(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 200948016 A1
(43)公開日： 中華民國 98 (2009) 年 11 月 16 日

(21)申請案號：098104185 (22)申請日： 中華民國 98 (2009) 年 02 月 10 日
(51)Int. Cl.： *H04L9/32 (2006.01)* *H04L29/06 (2006.01)*
(30)優先權：2008/02/14 日本 2008-033333
(71)申請人：日本電氣股份有限公司 (日本) NEC CORPORATION (JP)
日本
(72)發明人：稻葉勝 INABA, MASARU (JP)
(74)代理人：周良謀；周良吉
申請實體審查：有 申請專利範圍項數：11 項 圖式數：11 共 31 頁

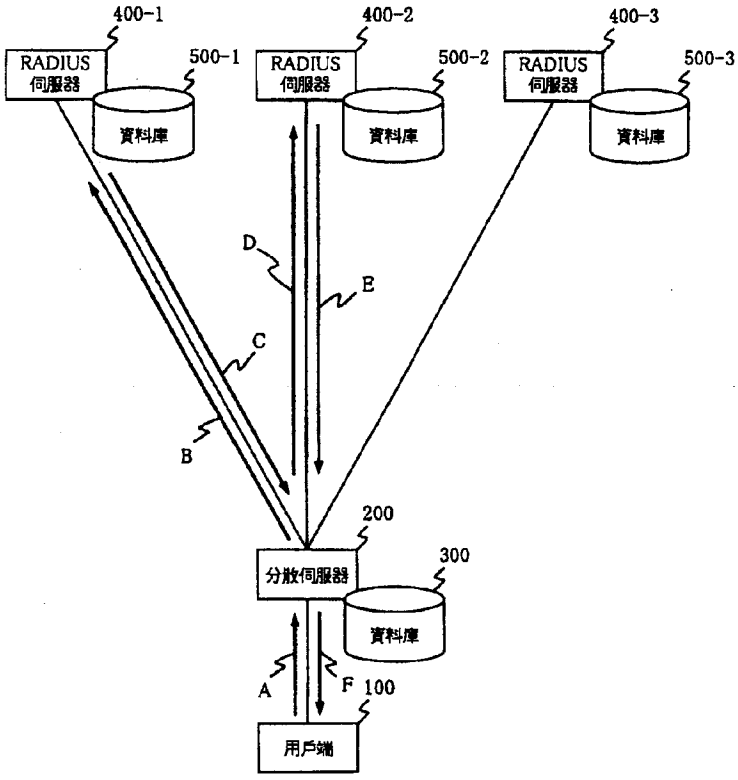
(54)名稱

分散處理系統、認證伺服器、分散伺服器、及分散處理方法

DISTRIBUTED PROCESSING SYSTEM, AUTHENTICATION SERVER, DISTRIBUTED SERVER, AND DISTRIBUTED PROCESSING METHOD

(57)摘要

本發明旨在提供一種分散處理系統、認證伺服器、分散伺服器及分散處理方法，其中於藉由使用預先取得之 TLS 參數之 TLS 通道內認證，在與終端機之間對利用終端機之使用者進行認證處理之認證伺服器內，自終端機傳送而來之使用者識別資訊不存在於認證資料庫內時，使使用者識別資訊與 TLS 參數包含於傳送要求信號中並將其朝分散伺服器傳送，藉由分散伺服器資料庫搜尋與包含於傳送要求信號之使用者識別資訊相對應之認證伺服器識別資訊，將使用者識別資訊與 TLS 參數朝被賦予所搜尋到的認證伺服器識別資訊之認證伺服器傳送之。



A~F：箭頭
100：用戶端
200：分散伺服器
300：資料庫
400－1 ～ 400－3：RADIUS 伺服器
500－1 ～ 500－3：資料庫

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 200948016 A1
(43)公開日： 中華民國 98 (2009) 年 11 月 16 日

(21)申請案號：098104185 (22)申請日： 中華民國 98 (2009) 年 02 月 10 日
(51)Int. Cl.： *H04L9/32 (2006.01)* *H04L29/06 (2006.01)*
(30)優先權：2008/02/14 日本 2008-033333
(71)申請人：日本電氣股份有限公司 (日本) NEC CORPORATION (JP)
日本
(72)發明人：稻葉勝 INABA, MASARU (JP)
(74)代理人：周良謀；周良吉
申請實體審查：有 申請專利範圍項數：11 項 圖式數：11 共 31 頁

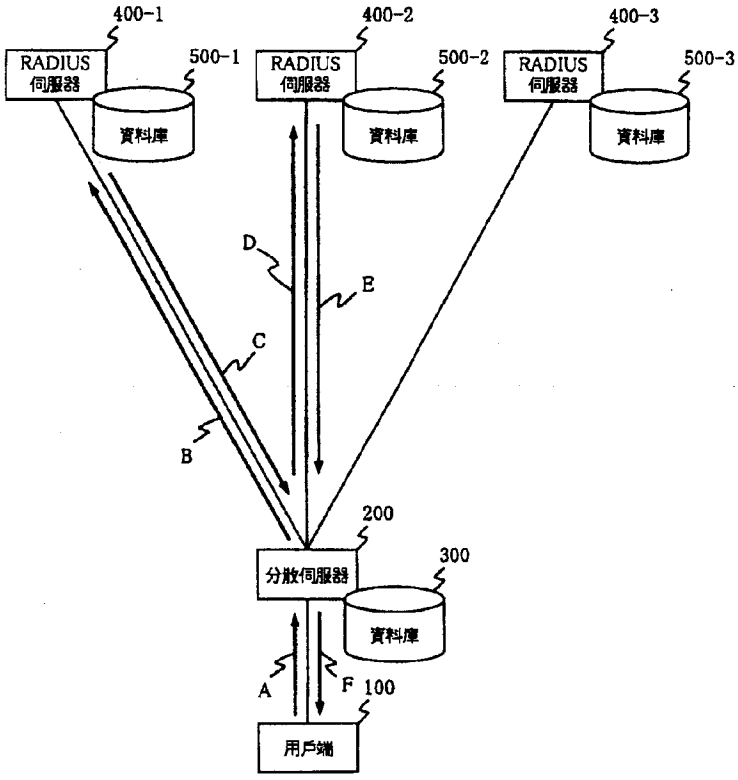
(54)名稱

分散處理系統、認證伺服器、分散伺服器、及分散處理方法

DISTRIBUTED PROCESSING SYSTEM, AUTHENTICATION SERVER, DISTRIBUTED SERVER, AND DISTRIBUTED PROCESSING METHOD

(57)摘要

本發明旨在提供一種分散處理系統、認證伺服器、分散伺服器及分散處理方法，其中於藉由使用預先取得之 TLS 參數之 TLS 通道內認證，在與終端機之間對利用終端機之使用者進行認證處理之認證伺服器內，自終端機傳送而來之使用者識別資訊不存在於認證資料庫內時，使使用者識別資訊與 TLS 參數包含於傳送要求信號中並將其朝分散伺服器傳送，藉由分散伺服器資料庫搜尋與包含於傳送要求信號之使用者識別資訊相對應之認證伺服器識別資訊，將使用者識別資訊與 TLS 參數朝被賦予所搜尋到的認證伺服器識別資訊之認證伺服器傳送之。



A~F：箭頭
100：用戶端
200：分散伺服器
300：資料庫
400－1 ～ 400－3：RADIUS 伺服器
500－1 ～ 500－3：資料庫

六、發明說明：

【發明所屬之技術領域】

【0001】　本發明係關於分散認證處理之分散處理系統、認證伺服器、分散伺服器及分散處理方法。

【先前技術】

【0002】　近年來，針對為利用網路或系統而對該網路或系統進行存取之使用者(user)進行認證處理，僅允許認證成功之使用者利用該網路或系統者增加。

【0003】　且為針對大量使用者進行認證處理，認證伺服器中處理負載會增加。因此，為減輕其處理負載，已知可實施一種方式，設置複數之認證伺服器，分割使用者設定檔資料庫並分別由認證伺服器所持有，以分別對應之認證伺服器進行認證處理。

