

MULTI-FRAME CYBER SECURITY ANALYSIS DEVICE AND RELATED COMPUTER PROGRAM PRODUCT FOR GENERATING MULTIPLE ASSOCIATED DATA FRAMES

BACKGROUND

[0001] 本發明涉及駭客入侵活動檢測技術，尤指一種用於產生多個連動式資料圖框的多圖框網路安全分析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，反覆地對受檢環境中大量的電腦活動歷史紀錄進行判讀、過濾、與交叉比對，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，而且資安分析人員在對為數眾多的電腦活動歷史紀錄重複過濾時，需要反覆利用不同的檢索條件來過濾資料，並自行記錄每次過濾後的結果來進行交叉比對。因此，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] 本說明書提供一種多圖框網路安全分析裝置的實施例，用於診斷一標的網路系統是否已受到駭客入侵，該多圖框網路安全分析裝置包含：一顯示裝置；一輸入裝置，設置成接收一使用者下達的操作指令；一非揮發性儲存電路，設置成儲存一資料庫與一連動式資料圖框產生程式，其中，該資料庫內儲存有與一標的網路系統中的多

個運算裝置有關的多種裝置活動記錄；以及一控制電路，耦接於該顯示裝置、該輸入裝置、與該非揮發性儲存電路，並設置成執行該連動式資料圖框產生程式，以依據該資料庫中所儲存的該多種裝置活動記錄進行一資料圖框產生運作，以產生與該標的網路系統有關的多個連動式資料圖框，並同時顯示該多個連動式資料圖框的內容；其中，該多個連動式資料圖框包含一導引圖框、一第一全域資料圖框、以及一區域資料圖框。

[0006] 本說明書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多圖框網路安全分析裝置的一非揮發性儲存電路中，允許該多圖框網路安全分析裝置依據一資料庫中所儲存的多種裝置活動記錄進行一資料圖框產生運作，以產生與一標的網路系統有關的多個連動式資料圖框，並同時顯示該多個連動式資料圖框的內容，其中，該多個連動式資料圖框包含一導引圖框、一第一全域資料圖框、以及一區域資料圖框。

[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中的多圖框網路安全分析裝置內的連動式資料圖框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多圖框畫面的一實施例簡化後的示意圖。

[0013] 圖6與圖7為本發明一實施例的產生多個連動式資料圖框的方法簡化後的流程圖。

[0014] 圖8至圖12為本發明不同實施例的多圖框畫面的局部內容簡化後的示意圖。

[0015] 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

[0016] 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。

[0017] 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。

[0018] 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。

[0019] 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）。

[0020] 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有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。

[0021] 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、以及一多圖框網路安全分析裝置140。

[0022] 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）。

[0023] 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）傳送給多圖框網路安全分析裝置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。

[0024] 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。

[0025] 如圖1所示，多圖框網路安全分析裝置140包含一顯示裝置141、一通信電路143、一輸入裝置145、一非揮發性儲存電路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設置成允許多圖框網路安全分析裝置140的使用者（例如，資安分析人員）對多圖框網路安全分析裝置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設置成儲存一資料庫152與一連動式資料圖框產生程式154，其中，資料庫152用來儲存與前述標的網路系統102中的多個運算裝置111~115有關的多種裝置活動記錄。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還設置成執行連動式資料圖框產生程式154，以進行一資料圖框產生運作（**data frame generating operation**）。在資料圖框產生運作中，控制電路149會依據資料庫152中所儲存的多種裝置活動記錄，產生與標的網路系統102有關的多個連動式資料圖框（**multiple associated data frames**），然後利用顯示裝置141同時顯示該多個連動式資料圖框的內容。

[0026] 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。

[0027] 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。資料庫152可以用各種關聯式資料庫來實現，也可以用各種非關聯式資料庫來實現。資料庫152跟連動式資料圖框產生程式154可以儲存在儲存電路147中的相同儲存介質內，也可以分別儲存在儲存電路147中的不同儲存介質內。顯示裝置141可用能夠呈現影像的單一螢幕或單一投影裝置來實現，也可以用多個螢幕的組合、或是多個投影裝置的組合來實現。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。

[0028] 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。

[0029] 另外，前述儲存在多圖框網路安全分析裝置140的儲存電路147中的連動式資料圖框產生程式154，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為多圖框網路安全分析裝置140內的連動式資料圖框產生程式154的一實施例簡化後的功能模塊示意圖。在圖3的實施例中，連動式資料圖框產生程式154包含一存取模塊310、一導引圖框產生模塊320、一全域資料圖框產生模塊330、一區域資料圖框產生模塊340、以及一圖框關聯控制模塊350。

[0030] 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。

[0031] 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「多圖框網路安全分析裝置」欄位中的部分，則是由多圖框網路安全分析裝置140所進行的流程。

[0032] 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。

[0033] 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。

[0034] 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。

[0035] 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。

[0036] 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。

[0037] 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。

[0038] 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。

[0039] 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以及多圖框網路安全分析裝置140進行處理或分析的資料量。

[0040] 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。

[0041] 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。

[0042] 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。

[0043] 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。

[0044] 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。

[0045] 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」。

[0046] 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」。

[0047] 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」。

[0048] 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**」。

[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**」。

[0050] 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**」。

[0051] 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**」。

[0052] 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**」。

[0053] 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**」。

[0054] 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**」。

[0055] 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。

[0056] 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。

[0057] 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。

[0058] 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。

[0059] 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。

[0060] 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。

[0061] 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。

[0062] 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）傳送給多圖框網路安全分析裝置140。

[0063] 在流程414中，多圖框網路安全分析裝置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。

[0064] 在流程416中，多圖框網路安全分析裝置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。

[0065] 在流程418中，控制電路149會執行儲存電路147中的連動式資料圖框產生程式154，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，進行一資料圖框產生運作，以產生並顯示同時包含有多個連動式資料圖框的一多圖框畫面。

[0066] 請參考圖5，其所繪示為多圖框網路安全分析裝置140透過顯示裝置141所顯示的多圖框畫面500的一實施例簡化後的示意圖。

[0067] 如圖5所示，顯示裝置141所顯示的多圖框畫面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）。多圖框畫面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。前述多個資料圖框510～540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。

