發明專利說明書 200423677

（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：93106830

※ 申請日期：93.3.15　　※IPC 分類：H04L 9/32

壹、發明名稱：（中文/英文）

通信裝置及鑑認裝置

COMMUNICATION APPARATUS AND AUTHENTICATION APPARATUS

貳、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

松下電器產業股份有限公司

MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.

代表人：（中文/英文）

中村邦夫/ NAKAMURA, KUNIO

住居所或營業所地址：（中文/英文）

日本國大阪府門真市大字門真 1006 番地

1006, OAZA KADOMA, KADOMA-SHI, OSAKA, 571-8501 JAPAN

國　籍：（中文/英文）

日本 / JAPAN

參、發明人：（共 2 人）

姓　名：（中文/英文）

1. 吉田順二/ YOSHIDA, JUNJI
2. 濱井信二/ HAMAI, SHINJI

住居所地址：（中文/英文）

1. 日本國大阪府寢屋川市池田新町 5 番 17 號

   5-17, IKEDASHINMACHI, NEYAGAWA-SHI, OSAKA 572-0038 JAPAN

2. 日本國大阪府門真市三島 77 番 9 號

   77-9, MITSUSHIMA, KADOMA-SHI, OSAKA 571-0015 JAPAN

國　籍：（中文/英文）

日本 / JAPAN

肆、聲明事項：

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為： 年 月 日。

◎本案申請前已向下列國家（地區）申請專利 ☑ 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】

1.日本；2003,04,01；特願2003-098596

2.

3.

4.

5.

☐ 主張國內優先權(專利法第二十五條之一)：

【格式請依：申請日；申請案號數 順序註記】

1.

2.

☐ 主張專利法第二十六條微生物：

☐ 國內微生物 【格式請依：寄存機構；日期；號碼 順序註記】

☐ 國外微生物 【格式請依：寄存國名；機構；日期；號碼 順序註記】

☐ 熟習該項技術者易於獲得，不須寄存。

玖、發明說明：

【發明所屬之技術領域】

發明領域

本發明係有關於一種作為一面確認伺服器之正當性，一面從伺服器接受服務提供之用戶端之通信裝置，特別是查驗由鑑認局所發行之伺服器證明書之正當性者。

【先前技術】

發明背景

近年來，網際網路迅速地普及、擴展，並提供電子郵件及網路購物等各式各樣之服務。然而，另一方面，則亦產生竊取或竄改經由網際網路通信之資料等之問題。為防止懷有此惡意之第 3 者之攻擊，乃想出各種安全技術並將之導入。舉例言之，安全技術有即使通信資料在通信途中被竊取亦不會得知內容之密碼或可查驗通信資料在通信途中有無遭竄改之鑑認等。

利用此技術，而可在網際網路善加使用之安全技術有稱為 SSL（Secure Sockets Layer）之方式。SSL 揭示於 U.S Patent 5657390，此方式係提供保證伺服器正當、在通信時，通信資料內容不會洩漏及接收之用戶端所接收之通信資料內容在途中未遭竄改三個條件之通信。

接著，利用第 1 圖及第 2 圖，說明 SSL 之通信方式之概要。第 1 圖係顯示 SSL 之鑰匙資訊及證明書之準備 2 者。在此顯示用以進行秘密通信之伺服器 103 及用戶端 102、及發行

顯示伺服器 103 之正當性之伺服器證明書之鑑認局 101。CA 公鑰 104 為對應鑑認局 101 之私鑰之公鑰，CA 私鑰 105 為鑑認局 101 之私鑰，CA 證明書 106 為顯示鑑認局 101 發行之伺服器證明書為正當之證明書，伺服器公鑰 107 為對應伺服器 103 之私鑰之公鑰，伺服器私鑰 108 為伺服器 103 之私鑰，伺服器證明書 109 為顯示伺服器 103 之正當性之證明書，簽章 101 為鑑認局 101 對伺服器證明書 109 之簽章。

第 2 圖係顯示 SSL 之通信協定者。在第 2 圖中，通信共通鑰匙 201 為用於秘密通信之共通鑰匙。

鑑認局 101 先生成 CA 公鑰 104 與 CA 私鑰 105 之組合，同時，作成記載有 CA 公鑰 104 及鑑認局 101 之資訊之 CA 證明書 106。

伺服器 103 於運作前先生成伺服器公鑰 107 與伺服器私鑰 108 之組合。然後，伺服器 103 將伺服器公鑰 107 與關於伺服器 103 之資訊傳送至鑑認局 101，以委託該鑑認局發行伺服器證明書 109。

鑑認局 101 使用 CA 私鑰 105，從自伺服器 103 接收之資訊或其他必要資訊作成簽章 110，並以包括自伺服器 103 接收之資訊或其他必要資訊及簽章 110 者作為伺服器證明書 109 發行給伺服器 103。

伺服器 103 保存所接收之伺服器證明書 109。

且用戶端 102 先從鑑認局 101 取得 CA 證明書 106，並加以保存。

在用戶端 102 與伺服器 103 間，秘密通信實際上如以下進行。

當用戶端 102 連接至伺服器 103 時，首先互相確認在秘密通信使用之加密方式之規格。

接著，伺服器 103 將伺服器證明書 109 送至用戶端 102。

用戶端 102 使用保存於其內部之 CA 公鑰 104，以確認伺服器證明書 109 是否正當。若伺服器證明書 103 正當，即伺服器證明書 109 所含之簽章 110 為以 CA 私鑰 105 而簽章者時，用戶端 102 便使用 CA 公鑰 104 加以查驗，藉此，可確認伺服器證明書 109 為正當。

用戶端 102 確認伺服器證明書 109 為正當後，便隨機作成用戶端共通鑰匙生成資訊，並將之送至伺服器 103。伺服器 103 隨機作成伺服器共通鑰匙生成資訊，並將之送至用戶端 102。

伺服器 103 及用戶端 102 使用伺服器共通鑰匙生成資訊及用戶端共通鑰匙生成資訊，生成通信用共通鑰匙 201。藉此，在用戶端 102 與伺服器 103 可共同擁有通信用共通鑰匙 201。

之後，用戶端 102 及伺服器 103 使用通信用共通鑰匙 201，進行通信之資料之加密及解密，而可進行秘密通信。此外，CA 證明書 106 及伺服器 109 之格式化大多使用經 ITU－T（國際電信聯盟）所定義之 X.509 證明書。

在 X.509 證明書中，於伺服器證明書 109 設定有效期限。這是由於私鑰之安全性與於從公鑰或通信資料計算私

鑰時所花費之時間長習習相關，若長時間使用同一鑰匙，則曝露私鑰之可能性將提高之故。

同樣地亦於 CA 證明書 106 設置有效期限，一般是設定較伺服器證明書 109 長之時間。

然而，當 CA 證明書之有效期限到期時，或是因某些緣故曝露 CA 私鑰時，必須儘速作成全新之鑰匙組，以發行或取得新之 CA 證明書。

舉例言之，當有相當數量之鑑證局同時存在，用戶端如 PC（個人電腦）般保持足夠之計算機資源，而可保有該等 CA 證明書全數或足夠數目時，伺服器可使用從取代失效之鑑認局之其他鑑認局所取得之伺服器證明書。用戶端依序使用所保有之 CA 證明書，進行伺服器證明書之鑑認，不論以任何一個 CA 證明書，可確認伺服器證明書之正當性時，便可確認該伺服器為正當。

又，有新之鑑認局出現，為取得其 CA 證明書，用戶端之使用者可從諸如鑑認局本身或可信賴之伺服器等取得，使用者可自行將之安裝於用戶端等，來執行。

又，當伺服器證明書之有效期限即將到期時，或伺服器證明書失效時，自動更新全新之伺服器證明書之裝置及方法揭示於諸如日本專利公開公報特開 2001－197054 號及特開 2002－215826 號。

然而，若為如家電機器等，無法充分保有記憶體等資源之用戶端時，則產生無法經常保有多數個 CA 證明書或不易組裝使用多數 CA 證明書查驗之程式或電路等之問題。

又，若為無法保有時鐘（日曆、定時器），或不具有可將時鐘設定為正確時間之用戶端時，則有不易判定CA證明書之有效期限，而當有效期限將近時，無法自動更新新CA證明書之問題。

【發明內容】

發明概要

因此，本發明即是鑑於習知之問題點而創作者，其目的在於提供當即使所擁有之資源少時，亦可安全且確實地更新 CA 證明書，並查驗伺服器之正當性之通信裝置及鑑認裝置。

為達成上述目的，本發明之通信裝置係用以確認以通信網路連接之伺服器之正當性者，包含有：第 1 記憶機構，係用以記憶具有第 1CA 證明書及次回更新用位址之第 1CA 資訊，其中該第 1CA 證明書係顯示表示前述伺服器之正當性之伺服器證明書為正當者，該次回更新用位址係顯示存放有具有當第 1CA 證明書失效時，接著成為有效之第 2CA 證明書之第 2CA 資訊之下載伺服器在前述通信網路上之位置者；鑑認機構，係藉使用前述第 1CA 證明書，查驗前述伺服器證明書，以鑑認前述伺服器之正當性者；及 CA 資訊更新機構，係從顯示前述次回更新用位址之前述下載伺服器取得前述第 2CA 資訊者，前述鑑認機構在前述第 1CA 證明書失效後，使用藉前述 CA 資訊更新機構取得之前述第 2CA 資訊所含之前述第 2CA 證明書，鑑認前述伺服器之正當性。藉此，由於可進入第 1CA 資訊所含之次回更新用

位址所示之下載伺服器，而取得接著成為有效之第 2CA 證明書，故不須先保持多數之 CA 證明書，即使為記憶體等之資源少之家電機器等，亦可更新 CA 證明書，並查驗伺服器之正當性。

在此，前述 CA 資訊更新機構亦可每逢一定期間，便嘗試連接至前述下載伺服器，當可連接時，便從該下載伺服器取得前述第 2CA 資訊。藉此，由於於第 1CA 證明書之有效期限期滿之一定期間前，啟動下載伺服器，通信裝置可取得次回有效之第 2CA 證明書，故不須日曆、定時器等之期限管理，所具有之資源少亦無妨。

又，前述 CA 資訊更新機構於前述鑑認機構無法使用前述第 1CA 證明書，鑑認前述伺服器之正當性時，亦可嘗試連接至前述下載伺服器，當可連接時，便從該下載伺服器取得前述第 2CA 資訊。藉此，即使當第 1CA 證明書於有效期限前已失效時，亦可即刻從下載伺服器取得接著成為有效之第 2CA 證明書。

又，前述鑑認機構於使用藉前述 CA 資訊更新機構取得之前述第 2CA 資訊所含之前述第 2CA 證明書，亦可嘗試前述伺服器之正當性之鑑認，而可鑑認時，便使用前述第 2CA 證明書取代前述第 1CA 證明書，以鑑認前述伺服器之正當性。藉此，當第 2CA 證明書有效之後，可即刻從第 1CA 證明書切換成第 2CA 證明書，通信裝置便毋須管理第 1 及第 2CA 證明書之有效期限。

又，前述通信裝置更包含有用以記憶前述第 2CA 資訊

之第 2 記憶機構，而前述 CA 資訊更機構將從前述下載伺服器取得之前述第 2CA 資訊儲存於前述第 2 記憶機構，前述鑑認機構在前述第 1CA 證明書失效後，可使用儲存於前述第 2 記憶機構之前述第 2CA 資訊所含之前述第 2CA 證明書，鑑認前述伺服器之正當性，或前述鑑認機構在前述第 1CA 證明書失效後，亦可將儲存於前述第 2 記憶機構之前述第 2CA 資訊移至前述第 1 記憶機構，而使用儲存於前述第 1 記憶機構之前述第 2CA 資訊所含之前述第 2CA 證明書，鑑認前述伺服器之正當性。藉此記憶體之運用方法，通信裝置可一面更新 CA 證明書，一面反覆進行僅保持現在有效之第 1CA 證明書與次回成為有效之第 2CA 證明書之 2 個世代之 CA 證明書之處理，而不須保持無用之 CA 證明書。