【0004】　例如已知一種技術，將該使用者之認證處理分配給對應自終端機傳送而來之使用者 ID 之認證伺服器(參照例如日本專利公開 2006－11989 號公報。)。

【0005】　圖 1 係顯示一般的分散處理系統之一形態圖。

【0006】　圖 1 所示之分散處理系統中，已預先將使用者之使用者設定檔資料分散至分別連接 RADIUS 伺服器 4000－1～4000－3 之資料庫 5000－1～5000－3。因此為由資料庫 5000－1～5000－3 所持有之使用者設定檔資料中無重複之狀態。

【0007】　圖 1 所示之分散處理系統中係由利用該系統之使用者自用戶端 1000 要求進行認證(箭頭 AA)。如此，即以分散伺服器 2000 將為要求進行認證而自用戶端 1000 所傳送之認證要求信號接收。藉由分散伺服器 2000 抽出使用者 ID，該使用者 ID 係使用者識別資訊，被存放在包含於所接收之認證要求信號中之 RADIUS 之 USER－NAME 屬性內，用以識別使用者。又，自 RADIUS 伺服器 4000－1～4000－3 中選擇用以根據所抽出之使用者 ID 認證該使用者之(與存放有該使用者之使用者設定檔資料之資料庫連接之)認證伺服器。此係根據預先由連接分散伺服器 2000

之資料庫 3000 所存放之使用者 ID，與用以分別識別 RADIUS 伺服器 4000－1～4000－3 之認證伺服器識別資訊之相對應關係而選擇者。

【0008】　在此，舉用以認證要求進行認證之使用者之認證伺服器係 RADIUS 伺服器 4000－1 之情形為例。藉由分散伺服器 2000 選擇 RADIUS 伺服器 4000－1，將自用戶端 1000 所傳送之認證要求信號朝 RADIUS 伺服器 4000－1 傳送(箭頭 BB)。又，藉由 RADIUS 伺服器 4000－1 對使用者進行認證。

【0009】　然而，以上述技術，如 EAP(Extensible Authentication Protocol) － TTLS(Tunneled Transport Layer Security)認證方式，將虛擬 ID 存放在 RADIUS 之 USER－NAME 屬性中時，無法以分散伺服器辨識使用者 ID。亦即，一旦將虛擬 ID 存放在 RADIUS 之 USER－NAME 屬性中，即無法以分散伺服器辨識用戶端原來的使用者 ID。因此存在一問題點，無法選擇傳送對象之認證伺服器，該傳送對象之認證伺服器用以對以分散伺服器傳送認證要求信號之使用者進行認證。

【0010】　且在為 RADIUS 協議之後繼者之 Diameter 協議中，已知藉由 Redirect－Host　AVP 將係認證要求信號之認證封包朝其他認證伺服器傳送之構造。藉由此構造雖可對應上述問題點，但需自最初起重新進行認證處理之認證手續，而有認證處理效率不佳之問題點。

【發明內容】

【0011】　本發明之目的在於提供解決上述課題之分散處理系統、認證伺服器、分散伺服器及分散處理方法。

【0012】　為達成上述目的，本發明係一種分散處理系統，包含下列者並由下列者所構成：

終端機，由使用者所操作；

複數之認證伺服器，藉由使用預先取得之 TLS 參數之 TLS 通道內認證在與該終端機之間進行該使用者之認證處理；及

分散伺服器，將該認證處理分散給該複數之認證伺服器中之一認證伺服器；

該分散處理系統之特徵在於：

該認證伺服器判斷自該終端機透過該分散伺服器傳送而來，以固有之方式賦予該使用者之使用者識別資訊是否存在於連接該認證伺服器之認證資料庫內，當判斷該使用者識別資訊不存在於該認證資料庫內時，使該使用者識別資訊與該 TLS 參數包含於表示要求傳送該使用者識別資訊之傳送要求信號中並將其朝該分散伺服器傳送之，

該分散伺服器根據包含於自該認證伺服器傳送而來之該傳送要求信號之該使用者識別資訊，藉由連接該分散伺服器之分散伺服器資料庫搜尋與該使用者識別資訊相對應之認證伺服器識別資訊，將該使用者識別資訊與該 TLS 參數朝被賦予該搜尋到的認證伺服器識別資訊之認證伺服器傳送之。

【0013】　又，本發明係一種認證伺服器，藉由使用預先取得之 TLS 參數之 TLS 通道內認證，在與該終端機之間對操作終端機之使用者進行認證，其特徵在於包含：

加密／解密部，將自該終端機傳送而來，要求認證之認證要求信號加以解密，自經解密之認證要求信號中抽出以固有之方式賦予該使用者之使用者識別資訊；

認證部，判斷以該加密／解密部所抽出之使用者識別資訊是否存在於連接該認證伺服器之認證資料庫內；及

分散伺服器介面部，當判斷該使用者識別資訊不存在於該認證資料庫內時，使該使用者識別資訊與該 TLS 參數包含於表示要求傳送該使用者識別資訊之傳送要求信號中並將其朝連接該認證伺服器之分散伺服器傳送之。

【0014】　又，本發明係一種分散伺服器，連接於：

終端機，由使用者所操作；及

複數之認證伺服器，藉由使用預先取得之 TLS 參數之 TLS 通道內認證在與該終端機之間對該使用者進行認證處理；

以將該認證處理分散給該複數之認證伺服器中之一認證伺服器，

該分散伺服器之特徵在於包含：

認證伺服器介面部，從自該認證伺服器傳送而來，表示要求傳送以固有之方式賦予該使用者之使用者識別資訊之傳送要求信號中抽出該使用者識別資訊；及

伺服器選擇部，根據以該認證伺服器介面部所抽出之該使用者識別資訊，藉由連接該分散伺服器之分散伺服器資料庫搜尋與該使用者識別資訊相對應之認證伺服器識別資訊；

且該認證伺服器介面部將該使用者識別資訊與自該認證伺服器傳送而來之該 TLS 參數朝被賦予以該伺服器選擇部所搜尋到之認證伺服器識別資訊之認證伺服器傳送之。

【0015】　又，本發明係一種分散處理方法，被使用在一種分散處理系統中，該分散處理系統包含下列者並由下列者構成：

終端機，由使用者所操作；

複數之認證伺服器，藉由使用預先取得之 TLS 參數之 TLS 通道內認證在與該終端機之間對該使用者進行認證處理；及

分散伺服器，將該認證處理分散給該複數之認證伺服器中之一認證伺服器；

該分散處理方法之特徵在於包含下列處理：

該認證伺服器判斷自該終端機透過該分散伺服器傳送而來，以固有之方式賦予該使用者之使用者識別資訊是否存在於連接該認證伺服器之認證資料庫內；

當該認證伺服器判斷該使用者識別資訊不存在於該認證資料庫內時，使該使用者識別資訊與該 TLS 參數包含於表示要求傳送該使用者識別資訊之傳送要求信號中並將其朝該分散伺服器傳送之；

該分散伺服器根據包含於自該認證伺服器傳送而來之該傳送要求信號之該使用者識別資訊，藉由連接該分散伺服器之分散伺服器資料庫搜尋與該使用者識別資訊相對應之認證伺服器識別資

訊；及

該分散伺服器將該使用者識別資訊與該 TLS 參數朝被賦予該搜尋到的認證伺服器識別資訊之認證伺服器傳送之。

【0016】　如以上說明，本發明中因構成如下，可高效率進行認證分散處理：於藉由使用預先取得之 TLS 參數之 TLS 通道內認證，在與終端機之間對利用終端機之使用者進行認證處理之認證伺服器內，自終端機傳送而來之使用者識別資訊不存在於連接該認證伺服器之認證資料庫內時，使使用者識別資訊與 TLS 參數包含於傳送要求信號中並將其朝連接該認證伺服器之分散伺服器傳送之，於分散伺服器之內，藉由連接該分散伺服器之分散伺服器資料庫搜尋與包含於傳送要求信號之使用者識別資訊相對應之認證伺服器識別資訊，將使用者識別資訊與 TLS 參數朝被賦予搜尋到的認證伺服器識別資訊之認證伺服器傳送之。

