公告本

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：92133851

※ 申請日期：92.12.2　　※IPC 分類：G06F 11/36 (2006.01) G06F 9/30 (2006.01)

壹、發明名稱：（中文/英文）

用於因應電腦入侵之方法及系統

METHOD AND SYSTEM FOR RESPONDING TO A COMPUTER INTRUSION

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

美商萬國商業機器公司

INTERNATIONAL BUSINESS MACHINES CORPORATION

代表人：（中文/英文）

傑拉德 羅森賽

ROSENTHAL, GERALD

住居所或營業所地址：（中文/英文）

美國紐約州阿蒙市新果園路

NEW ORCHARD ROAD, ARMONK, NY 10504, U.S.A.

國　籍：（中文/英文）

美國　U.S.A.

參、發明人：（共 5 人）

姓　名：（中文/英文）

1.保羅 T 巴菲斯

BAFFES, PAUL T.

2.約翰 麥克 卡利森

GARRISON, JOHN MICHAEL

3.麥克 吉菲克斯

GILFIX, MICHAEL

4.艾倫 徐

HSU, ALLAN

5.泰倫 傑羅德 史塔汀

STADING, TYRON JERROD

住居所地址：（中文/英文）

1.美國德州奧斯汀市杭尼沙克街8708號

8708 HONEYSUCKLE TRAIL, AUSTIN, TX 78759, U.S.A.

2.美國德州奧斯汀市賽路戴洞街4420號

4420 SECLUDED HOLLOW, AUSTIN, TX 78727, U.S.A.

3.美國德州奧斯汀市塔帕德拉屈斯街5700號221室

5700 TAPADERA TRACE LANE, APT. 221, AUSTIN, TX 78727, U.S.A.

4.美國俄亥俄州森特菲爾市泰布利街2522號

2522 TEDBURY COURT, CENTERVILLE, OH 45459, U.S.A.

5.美國德州奧斯汀市美力克路13401號112室

13401 METRIC BLVD., APT. 112, AUSTIN, TX 78727, U.S.A.

國　籍：（中文/英文）

1.2.4.5均美國　U.S.A.

3.加拿大　CANADA

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

☑ **本案申請前已向下列國家（地區）申請專利：**

1.美國；2002年12月05日；10/313,732

2.

3.

4.

5.

☑ **主張國際優先權(專利法第二十四條)：**

【格式請依：受理國家（地區）；申請日；申請案號數 順序註記】

1.美國；2002年12月05日；10/313,732

2.

3.

4.

5.

☐ **主張國內優先權(專利法第二十五條之一)：**

【格式請依：申請日；申請案號數 順序註記】

1.

2.

☐ **主張專利法第二十六條微生物：**

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

本發明概言之係關於資料處理領域，詳言之，係關於一種用於使用一惡意入侵影響之圖形表示來因應該入侵之經改良之資料處理系統及方法。

【先前技術】

大多數現代企業網路包括供遠端使用者通常經由網際網路存取之構件。此種存取設計用於使經授權之使用者爲諸如電子商務、共享內容及其他電子活動等目的與網路互動。由於該等網路被設計爲可供經授權之使用者輕易存取，因而其亦易於受到未經授權之使用者尤其係彼等懷有惡意存取該網路之意圖之使用者存取，此種惡意體現爲使用者之"入侵"形式。入侵被定義爲對網路或網路中之電腦之惡意電子存取。入侵之實例包括：病毒、未經授權之資料採擷(有時稱作"檔案遭駭客入侵(hacking of files)")、及分散式阻絕服務(DDOS)攻擊，其中在分散式阻絕服務(DDOS)攻擊中，電腦系統因遭該入侵而超載，從而無法再執行實際工作。

入侵事件被定義爲入侵之結果(影響)。入侵事件之實例係：資料檔案遭到破壞或非法複製，系統/電腦當機及系統/電腦減速。

抵制入侵通常係安全管理員之工作，安全管理員係借助風險管理軟體監控一電腦有無遭到入侵之資訊技術專家。儘管目前存在衆多用於偵測入侵及入侵事件之習知方法，

然而，管理對入侵之因應卻極其複雜。換言之，儘管事件偵測已衆所習知且可自動實施，但通常需手動採取管理及因應措施。由於入侵之複雜性質，安全管理員很難評估當前所發生之入侵係何種類型及如何正確因應。

因此，需要一種較佳以一自動或半自動方式來輔助安全管理員因應所偵測入侵之方法及系統。

【發明內容】

本發明係關於一種管理電腦入侵之方法及系統，其方式為：以圖形形式表示一已知先前入侵之入侵模式；然後比較一當前入侵之入侵模式與該先前入侵。若該已知入侵與當前入侵具有某些共同結果(入侵事件或共同受到影響之硬體)或結果皆相同，則安全管理員可執行指令碼因應，以修復由當前入侵所致之損壞，或至少防止當前入侵造成進一步損壞。

入侵模式既可基於入侵事件(入侵事件係由入侵或各種可提供一入侵類型簽章之活動所造成之影響)，亦可基於受到入侵影響之硬體拓撲。

入侵模式以圖形形式顯示給安全管理員，安全管理員可藉由執行指令碼因應而作出因應，在一較佳實施例中，該等指令碼因應顯示於與入侵模式中每一節點相關聯的各快顯視窗中。或者，亦可基於當前入侵與已知先前入侵之入侵模式中共有特徵之一預定百分比來自動因應入侵。

在下文詳細書面說明中，本發明之上述及其他目的、特徵及優點將變得一目了然。

【實施方式】

現在參照附圖，尤其係參照附圖1，其中展示一能夠與一網路(未圖示)通信之本發明較佳實施例之資料處理系統100。舉例而言，該資料處理系統100係可自位於Armonk，紐約的國際商業機器公司(International Business Machines Corporation)購得的其中一種型號的個人電腦或伺服器。該資料處理系統100既可僅包括一單處理器系統，亦可係一包括複數個處理器之多處理器(MP)系統。在所示實例中係展示一單處理器系統。亦可增設一第二處理器(未圖示)至所示系統，該第二處理器既可具有一單獨的L2快取亦可與處理器102共享L2快取108。處理器102可係一包含單獨的一階(L1)指令104及資料快取106於該處理器中之超純量精簡指令集計算(RISC)處理器。

處理器102連接至二階(L2)快取108。L2快取108連接至資料處理系統100之系統匯流排110。系統記憶體112亦連接至系統匯流排110，就如輸入/輸出(I/O)匯流排橋接器114一樣。I/O匯流排橋接器114耦合I/O匯流排118至系統匯流排110，以將資料處理自其中一匯流排中繼及/或轉換至另一匯流排。亦可連接其他裝置至系統匯流排110，例如記憶體對映圖形配接器116，該記憶體對映圖形配接器可提供使用者介面資訊至一顯示器124。

I/O匯流排橋接器114連接至I/O匯流排118，而該I/O匯流排118可連接至眾多其他裝置，例如一輸入裝置126(其可係一習知滑鼠、一軌跡球、一鍵盤或類似裝置)及一非揮發性

