I308306

公告本

97年11月5日修正/~~更正~~/補充

申請日期	91、6、26
案號	91114091
類別	G09C 1/00

A4
C4

（以上各欄由本局填註）

發明 專利說明書

一、發明名稱	中文	數位著作物保護系統、記錄／播放裝置、記錄媒體裝置、及模型變更裝置
	英文	DIGITAL WORK PROTECTION SYSTEM, RECORD/PLAYBACK DEVICE, RECORDING MEDIUM DEVICE, AND MODEL CHANGE DEVICE
二、發明人	姓名	1. 原田俊治 Shunji HARADA 2. 宮崎雅也 Masaya MIYAZAKI 3. 松居真一 Shinichi MATSUI 4. 井上信治 Shinji INOUE 5. 松崎棗彦 Natsume MATSUZAKI 6. 野口直彦 Naohiko NOGUCHI
	國籍	日本 Japan
	住、居所	1. 日本國大阪府大阪市西成區玉出西2-20-52 2-20-52, Tamadenishi, Nishinari-ku, Osaka-shi, Osaka-fu 557-0045 Japan 2. 日本國大阪府池田市旭丘1-6-14 1-6-14, Asahigaoka, Ikeda-shi, Osaka-fu 563-0022 Japan 3. 日本國兵庫縣神戶市東灘區西岡本1-5-16-302 1-5-16-302, Nishiokamoto, Higashinada-ku, Kobe-shi, Hyogo-ken 658-0073 Japan 4. 日本國大阪府寢屋川市東香里園町9-13-306 9-13-306, Higashikourien-cho, Neyagawa-shi, Osaka-fu 572-0081 Japan 5. 日本國大阪府箕面市粟生間谷西1-6-7-803 1-6-7-803, Aomadaninishi, Minou-shi, Osaka-fu 562-0023 Japan 6. 日本國神奈川縣橫濱市港北區太尾町1323-601 1323-601, Futoo-cho, Kouhoku-ku, Yokohama-shi, Kanagawa-ken 222-0031 Japan
三、申請人	姓名（名稱）	日商・松下電器產業股份有限公司 Matsushita Electric Industrial co., Ltd.
	國籍	日本 Japan
	住、居所（事務所）	日本國大阪府門真市大字門真1006番地 1006, Oazakadoma, Kadoma-shi, Osaka-fu, 571-8501 Japan
	代表人姓名	中村邦夫 Kunio NAKAMURA

裝 訂 線

本紙張尺度適用中國國家標準（CNS）A4規格（210×297公釐）

[S]

（由本局填寫）

承辦人代碼：	
大　　類：	
ＩＰＣ分類：	

A6
B6

本案已向：

日本　國（地區）　申請專利，申請日期：2001,7,.9　案號：特願2001-208532，☑有　☐無主張優先權

有關微生物已寄存於：　　，寄存日期：　　，寄存號碼：

（請先閱讀背面之注意事項再填寫本頁各欄）

裝　訂　線

五、發明說明（1）

【發明所屬之技術領域】

本申請案係根據在日本建檔之第 2001-208532 號專利申請案，其內容因而被納為參考。

本發明係有關於在網路上分配、接收、記錄及播放數位著作物之技術。

【先前技術】

感謝近來的技術進步，如數位化文件、音樂、影像與節目已在網際網路之典型網路被配銷，其讓使用者容易地經由一網路擷取各種數位著作物，並在分離的記錄媒體記錄被擷取之數位著作物以便播放。

然而，使用者被允許方便地複製數位著作物之上面的利益不可避免地附帶了數位著作物之版權會容易地被侵害的問題。

【發明內容】

針對此問題，本發明之一目標為要提供一數位著作物保護系統、一記錄/播放裝置、一記錄媒體裝置、一模型變更裝置、一記錄/播放方法、一記錄/播放程式及一記錄媒體儲存一記錄/播放程式，其每一個記錄儲存於記錄/播放裝置之內部記憶體中之數位著作物至可攜式記錄媒體裝置內，其方式為禁止以在記錄時被運用之記錄/播放裝置外的任何裝置播放該已記錄的數位著作物。

為達成上面的目標，在本發明之一層面中，一種用於記錄及播放數位著作物之數位著作物保護系統，包含：一可攜式的記錄媒體裝置，包括一儲存區且被附裝於一記錄/

五、發明說明（2）

播放裝置及該記錄/播放裝置。該記錄/播放裝置包括：一內部儲存單元可操作以儲存是為數位著作物之內容；一獨一資訊儲存單元可操作以預先儲存對該記錄/播放裝置為獨一的之裝置獨一資訊；一加密單元可操作以根據該預先儲存的裝置獨一資訊將儲存的內容加密以產生已加密之資訊；一寫入單元可操作以寫入所產生已加密之資訊至該記錄媒體裝置之儲存區內；一讀取單元可操作以自該記錄媒體裝置之儲存區讀取該已加密之資訊；一解密單元可操作以根據被儲存於該獨一資訊儲存單元之該預先儲存的裝置獨一資訊將所讀取的已加密之資訊解密以產生已解密之內容；以及一播放單元可操作以播放所產生的已解密之內容。

以此構造下，該記錄/播放裝置根據對該記錄/播放裝置為獨一的之裝置獨一資訊將該內容加密以產生該已加密之資訊，及將所產生的已加密之資訊記錄至該記錄媒體裝置上。為了播放該內容，該記錄/播放裝置根據儲存於記錄/播放裝置之該裝置獨一資訊將該已加密之資訊解密。因而，其有的效果為被儲存於該記錄媒體裝置的已加密之資訊不能用具有被儲存其中之獨一資訊的記錄/播放裝置之任何其他裝置加以解密或播放。

此處，較佳的是該加密單元使用該裝置獨一資訊為鑰匙將該內容加密以產生該已加密之資訊，及該解密單元使用該裝置獨一資訊為鑰匙將所讀取的已加密之資訊解密。

以此構造下，該內容使用該裝置獨一資訊為鑰匙被加密以產生該已加密之資訊，及所讀取的已加密之資訊使用

五、發明說明（3）

該裝置獨一資訊為鑰匙被解密。因而，被儲存於該記錄媒體裝置的已加密之資訊不能用不具有該裝置獨一資訊的任何裝置加以解密或播放。

此處較佳的是，該記錄/播放裝置進一步包括一狀況儲存單元可操作以儲存使用狀況資訊顯示使用該內容之許可狀況；以及一狀況判斷單元可操作以依據該使用狀況資訊來判斷使用該內容是否被許可的。

以此構造下，該記錄/播放裝置預先儲存該使用狀況資訊顯示使用該內容的許可狀況，依據該使用狀況資訊判斷使用該內容是否被許可的。該已解密之內容僅在該內容被判斷為許可的時被播放。因而，該內容被保護不會在該使用狀況資訊所顯示之狀況不符合時被使用。

此處較佳的是，該獨一資訊儲存單元與該狀況儲存單元二者均針對任何外部裝置為讀取保護及寫入保護的，除非該裝置明確地被許可以讀取或寫入該獨一資訊與該使用狀況資訊。

以此構造下，該獨一資訊儲存單元與該狀況儲存單元均針對任何外部裝置為讀取保護及寫入保護的。因而，該獨一資訊與該使用狀況資訊被保護免於外洩。

此處較佳的是，該加密單元產生對該內容為唯一的標題鑰匙，使用該裝置獨一資訊為鑰匙以將所產生之標題鑰匙加密，使用所產生之標題鑰匙為鑰匙將該內容加密以產生已加密之內容，以及產生由該已加密之標題鑰匙與該已加密之內容組成的已加密之資訊，該寫入單元寫入由該已

五、發明說明（4）

加密之標題鑰匙與該已加密之內容組成的已加密之資訊，該讀取單元讀取由該已加密之標題鑰匙與該已加密之內容組成的已加密之資訊，該解密單元使用該裝置獨一資訊為鑰匙將包括於所讀取的已加密之資訊解密以產生已解密之標題鑰匙，及使用已解密之標題鑰匙為鑰匙將包括於所讀取的已加密之資訊解密以產生該已解密之內容，以及該記錄媒體裝置包括儲存區用於儲存由該已加密之標題鑰匙與該已加密之內容組成的該已加密之資訊。

以此構造下，該記錄/播放裝置使用該裝置獨一資訊為鑰匙將所產生的標題鑰匙加密以產生已加密之標題鑰匙，並使用所產生的標題鑰匙為鑰匙將該內容加密以產生該已加密之內容。同時，該記錄/播放裝置使用該裝置獨一資訊為鑰匙將已加密之標題鑰匙解密以產生該已解密之標題鑰匙，並使用所產生的已解密之標題鑰匙為鑰匙以產生該已解密之內容。因而，儲存於記錄媒體裝置的該已加密之標題鑰匙不會被具有該裝置獨一資訊被儲存於具中之記錄/播放裝置外的任何其他裝置加以解密。結果為，該已加密之內容僅被該記錄/播放裝置解密。

此處較佳的是，該記錄/播放裝置進一步包括一第一認證單元可操作以在該寫入單元寫入該已加密之資訊至該儲存區內前或該讀取單元由該儲存區讀取該已加密之資訊前與包括於該記錄媒體裝置內之一第二認證單元實施相互認證，該記錄媒體裝置進一步包括該第二認證單元可操作以與包括於該記錄/播放裝置內之該第一認證單元實施相互

五、發明說明（5）

認證，及該儲存區包括一第一儲存區與一第二儲存區，該第二儲存區僅在該相互認證被該第一認證單元建立、該寫入單元寫入該已加密之內容至該第一儲存區，及僅在該相互認證被該第一認證單元建立、寫入該已加密之標題鑰匙至該第二儲存區內、且該讀取單元自該第一儲存區讀取該已加密之內容，及僅在該相互認證被該第一認證單元建立、自該第二儲存區讀取該已加密之標題鑰匙時為可寫入及可讀取的。

以此構造下，該記錄/播放裝置與該記錄媒體裝置彼此相互認證。僅在該相互認證被建立時，該記錄/播放裝置寫入該已加密之標題鑰匙至該記錄媒體裝置內，或自該記錄媒體裝置讀取該已加密之標題鑰匙。因此，其被防止該內容被任何不法的裝置讀取或寫入。

此處較佳的是，該記錄/播放裝置進一步包括：一狀況儲存單元可操作以儲存使用狀況資訊顯示使用該內容的許可狀況；以及一狀況判斷單元可操作以依據該使用狀況資訊判斷該內容之使用是否為被許可的。

以此構造下，該使用狀況被儲存於該記錄媒體裝置內，且有關使用該內容是否被許可的判斷係依據該使用狀況被做成。

此處較佳的是，該寫入單元自該狀況儲存單元讀取該使用狀況並僅在該相互認證被該第一認證單元建立時寫入所讀取之使用狀況資訊至該第二儲存區內，該讀取單元自該第二儲存區讀取該使用狀況並僅在該相互認證被該第一

五、發明說明（6）

認證單元建立時寫入所讀取之使用狀況至該使用狀況儲存單元內，及該狀況判斷單元依據儲存於該狀況儲存單元內之使用狀況資訊來判斷使用內容是否為被許可的。

以此構造下，該記錄/播放裝置與該記錄媒體裝置彼此相互認證。僅在該相互認證被建立時，該記錄/播放裝置寫入該使用狀況至該記錄媒體裝置內，或自該記錄媒體裝置讀取該使用狀況。進一步而言，該記錄/播放裝置依據所讀取之使用狀況資訊判斷使用內容是否被許可的。

此處較佳的是，儲存於該狀況儲存單元之使用狀況資訊顯示被許可的播放次數、被許可的播放期間、被許可的總播放時間、被許可的複製內容次數或被許可的移動內容次數，且該狀況判斷單元(1)僅在播放單元的實際播放次數小於或等於被許可的播放次數、內容將被播放單元播放的日期與時間在被許可的播放期間內、且總播放時間小於或等於被許可的總播放時間時判斷為要播放該內容，(2)僅在被許可的複製內容次數大於或等於 1 時判斷為要複製該內容至該記錄媒體裝置，以及(3)僅在被許可的移動內容次數大於或等於 1 時判斷要移動該內容至該記錄媒體裝置。

以此構造下，該使用狀況顯示被許可的播放次數、被許可的播放期間、或被許可的總播放時間、被許可的播放複製次數、或被許可的移動播放次數。因而，內容之使用被各種方式限制。

此處較佳的是，該記錄/播放裝置進一步包括一認證判斷單元可操作以判斷該記錄媒體裝置是否包括該第二認證

五、發明說明（7）

單元，且該加密單元進一步使用該裝置獨一資訊為鑰匙以在該記錄媒體裝置被判斷未包括該第二認證單元時產生該已加密之資訊，該寫入單元進一步在該記錄媒體裝置被判斷未包括該第二認證單元時寫入所產生的已加密之資訊至該記錄媒體裝置的儲存區內，該讀取單元進一步在該記錄媒體裝置被判斷未包括該第二認證單元時自該記錄媒體裝置的儲存區讀取該已加密之資訊，及該解密單元進一步使用該裝置獨一資訊為鑰匙以在該記錄媒體裝置被判斷未包括該第二認證單元時將所讀取的已加密之資訊解密。

以此構造下，該加密視該記錄媒體裝置是否包括一認證單元以不同的方式被完成，此使得該數位著作物保護系統以各種方式被使用為可能的。

此處較佳的是，該記錄媒體裝置進一步預先儲存對該記錄媒體裝置為獨一的之媒體獨一資訊，該內部儲存單元儲存與該內容相關的一獨一資訊型式，與獨一資訊型式根據該裝置獨一資訊或該媒體獨一資訊顯示將被加密之內容，該記錄/播放裝置進一步包括一獨一資訊判斷單元依據儲存於該內部儲存單元中之該獨一資訊型式判斷該內容是否根據該裝置獨一資訊或該媒體獨一資訊將被加密，該加密單元(1)在該獨一資訊判斷單元根據該裝置獨一資訊判斷將被加密之內容時根據該裝置獨一資訊將該內容加密以產生該已加密之資訊，及(2)在該獨一資訊判斷單元根據該媒體獨一資訊判斷之內容時根據該所讀取之媒體獨一資訊自該記錄媒體裝置讀取該媒體獨一資訊將該內容加密以產

五、發明說明（8）

生該已加密之資訊，該解密單元(1)在該獨一資訊判斷單元根據該裝置獨一資訊判斷將被加密之內容時根據該裝置獨一資訊將所讀取的已加密之資訊解密以產生該已解密之內容，及(2)在該獨一資訊判斷單元根據該裝置獨一資訊判斷將被加密之內容時使用所讀取的媒體獨一資訊自該記錄媒體裝置讀取該媒體獨一資訊將所讀取的已加密之資訊解密以產生該已解密之內容。

以此構造下，不同的獨一資訊視該獨一資訊而定在加密中被使用，此使得數位著作物保護系統以各種方式被使用為可能的。

或者，在本發明之另一層面中，所提供者為一模型變更裝置，用於因使用者與服務供應商間之合約變更而以一第二記錄/播放裝置取代第一記錄/播放裝置，雖然該第一記錄/播放裝置在合約下是可用的。該第一記錄/播放裝置包括：一第一內部儲存單元可操作以儲存數位著作物之內容；一第一獨一資訊儲存單元可操作以預先儲存對該第一記錄/播放裝置為獨一的之裝置獨一資訊；一第一加密單元可操作以根據儲存於該第一獨一資訊儲存單元之裝置獨一資訊將儲存於該第一內部儲存單元內之內容加密以產生已加密之資訊；一第一寫入單元可操作以寫入所產生的已加密之資訊至一記錄媒體裝置內的儲存區，一第一讀取單元可操作以自該記錄媒體裝置之儲存區讀取該已加密之資訊；一第一解密單元可操作以根據儲存於該第一獨一資訊儲存單元之該裝置獨一資訊以將所讀取的已加密之資訊解

五、發明說明（9）

密以產生已解密之內容；以及一第一播放單元可操作以播放所產生的已解密內容。該記錄媒體裝置包括儲存區用於儲存該已加密之資訊。該第二記錄/播放裝置包括：一第二內部儲存單元包括一內部儲存區用於儲存數位著作物之內容；一第二獨一資訊儲存單元包括一內部儲存區用於儲存裝置獨一資訊；一第二加密單元可操作以根據儲存於該第二獨一資訊儲存單元內之裝置獨一資訊將儲存於第二內部儲存單元內之內容加密；一第二寫入單元可操作以寫入所產生的已加密之資訊至記憶體裝置之儲存區內；一第二讀取單元可操作以自該記憶體之儲存區讀取該已加密之資訊；一第二解密單元可操作以根據儲存於第二獨一資訊儲存單元內之裝置獨一資訊將所讀取的已加密之資訊解密以產生已解密之內容；以及一第二播放單元可操作以播放所產生的已解密之內容。該模型變更裝置包括：一第三讀取單元可操作以讀取儲存於該第一獨一資訊儲存單元內之裝置獨一資訊，並自該第一獨一資訊儲存單元刪除該裝置獨一資訊；以及一第二寫入單元可操作以寫入該裝置獨一資訊至該獨一資訊儲存單元內。

以此構造下，該模型變更裝置讀取儲存於該第一記錄/播放裝置之第一獨一資訊儲存單元內的裝置獨一資訊，自該第一獨一資訊儲存單元刪除該裝置獨一資訊，及寫入所讀取之裝置獨一資訊至該第二記錄/播放裝置內之第二內部儲存單元內。因而，就算在模型變更後，被該第一記錄/播放裝置儲存於該記錄媒體裝置內之內容允許被該第二記

五、發明說明（10）

錄/播放裝置使用。此外在模型變更後，該第一記錄/播放裝置不再被允許使用該內容。

或者，在本發明之另一層面中，所提供者為一模型變更裝置用於取消在一使用者與一服務供應商之合約下曾為可用的一記錄/播放裝置。該記錄/播放裝置包括：一內部儲存單元可操作以儲存數位著作物之內容；一獨一資訊儲存單元可操作以預先儲存：(1)對該記錄/播放裝置為獨一的之裝置獨一資訊與(2)有關該合約之合約資訊，該裝置獨一資訊與該合約資訊為獨立無關的；一加密單元可操作以根據儲存於該獨一資訊儲存單元內之裝置獨一資訊將儲存於該內部儲存單元內之內容加密以產生已加密之資訊；一寫入單元可操作以寫入所產生的已加密之資訊至一記錄媒體裝置之一儲存區內；一讀取單元可操作以自該記錄媒體裝置之儲存區讀取該已加密之資訊；一解密單元可操作以根據儲存於該獨一資訊儲存單元內之裝置獨一資訊將所讀取的已加密之資訊解密；以及一播放單元可操作以播放所產生的已解密之內容。該記錄媒體裝置包括該儲存區用於儲存該已加密之資訊。該模型變更裝置包括：一讀取單元可操作以自該獨一資訊儲存單元讀取該合約資訊；以及一取消單元可操作以參照所讀取的合約資訊實施處理來取消該合約。

以此構造下，該記錄/播放裝置預先儲存與該合約資訊獨立無關的裝置獨一資訊。該模型變更裝置讀取儲存於該獨一資訊儲存單元內之合約資訊以參照所讀取的合約資訊

五、發明說明（11）

實施處理來取消該合約。因此就算取消該記錄/播放裝置在其下為可用的之合約後，被儲存於該記錄媒體裝置內之內容仍然允許被該記錄/播放裝置播放。

或者，在本發明之另一層面中，所提供者為一模型變更裝置被用以變更在其下一記錄/播放裝置為可用的之一第一合約為一第二合約。該第一合約在一使用者與一第一服務供應商間被完成及該第二合約在一使用者與一第二服務供應商間被完成。該記錄/播放裝置包括：一內部儲存單元可操作以儲存數位著作物之內容；一獨一資訊儲存單元可操作以儲存：(1)對該記錄/播放裝置為獨一之獨一資訊及(2)有關該第一合約之第一合約資訊，該裝置獨一資訊與該合約資訊為獨立無關的；一加密單元可操作以根據儲存於該獨一資訊儲存單元內之裝置獨一資訊將儲存於該內部儲存單元內之內容加密；一寫入單元可操作以寫入所產生的已加密之資訊至一記錄媒體裝置之一儲存區內；一讀取單元可操作以自該記錄媒體裝置之儲存區讀取該已加密之資訊；一解密單元可操作以根據儲存於該獨一資訊儲存單元內之裝置獨一資訊將所讀取的已加密之資訊解密以產生一已解密的內容；以及一播放單元可操作以播放所產生的已解密之內容。該記錄媒體裝置包括儲存區用於儲存該已加密之資訊。該模型變更裝置包括：一讀取單元可操作以自該獨一資訊儲存單元讀取該第一合約資訊；一合約取消及變更單元可操作以參照所讀取第一合約資訊實施處理來取消該第一合約及實施處理以使該第二合約產生有關該第二

五、發明說明（12）

合約之第二合約資訊；以及一寫入單元以寫入所產生的第二合約資訊至該獨一資訊儲存單元內，並自該獨一資訊儲存單元刪除該第一合約資訊。

以此構造下，該記錄/播放裝置預先儲存與該第一合約資訊獨立無關的之裝置獨一資訊。該模型變更裝置自該記錄/播放裝置讀取該第一合約資訊，參照該第一合約資訊實施處理以取消該第一合約，實施處理以使該第二合約產生有關該第二合約之第二合約資訊，寫入所產生的第二合約資訊至記錄/播放裝置之獨一資訊儲存單元內，及自該獨一資訊儲存單元刪除該第一合約資訊。因而，甚至在該記錄/播放裝置之服務供應商被變更為另一服務供應商後，被儲存於該記錄媒體裝置內之內容仍被播放。

