（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

國（地區）	申請專利，申請日期：	案號：	，□有 □無主張優先權
美國	2000 年 2 月 8 日	09/500,269	☑有 □無主張優先權

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（1）

發明領域

本發明係關於網路之領域，尤其，本發明有關接達網路安全易損性的領域。

先前技藝

目前發展中之資訊系統與電腦網路的基礎建設現在於考慮何者構成一可接受風險(或者充足保護)的前題下建造。像是一電腦網路之硬體，軟體及系統節點等系統資產必須保護達到與其價值相一致的程度。此外，此等資產必須保護直到該資產失去其價值爲止。任何安全特性及系統架構應同時於所處理資料其有效期間提供足夠的保護。爲了接達與一網路相關聯之任何風險是否可接受，一安全工程師通常收集所有切合的資訊，然後分析與網路相關聯的風險。

風險分析爲一複雜而費時的處理，其必需決定一網路內曝露情況及潛在損害。如一例子中，當分析一電腦網路之安全風險時，安全工程師通常遵循以下步驟：

1)識別整個計算系統的資產。

2)識別資產易損性。此步驟通常需有影像，以便預測該資產可能發生何種損害，以及來自何種來源。電腦安全之三個基本目標爲：確保安全，完整性及可用性。易損性爲可能造成減損該等三項品質之一的任何情況。

3)預測意外(爆發)之可能性，即決定每隔多久爆發每一曝露情況。意外可能性與現存控制的嚴格度，及某人或某事躲避現存控制的可能性有關。

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

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）

4)藉由決定每項偶發事件之預期成本，計算每年的任何未涵蓋成本(預期年損失)。

5)審視可應用控制及其成本。

6)計劃控制的年積蓄。

分析的最後步驟爲一成本利益分析，亦即，實行一控制，抑或接受該損失的預期成本，何者花費較少？風險分析引導出一安全劃規，用以識別某些行動的責任，進而改善安全。

現今，隨著增加的威力，科技之快速演進及電腦之激增主導貨架外商用(COTS)硬體與軟體組件的使用，成爲划算的解決方案。此種與COTS的強烈相依性表示商用等級安全機構足夠因應大部分應用。因此，安全架構必須將加以建構，使其以相對較弱的COTS組件建造具有作業上關鍵任務的電腦系統。可將較高保證組件放置於社區或資訊邊界，形成一屬地式安全架構，用以實行通往資訊保證的一全面防禦途徑。

現存一些設計工具，亦即軟體程式，可協助系統設計師於剩餘之開發預算內將可用的保護機構予以最大化。目前一代之風險分析工具通常爲一單一販售商解決方案，闡述風險的某特定方面。此等工具常歸類爲三種類別之一：

1)從佐證之易損性資料庫進行工作，而且可能修復已知易損性的工具。此類型工具之資料庫更新仰賴販售商，可能透過新的產品版本，或者經由用户服務。此類別的例子包括：ISS' Internet Scanner，Network Associates，Inc.'s

（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（3）

CyberCop及Harris' STAT。

2)巨型工具，使用各種參數計算一風險指示器。此等工具很難維護，而且於快速發展之微兆及技術環境下，難以保持最新。此工具類別的一例子爲Los Alamos Vulnerability Assessment (LAVA)工具。

3)此類工具用以檢查像是作業系統或資料庫管理系統等系統某特定方面，但忽略其他系統組件。例如SATAN，用以分析作業系統易損性，但忽略像是路由器的基礎建設組件。

使用來自多種販售商之多重工具從事一單一電腦網路分析爲一勞力密集的任務。通常，安全工程師必須以多重格式，多次輸入系統(網路)的一描述或表示法。然後，安全工程師必須手動分析，聯合及合併來自此等多重工具之成果輸出成爲一網路安全狀態的單一報告。而後，安全工程師可完成風險分析(計算預期年損失，審視控制等等)，然後重覆該處理，而從安全風險，系統效能，任務功能及開發預算間分析替代選擇。

同時，此等工具均不使用系統的一聚合"快照"途徑，其中以一"向下鑽"或分層式途徑協助吾人如何闡述系統其各層次上(網路，平台，資料庫等等)的風險。從安全風險，系統效能及任務功能間分析替代選擇時，此等工具系統對工程師提供極少幫助。反而提供一種"風險解決方案"，其中闡述風險之特定方面，爲設計一給定工具用以計算而得。爲了開發一綜合的風險接達，安全工程師必須精通多

（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（ 4 ）

種工具之使用，而且以手動使成果輸出關聯化。

成功之風險分析的某一方面具有完整而且精確的資料累積，用以產生供分析工具使用的系統模型。目前許多風險分析工具取決於由使用者，系統操作員，及分析師所填寫的審視，用以要求資料，供開發分析中所使用的一系統模型用。替代上，一工具可主動掃描一電腦網路，以測試不利於系統組件的各種易損性。

然而，此等方法有其缺點。本文或審視式知識請求技術對於分析師而言不但勞力密集而且有點乏味。許多現存工具重覆使用相同資訊分析系統安全的不同方面。較佳者，使用一集中式模型資料貯藏處，可於現存工具間提供共享輸入的一基礎。此貯藏處可用以產生資料組，供風險分析工具使用，允許以相同系統爲背景運行多重工具，不需分開之輸入活動，因而減少操作員錯誤的可能性。使用多重風險分析推理引擎或後端允許對系統之各種方面進行分析，不需花費成本開發一工具執行所有類型的分析。整合資訊與藉由應用多重工具而提供之成果情報的接達可產生一較穩固而精確的系統安全狀態圖像。此等結果可協助更多情報系統設計決策，提供一框架，供替代評價及比較用。

因此，本發明的一目標爲：提供一種資料處理系統及方法，用以接達一網路之安全易損性，不需多次分析該網路。

本發明包括一種用以接達一網路之安全狀態的方法，包

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準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（5）

含以下步驟：建立一系統物件模型資料庫，其代表一網路，其中該系統物件模型資料庫支援不同之網路易損性分析程式的資訊資料需求；

僅將來自代表該網路之系統物件模型資料庫的所需資料匯出至每一各別網路易損性分析程式；

以每一網路易損性分析程式分析該網路，而從每一程式產生資料結果；

將來自各別網路易損性分析程式之資料結果及該共同系統模型資料庫儲存於一資料事實庫內，而且於資料事實庫上應用目標導向模糊邏輯決定規則，以決定該網路的安全狀態。

一種方法和資料處理系統現在已準備就緒，允許接達一網路之安全易損性。該方法包含建立代表一網路的一系統物件模型資料庫之步驟。該系統物件模型資料庫支援不同之網路易損性分析程式的資訊資料需求。於該方法中，僅將來自代表該網路之系統物件模型資料庫的所需資料匯入至每一各別網路易損性分析程式。以程式分析該網路，而從每一程式產生資料結果。將來自各別網路易損性分析程式之資料結果及共同系統模型資料庫儲存於一資料事實庫內。然後於該資料事實庫上應用目標導向模糊邏輯決定規則，以決定該網路的易損性狀態。

於本發明的又另一方面，該方法包含透過與各別網路易損性程式相結合之濾波器，僅匯入來自系統物件模型資料庫的所需資料，以及透過一整合應用程式規劃介面予以匯

（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（6）

入之步驟。於本發明的又另一方面，可將網路模型化成爲一圖形使用者介面的一映像。可設立一類別階層，用以定義網路易損性分析程式之組件，其中該等網路易損性分析程式共享共同資料和程式規劃特點。同時可獲得屬於網路系統細節，網路拓樸，節點層易損性和網路層易損性之資料結果。

方便的是，一電腦程式常駐於一媒體上，而且可藉由一程式讀取，並且包含指令，用以引發一電腦建立一系統物件模型資料庫，其代表一網路，而且支援不同之網路易損性分析程式的資訊資料需求。一電腦程式引發該電腦僅將來自系統物件模型資料之所需資料匯入至每一各別網路易損性分析程式，而且以每一網路易損性分析程式分析該網路，而從每一程式產生資料結果。將該結果與該共同系統模型資料庫儲存於一資料事實庫內。該電腦程式同時建立指令，用以引發一電腦於資料事實庫上應用目標導向模糊邏輯決定規則，以決定該網路的易損性狀態。

一種資料處理系統接達一網路之安全易損性，而且包括複數個不同的網路易損性分析程式，用以分析一網路。一系統物件模型資料庫代表所分析之網路，而且支援網路易損性分析程式的資訊資料需求。一應用程式規劃介面將該網路之系統物件模型資料庫匯入至網路易損性分析程式。一濾波器與應用程式規劃介面及每一各別網路易損性分析程式相結合，其中網路易損性分析程式用以過濾來自系統物件模型資料庫之資料，而且僅匯入所需資料。

（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）

五、發明說明（7）

於分析該網路及共同系統模型資料庫後，將從各別網路易損性分析程式所獲得之結果儲存於資料事實庫，而且一模糊邏輯處理器藉由使用複數個模糊匯出規則，於事實資料庫上應用目標導向模糊邏輯決定規則，以合併來自網路易損性分析程式之結果，而且決定該網路的易損性狀態。

以下本發明現在將藉由例子，參照附圖，加以描述，其中：

圖1爲一網路的一示意方塊圖，顯示網路上經常發現問題之位置。

圖2爲一網路的另一示意方塊圖，顯示一識別之易損性，其係藉由本發明之系統及方法加以定位。

圖3爲另一方塊圖，顯示本發明之系統及方法的整體架構，同時顯示結合網路模型資料庫所使用的濾波器。

圖4爲本發明其架構的另一示意方塊圖，顯示模糊邏輯分析。

圖5爲另一示意方塊圖，顯示本發明之資料處理系統及方法的高階架構組件。

圖6爲本發明之資料處理系統的另一高階示意方塊圖。

圖7爲一圖形使用者介面的例子，其將網路模型成爲一映像。

圖8A和8B顯示放開式視窗，其提供於設立系統物件模型資料庫時的資料解析。

圖9爲一圖形使用者介面的例子，顯示該網路模型。

圖10爲一圖形使用者介面，顯示網路之安全狀態的各種

（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（ 8 ）

報告選項。

圖11爲一方塊圖，顯示目標導向模糊邏輯處理的基本處理組件，其中該目標導向模糊邏輯處理用於本發明之資料處理系統及方法。

圖12爲資料融合的一示意方塊圖，其中該資料融合用於本發明之資料處理系統及方法。

圖13爲另一示意方塊圖，顯示黃金式融合規則的一例子，其中該黃金式融合規則用於本發明之資料處理系統及方法。

圖14爲另一方塊圖，顯示模糊邏輯處理中所使用的邏輯處理基本處理步驟及組件，其中該模糊邏輯處理用於本發明之資料處理系統及方法。

圖15爲一方塊圖，顯示故障樹分析(DPLf)中所使用的基本組件，其中該故障樹分析(DPLf)用於證據累積與模糊證據推理規則。

圖16爲一方塊圖，顯示一物件/類別階層。

圖17爲一方塊圖，顯示本發明之系統類別圖。

圖1說明一傳統網路100的例子，其中具有內部伺服器102，連接至一外部路由器104，通訊網路105，及防火牆106。一內部路由器108連接至防火牆106，分公司107，同時連接至內部區域網路(LAN)之網路組件110以及一遠端存取伺服器112和遠端使用者114。

使用圖1中的例子，網路上經常發現之問題包括：主機，像是內部伺服器102，其中運行像是拒絕服務的不必

（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（9）

要服務；以及匿名FTP或不當配置的網路伺服器，其中的網路伺服器可爲一內部伺服器，例如CGI劇本，匿名FTP及SMTP。內部區域網路(LAN) 110可能包括未修補，過時，易損或內定配置之軟體和韌體以及弱密碼。區域網路(LAN)同時可能包括不當之匯出檔案共享服務，像是NetWare檔案服務及NetBIOS。內部區域網路(LAN) 110同時可能包括不當配置或未修補之視窗NT伺服器，以及由於缺乏綜合性政策，程序，標準和指導方針所造成的問題。一遠端存取伺服器112可能具有無保全遠端存取點，而外部路由器104可能具有經由以下服務的資訊洩漏：像是SNMP，SMIP，finger，roosers，SYSTAT，NETSTAT，TELNET banners，視窗NT TCP 139 SMB(伺服器訊息區塊)，以及轉移至未命名伺服器主機的區域轉移等。同時可能具有不當之日誌，監視及偵測功能。分公司107可能具有一不當之信託關係，像是RLOGIN，RSH，或REXEC。防火牆106可能不當配置，或者具有一不當配置之路由器存取控制清單。

雖然此等網路問題僅爲網路100上所發現之共同問題的一例，但如熟知此項技藝人士所知，尚可能發生許多其他問題。

本發明之系統及方法允許識別一網路系統易損性。資料處理系統及方法之軟體可位於如圖2所示的一使用者終端120，用以顯示一識別之節點112易損性，其中該節點112連接於內部區域網路(LAN) 110中。爲作描述之用，本發明

（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（ 10 ）

的資料處理系統及方法可稱爲一網路易損性工具(NVT)，亦即使用者用以決定網路易損性及風險的一項工具。

形成網路易損性工具(NVT)的資料處理系統可於運行視窗NT的一Pentium個人電腦平台上載入。此類型平台可提供一低成本的解決方案，其同時支援多種接達工具，於整個描述中，通稱爲網路易損性接達，或者風險分析程式。此等網路易損性分析程式通常爲安全工程師所知的標準COTS/GOTS程式，包括：HP Open View，其允許網路自動發現或手動網路模型化；ANSSR（網路系統安全風險分析），如Mitre公司製造的一GOTS網路系統分析工具，其允許被動資料收集及單一損失事件。同樣可使用稱爲RAM（風險接達模型）之NSA風險接達方法，而且以DPL-f決策支援程式規劃語言加以實行。風險接達模型(RAM)同時允許事件樹邏輯之被動資料收集，定出任務清單之優先，以及允許具有多重風險/服務的一數學模型。其爲相對於時間之事件式。

DPL（決策程式規劃語言）爲一決策支援軟體套裝，用以協助將複雜決策模型化。其允許使用者將不確定性及彈性納入一決策處理。決策程式規劃語言(DPL)提供一圖形介面，用以建立一模型，並且以該模型執行分析。DPL-f包含用以構成決策程式規劃語言(DPL)之功能，而且提供一圖形介面，用於故障樹建構。此特性允許模型建立人士建立故障樹，並且將其納入決策程式規劃語言(DPL)模型。DPL-f同時包含唯一的分析工具。此等工具包括詳盡

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準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（11）

計算樹中任何事件的可能性以及執行故障樹特有類型的靈敏度分析之能力。DPL-f提供一介面，用以將時間系列納入一模型。此允許一模型建立者解釋貶值，資本成長或其他時間相關的數量，不需改變模型結構。DPL-f提供風險接達模型(RAM)有關快速故障樹建構，嵌式故障樹館，一專家選項產生系統，割集之列舉和排序，以及相對於時間之風險的一圖形描繪之額外功能。