[0068] 在圖5的實施例中，資料圖框510～530用於呈現多圖框網路安全分析裝置140執行連動式資料圖框產生程式154後所產生的資料內容，且資料圖框510～530分屬三種

不同的圖框類型。具體而言，資料圖框510是用來顯示多個過濾條件的連動式資料圖框，以下稱為導引圖框510；資料圖框520是用來顯示與前述標的網路系統102中的局部裝置或全部裝置有關的特定全域屬性資料的連動式資料圖框，以下稱為第一全域資料圖框520；而資料圖框530則是用來顯示與前述多個運算裝置111～115的其中之一相對應的特定資料群組的連動式資料圖框，以下稱為區域資料圖框530。

[0069] 另外，資料圖框540則是屬於其他類型的圖框，其所顯示的內容並不會與前述的導引圖框510、第一全域資料圖框520、以及區域資料圖框530發生產生連動變化。

[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，以增加或減少各類型資料圖框的數量、調整個別資料圖框的大小或位置、選取個別資料圖框中的物件、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、並傳送給多圖框網路安全分析裝置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與多圖框網路安全分析裝置140之間的資料傳輸安全性。

[0072] 在連動式資料圖框產生程式154中，存取模塊310是其他模塊要存取資料庫152時的媒介。當其他模塊要存取資料庫152中所儲存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時，可指示存取模塊310利用控制電路149存取資料庫152中的資料。

[0073] 另外，存取模塊310也可依據資料庫152中的資料，界定出與標的網路系統102有關的多個可疑事件（suspicious events）、以及分別對應於多個可疑事件的多個時間記錄（time records）。

[0074] 對於存取模塊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）。存取模塊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。

[0075] 例如，存取模塊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，存取模塊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。

[0076] 再者，存取模塊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。

[0077] 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**）。

[0078] 存取模塊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，存取模塊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。

[0079] 倘若存取模塊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多個連動式資料圖框510～530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。

[0080] 為了降低這方面的問題，存取模塊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。

[0081] 在運作時，存取模塊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多個連動式資料圖框510～530中的裝置內部事件的類型、以及裝置互動事件的類型。

[0082] 例如，存取模塊310可限制最多只有8種類型的裝置內部事件能夠顯示在多個連動式資料圖框510～530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，存取模塊310可限制最多只有6種類型的裝置互動事件能夠顯示在多個連動式資料圖框510～530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。

[0083] 在另一實施例中，存取模塊310可限制最多只有3種類型的裝置內部事件能夠顯示在多個連動式資料圖框510～530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，存取模塊310可限制最多只有4種類型的裝置互動事件能夠顯示在多個連動式資料圖框510～530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。

[0084] 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，則取決於存取模塊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。

[0085] 在實際應用中，存取模塊310也可按照多個連動式資料圖框510～530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。

[0086] 存取模塊310可將界定出來的可疑事件與對應的時間記錄儲存到資料庫152中，以做為其他模塊產生相關圖框時的參考依據之一。

[0087] 以下將搭配圖6至圖7來進一步說明多圖框網路安全分析裝置140進行資料圖框產生運作的方式。圖6與圖7為本發明一實施例的產生多個連動式資料圖框的方法簡化後的流程圖。在圖6與圖7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「導引圖框產生模塊」欄位中的部分，是由連動式資料圖框產生程式154中的導引圖框產生模塊320所進行的流程；標記在「全域資料圖框產生模塊」欄位中的部分，是由全域資料圖框產生模塊330所進行的流程；標記在「區域資料圖框產生模塊」欄位中的部分，則是由區域資料圖框產生模塊340所進行的流程；而標記在「圖框關聯控制模塊」欄位中的部分，則是由圖框關聯控制模塊350所進行的流程。

[0088] 在流程602中，導引圖框產生模塊320會產生分別與多個過濾條件相應的多個候選物件，使得不同的候選物件分別對應於不同的過濾條件。前述的多個過濾條件，是可用來對資料庫152中為數眾多的資料進行檢索、過濾、或分類的各種條件，例如，日期、時間範圍、關鍵字詞、裝置風險類型與等級、裝置群組、裝置所屬網路區段

（IP位址範圍）、裝置連線類型、裝置互動類型等等。

[0089] 實作上，導引圖框產生模塊320可用各種圖案、影像、或文字來呈現個別的候選物件，且不同的候選物件的視覺表述方式（visual representation）可彼此相同、也可彼此不同。

[0090] 例如，在圖5的實施例中，導引圖框產生模塊320是用可選擇的日期格（selectable date grid）來做為多個候選物件（例如，圖5中的示例性候選物件511、513、與515）的視覺表述方式。在此情況下，不同的候選物件分別代表不同的日期。例如，候選物件511對應於一第一日期、候選物件513對應於一第二日期、候選物件515則對應於一第三日期。

[0091] 在流程604中，導引圖框產生模塊320會建立包含前述多個候選物件的導引圖框510。實作上，導引圖框產生模塊320可將前述多個候選物件以各種合適的方式排列組合，以方便資安分析人員區別不同的候選物件。

[0092] 例如，在圖5的實施例中，導引圖框產生模塊320可將前述的多個候選物件排列成一日曆選單的形式，並設置為導引圖框510。

[0093] 在流程606中，全域資料圖框產生模塊330會依據資料庫152中的資料，產生與標的網路系統102中的局部裝置或全部裝置有關的多個全域屬性資料，使得不同的全域屬性資料分別對應於不同的過濾條件。實作上，全域資料圖框產生模塊330可將資料庫152中所儲存的各種資料，整理成與前述的多個過濾條件相對應的多個全域屬性資料，例如，標的網路系統102內的網路拓樸資料、所有運算裝置的連網流量排名、所有運算裝置的資料吞吐量排名、所有運算裝置曾連線的惡意網址、在標的網路系統102內發現的所有惡意程式列表、在標的網路系統102內發現的所有運算裝置中異常事件清單、在標的網路系統102內發現的所有運算裝置中異常執行指令歷史紀錄、標的網路系統102內的裝置活動關聯圖、標的網路系統102內的可疑事件時序圖、標的網路系統102內的運算裝置活動統計圖、標的網路系統102內的可疑事件統計圖等等。

