二次 CC 國際研討會。
9	2002 年 5 月 13~14 日，在加拿大 Ottawa 舉辦第三次 CC 國際研討會。
10	2003 年 9 月 7~9 日，在瑞典 Stockholm 舉辦第四次 CC 國際研討會。
11	2004 年 9 月 28~30 日，在德國 Berlin 舉辦第五次 CC 國際研討會。



表四 資訊技術安全評估保證等級摘要

保證類別	保證屬別	保證組件(Component)評估保證等級						
(Class)	(Family)	EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
組態管理	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
交付和運行	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
開發	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
指導性文檔	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
生命週期支援	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
測試	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3

脆弱性	AVA_CCA					1	2	2
評鑑	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

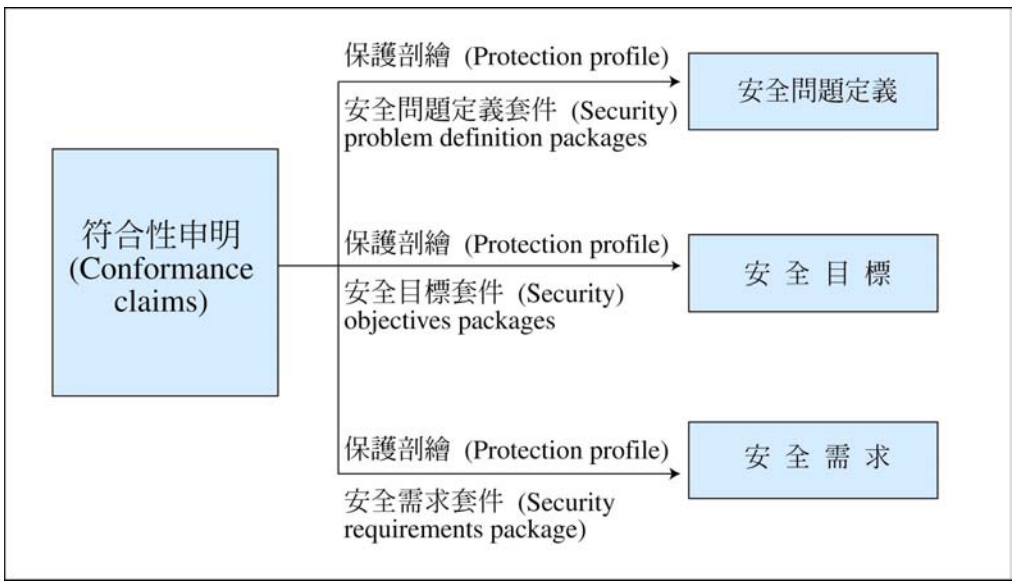
說明：ACM、AUT 等之定義請參考 ISO/IEC 15408 號標準。

表四中定義之七級評估保證等級（Evaluation Assurance Level，簡稱 EAL）之七級，其內含簡述如后：

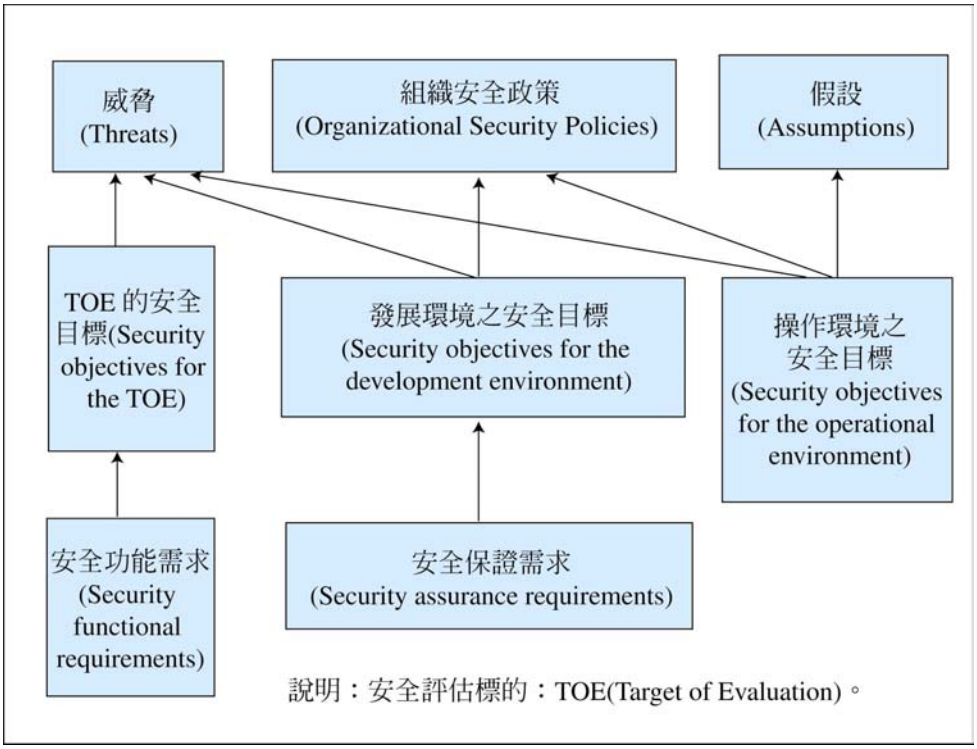
1. EAL1：功能測試，適用於要求正確操作而安全威脅認爲並不嚴重的情況，它對要求獨立安全保障來支持應有的內容保護是很有價值的，適用於個人（家庭）資訊使用環境的保護。
2. EAL2：結構測試，在交付設計文件和測試結果時，EAL2 需要研發者的合作，但不應超越與良好商業運作的一致性而要求研發方付出更多的努力。這樣，就不需要增加過多的費用或時間的投入。EAL2 適用於在缺乏現成可用的研發記錄時，需要一種低或中等級別的獨立保證的安全性。在保護傳統系統的安全或者限制對研發者的訪問時，會有這樣的情況。
3. EAL3：系統地測試和檢查，可使一個盡責的研發者，在設計階段能從有效的安全工程中獲得最大限度的保證，而不需要對現有的合理的研發實踐作大規模的改變。EAL3 適用於需要一個中等級別的獨立保證的安全性之使用環境。
4. EAL4：系統地設計、測試和覆查，可使研發者從有效的安全工程中獲得最大限度的保證，這種安全工程基於良好的商業研發實踐，這種實踐雖然很嚴格但並不需要大量專業知識、技巧和其他資源。在經濟合理的條件下，對一個已經存在的生產線進行翻新時，EAL4 是所能達到的最高等級。EAL4 適用於對常規產品需要一個中等到高等級別的獨立保證的安全性之使用環境，還適用於研發者或用戶準備負擔額外的安全專用工程費用的情況。
5. EAL5：半正規化設計和測試，可使一個研發者從系統安全工程中獲得最大限度的保證，這種安全工程基於嚴格的商業研發實踐，是靠適度應用專業安全工程技術來支持的。EAL5 適用於在有規劃的研發中需要高級別的獨立保證的安全性之使用環境，此時還需要有嚴格的研發方法。

