（此處由本局於收文時黏貼條碼）

發明專利說明書 200529016

（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：93138304

※ 申請日期：93.12.10 ※IPC 分類：G06F 17/30

一、發明名稱：（中文/英文）

保證資料錄集之完整性的方法

METHOD FOR ENSURING THE INTEGRITY OF A DATA RECORD SET

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

諾基亞股份有限公司

NOKIA CORPORATION

代表人：（中文/英文）福克約翰遜（Folke Johansson）

住居所或營業所地址：（中文/英文）

芬蘭艾斯甫 FIN-02150 凱拉拉登迪 4

Keilalahdentie 4, FIN-02150 Espoo, Finland

國　籍：（中文/英文）芬蘭/FI

三、發明人：（共 2 人）

姓　名：（中文/英文）

1 馬卡斯米丁寧/MARKUS MIETTINEN

2 奇摩哈都寧/KIMMO HATONEN

國　籍：（中文/英文）

1~2 芬蘭/FI

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：

芬蘭　2003/12/18　20031856

☐ 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】

本發明係關於一種可保證儲存於資料庫或類似資料儲存器之資料錄之完整性之方法，系統及電腦程式。

【先前技術】

許多電腦化應用程式會產生大量資料以供儲存。一般上電腦化應用程式之事件係被記錄於一日誌檔案。日誌檔案係系統操作者，軟體研發者，保安人員及其他多種組別之資訊之其中一種最重要來源。

傳統上日誌資料檔案係以順序方式被寫入日誌檔案中。大多數日誌檔案之類型之基本元素係日誌記錄，通常係以日誌檔案中之行(rows)予以代表。非常重要的是日誌檔案之結構及內容必須保持可鑑定性。尤其是保安監視方面在沒有管理者知會所作變更之情況下，無論如何該行不可被變更或刪除。

時至今日已有多種習知方法以保證日誌檔案之完整性。舉例而言，可利用訊息鑑定碼(MAC)或數碼標記以連結各日誌檔案之密碼。一旦檔案內容改變，數碼標記或鑑定碼將會改變，於是可檢測到繼後之非授權性變更。然而，在數碼標記或另一種鑑定碼被指定於欲受保護之檔案之前，該等方法無法保護其完整性。

然而，在多數應用程式中需要予以儲存之資料量很大。因此，有需要將日誌資料或類似資料儲存於相關之資料庫中。在此有關完整性保護之課題有所不同。資料

庫之資料係被儲存於具有所謂記錄之包含屬性值所組成之元組之列表中。一般上日誌輸入係被儲存於一資料庫中以供各日誌行對應於特定資料庫表之記錄。

相關資料庫中之完整性保護在傳統上係取決於限制資料庫用戶之存取權限，使非授權性用戶無法變更資料庫內容。利用相關之資料庫管理系統(RDBMS)可加強存取控制。保證資料庫之完整性之另一方法係將它存入磁碟檔案中並附加上述之密碼。

此項方法通常並不實用，因多數資料庫表之本質係屬動態，必須經常予以更新。例如在一日誌資料庫中，一天中所產生之日誌輸入必須被置入對應之資料庫表中，諸如銀行交易等欲予儲存之資料量很大。僅有在確定該表之內容不再需要新之情況下，凍結資料庫表內容及以加密碼核對和保護其完整性才會有效用。在一日誌資料庫中，此舉表示必須使用每天之資料庫表以儲存資訊。該種方法之一缺點在於存取數天份資料之查詢必須作成數個表搜索以執行查詢作業。

美國專利案第 5978475 號(Schneier 等人)揭示一種日誌檔案之完整性之驗證方法。然而該項專利並未揭述任何有關將資料設置於資料庫中以供管理者全權變更資料錄中之資料之方法。

傳統方式之最大缺失在於，當使用資料庫系統而資料庫管理者無法完全予以信任之情況下，無法進行設定。在多數 RDBM 系統中，資料庫管理者(DBA)幾近具

有無限制性權限以更改資料庫及其內容。任何置入資料庫之資料，既使是在加密保護以防未授權性變更之資料之前，均可被存心不良之管理者予以更改。

先行技術之重大缺失在於對資料庫之存取權限之控制問題。另一項缺失在於資料無法被儲存於檔案中以進行數碼標記作為任何時間之檔案變更。第三項缺失在於資料庫管理者必須可信任。時至今日，管理者一般上係一技術人員，他實際上甚至不需知道被儲存於資料庫中之資訊。因此有需要一種方法可供多人觀視及檢查資料庫之內容之完整性，同時具有將資料儲存於資料庫中之存取權限。