本發明之這些與其他目標、優點與特點將由下列描述配合顯示本發明之特定實施例的附圖被讀取時成為明白的。

圖式簡要說明

在圖中：

第 1 圖為一方塊圖，顯示一數位著作物配銷系統 100 之整個構造；

第 2 圖為一方塊圖，顯示一內容配銷伺服器裝置 200 之構造；

第 3 圖為一方塊圖，顯示一行動電話 300 與一記憶體卡 400 之構造；

第 4 圖為一流程圖，顯示該數位著作物配銷系統 100

五、發明說明（13）

之作業；

第5圖為一方塊圖，顯示一記憶體卡400b之構造；

第6圖為一方塊圖，顯示一行動電話300b之構造；

第7圖為一流程圖，顯示被行動電話300b實施之作業以產生一已加密之內容及寫入該已加密之內容至該記憶體卡400b內；

第8圖為一流程圖，顯示被行動電話300b實施之作業以自該記憶體卡400b讀取該已加密之內容及產生該內容；

第9圖顯示被行動電話A及行動電話X實施以播放該內容之作業；

第10圖為一方塊圖，顯示一行動電話300c與該記憶體卡400之構造；

第11圖為一流程圖，顯示行動電話300c之作業；

第12圖為一流程圖，顯示當該使用狀況為被許可之播放期間時行動電話300c的作業；

第13圖為一流程圖，顯示當該使用狀況為被許可之播放時間總量時行動電話300c的作業；

第14圖為一方塊圖，顯示一記憶體卡400d之構造；

第15圖為一方塊圖，顯示一行動電話300d之構造；

第16圖為一方塊圖，顯示一加密/解密單元380d之構造；

第17圖為一流程圖，顯示一數位著作物配銷系統100d之整個作業；

第18圖為一流程圖，顯示行動電話300d與記憶體卡

五、發明說明（14）

400d 間被實施之相互認證的作業；

第 19 圖為一流程圖，顯示被行動電話 300d 為儲存處理實施之作業；

第 20 圖為一流程圖，顯示被行動電話 300d 為讀取處理實施之作業；

第 21 圖為一方塊圖，顯示一模型變更系統 600e 之構造；

第 22 圖為一流程圖，顯示該模型變更系統 600e 之作業；

第 23 圖為一方塊圖，顯示一模型變更系統 600g 之構造；

第 24 圖為一方塊圖，顯示一模型變更系統 600m 之構造；

第 25 圖為一流程圖，顯示該模型變更系統 600m 之作業；

第 26 圖為一流程圖，顯示被修改的模型變更系統 600m 之作業；

第 27 圖為一方塊圖，顯示一行動電話 300i 與一記憶體卡 400i 之構造；

第 28 圖為一流程圖，顯示一數位著作物配銷系統 100i 之作業；

第 29 圖顯示被儲存於一內容配銷伺服器裝置 200j 之內容儲存單元 201 內的權利資訊表 610 之資料構造；

第 30 圖為一方塊圖，顯示一記憶體卡 400j 之構造；

五、發明說明（15）

第31圖為一流程圖，顯示被實施以自該內容配銷伺服器裝置200j獲取一內容之作業；

第32圖為一流程圖，顯示當一使用者錯將儲存於記憶體卡 400j 的已加密之內容刪除時用於再獲取該曾已獲取之內容的作業；

第33圖顯示被儲存於一內容配銷伺服器裝置200k之內容儲存單元201內的一內容資訊表620的資料構造；

第34圖為一方塊圖，顯示一行動電話300k與一記憶體卡400k之構造；

第35圖為一流程圖，顯示被行動電話300k實施以獲取一內容及寫入所獲取的內容至記憶體卡 400k 內之作業；以及

第36圖為一流程圖，顯示被行動電話300k實施以將儲存於記憶體卡400k內的一已加密之內容解密及播放該已解密之內容的作業。

【實施方式】

首先描述符合本發明第一實施例之一數位著作物配銷系統100。

該數位著作物配銷系統100目標為一數位著作物保護系統、一主要裝置及一記錄媒體裝置，其每一個使用如行動電話之一主要裝置記錄一數位著作物(如鈴聲弦律或待機畫面)至一可攜式記錄媒體裝置內，其方式為禁止用在記錄之際被使用的該主要裝置外的任何其他裝置播放該數位著作物。

五、發明說明（16）

如第 1 圖之方塊圖顯示者，數位著作物配銷系統 100 由一內容配銷伺服器裝置 200、網際網路 10、一閘道裝置 40、一行動電話網路 20、一無線電基地台 30、一行動電話 300 與一記憶體卡 400 組成。

內容配銷伺服器裝置 200 經由網際網路 10 與行動電話網路 20 被連接至無線電基地台 30。無線電基地台 30 經由無線電波與行動電話 300 來回傳輸資訊。閘道裝置連接網際網路 10 與行動電話網路 20，並實施網際網路 10 與行動電話網路 20 間之通訊協定變換。

在回應於由行動電話 300 接收之使用者作業下，內容配銷伺服器裝置 200 分配一數位著作物(即例如為一件音樂作品)至行動電話 300，所經由者為網際網路 10、行動電話網路 20 與無線電基地台 30。然後行動電話 300 接收該內容、將所接收的內容加密、及將所加密的內容記錄至記憶體卡 400 內。進而言之，行動電話 300 在回應於使用者作業下讀取儲存於記憶體卡 400 內的已加密之內容、將該內容解密、及然後播放該已解密之內容。

如第 2 圖之方塊圖顯示者，內容配銷伺服器裝置 200 由一內容儲存單元 201、一控制單元 202、及一傳輸/接收單元 203 組成。

更明確地說，內容配銷伺服器裝置 200 為由微處理器、ROM、RAM、硬碟單元、顯示器單元、鍵盤、滑鼠及其他單元組成之電腦系統。該 RAM 或硬碟儲存一電腦程式，且內容配銷伺服器裝置 200 用微處理器執行該電腦程

五、發明說明（17）

式而實施其功能。

內容儲存單元 201 預先儲存一內容 600，其例如為鈴聲弦律。此處使用之鈴聲弦律係指一件音樂作品，其被播放以對行動電話使用者發信號表示有來電。注意，該內容例如可為行動電話之待機畫面、音樂伴唱資料、及用 Java 撰寫之遊戲程式。

控制單元 202 經由無線電基地台 30、行動電話網路 20、網際網路 10 與傳輸/接收單元 203 自行動電話 300 接收一內容 ID 與付款資訊。此處，該內容 ID 與付款資訊之傳輸透過使用如 SSL(Secure Socket Layer)通訊協定之安全的認證通訊協定以安全的方式被實施。該內容 ID 為一辨識元用於辨識該使用者所選擇要購買之內容，及該付款資訊為表示為購買該內容所完成之付款的資訊。在接收該內容 ID 與付款資訊之際，該控制單元 202 實施處理用於根據付款資訊接收付款。

接著，控制單元 202 自內容儲存單元 201 讀取對應於所接收的內容 ID 之內容，並經由傳輸/接收單元 203、網際網路 10、行動電話網路 20 與無線電基地台 30 傳輸所讀取的內容至行動電話 300。此處，該內容透過使用如 EMMS(Electronic Music Management System)之安全的內容配銷系統以安全方式自內容配銷伺服器裝置 200 被傳輸至行動電話 300。

傳輸/接收單元 203 用經由網際網路 10 被連接於此的外部裝置實施資訊的傳輸與接收。

五、發明說明（18）

如第3圖顯示者，記憶體卡400包括一外部儲存單元410，其具有儲存區用於儲存各種型式之資訊。

記憶體卡400被使用者附裝於行動電話300，使得各種型式之資訊用行動電話300寫入至該外部儲存單元410及由之被讀取。

如第3圖顯示者，行動電話300係由天線367、一傳輸/接收單元361、一音頻控制單元362、一擴音器363、一麥克風364、一輸入單元365、一控制單元366、一顯示器單元368、一內容購買單元301、一內容獲取單元302、一內部儲存單元303、一播放單元304、一獨一資訊儲存單元310、一寫入單元330、一讀取單元350及一加密/解密單元380組成。該加密/解密單元380係由一加密單元320與一解密單元340組成。

更明確地說，行動電話300係由一微處理器、ROM、RAM、一液晶顯示單元、一個十鍵與其他元件組成。該RAM儲存一電腦程式且行動電話300用該微處理器依照該電腦程式操作而部分地實施其功能。

該傳輸/接收單元361實施音頻控制單元362與另一流程圖間經由行動電話網路20、無線電基地台30與天線367之各種型式資訊的傳輸及接收。此外，該傳輸/接收單元361經由網際網路10、行動電話網路20、無線電基地台30與天線367實施內容配銷伺服器裝置200與內容購買單元301間或內容配銷伺服器裝置200與內容獲取單元302間各種型式資訊的傳輸及接收。

五、發明說明（19）

音頻控制單元362變換自另一行動電話被接收之音頻資訊成為電氣類比信號，並輸出結果的信號至擴音器363。此外，該音頻控制單元362變換麥克風364所接收之電氣類比信號成為音頻資訊，並輸出結果的音頻資訊至另一行動電話。

擴音器363實施電氣類比信號變換為音頻資料，隨後有音頻輸出，而麥克風364實施音頻輸入變換為電氣類比信號，隨後輸出該等結果的信號至音頻控制單元362。

輸入單元365被提供一個十鍵與其他鍵，並自該使用者接收各種輸入。

控制單元366控制構成行動電話300之每一單元的作業。

顯示器單元368由一液晶顯示單元組成，並顯示各種型式之資訊。

獨一資訊儲存單元310係由一半導體記憶體組成，其被保護不會被如模型變更裝置之特別被許可的裝置外之任何其他裝置由外部讀取或寫入，此將在稍後被描述。獨一資訊儲存單元310預先儲存獨一資訊。

此處，該獨一資訊係指對行動電話300為獨一的之資訊，其係由分配給行動電話之電話號碼、或分配給行動電話之隨機產生的號碼之類組成。

內部儲存單元303係由不可由外部讀取或寫入之半導體記憶體組成，且具有儲存區用於儲存自內容配銷伺服器裝置200接收之內容。

五、發明說明（20）

內容購買單元 301 自輸入單元 365 接收一內容 ID 辨識該使用者所選擇要購買之內容、產生表示為購買該內容所須完成之付款的付款資訊、及傳輸內容 ID 與該付款資訊一起至內容配銷伺服器裝置 200，所經由者為傳輸/接收單元 361、天線 367、無線電基地台 30、行動電話網路 20 與網際網路 10。

此處，行動電話 300 與內容配銷伺服器裝置 200 間內容 ID 與付款資訊間之傳輸係例如透過使用 SSL 通訊協定以安全的方式被實施。

內容獲取單元 302 經由網際網路 10、行動電話網路 20、無線電基地台 30、天線 367 與傳輸/接收單元 361 自內容配銷伺服器裝置 200 接收一內容，並寫入所接收的內容至內部儲存單元 303 內作為內容 601。

此處，自內容配銷伺服器裝置 200 至行動電話 300 之內容傳輸係例如透過使用 EMMS 系統以安全的方式被實施。

播放單元 304 在回應於經由輸入單元 365 被使用者輸入之播放指令下自內部儲存單元 303 讀取內容 601，並播放所讀取的內容至輸出。

此處，在所讀取的內容為一件音樂作品的情形中，播放單元 304 變換該內容成為電氣類比信號，並輸出結果的信號至擴音器 363。

或者，在所讀取的內容為行動電話用之待機畫面的情形中，播放單元 304 變換所讀取的內容成為像素資訊，並

五、發明說明（21）

輸出結果的像素資訊至顯示器單元 368。

如上述者，播放單元 304 視內容型式實施不同的處理。

加密單元 320 在回應於經由輸入單元 365 被使用者輸入的寫入指令下自內部儲存單元 303 讀取該內容 601 及自獨一資訊儲存單元 310 讀取該獨一資訊。

接著，加密單元 320 使用所讀取的獨一資訊作為鑰匙應用加密法則 E1 至所讀取的內容，並輸出已加密之內容至寫入單元 330。

此處作為一例的是，加密法則 E1 為以 DES(資料加密標準)為基礎之法則。

注意第 3 圖顯示之每一方塊以連接線與另一方塊被連接，但某些連接線在圖中被省略。此處，每一連接線顯示信號與資訊被傳輸所經由的路徑。進而言之，在直接與代表加密單元 302 之方塊連接的數條連接線中，以鑰匙符號標示之每一連接線代表作用為一鑰匙之資訊被傳輸所經由的路徑。相同的描述被應用至解密單元 340，也被應用至其他圖中相對應的方塊圖。

寫入單元 330 自加密單元 320 接收已加密之內容，並寫入該已加密之內容作為一已加密之內容 602 至外部儲存單元 410，此被包括於記憶體卡 400 內。

讀取單元 350 在回應於經由輸入單元 365 被使用者經由之讀取指令下讀取自記憶體卡 400 之外部儲存單元 410 讀取該已加密之內容 602，並輸出該已加密之內容至該解密單元 340。

五、發明說明（22）

該解密單元340自該讀取單元350傳輸該已加密之內容，並自獨一資訊儲存單元310讀取該獨一資訊。

接著，解密單元340以使用所讀取的獨一資訊為鑰匙應用解密法則 D1 至所接收的已加密之內容而產生該內容，並寫入所產生的內容至內部儲存單元303內。

此處，解密法則D1為用於實施加密法則E1之逆轉的法則。解密法則D1之一例為以DES為基礎之法則。

現在參照第4圖顯示之流程圖描述數位著作物配銷系統100之作業。

行動電話300之內容購買單元301在經由輸入單元365接收一內容ID之際產生付款資訊(步驟S101)，並透過使用例如SSL通訊協定以安全的方式傳輸該內容ID與該付款資訊至內容配銷伺服器裝置200(步驟S102)。

內容配銷伺服器裝置200之控制單元202自行動電話300接收該內容ID與該付款資訊(步驟S102)，然後實施處理用於根據所傳輸的付款資訊接收該付款(步驟S103)。此後，控制單元202自內容儲存單元201讀取用所接收的內容ID被辨識的內容(步驟S104)，然後透過使用例如SSL通訊協定以安全的方式傳輸所讀取的內容至行動電話300(步驟S105)。

行動電話300之內容獲取單元302自內容配銷伺服器裝置200接收內容(步驟S105)，並寫入所接收的內容至內部儲存單元303內作為內容601(步驟S106)。

加密單元320在經由輸入單元365接收一內容寫入指

五、發明說明（23）

令之際(步驟 S107)。自內部儲存單元 303 讀取該內容 601，與自獨一資訊儲存單元 310 讀取該獨一資訊(步驟 S109)。接著，加密單元 320 使用所讀取的獨一資訊作為鑰匙施用加密法則而產生已加密之內容(步驟 S110)，且寫入單元 330 寫入該已加密之內容至記憶體卡 400 之外部儲存單元 410 內作為內容 602(步驟 S111)。

或者，在經由輸入單元 365 接收一內容讀取指令之際(步驟 S107)，讀取單元 350 自記憶體卡 400 之外部儲存單元 410 讀取該已加密之內容 602(步驟 S112)，且解密單元 340 自獨一資訊儲存單元 310 讀取該獨一資訊(步驟 S113)。接著，解密單元 340 使用所讀取的獨一資訊作為鑰匙施用解密法則 D1 至所接收的已加密之內容而產生該內容(步驟 S114)，且寫入所產生的內容至內部儲存單元 303 內(步驟 S115)。

或者，在經由輸入單元 365 接收一播放指令之際 (步驟 S107)，播放單元 304 自內部儲存單元 303 讀取該內容 601(步驟 S116)，並播放所讀取的內容(步驟 S117)。

此後描述行動電話 300 之使用者所實施之作業程序。

首先，在使用行動電話 300 之內容購買單元 301 下，使用者自儲存於內容配銷伺服器裝置 200 之內容儲存單元 201 的內容中選擇及購買一內容。然後在使用內容獲取單元 302 下，使用者獲取其已購買之內容。然後該內容被儲存於行動電話 300 之內部儲存單元 303 內。

接著，在所購買的內容例如為鈴聲弦律的情形中，使

五、發明說明（24）

用者設定行動電話 300 使得在接收來電之際用播放單元 304 播放該鈴聲弦律。

進而言之，使用者可以下列程序儲存其先前購買且儲存於內部儲存單元 303 內之內容 601 至記憶體卡 400 內。

使用者附裝記憶體卡 400 至行動電話 300，並指示行動電話 300 儲存所購買的內容至記憶體卡內。

在回應下，儲存於行動電話 300 內部儲存單元 303 內的內容 601 被加密單元 320 使用儲存於獨一資訊儲存單元 310 中之獨一資訊加以加密，且後果的已加密之內容被產生。然後，該已加密之內容被寫入單元 330 作為已加密之內容 602 被儲存於包括在記憶體卡 400 內之外部儲存單元 410。

再進一步言之，使用者可自包括在記憶體卡 400 內之外部儲存單元 410 取還已加密之內容，並以下列的程序儲存所取還的內容至行動電話 300 的內部儲存單元 303 內。

使用者附裝記憶體卡 400 至行動電話 300，並指示行動電話 300 自記憶體卡 400 取還該已加密之內容。

在回應下，儲存於包括在記憶體卡 400 內之外部儲存單元 410 中的已加密之內容 602 被行動電話 300 的讀取單元 350 讀取。然後所讀取的已加密之內容被解密單元 340 使用儲存於獨一資訊儲存單元 310 中的獨一資訊加以解密，且後果的內容被產生。然後所產生的內容被儲存於行動電話 300 的內部儲存單元 303 內。

上面描述用於儲存已購買之內容至記憶體卡 400 及用

五、發明說明（25）

於自記憶體卡 400 取還所儲存的內容之程序。然而，該內容是否被購買，即獲取該內容是否須某些費用之付款，並非本發明的根本事項。此即上面的程序不僅可應用於使用者已購買的內容，但也可應用於如免費樣本之內容，其已免費地被分配給使用者。

此處分別描述行動電話 300 與記憶體卡 400 的修改行動電話 300b 與記憶體卡 400b。

行動電話 300b 與記憶體卡 400b 分別具有類似於行動電話 300 與記憶體卡 400 的構造。因而，下面僅描述與行動電話 300 及與記憶體卡 400 的差異。

如第 5 圖顯示者，記憶體卡 400b 包括一第一外部儲存單元 412 與一第二外部儲存單元 411。

第二外部儲存單元 411 具有一儲存區用於儲存稍後將被描述的已加密之標題鑰匙，而第一外部儲存單元 412 具有一儲存區用於儲存一已加密之內容。

如第 6 圖顯示者，行動電話 300b 包括加密/解密單元 380b 取代行動電話 300 所包括的加密/解密單元 380。行動電話 300b 僅針對此點與行動電話 300 不同。構成行動電話 300b 之元件與構成行動電話 300 之元件相同而以相同元件標號表示。

加密/解密單元 380b 包括一標題鑰匙產生單元 321、一加密單元 322、一加密單元 323、一解密單元 342、及一解密單元 343。

標題鑰匙產生單元 321 在每次儲存於內部儲存單元

五、發明說明（26）

303 之內容被加密時產生一隨機數字，並輸出所產生的隨機數字至加密單元 322 與 323 作為對每一內容為獨一的之標題鑰匙。

加密單元 322 自獨一資訊儲存單元 310 讀取該獨一資訊，並自標題鑰匙產生單元 321 接收該標題鑰匙。接著，加密單元 322 使用所讀取的獨一資訊作為一鑰匙對所接收的標題鑰匙施用加密法則 E2 而產生一已加密之內容，並輸出該已加密之內容至寫入單元 330。

此處，加密法則 E2 為例如以 DES 為基礎。

加密單元 323 自標題鑰匙產生單元 321 接收標題鑰匙，並自內部儲存單元 303 讀取內容 601。接著，加密單元 323 使用所接收的標題鑰匙作為鑰匙施用加密法則 E3 至所讀取的內容，而產生一已加密之內容，並輸出所產生的已加密之內容至寫入單元 330。

寫入單元 330 自加密單元 322 接收該已加密之標題鑰匙，並寫入所接收的已加密之標題鑰匙至記憶體卡 400b 的第二外部儲存單元 411 內。進而言之，寫入單元 330 自加密單元 323 接收已加密之內容，並寫入所接收的已加密之內容至記憶體卡 400b 的第一外部儲存單元 412 內。

讀取單元 350 自第一外部儲存單元 412 讀取該已加密之內容及自第二外部儲存單元 411 讀取該已加密之標題鑰匙，此二單元均被包括於記憶體卡 400b 內。然後讀取單元 350 分別輸出所讀取的已加密之標題鑰匙與所讀取的已加密之內容至解密單元 342 與解密單元 343。

五、發明說明（27）

解密單元342自讀取單元350接收該已加密之標題鑰匙，自獨一資訊儲存單元310讀取該獨一資訊，使用所讀取的獨一資訊作為鑰匙對所接收的已加密之標題鑰匙施用解密法則D2而產生該標題鑰匙，及輸出所產生的標題鑰匙至解密單元343。

此處，解密法則D2為用於實施加密法則E2之逆轉的法則。解密法則D2之一例為以DES為基礎的法則。

解密單元343自讀取單元350接收該已加密之內容及自解密單元342接收該標題鑰匙。然後解密單元343使用所接收的標題鑰匙為鑰匙對所接收的已加密之內容施用解密法則D3而產生該內容，並寫入所產生的內容至內部儲存單元303內作為內容601。

此處，解密法則D3為用於實施加密法則E3之逆轉的法則。解密法則D3之一例為以DES為基礎的法則。

現在描述行動電話300b之作業。

注意，數位著作物配銷系統所實施的整體被顯示於第4圖之流程圖，而其中之步驟S108-S111與步驟S112-S115分別被下面描述的步驟S131-S137與S141-S146替換。

參照第7圖顯示之流程圖，所描述者為被行動電話300b實施以產生該已加密之內容以及寫入該已加密之內容至記憶體卡400b之作業。

標題鑰匙產生單元321產生一標題鑰匙(步驟S131)。接著加密單元322自獨一資訊儲存單元310讀取獨一資訊(步驟S132)，然後使用所讀取的獨一資訊為鑰匙對所接收

五、發明說明（28）

的標題鑰匙施用加密法則而產生一已加密之標題鑰匙(步驟 S133)。連續地，寫入單元 330 自加密單元 322 接收該已加密之標題鑰匙，並寫入所接收的已加密之標題鑰匙至包括於記憶體卡 400b 之第二外部儲存單元 411(步驟 S134)。然後加密單元 323 自內部儲存單元 303 讀取該內容(步驟 S135)，並使用所接收的標題鑰匙為鑰匙對所讀取的內容施用加密法則 E3 而產生該已加密之內容(步驟 S136)。此後，寫入單元 330 寫入該已加密之內容至包括於記憶體卡 400b 之第一外部儲存單元 412 內(步驟 S137)。

參照第 8 圖顯示之流程圖，所描述者為被行動電話 300b 實施以自記憶體卡 400b 讀取該已加密之內容及產生該內容之作業。

讀取單元 350 自包括於記憶體卡 400b 內之第二外部儲存單元 411 讀取該已加密之標題鑰匙(步驟 S141)。接著，解密單元 342 自獨一資訊儲存單元 310 讀取該獨一資訊(步驟 S142)，並使用所讀取的獨一資訊為鑰匙對所讀取的已加密之標題鑰匙施用解密法則 D2 而產生該標題鑰匙(步驟 S143)。接著，讀取單元 350 自包括於記憶體卡 400b 內之第一外部儲存單元 412 讀取該已加密之內容(步驟 S144)。隨後，解密單元 343 使用該標題鑰匙為鑰匙對所接收的已加密之內容施用解密法則 D3 而產生該內容(步驟 S145)，並寫入所產生的內容至內部儲存單元 303 作為該內容(步驟 S146)。

如上述者，加密單元 320 與解密單元 340 在一例中運

五、發明說明（29）

用一 DES 法則之加密法則。

在此情形中，儲存於獨一資訊儲存單元 310 內之獨一資訊可為具有 56 位元之獨一的鑰匙。

或者被分配給該行動電話之電話號碼可被用作為該獨一資訊。在此情形中，該電話號碼受到一祕密變換函數以輸出 56 位元之獨一資訊，其被用作為該獨一資訊。

此處，DES 加密可以下列的方式被運用作為該祕密變換函數。此即該電話號碼使用一祕密的具有 56 位元的固定值受到 DES 加密而輸出具有 64 位元之值。該值的最後 56 個位元被用作為該獨一資訊。

進而言之，該獨一資訊儲存單元 310 與該內部儲存單元 303 被保護，免於被如稍後要描述之模型變更裝置的特別受到許可外之任何外部裝置讀取或寫入。更明確地說，每一獨一資訊儲存單元 310 與內部儲存單元 303 係由抗擅改之硬體、抗擅改之軟體或二者之組合所組成。

進而言之，該獨一資訊儲存單元 310 可在一卡片內被構建，其可在該行動電話裝卸。此種卡之例子為行動電話所使用之 SIM(客戶身份模組)卡。

再進而言之，在使用 DES 加密法則將該內容加密之時，該內容被分為每一個具有 64 位元之資料塊，然後每一資料塊使用該 56 位元之獨一鑰匙被加密以產生 64 位元的已加密之資訊塊。然而因而所產生的已加密之資料塊被連結在一起，且所連結的已加密之資料塊被輸出作為該已加密之內容(ECB(Electronic Codebook))模態。或者，該加密