6. EAL6：半正規化查證的設計和測試，可使研發者通過把安全工程技術應用於嚴格的研發環境，而獲得高度的保證，以便保護高價值的資訊資產，對抗重大風險，EAL6 適用於高風險之使用環境。
7. EAL7：正規化查證的設計和測試，適用於在風險非常高的地方和/或有高價值資訊資產進而值得更高級之研究的地方。EAL7 的實際上只局限於那些非常關注能經受廣泛的正規化分析並修正安全功能的產品。

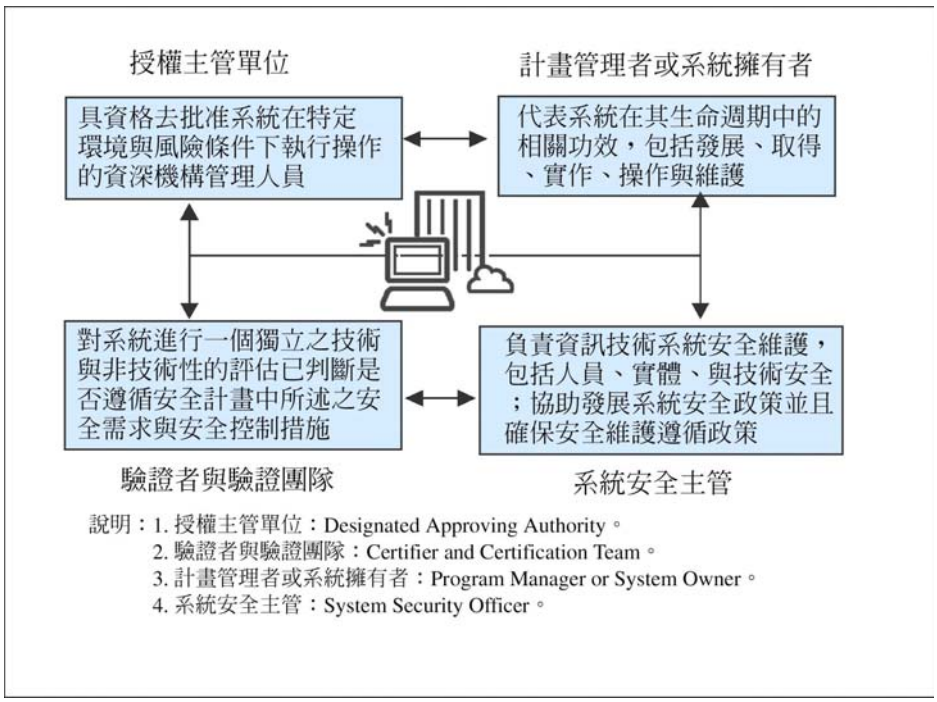
評估保證等級即是資訊技術安全驗證（Certification）機制中如圖八所示之符合性申明，至於圖八中之資訊安全目標等之關連，請參見圖九。在圖八中，我們可以清楚的瞭解保護剖繪的重要性，唯目錄服務之保護剖繪尚爲草案[18]；在此，我們僅將目錄服務，甚至所有資訊系統幾均需面對之使用者識別與鑑別問題中符記保護剖繪中之威脅整理如表五所示，僅供讀者參考，更進一步的資訊可以參閱參考文獻[19]。除了共同準則規範產品與系統之安全度外，在管理方面；作者尚未找到目錄管理資訊安全稽核方面的資料，僅以美國財政部針對電子銀行業務(註：類似目錄服務業務)之稽核規範[20]中國內較不注意的安全程式整理成表六，其他部分則列爲本文附錄供有興趣人士參考。本節之最後，謹以美國聯邦政府資訊技術系統安全保證驗證與認證過程計畫已公布之過程與主要參與角色分別整理如表七以及圖十所示並代爲本節結論。



圖八 符合性申明示意說明



圖九 資訊安全目標及需求關係示意



圖十 美國聯邦政府資訊技術系統安全驗證與認證計畫中之主要參與角色

表五 資訊安全之識別與鑑別使用之符記(Token)威脅示意

符記(Token)面對的威脅(Threats)

1. 物理攻擊 (Physical Attack)	1.1 T.E_Mainip 1.2 T.P_Modify 1.3 T.P_Probe 1.4 T.Power_Clock	說明：使用電磁技術等方式破解符記(例：智慧卡)之安全防護措施
2. 邏輯攻擊 (Logical Attack)	2.1 T.Bad_Load 2.2 T.Component_Fail 2.3 T.Developer_Flawed_Code 2.4 T.Flt_Ins 2.5 T.Forced_State_Change 2.6 T.Inv_Inp 2.7 T.Spoof 2.8 T.UA_Use	說明：使用駭客技巧等方式破解符記使用系統之安全防護措施
3. 存取控制 (Access Control)	3.1 T.First_Use 3.2 T.Impers	說明：使用符記啓動流程中易疏於防範的作業方式破解符記使用系統之安全防護措施
4. 非預期的交互作用(Unanticipated Interactions)	4.1 T.App_Ftn 4.2 T.Fail_Secure 4.3 T.LC_Ftn 4.4 T.Res_Con	說明：使用需求規範外之作業方式破解符記使用系統
5. 密碼功能 (Cryptographic Functions)	5.1 T.Crypt_Attk	說明：使用密碼分析等方式破解符記使用系統中之密碼方法
6. 監視資訊 (Monitor Information)	6.1 T.I_Leak 6.2 T.Link	說明：使用監視設備(例：網路管理設備)等蒐集之資訊，破解符記使用系統
7. 其他 (Miscellaneous)	7.1 T.Clon 7.2 T.Env_Strs 7.3 T.Lnk_Att 7.4 T.Rep_Atk	說明：不屬於前述 6 類之諸如使用相容但暗藏木馬之組件替換符記使用系統中之組件等方式，破解符記使用系統

資料來源：Hamilton, B.A. (2002) Department of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile(Medium Robustness), NSA(National Security Agency)。

