

發明專利說明書 200530805

(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：93129012

※ 申請日期：93-9-24

※IPC 分類：G06F 11/30 G06F 17/30

一、發明名稱：(中文/英文)

資料庫使用者運作行為監視系統與方法

DATABASE USER BEHAVIOR MONITOR SYSTEM AND METHOD

二、申請人：(共 1 人)

姓名或名稱：(中文/英文)

艾普鎖股份有限公司/IPLOCKS, INC.

代表人：(中文/英文)

雷恩 亞得連/LANE, ADRIAN

住居所或營業所地址：(中文/英文)

美國加州聖約瑟市西崔寶路 441-A 號

441-A West Trimble Road, San Jose, CA 95131, U.S.A.

國 籍：(中文/英文)

美國/U. S. A.

三、發明人：(共 4 人)

姓 名：(中文/英文)

1. 坂木明雄/SAKAMOTO, AKIO

2. 周重寬/CHOU, CHUNG-KUANG

3. 唐威尼 G./TANG, WANI G.

4. 胡建國/HU, JIANGUO

國 籍：(中文/英文)

1. 日本/Japan

2. 3. 美國/U. S. A.

4. 加拿大/Canada

四、聲明事項：

☐ 主張專利法第二十二條第二項 ☐ 第一款或 ☐ 第二款規定之事實，其事實發生日期為： 年 月 日。

☒ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號 順序註記】

☒ 有主張專利法第二十七條第一項國際優先權：

1. 美國；2004,03,09；10/796,932

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號 順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料 【格式請依：寄存機構、日期、號碼 順序註記】

國外生物材料 【格式請依：寄存國家、機構、日期、號碼 順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

發明領域

本發明係有關管理資料庫系統。特別本發明係有關一種監視資料庫系統之方法及裝置。

【先前技術】

發明背景

於網路化系統對資料的保護有關鍵重要性。可能威脅有價值資料之安全性之情況有多種不同類別，且隨著網路系統的崛起而更增加威脅安全性的情況。當安全性受到破壞時，重要地須可檢測出。否則，未來，資料仍然經常容易受到類似類別事件的侵害。

網路管理者保護有價值資料面對的問題類別，包括例如駭客攻擊、未經授權的使用、內部人士的欺騙或誤用、以及智慧資訊的竊取。

對網路系統所遭逢的若干常見問題已經發展出不同的因應辦法。例如防火牆及虛擬私人網路可防衛網路化系統，對抗外來網站的未經授權的存取。經由使用通行碼或指定特權進行存取控制，可提供某種程度的保護。但防火牆及虛擬私人網路無法保護資料不被內部竊取，通行碼可能被偷竊；特權難以管理，使用者經常存取超出其工作範圍以外的資料，安全性容易受到破壞。

本章節描述之辦法為可依循之辦法，但非必然為先前已經了解或依循的辦法。因此，除非另行指示，否則不可

單純由於含括於本節，即假設本章節所述任何辦法屬於先前技術。

【發明內容】

發明概要

5 本發明之具體例提供監視一資料庫系統之異常活動之技術。接受監視的一主題資料庫之相關使用者行為資訊可自動收集、分析，且與統計導出之基準及/或一或多項管制方策比較來檢測異常活動。具體實施例由多種不同來源，包括稽核軌跡及動態視圖，與資料庫之資料庫管理系統協
10 力合作，收集有關該主題資料庫之使用者行為資料。具體例採用基於統計之入侵檢測(SBID)、及基於法則之入侵檢測(RBID)中之一或多者，來檢測異常資料庫活動。於基於統計之入侵檢測，收集得之資訊係使用統計側繪分析，來決定正常使用側繪。於基於法則之入侵檢測，收集得之資
15 料係相對於明確詳盡安全法則作比較。若檢測得偏離正常使用模式之可疑資料庫存取，則進行鎖定目標操作，例如警告負責的安全人員、產生報告、電子郵件寄出警訊通知等。

 一具體例中，提供一項機制來由有關資料庫活動之歷史資訊，決定正常使用模式。以統計上顯著方式，偏離正
20 常使用模式之資料庫存取將被檢測出，且將發出警訊通知。使用模式之一例包括一天時間對資料庫之存取頻率。

 一具體例中，提供一項機制來讓使用者可規定明確詳盡安全法則。違犯該法則之資料庫存取則將被檢測出且警訊通知。若干安全法則範例包括可疑操作系統使用者或所

在位置。

一具體例中，資料庫存取資訊係使用由控制主題資料庫之資料庫管理系統所提供的設施來收集。例如，資料庫管理系統可提供稽核軌跡，其包括有關資料庫存取資訊。

- 5 資料庫管理系統也提供動態效能視圖，其提供目前資料庫使用資訊，例如目前使用者存取活動及資源利用。此項資訊可結合得自稽核軌跡之資訊使用。

- 具體例允許監視一或多個層面，包括資料庫物件層面監視、資料庫使用者層面監視及資料庫存取活動層面監視。
- 10 視。資料庫物件層面監視之焦點係放在一特定資料庫物件。資料庫使用者層面監視之焦點係放在資料庫使用者。資料庫存取活動層面監視之焦點係放在資料庫之登入處理。具體例可基於多種不同入侵檢測辦法，支援各個監視層面之各項安全性管制方策。

15 圖式簡單說明

本發明將於附圖各圖舉例說明本發明，而非限制性，附圖中類似之參考編號表示類似之元件，附圖者：

第1圖為方塊圖，顯示於一具體例，可實作資料庫監視技術之網路電腦系統之高階鳥瞰圖。

- 20 第2圖為線圖，顯示於一具體例，資料庫稽核引擎範例處理之高階鳥瞰圖。

第3A-3E圖為方塊流程圖，顯示於一具體例，資料收集、分析、及異常檢測處理之高階鳥瞰圖。

第4圖為線圖，顯示於一具體例，存取一資料庫之範例

機率分佈。

第5圖為方塊圖，顯示於一具體例，一資料庫監視系統之高階鳥瞰圖。

第6A-6M圖為畫面拍攝照片，顯示於一具體例，監視
5 操作之組配範例。

第7圖為硬體方塊圖，顯示代表性電腦系統，其可用於具體實作一具體例之一或多個組成元件。

【實施方式】

較佳實施例之詳細說明

10 綜論

說明一種監視一資料庫之方法及裝置。後文說明中，為求解說，陳述多種特定細節以供更徹底了解本發明。但顯然本發明可無此等特定細節實施。其它情況下，眾所周知之結構及裝置係以方塊圖形式顯示，以免不必要地混淆
15 本發明。

參照第3A圖，顯示根據本發明之一具體例，一種監視資料庫之方法。第3A圖所示方法，包括收集使用者行為資料，其指示一或多個使用者如何使用該資料庫(方塊310)。所示方法進一步包括處理資料及儲存該資料作為歷史資料
20 (方塊320)。分析歷史資料來決定行為模式(方塊330)也屬於所示方法之一部分。所示方法進一步包括接收一新資料集合(方塊340)，其指示一或多位使用者如何使用該資料庫。所示方法也包括進行該新資料集合與行為模式間之比較(方塊350)。基於該比較，判定該新資料集合是否滿足集合

標準(方塊360)，也屬於所示方法之一部分。所示方法也包括若新資料集合滿足該標準集合，則判定該新資料集合代表異常活動(方塊370)。回應於該項判定，進行鎖定目標之操作(方塊380)也含括於所示方法。

5 一具體例中，收集使用者行為資料進一步包括由資料庫管理者之稽核軌跡，讀取資訊。一具體例中，收集使用者行為資料進一步包括於一監視層面收集選自下列之資料：(1)有關一或多項選定之資料庫物件之資料庫存取資訊，(2)有關一或多項選定之資料庫使用者之資料庫存取資
10 訊，以及(3)有關一或多項選定之資料庫使用者存取活動之資料庫存取資訊。一具體例中，收集使用者行為資料進一步包括接收一類欲監視之資訊，由該類型資訊決定一監視層面，以及基於該決定之監視層面，激活該資料庫管理者之稽核選項。

15 一具體例中，分析歷史資料來決定行為模式，進一步包括由該歷史資料來決定一統計模型。一具體例中，由該歷史資料決定一統計模型進一步包括由該歷史資料決定資料庫存取頻率，對該資料庫存取頻率決定一機率函數，以及由該機率函數決定一累進機率函數。一具體例中，機率
20 函數可為波森機率分佈、常態機率分佈等。

 一具體例中，進行該新資料集合與行為模式間之比較，進一步包括使用該新資料集合對該統計模型測試一假說。一具體例中，使用該新資料集合對該統計模型測試一假說，進一步包括對該新資料集合決定資料庫存取頻率，

以及由一防護標準以及一機率函數參數決定臨限值。一具體例中，使用該新資料集合對該統計模型測試一假說，進一步包括將該新資料集合之資料庫存取頻率與該臨限值作比較。

- 5 歷史資訊可包括有關資料庫存取一或多個選定之資料庫物件之資訊。各具體例中，由該歷史資料決定資料庫存取頻率，包括測定以下一或多項之頻率：以一天時間之物件存取頻率、以一天時間及操作系統使用者之物件存取頻率、以一天時間及資料庫使用者之物件存取頻率、以一天
- 10 時間及所在位置之物件存取頻率，以一天時間或操作系統使用者、資料庫使用者、及所在位置中之至少二者之組合之物件存取頻率。

- 歷史資訊可包括有關資料庫存取一或多個選定之資料庫物件之資訊。各具體例中，由該歷史資料決定資料庫存取
- 15 頻率，包括測定以下一或多項之頻率：以一天時間之使用者存取頻率、以一天時間及操作系統使用者之使用者存取頻率、以一天時間及資料庫使用者之使用者存取頻率、以一天時間及所在位置之使用者存取頻率，以一天時間或操作系統使用者、資料庫使用者、及所在位置中之至少二者
- 20 之組合之使用者存取頻率。

 歷史資訊可包括有關對一或多項選定之資料庫使用者存取活動之資料庫存取資訊。各具體例中，由歷史資訊測定資料庫之存取頻率包括測定以下一或多項之頻率：每存取活動讀取的頁數、每存取活動之存取持續時間、或每單

位時間之讀取頁數。

各具體例中，進行鎖定目標之操作包括發出警報通知、送出電子郵件、產生報告及進行觀視中之一或多者。

一具體例中，進行判定該新資料集合是否違犯基於法
5 則之管制方策。若該新資料集合違犯基於法則之管制方
策，則判定該新資料集合代表異常活動。一具體例中，異
常活動包含可疑活動。

於其它面相，本發明之具體例涵蓋一種組配來進行前
述方法之裝置及電腦可讀取媒體。

10 術語

「資料庫」包括用來根據組織儲存資料之任何資料結
構。資料庫包括關係資料庫、物件資料庫、階層資料庫、
網路資料庫、多維資料庫等。

「資料庫觸動」表示回應於涉及一資料庫物件之特定
15 事件(例如當一表或視窗被選定或修改時)，自動觸發儲存資
料庫程序。

「資料庫存取活動」表示透過使用者的處理之特定使
用者連結至一資料庫。存取活動係由使用者連結開始，直
到使用者解除連結或離開該資料庫之應用程式為止。

20 「爪哇資料庫連結(JDBC)API」為一種標準SQL資料庫
存取介面，其允許使用者存取任何來自爪哇程式語言之資
料來源。

「波森分佈」為介於事件以指數方式分佈中間等候時
間之事件數目之機率分佈。

「稽核軌跡」為一系列電腦事件記錄。其係由監視系統活動之稽核系統所產生。該記錄可以各種形式儲存，包括(但非限制性)電腦檔案或資料庫表等形式儲存。

- 「特權」表示網路使用者或資料使用者允許執行之動作集合或操作集合。特權又稱為授權或授權集合。

系統說明

- 第1圖為方塊圖，顯示網路運算系統之高階鳥瞰圖，其中監視資料庫技術可以一具體例實作。根據第1圖所示具體例，資料庫稽核引擎110係藉網路106耦合至資料庫系統，該資料庫系統包含一資料庫伺服器130及一資料庫132，俾便由使用者及/或處理監視資料庫132的存取。一具體例中，網路106係經由防火牆124及路由器122而連結至網際網路108。防火牆124係組配來保護網路106及相關組成元件不會受到經由網際網路108所送來的有害程式侵害。路由器122管理且控制介於網際網路108與網路106間之網路資料流。

- 資料庫伺服器130維持資料於資料庫132。若干於資料庫132之資料對網路106之一或多個使用者可能具有關鍵重要性。關鍵重要資料例如包括(但非限制性)稽核記錄、客戶帳戶資訊、以及員工薪資資訊。於若干具體例，資料庫132可為資料庫伺服器130之一整合部分。管理站144讓管理者可於網路106執行管理功能。管理功能包括監視網路106之安全性，包括監視使用者活動。若干具體例中，其它元件及組成元件(未顯示於第1圖)可與網路106連結。

一具體例中，資料庫稽核引擎110包括一資料收集器

112、一資料分析器114、以及一異常檢測器116。資料收集器112係組配來於指定間隔時間或當出現指定條件(例如人工指令)時，讀取有關使用者行為資料，該使用者行為係與由資料庫伺服器130存取資料庫132相關行為；以及組配來
5 儲存該資料作為歷史資料。資料分析器114對資料收集器112儲存的歷史資料進行分析操作，來決定有關存取資料庫132之行為模式。當接收到新資料時，異常檢測器116基於比較該新資料與由歷史資料決定之行為模式，判定該新資料是否代表異常活動。若干具體例允許資料庫稽核引擎110
10 收集、分析、及發出警告信號，而對資料庫伺服器130之表現效能不會造成顯著影響。由資料收集器112、資料分析器114及異常檢測器116執行之處理範例之進一步細節將參照第3A-3E圖說明如後。