【實施方式】

【0018】　以下參照圖式說明關於本發明之實施形態。

【0019】　圖 2 係顯示本發明之分散處理系統實施之一形態圖。

【0020】　本形態如圖 2 所示，由用戶端 100、分散伺服器 200、資料庫 300、RADIUS 伺服器 400－1～400－3、資料庫 500－1～500－3 所構成。在此，雖舉 RADIUS 伺服器 400－1～400－3 及資料庫 500－1～500－3 分別各有 3 個之形態為例說明之，但當然亦可分別有 2 個或 4 個以上。

【0021】　用戶端 100 係使用者為要求認證而操作之終端機，具備用以輸入資訊之輸入功能及用以通信之通信功能。

【0022】　分散伺服器 200 將使用者之認證處理分散給 RADIUS 伺服器 400－1～400－3。

【0023】　圖 3 係顯示圖 2 所示之分散伺服器 200 之一構成例圖。

【0024】　圖 2 所示之分散伺服器 200 中如圖 3 所示，設

有用戶端介面部 201、RADIUS 伺服器介面部 202、伺服器選擇部 203。又，圖 3 中僅顯示關於本發明之構成要素。

【0025】　用戶端介面部 201 具有與圖 2 所示之用戶端 100 之介面功能，在與用戶端 100 之間發送接收信號。用戶端介面部 201 將自用戶端 100 傳送而來之信號朝 RADIUS 伺服器介面部 202 輸出。且用戶端介面部 201 將自 RADIUS 伺服器介面部 202 所輸出之信號中應朝用戶端 100 傳送之信號朝用戶端 100 傳送。

【0026】　RADIUS 伺服器介面部 202 具有與圖 2 所示之 RADIUS 伺服器 400－1～400－3 之介面功能，係在與 RADIUS 伺服器 400－1～400－3 之間發送接收信號之認證伺服器介面部。且 RADIUS 伺服器介面部 202 在表示要求傳送認證要求信號之傳送要求信號自 RADIUS 伺服器 400－1～400－3 被傳送來時，將包含於該傳送要求信號，係用以識別使用者之使用者識別資訊之使用者 ID 抽出以朝伺服器選擇部 203 輸出。且 RADIUS 伺服器介面部 202 根據伺服器選擇部 203 中 RADIUS 伺服器之搜尋結果，朝 RADIUS 伺服器 400－1～400－3 中任一 RADIUS 伺服器傳送認證要求信號。且 RADIUS 伺服器介面部 202 將自用戶端介面部 201 所輸出之信號朝 RADIUS 伺服器 400－1～400－3 中任一適當之 RADIUS 伺服器傳送。且 RADIUS 伺服器介面部 202 將自 RADIUS 伺服器 400－1～400－3 傳送而來之傳送要求信號以外之信號朝用戶端介面部 201 輸出。

【0027】　伺服器選擇部 203 根據自 RADIUS 伺服器介面部 202 所輸出之使用者 ID，搜尋由資料庫 300 所存放之資訊，自 RADIUS 伺服器 400－1～400－3 中選擇傳送認證要求信號之 RADIUS 伺服器。

【0028】　且資料庫 300 連接分散伺服器 200，係存放有判斷以分散伺服器 200 將使用者之認證處理分散給哪一 RADIUS 伺服器 400－1～400－3 之資訊之分散伺服器資料庫。資料庫 300 作為上述資訊存放有相對應資訊與認證伺服器資訊。

【0029】　圖 4 係顯示由圖 2 所示之資料庫 300 所存放之

相對應資訊之一例圖。且圖 5 係顯示由圖 2 所示之資料庫 300 所存放之認證伺服器資訊之一例圖。

【0030】　由圖 2 所示之資料庫 300 所存放之相對應資訊中，如圖 4 所示，下列者相對應：

使用者 ID，係為識別使用者而以固有之方式賦予使用者之使用者識別資訊；及

認證伺服器編號，係為識別 RADIUS 伺服器 400－1～400－3 而以固有之方式賦予 RADIUS 伺服器之認證伺服器識別資訊。

此係表示使用者之使用者設定檔資料由分別連接哪一 RADIUS 伺服器 400－1～400－3 之資料庫 500－1～500－3 所存放之資訊。亦即，係表示使用者以哪一 RADIUS 伺服器 400－1～400－3 認證才好之資訊。

【0031】　例如，使用者 ID「使用者 1」與認證伺服器編號「伺服器 1」相對應。此表示對使用者 ID 係「使用者 1」之使用者進行認證之 RADIUS 伺服器係認證伺服器編號係「伺服器 1」之 RADIUS 伺服器。且使用者 ID「使用者 2」與認證伺服器編號「伺服器 1」相對應。此表示對使用者 ID 係「使用者 2」之使用者進行認證之 RADIUS 伺服器係認證伺服器編號係「伺服器 1」之 RADIUS 伺服器。且使用者 ID「使用者 3」與認證伺服器編號「伺服器 1」相對應。此表示對使用者 ID 係「使用者 3」之使用者進行認證之 RADIUS 伺服器係認證伺服器編號係「伺服器 1」之 RADIUS 伺服器。且使用者 ID「使用者 4」與認證伺服器編號「伺服器 2」相對應。此表示對使用者 ID 係「使用者 4」之使用者進行認證之 RADIUS 伺服器係認證伺服器編號係「伺服器 2」之 RADIUS 伺服器。且使用者 ID「使用者 5」與認證伺服器編號「伺服器 2」相對應。此表示對使用者 ID 係「使用者 5」之使用者進行認證之 RADIUS 伺服器係認證伺服器編號係「伺服器 2」之 RADIUS 伺服器。且使用者 ID「使用者 6」與認證伺服器編號「伺服器 3」相對應。此表示對使用者 ID 係「使用者 6」之使用者進行認證之 RADIUS 伺服器係認證伺服器編號係「伺服器 3」

之 RADIUS 伺服器。且使用者 ID「使用者 7」與認證伺服器編號「伺服器 3」相對應。此表示對使用者 ID 係「使用者 7」之使用者進行認證之 RADIUS 伺服器係認證伺服器編號係「伺服器 3」之 RADIUS 伺服器。且使用者 ID「使用者 8」與認證伺服器編號「伺服器 3」相對應。此表示對使用者 ID 係「使用者 8」之使用者進行認證之 RADIUS 伺服器係認證伺服器編號係「伺服器 3」之 RADIUS 伺服器。

【0032】 伺服器選擇部 203 可藉由參照此相對應資訊，根據自 RADIUS 伺服器介面部 202 所輸出之使用者 ID，選擇進行為該使用者 ID 之使用者之認證之 RADIUS 伺服器。

【0033】 且由圖 2 所示之資料庫 300 所存放之認證伺服器資訊中，如圖 5 所示，上述認證伺服器編號與該認證伺服器之 IP 位址相對應。此係表示使用者進行認證之 RADIUS 伺服器之 IP 位址之資訊。

【0034】 例如，認證伺服器編號「伺服器 1」與 IP 位址「x.y.z.w1」相對應。此表示認證伺服器編號係「伺服器 1」之 RADIUS 伺服器之 IP 位址為「x.y.z.w1」。且認證伺服器編號「伺服器 2」與 IP 位址「x.y.z.w2」相對應。此表示認證伺服器編號係「伺服器 2」之 RADIUS 伺服器之 IP 位址為「x.y.z.w2」。且認證伺服器編號「伺服器 3」與 IP 位址「x.y.z.w3」相對應。此表示認證伺服器編號係「伺服器 3」之 RADIUS 伺服器之 IP 位址為「x.y.z.w3」。

【0035】 伺服器選擇部 203 可參照此相對應資訊，在選擇進行為該使用者 ID 之使用者之認證之 RADIUS 伺服器後，取得該 RADIUS 伺服器之 IP 位址。

【0036】 且 RADIUS 伺服器 400－1～400－3 係對使用者進行認證之認證伺服器。

【0037】 圖 6 係顯示圖 2 所示之 RADIUS 伺服器 400－1 之一構成例圖。又，關於圖 2 所示之 RADIUS 伺服器 400－2～400－3，其構成亦與 RADIUS 伺服器 400－1 相同。