表六 安全的程式稽核例

稽核項目	風險所在	稽核方法
確定開發者對於安全的程式技術是否有接受完善的訓練	程式撰寫員如果沒有接受適當的訓練，可能無意識的暴露出應用軟體的安全漏洞	驗證所有的程式撰寫員對於安全的程式技術，都有接受過完整的訓練
確定客製化程式(custom scripts)是如何分析使用者的輸入資訊	程式如果不能分析使用者的輸入資訊，可能經常遭受到惡意入侵者從遠端執行命令的攻擊	所有處理使用者輸入資訊的程式碼必須經過仔細的過濾
確定客製化程式是如何分析使用者獲得的輸出資訊	程式如果不能分析使用者獲得的輸出資訊，可能會遭受到惡意入侵者獲取無權檢索的資訊	所有處理使用者獲得輸出資訊的程式碼應有輸出資料驗證的規則
確定客製化程式是否使用暫存檔	• 使用者可能在應用程式執行前先產生假的檔案來破壞使用暫存檔之 CGI 程式 • 存在不被保護目錄的暫存檔，可能被惡意的入侵者利用其內含之敏感性資訊	• 驗證所有使用暫存檔的程式是否能在安全的目錄下隨機的產生檔案名稱 • 驗證所有程式在讀寫檔前能核對檔案是否存在
確定在回應客戶端需求，其程式是讀檔或是寫檔	根據使用者提供的資訊來存取檔案是一種不良程式設計，可能因遭受到破壞而允許惡意的入侵者存取任何檔案	• 核對所有的檔案名稱被定義在主機端且沒有嵌入 HTML 中 • 核對程式謹慎處理上一層目錄的存取(../)
確定在伺服器上儲存敏感資訊的應用服務程式	惡意的入侵者透過受攻擊的網站服務得到系統存取權限，可能再更進一步獲得安全傳輸資訊的存取權限	核對所有的敏感資訊均存放在受保護的檔案中或安全的遠端系統
確定在網頁服務執行程式的權限	具高權限且易遭受攻擊的程式，可能導致惡意入侵者擁有更大的權限	• 核對以 SUID 權限 (UNIX) 執行的程式 • 核對非網頁服務使用者有權限執行的程式

表七 美國聯邦政府資訊技術系統安全驗證與認證過程

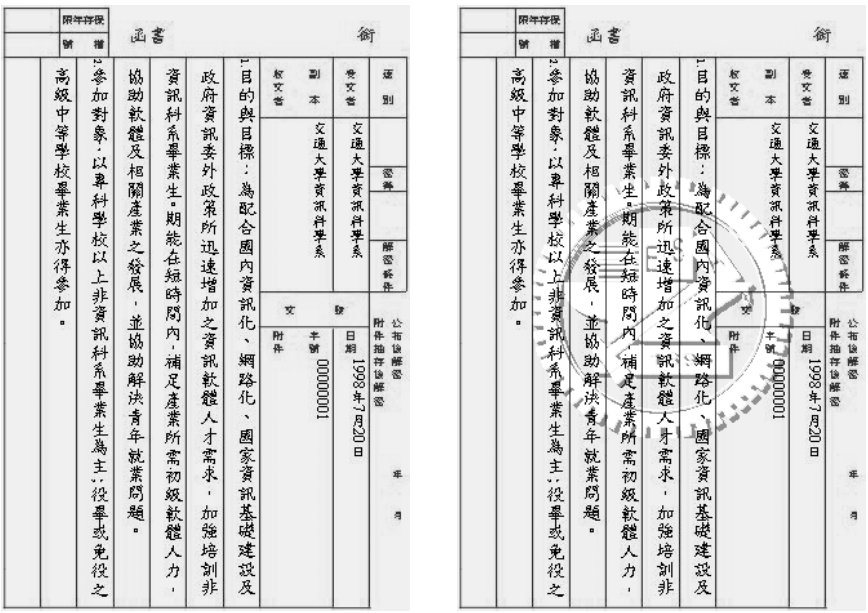
1. 驗證預評階段： 1.1 系統識別。 1.2 範疇決定與啓始式。 1.3 安全計畫確認。 1.4 安全控制措施確認與識別。 1.5 協商。 2. 驗證階段： 2.1 查證程序精細化。 2.2 安全測試與評估。 3. 認證階段： 3.1 風險評鑑總考。 3.2 安全計畫修正以切合實際狀況。 3.3 驗證發現。 3.4 認證決策。 4. 後認證階段： 4.1 修正風險評鑑以切合實際狀況。 4.2 全面複核之認證作業。 4.3 系統處理。

伍、結論

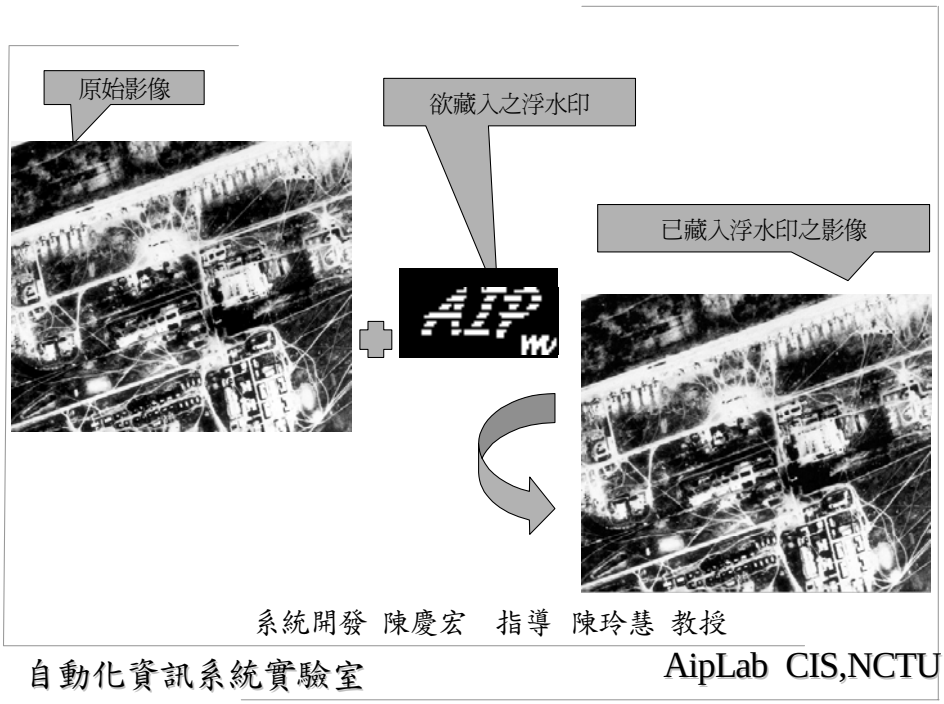
長久以來，因 OID 中國家(Country)代碼之爭議，目錄服務在我國僅少數單位研究、使用中，前述爭議在行政院主管單位之要求下，由經濟部標準檢驗局在 2002 年 12 月 31 日前頒布 OID 之註冊程序等國家標準與修定相關國家標準後告一段落；換言之，自 2004 年起，將有 OID 登錄、管理之主責機構，目錄服務在我國之普及已是指日可待之預期中事。根基於此，本文研析並提出物件識別符與目錄服

務在檔案立案、編目及其數位社會檔案檢索角色基存取控制方面的可能應用；在另一方面，數位典藏之影像、聲音等非文字檔案之安全性涉及如圖十一、圖十二、圖十三、圖十四及圖十五所示之資訊僞裝學與數位浮水印技術，本文並未探討，此方面技術在檔案管理上之使用是值得注意的發展[21]。

