模糊群體決策環境下以 OWA 運算子進行風險分析

Fuzzy Group Decision Making Using An OWA Operator Applied to Risk Analysis for Information Security Management

羅濟群 Chi-Chun Lo,
國立交通大學 資訊管理研究所 教授
Professor, Institute of Information Management
National Chiao Tung University

王 平 Ping Wang,
國立交通大學 資訊管理研究所 博士研究生
Graduate Student, Ph.D. Candidate, Institute of Information Management
National Chiao Tung University

趙國銘 K-M Chao
DSM Research Group, School of MIS, Coventry University, UK

摘 要

傳統的定量風險分析方法著重於危害事件機率的計算，只能適用於歷史資料為可數量化，但風險分析面對網際網路的不斷變化的危害事件，通常無法蒐集充足的數量化資訊提供危害事件機率的估算。本研究採用定性風險分析方法，結合模糊偏好關係，模糊多數 (fuzzy majority) 理論與OWA運算子作風險值之彙總，以求得資訊資產的風險等級。分析時允許專家運用語意量詞(linguistic quantifier)，研析風險項目的重要性及此風險項目發生時所造成損害程度(impact loss degree)的評估，取代傳統的方法對危害事

件機率(probability)及損害金額(money loss)的估算。最後舉一網路資料中心(Internet Data Center, IDC)實例說明。本研究擴展Hererra，Chiclana及Kacprzyk 等作者發展的群體決策理論至模糊環境的風險分析應用；經研究實證可知，面對不完整及模糊資料與多位專家參與風險決策時，所研提之方法可有效簡化風險分析過程的複雜性與大幅降低群體決策之共識達成所需時間。

關鍵詞：BS7799；ISO/IEC13355；風險分析；柔性共識；OWA運算子

Abstract

The traditional techniques of quantitative risk analysis determine the solution by the probability distribution function of threats and its impact loss. Since risk assessment process often holds under uncertain situation with incomplete information due to rapid change of advent attack events especially in the Internet. It is hard to accumulate adequate events to precisely estimate the probability of threats and impact losses in some real cases. In this paper, a qualitative risk analysis method is employed to prioritize the risk level of assets through the use of fuzzy preference relation, fuzzy majority concept, and the ordered weighted averaging (OWA) operator. The peoposed mothod allows the experts to express their risk preferences in linguistic quantifiers and explicitly represents the importance (weighting) of risk factor and the corresponding impact loss degree instead of probability of advent events and money loss. Finally, a real case of risk assessment for the Internet Data Center (IDC) is given to illustrate our approach. The proposed method extends the traditional risk analysis using fuzzy multiple-person decision making (MPDM) theory, developed by Hererra, Chiclana, and Kacprzyk, to risk analysis in fuzzy environment. From numerical illustrations, the proposed model can effectively decrease the complexity of the risk analysis and reduce the time required to reach a group consensus when the committee includes the opinions of many decision makers.

Keywords:BS7799；ISO/IEC13355；Risk assessment, Soft Consensus, OWA Operator

壹、前　言

近年來，由於資訊科技日新月異，網際網路的應用蓬勃發展，組織愈來愈依賴網路進行各種商業交易。企業面對廣大市場的競爭時代，要在這快速變化且競爭激烈的環境下成功，快速取得正確的資訊是組織獲取競爭力的關鍵因素之一，「資訊」因此成爲現今組織的重要命脈，企業爲了贏得客戶的信賴與提昇業務的競爭力，必須證明本身能夠適當的保護資訊的安全，保護內容包括組織本身、客戶及合作廠商等之資訊；但因爲網路環境日趨複雜，企業所處的資訊科技環境不斷的演進，也需持續引進各種所需的軟硬體產品，同時也帶來潛在的資訊安全弱點，再加上電腦病毒與駭客攻擊手法不斷推陳出新，其攻擊能力日漸提昇，因此，如何建置適當的資訊安全管理系統(Information Security Management Systems，簡稱 ISMS)，
便成爲組織極爲重要的課題。

依據美國電腦安全協會/聯邦調查局(Computer Security Institute/Federal Bureau of Investigations，CSI/FBI)2003[1] 統計 Internet 的攻擊事件由 1999 年的 57%增加到 2003 年的 78%，年成長率 5.25%;最新威脅的類型統計發現，病毒、內部濫用、筆記型電腦失竊、內賊、阻斷服務與外部入侵等爲最常發現的威脅類型，其中以病毒、內部濫用成長率最高。

有鑑於此，組織針對資訊安全進行風險管理的觀念已日漸受到重視，英國標準協會(British Standards Institution，簡稱 BSI)及國際標準組織(International Organization for Standardization，簡稱 ISO)等機構爲此也陸續制訂與資訊安全相關之標準，以便企業瞭解自身的資訊安全需求，並進行風險分析與管理，以確保資訊安全。

在國際標準組織(ISO)有關風險管理(Risk Management)之文件 ISO/IEC Guide 73: 2002(E/F)[38]中，對風險管理之定義如圖一所示。在圖一中，風險管理包含風險評鑑、風險處理、風險承受、風險溝通等四項，其中風險評鑑包含風險分析與風險評估，風險分析則包含來源識別與風險估計。針對圖一之各項主要名詞簡要說明如下：

圖一、風險管理示意圖

1. 風險(Risk)：統稱某事件發生的或然率及其後果，一般而言只有在可能導致負面後果時才會使用「風險」這個名詞。
2. 風險管理(Risk Management)：一般而言包括風險評鑑、風險處理、風險承受及風險溝通。
3. 風險評鑑(Risk Assessment)：涵蓋風險分析及風險評估的程序。

4.風險分析(Risk Analysis)：以有系統的方式利用資訊，以識別來源並估計風險的行爲。

5.來源識別(Source Identification)：尋找、列出並說明來源要素的程序。

6.風險估計(Risk Estimation)：用來決定某風險發生的機率及造成的後所用的程序。

7.風險評估(Risk Evaluation)：把預估的風險和已知的風險準則進行比較的程序，以決定風險的重要性。

8.風險處理(Risk Treatment)：選擇並執行應對措施的程序，以便修正風險。

9.風險規避(Risk Avoidance)：決定不與危險情況有關聯的行爲，或是撤出危險狀況的行爲。

10.風險最佳化(Risk Optimization)：與風險有關的程序，藉以降低負面後果、提升正面後果及其或然率。

11.風險轉移(Risk Transfer)：與另一方共同承擔風險帶來的損失責任或利益。

12.風險保留(Risk Retention)：接受特定風險帶來的損失責任或利益。

13.風險承受(Risk Acceptance)：接受某風險的決定。

14.風險溝通(Risk Communication)：決策者及其他關係人交換或共享風險相關資訊的行爲。

傳統風險分析方法在實務上有使用的限制，因爲面對不確定的環境與不完整的資訊，要專家明顯的判斷資產的威脅及損害有困難之處。此外，風險分析過程大都包括一組專家參與，面對不同意見要達成一致性的共識有實質上的困難。 然而，目前在資訊安全之相關參考文獻中[2,20,24]，大多使用定量風險分析，其著重於危害事件的機率計算與損害結果的預測，只能適用於資安歷史資料爲可靠且爲可數量化時，但風險分析面對網際網路的不斷變化的危害事件，通常無法蒐集充足的資訊後再以求危害事件機率，使用上受到限制。因此，爲滿足資訊安全風險分析在實務上的作法，本研究擴展 Hererra，Chiclana 及 Kacprzyk [6,14,21]等作者發展的群體決策理論，並將模糊邏輯導入風險分析模式中，期能發展一個合乎人性作爲(human behavior)的風險分析方法，且可降低群體決策之共識形成的困難度，期能提供組織日後執行資訊安全風險分析之參考