如網際網路安全系統公司(ISS)所開發之ISS Internet scanner允許現行資料收集，而且掃描由主機，伺服器，防火牆和路由器所構成的一網路，而且接達依循網路，作業系統和軟體應用之安全與政策。其允許一及時快照和一電腦網路依循報告。此等程式爲發明之網路易損性工具(NVT)允許予以整合的不同網路易損性分析程式。

網路易損性工具(NVT)係根據一知識請求框架，其中合併一網路拓樸的一圖形描述。此拓樸用以捕捉網路屬性，而後分析其安全易損性。同時使用圖形使用者介面改良網路模型的精確度。

根據本發明，網路易損性工具(NVT)之系統及方法自動映射一現存網路，而且像是圖7中所示，可於一圖形使用者介面依照一模型顯示現存網路。例如，HP Open View可圖解說明一網路拓樸。一旦給定軟體該網路的一內定路由器之IP位址後，本發明的網路易損性工具(NVT)可使用Open View，而且搜尋該網路附接的電腦及其他裝置。網路易損性工具(NVT)執行一現行搜尋，ping網路上可能的

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)

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線

五、發明說明（12）

IP位址，而且將所接收之任何響應資訊加至其網路映像。如所說明，網路易損性工具(NVT)同時提供一手動方法，以圖形使用者介面支援拖曳及放下，繪製一建議網路。一系統架構可加以定義而包括替代設計或節點編輯之安全關鍵資訊，如提供完整邏輯網路規劃所要求提供額外細節。一使用者同時可使用一子網路圖示代表一映像上的整個網路。

如圖16及17中的一例子所示，當完成一網路系統描述時，網路易損性工具(NVT)代表該描述，並且將其儲存於一物件/類別階層中，以下將加以解釋。一單一拓樸系統物件模型支援不同網路易損性分析程式(工具)之資訊資料需要。如圖10之圖形使用者介面所示，該結果的模糊邏輯處理允許使來自程式之結果與一內聚易損性/風險接達關聯化，以獲得網路的一易損性狀態。該系統之單一表示法簡化多重工具的使用，而且消除冗餘資料項目。其同時提供一基礎，用以闡述一給定之易損性接達工具以及進一步知識協商能力的不完整資料問題。

圖3於130說明整個網路視覺化工具(NVT)，即本發明之資料處理系統的一例子，其中以ANSSR 132，ISS Internet scanner 134，和風險接達模型(RAM) 136說明三個網路易損性分析程式(工具)。本發明之系統及方法建立一系統物件模型資料庫(網路模型DB) 138，用以代表一網路，並且支援網路易損性分析程式的資訊資料需求。系統物件模型資料庫138代表接達系統或設計的一單一表示法，而且闡

（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（13）

述需要一網路的一單一內部表示法，用以將資料提供予網路易損性分析程式。

模型138使用物件導向(OO)方法提供一類別階層中可擴充的一組組件，其中該等組件可加以組合，以代表一網路。類別階層提供以共享之共同特點定義組件的一方式，但保留與其他組件相異的說明。除了一隱含階層式關係外，物件導向技術提供一包含機構，其中一物件可包含任何物件的一參照，包括其本身。此提供一具彈性的機構，用以代表任何實體或邏輯實體。同時物件導向表示法將其引導至就緒的修正及擴充，而且爲理想的一資訊保障競技場，於該處每天出現改變和新技術。

如圖3所示，濾波器140與網路易損性分析程式132，134，136的每一程式相結合，而且僅允許將各別的一網路易損性程式其所需資料匯出至該工具(程式)。該濾波器爲一C++式的類別，其提供一組虛擬方法，允許網路易損性工具(NVT)系統與一程式間進行資料移動。該濾波器同時提供一種方式，供網路易損性工具(NVT)控制工具之執行以及一工具所需的完整資料。網路易損性工具(NVT)將每一工具視爲一濾波器，呼叫濾波器內之適當方法執行希望的任務，包括初始化，運行，匯入資料及匯出資料。每一工具可具有一具體之濾波器子類別，並且提供用以定義專用於該工具的每一方法之方式，更將一般而定義明確之程式規劃介面(API)提供予網路易損性工具(NVT)。此允許於網路易損性工具(NVT)內相同看待所有工具，允許加入及

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

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（14）

移除工具，不需改變任何現存網路易損性工具(NVT)碼。

使用濾波器方法可直接設立DPL-f與網路易損性工具(NVT)間之通訊。一DPL-f濾波器擔負建造及移植故障樹等細節的任務。如一分析工具，一內定樹可依照所開發代表一網路中的一節點，而且提供像是拒絕服務，遺失資料及資料折衷等事件的一可能性數值。事實上，DPL-f可作爲一最後結果的工具。

然後，以每一網路易損性分析程式分析該網路，而從每一程式產生資料結果。使該資料結果關聯化，以決定網路的一安全狀態。如以下所解釋，網路認證可透過本發明之模糊邏輯處理發生，而且系統GUI可提供一使用者顯示器的輸入。

一網路概觀藉由一自動網路發現或手動登錄144，像是透過HP Open View，依照一模型142加以建立，而且一適當濾波器146允許圖形使用者介面(GUI) 148透過一適當資料輸入150，將如圖7所示之網路模型顯示於使用者顯示器152。同時可能具有用以視覺化接達風險易損性的一風險圖形使用者介面(GUI) 154，風險/易損性報告的一日誌156，圖形使用者介面(GUI) 148其一部分的一風險接達158，其中全部透過網路認證160，而且使用如以將詳細描述的一插入或模糊規則組。同時可處置任何不完整資料解析161。

圖4說明類似圖3的一高階方塊圖，顯示系統物件模型資料庫138，其可結合一整合應用程式規劃介面162而設立

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

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（ 15 ）

及工作，允許將資料匯入如依照一模型工具所說明之各種工具164，發現工具以及資訊分析工具，而形成整個系統結果資料庫166。一應用程式規劃介面168及一圖形使用者介面(GUI) 170結合模型資料庫138而工作。一評估/接達管理員172（管理員）結合一應用程式規劃介面(API) 174和圖形使用者介面(GUI) 176而工作，使資料結果與虛線178表示之模糊邏輯處理關聯化，其中該虛線178表示之模糊邏輯處理包括專家關聯180及模糊推論與證據推理182，以產生關聯結果的易損性結果184和一圖形使用者介面(GUI) 186。雖然圖4代表一高階模型，顯示不同組件之例子，但其僅爲一種高階組件類型的一例，該種高階組件可與本發明之網路易損性工具(NVT)系統及方法連用。

圖5及6說明高階模型的其他例子，顯示資料來源200之基本組件及處理步驟(圖5)，連同系統圖像202，一個別工具分析204，一多重工具分析206，工具轉專家分析208，及報告媒體210。工具轉專家分析208可包括DPL-f 208a，爲資料事實庫中模糊邏輯處理的一部分，而且與CERT notes 208b以及用於專家關聯的一專家系統208c連用。如熟知此項技藝人士所知，報告可產生爲包括：如同一圖形使用者介面(GUI)上之圖示的輸出，本文，一EXCEL試算表，Access及組態。圖6同樣說明類似圖5的另一高階模型，其中用以形成一完整系統物件模型及模糊邏輯處理之工具可包括個別工具處理和多重工具關聯。

圖7-10詳細說明一圖形使用者介面(GUI) 220，其可包含

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準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（16）

於一電腦螢幕上，而且用以與網路易損性工具(NVT)進行互動，以及決定一網路的易損性狀態。如所說明，圖形使用者介面(GUI) 220爲一Windows™介面之標準類型。一系統設計視窗222准許顯示網路圖示224，以形成一網路映像，代表一網路內所包含之不同網路元件與節點間的關係。各別網路圖示224以對應於網路元件節點如何於網路內互連的安排鏈接起來。如圖7中所示，網路元件可透過連接線226鏈接起來，顯示實際網路元件與節點間所存在的互連。系統設計視窗222於左邊顯示一網路間檢視230，視窗右手邊則爲兩節點及一網路檢視232，用以說明一網路模型映像。一管理員視窗234已經打開，而且顯示網路元件的性質。

一選擇資料靈敏度爆出視窗(框)240可供使用者選擇，其係透過所選定之網路元件的選單選項(圖8A)，同時具有使用者選定項目，用以選擇網路元件靈敏度。於任何節點(圖8A所示例子中的節點1)上資料之靈敏度可以適當的OKay，隨機和內定按鈕選擇：未分類，靈敏，機密，祕密，限制祕密或者最高祕密。

圖8B中顯示一選擇節點組態編輯爆出視窗(框) 250，其中可具有使用者可選擇易損性輪廓，用以選擇一網路元件或節點的一易損性輪廓。圖9同時顯示網路模型圖，其中具有集中式集線器以及互連節點。一使用者可能能夠編輯管理員視窗234項目，其同時允許透過適當的選擇按鈕而發生網路發現。自然於必要時，可選擇及移動網路圖示，

（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（ 18 ）

糊邏輯決策規則透過模糊介面網路規則304及模糊證據推理規則306而作業，而且根據預定目標308決定一網路的安全狀態。

模糊邏輯處理使用資料融合，證據推理及推理網路技術。如熟知此項技藝人士所知，證據推理爲一種技術，其中收集事實，用以支援及反駁一給定假說。其結果爲：以一明確之信賴度證明或駁斥該假說。本發明之模糊邏輯處理使用證據推理，從有關每一規則之系統及工具結果累積證據，藉此將系統接達資料合併成一單一參考點，使系統遵循一特定規則。系統藉由供應一組融合規則而約束融合問題，以及縮小搜尋庫。證據推理前面已經用以執行第一層多重感測器資料融合，而且爲模糊專家系統中的一普遍之全域推理技術，像是熟知此項技藝人士已知之系統類型，如NASA所開發的模糊CLIPS。其結果爲一組模糊證據規則，用以累積給定的一組需求之證據。此潛在解析來自專家關聯之抵觸，混淆及冗餘資料，而且雖然可用資料不完整，但仍然以其得到結論。

結果精確度取決於可用資料之質與量，而且於應用模糊邏輯處理前，可能必需執行可用資料的額外細分，然而同時維護資料的可能本質。此細分使用推理網路，而且使用試探提供有關可能性的一推理方法，藉此排除對於擴充之演繹知識的需要。目標與潛在安全矩陣間之關係激勵交叉滋長。如熟知此項技藝人士所知，模糊CLIPS使用模糊事實，可假設爲介於0與1間的任何數值。該結果可以0與1

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準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（19）

爲垂直界線的一連續函數的一二維平面圖加以檢視。

資料融合與系統物件資料庫，資料結果資料物件庫連用。智慧資料融合爲一多重層次，多重紀律式資訊處理，從多重智慧來源(且可能爲多重智慧紀律)提供資訊整合，以產生有關一實體(其狀況，能力，及所加諸徵兆)之特定，綜合而且統一的資料。資料融合根據可用之輸入提供資訊。通常將智慧資料融合處理分割成四個層次，描述於以下表1中。

（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（ 20 ）

表1，智慧資料融合處理之層次及目的

資料融合層次		描述
1	物件細分	• 將資料轉換成一致的參考框 • 及時細分及擴充物件位置，動力學或屬性等估計 • 將資料指派予物件，允許估計處理應用 • 細分物件身份估計
2	狀況細分	• 開發環境背景中物件與事件間之目前關係的描述 • 一符號式推理處理，其中固定和追蹤實體之分散以及事件和活動藉此與一選擇性問題其背景中的環境和效能資料相結合
3	徵兆細分	• 將目前"狀況"投射於未來，而且推斷有關作業之徵兆，易損性及機會的推理
4	處理細分	• 監控處理效能，以提供資訊，供即時控制及長期改良用 • 識別改良多重層次融合產品所需爲何種資訊 • 決定來源特定資料需求，以聚集所需資訊 • 配置及指導來源，以達成任務目標

如以前所註明，網路易損性工具(NVT)組合來自多重來源之多重資料類型與其他本文資訊，形成一網路系統之安全狀態的一整合性檢視。網路易損性工具(NVT)提供使用者一給定系統或系統設計之易損性狀態的一簡單代表，而

（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（21）

且促成其得以執行功能，效能，及對策交易的"萬一"分析，以細分及改良系統或系統設計。

於電腦安全工程中，感測器爲各種易損性接達及風險分析工具，必要時，伴隨圖形使用者介面(GUI)收集來自使用者的資訊。來自此等工具之成果輸出採用來自不同販售商之多種格式的定性與定量資料形式。關於電腦安全工程，有趣的物件爲一網路(計算系統)中之節點，即資產，包括硬體，軟體和資料。有趣的情況爲一電腦網路區段之安全系統中其弱點的一接達，其中該弱點可能爆發，而造成損害，或者祕密性，完整性或可用性的降低。

接達一計算系統所面臨之風險包含所面臨的徵兆，其發生(爆發)可能性，以及預期損失(或損害)成本的接達。最後，網路(計算系統)可根據成本利益分析結果加以細分。此需有適用於特殊易損性及其成本之保護量測(控制或對策)的資訊。成本利益分析尋求決定：使用一控制或對策，抑或接受預期損失成本，何者成本較少。此引導出一安全規劃的開發，以改良一電腦網路系統安全。

表2包含用於電腦安全工程中之資料融合處理其一第一分割的一例子，其可與本發明連用，具有四個處理層次，對應於表1中所見到的四個層次。如圖12中所說明，此處理之輸入將由物件模型資料庫138，來自個別工具132，134，136之結果，及其他背景資訊構成。不同之資料融合層1-4大致以320，322，324和326表示。

（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（22）

表2，電腦安全風險分析之資料融合的初始處理層次

資料融合層次		描述
1	節點資料細分	• 將資料轉換成一致的參考框 • 細分網路節點層資料(電腦安全資料融合之物件) • 使(指派予適當節點之)來自多重工具的資料關聯化，而且可能於每一節點組合 • 細分物件身份的估計，網路節點(工作站)爲系統中的一系統，由一OS，關鍵應用，一資料庫及資料構成 • 此層次之易損性分析尚未訂定狀況接達
2	網路區段細分	• 網路區段層(系統中之系統層)之情況的細分 • 開發環境(一網路區段)背景中物件(節點)間之目前關係的描述 • 一符號式推理處理，有關實體(節點，網路區段)和環境之資訊藉此與有關電腦安全目標，需求的證據相結合 • 組合該網路區段層之工具結果 • 有趣的情況爲：網路區段其易損性或暴露之接達
3	風險細分	• 細分一計算系統內之損害(風險)暴露及其潛力 • 將目前"情況"(電腦網路系統情況)投射於未來，並且推斷有關作業之徵兆，易損性及機會的推理 • 根據易損性，考慮要項，背景，成本，徵兆 • 以降低一或更多易損性之控制的識別細分一系統設計 • 根據對策，組件，成本 • 識別改良多重層次融合產品所需爲何種資訊 • 協助系統之長期改良

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

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（23）

雖然本發明所使用之資料融合提供一概念性框架，以闡述合併來自多重易損性接達和風險分析工具之結果的問題，但是專家系統，推理網路和證據推理則實際用以實行融合觀念，以及合併工具結果。模糊決策技術，尤其模糊專家系統的彈性更提供闡述此等問題的方式。模糊專家系統的一主要好處爲使用及消化來自多重來源之知識的能力。

