論著 檔案季刊 第5卷1期（民國95年）：頁115～147。

開放源碼機敏性檔案存取控制安全技術評估初探

A Preliminary Study on Evaluating the Access Control Security Technology for OSC Sensitive/Confidential Records

樊國楨 Kwo-Jean Farn
國立交通大學資訊管理研究所兼任副教授
Associate Professor, Institute of Information Management, National Chiao-Tung University
長城安全網有限公司技術總監
Chief Technical Director of Level 5 ISMS Ltd.
e-mail : kjf@iim.nctu.edu.tw

盧公瑜 Kung-Yu Lu
中山科學研究院資訊通信研究所技士
Associate Technical Specialist, Chung-Shan Institute of Science and Technology Armaments Bureau
e-mail : Lky57@pchome.com.tw

林樹國 Shu-Kuo Lin
國立交通大學資訊管理研究所研究生
PhD Student, Institute of Information Management National Chiao-Tung University
e-mail : kuo@iim.nctu.edu.tw

摘　要

由於共同準則測試實驗室於我國已在建置中，開放源碼通過共同準則驗證提供安全性保證已是潮流之所趨。有鑑於此，本文探討根基於Linux，實作機敏性檔案角色基存取控制宜具備之安全規範。

Abstract

The testing laboratory of Common Criteria (CC) in our country is under construction; therefore, it is a current trend that Open Source Code (OSC) should pass the CC certification and provide security assurance. Based on this background, we discussed the essential security guidelines of Role-Based Access Control (RBAC) sensitive/confidential records for practical on the basis of Linux.

關鍵詞：共同準則，開放源碼，角色基存取控制，機敏性檔案
Keywords: common criteria, open source code, role-based access control, sensitive/confidential records

壹、前言

隨著資訊科技的一日千里，電腦與網路之結合已在20世紀末期，發生令人眩目之光芒，數位生活已成爲全球性的發展趨勢。政府做爲國家組成及資訊流之中心節點，在社會資訊化之進程中位居樞紐而又無可替代的作用。一般而言，電子化政府(Electronic Government)之建設，包括：

一、政府機關成員上網獲取機構內部與外部之工作所需要的資訊。

二、政府機關資訊上網，供社會大眾瞭解與使用。

三、政府機關事務，機關內、機關間、機關與公眾等事務經由網路處理。

由於「電子化政府」涉及機密性與敏感性（簡稱機敏性）資料之處理，其資訊系統如何確保機敏性資料不受未經授權之存取、使用、揭露、破解、修改與毀壞，以提供機密性、完整性和可用性的電子化政府相關資訊系統之應用，已是宜正視的問題。

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，標準的存在會提升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，鑑於沒有眞確性(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年開始制定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) CC 2.1版正式成爲ISO/IEC 15408號標準（註1），圖1是其發展簡史。換言之，在「電子化／網路化」的社會中，資訊技術的產品、系統及服務之安全測試標準將有調和一致的國際規範，開放源碼(Open Source Code，簡稱OSC)之產品亦宜通過共同準則的驗證提供安全性保證。根基於此，本文除了簡述共同準則；再分別探討根基於Linux之角色基存取控制(Role-Based Access Control，簡稱RBAC)實作及其宜遵循的保護剖繪(Protection Profile，簡稱PP)；最後提出本文之結論。

貳、共同準則簡介

CC是結合TCSEC、ITSEC與CTCPEC的優點，做爲經由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

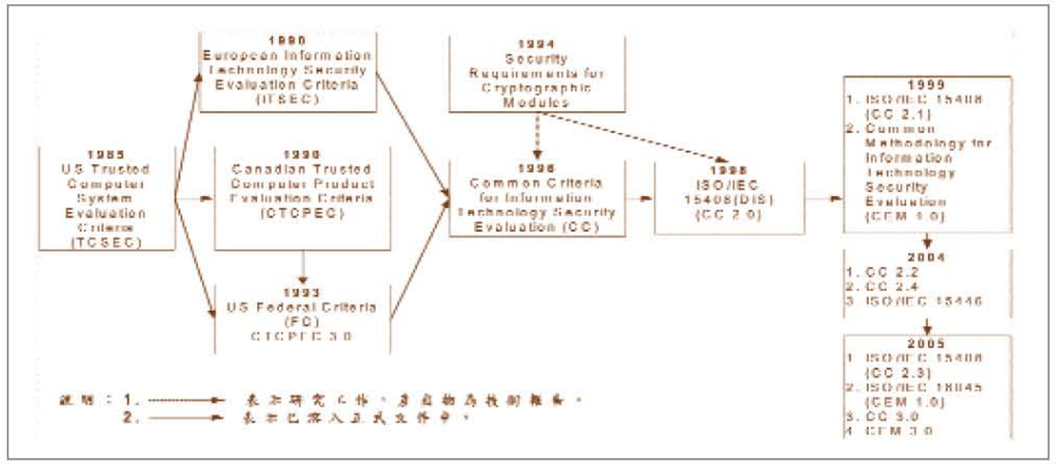


圖1 可信賴通資訊系統安全評估準則簡史

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，其使用示意請參見表1，表2是其保證評核等級檢測項目示意說明。

表1 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

表2 資訊技術安全評估保證等級摘要

保證類別 (Class)	保證屬別 (Family)	保證組件(Component)						
		評估保證等級						
		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	3	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
脆弱性評鑑	AVA_CCA					1	2	2
	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2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：

一、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。

二、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。

三、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。

四、EAL4：系統地設計、測試和複查，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。

五、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。

六、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。

七、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2所示之符合性申明，至於圖2中之資訊安全目標等之關聯，詳如圖3。在圖2中，我們可以清楚的瞭解保護剖繪的重要性。一般而言，機敏性檔案存取控制之保護剖繪之評估保證等級宜高於或等於EAL4（註2）。

共同準則之標的在進行資訊技術的安全評估，以提供信賴基礎之保障。共同準則要求加大以往資訊技術安全評估的廣度、深度與強度，來測試資訊技術產品或系統安全之有效性。PP及其ST提供使用者一個參考特定

安全需求集合的方法；如圖4與圖5所示，PP及其ST律定之安全規格，期能讓使用者對這些要求進行驗證工作時，更容易進行評估工作，表3是已確認之EAL4作業系統舉隅。以Linux爲例IBM之SuSE Linux已於2004年1月14日獲得共同準則受控存取保剖繪(Controlled Access Protection Profile，簡稱CAPP) EAL3之驗證合格證書（註3），SuSE Linux之TOE分爲TOE安全功能(TOE Security Function，簡稱TSF)與非TOE安全功能(non TSF)兩類，如圖6及圖7所示（註4）。

