M599062

(19)中華民國智慧財產局

(12)新型說明書公告本　**(11)證書號數：TW M599062 U**

**(45)公告日： 中華民國 109 (2020) 年 07 月 21 日**

(21)申請案號：109203649　(22)申請日： 中華民國 109 (2020) 年 03 月 30 日

(51)Int. Cl.：　*H04L9/32　(2006.01)*　*G06Q10/06　(2012.01)*

(71)申請人：台北富邦商業銀行股份有限公司(中華民國) TAIPEI FUBON COMMERCIAL BANK CO., LTD.　(TW)

臺北市大安區仁愛路 4 段 169 號

(72)新型創作人：蕭明輝 HSIAO, MIN HUI (TW)；林世哲 LIN, SHIH CHE (TW)；李有倍 LEE, YU PEI (TW)；陳慧芳 CHEN, HUI FANG (TW)；張浩哲 CHANG, HAO CHE (TW)

(74)代理人：林育雅

(NOTE)備註： 相同的創作已於同日申請發明專利(Another patent application for invention in respect of the same creation has been filed on the same date)

申請專利範圍項數：10 項　　圖式數：4　　共 23 頁

(54)名稱

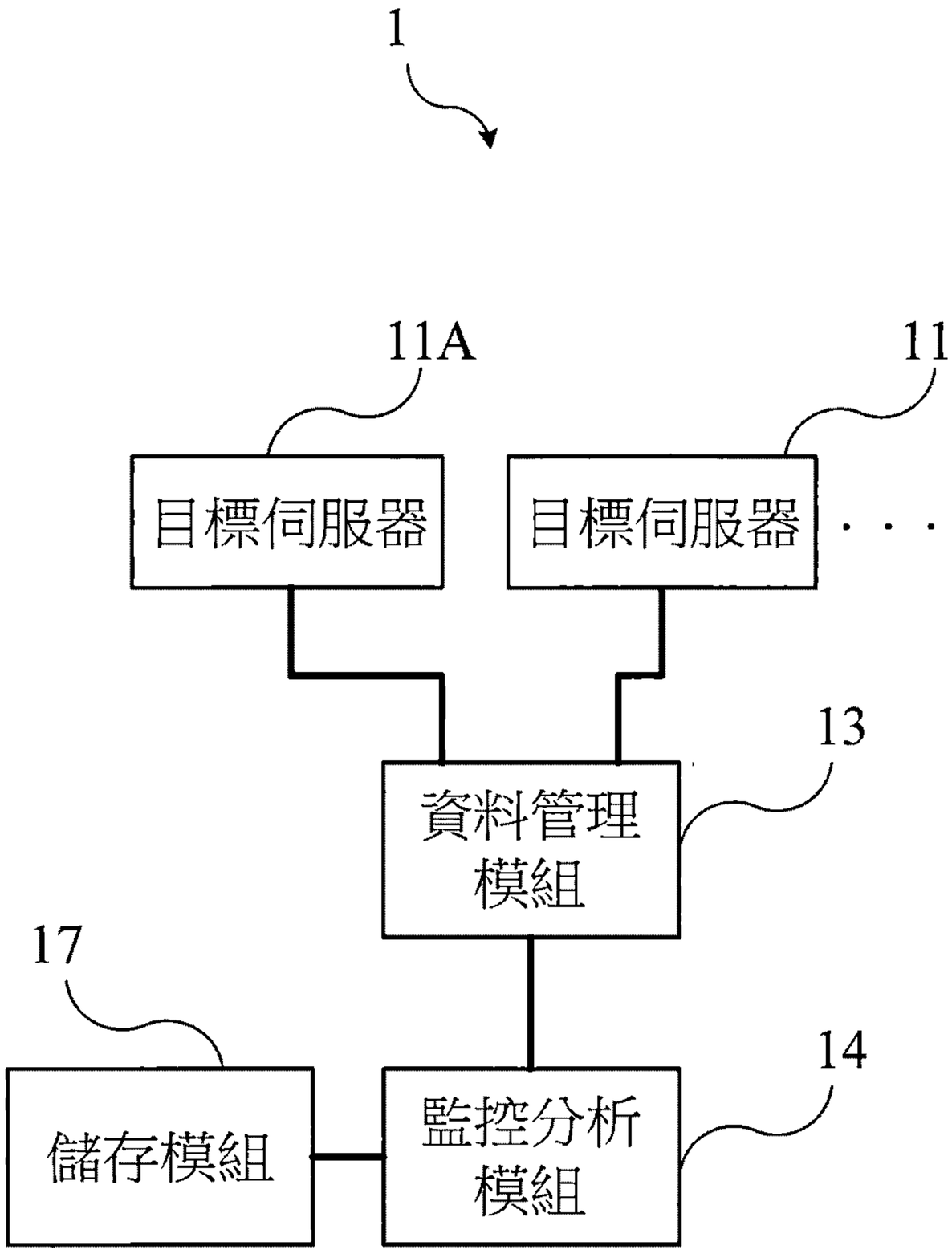
特權帳號管理系統

(57)摘要

本創作提供一種特權帳號管理系統，包含至少一目標伺服器、儲存模組、資料管理模組以及監控分析模組。目標伺服器包含伺服器資料及對應伺服器資料的至少一特權帳號。儲存模組用以儲存伺服器列表，並且伺服器列表包含所有目標伺服器的每一伺服器資料以及對應每一伺服器資料的至少一特權帳號。資料管理模組監控目標伺服器並建立特權帳號清單，並且於特定時間發送特權帳號清單。特權帳號清單包含目標伺服器的所有特權帳號。監控分析模組比對伺服器列表及特權帳號清單，並且選擇性地產生並發送警示訊號。

A privileged account management system includes at least one target server, a storing module, a data management module and a monitoring analysis module. The target server includes a server data and at least one privileged account corresponding to the server data. The storing module is configured for storing a server list, and the server list includes each server data of the target servers and the at least one privileged account corresponding to the server data. The data management module establishes a privileged account list by monitoring the target servers and sends the privileged account list at a specific time. The privileged account list includes all the privileged accounts of the target servers. The monitoring analysis module matches up between the server list and the privileged account list and selectively generates and sends a warning signal.