[0094] 另外，導引圖框產生模塊320所設置的過濾條件與全域資料圖框產生模塊330所產生的全域屬性資料之間，有可能是一對一的對映關係，也有可能是一對多的對映關係。在一實施例中，全域資料圖框產生模塊330會針對每個過濾條件產生一個相應的全域屬性資料。在另一實施例中，全域資料圖框產生模塊330則會針對每個過濾條件產生兩個或兩個以上種類的全域屬性資料。全域資料圖框產生模塊330可將產生的多個全域屬性資料儲存到資料庫152中，以供後續的運作時段使用。

[0095] 例如，在圖5的實施例中，全域資料圖框產生模塊330可依據資料庫152中的資料，建立起與標的網路系統102中的局部裝置或全部裝置對應的多個裝置活動關聯圖，且前述的多個裝置活動關聯圖分別對應於不同日期。舉例而言，前述的多個裝置活動關聯圖可包含與導引圖框510中的候選物件511所代表的第一日期相對應的第一裝置活動關聯圖、與候選物件513所代表的第二日期相對應的第二裝置活動關聯圖、以及與候選物件515所代表的第三日期相對應的第三裝置活動關聯圖。

[0096] 在流程608中，全域資料圖框產生模塊330會選擇多個全域屬性資料的其中之一做為第一目標全域屬性資料。實作上，全域資料圖框產生模塊330可選擇與導引圖框510中被選取的候選物件所代表的過濾條件相對應的一個全域屬性資料來做為第一目標全域屬性資料。在導引圖框510中的所有候選物件都沒有被選取的情況下，全域資料圖框產生模塊330可選擇與導引圖框510呈現的過濾條件類型相對應的一個預定的全域屬性資料來做為第一目標全域屬性資料。

[0097] 例如，假設此時導引圖框510中被選取的候選物件是候選物件511，則全域資料圖框產生模塊330可選擇候選物件511所代表的第一日期所對應的第一裝置活動關聯圖，來做為第一目標全域屬性資料。

[0098] 在流程610中，全域資料圖框產生模塊330會建立包含第一目標全域屬性資料的第一全域資料圖框520。實作上，全域資料圖框產生模塊330可單純將前述選取的第一目標全域屬性資料設置為第一全域資料圖框520。或者，全域資料圖框產生模塊330也可以將第一目標全域屬性資料跟其他的資料和/或選項一起組合，以形成第一全域資料圖框520。

[0099] 例如，在圖5的實施例中，全域資料圖框產生模塊330可將與第一日期相對應的第一裝置活動關聯圖設置為第一全域資料圖框520。

[0100] 在流程612中，全域資料圖框產生模塊330會在前述的第一目標全域屬性資料中，分別利用多個主視覺物件代表標的網路系統102中的局部裝置或全部裝置。實作上，全域資料圖框產生模塊330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可彼此相同、也可彼此不同。

[0101] 例如，在圖5的實施例中，全域資料圖框產生模塊330是用圓形圖案搭配簡要描述性文字來做為示例性的主視覺物件521、523、與525的視覺表述方式，並在第一全域資料圖框520所顯示的第一裝置活動關聯圖中，利用主視覺物件521、523、與525來代表標的網路系統102中的不同運算裝置。為了方便說明起見，以下假設主視覺物件

521、523、與525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。

[0102] 如圖5所示，全域資料圖框產生模塊330可根據第一裝置活動關聯圖的表達方式，將主視覺物件521、523、與525分別放置在第一全域資料圖框520中的適當位置。

[0103] 接著，連動式資料圖框產生程式154會進行圖7中的流程702。

[0104] 在流程702中，區域資料圖框產生模塊340會依據資料庫152中的資料，產生分別與標的網路系統102中的多個運算裝置111～115相對應的多個資料群組（data group）。實作上，區域資料圖框產生模塊340可從資料庫152找出與特定運算裝置有關的裝置特定資訊（device-specific information），以做為該特定運算裝置所對應的資料群組。前述與特定運算裝置有關的裝置特定資訊，可以是跟該特定運算裝置內部活動有關的區域屬性資料，例如，特定運算裝置內的可執行程式列表、特定運算裝置的內部程序執行主從關係圖、特定運算裝置的網路連線記錄（或相關統計結果）、特定運算裝置的內部歷史執行指令清單、特定運算裝置的內部異常事件清單、特定運算裝置的內部資安風險統計圖、特定運算裝置的內部異常日期統計圖、特定運算裝置的使用者帳戶基本資料、特定運算裝置的軟、硬體基本資料、特定運算裝置的內部特定檔案與其他類似檔案的關聯圖等等。

[0105] 例如，區域資料圖框產生模塊340可從資料庫152中搜尋與運算裝置111有關的裝置特定資訊，以產生對應於運算裝置111的一第一資料群組；可從資料庫152中搜尋與運算裝置112有關的裝置特定資訊，以產生對應於運算裝置112的一第二資料群組；並可從資料庫152中搜尋與運算裝置113有關的裝置特定資訊，以產生對應於運算裝置113的一第三資料群組。為了方便說明起見，以下假設前述的第一資料群組是運算裝置111的內部程式執行時序圖、第二資料群組是運算裝置112的內部程式執行時序圖、而第三資料群組則是運算裝置113的內部程式執行時序圖。

[0106] 在流程704中，區域資料圖框產生模塊340會選擇多個資料群組的其中之一做為一第一目標資料群組。實作上，區域資料圖框產生模塊340可選擇與第一全域資料圖框520中被選取的主視覺物件所代表的運算裝置相對應的一個資料群組來做為第一目標資料群組。在第一全域資料圖框520中的所有主視覺物件都沒有被選取的情況下，區域資料圖框產生模塊340可選擇與導引圖框510呈現的過濾條件類型相對應的一個預定的資料群組做為第一目標資料群組，或是可選擇與第一全域資料圖框520所顯示的全域屬性資料相應的一個預定的資料群組做為第一目標資料群組。