【發明內容】

本發明揭示一種可保證資料庫系統中之資料完整性之方法。本發明所揭示之方法具有公開觀看之資料庫，具有可用作完整性驗證之公開完整性核對和。根據本發明，完整性核對和係從欲儲存之資料之加密方法，前項資料錄之核對和及一儲存鍵而計算得出。儲存鍵僅用於具有核准可將資料標記於資料庫上之實體。標記實體應與資料庫管理者不同。其中一項解決方法係使用公用鍵加密，其中標記實體使用其私人按鍵以計算完整性核對和，而願意進行驗證者將使用其公用按鍵以進行驗證。所計算之完整性核對和將被附在資料錄上。第一資料錄係所產生之初始錄集或係用以計算其本身核對和所需之前所同意之前項核對和。在驗證中係以類似方式計算完

整性核對和，並用以比對附在特定資料錄上之前項計算之核對和。

本發明之效益在於可提供鑑定性資料庫之完整性檢查。根據本發明之方法，資料庫可予以標記使只有經過標記授權者可更改資料庫之內容。根據本發明，在未破解所計算之完整性核對和之情況下，無論如何均無法刪除或變更儲存在資料庫中之資料錄。

【實施方式】

以下附圖係用以進一步說明本發明並作為本說明書之一部份，本發明之實施例連同說明可使本發明之原理更趨明晰。

以下將參照附圖之實施例詳細說明本發明。

第 1 圖係用以說明本發明之完整性驗證基本原理之流程圖。如第 1 圖所示，輸入資料可以任何適當格式予以接收。然而本發明最適用於當許多資料輸入以快速方式予以接收。適用之輸入包括諸如一般上儲存於大型資料庫之銀行交易之日誌檔案之資料錄等。該日誌檔案必須為可鑑定性，同時必須包含每一事件，視需要可作為法庭認可。

如第 1 圖所示，資料係抵達標記實體 10。標記實體 10 具有其本身之授權管理者以進行資料錄之標記。標記之型式包括數碼標記，加密，或單向雜湊(hash)。本文中之標記係代表計算核對和及將所計算之核對和附在資料錄之程序。其後之標記鍵係指任何類型之標記鍵之可

作為儲存鍵者。另一方面，可使用傳統公用鍵加密方法以供加入標記者之姓名於各個標記記錄中。該鍵可用類似保安郵寄系統之方法設置於系統中，其中該鍵包括一秘密鍵檔案及鍵入加密裝置中之密碼部份。該鍵亦可用智慧卡等類似裝置予以嵌設。

本發明之方法係以從資料錄所計算之完整性核對和，前項資料錄之完整性核對和及儲存鍵標記於各個資料錄上。然後將所計算之完整性核對和附在資料錄上。可附在資料錄本身或具有完整性核對和之個別欄位之資料庫 11 上。因計算完整性核對和係取決於前項完整性核對和，因此在未破解完整性之情況下無法從資料錄之中間去除一或多行，因需要完整性核對和之完整連結以供驗證。具有完整性核對和之標記資料將被儲存在資料庫 11。資料庫管理者將進行多項工作以儲存資料，但他無法更改資料內容或私下刪除資料錄。

隨後之資料錄之完整性之驗證係以類似標記之方式予以進行。驗證實體 12 將根據欲予標記之資料錄，前項完整性核對和及儲存鍵以計算完整性核對和。以所計算之完整性核對和比對儲存在資料庫 11 之核對和。如果該二核對和不相等，表示資料庫已經被更改而不被鑑定。此項方法之優點在於不需檢視整個資料庫之完整性即可快速檢查資料錄之完整性。可在連續性資料錄流之任何一點開始進行驗證。須知從前項完整性核對和所搜尋之資料錄之驗證無法獲得保證。因此，必須經由搜尋在欲

驗證之資料錄之前之資料錄之完整性核對和以啟始驗證程序。

如果係採用公用鍵加密以進行標記，標記授權者將用他的私人鍵以標記在標記實體 10 中之錄集。該鍵必須產生以標記特定資料庫及與具有授權標記之信任團體共享。在完整性之驗證中，標記授權者之公用鍵係用於作為核對和之解密。

