張昭憲、莊秉諺（2017），『以行為狀態變遷為基礎之線上拍賣詐騙偵測方法』，*中華民國資訊管理學報*，第二十四卷，第一期，頁 97-130。

以行為狀態變遷為基礎之線上拍賣詐騙偵測方法

張昭憲*
淡江大學資訊管理學系

莊秉諺
淡江大學資訊管理學系

摘要

近年來，線上拍賣的蓬勃發展有目共睹。線上拍賣交易兼具便利性與隱蔽性，且不受時間與空間的限制，使得交易量逐年顯著提升。然而，面對如此蓬勃的交易平台，許多詐騙者開始混雜其中，謀取不法利益。詐騙的方式不但多樣化，且經常隨著時間、環境改變，令人防不勝防。為了協助交易者早期發現詐騙陷阱，避免蒙受不必要的損失，本研究以行為狀態分析為基礎，發展了一套線上拍賣詐騙偵測與預警方法。首先，針對詐騙者及正常者的交易記錄進行時序切割，再對其特徵值向量進行分群，以歸納出典型的交易者狀態。而後，針對資料集中所有的交易歷史進行狀態變遷切割，以產生與時序行為相關的偵測模型。在此同時，我們也利用狀態切割後的資料集，製作狀態標籤字串，並產生循序樣式，供使用者比對、監控可疑帳號。根據上述方法，本研究實作了一套簡易的線上拍賣交易輔助系統，輔助使用者在交易前觀察、分析交易對象的行為。為了驗證提出方法之有效性，本研究使用拍賣網站實際交易資料進行實驗，結果顯示本研究提出之方法確實有助於提升詐騙偵測之準確性與預警能力。

關鍵詞：詐騙偵測、網路詐騙、線上拍賣、資料探勘、電子商務

* 本文通訊作者。電子郵件信箱：jschang@mail.im.tku.edu.tw
2014/05/12 投稿；2015/10/15 修訂；2016/02/20 接受

Chang, J.S. and Jhuang, B.Y. (2017), 'An online auction early fraud detection method based on behavioral status transition of traders', *Journal of Information Management*, Vol. 24, No. 1, pp. 97-130.

An Online Auction Early Fraud Detection Method Based on Behavioral Status Transition of Traders

Jau-Shien Chang*
Department of Management Information Systems, Tamkang University

Bing-Yan Jhuang
Department of Management Information Systems, Tamkang University

Abstract

Purpose－The fraudsters' strategies of online auctions are diverse and changing rapidly. It results in the difficulty of fraud detection and prevention. The purpose of this paper is to develop effective methods to help discovering online auction fraud as early as possible.

Design/methodology/approach－This paper develops effective detection methods based on behavioral state transition of fraudsters. First, we partition and duplicate the transaction histories of traders according to trading events. Then, a reduction method based on state transition is developed to reduce the size of data set, which is then used to build the detection model. In addition, the state label strings are used to conduct the behavioral patterns of suspects for monitoring.

Findings－To demonstrate the effectiveness of the proposed methods, real transaction data are gathered from online auction sites for experiments. The results show that our methods do increase the detection accuracy and demonstrate that the early fraud detection by behavioral monitoring is possible.

Research limitations/implications－The limitations of this work is that the proposed method could be ineffective for the fraudsters who steal or buy other normal

* Corresponding author. Email: jschang@mail.im.tku.edu.tw
2014/5/12 received; 2015/10/15 revised; 2016/02/20 accepted

accounts for disguise. Albeit being difficult, it is still possible to discover them by monitoring their behavioral changes in some critical time point. Certainly, it needs newly-developed detection methods.

Practical implications－If the developed methods can be implemented and incorporated into the routine tasks of real online auction sites, the efforts of monitoring abnormal traders can be greatly reduced and the cost of maintaining a smooth trading environment can drop significantly. As a result, the fraud events will be effectively suppressing and the users will have more confidence in trading with online auctions.

Originality/value－To apply state transition concept to detect latent fraudsters, which extends intuitive decision tree and other learning models to more complicated time-based analysis. Thus, based on the proposed novel approaches, new methods can be developed to discover more well-camouflaged fraudsters.

Keywords: fraud detection, internet fraud, online auction, data mining, e-commerce

壹、緒論

近年來，線上拍賣的蓬勃發展有目共睹。線上拍賣交易兼具便利性與隱蔽性，且不受時間與空間的限制，對於交易量的提升有極大的幫助。在 2013 年第三季，世界最大網路拍賣業者－eBay 的拍賣營收便超過 600 億新台幣，其興盛程度可見一斑（eBay 2013）。然而，如此高的交易量也不可避免地產生許多交易糾紛，其中最嚴重的莫過於詐騙。詐騙的方式不但多樣化，且常隨著時間、環境改變，讓人難以防備（NW3C 2012）。由於詐騙者通常無需與受害者面對面，更讓這些罪犯有恃無恐。根據 NW3C（2009）的統計，2008 年拍賣詐騙佔所有網路詐騙的 50%以上，其嚴重程度可想而知。雖然近幾年來拍賣詐騙的案件已經降低，但損失金額仍高居網路犯罪的前五名（NW3C 2011; NW3C 2012）。上述現象顯示，現今的拍賣詐騙有了新的變化，也就是單一詐騙案件的損失金額增加，詐騙者的生命週期變短。此外，也進一步證明詐騙者為了增加成功率以及避免被識破，隨時可能發展出新的詐騙策略。

為了避免交易糾紛與日益猖獗的詐騙，網路拍賣業者經常提供簡易的名聲管理系統，供使用者挑選合適的交易對象。常見的設計為二元名聲系統，也就是每次交易後，買賣雙方互相給評，獲正評者加一分，獲負評者減一分，最後以總得分來代表交易者的名聲（eBay 1995）。面對如此簡易的設計，狡猾的詐騙者很快想出對策。針對不同目標與環境，詐騙者會使用不同策略來進行詐騙。當扮演賣方角色時，典型的詐騙手法為先以假交易（或低價商品交易）快速建立名聲，之後出售高價品，收到匯款後卻不出貨。當詐騙者扮演買方時，則可在收到物品後，百般挑剔，以瑕疵為由，恐嚇、檢舉無辜的賣方，以從中獲利（Chua & Wareham 2004）。詐騙本身是一種異常行為，有不同的執行策略，從簡單的單點異常（point anomaly），以至於最複雜的集合式異常（collective anomaly），均可能發生（Chandola et al. 2009）。線上拍賣詐騙者為了躲避偵測，通常使用複雜的策略，產生集合式異常。換言之，詐騙者會進行一系列的活動（activities），在某段時間內進行某種型態的交易，這些活動看似正常，若非一次檢視多個活動，很難看出其端倪（Fawcett & Provost 1999; Chang & Chang 2010b）。上述特質顯示詐騙是一種與時間相關的行為，而非一次性的事件。當執行完一系列的動作後，詐騙者可讓自己處於特定的偽裝狀態。例如，當詐騙者完成多次的低價商品交易後，可讓他處於「高評價、高交易密度、低平均單價」的狀態。或許，在這樣的狀態下，比較容易吸引無辜的交易者與他交易。因此，縱使有名聲系統的輔助，經驗較少的交易者不容易發覺這些精細的犯罪技巧，容易淪為詐騙受害者（Gavish & Tucci 2008）。

有鑑於名聲系統的重要，學者們紛紛發展更周詳的方式來計算交易名聲，以協助交易者挑選交易對象。為了提供可考的參考資訊，名聲系統應各種不同面向來檢視交易行為（Selvaraj and Anand 2012; Sherchan et al. 2013; Tavakolifard & Almeroth 2012）。例如，Schmidt 等（2007）建議將交易金額與評價時間列入計算名聲時的考量，以避免有人利用小額交易累計高評價，並防範長時間佈置的詐騙者。Chang 與 Wong（2011b）則進一步考量商品領域的相似度，希望根據買方的待購商品類型，計算賣方在此領域的名聲。Kaszuba、Hupa 與 Wierzbicki（2010）對拍賣網站的文字評語進行深入分析，將各種不良名聲分類，並提出一套新的信任度表示法。雖然複雜的名聲系統雖然能增加詐騙難度，但由於牽涉繁複的運算，對於動輒超過百萬甚至千萬會員的拍賣網站，可能產生極大的運算負擔。此外，名聲累計規則一旦公布，很難隨時更改，詐騙者便會針對其弱點，發展新的因應之道。因此，除了名聲系統外，許多學者也開始發展各種詐騙偵測方法，以更積極的方式協助使用者辨識可疑交易對象。

詐騙偵測是一種分辨正常交易者與詐騙者的流程。為了發展有效的詐騙偵測方法，通常需要一套合適的屬性集（Attribute Set）來描述、擷取交易者的特質（Yu & Liu 2004）。當這些特質擷取完畢後，還需一套特定的學習演算法來建立偵測模型。針對屬性集的發展，Chau 與 Faloutsos（2005）及 Chau、Pandit 與 Faloutsos（2006）與 Pandit 等（2007）提出了一套與價格相關的屬性集，並利用分類樹來建立偵測模型。為了提升偵測效果，Chang 等（2009; 2010a; 2010b）則發展以評價（feedbacks）為導向的屬性集，並以分類樹與 Instance-based learning 來實現其偵測方法。在發展詐騙偵測系統時，除了準確度外，還需考量潛伏期的詐騙者。狡猾的詐騙者經常有良好的偽裝，讓交易者不容易看出端倪。針對潛伏期詐騙者的早期預警，Chang 等（2010a; 2011a）進一步提出混階塑模（hybrid modeling）的方法，以有效偵測潛伏期的詐騙者。除了單一詐騙者外，某些詐騙者更會以集團犯罪的方式來增加其成功率。因此，詐騙偵測並不限於單一帳號，也需考慮共犯結構的分析。在組織犯罪的發掘上，可利用社會網路分析方法（social network analysis）來歸納特定的網路關係，以協助找出詐騙共犯（Wang & Chiu 2005）。Kobayashi 與 Ito（2007; 2008）則利用圖形理論將交易網路視覺化，幫助使用者以人工方式辨識不正常的交易關係。

即使前人研究提出的偵測方法具有一定效果，但以實際應用而言，仍有以下重要問題需要解決：首先，這些偵測方法通常只將受測帳號分為詐騙（fraud）與非詐騙（non-fraud）二大類，且經常有誤判情形。此問題並非完全導因於屬性集或塑模方法效率不彰，也可能是對於詐騙行為的分析不夠周詳所致，容易忽略偽裝完善的詐騙帳號。基本上，詐騙行為並非一種結果，而是一系列的過程。因此，若偵測方法只檢驗待測帳號在某個時間點的狀態並不恰當，容易將偽裝良好

的詐騙者誤判為正常者。事實上，潛伏中的詐騙者經常在其交易紀錄中留下蛛絲馬跡。因此，可疑帳號在交易歷史中的行為變化應受到嚴格的檢視，才能辨識出狡猾的詐騙手法，提升總體偵測準確率。其次，為了詐騙防治，偵測的目標應該以著重於事發於未然，而非在詐騙發生後才提出警告。更明白地說，偵測系統最好能在受害者出現前，就能標示出詐騙者。若以此為目的，嫌疑者應被持續關注、監測，而非只進行一次性的詐騙偵測。

