開放平台資訊科技日誌管理之研究

劉軒宏* 蔡敦仁** 曾奕霖*
*中國文化大學資訊管理學系 **中國文化大學資訊工程學系

摘要

資訊系統因服務轉型快速增加，雖然高度資訊系統化提升了工作效率，但隨著台灣於2012 年 10 月個人資料保護法實施後，政府機關與民間企業也都開始正視個人資料安全保護之問題，因資訊部門之開放平台(Open Source Platforms)作業系統造成後續資訊科技稽核(IT Audit)管理與實施之難度提高，由於系統稽核模式複雜且作業系統平台版本相當多，且目前稽核方式必須登入每台系統查核，過程中需從不同平台系統確認稽核之記錄，造成管理與稽核之不便。為解決稽核不便之問題，設計其跨平台稽核管理架構，以實做資料庫系統為主，使用甲骨文(Oracle)內建之資料庫稽核記錄(Database audit trail)機制，將各資料庫對不同使用者帳號設定收集登入(Login)、登出(Logout)與連線期間所執行之結構化查詢語言(Structured Query Language, SQL)產生的稽核資料(Auditing data)統一集中於獨立的資料庫儲存，最後將系統日誌(System Log)收集於系統日誌資料庫記錄，每天定時自動連線至各個資料庫收取日誌資訊，可提供系統管理人員與稽核來使用。

貢獻為導入後使用者可有效的於特定主機登入，以 SQL 語法方式查詢，且可產出報表，另一方面為系統日誌集中化後，可避免資料庫系統有不必要之 SQL 存取，可提升資料庫架構之系統效能，在此架構模式下面對系統稽核因管理平台眾多就可以快速查詢納入控管之系統，可即時追蹤提早發現系統異常存取，在未來新開放平台導入只需調整相關蒐集欄位。

關鍵詞：開放平台、資訊科技稽核、資料庫架構

1. 前言

開放平台應用多且廣泛於企業中使用，為了容易集中化管理，實做適合之稽核系統。

2. 文獻回顧

目前國際上就個資隱私保護的趨勢朝向標章認證模式，以促進電子商務環境下對於消費者個人資料保護，如美國的 TRUSTe、日本的 P Mark 和韓國 ePrivacy Mark 等。經濟部商業司已委託財團法人資訊工業策進會科技法律研究所研擬「台灣個人資料保護與管理制度(TPIPAS)」，並發表台灣第一個「資料隱私保護標章(Data Privacy Protection Mark, DP Mark)」，以 DP Mark 標章授與的方式，促進業者加強用戶隱私的保護，並降低業者違反個資法的風險[1]。

關聯式資料已成主要核心資料，因此為了保障這些核心資料不會被有心人士取得，資訊庫稽核系統更顯重要[2]。由於 Linux 是開放來源(open-source)平台系統中很特別的一類，且有很多類似的系統平台。在不同種類中都有不同的工具、應用程式、系統實用工具與桌面的環境應用。現在比較受歡迎的有 Red Hat、Ubuntu、Debian、SUSE 與 Gentoo，雖然上述開放作業系統平台皆有不同之處，在包裝管理(package management)、檔案系統結構(file system structure)也不相同，但卻有著相同的開發核心。另一方面如果想把稽核做好就必須持續不段的稽核，強烈建議從系統日誌中查看系統日誌是否出現了任何可疑的登錄或異常的行為存在，並嘗試加以對抗。為了防止異常與

可疑之情形，系統日誌記錄必須開啟使用且日誌系統不能被其他使用者自行編輯竄改。最後建議系統管理員，盡可能的嘗試記錄大多的系統日誌，以因應未來的稽核查詢[3]。

3. 設計方法

為了讓開放平台能夠安全穩定的運作，需先把管理系統之基本設定與防護到位後，再進行系統日誌蒐集。

root 帳號為最大的權限，因此建議密碼長度 8 字元，密碼中有英文、數字與特殊符號。

建議開啟的服務項目如下， atd、cpuspeed、crond、iptables、network、sshd、syslog、sysstat、xinetd，將基本開啟的服務減少，就可讓系統日誌不至於太過龐大而難以控管，另一方面也可節省系統資源，減少日後系統弱點與未來修補不至於影響應用程式運作。