指定代表圖：




符號簡單說明：

1:特權帳號管理系統

11A、11B:目標伺服器

13:資料管理模組

14:監控分析模組

17:儲存模組

圖1

109年05月20日 所提修正

公告本

M599062

# 新型摘要

**【新型名稱】**（中文/英文）

特權帳號管理系統 / PRIVILEGED ACCOUNT MANAGEMENT SYSTEM

**【中文】**

本創作提供一種特權帳號管理系統，包含至少一目標伺服器、儲存模組、資料管理模組以及監控分析模組。目標伺服器包含伺服器資料及對應伺服器資料的至少一特權帳號。儲存模組用以儲存伺服器列表，並且伺服器列表包含所有目標伺服器的每一伺服器資料以及對應每一伺服器資料的至少一特權帳號。資料管理模組監控目標伺服器並建立特權帳號清單，並且於特定時間發送特權帳號清單。特權帳號清單包含目標伺服器的所有特權帳號。監控分析模組比對伺服器列表及特權帳號清單，並且選擇性地產生並發送警示訊號。

**【英文】**

A privileged account management system includes at least one target server, a storing module, a data management module and a monitoring analysis module. The target server includes a server data and at least one privileged account corresponding to the server data. The storing module is configured for storing a server list, and the server list includes each server data of the target servers and the at least one privileged account corresponding to the server data. The data management module establishes a privileged account list by monitoring the target servers and sends the privileged account list at a specific time. The privileged account list includes all the privileged accounts of the target

servers. The monitoring analysis module matches up between the server list and the privileged account list and selectively generates and sends a warning signal.

【代表圖】

【本案指定代表圖】：圖1

【本代表圖之符號簡單說明】：

1：特權帳號管理系統

11A、11B：目標伺服器

13：資料管理模組

14：監控分析模組

17：儲存模組

# 新型專利說明書

（本說明書格式、順序，請勿任意更動）

**【新型名稱】（中文/英文）**

特權帳號管理系統/ PRIVILEGED ACCOUNT MANAGEMENT SYSTEM

**【技術領域】**

【0001】 本創作關於一種帳號管理系統，並且特別地，關於一種可提升資料安全的特權帳號管理系統。

**【先前技術】**

【0002】 在這個網路通訊快速、資料傳輸便利的時代，人們逐漸無法脫離網路，無論在商業交易、人際互動或生活形態，皆與網路息息相關，而企業內部電腦的資料溝通也可透過企業內部之網路進行傳輸。由於網路的便利性，許多資料都唾手可得，因此，企業必須建立取得資料或操作系統的權限，以限制與控管取得資料的人數，進而防止資料外洩。以銀行業為例，由於許多資料都包含客戶個人資料，因此如何保障客戶的個人資料外洩是重要的課題。另外，若系統未受到權限保護，則系統容易被提權受到攻擊。因此，通常企業都會建立特權帳號以控管資料並提升資料安全。

【0003】 然而，近年來惡意程式威脅日益嚴重，許多駭客入侵企業的防禦系統取得特權帳號進行提權而發動攻擊(如SWIFT駭客盜領事件、銀行ATM遭駭客攻擊吐鈔事件等)。因此，如何有效地管理特權帳號將是主要的問題之一。現行一般企業在提升管理特權帳號的方法中，係在企業的 伺服器以安裝應用程式或整合軟體的方式收集各伺服器的相關資訊後，再回傳到資安防禦系統進行比對分析以找出異常事件。但是，由於企業的伺服器

皆需安裝其他程式或軟體不僅提高成本也降低伺服器效能。

【0004】 因此，有必要研發一種特權帳號管理系統，以解決先前技術之問題。

## 【新型內容】

【0005】 有鑑於此，本創作之一範疇在於提供一種特權帳號管理系統，可降低成本並且可有效地提高資料安全。

【0006】 根據本創作之一具體實施例，特權帳號管理系統包含至少一目標伺服器、儲存模組、資料管理模組以及監控分析模組。至少一目標伺服器儲存至少一特權帳號，其中每一目標伺服器包含伺服器資料以及對應伺服器資料的至少一特權帳號。儲存模組用以儲存伺服器列表，其中伺服器列表包含所有目標伺服器的每一目標伺服器資料以及對應每一目標伺服器資料的每一特權帳號。資料管理模組耦接至少一目標伺服器。資料管理模組用以監控目標伺服器並建立特權帳號清單，並且於至少一特定時間發送特權帳號清單。特權帳號清單包含目標伺服器的所有特權帳號。監控分析模組耦接儲存模組以及資料管理模組。監控分析模組用以接收特權帳號清單並且比對伺服器列表以及特權帳號清單。當伺服器列表與特權帳號清單不符時，監控分析模組產生並發送警示訊號。

【0007】 其中，至少一特權帳號包含第一特權帳號。當特權帳號清單包含對應目標伺服器的第一特權帳號並且伺服器列表不包含對應目標伺服器的第一特權帳號時，監控分析模組產生並發送警示訊號。

【0008】 其中，至少一特權帳號包含第一特權帳號。當伺服器列表包含對應目標伺服器的第一特權帳號並且特權帳號清單不包含對應目標伺服

器的第一特權帳號時，監控分析模組產生並發送警示訊號。

【0009】 其中，特權帳號管理系統進一步包含收發模組，耦接至少一目標伺服器以及監控分析模組。收發模組用以回收對應特權帳號的特權帳號密碼。當收發模組於該特定時間所回收的特權帳號密碼所對應的特權帳號與伺服器列表不符時，監控分析模組產生並發送警示訊號。

【0010】 進一步地，至少一特定時間包含第一特定時間，至少一特權帳號包含第一特權帳號，並且第一特權帳號包含第一特定時間。當收發模組於第一特定時間未回收對應第一特權帳號的特權帳號密碼並且伺服器列表包含第一特權帳號時，監控分析模組產生並發送警示訊號。

【0011】 其中，特權帳號管理系統進一步包含申請模組，耦接收發模組以及監控分析模組。申請模組用以發送申請訊息至收發模組。申請訊息包含至少一目標伺服器資料以及對應至少一目標伺服器資料的至少一特權帳號。當申請訊息與伺服器列表不符時，監控分析模組產生並發送警示訊號。

