

**SUSPICIOUS EVENT ANALYSIS DEVICE AND RELATED COMPUTER
PROGRAM PRODUCT FOR GENERATING SUSPICIOUS EVENT SEQUENCE
DIAGRAM**

BACKGROUND

[0001] 本發明涉及駭客入侵活動檢測技術，尤指一種用於產生可疑事件時序圖的可疑事件研判裝置與相關的電腦程式產品。

[0002] 隨著各種網路應用越來越普及，駭客入侵事件在各地層出不窮。電腦中安裝的一般防毒軟體能夠偵測並阻擋常見的電腦病毒，但通常難以有效防範或偵測出駭客的入侵行為。例如，近年日益盛行的一種駭客攻擊手段，稱為「進階持續性滲透威脅」（Advanced Persistent Threat，APT），會針對特定企業或組織所做持續、進階且全方位的攻擊。這種駭客攻擊方式通常是由特定國家或組織所贊助的針對性攻擊行動，主要目的是竊取特定情資、加密虛擬貨幣（Cryptocurrency）、或特定人士的個人隱私等等，但一般的資安防護軟體很難發現這類的駭客攻擊行為。

[0003] 由於駭客攻擊手段非常多樣，當前的技術尚無法單純依賴電腦程式做出精確判斷。實務上，要檢測特定環境是否已遭受前述的進階持續性滲透威脅或其他類型的駭客手段攻擊，需要依賴有經驗的專業資安分析人員，收集受檢環境中大量的電腦活動歷史紀錄並進行判讀、比對，才能做出判斷。然而，前述的檢測方式高度仰賴資安分析人員的實務經驗，而且電腦活動歷史紀錄中存在大量的雜訊資料需要過濾，所以整個判斷過程非常耗費人力與時間，通常需要好幾個工作天才能做出初步判斷。

SUMMARY

[0004] 有鑑於此，如何提升檢測特定環境是否已遭受駭客攻擊的判斷效率與精確度，實為有待解決的問題。

[0005] 本說明書提供一種用於診斷一標的網路系統是否已受到駭客入侵的可疑事件研判裝置的實施例，其包含：一顯示裝置；一通信電路，設置成透過網際網路接收與該標的網路系統中的多個運算裝置有關的多個可疑活動記錄、以及相應的多個時間戳記與多個屬性標籤；一儲存電路，設置成儲存一可疑事件時序圖產生程式；以及一控制電路，耦接於該顯示裝置、該通信電路、與該儲存電路，並設置成執行該可疑事件時序圖產生程式，以依據該多個可疑活動記錄、該多個時間戳記、與該多個屬性標籤

進行一可疑事件時序圖產生運作，以界定出與該標的網路系統有關的多個可疑事件，界定出分別對應於該多個可疑事件的多個時間記錄，以及依據該多個可疑事件與該多個時間記錄，產生並顯示與該多個可疑事件相應的一可疑事件時序圖。

[0006] 本說明書提供另提供一種電腦程式產品的實施例。該電腦程式產品，儲存在一可疑事件研判裝置的一儲存電路中，允許該可疑事件研判裝置進行一可疑事件時序圖產生運作，該可疑事件時序圖產生運作包含：依據與一標的網路系統中的多個運算裝置有關的多個可疑活動記錄、以及相應的多個時間戳記與多個屬性標籤，界定出與該標的網路系統有關的多個可疑事件；界定出分別對應於該多個可疑事件的多個時間記錄；以及依據該多個可疑事件與該多個時間記錄，產生並顯示與該多個可疑事件相應的一可疑事件時序圖。

[0007] Both the foregoing general description and the following detailed description are examples and explanatory only, and are not restrictive of the invention as claimed.

BRIEF DESCRIPTION OF THE DRAWINGS

[0008] 圖1為本發明一實施例的網路安全漏洞診斷系統簡化後的功能方塊圖。

[0009] 圖2為圖1中的個別運算裝置內的裝置活動回報程式的一實施例簡化後的功能模塊示意圖。

[0010] 圖3為圖1中的可疑事件研判裝置內的可疑事件時序圖產生程式的一實施例簡化後的功能模塊示意圖。

[0011] 圖4為本發明一實施例的診斷標的網路系統是否已受到駭客入侵的方法簡化後的流程圖。

[0012] 圖5為圖1中的顯示裝置所顯示的影像畫面的一實施例簡化後的示意圖。

[0013] 圖6為本發明一實施例的產生可疑事件時序圖的方法簡化後的流程圖。

[0014] 圖7至圖9為本發明不同實施例的可疑事件時序圖的局部內容簡化後的示意圖。

[0015] 圖10為本發明產生可疑事件時序圖中的推論關係線的方法的一實施例簡化後的流程圖。

[0016] 圖11至圖12為本發明不同實施例的可疑事件時序圖的局部內容簡化後的示意圖。

[0017] 圖13為本發明另一實施例的網路安全漏洞診斷系統簡化後的功能方塊圖。

DETAILED DESCRIPTION

[0018] 以下將配合相關圖式來說明本發明的實施例。在圖式中，相同的標號表示相同或類似的元件或方法流程。

[0019] 圖1為本發明一實施例的網路安全漏洞診斷系統100簡化後的功能方塊圖。網路安全漏洞診斷系統100用於診斷一標的網路系統102是否已受到駭客入侵。如圖1所示，標的網路系統102中包含有多個運算裝置（例如，圖1中的示例性運算裝置111~115）。請注意，圖1中所繪示的運算裝置的數量，只是為了舉例說明，並非有意將標的網路系統102中的運算裝置數量侷限在特定數目。

[0020] 在說明書及申請專利範圍中所指稱的「運算裝置」一詞，指的是各種能執行特定作業系統（例如：Windows、Linux、macOS、Android、Chrome OS、HarmonyOS等等）進行運作、並支援合適的資料通信協定的電子設備，例如，桌上型電腦、筆記型電腦、平板電腦、伺服器、網路儲存裝置（Network Attached Storage，NAS）、智慧電視、智慧手機、或智慧音箱等等。前述的資料通信協定則可以是各種有線資料傳輸協定或無線資料傳輸協定，例如，TCP/IP通信協定、UDP（User Datagram Protocol）通信協定、USB（Universal Serial Bus）通信協定、IEEE 802.11系列通信協定、藍牙系列通信協定等等。

[0021] 在實際應用中，標的網路系統102可以是各種規模的企業、學校、研究機構、或組織的內部網路系統，所以標的網路系統102中的運算裝置的數量，從個位數、數十台、數百台、甚至超過千台以上都有可能。另外，標的網路系統102中的多個運算裝置，有可能都位於同一個地理區域，也有可能是分散在不同的地理區域（例如，不同的城市或國家）。

[0022] 標的網路系統102中的每個運算裝置可以透過適當的資料傳輸機制（例如，標的網路系統102的內部網路或資料傳輸線），與其他的一或多個運算裝置直接或間接進行各種資料通信。在運作時，標的網路系統102中可有一部分的運算裝置採用有線資料傳輸方式來進行資料通信，並有一部分的運算裝置採用無線資料傳輸方式來進行資料通信。換言之，不同的運算裝置所採用的資料傳輸方式可以有所不同。

[0023] 在圖1的實施例中，網路安全漏洞診斷系統100包含有多個裝置活動回報程式120、一活動記錄匯集裝置130、以及一可疑事件研判裝置140。

[0024] 網路安全漏洞診斷系統100中的多個裝置活動回報程式120，分別儲存並安裝

在標的網路系統102的前述多個運算裝置111~115中，用於產生與多個運算裝置111~115有關的多個可疑活動記錄（suspicious activities records）與多個時間戳記（time stamps），以及建立分別對應於多個可疑活動記錄的多個屬性標籤（attribute tags）。

[0025] 活動記錄匯集裝置130包含一通信電路131、一處理電路133、以及一儲存電路135。通信電路131耦接於標的網路系統102，並設置成透過適當的網路連線（例如，標的網路系統102的內部網路或網際網路）與前述的多個運算裝置111~115進行資料通信，以接收前述多個裝置活動回報程式120所產生的多個可疑活動記錄、以及相應的多個時間戳記與多個屬性標籤。處理電路133耦接於通信電路131，設置成控制通信電路131的運作，並對接收到的多個可疑活動記錄、多個時間戳記、與多個屬性標籤進行處理，以產生一回傳資料（return data）。處理電路133還會利用通信電路131將回傳資料透過合適的網路（例如，網際網路）傳送給可疑事件研判裝置140。儲存電路135耦接於處理電路133，並設置成儲存活動記錄匯集裝置130運作所需的資料或檔案。

[0026] 在實際應用中，前述的活動記錄匯集裝置130可以安裝在標的網路系統102所屬單位的內部，也可以安裝在標的網路系統102所屬單位以外的其他位置。

[0027] 如圖1所示，可疑事件研判裝置140包含一顯示裝置141、一通信電路143、一輸入裝置145、一儲存電路147、以及一控制電路149。顯示裝置141用於顯示各種資料與影像。通信電路143設置成透過合適的網路（例如，網際網路）接收前述的回傳資料。輸入裝置145設置成允許可疑事件研判裝置140的使用者（例如，資安分析人員）對可疑事件研判裝置140進行各種操作，例如，輸入指令、修改相關分析參數、調整相關的資料比對標準、或是調整顯示裝置141中的影像尺寸、影像位置、與影像內容等等。儲存電路147設置成儲存一可疑事件時序圖產生程式150。控制電路149耦接於顯示裝置141、通信電路143、輸入裝置145、與儲存電路147，並設置成從通信電路143所接收到的回傳資料中，擷取出與標的網路系統102中的多個運算裝置111~115有關的多個可疑活動記錄、以及相應的多個時間戳記與多個屬性標籤。控制電路149還設置成執行可疑事件時序圖產生程式150，以依據前述的多個可疑活動記錄、多個時間戳記、與多個屬性標籤進行一可疑事件時序圖產生運作（suspicious event sequence diagram generating operation）。在可疑事件時序圖產生運作中，控制電路149會界定出與標的網路系統102有關的多個可疑事件（suspicious events）、界定出分別對應於多個可疑事件的多個時間記錄（time records）、以及依據多個可疑事件與多個時間記錄產生與多個可疑事件相應的一可疑事件時序圖（suspicious event sequence diagram）。另一方面，控制電