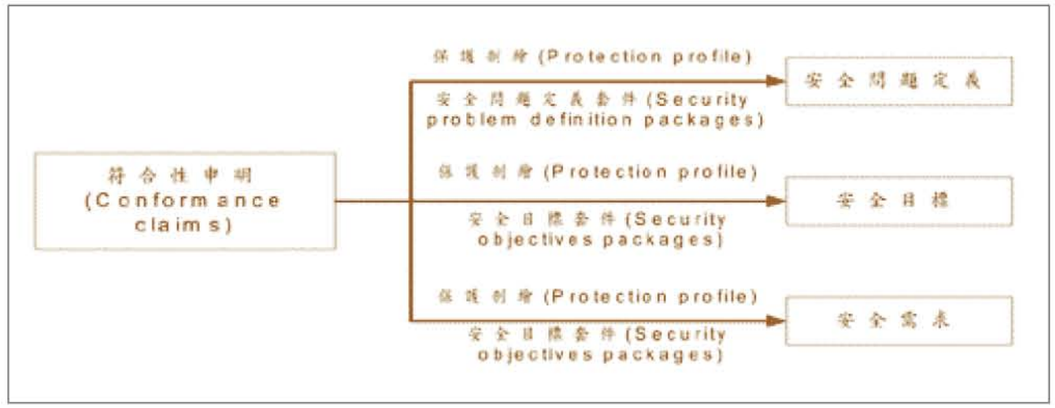


圖2 符合性申明示意說明

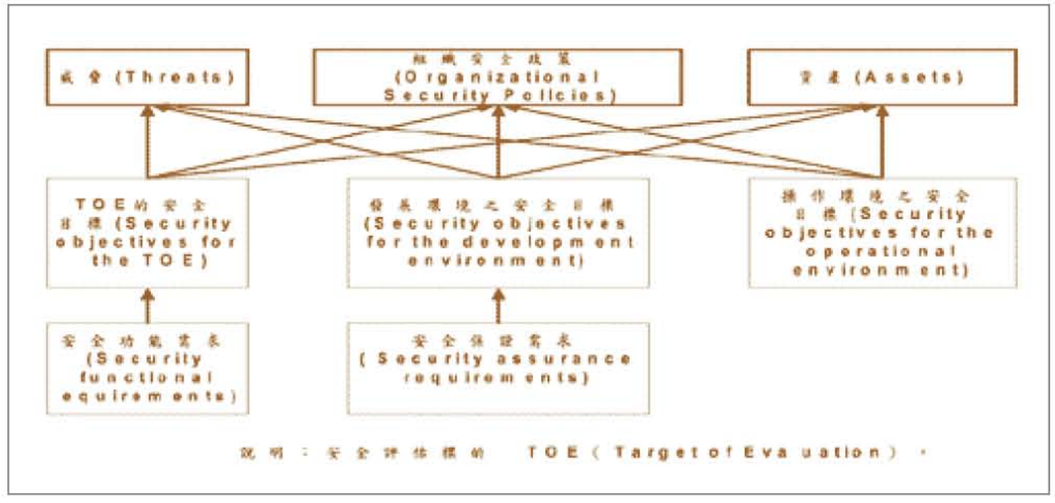


圖3 資訊安全目標及需求關係示意

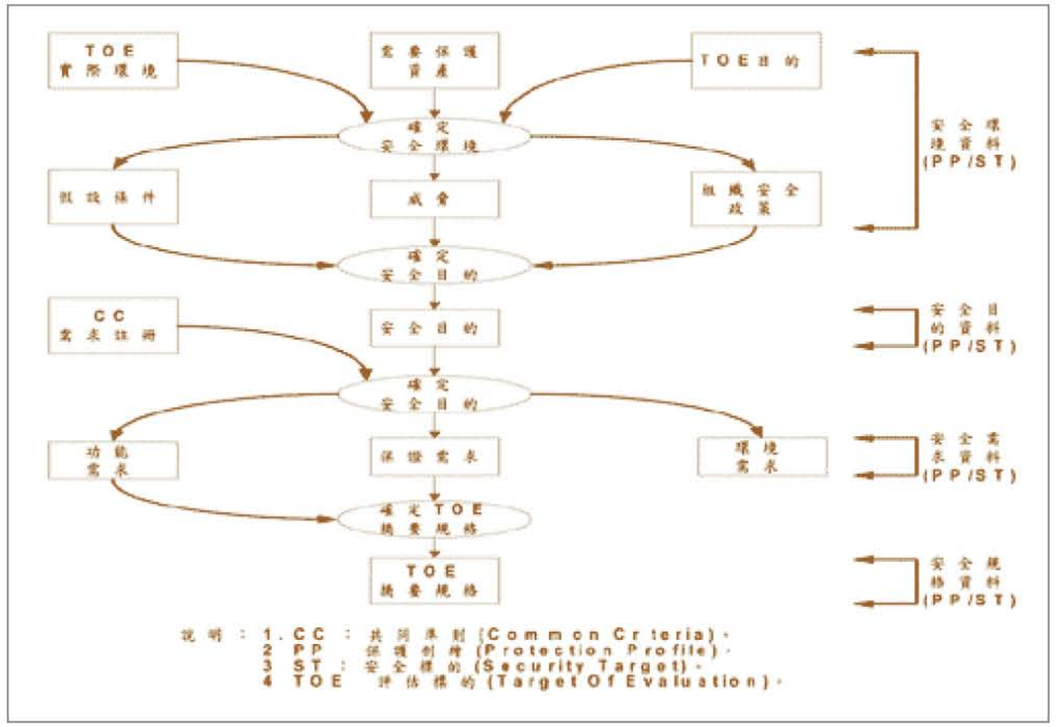


圖4 共同準則之需求和規格推導

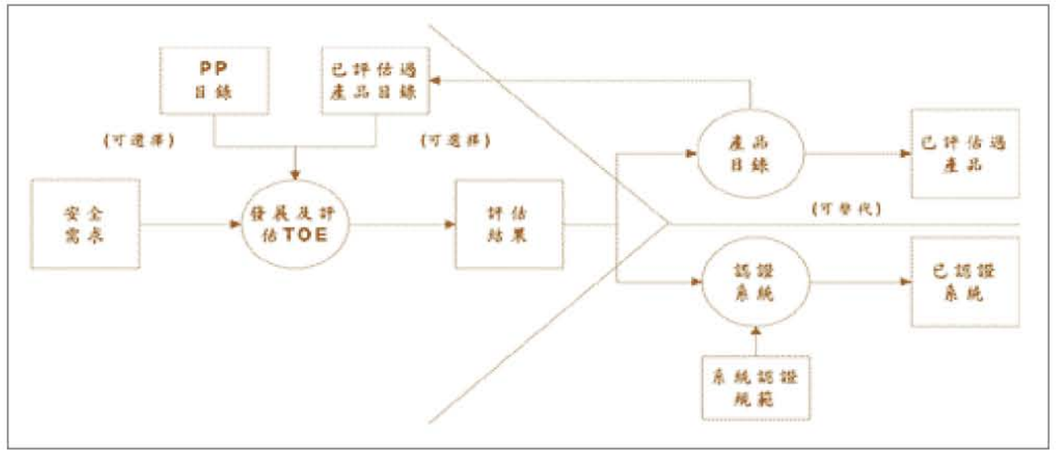


圖5 共同準則TOE評估結果的使用

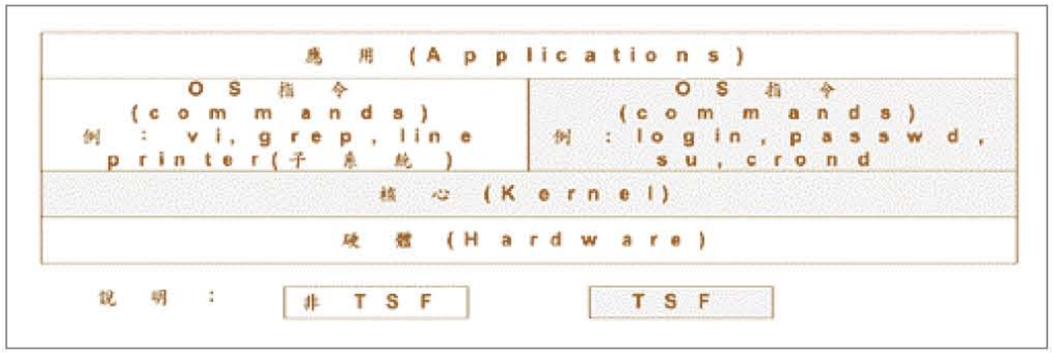


圖6 SuSE Linux TSF與非TSF軟體示意

表3 共同準則已確認(Validated)之EAL4作業系統舉隅

產品名稱	符合性宣告	確認日期	共同準則發證國家
AIX 5L for Power V5.2, Program Number 5765-E62	EAL4	2004年4月	德國
Hewlettt-Packard HP-UX(Ili) Version 11.11	EAL4	2001年9月	英國
Solaris 8 2/02	EAL4	2003年4月	英國
SUN Solaris Version 8 with Admin Suite v3.0.1	EAL4	2000年11月	英國
SUN Trusted Solaris, v8 4/01 Maintenance release Dec. 2003	EAL4	2002年6月	英國
Windows 2000 Professional Server and Advanced Server with SP3 and Q326886	EAL4 Augmented ALC_FLR.3	2002年10月	美國
XTS-400/STOP 6.0E	EAL4 Augmented ALC_FLR.3	2004年3月	美國

說明：ALC_FLR.3：Assurance Life cycle support-Systematic Flaw Remediation。

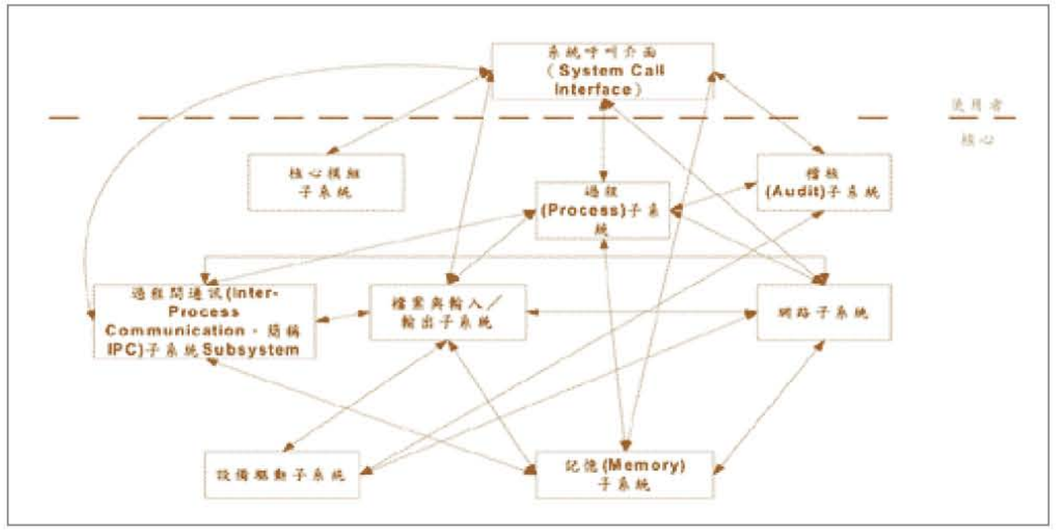


圖7 SuSE Linux核心子系統及其交互工作示意

微軟公司之Windows 2000作業系統(Windows 2000 Professional、Server and Advanced Server with Service Pack 3 (SP3) with Q326886 Hot fix)已於2002年10月18日獲得共同準則EAL4的驗證書（註5），EAL4是商用元件(Commerical Off The Shelf，簡稱COTS)安全性保證之標竿（同註1），相信Linux產品系列，亦將有EAL4之商品。

參、Linux與角色基存取控制

一、Linux介紹

一般而言，Linux核心之安全根基於過程與能力(Process and Capability)、檔案系統與封包控制之安全性，其中檔案系統及封包控制和一般常見之方法類似，過程與能力方面，簡述於后（註6）：

Linux中的使用者行爲都是藉由過程(process)來完成，一個過程通常具有以下幾個屬性：

（一）RUID，RGID：眞正用來執行過程的UID及GID。
（二）EUID，EGUID：用來做權限檢查。
（三）SUID，SGID：用來做權限轉換。
（四）umask：存取控制的設定。
（五）limits：資源使用的限制。
（六）FSUID，FSGID：用來做檔案系統存取權限的檢查，通常都會等於EUID、EGID。
（七）capabilities：POSIX capability資訊。

基於安全的考量，Linux給予一般使用者盡可能低的權限，而把全部的系統權限賦予一個單一的帳戶－root。root用來管理系統、安裝軟體、管理帳戶、執行某些服務等，但一般使用者很多的執行動作也需要root權限，此時可透過setuid來達到目的；而這種依賴單一帳戶執行權限的運作方式，卻增加了系統面臨的安全威脅，因爲某些程式需要root權限可能只是爲一個很簡單的執行

目的而已，例如：bind到特定port、打開一個只有root權限可以開啓的檔案等。但這些程式可能存在安全漏洞，若該程式不是以root的權限執行時，其存在的漏洞對系統造成的安全威脅就會降低。

從2.1版開始，核心開發人員在Linux核心中加入了能力(capability)的概念，其目的就是降低過程在執行某些動作時對root帳戶的依賴。從2.2版本的核心開始後，就可以用一些能力的基本功能。傳統UNIX的信任模型非常簡單，就是「root對一般使用者」模型。在這種模型中，一個過程不是什麼都能做，就是幾乎什麼也不能做，這取決於過程的UID。很顯然這樣對系統安全存在很大的威脅，UNIX系統中常見之的SUID的安全問題就是由這種信任狀模型造成的。

過程與能力之設定可以降低類似SUID等的安全風險，系統管理員爲了系統的安全可以刪減root的能力，這樣即使是root也無法進行某些執行動作。而這個過程又是不可逆的，也就是說如果一種能力被刪除，除非重新啓動系統，否則即使root也無法重新加入被刪除的能力。

能力是一種規範，它定義了能夠對某個目標進行之所有操作行爲，以及允許在這個目標上進行的操作行爲。能力的操作動作包括：複製某個能力、程序間某個能力之遷移、修改某個能力以及取消某個能力等。目前爲止，各種作業系統對能力(Capability)的應用程度並不相同。

舉例來說，File Descriptor就是一種能力，當使用者利用開啓(Open)這個系統呼叫(System call)來獲得檔案的讀或寫權限，如果Open執行成功，系統的核心就會建立一個File Descriptor。如果收到讀或寫的請求，核心就使用這個File Descriptor作爲一個資料結構的索引，檢查相關的操作是否已被允許。基於單一root之脆弱性的風險；因此，訂定資訊安全政策時，通常會建議管理者使用Linux核心定義的這些能力，依系統需求分割root的權限，避免因系統中root的權限過大所造成的安全風險（註7），表4是Linux中之能力表列（註6~8）。

現有之Linux作業系統以傳統Bell-LaPadula（同註6~8）安全機制爲主流，其對資料的完整性等安全需求有所不足的，因此美國國家安全局(National Security Agency，簡稱NSA)在2001年的Linux核心高峰會上，以Linux爲架構，提出研究發展近10年之安全增強Linux機制：SE Linux（註9），使用較具有彈性的flask（同註8）框架，將Linux安全等級提升至EAL4，同時具有資料標記及強制的存取控制（註10），號稱是最安全的Linux作業系統。SE Linux可以被用來規範最小特權，保護過程與資料的完整性、機密性及可歸責性宜有之職責區隔機制等。

SE Linux系統之安全體系結構如圖8所示，封裝於安全服務中之政策(Policy)與具體執行實施(Enforcement)的對象管理器兩部分組成；首先以政策語言(Policy language)提供系統管理者來制定安全政策(Security policy)，並由核心層存取控制檢查。SE Linux同時提供了範例政策(Example policy)，並允許使用者利用型態強化(Type Enforce，簡稱TE)與RBAC及可選之多級別安全性(Optional Multilevel Security)方式來客製化系統。