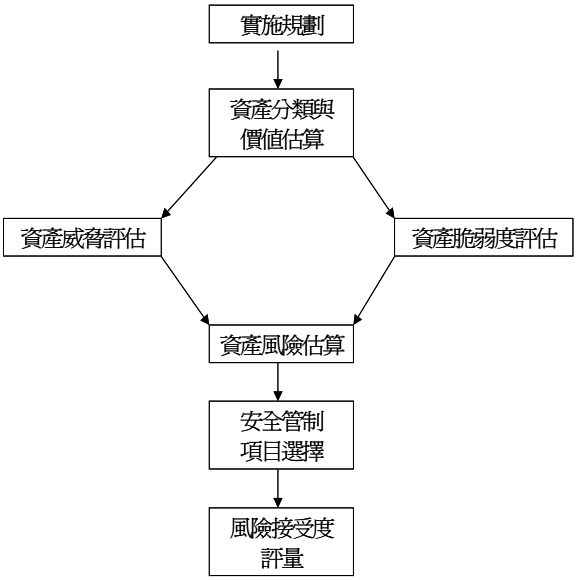
第二節中說明風險分析步驟及方法，介紹資訊安全管理相關標準，第三節介紹本研究研提的風險分析模式與程序，第四節舉一實例說明，第五節與其他方法作比較並討論如何選擇適當的風險模式，最後作出結論及建議未來研究方向。

貳、風險分析之方法論

一、風險分析之步驟

風險分析程序依據劉永禮、陳啓光(2002) [36]可區分成「實施規劃」、「資產確認與價值估計」、「資產威脅分析」、「資產脆弱分析」、「資產風險值計算」、「安全管制項目選擇」與「風險接受度評量」等七個步驟，如圖二。此外，風險分析的程序亦可參考美國商業部所屬國家技術與標準局(National Institute of Standards and Technology / NIST) [12]所建議的風險評鑑的程序，內容完整並涵概風險分析及風險評估程序，共有九個步驟說明如下： 1) 資產重要性的決定(system characteristics)、 2)威脅識別(threats identification)、 3)系統弱點識別(vulnerability identification)、 4)安

控分析(control analysis)、 5)風險發生可能性(likelihood determination)、 6)衝擊分析(impact analysis)、 7)風險程度的決定(risk determination)、 8)安控建議(control recommendations)、 9)分析結果的建議書(results document)，各組織可依作業需求及時程加以選擇合適的風險分析程序並作適當的程序裁適(tailing)。

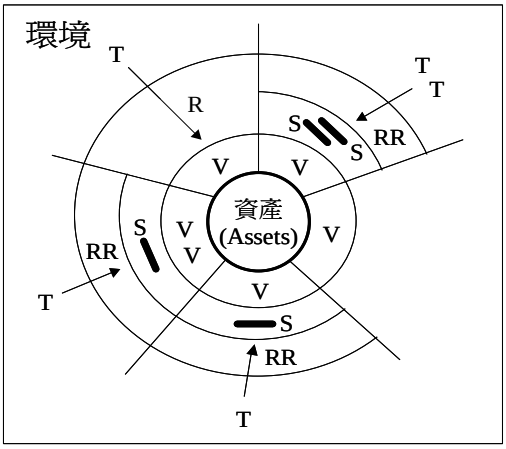


圖二、風險分析之程序

脆弱性、威脅模式

就資訊安全管理系統(ISMS)而言，風險(Risk)是由資產(Asset)、脆弱性(Vulnerability)與威脅(Threat)三者所共同形成，缺一不可。

根據 ISO/IEC Guide 73[38]，風險分析過程爲當某一資產遭受到威脅時，在考慮系統脆弱性下，假設發生資產失效後，對企業營運產生之風險水準之分析。 在 ISO/IEC TR 13335-1 [16] 文件中，有關資產、脆弱性與威脅三者間之關係亦可表示如圖三(圖例說明，V：脆弱性，T：威脅，S：保護措施，R：風險，RR：殘餘風險)，在圖三中，表示一項資產可能會有一個或多個脆弱性，而每個脆弱性亦可能會被一個或多個威脅所利用，進而對資產造成損害，因此，爲了保護資產的安全，必須採取一項或多項之保護措施，以降低其風險，或者接受其風險，不採取任何保護措施。



圖三、安全要素關係圖

三、常用的風險分析方法介紹

風險分析方法依據范淼(2002)[42]風險分析屬性(Attribute)的性質可區分成定量(Quantitative)與定性(Qualitative)兩種風險分析方法。「定性風險分析」是指對已界定出的風險分析其發生的可能性(likelihood)與衝擊損失程度(impact loss degree)，決定其對企業營運影響的優先等級。「定量風險分析」是指以計量方式分析每一項風險因素分析其對企業營運影響的程

度，常以換算成金額方式表示損失。「定性風險分析」主要作法是建立順序尺度以衡量風險值；而「定量風險分析」是採用機率模式以計算出風險值，個別風險評分(R) = 發生機率(P) * 衝擊(L)，最後針對個別風險項目作加總，求取資產的風險總分。

國內外許多學者[3,8,9,13,20,24]及組織研究資訊資產的風險分析方法和模式以協助使用者作出正確的決策。其中維吉尼亞大學(1991) [3]發展一個風險因素篩選的方法，命名爲風險排序篩選法(Risk Ranking and Filtering)，其運用德菲法(Delphi method)將風險因素排序，以過濾低風險因素。Halliday (1996) [13] 利用營運作業流程以發展一套資訊技術導向的風險分析和管理方法。Lichtenstein(1996) [24] 討論如何制定理想的風險分析的需求，和發展風險因素的評估方法。最近，Chen (2001) [8] 運用群體決策理論，計算軟體專案發展的風險。 Chen (2003) [9]採用模糊相似分析定理，介紹一個定性風險分析方法以決定資訊資產的風險等級。

其他知名的風險分析模式包括 HazOp (Hazard Operable Process) 分析、錯誤樹分析 (Fault Tree Analysis， FTA)、失敗模式和影響與關鍵性分析 (Failure Mode and Effect Criticality Analysis， FMECA)，CORAS (Consultative Objective Risk Analysis System)，COBRA (Consultative, Objective and Bi-functional Risk Analysis)等。因限於篇幅，本文不一一作介紹。Koller[20]將風險分析常用方法區分成五大類：(1) 鑑別功能分析 (Discriminant Function Analysis)，(2)貝氏理論(Bayesian Theorem)，(3)決策樹分析[35]，(4) 因素分析(Factor Analysis)及 (5)類神經網路(Neural Nets)等。其中鑑別功能分析、類神經網路與因素分析可用以計算風險因素的權重，進而決定風險評估架構；貝氏理論及決策樹分析可輔助分析危害事件發生機率與預測損害結果。

國內相關研究包括李慶民、莊謙亮(2001) [37]以BS7799 [4,5]爲基礎建構資訊安全分析模式—以虛擬私有網路系統爲例」，以加總量表法，將評審要項內容分成四分量表進行專家問卷調查；劉永禮、陳啓光(2002) [36] 運用 Carroll [2]所定義之資產分析價值(V)、單一事件損失預期值(SLE) 、年度發生率(ARO)、年度損失預期值(ALE)，以 BS7799 之 127 控管項目來計算系統整體風險值(R)。關寶全、羅濟群等(2003) [11]使用群體決策的德菲法(Delphi method)，分析每一項風險屬性對企業營運影響的程度，整合專家群的風險意見，將一個複雜的系統從風險類別層級加以拆解成細部風險屬性，例如資訊系統風險、人員管制風險、技術風險等，完整建立一個系統風險的評估架構，以系統化的決定風險水準與風險事件的可控制程度。

以下簡介常用的定性及定量風險分析方法如下：

1. 定量(quantitative) 風險分析：

風險係數分析法 [2]

進行量化分析時，可以利用表一中所列的常用風險分析係數，使決策者取得量化的數據，並且根據數字的大小進行分析。依據表一我們可求得年度損失預期值(ALE)= 單一事件損失預期值

(SLE) * 年度發生率(ARO);而單一事件損失預期值(SLE)=資產價值 × 暴露因子(EF)；

表一、常用的風險分析係數

觀念	衍生的公式
暴露因子(Exposure Factor / EF)	該威脅導致特定資產損失的百分比
單一事件損失預期值(Single Lose Expectancy / SLE)	資產價值 * 暴露因子(EF)
年度發生率(Annualized Rate of Occurrence / ARO)	該事件每年發生的頻率
年度損失預期值(Annualized Lose Expectancy / ALE)	單一事件損失預期值(SLE) * 年度發生率(ARO)

