發明專利說明書

（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：95138600　　H04L 9/32 (2006.01)

※ 申請日期：95.10.17　　※IPC 分類：G09C 1/00 (2006.01)

一、發明名稱：（中文/英文）

認證系統及認證對象裝置

二、申 請 人：（共 1 人）

姓名或名稱：（中文/英文）

日商新力電腦娛樂股份有限公司

SONY COMPUTER ENTERTAINMENT INC.

代表人：（中文/英文）

久多良木 健

KUTARAGI, KEN

住居所或營業所地址：（中文/英文）

日本國東京都港區南青山2-6-21

2-6-21, MINAMI-AOYAMA, MINATO-KU, TOKYO 107-0062, JAPAN

國　籍：（中文/英文）

日本　JAPAN

三、發明人：（共 1 人）

姓　名：（中文/英文）

濱田　幸治

HAMADA, KOJI

國　籍：（中文/英文）

日本　JAPAN

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：

1. 日本；2005年12月19日；特願2005-365622

2.

☐ 無主張專利法第二十七條第一項國際優先權：

1.

2.

☐ 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】

本發明係關於一種認證對象裝置與認證該認證對象裝置之認證要求裝置使用相互共用之密碼鍵進行認證之認證系統、及該認證系統所包含之認證對象裝置。

【先前技術】

近年來，包含家庭用遊戲機之各種家電產品高功能化，於家電產品之本體上連接周邊機器，可擴展其功能者亦正在增加。在此類產品中，為避免使用者誤連接其他公司之產品等問題，會有想要判斷周邊機器是否為正規品(純正品)之情形。

因此，亦想將一般在計算機系統中所使用之認證系統應用於家電產品本體與周邊機器之間，進行是否為正規品之確認。例如，於專利文獻1揭示有普通的詢問應答型之認證處理之例。作為實現此種認證處理之演算法例，有共用鍵密碼演算法，其係家電產品本體等要求認證之認證要求裝置與周邊機器等成為認證對象之認證對象裝置各自保持相互共用之密碼鍵(共用鍵)者。

[專利文獻1]日本特開平11-163853號公報

[發明所欲解決之問題]

上述先前例之技術中，在認證要求裝置與認證對象裝置之間，每當進行認證時均傳送、接收用特定之密碼鍵加密之資料。但，若用同樣之密碼鍵所加密之資料多次被第三者所接收，則所加密之資料被破解、密碼鍵洩露給第三者

之危險性增大。

為降低此種危險性，有準備多數的密碼鍵，於每次進行認證時使用不同密碼鍵之方法。但，例如有時周邊機器等因硬體上之限制而不能確保充分的記憶體容量，此時則難以保持多數之密碼鍵。

【發明內容】

本發明係鑒於上述情形而完成者，其目的之一在於提供一種在使用共用鍵密碼演算法進行認證時，能夠以少數的密碼鍵提高安全性之認證系統及包含於該認證系統之認證對象裝置。

[解決問題之方法]

為解決上述問題之本發明之認證系統，其特徵在於其係包含認證對象裝置、及認證該認證對象裝置之認證要求裝置，且該認證對象裝置與該認證要求裝置保持至少一個相互共用之密碼鍵者；前述認證要求裝置包含：第1加密碼生成機構，係使用前述密碼鍵加密認證用碼，生成第1加密碼者；轉換對象部分選擇機構，係選擇前述認證用碼中至少一對相互不同之部分作為轉換對象部分者；傳送機構，係將前述第1加密碼及特定前述轉換對象部分之轉換對象部分特定資訊，向前述認證對象裝置傳送者；及轉換機構，係轉換前述認證用碼之前述轉換對象部分，生成比較對象碼者；前述認證對象裝置包含：認證用碼解碼機構，係用前述密碼鍵將前述所傳送之第1加密碼解碼，復原前述認證用碼者；轉換機構，係根據前述所傳送之轉換

對象部分特定資訊，轉換前述復原之認證用碼之前述轉換對象部分，生成轉換認證用碼者；第2加密碼生成機構，係用前述密碼鍵加密前述轉換認證用碼，生成第2加密碼者；及傳送機構，係將前述第2加密碼向前述認證要求裝置傳送者；前述認證要求裝置係使用前述密碼鍵將前述所傳送之第2加密碼解碼後，復原前述轉換認證用碼，並藉由將其與前述比較對象碼比較，認證前述認證對象裝置。

此外，本發明之認證對象裝置，其特徵在於其係保持至少一個與認證要求裝置共用之密碼鍵，並成為藉由該認證要求裝置之認證對象者；且包含：第1加密碼接收機構，係從前述認證要求裝置接收使用前述密碼鍵加密認證用碼所得到之第1加密碼者；轉換對象部分接收機構，係從前述認證要求裝置接收特定前述認證用碼中至少一對相互不同之部分作為轉換對象部分之轉換對象部分特定資訊者；認證用碼解碼機構，係用前述密碼鍵將前述接收之第1加密碼解碼，復原前述認證用碼者；轉換機構，係根據前述接收之轉換對象部分特定資訊，轉換前述復原之認證用碼之前述轉換對象部分，生成轉換認證用碼者；第2加密碼生成機構，係用前述密碼鍵將前述轉換認證用碼加密，生成第2加密碼者；及第2加密碼傳送機構，係將前述第2加密碼向前述認證要求裝置傳送者；且前述第2加密碼供給於藉由前述認證要求裝置之認證處理。

此外，本發明之另一認證對象裝置，其特徵在於其係保持至少一個與認證要求裝置共用之密碼鍵，並成為藉由該

認證要求裝置之認證對象者；且包含：轉換對象部分接收機構，係從前述認證要求裝置接收特定前述密碼鍵中至少一對相互不同之部分作為轉換對象部分之轉換對象部分特定資訊者；第1加密碼接收機構，係從前述認證要求裝置接收第1加密碼，該第1加密碼係使用轉換前述密碼鍵之前述轉換對象部分之轉換密碼鍵，將認證用碼加密所得到者：轉換機構，係根據前述接收之轉換對象部分特定資訊，轉換前述密碼鍵之前述轉換對象部分，生成轉換密碼鍵者；認證用碼解碼機構，係使用前述轉換密碼鍵將前述接收之第1加密碼解碼，復原前述認證用碼者；第2加密碼生成機構，係將前述復原之認證用碼加密，生成第2加密碼者；及第2加密碼傳送機構，係將前述第2加密碼向前述認證要求裝置傳送者；且前述第2加密碼供給於藉由前述認證要求裝置之認證處理。

【實施方式】

以下參照圖式說明本發明之實施形態。本發明之一實施形態之認證系統1，如圖1所示，其係包含認證對象裝置10與認證要求裝置20而構成。

認證對象裝置10係成為藉由認證要求裝置20之認證對象之周邊機器等裝置，其包含控制部11、記憶部12及通信部13所構成。

控制部11係CPU等，其按照儲存於記憶部12之程式而動作。該控制部11進行實現作為認證對象裝置之功能之處理。具體而言，控制部11接收從認證要求裝置20所傳送之

資料，並根據該接收資料所包含之控制命令執行加密或解碼等各種處理。關於本實施形態中控制部11所執行之處理，將於後面詳細闡述。

記憶部12係包含快閃ROM(Read Only Memory)及RAM(Random Access Memory)等記憶元件所構成者。該記憶部12儲存有藉由控制部11所執行之程式及用於認證處理之密碼鍵資料。此外，該記憶部12亦作為儲存在控制部11處理過程中所需之各種資料之工作記憶體而動作。

通信部13例如包含串列通信埠而成，其與認證要求裝置20連接。又，通信部13包含暫時記憶資料之輸入暫存器與輸出暫存器之兩個暫存器。該通信部13向認證要求裝置20傳送控制部11向輸出暫存器輸出之資訊。並且，通信部13將從認證要求裝置20接收之資訊寫入輸入暫存器。寫入輸入暫存器之資訊由控制部11讀取。

認證要求裝置20係進行認證對象裝置10之認證之電氣機器本體等裝置，包含控制部21、記憶部22及通信部23所構成。

控制部21係CPU等，其按照儲存於記憶部22之程式而動作。該控制部21進行實現作為認證要求裝置之功能之處理。具體而言，控制部21生成認證用碼、並將其加密後作為加密碼向認證對象裝置10輸出。並且，控制部21接收從認證對象裝置10所傳送之資料，而取得加密碼，並藉由檢驗將該加密碼解碼而得到之資料，執行認證認證對象裝置10之認證處理。關於本實施形態中控制部21所執行之認證

處理，將於後面詳細闡述。

記憶部22係包含快閃ROM(Read Only Memory)及RAM(Random Access Memory)等記憶元件，與硬碟驅動器等磁碟裝置中之至少一方所構成者。該記憶部22儲存有藉由控制部21執行之程式及用於認證處理之密碼鍵資料。並且，該記憶部22亦作為儲存在控制部21處理過程中所需之各種資料之工作記憶體而動作。

通信部23例如係串列通信埠，其與認證對象裝置10之通信部13連接。通信部23按照從控制部21所輸入之指令向認證對象裝置10傳送資訊。並且，該通信部23向控制部21輸出從認證對象裝置10接收之資訊。

此處，就認證對象裝置10之控制部11所實現之功能進行說明。再者，在本實施形態中，認證對象裝置10之記憶部12預先儲存有複數之密碼鍵k0、k1、…。並且，與密碼鍵相對應附有作為用於依序特定密碼鍵之鍵號0、1、…。

