公告本

發明專利說明書

I220207

※ 申請案號：92120280

※ 申請日期：92 年 7 月 24 日　　※IPC 分類：G06F17/30

壹、發明名稱：（中文/英文）

用於可能安全曝露的預警指標之查詢回覆資料分析的方法

METHOD OF QUERY RETURN DATA ANALYSIS FOR EARLY WARNING INDICATORS OF POSSIBLE SECURITY EXPOSURES

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）

傑拉德羅森瑟爾/ Gerald Rosenthal

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, New York 10504, USA

國　籍：（中文/英文）

美國 / USA

參、發明人：（共 2 人）

姓　名：（中文/英文）

1.理查 D. 迪廷格爾 / Richard D. Dettinger

2.理查 J. 史帝文斯 / Richard J. Stevens

住居所地址：（中文/英文）

1.美國明尼蘇達州羅契斯特市西北肯辛頓巷 5305 號

5305 Kensington Lane N.W., Rochester, Minnesota 55901, U.S.A.

2.美國明尼蘇達州曼陀市第 252 大街 61432 號

61432 252nd Avenue, Mantorville, Minnesota 55955, U.S.A.

國　籍：(中文/英文)

1. 美國 / USA

2. 美國 / USA

肆、聲明事項：

◎本案申請前已向下列國家(地區)申請專利 [V] 主張國際優先權：

【格式請依：受理國家(地區)；申請日；申請案號數　順序註記】

美國；2002 年 10 月 31 日；10/284,944

玖、發明說明：

【發明所屬之技術領域】

本發明大致上與資料處理特別是與保護一資料庫免於不當或未授權存取的方法有關。

【先前技術】

資料庫為電腦化的資料儲存及擷取系統。一種關聯資料庫管理系統為一電腦資料庫管理系統(DBMS)，其使用關聯技術以儲存並擷取資料。最普遍的資料庫種類為關聯資料庫，為一種資料於其中被定義的表格式資料庫，因而可以數種不同的方法被重新組織及存取。

不論該特定結構，在一 DBMS 中一請求實體(例如一應用程式或作業系統)藉由送出一資料庫存取請求要求存取至一特定資料庫。這些請求可包含如簡易對話檢視要求或是處理及處理之結合，其操作、讀取、改變並增加特定記錄於該資料庫中。利用高階查詢語言例如結構化查詢語言(SQL)製作這些請求。說明地，SQL 用於製作互動式查詢以從一資料庫取得並更新資訊，該資料庫像是國際商業機器(IBM) 的 DB2、微軟的 SQL 伺服器以及甲骨文、Sybase 與 Computer Associates 的資料庫產品。“查詢”意指一組用於自一儲存的資料庫擷取資料的指令。查詢採取指令語言的形式使得程式設計者與程式選擇、插入、更新並找出資料的位置等等。

對資料庫而言，安全是一很重要的議題。資料庫通常

含有機密的或敏感的內容，其需要某種程度的安全以保護其存取。舉例來說，醫療記錄被認為是高度私人及秘密的。因此存取醫療記錄通常僅限於特定使用者。為了達到此目的，傳統的資料庫管理系統可實施指定一授權層級的使用者特性資料。一使用者是否可存取某些特定資料將視其各自特性資料中指定的使用者授權層級而定。

然而，先前的方式是高度無彈性且靜態的。實際上，此一方式可能會阻擋使用者存取較其所應得的範圍更為廣大的資料。因此一資料庫的效率可能會實質地受限。反之若安全過於鬆散則會危及敏感的資料。因而需要的是資料存取性及安全性的平衡。

為了描述傳統資料庫的缺點，舉例來說若一醫療資料庫中使用者唯一被允許看見的是臨床號碼，以確保在該資料庫具有記錄之病人的匿名性。一使用者藉由使用其已知資訊送出一連串精心製作的查詢，仍然可以一定程度地確定該病人的身份。此一過程在此處被稱之為查詢結合分析。以下為說明的一連串查詢，用於依照一臨床號碼識別一特定個人，以及每個查詢回報的一些獨特的病人記錄：

查詢	結果
1998 年被診斷患有阿茲海默症的人	1200
結婚並居住於加州的人	6000
介於 70 到 80 歲的人	14,000
在 1999 及 2001 年而未於其他年看診的人	6000

個別來說，前述每個查詢回報一合理數量的結果。然而整體而言，合乎每個條件的結果數量將會大大地變少，也許僅有一人。既已確定一個人的臨床號碼，一使用者可執行任何回報臨床號碼及任何其他資訊的查詢，並識別何資訊會對應至一個人。

前述僅為一種使用者如何可利用傳統資料庫的範例。可使用許多其他破壞性的技術以適當地繞過安全機制以保護資料庫中包含的資料。

因此對於資料庫而言需要改善的安全機制。

【發明內容】

本發明大致上係指用於資料庫安全之一方法、系統及物品之產品。

在一具體實施例中，提供一種提供關於資料之安全的方法。一具體實施例包含接收由一使用者向一資料庫送出之查詢；並基於至少一種以下方法判定一違反安全形式是否存在：(i)關於使用者先前送出之至少一其他查詢進行執行前比較分析；以及(ii)對於執行該查詢所回報之結果以及執行至少一先前送出的其他查詢所回報之結果進行執行後比較分析。

提供關於資料安全之其他方法包含接收一使用者送出的多個查詢；向一資料庫執行該多個查詢；接收該使用者隨後向該資料庫送出的查詢；並基於該多個查詢與隨後的查詢，有計畫地判定一使用者自該資料庫存取一未授權數

量資料的努力是否是可加以識別。

另外一種提供資料安全性的方法包含自一使用者接收多個查詢；向一資料庫執行該多個查詢；接收該使用者隨後向該資料庫送出的查詢；並基於該多個查詢及隨後的查詢，有計畫地判定一使用者繞過安全限制以阻止個人之唯一識別的努力是否可加以識別。

另外一種提供資料安全的方法具有一特定實體資料呈現，該方法包含提供一查詢規格，其含有多個用於定義抽象查詢的邏輯欄位；提供對應該多個邏輯欄位至該資料之物理實體的對應規則；提供安全規則；接收一使用者向該資料送出之一抽象查詢，其中依據該查詢規格定義該抽象查詢並配置至少一邏輯欄位數值。

仍有另一種具體實施例提供含有指令的一種電腦可讀取媒體，當執行該指令時執行一安全違反識別操作，其包含：接收由一使用者向一資料庫送出的一查詢；並基於至少一種以下方法判定一違反安全形式是否存在：(i)關於使用者先前送出之至少一其他查詢進行執行前比較分析；以及(ii)對於執行該查詢所回報之結果以及執行至少一先前送出的其他查詢所回報之結果進行執行後比較分析。

仍有另一種具體實施例提供含有安全確認指令的一電腦可讀取媒體，當執行該指令時執行一安全確認操作，其包含：接收來自一使用者的多個查詢；向一資料庫執行該多個查詢；接收該使用者隨後向該資料庫送出的查詢；執

行該隨後的查詢；並基於該多個查詢及隨後的查詢，有計畫地判定一使用者繞過安全限制以阻止個人之唯一識別的努力是否可加以識別。

仍有另外一種具體實施例提供一種含有資訊儲存於其上的電腦可讀取媒體，該資訊包含：包含多個用於定義抽象查詢的邏輯欄位；對應該多個邏輯欄位至資料之物理實體的多個對應規則；多個安全規則；可執行的一運行時元件以回應接收一使用者向該資料送出之一抽象查詢執行一安全違反動作偵測，其中依據該查詢規格定義該抽象查詢並配置至少一邏輯欄位數值。該安全違反動作偵測操作包含接收一使用者向該資料送出的一抽象查詢，其中依據該查詢規格定義該抽象查詢並配置至少一邏輯欄位數值；並分析關於先前自使用者接收之至少一抽象查詢的該抽象查詢以偵測安全違反動作的存在並提示調用一安全規則。

【實施方式】

本發明大致上係指用於判定使用者未授權的存取資料嘗試之一方法、系統及物品之產品。大致上，在執行之前於一查詢上執行分析且/或在執行該查詢所回報的結果上執行分析。在一具體實施例中，一可能的安全違反之偵測引起一個或多個待實施的安全措施。舉例來說，在一具體實施例中一使用者的查詢未被執行。在另一具體實施例中，該事件被記錄且/或向一管理員通知該事件。

在一具體實施例中，實施安全特徵為一資料邏輯模型的部分。實施該邏輯模型為資料儲存抽象層，其提供該潛在資料儲存的一邏輯觀點。在此方式中，該資料獨立於其被實體呈現的特定種類。一查詢抽象層也被提供且以該資料儲存抽象層為基礎。一執行時元件對一抽象查詢執行轉譯為一種可對一特定實體資料呈現使用之格式。然而，雖然此處描述之抽象模型提供本發明之一個或多個具體實施例，但習知技藝人士將瞭解此處提供之概念可以在沒有一抽象模型的情況下被實施而仍可提供相同或相似的結果。

實施本發明之一具體實施例為一程式產品以伴隨一電腦系統例如第 1 圖及以下所述之電腦系統使用。該程式產品之程式定義該具體實施例的功能(包含此處所述之方法)並可容納於數種攜帶訊號的媒體中。說明的攜帶訊號媒體包含但不限於：(i)資訊永久儲存於不可寫入儲存媒體上(例如一電腦中的唯讀記憶體像是 CD-ROM 光碟機可讀取的 CD-ROM)；(ii)可修改資訊儲存於可寫入儲存媒體上(例如一軟碟機中的軟碟或硬碟機)；或(iii)藉由一通訊媒體傳送至一電腦的資訊，例如透過一電腦或電話網路，包含無線通訊。之後的具體實施例特別地包含自網際網路或其他網路下載的資訊。當這些訊號攜帶媒體攜帶指出本發明之功能的電腦可讀取指令時，便代表本發明之具體實施例。

大體上，為了實施本發明之具體實施例所執行的常式可為一作業系統的部分或一特定應用程式、元件、程式、模組、物件或一連串指令。本發明的軟體典型地由許多指

令組成，其將由本機電腦轉換為一機器可讀取格式以及隨後可執行的指令。同時該程式由多種變數以及資料結構組成，該資料結構不是區域地位於該程式便是位於記憶體中或儲存裝置上。此外，可基於在本發明之一特定具體實施例中實施之應用程式的目的辨識此後所述之各種程式。然而應瞭解其遵循的任何特定術語僅是為了方便而使用，因此本發明不應限於在這些術語所定義及/或應用的任何特定應用程式中使用。

環境之實體觀點

第 1 圖描述本發明之具體實施例可被實施於其中的一網路系統 100 之一方塊圖。大體而言，該網路系統 100 包含一客戶端(例如使用者)電腦 102(三個此種客戶端電腦 102 顯示於圖中)以及至少一伺服器 104(一此類伺服器 104)。該客戶端電腦 102 以及伺服器電腦 104 透過一網路 126 相連。大體而言，該網路 126 可為一區域網路(LAN)及/或一廣域網路(WAN)。在一特定具體實施例中，該網路 126 為網際網路。

該客戶端電腦 102 包含一中央處理器(CPU)110 透過一匯流排 130 連接至一記憶體 112、儲存 114、一輸入裝置 116、一輸出裝置 119 以及一網路介面裝置 118。該輸入裝置 116 可為任何給予輸入至該客戶端電腦 102 的裝置。例如一鍵盤、鍵盤組、光筆、觸控螢幕、軌跡球或語音辨識單元、音訊/視訊播放器等等可被使用的。該輸出

裝置119可為任何給予輸出至該使用者的裝置，例如任何傳統顯示螢幕。雖然獨立於該輸入裝置116顯示，該輸出裝置119可與該輸入裝置116結合。例如內建觸控螢幕的一顯示螢幕、內建鍵盤的一顯示器、或可使用之與一文字語音轉換器結合的一語音辨識單元。

該網路介面裝置118可為任何進/出裝置，設置該裝置以允許該客戶端電腦102與該伺服器電腦104透過該網路126之網路通訊。舉例來說，該網路介面裝置118可為一網路配接器或其他網路界面卡(NIC)。

儲存114最好是一直接存取儲存裝置(DASD)。雖然圖上顯示為一單一裝置，其可為固定的及/或可移動儲存裝置的組合，例如為硬碟機、軟碟機、磁帶機、可移動記憶卡或光儲存器。該記憶體112與儲存114可為一包括多個主要及次要儲存裝置之虛擬位址空間的部分。

該記憶體112最好為一夠大的隨機存取記憶體以容納本發明必要的程式設計及資料結構。雖然該記憶體112被顯示為單一實體，應瞭解該記憶體112事實上包含許多模組，且該記憶體112可存在於多個層級，從高速暫存器或快取記憶體至低速但較大的DRAM晶片。

舉例說明地，該記憶體112包含一作業系統124。舉例說明之進一步使用的作業系統包含Linux及微軟的Windows®。更平常地，任何支援此處功能的作業系統均可被使用。

該記憶體112也同時顯示包含一瀏覽器程式122，當

其於 CPU 110 執行時提供各個伺服器 104 之間的導引並在一個或多個伺服器 104 上設置網路位址。在一具體實施例中，該瀏覽器程式 122 包含一植基於網路的圖形使用者介面(GUI)，其允許使用者顯示超文字標記語言(HTML)資訊。然而更平常地，該瀏覽器程式 122 可為任何可以演算該伺服器電腦 104 傳送出的資訊的程式。可以一種類似於該客戶端電腦 102 的方式實體地安排該伺服器電腦 104。因此，所示之伺服器電腦大致包含一 CPU 130、一記憶體 132 以及一儲存裝置 134，彼此透過一匯流排 136 相連。記憶體 132 可為一夠大的隨機存取記憶體以容納位於該伺服器電腦 104 之必要的程式設計以及資料結構。