若單純的數字大小無法區分出衝擊的程度，則可以事先以質的方法定義過某個程度的數字代表某個程度的衝擊(例如：受影響的人員大於 5 人，即爲嚴重威脅事件，其暴露因子 EF 爲 0.9, 0.0≦EF≦1.0)。

2. 定性(Qualitative)風險分析

定性風險分析可參考 ISO/IEC 13355 part 3 附錄 E [17]，共舉五個定性風險分析法，各組織可依需求加以選擇。

四、ISO/IEC13355

ISO/IEC13355 Information technology — Guidelines for the management of IT Security 是由國際標準組織(International Standard Organization, ISO)及國際電子技術協會(International Electro technical Commission, IEC)共同主導，目前已廣泛運用於各種組織的資訊風險管理，建構完整的風險控管機制。

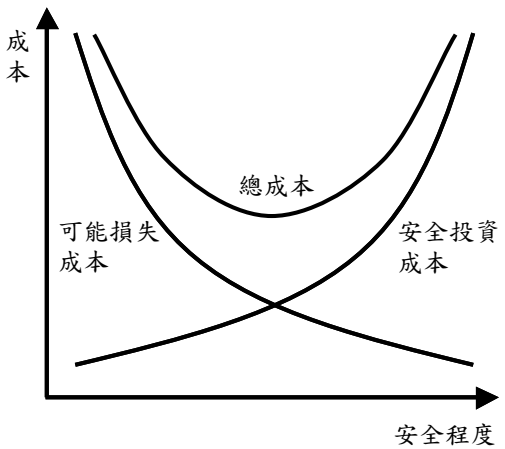
國際標準組織 ISO/IEC 技術組制訂 ISO/ IEC 13335 技術報告的目的，是針對資訊技術安全的管理方面提供指導原則，而不是解決方案。在組織內負責資訊技術安全的部門，應該能從這份報告中獲得滿足他們資安管理需求的資料。這份技術報告的主要目標包括：

1. 定義和描述管理資訊安全技術相關的概念。
2. 一般性地識別管理資訊安全技術和管理資訊技術之間的關係。
3. 提供數種能夠用來解釋資訊安全技術的模型。
4. 在資訊安全技術的管理上提供一般性的指導原則。

ISO/IEC TR 13335 由數個篇章共同組成。Part 1 [16]: Concepts and models for IT Security 描述資訊技術安全管理的基本概念和模型的概要；Part 2: Managing and planning IT Security 由管理和計畫的觀點描述資訊安全管理機制中的風險分析策略的選擇；Part 3 [17]: Techniques for the management of IT Security 描述在一個計劃的生命週期，期間牽涉到的管理活動所適當使用的安全技術，例如計畫、設計、執行、測試、獲得或使用者操作，其附錄有說明資訊安全管理機制中的風險方法並舉例說明；Part 4: Selection of safeguards 定義資訊安全管理機制中的風險處置；Part 5: Management Guidance on Network Security 說明資訊安全管理機制中的網路安全指引。

五、風險控制成本之考量

組織在完成資訊安全風險分析後，對於風險值高於可接受風險水準之資產項目將採取相對應的風險處理措施，但由於組織的資源有限，不可能毫無上限的從事於資訊安全方面的投資，因此，組織應根據本身的業務需求，考量自身所能承擔之風險及達到預期安全目標所需付出的成本，在安全程度與投資成本二者間做適當之抉擇(tradeoff)，如圖四所示，圖中表示要提昇組織的資訊安全程度愈高，必需投資之預防成本也愈高，但相對的也使得風險降低，並降低可能的損失成本。在 ISO/IEC 17799 中也提到，選擇控制措施時，應該根據實施成本與降低的風險之間、以及與安全破壞事件發生時潛在的損失之間的關係來衡量，同時，還應該考慮如聲譽損失等非金錢因素。



圖四、風險控制成本

參、風險分析模式

本風險分析模式是參考美國標準與技術局所制定的風險管理手冊(NIST SP3800-30)[12]中的風險分析步驟而來，但 NIST SP3800-30 所制定的風險分析程序並未考量群體決策的程序，故作者融入 Hererra，Chiclana 及 Kacprzyk 等作者發展的群體決策理論，將風險分析的決策模式擴展至的模糊群體決策(fuzzy group decision making)問題。研究的程序是透過分析資產的重要性、風險項目的權重、資產脆弱性和風險項目發生時所造成的衝擊損失程度，透過 OWA 運算子作專家群的風險偏好關係之加總，再運用優勢程度及非優勢程度以綜合判斷資產的相對風險強度。

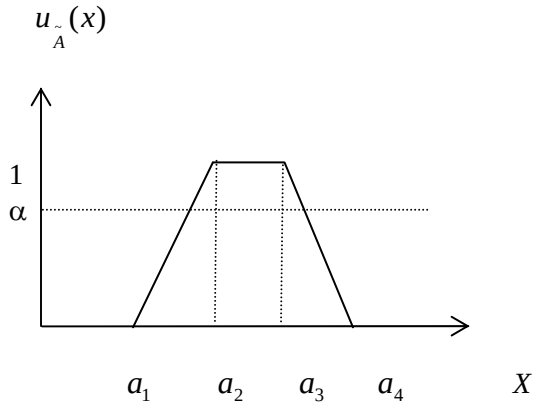
本研究根據 BS7799 [4,5] 的建議，將針對資產之機密性(confidentiality)、可用性(availability)、完整性(integrity)三項構面進行風險評估準則的分析。但三項構面中有關資產的威脅及其機率、脆弱性及其脆弱水準常缺乏歷史資料，面對不時變化的網路攻擊，時常無法等到長期的累積資料再作風險分析，故改採定性風險分析進行研究，運用 BS7799 標準建構一個完整的風險評估架構，以分析組織內的資訊資產的風險等級。發展的風險模式前的準備工作與相關定義說明如下：

一、事前準備(Preliminaries)

首先對模糊數、模糊關係、OWA 運算子及語意量詞作基本定義。

定義 1. 正梯形模糊數 $\tilde{A}$ 可以定義爲 (a_1, a_2, a_3, a_4) 其隸屬函數 $u_{\tilde{A}}(x)$ 定義如下及圖五. [19]

$$u_{\tilde{A}}(x)=\begin{cases}\dfrac{x-a_1}{a_2-a_1} & for \quad a_1\le x<a_2\\ 1 & for \quad a_2\le x\le a_3\\ \dfrac{a_4-x}{a_4-a_3} & for \quad a_3<x\le a_4\\ 0 & for \quad others\end{cases} \tag{1}$$



圖五.正梯形模糊數 $\tilde{A}$ 及 α-cuts

定義 2. 模糊數之數學運算.: [7]

加法⊕:

$$(a_1,a_2,a_3,a_4)\oplus(b_1,b_2,b_3,b_4)=(a_1+b_1,a_2+b_2,a_3+b_3,a_4+b_4)$$

減法Θ:

$$(a_1,a_2,a_3,a_4)\Theta(b_1,b_2,b_3,b_4)=(a_1-b_4,a_2-b_3,a_3-b_2,a_4-b_1)$$

乘法⊗:

$$\tilde{A}\otimes\tilde{B}=(a_1,a_2,a_3,a_4)\otimes(b_1,b_2,b_3,b_4)=(a_1b_1,a_2b_2,a_3b_3,a_4b_4)$$

$$k\otimes\tilde{A}=k\otimes(a_1,a_2,a_3,a_4)=(ka_1,ka_2,ka_3,ka_4),\forall k\in R \tag{2}$$

除法 ϕ:

$$\tilde{A}\phi\tilde{B}=(a_1,a_2,a_3,a_4)\phi(b_1,b_2,b_3,b_4)=(a_1/b_4,a_2/b_3,a_3/b_2,a_4/b_1)$$

定義 3. 模糊數 $\tilde{A}$ 之模糊偏好關係爲一模糊集合 $\tilde{A}\,X\,\tilde{A}$ 其隸屬函數 $u_r(\tilde{A},\tilde{B})$ 定義爲, $\forall\tilde{A},\tilde{B}\subseteq R$, $u_r(\tilde{A},\tilde{B})$ 爲對 $\tilde{A}$ 超過 $\tilde{B}$ 之偏好程度。