表4 Linux之能力表列

能力名稱(Capability Name)	代號	說明
CAP_CHOWN	0	允許改變檔案的所有權
CAP_DAC_OVERRIDE	1	忽略所有DAC的存取
CAP_DAC_READ_SEARCH	2	忽略所有對讀、搜索操作的限制
CAP_FOWNER	3	如果檔案屬於過程的UID，就取消對檔案的限制
CAP_FSETID	4	允許設置setuid
CAP_FS_MASK	0x1f	用來決定fall back到suers或fsuers
CAP_KIL	5	忽略過程間傳送signal時檢查uid的限制
CAP_SETGID	6	允許改變群組ID
CAP_SETUID	7	允許改變使用者ID
CAP_SETPCAP	8	允許向其它過程轉移能力及刪除能力
CAP_LINUX_IMMUTABLE	9	允許修改檔案的IMMUTABLE和APPEND-ONLY屬性
CAP_NET_BIND_SERVICE	10	允許應用程式bind小於1024的port
CAP_NET_BROADCAST	11	允許網路Broadcast和Multicast
CAP_NET_ADMIN	12	允許執行網路管理任務：socket、防火牆等
CAP_NET_RAW	13	允許使用raw socket
CAP_IPC_LOCK	14	允許鎖定IPC
CAP_IPC_OWNER	15	忽略IPC所有權檢查
CAP_SYS_MODULE	16	插入和刪除核心模組
CAP_SYS_RAWIO	17	允許對ioperm/iopl的存取
CAP_SYS_CHROOT	18	允許使用chroot system call
CAP_SYS_PTRACE	19	允許trace任何程序
CAP_SYS_PACCT	20	允許設定過程 accounting
CAP_SYS_ADMIN	21	允許執行系統管理任務，如：檔案系統控制、quota、設定網域名稱等
CAP_SYS_BOOT	22	允許重新啓動系統
CAP_SYS_NICE	23	允許提升nice值
CAP_SYS_RESOURCE	24	忽略資源限制
CAP_SYS_TIME	25	允許改變系統時間
CAP_SYS_TTY_CONFIG	26	允許設定TTY Device
CAP_SYS_MEM DUMP	27	允許傾印任何記體區塊
CAP_SYS_EERPOM	28	允許存取EEPROM
CAP_SYS_PSDUMP	29	允許列出所有執行過程
CAP_SYS_SIGTRIP	30	允許執行trace trap
CAP_MKNOD	31	允許使用mknod system call
CAP_LEASE	32	Allow taking of leases on files

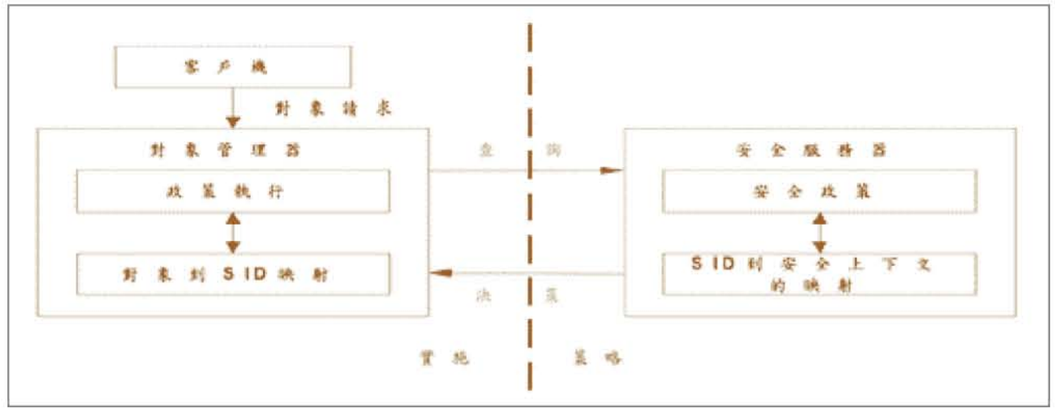


圖8 SE Linux安全體系結構圖

SE Linux系統中關於安全的請求和決策有三種情況（同註8~10）：

（一）標示決策(Labeling decision)：確定一個新的主體或受體採用什麼安全標示（如創建受體時）。

（二）存取決策(Access Decision)：確定主體是否能存取受體的某種服務（如文件讀寫）。

（三）多模態決策(Polyinstantiation Decision)：確定一個過程在訪問某個polyinstantiation受體時，可不可以轉爲另一個過程。

SE Linux設計精神主要由根據特定目的定義類別(Domain Type)，限制其存取物件類別之TE與如圖9所示RABC以及可選的多級別安全性混合制定而成。

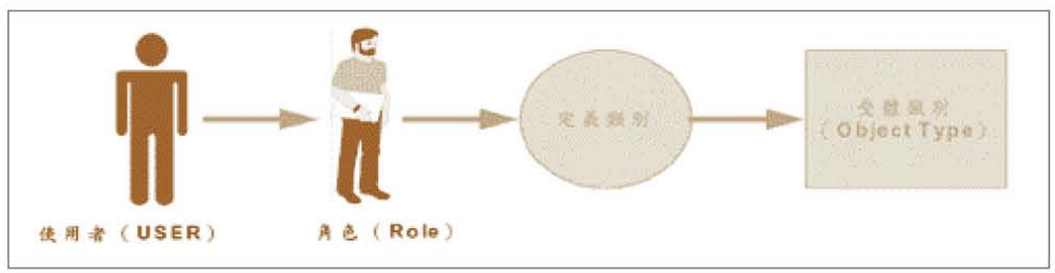


圖9 SE Linux為以角色為基底的存取控制

SE Linux複雜的安全政策固然提供管理者很大的安全制訂彈性，但因SE Linux語法複雜且龐大，例如由SE Linux所提供的政策範例(example policy)中，至少包含3個角色，29個object class，22個attribute，115個permission，253個type，及上萬行的語法，因此在使用SE Linux時所面臨設定及管理安全政策上的複雜及困難，也衍生出許多相關研究，例如所設定的規則是否符合使用者所要求的目標等；如欲善用SE Linux，宜先瞭解RBAC。

二、以角色為基礎的存取控制標準簡析

Ferraiolo, D.F.、R.Sandhu、S.Gavrila三位學者，在2001年發表了"A Proposed Standard for Role-Based Access Contro"同註12）一文，整理出過去學術界以及美國國家標準與技術研究院(National Institute of Standards and Technology，簡稱NIST)在RBAC領域的研究成果，根基於RBAC96（同註11）提出美國聯邦政府使用之標準建議的RBAC之定義與理論模型，將RBAC模型分成幾個部分，包括核心RBAC、階層式RBAC、限制式RBAC；限制式RBAC又可以分爲靜態權責區與動態權責區分兩種方式；其區別在於在存取控制的過程中，爲了避免發生濫用職權的情形，而加諸之不同的管制與限制方法；分述於后：

（一）核心RBAC：RBAC核心概念就是將角色指派給使用者，而每個角色則給予不同的權限。一個使用者可以被指派多個角色，而一個角色可以指派給多個使用者；另一個核心的概念是使用者期間(User Session)，當使用者選擇啓動一角色職位，就是一個使用者期間的開始，於期間中，使用者可以選擇性地啓動或終止角色職權的行使。相較於RBAC0並沒有使用者期間的觀念，核心RBAC則是將圖10中之RBAC2模組中的期間加入其中，圖10是其示意說明。

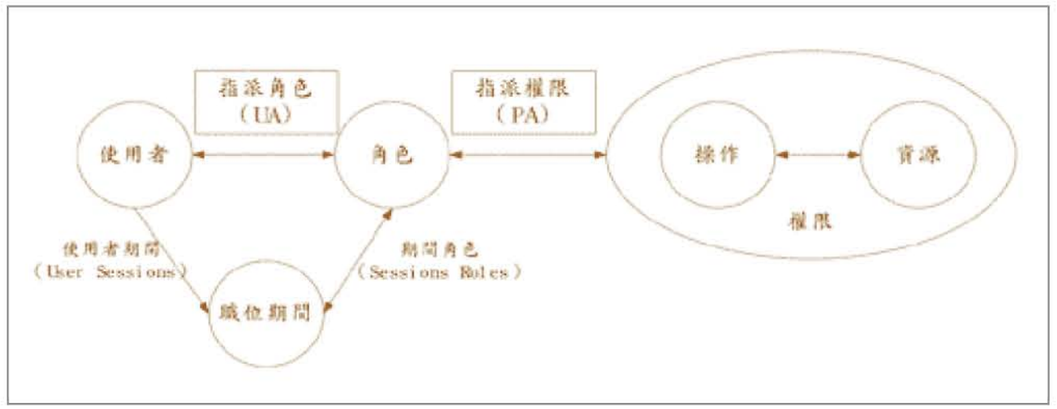


圖10 核心RBAC示意圖

（二）階層式RBAC：主要的觀念就是角色之間的層級關係與繼承關係。舉例來說，當角色甲具有角色乙所有的權限，則可以說角色甲與角色乙有繼承的關係；將一些共同的基本權限規劃於層級較低的角色，利用繼承的關係，免去每個角色都必須重複指派共同權限的動作，減輕管理的負擔。階層式RBAC又可以再分爲兩種：

1.一般職位階層模式：上層的角色可以繼承下層所有的權限，而沒有任何限制條件。

2.限制職位階層模式：一般而言，在組織運作實務中，職位階層模式常

常無法滿足管理的需求；因此，限制式的職位階層模組，強化繼承上的管理限制；上層角色所能繼承的權限範圍，應根據管理政策加以限制。

（三）靜態權責區分：權責區分的主要用意在於避免利益衝突(Conflict of Interests)的情形。具有利益上衝突的兩個角色，應將此二角色設定爲強互斥(Mutually Exclusive)，也就是說不能由同一人通時擔任這兩個角色。靜態權責區分的限制根基於角色層級的定義與使用者指派角色的情境上。

（四）動態權責區分：依據最小權限原則，某些角色可以指派給同一人，但是不可以同時啓動這些角色，這些角色間的關係稱爲弱互斥(Weak Exclusion)。動態權責區分的目的，在於提供組織實務運作上更大的彈性與效率，只要兩個角色在單獨啓動時不會有利益衝突的顧慮，則允許將這兩個角色指派給同一使用者。圖11是上述不同RBAC之示意說明。

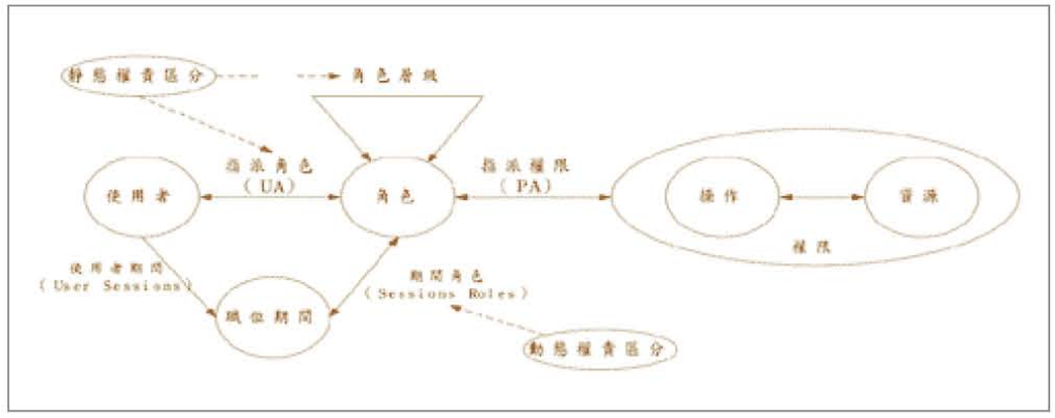


圖11 限制式RBAC示意圖

一般而言，RBAC具有下列2個優點：

1.容易理解與管理：使用者的權限已經融入角色之中，管理者針對單一使用者不必考慮要給予哪些權限，而是指派哪些角色給他。角色職權的設定不會因爲員工離職、調職而有所變更，僅需變更該員工的設定即可，在管理上是比較方便的。