路149也會利用顯示裝置141來顯示所產生的可疑事件時序圖。

[0028] 另外，圖1中的示例性惡意檔案提供裝置160，代表駭客在入侵標的網路系統102的過程中可能會使用到的釣魚網站、殭屍電腦、散播惡意程式碼的網站伺服器、或是其他扮演類似角色的各種裝置實體（device entity）的其中之一。在實際的駭客入侵行動中，駭客有可能透過更多數量的惡意檔案提供裝置來試圖攻擊標的網路系統102。

[0029] 實作上，前述的通信電路131與143皆可用各種有線傳輸電路、無線傳輸電路、或是同時整合前述兩種通信機制的混合電路來實現。處理電路133可以用一或多個處理器單元來實現。儲存電路135與147可用各種非揮發性儲存裝置來實現。顯示裝置141可用能夠呈現影像的各種螢幕或投影裝置來實現。輸入裝置145可用鍵盤、滑鼠、遙控器、觸控螢幕、觸控板、按鈕、聲控輸入裝置、手勢感應裝置、採用其他各種指令產生技術的電路、或前述裝置的組合來實現。控制電路149可用單一處理器模塊、多個處理器模塊的組合、電腦系統、伺服器、或雲端系統來實現。另外，前述的顯示裝置141和輸入裝置145也可以共同整合成單一觸控螢幕或多個觸控螢幕的組合。

[0030] 前述儲存在標的網路系統102的不同運算裝置中的裝置活動回報程式120，皆可用一個或多個功能模塊組成的電腦程式產品來實現。例如，圖2為圖1中的個別運算裝置內的裝置活動回報程式120的一實施例簡化後的功能模塊示意圖。在圖2的實施例中，裝置活動回報程式120包含一偵測模塊210、一屬性判斷模塊220、以及一傳送模塊230。

[0031] 另外，前述儲存在可疑事件研判裝置140的儲存電路147中的可疑事件時序圖產生程式150，同樣可用一個或多個功能模塊組成的電腦程式產品來實現。例如，圖3為圖1中的可疑事件研判裝置140內的可疑事件時序圖產生程式150的一實施例簡化後的功能模塊示意圖。在圖3的實施例中，可疑事件時序圖產生程式150包含一事件分析模塊310、一視覺物件產生模塊320、一排列模塊330、以及一信息標註模塊340。

[0032] 以下將搭配圖4來進一步說明網路安全漏洞診斷系統100的運作方式。圖4為本發明一實施例的診斷標的網路系統102是否已受到駭客入侵的方法簡化後的流程圖。

[0033] 在圖4的流程圖中，位於一特定裝置所屬欄位中的流程，即代表由該特定裝置所進行的流程。例如，標記在「運算裝置」欄位中的部分，是由標的網路系統102中的個別運算裝置111~115所進行的流程；標記在「活動記錄匯集裝置」欄位中的部分，是由活動記錄匯集裝置130所進行的流程；而標記在「可疑事件研判裝置」欄位中的部分，則是由可疑事件研判裝置140所進行的流程。

[0034] 在前述標的網路系統102的日常運作過程中，個別運算裝置會執行所安裝的裝置活動回報程式120，以進行圖4中的流程402至406。

[0035] 在流程402中，裝置活動回報程式120的偵測模塊210，會偵測及搜集與所屬的運算裝置有關的可疑活動記錄以及時間戳記。為了方便說明起見，以下舉運算裝置111為例來加以說明。

[0036] 安裝在運算裝置111中的裝置活動回報程式120，可在流程402中利用偵測模塊210讀取並分析運算裝置111內的特定非揮發性資料的內容，例如，系統日誌、開機自動啟動項目、執行紀錄、和/或特定類型檔案的檔案詮釋資料（meta data）等等。

[0037] 例如，在運算裝置111的作業系統是Windows系統的情況下，偵測模塊210可讀取並分析運算裝置111中所儲存的視窗事件日誌（Windows Event Log）、自動啟動登錄檔（Autorun Registry）、排程工作記錄（Schedule Job）、預取快取（Prefetch cache）、應用程式相容性快取（Shimcache和/或Amcache）、和/或.exe/.dll/.sys格式的可移植性可執行檔案（portable executable files，PE files）的檔案詮釋資料等等。

[0038] 又例如，在運算裝置111的作業系統是Linux系統的情況下，偵測模塊210可讀取並分析運算裝置111中的資料夾「/var/log/」底下的日誌項目、系統與服務管理工具（Systemd）、系統初始化腳本（SysV init script）、排程指令（crontab）、系統初始化程序（Upstart）、.php或.jsp格式的動態網頁（dynamic web pages）、指令執行腳本（shell scripts）、敏感性檔案（sensitive files）、指令歷史記錄（command histories）、系統日誌（syslog）、和/或.so/.ko格式的可執行與可連結格式檔案（Executable and Linkable Format files，ELF files）的檔案詮釋資料等等。

[0039] 又例如，在運算裝置111的作業系統是macOS系統的情況下，偵測模塊210可讀取並分析運算裝置111中的資料夾「/var/log/」底下的日誌項目、資料夾「/Library/LaunchAgents/」底下的記錄、資料夾「/Library/LaunchDaemons/」底下的記錄、指令執行腳本（shell scripts）、指令歷史記錄（command histories）、和/或Mach物件格式的可執行檔案（Mach object files，Mach-O files）的檔案詮釋資料等等。

[0040] 除了前述的非揮發性資料以外，偵測模塊210還可在流程402中偵測並分析運算裝置111當時的記憶體內容、和/或網路行為等特定揮發性資料的內容。例如，偵測模塊210可利用網路連線查詢指令「netstat」查詢運算裝置111和外部網路連線的狀況，也可利用各種方式偵測運算裝置111所存取的網路位址（IP address）、以及運算裝置111的網路連接埠（network ports）的運作狀況。

[0041] 在運作時，偵測模塊210可利用各種過濾及判斷演算法，對前述與運算裝置111有關的特定非揮發性資料和/或揮發性資料的內容進行初步分析，以從運算裝置111為數眾多的活動歷史記錄中，篩選出可能與駭客入侵活動有關的部分活動記錄做為可疑活動記錄，藉此減少後續需要由活動記錄匯集裝置130以及可疑事件研判裝置140進行處理或分析的資料量。

[0042] 在實際應用中，偵測模塊210所判定的可疑活動記錄，可能包含與運算裝置111有關的多種類型的檔案執行活動（file execution activity）、檔案產生活動（file creation activity）、檔案編輯活動（file editing activity）、網路存取活動（networking activity）、鍵盤側錄活動（keystroke logging activity）、密碼竊取活動（password stealing activity）、憑證傾印活動（credential dumping activity）、程式碼注入活動（code injection activity）、記憶體區塊修改活動（code manipulation activity）、和/或可執行碼存取活動（executable code accessing activity）等等的歷史記錄。

[0043] 從前述可疑活動記錄的名稱，可顧名思義理解個別可疑活動記錄的大致物理意義，而個別可疑活動記錄的詳細定義，則取決於偵測模塊210的記錄偵測規則。在不同的偵測規則下，同樣名稱的可疑活動記錄的具體定義可能會略有不同。

[0044] 另外，當偵測模塊210將某一活動記錄判斷為可疑活動記錄時，偵測模塊210還會將運算裝置111中關於該活動記錄的時間戳記記錄下來，以做為該可疑活動記錄的相應時間戳記。

[0045] 實作上，裝置活動回報程式120的偵測模塊210可在運算裝置111運作的過程中，即時（real time）進行前述流程402的運作，也可間歇性或週期性地進行前述流程402的運作。

[0046] 在流程404中，裝置活動回報程式120的屬性判斷模塊220會根據前述偵測模塊210對於可疑活動記錄的分析結果，建立對應於可疑活動記錄的屬性標籤。

[0047] 例如，屬性判斷模塊220可對被偵測模塊210判定為與已知的APT攻擊所使用的惡意程式家族有關的可疑活動記錄，設定一個相應的標籤「APT Malware」。

[0048] 又例如，屬性判斷模塊220可對被偵測模塊210判定為跟會自動在開機後啟動的程式有關的可疑活動記錄，設定一個相應的標籤「Autorun」。

[0049] 又例如，屬性判斷模塊220可對被偵測模塊210判定為跟具有網路活動的程式有關的可疑活動記錄，設定一個相應的標籤「Networking」。

[0050] 又例如，屬性判斷模塊220可對被偵測模塊210判定為與具有鍵盤側錄功能的

程式或記憶體內容有關的可疑活動記錄，設定一個相應的標籤「**Keystroke Logging**」。

[0051] 又例如，屬性判斷模塊220可對被偵測模塊210判定為跟具有竊取密碼或憑證功能的程式有關的可疑活動記錄，設定一個相應的標籤「**Password Stealer**」。

[0052] 又例如，屬性判斷模塊220可對被偵測模塊210判定為具有隱藏屬性的檔案有關的可疑活動記錄，設定一個相應的標籤「**Hidden Files**」。

[0053] 又例如，屬性判斷模塊220可對被偵測模塊210判定為與記憶體區塊中的可執行碼有關的可疑活動記錄，設定一個相應的標籤「**Executable Code**」。

[0054] 又例如，屬性判斷模塊220可對被偵測模塊210判定為涉及可疑的注入程式有關的可疑活動記錄，設定一個相應的標籤「**Code Manipulation**」。

[0055] 又例如，屬性判斷模塊220可對被偵測模塊210判定為與具有已知惡意程式特徵的記憶體內容有關的可疑活動記錄，設定一個相應的標籤「**Malware**」。

[0056] 又例如，屬性判斷模塊220可對被偵測模塊210判定為與具有密碼或憑證竊取功能的記憶體內容有關的可疑活動記錄，設定一個相應的標籤「**Access Credentials**」。

[0057] 經過屬性判斷模塊220設定屬性標籤之後，不同的可疑活動記錄可能具有相同的屬性標籤，也可能具有不同的屬性標籤。另外，屬性判斷模塊220有可能對同一個可疑活動記錄設定多個不同的屬性標籤，所以不同的可疑活動記錄的屬性標籤的數量有可能彼此不同。

[0058] 在流程406中，裝置活動回報程式120的傳送模塊230可透過適當的資料傳輸方式，將與運算裝置111有關的可疑活動記錄、及相應的時間戳記與屬性標籤，傳送給活動記錄匯集裝置130。