五、發明說明（30）

可使用 CBC(Cipher Feedback Chaining)模態被完成。ECB 模態與 CBC 模態之細節例如可在“Introduction to Cryptographic Theory (Ango-Riron Nyumon)”(Eiji OKAMOTO 著，Kyoritsu Shuppan Co., LTD.出版)中被找到，故其描述被省略。

一般而言，行動電話 300 之內部儲存單元 303 的記憶體容量有限。此限制慣常地有下列問題之結果。在內部儲存單元 303 充滿數位著作物的情形中，使用者被要求刪除儲存於內部儲存單元 303 內的某些數位著作物以在購買其他數位著作物前確保有自由的記憶體空間，或其只不過是要放棄購買另外的數位著作物。

然而，依據第一實施例，使用者被允許在其決定在短時間內不使用數位著作物時將儲存於行動電話之內部儲存單元的某些數位著作物儲存至附裝於行動電話的記憶體卡內。在此方式下，自由記憶體空間被確保於行動電話之內部儲存單元內而不致損失播放其所購買之這些數位著作物的權利。後果為該使用者被允許購買某些更多數位著作物。

此處，數位著作物的某些版權持有人不會允許下列的使用型態。此即，例如當一已加密之內容使用某行動電話被儲存至一記憶體卡內時，該內容之版權持有人欲於該內容被禁止用作何其他行動電話被解密或被播放，甚至該記憶體卡被附裝於此亦然。

此處，第一實施例符合此端，此在於播放使用某行動電話已儲存於一記憶體卡的已加密之內容不能用特定行動

五、發明說明（31）

電話外的任何其他者被解密或播放，甚至該記憶體卡被附裝於此亦然。

換言之，當被儲存於附裝在行動電話之記憶體卡內的數位內容未被在儲存該內容時所使用的特定行動電話外任何其他行動電話加以解密或播放時，版權持有人之權利受到保護。此有利的特點將參照第9圖詳細地被描述。

如第9圖顯示者，行動電話A儲存獨一資訊A，行動電話X儲存獨一資訊X。

在寫入內容至一記憶體卡之際，行動電話A使用獨一資訊A將一標題鑰匙加密，並儲存該已加密之標題鑰匙至包括於記憶體卡之外部儲存單元(步驟S151)。接著，行動電話A使用該標題鑰匙將該內容加密，並儲存該已加密之內容至記憶體卡之外部儲存單元內(步驟S152)。

在自該記憶體卡讀取該已加密之內容之際，行動電話A自包括於記憶體卡內之外部儲存單元讀取該已加密之標題鑰匙，並使用該獨一資訊A將已加密之標題鑰匙解密(步驟S153)。接著，行動電話A自該外部儲存單元讀取該已加密之內容，並使用該已解密之標題鑰匙將該已加密之內容解密(步驟S154)。

此處，被使用以將標題鑰匙加密之獨一資訊與被使用以將已加密之標題鑰匙解密的獨一資訊為二者相同的獨一資訊A，故該已加密之標題鑰匙正確地被解密。後果為，被用以將該內容加密之標題鑰匙與被用以將該已加密之內容解密之標題鑰匙為相同的，故該內容正確地被解密。

五、發明說明（32）

另一方面，當行動電話X企圖播放該內容時，行動電話X自包括於記憶體卡內之外部儲存單元讀取該已加密之標題鑰匙，並使用該獨一資訊X將該標題鑰匙解密(步驟S155)。

此處，由於被使用以將標題鑰匙加密之獨一資訊A與被使用以將標題鑰匙解密之獨一資訊X不同，後果為該標題鑰匙未正確地被解密，故該已加密之內容也未正確地被解密。

所以，行動電話X在播放該已加密之內容時失敗。

此後描述符合本發明第二實施例之數位著作物配銷系統100c。

該數位著作物配銷系統100c之目標為要提供一數位著作物保護系統、一主要裝置、與一記錄媒體裝置，其每一個僅在當該內容被提供如數位著作物之播放次數被允許的數目或被允許的期間之使用狀況資料時依據使用狀況資料的被允許狀況下允許用該主要裝置播放一數位著作物。此即，在用這些裝置下，此實施例之目標在於根據顯示使用該數位著作物之許可狀況允許用該主要裝置播放數位著作物。

在數位著作物配銷系統100c中，當一內容被提供如許可的播放次數、許可的播放期間、或許可的總播放時間量之使用狀況資料時，該系統之行動電話被允許僅在該使用狀況資料所加諸的限制內播放該內容。

數位著作物配銷系統100c具有類似於數位著作物配

五、發明說明（33）

銷系統 100 之構造。此處主要描述與數位著作物配銷系統 100 之差異。

數位著作物配銷系統 100c 分別包括內容配銷伺服器裝置 200c 與行動電話 300c 取代內容配銷伺服器裝置 200 與行動電話 300。

基本上，內容配銷伺服器裝置 200c 具有類似包括於數位著作物配銷系統 100 內之內容配銷伺服器裝置 200 的構造。因而此後主要描述與內容配銷伺服器裝置 200 之差異。

除了該內容外，包括於內容配銷伺服器裝置 200c 之內容儲存單元 201 依照該內容預先儲存一使用狀況。

該使用狀況例如為被許可的播放次數。該被許可的播放次數對使用者被許可播放對應於該使用狀況之所儲存的內容之總次數加以限制。例如當被許可的播放次數被設定為“10”時，該使用者被許可最多播放該內容十次。

注意，該使用狀況可替選地為被許可的播放期間。該被許可的播放期間對該使用者被許可播放對應於該使用狀況之所儲存的內容之期間加以限制。該被許可的播放期間包含的資料顯示許可開始日期與許可截止日期。該使用者僅在該等許可開始日期與許可截止日期之期間內播放該內容。在此期間內使用者播放內容的次數不受限制。

或者，該使用狀況可為被許可的播放總時間量。該被許可的播放總時間量對該使用者播放對應於該使用狀況之所儲存的內容之累積時間量加以限制。例如當該被許可的播放總時間量被設定為“10 小時”，則只要播放總時間量

五、發明說明（34）

為在10小時內，該使用者便被許可播放該內容。當播放總時間量超過10小時，內容之播放被禁止。

進而言之，該使用狀況可包括所有的限制，即被許可的播放次數、被許可的播放期間、或被許可的播放總時間量，或其可包括自上面三種限制被選擇的任何二限制。

控制單元202自內容儲存單元201讀取內容，其用內容ID與對應於該使用狀況被儲存的儲存被辨識。然後該控制單元202經由傳輸/接收單元203、網際網路10、行動電話網路20與無線電基地台30傳輸所讀取的內容與使用狀況至行動電話300。此處該傳輸係透過如使用EMMS系統以安全的方式被實施。

如第10圖顯示者，行動電話300c除了構成行動電話300之元件外包括一使用狀況儲存單元305與使用狀況判斷單元306。

內容獲取單元302經由網際網路10、行動電話網路20、無線電基地台30、天線367與傳輸/接收單元361自內容配銷伺服器裝置200c接收該內容與使用狀況。然後內容獲取單元302寫入所接收的內容至內部儲存單元303內作為內容601，及所接收的使用狀況至使用狀況儲存單元305內。在此情形中，該使用狀況為被許可的播放次數。

使用狀況儲存單元305具有一儲存區用於儲存該使用狀況。

使用狀況判斷單元306自使用狀況儲存單元305讀取該使用狀況(即被許可的播放次數)以判斷所讀取的被許可

五、發明說明（35）

之播放次數是否超過0。

在判斷所讀取的被許可之播放次數超過0時，使用狀況判斷單元306自所讀取的被許可之播放次數減去1，並以減除結果之值蓋掉儲存於使用狀況儲存單元305內之使用狀況。接著，使用狀況判斷單元306輸出許可播放使用狀況303所儲存的內容之許可資訊。

或者，在判斷所讀取的被許可之播放次數小於或等於0時，該使用狀況判斷單元306不輸出該許可資訊且後果為播放單元304不播放該內容。

播放單元304自使用狀況判斷單元306接收表示許可播放內容之許可資訊。

在接收該許可資訊之際，播放單元304讀取儲存在內部儲存單元303之內容，並播放所讀取的內容至輸出。

現在參照第11圖之流程圖描述行動電話300c之作業。

注意，獨一資訊儲存單元之整體作業在第4圖中被顯示，所提供的步驟S116與S117被下面描述的步驟S201-S205替換。

使用狀況判斷單元306讀取該使用狀況，即被許可的播放次數(步驟S201)，並判斷所讀取的被許可之播放次數是否超過0(步驟S202)。當判斷所讀取的被許可之播放次數超過0(步驟S202)(是)時，使用狀況判斷單元306自被許可之播放次數減去“1”(步驟S203)，並以減除結果之值蓋掉儲存於使用狀況儲存單元中之使用狀況(步驟S204)。接著，使用狀況判斷單元306輸出該許可資訊表示許可播放

五、發明說明（36）

儲存於內部儲存單元303之內容。在回應下，播放單元304自使用狀況判斷單元306接收該許可資訊、讀取儲存於內部儲存單元303之內容、並播放所讀取的內容至輸出(步驟S205)。

或者，在判斷所讀取的被許可之播放次數小於或等於0(步驟S202)(否)時，使用狀況判斷單元306不輸出該許可資訊，且後果為播放單元304不播放該內容。此處要在此階段設定要刪除該內容亦為可應用的。

現在參照第12圖顯示之流程圖，其描述該使用狀況為該被許可之播放期間的情形中行動電話300c之作業。

注意，第4圖之流程圖顯示的數位著作物配銷系統整體作業中步驟S116與S117以下面描述之步驟S211-S214被替換。

使用狀況判斷單元306自使用狀況儲存單元305讀取該使用狀況(步驟S211)，即被許可之播放期間、獲取目前的日期/時間(步驟 S212)、及判斷所獲取的目前的日期/時間是否在該被許可之播放期間(步驟S213)。當許可目前的日期/時間為在被許可之播放期間內(步驟S213)(是)時，該使用狀況判斷單元306輸出該許可資訊至播放單元304表示許可播放儲存於使用狀況303內之內容。在回應下，播放單元304自使用狀況判斷單元306接收該許可資訊、讀取儲存於內部儲存單元303之內容、並播放所讀取的內容至輸出(步驟S214)。

或者，在判斷該目前的日期/時間落在該被許可之播放

五、發明說明（37）

期間外(步驟 S213)(否)時，使用狀況判斷單元 306 不輸出該許可資訊，且後果為播放單元 304 不播放該內容。此處若該目前的日期/時間是在該被許可之播放期間後時，要刪除該內容之設定為可應用的。

接著，參照第 13 圖顯示之流程圖，其描述該使用狀況為該被許可之播放時間總量的情形中行動電話 300c 之作業。

注意，第 4 圖之流程圖顯示的數位著作物配銷系統整體作業中步驟 S116 與 S117 以下面描述之步驟 S221-S226 被替換。

此處，內容儲存單元 201 進一步具有一儲存區用於儲存實際的播放時間總量。播放時間總量為該內容已實際被播放的累積時間。進而言之，該內容包括播放時間資訊顯示播放整個內容所花費的時間。

使用狀況判斷單元 306 自使用狀況儲存單元 305 讀取該使用狀況，即被許可之播放時間總量及實際的播放時間總量(步驟 S221)，並自該內容獲取該播放時間資訊顯示播放該內容所花費的時間(步驟 S222)，及計算所讀取的實際播放時間總量與所獲取的播放資訊顯示之時間的和以比較因而所計算之和與被許可之播放時間總量(步驟 S223)。在判斷被許可之播放時間總量大於或等於所計算之和(步驟 S223)(是)時，該使用狀況判斷單元 306 輸出該許可資訊至播放單元 304 表示許可播放儲存於內部儲存單元 303 內之內容。在回應下，播放單元 304 自使用狀況判斷單元 306

五、發明說明（38）

接收該許可資訊、讀取儲存於內部儲存單元303之內容、並播放所讀取的內容至輸出(步驟S224)。然後，使用狀況判斷單元306藉由實施下列的等式：實際播放時間總量＝實際播放時間總量＋播放時間資訊來計算播放時間總量(步驟S225)，並以最新計算的實際播放時間總量蓋掉儲存於使用狀況儲存單元305中之實際播放時間總量(步驟S226)。

或者，在判斷該被許可之播放時間總量小於所計算的和(步驟S223)(否)時，使用狀況判斷單元306不輸出該許可資訊，且後果為播放單元304不播放該內容。此處，若被許可之播放時間總量小於實際播放時間總量要刪除該內容之設定為可應用的。進而言之，就算被許可之播放時間總量不足於播放整個內容，許可播放該內容之設定亦為可應用的。

如上面描述者，包括於內容配銷伺服器裝置200c內之該內容儲存單元201儲存該內容與彼此相關的使用狀況，且內容配銷伺服器裝置200c傳輸該內容與對應的使用狀況至行動電話300c。當使用者購買提供有該使用狀況之內容時，包括於行動電話300c內之內部儲存單元303儲存所購買的內容，且使用狀況儲存單元305儲存所傳輸的使用狀況。

當使用者企圖播放其稍早已購買之內容時，使用狀況判斷單元306根據儲存於使用狀況儲存單元305之對應的使用狀況判斷是否要許可播放該內容。在判斷要許可播放

五、發明說明（39）

內容時，使用狀況判斷單元306指示播放單元播放該內容。

進而言之，該使用狀況可為該內容許可被複製或移動的次數。此處，「複製」該內容係指複製儲存於內部儲存單元之內容及寫入該內容之複製至一記錄媒體裝置內。此處，注意僅有內容之第一代「複製」為受許可的，自內容之複製來烤貝是被禁止的。此外，「移動」內容係指寫入儲存於內部儲存單元之內容至一記錄媒體裝置內並刪除儲存於該內部儲存單元之內容。當該使用狀況為內容被複製或被移動的被許可次數時，該內容被許可以所許可的次數被複製或被移動。

將所購買的內容加密以儲存至記憶體卡400內之程序與自記憶體卡400讀取該已加密之內容至行動電話300c的程序與第一實施例者相同，故其描述被省略。此處，其應被注意使用狀況資料非被寫入至記憶體卡內，而是被保存在包括於行動電話300c之使用狀況儲存單元305內。

注意，使用狀況儲存單元305被保護不會被稍後將描述之特別受許可之裝置外任何其他裝置由外部加以讀取或寫入。更明確地說，使用狀況儲存單元305係由抗擅改之硬體、抗擅改之軟體或二者之組合所組成。

進而言之，該使用狀況儲存單元305可在一卡片內被構建，其可在該行動電話裝卸。此種卡之例子為行動電話所使用之SIM(客戶身份模組)卡。

以此構造下，當一內容被提供使用狀況時，該內容僅在符合該使用狀況時被許可加以播放。

五、發明說明（40）

一般而言，行動電話300之內部儲存單元303的記憶體容量有限。此限制慣常地有下列問題之結果。在獨一資訊儲存單元充滿數位著作物的情形中，使用者被要求刪除儲存於獨一資訊儲存單元內的某些數位著作物以在購買其他數位著作物前確保有自由的記憶體空間，或其只不過是要放棄購買另外的數位著作物。

然而，依據第二實施例，類似於第一實施例者，使用者被允許在其決定在短時間內不使用數位著作物時將儲存於行動電話之內部儲存單元303的某些數位著作物儲存至附裝於行動電話300c的記憶體卡400內。在此方式下，自由記憶體空間被確保於行動電話之內部儲存單元303內而不致損失播放其所購買之這些數位著作物的權利。後果為該使用者被允許購買某些更多數位著作物。

進而言之，以此構造下，當一內容用某一行動電話被加密並被儲存於附裝於此之記憶體卡內時，該已加密之內容不可能用此特定行動電話外之任何其他行動電話被解密或播放。也就是說，第二實施例達成滿足版權持有人之需求的效果，使用某一行動電話被儲存於記憶體卡的內容被禁止用任何其他行動電話(雖然該記憶體卡被附裝於此)加以解密或播放。

現在顯示符合本發明之第三實施例的數位著作物配銷系統100d。

類似於數位著作物配銷系統100c地，當使用狀況被提供時，數位著作物配銷系統100d僅在該狀況滿足該使用狀

五、發明說明（41）

況時允許行動電話播放該內容。

數位著作物配銷系統 100d 具有類似於數位著作物配銷系統 100c 之構造，故本描述主要針對與數位著作物配銷系統 100c 之差異。

數位著作物配銷系統 100d 包括一內容配銷伺服器裝置 200d、行動電話 300d 與記憶體卡 400d 分別取代內容配銷伺服器裝置 200c、行動電話 300c 與記憶體卡 400。注意內容配銷伺服器裝置 200d 與內容配銷伺服器裝置 200c 相同。

如第 14 圖顯示者，記憶體卡 400d 由第一外部儲存單元 412、一第二外部儲存單元 411 與一認證單元 490 組成。

認證單元 490 實施與包括於行動電話 300d 之認證單元 390(稍後描述)之挑戰回應式的相互認證。更明確地說，認證單元 490 等待認證單元 390 來認證該認證單元 390，然後認證該認證單元 390。只有在二認證過程過都為成功的，相互認證被視為成功的。由於挑戰回應式的認證為習知的技術，其描述被省略。

第一外部儲存單元 412 具有一儲存區用於儲存一已加密之內容。

第二外部儲存單元 411 為一儲存單元，其僅在認證單元 490 之認證已成功地被實施時由另一端(即行動電話 300d)被讀取或寫入。第二外部儲存單元 411 具有儲存區用於儲存稍後將被描述之所加密的已連結之資訊。

行動電話 300d 具有類似於行動電話 300c 之構造。

五、發明說明（42）

如第15與16圖顯示者，行動電話300d包括加密/解密單元380d取代包括行動電話300c之加密/解密單元380，且亦包括寫入單元331與332以及讀取單元351與352取代行動電話300c所包括的寫入單元330及讀取單元350。行動電話300d進一步包括認證單元390。其他的元件與構成行動電話300c者相同。

此處，主要描述與行動電話300c之差異。

認證單元390自控制單元366接收一認證指令。

在接收該認證指令之際，認證單元390實施與包括於記憶體卡400d之認證單元490之挑戰回應式的相互認證。更明確地說，認證單元490等待認證單元390來認證該認證單元390，然後認證該認證單元390。只有在二認證過程過都為成功的，相互認證被視為成功的。

當相互認證已成功地被實施，認證單元390輸出資訊表示相互認證成功。

如第16圖顯示者，加密/解密單元380d係由一標題鑰匙產生單元321d、一加密單元322d、一加密單元323d、一連結單元324、一解密單元342d、一解密單元343d、及一分割單元344組成。

標題鑰匙產生單元321d自控制單元366接收一儲存指令。

在自控制單元366接收該儲存指令之際，標題鑰匙產生單元321d以類似包括於加密/解密單元380b之標題鑰匙產生單元321的方式產生一標題鑰匙，並輸出所產生的標

五、發明說明（43）

題鑰匙至連結單元 324 與加密單元 323d。

加密單元自獨一資訊儲存單元 310 讀取該獨一資訊，並自連結單元 324 接收該連結資訊。接著，加密單元 322d 使用所讀取的獨一鑰匙資訊為鑰匙對所接收的已連結之資訊施用加密法則 E2，而產生所加密的已連結之資訊，並輸出所加密的已連結之資訊至該寫入單元。

加密單元 323d 自標題鑰匙產生單元 321d 接收該標題鑰匙，並自內部儲存單元 303 讀取該內容 601。接著，加密單元 323d 使用所接收的標題鑰匙為鑰匙對所讀取的內容施用加密法則 E3，而產生一已加密之內容，並輸出該已加密之內容至寫入單元 332。

連結單元 324 自標題鑰匙產生單元 321d 接收該標題鑰匙，並自使用儲存 305 讀取該使用狀況。接著，連結單元 324 用所讀取的使用狀況以所描述的順序連結所接收的標題鑰匙以產生已連結之資訊，並輸出所產生的已連結之資訊至加密單元 322d。

解密單元 342d 自讀取單元 351 接收所加密的已連結之資訊，並自獨一資訊儲存單元 310 讀取該獨一資訊。接著，解密單元 342d 使用所讀取的獨一資訊為鑰匙對所接收、加密的已連結之資訊施用解密法則 D2 而產生該已連結之資訊，並輸出所產生的已連結之資訊至該分割單元 344。

解密單元 343d 自寫入單元 352 接收該已加密之內容，及自分割單元 344 接收該標題鑰匙。然後解密單元 343d 使用所接收的標題鑰匙為鑰匙對所接收的已加密之內容施

五、發明說明（44）

用解密法則 D3 而產生該內容，並寫入所產生的內容至內部儲存單元 303 內。

分割單元 344 自解密單元 342d 接收該已連結之資訊，並分割所接收的已連結之資訊以產生該標題鑰匙與該使用狀況。然後分割單元 344 輸出所產生的標題鑰匙至解密單元 343d，並寫入所產生的使用資訊至使用狀況儲存單元 305。

寫入單元 331 自加密單元 322d 接收所加密的已連結之資訊，並寫入所接收、加密的已連結之資訊至包括於記憶體卡 400d 之第二外部儲存單元 411。

寫入單元 332 自加密單元 323d 接收該寫入，並寫入所接收的已加密之內容至第一外部儲存單元 412。

讀取單元 351 自控制單元 366 接收一讀取指令。

在接收該讀取指令之際，控制單元 366 自包括於記憶體卡 400d 之第二外部儲存單元 411 讀取所加密的已連結之資訊，並輸出所讀取、加密的已連結之資訊至解密單元 342d。

讀取單元 352 自包括於記憶體卡 400d 之第一外部儲存單元 412 讀取該已加密之內容 602，並輸出所讀取的已加密之內容至解密單元 343d。

控制單元 366 自輸入單元 365 接收一內容寫入指令與一內容讀取指令。在接收該內容寫入指令與該內容讀取指令之際，控制單元自認證單元 390 接收表示該認證是成功或失敗的資訊。

五、發明說明（45）

在自輸入單元365接收內容寫入指令以及自認證單元390接收表示認證成功的資訊之情形中，控制單元366輸出一儲存指令至加密/解密單元380d之標題鑰匙產生單元321d。

在自輸入單元365接收內容讀取指令以及自認證單元390接收表示認證成功的資訊之情形中，控制單元366輸出一讀取指令至該讀取單元351。

在接收該寫入指令或該讀取指令以及表示認證不成功的情形中，控制單元366棄置所接收的寫入指令或讀取指令，且後果為無寫入作業或讀取作業被實施。

此後描述數位著作物配銷系統100d之作業。

首先參照第17圖顯示之流程圖描述數位著作物配銷系統100d之整體作業。

行動電話300d之內容購買單元301自輸入單元365接收該內容ID以產生付款資訊(步驟S251)，並傳輸該內容ID與付款資訊至內容配銷伺服器裝置200d(步驟S252)。

內容配銷伺服器裝置200d之控制單元202由行動電話300d接收該內容ID與付款資訊(步驟S252)、根據所接收的付款資訊實施處理以接收付款(步驟S253)、自內容儲存單元201讀取用所接收的內容ID被辨識之內容(步驟S254)、及傳輸所讀取的內容至行動電話(步驟S255)。

行動電話300d之內容獲取單元302自內容配銷伺服器裝置200d接收被傳輸之內容(步驟S255)，並寫入所接收的內容至內部儲存單元303作為內容601(步驟S256)。