有不同方式以啟動資料庫。由於不存在前項完整性核對和，可使用啟動向量以取代資料庫第一行之前項完整性核對和。第一行包括實際資料或與啟動相關之資料。例如啟動向量包括諸如日期等與啟動相關之資訊，及作為核對和之負責人之數碼標記。於是第一實際資料錄集將有前項核對和。啟動向量或行亦可應用於資料庫之中間以供將資料設入區塊中。將資料設入區塊將不會更改驗證程序。

第 2 圖係用以說明一資料錄之儲存實施例之流程圖。在步驟 20 中，係從任何適當資訊系統接收資料。該資料係與第 1 圖所示之實施例者類似。接收資料後，在步驟 21 中計算完整性核對和。可用如第 1 圖所示之實施例中所揭述之預期之習知方法計算完整性核對和。完整性核對和係根據前項核對和予以計算，即附在前項資料錄之核對和，欲予標記之資料及儲存鍵。只有被授權以標記資料錄者知道該儲存鍵。從標記裝置之記憶體中讀取前項核對和。如果完整性核對和係經常從一資料庫中

讀取，由於完整性核對和之連結不會被破解，心存不良之資料庫管理者將可毫無困難地刪除完整性之最後一行。亦有其他方式以保證最後一行之鑑定性，例如以一執行序號作為核對和參數之一部份。

如步驟 22 所示，係將所計算之完整性核對和附在資料錄而完成資料錄之標記。經過標記之資料將被儲存在資料庫。該資料庫可具有個別之欄位予資料及完整性核對和。該資料庫亦可具有附加之資訊欄作為計算完整性核對之用，例如標記者之姓名等。在將資料儲存於資料庫之後，將完整性核對和儲存於標記裝置之記憶體中，如步驟 24 所示。此舉係用以保證繼後使用之前項完整性核對和一旦經過計算後將不會變更。

第 3 圖係本發明之一實施例之區塊圖。在第 3 圖中所有組件係被分開說明，但精於此藝者當知該組件亦可以電腦程式之形式予以實施。該系統係根據第 2 圖所示之方法操作。因此其功能性將不再詳細說明。

本發明之系統具有一資料源 30，一標記實體 31，一資料庫 32，一資料庫管理控制台 33 及一驗證實體 34。資料源 30 係可產生需要儲存在資料庫 32 之資料之任何資訊系統。標記實體 31 係諸如在連接至資料庫系統 32 之電腦上執行之電腦程式或在資料庫系統 32 中之程式模組。資料庫 32 及資料庫管理控制台 33 係任何通用之資料庫系統，包括 Oracle 資料庫系統等。驗證實體 34 係與標記實體 31 類似。如果使用公用鍵設施，標記實體

31 具有秘密鍵而驗證實體 34 具有對應之公用鍵。

在精進之技術下，精於此藝者當可以多種方式實施本發明之基本概念。此而本發明及其實施例不受限於上述之實施例；在申請專利範圍下可進行變更。

【圖式簡單說明】

第 1 圖係用以說明本發明之完整性驗證基本原理之流程圖，

第 2 圖係用以說明本發明之資料錄之儲存實施例之流程圖，

第 3 圖係第 2 圖所示系統之一實施例之區塊圖。

【主要元件符號說明】

10　標記實體

11　資料庫

12　驗證實體

30　資料源

31　標記實體

32　資料庫

33　資料庫管理控制台

34　驗證實體

五、中文發明摘要：

本發明揭示一種將資料儲存於一資料庫，而該資料庫之完整性及鑑定性可在繼後予以驗證之方法，系統及電腦程式。根據本發明，資料錄(data record)係以一核對和予以標記，該核對和係從前項核對和，待儲存之資料錄及一儲存鍵所計算。

六、英文發明摘要：

The invention discloses a method, a system and a computer program for storing data on a database in a manner that the integrity and authenticity of the database can be verified later. According to the invention a data record is signed with a checksum that is computed from the previous checksum, the data record to be stored and a storage key.

