申請日期	88.10.5
案號	88117342
類別	G06F 17/00

（以上各欄由本局填註）

公告本

A4
C4

498220

發明 新型 專利說明書

一、發明 新型 名稱	中文	資訊安全分析系統
	英文	INFORMATION SECURITY ANALYSIS SYSTEM
二、發明 創作 人	姓名	1. 麥克 P. 麥隆尼 2. 約翰 M. 蘇特 3. 克里斯多夫 J. 史考特 4. 法蘭西斯 M. 伍德茲 5. 里奇露伯 6. 約翰夫卡羅雪克
	國籍	美國
	住、居所	1. 美國馬里蘭州安阿魯多郡塞凡公園波庭園 248 號 2. 美國馬里蘭州安阿魯多郡帕沙第納戴洛大道 7873 號 3. 美國賓州中央郡普雷林特蓋帕史帝波蔡斯大道 265 號 4. 美國馬里蘭州巴爾的摩郡歐因斯米爾斯雪伍德農莊路 9733 號 5. 美國馬里蘭州安阿魯多郡葛倫柏妮福克斯山脈庭園 205 號 6. 美國馬里蘭州霍華德郡伍德賓舊站庭園 890 號
三、申請人	姓名（名稱）	美商・雷希恩股份有限公司
	國籍	美國
	住、居所（事務所）	美國麻塞薩諾塞州勒星頓水源街 141 號
	代表人姓名	大衛 L. 金辛爾

裝 訂 線

經濟部中央標準局員工消費合作社印製

（由本局填寫）

承辦人代碼：	A6 B6
大　　類：	
ＩＰＣ分類：	

本案已向：

國（地區）　申請專利，申請日期：　　案號：　　，☑有　□無主張優先權

本案已向美國申請專利；申請日：1998 年 7 月 21 日　案號：60/093,554 號

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

五、發明說明（　）

發明領域：

本發明係關於一種用來解決網際網路安全議題及電腦原始與可執行碼視覺化問題之資訊安全分析系統。此外，本發明亦關於一種用來攻擊及防守網際網路分析及商業與國家基礎設施的保護之資訊安全分析系統。

發明背景：

全球之網際網路的使用以一極快的速率持續的成長。使用者包括了政府，機構，商業，及個人，所有這些都為了進行日常的活動而連接至網際網路。很不幸地，被設計來讓網際網路成為一安全的通信(communication)方式之安全措施的發展及實施無法趕上在網路發展及相互連接性的擴張上之技術進步的腳步。其結果為，網際網路使用者及網路讓它們的資訊有受到駭客及懷有惡意之使用者危害的危險，這些人持續地在尋找方法來挖掘及破壞網路及資料。

如果被適當地使用的話，防火牆技術對於確保公司內的企業內網路(intranet)的"正門"的安全有所幫助，但這些技術卻無法趕上使用者對於應用，服務及安全性要求的腳步。雖然許多產品已被發展出來促進網路技術，但只有少數能夠被動地作用。

在政府及私人企業界中對於企業內網路安全性及監視需求正在持續增加。這在交易公告及網際網路組群中幾乎是被每天地被證實。更具體的證明在於對於與列在政府

（請先閱讀背面之注意事項再填寫本頁）
裝 訂 線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

提案中之要求技能相關之安全性需求持續增加。政府及私人企業都花費大量的時間及金錢來應付企業內網路映圖(mapping)，監視，指令偵測，及電腦安全。這已導致大量的公司提供企業內網路電腦安全性服務，分析工具，及相關的產品。

發明目的及概述：

本發明的系統被動地作用並提供一方法用來對在一監視期間被觀察到的資料執行一詳細的資料分析。

在不需要導入額外的運輸於一網路的前題下，本發明的系統產生網路使用及網路易受攻擊性的一視覺圖像。藉由將多個收及工具的輸入組織成視覺圖案，安全管理者在處理網路弱點及在確認執行安全措施的最佳地點上變成為早期主動(proactive)。藉由本發明的系統所送出的資訊，系統管理者可找出可能的運輸瓶頸，找到後門存在的位置，減少頻寬使用，確認使用者的輪廓，及找出不法的活動。

本發明的軟體系統包括了四個相互連接的模組：被動網路發現，網路資料記錄，網路資料剖析，及網路資料分析工具。網路資料視覺化能力是包含在被動網路發現及網路資料分析模組中。該軟體系統具有電腦碼分析及網路運輸與結構之3-D視覺及動畫。非必要之插入件(plug-in)進一步擴展及加強該軟體的能力，因此讓該軟體系統不論網路發展為何都能夠跟上潮流。

（請先閱讀背面之注意事項再填寫本頁）

裝

訂

線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

本發明的系統讓一網路管理者將該網路映圖(map)，決定正常與不正常的使用模式，找出病毒攻擊，管理網路配置，及顯示該網路。

更技術性地，該分析系統為在多個相互連接之電腦平台上之軟體程式的集合，結構及整合。該非電腦作業系統之軟體為感應器，分析，資料轉換及視覺化程式之組合。硬體平台包括了數種不同種類之相互連接的電腦，其經由一區域網路(LAN)分享軟體程式，資料檔案，及視覺化程式。此軟體的及合及整合及遷移至單一的電腦平台可獲致一種被動的及/或主動模式的 LA/WAN 監視方法。例如，路由器及防火牆軟體可以幾近即時的方式被監視用以決定碼是否不顧安全防備而被功能性地加以改變。包含在從資料鏈至 OSI 模式中之呈現層的通訊協定中之 LAN/WAN 資料可用來在二維及三維空間中分析。

該架構亦允許來自於用於分析之外部感應器，顯示器之數位資料輸入並讓源自於四個主要軟體概念組群的資料與顯示器相關連。這四個主要軟體概念組群為：病毒電腦碼偵測；電腦原始及可執行碼的分析；資料通信網路之動態監視；資料的 3-D 視覺及動畫。

本發明之分析系統以一圖形性的功能模式來顯示病毒電腦碼。目前的技術是依賴位元流或即時監視來偵測在主機(host)電腦中之電腦病毒。本發明之分析系統的方法檢查可疑的碼之功能性用以決定在該可疑碼於該主機電腦中執行之前決定一電腦病毒是否存在。該方法可被視為

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

推導出一起源結構，然後決定該起源結構是否存在一電腦程式，檔案，或電子郵件附件中。

再者，本發明的分析系統在多維空間中圖形地顯示及實施相似種類的電腦原始及可執行碼之間的比較用以決定該碼是否已經過單或多功能交替。該分析系統具有圖形分析，碼排序，及比較兩個或多個相似的原始碼及/或可執行電腦程式用以決定功能交替的程度。這可文件化的，圖形化的，動畫化的，動態的探究及決定在一單一的電腦原始或可執行碼中的功能。本發明的此一分析系統亦能夠藉由語言來將原始及可執行碼加以分類並將結果以圖形的功能格式顯示出來。例如，一路由器的過濾器圖表檔案可被週期地加以監視用以決定該檔案是否不顧標準的安全防備而被功能性地改變。

本發明的分析系統被動地發現數位資料通信網路的實體及虛擬的特性並同時以互動的方式顯示不同的數位通信網路。虛擬發現被定義為能夠決定該數位資料網路是如何被其參與者所使用及在任何一時間點決定誰連接到誰的能力。此處理亦決定在一可選擇的時間段中在數位通信網路中之外貌上的改變。以被動模式存在一 LAN/WAN 系統上之本發明的分析系統其在使用傳統的技術時是無法被偵測到的，其不需要使用者特權，其不消耗網路頻寬，且其不與在 LAN/WN 系統上之通信有界面。該分析系統能夠很快地映圖(map)SubNets 並在終端機活動增加時建構完整的網路。在該網路中之每一活動中的終端機目標

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

都被映圖且與隨附的資訊被顯示。該被顯示的資訊顯示實體與虛擬的關係，及網路上的符號。該分析系統亦可與網路探針結合在一起用以形成 LAN 系統之遠端監視，合作及發現。在此架構中，一終端機如一具有來自於遠端探針的輸入之主單元般地作用。在此操作模式中，一被動的操作模式可依照合作是在頻帶內(in-band)或在頻帶外(out-of-band)而停止或不停止。

本發明的此分析系統將接收自三個主要軟體組群之任何資料以三維或更多維的方式動態地顯示，旋轉，及動畫。在一實體及/或虛擬領域中同時觀看不同種類的數位資料是可能的。

根據本發明，每一種類的數位資料之相連性及功能性都被顯示。來自於該三個主要軟體組群中的每一者的資料可被顯示及旋轉於兩個或更多個不同但相連的視平面上的任何軸上。該處理亦顯示來自於該三個主要軟體組群之不同種類的資料之間的相連性用以包括來自於外部的感應器之資料輸入。該視覺化的軟體可附上使用者界定的符號(symbol)用以讓操作者或分析者更容易瞭解。該軟體經由一"滑鼠點選"及動態地揀取來與一節點互動，該軟體將與該節點相關連的資訊解碼並顯示，該節點是由該三個主要軟體組群所代表。在 3-D 節點圖變得很雜亂的例子中，分析者將數個節點縮為單一互連的共同節點。此能力提供分析者一不會雜亂之原始圖的代表，同時保持每個被濃縮的節點之功能性。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