【0038】圖 2 所示之 RADIUS 伺服器 400－1 中如圖 6 所示，設有分散伺服器介面部 411、加密／解密部 412 與認證部 413。又，圖 6 中僅顯示關於本發明之構成要素。

【0039】　分散伺服器介面部 411 具有與圖 2 所示之分散伺服器 200 之介面功能，在與分散伺服器 200 之間發送接收信號。且分散伺服器介面部 411 在與用戶端 100 之間進行係加密通信之 TLS(Transport Layer Security)通道通信時，將自用戶端 100 被加密並透過分散伺服器 200 傳送而來之認證要求信號朝加密／解密部 412 輸出。且分散伺服器介面部 411 使上述傳送要求信號包含 TLS 參數與自認證部 413 所輸出之使用者 ID 並將其朝分散伺服器 200 傳送。在此，所謂 TLS 參數係在進行 TLS 通道通信時，用以對認證要求信號等信號進行加密／解密之參數，係先於認證，已藉由 RADIUS 伺服器 400－1 與用戶端 100 之間之 TLS 交握取得者。可使用例如 Master-Secret(用以產生加密鍵之亂數)、Cipher-Suite(加密演算法與散列演算法之群組)或 Compression-Method(壓縮方法)。且分散伺服器介面部 411 將自加密／解密部 412 所輸出之信號透過分散伺服器 200 朝用戶端 100 傳送(通道通信)。

【0040】　加密／解密部 412 使用 TLS 參數將自分散伺服器介面部 411 所輸出之認證要求信號等信號解密。且自所解密之認證要求信號抽出使用者 ID 以朝認證部 413 輸出。且將自認證部 413 所輸出之認證回應信號加密而朝分散伺服器介面部 411 輸出。

【0041】　認證部 413 對自加密／解密部 412 所輸出之認證要求信號進行認證。具體而言，參照資料庫 500－1，當與包含於該認證要求信號內之使用者 ID 相同之使用者 ID 存在於資料庫 500－1 時，作為一認證回應信號將要求密碼之密碼要求信號朝加密／解密部 412 輸出。且當對應密碼要求信號之密碼自加密／解密部 412 被輸出而來時，藉由判斷該密碼是否係資料庫 500－1 中與該使用者 ID 相對應之密碼進行使用者 ID 之認證。當自加密／解密部 412 被輸出而來之密碼係資料庫 500－1 中與該使用者 ID

相對應之密碼時，將表示認證成功之認證回應信號朝加密／解密部412輸出。且當與包含於該認證要求信號內之使用者ID相同之使用者ID未存在於資料庫500－1時，將該使用者ID朝分散伺服器介面部411輸出。

【0042】　且資料庫500－1～500－3係使使用者之使用者ID與密碼相對應並將其存放之認證伺服器資料庫。在此，舉圖2所示之資料庫300中存放有圖4所示之相對應資訊之情形為例說明之。

【0043】　圖7係顯示由圖2所示之資料庫500－1所存放之資訊之一例圖。

【0044】　由圖2所示之資料庫500－1所存放之資訊中，如圖7所示，使用者ID「使用者1」與密碼「密碼1」相對應。此表示使用者ID為「使用者1」之使用者之密碼為「密碼1」。且使用者ID「使用者2」與密碼「密碼2」相對應。此表示使用者ID為「使用者2」之使用者之密碼為「密碼2」。且使用者ID「使用者3」與密碼「密碼3」相對應。此表示使用者ID為「使用者3」之使用者之密碼為「密碼3」。資料庫500－1中存放有使用者1、使用者2及使用者3之使用者設定檔資料。

【0045】　圖8係顯示由圖2所示之資料庫500－2所存放之資訊之一例圖。

【0046】　由圖2所示之資料庫500－2所存放之資訊中，如圖8所示，使用者ID「使用者4」與密碼「密碼4」相對應。此表示使用者ID為「使用者4」之使用者之密碼為「密碼4」。且使用者ID「使用者5」與密碼「密碼5」相對應。此表示使用者ID為「使用者5」之使用者之密碼為「密碼5」。資料庫500－2中存放有使用者4及使用者5之使用者設定檔資料。

【0047】　圖9係顯示由圖2所示之資料庫500－3所存放之資訊之一例圖。

【0048】　由圖2所示之資料庫500－3所存放之資訊中，如圖9所示，使用者ID「使用者6」與密碼「密碼6」相對應。此

表示使用者 ID 為「使用者 6」之使用者之密碼為「密碼 6」。且使用者 ID「使用者 7」與密碼「密碼 7」相對應。此表示使用者 ID 為「使用者 7」之使用者之密碼為「密碼 7」。且使用者 ID「使用者 8」與密碼「密碼 8」相對應。此表示使用者 ID 為「使用者 8」之使用者之密碼為「密碼 8」。資料庫 500－3 中存放有使用者 6、使用者 7 及使用者 8 之使用者設定檔資料。

【0049】　以下說明關於上述形態中之分散處理方法。首先，舉操作用戶端 100 之使用者係使用者 ID 為「使用者 1」之使用者之情形為例說明之。

【0050】　圖 10 係用以說明圖 2～9 所示之形態中，分散處理方法內使用者係使用者 ID 為「使用者 1」之使用者時之分散處理方法之程序圖。

【0051】　首先，在用戶端 100 與 RADIUS 伺服器 400－1～400－3 中任一者之間進行 TLS 交握。此係用以準備在用戶端 100 與 RADIUS 伺服器 400－1～400－3 之間進行稱為 TLS 通道通信之加密通信。一旦自用戶端 100 將係要求信號之 Access-Request 朝分散伺服器 200 傳送，即藉由分散伺服器 200 之 RADIUS 伺服器介面部 202，自 RADIUS 伺服器 400－1～400－3 中決定一者，作為 Access-Request 之傳送對象，以步驟 1、3 朝被決定為傳送對象之 RADIUS 伺服器傳送 Access-Request。在此階段中因使用虛擬 ID，無法利用資料庫 300 決定保有使用者 1 之資料之 RADIUS 伺服器。因此，此傳送對象之決定方法可隨機決定，亦可為循環法等既定具規則性之決定方法。在此，舉決定傳送對象為 RADIUS 伺服器 400－1 之情形為例說明之。

【0052】　一旦以 RADIUS 伺服器 400－1 接收所傳送之 Access-Request，即以步驟 2、4 將係對應所接收之 Access-Request 之回應信號之 Access-Challenge 自 RADIUS 伺服器 400－1 透過分散伺服器 200 朝用戶端 100 傳送之。此 TLS 交握與通常者相同。且進行此 TLS 交握時，在用戶端 100 與 RADIUS 伺服器 400－1 之間交換係進行 TLS 通道通信時所需之 TLS 參數之

Master-Secret、Cipher-Suite 或 Compression-Method，以用戶端 100 與 RADIUS 伺服器 400－1 取得之。

【0053】　其後，在用戶端 100 與 RADIUS 伺服器 400－1 之間進行通道內認證處理。一旦以步驟 5 自用戶端 100 透過分散伺服器 200 傳送係認證要求信號之 Access-Request，即以加密／解密部 412 使用 TLS 參數將藉由 RADIUS 伺服器 400－1 之分散伺服器介面部 411 所接收之認證要求信號解密。且自以加密／解密部 412 所解密之認證要求信號抽出使用者 ID，在此階段初次特定使用者 ID。將所抽出之使用者 ID 自加密／解密部 412 朝認證部 413 輸出。

【0054】　以認證部 413 參照資料庫 500－1，自資料庫 500－1 中搜尋與自加密／解密部 412 輸出而來之使用者 ID 相同之使用者 ID。在此，因舉使用者係使用者 ID 為「使用者 1」之使用者之情形為例，故在資料庫 500－1 中搜尋到該使用者 ID。

【0055】　一旦以認證部 413 在資料庫 500－1 中搜尋到該使用者 ID，即以步驟 6 將係認證回應信號之 Access-Challenge 自分散伺服器介面部 411 透過分散伺服器 200 朝用戶端 100 傳送之。