[0059] 其他運算裝置112～115中的裝置活動回報程式120，都可比照前述的方式獨自進行流程402～406的運作，以將相關運算裝置的可疑活動記錄、及相應的時間戳記與屬性標籤，傳送給活動記錄匯集裝置130。

[0060] 另外，前述運算裝置111～115中的多個裝置活動回報程式120，可在相同的預定時段同步進行前述流程402～406的運作，也可各自在不同的時段獨立進行前述流程402～406的運作。

[0061] 由前述說明可知，前述運算裝置111～115中的多個裝置活動回報程式120，會分別產生與運算裝置111～115有關的多個可疑活動記錄與多個時間戳記，並建立對應於多個可疑活動記錄的多個屬性標籤。

[0062] 在流程408中，活動記錄匯集裝置130的通信電路131會透過適當的網路連線

（例如，標的網路系統102的內部網路或網際網路），接收標的網路系統102中的多個運算裝置111～115傳來的多個可疑活動記錄、及相應的多個時間戳記與多個屬性標籤。

[0063] 在流程410中，活動記錄匯集裝置130的處理電路133會處理接收到的多個可疑活動記錄、及相應的多個時間戳記與多個屬性標籤，以產生一回傳資料。例如，處理電路133可對接收到的多個可疑活動記錄、及相應的多個時間戳記與多個屬性標籤，進行資料封裝、壓縮、加密、電子簽章、分割等各種處理，以產生適當格式的回傳資料。

[0064] 在流程412中，處理電路133會利用通信電路131將回傳資料透過合適的網路（例如，網際網路）傳送給可疑事件研判裝置140。

[0065] 在流程414中，可疑事件研判裝置140的通信電路143會透過合適的網路（例如，網際網路）接收活動記錄匯集裝置130所產生的回傳資料。

[0066] 在流程416中，可疑事件研判裝置140的控制電路149會對接收到的回傳資料進行處理，以從回傳資料中獲取與標的網路系統102有關的多個可疑活動記錄、及相應的多個時間戳記與多個屬性標籤。例如，控制電路149可對回傳資料進行組合、解壓縮、解密、驗證電子簽章等各種處理，以從回傳資料中擷取出前述的活動紀錄、時間戳記、與屬性標籤。

[0067] 在流程418中，控制電路149會執行儲存電路147中的可疑事件時序圖產生程式150，以依據前述的多個可疑活動記錄、及相應的多個時間戳記與多個屬性標籤，進行一可疑事件時序圖產生運作，以產生並顯示一可疑事件時序圖。

[0068] 請參考圖5，其所繪示為可疑事件研判裝置140中的顯示裝置141所顯示的影像畫面500的一實施例簡化後的示意圖。

[0069] 在圖5的實施例中，顯示裝置141所顯示的影像畫面500內包含有多個資料圖框（例如，圖5中的示例性資料圖框510～540）、以及一可疑事件時序圖550。影像畫面500中的每個資料圖框510～540可用於顯示裝置連線關係圖、裝置互動關聯圖、統計圖、分析圖、資料表單、選單、文件或檔案清單等各種不同類型的文字資訊或圖形化資訊。可疑事件時序圖550則用於呈現前述可疑事件研判裝置140執行可疑事件時序圖產生程式150後所產生的影像內容。前述資料圖框510～540與可疑事件時序圖550的內容，可供資安分析人員用來做為診斷標的網路系統102是否已受到駭客入侵時的判斷依據。

[0070] 在進行診斷的過程中，資安分析人員可透過輸入裝置145進行各種操作，以

增加或減少資料圖框的數量、調整個別資料圖框的大小或位置、修改相關分析參數、下達各式指令等等。

[0071] 由前述說明可知，標的網路系統102中的多個運算裝置111～115可將相關的可疑活動記錄、時間戳記、與多個屬性標籤，傳送給活動記錄匯集裝置130，然後活動記錄匯集裝置130再據以產生回傳資料、並傳送給可疑事件研判裝置140。這樣的方式有助於降低標的網路系統102的對外網路頻寬需求，也有助於提升活動記錄匯集裝置130與可疑事件研判裝置140之間的資料傳輸安全性。

[0072] 以下將搭配圖6至圖8來進一步說明可疑事件研判裝置140進行可疑事件時序圖產生運作的方式。圖6為本發明一實施例的產生可疑事件時序圖550的方法簡化後的流程圖。圖7與圖8為本發明不同實施例的可疑事件時序圖550的局部內容簡化後的示意圖。

[0073] 在圖6的流程圖中，位於一特定模塊所屬欄位中的流程，即代表由該特定模塊所進行的流程。例如，標記在「事件分析模塊」欄位中的部分，是由可疑事件時序圖產生程式150中的事件分析模塊310所進行的流程；標記在「視覺物件產生模塊」欄位中的部分，是由視覺物件產生模塊320所進行的流程；標記在「排列模塊」欄位中的部分，則是由排列模塊330所進行的流程；而標記在「信息標註模塊」欄位中的部分，則是由信息標註模塊340所進行的流程。前述的邏輯也適用於後續的其他流程圖中。

[0074] 在流程602中，可疑事件時序圖產生程式150的事件分析模塊310，會利用控制電路149依據前述的多個可疑活動記錄、及相應的多個時間戳記與多個屬性標籤，界定出與標的網路系統102有關的多個可疑事件、以及分別對應於多個可疑事件的多個時間記錄。

[0075] 對於事件分析模塊310而言，前述的多個可疑活動記錄、以及相應的多個時間戳記與多個屬性標籤，都是可用來分析在標的網路系統102中是否發生特定事件的數位證據（digital evidence）。事件分析模塊310可利用各種規則比對演算法或人工智慧演算法，對前述的多個可疑活動記錄、及相應的多個時間戳記與多個屬性標籤進行交叉比對與事件關聯分析（event correlation analysis），以界定出標的網路系統102中可能涉及駭客入侵活動的多個可疑事件，以及分別對應於前述多個可疑事件的多個時間記錄。

[0076] 例如，事件分析模塊310可對與一特定運算裝置有關的多個可疑活動記錄進行各種交叉比對與事件關聯分析，找出有足夠確切的數位證據能夠證明是在該特定運

算裝置內部發生的一個或多個可疑事件。另外，事件分析模塊310也可依據與兩個不同的運算裝置有關的多個可疑活動記錄進行各種交叉比對與事件關聯分析，找出有足夠確切的數位證據能夠證明是在這兩個運算裝置之間發生的一個或多個可疑事件。

[0077] 再者，事件分析模塊310還可依據前述的多個時間戳記，界定出個別可疑事件的起始時間、或是結束時間，以做為個別可疑事件的相應時間記錄。

[0078] 為了方便說明起見，在個別運算裝置內部所發生的可疑事件，以下稱為裝置內部事件（**device internal events**），而在兩個不同的運算裝置之間發生的可疑事件，以下則稱為裝置互動事件（**device interaction events**）。

[0079] 事件分析模塊310依據前述的數位證據（亦即，可疑活動記錄、時間戳記、與屬性標籤）所界定出來的裝置內部事件的類型與數量，取決於標的網路系統102的實際情況。同樣地，事件分析模塊310依據前述的數位證據所界定出來的裝置互動事件的類型與數量，也取決於標的網路系統102的實際情況。

[0080] 倘若事件分析模塊310所界定出來的裝置內部事件的類型過多、或是裝置互動事件的類型過多，容易導致後續產生的可疑事件時序圖550的內容過於擁擠或雜亂，反而會對資安分析人員造成信息雜訊干擾，進而影響到資安分析人員的判讀與分析效率。

[0081] 為了降低這方面的問題，事件分析模塊310可針對裝置內部事件的類型的個數設置一相應的第一上限，並針對裝置互動事件的類型的個數設置一相應的第二上限。前述的第一上限與第二上限的大小可以相同，也可以不同。

[0082] 在運作時，事件分析模塊310可依據事件類型的重要性、罕見性、敏感性、事件數量、和/或其他考量因素，篩選出最後要顯示在可疑事件時序圖550中的裝置內部事件的類型、以及裝置互動事件的類型。

[0083] 例如，事件分析模塊310可限制最多只有8種類型的裝置內部事件能夠顯示在可疑事件時序圖550中，分別是檔案產生事件（**file creation event**）、檔案存取事件（**file access event**）、註冊機碼產生事件（**registry creation event**）、排程工作事件（**schedule task event**）、檔案執行事件（**file execution event**）、記憶體模組偵測事件（**memory module detection event**）、記憶體程序產生事件（**memory process creation event**）、以及權限提升事件（**privileges escalation event**）。同時，事件分析模塊310可限制最多只有6種類型的裝置互動事件能夠顯示在可疑事件時序圖550中，分別是遠端登入事件（**remote logon event**）、暴力嘗試登入事件（**brute-force logon event**）、登入

失敗事件（attempt logon event）、遠端存取檔案事件（remote access event）、檔案移動事件（file moving event）、以及網路下載事件（network download event）。換言之，在本實施例中，前述的第一上限是8，而第二上限則是6。

[0084] 在另一實施例中，事件分析模塊310可限制最多只有3種類型的裝置內部事件能夠顯示在可疑事件時序圖550中，分別是前述的檔案產生事件、檔案執行事件、以及記憶體程序產生事件。同時，事件分析模塊310可限制最多只有4種類型的裝置互動事件能夠顯示在可疑事件時序圖550中，分別是前述的遠端登入事件、遠端存取檔案事件、檔案移動事件、以及網路下載事件。換言之，在本實施例中，前述的第一上限是3，而第二上限則是4。

[0085] 從前述事件類型的名稱，可顧名思義理解個別事件類型的大致物理意義，而個別事件類型的詳細定義，則取決於事件分析模塊310所進行的事件關聯分析的分析規則。在不同的分析規則下，同樣名稱的事件類型的具體定義可能會略有不同。

[0086] 在實際應用中，事件分析模塊310也可按照可疑事件時序圖550的顯示空間的大小，動態調整前述的第一上限與第二上限的大小，或是根據其他設計上的考量，彈性調整前述的第一上限與第二上限的大小。

[0087] 為了方便說明起見，以下假設事件分析模塊310在流程602中所界定出來的裝置內部事件共有3個類型，分別是前述的檔案產生事件、檔案執行事件、以及記憶體程序產生事件，並假設事件分析模塊310所界定出來的裝置互動事件共有4個類型，分別是前述的遠端登入事件、遠端存取檔案事件、檔案移動事件、以及網路下載事件。事件分析模塊310所界定出來的每個類型的可疑事件的數量，與標的網路系統102被駭客入侵的程度與範圍有關，所以可能會彼此不同。

