（此處由本局於收文時黏貼條碼）

公告本

I252662

751580

發明專利說明書

（本申請書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※申請案號：93102546

※申請日期：93 年 02 月 04 日　　※IPC 分類：H04L 9/30

壹、發明名稱：

(中) 公鑰憑證驗證之高速化方法及裝置

(外) 公開鍵証明書検証の高速化方法および装置

貳、申請人：(共 1 人)

1.姓　名：(中) 日立製作所股份有限公司

(英) HITACHI, LTD.

代表人：(中) 1.庄山悅彥

(英)

地　址：(中) 日本國東京都千代田區神田駿河台四丁目六番地

(英)

國籍：(中英) 日本　JAPAN

參、發明人：(共 5 人)

1.姓　名：(中) 熊谷洋子

(英) 熊谷洋子

地　址：(中) 日本國東京都千代田區丸之內一丁目五番一號新丸大樓日立製作所（股）知的財產權本部內

(英) 日本国東京都千代田区丸の内一丁目５番１号新丸ビル㈱日立製作所知的財産権本部内

2.姓　名：(中) 藤城孝宏

(英) 藤城孝宏

地　址：(中) 日本國東京都千代田區丸之內一丁目五番一號新丸大樓日立製作所（股）知的財產權本部內

(英) 日本国東京都千代田区丸の内一丁目５番１号新丸ビル㈱日立製作所知的財産権本部内

3.姓　名：(中) 鍛忠司

(英) 鍛忠司

地　址：(中) 日本國東京都千代田區丸之內一丁目五番一號新丸大樓日立製作所（股）知的財產權本部內

（英）日本国東京都千代田区丸の内一丁目５番１号新丸ビル㈱日立製作所知的財産権本部内

4.姓　名：（中）羽根慎吾
（英）羽根慎吾
地　址：（中）日本國東京都千代田區丸之內一丁目五番一號新丸大樓日立製作所（股）知的財產權本部內
（英）日本国東京都千代田区丸の内一丁目５番１号新丸ビル㈱日立製作所知的財産権本部内

5.姓　名：（中）下之薗仁
（英）下之薗仁
地　址：（中）日本國東京都千代田區丸之內一丁目五番一號新丸大樓日立製作所（股）知的財產權本部內
（英）日本国東京都千代田区丸の内１丁目５番１号新丸ビル㈱日立製作所知的財産権本部内

肆、聲明事項:

◎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　；2003/10/10；2003-351509 ☑有主張優先權

（英）日本国東京都千代田区丸の内一丁目５番１号新丸ビル㈱日立製作所知的財産権本部内

4.姓　名：（中）羽根慎吾
（英）羽根慎吾
地　址：（中）日本國東京都千代田區丸之內一丁目五番一號新丸大樓日立製作所（股）知的財產權本部內
（英）日本国東京都千代田区丸の内一丁目５番１号新丸ビル㈱日立製作所知的財産権本部内

5.姓　名：（中）下之薗仁
（英）下之薗仁
地　址：（中）日本國東京都千代田區丸之內一丁目五番一號新丸大樓日立製作所（股）知的財產權本部內
（英）日本国東京都千代田区丸の内１丁目５番１号新丸ビル㈱日立製作所知的財産権本部内

肆、聲明事項:

◎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　；2003/10/10；2003-351509 ☑有主張優先權

(1)

玖、發明說明

【發明所屬之技術領域】

本發明係有關於，在公鑰基礎架構（Public Key Infrastructure：以下簡稱 PKI）中，關於針對某台終端所收到的電子手續的署名予以驗證所需之公鑰憑證，確認其有效性的適用技術。

【先前技術】

民間系、公共系之各式各樣的組織、團體中，先前，爲了讓書面進行的各種手續走向電子化，而積極進行 PKI 的導入、整備。

圖 12 係在 PKI 中，認證台（Certificate Authority：以下稱 CA）有複數個時，各 CA 之關係的例圖。

如圖所示，進行公鑰憑證之發行及其管理的各 CA，是具有以根 CA1 爲頂點之樹狀構造的群組。該群組係稱爲安全網域，是以一個政策管理機關爲依據而運用 PKI 的單位。根 CA1，係對其本身下 1 階位置的各 $CA2_1 \sim CA2_n$ 發行公鑰憑證。又，$CA2_1 \sim CA2_n$，係對其本身下 1 階位置的各 $CA3_1 \sim CA3_{n1}$ 發行公鑰憑證。如此，在樹狀結構上，位於上位的 CA 會對其本身下 1 階的 CA 發行公鑰憑證。然後，在樹狀結構上，位於最下位的 CA（以下稱爲終端個體憑證發行 CA）$CAs_1 \sim CAs_{nm}$，係對進行電子手續的使用者（終端個體：End Entity，以下稱 EE）$EE_1 \sim EE_x$ 發行公鑰憑證。

(2)

EE_1～EE_x各個裝置在電子文書之署名產生之際所使用的密鑰（署名鑰）的正當性，是以收容其本身的終端收容認證台CAs_1～CAs_{nm}所發行的公鑰憑證來證明之；終端收容認證台CAs_1～CAs_{nm}各個裝置所發行的公鑰憑證之署名產生之際所使用之密鑰的正當性，是以收容其本身的憑證台$CA(s-1)_1$～$CA(s-1)_{n(m-1)}$所發行的公鑰憑證來證明之。因此，EE_1～EE_x各個裝置在電子文書之署名產生之際所使用的密鑰，最終會藉由根認證台CA1所發行的公鑰憑證來證明。將該EE_1～EE_x之裝置在產生屬明之際所使用的密鑰的正當性最終予以證明的認證台，換言之，受到EE_1～EE_x所信賴，在樹上，最上位的CA稱爲信賴起點CA（trust anchor CA）。

再來，圖12中，EE_1裝置針對欲送信至EE_x裝置的電子文書，會以EE_1所保持之本身的密鑰進行署名。然後，有署名的電子文書中，附加有CAs_1所發行之和前記密鑰成對的EE_1的公鑰憑證，送信至EE_x裝置。

EE_x裝置，可將自EE_1裝置收取到電子文書之署名，使用添附在該當電子文書內的EE_1的公鑰憑證予以驗證。可是，由於EE_1的公鑰憑證並非EE_x之憑證發行CAs_{nm}所發行，因此，EE_x，若不經由本身的信賴起點CA也就是根CA1來確認其爲證明該當公鑰憑證的有效性，就無法信賴該當公鑰憑證。公鑰憑證之有效性確認處理，是用以下的程序而進行。（1）檢索出從信賴起點CA起至公鑰憑證發行源CA止的路徑：將信賴起點CA（此處爲根

CA1）當作起點 CA，調查起點 CA 所發行之公鑰憑證的發行目標，該當發行目標中含有 CA 的時候則再調查該當 CA 所發行之公鑰憑證的發行目標，持續上述處理直到該當公鑰憑證的發行目標，是含有 EE 憑證發行 CA（此處爲發行 EE_1 之公鑰憑證的 CAs_1）爲止，以檢索出自信賴起點 CA 起至 EE 憑證發行 CA 止的路徑。（2）檢索路徑的驗證：從上記（1）所檢索到的路徑上的各 CA 手中，取得該當 CA 對於路徑上之下一階側 CA 所發行過的公鑰憑證。然後，將有效性確認對象之公鑰憑證（此處爲，對 EE 憑證發行 CAs_1 發行的公鑰憑證）的署名，以發行該當公鑰憑證的 CA（此處爲 EE 憑證發行 CAs_1）之上 1 階 CA 所發行之公鑰憑證來予以驗證，當能夠驗證時，則將該當上 1 階 CA 所發行之公鑰憑證的署名再以更上 1 階的 CA 所發行的公鑰憑證來予以驗證，持續該處理直到該當上 1 階 CA 是信賴起點 CA 爲止。然後，當此種公鑰憑證之署名驗證到達了信賴起點爲止時，就能確認有效性確認對象之公鑰憑證的有效性。

EE_x 裝置，可將自 EE_1 裝置收取到電子文書之署名，使用添附在該當電子文書內的 EE_1 的公鑰憑證予以驗證，同時，藉由按照上記（1）、（2）之程序確認該當電子文書之署名驗證所使用的 EE1 的公鑰憑證之有效性，而可確認該當電子文書的正當性。

此外，以上當中，是以公鑰憑證的有效性確認處理是在 EE 裝置上進行爲前提。可是，公鑰憑證的有效性確認

處理的負荷很重，爲了使其在 EE 上進行，該當 EE 裝置需要有高處理能力。於是，制定有關網際網路各種技術之標準化的團體 IETF（Internet Engineering Task Force）提出，在設置一透過網路連接 EE 裝置的憑證有效性確認台（Validation Authority，以下稱 VA），在該當 VA 裝置中，替代該當 EE 來進行公鑰憑證的有效性確認。在 VA 裝置中進行公鑰憑證的有效性確認時，首先，EE 裝置會將公鑰憑證的有效性確認的委託，發送至 VA 裝置。接著，在 VA 裝置上，進行上記（1）、（2）之處理，最後，將其結果送至 EE 裝置。

此時，爲了縮短 EE 裝置從發出公鑰憑證的有效性確認之委託起，至獲知其結果爲止的所費時間，而有以下方法被提出。

在 VA 裝置中，事先定期地將路徑予以檢索，並登錄在路徑資料庫中存放。然後，當有某台 EE 裝置送來公鑰憑證的有效性確認之委託時，就在 VA 裝置的路徑資料庫中，檢索出對應的路徑，並將檢索到的路徑進行驗證，藉此以確認前記公鑰憑證的有效性（例如參照專利文獻 1）。

另一個方法是，在 VA 裝置中，事先定期地將所有路徑予以檢索，並將檢索到的路徑進行驗證。只有驗證成功的路徑（有效路徑），才會登錄在路徑資料庫保存。然後，當有某台 EE 裝置送來公鑰憑證的有效性確認之委託時，就調查在 VA 裝置的路徑資料庫中，是否有對應路徑被

(5)

登錄，藉此確認前記公鑰憑證的有效性（例如參照專利文獻 2）

〔專利文獻 1〕

美國專利第 6134550 號說明書

〔專利文獻 2〕

美國專利申請公開第 2002/046340 號說明書

【發明內容】

〔發明所欲解決之課題〕

上記專利文獻 2 所記載的方法中，係當收到來自 EE 裝置之公鑰憑證的有效性確認委託所對應的路徑，不存在於路徑資料庫中時，就判斷有效性確認對象憑證爲並非有效者。可是，若依照此方法，當路徑檢索時不存在的路徑，在收到來自 EE 裝置之公鑰憑證的有效性確認委託之時又重新存在的情況下，有效的公鑰憑證就會被判斷成無效。上記專利文獻 2 中，並未記載有關此種情況之處理。

又，上記專利文獻 1 中，也未記載有關當收到來自 EE 裝置之公鑰憑證的有效性確認委託所對應的路徑，並未登錄在路徑資料庫中時之處理。

如此，當 VA 所收到之有效性確認委託所對應的路徑並未登錄在路徑資料庫中時，藉由重新進行路徑檢索、驗證，就可將適切的結果予以回應。但是，此情況之有效性確認處理的時間太長，是爲課題。

目前，民間、公共體系之各種組織、團體中，都在積

極進行PKI的導入、整被，可以預想其結果爲，多數的安全網域並列存在，而變成複雜的PKI構成。甚至，一旦利用PKI的應用軟體普及，可預想到將來會有許許多多的有效性確認委託。此種狀況下，從EE開始委託公鑰憑證的有效性確認起，至獲知其結果爲止所耗費的時間會越來越長，導致服務品質的下降。

〔用以解決課題之手段〕

本發明係提供，當路徑檢索時不曾存在的路徑，在路徑檢索時以後才形成的情況下，也能回應適切的結果之技術，及／或使得EE開始委通公鑰憑證的有效性確認起至獲知結果爲止的所費時間更爲縮短之技術。