【0056】　其後，以步驟 7、8 在用戶端 100 與 RADIUS 伺服器 400－1 之間交換包含有密碼等之封包，結束認證。

【0057】　其次，舉操作用戶端 100 之使用者係使用者 ID 為「使用者 4」之使用者之情形為例說明之。

【0058】　圖 11 係用以說明圖 2～9 所示之形態中，分散處理方法內使用者係使用者 ID 為「使用者 4」之使用者時之分散處理方法之程序圖。且在此由資料庫 300 所存放之認證伺服器編號為「伺服器 2」之伺服器係 RADIUS 伺服器 400－2。

【0059】　首先，與步驟 1～4 相同，以步驟 11～14 使用 TLS 交握在用戶端 100 與 RADIUS 伺服器 400－1～400－3 中任一者之間準備進行稱為 TLS 通道通信之加密通信。此與上述步驟 1～4 中之處理相同。且與上述例相同，舉決定傳送對象為 RADIUS 伺服器 400－1 之情形為例說明之。

【0060】　其後，在用戶端 100 與 RADIUS 伺服器 400－1 之間進行通道內認證處理。一旦自用戶端 100 以步驟 15 透過分散伺服器 200 傳送係認證要求信號之 Access-Request(圖 2 所示之箭頭 A 及 B)，即以加密／解密部 412 使用 TLS 參數將藉由 RADIUS 伺服器 400－1 之分散伺服器介面部 411 所接收之認證要求信號解密。且自以加密／解密部 412 所解密之認證要求信號抽出使用者 ID。將所抽出之使用者 ID 自加密／解密部 412 朝認證部 413 輸出之。

【0061】　以認證部 413 參照資料庫 500－1，自資料庫 500－1 中搜尋與自加密／解密部 412 輸出而來之使用者 ID 相同之使用者 ID。在此，舉使用者係使用者 ID 為「使用者 4」之使用者之情形為例，故在資料庫 500－1 中搜尋不到該使用者 ID。

【0062】　如此，即自認證部 413 朝分散伺服器介面部 411 輸出該使用者 ID。又，以步驟 16 自分散伺服器介面部 411 朝分散伺服器 200 傳送將意指要求傳送之屬性賦予包含有該使用者 ID 與上述 TLS 參數之 Access-Reject 之傳送要求信號(圖 2 所示之箭頭 C)。此時之屬性無法以 RADIUS 之標準屬性對應，故藉由 Vendor Specific Attribute 使用固有屬性。所需屬性內容如下。

・一旦附上 Access-Reject 即意指要求傳送(與 Diameter Redirect-Host AVP 相同)。

・存放 TLS 之 Master-Secret。

・存放 TLS 之 Cipher-Suite。

・存放 TLS 之 Compression-Method。

・存放以 TLS 通道內認證接收之使用者 ID。

【0063】　一旦藉由分散伺服器 200 之 RADIUS 伺服器介面部 202 接收自 RADIUS 伺服器 400－1 之分散伺服器介面部 411 所傳送之傳送要求信號，即以 RADIUS 伺服器介面部 202 自接收之傳送要求信號抽出使用者 ID。將所抽出之使用者 ID 自 RADIUS 伺服器介面部 202 朝伺服器選擇部 203 輸出之。

【0064】　又，藉由伺服器選擇部 203，根據所抽出之使用

者 ID 自 RADIUS 伺服器 400－1～400－3 搜尋傳送對象之 RADIUS 伺服器。具體而言，參照資料庫 300，自資料庫 300 之相對應資訊中取得與所抽出之使用者 ID 相對應之認證伺服器編號。且藉由伺服器選擇部 203，自資料庫 300 之認證伺服器資訊中取得所取得之認證伺服器編號之 IP 位址。在此，使用者 ID 為「使用者 4」，故取得認證伺服器編號「伺服器 2」(RADIUS 伺服器 400－2)。且已取得「伺服器 2」作為認證伺服器編號，故可取得 IP 位址「x.y.z.w2」。將所取得之 IP 位址自伺服器選擇部 203 朝 RADIUS 伺服器介面部 202 輸出之。

【0065】　又，藉由 RADIUS 伺服器介面部 202，將存放 TLS 參數之屬性與存放使用者 ID 之屬性附加給 Access-Request。其後，以步驟 17 將該 Access-Request 自 RADIUS 伺服器介面部 202 朝具有自伺服器選擇部 203 所輸出之 IP 位址之 RADIUS 伺服器 400－2 傳送之(圖 2 所示之箭頭 D)。

【0066】　一旦藉由 RADIUS 伺服器 400－2，判別出存在有於上述所追加之屬性，即可藉由沿用一齊追加之 TLS 參數，不需在用戶端 100 與 RADIUS 伺服器 400－2 之間重新進行交握，而作為以 TLS 交握後之認證封包開始 TLS 通道內認證加以處理。自 RADIUS 伺服器 400－2 將認證結果以步驟 18 透過分散伺服器 200 朝用戶端 100 傳送之(圖 2 所示之箭頭 E、F)。之後，以步驟 19、20 在用戶端 100、分散伺服器 200、RADIUS 伺服器 400－2 之間交換封包，結束認證。

【0067】　又，雖舉將使用者 ID 以固有之方式賦予使用者為例說明之，但亦可以固有之方式賦予用戶端 100 之終端機。

【0068】　且資料庫 300 亦可包含於分散伺服器 200。且各資料庫 500－1～500－3 亦可分別包含於 RADIUS 伺服器 400－1～400－3。

【0069】　如以上說明，如 EAP－TTLS 認證方式在信息交換之初期階段無法辨識使用者 ID 時，可藉由傳送以 TLS 交握而得之資訊，不自最初起重新進行認證手續而以其他認證伺服器繼續

進行認證，故可高效率地進行分散處理。

【0070】　以上雖已參照實施形態說明本發明申請案，但本發明申請案並不由上述實施形態所限定。本發明申請案之構成或詳細情形，可由熟悉本技藝者在本發明申請案之範圍內進行可理解之各種變更。

【0071】　本申請案主張以於 2008 年 2 月 14 日所申請之日本申請案特願 2008－033333 為基礎之優先權，將其所有揭示導入於此。

【圖式簡單說明】

【0017】

圖 1 係顯示一般的分散處理系統之一形態圖。

圖 2 係顯示本發明之分散處理系統實施之一形態圖。

圖 3 係顯示圖 2 所示之分散伺服器之一構成例圖。

圖 4 係顯示由圖 2 所示之資料庫所存放之相對應資訊之一例圖。

圖 5 係顯示由圖 2 所示之資料庫所存放之認證伺服器資訊之一例圖。

圖 6 係顯示圖 2 所示之 RADIUS 伺服器之一構成例圖。

圖 7 係顯示由圖 2 所示之資料庫所存放之資訊之一例圖。

圖 8 係顯示由圖 2 所示之資料庫所存放之資訊之一例圖。

圖 9 係顯示由圖 2 所示之資料庫所存放之資訊之一例圖。

圖 10 係用以說明圖 2～9 所示之形態之分散處理方法中，使用者係使用者 ID 為「使用者 1」之使用者時之分散處理方法之程序圖。

圖 11 係用以說明圖 2～9 所示之形態之分散處理方法中，使用者係使用者 ID 為「使用者 4」之使用者時之分散處理方法之程序圖。

【主要元件符號說明】

A~F、AA、BB: 箭頭

1~8、11~20: 步驟

100、1000: 用戶端

200、2000: 分散伺服器

201: 用戶端介面部

202: RADIUS 伺服器介面(部)

203: 伺服器選擇部

300、500－1～500－3、3000、5000－1～5000－3: 資料庫

400－1～400－3、4000－1～4000－3: RADIUS 伺服器

411: 分散伺服器介面部

412: 加密／解密部

413: 認證部

200948016

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：98104185

※ 申請日：98.2.10　　※IPC 分類：H04L 9/32 (2006.01)

H04L 29/06 (2006.01)