A7
B7

五、發明說明（　）

圖式簡單說明：

藉由參照下文之參考了附圖之詳細說明後可對本發明有更完整的瞭解，其中：

第 1 圖為一根據本發明之用於被動網路資料發現，視覺化及分析之資訊安全分析系統的方塊圖；

第 2 圖為第 1 圖之資訊安全分析系統的應用流程圖；

第 3 圖為一方塊圖，其顯示與第 1 圖之資訊安全分析系統一起使用之發現工具的架構；

第 4 圖示意地顯示第 3 圖中之發現工具的一典型的資訊結構；

第 5 圖為第 1 圖之資訊安全分析系統的 3D 視覺化模組的方塊圖；

第 6 圖為本發明之資訊安全分析系統被用作為一侵入者偵測器的方塊圖；

第 7 圖為本發明之資訊安全分析系統被用作為一用來測試一節點攻擊或資訊劫奪之攻擊工具之方塊圖；及

第 8 圖為一顯型的顯示器，其顯示依據本發明之一物件導向網路視覺化。

圖號對照說明：

10	資訊安全分析系統	12	發現工具
14	資料通道	16	知識庫
18	資料剖析工具	20	分析引擎
22	2-D 顯示器	24	3-D 顯示器

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210 × 297 公釐）

五、發明說明（　）

32　感應器管理	34　工具程式組
36　內部封包處理引擎	38　草稿引擎
40　遠端管理器	42　遠端感應器
80　感應器管理工具	82　網路觀看工具
84　物件觀看工具	90　拓樸顯示工具
94　質詢顧問工具	86　封包觀看工具
88　知識瀏覽工具	92　審理記錄器工具
96　知識庫剖析工具組	100　視覺化預處理器
102　視覺化設定檔	104　鏈結資訊檔
106　場域鑰匙檔	108　軟體鏈結
110　3-D 翻譯引擎	112　顯示器
114　輸入裝置	46,48,50,52　終端機
54　防火牆	56　網路
58　網路分析器	60　終端機
64,66,68　節點	70　終端機
72　網路分析器	74　防火牆
76　防火牆	

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線

發明詳細說明：

參照第 1 圖，其顯示一資訊安全分析系統 10，該系統包括一發現工具 12 用來主動地或被動地經由一資料通道 14 來監視一區域網路(LAN)。功能上地，該發現工具 12 包括：感應器管理，被動網路發現(網路觀看者，網路拓樸)；封包分析器，知識庫觀看，及改變與報告。此外，

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

該發現工具 12 收集運輸及使用資料並映圖該網路相連性。被該發現工具 12 所收集的資料變成為貯存在記憶體中之知識庫 16 的一部分。資料被組織為以下的主類別：Address, Host, LM-Host, Domain, LM-Domain, SubNet, IP-Address, WWW, MAC-Address, NetwareHost, NetwareNetwork, NetwareStation, Alert, NetwareServer Type, Application, OS, WWW-Browser, WWW-Server, HTTP-Server, NNTP-Server, Protocol, User, POP3-User, FTP-User, SMTP-Sender, SMTP-Receiver, POP3-Passward, FTP-Password, Router,及 Vender。

在知識庫 16 中的資料對於一資料剖析工具 18 而言是可獲得的，該資料剖析工具將從該發現工具 12 所擷取的網路資料轉換為該系統之下游程式所使用的形式。被該剖析工具 18 所取得的資料然後可被分析引擎 20 所擷取，該引擎是用來分析被發現工具 12 所擷取之資料並支援數個資料檔案的合併及網路使用模式的發展與比較。該分析引擎 20 可由 i2 公司所售之商標名為"Analyst's Notebook"的軟體來執行，另一種由美國國防部所製之稱為 PROPELLER 的分析引擎 20 亦可被使用。本發明亦能夠在有其它的引擎可用時，使用額外的分析引擎。分析引擎 20 為用來捕捉及顯示多組被稱為一"鏈結圖"格式之相關資料組之圖形工具的一動態組。藉由使用分析引擎 20，如"Analyst's Notebook"，被收集的資料可被探究用以將網路特性特徵化及文件化及/或用以找出可能的網路入侵者。在

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準 (CNS)A4 規格 (210 × 297 公釐)

五、發明說明（　）

收集及組織資料後，月該分析引擎可被用來在多個不同的資料圖表之間建立連結用以決定是相互關連或彼此不同。然後，可得到資料來源間的關係及資料來源的矩陣用以證明假設，用以讓多個資料組間的關係彼此相關及用以在一大的資料組中辨識出目標資料。網路資料需要加以分析用以讓知識庫資料與審理(session)資料，封包資料，及警鈴資料相關連。這些關係有助於測定誰曾經與誰說過話，及特定通訊協定(HTP, HTTP, NNTP, POP3, SMTP, TRLNET 及 IMAP)的運輸內容。在分析網路資料的處理中，其會作出什麼 IP 及/或 MAC 位址對於一個以上的資料組而言是相同的之測定。將該網路以此方式加以特徵化需要在一段時間內對被捕捉到的資料作一週期性的快速掃描(snapshot)。平均之 IP 及 MAC 位址被用來產生一代表每一位址組之間的運輸之鏈結圖表。此處理可將一網路的一部分或整個網路特徵化。

藉由該分析引擎 20 的操作，經常被重復使用的資源可藉由一取樣技術來測定。一有興趣之時段被辨識出，其將透漏出在該時段期間被捕捉到共同的使用及資料。例如，為了要測定在早上 11 點至晚上 11 點之間的電子郵件運輸量，將會在數週的期間對每一天取樣直到運輸來源與目的地之相似性很明顯為止。在完成取樣之後，該分析引擎 20 可產生一圖表，其詳列在取樣期間被辨識出之所有的 IP 及/或 MAC 位址。

對於顯示經過分析的資料而言有數種選擇，其包括了

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

2-D顯示器22及3-D顯示器24。工具12及18的每一者，該分析引擎20及顯示器22與24都被功能性地連接至一操作者軟體介面用以從該資訊安全分析系統10的一操作者處接受指示。

第1圖的系統10接受數位形式之外部感應器資料(即，生物測定資訊，帳單資料，SS7，PBX，呼叫器資訊)。當外部資料與網路發現及分析工具結合時，就會有整體通信安全性處理的清析影像被提供。因此，本發明的分析系統將實體上的安全需求與電子通訊系統及IS/IT/CIO部門結合成為一完整的監看套件。

根據操作者的指示，該系統記錄及重播貯存在資料庫中之被選取的部分以供之後的事實分析及二維或三維的視覺化之用。這可適用於外部感應器及/或入侵偵測資料。

此外，第1圖的系統10可將HTP, HTTP, NNTP, POP3, SMTP, TELNET及IMAP審理以幾近即時的方式解碼。本發明之之模組架構容許插入件(plug-in)模組加入用以進一步強化及擴張通訊協定解碼以包括審理重建。此結構允許該系統10自動地測定在一網際網路上旅行之資訊的內容。此資訊然後被放入節點圖表中以供網路安全人員來測定什麼資訊需要進一步的保護。其亦可被用來回答像是：是否合法的生意在網計網路上被進行；如果雇員對另一個人產生任何侵害的話；雇員花費時間在網際網路上的什麼地方，等問題。

在該資訊安全分析系統的一個實施中，一以

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明(　　)

WindowsNT4.0 作業系統為平台之裝有至少 166MHz 速度的奔騰(Pentium)微處理器的個人電腦被使用。再者，該分析系統 10 包括 64MB 的 RAM，1GB 的硬碟機及一個 7 英吋的監視器。該資訊安全分析系統 10 之更快速的操作是藉由使用一 Pentium-II/300 或更快的微處理器及具有 128MB 的 RAM，一 4GB 的硬碟機及一 21 英吋的監視器來達成。

參照第 2 圖，其顯示第 1 圖之資訊安全分析系統 10 的一個應用的流程圖。一被動的資料發現引擎(發現工具 12)被用來收集有關於一網路的資料且一但發現，該資料即被加入到該知識庫 16 中。詳言之，該發現工具 12 收集資料用以抓住在二維或三維空間中之小的電腦原始碼及可執行碼節點圖表。此資料的收集能夠縮放及顯示大的電腦碼節點圖表藉此允許觀看及觀察在一支援數位資料通信網路的電腦設備之大的碼本體內之互連關係的彈性。透過發現工具來收集電腦原始及執行碼亦讓本發明的系統能夠在觀看在 3-D 空間中之相關的節點圖表時，綜合地模擬小的電腦原始及可執行碼程式。這讓本發明的系統能夠測定一有害的碼可能會在一程式中的何處，在一程式執行完之後確認該資料在記憶體中之位置，及使用圖形向量作為模板來找出特定種類的碼模組(亦即，病毒，編密碼法則)。此外，發現工具 12 收集在企業內網路(即(LAN/WAN)上的資料用以以二維的方式同步顯示該實體及虛擬網路圖表。這讓本發明的系統分析能夠立即地顯示一資料通信

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

網路之實體設備網連接。舉例而言，藉由執行一加總及減法程式，一系統分析人員能夠測定何時新的終端機及/或其外貌從該網路上被加入或移除，用以包括企業內網路"後門"之可能的辨識。在網際網路上之此資料的收集讓該系統有虛擬的企業內網路圖表，藉此能夠即時分析該網路是如何被使用，誰在與誰通信，測定可能的瓶頸點及易受攻擊處，有限的"追蹤路徑"重建及被要求的全球資訊網服務的種類。

此外，該發現引擎收集在網路上之結構資訊，該網路及網路使用者的操作方法。一典型的發現引擎從都多個感應器來將資訊定座標用以提供網路資料之有深度(in-depth)圖片。此外，該發現引擎除了所有與知識庫一起被產生作為"平攤檔(flat file)"之後設(meta)資料之封包之外，其還收集在一網路的作業期間上的資料。除了收集及分析 LAN 運輸之外該發現引擎亦可被建構成可收集及分析在其它種類的網路運輸上之資料，如 ATM，WAN 通訊協定，及行動電話通訊。