五、發明說明（46）

在自輸入單元365接收一內容寫入指令的情形中，內容配銷伺服器裝置366輸出一認證指令至認證單元390(步驟S257)。在接收該認證指令之際，認證單元390與記憶體卡400d之認證單元490實施相互認證(步驟S258)。當該認證實施成功時，即自認證單元390接收表示認證成功的資訊(步驟S259)(是)時，控制單元366輸出一儲存指令至加密/解密單元380d，且加密/解密單元380d實施處理以儲存該內容(步驟S260)。或者，當認證不成功時，即自認證單元390接收表示認證不成功的資訊(步驟S259)(否)時，控制單元366棄置已接收的內容寫入指令。後果為無儲存處理被實施。

或者，在自輸入單元365接收一內容讀取指令的情形中，控制單元366輸入一認證指令至認證單元390(步驟S257)。在自控制單元366接收該認證指令之際，認證單元390與包括於記憶體卡400d之認證單元490實施相互認證(步驟S261)。當該認證實施成功時，即自認證單元390接收表示認證成功的資訊(步驟S262)(是)時，控制單元366輸出一讀取指令至讀取單元351，且讀取單元351在回應於下實施讀取處理(步驟S263)。或者，當該認證不成功時，即自認證單元390接收表示認證不成功的資訊(步驟S262)(否)時，控制單元366棄置已接收的讀取指令。後果為無讀取處理被實施。

或者，在自輸入單元365接收一內容播放指令的情形(步驟S257)中，控制單元366指示以實施播放處理(步驟

五、發明說明（47）

S264)。

現在參照第 18 圖描述行動電話 300d 與記憶體卡 400d 間被實施的相互認證作業。

注意此處所描述的相互認證為第 17 圖之流程圖顯示的步驟 S258 與 S261 實施的作業細節。

行動電話 300d 之認證單元 390 認證記憶體卡 400d 之認證單元 490。當在此步驟之認證成功地被實施(步驟 S272)(是)時，則認證單元 490 認證該認證單元 390(步驟 S273)。當在此步驟之認證成功地被實施(步驟 S274)(是)時，認證單元 490 輸出表示認證成功的資訊至控制單元 366(步驟 S275)。

當步驟 S271 之認證不成功(步驟 S272)(否)時，或步驟 S273 之認證不成功(步驟 S273)(否)時，認證單元 490 輸出表示認證成功的資訊至控制單元 366(步驟 S276)。

現在參照第 19 圖顯示之流程圖描述行動電話 300d 為儲存處理所實施之作業。

在自控制單元 366 接收儲存指令之際，加密/解密單元 380d 之標題鑰匙產生單元 321d 產生一標題鑰匙，並輸出所產生的標題鑰匙至連結單元 324 與加密單元 323d(步驟 S281)。

接著，連結單元 324 自標題鑰匙產生單元 321d 接收標題鑰匙，並自使用狀況儲存單元 305 讀取使用狀況(步驟 S282)。接著，連結單元 324 以所述之順序連結所接收的標題鑰匙與所讀取的使用狀況以產生已連結之資訊，並輸出

五、發明說明（48）

所產生的已連結之資訊至加密單元322d(步驟S283)。

接著，加密單元322d自獨一資訊儲存單元310讀取獨一資訊，並自連結單元324接收該已連結之資訊(步驟S284)。接著，連結單元322d使用所讀取的已連結之資訊為鑰匙對所接收的已連結之資訊施用加密法則E2，而產生所加密的已連結之資訊，並輸出所加密的已連結之資訊(步驟S285)。寫入單元331在回應下自加密單元322d接收該所加密的已連結之資訊，並寫入所接收、所加密的已連結之資訊至包括於記憶體卡400d之第二外部儲存單元411內。

接著，加密單元323d自標題鑰匙產生單元321d接收該標題鑰匙、並自內部儲存單元303讀取內容601(步驟S287)。進而言之，加密單元323d使用所接收的標題鑰匙為鑰匙對所讀取的內容施用加密法則E3而產生一已加密之內容，並輸出所產生的已加密之內容至寫入單元332(步驟S288)。寫入單元332在回應下自加密單元323d接收該已加密之內容，並寫入所接收的已加密之內容至第一外部儲存單元412(步驟S289)。

現在參照第20圖描述行動電話300d為讀取處理所實施之作業。

在自控制單元366接收該讀取指令之際，讀取單元351自包括於記憶體卡400d之第二外部儲存單元411讀取所加密的已連結之資訊，並輸出所讀取、加密的已連接之資訊至解密單元342d(步驟S291)。解密單元342d在回應下自

五、發明說明（49）

讀取單元 351 接收所加密的已連結之資訊、自獨一資訊儲存單元 310 讀取獨一資訊(步驟 S292)、使用所讀取的獨一資訊為鑰匙對所接收、加密的已連結之資訊施用解密法則 D2 而產生該已連結之資訊、然後輸出所產生的已連結之資訊至分割單元 344(步驟 S293)。

後果為，分割單元 344 自解密單元 342d 接收該已連結之資訊，並分割所接收的已連結之資訊以產生該標題鑰匙與該使用狀況。然後分割單元 344 輸出所產生的標題鑰匙至解密單元 343d，並讀取重新所產生的使用狀況至使用狀況儲存單元 305(步驟 S294)。

接著，讀取單元 342 自包括記憶體卡 400d 之第一外部儲存單元 412 讀取該已加密之內容 602，並輸出所讀取的已加密之內容至解密單元 343d(步驟 S295)。接著，解密單元 343d 分別自讀取單元 352 與分割單元 344 接收該已加密之內容與該標題鑰匙、使用所接收的標題鑰匙為鑰匙對所接收的已加密之內容施用解密法則 D3 而產生該內容(步驟 S296)、並寫入所產生的內容至內部儲存單元 303(步驟 S297)。

為寫入該內容至記憶體卡 400d 內，行動電話 300d 產生該標題鑰匙、讀取該使用狀況、並連結該標題鑰匙與該使用狀況以產生已連結之資訊。接著，行動電話 300d 使用該獨一資訊將該已連結之資訊加密、並寫入所加密的已連結之單元至包括於記憶體卡 400d 之第二外部儲存單元 411 內。接著，行動電話 300d 自內部儲存單元 303 讀取該內容，

五、發明說明（50）

並寫入該已加密之內容至包括於記憶體卡 400d 之第一外部儲存單元 412 內。

為自記憶體卡 400d 讀取內容，行動電話 300d 自包括於記憶體卡 400d 之第二外部儲存單元 411 讀取所加密的已連接之資訊，並使用該將所加密的已連接之資訊解密以產生該已連結之資訊。然後行動電話 300d 分割所產生的已連結之資訊以產生標題鑰匙與使用狀況，並寫入所產生的使用狀況至使用狀況儲存單元 305。接著，行動電話 300d 自包括於記憶體卡 400d 之第一外部儲存單元 412 讀取該已加密之內容，並使用該標題鑰匙為鑰匙將該已加密之內容解密而產生該內容，及寫入所產生的內容至內部儲存單元 303 內。

為播放該內容，行動電話 300d 順從儲存於使用標題鑰匙 305 之使用狀況播放儲存於內部儲存單元 303 之內容。

此後描述行動電話 300d 之使用者實施的作業程序。

首先，在使用行動電話 300d 之內容購買單元 301，使用者自被提供使用狀況且被儲存於內容配銷伺服器裝置 200d 之內容儲存單元 201 的每一內容選擇及購買一內容。然後在使用內容獲取單元 302 下，使用者接收其已購買之內容。然後該內容與該使用狀況分別被儲存於內部儲存單元 303 與使用已解密之內容 305 內，此二者均被包括於行動電話 300d 中。

接著，在所購買的內容例如為音樂伴唱資料且附掛於此的使用狀況為允許播放該內容十次的情形中，使用狀況

五、發明說明（51）

判斷單元306允許播放單元304播放該音樂伴唱資料達到十次。

進而言之，在下列的程序中，使用者可將內容601與使用狀況儲存於記憶體卡400d內，其原分別被儲存於內部儲存單元303與使用已解密之內容305內，此二者均被包括於行動電話300d中。

使用者附裝該記憶體卡400d至行動電話300d，並選擇一作業來儲存被提供有該使用狀況於該記憶體卡內之所購買的內容。

在回應下，對每一內容為唯一的之標題鑰匙被標題鑰匙產生單元321d產生。然後所產生的標題鑰匙被連結單元324用該使用狀況加以連結以產生已連結之單元。該已連結之單元被加密單元322d用儲存於獨一資訊儲存單元310之獨一資訊加以加密。假設相互認證在行動電話300d之認證單元390與記憶體卡400d之認證單元490間成功地被實施，該所加密的已連結之單元被寫入單元331儲存至包括於記憶體卡400d之第二外部儲存單元411。接著，儲存於內部儲存單元303之內容被加密單元323d使用該標題鑰匙加密，且該已加密之內容被儲存至包括於記憶體卡400d之第一外部儲存單元412內。

再進而言之，使用者可自儲存於記憶體卡400d之所加密的已連結之單元與該已加密之內容602擷取該使用狀況與該內容，並以下列程序儲存所擷取的內容與使用狀況至行動電話300d之內部儲存單元303內。

五、發明說明（52）

使用者附裝記憶體卡 400d 至行動電話 300d，並選擇一作業以自記憶體卡 400d 取還被提供該使用狀況之該已加密之內容。

在回應下，相互認證在行動電話 300d 之認證單元 390 與記憶體卡 400d 之認證單元 490 間被實施。假設該相互認證成功，儲存於第二外部儲存單元 411 之所加密的已連結之資訊被讀取單元 351 讀取。然後該所讀取的已連結之資訊被解密單元 342d 使用儲存於獨一資訊儲存單元 310 之獨一資訊加以解密。該所解密的已連結之資訊再被分割以產生該標題鑰匙與該使用狀況。該使用狀況被儲存於使用狀況儲存單元 305 內。進而言之，儲存於包括在記憶體卡 400d 之第一外部儲存單元 412 的已加密之內容被讀取單元 352 讀取。然後該所讀取的內容被解密單元 343d 使用一標題鑰匙解密以產生已解密之內容，且該已解密之內容被儲存於內部儲存單元 303 內。

在本發明之上述實施例中係描述儲存所購買的已被提供該使用狀況之內容至記憶體卡內的程序。然而，該內容是否已被購買對本發明並非根本事項。此即上面的程序例如對其被提供作為具有某種使用狀況的免費樣本之內容為可應用的。

DES 為在加密單元 322d 與 323d 及解密單元 342d 與 343d 所運用的加密系統之例子。

在運用 DES 加密的情形中，儲存於獨一資訊儲存單元 310 之獨一資訊可為具有 56 位元的唯一鑰匙。或者，被分

五、發明說明（53）

配給行動電話之電話號碼可被用作為該獨一資訊。在後者情形中，較佳地是運用一祕密轉換函數，其回應於該電話號碼的輸入重調一個 56 位元之獨一鑰匙。此處，轉換函數之一例為以下列方式使用 DES 加密。此即，該電話號碼使用具有 56 個位元之一祕密獨一值受到 DES 加密。被輸出之最後 56 個位元被用作為該獨一資訊。

進而言之，獨一資訊儲存單元 310、內部儲存單元 303 與使用狀況儲存單元 305 被保護免於被除了如下面被描述之模型變更裝置的特別受許可外之任何其他外部裝置加以讀取或寫入。更明確地說，每一獨一資訊儲存單元 310、內部儲存單元 303 與使用狀況儲存單元 305 係由抗擅改之硬體、抗擅改之軟體、或二者之組合所組成。

再進而言之，獨一資訊儲存單元 310 與使用狀況儲存單元 305 可在自行動電話可裝卸的如 SIM 卡內被構建。

再進而言之，在使用 DES 加密將該內容加密時，該內容被分為具有 64 位元之資料塊；然後每一資料塊使用該 56 位元之獨一鑰匙被加密以產生一個 64 位元之已加密的資料塊。該因而所產生的已加密之資料塊再被連結在一起，且該所連結的已加密之資料塊被輸出作為已加密之內容。

在上述之構造下，被提供使用狀況之內容僅在狀況符合使用狀況下被播放。

進而言之，一般而言，行動電話 300d 之內部儲存單元 303 的記憶體受限。慣常地，此限制的結果有下列的問題。

五、發明說明（54）

在內部儲存單元充滿數位著作物時，使用者被要求刪除儲存在內部儲存單元之某些數位著作物以在購買另外的數位著作物前確保有自由記憶體空間，或者其只不過要放棄另外的數位著作物。

然而，依據第三實施例，顯示於第一與第二實施例者，使用者被允許在其決定在短時間內不使用數位著作物時將儲存於行動電話300d之內部儲存單元303的某些數位著作物儲存至附裝於行動電話300d的記憶體卡400d內。在此方式下，自由記憶體空間被確保於行動電話300d之內部儲存單元303內而不致損失播放其所購買之這些數位著作物的權利。後果為該使用者被允許購買某些更多數位著作物以儲存至內部儲存單元303內。

以此構造下，當一內容被加密且被儲存於裝在某行動電話之記憶體卡時，已加密之內容不可能用特定行動電話外之任何其他行動電話被解密或播放。此即，第三實施例達成符合版權持有人之要求的效果，使用某一行動電話儲存於記憶體卡內之內容被禁止用任何其他行動電話被解密或播放，就算該記憶體卡被裝於此亦然。

現在描述另一第四較佳實施例。

此處描述一模型變更系統600e。

該模型變更系統600e目標在於提供一模型變更裝置被用以變更如行動電話之一記錄/播放裝置，其在一使用者與一服務供應商間對因變更合約所致的新記錄/播放裝置完成的合約下為可用的。在用此模型變更裝置進行模型變

五、發明說明（55）

更之際，儲存於原先使用的記錄/播放裝置之數位著作物對新的記錄/播放裝置為可用的，而無處理對該等數位著作物被實施。

例如在發表具有新特色的行動電話之際，使用者可能會要變更目前使用的電話為新的行動電話。在此情形中，使用者被允許用分配給目前使用者之電話號碼來使用新行動電話。此為藉由重新分配原先分配給目前行動電話的電話號碼至新行動電話而被完成。此種某電話號碼由某行動電話分配到另一行動電話的重新分配稱為行動電話之模型變更。

在上述的模型變更後，儲存在第一、第二、第三實施例之行動電話的已購買內容不再被新行動電話使用。為何這些內容不會被播放的原因已在上面被描述。

對使用者不利的是使用者購買已在記憶體卡儲存的內容因模型變更變成不可使用的。模型變更系統 600e 目標在針對此問題。

如第 21 圖顯示者，模型變更系統 600e 由行動電話 A 300e，模型變更裝置 500 與行動電話 B 300f 組成。行動電話 A 300e 與行動電話 B 300f 分別被連接至模型變更裝置 500。

行動電話 A 300e 除了獨一資訊儲存單元 310e 外具有與第一、第二、第三實施例之任何行動電話類似的構造。注意，其他的元件為簡單起見未在圖中顯示。該獨一資訊儲存單元 310e 預先儲存獨一資訊。

五、發明說明（56）

進而言之，行動電話 B 300f 除了獨一資訊儲存單元 310f 外具有與第一、第二、第三實施例之任何行動電話類似的構造。注意，其他的元件為簡單起見未在圖中顯示。該獨一資訊儲存單元 310f 具有儲存區用於預先儲存獨一資訊。

模型變更裝置 500 由資訊讀取單元 501 與資訊寫入單元 502 組成。

資訊讀取單元 501 自包括於行動電話 A 300e 之獨一資訊儲存單元 310e 讀取該獨一資訊，並接續地自獨一資訊儲存單元 310e 刪除該獨一資訊。然後資訊讀取單元 501 輸出所讀取的資訊至資訊寫入單元 502。

資訊寫入單元 502 自資訊讀取單元 501 接收該獨一資訊，並寫入所接收的獨一資訊至包括於行動電話 B 300f 之獨一資訊儲存單元 310f 內。此處，該獨一資訊為對行動電話 A 300e 為獨一的資訊。該獨一資訊之例為被分配給行動電話 A 300e 之電話號碼，即隨機地被產生及被分配給行動電話 A 300e 之隨機數字。

現在參照第 22 圖顯示之流程圖描述模型變更系統 600e 之作業。

資訊讀取單元 501 自獨一資訊儲存單元 310e 讀取該獨一資訊(步驟 S301)，並接續地自獨一資訊儲存單元 310e 刪除該獨一資訊(步驟 S302)。接著，資訊寫入單元 502 寫入自資訊讀取單元 501 接收的獨一資訊至獨一資訊儲存單元 310f(步驟 S303)。

五、發明說明（57）

以此構造下，行動電話B被允許不須對該等內容實施任何處理地讀取及播放用行動電話A購買且儲存於記憶體卡內之內容。

此處描述模型變更系統600g。

如第23圖顯示者，模型變更系統600g由行動電話A 300g、模型變更裝置500與行動電話B 300h組成。行動電話A 300g與行動電話B 300h分別被連接至模型變更系統500。

行動電話A 300g除了獨一資訊儲存單元310g與使用狀況儲存單元305g外具有類似第二、第三實施例之構造。注意，其他的元件為了簡單起見未被顯示。獨一資訊儲存單元310g預先儲存獨一資訊，及使用狀況儲存單元305g預先儲存該使用狀況。

行動電話B 300h除了獨一資訊儲存單元310h與使用狀況儲存單元305h外具有類似第二、第三實施例之構造。注意，其他的元件為了簡單起見未被顯示。獨一資訊儲存單元310h具有一儲存區獨一資訊，且該使用狀況儲存單元305h具有一儲存區用於儲存該使用狀況。

模型變更系統500由一資訊讀取單元501與一資訊寫入單元502組成。

資訊讀取單元501自包括於行動電話300g之獨一資訊儲存單元310g讀取該獨一資訊，並自使用狀況儲存單元305g讀取該使用狀況。隨後，資訊讀取單元501分別自獨一資訊儲存單元310e與使用狀況儲存單元305g刪除該獨

五、發明說明（58）

一資訊與該使用狀況。接著，資訊讀取單元 501 輸出所讀取的獨一資訊與使用狀況至資訊寫入單元 502。

在回應下，資訊寫入單元 502 自資訊讀取單元 501 接收該獨一資訊與使用狀況。接著，資訊寫入單元 502 分別寫入所接收的獨一資訊與使用狀況至獨一資訊儲存單元 310h 與使用狀況儲存單元 305h，此二者均被包括於行動電話 B 300h 內。

以此構造下，行動電話 B 被允許完全不須對該等內容實施任何處理地讀取及播放用行動電話 A 購買且儲存於記憶體卡內之內容。

正常而言，為了模型變更或合約取消，行動電話必須將其行動電話攜至以「Docomo 店」為類型之行動電話服務供應商，模型變更或取消合約之處理在此被實施。此處「取消合約」係指在行動電話使用者與行動電話服務供應商間已完成之合約的取消。在合約的取消後，在合約下被分配之電話號碼不再為可使用的。

此處描述一種模型變更系統，其消除使用者在取消其合約須做出至服務供應商店之旅次的麻煩。

在模型變更或取消合約時，下面的要求必須被滿足。

1.在行動電話模型變更之際，其被要求新行動電話(新近購買的行動電話)替換目前者，其被允許播放被儲存於該記憶體卡之內容。反過來，其被要求將被替換之行動電話(目前使用之行動電話)不再被允許播放儲存於記憶體卡內之內容。

五、發明說明（59）

2.就算在一行動電話之合約被取消後，其被要求儲存於記憶體卡內之內容仍被該行動電話播放。也就是在合約取消後，行動電話不再作用成電話，而作用成一播放裝置用於播放稍早已購買之內容。

3.就算行動電話(持用人)之服務供應商被變更為另一個，其被要求儲存於記憶體卡內之儲存仍被新持用人操作下為可使用的行動電話加以播放。例如，就算行動電話服務供應商已由“DoCoMo”變更為“au”，該行動電話仍須被允許播放儲存於儲存於記憶體卡之內容。

一模型變更系統 600m 目標為符合上面的「第一要求」。就此而言，模型變更系統 600m 經由一通訊網路儲存在目前使用中之行動電話所儲存的獨一資訊至新的行動電話，並接續地經由一通訊網路自目前的行動電話刪除該獨一資訊。

如第 24 圖顯示者，模型變更系統 600m 由行動電話 A 300m、一行動電話 B 300n、一個人電腦(PC)650、及一模型變更裝置 500m 組成。PC 650 與模型變更裝置 500m 經由網際網路 10 彼此被連接。行動電話 A 300m 為目前使用而將被替換之行動電話，且行動電話 B 300n 為替換目前者之新行動電話。

行動電話 A 300m 具有類似第一、二、三實施例所描述之任何行動電話的構造，除了獨一資訊儲存單元 310m 外。此外，行動電話 A 300m 包括判斷單元 360m。注意，其他的元件為了簡單起見未被顯示。

五、發明說明（60）

獨一資訊儲存單元 310m 預先儲存獨一資訊。

判斷單元 360m 在行動電話 A 300m 經由 PC 650 與網際網路 10 被連接時，自稍後將被描述之模型變更裝置 500m 接收第一模型變更資訊。然後，判斷單元 360m 根據包括於第一模型變更資訊之簽名資訊判斷所接收的第一模型變更裝置是否有效。由於該第一模型變更資訊之判斷認證性的技術被習知為數位簽名技術，故其詳細描述被省略。在判斷該資訊為有效時，判斷單元 360m 服從包括於該第一模型變更資訊之讀取指令，自獨一資訊儲存單元 310m 讀取該獨一資訊，且經由 PC 650 與網際網路 10 傳輸所讀取的獨一資訊至模型變更裝置 500m。此外，在判斷該資訊為有效時，判斷單元 360m 服從包括於該第一模型變更資訊之刪除指令，自獨一資訊儲存單元 310m 刪除該獨一資訊。或者，當判斷該資訊為無效時，判斷單元 360m 只不過棄置所接收的第一模型變更資訊，且不實施作業。

行動電話 B 300n 具有類似第一、二、三實施例所描述之任何行動電話的構造，除了獨一資訊儲存單元 310n 外。此外，行動電話 B 300n 包括判斷單元 360n。注意，其他的元件為了簡單起見未被顯示。

獨一資訊儲存單元 310n 具有一儲存區用於儲存獨一資訊。

判斷單元 360n 在行動電話 B 300n 經由 PC 650 與網際網路 10 被連接時，自稍後將被描述之模型變更裝置 500m 接收第二模型變更資訊。然後，判斷單元 360n 根據包括於

五、發明說明（61）

第二模型變更資訊之簽名資訊判斷所接收的第二模型變更資訊是否有效。在判斷該資訊為有效時，判斷單元 360n 服從包括於該第二模型變更資訊之寫入資訊自該第二模型變更資訊擷取該獨一資訊，並寫入所擷取的獨一資訊至獨一資訊儲存單元 310n。或者，當判斷該資訊為無效時，判斷單元 360n 只不過棄置所接收的第二模型變更資訊，且不實施作業。

更明確地說，PC 650 為一電腦系統，例如由微處理器、ROM、RAM、硬碟單元、顯示器單元、鍵盤、LAN 連接單元及行動電話用之連接單元組成。該電腦系統所使用的 RAM 或硬碟單元儲存電腦程式。PC 650 用依照電腦程式作業之微處理器實施其功能。

在接收使用者的模型變更作業之際，PC 650 經由網際網路 10 傳輸一模型變更指令至模型變更裝置 500m。

PC 650 連續地經由網際網路 10 實施行動電話 A 300m 與模型變更裝置 500m 間的資訊傳輸。然後 PC 650 經由網際網路 10 實施行動電話 B 300n 與模型變更裝置 500m 間的資訊傳輸。

模型變更裝置 500m 具有類似模型變更裝置 500 之構造，且額外地包括一傳輸/接收單元 505。

傳輸/接收單元 505 經由網際網路 10 接收模型變更指令。傳輸/接收單元 505 在接收模型變更指令之際產生第一模型變更資訊。此處，該第一模型變更資訊包括表示自我認證之簽名資料、一讀取指令以讀取該獨一資訊、及一刪