【0012】 進一步地，申請訊息包含第二目標伺服器資料以及第二特權帳號資料。當伺服器列表不包含第二目標伺服器資料時，收發模組建立第二目標伺服器資料以及對應第二目標伺服器資料的第二特權帳號資料於伺服器列表中。

【0013】 其中，特權帳號管理系統進一步包含顯示模組耦接監控分析模組。顯示模組用以接收並顯示監控分析模組所發送的警示訊號。

【0014】 其中，資料管理模組為系統中心配置管理器(System Center Configuration Manager，SCCM)。

【0015】 其中，收發模組、監控分析模組以及儲存模組整合於伺服器中。

【0016】 綜上所述，本創作之特權帳號管理系統可根據多種資料源交叉比對以準確地判斷未授權的特權帳號，進而提升資料安全。並且可藉由整合式的管理器取得各伺服器的特權帳號資料，而不需在各伺服器安裝其他相關整合及資料安全防禦軟體，進而降低成本並提高伺服器效能。

## 【圖式簡單說明】

【0017】

圖1係繪示根據本創作之一具體實施例之特權帳號管理系統的功能方塊圖。

圖2係繪示根據本創作之另一具體實施例之特權帳號管理系統的功能方塊圖。

圖3係繪示根據本創作之又一具體實施例之特權帳號管理系統的功能方塊圖。

圖4係繪示根據本創作之又一具體實施例之特權帳號管理系統的功能方塊圖。

## 【實施方式】

【0018】 為了讓本創作的優點，精神與特徵可以更容易且明確地了解，後續將以具體實施例並參照所附圖式進行詳述與討論。值得注意的是，這些具體實施例僅為本創作代表性的具體實施例，其中所舉例的特定方法、裝置、條件、材質等並非用以限定本創作或對應的具體實施例。又，圖中各裝置僅係用於表達其相對位置且未按其實際比例繪述，合先敘明。

【0019】 在本公開的各種實施例中，表述“或”包括同時列出的文字的任何組合或所有組合。例如，表述“A或B”可包括A、可包括B或可包括A和B二者。此外，本創作裝置或元件前的不定冠詞“一”、“一種”和“一個”對裝置或元件的數量要求(即出現次數)無限制性。因此“一”應被解讀為包括一或至少一，並且單數形式的裝置或元件也包括複數形式，除非所述數量明顯指單數形式。

【0020】 在本說明書的描述中，參考術語“一具體實施例”、“另一具體實施例”或“部分具體實施例”等的描述意指結合該實施例描述的具體特徵、結構、材料或者特點包含於本創作的至少一個實施例中。在本說明書中，對上述術語的示意性表述不一定指的是相同的實施例。而且，描述的具體特徵、結構、材料或者特點可以在任何的一個或多個實施例中以合適的方式結合。

【0021】 請參考圖1，圖1係繪示根據本創作之一具體實施例之特權帳號管理系統1的功能方塊圖。在本具體實施例中，特權帳號管理系統1包含目標伺服器11A及11B、儲存模組17、資料管理模組13以及監控分析模組14。目標伺服器11A及11B耦接資料管理模組13，並且監控分析模組14耦接資料管理模組13以及儲存模組17。於實務中，特權帳號管理系統1可應用於企業的資料安全管理。監控分析模組14以及儲存模組17可運作於一電腦主機(如：伺服器)中，並且目標伺服器11A及11B可以有線的或無線的連接於電腦主機中的資料管理模組13。請注意，圖1中的目標伺服器的數量不限於2個，也可為1個或3個以上。

【0022】 在本具體實施例中，目標伺服器11A包含伺服器資料以及對

應伺服器資料的至少一特權帳號。於實務中，目標伺服器11A可為工業電腦，並且可為企業待管理的資料庫、系統、線上平台的伺服器等。伺服器資料為可用以辨識目標伺服器11A的資料(如：電腦IP位置、電腦編號等)。特權帳號可為系統或資料庫等的最高權限帳號，並且特權帳號可為檔案的形式。舉例來說，當特權帳號管理系統1應用於銀行業時，目標伺服器11A可為金融資料庫，特權帳號為資料庫伺服器的最高權限帳號。請注意，目標伺服器11B的功能與目標伺服器11A的功能大致上相同，於此不再贅述。進一步地，當目標伺服器的數量為3個以上時，各目標伺服器的功能皆與目標伺服器11A的功能大致上相同。

【0023】 在本具體實施例中，儲存模組17用以儲存伺服器列表，其中伺服器列表包含所有目標伺服器的每一目標伺服器資料以及對應每一目標伺服器資料的至少一特權帳號。於實務中，儲存模組17可為硬碟、外接式硬碟等。伺服器列表可包含目標伺服器11A中的伺服器資料以及對應的特權帳號，以及目標伺服器11B中的伺服器資料以及對應的特權帳號。而伺服器列表可以預存或匯入的方式儲存於儲存模組17中。舉例來說，當企業的伺服器上架或現有的伺服器運作時，特權帳號的管理人員可先將所有已上架和現有的伺服器的伺服器資料以及對應伺服器的特權帳號儲存於儲存模組17中。

【0024】 在本具體實施例中，資料管理模組13監控目標伺服器11A及11B並建立特權帳號清單，而特權帳號清單包含目標伺服器11A及11B的所有特權帳號。於實務中，資料管理模組13可建立於運算晶片中或可為應用程式並且可辨識出特權帳號。資料管理模組13可判斷及得知位於目標伺服

器11A的所有特權帳號及目標伺服器11B的所有特權帳號。在一具體實施例中，資料管理模組13為系統中心配置管理器(System Center Configuration Manager，SCCM)。由於伺服器資料除了可為前述的電腦IP位置及電腦編號之外，也可包含作業系統資料(如：Windows作業系統)。於實務中，當目標伺服器11A與目標伺服器11B皆為Windows作業系統時，Windows系統中的SCCM可直接監控並得知目標伺服器11A及目標伺服器11B的特權帳號以建立特權帳號清單。請注意，資料管理模組13不限於SCCM，也可為其他任何可建立特權帳號清單的功能的管理器。因此，本創作的特權帳號管理系統1可直接得知伺服器的特權帳號，而不需在各伺服器額外安裝資料安全軟體，以提高伺服器的運作能力並且減少伺服器的負擔，進而以降低成本並提高伺服器效能。