為了解決上述問題，本研究以交易者的行為狀態分析為基礎，發展了一套線上拍賣詐騙早期預警與偵測方法，協助使用者在交易前做出更正確的判斷。為了分析交易行為的狀態變化，我們將詐騙者及正常者的交易記錄進行時序切割，再對其特徵值向量進行分群，以歸納出典型的交易者狀態。而後，針對資料集中所有的交易歷史進行狀態變遷切割，以產生與時序行為相關的分類樹偵測模型。此外，我們也利用狀態切割後的資料集，製作狀態標籤字串（state label strings），以產生循序樣本，供使用者比對、監控可疑帳號。根據上述方法，本研究實作了一套簡易的線上拍賣交易輔助系統，讓使用者能在交易前觀察、分析交易對象的行為。為了驗證提出方法之有效性，本研究使用拍賣網站實際交易資料進行實驗。結果顯示，與前人研究相較，本研究提出之方法對於詐騙偵測確實具有較佳準確性與預警能力，有助於提升線上拍賣的交易安全。

本論文章節內容架構如下：第貳節為背景知識與相關技術的介紹；第參節為本研究提出之線上拍賣詐騙行為之時序分析方法；第肆節為系統實作；第伍節為實驗結果；第陸節為結論及未來展望。

貳、相關技術與背景知識

本節將介紹與本研究相關之術語、技術與背景知識，以利後續之討論。

一、線上拍賣交易者行為

大部分現有的網拍平台（如 eBay、Yahoo 拍賣及露天拍賣等），均採用英式拍賣（English Auction）。由多人公開進行商品競標，過程中出價金額由低至高遞增，最後由最高出價者得標。完成交易之後買賣雙方即可互相給予評價，交易者的名聲便由累計的分數來表示。由於評價分數較高的交易者較容易被信任，許多詐騙者就利用此特性，以各種方式快速累計評價（獲取他人的信任），再進行詐騙。一般而言，詐騙者的生命週期包含二個階段（如圖 1 所示），一開始為潛伏期（latent period），其後為爆發期（execution period）（Chang & Chang 2011a）。潛伏中的詐騙者會使用者各種伎倆來進行偽裝，例如大量購買低價商品以累積正評價。在爆發期，則開始設定陷阱，以引誘不知情的買方上鉤。

圖 1：詐騙者生命週期

詐騙者偽裝而後攻擊的手法雖然有效，但並非無懈可擊。事實上，只要能小心檢視可疑帳號交易歷史中的細微變化，便可大幅提升發覺詐騙的機會。交易者的交易歷史由其完成的交易所組成，這些交易與時間相關，分布於其生命週期中。為了對交易者行為進行系統化分析，以量化方式描述交易事件便顯得不可或缺。事件的發生可造成交易者狀態的改變，因此可用交易者狀態改變來反映事件的效果。描述交易者狀態最簡單的方式為使用其正評個數，每完成一筆交易，便可能造成其正評個數的改變。此外，也可透過交易平均單價來描述，一個當連續販賣多個高價商品後，交易者的狀態便可能有中價位賣家轉換為高價位賣家。除了直接用上述數值來描述外，也可計算其移動平均量，以了解其改變的趨勢。然而，許多交易者具有超過千次以上的交易記錄，若將每次交易均視為有意義的事件並不恰當，也不利於詐騙行為變化的分析。

二、詐騙偵測

對於線上拍賣交易者而言，為了避免損失，經常需在交易前確定對方是否為詐騙者。因此，詐騙偵測便成為線上拍賣交易輔助系統的一項重要功能。開發詐騙偵測方法時，通常有以下三個典型步驟：

1. 定義詐騙偵測屬性集合（Attribute set）：偵測屬性集可用來擷取交易者交易記錄中與詐騙偵測相關的特徵（Goes et al. 2009）。常見的偵測屬性有交易者的「評價分數」、「正評價百分比」、「交易頻率」、與「平均單筆成交金額」等（Chau & Faloutsos 2005; Chau et al. 2006; Chang & Chang 2009; 2010; 2011a）。考量詐騙手法的多樣化，研究者曾提出許多不同類型的偵測屬性，某些與交易價格相關、某些則與評價分數或次數統計相關（Chang & Chang 2012）。
2. 建立資料集：偵測系統需由交易網站下載大量的交易記錄（包含正常者與詐騙者），以供後續分析之用。交易記錄內容龐雜，需配合偵測屬性集來擷取其中有用的訊息，產生屬性值向量（feature value vector）。例如，若只使用三個屬性{“正評百分比”, “交易次數”，”平均單價”}，則某位交易者的交易記錄可能被抽象化為<95.8%, 250, NT$833>。
3. 建立偵測模型：接下來，以訓練資料集為輸入，透過不同的學習演算法建

立偵測模型。常見的學習方法有決策樹（Decision Trees）、instance based learning、類神經網路（Neural Networks）、關聯規則（Association Rules）等（Witten & Frank 2005）。完成上述步驟後，便可利用偵測模型來檢視可疑帳號，並將結果做為是否與其交易的參考依據。

根據上述討論，表 1 列出本論文相關研究之方法特質，除了偵測屬性與塑模方法外，還包含了「帳號分類」，是否「切割交易歷史」，是否進行「共犯偵測」，以及是否以「早期預警」為發展目標。以「帳號分類」而言，大多數研究將帳號分為二類（詐騙/正常），但為了考慮組織犯罪，Chau 等（2006）、Pandit 等（2007）與 Zhang、Zhou 與 Faloutsos（2008）則將分類擴增為三類（詐騙/共犯/正常）。在評估詐騙偵測系統效能時，除了準確度外，還需能找出潛伏期的詐騙者。若等到受害者出現才提出警告，則系統的效果將大打折扣。然而，狡猾的詐騙者經常有良好的偽裝，因此需仔細分析其交易歷史，從中歸納異常行為模式，才能達成早期預警的功能。為了瞭解詐騙者在潛伏期的行為變化，Chang 與 Chang（2009; 2010a）提出了交易歷史切割的概念（參考圖 2）。在建立資料集合時，根據他們的經驗與實驗觀察，以定點切割（fixed-partition）方式，將每一位交易者的交易歷史依照時間（生命週期）分為數個階段（80%, 85%, 90%, 95%, 100%）後，再建立偵測模型。在 Chang 與 Chang（2011a）的研究中，進一步提出混階偵測模型（hybrid-phased detection models）的概念，將定點切割後的交易

表 1：詐騙偵測相關研究之特性

相關研究 / 特性	偵測屬性（變數）來源	詐騙偵測模型建立方法	帳號分類	切割交易歷史	共犯偵測	以早期預警為目標
王俊程、邱垂鎮、葛煥元（2005）	交易資料、個人資料、社會網路指標等	類神經網路	詐騙/正常			✓
Chau & Faloutsos (2005)	交易金額、交易次數等	分類樹	詐騙/正常			
Chau 等（2006），Pandit 等（2007)	交易金額、交易次數、交易網路關係等	分類樹、Belief Propagation	詐騙/共犯/正常		✓	
Zhang 等（2008）	交易網路關係	Loopy Belief Propagation	詐騙/共犯/正常		✓	
Chang & Chang（2011a）	交易評價、交易金額、交易次數等	分類樹	詐騙/正常	✓（定點切割）		✓

歷史加以混合，以偵測狀況未知的潛伏期詐騙者。為了精簡起見，本研究將 Chang 與 Chang 提出之在交易歷史特定時間點進行切割所建立之分類模型，稱之為 FP-Model（Fixed-Partition Model）。其實驗結果顯示，相較於其他研究，混階模型對於偵測潛伏期詐騙者，確實具有較佳偵測結果。以定點切割為基礎之混階塑模流程如圖 3 所示，其中的 HTS 即為針對所有選擇帳號之交易歷史進行定點切割後，所得之混合資料集。最後，再以 HTS 為輸入，使用不同的學習方法建立詐騙偵測模型。

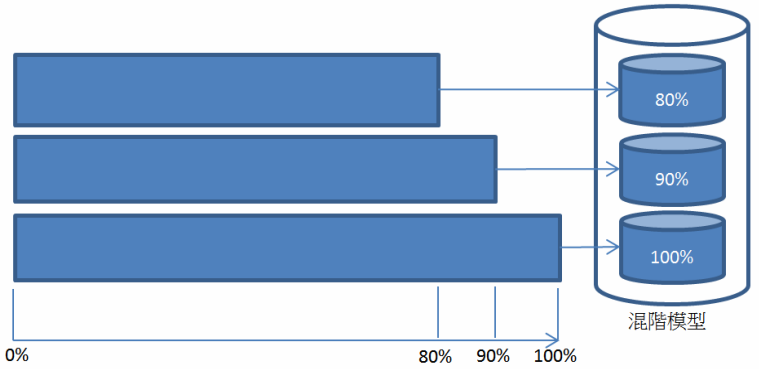

圖 2：以定點方式切割交易歷史並建立混階偵測模型（Chang & Chang, 2011a）

```
    TS: training set;  // 訓練資料集，由選定帳號之交易歷史所組成
    CT = {80%, 85%, 90%, 95%, 100%};  // 設定交易歷史切割時間點
    HTS = { };  // 混合式訓練集
    for each account c in training set TS do  //對每一個TS中的帳號c進行交易歷史切割
     for each time-point tp in CT do // 依照每一個預設時間點進行切割
         let hcp be the gathered transaction history
                              of c in the range (0, tp) of lifespan;
         let fvv be the feature value vector of hcp;
         HTS = HTS ∪ fvv ;
     end for
    end for
    build detection model by using HTS as the data input; // 利用建立偵測模型
```

圖 3：定點切割混階塑模之演算法虛擬碼（Chang & Chang, 2011a）

三、詐騙偵測之塑模方法

本研究使用分類樹做為建立詐騙偵測模型的方法。資料探勘常用的分類技術為 Quinlan（1986）提出的 ID3 演算法，根據特定的訓練資料集（Training Data），ID3 以各屬性（Attributes）的資訊增益（Gain Ratio）為評量標準，每次

找出最佳的屬性，以決定決策樹的分支節點。而後，在各個節點中不斷重複以上的選取過程，最後建構出決策樹。C4.5 演算法（Quinlan 1993）為 ID3 的改進版本，改用資訊增益率（Information Gain Ratio）做為屬性挑選依據。此外，C4.5 可同時處理連續與離散屬性，並加入樹枝修剪功能，分類效能較 ID3 為佳。因此，本研究使用 C4.5 演算法（Quinlan 1993）做為塑模方法，透過呼叫 Weka 工具集（Witten & Frank 2005; Weka 2014）中的 J48 API（C4.5 的 Java 實作版本），建立偵測模型。圖 4 所示為一簡化過之詐騙偵測決策樹，此模型顯示，若有一待測帳號的評價小於 50，且平均交易金額小於 300，則可被歸類為詐騙者。