十、申請專利範圍：

1.一種將資料錄儲存於資料庫系統之方法，其中係利用一標記實體以進行資料錄之標記，該方法之步驟包括：

接收欲儲存於資料庫之資料錄；

搜尋具有在欲儲存之資料錄之前之資料錄之第一完整性核對和；

利用加密方法根據儲存鍵，所搜尋之第一完整性核對和及欲儲存之資料錄以計算欲儲存之資料錄之第二完整性核對和；及

將資料錄及第二完整性核對和儲存於資料庫。

2.如申請專利範圍第 1 項所述之方法，其中該儲存鍵係公用鍵設施之一秘密鍵。

3.如申請專利範圍第 1 項所述之方法，其中資料庫第一行之所搜尋之完整性核對和係所產生之啟動向量。

4.如申請專利範圍第 1 項所述之方法，其中資料庫第一行之所搜尋之完整性核對和係標記實體之數碼標記。

5.如申請專利範圍第 1 項所述之方法，其中第一完整性核對和係搜尋自標記實體之記憶體。

6.如申請專利範圍第 1 項所述之方法，其中第二完整性核對和係儲存在標記實體之記憶體中。

7.如申請專利範圍第 1 項所述之方法，其中該完整性核對和具有一執行序號。

8.一種用以驗證在資料庫之資料錄之完整性之方法，其中係利用一驗證實體以驗證資料錄之完整性，該方法之步驟包括：

從資料庫中搜尋欲驗證之資料錄；

從資料庫中搜尋欲驗證之資料錄之完整性核對和；

搜尋在所搜尋之資料錄之前之資料錄之第一完整性核對和；

根據所搜尋之資料錄，第一完整性核對和及儲存鍵以計算所搜尋之資料錄之第二完整性核對和；及

用第二完整性核對和比對欲驗證之資料錄之完整性核對和，其中如果欲驗證之資料錄之完整性核對和與第二完整性核對和相等時，該資料錄係被視為可鑑定性。

9.如申請專利範圍第 8 項所述之方法，其中該儲存鍵係公用鍵設施之一公用鍵。

10.如申請專利範圍第 8 項所述之方法，其中資料庫

第一行之所搜尋之完整性核對和係產生之啟動向量。

11.如申請專利範圍第 8 項所述之方法，其中資料庫第一行之所搜尋之完整性核對和係標記授權者之數碼標記。

12.如申請專利範圍第 8 項所述之方法，其中第一完整性核對和係搜尋自驗證實體之記憶體。

13.如申請專利範圍第 8 項所述之方法，其中第二完整性核對和係儲存於驗證實體之記憶體。

14.如申請專利範圍第 8 項所述之方法，其中該完整性核對和係包括執行序號。

15.一種將資料錄儲存於資料庫系統之系統，其中係利用一標記實體以進行資料錄之標記，及利用一驗證實體以進行資料錄之完整性之驗證，其中該系統包括：

用以儲存及提供標記資料之資料庫；

用以提供欲儲存於資料庫之資料錄之資料源；