儲存器122(例如一硬碟機、一唯讀光碟記憶體(CD-ROM)光碟機、一數位視訊光碟(DVD)光碟機或類似儲存裝置)。

I/O匯流排118亦連接有一網路配接器120，該網路配接器120提供一介接一網路之邏輯介面，該網路可係一區域網路(LAN)、廣域網路(WAN)、網際網路或其他能使資料處理系統100與該網路中其他電腦通信的網路。

圖1所示實例性實施例僅提供用於闡釋本發明之目的，且熟習此項技術者應可瞭解，可在形式及功能上作出衆多修改。舉例而言，資料處理系統100可包括一音效卡及聲頻揚聲器、其他I/O裝置及通信埠、及衆多其他元件。所有此等修改皆應被視爲仍歸屬於本發明之範疇及主旨內。

現在參照圖2a，該圖展示由衆多不同入侵所致的可能入侵事件。該等入侵事件被定義爲由入侵激發之活動或影響。儘管該圖係以一樹狀結構展示該等入侵事件，然而，認識到所示該等入侵事件相互關聯可最佳地理解該等入侵事件。舉例而言，考量一入侵路徑200，該入侵路徑展示由一入侵A所致入侵事件(示於粗圓圈中)。入侵A(爲例示之目的，其可係一諸如"紅色警戒(Red Code)"等病毒)係一種以在一主電腦206中產生一分散式阻絕服務204之方式來影響多個主機202之入侵。該圖顯示由一Snort 208偵測到該入侵A，該Snort 208係一能夠對IP網路執行即時流量分析及封包日誌記錄之實例性入侵偵測系統。Snort 208可執行協定分析、內容搜尋/比對並可用於偵測衆多種攻擊及探查，例如緩衝器溢位、隱形埠掃描、共用閘道介面(CGI)攻擊、伺服

器訊息塊(SMB)探查、作業系統(OS)辨識企圖及諸如此類。

入侵A亦可自一入侵偵測系統(IDS)210觸發一因應，該入侵偵測系統(IDS)210檢查所有傳入及傳出網路活動並識別可指示一由某一企圖侵入或損害系統之人所作網路或系統攻擊的可疑模式。IDS 210偵測到一網路事件212，在本實例中該網路事件212係入侵A，其係一種由整個系統識別並影響整個系統之入侵事件214。

應注意，如入侵路徑200所示，入侵A亦影響電腦系統之其他部分。換言之，入侵A亦造成一主機事件216，該主機事件216在系統層218處影響一記憶體事件220及一使用權限事件222。此外，入侵A造成一外圍事件224，該外圍事件224被防火牆226偵測爲一掃描事件228且亦具有一不正確的資料封包230。如圖所示，該不正確的封包230係一傳輸控制協定(TCP)格式錯誤的協定封包232。

因此，由加黑粗線條邊界之入侵路徑200所示之模式係入侵A獨有之特徵入侵模式。現在參見圖2b，該圖展示一入侵路徑201，該入侵路徑基於一未知當前入侵之入侵事件。最初並不知曉當前入侵之動機，然而，由於該入侵模式與圖2a所示入侵A之入侵模式相同，因此，已遭入侵之電腦網路或電腦之安全管理員可認定當前入侵與入侵A相同或至少以相同方式作用。

在一本發明之較佳實施例中，每一節點皆與一指令碼因應相關聯，例如指令碼因應204a與阻絕服務事件204相關聯。指令碼因應係一用於對付入侵事件之預編指令碼。舉

例而言，指令碼因應204a可係一設計用於隔離正在破壞電腦系統之入侵然後使該入侵失效之程式。所示該等指令碼因應與每一事件描述節點相關聯，且較佳位於一現用視窗(例如一快顯視窗)中，該現用視窗僅需使用一滑鼠或類似指標裝置點擊即可啓動指令碼因應。儘管該等指令碼因應被展示爲單一項目，然而，在一替代較佳實施例中，展示了列於一清單中的多個建議指令碼因應且該等因應可於入侵路徑201中的一或所有節點處皆處於有效狀態。較佳以多個階層展示該等多個指令碼因應，並且依據使用指令碼因應之成功歷史資料、入侵之危急度、或安全管理員在開發風險管理程式時所決定用於評估入侵之其他因素，該等指令碼因應之一具有最高階層。舉例而言，一風險管理程式可確定：必須確保隔離任何攻擊任務關鍵資料之入侵，即使該種隔離會卸下電腦系統中未受影響之部分。在此一情況下，最高建議因應將卸下該電腦系統中之許多區域，並將被推薦作爲最高建議因應。

應注意，並非在入侵路徑必須完全相同時，方對安全管理員提供關於如何因應入侵之資訊。換言之，若已知入侵及未知入侵之入侵路徑具有一定數量之共同點，安全管理員即可啓動一因應來糾正當前未知入侵之大部分(若非全部)有害影響。

在本發明之一實施例中，由安全管理員手動選擇入侵路徑201中每一節點之每一指令碼因應。或者，如圖3所示流程圖所述，可選擇一設定來響應一入侵而自動啓動一用於

所有節點之最高建議因應。如方塊302所述，較佳由一能夠根據一入侵之特徵偵測該入侵之風險管理器來偵測一當前入侵。此等特徵可包括：接收到已知有害標頭資訊或其他資料封包、電腦系統中之軟體或硬體採取具有遭到入侵特徵的措施(例如掃描一網路中所有電腦以查找網際網路協定(IP)地址、驟然出現電腦效能降級或CPU使用方式)、及類似事件或狀態。如方塊304所述，將當前入侵之入侵事件與一已知入侵之彼等入侵事件相比較。如詢問塊306所闡釋，判定是否在未知當前入侵與已知先前入侵二者中發現一預定百分比的共有事件節點。換言之，比較已知入侵與當前入侵之入侵路徑。若已知先前入侵與未知當前入侵具有一較大數量之共有事件節點，則如方塊310所述自動執行所有節點之指令碼因應。而若在已知入侵與未知入侵之間不存在足夠之共有事件節點，則安全管理員立即爲每一事件節點手動選擇一指令碼因應。

亦可由電腦系統上的一風險管理程式作出自動執行所有指令碼因應之判定，該風險管理程式將入侵分類，以判定是否應啓動一自動因應。舉例而言，若該風險管理程式判定當前入侵係一已知分類類型，或具有可致使整個系統當機之已知嚴重性，則可啓動一自動指令碼因應。在一較佳實施例中，比對入侵之嚴重性與一指令碼因應結果之嚴重性。換言之，比對一嚴重入侵與一可能會對系統產生嚴重影響(例如搶先卸下該系統之一部分)之指令碼因應，然而，由於該種入侵之嚴重性質及該種入侵可能造成之潛在損

害，該嚴重影響仍可能較爲合算。

同樣，若已將風險管理程式設計爲，可得知安全管理員因應入侵之預期因應時間可能過長以致在安全管理員因應之前即會對系統造成嚴重損害，則可啓動一自動指令碼因應。同樣，若一特定入侵路徑已在先前多次(或僅一次)引發執行特定指令碼因應，則風險管理程式可根據該歷史來自動啓動執行該等指令碼因應。