該發現引擎(發現工具 12)產生一關於此網路的資料之知識庫及此資料被貯存在一該發現工具 12 之一被貯存的資料目錄中之一被適當地命名的檔案中。來自於該發現引擎之該平攤檔的格式現被加以處理以供該資訊安全分析系統 10 之進一步使用。

此知識庫平攤檔是由一資料剖析工具 18 來處理，其使用該知識庫檔案的一關鍵字搜尋來產生在不同領域內

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

的資料。例如，資料被組織成不同的領域，如：獨特使用者辨識，主機，LM主機，界域(domain)，LM-界域，SubNet，IP位址，WWW，MAC-位址，NetWare主機，NetWare網路，NetWare站台及許多其它存在的領域。

除了將知識庫16組織成許多領域之外，該剖析工具18亦可產生碎址(hashed)輸出檔。

在剖析該知識庫16之後，該分析引擎20回應該資料用以將其準備及轉換成為向量基礎的節點圖。典型地，該分析引擎20產生數個不同的圖表之間的關係用以測定該等資料圖表是否為相互有關連或是彼此不同。介於資料來源的一陣列之間的關係被用來證明假設，用來在多資料組之間建立相互關係及用來在一大的資料組中辨識目標資料。根據此分析，該資訊安全分析系統10能夠允許資源的發展用以管理一網路。

該分析引擎20分析網路資料用以將知識庫與審理資料，封包資料，及警鈴資料相關連，而這些關係被用來測定誰曾經跟誰談過話及對於特定的通訊協定而言該交談的內容為何。

在分析被該發現工具12(發現引擎)所接收到的網路資料的處理中，什麼通信存在多於一個資料組中之測定是必需被實施的。以此方式來將該資料特徵化運用了對在一時段中被捕捉到的資料採取一期性的快速掃描(snapshot)的方式。然後對於什麼關係存在加以平均用以產生一代表資料組之間的運輸之鏈結圖表。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

參照第 3 圖，其顯示第 1 圖之一典型的發現工具 12 的架構，其被示於第 2 圖的應用流程中。一或多個感應器被一特化的感應器所控制用以提供設定，收集，及傳送控制。對於一地區乙太網路(Ethernet)感應器而言，一乙太驅動器位在該 NDIS 層之上用以提供網路資料之原生(raw)封包。資料的封包被一感應器管理器 32 所佇列(queue)，然後被提供至在工具程式組(suite)34 中的所有工具。一內部的封包處理引擎 36 將資料封包解碼並將該原生資料轉換為可被工具程式組 34 中的所有工具所取用之資訊元件。此外，一原稿(script)引擎過濾有興趣的資訊並將知識輸入到該知識庫 16 中。此資料庫亦可被工具程式組 34 中的所有工具所取用。

除了一特化的感應器之外，發現工具 12 亦包括遠端感應器 42 的控制。遠端管理器 40 需要遠端感應器，例如，一網輻(web)基礎的監視器及質詢工具，被提供給工具程式組 34 中的所有工具。

如在第 3 圖中所示，發現工具 12 被組織為一緊密地連結的感應器/處理器其是根據一可內部操作的工具程式組所形成的。這些工具提供進來的資料之視覺化，映圖，及分析及經過處理的知識。該感應器管理工具 80 提供在該發現工具 12 中之感應器的輪廓及控制，其允許資料在沒有被送至該發現工具下被收集(區域或遠端感應器)。感應器管理工具 80 之不同的態樣包括了提供根據該主機被分序(sort)在上層之感應器的觀看，在一領域中之所有感

本紙張尺度適用中國國家標準(CNS)A4 規格(210×297 公釐)

經濟部智慧財產局員工消費合作社印製

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（　）

應器資料的收集，讓資料能夠從感應器傳送至該發現工具，再次藉由被選取的領域而允許從一遠端感應器至該發現工具的通信，添加一新的(遠端)主機及相關的感應器至感應器管理工具控制。

該網路觀看工具 82 提供網路節點及鏈結之自動發現，自動佈局，及自動視覺化。節點為電腦運輸的來源，並包括伺服器，主機及客戶。鏈結為端對端運輸的代表，且可傳送至較高層級網路元件(如路由器)。該網路觀看工具 82 讀取封包資訊並提供一或多個邏輯網路的實體圖片。一邏輯圖片顯示為了多封包而被聚合之節點及鏈結資訊。因為網路運輸(及點及鏈結)存在於該 OSI 網路模組(資料鏈等等)的許多時候，所以有效的視覺化是藉由檢查在許多不同的層上之來源網路而產生的。在該網路觀看工具 82 的一個實施例中，在一圖窗上的圓圈代表節點及表示通信鏈結的線。當該發現工具 12 自動低發現更多節點時，每一網路的計數會出現在與一網路標簽一起出現在圖窗上。當該節點代表為樹枝狀時，該計數為所有在該參考節點之下的節點的聚合。與一來自於知識庫 16 之節點相關連的資訊將被顯示於該物件觀看工具 84 的窗口中。

該物件觀看工具 84 是與該網路觀看工具 82，拓樸顯示工具 90，及質詢顧問工具 94 整合在一起。該物件觀看工具 84 作動可被認為一物件之關於所有過渡關係(非位址基礎的)之資訊的顯示。例如，如果一 IP 位址與該使用者有關連，及一使用者與一主機位址相關連，然後這些都將

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

會是該物件觀看工具顯示的一部分。然而，如果該主機位址進一步與另一 IP 位址相關連的話，則此過渡關係就不會顯示因為在解釋關係時會造成混淆。在節點為物件及鏈結為關係之下，該物件觀看工具 84 產生以類別被排序之被顯示物件的名單。

資料封包及資料封包結構的分析是藉由封包觀看工具 86 的啟動而被提供。這提供了網路在網路封包的結構及其內部的資訊且亦有助於瞭解新的，不尋常的及/或私有的通訊協定。當封包觀看工具 86 被啟動時，一封包過濾器(未示出)被起始地設定用以允許所有經過更新的封包被捕捉到。當一使用者對某些封包種類有興趣時，該封包觀看工具 86 允許該使用者經由一封包過濾器設定對話來選擇某些封包次組。雖然該封包觀看工具 86 對於通訊協定偵錯及發展很有用，但此工具的功能性對於瀏覽新的封包種類亦是很有用的。

接下來，關於知識瀏覽工具 88，此工具為知識庫 16 的一視覺界面且提供一樹枝狀方法來瀏覽在該知識庫 16 中之分類內的項目，此外並提供連結資訊用以追蹤被該發現工具被動地發現於該網路上的物件及資訊。該知識瀏覽工具 88 讓需要簡單性之自動化及使用者可取用之方便性之工作的網路資訊能夠質詢，組織，及分類。

一被該知識瀏覽工具 88 所瀏覽過的類別為在該知識資料庫 16 內之一被分類的資訊之項目，且可包含次類別，物件或兩者。類別的例子有 IP-ADDR，MAC-ADDR，及

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

SMTP-發送器。在本發明中被認定為一物件者為一類別的組件且是該知識庫 16 中的一具有特定網路資訊的項目。

該發現工具 12 包括用來處理在被接收到的通訊協定內之資訊元件之該草稿引擎 38(如一分離的線串般運轉)用以收集關於在一網路中之智慧。標準的物件種類包括使用者，主機，界域，應用及位址，且拓樸規範允許新的物件被加入。使用單向或雙向結合來傳遞資訊(例如只機及使用者)，相互關連性是藉由使用資訊元件跨越多個通訊協定/物件種類來建立。根據本發明之功能，一網路變成為一包含在多次元空間中之鏈結的圖形，其中關係被貯存為此空間內之向量間的鏈結。

接下來，關於拓樸顯示工具 90，此工具提供一網路之被該發現工具 12 所辨識之元件之精巧的，被自動地產生的景像(view)。第 8 圖顯示在該拓樸顯示工具 90 作用時之一典型的視窗顯示。根據包含在該知識庫 16 中之資訊，該拓樸顯示工具 90 顯示路由器，SubNet，及使用者節點。再者，在該知識庫 16 中之分類的一次組可被架設於此景像之上。例如，主機名及易受攻擊性可被顯示。

審理記錄器 92 具有封包重新組合，TCP/IP 審理(session)管理，及知識發現的功能。該工具為一用來觀察無法輕易在封包層級被處理之多審理種類，例如：HTTP，POP3，SMTP，SNMP，TELNET，NNTP 及 IMAP。藉由重心組合封包並尋找跨越該等被重新組合的封包的資訊之主要特性，該審理記錄工具 92 提供能夠觀察並學習關於

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準 (CNS)A4 規格 (210 × 297 公釐)

五、發明說明（　）

在該網路上之應用層級實體(entity)。

在操作時，該審理記錄工具 92 重新組合關係導向的流動或審理。這些層-4(layer-4)(如 TCP)及上述的審理構成多封包，其將被重新組合及剖析用以找出應用層級資訊。封包及細胞重建技術提供使用者狀態資訊(如呼叫程式及審理監視)，及應用層級資訊(例如，電子郵件位址)。運用在該審理記錄工具 92 內之與警報處理結合的審理搜尋技術，可彈性地建構出能力(如看出何時一特定的使用者收到電子郵件)。在該審理記錄工具 92 的一個實施中，提供了觀看下列審理：HTTP，POP3，FTP，SMTP，TELNET，NNTP 及 IMAP。在該審理記錄工具 92 的操作期間，當該工具偵測，處理及掃描不同資訊片段之審理時，資料可被加至該知識庫 16 中。