第2圖為方塊圖，顯示於一具體例，於一範例資料庫稽核引擎之各項處理之高階鳥瞰圖。

一具體例中，資料庫稽核引擎110係於資料庫伺服器130外部操作，來減少干擾資料庫伺服器。一具體例中，資料收集器112之操作而無需有例如於資料庫伺服器130之操作代理。此種具體例中，資料收集器112由資料庫伺服器130
20 所維持之稽核軌跡84收集有關使用者行為資訊，及/或採用「唯讀」存取資料庫132來收集資料。一具體例中，資料收集器112係基於欲監視之資料類型決定監視層面，以及基於此監視層面來激活資料庫管理者130之稽核選項。然後資料收集器112讀取由資料庫伺服器130對該組配之稽核選項所

形成的且所維持的稽核軌跡。若干具體例中，資料收集器也獲得動態效能視圖86，包含由資料庫管理系統(DBMS)所維持之資料庫使用資訊，例如使用者存取活動及資源利用。資料收集器112儲存得自稽核軌跡84及動態效能視圖86

5 之使用者行為資料作為歷史資料88。處理來收集使用者行為資料且儲存作為歷史資料之範例之進一步細節說明將參照第3B圖討論如後。

資料分析器114對資料收集器112所儲存之歷史資料88執行一項或多項分析處理。一具體例中，資料分析器114執行包括分析歷史資料88等一系列操作，來決定行為模式

10 90。一具體例中，資料分析器114由歷史資料88決定資料庫存取頻率。資料庫存取頻率可對一單位時間例如一日之小時等求出。其次，資料分析器114對資料庫存取頻率決定機率函數。分析歷史資料來決定行為模式之處理範例之進一步

15 細節將參照第3C圖討論如後。

當一新資料集合由資料庫伺服器130接收得時，異常檢測器116將此新資料集合與由歷史資料決定之行為模式比較。異常檢測器116基於新資料與由歷史資料88決定之行為模式比較，判定該新資料是否代表異常活動。一具體例中，

20 異常檢測器116也將該新資料與安全法則92比較，來進行基於法則之入侵檢測。一或多項分析操作可能要求使用安全法則92或其它由資料庫伺服器130之管理者或操作者所指定之法則及條件。安全法則92提供一機制，讓異常檢測器116可判定是否發生安全破壞事件。管理站144可管理安全

法則92。一旦識別異常資料，則異常檢測器116進行鎖定目標之操作。例如異常檢測器116可發送電子郵件警告通知96給管理站144，通知有入侵事件。異常檢測器116也可或額外提供報告94或形成視覺化處理98。

- 5 一具體例中，當一事件對資料庫伺服器130維持的資料造成不良影響時，資料庫稽核引擎110可檢測得該事件。例如，資料庫稽核引擎110檢測得未知使用者透過網際網路108存取網路106，該未知使用者未經授權存取及/或操作由資料庫伺服器所維持之資料。資料庫稽核引擎110也可判定
- 10 網路106使用者是否蓄意或非蓄意危害資料庫伺服器130所儲存的資料。當惡體影響資料庫伺服器130所維持的資料時，資料庫稽核引擎110可檢測得通過網路106之「惡體」的存在。影響資料庫伺服器130且可由資料庫稽核引擎110檢測得之其它事件範例包括(但非限制性)使用偷來的通行
- 15 碼進行未經授權的存取、內部人員欺騙、誤用、或濫用特權。內部人員欺騙範例為銀行櫃台人員拷貝有價值的顧客帳戶資訊。濫用特權之範例為資料庫管理者(DBA)存取員工薪資資訊。

- 第3A圖為流程圖，顯示於一具體例，資料收集、分析及異常檢測處理之高階鳥瞰圖。於方塊310，包含使用者行為資料之資料集合由資料庫伺服器收集。於方塊320，使用者行為資料儲存作為歷史資料。於方塊330，分析歷史資料來決定行為模式。於方塊340，由資料庫伺服器接收新資料集合。於方塊350，新資料集合與行為模式比較。於方塊
- 20

360，基於比較判定該新資料集合是否滿足標準集合。於方塊370，判定該新資料是否表示異常活動。於方塊380，當方塊370已經檢測得異常活動時，進行鎖定目標之操作。各具體例中，鎖定目標之操作包括發送電子郵件警告、產生
5 報告、進行視覺化處理等中之一或多者。

資料收集

本發明具體例使用多種技術中之一或多者來收集資料庫存取資訊，以及儲存資訊於內部資料庫作為歷史資料。由資料庫管理系統收集有關資料庫存取資訊之多種方式包
10 括(但非限制性)資料庫觸動、資料庫異動改變登入、資料庫稽核設施、及資料庫動態系統視圖。

稽核設施可由多種商用資料庫管理系統提供。稽核設施可組配來稽核多種事件。稽核設施產生稽核軌跡，該稽核軌跡含有資料庫存取資訊。典型地，由稽核設施追蹤之
15 資料庫存取資訊係依據資料庫管理系統決定，但多種資料庫管理系統可供追蹤稽核資訊，例如使用者名稱、物件名稱、動作、終端、時間戳記等。

多種商用資料庫管理系統也提供動態系統視圖。動態系統視圖提供目前使用者存取活動及資源利用之相關資
20 訊。例如普及之資料庫管理系統提供若干安全性相關之動態效能視圖，V_\$SESSION列舉各次目前使用者存取活動之資訊，V_\$SESS_IO列舉各次使用者存取活動之I/O統計數字，V_\$SESSTAT列舉使用者存取活動之統計數字，V_\$ACCESS顯示目前被鎖定之物件以及存取該等物件之

使用者存取活動，以及V_\$SQL顯示於SQL集合之SQL指令文字。

比較稽核軌跡，稽核軌跡典型為永久性記錄，資料庫動態視圖典型包含暫時性資料。資料庫動態視圖可經由對

5 資料庫定期取樣監視。使用定期取樣辦法可能無法檢測於該監視時間中間發生的可疑資料庫存取。為了最小化此種可能性，取樣間隔時間須設定為相當短。相反地，稽核辦法係對全部被稽核的事件提供，而出現於稽核軌跡直到淨化為止。此外，動態視圖係以相對粗糙程度提供有關資料

10 庫存取之概略資訊，而稽核軌跡則對資料庫物件提供較為詳細且特定的資訊。一具體例中，動態視圖可用作為補充資訊，或當無法取得稽核軌跡時，例如當資料庫稽核設施未經激活時，用作為替代資訊來源。

資料庫觸動也是另一種由欲監視之資料庫收集資訊之

15 技術，其可用於即時監視，而不會讓資料庫使用者視為太具有侵略性之應用用途。資料庫異動再處理登入屬於又另一種收集資料改變資訊之技術，其可用於無需有關唯讀存取資訊之應用用途。

第3B圖為流程圖，顯示於一具體例，資料收集處理之

20 高階鳥瞰圖。於方塊311，接收欲監視之資料類型。於方塊312，基於欲監視之資料類型決定監視層面。於方塊313，基於該監視層面，激活資料庫管理者之稽核選項。於方塊314，由該稽核軌跡讀取資料集合。於方塊315，處理該資料集合。於方塊316，進行測試來決定是否有更多資料有待

讀取。若有更多資料有待讀取，則控制返回方塊314。否則控制返回呼叫方。

資料收集器由稽核軌跡或動態效能視圖收集使用者行為資料，處理資訊，以及儲存該資料為歷史資料。歷史資料例如可儲存於內部資料庫。一具體例中，對各個感興趣之動作，記錄多種屬性於該歷史資料。例如SELECT動作或LOGIN動作將包括下列屬性例如(但非限制性):(1)操作系統使用者識別符(OSUSER);(2)進行該動作之使用者之資料庫使用者識別符(DBUSER);(3)主題綱目物件識別符(OBJECT);(4)物件擁有者(OWNER);(5)客端系統識別符(LOCATION);(6)動作識別符(ACTION);(7)動作時間(TIMESTAMP);(8)該存取活動之邏輯讀取次數(READ);(9)該存取活動之邏輯寫入次數(WRITE);以及(10)成功或失敗理由代碼(RETURNCODE)。

資料庫使用者行為監視可由不同面相來進行，各個面相各有不同的注意焦點，例如包括資料庫物件層面、資料庫使用者層面、及資料庫存取活動層面。

例如於一具體例中，資料庫物件層面監視包括監視資料庫存取選定之關鍵性資料庫物件或敏感性資料庫物件。資料庫物件可為資料庫表、資料庫視圖、或資料庫儲存程序。資料庫監視將追蹤此物件由任何使用者存取之人、事、時、地，以及存取頻率。關鍵資料庫物件例如為公司「員工」表，其含有員工薪資資訊。

另一例中，於一具體例，資料庫使用者層面監視包括

監視由選定之資料庫使用者對資料庫物件的存取。資料庫監視將追蹤此使用者存取任何物件之時、地、物、及頻率。選定之資料庫使用者可能是被懷疑由資料庫竊取資訊之員工。

- 5 另一例中，於一具體例，資料庫存取活動層面監視包括監視由選定之資料庫使用者所做資料庫連結或登入時段。資料庫監視將追蹤此使用者之登入持續時間、登入失敗或資源利用。

- 10 一具體例中，於資料庫之一或多個不同稽核選項將基於欲藉資料庫稽核引擎執行之監視層面而自動致能。被致能的稽核選項係取決於主題資料庫之資料庫管理系統。例如於一具體例中，為了支援資料庫之物件層面監視，資料庫監視系統對一特定物件自動致能物件稽核。為了支援資料庫使用者層面或存取活動層面監視，系統自動致能對特定使用者之陳述稽核。

15 資料分析

- 本發明之具體例可對入侵檢測資料分析實作一項或多項辦法。一具體例中，基於統計之入侵檢測(SBID)及基於法則之入侵檢測(RBID)可聯合用來檢測異常資料庫存取。於使用基於統計之入侵檢測之具體例中，進行使用者行為資訊史之統計分析，來產生使用者行為模式。任何顯著偏離此等使用者行為模式之隨後資料庫存取將被決定為表示異常活動。使用基於法則之入侵檢測之具體例，將維持包含安全法則或安全限制之知識庫，也稱作為管制方策。違反管制方策之資料庫存取將被判定為表示異常活動。
- 20

第3C圖為流程圖，顯示於一具體例執行基於統計之入侵檢測之資料分析處理的高階鳥瞰圖。於方塊331，由歷史資料決定資料庫存取頻率。基於該歷史資料，可建立有效用於檢測異常活動之統計模型。歷史資料之統計分析可決定正常資料庫存取率。

於方塊332，由方塊331決定之資料庫存取頻率，決定資料庫存取頻率之機率函數。資料庫存取頻率可配合機率分佈。特定具體例中，可使用各種機率分佈例如(但非限制性)常態機率分佈或波森機率分佈。

一範例中，使用者於白晝或夜晚隨機以固定速率存取資料庫。資料庫存取速率於白晝及夜晚可有不同。於此標準集合下，波森分佈可用來描述於指數分佈後兩次事件間之時間之資料庫存取頻率。設X表示每個時間間隔出現之隨機數目，m為每個時間間隔出現之隨機數目平均，以及P為於該時間間隔出現n次之X機率：

$$P(X=n)=e^{-m}\left[\frac{m^n}{n!}\right] \quad (1)$$

於方塊333，可決定累進分佈函數(CDF)。一使用波森分佈之具體例中，累進分佈函數獲得值小於或等於n之X機率，如方程式(2)所示：

$$F(n)=P(X\leq n)=\sum_{i=0}^n e^{-m}\left[\frac{m^i}{i!}\right] \quad (2)$$

資料分析器決定機率分佈函數之參數值。以波森分佈為例，該參數值為m值，對歷史資料每時間間隔出現之隨機

數目平均數。

例如出現可定義為對該資料庫發出SELECT指令之數目，以及時間間隔可定義為一日之小時數。於其它實作，出現可定義為其它類型指令或事件，時間間隔可定義為其它時段。於隨後處理中，異常檢測器基於該機率函數比較新資料點與歷史資料。

各具體例中，資料分析器係基於多重屬性維度來分析歷史資料，屬性包括(但非限制性)操作系統使用者、資料庫使用者、所在位置及物件。可對各個操作系統使用者、資料庫使用者、所在位置、物件或多重屬性組合計算存取頻率。基於各個維度之測量值可用於定量比較。

例如於一具體例，物件層面監視包括(但非限制性)下列一或多個測量值：以一天時間計之物件存取頻率、以一天時間及操作系統使用者計之物件存取頻率、以一天時間及資料庫使用者計之物件存取頻率、以一天時間及位置計之物件存取頻率、以及多重維度物件存取頻率法則，其包括以一天時間計之屬性組合(操作系統使用者、資料庫使用者及所在位置)計之物件存取頻率。

於另一具體例，物件層面監視包括(但非限制性)下列一或多個測量值：以一天時間計之使用者存取頻率、以一天時間及操作系統使用者計之使用者存取頻率、以一天時間及資料庫使用者計之使用者存取頻率、以一天時間及位置計之使用者存取頻率、以及多重維度使用者存取頻率法則，其包括以一天時間計之屬性組合(操作系統使用者、資料庫