該伺服器電腦 104 大致上由顯示位於記憶體 132 之作業系統 138 所控制。該作業系統 138 的範例包括 IBM OS/400®、UNIX、微軟 Windows®等等。更平常地，任何可支援此處描述之功能的作業系統均可被使用。

該記憶體 132 更更包含一個或多個應用程式 140 以及一抽象查詢介面 146。該應用程式 140 以及該抽象查詢介面 146 為軟體產品，其包含許多位於電腦系統 100 之各個記憶體及儲存裝置以及各個時間的指令。當伺服器 104 的一個或多個處理器 130 讀取並執行時，該應用程式 140 以及抽象查詢介面 146 使電腦系統 100 執行為了執行本發明各種態樣中包含之步驟或項目所必要之步驟。該應用程式 140(或更平常地說，任何請求實體包括該作業系統 138 以及最高階的使用者)向一資料庫(例如資料庫 $156_1 \ldots 156_N$，

全體被稱之為資料庫 156)送出查詢。如圖所示，該資料庫 156 為儲存 134 中一資料庫管理系統(DBMS)的部分。該資料庫 156 代表任何資料的蒐集而不論特定實體表示。藉由說明，可依據一相關方案(可被 SQL 查詢所存取)或依據一 XML 方案(可由 XML 查詢所存取)組織該資料庫 156。然而，本發明不限於一特定方案且已考慮到延伸至現今未知的方案。在此所使用之術語“方案”大致上係指一資料的特定安排。

在一具體實施例中，依據一包含每個應用程式 140 的應用程式查詢規格 142 定義由該應用程式所送出的查詢。該應用程式 140 所送出的查詢可預先定義(即硬體編碼為該應用程式 140 之部分)也可回應輸入(例如使用者輸入)而被建立。在任何一種情況下，使用由該抽象查詢介面 146 所定義之邏輯欄位組成/執行該查詢(在此處係指“抽象查詢”)。特別地，在該抽象查詢中使用的邏輯欄位是由該抽象查詢介面 146 之一資料儲存抽象元件 148 所定義。一執行時元件 150 執行該抽象查詢，其首先將該抽象查詢轉換成與 DBMS 中含有之資料的實體表示一致的格式。

在一具體實施例中，該資料儲存抽象元件 148 配有安全資訊 162。對於不以抽象模型(或其等同物)為基礎的具體實施例而言，該安全資訊可位於其他地方。在一具體實施例中，該安全資訊 162 包含與一個或多個欄位相關的線索。此線索的態樣將於以下進一步地描述。

操作該執行時元件 150 以執行各種分析且於某些具體

實施例中，依據執行分析得到之結果執行各種安全特性或採取其他行動。因此，圖中所示之執行時元件 150 配有一安全演算法 151(其可為代表性的或多個演算法)，其實施此處所述之方法。大體而言，該執行時元件 150 所實施之安全特性可應用至一特定使用者、一群使用者或所有使用者。

在一具體實施例中，一使用者透過一圖形使用者介面(GUI)指定一查詢的項目。該 GUIs 的內容是由該應用程式 140 所產生。在一特定具體實施例中，該 GUI 內容為一超文字標記語言(HTML)內容，其可在客戶端電腦系統 102 上利用瀏覽器程式 122 加以演算。因而該記憶體 132 包含一種用於服務來自該客戶端電腦 102 之請求的超文字傳輸協定(http)伺服器處理 152(例如一網頁伺服器)。舉例來說，該伺服器處理 152 可回應存取該資料庫 156 的請求，其如圖所示位於該伺服器 104。進入的客戶端對於來自一資料庫 156 之資料的請求調用一應用程式 140。當該處理器 130 加以執行時，該應用程式 140 使伺服器電腦 104 執行本發明各種態樣所包含之步驟或項目，包括存取該資料庫 156。在一具體實施例中，該應用程式 140 包含用於建立 GUI 項目之伺服器小程式，該 GUI 項目隨後由瀏覽器程式 122 演算。

第 1 圖僅為關於網路客戶端 102 電腦及伺服器電腦 104 之一硬體/軟體設置。本發明的具體實施例可應用至任何相較的硬體設置，不論該電腦系統是否為複雜的、多

使用者計算儀器、單一使用者工作站、或本身不具有非依電性儲存的網路裝置。此外，應瞭解雖然所參考的是包含HTML的特定標記語言，本發明並不限於一特定語言、標準或版本。因此，習知技藝人士將瞭解到本發明可適應其他標記語言以及非標記語言，且亦可適應一特定標記語言未來的改變以及其他目前未知的語言。同樣地，第1圖所示之http伺服器處理152僅為說明之用，其他用於支援任何已知或未知協定的其他具體實施例亦在考慮之中。

第2A-B圖顯示本發明之元件的一說明關係圖200。請求實體(例如應用程式140之一)送出一詢問202，該詢問由該請求實體各自的應用程式詢問規格142所定義。由於該詢問依照抽象(例如邏輯的)欄位所組成而非直接參照DBMS 154中潛在的物理資料實體，故結果詢問202在此係指一“抽象詢問”。因此，可定義該抽象查詢為獨立於所使用的特定潛在資料表示。在一具體實施例中，該應用程式詢問規格142可同時包含用於資料選擇之標準(選擇標準204)以及基於該選擇標準204之待回報欄位的一明確規格(回報資料規格206)。

第2B圖中所示之符合該抽象查詢202的一說明抽象查詢如以下第I表所示。藉由說明，使用XML定義該抽象查詢202。然而，任何其他語言也可有利地加以使用。

第I表 詢問範例

```
001 <?xml 版本="1.0"?>
```

```
002 <!--詢問串表示：(名="Mary" 及 姓="McGoon") 或
003 狀態="NC"-->
004 <詢問抽象>
005   <選擇>
006     <條件 內部 ID="4">
007       <條件 欄位="名" 運算子="EQ" 數值="Mary"
008 內部 ID="1">
009         <條件 欄位="姓" 運算子="EQ" 數值=
"McGoon"
010 內部 ID="3" rel 運算子="及"></條件>
011     </條件>
012     <條件 欄位="州" 運算子="EQ" 數值="NC" 內
013 部 ID="2" rel 運算子="或"></條件>
014   </選擇>
015   <結果>
016     <欄位 名稱="名"/>
017     <欄位 名稱="姓"/>
018     <欄位 名稱="州"/>
019   </結果>
020 </詢問抽象>
```

說明地，第 1 表中所示之抽象查詢包含一選擇規格(005-014 行)，其含有選擇標準以及一結果規格(015-019 行)。在一具體實施例中，一選擇標準由一欄位名稱(關於

一邏輯欄位)、一比較運算子(=, >, <,等等)以及一數值表示(該欄位所要比較的)組成。在一具體實施例中，結果規格為待回應作為查詢執行之一結果的抽象欄位的一列表。在該抽象查詢中的一結果規格可由一欄位名稱以及排列標準所構成。

由應用程式查詢規格 142 所指定並用於組成該抽象查詢 202 的邏輯欄位乃是由該資料儲存抽象元件 148 所定義。大體而言，該資料儲存抽象元件 148 揭露資訊作為一組可用於該應用程式 140(其可回應使用者輸入查詢條件)所送出之一查詢(例如該抽象查詢 202)中的邏輯欄位以指定資料選擇的標準並指定自一查詢操作所回報之結果資料的格式。該邏輯欄位乃獨立於該 DBMS 154 正在使用中的潛在資料表示而加以定義，因而形成該查詢與該潛在資料表示鬆散地連結。

大體而言，該資料儲存抽象元件 148 包含許多欄位規格 208_1、208_2、208_3...(藉由範例顯示三個)，全體被稱之為欄位規格 208。特別地，提供一欄位規格給各個可組成一抽象查詢的邏輯欄位。在一具體實施例中，一欄位規格 208 包含一邏輯欄位名稱 210_1、210_2、210_3(全體稱為欄位名稱 210)以及一相關存取方法 212_1、212_2、212_3(全體稱為存取方法 212)。

該存取方法 212 連接(即對應)該邏輯欄位名稱至一資料庫(例如資料庫 156 其中之一)中的一特定實體資料表示 214_1、214_2...214_N。透過圖示，兩個資料表示顯示於第 2A

圖中，分別為一 XML 資料表示 214_1 以及一相關資料表示 214_2。然而，該實體資料表示 214_N 指出不論已知或未知的任何其他資料表示均已加以考慮。

在一具體實施例中，一單一資料儲存抽象元件 148 含有用於兩個以上之實體資料表示 214 的欄位規格(伴隨相關存取方法)。在一替代的具體實施例中，提供不同的一單一資料儲存抽象元件 148 給每個獨立實體資料表示 214。而在另外一個具體實施例中，多個資料儲存抽象元件 148 揭露相同潛在實體資料的不同部分(其可包含一個或多個實體資料表示 214)。在此方式中，多個使用者可同時使用一單一應用程式 140 以存取該相同潛在資料，其中揭露至該應用程式之潛在資料的特定部分由個別的資料儲存抽象元件 148 決定。

任何數量的存取方法依待支援之不同種類的邏輯欄位數目而定。在一具體實施例中，提供存取方法給簡單欄位、過濾欄位以及組合欄位。欄位規格 208_1、208_2、208_3 個別地作為簡單欄位存取方法 212_1、212_2、212_3 的說明。簡單欄位直接地對應至潛在實體資料表示的一特定實體(例如一欄位對應至一給定資料庫表與欄。藉由圖示說明，第 B 圖所示之簡單欄位存取方法 212_1 對應該邏輯欄位名稱 210_1(“名”)至一名為“聯絡”之表中名為“f_名稱”的行。過濾欄位(第 2 圖中未舉例說明)識別一相關物理實體並提供用於定義該實體資料表示中的項目之一特定子集合的規則。一過濾欄位的範例為一紐約郵遞區號欄位，其對應至

郵遞區號的實體表示並將該資料僅限於那些紐約地區範圍的郵遞區號。組合存取方法(第 2 圖中未舉例說明)使用提供存取方法定義之部分的表式自一個或多個實體欄位計算一邏輯欄位。藉此可計算該潛在資料表示中未存在的資訊。一範例為一營業價格欄位與一營業稅率欄位相乘所組成的一營業稅欄位。

考慮到該潛在資料之任何給定資料種類(例如日期、小數等等)的格式可能有所改變。在一具體實施例中，欄位規格 208 包含一反映該潛在資料之格式的種類屬性。然而在另一具體實施例中，該欄位規格 208 的資料格式與相關潛在實體資料不同，在該情況中一存取方法負責回報該請求實體認為的適當格式之資料。因此該存取方法必須知道所認為的是何種格式的資料(即依據該邏輯欄位)以及該潛在實體資料的實際格式。該存取方法之後可轉換該潛在實體資料為該邏輯欄位的格式。

透過該範例，第 2 圖中所示之資料儲存抽象元件的欄位規格 208 為對應至呈現於相關資料表示 214_2 中的資料的代表。然而，其他的情況中該資料儲存抽象元件 148 對應該邏輯欄位至其他實體資料表示，例如 XML。

在一具體實施例中，伴隨上面第 1 圖中概述之安全資訊 162 配置一個或多個欄位規格 208。在圖示的具體實施例中，僅有欄位定義 208_3 與安全資訊 162 相結合。因此應瞭解並不是所有的欄位定義必須包含安全資訊。在本範例中，該安全資訊為一種具有“線索”數值的屬性 220。應

瞭解不需在該資料儲存抽象 148 中指定該線索數值，但卻可例如作為一配置檔案的數值。在操作中，一特定階段列表 153(許多顯示於第一圖中)具有一線索而為了每個欄位加以維護且使用者所擁有的包含於至少一查詢中。特別地，該列表 153(例如一雜湊表)包含所有已自該相關欄位在一特定階段所回報的數值。因此大致來說，一特定使用者的尺寸表隨著每個查詢增加，該查詢回報先前未回報的結果（即非重疊查詢結果）。在一具體實施例中，該表可為持續的，然而在另一具體實施例中當一使用者登出或在一使用者未行動一段時間後便將該表刪除。之後便可執行一查詢結果分析，將於以下更詳細的描述。在某些情況中，依據一安全動作定義 213 採取一行動。說明的行動將於以下描述。

第 II 表顯示與第 2 圖中所示之資料儲存抽象元件 148 一致的資料儲存抽象元件。藉由該說明，使用 XML 定義該資料儲存抽象 148。然而也可有利地使用任何其他語言。

第 II 表 資料儲存抽象範例

```
<?xml 版本="1.0">
<資料儲存>
 <目錄 名稱="人口統計學的">
   <欄位 可查詢的="是" 名稱="名" 可顯示="是">
    <存取方法>
```