又，前述 CA 資訊更新機構從前述下載伺服器取得顯示該下載伺服器之正當性之下載伺服器證明書後，依所取得之下載伺服器證明書，鑑認該下載伺服器之正當性後，取得前述第 2CA 資訊。藉此，由於在確認下載伺服器本身之正當性後取得第 2CA 資訊，故可安全地取得真正之第 2CA 證明書。

此外，本發明不僅可以此通信裝置（用戶端）而實現之，亦可以包含通信裝置之處理程序之伺服器之正當性確認方法，將伺服器證明書及 CA 證明書發行給通信裝置之鑑認裝置（鑑認局），包含鑑認裝置之處理程序之鑑認方法，使電腦執行該等方法所含之步驟之程式，記錄有該程

式之記錄媒體，或包含上述鑑認裝置及下載伺服器之運作程序之鑑認系統之運用方法而實現之。

如以上所述，藉本發明，即使為資源少之機器亦可不在意CA證明書之有效期限為何時，而可確實地進行CA證明書之取得及更新，特別是以家電機器等作為用戶端之鑑認系統之實用性價值極高。

圖式簡單說明

第 1 圖係顯示習知秘密通信之 SSL 之鑰匙資訊及證明書之準備者。

第 2 圖係顯示 SSL 之通信協定者。

第 3 圖係第 1 實施形態之通信系統之結構圖。

第 4 圖係顯示 CA 資訊之一例者。

第 5 圖係顯示第 2 實施形態之鑑認局及下載伺服器之運用例之流程圖。

第 6 圖係進行下載伺服器之結束判斷之流程圖。

第 7 圖係顯示鑑認局、用戶端、下載伺服器及應用伺服器之動作流程一例（正常時）者。

第 8 圖係顯示鑑認局、用戶端、下載伺服器及應用伺服器之動作流程一例（於鑑認局 B 運作前，CA 證明書 A 在期限前失效）者。

第 9 圖係顯示鑑認局、用戶端、下載伺服器及應用伺服器之動作流程一例（於鑑認局 B 運作中，CA 證明書 A 在期限前失效）者。

第10圖係1個鑑認局發行多數伺服器證明書及CA資訊

之通信系統者。

【實施方式】

較佳實施形態之詳細說明

以下，參照圖式，就本發明之實施形態進行說明。

（第 1 實施形態）

首先，利用第 3 圖及第 4 圖，就本發明之第 1 實施形態進行說明。

第 3 圖係本實施形態之通信系統之結構圖。此通信系統由以網際網路等通信網連接之鑑認局 A101a、鑑認局 B101b、應用伺服器 401、用戶端 415 及下載伺服器 B406b 所構成。在此，因有效期限等理由，應用伺服器 401 為先從鑑認局 A101a 取得鑑認，接者從鑑認局 B101b 取得鑑認者。

應用伺服器 401 為在某應用程式提供服務（例如對特定製造商之 DVD 播放器提供最新之韌體）之電腦裝置等，其具有 AP 伺服器私鑰 AP404a 及 AP 伺服器證明書 A402a。AP 伺服器私鑰 A404a 為此應用伺服器 401 之私鑰。AP 伺服器證明書 A402a 為鑑認局 A101a 所發行之顯示應用伺服器 A404a 之正當性之證明書，其包含對應 AP 伺服器私鑰 A404a 之公鑰 AP 伺服器公鑰 A403a 及鑑認局 A101a 對此 AP 伺服器證明書 A402a 之簽章之 AP 簽章 A405a。用戶端 415 為於確認應用伺服器 401 之正當性後，接受來自應用伺服器 401 之服務之提供（例如下載韌體）之家電機器等，其具有伺服器鑑認部 416、記憶體 418、備用記憶體 419、

CA 資訊更新部 417 及 DL 公鑰 414。伺服器鑑認部 416 為藉鑑認從應用伺服器 401 接收之 AP 伺服器證明書 A402a，以鑑認應用伺服器 401 之處理部。記憶體 418 為其初期狀態係保持用於 AP 伺服器證明書 A402a 鑑認之關於鑑認局 A101a 之 CA 資訊 A301a 之記憶體。備用記憶體 419 為當儲存於記憶體 418 之 CA 資訊 A301a 失效時，接續保持用以確認應用伺服器 401 之正當性（換言之，用以查驗鑑認局 B101b 所發行之顯示應用伺服器 401 之正當性之 AP 伺服器證明書 B)之鑑認局 B101b 之資訊 CA 資訊 B301b 者。CA 資訊更新部 417 為當儲存於記憶體 418 之 CA 資訊 A301a 失效時等，從下載伺服器 B406b 取得接著成為有效之 CA 資訊（CA 資訊 B301b）後，將之儲存於備用記憶體 419 之處理部。DL 公鑰 414 為對應下載伺服器 B406b 之 DL 伺服器私鑰 B410b 之公鑰。

鑑認局 A101a 為發行顯示應用伺服器 401 之正當性之 AP 伺服器證明書 A402a 及用以確認該 AP 伺服器證明書 A402a 為正當之 CA 資訊 A301a 之鑑認局，其具有 CA 私鑰 A105a、DL 私鑰 413 及 CA 資訊 A301a。CA 私鑰 A105a 為此鑑認局 A101a 之私鑰，DL 私鑰 413 為下載伺服器 B406b 之私鑰。CA 資訊 A301a 包含顯示鑑認局 A101a 所發行之伺服器證明書（在此為 AP 伺服器證明書 A402a 及 DL 伺服器證明書 B408b 等）為正當之 CA 證明書 A106a、置放接續此 CA 資訊 A301a 而成為有效之 CA 資訊 B301b 之下載伺服器 B406b 之 URL 之 URLB302b，使用對此 CA

資訊 A301a 之 DL 私鑰 413 的簽章 CA 簽章 A303a 等。

鑑認局 B101b 為發行接續在鑑認局 A101a 所發行之 CA 資訊 A301 成為有效之 CA 資訊 B301b 者，其具有 CA 私鑰 B105b、DL 私鑰 413 及 CA 資訊 B301b。CA 私鑰 B105b 為此鑑認局 B101b 之私鑰。CA 資訊 B301b 包含顯示鑑認局 B101b 所發行之伺服器證明書（在此為顯示應用伺服器 401 之正當性之 AP 伺服器證明書 B 等）為正當之 CA 證明書 B106b、置放接續此 CA 資訊 B301b 而成為有效之 CA 資訊 C 之下載伺服器 C 之 URL 之 URLB302c，使用了對此 CA 資訊 B301b 之 DL 私鑰 413 的簽章 CA 簽章 B303b 等。

下載伺服器 B406b 為用以下載用戶端 415 接著成為有效之 CA 資訊之伺服器裝置，其具有 CA 資訊 B301b、DL 伺服器證明書 B408b 及 DL 伺服器私鑰 B401b。CA 資訊 B301b 為接續 CA 資訊 A301a 而成為有效之 CA 資訊(從鑑認局 B 傳送之 CA 資訊 B301b)。DL 伺服器私鑰 B410b 為此下載伺服器 B406b 之私鑰。DL 伺服器證明書 B408b 為鑑認局 B101b 所發行，顯示下載伺服器 B406b 之正當性之伺服器證明書，其包含對應 DL 伺服器私鑰 B401b 之公鑰 DL 伺服器公鑰 B409b、鑑認局 A101a 對此 DL 伺服器證明書 B408b 之簽章 DL 簽章 B412b。

第 4 圖係顯示第 3 圖所示之 CA 資訊 A301a 及 B301b 之更詳細之資料結構者。CA 資訊 301 包含顯示伺服器為正當之 CA 證明書 106、顯示該 CA 證明書 106 之長度之資訊 116、置放接續此 CA 資訊 301 而成為有效之 CA 資訊之下

載伺服器之 URL302、顯示該 URL 之長度之資訊 312、及對該等 4 個資訊之 CA 簽章 303（在此為 DL 私鑰 413 之簽章）。此外，CA 證明書 106 包含用於確認鑑認局所發行之伺服器證明書之正當性之鑑認局之公鑰（CA 公鑰）。

用戶端 415 藉使用此 CA 資訊 301，可確認應用伺服器 401 之正當性。即，用戶端 415 對所獲得之 CA 資訊 301，使用 DL 公鑰 414，查驗 CA 簽章 303，確認 CA 資訊 301 本身之正當性後，使用該 CA 資訊 301 所含之 CA 證明書 106，確認從應用伺服器 401 接收之伺服器證明書之正當性，或藉進入該 CA 資訊 301 所含之 URL，獲得接續該 CA 資訊 301 而成為有效之 CA 資訊。

以下，就用戶端 415 之伺服器鑑認動作（用以確認應用伺服器 401 之正當性之處理）加以說明。

首先，應用伺服器 401 作成 SSL 通信用鑰匙組，AP 伺服器私鑰 A404a 與 AP 伺服器公鑰 A403a 後，將 AP 伺服器公鑰 A403a 及其他必要事項送至鑑認證局 A101a，以委託該鑑認局 A101a 發行伺服器證明書。

鑑認局 A101a 已先保有 CA 私鑰 A105a 與 CA 公鑰 A 之鑰匙組，當從應用伺服器 401 接收伺服器證明書之發行委託時，便發行 AP 伺服器證明書 A402a 與 CA 私鑰 A105a 之簽章，然後將之送至應用伺服器 401。

又，鑑認局 A101a 作成包含 CA 公鑰 A 之伺服器證明書 CA 證明書 A106a 後，作成包含該 CA 證明書 A106a 之 CA 資訊 A301a。附加於 CA 資訊 301a 之 URLB302b 為下

載伺服器 B406b 之 URL。

用戶端 415 之初期狀態係於內部之記憶體 418 保存有 CA 資訊 A301a，而於備有記憶體 419 則未保存任何東西。

用戶端 415 於與應用伺服器 401 進行 SSL 通信時，伺服器鑑認部 416 從應用伺服器 401 取得 AP 伺服器證明書 A402a 後，可以保存於記憶體 418 之 CA 證明書 A106a 內之 CA 公鑰 A 進行鑑認。

當證明 AP 伺服器 A402a 為正當時，如習知技術所說明，可在用戶端 415 與應用伺服器 401 間進行 SSL 通信。

接著，就用戶端 415 之 CA 資訊之更新動作加以說明。

當 CA 證明書 A106a 之有效期限將近時，用戶端 415 須預先取得新之 CA 證明書。為此，在 CA 證明書 A106a 之有效期限來臨前，系統之運用者使持有 CA 私鑰 B105b 與 CA 公鑰 B 之鑰匙組之新鑑認局 B101b 運作，鑑認局 B101b 便作成包含 CA 公鑰 B 之新 CA 證明書 B106b。但，在此時間點，鑑認局 B101b 不對應用伺服器 401 發行 AP 伺服器證明書。或者是即使發行伺服器證明書，在此時間點，應用伺服器 401 在與用戶端 415 之伺服器鑑認時，亦不使用自鑑認局 B101b 取得之 AP 伺服器證明書。

鑑認局 B101b 從已作成之 CA 證明書 B106b，作成新 CA 證明書 B301b。記載於內部之 URLC302c 為次回用以下載新 CA 資訊之下載伺服器 C 之 URL，CA 簽章 B303b 與 CA 署名 A303a 為以相同方式作成者。