五、發明說明（62）

除指令來指示要刪除該獨一資訊。接著，該傳輸/接收單元505傳輸所產生的第一模型變更資訊至行動電話A 300m。

進而言之，傳輸/接收單元505自行動電話A 300m接收該獨一資訊。

接著，傳輸/接收單元505產生第二模型變更資訊。此處，該第二模型變更資訊包括表示自我認證之簽名資料、一讀取指令以指示要讀取所接收的獨一資訊、及一寫入指令來指示要寫入該獨一資訊。接著，該傳輸/接收單元505傳輸所產生的第二模型變更資訊至行動電話B 300n。

現在參照第25圖顯示之流程圖描述模型變更系統600m之作業。

在此階段，使用者行動電話A 300m與行動電話B 300n二者至PC 650。

在接收使用的模型變更作業之際(步驟S501)，PC 650經由網際網路10傳輸一模型變更指令至模型變更裝置500m(步驟S502)。

在回應下，包括於模型變更裝置500m之傳輸/接收單元505經由網際網路10接收該模型變更指令(步驟S502)、產生該第一模型變更資訊(步驟S503)、及傳輸所產生的第一模型變更資訊至行動電話A 300m(步驟S504)。

在接收第一模型變更資訊之際(步驟S504)，包括於行動電話A 300m之判斷單元360m自獨一資訊儲存單元310m讀取該獨一資訊(步驟S505)，並經由PC 650與網際網路10傳輸所讀取的獨一資訊(步驟S506)。然後判斷單元

五、發明說明（63）

360m 自獨一資訊儲存單元 310m 刪除該獨一資訊(步驟 S507)。

在接收該第二模型變更資訊之際(步驟 S509)，行動電話 B 300n 之判斷單元 360n 自該第二模型變更資訊擷取該獨一資訊，並寫入所擷取的獨一資訊至獨一資訊儲存單元 310n 內(步驟 S510)。

此處描述對以符合上述「第二要求」之模型變更系統 600m 的修改。

在此處被描述之修改中，儲存於行動電話中之獨一資訊係自被分配給該行動電話之電話號碼外的獨一資訊被產生。因而，儲存於記憶體卡內之內容已非用該電話號碼而是另外的獨一資訊型式被加密。換言之，該等內容是以非電話號碼為方向，然後被儲存於記錄媒體裝置內。

進而言之，在取消該合約之時被分配給且儲存於該行動電話內將被刪除之電話號碼被刪除以使該電話號碼失效。不過，該行動電話仍保存該獨一資訊以允許內容之播放。

該修改的模型變更系統 600m 具有類似模型變更系統 600m 的構造。更明確地說，該修改過的模型變更系統 600m 由行動電話 A 300m、PC 650、與模型變更裝置 500m 組成。PC 650 與模型變更裝置 500m 經由網際網路 10 彼此被連接。此處，行動電話 A 300m 為該使用者將要取消其合約的電話。

行動電話 A 300m 之獨一資訊儲存單元 310m 儲存對行

五、發明說明（64）

動電話 A 300m 為獨一的資訊，如分配給行動電話 A 300m 之隨機號碼以及分配給行動電話 A 300m 之電話號碼。

使用者連接行動電話 A 300m 至 PC 650，並使用 PC 650 實施作業以取消該行動電話之合約。

在接收使用者的取消作業之際，PC 650 對行動電話 A 300m 輸出一取消指令。

在回應下，行動電話 A 300m 之判斷單元 360m 接收該取消指令。在接收之取消指令之際，判斷單元 360m 自獨一資訊儲存單元 310m 讀取該電話號碼，並經由 PC 650 與網際網路 10 傳輸所讀取的電話號碼至模型變更裝置 500m。

在回應下，模型變更裝置 500m 之傳輸/接收單元 505 接收該電話號碼，並實施處理用於根據所接收的電話號碼進行取消。

此處描述目標符合上述「第三要求」之模型變更系統 600m 的另一修改。

一般而言，當行動電話持用人變更為別人時其電話號碼也被變更。因此這裏所描述的修改中，該獨一資訊並非由電話號碼而是其他型式的獨一資訊被產生。因而，儲存於記憶體卡內之內容已非用該電話號碼而是另外的獨一資訊型式被加密。換言之，該等內容是以非電話號碼為方向，然後被儲存於記錄媒體裝置內。進而言之，該獨一資訊被維持儲存於該行動電話內，甚至持用人變更後亦然。

該修改的模型變更系統 600m 具有類似模型變更系統

五、發明說明（65）

600m 的構造。更明確地說，該修改過的模型變更系統 600m 由行動電話 A 300m、PC 650、與模型變更裝置 500m 組成。PC 650 與模型變更裝置 500m 經由網際網路 10 彼此被連接。此處，行動電話 A 300m 為該使用者將要變更其持用人的電話。

此處參照第 26 圖顯示之流程圖描述該修改後之模型變更系統 600m 的作業。

行動電話 A 300m 之獨一資訊儲存單元 310m 儲存對行動電話 A 300m 為獨一的資訊，如分配給行動電話 A 300m 之隨機號碼以及分配給行動電話 A 300m 之電話號碼。

使用者連接行動電話 A 300m 至 PC 650，並使用 PC 650 實施作業以取消該行動電話之合約。

在接收使用者為變更使用狀況資訊的作業之際(步驟 S531)，PC 650 輸出一讀取指令至行動電話 A 300m 以指示讀取目前的電話號碼(步驟 S532)。在回應下，包括於行動電話 A 300m 之判斷單元 360m 自獨一資訊儲存單元 310m 讀取目前的電話號碼，並輸出所讀取的電話號碼至 PC 650(步驟 S534)。

在回應下，PC 650 自行動電話 A 300m 接收目前的電話號碼、產生一持用人變更指令、及經由網際網路 10 傳輸所產生的持用人變更指令與所接收的目前電話號碼至模型變更系統 500m。

模型變更系統 500m 之傳輸/接收單元 505 實施處理以取消目前電話號碼之合約(步驟 S536)。然後，傳輸/接收單

五、發明說明（66）

元 505 實施處理以與服務供應商完成新合約(步驟 S537)、為新電話號碼實施設定作業(步驟 S538)、並經由網際網路 10 傳輸新設定的電話號碼至 PC 650(步驟 S539)。

在回應下，PC 650 接收新的電話號碼(步驟 S539)，並輸出所接收的新電話號碼至行動電話 A 300m(步驟 S540)。

在接收新電話號碼之際(步驟 S539)，行動電話 A 300m 之判斷單元 360m 自獨一資訊儲存單元 310m 刪除目前的電話號碼(步驟 S541)，並寫入所接收的新電話號碼至獨一資訊儲存單元 310m(步驟 S542)。

上面分別描述符合「第一、二、三要求」之每一模型變更系統。這些模型變更系統經由網際網路實施模型變更、合約取消或變更持用人。

然而，在符合「第一、二、三要求」之模型變更系統所運用的技術可被應用於不涉及網際網路連接之模型變更系統。即，不涉及網際網路連接之上面的模型變更系統 600e 可被構建以符合「第一、二、三要求」。類似地不涉及網際網路連接之模型變更系統 600g 可被構建以符合「第一、二、三要求」。

上面第四實施例之行動電話可被構建成在 SIM 卡內具有其獨一資訊儲存單元。在此情形中，於模型變更之際，使用者由行動電話 A 拆下 SIM 卡，並將由行動電話 A 拆下之 SIM 卡裝到行動電話 B。或者，在模型變更之際，該模型變更裝置可實施由行動電話 A 拆下 SIM 卡及將 SIM 卡裝到行動電話 B。

五、發明說明（67）

由上面描述明白的是，符合本發明之行動電話的內部儲存單元303一般而言其記憶體受限。慣常地，此限制的結果有下列的問題。在內部儲存單元充滿數位著作物時，使用者被要求刪除儲存在內部儲存單元之某些數位著作物以在購買另外的數位著作物前確保有自由記憶體空間，或者其只不過要放棄另外的數位著作物。

然而，依據本發明，使用者被允許在其決定在任何短時間內不使用數位著作物時將儲存於主要裝置(行動電話)之內部儲存區的某些數位著作物儲存至附裝於主要裝置的記錄媒體內。在此方式下，自由記憶體空間被確保於主要裝置之內部儲存區內而不致損失播放其所購買之這些數位著作物的權利。後果為該使用者被允許購買某些更多數位著作物以儲存至內部儲存區內。

進而言之，以此構造下，當一內容被加密且被儲存於裝在某主要裝置之記錄媒體時，已加密之內容不可能用特定主要裝置外之任何其他主要裝置被解密或播放雖然記錄媒體被裝於此。此即，達成符合版權持有人之要求的效果，使用某一行動電話儲存於記憶體卡內之內容被禁止用任何其他主要裝置被解密或播放，就算該記錄媒體被裝於此亦然。

再進而言之，本發明達成的效果為被提供某種使用狀況之內容僅在符合該使用狀況時被許可被播放。

再進而言之，本發明在模型由某一主要裝置之際達成效果。此即，已替換原先被使用之主要裝置的新主要裝置

五、發明說明（68）

被許可不須對該內容施用處理地讀取及播放用原始主要裝置購買並儲存在記錄媒體裝置內的內容。

現在描述符合本發明之第五實施例的數位著作物配銷系統 100i(未畫出)。

數位著作物配銷系統 100i 具有類似數位著作物配銷系統 100 之構造。因而，主要的是描述與數位著作物配銷系統 100 之差異。

數位著作物配銷系統 100i 包括行動電話 300i 與記憶體卡 400i 或記憶體卡 400p 分別替代行動電話 300 與記憶體卡 400。

使用者將記憶體卡 400i 或 400p 裝到行動電話 300i。

如第 27 圖顯示者，記憶體卡 400i 由一型式儲存單元 414、一認證單元 490、一第一外部儲存單元 412 與一第二外部儲存單元 411 組成。

型式儲存單元 414 預先儲存資訊顯示一第二型式為記憶體卡 400i 之型式。

認證單元 490 與包括於行動電話 300i 之認證單元 390 實施挑戰回應式的相互認證。

第二外部儲存單元 411 為一記憶體單元，其僅在認證單元 490 之認證已成功地被實施後被許可由另一端(即行動電話 300i)被讀取與被寫入。第二外部儲存單元 411 具有一儲存區用於儲存所加密的已連結之資訊，其將在稍後被描述。

如第 27 圖顯示者，記憶體卡 400p 由一型式儲存單元

五、發明說明（69）

415與一外部儲存單元410組成。

型式儲存單元415預先儲存資訊顯示一第一型式為記憶體卡400p之型式。

外部儲存單元410具有一儲存區用於儲存該已加密之內容。

此處，記憶體卡400i與記憶體卡400p不同之處在於記憶體卡400i具有認證單元，而記憶體卡400p不具有。

如第27圖顯示者，行動電話300i包括一第一加密/解密單元382與一第二加密/解密單元381取代行動電話300包括之加密/解密單元381。進而言之，行動電話300i包括一型式讀取單元301與認證單元390。至於其他方面，行動電話300i包括的元件類似於行動電話300者。

當記憶體卡400i或記憶體卡400p之一被裝到行動電話300i時，若為記憶體卡400i被裝，型式讀取單元391自記憶體卡400i之型式儲存單元414讀取該第二型式之資訊；若為記憶體卡400p被裝，型式讀取單元391自記憶體卡400p之型式儲存單元415讀取該第一型式之資訊。

型式讀取單元391輸出該等第一型式資訊或第二型式資訊，其任一個被讀取至控制單元366i。

控制單元366i自型式讀取單元391接收該等第一型式資訊或第二型式資訊。

在接收該第一型式資訊的情形中，控制單元366i指示第一加密/解密單元382以實施加密/解密處理。

在接收該等第二型式資訊的情形中，控制單元366i首

五、發明說明（70）

先指示認證單元390實施與記憶體卡400i之相互認證。在自認證單元390接收資訊表示認證成功之際，控制單元366i指示第二加密/解密單元381實施加密/解密處理。或者，在自認證單元390接收資訊表示認證不成功之際，控制單元366i終止該處理。

在自控制單元366i接收認證指令之際，認證單元390與記憶體卡400i之認證單元490實施挑戰回應式之相互認證，然後讀取資訊至控制單元366i顯示已實施之認證為成功或不成功。

第二加密/解密單元381具有類似加密/解密單元380b之構造。

此即，第二加密/解密單元381產生一標題鑰匙，並使用一獨一鑰匙將該標題鑰匙加密以產生一已加密之標題鑰匙。該第二加密/解密單元381亦使用該標題鑰匙將一內容加密以產生一已加密之內容。

此外，第二加密/解密單元381將自記憶體卡400i讀取之已加密的標題鑰匙解密以產生該標題鑰匙，然後使用所產生的標題鑰匙將自記憶體卡400i讀取的已加密之內容解密以產生該內容。

第一加密/解密單元382具有類似加密/解密單元380之構造。

此即，第一加密/解密單元382使用一獨一鑰匙將一內容加密以產生一已加密之內容。同樣地，加密/解密單元382使用一獨一鑰匙將自記憶體卡400p讀取之已加密之內

五、發明說明（71）

容解密以產生該內容。

現在參照第 28 圖顯示之流程圖描述數位著作物配銷系統 100i 之作業。

當記憶體卡 400i 或記憶體卡 400p 之一被裝到行動電話 300i 時，若為記憶體卡 400i 被裝，型式讀取單元 391 自記憶體卡 400i 之型式儲存單元 414 讀取該第二型式之資訊；若為記憶體卡 400p 被裝，型式讀取單元 391 自記憶體卡 400p 之型式儲存單元 415 讀取該第一型式之資訊。型式讀取單元 391 輸出所讀取的第一型式資訊或第二型式資訊至控制單元 366i(步驟 S351)。

在接收第一型式資訊之際(步驟 S352)，控制單元 366i 指示第一加密/解密單元 382 以實施加密/解密處理。在回應下，第一加密/解密單元 382 實施加密/解密處理(步驟 S358)。

另一方面，在接收第二型式資訊之際(步驟 S352)，控制單元 366i 首先指示認證單元 390 實施相互認證。在回應下，認證單元 390 認證記憶體卡 400i 之認證單元 490(步驟 S353)。當認證成功(步驟 S354)(是)時，認證單元 390 等候記憶體卡 400i 之認證單元 490 來認證該認證單元 390(步驟 S355)。當認證單元 490 之認證成功時(步驟 S356)(是)時，控制單元 366i 指示第二加密/解密單元 381 實施加密/解密處理。在回應下，第二加密/解密單元 381 實施加密/解密處理(步驟 S357)。

在步驟 S354 或步驟 S356 之認證不成功的情形中，控

五、發明說明（72）

制單元 366i 終止該處理。

如上述在第五實施例中，行動電話根據記憶體卡型式判斷裝於此之記憶體卡是否包括一認證單元。當判斷該記憶體卡包括一認證單元時，行動電話用第二加密/解密單元實施加密/解密處理。或者，當判斷該記憶體卡不包括一認證單元時，行動電話用第一加密/解密單元實施加密/解密處理。

現在描述符合本發明之第六較佳實施例的數位著作物配銷系統 100j(未畫出)。

數位著作物配銷系統 100j 具有類似數位著作物配銷系統 100c 之構造，因而主要描述者為與數位著作物配銷系統 100c 之差異。

數位著作物配銷系統 100j 包括一內容配銷伺服器裝置 200j、一行動電話 300i 與記憶體卡 400j 分別取代內容配銷伺服器裝置 200、行動電話 300 與記憶體卡 400。數位著作物配銷系統 100j 進一步包括一付款裝置(未畫出)。內容配銷伺服器裝置 200j 與付款裝置經由網際網路 10 彼此被連接。

如以第 29 圖為例顯示者，內容配銷伺服器裝置 200j 之內容儲存單元 201 包括一權利資訊表 610。

權利資訊表 610 具有數個儲存區用於儲存由使用者 ID 與使用權利資訊組成之使用資訊。使用者 ID 為用於辨識使用者之辨識元。

內容 ID 為用於辨識內容之辨識元。

五、發明說明（73）

使用權利資訊為使用者使用內容之權利。

如以第 30 圖為例顯示者，記憶體卡 400j 包括一第一外部儲存單元 412j 與一第二外部儲存單元 411j。

第一外部儲存單元 412j 具有一儲存區用於儲存一已加密之內容。第二外部儲存單元 411j 具有一儲存區用於儲存由內容 ID 與使用權利資訊組成之使用資訊。

注意，第二外部儲存單元 411j 僅在行動電話 300j 與記憶體卡 400j 被相互認證後為可讀取與可寫入的。

行動電話 300j 預先儲存使用辨識元者用於辨識行動電話 300j 之使用者。

數位著作物配銷系統 100j 之作業參照第 31 與 32 圖顯示之流程圖被描述。

首先描述為自內容配銷伺服器裝置 200j 獲取內容所實施之作業。

在自儲存單元 365 接收內容 ID 之際，行動電話 300j 之內容購買單元 301 傳輸內容 ID 與儲存於其內的使用者 ID 至內容配銷伺服器裝置 200j(步驟 S371)。

在接收使用者 ID 與內容 ID 之際(步驟 S371)，內容配銷伺服器裝置 200j 使用所接收的內容 ID 計算內容費用(步驟 S372)，並傳輸使用者 ID、內容 ID 與所計算的內容費用至付款裝置(步驟 S373)。

在接收使用者 ID、內容 ID 與內容費用之際(步驟 S373)，付款裝置為所接收的使用者 ID 辨識的使用者實施付款處理以依據所接收的內容費用進行付款(步驟 S374)，

五、發明說明（74）

並產生一付款憑證(步驟 S374)，及傳輸使用者 ID、內容 ID 與付款憑證至內容配銷伺服器裝置 200j(步驟 S375)。

在接收使用者 ID、內容 ID 與付款憑證之際(步驟 S375)，內容配銷伺服器裝置 200j 自內部儲存單元 201 讀取對應於所接收的內容 ID 之內容(步驟 S376)、為所讀取的內容產生該使用權利資訊(步驟 S377)、及寫入所接收的使用者 ID 與所產生的使用權利資訊相關之內容 ID 至在內部儲存單元 201 內被提供的權利資訊表 610 中(步驟 S378)。接著，內容配銷伺服器裝置 200j 傳輸讀取內容、所產生的使用權利資訊、與所接收的內容 ID 至行動電話 300j(步驟 S379)。

在接收該內容、使用權利資訊與內容 ID 之際(步驟 S379)，行動電話 300j 將所接收的內容加密並儲存該已加密之內容至包括於記憶體卡 400j 之第一外部儲存單元 412j(步驟 S380)。進而言之，行動電話 300j 寫入所接收的使用權利資訊與彼此相關的內容 ID 至包括於記憶體卡 400j 之第二外部儲存單元 411j。

接著，描述例如在使用者誤將儲存於記憶體卡 400j 之已加密之內容刪除的情形中重新獲取曾經獲取之內容的作業。

行動電話 300j 自包括於記憶體卡 400j 之第二外部儲存單元 411j 讀取內容 ID 與對應的使用權利資訊(步驟 S391)，並傳輸所讀取的內容 ID、使用權利資訊與使用者 ID 至內容配銷伺服器裝置 200j(步驟 S392)。

五、發明說明（75）

在接收使用者ID、內容ID與使用者權利資訊之際(步驟S392)，內容配銷伺服器裝置200j判斷權利資料表610是否包括與所接收的一組相同的使用者ID與內容ID組(步驟S393)。在判斷相同的使用者ID與內容ID在權利資訊表610出現(步驟S393)(是)時，內容配銷伺服器裝置200j自內部儲存單元201讀取對應於所接收的內容ID(步驟S394)，然後傳輸所讀取的內容至行動電話300j(步驟S395)。

在回應下，行動電話300j接收該內容(步驟S395)，將所接收的內容加密以寫入至記憶體卡400j內(步驟S396)。

或者，在判斷相同的使用者ID與內容ID未在權利資訊表610出現(步驟S393)(否)時，內容配銷伺服器裝置200j棄置所接收的使用者ID、內容ID與使用權利資訊，且不實施其他作業。

現在描述符合本發明第七較佳實施例之數位著作物配銷系統100k(未畫出)

數位著作物配銷系統100k具有類似數位著作物配銷系統100c之構造，因而主要描述者為與數位著作物配銷系統100c之差異。

數位著作物配銷系統100k包括一內容配銷伺服器裝置200k、一行動電話300k與記憶體卡400k分別取代內容配銷伺服器裝置200c、行動電話300c與記憶體卡400。

如以第33圖為例顯示者，數位著作物配銷系統200k之內部儲存單元201包括一內容資訊表620。

五、發明說明（76）

內容資訊表 620 包括數組內容資訊，每一組由內容 ID、對應的內容、與對應的獨一資訊之型式組成。

內容 ID 為用於辨識內容之辨識元。

該內容為一件音樂或電影之數位著作物。

該獨一資訊之型式顯示何種獨一資訊將被用以將被內容儲存於記憶體卡 400k 之際加以加密。如圖中顯示者，在此例中之獨一資訊型式顯示為「媒體獨一」型式或「裝置獨一」型式。

如第 34 圖顯示者，記憶體卡 400k 包括認證單元 490、一第一外部儲存單元 412k 與一第二外部儲存單元 411k。

第一外部儲存單元 412k 預先儲存對該記憶體卡 400k 為獨一的之媒體獨一資訊。進而言之，第二外部儲存單元 411k 具有儲存區用於儲存該獨一資訊型式與彼此相關的已加密之內容。

認證單元 490 實施與行動電話 300k 之認證單元 390 的挑戰回應式之相互認證。

如第 34 圖顯示者，行動電話 300k 包括一第一加密/解密單元 382 與一第三加密/解密單元 383 取代包括於行動電話 300 之加密/解密單元 380。行動電話 300k 進一步包括認證單元 390。針對此點，行動電話 300k 包括與行動電話 300 所包括的相同元件。

獨一資訊儲存單元 310 預先儲存裝置獨一資訊，其為實施對行動電話 300k 為獨一的資訊被產生。

認證單元 390 實施與記憶體卡 400k 之認證單元 490

五、發明說明（77）

的挑戰回應式相互認證，然後輸出資訊至控制單元 366k 顯示該認證為成功與否。

控制單元366k自認證單元390接收資訊表示該認證為成功與否。

在接收表示認證成功的資訊之際，控制單元366k選擇性地指示第一加密/解密單元382或第三加密/解密單元383實施加密/解密單元處理。此二加密/解密單元之選擇為依據該獨一資訊型式被完成。

第一加密/解密單元 382 具有類似加密/解密單元 380 之構造。

此即，第一加密/解密單元382使用該裝置獨一資訊將該內容加密以產生一已加密之內容。進而言之，第一加密/解密單元382使用裝置獨一資訊將已自記憶體卡400k讀取的已加密之內容解密。

第三加密/解密單元 383 讀取自包括於記憶體卡 400k 之第二外部儲存單元 411k 所儲存的媒體獨一資訊。

在加密之際，第三加密/解密單元383使用所讀取的媒體獨一資訊為鑰匙將該內容加密，並儲存與顯示「媒體獨一」型式的獨一資訊相關的已加密之內容至第一外部儲存單元 412 內。