具體而言，本發明中，透過網路連接至複數終端裝置（EE裝置）或CA裝置的VA裝置，係反應某台EE裝置的委託，而進行用來確認公鑰憑證之有效性的以下處理。

關於因發行公鑰憑證而被賦予關係的所有CA，將所有存在的路徑予以檢索，並針對前記路徑檢索所偵測到的路徑進行驗證。又，將位於所測得之路徑之端點的EE憑證發行CA之，關於其所發行之EE憑證的憑證撤銷清單（Certificate Revocation List，以下稱爲CRL）予以取得。針對所取得之CRL，除了確認該當CRL是否爲有效期限內，還藉由該當CRL之發行CA的公鑰憑證，進行該當CRL的署名驗證。然後，將可驗證的路徑，和不可驗證的路徑，予以分類，登錄在路徑資料庫中。該路徑資料庫作

成處理，是獨立於從 EE 來的公鑰憑證的有效性確認委託，而按照所定的規則，重複進行，例如定期地進行。

然後，當有來自某台 EE 的公鑰憑證的有效性確認委託時，調查對應於其的路徑，是否已經登錄在路徑資料庫中，若是有在路徑資料庫中被登錄成可驗證之路徑，則使用已登錄在路徑資料庫中的 CRL，確認該當公鑰憑證是否失效，藉此以確認該當公鑰憑證之有效性。

另一方面，對應該當公鑰憑證的路徑，若是以無法驗證之路徑而被登錄在路徑資料路徑資料庫時，則調查是否有除了該當登錄之非有效路徑外，還有其他有效路徑；當爲不存在時，則認定該當公鑰憑證係無法驗證。當有新的路徑或 CRL 被偵測出來的時候，則使用該當路徑或 CRL 來確認公鑰憑證的有效性，並將該當驗證結果，一併追加登錄至路徑資料庫。

又，當有效性確認委託之公鑰憑證所對應之路徑或 CRL，並未登錄在路徑資料庫中時，藉由重新進行路徑或 CRL 之檢索、驗證處理，以確認上記公鑰憑證之有效性。此時，當有新的路徑或 CRL 被偵測出時，則將該當路徑或該當 CRL 的驗證結果，一併追加登錄至路徑資料庫。

若根據本發明，則當收到來自 EE 的公鑰憑證的有效性確認委託時，即使當路徑檢索時之後有新路徑形成的情況下，上記（1）、（2）所示，該當 EE 之信賴起點 CA 起至該當公鑰憑證之 EE 憑證發行 CA 止的路徑之檢索、已偵測出之路徑的驗證，以及對應於該當公鑰憑證的 CRL

之署名的驗證，就沒有必要進行。又，當對應於有效性確認委託的路徑，是被登錄成無法驗證之路徑時，則只需進行路徑檢索、驗證，較少的處理即可。因此，從某台 EE 開始委託公鑰憑證的有效性確認起，至該當有效姓被確認爲止的所需時間，可以縮短。

【實施方式】

圖 1 係本發明之一實施形態所適用之 PKI 系統的概略構成圖。

本實施形態之 PKI 系統，係由：進行電子手續之複數 EE_1 裝置（11）～EE_N 裝置（11）（總稱爲 EE 裝置（11））），及進行公鑰憑證發行業務的 CA_1 裝置（13）～CA_M 裝置（13），及公鑰憑證之有效性確認台 VA（14），及將其分別予以連接的網際網路等之網路（以下稱爲 NET）16 所構成。

圖 2 係圖 1 所示 PKI 系統中之各 CA 的關係之一例圖。

如圖所示，本實施形態的 PKI 系統，是以民間係民間系、政府系這類複數安全網域 SD（SD1～SD2）並存爲前提。又，各安全網域 SD 之根 CA（圖 2 中爲 CA_{11}、CA_{21}），係例如，除了對橋接認證台 CAbridge 發行公鑰憑證，還取得自 CAbridge 發行之公鑰憑證，而和 CAbridge 之間進行相互驗證。藉此，隸屬於某安全網域 SD 之 CA 和隸屬於其他安全網域 SD 之 CA 彼此間，就形成了一個路

徑，其爲可用來將某一方 CA 所發行之公鑰憑證的有效性，在另一方 CA 上確認。

接著，針對構成圖 1 之 PKI 系統的各裝置予以說明。

首先，使用圖 3 來說明 EE 裝置（11）。

EE 裝置（11），係具有：處理部 30a 和記憶部 30b，及用來透過 NET16 和其他裝置進行通訊之通訊部 30c，及使用者（EE）所作成之電子文書或從其他 EE 所收到的電子文書之輸出入或接受來自使用者之指示的的輸出入部 30d。

處理部 30a，係具有：對電子文書產生署名的署名產生部 31，及進行署名之驗證的的署名驗證部 32，及統籌控制 EE 裝置之各部的控制部 33。

記憶部 30b，係具有：將利用者所作成之電子文書予以保持的電子文書保持部 34，及密鑰（署名鑰），及與此成對之公鑰的公鑰憑證，及將運用該當 EE 裝置之 EE 信賴 CA 之自我署名憑證予以保持的金鑰保持部 35，及將自其他 EE 所收取之附有署名的電子文書和公鑰憑證予以保持的驗證對象保持部 36。

在此種構成中，控制部 33，係一旦透過輸出入部 30d，收到指示要將保持在電子文書保持部 34 中的某件電子文書送信至其他 EE 之指示，則將該當電子文書自電子文書保持部 34 讀出，將其交予署名產生部 31。署名產生部 31，係使用被保存在金鑰保持部 35 的密鑰而對所交付的該當電子文書產生署名。

控制部 33，係在自電子文書保持部 34 讀出之電子文書中附上署名產生部 31 所產生的署名，作成附有署名的電子文書，並將所作成之附有署名的電子文書和金鑰保持部 35 中所保持的公鑰憑證，透過通訊部 30c、送信至使用者所指示的送信目標之 EE 裝置。控制部 33，係一旦透過通訊部 30c，收取到來自其他 EE 裝置之附有署名的電子文書和公鑰憑證，則除了將它們賦予關連而保持在驗證對象保持部 36 中，還將驗證它們之要求通知予署名驗證部 32。

署名驗證部 32 收到該要求後，將保持在驗證對象保持部 36 中的附有署名的電子文書的署名，使用對應之公鑰憑證而予以驗證。署名驗證部 32，係將上記署名驗證所用的公鑰憑證之有效性確認委託，送信至 VA 裝置（14）。此時，因應所需，可在前記確認委託中，包含有藉由前記附有署名的電子文書所欲進行之電子程序之相關原則（policy）（例如，交易額等之信賴度）的驗證委託。然後，在 VA 裝置（14）上，只有當亦含有上記原則之驗證的該當公鑰憑證之有效性是已被確認時，才將附有署名的電子文書視爲正當者，因應所需而自輸出入部 30d 輸出。

接著，使用圖 4 說明 CA 裝置（13）。

CA 裝置（13），係具備：處理部 40a、記憶部 40b、用來透過 NET16 和其他裝置進行通訊之通訊部 40c，及公鑰憑證等輸出入或接受來自該當裝置之操作者之指示或進行處理結果之輸出的輸出入部 40d。

處理部 40a，係具有：發行公鑰憑證之發行部 41，及管理發行部 41 所發行之公鑰憑證的管理部 42，及統籌控制 EE 裝置之各部的控制部 43。

記憶部 40b，係具有：將發行部 41 所發行之公鑰憑證予以保持的公鑰憑證資料庫 44，及將記述著公鑰憑證資料庫 44 所保持之各公鑰憑證之發行目標的發行目標管理清單予以保持的發行目標管理清單保持部 45，及失效憑證清單保持部 46。

此種構成中，控制部 43，一旦透過輸出入部 40d 或通訊部 40c 收到公鑰憑證之發行委託時，則將該要旨傳達至發行部 41。發行部 41 在收到此後，針對其產生公鑰憑證。此時，會以 CA 的密鑰在公鑰憑證加上署名。又，因應所需，在公鑰憑證，可以記述有：該當公鑰憑證的有效期限、非信賴之其他認證台的名稱（Name Constraints）、該當公鑰憑證之有效性確認所能容許之最大路徑常（路徑上容許之最大認證台數）、表示電子手續之交易額等原則。然後，所產生的公鑰憑證透過輸出入部 40d 或通訊部 40c，藉由郵寄或通訊，交付至發行委託源。又，除了將該公鑰憑證登錄至公鑰憑證資料庫 44 以外，還將該發行目標（也就是發行依賴源）的資訊，記錄在發行目標管理清單保持部 45 所保持之發行目標管理清單中。

控制部 43，係一旦透過輸出入部 40d 或通訊部 40c，收取到公鑰憑證之失效委託，則將該要旨傳達至管理部 42。管理部 42 收到此後，除了將失效對象的公鑰憑證從

公鑰憑證資料庫 44 中予以刪除，還將該當公鑰憑證的發行目標之資訊，從發行目標管理清單保持部 45 所保存之發行目標管理清單中刪除。然後，管理部 42，會定期地作成記述著因失效委託而自公鑰憑證資料庫 44 刪除之公鑰憑證的相關資訊的失效憑證清單，並將其保持在失效憑證清單保持部 46。此外，管理部 42，在所作成之失效憑證清單中，還記述有下次失效憑證清單的作成預定時間。

此外，控制部 43，係一旦透過通訊部 40c，收取到來自其他裝置的公鑰憑證之失效資訊之詢問時，便檢索失效憑證清單保持部 46 所保持的失效憑證清單，調查所詢問之公鑰憑證是否已經失效。然後，能將其結果，透過通訊部 40c，回答至來詢問的其他裝置。（此種詢問和回答所使用的通訊協定有，OCSP（Online Certification Status Protocol））。

管理部 42，係調查被存放在公鑰憑證資料庫 44 中的各公鑰憑證之有效期限，並將超過有效期限的公鑰憑證之發行目標資訊，自發行目標管理清單保持部 45 所保持之發行目標管理清單中刪除。

接著，使用圖 5，說明 VA 裝置（14）。

如圖所示，VA 裝置（14），係具有：處理部 50a、記憶部 50b、用來透過 NET16 和其他裝置進行通訊之通訊部 50c、進行公鑰憑證等之輸出輸入或接受來自使用者之指示的輸出入部 50d。

處理部 50a，係具備：路徑檢索部 51、路徑驗證部

52、有效期限／失效狀態調查部 53、有效性確認部 54，及統籌控制 VA 裝置之各部的控制部 55。又，記憶部 50b，具有：路徑資料庫 56、失效憑證清單作成預定日時資料庫 57。其中路徑資料庫 56，係具有：有效路徑資料庫 56A、非有效路徑資料庫 56B。

路徑檢索部 51，係例如定期地，將任意 CA 視爲信賴起點 CA，檢索出從該當信賴起點 CA 起，至發行 EE 憑證的所有 EE 憑證發行 CA 爲止的路徑，並取得所偵測之路徑的 EE 憑證發行 CA 所發行之 EE 憑證相關失效憑證清單（CRL）。信賴起點 CA，係所有 CA，或可藉由設定而將一部份 CA 視爲信賴起點 CA，來進行檢索。

路徑驗證部 52，係路徑檢索部 51 每次進行路徑檢索時，就進行該當路徑檢索部 51 所偵測到之路徑的驗證。又，當路徑檢索部 51 能夠取得對應於該當路徑的 CRL 時，就進行該當 CRL 的驗證。然後，位於該當路徑之兩端的信賴起點之名稱、EE 憑證發行 CA 之名稱的配對，將其對應於構成該當路徑之各 CA 名、各憑證及 EE 憑證相關之 CRL，反映該當驗證結果，登錄在有效路徑資料庫 56A，或是非有效路徑資料庫 56B。