【0025】 進一步地，資料管理模組13可於至少一特定時間發送特權帳號清單至監控分析模組14。於實務中，資料管理模組13可定期回報目標伺服器11A及11B中的特權帳號，以監控每一個目標伺服器的特權帳號使用情形。而特定時間可預存於資料管理模組13中，並且可根據需求而設定。舉例來說，特定時間可設定為每日的下午六點，因此，資料管理模組13可於每日的下午六點將特權帳號清單傳送至監控分析模組14。

【0026】 在本具體實施例中，當監控分析模組14接收到資料管理模組13所發送的特權帳號清單後，監控分析模組14比對資料管理模組13所建立的特權帳號清單以及儲存於儲存模組17中的伺服器列表。於實務中，監控分析模組14可建立於運算晶片中。監控分析模組14可藉由比對特權帳號清單以及伺服器列表判斷出各目標伺服器11A及11B是否有異常且未授權的特

權帳號，並且根據判斷結果產生並發送警示訊號。進一步地，特權帳號管理人員可根據警示訊號採取相對應的資安防護處理，進而提升資料安全。

【0027】 在一具體實施例中，當特權帳號清單包含對應目標伺服器11A的第一特權帳號，並且伺服器列表不包含對應目標伺服器11A的第一特權帳號時，監控分析模組14產生並發送警示訊號。於實務中，當資料管理模組13找到伺服器列表沒有紀錄的第一特權帳號時，也就是說，第一特權帳號不為目標伺服器原有的特權帳號，並且也不為企業的特權帳號管理人員於目標伺服器上架時所建立的帳號。換句話說，第一特權帳號有可能為駭客入侵目標伺服器11A所建立的未授權的特權帳號。進一步地，企業的特權帳號管理人員可根據監控分析模組14所發送警示訊息將此帳號自目標伺服器刪除，以提升企業的安全性。

【0028】 在一具體實施例中，當伺服器列表包含對應目標伺服器11A的第一特權帳號，並且特權帳號清單不包含對應目標伺服器11A的第一特權帳號時，監控分析模組14產生並發送警示訊號。於實務中，當資料管理模組13所發送的特權帳號清單不包含第一特權帳號時，也就是說，第一特權帳號已不存在。換句話說，目標伺服器11A可能已經下架，因此資料管理模組13無法取得第一特權帳號。然而，由於儲存模組17中的伺服器列表仍包含對應目標伺服器11A的第一特權帳號的資料，因此企業的特權帳號管理人員可根據監控分析模組14所發送警示訊息更新儲存模組17中的伺服器列表，以確實掌控企業所有特權帳號的流動。因此，特權帳號管理系統1可根據特權帳號清單以及伺服器列表自動判斷出異常的特權帳號，進而提升企業的安全管理效率。

【0029】 請參考圖2。圖2係繪示根據本創作之另一具體實施例之特權帳號管理系統1的功能方塊圖。本具體實施例與前述的具體實施例的不同之處，係在於本具體實施例的特權帳號管理系統1進一步包含收發模組12。收發模組12耦接目標伺服器11A及11B，並且耦接監控分析模組14。收發模組12用以回收對應特權帳號的特權帳號密碼。當收發模組12於特定時間所回收的特權帳號密碼所對應的特權帳號與伺服器列表不符時，監控分析模組14產生並發送警示訊號。於實務中，收發模組12可為資料傳輸晶片。收發模組12可在特定時間(如：下午6點)回收所有企業人員所申用的特權帳號的特權帳號密碼。而回收特權帳號密碼的方式可為變更密碼的形式，但不限於此。當收發模組12未回收對應特權帳號的特權帳號密碼時，即表示收回對應特權帳號的特權帳號密碼未執行變更，此時，企業的特權帳號管理人員可根據監控分析模組14所發送警示訊息將對應特權帳號的特權帳號密碼進行密碼變更，以控管及避免特權帳號的濫用。因此，特權帳號管理系統1也可透過收發模組12有效地管理特權帳號，提升企業的資料安全。

【0030】 而收發模組12所回收的對應特權帳號的特權帳號密碼除了可與儲存模組17中的伺服器列表分析與比對之外，也可與資料管理模組13所發送的特權帳號清單進行分析與比對。在一具體實施例中，收發模組12回收對應特權帳號的特權帳號密碼的同時，也根據特權帳號密碼所對應的特權帳號產生申用記錄。當資料管理模組13所發送的特權帳號清單與收發模組12的申用記錄不符時，監控分析模組14產生並發送警示訊號。舉例來說，當資料管理模組13所發送的特權帳號清單中，目標伺服器11A的使用紀錄包含第一特權帳號並且收發模組12所產生的申用記錄中不包含對應目標

伺服器11A的第一特權帳號時，也就是說，第一特權帳號並未行正常授權申用。企業的特權帳號管理人員可根據監控分析模組14所產生並發送的警示訊號尋找第一特權帳號的歷史紀錄。因此，特權帳號管理系統1可根據特權帳號清單以及回收的特權帳號密碼自動判斷出異常的特權帳號，以有效地管理企業的特權帳號，進而提升企業的安全管理效率。

【0031】 而前述的特定時間可為收發模組12回收特權帳號的時間，也可為回收各特權帳號的依據。在一具體實施例中，目標伺服器11A的第一特權帳號包含第一特定時間，當收發模組12於該第一特定時間未回收對應第一特權帳號的特權帳號密碼並且伺服器列表包含第一特權帳號時，監控分析模組14產生該警示訊號。本具體實施例中的第一特定時間與前述的特定時間的不同之處係在於，前述的特定時間係為固定的時間點，並且收發模組12於固定的時間點回收所有特權帳號；而本具體實施例的第一特定時間係為第一特權帳號的使用時間，進一步地，多個特權帳號可分別包含不同的使用時間，因此，收發模組12可根據各特權帳號的使用時間回收特權帳號。於實務中，第一特定時間可為第一特權帳號的使用期限(如：3小時)，並且第一特定時間可預設於收發模組12中。因此，當收發模組12於3小時後未回收到第一特權帳號時，監控分析模組14產生警示訊號。因此，特權帳號管理系統1也可藉由特權帳號的時效性比對回收的特權帳號以及特權帳號清單以判斷異常特權帳號，進而提升資料安全。