除圖2a及圖2b所示之共有事件模式外，入侵亦具有關於一硬體拓撲中何種硬體受到影響之特徵。現在參照圖4a，該圖展示可能受到一入侵影響之硬體。一入侵路徑400(在該圖中由粗體邊框方框標識)示出一受到如上述圖2a中的入侵A影響之電腦系統之硬體拓撲。由此可見，入侵A在一企業電腦系統之內部網路402中引起異常，該內部網路402受到內部網路402中一區域網路(LAN)A 404影響。在LAN A 404內，伺服器406、個人電腦(PC)408及入侵偵測系統(IDS)硬體410皆受到影響。其中在伺服器406內具有一受到影響的網站伺服器416，該網站伺服器416之入口B 418亦受到入侵A之影響。類似地，所有執行Window®作業系統之PC皆受到影響並在該圖中示爲基於Window® 之PC 414。同樣，執行具備Snort功能型硬體412之IDS硬體410記錄一表示已偵測到入侵A的事件。因此，該硬體以一類似於上文結合圖2a及圖2b所述入侵事件入侵模式之方式展示一特徵入侵模式。

現在參照圖4b，硬體拓撲入侵路徑401展示由入侵A所造

成之模式。當所出現的當前未知入侵具有與硬體拓撲入侵路徑401所示模式相同或相似之模式時，安全管理員以一種類似於針對上文入侵事件入侵模式所述之方式作出因應。因此，硬體拓撲入侵路徑401中每一事件節點皆包括一相關的包含指令碼因應之現用視窗，該(等)指令碼因應與上文在闡述圖2a及圖2b時所述之彼等指令碼因應相似。如同入侵事件之指令碼因應一樣，示於硬體拓撲入侵路徑401中的指令碼因應既可如圖所示係單一指令碼因應，亦可係一建議指令碼因應清單，較佳地對該清單實施記分以給出一最高指令碼因應。可採用一類似於上文針對入侵事件入侵路徑所述之方式自動啓動或手動啓動該等指令碼因應。

如同上文結合圖2a及圖2b所述及所示之入侵事件圖形顯示，並非在已知入侵與未知入侵之入侵路徑完全相同時，方對安全管理員提供關於如何因應入侵之資訊。換言之，若已知入侵與未知入侵之入侵路徑具有一定數量之共同點，安全管理員即可啓動一因應來糾正當前未知入侵之大部分(若非全部)有害影響。

可由安全管理員響應一通知而就地或遠程啓動應對入侵之指令碼因應。舉例而言，安全管理員可藉由一行動電話或個人數位助理(PDA)接收一告知其該入侵事件之通知。然後，安全管理員可藉由點擊PDA中的一互動式視窗，以電子方式啓動某些或所有指令碼因應，以使由電腦系統的一風險管理程式辨識該輸入，從而啓動所請求之指令碼因應。

因此，本發明提供一種用於建置並以圖形方式表示一已

知入侵之入侵模式，以供比較一當前入侵相之方法及裝置，該當前入侵可爲電腦系統之風險管理程式所已知或可爲其所未知。在根據以圖形方式表示的當前入侵之特徵入侵路徑辨識該當前入侵後，啓動指令碼因應來因應並控制該入侵。該等指令碼因應可基於已知入侵之歷史資料。已知入侵與當前入侵既可相同亦可不同，且建議指令碼因應係以圖形形式與受當前入侵影響之入侵路徑中某些或所有事件節點或硬體節點一起顯現。對於入侵路徑中的每一事件節點/硬體節點而言，指令碼因應可係一單一選項，或者可選自一階層式建議指令碼因應清單。

儘管上文已根據一資料處理系統及伺服器群闡述了本發明之態樣，然而應瞭解，至少本發明之某些態樣亦可構建爲一與一資料儲存系統或電腦系統共同使用之程式產品。定義本發明功能之程式可藉由衆多種信號攜載媒體傳送至一資料儲存系統或電腦系統，該等信號攜載媒體包括(但不限於)：不可寫式儲存媒體(例如CD-ROM)、可寫式儲存媒體(例如軟碟片、硬碟機、讀/寫式CD-ROM、光學媒體)、及諸如包括乙太網路在內的電腦及電話網路等通信媒體。因此，應瞭解，此等信號攜載媒體在載送或編碼用於導出本發明方法功能之電腦可讀指令時，即代表本發明之替代實施例。此外，應瞭解，可由一具有本文所述硬體、軟體、或軟體與硬體之一組合或其等價物形式之裝置之系統來實施本發明。

儘管上文係根據一較佳實施例詳細展示並闡述本發明，

然而，熟習此項技術者應瞭解，可對其中之形式及細節作出各種修改且並不背離本發明之精神及範疇。

【圖式簡單說明】

據信爲本發明所特有之新穎特徵闡述於隨附申請專利範圍中。然而，結合附圖閱讀本文對一闡釋性實施例之詳細說明，將會最佳瞭解本發明本身及一較佳使用模式、其他目的及優點，附圖中：

圖1係一方塊圖，其展示一可用於實施本發明之資料處理；

圖2a展示一入侵模式，該入侵模式基於包括一已知先前入侵在內之衆多不同入侵之入侵事件；

圖2b展示一入侵模式，該入侵模式基於一與一已知先前入侵之入侵模式相匹配之未知當前入侵之入侵事件；

圖3係一流程圖，其展示一用於自動執行對一未知當前入侵之指令碼因應之本發明較佳實施例；

圖4a展示一入侵模式，該入侵模式基於受到包括一已知先前入侵在內的衆多不同入侵影響的硬體拓撲；

圖4b展示一入侵模式，該入侵模式基於受到一與一已知先前入侵之入侵模式相匹配之未知當前入侵影響的硬體拓撲。

【圖式代表符號說明】

100　　資料處理系統

102　　處理器

104　　一階指令

106	資料快取
108	L2快取
110	系統匯流排
112	系統記憶體
114	I/O匯流排橋接器
116	圖形配接器
118	I/O匯流排
120	網路配接器
122	非揮發性儲存器
124	顯示器
126	輸入裝置
200	入侵路徑
202	多個主機
204	阻絕服務
206	主機
208	Snort
210	IDS
212	網路事件
214	入侵事件
216	主機事件
218	系統層
220	記憶體
222	使用權限事件
224	外圍事件

226	防火牆
228	掃描事件
230	不正確的封包
232	TCP格式錯誤的協定
201	入侵路徑
202a	指令碼因應
204a	指令碼因應
206a	指令碼因應
208a	指令碼因應
210a	指令碼因應
212a	指令碼因應
214a	指令碼因應
216a	指令碼因應
218a	指令碼因應
220a	指令碼因應
222a	指令碼因應
224a	指令碼因應
226a	指令碼因應
228a	指令碼因應
230a	指令碼因應
232a	指令碼因應
400	入侵路徑
402	內部網路
404	LAN A