一、發明名稱：（中文/英文）

分散處理系統、認證伺服器、分散伺服器、及分散處理方法/
DISTRIBUTED PROCESSING SYSTEM, AUTHENTICATION SERVER, DISTRIBUTED SERVER, AND DISTRIBUTED PROCESSING METHOD

二、中文發明摘要：

本發明旨在提供一種分散處理系統、認證伺服器、分散伺服器及分散處理方法，其中於藉由使用預先取得之 TLS 參數之 TLS 通道內認證，在與終端機之間對利用終端機之使用者進行認證處理之認證伺服器內，自終端機傳送而來之使用者識別資訊不存在於認證資料庫內時，使使用者識別資訊與 TLS 參數包含於傳送要求信號中並將其朝分散伺服器傳送，藉由分散伺服器資料庫搜尋與包含於傳送要求信號之使用者識別資訊相對應之認證伺服器識別資訊，將使用者識別資訊與 TLS 參數朝被賦予所搜尋到的認證伺服器識別資訊之認證伺服器傳送之。

三、英文發明摘要：

In an authentication server which performs authentication processing of a terminal user over a TLS tunnel established with the terminal using TLS parameters acquired in advance, in those cases where user ID information sent from the terminal is not present within an authentication database, the user ID information and TLS parameters are included in a transfer request signal and sent to a

distributed server. A search is then conducted in the distributed server database for authentication server ID information associated with the user ID information included in the transfer request signal, and finally the user ID information and TLS parameters are sent to the authentication server assigned the authentication server ID information identified by the search.

七、申請專利範圍：

1.一種分散處理系統，包含下列者並由下列者所構成：

終端機，由使用者所操作；

複數之認證伺服器，藉由使用預先取得之TLS參數之TLS通道內認證在與該終端機之間進行該使用者之認證處理；及

分散伺服器，將該認證處理分散給該複數之認證伺服器中之一認證伺服器；

該分散處理系統之特徵在於：

該認證伺服器判斷自該終端機透過該分散伺服器傳送而來，以固有之方式賦予該使用者之使用者識別資訊是否存在於連接該認證伺服器之認證資料庫內，且當判斷該使用者識別資訊不存在於該認證資料庫內時，使該使用者識別資訊與該TLS參數包含於表示要求傳送該使用者識別資訊之傳送要求信號中並將其朝該分散伺服器傳送之；

該分散伺服器根據包含於自該認證伺服器傳送而來之該傳送要求信號之該使用者識別資訊，藉由連接該分散伺服器之分散伺服器資料庫搜尋與該使用者識別資訊相對應之認證伺服器識別資訊，並將該使用者識別資訊與該TLS參數朝被賦予該搜尋到的認證伺服器識別資訊之認證伺服器傳送之。

2.如申請專利範圍第1項之分散處理系統，其中該認證伺服器從自該終端機透過該分散伺服器傳送而來，要求認證之認證要求信號中抽出該使用者識別資訊，並判斷該被抽出之使用者識別資訊是否存在於該認證資料庫內。

3. 如申請專利範圍第2項之分散處理系統，其中該認證伺服器包含：

加密／解密部，將自該終端機透過該分散伺服器傳送而來之該認證要求信號加以解密，並自經解密之認證要求信號抽出該使用者識別資訊；

認證部，判斷以該加密／解密部所抽出之使用者識別資訊是否存在於該認證資料庫內；及

分散伺服器介面部，當判斷該使用者識別資訊不存在於該認證資料庫內時，使該使用者識別資訊與該 TLS 參數包含於該傳送要求信號中並將其朝該分散伺服器傳送之；

該分散伺服器則包含：

認證伺服器介面部，從自該認證伺服器傳送而來之該傳送要求信號中抽出該使用者識別資訊；及

伺服器選擇部，根據以該認證伺服器介面部所抽出之該使用者識別資訊，藉由連接該分散伺服器之分散伺服器資料庫搜尋與該使用者識別資訊相對應之認證伺服器識別資訊；

且該認證伺服器介面部朝被賦予以該伺服器選擇部搜尋到的認證伺服器識別資訊之認證伺服器傳送該使用者識別資訊與該 TLS 參數。

4.如申請專利範圍第 1 或 2 項之分散處理系統，其中該認證伺服器包含該認證伺服器資料庫。

5.如申請專利範圍第 1 或 2 項之分散處理系統，其中該分散伺服器包含該分散伺服器資料庫。

6.一種認證伺服器，藉由使用預先取得之 TLS 參數之 TLS 通道內認證，在與該終端機之間對操作終端機之使用者進行認證，其特徵在於包含：

加密／解密部，將自該終端機傳送而來，要求認證之認證要求信號加以解密，自經解密之認證要求信號中抽出以固有之方式賦予該使用者之使用者識別資訊；

認證部，判斷以該加密／解密部所抽出之使用者識別資訊是否存在於連接該認證伺服器之認證資料庫內；及

分散伺服器介面部，當判斷該使用者識別資訊不存在於該認證資料庫內時，使該使用者識別資訊與該 TLS 參數包含於表示要求傳送該使用者識別資訊之傳送要求信號中並將其朝連接該認證伺服器之分散伺服器傳送之。

7.如申請專利範圍第 6 項之認證伺服器，其中包含該認證伺服器資料庫。

8.一種分散伺服器，連接：

終端機，由使用者所操作；及

複數之認證伺服器，藉由使用預先取得之 TLS 參數之 TLS 通道內認證在與該終端機之間對該使用者進行認證處理；

以將該認證處理分散給該複數之認證伺服器中之一認證伺服器，

該分散伺服器之特徵在於包含：

認證伺服器介面部，從自該認證伺服器傳送而來，表示要求傳送以固有之方式賦予該使用者之使用者識別資訊之傳送要求信號中抽出該使用者識別資訊；及

伺服器選擇部，根據以該認證伺服器介面部所抽出之該使用者識別資訊，藉由連接該分散伺服器之分散伺服器資料庫搜尋與該使用者識別資訊相對應之認證伺服器識別資訊；

且該認證伺服器介面部將該使用者識別資訊與自該認證伺服器傳送而來之該 TLS 參數朝被賦予以該伺服器選擇部所搜尋到之認證伺服器識別資訊之認證伺服器傳送之。

9. 如申請專利範圍第 8 項之分散伺服器，其中包含該分散伺服器資料庫。

10.一種分散處理方法，被使用在一分散處理系統中，該分散處理系統包含下列者並由下列者構成：

終端機，由使用者所操作；

複數之認證伺服器，藉由使用預先取得之 TLS 參數之 TLS 通道內認證在與該終端機之間對該使用者進行認證處理；及

分散伺服器，將該認證處理分散給該複數之認證伺服器中之一認證伺服器；

該分散處理方法之特徵在於包含下列處理：

該認證伺服器判斷自該終端機透過該分散伺服器傳送而來，以固有之方式賦予該使用者之使用者識別資訊是否存在於連接該認證伺服器之認證資料庫內；

當該認證伺服器判斷該使用者識別資訊不存在於該認證資料

庫內時，使該使用者識別資訊與該 TLS 參數包含於表示要求傳送該使用者識別資訊之傳送要求信號中並將其朝該分散伺服器傳送之；

該分散伺服器根據包含於自該認證伺服器傳送而來之該傳送要求信號之該使用者識別資訊，藉由連接該分散伺服器之分散伺服器資料庫搜尋與該使用者識別資訊相對應之認證伺服器識別資訊；及

該分散伺服器將該使用者識別資訊與該 TLS 參數朝被賦予該搜尋到的認證伺服器識別資訊之認證伺服器傳送之。

11. 如申請專利範圍第 10 項之分散處理方法，其中包含下列處理：

該認證伺服器從自該終端機透過該分散伺服器傳送而來，要求認證之認證要求信號中抽出該使用者識別資訊；及

該認證伺服器判斷該所抽出之使用者識別資訊是否存在於該認證資料庫內。

八、圖式：

庫內時，使該使用者識別資訊與該 TLS 參數包含於表示要求傳送該使用者識別資訊之傳送要求信號中並將其朝該分散伺服器傳送之；

該分散伺服器根據包含於自該認證伺服器傳送而來之該傳送要求信號之該使用者識別資訊，藉由連接該分散伺服器之分散伺服器資料庫搜尋與該使用者識別資訊相對應之認證伺服器識別資訊；及