然後，系統之運用者於以 URLB302b 所指定之場所(網

路上之網站等）使下載伺服器 B406b 運作，以可下載 CA 資訊 B301b。此時，在下載伺服器 B406b 中，亦生成 DL 伺服器公鑰 B409b 與 DL 伺服器私鑰 B410b 之鑰匙組，將 DL 伺服器公鑰 B409b 及必要事項送至鑑認局 A101a，而從鑑認局 A101a 取得 DL 伺服器證明書 B408b 作為伺服器證明書。

然後，用戶端 415 之 CA 資訊更新部 417 對記載於記憶體 418 之 CA 資訊 A301a 之 URLB302b 所示之下載伺服器在某段期間，例如每逢一個月便嘗試連接。由於當下載伺服器 B406b 未運作時，CA 資訊更新部 417 對下載伺服器 B406b 之連接失敗，故此時便判斷為不須更新。之後，每個月皆嘗試同樣之連接。

另一方面，當下載伺服器 B406b 運作時，由於 CA 資訊更新部 417 對下載伺服器 B406b 之連接成功，故先取得 DL 伺服器證明書 B408b 後，使用保存於記憶體 418 之 CA 公鑰 A（此包含於 CA 證明書 A106a），進行鑑認。

當確認 DL 伺服器證明書 B408b 之正當性後，CA 資訊更新部 417 接著從下載伺服器 B406b 取得 CA 資訊 B301b。CA 資訊更新部 417 以 DL 公鑰 414，鑑認所取得之 CA 資訊 B301b 內之 CA 簽章 B303b，當可確認 CA 資訊 B301b 之正當性時，便將 CA 署名 B303b 保存於備用記憶體 419。

接著，就 CA 證明書 A106a 之有效期限到期時之應用伺服器 401 與用戶端 415 之動作加以說明。

應用伺服器 401 在 CA 證明書 A106a 之有效期限到期

前或到期之同時，生成 AP 伺服公鑰與 AP 伺服器私鑰之新鑰匙組，而從鑑認局 B101b 取得新之 AP 伺服器證明書 B。應用伺服器 401 在 CA 證明書 A106a 之有效期限到期時，將舊之 AP 伺服器證明書 A402a 作廢，而在之後進行 SSL 通信時，送交 AP 伺服器證明書 B 作為伺服器證明書。

如此，當 CA 證明書 A106a 之有效期限到期時，用戶端 415 之伺服器鑑認部 416 在與應用伺服器 401 通信時，便接收新 AP 伺服器證明書 B。然而，在保存於記憶體 418 之 CA 證明書 A106a 內之 CA 公鑰 A 中，對 AP 伺服器證明書 B 之鑑認失敗。此時，伺服器鑑認部 416 使用保存於備用記憶體 419 之 CA 資訊 B301b 內之 CA 公鑰 B，進行 AP 伺服器證明書 B 之鑑認，當可確認 AP 伺服器證明書 B 之正當性時，用戶端 415 繼續與應用伺服器 401 之 SSL 通信。

此時，伺服器鑑認部 416 將保存於備用記憶體 419 之 CA 資訊 B301b 移至記憶體 418，之後，使備用記憶體 419 淨空。然後，伺服器鑑認部 416 將保存於記憶體 418 之 CA 資訊 B301b 用於與應用伺服器 401 之鑑認。

另一方面，當備用記憶體 419 未保存任何東西時，伺服器鑑認部 416 對 CA 資訊更新部 417 指示新 CA 資訊之取得。接收該指示之 CA 資訊更新部 417 以與上述同樣之程序從下載伺服器 B406b 取得新 CA 資訊 B301b。伺服器鑑認部 416 在取得新 CA 資訊 B301b 後，與上述同樣地，使用 CA 資訊 B301b，進行應用伺服器 401 之鑑認。

然後，當 CA 證明書之有效期限將近時，藉進行同樣之動作，用戶端 415 可自動取得新 CA 證明書，且，當 CA 證明書之有效期限到期時，可自動地進行使用新 CA 證明書之鑑認。

如上述，藉本實施形態，鑑認局 A101a 將與 CA 證明書成對且用以次回下載 CA 證明書之網站之下載伺服器 B406b 之 URL 送至用戶端 415。然後，當 CA 證明書之有效期限將近時，系統運用者使發行新 CA 證明書之鑑認局 B101b 運作，同時，使下載伺服器 B406b 運作。另一方面，用戶端 415 定期地嘗試進入下載伺服器 B406b 之 URL，若進入成功時，便下載新 CA 證明書，將之保存於備用記憶體 419。然後，通信對象之應用伺服器 401 之伺服器證明書無法以現在之 CA 證明書鑑認時，便以保存於備用記憶體 419 之新 CA 證明書鑑認，若可確認應用伺服器之正當性時，則刪除原本之 CA 證明書，以後便將新之 CA 證明書用於伺服器證明書之鑑認。

藉此，由於用戶端 415 僅保存下次成為有效之 CA 證明書，即可更新 CA 證明書，故毋須經常保有多數個 CA 證明書，或預先安裝使用多數 CA 證明書鑑認之程式或電路。且，由於用戶端 415 可定期地進入下載伺服器 B406b，取得新之 CA 證明書，而開始與應用伺服器之新通信，故不須使用時鐘，監視 CA 證明書之有效期限。因而，即使用戶端 415 為如家電機器般未保有充分資源之機器，亦可不在意 CA 證明書之有效期限為何時，而可確實地進行 CA 證

明書之取得及更新。

此外，在本實施形態中，CA 資訊更新部 417 每個月嘗試對記載於記憶體 418 所保存之 CA 資訊之 URL 所示之下載伺服器之連接，本發明並不限每個月，亦可為較長或較短之期間。又，此期間可相等，或不均等。重要的是只要從下載伺服器之運作開始至現在之 CA 證明書有效期限到期之期間確實地嘗試 1 次連接即可。

又，應用伺服器 401 在 CA 證明書之有效期限到期之同時，作成新之 AP 伺服器公鑰與 AP 伺服器私鑰之鑰匙組，亦可在 CA 證明書之有效期限內作成新之 AP 伺服器公鑰與 AP 伺服器私鑰之鑰匙組，以取得新之 AP 伺服器證明書。此時由於新之 AP 伺服器證明書亦包含相同之 CA 私鑰之簽章，故用戶端 415 可使用所保存之 CA 公鑰，進行新之 AP 伺服器證明書之鑑認。

又，第 4 圖之 CA 資訊 301 包含其他圖中未示之資訊亦可。

又，當 CA 資訊部 417 可確認下載之新 CA 資訊之正當性時，將新之 CA 資訊保存於備用記憶體 419，此時，不保存 CA 簽章 303 亦可。藉此，可削減備用記憶體 419 之容量。同樣地，初期狀態係於記憶體 418 保存 CA 資訊 A301a，而不保存 CA 簽章 A303a 亦可。

又，伺服器鑑認部 416 將保存於備用記憶體 419 之 CA 資訊 B301b 移至記憶體 418 後，使備用記憶體 419 淨空，相反地亦可使記憶體 418 淨空，之後使記憶體 418 與備用

記憶體 419 之角色交換，以後每當進行 CA 資訊之更新時，便使記憶體 418 與備用記憶體 419 之角色交換。

（第 2 實施形態）

其次，利用第 5 圖~第 9 圖，說明作為本發明第 2 實施之上述第 1 實施形態之鑑認局及下載伺服器之運用之一例。

第 5 圖係顯示鑑認局及下載伺服器之運用例之流程圖。

第 6 圖係進行下載伺服器之結束判斷之流程圖。

第 7 圖係正常時之鑑認局、用戶端、下載伺服器及應用伺服器之動作流程之一例。

第 8 圖係 CA 證明書 A 於有效期限前失效時之鑑認局、用戶端、下載伺服器及應用伺服器之動作流程之一例，為失效時，下個下載伺服器未運作之情形。

第 9 圖係 CA 證明書 A 於有效期限前失效時之鑑認局、用戶端、下載伺服器及應用伺服器之動作流程之一例，為失效時，下個下載伺服器已運作之情形。

在本實施形態中，令 CA 證明書 A106a 之有效期限為 20 年，CA 證明書 A106a 之有效期限到期之 5 年前，使新之鑑認局 B101b 及下載伺服器 B406b 運作。

又，下載伺服器為於前一個 CA 證明書指定之有效期限到期時，使運作結束者。舉例言之，下載伺服器 B406b 為 CA 證明書 A106a 所指定之有效期限，即從鑑認局 A101a 之運作開始，20 年後。

首先，利用第 5 圖及第 6 圖之流程圖，說明鑑認局及下載伺服器之運用例。在此，顯示管理鑑認局及下載伺服

器之系統之運用者之作業程序。

如第 5 圖所示，當運用開始時（步驟 501），首先使鑑認局 A101a 運作（步驟 502）。

接著，確認 CA 證明書 A106a 在有效期限前是否已失效，若失效時，便前進至步驟 511，若尚未失效，則前進至步驟 504。

若未失效（在步驟 503 為 NO），則確認是否為 CA 證明書 A106a 之有效期限到期之 5 年前（步驟 504），若不是 5 年前，便返回至步驟 503，若為 5 年前，則前進至步驟 505。

若為 5 年前時（在步驟 504 為 Yes），便使鑑認局 B101b 假運作（步驟 505），同時，使下載伺服器 B406b 運作（步驟 506）。此外，在此時間點，鑑認局 B101b 作成 CA 公鑰 B 與私鑰 B105b 之鑰匙組，並保有之，應用伺服器 401 送至用戶端 415 之伺服器證明書則維持 AP 伺服器證明書 A402a。

然後，確認 CA 證明書 A106a 是否在有效期限前已失效（步驟 507），若已失效時，便前進至步驟 509，若未失效，則前進至步驟 508。

若未失效時（在步驟 507 為 No），便確認 CA 證明書 A106a 之有效期限是否已到期（步驟 508），若未到期，便返回步驟 507，若到期時，則前進至步驟 509。

若有效期限到期時（在步驟 508 為 Yes），便使鑑認局 A101a 之運作結束（步驟 509），使鑑認局 B101b 真正運作（步驟 510）。此外，在此時間點，應用伺服器 401 送至用

戶端 415 之伺服器證明書為附加有 CA 私鑰 B105b 之 AP 伺服器證明書 B。

另一方面，若 CA 證明書 A106a 在有效期限前已失效時(在步驟 503 為 Yes)，則使下載伺服器 B406b 運作後(步驟 511)，使鑑認局 A101a 之運作結束（步驟 509)。

此外，使鑑認局 B101b 真正運作後（步驟 510)，對鑑認局 B 及 CA 證明書 B 分別進行至目前為止對鑑認局 A 及 CA 證明書 A 進行之處理，同時，對下次成為有效之鑑認局 C、CA 證明書 C 及下載伺服器 C 進行對鑑認局 B、CA 證明書 B 及下載伺服器 B 進行之處理，藉此，反覆進行同樣之處理（步驟 503~510)。

此外，是否使目前運作之下載伺服器之運作結束以第 6 圖所示之流程圖表示。

當下載伺服器運作時（步驟 601)，確認下載伺服器之運作期間（步驟 602)，若運作期間未結束時，便返回至步驟 602，等待至運作期間結束為止，若運作期間結束時，便前進至步驟 603。此外，下載伺服器之運作期間從現在有效之 CA 證明書之有效期限之 5 年前至有效期限為止。

當運作期間結束時（在步驟 602 為 Yes)，便使下載伺服器之運作結束（步驟 603)。舉例言之，在即將結束之前有效之 CA 證明書之有效期限屆滿後，便使下載伺服器結束。