定義 4. DPR. 對任兩個正梯形模糊數, $\tilde{A}$, $\tilde{B}\in R$,定義模糊關係爲 $r(\tilde{A}_j,\tilde{B}_k)$ 爲一差集模糊偏好關係 (Difference-scale Preference Relation ,DPR)其隸屬函數爲

$$r_{jk}=r(\tilde{A}_j,\tilde{B}_k)=\begin{cases}f(\tilde{A}_j,\tilde{B}_k) & \tilde{A}_j\neq\tilde{B}_k\\ \dfrac{1}{2} & \tilde{A}_j=\tilde{B}_k\end{cases} \tag{3}$$

其中 $f(\tilde{A}_j,\tilde{B}_k)=\frac{1}{2}(1+\sum_{l=1}^{4}\frac{(a_l-b_l)}{4})$

明顯的，$0\le r_{jk}\le 1$，很容易可證明 DPR 滿足反身性(reciprocal)，加法遞移性(additive transitive relation)，和最大－最小遞移性(max-min transitive relation)如下: [30]

$$r_{jk}+r_{kj}=1 \quad j,k=1,...,n \tag{4}$$

$$(r_{jk}-1/2)+(r_{kl}-1/2)=(r_{jl}-1/2)\ \forall j,k,l \tag{5}$$

$$r_{jk}\ge 1/2, r_{kl}\ge 1/2\Rightarrow r_{jl}\ge\min(r_{jk},r_{kl})\ \forall j,k,l \tag{6}$$

定義 5. OWA 運算子[10,32] Yager(1988) 提出 OWA (Ordered Weighted Averaging) 運算子並已廣泛被應用在決策問題上。 OWA 運算子可方便調整在彙整運算(aggregation)之交集程度(anding)與聯集程度(oring)。OWA 運算子 爲一 n 維度映射函數 F, $F:[0,1]^n\to[0,1]$，其須配合對應一組權重向量。令 $\{a_1,a_2,...,a_n\}$ 爲一組向量需要加總以求出彙整解, OWA 運算子 F 可定義爲

$$F(a_1,a_2,...,a_n)=W.B^T=\sum_{i=1}^{n}w_i.b_i \tag{7}$$

其中 $W=[w_1,...,w_n]$ 爲一組權重向量, $w_i\in[0,1]$ 且 $\sum_{i=1}^{n}w_i=1$，B 爲相關有序(ordered) 向量。每

一元素 $b_i \in B$ 爲($a_1, a_2, ..., a_n$)中第 ith 排序的數值。Yager 建議配合模糊語意量詞 (fuzzy quantifiers) 求取 OWA 運算子之權重向量：

$$w_i = Q(i/n) - Q(i-1/n), \quad i=1,\ldots,n \qquad (8)$$

其中 Q 爲一非漸減比例語意量詞(non-decreasing quantifiers)。從方程式(7), 我們很容易證明 OWA 運算子滿足資訊彙整所需特性－互換性(community), 單調性(monotonicity)，單一性(idemptency) [32]。

定義 6. 模糊多數(Fuzzy majority)爲一種柔性共識 (soft consensus)觀念是由Kacprzyk (1989) [21]所提出，其運用 Zadeh 之語意量詞加以表現,透過語意量詞之模糊邏輯加以求取模糊多數決的答案。

定義 7. 比例語意量詞(Proportional Linguistic Quantifier)：由 Zadeh (1975)所提出口語化語意量詞觀念。其中比例語意量詞[34] "*almost all, most, at least half, few, less than half*", 可由單元區間[0,1]之模糊子集合(fuzzy subsets)來表示。對任一個 $r \in [0,1]$， $Q(r)$ 代表正比於語意量詞 r 的程度。對一非漸減(non-decreasing)隸屬函數的語意量詞可以表現如下:

$$Q(r) = \begin{cases} 0 & if \quad r < a \\ \dfrac{r-a}{b-a} & if \ a \le r \le b \\ 1 & if \quad r > b \end{cases} \qquad (9)$$

其中 $a, b, r \in [0,1]$.

例如, Q='most' 可表示爲

$$Q_{most}(r) = \begin{cases} 1 & r \ge 0.8 \\ 2r - 0.6 & 0.3 \le r \le 0.8 \\ 0 & r \le 0.3 \end{cases} \qquad (10)$$

二、研提的風險分析模式

考量風險分析問題描述如下：由 m 個風險專家 $d_1, d_2, ..., d_m$ 組成委員會，以判斷 n 個資訊資產 $a_1, a_2, ..., a_n$ 之風險等級。每個風險專家獨立使用語意量詞執行「風險項目的重要性」及「該風險項目發生時所造成衝擊損失程度」的評估，並將評估的語意量詞轉成相對應之正梯形模糊數如表二、表三。

表二. 評估風險項目重要性的語意量詞

非常不重要(VU)	(0.0,0.0,0.0,0.1)
不重要 (U)	(0.0,0.0,0.1,0.3)
稍不重要 (MU)	(0.0,0.1,0.3,0.5)
普通(M)	(0.1,0.3,0.5,0.7)
稍爲重要(MI)	(0.3,0.5,0.7,0.9)
重要 (I)	(0.5,0.7,0.9,1.0)
非常重要(VI)	(0.7,0.9,1.0,1.0)

表三.分析衝擊損失程度之語意量詞

非常不嚴重(VL)	(0.0,0.1,0.3,0.5)
稍不嚴重(L)	(0.1,0.3,0.5,0.7)
普通 (M)	(0.3,0.5,0.7,0.9)
嚴重 (H)	(0.5,0.7,0.9,1.0)
非常嚴重(VH)	(0.7,0.9,1.0,1.0)

本風險分析方法參考風險管理手冊(NIST SP3800-30)中的風險分析步驟及融入群體決策理論而來，區分成以下五個步驟以分析風險等級：風險評分，風險彙整，風險排序，風險等級判斷，及風險排序結果之確認，詳細內容說明如下：

（一）風險評分(Risk Evaluation)

首先根據組織的資訊安全政策、作業程序建立風險評估架構如圖六，以執行資訊資產 $a_j(j=1,2,...,n)$ 的風險分析，假設風險評估架構為共有 q 個風險評估項目 $\tilde{c}_l(l=1,2,...,q)$。風險評估項目 l 的重要性為 $\tilde{w}_l(l=1,2,...,q)$。$\tilde{V}=\{\tilde{v}_{jl}\mid j=1,2,...,n;l=1,2,...,q\}$ 代表一個 $n\times q$ 模糊風險分析矩陣，其代表資產 a_j 的風險評估項目 c_l 所對應的風險評估值。

依據 Lee [23]和 Chen [8], 軟體專案發展的風險程度可以將個別的風險項目的權重(weighting)乘以對應項目的風險評估值，再依據各層風險項目作加總，以求取整體的風險總分；若為多層架構，須先由底層逐層作加總計算。風險在不同的應用中，有不同定義及計算方法(如積分法、加總法等)；在定性資訊安全分析法中，「風險評估項目的重要性」及「此風險項目發生時，所造成的衝擊損失可能程度」為影響資產的風險兩大因素；故風險評估值可以方程式 (11)計算如下:

$$\tilde{x}_j^i=\frac{1}{q}[(\tilde{v}_{j1}^i\otimes\tilde{w}_1^i)\oplus...\oplus(\tilde{v}_{jq}^i\otimes\tilde{w}_q^i)] \qquad (11)$$

其中 v_{jl}^i 為風險專家 d_i 對資產 a_j 因風險評估項目 l 發生所造成衝擊損失可能程度，w_l^i 為風險專家 d_i 對風險評估項目 l 重要性的估計值。

接下來，以定義 4 之差集模糊偏好關係(Difference-scale Preference Relation, DPR) 函數將模糊數對(pairwise)轉換成模糊偏好關係，定義 6. 可用來代表風險專家 d_i 對資產 a_j 及 a_k 之風險相對程度如下：

$$r_{jk}^i=f(\tilde{x}_j^i,\tilde{x}_k^i)=\frac{1}{2}(1+(\tilde{x}_j^i\Theta\tilde{x}_k^i)) \qquad (12)$$

其中 r_{jk}^i 為一模糊偏好關係，用以表達風險專家 d_i 對資產 a_j 及 a_k 的主觀風險高低程度；r_{jk}^i 數值介於區間 [0,1]，$0\le r_{jk}^i\le 1$如圖七；r_{jk}^i=0 代表風險專家 d_i 對資產 a_j 認為有絕對風險；此外，r_{jk}^i=1/2 代表風險專家 d_i 對資產 a_j 及資產 a_k 之有相同的風險估計值 ；r_{jk}^i=1 代表風險專家 d_i 對資產 a_k 認為有絕對風險。

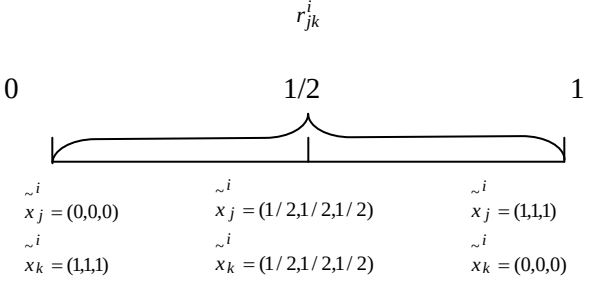


圖 七. 模糊偏好關係，r_{jk}^i.