406	伺服器
408	PC
410	IDS
412	Snort
414	基於Window之PC
416	網站伺服器
418	入口B
401	硬體拓撲入侵路徑
402a	指令碼因應
404a	指令碼因應
406a	指令碼因應
408a	指令碼因應
410a	指令碼因應
412a	指令碼因應
414a	指令碼因應
416a	指令碼因應
418a	指令碼因應

伍、中文發明摘要：

本發明揭示一種管理電腦入侵之方法及系統，其方式為：以圖形形式表示一已知先前入侵之入侵模式；然後比較該已知入侵之入侵模式與一當前入侵。入侵模式既可基於入侵事件(入侵事件係由入侵或提供一入侵類型簽章之活動所造成之影響)，亦可基於受到入侵影響之硬體拓撲。入侵模式以圖形形式與指令碼因應一起顯示，在一較佳實施例中，該等指令碼因應顯示於與入侵模式中每一節點相關聯的各快顯視窗中。或者，亦可基於當前入侵與已知先前入侵之入侵模式中共有特徵之一預定百分比來自動因應入侵。

陸、英文發明摘要：

A method and system for managing an intrusion on a computer by graphically representing an intrusion pattern of a known past intrusion, and then comparing the intrusion pattern of the known intrusion with a current intrusion. The intrusion pattern may either be based on intrusion events, which are the effects of the intrusion or activities that provide a signature of the type of intrusion, or the intrusion pattern may be based on hardware topology that is affected by the intrusion. The intrusion pattern is graphically displayed with scripted responses, which in a preferred embodiment are presented in pop-up windows associated with each node in the intrusion pattern. Alternatively, the response to the intrusion may be automatic, based on a pre-determined percentage of common features in the intrusion pattern of the known past intrusion and the current intrusion.