模糊邏輯提供用以代表及推論不精確，不明確或不可靠知識的技術。類似傳統專家系統，一模糊專家系統可代表以IF/THEN規則系統形式代表知識，其中其前因，後果，或兩者爲模糊，而非明快。模糊邏輯用以決定模糊事實與規則的匹配程度如何，以及此種匹配影響該規則的結論到達何種程度。根據本發明，一推理網路爲一試探規則階層，其可傳播可能性，不需擴充之演繹可能性(例如Bayesian網路)知識。試探規則可使用如何傳播可能性之專家知識加以開發，允許以有限的演繹可能性知識推斷結論。此導致於較高階結論中精確反應低階離散可能性。低階事件的可能性(像是根據壽命之密碼折衷的可能性)必需爲較高階事件(密碼易損性)中所推斷之任何結論的一部分。

網路易損性工具(NVT)之初始研究使用證據累積，以修正一模糊事實，以及代表目前系統所需的狀態改變。然後，使用此狀態改變模糊事實修正系統，而且使用全域貢獻，將新狀態回饋至一無窮週期之狀態規則改變中。模糊

（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（ 25 ）

其中兩工具目前用於網路易損性工具(NVT)的某一方面。該等工具之輸出同時爲定量(ANSSR)以及定性(Internet Scanner)。模糊邏輯允許系統於相同系統內代表兩種資料類型。然後，將一初始假說公式化，而且使用模糊邏輯收集證據，以反駁或支援該假說。

關於此例子，一初始假說可能爲：於一現存網路系統中稽核無效。然後，系統使用者運用ANSSR和ISS Internet Scanner工具。如果ANSSR供應一數目90（100中的），則稽核足夠。模糊邏輯允許網路易損性工具(NVT)以此作爲強烈反駁稽核無效之初始假說的證據。如果Internet Scanner供應User Access並未稽核之定性資料，則模糊邏輯以此作爲支援證據，而且與來自ANSSR的證據組合。當工具完成時，用以稽核之貢獻證據以一單一模糊事實作爲代表，其中該單一模糊事實提供稽核之實行如何良好的一量測。

如Florida，Melbourne之Harris公司所開發的FuzzyFusion™爲一種將網路易損性工具(NVT)內所使用之易損性接達和風險分析工具的結果聯合及合併成一統一報告的方式。尤其，FuzzyFusion™將加以開發，用以實行第1及2層融合。FuzzyFusion™係透過使用一模糊專家系統(目標導向模糊邏輯決策規則)加以完成，其中該模糊專家系統利用模糊CLIPS，而且組合以下各項：各種工具之輸出，使用者關注之系統風險與易損性，以及有關每一工具其結果，和如何將該等結果安裝於一較大的資訊系統安全圖像之專家判斷。因此，網路易損性工具(NVT)使用者獲得一給定之計

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準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（ 26 ）

算系統或系統設計其安全狀態的一簡單表達，而且可執行功能，效能，和對策交易的"萬一"分析。

圖14說明網路易損性工具(NVT) FuzzyFusion™組件架構，用以實行電腦安全工程的前二層資料融合。如圖示所說明，將模型化安全技能之任務分割成離散的任務。將專家關聯(資料框架合併規則)，模糊推理網路規則，和模糊證據推理規則加以分離可闡述脆弱之專家系統及計算爆炸的問題。其同時隔離低階資料關聯和融合與混淆/抵觸資料之解析以及將結果合併成一圖像。此可導致模糊專家系統，其較一大型綜合性系統更容易維護。此架構之元件說明於後。

資料模糊310將來自個別易損性接達及風險分析工具132，134，136之結果轉換成模糊事實，並且伴隨共同系統模型(CSM)，亦即系統物件模型資料庫138，將其儲存於(模糊CLIPS)事實庫302。(模糊後之)個別工具結果及CSM 138將匯出，供專家關聯處理330 (資料框架合併規則)，根據安全技能，解析系統資訊及整合工具輸出。專家意見可用以決定歸因於低階事件的特定模糊數值。

專家關聯(資料框架合併規則) 330爲模糊專家規則的一聚集，用以執行節點層資料細分(第1層)或者網路區段細分(第2層)。此等規則使用安全工程師之技能，將來自易損性接達和風險分析工具之(模糊化)輸出加以關聯化及聯合。此等規則發揮安全接達中之擴充經驗，用以解析低階系統資料及工具結果。此等規則解析系統資訊，並且整合

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準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（ 27 ）

工具輸出。專家關聯規則處理330同時可將低階資料從CSM及工具結果轉換成高階結論。例如，

如果此等旗標爲稽核中

而且稽核資料並未備份，

則稽核不可靠。

以事實庫302中之模糊事實進行工作，則一組第1層模糊規則可聯合每一節點之易損性，形成網路中每一節點的一易損性分級。此分級可匯入回網路易損性工具(NVT)，供顯示用。類似地，一組第2層模糊規則可聯合每一網路區段的易損性，形成每一網路區段的一易損性分級。此可再度匯入回去，供顯示用。

然後，該資料須經模糊推理網路規則處理304。其必需於應用模糊證據推理規則304前，執行可用資料之額外細分，但仍維護該資料的可能本質。此細分將使用推理網路，如熟知此項技藝人士所知，其爲一種提供使用試探式推理可能性之方法，藉此移除對於擴充演繹知識的需要。

模糊證據推理規則306爲模糊專家規則之聚集，用以將個別工具的結果從一系統層次透視圖，合併成一網路安全狀態的一較高層次接達。此等規則提供一機構，用以將CSM，工具結果及來自專家關聯(資料框架合併規則) 330之結果合併成一統一報告。此同時排除應付來自專家關聯中使用之轉送鏈接專家系統的不完整及抵觸資料之必要性。

證據推理使用一種技術，其中收集事實，用以支援及反

（請先閱讀背面之注意事項再填寫本頁）
裝
訂
線
經濟部中央標準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（28）

駁一給定之假說。其結果爲：以一明確的信賴度證明或駁斥假說。FuzzyFusion™使用證據推理，從有關每一規則之共同系統模型及工具結果累積證據，藉此將電腦網路系統接達資料合併成一單一參考點，使系統遵循特定規則。藉由供應模糊的一組融合規則，網路易損性工具(NVT)約束融合問題，而且減少搜尋空間，如早先所稱的目標式融合。其結果將爲一組模糊證據規則，其唯一目的爲：累積給定的一組需求之證據。其解析來自專家關聯(資料框架合併規則) 330之潛在抵觸，混淆及冗餘資料，而且即使可用資料不完整，仍可以其推斷結論。顯然，該結果之精確度取決於可用資料的數量及品質。

如以前所註明，模糊邏輯處理爲目標導向。證據累積處理350之目標可從一安全需求資料庫352，一電腦安全矩陣資料庫354，或者像是由AFCERT構成的一資料庫之易損性資料庫356導出。預先定義目標之界定融合限制計算次數。FuzzyFusion™目標提供用以獲得IA矩陣的機構。

FuzzyFusion™處理具有優於傳統途徑的一些優點。Crisp專家系統需要極大的知識庫，用以容納必要資料，然而尚且仍有資料不完整及結果抵觸的問題。Bayesian及可能性網路需要擴充而且通常不可用的可能性演繹知識。演算法解答無法適用於安全問題之可能和試探本質。

像是模糊CLIPS之網式專家系統根據系統中所出現的規則與事實數目，於執行時間中歷經幾何級數式增加。此引導至將分析分解成子網路。FuzzyFusion™將子網路與定標

（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（29）

功能相加。每一子網路之節點評定爲一群組，然後評定子網路群組。將每一分析類型之規則分組成不同模型可縮小網式網路的大小。除了減少執行時間外，其同時將引介一種用以分析網路之可縮放比例的方法，其中將分析之網路映射至網路易損性工具(NVT)所使用的網路模型。

如圖15中所示，其他可能之資料空間包括一徵兆知識資料庫360，成本資料庫362，爲第3層融合的一部分，以及一計數器量測知識庫，組件資料庫和成本資料庫，爲第4層融合的一部分。

一種方法和資料處理系統接達一網路之安全易損性。其中建立一系統物件模型資料庫，以支援不同之網路易損性分析程式的資訊資料需求。僅將來自代表該網路之系統物件模型資料庫的所需資料匯入程式，然後分析該網路，而從每一程式產生資料結果。將此等資料結果儲存於一共同系統模型資料庫中，進而儲存於資料事實庫內。應用該等目標導向模糊邏輯決定規則，以決定該網路的易損性狀態。

（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）

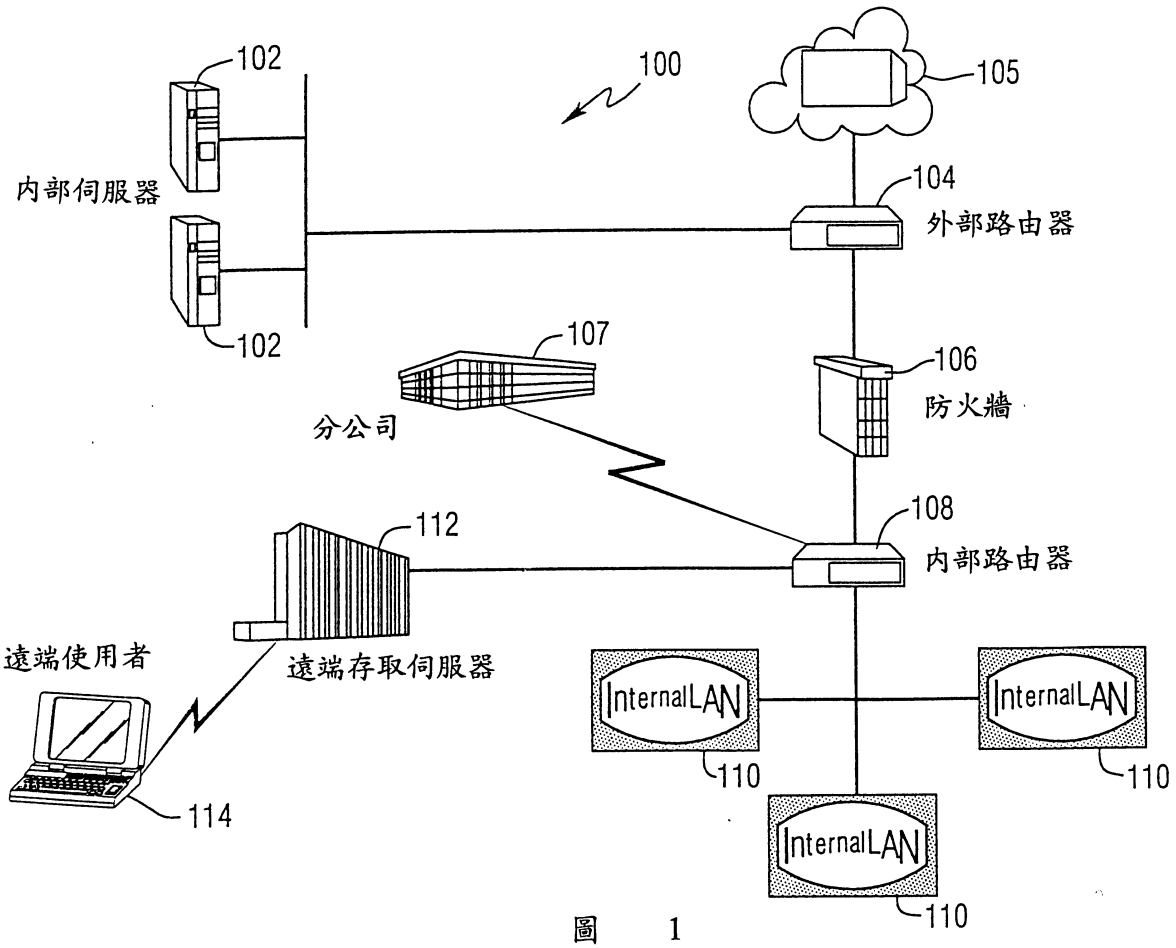
102
100
105
內部伺服器
104
外部路由器
102
107
106
分公司
防火牆
108
112
內部路由器
遠端使用者
遠端存取伺服器
InternalLAN
InternalLAN
110
110
InternalLAN
110
114

圖 1

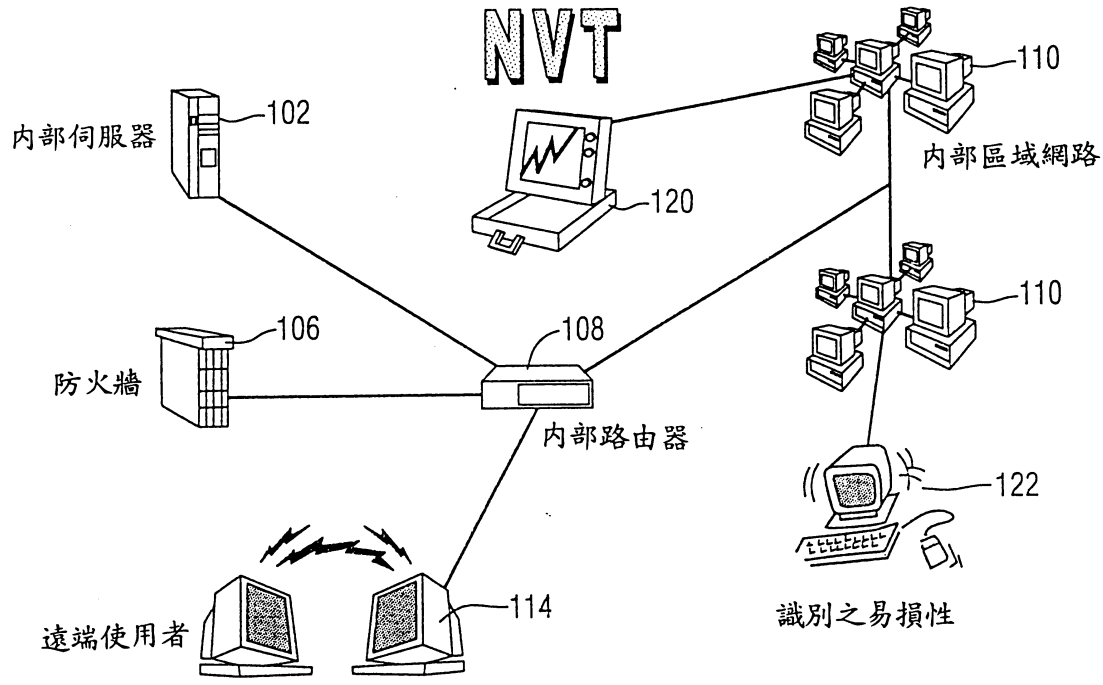
NVT
110
內部伺服器
102
內部區域網路
120
110
106
108
防火牆
內部路由器
122
114
遠端使用者
識別之易損性