<簡單 欄名稱="f_名稱" 表名稱="聯絡"></簡單>
</存取方法>
<種類 基本種類="Char"></種類>
</欄位>
<欄位 可查詢的="是" 名稱="姓" 可顯示="是">
<存取方法>
<簡單 欄名稱="l_名稱" 表名稱="聯絡"></簡單>
</存取方法>
<種類 基本種類="Char"></種類>
</欄位>
<欄位 可查詢的="是" 名稱="臨床號碼" 可顯示="是">
<存取方法>
<簡單 欄名稱="CN" 表名稱="聯絡"></簡單>
</存取方法>
<種類 基本種類="Char" 數值="真"></種類>
<安全>
<安全規則>
<使用者>所有</使用者>
<動作>執行及記錄</動作>
</安全規則>
<安全規則>
<使用者>安全人員</使用者>
<動作>執行及記錄</動作>

```
        </安全規則>
        <安全規則>
          <使用者>cujo</使用者>
          <動作>無動作</動作>
        </安全規則>
      </安全>
    </欄位>
  </目錄>
</資料儲存>
```

第 3 圖顯示一說明的執行時方法 300，該方法舉例說明該執行時元件之操作的一具體實施例。當該執行時元件 150 接收到一作為輸入的抽象查詢實體(例如第 2 圖中所示之抽象查詢 202)時，便引入該方法 300 於步驟 302。於步驟 304 中，該執行時元件讀取並分析該抽象查詢實體並定位個別選擇標準與所求結果欄位。於步驟 309 中執行某些預備陳述架構分析，該分析將伴隨以下所述之執行後結果分析有利地加以使用。特別地，於步驟 309 中計算一查詢共同數值(commonality value)。該查詢共同數值乃是藉由判定現在查詢與所有過去查詢之間的相對共同性來計算。舉例來說，如果一查詢具有兩種條件，臨床號碼<1000 以及診斷=z，則這兩種查詢具有 50%的共同性。

於步驟 306 中，該執行時元件輸入一迴路以處理呈現於該抽象查詢中的每個查詢選擇標準陳述，因而建立一具

體查詢的一資料選擇部分。在一具體實施例中，一選擇標準(在此也被稱為一條件)由一欄位名稱(關於一邏輯欄位)、一比較運算子(=, <, >, 等等)以及正與該欄位相比較的一數值表式所組成。於步驟 308 中，該執行時元件 150 使用來自於該抽象查詢之一選擇標準的欄位名稱以查詢資料儲存抽象 148 中欄位之定義。如上所述，該欄位定義包含用於存取與該欄位相關聯之實體資料之存取方法的一定義。

自步驟 310 開始採取進一步的步驟以執行陳述架構分析。特別地，於步驟 310 中對每個先前查詢輸入一迴路。意即一查詢歷史表 157(第 1 圖)被存取及遍覽(traversed)。大體而言，該查詢歷史表 157 為曾被執行之查詢的一列表。每次執行一新查詢時便將一新查詢填入該查詢歷史表 157。在一具體實施例中，此資料結構包含抽象形式的 SQL 查詢。可視該歷史何時釋出而配置該資料結構。釋出該歷史的一種選擇為當該階段終止時。另外一個選擇為經過一特定時期後。於步驟 312 中，該執行時元件 150 判定正在處理當中之查詢選擇(步驟 306)的欄位是否被用於在步驟 310 中由歷史查詢表 157 所擷取的先前查詢中。當識別一先前查詢具有正在處理當中之查詢選擇(步驟 306)的欄位時，便執行關於該查詢選擇以及已識別先前查詢的分析(步驟 314)。於步驟 316 中，該執行時元件 150 判定該分析的結果(於步驟 314 中)是否需要採取某些行動。在一具體實施例中，該行動被指定於資料儲存抽象元件 148(參見

地 II 表)。安全行動包括記錄使用者的查詢(或其他永久資訊)、阻止該查詢被執行且/或終止該使用者之階段。更普遍地，習知技藝人士將瞭解當引入一安全規則時，任何種類的回應均可能被採取。注意到在第 II 表所描述之範例中，安全行動乃是用於個別使用者(例如 Cujo)、使用者群組(例如安全工作人員)以及所有使用者。在一存在多個行動用於一特定欄位之具體實施例中，採用對一使用者最為量身訂做的行動。因此特定於一個別使用者的行動優先於所有其他的行動，且特定於一群組的行動優先於特定於所有使用者的行動。只有在沒有其他對該使用者量身訂做之行動存在時才會採取一特定於所有使用者的行動。如果步驟 314 被否定地回應(即不需採取行動)，便處理回報至步驟 310，於該步驟中其他的先前查詢自歷史查詢表 157 擷取以供檢查。如果於步驟 316 中需要一行動，便於步驟 318 採取該行動。如果該行動是致命的(步驟 320)，則不執行該使用者查詢(步驟 322)。否則，處理回報至步驟 310。一旦已檢查位於歷史查詢表 157 中的每個先前查詢關於處理中的現在查詢選擇之欄位的存在後，該方法 300 前進至步驟 324。

該執行時元件 150 之後對處理中的邏輯欄位建立(步驟 324)一具體查詢投寄(contribution)。如同此處之定義，一具體查詢投寄為一用於以現在邏輯欄位為基礎執行資料選擇之具體查詢的部分。一具體查詢為一種以像是 SQL 與 XML 查詢之語言呈現的一種查詢，且與一特定實體資

料儲存(例如一關係資料庫或 XML 儲存)一致。因此，該具體查詢是用於定位並自該實體資料儲存擷取資料，由第1圖中的 DBMS 154 所表示。對該現在欄位建立之具體查詢投寄隨後被附加至一具體查詢陳述。該方法 300 稍後回到步驟 306 以開始處理抽象查詢的下一個欄位。因此，加入步驟 306 的處理在抽象查詢中的每個資料選擇欄位被重複執行，因而投寄額外的內容至待執行的最終查詢。

在建立該具體查詢之資料選擇部分後，該執行時元件 150 識別該資訊以回報作為查詢執行之一結果。如上所述，在一具體實施例中，該抽象查詢定義抽象欄位的一列表以回報作為查詢執行之一結果，在此稱為結果規格。位於該抽象查詢中的結果規格可由一欄位名稱及排序標準組成。因此，該方法 300 於步驟 328 加入一迴路(由步驟 328、330、332、334 定義)以附加結果欄位定義至建立中的具體查詢。於步驟 330 中，該執行時元件 150 查詢資料儲存抽象 148 中的一結果欄位名稱(自該抽象查詢的結果規格)且隨後自資料儲存抽象 148 擷取一結果欄位定義以識別對於現在邏輯結果欄位之待回報資料的實體位置。該執行時元件 150 隨後對邏輯結果欄位建立(如步驟 332)一具體查詢投寄(其屬於識別待回報資料之實體位置的具體查詢)。於步驟 334 中，具體查詢投寄隨後被附加至具體查詢陳述。一旦該抽象查詢中的每個結果規格已被處理，便於步驟 336 執行該查詢。

依據步驟 310 與 318 用於對一邏輯欄位建立一具體查

詢投寄之一方法的一具體實施例可參考第4圖之說明。於步驟402中，該方法400查詢與現在邏輯欄位相關聯之存取方法是否為一簡單存取方法。如果是的話，便基於實體資料位置資訊建立該具體查詢投寄且處理隨後依據上述之方法300而繼續。否則處理繼續至步驟406以查詢與該現在邏輯欄位相關聯之存取方法是否為一過濾的存取方法。如果是的話，便基於實體資料位置資訊對某些物理資料實體建立該具體查詢投寄(步驟408)。於步驟410中，該具體查詢投寄隨著用於與該物理資料實體相關聯之子集合資料的附加邏輯(過濾選擇)而延伸。處理隨後基於上述之方法300而繼續。

如果該存取方法並非為一過濾存取方法，處理自步驟406進行至步驟412，於該步驟中該方法400查詢該存取方法是否為一組合存取方法。如果該存取方法為一組合存取方法，對於該組合欄位表式中每個子欄位參照的實體資料位置被定位與擷取於步驟414。於步驟416中，對該組合欄位表式之邏輯欄位參照加上該組合欄位表式之實體欄位位置資訊的副標題，並藉此建立該具體查詢投寄。處理隨後依據上述之方法300而繼續。

如果該存取方法不是一組合存取方法，處理便自步驟412進行至步驟418。步驟418為本發明之具體實施例中所考慮之任何其他存取方法種類的代表。然而應瞭解具體實施例所考慮的較所有被實施之可使用存取方法少。舉例來說，在一具體實施例中僅使用簡單存取方法。在另一具

體實施例中，僅使用簡單存取方法以及過濾存取方法。

如上所述，如果一邏輯欄位指定一種與該潛在實體資料不同的資料格式，便有可能需要執行一資料轉換。在一具體實施例中，當依據該方法 400 對一邏輯欄位建立一具體查詢投寄時，對每個各自的存取方法執行一初始轉換。舉例來說，可以該步驟 404、408、與 416 之部分執行該轉換，或在上述步驟之後執行。於步驟 322 執行該查詢後，執行一隨後轉換，將實體資料格式轉換為邏輯欄位格式。當然如果該邏輯欄位定義的格式與潛在實體資料相同，便不需要任何轉換。

參考第 5 圖，該圖顯示一方法 500，其說明於步驟 314 所執行之分析的一具體實施例。記得該分析被執行於具有一般格式<欄位><運算子><數值>的一選擇/條件之上。於步驟 502 中，該運算子以及數值乃是用於判定該查詢選擇所涵蓋的範圍。於步驟 504 中，該執行時元件 150 檢查關於在步驟 310 中擷取自該歷史查詢表 157 之先前查詢條件的一非重疊條件。在一具體實施例中，一非重疊條件被定義為一種條件，其具有較早查詢之一共同欄位但並未回報任何較早查詢所回報之結果(列)。舉例來說，考慮一先前查詢(儲存於歷史查詢表 157 中的條件)具有範圍條件“年齡>=0 且年齡<5”。假設現在正在分析該查詢具有範圍條件“年齡>=0 且年齡<5”。這些查詢條件顯示一形式，其猜測一使用者藉由刻意精心製作的查詢以避免回報任何相同列而正掃瞄一資料庫的很大部分。在另一具體實施例中，

一非重疊條件被定義為一種條件，其具有早期查詢之一共同欄位且其回報某些新結果(即先前查詢並未回報之結果)與某些舊結果(即先前查詢已回報之結果)。一種此非重疊條件的重複形式也可被定義為一未授權嘗試存取/累積該資料庫之一部分。

如果一非重疊條件被識別，便於步驟 316/318 處理該條件。在一具體實施例中，依據管理員設定處理該非重疊條件。特別地，管理員設定可指定必須在採取某些行動前識別之非相關查詢的數目。此外，一具體實施例可考慮到在該條件中某種程度的重疊或分離。因此在兩種名義上共同具有同樣結果數目之查詢間的條件仍然可被視為非重疊的。在此一情況中也許想要將一非重疊決定建立於不同查詢所涵蓋的條件範圍之基礎上。舉例來說，在某群具有一相關欄位之查詢的結果總範圍為 4000 且可由條件回報之重疊結果的實際數目為 4 的情況中，該查詢/條件實質上是非重疊的。另一方面，在某群具有一相關欄位之查詢的結果總範圍為 40 且可由條件回報之重疊結果的實際數目為 30 的情況中，該查詢/條件實質上可被視為重疊的。為了建立申請專利範圍的目的，“非重疊”查詢/條件一詞可視為包含實質的非重疊查詢/條件。額外地或替代地，其結果可被回報之不同病人數目可被管理員設定所定義。在一具體實施例中，可特別針對特定使用者制訂此管理員設定。因此，一第一使用者可被給予更多資料的存取而一第二使用者的存取可能相對地受到較多限制。

前文舉例說明執行前分析。額外的或替代的態樣包括執行後分析，其跟隨在第 3 圖之步驟 336 的執行一查詢之後。說明的執行後分析由區塊 338、340 以及 342 代表。大體而言，執行後分析包括在執行一查詢後且在一執行的查詢結果被回報至一使用者之前或/及之後執行處理。舉例來說，區塊 338 說明在提供該結果至一使用者前執行一非重疊查詢分析。一種用於執行區塊 338 之非重疊查詢分析之方法 600 的一具體實施例顯示於第 6 圖。一開始，該執行時元件 150 於步驟 602 加入一回路，其被執行於每個查詢欄。於步驟 604 中，該執行時元件 150 判定該欄是否為一線索欄(即已定義一線索的一欄)。如果不是，便類似地處理次一結果欄位。如果該結果的確包含一線索欄，對應至該線索欄之列表 153 的現在大小被擷取(步驟 606)。每個結果中未包含於列表 153 的數值被加入至該列表 153(步驟 608)。於步驟 610 中，該執行元件判定非重疊查詢是否被識別。在圖示具體實施例中，步驟 610 包含判定加入每個新數值(步驟 608)後該線索列表的大小是否等於新結果/數值數目與其原始大小(於步驟 606 擷取)的總和。在此方面一確認決定指出沒有新數值被該查詢回報並加入至列表 153 中(在關於先前查詢於步驟 336 執行的查詢為非重疊的情況下)。

前述關於執行前分析中，在某些情況下某種程度的重疊仍可被視為實質上非重疊的。因此，兩種名義上具有某些同樣數目結果之查詢間的結果仍可被視為非重疊的。在

此一情況中也許想要將一非重疊決定建立於所有回報結果之數量的基礎上。舉例來說，在某群具有一相關欄位之查詢的總結果為 4000 且重疊結果之數目為 4 的情況中，該查詢實質上是非重疊的。另一方面，在某群具有一相關欄位之查詢的總結果為 40 且重疊結果之數目為 4 的情況中，該查詢可被視為實質上重疊的。為了建立申請專利範圍的目的，“非重疊”查詢/條件一詞可視為包含實質的非重疊查詢/條件。如果於步驟 336 中執行的查詢被視為重疊的或實質上重疊的，便標記該結果(步驟 611)以回報給使用者，且處理繼續至下一欄。否則。該執行時元件 150 判定(步驟 614)是否需要某些先前定義的行動(前述已說明之範例)。如果需要的話，於步驟 616 採取該行動。如果該行動為致命的(於步驟 618 決定)，該請求被終止且不回報結果至該使用者(步驟 620)，該方法 600 隨後退出。如果該行動並非致命的，該處理回到步驟 602 並開始處理次一欄。如果所有欄均被成功地處理而未引入一致命行動，則於步驟 612 回報所有的結果至該使用者。

