植基於像素差值與邊緣吻合法之數位影像藏密技術

劉興漢 [a1] 林裕淇 [b] 李家明 [a]

[a] 國防大學管理學院資訊管理學系
[b] 致理科技大學創新設計學院資訊管理系

摘要

本論文所提出植基於像素差值的資訊藏密技術是使用 3×3 的區塊進行藏密，其以 9 個像素值為一組，藉由結合像素差值和邊緣吻合藏密法，最終產生 8 組像素差值，來達到藏密量的最大化，並維持可接受的 PSNR 值，實驗結果可看出本藏密技術其藏密量最高可達 808,760 bits，其 PSNR 值為 32.0283 dB，仍可被人類視覺系統所接受。為證明本論文所提方法的優越性，本論文同時進行與其他學者所提 PVD 藏密法的效能比較，實驗結果亦可看出本藏密技術的藏密量與其他學者所提方法相比較為最高，但亦可維持一定的 PSNR 值，可見本方法的優越性。

關鍵詞：藏密技術，像素差值，邊緣吻合，人類視覺系統

A Digital Image Data Hiding Scheme Based on Pixel-Value Differencing and Side-Match

Hsing H. Liu[a] Yu C. Lin[b] Chia M. Lee[a]

[a] Department of Information Management, MC, NDU, Taiwan, R.O.C.
[b] Department of Information Management, College of Innovation and Design, Chihlee University of Technology, Taiwan, R.O.C.

Abstract

This paper proposes a data hiding scheme based on the pixel-value differencing (PVD) scheme, utilizing a 3 by 3 block for hiding data while regarding nine pixel values as a group. The PVD scheme and the side match method are combined to ultimately produce eight groups of pixel-value differences, enabling maximum hiding capacity while maintaining an acceptable peak signal-to-noise ratio (PSNR). Experimental results demonstrate that the hiding capacity of this scheme can reach a maximum of 808,760 bits. Additionally, the PSNR value is 32.0283 dB, which is difficult to detect with human vision. A performance comparison with the PVD hiding schemes proposed by other scholars is conducted. The results confirm a higher capacity relative to the other methods while maintaining an acceptable PSNR, demonstrating the superiority of the proposed hiding scheme.

Keywords: Data Hiding Scheme, Pixel-Value Differencing, Side-Match, Human Visual System

[1] Email:liu.hansh@gmail.com、通訊地址：台北市中央北路二段 70 號、電話：0933915864、投稿組別：國防資訊安全。

壹、前言

近來資訊科技不斷進步，電腦與網路發展更是迅速，而多媒體等相關技術亦是蓬勃發展，文字、圖片、聲音及視訊都可在電腦的協助下轉換為數位資料，進行儲存或是快速地傳遞給接收方。而在這傳輸的過程中，也增加了機密資料曝光而被竊取的風險，安全性也大受挑戰。所以，值得信賴的資料傳輸正是目前網路科技的基本需求，而資訊安全總是衡量資訊價值的一項重要條件。

通常網路使用者經由對要傳送的資料進行加密來確保其安全性，例如資料加密標準(Data Encryption Standard, DES)、非對稱加密演算法：RSA 等方法將要傳送的資料轉換成密文，若在網路傳輸時被有心人擷取，除非有解密的金鑰，否則無法順利解開已加密的訊息。但利用資料加密的方法仍有缺點，亦即加密後的訊息內容無法清楚辨識，在利用網路傳輸的過程中，很容易被發現是在傳輸加密的重要資訊，這會引起別有心思的人士加以關注，其實是增加了有心人士想破解密碼然後進一步竊取到資料的風險。為了克服此問題，資訊安全的研究者提出了資訊隱藏(Information Hiding) (Wu and Tsai, 2003; Chan and Cheng, 2004; Chang and Huang, 2008;鐘國亮，2009)的技術。

資訊隱藏技術可把密文嵌入於平常的影像(稱為載體影像，Cover-image)，產生隱含機密訊息的藏密影像(Stego-image) (Westfeld, 2001)，藉此避免機密訊息被有心人士所發覺，完成秘密通訊。由於人類視覺系統(Human Vision System, HVS)無法察覺影像細微的改變，故藏密影像不容易被人類視覺發現有異之處，可有效增強資料傳輸過程的安全性。舉例來說，若要傳遞一個公司機密的工程設計圖片，如果我們能將欲傳遞的圖片先進行加密後，然後將加密的資訊再嵌入於藏密圖像後進行傳送。這樣就有雙重的保護，有心人士看不到亂碼，而也想不到此藏密圖像內有加密的訊息。想進行其破解就難上加難了。所以資訊隱藏技術可確保資料的機密性與安全，已是目前數位資訊時代重要的課題。

資訊隱藏技術已被廣泛的使用於所有權識別、軍事、商業和與反犯罪等相關應用中，其中最常用的是傳輸數位化資料時，將機密資料隱藏到影像當中，使得一般人從影像外觀不容易察覺到機密資料的存在，並且可以在需要時能將機密資料完整的抽取出來。而影像就是所謂載體。在藏入秘密資料之前的影像稱為載體影像，而藏入資料後的影像稱為藏密影像(楊勝凱和黃炳森，2012)。目前，有很多種多媒體類型都被拿來當作載體影像如數位影像、聲音、視訊影片等(吳南益等，2010)。其中，大部分的資訊隱藏技術大都以數位影像為主要選擇，這是因為使用數位影像來嵌入訊息具有三項優點。首先是「來源取得方便」，數位影像的檔案類型是日常生活中是一件極易取得之多媒體物件，在網際網路上就可以搜尋到成千上萬張的圖片檔案可自由下載，換言之，在網路上看到一張數位影像在傳送是一件極為平常的事情。其次為「數位影像的可塑性極高」，如一張灰階影像的像素值是由 8 個位元所組合而成的，但若只修改一個最低位元的數值，則該像素值的變化幅度最多是 0 變成 1 或是 1 變成 0，這樣很難被人類視覺所察覺到影像變化。最後為「影像失真性與訊息隱藏量容易評估與控制」，由於過去已經發展出許多種影像品質失真性評估方法，如高峰影像信號雜訊比（Peak Signal-to-Noise Ratio, PSNR）公式即為其中一種，因此要預估隱藏量與控制失真性大小，在數位影像檔案上是一件很容易的事。

一個秘密的資訊隱藏流程是發送方先將秘密資料嵌入載體影像後成為藏密影像，然後透過網路方式將藏密影像傳遞給接收方，接收方在接收後再從藏密影

像中把秘密資料抽取出來，如圖 1 所示。

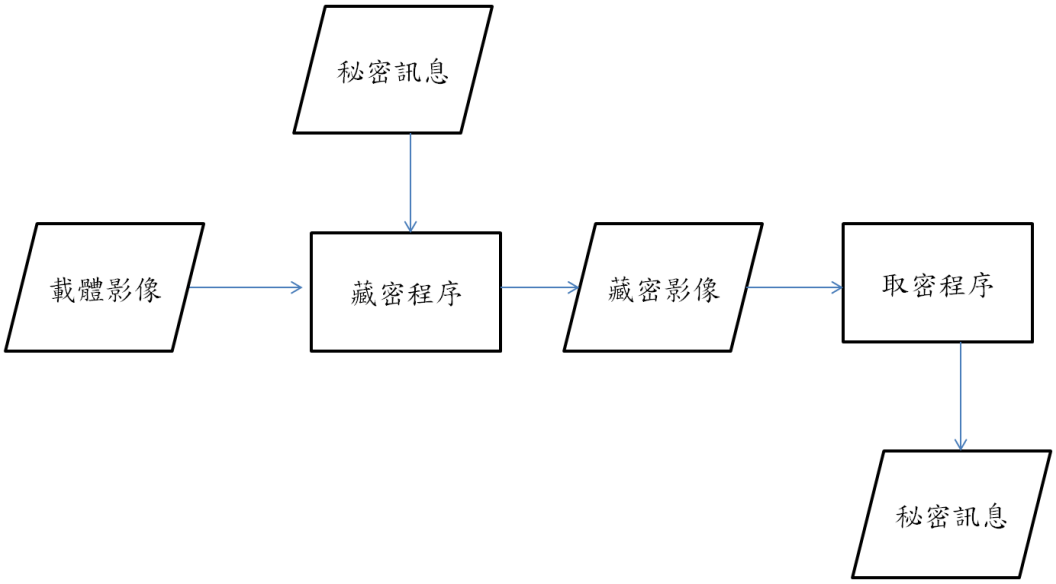


圖 1 資訊隱藏基本流程

資訊隱藏的藏密技術，依照處理方式的不同，大致可分為空間域(Spatial Domain)藏密技術及頻率域(Frequency Domain)藏密技術二種(鐘國亮，2009)。空間域的藏密技術主要是直接是將加密後的機密訊息以二進位的編碼方式嵌入於載體影像的最不重要位元（Least-Significant-Bit, LSB）(Chan and Cheng, 2004)或直接針對載體影像的像素值進行修改來達成隱藏機密資訊的目的；頻率域技術主要是把空間域中各影像的像素值轉換成頻率域的係數，再將秘密訊息隱藏在所選定的係數中，再反轉換為空間域像素值。頻率域的轉換一般都是線性的正交變換，它是以不同的角度來分析影像的能量分佈及特性(董俊良等，2002)。

若以相同影像失真率為考量，頻率域的藏密法之藏密量較空間域藏密法為低，故資訊隱藏技術的研究者大多投入於空間域藏密技術之研究。空間域藏密技術早期常用載體影像像素最不重要位元嵌入秘密訊息，此方法就是直接將 n 個位元的訊息密文，藏在影像每個像素的最後 1 個位元的位置，因此具有運算複雜度極低的優點，且在適當的藏密量下，人類視覺並不會察覺圖片的變化。但這種技術並不會考量到人類視覺對於像素與周圍之間變化的靈敏度，因為每一個像素的機密訊息嵌入位元數都是一樣多的，且今已有許多方法對最不重要位元取代藏密法有良好的偵測效果，如 x^2 偵測法(Westfeld and Pfitzmann, 1999)、RS 偵測法(Fridrich, Goljan, and Du, 2001)等。

基於以上所述，有部分學者運用人類視覺系統之概念，開發避免被統計分析軟體所檢測出來的資訊隱藏技術。Wu and Tsai 在 2003 年提出一個依據相鄰像素差值(Pixel-value Differencing, PVD)來決定藏密量大小的藏密方法，用兩兩相鄰的像素為一區塊，區塊中兩像素的差值愈大則愈可能屬於影像中紋理複雜區域；若差值越小，則可能屬於影像中的平滑區域。此隱藏機密訊息的方法是依像素差異值屬於那個區間(Range)，利用此區間的大小來判斷隱藏多少位元的藏密量。在嵌入機密訊息後會產生新的差異值，再將此新的差異值反推回去並產生新的像素值，其實驗結果證明可抵抗 RS 與 x^2 偵測法。

Wu, Wu , Tsai, and Hwang (2005)學者基於像素差值藏密法與最不重要位元取代藏密法提出了像素差值和最不重要位元取代合併法，他們認為像素差值藏密

法雖可依據影像的特徵做到藏密量的差異化，但卻浪費了部分潛在的藏密量，以他們所提出的方法，主要以像素差值為基礎，當像素差值小於某一門檻值時，直接以最不重要位元取代藏密法修改像素值來隱藏資料；若高於此門檻值時，則以像素差值藏密法來藏密，此方法在藏密後影像品質下降不多的情況下，藏密量也較像素差值藏密法為高。Yang and Huang(2011)更是基於像素差值藏密法和最不重要位元取代藏密法的方法來作進一步改善，在差值小於門檻值時使用最不重要位元取代藏密法，而大於門檻值時使用像素差值藏密法，並且在使用像素差值藏密法後再依照藏密後的像素值是否奇數偶來多藏匿 1 位元的藏密量。

Yang and Weng(2006)則用了另一種的思考方式，以四個像素為一組，用組別當中像素的最小值為基準，用像素差值藏密法來推算出其他三個的像素值，如此一來藏密量則是比原本像素差值藏密法多出許多，但其藏密影像品質也下降了不少。而 Chang, Chang, Huang, and Tu(2008)提出了以四個像素為一組，並以一對三的方式區分出三個像素差值組，然後使用與 Yang and Weng(2006)不同的選擇條件和調整像素的方法來改善 PSNR 值。

相較於 LSB 藏密法，PVD 藏密法的藏密量較高，且可避免被相關統計分析技術所偵測，因此近期以 PVD 為基礎的藏密技術(Wu, 2003；Wu, Wu, Tsai, and Hwang, 2005；Yang and Huang, 2011；Yang and Weng, 2006；Chang, Chang, Huang, and Tu, 2008)成為資訊隱藏的熱門研究領域。故本研究以 PVD 為基礎，不同像素區塊取樣為考量，並結合邊緣吻合法，提出新的空間域數位影像藏密技術。

貳、文獻探討

一、最不重要位元取代藏密法

最不重要位元取代藏密法(Chan and Cheng, 2004)是在空間域中最常見的資訊隱藏技術。其方法主要是利用人類視覺不易感受到像素微小變化之原理，所以將像素最小的幾個位元改變，以達到藏入資料之目的。我們以 1 位元密文進行最不重要位元的資訊隱藏為例：當影像的每一個像素值轉換成二進位後，最小的位元不是 0 就是 1，此時在每一個像素值中可更改與藏入的值不是 0 就是 1，所以理論上針對最小位元進行 0 或 1 的更換，實際上並不會影響整個影像品質，但如果每個像素的隱藏資料的位元過多，影像的品質將大受影響，PSNR 值會可能低於 35 或甚至低到 30 以下，故最不重要位元取代藏密法並不適用於過多位元以上的資訊隱藏，如圖 2 所示。

(a)使用 1 位元 LSB 的藏密影像 (b)使用 5 位元 LSB 的藏密影像

圖 2 使用 1 位元與 5 位元 LSB 的藏密影像比較

二、像素差值藏密法

Wu and Tsai(2003)所提出的 PVD 藏密法，主要是以兩個連續相鄰像素為主，並依照差值的大小來決定像素對的藏密量。因此，影像紋理愈平滑的區域就藏得很少，而變動量也相對地較少；若是影像紋理屬於複雜的區域，變動量相對地會比較大，則藏密量也較多，以下分別敘述其密文嵌入與取出程序。

（一）PVD藏密法密文嵌入程序

像素差值藏密法先利用兩像素之差值大小所對應的量化表(如表 1 所示)，決定出可隱藏資料的位元數，然後再進一步來調整兩像素之差值，並進而改變其像素值以達到藏入資料的目的。

表 1 差值範圍區間表

區域	差值範圍	可隱藏位元數(k)	該區域最小值(g)
1	0到7	3	0
2	8到15	3	8
3	16到31	4	16
4	32到63	5	32
5	64到127	6	64
6	128到255	7	128

步驟一：假設現在有一個灰階影像，其高度與寬度分別為M個與N個像素，則此影像總共包含了$M \times N$個像素。其中的每一個像素可以以明暗程度大小用二進位的8個位元視來作評估。將整張載體影像劃分成兩個連續相鄰像素為一組的1×2大小的子影像區塊，定義位置分別為(i, j)及$(i, j+1)$，而其所對應的像素值為 $f(i, j)$及$f(i, j+1)$ 並以Z字型的方式來掃瞄整張載體影像，每組區塊皆為不重疊。

步驟二：定義 d 為兩像素之差值$|f(i, j+1) - f(i, j)|$，則d值應介於0與255之間。差值愈大，代表該區塊位於載體影像紋理複雜區域；差值愈小，代表該區塊位於載體影像紋理平滑區域。

步驟三：把d值的可能範圍分成6個區域，分別為0到7、8到15、16到31、32到63、64到127及128到255(如表2-1)。其中每塊區域所對應的可隱藏資料位元數分別為3、3、4、5、6與7，用 k 代表可藏入之位元數量。當我們從密文資料中取出k位數，並將其二進位換算為十進位後的值定義為w，用接著將w加上該區域的最小值g 後得到d'。這為藏密後的新差值。其公式(1)為：

$$d' = w + g \tag{1}$$

步驟四：此時利用d'與d 來調整 $f(i, j)$及$f(i, j+1)$的像素值，以達到資訊隱藏之目的。依公式(2)、(3)、(4)及(5)計算出新的$f'(i, j)$與$f'(i, j+1)$。($\lceil\ \rceil$為上取整函數，$\lfloor\ \rfloor$為下取整函數) 。

Case 1：如果$f(i, j+1) \geq f(i, j)$且$d' \geq d$

$$f'(i, j) = f(i, j) - \left\lceil \frac{|d' - d|}{2} \right\rceil,\ f'(i, j+1) = f(i, j+1) + \left\lfloor \frac{|d' - d|}{2} \right\rfloor \tag{2}$$

Case 2：如果 $f(i,j+1)\geq f(i,j)$ 且 $d'<d$

$$f'(i,j)=f(i,j)+\left\lceil\frac{|d'-d|}{2}\right\rceil,\ f'(i,j+1)=f(i,j+1)-\left\lfloor\frac{|d'-d|}{2}\right\rfloor \quad (3)$$

Case 3：如果 $f(i,j+1)<f(i,j)$ 且 $d'\geq d$

$$f'(i,j)=f(i,j)+\left\lceil\frac{|d'-d|}{2}\right\rceil,\ f'(i,j+1)=f(i,j+1)-\left\lfloor\frac{|d'-d|}{2}\right\rfloor \quad (4)$$

Case 4：如果 $f(i,j+1)<f(i,j)$ 且 $d'<d$

$$f'(i,j)=f(i,j)-\left\lceil\frac{|d'-d|}{2}\right\rceil,\ f'(i,j+1)=f(i,j+1)+\left\lfloor\frac{|d'-d|}{2}\right\rfloor \quad (5)$$

步驟五：進行下一組1×2 大小的子影像區塊。

（二）PVD藏密法密文取出程序

取出機密資料的方法為則可利用反方向來進行，步驟如下。

步驟一：用已知的 $f'(i,j)$ 與 $f'(i,j+1)$ 求得 d' 如公式(6)

$$d'=|f'(i,j+1)-f'(i,j)| \quad (6)$$

步驟二：根據表1判斷 d' 是落在那一個差值範圍，求得該區域最小值 g。

步驟三：使用公式(1)，已知 d' 和 g，可求得十進位的定義值為 w。

步驟四：將十進位 w 值轉換成二進位，即可求得該1×2 大小的影像區塊所藏密的密文訊息。

三、結合像素差值與最不重要位元藏密法

Wu 等學者(2005)所提出的像素差值和最不重要位元取代合併法，主要是先計算兩個相鄰且不重疊像素之間的像素差值，然後根據此差值大小來決定藏密法。若差值小於預設之門檻值時，則使用最不重要位元取代法來改變像素值：不然，則利用像素差值法來進行藏密。

步驟一：假設現在有一個灰階影像，其高度與寬度分別為 M 個與 N 個像素，則此影像總共包含了 $M\times N$ 個像素。其中的每一個像素可以以明暗程度大小用二進位的8個位元視來作評估。將整張載體影像劃分成兩個連續相鄰像素為一組的1×2大小的子影像區塊，定義位置分別為 (i, j) 及 $(i, j+1)$，而其所對應的像素值為 $f(i, j)$ 及 $f(i, j+1)$ 並以Z 字型的方式來掃瞄整張載體影像，每組區塊皆為不重疊。

步驟二：定義 d 為兩像素之差值 $|f(i,j+1)-f(i,j)|$，則 d 值應介於0與255之間。差值愈大，代表該區塊位於載體影像紋理複雜區域；差值愈小，代表該區塊位於載體影像紋理平滑區域。

步驟三：若 d 值超過設定門檻值，則繼續用像素差值藏密法的步驟三繼續後續演算。

步驟四：若 d 值低於設定分界值，則定義藏密資料位元序列中即將要取出 6 位元數值為：$S=m1,m2,m3,m4,m5,m6$ 。

步驟五：使用 3 位元最不重要位元取代藏密法演算法，將 $m1, m2, m3$，3 位元數值將 $f(i,j)$ 替換成 $f'(i,j)$；使用 3 位元最不重要位元取代藏密法演算法，將 $m4, m5, m6$，3 位元數值將 $f(i,j+1)$ 替換成 $f'(i,j+1)$。

步驟六：依公式(6)計算新的差值 $d' = |f'(i,j+1) - f'(i,j)|$，並確認是否超過設定門檻值，如果沒有，則無需作調整的動作，但如果超過設定門檻值，則依調整公式來做調整，公式(2.7)如下：

$$\begin{matrix} f'(i,j) \\ f'(i,j+1) \end{matrix} = \begin{cases} f'(i,j)-8,\ f'(i,j+1)+8, & \text{if } f'(i,j) \geq f'(i,j+1) \\ f'(i,j)+8,\ f'(i,j+1)-8, & \text{if } f'(i,j) < f'(i,j+1) \end{cases} \quad (7)$$

步驟七：進行下一組1×2 大小的子影像區塊判斷。

楊勝凱與黃炳森(2012)提出整合像素差值法及最低位元取代法之影像藏密技術，稱為整合 PVD 與 LSB 藏密法。其藏密法與 Wu 等學者[15]提出的原始 PVD 方法相同，亦是利用修改兩個相鄰且不重疊的像素 P_i 及 P_{i+1} 之間的像素差值為基礎，計算出新的像素差值後，可得到新像素值 (P_i', P_{i+1}')。然後判斷 P_{i+1}' 像素的 LSB 值(令其為 r)是否與接續要隱藏的 1 位元資料(令其為 u)相同，此時會產生下列 4 組狀態：(r,u)=(0,0)、(0,1)、(1,0)或(1,1)。當 r 與 u 的值相同時，此時可視為已將要接續隱藏 1 位元資料嵌入 P_{i+1}'，完成這組像素的資訊隱藏動作。而當 r 與 u 的值不相同時，可分為以下情況處理。當(r,u)=(0,1)時，r 值將被修正為 1，故將 P_{i+1}' 的像素值減 1，此時為了維持新的像素差值，故將 P_i' 的像素值同步減 1。當(r,u)=(1,0)，r 值將被修正為 0，故將 P_{i+1}' 的像素值加 1，此時亦為了維持新的像素差值，故同步將 P_i' 的像素值加 1，完成這組像素的資訊隱藏動作。Yang 等學者提出的整合 PVD 與 LSB 藏密法與原始 PVD 法比較，可有效增加藏密的資訊量。

四、區塊式像素值差異法

Wu and Tsai(2003)提出了利用兩兩不重疊的像素，並利用像素的差值來嵌入機密訊息。而 Chang and Tseng(2004)提出了利用 side match 的方式來嵌入機密訊息。是利用像素與該像素側面的像素值來計算像素差值後並嵌入機密訊息，但側面的像素值並不會改變。

圖 3 為 Side Match 藏密技術示意圖，從圖 3 可以得知 70 與 80 的值固定不變，而差值與藏密的位元數與原本像素差值藏密法相同，在判斷差值落在那一個區間範圍後，利用該區間的最小值 g 加上要藏密的 k 位元數將其轉換成 w 計算出新的差值並參考公式(8)，計算出 $f'(i,j+1)$ 值，在此 $f'(i,j)$ 的數值不會變化。

$$f'(i,j+1) = \begin{cases} f'(i,j+1) = f(i,j) + d', & \text{if } f(i,j+1) \geq f'(i,j) \\ f'(i,j+1) = f(i,j) - d', & \text{if } f(i,j+1) < f'(i,j) \end{cases} \quad (8)$$

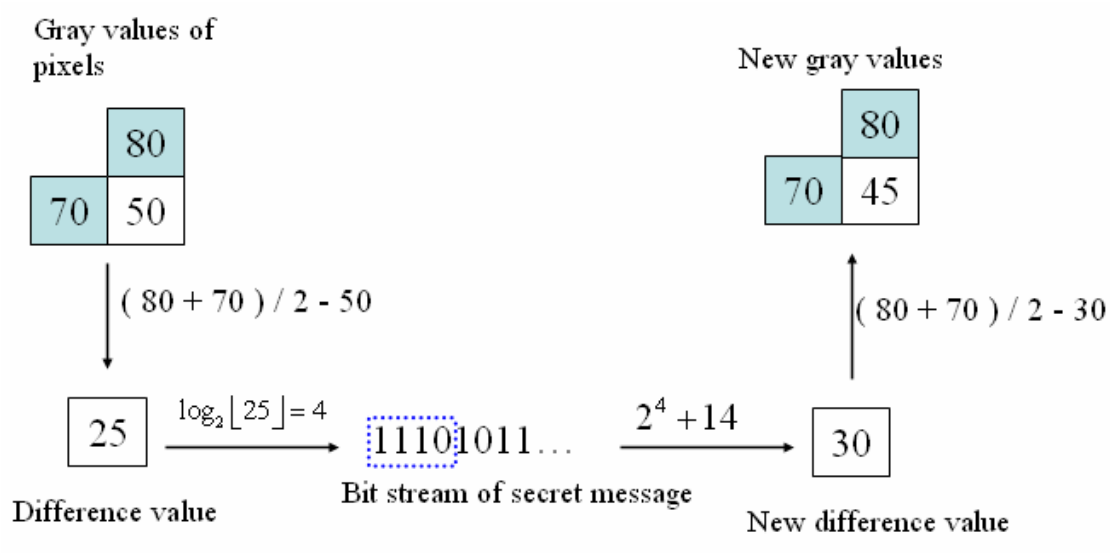


圖 3 Side Match 藏密技術示意圖

Yang and Weng(2006)這二位學者，提出了與原本像素差值藏密法兩兩相鄰方法不同出發點的方法。第一個不同點是根據新的差值並使用 Chang 和 Tseng(2004)的演算法，推算 $f'(i,j+1)$，但是 $f'(i,j)$ 的值卻是固定不變。而第二個不同點在於此方法不是抽取1×2 大小而是改抽取2×2 大小的子影像區塊，這代表了在四個區塊中，它最大可以用三個差值來嵌入機密訊息。這代表此方法的最大的藏密量會比原始的像素差值藏密法多出 1.5 倍，而在此 Yang and Weng(2006)的實驗結果是 1.44 倍。Yang 與 Weng 的方法描述如下。

在抽取 2×2 大小的子影像區塊後，定義位置分別為 (i,j)、$(i,j+1)$、$(i+1,j)$ 及 $(i+1,j+1)$。將像素值轉換成十進位，並比較大小。在此四個像素值中，找出最小的值，定義成 P_0，並用順時鐘的方式，依序定義 P_1、P_2 與 P_3，如圖4所示。定義完成後，以 P_0 為基礎點，計算出與 P_1、P_2 與 P_3 的差值。並定義為 D_1、D_2 與 D_3。並參照表1(在此方法中，差值如果為0不借位)，用可藏密的位元數與區間最小值，計算出新差值 D_1'、D_2' 與 D_3'。因為 P_0 是最小值，所以參考公式(8)就可以計算出新的 P_1'、P_2' 與 P_3'。$P_1'=P_0+D_1'$、$P_2'=P_0+D_2'$、$P_3'=P_0+D_3'$。實驗的結果雖然藏密量上升，但影像品質下降，所以最後Yang與Weng利用像素調整的改善方法，希望能最小化每一個像素改變的值來進一步改善影像品質，該方法為 $(P_0-P_0')^2+(P_1-P_1')^2+(P_2-P_2')^2+(P_3-P_3')^2$ 求最小化後統一調整 P_0'、P_1'、P_2' 與 P_3'。

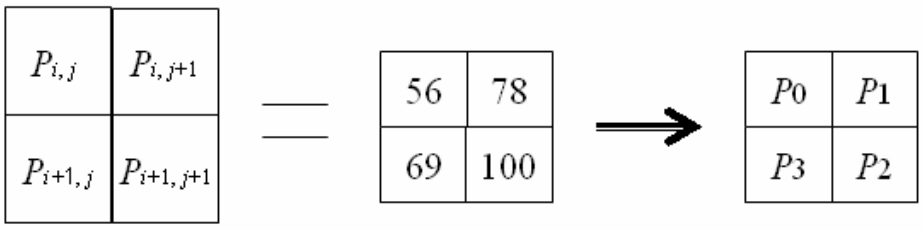


圖 4 區塊像素值命名規則

Chang 等學者(2008)學者為有效增加藏密量及改善像素值邊界溢出問題，提出 Tri-way PVD 藏密法，將用於藏密的像素區塊大小由1×2 更改成2×2，並計算 4 個相鄰像素間的差值。如圖 5 所示，四個相鄰像素定義為 $P(i,j)$ $P(i,j+1)$ $P(i+1,j)$ $P(i+1,j+1)$，而 P_0 可定義 $P(i,j)$ 與 $P(i,j+1)$ 之間的差值，P_1 定義為 $P(i,j)$ 與 $P(i+1,j)$ 的差值，P_2 定義為 $P(i,j)$ 與 $P(i+1,j+1)$ 的差值，P_3 為 $P(i+1,j)$ 和 $P(i+1,j+1)$ 之間的差值。

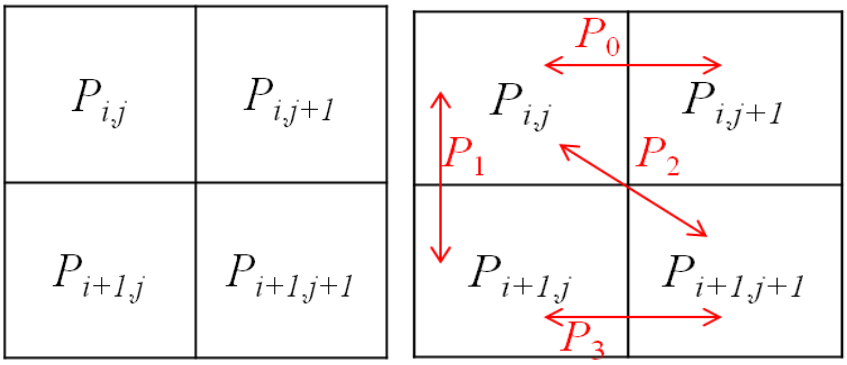


圖 5 2×2 像素區塊定義圖

雖然 Chang 等學者(2008)提出的方法是可行的嵌入大量機密數據，但嵌入大量的位元數會是引起影像容易失真。在此設計了以下兩個條件，以避免影像過多的變化。根據表 2-1，進行差值範圍區間內確認可藏密的機密訊息位元數的確認。為避免區塊藏密訊息位元數過多，影響藏密影像之品質，Chang et al.學者設定以下 2 組 Case：

Case A：embed_bit(P_0)≧5 且 embed_bit (P_1) ≧4
Case B：embed_bit(P_0)<5 且 embed_bit (P_2) ≧ 6

如果滿足差值滿足 Case A 或 Case B 其中之一的條件，表示此區塊藏密訊息位元數過多。在此不進行 Tri-way PVD 藏密法，而改使用原始的像素差值藏密法。即只操作二組差值 P_1 與 P_3 後，進行像素差值藏密法，計算出新差值 P_0' 後根據公式(2)~(5)推算出新的 $P'(i,j)$ 和 $P'(i,j+1)$ 與新差值 P_3' 後推算出新的 $P'(i+1,j)$ 和 $P'(i+1,j+1)$。但如果不符合這二個條件的情況下，在此 Chang(2008)會分別計算出 P_0，P_1，P_2。並進行三組機密訊息的嵌入動作。這時可能會產生 3 組不同的 $P'(i,j)$ 的數值。所以此演算法會將此三組的 $P'(i,j)$ 進行調整。在此定義 M 為舊差值與新差值的變化量。並進行 M_0、M_1、M_2 的計算，公式(9)為

$$M_i = P_i' - P_i \text{，} i \in [0,2] \tag{9}$$

可能的結果：

Case 1：M_i 的數值都大於 1 或都小於 -1。就選取絕對值最大的那一組，作為代表組。而其他二組數據依代表組作像素值的調整。

Case 2：如果 M_i 當中有正數和負數，選擇正負數數量多的那一組，並選擇當中的絕對值最小值為代表組。

Case 3：如果 M_i 當中有 0 的話，選擇 0 那組為代表組。

Case 4：如果有多個 0 的話，任選其中 1 個 0 為代表組。

參、研究方法

一、本研究所提方法之藏密程序

本研究的改良型藏密法是以像素差值藏密法(Wu and Tsai, 2003)為基礎，而不用最不重要位元取代藏密法來作改良。是因最不重要位元取代藏密法雖然藏密量高但至今已有許多方法對此藏密法有良好的偵測效果。雖然 Wu et al.(2005)和 Yang and Huang(2012)都有提出像素差值與最不重要位元藏密法的整合藏密法，但演算方式都是以相鄰像素的差值設定條件後並作篩選，並根據篩選結果選取像素差值或是最不重要位元藏密法進行藏密。但不管篩選的結果為何，其藏密影像還是會有明顯的最不重要位元藏密法特徵，很容易被偵測出來。

本研究的改良型藏密法是區塊式像素差異法為基礎，但有別於先前是用 2×2 的區塊(Yang and Weng, 2006)、(Chang et al., 2008)，而創新改良成 3×3 的區塊。並以 9 個像素值為一組，希望用像素差值藏密法(Wu and Tsai, 2003)和 Side match(Chang and Tseng, 2004)的方法進行整合，最終產生 8 組像素差值，來達到藏密量的最大化。

本研究的改良型藏密法先將整張載體影像劃分成連續相鄰像素 3×3 大小為一組的子影像區塊，則該 3×3 的陣列如圖 6 所示：

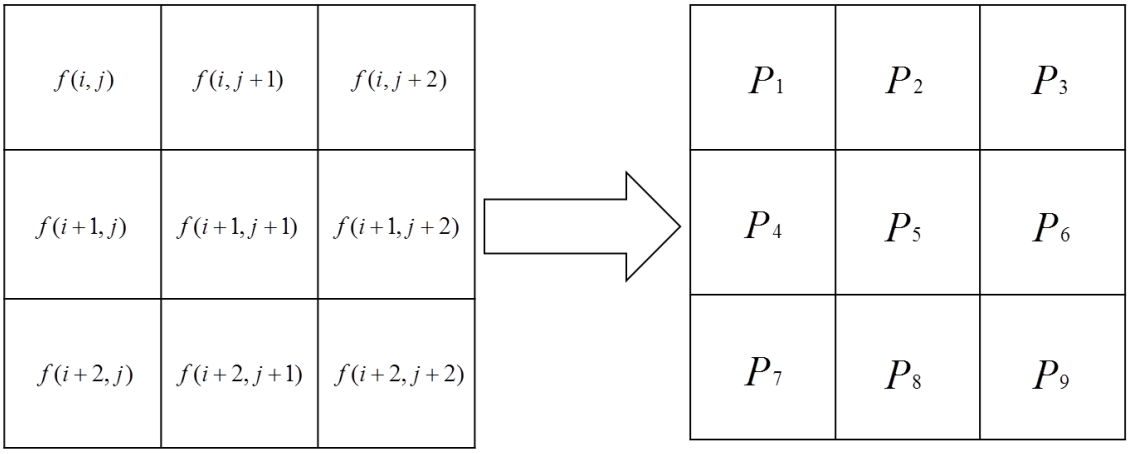


圖 6 3×3 像素陣列示意圖

其像素值：$f(i,j)$ 至 $f(i+2,j+2)$ 在此定義為 P_1 - P_9。此方法的前半段是用 P_5 為基準點，用差值公式(10)計算差值。

$$d = |P_5 - P_X| \quad X \in [2,4,6,8] \tag{10}$$

用 P_5 與周圍 4 個像素進行計算，並配合像素差值藏密法的差值範圍區間表，來進行前 4 組機密資料的藏密。如圖 7 的黃色區域所示：

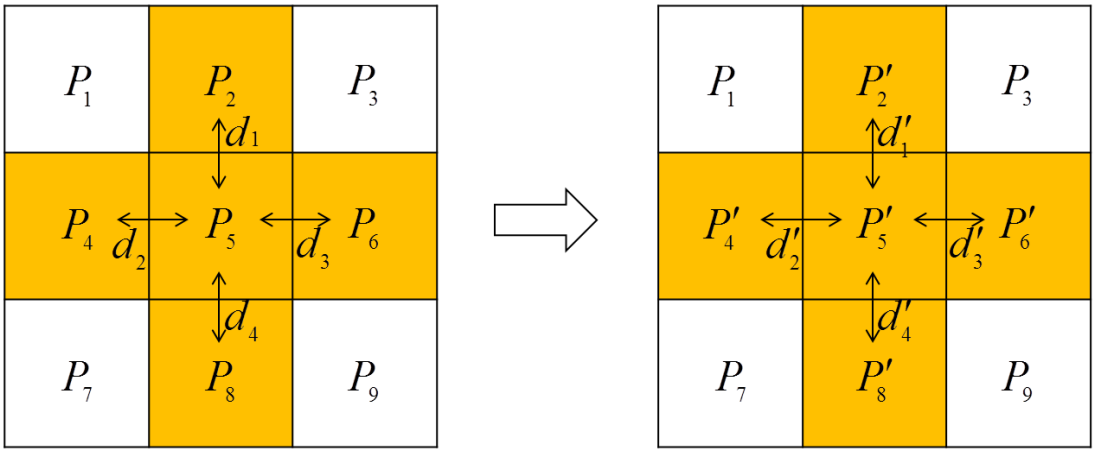


圖 7 前半段藏密程序示意圖

會得到新差值 d_1'、d_2'、d_3'、d_4'，在此使用公式(11)的像素調整方法。在此定義 M 為舊差值與新差值的變化量。並進行 M_1、M_2、M_3、M_4 的計算。

$$M_i = d_i' - d_i \text{，} i \in [1,4] \tag{11}$$

出現的結果可能為：

Case 1：M_i 的數值都大於 1 或都小於 -1。就選取絕對值最大的那一組，作為代表組。而其他三組數據依代表組作像素值的調整。

Case 2：如果 M_i 當中有正數和負數，選擇正負數數量多的那一組，並選擇當中的絕對值最小值為代表組。

Case 3：若正數和負數的數量相同，選擇進行全部的加總，若為正數，則選取正數當中的最小值，若為負數，選負數絕對值最小值為代表組。

Case 4：如果 M_i 當中有 0 的話，選擇 0 那組為代表組。

Case 5：如果有多個 0 的話，任選其中 1 個 0 為代表組。

從這四對當中選取最佳化的組合，來固定藏密後的 P_5' 值，並可計算出 P_2'、P_4'、P_6'、P_8'。此時前半段藏密步驟結束，進行後半段藏密步驟。因已知 P_5'、P_2'、P_4'、P_6'、P_8' 可用 Chang and Tseng(2004)學者提出的 side match 的方式。用已知 P_2' 和 P_4' 二數值的平均數與 P_1 進行差值運算並定義為 d_5，用已知 P_2' 和 P_6' 二數值的平均數與 P_3 進行差值運算並定義為 d_6，用已知 P_4' 和 P_8' 二數值的平均數與 P_7 進行差值運算並定義為 d_7，用已知 P_6' 和 P_8' 二數值的平均數與 P_9 進行差值運算並定義為 d_8，此時用 d_5 到 d_8 進行後半段 4 組的機密資料嵌入，會得到新的 d_5' 到 d_8'，並依據演算法計算出新的 P_1'、P_3'、P_7' 與 P_9'。如圖 8 黃色區域所示。

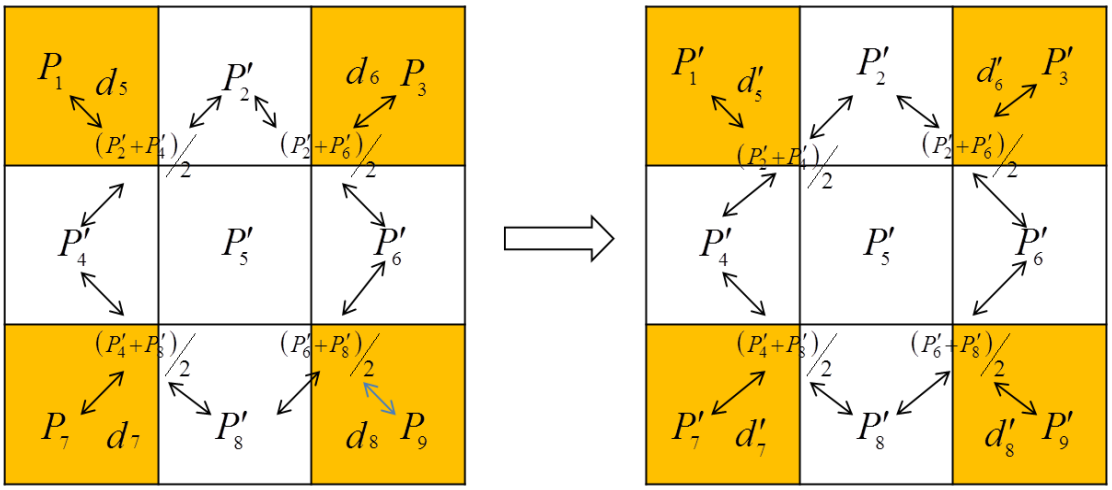


圖 8 後半段藏密程序示意圖

當需要抽取機密資料時。可以用 P'_5 與周圍 8 個像素 P'_1 到 P'_9 計算出 d'_1 到 d'_8，根據區間差值表求得區間最小值 g 並利用差值公式(12)，計算出 w 值，並進一步轉換成二位元的藏密資料。

$$d'_i = w_i + g_i \quad i \in [1,9] \tag{12}$$

本研究所提藏密方法之詳細步驟如下說明，程序圖如圖 9 所示。

步驟一：將整張載體影像劃分成連續相鄰像素為一組的 3×3 大小的子影像區塊，並以 Z 字型的方式來掃瞄整張載體影像，每組區塊皆為不重疊。

步驟二：使用公式(10)用 P_5 分別與 P_2、P_4、P_6、P_8 進行差值運算，並得到 d_1、d_2、d_3、d_4 值。

步驟三：參照表 2 與公式(12)，進行第一階段藏密程序。在第一階段的藏密程序中，總共可藏密 4 組機密資料後。計算出新的像素差值。可以得到新差值 d'_1、d'_2、d'_3、d'_4。

表 2 本研究所提方法使用差值範圍區間表

區域	差值範圍	可隱藏位元數(k)	該區域最小值(g)
1	0到7	3	0
2	8到15	3	8
3	16到31	4	16
4	32到63	5	32
5	64到95	5	64
6	96到127	5	96
7	128到159	5	128
8	160到191	5	160
9	192到223	5	192
10	224到255	5	224

步驟四：進行像素調整步驟，參考公式(11)，進行M_1、M_2、M_3、M_4的計算。並進行篩選的動作。在決定P_5'後，利用已知的d_1'、d_2'、d_3'、d_4'與公式(13)計算出P_2'、P_4'、P_6'、P_8'。

$$d' = \left|P_5' - P_X'\right| \quad X \in [2,4,6,8] \tag{13}$$

步驟五：檢查計算出來的像素值P_5'、P_2'、P_4'、P_6'、P_8'是否溢位(即數值大於255 或小於 0)。如果沒有溢位則進行步驟九，如果發現有溢位的情況下則進行步驟六。

步驟六：對該組像素值(P_5'、P_2'、P_4'、P_6'、P_8')進行第一階段溢位處理方法。

步驟七：再次檢查該組像素值(P_5'、P_2'、P_4'、P_6'、P_8')是否溢位。如果沒有溢位則進行步驟九，如果發現有溢位的情況下則進行步驟八。

步驟八：對出現溢位狀況的像素值進行第二階段的溢位處理方法。

步驟九：此時完成 4 組藏密，且P_2'、P_4'、P_5'、P_6'、P_8'已固定，不再變化。將進行第二階段後半段 4 組的資料藏密程序。用已知P_2'和P_4'二數值的平均值與P_1進行差值運算並定義為d_5，用已知P_2'和P_6'二數值的平均值與P_3進行差值運算並定義為d_6，用已知P_4'和P_8'二數值的平均值與P_7進行差值運算並定義為d_7，用已知P_6'和P_8'二數值的平均值與P_9進行差值運算並定義為d_8。

步驟十：最後參考表 2 與公式(12)，進行後半段藏密步驟，計算出新差值d_5'到d_8'，並用公式(14)：計算出P_1'、P_3'、P_7'與P_9'。

$$P_x', x \in [1,3,7,9] = \begin{cases} P_x' = \text{側邊平均值} - d', \text{當側邊平均值} \geq P_x \\ P_x' = \text{側邊平均值} + d', \text{當側邊平均值} < P_x \end{cases} \tag{14}$$

步驟十一：檢查計算出來的像素值P_1'、P_3'、P_7'、P_9'是否溢位。如果沒有溢位則進行步驟十三，如果發現有溢位的情況下則進行步驟十二。

步驟十二：對出現溢位狀況的像素值進行第二階段的溢位處理方法。

步驟十三：該區塊藏密步驟結束。

步驟十四：進行下一組藏密作業，若密文已嵌入完畢或無須進行下一組的藏密作業時，則完成載體影像全圖藏密程序。

至此整張圖片的藏密動作結束，在每一區塊中都可藏密 8 組訊息，且都經過像素調整和溢位的檢查和處理，藏密量可大幅的提升且有效降低錯誤的發生。

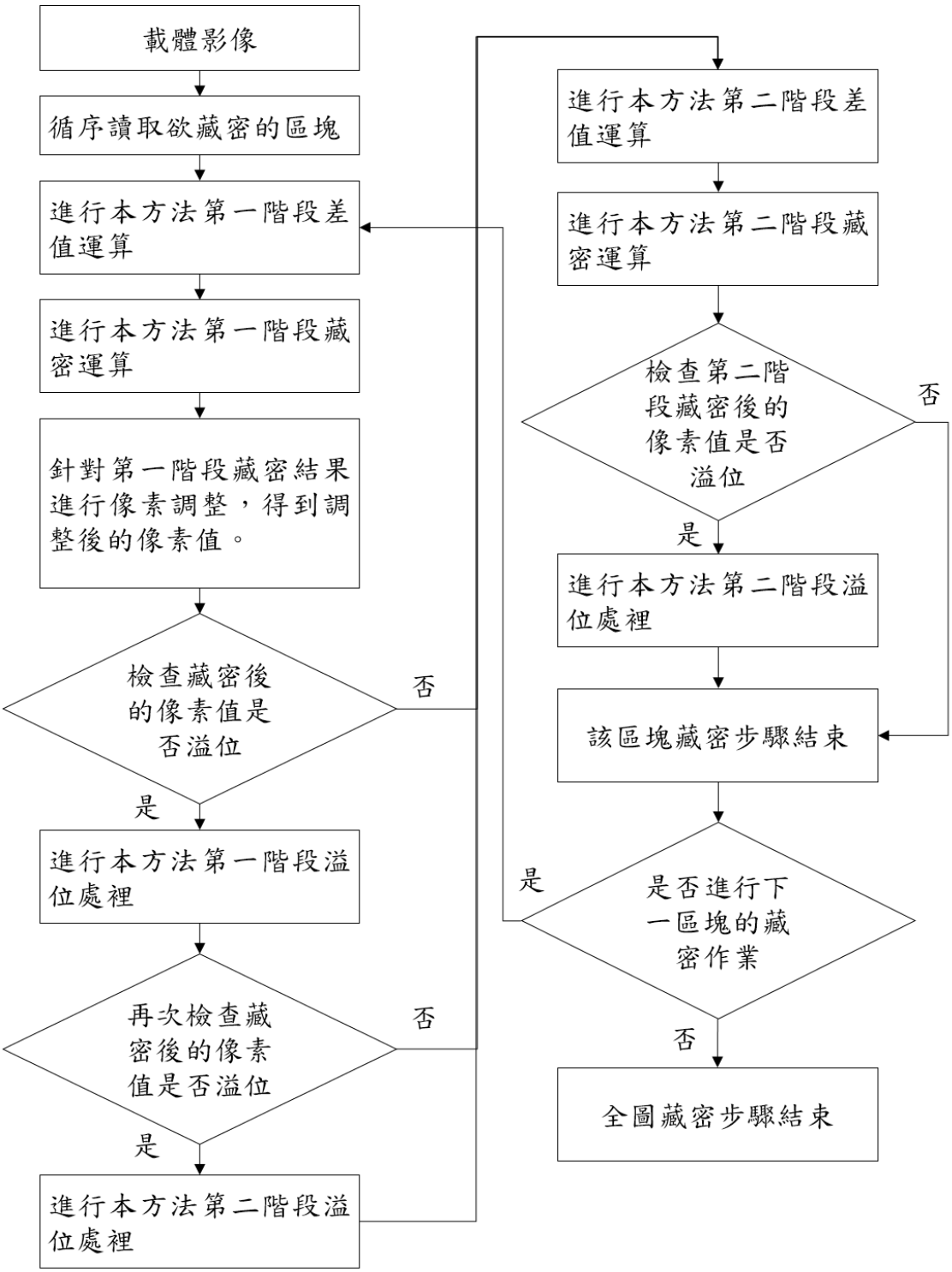


圖 9 本研究所提藏密方法之詳細程序圖

二、本研究所提方法之取密程序

步驟一：取出連續相鄰像素為 3×3 大小的子影像區塊，並以 Z 字型的方式來掃瞄整張載體影像，每組區塊皆為不重疊。

步驟二：進行本方法第一階段取密之差值計算步驟(計算出前半段的 4 組差值)，如圖 10 黃色區域所示。利用公式(15)計算出 d_1'、d_2'、d_3'與 d_4'。

$$d' = \left| P_5' - P_X' \right| \quad X \in [2,4,6,8] \tag{15}$$

步驟三：進行本方法第一階段取出密文運算步驟，根據差值範圍區間表和公式(12)，可計算出 w_1、w_2、w_3、w_4，並將這四組數值轉換成二進位，即完成前半段取密程序。

步驟四：進行本方法第二階段取密之差值計算步驟(計算出後半段取密步驟的 4 組差值)，如圖 10 灰色區域所示。P_2' 和 P_4' 二數值的平均數與 P_1' 進行差值運算並定義為 d_5'，P_2' 和 P_6' 二數值的平均數與 P_3' 進行差值運算並定義為 d_6'，P_4' 和 P_8' 二數值的平均數與 P_7' 進行差值運算並定義為 d_7'，P_6' 和 P_8' 二數值的平均數與 P_9' 進行差值運算並定義為 d_8'。

步驟五：進行本方法第二階段取出密文運算步驟，在已知 d_5'、d_6'、d_7' 與 d_8' 的情況下，配合差值範圍區間表和公式(12)可計算出 w_5、w_6、w_7、w_8，並將這四組數值轉換成二進位，即完成前後段取密程序。

步驟六：確認是否要進行下一組 3×3 的取密程序，如果有則重新進行取密流程，如果沒有下一組則完成藏密影像全圖取密步驟。

本研究所提藏密方法之取出密文詳細程序圖如圖 11 所示。

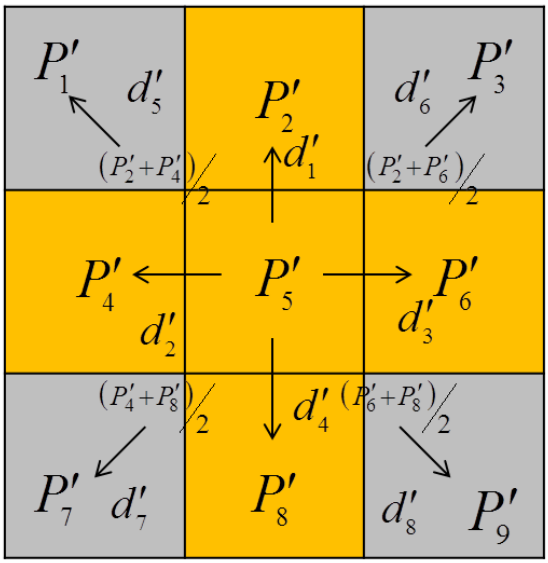


圖 10 取出密文時 3×3 陣列像素圖

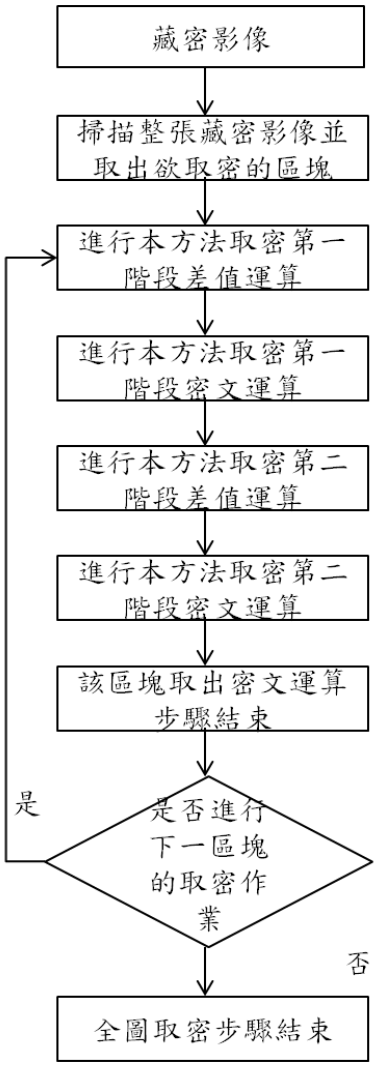


圖 11 本研究所提藏密方法之取出密文詳細程序圖

三、本研究所提方法之溢位處理程序

步驟一：在第一階段藏密結束後，檢查該區塊的像素值是否溢位，如果沒有溢位則進行第二階段的差值運算及藏密作業，如果發現有溢位情況下則進行第一階段的溢位處理。

步驟二：進行第一階段的溢位處理，若有像素值大於 255，將其最大值調整至 255，而其他像素值同步減值。如果發現像素值小於 0，將最小值調整至 0，將其他像素值同步加值。

步驟三：針對經過第一階段溢位處理後的像素值重新檢查是否溢位。如果沒有溢位則進行第二階段的差值運算及藏密作業，如果發現有溢位情況下則進行第二階段的溢位處理。

步驟四：進行第一階段的溢位處理，針對溢位的像素值進行差值的正負值反向計算。

步驟五：二階段溢位處理都已完成，將進行後續的藏密流程。

而在前半段藏密時，如果發生溢位的狀況。會先進行第一階段的溢位處理，在處理過後會針對已完成藏密的像素值，再次進行檢查。檢查是否有溢位問題。如果有，則針對該溢位的像素值進行第二階段的溢位處理。而最後的目標是確保

像素值在合理範圍內且新差值維持不變。

但在第二階段藏密時，一樣有可能發生溢位的狀況，但如果進行第一階段的溢位處理方法，根據公式(14)：P'_x 和側邊平均值都要同步調整。這會發現側邊平均值需要進行調整，這會導致第一階段藏密的差值就會異動。這在進行取密程序時就會發生錯誤。但如果同步調整 P'_5 、P'_2 、P'_4 、P'_6 、P'_8 ，則雖然可以確認第二階段的新差值維持不變，但有可能會將原本沒有溢位的數值改變(第一階段藏密處理完成的像素值)，這會發現第一階段藏密程序的溢位處理是白做工。而且如果要回到第一階段藏密程序重新處理溢位問題，這會導致整個藏密流程的混亂。所以在第二階段藏密程序中，僅會進行第二階段的溢位處理。本研究所提方法之溢位處理程序如圖 12 所示。

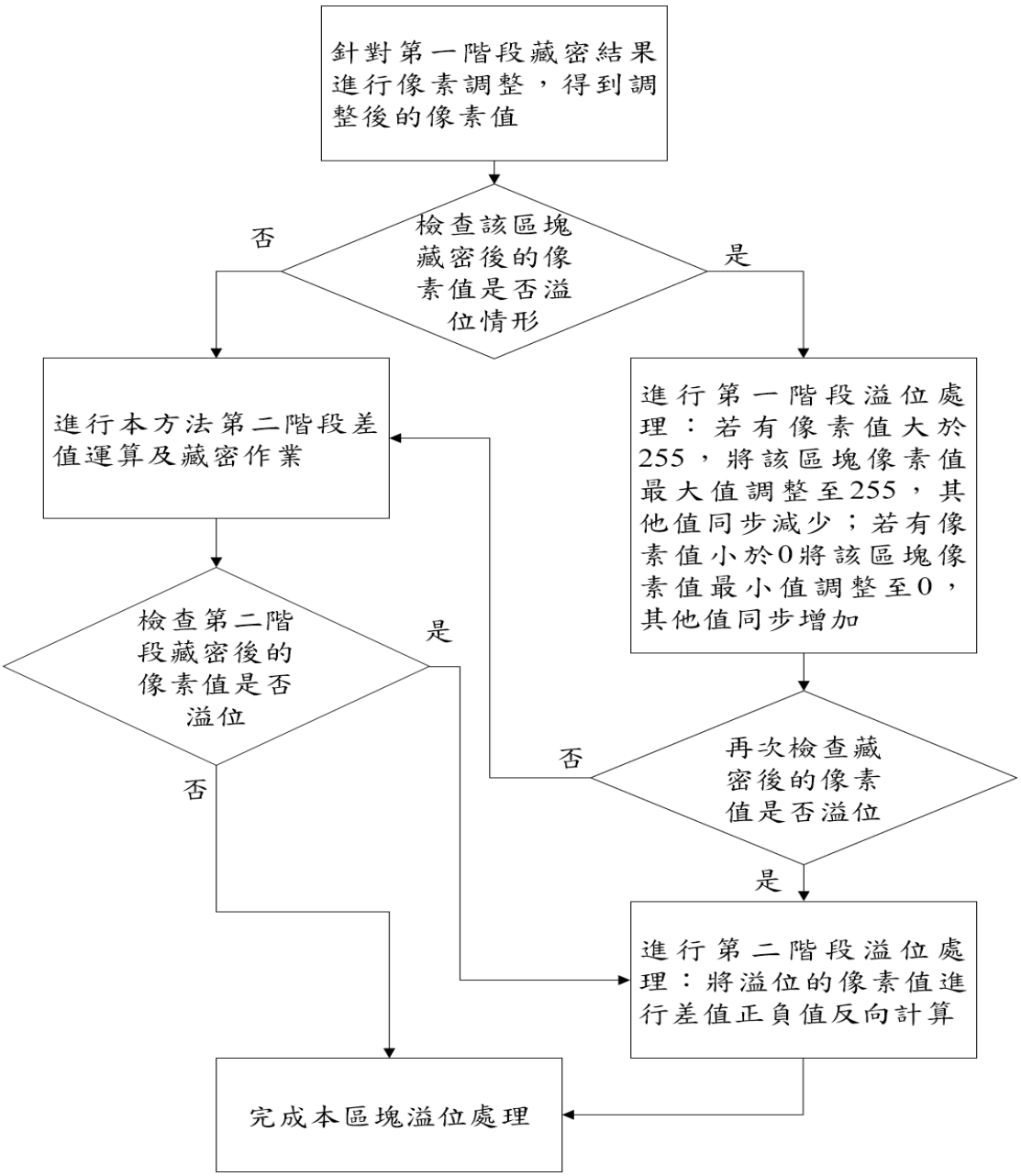


圖 12 本研究所提方法之溢位處理流程圖

肆、實驗結果與討論

一、實驗環境與測試標準

在演算法測試之實驗階段，本研究使用 MATLAB 軟體為工具、電腦硬體為 Intel(R) Core(TM) CPU i5-6400 16GB 的 RAM。測試圖像為八張尺寸為 512×512 的灰階影像(babara、boat、f16、goldhill、lena、mandrill、peppers、tiffany)，如圖 13 所示。

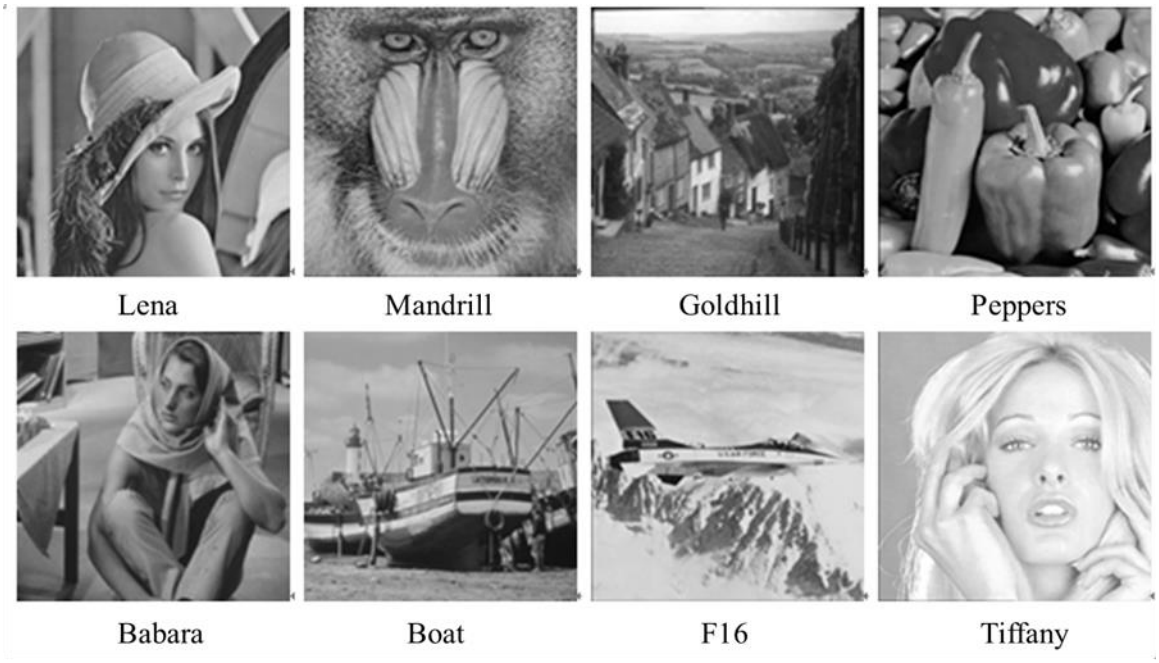


圖 13 八張測試圖片

藏密的密文為 MATLAB 的亂數指令產生，並執行 100 次亂數資料的平均值並驗證密文是否正確。如 3.1 節的說明，參照 PVD 藏密方法設計為十個像素差值域：$R_1 \in [0,7]$、$R_2 \in [8,15]$、$R_3 \in [16,31]$、$R_4 \in [32,63]$、$R_5 \in [64,95]$、$R_6 \in [96,127]$、$R_7 \in [128,159]$、$R_8 \in [160,191]$、$R_9 \in [192,223]$ 及 $R_{10} \in [224,255]$ 的範圍區間，而密文是由隨機亂數所組成的 2 進位數字資料。在藏密影像中評失真性評估方面，本研究採用了影像信號雜訊比（Peak Signal-to-Noise Ratio, PSNR，其單位為 dB），其計算公式如下：

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \text{ (dB)} \tag{15}$$

$$MSE = \left(\frac{1}{m \times n} \right) \sum_{i=1}^{M} \sum_{j=1}^{N} \left(p_{ij} - q_{ij} \right)^2 \tag{16}$$

$m \times n$ 為影像大小，i、j 代表圖片中的座標位置，p 代表藏密前的載體影像、q 代表藏密後的藏密影像，而 PSNR 數值以 30 以上為容許範圍，40 以上的值則幾乎與原圖無視覺差異。

二、實驗結果分析

如表 3 所示(PSNR 單位為 dB、藏密量單位為 bits)，可比較出 PVD 藏密法(Wu and Tsai, 2003)、TPVD(Chang et al., 2008)、Integrate PVD and LSB(楊勝凱、黃炳森, 2012)與本研究方法的藏密量與像素品質，雖然 PSNR 的數值比上述三種 PVD 藏密法還低，但還是在容許範圍之上。而藏密量大約為原 PVD 藏密法的 1.66 倍以上，與 TPVD 藏密法相比，效率提升約 17.5%、與 Integrate PVD and LSB 方法相比，效率提升約 33%。這顯示在維持一定水準的影像品質之時，本研究方法的藏密量優於其他三種方法。

表 3 本研究所提方法與其他 PVD Method 結果比較

測試影像	PVD Method		TPVD Method		Integrate PVD and LSB		本研究方法	
	PSNR	藏密量	PSNR	藏密量	PSNR	藏密量	PSNR	藏密量
Babara	38.2991	447300	35.0087	637340	35.8	584319	33.5597	764388
Boat	40.7588	416972	36.2228	623361	39.4	549304	35.874	724317
F16	41.4806	408742	36.753	613438	40	540906	36.1949	717511
Goldhill	41.4353	411509	36.5662	621216	40.62	542968	36.2306	720274
Lena	41.689	409269	37.3461	609259	40.7	540879	36.7029	712168
Mandrill	38.2005	454514	33.4261	674924	36.76	588177	32.0283	808760
Peppers	41.9673	406606	37.3744	608406	40.31	538715	34.8327	713062
Tiffany	41.8875	406543	37.4942	606786	40.43	538437	35.9074	709758

伍、結論

資訊隱藏技術的二項重要考量因素，其中是藏密量，另一是影像品質和完整性，而這二項是無法同時達到的，勢必是犧牲某一個因素，而專心追求另一個。本研究方法是空間域中的像素差值藏密法與 side-match 的整合，並改良調整像素方法和改善處理溢位問題的方法。在隱藏資料的最大化上，且在像素品質、溢位問題處理上能夠保持一定水平之上，這已透過本論文中的實驗結果得到驗證。

而與之前 PVD 相關的研究相比較，不管是區塊式的藏密法(TPVD)或是 Yang and Huang(2012)所提出 Integrate PVD and LSB 方法在藏密量的提升上，本研究所提方法均較為優越，就實驗結果而論，本研究的方法已達到藏密量的最大化。

未來建議能夠依本研究成果為基礎，研究更好的改善項目、更佳的像素調整方式。或是可朝向其他空間域的藏密技術的整合：如(A High Quality Steganographic Method with Pixel-Value Differencing and Modulus Functions：HPVD)(Wang et al., 2008)、植基於像素差值與模數函數之新型灰階影像資料隱藏技術(吳南益等，2010)：此二法都有較高的像素品質。而混合式的高容量空間域資訊藏密法(婁德權和賀盛志，2011)則有比原 PVD 方法較高的藏密量。透過相關領域的研究與方法上的整合，來進一步得到更好的影像品質與藏密量的結果與改良方法。

參考文獻

中文部分

吳南益、傅國欽、王宗銘，2010，植基於像素差值與模數函數之新型灰階影像資料隱藏技術，*網際網路技術學刊*，第十一卷・第七期：1071～1081頁

洪維恩，2013，*MATLAB程式設計*，旗標出版股份有限公司。

張智星，2010，*MATLAB程式設計入門篇*，碁峰資訊。

婁德權、賀盛志，2011，混合式的高容量空間域資訊藏密法，NCS全國計算機會議。

楊勝凱、黃炳森，2012，整合像素差值法及最低位元取代法之影像藏密法，*中正嶺學報*，第四十一卷・第二期：89～98頁。

鐘國亮，2009，*影像處理與電腦視覺導論*，東華書局。

董俊良、王偉華、廖琇怡、王贊鎮，2002，頻率域影像轉換之分析與比較，*勤益學報*，第二十卷・第二期：483～493頁。

英文部分

Chang, C.-C., and Tseng, H.-W. 2004, A Steganographic Method for Digital Images Using Side Match, *Pattern Recognition Letters* (25:12), pp. 1431-1437.

Chan, C.-K., and Cheng, L.-M. 2004, Hiding Data in Images by Simple LSB Substitution, *Pattern Recognition* (37), pp.469-474.

Chang, K.-C., Chang, C.-P., Huang, P.-S., and Tu, T.-M. 2008, A Novel Image Steganographic Method Using Tri-way Pixel-value Differencing, *Journal of Multimedia*(3:2), pp. 37-44.

Fridrich, J., Goljan, M., and Du, R. 2001, Reliable detection of LSB steganography in grayscaleand color images, *Proceedings of ACM, Special Session on Multimedia Security and Watermarking*, pp. 27-30.

Wang, C.-M., Wu, N.-I., Tsai, C.-S., and Hwang, M.-S. 2008, A High Quality Steganographic Method with Pixel-Value Differencing and Modulus Functions, *The Journal of Systems and Software* (81), pp. 150–158.

Westfeld, A. 2001, F5-A Steganographic Algorithm:High Capacity Despite Better Steganalysis *Proc. 4th Int'l Workshop Information Hiding*, *Springer-Verlag* (2137), pp. 289–302.

Westfeld, A., and Pfitzmann, A. 1999, Attacks on steganographic systems, *Proceedings of the 3rd International Workshop on Information Hiding*, pp. 61-76.

Wu, D.-C. and Tsai, W.-H. 2003, A steganographic method for images by pixel-value differencing, *Pattern Recognition Letters* (24), pp. 1613-1626.

Wu, H.-C., Wu, N.-I., Tsai, C.-S., and Hwang, M.-S. 2005, Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods, *IEE Proceedings on Vision, Image and SignalProcessing* (152:5), pp. 611-615.

Yang, C.-H., Weng, C.-Y. 2006, A Steganographic Method for Digital Images by Multi-Pixel Differencing, *Proceedings of the Internal Computer Symposium.*

Yang, S.-K., and Huang, P.-S. 2011, Image Steganographic Scheme by Improving the Combination of Pixel-value Differencing and LSB Replacement Methods, *Journal of Informatics & Electronics* (4:2), pp. 43-53.

網路部份

資料加密標準(Data Encryption Standard)。
https://en.wikipedia.org/wiki/Data_Encryption_Standard(2016/01/16)

Matlab 程式。

https:// www.mathworks.com/products/matlab/(2016/05/31)
NRCS 影像資料庫。
https://photogallery.nrcs.usda.gov/(2016/08/13)
PSNR 與 MSE 品質與計算。
https://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio(2016/10/02)
RSA 加密演算法。
https://en.wikipedia.org/wiki/RSA_(cryptosystem)(2016/03/25)

應用 STIX 於網路威脅情資之研究

傅振華 賴漢鍾 陳建誠

國防大學資訊管理學系

摘要

近年來，網際網路越來越普及，然而也產生了資訊安全等相關議題，網路威脅的發展速度比防禦方還要來得快，更有惡意軟體提供給任何想要發動網路攻擊的人承租。隨著越來越多的攻擊事件發生，有些組織或間體已經可以在攻擊發生之前，事先察覺到未來可能發生的網路威脅，並將網路威脅情資和信任夥伴們共享，一同來防禦各種的網路威脅。STIX 是一種標準化語言來描述網路威脅情資，用結構化的方式來更有效的協助網路威脅管理流程及自動化應用。本論文利用此語言特性，來建置網路威脅分享平台，描述網路威脅個案，並可匯出成 XML 格式與其他夥伴們分享威脅情資，已達成上述的目的。依據本研究分析與實作，藉此可考慮導入 STIX 結構化的共同機制，以達成網路威脅情資共享，也希望能有助於國內建置網路威脅情資之資訊分享及發展。

關鍵詞〈3-5 個〉：網路威脅情資、STIX、XML

國防相關應用：本研究應用 STIX 進行網路威脅情資的呈現，透過 STIX 的結構化呈現可以明確表達網路威脅情資，有效分享網路威脅情資；故本研究成果將可幫助國軍以具體的方式呈現與分享網路威脅情資，進而提升網路安全防護作為。

A Study on Cyber Threat Intelligence with STIX

Chen H. Fu　Han C. Lai　Chien C. Chen

Department of Information Management, National Defense University, Taiwan, R.O.C.

Abstract

Due to the increasing popularity of the Internet in recent years, this causes cyber security and other related issues. The developing speed of cyber threats is even faster than the defender; more malicious software is available to anyone who wants to lease and launch cyber attacks. As more and more attacks occur, some organizations or groups can perceive threats of the network may occur in the future before these attacks occur; they can share cyber threat intelligence with trusted partners and defend against all kinds cyber threats together.

STIX is a standardized language to describe the cyber threat intelligence with a structured approach. This structured approach is more effective to assist cyber threat management process and automation applications. In this paper, we used STIX of features to build cyber threat sharing platform. We also described threat cases with STIX and exported these cases in XML format. The threat intelligence in XML format will be shared with other partners; this can achieve the purpose of threat intelligence sharing. This study result shows that we can share threat intelligence with structured STIX implementation and achieve the Internet threat intelligence sharing. At last, we also hope to build a cyber threat intelligence information sharing platform with STIX in Taiwan.

Keywords: Cyber threat intelligence, STIX, XML

Relevance to National Defense: This study presents cyber threat intelligence with STIX. With STIX, cyber threat intelligence can be expressed structurally and definitely. Moreover, with STIX presentation, it can help to share cyber threat intelligence. Therefore, the study result can help R.O.C. military to present and share specifically and enhance cyber protection achievement.