[0107] 例如，假設此時第一全域資料圖框520中被選取的主視覺物件是主視覺物件521，則區域資料圖框產生模塊340可選擇對應於運算裝置111的第一資料群組，來做為第一目標資料群組。

[0108] 在流程706中，區域資料圖框產生模塊340會建立包含第一目標資料群組的區域資料圖框530。實作上，區域資料圖框產生模塊340可單純將前述選取的第一目標資料群組設置為區域資料圖框530。或者，區域資料圖框產生模塊340也可以將第一目標資料群組跟其他的資料和/或選項一起組合，以形成區域資料圖框530。

[0109] 例如，在圖5的實施例中，區域資料圖框產生模塊340可將對應於運算裝置111的第一資料群組設置為區域資料圖框530。

[0110] 在流程708中，圖框關聯控制模塊350會控制顯示裝置141同時顯示前述的導引圖框510、第一全域資料圖框520、與區域資料圖框530，以形成如圖5所繪示的態樣。

[0111] 如此一來，資安分析人員便能從導引圖框510、第一全域資料圖框520、與區域資料圖框530的內容中，同時獲取與標的網路系統102有關的不同面向或是不同維度的資料，並可利用這些資料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。

[0112] 在資安分析人員進行判斷的過程中，可能需要修改過濾條件來交叉比對不同過濾條件下的結果。此時，資安分析人員可操作輸入裝置145以下達相關操作指令，以調整多圖框畫面500的內容。

[0113] 在資安分析人員操作多圖框網路安全分析裝置140的過程中，連動式資料圖框產生程式154會持續性地進行圖7中的流程710與流程712。

[0114] 在流程710中，圖框關聯控制模塊350會監測導引圖框510中被選取的候選物件是否改變。實作上，圖框關聯控制模塊350可根據資安分析人員對於輸入裝置145的操作，來判斷導引圖框510中被選取的候選物件是否改變。倘若圖框關聯控制模塊350判定導引圖框510中被選取的候選物件沒有發生改變，則會繼續進行流程710。反之，倘若圖框關聯控制模塊350判定導引圖框510中被選取的候選物件發生改變，則會進行流程714。

[0115] 在流程712中，圖框關聯控制模塊350會監測第一全域資料圖框520中被選取的主視覺物件是否改變。同樣地，圖框關聯控制模塊350可根據資安分析人員對於輸入裝置145的操作，來判斷第一全域資料圖框520中被選取的主視覺物件是否改變。倘若圖框關聯控制模塊350判定第一全域資料圖框520中被選取的主視覺物件沒有發生改變，

則會繼續進行流程712。反之，倘若圖框關聯控制模塊350判定第一全域資料圖框520中被選取的主視覺物件發生改變，則會進行流程716。

[0116] 在流程714中，圖框關聯控制模塊350會指示全域資料圖框產生模塊330更換第一全域資料圖框520中的全域屬性資料。實作上，圖框關聯控制模塊350可將導引圖框510中新選取（newly selected）的候選物件的物件識別資料、物件代碼、或相應的過濾條件的識別資料、相應的過濾條件的條件代碼等信息，通知全域資料圖框產生模塊330，使全域資料圖框產生模塊330得知導引圖框510中新選取的候選物件為何。

[0117] 在此情況下，全域資料圖框產生模塊330會進行圖6中的流程614，選擇與導引圖框510中新選取的候選物件相應的全域屬性資料做為前述的第一目標全域屬性資料。接著，如圖6所示，全域資料圖框產生模塊330會進行前述的流程610與612，以將第一全域資料圖框520的內容更換成與導引圖框510中新選取的候選物件相應的全域屬性資料。換言之，此時全域資料圖框產生模塊330會將第一全域資料圖框520的內容，更換成符合新選取的候選物件所對應的過濾條件的全域屬性資料。然後，圖框關聯控制模塊350會控制顯示裝置141顯示第一全域資料圖框520更新後的內容。

[0118] 在某些實施例中，當圖框關聯控制模塊350判定導引圖框510中被選取的候選物件發生改變時，圖框關聯控制模塊350並不會指示區域資料圖框產生模塊340更換區域資料圖框530當時所顯示的目標資料群組。亦即，圖框關聯控制模塊350不會要求區域資料圖框產生模塊340隨著導引圖框510中被選取的候選物件的改變，而連帶改變區域資料圖框530中的目標資料群組。

[0119] 在另一些實施例中，當圖框關聯控制模塊350判定導引圖框510中被選取的候選物件發生改變時，圖框關聯控制模塊350會指示區域資料圖框產生模塊340更換區域資料圖框530當時所顯示的目標資料群組。例如，圖框關聯控制模塊350可指示區域資料圖框產生模塊340將當時區域資料圖框530中所顯示的目標資料群組，更換成與新選取的候選物件所代表的過濾條件相對應的一預定資料群組。換言之，圖框關聯控制模塊350也可以要求區域資料圖框產生模塊340隨著導引圖框510中被選取的候選物件的改變，而連帶改變區域資料圖框530中的目標資料群組。

[0120] 在流程716中，圖框關聯控制模塊350會指示區域資料圖框產生模塊340更換區域資料圖框530中所顯示的目標資料群組。實作上，圖框關聯控制模塊350可將第一全域資料圖框520中新選取的主視覺物件的物件識別資料、物件代碼、或相應的運算裝置的識別資料、相應的運算裝置的硬體代碼等信息，通知區域資料圖框產生模塊340，

使區域資料圖框產生模塊340得知第一全域資料圖框520中新選取的主視覺物件為何。

[0121] 在此情況下，區域資料圖框產生模塊340會進行圖7中的流程718，選擇與第一全域資料圖框520中新選取的主視覺物件相應的區域屬性資料做為前述的目標資料群組。

[0122] 接著，如圖7所示，區域資料圖框產生模塊340會進行前述的流程706，以將區域資料圖框530的內容更換成與第一全域資料圖框520中新選取的主視覺物件相應的區域屬性資料。換言之，此時區域資料圖框產生模塊340會將區域資料圖框530的內容，更換成符合新選取的主視覺物件所對應的運算裝置的區域屬性資料。然後，圖框關聯控制模塊350會控制顯示裝置141顯示區域資料圖框530更新後的內容。

