

加速器運轉資訊安全管理概述

黎家安、翁宗賢(光源組)

前言

進入二十一世紀網際網路的發達為人類帶來了前所未有的便利性。當我們要與他人資料交換時，可利用網路快速傳遞或接收。儀器控制也可經由網路達成。同步輻射加速器之操作就是透過網路搭起與系統控制介面的通訊聯結，藉此達到遠端控制之目的。當我們在使用遠端控制時需考慮到通訊封包交換的完整性，若通訊過程碰到阻斷可能造成封包漏失導致控制指令無法正確執行。要如何讓網路的使用不致受到干擾？最貼切的方法是導入資訊安全策略予以規範。也因此本文敘訴較著重於管理層面，以此亦可應用於與資安相關的議題上。

資訊安全的定義

首先我們要了解資訊是什麼？資訊應該是很重要的嗎？如果大眾對資訊的認知都屬於重要的，有無配合的政策可以妥善保護？根據國際著名的資訊安全管理規範BS7799的解釋“資訊是一項資產，如同企業內其他重要資產一樣，對企業有其持續地必要性，同時需要適當地被保護著”。如加速器運轉資訊所需保存的資料庫資料及加速器操作資訊安全應有的各項政策考量^[1]。

而資訊在使用及處理過程中，最大的考量是有無遺失、遭竊與被破壞，及可能有無被內部使用者不當使用呢？例如，運轉操作人員在進行電子束注射時所使用的磁格參數(operation lattice)。在正常情況下磁格參數經由射束動力小組根據儲存環目前磁鐵設定及動態調動狀態下所儲存的最佳化參數可讓注射效率達到12~17%，若此參數遭到不明更改則極有可能於

重新注射時，造成原儲存的電子束漏失與注射困難，勢必影響後續的用戶使用時間。又，如何可以達到資訊安全的標準呢？一般可依循資訊安全三要素的準則來一一解決管理上的疏失：

1. 機密性(confidentiality)
2. 完整性(integrity)
3. 可用性(availability)

如何管理好資訊安全呢？依據「行政院及所屬各機關資訊安全管理要點」有關法令，及參考「行政院及所屬各機關資訊安全管理規範」，藉由資訊安全管理制度(Information Security Management System, ISMS)資訊安全管理流程^[2]，透過合理的風險評估過程，讓組織以決定採取哪些手段來管理風險，並選擇適當機制進行。風險評估與風險管理的目的，在於透過列舉資訊資產，如前所述的運轉資訊資料庫、運轉磁格參數或是於工作站上透過人機介面的遠端控制與實體系統所做的封包交換等，皆為在加速器操作上可能面臨的潛在威脅與弱點，藉由資產價值與潛在威脅與弱點發生的機率或強度，決定該資訊資產所面臨之風險值，並由組織內部之資訊安全組織決定該臨界風險值，針對其風險值高於臨界風險值之資訊資產所面臨之潛在威脅與弱點，採取適當的控制措施，降低、預防、移轉或控制其風險在可接受的程度以內，確保資訊資產之安全，進而達到維持加速器持續運作的目的。

風險評估與管理

一旦決定建構加速器運轉資訊安全管理系統，風險管理的流程便不可避免，風險管理包含風險評估與風險控制二大步驟，然而在進入

風險管理之前，需先明確建構資訊安全管理系統的目標與範圍，訂定管理高層資訊安全政策，並著手收集相關資訊。

風險評估中之風險值取決於資產價值、威脅與弱點的關係如下：

1. 資訊資產的分類、清冊的建立與價值的訂定
2. 資產分群組
3. 威脅與弱點的評估
4. 計算風險值
5. 分析 ISMS 的企業業務需求
6. 分析 ISMS 的法律需求
7. 風險評估總結報告