柒、指定代表圖：

(一)本案指定代表圖為：第（ 3 ）圖。

(二)本代表圖之元件代表符號簡單說明：

（無元件代表符號）

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

（無）

拾、申請專利範圍：

1. 一種管理電腦入侵之方法，該方法包括：

以圖形形式表示一已知入侵之入侵路徑，該圖形表示包括一位於該入侵路徑中一節點處之指令碼因應；

依據該電腦之一當前入侵與該已知入侵之入侵路徑中的至少一共有特徵來比對該當前入侵與該已知入侵之圖形表示；及

響應於該已知入侵與該當前入侵之比對，啓動能夠因應該當前入侵之該指令碼因應。

2. 根據申請專利範圍第1項之方法，其中該入侵模式係基於入侵事件。

3. 根據申請專利範圍第1項之方法，其中該入侵模式係基於受到該已知入侵影響之硬體拓撲。

4. 根據申請專利範圍第1項之方法，其中該已知入侵與該當前入侵相同，且其中用於因應該當前入侵之該指令碼因應係基於該已知入侵之歷史資料。

5. 根據申請專利範圍第1項之方法，其中該已知入侵與該當前入侵相異，且其中用於因應該當前入侵之該指令碼因應係基於該已知入侵之歷史資料。

6. 根據申請專利範圍第1項之方法，進一步包括：

使一建議指令碼因應清單與該入侵路徑圖形表示中之每一節點相關聯；及

爲該入侵路徑圖形表示中之每一節點選取該等建議指令碼因應之一。

7. 根據申請專利範圍第6項之方法，進一步包括爲該入侵路徑圖形表示中之每一節點選取一最高建議指令碼因應。

8. 根據申請專利範圍第7項之方法，進一步包括爲該入侵路徑圖形表示中之所有節點同時選取該最高建議指令碼因應。

9. 根據申請專利範圍第7項之方法，進一步包括：

根據一爲該入侵路徑圖形表示中所有節點選取所有最高建議因應的歷史模式自動執行申請專利範圍第7項所述之方法。

10. 根據申請專利範圍第1項之方法，進一步包括：

根據一用於手動啓動該指令碼因應之預期因應時間自動執行申請專利範圍第1項所述之方法。

11. 根據申請專利範圍第1項之方法，進一步包括：

根據該當前入侵的一嚴重性自動執行申請專利範圍第1項所述之方法，其中該指令碼因應係處於一與該當前入侵之嚴重性相稱之嚴重性等級。

12. 根據申請專利範圍第1項之方法，進一步包括：

根據該當前入侵的一類型分類自動執行申請專利範圍第1項所述之方法。

13. 根據申請專利範圍第1項之方法，進一步包括：

對一遠端接收器通知該當前入侵；及

響應該關於該當前入侵之遠程通知，遠程啓動該指令碼因應。

14. 根據申請專利範圍第13項之方法，其中該遠端接收器係

一無線裝置。

15. 一種管理電腦入侵之系統，該系統包括：

一圖形表示構件，其用於以圖形形式表示一已知入侵之入侵模式，該圖形表示包括一位於該入侵路徑中一節點處之指令碼因應；

一比對構件，其用於依據該電腦之一當前入侵與該已知入侵之入侵路徑中的至少一個共有特徵來比對該當前入侵與該已知入侵之圖形表示；及

一啓動構件，其用於根據該已知入侵與該當前入侵之比對來啓動一用於因應該當前入侵之指令碼因應。

16. 根據申請專利範圍第15項之系統，其中該入侵模式係基於入侵事件。

17. 根據申請專利範圍第15項之系統，其中該入侵模式係基於一受到該已知入侵影響之硬體拓撲。

18. 根據申請專利範圍第15項之系統，其中該已知入侵與該當前入侵基本相同，且其中用於因應該當前入侵之該指令碼因應係基於該已知入侵之歷史資料。

19. 根據申請專利範圍第15項之系統，其中該已知入侵與該當前入侵相異，且其中用於因應該當前入侵之該指令碼因應係基於該已知入侵之歷史資料。

20. 根據申請專利範圍第15項之系統，進一步包括：

一建立關聯構件，其用於使一建議指令碼因應清單與該入侵路徑中之每一節點相關聯；及

一選取構件，其用於爲每一節點選取該等建議指令碼

因應之一。

21. 根據申請專利範圍第20項之系統，進一步包括用於爲每一節點選取一最高建議指令碼因應之構件。

22. 根據申請專利範圍第21項之系統，進一步包括用於爲所有節點同時選取該最高建議指令碼因應之構件。

23. 根據申請專利範圍第20項之系統，進一步包括：

一自動執行構件，其用於根據一爲所有節點選取所有最高建議因應的歷史模式自動執行申請專利範圍第20項所述之方法。

24. 根據申請專利範圍第15項之系統，進一步包括：

一自動執行構件，其用於根據一手動啓動該指令碼因應之預期因應時間自動執行申請專利範圍第15項所述之方法。

25. 根據申請專利範圍第15項之系統，進一步包括：

一自動執行構件，其用於根據該當前入侵的一嚴重性自動執行申請專利範圍第15項所述之方法，其中該指令碼因應係處於一與該當前入侵之嚴重性相稱之嚴重性等級。

26. 根據申請專利範圍第15項之系統，進一步包括：

一自動執行構件，其用於根據該當前入侵的一類型分類來自動執行申請專利範圍第15項所述之方法。

27. 根據申請專利範圍第15項之系統，進一步包括：

一通知構件，其用於對一遠端接收器通知該當前入侵；及

一啓動構件，其用於響應該關於該當前入侵之遠程通知，遠程啓動該指令碼因應。

28. 根據申請專利範圍第27項之系統，其中該遠端接收器係一無線裝置。

29. 一種管理電腦入侵之電腦可用媒體，該電腦可用媒體包括：

一電腦程式碼，其用於以圖形形式表示一已知入侵之入侵模式，該圖形表示包括一位於入侵路徑中一節點處之指令碼因應；

一電腦程式碼，其用於依據該電腦之一當前入侵與該已知入侵之入侵路徑中的至少一個共有特徵來比對該當前入侵與該已知入侵之圖形表示；及

一電腦程式碼，其用於根據該已知入侵與該當前入侵之比對來啓動一用於因應該當前入侵之指令碼因應。

30. 根據申請專利範圍第29項之電腦可用媒體，其中該入侵模式係基於入侵事件。

31. 根據申請專利範圍第29項之電腦可用媒體，其中該入侵模式係基於一受到該已知入侵影響之硬體拓撲。

32. 根據申請專利範圍第29項之電腦可用媒體，其中該已知入侵與該當前入侵基本相同，且其中用於因應該當前入侵之該指令碼因應係基於該已知入侵之歷史資料。

33. 根據申請專利範圍第29項之電腦可用媒體，其中該已知入侵與該當前入侵相異，且其中用於因應該當前入侵之該指令碼因應係基於該已知入侵之歷史資料。

34. 根據申請專利範圍第29項之電腦可用媒體，進一步包括：

一電腦程式碼，其用於使一建議指令碼因應清單與該入侵路徑中之每一節點相關聯；及

一電腦程式碼，其用於爲每一節點選取該等建議指令碼因應之一。

35. 根據申請專利範圍第34項之電腦可用媒體，進一步包括用於爲每一節點選取一最高建議指令碼因應之電腦程式碼。

36. 根據申請專利範圍第35項之電腦可用媒體，進一步包括用於爲所有節點同時選取該最高建議指令碼因應之電腦程式碼。

37. 根據申請專利範圍第36項之電腦可用媒體，進一步包括：

一電腦程式碼，其用於根據一爲所有節點選取所有最高建議因應的歷史模式自動執行申請專利範圍第36項所述之電腦可用媒體。

38. 根據申請專利範圍第29項之電腦可用媒體，進一步包括：

一電腦程式碼，其用於根據一手動啓動該指令碼因應之預期因應時間自動執行申請專利範圍第29項所述之電腦可用媒體。

39. 根據申請專利範圍第29項之電腦可用媒體，進一步包括：

一電腦程式碼，其用於根據該當前入侵的一嚴重性自動執行申請專利範圍第29項所述之電腦可用媒體，其中該指令碼因應係處於一與該當前入侵之嚴重性相稱之嚴重性等級。

40. 根據申請專利範圍第29項之電腦可用媒體，進一步包括：

一電腦程式碼，其用於根據該當前入侵的一類型分類來自動執行申請專利範圍第29項所述之電腦可用媒體。

41. 根據申請專利範圍第29項之電腦可用媒體，進一步包括：

一電腦程式碼，其用於對一遠端接收器通知該當前入侵；及

一電腦程式碼，其用於響應該關於該當前入侵之遠程通知，遠程啓動該指令碼因應。

42. 根據申請專利範圍第41項之電腦可用媒體，其中該遠端接收器係一無線裝置。

拾壹、圖式：

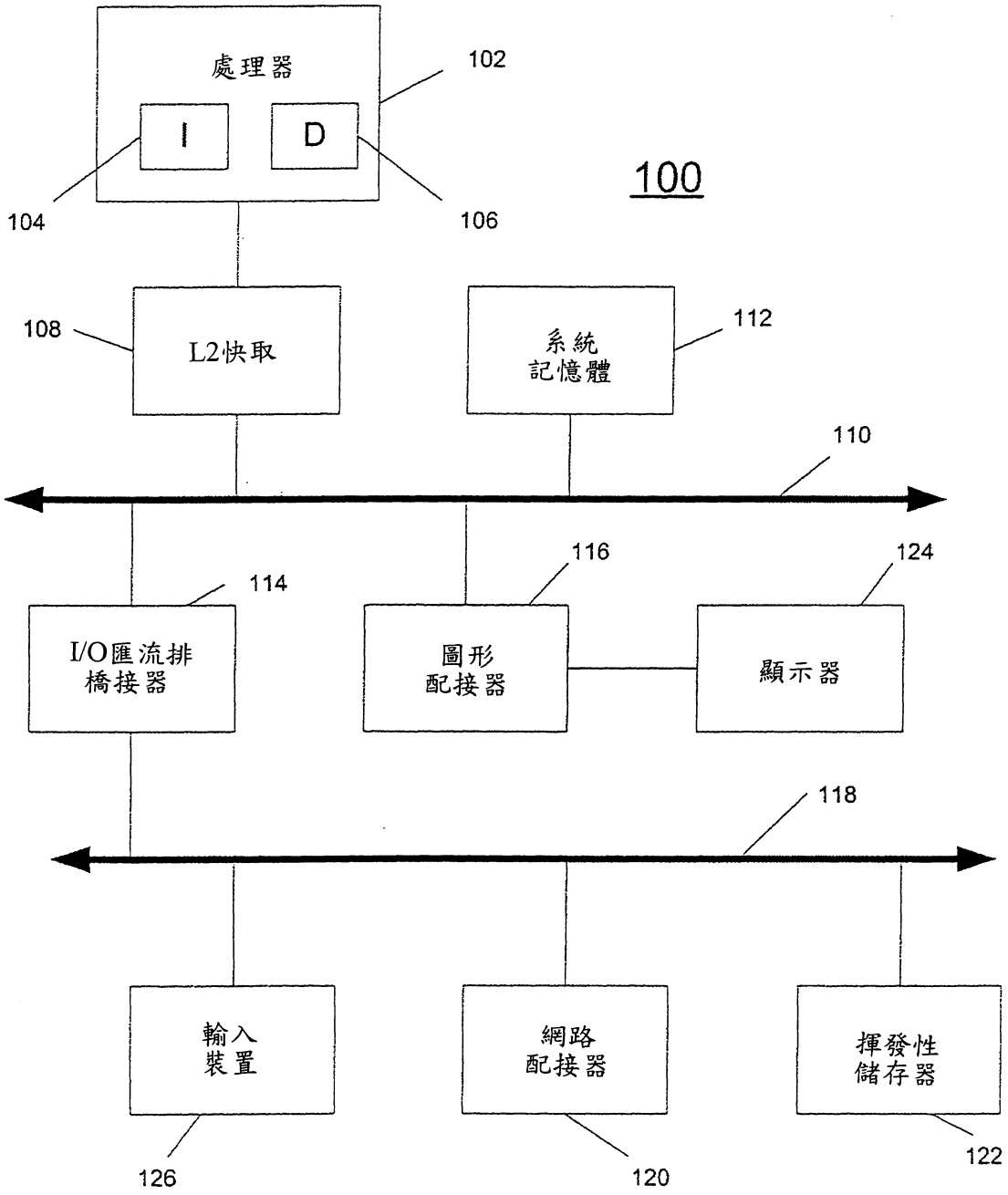
處理器
102
I
D
104
106
100
108
L2快取
系統
記憶體
112
110
114
116
124
I/O匯流排
橋接器
圖形
配接器
顯示器
118
輸入
裝置
網路
配接器
揮發性
儲存器
126
120
122