（二）風險彙整 (Risk Aggregation)

本研究之群體模糊偏好關係之計算是彙整 m 位決策者之模糊多數(fuzzy majority)[6]偏好值，意思是「多數人的偏好」是透過 OWA 運算子整合各專家的模糊語意量詞而所得。選擇 OWA 運算子是基於 Smolikova 的分析 [26]。他分析五類模糊彙整運算子－quasi-arithmetic mean 運算子、weighted mean 運算子、OWA 運算子、Sugeno integral 運算子及 Leximin ordering 運算子，作出下列建議： OWA 運算子為一強固(robust)，容易計算及提供比其他運算子操作上更彈性，可應用在群體多屬性決策(Group MCDM)問題。因此，OWA 運算子適合於本研究。為了彙整模糊多數偏好值，我們整合 OWA 運算子與模糊語意

量詞 Q 以求取群體(m 位)模糊偏好值[10]如下：

$$r_{jk} = F_Q(r_{jk}^1,...,r_{jk}^m) \quad (13)$$

其中 $F_Q(a_1,a_2,...,a_m) = \sum_{i=1}^{m} w_i.b_i$,

$w_i = Q(i/m) - Q((i-1)/m)$, F_Q 爲 OWA 運算子與模糊語意量詞 Q 函數。

（三）風險排序 (Risk Ranking)

目前有許多方法可作彙整之模糊偏好關係排序應用，本研究選擇模糊偏好關係之優勢程度(Dominance Degree, DD)代表風險專家對資產間風險的相對強度 [6,15]。我們使用語意量詞之優勢程度以決定資訊資產之相對風險程度，並利用風險層級矩陣(risk-level matrix , RLM) [12] 求取資產之相對風險強度如下：

$$DD(a_j) = F_Q(r_{jk}, k = 1...n, j \neq k) \quad (14)$$

其中 $F_Q(a_1,a_2,...,a_n) = \sum_{j=1}^{n} w_k.b_k$ and

$w_k = Q(k/n) - Q(k-1/n)$

（四）風險等級之判斷 (Determination of Risk-level)

美國標準與技術局所建議使用風險層級矩陣(Risk Level Matrix,RLM)以判斷資訊資產的風險等級；依據 RLM，五個風險等級(risk scale)提供判斷資訊資產的風險等級：高 (>0.75 to 1.0)，中高 (>0.5 to 0.75)，中 (>0.25 to 0.5)，中低 (0.15 to 0.25)，低 (0.0 to 0.15)。

（五）風險排序結果之確認 (Validation of Risk Ranking)

爲了確認本方法在風險分析之正確性，風險判斷結果需要由其他方法來加以確認。本研究使用 Orlovsky (1978)[25]發展之模糊偏好關係之非優勢程度 (Non-Dominance Degree, NDD) 來確認最高風險的資產，模糊偏好關係之非優勢程度計算式如下：

$$NDD(x_j) = F_Q(1-d_{kj}, k = 1...n, j \neq k) \quad (15)$$

其中 $d_{kj} = \max\{r_{kj} - r_{jk}, 0\}$, 和

$F_Q(1-a_1,1-a_2,...,1-a_n) = w_1.(1-b_1) + ... + w_n.(1-a_n)$.

綜整本研究程序：

步驟 1.

(1) 由 m 個風險專家 $d_1,d_2,...,d_m$ 組成委員會，以判斷 n 個資產 $a_1, a_2,..., a_n$ 之風險等級。每位風險專家獨立使用語意量詞執行每一資產之風險項目的重要性及風險項目所造成衝擊損失程度之估計，並將它轉成相對應之正梯形模糊數 $\tilde{x}_j^i$ 。

(2) 利用差集模糊偏好關係(Difference-scale Preference Relation ,DPR) 函數將兩兩模糊數轉換成模糊偏好關係

$r_{jk}^i = f(\tilde{x}_j^i, \tilde{x}_k^i) = \frac{1}{2}(1 + (\tilde{x}_j^i \Theta \tilde{x}_k^i))$.

步驟 2. 令 $w_i = Q(i/m) - Q(i-1/m)$，整合 OWA 運算子與模糊語意量詞 Q 以獲得群體模糊偏好值如下： $r_{jk} = F_Q(r_{jk}^1,...,r_{jk}^m)$,

其中 $F_Q(a_1,a_2,...,a_n)=\sum_{i=1}^{m} w_i.b_i$ ，和

$$Q(r)=\begin{cases}0 & if \quad r<a\\ \dfrac{r-a}{b-a} & if \ a\le r\le b\\ 1 & if \quad r>b\end{cases} \quad a,b,r\in[0,1].$$

步驟 3. 風險排序－加總各專家的風險評估值，針對每一資產計算語意量詞之風險主導(Dominance Degree)程度以求取資訊資產 a_j 之相對風險強度如下：

$$DD(a_j)=F_Q(r_{jk},k=1...n,\ j\neq k).$$

其中 $F_Q(a_1,a_2,...,a_n)=\sum_{k=1}^{n} w_k.b_k$ ，

$$w_k=Q(k/n)-Q((k-1)/n).$$

步驟 4. 風險等級之判斷－利用風險層級矩陣(risk-level matrix, RLM) 以決定資產之相對風險等級。

步驟 5. 風險判斷結果之再確認－使用 Non-Dominance Degree(NDD)確認最高風險的資產如下：

$$NDD(x_j)=F_Q(1-d_{kj},k=1...n,\ j\neq k)$$

其中 $d_{kj}=\max\{r_{kj}-r_{jk},0\}$ ，

$$F_Q(1-a_1,1-a_2,...,1-a_n)=(w_1.(1-b_1)+...+(w_n.(1-a_n)).$$

肆、實例說明

以下舉一網際網路資料中心 (Internet Data Center, IDC) 的風險評鑑實例來說明本文所提方法。其中風險分析區分成兩階段，第一階段是分析資訊安全管理(Information Security Management, ISM)制度，審查重點包括組織資安政策，資安作業程序(Standard Operation Procedure, SOP)，工作指導書(Working Instruction, WI)；第二階段是分析資訊安全管理制度與實作現況是否相符，兩者之差異爲何。

本範例包括四種不同資訊資產：資料庫伺服器(a_1)、郵件伺服器 (a_2)、防火牆(a_3)、和企業入口網站伺服器 (a_4)以執行風險分析，分析結果作爲 BS7799 資訊安全防護管理制度導入參考與改進依據。

步驟 1. 風險評分(Risk Evaluation)－假設由 *6* 個風險專家 $D=\{d_1,d_2,d_3,d_4,d_5,d_6\}$ 組成委員會，採用 BS7799 之十項資訊安全主要控管項目作爲風險評估項目 (risk items) 如圖六，風險專家獨立使用表一、表二所列之語意量詞，以判斷四項資訊資產 $A=\{a_1,a_2,a_3,a_4\}$之風險等級。首先組織透過營運作業流程(Business Service Process)，找出重要資訊資產，並將其作分類(Classification)及等級(Asset Priority)；參考危害事件之資料、系統廠商報告、資安廠商報告、或資安專家提供經驗數據來估測各風險評估項目的重要性，估算結果如表三；分析每一資產的脆弱點 (Vulnerability Factors)；依據資產重要等級及每個資產之脆弱點以估算當資產失效後之衝擊損失程度，估算的結果如表四。