用以標記具有根據資料錄，在欲予標記之資料錄之前之資料錄之完整性核對和及儲存鍵所計算之完整性核對和之資料庫中儲存之資料錄之標記實體；及

用以驗證具有根據資料錄，在欲予驗證之資料錄之

前之資料錄之完整性核對和及儲存鍵所計算之選擇資料錄之完整性，並比對所計算之完整性核對和與儲存在資料庫之完整性核對和之驗證實體。

16.如申請專利範圍第 15 項所述之系統，其中該標記實體及驗證實體係應用公用鍵設施以計算及驗證核對和。

17.一種將資料錄儲存於資料庫系統之電腦程式，其中該標記實體係用以進行資料錄之標記，其中該電腦程式在電腦中執行時係進行下列步驟：

接收欲儲存於資料庫之資料錄；

搜尋具有在欲儲存之資料錄之前之資料錄之第一完整性核對和；

利用加密方法根據儲存鍵，所搜尋之第一完整性核對和及欲儲存之資料錄以計算欲儲存之資料錄之第二完整性核對和；及

將資料錄及第二完整性核對和儲存於資料庫。

18.如申請專利範圍第 17 項所述之電腦程式，其中該儲存鍵係公用鍵設施之一秘密鍵。

19.如申請專利範圍第 17 項所述之電腦程式，其中資料庫第一行之所搜尋之完整性核對和係所產生之啟動

向量。

20.如申請專利範圍第 17 項所述之電腦程式，其中資料庫第一行之所搜尋之完整性核對和係標記實體之數碼標記。

21.如申請專利範圍第 17 項所述之電腦程式，其中第一完整性核對和係搜尋自標記實體之記憶體。

22.如申請專利範圍第 17 項所述之電腦程式，其中第二完整性核對和係儲存在標記實體之記憶體中。

23.如申請專利範圍第 17 項所述之電腦程式，其中該完整性核對和具有一執行序號。

24.一種用以驗證在資料庫之資料錄之完整性之電腦程式，其中該電腦程式在電腦中執行時係進行下列步驟：

從資料庫中搜尋欲驗證之資料錄；

從資料庫中搜尋欲驗證之資料錄之完整性核對和；

搜尋在所搜尋之資料錄之前之資料錄之第一完整性核對和；

根據所搜尋之資料錄，第一完整性核對和及儲存鍵以計算所搜尋之資料錄之第二完整性核對和；及

用第二完整性核對和比對欲驗證之資料錄之完整性核對和，其中如果欲驗證之資料錄之完整性核對和與第二完整性核對和相等時，該資料錄係被視為可鑑定性。

25.如申請專利範圍第 24 項所述之電腦程式，其中該儲存鍵係公用鍵設施之一秘密鍵。

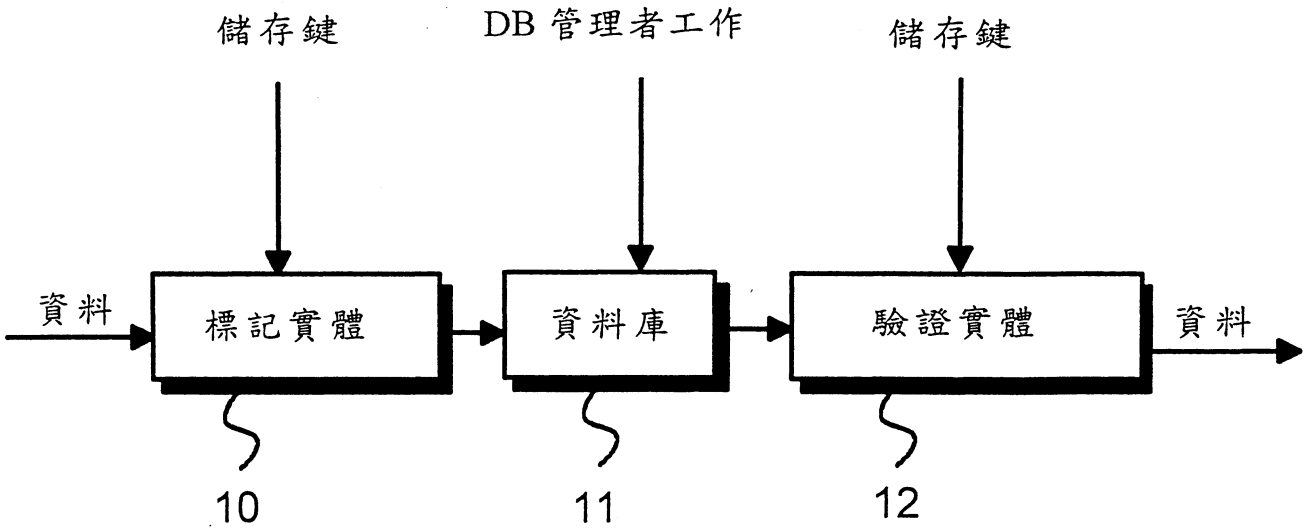
26.如申請專利範圍第 24 項所述之電腦程式，其中資料庫第一行之所搜尋之完整性核對和係所產生之啟動向量。