[0088] 以下將搭配圖7中所繪示的可疑事件時序圖550的局部內容來進一步說明圖6中的後續流程。

[0089] 在流程604中，視覺物件產生模塊320會建立分別與多個可疑事件所涉及的多個參與裝置相對應的多個主視覺物件，使得不同的主視覺物件分別對應於不同的參與裝置。

[0090] 在說明書及申請專利範圍中所指稱的「參與裝置」一詞，指的是涉及事件分析模塊310所定義出來的多個可疑事件的裝置實體（entity），有可能是指標的網路系統102中的運算裝置，也有可能是指位於標的網路系統102之外的其他裝置實體，例如，圖1中所繪示的惡意檔案提供裝置160。

[0091] 實作上，視覺物件產生模塊320可用各種圖案、影像、或文字框來呈現個別的主視覺物件，且不同的主視覺物件的視覺表述方式（visual representation）可彼此相同、也可彼此不同。

[0092] 例如，在圖7的實施例中，視覺物件產生模塊320是用圓角四邊形的圖框來做為示例性的主視覺物件701、703、與705的視覺表述方式。在此假設主視覺物件701、703、與705分別對應於標的網路系統102中涉及可疑事件的3個運算裝置111、112、與113。

[0093] 在流程606中，排列模塊330可將前述的多個主視覺物件701、703、與705水平排列在可疑事件時序圖550的一上部區域710中。

[0094] 在流程608中，信息標註模塊340可顯示每個主視覺物件701、703、與705所對應的參與裝置的摘要描述。實作上，信息標註模塊340可將能夠讓資安分析人員辨識個別主視覺物件所對應的參與裝置的信息，例如，裝置名稱、網路位址（IP address）、裝置代碼、硬體識別碼（例如，MAC位址）、裝置代表圖像、使用者名稱、使用者代碼、使用者暱稱、或使用者代表圖像等等，顯示在個別主視覺物件上或是個別主視覺物件的附近，以做為相應的參與裝置的摘要描述。

[0095] 例如，在此假設運算裝置111、112、與113的裝置名稱分別是「Web_Server」、「Bob's PC」、與「Candy's NB」。如圖7所示，信息標註模塊340可將運算裝置111、112、與113的裝置名稱，分別顯示在相應的主視覺物件701、703、與705中，以供資安分析人員辨識個別主視覺物件的物理意義。

[0096] 在流程610中，排列模塊330可將多個主視覺物件701、703、與705按照與在上部區域710中相同的順序，重複顯示在可疑事件時序圖550的一下部區域720中。

[0097] 請注意，在前述圖7的實施例中，視覺物件產生模塊320是用相同的視覺表述方式來呈現所有的主視覺物件701、703、與705，但這只是一示範性的實施例，並非侷限本發明的實際實施方式。實作上，視覺物件產生模塊320也可依據所對應的參與裝置的類型，來設置個別主視覺物件的視覺表述方式，以使得對應於不同類型的參與裝置的不同主視覺物件具有不同的視覺表述方式。

[0098] 在流程612中，視覺物件產生模塊320會建立分別與多個主視覺物件相對應的多個垂直圖案。實作上，視覺物件產生模塊320可用各種垂直線、垂直條紋、或垂直影像，來呈現個別的垂直圖案。

[0099] 例如，在圖7中，視覺物件產生模塊320是用垂直線的形式，來呈現分別與主

視覺物件701、703、與705相對應的示例性垂直圖案731、733、與735。

[0100] 在流程614中，排列模塊330可將前述的多個垂直圖案731、733、與735分別排列在多個主視覺物件701、703、與705的下方，以象徵個別主視覺物件所對應的時間軸。

[0101] 在流程616中，視覺物件產生模塊320會建立分別與多個裝置內部事件相對應的多個副視覺物件。實作上，視覺物件產生模塊320可用各種圖案、影像、或文字框來呈現個別的副視覺物件，且不同的副視覺物件的視覺表述方式可彼此相同、也可彼此不同。

[0102] 例如，在圖7中，視覺物件產生模塊320是用圓角四邊形的圖框形式來呈現示例性的副視覺物件741、742、743、744、745、與746，且不同的副視覺物件分別對應於不同的裝置內部事件。

[0103] 在流程618中，排列模塊330會將個別參與裝置所對應的副視覺物件，按照相應的裝置內部事件的時間順序，由上而下排列在相應的主視覺物件下方的垂直圖案上。

[0104] 例如，在圖7中，排列模塊330可將對應於運算裝置111的副視覺物件741、742、與743，按照相應的裝置內部事件的時間順序，由上而下排列在相應的主視覺物件701下方的垂直圖案731上的適當位置。另外，排列模塊330可將對應於運算裝置112的副視覺物件744，按照相應的裝置內部事件的時間順序，排列在相應的主視覺物件703下方的垂直圖案733上的適當位置。再者，排列模塊330還可將對應於運算裝置113的副視覺物件745與746，按照相應的裝置內部事件的時間順序，由上而下排列在相應的主視覺物件705下方的垂直圖案735上的適當位置。

[0105] 藉由排列模塊330的運作，可疑事件時序圖550中的任意兩個不同的副視覺物件在垂直方向上的相對位置，可反映出這兩個副視覺物件所對應的兩個裝置內部事件之間的時間先後順序。但請注意，在可疑事件時序圖550中，兩個不同的副視覺物件在垂直方向上的間隔距離，與所對應的兩個裝置內部事件之間的時間差距，並不一定要有絕對的比例關係。

[0106] 在流程620中，信息標註模塊340可顯示每個副視覺物件所對應的裝置內部事件的摘要描述。實作上，信息標註模塊340可將能夠讓資安分析人員理解個別副視覺物件所對應的裝置內部事件的概要內容的信息，例如，事件名稱、代表符號、代表圖像、或精簡文字敘述等等，顯示在個別副視覺物件上或是個別副視覺物件的附近，以做為相應的裝置內部事件的摘要描述。

[0107] 例如，在此假設前述的事件分析模塊310界定出運算裝置111曾發生3項裝置內部事件，按照時間先後順序分別是「針對檔案report.doc的檔案執行事件」、「針對檔案scvhost.exe的檔案執行事件」、以及「針對檔案scvhost.exe的檔案產生事件」；運算裝置112曾發生1項裝置內部事件：「針對檔案scvhost.exe的檔案產生事件」；且運算裝置113曾發生2項裝置內部事件，按照時間先後順序分別是「針對檔案scvhost.exe的檔案產生事件」、以及「針對檔案scvhost.exe的檔案執行事件」。如圖7所示，信息標註模塊340可將分別與運算裝置111曾發生的3項裝置內部事件相對應的精簡文字敘述「Execution report.doc」、「Execution scvhost.exe」、與「File Creation scvhost.exe」，分別顯示在相應的副視覺物件741、742、與743中。另外，信息標註模塊340可將與運算裝置112曾發生的1項裝置內部事件相對應的精簡文字敘述「File Creation scvhost.exe」，顯示在相應的副視覺物件744中。再者，信息標註模塊340還可將分別與運算裝置113曾發生的2項裝置內部事件相對應的精簡文字敘述「File Creation scvhost.exe」與「Execution scvhost.exe」，分別顯示在相應的副視覺物件745與746中。如此一來，資安分析人員便能夠依據個別副視覺物件上的摘要描述，明白相應的裝置內部事件的概要內容。

[0108] 請注意，前述個別裝置內部事件所對應的精簡文字敘述，只是一示範性的實施例，並非侷限本發明的實際實施方式。實作上，可疑事件時序圖產生程式150的設計者可針對各種不同的裝置內部事件的態樣，分別設計能夠讓資安分析人員理解的其他摘要描述方式，例如，代表符號與檔案名稱的組合、代表圖像與檔案名稱的組合、或事件名稱與檔案代表圖像的組合等等。

[0109] 另外，在前述圖7的實施例中，視覺物件產生模塊320是用相同的視覺表述方式來呈現所有的副視覺物件741~746，但這也只是一示範性的實施例，並非侷限本發明的實際實施方式。實作上，視覺物件產生模塊320也可依據所對應的裝置內部事件的類型，來設置個別副視覺物件的視覺表述方式，以使得對應於不同類型的裝置內部事件的不同副視覺物件具有不同的視覺表述方式。

[0110] 在流程622中，視覺物件產生模塊320會建立分別與多個裝置互動事件相對應的多條關係線。實作上，視覺物件產生模塊320可用直線、折線（broken line）、略微彎曲的線條（slightly-bended line）、波浪線（wavy line）、或其他類似功能的線條來做為個別關係線的視覺表述，且不同的關係線的視覺表述方式可彼此相同、也可彼此不同。

[0111] 例如，在圖7中，視覺物件產生模塊320是用水平直線的形式來呈現示例性的關係線751、752、753、754、755、與756，且不同的關係線分別對應於不同的裝置互動事件。在本實施例中，前述的關係線751、752、753、754、755、與756，都是以水平實線（solid line）做為視覺表述方式。

[0112] 在流程624中，視覺物件產生模塊320會在每條關係線上，依據該關係線所對應的裝置互動事件的內容，設置相應的指向符號，以指示裝置互動事件的方向性。實作上，視覺物件產生模塊320可用各種箭頭、手指圖案、或其他可表達方向性的圖案，來呈現個別的指向符號。

[0113] 例如，在圖7中，視覺物件產生模塊320是以箭頭做為指向符號761、762、763、764、765、與766的視覺表述方式，並將指向符號761、762、763、764、765、與766分別設置在關係線751、752、753、754、755、與756上，以表達相關裝置互動事件的方向性。

[0114] 在流程626中，排列模塊330會將多條關係線按照時間順序由上而下排列，並將每條關係線的兩端分別接觸所涉及的兩個參與裝置所對應的兩個垂直圖案。

[0115] 例如，在圖7中，排列模塊330可將對應於發生在運算裝置111與運算裝置112之間的裝置互動事件的示例性關係線751、752、與753，按照相應的裝置互動事件的時間順序，由上而下排列，並將關係線751、752、與753的兩端，設置成分別接觸運算裝置111所對應的垂直圖案731、以及運算裝置112所對應的垂直圖案733，使關係線751、752、與753位於垂直圖案731與垂直圖案733之間。另外，排列模塊330可將對應於發生在運算裝置112與運算裝置113之間的裝置互動事件的示例性關係線754、755、與756，按照相應的裝置互動事件的時間順序，由上而下排列，並將關係線754、755、與756的兩端，設置成分別接觸運算裝置112所對應的垂直圖案733、以及運算裝置113所對應的垂直圖案735，使關係線754、755、與756位於垂直圖案733與垂直圖案735之間。