系統中的密碼規則與設定檔也可以下定義設定於開放平台系統中，內容可由權責單位編寫資訊安全管理規範，一般使用者之密碼策略相當複雜，僅列舉以下提供參考，基本定義如下：
PASS_MAX_DAYS，密碼可使用天數。
PASS_MIN_DAYS，幾天內不可重新設定密碼。
PASS_WARN_AGE，密碼過期前幾天會顯示警告。
PASS_MIN_LEN，密碼最少的字元長度。
INACTIVE，密碼過期天數，未修改就鎖定帳號。
EXPIRE，密碼過期天數。
TMOUT，多少秒後自動登出。

表 1 密碼規則與閒置設定

項目	設定檔	說明
密碼規則	/etc/login.defs	PASS_MAX_DAYS=63 PASS_MIN_DAYS=7 PASS_WARN_AGE=14 PASS_MIN_LEN=8
	/etc/default/useradd	INACTIVE=7 EXPIRE=63
閒置登出	/etc/profile	Export TMOUT=1800

3.1 需求設計

因收集的資訊欄位總計約 43 個，篩選其中 15 個適用之欄位(如表 2) ，使用者可從系統選擇適合之欄位，調整適合公司特性之欄位。

表 2 建議欄位

DB Table name	說明
USERNAME	使用者名稱
SESSIONID	作業 session id
STATEMENTID	statement id
ENTRYID	entry sequence id
TIMESTAMP	執行日期時間
LOGOFF_TIME	登出日期時間
LOGON_STATUS	登入狀態(是否失敗)
ACTION_NAME	作業類型
OWNER	使用物件 OWNER
OBJ_NAME	使用物件名稱
SQL_BIND	SQL bind variable
SQL_TEXT	SQL text
OS_USERNAME	OS username
TERMINAL	terminal name
USERHOST	user host name

3.2 Log DB 資料提供方式：

可以資料庫為單位開放權限查詢，名稱規則為 $SID_AUDIT_TRAIL，例：PCCU DB 的系統日誌即為 PCCU_AUDIT_TRAIL。

使用者檢視以個人帳號登入稽核資料庫執行 SQL 語法檢視系統日誌內容[4]，資料庫上線後之維運有以下五點注意事項：

(1) Log data 減量。
(2) Log table 逐月進行壓縮。
(3) Log index 進行壓縮重建。
(4) Log data 減量與過濾，附帶產出的系統選擇(select DB)資訊不收集。
(5) Log size 壓縮減量後作業效能可同步提昇，減少系統磁碟使用過高。

3.3 Linux OS 資料提供方式：

使用 rsyslog/syslog 方式，於各開放系統中增加一筆 *.* @logsrv 即可設定完成[5]。系統日誌設定完成後呈現(如圖 1)

```
Jan 31 11:06:10 mypc sshd[6448]: SSH: Server;Ltype: Version;Remote: 192.168.1.1-64684;Protocol:
2.0;Client: PuTTY_Release_0.60
Jan 31 11:06:16 myweb sshd[6448]: Accepted keyboard-interactive/pam for ericl from 192.168.1.1 port 64684
ssh2
Jan 31 11:07:33 mypc su: - 0 ericl-oracle
Jan 31 11:12:19 mypc su: + 1 ericl-oracle
Jan 31 11:13:57 mypc sshd[6456]: SSH: Server;LType: Throughput;Remote: 172.16.1.1-64684;IN: 6932;OUT:
3168;Duration: 461.7;tPut_in: 15.0;tPut_out: 6.9

Jan 31 11:50:02 myweb ftpd[21129]: Data port : 20
Jan 31 11:50:02 myweb ftpd[21129]: FTP server (Revision 1.1 Version wuftpd-2.6.1(PHNE_38578) Fri Sep 5
12:10:13 GMT 2008) ready.
Jan 31 11:50:02 myweb ftpd[21129]: FTP LOGIN FROM mypc [192.168.1.2], testftp
Jan 31 11:50:03 myweb ftpd[21129]: FTP session closed
```