壹、緒論

網路安全是一個複雜且多面向問題的領域，我們對複雜的防禦技術依賴持續成長，並在同一時間，威脅環境也是持續成長且以動態及艱鉅的方式發展。傳統的網路安全防禦方式著重於對內的認知及針對漏洞、弱點和配置去做防禦補強。有效的防禦目前及未來威脅也需要著重於對外的防禦，其包括了解敵人的行為、能力和攻擊企圖。只有透過充分的理解敵人及自己，「知己知彼」才能足夠瞭解我們面臨的真正威脅性質，並做出明智的防禦決策。

我們可以從狙殺鍊（Kill Chain)了解一次網路攻擊可以分成好幾個步驟，並可以從中了解攻擊行為及如何去防範。由學者劉培文（2015）整理，狙殺鍊可定義七個階段（如圖 1)，在越早的狙殺鍊階段（Exploit 的左倒)，代表越能在攻擊者建立立足點（Foothold)之前主動偵測並減輕威脅。而在越後面狙擊鍊階段（Exploit 的右倒），代表已經進入到事件偵測及應變處理的程序。

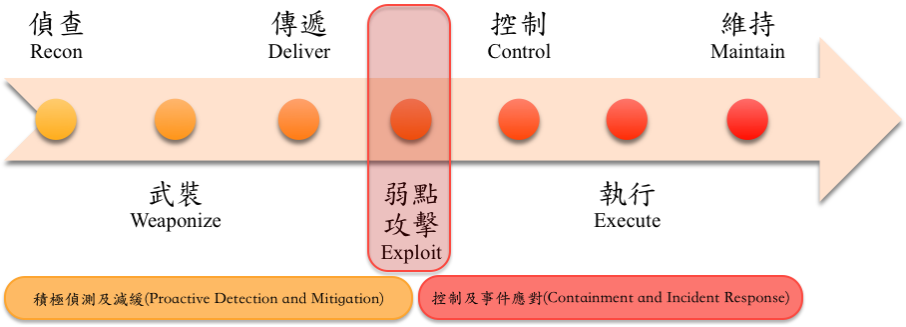


圖 1 狙殺鍊七階段

網路威脅情資（Cyber Threat Intelligence, CTI）的想法是提供識別和攻擊跡象，並經過分析及處理後分享資訊給信任夥伴或共享平台上，讓對網路威脅情資有興趣的組織可以拿來參考，並提早做預防及改進資訊安全措施，以防止相同事件重複發生。根據 SANS 組織調查報告（2015）顯示，在呈現 CTI 格式中，只有百分之三十八使用標準格式和著名的開放原始碼工具包（Open Source Toolkits），其中 STIX（Structured Threat Information Expression）結構化語言是在企業組織中最為普遍常見的標準格式。

隨著網路威脅的影響，企業越來越需要具備蒐集網路威脅情資的能力，並且要有足夠的情資分享能力，以能夠與信任的夥伴共享且一同防禦各種網路威脅。網路威脅情資與共享是能夠幫助企業組織面對現今龐大的網路安全議題，為了在共享情資過程中，需要一個有結構化、標準化的語言來訂定網路威脅情資標準格式，以防止當與其他組織共享時，對方沒辦法立即使用所得到的威脅情資內容，省掉事後再處理的不必要麻煩。

有鑒於目前國內尚未建立威脅情資分享平台，及缺乏網路威脅事件資料庫的建置之自動化架構及機制，以至於發生網路威脅事件時，沒辦法即時的處置或分享給其他單位，以避免相同的事件一再發生。本研究使用現今資訊安全產業裡最為普遍的網路威脅情資結構化語言：STIX，來實作網路威脅情資，試著將透過 STIX 標準化架構來描述和分享網路安全事件，以提供網路威脅情資給有興趣的防禦方，亦可提供給企業組織之資安或 IT 部門作為參考及評估其成效。

貳、文獻探討

本論文將針對 CTI 定義、STIX 和 CybOX（Cyber Observable eXpression）之標準化語言，搜集相關的論文及文獻，研讀後做為本研究的基礎。

一、網路威脅情資（CTI）

網路威脅情資是現在資訊安全領域裡一個很熱門的話題，資安廠商也都利用這波風潮，試著創出一番事業。但可以發現大部份廠商的網路威脅情資都是使用原始資訊（Raw Information）。例如，提供行為不良的 IP 位址資料或未經處理的指標轉儲到你的組織，或讓你的資安團隊去做整理，更多的原始資料不是你的團隊或你的資安技術所需要的。堆積如山的原始、未經過濾的資料只會加劇過載警報和不準確的議題，這是現今資安團隊所面臨的問題。

資訊（Information）和情資（Intelligence）之間的差異如表 1 所示，資訊是原始、未經過濾的，沒有被分析過，且從虛擬來源匯總而來，可能是真實的、虛假的、誤導性的、相關或不相關的，也不具可操作性。而情資是經過處理、整理過的資訊，經過分析師解析過的，且來源是可靠的，較為準確、即時、完整及經過相關性評估，具可操作性。

表 1 資訊與情資

Information	Intelligence
- 原始的、未經過濾的	- 處理、整理過的資訊
- 交付時未評判	- 評定且由受過訓練的情資分析師解析
- 從虛擬來源匯總的	- 從可靠的來源和準確性交叉關係
- 可能是真實的、虛假的、誤導性的、相關或不相關的	- 準確、及時、完全（盡可能的）、相關性評估
- 不可操作的	- 可操作的

資料來源：iSIGHT Partners Inc., 2015

CTI 之內容必須包括比原生資料還來得多，它要求只能由人工分析的應用程式創建出豐富的上下文資訊（Contextual Information），其上下文資訊包括各式各樣敵人過去、現在和未來的 TTP（Tactics, Techniques, and Procedures）認識。它還必須包括技術指標（例如，IP 位址和雜湊可疑檔案）、敵人、動機和意圖、及誰將成為目標的相關資訊。

透過融合即時地人類聚集情資和準確的技術情資，可以得到真正需要具豐富、準確且可操作的情報，可以通知你規劃工作、改進決策、和幫助你優先考量和應變現有或新出現的威脅。為了得到準確的技術情資，大量的資料是必須的，這應該包括從廣泛網路收集的 Open-source 資料、自己私有的日誌資訊、從不同行業群組或分享平台的資訊共享和安全技術合作夥伴。

二、STIX

STIX 是一個社區驅動（Community-driven）協作定義和開發一種標準化語言來表示結構化的網路威脅情資，用結構化的方式來更有效的協助網路威脅管理流程和自動化的應用。STIX 打算傳達全面的潛在網路威脅資訊，並力圖成為可充分表達（Fully Expressive）、靈活（Flexible）、可擴展（Extensible）、自動化（Automatable），並盡可能作為人類可讀（Human-readable）的資訊。網路安全的使用案例依賴這些資訊，包括：分析網路威脅、網路威脅特徵分類、管理網路威脅事件應變處理及分享網路威脅資訊。

STIX 提供一個共同機制，以解決結構化網路威脅資訊之涵蓋範圍，增進架構的一致性（Consistency）、效率性（Efficiency）、可互操作性（Interoperability）和整體情境感

知能力（Overall Situational Awareness）。此外，STIX 提供統一的架構，將以下網路威脅資訊建立其關聯，包括：網路觀測（Cyber Obervables）、威脅指標（Indicators）、突發事件（Incidents）；敵人的手法、技術和程序（TTP）則包括攻擊模式、惡意軟體、弱點攻擊、狙殺鍊、工具、基礎設施、受害目標（Victim Targeting）…等等；另利用目標（Exploit Targets）包括漏洞（Vulnerabilities）、弱點（Weaknesses）或配置（Configurations）；而行動方針（Courses of Action, COA）則包括事件應變、漏洞／弱點改善措施或緩解辦法（Mitigations）、攻擊者的動機（Cyber Attack Campaigns）及威脅人員（Cyber Threat Actors）。

(一)Use Cases

STIX 提供一個簡單的使用案例概貌（如圖 2），目標是支持全面的核心使用案例專注於網路威脅管理上 。

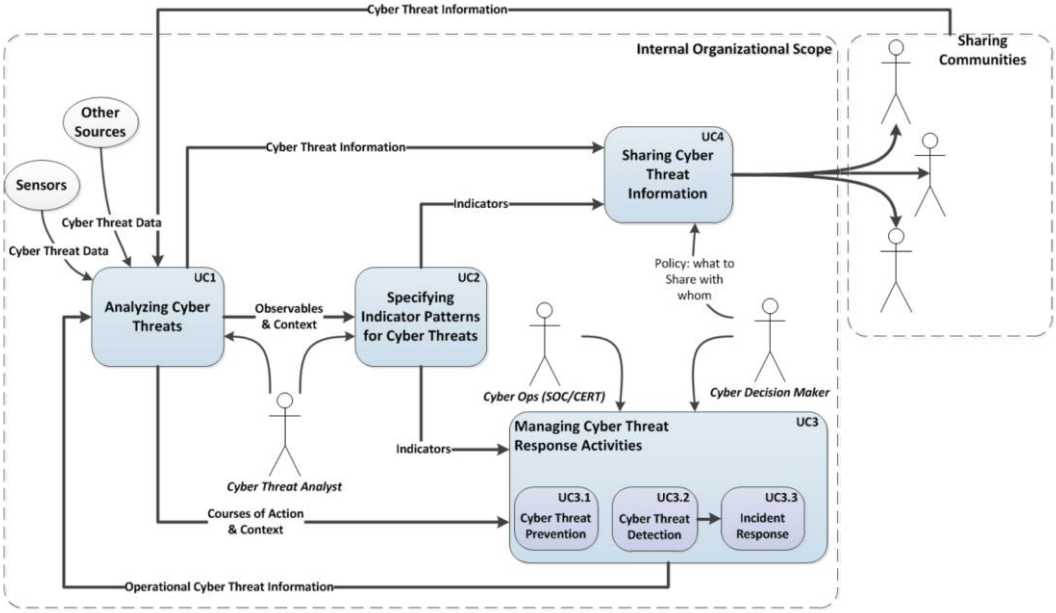


圖 2 STIX 提供之核心使用案例概貌

（資料來源：STIXTM White paper v1.1, 2014）

1.使用案例：分析網路威脅

網路威脅分析師可以從各種的手動或自動化的輸入資源，檢閱結構化或非結構化關於網路威脅活動等資訊，尋求了解相關威脅的性質、識別和充分描述他們，隨著時間的演變，威脅的相關知識可以被充分的描述，這些相關知識包括相關威脅行動（Threat-related Actions）、行為（Behaviors）、能力（Capabilities）、企圖（Intents）、參與者屬性（Attributed Actors）…等等。從這些了解及描述威脅，分析師可以將網路威脅特徵進行分類、威脅應變處理的建議行動方針和與其他信任夥伴分享資訊。

例如，在一個潛在的網路釣魚攻擊事件，網路威脅分析師可以分析和評估可疑的網路釣魚電子郵件（Phishing Email），分析任何電子郵件的附件和連結以確定是否有惡意行為，確定電子郵件是否被傳送到其他地方，評估誰成為釣魚攻擊的目標，確定惡意附件或連結是否被打開，並保留所有分析紀錄。

2.使用案例：網路威脅特徵分類

網路分析師指定測量模式表示網路威脅的觀測特徵，隨著威脅的環境（Context）和相關的詮釋資料（Metadata）來理解、處理和應用。這可以手動或使用自動化工具和結構化威脅資訊來協助完成。

例如，在一個潛在的網路釣魚攻擊事件，網路威脅分析師可以從釣魚電子郵件中分析獲得相關的觀測數據集合（例如，發送者或接收者位址、實體來源、主體、嵌入式 URL、附件的種類…等等），找出相關的 TTP 物證，運行狙殺鍊的相關攻擊，分配適當的機密跡象，確定適當的處理指導方針，對跡象產生出相關的自動化規則模式，指定建議行動方針，並將相關的紀錄打包分享給信任夥伴（使用案例 4），以及當作將來可以用來參考的紀錄。

3.使用案例：管理網路威脅應變行為

網路決策者和操作員為了預防、偵測和調查網路威脅而共同努力，及當偵測到相關事件時做出應變。預防行動方針可能是補救性質，以減輕漏洞、弱點或錯誤配置所造成的威脅。偵測和調查某特定事件後，應變行動方針可能是有用途的。例如，在一個被證實的網路釣魚攻擊事件，網路決策者及網路操作員充分瞭解網路釣魚攻擊的影響，包括惡意軟體安裝或惡意軟體執行，評估潛在行動方針的成本和有效性，並執行適當預防或偵測行動方針。

4.使用案例：網路威脅預防

網路決策者識別相關網路威脅，評估可能的預防行動方針，並選擇執行合適的操作。操作員執行被選擇的行動方針，以防止發生特定網路威脅， 不論是透過一般預防性減緩應用，或透過預測說明的領先指標來減緩特定目標。例如，在一個被證實的網路釣魚攻擊事件，網路決策者可以評估建議的預防行動方針（例如，在郵件閘道中執行封鎖規則），確認其相關成本和風險，並決定是否要執行它，如果確定要執行建議行動方針，網路操作員就得執行。

5.使用案例：網路威脅偵測

網路操作員運用機制（自動或手動）以監測和存取網路操作，以便偵測特定已發生的網路威脅，不論是透過以前的歷史證據，或目前正在發生的動態情境感知，或者透過演繹預測說明的領先指標。該偵測通常是透過網路威脅指標模型。例如，在一個被證實的網路釣魚攻擊事件，網路操作員可能從攻擊的定義跡象獲得任何可觀察到的模式，和在操作環境適當地運行它們，來檢測正在發生網路釣魚攻擊的任何證據。

6.使用案例：網路威脅應變

網路操作員對偵測到的網路威脅作出應變，調查發生了什麼或正在發生，試圖識別和描述實際發生威脅的性質，並執行具體的減緩操作或矯正行動方針。例如，在一個被證實的網路釣魚攻擊事件，網路操作員可進行調查活動，以確定網路釣魚攻擊在目標環境（例如，惡意軟體被安裝或被執行）中是否成功，並且如果是這樣，嘗試去描述那些影響的細節（例如，哪個系統被惡意軟體所影響，哪些資料被洩漏…等等），一旦結果被了解，網路操作員應執行適當的減輕操作或矯正行動方針（例如，抹除或恢復系統，封鎖洩漏通道…等等）。

7.使用案例：分享網路威脅資訊

網路決策者制定什麼樣的網路威脅資訊可以與其他夥伴分享的政策，以及基於一致認同的信任框架來處理被分享的網路威脅資訊。這樣的方式是為了保持資訊的一致性和管理的適當水平。這一政策隨後被執行來分享相應的網路威脅指標和其他網路威脅資訊。例如，在一個被證實的網路釣魚攻擊事件，由網路決策者預先定義好的資訊分享政策，可以使相關指標能夠被自動的或手動的與信任夥伴或社群上分享，使得他們可以利用所獲得的情資。

(二)STIX 架構（Architecture）

STIX 提供了一個標準資料架構，用來描述網路威脅情資，如圖 3，是一個獨立且可再使用的架構，描述每一個構造的內容及其相互關係。構造與構造之間的連結箭頭表示他們之間的關係，在每個連結箭頭標籤上括弧內的星號表示著每個關係可能存在零次到很多次，每個構造的結構化內容是以 XML 架構建置而成的。

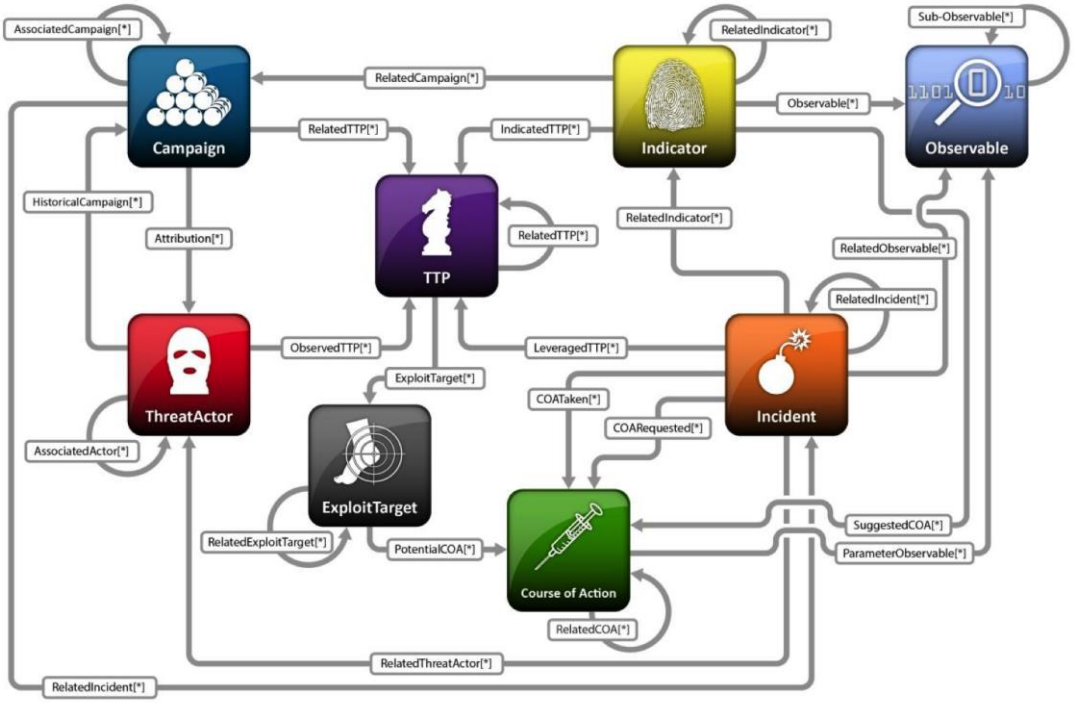


圖 3 STIX v1.1 架構
（資料來源：Barnum, S., 2014）

(三)STIX 結構（Structure）

下文將針對八個核心構造與一個跨組織的“Data Marking”構造做個簡要描述：

1.觀測（Observables）

是 STIX 架構中最基本的構造，Observables 是有狀態屬性或測量相關的事件操作，對網路及電腦運作環境來說，需要有固定角色隨時監控網路動態，以便日後的事件調查及處理。其資料包括檔案的相關資訊（檔名、雜湊值、檔案大小…等等），註冊金鑰值，服務被啟動或 HTTP 請求被傳送。STIX 利用 CybOX 語言來表示 Observables 內容，CybOX 將在下一章節做個簡要概述。

2.指標（Indicators）

主要是傳達特定 Observable 模型，結合環境資訊試圖表達人工因素（Artifacts）或網路安全環境的利益行為。由一個或多個 Observable 模型可以對應到相關的 TTP 和其他相關的元資料（處理的限制、驗證時間窗格、可能產生的影響、觀測指標、相關事件、建議行動方針、相關的 Indicators、Indicators 來源…等等）。鑑於目前標準化表示方法的限制，STIX 利用社群知識和最佳實踐（Best Practices）來定義一個新的 Indicator。

3.突發事件（Incidents）

是 Indicators 影響組織隨著資訊在事件應變調查期間被發現或被確定的個別事件。其資料包括時間相關的資訊、參與的當事人、受影響的資產、影響評估、相關的 Indicators、相關的 Observables、可利用的 TTP、威脅者的屬性、預期效果、危害的性質、要求的應變行動方針、已採取的行動方針、特徵的可靠度、操作指引、Incident 資訊來源、記錄所採取的措施…等等。

4.手法、技術及程序（Tactics, Techniques and Procedures, TTP）

是表示威脅者的行為或手法，這是從傳統軍事領域採取的一個術語，用來描述威脅者做了什麼和如何做到的。例如，手法可能會使用惡意程式來竊取信用卡憑證；相關技術可能會發送目標郵件給潛在的受害者，其中包含當被打開時會執行惡意程式碼的附加文件，捕捉從鍵盤輸入的信用卡資訊，並使用 HTTP 來與命令/控制伺服器傳送信用卡資訊；相關的程序可能會透過發送令人信服的社交工程郵件和文件給易受騙的個人，創造惡意軟體或漏洞來繞過目前防毒軟體的檢測，建立命令/控制伺服器來註冊銀行網域，然後將假的銀行網址給受害者。

TTP 包含威脅者的行為（攻擊模式、惡意軟體、漏洞）物證、利用的資源（工具、基礎建設、人物角色）、目標受害者的資訊（人事地）、相關的 ExploitTargets、預期效果、狙殺鍊階段、操作指引、TTP 資訊來源…等等。TTP 發揮網路威脅資訊和網路威脅情資中心作用，與 Indicators、Incidents、Campaigns 和 ThreatActors 相關聯，此外與 ExploitTargets 有密切關聯。

鑑於目前標準化方法的缺乏，STIX 利用社群知識和最佳實踐來定義一個新的 TTP 資訊。然而，某些 TTP 可以利用其他標準或工具來定義，例如 CAPEC 可以用來結構化描述 TTP 攻擊模式、MAEC 可以用來結構化描述 TPP 惡意軟體、CybOX 可以用來結構化描述攻擊所使用的工具和架構。

5.動機（Campaigns）

是 ThreatActors 追求的意圖，透過 Incidents 和 TPP 集合觀察到潛在跨組織性的事件。包括敵人推測的預期效果、利用相關的 TTP、相關的 Incidents 被認定為、歸屬 ThreatActors 該責任的責任、其他相關的 Campaigns、所採取的應變措施、Campaigns 資訊來源、操作指引…等等。

6.威脅者（Threat Actors）

是描述惡意威脅者的特徵，包括假定意圖和歷史觀察反應。包含描述身份、可疑動機、可疑的預期效果、歷史上觀察到所使用的 TPP、歷史上 Campaigns 相關的 ThreatActor、其他相關的 ThreatActor、資訊來源、操作指引…等等。

7.利用目標（Exploit Targets）

是由 ThreatActor 利用 TTP 來探索在軟體、系統、網路或配置中的漏洞或弱點，成為威脅者的攻擊目標。包括漏洞、弱點或配置的識別或表徵、潛在的行動方針、資訊來源、操作指引…等等。鑑於目前廣義描述標準化方法的缺乏，STIX 利用社群知識和最佳實踐來定義一個新的 ExploitTargets 結構並表示一個新的 ExploitTargets 資訊。然而，某些 ExploitTargets 可以用其他標準去定義這些漏洞、弱點和配置，例如從 CVE®（Common Vulnerabilities and Exposures）和 OSVDB（Open Source Vulnerability Database）的識別架構來鑑定公開揭露的漏洞；CVRF（Common Vulnerability Reporting Framework）格式可以用來在未被 CVE 或 OSVDB 識別出的漏洞，包括零時差漏洞（0-day）；CWETM（Common Weakness Enumeration）用來識別弱點；CCETM（Common Configuration Enumeration）用來識別配置上的議題。

8.行動方針（Courses Of Action, COA）

是要採取具體的措施來解決威脅，不論組織是否有採取矯正或預防措施來解決威脅者的 ExploitTargets，或應變措施來對抗、減輕 Incidents 的潛在影響。包括網路威脅管理的相關階段（例如，ExploitTarget 的補救或 Incident 的應變）、類型、描述介紹、目標、結構化表示（例如，IPS 規則或自動補丁／修復）、可能產生的影響、可能的成本花費、估計效果、觀察到的參數、操作指引…等等。

9.Data Markings

主要是負責將資料做標記，並提供交叉比對。由 STIX 定義 Data Markings 兩種具彈性的標記方法：首先，特定獨立案件的結構被標記（指向他們的位置），而不是到處嵌入（通常此技術的效率較低且不易更新和改進）；其次，允許定義和使用任何資料標記結構，只是作為基本類型結構的抽象化，使得不同標記的結構可以被利用和結合上述的獨立案件，也能夠容易地標記任何給定的資料，包括從不同的使用案例或是不同的社群。在初步實行 Data Marking 構造已利用 XML 架構（XSD）來創建，並不只是透過 XML 來實作 STIX，任何其他只要是基於 XML 的結構也可以表示此結構。

(四)CybOX

CybOX 像是 STIX，不是針對單一網路安全使用案例，而是為了有足夠彈性，以提供所有網絡安全的需求，處理網絡觀測能力的通用解決方案。CybOX 的目標是支援範圍廣泛的相關網路安全領域，包括：威脅評估與鑑定（詳細攻擊模式）、鑑定惡意軟體、操作事件管理、日誌紀錄（Logging）、網路情態感知、事件應變、跡象共享及數位鑑識（Digital Forensics）…等等。透過使用標準化 CybOX 語言，相關觀測事件或屬性可以被捕捉和分享，在指標或規則中定義，用來描繪攻擊模式和惡意軟體的輪廓，以配合邏輯模式建構真實世界的證據。事件應變和管理可以充分利用以上所有功能去調查發生的事故，提高整體情境感知能力和改善未來的攻擊偵測、預防及應變。CybOX 對資訊內容的範圍界定，堅持以下原則：關於網路觀測的資訊化內容，如果是一般用途到多個用途，並且不與任何支援的使用案例起衝突、關於網路觀測的資訊化內容，是特定於個別支援的使用案例領域應該在使用案例領域的特定標準進行管理，或利用 CybOX 對所有一般網路觀測資訊化的內容進行解決方案。具彈性的擴展機制是納入 CybOX 來支援這種利用特定領域標準和解決方案。

參、研究方法與架構

本研究主要是以 Python 程式語言利用 STIX API 函式庫來針對一個資安事件，用 STIX 架構格式描述，輸出成 XML 格式與信任夥伴分享此網路威脅情資，提早預防免於再受到相同威脅攻擊影響。

我們先以惡意網址為例來說明 STIX 部分構造之功能：一個非常常見的網路威脅方法是透過特定的網址，傳送惡意軟體給潛在目標（受害者），受害者透過釣魚郵件或點擊網址連結時，會被導向至含有惡意程式的網站並遭受病毒侵入。惡意網址的分享清單可以有效的和以廉價的方式去拆穿惡意代碼。

假設有一個 indicator 為已知的惡意網址：http://x4z9arb.cn/4712/，不像是 C2（Command and Control）及惡意軟體雜湊，在這情況下產生的 indicator 沒有任何特定的 context，因此選擇無附加 context 的 indicator（如圖 4）。根據這個 indicator，惡意網址被表示為 URL 物件，其 Type 欄位設定為“URL”及 Value 欄位設定惡意網址（http://x4z9arb.cn/4712/）。

Indicator	
ID	example:Indicator-d81f86b9-975b-bc0b-775e-810c5ad45a4f
Title	Malicious site hosting downloader
Type	URL Watchlist IndicatorTypeVocab-1.1
Observable	
Object	
Properties	URIObjectType
Type	URL
Value	http://x4z9arb.cn/4712/
Condition	Equals

圖 4 圖解惡意網址之 Indicator

（資料來源：http://stixproject.github.io/documentation/idioms/malicious-url/）

實作 XML 部分：

```
1 <stix:Indicator id="example:Indicator-d81f86b9-975b-bc0b-775e-810c5ad45a4f" xsi:type
='indicator:IndicatorType'>
2 <indicator:Title>Malicious site hosting downloader</indicator:Title>
3 <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.0">URL Watchlist</indicato
r:Type>
4 <indicator:Observable id="example:Observable-ee59c28e-d922-480e-9b7b-a79502696505
">
5 <cybox:Object id="example:URI-b13ae3fc-80af-49c2-9de9-f713abc070ba">
6 <cybox:Properties xsi:type="URIObj:URIObjectType" type="URL">
7 <URIObj:Value condition="Equals">http://x4z9arb.cn/4712</URIObj:Value>
8 </cybox:Properties>
9 </cybox:Object>
10 </indicator:Observable>
11 </stix:Indicator>
```

（資料來源：http://stixproject.github.io/documentation/idioms/malicious-url/）

實作 Python Producer 部分：

```
1 indicator = Indicator()
2 indicator.id_ = "example:package-382ded87-52c9-4644-bab0-ad3168cbad50"
3 indicator.title = "Malicious site hosting downloader"
4 indicator.add_indicator_type("URL Watchlist")
5
6 url = URI()
7 url.value = "http://x4z9arb.cn/4712"
8 url.type_ = URI.TYPE_URL
9 url.condition = "Equals"
10
11 indicator.add_observable(url)
12 print indicator.to_xml()
```

（資料來源：http://stixproject.github.io/documentation/idioms/malicious-url/）

實作 Python Consumer 部分：

```
1 print "== MALWARE =="
2 for ind in pkg.indicators:
3         print "---"
4         print "Title : " + ind.title
5         print "ID : " + ind.id_
6         for ind_type in ind.indicator_types:
7                 print "Type: " + str(ind_type)
8
9         for obs in ind.observables:
10        print "URL : " + str(obs.object_.properties.value)
```

（資料來源：http://stixproject.github.io/documentation/idioms/malicious-url/）

本研究之研究工具及開發環境如表 2 所示，使用 Python 版本 2.7 來撰寫系統，透過 STIX API 套件來實作 STIX 網路威脅情資，並可匯出 XML 檔案，以滿足情資分享之性質，其中使用 Python-stix 時，Lxml（為處理 XML 及 HTML）、Python-cybox（為解析、操作及產生 CybOX 內容）及 Python-dateutil（為解析日期時間資訊）等函式庫是被要求的。

以 PyCharm 為開發環境，安裝於 OS X EI Capitan 作業系統上，並透過 Web 應用框架 Django 來架設及實作 STIX 網路威脅情資應用之網站。

表 2 研究工具及開發環境

研究工具	➢Python 2.7 ➢STIX API: Python-stix 1.2.0.0 使用 Python-stix 時，以下函式庫是被要求的： ● Lxml（本研究使用版本：3.4.4） ● Python-cybox（本研究使用版本：2.1.0.12） ● Python-dateutil（本研究使用版本：1.5）
研究環境	作業系統：OS X EI Capitan 10.11.3 IDE: PyCharm 5.0.4 Professional Edition Web 應用框架：Django 1.9.0

肆、雛形系統建置與實作

本研究實作了一個雛形系統，其中包括 STIX 中的八大構造，和構造與構造之間的關聯性。使用者可以透過本研究之 Web 應用系統，來完成建立 STIX 結構化的網路威脅情資。本章就依雛形系統之各個功能做詳述說明。

一、雛形系統功能介紹

本雛形系統依據 STIX 官方提供之資料模型（版本：1.2）如圖 5 所示，建立各個構造之新增、修改及刪除及檢視功能，詳述說明如下：

圖 5 系統首頁

(一)Indicator

根據 STIX 官方之資料模型文件，可得知 Indicator 構造資料內容如圖 6 所示，建立其新增及修改畫面。此功能可定義 Indicator 之類別、可能產生的影響、建議的行動方針、信任度及情資來源……等等。其中 Type 欄位的預設詞彙包括：Malicious E-mail, IP Watchlist, File Hash Watchlist, Domain Watchlist, URL Watchlist, Malware Artifacts, C2, Anonymization, Exfiltration, Host Characteristics, Compromised PKI Certificate, Login Name, IMEI Watchlist 及 IMSI Watchlist。

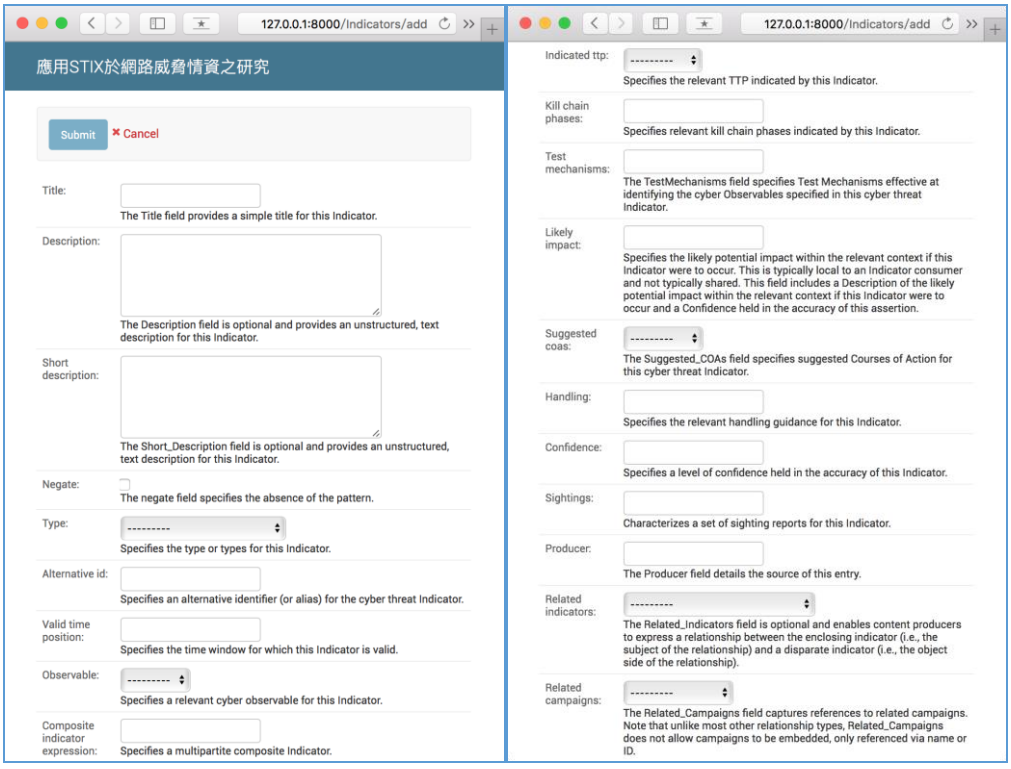


圖 6 Indicator 新增與修改畫面

(二)Incident

根據 STIX 官方之資料模型文件，可得知 Incident 構造資料內容如圖 7 所示，建立其新增及修改畫面。此功能可定義 Incident 之種類、回報者、參與的當事人、受害者、影響資產、影響評估、狀態、攻擊者屬性、預期效果、發覺方法、信任度及來源……等等。其中 Status 欄位預設詞彙包括：New, Open, Stalled, Containment Achieved, Restoration Achieved, Incident Reported, Closed, Rejected 及 Deleted。

Intended_Effect 欄位的預設詞彙包括：Advantage: Advantage, Economic, Military, Political; Theft: Theft, Intellectual Property, Credential Theft, Identity Theft, Theft of Proprietary Information; Account Takeover, Brand Damage, Competitive Advantage, Degradation of Service, Denial and Deception, Destruction, Disruption, Embarrassment, Exposure, Extortion, Fraud, Harassment, ICS Control, Traffic Diversion 及 Unauthorized Access。

Security_Compromise 欄位的預設詞彙包括：Yes, Suspected, No 及 Unknown。

Discovery_Method 欄位的預設詞彙包括：Agent Disclosure, External - Fraud Detection, Monitoring Service, Law Enforcement, Customer, Unrelated Party, Audit, Antivirus, Incident Response, Financial Audit, Internal - Fraud Detection, HIPS, IT Audit, Log Review, NIDS, Security Alarm, User 及 Unknown。

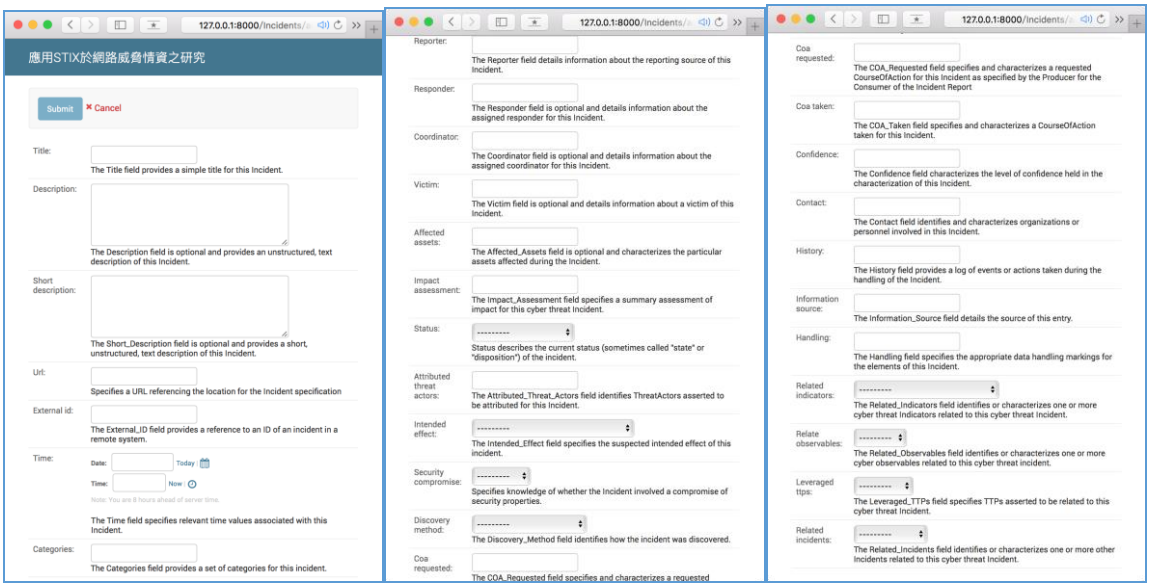


圖 7 Incident 新增與修改畫面

(三)TTP

根據 STIX 官方之資料模型文件，可得知 TTP 構造資料內容如圖 8 所示，建立其新增及修改畫面。 此功能可定義 TTP 之預期成果、行為、資源、目標受害者、狙殺鍊階段及利用目標……等等。

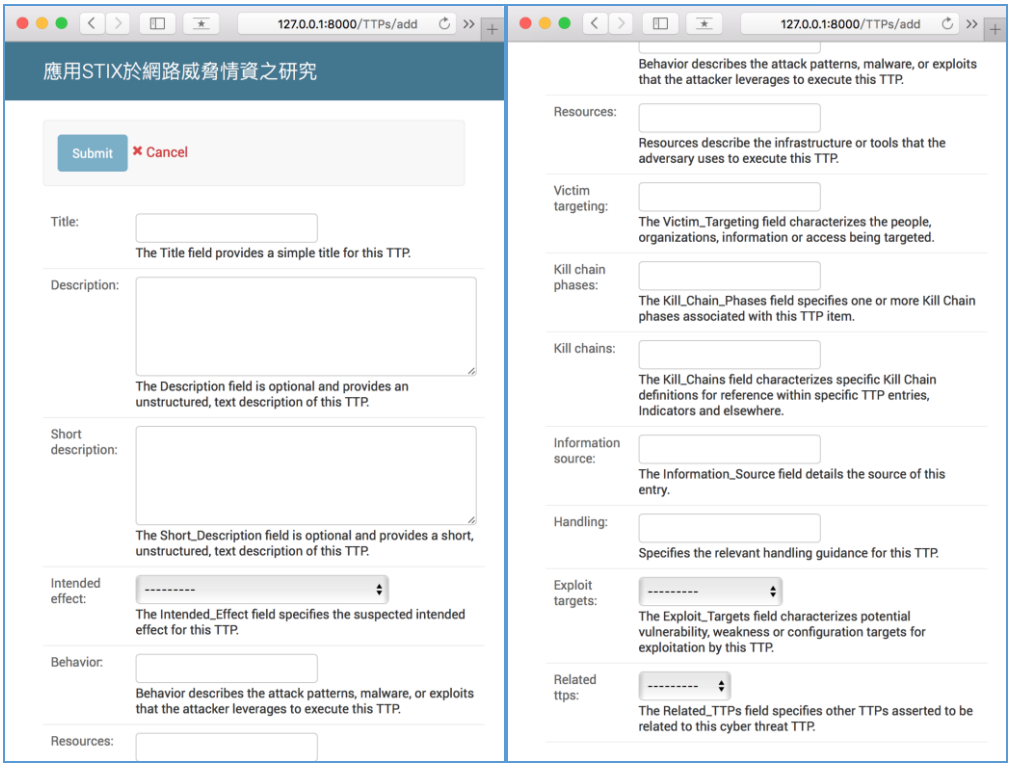


圖 8 TTP 新增與修改畫面

(四)Campaign

根據 STIX 官方之資料模型文件，可得知 Campaign 構造資料內容如圖 9 所示，建立其新增及修改畫面。 此功能可定義 Campaging 之預期成果、狀態、屬性、信任度、活躍及情資來源……等等。其中 Status 欄位的預設詞彙包括：Future, Historic 及 Ongoing。

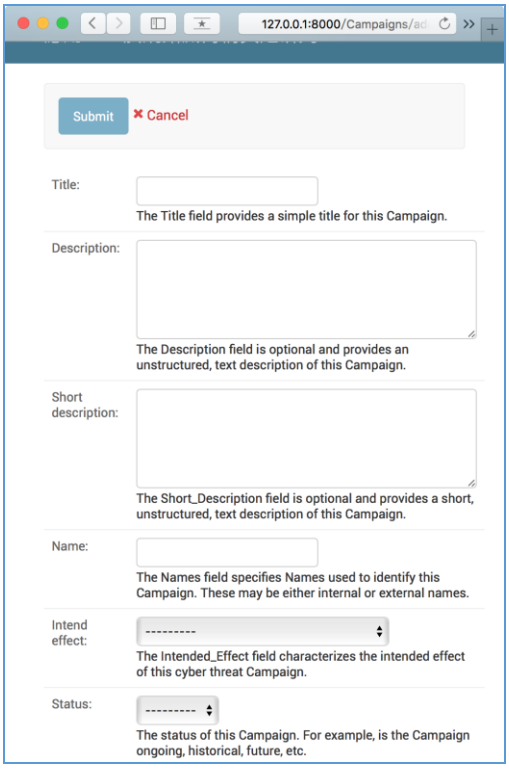


圖 9 Campaign 新增與修改畫面

(五)ThreatActor

根據 STIX 官方之資料模型文件，可得知 ThreatActor 構造資料內容如圖 10 所示，建立其新增及修改畫面。 此功能可定義 ThreatActor 之識別、類別、動機、程度、預期成果、計畫及操作支援、信任度及情資來源……等等。

其中 Type 欄位的預設詞彙包括：Cyber Espionage Operations, Hacker: White hat, Gray hat, Black hat; Hacktivist, State Actor / Agency, eCrime Actor: Credential Theft Botnet Operator, Credential Theft Botnet Service, Malware Developer, Money Laundering Network, Organized Crime Actor, Spam Service, Traffic Service, Underground Call Service; Insider Threat 及 Disgruntled Customer / User。

Motivation 欄位的預設詞彙包括：Ideological: Anti-Corruption, Anti-Establishment, Environmental, Ethnic / Nationalist, Information Freedom, Religious, Security Awareness, Human Rights; Ego, Financial or Economic, Military, Opportunistic 及 Political。Sophistication 欄位的預設詞彙包括：Innovator, Expert, Practitioner, Novice 及 Aspirant。

Planning_And_Operational_Support 欄位的預設詞彙包括：Data Exploitation: Analytic Support, Translation Support; Financial Resources: Academic, Commercial, Government, Hacktivist or Grassroot, Non-Attributable Finance; Planning: Open-Source Intelligence (OSINT) Gathering, Operational Cover Plan, Pre-Operational Surveillance and Reconnaissance, Target Selection; Skill Development / Recruitment: Contracting and Hiring, Document Exploitation (DOCEX) Training, Internal Training, Military Programs, Security / Hacker Conferences, Underground Forums 及 University Programs。

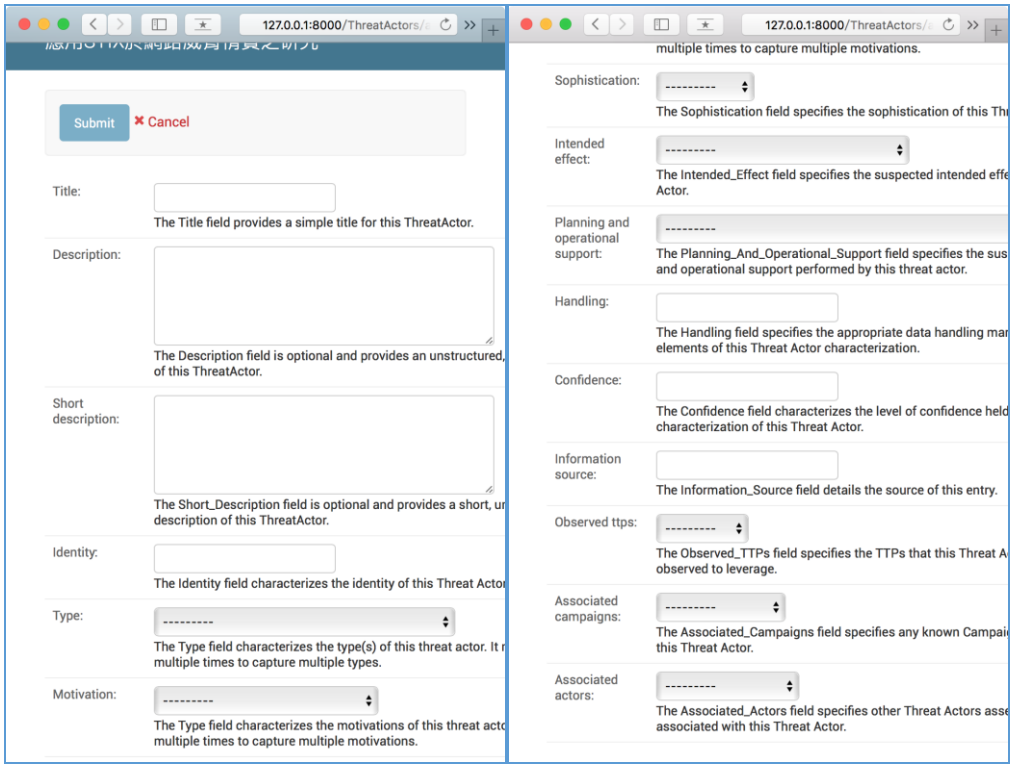


圖 10 ThreatActor 新增與修改畫面

(六)ExploitTarget

根據 STIX 官方之資料模型文件，可得知 ExploitTarget 構造資料內容如圖 11 所示，建立其新增及修改畫面。 此功能可定義 ExploitTarget 之漏洞、弱點、配置、潛在的行動方針及情資來源……等等。

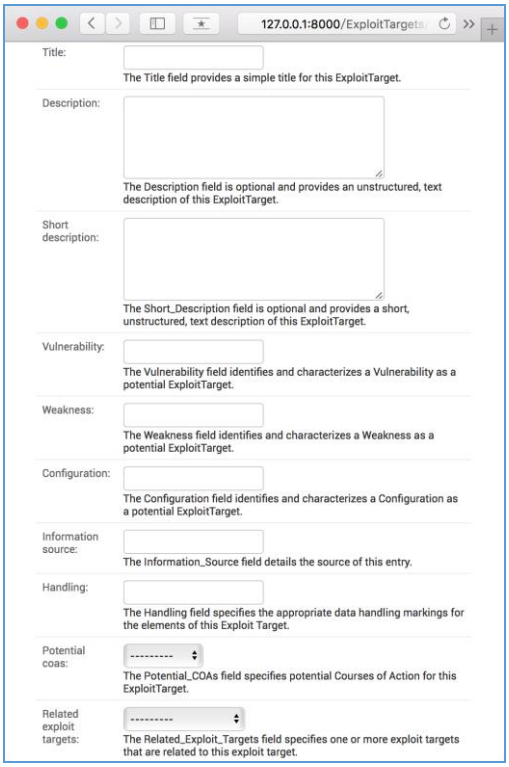


圖 11 ExploitTarget 新增與修改畫面

(七)Course Of Action

根據 STIX 官方之資料模型文件，可得知 Course Of Action 構造資料內容如圖 12 所示，建立其新增及修改畫面。 此功能可定義 COA 之階段、類別、影響、成本、效益及情資來源……等等。

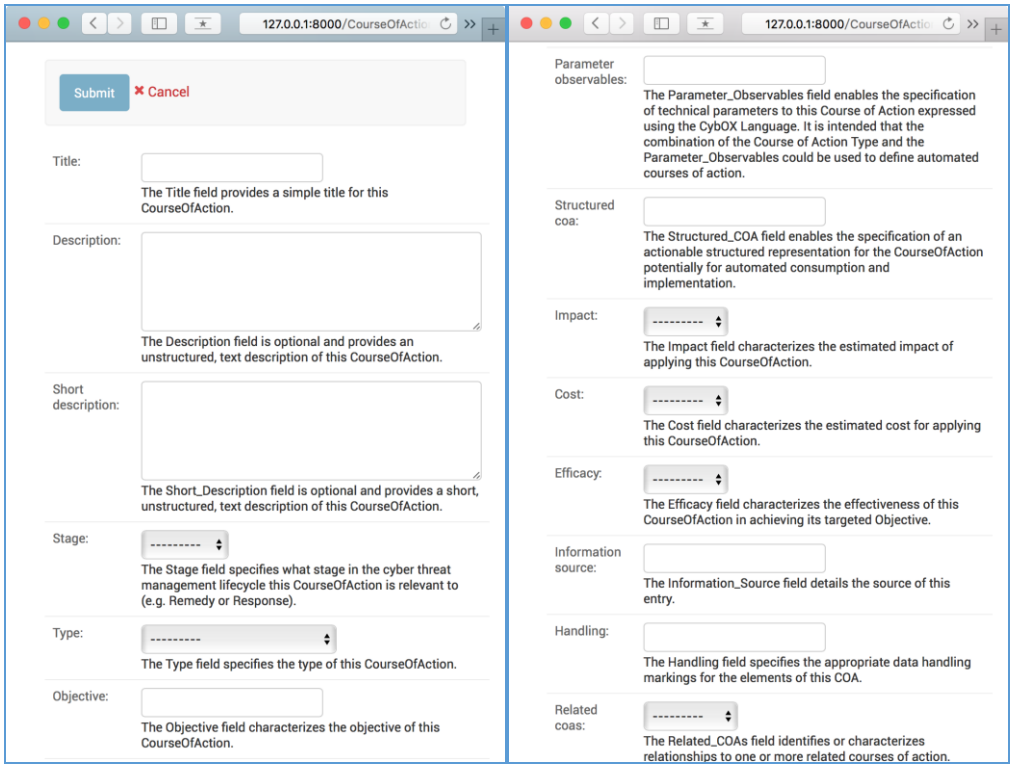


圖 12 CourseOfAction 新增與修改畫面

其中 Stage 欄位的預設詞彙包括：Remedy 及 Response。

Type 欄位的預設詞彙包括：Perimeter Blocking, Internal Blocking, Redirection, Redirection (Honey Pot), Hardening, Patching, Eradication, Rebuilding, Training, Monitoring Service, Physical Access Restrictions, Logical Access Restrictions, Public Disclosure, Diplomatic Actions, Policy Actions 及 Other。Impact, Cost 和 Effiacy 欄位的預設詞彙均包括：High, Medium, Low, None 及 Unknown。

二、雛形系統實作案例

本章節以封鎖網路流量的行動方情境來解說部分功能：假設有一個組織希望透過 COA 行動方針來描述一個已知的 PIVY C2 伺服器位於特定 IP 位址上，並進行封鎖。Title 欄位填入人類可讀的標頭，如果需要更長、更詳細的敘述主體，可以在 Description 和 Short Description 欄位填寫；Stage 欄位是用來描述 COA 在使用過程中的應變處理階段，在上述範例情境中，該行動是回覆一些已知的活動，所以設定為“Response” ；Type 欄位表示一般類型的行動方針是怎麼被描述，此範例情境 COA 為描述阻擋由周圍防火牆的 IP 位址，故設定成“Perimeter Blocking”；Objective 欄位為描述在技術層面上 COA 的預期目的；Impact 欄位用來描述實行 COA 對一般操作的預期影響，此範例因為 COA 封鎖的 IP 位址未用於任何合法目的操作，故設定為 Low；Cost 欄位描述實行此 COA 所產生的估計成本，此範例僅執行防火牆規則是便宜的，故設定為 Low；Efficacy 欄位描述 COA 假如實行成功時其效用為何；Parameter Observables 欄位是描述 COA 的技術參數，此範例為應阻止的 IP 位址。輸入畫面如圖 13-15 所示。

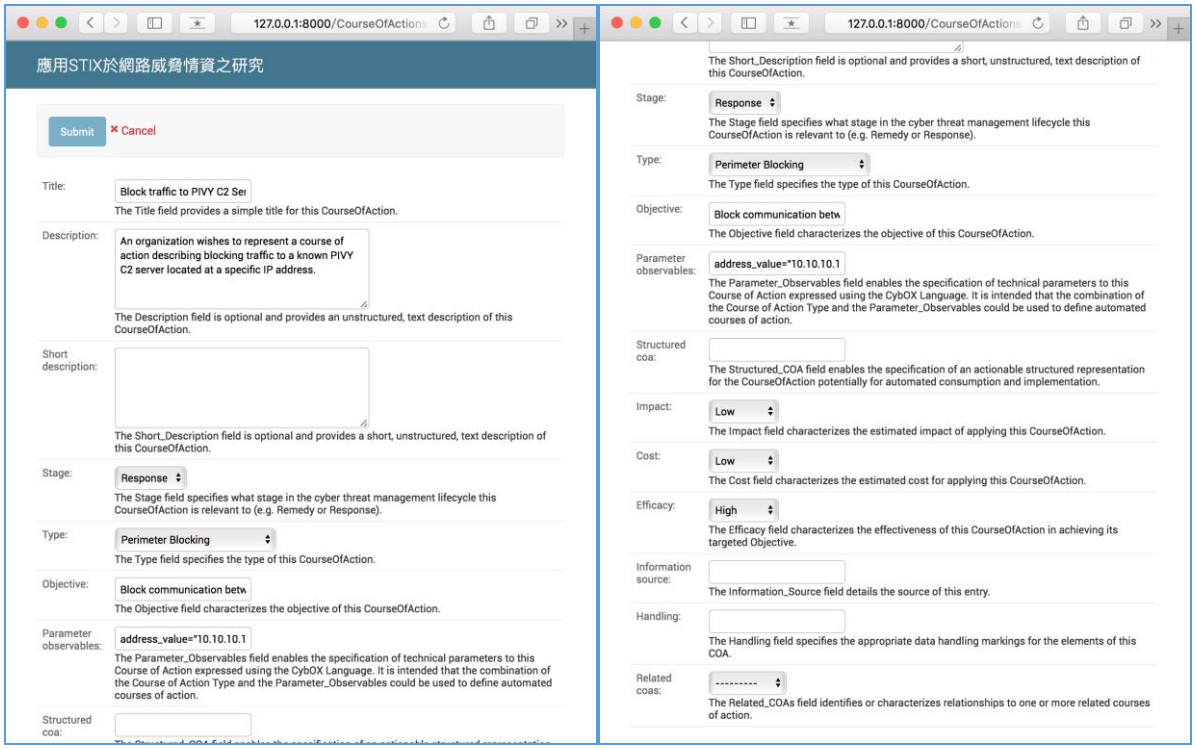


圖 13 情境範例 COA 輸入畫面

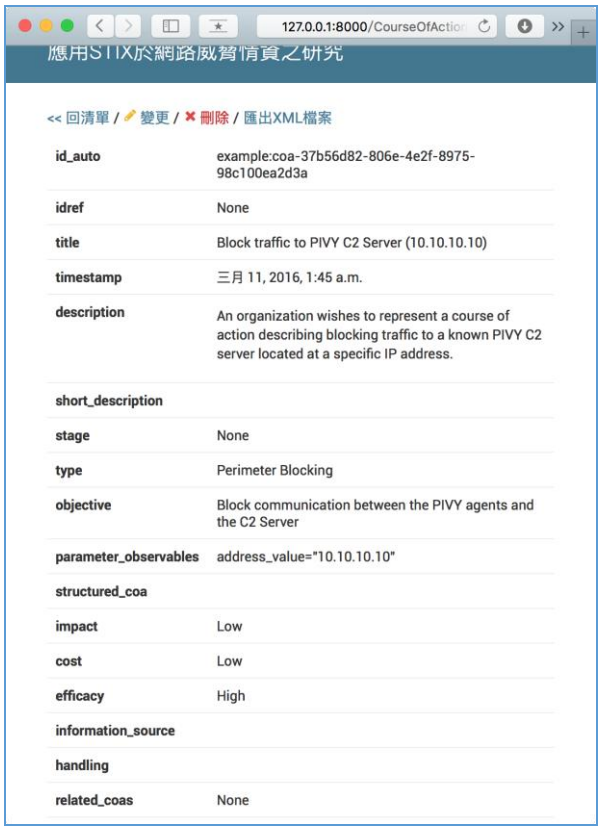


圖 14 輸入完成之檢視畫面

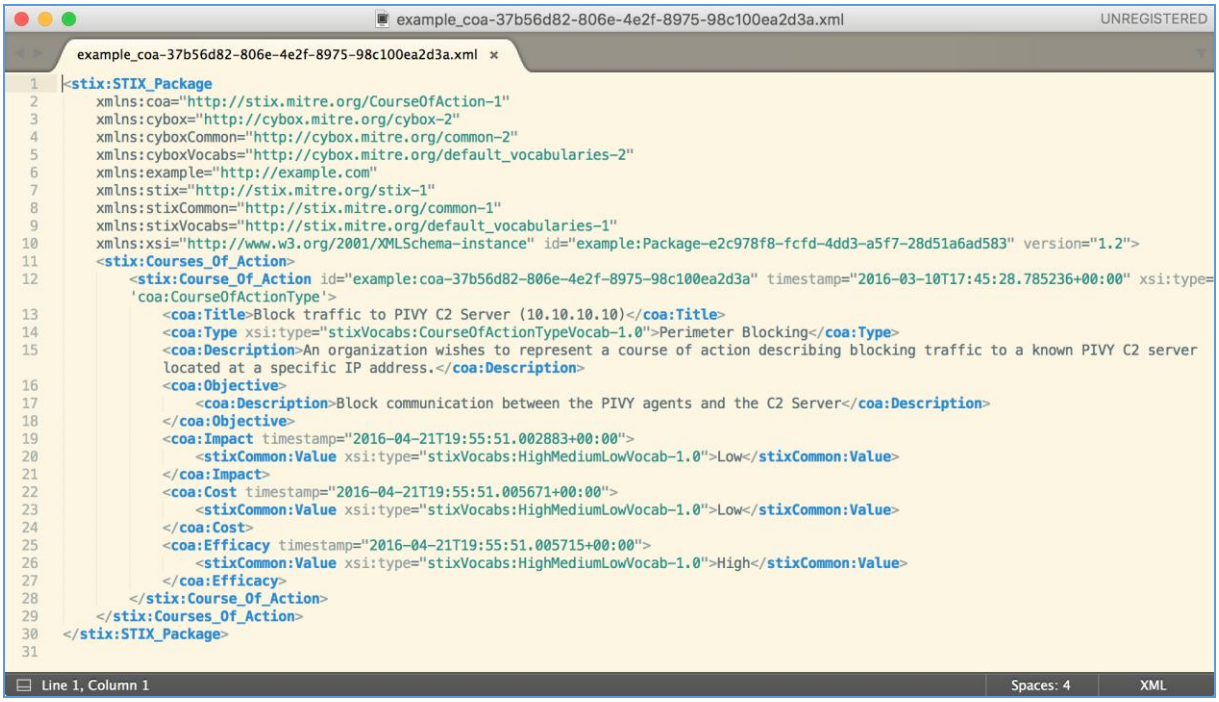


圖 15 匯出成 xml 格式

伍、結論與未來研究方向

綜合本論文在第三章及第四章的研究成果，結論如下三點：

一、針對網路威脅個案分析：

透過 XML 格式呈現 STIX 結構化的威脅情資，包括個案發生之原因、過程及應變處理方針…等等資訊，藉此一窺網路威脅個案之全貌，並將經過處理的網路威脅情資與信任夥伴共享，一同防範廣大的網路威脅，降低網路威脅傷害。

二、STIX 之結構化語言

以 python 撰寫網路威脅情資平台，透過 XML 格式呈現 STIX 之網路威脅內容，提供網路威脅情資之分享及交流，並藉此窺探威脅個案全貌。

三、缺乏網路威脅事件之資料庫資源：

當網路威脅事件發生時，無法即時地將威脅情資分享給其他信任夥伴。為避免同樣的資安事件發生，藉此可考慮導入 STIX 結構化的共同機制，以達成能與信任夥伴共享威脅情資，且透過標準化的結構模型，能更有效的管理網路威脅情資（CTI）及互操作性。依據本研究分析與實作，希望能有助於國內建置網路威脅情資之資訊分享及發展。

參考文獻

英文部分

Barnum, S., 2014, Standardizing Cyber Threat Intelligence Information with the Structured Threar Information eXpression, MITER Corporation.

Kessel, P., & Allan, K., 2014, Cyber threat intelligence - how to get ahead of cybercrime, EY Global.

Ponemon Institute, 2015, The Importance of Cyber Threat Intelligence to a Strong Security Posture, Ponemon Institute© Research Report.

Shackleford, D., 2015, Who's Using Cyberthreat Intelligence and How?, SANS Institute.

Sykosch, A., & Wubbeling, M., 2015, STIX 2 IDS, Coordinating Attack Response at Internet Scale (CARIS) Workshop.

Von Solms, R., & Van Niekerk, J., 2013, From information security to cyber security, Computers & Security (38), pp. 97-102.

網路部分

林子煒，淺談以 STIX 實現網路威脅情報標準化框架，參見 ITs 通訊網站：http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=3010 [visited in 2015/9/2]

劉培文，網際攻擊狙殺鍊，參見行政院國家資通安全會報技術服務中心網站：https://www.icst.org.tw/ArticlesDetail.aspx?seq=1318&lang=zh [visited in 2015/9/2]

網路資訊雜誌，Websense 安全實驗室 2015 威脅報告 8 大關鍵趨勢呼籲企業注意新興攻擊戰術，參見網路資訊雜誌網站：http://news.networkmagazine.com.tw/classification/security/2015/05/13/65115/ [visited in 2015/10/14]

iThome，從駭客角度看失敗的企業資安，從 CTI 找到生路，參見 iThome 網站：http://www.ithome.com.tw/pr/97818 [visited in 2015/9/7]

Barnum, S., "The Secret to Effective Cyber Threat Intelligence and Information Sharing", RSA Conference 2013, 2013 (available online at http://www.rsaconference.com/writable/presentations/file_upload/dsp-r31.pdf). [visited in 2015/8/31]

iSIGHT Partners Inc., “What is Cyber Threat Intelligence and why do I need it?”, (available online at http://info.isightpartners.com/why-do-i-need-cyber-threat-intelligence). [visited in 2015/8/22]
MITRE Corp., “Cyber Observable eXpression (CybOXTM)”, (available online at http://cybox.mitre.org/). [visited in 2015/8/25]
MITRE Corp., “python-cybox 2.1.0.12 Documentation”, (available online at http://cybox.readthedocs.org/en/stable/). [visited in 2015/9/11]
MITRE Corp., “python-stix 1.2.0.0 Documentation”, (available online at http://stix.readthedocs.org/en/stable/index.html). [visited in 2015/9/8]
MITRE Corp., “Structured Threat Information eXperssion (STIXTM)”, (available online at https://stix.mitre.org/). [visited in 2015/8/25]
Niemeyer, G., “python-dateutil”, (available online at http://labix.org/python-dateutil). [visited in 2015/9/20]

OASIS Open, “STIX[TM] Version 1.2.1. Part 1: Overview”, (availabe online at http://docs.oasis-open.org/cti/stix/v1.2.1/csprd01/part1-overview/stix-v1.2.1-csprd01-part1-overview.html). [visited in 2016/02/18]
Richter, S., “lxml - XML and HTML with Python”, (available online at http://lxml.de). [visited in 2015/9/17]
Thoreson, H., “How to Use STIX for Automated Sharing and Graphing of Cyber Threat Data”, (available online at https://www.recordedfuture.com/stix-overview/). [visited in 2015/9/23]
Websense Inc., “Websense 2015 Threat Report”, (available online at https://www.websense.com/assets/reports/report-2015-threat-report-en.pdf). [visited in 2015/10/13]

物聯網環境下資訊安全與個資保護關鍵成功要素之研究--以某醫療機構為例

李德威[a] 林裕淇[b] 賀盛志[a]

[a]國防大學管理學院資訊管理學系
[b]致理科技大學資訊管理學系

摘要

醫療資訊系統的發展與時俱進，每當醫療機構面對政府政策變革、作業流程改變時，最終雖可達到提升醫療院所行政作業效率的目的，然每次面臨改革時，均需通盤檢討諸多內、外部環境及法律、法規等不同議題的挑戰，管理階層從不同構面審慎思考，從而決斷關鍵成功要素，當前物聯網繼網際網路之後，成為影響醫療機構資通基礎建設服務品質的重大因素，故物聯網環境下醫療資訊系統整合物聯網科技產品在資訊安全與個資保護方面的議題，為本研究的主要背景和主軸。

本研究嘗試以 Saaty 等學者提出之 AHP 為主要研究技術，研究過程並透過文獻探討、專家訪談及問卷分析等方法，針對在物聯網環境下可能影響資訊安全和個資保護的重要關鍵因子，爰提相關資訊管理決策建議，以協助醫療院所可充分掌握物聯網新科技發展先機，縮短導入進程，形塑有利的營運契機，經本研究探討發現一些值得參考的決策因子，可供產業應用。

關鍵詞：物聯網、醫療資訊系統、資訊安全與個資保護、層級分析法

國防相關應用：可協助軍醫體系醫療院所掌握物聯網新科技發展先機，縮短導入進程，形塑有利的組織改造、資通基礎建設改善之營運契機。

A Case Study of the Critical Success Factors of Information Security and Personal Data Protection Based on a Medical Institute

Te-Wei Li[a] Yuh-Chi Lin[b] Sheng Chih Ho[a]

[a]Department of Information Management, Management College, National Defense University, Taiwan, R.O.C.
[b]Department of Information Management, Chihlee University of Technology, Taiwan, R.O.C.

Abstract

With the advancement of information technology, the medical information system changes considerably. When we are faced with changes in government policy or workflow to enhance the administrative efficiency of medical institutions or to improve service quality, the medical institutions should review the internal and external environment and the challenges of legal and regulatory issues. The management should carefully consider key success factors from different perspectives. Following the Internet, the Internet of Things(IoT) has become a major technological change that affects the information infrastructure of medical institutions. After the integration of the Internet of Things and medical information systems, the ICT system handles a large number of sensitive medical-related personal information, thus, how to protect information security and secure personal information is the main motivation of this study. In this study, we use the AHP method of Saaty as the main research technique, and we used literature review, expert interviews and questionnaire analysis as well. We use a systematic approach to identify key factors that affect information security and the personal information protection. And finally, we propose a couple of information management decision-making recommendations on information security, and personal data protection issues to help medical institutions to fully grasp the new chance of IoT technology, to shorten the process of introduction of technology and to create business competitive advantage.

Keywords: Internet of Things, Information Security Management System, Personal Information Management System, Analytical Hierarchy Process

Relevance to National Defense: Providing decision support for assisting the military medical system to master the new scientific and technological development opportunities, to shorten the construction period, to shape a favorable chance of organizational transformation and infrastructure improvement.

壹、緒論

1.1 研究背景與動機

在物聯網時代許多資訊必須保密，例如智慧門鎖的系統會自動紀錄何時出門、何時回家，並且記錄客人來訪次數、時間，物聯網是在網際網路的基礎上，如果科技會與生活這麼的緊密結合，將會有更多人在意隱私，也是目前科技服務所面臨的一大挑戰。而長期以來網路的研究，從 2005 年開始隱私的部份為最受到關注的議題。個人隱私的保護在互聯網已經成為嚴重的問題，所以在物聯網上將形成更嚴重問題。然而物聯網將可創造新的生活型態、達到智慧生活的目標，但資訊流通的安全性將成為一大隱憂。所以物聯網的應用延伸到消費者生活上，伴隨而來的的資訊安全問題應受重視。

隨著資通訊作業環境的改變，醫療產業作業環境已隨著資通訊技術演化而進入的物聯網時代，民國 92 年健保局完成全民健保卡全面 IC 化後，醫療機構紙本作業模式已逐步被電子檔案所取代，102 年 7 月，健保局建置了以病人為中心的健保雲端藥歷系統，可以即時查詢病人過去三個月的用藥紀錄，都皆已顯示資通訊技術演化之快速，然而隨著物聯網概念的崛起，部分醫療產業環境也開始逐漸在使用相關的技術。故本研究的主

軸為，探索當前物聯網繼網際網路之後，成為影響醫療機構資通基礎建設服務品質的重大因素。

1.2 研究目的

基於學者劉欣儀研究對物聯網方面的發現，促使我們可以深刻體認到未來物聯網的應用。隨者物聯網將會在未來遍及於人類的生活中，當所有物品與網路連接成為了智慧產品，實現遠端監看、監控及最佳化，物聯網的新時代將為人們帶來生活上的新體驗，在不久的將來可能成為生活重要的一環，因此在物聯網的環境下，消費者對於新科技的接受度是值得探討的。

雖然物聯網產品將提供一系列全新且豐富的價值創造與行銷模式，然而它也將面臨到許多的挑戰，尤其消費者對於相關服務內容的認知仍處於陌生階段，無法具體判斷採用物聯網服務後所能帶來的效益，而且個人資訊在物聯網應用流程中的傳輸、處理及運用，目前也沒有明確的法令規範與保護，根據資策會智慧網通系統研究所與產業情報研究所針對台灣民眾的物聯網應用需求進行調查發現，現今消費者愈來愈重視個人資訊及隱私的網路安全性，尤其對於「可能造成資訊安全問題或個人隱私風險」關切度較高，這些因素都將可能成為未來業者推動物聯網過程中，決定要不要採用的阻礙。

為了想瞭解當醫療機構欲導入物聯網技術時，相關的從業人員可能會有哪些疑慮及考量點，透過解決可能面臨到的資訊安全、個資保護議題，將來可作為陸續導入物聯網技術或欲改善作業流程之相關醫療機構的參考案例。

貳、文獻探討

2.1 物聯網的定義

學者高佑嘉於 2010 年提及物聯網指的是將無處不在的終端設備或設施,其中包括具備「內在智能」的感測器、移動終端、工業系統、樓控系統、家庭智能設施、視頻監控系統等和「外在使能」的物件，如貼上 RFID 的各種資產、攜帶無線終端的個人與車輛等等「智能化物件或動物」或「智能塵埃」,通過各種無線、有線的長距離或短距離通訊網串聯起來交換資訊。大家耳熟能詳的 Web4.0 即是物聯網絡實現互聯互通、應用大集成、以及基於雲計算的 SaaS 營運等模式，在 Intranet、Extranet 和 Internet 環境下，採用適當的信息安全保障機制，提供安全可控乃至客製化的時時在線監測、定位追溯、報警聯動、調度指揮、預案管理、遠程控制、安全防範、遠程維保、在線升級、統計報表、決策支持、領導桌面等管理和服務功能，實現對「萬物」(everyThing)的「高效、節能、安全、環保」的「管、控、營」一體化 TaaS(Thing as a Service)服務。物聯網及其相關的 TaaS 業務，在基於 Semantic Web 技術的 Web 3.0 基礎上，將構成 Web 4.0 的主體。

2.2 物聯網安全性探討

依據目前歐美先進國家及主要物聯網領導廠商的研究報告內容指出，目前探討物聯網安全性的議題包括:

2.2.1 巨量資料挑戰

隨著物聯網技術和應用的的推陳出新，連線上網的物體不侷限於電腦或網路設備，可連網物體成長迅速，醫療資料累積也呈指數規模持續增長，未來組織導入物聯網後，因連網裝置遽增將導致管理增加的資料量帶來了諸多挑戰，包括：

一、連線到資料中心的現有連結的頻寬容量

二、使用者資料的隱私問題

三、管理資料以進行即時通訊

四、選擇和分析適當的資料

2.2.2 安全策略

透過物聯網通訊時，大量不安全的裝置從未必安全的位置傳輸資料，以既有的網路架構言，無法確保現有的物聯網解決方案是安全無虞的，由於很多感應器、智慧物件和裝置連線到網路時，允許不安全的裝置存取組織網路，因此可能帶來的資料洩漏潛在危害，對於眾多醫療機構而言，存在潛在的資安挑戰。故探索物聯網中安全性議題無處不在，導入物聯網時通常應具有以下安全考量：

一、一致、自動化且可延伸，以保護組織的邊界

二、動態，以透過即時預測分析更好地確定安全威脅

三、智慧，提供跨所有連線和基礎架構元素的可見度

四、可延展，以滿足逐漸壯大的組織的需求

五、靈活，能夠即時做出反應

六、全面的端對端安全性

2.3 醫療資訊化應用系統介紹

2.3.1 醫院資訊管理系統(HIS)

學者黃昭瑋 2013 年的研究中指出醫院資訊管理系統 HIS(Hospital Information System）是以電腦為基礎，用於簡化所有醫院醫療和管理資訊。按照 Morris F. Collen 所給的定義：利用電子電腦和通訊設備，為醫院所屬各部門提供病人診療資訊(Patient Care Information)和行政管理資訊(Administration Information)的收集(Collect)、存儲(Store)、處理(Process)、提取(Retrieve)和數據交換(Communicate)的能力，並滿足所有授權用戶(Authorized)的功能需求。每個系統各司其職，分別支援醫療作業例：門急診住院醫屬開立；支援醫務行政作業例：掛號、批價、申報；支援醫院管理作業例：人力、資材；支援教學研究作業例：醫療個案研究。

目前我國醫療資訊系統的發展朝著整合式雲端服務的方向邁進，包含了整合臨床資訊系統(CIS)、醫學影像資訊系統(PACS)和檢驗資訊系統(LIS)、放射資訊系統 (RIS)。請參閱表 1　CIS、PACS、LIS、RIS 介紹:

表 1　CIS、PACS、LIS、RIS 介紹

LIS	RIS	PACS	CIS
醫囑簽收作業	醫囑簽收作業	放射儀器連線作業	資料接收轉換作業
檢查排程作業	檢查排程作業	放射影像管理作業	臨床研究作業
檢查報告作業	檢查報告作業		教學作業
檢驗儀器連線作業			
異常報告篩選作業			

2.3.2 臨床資訊系統(CIS)

陽明系統與合成生物學研究中心 2015 年的報告中指出美國神經病變與中風研究所開發出臨床資訊管理系統(Clinical Informatic and Management System，CIS)，並自 2003 年起正式啟用此系統，到現在已有約 8 年左右，目前美國國立衛生研究所(National Institutes of Health，NIH)的 20 多個研究中心或研究所，已有 90% 以上使用 CIS，此系統分為人體試驗暨研究倫理委員會(Institutional Review Board，IRB)使用的計畫追蹤與管理系統(Protocol Tracking and Management System，PTMS)與臨床研究資訊系統(Clinical Study Information System，CSIS)兩部份。PTMS 主要控管臨床研究計畫的產生、申請、審查與管理，讓研究者、審查委員及人體試驗委員會的行政人員彼此透過線上系統溝通，提升申請與管理計畫的效率與便利性。CSIS 則是管理試驗文件與病患資料，其可幫助研究者設計表單、病人管理、病人資料收集及資料分析分析。

2.3.3 醫學影像資訊系統(PACS)

2015 年維基百科資料說明醫學影像存檔與通信系統（Picture archiving and communication system，PACS）是一種專門用來儲存、取得、傳送與展示醫療影像的電腦或網路系統，PACS 這個名詞是由 Andre Duerinckx 博士所提出。

完整的醫療影像儲傳系統可以由不同的醫學影像器材取得影像，如：超音波影像、核磁共振、正子斷層掃描、電腦斷層掃描、乳房攝影與 X 光攝影等器材，而小規模的醫療影像儲傳系統則是由單一的醫療影像器材取得影像，通常這樣的系統會叫做 mini-PACS。

PACS 取代了傳統處理醫療影像的方式，如相片等，可使傳統之醫學影像系統具有遠端查閱與檢閱報告的能力。除此之外，它可使不同的醫療人員可以在不同的地點檢閱同一份醫療影像報告。並且由於數位儲存的成本降低，PACS 將可以減少傳統以相片儲存醫學影像，所需花費的大量經濟與空間成本，PACS 目前主要由幾個有名的醫學影像器材廠商所提供，相對於 PACS 所使用的硬體設施，PACS 的價格相當的昂貴與高成本。目前主要的供應商有： 台灣商之器(EBM)、美得康(Medincom)，美國奇異公司(GE)，愛克發(AGFA)，康世(Carestream Health)，柯達，韓國英非特(Infinitt)。但因 PACS 在建設的過程中常常需要配合當地法令、管理模式或習慣等因素進行客製化介面修改，並需常態性的系統維護，使得國內廠商亦有相當大的市場空間。

2.3.4 實驗室信息系統 LIS

實驗室信息系統（Laboratory Information System，縮寫 LIS）是一類用來處理實驗

室過程資訊的軟體。這套系統通常與其他資訊系統比如醫院資訊系統（HIS）連接。實驗室資訊系統由多種實驗室流程模組構成，這些模組可以依據客戶的實際情況進行選擇和配置。選擇適合的實驗室資訊系統對於使用者非常重要，往往要通過幾個月的研究和計劃。系統的安裝調試對於不同的研究階段也從幾周到幾個月不等，實驗室的研究工作有多少種就有多少種實驗室資訊系統。大型的實驗室信息系統幾乎包括了所有的實驗室研究的學科內容，比如血液學、化學、免疫學、血庫、外科病理學、解剖病理學、在線細胞計數和微生物學。這個條目將說明臨床實驗室的信息系統，包括了血液學、化學和免疫學內容。

2.4 台灣地區導入 ISMS&PIMS 主要醫療機構

2.4.1 臺大醫院

臺大醫院資訊機房於 2015 年 5 月取得 ISO/IEC 27001:2013 年版之驗證並於 2015 年 6 月 22 日 ISMS 資訊安全管理系統（ISO 27001）通過覆評。該院從 2008 年起持續積極推動資訊化及提升資訊安全防護能力及 ISO 27001 流程面及作業面改善，經歷 10 個月完成資訊安全政策、人員安全、實體與環境安全、存取控制、資訊安全事件管理等資訊室整體資訊安全管理制度的落實，強化該院之安全防護與應變作業，確保就醫民眾之病歷隱私及資料安全的權益。

2.4.2 中山醫學大學附設醫院

中山醫學大學附設醫院為提升院區資訊安全系統效能與提高院所服務品質，於 2010 年 4 月 21 日榮獲英國標準協會(British Standards Institution, 簡稱 BSI)頒發 ISO 27001 與中華民國 TAF CNS 27001 資訊安全管理系統雙驗證證書，並宣告正式啟動電子病歷元年，響應政府推動電子病歷，保證病患的個資安全，驗證範圍包括資訊安全管理、資訊安全政策、資安組織、資訊資產管理、人力資源安全、實體與環境安全、通訊與作業管理、存取控制、資訊系統獲取開發及維護、資訊安全事故與業務持續等作業。

中山醫學大學附設醫院在醫療機構推動電子病歷的過程中，發現規劃建置資訊安全管理機制時，如何確保完整的資訊安全管理系統是該院電子病歷系統服務品質良窳的重要考量，現階段該院持續改善 ISMS 管理系統，遵循 PDCA 精神永續經營，已可有效保障個人健康資訊隱私及個資安全。

2.4.3 馬偕醫院

馬偕醫院資訊中心於 2015 年 9 月 2 日審查通過新版 ISO27001:2013 資安標準之驗證並取得證書，該院資訊中心致力執行教育部 ISMS 要求項目外，並通過比教育部版更加嚴謹的 ISO27001:2013 驗證，在 ISMS 實踐上，已達國際標準並與國家政策要求同步，其驗證範圍包括資訊安全管理、實體與環境安全、AD Server 安全管理等作業。

2.4.4 慈濟醫院

行政院衛生署於 2004 年起透過「國民健康資訊建設計畫」(National Health Informatics Project)成功推動「電子病歷」，醫院將過去紙本的病歷電子化，也要讓病人能夠隨時讀取自己的電子病歷，為能有效保障病歷的保密性；該院於 2008 年開始實施電子病歷子計畫，2009 年完成電子病歷的資訊安全強化案，並於通過 ISO27001:2005 驗

證，並於短短六個月內慈濟六院區陸續通過資訊安全國際標準 ISO27001:2005 及國家標準 CNS27001:2007 的評鑑，這是實施電子病歷與跨院病歷互通的資安重要關卡，奠定該院資訊安全際個資保護的政策宏規。

2.4.5 亞東醫院

亞東醫院於 2015 年 10 月 1 日通過 ISO 27001:2013 國際資訊安全標準的驗證，其驗證範圍為資訊處環境安全、機房維運、電子病歷系統維運。該院的目標係建立全面電子化的醫院，現階段該院全院的作業流程，均可透過資訊系統管控，可確保全院資訊系統的可用性，資料的完整性與隱私性，其 ISMS 驗證範圍包括:資訊處環境安全、機房維運、入出院病歷摘要系統維運等作業。

2.5 關鍵成功因素

2.5.1 關鍵成功因素定義

關鍵成功因素(Key Success Factors, KSF 或 Critical Success Factors, CSF)的觀念，最早是由 Daniel（1961）所發表的文章「管理資訊的危機」所提出。他認為大部份的產業都具有三到六個決定成功與否的關鍵要素，如果一個公司能夠將這些關鍵成功因素做好，那麼這個公司便能成功。而後許多行業都引用關鍵成功因素的策略觀點，希望藉此鞏固企業地位以達成永續經營。

茲列舉一些學者對關鍵成功因素所下定義如表 2：

表 2 學者對關鍵成功因素的定義

學　者	定　義
Daniel（1961）	一個公司要成功必須做得特別好的部分。
Boyton＆Zmud（1984）	確認行業的關鍵成功因素，把企業資源集中投入可取得競爭優勢的特定領域中，是尋找策略優勢的途徑之一。
Ferguson＆Dickinson（1982）	組織為成功必須做好的關鍵領域。
大前研一（1983）	關鍵成功因素是尋找策略優勢的途徑之一，把企業的資源集中投入在特定領域中，以獲取產業競爭優勢。
Leideckerand and Bruno (1984)	關鍵成功因素是一企業或經理人欲獲得良好績效或成功，而必須給予特別且持續注意的一些事情。關鍵成功因素包括目前及未來影響該企業營運活動成功的主要因素。
Aaker（1984）	關鍵成功因素係指企業最重要的競爭能力或競爭資產。
吳思華（1988）	關鍵成功因素係指在特定產業中，能夠成功地與其他競爭者競爭，所需具備的技術或資產。
Davis (1979)	關鍵成功因素是企業在環境不確定之下的一個方向性規範。
Rockart (1979)	關鍵成功因素是管理階層必須時時注意的某些活動，執行良好可以帶給組織成功的競爭的表現。