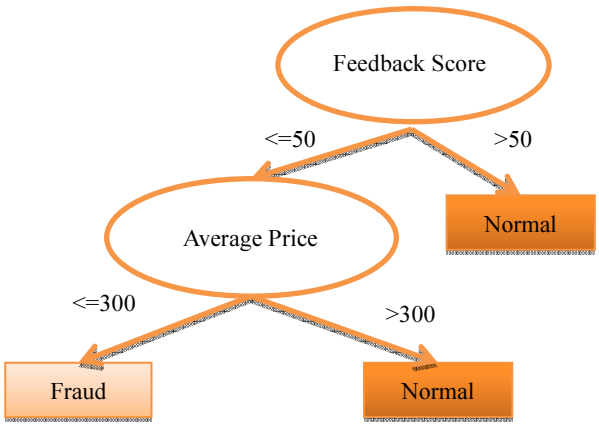

圖 4：詐騙偵測決策樹範例

為了歸納交易者的行為特質，本研究使用群集分析（Clustering）來找出各種典型，並將其應用在交易歷史分析中。透過分群結果，更容易看出詐騙者與正常者特徵之不同，並有利於交易行為狀態變遷的觀察。K-Means 演算法為最常見的分群演算法，各群的群心可用來代表各群聚的典型特質。然而，K-means 演算法需要事先決定 k 值得大小，在應用時經常造成困擾。為避免需事先決定群聚個數，本研究決定改採 X-means 分群演算法（Pelleg & Moore 2000; Ishioka 2005）來分析交易者的特質。X-means 使用 k-means 做為核心演算法，但會自行分裂群聚，並以 Bayesian Information Criterion（BIC）做為評量指標，以決定某次的分裂是否能產生更合適的群聚結構。當所有分裂步驟均停止時，便以當時群聚結構做為最後的分群結果。

循序樣式探勘（Sequential Pattern Mining）被用來找出經常出現的事件序列（Agrawal & Srikant 1995;1996; Pei & Han 2001; 2002），本研究將其應用在交易行為狀態序列的歸納，以做為後續監控與早期預警的根據。探勘出的循序樣式如 <abd>，表示 a, b, d 事件依序發生，但有先後關係，其中 b 與 c 則一起發生。以

詐騙偵測而言，a 可能對應至「高正評密度」，b 可能代表「高平均售價」，d 則可能是「高負評比」。這樣的樣式標示出，詐騙者可能一開始以獲得高正評密度為目標，之後再以高單價貨品為誘餌（並及於成交），最後則以獲得眾多負評來結束。找出詐騙者在其生命週期中行為變化的特質，與在資料集中探勘出時間相關的循序樣本類似。在詐騙偵測時，每筆記錄代表一位交易者的特徵值向量（feature value vector），每個特徵值則由分析、統計該位交易者的交易歷史而得。若能分析詐騙行為常見的事件集，對於了解詐騙發生的背景與時間點有很大的幫助（Brown & Oxford 2001）。只是，如何在線上拍賣的應用中定義何謂「顯著事件（significant events）」，是一件具有挑戰性的工作。

參、以狀態變遷為基礎之詐騙偵測方法

如前所述，詐騙偵測系統應在詐騙發生前，對使用者提出警告，才有實用價值。為了事發於未然，分析詐騙者潛伏期行為的變化，是必要的步驟。為了達成此目的，本研究提出一套狀態變遷為基礎之詐騙偵測方法，從交易歷史中找出交易者屬性值產生變化的交易事件，以產生包含交易歷程特質的資料集。之後，再據以產生更具辨別能力的早期預警詐騙偵測模型，其細節將在以下各小節敘述。

一、產生時序相關的資料集：交易歷史的切割與複製

如前所述，為了瞭解詐騙者在潛伏期的行為變化，Chang 與 Chang（2009; 2010a, 2011a）提出了交易歷史切割的概念。在建立資料集合時，以定點切割方式，將每一位交易者的交易記錄分為數個階段（80%, 85%, 90%, 95%, 100%）後，再進行混階塑模。然而，根據我們的觀察，此種定點分割方式最大缺點為切割單位的決定不易。若間隔太大，容易漏失重要歷程，間隔太小則與窮舉法無異。此外，由於每位交易者的生命週期並不相同，定點切割法卻以一視同仁的方式，在特定時間點切割、擷取他們的分段交易特徵，顯然有改善空間。為解決上述問題，本研究提出了一套以狀態變遷為基礎之交易歷史切割方法，以下說明方法之詳細步驟與特點。

以狀態變遷為基礎之詐騙偵測包含二個主要程序：(1)切割與複製，(2)狀態變遷縮減。圖 4 所示為程序一（切割與複製）之虛擬碼，此程序針對每位交易者，以其歷次交易事件為切割點，產生多份部分重複之交易歷史。相關細節說明如下：假設蒐集而得的交易歷史共有 n 筆，令 $TH=\{H_1,H_2,\ldots,H_n\}$表示此集合，且 H_i 對應至交易者 C_i 的交易歷史。再假設塑模所用之偵測屬性集合為 $AS=\{A_1,A_2,\ldots,A_m\}$，交易者 C_i 的交易記錄可使用一個屬性值向量 $AV(TH_i)=<a_{1,i},a_{2,i},..,a_{m,i}>$來表示。舉例而言，若 AS={“總評價”,”平均交易金額”,”買

賣比例"}，則某為交易者 C_k 的屬性值向量 $AV(TH_k)$可能為<85, NT$475, 0.25>。為了分析每位交易者最近的行為特質，首先將 C_i 的交易歷史 H_i 分割為 $H_i = H_i(W)' \cup H_i(W)$，其中 $H_i(W)$為 C_i 最後 W 天的交易記錄。假設 C_i 在最後 W 天內共完成 T_i 筆交易，則可令 $H_i(W)=<TRB_{i,1}, TRB_{i,2},\ldots, TRB_{i,|Ti|}>$。據此，$C_i$ 的交易歷史 H_i 將被切割複製為 T_i 份後，其中 $P_{i,1}=H_i(W)' \cup \{TRB_{i,1}\}$, $P_{i,j}=P_{i,j-1} \cup \{TRB_{i,j}\}$。至此，便可將每一筆 $AV(P_{i,j})$加入資料集合 DS 中。持續切割每一筆 H_i，將其屬性值向量加入 DS，則為後 DS 集合的元素個數當為 $|DS| \sum_{i=1}^{n} |T_i|$。以圖 5 的交易記錄為例，假設 W=90，使用者在最後 90 天內有 4 筆交易，則切割後，將產生 4 組屬性值向量。

```
// === 程序一:交易歷史的分割與複製 ===
// 任務:以交易歷史中的交易事件為斷點，逐一切割並複製留存每位交易者的交易歷史
Procedure Partition_And_Duplication
input:      TH={H1,H2,…,Hn} //  TH 代表所有交易者(C1,C2,…,Cn)之交易歷史集合
AS={A1,A2,…,Am} //  代表選用的偵測屬性集(attribute set)
W // 回溯天數
output: DS  // 儲存經過切割、複製後的交易歷史之屬性向量
       APS // 內含 n 個集合，每個集合代表每位交易者切割、複製後之交易歷史屬性向量
begin
 // 產生集合 DS，負責儲存所有經過切割、複製後的交易歷史之屬性向量
DS = {} ;
  // 產生集合 APS，以交易者為單位，儲存切割、複製後的交易歷史屬性向量(將包含 n 個集合)
APS = {} ;
  //-- 以下迴圈將對每位交易者的交易歷史(Hi)進行切割與複製，並將結果存於 DS 與 APS --
for each Hi in TH do
       Let Li be the lifetime of trader Ci ; // Li 為 Ci 之生命週期，單位(天)
       // 擷取交易者 Ci 前 Li-W 天的交易歷史，儲存於 Hi(W)'
Let Hi(W)' contain transactions in the first Li-W days;
       // 擷取交易者 Ci 最後 W 天的交易歷史，儲存於 Hi(W)
       Let Hi(W) contain transactions in the last W days ;
APi = {} // 儲存交易者 Ci 切割後的交易歷史之屬性值向量，為一有序集合
Pi = Hi(W)' ;
// -- 以下迴圈針對交易者 Ci 最後 W 天的每筆交易進行以下累積彙整動作 --
for each trade TRBi,j in Hi(W) do
Pi = Pi U {TRBi,j}; // 將一筆交易紀錄 TRBi,j 加入前 Li-W 天的集合 Pi 中
APi = APi U AV(Pi); // 將 Pi 轉換為屬性向量 AV(Pi)，並存於 APi 中
            DS = DS U AV(Pi) ;  // 將 AV(Pi)也存於 DS 中以備後續分析
end for
APS = APS U {APi} // 獲得交易者 Ci 切割、複製後的交易歷史屬性向量 AV(Pi)
end for
// 經過上述程序處理後，呼叫者將取得交易歷史分割與複製的結果(DS 與 APS)
end procedure
```

圖 4：將原始資料集中之交易歷史依照交易事件進行切割與複製之流程

上述切割方式的主要優點為：每一位交易者的每一筆交易所造成的影響，都被涵蓋在後續的分析中，對於了解潛伏期詐騙者的行為特徵，應有明顯的助益。然而，對於交易頻繁的交易者而言，上述切割方式將產生龐大的子交易歷史，對塑模造成負擔。此外，在同一個交易歷史中，並非每一筆交易都能造成明顯的狀

態改變，若$AV(P_{i,j})\cong AV(P_{i,j+1})$，則同時將$AV(P_{i,j})$與$AV(P_{i,j+1})$加入DS則不太具有意義。相反地，很可能因為重複性資料的加入，扭曲後續的分析結果。有鑑於此，以下將進行交易行為狀態分析，在儘量不減損交易資訊的前提下，縮減DS的大小。

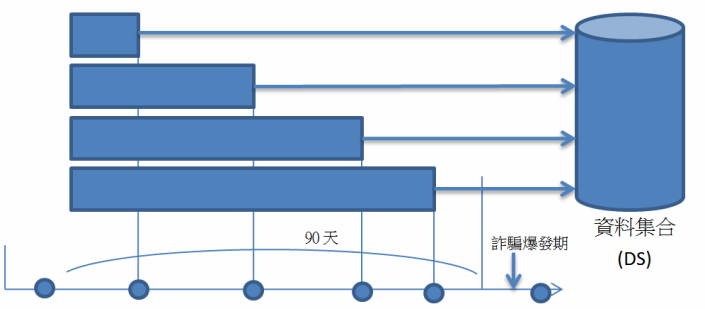

圖 5：以交易事件作為切割點

二、以狀態變遷為基礎的資料集縮減方法

根據上一節的切割、複製過程，可能會產生一個龐大的資料集（DS），影響後續的分析。為了縮減資料集，並保持其中所隱含的訊息，我們提出了一套以狀態變遷為基礎的縮減方法。首先，我們將針對交易歷史向量 DS 中包含完整生命週期之資料（100%）進行群集分析，以找出交易者典型的行為狀態。執行前，先區分詐騙者（$DS\_F_{100\%}$）及正常者（$DS\_NF_{100\%}$）的記錄，再分別進行群聚分析。如前所述，本研究使用 X-means 演算法進行分群，以避免事先決定群聚的個數。根據上述狀態分析結果，我們將 P_i 中的每個元素進行以下的縮減處理，$\forall i > 1$ 若 $State(P_{i,j-1})=State(P_{i,j})$，則 $P_i=P_i-\{P_{i,j}\}$。對於交易歷史 h，State(h)為與 AV(h)最接近之群心，對於正常者而言，其狀態只能為 NS0~NS3，對詐騙者則只能為 FS0~FS3。以圖 6 為例，若應用上述狀態分析，則可縮減為三筆記錄。這樣的縮減，既可保存交易者行為變化的特質，又能有效縮減 DS 中元素的個數。上述縮減流程的細節，請參考圖 7 中的虛擬碼。