該分散伺服器將該使用者識別資訊與該 TLS 參數朝被賦予該搜尋到的認證伺服器識別資訊之認證伺服器傳送之。

11. 如申請專利範圍第 10 項之分散處理方法，其中包含下列處理：

該認證伺服器從自該終端機透過該分散伺服器傳送而來，要求認證之認證要求信號中抽出該使用者識別資訊；及

該認證伺服器判斷該所抽出之使用者識別資訊是否存在於該認證資料庫內。

八、圖式：

圖式

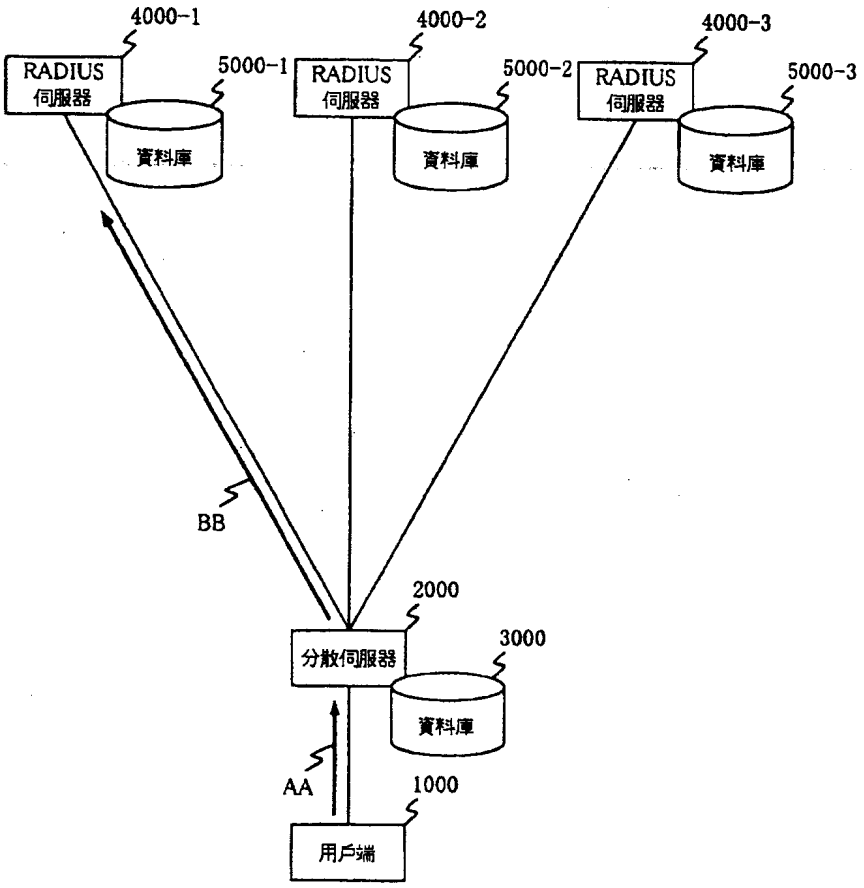

4000-1
RADIUS
伺服器
5000-1
資料庫
4000-2
RADIUS
伺服器
5000-2
資料庫
4000-3
RADIUS
伺服器
5000-3
資料庫
BB
2000
分散伺服器
3000
資料庫
AA
1000
用戶端

圖 1

圖式

圖 2

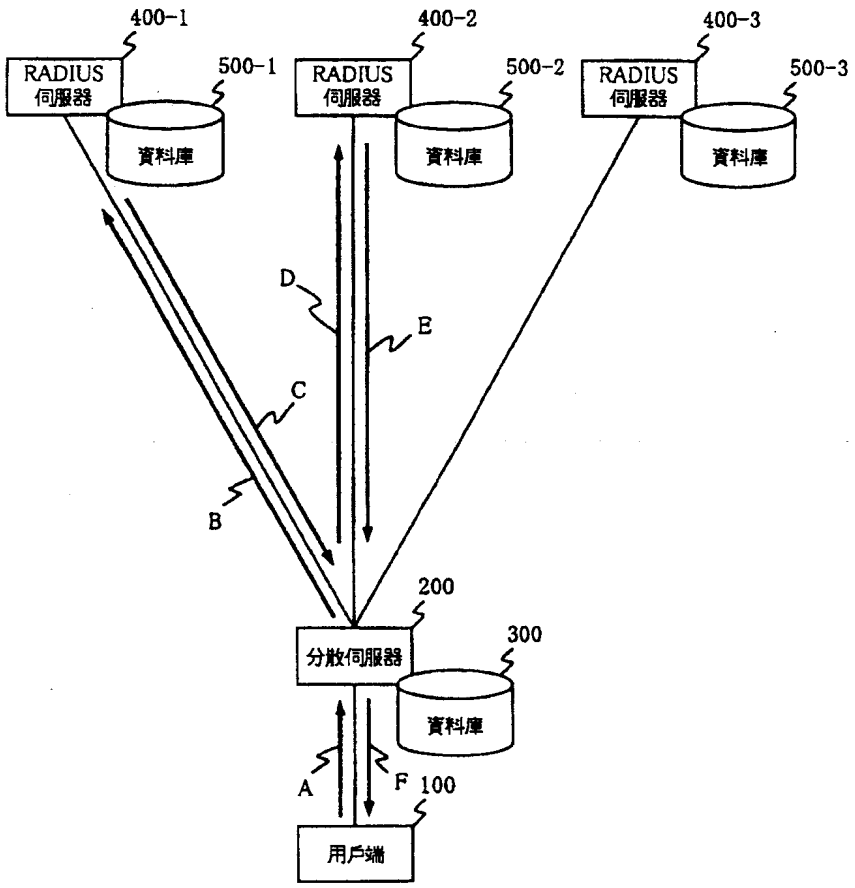
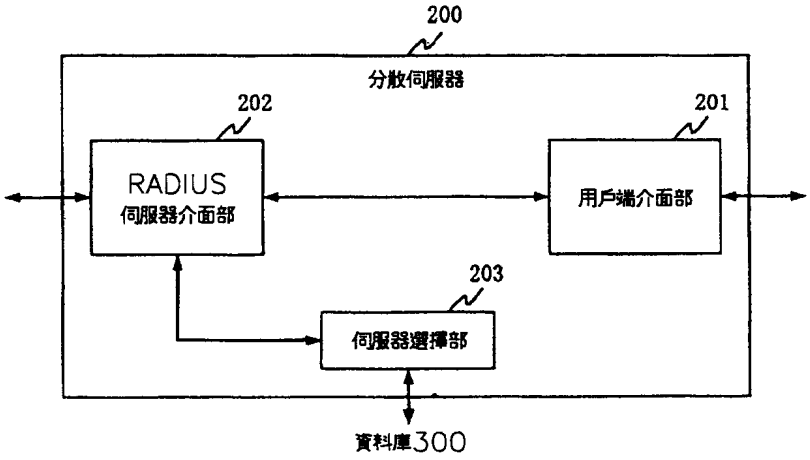

400-1
RADIUS
伺服器
500-1
資料庫
400-2
RADIUS
伺服器
500-2
資料庫
400-3
RADIUS
伺服器
500-3
資料庫
D
E
C
B
200
分散伺服器
300
資料庫
A
F
100
用戶端

圖 3


200
分散伺服器
202
RADIUS
伺服器介面部
201
用戶端介面部
203
伺服器選擇部
資料庫300

圖式

圖 4

使用者ID	認證伺服器編號
使用者1	伺服器1
使用者2	伺服器1
使用者3	伺服器1
使用者4	伺服器2
使用者5	伺服器2
使用者6	伺服器3
使用者7	伺服器3
使用者8	伺服器3