綜合上述學者的觀點，可得知關鍵成功因素會隨著產業、時間、地域而有所不同，而其本質是企業為取得競爭優勢，所應具備的競爭能力、資源與條件，而透過將有限的資源運用在攸關的競爭領域上，以建立產業中的優勢地位。本研究認為關鍵成功因素乃是企業經營成功的必備條件，使企業能在產業中取得競爭優勢，所必須具備的技術或資產，其不僅能使企業有效達成既定目標，更能讓企業在產業中獲得持久的競爭優勢，達到永續經營的目的，同時，本研究也認為關鍵成功因素也會是物聯網技術及應用導入與

人的生命、尊嚴息息相關的醫療產業前，應藉由學術探討與分析，讓學者、未來的應用者都能了解個關鍵因素及其重要性。

2.5.2 關鍵成功因素的特性

關鍵成功因素可用來分析企業在產業競爭中的成功因素、分析資訊系統成功要素，也可用來找出個人成功的特質。不同的學者所從事研究目標領域主要有：資訊系統、策略管理等 。

一、根據以往文獻，孟德芸(1988)將關鍵成功因素的功能歸納為五大項：

(一)用為組織在分配其資源時的指導原則。

(二)簡化高階管理者的工作。

(三)做為企業經營成敗的偵測系統。

(四)做為規劃管理資訊系統時的工具。

(五)利用 CSF 作為分析競爭對手強弱的工具。

二、Aaker(1984)認為在考慮關鍵成功因素時應注意下列幾項特性：

關鍵成功因素因產業、產品、市場之不同而各異。

(一)關鍵成功因素也應考慮到未來發展之趨勢，如果沒有瞭解其改變的方向，而貿然投入該產業，將會給公司帶來很大的災難。

(二)關鍵成功因素亦隨產業之生命週期之改變而變化。

(三)關鍵成功因素隨產業不同而各異，也因時間改變而改變。

(四)管理者不應將所有的事情都當做關鍵成功因素，而必須集中於某些特定事物上，來決定產業的關鍵成功因素，管理者必須深入研究、評估與分析並大膽致力於少數幾個關鍵成功因素，以作為策略形成。

綜上所述，關鍵成功因素的特性簡單來說，它可能會隨著環境、時間、產品等的改變而改變，皆是企業為求生存、為提升競爭力所必須重視的資源和相關因素。因此，管理者在當中必須扮演一個能隨時應變與找出關鍵因素的角色，即能獲得更大的相對競爭優勢及能耐，才能使企業在此產業環境中更勝出。

2.6 層級分析法

一、AHP 之意義

層級分析法(Analytical Hierarchy Process, AHP) 主要是美國匹茲堡大學教授 Thomas L. Saaty(1980)為在不確定情況下處理複雜的決策問題上，用來評估各種相關要素間之重要性高低程度，在 1980 年提出一個有系統性的決策模式。由於 AHP 理論本身簡單而且具備高度實用價值，其主要意義在於彙整有關學者專家或者使用者之意見，進行一種集體決策之模型分析。

AHP 法是將複雜的問題簡化為簡明的要素層級系統。再彙集學者專家的意見及各階層決策者的意見，進行各要素間的成對比較(Pairwise Comparison)，予以量化後建立成對比較矩陣(Pairwise Comparison Matrix)，據以求出各矩陣之特徵向量(Eigenvector)。並依其特徵向量作為層級各要素間的優先順序，並求算出最大特徵值，用予以評定成對比較矩陣一致性指標的相對權重之強弱，以提供決策者做決策時的參考指標。其層級是由至

少兩個以上的層級所組成，而 AHP 則將各個層級連結起來，計算出 AHP 層級之各因素間相對整個層級的優先名、相對權重。接著，AHP 可建立連接所有成對比較矩陣之一致性指標(Consistency Index, C.I.)與一致性比率(Consistency Ratio , C.R.)。依此程式最後評估出整個層級的一致性的高低程度。(鄧振源、曾國雄, 1989)

二、AHP 之優缺點

根據鄧振源、曾國雄（1989）及溫博煌（2003）提出層級分析法相關文獻整理後主要有以下之優缺點：

(一)優點

1. 在處理較抽象的因果關係上，較絕對性的處理方式量化客觀。
2. 可藉由一致性篩選有效問卷，以控制結果的可信度。
3. 操作過程相當簡易，無繁瑣的計算。
4. 利用要素個體形成層級形式，易於達成工作。
5. 有助於描述高層級要素對低層級要素的影響程度。
6. 對整個系統的結構面與功能面，能詳細的描述。
7. 自然系統都是以層級的方式組合而成，而且是一種有效的方式。
8. 層級具有穩定性（Stability）與富有彈性（Flexibility）；即微量的改變能形成微量的影響，同時新層級的加入，對一結構良好的層級而言，並不會影響整個系統的有效性。

(二)缺點

1. 階層中各因素的評定階層關係的建立並無一定的準則，而此步驟又是 AHP 的重要關鍵，因此在建構時宜格外謹慎小心，多收集有關的資訊。
2. 由於量化的基礎是建立在各受訪者主觀的判斷，容易受到極端的影響。另外，由於整個階層包含的課題太廣，部分受訪者可能只專精於某些項目，而非整個問卷內容，可能會影響整個問卷的有效性。
3. 用於量化的名目尺度並非量化的尺度，可能導致比較時不確定的現象。
4. Saaty 建議以九分法建立名目尺度，共有 17 個比重值，在實際填寫時可能過於細分而無法明確決定比重的困擾，因此可視問題的複雜程度調整名目尺度的劃分法。

三、AHP 之應用

一般採取 AHP 乃根據於如下四項理由：

(一)理論基礎簡單，使用容易，能擷取大部分專家及決策者之共識意見。

(二)對於可能影響研究目標產業經營成功之要素，都能清楚納進模型之中，配合週邊環境，考慮到各種不同構面。

(三)對於一些計量因素，經過專家、學者評估及數學分析後，皆能以具體的數字顯示各要素的先後順序。

(四)將複雜的評估要點以容易理解的層級表現出來，方便決策者所參考。

2.7 隱私與物聯網的關係與影響

網路的發展，為人類帶來便捷而迅速的生活，但也讓網路隱私影響到個人的權益(陳

煌勛,2005）。然而物聯網是在網際網路的基礎上，並利用許多的感測元件，構造一個萬事萬物的聯網。Huaiqing 等學者認為，隱私通常被認為個人的資訊，而侵權的行為發生會被形容成，例如未經過許可的搜集、揭露而使用個人資訊。當個人訊息變成掌握在他人手裡，就使得隱私的問題不斷出現（Westin,1967;Flaherty,1989; Singer, Mathiowetz & Couper,1993）。

本研究針對個資法施行細則，有關個資的定義包含一般個資及敏感個資，強調保有個資之單位須強化其個資保護，根據個資法施行細則第 12 條規定計有配置管理之人員及相當資源、界定個人資料之範圍、個人資料之風險評估及管理機制等 11 項保護原則可參考。

2.8 資通安全管理法草案

隨著資通科技的蓬勃發展，無線網路、行動裝置、雲端服務與智慧聯網等新興科技之使用，已然是每個人生活中重要的一環，隨之而來的資通安全風險也大幅增加，資通安全也越來越受到重視。

參諸國際近年對於資通安全之保護，已逐漸以訂立專法之方式加以規範，例如：美國的聯邦資訊安全現代化法、網路安全法，日本的網路安全基本法等；在國際組織部分，歐盟近日亦甫通過網絡暨資訊系統安全指令。於我國，在公務機關目前已設有資通安全推動單位與相關遵行規則，包括行政院及所屬機關資訊安全管理要點、行政院及所屬各機關資訊安全管理規範、國家資通安全通報應變作業綱要等，若能進一步透過專法之設立，賦予各機關資通安全維護義務之法律基礎，將更能有效提昇我國公務機關之資通安全能量。

2016 年 7 月 28 日，隸屬總統府國安會，負責國家整體資安方向的諮詢委員李德財，為了讓下設的資通安全辦公室（簡稱國安辦）和同年 8 月 1 日正式成立的行政院資通安全處（簡稱資安處）發揮相輔相成的效果，指派國發會管制考核處處長何全德兼任國安辦主任一職。國安辦、資安處以及 NCC（監督電信網路安全），形成政府資安鐵三角。

今年 8 月 28 日，國發會科技政委吳政忠表示，為了打造數位經濟時代所需的生態系統，將力推《資通安全管理法》在年底前完成三讀。

目前該草案正在推導當中，ISMS 即將法制化，法制化後將要求各目的事業主管機關所屬之督導單位，例如衛福部要求各醫療院所單位內必須強制通過驗證 ISMS 驗證，組織內必續配置相對人力及能量來維護資訊安全。

參、研究方法

本研究透過文獻探討、相關文獻分析與專家訪談等方法，找出可能影響醫療機構在物聯網環境下資訊安全與個資保護關鍵成功因素，主要運用 AHP 法，並採取專家訪談及問卷的研究方式實施。第一階段專家訪談取得專家共識，篩選出影響醫療產業環境下導入物聯網技術及應用之重要關鍵成功因素指標；第二階段運用 AHP 法來作為關鍵成功因素之分析，建構評估指標之權重體系。

3.1 文獻分析法

本研究首先以文獻探討方法，透過蒐集國內醫療機構進行醫療資訊化時對於資訊安全風險評估及安全管理機制之來源與相關政策內涵，據以彙整出訪談所需之題目及建議意見，參考文獻包含專書著作、學術研究期刊、網路新聞及公報等國內外資料。

3.2 專家訪談法

本研究運用半結構式之專家訪談法，訪談對象為本研究訪談對象為某醫療機構資訊室及某上市醫療系統協力廠商，其負責及經手之業務涵蓋醫療機構之基礎建設、醫療醫訊系統維護或開發等，工作內容涉及資安業務且接觸個人資料之管理人或資深幕僚合計 15 員，如表 3 所示，並依所蒐集之文獻，結合作者工作經驗，先行擬定訪談大綱，再依訪談結果調整研究層級架構，以增加研究之信效度。

表 3 專家訪談對象一覽表

編號	單位名稱	職稱	工作年資
1	某醫療機構資訊室	主任	7 年以上
2	某醫療機構資訊室	副主任	7 年以上
3	某醫療機構資訊室	副主任	5 年以上
4	某醫療機構資訊室	組長	5 年以上
5	某醫療機構資訊室	副組長	5 年以上
6	某醫療機構資訊室	副組長	3 年以上
7	某醫療機構資訊室	管理師	3 年以上
8	某醫療機構資訊室	管理師	3 年以上
9	某醫療機構資訊室	副管理師	3 年以下
10	某醫療機構資訊室	副管理師	3 年以下
11	某上市醫療系統資訊團隊	專案經理	5 年以上
12	某上市醫療系統資訊團隊	資深工程師	5 年以上
13	某上市醫療系統資訊團隊	資深工程師	5 年以上
14	某上市醫療系統資訊團隊	工程師	3 年以下
15	某上市醫療系統資訊團隊	工程師	3 年以下

3.3 層級分析法(AHP)

本研究係運用 AHP 法決定關鍵因素之優先順序，作為本研究之主要研究方法。分析層級程序法發展的目的就是將複雜的問題系統化，減少決策錯誤的風險，以提供決策者做最適之選擇。本研究仍採此法來做為物聯網環境下資訊安全與個資保護關鍵成功要素之研究(AHP 問卷產製與處理流程如圖 1)：

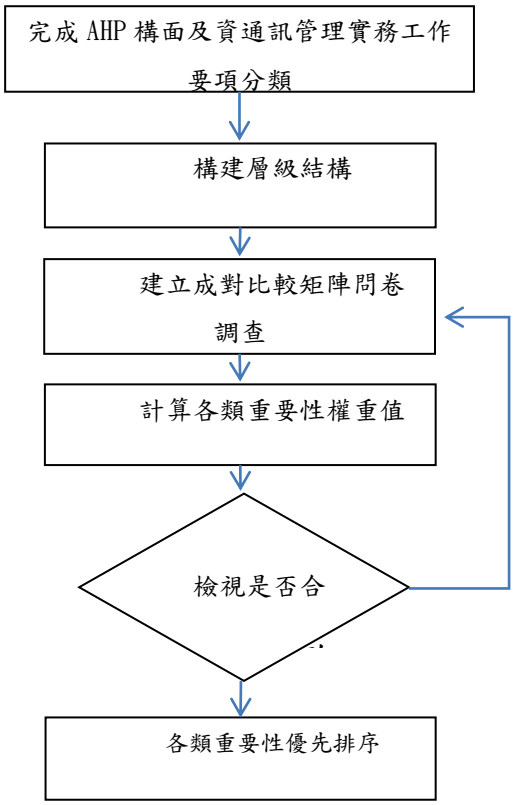


圖 1　AHP 問卷產製與處理流程圖

肆、研究架構

本研究係採取文獻探討方式進行，蒐集國內各大醫療機構導入ISO 27001及醫療資訊系統相關文獻，綜整文獻中醫療機構對於醫療作業資訊化之作業要求項目，找出可能影響在物聯網環境下影響資訊安全與個資保護關鍵成功要素之評估指標，第一階段透過專家訪談取得共識，篩選出可能的成功因素指標後，第二階段藉由運用AHP分析法建構評估指標之權重體系。本研究架構如圖2所示：

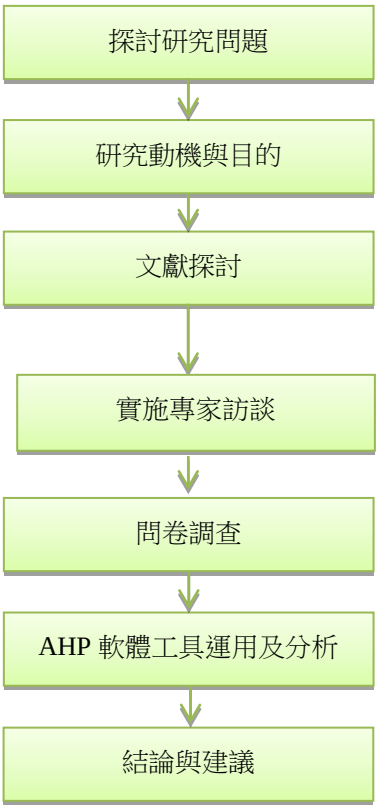


圖 2 研究架構圖

4.1 本研究關鍵成功要素的主要構面及相關要素

經由相關文獻探討中發現針對環境因素計有:裝置、設備是否為符合法規、建置物聯網系統合乎成本效益、感測器昂貴且仰賴進口，阻礙物聯網發展等 14 項影響因素，經訪談專家後取得的共識計有導入物聯網法規限制、操作行動平台實施行動醫療行為的法規限制(如，必須要有具備執業許可的醫師，才能使用 APP 診斷疾病、治病)、社會期望或要求、政治力介入或要求、非蓄意使用之法律責任影響使用者意願、物聯網設備存在安全漏洞對隱私侵犯的可能性等共計 12 項共識；針對組織因素計有使用者（醫師及護理人員）對物聯網系統的需求和科技接受、建置物聯網系統合乎成本效益、醫師對於物聯網系統功能之「使用動機」等 14 項影響因素，訪談專家後取得的共識有使用者（醫護理人員）對物聯網科技、系統功能、使用意願的接受度、導入物聯網系統於醫護作業上，使用者的接受度（認知易用性與認知有用性）、醫護高階主管的支持度及全員參與意願等計 14 項共識；針對技術因素計有物聯網系統資料存取的安全性、醫院的資訊基礎建設架構、物聯網系統所產生磁場強度對醫院儀器和病人的影響等 14 項影響因素，訪談專家後取得的共識有醫院的資訊基礎建設架構、導入物聯網後個資隱私及及資安衝擊分析識別、加解密控制措施等計 11 項共識如以下附表 4 所示。

表 4 本研究物聯網環境下訊安全與個資保護之影響因素前後對照表

調　整　前		調　整　後	
構面	影響因素項目	構面	影響因素項目
環境因素	1. 裝置、設備是否為符合法規只能以標示非醫療器材且不可強調療效。 2. 建置物聯網系統合乎成本效益，能否為公司帶來大幅度的經濟成長效益。 3. 感測器昂貴且仰賴進口，阻礙物聯網發展。 4. 醫療設備稍有故障、誤動作可能就會造成醫療失誤，甚至危及用戶健康與生命，應檢視是否符合應用需求設置的法規。 5. 需定義裝置是否為正統醫療裝置的附屬配件，還只是將行動平台轉成醫療器材。 6. 若要將行動平台藉由行動醫療 Apps 轉成合法的醫療器材，則限制必須要有具備執業許可的醫師，使用它來診斷疾病、治病。 7. 低於社會期望。 8. 政治力介入。 9. 智慧財產權。 10. 非蓄意使用之法律責任。 11. 安全漏洞或隱私侵犯。 12. 跨越國界的資訊流。 13. 依法實施的監視設備與人權之間之衝突。 14. 員工及承包商應敘明雙方對資訊安全的責任並簽訂之契約化協議書。	環境因素	1.導入物聯網法規限制。 2.操作行動平台實施行動醫療行為的法規限制(如，必須要有具備執業許可的醫師，才能使用 APP 診斷疾病、治病)。 3.社會期望或要求。 4.政治力介入或要求。 5.非蓄意使用之法律責任影響使用者意願。 6.物聯網設備存在安全漏洞對隱私侵犯的可能性。 7.產生跨越國界或組織邊界的資訊流，肇生違法或違規的可能性。 8.要求員工及承包商簽署資訊安全契約化協議書是否存在窒礙。 9.存在侵犯智慧財產權的可能性。 10.存在侵犯隱私權保護的可能性。 11.營銷模式的創新具有投資誘因。 12.導入物聯網可能造成法律、法規遵循性問題(如，違反當地或國際法規)。

續 1

調　整　前		調　整　後	
構面	影響因素項目	構面	影響因素項目
組織因素	1.使用者（醫師及護理人員）對物聯網系統的需求和科技接受。 2.導入物聯網系統於醫護作業上，使用者的接受度（認知易用性與認知有用性） 3.醫師對於物聯網系統功能之「使用動機」 4.導入的接受度，特別在「認知易用性」的「資訊教育程度」、「系統」因素 5.導入醫護作業工作中之使用意願 6.高階主管是否支持。 7.資訊應依法律 要求、價值、重要性及對未經授權揭露 或修改之敏感性分級。 8.制定相關的資安政策 9.資訊、系統操作人員是否有資安意識，有無良好的教育訓練。 10.員工及外部使用者於離職或契約協議終止時，應歸還其據有之全部組織資產。 11.是否符合資料保留及銷毀政策。 12.組織人員異動，廠商專案改組。 13.資訊安全政策應依規劃之期間 當系統或架構發生重大變更時，資訊安全政策應再次審核以確保其持續的合宜性、適切性及有效性 14.成本超支、過度壓縮專案進度，超過完工時程。	組織因素	1.使用者（醫護理人員）對物聯網科技、系統功能、使用意願的接受度。 2.導入物聯網系統於醫護作業上，使用者的接受度(認知易用性與認知有用性） 3.醫護高階主管的支持度及全員參與意願。 4.資訊安全、個資保護政策。 5.資安意識培養及教育訓練。 6.對現有組織人員造成異動或專案改組。 7.營運持續計畫之衝擊。 8.造成單位成本超支或失控。 9.人力資源安全。 10.影響個資範圍界定(尚未建立或需重新界定)。 11.影響個資風險評估及管理機制(尚未建立或需重新界定)。 12.事故預防、通報及應變機制(尚未建立或需重新界定)。 13.導入物聯網對個資蒐集、處理、利用織內部管理作業程序之影響。 14. 資產管理。

續 2

調整前		調整後	
構面	影響因素項目	構面	影響因素項目
技術因素	1. 物聯網系統資料存取的安全性 2. 醫院的資訊基礎建設架構 3. 物聯網系統所產生磁場強度對醫院儀器和病人的影響。 4. 物聯網系統資料的存取速度。 5. 物聯網系統資料存取的安全性。 6. 資料保護依層級設置存取權限。 7. 應依適用之相關法令、法規中之要求，以確保個人可識別資訊之隱私及保護。 8. 應存取控制政策要求時，得以保全登入程序，利用雙因子控制認證對系統及應用之存取。 9. 網路芳鄰、USB 儲存媒體裝置是否禁用，或經由控管方能申請特殊權限。 10. 外部儲存媒體應由專人管控，並按照正式程序加以安全汰除或更換。 11. 是否遵循營運及資訊安全要求事項，建立、文件化及審查存取控制政策。 12. 資產擁有者或系統管理人是否定期審查使用者之存取權限。 13. 是否使用互動式通行碼系統，並應確保嚴謹通行碼，不被機器人程式破解。 14. 資訊服務、使用者網路及資訊系統網路是否區隔。 15. 於使用秘密鑑別資訊時，應要求使用者遵循組織之實務規定。 16. 智慧型手機或是平板是否裝設防毒軟體。	技術因素	1. 醫院的資訊基礎建設架構(資料、語音、物聯網等)之相容性及支援程度(存取速度、安全性及權限控管等)。 2.導入物聯網後個資隱私及及資安衝擊分析識別。 3. 加解密控制措施。 4.實體及環境安全控管。 5.內外部安全稽核機制。 6.使用紀錄、軌跡資料及證據保存。 7. 存取控制與身份識別。 8. 通訊安全。 9. 系統開發、獲取及維護 10. 行動裝置及遠距工作 11. 運作安全

肆、資料分析和研究結果

本研究主要是將問卷發放至相關人員填寫回收後，對所回收之問卷資料加以整理與分析，運用 Microsoft Excel 2013 與 Expert Choice 2000 軟體進行資料統計分析，計算其權重值及一致性檢定，以獲得最終本研究結果。

4.2 問卷結果與資料分析

本研究根據文獻探討所擬出的評估指標，彙整相關專家學者看法後，對問卷項目之內容進行評估與修訂，使問卷具有一定之內容效度後，以某醫療個案單位人員為研究對象，於 2016 年 7 月 1 日至 2016 年 8 月 30 日進行問卷調查，以網路問卷、電子郵件方式發放問卷，共發出 60 份問卷，計回收 52 份問卷，回收率為 86%。在資料分析工具方面，本研究採用 Expert Choice 2000 軟體，計算出權重值與一致性檢定。

一、樣本結構分析

Expert Choice 2000 軟體中，其一致性檢驗是以 I.R 值表示不一致比例(Inconsistency Ratio, I.R.)，其決斷值已不超過 0.1 為佳。故剔除 8 份無效問卷後，餘 44 份有效問卷基礎資料彙整如表 4。

(一)受訪者基本資料分析

1.年資：1-3 年回收 4 份，佔有效問卷百分比 9.09%；4-6 年回收 23 份佔有效問卷百分比 52.27%；7-9 年以上回收 10 份佔有效問卷百分比 22.73%；10 年以上回收 7 份佔有效問卷百分比 15.91%。

2.工作職稱：技術人員回收 30 份，佔有效問卷百分比 68.18%；主任工程師回收 11 份，佔有效問卷百分比 25%；主管回收 3 份，佔 6.82%。

3.教育程度：在專科(含以下)回收 5 份，佔有效問卷百分比 11.36%，具有大學/技術學院學歷者回收 29 份，佔有效問卷百分比 65.91%，具有碩士學位者回收 7 份，佔有效問卷百分比 15.91%；具有博士學位者回收 3 份，佔有效問卷百分比 6.82%。

表 4 樣本結構分析數值表

項目	資料類別	樣本數	有效問卷百分比
年資	1-3 年	4	9.09%
	4-6 年	23	52.27%
	7-9 年	10	22.73%
	10 年以上	7	15.91%
工作職稱	醫護人員	30	68.18%
	資訊人員	11	25%
	醫護、醫護主管	3	6.82%
教育程度	專科(含以下)	5	11.36%
	大學/技術學院	29	65.91%
	碩士	7	15.91%
	博士	3	6.82%

二、本研究目標劃分第一層與第二層級間衡量因素分析說明

運用本研究目標「物聯網環境下資訊安全與個資保護關鍵成功要素之研究」劃分第二層級衡量因素即為「環境層面」、「組織層面」及「技術層面」等三個因素，經以

Expert Choice 2000 軟體運算，由於無效問卷已剔除，求得第一層級要素之一致性指標 Incon=0.00＜0.1，顯示其一致性程度可被接受，其相對權重及次序如表 5 及圖 3 所示

表 5 第二層及構面之權重排序表

衡量要素	相對權重	次序	一致性指標
組織層面	0.302	2	Incon=0.00 with 0 missing judgments.
環境層面	0.23	3	
技術層面	0.468	1	

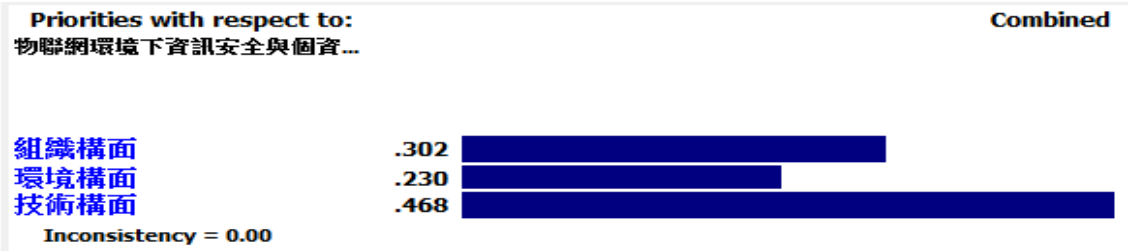


圖 3 主要構面相對權重分配長條圖

依上述結果分析，第二層要素的評估優先順序依次為「技術層面」>「組織層面」>「環境層面」，代表多數人認為「技術層面」為最重要階段(權重值為 0.468)，應列為物聯網環境下資訊安全管理與個資管理最重要的考量因素。

三、各構面評估指標之相對權重結果分析

(一)「技術層面」

個案單位對於「技術層面」之評估指標的相對重要性從表 6 及圖 4 可看出，以不一致性指標（IR）為 0.07，符合小於 0.1 之要求，表示判斷結果皆符合一致性，在一致性檢定方面皆符合標準。

表 6「技術層面」構面所包含要素之權重排序表

衡量要素	相對權重	次序	一致性指標
資訊安全	0.165	3	Incon=0.07 with 0 missing judgments.
行動裝置及遠距工作	0.222	2	
導入物聯網後個資隱私及及資安衝擊分析識別	0.046	6	
系統開發、獲取及維護	0.113	4	
實體及環境安全控管	0.031	7	
醫院的資訊基礎建設架構(資料、語音、物聯網等)之相容性及支援程度(存取速度、安全性及權限控管等)	0.077	5	
存取控制與身份識別	0.345	1	

資料來源：本研究整理

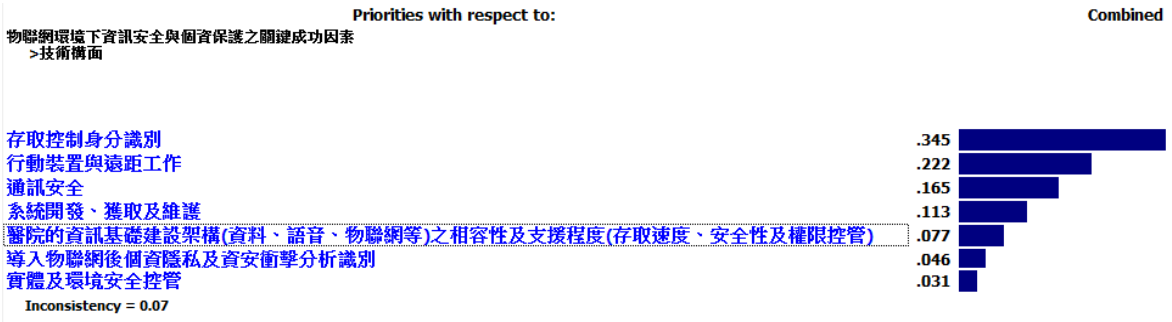


圖 4 技術層面評估指標相對權重分配長條圖

依上述結果分析，於「技術層面」第三層要素的評估優先順序依次為存取控制與身份識別(0.345) ＞行動裝置及遠距工作(0.222) ＞通訊安全(0.165) ＞系統開發、獲取及維護(0.113) ＞醫院的資訊基礎建設架構(資料、語音、物聯網等)之相容性及支援程度(存取速度、安全性及權限控管等) (0.077) ＞導入物聯網後個資隱私及及資安衝擊分析識別(0.046) ＞實體及環境安全控管(0.031)。

因此，在物聯網環境下之醫療機構在既有資訊安全政策及個資管理下於「技術層面」最重要且應優先考量的技術因子之項目為「存取控制與身份識別」。

(二)組織層面

個案單位對於組織構面之評估指標的相對重要性從表 7 及圖 5 可看出不一致性指標（IR）為 0.07，符合小於 0.1 之要求，表示判斷結果皆符合一致性，在一致性檢定方面皆符合標準。

表 7「組織層面」構面所包含要素之權重排序表

衡量要素	相對權重	次序	一致性指標
造成單位成本超支或失控	0.121	4	Incon=0.07 with 0 missing judgments.
資安意識培養及教育訓練	0.234	2	
影響個資風險評估及管理機制(尚未建立或需重新界定) (0.050)	0.05	6	
醫護高階主管的支持度及全員參與意願	0.167	3	
導入物聯網系統於醫護作業上，使用者的接受度（認知易用性與認知有用性）	0.081	5	
資訊安全、個資保護政策	0.325	1	
資產管理	0.023	7	

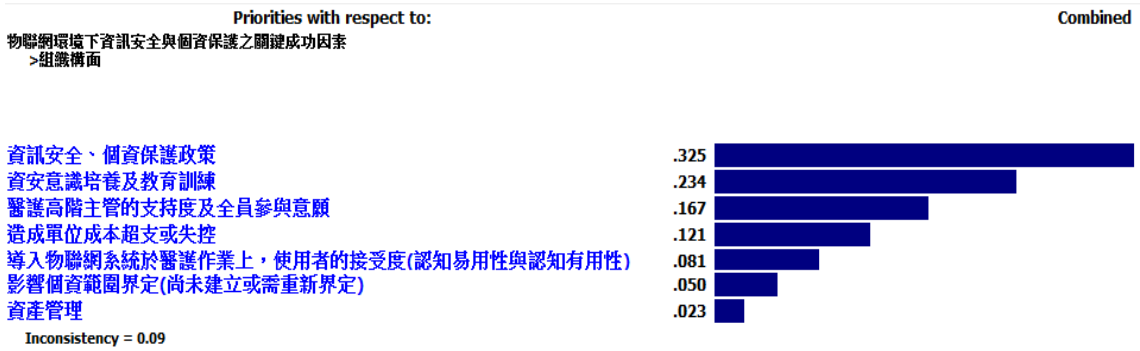


圖 5 組織層面評估指標相對權重分配長條圖

依上述結果分析，於「組織層面」第三層要素的評估優先順序依次為資訊安全、個資保護政策(0.325) ＞資安意識培養及教育訓練(0.234) ＞醫護高階主管的支持度及全員參與意願(0.167) ＞造成單位成本超支或失控(0.121) ＞導入物聯網系統於醫護作業上，使用者的接受度（認知易用性與認知有用性）(0.081) ＞影響個資風險評估及管理機制(尚未建立或需重新界定) (0.050) ＞資產管理(0.023)。

因此，在物聯網環境下於「技術層面」應以最重要且應優先考量的組織影響因子之項目為「資訊安全、個資保護政策」。

(三)環境層面

個案單位對於環境構面之評估指標的相對重要性從表 8 及圖 6 可看出不一致性指標（IR）為 0.07，符合小於 0.1 之要求，表示判斷結果皆符合一致性，在一致性檢定方面皆符合標準。

表 8「環境層面」構面所包含要素之權重排序表

衡量要素	相對權重	次序	一致性指標
要求員工及承包商簽署資訊安全契約化協議書是否存在窒礙	0.032	7	Incon=0.07 with 0 missing judgments.
存在侵犯隱私權保護的可能性	0.315	1	
社會期望或要求	0.175	3	
產生跨越國界或組織邊界的資訊流，肇生違法或違規的可能性	0.126	4	
營銷模式的創新具有投資誘因	0.086	5	
導入物聯網可能造成法律、法規遵循性問題(如，違反當地或國際法規)	0.22	2	
非蓄意使用之法律責任影響使用者意願	0.048	6	

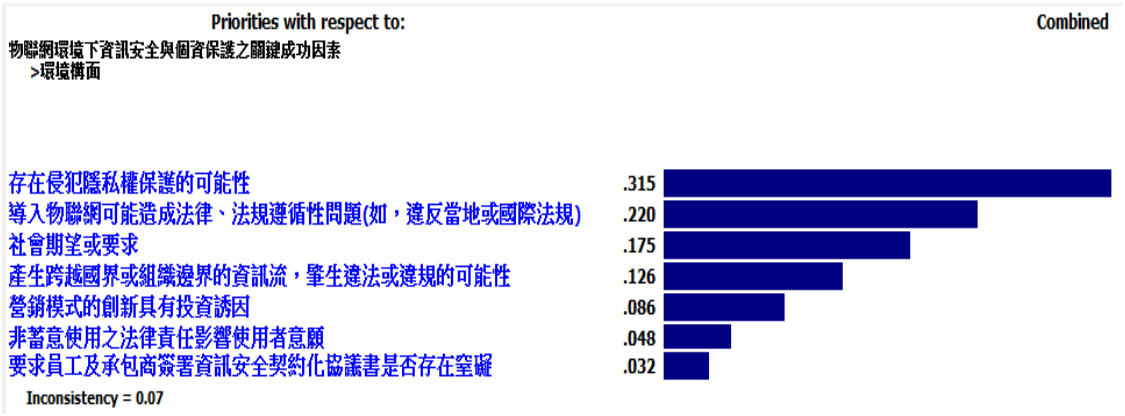


圖 6 環境層面評估指標相對權重分配長條圖

依上述結果分析，於「環境層面」第三層要素的評估優先順序依次為存在侵犯隱私權保護的可能性(0.315) ＞導入物聯網可能造成法律、法規遵循性問題(如，違反當地或國際法規) (0.220) ＞社會期望或要求(0.175) ＞產生跨越國界或組織邊界的資訊流，肇生違法或違規的可能性(0.126) ＞營銷模式的創新具有投資誘因(0.086) ＞非蓄意使用之法律責任影響使用者意願(0.048) ＞要求員工及承包商簽署資訊安全契約化協議書是否存在窒礙(0.032)。

因此，在物聯網環境下於「環境層面」應以最重要且應優先考量的環境影響因子之項目為「存在侵犯隱私權保護的可能性」。

4.3 整體評估指標權重結果分析

本研究在最終評估目標「物聯網環境下資訊安全與個資保護之關鍵成功因素」之下，首先進行整體層級的一致性檢定，如圖 7 所示。每一層級下各分項內皆可算出其權重值，將其與各層級之目標權重值相乘，即可得出各評估指標之整體權重值，繼而進行各重要因素之綜合評點，分別計算其權重並依權重高低排序歸納出在物聯網環境下資訊安全與個資保護之關鍵成功因素。

經由整體評估結果顯示，以 OII 取代 CRH，整體階層一致性考驗之 O.I.I 值為 0.05，小於等於 0.1 之臨界值，表示整體因素層級結構符合一致性，表示各矩陣一致性比率高，所得之權重分配值可以接受。

其評估指標整體權重結果與排序如下：

存取控制與身份識別(0.155) ＞行動裝置及遠距工作(0.100) ＞資訊安全、個資保護政策(0.100)＞存在侵犯隱私權保護的可能性(0.076) ＞通訊安全(0.074) ＞資安意識培養及教育訓練(0.072) ＞導入物聯網可能造成法律、法規遵循性問題(如，違反當地或國際法規) (0.053) ＞醫護高階主管的支持度及全員參與意願(0.052)＞系統開發、獲取及維護(0.051) ＞社會期望或要求(0.042) ＞造成單位成本超支或失控(0.037)＞醫院的資訊基礎建設架構(資料、語音、物聯網等)之相容性及支援程度(存取速度、安全性及權限控管等)(0.035) ＞產生跨越國界或組織邊界的資訊流，肇生違法或違規的可能性(0.030) ＞導入物聯網系統於醫護作業上，使用者的接受度（認知易用性與認知有用性）(0.025) ＞營銷模式的創新具有投資誘因(0.021) ＞導入物聯網後個資隱私及及資安衝擊分析識別

(0.021)＞影響個資風險評估及管理機制(尚未建立或需重新界定) (0.015)＞實體及環境安全控管(0.014)＞非蓄意使用之法律責任影響使用者意願(0.012) ＞要求員工及承包商簽署資訊安全契約化協議書是否存在窒礙(0.008) ＞資產管理(0.007)。

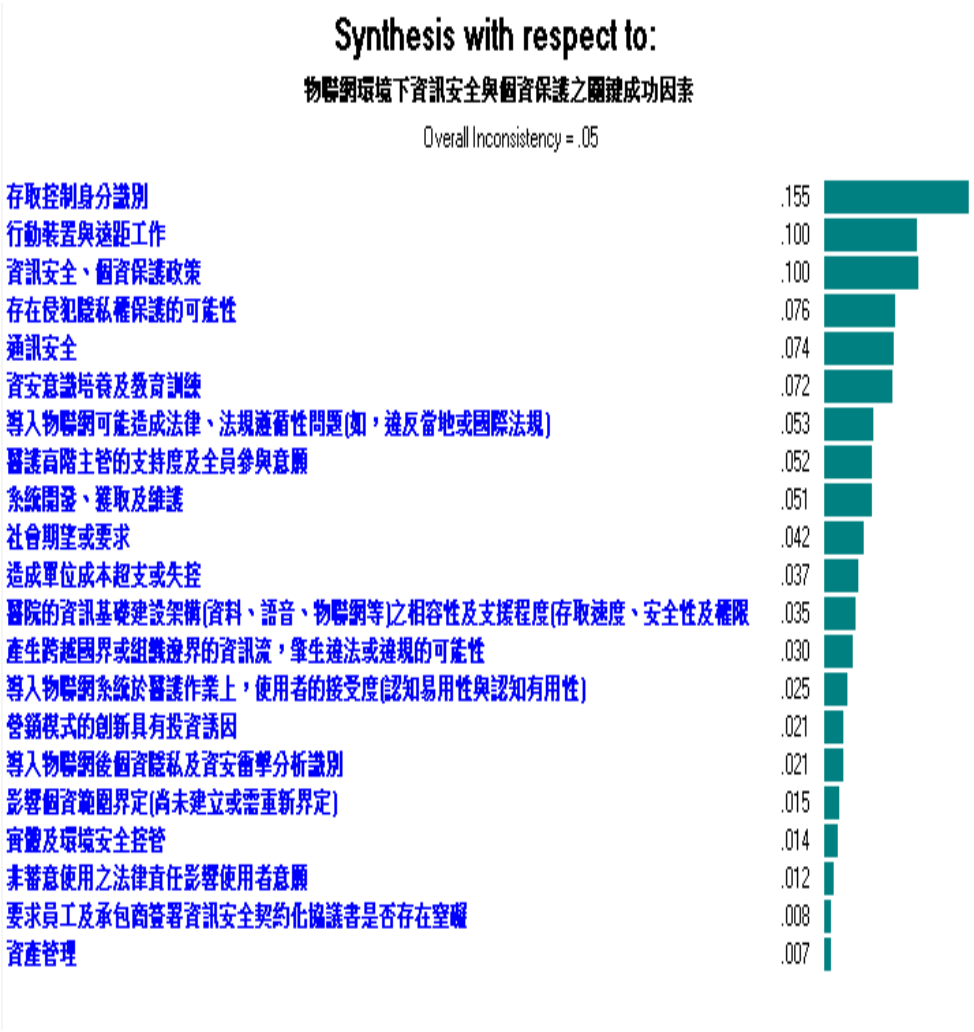


圖 7 評估指標之整體權重分配長條圖

如圖 7 所示，各評估指標之整體權重值，經過整體評估結果顯示，個案單位一致認為第一名為存取控制與身份識別(0.155)，第二名為行動裝置及遠距工作(0.100)，第三名為資訊安全、個資保護政策(0.100)，第四名為存在侵犯隱私權保護的可能性(0.076)，第五名為通訊安全(0.074)，第六名為資安意識培養及教育訓練(0.072)，第七名為導入物聯網可能造成法律、法規遵循性問題(如，違反當地或國際法規) (0.053)，第八名為醫護高階主管的支持度及全員參與意願(0.052)，第九名為系統開發、獲取及維護(0.051)，第十名為社會期望或要求(0.042)，第十一名為造成單位成本超支或失控(0.037)，第十二名為醫院的資訊基礎建設架構(資料、語音、物聯網等)之相容性及支援程度(存取速度、安全性及權限控管等) (0.035)，第十三名為產生跨越國界或組織邊界的資訊流，肇生違法或違規的可能性(0.030)，第十四名為導入物聯網系統於醫護作業上，使用者的接受度（認知易用性與認知有用性）(0.025)，第十五名為營銷模式的創新具有投資誘因(0.021)，第

十六名為導入物聯網後個資隱私及及資安衝擊分析識別(0.021)，第十七名為影響個資風險評估及管理機制(尚未建立或需重新界定) (0.015)，第十八名為實體及環境安全控管，第十九名為非蓄意使用之法律責任影響使用者意願(0.012)，第二十名為要求員工及承包商簽署資訊安全契約化協議書是否存在窒礙(0.008)，第二十一名為資產管理(0.007) 。

由以上整體綜合評估結果可以發現，在物聯網環境下資訊安全與個資保護之關鍵成功因素，其前七名為存取控制與身份識別(0.155)、行動裝置及遠距工作(0.100)、資訊安全、個資保護政策(0.100)、存在侵犯隱私權保護的可能性(0.076)、通訊安全(0.074) 、資安意識培養及教育訓練(0.072)、導入物聯網可能造成法律、法規遵循性問題(如，違反當地或國際法規)，最受個案單位人員重視，個別分析如下：

第一名為存取控制與身份識別(0.155)，顯示個案單位認為存取控制與身份識別(0.155) 最具影響力，當應用程式和服務存在雲端之上，身分驗證與存取的授權就顯得十分重要，因此透過識別與存取管理(Identity and Access Management ,IAM)，能夠去定義身分角色、責任和應用程式存取層級，以控管對關鍵資源的存取。

第二名為行動裝置及遠距工作(0.100)，系統應配置行動裝置管理 (Mobile Device Management, MDM)，範圍包括強制複雜性密碼、相機、網路設定、遠端清除裝置，或是強制裝置設定密碼等功能控管；與裝置行動應用程式管理(Mobile Application Management, MAM)，強制安裝或禁止使用特定應用程式，以及針對行動裝置的電子郵件，使用者的權限與隱私，可存取的各類文件內容控管來應對配置、安全存取、遠端控制和 DLP 技術方面的挑戰。

第三名為資訊安全、個資保護政策(0.100)，資訊安全與個資保護政策將影響未來資訊安全管理系統各項文件、程序與作法，如果不謹慎考量，將造 成嚴重的資安及個資洩漏風險，其中概括人力與財務損失，建議應參考相關資通訊安全標準法規條文，確保其具機密性、完整性、可用性、鑑別性與不可否認性之資訊安全、個資等機敏性資料於個案機構內皆受到高強度的控管及保護，遵循 PDCA 精神修訂政策適用範圍以符合法規之要求，使其免於遭受內、外部的蓄意或意外之威脅。

第四名為存在侵犯隱私權保護的可能性(0.076)，病歷在本質、功能及目的之探討可從「法律規定」及「臨床見解」兩方面來進行。在「法律規定」的部份，根據醫療法第 67 條及醫師法第 12 條的內容，可定義為「由醫師及其他醫事人員依法執行業務所製作之有關病人基本資料、治療記錄、各項檢查及檢驗報告資料」; 在「臨床見解」的層面，則具備了全民健康保險給付稽核、臨床醫學研究來源、法律證據提供與醫療管理營運之功能。而根據與病歷資訊隱私相關之法律規定，醫療機構及內部人員有義務對所保管之病歷善盡管理之責，並對病歷內容資訊予以保密，不得洩露。

近年隨著政府不斷提倡醫療資訊數位化，各醫療機構在加速病歷電子化的過程中也應該結合軟硬體技術與稽核管理制度的提升來實現隱私權維護的目標。透過「醫療機構電子病歷製作及管理辦法」中針對病歷系統的建置、維護、稽核及管制之規範制定標準作業程序，並就病歷存取、增刪、查閱及複製等使用權限設立管控機制，既可促進醫療品質的提升，亦可確保病人隱私權不致因醫療機構不當病歷管理而遭受侵犯。

第五名為通訊安全(0.074)，機構應識別所有網路之安全機制、服務等級及管理要求

事項，對於不同服務之系統設施應依照其重要性分級控管，如為 A 級(重要)以上之服務設施，應套用防火牆訪問政策、專屬維運終端訪問維運系統，且對於不同服務型態之網路應做區隔，如使用者網路及資訊系統的網路，應所屬不同網路分層，以避免造成網路攻擊及資料外洩之風險。

第六名為資安意識培養及教育訓練(0.072)，企業裡的員工是資安防護重要的一部份，因為他們可能會被駭客誤導，或造成導致惡意軟體感染與意外資料外洩的錯誤，公司定期教育使用者可協助提高其警覺性，培養更機警的資安意識。此外，增加各類型安全威脅的知識訓練，也可以讓員工即時防範及補救資安事件的傷害。

第七名為導入物聯網可能造成法律、法規遵循性問題(如，違反當地或國際法規)(0.053)，用戶在採用雲端服務之前，就必須要先了解供應商所提供的雲端服務是否能夠實現符合法規的要求，以及是否可能產生無法接受的風險。例如在新版個人資料保護法中，醫療資訊的蒐集是受到限制的，如果透過雲端服務去蒐集民眾的醫療相關資訊，並且作為資訊交換平台再提供給第三方合作業者的查詢利用，很可能就會有違法之虞，這時候雲端服務就不該是組織應考量的實務作法。

伍、結語

本研究主要是取得專家學者之共識而獲得有效之正式問卷，利用 Windows 作業環境下之 Expert Choice 2000 進行運算，衡量各評量估指標之相對權重值，推論出在物聯網環境下建立資訊安全與個資保護關鍵成功要素準則，經由本研究重要分析結果，做一綜合性整理，提出本研究的結論與建議，提醒醫療機構在導入物聯網系統環境時對於資訊安全及個資保護應重複檢視醫療機構的資訊安全現況是否符合資訊安全需求，並期望能將本研究結果能給予相關單位及決策者資源分配時作為參考。

5.1研究結論

依據本研究問卷調查與醫療機構資訊安全主管訪談結果，綜合本研究之目的，共可歸納出以下幾項結論：

一、本研究以德菲法之精神實施專家訪談取得資訊專業及資訊實務相關領域專家協助，篩選出影響物聯網環境下資訊安全與個資保護重要關鍵成功因素 21 項重要的評估指標，做為建立 AHP 層級架構之基礎；並依各重要因素屬性之不同於「在物聯網環境下資訊安全與個資保護之關鍵成功因素」目標下，分類為產業環境因素、組織因素、物聯網資訊系統的特性三個主要構面，分析出的關鍵權重進行驗證，經由評估構面與關鍵因素之權重計算、評估指標的排序和計算一致性，得知與問卷和實驗出來的數據相符合，一致性比率(CR)與整體階層一致性(CRH)均小於等於 0.1，在一致性檢定方面皆符合標準，顯示本研究 AHP 權重之一致性已可接受，證實本研究的關鍵成功要素確實可作為相關企業或單位在未來進行計畫時的參考，並對後續相關研究者提出個人之建議。

二、在物聯網環境下資訊安全與個資保護重要關鍵成功因素中，主要三大構面因素，最

重視「技術因素」，顯示個案單位認為物聯網環境下萬物聯網，對於醫療機構的基礎建設、加密存取機制、身分識別與權限控制等的相容性技術提升帶來許多的便利性，增加工作效率降低相關繁瑣的醫療彙整、分析作業，但也可能因不當的存取設定和錯誤的身分識別，帶來資安事件和造成個資外流等影響，不僅為醫療機構帶來負面形象也可能面對額鉅賠償，造成損失。

(一) 在「技術因素」構面中，個案單位最重視存取控制與身份識別，當應用程式和服務存在雲端之上，身分驗證與存取的授權就顯得十分重要，因此透過識別與存取管理(Identity and Access Management ,IAM)，能夠去定義身分角色、責任和應用程式存取層級，以控管對關鍵資源的存取行動裝置的普及。

(二) 在「組織因素」構面中，個案單位最重視資訊安全、個資保護政策，資訊安全與個資保護政策將影響未來資訊安全管理系統各項文件、程序與作法，如果不謹慎考量，將造 成嚴重的資安及個資洩漏風險，其中概括人力與財務損失，建議應參考相關資通訊安全標準法規條文，確保其具機密性、完整性、可用性、鑑別性與不可否認性之資訊安全、個資等機敏性資料於個案機構內皆受到高強度的控管及保護，遵循 PDCA 精神修訂政策適用範圍以符合法規之要求，使其免於遭受內、外部的蓄意或意外之威脅，經由風險評鑑決定接受風險的準則與可接受風險等級的準則，識別資產所面臨的各項威脅，並能評估各項脆弱性及其發生的可能性，且可藉由量化方式，估計可能造成的衝擊。組織自行可以根據其風險評鑑目標提供以符合由風險評鑑及適用之法規要求所決定之安全要求的資訊安全，使風險管控在可控制的範圍內。

(三) 在「環境因素」構面中，個案單位最重視存在侵犯隱私權保護的可能性，近年隨著政府不斷提倡醫療資訊數位化，各醫療機構在加速病歷電子化的過程中也應該結合軟硬體技術與稽核管理制度的提升來實現隱私權維護的目標。透過附錄三「醫療機構電子病歷製作及管理辦法」中針對病歷系統的建置、維護、稽核及管制之規範制定標準作業程序，並就病歷存取、增刪、查閱及複製等使用權限設立管控機制，既可促進醫療品質的提升，亦可確保病人隱私權不致因醫療機構不當病歷管理而遭受侵犯。

三、在物聯網環境下資訊安全與個資保護關鍵成功因素」目標下，整體評估結果分析可以發現，在物聯網環境下資訊安全與個資保護關鍵成功因素，其前七名分別為存取控制與身份識別、行動裝置及遠距工作、資訊安全、個資保護政策、存在侵犯隱私權保護的可能性、通訊安全、資安意識培養及教育訓練、導入物聯網可能造成法律、法規遵循性問題(如，違反當地或國際法規)。此七項關鍵成功因素之歸類，存取控制與身份識別、行動裝置及遠距工作、通訊安全等因素皆屬於「技術層面」構面下之因素，顯示技術層面構面為目前在物聯網環境下資訊安全與個資保護關鍵成功因素為個案單位最重視的因素。其中存取控制與身份識別(0.155)為第一名最具影響力，存取控制與身份識別，當應用程式和服務存在雲端之上，身分驗證與存取的授權就顯得十分重要，因此透過識別與存取管理(Identity and Access Management ,IAM)，能夠去定義身分角色、責任和應用程式存取層級，以控管對

關鍵資源的存取行動裝置的普及，可提供已導入物聯網之醫療機構之單位重新檢視資訊安全及個資保護之強度，或提供有興趣之企業或單位評估是否已達導入之條件，可作為後續相關企業或單位未來有意導入之導引。

5.2建議與未來研究方向

根據本研究之分析結果，針對相關計畫及未來單位提出數項建議，以期對實務和學術上有所貢獻，供後續研究者未來作為改善的參考。

一、本研究僅針對某醫療單位的樣本作分析，進行在物聯網環境下資訊安全與個資保護關鍵成功因素之分析，研究的結果恐過於狹隘而欠缺代表性，建議後續研究者可擴大地域範圍，針對更多的產業進行調查與研究，將更有助於不同類型的企業在導入時的參考。

二、針對在物聯網環境下資訊安全與個資保護關鍵成功因素，後續研究者未來可以增加深度訪談以補足研究變數的完整性，或者藉由專家訪談聚焦主要的研究變數。

三、本研究透過 AHP 法來尋找物聯網環境下資訊安全與個資保護關鍵成功因素，建議後續研究者利用其他不同的研究方法，如田野研究法、紮根理論法等，針對同類型調查分析其經營關鍵成功因素來做分析，期使研究成果更為周延。

陸、參考文獻

吳柏均，2015，物聯網環境之消費者使用行為意向探討—隱私及信任的角色，明新科技大學資訊管理學系碩士論文。

薛元鳳，2014，自攜式設備環境下資料外洩防護關鍵成功因素之研究，國防大學管理學院資訊管理學系碩士論文。

鄧振源、曾國雄，1989，層級分析法（AHP）的內涵特性與應用（上），中國統計學報，第二十七卷，第六期，5~22 頁。

鄧振源、曾國雄，1989，層級分析法（AHP）的內涵特性與應用（下），中國統計學報，第二十七卷，第六期，1~20 頁。

黃昭瑋，2013，從醫療資訊系統導入 探討對醫學中心行政流程效率與醫療品質再提升 - 以手術麻醉系統為例

王學弘，1994，以分析層級程序法進行彈性製造系統供應商之評選，中原大學工業工程研究所碩士論文。

謝俊雄、翁宇能，2009，應用 AHP 於資訊部門績效評估研究，國立中央大學資訊管理學系碩士論文。

陳福基、蕭世榮、陳啟元、杜素珍，2005，影響醫院接受行動護理站因素之研究－以南部某區域教學醫院為例。資訊管理學報，12 卷，S 期，67-89 頁。

陳瑩玲，2003，影響區域級以上(含)醫院護理站導入無線區域網路之重要因素探討。中正大學資訊管理研究所碩士論文。

黃興進，2002，資訊管理於醫療產業相關議題之探討。資訊管理學報，9 卷，101-116 頁。

張芳聆，2002，行動化臨床資訊系統－以應用於加護病房為例。國立陽明大學衛生資訊與管理決策研究所碩士論文。

張怡秋、劉忠峰、蕭世榮、陳瑩玲，2005，護理站導入無線區域網路之關鍵因素研究。資訊管理學報，12 卷，4 期，107-119 頁。

趙福義，2003，以資訊技術提升護理品質及改進對病人的照顧。成功大學工程科學系專班碩士論文。

顏大為，2004，以平板電腦與無線區域網路為基礎之行動醫囑系統雛形規劃與設計。中國醫藥大學醫務管理系研究所碩士論文。

黃昭偉，2013，從醫療資訊系統導入 探討對醫學中心行政流程效率與醫療品質再提升 - 以手術麻醉系統為例。

孟德芸，1998，企業成功關鍵因素之研究—以個人電腦產業為實證，國立中興大學企業管理研究所碩士論文。

陳煌勛，2005，網路隱私權保護之研究，台灣大學國家發展研究所碩士論文。

經濟部標準檢驗局，2006，中華民國國家標準 CNS 資訊技術-安全技術-資訊安全風險管理(CNS 27001)，台北：經濟部標準檢驗局。

經濟部標準檢驗局，2007，中華民國國家標準 CNS 資訊技術-安全技術-資訊安全風險管理(CNS 27002)，台北：經濟部標準檢驗局。

溫博煌，2003，台中舊市中心區再發展目標與策略之研究-分析階層程式法之應用，逢甲大學土地管理系碩士在職專班碩士論文。

Aaker, D. A., 1984, Strategic Market Management, New York: John Wiley & Sons Inc.

Boynton, Andrew C. and Robert W. Zmud, 1984, “An Assessment of Critical Bullen, V. L. and Rockart, J. F. , 1984, “A Primer on Critical Success Factors”, CISR Working paper, SSM/MIT, pp 69.

Cheng, C. H. & Mon, D.L. (1994). Evaluation weapon system by AHP based on fuzzy scales. Fuzzy Set and Systems, 63, 1-10.

Davis, F., 1979, “Yearning for yesterday: Sociology of nostalgia” , New York: Free Press.

Dalkey, N.C. (1969) “The Delphi Method: An Experimental Study of Groupopinion,”The Rand Corporation, Research Paper, RM-5888- PR , June.

Daniel,R.D., 1961, “Management Information Crisis”, Harvard BusinessReview , pp.111-121.

Fuerguson, C.R and Dickinson, R. . , 1982,"Critical Success Factor for Directors in the Eighties", Business Horizons, pp.14-18.

Flaherty D. H. "Protecting Privacy in Surveillance Societies," The University of Carolina press, Chapel Hill, NC. 1989

Huaiqing W., matthew K. O. Lee and Chen W., “Consmer Privacy Concerns about Marketing”, Communications of the ACM 41, 3 (March. 1998), pp63-70.

Leidecker, J. K. , & Bruno, A. V. , 1984, Identifying and Using Critical Success Factors. Long Range Planning, 17(1), pp. 23-32.Porter, M.E. , 1980, “Techniques for Analyzing Industries and Competitors”, Competitive Strategy, New York: Free Press.

heir Own DataNeeds”, Harvard Business Review, 1979, pp.81-93.

Rockart,John F. 1979, Chief Executive Define Their Own Data Needs, Harvard Business Review.

Saaty, T.L., 1980, The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation. Mc Graw-Hill, New York.

Saaty, T.L. and E.H. Forman, 1996, “The Hierarchon : A Dictionary of Hierarchies .,” AHP Series Vo. 5, RWS Publications, pp.496.

Satty, T.L, and Vargas, Luis G.., 1982,”The Logic of Priorities.”, Boston:Kluwer-Nijhoff. .

Singer, E., Mathiowetz, N., & Couper, M. (1993). The impact of privacy and confidentiality concerns on survey participation: The case of the 1990 United States Census. Public Opinion Quarterly, 57(4), 465-482

Westin, A. (1967). Privacy and Freedom, 7. New York : Atheneum.

以科技接受模式探討共同供應契約資訊系統使用之研究
－以空軍為例

劉興漢[1] 郭乃菁 林杰彬

國防大學管理學院資訊管理學系

摘要

本研究以空軍各單位「共同供應契約資訊系統」使用者為研究對象，以科技接受模式來探討持續使用此系統的可能影響因素。透過問卷設計和收集調查資料進行統計分析，以回收的 174 份有效問卷作此模式的統計分析。研究結果顯示，對行為意圖直接而顯著地影響者，以知覺易用性居高，知覺有用性則是緊接其後，其次是便利性；此外研究顯示電腦能力較佳的使用者，對於「共同供應契約資訊系統」的適應期短，熟練程度較高，而有系統容易操作的認知，也認同「共同供應契約資訊系統」對使用者在採購業務上有所幫助。同時，便利性也顯著正向影響使用態度，表示使用者認為使用「共同供應契約資訊系統」來完成採購任務可節省時間和精力的知覺程度，但卻不認為便利性會強化使用者在「共同供應契約資訊系統」容易操作並對採購業務上有所幫助的認知。

關鍵詞：共同供應契約資訊系統、科技接受模式、電腦自我效能、便利性

Applying TAM to Explore the Adoption of Information System for Common Supply Contracts by Users of Taiwan Air Force

Hsing H. Liu　Nai J. Guo　Chieh P. Lin

Department of Information Management, MCNDU, Taiwan, R.O.C.

Abstract

The study focuses on investigating the adoption and influencing factors from the Air Force procurement staff users of the CSCIS. To explore the possible influencing factors, we apply TAM to the modeling.The study had done statistical analysis through designed questionnaire and collection of survey data, which recover 174 valid questionnaires. The results of the study show that perceived ease of use is the most, perceived usefulness (PU) is the second and convenience is the third. In addition, users who have better computer skills showed a short adaptation period and a high degree of proficiency and easy to operate the CSCIS. Those also recognize that the CSCIS can help users in the procurement business.Meanwhile, convenience also significantly influenced users attitudes, indicating that users perceived the use of the CSCIS to accomplish procurement tasks that could save time and effort perception, but did not perceive that convenience could enhance operate the CSCIS easily for the users and has a useful understanding of the procurement business.

Keywords: Common Supply Contract Information System, Convenience, Science and Technology Acceptance Model, Computer Self - Efficacy

[1] Email:liu.hansh@gmail.com、通訊地址：台北市中央北路二段 70 號、電話：0933915864、投稿組別：國防資訊管理。

壹、前言

我國自民國87年5月27日公告施行「政府採購法」，是採購制度史上的重大變革，對各機關承辦採購業務人員及承攬政府採購業務廠商造成相當大的衝擊。在「政府採購法」施行前，係依據「機關營繕工程及購置定製變賣財物稽察條例」第十五條第一項前段規定：「營繕工程及購置、定製財物決標時，應以合於投標須知之規定，並在底價以內最低標價為得標原則」，而電腦設備購置或租用採購，則依據「中央政府各機關、學校、事業及研究機構辦理電腦設備購置或租用原則」第三項規定：「公開招請廠商提出建議書，對建議書內容之評審，須同時就其價格、硬體及軟體設備功能、技術服務及支援能力、以及廠商信譽等影響業務運作之因素，訂定評審標準及條件，進行評審，以選出合格廠商決標」，其餘採購案件均以價格競爭為決標方式唯一的考量。此種單以價格競爭為選商考量，只要合於招標規定，所有合格廠商一視同仁，全依價格高低來決定得標與否，而不考慮各個廠商所提供之工程、財物或勞務，在品質、性能及售後服務等方面效益上差異（徐孝利，2007）。

但在政府採購法施行後，機關採用的決標方式已具彈性，可依據不同採購需求，有不同的決標方式可供機關選擇，其施行主要目標有：「建立公開、透明、公平、競爭之政府採購作業制度，減少弊端」、「提昇採購效率，配合政府施政及經濟發展需要」、「創造良好之競爭環境，使廠商能公平參與」、「引入外國優良措施，改善現有制度之缺失，創新政府採購作業」及「落實分層負責、權責分明之採購行政」（公共工程委員會，1998）。在「政府採購法」研訂過程之中，興利及防弊均極為注重，對於現行有礙採購效率，且常遭一般廠商或機關詬病之措施，亟思予以改善。即便如此，採購案件仍難避免冗長的計畫申購與招標定約程序，遑論與廠商之間如存在疑義與異義時，所耗費的採購的期程。

試想每一個採購案件必須經過繁複的作業流程，自擬定計畫、商情訪查（詢價、估價）、核定採購、公告招標、等標、開標、決標，再到訂約、履約、驗收、付款結案，計算從計畫到訂約階段，每件採購案動輒數月不等，當中所需的人力更是難數，若辦理購案的人又非專業人員，產生的問題更是拖長了購案的程序，因此如何縮短採購時程、減少人力資源虛耗並提升採購效率成為重大課題。

所幸政府頒布共同供應契約的實施，利用集中與聯合採購的方式，將前半段冗長的計畫、招標、訂約流程委託專業機構代辦，完成後的契約公開於政府電子採購網的「共同供應契約資訊系統」，由適用機關自行選用，可使各機關免去通用型需求（如文具、紙張等）各自成立採購案件，形成人力及資源浪費，同時，省略了前段計畫、招標、訂約流程，亦大幅提升了機關之採購效率。

目前針對「共同供應契約資訊系統」之學術研究可分為以下幾個面向，包含政府機關導入電子化採購、共同供應契約採購制度、工程委託技術服務採共同供應契約、採購人員對共同供應契約電子採購系統滿意度調查、政府共同供應契約採購平台銷售額之影響因素探討等。從上述幾個研究面向可看出，大部分的研究僅針對採購制度及滿意度層面進行探討，鮮少針對國軍人員對「共同供應契約資訊系統」看法及使用情況進行研究。

為能有效瞭解國軍採購人員對使用「共同供應契約資訊系統」的想法與使用意圖，本研究以空軍採購人員為研究樣本，並以科技接受模式為模型，進而探討其在使用「共同供應契約資訊系統」之行為意圖與態度，其構面包含知覺有用性、知覺易用性、使用態度及行為意圖。根據前述研究動機，本研究將結合科技接受模式建構研究架構，探討影響空軍人員使用「共同供應契約資訊系統」的各項因素間因果關係，作為提供主管

機關後續改版修正參考。本研究方向如下：

1.分析影響空軍人員在使用共同供應契約資訊系統上的行為態度及使用意願因素。

2.結合科技接收模式來探討對此系統的接受情形及因果關係。

3.探討服務便利性對使用「共同供應契約資訊系統」之知覺有用性及知覺易用性的影響關係。

本研究將藉由文獻搜集探討及分析，並透過問卷調查方式彙整相關資訊，運用SPSS軟體來進行資料分析。研究範圍則以空軍使用「共同供應契約資訊系統」人員為研究對象，瞭解使用者行為態度、意願、採購效率與滿意度及窒礙。

貳、文獻探討

一、共同供應契約

「共同供應契約」一詞，係源自政府採購法第93條，規定各機關得就具有共通需求特性之財物或勞務，與廠商簽訂共同供應契約。所稱之共同供應契約，指一機關為二以上機關具有共通需求特性之財物或勞務與廠商簽訂契約，使該機關及其他適用機關均得利用該共同供應契約辦理採購。對於廠商而言，與訂約機關簽訂共同供應契約後，即有義務依約供應採購標的予該契約之所有適用機關（中央信託局共同供應契約簡介，2004）。

此制度在實施初期，原名為「中央機關財物集中採購實施方案」（行政院88年7月21日台（88）會授三字第06461號函），後行政院於92年核定「中央機關財物集中採購實施方案」修正為「中央機關共同供應契約集中採購實施要點」。係「為利中央政府各機關、學校、公營事業（以下簡稱中央機關）辦理財物、勞務集中採購，依政府採購法第九十三條與廠商簽訂共同供應契約，經由集中採購，以節省人力，發揮大量採購之經濟效益，提升採購執行績效」，可見其具有「集中採購」與「聯合採購」的特性，免除了購案前段繁複的計畫、招標過程，讓各機關能節省人力及減少採購程序，並購得價廉物美的產品（行政院公共工程委員會主管會談紀錄，2008），共同供應契約採購流程如圖1所示。

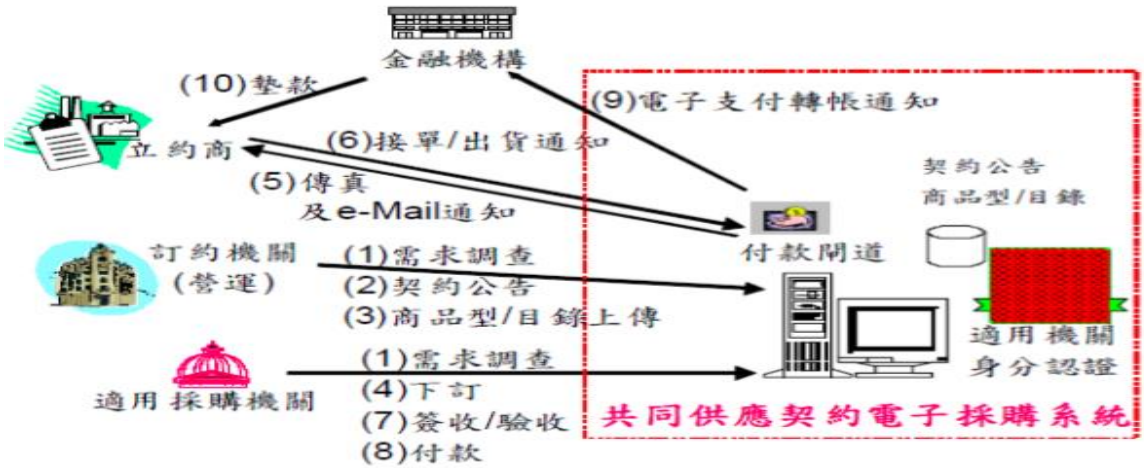


圖 14 共同供應契約採購流程（黃忠祥，2012）

然而要使共同供應契約更加普及至各適用機關，就必須有更好的採購系統來輔助，因此，政府在民國91年07月17日公布了「電子採購作業辦法」，同時設立了政府電子採購網，由行政院公共工程委員會主導，以電子化方式辦理採購，包含電子下訂與電子支付。行政院公共工程委員會亦依「中央機關共同供應契約集中採購實施要點」指定訂約

機關及採購項目表（如表4所示），初期主要機關為中央信託，後由台灣銀行接續。並依所訂契約公告於政府採購網「共同供應契約資訊系統」上，機關透過該系統於網路進行共通性採購需求調查，進行共同供應契約公告與查詢、訂購及付款，使採購流程全面電子化，節省採購成本，提昇採購效率。

表 4 行政院公共工程委員會指定訂約機關及採購項目

訂約機關	採購項目
內政部警政署	警用裝備之採購，包括員警制服、警用武器、彈藥、防彈裝備及警用車輛等
國防部	軍用武器、油料、物資及國防部所屬醫療機構之醫療衛材及藥品等
教育部	所屬醫療機構之醫療衛材及藥品等
行政院國軍退除役官兵輔導委員會	所屬醫療機構之醫療衛材及藥品等
行政院衛生署	一、全國預防接種及疾病防治所需各類疫苗 二、行政院衛生署所屬醫療機構之醫療衛材及藥品等
行政院環境保護署	環保設備
內政部消防署	消防車輛及消防器材
臺灣銀行股份有限公司	一、公務用機車及公務車輛租賃 二、各項事務設備，如辦公桌、辦公椅、傳真機、影印機、投影機、冷氣機（窗型及分離式）、電視機、電冰箱、飲水機、辦公室公文櫃、屏風及影印機租賃（含二手影印機）、省水器材等

依據工程會年報揭露101年度政府各適用機關運用共同供應契約之總採購金額已達新臺幣871億餘元，訂購筆數亦達141萬筆，工程會政府電子採購網之共同供應契約資訊系統自91年7月起，開始提供機關利用電子化方式進行訂購，又自92年起，提供人工傳真訂單補登功能。另據政府電子採購網資料，近年所有訂約機關辦理共同供應契約之每年訂購總金額已達700至千餘億元，顯見適用機關更加利用共同供應契約辦理共通需求特性之財物或勞務，而臺灣銀行每年接受其他機關委託代辦共同供應契約採購者之採購金額亦達300億元之多，若含工程會指定項目之總採購金額則約達500億元（每年訂購筆數可達60萬筆以上），突顯臺灣銀行辦理之共同供應契約採購案，已成為全國中央及地方機關極為仰賴使用之對象（監察院調查報告，2014）。

從表5中信局與臺灣銀行辦理共同供應契約採購案之情形可以發現，根據監察院2014年調查報告，利用共同供應契約採購不論是「決標案件」、「決標項次」、「契約件數」或是「機關訂購筆數」、「機關採購金額」，都呈現逐年增加之趨勢，顯見各機關確實逐年大幅提升了運用此系統辦理採購之比例，亦凸顯共同供應契約之重要性。

表 5 中信局與臺灣銀行辦理共同供應契約採購案之情形

項目 年度	決標 案件	決標 項次	契約 件數	機關 訂購筆數	機關採購金額 （千元）

88	9	43			47	2,561	152,803
89	11	161			121	16,884	3,208,855
90	22	590			361	54,435	10,432,954
91	26	812			1,154	94,466	14,135,992
92	38	2,394			4,081	164,157	21,904,139
93	41	2,825			5,286	260,137	26,304,030
94	31	2,870			5,727	353,114	29,322,397
95	66	2,963			6,364	451,255	35,149,327
96	75	5,163			8,259	553,478	37,637,331
97	92	6,338			7,960	550,765	46,131,516
98	75	5,270			9,706	694,674	52,771,851
99	82	6,120			11,951	655,943	45,387,025
工程會指定		100	1	6	28	226,394	6,267,817
		101	3	12	35	295,446	7,815,327
		102	1	8	28	233,350	6,600,565
接受委託代辦		100	103	8,132	12,566	322,844	35,297,500
		101	92	8,361	11,323	371,149	37,751,656
		102	61	2,423	5,506	233,423	26,945,969

二、理性行為理論（The Theory of Reasoned Action）

要探討科技接受模式，就必須先由理性行為理論（TRA）說起，其基礎係源自社會心理學，此一模型常被用於探討人類行為的意圖（Behavior Intention）（Fishbein and Ajzen,1975;1980），根據TRA理論，人類行為的表現取決於人的行為意圖（Behavior intention），而行為的意圖又受個人對此行為的態度（Attitude Toward Behavior）與主觀規範（Subjective Norm）所影響（Davis, 1989），因此，當個人對行為的態度愈正向，則行為意向愈高；反之，當個人對行為的態度愈負向，則行為意向愈低。

另一方面，主觀規範涉及社會習俗、他人意見或壓力等相關因素，相對的也就影響了行為意向。此外，直接經驗與態度同時存在時，也會直接影響態度與行為之間的張力。所以，個人的態度透過對事物或狀況所反應的行為，將會形成個人經驗。模型與各變數簡述如圖 15 所示。

三、科技接受模式（Technology Acceptance Model）

Davis（1989）以 TRA 為理論基礎，探討認知與情感因子與科技使用的關係，發展出科技接受模型（TAM）的模型，解釋個人對新資訊科技接納程度的決定因素，兩者相異之處在於科技接受模式不包含主觀規範，改以知覺有用性與知覺易用性做為影響使用者態度的關鍵因素，此模型希望能普遍地應用於解釋或預測資訊科技使用的影響因子。

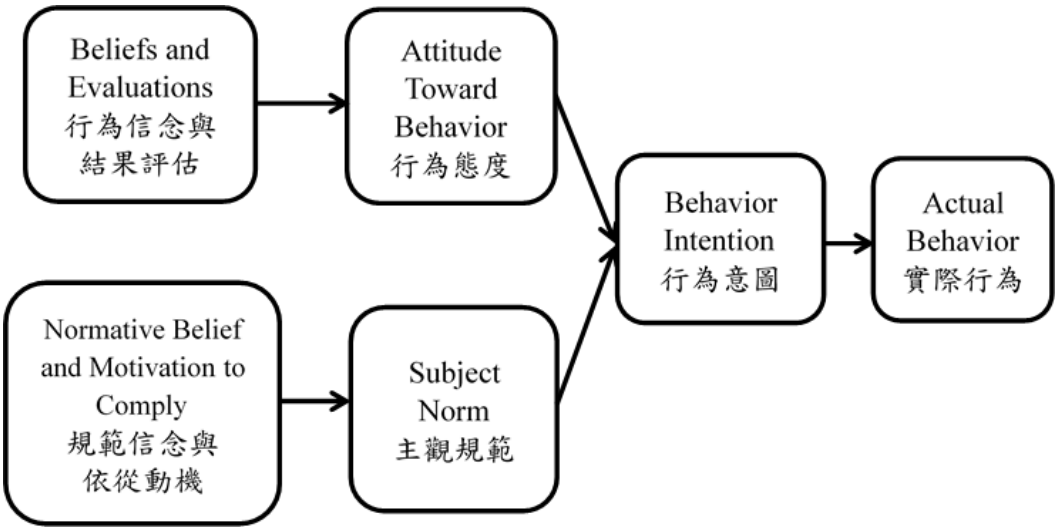


圖 15 理性行為理論模型

若只從使用認知層面探討人們對於科技的行為意圖，經會忽略其他重要外部因素的影響，因此Davis 認為應以科技接受模式為基礎，再延伸不同理論擴充外部變數，擴大探討其他影響科技接受程度的因素。TAM的模型與各變數簡述如圖16所示。

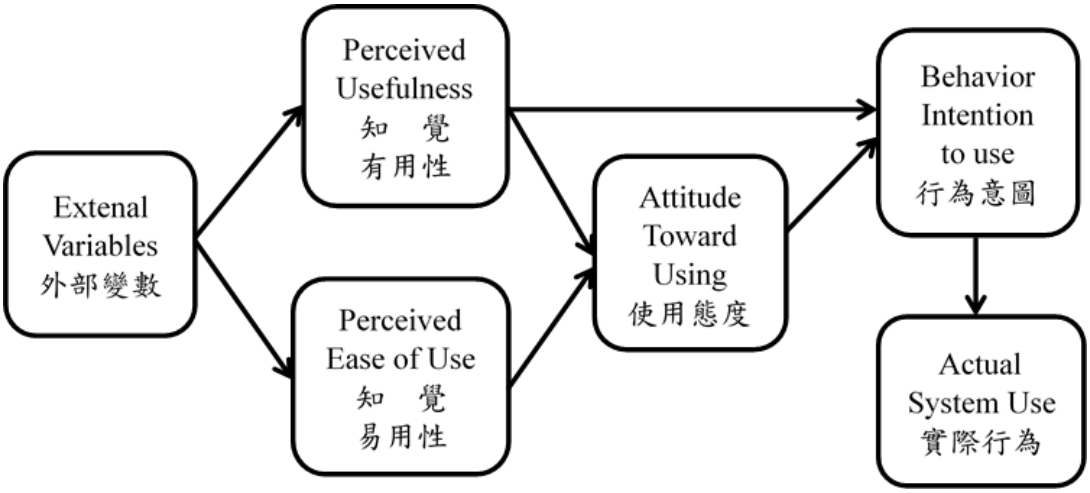


圖 16 TAM 模型架構圖

如何在最短期程內，以最精簡人、物力獲取最大效益，是近年組織機關努力達成的目標，期望藉由各種新科技的引進，達成組織人力精簡及行政效益最大化雙贏目標，關鍵就在於組織成員對新科技的接受度。科技接受模式即針對資訊系統的使用者接受度所提出的模型，藉由研究使用者對資訊科技的接受度，作出有效分析與結論，做為研究使用者接受資訊科技的重要理論基礎，本研究即是以此為主要的理論架構。