使用者及所在位置)計之使用者存取頻率。

- 除了物件存取頻率或使用者存取頻率外，其它測量值也可用於各具體例之存取活動層面監視例如(但非限制性)以每一存取活動讀取頁數測得之以存取活動計之存取頻率、以每一存取活動之小時數測得之以存取活動計之存取持續時間、以及以每分鐘讀取頁數測得之存取比。

異常檢測

- 第3D圖為流程圖顯示於一具體例處理之異常檢測之高階鳥瞰圖。於方塊351，對新資料集合測定資料庫存取頻率。於方塊352，由防護標準及機率函數參數測定臨限值頻率。一具體例中，機率函數參數為先前於方塊331藉資料分析器測得之歷史資料存取頻率。一具體例中，存取頻率為以一天時間計之SELECT操作平均數。

- 例如若資料分析器由歷史資料決定上午2點之平均存取頻率為1.5，接收得新資料，指示上午2點之目前存取頻率為7，新資料是否超出正常範圍。答案係依據防護標準決定。一具體例中，防護標準表示為機率百分比。異常檢測器由防護標準機率百分比及機率函數參數(亦即於方塊331藉資料分析器算出的歷史存取頻率)測得臨限值存取頻率值。任何超出臨限值之頻率值將無法測試，而可視為異常。防護百分比愈低，則事件歸類為異常愈困難，出現的錯誤警訊愈少。

例如若防護機率標準規定為0.1%，異常檢測器計算臨限值n，具有超過n值之機率小於0.1%，如方程式(3)所示：

$$P(X>n)=1-P(X\leq n)<0.1\% \quad (3)$$

如此等於測定臨限值 n ，數值小於或等於 n 之機率高於99.9%，如方程式(4)所示：

$$F(n)=P(X\leq n)>99.9\% \quad (4)$$

- 5 以得自方程式(4)之 $F(n)>99.9\%$ 及 m 值為1.5(機率函數參數、歷史資料平均存取頻率)代入方程式(2)之累進分佈函數，結果獲得臨限值 $n=6$ 。

因新資料集合之存取頻率為7，超過臨限值存取頻率值6，故檢測得異常。

- 10 於方塊353，目前存取頻率值(得自方塊351)對臨限值存取頻率(得自方塊352)比較。

一具體例中，異常檢測器基於動態統計模式及/或基於靜態法則之管制方策，檢測得可疑歷史資料資料庫存取，且產生電子郵件警告。也產生報告或線圖。

- 15 安全性管制方策可用來監視資料庫使用者行為。例如於一具體例，有兩類不同安全性管制方策：(1)存取頻率管制方策及(2)存取違犯管制方策。存取頻率管制方策致能資料庫稽核引擎基於各種維度來防護以一天時間計之存取次數。如前文討論，此種入侵檢測可為基於統計學，及/或基於法則。於一具體例，防護臨限值可以一天時間計存取次數等為單位，規定為絕對值。存取違犯管制方策致能資料庫稽核引擎使用明確安全性法則來防衛個別資料庫存取。
- 20 表1列舉於一具體例可用來監視資料庫使用者行為之各項安全性管制方策。

表1:安全性管制方策			
監視層面	類別	安全性管制方策	入侵檢測方法
物件層面監視	存取頻率	以一天時間計之物件存取頻率	基於統計或基於法則
		以一天時間及操作系統使用者計之物件存取頻率	基於統計或基於法則
		以一天時間及資料庫使用者計之物件存取頻率	基於統計或基於法則
		以一天時間及所在位置計之物件存取頻率	基於統計或基於法則
		多重維度物件存取頻率法則	基於統計或基於法則
	存取違犯	物件存取安全性違犯	基於法則
		可疑操作系統使用者之物件存取	基於法則
		可疑資料庫使用者之物件存取	基於法則
		可疑位置之物件存取	基於法則
		多重維度物件存取違犯法則	基於法則
使用者層面監視	存取頻率	以一天時間計之使用者存取頻率	基於統計或基於法則
		以一天時間及操作系統使用者計之使用者存取頻率	基於統計或基於法則
		以一天時間及資料庫物件計之使用者存取頻率	基於統計或基於法則
		以一天時間及所在位置計之使用者存取頻率	基於統計或基於法則
		多重維度使用者存取頻率法則	基於統計或基於法則
	存取違犯	使用者存取安全性違犯	基於法則
		可疑操作系統使用者之使用者存取	基於法則
		可疑資料庫物件之使用者存取	基於法則
		可疑位置之使用者存取	基於法則
		多重維度使用者存取違犯法則	基於法則
存取活動層面監視	存取頻率	高讀取比(頁/分鐘)	基於統計或基於法則
		過量讀取活動	基於統計或基於法則
		極長登入存取活動	基於統計或基於法則
	存取違犯	登入失敗	基於法則
		於可疑時框登入	基於法則
		由可疑操作系統使用者登入	基於法則
		由可疑位置登入	基於法則
		多重維度存取活動法則	基於法則

例如各具體例中可對物件層面監視規定以下存取違犯法則：(1)物件存取安全性違犯，其中對任何未經適當許可而嘗試讀取特定物件失敗皆發出警訊；(2)由可疑操作系統使用者存取物件，其中對無效操作系統使用者任一次成功地讀取特定物件皆發出警訊。一具體例中可界定有效操作系統使用者表單，任何非於表單之操作系統使用者存取皆發出警訊。另一具體例中，可界定無效操作系統使用者表單，任何於表單之操作系統使用者存取皆發出警訊；(3)由可疑資料庫使用者作物件存取，其中由無效資料庫使用者任何成功地讀取特定物件皆發出警訊。一具體例中，界定有效及/或無效資料庫使用者表單；(4)來自可疑位置之物件存取，其中來自無效客端系統之任何成功的讀取特定物件皆發出警訊。一具體例中，可界定有效位置及/或無效位置表單；以及(5)多重維度物件存取法則，其中以無效屬性(操作系統使用者、資料庫使用者及所在位置)組合任何成功地讀取特定物件皆發出警訊。

另一例中，可對使用者層面監視規定以下存取違犯法則：(1)使用者存取安全性違犯，其中任何未經適當允許之特定資料庫使用者嘗試讀取失敗皆發出警訊；(2)由可疑操作系統使用者存取使用者，其中任何來自無效操作系統使用者由特定資料庫使用者之任何成功的讀取皆發出警訊。一具體例中可界定有效操作系統使用者及/或無效操作系統使用者表單；(3)由可疑資料庫物件作使用者存取，其中由特定資料庫使用者成功地讀取無效資料庫物件皆發出警

訊。一具體例中，界定有效及/或無效物件表單；(4)來自可疑位置之使用者存取，其中由來自無效客端系統之特定資料庫使用者之任何成功的讀取皆發出警訊。一具體例中，可界定有效位置及/或無效位置表單；以及(5)多重維度使用者存取法則，其中以無效屬性(操作系統使用者、資料庫使用者及所在位置)組合任何成功地讀取特定資料庫使用者皆發出警訊。

另一例中，於各具體例中，可對處理時段層面監視規定下列存取違犯法則，可規定如下存取違犯法則：(1)登入失敗，其中因無效通行碼造成登入失敗發出警訊；(2)於可疑時框登入，其中超出特定正常時間的登入時間發出警訊；(3)由可疑操作系統使用者登入，其中由特定資料庫使用者及無效操作系統使用者成功地登入發出警訊。一具體例中，可界定有效操作系統使用者及/或無效操作系統使用者表單；(4)由可疑位置登入，其中由無效客端系統之特定資料庫使用者成功地登入發出警訊。一具體例中可界定有效位置及/或無效位置表單；以及(5)多重維度處理時段法則，其中以無效屬性組合(操作系統使用者及所在位置)之任何成功的登入發出警訊。

20 監視實施例

一具體例之資料庫監視操作將使用參照第3E圖流程圖以及第6A-6M圖所示拍攝得之畫面討論之資料庫監視操作之組配及使用範例作說明。一具體例中，以使用網路瀏覽器實作之圖形使用者介面來組配監視操作。於第6A-6M圖

所示使用者介面畫面中，使用者可遵循前一或次一瀏覽箭頭來逐步通過一監視操作之組配過程。另外，使用者可由面板頂端之選單列中選擇一項，或由面板左方之階層樹狀視圖中點選一條鏈路連結。

- 5 使用者藉開啟欲監視之資料庫而開始處理，如第3E圖所示，方塊410。一具體例中，開啟資料庫包括藉規定主機名稱、資料庫名稱、使用者資料庫及通行碼來界定一資料庫連結，如第6A圖所示。使用者連結至特定資料庫，如第6B圖所示。

- 10 於方塊420，使用者對特定資料庫組配一監視排程。於監視排程之處理過程包括使用者規定資料分析器以何種頻率來「習得」使用者行為資料，且重構統計模型，如第6C圖所示。使用者也規定異常檢測器「防衛」異常資料頻次，及送出警報頻次，再度係使用第6C圖所示畫面。

- 15 於方塊430，使用者組配電子郵件接收器。使用者規定於一具體實施例，使用第6D圖所示畫面，出現異常時發送警報電子郵件給何人。

- 於方塊440，使用者組配監視管制方策。第6E-6F圖所示畫面顯示於一具體實施例之監視管制方策之組配。使用者
20 者選擇一「關鍵」物件來監視，如第6E圖所示。使用者選擇存取違犯管制方策來激活此物件，如第6F圖所示。使用者規定允許何人存取此一物件。對於多重維度物件法則，則界定作為屬性組合。例如資料庫使用者WANI唯有其登入作為操作系統使用者 IPLOCKS/WTANG 且由客端系統

WLINUX登入時才可存取本物件，如第6G圖所示。使用者也規定存取頻率管制方策被激活來監視此物件，如第6H圖所示。

於方塊450，使用者開始監視。一具體例中，經由點選第6I圖所示狀態畫面的打勾框而開始監視。

- 5 於方塊460，使用者觀視警報及/或線圖。於一假想範例，屬於資料庫使用者WANI的資料庫通行碼被竊，壞人試圖使用竊來的通行碼由非該通行碼指定使用之機器存取一資料庫物件。壞人的嘗試使用造成存取違犯多重維度物件法則，如第6J圖所示。例如組配之多重維度物件法則指示
- 10 資料庫使用者 WANI 只可藉操作系統使用者 IPLOCKS/WANI 且由所在位置 WLINUX 存取物件 HR.EMP(如第6G圖所示)。壞人試圖由不同的操作系統使用者 IPLOCKS/CKCHOU、且由不同的所在位置 CKDESKTOP 以資料庫使用者 WANI 存取物件，造成存取違犯。則可觸動
- 15 鎖定目標之操作。於第6J圖所示範例中，電子郵件警訊將發送給電子郵件接收器，使用如第6D圖所示畫面界定。使用者視圖透過圖形使用者介面發出警訊，如第6K圖所示。使用者也觀視到由任何使用者對任何物件之存取模式，如第6L圖所示。若使用者違犯存取頻率臨限值或百分比，則
- 20 也將發出警訊。

於方塊470，使用者產生報告。使用者對該摘要產生報告，有助於分析該問題，如第6M圖所示。前文參照第3E圖及第6A-6M圖說明之處理僅為使用一具體例之範例。其它具體例將包括其它處理及其它畫面(為求簡明於此處不做

討論)，及/或可刪除若干此處所述之處理及/或畫面。

第4圖為線圖，顯示於一具體例中對一資料庫之存取機率分佈範例。第4圖顯示於24小時時間由特定使用者之資料庫存取活動範例。第4圖中，各柱表示由此使用者每小時存取物件數目。第4圖所示範例機率分佈中，使用者存取資料庫之機率有二尖峰，一個尖峰可能出現於上午中間時間，另一個尖峰可能出現於下午中間時間。於此時框以外之過度資料庫存取活動皆可疑。

第5圖為方塊圖，顯示於一具體例，一資料庫監視系統之高階鳥瞰圖。如第5圖所示，一資料庫監視系統包含三層級架構。於第一層級，資料庫監視系統包括一網路瀏覽器以供存取資料庫監視功能。於一具體例，爪哇割頁(JSP)提供使用者介面。

於第二層級，資料庫監視系統使用一網路伺服器，於一具體例係使用Apache Tomcat實作，以及使用儲存歷史資料之一內部資料庫，於一具體例係使用PostgreSQL資料庫實作。本發明之具體例可駐在任何運算平台之外，例如(但非限制性)Pentium或相當功能硬體平台結合安全Linux操作系統執行。資料庫監視系統之組成元件包括資料收集器、資料分析器及異常檢測器。支援組成元件包含以下一或多者：(1)一組配器，其讓使用者可根據實作特定需求(例如排程設定值及管制方策設定值)依客戶需求製作資料庫監視系統；(2)電子郵件警報及發出警訊給指定之安全官；(3)報告管理者且產生偵錯報告；以及(4)視覺化處理器其產生表