之後，重複同樣之動作，進行鑑認局及下載伺服器之運作與結束。

如以上所述，藉本實施形態，不僅在 CA 證明書在有效期限結束時，在有效期限前失效時，與第 1 實態同樣地，由於用戶端 415 僅保持下次成為有效之 CA 證明書，即可更新 CA 證明書，故毋須經常保有多數個 CA 證明書，或預先安裝使用多數 CA 證明書鑑認之程式或電路。且，由於用戶端 415 可定期地進入下載伺服器 B406b，取得新之 CA 證明書，而開始與應用伺服器之新通信，故不須使用時鐘，監視 CA 證明書之有效期限。因而，即使用戶端 415 為如家電機器般未保有充分資源之機器，亦可不在意 CA 證明書之有效期限為何時，而可確實地進行 CA 證明書之取得及更新。

此外，在第 5 圖中，步驟 505 與步驟 506 之順序相反亦可，同時進行亦可。同樣地，步驟 509 與步驟 510 之順序相反亦可，同時進行亦可。

接著，依第 5 圖及第 6 圖之流程圖，說明進行鑑認局及下載伺服器之運用時，在一般情形（CA 證明書因有效期限到期而失效）及在有效期限到期前 CA 證明書因某些理由而失效時，用戶端、下載伺服器及應用伺服器之動作流程。此外，CA 證明書在有效期限到期前因某些理由失效時之動作流程係就在失效之時間點，下個下載伺服器已運作及未運作 2 點來說明。

第 7 圖係正常時之用戶端、下載伺服器及應用伺服器之動作流程。

在初期狀態之用戶端 415 中，於記憶體 418 內保存有

CA 資訊 A301a，而備用記憶體 419 則未保存任何東西。

由於在 CA 證明書 A106a 之有效期限內，應用伺服器 401 所送之 AP 伺服器證明書 A 可以 CA 公鑰 A 予以鑑認，故用戶端 415 可使用本身所保持之 CA 資訊 A301a，確認應用伺服器 401 之正當性。

又，用戶端 415 定期嘗試對 URLB302b 所示之下載伺服器 B406b 之連接，但由於在 CA 證明書 A106a 之有效期限到期之 5 年前，下載伺服器 B406b 尚未運作，故連接必定失敗。

在 CA 證明書 A106 之有效期限未到，而已到 5 年前之時間點，使新之鑑認局 B101b 運作，作成新之 CA 證明書 B106b 與 CA 資訊 B301b。同時使可下載 CA 資訊 B301b 之下載伺服器 B406b 運作。

當下載伺服器 B406b 運作時，用戶端 415 對下載伺服器 B406b 之連接成功，而可取得 CA 資訊 B301b。用戶端 415 確認 CA 資訊 B301b 為正當時，便將 CA 資訊 B301b 保存於備用記憶體 419。

由於用戶端 415 定期地嘗試對下載伺服器 B406b 之連接，故在 CA 證明書 A106a 之有效期限到期前，即使已取得 CA 資訊 B301b，對下載伺服器 B406b 與 CA 資訊 B301b 之取得仍繼續進行。此時，若備用記憶體 419 內之 CA 資訊與所取得之 CA 資訊相同時，亦可不保存於備用記憶體 419，若取得之 CA 資訊為正當，經常將之寫入亦可。

接著，當 CA 證明書 A106a 之有效期限到期時，應用

伺服器 401 將以新之 CA 證明書 B106b 鑑認之 AP 伺服器證明書 B 用於伺服器鑑認。之後，用戶端 415 開始與應用伺服器 401 之 SSL 通信時，所取得之伺服器證明書為 AP 伺服器證明書 B，在所保持之 CA 證明書 A106a 中，AP 伺服器證明書 B 之鑑認失敗。

如此，用戶端 415 使用保存於預備記憶體 419 之 CA 資訊 B301b 內之 CA 證明書 B106b，進行 AP 伺服器證明書 B 之鑑認。當用戶端 415 確認 AP 伺服器證明書 B 為正當時，便繼續 SSL 通信，同時，將備用記憶體 419 內之 CA 資訊 B301b 移至記憶體 418，並刪除備用記憶體 419 內之資訊。

之後，用戶端 415 使用 CA 證明書 B106b，進行伺服器鑑認，且定期地進行對 CA 資訊 B301b 內之 URLC302c 所顯示之下載伺服器 C 之連接。

此時，下載伺服器 B406b 在 CA 證明書 A106a 失效時，同時結束運作。

以下，藉繼續進行同樣之動作，即使鑑認局及 CA 證明書為新時，用戶端 415 仍可進行應用伺服器之鑑認及 CA 證明書之更新。

而當解讀 CA 私鑰 A105a 等，而無法保證 CA 私鑰 A106a 之安全性時，則須迅速地使 CA 證明書 A106a 失效，同時，使新之鑑認局 B101b 運作，以發行新之 CA 證明書 B106b。同時，應用伺服器 401 必須從新之鑑認局 B101b 接收新之 AP 伺服器證明書，以將之用於伺服器鑑認。

第 8 圖係顯示用以下載次回之 CA 資訊之下載伺服器運作前，目前之 CA 證明書失效時之鑑認局、用戶端、下載伺服器及應用伺服器之動作流程。

CA 證明書 A106a 失效前之各動作與第 7 圖相同。

由於在 CA 證明書 A106a 失效之時間點，鑑認局 B101b 尚未運作，故系統之運用者迅速地使新之鑑認局 B101b 運作，以發行新之 CA 證明書 B106b，同時，作成 CA 資訊 B301b。且，與此同時，使下載伺服器 B406b 運作，而可下載 CA 資訊 B301b。

在 CA 證明書 A106a 失效後，用戶端 415 在進行應用伺服器 401 之伺服器鑑認前，對下載伺服器 B406b 之連接碰巧成功，而可取得新之 CA 資訊 B301b 時，用戶端 415 可與平常動作時同樣地進行 CA 資訊之更新。

然而，在取得 CA 資訊 B301b 前，當用戶端 415 進行應用伺服器 401 之伺服器鑑認時，用戶端 415 對 AP 伺服器證明書 B 之鑑認失敗，此時，備用記憶體 419 並未保存新之 CA 資訊 B301b，此時，用戶端 415 便即刻嘗試對下載伺服器 B406b 之連接。由於在此時間點，下載伺服器 B406b 已運作，故用戶端 415 可從下載伺服器 B406b 取得新之 CA 資訊 B301b。

在取得新之 CA 資迅 B301b 後，反覆進行與平常相同之動作。而如第 8 圖所示，若 CA 證明書 A106a 在有效期限前失效時，下載伺服器 B406b 仍可繼續運作至 CA 證明書 A106a 之原本之有效期限之時間點。

第 9 圖係用以下載次回之 CA 資訊之下載伺服器運作後，目前之 CA 證明書失效時之鑑認局、用戶端、下載伺服器及應用伺服器之動作流程。

CA 證明書 A106a 失效前之各動作與第 7 圖相同。

在 CA 證明書 A106a 失效之時間點，應用伺服器 401 將從新之鑑認局 B101b 所發行之新 AP 伺服器證明書 B 用於與用戶端 415 之伺服器鑑認。

又，由於在 CA 證明書 A106a 失效之時間點，鑑認局 B101b 及下載伺服器 B406b 正運作，故用戶端 415 可取得 CA 資訊 B301b。因此，用戶端 415 已取得 CA 資訊 B301b，並將之保存於備用記憶體 419 時，與第 7 圖同樣地，可在 AP 伺服器 B 之鑑認失敗之時間點，進行 CA 資訊之更新。

又，用戶端 415 在取得 CA 資訊 B301b 前，若 AP 伺服器證明書 B 之鑑認失敗時，與第 8 圖同樣地，在該時間點，連接至下載伺服器 B406b，進行新 CA 資訊 B301b 之取得，以繼續 AP 伺服器證明書 B 之鑑認。

之後，重覆與平常時相同之動作。但，如第 9 圖所示，CA 證明書 A106a 在有效期限前失效時，下載伺服器 B406b 繼續運作至 CA 證明書 A106a 之原本之有效期限之時間點。

以下，藉繼續進行同樣之動作，即使 CA 證明書在有效期限失效前，用戶端 415 亦可進行應用伺服器 401 之鑑認及 CA 證明書之更新。

此外，在本實施形態中，令 CA 證明書之有效期限為 20 年，且在 CA 證明書之有效期限到期之 5 年前，使新鑑

認局及下載伺服器運作，本發明中，有效期限亦可不為 20 年，且鑑認局及下載伺服器之開始運作不為 CA 證明書之有效期限之 5 年前亦可。又，CA 證明書之有效期限不一定皆為 20 年，可依 CA 證明書而異。

又，將保存於備用記憶體 419 之 CA 資訊 B301b 保存於記憶體 418 後，使備用記憶體 419 淨空，相反地亦可使記憶體 418 淨空，之後使記憶體 418 與備用記憶體 419 之角色交換，以後每當進行 CA 資訊之更新時，便使記憶體 418 與預備記憶體 419 之角色交換。

又，在本實施形態中，設置多數之鑑認局 A101a 及鑑認局 B101b，如第 10 圖所示之系統結構，亦可 1 個鑑認局發行多數個伺服器證明書及 CA 資訊。在第 10 圖中，1 個鑑認局 120 具有 2 個證明書發行部 A120a 及 B120b。證明書發行部 A120a 相當於第 3 圖之鑑認局 A101a，證明書發行部 B120b 相當於第 3 圖之鑑認局 B101b。下載伺服器方面亦相同。換言之，本實施形態之鑑認局及下載伺服器並非物理性，而是以與在同一電腦裝置內實現或在不同之電腦裝置內實現等無關之機能性單位而定義之。

又，在本實施形態中，是由系統運用者進行鑑認局及下載伺服器之啟動及結束，本發明不限於以人工作業，亦可在依預設之運作計畫動作之管理用電腦下，使鑑認局及下載伺服器之啟動及結束自動化。

本發明可利用作一面確認伺服器之正當性，一面接受從伺服器提供之服務之用戶端機器（通信裝置），特別是記

憶體等之資源少之AV機器等家電機器。

【圖式簡單說明】

第1圖係顯示習知秘密通信之SSL之鑰匙資訊及證明書之準備者。

第2圖係顯示SSL之通信協定者。

第3圖係第1實施形態之通信系統之結構圖。

第4圖係顯示CA資訊之一例者。

第5圖係顯示第2實施形態之鑑認局及下載伺服器之運用例之流程圖。

第6圖係進行下載伺服器之結束判斷之流程圖。

第7圖係顯示鑑認局、用戶端、下載伺服器及應用伺服器之動作流程一例（正常時）者。

第8圖係顯示鑑認局、用戶端、下載伺服器及應用伺服器之動作流程一例（於鑑認局B運作前，CA證明書A在期限前失效）者。

第9圖係顯示鑑認局、用戶端、下載伺服器及應用伺服器之動作流程一例（於鑑認局B運作中，CA證明書A在期限前失效）者。

第10圖係1個鑑認局發行多數伺服器證明書及CA資訊之通信系統者。

【圖式之主要元件代表符號表】

101...鑑認局

101a...鑑認局A

101b...鑑認局B

101c...鑑認局C

102...用戶端

103...伺服器

104...CA公鑰

105...CA私鑰

105a...CA私鑰A

105b...CA私鑰B

106...CA證明書

106a...CA證明書A

106b...CA證明書B

107...伺服器公鑰

108...伺服器私鑰

109...伺服器證明書

110...簽章

201...通信用共通鑰匙

301a...CA資訊A

301b...CA資訊B

302...URL

302b...URLB

302c...URLC

303...CA簽章

303a...CA簽章A

303b...CA簽章B

312...資訊

401...應用伺服器

402a...AP伺服器證明書A

403a...AP伺服器公鑰A

404a...AP伺服器私鑰A

405a...AP簽章A

406b...下載伺服器B

406c...下載伺服器C

408b...DL伺服器證明書

409b...DL伺服器公鑰B

410b...DL伺服器私鑰B

412b...DL簽章412b

413...DL私鑰

414...DL公鑰

415...用戶端

416...伺服器鑑認部

417...CA資訊更新部

418...記憶體

419...備用記憶體

伍、中文發明摘要：

本發明之通信裝置具有記憶體、伺服器鑑認部、CA資訊更新部等，該記憶體係用以記憶包含CA證明書A及URLB之CA資訊A者，該CA證明書A係顯示表示應用伺服器之正當性之AP伺服器證明書A為正當者，該URLB係顯示置放有包含接著成為有效之CA證明書B之CA資訊B之下載伺服器B的URL者，該伺服器鑑認部係使用CA證明書A，查驗AP伺服器證明書A者，該CA資訊更新部係從URLB所示之下載伺服器B，取得CA資訊B者，而伺服器鑑認部在CA證明書失效後，使用藉CA資訊更新部取得之CA資訊B所含之CA證明書B，鑑認應用伺服器之正當性。