四、系統自我效能

Bandura（1977）提出自我效能理論（Self-Efficacy Theory）認為：自我效能是指一個人對於自己能夠成功達成任務或行為之能力有足夠的信心。之後Bandura（1991）進一步闡述「人對於自己本身效能的信念會影響他們所做的選擇、抱負（aspirations）、下多少心力在特定任務上及面對困難與挫折時能夠堅持多久。」 根據自我效能的定義，強調的是完成特定任務的能力（Ability）而非技能（skill）。Bandura（1984）以開車的自我效能為例來區別能力與技能的差別：控制方向盤、煞車、打方向燈等屬於開車的技能，能夠行駛在高速公路或是在崎嶇的山路上則是指開車的能力。

而電腦自我效能是指個人認為可以使用電腦來進行某項或完成一特定任務的能力，非指一項簡單的技能（如開、關機），此認知將會影響其對使用電腦結果的期望。根據Compeau and Higgins（1995）研究結果顯示，電腦自我效能為個人決定其使用資訊科技行為之重要影響因素。Venkatesh & Davis（1996）研究則顯示電腦自我效能對認知易用性有正向影響。而在美國一份對21,616位在職人員所做的調查報告更指出，自我效能與工作表現之間存在著正相關（康裕民，2001），所以，若能瞭解影響個人自我效能的因素，就可以影響其行為與態度，進而提高其工作表現。

五、便利性

在探討科技接受模式與服務便利性前，須先探討一下「共同供應契約資訊系統」性質，本研究目的中所探討「共同供應契約資訊系統」隸屬一種自助性的服務科技，所謂自助服務科技（Self-Service Technologies, SSTs）指是將科技導入服務當中，讓消費者可以自行完成服務的方式，所以新科技將會影響到消費者對於自助服務科技的使用態度。Meuter（2000）將自助服務科技（Self-Severice Technology, SST）定義為一種科技界面，消費者可以透過此介面自行完成某一特定工作或任務，而不需直接與服務人員接觸。

Meuter 亦將顧客滿意歸納出八項因素，有解決強烈需求、容易使用、避免服務人員打擾、節省時間、隨時、隨地、節省金錢與自助服務科技本身的品質等。Meuter（2003）指出消費者選擇以人互動之服務方式或者以科技為基礎的服務方式，端賴自助服務科技是否能為消費者帶來使用上的利益與舒適感。

從消費者角度而言，使用自助式服務科技最大的好處是時間及成本的節省，減少等待時間，更具效率、彈性及便於使用，使消費者認知的客製化（Customization）程度更高（Meuter & Bitner, 1998）。

Berry, Seiders and Grewal（2002）將便利性定義為：「消費者購買或使用服務時，對時間與精力支出的認知」。在過去便利性的分類研究中，Yale and VenKatseh（1986）將便利性分為時間效用等六大類。而Brown（1989）根據韋氏字典對便利性一詞之定義，提出便利性不應僅是節省時間而已，他認為產品或是服務提供者能夠加入愈多的便利性，就愈可以增加消費者對於其產品與服務之注意力並提高其購買與使用意願，故應將便利性視為具有多重構面之構念，分為時間等五大構面。Berry等學者（2002）認為消費者對於可節省時間（Time）和精力（Effort）的知覺，是為服務便利性，將便利性分為決策便利性等五種類型，綜整如表6所示。

通常一項具便利性的產品和服務會同時擁有多個便利性的屬性，消費者在購買服務時可以決定自己要花多少時間或心力來獲取這項產品或服務，如自動櫃員機，除提供時間便利性之外，也提供地點、獲取及使用構面多種屬性的便利性（Hornik, 1984）。

表 6 不同學者提出各項便利性構面分類彙整表

學者	便利性構面
Yale and VenKatseh（1986）	時間效用（Time Utilization）、容易獲得（Accessibility）、攜帶方便（Portability）、適用性（Appropriateness）、巧妙靈活（Handiness）、避免不悅（Avoidance of Unpleasantness）

Brown（1989）	時間構面（Time Dimension）：提供服務的時間對於消費者而言是便利的
	地點構面（Place Dimension）：提供服務的地點對於消費者而言是便利的
	獲取構面（Acquisition Dimension）：廠商提供財務或是其他管道以便利於消費者購買他們的服務，如刷卡或傳真訂購
	使用構面（Use Dimension）：服務能讓消費者使用起來感到便利
	執行構面（Execution Dimension）：可選擇由自己或他人執行、代勞的便利。
Berry等學者（2002）	決策便利性（Decision Convenience）：消費者在決定如何獲取想要的服務時，所耗費的時間與精力
	取得便利性（Access Convenience）：消費者開始與服務進行接觸時，所知覺到時間與精力的支出
	交易便利性（Transaction Convenience）：在進行交易時，消費者所知覺到時間與精力的支出
	利益便利性（Benefit Convenience）：消費者於體驗服務之核心利益時，所知覺到時間與精力的支出
	後續利益便利性（Postbenefit Convenience）：在享受服務之後，消費者再次與公司進行接觸時，所知覺到時間與精力的支出

六、科技接受模式與電腦自我效能

Davis根據Fishbein和Ajzen的「動機行為理論（Theory of Reasoned Action；TRA）」建構了「科技接受模式（Technology Acceptance Model；TAM）」，來解釋電腦使用的行為（Davis等學者，1989）。根據Davis等對科技接受模式的驗證，獲得下列幾個電腦使用上的觀點：

（1）我們可以透過使用者的意圖來預測他們使用電腦的行為。

（2）認知上的有用性是人們使用電腦的意圖的一個首要決定因素。

（3）認知上的易用性是人們使用電腦的意圖的一個次要決定因素。

過去的研究報告也指出，個人認知上的有用性和易用性確實對其在電腦的使用上有顯著的影響。因此，在評估使用者的使用績效之前，先對他們認知上的看法作一解析，或許能夠更清楚瞭解隱含在成功或失敗之下的意義。

七、科技接受模式與便利性

無論是理性行為理論（TRA）或科技接受模式（TAM）皆指出尚有其它變數會影響使用者使用某項科技的行為意圖，如使用者的個人特質，此外系統特性亦會透過信念或態度形成間接影響。這些可能影響潛在使用者採用某項資訊科技或系統的因素稱之為外部變數（External Variable）。

在新科技的使用上，有越來越多學者將便利性設定為外部變數與科技接受模式進行研究，如曹勛（2012）在影響消費者使用NFC行動付款服務之研究結果顯示，便利性與系統品質顯著影響消費者的認知有用性與認知易用性，並進而影響消費者使用NFC行動

付款的行為意圖；另外王俊嘉、陳美鐘、曾珈儒、周珉如（2013）在以科技接受模式探討智慧型手機與QR Code結合的購買行為意圖的研究顯示，認知便利性正向影響認知有用性、認知便利性正向影響使用態度。

參、研究方法

一、研究架構

本研究旨在探討影響空軍採購人員使用「共同供應契約資訊系統」的因素，包含空軍採購人員的電腦自我效能與服務便利程度，經過相關文獻探討歸納，本研究利用科技接受模式（知覺有用性、知覺易用性、使用態度、行為意圖）為基本模型，將電腦自我效能及便利性列入研究之外部變數，另將便利性列入本研究之調節變數，來衡量知覺有用性與知覺易用性對「共同供應契約資訊系統」使用意願之影響程度，本研究之架構如圖4，各變項的操作型定義與所使用的問卷題項之參考文獻整理如表4。

表7 本研究各變項的操作型定義

構面		變項操作型定義	文獻
科技接受模式	知覺有用性	使用者認為使用「共同供應契約系統」可以感受到工作效率增加的有效程度。	Davis（1989） Davis et al（1989）
	知覺易用性	使用者對使用「共同供應契約資訊系統」容易使用的程度。	Davis（1989）
	使用態度	使用者對使用「共同供應契約資訊系統」有正面的態度。	Davis（1989）
	行為意圖	個人將來願意繼續使用，或者願意推薦給其他人使用的意願。	Davis（1989）
電腦自我效能		個人對自己操作電腦和使用此系統（共同供應契約資訊系統）的能力判斷與信心。	Compeau and Higgins （1995）
便利性		服務的時間、地點對於消費者而言是便利的。 廠商提供財務或是其他管道以便利於消費者購買他們的服務，如刷卡訂購或傳真訂購。 服務能讓消費者使用起來感到便利。	Brown（1989）

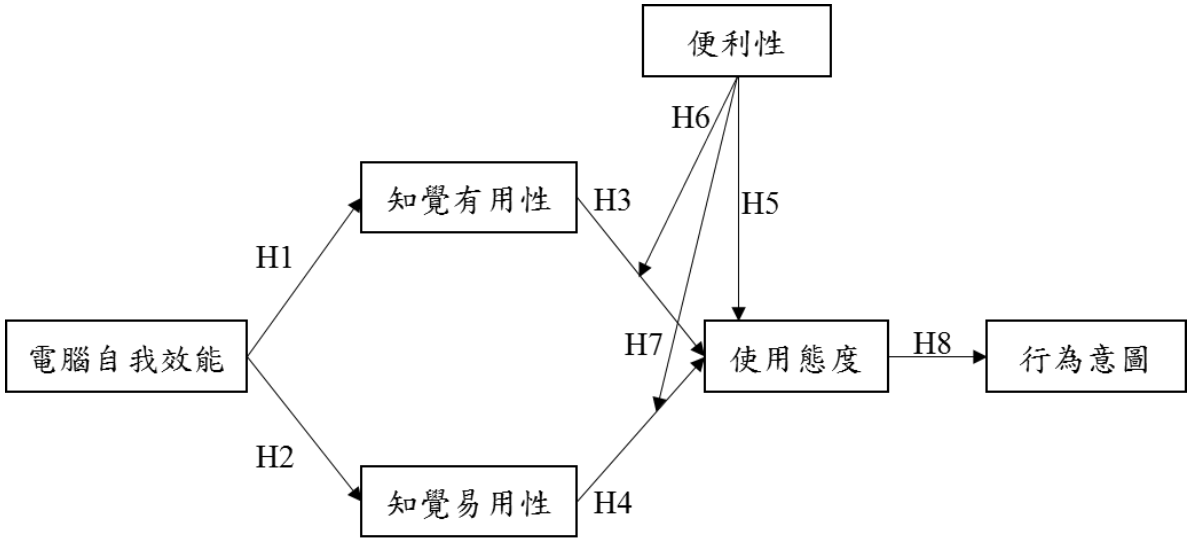


圖 17 研究架構圖

二、研究假設

本研究係依據科技接受模式來探討空軍人員對共同供應契約資訊系統的使用意願與行為態度，從文獻探討的結果，提出以下假說。

電腦自我效能指個人認為可以使用電腦來進行某項或完成一特定任務的能力，本研究則指使用者對本身使用「共同供應契約資訊系統」完成採購任務的能力。過去有許多電腦效能與科技接受模式的行為意願相關研究，其中周致中（2003）在網路報稅混合式資訊科技接受模式之研究中發現，電腦效能會部分顯著正向影響納稅義務人使用網路報稅的行為意願，另外徐浩宸（2007）在以科技接受模式探討基金網路交易系統使用意願之影響因素中發現，影響使用者在電腦自我效能方面對於基金網路系統的知覺有用性、知覺易用性呈現正向相關，對於基金網路系統的知覺有用性與易用性具有提升的效果。本研究仍依據Davis等學者（1989）的科技接受模式，推論電腦自我效能對知覺易用性與知覺有用性正向關係，因此本研究提出假設1及假設2：

H1：電腦自我效能對知覺有用性有正向影響
H2：電腦自我效能對知覺易用性有正向影響

「知覺有用」代表使用者經由使用某項資訊科技，來提升其本身工作績效。在本研究中，即是探討使用者經由「共同供應契約資訊系統」所提供之網路訂購、驗收、電子支付等服務，是否有效提升使用者工作上之績效；在Davis（1993）、Mathieson等（2001）、Shih（2004）、Vander Heijden（2003）及Bruner II and Kumar（2005）等學者的研究中發現，如使用資訊科技可以提升使用者較高的績效時，使用者對於資訊科技會有較正面的感受；因此，使用者對資訊科技的「知覺有用」與本身的「使用態度」會有正向的影響，因此本研究提出假設3：

H3：「知覺有用性」對「使用態度」有正向的影響

在Davis（1993），Mathieson， Peacock & Chin（2001），Shih（2004）等人的研究中可以發現，使用者花費較少心力所學得之資訊科技，會對資訊科技有較正面的感受，使用者對資訊科技的「知覺易用性」對於其本身的「使用態度」將會有正向的影響。如果「共同供應契約資訊系統」的使用者認為該系統在操作上是簡單易學，將對使用該系

統產生正面、接受的態度，因此本研究提出假設4：

H4：「知覺易用性」對「使用態度」呈現顯著正向影響

Brown（1989）認為產品或服務提供者若能夠加入愈多的便利性，就愈可增加消費者對於其產品與服務之注意力並提高其購買與使用意願。Eastin（2002）在其研究便提出「便利性」是可以衡量消費者是否使用網路銀行之重要因素；黃淑宜（2004）也在其研究指出，當使用者對於使用科技產品方面態度越正面，即會對此產品帶來之便利性有正向之影響。曹勛（2012）在影響消費者使用NFC行動付款服務之研究中亦得出NFC行動付款的便利性會影響消費者的認知易用性與認知有用性。此外，Szymanski & Hise（2000）指出便利性、網站設計及財務安全性是影響消費者對於電子服務之滿意度的重要因素，其中以便利性影響最大，Berry，Seider & Grewal（2002）指出消費者對於使用網路系統來完成其工作任務所花費之時間、精力越少時，其知覺到便利性就越高，而Berry等學者（2002）則定義為消費者對於可節省時間和精力的知覺程度，本研究綜合以上文獻，推論使用「共同供應契約資訊系統」的便利性對知覺易用性與知覺有用性具及使用態度具有正向關係，因此本研究提出假設5、假設6及假設7：

H5：「便利性」對「使用態度」呈現顯著正向影響
H6：「便利性」會強化「知覺有用性」與使用態度間之正向影響
H7：「便利性」會強化「知覺易用性」與使用態度間之正向影響

根據科技接收模式理論，認知有用性與認知易用性會影響使用者的使用態度，進而影響使用者的使用行為意圖與實際使用行為，在Hu等學者（1999），Moon & Kim（2001），Van der Heijden（2003），Bruner II & Kumar（2005）等研究中發現，使用者若對資訊科技有較正面的感受，其使用資訊科技的可能性也會較高，使用者對資訊科技的「使用態度」對於本身的「行為意願」會有正向的影響，因此本研究假設若使用者對於「共同供應契約資訊系統」具有正面的態度，那麼其使用該系統的可能性也會較高，因此本研究提出假設8：

H8：「使用態度」對「行為意圖」呈現顯著正向影響

三、問卷設計與分析方法

本研究針對「共同供應契約資訊系統」的使用者對該系統的電腦自我效能、便利性、知覺有用性、知覺易用性、使用態度及行為意圖等面向設計問卷，採用李克特（Likert, R, 1932）五點尺度衡量表（Likert Scale），依認同程度給予不同的評分，分別為「非常同意」、「同意」、「普通」、「不同意」、「非常不同意」，量表分別以5至1的分數來代表。問卷分為「電腦自我效能」、「知覺有用性」、「知覺易用性」、「便利性」、「使用態度」及「使用意圖」等六構面。

本研究係針對樣本進行描述性分析，包含性別、年齡、學歷、階級、年資與編制專長等。其次，再以Cronbach’s信賴係數法（Cronbach's alpha）（L.J. Cronbach, 1951）進行信度分析。而在效度分析部分，由於本研究所使用的問卷均參考相關文獻，故具有一定的內容效度。最後，本研究以相關分析來驗證研究架構。透過問卷收集相關數據，並運用下列5種方式對SPSS統計軟體結果分析。

1. 樣本結構敘述性統計分析（Descriptive Statistics Analysis）

敘述統計係用於說明樣本資料結構，將其問卷資料進行單一變數敘述統計，求取各變數之平均數、中位數、標準差等資料，並將基本個人變項：性別、年齡、學歷、階級、年資與編制專長等，彙整描述其資料類別特性與比例分配情形，俾瞭解空軍現行或實際

執行過「共同供應契約資訊系統」人員，之基本變項與量表之次數分配情形。

2. 信、效度分析（Reliability Analysis）

信度（Reliability）是指測量的可靠程度（Trustworthiness），亦可檢測量表中各項目的內部一致性（Internal Consistency）或內部同質性（Internal Homogeneity）。本研究採用 Cronbach's Alpha 係數作為量表信度分析之分析方法。本研究之研究變項的衡量，有關電腦自我效能、便利性、知覺有用性、知覺易用性、使用態度及行為意圖等量表，係參考國內、外學者發展的問卷修改，因研究對象不同，故再進行量表信度測試，以 Cronbach's Alpha 值來衡量量表的內部一致性。所謂 Cronbach's Alpha 係數是目前行為及社會科學研究最常使用之信度指標。其建立在抽象的理論上，在一些合理的假定之下，根據觀察值就可以計算 Cronbach's Alpha 。效度（Validity）是指測量的正確性，亦即能夠真正測得變數性質之程度。本研究係藉由因素分析與內部一致性檢定來輔助建構效度（Construct Validity）分析。

3. 因素分析（Factor Analysis）

將本研究所探討的外顯變數，按各構面萃取成少數幾個具有意義的內隱因素。因素分析理論方法說明如下：

因素分析主要目的在希望能降低變數的數目，當我們欲在一群具有相關性且不易解釋的資料中，找出部分概念上有意義而且彼此之間接近獨立的，並足以影響原始資料共同因素。也就是說，將觀測資料之精簡描述，並試圖從一組可觀測變數之共變異數矩陣中尋找較少數的新變數，使儘可能再製原共變異數矩陣，亦即尋找且定義基本構面（dimensions），其被視為構成這些原來變數之基礎。

4. 相關性分析（Analysis of Correlation）

本研究以 Pearson 相關分析性受訪者基本資料變數包括性別、年齡、教育程度、軍事教育程度、階級、工作年資、役別、編制專長等與依變數「使用態度」間之相關程度及其顯著水準，並將這些受訪者基本資料變數與依變數關係較為顯著，納入階層迴歸分析。

5. 迴歸分析（Multi-regression Analysis）

本研究以迴歸分析驗證電腦自我效能、知覺有用性、知覺易用性、使用態度、行為意圖等變數間有何影響；同時藉由多元迴歸方式中之階層迴歸，採取強迫進入（Enter）方式，分析自變項（知覺有用性、知覺易用性）及干擾變項（便利性）之交互作用，對依變項（使用態度）干擾效果的影響。

肆、資料分析與結果

本研究進行前測以驗證信、效度，於正式問卷回收後，剔除無效問卷，將有效問卷編碼，並以SPSS 19.0統計分析軟體，驗證研究模型(圖17)H1至H8的假設是否成立，藉此說明空軍採購人員（非單指採購編制專長人員，泛指空軍各單位實際從事請購業務，包含：人事、行政、作戰等各專長人員）使用共同共應契約系統的行為態度、意願、滿意度，期望藉由本研究所呈現的使用現況，提供主管機關參考。本章共分為6小節，分別針對前測、正式問卷、樣本資料分析、因素與信效度分析、實證分析、結果分析等逐一說明。

一、前測

在進行正式問卷調查前，為使受測者明確瞭解問卷題項意涵，並使問項可以適當衡量出研究中的變數，多數研究者在預試量表完成後，進行試探性的信度分析，以做為題目改善的依據（邱皓政，2003）。據此，本研究於105年6月20至24日針對空軍司令部曾

經使用過「共同供應契約資訊系統」人員實施前測，計發放問卷45份，扣除無效問卷4份，有效問卷為41份，有效問卷回收率為91.11%。邱皓政（2008）指出，問卷回收後可透過信度分析來檢驗問卷的一致性，有兩個數值可以當做指標：第一是依據修正的項目總相關係數來衡量，在係數值小於0.3時則可以考慮刪除；第二則是以Cronbach’s α係數值來測量所自然形成的題項，是否有足夠的一致性，採用的標準是Cronbach （1951）和Nunnally（1978）所建議的0.7。本問卷前測經過SPSS19.0軟體分析後，各 構 面 的 Cronbach’s α信度係數分別為：電腦自我效能0.776、知覺有用性0.728、知覺易用性0.199、便利性0.639、使用態度0.763、及行為意圖0.821，綜整如表8。

表 8 前測問卷各構面及變項之信度分析

構面	題號	crobanch's Alpha 值	修正的項目總相關	題項刪除時的 crobanch's Alpha 值	備註
電腦自我效能	1-1	0.776	0.596	0.725	
	1-2		0.613	0.700	
	1-3		0.535	0.732	
	1-4		0.589	0.703	
知覺有用性	2-1	0.728	0.608	0.590	
	2-2		0.384	0.745	
	2-3		0.585	0.634	
	2-4		0.516	0.662	
知覺易用性	3-1	0.199	0.307	-0.113	刪除
	3-2		0.244	-0.004	刪除
	3-3		0.343	0.569	刪除
	3-4		0.272	-0.030	刪除
	3-5		0.146	0.112	刪除
便利性	4-1	0.639	0.539	0.507	
	4-2		0.399	0.627	
	4-3		0.179	0.720	刪除
	4-4		0.552	0.515	
	4-5		0.510	0.542	
使用態度	5-1	0.763	0.656	0.662	
	5-2		0.510	0.739	
	5-3		0.666	0.645	
使用意圖	6-1	0.821	0.643	0.775	
	6-2		0.671	0.763	
	6-3		0.619	0.786	
	6-4		0.643	0.775	

由表 8 可以看出，構面三知覺易用性及構面四便利性之 crobanch's α 值未達 Cronbach（1951）和 Nunnally（1978）所建議的 0.7，構面三知覺易用性考量信度過低（0.199）且位於各項修正的項目總相關與建議刪除值 0.3 左右，故將本構面題項全數刪除，另行參考相關研究問卷題目修正後再執行乙次前測；另構面四題項三之各項修正的項目總相關值為 0.179，低於建議刪除值 0.3，故本題予以刪除，刪除後構面四信

度提升至 0.720，修正的項目總相關分別為 0.607、0462、0.488 及 0.485，均高於建議刪除值 0.3。經參考科技接受模式（TAM）相關學術研究之問卷修改構面三題目，並進行第二次前測結果，構面三 Cronbach’s α 信度係數提升至 0.766，符合建議值 0.7，修正的項目總相關分別為 0.707、0.506、0.492 及 0.572，表示本問卷量表信度良好。

二、正式問卷

本研究於 2016 年 8 月 1 日至 2016 年 8 月 15 日期間，針對空軍所屬計 17 單位之「共同供應契約資訊系統」使用者進行問卷調查以收集資料，共發出問卷 200 份，實際回收 185 份，回收率 92.5%，剔除無效問卷 11 份，有效問卷為 174 份，有效問卷回收率為 94.05%。

問卷經整理編碼後，利用 SPSS 19.0 統計分析軟體，根據研究假設之檢定結果依據本研究所列之資料分析方法進行分析，包含樣本結構敘述性統計分析、信度分析、效度分析、因素分析、相關性分析與迴歸分析等，驗證圖 17 的 H1 至 H8 的假設是否成立，藉此說明空軍採購人員使用共同共應契約系統的行為態度、意願、滿意度。

本研究之使用者基本資料依性別、年齡、教育程度、軍事教育程度、階級、工作年資、役別、編制專長，綜整如表9至表12，分別敘述如下。

由表9可知，受訪者男性佔69%，女性佔31%，年齡則以31~35歲比例最高，佔40.2%，其次依序為26~30歲（25.9%）、36~40歲（16.7%）、20~25歲（9.2%，16人、41~45歲（5.2%）、51歲以上（1.7%）、46~50歲（1.1%）。

由表10可知，受訪者教育程度以大學（專）比例最高，佔76.4.1%，其次依序為高中（職）(12.6%)、碩士（10.3%）、博士（0.6%），顯示操作此系統人員教育程度呈現相當高水準，大多數為大專院校以上學歷；在軍事教育上，以受過士高班訓練之士官比例最高，佔32.8%，其次依序為士長班（25.3%）、未受過軍事教育人員與受過軍官深造教育班相同（17.2%）、正規班（6.9%）、戰爭學院（0.6%），顯示80%以上受訪者均已接受過基礎軍事教育。

表 9 基本資料-性別與年齡分析結果

基本資料變項	變項	人數	百分比（%）	累積百分比（%）
性別	男	120	69	69
	女	54	31	100
年齡	20-25 歲	16	9.2	9.2
	26-30 歲	45	25.9	35.1
	31-35 歲	70	40.2	75.3
	36-40 歲	29	16.7	92
	41-45 歲	9	5.2	97.1
	46-50 歲	2	1.1	98.3
	51 歲以上	3	1.7	100

表 10 基本資料-教育與軍事教育分析結果

基本資料變項	變項	人數	百分比（%）	累積百分比（%）
教育程度	高中(職)	22	12.6	12.6
	大學(專)	133	76.4	89.1
	碩士	18	10.3	99.4
	博士	1	0.6	100

軍事教育	未受訓	30	17.2	17.2
	士高班	57	32.8	50
	士長班	44	25.3	75.3
	正規班	30	17.2	92.5
	指參班	12	6.9	99.4
	戰略班	1	0.6	100

由表11可知，受訪者以上士比例最高，佔24.7%，其次依序為士官長（21.8%）、上尉（17.2%）、少校（13.2%、中士（7.5%）、中尉（5.7%）、中校（4.0%）、聘僱人員（2.9%）、下士（1.7%）、少尉與上校相同（0.6%），顯示操作此系統人員以低階軍士官為主。此外，幕僚佔96%，主官4%，顯示受訪人員以幕僚為主；志願役佔97.1%，聘僱人員2.9%，顯示此系統操作人員以軍職為主。

表 11 基本資料-階級、職稱與役別分析結果

基本資料變項	變項	人數	百分比（%）	累積百分比（%）
階級	下士	3	1.7	1.7
	中士	13	7.5	9.2
	上士	43	24.7	33.9
	士官長	38	21.8	55.7
	少尉	1	0.6	56.3
	中尉	10	5.7	62.1
	上尉	30	17.2	79.3
	少校	23	13.2	92.5
	中校	7	4	96.6
	上校	1	0.6	97.1
	聘僱人員	5	2.9	100
職稱	主官	7	4.0	4.0
	幕僚	167	96.0	100
役別	志願役	169	97.1	97.1
	義務役	0	0	97.1
	聘僱人員	5	2.9	100

表 12 基本資料-工作年資與編制專長分析結果

基本資料變項	變項	人數	百分比（%）	累積百分比（%）
工作年資	0-5 年	28	16.1	16.1
	6-10 年	56	32.2	48.3

	11-15 年	43	24.7	73
	16-20 年	39	22.4	95.4
	21 年以上	8	4.6	100
編制專長	採購	52	29.9	29.9
	通資	18	10.3	40.2
	兩者皆非	104	59.8	100

由表12可知，受訪者以年資6~10年最高，佔32.2%，其次依序為11~15年（24.7%）、16~20年（22.4%）、0~5年（16.1%）、21年以上（4.6%），顯示此系統操作人員大多已有相當部隊工作經驗，了解並熟悉業務流程。

在編制專長部分，依研究性質分為「採購」、「通資」與「兩者皆非」，以兩者皆非比例最高佔59.8%、採購29.9%、通資10.3%，顯示多數操作系統人員非採購專業人員或具電腦相關專長。

三、因素分析及信、效度分析

1.因素分析

本研究之問卷係經空軍營級（含以上）單位人員現行或實際執行過「共同供應契約資訊系統」針對問卷問項內容，依照實際感受程度填答，據以完成資料蒐集。首先針對各變項量表進行因素分析，驗證其各因素構面與內容是否合乎各變數之定義與內容。

對於判別量表變項是否進行因素分析，首先觀察其 KMO（Kaiser-Meyer-Olkin measure of sampling adequacy）取樣適當性檢定及與球型檢定（Bartlett test of sphericity）；根據 Kaiser（1974）觀點，因素分析的適切性良好 KMO 檢定值最好在 0.8 以上，一般而言大於 0.7 以上即可實施因素分析，如果 KMO 的值小於 0.5 時，則較不適宜進行因素分析，而 KMO 值越大，因素分析的效果亦越好；此外，Bartlett 球型檢定其 P 值為＜0.001 達顯著，表示母群體的相關矩陣間有共同因素存在，適合進行因素分析。

本研究在因素分析方面採主軸法之主成份分析（principal component analysis）模式，萃取因素設定為 1 個因素；吳明隆（2008）於「多變量分析實務」一書指出在社會科學領域中，萃取因素對所有指標變數的累積變異最低的接受標準最好在 50%以上，因素負荷量大小的取捨方面，最低的接受標準應在.30 以上，較佳的數值為.40 以上。

依據前述標準，本研究針對各變項進行因素分析結果，構面 1-6 KMO 值分別為 0.684、0.819、0.788、0.723、0.691 及 0.832，Bartlett 球型檢定其 P 值均為 0.000＜0.001 達顯著，代表本問卷各題項間具有共同因素存在，適合進行因素分析；各項數值統計如表 13。

2.信度分析

信度是指對同一或相似母體重複進行調查或測驗，所得結果相互一致之程度，Cronbach's α 統計係數是最常被用來衡量內在一致性的檢定方法。本研究即採用此法，就各變數的 Cronbach's α 值而言，變數的信度皆在 0.70 以上，知覺有用性、知覺易用性、使用態度、使用意圖 Cronbach's α 值更在 0.80 以上，分別為分別為 0.853、0.859、0.841、0.897，因而本研究問卷題目信度甚佳。

3.效度分析

在效度分析方面，本研究係藉由因素分析與內部一致性檢定來輔助建構效度（Construct Validity）分析，主要針對「電腦自我效能」、「知覺有用性」、「知覺易用性」、「便利性」、「使用態度」與「使用意圖」量表進行因素分析，驗證其各因素構面與內容是否合乎各變數之定義與內容。透過因素分析可瞭解測量變項之因素負荷量（factor loading）

皆大於0.4以上，並為各因素命名之依據，各量表經縮減後因素之總累積解釋變異量達50%以上，因素量表各構面效度衡量尚可接受。問卷信、效度分析結果整理如表13。

表 13 共同性及信、效度統計

構面	題號	crobanch's α 值	KMO 值	球型檢定 Bartlett test of sphericity	因素負荷量	解說變異量累積%
電腦自我效能	1-1	0.714	0.684	.000	.646	55.847
	1-2				.836	
	1-3				.756	
	1-4				.739	
知覺有用性	2-1	0.853	0.819	.000	.840	69.667
	2-2				.795	
	2-3				.853	
	2-4				.850	
知覺易用性	3-1	0.859	0.788	.000	.811	70.381
	3-2				.803	
	3-3				.873	
	3-4				.866	
便利性	4-1	0.756	0.723	.000	.657	58.047
	4-2				.767	
	4-3				.787	
	4-4				.826	
使用態度	5-1	0.841	0.691	.000	.911	76.021
	5-2				.885	
	5-3				817	
使用意圖	6-1	0.897	0.832	.000	.881	76.491
	6-2				.876	
	6-3				.873	
	6-4				868	

四、實證分析

本研究以空軍營級（含以上）實際執行過「共同供應契約資訊系統」人員為實證研究對象，將獲得資料進行統計分析，在分析方法上主要以簡單及階層迴歸法探討各變數之間主要影響及干擾作用影響。

(一)簡單迴歸分析

本小節主要分析探討並解釋在一對一的變數間相關的關係，依據本研究所建立的假說，均為單一X變數對Y變數之影響，故以簡單迴歸分析探討解釋兩者間是否具有正向影響，各假說分析如下。

H1：「電腦自我效能」對「知覺有用性」有正向影響之統計分析

表14為「電腦自我效能」對「知覺有用性」迴歸係數統計量，電腦自我效能的標準化迴歸係數值（Beta值）為.392，迴歸係數顯著性考驗的t值為5.590（p=.000<.05），顯示電腦自我效能對知覺有用性有正向顯著關係，表示受訪者在電腦自我效能上對知覺有用性有正向顯著的效果，因此本研究H1成立。

表 14 「電腦自我效能」對「知覺有用性」迴歸係數

模式	未標準化係數		標準化係數	t	顯著性
	B 之估計值	標準誤差	Beta 分配		
1 (常數)	2.205	.288		7.661	.000
自我效能@	.435	.078	.392	5.590	.000

a.依變數：知覺有用性

H2：「電腦自我效能」對「知覺易用性」有正向影響之統計分析

表15為「電腦自我效能」對「知覺易用性」迴歸係數統計量，電腦自我效能的標準化迴歸係數值（Beta值）為.491，迴歸係數顯著性考驗的t值為7.382（p=.000<.05），顯示電腦自我效能對知覺易用性有正向顯著關係，表示受訪者在電腦自我效能上對知覺易用性有正向顯著的效果，因此本研究H2成立。

表 15 「電腦自我效能」對「知覺易用性」迴歸係數

模式	未標準化係數		標準化係數	t	顯著性
	B 之估計值	標準誤差	Beta 分配		
1 (常數)	1.871	.259		7.236	.000
自我效能@	.516	.070	.491	7.382	.000

a.依變數：易用性

H3：「知覺有用性」對「使用態度」有正向的影響之統計分析

表16為「知覺有用性」對「使用態度」迴歸係數統計量，知覺有用性的標準化迴歸係數值（Beta值）為.616，迴歸係數顯著性考驗的t值為10.243（p=.000<.05），顯示知覺有用性對使用態度有正向顯著關係，表示受訪者在知覺有用性上對使用態度有正向顯著的效果，因此本研究H3成立。

表 16 「知覺有用性」對「使用態度」迴歸係數

模式	未標準化係數		標準化係數	t	顯著性
	B 之估計值	標準誤差	Beta 分配		
1 (常數)	1.366	.235		5.806	.000
有用性	.626	.061	.616	10.243	.000

a.依變數：使用態度

H4：「知覺易用性」對「使用態度」呈現顯著正向影響之統計分析

表17為「知覺易用性」對「使用態度」迴歸係數統計量，知覺易用性的標準化迴歸係數值（Beta值）為.725，迴歸係數顯著性考驗的t值為13.794（p=.000<.05），顯示知覺易用性對使用態度有正向顯著關係，表示受訪者在知覺易用性上對使用態度有正向顯著的效果，因此本研究H4成立。

表 17 「知覺易用性」對「使用態度」迴歸係數

模式	未標準化係數		標準化係數	t	顯著性
	B 之估計值	標準誤差	Beta 分配		
1 (常數)	.822	.214		3.834	.000
知覺易用性	.777	.056	.725	13.794	.000
a.依變數：使用態度					

H5：「便利性」對「使用態度」呈現顯著正向影響之統計分析

表18為「便利性」對「使用態度」迴歸係數統計量，便利性的標準化迴歸係數值Beta值）為.602，迴歸係數顯著性考驗的t值為9.875（p=.000<.05），顯示便利性對使用態度有正向顯著關係，表示受訪者在便利性上對使用態度有正向顯著的效果，因此本研究H5成立。

表 18 「便利性」對「使用態度」迴歸係數

模式	未標準化係數		標準化係數	t	顯著性
	B 之估計值	標準誤差	Beta 分配		
1 (常數)	1.036	.277		3.745	.000
便利性	.714	.072	.602	9.875	.000
a.依變數：使用態度					

H8：「使用態度」對「行為意圖」呈現顯著正向影響之統計分析

表19為「使用態度」對「行為意圖」迴歸係數統計量，便利性的標準化迴歸係數值（Beta值）為.594，迴歸係數顯著性考驗的t值為9.680（p=.000<.05），顯示使用態度對行為意圖有正向顯著關係，表示受訪者在使用態度上對行為意圖有正向顯著的效果，因此本研究H8成立。

表 19 「使用態度」對「行為意圖」迴歸係數

模式		未標準化係數		標準化係數	t	顯著性
		B 之估計值	標準誤差	Beta 分配		
1	(常數)	1.562	.239		6.523	.000
	使用態度	.610	.063	.594	9.680	.000
a.依變數：行為意圖						

綜上驗證結果可以得知，在本研究模型中，假說1-5及8均為成立，亦即：「電腦自

我效能」對「知覺有用性」有正向影響、「電腦自我效能」對「知覺有用性」有正向影響、「知覺有用性」與「使用態度」有正向的影響、「知覺易用性」與「使用態度」呈現顯著正向影響、「便利性」與「使用態度」呈現顯著正向影響及「使用態度」與「行為意圖」呈現顯著正向影響。

(二)階層迴歸分析

本研究針對「便利性」干擾效果的檢驗，採用Baron和Kenny(1986)的做法，透過階層迴歸分析，逐次加入控制變數(編制專長)，自變數(知覺有用性、知覺易用性)，干擾變數(便利性)及交互作用項(知覺有用性*便利性，知覺易用性*便利性)，其主要目的在驗證「便利性」是否會強化使用「知覺有用性」與「使用態度間」之正向影響及「便利性」是否會強化使用「知覺易用性」與「使用態度間」之正向影響。

H6：「便利性」會強化使用「知覺有用性」與使用態度間正向影響之統計分析

表 20 使用態度之階層迴歸分析彙整表 1

	M1	M2	M3	M4
編制專長	-.234**	-.103	-.100	-.103
知覺有用性		.593***	.357***	.373***
便利性			.325***	.329***
知覺有用性*便利性				.048
R^2	.055	.389	.439	.441
R^2改變量	.055	.334***	.050***	.002
*:p<.05 **:p<.01 ***:p<.001				

在表20第一個模式（M1）中首先將編制專長納入控制變項，根據陳寬裕、王正華（2012）於「論文統計分析實務」一書指出，研究的問卷中為避免欲研究的自變數、干擾變數與依變數間的關係，可能受某些其他變數的干擾而遭到扭曲，因此有必要將這些可能干擾的變數控制住，這些可能會干擾研究結果的變數，即稱稱為控制變數，故於階層迴歸分析中，建立區組時，首先要考慮的狀況，先將受訪者基本資料變數的影響力控制下來；可根據相關分析將這些受訪者基本資料變數與依變數關係較為顯著，納入建模考量。

本研究受訪者基本資料變數包括性別、年齡、教育程度、軍事教育程度、階級、工作年資、役別、編制專長等，與依變數「使用態度」進行相關分析，得知受訪者的編制專長與「使用態度」關係較為顯著；因此，於階層迴歸分析中，建立區組時，將編制專長納入控制變項，結果發現可解釋使用態度R^2=5.5%，受訪者的「編制專長」(β=-.234，p<.01)對「使用態度」有顯著負向影響。

在表20第二模式（M2）中發現，加入受訪者的「知覺有用性」（β=.593，p<.001）對「使用態度」有顯著正向影響；當模式3（M3）加入受訪者「便利性」（β=.325，p<.001）變數後，對整體「使用態度」的解釋變異量R^2=43.9%有提升且顯著，顯示「便利性」變數加入模型是有意義的；在模型4（M4）加入「知覺有用性」與「便利性」之交互作用項後，對受訪者整體「使用態度」的解釋變異量R^2=44.1%並無明顯提升且不顯著。

依據以上結果顯示，交互作用項「知覺有用性」與「便利性」對受訪者「使用態度」並不具顯著影響力，說明「使用態度」不會干擾受訪者對「知覺有用性」與「便利性」間的關係，亦即「便利性」並無強化「知覺有用性」正向效果，故H6：「便利性」會

強化使用「知覺有用性」與使用態度間之正向影響不成立。

H7：「便利性」會強化使用「知覺易用性」與使用態度間正向影響之統計分析

表 21 使用態度之階層迴歸分析彙整表 2

	M1	M2	M3	M4
編制專長	-.234**	-.098	-.071	-.071
知覺易用性		.706***	.557***	.558***
便利性			.328***	.328***
知覺易用性*便利性				.005
R^2	.055	.535	.618	.618
R^2改變量	.055	.480***	.083***	.000

*:p<.05　**:p<.01　***:p<.001

在表21第二模式（M2）中發現，加入受訪者的「知覺易用性」（β=.706，p<.001）對「使用態度」有顯著正向影響；當模式3（M3）加入受訪者「便利性」（β=.328，p<.001）變數後，對整體「使用態度」的解釋變異量R^2=61.8%有提升且顯著，顯示「便利性」變數加入模型是有意義的；在模型4（M4）加入「知覺易用性」與「便利性」之交互作用項後，對受訪者整體「使用態度」的解釋變異量量R^2=61.8%並無提升且不顯著。

依據以上結果顯示，交互作用項「知覺易用性」與「便利性」對受訪者「使用態度」不具顯著影響力，說明「使用態度」不會干擾受訪者對「知覺有用性」與「便利性」間的關係，亦即「便利性」並無強化「知覺易用性」之正向效果，故H7：「便利性」會強化使用「知覺易用性」與使用態度間之正向影響不成立。

(三)研究結果與分析

依據 H1~H8 的研究分析結果，除「H6：『便利性』會強化『知覺有用性』與『使用態度』間之正向影響」及「H7：『便利性』會強化『知覺易用性』與『使用態度』間之正向影響」兩者並不成立外，其餘五個假說均為成立；從標準化迴歸係數來看，進入迴歸模式五個預測變項的 β（迴歸係數）值分別為.392、.491、.616、.725、.602、.594，β（迴歸係數）值均為正數，表示其對依變數的影響均為正向，其中，「知覺易用性」對「使用態度」的 β 值較高，達.725 表示當受訪者認為「**共同供應契約資訊系統」愈**容易使用時，對此系統的使用**愈**有正面的態度；另「電腦自我效能」對「知覺有用性」的 β 值**較**低，僅.392，表示對受訪者來說「**共同供應契約資訊系統」應更**具備資訊科技設備常識與背景，對此系統能感受到工作效率增加的有效程度會相對提升。本研究模型假說驗證結果及這構面 β 值整理如圖 18。

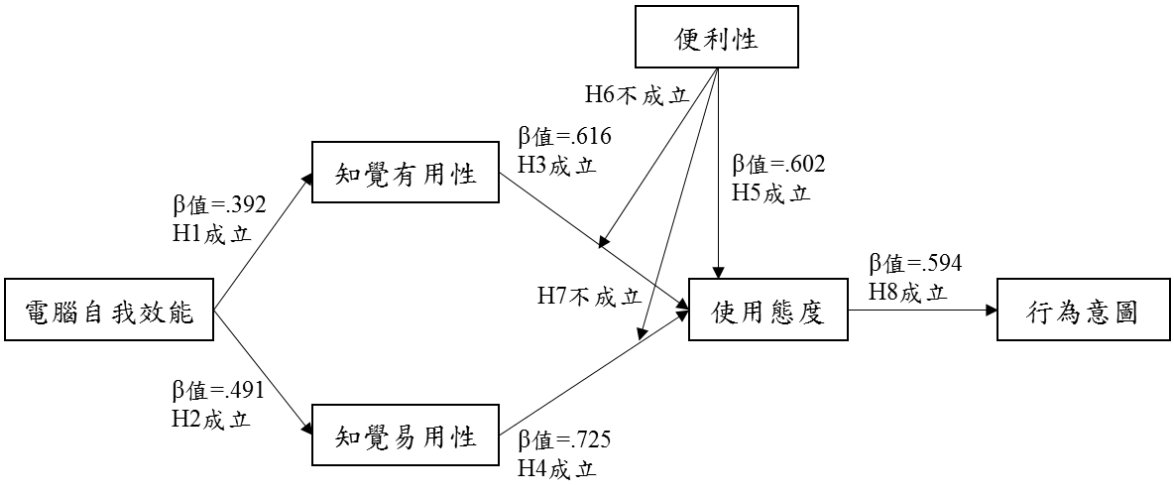


圖 18 研究模型假說結果及 β 值整理

本研究係以科技接受模式（TAM）為理論基礎架構，並以電腦自我效能及便利性為外在變數，另以便利性為調節變數，分析使用者對使用「共同供應契約資訊系統」之「知覺有用性」與「知覺易用性」等構面，進一步驗證影響此系統使用行為的因素。

在本研究各假說部分，「電腦自我效能」對「知覺有用性」有正向影響假說成立，表示使用者具備相當的資訊科技設備常識與背景，也認同「共同供應契約資訊系統」對使用者在採購業務上有所幫助。

「電腦自我效能」對「知覺易用性」有正向影響假說成立，表示使用者在科技資訊上有一定能力，對於「共同供應契約資訊系統」的適應期短，熟練程度較高，而有系統容易操作的認知。

「知覺有用性」與「使用態度」有正向的影響假說成立，表示使用者認同「共同供應契約資訊系統」對使用者在採購業務上有所幫助，並對於「共同供應契約資訊系統」有正面的感受。

「知覺易用性」與「使用態度」呈現顯著正向影響假說成立，表示使用者花費較少心力所學得之資訊科技，會對資訊科技有較正面的感受，也就是說使用者認為「共同供應契約資訊系統」在操作上是簡單易學的，並對使用該系統產生正面、接受的態度。

「便利性」與「使用態度」呈現顯著正向影響假說成立，表示使用者認為使用「共同供應契約資訊系統」來完成採購任務可節省時間和精力的知覺程度，對使用該系統之「使用態度」產生正面、接受的態度。

「便利性」會強化使用「知覺有用性」與使用態度間之正向影響假說不成立，表示「便利性」並不會強化使用者在使用「共同供應契約資訊系統」對採購業務上有所幫助的認知。

「便利性」會強化使用「知覺易用性」與使用態度間之正向影響假說不成立，表示「便利性」並不會強化使用者認為「共同供應契約資訊系統」容易操作的認知。

「使用態度」與「行為意圖」呈現顯著正向影響假說成立，表示使用者對於「共同供應契約資訊系統」有正面的感受，並有極高的可能性繼續使用該系統。以下將各構面的假設結果臚列於表 22。

表 22 假說驗證結果

研究假設	假說檢定

H1	電腦自我效能對知覺有用性有正向影響	成立
H2	電腦自我效能對知覺易用性有正向影響	成立
H3	「知覺有用性」與「使用態度」有正向的影響	成立
H4	「知覺易用性」與「使用態度」呈現顯著正向影響	成立
H5	「便利性」與「使用態度」呈現顯著正向影響	成立
H6	「便利性」會強化使用「知覺有用性」與使用態度間之正向影響	不成立
H7	「便利性」會強化使用「知覺易用性」與使用態度間之正向影響	不成立
H8	「使用態度」與「行為意圖」呈現顯著正向影響	成立

伍、結論

行政院研考會因應網路應用的漸成趨勢，於民國八十五年起陸續建置規劃政府電子採購網，目的在提高機關執行效率、減少資源浪費及提昇競爭力，而「共同供應契約資訊系統」即是其中的一環，期能使各級機關採購人員均能摒除不必要的詢價及招標程序，透過此系統完成採購作業。

本研究即是以空軍各級單位現行或曾經運用「共同供應契約資訊系統」之使用者為研究對象，透過科技接受模式探討使用者持續使用此系統的可能影響因素。科技接受模式應用在資訊系統的常見部份，是以持續行為意願作為構面，加上中介構面的知覺有用性與知覺易用性，透過外部變數之電腦自我效能、便利性，來反應使用者對系統的接受性；此外，本研究並設計便利性作為另外一個中介變數，想藉此瞭解便利性對知覺有用性與知覺易用性是否具有進一步強化之作用。

根據本研究結果顯示，對行為意圖直接而顯著地影響者，以知覺易用性居高，緊接其後者為知覺有用性，再其次是便利性；此外研究結果也顯示電腦能力較佳的使用者，對於「共同供應契約資訊系統」的適應期較短，且熟練程度較高，而產生有系統容易操作的認知，並且認同「共同供應契約資訊系統」對使用者在採購業務上有所幫助。

同時,本研究亦顯示便利性也顯著正向影響使用態度,表示使用者普遍認為使用「共同供應契約資訊系統」來完成採購任務可節省時間和精力的知覺程度，但卻不認為便利性會強化使用者在「共同供應契約資訊系統」容易操作並對採購業務上有所幫助的認知，可知在使用「共同供應契約資訊系統」上，便利性的影響並不如預期顯著。

參考文獻

中文部分

王俊嘉、周珉如、陳美鐘、曾珈儒,2013,以科技接受模式探討智慧型手機與 QR Code 結合的購買行為意圖之研究，TANET2013臺灣網際網路研討會

史麗伶，2011，政府機關導入電子化採購之研究-以共同供應契約電子採購平台系統為例，樹德科技大學資訊管理研究所碩士論文

李淑芳、紀文章，2005，年輕消費者行動電話上網便利性之研究，*經濟與管理論叢*，2005，第一卷，第二期：163~186頁

林宏達，2002，影響資訊人員開發資訊系統自我效能之因素分析，中華大學資訊管理學系碩士班論文

吳明隆，2006，SPSS統計應用學習實務：問卷分析與應用統計，三版，台北，知城

數位科技。
邱皓政，2003，量化研究與統計分析-SPSS中文視窗版資料分析範例解析，台北，五南圖書公司
邱皓政，2008，研究設計與資料處理（量化研究法一）（第一版修訂版），台北，雙葉書廊圖書公司
周君倚、陸洛，2014，以科技接受模式探討數位學習系統使用態度-以成長需求為調節變項，*資訊管理學報*，第二十一卷，第一期：83~106頁
康裕民審閱，Robert, K. & Angelo, K.著，2001，組織行為第五版，台北麥格羅·希爾出版公司
徐孝立，2007，政府採購最有利標機制之研究，國立政治大學社會科學學院行政管理碩士學程碩士論文
徐浩宸，2007，以科技接受模式探討基金網路交易系統使用意願之影響因素，銘傳大學管理學院高階經理碩士學程在職專班碩士論文
陳寬裕、王正華，2012，論文統計分析實務，台北，五南圖書公司
黃淑宜，2004，現金卡服務便利性對服務品質影響之研究，大葉大學人力資源暨公共關係學系碩士論文
黃忠群，2012，以科技接受模式探討共同供應契約資訊系統-以嘉義縣國小使用人員為例，南華大學資訊管理學系碩士論文
曹勛，2012，影響消費者使用NFC行動付款服務之研究，開南大學資訊及電子商務學系碩士論文
歐勁麟，2012，以科技接受模式探討智慧型手機購買意願-以iPhone手機為例，管理創新與行銷專案研討會，國立高雄應用科技大學主辦
林姍儒，2005，消費者知覺便利性影響因素之探討-以東森購物為例，國立嘉義大學行銷與流通管理研究所碩士論文
劉家禎，2011，資訊科技設備常識與背景，中華大學資訊科技管理學系研究所碩士論文

英文部分
Bandura, A. 1977. Self-efficacy： Toward a unifying theory of behavioral change. Psychological Review, 84, 191–215.
Bandura, A. 1984. “Recycling misconceptions of perceived self-efficacy,” Cognitive Therapy and Research, 8（3）, pp.231-255.
Bandura, A. 1991.“Social cognitive theory of self-regulation,” Organizational Behavior and Human Decision Process, 50, pp.248-287.
Baron, Reuben M. and Kenny, David A., 1986. “The moderator–mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations”, *Journal of Personality and Social Psychology*, Vol 51(6), pp. 1173-1182.
Berry, L. L., K. Seiders, and D. Grewal, 2002 “Understanding Service Convenience，“*Journal of Marketing*,66,1-17.
Brown, L. G., 1989, “The Strategic and Tactical Implications of Convenience in Consumer Product Marketing,” *Journal of Consumer Marketing*, 6, 13-19.
Bruner, G. C. & Kumar, A. 2005, “Explaining consumer acceptance ofhandheld internet devices”, *Journal of Business Research*, Vol. 58（5）, pp. 553-558.
Cerny, C.A., & Kaiser, H.F. 1977. A study of a measure of sampling adequacy for factor-analytic correlation matrices. *Multivariate Behavioral Research*, 12(1), 43-47.
Compeau, D.R. & C.A, Higgins. 1995 “Computer self-efficacy： Development of a measure

and initial test" *MIS Quarterly*, June, 1995, pp：189-211.

Cronbach L.J., 1951. "Coefficient alpha and the internal structure of tests".Psychometrika 16（3）： 297–334.

Davis, F. D., 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13（3）, 319-340.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. 1989. "User acceptance of computer technology： A comparison of two theoretical models", *Management Science*, 35（8）, 982-1003.

Davis, F. D., 1993, "User Acceptance of Information Technology: System Characteristics, User Perceptions, and Behavioral Impacts, International Journal of Man Machine Studies", Vol. 38（3）, pp. 475-487

Eastin, M., 2002 "Diffusion of E-commerce： an Analysis of the Adoption of Four E-commerce Activities,"*Telematics and Informatics*, Vol. 19（3）,251-267

Fishbein, M.,Ajzen, I., 1975,Belief, Attitude, Intention, and Behavior： An Introduction to Theory and Research, MA： Addison-Wesley.

Hu, P. J., Chau, P. Y. K., Liu, O. R., and Tam, K. Y., 1999, "Examining the Technology Acceptance Model Using Physician Acceptance of Telemedicine Technology", *Journal of Management Information Systems*, Vol. 16（2）: pp. 91-112.

Hornik, J. 1984. Subjective vs. Objective time measures： A note on the perception of time in consumer behavior. *Journal of Consumer Research*, 11（1）, 615-618.

Kaiser, H. 1974. An index of factor simplicity. *Psychometrika* 39: 31–36.

Likert, R. 1932. A Technique for the Measurement of Attitudes. *Archives of Psychology*, 140, 1–55.

Mathieson, K., Peacock, E. & Chin, W. W., 2001, "Extending the Technology Acceptance Model: The Influence of Perceived User Resources", *The DATA BASE for Advances in Information Systems*, Vol. 32（3）, 86-112.

Meuter, M. L., and Bitner, M. J. 1998.Self-Service Technologies：Extending Service Framework and Identifying Issue for Reasearch. AMA Winter Educators' Conference, pp.12-19.Chicago.

Meuter, M. L., Ostrom, A. L., Roundtree, R. I. and Bitner, M. J. "Self-ServiceTechnologies： Understanding Customer Satisfaction with Technology-Based Service Encounters," *Journal of Marketing* （64：3）, 2000, pp. 50-64.

Moon, J.W. and Kim Y.G. 2001, "Extending TAM for a World-Wide-Web Context" , *Information and Management*, Vol. 38, pp. 217-230.

Shih, H.P., 2004, "Extended Technology Acceptance Model of Internet Utilization Behavior", *Information & Management*, Vol. 41（6）, pp. 719-729.

Vander Heijden, H., 2003, "Factors Influencing the Usage of Websites: The Case of a Generic Portal in the Netherlands", *Information & Management*, Vol. 40（6）, pp. 541-549.

Venkatesh, V. and F.D. Davis 1996. "A model of the antecedents of perceived ease of use： development and test," *Decision Sciences*, 27（3）, pp.451-481.

Venkatesh, V. and Davis, F.D. 2000, "A theoretical extension of the technology acceptance model： four longitudinal field studies", *Management Science*, Vol. 46, No. 2, pp. 186-204.

Yale, L. and Venkatesh A. 1986. "Toward the Construct of Convenience in Consumer

Research”, Advances in Consumer Research Vol. 13, pp. 403-408.

網路部份

台灣銀行，共同供應契約一覽表 http：//www.bot.com.tw › 臺灣銀行 › 採購資訊 › 共同供應契約。

中央信託局共同供應契約簡介，http://www.bot.com.tw/SiteCollectionDocuments/picture_232/LP-1.pdf。

中華民國內政部採購稽核小組，http：//web.moi.gov.tw/psu/news_content.aspx?id=115。

行政院公共工程委員會，政府電子採購系統-政府電子採購網 http：//web.pcc.gov.tw/pishtml/pisindex.html。

行政院公共工程委員會主管會談紀錄，https://www.pcc.gov.tw/pccap2/FMGRfrontend/DownloadQuoteFile.do;jsessionid...

監察院調查報告，https://www.cy.gov.tw/CYBSBoxSSL/edoc/download/7554。

資訊證照認知與實質效益之研究
─兼論專業能力與社會支持影響

陳良駒 [a]　鄭宜珊 [b]

[a] 國防大學管理學院資訊管理學系
[b] 香港商翰竺有限公司台灣分公司

摘要

隨著知識經濟時代的來臨，科技產業是二十一世紀強化國家競爭力的重要因素，而企業體亦深刻體會到資訊人才的培養與獲得已成為了長遠競爭力的重要指標。在全球化、競爭激烈的世代，高學歷不再是高薪就業的保證，求職者如果有一張證照，對自己能力除了可以提出有力「證明」，也會從眾多求職者脫穎而出；然而，隨著認證發放的浮濫，證照的可信度逐漸受到嚴重的質疑，有許多的企業認同市場上的證照種類太多，已無法從證照判斷一個人所具備的專業能力，故如何彰顯出證照與專業能力之間的關係，已是現今需要正視的首要課題。

本研究以欲成為資訊從業人員及已是資訊從業人員者為對象，透過文獻探討蒐整相關資料及以 SEM 模式設定研究假設，設計問卷題項研究渠等專業能力表現及社會支持程度影響資訊證照認知對實質效益之影響。結果顯示，社會支持及專業能力均會正向影響資訊從業人員對資訊證照的認知，然對非資訊從業人員則無顯著影響，但兩者均認同加強資訊證照的認知可加強日後的工作認同度、工作績效等實質效益。綜上所述，研究對象目前是否處於資訊產業中，對各構面而言均有一定程度的差異，但仍可獲得大致相同的結論。

關鍵詞：資訊證照、社會支持、專業能力、實質效益

A Study on the Relationship between IT Certificate and Effectiveness: Also on the Effect of Professional Competence and Social Support

Liang-Chu Chen[a] Yi-Shan Cheng[b]

[a] Department of Information Management, Management College, National Defense University, Taiwan, R.O.C.

[b] ITMS International Limited Taiwan Branch (H.K.)

Abstract

With the coming of knowledge economy era, science and technology industry is an important factor in the twenty-first century to strengthen the country's competitiveness. And companies have deeply appreciated that information professionals training and obtaining has become an important indicator of the long-term competitiveness. In a globalized and competitive generation, highly educated is no longer a guarantee of high-paying employment. Job seekers can not only make a convincing "proof", but also will stand out from others, if they have a license. However, with the abuse of certification granting, license credibility gradually being seriously questioned. Many companies agree that there are too many license types on the market to determine a man's professional competence from his license. Therefore, the most important issue now is how to highlight the relationship between the license and professional competence.

In this study, we take people who want to be IT practitioners and people who have been IT practitioners as the targets. By searching the relevant information through Discussion Document and setting research hypothesis in SEM mode, we can design questionnaire to study how their performance of professional competence and the degree of social support influence the impact of the cognitive of information license on the effectiveness. The results show that social support and professional competence will positively affect IT practitioners awareness of information license, however no significant effects on non-IT practitioners. But both agree to strengthen information license cognitive will strengthen work acceptance, job performance and other effectiveness after. In summary, the research targets are in the IT industry or not, the degree of difference in terms of the various facets, but still get roughly the same conclusion.

Keywords: information license, social support, professional competence , effectiveness

壹、前言

隨著知識經濟時代的來臨，資訊科技產業是二十一世紀強化國家競爭力的重要因素，也是驅動整體產業向上發展的原動力，亦是產業永續經營的泉源。在當今這股知識經濟潮流裡，企業體都深刻體會到資訊人才的培養與獲得，已然成為企業是否具備長遠競爭力的重要指標。

在全球化、競爭激烈的世代，高學歷不再是高薪就業的保證，反倒擁有專業能力、專業證照才能贏在職場起跑點，求職者如果有一張(最好數張以上)證照，對自己能力除了可以提出有力「證明」，也會從眾多求職者脫穎而出，成為面試主管審慎考慮的對象，放眼看現在企業界所找尋的專業資訊人才，逐漸注重資訊人才的專業能力鑑定與認證，可透過專業證照之推廣，來強化資訊技術之重要性(李育杰，2013)。

然而，根據104人力銀行調查「企業不從證照判別人才具有的資訊能力」的各項原因中，有67.9%的企業認同市場上的證照種類太多，無法單純從證照判斷一個人所具備的專業能力，故考取證照已無法保證能在薪資或職務提升上有所回饋，彰顯出證照與專業能力之間的問題！也是現今需要正視的首要課題。

當今企業的人才招募取向，除了以學歷為基本錄取門檻，更將專業能力與證照取得作為企業是否錄用應徵者的衡量指標，以CCNA(Cisco Certified Network Associate)為例，思科系統公司所推出的CCNA基礎認證，目的是為了幫助欲從事資訊工作的個人，迅速了解企業大型網路運作原理與基本架構的入門證照，故而CCNA便成為資訊業招募人才的預設門檻，這也促使眾多非資訊相關背景的人們，為了擠進資訊窄門而使出渾身解數、想方設法取得這張專業證照。

因應資訊業隨時求新求變的革命浪潮，欲成為資訊從業人員應及早預劃未來職涯發展，故須有系統的學習來規劃未來方向。欲成為資訊從業人員及已是資訊從業人員者，從社會支持及專業能力對資訊證照認知的影響，以及資訊證照認知與實質效益之相互關係，正是本研究計畫的立論方向。目前影響資訊從業人員職涯發展的因素已不僅止於教育程度所造成的差別，具備專業能力及相關專業證照的新一代人力資源將成為企業取材的重要來源。此間差異關係亦是促使發起本研究的主要動機。

本研究係以欲成為資訊從業人員及已是資訊從業人員者為對象，主要是研究前述兩者的社會支持程度及專業能力表現影響資訊證照認知對實質效益之相互關係。研究目的說明如下：

一、了解社會支持程度、專業能力表現分別影響資訊證照認知及資訊證照認知對實質效益之相互關係。

二、了解資訊從業人員及非資訊從業人員對此研究架構模式之差異性。

三、了解資訊從業人員及非資訊從業人員分別對社會支持、專業能力、資訊證照認知及實質效益的差異性。

貳、文獻探討

2.1 資訊證照的認知

資訊領域的認證制度自1985年由美國資訊廠商Novell所推出的CNE(Certified Novell Engineer)認證。當時，隨著Novell的網路作業系統NetWare廣受企業使用，Novell為了因應此產品的市場銷售與客戶服務，並同時確保專業品質，因而推出該制度(黃文風，2010)。

隨著全球化與知識經濟時代來臨，因應產業結構與技術快速變遷，需建立專業人員證照制度，作為培訓產業需求，以提升產業競爭力。專業證照係指對某一職業從業人員從業資格的一種認定，不但認定了證照持有者具有從事某特定工作所需的技術能力或專業知能，甚至可作為某特定工作執業的憑藉。而證照的建立亦可提升從業人員的專業水

準，進而保障消費者權益(康龍魁，1993；劉照金，1997)。證照可有效地將個人專業外顯、具體化，並代表個人執行工作時具有一定程度的可靠性與有效性，此代表性儼然成為個人在職場就業與競爭力的重要指標。而不同產業的相關證照研究也指出，相較之下，證照擁有者有較高專業能力，且從個人角度出發，大部份產業對於證照仍抱持正面態度，認為可提升職場競爭力及較多的求職、職務升遷及加薪機會(黃同圳，2009)。

而國外推動證照制度亦十分盛行，以歐盟為例，2006年9月歐盟執委會發布了歐盟議會及歐盟理事會共同倡議「歐盟職能標準架構」(European Qualifications Framework)指導方針，建議歐盟會員國在2009年前建立相對應的職能標準架構，後續在2012年所推動的求學與工作護照-「歐洲通行證」(Europass)中，附加了申請者的「歐盟職能標準架構」證明文件。據此，可了解專業證照的重要性除了證明自我專業能力外，更能跨出國際、與全球相關企業接軌。

2.2 社會支持

Caplan(1974)以社會交換的觀點來說明社會支持是透過社會互動所產生的個人回饋，能幫助人們在各種環境下抵抗壓力。也就是說，社會支持透過社會互動之依賴感，可促使人面對挑戰與壓力。社會支持是自我與他人互動之喜愛、同情、了解、接納、認可與信任等心理情感，或忠告、訊息及財務等實質上的協助，藉以滿足情感、自尊、讚賞、歸屬、認同及安全感等基本需求的歷程(張笠雲，1986)；故提供有效的幫助即是社會支持的一環，藉由透過他人或團體的幫助，使自我獲得協助、滿足需求(Mina, Jessica & Nancy, 2009)。

參據各學者對於社會支持的看法，社會支持產生於個體與個體或個體與團體的互動，因此社會支持來源也隨所處的環境而有不同的提供者，來源可來自家庭中的家人、親友、工作場所的同仁、或是學校中的師長、同學，甚至是社會團體。又因家庭社經背景、參與度、成績表現等人口背景變項的差異，連帶使得社會支持不盡相同。Cutrona & Russell(1990)曾將社會支持分為下列五種：

一、資訊支持(Informational Support)：指的是社會支持提供者提供需求者建議或解決問題的可能策略。

二、情感支持(Emotional Support)：在需要時給予即時的關懷與安慰，讓需求者感受到自己是被人關心的。

三、尊重的支持(Esteem Support)：給予需要社會支持的個體正面回饋，讓對方感受到他是有能力完成某項任務，並且可以面對壓力事件。

四、實際的幫助(Tangible Aid)：具體的工具性支持(Instrument Support)，給予社會支援需求者必要資源，如金錢，以便助其渡過壓力。

五、社會網絡的支持(Socialnetwork Support)：又稱為「社會整合(Social Integration)」的支持，讓個體感受到自己屬於一個團體，使其具有歸屬感。

本研究基於Cutrona & Russell(1990)學者對於社會支持的概念，及吳明燕(2014)所彙整國內學者因研究對象及主題不同而有不同來源分類，將本研究社會支持問項從主管支持及同仁支持等兩個面向進行研究。

2.3 專業能力

專業能力一般定義為執行專案工作時所需之知識、能力、技術與價值觀等，故通常可透過專業能力來預估一個人在工作行為或工作績效上的表現(陳姿伶，2011)。專業通常是指經過某種特殊訓練後，運用專門性和學術性的知識與技能來執行職務成為有價值的行為，導致有價值的成就(林麗婷，2001)。而能力的定義則是在某一領域中，能勝任某一項工作，或者從事某一工作所具備的知識、技能和態度等。因此，能力的概念並不

只是知識而已，而是能夠確實執行或從事某一工作(黃政傑，1985)。

Chisholm & Ely(1976)則對專業能力提出三個因素，本研究亦將以此三個因素做為研究變項：

一、 專業知識：係指專業人員於工作時所需瞭解的資料與事實，透過所獲得之資訊，能有效率地達成某一任務，在傳統的專業訓練中最重視知識能力的訓練，因為知識是工作能力實際表現的必備條件，而且知識層級的能力較容易評量。

二、 專業技能：係指專業人員運用知識以解決特殊問題的能力，其評量的方式可從觀察解決問題的實際表現或處理過程的具體結果加以評定。

三、 專業態度：係指一種情感的趨避作用，由觀察特定人員的對話或行為表現以評量特定人員的態度，雖然態度的評量較不易客觀，卻不失為衡量專業能力的指標。

2.4 實質效益

Herzberg et al.在1959年所提出的雙因子理論(Two Factors Theory)，又稱「激勵─保健理論」(Motivator Hygiene Theory)。根據Herzberg等學者的說法，造成工作滿足與工作不滿足的原因是各自獨立的因素，使員工不滿足的因素多與「外在環境」有關，例如：工作環境、工作地位、人際關係、薪資福利、工作條件、公司政策等，稱為保健因素，此因素只能預防員工的不滿足，但卻不一定能激勵他，使他對工作感覺到滿足。要使員工感覺到滿足則要從與「工作本身」有關的因素著手，例如成就感、認同感、工作本身、責任、升遷和個人成長等因素，這些因素稱之為激勵因素。這些因素，才能使員工產生工作滿足感。換句話說，「保健因子」則是用來防止工作不滿足的因素，使員工工作情緒、效率與品質等保持原狀而不降低之措施。「激勵因子」，係指可以激發員工的工作動機意願、提高士氣、生產力，是一種影響員工工作滿足的因素。

綜合上述的雙因子理論，本研究將實質效益定義涵蓋了工作認同度、工作績效、薪資與福利、職務升遷分別探討激勵因素與保健因素之影響。

參、研究架構

3.1 研究架構與假說設定

本研究旨在探討資訊從業人員及非資訊從業人員在社會支持、專業能力、資訊證照認知及實質效益認知的差異情況。Friedman(1982)曾說明證照制度建立之重要性包含了社會認同、提升自我肯定、達成專業目標、促進專業發展及促進公平就業等項，並從Cutrona & Russell(1990)學者對於社會支持的概念、Chisholm & Ely(1976)對專業能力看法及(Herzberg et al., 1959)雙因子理論中所含涵蓋的實質效益，本研究擬以社會支持、專業能力、資訊證照認知及實質效益等四個構面形成本研究之架構，如圖1所示。

依據研究架構及目的，設立研究假設如下。

一、研究假設 1(H1)：社會支持會正向影響資訊證照認知。

社會支持即是透過人與團體提供的幫助，使個體可獲得有實質效益的協助、滿足需求(Mina, Jessica & Nancy, 2009)，從他人的勸誡、勉勵、即時的訊息及物質服務的行為中，個體可提升面臨困境的能力，改變因壓力造成的影響(Thoits, 1986)，故社會支持為個人與個人，或個人與團體間的一種依賴與互動，使個人在面對挑戰、壓力和困難時，可增進其適應力；Cutrona & Russell(1990)將社會支持分為資訊支持、情感支持、尊重的支持、具體的工具性支持及社會網絡的支持。故本研究提出研究假設 1：社會支持會正向影響證照認知。

二、研究假設 2(H2)：專業能力會正向影響資訊證照認知。

由於專業能力係經由學習者學習後，所表現出的學養、技術以及反應，所以專業能力包涵專業知識、專業技能與專業態度三要素，而這些要素將相互作用且同時

發生(Chisholm & Ely, 1976)；陳姿伶(2011)也指出：專業能力係指從事一個專業應具備之所有內涵條件和從事此項工作時應具備之整體能力。綜合以上學者之研究，專業能力即是各職業、各職務或各作業人員需具備相對應其職務的能力。

透過證照的考試制度，可提升個人更多的專業知識並予以應用(林博文，徐志明，2001)，而為了順應現今的資訊產業型態，資訊從業人員需要不斷提升所需技能和知識，同時為了擁有更多的專業認同，也必須不斷學習新技能或是取得相關證照，以獲得組職對他們的專業認可(黃心怡，2004)。因此，本研究提出研究假設2：專業能力會正向影響證照認知。

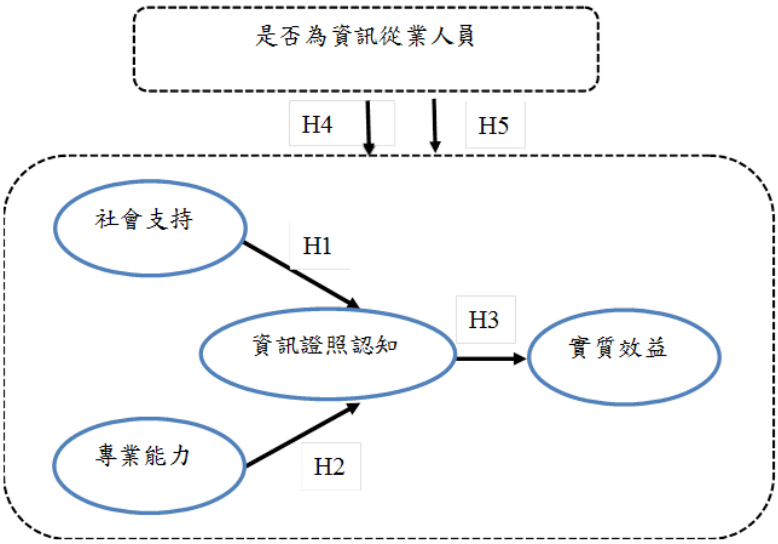


圖 1、研究架構

三、研究假設 3(H3)：資訊證照認知會正向影響實質效益。

一般來說，大部分的求職者認為擁有證照就等於擁有一張工作的通行證(彭幸璇，2003)，而證照的取得也可獲得更好的職位與收入報酬等工作條件(黃心怡，2004)，故本研究從實質效益著點來了解對資訊證照認知的差異，參考陳美伶(2007)所提出實質效益構面，提出研究假設3：證照認知會正向影響實質效益。

四、研究假設 4(H4)：資訊從業人員/非資訊從業人員在整體結構影響具有顯著差異性。

在文獻探討中，發現過去各學者探討證照對各構面影響的研究裡，研究對象均以目前已是從業人員或學生為主，未從目前已在產業的從業人員及未來想進入該產業人員中切入探討，故本研究擬以上述兩者做為研究對象，以資訊從業人員及未來想進入資訊職場的非資訊從業人員的角度來了解此整體結構，而研究所得結果亦可提供未來想進入資訊產業之從業人員參考，故提出研究假設 4：資訊從業人員/非資訊從業人員在整體結構影響具有顯著差異性。

五、研究假設 5(H5)：資訊從業人員/非資訊從業人員在社會支持、專業能力、資訊證照認知及實質效益具有顯著差異性。

承研究假設4，在探討資訊從業人員/非資訊從業人員在整體結構影響具有顯著差異性後，賡續從這兩種不同的人員角度來個別了解他們對社會支持、專業能力、資訊證照認知及實質效益之差異。故提出研究假設5：資訊從業人員/非資訊從業人員在社會支持、專業能力、資訊證照認知及實質效益具有顯著差異性。

3.2 研究變數與操作型定義

本研究說明研究架構所提出社會支持、專業能力、資訊證照認知、實質效益等四個構面，各研究變項之操作型定義如下：

一、社會支持變項

本研究參考吳明燕(2014)提出對社會支持的定義，將社會支持問項從主管支持及同仁支持兩個角度出發而設計該構面之問項，研究變項之操作型定義如下：

(一)主管支持：主管支持係指主管可提供員工解決問題之建議並給予適當的關懷，使員工在遇到學習上的問題時能得到正面回饋，讓員工感受到是有能力完成某項任務，並且能夠面對壓力及隨壓力而來的種種影響。

(二)同仁支持：同仁支持係指同仁可提供員工一起解決問題之建議並給予適當的關懷，使員工在遇到學習上的問題時能得到正面回饋，讓員工感受到是有能力完成某項任務，並且能夠面對壓力及隨壓力而來的種種影響。

二、專業能力變項

本研究參考 Chisholm & Ely(1976)提出對專業能力的定義，將專業能力問項從專業知識、專業技能及專業態度三個角度出發而設計該構面之問項。

(一)專業知識：專業知識係指專業人員於工作時所需瞭解的資料與事實，透過所獲得之資訊，能有效率的達成某一任務。

(二)專業技能：專業技能係指專業人員運用知識以解決特殊問題的能力，其評量的方式可從觀察解決問題的實際表現或處理過程的具體結果而加以評定。

(三)專業態度：係指一種情感的趨避作用，由觀察特定人員的對話或行為表現以評量特定人員的態度，雖然態度的評量較不易客觀，卻不失為衡量專業能力的指標。

三、資訊證照認知變項

本研究參考呂宇倫(2005)、黃文風(2010)提出對證照的意義與功能認知變項，變項的操作型定義為個人對證照取得的態度及證明專業能力，並予以應用於工作上，以提升競爭力及取得較好的實質效益。

四、實質效益變項

本研究參考陳美伶(2007)提出對實質效益的定義，將實質效益問項從工作的認同度、工作績效、薪資及福利及職務升遷四個角度出發而設計該構面之問項，研究變項之操作型定義如下：

(一)工作的認同度：係指員工經由工作上的付出所得到的成就感及組職、客戶所給予的肯定，可讓員工提升工作熱忱。

(二)工作績效：係指一個組織成員為完成組職所規定、期望的需求時所表現的所有行為，而這些行為必須對於組織目標有所貢獻。

(三)薪資及福利：係指員工在工作上的付出，組織所給予對等的報酬作為回報，而報酬的大小及形式，通常取決於工作的內容、複雜度、員工技能、績效表現等因素。

(四)職務升遷：係指對現職人員之職務作有計畫的升遷、培訓、進修及外派等。

3.3 研究問卷設計方法

本研究採用問卷調查法作為研究工具，問卷編制是依據研究目的、研究架構及相關文獻，並參考龔永宏(2004)、呂宇倫(2005)、陳建陽(2005)、陳美伶(2007)、黃文風(2010)、吳明燕(2014)等問卷據以修改編製出本研究之問卷。問卷內容主要分為社會支持、專業能力、資訊證照認知、實質效益及、基本資料變項等五大類別，採用李克特(Likert)五點尺度量表，從「非常不同意」至「非常同意」，分別給予1至5分，得分越高表示對此題項認同度越高。

本研究旨在探討資訊從業人員/非資訊從業人員在社會支持、專業能力、資訊證照認

知及實質效益認知的差異情況，以下就分別就對象定義、發送方式及發送對象說明。

一、對象定義：資訊從業人員為目前已從事資訊專業相關工作之工程師；非資訊從業人員為未來欲從事資訊專業相關工作者。

二、發送方式：以紙本問卷及網路問卷 2 種。

三、發送對象：紙本問卷回收中，資訊從業人員之問卷發送對象，主要以 A 教育訓練中心 2014-2015 年之目前已是資訊從業人員實施調查;非資訊從業人員之問卷發送對象主要以 B 教育訓練中心 2015 年之目前非資訊從業人員且未來想進入資訊相關產業工作者實施調查。網路問卷則放至網路平台中調查。