圖 1 系統日誌蒐集

作業系統的系統日誌可由系統管理者每週定期審核，平時由監控系統監控有無異常事件。如圖 2 系統日誌保存，作業系統的系統日誌產生路徑，原則上依系統預設，需另安裝 open source syslog-ng，設定將系統日誌另外抄送至獨立的系統日誌主機集中保存，以便查核，並定期查核資料完整性，優點為橫向擴充簡單。系統日誌主機每天兩次將日誌資料同步(中午 12:00 與 00:00 進行資料同步之作業) 。

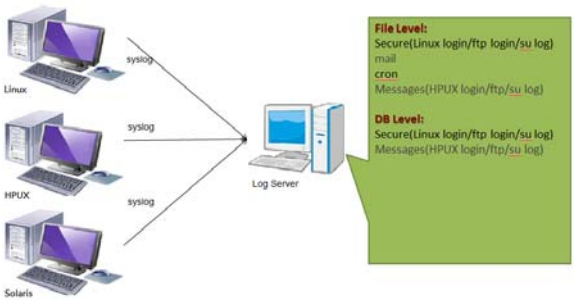

圖 2 系統日誌蒐集示意圖

4. 結論

建議可蒐集平日一般使用者的使用行為模式，在一段時間的學習後，可整理分析提供自動告警機制之參考，或是可以採用語法組合使用方式查核通用之 SQL 再提供予一般使用者參考，目前執行方式為：

(1) 登入使用系統確認有那些帳號
檢查使用 SQL 語法之帳號，是否出現特定同仁平常較少需要碰觸機密資料者，特別觀察該同仁所下的 SQL 內容是否與近期工作相關。

(2) 誰使用到資安議題的資料表(Table)或欄位
可檢查使用到哪幾個重要 TABLE 的使用者(例如主檔)，瀏覽該使用者所 SQL 語法是否與近期指派的工作有關或有需求才可使用。

(3) 特定帳號查看
針對單一用戶查詢資料的 SQL(特別是主檔)，對於查詢頻率較高的幾個帳號，可檢查前後所下的 SQL 是否在進行正常的資料驗證。

(4) 查核方式可分為 1.資料庫(DB) 2.系統主機(System Server)
1. 資料庫(DB)：登入稽核資料庫，以 SQL 查詢最近一個特定系統帳號是否有個人登入使用的記錄，若有個人以系統帳號登入之使用記錄，查核者必須訪談使用原因並加以記錄。
2. 系統主機(System Server)：以系統帳號直接登入主機，驗證是系統日誌與稽核資料庫，驗證該系統日誌是否能完整傳送至稽核資料庫。

參考文獻

[1] 陳佑寰(2011)，駭客事件不斷上演 個資保護標章制度勢在必行，http://www.mem.com.tw/article_content.asp?sn=1109140007。

[2] 鄭偉麟(2012)，資料庫稽核系統導入研究，朝陽科技大學資訊管理系研究所，碩士論文。

[3] Chris Davis,Mike Schiller(2011).IT Auditing: Using Controls to Protect Information Assets *Seminar on Enterprise Software.* http://courses.cs.ut.ee/2011/enterprise/uploads/Main/VassarReport.pdf

[4] Oracle.(2013). Introduction to Auditing, OracleR Database Security Guide12c Release 1 (12.1), from http://docs.oracle.com/cd/E16655_01/network.121/e17607/auditing.htm

[5] Red Hat.(2013).Viewing and Managing Log Files, from https://access.redhat.com/site/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Deployment_Guide/ch-Viewing_and_Managing_Log_Files.html