有效期限／失效狀態調查部 53，係針對被登錄在有效路徑資料庫 56A 之每一路徑，調查構成該當路徑的各公鑰憑證之有效期限或有無失效。然後，因應該當結果來更新路徑資料庫 56。又，有效期限／失效狀態調查部 53，係將從各 CA 之失效憑證清單保持部 46 所取得之失效

憑證清單所描述之下次失效憑證清單作成預定日時，對應於CA，登錄至失效憑證清單作成預定日時資料庫57中。

有效性確認部54，係依從EE裝置來的委託，將信賴起點CA視爲信賴的起點，進行公鑰憑證的有效性確認。

此外，圖3～圖5所示之每一台EE裝置（11）、CA裝置（13）和VA裝置（14），係例如，如圖6所示，具備CPU61、記憶體62、硬碟等外部記憶裝置63、自CD－ROM等具有可攜性之記憶媒體69讀取資訊的讀取裝置64、用來透過NET16和其他裝置進行通訊之通訊裝置65、鍵盤或滑鼠等輸入裝置66、顯示器或印表機等輸出裝置67，以及和這些裝置進行資料收授的介面68，是可在一般的電子計算機上就能構築。

然後，藉由CPU61執行從外部記憶裝置63載入至記憶體62上的所定程式，就可實現上述各部處理。亦即，通訊部30c、40c、50c，係藉由CPU61利用通訊裝置65而實現；輸出入部30d、40d、50d，係藉由CPU61利用輸入裝置66或輸出裝置67或讀取裝置64而實現；而且記憶部30b、40b、50b，係藉由CPU61利用記憶體62或外部記憶裝置63而實現。又，處理部30a、40a、50a，係以CPU61之處理程序而實現。

上記之所定程式，可事先存放在外部記憶裝置63，或可存放在上記電子計算機可利用之記憶媒體69內，透過讀取裝置64，因應所需而讀出，或是，亦可爲屬於上記電子計算機可利用之通訊媒體的網路或從連接在網路上

利用載波傳輸之其他裝置，因應所需而下載，導入外部記憶裝置 63 者。

接著，說明上記構成之 VA 裝置（14）的動作。

本實施形態之 VA 裝置（14）的動作，係分成路徑檢索、驗證及管理動作，以及公鑰憑證的有效性確認動作。

使用圖 7～圖 8 的流程圖，說明 VA 裝置（14）上所進行之路徑檢索、驗證及管理動作。

控制部 55，係一旦經過了 VA 之營運者所制定之所定時間（例如 1 日）（步驟 S1001），則將路徑資料庫 56 之登錄內容予以清除（步驟 S1002），並向路徑檢索部 51 委託路徑檢索。路徑檢索部 51 收到此後，就將任意 CA 視爲信賴起點 CA，檢索至 EE 憑證發行 CA 爲止之路徑（步驟 S1003）。

具體而言，路徑檢索部 51，係存取信賴起點 CA，將憑證管理中心所發行、保持在發行目標管理清單保持部 45 之公鑰憑證的發行目標資訊予以取得。然後，當所獲得之各發行目標爲 CA 時，則存取各發行目標，再調查被保持在發行目標管理清單保持部 45 之，各 CA 所發行之公鑰憑證的發行目標。此處理，會一直持續直到公鑰憑證的發行目標爲 EE 爲止，藉此以檢索出自信賴起點 CA 起至 EE 憑證發行 CA 爲止之路徑。此處，爲了防止路徑回圈造成上記處理無限循環，而當自某台 CA 獲得之發行目標中，是含有已經存在於目前爲止已經形成之部份路徑之 CA 時，就不進行將該當 CA 視爲發行目標之上記處理，

並取得曾經向位於路徑端點之 EE 發行過憑證的 CA 所發行之 CRL。

步驟 S1003 中之路徑檢索處理，以圖 2 表示之各 CA 的關係爲例，進行更具體之說明。

首先，路徑檢索部 51，將信賴起點 CA 視爲 CAbridge 而進行路徑檢索。路徑檢索部 51，係存取 CAbridge，取得被保持在發行目標管理清單保持部 45 中之，CAbridge 所發行過的公鑰憑證的發行目標之資訊，也就是 CA_{11}、CA_{21} 的資訊。

接著，路徑檢索部 51，會注目在從 CAbridge 所獲得之發行目標（CA_{11}、CA_{21}）中之其中任一者，執行以下之處理。亦即，若注目之發行目標爲 CA（以下將其稱爲注目 CA），則設定 CAbridge－注目 CA 此一部份路徑。然後，存取注目 CA 之發行目標管理清單保持部 45，再取得該當注目 CA 已發行過公鑰憑證之發行目標之資訊。此處，若令受注目的發行目標爲 CA_{11}，則設定 CAbridge－CA_{11} 此一部份路徑，並從 CA_{11}，取得發行目標資訊，也就是 CAbridge、CA_{12}、CA_{13} 之資訊。

接著，路徑檢索部 51，會調查在從認證台 CA_{11} 獲得之發行目標（CAbridge、CA_{12}、CA_{13}）中，是否含有部份路徑上之 CA（以下稱作回圈 CA）。當含有時則將發行目標排除在注目對象以外。因此，此處，會將 CAbridge 排除在注目對象以外。接著，路徑檢索部 51，會調查從 CA_{11} 所獲得之發行目標中是否含有 EE。當某台 CA 所發

行憑證的發行目標中含有 EE 時，該 CA 就成爲 EE 憑證發行 CA。可是，由於從 CA_{11} 所獲得之發行目標中並未含有 EE，因此 CA_{11} 並非 EE 憑證發行 CA。因此，CAbridge－CA_{11} 此一部份路徑，會一直延長直到 EE 憑證發行 CA 爲止，而注目在從 CA_{11} 所獲得之回圈 CA 除外的發行目標（CA_{12}、CA_{13}）之中的任何一者。

若已注目之發行目標爲 CA，則將連接該注目 CA 的部份路徑，設定在至其爲止已設定之部份路徑中。然後，存取該 CA 之發行目標管理清單保持部 45，再取得該當注目 CA 已發行過之公鑰憑證的發行目標之資訊。此處，假設已注目之發行目標爲 CA_{12}，則設定 CAbridge－CA_{11}－CA_{12} 此一路徑，從 CA_{12} 取得發行目標之資訊，也就是 EE_1、EE_2。

接著，路徑檢索部 51，會調查從 CA_{12} 取得之發行目標（EE_1、EE_2）當中，是否含有回圈 CA。若含有時則將該發行目標排除在注目對象以外。此處，由於不含有回圈 CA，因此路徑檢索部 51 會進入下一處理，調查從 CA_{12} 取得之發行目標當中，是否含有 EE。此處，由於所取得之發行目標全部都是 EE，因此 CA_{12} 就是 EE 憑證發行 CA。於是，就將該 CA_{12} 視爲端點的路徑，偵測成從信賴起點 CAbridge 起，至 EE 憑證發行 CA_{12} 爲止之路徑（CAbridge－CA_{11}－CA_{12}）。

再者，路徑檢索部 51，當偵測出至 EE 憑證發行 CA 爲止的路徑時，會存取失效憑證清單保持部 46，取得將

該當 EE 憑證發行 CA_{12} 所發行之 CRL。

接著，路徑檢索部 51，會調查從位於所偵測到之路徑上之端點的 CA_{12} 取得之發行目標資訊中，是否含有還未注目的發行目標（回圈 CA 以外之 CA），若還有此種發行目標，則將其視爲注目 CA，持續上記處理。另一方面，若沒有此種 CA，則調查從位於前一位置之 CA_{11} 取得之發行目標資訊中，是否含有還未注目的發行目標（回圈 CA 以外之 CA）。然後，若還有此種發行目標，則將其視爲注目 CA，持續上記處理。此處，因爲從 CA_{11} 取得之發行目標資訊中，CA_{13} 仍未受到注目，因此藉由將其視爲注目 CA 而進行上記處理，偵測出從 CAbridge 至 EE 憑證發行 CA_{13} 爲止的路徑（CAbridge－CA_{11}－CA_{13}）以及 CA_{13} 所發行之 CRL。

如此，路徑檢索部 51，係針對位於所偵測路徑上之每台 CA，持續進行上記處理，直到從該當 CA 所取得之發行目標資訊中，都沒有仍未被注目之發行目標（回圈 CA 以外之 CA），以偵測出從 CAbridge 至 EE 憑證發行 CA 爲止的路徑。

以上，是將任意 CA 視爲信賴起點 CA 時的步驟 S1003 之處理。

如後述，關於將 CA_{11}、CA_{21} 分別視爲信賴起點 CA 時，也是同樣地進行路徑檢索。

控制部 55，係一旦路徑檢索部 51 偵測出路徑（步驟 S1004 爲 Yes），則向路徑驗證部 52 委託路徑之驗證。路

徑驗證部 52 收到此後，就進行路徑檢索部 51 所測出之路徑的驗證（步驟 S1005）。

具體而言，是針對路徑檢索部 51 所測出之每一路徑，進行以下處理。

亦即，首先，路徑驗證部 52，係存取至路徑上之各 CA 的公鑰憑證資料庫 44，將各 CA 對於位在該當路徑上之下一 CA（存取目標 CA 爲 EE 憑證發行 CA 時則爲 EE）所發行過之公鑰憑證予以取得。

接著，路徑驗證部 52，係將位於路徑最後之 EE 憑證發行 CA 所發行之公鑰憑證的署名，以 EE 憑證發行 CA 之公鑰憑證進行驗證，當可驗證時則將該當 EE 憑證發行 CA 之公鑰憑證的署名再以前一位置之 CA 的公鑰憑證進行驗證。持續該處理直到該當前一位置之認證台成爲信賴起點 CA 爲止，以驗證該當路徑。再者，關於該當 EE 憑證發行 CA 所發行的 CRL，是以該當 EE 憑證發行 CA 之公鑰憑證來予以驗證。

例如，圖 2 中，當要驗證從 CAbridge 至 EE 憑證發行 CA_{12} 爲止之路徑（CAbridge－CA_{11}－CA_{12}）以及 CRL 時，首先，將 EE 憑證發行 CA_{12} 之公鑰憑證之署名，使用路徑中之 CA_{12} 之前一位置之 CA_{11} 之公鑰憑證來予以驗證。然後，當能夠驗證時，就將 CA_{11} 之公鑰憑證的署名，使用路徑中之較 CA_{11} 更前一位置的 CAbridge 的公鑰憑證來予以驗證。然後，當其爲可驗證時，更進一步，針對該當 EE 憑證發行 CA_{12} 所發行之 CRL，是以該當 EE 憑證發

行 CA_{12} 之公鑰憑證來予以驗證。當該路徑及 CRL 都爲可驗證時，則將 CAbridge 起至 EE 憑證發行 CA_{12} 爲止的路徑視爲暫時可驗證。

接著，路徑驗證部 52，若路徑爲暫時可驗證，則調查在從該當路徑上之各認證台 CA 所取得之公鑰憑證中，是否有非信賴之其他認證台的名稱（Name Constraints）或該當公鑰憑證之有效性確認用之容許最大路徑長（路徑上之容許最大認證台數）等之限制的描述。當有這類描述時，就調查該當路徑是否滿足該限制，只有當其爲滿足時，才將該當路徑視爲已完成認證。

然後，控制部 55，係如上述般，若對於路徑檢索部 51 所測出之每一路徑之路徑驗證部 52 的驗證結束，則進行登錄處理。控制部 55，當路徑驗證部 52 上的路徑驗證完成時（步驟 S1006，Yes），則將該當路徑和信賴起點 CA、EE 憑證發行 CA、EE 憑證發行 CA 所發行之 CRL，賦予對應關係，登錄在有效路徑資料庫 56A（步驟 S1007），進入步驟 S1003。又，控制部 55，係當路徑驗證部 52 上的路徑無法驗證時（步驟 S1006，No），則將該當路徑和信賴起點 CA、EE 憑證發行 CA、EE 憑證發行 CA 所發行之 CRL，賦予對應關係，登錄在非有效路徑資料庫 56B（步驟 S1008），進入步驟 S1003。