3.4 資料分析方法

本研究依據研究目的及假設之檢定所需，透過信度分析，篩選出具有內部一致性的題目，進行問卷調查。使用SPSS統計軟體及AMOS結構方程模式分析軟體做為資料分析工具。進行各量表間的驗證性因素分析與因果關係檢驗其分析。

肆、研究成果

本研究之根據，是否為資訊從業人員連行採立意抽樣(Purposive Sampling)方式進行問卷調查。正式問卷總計發送 600 份問卷，回收問卷總計 334 份，其中，資訊從業人員問卷回收計 171 份，有效問卷 150 份，無效問卷 21 份；非資訊從業人員問卷回收計 163 份，有效問卷 150 份，無效問卷 13 份。

本部份針對性別、年齡、學歷、教育背景、目前是否為資訊從業人員、從事資訊相關工作年資、職位等七項進行敘述性統計分析(資料詳如表1)。

表1、受訪者資料統計分析

類別	項目	人數	百分比	累計百分比
性別	男性	278	92.7	92.7
	女性	22	7.3	100.0
年齡	20歲以下	2	0.7	0.7
	21-30歲	172	57.3	58.0
	31-40歲	73	24.3	82.3
	41歲以上	53	17.7	100.0
學歷	研究所(含)以上	86	28.7	28.7
	大學/專科	213	71.0	99.7
	高中職(含)以下	1	0.3	100.0
教育背景	資訊相關科系畢業	140	46.7	46.7
	非資訊相關科系畢業	160	53.3	100
目前是否為資訊從業人員	是	150	50.0	50.0
	否，但未來想進入資訊產業	150	50.0	100.0
資訊工作年資	無經驗	144	48.0	48.0
	5年以下	47	15.7	63.7
	6-10年	52	17.3	81.0
	11-15年	26	8.7	89.7
	16-20年	20	6.7	96.3
	21年以上	11	3.7	100.0
職務	非主管職務	279	93.0	93.0
	主管職務	21	7.0	100.0

本研究以 Cronbach’s α 來檢定問卷中各因素之衡量變數的內部一致性程度。問卷各

構面之 Cronbach' s α 介於 0.930 至 0.962 之間，均高於 0.80 之標準。本研究的衡量變數是根據文獻探討，以及專家學者之意見所修訂而成，並經過預試的過程，因此本研究具有相當的內容效度(Content Validity)及表面效度(Face Validity)。各項構面之建構效度透過驗證性因素分析之測試，多數均符合良好適配度的標準。據此，可進行整體模式適配度的檢定。

從社會支持、專業能力、資訊證照認知及實質效益的所有題項的標準化迴歸係數(因素負荷量)介於 0.561 至 0.919 之間，且 t 值均大於 1.96，表示係數呈現顯著的情況；再觀察整體建構效度驗證表，如表 2，各構面的建構信度皆大於 0.60；各構面的平均變異抽取量亦均大於 0.50，各項係數都符合收斂效度的要求，顯示整體測量模型的內在品質為佳。

表2、整體建構效度的驗證表

構面	項目數	建構信度	平均變異抽取量	相關係數			
				社會支持	專業能力	資訊證照認知	實質效益
社會支持	3	0.947	0.751	1			
專業能力	8	0.947	0.643	-0.270	1		
資訊證照認知	5	0.946	0.688	0.478	-0.066	1	
實質效益	3	0.967	0.833	0.465	-0.026	0.741	1

從整體建構效度驗證表，表 2 各構面的平均變異抽取量的最小值為 0.643，大於各構面間相關係數最大值的平方$(0.741)^2$，故本研究模型亦符合區別效度之要求，因此，可再次證照測量模型的內在品質頗佳。

4.2 結構模式

本研究目的在討探社會支持、專業能力、資訊證照認知、實質效益等變項之間關係，並以AMOS進行路徑分析，建構變項間之線性結構關係模式，以驗證本研究之假設。

一、整體結構模型評鑑

本研究之實質效益模型適配度指標詳如表3，此模型已經過模式修正(Modification Index, MI)，修正後本模式絕對配適檢定指標、增量配適檢定指標及精簡配適檢定指標中AGFI為0.859、NFI為0.895、RFI為0.880，皆相當接進0.9，惟仍於可接受範圍內，其他皆符合良好適配度的標準。據此，可進行整體模式適配度的檢定。

表3、整體模型配適度指標檢定表

模型適配指標	檢定結果	模型適配指標	檢定結果
絕對適配指標		增值適配指標	
χ^2	359.584	AGFI	0.859
χ^2/df	2.413	NFI	0.895
GFI	0.890	NNFI	0.926
RMR	0.057	CFI	0.935
RMSEA	0.069	RFI	0.880
簡效適配指標		IFI	0.936
PNFI	0.780		
PGFI	0.698		

二、模式基本配適度

本研究之整體模式基本配適度指標詳如表4，各構面的衡量指標之因素負荷量介於0.601至0.926，皆超過0.5以上，且t值大於1.96(p<0.001)，均達顯著水準；衡量誤差變異

數皆為正數，皆達顯著水準，整體而言為可接受範圍。

表 4、整體模式基本配適度指標

參數	估計值	t值	誤差變異數	解釋能力
SS_2→社會支持	0.836	--	0.209	0.699
SS_8→社會支持	0.780	13.705***	0.274	0.608
SS_{12}→社會支持	0.785	13.781***	0.254	0.616
PA_2→專業能力	0.601	--	0.403	0.361
PA_3→專業能力	0.658	9.223***	0.356	0.433
PA_4→專業能力	0.713	9.761***	0.318	0.508
PA_5→專業能力	0.719	9.826***	0.284	0.517
PA_6→專業能力	0.710	9.736***	0.304	0.504
PA_7→專業能力	0.684	9.481***	0.336	0.468
PA_8→專業能力	0.824	10.725***	0.225	0.679
PA_{11}→專業能力	0.690	9.540***	0.176	0.476
CC_1→資訊證照認知	0.779	--	0.175	0.607
CC_3→資訊證照認知	0.857	15.819***	0.120	0.734
CC_6→資訊證照認知	0.689	12.233***	0.322	0.475
CC_9→資訊證照認知	0.602	10.492***	0.413	0.362
CC_{13}→資訊證照認知	0.767	13.869***	0.219	0.588
EB_3→實質效益	0.897	--	0.092	0.805
EB_4→實質效益	0.926	24.977***	0.052	0.857
EB_6→實質效益	0.893	23.100***	0.072	0.797

註：*p<0.05, **p<0.01, ***p<0.001

社會支持構面因素負荷量介於0.780至0.836之間，且t值均大於1.96(p<0.001)，表示係數呈現顯著的情況；在R^2方面介於0.608至0.699之間，皆大於0.5，表示具解釋能力。從社會支持構面之因素負荷量比較得知，個人對社會支持之程度，以SS_2「主管會關心我學習的狀況」為最重要的因素，其次為SS_8「同仁會聽我說準備資訊證照的經驗」，最後為SS_{12}「當我表現不好時，同仁會鼓勵我不要氣餒」。

專業能力構面因素負荷量介於0.601至0.824之間，且t值均大於1.96，表示係數呈現顯著的情況；在R^2方面，除了PA_2「我對資訊相關法令均能了解」為0.361，未達大於0.4理想標準，解釋能力較低，其於皆介於0.433至0.679之間，皆大於0.4，表示具解釋能力。從專業能力構面之因素負荷量比較得知，個人對專業能力之程度，以PA_8「我能迅速幫客戶解決資訊專業問題，並滿足客戶需求」為最重要的因素，其次為PA_5「我有接受足夠的資訊專業訓練，對基本的資訊知識有基礎的掌握」，而PA_2「我對資訊相關法令均能了解」則為最低。

資訊證照認知因素負荷量介於0.602至0.857之間，且t值均大於1.96，表示係數呈現顯著的情況；在R^2方面，除了CC_9「透過證照考試可以更熟悉相關業務內容」為0.362，未達大於0.4理想標準，解釋能力較低，其於皆介於0.475至0.734之間，皆大於0.4，表示具解釋能力。從資訊證照認知構面之因素負荷量比較得知，個人對資訊證照認知之程度，以CC_3「資訊證照可以提升資訊從業人員整體素質，增加專業服務水準」為最重要的因素，其次為CC_1「我認為資訊證照對資訊從業人員很重要」，而CC_9「透過證照考試可以更熟悉相關業務內容」則為最低。

實質效益因素負荷量介於0.893至0.926之間，且t值均大於1.96，表示係數呈現顯著的情況；在R^2方面介於0.797至0.857之間，皆大於0.5，表示具解釋能力。從實質效益構

面之因素負荷量比較得知，個人對實質效益之程度，以EB_4「提升我對資訊專業上的自我肯定」為最重要的因素，其次為EB_3「提升我對資訊專業的認同度」，最後為EB_6「提升工作成員對我的資訊專業信任度」。

三、整體結構因果模式

本研究所建構之社會支持、專業能力、資訊證照認知及實質效益關係之整體結構模式如圖2所示。並依實證分析結果，進研究假設驗證，如表5所示。以下就各構面之驗證及研究模式茲分述說明。

(一)社會支持會正向影響資訊證照認知

社會支持對資訊證照認知的路徑係數為0.598，t值為8.843，大於1.96之標準(P<0.001)，表示具有正向的影響，故本研究之「研究假設H1：社會支持會正向影響資訊證照認知」為成立， 由此可知，當對社會支持程度越深，對於資訊證照認知影響就越高。因此，若能加深社會支持的程度，即能強化對資訊證照認知的看法。

(二)專業能力會正向影響資訊證照認知

專業能力對資訊證照認知的路徑係數為0.060，t值為1.084，t值小於1.96之標準(P=0.278)，表示無顯著之影響，故本研究之「研究假設H2：專業能力會正向影響資訊證照認知」為不成立，由此可知，若加深其專業能力的程度，不一定能強化對資訊證照認知的看法。

(三)資訊證照認知會正向影響實質效益

資訊證照認知對實質效益的路徑係數為0.841，t值為13.886，大於1.96之標準(P<0.001)，表示具有正向的影響，故本研究之「研究假設H3：資訊證照認知會正向影響實質效益」為成立，由此可知，當資訊證照認知程度越深，對於實質效益之影響就越高。因此，若能加深對其資訊證照認知的程度，即能強化對實質效益的看法。

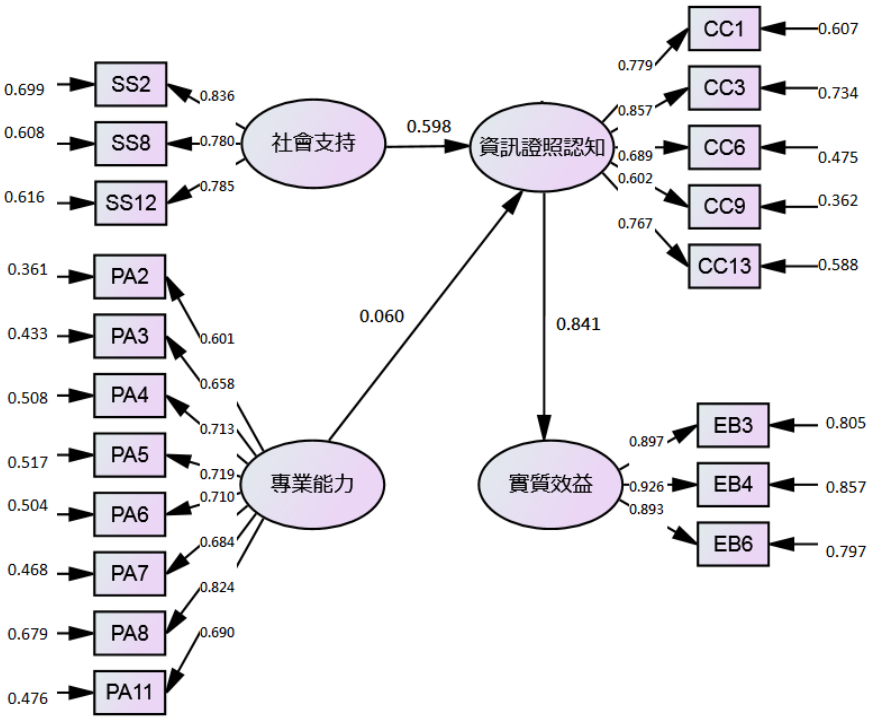


圖 2、整體結構模式圖

在整體結構模式中可看出，影響資訊證照認知最重要的為實質效益，其次為社會支

持，而專業能力則為無顯著。黃心怡(2004)曾提出「資訊從業人員需要不斷提升所需技能和知識，同時為了擁有更多的專業認同，也必須不斷學習新技能或是考取相關證照，以取得組職對他們的專業認可」，黃文風(2010)亦提及「擁有資訊證照對資訊從業人員專業技能具有加分的效果，可以讓人更加肯定本身的專業技能」，在本研究的發現，專業能力對於資訊證照認知中與以往認知上有所差異，專業能力的高低對於資訊證照的認知無絕對的關係。

表 5、整體模式結構路徑表

假設	路徑關係	路徑值	t 值	檢定結果
H_1	社會支持→資訊證照認知	0.598	8.843***	成立
H_2	專業能力→資訊證照認知	0.060	1.084	不成立
H_3	資訊證照認知→實質效益	0.841	13.886***	成立

註：*p<0.05, **p<0.01, ***p<0.001

4.3 資訊從業人員與非資訊從業人員於相同結構模式分析

本研究之資訊從業人員及非資訊從業人員相同結構模式檢驗結果詳如表6，資訊從業人員群及非資訊從業人員群之結構模式如圖3、4所示。進行兩群體路徑之比較，在社會支持對資訊證照認知，資訊從業人員群之路徑(路徑值= 0.611，t值= 5.175，p<0.001)顯著高於非資訊從業人員群之路徑(路徑值= -0.014，t值= -0.163，p=0.871)，得知資訊從業人員與非資訊從業人員對於社會支持程度不同，所產生的資訊證照認知效果亦有不同；專業能力對資訊證照認知，資訊從業人員群之路徑(路徑值=0.452，t值=5.244，p<0.001)顯著高於非資訊從業人員群之路徑(路徑值= -0.199，t值= -1.456，p=0.145)，得知資訊從業人員與非資訊從業人員對於專業能力程度不同所產生的資訊證照認知效果亦有不同；資訊證照認知對實質效益，資訊從業人員群之路徑(路徑值=0.882，t值=9.00，p<0.001)顯著高於非資訊從業人員之路徑(路徑值=0.651，t值=7.249，p<0.001)，可知資訊從業人員與非資訊從業人員對於資訊證照認知程度不同，所產生的實質效益認知程度便有所不同。綜上所述，檢視「研究假設4：資訊從業人員/非資訊從業人員在整體結構影響具有顯著差異性」，無論是資訊從業人員或是非資訊從業人員的樣本，資訊證照認知對實質效益均為正向影響，而資訊從業人員及非資訊從業人員對於社會支持、專業能力程度認知不同，對資訊證照認知就有所不同。其中資訊從業人員對於「社會支持對於資訊證照認知」、「專業能力對於資訊證照認知」、「資訊證照認知對於實質效益」皆為正向影響，最為相關者為實質效益，其次為社會支持，最末為專業能力；而非資訊從業人員僅對於「資訊證照認知對於實質效益」為正向影響，「社會支持對於資訊證照認知」、「專業能力對於資訊證照認知」則無顯著影響，因本研究之非資訊從業人員為欲成為資訊從業人員者，故對資訊證照認知以實質效益為重，而社會支持、專業能力分別對資訊證照的看法則無顯著影響。由此可知，社會支持、專業能力程度高低不會直接影響非資訊從業人員對資訊證照的認知。

表6、資訊從業人員及非資訊從業人員相同結構模式檢驗結果

影響路徑	資訊從業人員		非資訊從業人員	
	路徑值	t 值	路徑值	t 值
社會支持→ 資訊證照認知	0.611	5.175***	-0.014	-0.163
專業能力→ 資訊證照認知	0.452	5.244***	-0.199	-1.456
資訊證照認知→ 實質效益	0.882	9.00.***	0.651	7.249***

註：檢定結果均為資訊從業人員>非資訊從業人員 (*p<0.05, **p<0.01, ***p<0.001)

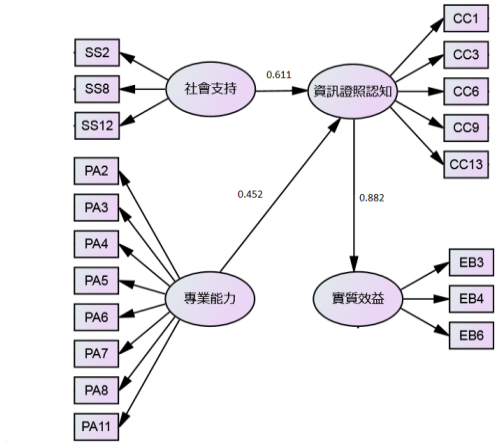


圖 3、資訊從業人員群之結構模式圖

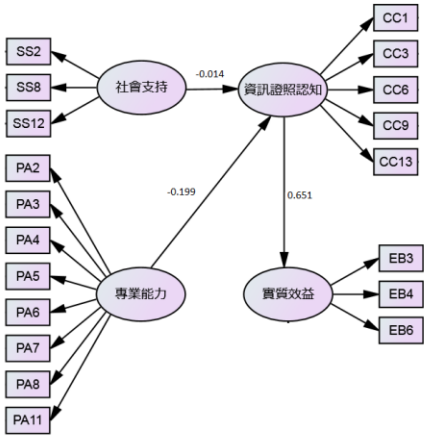


圖 4、非資訊從業人員群之結構模式圖

4.4 獨立樣本 T 檢定

本研究之資訊從業人員及非資訊從業人員之獨立樣本t檢定結果詳如表7，從表中可發現，社會支持、專業能力、資訊證照認知、實質效益等四個構面的p值小於0.05，具有顯著性，表示資訊從業人員及非資訊從業人員在這四個構面中具有顯著差異。

表 7、資訊從業人員及非資訊從業人員獨立樣本 t 檢定結果

構面	資訊從業人員		非資訊從業人員		t 值
	平均數	標準差	平均數	標準差	
社會支持	3.600	0.661	4.380	0.549	-11.118
專業能力	2.907	0.357	2.318	0.217	17.250
資訊證照認知	3.936	0.609	4.420	0.428	-7.973
實質效益	4.136	0.597	4.520	0.512	-5.988

本研究之「研究假設5：資訊從業人員/非資訊從業人員在社會支持、專業能力、資訊證照認知及實質效益具有顯著異性」，各構面分析如下：

(一) 社會支持

在個人對社會支持程度中，有顯著差異存在(t=-11.118，p<0.001)，非資訊從業人員(M=4.380)高於資訊從業人員(M=3.600)，可見非資訊從業人員對於「主管會關心我學習的狀況」、「同仁會聽我說準備資訊證照的經驗」、「當我表現不好時，同仁會鼓勵我不要氣餒」，皆高於資訊從業人員，從此研究可了解，非資訊從業人員對於社會支持上的程度高於資訊從業人員。

(二) 專業能力

在個人對專業能力表現中，有顯著差異存在(t=17.250，p<0.001)，資訊從業人員(M=2.907)高於非資訊從業人員(M=2.318)，可見資訊從業人員對於「我對資訊相關法令均能了解」、「我對資訊業務工作的處理程序均能了解」、「我能根據不同之客戶狀況，立即給予資訊專業服務與幫助，並作適當的處理」、「我有接受足夠的資訊專業訓練，對基本的資訊知識有基礎的掌握」、「我能依據客戶所提供的資訊專業問題，來研判客戶可能發生的原因」、「我會常常學習與資訊業務相關的新專業知識」、「我能迅速幫客戶解決資訊專業問題，並滿足客戶需求」、「我對資訊業務上，常以嚴謹的工作態度去面對」，皆高於非資訊從業人員，從此研究可了解，資訊從業人員對於專業能力上的程度高於非資訊從業人員。

(三) 資訊證照認知

在資訊證照認知程度中，有顯著差異存在(t=-7.973，p<0.001)，非資訊從業人員(M=4.420)高於資訊從業人員(M=3.936)，非資訊從業人員對於「我認為資訊證照對資訊從業人員很重要」、「資訊證照可以提升資訊從業人員整體素質，增加專業服務水準」、「資訊證照可作為人事升遷管理制度的依據」、「透過證照考試可以更熟悉相關業務內容」、「面對不同資訊職位，應具備不同等級之證照」，高於資訊從業人員，從此研究可了解，非資訊從業人員對於資訊證照認知上的程度高於資訊從業人員。

(四) 實質效益

在資訊證照可獲得之實質效益中，有顯著差異存在(t=-5.988，p<0.001)，非資訊從業人員(M=4.520)高於資訊從業人員(M=4.136)，可見非資訊從業人員對於「提升我對資訊專業的認同度」、「提升我對資訊專業上的自我肯定」、「提升工作成員對我的資訊專業信任度」，皆高於資訊從業人員，從此研究可了解，非資訊從業人員對於資訊證照認知上的程度高於資訊從業人員。

從以上結果可發現，非資訊從業人員對於社會支持、資訊證照認知、實質效益之程度皆大於資訊從業人員，只有專業能力程度小於資訊從業人員。

伍、結論與未來研究

5.1 研究結論

在全球化、競爭激烈的世代，高學歷不再是高薪就業的保證，資訊從業人員於職場轉換跑道時，若持有一張證照，對自己的專業能力除了可以提出有力「證明」外，相信也較容易從眾多求職者中脫穎而出；但非資訊從業人員若想進入資訊產業，則普遍認為擁有資訊證照即可證明其專業能力；惟隨著認證發放浮濫，在證照可信度強烈遭受質疑的情況下，有許多企業認為市場上的證照種類太多，已無法單從證照判斷一個人所具備的專業能力。據此，本研究以欲成為資訊從業人員及已是資訊從業人員者為對象，分別從社會支持對於資訊證照認知、專業能力對於資訊證照認知、資訊證照認知對於實質效益、資訊從業人員/非資訊從業人員在各構面之影響等 4 個角度切入，做出以下說明：

一、社會支持對於資訊證照認知之影響

根據本研究分析結果發現，整體而言，社會支持會正向影響資訊證照認知，但若改以資訊從業人員及非資訊從業人員之角度來看，則資訊從業人員對於周遭主管、同仁的關心、鼓勵，以及分享資訊證照準備的經驗，都會正向地影響其資訊證照認知；而非資訊從業人員卻在「社會支持對於資訊證照認知」方面未有顯著影響，可能是因為非資訊從業人員在尚未進入資訊領域之前，甚少接觸相關領域且具有相當程度之專業知識的從業人員給予較具建設性的關心和建議，故而無法立即感受到周遭主管、同仁所提供關於資訊證照方面的正向支持。

二、專業能力對於資訊證照認知之影響

這部分研究發現，專業能力對資訊證照認知並無顯著之影響，亦即專業能力的高低並不直接影響對資訊證照的認知程度。若從資訊從業人員及非資訊從業人員的角度剖析，可知資訊從業人員對於資訊專業訓練、資訊專業相關法令、資訊業務均能有一定程度了解及掌握，亦能根據不同客戶狀況，研判客戶可能發生的問題，並立即給予幫助，其所展現的專業知識、專業技能、專業態度都會正向地影響資訊證照認知；反之，非資訊從業人員在「專業能力對於資訊證照認知」方面則未見其顯著影響，可能係因非資訊從業人員目前急於進入資訊產業，對於專業能力與資訊證照考取，兩者間的關聯性之認知不夠全面也較不客觀，以致演變成欲從事資訊產業者僅以考取資訊相關證照為目標，而未將進入資訊產業後的職涯規劃一併列入考慮，忘卻考取資訊證照的本質是為了證明自己已具備進入該產業所需的基礎技術和專業知能。

三、資訊證照認知對於實質效益之影響

經過問卷調查及相關分析歸納後得出，已擁有資訊證照者認為既已具備足夠專業能量，更應正向地實現其所能帶來的實質效益，才不致枉費當初為了考取證照所下的苦功。另一方面，從資訊從業人員及非資訊從業人員的兩者的角度觀之，大致可獲得相同的結論，也就是說，加強資訊證照的認知，便可加強其往後的工作認同度、工作績效等實質效益，且根據統計數據顯示，對資訊從業人員之影響尚有大於非資訊從業人員的跡象！

四、資訊從業人員及非資訊從業人對各構面之影響

資訊及非資訊從業人員對於社會支持、專業能力、資訊證照認知及實質效益等各個構面，均呈現顯著影響結果，其中以影響程度來看，就社會支持、資訊證照認知及實質效益等方面，非資訊從業人員皆有高於資訊從業人員的趨勢；惟獨專業能力構面，資訊從業人員高於非資訊從業人員。由此可知，目前是否處於資訊產業中，對各構面而言均有一定程度的差異，以資訊從業人員而言，可能會因為公司文化、公司體制、工作環境及其所面對的客戶等外在因素，因長期處於有績效壓力及專案急迫性的職場環境下，而淡忘當初獲取資訊證照的初衷，肇致在社會支持、資訊證照認知及實質效益等三方面，均產生影響反低於非資訊從業人員的現象。

5.2 未來研究

一、本研究問卷範圍僅針對國內地區，惟問卷結果可能因國內外之國家文化、價值觀等不同而有所差異，後續建議可再針對國外地區實施問卷調查，以比較不同國家環境背景及觀念之差異。

二、由於現今社會變遷及網路發展快速，影響資訊證照認知因素除了社會支持、專業能力等構面外，可再加入社群影響、社會文化、價值觀、未來職涯等因素加以分析探討，以進一步了解影響資訊證照認知之其他原因所在。

三、本研究礙於時間及人力限制，無法個別就資訊專業證照加以分門別類做分析，建議後續可以依國內或國際資訊專業證照的種類逐項進行探討，以突顯個別資訊證照在資訊產業中獨一無二的人力資源養成價值。

參考文獻

中文部分

呂宇倫，2005年，我國壽險業從業人員對專業證照認知之研究-以本業與非本業證照探討，朝陽科技大學保險金融管理系碩士論文。

李育杰，2013年，資訊專業證照研析報告2013年度報告，教育部資訊軟體人才培育中程計畫。

林麗婷，2001年，國中公民與道德科教師經濟教育專業能力之研究-以高雄地區為例，國立台灣師範大學公民訓育研究所碩士論文。

林博文、徐志明，2001年，如何培養國際化知識創新能耐，科技發展政策報導，SR9009，頁680-688。

吳明燕，2014年，舞動人生：大臺北地區國小學童運動舞蹈參與動機與社會支持之研究。國立臺灣師範大學運動休閒與餐旅管理研究所碩士論文。

陳美伶，2007，軟體品質工程師證照的實質效益研究，國立臺灣科技大學資訊管理系碩士學位論文。

陳姿伶，2011年，析論專業能力與能力模型之建構，T&D飛訊第124期，頁1-4。

陳建陽，2005年，人格特質、知識管理認知、專業能力對工作績效影響之研究-以警察機關交通事故處理為例，南華大學管理科學研究所碩士論文。

張笠雲，1986年，社會變遷中各類社會支持系統功能的討論，行政院研究發展考核委員會：加強家庭促進桂會和諧學術研討會論文集。

康龍魁，1993年，追求另一張技職文憑：淺談商業類職業證照制度之現況與展望，技術及職業教育雙月刊，第17期，頁13。

黃心怡，2004年，對人力資本論的再省思：資訊技能訓練與資訊證照取得在勞動市場中的角色，資訊社會研究期刊，頁255-270。

黃同圳，2009年，改善證照制度提升臺灣競爭力，行政勞工委員會職訓局泰山職業訓練中心-訓練與研發期刊，頁24-29。

黃文風，2010年，資訊從業人員對資訊證照重要性認知及取得態度之研究，中華大學資訊管理學系碩士班碩士論文。

黃政傑，1985年，課程改革，臺北：漢文書店。

彭幸璇，2003年，知識型服務業推動技能管理及證照制度之研究-以經濟部 ITIS計畫為例，銘傳大學管理科學研究所碩士論文。

劉照金，1997年，我國運動教練指導人員證照制度之架構探討，國民體育季刊二十六卷第四期，頁22-28。

葉怡屏，2012年，金融從業人員應用知識管理對專業能力及知識效能關係之研究-以A銀行為例，國立高雄應用科技大學商務經營研究所碩士論文。

龔永宏，2004年，消防機關警及救護人員知識管理、專業能力與工作績效關係之研究，南華大學管理科學研究所碩士論文。

英文部份

Caplan, G. (1974). Support system and community mental health: Lectures on concept development. New York NY: Behavior Publication.

Chisholm, M. E. and Ely, D. P., (1976). Media Presonnel in Education: A Competency Approach. Englewood Cliffs, New York: Prentice-Hall.

Cutrona, C. E., & Russell, D. W. (1990). Type of social support and specific stress: Toward a theory of optimal mathching. *Social support: An interactional view*. New York NY: Wiley. 319-366.

Friedman, M.(1982).Capitalism and Freedom.Chicago:University of Chicago Press.

Herzberg, F., Mausner, B., & Synderman, B. S. (1959). The motivation to work. New York: Wiley & Sons, Inc.

Mina, P., Jessica, T. R., & Nancy, H. L. (2009). Perceived social support and domain-specific adjustment of children with emotional and behavioral difficulties. *Emotional and Behavioural Difficulties, 14*(3), 195-213.

Thoits, (1986). Social support as coping assistance, Journal of consulting and clinical psychology, 54(4), 416-423

國軍衛星通信系統性能提升之研究

李建鵬[a] 曾仁傑[b]

[a]國防大學管理學院

[b]國防大學海軍指參學院

摘要

天頻系統是國軍於 90 年代左右完成部署的衛星通信系統，它正面臨與所有通信系統相同的命運，雖設計時已將抗干擾能力、傳輸速率及天線自動追蹤等先進功能納入設計，但因通信服務的需求增加、更高的資料流量與更穩定的天線需求等，天頻系統已無法滿足客戶。通信容量飽和、系統效能不彰及因老舊導致裝備故障等問題在在證明了該系統已屆其壽限。因此，於 2012 年起國軍執行衛星通信系統性能提升專案以提升其效能，諸如:加大頻寬、提升資料流量、強化抗干擾能力及整合 C4ISR 運用等，旨在取代老舊系統，滿足國軍遠距通信需求。

本研究係經由文獻蒐集及問卷調查等客觀科學方式，完成國軍衛星通信系統性能提升作業之評估條件及層級架構，並以層級分析法將各專家之專業意見予以量化，以獲得各評估條件之權重及優先順序。研究目標係分析在執行國軍衛星通信系統性能提升作業過程中之關鍵成功因素，運用關鍵成功因素建構乙套決策模式，提供未來國軍在執行衛星通信系統性能提升作業時運用。

關鍵詞：衛星通信系統、性能提升、層級分析法

Performance Enhancement Study on Satellite Communication System of R.O.C. Armed Forces

Chien-Peng Lee[a] Jen-chieh Tzeng[b]

[a] National Defence Management College, National Defense University Taiwan,R.O.C.

[b] Navy Command and Staff College, National Defense University Taiwan, R.O.C.

Abstract

TIAN-PIN system, a Satellite communication system R.O.C. Armed Forces deployed since the 90s, is facing the same fate as all communication systems. Although that it was designed with advanced functions such as anti-jamming, high transmission rate and antenna automatic tracking, due to the increasing demand on more communication services, higher data rate and more reliable antennas, the TIAN- PIN can no longer keep up with the customer's requirement. Problems such as capacity saturation, lack of efficiency and equipment malfunctions caused by ageing have proved that it has reached its end of life cycle. Therefore, the R.O.C. Armed Forces have carried out a performance enhancement project on satellite communication system since 2012, to enhance the performance including larger bandwidth, higher data rate, to robust anti-jamming capability and to integrate C4ISR applications etc. This project is aiming to replace the out of date system and hopefully, to satisfy the R.O.C. Armed Forces' long range communication requirement.

This study has adopted objective scientific methods such as document collection and questionnaire inquiry. Assessment criteria and hierarchy architecture was drafted to aim at satellite communication system performance enhancement. By using Analytic Hierarchy Process（AHP）, professional opinions were quantified and criteria's weighting and priority were derived to support analysis of alternative assessment. The goal of this study is to analyze the critical successful factors in regard to the satellite communication system's performance enhancement project. Furthermore, to apply the critical successful factors to help developing strategic decision model. The R.O.C. Armed Force can benefit from this model in the future project to enhance the satellite communication system performance.

Keywords: Satellite Communication System, Performance Enhancement, Analytic Hierarchy Process（AHP）

壹、緒論

一、研究背景與動機

(一)研究背景

國軍天頻系統係於 90 年代陸續完成部署，平時為重要指管命令及情資傳遞輔助手段，戰時配合戰況快速機動部署，支援作戰指管需求；隨著「資訊戰」及「網狀化作戰」概念的興起，對高速、寬頻、大容量衛星通信網之運用需求也日益增加（如欲介接其它系統恐造成資源排擠），因此，針對通信容量飽和（頻寬不足），系統效能欠佳及相關裝備性能已不敷所需（含抗干擾能力、傳輸速率及天線自動追蹤能力）等問題，國軍已於 101 年起陸續執行相關裝備性能提升作業，俾強化抗干擾能力、提升傳輸速率及整合 C4ISR 運用。現階段在國軍衛星通信系統涵蓋範圍受限狀況下，僅能運用國際海事衛星通信系統（INMARSAT）彌補其涵蓋範圍不足之問題（如圖 1），原第 3 代國際航海衛星系統於 2016 年停止提供通信服務，故國軍已全面換裝為第 4 代國際航海衛星系統，另有關國際海事衛星通信系統係「國際海事衛星組織」於 1979 年成立後建置，旨在為海上船舶提供全球、全時、全天侯的海事衛星安全和商務通信服務，惟該組織已於 2005 年上市（民營化），因此，通信保密與安全之問題恐成為隱憂。

近年，國軍面對共軍跨區長航的力道，或釣魚臺、東海情勢變化，以及南海局勢波濤洶湧狀況下，海軍必須走出去，面向海洋、面對艱鉅的挑戰，而衛星通信絕對是海軍遠距通信不可或缺的手段，因此，惟有不斷提升國軍遠距通信能力，才能支撐國軍日益嚴峻的戰演訓任務。

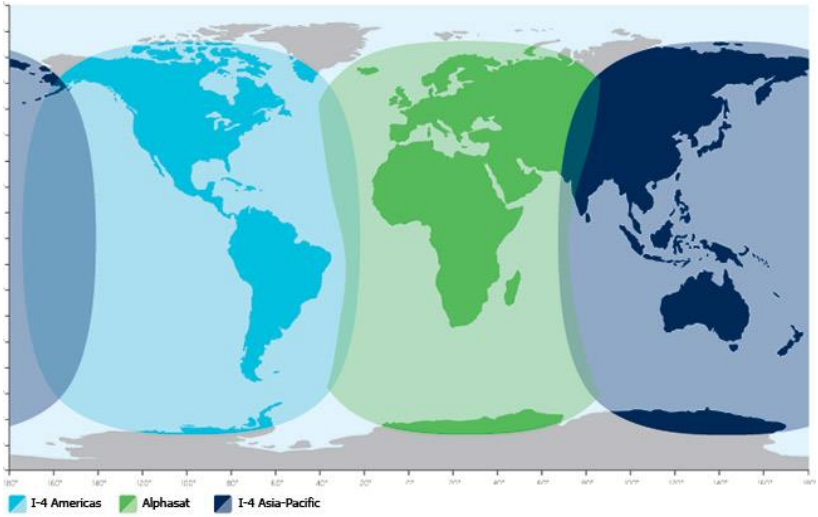


圖 1 INMARSAT 涵蓋範圍圖

資料來源：https://www.google.com.tw/search，檢索日期：2016 年 9 月 20 日。

(二)研究動機

筆者於近年執行衛星通信系統性能提升時，於作業層面發現諸多問題，簡述如下：

1.裝備適用性：國軍於規劃性能提升作業時，雖然欲換裝之裝備皆為現階段各國服勤中之裝備，惟衛星通信與大氣環境以及運用方式習習相關，故適用於其它國家之裝備，未必全然適合我國軍部隊使用，故於執行裝備性能提升時將面臨裝備適用性之問題，因此，在各單位執行裝備性能提升的同時，即須

根據突發狀況，變更裝備功能以適應我國作戰環境使用，故增加專案執行之困難與複雜度。

2.欠缺專業團隊：因專案管理之精神在於如期、如質、如預算執行，在現今制度面卻無擇優汰劣的機制，因此，只要專案管理團隊中之任一成員欠缺足夠專業抑或沒有使命感，即可能因為各層面環環相扣，致性能提升作業無法順利推行且增添更多變數，嚴重影響專案執行之進度，肇生外界疑慮。

3.整體功能不足：綜觀各種通信手段，衛星通信系統為國軍遠距通信之主要手段，相關系統儘管經過前述之性能提升作業，尚有許多功能尚待精進的地方，例如：網路頻寬不足、傳輸速率過低、抗干擾能力不足、整合無人飛行載具（UAV）及發展潛艦衛星通信能力等問題。

綜合以上面臨之問題，促使筆者研究如何有效執行衛星通信系統性能提升作業之關鍵成功因素，用以作為未來建案規劃參考，俾對現存問題之改善有所助益。

二、研究目的

(一)藉由蒐集各國衛星通信系統發展相關文獻及最新資料，以瞭解現今各國衛星通信系統發展趨勢，俾掌握未來衛星通信發展重點。

(二)依據歷年經驗及文獻歸納，分析國軍執行衛星通信系統性能提升之能力與限制。

(三)探討國軍執行衛星通信系統性能提升時，所需考量之評估準則，在層級分析法評選模式下，藉由專家問卷方式，構建關鍵成功因素之層級架構及分析其權重。

(四)依據本研究成果，提出影響國軍執行衛星通信系統性能提升作業之關鍵成功因素，作為國軍未來執行裝備性能提升作業時之參考。

貳、文獻探討

一、層級分析法

AHP(Analytic Hierarchy Process, AHP)是由美國賓州匹茲堡大學教授 Saaty 於 1971 年所發展出的一套決策方法，並於 1980 年整理成書，該分析法主要是在解決多準則決策問題，透過對複雜的問題進行切割、分類，使其分解為一樹枝狀的結構層級，研究者除了可以對問題的本質更為清晰外，也讓決策結果更加準確，例如呂政翰(2002)利用 AHP 建構 7 個構面與 15 個主要考量因素之層級架構，以得知衡量企業導入 ERP 可行性指標的相對重要性權重；陳旭雄(2007)以 AHP 分析 4 項物流引進 RFID 的主要關鍵因素之權重排序，以作為物流業在考慮是否導入 RFID 時之重要參考。

此方法係利用層級結構(Hierarchical Structure)的概念，協助研究者對事物的了 解。將一待解問題或系統依據其目標或焦點由上而下分解(Decomposition)成為多個層級及其元素。其後再根據某些基準進行評估，並依照所發展的步驟，來處理複雜的決策問題。然後再由下至上予以綜合(Synthesis)，而得到一整體性的解答（如圖 2 所示）。

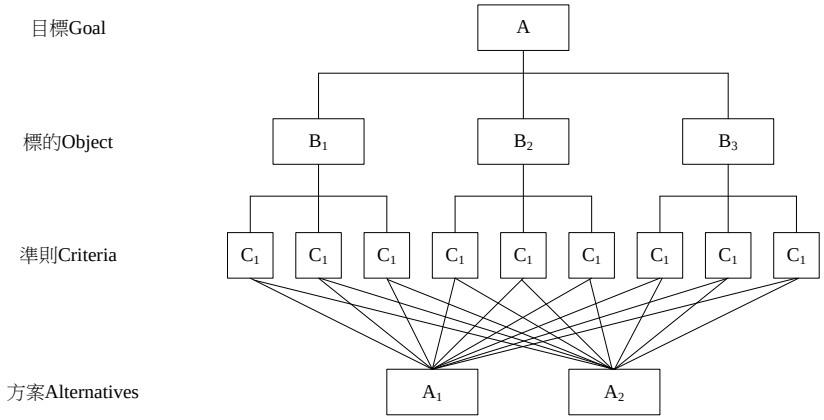


圖 2 AHP 層級架構示意圖

資料來源：曾國雄、鄧振源，1989

AHP 除了將問題及其間的關係圖像化以協助容易了解外，又能處理複雜的評估因素，尤以處理不具體因素(Intangible Factors)的影響。故 AHP 就是將複雜的問題予以系統化，並將問題的各個考慮層面予以層級化的架構，因為層級結構有助於決策者對於事物的整體了解，同時利用評估要素建構為層級形式，使工作易於達成。因此，Vargas (1990)認為層級式架構具有下列的優點：

(一)具有彈性：就彈性而言，若發生資料不足或遺漏部分資料時，可透過層級架構的模式彌補資料缺失，作適時的擴充或修改。

(二)易於瞭解：在層級架構中，各層級元素的優先順序是逐層演變的結果，可以清楚的觀察同一層元素間的彼此關係（具獨立性）及上下層元素間的彼此影響力。故在研究問題時，可利用此一關係來作元素間的分類或整合。

(三)合乎邏輯：層級架構是依層級程序逐步推演的，藉此將複雜的決策問題系統化成簡明的架構，使決策者在分析時可兼顧不同元素間的邏輯關係，對於決策的正確性具有正面之幫助。將問題描述建構成層級架構後，透過量化的判斷，找出脈絡後加以綜合評估決定替代方案的優先順序，以選擇最適當(或最佳)的方案，減少決策錯誤的發生機率。

AHP 在使用上，主要可分為兩個部分，分別是層級架構的建立與層級評估。在建立層級架構部分，研究者須對研究問題進行闡述，並列出要評估的要素和可供選擇的方案，進而得以建構整個層級架構。在層級評估部分，則是請專家對同層級要素進行兩兩評估，然後研究者除了進一步將評估結果轉換成同層級要素的相對權重外，研究者亦需對專家的評估結果進行邏輯診斷，以避免專家評估的結果不符邏輯。

二、衛星通信系統類型及運用

(一)衛星通信系統之類型：

1.依據人造衛星運行軌道距離地球高度的差異來判別，目前衛星通信系統主要分成三種類型：

(1)同步軌道（Geostationary Earth Orbit,GEO）衛星，其軌道高度約為36,000公里。

(2)中軌道（Medium Earth Orbit,MEO）衛星，軌道高度介於同步軌道衛星以及

低軌道衛星之間。

(3)低軌道（Low Earth Orbit,LEO）衛星，此類衛星通常存在於距離地表高度500-1500公里。

2.依據衛星通信系統的通道特徵及其傳輸環境區分為兩種類型：

(1)行動通道（mobile channel）：係指行動終端至衛星間建立的通訊鏈結。

(2)固定通道（fixed channel）：係指固定終端至衛星間建立的通訊鏈結。

3.導航衛星兼具衛星通信功能：「北斗二號」衛星導航系統具備四個主要功能：導航定位、測速、短信功能、授時功能。其中短信功能（民用版一次傳送49個漢字，軍用版120個漢字），是全球其它衛星導航系統所不具備的功能。

4.儲存-轉發通信方式的通信衛星：屬中、低軌道衛星通信系統，該衛星經過上空時，地面移動用戶可用掌上型發射機發送資料，衛星接收並存儲這些資料，到達地面接收站上空時再轉發下來。主要用來將駐守於國外之部隊和情報單位的資料傳送回國內。

(二)衛星通信系統的運用：

1.自主研發衛星通信設備：中新一號（ST-1）衛星於民國100年屆齡，中新二號衛星（ST-2）升空取代中新一號衛星。配合新衛星升空，同步精進地面衛星通信裝備及網路管理系統。

2.國際海事衛星系統第四代：此系統提供使用者，可攜帶至任何地方使用的衛星通訊，其運用包括語音、數據、傳真及影像等服務。

3.衛星通信系統使用頻段特性與運用：在衛星通信中，依使用頻率不同可概分為UHF、L、C、X、Ku、Ka等六種，載波頻率的選擇主要考慮，係在於須避開其它太空通訊和地面微波通訊的干擾。但是隨著衛星通訊業務的迅速增長，該頻段已不能滿足所需。目前衛星通訊的工作頻段已提高到20G至30GHz，並已開發研究40G至50GHz頻段。目前國軍所使用之中新二號衛星即為Ku頻段，而海軍又是國軍中擁有衛星通信站臺數量最多，且使用衛星通信頻率最頻繁的專業軍種。當我海軍軍艦執行任務時，如一般的通信裝備無法使用時（如HF、VHF、UHF等頻段通信裝備），衛星通信就成為唯一且不可或缺的通聯工具，惟衛星通信裝備在遇到惡劣環境及天侯時，極可能會發生通信品質不良甚至斷訊的狀況，因此，瞭解電磁波特性，依據戰場地理位置及大氣環境，選擇適當通信頻段，亦是確保衛星通信鏈路品質之關鍵成功因素。

三、衛星通信系統未來發展趨勢

(一)衛星通信應用於UAV的發展：

衛星通信具有廣域、寬頻、靈活及無瑕隙之通信特性，能達到通訊無死角、構連無縫隙及提升系統容量、提高資訊傳輸速率和確保通訊品質之獨特性，使其在軍民領域上皆有廣泛的應用。其中，衛星通信在UAV（Unmanned Aerial Vehicle,UAV）上之應用，可輕易解決UAV因微波通信距離短造成航程受到限制的難題。

衛星通信在UAV的應用主要有以下優點：

1.延伸作業距離：有效解決因微波通信造成距離的限制，衛星通信廣泛的涵蓋範圍，提升UAV的遠距操控能力。

2.提升大量且即時之訊息傳輸：在衛星通信提供的高頻寬下，可提供戰場上即時高畫質或高速率的傳輸品質。

因此，我國在未來UAV的發展上如能結合衛星通信技術，如美方之掠奪者及全球之鷹（如圖3），將可建立我國完全自主的空中監視偵測能力，有助不對稱作戰戰力之實現。

圖 3 RQ-1B 掠奪者及 Global Hawk 全球之鷹

資料來源：https://www.bing.com/images/search，檢索日期：2016年10月3日。

(二)寬頻衛星的發展：

經過多年研究發展，寬頻衛星通訊技術在整合無線通訊系統上的運用已相當純熟，尤其配合無線通信系統的演進和電子技術的進步，衛星通訊技術不斷朝向Ka頻段發展，並加強星載處理技術能力的提升，以提供更多通信容量與更高的傳輸速率。另衛星間通信鏈結則可能採用雷射通信技術，進一步提升通信容量外，還可以大幅降低敵方直接對衛星進行偵蒐與干擾之衝擊。

(三)星載處理之設計與發展：

星載處理目的是要提高衛星鏈路的性能及有效性，降低費用並增加通訊容量；進而增加整個網路的有效性和靈活性。星載處理的功能，除了信號放大和頻率轉換外，還包括：解調、檢錯、糾錯、轉換定址和控制資訊。它與信號再生和信號傳輸有關，包括資料的交換與定址、波束形成、資料緩衝和資料複用。

(四)激光通信的發展：

現階段數據傳輸量成指數級增長，對衛星通信容量和數據傳輸速率提出了更高的需求，而且近地軌道衛星通常需等待經過地面站上方的時機與地面交換數據信息，導致通信延遲，相較通信頻寬已達瓶頸的傳統射頻通信，空間激光通信具有高速即時性、高容量特性和保密穩定性等特點。將成為未來軍事和商業空間網絡的重要組成系統。

參、研究設計

本研究係針對國軍執行衛星通系統性能提升作業時，所需考量因素以層級分析法（Analytic Hierarchy Process,AHP）評估各項關鍵成功因素之權重，以建立乙套決策架

構，提供未來國軍執行衛星通信系統性能提升作業時運用。

一、衛星通信系統性能提升各項關鍵成功因素之探討

綜合國內外學者專家之意見，彙整出性能提升關鍵成功因素之主次準則，後續據此執行準則評估及權重分析，有關準則來源說明如后：

(一)通信安全性：

林澄芳於衛星通訊電子干擾與防制文中，提到有關衛星通信系統運用於數位戰場，將面對資訊戰及電子戰之威脅；資訊戰提及國防安全網路之侵入與破壞；至於電子戰則強調對於通信鏈路之攻擊。因此，假如衛星通信系統遭敵攻擊、破壞，將無法確保通信的安全，故將通信安全性納入主準則運用。

1.系統抗干擾能力：

林澄芳於衛星通訊電子干擾與防制文中，提及衛星通訊常用的干擾技術如寬頻雜波干擾、部分頻段干擾、掃頻干擾及多成音干擾等，因此，如何加強抗干擾能力，防範敵人的蓄意干擾更顯重要，以確保衛星通信系統的可用性，故將系統抗干擾能力納入次準則運用。

2.確保資訊安全：

李立等4員於衛星跳頻通信網路管理系統之研究中，提及為確保資訊安全，必須將所有經過衛星傳輸之信令及資料，經過加解密處理才能確保資訊的安全，故將確保資訊安全納入次準則運用。

3.提升系統妥善及通達率：

李立等4員於衛星跳頻通信網路管理系統之研究中，提及衛星通信已成為軍方通信之必然發展趨勢，我國亦積極投注大量研發能量於發展自製發射人造衛星，而提供衛星通信服務通達率高低，將成為決定衛星通信系統之關鍵成功因素，原因即在於無論衛星通信系統技術多先進，假如無法確保系統妥善與通達率，系統即喪失效用，因此，將提升系統妥善及通達率納入次準則運用。

(二)系統整合性：

Terry Neumann於“Plotting the Future of Maritime Mobility“文中表示，隨著使用者需求不斷增加，而衛星在資源有限狀況下，下一代的衛星通信系統將會以整合C-、Ku-及Ka-等頻段之波束，並運用頻率重複使用之技術，以優化衛星系統效能，滿足使用者需求。而如何整合不同頻段之衛星通信系統更形重要，因此，將系統整合性列入主準則運用。

1.整合C4ISR各系統能力：

張新征於美國陸軍戰術資訊網絡建設的最新進展與編配運用研究中，說明WIN-T是美國陸軍的戰術網絡，它讓部隊更加機動化，使其能擺脫對固定通信設施的依賴，對於陸軍具有革命性的意義，因此，WIN-T系統將形成天、空、地相結合的全域性動態資訊網路架構，足見衛星通信整合C4ISR之重要性，故將整合C4ISR各系統能力納入次準則運用。

2.專案管理執行能力：

Harold Kerzner於「專案管理」乙書中提到，早在第二次世界大戰後，美國國防部便不再運用傳統的「柵欄範圍」的方式來管理專案，如對B52轟炸機、民兵洲際彈道導彈，以及北斗星潛艇等專案的管理。政府需要的是，對專案的所有階段負全責的專案經理。此書作者更以航空航太與國防工業中的專案為例，認為對於持續十年甚至二十年的專案來說，對其技術發展的預測是極其困難的。而衛星通訊需要確保鏈路的持續與穩定性，因此需要針對通訊架構執行通訊鏈路品質分析，乃至於執行系統規劃、設計籌建、技術開發及裝備安裝組測等，均有賴專案管理團隊應用其知識執行整合工作。足見專案管理執行能力的重要性，因此，將專案管理執行能力納入次準則運用。

3.整合各衛星系統提高通達範圍（高覆蓋率）:

Terry Neumann於“Plotting the Future of Maritime Mobility“文中表示，為了滿足使用者的需求，提供涵蓋全球之衛星通信系統是必然的，如此，方能提供全球的通信服務。而提供全球的衛星通信能力，勢必要有涵蓋全球之波束涵蓋範圍始能達成，因此，將整合各衛星系統提高通達範圍（高覆蓋率）列入次準則運用。

(三)系統成長性：

張新征於美國陸軍戰術資訊網絡建設的最新進展與編配運用研究中，說明WIN-T系統大量使用衛星通信，使資訊傳輸能力大幅提升，可有效支援語音，即時視訊和資料傳輸；因此，將系統成長性列為主準則運用。

1.提升通信容量：

常麗萍在商業通信衛星市場發展趨勢淺析文中，表示高通量衛星是現在衛星工業的重要發展趨勢。高通量衛星透過頻率重複使用和點波束來滿足日益增長的頻寬需求。因此，將提升通信容量納入次準則運用。

2.提高傳輸速率：

林高洲於寬頻衛星通訊系統之運用與展望文中表示，為滿足無縫隙、高彈性運用需求，寬頻衛星通信系統已日漸受到重視，因衛星通訊是達成通訊無死角及構連無縫隙之通信手段，因其系統容量的增加始能滿足高資訊傳輸速率的需求，以確保資訊快速傳遞。因此，將提高傳輸速率納入次準則運用。

(四)國防自主性：

國防部編撰之中華民國104年國防報告書中，於科技發展成效內表示，國防科技發展依「創新/不對稱」思維，及「科技先導、資電優勢、聯合截擊、國土防衛」建軍指導，發展符合聯合作戰需求之近、中、遠程國防科技，置重點於受國際輸出限制之關鍵技術，以達成國防自主與支援建軍備戰之目標。正因國防自主之重要性，故將國防自主性納入主準則運用。

1.開發關鍵技術能力：

黃忠良等4員於無人飛行載具(UAV)衛星通信簡介乙文中，提到有關美國的「掠奪者」(Predator)無人飛行載具系統採用Ku頻段衛星中繼數據鏈，其偵察資訊傳輸速率可達1.544Mbps，作用距離達900至3700公里，續航時間40

小時。因此，我國如果開發此項關鍵技術，將有助不對稱作戰戰力之實現。故將開發關鍵技術能力納入次準則運用。

2.掌握系統主控權：

羅春秋於中共「北斗」導航衛星發展及其軍事戰略意涵乙文中提到，目前共軍雖可使用美國的GPS、俄羅斯的「格洛納斯」系統，以及建構中歐盟的伽利略系統，依然不斷發展自已的北斗衛星導航系統。因為合理而言，在戰時或發生衝突與爭議時，禁止或拒絕別的國家使用其自身的系統是可以預期的結果。而以世界上使用率最為普及的GPS系統來說，儘管美國將其開放民間使用，但是本質上仍是美國軍用系統，可能限制甚至禁止中共使用。因此，惟有掌控了系統的主控權，擁有獨立自主發展的北斗導航衛星系統，才能夠擺脫對其他衛星導航定位系統的依賴。故將掌握系統主控權納入次準則運用。

3.軍民科技及資源整合能力：

李宗孝於中共衛星發展對我防衛作戰之影響及因應作為研究中，針對因應中共衛星發展具體作為之建議，提及航太科技在未來戰爭中將扮演關鍵角色，因此，現階段應該成立專責機構（如中共之航太科技集團），積極整合國內相關軍、公、民營太空衛星發展，做長遠並且是整體性之規劃，研擬未來我國衛星發展的具體可行作法，才能建立可恃之戰力，因此，將軍民科技及資源整合能力納入次準則運用。

二、層級架構建立及問卷設計

本階段是將文獻探討發展出之初步主、次準則，設計成專家訪談問卷，針對執行衛星通信系統性能提升作業相關之專家發出調查問卷，彙整專家意見後，確立國軍衛星通信系統性能提升評估要素之層級架構。

(一)準則歸納

依據學者對衛星通信系統之研究文獻與資料，彙整衛星通信系統性能提升之關鍵成功因素，初步擬出影響執行國軍衛星通信系統性能提升之四大主準則及十一個次準則，其中通信安全性主準則，有三項因素；系統整合性主準測，有三項因素；系統成長性主準則，有二項因素；國防自主性主準則，有三項因素。

後續將以專家問卷方式修正影響「國軍衛星通信系統性能提升之研究」主次準則要項，進而確認本研究之層級架構。

(二)專家問卷彙整結果：

本研究之主準則及次準則經由專家問卷調查表，綜整各領域專家意見及建議，彙整如后：

1.中科院資通所所長林高洲博士建議事項摘述如后：

(1)林博士認為衛星通信系統係結合各類型的終端設備使用，故管理這些終端之網管技術亦十分重要，始能發揮該通信系統之效益，建議於主準則「系統整合性」內新增兩項次準則「網路管理能力」及「各類型終端整合能力」。

(2)在提升整合衛星通信系統成長的同時，如何維持系統的妥善乃須一併兼顧之

議題，林博士認為將主準則「通信安全性」內之次準則「提升系統妥善及通達率」，移至主準則「系統成長性」下較為合理。

2.中科院天頻計畫主持人謝全益博士建議事項摘述如后：

(1)通常系統安全性主要包括傳輸安全（抗干擾能力）、通信安全（加/解密能力）、資訊安全（資訊存取之認證能力）等三項要求，故建議將主準則名稱「通信安全性」修訂為「系統安全性」，並於次準則中新增一項「保密安全」（或通信安全）。

(2)主準則「系統整合性」內次準則「提高系統通達範圍（高覆蓋率）能力」部分，謝博士認為國軍現階段使用之衛星通信系統覆蓋率不足，未來仍具成長性，建議將此項次準則置於「系統成長性」較為恰當。

(3)考量國軍衛星通信目前狀況，認為未來衛星通信系統尚有許多成長空間，故建議於主準則「系統成長性」內增加二項次準則，分別為「提升系統妥善及通達率」及「提高系統通達範圍」。

3.中科院天頻計畫副主持人黃忠良上校建議事項摘述如后：

(1)考量衛星通信系統在面對資訊戰及電子戰之威脅，該通信手段可能遭受偽造、竄改與截取，其通信安全至關重要；故建議於主準則「系統安全性」內新增一項次準則「通信安全」。

(2)建議於主準則「系統整合性」內新增一項次準則「網路管理能力」，黃上校認為在衛星通信的領域內要執行系統整合工作，其網管能力扮演相當重要之角色，因為，網管系統相當於整個系統之中樞，如欠缺完善之網管系統，將無法發揮系統應有之效能。

4.中華電信公司衛星事業處黃賢杰科長表示，建議於主準則「通信安全性」內新增一項次準則「多系統備援機制」；因為，中華電信公司在與日本電信界交流之過程，其發現日本政府，為了應付各種突發之狀況，針對通信的手段係採取多重備援機制，例如運用骨幹光纖、微波及衛星等，執行多系統備援作業，以應付各種可能的突發狀況。

經彙整專家意見後重新修訂影響國軍衛星通信系統性能提升之關鍵成功因素，計有四大主準則及十五個次準則，其中系統安全性主準則，有四項因素；系統整合性主準測，有四項因素；系統成長性主準則，有四項因素；國防自主性主準則，有三項因素；故「國軍衛星通信系統性能提升之研究」關鍵成功因素評估之層級架構已確立（如圖4）。

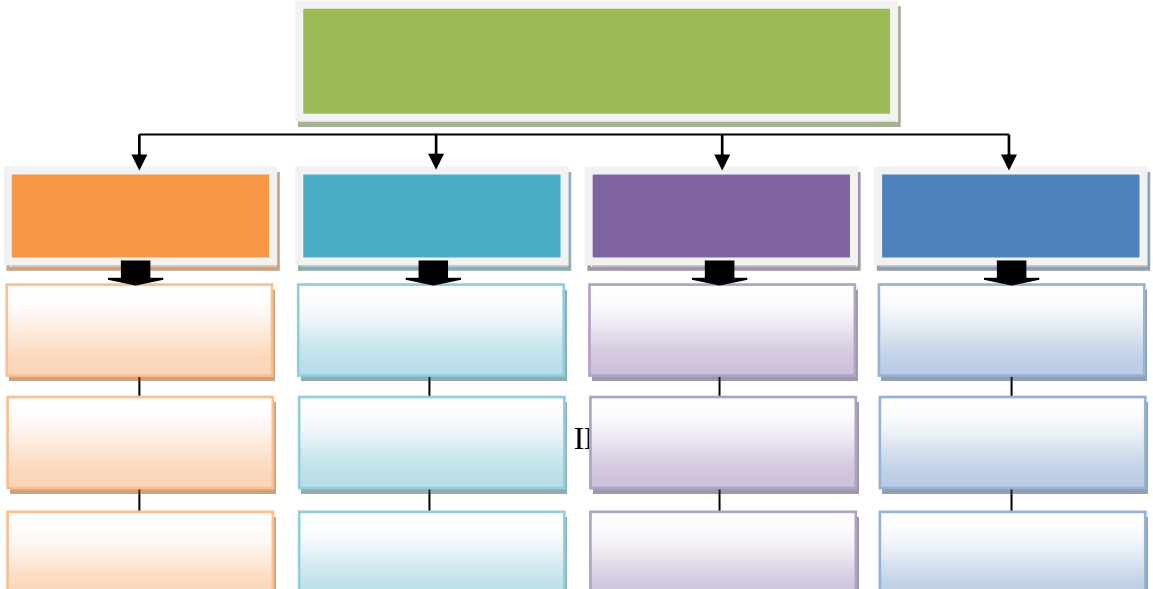


圖4 國軍衛星通信系統性能提升關鍵成功因素之層級架構圖

(三)AHP層級分析問卷設計

本階段是根據第一階段問卷結果所建立之AHP層級分析架構，利用AHP分析方法設計問卷，進行層級各影響因素之間兩兩比較，目的在求得建置評估之主準則優序及次準則權重的相對重要性。

本次AHP問卷於105年11月20日至12月15日以透過親自送達、e-mail寄達及回收方式進行，共送達30份，後續將回收之AHP問卷統計結果實施分析作業。

四、研究結果分析

依據前述的文獻探討整理及專家問卷方式，分析「國軍衛星通信系統性能提升」之關鍵成功因素，將其整理為本研究之權重問卷調查表，並以此針對國防部、司令部層級、中科院天頻計畫及中華電信公司衛星事業處等單位，從事衛星通信系統性能提升作業具實務經驗之專業人員進行問卷調查。經由問卷調查所得結果，使用以 Expert Choice 11 版軟體加以分析，以求得各影響因素之優先權重；並依受訪者職務屬性區分決策階層、管理階層及執行階層等類別，分析其對本研究之看法，並將所有專家的意見加以整合分析，期望能夠歸納出影響「國軍衛星通信系統性能提升」之關鍵成功因素。

一、問卷調查資料分析

本次 AHP 問卷調查表於民國 105 年 11 月 20 日至 105 年 12 月 15 日，針對 30 位專家實施填答，其中依受訪者職務屬性區分為決策階層(國防部 6 員)、管理階層（各軍種司令部 7 員）及執行階層(包含中科院及中華電信公司等 17 員)以透過親自送達及 e-mail 寄達、回收方式進行，共送達 30 份，回收 30 份，回收率為 100%，繼之將依問卷調查所得結果，以 Expert Choice 11 版軟體檢測其一致性。經實證檢驗得無效問卷 4 份，有效問卷 26 份(如表 1)，分析結果分述如下：

(一)決策階層問卷調查資料分析：

1.主準則優序權重分析結果：

各主準則優先權重順序依次為「系統安全性」0.462、「系統成長性」0.222、「國防自主性」0.162、「系統整合性」0.154，代表決策階層專家多數認為「系統安全性」相較其它三項主準則，應列為評估國軍衛星通信系統性能提升之關鍵成功因素時所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「通信安全」0.170、「確保資訊安全」0.133、

「系統抗干擾能力」0.107，代表專家多數認為在主準則「系統安全性」下之「通信安全」相較其他次準則，應列為評估國軍衛星通信系統性能提升關鍵成功因素時所應考量之首要因素。

(二)管理階層問卷調查資料分析：

1.主準則優序權重分析結果：

各主準則優先權重順序依次為「系統安全性」0.434、「國防自主性」0.274、「系統成長性」0.168、「系統整合性」0.124，代表管理階層專家多數認為「系統安全性」相較其它三項主準則，應列為評估國軍衛星通信系統性能提升關鍵成功因素時所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「通信安全」0.218、「掌握衛星（系統）主控權」0.137、「系統抗干擾能力」0.086，代表專家多數認為在主準則「系統安全性」下之「通信安全」相較其他次準則，應列為評估國軍衛星通信系統性能提升關鍵成功因素時所應考量之首要因素。

(三)執行階層問卷調查資料分析：

1.主準則優序權重分析結果：

各主準則優先權重順序依次為「國防自主性」0.419、「系統安全性」0.377、「系統成長性」0.106、「系統整合性」0.098，代表執行階層專家多數認為「國防自主性」相較其它三項主準則，應列為評估國軍衛星通信系統性能提升關鍵成功因素時所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「掌握衛星（系統）主控權」0.189、「通信安全」0.170、「確保資訊安全」0.117，代表專家多數認為在主準則「國防自主性」下之「掌握衛星（系統）主控權」相較其他次準則，應列為評估國軍衛星通信系統性能提升關鍵成功因素時所應考量之首要因素。

(四)整體問卷調查資料分析：

1.主準則優序權重分析結果：

各主準則優先權重順序依次為「系統安全性」0.424、「國防自主性」0.310、「系統成長性」0.147、「系統整合性」0.120，代表各階層專家多數認為「系統安全性」相較其它三項主準則，應列為評估國軍衛星通信系統性能提升關鍵成功因素時所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「通信安全」0.188、「掌握衛星（系統）主控權」0.137、「確保資訊安全」0.106，代表專家多數認為在主準則「系統安全性」下之「通信安全」相較其他次準則，應列為評估國軍衛星通信系統性能提升關鍵成功因素時所應考量之首要因素。

表 1 一致性檢測結果統計表

問卷編號	以 Expert Choice 檢測之 I.R. (Inconsistency Ratio)值	採用

	主準則	次準則一	次準則二	次準則三	次準則四	
P0	0.04	0.08	0.02	0.02	0.00	V
P2	0.08	0.10	0.00	0.04	0.05	V
P3	0.02	0.04	0.00	0.04	0.02	V
P4	0.02	0.03	0.02	0.05	0.02	V
P5	0.09	0.02	0.07	0.03	0.04	V
P6	0.07	0.10	0.03	0.03	0.04	V
P7	0.10	0.05	0.04	0.02	0.02	V
P8	0.05	0.03	0.02	0.02	0.09	V
P9	0.10	0.05	0.07	0.05	0.00	V
P10	0.05	0.01	0.04	0.01	0.00	V
P11	0,02	0.07	0.03	00.05	0.05	V
P12	0.05	0.04	0.01	0.04	0.01	V
P13	0.07	0.06	0.02	0.00	0.04	V
P14	0.02	0.01	0.03	0.02	0.04	V
P15	0.02	0.05	0.02	0.03	0.05	V
P16	0.01	0.01	0.02	0.02	0.01	V
P17	0.03	0.01	0.02	0.01	0.02	V
P18	0.04	0.01	0.01	0.03	0.05	V
P19	0.10	0.00	0.03	0.04	0.05	V
P20	0.05	0.00	0.02	0.03	0.07	V
P21	0.04	0.05	0.01	0.04	0.08	V
P22	0.02	0.02	0.02	0.04	0.08	V
P23	0.06	0.02	0.03	0.03	0.04	V
P24	0.02	0.01	0.03	0.04	0.02	V
P25	0.05	0.02	0.00	0.03	0.04	V
P26	0.01	0.04	0.01	0.10	0.03	V
P27	0.35	0.41	0.42	0.41	0.53	X
P28	0.26	0.39	0.36	0.17	0.42	X
P29	0.19	0.10	0.22	0.38	0.47	X
P30	0.22	0.19	0.20	0.36	0.48	X

二、綜合分析（如表 2）

(一)主準則分析：

「系統安全性」為整體評選結果較優先考量者。所謂系統安全係指使系統免於發生災害及風險，並透過系統安全工程及管理之技術與分析方法，儘量於危害發生前找出危害因子，同時採取預防作為，以使風險降至最低程度，確保系統處於合理的安全環境。

分析系統安全性最後獲評選為相對重要準則之原因，可由系統安全性涵蓋「系統抗干擾能力」、「確保資訊安全」、「多系統備援機制」及「通信安全」等4項次準則，瞭解其包含了諸多面向，諸如衛星通信系統資訊傳輸安全、資料加解密能力、保密安全及資訊存取之認證能力等，均屬於系統安全之範圍；因此，學者專家認為當執行衛星通信系統性能提升作業時，相較於「國防自主性」、「系統成長性」及「系統整合性」等三項主準則而言，須優先考量系統安全性，以確保建立強韌、抗干擾之衛星鏈路。

(二)「系統安全性」次準則分析：

「通信安全」為整體評選結果較優先考量者；所謂通信安全包含通信與作業管理、存取控制及更新程序等，其內涵是確保通信時，衛星通信系統所傳遞的情資避免遭受敵方截收、通信的內容不為敵方偽冒及頻寬資源不被惡意盜用等。

而國軍長久以來，本、外島有無線電通信係以海底、地面光纖及空中微波系統為主，前者易遭人為及地震破壞，後者易受天侯影響，造成通信中斷，故多數專家均認為須建立以衛星通信為主之備援接替系統，以提供多重路徑之路由，增加通資系統之戰場存活率，才能確保通信安全。

(三)「系統整合性」次準則分析：

「系統（介面）整合能力」為整體評選結果較優先考量者；因國軍執行衛星通信系統性能提升作業時，須整合之系統相當的多，例如船位自動回報系統、寰網系統、大成系統及迅安系統等，因此，多數專家學者普遍認為衛星通信系統與其它系統之整合能力相當重要，因為，假如指管系統無法整合衛星通信系統使用，國軍的兵力一旦脫離指管系統本身通信機之涵蓋範圍（其它無線電通信手段之有效通達距離），其指管系統將喪失其功能，故惟有整合相關之系統才能確保國軍指管能力及發揮衛星通信系統最大投資效益，而專家評選結果亦證實了系統（介面）整合能力，在整個衛星通信系統性能提升規劃作業階段乃至於建案執行階段之重要性。

(四)「系統成長性」次準則分析：

「提高系統通達及波束涵蓋範圍能力」為整體評選結果較優先考量者，分析其原因係現用的無線電通信裝備，易受地形、地物影響，產生通信盲區，且通信距離亦受限制；因此，惟有衛星通信系統具備安全、強韌、抗干擾之資訊處理能力，可不受地形、地物、通信盲區限制，如國軍平時執行南巡護漁、遠至菲律賓、帛琉賑災之慈航任務，或是國內發生災情時，執行救災任務（如蘇迪勒颱風、水災及搜救等任務），還有年度的敦睦遠航任務，均可藉由衛星通信系統無遠弗界之特性來滿足超視距通信需求；此外，隨著科技的進步，衛星天線技術的提升，使得其輻射波束（footprint）比起從前更能適當的涵蓋所需通信之地區，以有效支援作戰任務遂行。因此，提高系統通達及波束涵蓋範圍能力在國軍執行衛星通信系統性能提升作業中，獲得各位專家評選為相對重要之準則。

(五)「國防自主性」次準則分析：

「掌握衛星（系統）主控權」為整體評選結果較優先考量者，分析其原因，可從「1996年臺灣海峽局勢緊張時，中國軍隊展開了一次大規模軍事演習，在關鍵時刻發現導彈無法正常追蹤，調查結果顯示為美軍將GPS訊號關閉所致。」這一事件，不但讓中共體認到建立自主衛星導航系統之重要，亦讓我國體認到國防自主之重要性。

再者，因現階段國軍使用之衛星通信系統，如國際海事衛星通信系統及自主建置之衛星通信系統，其資料之傳遞（包含語音、視訊、數據、傳真、廣播及多媒體情資等），均需透過網管中心（地面投落點）執行資訊轉發作業，所以衛星通信系統之網管中心絕對有能力掌握用戶傳遞之資訊，儘管訊息均已經由保密器執行資料加解密作業，但是，這些經過加密的訊息仍存在遭破密之風險。

(六)各次準則整體優先順序權重：

各項次準則整體評選結果，優先權重順序前三項依次為「通信安全」、「掌握衛星（系統）主控權」及「確保資訊安全」等三項。

從分析結果我們可以瞭解到，參與評選之專家學者認為「通信安全」、「掌握衛星（系統）主控權」及「確保資訊安全」等三項，在國軍執行衛星通信系統性能提升作業時，相較於其它次準則重要，歸納原因如后：

1.通信安全：選擇方案須考量衛星通信系統擔負戰備任務時，所傳遞的情資須達到避免遭受敵方截收、通信內容不為敵方偽冒、資源不被惡意盜用及其資料加解密能力等，惟有如此，才能確保衛星通信手段可有效支援國軍作戰任務。

2.掌握衛星（系統）主控權：所建置地面站臺之裝備及系統，須將掌握主控權乙事納入考量，惟有掌握系統的主控權，才能確保戰時可運用衛星通信系統支援指管系統提供部隊共同作戰圖像，確保指管通信。

3.確保資訊安全：現階段建置的衛星通信系統，均採用網路基礎（IP-Based）架構介面，考量其所傳遞資訊之機敏性，必須確保資訊不可遭竊取、竄改、損毀或破壞；而所謂資訊安全包含了資料傳遞的安全管理（如使用者憑證卡）、資料處理系統安全（如駭客攻防、稽核管理）及確保資料安全的機制（如管理機制、安全認證）等；簡言之，就是於性能提升方案選擇時，須針對資訊安全的諸多面向一併納入考量。

表 2 各階層綜合分析結果總表

分類	項目	決策		管理		執行		總體評選	
		權值	排序	權值	排序	權值	排序	權值	排序
主準則	系統安全性	0.462	1	0.434	1	0.377	2	0.424	1
	系統整合性	0.154	4	0.124	4	0.098	4	0.120	4
	系統成長性	0.222	2	0.168	3	0.106	3	0.147	3
	國防自主性	0.162	3	0.274	2	0.419	1	0.310	2
次準則	系統抗干擾能力	0.107	3	0.086	3	0.069	6	0.086	4
	確保資訊安全	0.133	2	0.062	6	0.117	3	0.106	3
	多系統備援機制	0.071	6	0.051	9	0.084	4	0.074	5
	通信安全	0.170	1	0.218	1	0.170	2	0.188	1
	系統（介面）整合能力	0.057	8	0.049	10	0.044	9	0.053	7
	專案管理執行能力	0.051	9	0.062	6	0.020	14	0.037	12
	各類型終端整合能力	0.020	14	0.015	14	0.021	13	0.021	14
	網路管理能力	0.046	11	0.023	12	0.022	12	0.029	13
	提升通信容量	0.034	12	0.015	14	0.018	15	0.021	14
	提高傳輸速率	0.076	5	0.019	13	0.040	10	0.039	11
	提升系統妥善及通達率	0.049	10	0.053	8	0.046	8	0.050	9
	提高系統通達及波束涵蓋範圍能力	0.082	4	0.084	4	0.048	7	0.065	6
	開發關鍵技術能力	0.028	13	0.044	11	0.072	5	0.052	8
	掌握衛星（系統）主控權	0.060	7	0.137	2	0.189	1	0.137	2
	軍民科技及資源整合能力	0.016	15	0.082	5	0.040	10	0.040	10

伍、結論

一、建立衛星通信系統性能提升決策模式實屬必要：

國軍於執行衛星通信系統性能提升換裝作業，所需預算動輒數十億元，因此，往往成為有心人士覬覦的目標，而執行方案如果又無有效之量化分析做支撐，更容易受到外界（如審計部、立法院或是監察院）質疑；所以，在確認國軍作戰需求後，國軍衛星通信系統性能提升作業之建案承辦人在執行系統分析作業時，即須執行量化及非量化的分析，而針對量化分析部分，現階段國內因尚未建立一套決策模式可供運用，故對於國軍而言，執行衛星通信系統性能提升作業存在相當高之風險；因此，本次研究建立之衛星

通信系統性能提升方案選用之決策模式絕對有其必要性。

二、本研究建立之整體決策層級架構具可用性：

(一)綜合上述結果，研究得出各專家一致性看法，且決策模式中之各項主次準則均屬合理，與國軍衛星通信系統性能提升作業之事實相符；可作為國軍建案承辦單位於未來執行選擇方案分析時，瞭解達成性能提升作業之關鍵成功因素，以期建置乙套符合國軍作戰需求之衛星通信系統。

(二)研究分析國軍各階層執行衛星通信系統性能提升之意見，建立了整體決策層級架構（模式），可作為後續建案作業之參考；惟決策模式中之主次準則，是否須根據選擇方案之不同而作適當之調整部分，可再予深入探討及研究，值得我們作為持續研究衛星通信系統性能提升關鍵成功因素的參考方向。

三、建議事項：

(一)未來國軍可運用決策模式優化衛星通信系統性能提升作業：

世界各國衛星通信發展的趨勢，均朝向 Ka 寬頻通信衛星發展，我國亦不例外，有關 Ka 寬頻通信衛星之發展，係屬中、長期目標，而本研究已針對國軍現用之 Ku 頻段衛星通信系統實施分析，一旦國家衛星政策發展確認，即可能馬上啟動一個長達 10 年的 Ka 頻段衛星通信系統建案作業，故建議可運用本決策模式選擇衛星通信系統性能提升作業之最佳執行方案，可彌補現行無決策模式可用之缺口，期提升系統性能以滿足作戰需求。

(二)持續挹注國防資源提升衛星通信技術能量：

1.近年來，衛星通信技術及系統發展迅速，無論是從經濟或軍事角度來看，現代化衛星通信具有無遠弗屆的大範圍通信覆蓋率之傳輸特性，正扮演著掌握戰場資訊、加快作戰節奏的關鍵角色，在現今眾多通訊技術中是無可取代的。在現今各科技強國愈來愈重視衛星通信技術情形下，科技實力一向不遜色的我國也應該重視這個領域的技術發展，以備不時之需。

2.「無科技即無國防」，縱使面對中共與日俱增的太空科技優勢與我國防資源不足的劣勢，我國仍應持續投注資源於自主衛星通信系統科技研究方面，並妥善運用、整合政府與民間相關科研資源，積極強化與累積衛星通信關鍵技術，必能有效提升國軍自主之衛星通信能力，以符未來建軍備戰所需，期有效厚植國軍戰力，確保國家安全。

參考文獻

李勝義，黃雯禧，2012。「中共太空衛星科技的發展現況與趨勢探討」，國防雜誌第 27 卷第 4 期。

李澤漢，「自主軍事微衛星與小型載具之發展策略」，新新季刊第 36 卷第 4 期。

李立・陳文傑・羅浩綸・王中期（民 104），「衛星跳頻通信網路管理系統之研究」，新新季刊第 43 卷第 3 期。

李宗孝 2004。「中共衛星發展對我防衛作戰之影響及因應作為研究」，國防雜誌第十九卷第九期。

李貴發，2011。「淺談太空作戰及臺灣因應之道－下」，尖端科技第 320 期。

李雲治，2015。「探究中共北斗衛星導航系統之發展、效益與影響」，中華戰略學刊。

吳勤，2008。「透視俄羅斯軍用衛星發展現狀」，現代軍事。
吳岳峻・楊銘駿・李玠昆・黃忠良，2013。「無人飛行載具(UAV)衛星通信簡介」，新新季刊第 41 卷第 4 期。
林進豐，2007。「行動衛星通訊」。五南，台北市。
林高洲，2006。「國防寬頻衛星通信技術展望與設計考量」，新新季刊第 34 卷第 4 期。
林高洲，「寬頻衛星通訊系統之運用與展望」，IECQ 報導第 46 期。
林澄芳，2007。「衛星通訊電子干擾與防制」，新新季刊第卅五卷第三期。
林志章，2015。「建構網路戰部隊能力評估指標之研究」，國防大學海軍指揮參謀學院正規班/軍事專題研究。
林東清，2008。「資訊管理-e 化企業的核心競爭能力」。智勝文化，臺北。
柯正和，2014。「國軍新一代行動衛星通信車」，新新季利第 42 卷第 1 期。
洪健藏，2003。「微波或衛星通信頻段之防雨衰對策研究」，國防通信電子及資訊季刊。
星輝，2008。「在無人機上加裝衛星通信系統豐重要性」，國際航空雜誌（International Aviation）。
時先文，「有時無人（UAV）勝有人-未來戰爭趨勢」，空軍學術雙月刊第 622 期。
宿東，2016。「“長征“箭又起“北斗“再升空」，中國航天。
陳克任，1999。「衛星通訊 NII 主角」。儒林，台北市。
黃雯禧，2012。「中共太空衛星科技的發展現況與趨勢探討」，國防雜誌第 27 卷第 4 期。
黃志文，2007。「小型衛星的發展與運用」，IECQ 報導第 51 期。
張新征，2016。「美國陸軍戰術資訊網絡建設的最新進展與編配運用研究」，現代軍事。
常麗萍，2016。「商業通信衛星市場發展趨勢淺析」，中國航天。
國防部，2015。〈中華民國 104 年國防報告書〉，2015 年 10 月。
黃志文，謝全益，蔡燈城，2010。「軍用衛星通信發展現況與趨勢」，新新季刊第 38 卷第 4 期。
湯福昌，2010。「中共衛星發展之研析」，陸軍學術雙月刊第 46 卷第 511 期。
賈平，李輝，2016。「從 EDRS 看國外空間激光通信發展」，中國航天。
鄧振源，曾國雄，1989。「層級分析法（AHP）的內涵特性與應用（上）」，中國統計學報第 27 卷第 6 期，頁 13707-13724。
鄧振源，曾國雄，1989。「層級分析法（AHP）的內涵特性與應用（下）」，中國統計學報第 27 卷第 7 期，頁 13767-13870。
劉啟文，2008。「中共發展北斗衛星對我之影響與因應之道」，國防雜誌第 23 卷第 6 期。
維基百科，2016。國際海事衛星組織，下載於 https://zh.wikipedia.org/zh-tw/(2016 年 9 月 27 日)。
維基百科網，2016。〈人造衛星〉，下載於 https://zh.wikipedia.org/zh-tw/(105 年 10 月 7 日)。
蔡和順，2008。「中共衛星發展對我地面防衛作戰威脅」，陸軍學術雙月刊第 44 卷第 498 期。
賴俊池，2012。「通信衛星設備概論」，新新季刊第 40 卷第 1 期。
應紹基，2014。「中共北斗衛星導航系統的研建歷程與面對的挑戰」，海軍學術雙月刊第 48 卷第 4 期。
羅春秋，2014。〈中共「北斗」導航衛星發展及其軍事戰略意涵〉，國防雜誌第 29 卷第 6 期。
Claude Rousseau & Jose Del Rosario,Senior Analyst,2012.NSR,“Asia:The Next Hub of Government and Military SatcomMarkets“,*APSCC(Asia-Pacific Satellite Communication Councial・ISSN 1226-8844)Newsletter*,2012,Q4.