2.擴充性高：在一個使用者眾多的系統之中，角色的數量一定是小於所有使用者的數量。以電子商務爲例，角色可能包含買家、賣家、管理人員，但是實際的使用者數量可能是超過幾千、幾萬人。與傳統的存取控制比起來，RBAC在應用於大量使用者的環境，更具有擴充性。

具有最小權限、權責區分、權限繼承的概念：綜合以上對於RBAC的介紹，強調RBAC於資源存取控制上，基於最小權限原則，授與使用者完成任務所需的最小權限；基於避免利益衝突的原則，可以設定角色之間的關係爲靜態的強互斥，或是動態的弱互斥；在角色層級的設定上，具有繼承權限的觀念，減少被指派權限的管理工作，而在繼承權限時，也可以指定繼承部分的權限，提供一個可以代理角色的機制。

根基於RBAC之塑模，其實作系統架構，可以區分爲以下兩種（註11~15）：

（一）以使用者端爲主的架構(User-Pull Architecture)：當使用者要存取資源時，必須由使用者端主動獲取角色資訊，提供給網頁伺服器，作爲判斷是否有權限存取的依據。

（二）以伺服器爲主的架構(Server-Pull Architecture)：本架構將角色資訊儲存於伺服器端的目錄伺服器中，當使用者要求存取資源時，網頁伺服器必須向目錄伺服器取得角色資訊，加上原本就儲存在伺服器端的角色層級資訊、權限資訊，判斷該使用者是否具備存取某資源的權限。

上述兩種架構分如圖12與圖13所示（註15），其包括：使用者端使用上的便利性、整體系統的效能、可重複使用性、角色資訊更新的難易度與發生單點錯誤的影響等之比較如表5所示，說明如后：

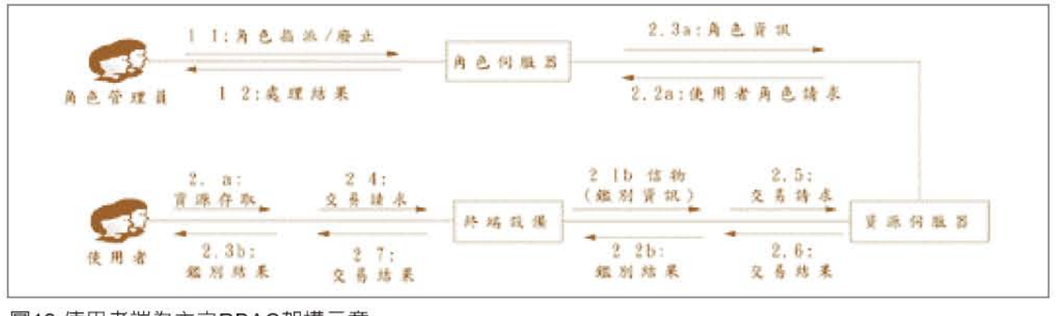


圖12 使用者端為主之RBAC架構示意

1.使用者便利性：以使用者爲主的架構來說，必須在使用者的平台上加裝軟體，對於使用者而言無異是一項負擔。在使用上，必須由使用者端主動提出角色資訊，造成使用者端於效能上的減低。

2.整體系統效能：因爲伺服器爲主的架構，將所有處理角色資訊的工作，完全置於伺服器端來完成，所以造成伺服器端必須分配額外的資源加以處理，間接影響到處理網頁服務的能力，整體系統的效能也跟著降低。

3.可重複使用性：使用者端取出角色資訊之後，這一份角色資訊理應存放於伺服器上，等待使用者端下一次要求連線時使用。這是屬於一般快取的機制，增加了資訊的可重複使用的特性，也減少了網路傳輸的負擔。

4.角色資訊更新速度：因爲角色資訊統一存放於伺服器端，等待使用者端要求連線始取出使用，一旦角色資訊有需要更新的情形，僅需要更新中央資料庫即可。相較之下，以使用者端爲主的架構，必須更新使用者端的角色資訊，還要判斷目前是否有使用中的角色資訊，必須要一併更新，增加工作之負荷。

(5)發生單點錯誤的影響：以使用者端爲主的架構，如果錯誤發生於單一使用者端，其影響的範圍僅限於該端點。如果錯誤發生於伺服器爲主的架構下，影響的範圍可能擴散至整個系統。

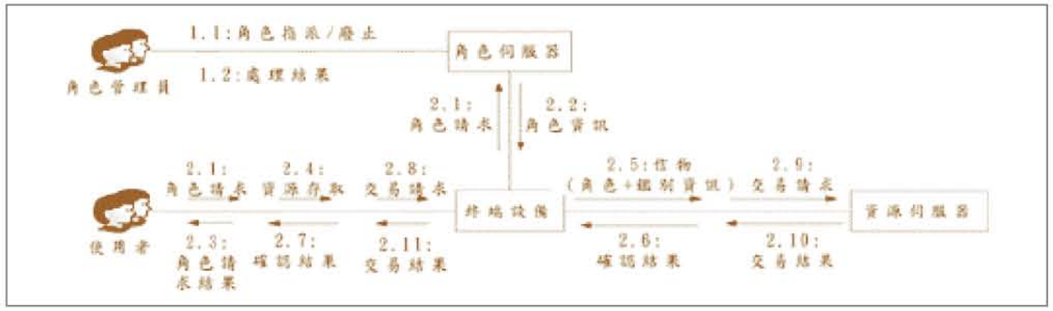


圖13 伺服器端為主之RBAC架構示意

表5 RBAC系統架構的比較

項目	User-Pull架構	Server-Pull架構
使用者便利性	低	高
整體系統效能	高	低
可重複使用性	高	低
角色資訊更新速度	低	高
發生單點錯誤的影響	低	高

由於SE Linux已獲得世界性的公認爲Linux的安全性加強工具，同時SE Linux本身安全政策語法繁雜，淺述於后。SE Linux是否有權存取是針對受體(Object)及主題(Subject)的安全上下文(Security context)來決定，而安全上下文主要是以user: role: type來表示。此外SE Linux主要以TE及RBAC方式制定安全政策。本節將針對SE Linux政策語言簡介說明。

SE Linux政策語言主要包含四種表達方式：宣告(declarations)，規則(rules)，限制(constraints)與主張(assertions)；根基於此，建置EAL4之RBAC系統將有事半功倍的效果(註16~17)。

肆、RBAC簡介與系統實作初探

一、RBAC簡介

組織中，每位工作人員所擁有的職權與職責是基於其所擔任的角色而定，而非工作人員本身。在過去我們採用「隨意性存取控制」(Discretional Access Control，簡稱DAC)與「強制性的存取控制」(Mandatory Access Control，簡稱MAC)做存取控制的控管，然而這兩種存取控制控管模式隨著組織結構的日益複雜化和安全需求的提高已不足以適用。因此，多位學者提出了“以角色爲基礎”的想法，透過角色本身所擁有的職權與責任、職位與工作等角色之間的互動關係與組織管理政策的結合，提出了「以角色爲基礎的存取控制管制」的參考模式（註11）。

角色本身代表了職權與責任等的組合，例如組織定義了「人事部經理」這個角色，規範出它應負的責任，即公司人事及薪資的管理，同時也授與它相對的權力，如人事任用決定權。在更完整的職務模式(Role Model)中包含了角色之間的關聯性，以及其限制條件（註12）。在1996年提出並形成共識之RBAC96模式（同註11）依照應用的層面分爲RBAC0、RBAC1、RBAC2、和RBAC3，其關聯性如圖14所示。

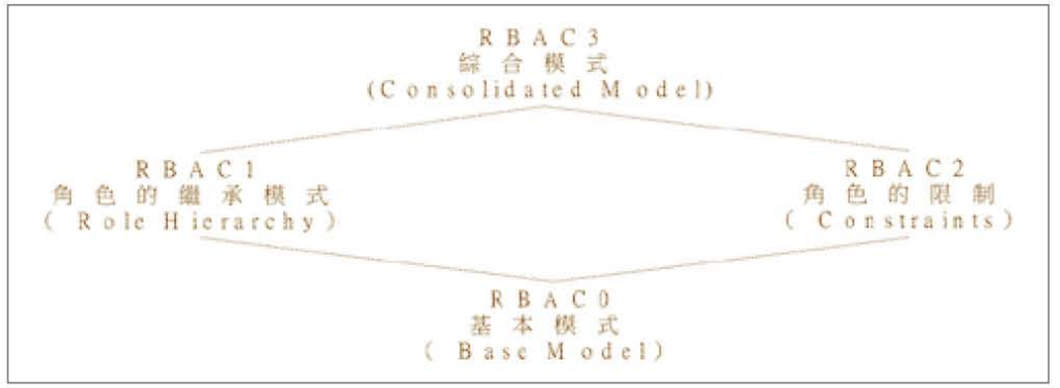


圖14 以角色為基礎的存取控制模式

RBAC中之基本模式定義了使用者、角色及權限三者之間的關聯。在角色的繼承模式中包含了基本模式，另外加入角色繼承的觀念，在角色的限制方面，RBAC96認爲在此可加入組織內部的控制方法，如權責區分、情境限制等，以符合大部份組織長久以來所規範的管理原則。在綜合模式中，將以上三者做整合，提供完整的角色存取控制方案。在RBAC0中定義了三個主要的個體，分別爲使用者、角色、以及權限三者。另外也納入連線的觀念，其關係如圖15所示：

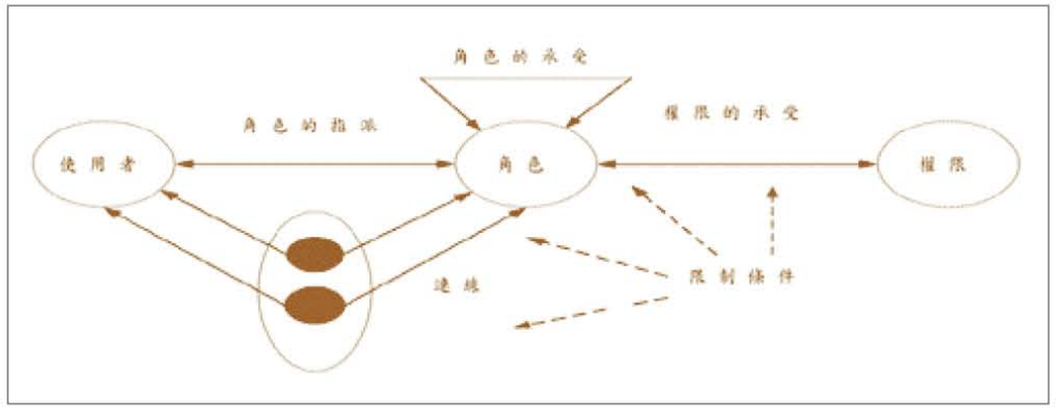


圖15 以角色為基礎的存取控制管制基礎架構

使用者可透過角色的指派取得其所擔任的職位應有的職權與責任，例如吳茲仁先生爲採購部主管，那麼他便可以經由角色的指派取得採購部主管的權力。而每一個角色可以執行的作業程序則在權限的指派來做設定；例如採購部主管的權限爲核准採購單，因此我們便可以將“核准採購單”這個作業程序指定給“採購部主管”這樣的角色。另外連線也是一種使用者與角色之間的關聯性，不同的是它是在動態執行時所產生，代表了使用者目前在執行中的角色集合。