圖 1

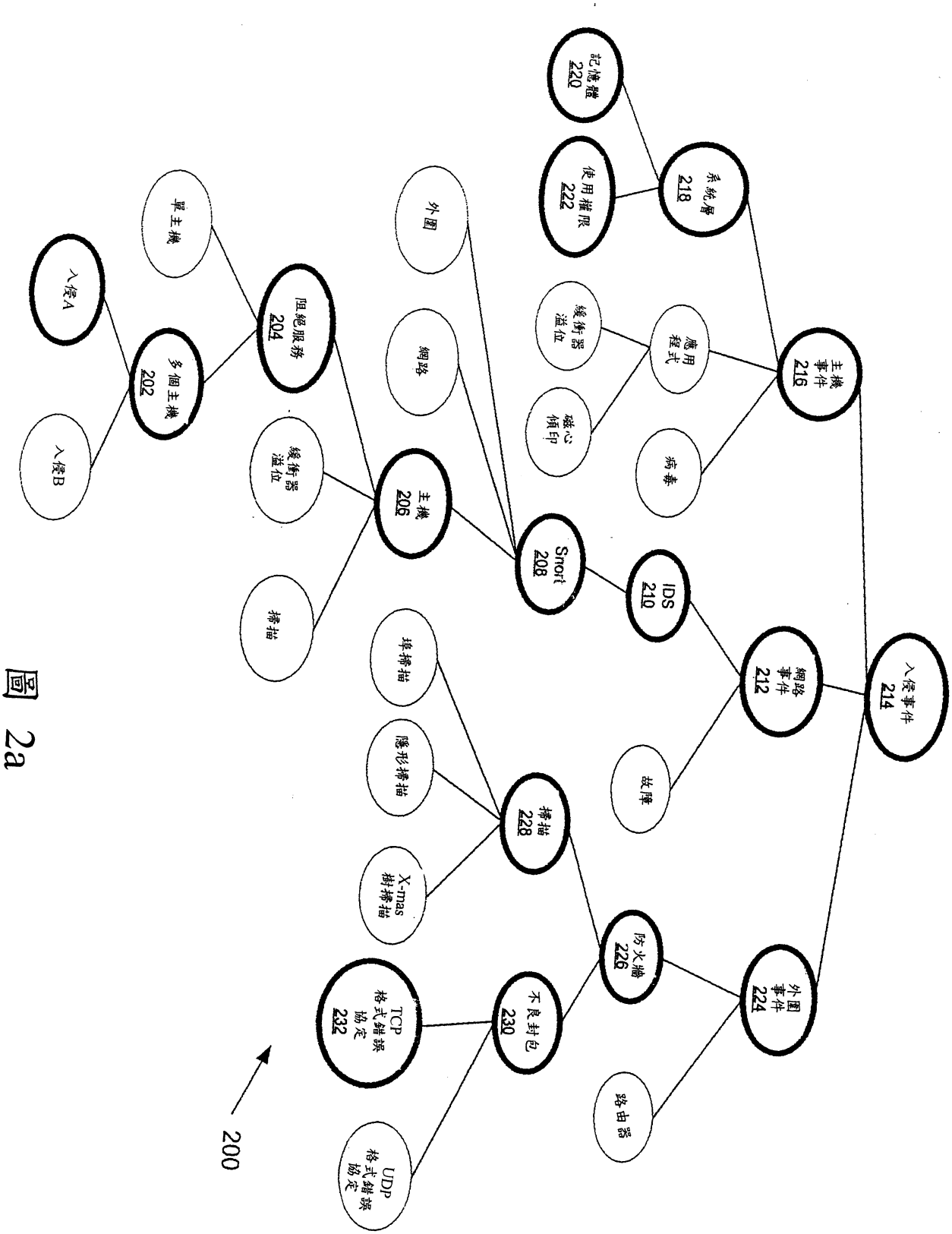
入侵事件 214
主機事件 216
網路事件 212
外圍事件 224
系統層 218
應用程式
病毒
緩衝器溢位
磁心傾印
使用權限 222
記憶體 220
Snort 208
IDS 210
故障
主機 206
網路
外圍
掃描
埠掃描
隱形掃描
X-mas樹掃描
阻絕服務 204
緩衝器溢位
單主機
多個主機 202
入侵A
入侵B
掃描 228
防火牆 226
不良封包 230
路由器
TCP格式錯誤協定 232
UDP格式錯誤協定
200