該質詢顧問工具 94 提供一文字基礎的界面給該知識庫 16。藉由運用此質詢顧問工具 94，一使用者能夠測定該知識庫 16 是否包含一物件(例如個人的 IP 位址)或測定該組物件屬於該知識庫 16 的一個分類(例如，IP-ADDR)。在該質詢顧問工具 94 的一個實施中，該知識庫 16 被質詢上層分類名稱，物件屬於一已知分類及特定分類物件。

除了工具程式組 34 之外，該發現工具 12 包括一知識庫剖析工具組 96，如第 3 圖所示。從該網路上發現該資料之後，該資料然後被適當地格式化以供該分析引擎 20 之用。該知識庫剖析工具組 96 的功能是將該被收集的資料及將其置於該適當的格式中以供該分析引擎 20 之用。在

本紙張尺度適用中國國家標準(CNS)A4 規格(210×297 公釐)

經濟部智慧財產局員工消費合作社印製

（請先閱讀背面之注意事項再填寫本頁）

裝 訂 線

五、發明說明（　）

該知識庫剖析工具組 96 內之個別的工具能夠剖析來自於該知識庫 16 的資料並從被儲存的記載檔案(log file)及經過重新組合的審理檔案中抽取資訊。該知識庫剖析工具組 96 包含了 8 個工具：KB 剖析，電子郵件擷取，審理結合，網輻(web)擷取，圖形擷取，KB 加總，檔案處理，及欄位分割。

該網路發現工具產生資料該知識庫 16，該資料是有關於一網路。此資料被貯存在一平攤式文字檔案中且被儲存以供該發現工具 12 之再使用，以供一網路的顯示器之用。然而，該文字的格式對於接下來的處理並沒有用處。該 KB 剖析工具將該資料加以分析用以被輸出顯示在一欄位檔案中，用以被輸入至一資料庫，或分析以擎 20 中。此外，該 KB 剖析工具被用作為一關鍵字搜尋用以產生在不同領域中之資料。

如前所解釋的，該審理記錄工具 92 是一個用來觀察多審理種類並產生包含經過重新組合的審理資料之檔案的機制。在一單一資料收集期間內所產生之檔案數目可超過 10000 個。在該知識庫剖析工具組 96 內之電子郵件擷取工具提供將 POP3 及 SMTP 檔案組織成為摘要描述。該摘要描述然後被輸入一資料庫或該分析引擎 20 中。該電子郵件擷取工具包含一關鍵字搜尋機制及其它種類的資料剖析。

如前所述，該發現工具 12 產生一被收集之有關於一網路之平攤式檔案資料的知識庫。該知識庫剖析工具組 96

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

的網輻擷取工具有助於來自於 HTML 平攤式檔案資料的剖析及格式化，其然後被輸入至一資料庫或該分析引擎 20 中。該網輻擷取工具包含一標簽(與一關鍵字相似)搜尋機制及其它種類的資料處理法則。

該知識庫剖析工具組 96 的圖形擷取工具提供來自於一被記錄的格式之影像檔案的重新組合。審理記錄工具 92 的顯示提供 HTTP 審理的記錄。這些審理檔包含一說明該審理及與該審理相關之資料的檔頭。當一 JPG 或 GIF 影像被下載時，該資料於審理期間被重新組合。然而，此資料並無法以該被記錄的格式顯示。該圖形擷取工具將該經過重新組合的 HTTP 審理檔轉換成包含 JPG 及 GIF 資料並產生一包含名稱及影像之新的記載檔案。

被該發現工具 12 的操作而儲存在一平攤式文字檔中之資料被該知識庫剖析工具組 96 的 KB 加總工具所使用，用以產生被包含在封包及審理記載中之資料的一統計矩陣。例如，一通訊協定可被用作為 Y 入口(access)及 IP 位址可被用作為 X 入口(access)。在該封包或審理記載的選擇已被作成之後，該 KB 加總工具過濾適當的適當的記載檔案並顯示可用之取得準據(criteria)用以產生一圖。在一典型的網路的分析中，大量的檔案將會被產生。該知識庫剖析工具組 96 之檔案處理工具提供一界面用以減少必需被分序之檔案數量。其允許往案為了促進後續的處理而根據檔案的大小，種類，或內容被刪除或移除。被產生的檔案都根據適用於一組群中之所有檔案的一被選定之準據

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準(CNS)A4 規格(210×297 公釐)

五、發明說明（　）

來加以處理。

該發現工具 12 之被記錄的審理會偶爾被截斷並重新被儲存成為一新的審理。這些被截斷的審理最好是在被再次觀看之前加以重新組合。該知識庫剖析工具組 96 之審理結構工具將所有被截斷的審理結合成為完整的副本。

一分割資料欄位工具亦被包括於該知識庫剖析工具組 96 之內。該工具被用來將不要的資料欄位從記載檔中移除。

參照第 4 圖，其顯示在該知識庫 16 中之資訊的結構。該知識的定義及結構被考慮進去用以改進在處理網路資訊之前瞭解該知識的能力。第 4 圖為被該發現工具 12 組合於該知識庫中之資訊之有組織的分類圖表。該知識庫為一物件導向之關係實體其被儲存為一平攤式的文字檔且是從資料通道 14 上的封包被收集的資訊。

參照第 5 圖顯示該 3-D 顯示器 24 的一方塊圖，其包括一視覺化預處理器 100 用來從該分析引擎 20 接收原生 ASCII 資料。而且，經由一軟體鏈 108 輸入至該視覺化預處理器 100 的是一視覺化設定檔 102，一鏈結資訊檔 104，及一場域鑰匙檔 106。在處理來自於該分析工具 20 的資料之後，該視覺化預處理器 100 將該經過處理的資料輸送至一 3-D 翻譯引擎 110。該翻譯引擎 110 將該資訊根據來自於一輸入裝置 114 的使用者指示格式化並安排該資訊用以輸入至一顯示器 112。

經由使用頭裝式顯示器技術及六個自由度的軌跡系

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4 規格（210 × 297 公釐）

五、發明說明（　）

統來接收來自於該預處理器 108 的資料，一使用者將可體驗到在該網路內之用在該知識庫 6 中之資料加以辨識之完全的觀看印象。此技術提供使用者及能夠有進一步的能力來與該網路資料顯示器互動及交涉，其與傳統的平面顯示器相反。

再次參照第 1 圖，該 3-D 顯示器 24 加入一第三次元(dimension)至被該發現工具 12 所收集之任何資料用以在 3D 空間中觀看，動畫及分析複雜的節點圖。此有需要的因為該原生資料檔只包含兩個次元。如果來自於該等分析引擎的資料輸出三或更多次元的話，則 3-D 顯示器將不會需要添加一第三次元。一第三向量的添加允許根據來自於該失無入裝置 94 之使用者指示來同時觀看在相互連接的平面上之大的複雜圖。第 5 圖的顯示器允許一分析者在任何軸上旋轉該圖藉以觀看在二維平面上會被阻擋到之關係。

參照第 6 圖，其顯示被示於第 1 圖中之本發明的分析系統 10 的一代表性應用。該分析系統 10 是在一終端機 46 上被操作的，該終端機為一包含了終端機 48，50 及 52 的網路的一部分。該包括了終端機 46，48，50 及 52 的網路是經由一防火牆 54 而彼此相連。該防火牆 54 與一包括網路分析器 58 的網路 56 接觸。該分析器 58 為了與一回向(inbound)至該網路有關的入侵者的" 後設資料(meta data)"，而分析到達終端機及監視器的回向內的運輸。典型地，該分析器 58 建立與一回向入侵有關連之特定的後

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

五、發明說明（　）

設資料。如第6圖所示，網路56連接至一通路60及一終端機其代表入侵至終端機48之遠端入侵者。

在此例子中，將被假設的是，在終端機60上之遠端入侵者嘗試要送一電子郵件給在防火牆54之後的目標終端機48。運轉於終端機46上之本發明的分析系統10透過發現工具12監視乙太網路層級的回向電子郵件。該分析系統10將該回向電子郵件記錄為該知識庫16的一部分，如郵局通訊協定版本3(POP3)及簡單郵件輸送通訊協定(SMTP)。此外，該分析系統10檢查與回向電子郵件相關之後設資料並進一步檢查回向至該目標終端機48的SMTP/POP3封包。回向至該目標終端機48之經過辨識的SMTP/POP3被送至該分析引擎20以供其分析。如先前解釋過的，該分析引擎20輸入該由發現工具12送來之後設資料而加以分析及顯示。

參照第7圖，其顯示本發明之分析系統10在一多節點網路環境中之應用。如所示的，該網路包括節點64，66及68。連接至節點68的是一終端機70，第1圖之分析系統在該終端機上運轉。同樣連接至該終端機68的是一網路分析器72。每一節點64，66及68都連接至一防火牆74。防火牆74是在一連接至一廣域網路(未示出)之額外的防火牆76之後。

在此例子中，運轉於終端機70上之該分析系統10監視企業內網路運輸的層級並記錄來自於不同節點之每一終端機的資料封包。對一受到攻擊的終端機，如終端機

本紙張尺度適用中國國家標準(CNS)A4規格(210×297公釐)

經濟部智慧財產局員工消費合作社印製

（請先閱讀背面之注意事項再填寫本頁）

裝　訂　線

五、發明說明（　）

64a，而言該分析系統建立一目標來源封包結構並藉由可被修改之本發明的分析引擎 20 來關掉被攻擊的目標終端機。

應被瞭解的是，第 6 及第 7 圖只是應本本發明之分析系統 10 的兩個例子。該資訊安全分析系統 10 的其它使用包括了攻擊的及防守的資訊觀看，同時的電子郵件，FTP 及 TELNET 審理之關係節點視覺化，電腦原始碼及可執行碼的分析，實體及虛擬相連的區域網路或廣域網路之被動地及動態地發現，偵測一區域網路或廣域網路，如參照第 6 圖所描述者，內部與外部的入侵，自動警鈴並在一網路受到攻擊時採取改正動作，第 7 圖，及電腦病毒的偵測。