[0123] 然而，當圖框關聯控制模塊350判定第一全域資料圖框520中被選取的主視覺物件發生改變時，圖框關聯控制模塊350並不會指示導引圖框產生模塊320改變導引圖框510的內容。亦即，圖框關聯控制模塊350不會要求導引圖框產生模塊320隨著第一全域資料圖框520中被選取的主視覺物件的改變，而連帶改變導引圖框510中的多個候選物件的內容。

[0124] 例如，由前述說明可知，在圖5所繪示的多圖框畫面500中，導引圖框510中被選取的候選物件是候選物件511，而第一全域資料圖框520中所顯示的第一目標全域屬性資料，則是對應於候選物件511所代表的第一日期的第一裝置活動關聯圖。在此情況下，倘若使用者透過輸入裝置145選取導引圖框510中的候選物件513，則圖框關聯控制模塊350會進行流程714，以指示全域資料圖框產生模塊330更換第一全域資料圖框520中的全域屬性資料。

[0125] 接著，全域資料圖框產生模塊330會按照圖框關聯控制模塊350的指示，進行流程614，以選擇與新選取的候選物件513所代表的第二日期相對應的第二裝置活動關聯圖做為第一目標全域屬性資料，並將第一全域資料圖框520的內容更換成對應於前述第二日期的第二裝置活動關聯圖。圖框關聯控制模塊350則會進行流程708，以控制顯示裝置141顯示第一全域資料圖框520更新後的內容，使得多圖框畫面500的內容變成圖8所繪示的態樣。

[0126] 在圖8的實施例中，此時圖框關聯控制模塊350並不會指示區域資料圖框產生模塊340更換區域資料圖框530當時所顯示的目標資料群組，所以在圖8的多圖框畫面500中，區域資料圖框530的內容會跟在圖5的情境中相同，都是前述的第一資料群組。

[0127] 換言之，在圖8所繪示的多圖框畫面500中，導引圖框510中被選取的候選物

件是候選物件513，第一全域資料圖框520中所顯示的第一目標全域屬性資料，是對應於候選物件513所代表的第二日期的第二裝置活動關聯圖，而區域資料圖框530中所顯示的目標資料群組，則是對應於運算裝置111的第一資料群組。在此情況下，倘若使用者透過輸入裝置145選取第一全域資料圖框520中的第一主視覺物件521，由於區域資料圖框530中所顯示的內容已經是對應於運算裝置111的第一資料群組，所以區域資料圖框530的內容並不會有所改變。然而，倘若使用者透過輸入裝置145選取第一全域資料圖框520中的第二主視覺物件523，則圖框關聯控制模塊350會進行流程716，以指示區域資料圖框產生模塊340更換區域資料圖框530中所顯示的區域屬性資料。

[0128] 接著，區域資料圖框產生模塊340會按照圖框關聯控制模塊350的指示，進行流程718，以選擇與新選取的主視覺物件523所代表的運算裝置112相應的第二裝置資料群組，做為目標資料群組，並將區域資料圖框530的內容更換成對應於運算裝置112的第二裝置資料群組。圖框關聯控制模塊350則會進行流程708，以控制顯示裝置141顯示區域資料圖框530更新後的內容，使得多圖框畫面500的內容變成圖9所繪示的態樣。

[0129] 如前所述，圖框關聯控制模塊350不會要求導引圖框產生模塊320隨著第一全域資料圖框520中被選取的主視覺物件的改變，而連帶改變導引圖框510中的多個候選物件的內容。因此，在圖9的多圖框畫面500中，導引圖框510的內容會跟在圖8的情境中相同，而不會有所改變。

[0130] 在實作上，連動式資料圖框產生程式154所產生多圖框畫面500中也可以同時包含複數個全域資料圖框，和/或複數個區域資料圖框。例如，在圖10所繪示的實施例中，連動式資料圖框產生程式154所產生的連動式資料圖框，除了前述的導引圖框510、第一全域資料圖框520、以及區域資料圖框530之外，還包含一第二全域資料圖框1020。

[0131] 如前所述，全域資料圖框產生模塊330可針對每個過濾條件產生兩個或兩個以上種類的全域屬性資料。例如，全域資料圖框產生模塊330可針對每個日期產生兩個不同種類的全域屬性資料。

[0132] 當導引圖框510中被選取的候選物件是候選物件511時，全域資料圖框產生模塊330可選擇對應於候選物件511所代表的第一日期的第一種全域屬性資料，做為前述的第一目標全域屬性資料，並選擇對應於該第一日期的第二種全域屬性資料，做為一第二目標全域屬性資料。如圖10所示，全域資料圖框產生模塊330除了會建立包含第一目標全域屬性資料的第一全域資料圖框520之外，還會建立包含第二目標全域屬性資料的第二全域資料圖框1020。此外，圖框關聯控制模塊350還會在控制顯示裝置141顯示

第一全域資料圖框520時，同時也控制顯示裝置141在多圖框畫面500中顯示第二全域資料圖框1020。

[0133] 與第一全域資料圖框520中的情況相同，全域資料圖框產生模塊330在前述的第二目標全域屬性資料中，也會分別利用多個主視覺物件代表標的網路系統102中的局部裝置或全部裝置。全域資料圖框產生模塊330在第二目標全域屬性資料中所使用的主視覺物件的視覺表述方式，可以跟在第一目標全域屬性資料中所使用的視覺表述方式相同，也可以有所不同。

[0134] 換言之，在圖10所繪示的多圖框畫面500中，導引圖框510中被選取的候選物件是候選物件511，第一全域資料圖框520中所顯示的第一目標全域屬性資料，是對應於第一日期的第一種全域屬性資料，而第二全域資料圖框1020中所顯示的第二目標全域屬性資料，則是對應於第一日期的第二種全域屬性資料。在此情況下，倘若使用者透過輸入裝置145選取導引圖框510中的候選物件513，則圖框關聯控制模塊350會進行流程714，以指示全域資料圖框產生模塊330更換第一全域資料圖框520中的第一目標全域屬性資料，並更換第二全域資料圖框1020中的第二目標全域屬性資料。