陸、英文發明摘要：

A communication apparatus includes: a memory (418) that holds CA information A(301a) including (i) a CA certificate A(106a) indicating that an AP server certificate A(402a) that indicates the validity of an application server (401) is valid and (ii) a URL B(302b) indicating the URL of a download server B(406b) where CA information B(301b) including the next valid CA certificate B(106b) is stored; a server authentication unit (416) that verifies the AP server certificate A(402a) using the CA certificate A(106a); and a CA information update unit (417) that obtains the CA information B(301b) from the download server B(406b) indicated by the URL B(302b), wherein when the CA certificate A(106a) becomes revoked, the server authentication unit (416) thereafter authenticates the application server (401) using the CA certificate B(106b) included in the CA information B(301b) obtained by the CA information update unit (417).

拾、申請專利範圍：

1. 一種通信裝置，係用以確認以通信網路而連接之伺服器之正當性者，包含有：

第 1 記憶機構，係用以記憶具有第 1CA 證明書及次回更新用位址之第 1CA 資訊者，其中該第 1CA 證明書係顯示表示前述伺服器之正當性之伺服器證明書為正當者，該次回更新用位址係顯示存放有具有當第 1CA 證明書失效時，接著成為有效之第 2CA 證明書之第 2CA 資訊之下載伺服器在前述通信網路上之位置者；

鑑認機構，係藉使用前述第 1CA 證明書，查驗前述伺服器證明書，以鑑認前述伺服器之正當性者；及

CA 資訊更新機構，係從顯示前述次回更新用位址之前述下載伺服器，取得前述第 2CA 資訊者，

前述鑑認機構在前述第 1CA 證明書失效後，使用藉前述 CA 資訊更新機構所取得之前述第 2CA 資訊所含之前述第 2CA 證明書，鑑認前述伺服器之正當性。

2. 如申請專利範圍第 1 項之通信裝置，其中前述 CA 資訊更新機構每逢一定期間，便嘗試連接至前述下載伺服器，當可以連接時，便從該下載伺服器取得前述第 2CA 資訊。

3. 如申請專利範圍第 1 項之通信裝置，其中前述 CA 資訊更新機構於前述鑑認機構無法使用前述第 1CA 證明書，鑑認前述伺服器之正當性時，便嘗試連接至前述下載伺服器，當可以連接時，便從該下載伺服器取得前述

第 2CA 資訊。

4. 如申請專利範圍第 1 項之通信裝置，其中前述鑑認機構於使用藉前述 CA 資訊更新機構取得之前述第 2CA 資訊所含之前述第 2CA 證明書，嘗試前述伺服器之正當性之鑑認，而當可鑑認時，便使用前述第 2CA 證明書取代前述第 1CA 證明書，鑑認前述伺服器之正當性。

5. 如申請專利範圍第 1 項之通信裝置，更包含有用以記憶前述第 2CA 資訊之第 2 記憶機構，而前述 CA 資訊更新機構將從前述下載伺服器所取得之前述第 2CA 資訊儲存於前述第 2 記憶機構，

前述鑑認機構在前述第 1CA 證明書失效後，便使用儲存於前述第 2 記憶機構之前述第 2CA 資訊所含之前述第 2CA 證明書，鑑認前述伺服器之正當性。

6. 如申請專利範圍第 1 項之通信裝置，更包含有用以記憶前述第 2CA 資訊之第 2 記憶機構，而前述 CA 資訊更機構將從前述下載伺服器所取得之前述第 2CA 資訊儲存於前述第 2 記憶機構，

前述鑑認機構在前述第 1CA 證明書失效後，將儲存於前述第 2 記憶機構之前述第 2CA 資訊移至前述第 1 記憶機構，而使用儲存於前述第 1 記憶機構之前述第 2CA 資訊所含之前述第 2CA 證明書，鑑認前述伺服器之正當性。

7. 如申請專利範圍第 1 項之通信裝置，其中前述 CA 資訊更新機構從前述下載伺服器取得顯示該下載伺服器之正當性之下載伺服器證明書後，依所取得之下載伺服器證

明書，鑑認該下載伺服器之正當性之後，取得前述第 2CA 資訊。

8. 一種伺服器之正當性確認方法，係用以確認以通信網路連接之伺服器之正當性者，包含有：

記憶步驟，係將具有第 1CA 證明書及次回更新用位址之第 1CA 資訊儲存於記憶機構，其中該第 1CA 證明書係顯示表示前述伺服器之正當性之伺服器證明書為正當者，該次回更新用位址係顯示存放有具有當第 1CA 證明書失效時，接著成為有效之第 2CA 證明書之第 2CA 資訊之下載伺服器在前述通信網路上之位置者；

鑑認步驟，係藉使用前述第 1CA 證明書，查驗前述伺服器證明書，以鑑認前述伺服器之正當性者；及

CA 資訊更新步驟，係從顯示前述次回更新用位址之前述下載伺服器，取得前述第 2CA 資訊者，

在前述鑑認步驟中，前述第 1CA 證明書失效後，使用在前述 CA 資訊更新步驟中所取得之前述第 2CA 資訊所含之前述第 2CA 證明書，鑑認前述伺服器之正當性。

9. 一種程式，係用以確認以通信網路連接之伺服器之正當性者，並使電腦執行申請專利範圍第 8 項所載之正當性確認方法所含之步驟者。

10. 一種鑑認裝置，係用以保證以通信網路連接之伺服器之正當性者，包含有：

伺服器證明書發行機構，係發行用以保證前述伺服器之正當性之伺服器證明書者；及

CA 資訊發行機構，係發行具有第 1CA 證明書及次回更新用位址之第 1CA 資訊，其中該第 1CA 證明書係顯示表示前述伺服器證明書為正當者，該次回更新用位址係顯示存放有具有當第 1CA 證明書失效時，接著成為有效之第 2CA 證明書之第 2CA 資訊之下載伺服器在前述通信網路上之位置者。

11. 一種鑑認方法，係用以保證以通信網路連接之伺服器之正當性者，包含有：

伺服器證明書發行步驟，係發行用以保證前述伺服器之正當性之伺服器證明書者；及

CA 資訊發行步驟，係發行具有第 1CA 證明書及次回更新用位址之第 1CA 資訊，其中該第 1CA 證明書係顯示表示前述伺服器證明書為正當者，該次回更新用位址係顯示存放有具有當第 1CA 證明書失效時，接著成為有效之第 2CA 證明書之第 2CA 資訊之下載伺服器在前述通信網路上之位置者。

12. 一種程式，係供用以保證以通信網路連接之伺服器之正當性之鑑認裝置用者，並使電腦執行申請專利範圍第 11 項所載之鑑認方法所含之步驟者。

13. 一種通信系統之運用方法，該通信系統包含以通信網路連接之第 n 鑑認裝置、第（n＋1）鑑認裝置及第（n＋1）下載伺服器，其特徵在於：

前述第 n 鑑認裝置具有：

第 n 伺服器證明書發行機構，係發行用以保證應用伺服

器之正當性之第 n 伺服器證明書者；及

第 nCA 資訊發行機構，係發行具有第 nCA 證明書及第（n＋1）回更新用位址之第 nCA 資訊者，其中該第 nCA 證明書係顯示表示前述第 n 伺服器證明書為正當者，該第（n＋1）回更新用位址係顯示前述第（n＋1）下載伺服器在前述通信網路上之位置者，

前述第（n＋1）鑑認裝置具有：

第（n＋1）伺服器證明書發行機構，係發行用以保證應用伺服器之正當性之第（n＋1）伺服器證明書者；及

第（n＋1）CA 資訊發行機構，係發行具有第（n＋1）CA 證明書及第（n＋2）回更新用位址之第（n＋2）CA 資訊，其中該第（n＋1）CA 證明書係顯示表示前述第（n＋1）伺服器證明書為正當者，該第（n＋2）回更新用位址係顯示存放有具有當第（n＋1）CA 證明書失效時，接著成為有效之第（n＋2）證明書之第（n＋2）資訊之下載伺服器在前述通信網路上之位置者，