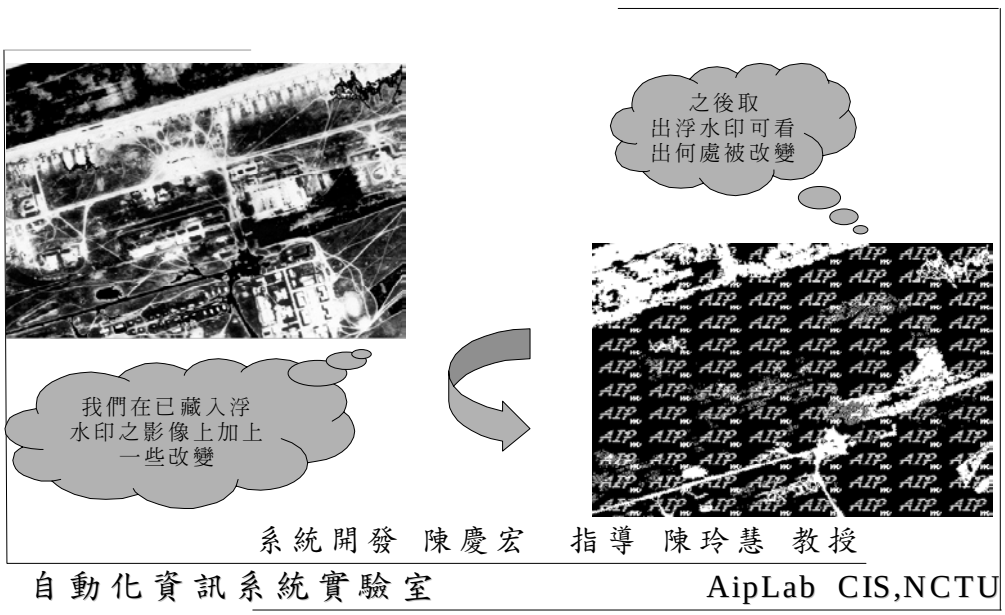
圖十一 彩色可視數位浮水印



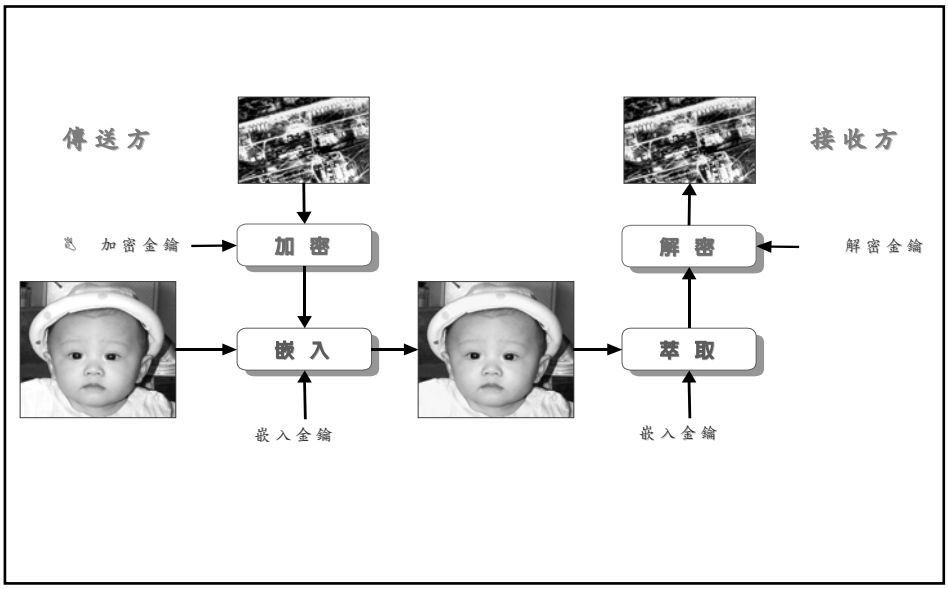
圖十二 二進制(Binary) 可視數位浮水印



圖十三 影像驗證系統(不可視數位浮水印之應用)之一



圖十四 影像驗證系統(不可視數位浮水印之應用)之二



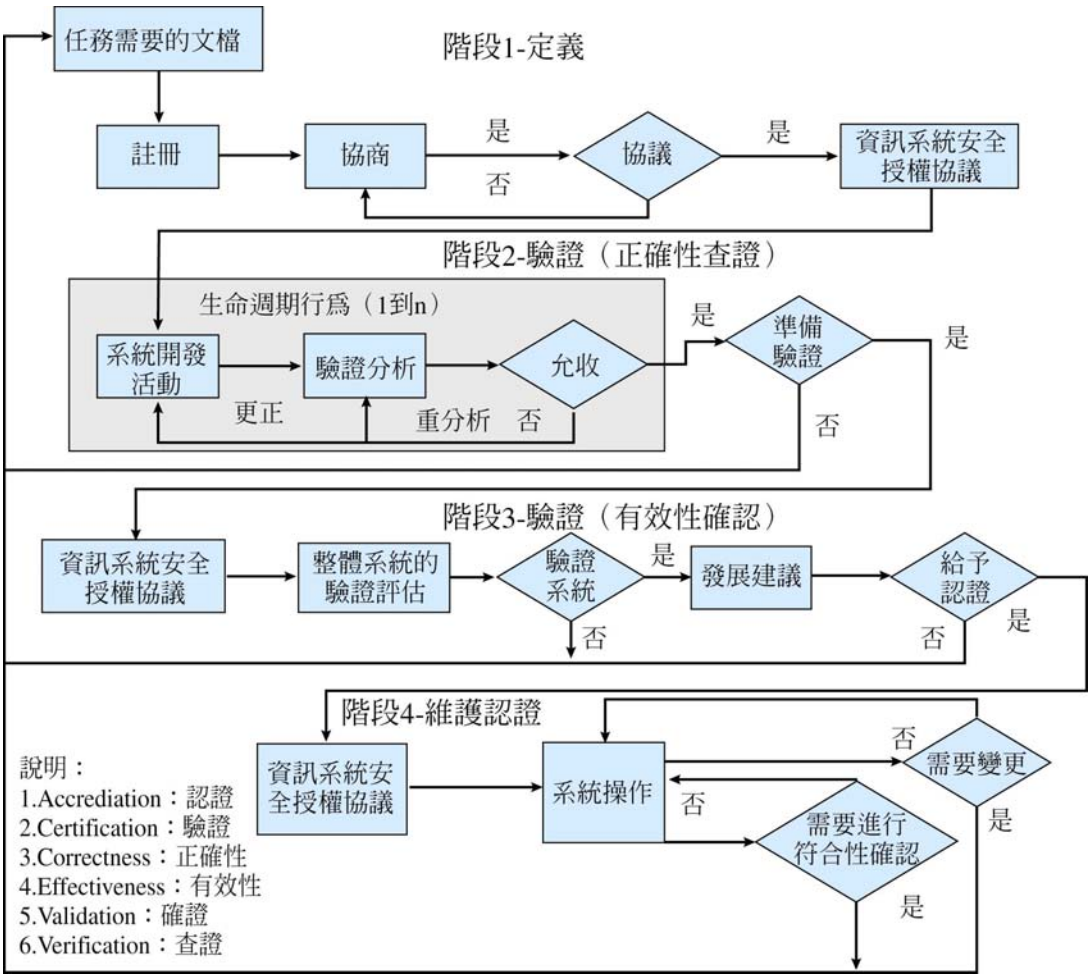
圖十五 影像資訊僞裝系統(Image Steganographic System)