[0116] 藉由排列模塊330的運作，可疑事件時序圖550中的任意兩條不同的關係線在垂直方向上的相對位置，可反映出這兩條關係線所對應的兩個裝置互動事件之間的時間先後順序。但請注意，在可疑事件時序圖550中，兩條不同的關係線在垂直方向上的間隔距離，與所對應的兩個裝置互動事件之間的時間差距，並不一定要有絕對的比例關係。

[0117] 在流程628中，信息標註模塊340可顯示每條關係線所對應的裝置互動事件的摘要描述。實作上，信息標註模塊340可將能夠讓資安分析人員理解個別關係線所對應

的裝置互動事件的概要內容的信息，例如，事件名稱、代表符號、代表圖像、或精簡文字敘述等等，顯示在個別關係線上或是個別關係線的附近，以做為相應的裝置互動事件的摘要描述。

[0118] 例如，在此假設前述的事件分析模塊310界定出運算裝置111與運算裝置112之間曾發生3項裝置互動事件，按照時間先後順序分別是「關於用戶名稱bob的遠端登入事件」、「針對檔案scvhost.exe的遠端存取檔案事件」、以及「針對檔案scvhost.exe的檔案移動事件」；並假設事件分析模塊310界定出運算裝置112與運算裝置113之間曾發生3項裝置互動事件，按照時間先後順序分別是「關於用戶名稱candy的遠端登入事件」、「針對檔案scvhost.exe的遠端存取檔案事件」、以及「針對檔案scvhost.exe的檔案移動事件」。如圖7所示，對於運算裝置111及運算裝置112之間曾發生的3項裝置互動事件，信息標註模塊340會將3個描述信息771、772、與773分別顯示在相應的關係線751、752、與753的上方，且描述信息771、772、與773的內容分別是與前述3項裝置互動事件相對應的精簡文字敘述「Logon: bob」、「File Accessed: scvhost.exe」、與「File Movement: scvhost.exe」。另外，對於運算裝置112及運算裝置113之間曾發生的3項裝置互動事件，信息標註模塊340會將3個描述信息774、775、與776分別顯示在相應的關係線754、755、與756的上方，且描述信息774、775、與776的內容分別是與前述3項裝置互動事件相對應的精簡文字敘述「Logon: candy」、「File Accessed: scvhost.exe」、與「File Movement: scvhost.exe」。如此一來，資安分析人員便能夠依據個別關係線上方的摘要描述，明白相應的裝置互動事件的概要內容。

[0119] 請注意，前述個別裝置互動事件所對應的精簡文字敘述，只是一示範性的實施例，並非侷限本發明的實際實施方式。實作上，可疑事件時序圖產生程式150的設計者可針對各種不同的裝置互動事件的態樣，分別設計能夠讓資安分析人員理解的其他摘要描述方式，例如，代表符號與檔案名稱的組合、代表符號與用戶名稱的組合、代表圖像與檔案名稱的組合、代表圖像與用戶名稱的組合、或事件名稱與檔案代表圖像的組合等等。

[0120] 另外，在前述圖7的實施例中，視覺物件產生模塊320是用相同的視覺表述方式來呈現所有的關係線751~756，但這也只是一示範性的實施例，並非侷限本發明的實際實施方式。實作上，視覺物件產生模塊320也可依據所對應的裝置互動事件的類型，來設置個別關係線的視覺表述方式，以使得對應於不同類型的裝置互動事件的不同關係線具有不同的視覺表述方式。

[0121] 由前述說明可知，可疑事件時序圖產生程式150會依據與標的網路系統102有關的多個可疑活動記錄、及相應的多個時間戳記與多個屬性標籤，分析出多個可疑事件，並過濾掉多餘的雜訊資料。換言之，可疑事件時序圖產生程式150所產生的可疑事件時序圖550，能大幅減少資安分析人員需要關注的資料量，所以能有效減輕大量雜訊資料干擾資安分析人員的問題。

[0122] 此外，可疑事件時序圖產生程式150還會將重要的可疑事件、涉及可疑事件的參與裝置、可疑事件在時序上的相關性、內部網路中的裝置互動行為、以及可疑事件的擴散方向等多種維度的參考資訊，以精簡的視覺表述方式同時呈現在可疑事件時序圖550中。因此，資安分析人員可從可疑事件研判裝置140所產生的前述可疑事件時序圖550中，迅速獲取多個可疑事件、涉及的參與裝置、可疑事件之間的時序關係、以及可疑事件的擴散方向等多種維度的重要參考資訊。如此一來，資安分析員人便無需耗費大量時間從數量眾多的數位證據中慢慢釐清發生的可疑事件、以及歸納出可疑事件之間的時間順序與因果關係。

[0123] 再者，根據認知科學的研究可以發現，人類對於圖像化信息的理解效率，要比對於純文字內容的理解效率高出許多。由於可疑事件時序圖產生程式150所產生的可疑事件時序圖550，能將前述的多種維度的參考資訊，以直觀的視覺化方式呈現給資安分析人員，因此有助於大幅減少資安分析人員耗費在分析數位證據所需的時間，進而能夠有效提升診斷標的網路系統102是否已受到駭客入侵的效率。

[0124] 在某些應用情境中，個別可疑事件的起始時間、個別可疑事件的結束時間、和/或不同可疑事件之間的時間差距，可能是資安分析人員在判斷標的網路系統102是否已受到駭客入侵時的重要考量因素之一。為了提供這方面的參考資訊給資安分析人員，信息標註模塊340還可在前述的流程620中顯示每個副視覺物件所對應的裝置內部事件的相應時間記錄，和/或在前述的流程628中顯示每條關係線所對應的裝置互動事件的相應時間記錄。

[0125] 實作上，信息標註模塊340可將個別副視覺物件所對應的裝置內部事件的時間記錄，顯示在個別副視覺物件上或是個別副視覺物件的附近。另一方面，信息標註模塊340可將個別關係線所對應的裝置互動事件的時間記錄，顯示在個別關係線上或是個別關係線的附近。

[0126] 例如，在圖8所繪示的可疑事件時序圖550的局部內容中，信息標註模塊340可在個別副視覺物件中，標示該副視覺物件所對應的裝置內部事件的時間記錄，並可

在個別關係線的上方，標示該關係線所對應的裝置互動事件的時間記錄。由前述說明可知，信息標註模塊340顯示在可疑事件時序圖550中的時間記錄，可以是相應可疑事件的起始時間、或是結束時間。

[0127] 如此一來，資安分析人員便能夠依據可疑事件時序圖550中顯示的時間記錄，迅速辨別個別裝置內部事件或裝置互動事件的時間信息，並用來做為判斷依據，以進一步提升判斷標的網路系統102是否已受到駭客入侵的精確度。

[0128] 前述有關圖7中的其他視覺元素的產生方式、代表的物理意義、以及相關優點等說明，亦適用於圖8的實施例。為簡潔起見，在此不重複敘述。

[0129] 請參考圖9，其所繪示為本發明另一實施例的可疑事件時序圖550的局部內容簡化後的示意圖。如前所述，可疑事件時序圖產生程式150的事件分析模塊310會在前述流程602中，利用控制電路149界定出與標的網路系統102有關的多個可疑事件與相應的多個時間記錄。在某些應用情境中，事件分析模塊310所界定出來的多個可疑事件，不僅會涉及標的網路系統102中的參與裝置，也可能涉及位於標的網路系統102之外的其他參與裝置（例如，前述的惡意檔案提供裝置160）。在此情況下，視覺物件產生模塊320在前述的流程604中也會針對位於標的網路系統102之外的其他參與裝置建立相應的主視覺物件。

[0130] 在圖9的實施例中，可疑事件時序圖550包含有示例性的主視覺物件901、903、905、907、與909；示例性的垂直圖案931、933、934、937、與939；示例性的副視覺物件941、942、943、944、與945；示例性的關係線951、952、953、954、955、與956；示例性的指向符號961、962、963、964、965、與966；以及示例性的描述信息971、972、973、974、975、與976。

[0131] 為了方便說明起見，在此假設圖9中的主視覺物件901對應於位於標的網路系統102外部的惡意檔案提供裝置160，且惡意檔案提供裝置160的網路位址是「123.0.0.1」；主視覺物件903、905、907、與909，分別對應於標的網路系統102中涉及可疑事件的3個運算裝置111、112、113、與114，且運算裝置111、112、113、與114的裝置名稱分別是「Web_Server」、「Bob's PC」、「Candy's NB」、與「AD Server」；副視覺物件941與942分別對應於運算裝置111曾發生的2項裝置內部事件，按照時間先後順序分別是「針對檔案m.exe的檔案產生事件」與「針對檔案m.exe的檔案執行事件」；副視覺物件943對應於運算裝置112曾發生的1項裝置內部事件，其為「針對檔案m.exe的檔案產生事件」；副視覺物件944與945分別對應於運算裝置113曾發生

的2項裝置內部事件，按照時間先後順序分別是「針對檔案p.exe的檔案產生事件」與「針對檔案p.exe的記憶體程序產生事件」；關係線951對應於惡意檔案提供裝置160與運算裝置111之間曾發生的1項裝置互動事件，其為「針對檔案m.exe的網路下載事件」；關係線952與953分別對應於運算裝置111與運算裝置112之間曾發生的2項裝置互動事件，按照時間先後順序分別是「關於用戶名稱administrator的遠端登入事件」與「針對檔案m.exe的遠端存取檔案事件」；關係線954對應於運算裝置112與運算裝置113之間曾發生的1項裝置互動事件，其為「關於用戶名稱candy的遠端登入事件」；關係線955對應於運算裝置111與運算裝置113之間曾發生的1項裝置互動事件，其為「針對檔案p.exe的網路下載事件」；且關係線956對應於運算裝置113與運算裝置114之間曾發生的1項裝置互動事件，其為「關於用戶名稱admin的遠端登入事件」。