在解密之際，第三加密/解密單元383使用所讀取的媒體獨一資訊為鑰匙以將已自第一外部儲存單元 412k 讀取的已加密之內容解密以產生該內容。

現在參照第 35 與 36 圖顯示之流程圖描述數位著作物

五、發明說明（78）

配銷系統 100k。

首先描述當行動電話 300k 獲取一內容並寫入該內容至記憶體卡 400k 時所實施的作業。

行動電話 300k 傳輸用於辨識將被獲取之內容的內容 ID 至內容配銷伺服器裝置 200k(步驟 S421)。內容配銷伺服器裝置 200k 自內容資訊表 620 擷取資訊，其具有與所接收的內容 ID 相同的內容 ID(步驟 S422)，並傳輸該內容與包括於所擷取的內容資訊的獨一資訊型式至行動電話 300k(步驟 S423)。

認證單元 390 實施與記憶體卡 400k 之相互認證(步驟 S424)。當相互認證成功地被實施(步驟 S425)(是)時，控制單元 366k 接收該內容與獨一資訊之型式。在判斷已接收之獨一資訊型式顯示「裝置獨一」型式時(步驟 S426)，控制單元 366k 實施第一加密/解密單元 382 實施加密處理。在回應下，第一加密/解密單元 382 自獨一資訊儲存單元 310 讀取該裝置獨一資訊(步驟 S427)，並自獨一資訊儲存單元 303 讀取該內容。然後第一加密/解密單元 382 使用該裝置獨一資訊為鑰匙將所讀取的內容加密(步驟 S428)，並儲存顯示「裝置獨一」型式之獨一資訊型式相關的已加密之內容至記憶體卡 400k 之第一外部儲存單元 412k 內(步驟 S429)。

或者，在判斷已接收之獨一資訊型式顯示「媒體獨一」型式時(步驟 S426)，控制單元 366k 實施第三加密/解密單元 383 實施加密處理。在回應下，第三加密/解密單元 383

五、發明說明（79）

自第二外部儲存單元 411k 讀取該媒體獨一資訊(步驟 S430)，並自獨一資訊儲存單元 303 讀取該內容。然後第三加密/解密單元 383 使用該媒體獨一資訊為鑰匙將所讀取的內容加密(步驟 S431)，並儲存顯示「媒體獨一」型式之獨一資訊型式相關的已加密之內容至記憶體卡 400k 之第一外部儲存單元 412k 內(步驟 S432)。

在記憶體卡與認證單元 390 間之相互認證失敗(步驟 S425)(否)時，該處理在此階段終止。

接著，描述當行動電話 300k 解密以播放於記憶體卡 400k 的已加密之內容所實施的處理。

行動電話 300k 之認證單元 390 實施與記憶體卡 400k 之相互認證(步驟 S411)。當該相互認證成功地被實施(步驟 S442)(是)時，讀取單元自包括於記憶體卡 400k 讀取該已加密之內容與獨一資訊型式，並輸出獨一資訊之型式至控制單元 366k(步驟 S443)。在接收獨一資訊型式之際，控制單元 366k 判斷所接收的型式資訊為「裝置獨一」型式或「媒體獨一」型式(步驟 S444)。在判斷該獨一資訊型式為「裝置獨一」時(步驟 S444)，控制單元 366k 指示第一加密/解密單元 382 實施解密處理(步驟 S445)。在回應下，第一加密/解密單元 382 自獨一資訊儲存單元 310 讀取該裝置獨一資訊(步驟 S445)，並自讀取單元 350 接收該已加密之內容。然後第一加密/解密單元 382 使用所讀取的裝置獨一資訊為鑰匙將該已加密之內容解密(步驟 S446)，並寫入該已解密之內容至內部儲存單元 303。然後，播放單元 304 播

五、發明說明（80）

放該內容(步驟 S447)。

或者，在判斷該獨一資訊型式為「媒體獨一」時(步驟 S444)，控制單元 366k 指示第三加密/解密單元 383 實施解密處理。在回應下，第三加密/解密單元 382 經由讀取單元 350 自包括於記憶體卡 400k 之第二外部儲存單元 411k 讀取該媒體獨一資訊(步驟 S448)，並自讀取單元 350 接收該已加密之內容。然後第三加密/解密單元 383 使用所讀取的媒體獨一資訊為鑰匙將該已加密之內容解密(步驟 S449)，並寫入該已解密之內容至內部儲存單元 303。然後，播放單元 304 播放該內容(步驟 S450)。

如上述者，本發明係被導向於用於記錄及播放內容(即數位著作物)之數位著作物保護系統，其由一主要裝置與可在該主要裝置裝卸之記錄媒體裝置組成。該主要裝置包括：一內部儲存區用於儲存一內容；一獨一資訊儲存區用於儲存對該主要裝置為獨一的之獨一資訊；一加密單元使用儲存於該內部儲存區之該獨一資訊為鑰匙將儲存於該內部儲存區之內容加密；一寫入單元寫入被加密單元加密之內容至該記錄媒體裝置；一讀取單元自該記錄媒體裝置讀取該已加密之內容；一解密單元將該讀取單元所讀取的該已加密之內容解密；以及一播放單元播放該內容。該記錄媒體裝置具有一外部儲存區用於儲存該已加密之內容，其被該主要裝置的寫入單元寫入或被該主要裝置的讀取單元讀取。

此處，主要裝置之加密單元使用該獨一資訊為鑰匙將

五、發明說明（81）

對該內容為獨一的之標題鑰匙加密，並使用該標題鑰匙將該內容加密。寫入單元寫入被加密單元加密的已加密之內容與已加密之標題鑰匙至記錄媒體裝置。該讀取單元自記錄媒體裝置讀取該已加密之內容與該已加密之標題鑰匙。該解密單元使用該獨一資訊將已加密之標題鑰匙解密，並使用該已解密之標題鑰匙將該已加密之內容解密。記錄媒體裝置儲存被主要裝置之寫入單元寫入或被主要裝置之讀取單元讀取的已加密之內容與已加密之標題鑰匙。

此處，該主要裝置進一步包括：一使用狀況儲存區與一使用狀況判斷單元。該使用狀況儲存區為該內容儲存使用狀況資料，及該使用狀況判斷單元依據該使用狀況資料判斷是否要播放該內容。

此處，該主要裝置進一步包括一認證單元。該記錄媒體裝置包括一認證單元。該內部儲存區包括一第一儲存區與一第二儲存區。在該主要裝置寫入該已加密之標題鑰匙至記錄媒體裝置內或該主要裝置自該記錄媒體裝置讀取該已加密之標題鑰匙前，主要裝置之認證單元認證該記錄媒體裝置且記錄媒體裝置之認證單元認證該主要裝置。當二認證作業均成功地被實施時，已加密之標題鑰匙的寫入或讀取被實施。記錄媒體裝置分別儲存該已加密之內容與該已加密之標題鑰匙至第一外部儲存區與第二外部儲存區內。

此處，主要裝置包括一使用狀況判斷單元，在主要裝置寫入內容之使用狀況資料至記錄媒體裝置內或該主要裝

五、發明說明（82）

置自記錄媒體裝置讀取該使用狀況資料前，該主要裝置之認證單元認證該記錄媒體裝置且該記錄媒體裝置之認證單元認證該主要裝置。當二種認證作業均成功時，該使用狀況之寫入或讀取被實施。該使用狀況判斷單元判斷是否要依據該使用狀況資料播放該內容。該記錄媒體裝置儲存該使用狀況資料至該第二外部儲存區內。

此處，該使用狀況資料包括用於限制播放內容的被許可次數之資訊、用於限制播放內容的被許可期間之資訊或用於限制播放內容的被許可時間總量之資訊。

此處，該主要裝置進一步包括一內容購買單元與一內容接收單元。該內容購買單元自外部來源購買一內容。該內容接收單元接收該已被購買之內容以儲存所接收的內容至內部儲存區中。

此處，該主要裝置進一步包括一內容判斷單元。該內容判斷單元判斷儲存於內部儲存單元之內容是否被許可用該獨一資訊被該加密單元加密及被該寫入單元寫入至該記錄媒體裝置內。

此處，該主要裝置進一步包括記錄媒體裝置判斷單元。該記錄媒體裝置判斷單元判斷裝於該主要裝置之記錄媒體裝置是否為被許可使用該獨一資訊以該加密單元將儲存於內部儲存區之內容加密及以該寫入單元將已加密之內容寫入至該記錄媒體裝置內。

此處，該獨一資訊儲存區與該使用狀況儲存區為針對特別被許可讀取或寫入獨一資訊與使用狀況資料之模型變

五、發明說明（83）

更裝置外的任何外部裝置受到寫入保護及讀取保護。

在另一層面，本發明被導向一主要裝置，記錄媒體裝置可在此被裝卸。該主要裝置包括：一內部儲存區儲存一內容；一獨一資訊儲存區儲存對該主要裝置為獨一的獨一資訊；一加密單元使用該獨一資訊將對該內容為獨一的之標題鑰匙加密及使用該標題鑰匙將該內容加密；一寫入單元寫入二者均被該加密單元加密之該已加密之內容與該已加密之標題鑰匙；一讀取單元自該記錄媒體裝置讀取該已加密之內容與該已加密之標題鑰匙；一讀取單元使用該獨一資訊將該已加密之標題鑰匙解密及使用該已解密之標題鑰匙將該已加密之內容解密；以及一播放單元播放該內容。

此處，該主要裝置進一步包括一認證單元。在該主要裝置寫入該已加密之標題鑰匙至記錄媒體裝置內或自該記錄媒體裝置讀取該已加密之標題鑰匙前，該主要裝置之認證單元實施與記錄媒體裝置之相互認證。該已加密之標題鑰匙的寫入或讀取僅在該相互認證成功時被實施。

在另一層面中，本發明被導向於一記錄媒體裝置可在一主要裝置裝卸。該記錄媒體裝置具有一外部儲存區用於儲存一已加密之內容與一已加密之標題鑰匙，其被該主要裝置之一寫入單元寫入或被該主要裝置之一讀取單元讀取。

此處，該記錄媒體裝置進一步包括一認證單元。在該主要裝置寫入該已加密之標題鑰匙至記錄媒體裝置內或自該記錄媒體裝置讀取該已加密之標題鑰匙前，該記錄媒體

五、發明說明（84）

裝置之認證單元實施與主要裝置之相互認證。該已加密之標題鑰匙僅在該相互認證時被寫入至該第二外部儲存區內。

在另一層面中，本發明包括一獨一資訊讀取/寫入單元特別許可自一第一主要裝置之獨一資訊儲存區讀取獨一資訊，並寫入所讀取的獨一資訊至一第二主要裝置之獨一資訊儲存單元內。

此處，該模型變更裝置進一步包括一使用狀況讀取/寫入單元特別被許可自該第一主要裝置之使用狀況儲存區讀取使用狀況資料以在假設該主要裝置與該主要裝置分離地均具有使用狀況儲存區時，寫入所讀取的使用狀況資料至該第二主要裝置之使用狀況儲存區。

此處，該模型變更裝置以規律性的基準或必要時經由一網路被連接至該主要裝置。該主要裝置進一步包括一模型變更資訊判斷單元判斷該模型變更資訊之認證。該模型變更裝置依據該主要裝置之合約狀況資料傳輸該模型變更資訊至該主要裝置。該主要裝置之模型變更資訊判斷單元判斷所接收的模型變更資訊之認證。該模型變更裝置進一步包括一獨一資訊讀取/寫入單元。當所接收的模型變更資訊之認證被模型變更判斷單元建立時，該獨一資訊讀取/寫入單元寫入包括於模型變更資訊且對該主要裝置為獨一的之獨一資訊至該主要裝置之獨一資訊儲存單元內，或刪除該獨一資訊。

此處，一第二記錄媒體裝置被裝到該主要裝置。該第

五、發明說明（85）

二記錄媒體裝置包括：一獨一資訊儲存區用於儲存該主要裝置之獨一資訊；及一單元用於將已被裝到該第一主要裝置之該第二記錄媒體裝置裝到該第二主要裝置。

在一數位著作物保護系統中，一主要裝置、一記錄媒體裝置及一模型變更裝置符合本發明，該主要裝置之內部儲存區的記憶體容量在大多數情形受到限制。因而慣常地，此限制的結果有下列的問題。此即，在內部儲存區充滿數位著作物時，使用者被要求刪除儲存在內部儲存區之某些數位著作物以在購買另外的數位著作物前確保有自由記憶體空間，或者其只不過要放棄另外的數位著作物。然而，依據本發明，使用者被允許在其決定在短時間內不使用數位著作物時將儲存於內部儲存區的某些數位著作物儲存至附裝於該主要裝置的記錄媒體裝置內。在此方式下，自由記憶體空間被確保於該主要裝置之內部儲存區內而不致損失播放其所購買之這些數位著作物的權利。後果為另一數位著作物可被購買。

進而言之，以此構造下，當一內容被加密且被儲存於裝在某主要裝置之記錄媒體時，已加密之內容不可能用特定主要裝置外之任何其他主要裝置被解密或播放，雖然記錄媒體被裝於此。此即，本發明達成符合版權持有人之要求的效果，使用某一主要裝置儲存於記錄媒體裝置內之內容被禁止用任何其他主要裝置被解密或播放，就算該記錄媒體被裝於此亦然。

再進而言之，本發明達成的效果為被提供某種使用狀

五、發明說明（86）

況之內容僅在符合該使用狀況時被許可被播放。

再進而言之，本發明在模型由某一主要裝置變更為另一主要裝置之際達成下列效果。此即，已替換原先被使用之主要裝置的新主要裝置被許可不須對該內容施用處理地讀取及播放用原始主要裝置購買並儲存在記錄媒體裝置內的內容。

到此為止，已描述與本發明相符之數位著作物配銷系統。然而不用說的是本發明不受限於上述的特定實施例。例如，下列的構造為可應用的。

在上面的實施例中，所描述者為運用行動電話之數位著作物配銷系統，但本發明不受限於此。例如取代行動電話可應用的為包括L型備妥之桌面型電話、可攜式資訊終端機、個人電腦、或如電視機之家用設備，其能用網際網路連接。

進而言之，其被描述內容配銷伺服器裝置200與行動電話300經由網際網路10、行動電話網路300與無線電基地點被連接。不過，此連接可用其他方式被完成。例如，內容配銷伺服器與可攜式終端機可用網際網路被連接。或者，該內容配銷伺服器裝置可被連接至一廣播裝置，使得包括內容之各種資訊以廣播波之形式被廣播。此處，如電視機之家用設備接收該廣播波，並自所接收的廣播波擷取各種資訊。

雖然DES加密法則在上述的實施例中被運用，可應用的加密法則不限於此。進而言之，雖然在上述實施例被使

五、發明說明（87）

用的獨一資訊為一個56位元之獨一鑰匙，其位元長度不限於此。

雖然在上述的實施例中內容係被儲存於記憶體卡內，但本發明不限於此。例如，該內容可被儲存於如光碟之記錄媒體內。

雖然在上述的實施例中整個內容被加密，將一部分的內容加密為可應用的。

在上面的實施例中，儲存於記憶體卡的已加密之內容係被主要裝置解密(在上面的實施例中即為行動電話)，且被儲存至主要裝置之內部儲存區中。然而，用主要裝置將儲存於記憶體卡的已加密之內容解密並以即時播放已解密之內容為可應用的。類似地，儲存在記憶體卡且被提供使用狀況之資訊可被主要裝置解密。當使用狀況判斷單元允許內容被使用時，已解密之內容可被播放單元即時播放。

在上面的實施例中，電話號碼被使用作為儲存於獨一資訊儲存單元之資訊。然而，本發明不限於此。例如，行動電話之序列號碼只要是為獨一的便可被使用。

在上面的實施例中，該使用狀況以內容基準在一內容上被提供。然而，本發明不限於此。使用狀況許可每月購買100件音樂伴唱資料為可應用的。在此情形中，例如當以月計基準之合約被取消時，該使用狀況單元禁止下個月重製儲存於主要裝置之記憶體卡或內部儲存區的內容。

在上面的實施例中，該內容或標題鑰匙總是使用獨一資訊被加密且儲存於記憶體卡內。然而，本發明不限於此。

五、發明說明（88）

為行動電話提供內容判斷單元亦為可應用的，故其可視該內容是要使用該獨一資訊將該內容本身或該標題鑰匙加密而為可選擇的。

在上面的實施例中，模型變更裝置將儲存於行動電話 A 之獨一資訊儲存區的獨一資訊移至行動電話 B 者。然而，本發明不限於此。例如，該模型變更裝置可被構建以移動儲存於該主要裝置之內部儲存區的已購買之內容。

除了該內容外，該行動電話可自內容配銷伺服器裝置獲取內容判斷資訊以儲存至內部儲存區內。此處，該內容判斷資訊顯示該內容是否被許可使用該獨一資訊事先被加密且被寫入至記憶體卡內。

該行動電話可進一步包括該內容判斷單元。該內容判斷單元判斷在內部被儲存之內容是否被許可使用該獨一資訊事先被加密單元加密並被該寫入單元寫入至該記憶體卡內。當該內容為內容判斷單元判斷為被許可的時，該加密單元實施加密。當該內容為內容判斷單元判斷為被許可的時，該寫入單元實施寫入。

記憶體卡可進一步預先儲存型式資訊顯示該記憶體卡之型式。更明確地說，此處所使用之記憶體卡型式顯示依據記憶體卡之外形的型式、依據為連接行動電話所運用之拓樸的型式、依據製造商的型式、依據記憶體容量的型式、依據資訊儲存方法的型式、或依據存取方法的型式。進而言之，該型式資訊顯示該記憶體卡是否被許可使用獨一資訊以加密單元將儲存於行動電話的內容加密及以該寫入單

五、發明說明（89）

元寫入該已加密之內容至該記憶體卡。

該行動電話進一步包括該記錄媒體裝置判斷單元。該記錄媒體裝置判斷單元依據儲存於該記憶體卡之型式資訊判斷裝於行動電話之記憶體卡是否為被許可使用獨一資訊以加密單元將儲存於行動電話的內容加密及以該寫入單元寫入該已加密之內容至該記憶體卡之記憶體卡。

當判斷該內容被記錄媒體裝置判斷單元許可時，該加密單元將該內容加密。當判斷該內容被記錄媒體裝置判斷單元許可時，該寫入單元寫入該內容至該記憶體卡。

本發明可被實施為如上述之方法或用電腦實作上面之方法的電腦程式、甚或代表上面電腦程式之數位信號。

進而言之，本發明可被實施為儲存該電腦程式或該數位信號之電腦可讀取的媒體。此處，該電腦可讀取的媒體例如為磁碟片、硬碟，CD-ROM，MO，DVD，DVD-ROM，DVD-RAM，BD(Blu-ray 碟)，或半導體記憶體。或者，本發明可為儲存於如上之記錄媒體的電腦程式或數位信號。

進而言之，本發明可被實施為經由電信網路、有線或無線通信線路、或以網際網路為例的網路之類被傳輸的電腦程式或數位信號。

再進而言之，本發明可被實施為被提供微處理器與儲存上述電腦程式之記憶體的電腦系統，使得該微處理器依照該程式作業。

再進而言之，電腦程式或數位信號可被記錄於上面任何記錄媒體且被傳送至其他位置。或者該等電腦程式或數

五、發明說明（90）

位信號可經由上面任何網路被傳輸。此後，該等電腦程式或數位信號可被另一獨立的電腦系統執行。

進而言之，本發明可被實施成上面修改之組合。

雖然本發明已參照附圖以舉例的方式完全地被描述，其將被注意各種變更與修改對習知本技藝者為明白的。所以，除非這類變更與修改偏離本發明之領域，其應被構建成被包括於其內。

【圖式簡單說明】

第 1 圖為一方塊圖，顯示一數位著作物配銷系統 100 之整個構造；

第 2 圖為一方塊圖，顯示一內容配銷伺服器裝置 200 之構造；

第 3 圖為一方塊圖，顯示一行動電話 300 與一記憶體卡 400 之構造；

第 4 圖為一流程圖，顯示該數位著作物配銷系統 100 之作業；

第 5 圖為一方塊圖，顯示一記憶體卡 400b 之構造；

第 6 圖為一方塊圖，顯示一行動電話 300b 之構造；

第 7 圖為一流程圖，顯示被行動電話 300b 實施之作業以產生一已加密之內容及寫入該已加密之內容至該記憶體卡 400b 內；

第 8 圖為一流程圖，顯示被行動電話 300b 實施之作業以自該記憶體卡 400b 讀取該已加密之內容及產生該內容；

第 9 圖顯示被行動電話 A 及行動電話 X 實施以播放該

五、發明說明（91）

內容之作業；

第 10 圖為一方塊圖，顯示一行動電話 300c 與該記憶體卡 400 之構造；

第 11 圖為一流程圖，顯示行動電話 300c 之作業；

第 12 圖為一流程圖，顯示當該使用狀況為被許可之播放期間時行動電話 300c 的作業；

第 13 圖為一流程圖，顯示當該使用狀況為被許可之播放時間總量時行動電話 300c 的作業；

第 14 圖為一方塊圖，顯示一記憶體卡 400d 之構造；

第 15 圖為一方塊圖，顯示一行動電話 300d 之構造；

第 16 圖為一方塊圖，顯示一加密/解密單元 380d 之構造；

第 17 圖為一流程圖，顯示一數位著作物配銷系統 100d 之整個作業；

第 18 圖為一流程圖，顯示行動電話 300d 與記憶體卡 400d 間被實施之相互認證的作業；

第 19 圖為一流程圖，顯示被行動電話 300d 為儲存處理實施之作業；

第 20 圖為一流程圖，顯示被行動電話 300d 為讀取處理實施之作業；

第 21 圖為一方塊圖，顯示一模型變更系統 600e 之構造；

第 22 圖為一流程圖，顯示該模型變更系統 600e 之作業；

五、發明說明（92）

第 23 圖為一方塊圖，顯示一模型變更系統 600g 之構造；

第 24 圖為一方塊圖，顯示一模型變更系統 600m 之構造；

第 25 圖為一流程圖，顯示該模型變更系統 600m 之作業；

第 26 圖為一流程圖，顯示被修改的模型變更系統 600m 之作業；

第 27 圖為一方塊圖，顯示一行動電話 300i 與一記憶體卡 400i 之構造；

第 28 圖為一流程圖，顯示一數位著作物配銷系統 100i 之作業；

第 29 圖顯示被儲存於一內容配銷伺服器裝置 200j 之內容儲存單元 201 內的權利資訊表 610 之資料構造；

第 30 圖為一方塊圖，顯示一記憶體卡 400j 之構造；

第 31 圖為一流程圖，顯示被實施以自該內容配銷伺服器裝置 200j 獲取一內容之作業；

第 32 圖為一流程圖，顯示當一使用者錯將儲存於記憶體卡 400j 的已加密之內容刪除時用於再獲取該曾已獲取之內容的作業；

第 33 圖顯示被儲存於一內容配銷伺服器裝置 200k 之內容儲存單元 201 內的一內容資訊表 620 的資料構造；

第 34 圖為一方塊圖，顯示一行動電話 300k 與一記憶體卡 400k 之構造；

五、發明說明（93）

第35圖為一流程圖，顯示被行動電話300k實施以獲取一內容及寫入所獲取的內容至記憶體卡 400k 內之作業；以及

第36圖為一流程圖，顯示被行動電話300k實施以將儲存於記憶體卡400k內的一已加密之內容解密及播放該已解密之內容的作業。

【主要元件符號說明】

元件編號	譯名	元件編號	譯名
10	網際網路	300B	行動電話
20	行動電話網路	300C	行動電話
30	無線電基地台	300b	行動電話
40	閘道裝置	300c	行動電話
100	數位著作物配銷系統	300d	行動電話
100c	數位著作物配銷系統	300e	行動電話
100d	數位著作物配銷系統	300f	行動電話
100i	數位著作物配銷系統	300g	行動電話
100j	數位著作物配銷系統	300h	行動電話
100k	數位著作物配銷系統	300i	行動電話
200	內容配銷伺服器裝置	300j	行動電話
200c	內容配銷伺服器裝置	300k	行動電話
200d	內容配銷伺服器裝置	300m	行動電話
200j	內容配銷伺服器裝置	300n	行動電話
200k	內容配銷伺服器裝置	301	內容購買單元
201	內容儲存單元	302	內容獲取單元