27.如申請專利範圍第 24 項所述之電腦程式，其中資料庫第一行之所搜尋之完整性核對和係標記實體之數碼標記。

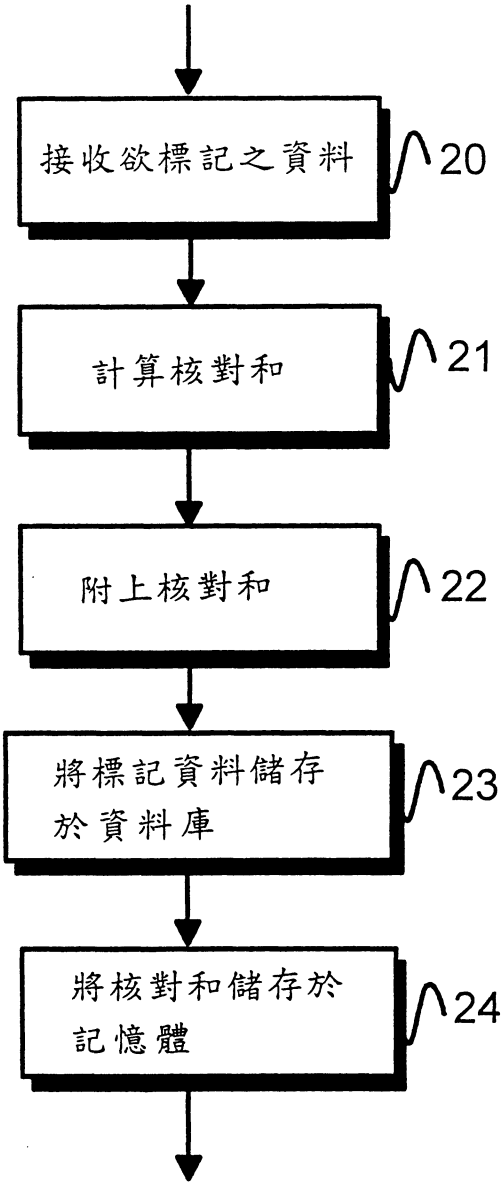
28.如申請專利範圍第 24 項所述之電腦程式，其中第一完整性核對和係搜尋自標記實體之記憶體。

29.如申請專利範圍第 24 項所述之電腦程式，其中第二完整性核對和係儲存在標記實體之記憶體中。

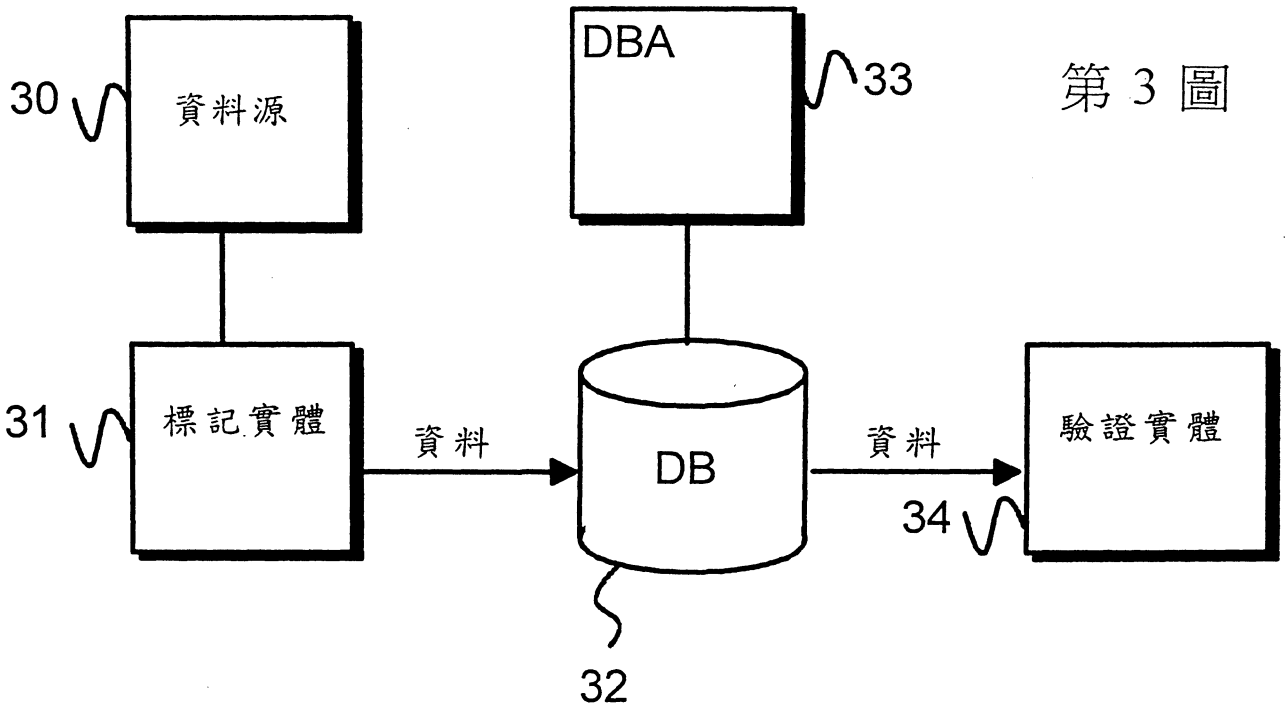
30.如申請專利範圍第 24 項所述之電腦程式，其中該完整性核對和具有一執行序號。



第 1 圖



第 2 圖



第 3 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:

10 標記實體

11 資料庫

12 驗證實體

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：