雖然本發明已根據一較佳實施例加以描述，但這並不是要將本發明的範圍限制於前述之特定的形式，相反的，是要涵蓋可能會被包括在下面申請專利範圍所界定的精神及範圍內之變化，修改及等效物。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4 規格（210 × 297 公釐）

A5
B5

四、中文發明摘要（發明之名稱：　　）

資訊安全分析系統

分析系統為在多個相互連接之電腦平台上之軟體程式的集合，結構及整合。該非電腦作業系統之軟體為感應器，分析，資料轉換及視覺化程式之組合。硬體平台包括了數種不同種類之相互連接的電腦，其經由一區域網路(LAN)分享軟體程式，資料檔案，及視覺化程式。此軟體的及合及整合及遷移至單一的電腦平台可獲致一種被動及/或主動模式的 LA/WAN 監視方法。該架構允許來自於用於分析之外部感應器，顯示器之數位資料輸入並讓源自於四個主要軟體概念組群的資料與顯示器相關連。這四個主要軟體概念組群為：病毒電腦碼偵測；電腦原始及可執

英文發明摘要（發明之名稱：INFORMATION SECURITY ANALYSIS SYSTEM　　）

The analysis system is a collection, configuration and integration of software programs that reside on multiple interconnected computer platforms. The software, less computer operating systems, is a combination of sensor, analysis, data conversion, and visualization programs. The hardware platforms consist of several different types of interconnected computers, which share the software programs, data files, and visualization programs via a Local Area Network (LAN). This collection and integration of software and the migration to a single computer platform results in an approach to LAN/WAN monitoring in either a passive and/or active mode. The architecture permits digital data input from external sensors for analysis, display and correlation with data and displays derived from four major software concept groups. These are: Virus Computer Code Detection; Analysis of Computer Source and Executable Code; Dynamic Monitoring of Data Communication Networks; 3-D Visualization and Animation of Data.

（請先閱讀背面之注意事項再填寫本頁各欄）
裝
訂
線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A5
B5

四、中文發明摘要（發明之名稱：　　）

行碼的分析；資料通信(communication)網路之動態監視；資料的 3-D 視覺化及動畫化。

英文發明摘要（發明之名稱：　　）

（請先閱讀背面之注意事項再填寫本頁各欄）
裝
訂
線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

1.一種資料通信網路的動態監視方法，該方法至少包含：

收集在一資料通信網路的實體及虛擬特徵上的資訊；

產生該被收集的資訊之知識庫；

剖析在該被產生的知識庫中之資訊用以產生在被選取的分類中之可讀格式的資料；

分析在該被選取的分類中之該資料用以產生關連性用以將資料通信特徵化；及

將該經過分析的資料視覺化用以測定該資料通信網路的參與者的使用。

2.如申請專利範圍第1項所述之資料通信網路的動態監視方法，其中產生一知識庫包括了一節點網路圖的建構。

3.如申請專利範圍第1項所述之資料通信網路的動態監視方法，其中產生一知識庫包括了測定內部及外部入侵的嘗試。

4.如申請專利範圍第1項所述之資料通信網路的動態監視方法，其中產生一知識庫包括了將該資料文件化及組織化成一網路功能的結構。

5.如申請專利範圍第1項所述之資料通信網路的動態監視方法，其中產生一知識庫包括了產生該被收集的資訊之

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

六、申請專利範圍

封包及次封包。

6.如申請專利範圍第1項所述之資料通信網路的動態監視方法，其中該收集資訊包括了收集資訊用以測定該通信網路在一已知的時間點之參與者的使用。

7.如申請專利範圍第6項所述之資料通信網路的動態監視方法，其中該收集資訊進一步包括收集在可被選定的時段中之該通信網路內之結構改變的資訊。

8.如申請專利範圍第1項所述之資料通信網路的動態監視方法，其中該分析資料包括了將該被收集的資料轉變為向量基礎的節點圖。

9.如申請專利範圍第1項所述之資料通信網路的動態監視方法，其中分析該資料包括了將該知識庫資料與該通信網路的審理(session)資料及封包資料建立起關連性。

10.一種資料通信網路的動態監視方法，該方法至少包含：

被動地收集在該資料通信網路的節點及鏈結之實體及虛擬特徵上的資訊；

產生該被被動地收集的資訊之知識庫；

剖析在該被收集的知識庫中之資訊用以產生在被選取的分類中之可讀格式的資料；

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部智慧財產局員工消費合作社印製
本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

六、申請專利範圍

分析在該被選取的分類中之該資料用以產生節點及鏈結的關連性藉以將該資料通信網路特徵化；及

將該經過分析的資料視覺化用以測定該資料通信網路的參與者的使用。

11.如申請專利範圍第10項所述之資料通信網路的動態監視方法，其中該將經過分析的資料視覺化包括了：

將一視覺化設定資料檔儲存起來，用以供應處理所需的資訊及資料；

將於該通信網路相關連的網路鏈結資料檔儲存起來；

在一選扯性的基礎上讀取每一該等被儲存的檔案；

將該被讀取的檔案資料傳送至一視覺化處理器；及

處理該被讀取的檔案資料及該經過分析的資料用以測定該資料通信網路的參與者的使用。

12.如申請專利範圍第10項所述之資料通信網路的動態監視方法，其中該經過分析的資料包括與該資料通信網路相關之連結性及功能性資料，及其中：

將該經過分析的資料視覺化包括將該連結性及功能性資料傳送至該視覺化處理器；

處理被讀取之檔案資料，該連結性及功能性資料用以產生用於顯示之網路資料訊號；及

在一 3-D 翻譯引擎中處理該被產生的網路資料訊號

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

六、申請專利範圍

用以輸出網路連結性及功能性顯示訊號。

13.如申請專利範圍第12項所述之資料通信網路的動態監視方法，其中將該經過分析的資料視覺化進一步包括了：

產生用來控制該3-D翻譯引擎之使用者輸入資料；

將該使用者輸入傳送至該3-D翻譯引擎；及

在該3-D翻譯引擎中處理該使用者輸入及該被產生的網路資料用以根據該使用者輸入來輸出網路連結性及功能性顯示訊號。

14.如申請專利範圍第10項所述之資料通信網路的動態監視方法，其中產生一知識庫包括了測定內部及外部入侵的嘗試。

15.如申請專利範圍第10項所述之資料通信網路的動態監視方法，其中該收集資訊進一步包括收集在可被選定的時段中之該通信網路內之結構改變的資訊。

16.如申請專利範圍第10項所述之資料通信網路的動態監視方法，其中將該經過分析的資料視覺化包括了將可由使用者界定之符號附在該經過分析的資料上。

17.一種動態監視多個資料通信網路的方法，該方法至少包

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

六、申請專利範圍

含：

收集在該等資料通信網路上的每一網路之實體及虛擬特徵上的資訊；

產生該被收集的資訊之一知識庫；

剖析在該被收集的知識庫中之資訊用以產生在被選取的分類中之可讀格式的資料；

分析在該被選取的分類中之該資料用以產生關連性藉以將該等資料通信網路中的每一者特徵化；及

將該經過分析的資料視覺化用以測定在任何時間點上該等資料通信網路之參與者的使用及互動。

18.如申請專利範圍第17項所述之動態監視多個資料通信網路的方法，其中分析該資料包括了網路系統的遠端監視，合作及發現。

19.如申請專利範圍第17項所述之動態監視多個資料通信網路的方法，其中視覺化該經過分析的資料包括了在一互動的架構中同時地顯示一或多個通信網路。

20.如申請專利範圍第17項所述之動態監視多個資料通信網路的方法，其中分析該資料包括了映圖次網路用以將網路重新架構為一網路繁殖中的終端機活動。

21.如申請專利範圍第17項所述之動態監視多個資料通信

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線

經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

A8
B8
C8
D8

六、申請專利範圍

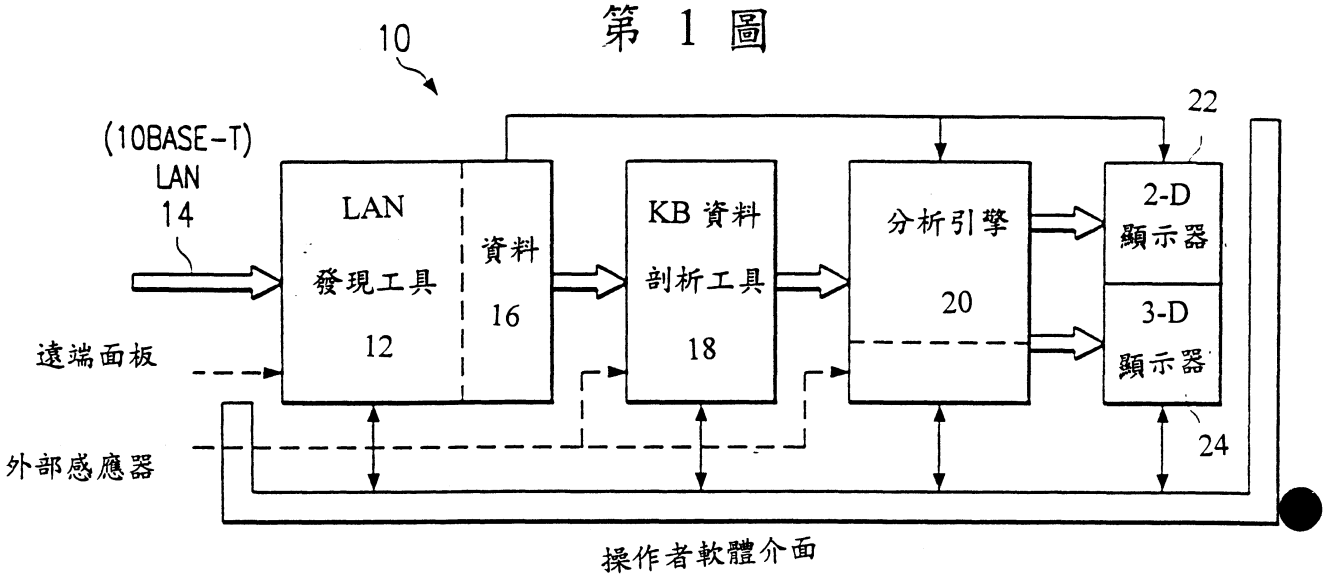
網路的方法，其中視覺化該經過分析的資料包括了顯示在一網路中每一活動中的終端機及節點，鏈結與附加的資訊。