【0032】 而本創作的特權帳號管理系統1也可進一步包含申請模組18。申請模組18耦接收發模組12及監控分析模組14，並且用以發送申請訊息至收發模組12。申請訊息包含至少一目標伺服器資料以及對應目標伺服

器的特權帳號。於實務中，申請模組18可為申請特權帳號的應用程式、系統或介面，並且申請模組18可整合於電腦或伺服器中。當企業人員需申用或申請新增目標伺服器11A的特權帳號時，申請模組18可發送包含目標伺服器11A的伺服器資料以及對應伺服器資料的特權帳號的申請訊息至收發模組12。而當申請訊息與伺服器列表不符時，監控分析模組14產生並發送警示訊號。

【0033】 在一具體實施例中，當申請訊息包含第二伺服器資料以及第二特權帳號，並且伺服器列表不包含第二伺服器資料以及第二特權帳號時，收發模組12建立第二伺服器資料以及對應第二伺服器資料的第二特權帳號於伺服器列表中。於實務中，當伺服器列表不包含第二伺服器資料時，也就是說，包含第二伺服器資料的第二伺服器不為現有的伺服器，因此，第二伺服器有可能是即將上架的伺服器，而申請訊息為伺服器管理人所新增申請的特權帳號。因此，企業的特權帳號管理人員可根據監控分析模組14所發送警示訊息確認即將上架的伺服器的訊息，以確實掌控企業所有的特權帳號。

【0034】 進一步地，監控分析模組14也可比對申請模組18所發送的申請訊息、儲存於儲存模組17的伺服器列表以及資料管理模組13所發送的特權帳號清單。在一具體實施例中，申請訊息以及伺服器列表包含目標伺服器11A的第一特權帳號，當特權帳號清單包含目標伺服器11A的第一特權帳號以及第二特權帳號，而伺服器列表不包含目標伺服器11A的第二特權帳號時，監控分析模組14產生並發送警示訊號。於實務中，當特權帳號清單包含第二特權帳號，但是伺服器列表不包含第二特權帳號時，也就是說，目

標伺服器11A中的第二特權帳號不為原有的而係新增的。然而，申請訊息中包含了目標伺服器11A的特權帳號申請紀錄。因此，特權帳號管理人員可根據監控分析模組14所產生並發送的警示訊息尋找申用目標伺服器11A的特權帳號的企業人員，進而判斷第二特權帳號建立的合法性。因此，特權帳號管理系統1可藉由多個資料來源進行交叉比對，進而提升企業資料安全。

【0035】 請繼續參考圖2。本具體實施例的特權帳號管理系統1進一步包含顯示模組15耦接監控分析模組14。顯示模組15用以接收並顯示監控分析模組14所發送的警示訊號。於實務中，警示訊號可為文字、圖像及聲音等，並且顯示模組15可為電腦螢幕、手機螢幕及可用以顯示的裝置。而監控分析模組14也可將未授權帳號、異常帳號數量顯示於顯示模組15，因此，特權帳號管理人員可透過顯示模組15所顯示的警示訊號進行後續的資安防護作業，以提升資料安全。

【0036】 請參考圖3，圖3係繪示根據本創作之又一具體實施例之特權帳號管理系統1的功能方塊圖。本具體實施例與先前具體實施例的不同之處係在於本具體實施例的特權帳號管理系統1中的收發模組161、監控分析模組162以及儲存模組163整合於伺服器16中。於實務中，伺服器16可為由特權帳號管理人員所管理的電腦主機。因此，特權帳號的建立、儲存及收發皆可集中管理，以提升資料安全。請注意，本具體實施例的收發模組161、監控分析模組162以及儲存模組163的功能與前述的具體實施例的收發模組、監控分析模組以及儲存模組的功能大致相同，於此不再贅述。請參考圖4，圖4係繪示根據本創作之又一具體實施例之特權帳號管理系統1的功能方塊圖。在本具體實施例中，特權帳號管理系統中的收發模組261、監控分

析模組262、儲存模組263以及顯示模組264整合於伺服器26中。請注意，本具體實施例的收發模組261、監控分析模組262、儲存模組263及顯示模組264的功能與前述的具體實施例的收發模組、監控分析模組、儲存模組及顯示模組的功能大致相同，於此不再贅述。

【0037】 綜上所述，本創作之特權帳號管理系統可根據多種資料源交叉比對以準確地判斷未授權的特權帳號，進而提升資料安全。並且可藉由整合式的管理器取得各伺服器的特權帳號資料，而不需在各伺服器安裝其他相關整合軟體，進而降低成本並提高伺服器效能。

【0038】 藉由以上較佳具體實施例之詳述，係希望能更加清楚描述本創作之特徵與精神，而並非以上述所揭露的較佳具體實施例來對本創作之範疇加以限制。相反地，其目的是希望能涵蓋各種改變及具相等性的安排於本創作所欲申請之專利範圍的範疇內。因此，本創作所申請之專利範圍的範疇應根據上述的說明作最寬廣的解釋，以致使其涵蓋所有可能的改變以及具相等性的安排。

【符號說明】

1：特權帳號管理系統

11A、11B：目標伺服器

12、161、261：收發模組

13：資料管理模組

14、162、262：監控分析模組

15、264：顯示模組

16、26：伺服器

17、163、263：儲存模組

18：申請模組

# 申請專利範圍

1. 一種特權帳號管理系統，其包含：

至少一目標伺服器，儲存至少一特權帳號，其中每一該目標伺服器包含一伺服器資料以及對應該伺服器資料的該至少一特權帳號；

一儲存模組，用以儲存一伺服器列表，其中該伺服器列表包含所有該目標伺服器的每一該目標伺服器資料以及對應每一該目標伺服器資料的該至少一特權帳號；

一資料管理模組，耦接該至少一目標伺服器，該資料管理模組用以監控該至少一目標伺服器並建立一特權帳號清單，並且於至少一特定時間發送該特權帳號清單，該特權帳號清單包含該至少一目標伺服器的所有特權帳號；以及

一監控分析模組，耦接該儲存模組以及該資料管理模組，該監控分析模組用以接收該特權帳號清單並且比對該伺服器列表以及該特權帳號清單，當該伺服器列表與該特權帳號清單不符時，該監控分析模組產生並發送一警示訊號。