圖 2a

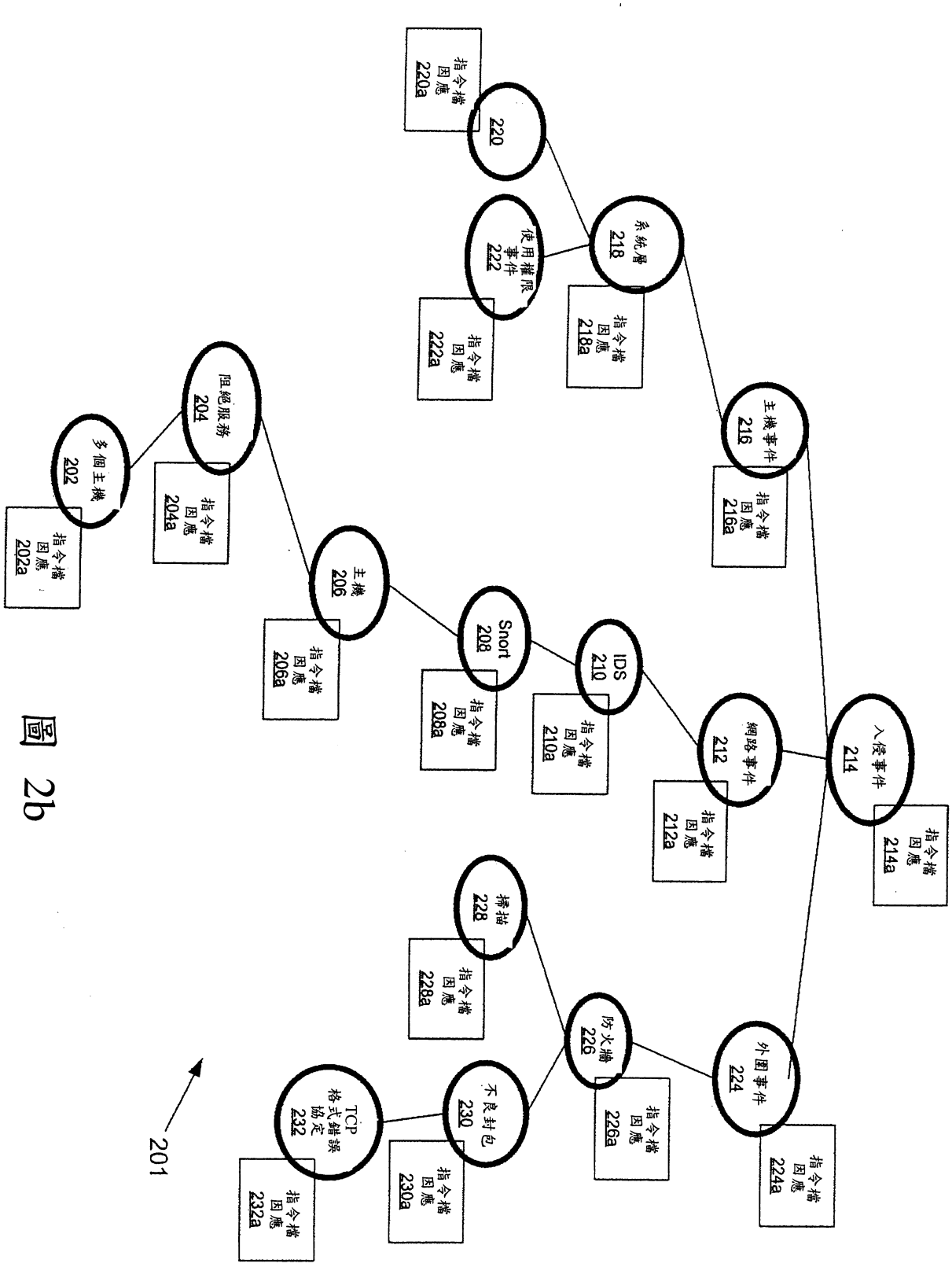
入侵事件
214
指令檔因應
214a
主機事件
216
指令檔因應
216a
網路事件
212
指令檔因應
212a
外圍事件
224
指令檔因應
224a
系統層
218
指令檔因應
218a
使用權限事件
222
指令檔因應
222a
220
指令檔因應
220a
IDS
210
指令檔因應
210a
Snort
208
指令檔因應
208a
主機
206
指令檔因應
206a
阻絕服務
204
指令檔因應
204a
多個主機
202
指令檔因應
202a
防火牆
226
指令檔因應
226a
掃描
228
指令檔因應
228a
不良封包
230
指令檔因應
230a
TCP格式錯誤協定
232
指令檔因應
232a
201

圖 2b

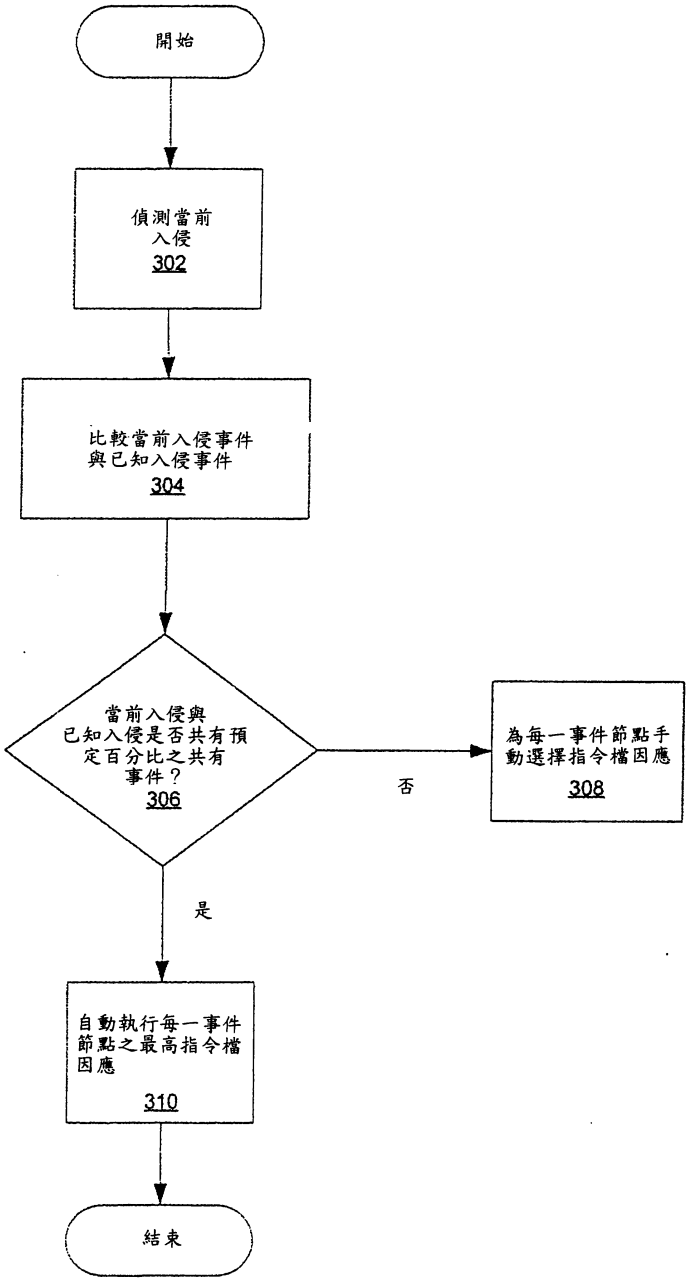
開始
偵測當前入侵
302
比較當前入侵事件與已知入侵事件
304
當前入侵與已知入侵是否共有預定百分比之共有事件？
306
否
為每一事件節點手動選擇指令檔因應
308
是
自動執行每一事件節點之最高指令檔因應
310
結束