圖 2

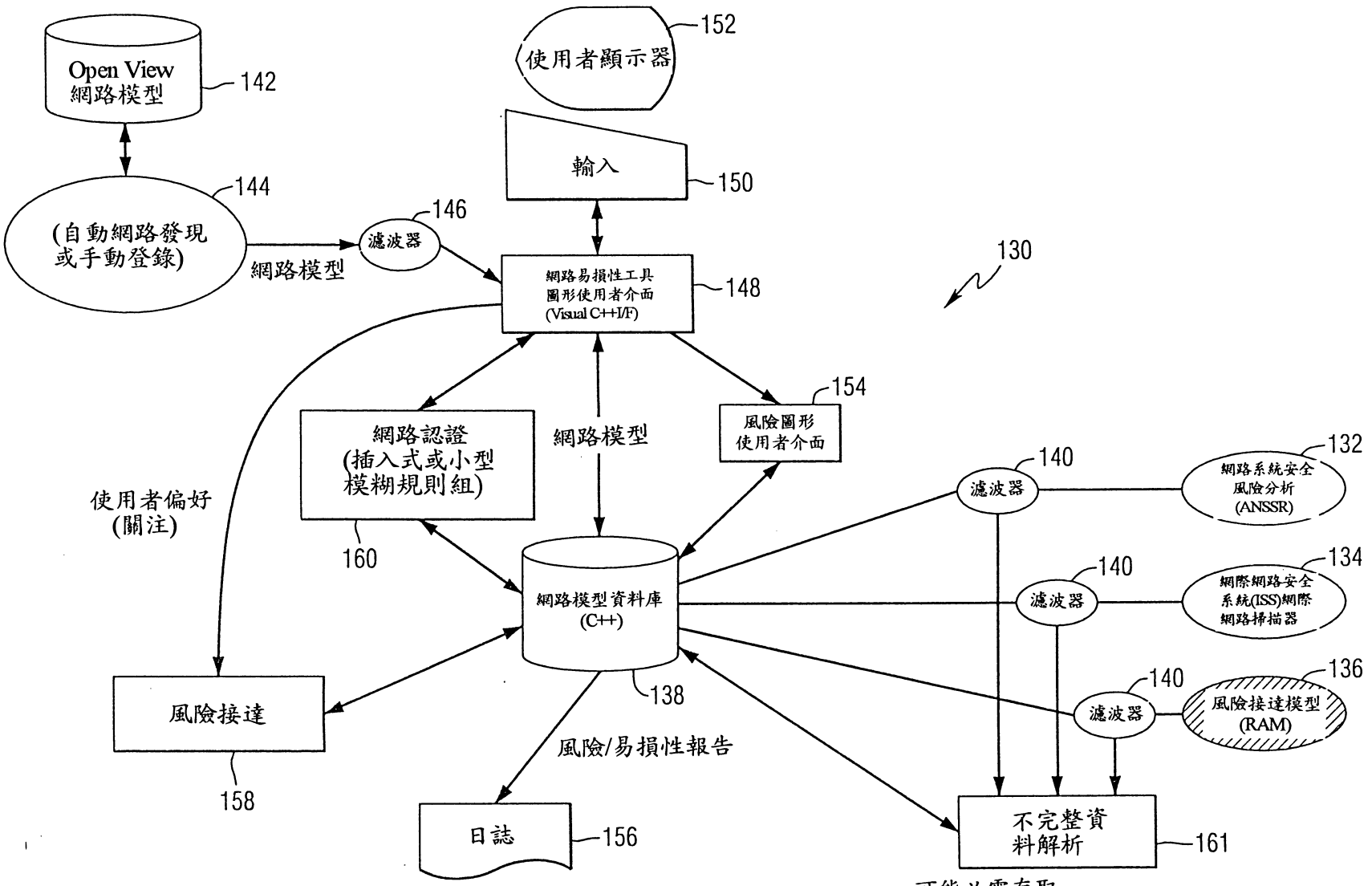
Open View
網路模型
142
使用者顯示器
152
輸入
150
144
(自動網路發現
或手動登錄)
網路模型
146
濾波器
網路易損性工具
圖形使用者介面
(Visual C++I/F)
148
130
154
網路認證
(插入式或小型
模糊規則組)
160
網路模型
風險圖形
使用者介面
使用者偏好
(關注)
140
濾波器
網路系統安全
風險分析
(ANSSR)
132
140
濾波器
網際網路安全
系統(ISS)網際
網路掃描器
134
網路模型資料庫
(C++)
138
140
濾波器
風險接達模型
(RAM)
136
風險接達
158
風險/易損性報告
日誌
156
不完整資
料解析
161
可能必需存取
Open View，
網路易損性工具圖形使用者介面，
ISS網際網路掃描器等

圖　3

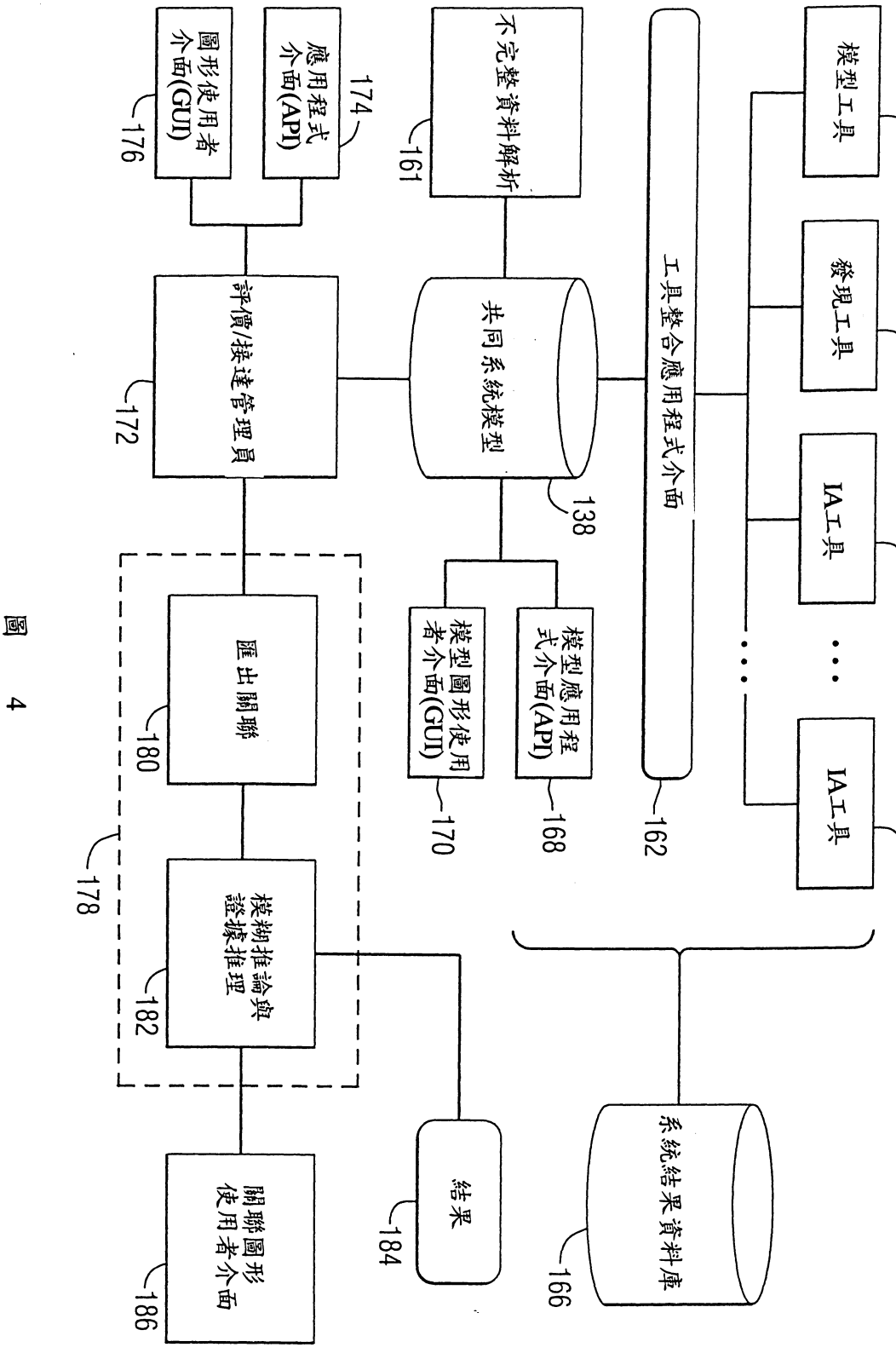
模型工具
164
發現工具
164
IA工具
164
IA工具
164
工具整合應用程式介面
162
不完整資料解析
161
共同系統模型
138
模型應用程式介面(API)
168
模型圖形使用者介面(GUI)
170
系統結果資料庫
166
應用程式介面(API)
174
圖形使用者介面(GUI)
176
評價/接達管理員
172
匯出關聯
180
模糊推論與證據推理
182
結果
184
關聯圖形使用者介面
186
178

圖 4

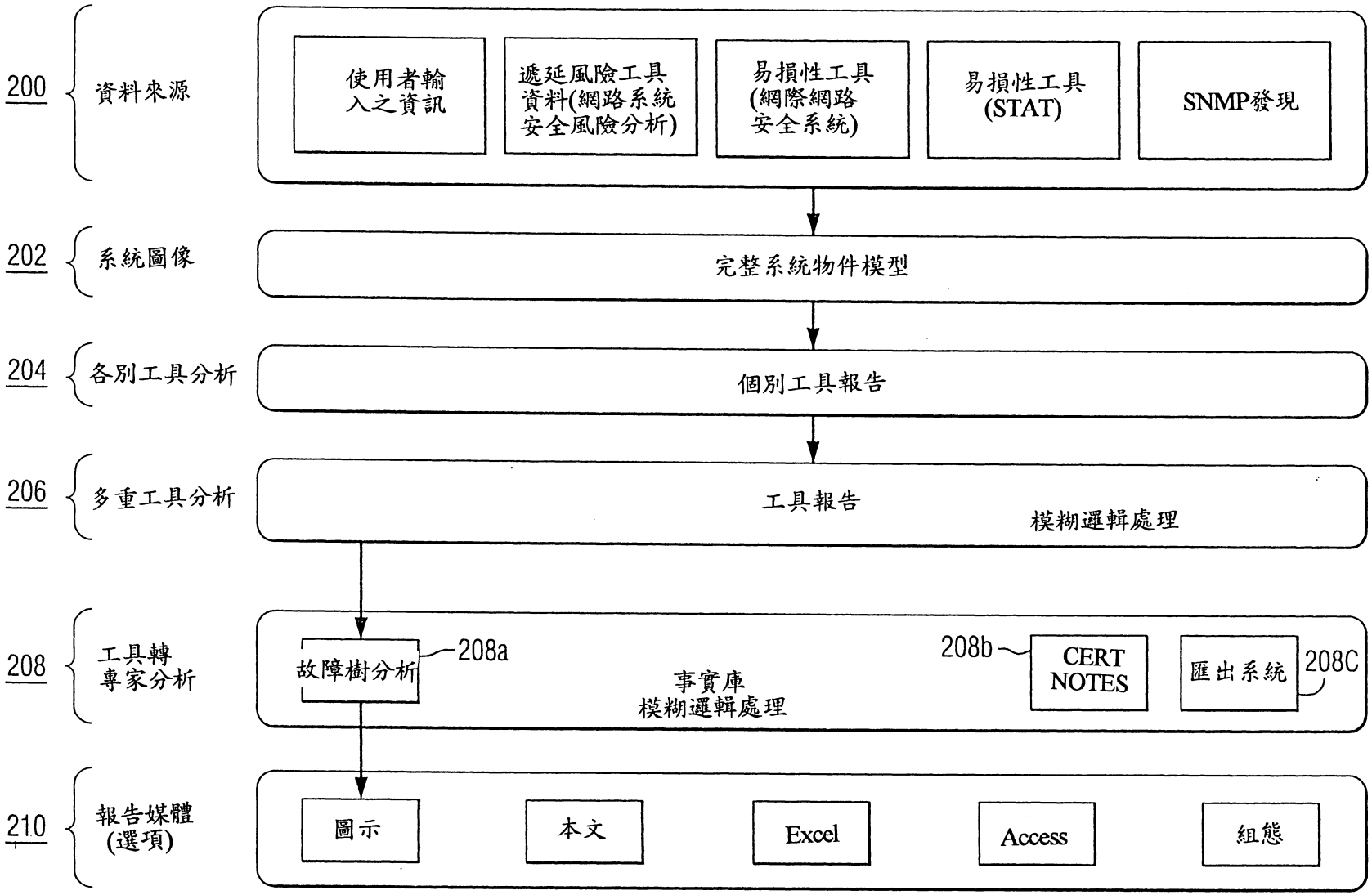
200
資料來源
使用者輸入之資訊
遞延風險工具資料(網路系統安全風險分析)
易損性工具(網際網路安全系統)
易損性工具(STAT)
SNMP發現
202
系統圖像
完整系統物件模型
204
各別工具分析
個別工具報告
206
多重工具分析
工具報告
模糊邏輯處理
208
工具轉專家分析
故障樹分析
208a
事實庫
模糊邏輯處理
208b
CERT NOTES
匯出系統
208C
210
報告媒體(選項)
圖示
本文
Excel
Access
組態