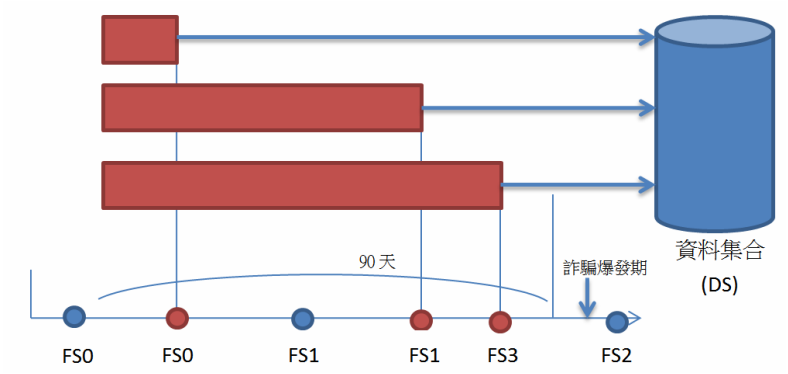

圖 6：以狀態改變之交易事件作為切割點

```
// === 程序二: 縮減交易歷史資料集 ===
// 任務:以本研究提出之狀態變遷方法為基礎，檢視並去除無法產生狀態變遷之交易歷史片段
Procedure Reduction_by_StateTransition
Input:      DS    // 內含所有交易者經過切割、複製後產生之屬性向量資料集
       APS   // 內含 n 個集合，每個集合代表每位交易者切割、複製後之交易歷史屬性向量
Output: DSR // 以狀態變遷方法縮減後的綜合資料集(包含詐騙者與正常者)
begin
  // 建立一集合 DSR，儲存狀態變遷縮減後的綜合資料集
  DSR = {} ;
  // 將交易歷史屬性向量集合 DS(參考圖 4)分割為詐騙者集合(DS_F)與正常者集合(DS_NF)
  Partition DS into DS_F, DS_NF;
  // 利用 XMeans 分群演算法對 DS_F 與 DS_NF 進行群集分析，但只使用 100%生命週期之資料
Cluster_F = XMeans(DS_F100%) ;    //  產生正常者群集
Cluster_NF = XMeans(DS_NF100%) ; //  產生詐騙者群集
// --- 透過以下迴圈去除 APS 中與交易狀態變遷無關之屬性向量集，以縮減原始資料集 ---
for each APi in APS do
  // 根據交易者 Ci 的屬性(詐騙者、正常者)選取群集集合(Cluster_F 或 Cluster_NF)
  if (Ci is a fraudster)
       Groups = Cluster_F ;
  else
       Groups = Cluster_NF ;
  // -- 根據 Ci 的交易記錄屬性向量值(APi,j)是否造成 Ci 的狀態改變來縮減資料集 --
  for each APi,j in APi do
       // 若 APi,j 確實造成狀態變遷，才將其納入縮減資料集 DSR 中
       if (State(Groups,APi,j) != State(Groups,APi,j-1))
            DSR= DSR U {APi,j}
  end for
end for
// 經過上述程序處理後，呼叫者將獲得縮減後的資料集 DSR
end procedure
```

圖 7：以狀態改變為基礎之資料集縮減方法

為了找出正常者（Cluster_NF）與詐騙者（Cluster_F）群集（參考圖 7 中虛擬碼），我們蒐集 Yahoo!Taiwan 的實際交易資料，以 X-Means 演算法進行分析。分群後的結果參考表 2，詐騙者及一般交易者正好皆分為 4 群。我們分別以 FS0~FS4 來代表詐騙者群聚，NS0~NS3 代表正常者的群聚。在後續運用中，各群聚將以其群心（centroid）來表示（代表某一類群集之典型行為特質），並將其稱

之為交易者典型狀態（state）。表 3 與表 4 所示為這 8 種狀態（群聚）的群心，均以屬性值向量來呈現（每列即為一個屬性值向量）。這些狀態將被應用於後續實驗，以驗證本研究提出方法之有效性。

表 2：詐騙者與正常者之交易行為狀態分析

詐騙者		正常者	
狀態個數（群聚個數）	群聚中的元素個數	狀態個數（群聚個數）	群聚中的元素個數
FS0	292（22%）	NS0	1967（39%）
FS1	477（36%）	NS1	604（12%）
FS2	261（20%）	NS2	1596（32%）
FS3	282（21%）	NS3	879（17%）

表 3：詐騙者分群結果

狀態屬性	以切割、複製流程產生之實例數：1312									
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
FS0	0.240	0.476	0.952	0.029	0.466	0.226	0.245	0.121	0.271	0.263
FS1	0.324	0.366	0.991	0.005	0.970	0.007	0.012	0.002	0.012	0.012
FS2	0.821	0.845	0.899	0.046	0.131	0.838	0.852	0.756	0.810	0.796
FS3	0.213	0.924	0.885	0.067	0.090	0.216	0.211	0.219	0.926	0.915

表 4：一般交易者分群結果

狀態／屬性	以切割、複製流程產生之實例數：5046									
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)
NS0	0.892	0.974	0.983	0.003	0.046	0.885	0.891	0.945	0.988	0.989
NS1	0.935	0.379	0.973	0.007	0.132	0.889	0.946	0.918	0.402	0.402
NS2	0.250	0.952	0.982	0.004	0.060	0.228	0.236	0.347	0.959	0.960
NS3	0.344	0.277	0.968	0.009	0.289	0.250	0.283	0.160	0.234	0.233

三、建立詐騙偵測模型

根據切割、複製與縮減步驟所產生的資料集合 DSR，便可被用來建立詐騙偵測模型。本研究使用 C4.5 演算法做為塑模工具，以建立分類樹模型（請參閱 2.3 節的說明）。與前人研究不同（Chau et al. 2005, 2006; Pandit et al. 2007; Chang &

Chang 2011）之處，前人所建立的分類樹的判斷結果只有 Fraud 與 Normal 二種類別，但本研究提出的方法卻可有 8 種狀態類別（參考表 2 與表 3）。這樣的設計至少有以下好處：首先，對於潛伏期詐騙者可做更精細的分類，處於不同狀態的潛伏期詐騙者（FS0~FS3）可能會有不同的行為模式，有助於後續的監控或應對。其次，詐騙偵測系統的設計者可更仔細了解誤判案例的特質，據以改善系統設計。例如，若 FS1 的詐騙者經常被誤判為 NS2 的正常者，則可針對其特質額外設計二次偵測流程。綜合前述各節的說明，本研究提出之以狀態變遷為基礎之詐騙偵測方法，可歸納為以下之流程：

1. 令訓練資料集（Training Set）為 S1，測試資料集（Test Set）為 S2。
2. 將 S1 做為程序一（參考圖 4）的輸入，進行以事件為基礎之交易歷史切割與複製，產生與時序相關之資料集（DS 與 APS）。
3. 執行程序二（參考圖 7），以狀態變遷為基礎，縮減 APS，去除因複製所產生的冗餘資料，產生縮減資料集（DSR）。
4. 以程序二產生之縮減資料集（DSR）做為訓練集，利用合適的學習演算法（如 C4.5 分類樹演算法），建立詐騙偵測模型 M。
5. 利用 M 對測試集 S2 進行分類，並統計分類結果。

此外，本研究根據線上拍賣網頁上所公布之交易歷史，挑選常用的偵測屬性，其內容大致與金額，評價，與時間等因素相關。表 5 所示即為本研究使用於交易資料分析之屬性集，其中，前四項與評價相關，5～8 項與金額相關，最後二項則與賣方特質相關。為了使學習演算法的成效不會因數值差異性太大，而導致訓練成效無法達到預期，因此在作資料分析之前，先將所有屬性進行正規化。以統計方法找出所有使用者屬性值的分佈情形，並計算其平均數 q 與標準差 s。假設考慮的樣本為常態分佈，則大約有 95%的資料會分佈在離平均數兩個標準差 $(q \pm s \times 2)$ 的範圍之內。因此設定該屬性值之上限 ub 及下限 lb，以公式 $(value-lb)/(ub-lb)$ 將屬性值 value 計算為 0～1 之間的數。由於某些屬性值本身就是從 0 到 1 的數，例：正評百分比，因此這類的屬性值將直接使用，不作正規化。

表 5：交易記錄屬性

指標名稱（英文）	指標名稱（中文）	描述
(1)累計正評	accFeedback	目前所累積正評數
(2)正評百分比	posPercent	正評佔總交易數之百分比
(3)負評百分比	negPercent	負評佔總交易數之百分比
(4)賣東西正評數	SellingNumberOfPos	賣東西所獲得的正評數
(5)平均交易金額	avgPrice	不分正負評之平均交易金額

(6)後 30 天平均賣價	MeanSellingLast30	後 30 天平均賣價
(7)總平均賣價	MeanSelling	總平均賣價
(8)總賣價標準差	StdSelling	總賣價標準差
(9)評價來自賣家的比例	RatioOfSToS	本身為賣家，正評來自賣家的比例
(10)賣東西數	SellingNumber	賣東西的交易次數

肆、線上拍賣交易者之狀態監控

詐騙偵測的重要性有目共睹，但對於潛伏期的嫌疑者，效果卻可能有限。原因很簡單，若無犯罪事實（或違反規定），拍賣網站當局並無法對特定帳號進行停權處分，且需容許他們繼續進行交易。這樣的客觀事實，很容易讓正常的交易者暴露在詐騙者的圈套之中。有鑑於此，本節將探討如何進一步運用本研究提出之狀態變遷方法，將交易歷史記錄轉換為轉換為狀態標籤字串（State Label String），探勘出詐騙者與正常者慣有的行為變化樣式（patterns），以供後續監控或偵測之用。對於逐步進入爆發期的詐騙者而言，這樣的監控流程，將有助於交易者事先避免無謂交易糾紛，進一步降低詐騙的發生率。