2. 如申請專利範圍第1項所述之特權帳號管理系統，其中該至少一特權帳號包含一第一特權帳號，當該特權帳號清單包含對應該目標伺服器的該第一特權帳號並且該伺服器列表不包含對應該目標伺服器的該第一特權帳號時，該監控分析模組產生並發送該警示訊號。

3. 如申請專利範圍第1項所述之特權帳號管理系統，其中該至少一特權帳號包含一第一特權帳號，當該伺服器列表包含對應該目標伺服器的該第一特權帳號並且該特權帳號清單不包含對應該目標伺服器的該第一特權帳

號時，該監控分析模組產生並發送該警示訊號。

4. 如申請專利範圍第1項所述之特權帳號管理系統，進一步包含一收發模組，耦接該至少一目標伺服器以及該監控分析模組，該收發模組用以回收對應該至少一特權帳號的至少一特權帳號密碼，當收發模組於該特定時間所回收的該至少一特權帳號密碼與該伺服器列表不符時，該監控分析模組產生並發送該警示訊號。

5. 如申請專利範圍第4項所述之特權帳號管理系統，其中該至少一特定時間包含一第一特定時間，該至少一特權帳號包含一第一特權帳號，並且該第一特權帳號包含該第一特定時間，當該收發模組於該第一特定時間未回收對應該第一特權帳號的該至少一特權帳號密碼並且該伺服器列表包含該第一特權帳號時，該監控分析模組產生該警示訊號。

6. 如申請專利範圍第4項所述之特權帳號管理系統，進一步包含一申請模組，耦接該收發模組及該監控分析模組，該申請模組用以發送一申請訊息至該收發模組，該申請訊息包含該至少一目標伺服器資料以及對應該至少一目標伺服器資料的該至少一特權帳號，當該申請訊息與該伺服器列表不符時，該監控分析模組產生並發送該警示訊號。

7. 如申請專利範圍第6項所述之特權帳號管理系統，其中該申請訊息包含一第二伺服器資料以及一第二特權帳號，當該伺服器列表不包含該第二伺服器資料時，該收發模組建立該第二伺服器資料以及對應該第二伺服器資料的該第二特權帳號於該伺服器列表中。

8. 如申請專利範圍第1項所述之特權帳號管理系統，進一步包含一顯示模組耦接該監控分析模組，該顯示模組用

以接收並顯示該監控分析模組所發送的該警示訊號。

9. 如申請專利範圍第1項所述之特權帳號管理系統，其中該資料管理模組為系統中心配置管理器(System Center Configuration Manager，SCCM)。