控制部11其於功能上，如圖2所例示，係包含控制命令處理部31、轉換處理部32及密碼處理部33所構成。

控制命令處理部31藉由從輸入暫存器讀取，而取得通信部13從認證要求裝置20接收之包含有關認證處理之各種控制資訊之控制命令。

作為控制命令所包含的控制資訊，例如有如下之資訊：

(1) 指令是否對密碼鍵及認證用碼分別進行轉換之轉換處理指令資訊；

(2) 指令進行加密、解碼中之任一處理，或不進行任何

處理之密碼處理指令資訊；

(3) 特定讀取成為處理對象之對象資料之位置之輸入位置特定資訊；

(4) 特定寫入對於對象資料執行特定處理之結果之位置之輸出位置特定資訊；

(5) 特定用於加密或解碼處理之密碼鍵之密碼鍵特定資訊；

(6) 分別對在密碼鍵及認證用碼中根據轉換處理指令資訊被指定作為轉換對象之各資料，特定轉換對象部分之轉換對象部分特定資訊。

取得控制命令之控制命令處理部31根據控制命令所包含之控制資訊執行各種處理。具體而言，首先，根據輸入位置特定資訊特定讀取成為處理對象之對象資料之位置。作為讀取位置，有通信部13之輸入暫存器或記憶部12內之特定之工作記憶區域。作為讀取位置在指定為輸入暫存器時，控制命令處理部31藉由從輸入暫存器讀取、而取得由認證要求裝置20經由通信部13所傳送之對象資料。

繼之，控制命令處理部31根據轉換處理指令資訊及密碼處理指令資訊，以特定之順序，使轉換處理部32執行將對象資料及/或密碼鍵之轉換對象部分轉換之轉換處理，或使密碼處理部33執行對象資料之加密或解碼。

作為具體例，在作為密碼處理指令資訊包含有進行加密之指令資訊時，控制部11按照轉換處理指令資訊之內容，在進行對象資料之轉換處理與由密碼鍵特定資訊所特定之

密碼鍵之轉換處理後，進行對象資料之加密。此外，作為密碼處理指令資訊包含有進行解碼之指令資訊時，控制部11按照轉換處理指令資訊之內容，在進行由密碼鍵特定資訊所特定之密碼鍵轉換處理後，進行對象資料之解碼，並進一步按照轉換處理指令資訊之內容，進行業已解碼之對象資料之轉換處理。

再者，控制命令處理部31將對於對象資料完成其轉換處理及加密、解碼等處理所得到之資料，作為輸出資料寫入根據輸出位置特定資訊而特定之寫入位置。作為寫入位置，有通信部13之輸出暫存器或記憶部12內特定之工作記憶區域。並且，寫入輸出暫存器之資料藉由通信部13向認證要求裝置20傳送。

轉換處理部32根據控制命令處理部31所取得之控制命令中所包含的控制資訊，進行對象資料及/或密碼鍵之轉換對象部分之轉換處理。成為轉換對象之轉換對象資料的種類(對象資料或密碼鍵)，由控制命令中所包含之轉換處理指令資訊指定。並且，在密碼鍵作為轉換對象被指定時，保持於記憶部12之密碼鍵中之由控制命令所包含之密碼鍵特定資訊所特定之密碼鍵，成為轉換對象資料。

此外，轉換處理部32根據控制命令所包含之轉換對象部分特定資訊，特定轉換對象資料中之轉換部分。轉換對象部分特定資訊，具體而言，例如其係包含指定轉換對象資料中之2個位置之指定部分的2個數值之資訊。此時，轉換處理部32相互轉換藉由轉換對象部分特定資訊所特定之2

個位置之指定部分。例如轉換對象資料為128位元，將其以8位元單位分割之16個位元塊作為轉換處理單位。此時，於轉換對象部分特定資訊中，包含在從0至15中相互不同之2個數值，轉換處理部32以藉由該數值所特定之2個位元塊作為轉換對象部分進行特定。作為一例，在轉換對象部分特定資訊係由3與5此2個數值構成時，轉換處理部32轉換轉換對象資料所包含之16個位元塊中之從0開始數之第3個位元塊、與第5個位元塊。

此外，轉換對象部分特定資訊亦可為包含指定轉換對象資料中之1個位置之指定部分的1個數值之資訊。此時，轉換處理部32將藉由轉換對象部分特定資訊所指定之指定部分，與對應該指定部分而決定之對應部分作為轉換對象部分進行特定，並轉換該等2個部分。作為具體之例，在以由前述之16個位元塊構成之128位元之轉換對象資料為例的情形時，轉換對象部分特定資訊中包含從0至15中之任意之1個數值。轉換處理部32按照該數值決定對應之從0至15中任意之數值，並將藉由決定之數值所指定之部分作為對應部分。作為一例，在轉換對象部分特定資訊中所包含之數值為6(0110b)時，轉換處理部32藉由對該數值進行4位元之位元反轉處理，而得到指定對應部分之9(1001b)之數值，然後，將從0開始數之第6個位元塊(指定部分)與第9個位元塊(對應部分)作為轉換對象部分特定、並進行轉換。如此藉由根據指定1個轉換對象部分之轉換對象部分特定資訊，特定2個位置之轉換對象部分，可減少轉換對象部

分特定資訊所包含之資料，並可減少在認證對象裝置10與認證要求裝置20之間傳送、接收之資料量。

轉換處理部32在對記憶於特定之工作記憶區域之對象資料進行轉換時，亦可在該工作記憶區域覆寫轉換後之對象資料。此外，在對快閃ROM等不可覆寫之記憶區域所記憶之密碼鍵進行轉換時，將轉換後之密碼鍵寫入特定之工作記憶區域。

密碼處理部33根據控制命令處理部31所取得之控制命令中所包含之控制資訊，對對象資料進行加密或解碼處理。作為加密或解碼之演算法，例如可使用DES(Data Encryption Standard)或AES(Advanced Encryption Standard)等任意之共用鍵密碼演算法。

再者，若轉換處理部32對象資料進行轉換處理，則密碼處理部33對業已完成轉換之對象資料進行加密。並且，密碼處理部33，係使用儲存於記憶部12之密碼鍵中的藉由控制命令所包含之密碼鍵特定資訊所特定之密碼鍵作為用於各個處理之密碼鍵，進行加密或解碼。此時，若轉換處理部32對該特定之密碼鍵進行轉換處理，則密碼處理部33使用業已完成轉換之密碼鍵進行加密或解碼。

其次，就認證要求裝置20之控制部21所實現之功能進行說明。此外，本實施形態中，認證要求裝置20之記憶部22儲存有與認證對象裝置10同樣的複數之密碼鍵k0、k1、…。

該控制部21其在功能上，如圖3所例示，係包含認證處

理部41、轉換處理部42及密碼處理部43所構成。

認證處理部41係以認證要求裝置20之電源進入之時點、認證對象裝置10連接於認證要求裝置20之時點、或從上次認證處理後經過特定時間之時點等之特定時點進行認證處理。

作為具體之例，認證處理部41首先生成用於認證之認證用碼。並且，在認證處理中進行密碼鍵或認證用碼之轉換時，作為隨機值生成轉換對象部分特定資訊。然後，使轉換處理部42執行認證用碼等成為處理對象之對象資料或密碼鍵之轉換，或使密碼處理部43執行對象資料之加密或解碼。

此外，認證處理部41，藉由與所加密之認證用碼一起，對認證對象裝置10輸出控制命令，而向認證對象裝置10傳送認證用碼。並且，藉由對認證對象裝置10輸出控制命令，將傳送至認證對象裝置10之認證用碼或對認證用碼經完成轉換處理而得到之轉換認證用碼等資料加密後傳送。認證處理部41藉由將接收之資料解碼後得到之資料，與認證要求裝置20保持之資料進行比較，進行認證對象裝置10之認證。關於認證處理部41進行處理之詳細，將於後面進行詳細闡述。

轉換處理部42根據認證處理部41之要求，與認證對象裝置10之轉換處理部32同樣，進行將對象資料或密碼鍵之轉換對象部分轉換之轉換處理。此外，密碼處理部43根據認證處理部41之要求，使用與認證對象裝置10之密碼處理部

33同樣的加密演算法，執行對象資料之加密或解碼之處理。

其次，聯繫以上說明之各部分，就進行認證對象裝置10之認證之認證處理的若干例進行說明。

首先，根據圖4之流程圖，就伴有認證用碼轉換之認證處理例進行說明。

認證要求裝置20之認證處理部41首先生成認證用碼R(S1)。此處作為具體例，認證用碼R設為128位元之隨機值。並且，以下作為一例，就認證用碼R的值為0x00112233445566778899AABBCCDDEEFF之情形進行說明。

其次，認證處理部41生成用於認證用碼R轉換之轉換對象部分特定資訊(S2)。此處作為具體例，轉換對象部分特定資訊係在將128位元之認證用碼分割成8位元大小之16個位元塊時，作為轉換對象部分指定1個位元塊之1個值，設為隨機決定之從0至15中之任意數值。並且，以下作為一例，就轉換對象部分特定資訊為0x06之情形進行說明。

繼之，認證處理部41生成對認證對象裝置10之控制命令(S3)。此處，設定認證處理部41生成之控制命令包含如下控制資訊：

(1) 作為轉換處理指令資訊，指令執行僅轉換認證用碼之資訊；

(2) 作為密碼處理指令資訊，指令執行解碼處理之資訊；

(3) 作為輸入位置特定資訊，顯示輸入暫存器之資訊；

(4) 作為輸出位置特定資訊，顯示特定之工作記憶區域M之資訊；

(5) 作為密碼鍵特定資訊，密碼鍵k0之鍵號為"0"；

(6) 作為相對認證用碼之轉換對象部分特定資訊，為"0x06"。

然後，根據認證處理部41之要求，密碼處理部43用密碼鍵k0將認證用碼R加密，生成加密碼(S4)。此處，若設定用密碼鍵k將成為對象之資料d加密為ENC(d，k)，則在該S4之處理中所生成之加密碼為ENC(R，k0)。