Don Brown,2012.“2012:A Milestone in the History of Military Satellite Communications on Commercial Satellites“, *APSCC (Asia-Pacific Satellite Communication Councial)Newsletter*,2012,Q4.

Harold Kerzner 著，楊愛華・楊敏・王麗珍等譯，2008。《專案管理》（PROJECT MANAGEMENT）,2008 年 11 月。

M. F. Othman, N. A. Kamarudin, M. R.Samsudin,N. Hamzah& A. Sabirin,2009.“Parametric Analysis of the Communication Satellite Characteristics”, *International Conference on Space Science and Communication*.

Nile Suwansiri,2016.“The Future of High Throughput Satellites“, *APSCC (Asia-Pacific Satellite Communication Councial)Newsletter*, 2016,Q1.

Reg Austin,2010.Unmanned Aircraft Systems UAVs Design, Development and Deployment.

Tulin E. Mangir,1995.The future of public satellite communications, March.

Terry Neumann,2014.“Plotting the Future of Maritime Mobility“, *APSCC (Asia-Pacific Satellite Communication Councial)Newsletter*, 2014,Q1.

Wei Li,2015.“New Satellite Systems and Date Intensive Applications to Drive the Maritime Market“, *APSCC (Asia-Pacific Satellite Communication Councial)Newsletter*,2015,Q3.

Android 應用程式安全性分析之研究-以即時通 APP 為例

傅振華 王正喆 邱金燕

國防大學資訊管理學系

摘要

智慧手機行動網路發展所帶來的衝擊，除了便利性外，也帶來資安風險。有鑑於 Android 發展與通訊軟體應用之趨勢，本研究之目的將針對在 Android 平台上之通訊軟體(LINE)進行安全性分析研究及探討，希望能夠透過實際擷取伺服器與使用者端資料傳送的封包內容即時分析，了解「在資料傳送過程時，如何產生相關的資安問題或弱點」。

本研究將運用 Wireshark 及 TCP dump 等軟體工具，擷取通訊軟體(LINE)封包，並進行分析作業，另運用 File Sync、Ultra Edit 及 SQLite Manager 進行檔案資料分析；並嘗試瞭解通訊軟體(LINE)所採取的安全防護、加密機制，如該即通時訊軟體所採用之加密技術容易突破，則表示即時通訊軟體將肇生高風險資安疑慮，反之，則得到相對資訊安全的使用環境，並提供 APP 開發團隊做為資訊安全防護所需考量的議題。

關鍵詞：Android、LINE App、封包擷取、資料比對

A Study on Security Analysis ofAndroid Application-a Case of Instant Message App

Chen H. Fu　Liang C. Wang　ChingY.Chiu

Department of Information Management, National Defense University, Taiwan, R.O.C.

Abstract

The impact of the development of the mobile network of smart phones, in addition to greater convenience, but also bring more security risks.In view of Android development and communication software application trends, the purpose of this study will be in the Android platform on the communication software (LINE) for security analysis and research, hoping to capture the actual server and user data transmission Analyze packet content in real-time to understand "how information security issues or weaknesses are related to the data transmission process."

In this study, we will use the software tools such as Wireshark and TCP dump to extract and analyze the LINE packet, and use File Sync, Ultra Edit and SQLite Manager to analyze the files. Therefore, it is important to understand the various methods of encryption, such as the encryption technology used in the instant messaging software, which is easy to break, communication software will be a high-risk information security concerns. On the contrary, the relative use of information security environment can provide APP development team as information security protection required Consider the issue.

Keywords: Android, LINE App, Packet Retrieval, Data Matching

壹、緒論

一、研究背景與動機

西元1994年8月16日，IBM公司發表了全世界第一隻智慧手機(Simon)，除了基本的手機功能外，已結合一些應用程式及連線至傳真機的功能，得到部分商務人士的喜愛(BBC NEWS Technology,2014)；但因為售價偏高(需約美金899元)，行動網路技術發展亦未完全成熟，且電池續航力不足(僅可使用約1小時)，開賣2年後，僅賣出50,000隻手機。最終，史上第一隻智慧型手機也就這樣淹沒在時代洪流之中。

直到西元2007年，蘋果公司發表了旗下智慧型手機iPhone第一代，它搭載蘋果公司研發的iOS(以前是OS)手機作業系統，在使用者介面上，建立圍繞手機的多點觸控螢幕(6s後的款式增加了壓力感觸)，當中包括了虛擬鍵盤，是一款結合了拍照功能、個人數位助理、媒體播放器，擁有收發電子郵件、無線通信裝置、網頁瀏覽等功能的智慧型手機(Smart Phone)，並支援Wi-Fi、2G、3G和4G LTE連接。它還可以拍攝視頻(iPhone 3GS後才成為標準功能)，拍照、聽音樂，收發語音留言和電郵、及瀏覽網頁。其他功能如電玩遊戲、參考工作、GPS導航及連接社交網路...等，這些都可以透過下載應用程式(Application,Apps)來提供多樣的服務，等於是一台縮小的個人電腦(Apple Press Info, 2012)。人們對於手機的使用目的已不再是簡單的撥打電話或傳簡訊，而是期望能夠隨時瀏覽網頁、收發電子郵件、即時網路通訊等更多元化的用途，智慧型手機儼然已成為人們日常生活與工作中不可或缺的重要裝置。

同一時間，在2007年11月，Google公司與84家硬體製造商、軟體開發商及電信營運商成立開放手機聯盟來共同研發改良Android。隨後，Google以Apache免費開放原始碼許可證的授權方式，發布了Android的原始碼，讓生產商推出搭載Android的智慧型手機，Android後來更逐漸拓展到平板電腦及其他領域上。2010年末資料顯示，僅正式推出二年的Android作業系統在市場佔有率上已經超越稱霸逾十年的諾基亞Symbian系統，成為全球第一大智慧型手機作業系統，而在2014年6月Google I/O開發者大會上宣布：過去30天裡有10億台活躍的Android裝置，相較於2013年6月則是5.38億(Justin Kahn,2014)。

依據市場研究調查機構IDC的報告指出，2015年第3季出貨的智慧手機中，Android作業系統占了77.8%，是現今市場的主流；因此Android App發展越來越迅速，相關資安問題也伴隨而來。為了滿足各種服務的需求，相信很多人常常會在智慧型手機內下載有趣、方便又實用的App。然而，不是所有App都是安全的。資安公司趨勢科技在2015上半年行動裝置資安情勢總評報告中指出：「行動惡意程式的問題將越演越烈。在我們監控行動威脅情勢的期間，行動惡意程式的數量從去年的 426 萬成長至2015上半年的710萬(趨勢科技，2015)。」

因網際網路的普及與行動通訊的盛行，使得人們得以透過行動通訊裝置及App達到即時通訊，並可隨時隨地的存取或分享資料，再也不會因為不在電腦旁邊，無法收發電子郵件而苦惱不已。2015年2月LINE全球事業部資深副總裁姜玄玭表示，截至目前為止LINE全球註冊人數已超過6億，月活躍用戶數為1.81億，台灣註冊用戶數超過1,700萬，基本上所有用戶都是活躍用戶，僅次於日本與泰國。若依人口比率估算，在台灣，每10個人中就有7.3人使用LINE，且智慧型手機的持有者平均每天使用LINE的時間為71.8分鐘，遠高於使用Facebook的60.5分鐘。

二、研究目的

資訊安全一直是人們所關心的議題，而智慧手機行動網路發展所帶來的衝擊，除了更大

的便利性之外，也帶來更多的資安風險。有鑑於Android發展與通訊軟體應用之趨勢，本研究之目的將針對在Android平台上之通訊軟體(LINE)進行安全性分析研究及探討,希望能夠透過實際擷取伺服器與使用者端資料傳送的封包內容即時分析，了解「在資料傳送過程時，如何產生相關的資安問題或弱點」。

此外，並嘗試瞭解通訊軟體(LINE)所採取的安全防護、加密機制，以及在運作中所面臨的各項資訊安全性弱點，因此對於各種加密技術破解方法進行了解，如該即通時訊軟體所採用之加密技術容易突破，則表示即時通訊軟體將肇生高風險資安疑慮，反之，則得到相對資訊安全的使用環境，除可提供使用者對於資訊安全問題更一步的認識外，亦可提供APP開發團隊做為資訊安全防護所需考量的議題。

三、研究方法與步驟

本論文首先蒐集國內、外學者對於智慧型手機、Android 作業系統架構、Android 應用程式運作模式等文獻，加強對 Android 作業系統、應用程式及網路傳輸協定相關知識的瞭解，並整理成為本研究理論之基礎；另說明網路封包擷取及資料比對做為研究方法運用的基礎。本研究步驟區分以下 5 個部份，如表 1-1 所示。

表 1-23 研究步驟及內容

步驟	章節	內容
一	研究動機與目的	➢藉由文獻探討目前智慧型手機趨勢及未來所需面對的威脅，並說明本研究為何以Android應用程式做為研究標的。 ➢瞭解即時通App運作流程中所可能面臨的安全性弱點。
二	文獻探討	➢智慧型手機。 ➢Android作業系統、應用程式相關介紹。 ➢網路傳輸協定。 ➢網路封包擷取工具。 ➢即時通訊軟體安全性研究。
三	Android網路封包擷取及資料比對	➢建立Android網路封包擷取所需環境，並安裝網路封包擷取軟體。 ➢說明本研究網路封包擷取的步驟。 ➢針對智慧型手機資料夾內存資料進行研究。 ➢進行資料比對。
四	實作結果之安全性分析	➢擷取即時通訊服務使用者端資料傳送的封包，進行封包內容的分析，以確定資料傳送過程時之安全性。 ➢運用工具進行資料夾內含資料庫分析，查找異同之處，確認其資料安全性。
五	結論與建議	將本研究做歸納與整理，針對本研究的結果做結論，並且對後續研究者提出未來研究建議。

四、研究範圍限制

本論文所提研究範圍與限制分述二點：

一、隨著 Android 智慧型手機的市占率與即時通訊軟體應用之未來趨勢，使得各式軟體服務提供商提供眾多手機版的即時通訊 App，但本研究的範圍僅針對所選定的即時通訊 App 個案(Android 作業系統 4.3 版、LINE 6.9.1 版為主)進行探討，其他的即時通訊 App 不在本研究討論之範圍。

二、實作所需的 Android 手機是已取得系統的最高使用權限(Root)，如何取得 Root 權限不在此研究範圍中進行討論。

貳、文獻探討

一、Android 應用程式

(一)Android 安全性相關研究

由於 Android 開放源始碼的特性，使得投入應用程式的開發者眾多，上傳到應用程式市集 Google Play 的應用程式又沒有一套很嚴謹的審機制，導致 Android 應用程式的素質是良莠不齊，一般使用者只能被動的選擇評分高或風評好的開發者下載。但除了在 Google Play 下載之外，很多人也會到第三方市集或不知名網站下載應用程式，在這種情況下很容易就下載到劣質，甚至是危害系統，洩露個人資料的惡意軟體(林志剛，2013)。即使 Android 更新版本不斷推出，對於資訊安全的角度而言，仍然是遠遠不足以對抗各形各類的惡意 App 或惡意行為。故國內外學者均持續積極的探討並發表學術文章，提供相關使用者及軟體開發商參考運用：

1、Enck, Octeau, McDaniel and Chaudhuri (2011)：

藉由將 App 解壓縮進行逆向工程，再分析其中的原始碼來找出 App 將可能利用到的隱私資料。他們蒐集了 1100 個 App 的程式，藉由分析其中的原始碼，發現了有 27 個程式會將個人隱私資訊洩漏給廣告公司或是惡意攻擊的伺服器主機。

2、林愷庭(2012)：

針對 Android 智慧型手機惡意程式 DroidDream 進行逆向工程分析，並使用 DroidBox 工具進行惡意程式的動態分析，逐步檢視 Android 惡意程式的執行過程及目的。研究結果得知 DroidDream 惡意程式的主要目的在於竊取手機的 IMEI、IMSI、Device Model、SDK Version 等機密資訊，透過網路回傳到 184.105.245.17:8080 的主機，並主動下載安裝 DownlodProviderManager.apk 程式以持續接受攻擊者的監控。

3、Yang et al. (2013)：

許多技術容易判斷敏感資料是否從手機中傳播出去，但敏感資料的傳播不一定就表示隱私資料的洩露。根據用戶對敏感資料的流出是否知情，來判斷是否存在洩露隱私資料，故提出 AppIntent 分析框架，提供一系列 GUI 操作(敏感資料傳播的輸入)對應一系列的事件(輸入可能觸發敏感資料的傳播)，導致資料的傳輸。當經過用戶意圖表示敏感資料的傳播並不是隱私資料的洩露，相反則隱私資料可能被洩漏。

(二)LINE 安全性探討

LINE App 於 2011 年 6 月於首次於日本發表推出，使用者間可以通過網際網路並且在不額外增加費用情況下與其他使用者傳送若干文字、圖片、動畫、音訊和影片等多媒體資訊（包含語音通話）。LINE 起始平台以 Android 和 iOS 為主，並陸續在各行動平台及終端裝置推出應用程式，包含 BlackBerry(2012 年 8 月)、Windows Phone(2013 年 7 月)和 Firefox OS(2014 年 2 月)。此外，亦提供在 Microsoft Windows 和 Mac OS 平台上彼此通訊，迄 2014 年 10 月，LINE 於全球擁有約 5 億 6 千萬註冊使用者，其中包含約 1 億 7 千萬活躍使用者。

LINE 服務性質相當於舊有電信商提供的多媒體簡訊或簡訊等服務或即時通訊之演進，但受惠於智慧型手機的特性而視覺效果更為豐富；而除了無線網路費用(4G、3.5G)及電信資料量可能造成的額外費用外，通常 LINE 基本使用與少數貼圖免費，只在額外販售的貼圖或其他服務計價。有關其他參考文獻中 LINE 與幾套同性質 app（Whatsapp、Viber 及 Skype）來進行簡單安全性功能比較如表 2-1(軟體玩家，2012)。

表 2-1LINE App 與同性質 App 安全性功能比較表

項目	LINE	Whatsapp	Viber	Skype
中文界面	○	○	╳	○
支援平台	各類 Android/iOS/ Windows Phone 一般 PC	各類 Android/iOS/ Windows Phone	Android/iPhone	Android/iPhone Symbian/iPad/ PC
支援群聊	○	○	╳	○
支援語音通話	○	○	○	○
支援視訊通話	○	╳	╳	○
聊天表情圖示	○	○	╳	○
自動加入通訊錄	○	○	○	╳
即時拍照上傳	○	○	○	○
發送定位訊息	○	○	○	╳
搜尋對方的 ID	○	╳	╳	○

(資料來源，軟體玩家，2012 年 1 月)

二、SSL 網路傳輸協定

當不同的電腦系統透過網路來連接並交換訊息時，必須要有一個共通的標準，如此才能在不同的電腦之間交換訊息。而這個共通的標準就叫做協定。

SSL 是安全通道層(Secure Socket Layer)的縮寫，也就是將常見的 http 協定經過加密後的版本，目前已是網路上進行加密通訊之全球化標準。SSL 的目標在於保證二個應用間通訊的機密性和完整性以及可驗證伺服器身分，目前已廣泛的應用在 HTTP 連線上，當使用者以「https://」方式連上網站，如果瀏覽器的右下角有一個鑰匙，即代表該網站有支援 SSL。

SSL 的基礎演算法由網景(Netscape)公司的首席科學家 Taher Elgamal 編寫，並於 1994 年首先提出標準草案 SSLv1，於 1996 年發展出 SSLv3 更新版本；並且成為網際網路草案。國際標準組織 IETF(Internet Engineering Task Force)成立 TLS(Transport Layer Security)工作小組負責將 SSLv3 修改，在 1999 年 TLS 制訂出最初版本 TLSv1，使其成

為網際網路的標準。基本上，TLS 第一版可以視為 SSLv3.1，所以跟 SSLv3 相當類似(賴榮樞譯，2007)，主要差異如表 2-2 所示。

表 2-2 SSL 與 TLS 差異

差異性	SSL	TLS
版本號碼	SSLv3	SSLv3.1
訊息認證碼	填補區塊與秘密金鑰做串接	填補區塊與秘密金鑰做 XOR
密碼套件	支援 Fortezza 加密法	不支援 Fortezza 加密法
警訊代碼	提供 12 種警訊	不支援 SSL 中的 no_certificate 警訊，但新增一些其他警訊，共提供 23 種警訊
位元的填補(padding)方式	最短長度為限	任意長度，最多不能超過 255 個位元組

SSL 協定的通訊雙方分為二個不同的角色，一個系統為用戶端，另一個系統為伺服器。用戶端是負責發起安全通訊，而伺服器則要回應用戶端的請求。在 SSL 協定最常見的應用中，亦即確保使用者在瀏覽 Web 時的安全性，Web 瀏覽器是 SSL 協定的用戶端，而 Web 伺服器是 SSL 協定的伺服器。此外，SSL 使用對稱式加密系統與非對稱式加密系統的演算法，使用非對稱式加密系統產生交談金鑰，再利用對稱式加密系統與交談金鑰來加解密資料，SSL 提供安全連線主要有下列三項特點(Freier et al., 1996)：

(一)連線私密性(Confidentiality)：

伺服器與用戶端所傳送的資料將會在交握協定(Handshake Protocol)階段產生的交談金鑰所保護，除了伺服器與用戶端雙方以外，其他人無法得知他們所交談的內容。

(二)身分認證性(Authentication)：

在 SSL 交握協定過程中，可以驗證雙方的身分，驗證方法是使用非對稱式密碼系統如 RSA、DSS 和 X.509 憑證(Certificate)等公開金鑰加密技術。

(三)訊息完整性(Integrity)：

訊息的傳遞是使用訊息驗證碼(Message Authentication Code, MAC)來驗證訊息的完整性，其產生是由雜湊函數(SHA1、MD5)計算而來，可以保證所傳送訊息的完整性，亦即訊息沒有經過任何的竄改。

三、網路封包擷取工具

網路封包是網路用來傳送資料的最小單位。封包因為不同的應用服務或通訊協定，而有各種不同的大小。一個封包由標頭(Header)和資料(Data)所組成，封包的屬性被詳細地定義在標頭中，包括所使用的通訊協定、來源的 IP 位址、來源的通訊埠、目的地的 IP 位址、目的地的通訊埠等欄位，不過並非所有的通訊協定都有相同的欄位資料，由於採用不同的通訊協定，網路封包的結構都有些許的差異。

(一)、封包擷取

封包擷取意指透過網路介面(network interface)與軟體工具於網路上蒐集用戶端與伺

服器之間往來經過的封包，蒐集封包的意圖多為希望從封包內容中分析出有價值的資訊，這些資訊包括使用者連線行為、連線資料、網路流量、特定網路服務使用情況等(邱議賢，2005)。許多網路監聽工具已被開發用於有線或無線網路的監測，其最知名的是 TCPdump、Wireshark、Kismet 工具(Tan and Kotz, 2010)。本研究所採用封包擷取的工具如表 2-3 所示。

表 2-3 封包擷取工具

封包擷取工具	簡介	主要執行環境	操作方式
TCPdump	是一種使用命令列輸入參數選項的網路流量記錄工具程式，提供許多不同的命令列選項，可供使用者來檢視 TCP/IP 的封包內容。(註：TCPdump 必須使用系統管理最高權限執行)	Linux	文字介面，皆須要以指令下達來執行運作。
Wireshark	Wireshark 被廣泛應用在網路封包的解析，目前能夠解析超過七百種的通訊協定，所以對於網路上所使用的通訊協定，幾乎都能夠辨識與解析。Wireshark 也結合了過濾器功能，讓使用者可以針對特定的目標分析網路封包，有助於通訊協定的行為研究與異常行為的偵測。	Windows	圖形介面，以點選的方式操作功能表、工具列、網路封包清單等。

四、資料分析工具

在使用 LINE App 時，需經常需連線至伺服器更新或傳送各種類型資料，並且在手機目錄「/data/data」下建立「jp.naver.line.andriod」資料夾，以方便用戶儲存相關資料或檔案；故資料分析比對時，需採用相關工具以加速作業時間，本研究所採用資料分析比對工具計有：File Sync、Ultra Edit 及 SQLite Manager 等 3 種如表 2-4 所示。

表 2-4 資料分析工具

資料分析工具	簡介	主要執行環境	操作方式
File Sync	File Sync 是一套專門對檔案、資料夾作差異比對、同步備份的工具，並且還能夠在資料夾間同步進行備份複製工作，以利使用者比對出來源資料夾與目的資料夾不同的檔案，並由自己決定同步(同步的模式共有三種可以選擇，分別是鏡像、升級、雙向同步)的方式。	Windows	圖形化介面，以滑鼠點選方式，操作功能表、工具列、檔案資料夾清單及比對、內容項目等。
Ultra Edit	UltraEdit 是一套功能強大的文件編輯	Windows	圖形化介面，以

資料分析工具	簡介	主要執行環境	操作方式
	器，可以編輯文件、十六進制、ASCII 碼，完全可以取代原始的記事本，內建英文單字檢查、C++ 及 VB 指令突顯，可同時編輯多個文件。UltraEdit 即使開啟很大的文件速度也不會變慢，軟體附有 HTML 標籤顏色顯示、搜尋替換以及無限制的還原功能，一般用其來修改 EXE 或 DLL 文件。		滑鼠點選方式，操作功能表、工具列、檔案資料夾清單及比對、內容項目等。。
SQLite Manager	SQLite 是個很小巧的資料庫，而它的運用範圍相當的廣泛，且它也無需任何資料庫伺服器，就可直接運作，並且也支援 SQL 的指令，因此像未來的 HTML5 或是手機應用程式，都可以透過 SQLite 來存取資料，相當的方便；為了方便管理 SQLite 資料庫，除了透過指令的方式來新建資料庫外，亦可以運用 Firefox 瀏覽器中附加元件「SQLite Manager」來協助執行相關管理及新增修改資料庫內容。	Windows	圖形化介面，以滑鼠點選方式，操作功能表、工具列、資料庫清單內容項目等。

參、Android 網路封包擷取及資料比對

本章節將開始針對 LINE App 資料安全性分析進行實作方法說明，並區分為「封包擷取分析」及「檔案比對分析」2 大部分，如圖 3-1 所示。

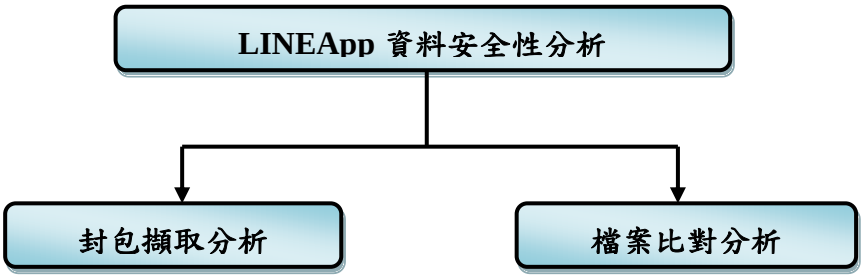


圖 3-19 資料安全性分析步驟

一、網路封包擷取

本研究之實作環境係以 Windows 7 作業系統及 Samsung Galaxy S3 (Android 4.3)為平台，網路環境則以 WIFI 無線網路做為測試。將以網路封包擷取之實作方式探究與分析即時通訊軟體(LINE)伺服器與使用者端資料傳送機制所可能面臨的相關防護弱點與資訊安全問題。網路封包擷取的實作環境建置及步驟如圖 3-2 所示。

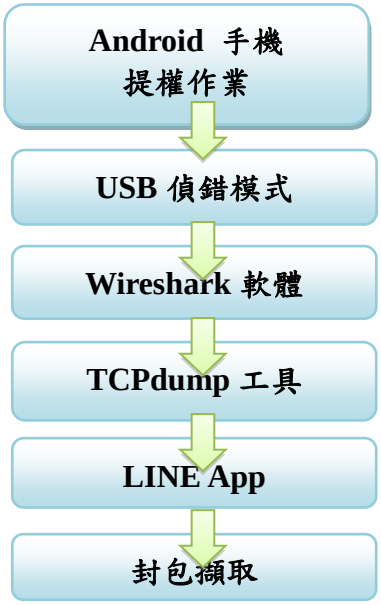


圖 3-20 網路封包擷取流程

(一) Android 手機提權作業

本研究所使用之 Android 手機，均需事先完成 Root 作業，亦即為取得最高管理者權限後，方得進行下一步驟，如何取得 Root 權限不在此研究範圍中進行討論(請參考研究範圍限制)。

(二)USB 偵錯模式

將手機與電腦連線，手機開啟 USB 偵錯模式，設定→開發人員選項→勾選「USB 偵錯」後，在命令提示字元輸入「adb devices」，若出現手機序號即代表手機與電腦連線成功，如圖 3-3 及圖 3-4 所示。

圖 3-21 網路封包擷取流程

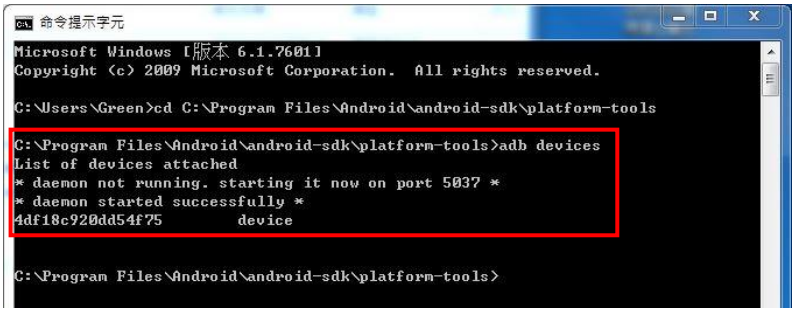


圖 3-22 手機與電腦連線成功畫面

(三)Wireshark 軟體

自 Wireshark 官方網站下載軟體並安裝在電腦中。

(四)TCPdump 工具

自 http://www.strazzere.com/android/tcpdump 下載 TCPdump 存放至電腦後，開啟「Root Browser」APP，並將該工具複製到手機目錄為「/data/local/tcpdump」，如圖 3-6 所示。

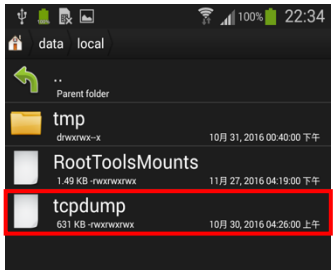


圖 3-23 完成 TCPdump 安裝至手機

(五)LINE App(Android 版)

自 Google Play 下載並安裝 LINE App(6.9.1 版本)，並且使用 Facebook 帳號註冊新帳號為「AaronWang-1」，如圖 3-7 所示。

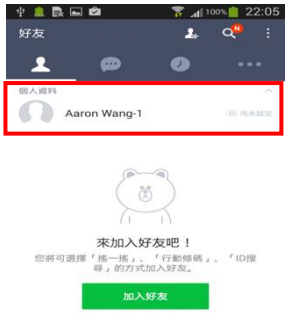


圖 3-24 完成 LINE 帳號申請及安裝

(六)封包擷取

1、建立*.pcap 檔案：

開啟「Root Browser」APP，並在手機目錄「/data」下建立檔案「packet1204.pcap」，以利後續運用 WireShark 進行封包分析作業。

2、設定防火牆白名單：

為簡化封包分析內容，開啟「DroidWall」APP，建立防火牆白名單，並設定規則「只允許 LINE 對外連線」，如圖 3-8 所示。

圖 3-8 設定防火牆

3、取得權限：

命令提示字元輸入「adb shell」即進入 Android 系統指令列模式，輸入「su」指令獲取系統最高權限，即可進行手機封包擷取，如圖 3-9 所示；封包擷取指令為「/data/local/tcpdump -p –vv -s 0 -w /sdcard/LINE.pcap」，相關指令說明如后：

(1)、–p：不使用混雜模式。

(2)、-vv：可抓到細部資料。

(3)、-s 0：s 是指定封包捕獲的長度此處指定為 0，意指擷取完整的封包。

(4)、–w：將結果寫入 pcap 文件，而不在終端上直接顯示。

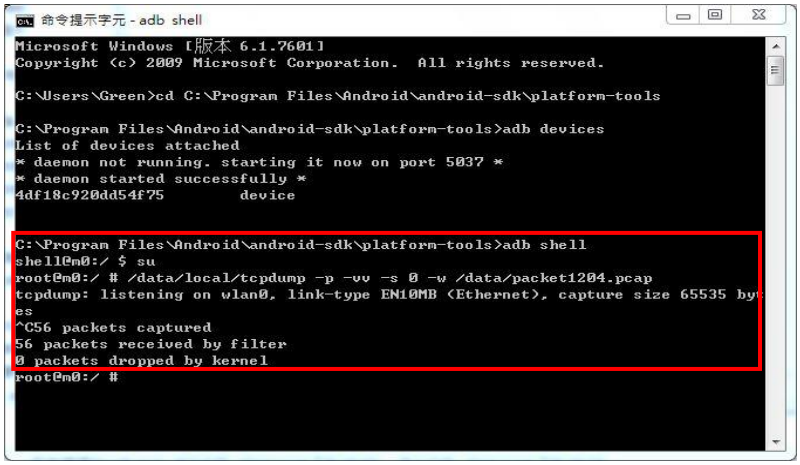


圖 3-9 封包擷取畫面

4、登入即時通訊軟體 LINE App 擷取封包：

輸入帳號密碼後登入，並同步傳送訊息，如圖 3-10 所示，若已完成封包擷取，則於命令提示字元按下 ctrl+c 停止。

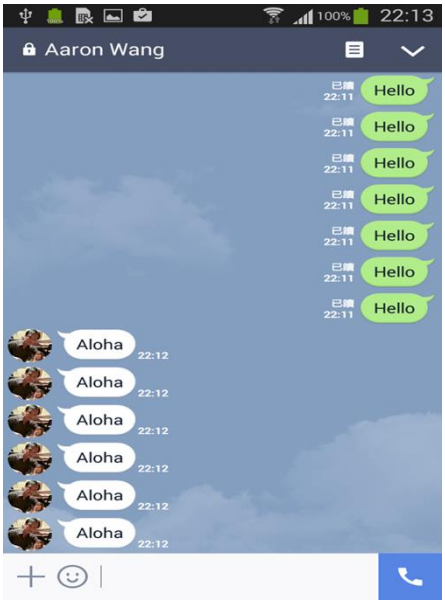


圖 3-10 傳送訊息畫面

5、傳送擷取封包：

開啟「Root Browser」APP，並找到「/data/packet1204.pcap」目錄複製後，即可將擷取封包文件檔案傳送至電腦中。

6、封包解析：

使用 Wireshark 開啟封包檔案，並於論文第四章進行分析作業。

二、資料內容比對

為強化整體安全性，即時通訊軟體(LINE)在 5.3.0 或以上版本即加入 Letter Sealing 功能，亦即為端點對端點加密(End To End Encryption，E2EE)。此功能本身採用 Diffie-Hellman (DH)來進行密鑰交換；一般用戶現時除了擁有 public key 之外，亦會自己擁有 private key，而當用戶向另一位用戶傳送訊息時，只會向接收訊息的用戶交換 public key 以進行解密工作，這種做法便可令收發雙方的訊息只可通過相互匹配的 public key 進行解密，從而省去了於 LINE 伺服器之中的解密過程，令訊息的安全大大提升。因此本研究將另外針對存放於手機儲存空間中的「LINE」資料夾進行分析研究，實作環境建置及步驟如圖 3-11 所示。

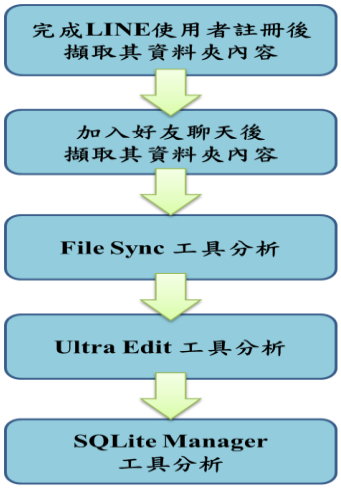


圖 3-11 資料比對步驟

(一) LINE 使用者註冊完成後，擷取資料夾內容

完成即時通訊軟體 LINE 下載安裝並使用新帳號註冊後，開啟「Root Browser」APP，在手機目錄「/data/data」下找到「jp.naver.line.andriod」資料夾，如圖 3-12 所示，並將其打包壓縮後存至電腦。

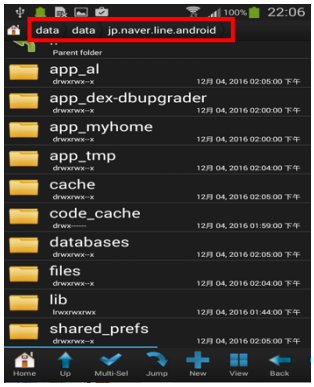


圖 3-12 僅註冊帳號之資料夾內容

(二)加入好友聊天後，擷取資料夾內容

完成前項資料夾壓縮打包後，即可加入好友並輸入訊息進行聊天，並比照前述方法，將此時資料夾再打包壓縮乙次存至電腦；本研究申請計 6 組帳號，並採用相同密碼進行資料夾打包動作，如表 3-1 所示。

表 3-24 帳號密碼表

項次	使用帳號	設定密碼	備考
1	ccwang0716@gmail.com	janice16oct	
2	ccwang07166@gmail.com	janice16oct	
3	cccwang0716@gmail.com	janice16oct	
4	ccwanggg0716@gmail.com	janice16oct	
5	ccwwaanngg0716@gmail.com	janice16oct	
6	aaww0716@gmail.com	janice16oct	

(三)使用 File Sync 工具分析

由於檔案資料眾多，使用「File Sync」工具，進行資料夾比對，左側資料夾為「僅完成註冊」，右側資料夾為「加入好友並聊天」，找出差異性檔案，如圖 3-13 所示，表 示項目具有不同內容，表 存在右側項目中。

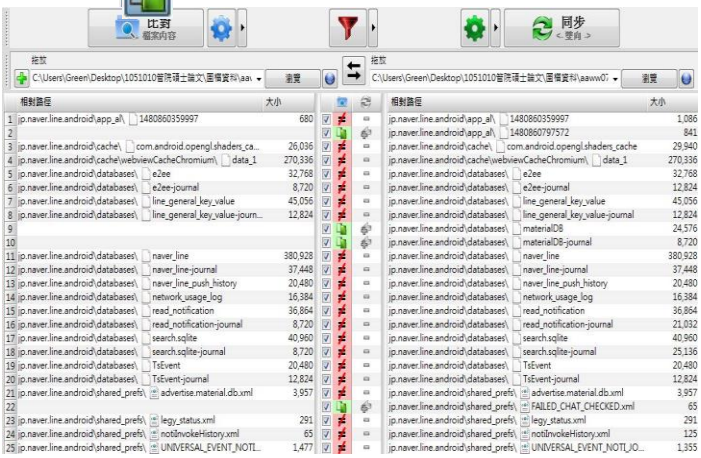


圖 3-25File Sync 比對結果

(四)使用 Ultra Edit 工具分析

找出差異性後，發現大多異動資料為「jp.naver.line.android\databases\」內檔案，故運用「Ultra Edit」工具分析異動資料內容，經實作結果，將針對「line_general_key_value 及 search.sqlite」其內容進行分析，如圖 3-14 所示，並於第四章進行分析作業。

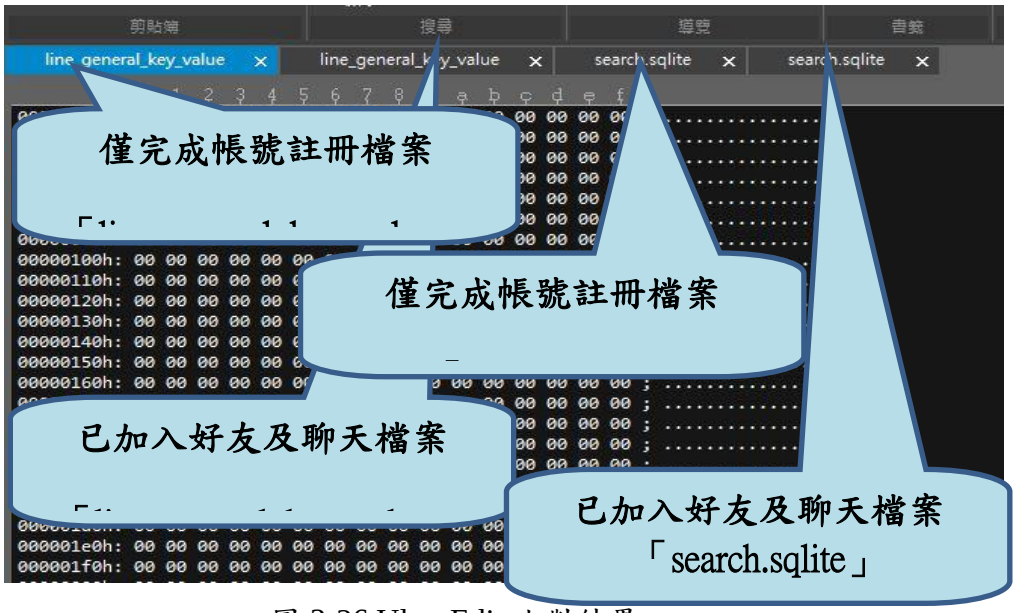


圖 3-26 Ultra Edit 比對結果

(五)使用 SQLite Manager 工具分析

最後使用「SQLite Manager」分析「naver_line」內容，如圖 3-15 所示，並於論文第四章進行分析作業。

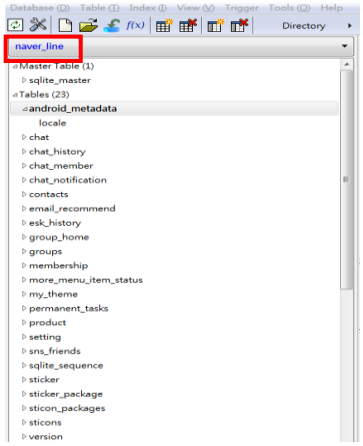


圖 3-5 SQLite Manager 分析結果

肆、實作結果之安全性分析

一、通訊軟體 LINE 傳送訊息封包分析

本次實作係運用 TCPdump 及 Wireshark 等工具軟體進行封包傳遞內容分析，以 Samsung Galaxy S3(Android 作業系統 4.3 版)手機 WIFI 上網，使用通訊軟體 LINE(6.9.1 版，更新時間 105 年 12 月 2 日)傳送訊息，實作環境如圖 4-1。

圖 4-27 實作環境

(一)TCP 封包分析

1、使用 Wireshark 內建「Expression to display fiIter」找出 TCP 封包，另運用 TCP Stream，彙整 TCP 封包內容，如圖 4-2 所示。

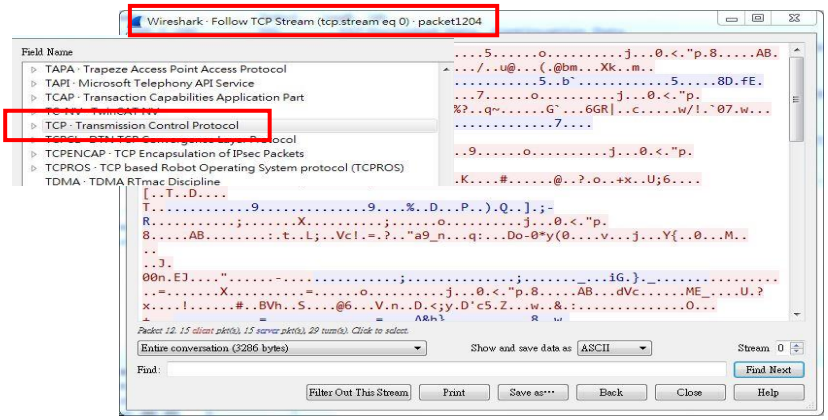


圖 4-28 TCP 封包彙整結果

2、經搜尋訊息內容「Hello」及「Aloha」等關鍵字均無發現，如圖 4-3 所示。

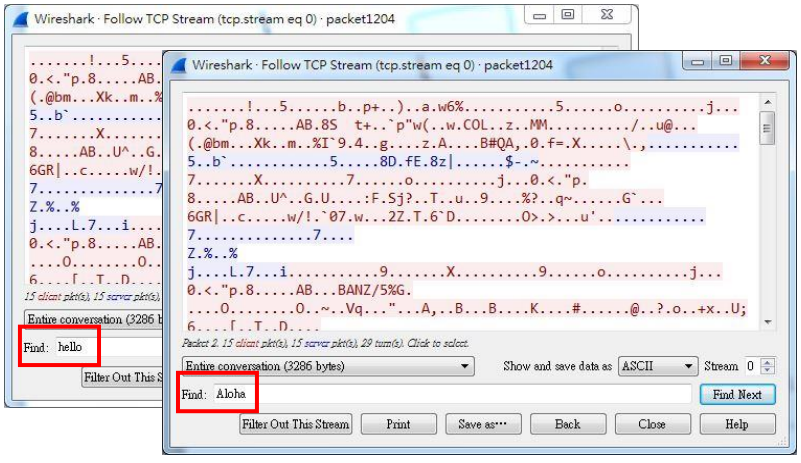


圖 4-29 TCP 封包搜尋訊息結果

(二)SSL 封包分析

1、使用 Wireshark 內建「Expression to display fiIter」找出 SSL 封包，另運用 SSL Stream，彙整 SSL 封包內容，如圖 4-4 所示。

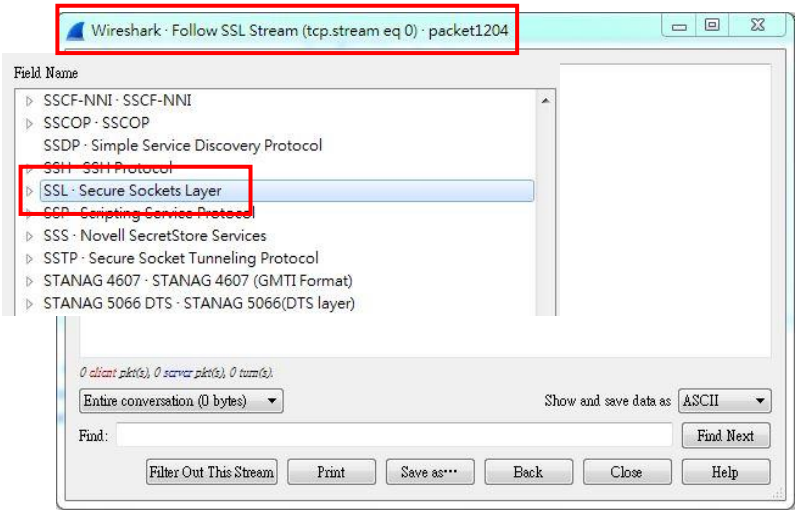


圖 4-30 SSL 封包彙整結果

2、因 SSL 封包已加密，故相關資料均無顯示，如圖 4-5 所示。

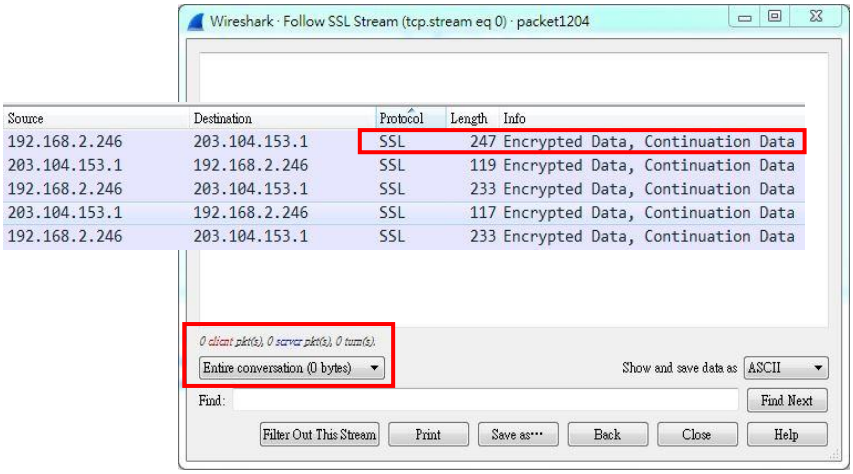


圖 4-31 SSL 封包搜尋訊息結果

(三)綜合分析

依前揭封包擷取內容而言，目前通訊軟體 LINE 均已使用 SSL 方式將資料加密，並且在 5.3.0 或以上版本即加入 Letter Sealing 功能，大大強化其網路傳輸資料之安全性，只要是在網路傳輸訊息的情況下，被惡意人士擷取封包，亦無法立即有效解讀訊息內容。

二、「line_general_key_value 及 search.sqlite」資料內容分析

假設依現行 LINE 公司對外宣稱，其訊息傳遞係採 E2EE 方式執行，那麼合理推斷相關加密金鑰訊息應存放在其手機資料夾內建「資料庫」，經過 File Sync 工具比對後，發現「line_general_key_value 及 search.sqlite」在 LINE 帳號完成註冊及加入好友聊天前後，資料內容均具有不同項目，現運用 Ultra Edit 工具進行分析，期發現相關資料安全性問題。

(一)「line_general_key_value」資料內容分析

1、人工比對資料內容結果，行數：00000d10h、0000afb0h 及 000009f70h 等 3 處，前後檔案資料內容對照後均相符，如圖 4-6、圖 4-7 及圖 4-8 所示。其中 000009f70h 可明顯看出使用者所使用之帳號(郵件信箱)，研判登入密碼以亂數方式呈現，字串內容如后：

【..(..31IDENTITY_IDENTIFIERaaww0716@gmail.com>...uGA_TMID01|mvsMQYKCouPMOox0xfdkzXoPld22hgC+VSwGkv+w460=@LINE"..C.PRIVACY_ALLOWFRIEND_REQUESTture.....?.???.)】

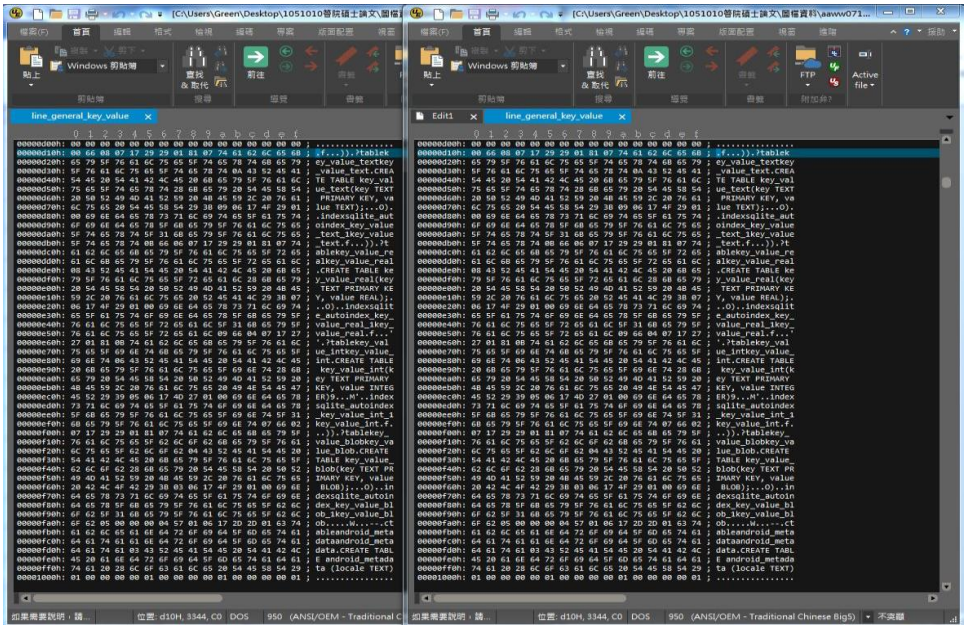


圖 4-32Ultra Edit 資料比對結果之一

圖 4-33 Ultra Edit 資料比對結果之二

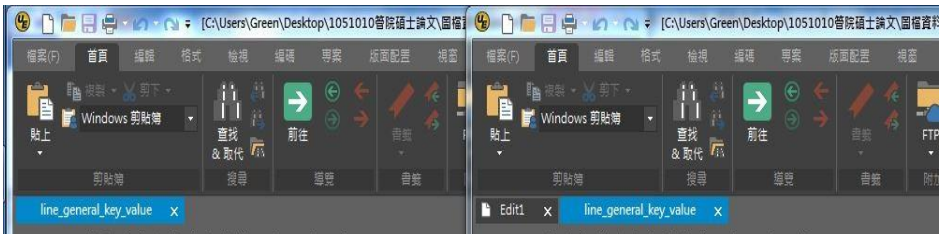


圖 4-34 Ultra Edit 資料比對結果之三

2、人工比對資料結果，前後檔案資料內容對照不相符者計有：

(1)行數：000005ce0h 處，後者檔案多出字串【_.CHATROOM_E2EE_ICON_DESCRIPTION_AUTO_SHOWN!..I.NEARBY_FRIEND_REQUEST_NEW_FLAG】，應指聊天室需採用 E2EE 圖示自動展示，且與附近的朋友回應(應指好友)訊息時要帶有新的圖示，如圖 4-9 所示。

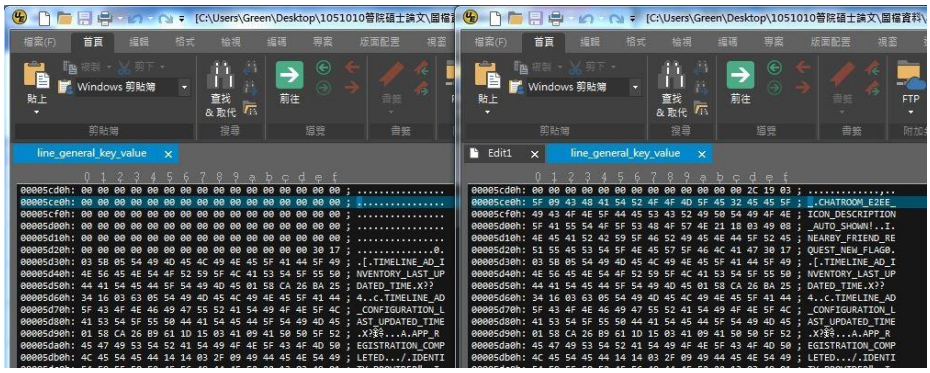


圖 4-35 Ultra Edit 資料比對結果之四

(2)行數：000006cf0h 處，後者檔案多出字串與 000005ce0h 處相同，如圖 4-10 所示。

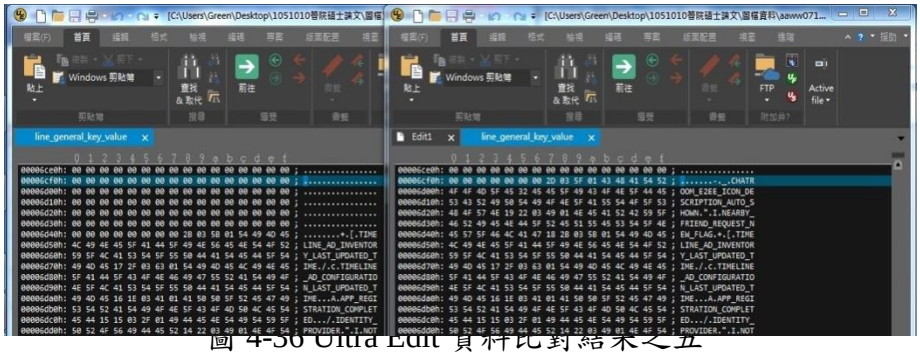


圖 4-36 Ultra Edit 資料比對結果之五

(二)「search.sqlite」資料內容分析

1、人工比對資料內容結果，行數：00000c40h 等乙處，前後檔案資料內容對照後均相符，如圖 4-11 所示。

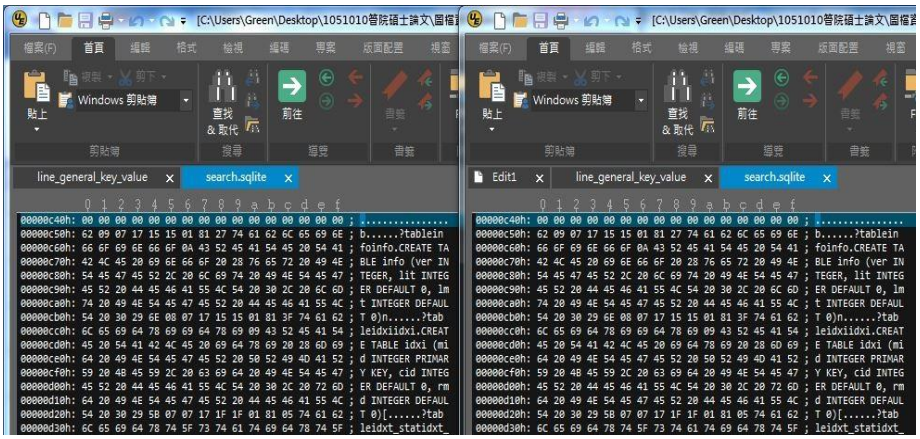


圖 4-37 Ultra Edit 資料比對結果之六

2、人工比對資料結果，前後檔案資料內容對照不相符者計有：

(1)行數：000004ea0h 處，後者檔案多出字串，明顯看出為使用者使用訊息交談內容，如圖 4-12 所示。

【....N...."...aloha.....9...."...aloha.....$...."...aloha....."...aloha.....?..."...aloha.....?..."hello.....?..."...hello.....?..."....."...aloha....."...aloha....."..aloha....."..aloha....H.....?..aloha.....hello.....?.????.???????.????】

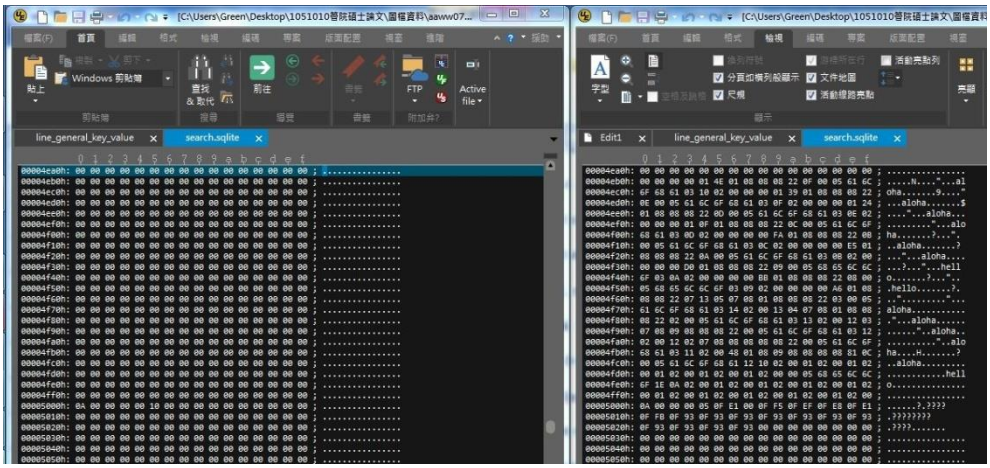


圖 4-38 Ultra Edit 資料比對結果之七

(2)行數：000005f90h、000007ff0h 及 000008f40h 等 3 處，前後檔案資料內容對照不相符，如圖 4-13、圖 4-14 及圖 4-15。

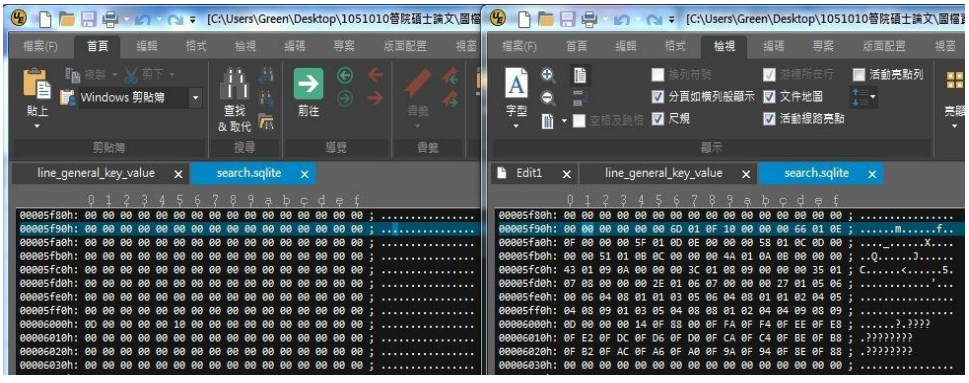


圖 4-39 Ultra Edit 資料比對結果之八

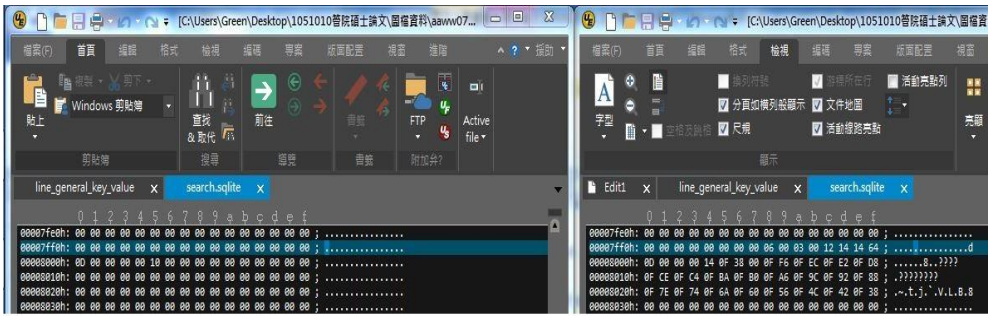


圖 4-40 Ultra Edit 資料比對結果之九

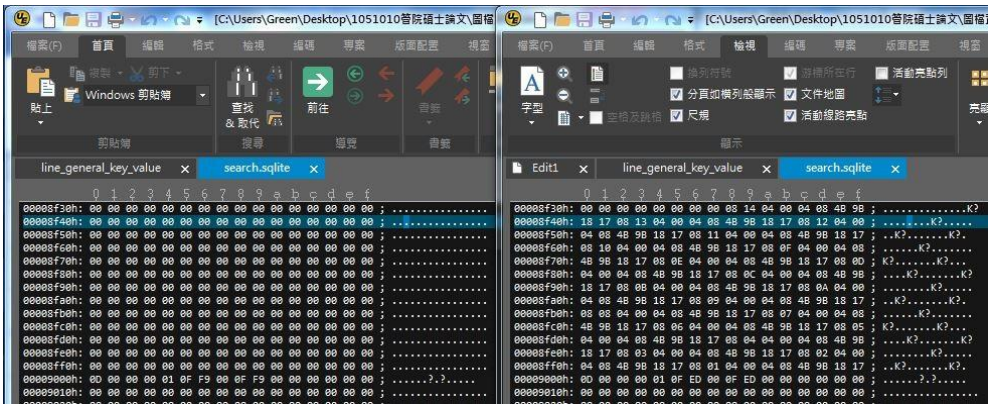


圖 4-41 Ultra Edit 資料比對結果之十

3、綜合分析

運用 Ultra Edit 深入比對檔案內容發現，即時通訊軟體 LINE 係將用戶帳號及傳送之訊息以明文方式儲存，密碼部分研判以密文方式儲存，換言之，若是手機送維修或是遺失情況之下，相關訊息都可能被竊取，輕則個人資料外洩，重則造成公司或企業內部機敏資訊的遺失，故使用通訊軟體 LINE 時，應當減少恰談公務或機敏資訊，避免資料外流情況發生。

三、「naver_line」資料內容分析

「naver_line」這個資料主要用來儲存與 LINE 相關之訊息，故僅針對「已加好友傳送訊息」資料內容分析，運用「SQLite Manager」即可開啟其內容及資料，開啟檔案後，可看見共計有 23 個 Tables，如圖 4-16 所示。

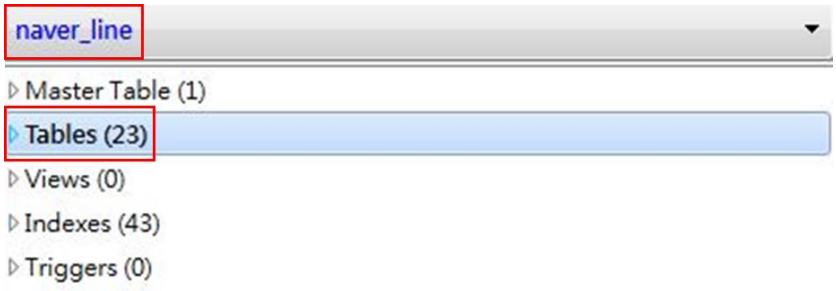


圖 4-42 naver_line 資料表

(一)「chat 資料表」分析

1、雙擊「chat」資料表會出現 chat_id、chat_name、owner_mid、last_from_mid 等資料欄位，其中 chat_id「u1a1a1e656767b0f0d1f6a8842aecd936」這個數值即代表好友在資料庫中的值，而自己本身即為 owner_mid「u8fbd7161f8a4e241a93382fbafa6f15d」這個數值，如圖 4-17 所示。

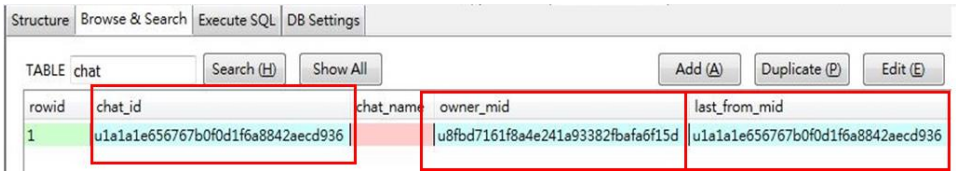


圖 4-43 chat 資料表之一

2、此外，亦可同時得知最後傳遞訊息、最後通訊時間、訊息總數及已讀訊息總數，訊息內容同為明文，如圖 4-18 所示。

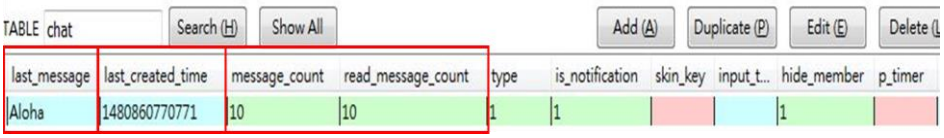


圖 4-44 chat 資料表之二

(二)「chat history 資料表」分析

雙擊「chat history」資料表會出現 id、server_id、chat_id、contect 等欄位，其中「chat_id」欄位裡面的值等同「chat」資料表欄位「chat_id」，而「contect」欄位則包含傳遞訊息內容，同為明文，如圖 4-19 所示。

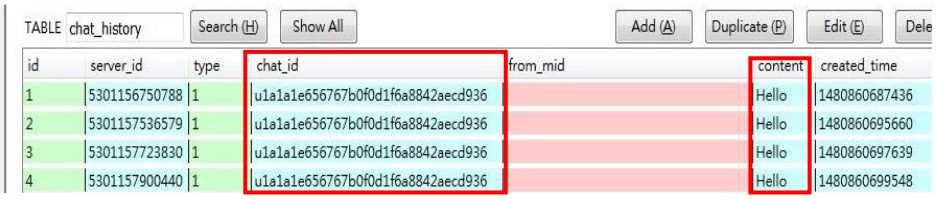


圖 4-45 chatstory 資料表

(三)「contacts 資料表」分析

1、雙擊「contacts」資料表會出現 m_id、name、server_name 等欄位，其中「m_id」欄位裡面的值等同「chat」資料表欄位「chat_id」，而「name」及「server_name」等欄位則表示聯絡人所用的名稱，如圖 4-20 所示。

圖 4-46 contacts 資料表之一

2、在「status_msg」欄位內，可完整看見聯絡人所使用的說明訊息【成功就是，做出自己能做的最好選擇，然後接受這個選擇】，如圖 4-21 所示。

圖 4-47 contacts 資料表之二

(四)綜合分析

承前揭所分析之「naver_line」資料內容，所有訊息完全是明文未加密的情況，意味著資料外洩的風險一直存在，無論是手機維修、遺失或是中毒、感染惡意程式諸般情況下，在不知不覺中，就有可能把相關的重要資訊外洩，造成不可彌補的後果。

伍、結論與建議

一、結論

本論文主要以LINE App Android版本進行安全性探究，藉由使用者透過Android手機登入LINE時並且傳遞訊息時，擷取伺服器與使用者間網路封包的內容、手機內部儲存的資料進行分析及研究。在網路傳輸的部分，LINE採用「訊息保護(Letter Sealing)」點對點加密技術(E2EE)保護聊天對話訊息，對話雙方的訊息經加密後，除了傳訊者及收訊者之外，任何第三方都將無法解密也無法窺知訊息內容，大大提升網路傳輸上的安全性。

然而，在用戶手機端所存放的資料夾內容，幾乎是採全部明文方式儲存，不論是傳送訊息內容、訊息時間、訊息數量、聯絡人資料等等，都可以一目瞭然及完全掌握，這造就了一個相當高的風險，手機不能中毒或感染惡意程式、不能遺失、送修又是一個風險，隨時都有可能導致私人訊息外洩；部分政府單位亦常常使用LINE群組開會討論重要決策事項、公司企業、學校家庭亦常常以「群組」方式通知相關訊息或傳遞資訊。關於這個弱點風險項目的存在，可讓使用者對於LINE App的安全性問題更一步的瞭解外，亦可提供相關App開發者做為資訊安全防護所需考量的問題。

二、建議

雖然智慧型手機與其相關 App 帶來許多便利，但便利的同時也面臨了各種資安威脅。目前眾多新開發的 Android 應用程式可能有意或無意間，未經過完善的安全性審核機制，即提供給人們下載使用(含 APK 檔)，對於機敏資訊的防護程度並不甚了解。為了能提供更完善的 Android 應用程式安全性分析，關於後續研究方向將可進一步針對市面上其餘即時通訊軟體(如微信、揪科等)以及本研究主題 LINE 的圖片、表情、語音、視訊等功能面向，以反組譯方式探究 App，經由分析反組譯後的原始程式碼來理解程式碼的功能與運作流程，並可確認 App 是否採用明文方式或其他加密方式進行任何資料的傳送。

參考文獻

尤克熙，2002，Smart Phone 發展現況與趨勢分析，MIC財團法人資訊工業策進會研究報告。

王英裕，2004，智慧型行動電話技術發展藍圖，工業技術研究院。

邱議賢，2005，應用 session 分析與雜湊函數之即時封包追蹤還原機制，國立雲林科技大學資訊管理系碩士班碩士論文。

林愷庭，2012，Android 智慧型手機應用程式逆向工程之研究，中央警察大學資訊管理研究所碩士論文。

林志剛，2013，Android 應用程式安全與權限分析，宜蘭大學多媒體網路通訊數位學習碩士在職專班學位論文。

陳會安，2012，新觀念Android SDK程式設計範例教本，台北市：旗標出版股份有限公司。

梁文耀，2010，元件化架構與元件間通訊機制－深入了解Android系統架構運作原理，Android 開發大會財團法人資訊工業策進會主辦。

張意珮，2003，真的很smart的smartphone－談智慧型手機定義及未來趨勢，拓墣產業研究所焦點報告。

黃彥達，2005，智慧型手機榮景背後的深思，台北市：e天下雜誌。

楊銀濤，2009，智慧型手機發展趨勢研究，國立成功大學企業管理研究所碩士論文。

賴榮樞譯，William Stallings 原著，2007，密碼學與網路安全第四版，香港：培生教育出版亞洲股份有限公司。

簡唯倫，2012，智慧型手機功能發展趨勢與造形風格演變之研究-以Apple iPhone為例，大同大學工業設計研究所碩士論文。

鐘子杰，2002，應用LDAP於公開金鑰基礎架構之研究與實作，東海大學資訊工程與科學系碩士論文

Colin, W., 2009, Getting Started with Android Development for Embedded Systems, Mentor Graphics Corporation Embedded Systems White Paper.

Enck, W., Octeau, D., McDaniel, P., & Chaudhuri, S., 2011, A Study of Android Application Security, In USENIX Security Symposium.

Freier, A.O., Karlton, P., Kocher, P.C., 1996, The SSL Protocol Version 3.0, Internet Draft.

Jansen, W., Ayers, R., 2007, Guidelines on Cell Phone Forensics, NIST Special Publication .

Liu, J., Yu, J., 2011, Research on Development of Android Applications, Fourth International Conference on Intelligent Networks and Intelligent Systems , pp69 -72.

Maiwald, E., 2001, Network security: a beginner's guide, McGraw-Hill Professional.

Park, Y., Chen, J.V., 2007, Acceptance and adoption of the innovative use of smartphone, Industrial Management & Data Systems (107:9), pp. 1349-1365.

Tan, K., & Kotz, D., 2010, Saluki: a high-performance Wi-Fi sniffing program, Modeling and Optimization in Mobile, Ad Hoc and Wireless Networks (WiOpt), 2010 Proceedings of the 8th International Symposium on IEEE, pp. 591-596.

Yang, Z., Yang, M., Zhang, Y., Gu, G., Ning, P., & Wang, X. S., 2013, Appintent: Analyzing sensitive data transmission in android for privacy leakage detection, In Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pp. 1043-1054.

具權重設計之代理盲簽章門檻機制

蘇品長 楊顓豪 曾健豪 葉家維 高晨栩

國防大學管理學院資訊管理學系

摘要

隨著網路興盛發展，數位簽章的應用也更具多樣化，其中，代理盲簽章的廣泛應用程度也特別被重視。所謂代理盲簽章，其概念就是結合盲簽章和代理簽章的特性，由原始簽章者授權給代理簽章者，使代理人可對簽署文件實施盲簽章，也就視同原始簽章者對該文件簽署的認可；此外，有學者提出門檻式簽章的概念，藉由改變門檻值的大小，調整系統的安全性與操作效率；後續更有學者導入權重構想，配合彈性化簽章架構，調整各成員決策權比重，使其更能符合實務需求。本研究為一創新應用構想，整合權重的演算方式導入代理盲簽章及門檻式簽章機制，並採用橢圓曲線密碼系統使運算速度比現行其他非對稱密碼系統快速之特性，設計出一套具權重之代理盲簽章門檻機制，將可適用於高彈性任務編組的客製化環境。

關鍵詞：權重、門檻、代理盲簽章、橢圓曲線密碼系統

A Design of Weighted Threshold Mechanism for Proxy Blind Signature

Pin-Chang Su Chuan-Hao Yang Jian-Hao Zeng
Chia-Wei Yeh Chen-Syu Kao

Department of Information Management, National Defense University, Taiwan, R.O.C.

With the prosperity development on Internet, it has brought diverse applications of digital signatures. One of the most generally discussed mechanisms is the proxy blind signature. The concept of the proxy blind signature is to combine the characteristics of the proxy signature and the blind signature. With the authorization from the original signer, the proxy signer can apply blind signature to the document, which is considered approved by the original signer. Besides, some researchers proposed the concept of threshold signatures, that is, to adjust the system security and operating efficiency by altering the threshold value. The subsequent researchers then introduced the concept of weights to operate in coordination with the flexible enterprise architecture by adjusting the decision weights of individual members. This was proven better in meeting practical requirements. This research presents a novel application construct which combines the proxy blind signature, the threshold signature, and the weighting mechanism, applies the Elliptic Curve Cryptosystem which is faster than other asymmetric cryptography systems, and designs a signing mechanism for the weighted threshold-oriented proxy blind signature, which can be applied to the use of a highly-flexible task force in a customized environment.