五、發明說明（94）

202	控制單元	303	內部儲存單元
203	傳輸/接收單元	304	播放單元
300	行動電話	305	使用狀況儲存單元
300A	行動電話	305g	使用狀況儲存單元
305h	使用狀況儲存單元	342d	解密單元
306	使用狀況判斷單元	343	解密單元
310	獨一資訊儲存單元	343d	解密單元
310e	獨一資訊儲存單元	344	分割單元
310f	獨一資訊儲存單元	350	讀取單元
310g	獨一資訊儲存單元	351	讀取單元
310h	獨一資訊儲存單元	352	讀取單元
310m	獨一資訊儲存單元	360m	判斷單元
320	加密單元	360n	判斷單元
321	標題鑰匙產生單元	361	傳輸/接收單元
321d	標題鑰匙產生單元	362	音頻控制單元
322	加密單元	363	擴音器
322d	加密單元	364	麥克風
323	加密單元	365	輸入單元
323d	加密單元	366	控制單元
324	連接單元	366i	控制單元
330	寫入單元	366k	控制單元
331	寫入單元	367	天線
332	寫入單元	368	顯示器單元
340	解密單元	380	加密/解密單元

五、發明說明（95）

341	解密單元	380b	加密/解密單元
342	解密單元	380d	加密/解密單元
381	加密/解密單元	500	模型變更裝置
382	加密/解密單元	500m	模型變更裝置
383	加密/解密單元	501	資訊讀取單元
390	認證單元	502	資訊寫入單元
391	型式讀取單元	505	傳輸/接收單元
400	記憶體卡	600	模型變更系統
400b	記憶體卡	600e	模型變更系統
400d	記憶體卡	600g	模型變更系統
400i	記憶體卡	600m	模型變更系統
400j	記憶體卡	601	內容
400k	記憶體卡	602	已加密之內容
400p	記憶體卡	610	權利資訊表
410	外部儲存單元	620	內容資訊表
411	外部儲存單元	650	個人電腦
411j	外部儲存單元	415	型式儲存單元
411k	外部儲存單元	490	認證單元
412	外部儲存單元		
412j	外部儲存單元		
412k	外部儲存單元		
414	型式儲存單元		

A5
B5

四、中文發明摘要（發明之名稱：數位著作物保護系統、記錄/播放裝置、記錄媒體裝置、及模型變更裝置）

所揭示者為由一主要裝置與一記錄媒體裝置組成之系統。該主要裝置包括：一接收單元自一外部配銷伺服器接收數位著作物；一內部儲存區用於讀取該數位著作物；一播放單元播放該數位著作物；一獨一資訊儲存區用於儲存對該主要裝置為獨一的資訊；一加密單元使用該獨一資訊將該數位著作物加密；一解密單元使用該獨一資訊將已由該記錄媒體裝置被讀取之已加密的數位著作物解密；一寫出單元將已加密之數位著作物寫出至可攜帶式的記錄媒體裝置內；以及一讀取單元自該記錄媒體裝置讀取該已加密之數位著作物。

英文發明摘要（發明之名稱：DIGITAL WORK PROTECTION SYSTEM, RECORD/PLAYBACK DEVICE, RECORDING MEDIUM DEVICE, AND MODEL CHANGE DEVICE）

Disclosed is a system composed of a main device and a recording medium device. The main device includes: a reception unit that receives a digital work from an external distribution server; an internal storage area for storing the digital work; a playback unit that plays back the digital work; a unique information storage area for storing information that is unique to the main device; an encryption unit that encrypts the digital work using the unique information; a decryption unit that decrypts, using the unique information, the encrypted digital work having been read from the recording medium device; a write unit that writes the encrypted digital work into the recording medium device which is portable; and a read unit that reads the encrypted digital work from the recording medium device.

六、申請專利範圍

第91114091號申請案申請專利範圍修正本 97.11.27.

1. 一種記錄/播放裝置，用於把數位作品記錄在一可攜式記錄媒體裝置上並播放數位作品，該可攜式記錄媒體裝置包括：用於與和該可攜式記錄媒體裝置相連接的一裝置進行相互認證的第二認證單元；以及儲存單元，它具有第一儲存區域和第二儲存區域，第一儲存區域用於儲存資訊，而第二儲存區域只可由一個與其確立了相互認證的裝置來讀取及寫入，該記錄/播放裝置包括：

內部儲存單元，用來儲存作爲數位作品的內容；

獨一資訊儲存單元，用來預先儲存該記錄/播放裝置特有的裝置獨一資訊；

加密單元，用來產生該內容特有的標題鑰匙，利用該裝置獨一資訊對該標題鑰匙進行加密，以便產生加密的標題鑰匙，利用該所產生的標題鑰匙對該內容進行加密，以便產生加密內容，並產生包括該加密標題鑰匙和該加密內容的該加密資訊；

寫入單元，用來把該所產生的由該加密標題鑰匙和該加密內容組成的加密資訊寫入該記錄媒體裝置的該儲存單元；

讀取單元，用來從該記錄媒體裝置的該儲存單元中讀取由該加密標題鑰匙和該加密內容組成的該加密資訊；

解密單元，用來利用該裝置獨一資訊作為鑰匙，對

[5]

六、申請專利範圍

包含在該讀取的加密資訊中的該加密標題鑰匙進行解密，以便產生解密的標題鑰匙，並利用該解密標題鑰匙作為鑰匙，對包含在該讀取的加密資訊中的該加密內容進行解密，以便產生解密內容；

播放單元，用來播放該所產生的解密內容；以及

第一認證單元，用來在該寫入單元把該加密資訊寫入該記錄媒體裝置的儲存單元之前，或在該讀取單元從該記錄媒體裝置的儲存單元中讀取該加密資訊之前，執行與該記錄媒體裝置的該第二認證單元的相互認證，其中：

該寫入單元把該加密內容寫入該第一儲存區域，並且只有當該第一認證單元確立該相互認證時，才把該加密標題鑰匙寫入該第二儲存區域；以及

該讀取單元從該第一儲存區域中讀取該加密內容，並且只有當該第一認證單元確立該相互認證時，才從該第二儲存區域中讀取該加密標題鑰匙。

2. 如申請專利範圍第 1 項之記錄/播放裝置，其中還包括：

狀況儲存單元，用來儲存表示該內容的使用許可狀況的使用狀況資訊；以及

狀況判斷單元，用來根據該使用狀況資訊來判斷是否允許使用該內容。

3. 如申請專利範圍第 2 項之記錄/播放裝置，其中：

該寫入單元只有當該第一認證單元確立該相互認證時，才從該狀況儲存單元中讀取該使用狀況，並把

[5]

六、申請專利範圍

該讀取的使用狀況資訊寫入該第二儲存區域；

該讀取單元只有當該第一認證單元確立該相互認證時，才從該第二儲存區域中讀取該使用狀況，並把該讀取的使用狀況寫入該使用狀況儲存單元；以及

該狀況判斷單元根據儲存在該狀況儲存單元中的該使用狀況資訊，來判斷是否允許使用該內容。

4. 如申請專利範圍第 3 項之記錄/播放裝置，其中：

儲存在該狀況儲存單元中的該使用狀況資訊表明允許播放次數、允許播放時段、允許總播放時間、允許複製該內容的次數、或允許移動該內容的次數；以及

該狀況判斷單元：(i)只有當該播放單元實際播放該內容的次數等於或小於該允許播放次數、該播放單元要播放該內容的日期和時間在該允許播放時段內、以及實際播放的總時間等於或小於該允許總播放時間時，才判定播放該內容；(ii)只有當該允許複製該內容的次數等於或大於 1 時，才判定把該內容複製到該記錄媒體裝置；以及(iii)只有當該允許移動該內容的次數等於或大於 1 時，才判定把該內容移到該記錄媒體裝置。

5. 如申請專利範圍第 2 項之記錄/播放裝置，其中：

該獨一資訊儲存單元和該狀況儲存單元這兩者對任何外部裝置都具有被讀取及寫入保護，除非該外部裝置被特別允許讀取或寫入該獨一資訊及該使用狀況

六、申請專利範圍

資訊。

6. 如申請專利範圍第 1 項之記錄/播放裝置，其中還包括：

認證判斷單元，用來判斷該記錄媒體裝置是否包括該第二認證單元，其中：

當判定該記錄媒體裝置不包含該第二認證單元時，該加密單元還利用該裝置獨一資訊作為鑰匙，對該內容進行加密，以便產生該加密資訊；

當判定該記錄媒體裝置不包含該第二認證單元時，該寫入單元還把該所產生的加密資訊寫入該記錄媒體裝置的該儲存單元；

當判定該記錄媒體裝置不包含該第二認證單元時，該讀取單元還從該記錄媒體裝置的該儲存單元中讀取該加密資訊；以及

當判定該記錄媒體裝置不包含該第二認證單元時，該解密單元還利用該裝置獨一資訊作為鑰匙，對該讀取的加密資訊解密。

7. 如申請專利範圍第 1 項之記錄/播放裝置，其中還包括：

內容購買單元，用來通過向外部源發送對該內容付費的支付資訊來購買該內容；以及

內容接收單元，用來接收已購買的該內容，並把該接收的內容寫入該內部儲存單元。

8. 如申請專利範圍第 1 項之記錄/播放裝置，其中還包括：

內容判斷單元，用來判斷儲存在該內部儲存單元中的內容是否為具有預先接收的許可的該內容，其中該

[5]

六、申請專利範圍

許可是該加密單元根據該裝置獨一資訊對該內容進行加密以及該寫入單元把該內容寫入該記錄媒體裝置的許可，其中：

當該內容判斷單元判定該內容具有該許可時，該加密單元執行該加密；以及

當該內容判斷單元判定該內容具有該許可時，該寫入單元執行該寫入操作。

9. 如申請專利範圍第1項之記錄/播放裝置，其中還包括：

記錄媒體裝置判斷單元，用來判斷連接到該記錄/播放裝置的記錄媒體裝置是否為具有預先接收的許可的該記錄媒體裝置，其中該許可是該加密單元根據該裝置獨一資訊對儲存在該內部儲存單元中的該內容進行加密以及該寫入單元把該加密資訊寫入該記錄媒體裝置的許可，其中：

當該記錄媒體裝置判斷單元判定該記錄媒體裝置具有該許可時，該加密單元執行該加密；以及

當該記錄媒體裝置判斷單元判定該記錄媒體裝置具有該許可時，該寫入單元執行該寫入操作。

10. 如申請專利範圍第1項之記錄/播放裝置，其中：

該記錄媒體裝置還預先儲存該記錄媒體裝置特有的媒體獨一資訊；

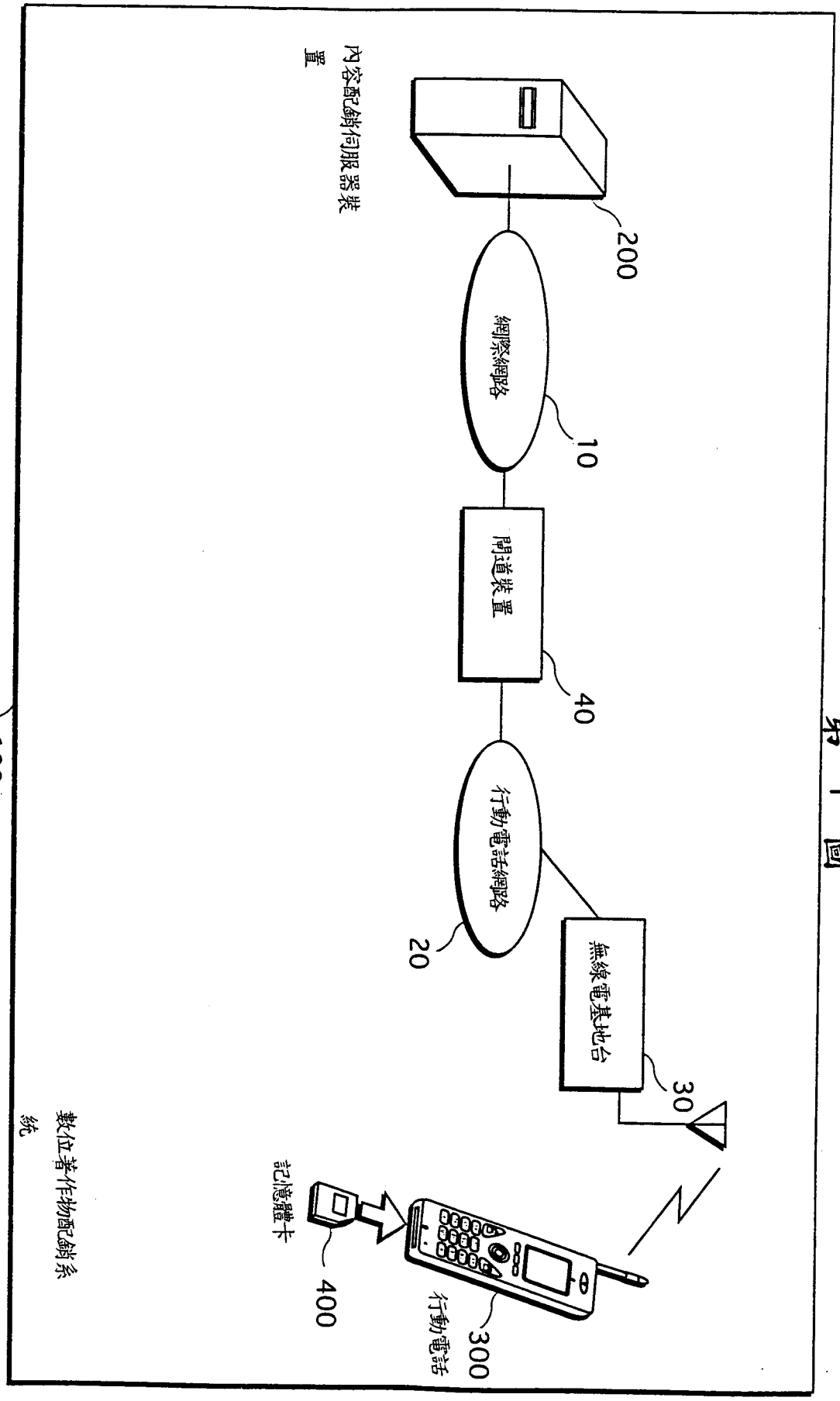
該內部儲存單元儲存與該內容有關的獨一資訊類型，該獨一資訊類型表示該內容係根據該裝置獨一資訊還是根據該媒體獨一資訊被加密；

六、申請專利範圍

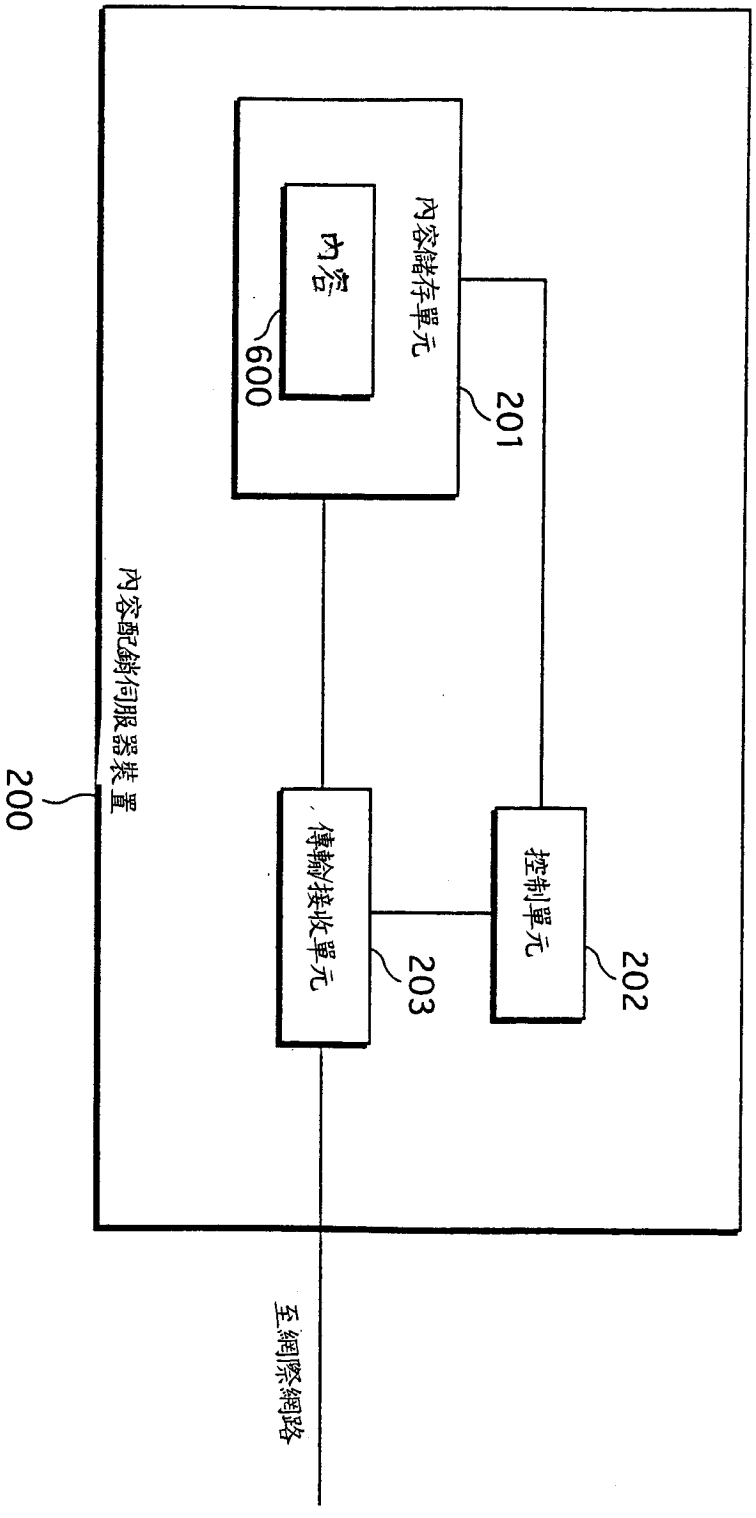
該記錄/播放裝置還包括獨一資訊判斷單元，用來根據儲存在該內部儲存單元中的該獨一資訊類型，判定該內容係根據該裝置獨一資訊還是根據該媒體獨一資訊被加密；

該加密單元：(i)在該獨一資訊判斷單元判定該內容是根據該裝置獨一資訊被加密時，根據該裝置獨一資訊對該內容進行加密，以便產生該加密資訊；以及(ii)在該獨一資訊判斷單元判定該內容是根據該媒體獨一資訊被加密時，從該記錄媒體裝置中讀取該媒體獨一資訊，以便根據該讀取的媒體獨一資訊對該內容進行加密，產生該加密資訊；以及

該解密單元：(i)在該獨一資訊判斷單元判定該內容係根據該裝置獨一資訊被加密時，根據該裝置獨一資訊對該讀取的加密資訊進行解密，以便產生該解密內容；以及(ii)在該獨一資訊判斷單元判定該內容係根據該裝置獨一資訊被加密時，從該記錄媒體裝置中讀取該媒體獨一資訊，以便利用該讀取的媒體獨一資訊對該讀取的加密資訊進行解密，產生該解密內容。

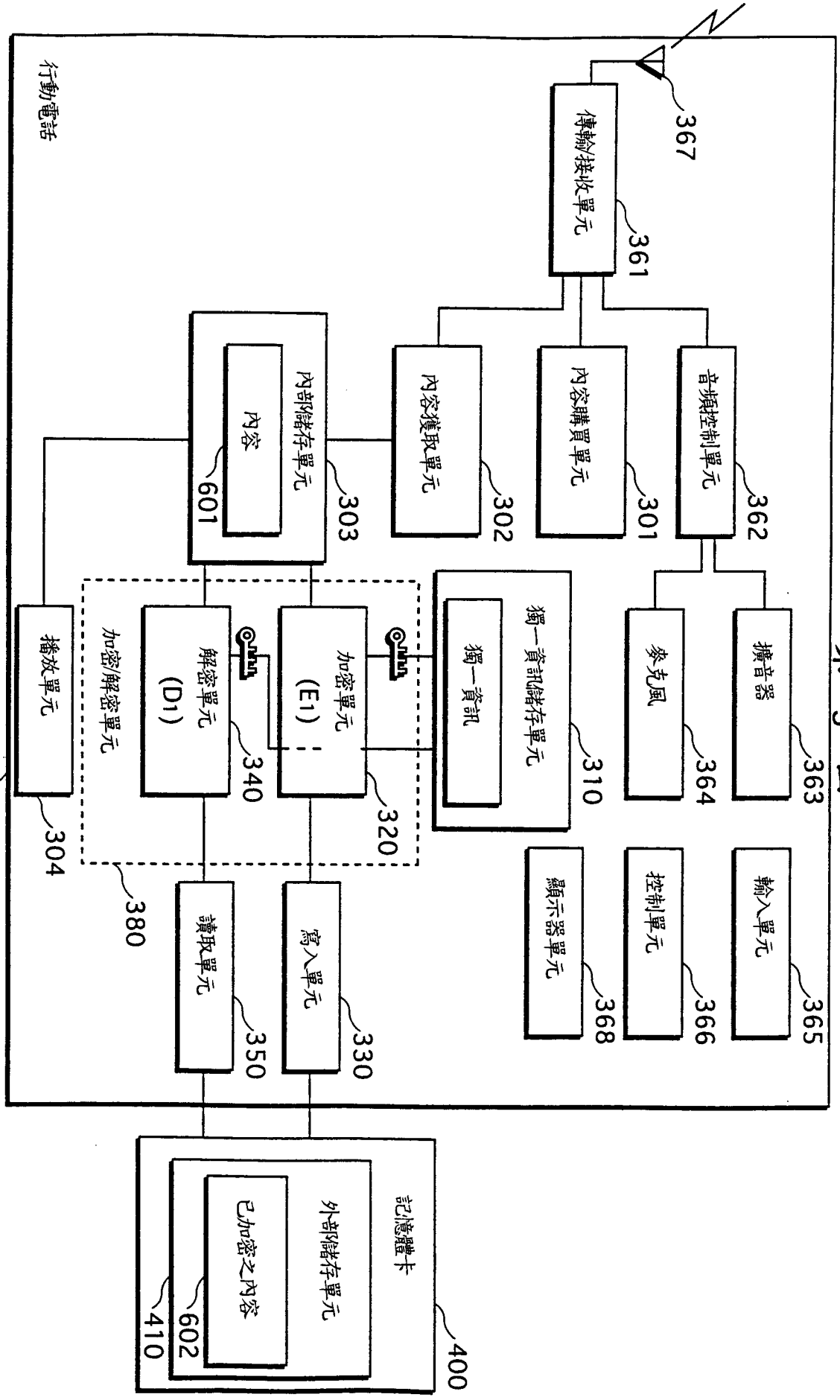

數位著作物配銷系統
100
內容配銷伺服器裝置
200
網際網路
10
閘道裝置
40
行動電話網路
20
無線電基地台
30
行動電話
300
記憶體卡
400