一、將交易歷史轉換為狀態字串

將交易歷史轉換為狀態標籤字串，有助於找出使交易者狀態改變之顯著事件。轉換過程需先統計每個交易事件切割點的屬性值向量，再根據交易者所屬類別之狀態計算的相似度（距離）附加狀態標籤字串（state label string; SLS）。假設行為塑模所用之詐騙分群狀態集為 FS={FS_0, FS_1 , ... FS_P}，待轉換之交易歷史為 H_i，且交易事件切割、複製後之資料段數為 m，則 H_i 對應之完整狀態標籤字串 SLS(H_i ,FS)可表示為

$$SLS(H_i,FS) = (s_{i,1},s_{i,2}, \ldots, s_{i,m})，其中\ s_{i,k} \in FS$$

以下舉例說明標籤字串的建立方式。表 6 所示為 Yahoo!Taiwan 公布之某位詐騙者（yangXXX）的交易歷史，其中並不包含詐騙爆發後的交易行為，以符合早期預警的前提。此帳號使用交易事件切割方式可建立 4 個切割點（圖 8），並根據正規化後的屬性值，附加最相似的狀態標籤，可得到四個狀態標籤。根據圖中所示，此交易記錄所產生的完整狀態標籤字串為

$$SLS(H_i,FS)=<FS0,FS0,FS1,FS3>$$

為了避免過多狀態樣式導致後續的訓練效果不佳，將交易事件點狀態相同之

區間合併，只記錄狀態有改變的行為。從此範例中透過狀態的合併縮減之後可得到一組精簡後的標籤字串（Compact State Label String）：

$$CSLS(H_i,FS)=<FS0,FS1,FS3>$$

表 6：詐騙者交易記錄

編號	結標時間	評價	給評方	交易帳號	金額	評價日期
1	2009-06-11	良好	買家	aabbccXXXXX	220	2009-06-11
2	2009-06-11	良好	買家	DingjXXXXX	650	2009-06-12
3	2009-06-16	良好	買家	mXXXXX	85	2009-06-16
4	2009-06-17	良好	買家	poroXXXXX	59	2009-06-18
5	2009-06-22	良好	買家	u294XXXXX	50	2009-06-22

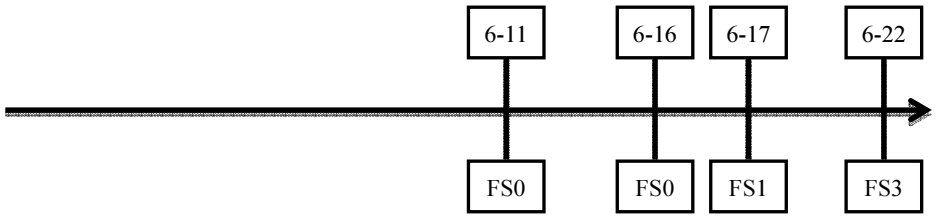

圖 8：交易事件切割點

根據上述轉換方法，對於一蒐集而得的交易歷史資料集 $TH=\{H_1,H_2,\ldots,H_n\}$，最後可獲得一精簡狀態字串集

$$CSLS(H,S)=\{CSLS(H_1,S),CSLS(H_2,S),\ldots,CSLS(H_n,S)\}$$

其中 $S\in\{FS, NS\}$，之後便可在 CSLS(H,S)進行循序樣本探勘，以建立行為樣式庫，做為後續監控與交易決策之用。

二、詐騙狀態監控與預警

根據上一節分析所得的精簡狀態字串集合，以下說明如何利用循序樣式庫來協助監控可疑的交易者。針對一可疑帳號 C_i，監控流程如下：

1. 先將 C_i 之歷史記錄 H_i 以週為單位，回溯切割 b 週後，進行狀態字串轉換，分別得到合併縮減後的詐騙循序樣式 $SLS(H_i, FS)$及一般循序樣式 $SLS(H_i, NS)$。
2. 利用字串相似度比對方法，分別對樣式庫中的樣式作比對，計算該帳號樣

式對詐騙及一般使用者的相似度。

3. 無論判斷結果為正常或有詐騙可能，使用者均可持續利用上述方法進行監控。若持續正常，則可考慮與其交易，若詐騙可能性持續增高，則應停止考慮購買 C 的商品。

有關字串相似度的計算，本研究採用 Levenshtein Distance 演算法（Levenshtein 1965），利用字串編輯距離（將一個字串轉換為另一個字串所需的最少編輯次數），來代表兩字串之間的相似程度。計算距離時之編輯操作包含「插入一個字元（Insertion）」、「刪除一個字元（Delection）」及「替換為另一個字元（Replace）」。其演算法概略步驟如下：假設要計算兩字串 a, b 的編輯距離，首先建立一個 m*n 的矩陣 M，其中 m 為 a 的字串長度+1，n 為 b 的字串長度+1。接著將此陣列 M 初始化，M[0][j], j=0,1,...m-1 的值設為 0,1,...m-1，M[i][0],i=0,1,...n-1 的值設為 0,1,...n-1。初始化完畢後，接下來可依照下述三個公式算出的最小值，設定陣列中其他的元素 M[i][j], i=1,2...n-1, j=1,2,...m-1。最後，M[n-1][m-1]即為 a, b 兩字串的編輯距離（相似度）。

M[i-1][j] +1 (Insertion)
M[i][j-1] +1 (Deletion)
M[i-1][j-1] +1 (Replace)

以下舉例說明上述的監控流程。為了簡化起見，我們只分別從詐騙及一般資料集中隨機取 100 筆資料之狀態循序樣式，以產生循序樣式庫（如表 7 與表 8 所示），並假設回溯週數 b=8。當某帳號 C_i 前八週之交易紀錄所產生的狀態樣式分別為 $SLS(H_i, FS) = \{FS1, FS0\}$, $SLS(H_i, NS) = \{NS3, NS1, NS0\}$，其樣式與樣式庫以編輯距離所計算之相似度如表 7、表 8。由表中最後一欄之加權平均相似度可知，C_i 與詐騙者樣式的加權平均相似度（0.52）高於正常者樣式之相似度（0.08）。由此分析結果，使用者可決定先不與 C_i 進行交易，靜待一段時間後，若 C_i 未成為詐騙者，且其狀態字串發生改變，再重新進行上述分析。

三、一套詐騙偵測與監控流程

綜合第參節與第肆節提出的方法，本研究提出了一套詐騙偵測與監控流程。參考圖 9，假設使用者欲與帳號 C 進行交易，但不確定其是否可信，便可依照以下流程進行偵測或監控，再決定是否與其進行交易：

1. 蒐集待測帳號 C 所屬拍賣網站的歷史交易資料，產生訓練集 TS（training set）。
2. 根據第參節提出之方法，產生以狀態變遷為基礎之詐騙偵測分類樹模型。
3. 根據第肆節的方法建立交易行為樣式庫，內含正常者與詐騙者之狀態樣式

（Fraud State Rule 與 Normal State Rule）。

4. 擷取待測帳號 C 最近 W 天（目前設定為 90 天）的交易資料，並進行以下偵測與比對：
   (1) 利用詐騙偵測模型對 C 進行偵測，並產生分類結果（Fraud 或 Normal）。
   (2) 將 C 的交易資料轉換為狀態標籤字串（SLS），再利用交易行為樣式庫進行相似度比對，並產生比對結果（Fraud 或 Normal）。
5. 使用者根據上述(1)、(2)的偵測與比對結果，決定是否與 C 進行交易。若無法決定，則持續觀察，重複步驟 4.的流程，再進行決定。

表 7：詐騙樣式庫與交易者 Ci 之相似度

編號	詐騙者狀態樣式	個數	相似度	加權相似度
1	FS1	53	0.5	26.5
2	FS1 FS0	9	1.0	9.0
3	FS1 FS2	6	0.5	3.0
4	FS1 FS3	2	0.5	1.0
5	FS1 FS0 FS3	4	0.67	2.68
6	FS0	6	0.5	3.0
7	FS1 FS0 FS2	4	0.67	2.68
8	FS1 FS0 FS1	4	0.67	2.68
9	FS0 FS2	5	0.0	0.0
10	FS0 FS2 FS0 FS2	1	0.25	0.25
11	FS2	1	0.0	0.0
12	FS0 FS3 FS2 FS3	1	0.0	0.0
13	FS2 FS0 FS2	2	0.33	0.66
14	FS0 FS3	1	0.0	0.0
15	FS1 FS0 FS1 FS0	1	0.5	0.5
平均相似度			0.41	0.52

表 8：正常者行為樣式庫與交易者 Ci 之相似度

編號	正常者狀態樣式	個數	相似度	加權相似度
1	NS1 NS3	1	0	0
2	NS3 NS1 NS3	1	0	0

3	NS3 NS2	14	0	0
4	NS1	12	0	0
5	NS3 NS2 NS0	2	0.33	0.66
6	NS1 NS2	14	0.33	4.62
7	NS3	33	0	0
8	NS3 NS1 NS0	6	0.33	1.98
9	NS3 NS1 NS0 NS2 NS0	2	0.2	0.4
10	NS3 NS1	8	0	0
11	NS1 NS3 NS1	1	0	0
12	NS1 NS3 NS1 NS0	1	0.25	0.25
13	NS3 NS2 NS0 NS2 NS0 NS2 NS0 NS2	1	0.13	0.13
14	NS1 NS2	1	0	0
15	NS3 NS1 NS2 NS0	1	0.25	0.25
16	NS3 NS2 NS0 NS2 NS0	1	0.2	0.2
平均相似度			0.12	0.08

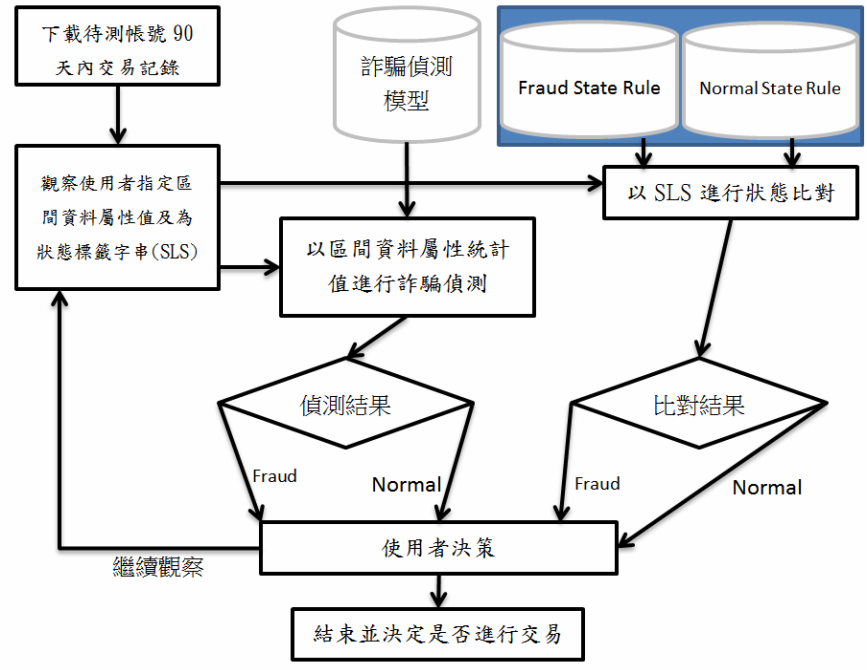

圖 9：行為監控與預警流程圖

伍、效能評估與系統實作

為驗證本研究提出方法之有效性及早期預警效果，本節將以實際拍賣網站的交易記錄進行實驗，並針對第參節所提出之詐騙偵測方法，與前人提出的方法進行比較。

一、實驗設定

本研究擷取 Yahoo!Taiwan 拍賣網站（http://tw.bid.yahoo.com）實際交易記錄進行實驗，資料集總共包含 1599 筆會員交易紀錄，其中正常者資料筆數為 1034 筆，詐騙者資料筆數為 565 筆。實驗之前，先進行詐騙資料的過濾，排除詐騙爆發期（最後一週）的資料後，並將前 90 天內無交易紀錄的詐騙者過濾掉。過濾後可用的詐騙資料筆數為 417 筆，接著根據前面章節所描述的切割方式，即可將資料筆數擴增。實驗時，為取得較客觀精確的數據，以 10 次隨機抽樣進行實驗的方式，模擬 10-fold 的交叉驗證。資料抽樣的比例根據前人研究，為提高鑑別度以 1:2 的比例做為詐騙及一般交易者資料比，並將最後測試結果取平均值。

為了評量詐騙偵測結果的優劣，本研究使用以下各種指標做為比較標準：

True Positive Rate (TP Rate) = TP/(TP+FN),

False Positive Rate (FP Rate) = FP/(FP+TN),

Precision = TP/(TP+FP),

Recall = TP/(TP+FN)　(similar to TP Rate),

Accuracy (Success Rate) = (TP+TN)/(TP+FP+FN+TN).