在完成風險評估總結報告之後，接下來即將採取相對應的風險管理控制，但由於資訊安全的要求是沒有上限的，所以應根據本身的需求，考量自身所能承擔之風險及達到預計安全目標所需付出的成本，在安全度與資訊安全投資成本二者之間，做一最適當之考量，使其能達到資訊安全要求而發生的費用是組織可承擔的範圍。

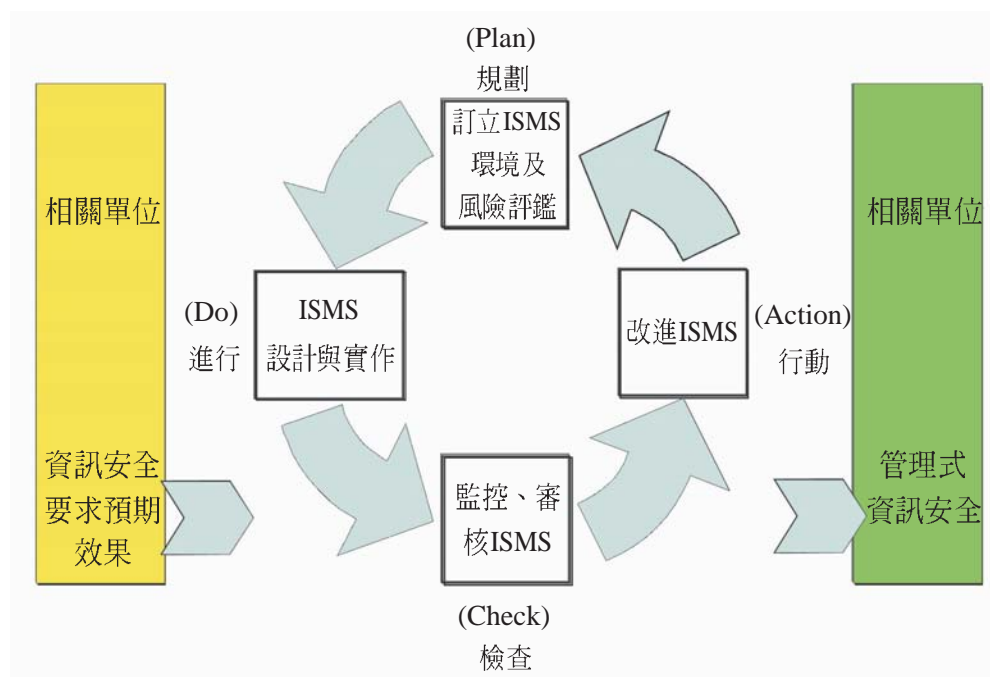
目前組內可以經由「計畫－執行－檢查－行動」(Plan-Do-Check-Act, PDCA) 模式（如圖一）不斷地循環檢查機制^[3]，建立起符合本身的資訊安全基礎架構。

總結

為確保加速器運轉經由網路遠端操控的封包交換或歷史紀錄資料庫內的資料完整，資訊安全管理策略導入是有其必要，而其導入成功的因素，最重要的是有高階管理階層的承諾，其次是系統能否符合企業的安全政策，最後是針對人員及所有使用者提供適當的資訊安全概念訓練及教育、安全意識建立、法令宣導，到進階資訊安全事件的自動即時回報系統(如防火牆、入侵偵測系統等)，以收管理及技術的完整結合。國內推行資訊安全管理政策不遺餘力。如 ISO/IEC 17799 使用者論壇聯誼會的成立，提供一個針對資訊安全管理經驗交流、相互學習及交換新知的場合，以期還給大眾一個安全無慮的網路使用空間。

參考文獻

- [1] CERT/CC Statistics 1988-2003, http://www.cert.org/stats/cert_stats.html
- [2] 劉智勇，網路通訊雜誌 **146**, 38 (2003)。
- [3] 經濟部標準檢驗局，“CNS17800 資訊安全管理規範”，**12**, 2 (2002)



圖一 PDCA 過程模式