[0135] 接著，全域資料圖框產生模塊330會按照圖框關聯控制模塊350的指示，進行流程614，以選擇與新選取的候選物件513所代表的第二日期相對應的第一種全域屬性資料做為第一目標全域屬性資料，並選擇與第二日期相對應的第二種全域屬性資料做為第二目標全域屬性資料。另外，全域資料圖框產生模塊330還會將第一全域資料圖框520中的內容更換成對應於前述第二日期的第一種全域屬性資料，並將第二全域資料圖框1020中的內容更換成對應於前述第二日期的第二種全域屬性資料。圖框關聯控制模塊350則會進行流程708，以控制顯示裝置141顯示第一全域資料圖框520與第二全域資料圖框1020兩者更新後的內容，以使得多圖框畫面500的內容變成圖11所繪示的態樣。

[0136] 在圖11的實施例中，此時圖框關聯控制模塊350並不會指示區域資料圖框產生模塊340更換區域資料圖框530中的目標資料群組，所以在圖11的多圖框畫面500中，區域資料圖框530的內容會跟在圖10的情境中相同。

[0137] 在前述的實施例中，導引圖框510中的多個候選物件所對應的過濾條件的態樣，以及區域資料圖框530中的目標資料群組的態樣，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，圖12為本發明另一實施例的多圖框畫面500的局部內容簡化後的示意圖。在圖12的實施例中，導引圖框510中的多個示例性候選物件1211～1215所對應的過濾條件，是依照一預定條件分類後的裝置群組，而區域資料圖框530中

的目標資料群組，則是特定運算裝置的軟、硬體基本資料。

[0138] 實作上，導引圖框510中的多個候選物件所對應的過濾條件的態樣，以及區域資料圖框530中的目標資料群組的態樣，都可以依據實際需要來調整設計方式。

[0139] 由前述說明可知，一旦導引圖框510中被選取的候選物件有所改變，第一全域資料圖框520的內容會連動改變。但此時區域資料圖框530的內容有可能會連動改變，也可能不會改變，這部分取決於圖框關聯控制模塊350的規則設定。

[0140] 另一方面，一旦第一全域資料圖框520中被選取的主視覺物件有所改變，區域資料圖框530的內容會連動改變，但導引圖框510的內容並不會改變。

[0141] 因此，資安分析人員可藉由改變在導引圖框510所選取的候選物件、和/或在第一全域資料圖框520中所選取的主視覺物件，來調整其所使用的過濾條件組合，並從多圖框畫面500中觀察過濾條件調整前後的資料圖框的內容變化。

[0142] 從另一角度而言，當導引圖框510中被選取的候選物件發生變化時，會單向造成第一全域資料圖框520的內容發生連帶變化，但當第一全域資料圖框520中被選取的主視覺物件發生變化時，卻不會造成導引圖框510的內容產生變化。前述資料圖框連動方式的主要設計目的，是要在第一全域資料圖框520中被選取的主視覺物件發生變化而連帶改變區域資料圖框530的內容時，能夠將導引圖框510中的多個候選物件同時呈現在多圖框畫面500中，且不改變候選物件的內容。

[0143] 這樣的設計是有好處的。因為傳統上供資安分析人員使用的分析工具，通常都會要求資安分析人員藉由輸入檢索字串的方式來進行資料過濾。當資安分析人員要更換成不同的過濾條件時，原先的過濾條件就會被清除，所以資安人員得依賴記憶力或記錄自己曾使用過的過濾條件，而難以用多階層式的過濾條件組合來篩選資料，所以遇到要分析的資料量為數眾多的情況時，就經常需要重複輸入許多相同的過濾條件，徒然浪費許多人力與時間。

[0144] 相較之下，前述連動式資料圖框產生程式154所產生的多個連動式資料圖框510~530，可以將多個不同層次的過濾條件同時呈現在多圖框畫面500中。因此，資安分析人員不僅可藉由操控導引圖框510和第一全域資料圖框520中的物件的方式，來快速調整其所使用的過濾條件組合，而且部分層級的過濾條件也會同時呈現在多圖框畫面500中供資安分析人員隨時評估是否要更換過濾條件。因此，前述資料圖框的連動方式設計，有助於改善篩選大量資料所需的時間，尤其是在診斷特定網路環境是否已受到駭客入侵的應用中更有助於提升整體的判斷效率。

[0145] 此外，連動式資料圖框產生程式154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進行分析、過濾掉多餘的雜訊資料，並產生用於顯示多個過濾條件的導引圖框510、用於顯示與標的網路系統102中的局部裝置或全部裝置有關的特定全域屬性資料的第一全域資料圖框520、以及用於顯示與標的網路系統102的其中一個運算裝置相對應的特定資料群組的區域資料圖框530。因此，前述連動式資料圖框產生程式154所產生的多個連動式資料圖框510~530，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。

[0146] 另外，由於連動式資料圖框產生程式154會控制顯示裝置141同時顯示前述的導引圖框510、第一全域資料圖框520、與區域資料圖框530，所以資安分析人員可從導引圖框510、第一全域資料圖框520、與區域資料圖框530中，同時獲取與標的網路系統102有關的不同面向或是不同維度的重要參考資料，有助於提升判斷的效率。

[0147] 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。由於連動式資料圖框產生程式154所產生的多個連動式資料圖框510~530，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。

[0148] 請注意，前述圖6與圖7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，流程602與604的執行時序，與流程606至612的執行時序沒有特定的關聯，所以流程606至612也可以調整到流程602與604之前進行。又例如，流程602與604的執行時序，與流程702至706的執行時序沒有特定的關聯，所以流程702至706也可以調整到流程602與604之前進行。又例如，流程606至612的執行時序，與流程702至706的執行時序沒有特定的關聯，所以流程702至706也可以調整到流程606至612之前進行。又例如，流程610與612的順序可以對調，也可以同時進行。又例如，在圖7中，流程710與712的順序可以輪流進行，也可以同時進行。

[0149] 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。

[0150] 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。

[0151] 在某些實施例中，前述資料庫152中所儲存的資料，可以是透過其他管道載入到資料庫152中，而不侷限於要透過前述多圖框網路安全分析裝置140中的通信電路143接收。在此情況下，可將通信電路143省略。

[0152] 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。

[0153] 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）傳送給多圖框網路安全分析裝置140。

[0154] 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。

[0155] 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.