前述第（n＋1）下載伺服器具有：

CA 資訊記憶機構，係用以記憶具有當前述第 nCA 證明書失效時接著成為有效之第（n＋1）CA 證明書之第（n＋1）CA 資訊者；及

輸出機構，係將記憶於前述 CA 資訊記憶機構之第（n＋1）CA 資訊輸出至經由前述通信網路連接之通信裝置者，

而前述運用方法重覆以下之步驟 n 次，n 為 1 以上之整

數：

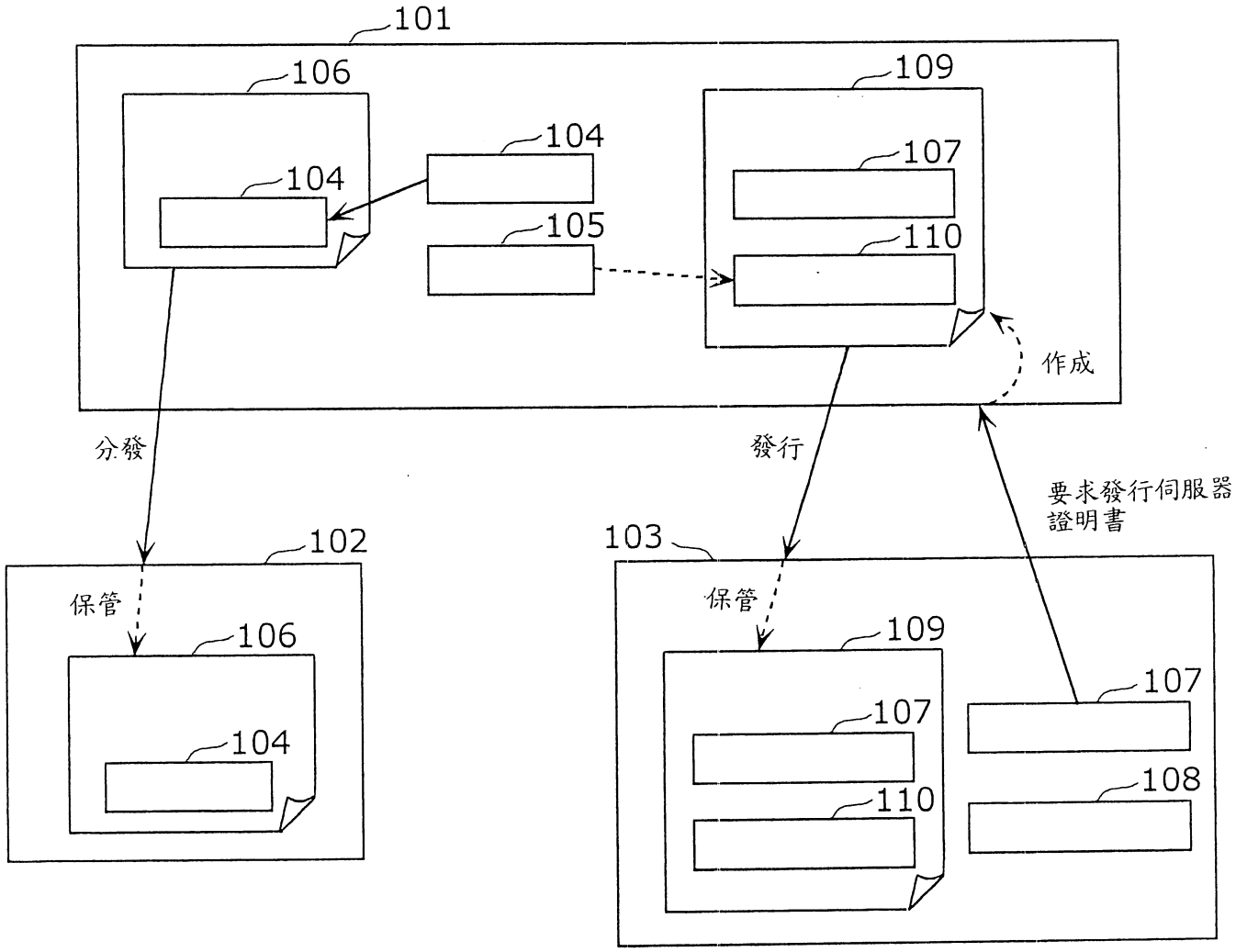
第 n 運作步驟，係使前述第 n 鑑認裝置運作者；及

第（n＋1）運作步驟，係在前述第 nCA 證明書之有效期限到期前，使前述第（n＋1）鑑認裝置及前述第（n＋1）下載伺服器運作者。

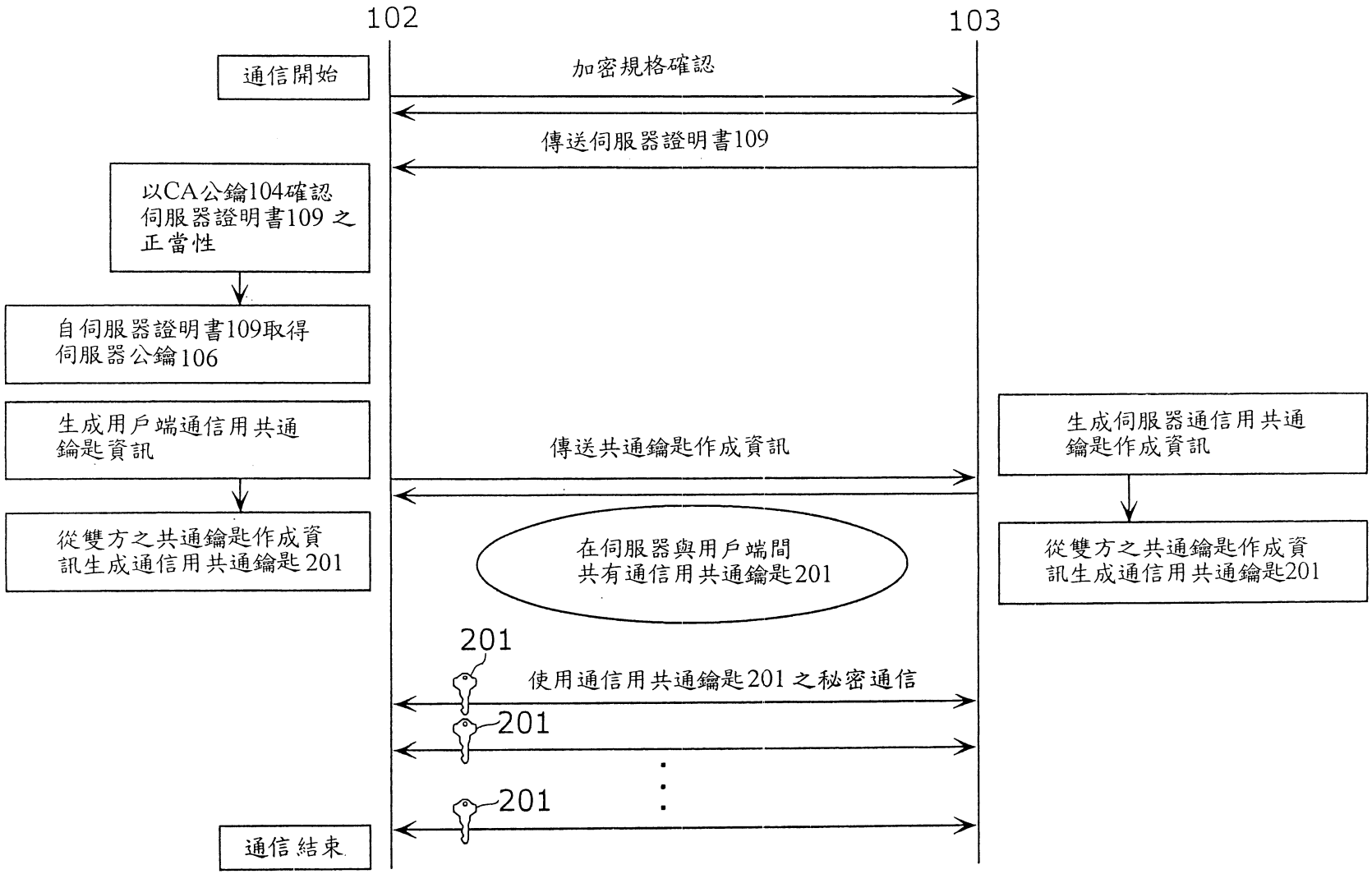
14. 如申請專利範圍第 13 項之運用方法，其中在前述第（n＋1）運作步驟中，當前述第 nCA 證明書失效時，使前述第（n＋1）鑑認裝置及前述第（n＋1）下載伺服器運作。