參考表 9 的分類矩陣（Confusion Matrix），上述指標中的 True Positive（TP）變數代表實際上是 Fraud，也被檢測為 Fraud；False Positive（FP）代表實際上是 Fraud 但被檢測為 Normal; False Negative（FN）代表實際上是 Normal 卻被誤判為 Fraud; True Normal（TN）代表實際上是 Normal 同時也被檢測為 Normal。

表 9：分類矩陣（Confusion Matrix）

預測 / 實際	Fraud	Normal
Fraud	True Positive (TP)	False Positive (FP)
Normal	False Negative (FN)	True Negative (TN)

為了驗證第參節提出之方法是否確實有助於提升詐騙偵測效能，本研究使用以下兩種方式來建立偵測模型，並進行效能比較：

1. 定點切割混階模型（Fixed-Partition hybrid Model, 簡稱 FP-Model）：此種乃

根據 Chang & Chang（2011a）的做法，在特定時間點將一個帳號的交易歷史進行切割，並回溯 m 個週期（例如以週為單位），複製產生出 m 筆資料。若訓練集中原有 n 筆交易記錄，特過定點切割，便可擴充為 m*n 筆記錄。最後再根據切割後的資料集合，建立混階偵測模型（參考貳、二節）。

2. 以狀態變遷切割為基礎之偵測模型（state transition based model，簡稱 ST-Model）：此種方式則是根據本研究提出之之狀態變遷縮減法來切割交易歷史，每個帳號之交易歷史所產生的資料筆數不一定相同。當縮減完成後，再根據縮減資料集（DSR）建立詐騙偵測模型（參考參、一節與參、二節）。

接下來，繼續說明實驗時所使用之測試資料集產生方式。考量拍賣網站保留交易歷史記錄具有一定期限，我們只擷取每位交易者最後 90 天的交易歷史做為測試資料。為了瞭解不同的偵測模型是否有助於早期預警，再將每位交易者的交易歷史紀錄以週為單位定點切割，擴增資料筆數（參考圖 10）。最後，依照所要測試的預警能力強弱，排除最後 w 週的資料。以 w=4 為例，表示此測試集合並未包含交易者（詐騙者與正常者）最後四週的交易記錄，藉此可測出偵測模型是否能找出距離爆發期四週前的詐騙者。圖中的混合測試集則由 w=0,1,2,..,8 之測試資料集所組成，以測試偵測模型之綜合預警能力。

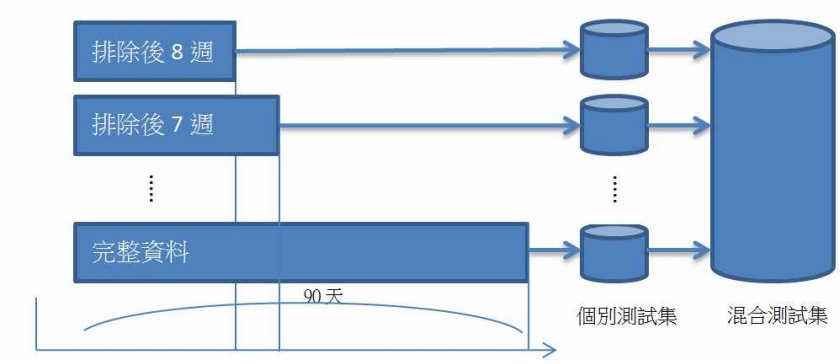

圖 10：測試集資料集合

某些詐騙者會盜取他人帳號進行詐騙，但在詐騙前會先保持交易空窗，以免引起帳號擁有者的注意。在此狀況下，在詐騙爆發前 90 天內可能沒有（或鮮少）有交易行為，因此很難找出行為變化樣式。為了考慮此狀況，在進行資料探勘前，先將在最後 90 天將交易行為稀少之帳號先行過濾。由於詐騙者進行假交易所累積的正評數量有限，為了能正確找出該類型詐騙者的行為模式，進行第二次的資料過濾，其過濾的方式是先設定正評數（Score）的下限（lower bound）及上限（upper bound），若帳號 90 天之前所累積的正評數在此界限之間就將此帳

號加入分析。此外，我們只選取正評數（Feedback Score）15～600 之間的帳號進行實驗，以避免極端的評價分數影響結果的客觀性。實驗時，依照比例隨機由資料集中抽選訓練集與測試集，進行十次實驗後再取其平均，做為最後結果。

二、詐騙偵測效能驗證

接下來，我們將比較本研究提出的狀態變遷切割方式所建立的偵測模型（state transition based model, 簡稱 ST-Model）及前人研究（Chang & Chang 2011a）所提出之定點切割混階模型（fixed-partition hybrid model, 簡稱 FP-Model）。表 9 為使用 ST-Model 與 FP-Model 分別針對以下四種測試集進行效能驗證：(1)完整交易記錄、(2)排除最後 4 週交易記錄之測試集、(3)排除最後 6 週資料之測試集、以及(4)混合測試資料集的實驗結果。實驗時，ST-Model 與 FP-Model 均使用相同的訓練集與測試集。

參考表 10(a)與 10(b)的第一列，當使用完整交易歷史做為測試集時，本研究提出方法（ST-Model）之準確率（Accuracy）高達 0.814，明顯高於前人研究（FP-Model）所獲得之 0.763。此外，無論對於詐騙者（F）還是正常者（NF），ST-Model 之綜合表現指標（F-Measure）均優於 FP-Model，顯示本研究提出之方法確能有效提升總體偵測準確率，改善詐騙偵測的品質。為了驗證不同方法對於潛伏期詐騙者的偵測能力，我們使用排除最後四週交易記錄之測試集來進行實驗，以模擬詐騙者在潛伏期（爆發前的一個月）的狀態。由表 10(a)與 10(b)中第二列的結果可看出，無論是 ST-Model 或是 FP-Model，其準確率均明顯下降，分別為 0.763 與 0.719。此結果導因於最後四週交易記錄的排除，使得詐騙者的特徵不明顯，與正常者不容易分辨。縱使如此，本研究提出的方法（ST-Model）之偵測結果仍明顯優於 FP-Model。當以詐騙者在爆發前 6 週的資料來進行測試時（見於表之第三列，排除後 6 週資料），亦可獲得與上述結果類似之觀察。為了測試偵測對於潛伏期詐騙者的綜合表現，我們最後使用混合資料集來進行實驗（參考 5-1 節的說明）。實驗結果顯示，本研究提出之方法（ST-Model）獲得 0.769 之準確率，優於前人研究（FP-Model）之 0.726。以上結果說明本研究提出之方法，對於潛伏期詐騙者，確實能提供比前人研究更準確之偵測結果。

接下來，將對本研究提出之方法（ST-Model）與 Chang & Chang（2011a）提出之 FP-Model 進行執行時間比較，執行環境如下：作業系統為 Windows 7，CPU：Intel Core i5-2410M，RAM：4G，開發語言為 Java。參考表 11 中之統計數據，建立偵測模型之前置動作「資料過濾」與「資料離散化」分別耗費 6.7 及 0.17 秒，產生四種測試集的時間則分別為 0.04, 0.01, 0.01 與 0.04 秒。以上為 ST-Model 與 FP-Model 共同所需的執行步驟，因此時間均相同。接下來比較 ST-

Model 與 FP-Model 在建立偵測模型與測試時之時間：

1. 建立偵測模型：此步驟 ST-Model 與 FP-Model 之執行時間分別為 3.81 秒與 0.95 秒。此差距應導因於 ST-Model 除交易紀錄切割外，還需進行後續的複製與狀態縮減（參考圖 4 與圖 7 的演算法）。此乃為產生更準確的偵測模型所付出的成本，以等待時間而言，3.81 秒並非無法容忍，且偵測模型一旦建立，便可持續使用，無需重複產生。
2. 測試：在測試時，四種不同測試集的執行時間，除排除後 6 週資料之測試集外，FP-Model 的執行時間均較 ST-Model 為少，但最大時間差異僅 0.07 秒（排除後 6 週資料）。以如此些微的時間差異，換取 4%~5%準確率之提升，對詐騙偵測而言應屬合理。

表 10：ST-Model 及 FP-Model 對不同測試集的十次平均偵測結果

使用交易資料：爆發前 90 天資料, 累積正評數：15 – 600 的帳號
資料筆數：Training Set(Fraud: Normal = 200:400), Test Set(Fraud : Normal = 200: 400)

(a) ST-Model：本研究提出之以狀態變遷為基礎切割塑模

排除 n 週/統計值	Accuracy	TP Rate	FP Rate	Precision	Recall	F-measure	Class
完整資料	0.814	0.703	0.133	0.728	0.708	0.718	F
		0.868	0.298	0.856	0.868	0.862	NF
排除後 4 週資料	0.763	0.670	0.191	0.637	0.670	0.653	F
		0.809	0.330	0.831	0.809	0.820	NF
排除後 6 週資料	0.748	0.667	0.211	0.612	0.667	0.638	F
		0.789	0.333	0.826	0.789	0.807	NF
混合測試集	0.769	0.694	0.194	0.642	0.694	0.667	F
		0.807	0.307	0.840	0.807	0.823	NF

(b) FP-Model：以定點切割（週為單位）混合塑模（Chang & Chang, 2011a）

排除 n 週/統計值	Accuracy	TP Rate	FP Rate	Precision	Recall	F-measure	Class
完整資料	0.763	0.648	0.179	0.644	0.648	0.646	F
		0.821	0.352	0.823	0.821	0.822	NF
排除後 4 週資料	0.719	0.571	0.207	0.580	0.571	0.576	F
		0.793	0.429	0.787	0.793	0.790	NF
排除後 6 週資料	0.717	0.569	0.209	0.576	0.569	0.578	F
		0.791	0.431	0.786	0.791	0.788	NF

混合測試集	0.726	0.611	0.216	0.586	0.611	0.598	F
		0.784	0.389	0.801	0.784	0.793	NF

表 11：本研究提出之 ST-Model 與 FP-Model（Chang & Chang 2011a）執行時間比較

（單位：秒）

執行時間（秒） 測試資料類型	資料過濾	離散化（分群）	建立偵測模型 (ST-Model[a]/FP-Model[b])	產生測試集	測試 (ST-Model[a]/FP-Model[b])
完整資料	6.7	0.17	3.81/0.95	0.04	0.06/0.02
排除後 4 週資料				0.01	0.01/0.01
排除後 6 週資料				0.01	0.09/0.02
混合測試集				0.04	0.08/0.03