繼之，認證處理部41將藉由S3之處理而生成之控制命令，與藉由S4之處理密碼處理部43生成之加密碼ENC(R，k0)，經由通信部23向認證對象裝置10輸出(S5)。

在藉由S5之處理傳送後，轉換處理部42根據認證處理部41之要求，進行認證用碼R之轉換(S6)。此處，轉換對象部分特定資訊為"0x06"，對應藉此所指定之指定部分之另一轉換對象部分(對應部分)，例如藉由4位元之位元反轉處理由0x09所指定之部分決定。此處，若設定將相對成為對象之資料d、轉換由轉換對象部分特定資訊s所特定之轉換對象部分之資料標記為SHF(d，s)，則轉換後之認證用碼為SHF(R，0x06)。此處，SHF(R，0x06)的值成為0x00112233445599778866AABBCCDDEEFF。

另一方面，認證對象裝置10之控制命令處理部31，從通信部13之輸入暫存器讀取藉由S5之處理由認證要求裝置20

所傳送之控制命令及加密碼ENC(R，k0)。

在由認證要求裝置20所傳送之控制命令中所包含之密碼處理指令資訊為指令解碼之資訊時，認證對象裝置10在認證用碼之轉換處理前執行解碼處理。因此，首先密碼處理部33根據控制命令處理部31之要求，進行加密碼之解碼，復原認證用碼(S7)。此時，成為解碼對象之對象資料係從藉由輸入位置特定資訊所特定之輸入暫存器讀取之加密碼ENC(R，k0)。此外，密碼處理部33使用藉由密碼鍵特定資訊所特定之密碼鍵k0進行解碼。藉此得到加密前之認證用碼R。

繼之，根據控制命令處理部31之要求，轉換處理部32進行藉由S7之處理已被解碼之認證用碼R之轉換，生成轉換認證用碼(S8)。此處，因為轉換對象部分特定資訊為"0x06"，故與認證要求裝置20之轉換處理部42同樣，轉換16個位元塊中從第0個開始數之第6個位元塊與第9個位元塊。藉此，作為轉換認證用碼，得到與藉由S6之處理所得到之資料相同的SHF(R，0x06)。

控制命令處理部31將藉由此等一系列處理而得到之轉換認證用碼SHF(R，0x06)，寫入藉由輸出位置特定資訊所特定之工作記憶區域M(S9)。藉此，認證對象裝置10結束對藉由S5之處理所傳送之控制命令之處理，並向認證要求裝置20輸出正常結束之宗旨之應答(S10)。

認證要求裝置20之認證處理部41接收到藉由S10處理之正常結束之宗旨之應答後，繼續執行以下之處理。

首先，認證處理部41生成128位元之隨機值q(S11)。再者，所生成之隨機值q係作為虛擬資料所使用，而不是認證處理所必需者。

然後，認證處理部41與S2之處理同樣，生成新的轉換對象部分特定資訊(S12)。以下作為一例，就轉換對象部分特定資訊為0x02之情形進行說明。

繼之，認證處理部41生成對認證對象裝置10之新的控制命令(S13)。此處，作為具體例，設定生成包含如下控制資訊之控制命令：

(1) 作為轉換處理指令資訊，指令執行僅轉換認證用碼之資訊；

(2) 作為密碼處理指令資訊，指令執行加密處理之資訊；

(3) 作為輸入位置特定資訊，顯示工作記憶區域M之資訊；

(4) 作為輸出位置特定資訊，顯示輸出暫存器之資訊；

(5) 作為密碼鍵特定資訊，密碼鍵k1之鍵號為"1"；

(6) 作為相對認證用碼之轉換對象部分特定資訊，為"0x02"。

此處，亦可根據認證處理部41之要求，密碼處理部43將藉由S11生成之隨機值q加密。藉此，可使前述之從S1至S6之處理與從S11至後述之S15之處理之流程一致，可藉由共用程式程序實現認證處理部41所執行之部分功能。但，因隨機值q係作為虛擬資料所使用，故加密處理不是必須

者。

繼之，認證處理部41將藉由S13之處理而生成之控制命令與作為虛擬資料之藉由S11之處理而生成之隨機值q(或被加密之隨機值q)，經由通信部23向認證對象裝置10輸出(S14)。此外，因為藉由控制命令所包含之輸入位置特定資訊所特定之讀取位置不是輸入暫存器而是工作記憶區域，故藉由S14之處理而傳送之隨機值q(或被加密之隨機值q)在認證對象裝置10中不被使用。但，在此種情形下，亦可藉由將虛擬資料與控制命令合併傳送，可使得從通信內容難以推測處理內容，而進行對通信之第三者之更強的認證處理。

在藉由S14之處理之傳送後，轉換處理部42根據認證處理部41之要求，對藉由S6之處理所得到之轉換後的認證用碼SHF(R，0x06)進一步進行轉換(S15)。此處，轉換對象部分特定資訊係藉由S13所生成之"0x02"，對應藉此所指定之指定部分之另一轉換對象部分(對應部分)，係藉由4位元之位元反轉處理由0x0d所指定之部分決定。藉由轉換處理所生成之用作比較對象之轉換後之認證用碼(比較對象碼)成為SHF(SHF(R，0x06)，0x02)。此處，SHF(SHF(R，0x06)，0x02)的值為0x0011DD33445599778866AABBCC22EEFF。

另一方面，認證對象裝置10之控制命令處理部31，從通信部13之輸入暫存器讀取藉由S14之處理由認證要求裝置20所傳送之控制命令。

在控制命令所包含之密碼處理指令資訊為指令加密之資

訊時，認證對象裝置10在加密處理前進行轉換處理。因此，轉換處理部32首先根據控制命令處理部31之要求，對對象資料進行轉換，更新轉換認證用碼(S16)。此處，成為轉換對象之對象資料係轉換認證用碼SHF(R，0x06)，其係藉由S10之處理儲存於藉由輸入位置特定資訊所特定之讀取位置之工作記憶區域M者。此處，由於轉換對象部分特定資訊為"0x02"，故與S15之處理結果相同，作為更新後之轉換認證用碼可得到SHF(SHF(R，0x06)，0x02)。

繼之，根據控制命令處理部31之要求，密碼處理部33對S16之處理所得到結果之轉換認證用碼進行加密，生成新的加密碼(S17)。此時，密碼處理部33使用藉由密碼鍵特定資訊所特定之密碼鍵k1進行加密。藉此，得到加密碼ENC(SHF(SHF(R，0x06)，0x02)，k1)。

控制命令處理部31將藉由此等一系列處理所得到之加密碼，寫入藉由輸出位置特定資訊所特定之寫入位置之輸出暫存器(S18)。藉此，加密碼ENC(SHF(SHF(R，0x06)，0x02)，k1)向認證要求裝置20傳送。

接受由認證對象裝置10所傳送之加密碼之認證要求裝置20，以如下方式進行最終是否認證認證對象裝置10之判定處理。首先，根據認證處理部41之要求，密碼處理部43使用密碼鍵k1將藉由S18之處理所傳送之加密碼解碼(S19)。藉此，得到轉換認證用碼SHF(SHF(R，0x06)，0x02)。

繼之，認證處理部41將藉由S19之處理所解碼之轉換認證用碼，與S15之處理結果所得到之比較對象碼進行比

較，藉此判定認證對象裝置10之認證成功與否(S20)。

在認證對象裝置10中，如果正常地進行轉換處理及藉由與認證要求裝置20共用之密碼鍵的加密、解碼處理，則藉由S20之處理所比較之2個碼均為SHF(SHF(R，0x06)，0x02)，為一致。此時，判定認證成功，認證要求裝置20進行使認證對象裝置10之功能為有效等之處理。另一方面，如果從認證作對象裝置10取得之轉換認證用碼與在認證要求裝置20內生成之比較對象碼不一致時，則判定認證失敗，認證要求裝置20按照判定結果，進行使認證對象裝置10之至少部分功能失效之處理。

此外，在以上說明之處理中，係設定在S3及S13生成之2個控制命令之雙方包含指令認證用碼轉換之轉換處理指令資訊，轉換處理部32及42均對認證用碼進行合計2次之轉換處理。但，對於轉換處理亦可設定為某一方只進行一次。此時，作為2個控制命令中之任一控制命令所包含之轉換處理指令資訊，藉由使用指令不進行轉換處理之資訊，可不伴隨有轉換處理而進行加密碼之傳送或接收之處理。

此外，轉換處理部32及42亦可設定為進行3次以上之轉換處理。此時，例如認證處理部41在S10與S11之處理之間，進一步進行如下之處理。亦即，向認證對象裝置10輸出控制命令，該控制命令包含指令不進行任何加密、解碼之密碼處理指令資訊，與指令對認證用碼進行轉換處理之轉換處理指令資訊。藉此，認證對象裝置10不進行加密及

解碼處理，而單純地對自己本身所保持之轉換認證用碼再次進行轉換處理。另一方面，認證要求裝置20亦對自己本身所保持之轉換後之認證用碼進行同樣之轉換處理。藉由將該處理反覆進行特定次數，多次轉換用於認證之認證用碼，可在與最初傳送時生成加密碼之原資料所不同之資料中更新認證用碼。