[0132] 在產生圖9的可疑事件時序圖550的過程中，可疑事件時序圖產生程式150的視覺物件產生模塊320會進行圖6中的流程604、612、616、與622，以建立前述的主視覺物件901～909、垂直圖案931～939、副視覺物件941～945、以及關係線951～956。此外，視覺物件產生模塊320還會進行圖6中的流程624，以設置前述的指向符號961～966。

[0133] 與前述圖7與圖8的實施例類似，排列模塊330會進行圖6中的流程606、610、614、618、及626，以將主視覺物件901～909、垂直圖案931～939、副視覺物件941～945、關係線951～956、以及指向符號961～966，排列成如圖9所繪示的態樣。

[0134] 信息標註模塊340則會進行圖6中的流程608、620、及628，以顯示個別主視覺物件所對應的參與裝置的摘要描述、個別副視覺物件所對應的裝置內部事件的摘要描述、以及個別關係線所對應的裝置互動事件的摘要描述。

[0135] 例如，如圖9所示，信息標註模塊340可將惡意檔案提供裝置160的網路位址顯示在相應的主視覺物件901中做為摘要描述，並將運算裝置111～114的裝置名稱分別顯示在相應的主視覺物件903～909中做為摘要描述，以供資安分析人員能夠辨識個別主視覺物件的物理意義。

[0136] 另外，信息標註模塊340可將分別與運算裝置111曾發生的2項裝置內部事件相對應的精簡文字敘述「File Creation m.exe」與「Execution m.exe」，分別顯示在相應的副視覺物件941與942中做為摘要描述；將與運算裝置112曾發生的1項裝置內部事件相對應的精簡文字敘述「File Creation m.exe」，顯示在相應的副視覺物件943中做為摘要描述；並將分別與運算裝置113曾發生的2項裝置內部事件相對應的精簡文字敘述

「File Creation p.exe」與「Process p.exe」，分別顯示在相應的副視覺物件944與945中做為摘要描述。如此一來，資安分析人員便能夠依據個別副視覺物件上所顯示的摘要描述，明白個別副視覺物件所代表的裝置內部事件的概要內容。

[0137] 對於惡意檔案提供裝置160及運算裝置111之間曾發生的1項裝置互動事件，信息標註模塊340可將描述信息971顯示在相應的關係線951的上方做為摘要描述，且描述信息971的內容是與前述裝置互動事件相對應的精簡文字敘述「Network: m.exe」。對於運算裝置111及運算裝置112之間曾發生的2項裝置互動事件，信息標註模塊340可將描述信息972與973分別顯示在相應的關係線952與953的上方做為摘要描述，且描述信息972與973的內容分別是與前述2項裝置互動事件相對應的精簡文字敘述「Logon: administrator」與「File Accessed: m.exe」。對於運算裝置112及運算裝置113之間曾發生的1項裝置互動事件，信息標註模塊340可將描述信息974顯示在相應的關係線954的上方做為摘要描述，且描述信息974的內容是與前述裝置互動事件相對應的精簡文字敘述「Logon: candy」。對於運算裝置111及運算裝置113之間曾發生的1項裝置互動事件，信息標註模塊340可將描述信息975顯示在相應的關係線955的上方做為摘要描述，且描述信息975的內容是與前述裝置互動事件相對應的精簡文字敘述「Network: p.exe」。此外，對於運算裝置113及運算裝置114之間曾發生的1項裝置互動事件，信息標註模塊340可將描述信息976顯示在相應的關係線956的上方做為摘要描述，且描述信息976的內容是與前述裝置互動事件相對應的精簡文字敘述「Logon: admin」。如此一來，資安分析人員便能夠依據個別關係線上方的摘要描述，明白個別關係線所代表的裝置互動事件的概要內容。

[0138] 與前述圖7與圖8的實施例相較，圖9中的可疑事件時序圖550不只呈現出標的網路系統102中涉及可疑事件的運算裝置，還同時呈現出涉及可疑事件的外部裝置實體（例如，前述的惡意檔案提供裝置160），以及標的網路系統102與外部裝置實體之間的可疑互動事件的簡要內容、發生次數、以及與其他可疑事件在時序上的相關性。

[0139] 很明顯地，可疑事件時序圖產生程式150所產生的可疑事件時序圖550，能夠將標的網路系統102的內部裝置之間的可疑互動關係、標的網路系統102與外部裝置之間的可疑互動關係、以及其他多種維度的參考資訊，以直觀的視覺化方式呈現給資安分析人員。這樣的方式不僅能大幅減少資安分析人員需要關注的資料量，還有助進一步提升資安分析人員診斷標的網路系統102是否已受到駭客入侵的效率與準確度。

[0140] 前述有關圖7與圖8中的其他相關優點等說明，亦適用於圖9的實施例。為簡

潔起見，在此不重複敘述。

[0141] 在前述圖7至圖9的實施例中，由可疑事件時序圖產生程式150的事件分析模塊310所產生的個別副視覺物件，代表有足夠確切的數位證據能夠證明的一項裝置內部事件。由事件分析模塊310所產生的個別關係線，則代表有足夠確切的數位證據能夠證明的一項裝置互動事件。

[0142] 有時候，駭客攻擊行動所衍生的某些數位證據，可能會讓事件分析模塊310所界定出來的某些裝置內部事件與某些裝置互動事件之間，存在一定程度以上的關聯性。

[0143] 然而，有些較縝密的駭客攻擊行動可能會清除掉攻擊過程中產生的部分數位證據。另外，安裝在個別運算裝置中的裝置活動回報程式120，在偵測及搜集所屬運算裝置的可疑活動記錄以及時間戳記的過程中，可能會因裝置進入省電模式、睡眠模式、系統資源限制、意外的電力中斷等各種不同的原因而有所遺漏。在前述的情況下，有可能導致事件分析模塊310無法根據取得的數位證據直接確定是否發生某些可疑事件。

[0144] 為了因應前述的問題，可疑事件時序圖產生程式150可在收集到的數位證據不夠完整的情況下，對已界定出來的可疑事件及相關時間記錄進行交叉比對分析，以進一步研判在標的網路系統102中是否還存在其他有可能發生的可疑事件。如果有，則可疑事件時序圖產生程式150可將推論出來的可疑事件（*speculated suspicious event*）的相關資訊，一併呈現在可疑事件時序圖550中供資安分析人員做為判斷時的輔助資料。

[0145] 以下將搭配圖10來進一步說明可疑事件時序圖產生程式150如何判斷是否存在遺漏的可疑事件。圖10為本發明產生可疑事件時序圖550中的推論關係線的方法的一實施例簡化後的流程圖。

[0146] 在運作時，倘若事件分析模塊310利用控制電路149界定出一第一參與裝置曾發生一第一裝置內部事件、且一第二參與裝置曾發生一第二裝置內部事件，但無法根據現有的數位證據直接確定第一參與裝置與第二參與裝置之間是否曾發生一預定類型的裝置互動事件，則可疑事件時序圖產生程式150可進行圖10中的運作以做進一步的交叉比對，以判斷在第一參與裝置與第二參與裝置之間是否曾發生預定類型的裝置互動事件。

[0147] 在流程1002中，事件分析模塊310會計算第一裝置內部事件所對應的第一時間記錄與第二裝置內部事件所對應的第二時間記錄兩者間的時間差。

[0148] 為了便於理解，在此用前述圖9中的可疑事件時序圖550為例來加以說明。從

前述圖9的內容描述可知，事件分析模塊310在前述的流程602中會界定出運算裝置111曾發生2項裝置內部事件，亦即，「針對檔案m.exe的檔案產生事件」與「針對檔案m.exe的檔案執行事件」；運算裝置112曾發生1項裝置內部事件，亦即，「針對檔案m.exe的檔案產生事件」；且運算裝置111與運算裝置112之間曾發生2項裝置互動事件，亦即，「關於用戶名稱administrator的遠端登入事件」與「針對檔案m.exe的遠端存取檔案事件」。

[0149] 然而，在圖9的可疑事件時序圖550中，並未顯示任何用於代表運算裝置111與運算裝置112之間曾發生「針對檔案m.exe的檔案移動事件」的關係線。這表示事件分析模塊310無法根據已取得的數位證據，直接確定運算裝置111與運算裝置112之間是否曾發生「針對檔案m.exe的檔案移動事件」。在此情況下，可疑事件時序圖產生程式150可進行圖10中的運作，以判斷在運算裝置111與運算裝置112之間是否曾發生「針對檔案m.exe的檔案移動事件」。

[0150] 例如，事件分析模塊310在流程1002中，可選擇運算裝置111中的「針對檔案m.exe的檔案產生事件」做為前述的第一裝置內部事件，並選擇運算裝置112中的「針對檔案m.exe的檔案產生事件」做為前述的第二裝置內部事件，然後計算這兩個裝置內部事件之間的時間差。由前述說明可知，事件分析模塊310會在前面的流程602中，界定出與個別可疑事件相對應的時間記錄。因此，事件分析模塊310只需將前述兩個「針對檔案m.exe的檔案產生事件」所對應的時間記錄的數值相減，即可算出兩個裝置內部事件之間的時間差。

[0151] 在流程1004中，事件分析模塊310會比較時間差與一預定臨界值。實作上，事件分析模塊310可將前述的預定臨界值設置成合理的時間長度，例如，5分鐘、3分鐘、2分鐘、或1分鐘等等。

[0152] 倘若前述兩個裝置內部事件之間的時間差大於或等於預定臨界值，則事件分析模塊310可判定這兩個裝置內部事件屬於獨立事件，彼此間沒有特別明顯的關聯性。因此，事件分析模塊310可以不需要對前述兩個裝置內部事件做其他的交叉比對。

[0153] 反之，倘若前述兩個裝置內部事件之間的時間差小於預定臨界值，代表這兩個裝置內部事件之間存在密切的時序關聯性。因此，事件分析模塊310可判定這兩個裝置內部事件屬於關聯事件，並可推論在運算裝置111與運算裝置112之間很可能曾發生一預定類型的裝置互動事件。在本實施例中，前述預定類型的裝置互動事件指的是「針對檔案m.exe的檔案移動事件」。在此情況下，事件分析模塊310會進行流程1006。

[0154] 在流程1006中，事件分析模塊310會產生與前述的預定類型的裝置互動事件相應的一推論關係線產生要求（speculated relation line generation request），並將推論關係線產生要求傳送給視覺物件產生模塊320。