15. 如申請專利範圍第13項之運用方法，更具有結束步驟，係在前述第nCA證明書之有效期限屆滿後，使前述第n鑑認裝置及前述第（n＋1）下載伺服器之運作結束者。

第 1 圖

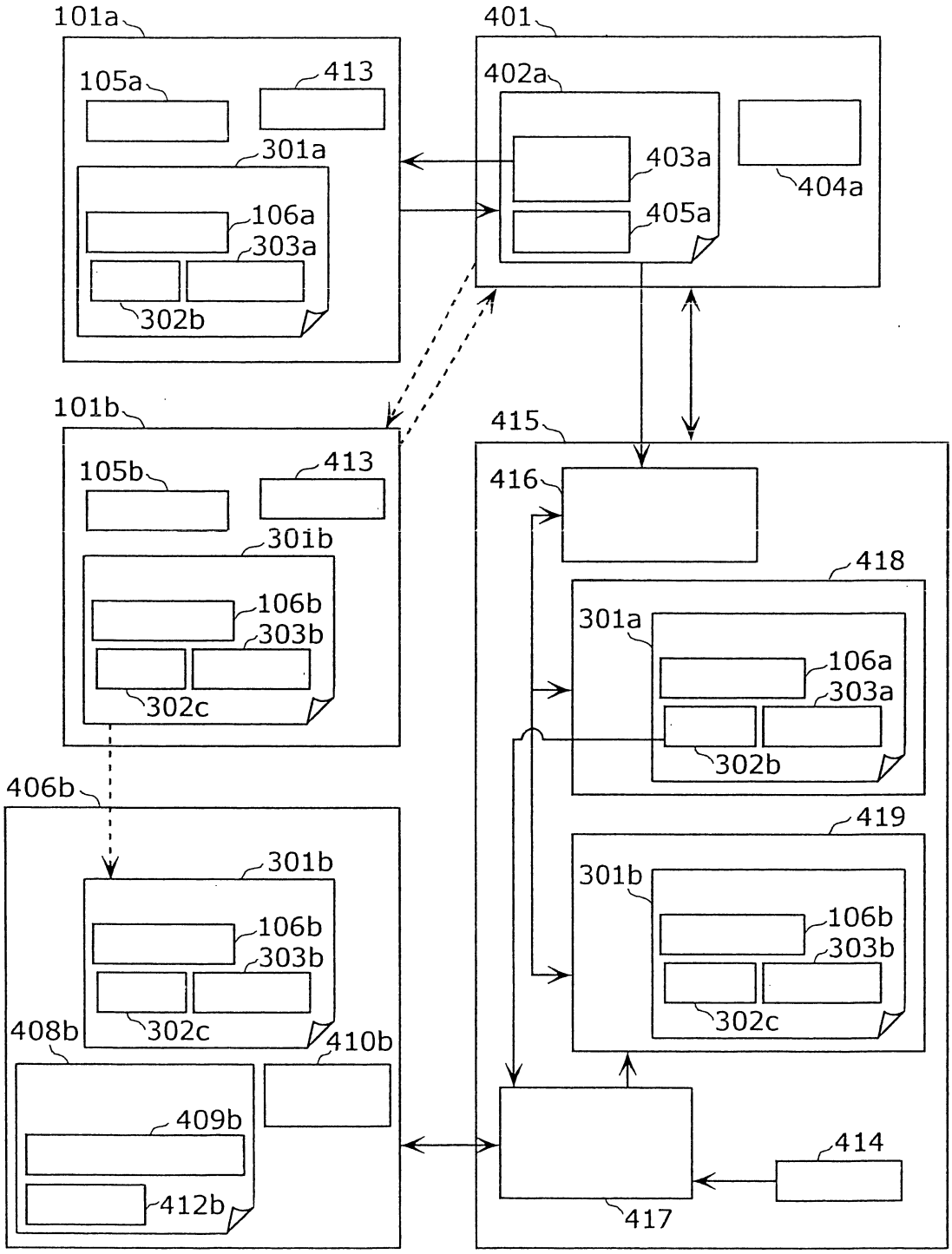


第 2 圖

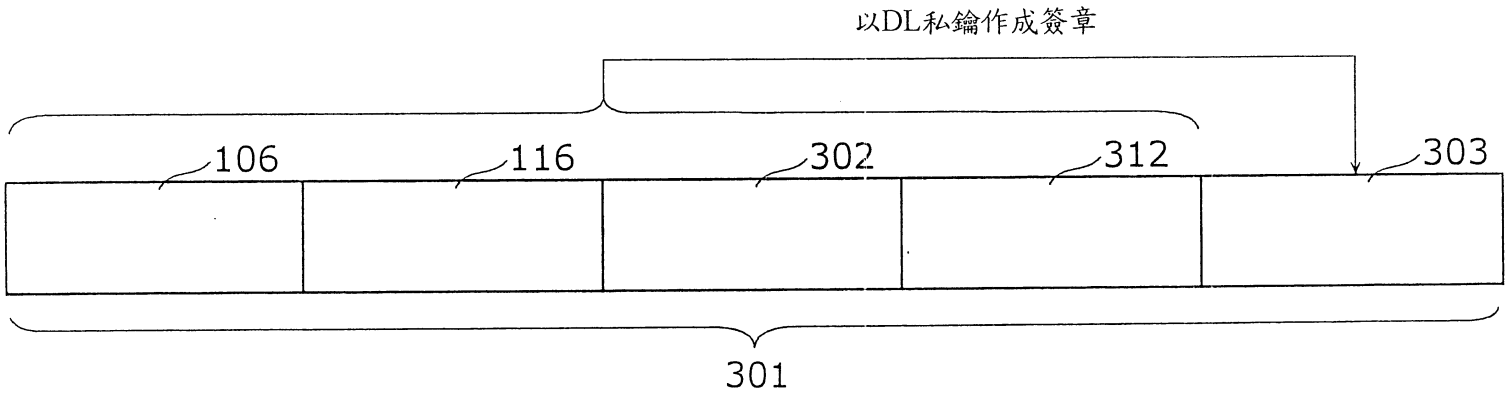


200423677

第 3 圖

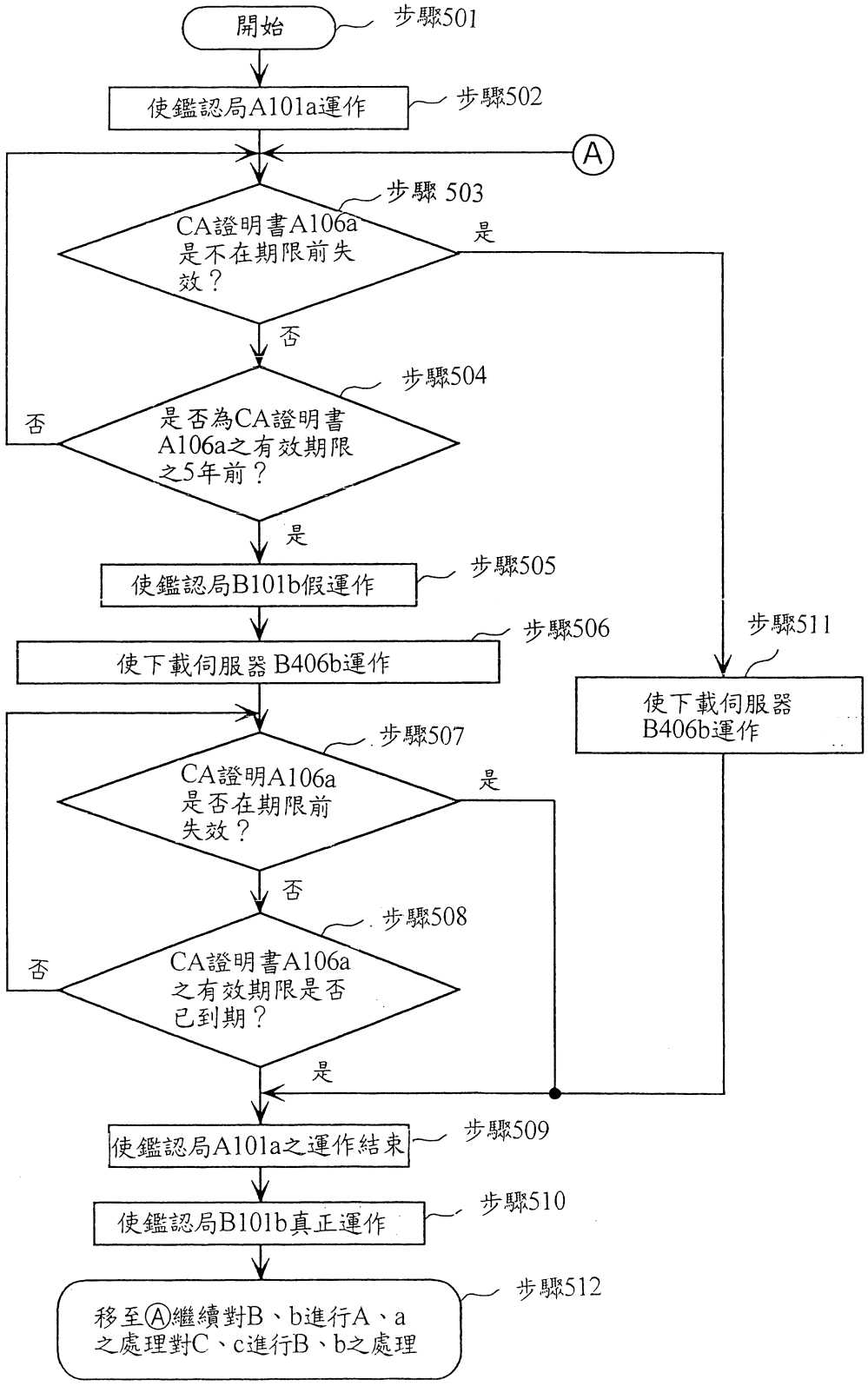

101a
105a
413
301a
106a
303a
302b
401
402a
403a
405a
404a
101b
105b
413
301b
106b
303b
302c
415
416
418
301a
106a
303a
302b
419
301b
106b
303b
302c
406b
301b
106b
303b
302c
408b
410b
409b
412b
414
417

第 4 圖

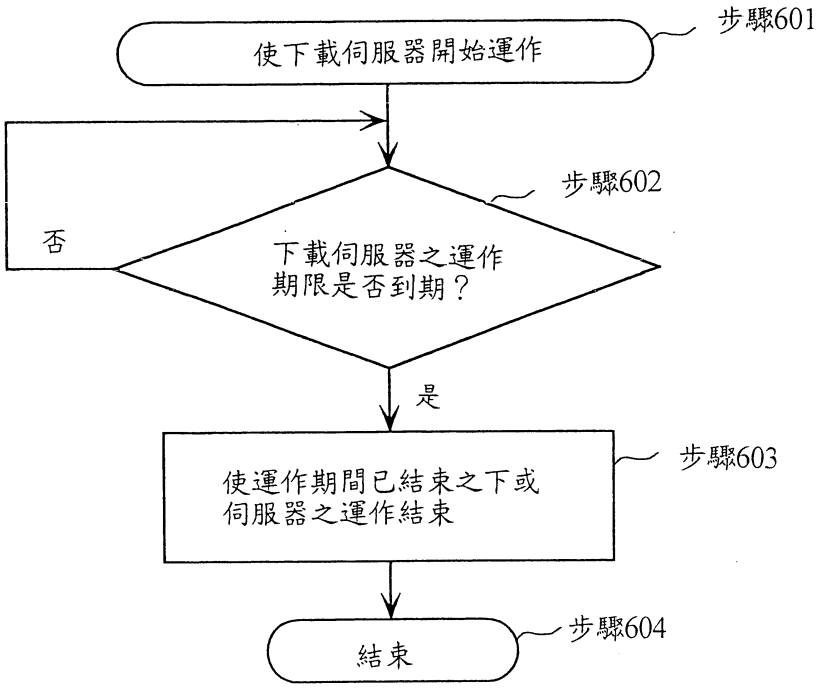


200423677

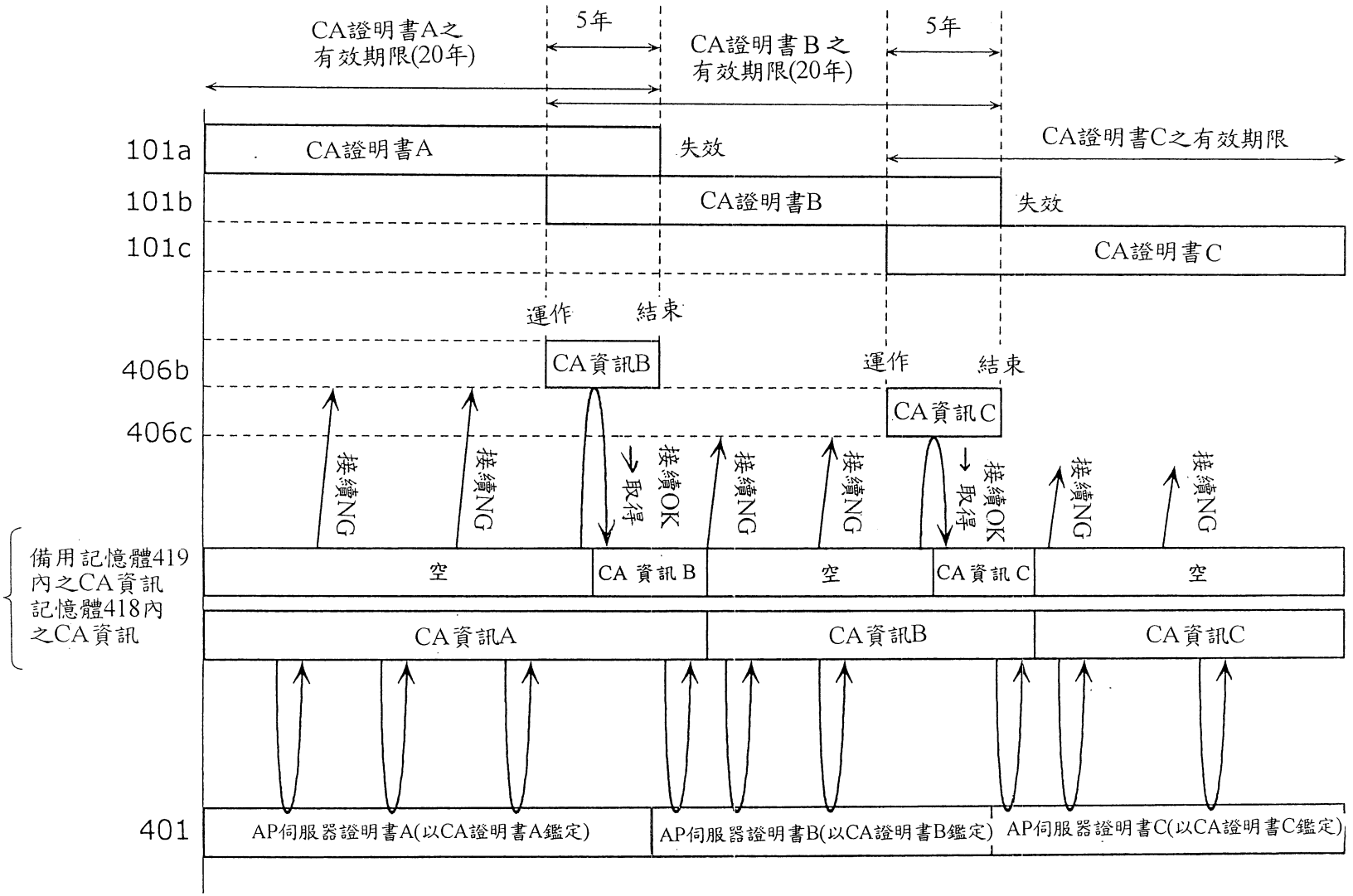
第 5 圖


開始
步驟501
使鑑認局A101a運作
步驟502
A
步驟 503
CA證明書A106a是不在期限前失效？
是
否
步驟504
否
是否為CA證明書A106a之有效期限之5年前？
是
使鑑認局B101b假運作
步驟505
使下載伺服器 B406b運作
步驟506
步驟511
使下載伺服器B406b運作
步驟507
CA證明A106a是否在期限前失效？
是
否
步驟508
否
CA證明書A106a之有效期限是否已到期？
是
使鑑認局A101a之運作結束
步驟509
使鑑認局B101b真正運作
步驟510
移至Ⓐ繼續對B、b進行A、a之處理對C、c進行B、b之處理
步驟512