圖　5

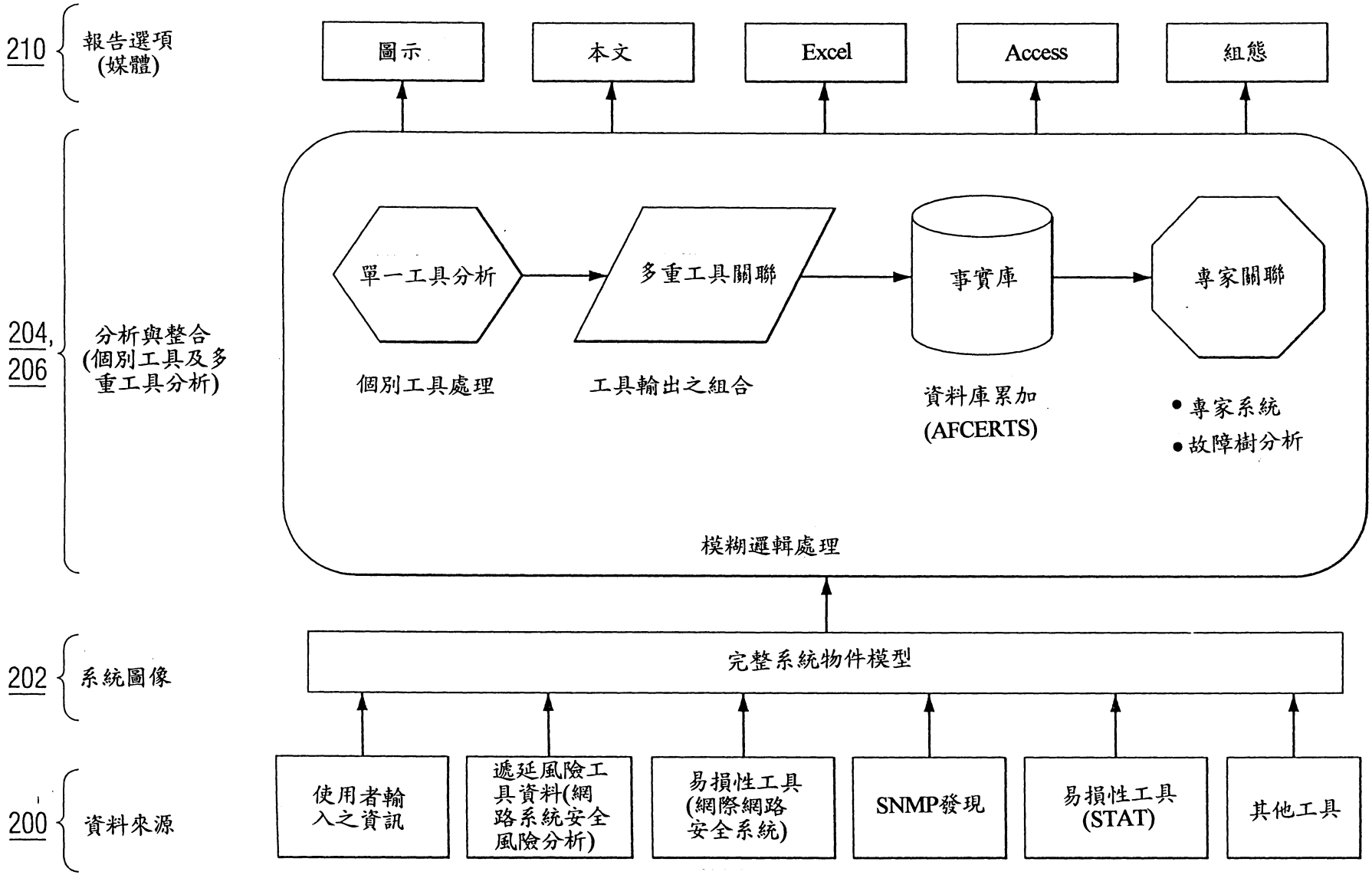
210
報告選項
(媒體)
圖示
本文
Excel
Access
組態
204,
206
分析與整合
(個別工具及多
重工具分析)
單一工具分析
多重工具關聯
事實庫
專家關聯
個別工具處理
工具輸出之組合
資料庫累加
(AFCERTS)
• 專家系統
• 故障樹分析
模糊邏輯處理
202
系統圖像
完整系統物件模型
200
資料來源
使用者輸
入之資訊
遞延風險工
具資料(網
路系統安全
風險分析)
易損性工具
(網際網路
安全系統)
SNMP發現
易損性工具
(STAT)
其他工具

圖 6

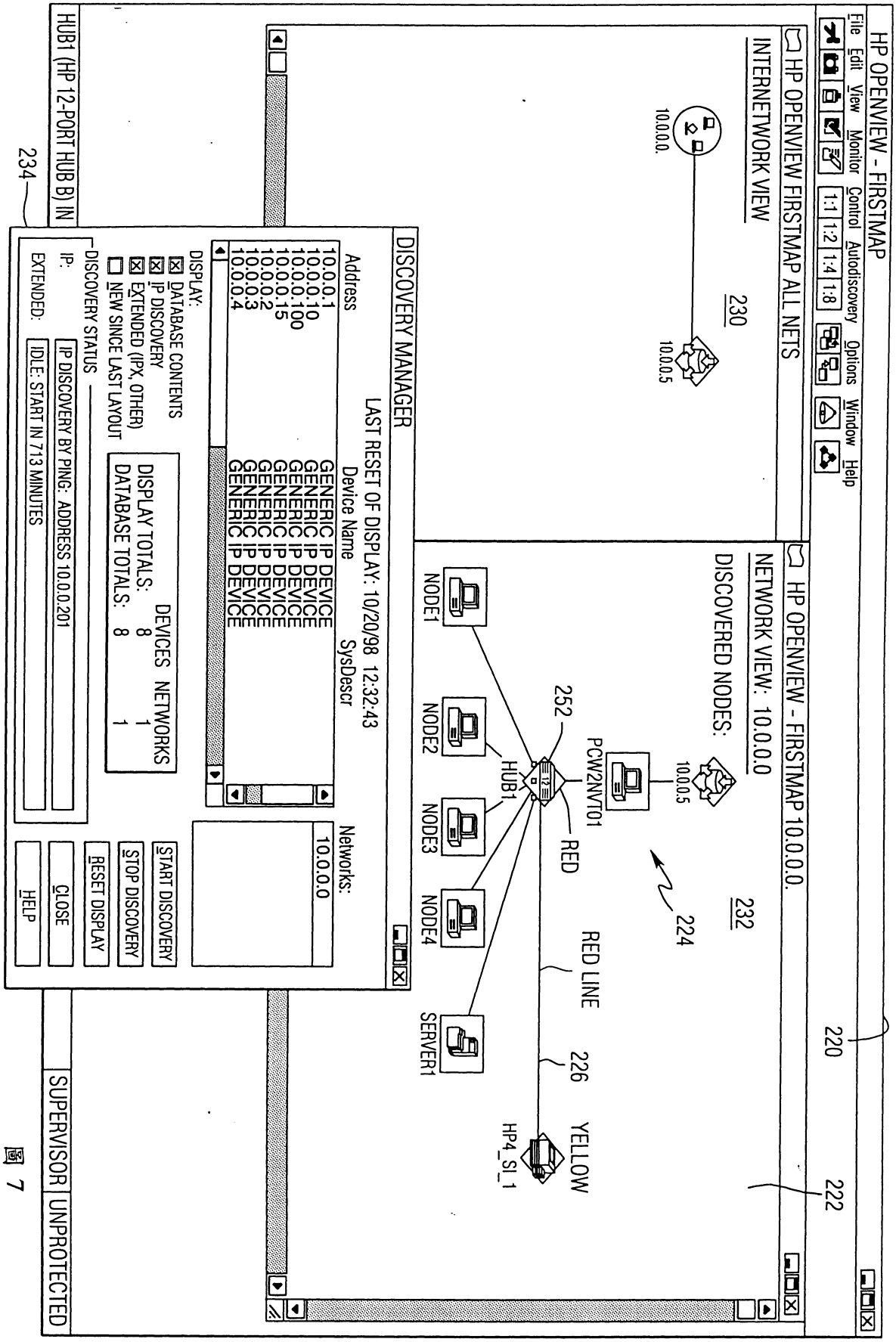
HP OPENVIEW - FIRSTMAP
File Edit View Monitor Control Autodiscovery Options Window Help
1:1 1:2 1:4 1:8
HP OPENVIEW FIRSTMAP ALL NETS
INTERNETWORK VIEW
230
10.0.0.0
10.0.0.5
HP OPENVIEW - FIRSTMAP 10.0.0.0.
NETWORK VIEW: 10.0.0.0
DISCOVERED NODES:
232
10.0.0.5
224
PCW2NVT01
252
HUB1
RED
RED LINE
226
YELLOW
HP4_SI_1
NODE1
NODE2
NODE3
NODE4
SERVER1
220
222
DISCOVERY MANAGER
LAST RESET OF DISPLAY: 10/20/98 12:32:43
Address
Device Name
SysDescr
10.0.0.1 GENERIC IP DEVICE
10.0.0.10 GENERIC IP DEVICE
10.0.0.100 GENERIC IP DEVICE
10.0.0.15 GENERIC IP DEVICE
10.0.0.2 GENERIC IP DEVICE
10.0.0.3 GENERIC IP DEVICE
10.0.0.4 GENERIC IP DEVICE
Networks:
10.0.0.0
DISPLAY:
DATABASE CONTENTS
IP DISCOVERY
EXTENDED (IPX, OTHER)
NEW SINCE LAST LAYOUT
DISPLAY TOTALS: DEVICES 8 NETWORKS 1
DATABASE TOTALS: 8 1
START DISCOVERY
STOP DISCOVERY
RESET DISPLAY
CLOSE
HELP
DISCOVERY STATUS
IP: IP DISCOVERY BY PING: ADDRESS 10.0.0.201
EXTENDED: IDLE: START IN 713 MINUTES
HUB1 (HP 12-PORT HUB B) IN
234
SUPERVISOR
UNPROTECTED

圖 7

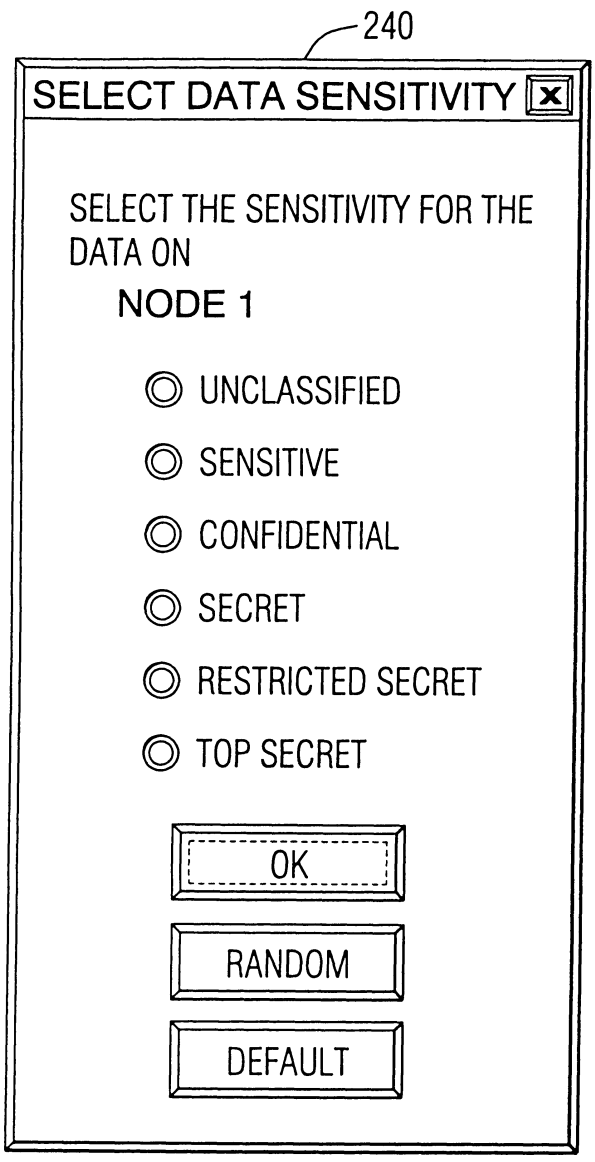
240
SELECT DATA SENSITIVITY
SELECT THE SENSITIVITY FOR THE DATA ON
NODE 1
UNCLASSIFIED
SENSITIVE
CONFIDENTIAL
SECRET
RESTRICTED SECRET
TOP SECRET
OK
RANDOM
DEFAULT

圖 8A

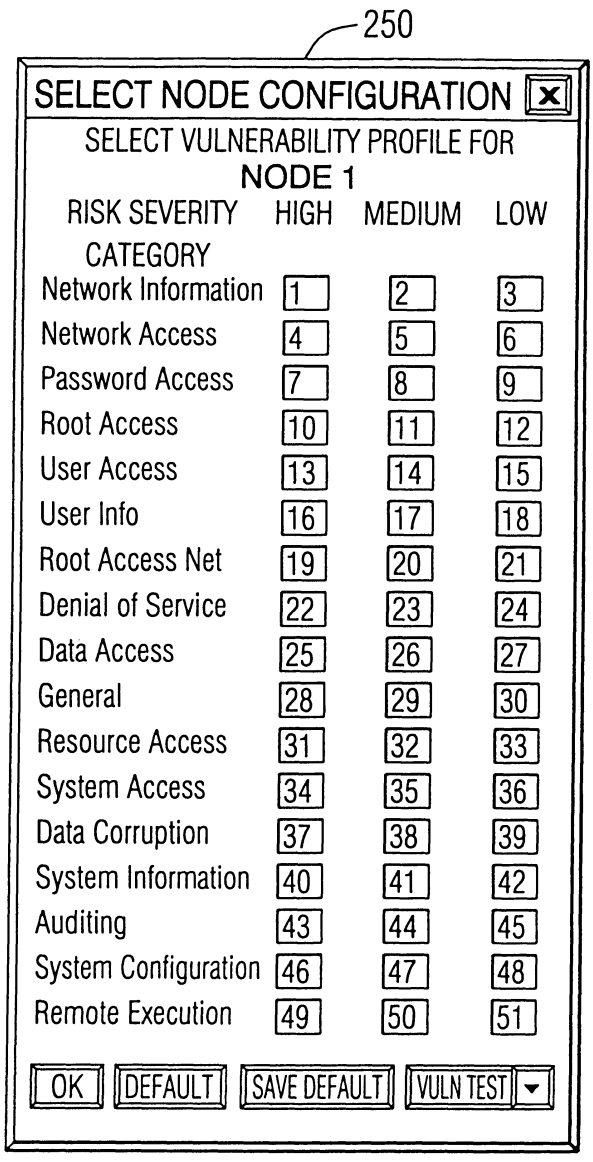
250
SELECT NODE CONFIGURATION
SELECT VULNERABILITY PROFILE FOR
NODE 1
RISK SEVERITY
CATEGORY
HIGH
MEDIUM
LOW
Network Information 1 2 3
Network Access 4 5 6
Password Access 7 8 9
Root Access 10 11 12
User Access 13 14 15
User Info 16 17 18
Root Access Net 19 20 21
Denial of Service 22 23 24
Data Access 25 26 27
General 28 29 30
Resource Access 31 32 33
System Access 34 35 36
Data Corruption 37 38 39
System Information 40 41 42
Auditing 43 44 45
System Configuration 46 47 48
Remote Execution 49 50 51
OK
DEFAULT
SAVE DEFAULT
VULN TEST