保護資訊資產之安全，已成爲當今數位空間的共識，亦爲民主法制國家、社會與人民必備之素養。然而，人性本非全然良善，監守自盜損害資訊資產、木馬藏兵入侵資訊系統等事件，所在多有；如何確保：「在資訊之處理作業中，經由確認資訊與資訊系統可用性、完整性、鑑別性、機密性及不可否認性來保護、偵測以及反應能量以提供資訊系統損害後的復原」的資訊保證標的之達成已成爲數位空間安全的基礎建設之礎石。本文探討之資訊技術安全評估共同準則已是資訊保證之基石，至於角色基存取控制之標準已在制定中[22]，有興趣的讀者可以自行參考。

美國自 2000 年起，正式開始評鑑資訊安全評鑑工作，並規劃確實可行之驗證與認證（Certification and Accreditation，簡稱 C&A）過程方法，預定於 2005 年在聯邦政府正式實施。美國 C&A 過程計畫已提出了資訊安全管理系統稽核作業中，IT 系統驗證與認證實作及評鑑之框架，C&A 過程計畫根基於威脅與資產之分類與分級。表八與圖十六分是 C&A 計畫中潛在影響之分級定義[23]及作業過程[24]，C&A 計畫的評鑑準則已成爲 ISO 據以制定運行中資訊系統安全評鑑國際標準的重要參考資料[25~27]。

表八　安全目標的潛在影響定義

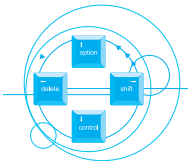
	潛在影響		
安全目標	低度	中度	高度
機密性 保存對資訊存取與公開經授權的限制，包括保護個人隱私及私有資訊。	未經授權的資訊公開可能會對組織營運、組織資產或個人有有限的有害效果。	未經授權的資訊公開可能會對組織營運、組織資產或個人有嚴重的有害效果。	未經授權的資訊公開可能會對組織營運、組織資產或個人有劇烈的或災難性的有害效果。
完整性 保衛資訊不被不適當的修改或破壞，包括確保資訊的不被拒絕與可信賴性。	未經授權的資訊修改或破壞可能會對組織營運、組織資產或個人有有限的有害效果。	未經授權的資訊修改或破壞可能會對組織營運、組織資產或個人有嚴重的有害效果。	未經授權的資訊修改或破壞可能會對組織營運、組織資產或個人有劇烈的或災難性的有害效果。
可用性 確保及時與可信賴的資訊存取與使用。	資訊或資訊系統的存取或使用遭到瓦解可能會對組織營運、組織資產或個人有有限的有害效果。	資訊或資訊系統的存取或使用遭到瓦解可能會對組織營運、組織資產或個人有嚴重的有害效果。	資訊或資訊系統的存取或使用遭到瓦解可能會對組織營運、組織資產或個人有劇烈的或災難性的有害效果。



圖十六 美國國家資訊安全保證驗證與認證作業

檔案管理目錄服務之標的在於：「從確保資訊資源的合法存取，到在所有可能遭受資訊攻擊之階段，提供完整、未中斷的資訊系統運行」。我國開始關心檔案管理目錄服務作業，時間爲短、經驗的累積不多，許多應建立的價值、觀念與制度，大家都還在摸索之中。在這樣的環境下，如何因應我國民生息息相關之資訊基礎建設的檔案管理目錄服務作業之議題，實應展開更深入的思考及討論。身爲數位時代之一員，我們不要辜負了這個全民參與建立資訊社會安全典範的機會。本文之淺見，是我們對檔案管理目錄服務作業繳出的一份學習報告，尚望先進宏達不吝指正。

【原刊載於檔案管理局出版之檔案季刊（九十二年三月）第二卷第一期】



誌謝詞：

本文作者在此對國立交通大學資訊科學系所自動化資訊系統實驗室陳玲慧教授概允使用圖十一~圖十五等數位浮水印圖檔暨國立交通大學資訊管理研究所方仁威同學蒐集資料之協助，謹申謝忱！

參考資料：

[1] 行政院研究發展考核委員會，檔案法草案制度過程資料彙編，行政院研究發展考核委員會，民國 86 年。

[2] 郭介恒，檔案管理法制之建構，檔案季刊，創刊號，頁 6~14，檔案管理局檔案季刊社，民國 90 年。

[3] 薛理桂，推廣檔案應用服務的途徑，檔案季刊，創刊號，頁 15~22，檔案管理局檔案季刊社，民國 90 年。

[4] 林秋燕，全國檔案資訊系統之規劃，檔案季刊，創刊號，頁 23~31，檔案管理局檔案季刊社，民國 91 年。

[5] 林秋燕，建立我國檔案標準化作業，檔案季刊，第一卷，第一期，頁 10~19，檔案管理局檔案季刊社，民國 91 年。

[6] 陳昭珍，國家檔案數位典藏面臨的挑戰與發展方向，檔案季刊，第一卷，第一期，頁 61~68，檔案管理局檔案季刊社，民國 91 年。

[7] 李超良、潘彥谷與洪進福，LDAP View： Web-Based 目錄伺服器管理系統之設計與開發，電信研究雙月刊，第 32 卷第 2 期，頁 137~172，民國 91 年。

[8] ISO ISO/IEC 9594：Information Technology － Open Systems Interconnection － The Directory (All parts), ISO (1995) 。

[9] ISO ISO/IEC 9834：Information Technology － Open Systems Interconnection － Procedures for the Operation of OSI Registration Authorities (All parts), ISO

(1998)。

[10] 樊國楨，資訊技術－ 開放系統互連－ 物件識別符的註冊程序(草案)，經濟部標準檢驗局，民國 91 年。

[11] 張玉華，邁向檔案管理制度化的基石－ 檔案立案與編目，檔案季刊，第一卷，第一期，頁 20~28，檔案管理局檔案季刊社，民國 91 年。

[12] Mclean, I. Windows 200 Security Little Black Book, The Coriolis Group LLC(2001)。

[13] 黃明祥，電子檔案儲存安全之認證研究，RDEC-NA-090-001，檔案管理局籌備處，民國 90 年。

[14] 賴威伸，設計以角色爲基礎之存取控制於目錄服務與公開金鑰基礎架構，國立交通大學資訊工程系博士論文，民國 91 年 6 月。

[15] http://www.oasisopen.org/committees/security/#documents。

[16] http://www.iatf.net。

[17] ISO Information technology－ Security techniques－ Evaluation criteria for IT security (All parts), ISO/IEC 15408：1999(E), ISO。

[18] Galitzer, S. et al. Directory for US Department of Defense Class 4 PKI Protection Profile, Strawman Draft Version 0.2, 2002。

[19] 樊國楨、陳祥輝、蔡敦仁，資料庫濫用軌跡塑模，政府機關資訊通報，第 160 期，頁 12~21，民國 90 年。

[20] 紀慧敏（2000）美國金融業電子銀行業務之網路架構安全控管及稽核方式之研究，中央存款保險股份有限公司(出國報告)，民國 89 年。

[21] Noda, H., E. Kawaguchi and K. Imamura eds. (2002)Proceedings of Pacific Rim Workshop on Digital Steganography 2002, Kyushu Institute of Technology, Kitakyushu, Japan。

[22] Ferraiolo, D.F. etal. Role-Based Access Control, Artech House(2003).