10. 如申請專利範圍第4項所述之特權帳號管理系統，其中該收發模組、該監控分析模組以及該儲存模組整合於一伺服器中。

# 圖式

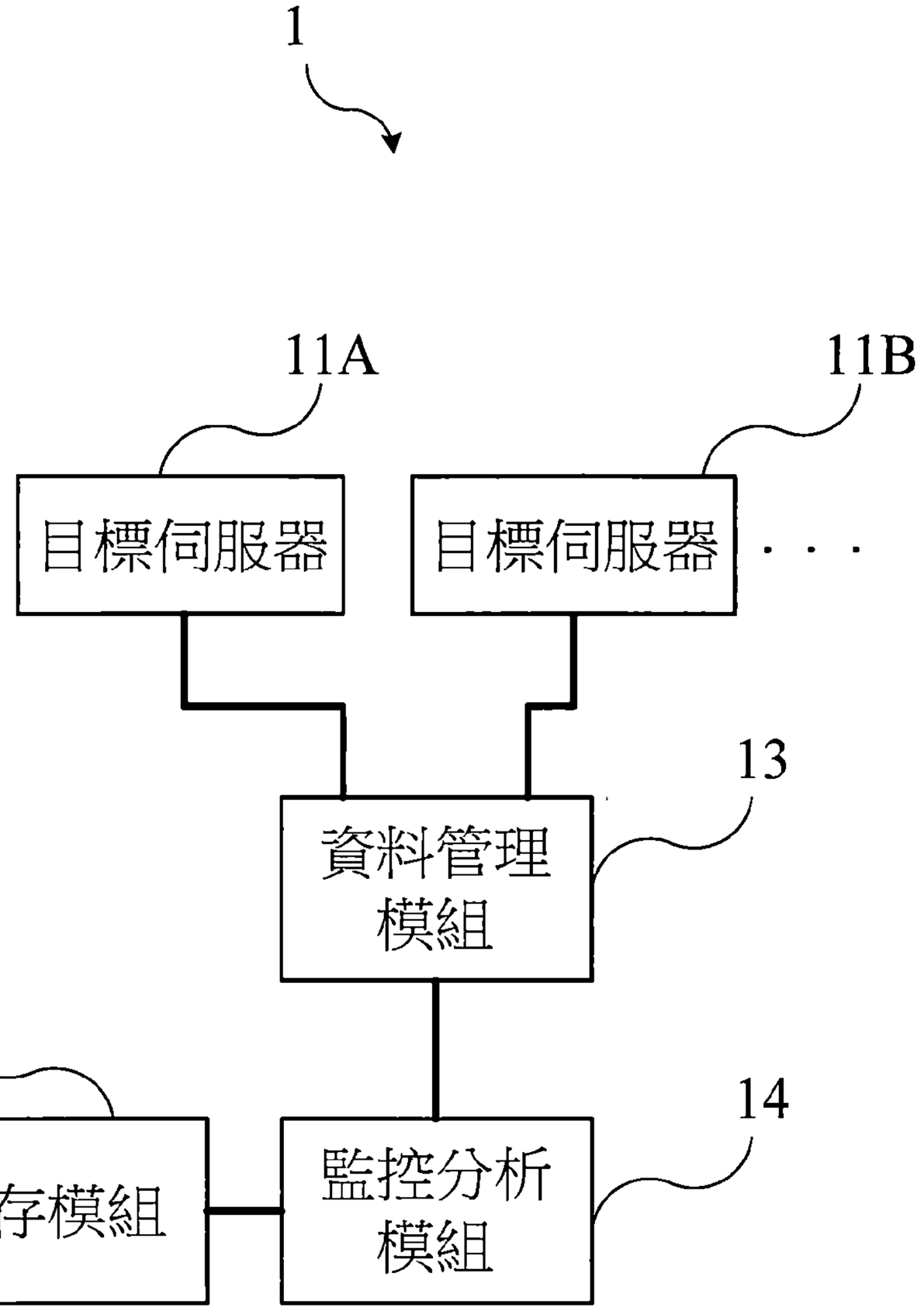



圖1

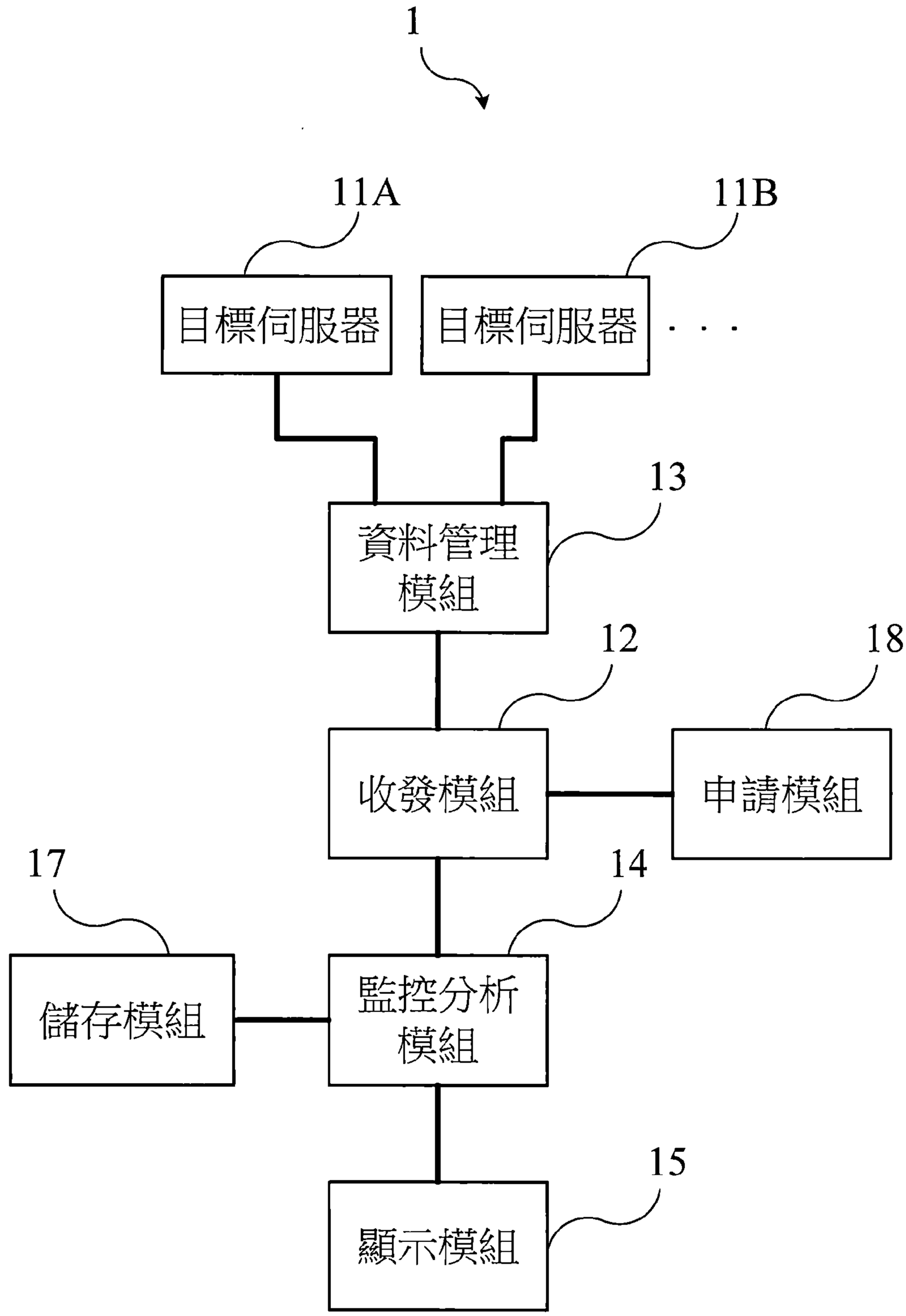

1
11A
11B
目標伺服器
目標伺服器
· · ·
13
資料管理
模組
12
18
收發模組
申請模組
17
14
儲存模組
監控分析
模組
15
顯示模組