圖 8B

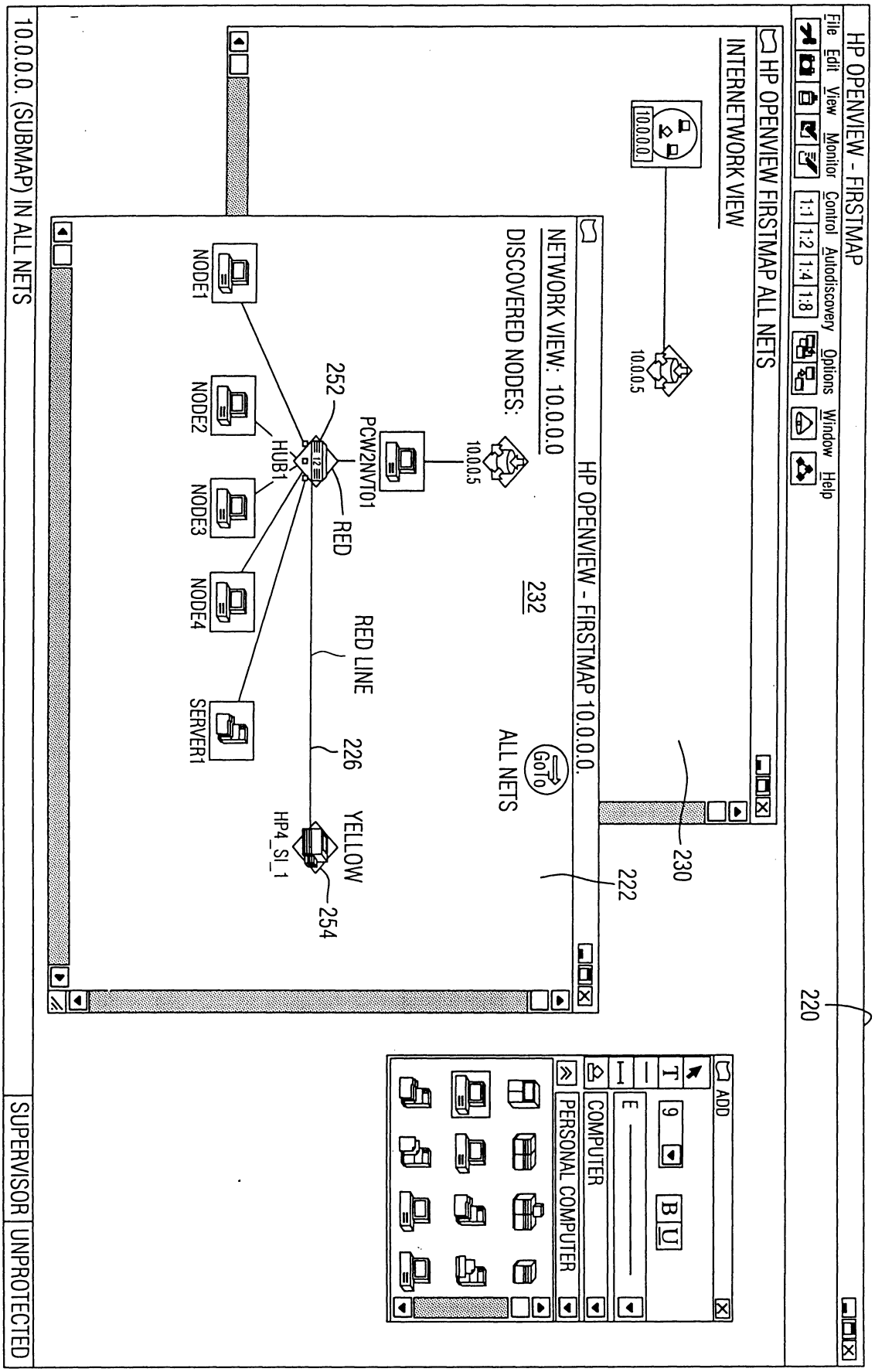
HP OPENVIEW - FIRSTMAP
File Edit View Monitor Control Autodiscovery Options Window Help
1:1 1:2 1:4 1:8
HP OPENVIEW FIRSTMAP ALL NETS
INTERNETWORK VIEW
10.0.0.0
10.0.0.5
230
220
222
HP OPENVIEW - FIRSTMAP 10.0.0.0
NETWORK VIEW: 10.0.0.0
DISCOVERED NODES:
10.0.0.5
232
GoTo
ALL NETS
NODE1
NODE2
NODE3
NODE4
SERVER1
HUB1
252
PCW2NVT01
RED
RED LINE
226
YELLOW
HP4_SI_1
254
ADD
COMPUTER
PERSONAL COMPUTER
10.0.0.0. (SUBMAP) IN ALL NETS
SUPERVISOR
UNPROTECTED

圖 9

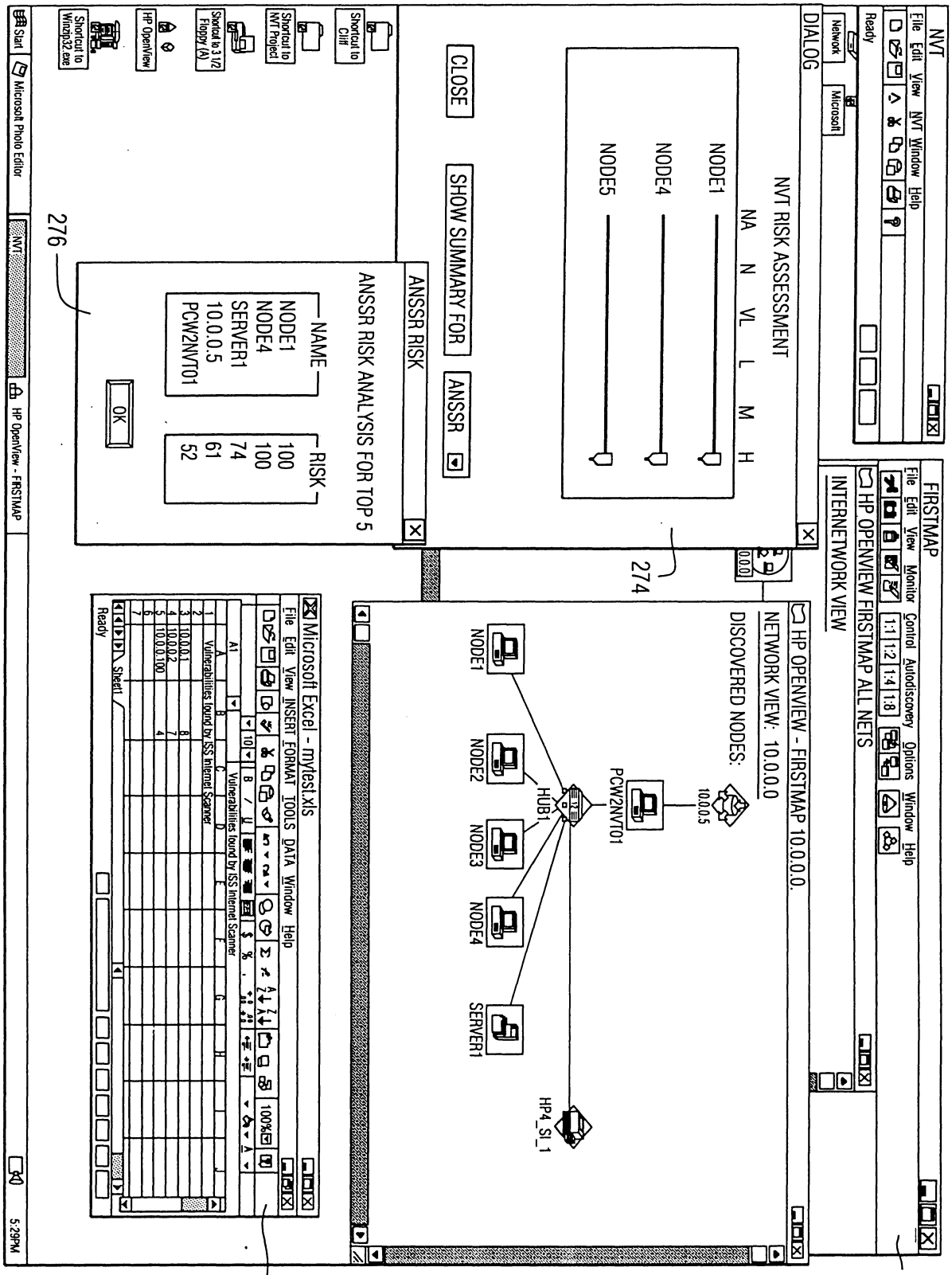
NVT
File Edit View NVT Window Help
Ready
Network
Microsoft
DIALOG
NVT RISK ASSESSMENT
NA N VL L M H
NODE1
NODE4
NODE5
CLOSE
SHOW SUMMARY FOR
ANSSR
ANSSR RISK
ANSSR RISK ANALYSIS FOR TOP 5
NAME
NODE1
NODE4
SERVER1
10.0.0.5
PCW2NVT01
RISK
100
100
74
61
52
OK
274
276
FIRSTMAP
File Edit View Monitor Control Autodiscovery Options Window Help
HP OPENVIEW FIRSTMAP ALL NETS
INTERNETWORK VIEW
HP OPENVIEW - FIRSTMAP 10.0.0.0
NETWORK VIEW: 10.0.0.0
DISCOVERED NODES:
10.0.0.5
PCW2NVT01
HUB1
NODE1
NODE2
NODE3
NODE4
SERVER1
HP4_SI_1
270
Microsoft Excel - mytest.xls
File Edit View INSERT FORMAT TOOLS DATA Window Help
Vulnerabilities found by ISS Internet Scanner
10.0.0.1
10.0.0.2
10.0.0.100
Ready
Sheet1
272
Start
Microsoft Photo Editor
NVT
HP OpenView - FIRSTMAP
5:29PM

圖 10

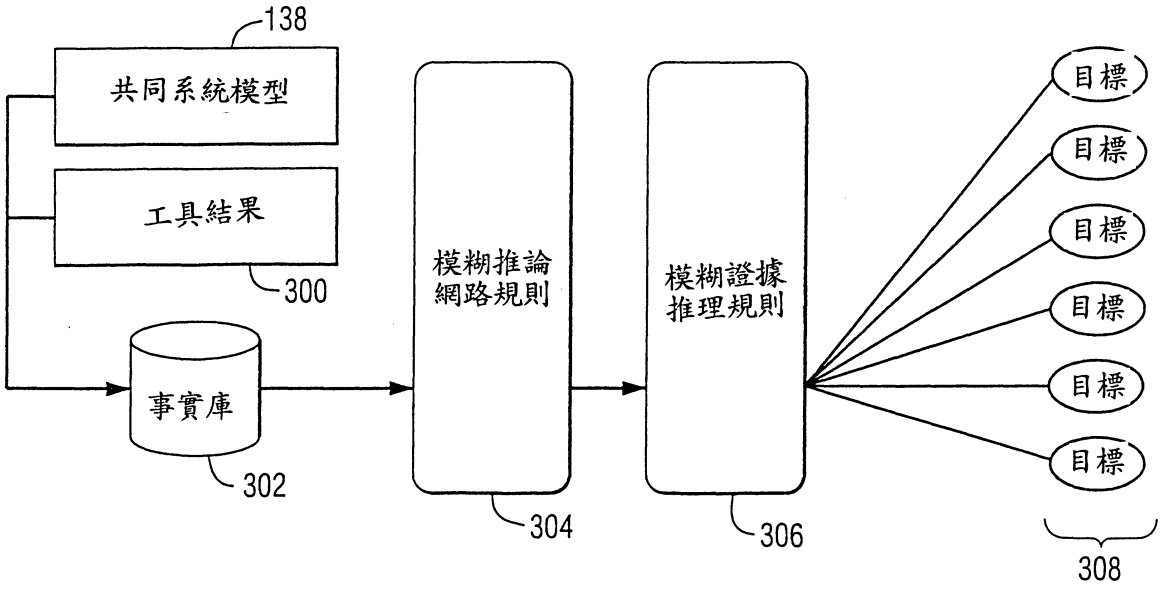
138
共同系統模型
工具結果
300
事實庫
302
模糊推論
網路規則
304
模糊證據
推理規則
306
目標
目標
目標
目標
目標
目標
308

圖 11

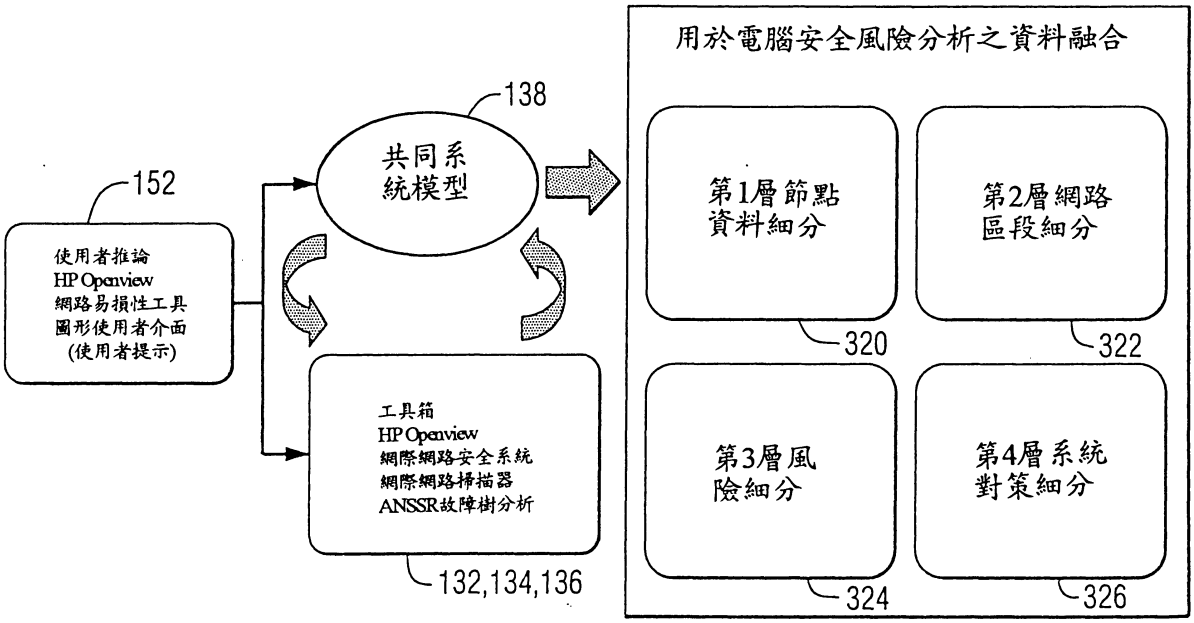
用於電腦安全風險分析之資料融合
138
共同系
統模型
152
使用者推論
HP Openview
網路易損性工具
圖形使用者介面
(使用者提示)
工具箱
HP Openview
網際網路安全系統
網際網路掃描器
ANSSR故障樹分析
132,134,136
第1層節點
資料細分
320
第2層網路
區段細分
322
第3層風
險細分
324
第4層系統
對策細分
326