[23] NIST Standards for Security Categorization of Federal Information and Information Systems, PUB (Publication) 199, NIST(2003)。

[24] Ross, R. and M. Swanson (2004) Guidelines for the Security Certification and Accreditation of Federal Information Technology System, NIST Special Publication 800-37, May 2004, NIST。

[25] Katzke, S. (2003) Protection Federal Information System and Network, in Presentation of the 4th International Common Criteria Conference, September 7~9, 2003, Stockholm, Sweden。

[26] ISO/IEC JTC1/SC27 (2004) Information technology-Security techniques-Security assessment of operational systems, ISO/IEC 19791, ISO/IEC JTC1/SC27 N4001。

[27] Tabuchi, H. (2004) Security Assessment of Operational Systems, in Presentation of the 5th International Common Criteria Conference, September 28~30, Berlin, Germany。

附錄：網站伺服器之稽核

網站（Web Site）是數位化目錄服務的窗口，近年來，國內外知名機構網站首頁被竄改，甚至成爲駭客攻擊它人跳板之新聞時有所聞[註 22]；基於網站安全在推動數位化服務的重要性，美國聯邦存款保險公司於 1997 年 1 月公布包含：

1. 網頁服務內容及位址（Web service content and location）。
2. 網站伺服器的軟硬體配備及其功能（Web server configuration and functionality）。
3. 安全的網站伺服器（Secure web servers）。
4. 存取控制及帳戶資料庫（Access control and account databases）。
5. 網站伺服器的執行效率及安全管制記錄（Web server performance and logging）。
6. 網站伺服器與後端程式之整合性（Integration of the server with back end scripts）。
7. 安全的程式（Secure Programming）。
8. 網站伺服器的安全管理（Administration server setup）。

八項內容之網站稽核檢查清單（Web Site Audit Checklist）作爲稽核人員檢查作業的指導綱要，其中的第 7 項「安全的程式」已整理於文中之表六，另 7 項分述於后[註 20]：

1. 網頁服務內容及位址稽核例

爲控制經由網站服務（Web service）、企業內部網路（Intranet）及企業間網路（Extranet）之分散資訊，必須先了解（1）資訊可能被取得的管道，（2）網路環境、主機、服務通訊埠碼（Service port numbers）、網頁服務及內容的主要目錄等之位址。

稽核項目	風險所在	稽核方法
確定在網路上的所有網站伺服器	所有網站伺服器必須能被辨識，且被控制在最小風險的狀況下	• 由網路管理者取得最新的網路架構圖及網域名稱伺服器（DNS；Domain Name Server）資訊。 • 檢測網站資訊服務是設定在通訊埠碼（Port No）21,80,81,443,8000,8080。
確定網頁服務之通訊埠碼是否設定在內定值 80 以外的號碼	• 由於防火牆及過濾封包路由器的環境設定，造成客戶端可能無法取得網頁資訊。 • 網站伺服器之通訊埠碼如果設定值大於 1023 可能會遭受到癱瘓主機系統（Denial of Service）型態的攻擊。	• 必須定義對外提供服務之網站僅限使用內定值通訊埠碼的策略。 • 使用 UNIX 作業系統者，必須限制網頁服務設定在可信賴之通訊埠碼
確定網頁內容是否儲存在有存取控管且能防止被竄改之檔案系統（File System）中	如果網頁內容不是儲存在有存取控管之檔案系統中，將有遭入侵者竄改內容之風險。	• 確認所有網頁內容都被儲存在具備存取控管之檔案系統中（NTFS 在 Windows Systems） • 驗證一般使用者是沒有網頁內容寫入的權利，除非有特殊狀況

稽核項目	風險所在	稽核方法
確定網頁內容是否儲存在本機或網路檔案系統中	網頁內容可能遭受到檔案分享協定（File sharing protocol ）方式之攻擊	確定所有靜態內容是由網站伺服器主機提供服務的
網站伺服器主機是否提供多個網站服務	在相同硬體主機上會因提供多個網站服務而增加其網頁間互動的風險（例：透過 CGI 程式）	• 確認不同之網站內容具備定義不同的環境參數檔以達到有效的區隔 • 確認每一個網站伺服器之使用者名稱及群組是分開的
檢查所有轉接內容（Redirect content）	入侵者轉接客戶端的需求到僞裝的網站	確認所有客戶端的需求能轉接到合法位址
確定網站伺服器是否支援目錄瀏覽（Directory browsing）	如果目錄瀏覽是許可的，入侵者將有機會了解很多網頁提供之應用系統及舊版本的內容	驗證目錄瀏覽是不許可的，尤其是含有可執行程式之目錄（例如：CGI-BIN 目錄）
確定網站伺服器是否支援符號連結（Symbolic links）	惡意的入侵者可以建立符號連結至檔案系統中較敏感的部份	驗證符號連結是不許可的，或者符號連結沒有導引客戶端至超出網頁內容範圍的位址
在新的版本刊登前，容許網頁作者建置在測試系統上	對於網頁作者如沒有管制其網站伺服器寫入權限，將是網頁服務完整性及安全性之一大挑戰	• 只容許網站站長在正式網站上更新網頁內容 • 確認開發環境是爲一般使用者無法存取的 • 確認有一套適當的網頁變更控制程序
確定具備有上傳新的網頁內容至正式網站的移轉機制	開啓檔案分享協定（File sharing protocol ）將增加網站遭受非法存取的風險	• 確認由網站站長移轉網頁內容至正式網站有一套安全的程序 • 儘量減少使用檔案分享協定

稽核項目	風險所在	稽核方法
確定存在有防止網頁作者非法變更其他作者網頁內容的控管權限	對於有多個網頁作者的網站，如果存取控管權限設定不適當，將招致非法竄改的風險	確認在開發環境中，對於新的網頁內容具備存取控管的權限
確定開發者使用憑證簽署 Java、Javascript 、Active X	惡意使用者若有金鑰的存取權可能僞造產生 Controls 或 Applets	• 確認金鑰的存取權是受到管制的 • 確定開發者不能以組織的金鑰產生個人的 Controls
檢查網站的舊版本	• 入侵者可能置放非法的內容於網站上 • 客戶端可能看到舊內容	利用網站稽核工具，以檢查 所有超文件連結是有有效的 2.沒有孤兒檔案（檔案沒有被連結）

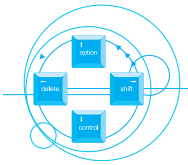
2. 網站伺服器的軟硬體配備及其功能稽核例

因不良的網頁服務安裝及環境設定將遭到入侵者以各種不同的探索方式闖入，必須要能確定（1）所有網站安裝最適當的服務項目且設定正確的環境參數值，（2）網站站長能充份了解網頁服務的特性及受到新的安全威脅時，具備及時修護的能力。