此外，在以上說明之認證處理後，認證處理部41再次進行認證時，在S1之處理中亦可代替將認證用碼作為隨機值生成之處理，使用例如在前次之S20之處理成為比較對象、對最初的認證用碼R進行複數次轉換處理之轉換認證用碼。藉此，可不進行生成隨機值之處理，而使用與最初的認證處理中之認證用碼不同之認證用碼進行認證處理。若根據此種方法，每逢反覆進行認證處理時，認證用碼均藉由轉換處理而從最初的值偏離，例如即使複數次之認證處理中之一系列傳送接收資料被第三者所接收，亦難以解析詳細之認證處理。

其次，根據圖5之流程圖，就伴隨有密碼鍵轉換之認證處理之例進行說明。

認證要求裝置20之認證處理部41，首先生成認證用碼R(S21)。此處，與前述之例同樣，設認證用碼R為128位元之隨機值。

然後，認證處理部41生成用於密碼鍵轉換之轉換對象部分特定資訊(S22)。與認證用碼之情形相同，轉換對象部分特定資訊在將128位元之密碼鍵分割成8位元大小之16個

位元塊時，作為轉換對象部分係指定1個位元塊之1個值，設為隨機決定之從0至15之任意數值。再者，以下作為具體例，就轉換對象部分特定資訊為0x00之情形進行說明。

繼之，根據認證處理部41之要求，轉換處理部42使用藉由S22之處理所生成之轉換對象部分特定資訊進行密碼鍵之轉換(S23)。此外，此處作為成為轉換對象之密碼鍵設定使用密碼鍵k0。藉此，轉換處理部42生成轉換密碼鍵SHF(k0，0x00)。

然後，認證處理部41生成對認證對象裝置10之控制命令(S24)。此處作為具體例，生成包含如下控制資訊之控制命令。

(1) 作為轉換處理指令資訊，指令執行僅轉換密碼鍵之資訊；

(2) 作為密碼處理指令資訊，指令執行解碼處理之資訊；

(3) 作為輸入位置特定資訊，顯示輸入暫存器之資訊；

(4) 作為輸出位置特定資訊，顯示工作記憶區域M之資訊；

(5) 作為密碼鍵特定資訊，密碼鍵k0之鍵號為"0"；

(6) 作為對認證用碼之轉換對象部分特定資訊，為"0x00"。

其次，根據認證處理部41之要求，密碼處理部43使用藉由S23之處理所生成之轉換密碼鍵SHF(k0，0x00)將認證用碼R加密，而生成加密碼(S25)。所生成之加密碼為

ENC(R，SHF(k0，0x00))。

繼之，認證處理部41將藉由S24之處理生成之控制命令，與藉由S25之處理密碼處理部43生成之加密碼ENC(R，SHF(k0，0x00))，經由通信部23向認證對象裝置10輸出(S26)。

認證對象裝置10之控制命令處理部31，從通信部13之輸入暫存器讀取藉由S26之處理由認證要求裝置20所傳送之控制命令及加密碼ENC(R，SHF(k0，0x00))。

由認證要求裝置20所傳送之控制命令所包含之轉換處理指令資訊為指令密碼鍵轉換之資訊時，認證對象裝置10於進行加密或解碼之處理前執行密碼鍵之轉換處理。因此，首先轉換處理部32根據控制命令處理部31之要求，進行密碼鍵之轉換，生成轉換密碼鍵(S27)。此時，成為轉換處理對象之轉換對象資料為藉由控制命令所包含之密碼鍵特定資訊所特定之密碼鍵k0。藉此，轉換處理部32生成與在S23認證要求裝置20所生成者相同的轉換密碼鍵SHF(k0，0x00)。

然後，密碼處理部33根據控制命令處理部31之要求，進行加密碼之解碼，復原認證用碼(S28)。此時，成為解碼對象之對象資料，係從藉由輸入位置特定資訊所特定之輸入暫存器所讀取之加密碼ENC(R，SHF(k0，0x00))。並且，密碼處理部33使用藉由S27之處理所生成之轉換密碼鍵SHF(k0，0x00)進行解碼。藉此，得到加密前之認證用碼R。

控制命令處理部31將藉由該等一系列之處理所得到之認證用碼R，寫入藉由輸出位置特定資訊所特定之工作記憶區域M(S29)。藉此，認證對象裝置10結束對藉由S26之處理所傳送之控制命令之處理，向認證要求裝置20輸出業已正常結束之宗旨之應答(S30)。

認證要求裝置20之認證處理部41接收到藉由S30處理之正常結束宗旨之應答，繼續執行以下之處理。

首先，認證處理部41生成128位元之隨機值q(S31)。並且，所生成之隨機值q與前述之伴有認證用碼轉換之認證處理例同樣，係虛擬資料。

然後，認證處理部41生成新的轉換對象部分特定資訊(S32)。以下作為一例，就轉換對象部分特定資訊為0x05之情形進行說明。

繼之，根據認證處理部41之要求，轉換處理部42使用藉由S32之處理所生成之轉換對象部分特定資訊進行密碼鍵之轉換(S33)。此外，此處作為成為轉換對象之密碼鍵，設定使用密碼健k1。藉此，轉換處理部42生成轉換密碼鍵SHF(k1，0x05)。

再者，認證處理部41生成對認證對象裝置10之新的控制命令(S34)。此處作為具體例，設定生成包含如下控制資訊之控制命令。

(1) 作為轉換處理指令資訊，指令執行僅轉換密碼鍵之資訊；

(2) 作為密碼處理指令資訊，指令執行加密處理之資

訊；

(3) 作為輸入位置特定資訊，顯示工作記憶區域M之資訊；

(4) 作為輸出位置特定資訊，顯示輸出暫存器之資訊；

(5) 作為密碼鍵特定資訊，密碼鍵k1之鍵號為"1"；

(6) 作為對認證用碼之轉換對象部分特定資訊，為"0x05"。

此處，亦可與前述之伴有認證用碼轉換之認證處理例同樣，將密碼處理部41在S31生成之隨機值q加密。繼之，認證處理部41將藉由S34之處理而生成之控制命令，與藉由S31之處理而生成之作為虛擬資料之隨機值q(或加密之隨機值q)，經由通信部23向認證對象裝置10輸出(S35)。

認證對象裝置10之控制命令處理部31，將藉由S35之處理由認證要求裝置20所傳送之控制命令，從通信部13之輸入暫存器讀取。

因為控制命令所包含之轉換處理指令資訊係指令密碼鍵轉換之資訊，故與S27之處理同樣，認證對象裝置10於加密處理前執行轉換處理。因此，首先轉換處理部32根據控制命令處理部31之要求，對密碼鍵進行轉換，生成轉換密碼鍵(S36)。此處，成為轉換對象之密碼鍵為藉由密碼鍵特定資訊所特定之密碼鍵k1。並且，由於轉換對象部分特定資訊為0x05，故轉換處理部32與S33之處理結果同樣，作為轉換密碼鍵生成SHF(k1，0x05)。

繼之，根據控制命令處理部31之要求，密碼處理部33對

對象資料進行加密，生成加密碼(S37)。此處，成為加密對象之對象資料係認證用碼R，該認證用碼R係藉由S29之處理儲存於藉由輸入位置特定資訊所特定之讀取位置之工作記憶區域M。此時密碼處理部33，使用藉由S36之處理所生成之轉換密碼鍵SHF(k1，0x05)進行加密。藉此，得到加密碼ENC(R，SHF(k1，0x05))。

控制命令處理部31將藉由此等一系列處理所得到之加密碼，寫入藉由輸出位置特定資訊所特定之寫入位置之輸出暫存器(S38)。藉此，加密碼ENC(R，SHF(k1，0x05)向認證要求裝置20傳送。

接受由認證對象裝置10所傳送之加密碼之認證要求裝置20，以如下方式進行最終是否認證認證對象裝置10之判定處理。首先，根據認證處理部41之要求，密碼處理部43將藉由S38之處理所傳送之加密碼解碼(S39)。此時，密碼處理部43使用藉由S33之處理所生成之轉換密碼鍵SHF(k1，0x05)進行解碼，藉此，得到認證用碼R。

繼之，認證處理部41將藉由S39之處理所解碼之認證用碼，與由S21之處理而在最初生成之認證用碼R進行比較，藉此判定認證對象裝置10之認證成功與否(S40)。在認證對象裝置10中，如果正常地進行處理，藉由S40處理所比較之2個碼均為R，因為一致故判定認證成功。另一方面，如果從認證作對象裝置10取得之認證用碼與在認證要求裝置20內生成之認證用碼不一致時，則判定認證失敗。

此外，在以上說明之處理中，係設定在S24及S34生成之

2個控制命令之雙方包含指令密碼鍵轉換之轉換處理指令資訊，但轉換處理亦可設定某一方只進行一次。此外，轉換處理部32及42亦可設定分別進行3次以上密碼鍵之轉換處理。此時，認證要求裝置20與前述之伴有認證用碼轉換之認證處理之情形同樣，對認證對象裝置10輸出控制命令，該控制命令包含指令不進行任何加密、解碼之密碼處理指令資訊與指令進行密碼鍵轉換處理之轉換處理指令資訊；並且，對自己本身保持之密碼鍵亦進行同樣之轉換處理。藉由將該處理反覆進行特定次數，可進一步用與最初保持者所不同之密碼鍵進行加密、及解碼處理。