控制部 55，係將步驟 S1003～步驟 S1008 之步驟，重複進行直到檢測不到路徑（步驟 S1004，No）爲止，並產生路徑資料庫 56。此時，將全部的 CA 視爲信賴起點 CA

，檢索所有對應之路徑。CA 的構成爲圖 2 的情況下，則將 CA_{11}、CA_{21}、CAbridge 之三台 CA 視爲信賴起點 CA，而一一檢索對應之所有路徑。

步驟 S1003～步驟 S1008 爲止的處理進行之結果，當各 CA 爲如圖 2 所示之關係的情況下，路徑檢索部 51 所偵測出的所有路徑，如圖 9 所示。

另一方面，有效期限／失效狀態調查部 53，會調查登錄在有效路徑資料庫 56A 之公鑰憑證中，是否存在有效期限過期之公鑰憑證（步驟 S1009）。當有有效期限過期之公鑰憑證存在時，則存取該當公鑰憑證之發行源 CA 之公鑰憑證資料庫 44，檢索出對該當公鑰憑證之發行源重新發行過的公鑰憑證（步驟 S1010）。

然後，若在前記發行源 CA 之公鑰憑證資料庫 44 中沒有存在此種公鑰憑證，則將對應於前記有效期限過期之公鑰憑證過而登錄之路徑的相關資訊，從有效路徑資料庫 56A 中予以刪除，並登錄至非有效路徑資料庫 56B（步驟 S1011）。另一方面，若前記發行源 CA 之公鑰憑證資料庫 44 中存在有此種公鑰憑證，則將其予以取得。然後，代替該當有效期限過期之公鑰憑證改用新取得之公鑰憑證，將登錄在有效路徑資料庫 56A 之路徑的驗證，以相同於上記步驟 S1005 的要領進行之（步驟 S1012）。

然後，當路徑爲完成驗證時（步驟 S1013，Yes），則將對應於該當路徑而登錄在有效路徑資料庫 56A 的前記有效期限過期之公鑰憑證，置換成新取得之公鑰憑證（

步驟 S1014）。另一方面，當路徑無法驗證時（步驟 S1013，No），則將對應於前記有效期限過期之公鑰憑證而登錄之路徑，從有效路徑資料庫 56A 中予以刪除，並將置換成新取得之公鑰憑證的路徑，置換至非有效路徑資料庫 56B（步驟 S1015）。

接著，有效期限／失效狀態調查部 53，會調查失效憑證清單作成預定日時資料庫 57，檢索已經經過之失效憑證清單作成預定日時所對應之 CA（步驟 S1016）。當此種認證台 CA 爲存在時（步驟 S1017，Yes），則存取該當 CA 之失效憑證清單保持部 46，取得該當 CA 所發行之最新失效憑證清單（步驟 S1018）。然後，失效憑證清單作成預定日時資料庫 57 中，將對應於該當認證台 CA 而登錄之失效憑證清單作成預定日時，更新成已取得之最新失效憑證清單中所描述之失效憑證清單作成預定日時（步驟 S1019）。

然後，有效期限／失效狀態調查部 53，會調查已取得之最新之失效憑證清單所描述之公鑰憑證，是否登錄在有效路徑資料庫 56A 中（步驟 S1020）。當有登錄時，將對應該當公鑰憑證之路徑的相關資訊從有效路徑資料庫 56A 中刪除，登錄至非有效路徑資料庫 56B 中（步驟 S1021）。

接著，針對公鑰憑證之有效性確認動作予以說明。

圖 10～圖 11，係用來說明本實施形態之 VA 裝置（14）所進行之公鑰憑證之有效性確認動作的流程圖。

控制部 55，係一旦透過通訊部 50c，從 EE 收取到，至少含有該當 EE 所信賴之信賴起點 CA 之名稱的其他 EE 之公鑰憑證的有效性確認委託（步驟 S2001），則將該要旨通知至有效性確認部 54。

有效性確認部 54 收到此後，會調查被憑證之有效性確認委託之描述所特定之信賴起點 CA、發行該當憑證之 EE 憑證發行 CA 所對應之路徑，是否被登錄在有效路徑資料庫 56A 中（步驟 S2002）。

其結果，若憑證之有效性確認委託所描述之信賴起點 CA、發行該當憑證之 EE 憑證發行 CA 所對應之路徑，可以確認是被登錄在有效路徑資料庫 56A（步驟 S2002，Yes），則有效性確認部 54，會使用身爲該當路徑之端點的 EE 憑證發行 CA 之公鑰憑證，進行 EE 憑證之署名驗證。再者，有效性確認部 54，會使用對應於該當路徑而登錄之 CRL，確認 EE 憑證是否已經失效（步驟 S2003）。

當 EE 憑證之署名驗證失敗時（步驟 S2003，No），或 EE 憑證爲記述在 CRL 中且已經失效時，有效性確認部 54，會判斷 EE 憑證爲非有效者，並將其要旨，透過通訊部 50c，通知委託源之 EE（步驟 S2009）。

另一方面，各憑證中，具有能夠描述非信賴之認證台名所致之限制、或該當公鑰憑證之有效性確認所需之容許最大路徑長（路徑上之容許最大認證台數）。步驟 S2003 中，當 EE 憑證之署名驗證，以及是否已失效之確認爲成功時（Yes 的情況），則再度調查 EE 憑證及該當路徑中

所含之各 CA 的憑證當中，是否有描述上述之限制（步驟 S2004）。

當沒有這類描述時，就進入步驟 S2006。

步驟 S2006 中，有效性確認部 54，會調查從 EE 裝置（11）收取到的確認委託中，是否含有表示欲對該當 EE 進行之電子手續的交易額等之原則（policy）。

當含有原則時，則再調查 EE 憑證及構成該當路徑之各公鑰憑證中，是否有滿足前記原則之原則的描述（步驟 S2007）。

當 EE 憑證及該當路徑中，不具有滿足前記原則之原則描述時，則將 EE 憑證，判斷爲無法利用在委託源 EE 所欲進行之電子程序所需之公鑰憑證之有效性確認者，並將公鑰憑證爲非有效之要旨，透過通訊部 50c，通知至 EE 裝置（11）（步驟 S2009）。

另一方面，當從 EE 收取到的確認委託中不含有表示該當 EE 所欲進行之電子手續之原則時（步驟 S2006，No），或即使有含，但該當路徑及 EE 憑證所描述之原則爲滿足前記原則時（步驟 S2007，Yes），則判斷公鑰憑證爲有效，並將公鑰憑證爲有效之要旨，透過通訊部 50c，通知至委託源 EE（步驟 S2008）。

又，於步驟 S2002 中，憑證之有效性確認委託中所描述之，對應於信賴起點 CA、發行該當憑證之 EE 憑證發行 CA 的路徑，並非登錄在有效路徑資料庫 56A 時（步驟 S2002，No），則確認該當路徑是否有被登錄在非有效路

徑資料庫 56B（步驟 S2010）。當非有效路徑資料庫 56B 中，並未登錄該當路徑時（步驟 S2010，No），則進入圖 11 的步驟 S2012。

步驟 S2012 中，路徑檢索部 51，會檢索自確認委託所描述之信賴起點 CA 起，至確認對象之 EE 憑證爲止的路徑。該檢索，係異於聽從路徑檢索部 51 所事先制定之所定規則而進行者，而是臨時進行。

路徑檢索部 51，係當無法偵測到自信賴起點 CA 起至 EE 憑證止之路徑時（步驟 S2013，No），則有效性確認部 54，會將 EE 憑證爲非有效之要旨，透過通訊部 50c，通知至委託源之 EE（步驟 S2019）。另一方面，當路徑檢索部 51，偵測出自信賴起點 CA 起至 EE 憑證爲止的路徑時（步驟 S2013，Yes），則於路徑驗證部 52 中，進行已測出之路徑的驗證（步驟 S2014）。

當所測出之路徑爲可驗證時（步驟 S2015，Yes），則將自該當路徑之信賴起點 CA 起，至 EE 憑證發行 CA 爲止的路徑，及 EE 憑證發行 CA 所發行之 CRL，登錄至有效路徑資料庫（步驟 S2016）。然後，有效性確認部 54，會將 EE 憑證爲有效之要旨，透過通訊部 50c，通知至委託源 EE（步驟 S2017）。

另一方面，在步驟 S2015 中，當所測出之路徑爲不可驗證時（步驟 S2015，No），則將自該當路徑之信賴起點 CA 起，至 EE 憑證發行 CA 爲止的路徑，及 EE 憑證發行 CA 所發行之 CRL，登錄至非有效路徑資料庫 56B（步驟

S2018）。然後，進入步驟 S2011，進行檢索找出除了至目前爲止所測出的路徑以外，是否存在其他路徑，並同樣地執行之後的步驟。

又，圖 10 之步驟 S2010 中，當非有效路徑資料庫 56B 中，有登錄該當路徑時（步驟 S2010，Yes），又在該當已登錄之路徑以外，偵測到對應於有效性確認委託之路徑時（步驟 S2011，Yes），則進入步驟 S2014，進行該當已測出之路徑的驗證、登錄處理（步驟 S2014～步驟 S2019）。

另一方面，當除了該當已登錄之路徑以外，沒有偵測到其他對應於有效性確認委託的路徑時（步驟 S2011，No），則有效性確認部 54，會將公鑰憑證不具有效性之要旨，透過通訊部 50c，通知至委託源 EE（步驟 S2009）。

以上之實施形態中，信賴起點 CA 起至 EE 憑證發行 CA 止之路徑的檢索及驗證，係依從獨立於來自 EE 之公鑰憑證的有效性確認的所定規則，例如，爲定期地進行。

已檢索、驗證之路徑，會分類成有效路徑或非有效路徑，而登錄在路徑資料庫中保存。然後，藉由調查對應於有效性確認委託之路徑，是被當作有效路徑而登錄，還是被當作非有效路徑而登錄，以判斷該當 EE 憑證是否爲有效。

此時，對應於該當有效性確認委託的路徑，若被登錄成非有效路徑時，則針對是否存在該當非有效路徑以外之對應路徑，進行檢索、驗證、確認。又，對應於該當有效

性確認委託的路徑，沒有被登錄在路徑資料庫中時，則臨時進行路徑檢索、驗證。因此，即使當確認台之構成有變化時，也因根據最新路徑資訊而進行驗證，故可回應出適切的有效性確認結果。此外，藉由將非有效之路徑放在快取當中，使得自公鑰憑證收授起，至該當有效性確認爲止所需時間能夠縮短。

又，在本態中，進行路徑登錄之際，會將位於路徑端點之 EE 憑證發行 CA 所發行的 CRL，和該當 CRL 之驗證結果一併登錄。然後，當收到來自某台 EE 之公鑰憑證之公鑰憑證的有效性確認時，就使用該當 CRL，確認該當 EE 憑證是否爲失效。因此，可更加縮短公鑰憑證之有效性確認的所費時間。

此外，本發明並非侷限於上記實施形態，在該要旨範圍以內可有各種變形。

例如，上記實施形態中，VA 係在將路徑登錄至資料庫之際，分類成有效路徑資料庫 56A 及非有效路徑資料庫 56B，兩個資料庫而登錄。可是，亦可在一個資料庫中，附加代表該當路徑之狀態的旗標，來分類有效路徑和非有效路徑。

此外，上記實施形態中，雖然爲了說明理解方便，而假定如圖 2 所示，EE 憑證發行 CA 係只對 EE 發行公鑰憑證，而其他 CA 是只對 CA 發行公鑰憑證，但即使當含有對 EE 和 CA 兩者都發行公鑰憑證之 CA 時，亦能適用本發明。