稽核項目	風險所在	稽核方法
確定網站伺服器的程式修補歷程	• 網站伺服器新的程式錯誤，將導致非法的遠端存取 • 錯誤沒有被修補的系統，將導致持續的被攻擊	• 確認網站管理員能提供證明顯示伺服器已被修補至最新版。 • 與廠商核對尚未解決之程式錯誤 • 檢查網站站長收到來自廠商的安全警告通知

稽核項目	風險所在	稽核方法
檢查網站站者擁有一份所有執行檔的清單	入侵者很容易操控具備所有功能的系統	• 確認只安裝有需要的執行碼及應用系統 • 驗證網站管理長能說明安裝在伺服器所有的模組、執行檔、程式及程式館
檢查程式碼已從正式的網站中移除	• 網路管理員繞過測試程序而以原始程式碼安裝在網站伺服器 • 駭客可能利用編譯程式而置入非法執行檔於網站中 • 客製化的程式碼（Custom written code）可能被非法使用者檢視及利用	確認所有的原始程式碼已從正式的網站中移除
檢查網站服務的使用帳號	遠端使用者的非法存取將導致特權存在	• 確認匿名者存取是一個沒有特權的帳號 • 確認網頁服務帳號是沒有與其他服務或使用者共用的
網站站長是否以可被充份稽核的唯一帳號簽入	如果管理工作以共用的帳號執行或者是以無法被充份稽核的帳號執行，非法的網頁服務設定檔就無法被檢測出。	• 確認網站管理長是以一個特殊帳號簽入以執行網站管理工作 • 確認網站站長帳號是可被稽核的，且稽核記錄須定期審核

稽核項目	風險所在	稽核方法
確定網站伺服器環境設定檔之位址	入侵者可能竄改環境設定檔之內容	• 確認網站站長能正確的辨識所有的環境設定檔及資料庫 • 驗證舊版的環境設定檔已從網站伺服器移除
確定那些使用者可檢視及變更環境設定檔之內容	• 非法使用者可能變更環境設定檔以釋放安全控管權限 • 非法使用者可能有能力檢視網站伺服器之環境設定檔並窺探系統安全漏洞	• 確認環境設定檔僅能由授權的使用者及群組變更
檢測網頁服務都有對應一個特定的 IP 位址，或有一組 IP 位址(在 Windows NT)	NT 系統的網路服務其所對應 IP 位址爲 0.0.0.0，則可能遭受到使用者置換服務項目的風險	在 Windows NT 網路服務的環境設定給予一個非內定值 0.0.0.0 的 IP
確定網頁上所有可供存取之應用服務項目	網頁開發者可能無意識的透過網頁介面提供網路服務，除非在防火牆有阻隔	確認在網頁上提供的應用服務項目被很謹慎的控制在洩露給非法的使用者最少量的情況下
確定遠端使用者可以透過 FTP 服務存取網頁資訊	• 即使已設定存取控管規則（ACL；Access control list）保護網頁，使用者仍可能透過 FTP 服務來存取網頁內容 • 使用者可能利用 FTP 來瀏覽在網頁服務禁止使用之目錄	確認網頁與 FTP 路徑是分開的



稽核項目	風險所在	稽核方法
辨識傳送儲存敏感資訊的 Cookie 至客戶端的應用服務項目	• 惡意的使用者可能截取在 Cookie 內敏感資訊的封包 • 即使採用安全機制傳送 Cookie 到客戶端，仍有可能遭致蓄意的 Java，Javascript.或 Active X 程式的破壞	• 確認非敏感資訊沒用使用加密傳輸 • 確認 Cookie 僅能被傳回原主機端 • 確認 SAVE_COOKIE 是用來防止在不安全的狀況下傳輸敏感資訊
辨識傳送儲存敏感性資訊的 HIDDEN INPUT 標籤至客戶端的應用服務項目	惡意的使用者可能收集會利用到使用者表格資訊的後端程式，再以之攻擊網站伺服器	• 確認在客戶端網頁的隱藏資訊不直接傳回主機端程式 • 確認敏感性的主機端資訊（如客戶名稱、檔案路徑等）不要放在 HIDDEN INPUT 內
檢查依賴客戶端 JavaScript 程式來過濾使用者所提供資料的應用服務項目	• 惡意的使用者可以繞過客戶端的驗證路經，直接傳遞表格資訊至程式中 • 使用者可能將瀏覽器的 Javascript 關閉	• 確認除了在客戶端以 Javascript 過濾使用者提供的資料外，主機端程式亦得過濾使用者提供的資料
網站伺服器是否支援 HTTP PUT 及 DELETE	如果允許使用 PUT and DELETE，惡意的使用者可以輕易修改網頁內容	• 確認網站伺服器僅支援 HTTP GET 及 POST • 如果必須開放 PUT 及（或）DELETE 時，則確認只能提供給認證且授權的使用者個人

3. 安全的網站伺服器稽核例

敏感的應用服務領域如電子商務或企業間網路環境，需要安全的網站伺服器；網頁服務的完整性對於迎得顧客的信任及服務的持續性是非常關鍵性的。

稽核項目	風險所在	稽核方法
確定網站伺服器是否支援 SSL	任何必須傳送或接收敏感性資訊之網站，應該使用加密機制	檢核伺服器之設定或網路狀態清單上之 Port No.（通常是設定在 443）
確定私密金鑰是加密存在磁片上	私密金鑰應該完善的保護，以免駭客盜取	驗證當網站伺服器重新啓動時，網站管理者被要求輸入 Key 值
確定負責安裝、啓動及維護 SSL key 的使用者及君組	• 私密金鑰之存取必須被控管好，以防止內部使用者拷貝 • 主機端金鑰必須備份，以確定當網站管理者遺失金鑰、離開公司或其他理由時能繼續提供服務	• 與網站站長核對擁有私密金鑰的使用者名單 • 確認金鑰被安全的保存在磁片、紙張等

4. 存取控制及帳戶資料庫稽核例

網站伺服器必須允許網站管理者有權保護網頁內容杜絕非法使用；每一網站伺服器均能利用不同的技術來控制存取權限，而了解伺服器如何利用存取控管權限（Access Control List）資訊防止非法入侵及網頁內容遭到竄改是相當重要的。

稽核項目	風險所在	稽核方法
確定如何控管網頁內容	如果採用不適當的存取控管規則或管理者不了解如何應用存取控管規則，將引發駭客存取機密性資訊	• 非法使用者可能以假冒 IP 方式，讀取網頁內容 • 非法使用者可能以網路監聽方式竄取密碼後，存取網頁內容 • 確認不明確的安全機制不能用來控管網頁內容存取權限