在RBAC1中除了RBAC0對角色的基本定義外，納入了組織內角色承授的概念；也就是在組織中職位高的員工可以繼承職位低的員工的工作。舉例來說，在電腦軟體部門裡，主管除了可以執行相關的管理工作外，也可以做程式撰寫的工作（此爲程式設計師的工作內容），如圖16所示。

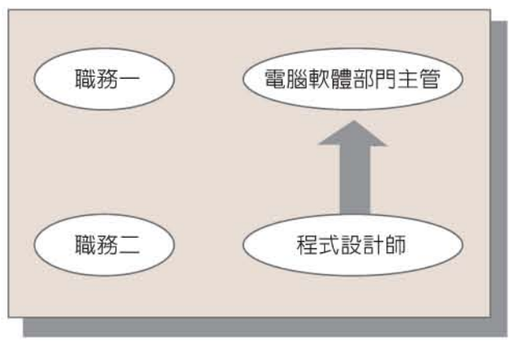


圖16 RBAC中角色之繼承概念

在RBAC2中納入了許多角色實行時的限制條件，這些限制條件在組織的運作上組成了重要的控制點，用以實現傳統企業的內部控制原則。其中包括權責區分、組織取得的必備條件限制、指派組織的數量限制、被啓動的組織限制等。

在RBAC理論中，由於考慮到組織的實際需求，因此相較於傳統的存取控制理論(如DAC或MAC)，具有以下的優點（註11~13）：

（一）對於屬於同一個角色的數個員工，其工作權限只需定義一次。

（二）當員工轉換個職位時（如升遷或離職），角色的工作權限不需要更動，只需將此員工指派至新角色即可。

（三）許多內部控制的原則，如權責區分及角色代理，皆可在角色本身或角色與角色間加入限制條件來達成；在另一方面，角色基存取控制還可以與身分鑑別機制整合，提升資訊系統整體之安全性與可用性，目前已成爲Web Service之工業標準（註13）。

二、RBAC系統實作初探

在本節中，我們分別介紹根基於安全標章之使用者端RBAC系統與根基於目錄伺服器之伺服器端RBAC系統實作概要。

（一）根基於安全標章(Secure Cookies)之使用者端RBAC系統簡介

因爲傳統的標章的安全性不高，安全標章針對傳統標章的安全弱點，改善其安全上的脆弱性。傳統的標章因其在傳輸時並有加密保護，從伺服端到用戶端的網路傳輸中，很可能被擷取，而且直接可以加以重送使用；在另一方面，傳統的標章傳輸到用戶端之後，是以檔案的型態儲存於硬碟中，如果用戶將內容複製到其他電腦，伺服端亦不會察覺被複製的情形，表6是其弱點與防護方法之示意說明。

表6 傳統標章(Cookie)之安全弱點及防護方法

弱點名稱	防護方法
來自網路上安全的威脅	建議使用Secure Sockets Layer(SSL)，但是SSL只支援安全標章(Secure Cookie)。
來自用戶端的威脅	利用加密的方法保護儲存在用戶端的標章。
標章本身遭到複製重送的威脅	程式中加入鑑別的安全協定來防止。

安全標章提供了：鑑別服務、完整性服務與機密性之三種服務，透過共同閘通道(Common Gateway Interface，簡稱CGI)的呼叫程式，達成加、解密及簽章的功能，而安全標章必須能夠做到產生簽章、查證以及提供使用階段所需要的角色資料，其資料結構如表7所示，圖17是根基於安全標章之使用者端RBAC系統的示意說明。

表7 安全標章之資料結構示意說明

	網域	旗標	路徑	資料名稱	值	目期
名稱Cookie	iss.com	True	／	名稱Cookie	愛麗絲#	12/31/2002
角色Cookie	iss.com	True	／	角色Cookie	經理#	12/31/2002
Cookie週期	iss.com	True	／	Cookie週期	3年	12/31/2002
通行碼Cookie	iss.com		／	通行碼Cookie	通行碼的碎映(Hashing)	12/31/2002
其他Cookie	iss.com	True	／	其他Cookie	******	12/31/2002
金鑰Cookie	iss.com	True	／	金鑰Cookie	加密過的交談金鑰	12/31/2002
彌封Cookie	iss.com	True	／	彌封Cookie	彌封資料	12/31/2002
說明：標記“#”的欄位表示具敏感性欄位，應該使用交談金鑰(session key)加密。						

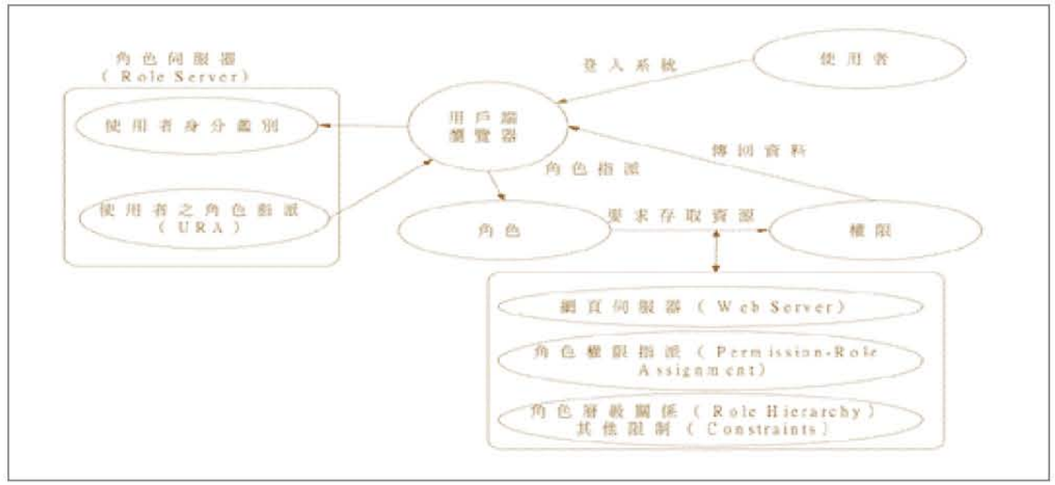
在圖17中，伺服器要如何相信使用者所提供的角色資訊是可靠的呢？圖18是其運作之示意說明，以吳茲仁先生使用網頁的例子說明如后：

1.開始先建立交談。

2.角色伺服器鑑別過吳茲仁先生的身分之後，再由使用者的角色指派資料庫中找到吳茲仁先生的角色，並建立一安全標章。

3.將安全標章傳送給吳茲仁先生的瀏覽器，存放於吳茲仁先生的電腦磁碟中，如此一來吳茲仁先生在本安全標章還未失效、過期之前，不需要再向角色伺服器要求重新鑑別與取得安全標章。

4.吳茲仁先生要開始進入網頁伺服器，送出



說明：a) 角色伺服器(Role Server)負責使用者的角色指派(User-Role Assignment，簡稱URA)，一般而言分為使用者身分鑑別與使用者2個模組。

b) 網頁伺服器負責角色層級關係(Role Hierarchies)，角色權限指派(Permission- Role Assignment，簡稱PRA)的資訊以及包括一些安全政策上的限制之存取控制。

圖17 根基於安全標章之系統示意說明

一個URL的請求，吳茲仁先生的瀏覽器也幫他將相關的安全標章傳給網頁伺服器。

5.網頁伺服器透過鑑別該標章的擁有者，以及其餘的資訊可以由來源位址和通行碼取得與鑑別。

6.網頁伺服器透過彌封資料與角色伺服器的公開金鑰，驗證標章的完整性。

7.當所有的標章都經過驗證是正確的，網頁伺服器便可以相信該角色的資訊是可靠的，接下來便可以將該角色的資訊，應用於網頁伺服器上的角色層級、角色權限指派等RBAC之機制。

實作時，可以使用如PGP(Pretty Good Privacy)等工具建置安全標章，圖19是產生安全標章之示意說明，其產生之步驟如下：

1.傳送使用者識別、通行碼與IP位址給角色伺服器。

2.進入產生安全標章的程序(Set-cookie.cgi)