此外，上記實施形態中，雖然爲了說明理解方便，而假定CA的構成是階層構造，但即使當CA的構成爲更複雜之網狀（mesh）構造，本發明亦能適用。

〔發明之效果〕

若根據本發明，則即使當路徑檢索時之後有新路徑形成的情況下，也能將適切的結果予以回應，及／或可以縮短從某台EE開始委託公鑰憑證的有效性確認起，至該當有效姓被確認爲止的所需時間。

【圖式簡單說明】

〔圖1〕本發明之一實施形態所適用之PKI系統的概略構成圖。

〔圖2〕圖1所示PKI系統之各CA的關係之一例圖。

〔圖3〕圖1所示EE之概略構成圖。

〔圖4〕圖1所示CA之概略構成圖。

〔圖5〕圖1所示VA之概略構成圖。

〔圖6〕圖1～圖5所示各EE、VA、CA的硬體構成例圖。

〔圖7〕用來說明圖5所示VA上所進行之路徑的檢索、驗證以及管理動作之流程圖。

〔圖8〕用來說明圖5所示VA上所進行之路徑的檢索、驗證以及管理動作之流程圖。

〔圖 9〕當各 CA 爲圖 2 所示之關係時，VA 的路徑檢索部 51 所偵測之所有路徑之圖。

〔圖 10〕用來說明圖 5 所示 VA 所進行之公鑰憑證之有效性確認動作之流程。

〔圖 11〕用來說明圖 5 所示 VA 所進行之公鑰憑證之有效性確認動作之流程。

〔圖 12〕在先前之 PKI 中，當認證台有複數台情況下，CA 關係之一例圖。

〔符號說明〕

CA…認證台

VA…憑證之有效性確認台

EE…終端個體

SD…安全網域

11…EE_1

12…EE_N

13…CA_1

14…CA_M

15…VA

16…VA

30a、40a、50a…處理部

30b、40b、50b…記憶部

30c、40c、50c…通訊部

30d、40d、50d…輸出入部

(30)

31… 署名產生部

32… 署名驗證部

33、43、55… 控制部

34… 電子文書保持部

35… 金鑰保持部

36… 驗證對象保持部

41… 發行部

42… 管理部

44… 公鑰憑證資料庫

45… 發行目標管理清單保持部

46… 失效憑證清單保持部

51… 路徑檢索部

52… 路徑驗證部

53… 有效期限／失效狀態調查部

54… 有效性確認部

56… 路徑資料庫

56A… 有效路徑資料庫

56B… 非有效路徑資料庫

57… 失效憑證清單作成預定日時資料庫

61… CPU

62… 記憶體

63… 外部記憶裝置

64… 讀取裝置

65… 通訊裝置

66… 輸 入 裝 置

67… 輸 出 裝 置

68… 介 面

69… 記 憶 媒 體

伍、中文發明摘要

發明名稱：公鑰憑證驗證之高速化方法及裝置

即使在路徑檢索之後才有新路徑存在時，也能回答適切的結果，且縮短自終端個體開始委託公鑰憑證之有效性確認起至獲知該結果爲止的所需時間。

憑證之有效性確認台，係事先定期地進行路徑及失效憑證清單的檢索、驗證，因應該當驗證結果，而分類成有效路徑及非有效路徑，登錄至資料庫中。又，當有來自終端個體之憑證的有效性確認委託時，調查對應該當委託的路徑，是被登錄在有效路徑資料庫或是非有效路徑資料庫當中的哪一者，而判斷該當公鑰憑證的有效性。另一方面，當對應於該當有效性確認委託之路徑並未登錄在資料庫中時，則重新進行路徑檢索、驗證，藉此已進行該當公鑰憑證之有效性確認。

陸、英文發明摘要

發明名稱：

(1)

拾、申請專利範圍

1. 一種公鑰憑證之有效性確認方法，係屬於在憑證之有效性確認台裝置上，回應委託而進行之公鑰憑證之有效性確認方法，其特徵爲，具備：

事先進行路徑之檢索及已檢索之路徑的驗證步驟；及

將前記檢索和驗證的結果，依據事先制定的基準，將前記路徑予以分類，登錄至資料庫的路徑登錄步驟；及

接受來自終端裝置之公鑰憑證的有效性確認委託，使用事先已登錄之路徑進行驗證的有效性確認步驟。

2. 如申請專利範圍第 1 項之公鑰憑證之有效性確認方法，其中，

於前記有效性確認步驟中，當對應於該當有效性確認委託的有效路徑並未登錄時，則藉由重新進行路徑檢索以及驗證，進行前記公鑰憑證之有效性確認。

3. 如申請專利範圍第 1 項之公鑰憑證之有效性確認方法，其中，

在前記路徑登錄步驟中，前記所謂事先制定之基準，係反映驗證結果，而分成有效路徑或非有效路徑；

前記有效性確認步驟中，對應於該當有效性確認委託之路徑，是被當作成有效路徑或非有效路徑而登錄在前記資料庫時，則依從前記登錄結果，進行前記被委託之公鑰憑證的有效性確認。

4. 如申請專利範圍第 3 項之公鑰憑證之有效性確認方法，其中，具有：

(2)

在前記有效性確認步驟中，即使對應該當有效性確認委託的路徑，被登錄成有效路徑時，該當公鑰憑證或該當路徑所含之公鑰憑證中，有記述著限制事項時，則因應前記有效性確認委託而進行路徑驗證，並調查該當公鑰憑證及該當路徑，是否滿足前記限制事項之步驟；及

若滿足限制事項，則判斷爲有效路徑之步驟。

5. 如申請專利範圍第 3 項之公鑰憑證之有效性確認方法，其中，具有：

在前記有效性確認步驟中，即使對應該當有效性確認委託的路徑，被登錄成有效路徑時，該當公鑰憑證或該當路徑所含之公鑰憑證中，有記載著原則（policy）時，則因應前記有效性確認委託而進行路徑驗證，並調查該當公鑰憑證及該當路徑，是否滿足電子手續之原則的步驟；及

若滿足前記原則時，則判斷爲有效路徑之步驟。

6. 如申請專利範圍第 3 項之公鑰憑證之有效性確認方法，其中，前記路徑登錄步驟，具有：

將自信賴起點 CA 起，至發行終端個體憑證之認證台爲止的路徑予以檢索之步驟；及

將發行該當終端個體憑證之認證台所發行之有關終端個體憑證的失效清單予以取得、驗證之步驟；及

將該當失效清單的驗證結果，和失效清單一併登錄之步驟。

7. 如申請專利範圍第 6 項之公鑰憑證之有效性確認方法，其中，

(3)