[a] 本研究提出之方法 [b]Chang & Chang（2011a）提出之方法

除了執行時間之外，為清楚呈現與前人研究之偵測效能差異，以下以分類矩陣來進行說明。參考表 12(a)，其中的數據為使用本研究提出方法（ST-Model）所獲得之平均結果（使用完整資料集），在 200 個詐騙測試帳號中，共有 141 個被正確檢出，精度（precision）為 73%；而對於 400 個正常者測試帳號，則有 347 個被正確檢出，精度為 85%。反觀 Chang 與 Chang（2011a）的方法（參考表 12(b)），其詐騙者之偵測精度僅有 64%，正常者之精度則為 82%。很明顯地，本研究提出方法之詐騙偵測精度（73%），大幅優於前人研究（64%）。此外，本研究（ST-Model）之平均誤判率為18.6%(=(53+59)/600)，亦優於前人研究（FP-Model）之23.6%(=(72+70)/600)。當使用混合測試資料集時（參考表 13），由於許多帳號之交易歷史末期的記錄刻意被刪除，以模擬潛伏期的詐騙者的行為，因此詐騙偵測的精度（precision）明顯下降（因為詐騙者之異常特徵減少）。但本研究提出之 ST-Model 仍有 64%之精度，FP-Model 則僅有 59%。根據上述討論，進一步驗證本研究提出之方法無論在「詐騙者」或「正常者」的偵測上，均一致優於 FP-Model。

表 12：使用分類矩陣說明本研究提出方法與前人研究之效能差異（使用完整資料集）

ST-Model：使用完整資料集（本研究提出）				FP-Model：使用完整資料集合（Chang & Chang, 2011a）			
實際 / 預測	Fraud	Normal	precision	實際 / 預測	Fraud	Normal	precision
Fraud	141	53	73%	Fraud	130	72	64%
Normal	59	347	85%	Normal	70	328	82%
帳號個數	200	400	600	帳號個數	200	400	600

表 13：使用分類矩陣說明本研究提出方法與前人研究之效能差異（使用混合資料集）

ST-Model：使用混合資料集（本研究提出）				FP-Model：使用混合資料集合（Chang & Chang, 2011a）			
實際 / 預測	Fraud	Normal	precision	實際 / 預測	Fraud	Normal	precision
Fraud	139	77	64%	Fraud	122	86	59%
Normal	61	323	84%	Normal	78	314	80%
帳號個數	200	400	600	帳號個數	200	400	600

三、詐騙偵測與監控系統

本研究依照上述的詐騙行為之時序分析方法，本研究使用 Java 語言發展一套詐騙偵測與監控系統，並將系統嵌入 DJ Project API 中的 Java-based Web Browser（DJ Project 2014）中，讓使用者在瀏覽網頁時便可進行詐騙偵測（目前檢測對象僅限台灣 Yahoo 拍賣的帳號）。圖 11 與圖 12 為系統操作介面，使用者可直接輸入帳號，或點選取本機端資料庫中已分類資料，系統會自動進行詐騙偵測，並顯示 8 週內詐騙偵測的結果、帳號狀態改變的趨勢及其相似度，提供給使用者作交易前的決策支援。

本系統介面左邊為本機端的帳號列表，系統啟動時會自動將存於本機端的資料載入到此列表中。右邊可分上下兩個區塊，上面的介面為交易歷史紀錄瀏覽視窗，讓使用者瀏覽帳號完整或解析過的交易歷史紀錄。系統目前是透過本機端已存的資料進行詐騙偵測，一旦使用者按下載入的按鈕，系統會開始搜尋本機端資料庫內是否有符合輸入的帳號，並顯示該帳號之歷史交易紀錄。使用者也可按下更新的按鈕，將該帳號的資料重新上網下載。假如該帳號不存在於本機端資料，系統會自動連上 Yahoo 拍賣網站查詢此帳號是否存在，並提示使用者是否進行歷史交易紀錄的下載。下方的介面則是提供資料分析後的結果，主要有兩個頁面：

1. 詐騙偵測會將帳號八週內的偵測結果顯示在下方。
2. 狀態監控則是顯示帳號八週內詐騙及一般狀態改變的趨勢，以及相似度計算的結果。

圖 11：系統操作介面－詐騙偵測

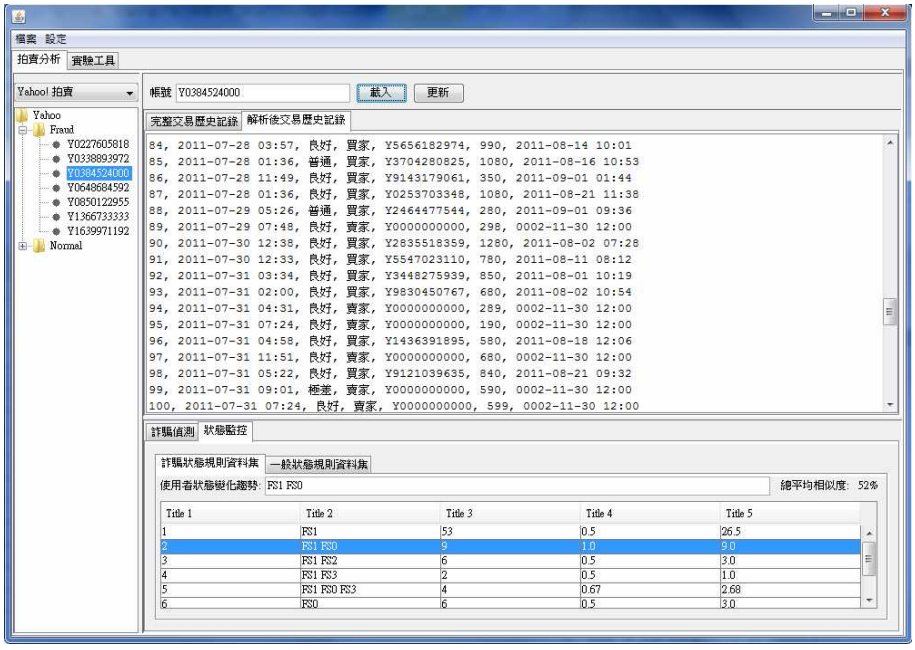

圖 12：系統操作介面－狀態監控

四、研究限制

根據上述實驗結果，本論文提出之方法，對於潛伏期的詐騙者能提供較佳之偵測與監控效果。然而，這些方法與結果在實際應用時，有以下限制：

1. 本研究假設詐騙者在潛伏期會產生與正常交易者不同的行為樣式，並據以發展偵測與監控方法。這樣的假設不適用於剛盜取、借用或購買他人帳號的詐騙者，亦不適用於臨時起意的詐騙者。因為他們在開始詐騙前的表現，與一般正常者無異，無法使用本研究提出之方法來偵測。
2. 本研究假設線上拍賣交易者的行為可用交易金額、交易次數與評價百分比等量化數據來表示。但在實務上，每次交易完成後，雙方除了互給評價分數外，也會留下文字評語。若能仔細分析這些文字評語（Pavlou & Dimoka 2006），亦可獲得隱含的寶貴資訊，進一步判別服務品質的真實性。然而，這需牽涉複雜的文字探勘，已超越本論文的研究範圍。
3. 本研究將詐騙者與正常者分為多種類型，以增加偵測模型的解析度，並用以改善準確率。事實上，若要積極應用此特點，在完成偵測後，需有進一步的配套措施（例如，根據不同類型詐騙者，給予不同處置）。由於本研究未將後續配套措施設定為研究目標，因此，在統計實驗數據時，仍只將結果歸總為正常（Non-Fraud）與詐騙（Fraud）等二大類。

陸、結論

隨著線上拍賣使用人數不斷增加，線上拍賣業者的收益也逐年提升，但業者的管理方式卻讓消費者需承擔更多的風險。二元名聲系統有太多漏洞，讓不懷好意的有心人士能趁虛而入，進行詐騙。管理者雖能在詐騙爆發後，將該帳號進行停權，但傷害已經造成。因此，為提升網路拍賣交易安全性，本研究已發展一套線上拍賣詐騙行為之時序分析方法，並實作一套線上拍賣交易輔助系統，協助使用者挑選交易對象。本研究提出之方法以交易事件為切割點，觀察其狀態變化趨勢，進而判斷詐騙與正常交易者之差異。而後，針對資料集中所有的交易歷史進行狀態變遷切割，以產生與時序行為相關之分類樹偵測模型。此外，我們也利用狀態切割後的資料集，製作狀態標籤字串，並產生循序樣本庫，供使用者比對、監控可疑帳號。實驗結果顯示，觀察使交易者狀態改變之顯著事件，確實有助於詐騙偵測之早期預警。與前人研究相較（Chang & Chang 2011a），本研究能在合理時間成本內，獲得更佳的偵測準確率。

綜觀前述介紹，本論文之整體研究成果如下：

1. 線上拍賣是電子商務重要的成功典範之一，但詐騙卻嚴重影響其發展，讓正常的消費者卻步。透過早期發現詐騙者，才能消除疑慮，讓總體營收再

創高峰。但詐騙偵測的早期預警並非易事，詐騙者在爆發期前的行為幾乎與正常者無異，交易者縱使小心審視，也不易發現。因此，透過本研究發展之方法，將可協助交易者早期辨識具有風險性的交易對象。

2. 為辨識潛伏期詐騙者，前人研究（Chang & Chang 2009; 2010; 2011）曾試圖在交易歷史中找出蛛絲馬跡，並以定點方式切割交易歷史，再進行塑模。此類型方法對於詐騙之早期偵測具有一定效果，但卻無法兼顧各種不同的詐騙行為模式。舉例而言，並非所有詐騙者均在生命週期 80%後才開始進行詐騙；此外，前人研究以 5%為增量來切割交易歷史，也無法兼顧行為變化的細節。為此，本研究以交易者狀態變遷為基礎，嘗試消除無益於偵測效能之樣本，產生更具參考價值的早期預警資訊。透過更合理的資料分割方式，將每位詐騙者的潛伏樣式以更精確方式呈現在偵測模型中。在實務上，確準的早期預警正是讓詐騙者消聲匿跡的關鍵，也是線上拍賣網站最有價值的監測資訊之一。
3. 詐騙偵測是異常偵測的一種，所發展之方法應可用來解決其他類似問題。例如，由於網路基礎建設的成熟，讓電子商務再度蓬勃發展。然而，虛擬商場中良莠不齊的狀況相當嚴重。許多不誠實賣家遊走於法律邊緣，販賣不良品與仿冒品，讓消費者蒙受重大損失。對於上述問題，便可將本研究提出的方法用於不誠實商家的偵測，分析網路商店的交易歷史，早期發現具有不誠實傾向之賣方。又如，健保給付一直是政府與國民的重大負擔，除了醫療浪費外，更有不肖醫療院所假借人頭（或進行無必要性之醫療）來套取健保給付。對於這些不誠實的醫院，便可運用本研究提出之方法，仔細分析其給付申請歷史，配合過往案例的分析，早期發現其是否有詐欺嫌疑。果真如此，相關單位便可適時提出警告，除可省去後續的追討行為，更可讓醫療資源及時應用在需要的案例上。此外，信用卡詐欺一直是銀行重要的監管項目，相關偵測方法亦已發展多年。然而，若能應用本研究提出之方法，隨時監測所有帳戶的消費歷史，便可早期發現詐欺嫌疑者。透過監控與提醒，避免案件的發生，對於後續的法務問題，更可收事半功倍之效。