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線

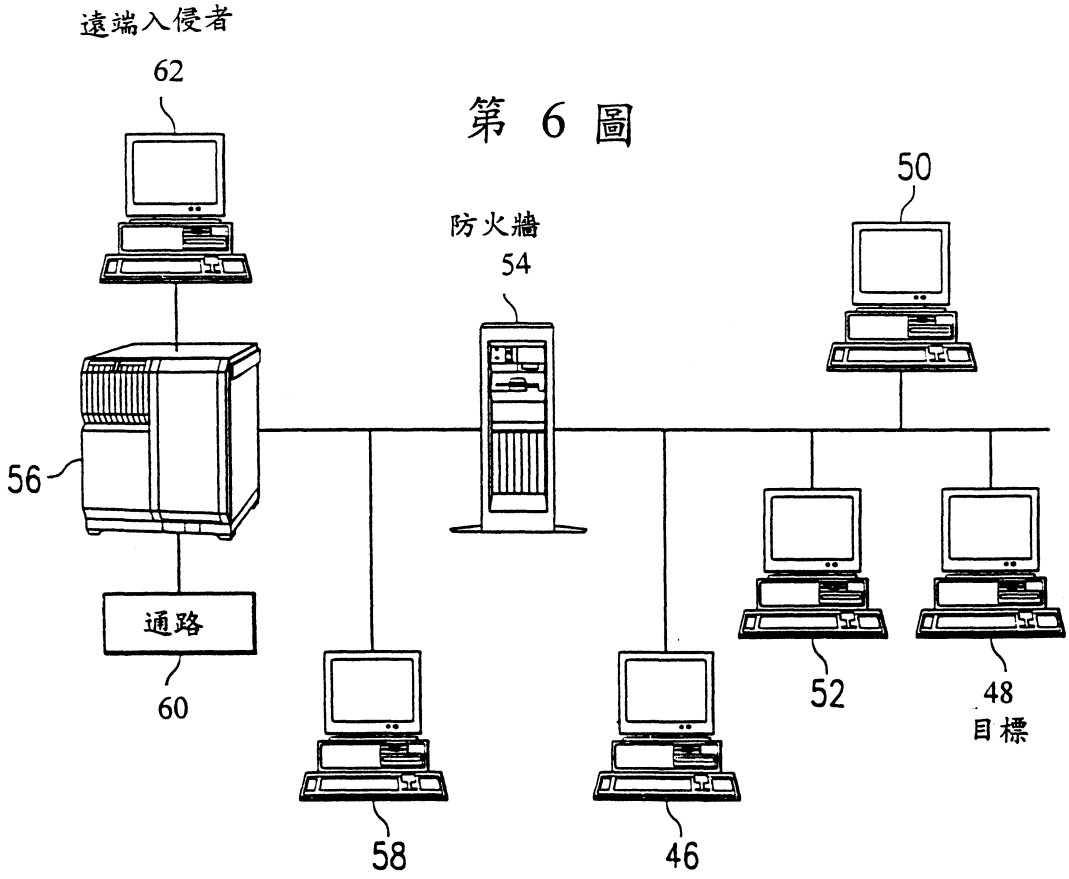
經濟部智慧財產局員工消費合作社印製

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

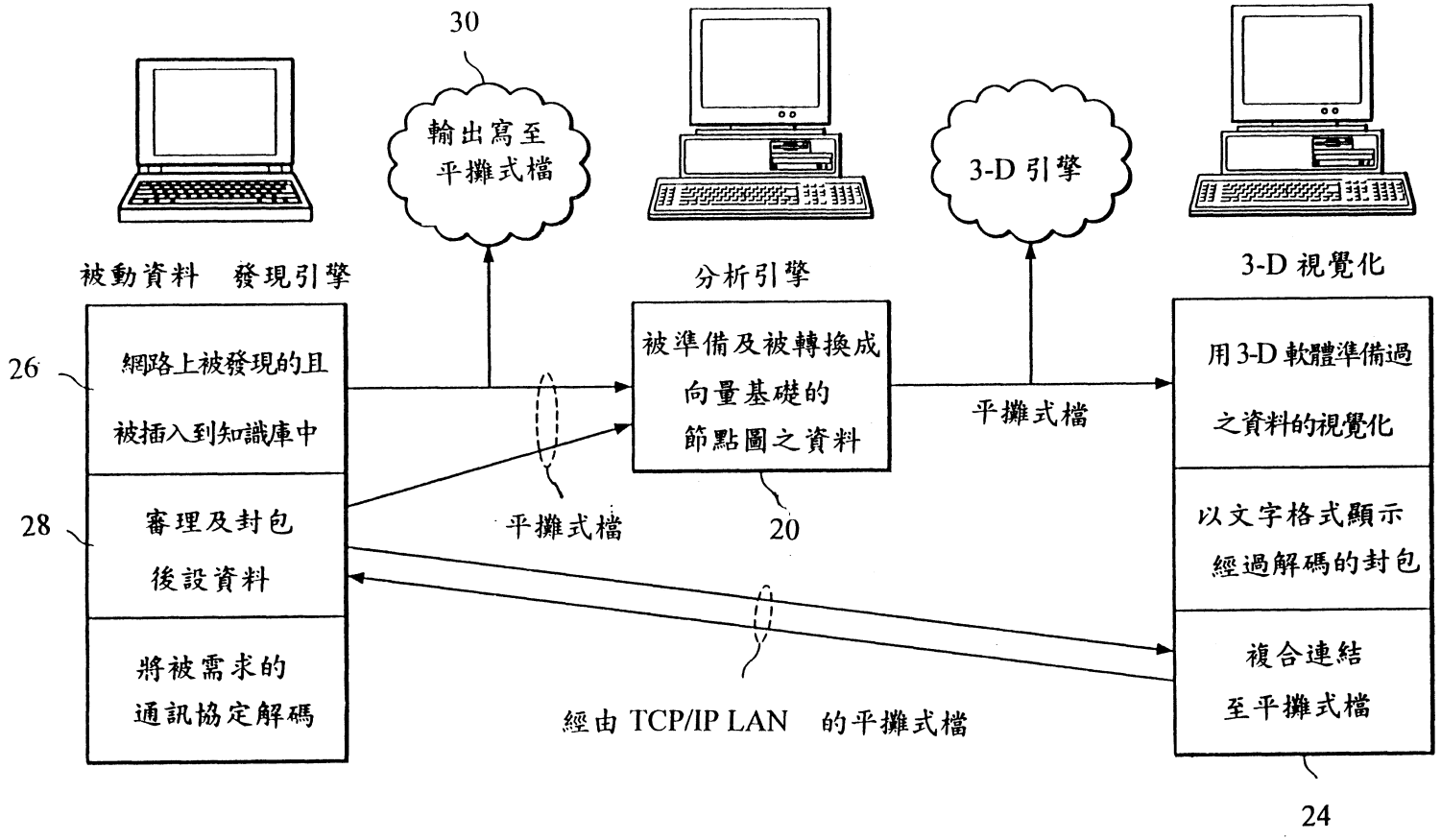
第 1 圖


10
(10BASE-T)
LAN
14
LAN
發現工具
12
資料
16
KB 資料
剖析工具
18
分析引擎
20
22
2-D
顯示器
3-D
顯示器
24
遠端面板
外部感應器
操作者軟體介面