在前記有效性確認步驟中，當對應於該當有效性確認委託之路徑，是被當作有效路徑而登錄在前記資料庫中時，則不進行前記失效清單的驗證，而確認該當公鑰憑證爲並非失效。

圖1

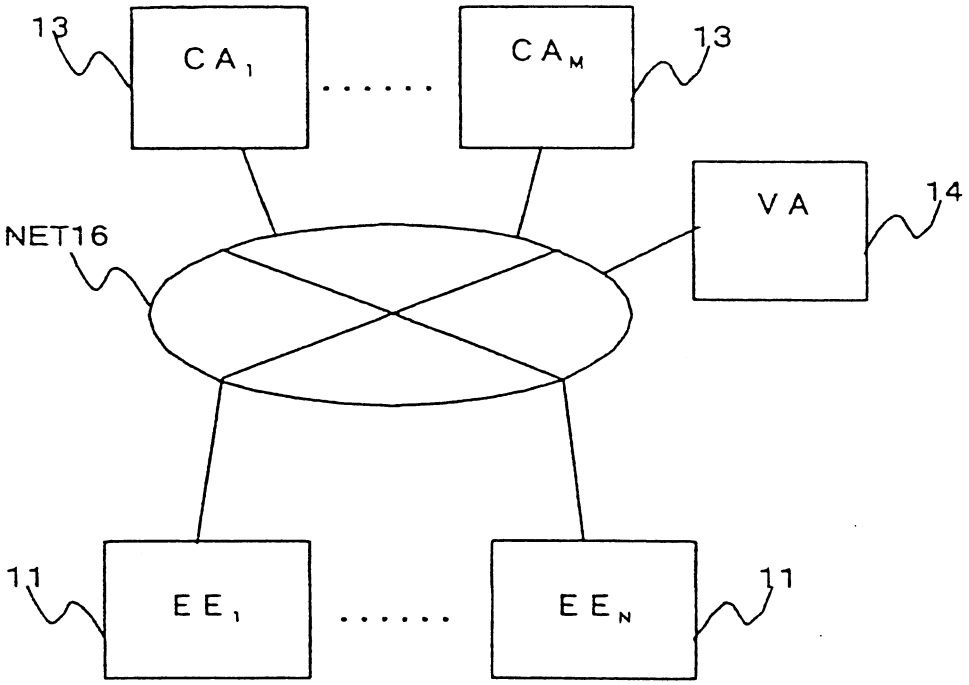


圖2

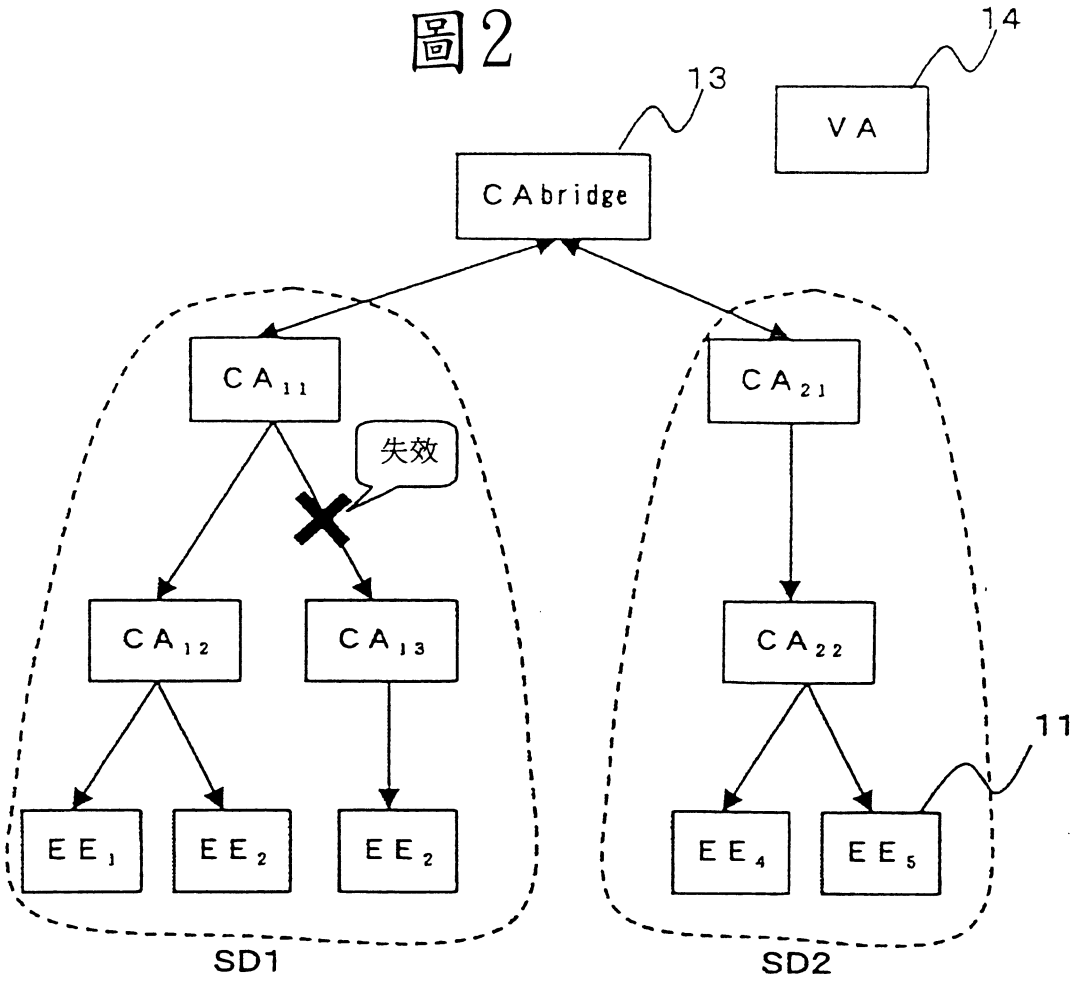

14
13
VA
CAbridge
CA11
失效
CA12
CA13
CA21
CA22
11
EE1
EE2
EE2
EE4
EE5
SD1
SD2

圖3

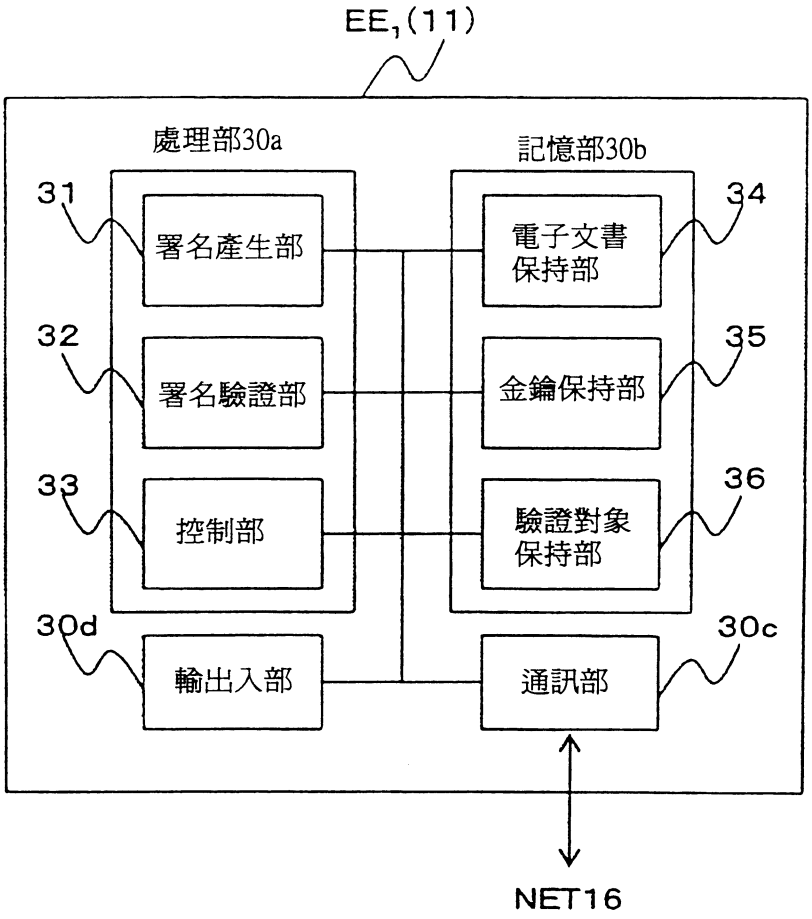

EE,(11)
處理部30a
記憶部30b
31
署名產生部
32
署名驗證部
33
控制部
30d
輸出入部
34
電子文書
保持部
35
金鑰保持部
36
驗證對象
保持部
30c
通訊部
NET16

圖4

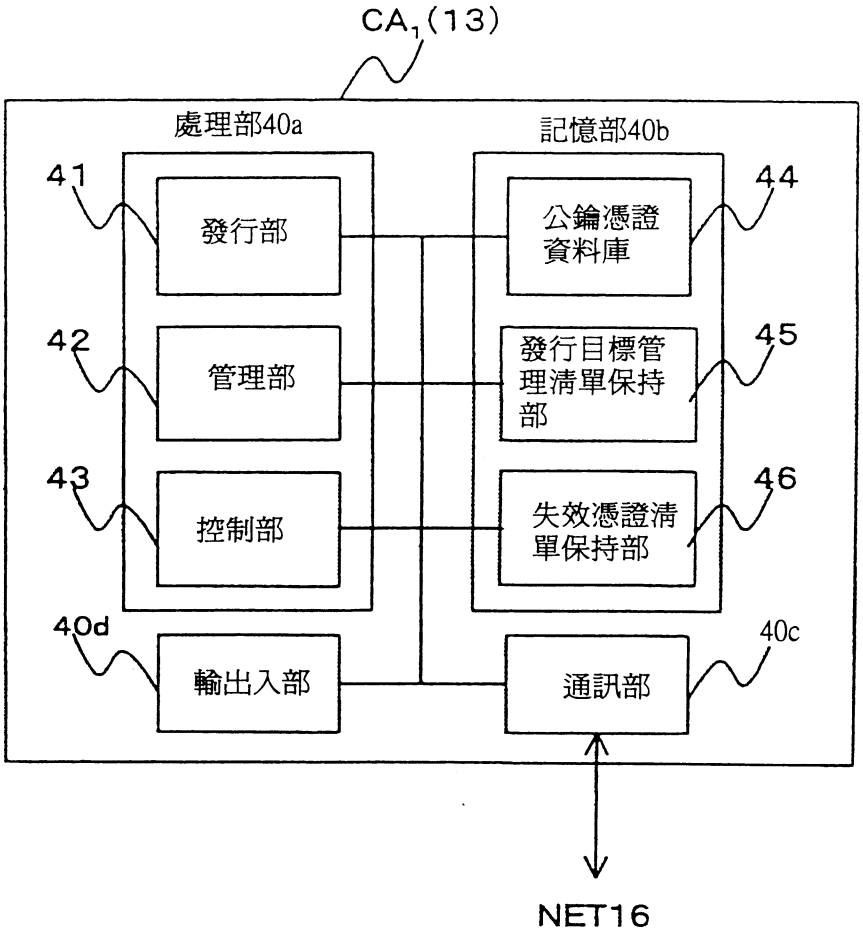

CA1(13)
處理部40a
記憶部40b
41
發行部
42
管理部
43
控制部
40d
輸出入部
公鑰憑證資料庫
44
發行目標管理清單保持部
45
失效憑證清單保持部
46
通訊部
40c
NET16

圖5

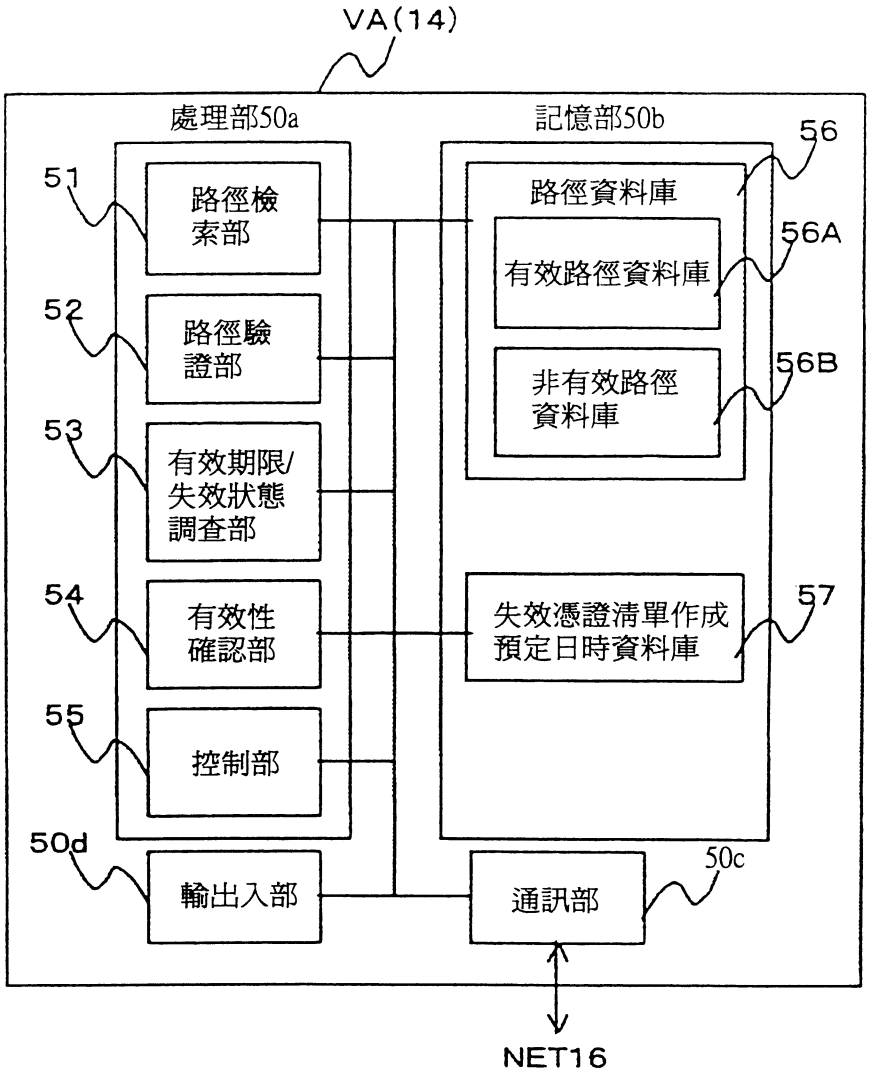

VA(14)
處理部50a
記憶部50b
56
51
路徑檢索部
路徑資料庫
56A
有效路徑資料庫
52
路徑驗證部
56B
非有效路徑資料庫
53
有效期限/失效狀態調查部
54
有效性確認部
57
失效憑證清單作成預定日時資料庫
55
控制部
50d
輸出入部
50c
通訊部
NET16