此外，在以上說明之認證處理後，認證處理部41再次進行認證時，亦可使用業已完成轉換處理之轉換密碼鍵進行認證處理。此時，認證要求裝置20使用藉由上次之S23或S33之處理等而生成之轉換密碼鍵進行認證處理。並且，在該情形下之下次認證處理中，亦可再次進行伴有密碼鍵轉換之認證處理。此外，認證對象裝置10預先將藉由上次之S27或S36之處理等而生成之轉換密碼鍵保持在特定之工作記憶區域等，並使用該等轉換密碼鍵進行根據來自認證要求裝置20之控制命令之加密、解碼處理。藉此，每當反覆進行認證處理時，密碼鍵藉由轉換處理而從最初的密碼鍵偏離，故與反覆使用相同密碼鍵之情形相比較，密碼鍵之解析變得困難。

再者，認證要求裝置20亦可將以上說明之認證用碼之轉換處理與密碼鍵之轉換處理組合使用。此時，可藉由於認

證要求裝置20生成之控制命令中，包含指令對認證用碼與密碼鍵雙方進行轉換之轉換處理指令資訊，使用已完成轉換處理之密碼鍵進行加密、或解碼，並可在認證處理途中轉換認證用碼。藉此，即使通信資料被第三者接收，認證處理之詳細程序亦變得更加難以解析，可提高安全性。

繼之，根據圖6之流程圖，就伴有密碼鍵轉換之認證處理之另一例進行說明。

認證要求裝置20之認證處理部41，首先生成認證用碼R(S41)。此處與前述之例同樣，設定認證用碼R為128位元之隨機值。

然後，認證處理部41生成用於密碼鍵轉換之轉換對象部分特定資訊(S42)。與前述之例同樣，轉換對象部分特定資訊係在將128位元之密碼鍵分割成8位元大小之16個位元塊時，作為轉換對象部分指定1個位元塊之1個值，設為隨機決定之從0至15之任意數值。再者，以下作為具體例，就轉換對象部分特定資訊為0x07之情形進行說明。

其次，認證處理部41生成對認證對象裝置10之控制命令(S43)。此處作為具體例，生成包含如下控制資訊之控制命令。

(1) 作為轉換處理指令資訊，指令執行僅轉換密碼鍵之資訊；

(2) 作為密碼處理指令資訊，指令執行解碼處理之資訊；

(3) 作為輸入位置特定資訊，顯示輸入暫存器之資訊；

(4) 作為輸出位置特定資訊，顯示工作記憶區域M之資訊；

(5) 作為密碼鍵特定資訊，密碼鍵k0之鍵號為"0"；

(6) 作為對認證用碼之轉換對象部分特定資訊，為"0x07"。

其次，根據認證處理部41之要求，密碼處理部43使用密碼鍵k0將認證用碼R加密，生成加密碼(S44)。所生成之加密碼為ENC(R，k0)。

繼之，認證處理部41將藉由S43之處理而生成之控制命令與藉由S44之處理密碼處理部43生成之加密碼ENC(R，k0)，經由通信部23向認證對象裝置10輸出(S45)。

進一步，根據認證處理部41之要求，轉換處理部42使用藉由S42之處理所生成之轉換對象部分特定資訊進行密碼鍵之轉換(S46)。此處成為轉換對象之密碼鍵，係藉由密碼鍵特定資訊所特定之密碼鍵k0，而該密碼鍵特定資訊係包含於藉由S43之處理所生成之控制命令中。藉此，轉換處理部42生成轉換密碼鍵SHF(k0，0x07)。

繼之，根據認證處理部41之要求，密碼處理部43對藉由S45之處理而向認證對象裝置10傳送之加密碼ENC(R，k0)進行解碼處理(S47)。但，作為此時之密碼鍵，使用由S46之處理所生成之轉換密碼鍵SHF(k0，0x07)。在本實施形態中，密碼處理部43使用共用之密碼鍵進行加密及解碼之共用鍵密碼演算法。因此，即使將用密碼鍵k0加密之加密碼用轉換密碼鍵SHF(k0，0x07)解碼，原來之認證用碼R

亦不能復原，而得到另外的128位元之比較對象碼R'。

另一方面，認證對象裝置10之控制命令處理部31將藉由S45之處理由認證要求裝置20傳送之控制命令及加密碼ENC(R，k0)從通信部13之輸入暫存器讀取。

此處，與前述之伴有密碼鍵轉換之認證處理之第1例之情形同樣，首先，轉換處理部32根據控制命令處理部31之要求，進行密碼鍵之轉換，生成轉換密碼鍵(S48)。此時，成為轉換處理對象之轉換對象資料，係由控制命令所包含之密碼鍵特定資訊所特定之密碼鍵k0。藉此，轉換處理部32生成與在S46認證要求裝置20生成者相同之轉換密碼鍵SHF(k0，0x07)。

然後，密碼處理部33根據控制命令處理部31之要求，進行加密碼之解碼處理(S49)。此時，成為解碼對象之對象資料，係從藉由輸入位置特定資訊所特定之輸入暫存器所讀取之加密碼ENC(R，k0)。此外，密碼處理部33使用藉由S48之處理所生成之轉換密碼鍵SHF(k0，0x07)進行解碼處理，並得到處理結果碼R"。此處亦因為被用於加密之密碼鍵k0與用於解碼之密碼鍵不一致，故作為解碼處理結果所得到之處理結果碼R"與加密的原認證用碼R不同，而與藉由S47之處理在認證要求裝置20所生成之比較對象碼R'一致。

控制命令處理部31將藉由該等一系列之處理所得到之處理結果碼R"，寫入藉由輸出位置特定資訊所特定之工作記憶區域M(S50)。藉此，認證對象裝置10結束對藉由S46之

處理所傳送之控制命令之處理，向認證要求裝置20輸出業已正常結束之宗旨之應答(S51)。

繼之，認證要求裝置20及認證對象裝置10進行加密碼應答通信(S52)。具體而言，根據認證處理部41向認證對象裝置10輸出之控制命令，認證對象裝置10將藉由S50之處理被寫入工作記憶區域M之處理結果碼R"加密後所得到之加密碼，向認證要求裝置20輸出。然後，認證要求裝置20將從認證對象裝置10所傳送之加密碼解碼，復原處理結果碼R"。特別是伴有密碼鍵轉換之加密碼應答通信，係與前述伴有密碼鍵轉換之認證處理之第1例之情形中從S31至S39之處理為同樣之處理。

然後，認證要求裝置20之認證處理部41，藉由將由S52之處理而復原之處理結果碼R"與由S47之處理而生成之比較對象碼R'相比較，進行認證對象裝置10之認證(S53)。在認證對象裝置10中，如果正常地進行處理，藉由S53之處理所比較之處理結果碼R"與比較對象碼R'一致，故判定認證成功。另一方面，如果從認證對象裝置10取得之處理結果碼R"與在認證要求裝置20內生成之比較對象碼R'不一致時，則判定認證失敗。

根據以上說明之認證處理例，從認證要求裝置20向認證對象裝置10所傳送之作為加密碼加密前之資料之認證用碼R，與從認證對象裝置10向認證要求裝置20所傳送之作為加密碼加密前之資料之處理結果碼R"，成為一見即可認為其係無關聯性之完全不同的資料。因此，即便在認證處理

中傳送、接收之通信被第三者所接收，亦難以解析認證處理之詳細，可提高安全性。

此外，在以上說明之本實施形態之認證系統1中，係設定認證要求裝置20與認證對象裝置10保持複數之共用密碼鍵，但各裝置保持之密碼鍵亦可為1個。此時，亦可藉由進行密碼鍵之轉換，使從認證要求裝置20向認證對象裝置10傳送之用於加密之密碼鍵，與從認證對象裝置10向認證要求裝置20傳送之用於加密之密碼鍵成為不同者。

此外，認證系統1亦可替代作為用於認證處理之從最初所保持之密碼鍵，而使用認證要求裝置20作為隨機值而生成之對稱金鑰。此時，認證要求裝置20使用在最初共用而保持之密碼鍵將對稱金鑰加密後向認證對象裝置10傳送。然後，認證對象裝置10使用從最初保持之密碼鍵將所傳送之資料解碼後復原對稱金鑰，並保持於特定之工作記憶區域。藉此，認證系統1可使用以後共用而保持之對稱金鑰進行認證處理。即便為該情形，認證系統1反覆進行認證處理時，例如在藉由對對稱金鑰進行轉換處理而進行認證處理，多次生成對稱金鑰而配信時，亦能夠以比較簡單且容易之處理進行每次使用不同密碼鍵之認證處理。

此外，在以上之說明中，認證要求裝置20與認證對象裝置10係以一對一之關係進行的認證。但本發明之實施形態不限於此等。例如，認證要求裝置20亦可進一步連接於其他的上位認證要求裝置。作為一例，在認證要求裝置20根據上位認證要求裝置之指令，進行對認證對象裝置10之認

證之同時，上位認證要求裝置藉由同樣之認證處理進行對認證要求裝置20之認證。此時，認證要求裝置20對於上位認證要求裝置係作為本發明實施形態中之認證對象裝置而起作用。再者，例如當在認證要求裝置20與認證對象裝置10之間用於認證之密碼鍵洩露於外部等情形時，上位認證要求裝置亦可將用於以後認證處理之新的密碼鍵加密、配信。藉此，即便部分密碼鍵洩漏於外部，亦可使用新配信之密碼鍵進行與迄今之安全等級同樣之認證處理。

此外，上位認證要求裝置亦可在進行對認證要求裝置20之認證之同時，經由認證要求裝置20對認證對象裝置10進行認證。此時，認證要求裝置20係作為中繼裝置而起作用，其係中繼從上位認證要求裝置向認證對象裝置10所傳送之控制命令及加密碼，及從認證對象裝置10向上位認證要求裝置所傳送之加密碼等。