第 6 圖

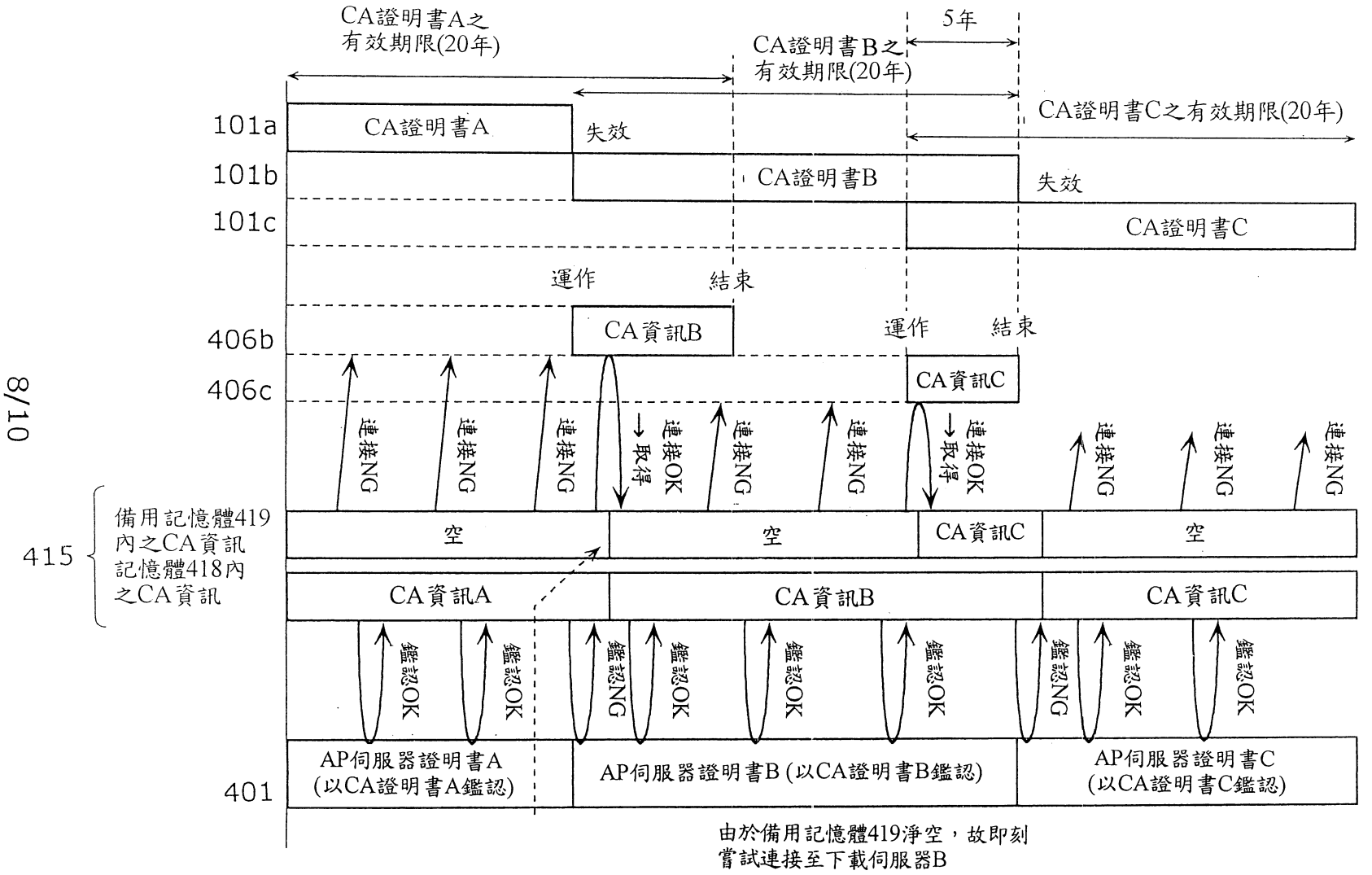

使下載伺服器開始運作
步驟601
步驟602
下載伺服器之運作
期限是否到期？
否
是
使運作期間已結束之下或
伺服器之運作結束
步驟603
結束
步驟604

第 7 圖



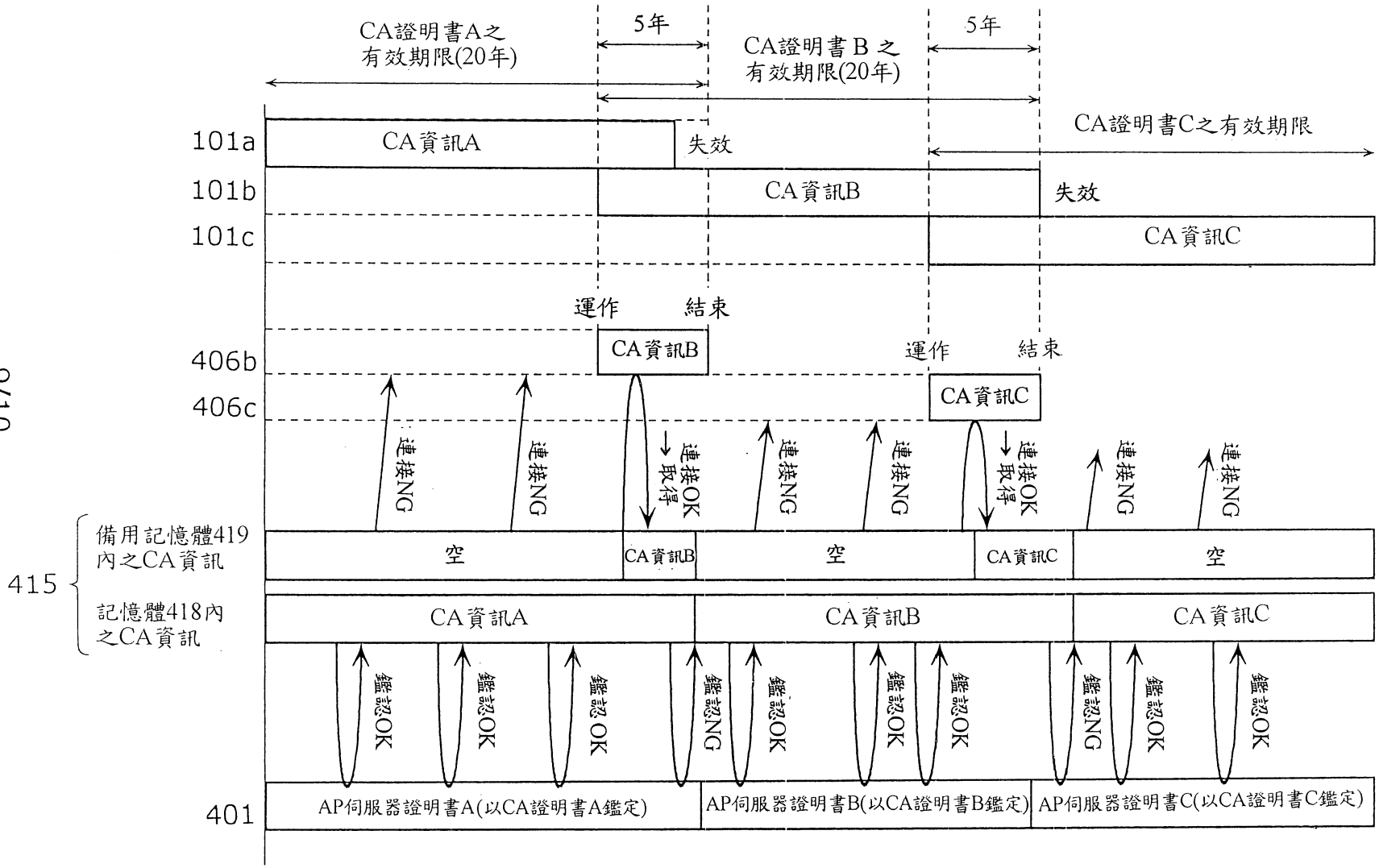
200423677

第 8 圖



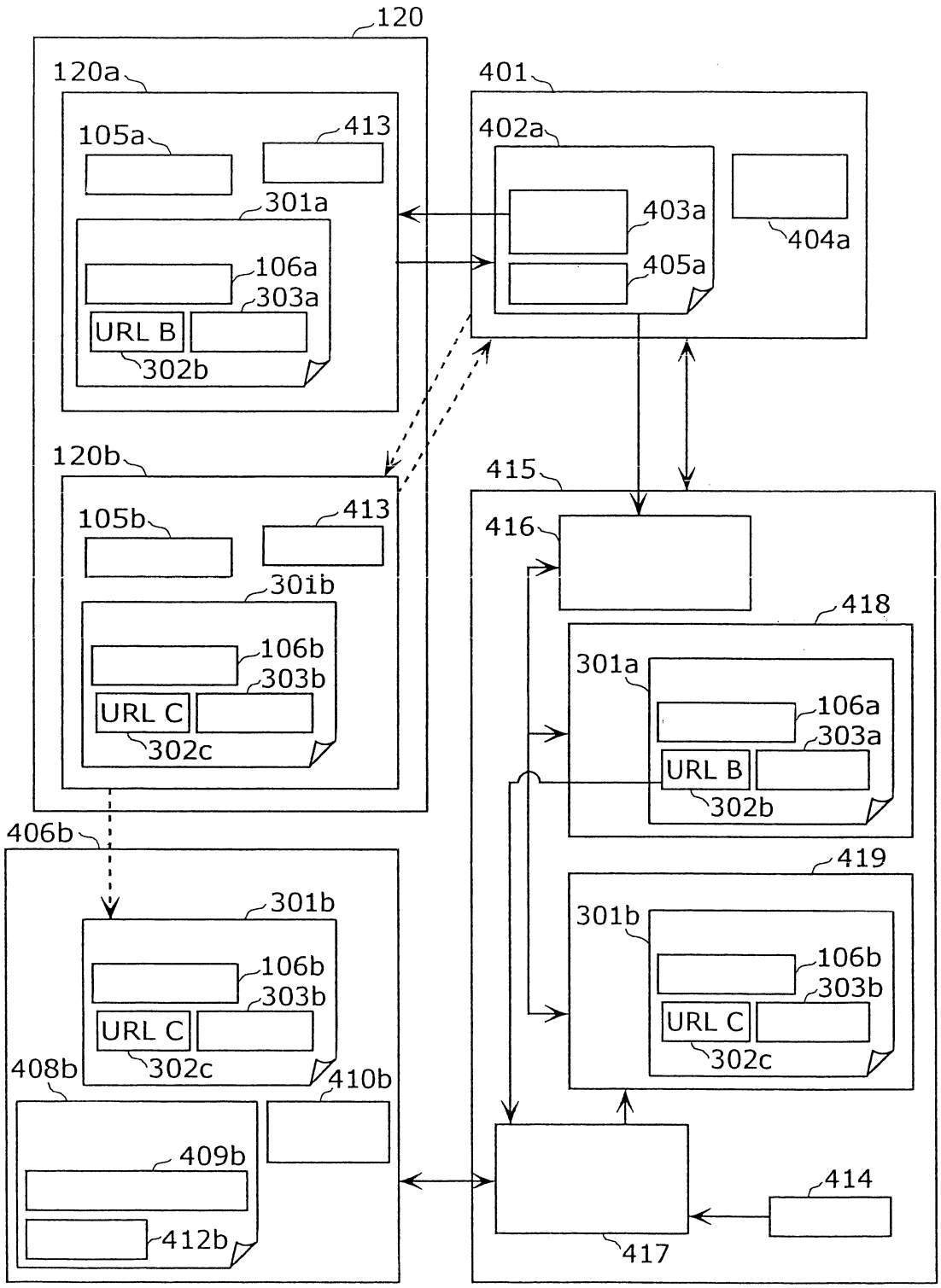
200423677

第 9 圖



200423677

第 10 圖


120
120a
105a
413
301a
106a
303a
URL B
302b
120b
105b
413
301b
106b
303b
URL C
302c
406b
301b
106b
303b
URL C
302c
408b
410b
409b
412b
401
402a
403a
404a
405a
415
416
418
301a
106a
303a
URL B
302b
419
301b
106b
303b
URL C
302c
414
417

柒、指定代表圖：

(一)本案指定代表圖為：第（ 7 ）圖。

(二)本代表圖之元件代表符號簡單說明：

101a...鑑認局A
101b...鑑認局B
101c...鑑認局C
401...應用伺服器
406b...下載伺服器B
406c...下載伺服器C
418...記憶體
419...備用記憶體

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：