依照執行後查詢之一範例以識別非重疊查詢，考慮一使用者執行一回報 1000 種不同臨床號碼之第一查詢。在關於臨床號碼之適當線索列表 153 中追蹤該 1000 種臨床號碼。該使用者隨後執行一回報 1500 種不同臨床號碼的第二查詢。假設該第一查詢以及第二查詢回報完全獨立的號碼，該臨床號碼的線索列表 153 隨後將包含 2500 種不同的臨床號碼且該查詢會被視為非重疊的。如果該查詢回

報的結果共用至少一相同值，將採取步驟已判定該查詢是否仍然是實質上非重疊的(如上所述)。更一般地說，可實施各種可配置設定以決定非重疊查詢之一形式並避免倉促的致命行動(即避免回報結果給使用者)。舉例來說，在採取行動前可被回報之非重疊線索數值的數量可被預先定義。替代地或附加地，可在採取行動前執行之非重疊或實質上非重疊查詢的數量可被預先定義。習知技藝人士將瞭解其他規則亦可被有利地實施。

應注意到一預先定義線索之使用僅為一種用於執行數種查詢分析之具體實施例。更一般地說，任何可追蹤查詢間共同性的方法均已加以考慮。舉例來說，一預先定義線索的一種替代品為由相同使用者檢驗一連串查詢以判定一共同欄位的存在。隨後可指定並使用該共同欄位作為一線索以供執行趨勢分析(例如決定非重疊查詢)之用。

另外一種執行後查詢分析由第 3 圖中的區塊 340 所代表，在此稱之為查詢結合分析偵測。查詢結合分析的一範例已如上述。一般地，查詢結合分析偵測檢驗一連串的查詢並判定明顯未相連查詢(由不同條件組成)之一形式，其仍然包含一個或多個共同結果值於一降冪結果組合中。一種關於偵測並處理查詢結合分析的具體實施例為第 7 圖中所示之方法 700，該方法在執行查詢後被加入。於步驟 702 中，該安全演算法 151 判定一結果列表是否存在以追蹤查詢之結果。如果不存在的話，便建立一結果列表 161 並儲存結果於其中(步驟 704)。該方法 700 雖後退出。然而如

果一結果列表已經存在，該演算法151操作以丟棄該結果列表161中所有不同的數值。意即所有包含於結果列表161中的數值也不是自執行該查詢所回報之結果的部分。於步驟708中，該演算法151判定該結果列表大小是否降低超過一大小臨界值(在一具體實施例中，在大小臨界值是可自訂的)。如果不是的話，該結果被回報至該使用者(步驟710)且該方法700退出。反之，該演算法151判定該共同值(於第3圖之步驟305決定)是否低於一共同值臨界值(步驟712)。如果不是的話，該結果被回報至該使用者(步驟710)且該方法700退出。反之，於步驟714採取一預先定義的安全行動。如果該安全行動是致命的(於步驟716中決定)，停止該使用者請求且該方法700退出。如果該安全行動為非致命的，該結果被回報至該使用者(步驟710)且該方法700退出。

另外一種執行後查詢分析由第3圖之區塊342表示，且在此稱為簡化分析偵測。簡化分析係指執行一廣泛查詢的處理，其回報的列數量相對較多且隨後持續有系統地利用隨後查詢將縮小該初始結果的範圍。在一態樣中，簡化分析為結合查詢分析的一種變化；兩種方法均有利地利用一使用者已知之資訊以限制回報結果的大小。考慮一使用者送出一關於名為Alzheimer之人的第一查詢。當察看處理該第一查詢所回報之結果時，該使用者決定可藉由限制該查詢為住在加州之人達成更大程度的特定性。因此，該使用者送出一關於名為Alzheimer且住在加州之人的一第

二查詢。接著該使用者進一步限制該查詢為一特定年齡之人。該使用者可持續此形式縮小任何數目之查詢的範圍以減少回報的結果。

第 8 圖說明一執行後簡化偵測方法 800 的一具體實施例，該方法在執行一查詢並接收結果後被加入。於步驟 804 中，該執行時元件 150 判定該結果總數是否低於一追蹤臨界值。說明地，該追蹤臨界值乃是依據何時應執行簡化偵測而選擇之一預先定義值。意即如果結果總數高於追蹤臨界值便不執行簡化偵測，以給予使用者某種程度的搜尋能力。因此，如果步驟 804 之回應是否定的，便回報該查詢執行的結果至該使用者(步驟 806)。然而如果該結果總數低於追蹤臨界值，該執行時元件 150 判定在先前調用該簡化偵測方法時是否已經存在一個或多個結果列表 161(第 1 圖)。大體而言，一結果列表 161 含有一執行查詢的結果以執行簡化偵測。如果(於步驟 808 中)一結果列表尚未存在，目前的結果便儲存於一結果列表 161(步驟 810)且隨後被回報至該使用者(步驟 806)。如果至少一結果列表確實存在，該執行時元件 150 隨後判定該目前結果是否為任何一既存結果列表之一子集合(步驟 812)。如果不是的話，該目前結果便被儲存於一獨立結果列表(步驟 814)。因此可能存在多個結果列表，各包含不同查詢所回報之不相關結果的子集合。然而如果目前結果為既存結果列表之一的子集合一種簡化形式已被偵測且一安全行動被採用(步驟 816)說明地安全行動已於前述。如果該安全行動是致命的

(於步驟 818 決定)，便不回報該目前結果給該使用者且可阻止該使用者執行任何進一步的查詢(步驟 820)。如果該安全行動不是致命的，可回報該結果至該使用者(步驟 806)。

在前述簡化方法 800 中，可僅於兩查詢之後偵測一簡化形式，假設兩查詢之結果總數低於該追蹤臨界值(於步驟 804 決定)。然而應瞭解用於偵測一簡化行事的特定標準是可調整的。舉例來說，該簡化演算法可要求(除了一結果總數低於一追蹤臨界值之外)該簡化形式擴展查詢之某數目 N，其中 N>2。再者，該簡化演算法可要求該簡化形式發生於各個隨後的/連續的查詢。習知技藝人士將瞭解可有利地使用其他標準。

在一具體實施例中，有利地使用一“熱表”。該熱表包含得到更高層級安全之選定使用者。在一具體實施例中，一單一熱表用於所有查詢而不論使用者為何。此方式在熱表中所列之個人為名人時可能為有用的。在另一具體實施例中，該熱表針對每個使用者加以個人化，因而該列表包含各個使用者知道的個人。在此方式中，一使用者針對其熱表中一個或多個個人所做的搜尋可被偵測並處理以維護匿名性及機密性。

如上所述，該資料儲存抽象元件 148 僅為一提供各種優點之具體實施例的說明性元件。在一態樣中，藉由在該應用程式查詢規格與潛在資料表示間定義一鬆散結合以達到優點。該應用程式以一更抽象的方式定義資料查詢需求

而非在使用 SQL 時以特定表、欄與關係資訊加密一應用程式，隨後在執行時將該資料查詢需求附著於一特定資料表示。本發明之鬆散查詢-資料結合使需求實體(例如應用程式)得以運作，即使該潛在資料表示被調整或該需求實體是伴隨一全新資料表示被使用而非在該資料實體被建立時被使用。在一給定實體資料表示被調整或重新建立的情況中，更新該對應資料儲存抽象以反應對潛在實體資料模型所做的改變。該邏輯欄位的相同集合可供查詢使用，且僅連接至實體資料模型中不同的實體或位置。因此，寫入至該抽象查詢介面的請求實體持續不變地運作，即使該對應實體資料模型已經歷重大改變。在一請求實體是伴隨一全新實體資料表示使用而非在該請求實體被建立時使用的情況中，可使用相同技術(例如相關資料庫)但遵循不同的命名及組織資訊策略(例如一不同方案)實施該新的實體資料模型。該新方案將包含可對應至邏輯欄位集合的資訊，而該應用程式需要該邏輯欄位集合並使用簡單的、過濾的以及組合的欄位存取方法技術。替代地，該新實體表示可使用一種呈現相似資訊的替代技術(例如使用與一相對資料系統相對的一 XML 基礎資料儲存)。在任何一種情況中，寫入以使用該抽象查詢介面之既存請求實體可輕易地移開以使用該新實體資料表示伴隨一替代資料儲存抽象的提供，該替代資料儲存抽象對應該查詢中參考的欄位至該新實體資料模型中的位置及實體表示。

關於終端使用者，該資料儲存抽象提供一資料過濾機

制、揭露適當的資料並避免存取至選擇的內容。然而應瞭解到該資料儲存抽象僅為本發明之一具體實施例。更一般地說，可以任何提供依使用者-資料依賴性執行一查詢的方式實施本發明。意即查詢執行乃是依賴該終端使用者以及由該查詢在執行時存取/回報的特定資料。

然而應強調習知技藝人士會容易地瞭解本發明之安全特性與機制可獨立於該資料儲存抽象元件而被實施。舉例來說，在傳統關係資料庫的情形中，一具體實施例使用來自一查詢剖析器的結構，其會留在該資料庫引擎中以執行此處所述之分析。

雖然前文乃針對本發明之具體實施例，可在不違背本發明之基本範圍的情況下設計本發明之其他與進一步的具體實施例，而本發明之範圍由以下申請專利範圍所決定。

【圖式簡單說明】

本發明上述特性之方法可詳細地加以瞭解，且以上簡略概述的本發明可參照附加圖示中描述的具體實施例得到更精確的說明。

然而要注意該附加圖示僅描述本發明之典型的具體實施例，因此不會被認為是限制其範圍，而本發明可容許其他同樣有效的具體實施例。

第1圖為一電腦系統的一具體實施例；

第2A圖為本發明之一具體實施例的軟體元件的一邏輯/實體圖；

第 2B 圖為一抽象查詢及一抽象的資料儲存的一邏輯圖；

第 3 圖為說明一執行時元件之操作的一流程圖；

第 4 圖為說明一執行時元件之操作的一流程圖；

第 5 圖為一流程圖，其說明一執行時元件之操作以使用事前處理分析識別與處理非重疊條件；

第 6 圖為一流程圖，其說明一執行時元件之操作以使用事後處理分析識別與處理非重疊條件；

第 7 圖為一流程圖，其說明一執行時元件之操作以使用事後處理分析識別與處理查詢結合分析；以及

第 8 圖為一流程圖，其說明一執行時元件之操作以使用事後處理分析識別與處理簡化分析。

【元件代表符號簡單說明】

100 網路系統

102 電腦

104 伺服器

110,130 中央處理器(CPU)

112 記憶體

114,134 儲存裝置

116 輸入裝置

118 網路介面裝置

119 輸出裝置

122 瀏覽器程式

124,138 作業系統

126 網路

130 處理器

132 主記憶體

136 匯流排

140 應用程式

142 應用程式查詢規格

146 抽象查詢介面

148 資料儲存抽象元件

150 執行時元件

151 安全演算法

152 超文字傳輸協定(http)伺服器處理

153 線索列表

154 電腦資料庫管理系統(DBMS)

157 查詢歷史表

161 結果列表

162 安全資訊

200 關係圖

202 抽象查詢

204 選擇標準

206 回報資料規格

208 欄位規格

210 欄位名稱

212 存取方法

213 安全動作定義

214 資料表示

2141 XML 資料表示

2142 相關資料表示

214N 其他資料表示

220 屬性

300 執行時方法

302 開始

304 讀取抽象查詢定義

305 估計共同性

306 對於每個選擇

308 自儲存抽象取得查詢欄位定義

310 對於每個先前查詢

312 欄位被使用？

314 對那些先前條件執行此條件之分析

316,614 需要行動嗎？

318,616,714,816 採取行動

320,618,716,818 致命的？

321,334 附加至具體查詢陳述

322,620,718,820 停止請求(第 3A 圖) 執行查詢(第 3B 圖)

324 對欄位建立具體查詢投寄

328 更多結果欄位？

330 自儲存抽象取得結果欄位定義

332 對欄位建立具體查詢投寄

336 執行後查詢分析

338 非重疊

340 查詢結合分析

342 簡化分析

400,500,600,700 方法

402 簡單存取方法？

404,408 基於實體欄位位置建立查詢投寄

406 過濾的存取方法？

410 加上過濾選擇延伸投寄

412 組合存取方法

414 混合地擷取欄位之實體位置

416 使用實體位置與混合表式建立投寄

418 其他存取方法處理

502 使用操作及數值以判定條件所涵蓋的範圍

504 檢查與先前查詢條件有關之非重疊條件

602 對於結果中的每個欄

604 結果具有線索欄？

606 取得該列表的目前大小

608 在列表上尚未有數值處附加各個數值至適當的線索列表

610 非重疊查詢被識別？

612 回報結果至使用者

702 結果列表存在？

704 建立列表

706 忽略所有非共同數值

708 列表大小低於大小臨界值？

710,806 回報結果

712 共同性小於共同性臨界值？

804 結果數量低於追蹤臨界值？

808 已有結果列表？

812 此列表為結果列表的一子集合？

814 結果列表(查詢不相關)

伍、中文發明摘要：

一種用於保護資料之系統、方法及製品。分析查詢以偵測是否有安全違反事件。在一具體實施例中，實施用於偵測特定安全違反樣式之演算法。通常可在執行一查詢之前與之後偵測樣式。說明的樣式包含結合查詢分析、簡化分析、非重疊分析等等。

陸、英文發明摘要：

System, method and article of manufacture for securing data. Queries are analyzed to detect security violation efforts. In one embodiment, algorithms for detecting selected security violation patterns are implemented. Generally, patterns may be detected prior to execution of a query and following execution of a query. Illustrative patterns include union query analysis, pare down analysis, non-overlapping and others.