3.對身分鑑別資料庫要求鑑別。

4.得到身分鑑別結果。

5.將使用者識別送入角色指派資料庫。

6.取出該使用者的角色資訊。

7.將通行碼送入產生碎映(Hashing)值的程序。

8.要求PGP工具程式產生碎映值。

9.傳回通行碼的碎映值。

10.將通行碼的碎映值送入產生安全標章的程序。

11.將產生安全標章送入簽章的程序。

12.要求PGP工具程式產生簽章。

13.傳回簽章值。

14.傳回加上簽章的安全標章。

15.傳回安全標章給角色伺服器。

16.傳回安全標章給使用者端的瀏覽器。

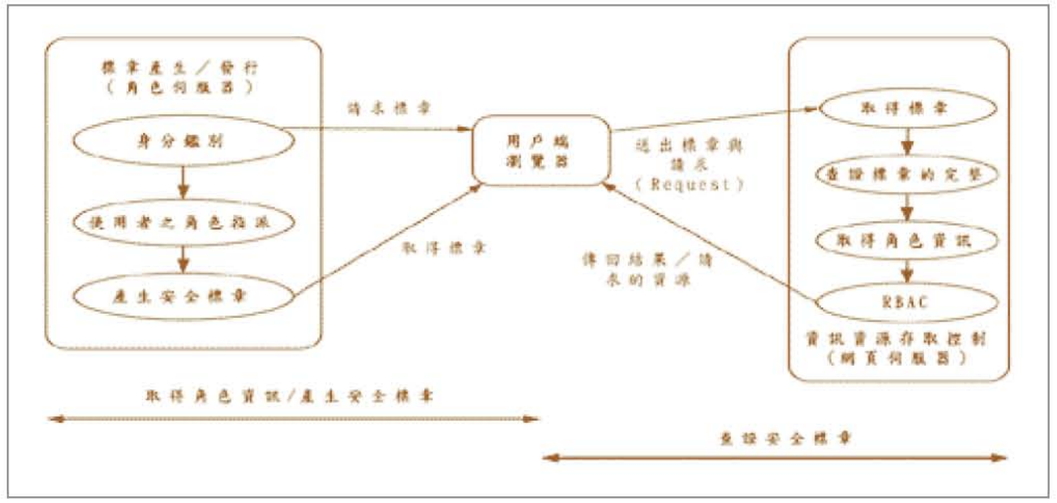


圖18 安全標章運作之示意說明

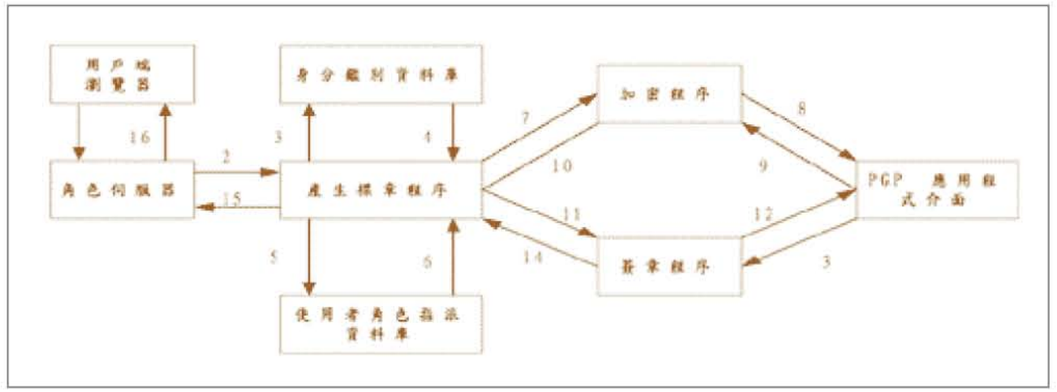


圖19 產生安全標章步驟示意說明

圖20是查證安全標章之示意說明，我們簡述查證安全標章的步驟如后：

1.將標章、使用者識別、通行碼與IP位址送到網頁伺服器。

2.將標章、使用者識別、通行碼與IP位址送入確認程序中。

3.通過IP位址的檢查之後，將標章、使用者識別、通行碼傳入通行碼的查證程序。

4.向PGP應用程式介面要求作解密的程序。

5.解密的結果。

6.送入查證簽章的程序。

7.向PGP應用程序介面要求查證簽章。

8.查證簽章的結果。

9.將角色資訊提供給RBAC的應用系統。

10.利用合法的角色進行操作。

11.存取資訊資源。

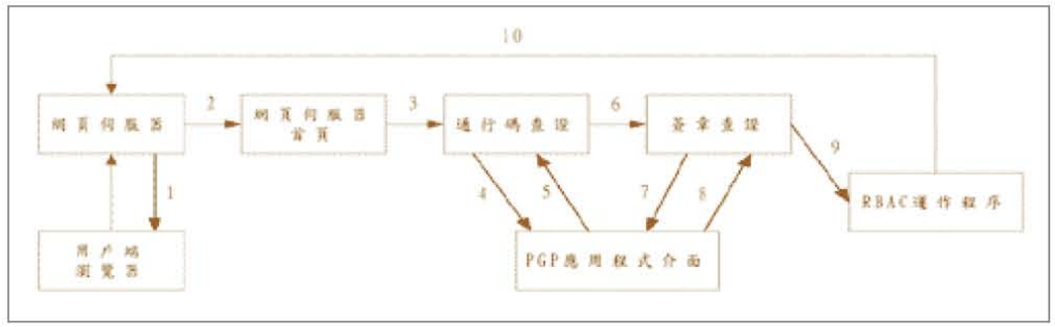


圖20 查證安全標章的步驟

經過產生、查證的安全標章，最後要用在網頁伺服器上面的RBAC系統之上才能發揮功能，一般而言，使用者假悍客要越權存取不該存取的網頁，縱使他的彌封標章通過查證，但是在簽章查證的階段依舊會被識破。

（二）根基於目錄伺服器之伺服端RBAC系統簡介

一般而言，使用目錄伺服器(Directory Server，簡稱DS)與SSL(Security Sockets Layer)即可建置Server-Pull架構之RBAC系統（註13），圖21是示意說明，其作業流程說明如后：

1.鑑別使用者端（使用通行碼等）。
2.顯示初始頁面。
3.讓使用者送出要求資源的URL。
4.建立目錄伺服器與網頁伺服器間的SSL通道。
5.網頁伺服器透過SSL送出請求指令，取得角色資訊。
6.目錄伺服器透過SSL傳回使用者的角色資訊給網頁伺服器。
7.繼續進行資訊資源（網頁）的傳送。

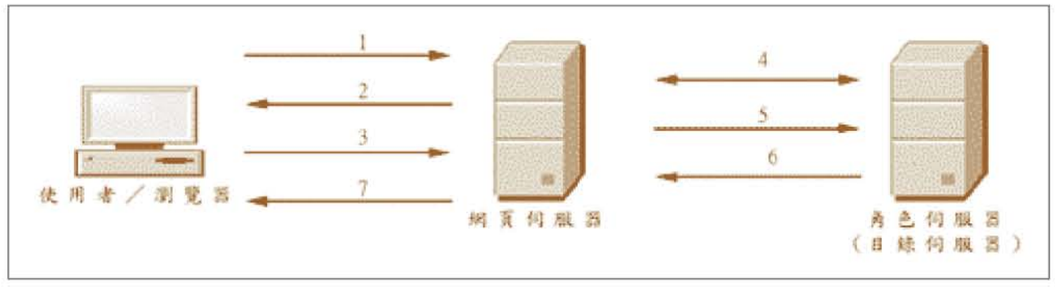


圖21 使用目錄伺服器與SSL實作伺服端RBAC系統與流程示意

整合身分鑑別與存取控制之RBAC系統，已是諸如SE Linux、Windows Server 2003等下一代存取控制之核心工程；一般而言，小型組織較適用於使用者端之RBAC系統，大型組織宜採用伺器端之RBAC系統。

伍、開放源碼機敏性檔案存取控制保護剖繪初探

資訊系統處理國家安全相關資訊已是事實，如何確保機敏性資料及其資訊系統不受未經授權之存取、使用、揭露、破解、修改與毀壞，以提供機密性、完整性和可用性的電子化政府相關資訊系統之應用已是各國政府應面對的問題。根基於此，提出「開放源碼處理機密性及敏感性(以下簡稱機敏性)檔案存取控制系統保護剖繪(Open Source Code RBAC PP，簡稱OSCAC PP)芻議」，以爲實作時安全遵循的參考（註18）。

共同準則(ISO/IEC 15408)之標的在提供資訊技術進行安全評估之準則，以提供信賴之基礎的保障。共同準則要求加大以往資訊技術安全評估之廣度、深度與強度，來測試資訊技術產品或系統安全的有效性。如圖22所示，保護剖繪提供使用者一個參考特定安全需求集合之方法，期能讓使用者對這些要求，如圖23所示之評估變得較容易（註14），根基於圖23、圖24與圖25的方法，在實作中探討之開放源碼機敏性檔案存取機制時，分別律定其宜具備之安全功能與保證，其保護剖繪內涵如下（同註18）：

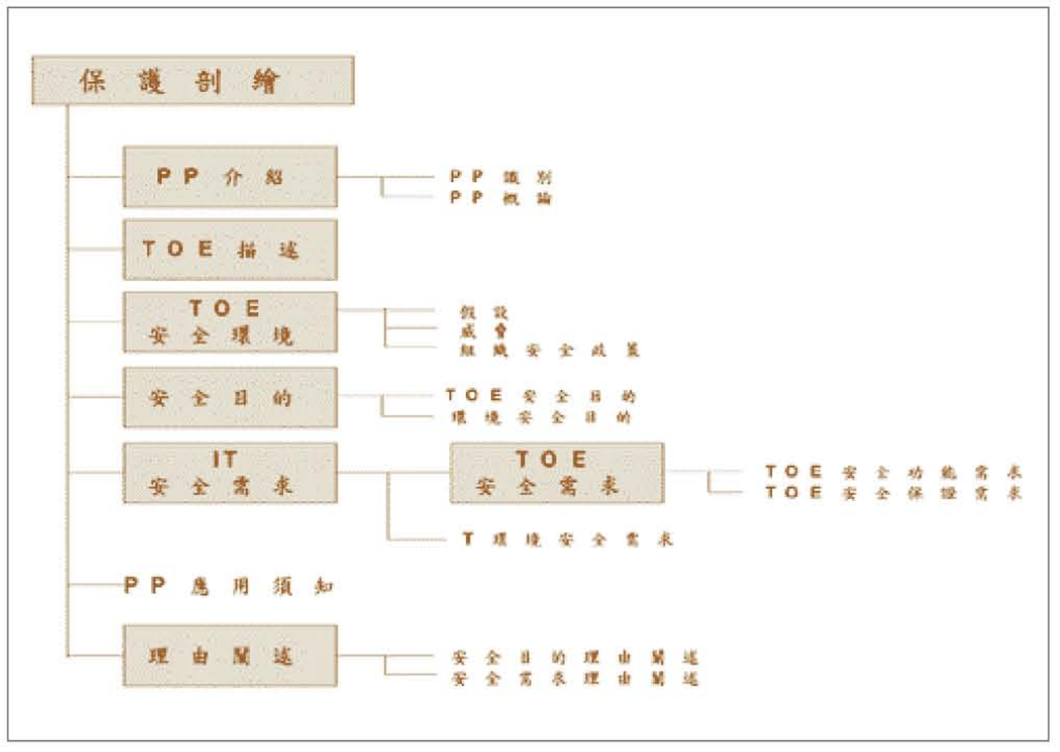


圖22 保護剖繪內容

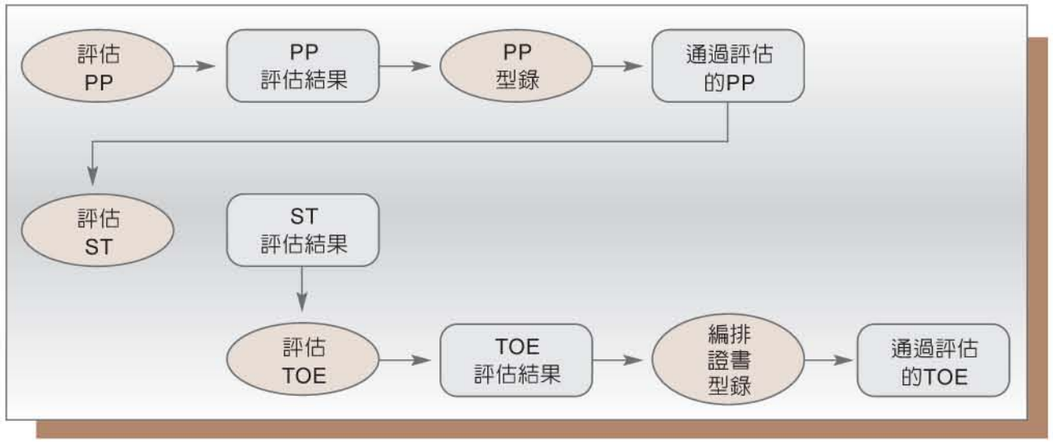
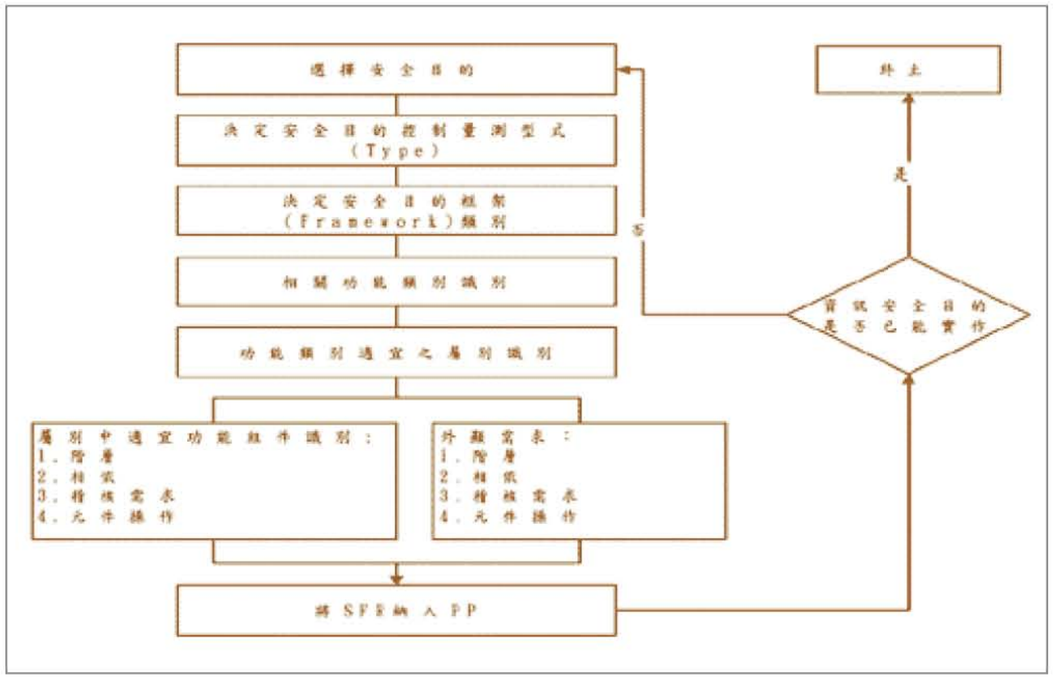
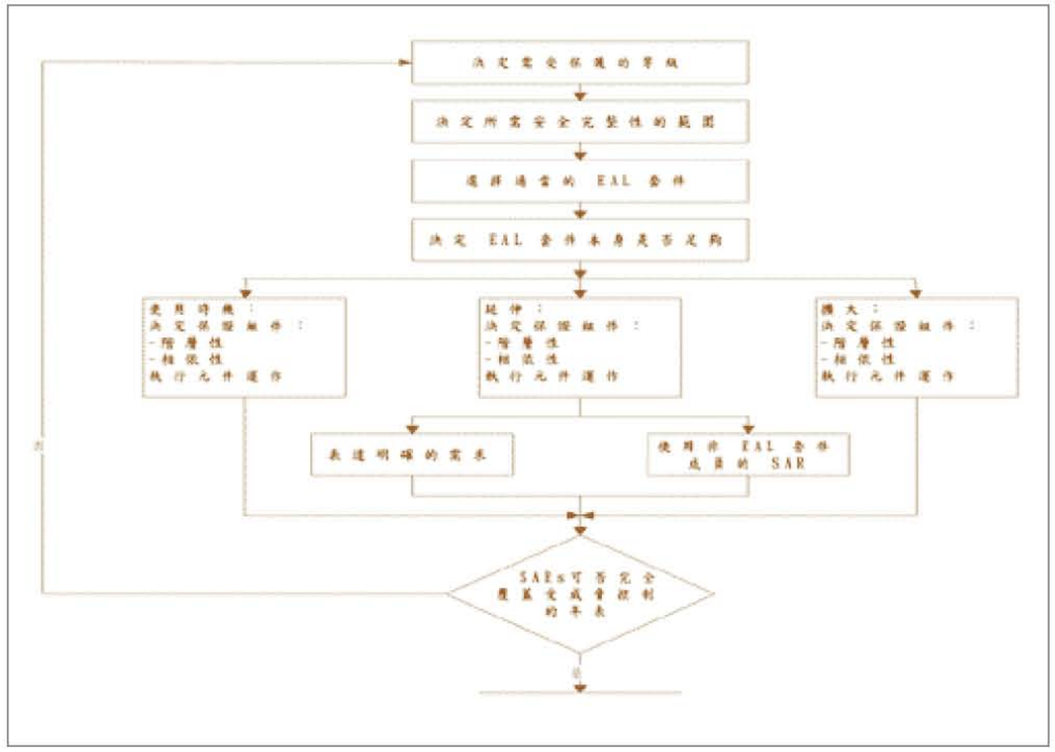