圖6

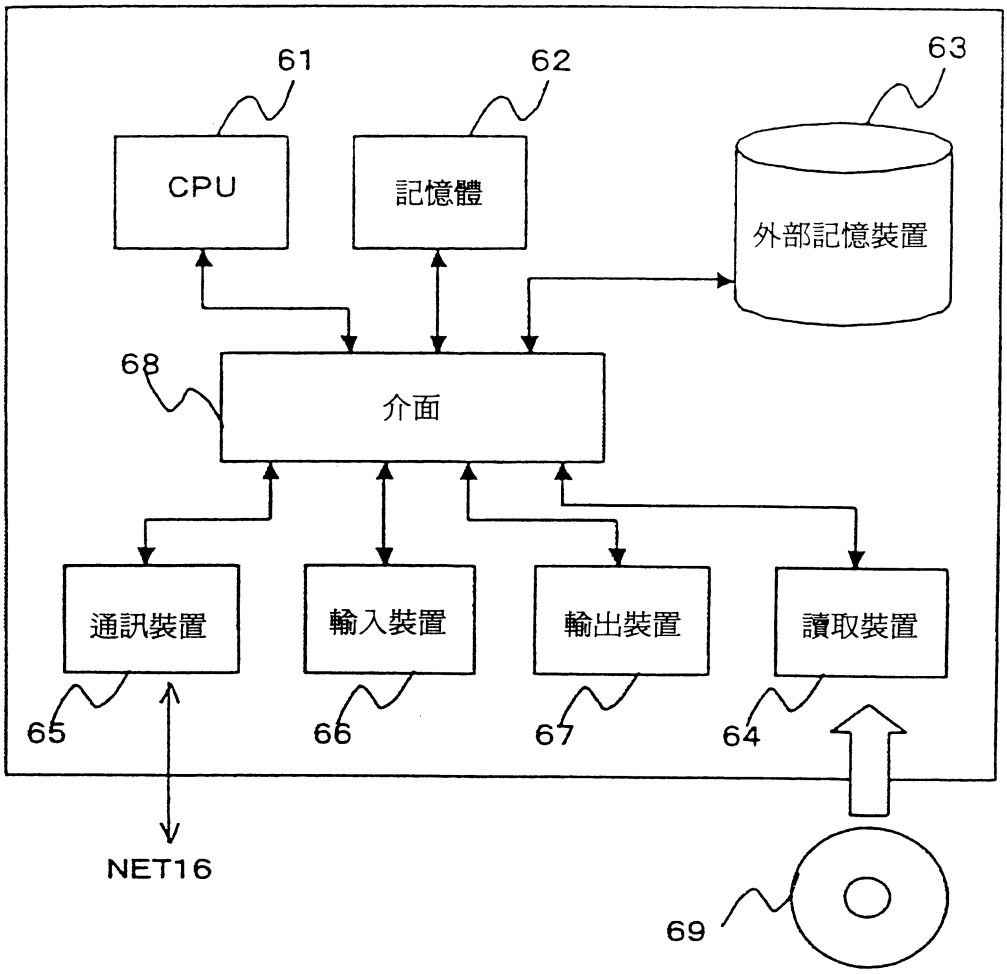

61
62
63
CPU
記憶體
外部記憶裝置
68
介面
通訊裝置
輸入裝置
輸出裝置
讀取裝置
65
66
67
64
NET16
69

圖7

路徑之檢索、驗證以及管理動作

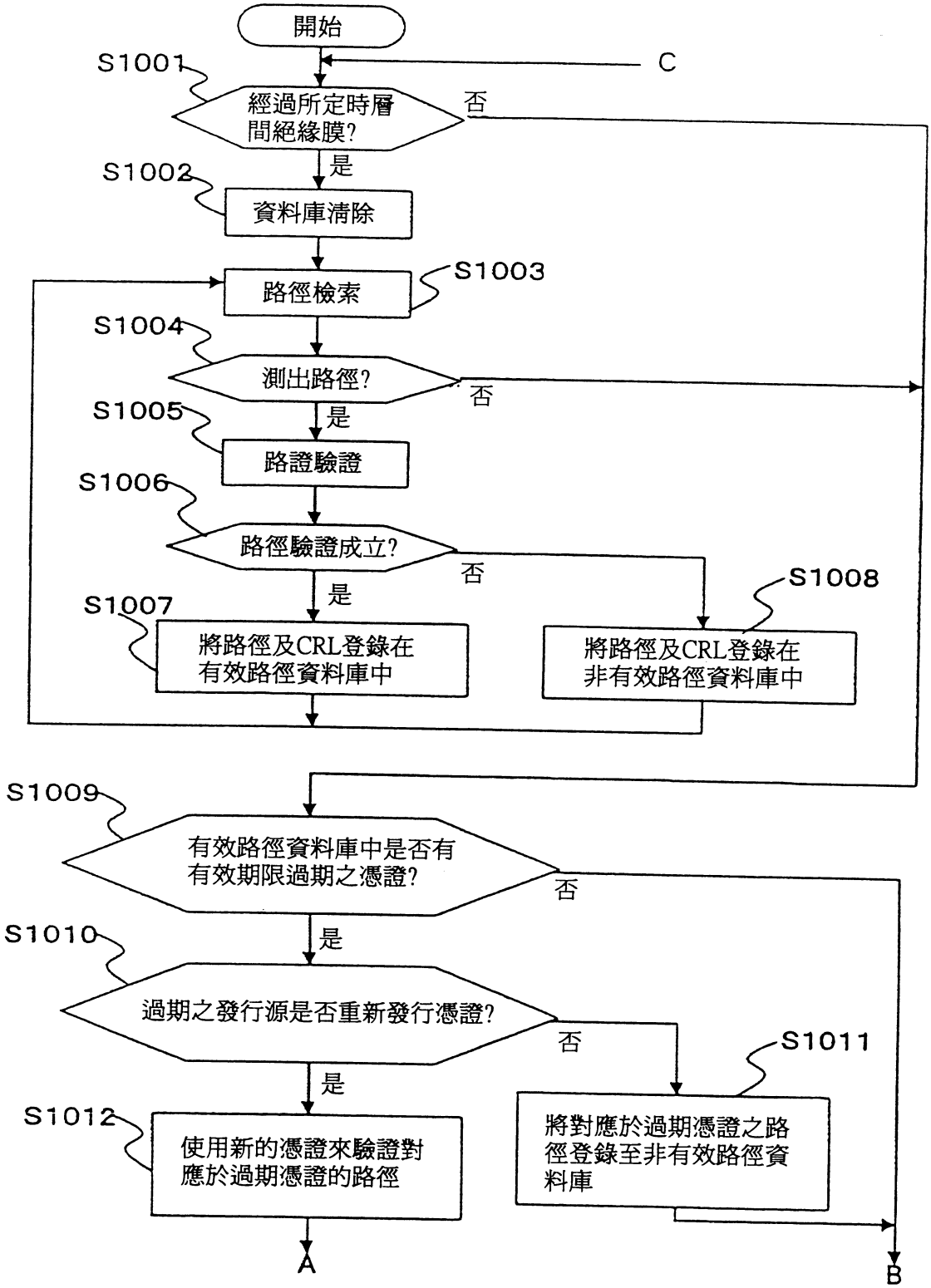


圖8

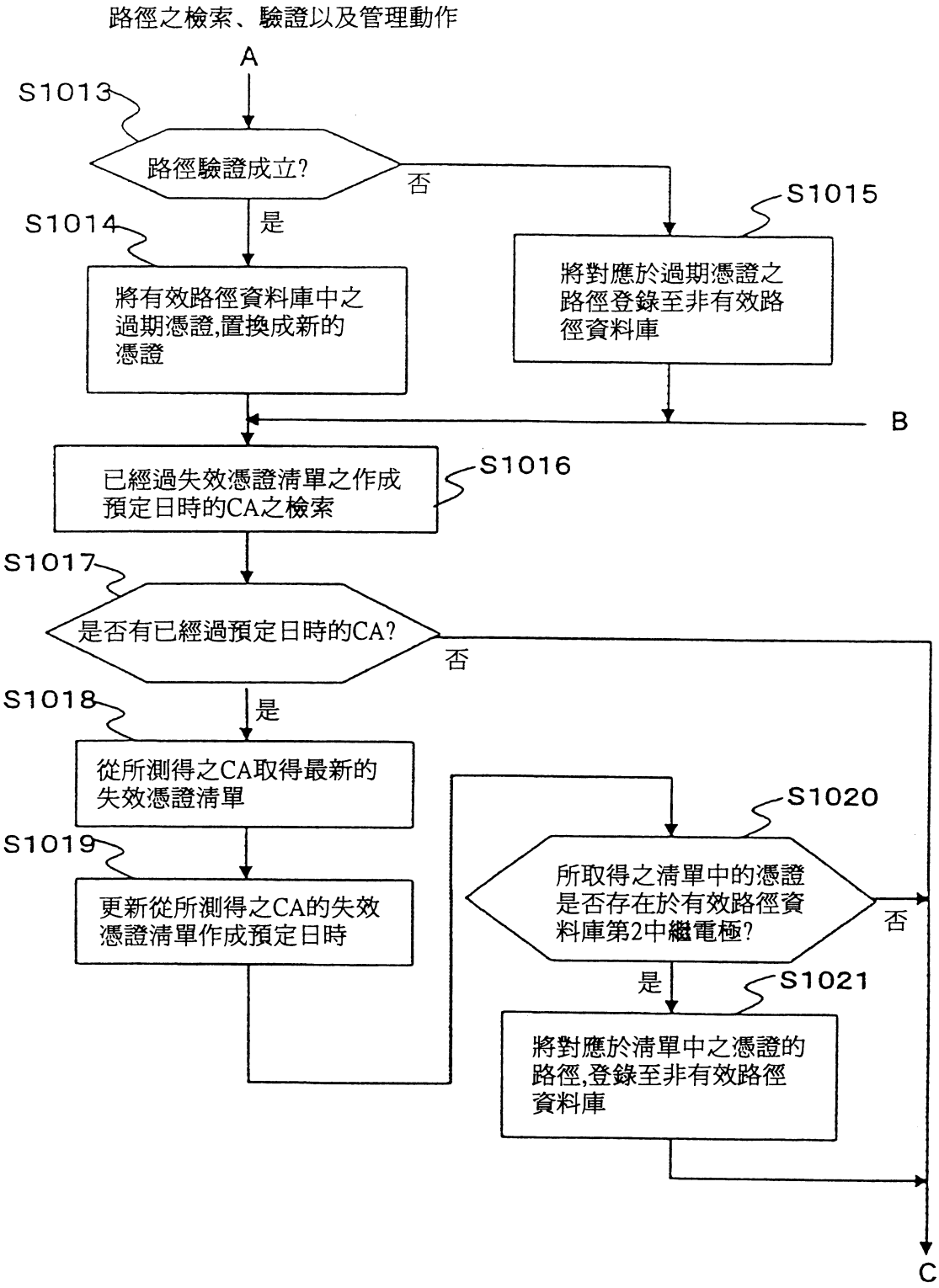

路徑之檢索、驗證以及管理動作
A
S1013
路徑驗證成立?
否
是
S1014
將有效路徑資料庫中之過期憑證,置換成新的憑證
S1015
將對應於過期憑證之路徑登錄至非有效路徑資料庫
B
已經過失效憑證清單之作成預定日時的CA之檢索
S1016
S1017
是否有已經過預定日時的CA?
否
是
S1018
從所測得之CA取得最新的失效憑證清單
S1019
更新從所測得之CA的失效憑證清單作成預定日時
S1020
所取得之清單中的憑證是否存在於有效路徑資料庫第2中繼電極?
否
是
S1021
將對應於清單中之憑證的路徑,登錄至非有效路徑資料庫
C

圖9

路徑檢索結果(圖2之情況)

有效路徑			
信賴起點CA	EE憑證 發明CA	路徑	CRL
CA_{11}	CA_{12}	$CA_{11}-CA_{12}$	有效
	CA_{22}	$CA_{11}-CAbridge-CA_{21}-CA_{22}$	有效
CA_{21}	CA_{12}	$CA_{21}-CAbridge-CA_{11}-CA_{12}$	有效
	CA_{22}	$CA_{21}-CA_{22}$	有效
CAbridge	CA_{12}	$CAbridge-CA_{11}-CA_{12}$	有效
	CA_{22}	$CAbridge-CA_{21}-CA_{22}$	有效

非有效路徑			
信賴起點CA	EE憑證 發行CA	路徑	CRL
CA_{11}	CA_{13}	$CA_{11}-CA_{12}$	無效
CA_{21}	CA_{12}	$CA_{21}-CAbridge-CA_{11}-CA_{12}$	無效
CAbridge	CA_{12}	$CAbridge-CA_{11}-CA_{12}$	無效