柒、指定代表圖：

(一)、本案指定代表圖為：第 2A 圖。

(二)、本代表圖之元件代表符號簡單說明：

140 應用程式
142 應用程式查詢規格
148 資料儲存抽象元件
150 查詢執行執行
151 安全演算法
200 邏輯/抽象表示 實體執行時表示
202 抽象查詢
214_1 XML 資料表示
214_2 相關資料表示
214_N 其他資料表示

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

拾、申請專利範圍：

1. 一種提供關於資料之安全的方法，至少包含：

接收由一使用者向一資料庫送出的一查詢；且

基於以下至少一種方式判定是否存在一違反安全形式：

(i) 關於使用者先前送出之至少一其他查詢進行執行前比較分析；以及

(ii) 對於執行該查詢所回報之結果以及執行至少一先前送出的其他查詢所回報之結果進行執行後比較分析。

2. 如申請專利範圍第 1 項所述之方法，其中該先前送出之至少一查詢僅包含該使用者在目前登入階段所送出的查詢。

3. 如申請專利範圍第 1 項所述之方法，其中該基於步驟(i)來判定是否存在該違反安全形式的步驟至少包含在該查詢與先前送出之至少一其他查詢間判定一相對共同性。

4. 如申請專利範圍第 3 項所述之方法，其中該基於步驟(i)來判定是否存在該違反安全形式的步驟更包含：

判定該相對共同性是否低於一預先定義的數值；且

如果是的話，採用一安全規則。

5. 如申請專利範圍第3項所述之方法，其中該基於步驟(ii)來判定是否存在該違反安全形式的步驟更包含：

判定在執行該查詢所回報之結果與執行先前送出之至少一其他查詢所回報之結果之間的共同結果數目是否減少；

如果是的話，判定該相對共同性是否低於一預先定義的數值，且如果是的話，採用一安全規則。

6. 如申請專利範圍第1項所述之方法，其中該基於步驟(i)來判定是否存在該違反安全形式的步驟至少包含偵測該查詢之共同查詢條件與先前送出之至少一其他查詢被設置以回報非重疊結果。

7. 如申請專利範圍第1項所述之方法，其中該基於步驟(i)來判定是否存在該違反安全形式的步驟至少包含偵測一使用者嘗試取得一資料庫之一未授權數量，其特徵為存在一個或多個該查詢之共同查詢條件以及先前送出之至少一其他查詢被設置以回報至少部分的非重疊結果。

8. 如申請專利範圍第1項所述之方法，其中該基於步驟(i)來判定是否存在該違反安全形式的步驟係僅在該查詢以及該先前送出之至少一其他查詢被設置以存取一共同表欄時才被執行。

9. 如申請專利範圍第 1 項所述之方法，其中該基於步驟(ii)來判定是否存在該違反安全形式的步驟至少包含偵測執行該查詢所回報之結果與執行該先前送出之至少一其他查詢所回報之結果為非重疊的。

10. 如申請專利範圍第 1 項所述之方法，其中該基於步驟(ii)來判定是否存在該違反安全形式的步驟至少包含偵測一種結果子集合的形式。

11. 如申請專利範圍第 1 項所述之方法，更包含如果存在該違反安全形式時，採用一安全規則。

12. 如申請專利範圍第 11 項所述之方法，其中在執行步驟(i)後判定存在該違反安全形式時採用該安全規則的步驟至少包含終止該查詢。

13. 如申請專利範圍第 11 項所述之方法，其中在執行步驟(ii)後判定存在該違反安全形式時採用該安全規則的步驟至少包含對該使用者保留執行該查詢所回報之結果。

14. 一種提供關於資料之安全的方法，至少包含：

自一使用者接收多個查詢；

向一資料庫執行該多個查詢；

接收一使用者隨後向該資料庫送出的查詢；且

基於該多個查詢以及該隨後查詢，有計畫地判定一使用者努力要自該資料庫存取未授權數量資料是否為可識別的。

15. 如申請專利範圍第 14 項所述之方法，其中該有計畫地判定至少包含該隨後查詢之共同查詢條件以及該多個查詢被設置以回報至少部分非重疊的結果。

16. 一種提供關於資料之安全的方法，至少包含：

自一使用者接收多個查詢；

向一資料庫執行該多個查詢；

接收一使用者隨後向該資料庫送出的查詢；

執行該隨後查詢；且

基於該多個查詢以及該隨後查詢，有計畫地判定一使用者努力要繞過安全限制而阻止個人之唯一識別是否為可識別的。

17. 如申請專利範圍第 16 項所述之方法，其中該有計畫地判定至少包含：

判定該後續查詢以及該多個查詢間的一相對共同性；

判定執行該後續查詢所回報之結果與執行該多個查詢

所回報之結果間的共同結果數目是否減少；

如果是的話，判定該相對共同性是否低於一預先定義的數值；且如果是的話，採用一安全規則。

18. 如申請專利範圍第 16 項所述之方法，其中該有計畫地判定至少包含偵測結果子集合的一種形式。

19. 一種具有一特定實體資料表示以提供資料安全的方法，至少包含：

提供一查詢規格，其包含多個用於定義抽象查詢的邏輯欄位；

提供對應規則，其對應該多個邏輯欄位至該資料的物理實體；

提供安全規則；

接收一使用者向該資料送出的一抽象查詢，其中該抽象查詢乃依據該查詢規格而定義且被設置至少一邏輯欄位值；且

分析與自該使用者先前接收之至少一抽象查詢有關的抽象查詢以偵測一安全違反活動的存在而促使採用一安全規則。

20. 如申請專利範圍第 19 項所述之方法，其中分析該抽象查詢以及自該使用者先前接收之至少一抽象查詢以偵

測一違反安全活動之存在的步驟至少包含執行該抽象查詢以及該使用者先前送出之至少一其他抽象查詢的一執行前比較分析。

21. 如申請專利範圍第 19 項所述之方法，其中分析該抽象查詢以及自該使用者先前接收之至少一抽象查詢以偵測一違反安全活動之存在的步驟至少包含執行自執行該抽象查詢所回報之結果與執行該先前送出之至少一其他抽象查詢所回報之結果的執行後比較分析。

22. 如申請專利範圍第 19 項所述之方法，其更包含：

偵測該安全違反活動的存在；且

採用該安全規則。

23. 一種包含指示之電腦可讀取媒體，當該指示被執行時可執行一安全違反識別操作，該電腦可讀取媒體至少包含：

接收一使用者向一資料庫送出之一查詢；且

基於至少以下之一判定一違反安全形式是否存在：

(i) 關於使用者先前送出之至少一其他查詢進行執行前比較分析；以及

(ii) 對於執行該查詢所回報之結果以及執行至少一先前送出的其他查詢所回報之結果進行執行

後比較分析。

24. 如申請專利範圍第 23 項所述之電腦可讀取媒體，其中該先前送出之至少一其他查詢僅包含來自該使用者一目前登入階段的查詢。

25. 如申請專利範圍第 23 項所述之電腦可讀取媒體，其中該基於步驟(i)以判定是否存在該違反安全形式的步驟至少包含判定該查詢以及該先前送出之至少一其他查詢間的一相對共同性。

26. 如申請專利範圍第 25 項所述之電腦可讀取媒體，其中該基於步驟(i)以判定是否存在該違反安全形式的步驟更包含：

判定該相對共同性是否低於一預先定義數值；且

如果是的話，採用一安全規則。

27. 如申請專利範圍第 25 項所述之電腦可讀取媒體，其中該基於步驟(ii)以判定是否存在該違反安全形式的步驟更包含：

判定在執行該查詢所回報之結果與執行先前送出之至少一其他查詢所回報之結果之間的共同結果數目是否減少；

如果是的話，判定該相對共同性是否低於一預先定義的數值，且如果是的話，採用一安全規則。

28. 如申請專利範圍第 23 項所述之電腦可讀取媒體，其中該基於步驟(i)來判定是否存在該違反安全形式的步驟至少包含偵測該查詢之共同查詢條件與先前送出之至少一其他查詢被設置以回報非重疊結果。

29. 如申請專利範圍第 23 項所述之電腦可讀取媒體，其中該基於步驟(i)來判定是否存在該違反安全形式的步驟至少包含偵測一使用者嘗試取得一資料庫之一未授權數量，其特徵為存在一個或多個該查詢之共同查詢條件以及先前送出之至少一其他查詢被設置以回報至少部分的非重疊結果。

30. 如申請專利範圍第 23 項所述之電腦可讀取媒體，其中該基於步驟(i)來判定是否存在該違反安全形式的步驟係僅在該查詢以及該先前送出之至少一其他查詢被設置以存取一共同表欄時才被執行。

31. 如申請專利範圍第 23 項所述之電腦可讀取媒體，其中該基於步驟(ii)來判定是否存在該違反安全形式的步驟至少包含偵測執行該查詢所回報之結果與執行該先前

送出之至少一其他查詢所回報之結果為非重疊的。

32. 如申請專利範圍第 23 項所述之電腦可讀取媒體，其中該基於步驟(ii)來判定是否存在該違反安全形式的步驟至少包含偵測一種結果子集合的形式。

33. 如申請專利範圍第 23 項所述之電腦可讀取媒體，更包含如果存在該違反安全形式時，採用一安全規則。

34. 如申請專利範圍第 33 項所述之電腦可讀取媒體，其中在執行步驟(i)後判定存在該違反安全形式時採用該安全規則的步驟至少包含終止該查詢。

35. 如申請專利範圍第 33 項所述之電腦可讀取媒體，其中在執行步驟(ii)後判定存在該違反安全形式時採用該安全規則的步驟至少包含對該使用者保留執行該查詢所回報之結果。

36. 一種包含安全確認指示之電腦可讀取媒體，該指示被執行時可執行一至少包含下列步驟之安全確認操作：

自一使用者接收多個查詢；

向一資料庫執行該多個查詢；

接收一使用者隨後向該資料庫送出的查詢；且

基於該多個查詢以及該隨後查詢，有計畫地判定一使用者努力要自該資料庫存取未授權數量資料是否為可識別的。

37. 如申請專利範圍第 36 項所述之電腦可讀取媒體，其中該有計畫地判定至少包含該隨後查詢之共同查詢條件以及該多個查詢被設置以回報至少部分非重疊的結果。

38. 一種包含安全確認指示之電腦可讀取媒體，該指示被執行時可執行一至少包含下列步驟之安全確認操作：

自一使用者接收多個查詢；

向一資料庫執行該多個查詢；

接收一使用者隨後向該資料庫送出的查詢；

執行該隨後查詢；且

基於該多個查詢以及該隨後查詢，有計畫地判定一使用者努力要繞過安全限制而阻止個人之唯一識別是否為可識別的。

39. 如申請專利範圍第 38 項所述之電腦可讀取媒體，其中該有計畫地判定步驟至少包含：

判定該後續查詢以及該多個查詢間的一相對共同性；

判定執行該後續查詢所回報之結果與執行該多個查詢所回報之結果間的共同結果數目是否減少；

如果是的話，判定該相對共同性是否低於一預先定義的數值；且如果是的話，採用一安全規則。

40. 如申請專利範圍第 38 項所述之電腦可讀取媒體，其中該有計畫地判定步驟至少包含偵測結果子集合的一種形式。

41. 一種儲存了資訊於其上之電腦可讀取媒體，該資訊至少包含：

一查詢規格，其包含多個用於定義抽象查詢的邏輯欄位；

多個對應規則，其對應該多個欄位至資料的物理實體；

多個安全規則；

一執行時元件，其可被執行以反應接收一使用者向該資料送出之一抽象查詢而執行一安全違反行動偵測，其中該抽象查詢乃是依據該查詢規格加以定義且被設置至少一邏輯欄位數值，該安全違反行動偵測操作至少包含：

接收一使用者向該資料送出的一抽象查詢，其中該抽象查詢乃依據該查詢規格而定義且被設置至少一邏輯欄位值；且

分析與自該使用者先前接收之至少一抽象查詢有

關的抽象查詢以偵測是否存在一安全違反活動而促使採用一安全規則。

42. 如申請專利範圍第 41 項所述之電腦可讀取媒體，其中分析該抽象查詢以及自該使用者先前接收之至少一抽象查詢以偵測是否存在一安全違反活動的步驟至少包含執行該抽象查詢以及該使用者先前送出之至少一其他抽象查詢的一執行前比較分析。

43. 如申請專利範圍第 41 項所述之電腦可讀取媒體，其中分析該抽象查詢以及自該使用者先前接收之至少一抽象查詢以偵測是否存在一安全違反活動的步驟至少包含執行自執行該抽象查詢所回報之結果與執行該先前送出之至少一其他抽象查詢所回報之結果的執行後比較分析。