在執行風險評分之彙總(aggregation)時，因爲風險分析模式爲兩層式架構，因爲本案之第二層風險項目之各評估準則的重要性資料不完整，故資訊資產的衝擊損失可能程度可由方程式(16)來估算；方程式(16)計算系統之衝擊損失程度是求

取第二層風險項目 $(\tilde{v}^{i}_{jl2}, l2 = 1,..., q_2)$ 的模糊平均值如下：

$$\tilde{v}^{i}_{jl} = \frac{1}{q_2}((\tilde{v}^{i}_{j1}) \oplus ... \oplus (\tilde{v}^{i}_{jq2})) . \quad (16)$$

接下來，運用方程式(11)來計算資訊資產的風險評分，並轉成對應之正梯形模糊數 $\tilde{x}^{i}_{j}$ ，結果如表五。再以方程式(12)將六位評估者的模糊數轉換成個別的模糊偏好關係矩陣如下：

$$R^1 = [r^1_{ij}] = \begin{bmatrix} 0.5 & 0.389 & 0.424 & 0.341 \\ 0.613 & 0.5 & 0.536 & 0.453 \\ 0.576 & 0.464 & 0.5 & 0.417 \\ 0.656 & 0.547 & 0.583 & 0.5 \end{bmatrix}$$

$$R^2 = [r^2_{ij}] = \begin{bmatrix} 0.5 & 0.670 & 0.530 & 0.345 \\ 0.23 & 0.5 & 0.360 & 0.175 \\ 0.47 & 0.640 & 0.5 & 0.315 \\ 0.655 & 0.825 & 0.685 & 0.5 \end{bmatrix}$$

$$R^3 = [r^3_{ij}] = \begin{bmatrix} 0.5 & 0.425 & 0.230 & 0.395 \\ 0.595 & 0.5 & 0.325 & 0.490 \\ 0.770 & 0.675 & 0.5 & 0.665 \\ 0.605 & 0.510 & 0.335 & 0.5 \end{bmatrix}$$

$$R^4 = [r^4_{ij}] = \begin{bmatrix} 0.5 & 0.310 & 0.495 & 0.545 \\ 0.690 & 0.5 & 0.685 & 0.735 \\ 0.505 & 0.315 & 0.5 & 0.550 \\ 0.455 & 0.265 & 0.450 & 0.5 \end{bmatrix}$$

$$R^5 = [r^5_{ij}] = \begin{bmatrix} 0.5 & 0.320 & 0.550 & 0.510 \\ 0.680 & 0.5 & 0.730 & 0.690 \\ 0.45 & 0.270 & 0.5 & 0.460 \\ 0.490 & 0.310 & 0.540 & 0.5 \end{bmatrix}$$

$$R^6 = [r^6_{ij}] = \begin{bmatrix} 0.5 & 0.280 & 0.500 & 0.580 \\ 0.72 & 0.5 & 0.72 & 0.800 \\ 0.50 & 0.28 & 0.5 & 0.580 \\ 0.420 & 0.200 & 0.42 & 0.5 \end{bmatrix}.$$

步驟 2. 風險彙整 (Risk Aggregation)－彙整m位決策者之模糊多數(fuzzy majority)偏好值；本研究採用模糊多數(Fuzzy majority)量測 "超過半數的決策者同意大部份資產的風險評估結果"("*at least half* "of decision makers are agree to "*most*" of the risk rating on information assets)，其中語意量詞 Q_1 = "*most*"且 Q_2 = "*at least half*"。令 $w_i = Q(i/m) - Q((i-1)/m)$ ，針對 Q_1 = "*most*" 其語意函數區間爲 (0.3, 0.8)，利用方程式(8)計算OWA運算子之權重向量：

$w_1 = Q(1/6) - Q(0/6) = 0$ ， $w_2 = Q(2/6) - Q(1/6) = 0.06$ ，$w_3 = Q(3/6) - Q(2/6) = 0.34$。依相同程序可獲得權重向量 $W = [0.0, 0.06, 0.34, 0.333, 0.267, 0.0]$。接下來，利用方程式(13)整合 OWA 運算子與模糊語意量詞 Q 以獲得群體模糊偏好值如下：

$$R = [r_{ij}] = \begin{bmatrix} 0.5 & 0.347 & 0.480 & 0.429 \\ 0.635 & 0.5 & 0.551 & 0.563 \\ 0.498 & 0.376 & 0.50 & 0.4869 \\ 0.530 & 0.380 & 0.481 & 0.5 \end{bmatrix}$$

針對 Q_2 = "*at least half*"權重向量其語意函數區間爲 (0.0,0.5); 依相同程序可獲得權重向量 $W = [0.667, 0.333, 0.0]$。

步驟 3. 風險排序－使用方程式(14)求取群體語意量詞之風險主導(Dominance Degree, DD)程度，其代表資訊資產 a_j 相對於其他資產的風險強度如下：

	a_1	a_2	a_3	a_4
$DD(a_j)$	0.463	0.611	0.494	0.513

編號 2 的資訊資產有最高的風險值，資訊資產之風險排序爲 $a_2 \succ a_4 \succ a_3 \succ a_1$ 。

步驟 4. 風險等級之判斷－ 利用風險層級矩陣 (risk-level matrix, RLM) 以決定資產之相對風險等級如表六。

步驟 5. 風險判斷結果之確認－使用方程式(15)求取個資產之風險非主導 (Non-Dominance Degree, NDD)程度，以確認最高風險資產：

	a_1	a_2	a_3	a_4
$NDD(a_j)$	0.955	1.000	1.000	0.998

從表六及步驟三的結果得知編號 2 的資訊資產有最高的風險值， Non-Dominance Degree 之計算結果與 Dominance Degree 獲得相同的結論。

當組織完成風險等級計算後，即可依據組織之資訊安全政策並考量預算限制，訂定可接受之風險水準，凡風險值高於可接受風險水準之資產項目視爲關鍵項目予以優先處理，選擇適當之風險處理方式，以確保將風險降低至可接受的程度。

伍、討論

本研究採用群體決策理論進行資訊資產之風險分析，針對本研究所提的方法須與先前研究的定性風險分析法作比較，以驗證方法論之正確性。此外，實務上對風險分析方法選擇及須注意事項亦在本節作討論。

一、方法之比較

爲確認方法的正確性，本研究將研擬方法與模糊簡單加權決策方法(Fuzzy Simple Additive Weighting, FSAW)[7,8]作比較，兩方法運用於相同之範例資料，並將比較結果說明如下：

因爲每位參與分析風險專家之認知與經驗不同，風險評分值之權重向量亦隨之改變。在缺乏風險專家之背景資訊或爲求公平起見，通常將權重向量設爲 1/m，其中 m 爲專家數目，運用平均運算子以彙整各專家之風險評分值如下：

$$r_j = \sum_{i=1}^{m} w_i \otimes r_j^i = (1/m) \otimes (r_j^1 \oplus ... \oplus r_j^m) \qquad (17)$$

其中， $r_j^i = \frac{1}{n-1} \sum_{\substack{k=1 \\ k \neq j}}^{n} r_j^i w_i = [1/6,1/6,1/6,1/6,1/6,1/6]$ ，i=1,…,6；符號⊗代表模糊乘法，而符號⊕代表模糊加法。r_j 爲 m 個專家風險評分值之模糊平均值。

對模糊簡單加權決策法之計算結果，我們將它記錄於表六。明顯的，編號 2 的資訊資產有最高的風險值，資訊資產之風險排序爲 $a_2 \succ a_4 \succ a_3 \succ a_1$。 模糊簡單加權決策法之計算結果與本研究所提方法獲得相同的結果。

從表六及方程式(17)，因爲風險分析牽涉個人主觀意見，傳統模糊方法無法分析群體之多數決，本研究導入群體決策理論之柔性共識方法，改善傳統模糊方法之平均共識的單一作法。此外，傳統模糊方法無法依需求在資訊彙整過程中區別不同的風險強度(權重向量)，其代表的意義爲無法分別專家間風險分析意見的權威性。