在後續發展上，可考慮加強偵測指標的多樣性，將詐騙嫌疑人可能參與之社群網路納入考量，進行特徵分析。在王俊程等（2005）的研究中，曾將交易網路特徵納入偵測屬性，以獲得更精確的偵測資訊。Pandit 等（2007）亦曾利用交易網路進行二階段偵測，以掌握共犯結構。因此，若能檢視嫌疑人所參與之社群網路活動，應可獲得更進一步的資訊，擷取出不同的行為特徵（甚至找出共犯結構）。其次，在大數據時代中，亦可考慮進行更精細的資料蒐集方式。逐次、逐日擷取整個交易網站的活動，以獲得解析度更高的交易細節。龐大的資料集雖然

不利於資料過濾與屬性設計，但對於行為特徵的擷取，卻可提供更考靠的分析依據。若能解決龐大資料量帶來的負面影響，相信必可發展出準確度更高的詐騙偵測方法。最後，在系統實作上應該考慮以 APP 方式來呈現。事實上，任何有助於決策的軟體，均可考慮製作成 APP，以拓展其使用族群，讓廣大消費者實際受惠。為增加實用性，亦可考慮將發展之方法實作為外掛程式，安裝在用戶端的瀏覽器中。當使用者瀏覽拍賣網頁時，便可提供即時監控，並在必要時提出警告。同樣地，若線上拍賣業者願採用本研究提出之方法，監控會員在網站上的日常交易活動，便可早期發覺可疑交易，甚至進行預防性停權，以避免交易糾紛的產生。相較於被動式的停權（等受害者申訴），及時監控顯然具有積極的正面意義，能進一步維護拍賣平台的交易安全。

參考文獻

王俊程、邱垂鎮、葛煥元（2005），『以交易記錄的社會網絡結構建立線上拍賣哄抬評價的偵測指標』，*資訊管理學報*，12 卷 4 期，頁 143-184。

Agrawal, R. and Srikant, R. (1995), 'Mining Sequential Patterns.', *Proceedings of International Conference on Data Engineering*, Taipei, Taiwan, March 6-10,pp.3-14.

Agrawal, R. and Srikant, R. (1996). 'Mining Sequential Patterns: Generalizations and Performance improvements', *Proceedings of the 5th Int. Conf. Extending Database Technology*, EDBT, London, UK, March 25 - 29, Vol. 1057, pp. 3-17.

Brown, D.E., and Oxford, R.B. (2001), 'Data Mining Time Series with Applications to Crime Analysis', *Proceeding of the 2001 IEEE conference*, Tucson, Arizona, USA., Oct.7-10, Vol. 3, pp. 1453-1458.

Chandola, V., Banerjee, A. and Kumar, V. (2009), 'Anomaly Detection: A Survey', *ACM Computing Surveys*, Vol. 41(3), Article 15.

Chang, J.S. and Chang, W.H. (2009), 'An Early Fraud Detection Mechanism for Online Auctions Based on Phased Modeling', *Proceeding the 2009 International Workshop on Mobile Systems E-commerce and Agent Technology* (MSEAT 2009), Taipei, Taiwan, December 3-5, pp. 743-748.

Chang, J.S. and Wong, H.J. (2011b), 'Selecting appropriate sellers in online auctions through a multi-attribute reputation calculation method', *Electronic Commerce Research and Applications*, Vol. 10, No. 2, pp. 144-154.

Chang, W. and Chang, J. (2011a), 'A Novel Two-Stage Phased Modeling Framework for Early Fraud Detection in Online Auctions', *Expert System with Applications*,

Vol. 38, No.9 , pp. 11244-11260.

Chang, W.H. and Chang, J.S. (2010a), 'A Multiple-Phased Modeling Method to Identify Potential Fraudsters in Online Auctions', *Proceedings of the 2nd International Conference on Computer Research and Development* (ICCRD 2010), Kuala Lumpur, Malaysia., May 7-10, pp. 186-190.

Chang, W.H. and Chang, J.S. (2010b), 'An Online Auction Fraud Screening Mechanism for Choosing Trading Partners', *Proceeding of 2010 the 2nd International Conference on Education Technology and Computer* (ICIEE 2010), Shanghai, China, June 22-24, Vol. 5, pp. V5-56.

Chang, W.H. and Chang, J.S. (2012), 'An Effective Early Fraud Detection Method for Online Auctions', *Electronic Commerce Research and Applications*, Vol. 11, No. 4, 2012, pp. 346-360.

Chau, D., Pandit, S., Faloutsos, C. (2006), 'Detecting Fraudulent Personalities in Networks of Online Auctioneers', *Proceedings of the 10th European conference on Principle and Practice of Knowledge Discovery in Databases,* Berlin, Germany, September 18-22, pp. 103-114.

Chau, D.H. and Faloutsos, C. (2005), 'Fraud Detection in Electronic Auction', *Proceedings of European Web Mining Forum (EWMF 2005) at ECML/PKDD 2005*, Porto, Portugal, October 3-7, pp. 87-97.

Chua, C.E. and Wareham, J. (2004), 'Fighting Internet Auction Fraud: An Assessment and Proposal', *Computer*, Vol. 37, No. 10 , pp. 31-37.

DJ Project (2014), 'Java Web Browser', available at http://djproject.sourceforge.net/ns/ (accessed 1 May 2014).

eBay Inc. (1995), 'How Feedback works' , available at http://pages.ebay.com/help/feedback/howitworks.html (accessed 30 December 2016).

eBay Inc. (2013), '2013 Quarterly Report ', available at http://investor.ebay.com/annuals.cfm (accessed 1 December 2013).

Fawcett, T. and Provost, F. (1999), 'Activity monitoring: noticing interesting changes in behavior', *Proceedings of the 5th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, ACM Press, San Diego, California, USA, August 15-18, pp. 53-62.

Gavish, B. and Tucci, C. (2008), 'Reducing Internet Auction Fraud', *Communications of the ACM*, Vol. 51, No. 5 , pp. 89-97.

Goes, P., Tu, Y. and Tung, A. (2009), 'Online Auctions Hidden Metrics', *Communications of the ACM*, Vol. 52, No.4 , pp. 147-149.

Ishioka, T. (2005), 'An expansion of x-means for automatically determining the optimal number of clusters-progressive iterations of k-means and merging of the clusters', *Proceedings of fourth IASTED international conference computational intelleigence*, Calgery, Alberta, Canada, July 4-6, pp. 91-96.

Kaszuba, T., Hupa, A. and Wierzbicki, A. (2010), 'Advanced Feedback Management for Internet Auction Reputation Systems', *IEEE Internet Computing*, Vol. 14, No. 5 , pp. 31-37.

Kobayashi, M. and Ito, T. (2007), 'A transactional relationship visualization system in internet auctions', *IEEE Computer Society* , pp. 248-251.

Kobayashi, M. and Ito, T. (2008), 'A Transactional Relationship Visualization System in Internet Auctions', *Electronic Commerce - Studies in Computational Intelligence*, Vol. 110, pp. 87-99.

Levenshtein, V.I. (1965), 'Binary codes capable of correcting deletions, insertions, and reversals', *Soviet Physics Dokl*. Vol.10, pp.707-710.

National White Collar Crime Center (NW3C) (2011), '2010 Internet Crime Report', *Internet Crime Complaint Center*, available at http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf (accessed 1 May 2014)

National White Collar Crime Center(NW3C) (2009) , '2008 Internet Crime Report', available at http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf (accessed 1 May 2014)

National White Collar Crime Center(NW3C) (2012), '2011 Internet Crime Report', *Internet Crime Complaint Center*, available at http://www.ic3.gov/media/annualreport/2011_IC3Report.pdf (accessed 1 May 2014)

Pandit, S., Chau, D., Wang, S. and Faloutsos, C. (2007), 'Netprobe: a fast and scalable system for fraud detection in online auction networks', *Proceedings of the 16th international conference on World Wide Web,* Banff, Alberta, Canada, May 8-12, pp. 201-210.

Pavlou, P. and Dimoka, A. (2006), 'The nature and role of feedback text comments in online marketplaces: implications for trust building, price premiums, and seller differentiation', *Information Systems Research*, Vol. 17, No. 4, pp. 392-414.

Pei, J., et al. (2001), 'PrefixSpan: Mining sequential patterns efficiently by prefix-projected pattern growth', *Proceedings of Int. Conf. Data Engineering (ICDE '01)*, Heidelberg, Germany, April 2-6, pp.215-224.

Pei, J., Han, J. and Wang, W. (2002), 'Mining Sequential Patterns with Constraints in Large Databases', *Proceedings of the eleventh international conference on*

Information and knowledge management, McLean, Virginia, USA, Nov. 4-9, pp. 18-25.

Pelleg, D. and Moore, A. (2000), 'X-means: Extending K-means with Efficient Estimation of the Number of Clusters', *Proceedings of the 17th International Conference on Machine Learning*, San Francisco, CA, USA, June 29-July 2,pp. 727-734.

Quinlan, J.R. (1986), 'Induction of Decision Trees', *Machine Learning*, Vol. 1, No. 1,pp. 81-106.

Quinlan, J.R. (1993), *C4.5 Programs for machine learning*, Morgan Kaufmann, San Francisco, CA, USA.

Schmidt, S., Steele, R., Dillon, T. and Chang, E. (2007), 'Fuzzy trust evaluation and credibility development in multi-agent systems', *Applied Soft Computing*, Vol. 7, No. 2,pp. 492-505.

Selvaraj, C. and Anand S. (2012) 'A Survey on Security Issues of reputation Management Systems for Peer-to-Peer Networks', *Computer Science Review*, Vol. 6,pp. 145-160.

Sherchan, Wanita, Nepal, Surya, and Paris, C. (2013), 'A Survey of Trust in Social Networks', *ACM Computing Survey*, Vol. 45, No. 4, Article 47.

Tavakolifard, M. and Almeroth, K.C. (2012), 'Social Computing: An Intersection of recommender Systems, Trust/Reputation Systems, and Social Network', *IEEE Network*, Vol. 26, No. 4, pp. 53-58.

Wang, J. and Chiu, C. (2005), 'Detecting Online Auction Inflated-Reputation Behaviors using Social Network Analysis', *Proceedings of NAACSOS Conference*, Indiana, USA, June 26-28, pp. 26-28.

Weka (2014),'Weka 3 - Data Mining with Open Source Machine Learning Software in Java', available at http://www.cs.waikato.ac.nz/ml/weka (accessed 1 May 2014).

Witten, I. and Frank, E. (2005), *Data mining: practical machine learning tools and techniques*, Mogan Kaufmann, San Francisco, CA, USA.

Yu, L. and Liu, H. (2004), 'Efficient Feature Selection via Analysis of Relevance and Redundancy', *Journal of Machine Learning Research*, Vol.5 , pp. 1205-1224.

Zhang, B., Zhou, Y. and Faloutsos, C. (2008), 'Toward a comprehensive model in Internet auction fraud detection', *Proceedings of the 41st Annual Hawaii International Conference on System Science*, Waikoloa, USA, Jan 7-10, pp. 1-9.