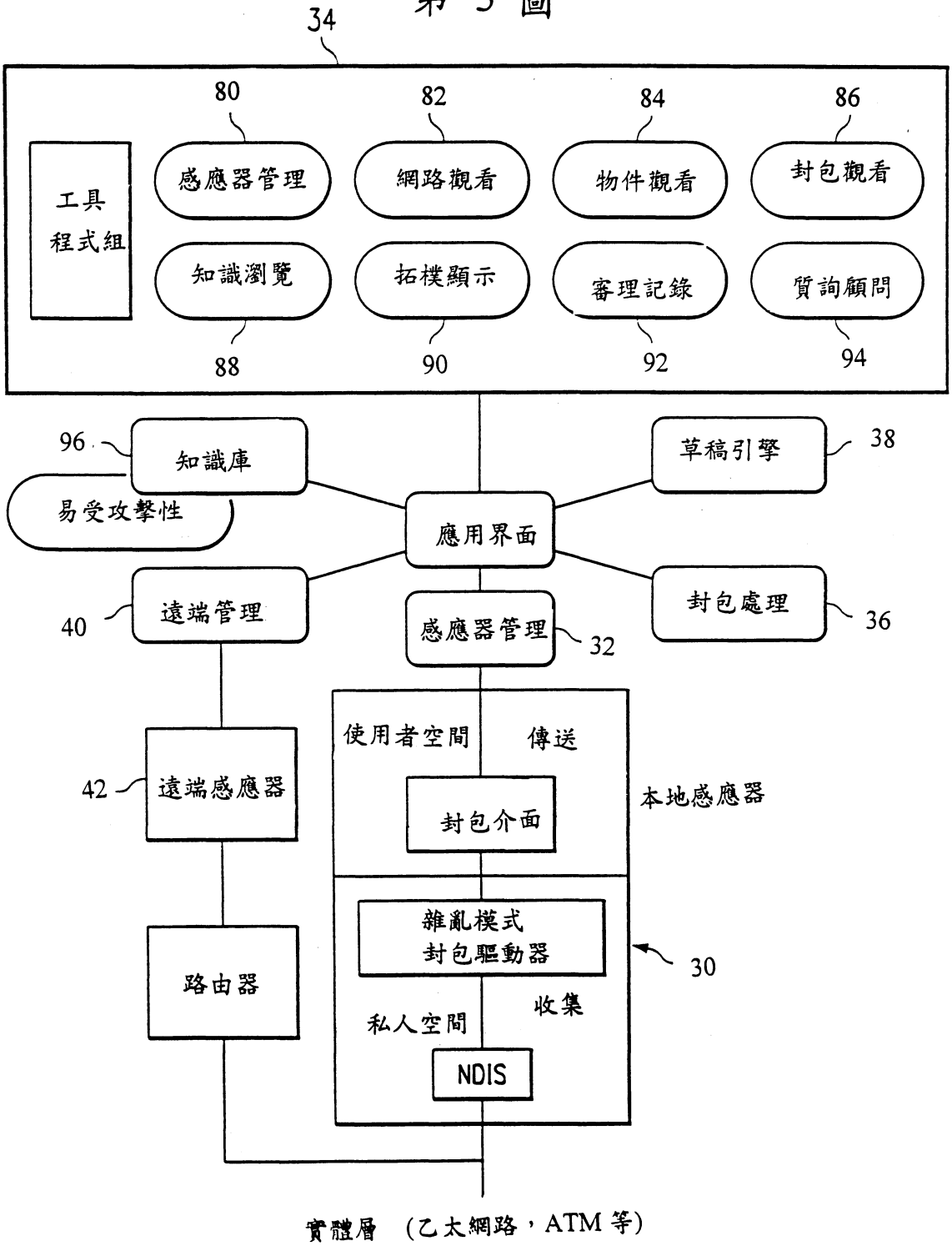
第 6 圖


遠端入侵者
62
防火牆
54
50
56
通路
60
58
46
52
48
目標

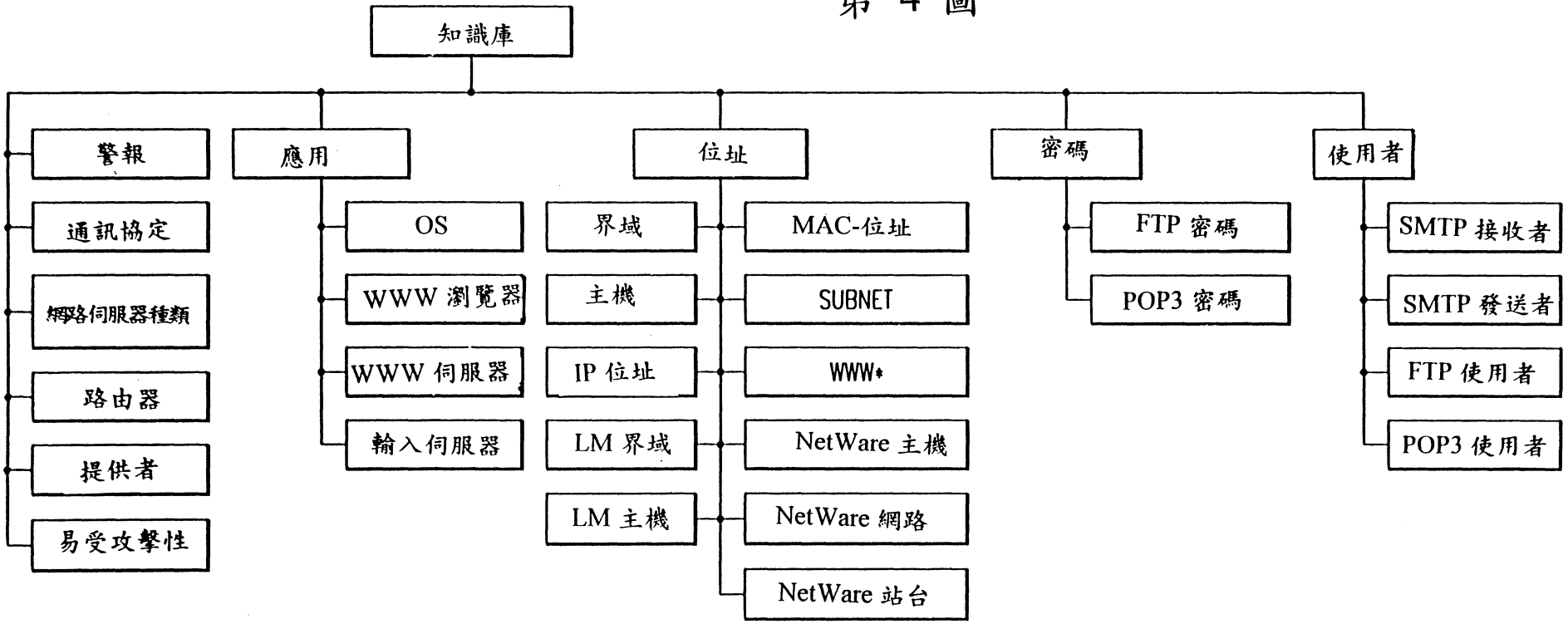
第 2 圖


30
輸出寫至
平攤式檔
3-D 引擎
被動資料 發現引擎
分析引擎
3-D 視覺化
26
網路上被發現的且
被插入到知識庫中
被準備及被轉換成
向量基礎的
節點圖之資料
用 3-D 軟體準備過
之資料的視覺化
平攤式檔
28
審理及封包
後設資料
平攤式檔
20
以文字格式顯示
經過解碼的封包
將被需求的
通訊協定解碼
複合連結
至平攤式檔
經由 TCP/IP LAN 的平攤式檔
24

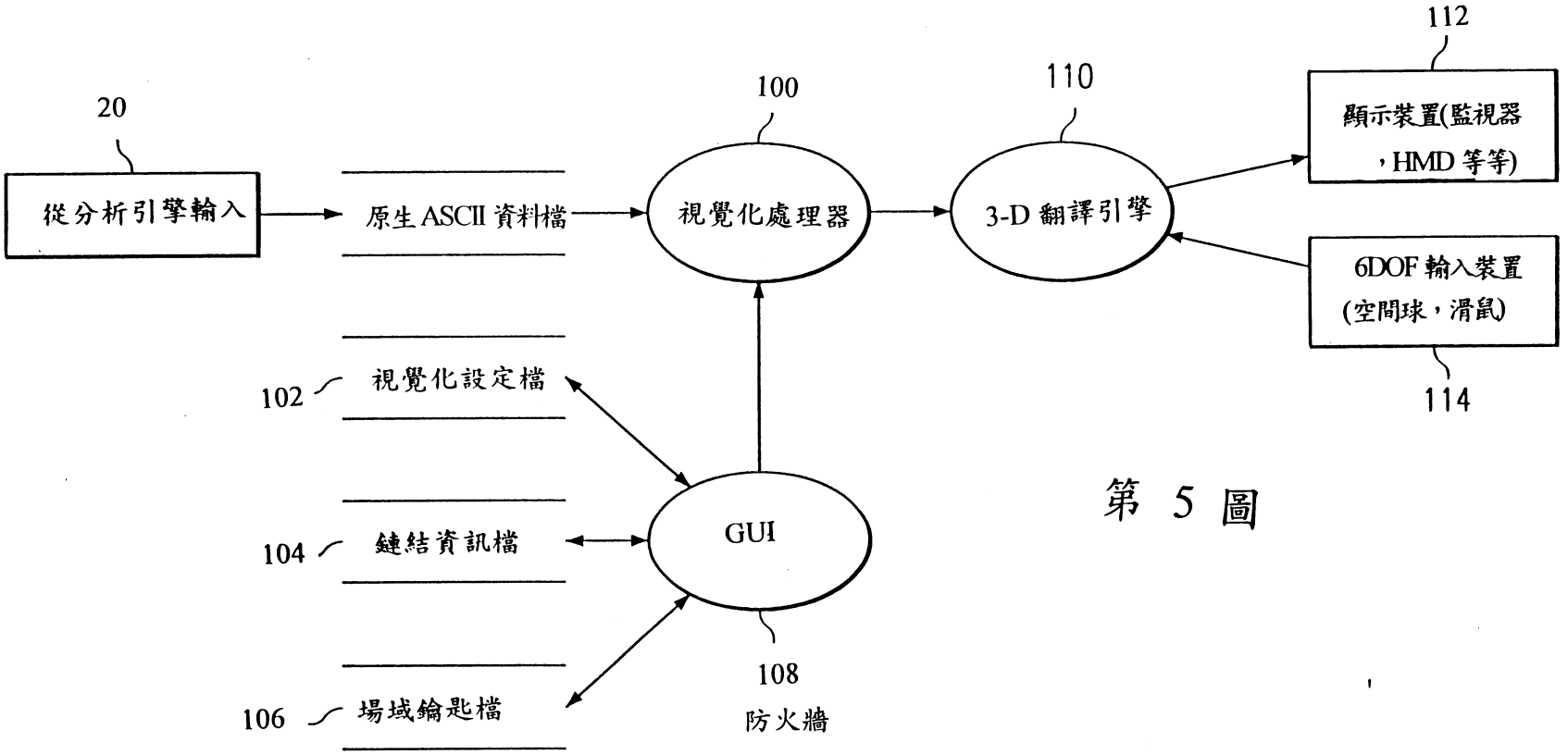
第 3 圖


34
80
82
84
86
工具
程式組
感應器管理
網路觀看
物件觀看
封包觀看
知識瀏覽
拓樸顯示
審理記錄
質詢顧問
88
90
92
94
96
知識庫
易受攻擊性
草稿引擎
38
應用界面
遠端管理
40
感應器管理
32
封包處理
36
使用者空間
傳送
42
遠端感應器
封包介面
本地感應器
雜亂模式
封包驅動器
30
路由器
私人空間
收集
NDIS
實體層 (乙太網路，ATM 等)