圖23 共同準則評估結果



資料來源：Herrmann, D. S., Using the Common Criteria for IT Security Evaluation, P.90, Exhibit 21, Auerbach Publications, 2003.

圖24 PP資訊技術安全功能需求(Security Function Requirements，簡稱SFR)選擇過程



資料來源：Herrmann, D. S., Using the Common Criteria for IT Security Evaluation, P.106, Exhibit 25, Auerbach Publications, 2003.

圖25 PP資訊技術安全保證需求(Security Assurance Requirements，簡稱SAR)選擇過程

於OSCAC保護剖繪之安全功能與保證部分，在理由闡述中一併說明：

一、安全環境

（一）威脅

組織安全政策的條例將推導出所有OSCAC PP的安全目的，而在我們綜整受控存取保護剖繪(Controlled Access Protection Profile，簡稱CAPP)（註19），Windows 2000安全標的(Security Target，簡稱ST)（註20），以及入侵偵測系統(Intrusion Detection System，簡稱IDS)相關保護剖繪（註21~24）之安全威脅後，OSCAC PP可能會遭遇那些威脅說明如下：

1. T.AUDIT_CORRUPT

未被授權的使用者可能篡改稽核資料，或者未被授權的使用者可能由於系統對稽核資料的保護措施失效而造成稽核資料的遺失。

2. T.CONFIG_CORRUPT

由於系統保護資料的措施失效造成組態資

料或被信任的資料遭未被授權的使用者篡改。

3. T.OBJECTS_NOT_CLEAN

使用者可能需要資源的存取及獲得資訊的未經授權存取，因爲該系統無法適當地從不同使用者間的目的中移除資料，因而洩漏資訊給下一個使用者。

4. T.SPOOF

一個僞裝成IT系統且有敵意的個體可能從已獲授權的且誤以爲正與IT系統溝通的使用者獲得鑑別資料的未授權的存取，當該使用者企圖開始登入時。

5. T.SYSACC

由於該系統無法限制存取，一個獲授權的使用者可能獲得該系統未經授權的存取且擔任管理者或其他的可信賴的人員。

6. T.UNAUTH_ACCESS

由於該系統無法限制存取，一個未經授權使用者可能獲得該系統資料的存取。

7. T.UNAUTH_MODIFICATION

由於該系統無法保護它的安全強化功能，一個未經授權使用者可能造成該系統中安全強化功能的修改，且因而獲得該系統及使用者資源的未經授權的存取。

8. T.UNDETECTED_ACTIONS

由於該系統無法記錄行爲，一個未經授權使用者可能執行不被偵測到的未經授權的行爲。

9. T.USER_CORRUPT

由於該系統無法加強限制已獲授權的使用者的資料，使用者資料可能會被未獲授權的使用者竄改。

（二）組織安全政策

所謂組織安全政策是一條條規則或程序，組織想靠其運作以防護組織敏感的資料。下列的組織安全政策乃源於共同準則標準系列。

1. P.ACCOUNTABILITY

該系統之使用者在系統內之一切舉動應被權責歸屬可說明的記錄。

2. P.ADD_IPSEC

該系統必須有能力保護在受保護系統的分散點間傳送的系統資料。

3. P.AUTHORIZATION

該系統必須有能力限制每個使用者的授權的範圍。

4. P.AUTHORIZATION_USERS

只有那些已被授權可以存取系統內訊息的那些使用者才能存取該系統。

5. P.NEED_TO_KNOW

在被授權使用者具有資訊「僅知原則」的情況下，系統還是必須限制其存取、修改、及破壞這個在保護資源內的訊息。

6. P.WARN

該系統必須有能力警告使用者關於該系統未經授權的使用。

（三）安全用法之假設

本節說明該TOE未來或目前意欲被使用之環境的安全部分。此包括有關實體、個人、及連線環境方面的訊息。

若在能被正確的建置、管理及使用下，符合OSCAC PP的TOE須能提供有效的安全措施於企業內沒有懷有敵意的環境。運作的環境必須依據保證需求的文件來處理，包括傳送文件、操作文件、及使用者指引／管理者指引。以下的特定情況被假定存在於符合OSCAC PP的TOE之環境中。

1. 實體上的假設

符合OSCAC PP的TOE意欲應用於有實體控制及監視的使用者區域。假設以下的實際狀況會存在：

(1) A.LOCATE

TOE之處理資源將被放置在控制存取設施內，該設施能避免未經授權的實體存取。

(2) A.PROTECT

對安全政策施行有關鍵性影響的硬體與軟體，將加以保護以防止未經授權之實體修改。

2. 人員上的假設

其假設存在以下的一些人員情況：

(1) A.COOP

被授權之使用者擁有必須之授權，以存取由TOE所管理的訊息，且其被期盼能在良性的環境中以合作的態度來運作。

(2) A.MANAGE

允許一個或多個有能力之個人被委派處理及其包含訊息之安全的該TOE。

(3) A.NO_EVIL_ADM

系統之管理者不可以是個粗心、有意的疏忽、或敵對的人，而且將遵循並依從管理文件來作業。

3. 通訊上的假設

此OSCAC PP不包括明確之網路或一些分散式系統的要求，然被假定存在以下之通訊狀況（註25）：

(1) A.CONNECT

與週邊設備相連接之所有接線均必須在OSCAC PP所在之作業系統控制的存取設備中，符合OSCAC PP之TOE透過一些業經授權的進出點，僅發出針對與TOE處理有關之安全考量。一般如終端存取點的內部通訊路徑，被假設爲已適當地保護。

(2) A.PEER

與TOE通訊之其他系統，被假設在相同之管理控制與相同的安全限制下運作。只有在整個網路運作於一些相同之限制下，且內斂於一單一管理定義域內時，符合OSCAC PP的TOE方可適用於一些被連接成網路的或被分配之環境，沒有針對依賴一些外部系統或連接至該等系統之安全需求。

二、安全目的

安全目的可分爲資訊技術(Information Technology，簡稱IT)安全目的或非資訊技術(Non-IT)安全目的。安全目的反映出可能會面對確認的威脅，或遵守確認之組織安全政策。所有被確認的威脅與組織政策推展出之安全目的將在下幾節中描述。

（一）IT安全目的

OSCAC PP IT的安全目的：

1. O.ALERT

TSF必須提供所有警示功能，以支援使用者保護資訊資源之職責。

2. O.AUDITING

TSF必須記錄該TOE之使用者所有與安全相關的動作。TSF必須呈現這些訊息給被授權之管理者。

3. O.AUDIT_PROTECTION

TSF必須提供保護與個別使用者相關的稽核資訊的能力。

4. O.AUTHORIZATION

TSF必須確保僅有被授權之使用者才能存取TOE及其資源。

5. O.DISCRETIONARY_ACCESS

TSF必須根據使用者之身份控制被存取的資源。TSF必須允許被授權之使用者明確說明那一些資源可以被那一些使用者存取。

6. O.ENCRYPTED_DATA

TSF必須確保只有加密資料的使用者可以收到解密的資料。

7. O.ENFORCEMENT

TSF必須被設計與實作出來，以確保組織政策執行於標的環境中。

8. O.IPSEC

TSF必須有能力保護在TOE的分散點間傳送的系統資料。

9. O.LEGAL_WARNING

TSF 必須提供機制以建議合法的使用者包括在允許該使用者存取由TSF所控制的資源之前的TOE 的使用。

10. O.LIMIT_AUTHORIZATION

TSF必須提供限制每個使用者的授權的範圍的能力。

11. O.MANAGE

TSF必須提供所有功能及設施，以支援被授權之管理者能對管理TOE之安全負責任。

12. O.PROTECT

TSF 必須保護它自己的資料和資源且必須保留一個網域以使它執行免於外界的干擾或竄改 。

13. O.RESIDUAL_INFORMATION

TSF必須確保當資源被回收時，被保護資源內之任一訊息不致被釋出。

14. O.TRUSTED_PATH

在開始的使用者鑑別期間，TSF必須提供允許使用者確保他們並非和其他的偽裝成TSF的實體溝通的能力。

（二）Non-IT安全目的

符合OSCAC PP的TOE被假定爲完整的與自滿自足的，並不依賴任何其他產品就能適當地運作。然而，有關於一般操作環境的目的必須被符合。以下是OSCAC PP之Non-IT安全目的：

1. O.CREDEN

TOE必須盡責的確保使用者採用維護IT安全目的的所有憑證，諸如通行碼或其他鑑別訊息。

2. O.INSTALL

TOE必須盡責的確保TOE的傳送、建置、處理、與操作以維護IT安全目的。

3. O.PHYSICAL

TOE必須盡責的確保對安全政策有關鍵性影響的TOE之信物部分，免於實體上的攻擊而破解IT安全目的。

三、理由闡述 (Rationale)