示資料庫使用者行為模式之線圖代表圖。

於第三層級，資料庫監視系統使用爪哇資料庫連結(JDBC)API來存取目標資料庫。

硬體綜論

- 5 一具體例中，第1圖所示運算環境100之各個組成元件可實作為可由一或多部處理器執行的指令集。第7圖顯示可用來執行此等組成元件之電腦系統700之硬體方塊圖。電腦系統700包括一匯流排702或其它通訊資訊之通訊機構，以及一耦合至匯流排702用來處理資訊之處理器704。電腦系
- 10 統700也包括一主記憶體706例如隨機存取記憶體(RAM)或其它動態儲存裝置耦合至匯流排702用來儲存欲藉處理器704執行之資訊及指令。主記憶體706也用來儲存於執行欲藉處理器704執行之指令期間，之各項暫時變數及其它中間資訊。電腦系統700進一步包括一唯讀記憶體(ROM)708或
- 15 其它耦合至匯流排702用來儲存處理器704之靜態資訊及指令之靜態儲存裝置。一儲存裝置710(例如磁碟或光碟)經設置且耦合至匯流排702供儲存資訊及指令。

- 電腦系統700可透過匯流排702耦合至顯示器712(如陰極射線管(CRT))來顯示資訊給電腦使用者。一輸入裝置714
- 20 包括文數鍵及其它鍵係耦合至匯流排702，用來通訊資訊及指令選擇給處理器704。另一型使用者輸入裝置為游標控制裝置716，例如滑鼠、軌跡球、或游標方向鍵用來通訊方向資訊及指令選擇給處理器704，且用來控制游標於顯示器712之移動。此輸入裝置典型於二軸亦即第一軸(如x軸)以及

第二軸(如y軸)有二度自由度，其允許裝置規定於一平面位置。

根據一具體例，本發明之功能係由電腦系統700回應於執行含於主記憶體706之一或多項指令之一或多種順序提供。此種指令可由任何電腦可讀取媒體如儲存裝置710讀取
5 入主記憶體706。含於主記憶體706之指令順序的執行造成處理器704執行此處所述方法步驟。另一具體例中，硬體電路可用來替代或組合軟體指令來實作本發明。如此本發明之具體例非僅限於任何特定硬體電路與軟體的組合。

此處使用「電腦可讀取媒體」一詞表示任何可參與提
10 供指令給處理器704供執行的媒體。此種媒體可呈多種形式包括(但非限制性)非依電性媒體、依電性媒體、及傳輸媒體。非依電性媒體例如包括光碟或磁碟如儲存裝置710。依電性媒體包括動態記憶體如主記憶體706。傳輸媒體包括同軸纜線、銅線、及光纖包括包含匯流排702之導線。傳輸媒
15 體可呈聲波或光波形式，例如於射頻波及紅外線資料傳輸所產生之波。

常見電腦可讀取媒體形式包括例如軟碟、可撓性碟片、硬碟、磁帶或任何其它磁性媒體、CD-ROM、任何其它光學媒體、打孔卡片、紙帶、任何其它帶有孔圖案的實
20 體媒體、RAM、PROM及EPROM、FLASH-EPROM、任何其它記憶體晶片或卡匣、如後文說明之載波或任何其它電腦可讀取的媒體。

多種形式之電腦可讀取媒體涉及攜帶一或多項指令之一或多種順序供處理器704執行。例如指令初步可載於遠端

電腦磁碟。遠端電腦可將指令載入其動態記憶體，且使用數據機透過電話線發送指令。電腦系統當地的數據機接收到電話線上的資料，使用紅外光發射器來將資料轉成紅外光信號。紅外光檢測器可接收紅外光信號中所載有的資料，適當電路可將資料置於匯流排702。匯流排702將資料載至主記憶體706，處理器704由主記憶體取還指令且執行指令。主記憶體706接收之指令可於處理器704執行之前或之後，儲存於儲存裝置710。

電腦系統700也包括通訊介面718耦合至匯流排702。通訊介面718提供雙向資料通訊耦合至一網路鏈路720，其係連結至一本地網路722。例如通訊介面718可為整合式服務數位網路(ISDN)卡或數據機，來提供資料通訊連結至對應類型之電話線。至於另一例，通訊介面718可為區域網路(LAN)卡來提供資料通訊連結至可相容之LAN。也可實作無線鏈路。於任一種實作，通訊介面718發送且接收電信號、電磁信號或光信號其載有表示各類型資訊之數位資料流。

網路鏈路720典型提供經由一或多個網路，資料通訊至其它資料裝置。例如網路鏈路720提供由本地網路722連結至主機電腦724，或連結至由網際網路服務提供者(ISP)726所操作的資料設備。ISP 726又經由今日俗稱為「網際網路」728之全球封包資料通訊提供資料通訊服務。本地網路722及網際網路728皆使用載有數位資料流之電信號、電磁信號或光信號。通過各網路之信號、以及於網路鏈路720且通過通訊介面718之信號(其攜帶數位資料來去於電

腦系統700)屬於轉運資訊之載波之範例形式。

電腦系統700可經由網路、網路鏈路720及通訊介面718發送訊息及接收資料包括程式碼。於網際網路範例中，伺服器730可經由網際網路728、ISP 726、本地網路722及通訊
5 介面718發送對應用程式的請求碼。接收得之碼於接收時由處理器704執行，及/或儲存於儲存裝置710，或儲存於其它非依電性儲存裝置供後來執行之用。藉此方式電腦系統700可以載波形式獲得應用程式碼。

前述說明書中已經指出雖然本發明係參照特定具體例
10 作說明，但絕非視為限制性。熟諳技藝人士了解本揭示內容可未悖離本發明之精髓做出多項修改。如此本發明並非限於特定具體例，特定具體例係用來舉例說明本發明，本發明只受所核准之申請專利範圍之範圍所限。如此說明書及附圖僅視為說明性而非限制性。

15 **【圖式簡單說明】**

本發明將於附圖各圖舉例說明本發明，而非限制性，附圖中類似之參考編號表示類似之元件，附圖者：

第1圖為方塊圖，顯示於一具體例，可實作資料庫監視技術之網路電腦系統之高階鳥瞰圖。

20 第2圖為線圖，顯示於一具體例，資料庫稽核引擎範例處理之高階鳥瞰圖。

第3A-3E圖為方塊流程圖，顯示於一具體例，資料收集、分析、及異常檢測處理之高階鳥瞰圖。

第4圖為線圖，顯示於一具體例，存取一資料庫之範例

機率分佈。

第5圖為方塊圖，顯示於一具體例，一資料庫監視系統之高階鳥瞰圖。

第6A-6M圖為畫面拍攝照片，顯示於一具體例，監視
5 操作之組配範例。

第7圖為硬體方塊圖，顯示代表性電腦系統，其可用於具體實作一具體例之一或多個組成元件。

【主要元件符號說明】

84...稽核軌跡	144...管理站
86...動態效能視圖	310-370、311-316、331-333、
88...歷史資料	351-353、410-470...方塊
90...行為模式	700...電腦系統
92...安全法則	702...匯流排
94...報告	704...處理器
96...電子郵件警訊	706...主記憶體
98...視覺化處理	708...唯讀記憶體，ROM
100...電腦系統	710...儲存裝置
106...網路	712...顯示器
108...網際網路	714...輸入裝置
110...資料庫稽核引擎	716...游標控制裝置
112...資料收集器	718...通訊介面
114...資料分析器	720...網路鏈路
116...異常檢測器	722...本地網路
122...路由器	724...主機電腦
124...防火牆	726...網際網路服務提供業者、ISP
130...資料庫伺服器	728...網際網路
132...資料庫	730...伺服器

五、中文發明摘要：

本發明之具體例提供監視一資料庫系統之異常活動之技術。接受監視之一主題資料庫之相關使用者行為資訊可自動收集、分析，且與一或多項管制方策比較來檢測異常活動。具體實施例由多種不同來源，包括稽核軌跡及動態視圖，與資料庫之資料庫管理系統協力合作，收集有關該主題資料庫之使用者行為資料。具體例採用基於統計之入侵檢測(SBID)、及基於法則之入侵檢測(RBID)中之一或多者，來檢測異常資料庫活動。若檢測得偏離正常使用模式之可疑資料庫存取，則進行鎖定目標操作，例如警知負責的安全人員、產生報告、電子郵件寄出警訊通知等。

六、英文發明摘要：

Embodiments of the present invention provide techniques for monitoring a database system for anomalous activity. User behavior information relative to a subject database being monitored may be automatically collected, analyzed and compared with one or more policies to detect anomalous activity. Embodiments collect user behavior data regarding the subject database from a variety of sources, including an audit trail and dynamic views in cooperation with the database management system of the database. Embodiments employ one or more of statistics-based intrusion detection (SBID) and rule-based intrusion detection (RBID) to detect anomalous database activity. If suspicious database access that deviate from the normal usage pattern are detected, a targeted operation, such as alerting the responsible security officers, generating reports, email alerts or the like, is performed.

十、申請專利範圍：

1. 一種監視一資料庫之方法，包含：
 - 收集使用者行為資料，其指示一或多個使用者如何使用該資料庫；
 - 5 處理及儲存該資料作為歷史資料；
 - 分析歷史資料來決定行為模式；
 - 接收一新資料集合，其指示一或多個使用者如何使用該資料庫；
 - 進行新資料集合與該行為模式的比較；
 - 10 基於該比較，判定該新資料集合是否滿足標準集合；
 - 若該新資料集合滿足該標準集合，則判定該新資料集合表示異常活動；以及
 - 回應於該判定，執行鎖定目標之操作。
- 15 2. 如申請專利範圍第1項之方法，進一步包含：
 - 決定新資料集合是否違犯基於法則之管制方策；以及
 - 若該新資料集合違犯基於法則之管制方策，則決定該新資料集合是否表示異常活動。
3. 如申請專利範圍第2項之方法，其中收集使用者行為資料進一步包含：
 - 20 由資料庫管理者之稽核軌跡或動態效能視圖讀取資訊。
4. 如申請專利範圍第3項之方法，其中收集使用者行為資料進一步包含：

於選自下列之至少一個監視層面收集資訊：

有關對一或多個選定資料庫物件之資料庫存取資訊；

5 有關對一或多個選定資料庫使用者之資料庫存取資訊；以及

有關對一或多個選定資料庫使用者存取活動之資料庫存取資訊。

5. 如申請專利範圍第3項之方法，其中收集使用者行為資料進一步包含：

10 接收一類欲監視之資訊；

由該資訊類型決定一監視層面；以及

基於決定之監視層面激活該資料庫管理者稽核操作。

6. 如申請專利範圍第2項之方法，其中分析該歷史資料來決定行為模式進一步包含：

15

由該歷史資料決定一統計模型。

7. 如申請專利範圍第6項之方法，其中由該歷史資料決定一統計模型進一步包含：

由該歷史資料決定資料庫存取頻率；

20 對該資料庫存取頻率決定一機率函數；以及

由該機率函數決定一累進機率函數。

8. 如申請專利範圍第7項之方法，其中進行新資料集合與該行為模式之比較進一步包含：

使用該新資料集合對該統計模型測試一假說。

9. 如申請專利範圍第8項之方法，其中使用該新資料集合對該統計模型測試一假說進一步包含：

對該新資料集合決定資料庫存取頻率；以及

由一防護標準及一機率函數參數決定該臨限值。

- 5 10. 如申請專利範圍第9項之方法，其中使用該新資料集合對該統計模型測試一假說進一步包含：

比較該新資料集合之資料庫存取頻率與該臨限值。

11. 如申請專利範圍第7項之方法，其中該歷史資訊係有關對一或多個選定資料庫物件之資料庫存取，以及其中由
10 該統計資料決定資料庫存取頻率進一步包含決定以下列至少一者之頻率：

以一天時間計之物件存取頻率、以一天時間計操作系統使用者計之物件存取頻率、以一天時間計資料庫使用者計之物件存取頻率、以一天時間計位置計之物件存取頻率、以一天時間計操作系統使用者、資料庫使用者
15 與位置中之至少二者的組合之物件存取頻率。

12. 如申請專利範圍第7項之方法，其中該歷史資訊係有關對一或多個選定資料庫使用者之資料庫存取，以及其中
20 由該統計資料決定資料庫存取頻率進一步包含決定以下列至少一者之頻率：

以一天時間計之使用者存取頻率、以一天時間計操作系統使用者計之使用者存取頻率、以一天時間計資料庫使用者計之使用者存取頻率、以一天時間計位置計之使用者存取頻率、以一天時間計操作系統使用者、資料

庫使用者與位置中之至少二者的組合之使用者存取頻率。

13. 如申請專利範圍第7項之方法，其中該歷史資訊係有關對一或多個選定資料庫使用者存取活動之資料庫存取，以及其中由該統計資料決定資料庫存取頻率進一步包含決定以下列至少一者之頻率：

每次存取活動讀取頁數、每次存取活動存取時間、每單位時間讀取頁數。

14. 如申請專利範圍第1項之方法，其中執行一鎖定目標操作包含下列至少一者：產生一警訊；發送一電子郵件；產生一報告；執行視覺化處理。

15. 一種電腦可讀取媒體，載有一或多個指令順序，用來回應於裝置錯誤回復至復原組配結構，該指令當由一或多個處理器執行時，造成該一或多處理器進行下列步驟：

收集使用者行為資料，其指示一或多個使用者如何使用該資料庫；

處理及儲存該資料作為歷史資料；

分析歷史資料來決定行為模式；

接收一新資料集合，其指示一或多個使用者如何使用該資料庫；

進行新資料集合與該行為模式的比較；

基於該比較，判定該新資料集合是否滿足標準集合；

若該新資料集合滿足該標準集合，則判定該新資料

集合表示異常活動；以及

回應於該判定，執行鎖定目標之操作。

16. 如申請專利範圍第15項之電腦可讀取媒體，進一步包含指令其當由一或多個處理器執行時，造成一或多處理器進行下列步驟：

決定新資料集合是否違犯基於法則之管制方策；以及
若該新資料集合違犯基於法則之管制方策，則決定該新資料集合是否表示異常活動。

17. 如申請專利範圍第16項之電腦可讀取媒體，其中該進行收集使用者行為資料步驟之指令進一步包含指令供執行下述步驟：

由資料庫管理者之稽核軌跡讀取資訊。

18. 如申請專利範圍第17項之電腦可讀取媒體，其中該進行收集使用者行為資料步驟之指令進一步包含進行於一監視層面收集資訊之步驟之指令，該監視層面係選自下列至少一者：