稽核項目	風險所在	稽核方法
確定網站伺服器如何解讀存取控制規則	了解網站伺服器如何解讀存取控制規則將可確保網站安全	確定初始設定值爲拒絕存取 確定如何處理存取控制規則： 1.第一次先停止使用 2.處理所有存取控制規則及累積權利 3.處理所有存取控制規則及最少的權利 4.以 IP 基準之存取控制規則能與使用者之存取控制規則合併 5.以其他方式處理存取控制規則
檢查所有網站內容之 ACL	不良的目錄 ACL 設定，將導致非法使用者存取網頁內容	確定 ACL 符合書面上的規則
確定帳戶資料庫的位址	• 帳戶資料庫必須被完善的保護，以確保密碼不會被偷取 • 支援目錄 ACL 的網站伺服器可能因使用多個帳戶資料庫而造成控管上的困擾	• 確定帳戶資訊存在控管的資料庫中 • 確認每一目錄 ACL 不使用本機端資料庫

5. 網站伺服器的執行效率及安全管制記錄稽核例

在電子商務環境中的網頁服務執行效率及持續性是很重要的；而高水準的服務則有賴對於系統之安全管制記錄檔及執行效率採取即時監控的方式。

稽核項目	風險所在	稽核方法
確定有啓動網站伺服器、作業系統、CGI 程式及後端元件之安全管制記錄功能（logging）	沒有啓動安全管制記錄功能，非法的活動或試圖闖入網頁之情事均無法得知	• 確認具備網頁服務的安全管制記錄及行政管理活動安全管制記錄，如停止或啓動服務 • 確認有定期審核安全管制記錄檔
確定安全管制記錄檔儲存在可防止非法使用者存取的位址	任意置放安全管制記錄檔，將導引非法存取敏感性資訊	• 檢測對於適當的操作人員，安全管制記錄檔是可閱讀的 • 檢測安全管制記錄檔的成長量不會影響其他系統活動
確定有設定警告服務以監控安全管制記錄檔	如果沒有警告訊息設備，非法的活動將無法得知	• 檢測安全管制記錄檔監控工具的或主機侵入偵測系統之有效性及設定檔，包括： 1.來自某特定客戶端不尋常的高度活動 2.高頻率的’合法訊息需求’ 3.大量的‘找不到訊息’ 4.不尋常的 CGI 程式需求
確定網站伺服器有執行效率監控	網站伺服器的執行效率應該定期監控，以確保有良好的服務品質	• 檢測網站站長正使用網站伺服器或作業系統提供之執行效率監控工具 • 檢核頻寬使用量、每秒連結數目、每秒傳輸速率、CPU 及硬碟使用量

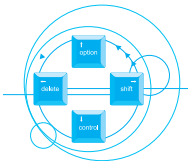
稽核項目	風險所在	稽核方法
確定有啓動網站伺服器、作業系統、CGI 程式及後端元件之安全管制記錄功能（logging）	沒有啓動安全管制記錄功能，非法的活動或試圖闖入網頁之情事均無法得知	• 確認具備網頁服務的安全管制記錄及行政管理活動安全管制記錄，如停止或啓動服務 • 確認有定期審核安全管制記錄檔
確定網站伺服器限制同時間連結的數目及（或）頻寬使用量	• 網站伺服器沒有限制每秒連結數，將遭致連結泛濫的攻擊 • 執行傳輸大量資料的網頁應用服務項目，將迫使無法接受	• 檢測網站伺服器的設定檔能限制同時間的連結數目 • 檢測網站伺服器、防火牆及其他設備對於應用服務之傳輸資料量到達某特定值時，能限制同時間的連結數目

6. 網站伺服器與後端程式之整合性稽核例

網路伺服器可能以各種不同的方式連結後端程式，如建立資料庫連結及撰寫 CGI 程式等，而設計不良的 CGI 程式將引來入侵者上載非授權之內容至網站伺服器上。

稽核項目	風險所在	稽核方法
辨識所有在網站伺服器與後端應用服務程式，如資料庫，間之資料流程	惡意的入侵者可能探索環境設定檔設定之弱點，而讀寫或變更儲存在後端資料庫之敏感性資訊	• 確定後端應用服務系統之使用者如何認證 • 確定網頁使用者及其他應用服務系統之使用者的存取權限 • 辨識網站伺服器及應用服務系統間之網路路徑

稽核項目	風險所在	稽核方法
辨識能簡化客戶端與後端應用服務系統間傳輸資訊之伺服器程式（Servlets）	防火牆必須能緊密控管所有外部至內部的存取	• 檢查所有伺服器端之應用服務系統的 Netstat 清單 • 驗證防火牆能完善的處理至 Servlets 的交通流量
確定網站伺服器能支援 CGI 程式	惡意的入侵者可能強制遭受破壞之 CGI 程式執行任意的程式或查看檔案	• 確認只有在必要時才能啓動 CGI 程式支援 • 確認程式開發者對於安全議題能有充份了解及訓練 • 確認所有由網頁提供之 CGI 程式示範是無效的
檢查執行程式之位址	入侵者可能獲得程式之原始碼並偵測程式之弱點	確認程式安裝在僅供執行的目錄
檢查是否在可執行區有命令列之編譯程式	命令列之編譯程式（Command line interpreter）儲放在 CGI-BIN 目錄，將允許遠端客戶執行任意命令	從 CGI-BIN 目錄清除所有命令列之編譯程式（例如：perl.exe 、cmd.exe 、sh 、ksh 、csh etc 等）
確定是否網站伺服器支援伺服端之 includes	• 惡意的入侵者可能隱藏 SSI 敘述在網頁內，導致非法的命令執行 • 網站伺服器若檢查所有網頁是否嵌入 SSI 敘述，可能會影響網頁服務的執行效率	• 確定 SSI 支援無效 • 支援 Guest Book 型態的應用服務之網站伺服器，必須從使用者提供的輸入資料中過濾所有的 HTML 標識 • 確認含 SSI 敘述之網頁有一特殊延伸檔名（如：shtml），以資與一般網頁有所區別



7. 網站伺服器的安全管理稽核例

網站管理服務必須非常謹慎小心的防護才行，許多網站伺服器允許網站管理者由遠端簽入管理網站，這是引導駭客的最佳途徑。

稽核項目	風險所在	稽核方法
核對遠端管理服務	如果管理員不能快速處理入侵者的攻擊，將導致大量的當機。在很多情況下，管理員被要求透過遠端連結解決問題	• 驗證可透過遠端連結來管理網頁服務 • 確定提供管理服務之通訊埠碼 • 驗證管理員可收到服務警訊
確定採取安全方式連結到網頁管理服務	管理員與網站服務的溝通可藉由封包監聽予以攔截非法的使者可能以癱瘓主機的方式，試圖中斷管理服務	• 確認使用加密及認證方式執行網頁管理服務 • 確定可存取管理服務之位址 • 確認防火牆之設定允許連結至所有網頁管理服務 • 檢測防火牆能防止 TCP/IP 癱瘓主機攻擊
確定有權利管理網站伺服器之使用者及群組	對於有管理服務存取權限之使用者若缺乏控管，將導致非授權之變更	核對有管理服務存取權限之使用者及群組之設定檔