圖 12

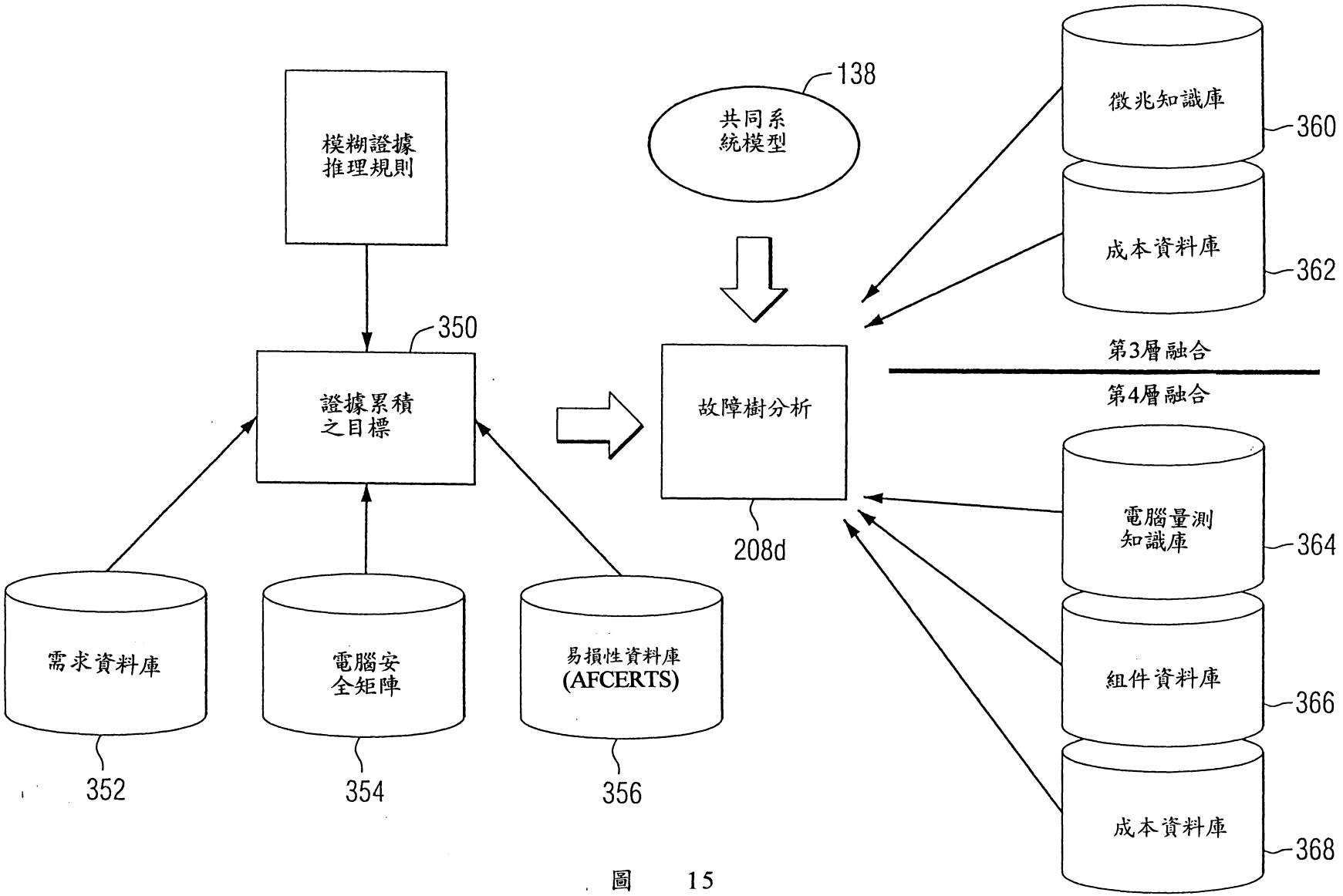
模糊證據
推理規則
138
共同系
統模型
微兆知識庫
360
成本資料庫
362
350
證據累積
之目標
故障樹分析
第3層融合
第4層融合
208d
電腦量測
知識庫
364
需求資料庫
電腦安
全矩陣
易損性資料庫
(AFCERTS)
組件資料庫
366
成本資料庫
368
352
354
356

圖 15

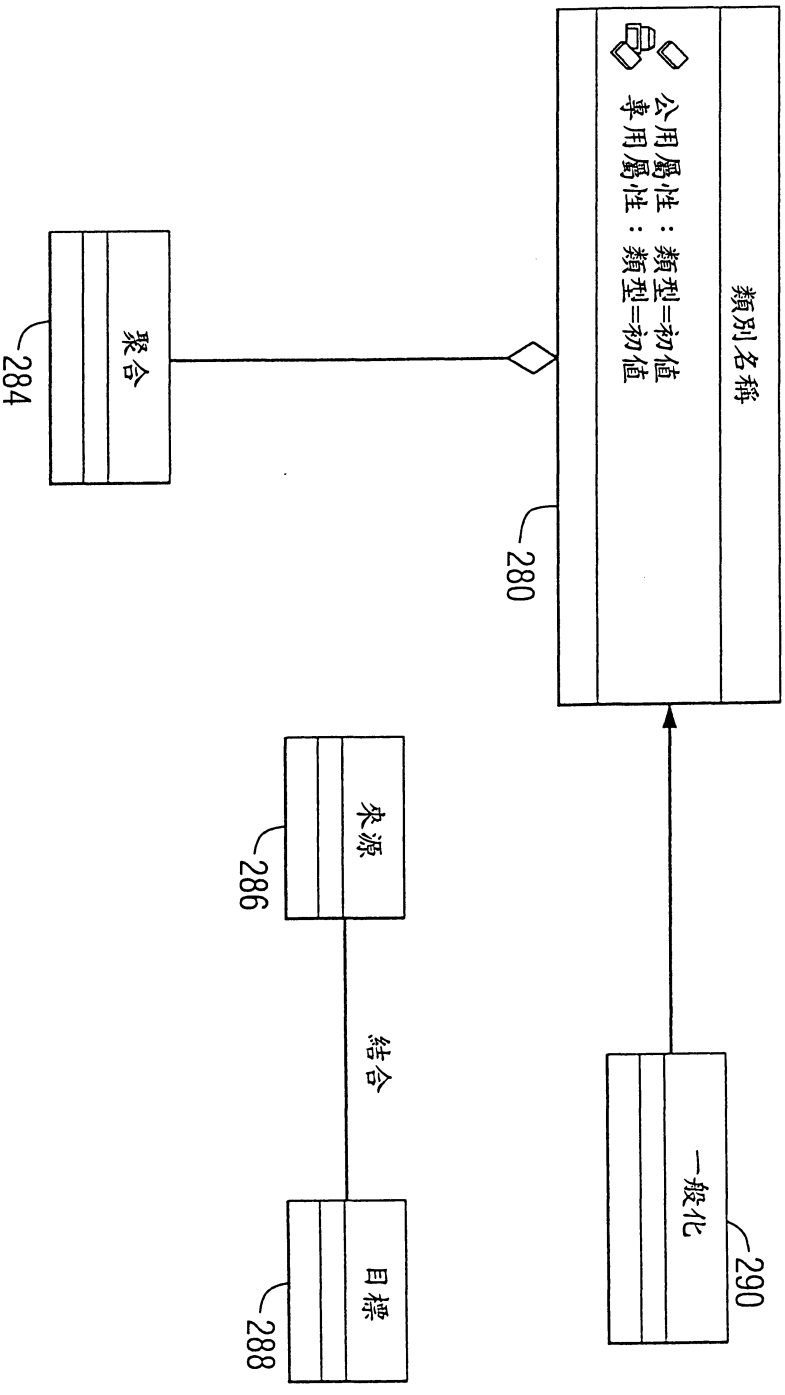

圖 16

公告本

申請日期	90. 2. 08
案　　號	090102785
類　　別	G06F 17/00

（以上各欄由本局填註）

A4
C4

中文說明書替換頁(92年10月)

發明 ~~新型~~ 專利說明書

I221985

一、發明 ~~新型~~ 名稱	中　文	評估網路的安全狀態之方法、電腦可讀取媒體及資料處理系統
	英　文	METHOD, COMPUTER-READABLE MEDIUM AND DATA PROCESSING SYSTEM FOR ASSESSING THE SECURITY POSTURE OF A NETWORK
二、發明 ~~創作~~ 人	姓　名	1. 凱文　福克斯 KEVIN FOX 2. 隆達　漢寧 RONDA HENNING 3. 約翰　法瑞爾 JOHN FARRELL 4. 克里夫　密勒 CLIFFORD MILLER
	國　籍	均美國
	住、居所	1. 美國佛羅里達州棕梠灣市海德NE街438號 2. 美國佛羅里達州西美爾鉢市艾希里湖路569號 3. 美國佛羅里達州美爾鉢市楚伯路1742號 4. 美國佛羅里達州棕梠灣市安傑羅SE路164號
三、申請人	姓　名 （名　稱）	美商賀利實公司 HARRIS CORPORATION
	國　籍	美國
	住、居所 （事務所）	美國佛羅里達州美爾鉢市那沙路1025號
	代表人 姓　名	威廉．A．楚納 WILLIAM A. TRONER

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂 線

五、發明說明（ 17 ）

以編輯及設計替代選擇。

於透過系統設立安全狀態後，高風險網路元件之圖示代表可轉變顏色，像是紅色，如集線器252。其他選定圖示可能轉變成黃色，表示為一較不嚴重的風險節點，像是圖7及9中所示之HP4節點254。圍繞網路之節點或部分的陰影區域其顏色可能變紅或變黃，表示為較高風險易損性。同時連接線可能變紅或變黃，表示元件間具有一不良連接。

圖10說明一易損性狀態視窗270，用以顯示使用者可讀取圖示，代表易損性網路元件及圖示。整個系統模型顯示為一開放式系統設計視窗的一部分。然而，其中說明一試算表272，而且一網路易損性工具(NVT)風險接達圖274具有風險接達滑塊軸。同時說明顯示前五風險分析元件的一風險分析視窗276。

圖16更詳細顯示一類別階層，其中類別名稱280為公用屬性及專用屬性，來源286與目標288之聚合282和結合284，以及其一般化290。圖17說明一系統類別圖的一例子，其中具有各種組件501-551，標示於方塊中。自然如熟知此部分人士所知，圖17僅為一系統類別圖，而且為本發明之系統及方法能夠使用的一例子。

現在詳細參照圖11-15，說明目標導向模糊邏輯決策訂定。如圖11所示，來自各別網路易損性分析程式之系統模型資料庫138與結果300使用一應用程式規劃介面及專家關聯，透過資料模糊，形成一資料事實庫302。目標導向模

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂 線

五、發明說明（ 24 ）

CLIPS 允許定義模糊事實類型，但每一類型僅存在一事實。因此，操作該事實類型的每一規則實際上修正一單一事實，進而導引出證據累積。

全域貢獻及證據累積導引出一模糊 CLIPS 方法，其中定義代表不同易損性狀態的模糊事實。此等事實將使用全域貢獻及證據累積，以獲得用以反應測試系統之易損性的最終數值，即證據推理。此方法反應定義明確之模糊邏輯控制系統用法，將該執行限制於一有限週期數，而非允許其連續運行。FuzzyFusion™ 已經由 Florida，Melbourne 之 Harris 公司加以開發，而且使用此方法，根據來自網路安全專家之知識，累積來自規則的證據。尤其，FuzzyFusion™ 使用證據推理作為一技術，其中收集事實，以支援及反駁一給定的假說。其結果為：以一明確之信賴度證明或駁斥該假說。

初始知識萃取導致安全需求之使用，進而累積證據，亦即一系統與需求的符合程度如何。如圖 13 中所說明，其中展示驗證一資料庫 (例如 AFCERTS) 401 與驗證安全需求 403 之方法間的一強烈關聯，進而引導出使用資料庫 401 和需求 403 作為全域貢獻事實，以累積證據。此同時顯示變化眾多目標如何直接影響眾多接達，亦即將與目標一樣詳細。證據累積將視為一目標導向途徑，用以獲得結果，但仍維護一轉送推理技術之使用，現在謂之"目標式融合"405 和 407。

如何可以電腦安全中合併工具之結果應用模糊邏輯的一例子使用來自 ANSSR 和 ISS Internet Scanner 其結果的組合，

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂 線

五、發明說明（ 30 ）

圖式元件符號說明

100	傳統網路
102	內部伺服器
104	外部路由器
105	通訊網路
106	防火牆
107	分公司
108	內部路由器
110	內部本地區域網路（LAN）之網路組件
112	遠端存取伺服器
114	遠端使用者
120	使用者終端
130	整個網路視覺化工具（NVT）
132	ANSSR
134	ISS 網際網路掃描器
136	風險接達模型（RAM）
138	系統物件模型資料庫
140	濾波器
142	模型
144	自動網路發現或手動登錄
146	適當濾波器
148	圖形使用者介面（GUI）
150	適當資料輸入
152	使用者顯示器

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝　訂　線

五、發明說明 (31)

154	風險圖形使用者介面（GUI）
156	日誌
158	風險接達
160	網路認證
161	不完整資料解析
162	整合應用程式規劃介面
164	工具
166	整個系統結果資料庫
168	應用程式規劃介面
170	圖形使用者介面（GUI）
172	評估/接達管理員
174	應用程式規劃介面（API）
176	圖形使用者介面（GUI）
178	虛線
180	專家關聯
182	模糊推論與證據推理
184	易損性結果
186	圖形使用者介面（GUI）
200	資料來源
202	系統圖像
204	個別工具分析
206	多重工具分析
208	工具轉專家分析
208a	DPL-f

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂 線

五、發明說明（ 32 ）

208b	CERT note
208c	專家系統
210	報告媒體
220	圖形使用者介面（GUI）
222	系統設計視窗
224	網路圖示
226	連接線
230	網路間檢視
232	網路檢視
234	管理員視窗
240	選擇資料靈敏度爆出視窗（框）
250	選擇節點組態編輯爆出視窗（框）
252	集線器
254	HP4 節點
270	易損性狀態視窗
272	試算表
274	網路易損性工具（NVT）風險接達圖
276	風險分析視窗
280	類別名稱
282	聚合
284	結合
286	來源
288	目標
290	一般化

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂 線

五、發明說明 (33)

300	結果
302	資料事實庫
304	模糊介面網路規則
306	模糊證據推理規則
308	預定目標
310	資料模糊
320	資料融合層 1
322	資料融合層 2
324	資料融合層 3
326	資料融合層 4
330	專家關連處理
350	證據累積處理
352	安全需求資料庫
354	電腦安全矩陣資料庫
356	易損性資料庫
360	徵召知識資料庫
362	成本資料庫
401	AFCERT 資料庫
403	安全需求
405	目標式融合
407	目標式融合
501-551	組件

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂 線

四、中文發明摘要（發明之名稱：評估網路的安全狀態之方法、電腦可讀取媒體及資料處理系統）

一種方法和資料處理系統接達一網路之安全易損性。其中建立一系統物件模型資料庫，以支援不同之網路易損性分析程式的資訊資料需求。僅將來自代表該網路之系統物件模型資料庫的所需資料匯入程式，然後分析該網路，而從每一程式產生資料結果。將此等資料結果儲存於一共同系統模型資料庫中，進而儲存於資料事實庫內。應用該等目標導向模糊邏輯決定規則，以決定該網路的易損性狀態。

英文發明摘要（發明之名稱：METHOD, COMPUTER-READABLE MEDIUM AND DATA PROCESSING SYSTEM FOR ASSESSING THE SECURITY POSTURE OF A NETWORK）

A method and data processing system assesses the security vulnerability of a network. A system object model database is created and supports the information data requirements of disparate network vulnerability analysis programs. Only the required data from the system object model database representing the network is imported to the programs, which then analyze the network to produce data results from each program. These data results are stored in a common system model database and within the data fact base. Goal oriented fuzzy logic decision rules are applied to determine the vulnerability posture of the network.