Keywords: Weight, Threshold, Proxy Blind Signature, Elliptic Curve Cryptosystem

壹、緒論

一、研究目的

2013 年，電影「全面攻佔：倒數救援」預設了一個場景，北韓恐怖分子實施恐怖攻擊，挾持了美國總統、國防部長及參謀總長，並且企圖引爆炸彈引發恐怖災難，由於被綁架的三人手上各擁有不同的三組密碼可引爆炸彈，且無任何授權代理機制，其他人均無權停止，事發緊急，唯一希望就是男主角救出人質，阻止恐怖攻擊。這是劇本預設的場景，但在現實世界中，卻可能出現決策權掌握在少數指揮者手上，倘若無任何授權代理機制，一旦出現決策者不便行使權力情況，將可能導致決策無法持續推行；若能在數位簽章應用設計下導入代理簽章及盲化機制，並加入權重及門檻特性，將可避免指揮者於不便行使權力時，下授給其他代理者行使，並因任務性質設定基礎門檻值及賦予各成員權重，使代理者在代理期間不會行使錯誤的決策。

當發生天災人禍，國軍支援救災任務，由軍團開設救災指揮所，資電群配合架設通資電中心，囿於時間急迫，通常由指揮官特業(通資電兵科)參謀地圖上直接選定，但地點通常不甚理想；或將決定權直接委託各通資電台、組長依據專業立場及現況，判斷可支援的通資電能量來共同商議架設地點，惟各台、組長此時太多分處於各管轄基地，無法集合開會表決。針對上述場景，倘若於國軍資訊應用平台上運作，且依權責賦予權重，設計具彈性的代理盲簽章門檻機制，救災應變及密鑰管理的問題將可迎刃而解。如何設計具權重之代理盲簽章門檻機制，符合機動性高的救災應變及安全性強的密鑰管理需求，值得探討與研究；此外，現行簽章機制，基於演算法的設計，導致過多的計算量，直接運用在行動式資訊平台並不合適，如何對未來的數位化戰場及國防管理作為，提出具體可行的安全應用，值得研究。綜上所述，本研究在預期達成以下目標：

- 本研究同時導入權重與門檻機制，設計一套可依需求強化決策品質的輔助機制，能有效強化決策品質。
- 系統中利用門檻機制特性，若無法達到獲得次密鑰之門檻，將無法正確還原密文。
- 將權重概念導入國軍現行系統架構，使系統可依使用者需求彈性調整權重，不因組織或任務調整需要重新設計系統。
- 針對安全性及效益分析探討，使其符合代理盲簽章、門檻式簽章及權重門檻式簽章等三種機制的安全規範，並滿足系統效益的實用性。
- 本研究採用橢圓曲線密碼系統機制，在相同金鑰長度下，擁有更高安全性之特性，未來可應用於行動資訊設備上之需求。

二、研究限制與範圍

本研究建構在代理盲簽章及門檻式簽章的基礎架構上，並導入彈性調整權重的概念，提出新式數位簽章機制，本研究著重在整體系統架構及其運用流程，以下幾點列為限制因素，將不予以討論：

- 橢圓曲線的產生、選取及基點定義等需符合 ISO 27002、ANSI X9.63、IEEE P1363、FIPS 186-4、NIST 800-170 等國際標準，符合以上標準之橢圓曲線才稱為安全的橢圓曲線，本研究對如何選取一個安全的橢圓曲線並不加以討論。

‧本研究著重於系統整體的演算法設計及安全性與可行性分析，故系統運作全程預設無通信滯礙問題，對如何通聯及維護品質方面不討論。

‧本論文著重於技術層面及演算法探討，提出具彈性調整之代理盲簽章門檻機制，對權重及門檻值設定等，屬國防政策範圍，文中不予討論。

貳、文獻探討

由於電子商務蓬勃興起，密碼技術也開拓了一個新領域，數位簽章應用因而產生，過去人類利用簽名或是蓋印章的方式來達到不可否認性，而數位簽章則是將平台轉變成網路世界。在數位網路環境中，為了達到不可否認性，簽章者利用自己的私密金鑰將要傳送的訊息做簽署的動作，對方收到簽章後利用與簽章者對應的公開金鑰做驗證，以確保此數位簽章合法性；雲端運算安全機制設計便是以數位簽章為基礎(Suresh et al., 2015)。一般而言，數位簽章必須具有以下特性(Stallings, 2004)：

‧必須能夠驗證簽章日期和時間與擁有簽章者身分等相關資訊。

‧在簽章的同時，必須能夠確認文件的內容。

‧為避免產生糾紛，驗證簽章時需由第三者來驗證。

‧簽章為避免被偽造或否認，需使用只有傳送者才有的一些訊息。

‧簽章的產生方式、辨識與驗證必須是很簡單。

數位簽章的應用相當廣泛，本研究彙整所探討的代理盲簽章(Proxy Blind Signature)、門檻式簽章(Threshold Signature)及權重式門檻簽章(Weighted Threshold Signature)等三個簽章應用機制的發展演進，說明如后。

一、代理盲簽章

代理盲簽章顧名思義就是結合代理簽章和盲簽章的特性，經由原始簽章者授權給代理簽章者後，代理簽章者可以對欲簽署文件產生盲簽章，當然也就視同原始簽章者對該文件簽署的認可；代理盲簽章具有五種特性(Tan et al., 2002)：

‧可驗證性(Verifiability)：從代理簽章中，驗證者可以驗證簽章的正確性，並相信原始簽章者同意此簽署文件。

‧不可偽造性(Unforgeability)：經過原始簽章者授權的代理簽章者能產生合法的代理盲簽章，而原始簽章者和其他沒有授權的第三者都不能偽造代理盲簽章。

‧不可否認性(Non-repudiation)：一旦代理簽章者代表原始簽章者產生合法的代理盲簽章之後，他不能否認自己曾簽署過該文件，以確保責任的歸屬。

‧不可連結性(Unlinkability)：當公開訊息之後，代理簽章者無法從訊息中追蹤所簽文件與簽章要求者的關係，也沒有辦法追蹤文件與當時所簽署文件之間的關聯性。

‧可區別性(Distinguish-ability)：每個人都能區別出該代理盲簽章是由原始簽章者所產生還是由代理簽章者所產生。

二、門檻式簽章

門檻式密碼系統(Threshold Secret Sharing Scheme)是一種簡單且有效的秘密分享(Secret Sharing)方法(Shamir, 1979)及(Blakley, 1979)；系統中有兩個重要參數：門檻值 t (Threshold Value)，及次密鑰的數目 n，一般皆採用(t, n)來表示，莊家(Dealer)將其所選定

的主密鑰 K 打造成 n 份不同的次密鑰，並讓每一位參與者(Shadow Holder)皆獲得一支次密鑰；(t, n)門檻式簽章便是結合數位簽章與門檻式密碼系統，提出一種同時將簽章權力與訊息認證分享給團體的機制(Desmedt et al., 1991)；門檻式簽章具有二種特性(Shamir., 1979)：

·當次密鑰的數目超過或等於門檻值t的時候可以推導出主密鑰K。

·當次密鑰的數目小於門檻值t的時候，則無法推導出主密鑰K。

門檻式密碼系統最早是根據 Lagrange 多項式(Shamir., 1979)及線性幾何投影法(Blakley., 1979)，陸續有學者以先前研究為基礎，提出一種新機制，聲稱能抵擋共謀攻擊(Jan et al., 1999)；共謀攻擊(Conspiracy Attack)，顧名思義，系統中的參與者們若交換手中的資訊，便能合力導出主密鑰；爾後，又有學者指出前者在實際狀況下，無法抵擋參與者共謀獲取系統的主密鑰，並運用離散對數設計了一套嶄新的方案(Chung et al., 2014)，最近，又有學者運用中國餘式定理設計出新的方法(Harn et al., 2016)；(t, n)門檻式簽章目前應用於針對病人健康看護資料在雲端架構的存取控制上(Harn et al., 2016)。

三、權重式簽章

權重式簽章是一種以權重為基底的群體導向(Group-Oriented)數位簽章技術，現實生活中，群體之間傳遞訊息的問題已愈顯重要，藉由設定個人在這個群體的權重，再依組織的機密性設定群體加解密的授權權重(蘇品長，1996)；理想的權重式簽章必需具備三種特性(Beimel et al., 2004)；：

·適用於任何的組織體系，包含階層式及平行式的架構。

·最少能滿足三個門檻的架構，將群體分類，分別客製化賦予門檻值及權重，需同時達到門檻才能執行。

·群體必須由系統賦予的權重來區分使用者，權重值高為強使用者，權重值低為弱使用者。

參、研究方法

本研究引進背包密碼系統分格計算的架構，導入權重應用的構想，並運用了橢圓曲線密碼系統相較於其他非對稱密碼系統具較高的安全性及效益，有效提升系統的執行效率，針對研究流程及架構說明如下：

一、本系統整體運作流程架構及參數表

本研究之設計構想圖如圖 3-1，符號說明表如表 3-1 所示：

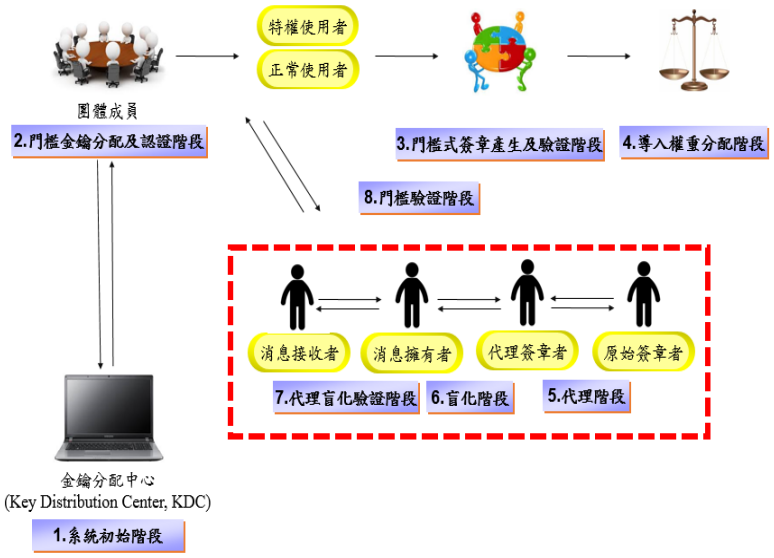


圖3-1 本研究之設計構想圖

(資料來源：本研究)

表3-1 符號說明表

項次	符號	說明	項次	符號	說明
1	$E(F_q)$	有限域F_q中的一條橢圓曲線	19	id_i	門檻式簽章團體p_i成員的身分
2	G	橢圓曲線中的基點	20	d_i	門檻式簽章p_i在團體中的私鑰
3	n	橢圓曲線上基點的秩	21	Y_i	門檻式簽章p_i在團體中的公鑰
4	q	$q > 2^{224}$之大質數	22	(r_i, s_i)	簽章p_i在團體中的個別數位簽章
5	a_0, b_0	門檻式簽章主密鑰	23	(r, s)	門檻式簽章團體數位簽章
6	PK_{KDC}	代理盲簽章主公鑰	24	U_z	代理盲簽章隨機因子
7	sk_{KDC}	代理盲簽章主私鑰	25	h_1	代理盲簽章用戶身分ID_u與W_u點轉換成值的雜湊函數
8	sk_u	代理盲簽章自選之部份私鑰	26	h_2	門檻式簽章u_i與id_i共同轉換成值的雜湊函數
9	ID_u	用戶身分	27	h_3	將m轉換成值的雜湊函數
10	W_u	ID_u由sk_{KDC}所產生部份公鑰	28	h_4	將明文序列$(h_3(m), x_i)$點轉換成值的雜湊函數
11	t_u	ID_u由sk_{KDC}所產生部份私鑰	29	H_5	明文序列m_w轉成點的雜湊函數
12	U_u	ID_u自行運算所產生部份公鑰	30	m_w	代理盲簽章中，接收 C 授權給代理簽名者 D 範圍內的認證訊息
13	r_u	ID_u自行運算所產生部份私鑰	31	Y_p	簽証公鑰
14	d	門檻式簽章團體私鑰	32	k_o	C 隨選之任意值，計算公鑰R_o。
15	Y	門檻式簽章團體公鑰	33	R_o	授權公鑰
16	p_i	門檻式簽章團體個別成員	34	k_p	代理簽章者 D 隨選之任意值，計算代理私鑰R_p。

17	u_i	莊家為p_i選取隨機參數	34	R_p	代理私鑰R_p。
18	σ_i	門檻式簽章團體驗證p_i參數	36	z_1, z_2	代理盲簽章盲因子

二、具權重之代理盲簽章門檻機制

(一)系統初始階段

·金鑰分配中心(Key Distribution Center, KDC)系統建置階段：系統在有限域上選取一條安全的橢圓曲線$E(F_q)$，(q為一個224bits以上大質數)，並在$E(F_q)$上選一階數(Order)為n的基點G，使得$n \cdot G = O$，O為此橢圓曲線之無窮遠點，並選取五個單向雜湊函數$\{h_1(),h_2(), h_3(),H_4(),H_5()\},H()$為數值轉點的單向雜湊函數，$h()$為數值轉數值的單向雜湊函數，計算公開參數。

·KDC 建立兩個密鑰為$\{a_0, b_0\}$的(*t*, *n*)門檻式簽章，其對應的多項式$f(x), g(x) \in F_q(x)$。

$$f(x) \equiv a_0 + a_1 x + \cdots + a_{t-1} x^{t-1} \quad (3\text{-}1)$$

$$g(x) \equiv b_0 + b_1 x + \cdots + b_{t_1-1} x^{t_1-1} \quad (3\text{-}2)$$

$a_0 = f(0), b_0 = g(0), \{a_i, b_j \in Z_n^*\}$。

$i = 1, 2, \ldots, t-1; j = 1, 2, \ldots, t_1 - 1$。

·此階段假設有四個角色，分別為消息擁有者A、訊息接收者B、原始接收者C及代理簽章者D，若成員有事需代理時，KDC給每位成員身分ID_u，KDC隨機選取$\{sk_u \in Z_n^*\}$，計算：

$$PK_{KDC} \equiv sk_{KDC} \cdot G \quad (3\text{-}3)$$

$$W_u \equiv sk_u \cdot G \quad (3\text{-}4)$$

$$t_u \equiv sk_u + sk_{KDC} \cdot h_1(ID_u, W_u) \quad (3\text{-}5)$$

最後公開相關參數。

·KDC 分別選擇$\{sk_A, sk_B, sk_C, sk_D \in Z_n^*\}$為系統主密鑰，並計算出部份公鑰$\{W_A, W_B, W_C, W_D\}$及私鑰$\{t_A, t_B, t_C, t_D\}$。

·由此可知，消息擁有者ID_A的部分公鑰$\{W_A\}$、私鑰$\{t_A\}$為

$$W_A \equiv sk_A \cdot G, t_A = sk_A + sk_{CA} \cdot h_1(ID_A, W_A) \quad (3\text{-}6)$$

簽名接收者ID_B的部分公鑰$\{W_B\}$、私鑰$\{t_B\}$為

$$W_B \equiv sk_B \cdot G, \ t_B = sk_B + sk_{CA} \cdot h_1(ID_B, W_B) \quad (3\text{-}7)$$

原始接收者ID_C的部分公鑰$\{W_C\}$、私鑰$\{t_C\}$為

$$W_C \equiv sk_C \cdot G, \ t_C = sk_C + sk_{CA} \cdot h_1(ID_C, W_C) \quad (3\text{-}8)$$

代理簽名者ID_D的部分公鑰$\{W_D\}$、私鑰$\{t_D\}$為

$$W_D \equiv sk_D \cdot G, \ t_D = sk_D + sk_{CA} \cdot h_1(ID_D, W_D) \quad (3\text{-}9)$$

·給定用戶身分ID_u，部分公鑰$\{W_u\}$、私鑰$\{t_u\}$，由用戶任選$\{r_u \in Z_n^*\}$作為ID_u的祕密值，計算$U_u \equiv r_u \cdot G$，ID_u公鑰為$PP_u = \{W_u, U_u\}$，私鑰為$PS_u = \{t_u, r_u\}$。

·消息擁有者ID_A公鑰為$PP_A=\{W_A,\ U_A\}$，私鑰為$PS_A=\{t_A,\ r_A\}$，簽名接收者ID_B公鑰為$PP_B=\{W_B,\ U_B\}$，私鑰為$PS_B=\{t_B,\ r_B\}$，原始簽名者ID_C公鑰為$PP_C=\{W_C,\ U_C\}$，私鑰為$PS_C=\{t_C,\ r_C\}$，代理簽名者ID_D公鑰為$PP_D=\{W_D,\ U_D\}$，私鑰為$PS_D=\{t_D,\ r_D\}$。

(二)門檻金鑰分配及認證階段

·KDC利用(3-1)、(3-2)式產生團體私鑰。

$$d=(f(0)+g(0)) \tag{3-10}$$

並計算團體公鑰為

$$Y=d\cdot G=(f(0)+g(0))\cdot G \tag{3-11}$$

·團體成員p_i隨機選擇$\{k_i\in Z_n^*\}$，並計算R_i，給莊家。

$$R_i=k_i\cdot G \tag{3-12}$$

·每位團體成員計算σ_i：

$$\sigma_i=h_2(u_i||ID_i) \tag{3-13}$$

·將σ_i傳送給莊家，同時，也將R_i透過團體通道實施匿名的廣播；莊家檢查(3-13)是否成立，判別合法使用者，決定是否該分配團體私鑰。

·假設莊家若想撤銷p_j的參與，只要p_j的公開參數值改為1，當驗證身分合法性時，發現$\sigma_i=h_2(1)$，p_j便無法參與團體簽章。

·假設p_i是一個正常的使用者，KDC分配其相對應的私鑰，並透過廣播公佈公鑰

$$Y_i=d_i\cdot G=f(x_i)\cdot G \tag{3-14}$$

·但假設p_i是一個具有特權的使用者，KDC分配其相對應的私鑰，並透過廣播公佈公鑰

$$d_i=(f(x_i)+g(x_{ij})) \tag{3-15}$$

$$Y_i=d_i\cdot P=(f(x_i)+g(x_{ij}))\cdot G \tag{3-16}$$

·團體成員根據成員屬性，利用(3-17)、(3-18)驗證d_i的合法性：

假設p_i是一個正常的成員，必須證明

$$d_i\cdot G=\sum_{j=0}^{t-1}i^j(a_j\cdot G) \tag{3-17}$$

假設p_i是一個具有特權的成員，必須證明

$$d_i\cdot G=\sum_{j=0}^{t-1}i^j(a_j\cdot G)+\sum_{j=0}^{t_1-1}i^j(b_j\cdot G) \tag{3-18}$$

·假設等式成立，KDC分配給團體成員的d_i是可信賴的，若不成立，代表KDC監守自盜。

(三)門檻式簽章產生階段

·假設共有t位團體成員構成團體簽章，訊息為m，簽章產生步驟：

團體中每位成員p_i計算：

$$R_i = k_i \cdot \mathrm{G} = (x_i, y_i) \tag{3-19}$$

$$r_i = H_4(h_3(m), x_i) \tag{3-20}$$

·假設p_i是一個正常的成員，必須計算

$$s_i = (r_i \cdot d_i \cdot C_i + k_i) = (r_i \cdot f(x_i) \cdot C_i + k_i) \tag{3-21}$$

·假設p_i是一個具有特權的成員，必須計算

$$s_i = (r_i \cdot d_i \cdot C_i + k_i) = (r_i \cdot f(x_i) + g(x_{ij}) \cdot C_i + k_i) \tag{3-22}$$

C_i可透過(3-22)獲得

$$C_i = \frac{\prod_{j=1,\ j\neq 1}^{t} -x_i}{x_i - x_j} \tag{3-23}$$

p_i傳送(r_i, s_i)給莊家，而(r_i, s_i)視為對團體成員對訊息m個別簽章。

·莊家接受個別簽名 s_i，並使用簽章者的公鑰去驗證其正確性

$$R_i = s_i \cdot P - r_i \cdot C_i \cdot Y_i \tag{3-24}$$

假設等式成立，莊家便接受成員的簽章。

(四)導入權重分配階段

·針對進入門檻的訊息，依據屬性問題，賦予各成員不同的權重，此權重由KDC客製化分配，以8種權重為例，本研究將權重設計為{(0, 0, 0) – (1, 1, 1) }，由KDC依據企業的性質可自行調整。

·KDC隨機選取n維向量$B = (b_1, \ldots b_i \ldots, b_n)$, $b_1 = \max(b_i)$, b_i為正整數且不得重複。

·任取質數w和m，且$\sum_{i=1}^{n} b_i < m < 2b_i$；計算$D = (d_1, d_2 \ldots, d_n)$

$$d_i = w \times b_i (\mathrm{mod} m), i = 1, \ldots, n \tag{3-25}$$

·將d_i進行不對稱的分組，由左至右在第j位元區分為左右二部分，形成e_i及v_i，分別有j位元及$n-j$位元；且

$$j \gg n - j, d_i = e_i \times 2^{n-j} + v_i \tag{3-26}$$

選取正整數t，滿足$(e_i + t \times v_i) < 2^j - 1$，即表示$e_i$無進位，且

$$u_i = e_i + t \times v_i, i = 1, \ldots, n \tag{3-27}$$

隨機選取兩個質數p和q，滿足

$$p > \sum_{i=1}^{n} u_i, q > \sum_{i=1}^{n} v_i \tag{3-28}$$

利用中國餘式定理計算公鑰：

$$A = (a_1, a_2, \ldots, a_n), 0 \le a_i \le pq - 1 \tag{3-29}$$

$$a_i = u_i (\mathrm{mod} p) = v_i (\mathrm{mod} q), i = 1, \ldots, n \tag{3-30}$$

私鑰為$\{p, q, t, w^{-1}, m\}$，w^{-1}為w的反元素。

·將權重$(x_{w1}, x_{w2}, x_{w3})_2$轉換為二元進位

$$(x_{w1}, x_{w2}, x_{w3})_2 = \{(x_1, x_2, x_3) \ldots (x_{n-2}, x_{n-1}, x_n)\}, x_i \in \{0, 1\} \tag{3-31}$$

將訊息$(x_{w1}, x_{w2}, x_{w3})_2$與公鑰$A$加密。

$$c = a_1x_1 + a_2x_2 + \cdots + a_nx_n \tag{3-32}$$

計算$u = c(\mathrm{mod}p), v = c(\mathrm{mod}q)$。

$$e = u - t \cdot v \tag{3-33}$$

$$d = e \cdot 2^{n-j} + v \tag{3-34}$$

$$y = w^{-1} \cdot d(\mathrm{mod}m) \tag{3-35}$$

運用初始超增序列B計算求解明文x，並進一步解出權重值。

(五)代理階段

·若成員有事需代理時，原始簽名者C無法親自簽署，必須請代理簽章者D代理簽署，任選$\{k_o \in Z_n^*\}$，計算授權公鑰R_o。

$$R_o \equiv k_o \cdot G \equiv (R_{o_x}, R_{o_y}) \tag{3-36}$$

$$n_1 \equiv t_C \cdot R_{o_x} + r_C \tag{3-37}$$

$$N_2 \equiv W_D + PK_{CA} \cdot h_1(ID_D, W_D) \tag{3-38}$$

$$Y_p \equiv n_1 \cdot U_D \tag{3-39}$$

·Y_p為簽名驗證公鑰，將$\{R_o, n_1, N_2, m_w\}$透過安全通道傳給代理簽名者D，其中m_w是指C授權給D範圍內的認證訊息，代理簽名者D收到後再實施驗證。

·產生代理(λ_p, σ_p)作為代理簽名者的代理簽署私鑰。

$$\lambda_p \equiv t_D \cdot R_o = (\lambda_{p_x}, \lambda_{p_y}) \tag{3-40}$$

$$\sigma_p \equiv r_D \cdot n_1 \tag{3-41}$$

(六)盲化階段

·消息擁有者A發送簽名請求，要求簽名者對之前協議的m_w實施簽署，計算$\{T_1, T_2\}$參數。

$$T_1 \equiv r_A \cdot H_5(m_w) = r_A \cdot M_w \tag{3-42}$$

$$T_2 \equiv t_A \cdot G \tag{3-43}$$

·將$\{T_1, T_2\}$發送給簽名者，簽名者收到後驗證$\{PK_{CA}, W_A\}$。

·$T_1 + T_2 \equiv (r_A \cdot M_w) + \left(sk_A + sk_{CA} \cdot H_1(ID_A, W_A)\right) \cdot G$

$$\equiv (r_A \cdot M_w) + (W_A + PK_{CA} \cdot H_1(ID_A, W_A))$$

$$\equiv r_A \cdot M_w + h_1(ID_A, W_A) \cdot PK_{CA} + W_A \tag{3-44}$$

·驗證成功，代理簽章者D任選$\{k_p \in Z_n^*\}$，計算R_p為代理私鑰：

$$\alpha \equiv k_p \cdot R_o = (\alpha_x, \alpha_y) \tag{3-45}$$

$$\beta \equiv t_D \cdot G \tag{3-46}$$

$$R_p \equiv \alpha \cdot \beta = k_p \cdot R_{o_x} \cdot t_D \cdot G \tag{3-47}$$

·將R_p傳送給消息擁有者A，但A不希望簽名者看到訊息m_w，便對訊息盲化，任取$\{z_1, z_2 \in Z_n^*\}$，計算隨機因子U_z。

$$U_z \equiv z_1 \cdot G + z_2 \cdot R_p \equiv (U_x, U_y) \tag{3-48}$$

$$R_z \equiv H_5(m_w) + U_z \equiv M_w + U_z \equiv (R_{z_x}, R_{z_y}) \tag{3-49}$$

$$m_w{}' \equiv R_{z_x} \cdot z_2{}^{-1} \tag{3-50}$$

將$m_w{}'$加密，消息擁有者A隨機選擇$\{z_3 \in Z_n^*\}$，消息擁有者A利用代理簽章者D的公鑰U_D設計一套加密演算法

$$E \equiv z_3 \cdot U_D \tag{3-51}$$

·消息擁有者A利用自己私鑰r_A與訊息$m_w{}'$結合，產生$\{R', S'\}$

$$R' \equiv m_w{}' \cdot G + E \tag{3-52}$$

$$S' \equiv z_3 \cdot G - r_A \cdot R' \tag{3-53}$$

將$\{R', S'\}$傳送給代理簽章者D還原E。

$$E \equiv z_3 \cdot U_D \tag{3-54}$$

·消息擁有者A運用祕密通道將U_{AD}傳送給代理簽章者D：

$$U_{AD} \equiv r_A \cdot r_D \cdot G \tag{3-55}$$

$$m_w{}' \cdot G \equiv R' - E \tag{3-56}$$

檢查附加在訊息m'之後的冗餘，以此檢驗是否為合法的簽章。

·檢驗完成後，代理簽名者D用代理私鑰$\{\lambda_p, r_D\}$計算$s_Z{}'$：

$$s_Z{}' \equiv k_p \cdot \lambda_{p_x} + m_w{}' \cdot \sigma_p \tag{3-57}$$

並將$s_Z{}'$通過安全管道傳給消息擁有者A，接著計算s_z：

$$s_z \equiv s_Z{}' z_2 + z_1 \tag{3-58}$$

·並將$\{U_Z, s_Z\}$作為盲簽章通過安全通道傳給消息接收者B，同時將R_z透過秘密通道給消息接收者B，供解代理盲階段使用。

(七)代理盲化驗證階段

·消息接收者接收(U_Z, s_Z)後，利用秘密通道得到的R_z求出M_{w_1}：

$$M_{w_1} \equiv R_Z - s_z \cdot G + R_{Z_X} \cdot Y_p \tag{3-59}$$

接著求R_1，$R_1 \equiv M_{w_1} + U$。驗證$R_z = R_1$，$M_{w_1} = M_w$為原本訊息。

·將接收到的簽章(U_Z, s_Z)和通過解密得到的訊息M_w代入

$$s_Z \cdot G \equiv U_Z + R_{Z_X} \cdot Y_p \tag{3-60}$$

若成立，則$\{U_Z, s_Z\}$就是原消息m_w簽章。

(八)門檻驗證階段

·莊家接受個別簽名s_i，並使用簽章者的公鑰去驗證其正確性

$$R_i = s_i \cdot P - r_i \cdot C_i \cdot Y_i \tag{3-61}$$

假設等式成立，莊家便接受成員的簽章。

·假設團體中的成員接受個別簽章數滿足(t,n)及(t_1,n_1)的門檻值要求，莊家便計算

$$s=\sum_{i=1}^{t}s_i \tag{3-62}$$

$$r=\sum_{i=1}^{t}r_i \tag{3-63}$$

肆、安全性及效益分析

本研究為創新密碼技術應用構想，運用背包密碼及橢圓曲線密碼系統，整合代理盲簽章及(*t*, *n*)門檻式密碼系統的基礎架構，並導入可彈性調整權重概念，滿足數位簽章需求，本章節與相關文獻之安全分析比較如后說明。

綜整文獻所提及的演算機制，本研究均能滿足鑑別性(Authentication)、機密性(Confidentiality)、完整性(Integrity)、隱匿性(Anonymity)、不可否認性(Non- repudiation)、驗證性(Verifiability)、可註銷性(Log out)、不可偽造性(Unforgeability)、門檻特性(Threshold characteristics)、防共謀攻擊(Anti-collusion attack)等十項安全特性，其中代理盲簽章符合前五種安全特性鑑別性、機密性、完整性、隱匿性、不可否認性，而門檻式簽章及權重式簽章必須滿足後五種特性鑑別性、機密性、完整性、隱匿性、不可否認性，概述如下：

一、鑑別性(Authentication)

鑑別性(Stallings, 2004)是指確保主體如使用者、程序、系統與資訊等實體或資源之識別，也就是其所聲明者的特性。承繼題意，描述本研究符合鑑別性之特色及如何避免非善意的攻擊手法，詳述如后：

·合法的接收到的簽章(U_Z,s_Z)並通過解簽章後得到的訊息M，需帶入式(3-60)進行驗證，透過式(3-48)、(3-59)的檢驗，若成功通過驗證，即證明為原訊息M的合法簽章，符合鑑別性的定義。

·假設攻擊者偽冒代理簽章者 D 要獲得消息擁有者 A 訊息時，必須偽造$(R',\ s')$；在(3-52)-(3-54)式，消息擁有者 A 任選$\{z_3 \in Z_n^*\}$；r_A為消息擁有者 A 的私鑰，在無法得知的情況下，假設消息擁有者 A 想要偽造代理簽名者 D 的簽章，必須偽造(U_Z,S_Z)；在(3-48)、(3-58)式，必須偽造$\{R_p,s_z'\}$；透過(3-45)-(3-47)與(3-57)式，方能通過驗證，由於$\{k_p,\lambda_{p_x},\sigma\}$僅掌握在代理簽名者 D 手中，攻擊者必須面臨解決 ECDLP 的難題。

二、機密性(Confidentiality)

機密性(Stallings, 2004)是指資料不得被未經授權之個人、實體或程序所取得或揭露的特性；本系統中使用橢圓曲線公開金鑰之加密方式。承繼題意，描述本研究符合機密性之特色及如何避免非善意的攻擊手法，詳述如后：

·攻擊者想解開訊息m_w，必須得到(t_D,r_D)，消息擁有者 D 的私鑰，將獲得的(t_D,r_D)透過(3-40)-(3-41)式實施驗證，但攻擊者無法得知(t_D,r_D)，即便是取得公鑰(W_D,U_D)，想取得私鑰(t_D,r_D) 必需面臨解 ECDLP 的難題，符合機密性的定義。

·假設攻擊者想從團體簽章方面著手，攻擊者沒有團體私鑰d，無法通過(3-23)-(3-24)式認證，若想求出團體私鑰d，便面臨解 FDP 背包密碼系統難題，即便是擁有團體公鑰Y，也無法直接從(3-21)-(3-22)式得到團體私鑰d，故可驗證群體簽章的機密性。

三、完整性(Integrity)

完整性(Stallings, 2004)是指對資料之精確與完整安全保證的特性，也就是確認資料

未遭受竄改及破壞。承繼題意，描述本研究符合完整性之特色及如何避免非善意的攻擊手法，詳述如后：

·攻擊者想要偽冒原始消息擁有者 A 發送訊息給代理簽名者 D 簽署，必須獲得代理簽署私鑰(λ_p, σ_p)，代理簽署私鑰是透過(3-40)-(3-41)式產生的，由式子可知，除了要知道代理簽名者 D 的私鑰(t_D, r_D)外，也必須得到$\{n_1, N_2, Y_p\}$參數，透過(3-36)-(3-39)式，攻擊者無法任意更改資料，故符合其特性。

·假設攻擊者想竄改代理簽名者 D 簽章訊息而不被發現，透過(3-45)-(3-50)式，將面臨破解單向雜湊函數(One-Way Hash Function, OWHF)難題，無法實施竄改而不被發現，且無法得到代理簽名者 D 的私鑰(t_D, r_D)，符合完整性需求。

四、隱匿性(Anonymity)

隱匿性(Tan et al., 2002)一種不具名或使用化名的行為，相對於具真實身份的行為，目的是不想表露自己身份，也是網際網路獨特的一種特性，又稱盲化。承繼題意，描述本研究符合隱匿性之特色及如何避免非善意的攻擊手法，詳述如后：

·攻擊者企圖從代理階段獲得訊息詳細的內容，在(3-48)-(3-50)式中，消息擁有者 A 在訊息發送前先對訊息進行處理，訊息擁有者 A 任意選取$\{z_1, z_2 \in Z_n^*\}$，攻擊者若想獲得訊息詳細的內容，必須破解$\{z_1, z_2\}$，面臨 ECDLP 難題，故符合其隱匿性。

·假設攻擊者想從團體簽章中，推導出參與團體簽章的一般或特權的成員，從(3-19)-(3-24)式中，將面臨背包密碼系統難題而無法得知，從(3-61)-(3-63)門檻驗證中，也同樣無法得知參與團體簽章的成員，故符合其隱匿性。

五、不可否認性(Non-repudiation)

不可否認性(Tan et al., 2002)指的是對一已發生之行動或事件的證明，使該行動或事件往後不能被否認的能力。承繼題意，描述本研究符合不可否認性之特色及如何避免非善意的攻擊手法，詳述如后：

·假設代理簽名者 D 為存取惡意的攻擊者，在代理簽署文件後，便否認自己曾經代理簽署，在(3-36)-(3-39)式，Y_p為簽證公鑰，並結合了代理簽名者 D 與原始接收者 C 的公、私鑰，故代理簽名者 D 無法否定提出服務請求或使用過該服務，原始接收者 C 也同樣無法否認曾經授權給代理簽名者 D 簽章，故符合其不可否認性。

·假設原始接收者 C 想要否認曾經授權給代理簽名者 D 簽章，由於後續將$\{R_o, n_1, N_2, m_w\}$透過安全通道傳送給代理簽名者 D，在(3-40)-(3-41)式中，產生(λ_p, σ_p)作為代理簽署私鑰，由於(3-37)式中，有運用原始接收者 C 私鑰產生參數n_1，故原始接收者 C 無法否認，故滿足其不可否認性。

六、驗證性(Verifiability)

驗證性(Tan et al., 2002)指的是簽署文件能通過驗證者的認證，證明文件為指定的簽署者認證。承繼題意，描述本研究符合驗證性之特色及如何避免非善意的攻擊手法，詳述如后：

·假設攻擊者想要偽造盲簽章$\{U_Z, S_Z\}$，盲簽章$\{U_Z, S_Z\}$是由(3-36)-(3-39)式中所產生的參數$\{R_o, n_1, N_2, Y_p\}$，在(3-48)及(3-58)式中結合盲因子$\{z_1, z_2\}$所產生，可經由(3-49)式所產生R_z及代理簽章者 D 的私鑰進行驗證，驗證其正確性，故符合驗證性需求。

·原始接收者 C 在(3-37)-(3-38)式中，運用本身的私鑰及代理簽名者 D 的公鑰產生

參數$\{n_1, N_2\}$，使(λ_p, σ_p)可藉$\{n_1, N_2\}$實施參數運算實施驗證，故符合其驗證性

七、可註銷性(Log out)

可註銷性(Beimel et al., 2004)是授權者想回收之前釋放出去的權力，之前參與的成員可能離職，授權者必須要能收回參與者的權力。承繼題意，描述本研究符合可註銷性之特色及如何避免非善意的攻擊手法，詳述如后：

·假設代理簽章者 D 為懷有惡意的攻擊者，原始簽章者 C 必須回收代理簽章權，在代理階段中，原始簽章者 C 任選$\{k_o \in Z_n^*\}$，經由(3-36)-(3-39)式運算，求出授權公鑰R_o及簽名驗證公鑰Y_p；此階段，原始接收者 C 只需要在系統內公布代理公鑰Y_p失效，之後利用Y_p所生成的代理簽章均無效用，故滿足其可註銷性。

·原始接收者 C 在系統內公布代理公鑰Y_p失效，(3-37)-(3-38)式產生參數$\{n_1, N_2\}$也跟著失效，授權公鑰R_o的權力也被收回，可視為原始接收者 C 註銷代理簽章者 D 的權力，故滿足其可註銷性。

八、不可偽造性(Unforgeability)

不可偽造性(Beimel et al., 2004)若攻擊者試圖偽造文件或簽章，任何人能夠經由參數驗證得知文件或簽章是否具有真實性。承繼題意，描述本研究符合可註銷性之特色及如何避免非善意的攻擊手法，詳述如后：

·假設攻擊者在團體簽章部分，想偽造成團體成員，在(3-10)-(3-11)式，KDC 產生團體公、私鑰，在(3-12)-(3-16)式，成員p_i藉由任選$\{k_i \in Z_n^*\}$，交由莊家判定是否為合法的使用者，在由 KDC 依一般或特權使用者賦予對應的私鑰，攻擊者無法獲得團體私鑰d及使用者私鑰d_i，故滿足其不可偽造性。

·在團體簽章中，一個使用者必須經由(3-14)-(3-16)式，交由 KDC 分配成員p_i相對應的私鑰d_i，並透過廣播公佈公鑰，團體成員則利用(3-17)-(3-18)式驗證私鑰d_i是否為可信賴的，故符合其不可偽造性。

九、門檻特性(Threshold characteristics)

門檻特性(Shamir., 1979)將指莊家選定主密鑰 *K* 打造成 *n* 份不同的次密鑰並讓每一位參與者皆獲得，當次密鑰的數目超過或等於門檻值 *t* 時，可以導得主密鑰，反之則無法。承繼題意，描述本研究符合門檻特性之特色及如何避免非善意的攻擊手法，詳述如后：

·假設攻擊者想通過門檻機制，獲得團體簽章的權力；本研究是基於雙重秘密分享概念，根據(3-1)-(3-2)式，由 KDC 任意選取兩個多項式，在(3-10)-(3-11)式中，KDC 賦予團體私鑰d，在(3-12)-(3-16)式，KDC 賦予成員使用者私鑰d_i，根據(3-17)-(3-18)式，群體內正常的成員若未超過 *t*，具有特權的成員若未超過t_1，便無法實施團體簽章，故滿足其門檻特性。

·門檻式簽章產生是由(3-19)-(3-20)式構成團體簽章，不論成員p_i是否為具有特權的使用者，必須透過(3-21)-(3-23)式產生，接著運用(3-24)式驗證團體簽章的正確性，故符合其門檻特性。

十、防共謀攻擊(Anti-collusion attack)

防共謀攻擊(Shamir., 1979)群體中的成員們若彼此交換手中的機敏資訊，共同串通謀劃，合力導出主密鑰的攻擊。承繼題意，描述本研究符合門檻特性之特色及如何避免非善意的攻擊手法，詳述如后：

·假設攻擊者想透過共同串通，獲得團體簽章的權力，首先必須恢復$\{f(0), g(0)\}$團體私鑰，本研究基於雙重秘密分享概念，根據(3-1)-(3-2)式，特權使用者無法

到達門檻值，故此機制能有效防止共謀攻擊。

團體中的成員，依據成員屬性，利用(3-17)-(3-18)式驗證d_i的合法性，根據(3-17)式，一般成員人數未到達t門檻值，恢復$g(0)$是不可能的；同樣的，即使特權使用者人數未到達t_1門檻值，根據(3-18)式，要恢復$f(0)$群體私鑰也是不可能的，故此機制能防止共謀攻擊。

伍、結論與未來研究發展

本研究運用背包密碼及橢圓曲線密碼系統，整合代理盲簽章及(*t*, *n*)門檻式密碼系統的基礎架構，並導入可彈性調整權重概念，可滿足數位簽章需求，本研究貢獻如下：

一、本研究結合門檻式密碼系統架構，當解密人數未達到門檻值時則無法將密鑰解開，此架構可為簽章系統增加一套安全防護機制，為嶄新的秘密分享概念，並可增加系統設計的安全性。

二、本研究利用代理盲簽章機制，當擁有權力者因有故無法行使權力時，可以將權力下授給眾多代理者使用，並運用盲化機制實施表決。

三、本研究將權重概念導入代理盲簽章架構，使系統可依使用者需求調整權重，不因組織或任務調整需要重新設計系統，未來可適用於國軍的決策支援系統。

四、本研究可符合代理盲簽章、門檻式簽章及權重門檻式簽章等三種安全機制要求，從安全性及效益分析，本系統更具實用性。

五、本研究運用橢圓曲線密碼系統的特性，由於其運算速度比現行非對稱密碼系統的認證演算法快速，可供結合於行動資訊設備或通行識別證認證金鑰上。

本研究針對權重的概念僅概略提出導入權重的方法與應用，未來可針對此部分加以討論，若將此概念結合未來建軍備戰上，將可節省更多繁文縟節，避免影響戰備任務遂行，後續會以實作方式驗證其系統可行性。

國防應用方面以救災應變為例：倘若天災突然發生軍團需開設救災指揮所，資電群配合架設通資電中心，如能建立一套機制，使各台、組長能迅速透過智慧型手機，配合權重賦予決定通資電中心合適位置，便能節省開設通資電中心時間，軍團指揮官也能即時掌握通資電能量，以最快的速度將救災兵力迅速投入災區，減少人員傷亡及財產損失。

參考文獻

中文部分

李南逸、王智弘、林峻立、張智超、溫翔安、葉禾田，2008，*網路安全與密碼學概論*，台中：滄海書局。

許建隆、吳宗成，2000，簽章加密法及其應用，*資訊安全通訊*，第六卷，第一期：33～41頁。

覃海生、張雷，2013，無對運算的代理盲簽章方案設計，*計算機應用研究*，第三十九卷，第四期：169～173頁。

蘇品長，1996，群體導向的數位簽章技術之研究，*全國管理碩士論文獎暨研討會*，第三十九卷，第四期：1~9 頁。

蘇品長，2007，植基於LSK和ECC技術之公開金鑰密碼系統，長庚大學電機工程系研究所博士論文。

蘇品長，2008，適用於Ad Hoc網路之快速交換金鑰機制設計，中正嶺學報，第53卷第1期：219~228頁。

英文部分

Beimel, A., Tassa, T., and Weinreb, E., Characterizing Ideal Weighted Threshold Secret Sharing, *SIAM Journal on Discrete Mathematics* (22:1), pp.360–397.

Blakley, G. R., 1979, Safeguarding Cryptographic Keys, *Proceedings of the National Computer Conference*, (32:1), pp. 313-317.

Chande, M. K., 2015, An Enhanced Proxy Blind Signature with Two Intractable Problems, *International Journal of Computer Applications*, pp. 1-5.

Chaum, D., 1982, Blind signatures for untraceable payments. *In Proceedings of Advances* in Cryptology—CRYPTO, pp. 199-203.

Chung, Y. F.., Chen., T. S., and Chen., T. L., 2014, An Efficient Threshold Signature Scheme Resistible to Conspiracy Attack, Applied Mathematics & Information Sciences(8:6), pp.3027-3032.

Desmedt, Y., and Frankel, Y., 1991, Shared generation of authenticators and signatures, *in Proc. of Advances in CRYPTO'91*, pp. 457-469.

Diffie, W., and Hellman, M, E., 1976, New Directions in Crytrography, *Proceedings of the IEEE* (22:6), pp. 644-654.

Foster, I., Kesselman, C., Tsudik, G., and Tuecke, S., 1998, A security architecture for computational grids. *in*: *Fifth ACM Conference on Computers and Communications Security*, pp. 83-92.

Girault, M., 1991, Self-Certified Public Keys. *Advances in Cryptology- Eurocrypt'91*(547), pp. 490-497.

Guo, C., and Chang C. C., 2012, Weighted Threshold Signature Based on Generalized Chinese Remainder Theorem, *Journal of Electronic Science and Technology*, (10:3), pp. 250-255.

Harn, L., 1995, Cryptanalysis of the blind signatures based on the discrete logarithm problem. *IEEE Elctronic Letteers* (31:14), pp. 1136-1137.

Harn, L., and Wang, F., 2016, Threshold Signature Scheme without Using Polynomial Interpolation, *International Journal of Network Security* (18:4), pp. 710-717.

Hu, L., Zheng, K., Hu, Z., and Yang, Y., 2009, A Secure Proxy Blind Signature Scheme Based on ECDLP. *2009 International Conference on Multimedia Information Networking and Security*, pp. 454-457.

Iftene, S., 2007, General secret sharing based on the Chinese remainder theorem with applications in e-voting, *Electronic Notes in Theoretical Computer Science*, (186:3), pp. 67-84.

Jan, J. K., Tseng. Y. M., and Chien, H. Y., 1999, A Threshold Signature Scheme Withstanding the Conspiracy Attack, *Communications of Institute of Information and Computing Machinery*, (27:2), pp. 31-38.

Jeng, F. G., Chen, T. L., and Chen, T. S., 2010, An ECC-Based Blind Signature Scheme. *Journal of networks* (5:8), pp. 921-928.

Juang, W. S., and Lei C. L., 1996, Blind Threshold Signatures Based on Discrete Logarithm. *Proceedings Second Asian Computing Science Conference on Networking and Security* (1179), pp.172-181.

Kaya, K., and Selçuk, A. A., 2008, Robust threshold schemes based on the Chinese remainder theorem, *in Proc. of Advances in Cryptology-AFRICACRYPT 2008*, pp. 94-108.

Khan, A. U., Sahoo, J., and Dash, S., 2013, An Improved Proxy Blind Signature Scheme Based on Time Stamp Value, *International Journal of Modeling and Optimization*, (3), pp. 80-83.

Koblitz, N., 1987, Elliptic Curve Cryptosystems, *Mathematics of Computation American Mathematical Society*, (48), pp. 203-209.

Lal, S., and Awasthi, A. K., 2003, Proxy Blind Signature Scheme, *to appear in Journal of Information Science and Engineering*, (2), pp. 5-11.

Li, J. G., and Wang, S. H., 2007, New Efficient Proxy Blind Signature Scheme Using Verifiable Self-certified Public Key, *International Journal of Network Security*, (4), pp.193-200.

Lin, W. D., and Jan, J. K., 2000, A security personal learning tools using a proxy blind signature scheme, *Proc. of International Conference on Chinese Language Computing*, pp. 273-277.

Menezes, A. and Vanstone, S., 1993, Elliptic Curve in Cryptosystems and Their Implementation, *Journal of Cryptology*, pp. 203-209.

Miller, V. S., 1985, Use of Elliptic Curve in Cryptography, *Advance in Cryptography-Crypto*, New York: Spring-Verlag, pp. 417-426.

Park, H., and Lee, I., 2001, A digital nominative proxy signature scheme for mobile communication, *in: Information and Communications Security, ICICS 2001*, pp. 451-455.

Pierre, J., and Peters., B. G, 2000, *Governance, Politics and the State. New York: St. Martin's Press* (11:1), pp. 12-13.

Pradhan, S., and Mohapatra, R. K., 2011, Proxy blind signature scheme based on ECDLP, *International Journal of Engineering Science & Technology*, (3), pp.73-79.

Rabin, T. R., 1994, Sharing of Secrets When the Dealer is Honest of Cheating , *J. ACM* (41:3) , pp. 1089-1109.

Shamir, A., How to share a secret, *Communications of the ACM*, (22:11), 1979, pp. 612-613.

Shannon, C. E., 1949, Communication Theory of Secret Systems, *Bell System Technical Journal*, (28:4), pp. 656-715.

Stallings, W., 2004, Cryptography and Network Security Principle and Practices, *Prentice Hall*, pp. 203-204.

Suresh, D., and Florence, M. L., 2015, RSA Algorithm & Signature In Cloud A Review, 27th Proceedings of the UGC Sponsored National Conference on Advanced Networking and

Applications, pp. 135-140.

Sun, H. M., Hsieh, B. T., and Tseng, S. M., 2005, On the security of some proxy blind signature schemes, *The Journal of Systems and Software*, pp. 297-302.

Sunitha, H., and Amberker, B., 2008, Proxy Signature Schemes for Controlled Delegation, *Journal of Information Assurance and Security*, pp. 159-174.

Tan, Z., Liu, Z., and Tang, C., 2002, Digital proxy blind signature schemes based on DLP and ECDLP, MM Research Preprints, MMRC, AMSS, Academia, Sinica, Beijing, (21), pp. 212-217.

Wang, H. Y., and Wang, R. C., 2005, A proxy blind signature scheme based on ECDLP, *Chinese Journal of Electronics*, (14), pp.281-284.

Wang, Q., and Cao, Z., 2006, An Identity-based Strong Designated Verifier Proxy Signature Scheme, *Wuhan University Journal of Natural Sciences*, (11), pp. 1633-1635.

Xu, Q., and Cao, Z., 2004, A New Proxy Blind Signature Scheme with Warrant, *2004 IEEE Conference on Cybernetics and Intelligent Systems*, pp.1386-1391.

Yang, X., and Yu, Z., 2008, Security Analysis of a proxy blind signature scheme based on ECDLP, in *Proc. 4th International Conference on Wireless Communications, Networking and Mobile Computing* (*WiCOM'08*), pp. 1-4.

Yu, X., and He, D., 2008, A new efficient blind signcryption, *Wuhan University Journal of Natural Sciences* (13:6), pp.662-664.

Yu, Y., Mu, Y., Susilo., W., and Au, M. H., 2014, Security pitfalls of an efficient threshold proxy signature scheme for mobile agents, *Information Processing Letters*, pp. 5-8.

應用虛擬亂數對稱式區塊加密機制於帳密登入作業之研究

傅振華[a] 張敦仁[b] 邱俊尹[a] 林聖翔[a]

[a]國防大學資訊管理學系
[b]實踐大學國際經營與貿易學系

摘要

本研究提供一個能加強安全於網頁伺服器的登入方案，方案中建議採用對稱式加密機制並包含 LCG 虛擬亂數產生器，將用戶端所輸入的密碼轉換成長度為 64 位元且對人不具意義的編碼。所建議採用的對稱式加密機制具六種攪亂功能函數，目的是來攪亂使用者輸入的密碼；經攪亂計算的輸出值，還使用 MD5 雜湊演算法轉換成長度同樣為 64 位元的雜湊值，同樣也是對人不具意義。最後，網頁伺服器依賴於用戶端的登入帳號和 MD5 雜湊值來處理登入帳號的過程。本研究利用 PHP / Apache / MySQL 建置一網頁伺服器，以驗證所建議的方案。所實作的網頁伺服器，實現了 PHP 網站程式呼叫 C 語言撰寫之對稱式加密機制暨 LCG 虛擬亂數產生器的功能，驗證了所建議的方案確實可以加強網頁伺服器的安全性。

關鍵詞：對稱式區塊加密法、虛擬亂數、線性同餘法、MD5

國防相關應用：本研究應用 LCG 虛擬亂數產生器於對稱式加密機制，將用戶端所輸入的密碼轉換成長度為 64 位元且對人不具意義的編碼，提供一個能加強安全於網頁伺服器的登入方案；本研究所提研究成果可應用於國軍資訊系統帳密登入作業處理，降低國軍資訊系統被入侵的可能性，強化國軍資訊系統作業的安全性。

A Study on User Account Login Process Bases on Symmetric Block Encryption Scheme with Pseudo Random Number Measures

Chen H. Fu[a] Tun R. Chen[b] Chun Y. Chiu[a] Sheng H. Lin[a]

[a] Department of Information Management, National Defense University, Taiwan, R.O.C.
[b] Department of International Business, Shih Chien University, Taiwan, R.O.C.

Abstract

For strengthening a login mechanism of a web server, this study proposes a security enhancement login scheme for a web server. In this proposed login scheme, this study adopts a symmetric block encryption scheme with a LCG pseudo random generator to convert a user's input password into a 64-bytes unreadable code. The proposed symmetric block encryption scheme uses 6 scramble functions to encrypt an input password. Moreover, this study also uses a MD5 hashing function to generate a message digest of the 64-bytes unreadable code. Finally, a web server depends on a user's login account and a MD5 hashing value of the 64-bytes unreadable code to handle a login procedure. In this study, we implement a PHP/Apache/MySQL web server and code the symmetric block encryption scheme with C. With the implemented web server and the proposed login scheme, we perform several login practices and find the proposed login scheme works well. Therefore, the proposed login scheme could be used to enhance a login process security for a web server.

Keywords: Symmetric Block Encryption, Pseudo Random, LCG, MD5

Relevance to National Defense: This study bases on a symmetric encryption scheme with LCG pseudo random number generator to convert user's password into unreadable codes in 64 bytes. This would improve security of login process in a web server. The proposed scheme in this study can be applied to login operations of information systems for R.O.C. military. It will reduce the possibility that information systems are invaded to strengthen operation security of information systems in R.O.C. military.

壹、緒論

本研究應用虛擬亂數的區塊加密機制，不但能加強密碼的複雜度，藉以避免 PHP 網頁在帳號登入時，MD5 雜湊運算法容易事前被駭客預測，更讓使用者資料受到保護且不遭受駭客之攻擊，安全度相對提升。架設網站伺服器容易被駭客入侵的主要原因是網站管理者對於資訊安全知識不夠深入及了解其中，加上主機全天候 24 小時都是持續啟動且暴露在網路的環境下，不論是駭客或者是企業內部員工，都能利用各種漏洞及破解工具攻破網站伺服器，如果本身安全防護機制未建置完整，資訊安全事件只會再次發生，為了避免登入帳號的密碼容易被預測，以往網站的密碼加密模式，大多是利用 MD5 訊息摘要演算法，而且現在很多開發工具是使用 ASP 與 JSP 為主，但相對軟體成本會增加許多。

所以本研究將會提出以 PHP 語言為主要系統開發工具，建置帳號登入的網站平台，密碼加密方式則是透過陳易佑（2010）研究論文所提出的「以虛擬亂數為基動態變化方式之對稱式區塊加密機制研究」為延伸應用在網站伺服器之可行性，再利用虛擬亂數加密機制為基礎理論，加上搭配 Open Source 的開發環境，使 PHP 語言在實作建置一個帳號登入過程中不易被猜測到密碼的網站伺服器。加密機制是針對區塊加密法進行研究變化，雖然串流加密法較為快速，通常較適合用於語音傳輸的即時加密，而區塊加密法比較適合於本研究在明文檔案之間的加密，廣為使用的加密標準分為 DES（Data Encryption Standard）、3DES（Triple Data Encryption Algorithm）及 AES（Advanced Encryption Standard）等，關於 AES 加密的基本定義，區塊長度及密鑰長度相對前二種加密技術更為複雜，因此將帳號登入的密碼藉由此加密方式可存於明文檔案，故發展一個透過加密文件能實際運用在系統環境中，期望此研究所產生出的結果，對於網站安全性能提昇。另外資料加密可藉由電腦計算所產生的亂數，將原有資料搗亂而達到另一種加密的效果，為了能有效地強化各種加密法，則利用亂數產生器不可預測性所產生出來的值搭配加密、解密運算中，通常稱之為「虛擬亂數產生器」（Pseudo Random Number Generate, PRNG），早期用於虛擬亂數產生器是由 Lehmer（1951）所發表的演算法，而現在最被廣泛使用及進一步改良的亂數產生器亦稱為「線性同餘法」（Linear Congenital Generator），本研究以 AES 為基之加密技術和線性同餘法虛擬亂數為核心基礎，進而運用並評估將其網站密碼加強複雜度之目的。

貳、文獻探討

一、AES 加密法類型

(一)AES 之發展及概述

避免 DES 相關對稱式演算法在未來可能會遭受暴力破解法攻擊，美國國家標準技術研究所（National Institute of Standards and Technology, NIST）為了要能取代 DES，於 1997 年正式邀約並徵求下一代的區塊加密法，以用來保護敏感及非機密的聯邦資料，最後經過四年甄選的結果，則是採用比利時密碼學家 Daemen and Rijmen（1999）所設計之 Rijindeal 加密演算法替代原先的 DES 演算法，後續 NIST 再將其 Rijindeal 加密演算法定為進階加密標準，並且發佈於（FIPS PUB 197），簡稱 AES 加密法。而如表 2-2 所示，可簡略說明 DES、3DES、AES 這三種加密法之間的差異性。

表 2-2 三種對稱式加密法比較表

類型	定義	明文長度(Bits)	金鑰長度(Bits)	加密效率	安全性
DES	速度稍快 適用於加密大量數據	56	56	中	弱

3DES	使用三組不同的密鑰 進行三次加密 強度更高	56	168	差	中
AES	這一代的標準加密法 速度快 安全級別高	128	128 192 256	好	強

透過 Rijindeal 加密演算法所設計之密鑰長度可區分為 128、192、256 位元，若是其他不同輸入、輸出之密鑰長度，將列為不符合金鑰之定義標準（楊政穎，2007）。且 AES 在應用上具有下列特色：高彈性、高安全性、低成本、演算法公開，故成為現代對稱式金鑰加密的主流，並廣為全世界所使用。所謂的高彈性是適合軟、硬體互相搭配實作，高安全性金鑰長度至少須具備 128 位元，低成本在於使用記憶體需求量較少。

(二)AES 加、解密架構

AES 的運作過中的回合數會因為金鑰長度而有所變化，但每回合中必包含位元組置換（SubBytes）、偏移列數（ShiftRows）、混合行數（MixColumns）及加入回合金鑰（AddRoundKey）四個階段。各階段之間資料輸入及輸出的形式稱為「狀態」（State），由 4*4 個位元組所組成（Daemen and Rijmen，1999）；惟不論是加密或是解密的程序，最後一回合僅使用 3 個階段（不包含行的混合），這樣設計的目的就是為了讓整個 AES 架構具有可逆性。依照各階段功能逐一說明如下：

●位元組置換（SubBytes）

AES 演算法是使用查表的方式來置換明文中的信息，並定義 S-Box 為一個 16*16 的位元組矩陣，當中包含所有可能的 8 位元數值（共 256 個）。在位元組置換的步驟中，將每個 8 位元數值的前 4 個位元當成 S-Box 的列（Row）索引，後 4 個位元為行（Column）索引，利用（列、行）的組合對應到 S-Box 中的陣列位置，並置換其內容（賴榮樞，2007）。

●偏移列數（ShiftRows）

此功能是使用的 AES 演算法（區塊大小 128 位元）中且透過循環位移之方式，讓每一豎列的矩陣，是由輸入矩陣中的每個不同列中的元素而組成。事先補充，128 位元及 192 位元的區塊分別在此步驟的位移模式也是相同。陣列中的第一列位置不會做位移動作，在最後三列的字元會各別被循環移動到不同行列的位置。第二列每個值則是向左循環位移 1 個位元組，第 1 個位元組則會移動到序列的最後面，第三列的每個元素向左位移 2 個位元組，第 1 個位元組及第 2 個位元組則移到序列的後面，第四列的每個元素向左位移 3 個位元組。

●混合行數（MixColumns）

是以行矩陣為單位來執行替換的一種方法，此法下會依據陣列中每一行轉換成函數，透過線性變化在矩陣中的對映做乘積，藉以替換每個值；換言之，係將一行四位元組經過特殊矩陣運算，得到新的四位元組。

●加入回合金鑰（AddRoundKey）

整個加密過程最重要為加入金鑰，雖然資料經上述三步驟後已達到混淆、擴散及非線性的效果，但攻擊者仍可能推導出轉換的公式而解開密文，故金鑰的加入可進一步提升安全性。將整個狀態資料與回合金鑰進行逐一位元的 XOR 運算，在每次的加密迴圈中，都會由主密鑰產生一把回合金鑰（透過 Rijndael 密鑰生成方案產生），這把金鑰大小會跟原矩陣一樣，再以矩陣加法的概念將回合金鑰加入原矩陣中每個對應的位元組。

二、線性同餘法之探究

Lehmer 在 1951 年代所提出的線性同餘法(Linear Congruential Method, LCG)，是目前最被廣泛運用的虛擬亂數產生器演算法。以四個參數來決定一個虛擬亂數，其遞迴方程式如下所示：

$$y_{i+1} = (a*y_i + c) \bmod m$$

y_0：種子值（Seed）

a：固定乘數（Constant multiplier）

c：增加量（Increment）

m：除數（Modulus）

以上四個參數皆為整數。

首先將種子的初始值設為 y_0，數值於起始時並不是隨機所產生出來，而是於運算前先行選定，其他的數列則是按照前一個所產生的種子數，再藉以輸入公式而循序產生出來，這裡選擇適合的 a、c、m 三種數值，便能夠得到不重複的整數；例如：設定 a=5，c=3，m=16，y_0=7，LCG 虛擬亂數產生器之亂數數值產生週期方式，如表 2-3 所示。

表 2-3 線性同餘法週期表

i	y_i	$5y_i$	$5y_i+3$	$(5y_i+3)/16$	y_i+1	U_i
0	7	35	35	38	38/16	6
1	6	30	30	33	33/16	1
2	1	5	5	8	8/16	8
3	8	40	40	43	43/16	11

(資料來源：周旭東等譯，2008)

藉由表 2-3 的週期表，取出 i、y_i 及 U_i 值之結果，如表 2-4 所示，這裡可推算出 $y_{17}=y_1=6$，$y_{18}=y_2=1$，$y_{19}=y_3=8$，由 i=17 至 i =32 能夠發現有相同順序 y_i 值及 U_i 值，更可以定義 i =1 到 i =16 是為一個週期。

表 2-4 線性同餘法週期表之舉例

i	y_i	U_i	i	y_i	U_i	I	y_i	U_i	i	y_i	U_i
0	7	---	5	10	0.625	10	9	0.563	15	4	0.250
1	6	0.375	6	5	0.313	11	0	0.000	16	7	0.483
2	1	0.063	7	12	0.750	12	3	0.188	17	6	0.375
3	8	0.500	8	15	0.938	13	2	0.125	18	1	0.063
4	1	0.688	9	14	0.875	14	13	0.813	19	8	0.500

(資料來源：周旭東等譯，2008)

為了避免亂數運算時產生出重複的數值，LCG 必須符合「全週期」（Full period）之條件，至於亂數序列則取決於隨機挑選的 a、c、m 三種數值，這樣才能夠產生更長的亂數，例如 a=c=1 時，數字序列相對就不夠「亂」，由此可知，就必須讓 m 值增大到一定程度，這樣亂數值及區間也會更大，這就是所謂的 m 值最大正整數。按照全週期之特性條件，LCG 需要滿足以下三列情況之特性（賴溪松等譯，2004）：

●m、c 兩者為互值。

●假設某一質數為 q，若 q 能夠除盡 m，則 q 就可以除盡 a-1。

●假如 4 能夠除盡 m，則 4 就可以除盡 a-1。

三、訊息摘要演算法

MD5 的是由 Rivest, R.（1992）所設計的訊息摘要演算法，常用於帳號的身分驗證、加強企業網路的安全性及電子商務的需求，可有效地防止盜用他人帳號。加密的原理是

將一個任意長度的字串轉換成一個 128bit 的整數長度，換句話說就是，不論何種加密的過程，運算結果都會成為另一固定的長度值。

舉例來說，以 512 位元或倍數為一個原始訊息的長度，第一個步驟是加入填入位元（Padding bit）至原始訊息中，也就是讓 512 位元減少 64 位元。

第二個步驟則是附加長度（主要是排除填入位元的長度，而只計算填入位元之前的長度），假如原始訊息為 1600 位元，加入一個 384 的填入位元，使其訊息長度為 2048（512 的倍數）再減少 64 位元，它的長度最後仍為 1600，而不是 1984 的長度，。

第三個步驟是設定 MD5 的初始值，將「需要進行雜湊的資料」分割成（A、B、C、D）四個暫存區的區塊（以十六進制值），暫存區設定如圖 2-12 所示：

A = 0X01234567
B = 0X89abcdef
C = 0Xfedcba98
D = 0X76543210

圖 2-12 初始化 Message digest 暫存區
(資料來源：Rivest, R.，1992)

第四個步驟是將一個非線性函數的公式導入至所有的區塊之中，經過多次程式迴圈運算及碰撞後，得其產生結果是 32 位元的整數資料，並由 16 進制所轉換的 MD5 碼，如圖 2-13 所示。

$$F(X,Y,Z) = (X \wedge Y) \vee (\neg X \wedge Z)$$
$$G(X,Y,Z) = (X \wedge Z) \vee (Y \wedge \neg Z)$$
$$H(X,Y,Z) = X \oplus Y \oplus Z$$
$$I(X,Y,Z) = Y \oplus (X \vee \neg Z)$$

$\oplus, \wedge, \vee, \neg$ 是 *XOR*, *AND*, *OR* , *NOT*的符號

圖 2-13 MD5 布林函數的運算公式
(資料來源：Rivest, R.，1992)

參、應用虛擬亂數對稱式區塊加密機制於帳密登入機制

一、研究架構

本研究「應用虛擬亂數對稱式區塊加密機制於帳密登入機制」，係將使用者於 PHP 網頁中所輸入的帳號及密碼做為本研究所提機制執行虛擬亂數所需之種子數值，種子數值藉以 AES 為基之加密技術及搭配線性同餘法虛擬亂數做為主要加密作業核心要素，為了加強密碼的複雜度，並混入了多種不同的功能模組之演算法來攪亂原先的種子數值；在加密的過程中，利用 C 語言程式隨機挑選加密機制所需功能模組演算法去產生一組密文密碼，此密文密碼無論使用者於註冊後、進行帳號登入之動作或是使用者不小心看到密文密碼的資料內容，也無法瞭解程式當初是採用何種模組及演算法做為基礎加密，並且於最後還會透過 PHP 內建 MD5 加密機制，將其密文密碼再一次雜湊運算並儲存在網頁伺服器的資料庫之中，此法不但可避免外部攻擊者竊取到密文密碼後，再次反解密成明文密碼，換句話說，多種加密演算法在邏輯複雜度並非一般正常人能夠反向推算。

如圖 3-1 所示，使用者藉由 PHP 網頁進行帳號及密碼註冊之動作，並於過程中將其密碼進行加密；如同加密過程中之架構所提及，至於如何將「PHP 頁面程式」、「加密模組之金鑰」、「網頁伺服器」相互搭配及運用，依照各項功能分述如下：

圖 3-1 使用者註冊時進行虛擬亂數產生器加密之流程圖
（資料來源：本研究整理製作）

(一)PHP 頁面程式

本研究 PHP 雛型程式主要是利用動態網頁的概念來應用於使用者與伺服器互動式的溝通，通常程式設計者會在網頁設計一個能夠輸入帳號及密碼的登入方框，使用者填入資料完畢並按下確認，會經由伺服器自動比對及確認使用者所填入的資料無誤後，伺服器將會傳回一個登入成功或是登入失敗的訊息給使用者端。主要撰寫網頁的核心語法是採用 PHP 語言，另外再搭配少部份 HTML（HyperText Markup Language）語法做一些簡易的程式呼叫及文字彈出視窗，讓網頁能以多樣化的視覺化方式來呈現畫面。

PHP 自身具備各項功能模組，可延伸於各種系統及軟體，如下所述：

- 「相容性高」：
  PHP 可建置在各項作業系統上，例如 Linux、Microsoft Windows、MacOS 等都能夠正常運作。PHP 本身也能使用在許多知名的網頁伺服器上，如 Apache、Microsoft Internet Information Server、Joomla!及 Xitami 等，並且還具備輸出 CSV、XML 及 TXT 等各種文字檔之功用。
- 「呼叫外部程式」：
  PHP 內建函數語法，可執行副檔名「.exe」、「.bat」及「txt」等檔案。
- 「連結資料庫」：
  PHP 內建函數語法，可連結 MySQL 及 Microsoft SQL Server 等資料庫軟體。
- 「內建 MD5 加密演算法」：
  PHP 本身內建 MD5 單向加密演算法，可將其文字進行雜湊運算，但不可以反向解密。

(二)加密模組之金鑰

建置在帳號登入的網頁系統，使用者通常於註冊時所輸入的密碼複雜度，相較之下組合排序都相當簡單；普遍來說，是由英數大小寫及部份特殊符號搭配混合，而且具有規則性並容易猜測。本研究為了有效地強化密碼的複雜度，透過虛擬亂數產生器的程式將其密碼加密，額外產生一組密文密碼，如圖 3-2 所示，帳號代碼為「A」、密碼代碼為「B」、虛擬亂數產生器代碼為「X」；加密過程中程式會將「A+B」的字串資料帶進「X」去處理，如後續第三章第二節所提，X 會搭配各種加密模組的演算法，代碼稱之為「Y」，X 會從 Y 隨機挑選[Y_0,Y_1,Y_2,Y_3,Y_4,Y_5,Y_6]等模組，最後於資料夾中產生一組代碼為「Z」的密文金鑰檔。

圖 3-2 密文金鑰檔產生之流程圖
（資料來源：本研究整理製作）

(三)網頁伺服器

以 Windows 作業系統為網頁伺服器之底層，至於架站工具分別為「Apache Server」、「PHP 程式語言」及「MySQL 資料庫」等三套應用程式軟體，安裝過程及設定數據都是採用系統預設值，唯一需要特別調校的設定為 MySQL 資料庫的欄位(Schema)結構；依照本研究之系統架構，需新增一組「account」和一組「password」varchar 欄位設定，主要是負責儲存使用者註冊時的帳號及密碼之用。

二、加密模組說明

加密模組可區分為兩種特性，架構在區塊加密的「取代」（Substitution）與「換位」（Transposition）應用這兩種概念作延伸變化：

- 「取代」：主要功能模組是將明文密碼置換成不同的 ASCII（American Standard Code for Information Interchange）內碼，使原先內容變得無法辨識；置換模式區分為以下三種「一個位元組置換運算」、「兩個位元置換運算法」、「四個位元置換運算法」。
- 「換位」：主要功能是將明文密碼內容攪亂，透過位置轉換及各種移動方式，重新排序明文資料位元組；攪亂模式區分為以下三種「一維陣列攪亂運算法」、「二維陣列位移量攪亂運算法」、「X 軸與 Y 軸座標交換處理」。

(一)「一個位元組置換運算」功能模組

此功能模組之攪亂運算方式，是藉由明文資料在位元之間作「位元位置」之間的相互置換，透過使用者輸入參數所產生的虛擬亂數，建立一個 16*16 位元組之二維矩陣，二維矩陣數值內容為（0-255）總共 256 個位元。這 256 個位元會隨機擺放在二維陣列置換之對照表中，明文裡每一個位元組之 16 進位 ASCII 內碼作為置換對照表，如圖 3-3 所描述，將其並註標成「行、列」，最後透過明文字元相對應之密文置換內容，將其明文及密文作置換的工作。置換對照表所產生的內容為 16*16 位元組，可採用之置換表內容共有 256！（8.57817775342842654119082271681 23e+506）種方式可做置換。

(二)「二個位元置換運算」功能模組

此功能模組之攪亂運算方式同上述「一個位元組置換運算」之理論，主要是建立一個 2*2 位元之二維矩陣對照表，數值內容只有（0-3）總共 4 個位元，也是由虛擬亂數隨機排列而組成。置換時會將區塊中各個資料轉換成 8 個位元為一個單位，然後以 2 個位元數成為一組做置換單位，經由「置換對照表」所定義之內容作註標「行、列」，依序置換整個位元組相對應之密文置換內容。

(三)「四個位元置換運算」功能模組

置換方式同上述的「二個位元置換運算」，依據使用者所輸入參數隨機產生之虛擬亂數，建立一個 4*4 位元之二維矩陣對照表，對照表內容為（0-15）總共 16 個位元，置換單位則是以 4 個位元數為一組，如圖 3-5 所描述。明文資料之 A 數據為 41，經過 2

進制轉換後，A 數據則置換為（0100，0001），再次參照置換對照表之內容，將其數據資料轉換成 16 進制（0010，0111），密文資料之 A 數據最後結果為 27。

(四)「一維陣列攪亂運算」功能模組

攪亂運算與上述的置換運算有很大的不同，攪亂運算是將 256 個位元組所組成的明文區塊依序排列成一維陣列之結構，然後依照虛擬亂數將一維陣列上的明文資料重新排列位置，最後回復成區塊資料的狀態。在此以 4*4 位元組區塊資料為範例，如圖 3-6 所表示，模組在加密時會先將區塊資料轉換為一維陣列，在經過虛擬亂數重排此一維陣列，最後將攪亂過的一維陣列重新組合成 4*4 位元組之密文資料區塊，例如：某區塊內容依序排列為[A,B,C,D]、[E,F,G,H]、[I,J,K,L]、[M,N,O,Q]，然而將其轉換成「一維陣列」，結果則會呈現[A,B,C,D,E,F,G,H,I,J,K,L,M,N,O,Q]，進而透過攪亂運算方式做「重新排列」，區塊順序則會改變成[J,G,N,D,H,O,C,M,L,I,A,L,F,B,Q,E] ，之後再將一維陣列置換成密文區塊，得到[J,G,N,D]、[H,O,C,M]、[L,I,A,K]、[F,B,Q,E]之結果。

(五)「二維陣列位移量攪亂運算」功能模組

運作方式共有「行位移量陣列（向上攪亂）」、「列位移量陣列（向右攪亂）」與「雙對角線位移量陣列（左上右下對角線攪亂及右上左下對角線攪亂）」，運用「位移方向」不變，但「位移量」改變之方式來達到資料區塊攪亂之目的，區塊中各行、各列攪亂位移量的多寡均由虛擬亂數與資料區塊同餘計算所產生。位移方式描述如後：

●行位移量陣列（向上攪亂）：

假設欲加密之明文區塊陣列，某行內容為[C0,C1,C2,C3,C4,C5,C6,C7]，若攪亂位移量為 3，則陣列內之資料位元組向上移動 3 格，結果將攪亂成[C3,C4,C5,C6,C7,C0,C1,C2]狀態。

●列位移量陣列（向右攪亂）：

假設欲加密之明文區塊陣列，某列內容為[R0,R1,R2,R3,R4,R5,R6,R7]，若攪亂位移量為 4，陣列內之資料位元組向右移動 4 格，攪亂成[R4,R5,R6,R7,R0,R1,R2,R3]狀態。

●雙對角線位移量陣列（左上右下對角線攪亂）：

將欲加密之明文資料區塊，取其左上到右下的對角線區塊，內容為[DL0,DL1,DL2,DL3,DL4,DL5,DL6,DL7]，以此對角線為基準，若攪亂位移量為 3，則陣列內之位元組沿對角線向左上方移動 3 格，攪亂成[DL3,DL4,DL5,DL6,DL7,DL0,DL1,DL2]狀態。

●雙對角線位移量陣列（右上左下對角線攪亂）：

運作方法同上，取明文資料區塊右上至左下的對角線區塊，內容為[DR0,DR1,DR2,DR3,DR4,DR5,DR6,DR7]，若攪亂位移量為 3，則位元組向右上方移動 3 格，攪亂成[DR4,DR5,DR6,DR7,DR0,DR1,DR2,DR3]狀態。

(六)「X 軸與 Y 軸座標交換處理」功能模組

選擇明文區塊陣列對角線[A(0,0),F(1,1),K(2,2),P(3,3)]，再分別將對角線兩邊元素對換。

肆、雛型程式建置與實作分析結果

一、雛型程式設計

本研究之雛型系統架構，如圖 4-1 所示，作業系統是以 Windows 7 為建置平台，並搭配 Apache Server 軟體加上 MySQL 資料庫做為網頁伺服器之介面平台，軟體工具會採用 PHP 語言來設計帳號及密碼的登入，並且以網頁的方式來呈現帳號登入成功或是失敗的畫面，至於主要的核心程式則是以 C 語言為基，透過 C 語言的雛型程式將「虛擬亂數

對稱式區塊加密機制」及各種加密演算法導進程式之中，而 C 語言本身處理核心速度快、

程式相容性較高及可攜帶性等各項優點之特點，即使介於不同程式語言亦能相互配合且操作執行。

圖 4-1 系統架構與程式應用

(資料來源:本研究整理)

(一)核心程式

程式主要分成兩個架構，分別是：「以 C 語言撰寫程式碼之虛擬亂數區塊加密核心程式」與「PHP 撰寫程式碼之雛型網頁系統」，主要是讓 PHP 網頁架構能藉由 C 語言的雛形程式去展現密碼強化之效果。

核心程式的操作流程依序係將使用者從 PHP 網頁上所輸入的「帳號」及「明文密碼」，透過具有「虛擬亂數與線性同餘法」及六種「加密功能運算模組」的加密程式將輸入的帳號及明文密碼合併，於處理的過程中會在應用「虛擬亂數對稱式區塊加密機制」之研究理論去攪亂明文資料，最後產生一組密文金鑰檔。

(二)加密轉換機制

延續上節所描述其結果，經過加密的資料會需要在核心程式實施前注意三個步驟，相關步驟之說明如下：

- 輸入「帳號與密碼」：PHP 程式會要求「帳號」單位代碼長度為 4 碼以上，而「密碼」長度是 8 碼以上，輸入密碼之原則亦需符合密碼強度及複雜度之要；在本研究的帳號及密碼定義，一般使用者的帳號密碼會禁止輸入某部分的特殊符號，例如：「單引號」、「雙引號」、「分號」、「頓號」、「正反斜線」、「冒號」、「星號」、「豎號」等特殊符號，這樣做是可避免程式語言在互相溝通時，某些特殊符號會被程式底層判斷成語法錯誤，所以基本上建議輸入參數時，仍以英文大小寫及數字為基才較有可行性。
- 核心程式檔案是由 C 語言所撰寫虛擬亂數對稱式區塊加密程式，進行登入密碼加密時，將依據密碼本身的字元內容加以轉換做為虛擬亂數對稱式區塊加密程式挑選加密功能模組及挑選所需相關參數設定的依據，然後進行密碼攪亂作業；最後程式執行完成後會產生一個副檔名「*.txt」的密文金鑰，資料裡頭會是一組由 ASCII（字碼 0-255）所呈現的密碼，相關資料文件可參考附錄 A。
- 延續步驟一、二所描述，ASCII（字碼 1-127）包含「單引號」、「雙引號」、「分號」、「正反斜線」等特殊符號，以及 ASCII（字碼 128-255）許多特殊符號在 C 語言與 MySQL 資料庫之間溝通時，這些特殊符號會被程式判定成語法錯誤，這時藉由 PHP 的 MD5 訊息摘要演算法再次進行雜湊運算，可將特殊符號及無法識別的內碼轉換成 16 進位來表示，換句話說，將原先所輸入的密碼多一次強化。