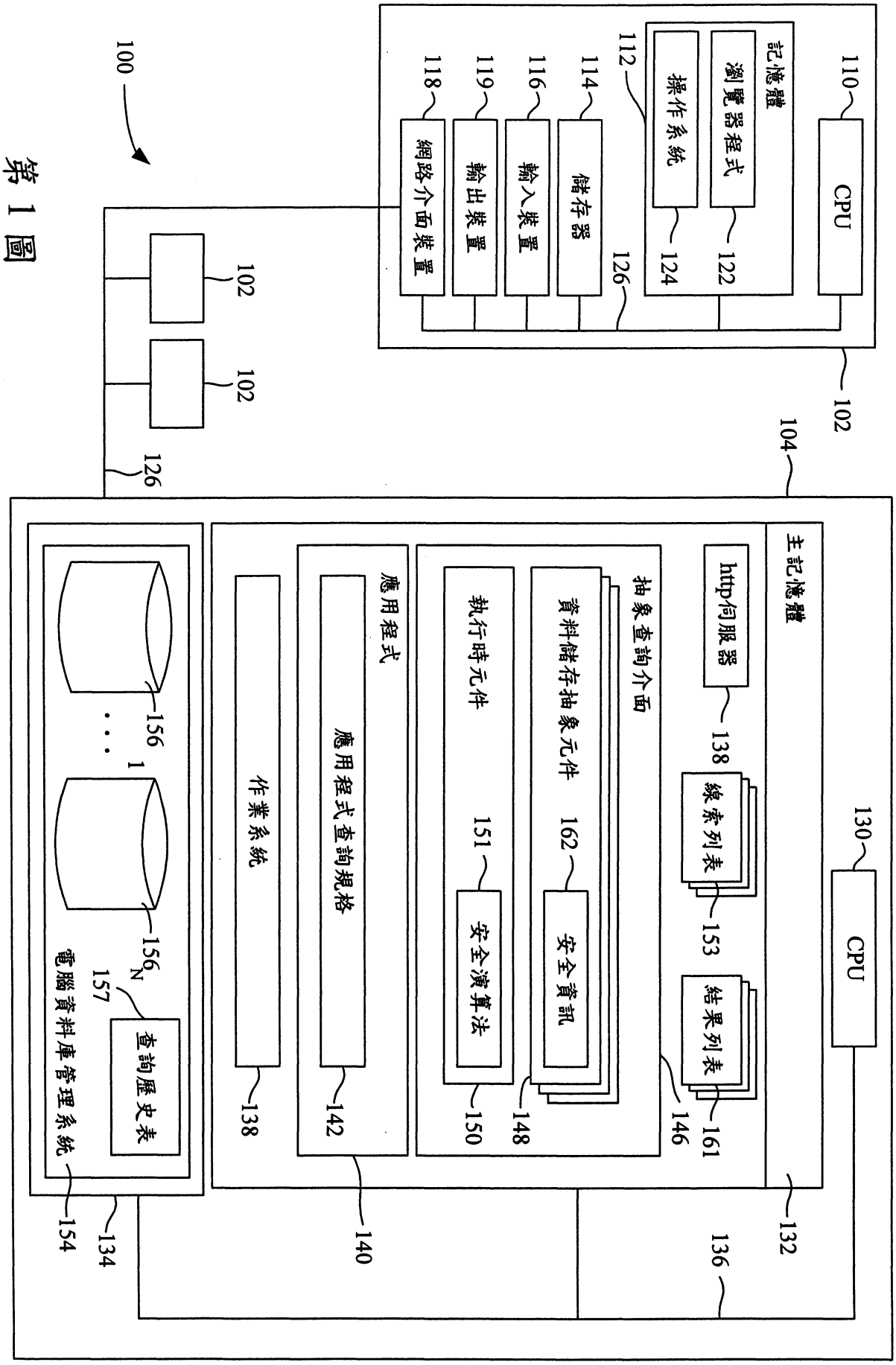
44. 如申請專利範圍第 41 項所述之電腦可讀取媒體，更包含：

偵測該安全違反活動的存在；且

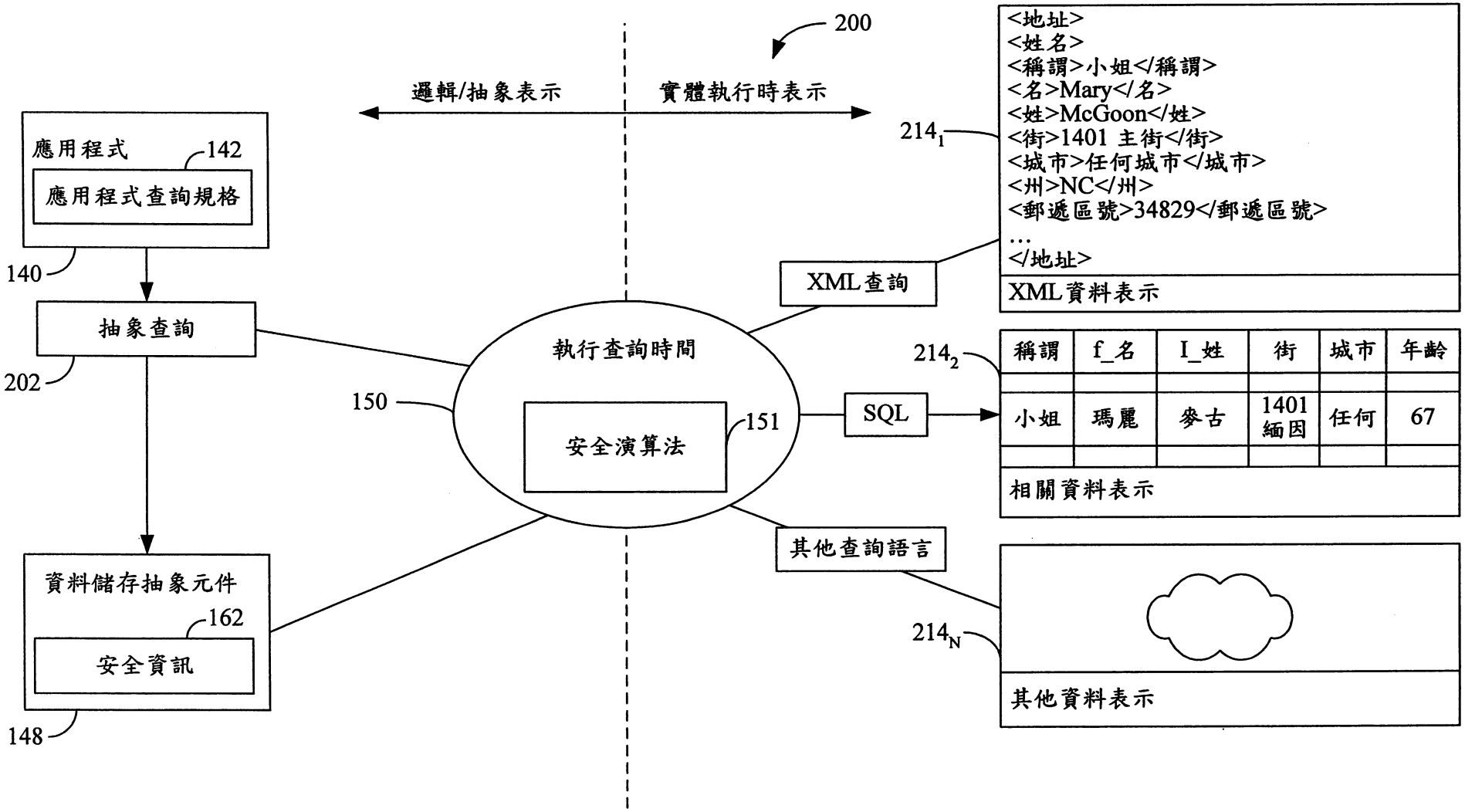
採用該安全規則。

45. 如申請專利範圍第 41 項所述之電腦可讀取媒體，其中該安全規則阻止該抽象查詢的執行。

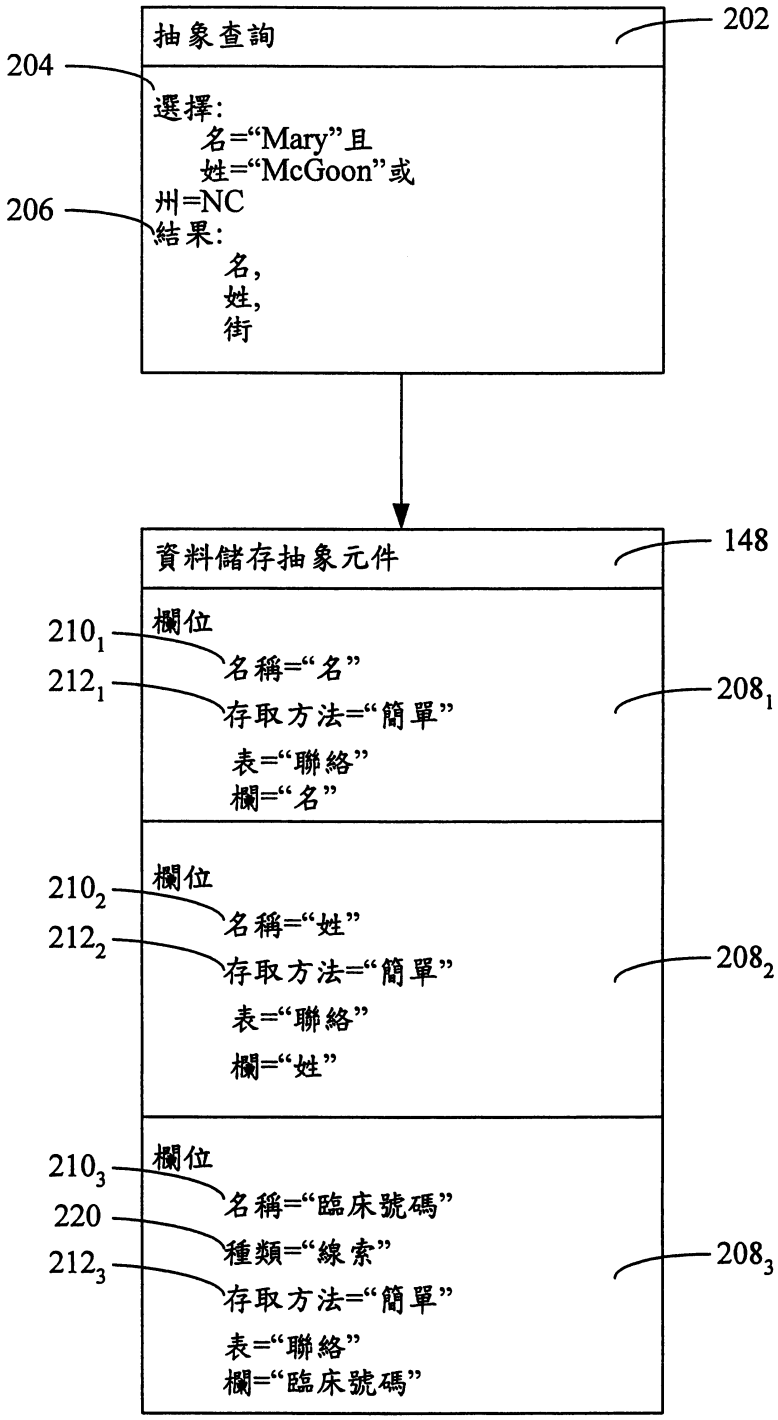
46. 如申請專利範圍第 41 項所述之電腦可讀取媒體，其中該安全規則係被定義以記錄自該使用者接收該抽象查詢。


100
110
CPU
記憶體
瀏覽器程式
122
操作系統
124
112
126
114
儲存器
116
輸入裝置
119
輸出裝置
118
網路介面裝置
102
102
126
104
102
主記憶體
130
CPU
http伺服器
138
線索列表
153
結果列表
161
146
抽象查詢介面
資料儲存抽象元件
162
安全資訊
148
執行時元件
151
安全演算法
150
應用程式
應用程式查詢規格
142
作業系統
138
140
132
136
156
1
156N
157
查詢歷史表
電腦資料庫管理系統
134
154