圖2

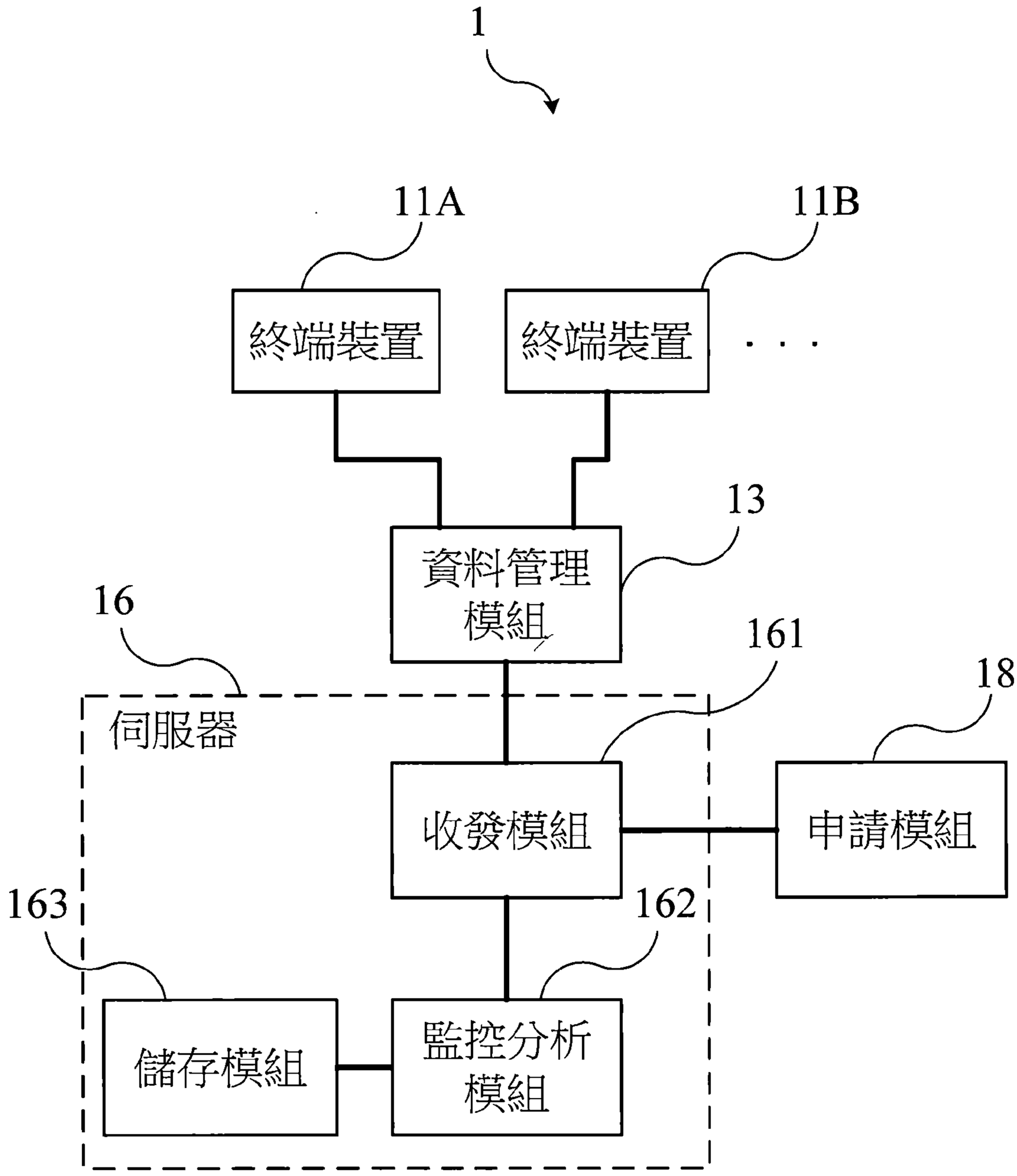

1
11A
11B
終端裝置
終端裝置
. . .
13
資料管理模組
16
161
18
伺服器
收發模組
申請模組
163
162
儲存模組
監控分析模組

圖3

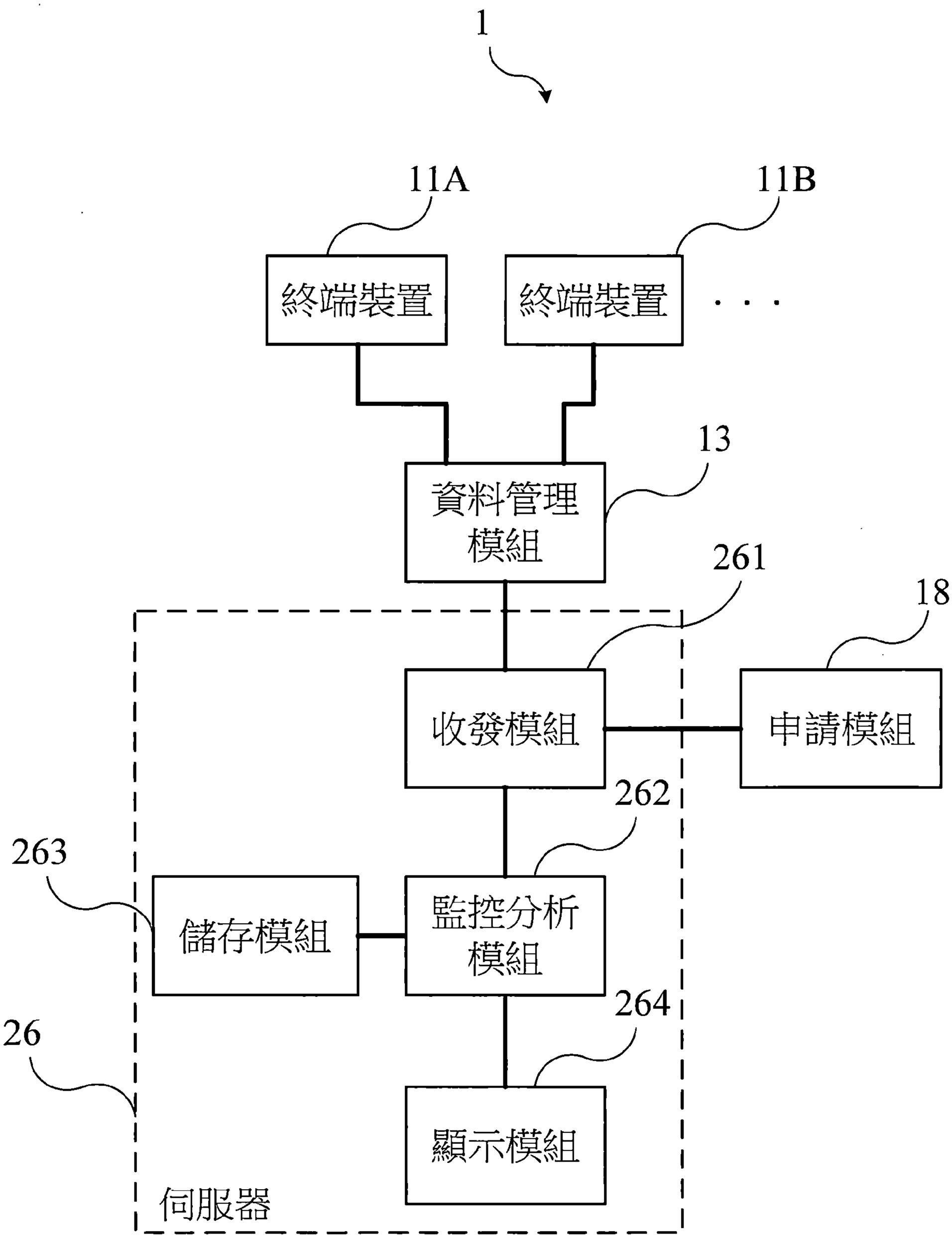

1
11A
11B
終端裝置
終端裝置
. . .
13
資料管理
模組
261
18
收發模組
申請模組
262
263
儲存模組
監控分析
模組
264
26
顯示模組
伺服器

圖4