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂 線

公告本

A8
B8
C8
D8

六、申請專利範圍

1. 一種用以接達一網路之安全狀態的方法，包含下列步驟：

建立一系統物件模型資料庫，其代表一網路，其中該系統物件模型資料庫支援不同之網路易損性分析程式的資訊資料需求；

僅將來自代表該網路之系統物件模型資料庫的所需資料匯出至每一各別網路易損性分析程式；

以每一網路易損性分析程式分析該網路，而從每一程式產生資料結果；

將來自各別網路易損性分析程式之資料結果及共同系統模型資料庫儲存於一資料事實庫內；以及

於資料事實庫上應用目標導向模糊邏輯決定規則，以決定該網路的安全狀態。

2. 如申請專利範圍第 1 項之方法，其特徵為：透過與各別網路易損性程式相結合之濾波器，僅匯出來自系統物件模型資料庫的所需資料。

3. 如申請專利範圍第 1 項之方法，其特徵為：透過一整合應用程式規劃介面，將系統物件模型資料庫匯出至網路易損性分析程式。

4. 如申請專利範圍第 1 項之方法，其特徵為：將該網路模型化成為一圖形使用者介面的一映像。

5. 如申請專利範圍第 1 項之方法，其特徵為：設立一類別階層，用以定義網路易損性分析程式之組件，其中該等網路易損性分析程式共享共同資料和程式規劃特點。

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂

六、申請專利範圍

6. 如申請專利範圍第1項之方法，其特徵為：運行該網路易損性分析程式，以獲得屬於網路系統細節，網路拓樸，節點層易損性和網路層易損性之資料結果。

7. 一種用以接達一網路之安全狀態的方法，包含下列步驟：

建立一系統物件模型資料庫，其代表一網路，其中該系統物件模型資料庫支援不同之網路易損性分析程式的資訊資料需求，而且僅將來自系統物件模型資料庫之所需資料匯出至各別網路易損性分析程式，而從每一程式產生資料結果；

將來自各別網路易損性分析程式之資料結果及共同系統模型資料庫儲存於一資料事實庫內，而且藉由使用複數個模糊匯入規則，於資料事實庫上應用目標導向模糊邏輯決定規則，以合併來自網路易損性分析程式之結果，而且決定該網路的安全狀態。

8. 如申請專利範圍第7項之方法，其特徵為：根據證據推理應用模糊邏輯決定規則。

9. 如申請專利範圍第7項之方法，其特徵為：透過與各別網路易損性程式相結合之濾波器，僅匯出所需資料。

10. 如申請專利範圍第7項之方法，其特徵為：透過一整合應用程式規劃介面，將系統物件模型資料庫匯出至網路易損性分析程式。

11. 如申請專利範圍第7項之方法，其特徵為：將該網路模型化成為一圖形使用者介面的一映像。

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂

六、申請專利範圍

12. 如申請專利範圍第7項之方法，其特徵為：設立一類別階層，用以定義不同網路易損性分析程式之組件，其中該等網路易損性分析程式共享共同資料和程式規劃特點。

13. 如申請專利範圍第7項之方法，其特徵為：運行網路易損性分析程式，以獲得屬於網路系統細節，網路拓樸，節點層易損性和網路層易損性之資料結果。

14. 一種含有一電腦程式之電腦可讀取媒體，其中該電腦程式包含指令，用以引發一電腦建立一系統物件模型資料庫，其代表一網路，其中該系統物件模型資料庫支援不同之網路易損性分析程式的資訊資料需求；

僅將來自代表該網路之系統物件模型資料庫的所需資料匯出至每一各別網路易損性分析程式；

以每一網路易損性分析程式分析該網路，而從每一程式產生資料結果；

將來自各別網路易損性分析程式之結果及共同系統模型資料庫儲存於一資料事實庫內，而且於資料事實庫上應用目標導向模糊邏輯決定規則，以決定該網路的安全狀態。

15. 如申請專利範圍第14項之電腦可讀取媒體，其特徵為：藉由使用複數個模糊匯出規則，而應用模糊邏輯決定規則，以合併來自網路易損性分析程式之結果。

16. 如申請專利範圍第14項之電腦可讀取媒體，其特徵為：根據證據推理應用模糊邏輯決定規則。

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

17. 如申請專利範圍第14項之電腦可讀取媒體，其特徵為：透過與各別網路易損性程式相結合之濾波器，僅匯出所需資料。

18. 如申請專利範圍第14項之電腦可讀取媒體，其特徵為：透過一整合應用程式規劃介面，將系統物件模型資料庫匯入至網路易損性分析程式。

19. 如申請專利範圍第14項之電腦可讀取媒體，其特徵為：將該網路模型化成為一圖形使用者介面的一映像。

20. 如申請專利範圍第14項之電腦可讀取媒體，其特徵為：設立一類別階層，以定義網路易損性分析程式之電腦，其中該等網路易損性分析程式共享共同資料和程式規劃特點。

21. 如申請專利範圍第14項之電腦可讀取媒體，其特徵為：運行網路易損性分析程式，以獲得屬於網路系統細節，網路拓樸，節點層易損性和網路層易損性之資料結果。

22. 一種用以接達一網路之安全狀態的資料處理系統，包含：

複數個不同之網路易損性分析程式，用以分析一網路；

一系統物件模型資料庫，其代表分析之網路，其中該系統物件模型資料庫支援網路易損性分析程式的資訊資料需求；

一應用程式規劃介面，用以將該網路之系統物件模型資料庫匯入至網路易損性分析程式；

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

一濾波器，與應用程式規劃介面和每一各別網路易損性分析程式相結合，用以過濾來自系統物件模型資料庫之資料，而且僅匯入所需資料；

一資料事實庫，於分析該網路和共同系統模型資料庫後，用以儲存從各別網路易損性分析程式所獲得之結果，以及

一模糊邏輯處理器，藉由使用複數個模糊匯出規則，於事實資料庫上應用目標導向模糊邏輯決定規則，以合併來自網路易損性分析程式之結果，而且決定該網路的安全狀態。

23. 如申請專利範圍第22項之資料處理系統，其特徵為：該模糊邏輯決定規則係根據證據推理。

24. 如申請專利範圍第22項之資料處理系統，其特徵為：用以匯出系統物件模型資料庫之應用程式規劃介面包含一圖形使用者介面。

25. 如申請專利範圍第22項之資料處理系統，其特徵為：一圖形使用者介面，用以將該網路模型化成為一映像。

26. 如申請專利範圍第22項之資料處理系統，其特徵為：一圖形使用者介面，用以顯示該網路的安全狀態。

27. 如申請專利範圍第22項之資料處理系統，其特徵為：該資料庫進一步包含一物件導向類別階層，用以定義網路易損性分析程式之組件，其中該等網路易損性分析程式共享共同資料和程式規劃特點。

本紙張尺度適用中國國家標準(CNS) A4規格(210×297公釐)

裝 訂

年 月 日 修正 補充

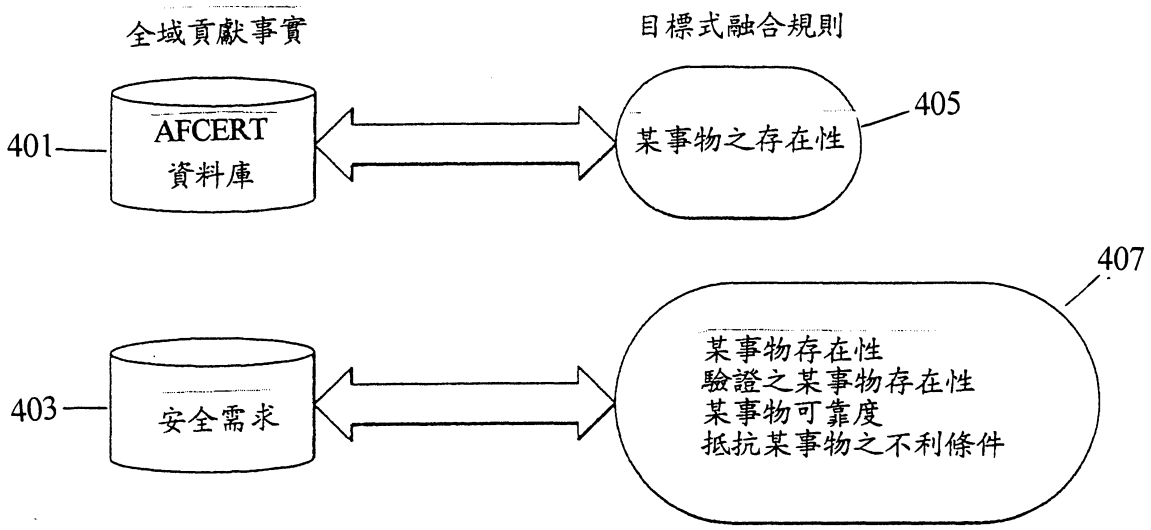

圖 13

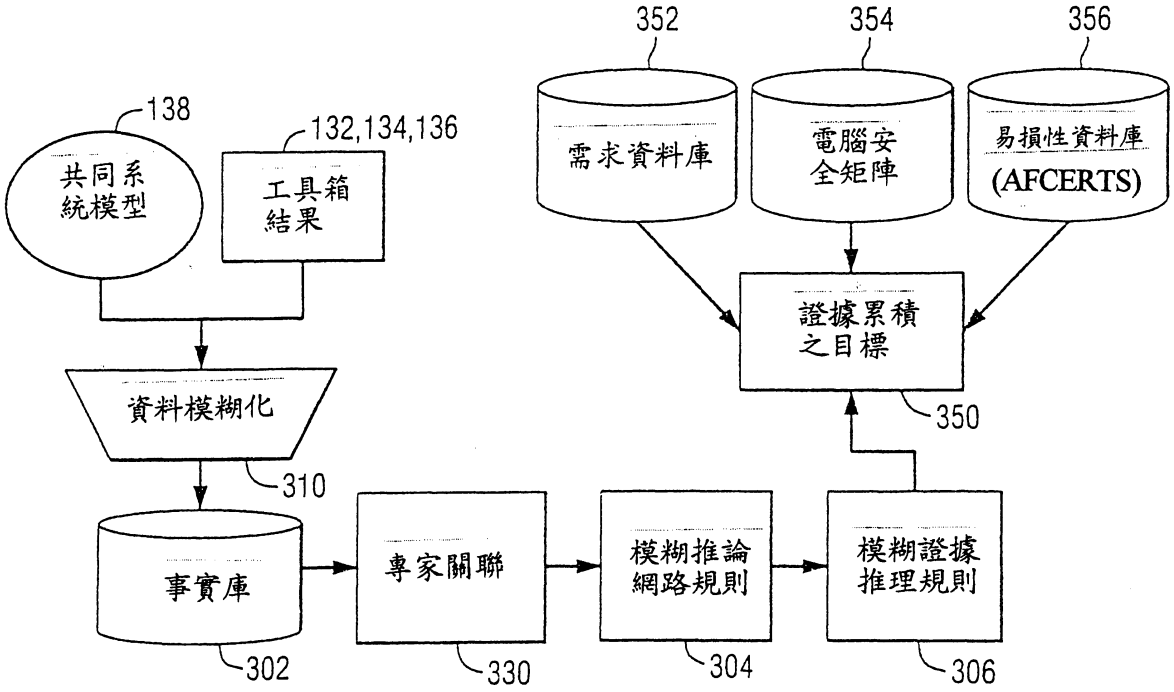

圖 14

修正補充
年 月 日

系統類別圖

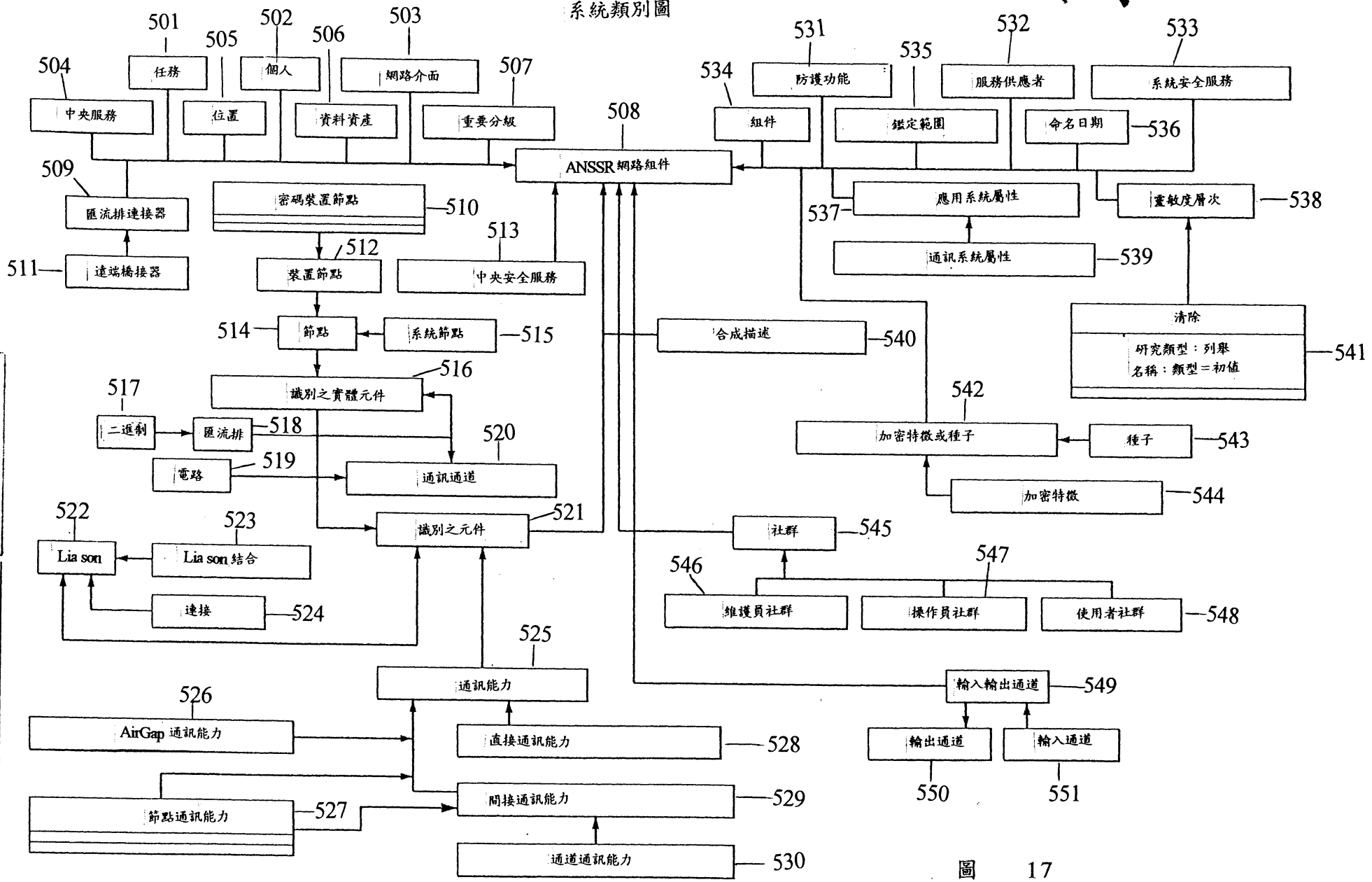

圖 17