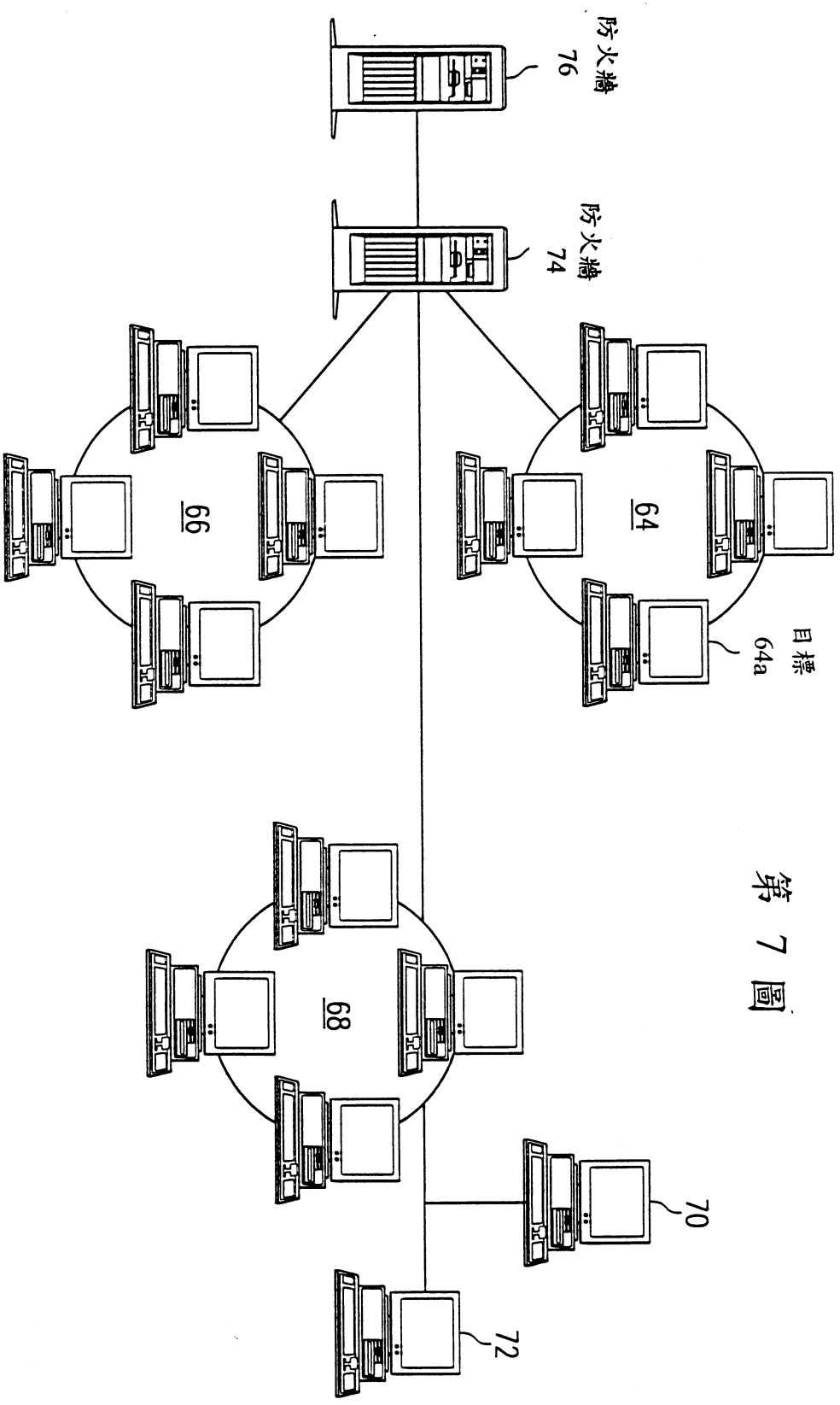
第 4 圖


知識庫
警報
通訊協定
網路伺服器種類
路由器
提供者
易受攻擊性
應用
OS
WWW 瀏覽器
WWW 伺服器
輸入伺服器
位址
界域
主機
IP 位址
LM 界域
LM 主機
MAC-位址
SUBNET
WWW*
NetWare 主機
NetWare 網路
NetWare 站台
密碼
FTP 密碼
POP3 密碼
使用者
SMTP 接收者
SMTP 發送者
FTP 使用者
POP3 使用者

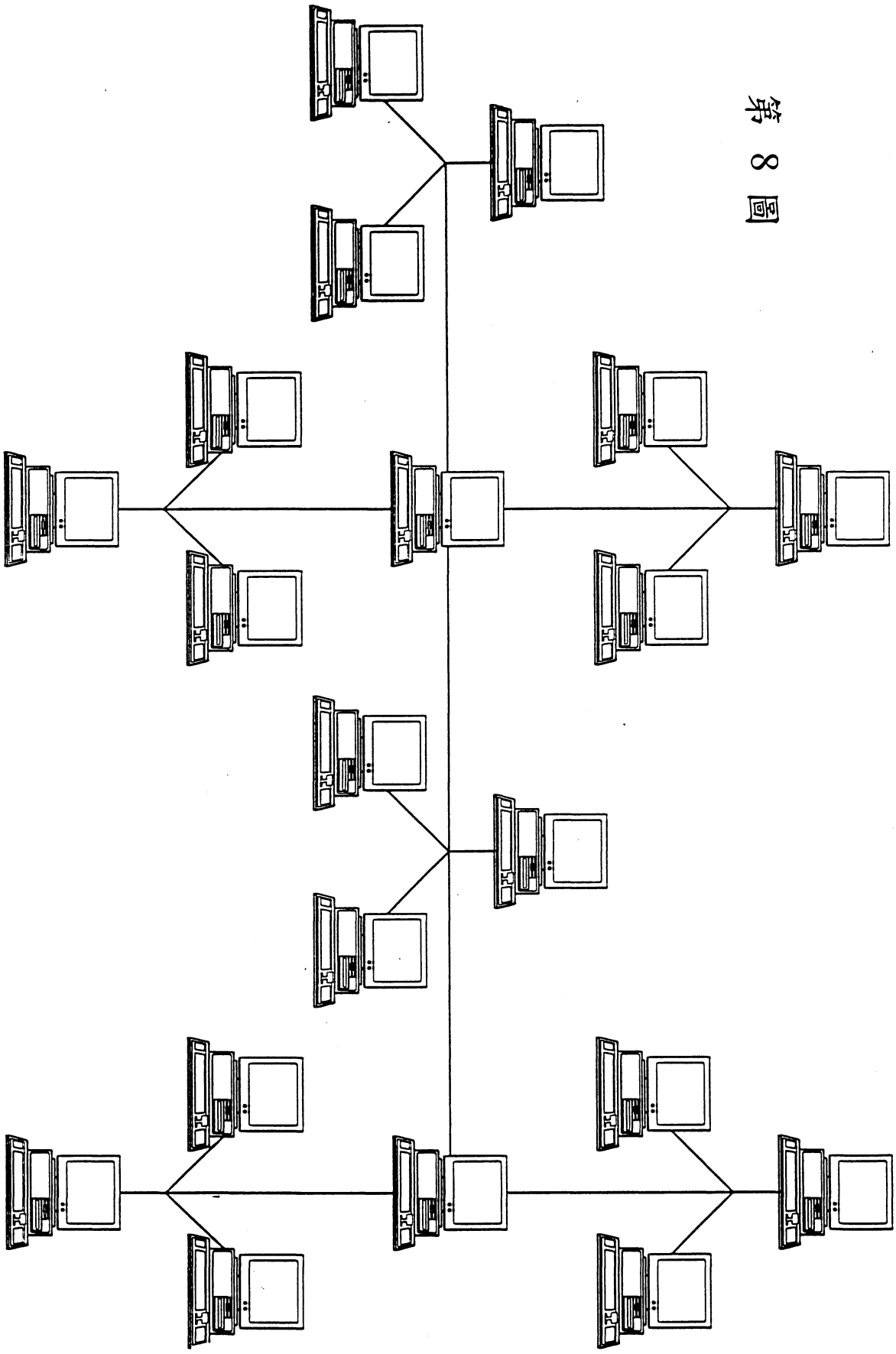
498220


20
從分析引擎輸入
原生ASCII資料檔
100
視覺化處理器
110
3-D 翻譯引擎
112
顯示裝置(監視器，HMD 等等)
6DOF 輸入裝置(空間球，滑鼠)
114
102
視覺化設定檔
104
鏈結資訊檔
106
場域鑰匙檔
GUI
108
防火牆

第 5 圖



第 7 圖



第 8 圖