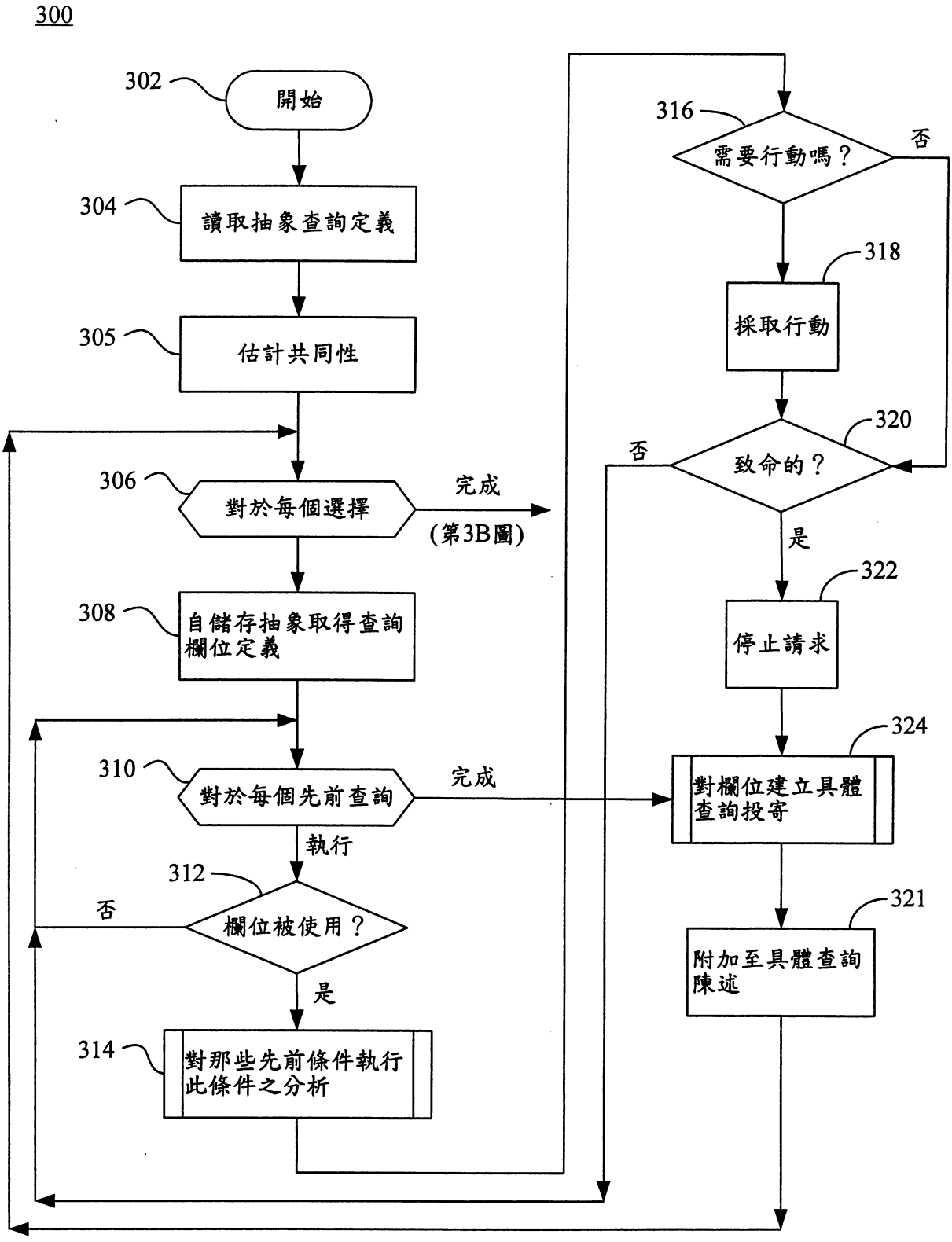
第 1 圖


200
邏輯/抽象表示
實體執行時表示
應用程式
142
應用程式查詢規格
140
抽象查詢
202
資料儲存抽象元件
162
安全資訊
148
執行查詢時間
150
安全演算法
151
XML查詢
SQL
其他查詢語言
214₁
<地址>
<姓名>
<稱謂>小姐</稱謂>
<名>Mary</名>
<姓>McGoon</姓>
<街>1401 主街</街>
<城市>任何城市</城市>
<州>NC</州>
<郵遞區號>34829</郵遞區號>
…
</地址>
XML資料表示
214₂
稱謂 | f_名 | l_姓 | 街 | 城市 | 年齡
小姐 | 瑪麗 | 麥古 | 1401 緬因 | 任何 | 67
相關資料表示
214_N
其他資料表示

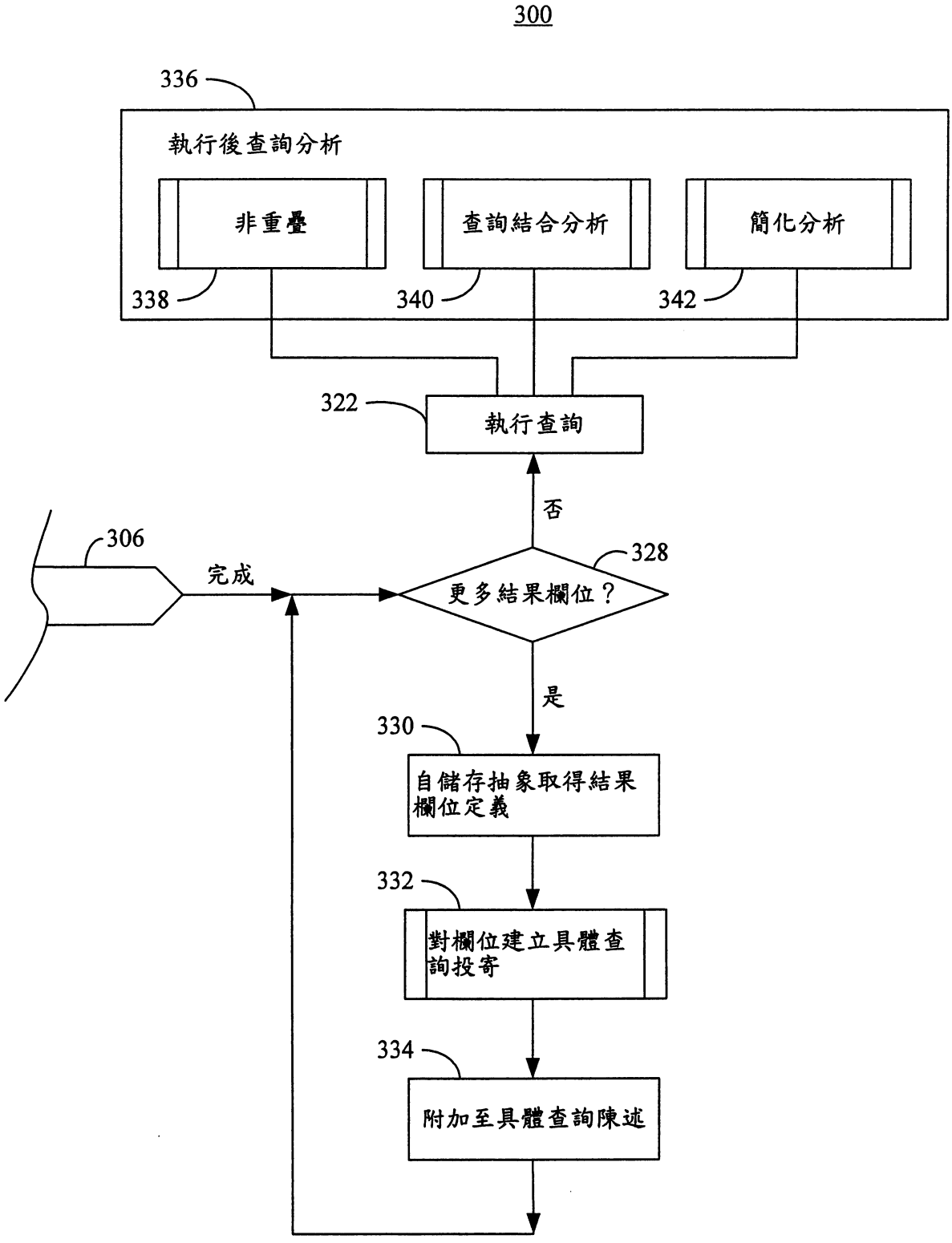
第 2A 圖


抽象查詢
202
204
選擇:
名="Mary"且
姓="McGoon"或
州=NC
206
結果:
名,
姓,
街
資料儲存抽象元件
148
欄位
210_1
名稱="名"
212_1
存取方法="簡單"
表="聯絡"
欄="名"
208_1
欄位
210_2
名稱="姓"
212_2
存取方法="簡單"
表="聯絡"
欄="姓"
208_2
欄位
210_3
名稱="臨床號碼"
220
種類="線索"
212_3
存取方法="簡單"
表="聯絡"
欄="臨床號碼"
208_3

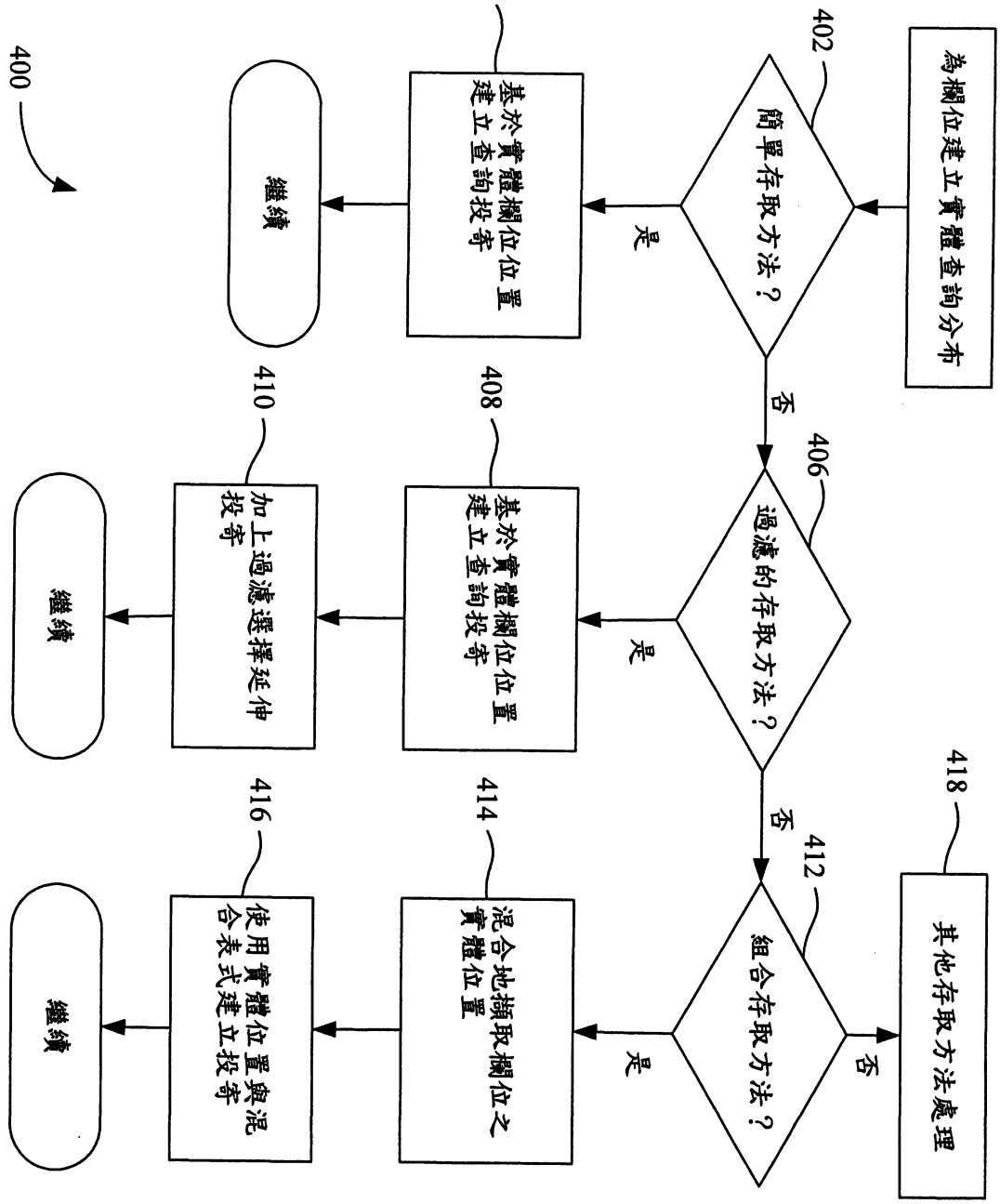
第 2B 圖


300
302
開始
304
讀取抽象查詢定義
305
估計共同性
306
對於每個選擇
完成
(第3B圖)
308
自儲存抽象取得查詢欄位定義
310
對於每個先前查詢
完成
執行
312
欄位被使用？
否
是
314
對那些先前條件執行此條件之分析
316
需要行動嗎？
否
318
採取行動
320
致命的？
否
是
322
停止請求
324
對欄位建立具體查詢投寄
321
附加至具體查詢陳述

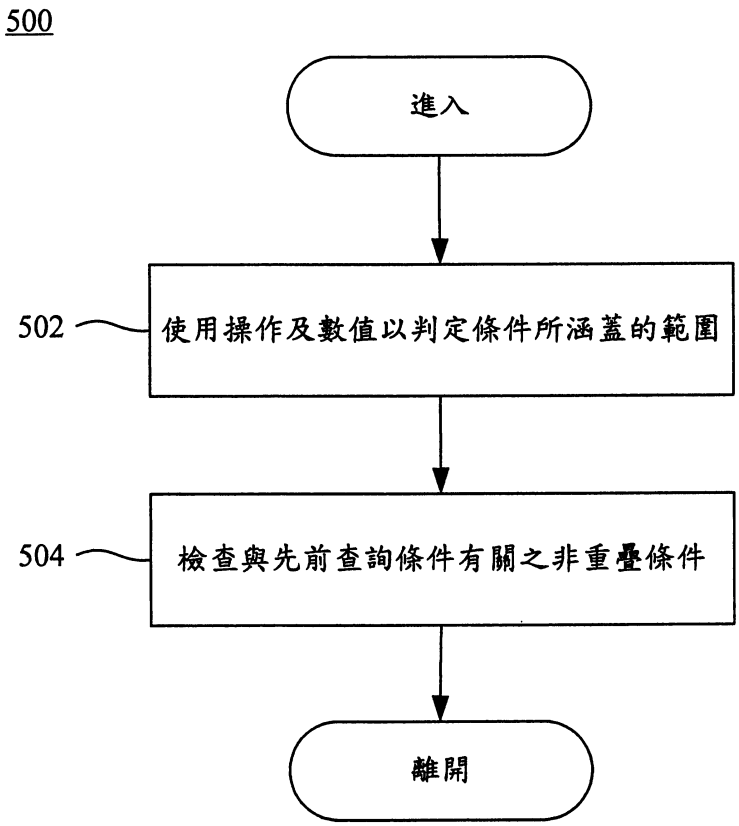
第 3A 圖


300
336
執行後查詢分析
非重疊
查詢結合分析
簡化分析
338
340
342
322
執行查詢
否
306
完成
328
更多結果欄位？
是
330
自儲存抽象取得結果欄位定義
332
對欄位建立具體查詢投寄
334
附加至具體查詢陳述