[0156] 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.

[0157] 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. 一種多圖框網路安全分析裝置（140），用於診斷一標的網路系統（102）是否已受到駭客入侵，該多圖框網路安全分析裝置（140）包含：

一顯示裝置（141）；

一輸入裝置（145），設置成接收一使用者下達的操作指令；

一非揮發性儲存電路（147），設置成儲存一資料庫（152）與一連動式資料圖框產生程式（154），其中，該資料庫（152）內儲存有與一標的網路系統（102）中的多個運算裝置（111～115）有關的多種裝置活動記錄；以及

一控制電路（149），耦接於該顯示裝置（141）、該輸入裝置（145）、與該非揮發性儲存電路（147），並設置成執行該連動式資料圖框產生程式（154），以依據該資料庫（152）中所儲存的該多種裝置活動記錄進行一資料圖框產生運作，以產生與該標的網路系統（102）有關的多個連動式資料圖框（510、520、530、1020），並同時顯示該多個連動式資料圖框（510、520、530、1020）的內容；

其中，該多個連動式資料圖框（510、520、530、1020）包含一導引圖框（510）、一第一全域資料圖框（520）、以及一區域資料圖框（530）。

2. 如請求項 1 所述的多圖框網路安全分析裝置（140），其中，該資料圖框產生運作包含：

產生分別與多個過濾條件相應的多個候選物件（511、513、515），其中，該多個候選物件（511、513、515）包含對應於一第一過濾條件的一第一候選物件（511）、以及對應於一第二過濾條件的一第二候選物件（513）；

建立包含該多個候選物件（511、513、515）的一導引圖框（510）；

依據該資料庫（152）中的資料，產生與該標的網路系統（102）中的局部裝置或全部裝置有關的多個全域屬性資料，其中，該多個全域屬性資料包含對應於該第一過濾條件的一第一全域屬性資料、以及對應於該第二過濾條件的一第二全域屬性資料；

選擇該多個全域屬性資料的其中之一做為一第一目標全域屬性資料；

建立包含該第一目標全域屬性資料的一第一全域資料圖框（520）；

在該第一目標全域屬性資料中分別利用多個主視覺物件（521、523、525）代表該標的網路系統（102）中的局部裝置或全部裝置，其中，該多個主視覺物件包含對應於一第一運算裝置（111）的一第一主視覺物件（521）、以及對應於一第二運算裝置（112）的一第二主視覺物件（523）；

依據該資料庫（152）中的資料，產生分別與該多個運算裝置（111~115）相對應的多個資料群組，其中，該多個資料群組包含對應於該第一運算裝置（111）的第一資料群組、以及對應於該第二運算裝置（112）的一第二資料群組；

選擇該多個資料群組的其中之一做為一目標資料群組；

建立包含該目標資料群組的一區域資料圖框（530）；

利用該顯示裝置（141）同時顯示該導引圖框（510）、該第一全域資料圖框（520）、與該區域資料圖框（530）的內容；以及

控制該導引圖框（510）、該第一全域資料圖框（520）、與該區域資料圖框（530）之間的連動關係，以致使該第一全域資料圖框（520）的內容會隨著該使用者對該導引圖框（510）的操作而改變，且該區域資料圖框（530）的內容會隨著該使用者對該第一全域資料圖框（520）的操作而改變，但該導引圖框（510）的內容不會隨著該使用者對該第一全域資料圖框（520）的操作而改變。

3. 如請求項 2 所述的多圖框網路安全分析裝置（140），其中，該資料圖框產生運作還包含：

在該導引圖框（510）中被選取的一候選物件是該第一候選物件（511）、且該第一全域資料圖框（520）所顯示的該第一目標全域屬性資料是該第一全域屬性資料的情況下，倘若該使用者透過該輸入裝置（145）選取該導引圖框（510）中的該第二候選物件（513），則將該第一全域資料圖框（520）中所顯示的該第一目標全域屬性資料更換成對應於該第二過濾條件的該第二全域屬性資料。

4. 如請求項 3 所述的多圖框網路安全分析裝置（140），其中，該資料圖框產生運作還包含：

在該第一全域資料圖框（520）所顯示的該第一目標全域屬性資料是該第二全域屬性資料、該第一全域資料圖框（520）中被選取的一主視覺物件是該第一主視覺物件（521）、且該區域資料圖框（530）中所顯示的該目標資料群組是該第一資料

群組的情況下，倘若該使用者透過該輸入裝置（145）選取該第一全域資料圖框（520）中的該第二主視覺物件（523），則將該區域資料圖框（530）中所顯示的該目標資料群組更換成對應於該第二運算裝置（112）的該第二資料群組，但不改變該導引圖框（510）的內容。

5. 如請求項 3 所述的多圖框網路安全分析裝置（140），其中，該資料圖框產生運作還包含：

將該區域資料圖框（530）中所顯示的該目標資料群組更換成該第二過濾條件所對應的一預定資料群組。

6. 如請求項 3 所述的多圖框網路安全分析裝置（140），其中，該多個全域屬性資料還包含對應於該第一過濾條件的一第三全域屬性資料、以及對應於該第二過濾條件的一第四全域屬性資料，該資料圖框產生運作還包含：

選擇該第三全域屬性資料做為一第二目標全域屬性資料；

建立包含該第二目標全域屬性資料的一第二全域資料圖框（1020）；

在顯示該第一全域資料圖框（520）時，同時顯示該第二全域資料圖框（1020）；以及

在該第二目標全域屬性資料中分別利用多個主視覺物件（521、523、525）代表該標的網路系統（102）中的局部裝置或全部裝置。

7. 如請求項 6 所述的多圖框網路安全分析裝置（140），其中，該資料圖框產生運作還包含：

在該導引圖框（510）中被選取的一候選物件是該第一候選物件（511）、該第一全域資料圖框（520）所顯示的該第一目標全域屬性資料是該第一全域屬性資料、且該第二全域資料圖框（1020）所顯示的該第二目標全域屬性資料是該第三全域屬性資料的情況下，倘若該使用者透過該輸入裝置（145）選取該導引圖框（510）中的該第二候選物件（513），則將該第一全域資料圖框（520）中所顯示的該第一目標全域屬性資料更換成對應於該第二過濾條件的該第二全域屬性資料，並將該第二全域資料圖框（1020）中所顯示的該第二目標全域屬性資料更換成對應於該第二過濾條件的該第四全域屬性資料。