有關對一或多個選定資料庫物件之資料庫存取資訊；

- 有關對一或多個選定資料庫使用者之資料庫存取資訊；以及

有關對一或多個選定資料庫使用者存取活動之資料庫存取資訊。

19. 如申請專利範圍第17項之電腦可讀取媒體，其中該進行收集使用者行為資料步驟之指令進一步包含進行下列

步驟之指令：

接收一類欲監視之資訊；

由該資訊類型決定一監視層面；以及

基於決定之監視層面激活資料庫管理者之稽核操

5 作。

20. 如申請專利範圍第16項之電腦可讀取媒體，其中該進行
分析歷史資料來判定行為模式之步驟之指令進一步包
含進行下列步驟之指令：

由該歷史資料決定一統計模型。

10 21. 如申請專利範圍第20項之電腦可讀取媒體，其中該進行
由歷史資料決定統計模型之步驟之指令包含進行下列
步驟之指令：

由該歷史資料決定資料庫存取頻率；

對該資料庫存取頻率決定一機率函數；以及

15 由該機率函數決定一累進機率函數。

22. 如申請專利範圍第21項之電腦可讀取媒體，其中該進行
執行新資料集合與該行為模式間之比較之步驟之指令
進一步包含進行下述步驟之指令：

使用該新資料集合對該統計模型測試一假說。

20 23. 如申請專利範圍第22項之電腦可讀取媒體，其中該進行
使用該新資料集合對該統計模型測試一假說之步驟之
指令進一步包含進行下列步驟之指令：

對該新資料集合決定資料庫存取頻率；以及

由一防護標準及一機率函數參數決定該臨限值。

24. 如申請專利範圍第23項之電腦可讀取媒體，其中該進行使用該新資料集合對該統計模型測試一假說之步驟之指令進一步包含進行下列步驟之指令：

比較該新資料集合之資料庫存取頻率與該臨限值。

5 25. 如申請專利範圍第21項之電腦可讀取媒體，其中該歷史資訊係有關對一或多個選定之資料庫物件之資料庫存取，以及其中該進行由歷史資料決定資料庫存取頻率之步驟之指令進一步包含進行決定下列至少一種頻率之步驟之指令：

10 以一天時間計之物件存取頻率、以一天時間計操作系統使用者計之物件存取頻率、以一天時間計資料庫使用者計之物件存取頻率、以一天時間計位置計之物件存取頻率、以一天時間計操作系統使用者、資料庫使用者與位置中之至少二者的組合之物件存取頻率。

15 26. 如申請專利範圍第21項之電腦可讀取媒體，其中該歷史資訊係有關對一或多個選定之資料庫使用者之資料庫存取，以及其中該進行由歷史資料決定資料庫存取頻率之步驟之指令進一步包含進行決定下列至少一種頻率之步驟之指令：

20 以一天時間計之使用者存取頻率、以一天時間計操作系統使用者計之使用者存取頻率、以一天時間計資料庫使用者計之使用者存取頻率、以一天時間計位置計之使用者存取頻率、以一天時間計操作系統使用者、資料庫使用者與位置中之至少二者的組合之使用者存取頻

率。

27. 如申請專利範圍第21項之電腦可讀取媒體，其中該歷史資訊係有關對一或多個選定之資料庫使用者存取活動之資料庫存取，以及其中該進行由歷史資料決定資料庫存取頻率之步驟之指令進一步包含進行決定下列至少一種頻率之步驟之指令：

每次存取活動讀取頁數、每次存取活動存取時間、每單位時間讀取頁數。

28. 如申請專利範圍第15項之電腦可讀取媒體，其中該進行執行鎖定目標操作之步驟之指令包含進行下列至少一者之指令：產生一警訊；發送一電子郵件；產生一報告；執行視覺化處理。

29. 一種裝置，包含：

收集手段，其係用來收集使用者行為資料，其指示一或多個使用者如何使用該資料庫；

處理與儲存手段，其係用來處理及儲存該資料作為歷史資料；

分析手段，其係用來分析歷史資料來決定行為模式；

接收手段，其係用來接收一新資料集合，其指示一或多個使用者如何使用該資料庫；

執行手段，其係用來進行新資料集合與該行為模式的比較；

決定手段，其係用來基於該比較，判定該新資料集

合是否滿足一標準集合；

決定手段，其係用來若該新資料集合滿足該標準集合，則判定該新資料集合表示異常活動；以及

回應手段，其係用來回應於該判定，執行鎖定目標之操作。

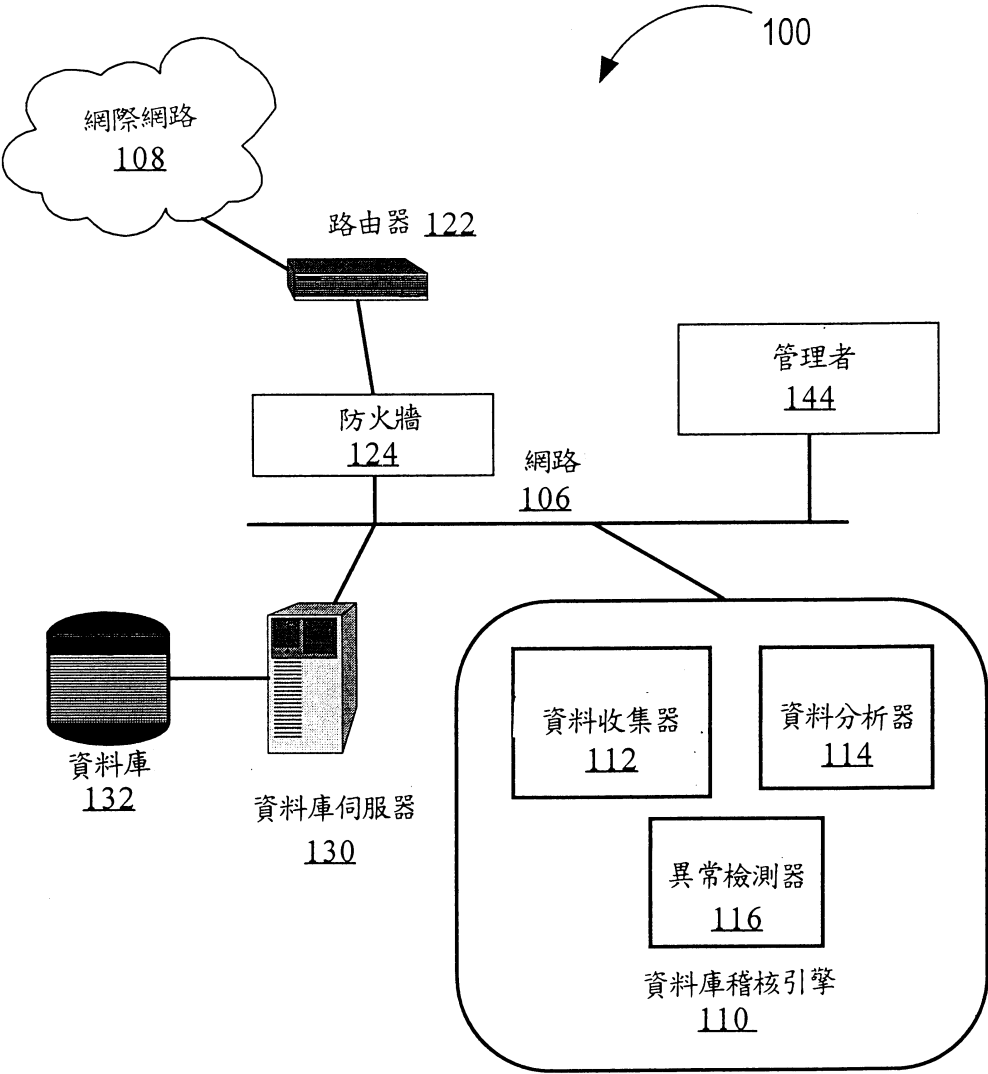
30. 一種裝置，包含：

一資料收集器，用來收集使用者行為資料，其指示一或多個使用者如何使用該資料庫且處理及儲存該資料作為歷史資料；以及接收一新資料集合，其指示一或多個使用者如何使用該資料庫；

一資料分析器，用來分析該歷史資料來決定行為模式；以及

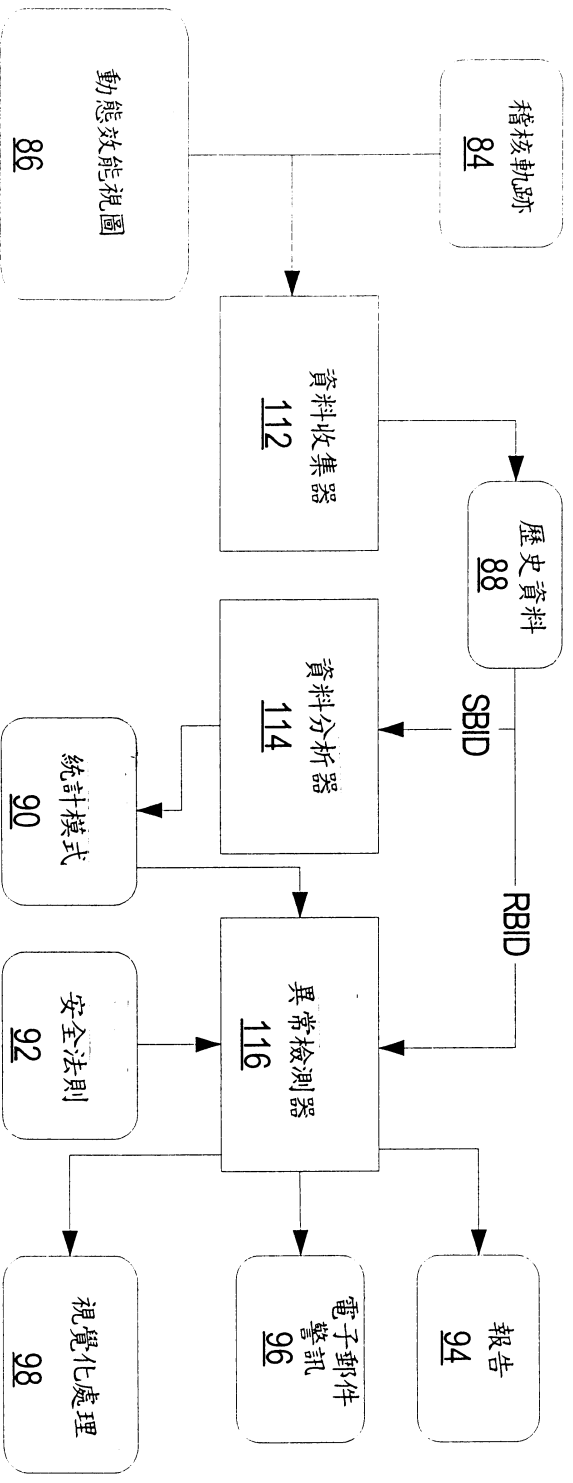
一異常檢測器，用來進行新資料集合與該行為模式的比較；基於該比較，判定該新資料集合是否滿足一標準集合；若該新資料集合滿足該標準集合，則判定該新資料集合表示異常活動；以及回應於該判定，執行鎖定目標之操作。