根據以上說明之本實施形態，藉由進行認證用碼或密碼鍵之轉換，在每次傳送、接收時可改變成為加密對象之資料及用於加密之密碼鍵。藉此，即便在只保持少數的密碼鍵之情形時，亦可改變所傳送、接收之加密碼，可使認證處理之詳細難以解析，而提高安全性。

【圖式簡單說明】

圖1係顯示本發明之實施形態之認證系統之概略構成方塊圖。

圖2係顯示認證對象裝置10之功能之一例之功能方塊圖。

圖3係顯示認證要求裝置20之功能之一例之功能方塊圖。

圖4係顯示藉由本發明之實施形態之認證系統之認證處理之一例之方塊圖。

圖5係顯示藉由本發明之實施形態之認證系統之認證處理之另一例之方塊圖。

圖6係顯示藉由本發明之實施形態之認證系統之認證處理之另一例之方塊圖。

【主要元件符號說明】

10	計算機系統
11	CPU
12	記憶體
13	輸入部
14	輸出部
15	記憶媒體
101~104	佈線
105、107	間隔
106	間隔模擬對象外區域
111~114	評價邊緣
121	邊緣分割點
122	模擬評價點數
131	閘極電路佈線
132	源極·汲極擴散層(Diffision)
133	邊緣部

141	閘極電路(Gate)
142	接觸孔(Contact/Via)包含部
143	端帽部(End cap)
144	虛擬圖案
151、152	對象範圍

五、中文發明摘要：

本發明係提供一種能夠以少數的密碼鍵提高安全性之認證系統。

該認證系統之認證要求裝置(20)與認證對象裝置(10)保持共用之密碼鍵，認證要求裝置(20)將認證用碼加密，並選擇認證用碼中相互不同之部分作為轉換對象部分，向認證對象裝置(10)傳送加密之認證用碼及轉換對象部分之資訊，並將認證用碼之轉換對象部分加以轉換，而生成比較對象碼。認證對象裝置(10)將所傳送的碼解碼後所得到之認證用碼之轉換對象部分加以轉換，生成轉換認證用碼，並將轉換認證用碼加密後向認證要求裝置(20)傳送。認證要求裝置(20)藉由將所傳送的碼解碼後所得到之轉換認證用碼與比較對象碼加以比較，認證認證對象裝置(10)。