[0155] 在流程1008中，視覺物件產生模塊320會接收事件分析模塊310所產生的推論關係線產生要求。

[0156] 在流程1010中，視覺物件產生模塊320會依據該推論關係線產生要求，建立視覺表述與其他關係線相異的一條推論關係線。實作上，視覺物件產生模塊320可用直線、折線、略微彎曲的線條、波浪線、或其他類似功能的線條來做為推論關係線的視覺表述。

[0157] 例如，在圖11的實施例中，視覺物件產生模塊320會依據該推論關係線產生要求，在可疑事件時序圖550中建立一條推論關係線1157，並以水平虛線做為推論關係線1157的視覺表述方式，以凸顯出與其他關係線951～956的區別。如此一來，資安分析人員便能夠從推論關係線1157的視覺表述方式，明白推論關係線1157所代表的裝置互動事件屬於推論性質，並沒有足夠確切的數位證據能夠直接證明。

[0158] 在流程1012中，視覺物件產生模塊320可依據前述的第一裝置內部事件與第二裝置內部事件兩者的時間記錄，在推論關係線1157上設置一相應的指向符號1167，以指示該預定類型的裝置互動事件的方向性。實作上，視覺物件產生模塊320可用各種箭頭、手指圖案、或其他可表達方向性的圖案，來呈現指向符號1167。

[0159] 例如，在圖11中，視覺物件產生模塊320是以箭頭做為指向符號1167的視覺表述方式，並將指向符號1167設置在推論關係線1157上，以表達前述預定類型的裝置互動事件的方向性。

[0160] 在流程1014中，排列模塊330會將對應於前述預定類型的裝置互動事件的推論關係線1157，按照時間順序排列在相應的兩個垂直圖案之間，並將推論關係線1157的兩端分別接觸相關的兩個垂直圖案。

[0161] 例如，在圖11中，排列模塊330可將推論關係線1157按照前述預定類型的裝置互動事件的可能發生時間，排列在主視覺物件903所對應的垂直圖案933以及主視覺物件905所對應的垂直圖案935之間的適當位置，並將推論關係線1157的兩端，設置成分別接觸垂直圖案933與垂直圖案935。

[0162] 在流程1016中，信息標註模塊340可顯示關於預定的裝置互動事件的摘要描述。實作上，信息標註模塊340可將能夠讓資安分析人員理解推論關係線1157所對應的

裝置互動事件的概要內容的信息，例如，事件名稱、代表符號、代表圖像、或精簡文字敘述等等，顯示在推論關係線1157上或是推論關係線1157的附近，以做為相應的裝置互動事件的摘要描述。

[0163] 例如，在前述的運作中，事件分析模塊310已推論出在運算裝置111與運算裝置112之間很可能曾發生「針對檔案m.exe的檔案移動事件」。因此，如圖11所示，對於前述推論出來的裝置互動事件，信息標註模塊340可將1個描述信息1177顯示在推論關係線1157的上方，且描述信息1177的內容是與前述推論出來的裝置互動事件相對應的精簡文字敘述「File Movement: m.exe」。如此一來，資安分析人員便能夠依據推論關係線1157上方的摘要描述，明白可疑事件時序圖產生程式150所推論出來的裝置互動事件的概要內容，亦即，在運算裝置111與運算裝置112之間很可能曾發生一預定類型的裝置互動事件（在本實施例中指的是「針對檔案m.exe的檔案移動事件」）。

[0164] 與前述圖8的實施例類似，信息標註模塊340還可將副視覺物件941~945所對應的裝置內部事件的時間記錄，分別顯示在個別副視覺物件上或是個別副視覺物件附近。另一方面，信息標註模塊340也可將關係線951~956所對應的裝置互動事件的時間記錄，顯示在個別關係線上或是個別關係線的附近。

[0165] 例如，在圖12所繪示的可疑事件時序圖550的局部內容中，信息標註模塊340可在個別副視覺物件中，標示該副視覺物件所對應的裝置內部事件的時間記錄，並可在個別關係線的上方，標示該關係線所對應的裝置互動事件的時間記錄。由前述說明可知，信息標註模塊340顯示在可疑事件時序圖550中的時間記錄，可以是相應可疑事件的起始時間、或是結束時間。

[0166] 另外，信息標註模塊340也可將推論關係線1157所對應的裝置互動事件的時間記錄，顯示在推論關係線1157上或是推論關係線1157的附近。

[0167] 例如，在圖12的實施例中，信息標註模塊340可在推論關係線1157的上方，標示前述推論出來的裝置互動事件的可能時間記錄（亦即，推論的時間記錄）。同樣地，信息標註模塊340為推論關係線1157所標示的時間記錄，可以是前述推論出來的裝置互動事件的可能的起始時間、或是可能的結束時間。

[0168] 如此一來，資安分析人員便能夠依據圖12中所顯示的時間記錄，迅速辨別個別裝置內部事件或裝置互動事件的時間信息，並用來做為判斷依據，以進一步提升判斷標的網路系統102是否已受到駭客入侵的精確度。另外，資安分析人員也能夠依據推論關係線1157的時間記錄，迅速辨別前述推論出來的裝置互動事件的可能時間，並參

考其他資料來研判該裝置互動事件的真實性。這樣的方式不僅有助於提升資安分析人員的判斷效率，還能降低資安分析人員發生誤判的可能性。

[0169] 請注意，在前述的流程1002中，事件分析模塊310所選擇的第一裝置內部事件與第二裝置內部事件，分別是運算裝置111中的「針對檔案m.exe的檔案產生事件」與運算裝置112中的「針對檔案m.exe的檔案產生事件」，所以第一裝置內部事件與第二裝置內部事件兩者是相同類型的裝置內部事件（在本例中，兩者都是針對同一檔案的檔案產生事件）。但這只是一示範性的實施例，並非侷限本發明的實際實施方式。

[0170] 例如，在前述的流程1002中，事件分析模塊310亦可改選擇運算裝置111中的「針對檔案m.exe的檔案執行事件」做為前述的第一裝置內部事件，然後計算其與運算裝置112中的「針對檔案m.exe的檔案產生事件」之間的時間差。換言之，事件分析模塊310在前述流程1002中計算時間差的對象，並不侷限於相同類型的裝置內部事件。

[0171] 另外，可疑事件時序圖產生程式150可在產生前述可疑事件時序圖550過程中的任何時間，進行前述圖10的運作。

[0172] 前述有關圖10中的其他視覺元素的產生方式、代表的物理意義、以及相關優點等說明，亦適用於圖11與圖12的實施例。為簡潔起見，在此不重複敘述。

[0173] 請注意，前述圖6與圖10中的流程執行順序只是一示範性的實施例，並非侷限本發明的實際實施方式。例如，在圖6中，視覺物件產生模塊320所進行的流程604、612、616、與622之間，並沒有執行順序上的限制而可彈性調整順序、或同時進行。排列模塊330所進行的流程606、610、614、618、與626之間，也沒有執行順序上的限制而可彈性調整順序、或同時進行。信息標註模塊340所進行的流程608、620、與628之間，也沒有執行順序上的限制而可彈性調整順序、或同時進行。

[0174] 另外，信息標註模塊340所進行的流程，也可調整到排列模塊330所進行的流程之前進行。再者，流程624也可調整到流程626或流程628之後進行。

[0175] 又例如，在圖10中，流程1014也可調整到流程1010與1012之間進行。流程1012也可調整到流程1016之後進行。

[0176] 在前述的實施例中，與多個可疑活動紀錄相對應的多個屬性標籤，是由安裝在個別運算裝置中的裝置活動回報程式120在流程404中進行設定，但只是一示範性的實施例，並非侷限本發明的實際實施方式。

[0177] 實作上，流程404的運作亦可改由活動記錄匯集裝置130來進行。亦即，在前述圖4的運作中，裝置活動回報程式120只需進行流程402與406，且裝置活動回報程式

120在流程406中只需傳送可疑活動紀錄及相應的時間戳記給活動記錄匯集裝置130即可。等到活動記錄匯集裝置130接收到可疑活動紀錄及相應的時間戳記後，再由活動記錄匯集裝置130進行流程404，以建立分別對應於多個可疑活動紀錄的多個屬性標籤。

[0178] 在某些實施例中，可將可疑事件時序圖550中的推論關係線（例如，圖11與圖12中的推論關係線1157）的視覺表述方式，改成其他形式，或是改成與可疑事件時序圖550中的其他關係線（例如，圖8中的關係線751～756或是圖11中的關係線951～956）相同。

[0179] 另外，在某些實施例中，也可將位於可疑事件時序圖550的下部區域720中的主視覺物件省略。

[0180] 在標的網路系統102中的運算裝置數量不多、或是標的網路系統102的對外網路頻寬非常充足的應用環境中，也可將前述網路安全漏洞診斷系統100中的活動記錄匯集裝置130省略。

[0181] 例如，圖13為本發明另一實施例的網路安全漏洞診斷系統100簡化後的功能方塊圖。在圖13的實施例中，省略了前述圖1架構中的活動記錄匯集裝置130，而原先由活動記錄匯集裝置130負責進行的流程408～412的運作，則可改由個別的裝置活動回報程式120來進行。換言之，在圖13的網路安全漏洞診斷系統100中，安裝在個別運算裝置中的裝置活動回報程式120，會對多個可疑活動紀錄、多個時間戳記、與多個屬性標籤進行處理，以產生回傳資料，並將回傳資料透過合適的網路（例如，網際網路）傳送給可疑事件研判裝置140。

[0182] 前述有關圖1中的其他元件的連接關係、實施方式、運作方式、以及相關優點等說明，亦適用於圖13的實施例。為簡潔起見，在此不重複敘述。

[0183] Certain terms are used throughout the description and the claims to refer to particular components. One skilled in the art appreciates that a component may be referred to as different names. This disclosure does not intend to distinguish between components that differ in name but not in function. In the description and in the claims, the term “comprise” is used in an open-ended fashion, and thus should be interpreted to mean “include, but not limited to.” The term “couple” is intended to compass any indirect or direct connection. Accordingly, if this disclosure mentioned that a first device is coupled with a second device, it means that the first device may be directly or indirectly connected to the second device through electrical connections, wireless communications, optical communications, or other signal connections with/without other intermediate devices or connection means.

[0184] The term “and/or” may comprise any and all combinations of one or more of the associated listed items. In addition, the singular forms “a,” “an,” and “the” herein are intended to comprise the plural forms as well, unless the context clearly indicates otherwise.