圖 5

認證伺服器編號	IP位址
伺服器1	x.y.z.w1
伺服器2	x.y.z.w2
伺服器3	x.y.z.w3

圖式

圖 6

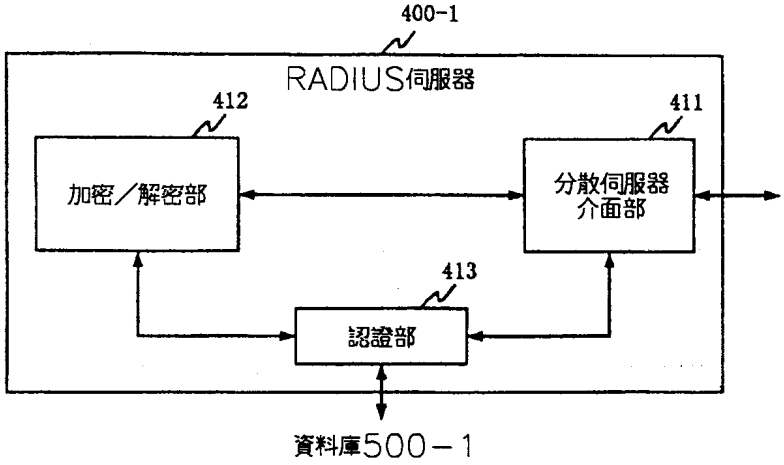


圖 7

使用者ID	密碼
使用者1	密碼1
使用者2	密碼2
使用者3	密碼3

圖 8

使用者ID	密碼
使用者4	密碼4
使用者5	密碼5

圖式

圖 9

使用者ID	密碼
使用者6	密碼6
使用者7	密碼7
使用者8	密碼8

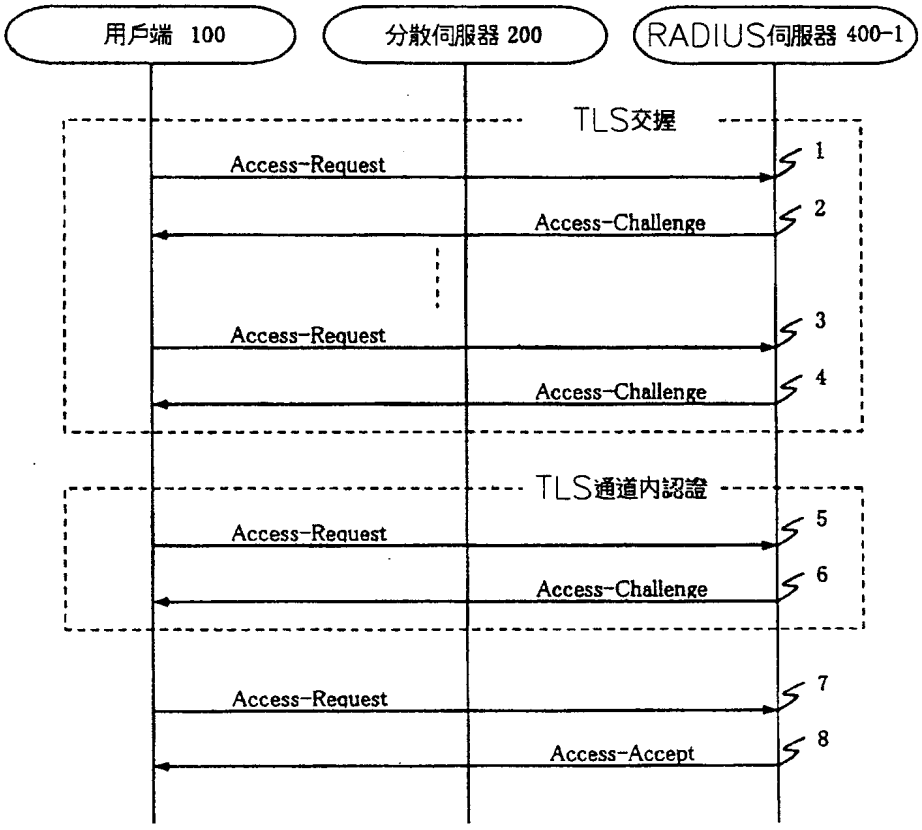


圖 10

圖式

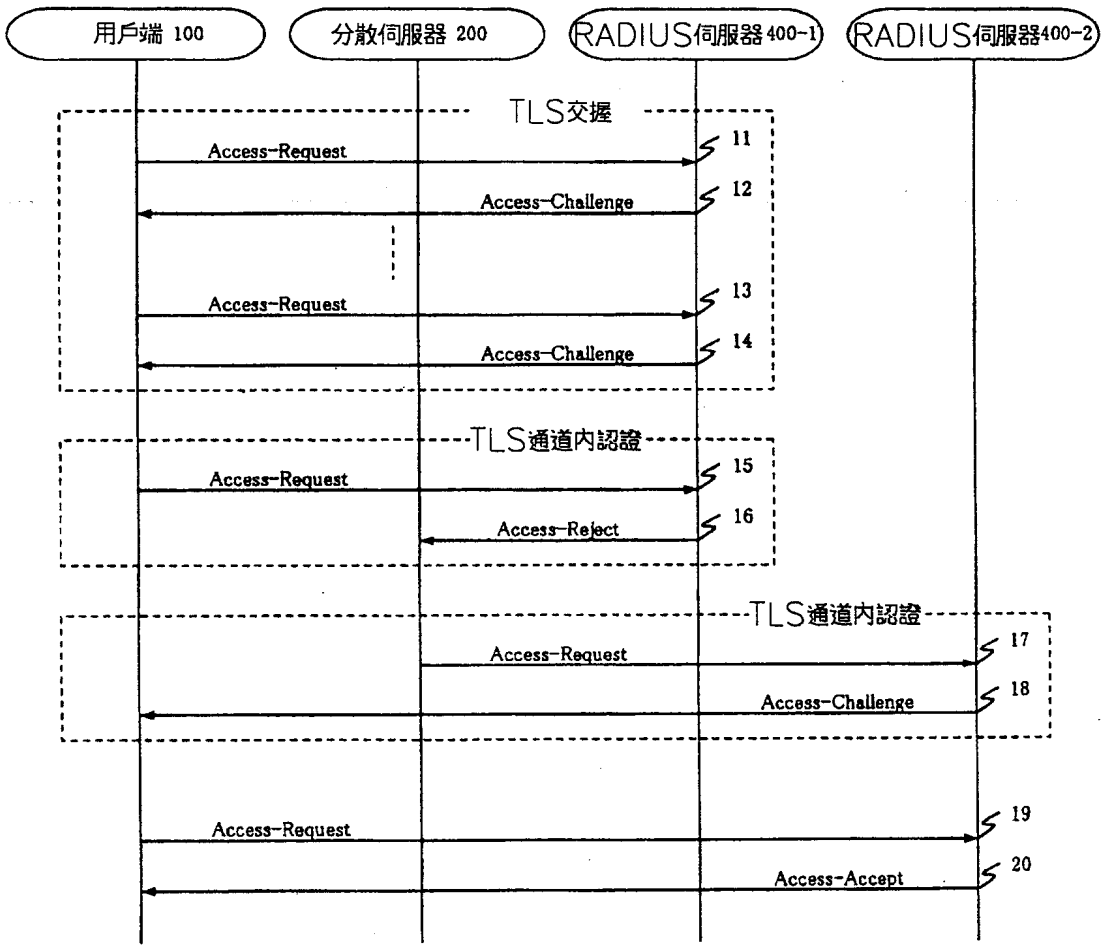

用戶端 100
分散伺服器 200
RADIUS伺服器400-1
RADIUS伺服器400-2
TLS交握
Access-Request
11
Access-Challenge
12
Access-Request
13
Access-Challenge
14
TLS通道內認證
Access-Request
15
Access-Reject
16
TLS通道內認證
Access-Request
17
Access-Challenge
18
Access-Request
19
Access-Accept
20

圖 11

四、指定代表圖：

(一)本案指定代表圖為：第（ 2 ）圖。

(二)本代表圖之元件符號簡單說明：

A~F: 箭頭

100: 用戶端

200: 分散伺服器

300: 資料庫

400－1～400－3: RADIUS 伺服器

500－1～500－3: 資料庫

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

無。