8. 一種電腦程式產品（154），儲存在一多圖框網路安全分析裝置（140）的一非揮發性儲存電路（147）中，允許該多圖框網路安全分析裝置（140）依據一資料庫（152）中所儲存的多種裝置活動記錄進行一資料圖框產生運作，以產生與一標的網路系統（102）有關的多個連動式資料圖框（510、520、530、1020），並同時顯示該多個連動式資料圖框（510、520、530、1020）的內容，其中，該多個連動式資料圖框（510、520、530、1020）包含一導引圖框（510）、一第一全域資料圖框（520）、以及一區域資料圖框（530）。
9. 如請求項 8 所述的電腦程式產品（154），其中，該資料圖框產生運作包含：
- 產生分別與多個過濾條件相應的多個候選物件（511、513、515），其中，該多個候選物件（511、513、515）包含對應於一第一過濾條件的一第一候選物件（511）、以及對應於一第二過濾條件的一第二候選物件（513）；
- 建立包含該多個候選物件（511、513、515）的一導引圖框（510）；
- 依據該資料庫（152）中的資料，產生與該標的網路系統（102）中的局部裝置或全部裝置有關的多個全域屬性資料，其中，該多個全域屬性資料包含對應於該第一過濾條件的一第一全域屬性資料、以及對應於該第二過濾條件的一第二全域屬性資料；
- 選擇該多個全域屬性資料的其中之一做為一第一目標全域屬性資料；
- 建立包含該第一目標全域屬性資料的一第一全域資料圖框（520）；
- 在該第一目標全域屬性資料中分別利用多個主視覺物件（521、523、525）代表該標的網路系統（102）中的局部裝置或全部裝置，其中，該多個主視覺物件包含對應於一第一運算裝置（111）的一第一主視覺物件（521）、以及對應於一第二運算裝置（112）的一第二主視覺物件（523）；
- 依據該資料庫（152）中的資料，產生分別與該多個運算裝置（111~115）相對應的多個資料群組，其中，該多個資料群組包含對應於該第一運算裝置（111）的第一資料群組、以及對應於該第二運算裝置（112）的一第二資料群組；
- 選擇該多個資料群組的其中之一做為一目標資料群組；
- 建立包含該目標資料群組的一區域資料圖框（530）；
- 利用該顯示裝置（141）同時顯示該導引圖框（510）、該第一全域資料圖框（520）、與該區域資料圖框（530）的內容；以及

控制該導引圖框（510）、該第一全域資料圖框（520）、與該區域資料圖框（530）之間的連動關係，以致使該第一全域資料圖框（520）的內容會隨著該使用者對該導引圖框（510）的操作而改變，且該區域資料圖框（530）的內容會隨著該使用者對該第一全域資料圖框（520）的操作而改變，但該導引圖框（510）的內容不會隨著該使用者對該第一全域資料圖框（520）的操作而改變。

10. 如請求項 9 所述的電腦程式產品（154），其中，該資料圖框產生運作還包含：在該導引圖框（510）中被選取的一候選物件是該第一候選物件（511）、且該第一全域資料圖框（520）所顯示的該第一目標全域屬性資料是該第一全域屬性資料的情況下，倘若該使用者透過該輸入裝置（145）選取該導引圖框（510）中的該第二候選物件（513），則將該第一全域資料圖框（520）中所顯示的該第一目標全域屬性資料更換成對應於該第二過濾條件的該第二全域屬性資料。
11. 如請求項 10 所述的電腦程式產品（154），其中，該資料圖框產生運作還包含：在該第一全域資料圖框（520）所顯示的該第一目標全域屬性資料是該第二全域屬性資料、該第一全域資料圖框（520）中被選取的一主視覺物件是該第一主視覺物件（521）、且該區域資料圖框（530）中所顯示的該目標資料群組是該第一資料群組的情況下，倘若該使用者透過該輸入裝置（145）選取該第一全域資料圖框（520）中的該第二主視覺物件（523），則將該區域資料圖框（530）中所顯示的該目標資料群組更換成對應於該第二運算裝置（112）的該第二資料群組，但不改變該導引圖框（510）的內容。
12. 如請求項 10 所述的電腦程式產品（154），其中，該資料圖框產生運作還包含：將該區域資料圖框（530）中所顯示的該目標資料群組更換成該第二過濾條件所對應的一預定資料群組。
13. 如請求項 10 所述的電腦程式產品（154），其中，該多個全域屬性資料還包含對應於該第一過濾條件的一第三全域屬性資料、以及對應於該第二過濾條件的一第四全域屬性資料，該資料圖框產生運作還包含：
選擇該第三全域屬性資料做為一第二目標全域屬性資料；
建立包含該第二目標全域屬性資料的一第二全域資料圖框（1020）；

在顯示該第一全域資料圖框（520）時，同時顯示該第二全域資料圖框（1020）；以及

在該第二目標全域屬性資料中分別利用多個主視覺物件（521、523、525）代表該標的網路系統（102）中的局部裝置或全部裝置。

14. 如請求項 13 所述的電腦程式產品（154），其中，該資料圖框產生運作還包含：
在該導引圖框（510）中被選取的一候選物件是該第一候選物件（511）、該第一全域資料圖框（520）所顯示的該第一目標全域屬性資料是該第一全域屬性資料、且該第二全域資料圖框（1020）所顯示的該第二目標全域屬性資料是該第三全域屬性資料的情況下，倘若該使用者透過該輸入裝置（145）選取該導引圖框（510）中的該第二候選物件（513），則將該第一全域資料圖框（520）中所顯示的該第一目標全域屬性資料更換成對應於該第二過濾條件的該第二全域屬性資料，並將該第二全域資料圖框（1020）中所顯示的該第二目標全域屬性資料更換成對應於該第二過濾條件的該第四全域屬性資料。