+

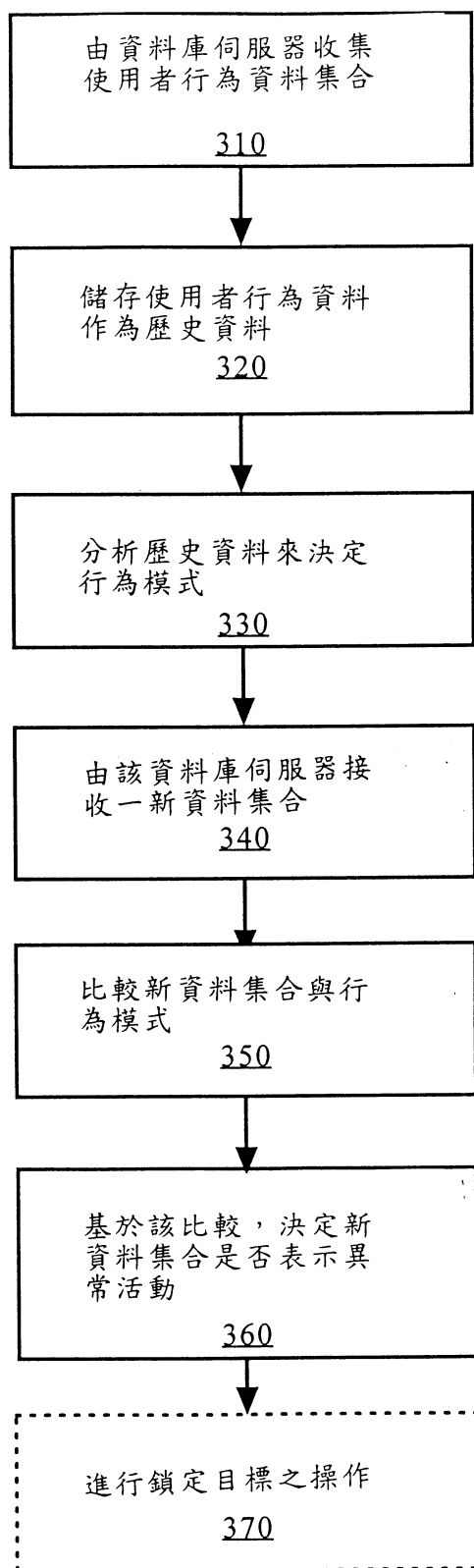


第 1 圖

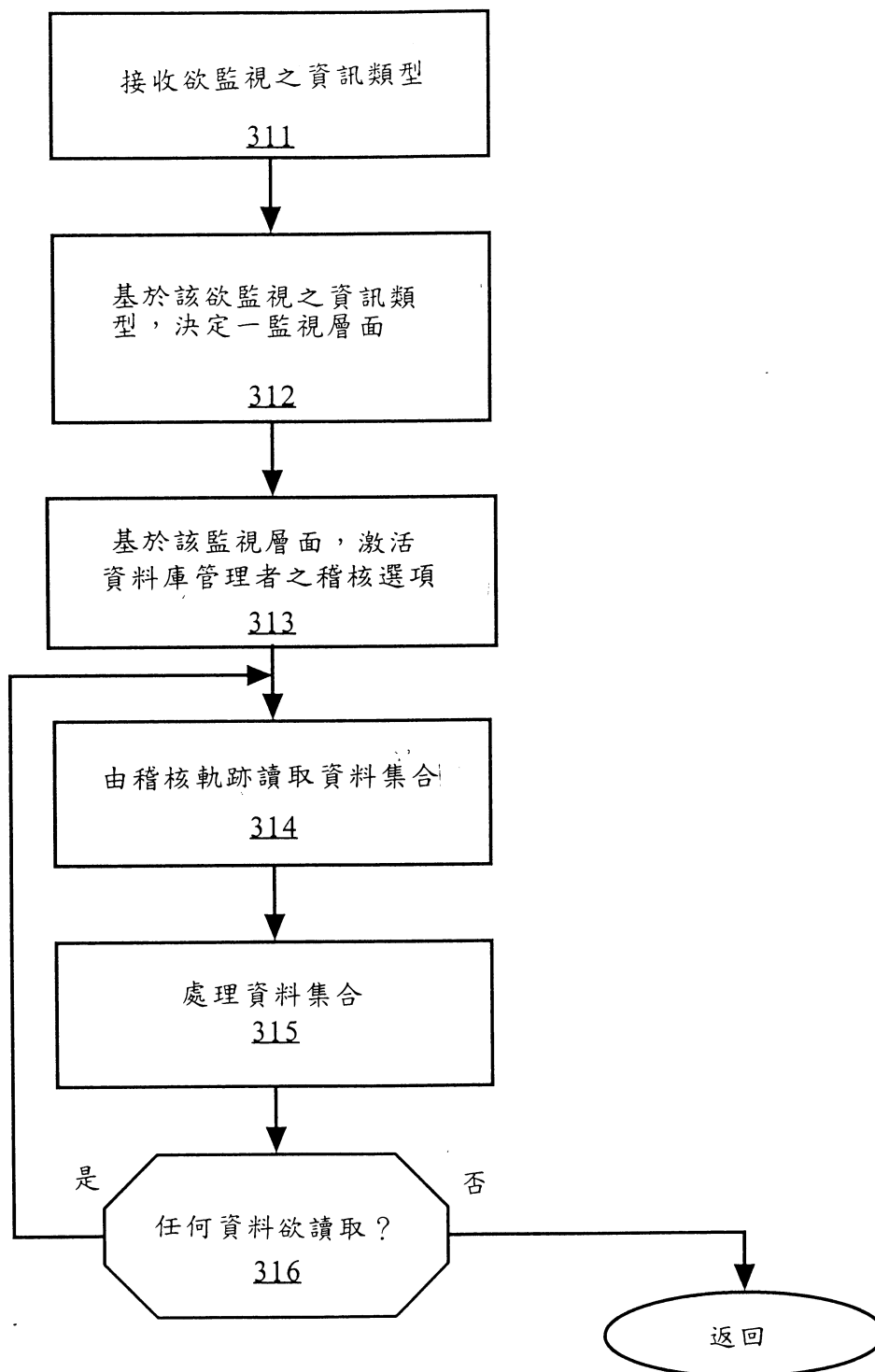
+



第 2 圖



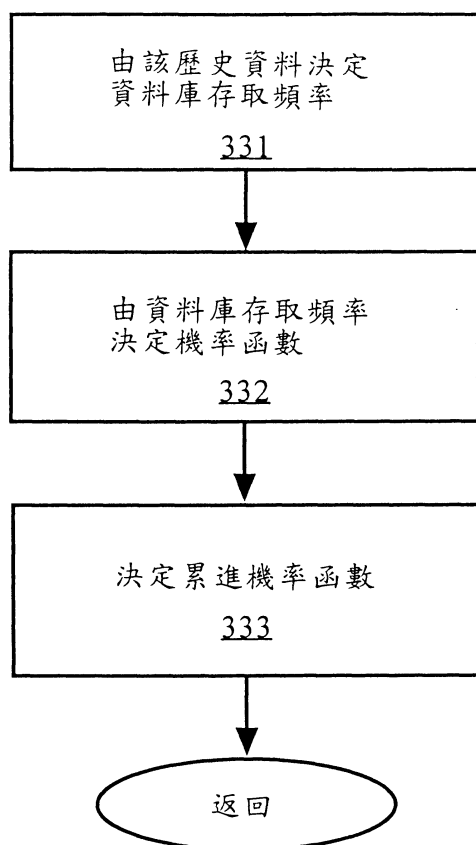
第3A圖



第3B 圖

+

5/23

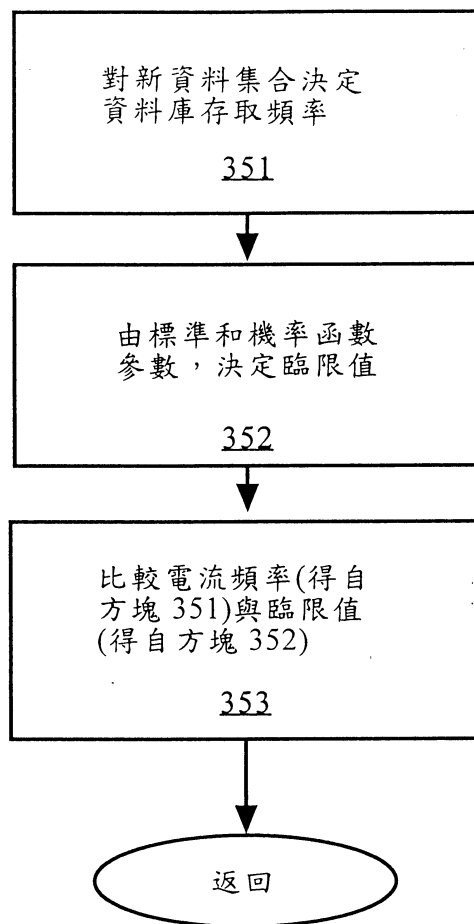


第3C圖

+

+

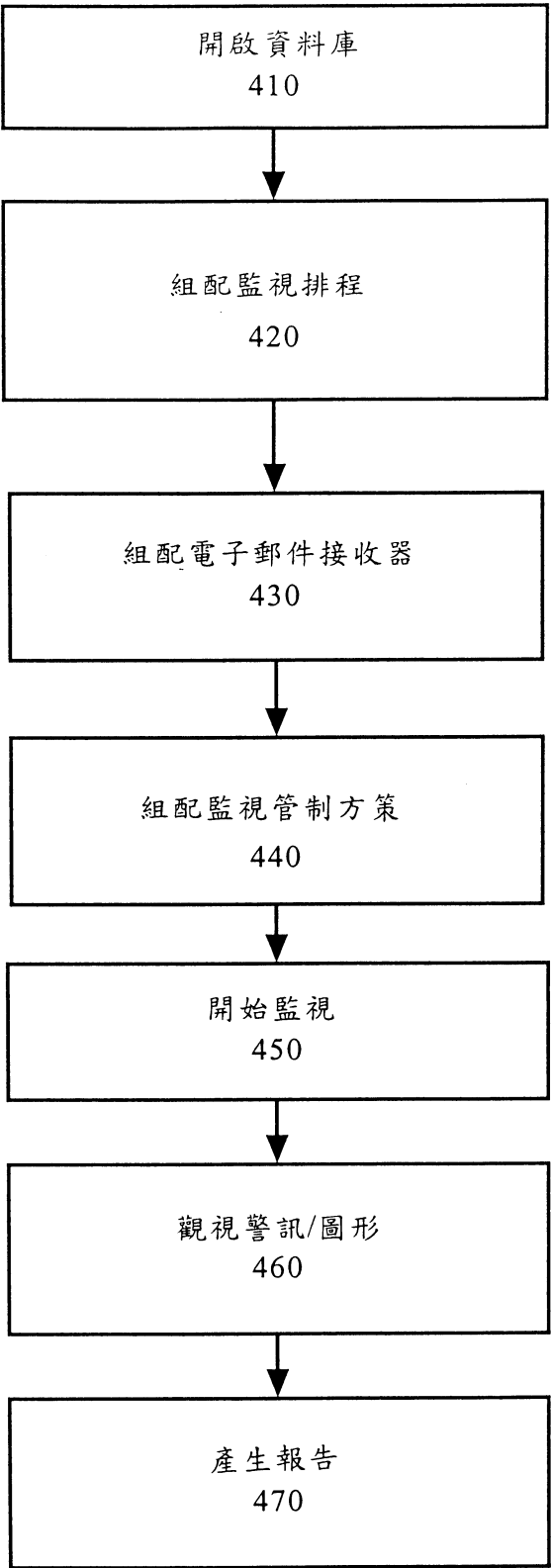
6/23



第3D圖

+

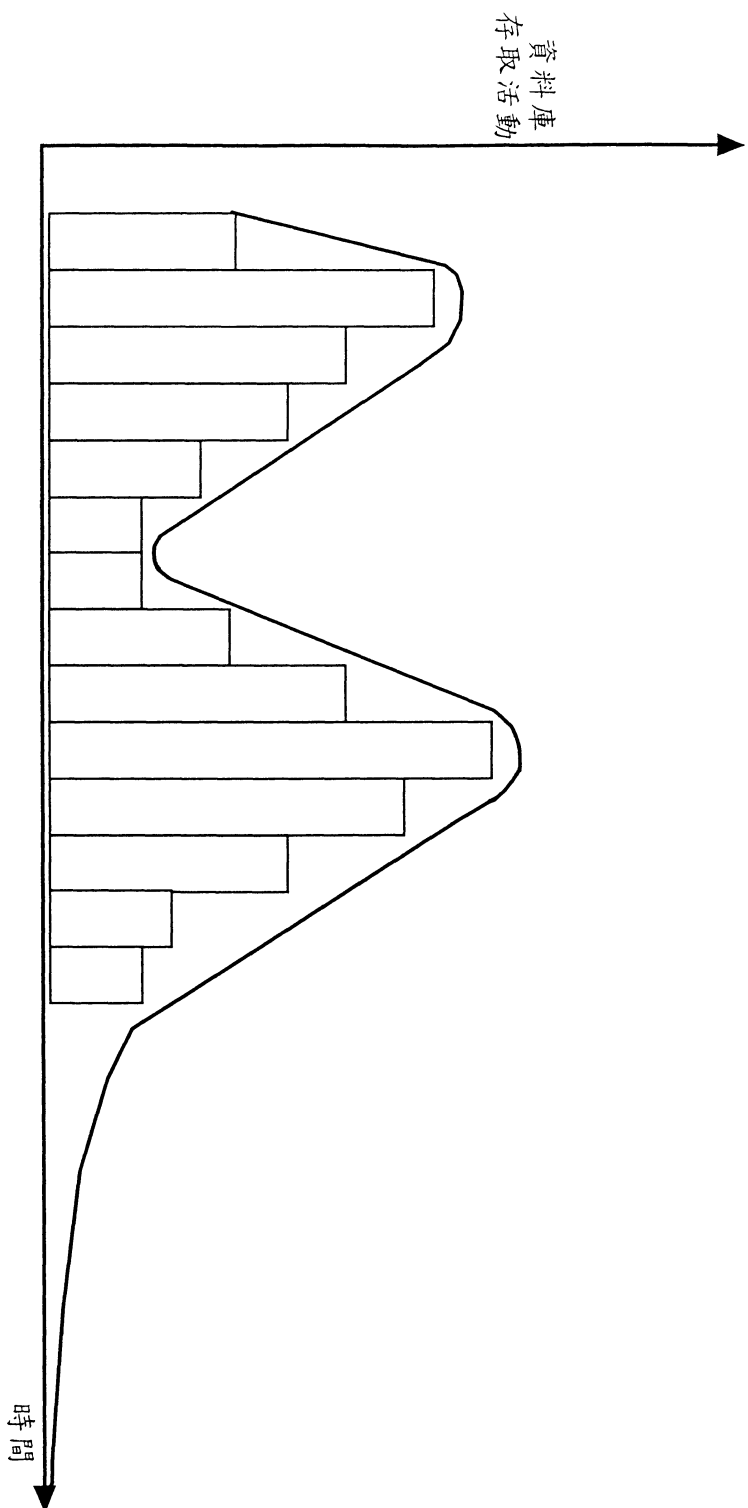
+

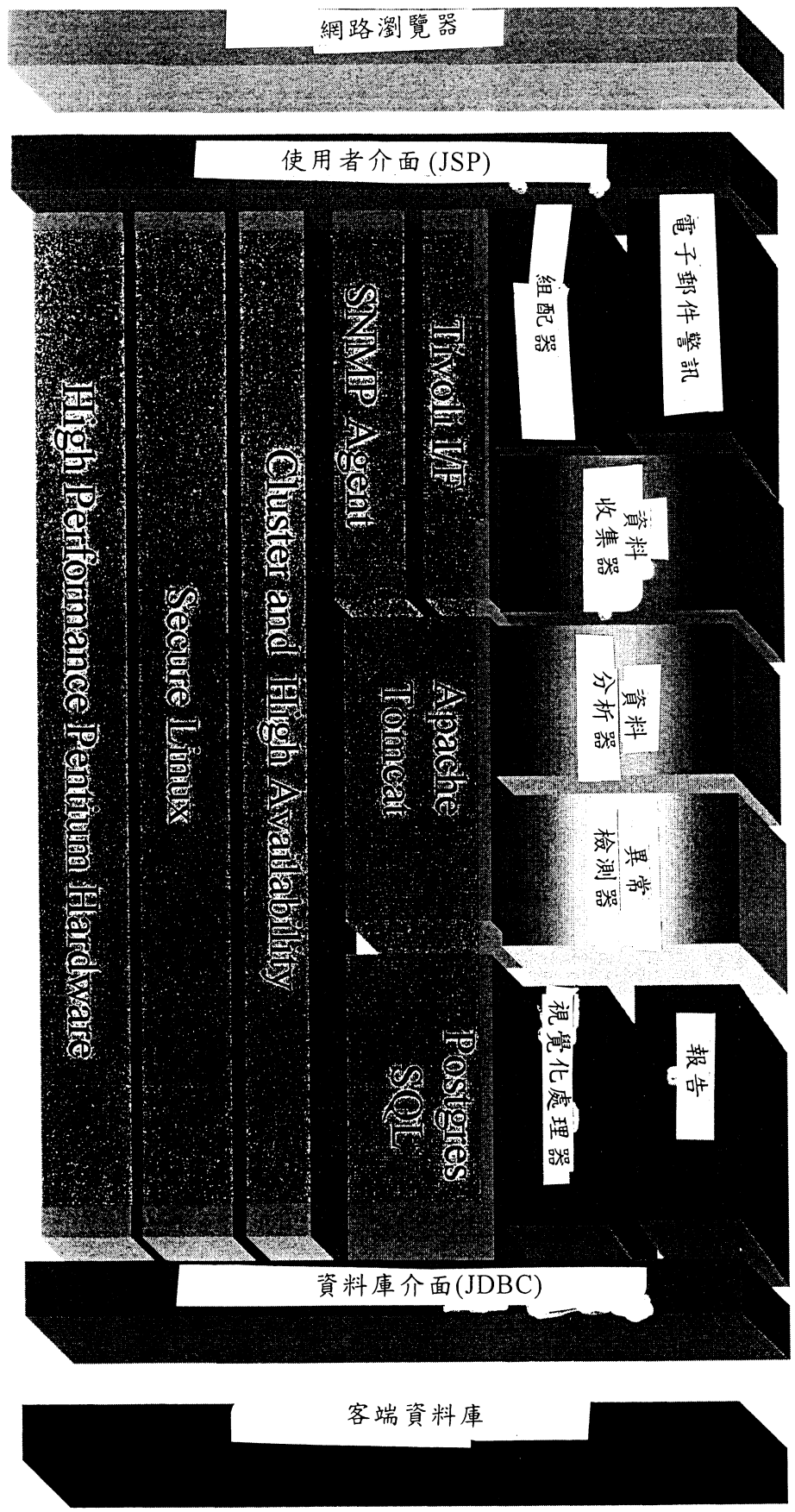


第3E圖

+

第 4 圖





第 5 圖

IPLOCKS User Behavior Monitor - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back

Address http://basd2650/Iplocks/Idm/jsy/dbguardhome.jsp

Search Favorites Media

MY ACCOUNT ABOUT IPLOCKS PRODUCT OVERVIEW DOCUMENTATION LOGOUT

Go Links

IPLOCKS

Database Set Defaults Set Policies Analysis Help

basd2650 Status

No database specified.

User Behavior Monitor

User Behavior Monitor Module

No database is currently opened. Click this link and go to Open Database page. If you don't have any database exist, please go to Create New Database Connection page first.

Module Learn Schedule Setting

Module Guard Schedule Setting

Database Learn Schedule Setting

Database Guard Schedule Setting

Default Email Settings

Create New Database Connection

* required fields

Database Connection Name *	cctest2	Monitored Application Name	
Database Server Name/IP (with port) *	198.245.1.32:1521	Database Location	
Database Name *	cctest2	Region	
Database Server type *	Oracle	Division	
Username *	system	Business Unit	
Password *	*****	Usage	
DBA1 Name		DBA2 Name	
DBA1 Tel		DBA2 Tel	
DBA1 Email		DBA2 Email	

Create Upload

Previous - Main Page

Next - Open Target Database

Local intranet

第 6A圖

IPLOCKS

User Behavior Monitor

User Behavior Monitor Module

- No database is currently opened. Click this link and go to Open Database Page. If you don't have any database exist, please go to Create New Database Connection page first.
- Module Learn Schedule Setting
- Module Guard Schedule Setting
- Database Learn Schedule Setting
- Database Guard Schedule Setting
- Default Email Settings

IPLOCKS

dssd2650 status

No database specified

Open Target Database

Choose The Target Database

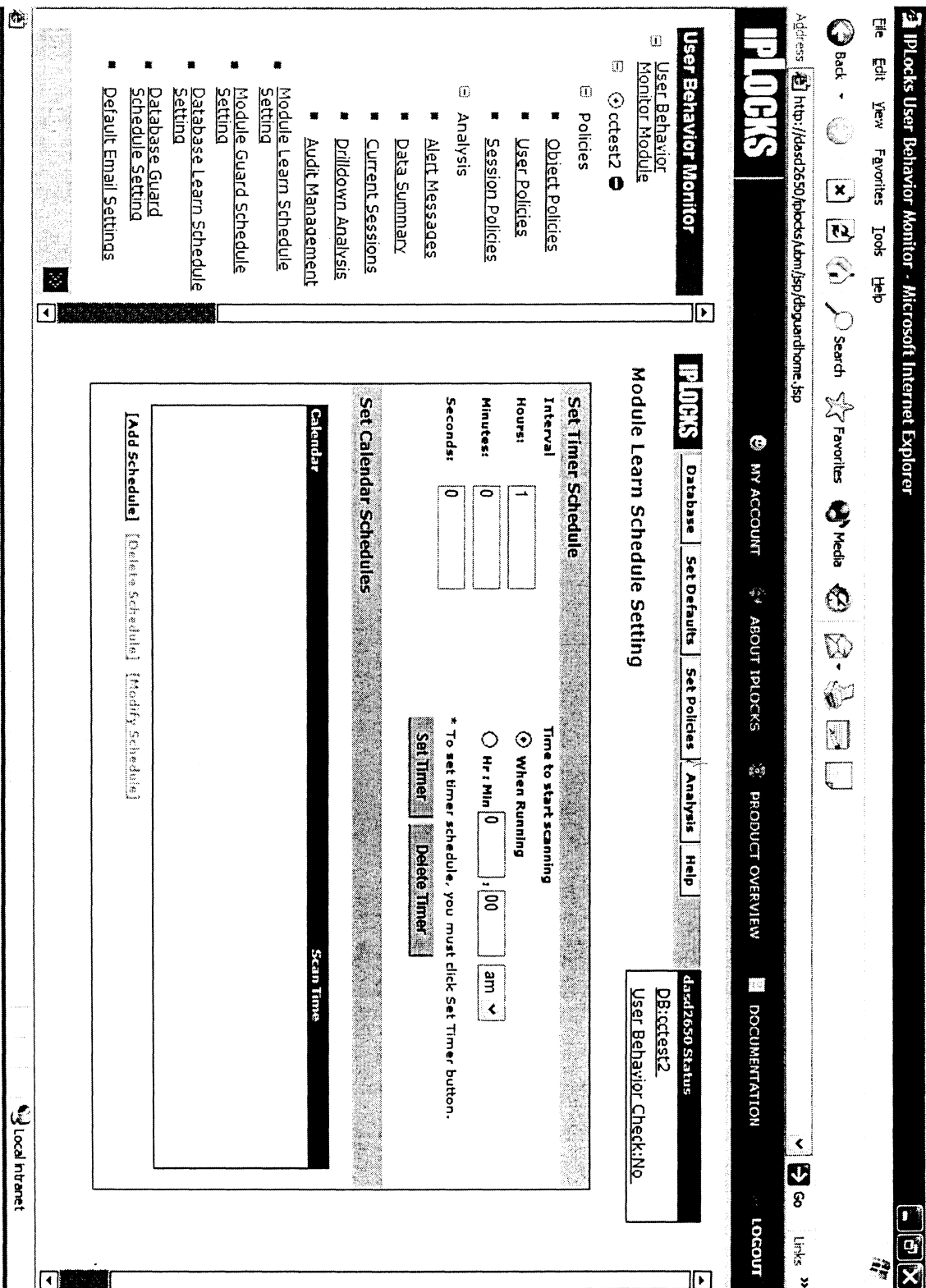
ctes12
db_oracle8_db2serv_o817
db_oracle9_boradd1_md9i
db_oracle8_dboral_ctes12
db_oracle8_ipora8_ip8i
db_oracle8_ipora8_orack
db_oracle8_ipora8_qlst
db_oracle8_ipora8_or8db
db_oracle9_sonyfnv27_wani
db_oracle7_orat_dmdb
db_oracle7_orat_emdb
db_oracle8_sunv100

[Modify] [Delete]

[Open] [Open and Run] [Close]

Previous - Create New Database Connection

Next - Module Schedule Setting



第 6C 圖

EditViewFavoritesToolsHelp

Back

http://dsad2650/locks/Album/jsp/dbguardhome.jsp

Go Links

LOCKS

MY ACCOUNTABOUT IPLOCKSPRODUCT OVERVIEWDOCUMENTATIONLOGOUT

User Behavior Monitor

User Behavior Monitor Module

DB:ctest2

User Behavior Check:No

Polices

Object Policies

User Policies

Session Policies

Analysis