二、風險分析方法選擇

因爲風險分析是一項專業工作，目前各研究機構已發展數個風險分析模式以協助組織客觀決定系統的風險值。風險分析方法因不同目標與應用有不同的計算方法，方法與工具選擇須經過

資訊安全專家確認後方可應用，並不加以限定某一方法。但各企業可依據需求，參考相關文獻，選擇合乎本身需求的風險分析模式。以下說明執行風險分析需注意事項。

（一）選擇適用之風險分析方法

由於每個組織的營運特性、內外部環境皆有所差異，即使面對相同的威脅與脆弱性，其發生機率或強度都可能有所不同，所以組織內部應先就面臨的威脅與脆弱性之發生機率或強度達成共識，才可決定資訊資產風險值，在本文第三節中所介紹之風險分析模式使用限制－資安輔導的顧問須在資產風險分析前作決策規則說明，當風險專家對資訊資產的風險因素及其影響認知不同時,“多數決”是如何決定，若有重大爭議時是保留待下一階段決定或逕行以“多數決”作決策是須於事前說明並取得顧客及(外部/內部)評審的諒解！若對決策規則說明缺乏共識情況下，不可直接引用本方法。

（二）使用適當的軟體輔助工具

如前面所述，一項資產可能會有一個或多個脆弱性，而每個脆弱性亦可能會被一個或多個威脅所利用，組織在進行風險分析時，必須定義資產、脆弱性與威脅三者間之關聯性，並計算其風險值，當資產項目越多，其定義關聯性與計算風險值之工作將越繁重，另一方面，因組織爲反映業務之最新狀況，須定期或不定期對各項業務服務過程中之重要資產重新進行資訊安全風險分析，在進行風險分析時，通常是以團隊集體討論之方式進行，對問題之研討經常須反覆檢討修訂，資料維護工作將更爲頻繁，因此，爲使風險分析之過程更有效率，建議組織應視實際狀況自行開發適用之軟體工具或選用合適的市售套裝軟體。

總之，資訊資產是組織活動的核心，組織藉由風險分析與風險管理程序，系統化的瞭解其資訊資產所面臨的威脅與脆弱點，並採取相對應之控管措施，以確保資訊資產之安全，然而，由於組織內部與外在環境不斷在變化，風險分析與風險管理亦應定期或不定期進行，以反映政府資訊安全管理政策、法令、技術及組織業務之最新狀況，以確保資訊安全之實務作業確實遵守資訊安全政策，及確保資訊安全實務作業之可行性及有效性。

陸、結　語

本研究將風險分析問題視爲群體風險決策問題，面對不完整及模糊資料，所提的方法可提供組織作風險分析與決策建議使用。經實例證明，本方法爲一簡單好用的風險分析作法，可有效降低群體共識之複雜度及決策所需的時間。未來研究方向可朝風險決策發生意見不一致及衝突時，如何尋求一個妥協解答及妥協解區間的估算，與風險決策的協商的數學模式亦可爲研究方向。

參考文獻

1. 2003 CSI/FBI Computer Crime and Security Survey, http://www.visionael.com/products/security_audit/ FBI_CSI_2003.pdf.
2. Carroll, J. M., “Decision support for risk analysis, “ Computers & Security, Vol. 2, Issue

3, pp. 230-236, Nov. 1983.

3. Center of Risk Management of Engineering System (CRMES), Ranking of Space Shuttle FMEA/CIL items: the Risk Ranking and Filtering (RRF) method, university of Virginia, Charlottesville, 1991.
4. BS7799-2:1999, “Information security management - part 2: Specification for information security management systems”.
5. BS7799-2:2002, “Information security management systems- Specification with guidance for use”.
6. Chiclana, F., Herrera, F., Herrera-Viedma E., “A classification method of alternatives for multiple preference ordering criteria based on fuzzy majority,” J. Fuzzy Math., Vol. 34, pp. 224 –229, 1996.
7. Chen, S-H and Hwang, C.L., “Fuzzy Multiple Attribute Decision Making Methods and Applications,” Springer-Verlag, Berlin, Heidelberg, New York, 1992, pp. 491-493.
8. Chen, S-M, “Fuzzy group decision making for evaluatting the rate of aggregative risk in software development,” Fuzzy set and Systems, Vol. 118, pp.75-88, 2001.
9. Chen, S-J, and Chen, S-M, “Fuzzy risk analysis based on similarity measures of generalized fuzzy numbers,” IEEE Trans on fuzzy sysytems, Vol. 11, No. 11, Feb 2003.
10. Filev, D. and Yager, R.R., “On the Issue of obtaining OWA Operator Weights,” Fuzzy set and Systems, Vol.94, pp.157-169, 1998.
11. Guan, B.C., Lo, C.C., Wang, P., Hwang, J. S., “Evaluation of information security related risks of an organization- The application of multi-criteria decision-making method,” IEEE 37th International Carnahan Conference on Security Technology (ICCST), 2003.
12. Gary, S. et al., “Risk Management Guide for Information Technology Systems”, Special Publication 800-300, National Institute of Standards and Technology, 2001.
13. Halliday, S. et al, ”A Business Approach to Effective Information Technology Risk Analysis and Management”, Information Management & Computer Security, Vol.4, pp. 27-28, 1996.
14. Herrera, F. et al, “A Rational Consensus Model in Group Decision Making Using Linguistic Assessments,” Fuzzy set and Systems, Vol.88, pp. 31-49, 1997.
15. Herrera-Viedma, Herrera, E., F., and Chiclana, F., "A Consensus Model for Multiperson Decision Making With Different Preference Structures," IEEE Transactions on Systems, Man and Cybernetics, IEEE, Vol. 32, 2002, pp. 394 – 402.
16. ISO/IEC TR13355, Part 1: The Concept and Model of IT Security.
17. ISO/IEC TR13355, Part 3: Techniques for the management of IT Security.
18. ISO/IEC 17799:2000, “Information technology-code of practice for information security management”.
19. Kaufmann, A. and Gupta, M. M. Introduction to Fuzzy Arithmetic Theory and Application, New York, 1991.
20. Koller, G. R., “Risk assessment and decision

making in business and industry: a practical guide," CRC press, 2000.

21. Kacprzyk, J. and Fedrizzi, M., "A human -consistent" degree of consensus based on fuzzy logic with linguistic quantifiers," Mathematical Social Sciences Vol. 18, pp. 275-290, 1989.
22. Klir, G. and Yuan, B., Fuzzy sets and fuzzy logic, Prentice Hall International, Inc. London, 1995.
23. Lee, H. M., "Group decision making using fuzzy sets theory for evaluating the rate of aggregative risk in software development," Fuzzy Sets and Systems, Vol. 80, Issue 3, pp. 261-271, 24 June 1996.
24. Lichtenstein, S., "Factors in the selection of a risk assessment method," Information Management & Computer Security, 4/4 20-25, 1996.
25. Orlovski, S. A., "Decision-making with a fuzzy preference relation," Fuzzy Sets and Systems Vol.1, pp.155-167, 1978.
26. Smolikova, R. and Wachowiak, M.P., "Aggregation operators for selection problems," Fuzzy Sets and Systems, Vol. 131, pp.23-34, 2002.
27. http://www.security-risk.analysis.com.tw/
28. Tanino, T., "Fuzzy preference ordering in group decision making," Fuzzy set and Systems, Vol. 12, pp.117-131, 1984.
29. Tsaur, S-H, Tzeng, G-H, and Wang, K-C, "Evaluation Tourist Risks from Fuzzy Perspectives," Annual of Tourism Research, Oct. 1997.
30. Tanino, T., "Fuzzy preference ordering in group decision making," Fuzzy set and Systems, Vol. 12, pp.117-131, 1984.
31. Wang, J., LIN, Y-I, "A Fuzzy Multicriteria Group Decision Making Approach to Select Configation Items for Software Development," Fuzzy Sets and Systems, Elsevier Science, Vol. 134, 2003, PP. 343–363.
32. Weber, P. "Fuzzy fault tree analysis," IEEE World Congress on Comp. Intelligence, Proceedings of the Third IEEE Conference on Fuzzy Systems vol.3, pp.1899-1904, June 1994.
32. Yager, R. R., "On ordered weighted averaging aggregation operators in multi criteria decision making," IEEE Trans. Systems Man, Cybernet. Vol.18, pp.183-190, 1988.
33. Yacov, Y. H., Risk Modeling, Assessment and Management, John Wiley publication, 1998.
34. Zadeh, L. A., "A computational approach to fuzzy quantifiers in natural languages," Comput. Math. Appl. 9, pp. 149-184, 1983.