圖10

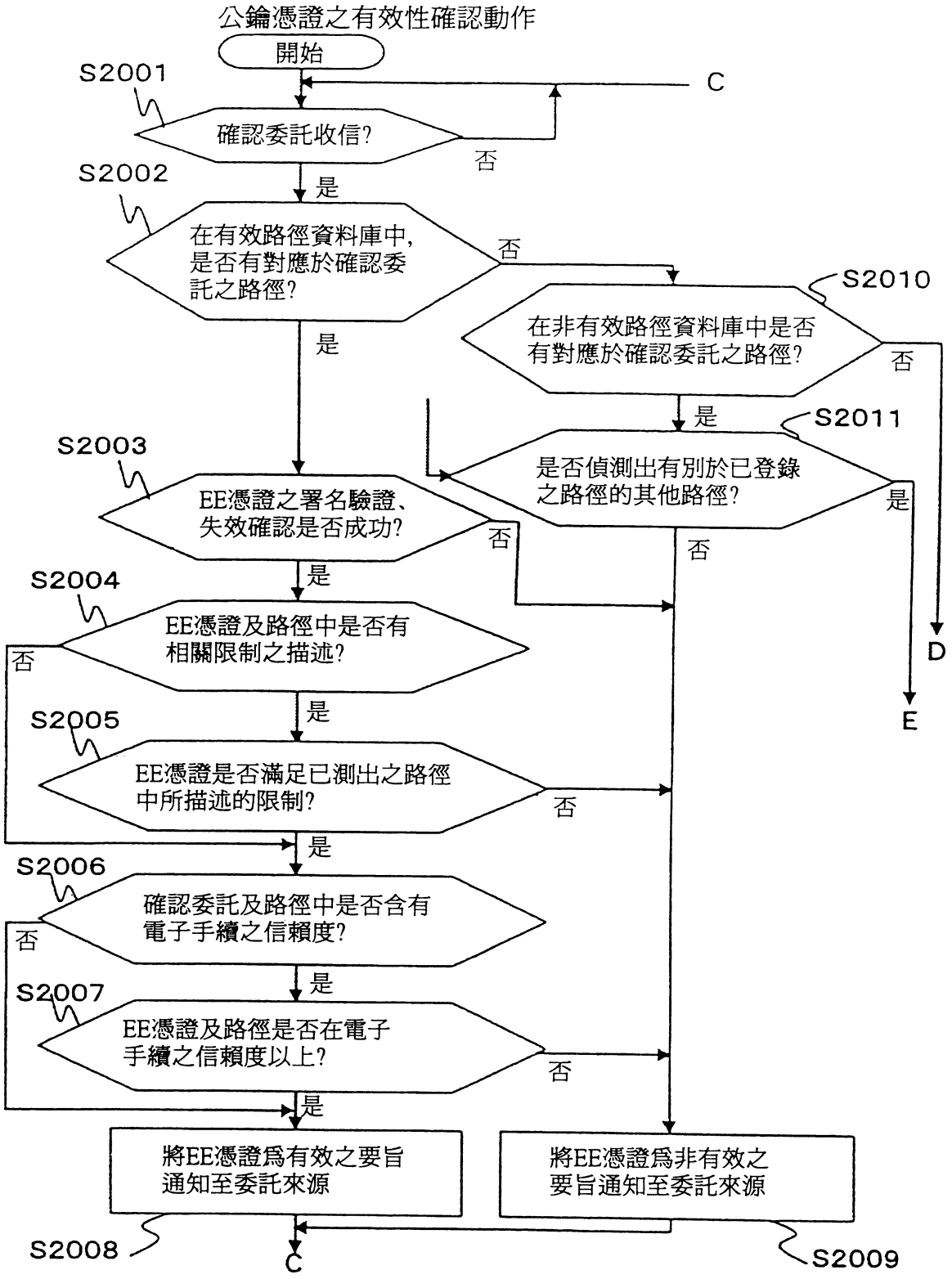

公鑰憑證之有效性確認動作
開始
S2001
確認委託收信?
否
C
S2002
是
在有效路徑資料庫中,是否有對應於確認委託之路徑?
否
S2010
在非有效路徑資料庫中是否有對應於確認委託之路徑?
否
D
是
S2011
是否偵測出有別於已登錄之路徑的其他路徑?
是
E
否
S2003
是
EE憑證之署名驗證、失效確認是否成功?
否
S2004
是
EE憑證及路徑中是否有相關限制之描述?
否
S2005
是
EE憑證是否滿足已測出之路徑中所描述的限制?
否
S2006
是
確認委託及路徑中是否含有電子手續之信賴度?
否
S2007
是
EE憑證及路徑是否在電子手續之信賴度以上?
否
是
將EE憑證爲有效之要旨通知至委託來源
將EE憑證爲非有效之要旨通知至委託來源
S2008
S2009
C

圖11

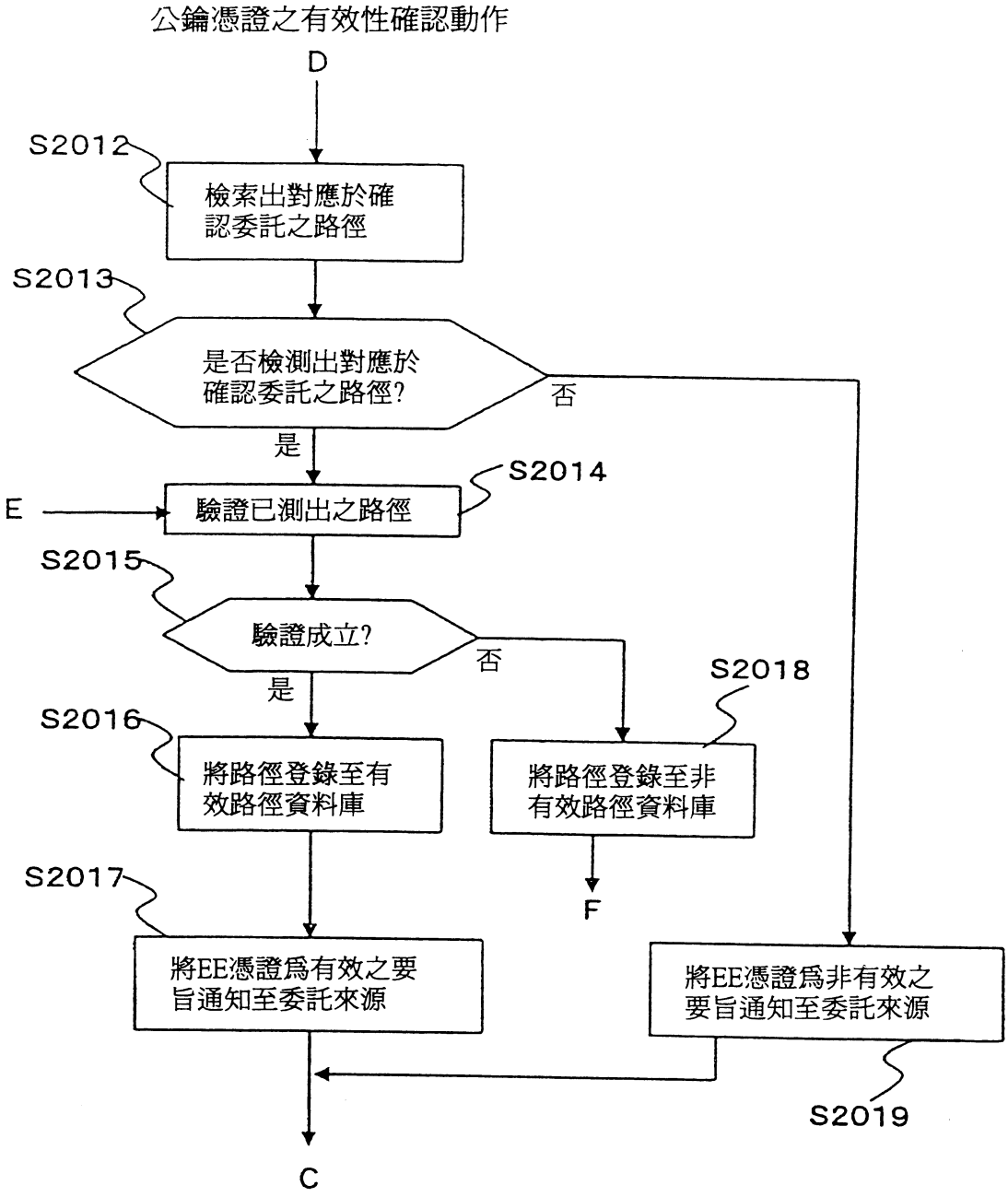
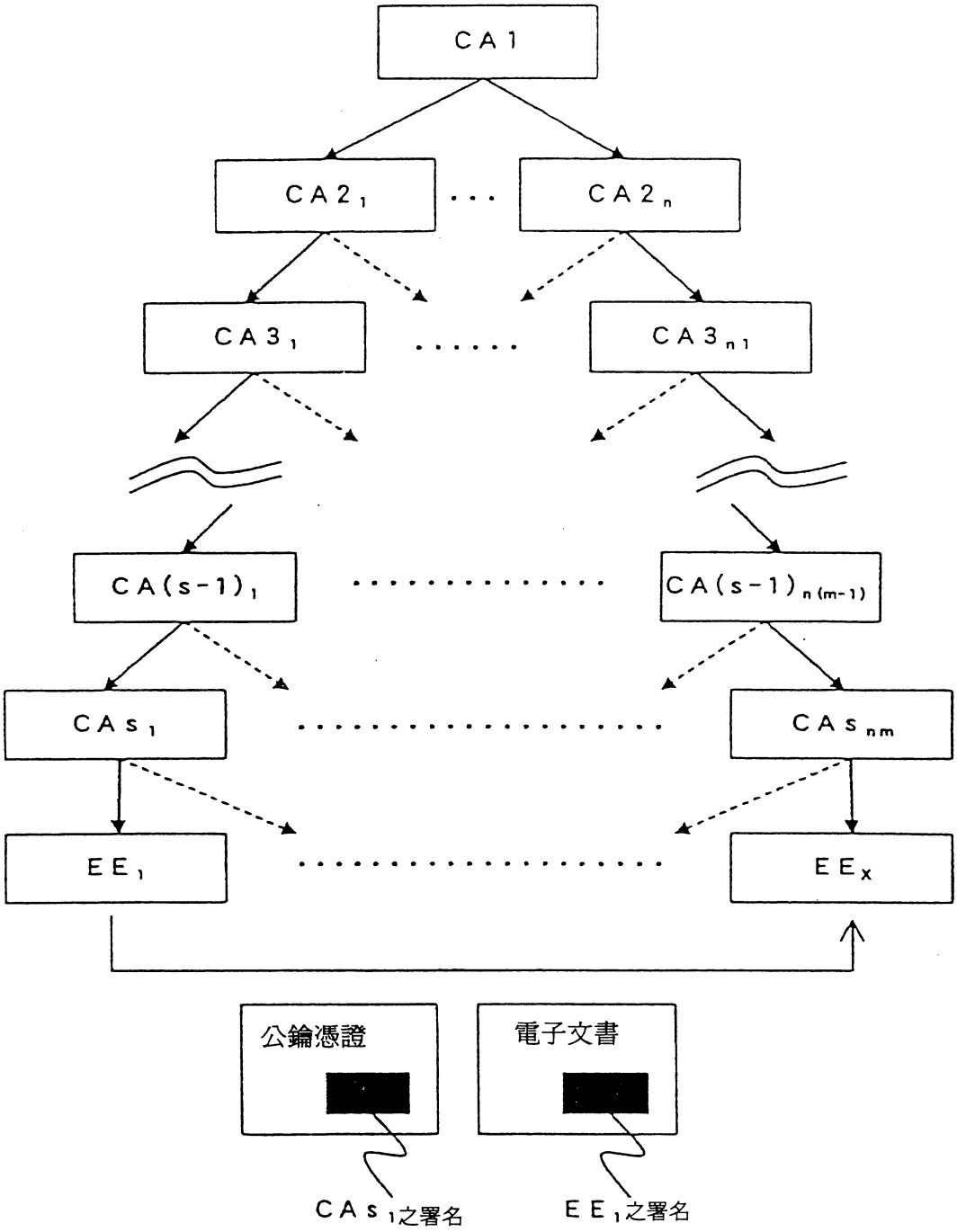

公鑰憑證之有效性確認動作
D
S2012
檢索出對應於確認委託之路徑
S2013
是否檢測出對應於確認委託之路徑?
否
是
S2014
E
驗證已測出之路徑
S2015
驗證成立?
否
是
S2018
S2016
將路徑登錄至有效路徑資料庫
將路徑登錄至非有效路徑資料庫
F
S2017
將EE憑證爲有效之要旨通知至委託來源
將EE憑證爲非有效之要旨通知至委託來源
S2019
C

圖12


CA1
CA2₁
CA2ₙ
CA3₁
CA3ₙ₁
CA(s-1)₁
CA(s-1)ₙ₍ₘ₋₁₎
CAs₁
CAsₙₘ
EE₁
EEx
公鑰憑證
電子文書
CAs₁之署名
EE₁之署名

柒、（一）、本案指定代表圖為：第 2 圖

（二）、本代表圖之元件代表符號簡單說明：

11…終端個體

13…橋接 CA

14…VA

SD…安全網域

捌、本案若有化學式時，請揭示最能顯示發明特徵的化學式：