[0185] Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention indicated by the following claims.

CLAIMS

What is claimed is:

1. 一種可疑事件研判裝置（140），用於診斷一標的網路系統（102）是否已受到駭客入侵，該可疑事件研判裝置（140）包含：

一顯示裝置（141）；

一通信電路（143），設置成透過網際網路接收與該標的網路系統（102）中的多個運算裝置（111～115）有關的多個可疑活動記錄、以及相應的多個時間戳記與多個屬性標籤；

一儲存電路（147），設置成儲存一可疑事件時序圖產生程式（150）；以及

一控制電路（149），耦接於該顯示裝置（141）、該通信電路（143）、與該儲存電路（147），並設置成執行該可疑事件時序圖產生程式（150），以依據該多個可疑活動記錄、該多個時間戳記、與該多個屬性標籤進行一可疑事件時序圖產生運作，以界定出與該標的網路系統（102）有關的多個可疑事件，界定出分別對應於該多個可疑事件的多個時間記錄，以及依據該多個可疑事件與該多個時間記錄，產生並顯示與該多個可疑事件相應的一可疑事件時序圖（550）。

2. 如請求項 1 所述的可疑事件研判裝置（140），其中，該多個可疑事件包含有多個裝置內部事件以及多個裝置互動事件，該可疑事件時序圖產生運作還包含：

建立分別與該多個可疑事件所涉及的多個參與裝置相對應的多個主視覺物件（701～705；901～909），其中，該多個主視覺物件（701～705；901～909）中至少有一部分是對應於該標的網路系統（102）中的運算裝置；

將該多個主視覺物件（701～705；901～909）水平排列在該可疑事件時序圖（550）的一上部區域（710）中；

建立分別與該多個主視覺物件（701～705；901～909）相對應的多個垂直圖案（731～735；931～939）；

將該多個垂直圖案（731～735；931～939）分別排列在該多個主視覺物件（701～705；901～909）的下方；

建立分別與該多個裝置內部事件相對應的多個副視覺物件（741～746；941～946）；

將個別參與裝置所對應的一或多個副視覺物件，按照相應的裝置內部事件的時間順序，由上而下排列在一相應的主視覺物件下方的一垂直圖案上；
建立分別與該多個裝置互動事件相對應的多條關係線（751～756；951～956）；
將該多條關係線（751～756；951～956）按照時間順序由上而下排列，並將每條關係線的兩端分別接觸所涉及的兩個參與裝置所對應的兩個垂直圖案；
在每條關係線上，依據該條關係線所對應的一裝置互動事件的內容，設置一相應的指向符號（761～766、961～966），以指示該裝置互動事件的方向性；以及
顯示每條關係線所對應的裝置互動事件的摘要描述。

3. 如請求項 2 所述的可疑事件研判裝置（140），其中，該可疑事件時序圖產生運作還包含：

顯示每個主視覺物件所對應的參與裝置的摘要描述；以及
顯示每個副視覺物件所對應的裝置內部事件的摘要描述。

4. 如請求項 3 所述的可疑事件研判裝置（140），其中，該可疑事件時序圖產生運作還包含：

顯示每個副視覺物件所對應的裝置內部事件的相應時間記錄；以及
顯示每條關係線所對應的裝置互動事件的相應時間記錄。

5. 如請求項 2 所述的可疑事件研判裝置（140），其中，該可疑事件時序圖產生運作還包含：

將該多個主視覺物件（701～705；901～909）按照與在該上部區域（710）中相同的順序，重複顯示在該可疑事件時序圖（550）的一下部區域（720）中。

6. 如請求項 2 所述的可疑事件研判裝置（140），其中，該可疑事件時序圖（550）中包含有：與一第一參與裝置（111）相應的一第一主視覺物件（903）、與一第二參與裝置（112）相應的一第二主視覺物件（905）、與該第一主視覺物件（903）相應的一第一垂直圖案（933）、與該第二主視覺物件（905）相應的一第二垂直圖案（935）；
其中，當該可疑事件研判裝置（140）界定出該第一參與裝置（111）曾發生一第一裝置內部事件、且該第二參與裝置（112）曾發生一第二裝置內部事件、但無法

確定該第一參與裝置（111）與該第二參與裝置（112）之間是否曾發生一預定類型的裝置互動事件時，該可疑事件時序圖產生運作還包含：

計算該第一裝置內部事件所對應的第一時間記錄與該第二裝置內部事件所對應的第一時間記錄兩者間的一時間差；

比較該時間差與一預定臨界值；

倘若該時間差小於該預定臨界值，則建立與該預定類型的裝置互動事件相應的一條推論關係線（1157）；

將該條推論關係線（1157）的兩端分別接觸該第一垂直圖案（933）與該第二垂直圖案（935）；

依據該第一時間記錄與該第二時間記錄兩者的相對大小，在該條推論關係線（1157）上設置一相應的指向符號（1167），以指示該預定類型的裝置互動事件的方向性；

以及

顯示該預定類型的裝置互動事件的摘要描述。

7. 如請求項 6 所述的可疑事件研判裝置（140），其中，該第一裝置內部事件與該第二裝置內部事件兩者都是針對同一檔案的檔案產生事件。

8. 如請求項 2 所述的可疑事件研判裝置（140），其中，當該多個參與裝置包含位於該標的網路系統（102）之外的一或多個惡意檔案提供裝置（160）時，該多個主視覺物件（701～705；901～909）中至少有一部分是對應於該一或多個惡意檔案提供裝置（160）。

9. 一種電腦程式產品（150），儲存在一可疑事件研判裝置（140）的一儲存電路（147）中，允許該可疑事件研判裝置（140）進行一可疑事件時序圖產生運作，該可疑事件時序圖產生運作包含：

依據與一標的網路系統（102）中的多個運算裝置（111～115）有關的多個可疑活動記錄、以及相應的多個時間戳記與多個屬性標籤，界定出與該標的網路系統（102）有關的多個可疑事件；

界定出分別對應於該多個可疑事件的多個時間記錄；以及

依據該多個可疑事件與該多個時間記錄，產生並顯示與該多個可疑事件相應的一可疑事件時序圖（550）。

10. 如請求項 9 所述的電腦程式產品（150），其中，該多個可疑事件包含有多個裝置內部事件以及多個裝置互動事件，該可疑事件時序圖產生運作還包含：

建立分別與該多個可疑事件所涉及的多個參與裝置相對應的多個主視覺物件（701～705；901～909），其中，該多個主視覺物件（701～705；901～909）中至少有一部分是對應於該標的網路系統（102）中的運算裝置；

將該多個主視覺物件（701～705；901～909）水平排列在該可疑事件時序圖（550）的一上部區域（710）中；

建立分別與該多個主視覺物件（701～705；901～909）相對應的多個垂直圖案（731～735；931～939）；

將該多個垂直圖案（731～735；931～939）分別排列在該多個主視覺物件（701～705；901～909）的下方；

建立分別與該多個裝置內部事件相對應的多個副視覺物件（741～746；941～946）；

將個別參與裝置所對應的一或多個副視覺物件，按照相應的裝置內部事件的時間順序，由上而下排列在一相應的主視覺物件下方的一垂直圖案上；

建立分別與該多個裝置互動事件相對應的多條關係線（751～756；951～956）；

將該多條關係線（751～756；951～956）按照時間順序由上而下排列，並將每條關係線的兩端分別接觸所涉及的兩個參與裝置所對應的兩個垂直圖案；

在每條關係線上，依據該條關係線所對應的一裝置互動事件的內容，設置一相應的指向符號（761～766、961～966），以指示該裝置互動事件的方向性；以及顯示每條關係線所對應的裝置互動事件的摘要描述。

11. 如請求項 10 所述的電腦程式產品（150），其中，該可疑事件時序圖產生運作還包含：

顯示每個主視覺物件所對應的參與裝置的摘要描述；以及

顯示每個副視覺物件所對應的裝置內部事件的摘要描述。

12. 如請求項 11 所述的電腦程式產品（150），其中，該可疑事件時序圖產生運作還包含：

顯示每個副視覺物件所對應的裝置內部事件的相應時間記錄；以及

顯示每條關係線所對應的裝置互動事件的相應時間記錄。

13. 如請求項 10 所述的電腦程式產品（150），其中，該可疑事件時序圖產生運作還包含：

將該多個主視覺物件（701~705；901~909）按照與在該上部區域（710）中相同的順序，重複顯示在該可疑事件時序圖（550）的一下部區域（720）中。

14. 如請求項 10 所述的電腦程式產品（150），其中，該可疑事件時序圖（550）中包含有：與一第一參與裝置（111）相應的一第一主視覺物件（903）、與一第二參與裝置（112）相應的一第二主視覺物件（905）、與該第一主視覺物件（903）相應的一第一垂直圖案（933）、與該第二主視覺物件（905）相應的一第二垂直圖案（935）；

其中，當該可疑事件研判裝置（140）界定出該第一參與裝置（111）曾發生一第一裝置內部事件、且該第二參與裝置（112）曾發生一第二裝置內部事件、但無法確定該第一參與裝置（111）與該第二參與裝置（112）之間是否曾發生一預定類型的裝置互動事件時，該可疑事件時序圖產生運作還包含：

計算該第一裝置內部事件所對應的一第一時間記錄與該第二裝置內部事件所對應的一第二時間記錄兩者間的一時間差；

比較該時間差與一預定臨界值；

倘若該時間差小於該預定臨界值，則建立與該預定類型的裝置互動事件相應的一條推論關係線（1157）；

將該條推論關係線（1157）的兩端分別接觸該第一垂直圖案（933）與該第二垂直圖案（935）；

依據該第一時間記錄與該第二時間記錄兩者的相對大小，在該條推論關係線（1157）上設置一相應的指向符號（1167），以指示該預定類型的裝置互動事件的方向性；
以及

顯示該預定類型的裝置互動事件的摘要描述。

15. 如請求項 14 所述的電腦程式產品（150），其中，該第一裝置內部事件與該第二裝置內部事件兩者都是針對同一檔案的檔案產生事件。

16. 如請求項 10 所述的電腦程式產品（150），其中，當該多個參與裝置包含位於該標的網路系統（102）之外的一或多個惡意檔案提供裝置（160）時，該多個主視覺物件（701～705；901～909）中至少有一部分是對應於該一或多個惡意檔案提供裝置（160）。