六、英文發明摘要：

十、申請專利範圍：

1. 一種認證系統，其特徵在於其係包含認證對象裝置、及認證該認證對象裝置之認證要求裝置，且該認證對象裝置與該認證要求裝置保持至少一個相互共用之密碼鍵者；

前述認證要求裝置包含：

第1加密碼生成機構，係使用前述密碼鍵將予以認證用碼加密，生成第1加密碼者；

轉換對象部分選擇機構，係選擇前述認證用碼中之至少一對相互不同之部分作為轉換對象部分者；

傳送機構，係將前述第1加密碼及特定前述轉換對象部分之轉換對象部分特定資訊，向前述認證對象裝置傳送者；及

轉換機構，係將前述認證用碼之前述轉換對象部分予以轉換，生成比較對象碼者；

前述認證對象裝置包含：

認證用碼解碼機構，係用前述密碼鍵將前述所傳送之第1加密碼解碼後，復原前述認證用碼者；

轉換機構，係根據前述所傳送之轉換對象部分特定資訊，將前述復原之認證用碼之前述轉換對象部分予以轉換，生成轉換認證用碼者；

第2加密碼生成機構，係用前述密碼鍵將前述轉換認證用碼予以加密，生成第2加密碼者；及

傳送機構，係將前述第2加密碼向前述認證要求裝置

傳送者；且

前述認證要求裝置使用前述密碼鍵將前述所傳送之第2加密碼解碼後，復原前述轉換認證用碼，並藉由將其與前述比較對象碼相比較，認證前述認證對象裝置。

2. 一種認證對象裝置，其特徵在於其係保持至少一個與認證要求裝置共用之密碼鍵，並成為藉由該認證要求裝置之認證對象者；且包含：

第1加密碼接收機構，係從前述認證要求裝置接收使用前述密碼鍵將認證用碼予以加密所得到之第1加密碼者；

轉換對象部分接收機構，係從前述認證要求裝置接收特定前述認證用碼中之至少一對相互不同之部分作為轉換對象部分之轉換對象部分特定資訊者；

認證用碼解碼機構，係用前述密碼鍵將前述接收之第1加密碼解碼後，復原前述認證用碼者；

轉換機構，係根據前述接收之轉換對象部分特定資訊，將前述復原之認證用碼之前述轉換對象部分予以轉換，生成轉換認證用碼者；

第2加密碼生成機構，係用前述密碼鍵將前述轉換認證用碼予以加密，生成第2加密碼者；及

第2加密碼傳送機構，係將前述第2加密碼向前述認證要求裝置傳送者；且

前述第2加密碼供給於藉由前述認證要求裝置之認證處理。

3. 一種認證對象裝置，其特徵在於其係保持至少一個與認證要求裝置共用之密碼鍵，並成為藉由該認證要求裝置之認證對象者；且包含：

轉換對象部分接收機構，係從前述認證要求裝置接收特定前述密碼鍵中之至少一對相互不同之部分作為轉換對象部分之轉換對象部分特定資訊者；

第1加密碼接收機構，係從前述認證要求裝置接收第1加密碼，該第1加密碼係使用轉換前述密碼鍵之前述轉換對象部分之轉換密碼鍵，將認證用碼加密所得到者；

轉換機構，係根據前述接收之轉換對象部分特定資訊，將前述密碼鍵之前述轉換對象部分予以轉換，生成轉換密碼鍵者；

認證用碼解碼機構，係使用前述轉換密碼鍵將前述接收之第1加密碼予以解碼後，復原前述認證用碼者；

第2加密碼生成機構，係將前述復原之認證用碼予以加密，生成第2加密碼者；及

第2加密碼傳送機構，係將前述第2加密碼向前述認證要求裝置傳送者；且

前述第2加密碼供給於根據前述認證要求裝置之認證處理。

十一、圖式：

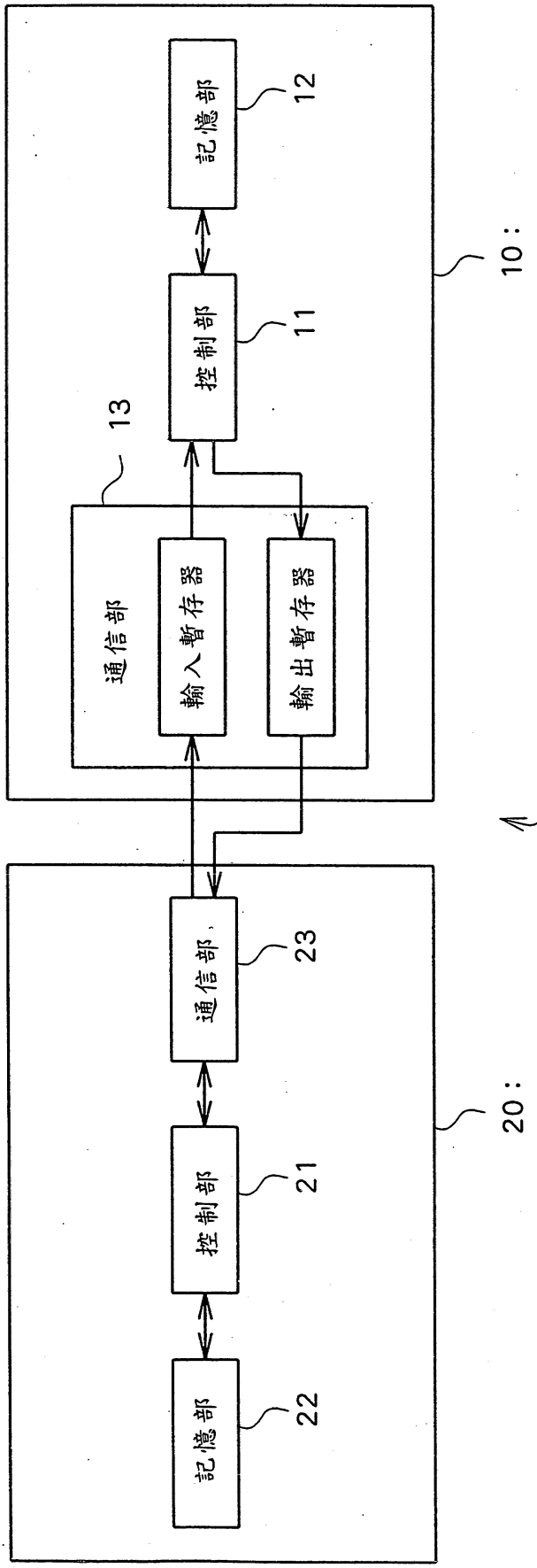

圖 1

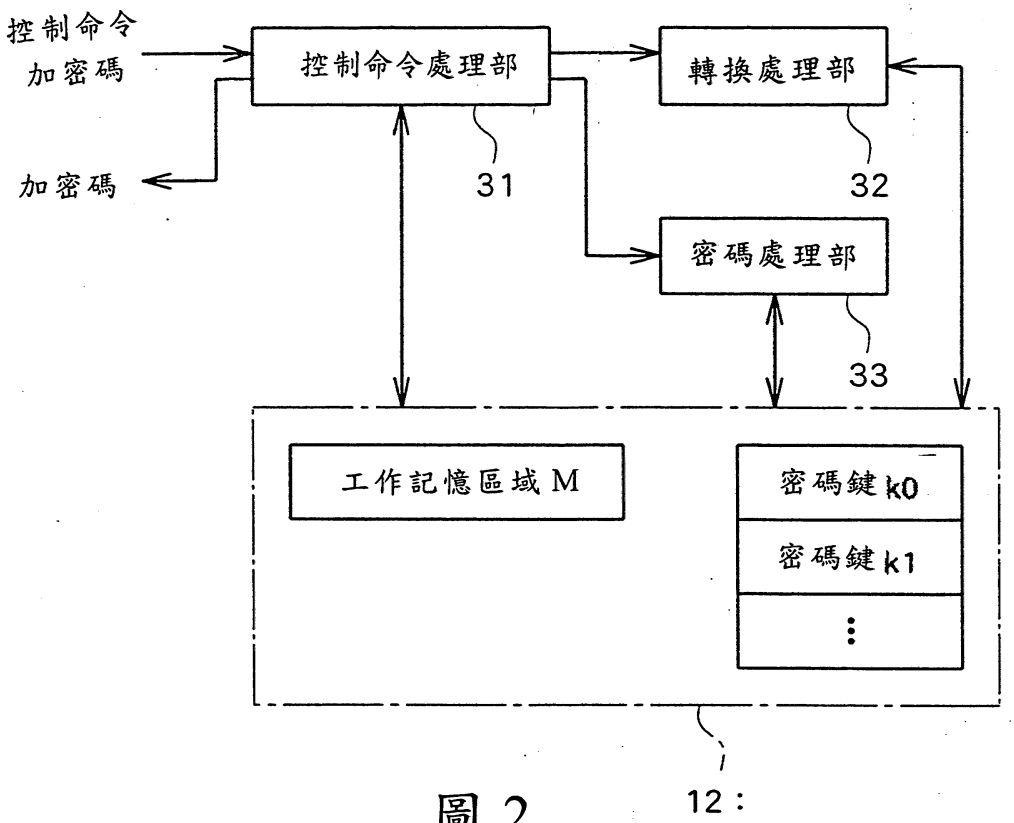
控制命令
加密碼
加密碼
控制命令處理部
轉換處理部
31
32
密碼處理部
33
工作記憶區域 M
密碼鍵 k0
密碼鍵 k1
12：

圖 2

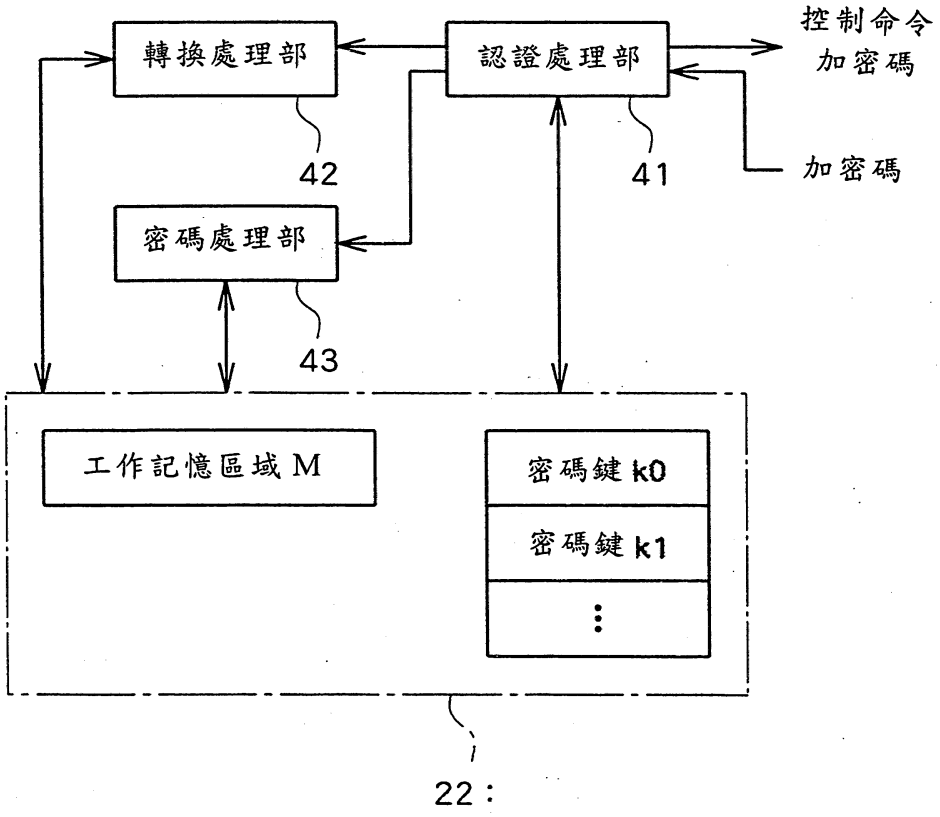
轉換處理部
認證處理部
控制命令
加密碼
42
41
加密碼
密碼處理部
43
工作記憶區域 M
密碼鍵 k0
密碼鍵 k1
22：

圖 3

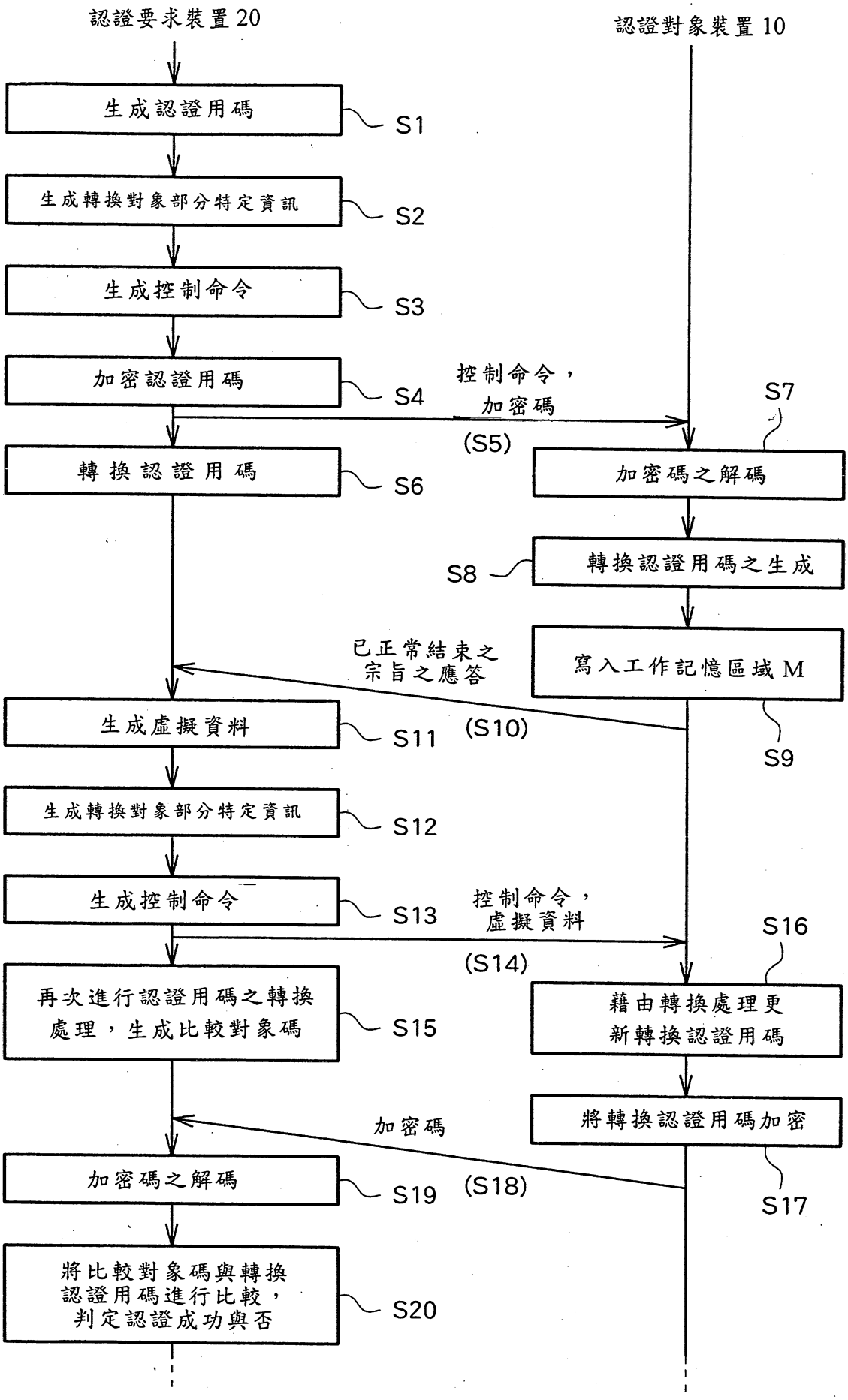
認證要求裝置 20
認證對象裝置 10
生成認證用碼
S1
生成轉換對象部分特定資訊
S2
生成控制命令
S3
加密認證用碼
S4
控制命令，
加密碼
(S5)
S7
轉換認證用碼
S6
加密碼之解碼
S8
轉換認證用碼之生成
寫入工作記憶區域 M
已正常結束之
宗旨之應答
(S10)
S9
生成虛擬資料
S11
生成轉換對象部分特定資訊
S12
生成控制命令
S13
控制命令，
虛擬資料
(S14)
S16
再次進行認證用碼之轉換
處理，生成比較對象碼
S15
藉由轉換處理更
新轉換認證用碼
將轉換認證用碼加密
加密碼
(S18)
S17
加密碼之解碼
S19
將比較對象碼與轉換
認證用碼進行比較，
判定認證成功與否
S20