Alert Messages

Data Summary

Current Sessions

Drilldown Analysis

Audit Management

Module Learn Schedule Setting

Module Guard Schedule Setting

Database Learn Schedule Setting

Database Guard Schedule Setting

Default Email Settings

Default Email Settings

From this page you can manage the list of email receivers for the DSAS server. You should set the SMTP Host to your email server, and set the sender email address (will appear in the "From" section of alert emails). To add a new receiver, click the "Add Receiver" link and enter information for that receiver, clicking the "Save" button to finalize your changes. To delete or modify a receiver, select that receiver by clicking on the receiver name and clicking "Delete Selected" or "Modify Selected". To select the default receivers, check the receivers who will get messages by default and click "Set Default Receivers".

Sender

SMTP Host IPipemail.iplocks.com

Sender Emaildsasadmin@iplocks.com

Set Sender

Receivers

Email GroupShow All Groups

Add GroupDelete GroupRename Group

Default Receiver(s)Wani Tang (wtang@iplocks.com)

Add ReceiverDelete SelectedModify SelectedSet Default Receiver(s)

Previous - Database Guard Schedule Setting

Next - Object Policies

第 6D 圖

13/23

User Behavior Monitor

User Behavior Monitor Module

cctest2

Policies

Object Policies

User Policies

Session Policies

Analysis

Alert Messages

Data Summary

Current Sessions

Drilldown Analysis

Audit Management

Module Learn Schedule

Module Guard Schedule

Setting

Database Learn Schedule

Setting

Database Guard

Schedule Setting

Default Email Settings

Database Connection Name

cctest2

Enabled Disabled Default Receivers Item Specific Receivers
Default Learn Schedule Default Guard Schedule Item Specific Learn Schedule Item Specific Guard Schedule

Add Object Policies Guard Item

Enter information about this guarded item in the tabs below.

Item Settings

Access Violation Settings

Access Frequency Settings

Select a table to guard.

Schema: HR

Table

BONUS
DEPT
DUMMY
EMP
SALGRADE

IPlocks User Behavior Monitor - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back - X Stop Search Favorites Media

Address http://daseid2650/iplocks/ibm/jsn/ibguardhome.jsp

IPLOCKS

MY ACCOUNT

ABOUT IPLOCKS

PRODUCT OVERVIEW

DOCUMENTATION

LOGOUT

Go link5

User Behavior Monitor

User Behavior Monitor Module

ctest2

Policies

Object Policies

User Policies

Session Policies

Analysis

Alert Messages

Data Summary

Current Sessions

Drilldown Analysis

Audit Management

Module Learn Schedule

Setting

Module Guard Schedule

Setting

Database Guard

Schedule Setting

Default Email Settings

Current Object Policies Guarded Items

Select Status Guarded Item Description

Schedule Receivers

Severity

Add Object Policies Guard Item

Enter information about this guarded item in the tabs below.