圖 3

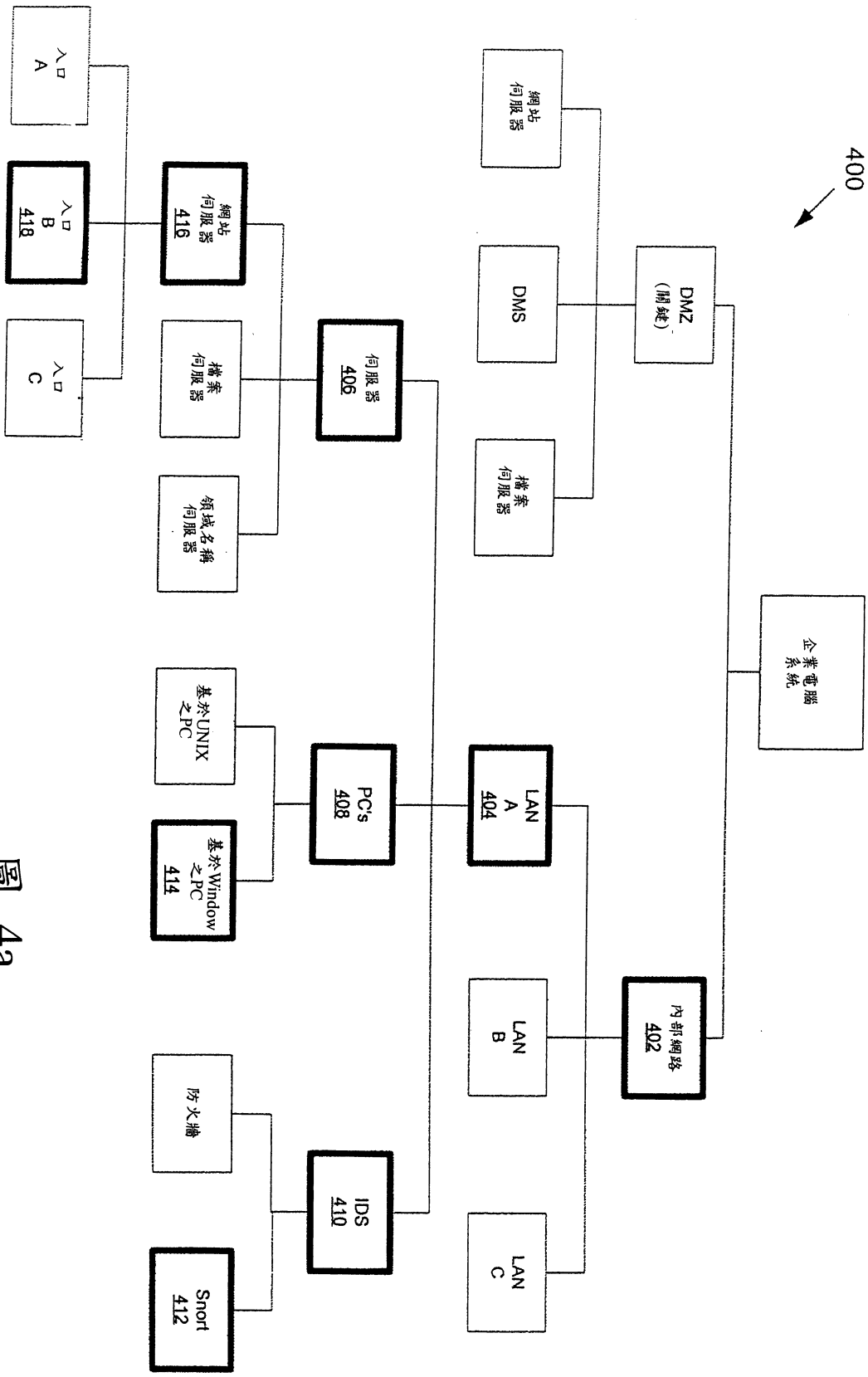
400
網站伺服器
DMS
檔案伺服器
DMZ（隔離）
企業電腦系統
內部網路 402
LAN A 404
LAN B
LAN C
伺服器 406
檔案伺服器
領域名稱伺服器
網站伺服器 416
入口 A
入口 B 418
入口 C
PC's 408
基於UNIX之PC
基於Window之PC 414
IDS 410
防火牆
Snort 412

圖 4a

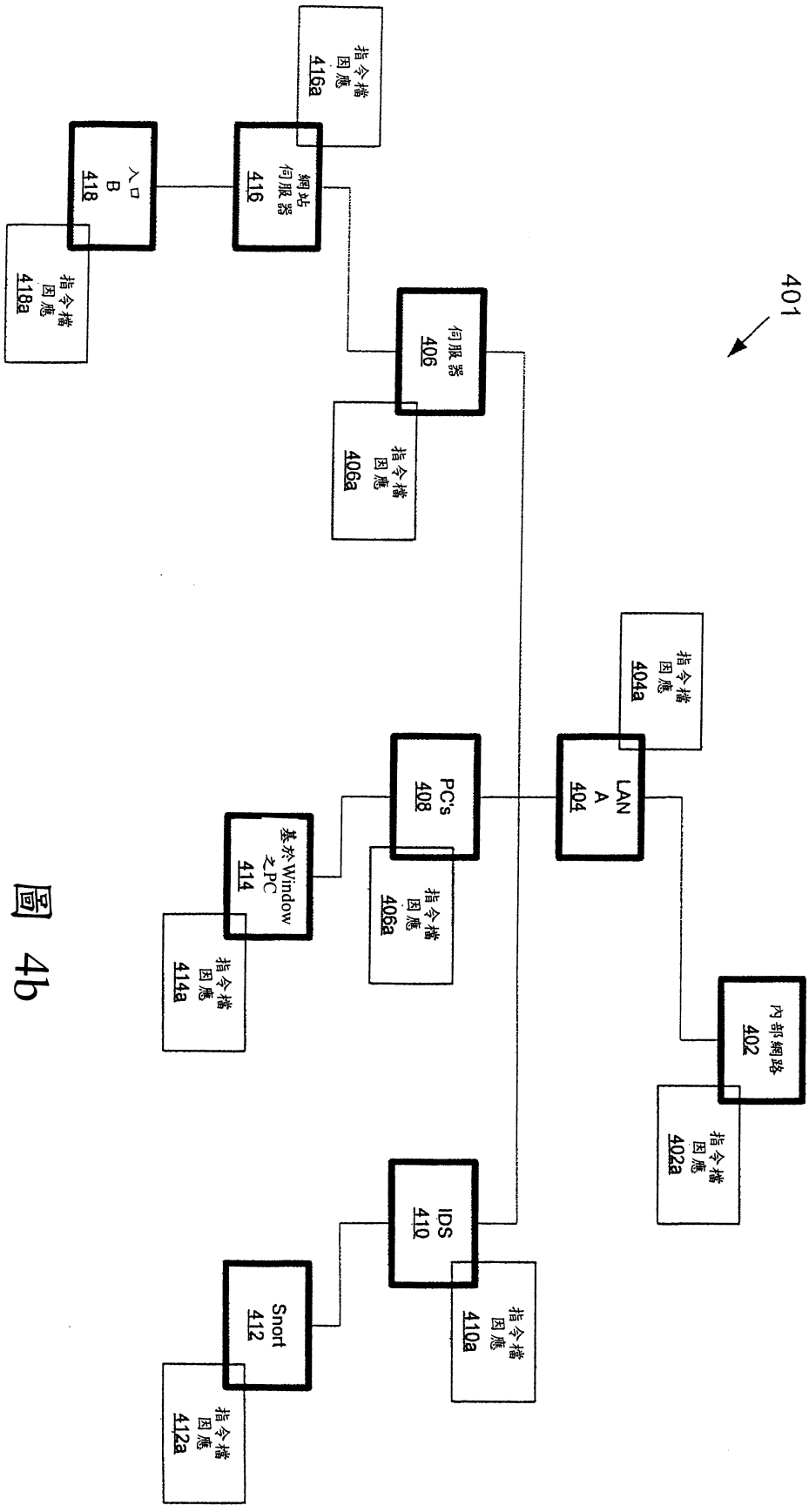
401
內部網路
402
指令檔
因應
402a
LAN
A
404
指令檔
因應
404a
PC's
408
指令檔
因應
406a
伺服器
406
指令檔
因應
406a
網站
伺服器
416
指令檔
因應
416a
入口
B
418
指令檔
因應
418a
基於Window
之PC
414
指令檔
因應
414a
IDS
410
指令檔
因應
410a
Snort
412
指令檔
因應
412a

圖 4b