圖 4

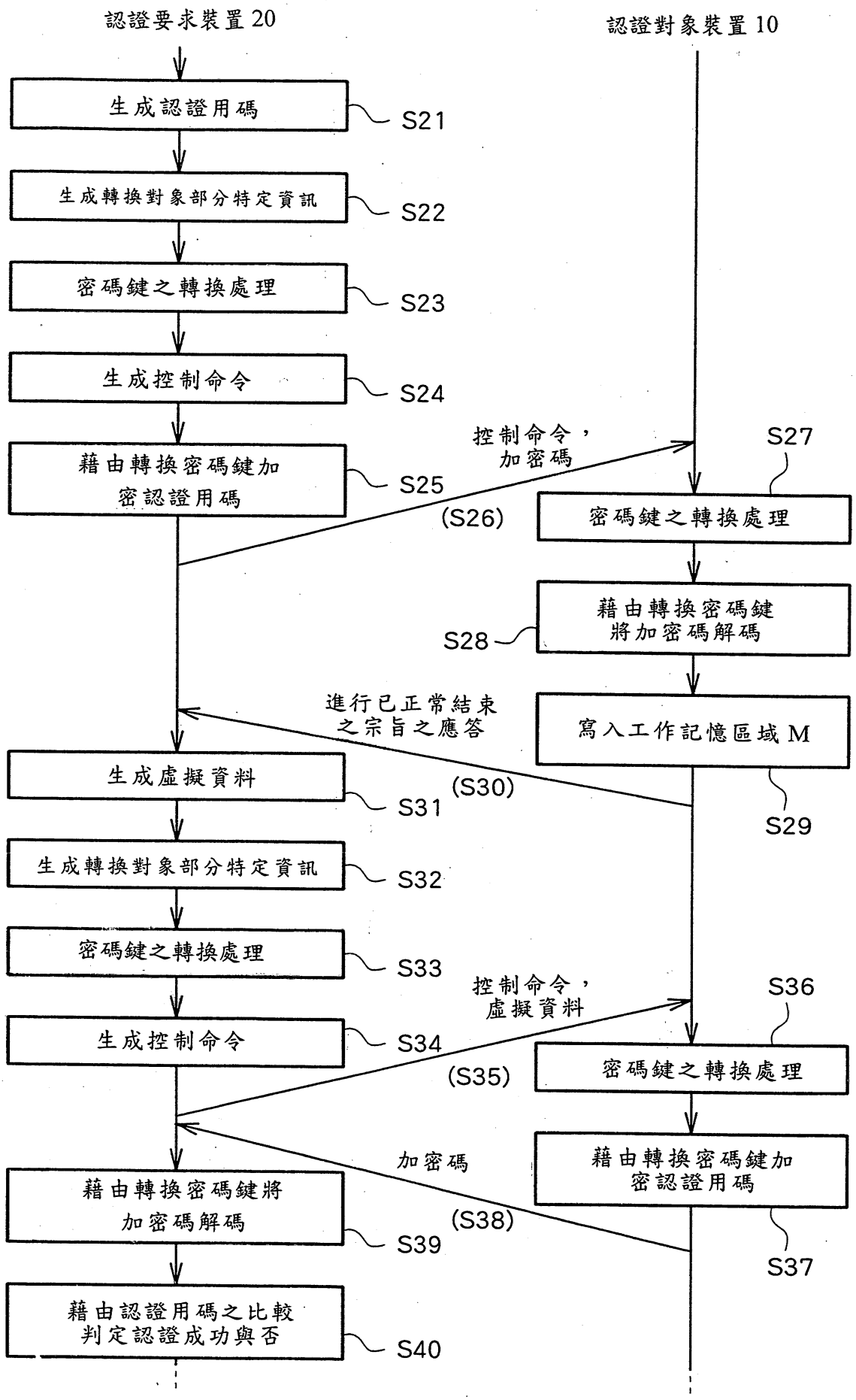
認證要求裝置 20
認證對象裝置 10
生成認證用碼
S21
生成轉換對象部分特定資訊
S22
密碼鍵之轉換處理
S23
生成控制命令
S24
藉由轉換密碼鍵加密認證用碼
S25
控制命令，加密碼
(S26)
S27
密碼鍵之轉換處理
藉由轉換密碼鍵將加密碼解碼
S28
寫入工作記憶區域 M
S29
進行已正常結束之宗旨之應答
(S30)
生成虛擬資料
S31
生成轉換對象部分特定資訊
S32
密碼鍵之轉換處理
S33
生成控制命令
S34
控制命令，虛擬資料
(S35)
S36
密碼鍵之轉換處理
藉由轉換密碼鍵加密認證用碼
S37
加密碼
(S38)
藉由轉換密碼鍵將加密碼解碼
S39
藉由認證用碼之比較判定認證成功與否
S40

圖 5

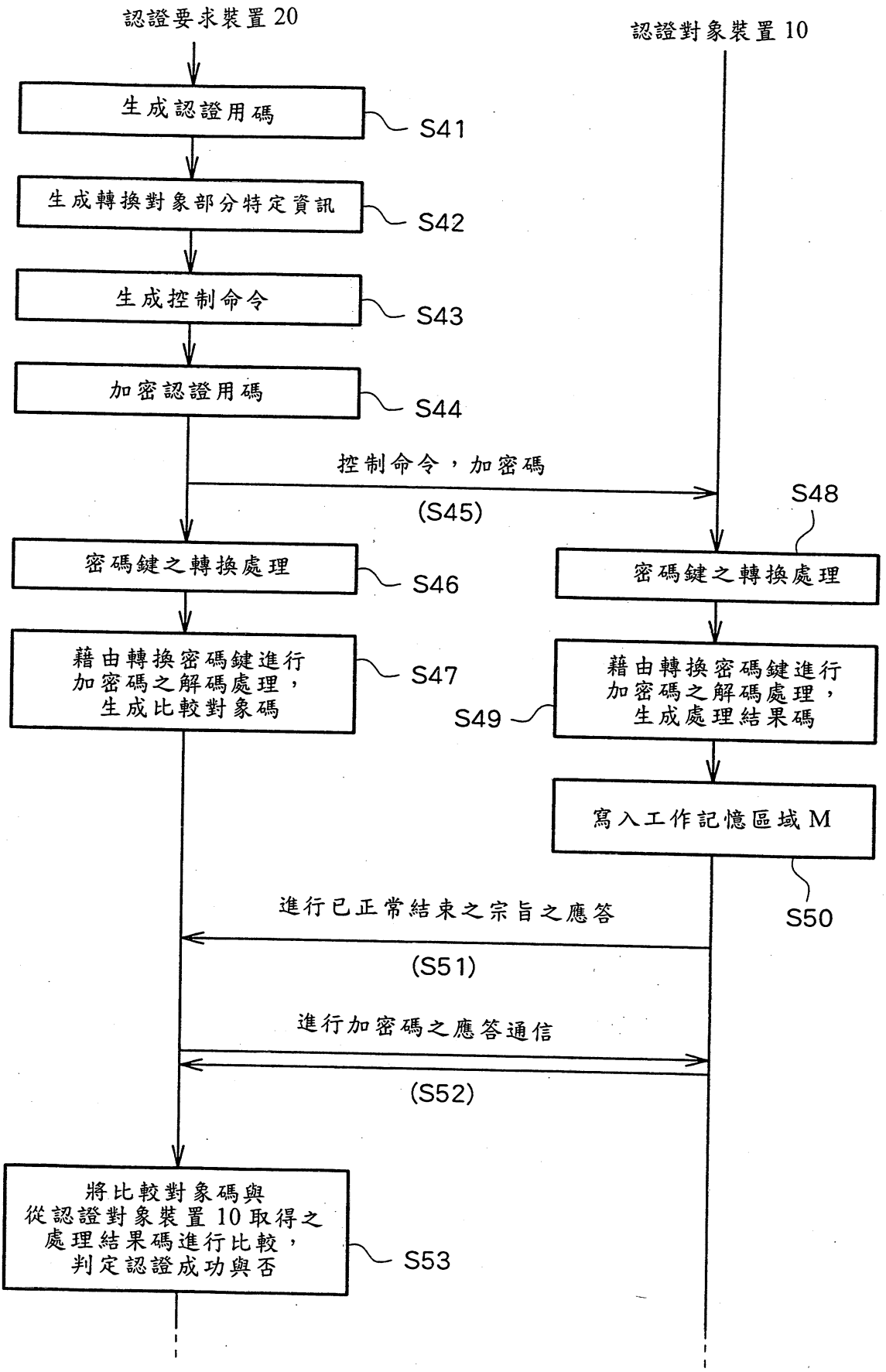
認證要求裝置 20
認證對象裝置 10
生成認證用碼
S41
生成轉換對象部分特定資訊
S42
生成控制命令
S43
加密認證用碼
S44
控制命令，加密碼
(S45)
S48
密碼鍵之轉換處理
S46
密碼鍵之轉換處理
藉由轉換密碼鍵進行
加密碼之解碼處理，
生成比較對象碼
S47
藉由轉換密碼鍵進行
加密碼之解碼處理，
生成處理結果碼
S49
寫入工作記憶區域 M
S50
進行已正常結束之宗旨之應答
(S51)
進行加密碼之應答通信
(S52)
將比較對象碼與
從認證對象裝置 10 取得之
處理結果碼進行比較，
判定認證成功與否
S53

圖 6

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：

1	認證系統
10	認證對象裝置
11	控制部
12	記憶部
13	通信部
20	認證要求裝置
21	控制部
22	記憶部
23	通信部

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

(無)