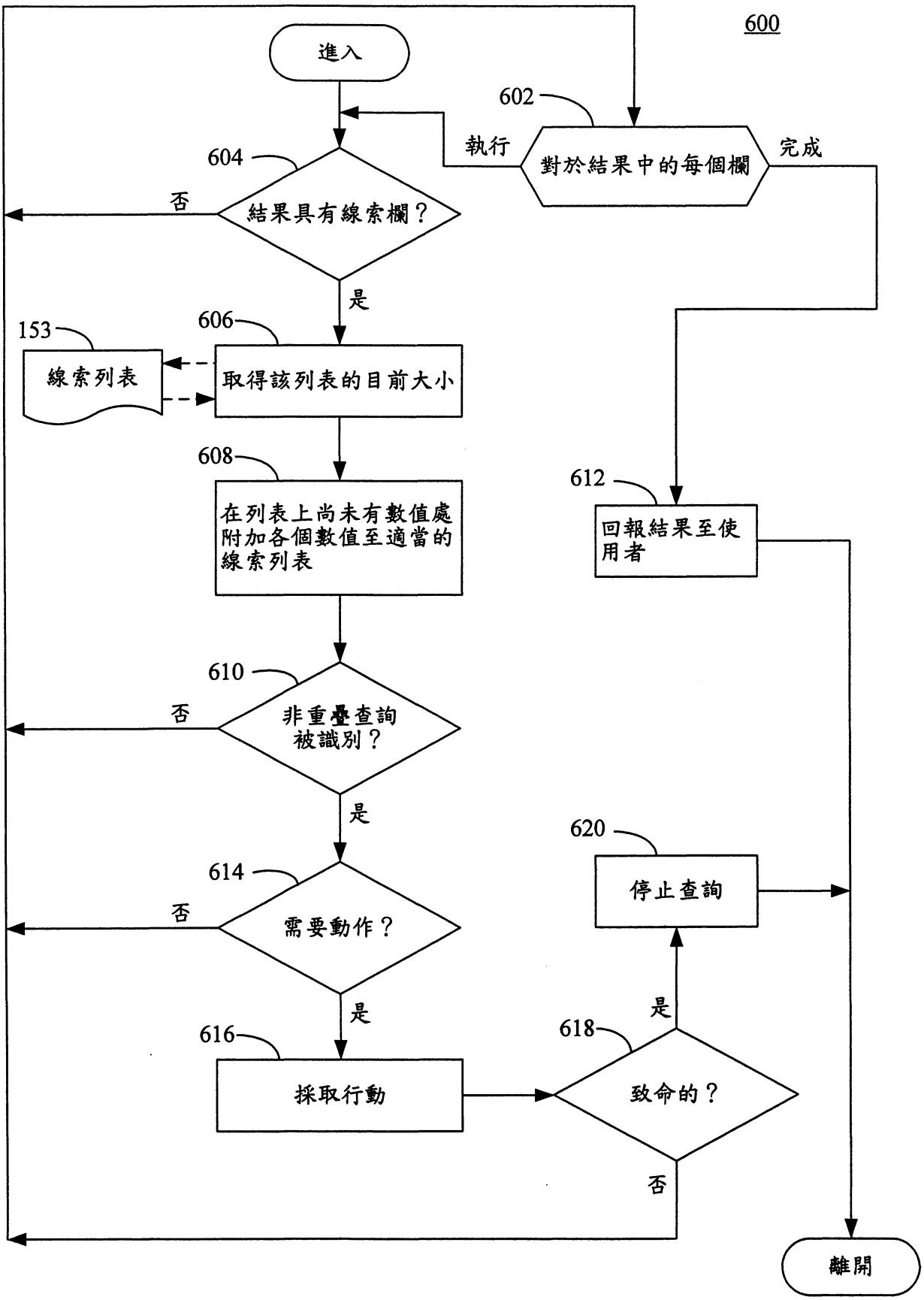
第 3B 圖


為欄位建立實體查詢分布
402
簡單存取方法？
是
否
404
基於實體欄位位置建立查詢投寄
繼續
406
過濾的存取方法？
是
否
408
基於實體欄位位置建立查詢投寄
410
加上過濾選擇延伸投寄
繼續
412
組合存取方法？
是
否
414
混合地擷取欄位之實體位置
416
使用實體位置與混合表式建立投寄
繼續
418
其他存取方法處理
400

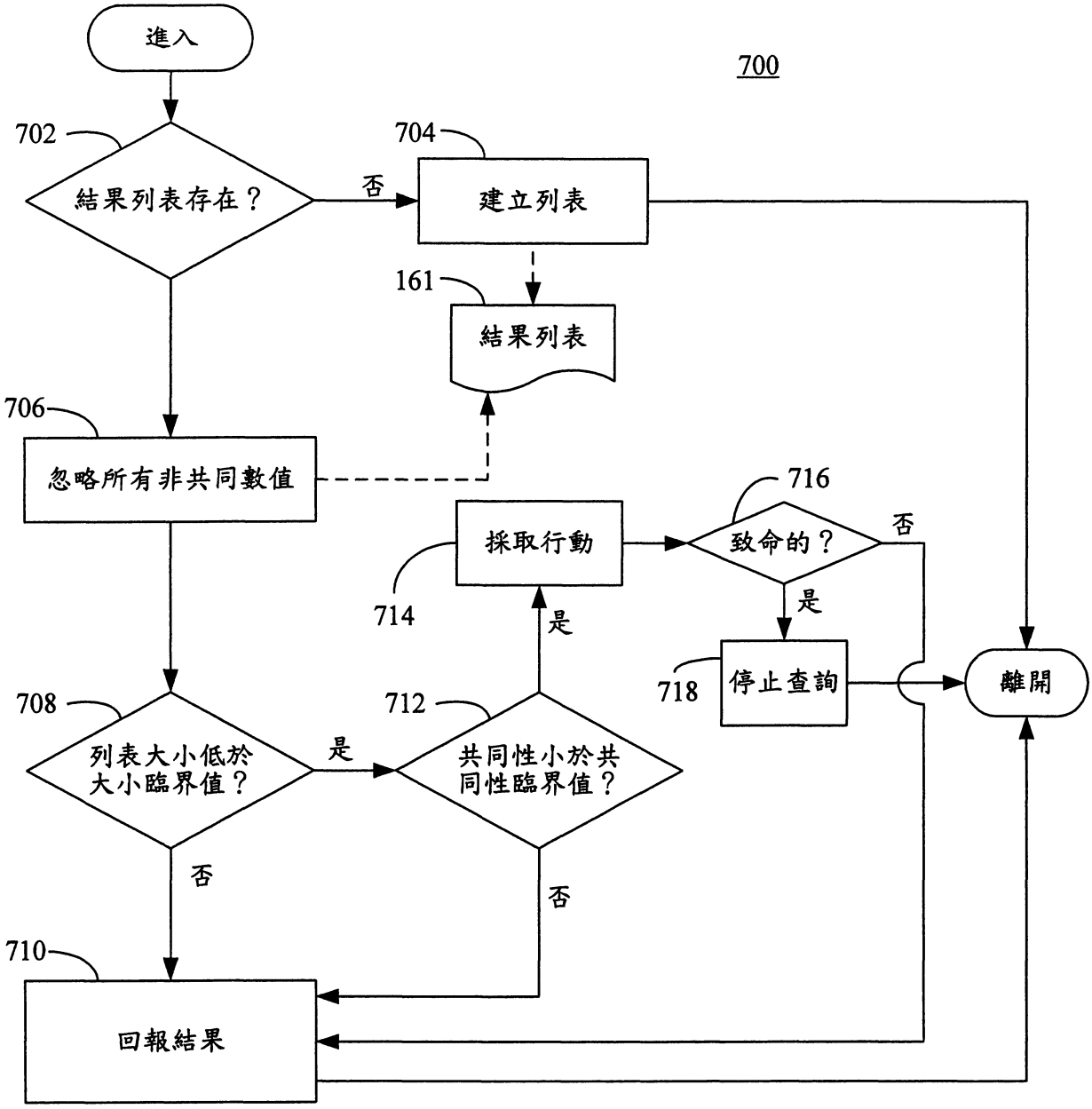
第 4 圖



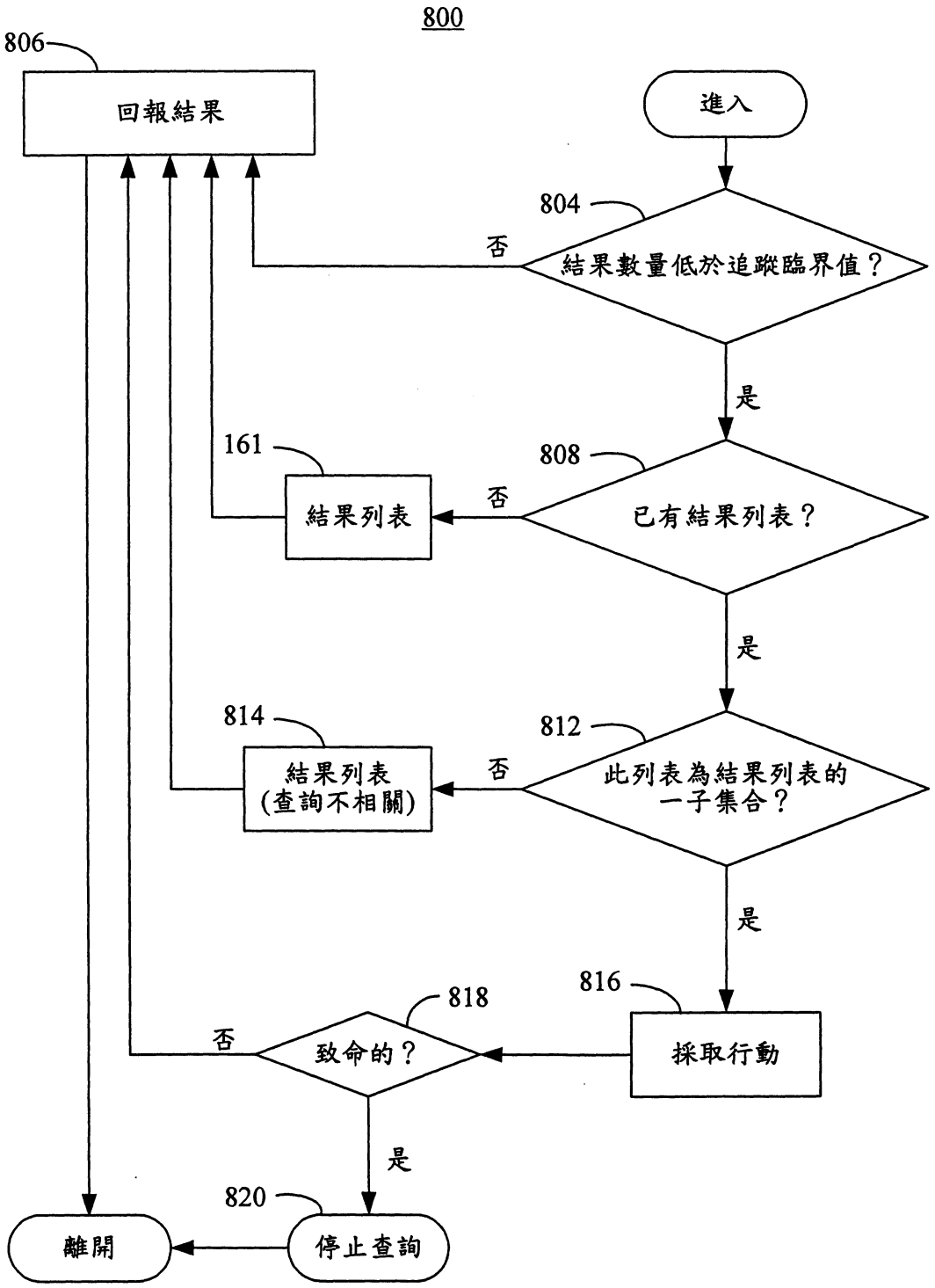
第 5 圖


600
進入
602
執行
對於結果中的每個欄
完成
604
否
結果具有線索欄？
是
153
線索列表
606
取得該列表的目前大小
608
在列表上尚未有數值處附加各個數值至適當的線索列表
610
否
非重疊查詢被識別？
是
614
否
需要動作？
是
616
採取行動
618
是
致命的？
否
620
停止查詢
612
回報結果至使用者
離開

第 6 圖


進入
700
702
結果列表存在？
否
704
建立列表
161
結果列表
706
忽略所有非共同數值
716
致命的？
否
採取行動
714
是
是
718
停止查詢
離開
708
列表大小低於
大小臨界值？
是
712
共同性小於共
同性臨界值？
否
否
710
回報結果

第 7 圖


800
806
回報結果
進入
804
否
結果數量低於追蹤臨界值？
是
161
808
結果列表
否
已有結果列表？
是
814
812
結果列表
(查詢不相關)
否
此列表為結果列表的
一子集合？
是
816
818
否
致命的？
採取行動
是
820
離開
停止查詢

第 8 圖