Item Settings

Access Violation Settings

Access Frequency Settings

Active Rule

Rule Description

Edit

☒ Security Violation

Alert any failed attempt to read selected object without proper permission

☐ Suspicious OS User

Alert any successful read to selected object by invalid OS users

☐ Suspicious Database User

Alert any successful read to selected object by invalid database users

☐ Suspicious Location

Alert any successful read to selected object from invalid client systems

☒ Multiple Dimension Object Rule

Alert any successful read to selected object with invalid combination of attributes (OS user, Location and DB User)

第 6F 圖

File Edit View Favorites Tools Help

Address http://193.42.26.50/iplocks/ADMIN/jsplbkguardhome.jsp

Back Search Favorites Media

MY ACCOUNT ABOUT IPLOCKS PRODUCT OVERVIEW DOCUMENTATION LOGOUT

User Behavior Monitor

User Behavior Monitor Module

o ctest2

Policies

Object Policies

User Policies

Session Policies

Analysis

Alert Messages

Data Summary

Current Sessions

Drilldown Analysis

Audit Management

Module Learn Schedule Setting

Module Guard Schedule Setting

Database Learn Schedule Setting

Database Guard Schedule Setting

Default Email Settings

Current Object Policies Guarded Items

Select Status Guarded Item Description

Schedule Receivers Severity

Add Object Policies Guard Item

Enter information about this guarded item in the tabs below.

Item Settings Access Violation Settings Access Frequency Settings

Active Rule

Rule Description

Threshold Percentile Edit

Active Rule	Rule Description	Threshold	Percentile	Edit
☒ Time Violation	Alert excessive read to selected object within 24HR time slot	100	0	%
☐ OS User and Time Violation	Alert excessive read to selected object within 24HR time slot grouped by OS User	0	0	%
☐ DB User and Time Violation	Alert excessive read to selected object within 24HR time slot grouped by DB User	0	0	%
☐ Terminal and Time Violation	Alert excessive read to selected object within 24HR time slot grouped by Terminal	0	0	%
☒ Multiple Dimension Object Rule	Alert excessive read to selected object within 24HR time slot grouped by a combination of attributes (OS User, Terminal and DB User)	0	0.1	%

Local intranet

第 6H 圖

17/23



Address http://dasd2650/iplocks/htm/jsq/dqguardhome.jsp

MY ACCOUNT

ABOUT IPLOCKS

PRODUCT OVERVIEW

DOCUMENTATION

Logout

IPLOCKS

User Behavior Monitor

User Behavior Monitor Module

cctest2

Policies

Object Policies

User Policies

Session Policies

Analysis

Alert Messages

Data Summary

Current Sessions

Drilldown Analysis

Audit Management

Module Learn Schedule

Setting

Module Guard Schedule

Setting

Database Guard

Schedule Setting

Default Email Settings

IPLOCKS

Database

Set Defaults

Set Policies

Analysis

Help

Status

The following database is opened: cctest2

Database Server Name(IP): 192.168.1.167:1521

DSAS Host Name: dasd2650

Database Name: cctest2

Database Connection Name: cctest2

User Behavior Check is running.

User Behavior Check ☒ Yes

* To start/stop security check/uncheck the boxes and click update button.

Update

Previous - Session Policies

Next - Alert Messages

Done

Local intranet

cautionary UBM alert raised from cctest2 (Object Policies:HR,EMP) - Message (HTML) - Unicode (UTF-8)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: dssadrin@plocks.com

To: Wanl Tang

Cc:

Subject: cautionary UBM alert raised from cctest2 (Object Policies:HR,EMP)

Brief Description:

Alarm ID: 1,782

Severity: cautionary

Violated Policy: Object Policies

Guarded Item: HR,EMP

Alarm Generated Time: 2004-01-23 14:24:22

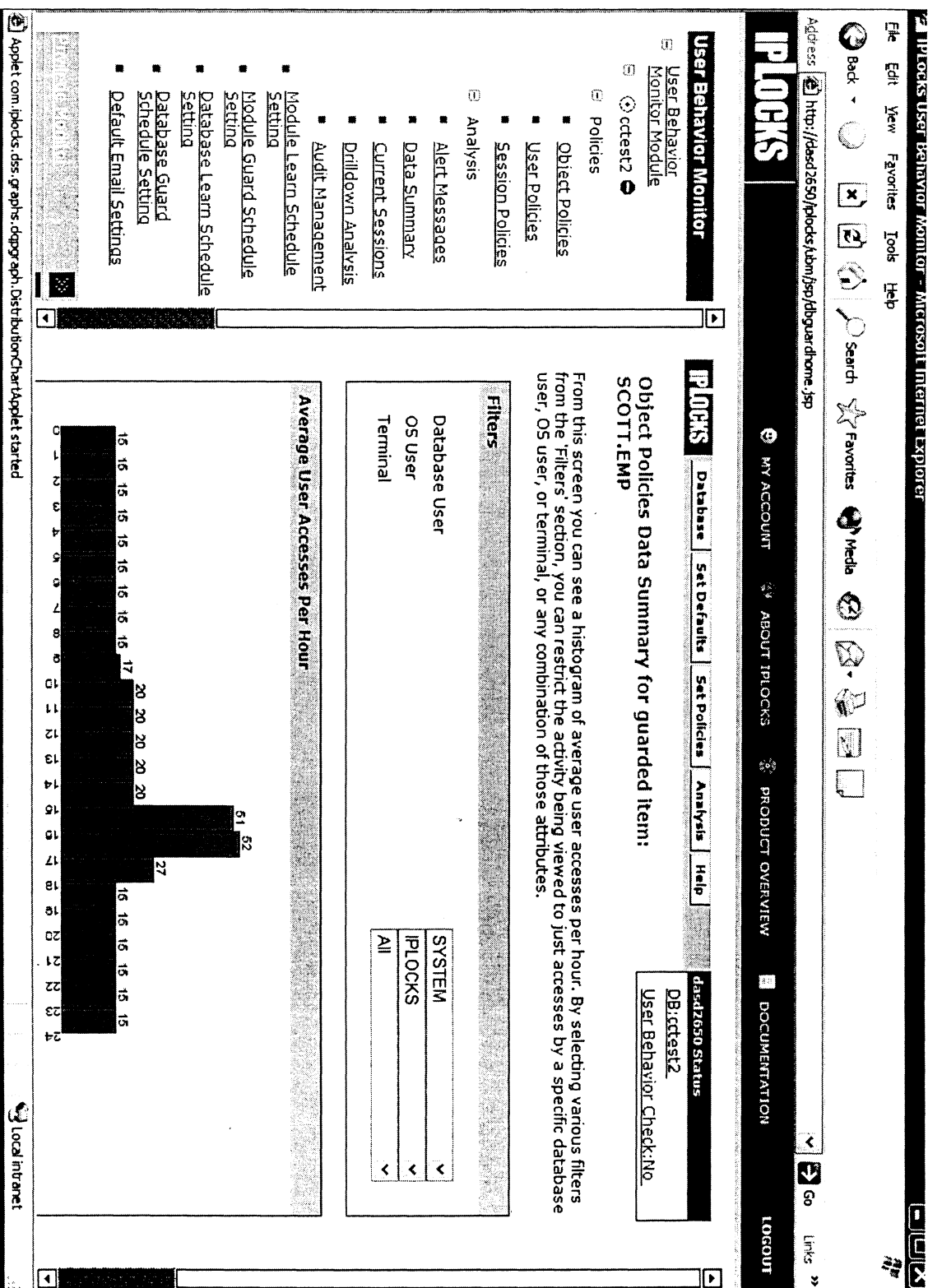
Application: UBM@dassd2650:80

Database: CCTEST2@192.168.1.166:1521

Detailed Description:

Database object HR,EMP is accessed by DB user WANI at 1/23/04 2:11 PM with suspicious attribute combination:
Terminal=CKDESKTOP, OS User=ILOCKS\CKCHOU and DB User=WANI

To update alarm status use the link:[Update Status](#)



第 6L 圖

IPlocks

MY ACCOUNT

ABOUT IPLOCKS

PRODUCT OVERVIEW

DOCUMENTATION

LOGOUT

Alarm Report Manager

- Alarm Report Manager
- Current Reports
- Schedule Setting
- Default Email Settings

IPLOCKS

Set Defaults Reports Help

Preview Report Setting

Report Information

Report Name: ubm-ctest2
 Date Generated: 2004-01-16 14:17:10
 Applications: UBM
 Database: cctest2
 Number of Alarms Meeting Criteria: 5
 * To sort column click on header.

dasd2650 Status
 Report Running: No

ID	App	Database	Policy	Guarded Item	Severity	Status	Time
1156	UBM	cctest2	User Policies	CCHEN	cautionary	Error_Corrected	2003/12/19 11:32
1157	UBM	cctest2	Session Policies	SCOTT	cautionary	Not Handled	2003/12/19 11:33
1616	UBM	cctest2	Session Policies	SCOTT	cautionary	Not Handled	2004/01/16 13:36
1618	UBM	cctest2	Object Policies	SCOTT.EMP	cautionary	Not Handled	2004/01/16 13:54
1619	UBM	cctest2	Session Policies	WANI	cautionary	Acknowledged	2004/01/16 14:11

Informational 0 Cautionary 5 Minor 0 Major 0 Critical

Export to Excel Tab Delimited Comma Delimited

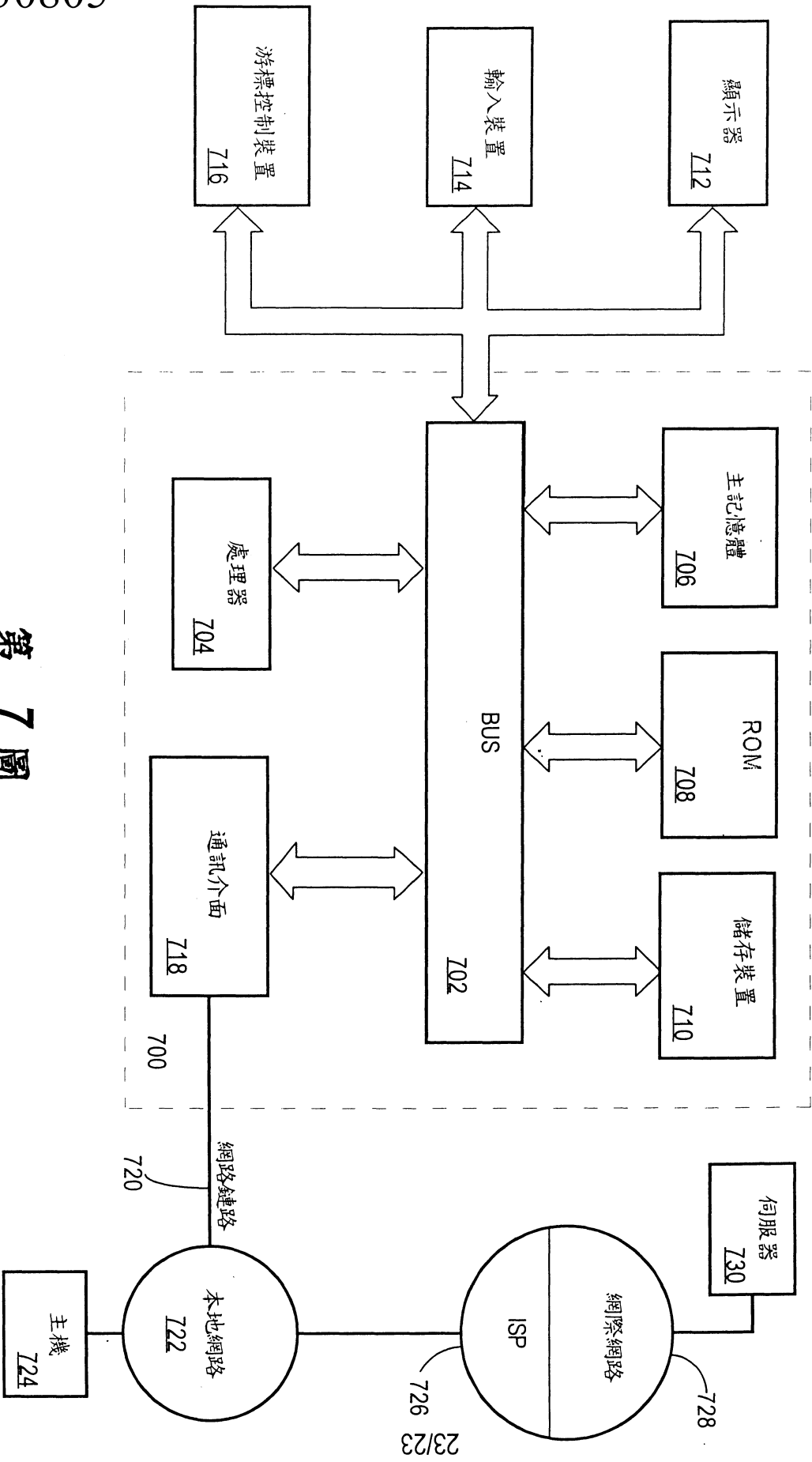
Previous - Current Reports

Next - Status

Done

local intranet

第 6M 圖



第 7 圖

七、指定代表圖：

(一)本案指定代表圖為：第（ 1 ）圖。

(二)本代表圖之元件符號簡單說明：

100...電腦系統	116...異常檢測器
106...網路	122...路由器
108...網際網路	124...防火牆
110...資料庫稽核引擎	130...資料庫伺服器
112...資料收集器	132...資料庫
114...資料分析器	144...管理站

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：