有關OSCAC PP安全政策、安全目的與安全組件的選擇、產生、及使用的理由闡述，分爲以安全政策爲基礎的安全目的之存在理由闡述，安全目的爲基礎的功能性與保證性組件存在的低階理由闡述，如表8、表9與表10所示；至於安全目的其相對映之安全組件的分析，與安全組件其相對映之安全目的的分析等，因囿於篇幅，有興趣之讀者請見參考文獻（註18~26），OSCAC PP的符合性宣告宜爲EAL4 Argumented ALC_FLR.3。

表8 資訊技術(IT)環境安全目的理由闡述

IT 安全目的	威脅與組織政策
O.ALERT	T.UNDETECTED_ACTIONS P.ACCOUNTABILITY P.AUTHORIZED_USERS P.NEED_TO_KNOW
O.AUDITING	T.UNDETECTED_ACTIONS P.ACCOUNTABILITY
O.AUDIT_PROTECTION	T.AUDIT_CORRUPT
O.AUTHORIZATION	T.SYSACC T.UNAUTH_ACCESS P.AUTHORIZED_USERS
O.DENIAL_MALWARE	T. DENIAL_MALWARE
O.DISCRETIONARY_ACCESS	T.USER_CORRUPT P.NEED_TO_KNOW
O.ENCRYPTED_DATA	T.USER_CORRUPT T.UNAUTH_ACCESS
O.ENFORCEMENT	P.ADD_IPSEC P.ACCOUNTABILITY P.AUTHORIZED_USERS P.NEED_TO_KNOW
O.IPSEC	P.ADD_IPSEC
O.LEGAL_WARNING	P.WARN
O.LIMIT_AUTHORIZATION	P.AUTHORIZATION
O.MANAGE	P.ACCOUNTABILITY P.AUTHORIZED_USERS P.NEED_TO_KNOW
O.PROTECT	T.CONFIG_CORRUPT T.UNAUTH_ACCESS T.UNAUTH_MODIFICATION T.USER_CORRUPT
O.RESIDUAL_INFORMATION	T.OBJECTS_NOT_CLEAN P.NEED_TO_KNOW
O.TRUSTED_PATH	T.SPOOF

表9 非資訊技術(Non-IT)環境安全目的理由闡述

Non-IT安全目的	環境假設
O.CREDEN	A.COOP
O.INSTALL	A.MANAGE A.NO_EVIL_ADM A.PEER
O.PHYSICAL	A.CONNECT A.LOCATE A.PROTECT

表10 資訊安全功能組件與安全目的理由闡述

Requirement	O.ALERT	O.AUDITING	O.AUDIT_PROTECTION	O.AUTHORIZATION	O.DENIAL_MALWARE	O.DISCRETIONARY_ACCESS	O.ENCRYPTED_DATA	O.ENFORCEMENT	O.IPSEC	O.LEGAL_WARNING	O.LIMIT_AUTHORIZATION	O.MANAGE	O.PROTECT	O.RESIDUAL_INFORMATION	O.TRUSTED_PATH
FAU_GEN.1		X													
FAU_GEN.2		X													
FAU_SAR.1		X										X			
FAU_SAR.2		X													
FAU_SAR.3		X										X			
FAU_STG.1		X	X												
FAU_STG.3		X										X			
FAU_STG.4		X	X									X			
FCS_COP.1							X								
FDP_ACC.1						X									
FDP_ACC.2					X										
FDP_ACF.1						X									
FDP_IFC.2					X										
FDP_IFF.5					X										
FDP_RIP.2															X
Note1_EX															X
FIA_AFL.1				X											
FIA_ATD.1				X		X					X				
FIA_SOS.1				X											
FIA_UAU.2				X											
FIA_UAU.7				X											
FIA_UID.2				X											
FIA_USB.1_EX		X				X									
FMT_MOF.1				X					X			X			
FMT_MSA.1						X						X			
FMT_MSA.3						X						X			
FMT_MTD.1		X		X						X		X	X		
FMT_MTD.2				X								X			
FMT_REV.1						X					X	X			
FMT_SAE.1				X								X			
FMT_SMR.1											X	X			
FMT_SMR.3												X			
FPT_ITC.1	X														
FPT_ITI.1	X														
FPT_ITI.2	X														
FPT_RVM.1	X							X							
FPT_SEP.1	X							X					X		
FPT_STM.1		X													
FPT_TST.1	X														
REPLICATION_EX												X			
TRANSFER_PROT_EX									X				X		
FRU_RSA.1				X											
BANNERS_EX										X					
FTA_SSL.1				X											
FTA_SSL.2				X											
FTA_TSE.1				X											
FTP_TRP.1															X

備考：

1. Note1_EX：此TSF將確保資源的任何資訊內容，已經無法再將該資源分配給其他主題。每一個處理序(Process)皆被分配新的記憶體及執行碼(Execution context)，記憶體在分配之前會被歸零或覆寫，當執行緒(Thread)產生或執行碼閘(Switch)出現時，執行將被初始化或重新初始化。
2. FIA_USB.1_EX：每一個處理序及執行緒均具有一個組合的符記(Token)，以識別此處理序或執行緒所代表的持有者其所需負責任的使用者(用來稽核及取存)、組合群組(用來取存)、特權、及登入的權限。
3. REPLICATION_EX：此TOE將確保改變到TSF的資料已被複製一份至部分的TOE，且TOE所接收到的TSF資料只有在較現在的值為新時才會被接受。
4. TRANSFER_PROT_EX：當TSF資料在分離的TOE間傳送時，此TSF將可以保護該資料以避免被揭露及修改。
5. BANNERS_EX：在建立使用者期間(Session)之前，此TSF將可以顯示一個有關未獲授權使用TOE的警告訊息。一個獲授權的管理者可以定義及修改顯示在允許使用者登入之前的橫幅(Banner)。

陸、結論

管理資訊使用者角色之設定，根據使用目的指派角色，限制使用者權限，制定適宜的安全政策，降低潛在之風險已是作業系統安全設計的基石。微軟公司之Windows 2000/XP遵循根基於目錄伺服器之伺服端RBAC系統的框架，採用Kerberos第5版之鑑別協定(Authentication)、網際網路協定安全(Internet Protocol Security，簡稱IPSEC)、憑證管理(Certificate Management)等實作滿足EAL4的作業系統（同註5）。根基於Linux核心資源，海峽對岸自主開發之安勝安全操作系統，已達到了作業系統EAL4的安全功能

要求並通過測評認證（同註8）。根基於SE Linux，建置一個採用安全標章之使用者端RBAC系統，於我國已使用公開金鑰基礎建設(Public Key Infrastructure，簡稱PKI)的電子化政府之環境，應有一定的優勢（註27），希望早日看到通過EAL4驗證之台灣版的能處理機敏性檔案之存取控制的開放源碼作業環境（註28~29），表10中增加之5個安全功能組件的FIA_USB.1_EX已預留可信賴平台模組(Trust Platform Module，簡稱TPM)之介面規範（註30）。

我國關心開放源碼與共同準則相關作業，時間尚短、經驗之累積不多，許多應建立的價值、觀念及制度，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開放源碼以及共同準則驗證作業等之議題，實應展開更深入的思考與研討。身為數位時代開放系統之一員，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，本文之內容，是我們對開放源碼與共同準則繳出的一份學習報告，尚望先進宏達不吝指正。

註釋

註1：ISO, Information technology - Security techniques - Evaluation criteria for IT security (all parts), ISO/IEC 15408, 1999.

註2：Hamilton, B.A., Depart of Defense Public Key Infrastructure and Key Management Infrastructure Token Protection Profile (Medium Robustness), NSA (National Security Agency), 2002.

註3：NSA (National Security Agency), Controlled Access Protection Profile (CAPP), Version 1.d, October 8, 1999.

註4：GmbH, & IBM, SuSE Linux Enterprise Server Version 8 with Service Pack 3, Security Target for CAPP Compliance, November 26, 2003.

註5：Science Applications International Corporation, Windows 2000 Security Target ST Version 2.0, October 18, 2002.

註6：陳奕明主編，Linux系統安全分析，行政院國家科學委員會技術資料中心，臺北，2003。

註7：Mann, S., & E.L. Mitchell, Linux System Security, Prentice Hall, 2000.

註8：卿斯漢等，操作系統安全導論，科學出版社，臺北，2003。

註9：<http://www.nsa.gov/SELinux> (2004/7/29).

註10：NSA, Labeled Security Protection Profile, Version 1.b, October 8, 1999.

註11：Sandhu, R.S., E.J. Coyne, H.L. Feinstein, & C.E. Youman, IEEE Computer, Vol.29, No.2, pp38~47, 1996.

註12：Ferraiolo, D.F., S. Sandhu, D. Gavrila, D.R. Kuhn, & R. Chandramouli, "A Proposed Standard for Role-Based Access Control," ACM Transactions on Information and Systems Security, Vol.4 , No.3 , pp224~274, 2001.

註13：Bacon, J., K. Moody, & W. Yao, "A Model of OASIS Role-Based Access Control and its Support for Active Security," ACM Transactions on Information and Systems Security, Vol.5, No.4, pp492~540, 2002.

註14：Bartion, E., B. Catania, E. Ferrari, & P. Perlasca, "A Logical Framework for Reasoning about Access Control Models," ACM Transactions on Information and System Security, Vol.6, No.1, PP.71~127, 2003.

註15：Park, J.S., G.-J, Ahn, & R. Sandhu, "Role-Based Access Control on the WEB using LDAP," Database and Application Security XV, eds by Oliver, M.S., & D.L. Spooner, Kluwer Academic Publishers, pp.19~30, 2002.

註16：Ferraiolo, D.F., D.R. Kuhn, & R. Chandramouli, Role-Based Access Control , Artech House, 2003.

註17：鈺松國際資訊股份有限公司，網路服務效能式防火牆之開發（期末報告），2004。

註18：Farn, Kwo-Jean, et al., "A Study on the Information Security Audit and Alarm Protection Profile," Proceeding of the 5th International Common Criteria Conference, Sept. 2004.

註19：<http://niap.nist.gov/cc-scheme/pp/PP_CAPP_V1.d.pdf>, (2004/08/01).

註20：<http://niap.nist.gov/cc-scheme/st/ST_VID4002-ST.pdf>, (2004/08/01).

註21：<http://niap.nist.gov/cc-scheme/pp/PP_IDSSYPP_V1.4.pdf>, (2004/08/01).

註22：<http://niap.nist.gov/cc-scheme/pp/PP_IDSAPP_V1.1.pdf>, (2004/08/01).

註23：同註22。

註24：同註22。

註25：國防部中山科學研究院(2004)泰泓字第0930001080號函。

註26：<http://www.commoncriteriaportal.org/>, (2004/08/01).

註27：行政院研究發展考核委員會，2003電子化政府報告書(九十二年度)，臺北，2004。

註28：Shanker, K.S., & H. Kurth, "Certifying Open Source - The Linux Experience," IEEE Security & Privacy, Vol. 2, No. 6, pp.28~33, 2004.

註29：Williams J ., et a l ., A Guide to Understanding Security Modeling in Trusted System, NSA, 1992.

註30：Ren, J. et al. (2005) "Design and Implementation of TPM SUP320," in Security and Privacy in the Age of Ubiquitous Computing, pp. 143~154, eds by Sasaki, R. et al. Springer.