附錄

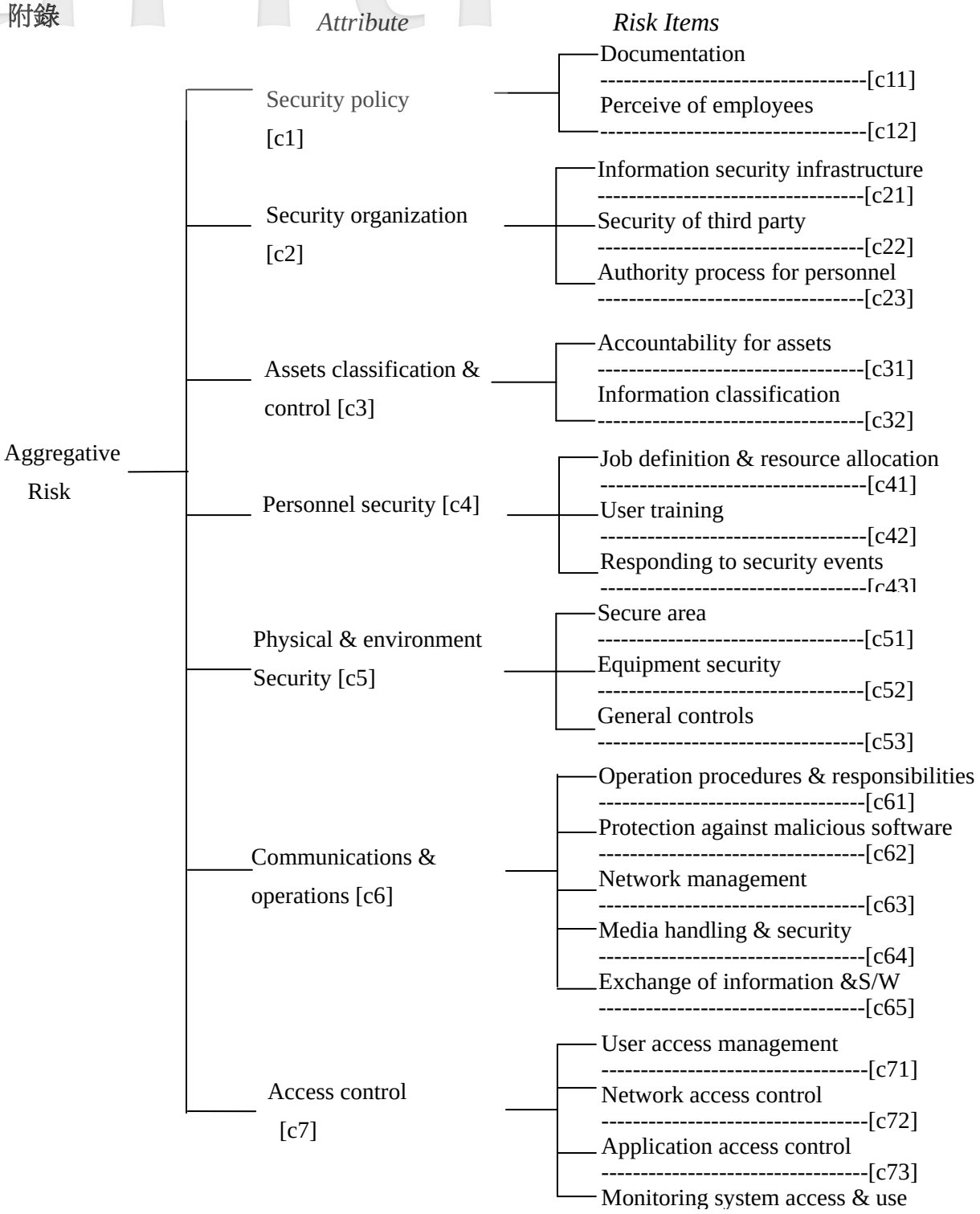


圖 六. 網路資料中心之風險分析架構圖 (Represents the Sign of Each Risk Item)

表 3. 專家 d_1 分析風險項目重要性的語意量詞

Assets \ Risk Items	c_{11}	c_{12}	c_{21}	c_{22}	c_{23}	c_{31}	c_{32}	c_{41}	c_{42}	c_{43}	c_{51}
a_1	M	MI	I	I	MI	MI	M	M	MI	MI	MI
a_2	M	I	VI	MI	MI	I	MI	M	I	MI	MI
a_3	M	I	I	MI	M	I	M	MI	I	I	MI
a_4	MU	I	I	VI	M	MI	MU	I	VI	M	MI

Assets \ Risk Items	c_{52}	c_{53}	c_{61}	c_{62}	c_{63}	c_{64}	c_{65}	c_{71}	c_{72}	c_{73}	c_{74}
a_1	MU	M	I	I	MI	I	I	I	VI	I	MI
a_2	M	MI	VI	I	VI	I	VI	I	I	VI	MI
a_3	MU	MI	I	I	M	I	I	MI	I	I	MI
a_4	M	MI	I	VI	I	VI	I	I	VI	I	I

(Note: linguistic terms for the likelihood of threats of each alternative for decision makers $d_2 \sim d_6$ are omitted)

表 4. 專家 d_1 分析衝擊損失程度之語意量詞

Assets \ Risk Items	c_1	c_2	c_3	c_4	c_5	c_6	c_7
a_1	M	M	M	M	H	H	H
a_2	L	L	VL	H	VH	VH	VH
a_3	M	L	L	VH	M	H	H
a_4	L	M	M	H	H	H	M

表 5. 資訊資產的風險分析(模糊數)

DMs \ Assets	a_1	a_2	a_3	a_4
d_1	(0.15,0.43,0.65,0.77)	(0.23,0.45,0.66,0.83)	(0.35, 0.50,0.61,0.85)	(0.43,0.54,0.76,0.88)
d_2	(0.42,0.53,0.75,0.88)	(0.45, 0.67,0.79,0.94)	(0.52,0.59,0.69,0.73)	(0.37,0.49,0.65,0.79)
d_3	(0.45,0.55,0.65,0.87)	(0.51,0.56,0.75,0.89)	(0.55, 0.75,0.84,0.92)	(0.51,0.66,0.76,0.80)
d_4	(0.33,0.47,0.65,0.79)	(0.53,0.65,0.77,0.87)	(0.44, 0.55,0.65,0.71)	(0.41,0.55,0.63,0.66)
d_5	(0.54,0.63,0.78,0.90)	(0.62,0.75,0.88,0.96)	(0.47,06.9,0.77,0.82)	(0.45,0.66,0.75,0.87)
d_6	(0.35,0.55,0.76,0.88)	(0.56,0.77,0.81,0.94)	(0.45, 0.57,0.69,0.93)	(0.35,0.47,0.69,0.87)

表 6. 資訊資產的風險等級

Information Asset	*FSAW*	$DD(a_j) = F_Q(r_{kj})$	
	Risk Value	Risk Value	Risk Level
(a_1) database server	0.434	0.463	Medium
(a_2) mail server	0.574	0.611	Medium High
(a_3) firewall device	0.495	0.494	Medium
(a_4) portal web server	0.498	0.513	Medium High

作者簡介

Chi-Chun Lo. He is the professor of department of Information Management, National Chiao Tung University. His research interests include computer network, computer security, data communication protocol, operating systems, and parallel processing.

Ping Wang. He received the Ph. D. degree in information management from National Chiao Tung University, Hsinchu, in 2005. His research interests include risk assessment, computer security, software engineering, software development for real-time system and project management.

K-M Chao. He is the professor of department of Information Management, Coventry University, UK. His research interests include decision analysis, semantics web technique and artificial intelligence.