二、雛型系統實作

本研究預計實作主程式以 PHP 語言撰寫「帳號及密碼平台登入程式」為主要網頁的顯示介面，加密模組程式則是透過 C 語言核心程式「隨機加密模組程式」，執行並將其所產生的密文資料會與 MySQL 資料庫先前所儲存的密碼作比對，若比對成功將會顯示帳號登入成功，如果使用者的密碼輸入錯誤，程式將會回到原先帳號登入之頁面。

(一)註冊帳號

利用本研究之雛型程式於事前註冊一組使用者的帳號及密碼在 MySQL 資料庫之中，因此，在註冊帳號之前，使用者必須先登入 PHP 的註冊網頁，並填入新帳號和新密碼，若是填入的帳號少於 4 碼的長度，系統將會出現「會員帳號需大於 4 個字」之彈出視窗，如圖 4-2 所示。

圖 4-2 會員帳號未符合單位長度

(資料來源:本研究整理)

若是輸入的密碼長度少於 8 碼，將會出現「會員密碼需大於 8 個字」之彈出視窗，如圖 4-3 所示。

圖 4-3 會員密碼未符合單位長度

(資料來源:本研究整理)

當帳號及密碼符合註冊時程式所訂定的規則後，就可以按下「會員註冊」的按鈕進行註冊，接著會於網頁上顯示「註冊成功」的畫面來表示使用者已經完成註冊的動作；

事先提醒，測試帳號是以帳號名稱「abcd」、密碼「xxxxxxxx」為例，並做為後續實作的主要範例，如圖 4-4 所示。

圖 4-4 帳號註冊成功之畫面
(資料來源:本研究整理)

當使用者完成註冊的程序後，可從 MySQL 資料庫的欄位看到新註冊的帳號及 MD5 加密過的密碼，如圖 4-5 所示。

圖 4-5 於 MySQL 新增一個帳號之畫面
(資料來源:本研究整理)

根據上述的操作步驟，最後在使用者的資料夾中，可看到一個帶有使用者帳號「.txt」的文件檔，例如：abcd.txt；文件內容將會是透過 C 語言的核心程式加密，產生一組由 ASCII 所排列的密文資料，如圖 4-6 所示。

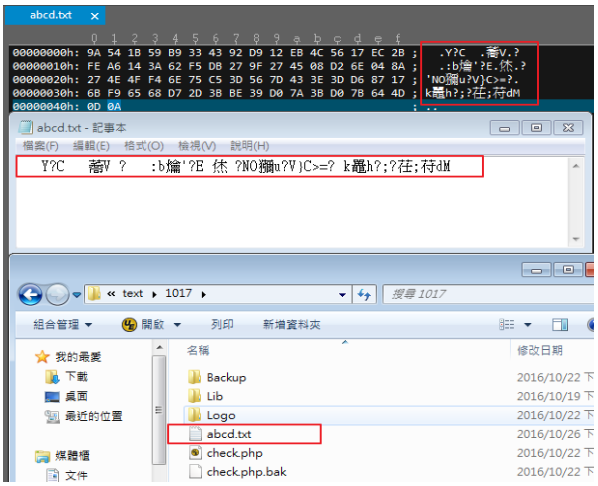


圖 4-6 密文金鑰檔及 16 進制之內容
(資料來源:本研究整理)

(二)帳號登入驗證

使用者如果已經完成帳號註冊的步驟，後續步驟是用來確認使用者註冊的帳號及密碼是否正確，如 4.2.1 小節所描述，執行過程中會產生一個「abcd.txt」的文件檔在資料夾之中；當使用者於登入畫面輸入帳號「abcd」及密碼「xxxxxxxx」，接著按下「會員登入」的按鈕，網頁上就會出現「登入成功」之文字畫面，如圖 4-7 所示。

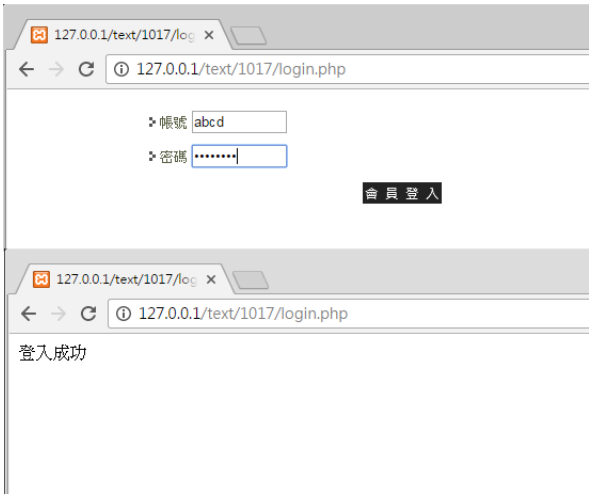


圖 4-7 帳號登入成功之畫面
(資料來源:本研究整理)

(三)MD5 密碼驗證

延續第(一)小節所描述，當使用者在進行帳號註冊的同時，ASCII 的密文資料會被 PHP 讀取並暫存至記憶體，接著透過 PHP 內建的 MD5 加密運算模組，將攪亂過的 ASCII 字碼，轉換成 16 進制的 32 個整數，產生其結果僅儲存於 MySQL 資料庫裡；至於本研究主要目的是在「帳號平台登入程式」進行實作測試，雛型系統實際上也是模擬一般對外連線的網頁伺服器，因此，「密碼」基於資訊安全之顧慮，本身是不可被反向推算及還原成明文的資料，所以，此次實作是為了驗證 MySQL 資料庫的 MD5 密碼之正確性，並確認轉換前的資料來源是否由資料夾的密文資料所提供，在執行的過程，PHP 網頁僅輸入使用者帳號「abcd」，按下「密碼驗證」後，會直接讀取資料夾「abcd.txt」的文件內容，後續 ASCII 字碼會經由 MD5 加密模組的轉換，而變成 16 進制的 32 個整數。爾後，將其結果與 MySQL 資料庫做比對，如圖 4-8 所示。

圖 4-8 密文資料經由 MD5 加密之結果
(資料來源:本研究整理)

三、系統實作結果分析

(一)驗證帳號/密碼之特殊符號

避免使用者在註冊時會有輸入到特殊符號之情形，已從 PHP 程式語言先行定義某些特殊符號之限制條件，若是使用者這時卻輸入已被限制的特殊符號，將會彈出「請輸入正確的會員帳號，不可包含特殊符號!」之視窗，而此次實作範例是以「單引號」做表示，如圖 4-9 所示。

圖 4-9 網頁程式強制帳號去輸入特殊符號
(資料來源:本研究整理)

使用者本身並非只在帳號的欄位輸入特殊符號，基於密碼創意度及密碼強度之考量，使用者也有可能在密碼的欄位輸入特殊符號；另外，避免使用者在輸入密碼的同時，被有心人士看到明碼，因此，程式將密碼的明碼轉成暗碼來顯示，此次實作範例是在密碼欄位輸入「斜線」，如圖 4-10 所示。

圖 4-10 網頁程式強制密碼去輸入特殊符號

(資料來源:本研究整理)

(二)驗證帳號/密碼之重覆註冊

考量使用者在註冊新帳號時，想取名的帳號已被其他人註冊過，避免註冊帳號有此情況發生，於 PHP 雛型程式仍然設計了帳號比對的功能，如圖 4-11 所示。

圖 4-11 通知使用者帳號已被註冊之畫面

(資料來源:本研究整理)

(三)驗證帳號/密碼之最大長度限制

延續前述，使用者帳號長度不可少於 4 碼、密碼長度不可少於 8 碼，主要原因是為了防止帳號及密碼被輕易猜到，另外一個角度去思考，帳號及密碼的長度若是超過 25 碼，使用者久而久之就會有遺忘的情形，避免此種問題發生，在程式裡已設計帳號及密碼的最大長度限制。

圖 4-12 帳號及密碼最大長度限制

(資料來源:本研究整理)

(四)密文資料攪亂之分析總結

以本研究所提之虛擬亂數對稱式區塊加密機制為例，核心程式是透過 C 語言所撰寫的一個「.exe」執行檔，於執行檔後方空一格，帶入帳號「A」的參數，接著空一格，帶入密碼「B」的參數，如圖 4-13 所示。

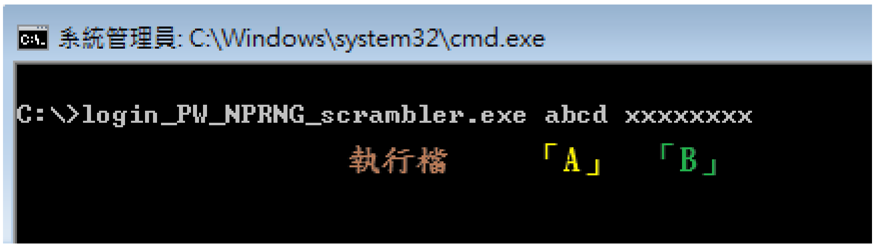


圖 4-13 帳號及密碼最大長度限制

(資料來源:本研究整理)

將「A」與「B」兩個參數合併，透過 PRNG 的核心程式攪亂明文資料，在資料夾中會產生一組密文金鑰檔，如圖 4-14 所示。

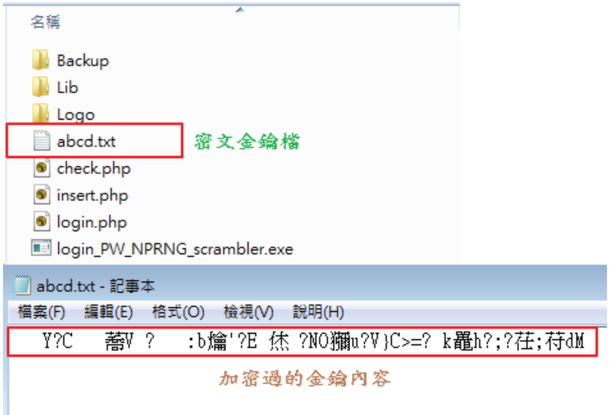


圖 4-14 密文金鑰檔的檔案格式與金鑰內容

(資料來源:本研究整理)

本研究藉由複雜的加密機制去強化密碼的理念，針對不同條件所產生的密文資料進行多次確認及驗證，利用實作的方式蒐整相關數據，如表 4-1 所示，即使帳號「取名相似」、「同英文字母但數量不同」、「純阿拉伯數字」、「英文與數字合併」之條件，加上密碼取名相同，到最後所產生的密文資料仍不盡相同且差異相當大。

表 4-1 核心程式實施不同帳號、密碼一致之密文資料對照表

帳號	密碼	密文資料
abcd	xxxxxxxx	Y?C 蕎V ? :b熗'?E 怺 ?NO攞u?V}C>=? k龍h?;?荏;荇dM
abcde	xxxxxxxx	鷗 ??r話?$;?Cs ?}?
abcdef	xxxxxxxx	?梄^?? 蕻g u示?腡盡猗 ?它? 弟? ? ?ﾓ瘮??Q?<,
abcdefg	xxxxxxxx	? M?緎8菹怌鴘 5G醲 l}縻3 1︾禦燚揹"M?樞 ?3a梧4 翆輐
aaaa	xxxxxxxx	?> B
aaaaa	xxxxxxxx	{ &蝖m? ;;黍?遏j?u27~糴>壽 !宇 {5Q?tHz l烇PO?:D孍?
aaaaaa	xxxxxxxx	瓠}L嵕 蚜, L9 D?部 ?hB?R轇 . J? < ?欣 d8q[搜捊`)菡
aaaaaaa	xxxxxxxx	4d淤 GE緼Y40\?烓P ?擁:唄d]?\?{7M ??O乂???iE 祚] ?
1234	xxxxxxxx	X鴃 K皒?鑿FOZ B @
12345	xxxxxxxx	??d?qn] ?}? ' ?E Ur闢? S %G^孌疪?3 ? ? 巳
123456	xxxxxxxx	R?V4 麱R??,BvDl?篠F" U鵊?躓繖 o財 掀蘺Q? ? S?焠?摟r
1234567	xxxxxxxx	&壇a ? ?囫 J *J?)<稔蔆 帙?a?E 恷t? g$? S
abcd1	xxxxxxxx	?'?y~ ?+? &擒鸏P濔T劢?- um. ?嚚C<'蕵? 2 棐 呯3? BC^`
abcd2	xxxxxxxx	EQ驝鬆腓鏫袮s9Q饑!i E? k:lR }輒掁?揗> 鐢~\ j J尒?r?z
abcd3	xxxxxxxx	?h??h h禴$??嘓<?Lj$A穡?? ?Z3?噥?靨Pm? ,? 鷙鉩f?
abcd4	xxxxxxxx	?梄^?? 蕻g u示?腡盡猗 ?它? 弟? ? ?ﾓ瘮??Q?<,

(五)密文資料反解密之分析

如上節所驗證之結果，如何確認本研究之密文資料是無法被反推回原先所定義的明文密碼，這裡參考彩虹表著名的破解工具 ophcrack 之官方網站，如圖 4-15 所示，Table 裡儲存著能在 Windows 7 執行的破解密碼表，檔案由小排列至大，單位從 461MB 到 2TB 不等。

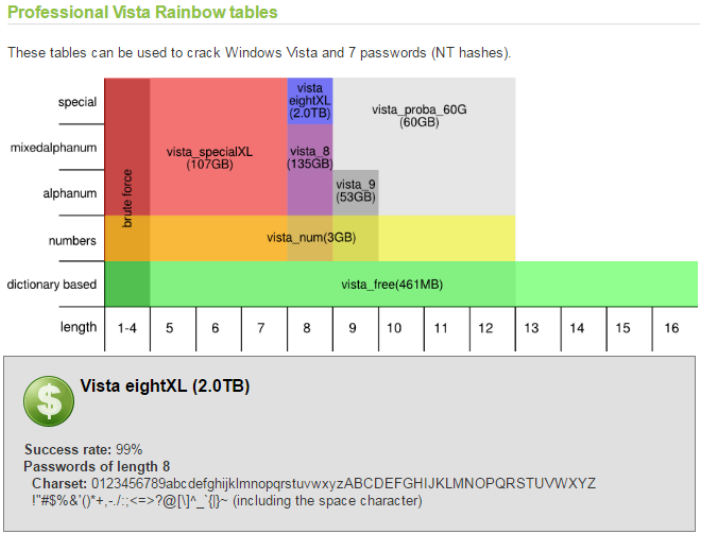


圖 4-15 ophcrack Professional Vista Rainbow tables

(資料來源：ophcrack 官方網站)

在 2TB 視窗內容所描述的資訊，可看到被破解的編碼定義為「012345 6789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~」等 95 種的明碼所組合而成的編碼表。可是參照本研究 4.1.2 節所定義的加密機制之編碼範圍是 ASCII（字碼 0-255），如附錄 A 所示，於後段字碼(128-255)的字元，通常在編碼已經被定義為隱碼。由此可知，現有的破解工具，並非加入了(字碼 128-255)的內碼，也因此無法透過工具長時間將本研究 MD5 所轉換的編碼，再次反推回經過隨機加密機制轉換的密文資料。

另一種知名彩虹表的破解工具，稱之為「RainbowCrack」，反解密的方式跟 ophcrack 相似，將經過加密運算的編碼也是儲存成一張表清單，如圖 4-16 所示，Table 裡儲存著能在 Windows 7 執行的破解密碼表，檔案由小排列至大，單位從 52GB 到 690GB 不等。

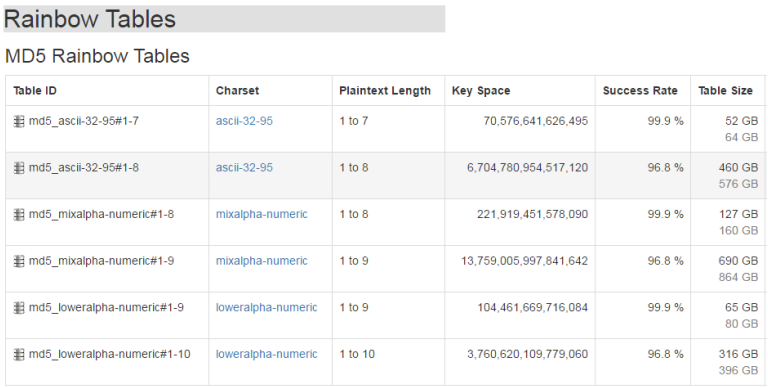


圖 4-16 MD5 Rainbow Tables

(資料來源：RainbowCrack 官方網站)

之後點進 Charset 的連結位置，就會顯示 RainbowCrack 的編碼字元列表，如圖 4-17 所示，看到被破解的編碼定義總共有 95 種的明碼字元，包含

「 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~ 」這些可辨識的字元也是屬於 ASCII（字碼 0-127）前段的編碼。由此推論，就能再次證明本研究於密碼加密機制加了隱碼字元的選擇，即使 Rainbow Table 破解工具在長時間也是無法反推回原先經過加密機制的明文密碼。

```
# This is the charset definition file for RainbowCrack.
# Each charset is defined in one line, with the characters of the charset enclosed by "[" and "]".

numeric            = [0123456789]

alpha              = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
alpha-numeric      = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]

loweralpha         = [abcdefghijklmnopqrstuvwxyz]
loweralpha-numeric = [abcdefghijklmnopqrstuvwxyz0123456789]

mixalpha           = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]
mixalpha-numeric   = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]

# The charset "ascii-32-95" includes all 95 characters on standard US keyboard
ascii-32-95                 = [ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~]
ascii-32-65-123-4           = [ !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`{|}~]
alpha-numeric-symbol32-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]
```

圖 4-17 MD5 Rainbow Tables Charset

(資料來源：RainbowCrack 官方網站)

伍、結論與未來研究方向

本研究是採用應用虛擬亂數對稱式區塊加密機制之基礎，加密機制則是應用 AES 加密法為主體，加密核心功能是以置換、位移、攪亂、座標交換等六種運算模組為輔，另外使用軟體工具 PHP 程式語言、Apache 網站伺服器及 MySQL 資料庫所撰寫帳密登入機制的登入畫面，並透過虛擬亂數產生器於密碼之間做加密轉換，而運算過程中所得到之密文金鑰，會於使用者和網頁伺服器交談時，將其密文金鑰之內容利用 PHP 程式語言所內建的 MD5 功能模組進行雜湊運算，經過系統計算後會產生一組不具意義 64 位元的雜湊值，最後才將其數值儲存至 MySQL 資料庫中；藉由實作的測試結果並彙齊相關數據，做為本研究探討強化使用者密碼在網頁伺服器之依據。

經由分析實作結果，本研究發現不同的使用者在註冊時所產生的密文密碼，會因填入的英文數字名稱些許的不同，產生無法辨識且差異性過大的亂數密碼，後續再次利用 MD5 訊息摘要演算法產生出一組 16 進制的密碼，儲存至網站伺服器之中。若駭客及系統管理員竊取到 MySQL 資料庫的整串編碼，也因密文資料為 ASCII 隱碼，最後仍然是無法反向推算及還原成使用者在註冊時所填入的明文密碼。

綜觀上述分析比較說明，本研究的加密機制優於一般網站程式所內建的加密法，單一加密機制其意味著密碼被暴力破解法攻破的風險，也無法提高網站的安全性。

參考文獻

中文部分

王小鑑、廖曉峰、黃宏宇，2013，基於歸約函數數量裁減的彩虹表技術改進。

巫坤品、王青青譯，2004，William Stallings 原著，密碼學與網路安全原理與實務，第三版，碁峰出版股份有限公司。

林則孟，2001，系統模擬理論與應用，滄海書局。

周旭東、傅振華，2008，「應用變形 LCG 虛擬亂數機制於資料串流加密之研究」，第十六屆國防管理學術暨實務研討會與國防軍備管理年會。

陳祥輝，2009，TCP/IP 網路通訊協定，滄海書局。

陳宏仁，2012，應用虛擬亂數與動態資料攪亂模組於對稱式加密機制之研究，國防大學碩士論文。

陳易佑，2010，以虛擬亂數為基動態變化方式之對稱式區塊加密機制研究，國防大學碩士論文。

楊政穎譯，Atul Kahate 原著，2007，網路安全與密碼學，美商麥羅格。希爾國際股份有限公司。

楊宗偉，2008，密碼學的發展與應用，靜宜大學應用數學研究所學位論文，1～58頁。

楊欽舜，2008，「應用 GPS 資訊於虛擬亂數為基之對稱式區塊加密機制研究」碩士論文。

賴溪松、韓亮、張真誠，近代密碼學及其應用，台北:旗標出版股份有限公司，2004。

賴榮樞譯，William Stallings 原著，2007，密碼學與網路安全第四版，香港：培生教育出版亞洲股份有限公司。

鍾慶豐，2005，近代密碼學與其應用，儒林圖書公司。

英文部分

Biham, E., & Knudsen, L. R. (1998). *Cryptanalysis of the ANSI X9. 52 CBCM Mode* (pp. 100-111). Springer Berlin Heidelberg.

Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. *Journal of CRYPTOLOGY*, *4*(1), 3-72.

Daemen, J., & Rijmen, V. (1999). AES proposal: Rijndael.

Diffie, W., & Hellman, M. E. (1977). Special feature exhaustive cryptanalysis of the NBS data encryption standard. *Computer*, (6), 74-84.

Feistel, H. (1973). Cryptography and computer privacy. *Scientific american*,*228*, 15-23.

Kuo, C. J. E-mail: jimkuo@aa.nctu.edu.tw Graduate Institute of Communication Engineering National Taiwan University, Taipei, Taiwan, ROC.

Lehmer, D. H. (1951). Mathematical methods in large-scale computing units. In*Proc. 2nd Symp. on Large-Scale Digital Calculating Machinery* (pp. 141-146). Harvard Univ. Press Cambridge, MA.

Maiwald, E. (2001). *Network security: a beginner's guide*. McGraw-Hill Professional.

Rivest, R. (1992). The MD5 message-digest algorithm.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120-126.

Shannon, C. E. (1949). Communication theory of secrecy systems*. *Bell system technical journal*, *28*(4), 656-715.

William, S., & Stallings, W. (2006). *Cryptography and Network Security, 4/E*. Pearson Education India.

Yan, S. Y. (2007). Modern Cryptography. *Computational Number Theory and Modern Cryptography*, 263-263.

網路部分

彩虹表，參考網址：https://zh.wikipedia.org/wiki/%E5%BD%A9%E8%99%B9%E8%A1%A8 [visited in 2016/6/14]

ASCII 字元碼，參考網址：https://msdn.microsoft.com/zh-tw/library/4z4t9ed1%20(v=vs.80).aspx [visited in 2016/8/22]

MD5 訊息摘要演算法，參考網址：https://zh.wikipedia.org [visited in 2016/9/15]

Aamir Majeed Usman Aziz Salman Ul Haq, Jawad Masood. Bulk encryption on GPUs, (available online at http://developer.amd.com/ resources/documentation-articles/articles-whitepapers/bulkencryption-on-gpus/ [visited in 2015/10/2]

Ophcrack (available online at http://ophcrack.sourceforge.net/tables.php [visited in 2015/8/27]

RainbowCrack (available online at http://project- rainbowcrack.com/ table.htm [visited in 2015/8/28]

3D 地理資訊系統（GIS）導入空軍自動化防空系統建置之研究

李建鵬[a] 范姜群智[b]

[a]國防大學管理學院
[b]國防大學空軍指揮參謀學院

摘要

隨著科技進步，各種空間關聯產業分析均已運用地理資訊系統（GIS）來輔助，藉以得出更佳的判斷成果，而為了能以迅速、直接且動態的方式認知空間，3維的概念更是不可或缺的要素。現行空軍自動化防空指管系統，雖具備基本地形圖資資料，惟相關地圖情資在系統上均以2D方式呈現，亦無相關資訊可供查詢，如可利用3D地理資訊系統（GIS）之優點，即可幫助戰術管制人員及飛行員先期掌握執行任務路徑、地貌地物概況，並彌補視覺效果、3D概念的不足。

本研究係由影響3D 地理資訊系統（GIS）導入空軍自動化防空系統建置之關鍵成功因素，分析空軍在執行空軍自動化防空系統性能提升作業時所應考慮因素，以提供相關單位擬定系統後續建案規劃決策參考。

關鍵詞：地理資訊系統、空軍自動化防空系統、3D GIS、C^4ISR

3D Geographic Information System Used in Air Force Automation Air Defense System

Chien-Peng Lee[a] Chun-Chih. Fan Chiang[b]

1.[a] Management College, National Defense University,Taiwan, R.O.C.

[b] Air Command and Staff College, National Defense University, Taiwan, R.O.C.

Abstract

As the progress of science and technology, Geographic Information Systems (GIS) has been used by the variety of industries which relate to geospatial analysis. In order to acquire more quickly, precisely analyzing, and to explore or recognize the spatial data, the Three Dimensional (3D) implementation GIS is the essential element. The current Air Force Automation Air Defense System although with basic terrain map capital information, but the relevant map information in the system are presented in 2D way, and no relevant information for inquiries, if current Air Force Automation Air Defense System (AADS) takes advantage of 3D Geographic Information System (GIS), the tactical control personnel and pilots will aware of the fly path with the area terrain in advance, and acquire more stereoscopic visual acuity and relief map concept.

This study is to explore the Critical Success Factors (CSF) of 3D GIS implementation of Air Force AADS, and to provide the planning decision-making reference for the investment of AADS enhancement in the future.

Keywords: Geographic Information System, Air Force Automation Air Defense System, 3D GIS, C^4ISR

壹、緒論

一、研究背景與動機

(一)研究背景

地理資訊系統（GIS），以狹義而言，是一種可整合處理地理空間資訊及其相關描述資訊的電腦軟體，並且可進行視覺化、操作、分析及展現地理資料（包含空間及相關描述資訊），而以廣義而言，地理資訊系統為結合電腦軟體、硬體、地理資料、專業人員及作業程序等五大要素，藉以執行效率化的資料蒐集、儲存、更新、處理、分析及展現各種地理相關資訊。

地理資訊系統做為一個空間資訊處理及管理的系統，對國防軍事應用而言是非常具有實用價值的系統。美軍早在1980年代即已利用地理資訊系統來協助進行空間分析等軍事應用，例如1982年，美國陸軍便開發了一套名為GRASS（Geographic Resources Analysis Support System）的地理資訊系統，而美軍在圖資生產部分亦運用了地理資訊系統，在整體規劃中除了有良好的生產維護機制外，在資料的供應上更是多元化（包括數值圖與紙圖等），資料的供應採取標準化的規格，能密切的與武器系統整合，發揮更大的綜效。

而科技時代持續演進，為了呈現真實的世界，越來越多的應用期望能以三維的空間來表現與處理問題，著名的搜尋引擎Google在2005年由於Google Map/Earth的問世（如圖1），更為GIS帶來了震撼的衝擊，3D GIS已經是現在地理資訊系統中的熱門主題。國內GIS領域包括學術、政府、軍事機關以及業界對 3D GIS也已逐步的由理論的建構發展至實作與應用的階段。

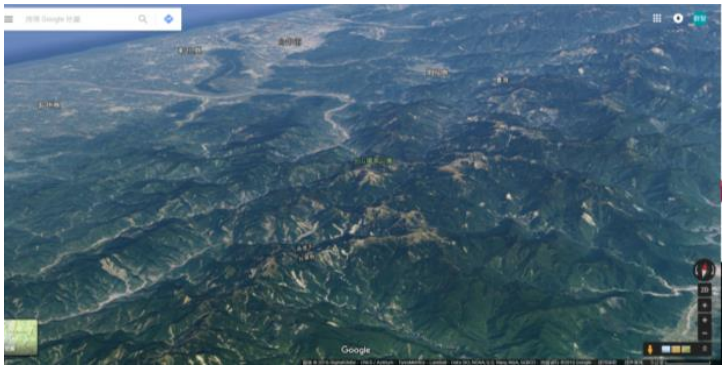


圖 1 Google Map/Earth所繪製之 3D 臺灣中央山脈地勢圖

反觀現行空軍自動化防空指管系統，雖具備基本地形圖資資料，惟相關地圖情資在系統上均以2D方式呈現，亦無相關資訊可供查詢，如可利用3D地理資訊系統（GIS）之優點，即可幫助戰術管制人員及飛行員先期掌握執行任務地標路徑、周圍之地貌地物、概況，並彌補視覺效果、3D概念的不足，並強化任務勤前提示整備及飛行完成後的歸詢檢討，藉以提升訓練成效，另可於飛安事故發生利用地理圖資加強搜救研判，對於空軍自動防空系統實有相當之助益。

(二)研究動機

空軍新一代防空系統於建置時期，以提升系統功、效能為主要考量，故並未針對地理圖資功能多加著墨，於系統運作後，人員對於地理圖資之需求陸續產生，而圖資不利人員判讀、無法以視覺化方式獲知地貌概況等系統運用問題亦相繼出現。在現行地理圖資支援不足的情況下，空軍自動化防空系統未來之提升建案是否仍維持2D地理圖資，或是與時俱進導入3D地理資訊系統（GIS），徹底解決日後圖資判讀、地物辨識、任務地貌認知等問題，提升系統運用功能，確保系統支援戰、演、訓任務順遂，為本研究之研究動機。

二、研究目的

本研究係藉由3D地理資訊系統（GIS）導入空軍自動化防空系統建置上，評估建置時主要需考量之指標，並藉由收集各單位之戰管人員及系統維護專家人員經驗與專業意見，進一步執行歸納、整理及篩選，期能達到目的如下：

(一)探討空軍自動化防空系統建置導入3D地理資訊系統與維持2D系統圖資之優缺點，藉以解決系統使用人員對於圖資判讀、地物辨識、地貌認知等運用問題。

(二)分析影響3D地理資訊系統導入空軍自動化防空系統建置各關鍵成功因素之影響權重，於擬訂關鍵之評選指標與整體架構後，依各單位專家針對自動化防空系統運用、建案經歷或建構其他資訊系統所遇經驗，決定需考量之主要層面與指標的權重，進而針對各位專家所提供得出之結果，探討分析各指標間對3D地理資訊系統導入空軍自動化防空系統建置之相對重要程度。

(三)依據研究結果，對空軍自動化防空系統相關建案使用及維護單位提出具體建議，以提供相關單位擬定空軍自動化防空系統後續建案規劃決策參考。

貳、文獻探討

一、地理資訊系統定義

地理資訊系統，顧名思義是由地理、資訊以及應用系統所架構而成，英文全名為Geographic Information System，一般簡稱GIS。地理資訊系統是一門整合下的科學，它的核心技術整合了地理、數學、測量學、電腦科學等，GIS 是一種處理空間資訊的系統，其具備同時處理空間資料及資料庫管理功能，而其應用領域除了製作地圖之外，幾乎包含所有地表上下可見之事物，如土地利用、資源保育、污染防治等等。地理資訊系統可以結合網際網路、全球定位系統（Global Positioning System，GPS）、專家系統、人工智慧、決策資源系統及其他有關空間資訊的工具，GIS 是一門跨領域、跨平台的科學，所以GIS亦有人建議稱為Geographic Information Science。

國外學者對於地理資訊系統亦有許多定義，詳如表一所示：

第一章表 1 GIS 定義比較

提出者	定　義
Understanding GIS（ESRI）	GIS 是設計用來有效的擷取、儲存、更新、處理、分析及展示各種形式地理資訊的系統，包括電腦硬軟體、地理資料庫及操作維護人員。
Burrough P. A.	GIS 是一組強大的工具，可以自實際世界中進行空間資料的收集、儲存、取用、轉換及顯示。
Stan Aronoff（GIS:A Management Perspective）	GIS 是設計用來搜集、儲存、分析具有地理區位特性事物與現象的資訊系統。
Jean Muller（ITC, Netherlands）	GIS 大多是高投資的大規模電腦作業系統，通常是由中央、省及地方政府出資建置。主要的目的是協助行政主管有效的管理自然及人文資源。
David Cowen（University of South Carolina）	GIS 是具有整合空間資訊及協助解決真實世界問題的決策支援系統。
Phillip Parent and Richard Church	GIS 的主要目的是透過疊圖及空間分析功能，將原始地理資料轉變為能支援空間決策的資訊。
Davis	GIS 是一套以電腦為基礎的系統，可以由地圖上輸入、儲存、管理、分析及展示空間（及非空間相關）資料；結合資料庫及空間分析能力，並製作系列性產品。
Bernhardsen	GIS 是可以利用一般電腦為基礎來處理與分析地理資料的系統，該系統包括硬體軟體周邊相關製圖及交流設備。

資料來源：李若愚，2011。

二、動態3D地理資訊系統（GIS）應具備之功能：

(一)於3D環境下展示及查詢：

得到各項數化圖資基本屬性，進行全方位、多角度移動，特別是鉅量資料（GB以上的影像檔），對於目標區能順暢瀏覽有完整之了解。可由瀏覽者於網際網路上自行設定移動及飛行參數，包括飛行的速度、速度增減、離地高度、轉彎及傾角方式，獲得全區之最佳觀察效果。

(二)聯結單位之空間資料庫（Spatial DB）引擎：

如Oracle、SQL 及其他地物資料庫，整合建置資料庫檔案，並可針對顏色、線型、線寬等修改後進行導覽。單位現有之GIS檔案、網頁，並重新設計調整使用者介面，在3D環境下充分展現衛星影像、各應用系統成果及物件資料的成果，提供各式業務隨時運用3D環境進行專業性分析考量。

(三)快速計算各種空間幾何資訊：

透過查詢立體之物件或主體的資訊，並可量測目標物空間距離、物件高度、垂直高度、平面位置、座標角度及區域面積，獲得地表資訊及地形分析功能，協助分析判斷決策。可即時針對特定地區繪出剖面圖、高度分層設色圖，俾利了解地形之高低起伏，對於地形地物上受到視線影響之通視分析可及時掌握，確保完整之景觀。

(四)資訊呈現多元化方式（影像、網頁）：

資料庫中詳細的資訊連接到3D模型上提供查詢及分析並提供資料庫的整合性和可維護性（局部更新），顯示出需展示的標誌、照片或影像，以利了解在各項業務專案特性，並可將3D互動場景燒錄CD提供各式運用。

(五)3D環境狀態飛行：

所查詢之地物資訊，需動態更新資料庫及多種監測或監控器材，平時由各管理單位維護，演習操作或瀏覽時，可結合進此3D資料庫作同步顯示。

(六)系統預留彈性：

提供系統未來發展平台及工具，以利自行增加新的地物或製作展示所需之3D場景，並和現有電腦輔助設計系統與GIS系統兼容，以及格式標準的支援。未來網路語言支援整合平台下，建立在CyberSpace上的多屬性資訊呈現查詢及分析動態現象的功能，提供多種語言程式撰寫並須支援Internet，構建互動式Web 3D GIS 環境操作系統界面直覺化並易於使用。

(七)整合新式資料結構：

從不同的資料來源，在此構建環境空間完整、精確的多層次空間資料模型，在不同的比例表現，使得鉅量資料能快速呈現應有之精細度，呈現出向量、網格資料與物件資料整合的資料結構。

(八)多元方式瀏覽場景：

透視及正射視圖，使用者定義的觀察方向、視點及伸展，像片擬真及純影像圖，支援動畫，且使用者能隨意控制觀看（放大、縮小、漫遊、旋轉、或從不同的方向觀看），亦可藉由滑鼠、鍵盤、搖桿來控制三維空間移動，透過目標區導覽畫面、導航鷹眼地圖及屬性顯示。

三、空軍自動化防空系統功能及特性：

空軍自動化防空系統之功能在提供各級指揮官及作業人員所需之戰場狀況情資，並達成空情監視、鑑別及防空武器運用，了解敵我空軍動態，適切選擇作戰區，創造或利用戰機，支配戰局，充分運用空軍大速度與高高度之特性，以爭取與保持作戰地區之空優，期創造或獲得決戰最大之成功公算與有利之效果。故空軍自動化防空系統可直接掌握全部空域敵我空中動態，使空中兵力運用機動靈活，簡化指揮體系，可收統一之成效，

具有非常重要之影響力。為使自動化防空系統作業可在瞬息萬變的戰場環境下，有效地遂行任務，必須具備以下特性：

(一)發揮整體功能：自動化防空系統之建立，務使地面系統與空用系統密切組合；並使指揮中心與管制單位結成一體，充分發揮整體戰力。

(二)確保安全可靠：自動化防空系統首重安全，各類設施應朝地下化發展，注意保密及嚴密防護並運用諸般手段，防止敵對我實施偵測、干擾、破壞，以確保我系統正常運作。

(三)保持支援彈性：系統裝備、通信網路及陣地建置皆以多重備援方式配置，並屯儲足量器材及搶修人員編組，俾適應狀況之發展，支援全程作戰。

(四)講求機動與速度：應具迅捷之組合力與機動力，發展自動化通資電系統，以確保通資電作業之迅捷有效。

(五)運用尖端科技：自動化防空系統之整備，以模組化、數位資訊化為目標，達成更迅速、安全、確實之基本要求。

四、空軍自動化防空系統運用現況：

空軍自動化防空系統透過網路化、數位化構聯，整合各雷達陣地、空軍基地、氣象中心等單位情資，經由系統即時運算處理產生整體空情圖，並呈現雷達點、航跡、參考點、地圖及空域等相關資訊，構成整體、即時、有效之早期預警及防空指管自動化系統。

現行系統於建置時期，以提升系統功、效能為主要考量，故並未針對地理圖資功能多加著墨，當時所採用之系統圖資為國防部聯合後勤司令部所提供，其資料建立了台灣本島當面 800 浬範圍內之數位圖資及測量高程，無任何建築、地標等地物資訊，而數據資料時間為民國 92 年，距今已逾 10 年，相關情資在整體空情圖呈現方式為 2D 展示，類似中央氣象局所產製之雷達回波圖畫面（如圖 2）。

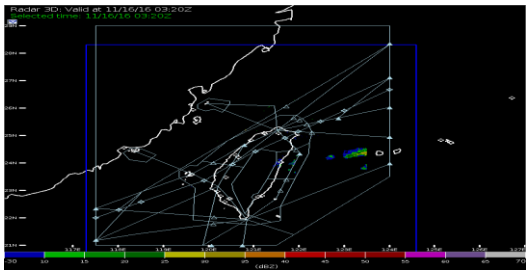


圖 2 雷達回波圖

資料來源：航空氣象服務網

而本系統運作至今，經檢討 2D 圖資於戰演訓任務及災害搶救之運用上，有部分不利人員操作之處，概述如后：

(一)現有圖資不利人員判讀：

由於系統圖資均以2D方式呈現，僅能以滑鼠單點方式查詢地形高度，缺乏了三維空間立體感，亦無相關地物資訊可供查詢，使人員無法於任務執行當下以視覺化方式立即掌握地理資訊，而於飛安事故發生時，亦無法依據現行系統圖資判讀可能失事地點或應執行搜救之範圍，僅能以雷達光點及航向大概判讀失事地點，準確性低，耗費了大量時間及人、物力。

(二)不利判斷雷達遮蔽範圍：

執行飛安事故搶救、山難人員搜救等任務時，須由戰管人員進行慢速機（直升機）導引，當飛行於地勢較低之地形或起降時，將因山脈遮蔽而無從以雷達光點方式追蹤，而現有之2D圖資無法使人員判斷該情況是否為地形所影響，且因無相關地貌資訊（如山脈走勢、主峰等），亦無法判讀飛行器可能之飛行航路、搜救範圍以及起降點。

(三)無法以視覺化方式獲知作戰目標地點地貌概況：

飛行員執行對地偵照任務、地對面戰術科目（SAT）或實施國防展演（飛機衝場）等地面科目時，無法以現有圖資了解任務地點之地物、地貌資訊，而戰管人員亦無法以視覺化方式認知飛行路線是否有危安地形，亦無法掌握飛行器是否已確切到達任務地點（總統府、飛行基地、棒球場等），而此因素對人員之空間概念及地貌認知有所影響，不利任務執行。

(四)現有圖資已不符現況：

台灣本島颱風、地震頻繁，地貌常因地殼變動、山脈崩塌及土石流所影響而改變，且地物建築逐年改變，現有圖資卻因系統原始設計限制，無法適時更新，故現行圖資所提供之地形高度已有相當程度之落差，僅能供飛行員及系統操作人員參考使用，欠缺正確性及完整性。

C^4ISR 系統主要任務是要能提供軍事指揮官明確的掌握所屬部隊軍事動態，而空軍現行所運用的自動化指管系統亦具有此特性，但隨著科技進展，三維的概念已逐步運用於各產業及軍事用途，將三維概念導入已是未來不可避免的趨勢，但在此同時，如何維持即時性、正確性及可靠性的資訊、提供即時情資獲取及正確的分析軟體，仍是 3D 地理資訊系統導入須善加考量的因素，惟有透過周延完整的規劃研析，才能展現出 3D GIS 的優點以及價值，也才能提供指揮者、管制人員及飛行員等運用人員真正所需的指管作戰決策支援系統。

參、研究設計

本研究係針對 3D 地理資訊系統（GIS）導入空軍自動化防空系統建置時，所需考量因素以層級分析法（Analytic Hierarchy Process, AHP）評估各項關鍵成功因素之權重，以建立乙套決策架構，提供未來系統性能提升作業時運用。

一、3D 地理資訊系統（GIS）導入空軍自動化防空系統建置各項關鍵成功因素之探討

綜合國內外學者專家之意見，彙整出性能提升關鍵成功因素之主次準則，後續據此執行準則評估及權重分析，有關準則來源說明如后：

(一)顯示資料展示：

外文專書Understanding GIS（ESRI）中提出地理資訊系統（GIS）是設計用來有效的擷取、儲存、更新、處理、分析及展示各種形式地理資訊的系統；外國學者Burrough P.A.也提出GIS是一組強大的工具，可以自實際世界中進行空間資料的收集、儲存、取用、轉換及顯示；朱子豪等2員提及空間表現的需精細考慮資料表現品質及互動三維的表現方式，樊先達提及三維景觀模型直觀的表達現實世界，使數位化擬真物件的呈現更符合美感，游豐吉等2員提及三維時代的GIS 須具備強大的 3D 展示功能。由上述各學者論點可得知顯示資料的呈現，是3D GIS系統建構的重要關鍵指標，故將「顯示資料展示」納入主準則運用。

1.顯示元件設定：

朱子豪等2員在「GIS 空間資料在動態3D GIS 上的資料形態與展現探析」文中，提及3D GIS系統須將各式2D及3D圖形元件置入易將各種元件結合並做移動，由此可知圖形元件的設定，關係到圖形資料的展示與呈現，並可讓使用者易於使用及解讀，故將「顯示元件設定」納入次準則運用。

2.資料完整性：

樊先達在「多維度動態時空資料的資料架構與可視化概論」文中，提及擬真是3D GIS系統必須達成的要求，大量影像的結合以及地物物件與地形的結合，同時又能聯結外部的程式及檔案，提供多元化的應用互動資料平台，正是空間資訊的完整場景表達，三維景觀模型的表面貼覆像片紋理圖樣，可以

給出現實世界真實、直觀的表達，使得3D 數位化資料的呈現更符合人的期望，由此可知顯示資料的完整性，可讓使用者直觀且正確地理解空間概念，故將「資料完整性」納入次準則運用。

3.畫面解析度：

朱子豪等2員在「GIS空間資料在動態3D GIS上的資料形態與展現探析」文中，提及GIS系統應可讓使用者根據展現的物件的距離，在不同等級的精細度影像做調整，由於顯示資料精細度將決定使用者直觀感受，並直接關係到地貌及地物的影像展現程度，故將「畫面解析度」納入次準則運用。

4.顯示效率性：

朱子豪等2員在「GIS空間資料在動態3D GIS上的資料形態與展現探析」文中，提及3D GIS呈現立體物件與地形等場景，繪出速度成為重要的關鍵，另游豐吉等2員在「三維時代的GIS 技術探討」文中，提及GIS圖資因測繪技術的發展讓精確度也愈來愈高，於是GIS 軟體必須承受海量資料並作快速展現的功能也變成不可或缺的基本需求，由此上述學者觀點可知顯示資料呈現速度是GIS系統的最基本要求，也直接關係使用者的視覺感官接受程度，故將「顯示效率性」納入次準則運用。

(二)介面操作性：

朱子豪等2員提及GIS系統需使用滑鼠、鍵盤、搖桿控制三維空間全方位、多角度移動，設定移動及飛行參數，速度、離地高度、轉彎及傾角方式，多元化方式瀏覽場景，另樊先達也提及GIS需藉由滑鼠、鍵盤控制三度空間全方位、多角度移動，設定移動及飛行參數，速度、離地高度、轉彎及傾角方式，並結合網路上多種訊息呈現，多資料來源將影像、網頁、熱連結瀏覽場景，隨意控制觀看漫遊、旋轉，善用滑鼠的右鍵進行目標物的多元方向瀏覽及資訊查詢，由上述學者觀點可知介面操作是關係到使用者運用系統之重要關鍵，亦是3D GIS系統建構之基本要求，故將「介面操作性」納入主準則運用。

1.操作便利性：

朱子豪等2員在「GIS 空間資料在動態3D GIS上的資料形態與展現探析」文中，提及操作便利性為3D GIS系統基本要求，由滑鼠、鍵盤、搖桿控制三維空間全方位、多角度移動，設定移動及飛行參數，速度、離地高度、轉彎及傾角方式，多元化方式（影像、網頁）瀏覽場景，為求操作的便利，善用滑鼠的右鍵，進行目標物的繞圓形、橢圓形、上下震盪、設定起始點等瀏覽的方式，以及物件屬性或座標的查詢等基本功能項均可，由此可知操作便利性，關係到使用者運用系統的便捷程度，並可讓作業進行地更加有效快速，故將「操作便利性」納入次準則運用。

2.操作流暢性：

許志傑於「運用正型法於C^4ISR系統開發之研究」論文中，提及C^4ISR系統是分散式網路架構，需要有嚴格時間的即時性限制，避免資料延遲等狀況，由此可知操作流暢度對空軍自動化防空系統極為重要，亦關係到使用者運用系統的效率，並可藉由操作指令及反應直接回饋而加快作業進度，故將「操作流暢性」納入次準則運用。

3.視窗配置彈性：

游豐吉等2員在「三維時代的GIS 技術探討」文中，提及真正的Web 3D GIS應具有整合GIS與類似Google Earth的網際網路大型3D及影像流覽功能的網際網路三維地理資訊展示系統，意即具備所有GIS功能與3D及影像瀏覽功

能，而且讓Server 端與Client端均可以依照專案需求開發專屬的3D瀏覽程式，而就現行空軍自動化防空系統而言，主要飛行任務之指揮管制及帶領，還是以2D模式為主，3D GIS模式應屬輔助圖資，故各類型視窗（2D、3D、飛行數據）的適當擺放，關係到使用者對於資訊掌握的便捷程度，故將「視窗配置彈性」納入次準則運用。

4.客製化介面：

朱子豪等2員在「GIS 空間資料在動態3D GIS 上的資料形態與展現探析」文中，提及GIS系統需整合建置資料庫檔案，並可針對顏色、線型、線寬等修改後進行導覽，單位現有之GIS 檔案、網頁，並重新設計調整使用者介面，在3D 環境下充分展現衛星影像、各應用系統成果及物件資料的成果，提供各式業務隨時運用3D 環境進行專業性分析考量，而使用者介面關係到系統運用之流暢度，使系統提高運用價值，故將「客製化介面」納入次準則運用。

(三) 系統功能性：

外國學者David Cowen提出GIS是具有整合空間資訊及協助解決真實世界問題的決策支援系統，朱子豪等提出3D GIS系統之量測、查詢及顯示等基本功能都須簡易可行，以減省專案作業人員的負擔，並說明除了3D 空間顯現及查詢功能外，在呈現3D 空間資料的環境下，應再加以提昇功能，樊先達提出GIS 軟體在3D運用上多以網格式（Grid）數值高程模型（DEM）的呈現及運算，如可視域分析，更應將地形上的地物是否遮蔽視線考量在內，上述學者皆認為GIS系統應具備各種功能，以協助使用者進行決策，俾利妥善運用，故將「系統功能性」納入主準則運用。

1.空間分析功能：

朱子豪等2員於「GIS 空間資料在動態3D GIS 上的資料形態與展現探析」文中，提及3D GIS系統應可透過查詢立體之物件或主體的資訊，量測目標物空間距離、物件高度、垂直高度、平面位置、座標角度及區域面積，獲得地表資訊及地形分析功能，協助分析判斷決策，並可即時針對特定地區繪出剖面圖、高度分層設色圖，俾利了解地形之高低起伏，對於地形地物上受到視線影響之通視分析可及時掌握，確保完整之景觀，由上述觀點可知GIS系統必須包含計算、分析功能，以協助指揮者進行決策，故將「空間分析功能」納入次準則運用。

2.系統預留彈性：

朱子豪等2員於「GIS 空間資料在動態3D GIS 上的資料形態與展現探析」文中，提及3D GIS系統應提供系統未來發展平台及工具，以利自行增加新的地物或製作展示所需之3D 場景，並和現有電腦輔助設計系統與GIS系統兼容，格式標準的支援、多屬性資訊呈現查詢及分析動態現象的功能，提供多種語言程式撰寫並須支援Internet，構建互動式Web 3D GIS 環境操作系統界面，直覺化並易於使用，由上述觀點可知GIS系統的功能擴充性及發展性對於系統的永續運作維持十分重要，故將「系統預留彈性」納入次準則運用。

3.航跡運算導覽功能：

樊先達於「多維度動態時空資料的資料架構與可視化概論」文中，提及3D GIS系統應可設定物件的運動速度或是結合GPS後，隨時間變化的差異，模擬出動態環境，且因空間具有座標，物件具有速度，故可由此決定出時間的影響進行物件移動，表現出時間與空間的交互變化情形，並提出系統應可設定環境導覽路徑規劃，可自行定義空中及地面不同路徑移動；選定導覽方式即自行運動導覽，可定義目標物或景點的不同瀏覽方式，至少隨行、繞圓、飛近、

飛離、跳進、跳離等，由上述觀點可知GIS系統可計算並表現出物件與時間交互變化情況，協助使用者進行空間審視及導覽，另可保存相關歷史數據，以供使用者運用參考，故將「航跡運算導覽功能」納入次準則運用。

4.監控告警功能：

朱子豪等2員於「GIS 空間資料在動態3D GIS 上的資料形態與展現探析」文中，提及3D GIS系統所查詢之地物資訊，需動態更新資料庫及多種監測或監控器材，平時由各管理單位維護，演習操作或瀏覽時，可結合進此3D 資料庫作同步顯示，另許志傑於「運用正型法於C^4ISR系統開發之研究」論文中，亦提出C^4ISR系統是屬於即時情資獲取及分析軟體,隨時對周遭環境事件發生時加以監控與分析，由上述觀點可知GIS系統亦應具備監控功能，如在防空系統運用上則應加強相關提醒或警示，以確使操作人員預警並注意危安事件之發生（如空中接近事件、航機接近地形地物之情況），故將「監控告警功能」納入次準則運用。

5.影像多元輸出：

朱子豪等2員於「GIS 空間資料在動態3D GIS 上的資料形態與展現探析」文中，提及3D GIS系統資料庫中詳細資訊，應可提供查詢及分析並提供資料庫的整合性和可維護性（局部更新），顯示出需展示的標誌、照片或影像，並可將3D 互動場景燒錄CD 提供各式運用，由上述觀點可知GIS系統應具備影像資料展示及輸出性，故將「影像多元輸出」納入次準則運用。

二、層級架構建立及問卷設計

(一)準則歸納：

本研究以文獻探討方式先歸納整理過去學者對 3D 地理資訊系統（GIS）之研究文獻與資料,作為尋找 3D GIS 導入空軍自動化防空系統建置的關鍵成功因素主要來源。首先，經由各種相關研究文獻之探討，先將所有可能影響建置 3D GIS 之變數羅列出來，希望以此避免遺漏可能之影響變數，初步擬出影響建置 3D GIS 之 3 大主準則及 13 項次準則，其中顯示資料展示主準則，有 4 項因素；介面操作性主準則，有 4 項因素；系統功能性主準則，有 5 項因素，詳如表 2 所示。

第二章表 2 評估要素彙整表

目標	主準則	次準則
導入空軍自動化防空系統3D地理資訊系統（GIS）建置之研究	顯示資料展示	顯示元件設定
		資料完整性
		畫面解析度
		顯示效率性
	介面操作性	操作便利性
		操作流暢性
		視窗配置彈性
		客製化介面
	系統功能性	空間分析功能
		系統預留彈性
		航跡運算導覽功能
		監控告警功能
		影像多元輸出

後續以專家問卷方式修正影響「3D 地理資訊系統（GIS）導入空軍自動化防空系統建置」主次準則要項，進而確認本研究之層級架構。

(二)專家問卷彙整結果：

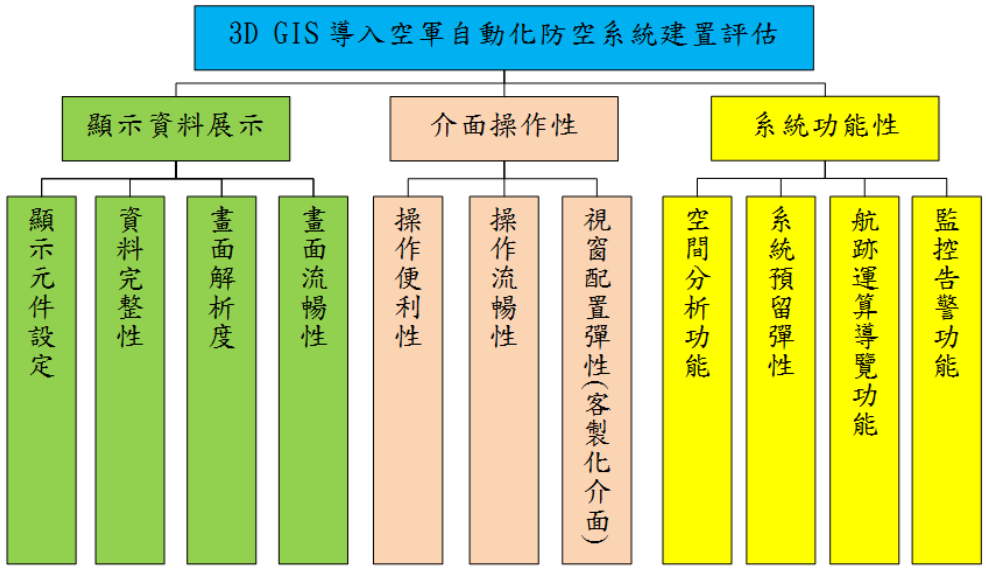
本次專家訪談問卷量表於民國 105 年 12 月 1 日至 105 年 12 月 10 日，針對 26 位專家以親自送達、電話訪問及回收方式進行。本研究之主準則及次準則經由專家問卷調查表，綜整各領域專家意見及建議，彙整如后：

1.指管系統維護中心少校參謀及戰管中心少校攔管長表示，於主準則「顯示資料展示」內之「顯示效率性」，係代表畫面圖像變化、視角轉向、畫面切換的顯示效率及呈現速度，惟次準則名稱容易遭誤解為系統處理效能，故建議將「顯示效率性」將修訂為「畫面流暢性」。

2.戰管聯隊上校副聯隊長、戰管聯隊系管科科長及空軍司令部系整組中校參謀均表示，於主準則「介面操作性」內之次準則「視窗配置彈性」代表使用者可以依需求改變主視窗顯示大小及位置，性質與次準則「客製化界面」雷同，故建議將上述兩項次準則合併。

3.主準則「系統功能性」內之次準則「影像多元輸出」，僅佔專家勾選比例約 6 成（勾選次數 16 次），代表多數專家不認同此項次準則屬於 3D 地理資訊系統（GIS）導入空軍自動化防空系統建置之重要影響評估指標，故刪除本項次準則。

本研究之主準則及次準則經由專家以同性質合併、名稱修訂及不適用刪除等方式，經統計結果執行修訂完成後，歸納影響 3D GIS 導入空軍自動化防空系統建置計有 3 大主準則及 11 個次準則，其中顯示資料展示主準則，有 4 項因素；介面操作性主準則，有 3 項因素；系統功能性主準則，有 4 項因素；故本研究之 3D GIS 導入空軍自動化防空系統建置評估要素之層級架構已確立（層級架構圖詳如圖 3 所示），可設計本研究後續之 AHP 分析層級問卷。



第三章圖 3 層級架構圖

(三) AHP層級分析問卷設計：

本研究問卷採 AHP 層級分析法設計，問卷設計步驟說明如下。

1.問卷所需資料蒐集：依據本研究之動機與目的蒐集、彙整文獻中對 3D GIS 系統及空軍自動化防空系統之定義，初步擬出 3D GIS 導入空軍自動化防空系統建置之關鍵成功因素主準則及次準則，並透過第一階段專家問卷確立層級架構，作

為問卷設計之基礎。

2.決定問卷調查方法：本問卷將以透過親自送達、電話訪談及 E-mail 寄達、回收方式進行。

3.決定問卷之形式：本問卷採封閉式方式進行設計，以 AHP 分析層級法之評量尺度為評分標準，以九個尺度來描述兩兩成對比較其重要性之問卷內容，讓受訪者能充分表達每個評選項目之重要性而進行勾選，問卷量表範例如表 3。

第四章表 3 問卷量表

評估指標	強度比例（←左邊愈重要　右邊愈重要→）																評估指標
	絕強 9:1	8:1	極強 7:1	6:1	頗強 5:1	4:1	稍強 3:1	2:1	等強 1:1	1:2	稍強 1:3	1:4	頗強 1:5	1:6	極強 1:7	1:8	絕強 1:9	
顯示資料展示																		介面操作性

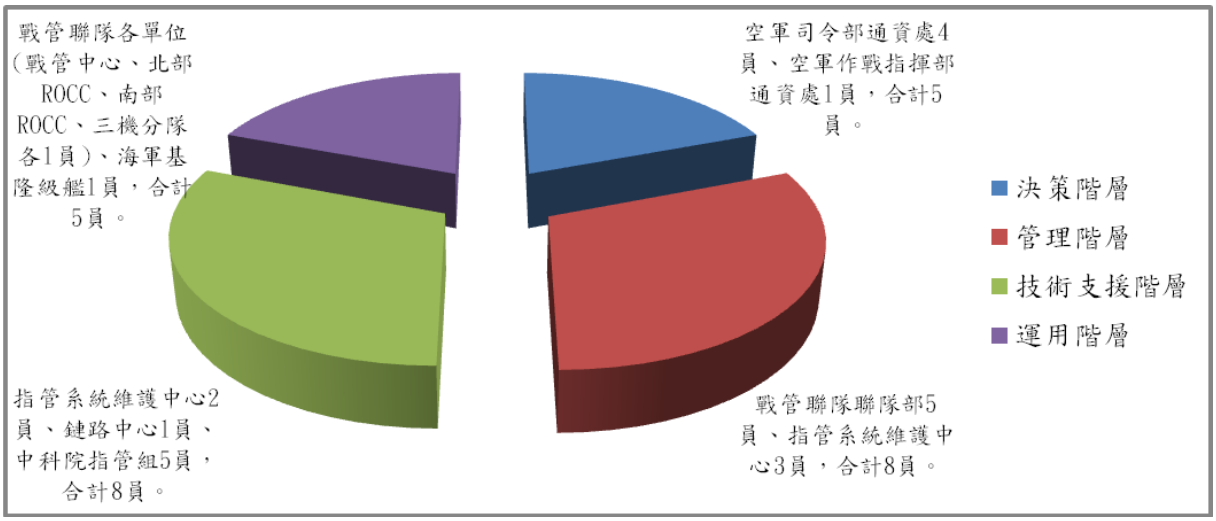
肆、研究成果分析

一、問卷調查資料分析：

本次 AHP 訪談問卷調查表於民國 106 年 1 月 2 日至 106 年 1 月 20 日，針對 26 位專家（專家之背景如表，人員資料如表 4，人員組成如圖 4）實施填答，其中依受訪者職務屬性區分為決策階層（空軍司令部及空作部等 5 員）、管理階層（戰管聯隊及系維中心等 8 員）、技術支援階層（系維中心、鏈路中心及中科院等 8 員）及運用階層（戰管聯隊各單位及海軍基隆級艦等 5 員），以透過親自送達及 E-mail 寄達、回收方式進行，共送達 26 份，回收 26 份，回收率為 100%，繼之將依問卷調查所得結果，以 Expert Choice 11 版軟體檢測其一致性。

第五章表 4 問卷量表

單位	人數	說明
決策階層	5	空軍司令部通資處 4 員、空軍作戰指揮部通資處 1 員，合計 5 員。
管理階層	8	戰管聯隊聯隊部 5 員、指管系統維護中心 3 員，合計 8 員。
技術支援階層	8	指管系統維護中心 2 員、鏈路中心 1 員、中科院指管組 5 員，合計 8 員。
運用階層	5	戰管聯隊各單位(戰管中心、北部 ROCC、南部 ROCC、三機分隊各 1 員)、海軍基隆級艦 1 員，合計 5 員。
合計(總體評選)	26	共計 26 員。



第六章圖 4 專家人員組成資料圖

由於在 Expert Choice 11 軟體中，其一致性檢驗是以 I.R.值（Inconsistency Ratio,I.R.）表示不一致比例，其在決斷值以不超過 0.1 為佳。經實證檢驗得無效問卷 2 份，有效問卷 24 份，故本研究問卷分析以此 24 份有效問卷為決策群體。所有 AHP 問卷之分析結果如表 5。

第七章表 5 本研究所有 AHP 問卷之分析結果

問卷編號	以 Expert Choice 檢測之 I.R.值（Inconsistency Ratio）				採用
	主準則	次準則一	次準則二	次準則三	
P1	0.01	0.08	0.08	0.07	V
P2	0.04	0.08	0.08	0.02	V
P3	0.00	0.06	0.03	0.05	V
P4	0.02	0.08	0.00	0.05	V
P5	0.01	0.04	0.04	0.10	V
P6	0.00	0.06	0.03	0.00	V
P7	0.02	0.09	0.00	0.02	V
P8	0.04	0.09	0.09	0.08	V
P9	0.04	0.04	0.04	0.09	V
P10	0.00	0.09	0.03	0.07	V
P11	0.04	0.06	0.04	0.07	V
P12	0.05	0.09	0.09	0.00	V
P13	0.27	0.29	0.07	0.41	X
P14	0.06	0.09	0.06	0.04	V
P15	0.04	0.01	0.06	0.01	V
P16	0.00	0.05	0.00	0.00	V
P17	0.05	0.09	0.02	0.05	V
P18	0.02	0.05	0.05	0.02	V
P19	0.00	0.26	0.00	0.39	X
P20	0.08	0.09	0.00	0.03	V
P21	0.00	0.07	0.00	0.08	V
P22	0.09	0.09	0.00	0.09	V
P23	0.08	0.10	0.00	0.09	V
P24	0.07	0.09	0.08	0.06	V
P25	0.10	0.02	0.00	0.07	V
P26	0.09	0.06	0.05	0.07	V

二、問卷調查資料分析：

(一)決策階層問卷調查資料分析：

1.主準則優序權重分析結果：

各主準則優先權重順序依次為「顯示資料展示」0.456、「系統功能性」0.353、「介面操作性」0.191，代表決策階層專家多數認為「顯示資料展示」相較其它兩項主準則，應列為所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「畫面流暢性」0.249、「監控告警功能」0.193、「資料完整性」0.119，代表專家多數認為在主準則「顯示資料展示」下之「畫面流暢性」相較其他次準則，應列為所應考量之首要因素。

(二)管理階層問卷調查資料分析：

1.主準則優序權重分析結果：

各主準則優先權重順序依次為「系統功能性」0.510、「介面操作性」0.280、「顯示資料展示」0.210，代表管理階層專家多數認為「系統功能性」相較其它兩項主準則，應列為所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「監控告警功能」0.237、「航跡運算導覽功能」0.174、「操作流暢性」0.130，代表專家多數認為在主準則「系統功能性」下之「監控告警功能」相較其他次準則，應列為所應考量之首要因素。

(三)技術支援階層問卷調查資料分析：

1.主準則優序權重分析結果：

主準則優先權重順序依次為「系統功能性」0.522、「介面操作性」0.282、「顯示資料展示」0.196，代表技術支援階層專家多數認為「系統功能性」相較其它兩項主準則，應列為所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「監控告警功能」0.221、「航跡運算導覽功能」0.141、「操作流暢性」0.120，代表專家多數認為在主準則「系統功能性」下之「監控告警功能」相較其他次準則，應列為所應考量之首要因素。

(四)運用階層問卷調查資料分析：

1.主準則優序權重分析結果：

各主準則優先權重順序依次為「顯示資料展示」0.618、「系統功能性」0.225、「介面操作性」0.158，代表運用階層專家多數認為「顯示資料展示」相較其它兩項主準則，應列為所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「畫面流暢性」0.262、「資料完整性」0.191、「畫面解析度」0.120，代表專家多數認為在主準則「顯示資料展示」下之「畫面流暢性」相較其他次準則，應列為所應考量之首要因素。

(五)整體問卷調查資料分析：

1.主準則優序權重分析結果：

主準則優先權重順序依次為「系統功能性」0.430、「顯示資料展示」0.324、「介面操作性」0.246，代表各階層專家多數認為「系統功能性」相較其它兩項主準則，應列為所應考量之首要因素。

2.各次準則權重分析結果：

各次準則整體優先權重順序依次為「監控告警功能」0.195、「畫面流暢性」

0.147、「航跡運算導覽功能」0.134，代表專家多數認為在主準則「系統功能性」下之「監控告警功能」相較其他次準則，應列為所應考量之首要因素。

三、綜合分析：

研究之專家問卷係區分決策、管理、技術支援及運用等 4 個階層計 26 位專家問卷，有效問卷計 24 份，決策階層問卷 5 份、管理階層問卷 7 份、技術支援階層問卷 7 份、運用階層問卷 5 份，並求得其各主次準則優先順序及總體評選資料，以利分析其中差異(綜合資料如表 6)。

表 6 各階層 AHP 結果綜合資料表

分類	項目	決策		管理		技術支援		運用		總體評選	
		權值	排序	權值	排序	權值	排序	權值	排序	權值	排序
主準則	顯示資料展示	0.456	1	0.210	3	0.196	3	0.618	1	0.324	2
	介面操作性	0.191	3	0.280	2	0.282	2	0.158	3	0.246	3
	系統功能性	0.353	2	0.510	1	0.522	1	0.225	2	0.430	1
次準則	顯示元件設定	0.034	10	0.027	11	0.013	11	0.067	6	0.032	11
	資料完整性	0.119	3	0.030	10	0.083	6	0.191	2	0.093	5
	畫面解析度	0.081	5	0.035	9	0.024	10	0.120	3	0.057	9
	畫面流暢性	0.249	1	0.098	4	0.059	9	0.262	1	0.147	2
	操作便利性	0.039	8	0.062	7	0.073	7	0.040	8	0.057	7
	操作流暢性	0.104	4	0.130	3	0.120	3	0.067	6	0.112	4
	視窗配置彈性(客製化介面)	0.023	11	0.050	8	0.117	4	0.024	11	0.049	10
	空間分析功能	0.047	7	0.093	5	0.085	5	0.029	9	0.068	6
	系統預留彈性	0.039	8	0.065	6	0.066	8	0.028	10	0.054	8
	航跡運算導覽功能	0.072	6	0.174	2	0.141	2	0.096	4	0.134	3
	監控告警功能	0.193	2	0.237	1	0.221	1	0.076	5	0.195	1

(一)主準則分析：

1. 整體評選各主準則優先權重順序依次為「系統功能性」0.430>「顯示資料展示」0.324>「介面操作性」0.246。
2. 「系統功能性」為整體評選結果較優先考量者；所謂系統功能性係指，可提供使用者簡易的操作環境，透過簡單的操作介面，讓使用者很容易地使用電腦系統資源，處理各項事務，並監控整個程式的執行過程，同時調配各種電腦資源，以期程式能作充份而正確的使用，而自動化防空系統之功能在提供各級指揮官

及作業人員所需戰場狀況情資，並達成空情監視、鑑別及防空武器運用，以了解敵我空軍動態，故更應具備各種功能，以協助進行決策，俾利妥善運用。而分析「系統功能性」最後獲評選為相對重要準則之原因，可由系統功能性涵蓋「空間分析功能」、「系統預留彈性」、「航跡運算導覽功能」及「監控告警功能」等 4 項次準則，瞭解其下包含了諸多面向，諸如空間資訊的分析、系統的未來擴充發展程度、系統航跡預覽及飛行路線規劃，以及空情狀況監控告警等功能，均屬於系統功能之範疇。系統功能性越完善，指揮官及作業人員對於戰場全般判斷、飛航路線預劃及突發狀況掌握均可獲得充分支援；因此，學者專家認為當執行 3D 地理資訊系統（GIS）導入空軍自動化防空系統建置時，相較於「顯示資料展示」及「介面操作性」等兩項主準則而言，須優先考量「系統功能性」，以確保建立功能強大完善，且合於使用者需求之支援決策系統。

(二)「顯示資料展示」次準則分析：

1. 整體評選在「顯示資料展示」各次準則整體優先權重順序依次為「畫面流暢性」0.447>「資料完整性」0.281>「畫面解析度」0.174>「顯示元件設定」0.098。
2. 「畫面流暢性」為整體評選結果較優先考量者；所謂畫面流暢性代表畫面圖像變化、視角轉向、畫面切換的顯示效率及呈現速度等，而顯示資料呈現速度也是 GIS 系統的最基本要求，並直接關係使用者的視覺感官接受程度。空軍自動化系統各項作業務求迅速，配合裝備運作，爭取作戰反應時間，且空軍作戰講求時效，分秒必爭，迅速展示「即時狀況」及動態資料，使指揮官能及時下達決心，掌握戰機，顯示畫面的流暢也關係到作業人員的直覺判斷速度及指管作業效率，故多數專家均認為「畫面流暢性」為「顯示資料展示」層面中最為重要的一環。

(三)「介面操作性」次準則分析：

1. 整體評選在「介面操作性」各次準則整體優先權重順序依次為「操作流暢性」0.513>「操作便利性」0.261>「視窗配置彈性(客製化介面)」0.226。
2. 「操作流暢性」為整體評選結果較優先考量者；空軍自動化防空系統提供操作人員一套圖形化軟體操控介面，透過鍵盤、滑鼠點擊畫面選單上各種功能，執行系統監控、資料輸入、任務預劃、指管命令下達等各項鍵鈕行動，遂行戰、演訓任務。系統除穩定運作外，為使系統作業可在瞬息萬變的戰場環境下，有效地遂行任務，亦須講求機動與速度，具備即時性，對戰情資料及戰術處置，迅速反應，自動處理，以增進指揮速度，「操作流暢性」關係著作業人員運用系統的效率，並可藉由操作指令及反應直接回饋而加快作業進度，而專家評選結果，亦證實了「操作流暢性」對於 3D 地理資訊系統（GIS）導入空軍自動化防空系統建置規劃之重要性。

(四)「系統功能性」次準則分析：

1. 整體評選在「系統功能性」各次準則整體優先權重順序依次為「監控告警功能」0.432>「航跡運算導覽功能」0.296>「空間分析功能」0.151>「系統預留彈性」0.121。
2. 「監控告警功能」為整體評選結果較優先考量者；未來自動化防空系統發展目標，係依攻防一體之整體戰略構想，以支援在無預警狀況下之攻防作戰，並以自動化、地下化、數據化、機動化為原則，對抗敵可能之海空突襲，且 C^4ISR 系統是屬於即時情資獲取及分析軟體，隨時對周遭環境事件發生時加以監控與分析，系統如具備自動化的監控能力，可強化指揮者及作業人員決策判斷、反應作為以及處置時效，如在作戰指揮運用上提供航機監控及提醒警示，以預警

並注意危安事件之發生（如空中接近事件、航機接近地形地物之情況）；對於系統維護者來說，可監控系統運作狀況，監測及控制雷達及外部系統之連線，提供性能監控及故障點檢出功能，高度監控自動化防空系統資源（網路狀況、資料處理、系統航跡數量及程式負載量等），並提供告警及處置建議。因此，「監控告警功能」在 3D 地理資訊系統（GIS）導入空軍自動化防空系統建置作業中，獲得各位專家評選為相對重要之準則。

伍、結論

隨著科技進步，在許多專業人員的研究之下，以往所認知的空間資料已逐步由文數字顯示進步為視覺呈現應用，再到分析決策、判斷的多元應用，各種空間關聯產業分析均已運用地理資訊系統（GIS）來輔助，藉以得出更佳的判斷成果，而為了能以迅速、直接且動態的方式認知空間，3 維的概念更是不可或缺的要素。3D GIS 運用的重點在於顯示資料的展示、介面操作以及系統功能，如將其導入導入空軍自動化防空系統建置，建構一立體、完整、即時、便於操作、方便維護及具分析功能的整體空情圖像，正可解決作業人員對於圖資判讀、地物辨識、任務地貌認知等系統運用問題，並得以發揮系統最大效益。

在主準則評估方面，就專家評估後分析得知，以「系統功能性」排序第一，顯示 3D 地理資訊系統（GIS）導入空軍自動化防空系統建置時，系統功能是否完善，是否可發揮功能及有效運用系統資源等優點，對系統管理者及系統運作具重大影響，系統功能性越完善，指揮官及作業人員對於戰場全般判斷、飛航路線預劃及突發狀況掌握均可獲得充分支援，若無法滿足標準，將會降低 C^4ISR 系統運作效能，影響系統支援戰、演、訓任務執行成效。

在次準則評估方面，就專家評估後分析得知，「畫面流暢性」、「操作流暢性」、「監控告警功能」等 3 項，為 3D 地理資訊系統（GIS）導入空軍自動化防空系統建置時最關鍵指標。空軍自動化系統各項作業務求迅速，配合裝備運作，爭取作戰反應時間，且空軍作戰講求時效，分秒必爭，迅速展示「即時狀況」及動態資料，使指揮官能及時下達決心，掌握戰機，而「畫面流暢性」及「操作流暢性」均關係到作業人員的直覺判斷速度及指管作業效率；系統具備完善的「監控告警功能」，則可強化指揮者及作業人員決策判斷、反應作為以及處置時效。

本研究所歸納出之各項主次準則，均為專家評估後所認同之指標，亦為 3D 地理資訊系統（GIS）導入空軍自動化防空系統建置之關鍵成功因素，可作為國軍建案承辦單位於未來執行選擇方案分析時，達成系統性能提升作業關鍵成功因素之決策參考，以期建置乙套符合作戰需求之空軍自動化防空系統。綜上所述，C^4ISR 系統首重精確性、穩定性及安全性，係因 C^4ISR 系統主要任務旨在整合各類即時戰場情資，以作為指揮官下達決心之依據，在須臾之間面對攸關作戰成敗之際，戰場圖資的展示、畫面顯示及操作的流暢性，監控預警功能的適切性、正確性及完整性，均具備失之毫釐差之千里的重要地位。在執行系統建置時，維持即時性、正確性及可靠性的資訊、提供即時情資獲取及正確的分析軟體，亦是 3D 地理資訊系統導入須善加考量的因素，惟有透過周延完整的規劃研析，才能展現出 3D GIS 的優點以及價值，也才能建置符合指揮者、管制人員、飛行員及維護人員等真正所需的指管作戰決策支援系統。

參考文獻

朱子豪、樊先達，2006。GIS 空間資料在動態 3D GIS 上的資料形態與展現探析，國土資訊系統通訊，第 60 期，3-5。

李若愚，2011。地理資訊系統概論（第三版），臺北：全華，2-2，2-3。

辛希、林永青、謝銘智、蕭釧瑛、黃舒郁、林晉廷，2013。網際網路 3D GIS 在工程應用之初探，中興工程，第 120 期，55-63。

陳錦嫣，2003。GIS 技術與實務應用，新北：新文京。

陳錦嫣、黃國展，2013。ArcGIS 地理資訊系統入門與應用，新北：新文京。

許志傑，2003。運用正型法於 C^4ISR 系統開發之研究，國防大學國防資訊研究所碩士論文。

黃敏郎、劉守恆，2005。地理資訊系統 – 基礎操作實務，臺北：文魁， 1-3。

國防部空軍司令部，2009。空軍自動化防空系統教範，臺北：空軍司令部，1-1，1-2。

游豐吉、李錦昌，2007。三維時代的 GIS 技術探討，臺灣地理資訊學刊，第 5 期，33-35。

鄧振源、曾國雄，1989。層級分析法(AHP)的內涵特性與應用(上)，中國統計學報，第 27 卷第 6、7 期。

樊先達，2006。多維度動態時空資料的資料架構與可視化概論，國土資訊系統通訊，第 60 期，44-45。

滕春元，2013。國軍防救災地理資訊系統建構之理論與實作，國防大學管理學院資訊管理學系碩士論文。

簡定華、林開輝，2006。地理資訊系統於國防上之應用，國土資訊系統通訊，第 60 期，60。