第1圖

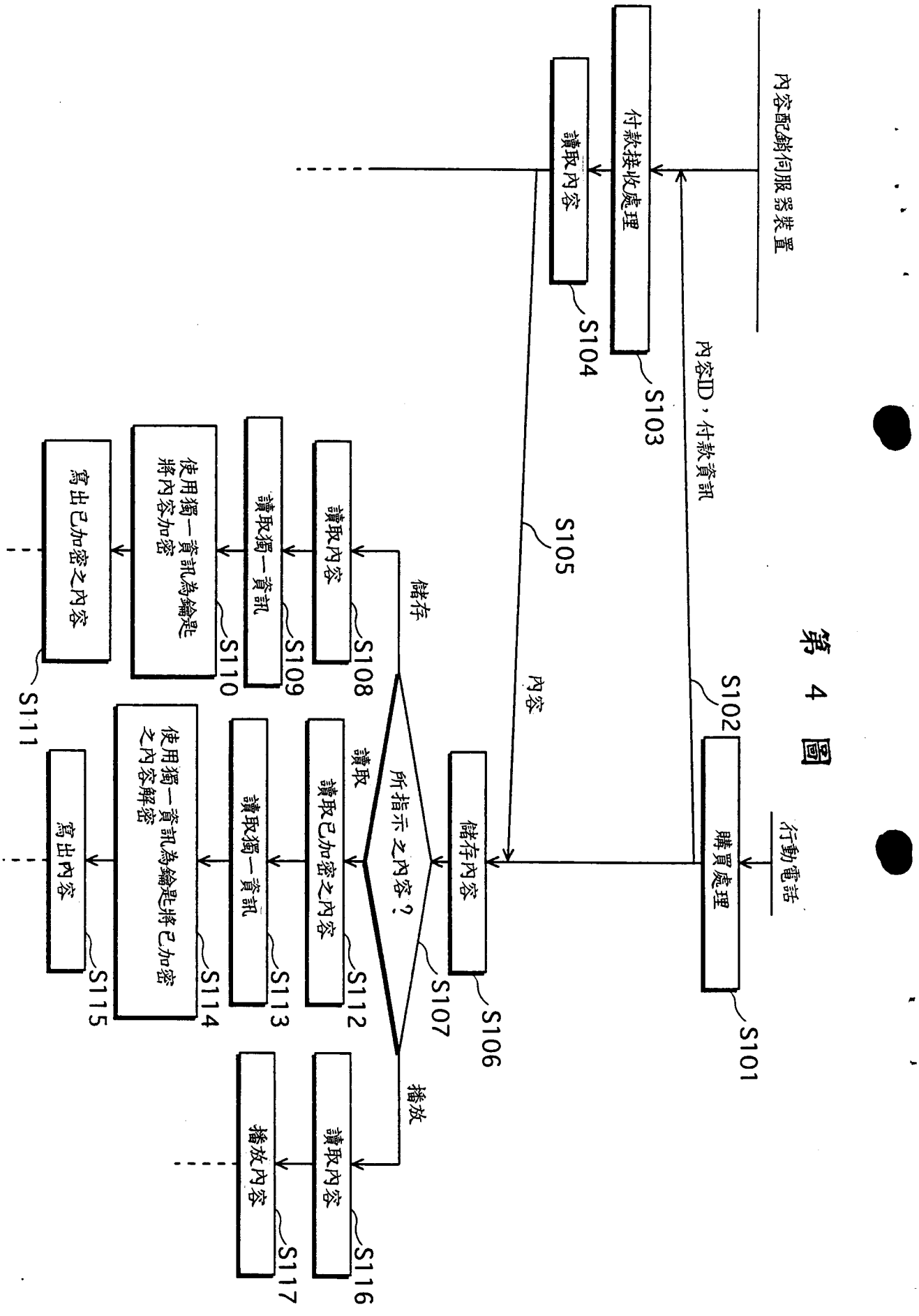


第 2 圖

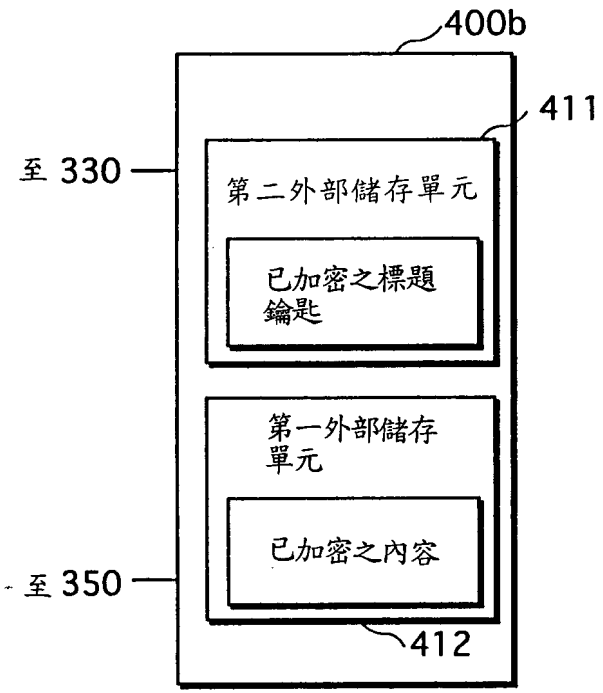
第 3 圖


行動電話
367
傳輸接收單元
361
音頻控制單元
362
內容購買單元
301
內容獲取單元
302
內部儲存單元
303
內容
601
擴音器
363
參克風
364
獨一資訊儲存單元
310
獨一資訊
輸入單元
365
控制單元
366
顯示器單元
368
播放單元
304
加密解密單元
380
解密單元
(D1)
340
加密單元
(E1)
320
寫入單元
330
讀取單元
350
300
記憶體卡
400
外部儲存單元
已加密之內容
602
410

第 4 圖

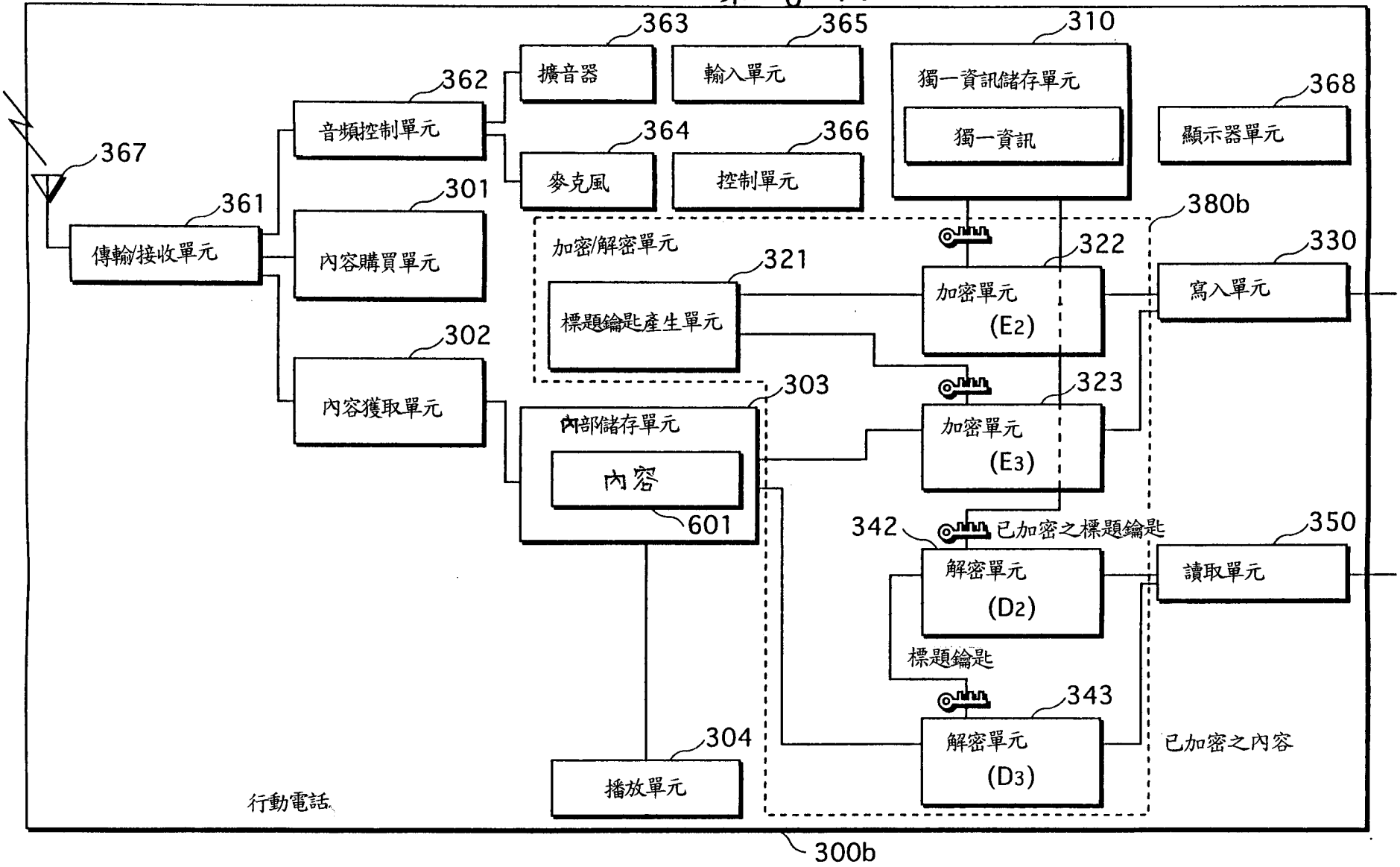

行動電話
內容配銷伺服器裝置
購買處理
S101
S102
內容ID，付款資訊
付款接收處理
S103
讀取內容
S104
內容
S105
儲存內容
S106
所指示之內容？
S107
儲存
讀取內容
S108
讀取獨一資訊
S109
使用獨一資訊為鑰匙將內容加密
S110
寫出已加密之內容
S111
讀取
讀取已加密之內容
S112
讀取獨一資訊
S113
使用獨一資訊為鑰匙將已加密之內容解密
S114
寫出內容
S115
播放
讀取內容
S116
播放內容
S117

第 5 圖

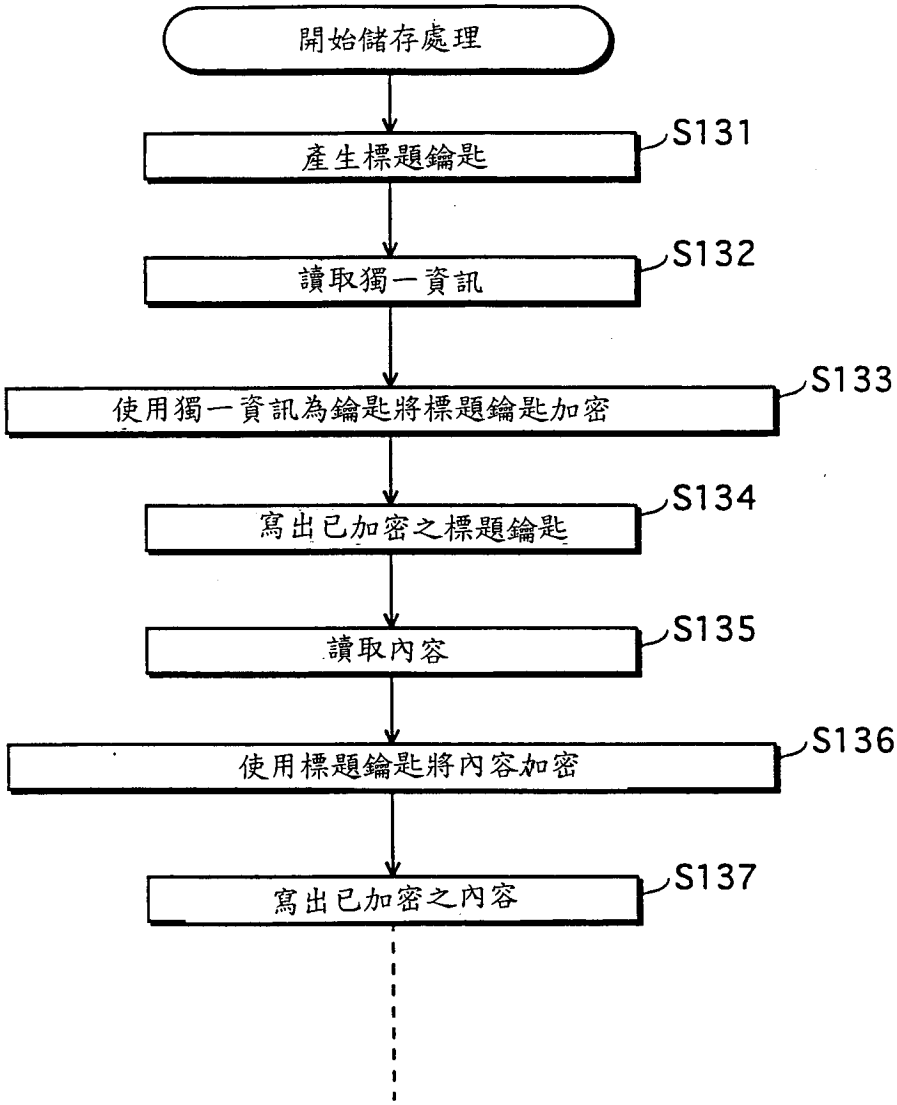


I308306

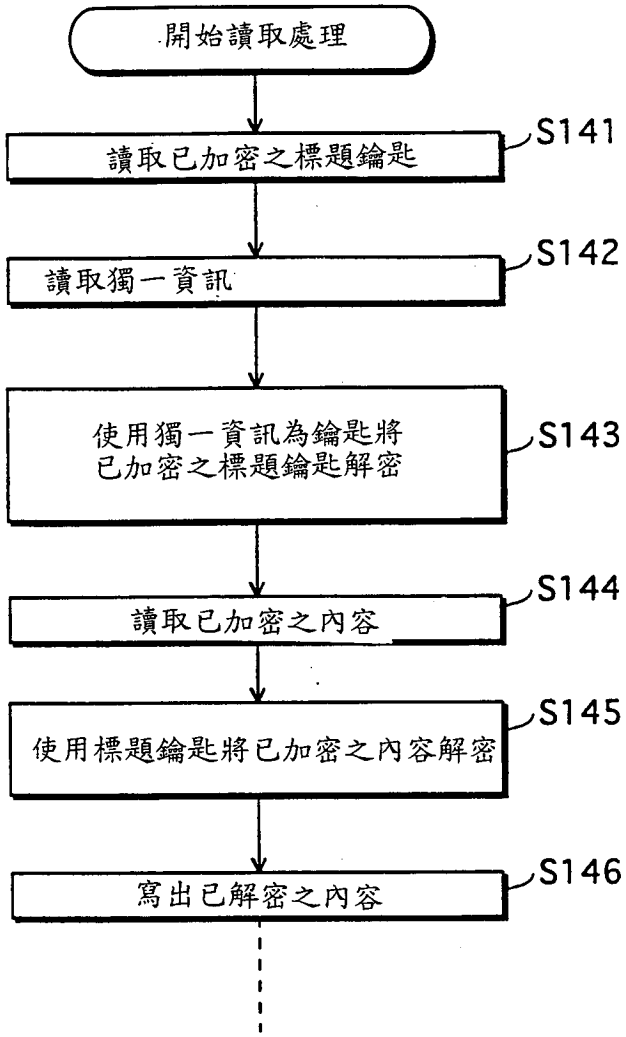
第 6 圖


363
365
310
擴音器
輸入單元
獨一資訊儲存單元
362
368
音頻控制單元
獨一資訊
顯示器單元
364
366
367
麥克風
控制單元
301
361
380b
加密/解密單元
傳輸/接收單元
內容購買單元
321
322
330
標題鑰匙產生單元
加密單元
(E2)
寫入單元
302
內容獲取單元
303
323
內部儲存單元
加密單元
(E3)
內容
601
342
已加密之標題鑰匙
350
解密單元
(D2)
讀取單元
標題鑰匙
343
304
解密單元
(D3)
已加密之內容
播放單元
行動電話
300b

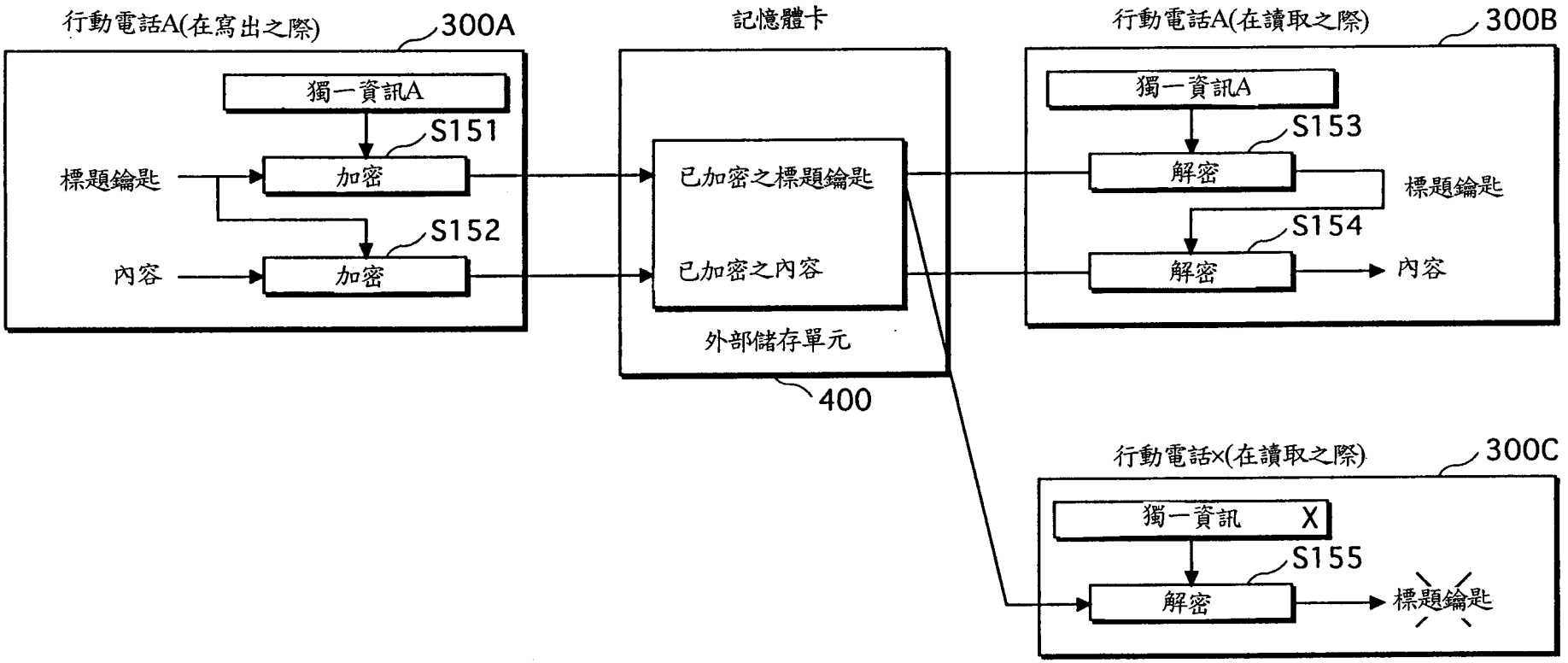
第 7 圖


開始儲存處理
產生標題鑰匙
S131
讀取獨一資訊
S132
使用獨一資訊為鑰匙將標題鑰匙加密
S133
寫出已加密之標題鑰匙
S134
讀取內容
S135
使用標題鑰匙將內容加密
S136
寫出已加密之內容
S137

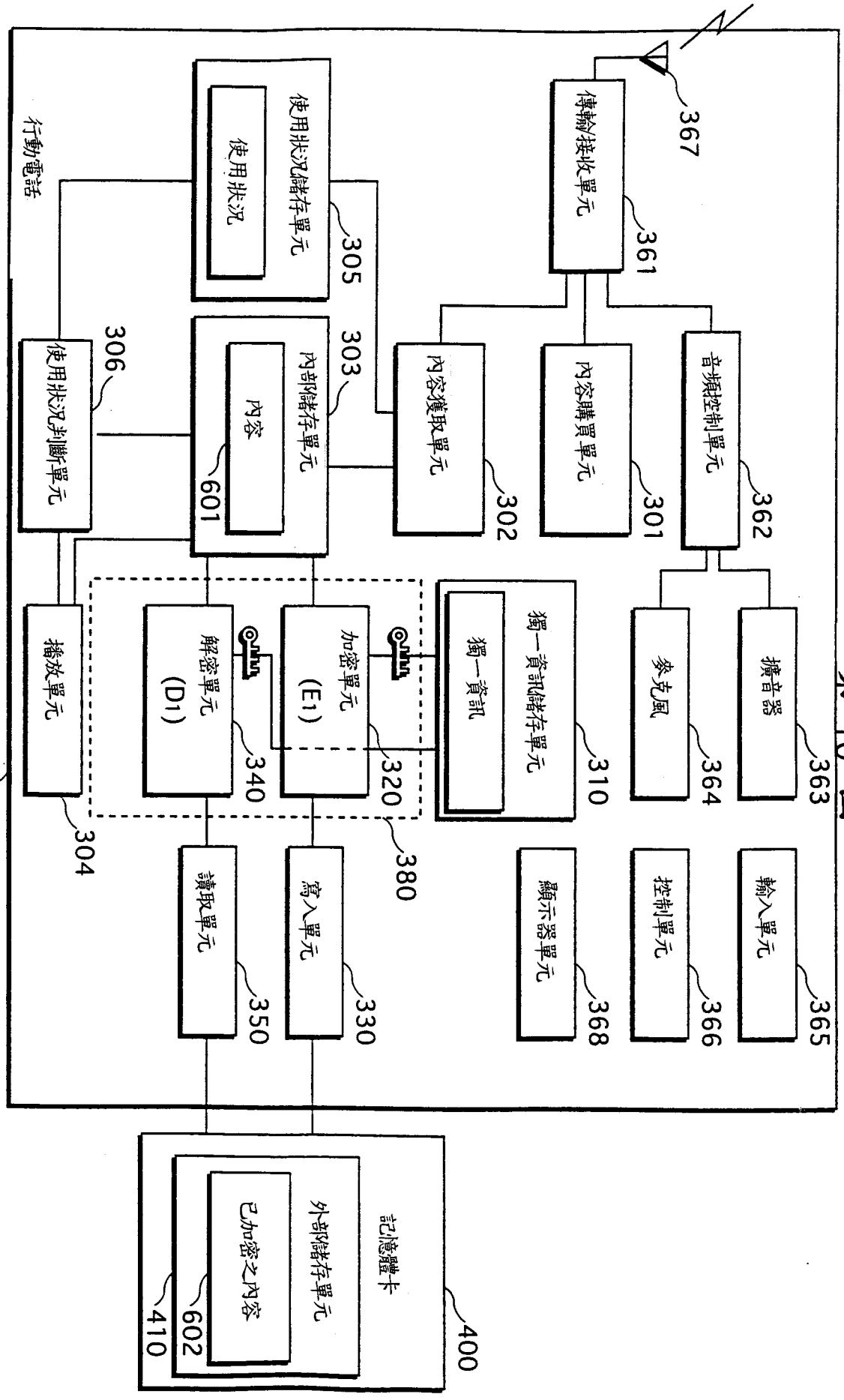
第 8 圖


開始讀取處理
讀取已加密之標題鑰匙
S141
讀取獨一資訊
S142
使用獨一資訊為鑰匙將
已加密之標題鑰匙解密
S143
讀取已加密之內容
S144
使用標題鑰匙將已加密之內容解密
S145
寫出已解密之內容
S146

第 9 圖

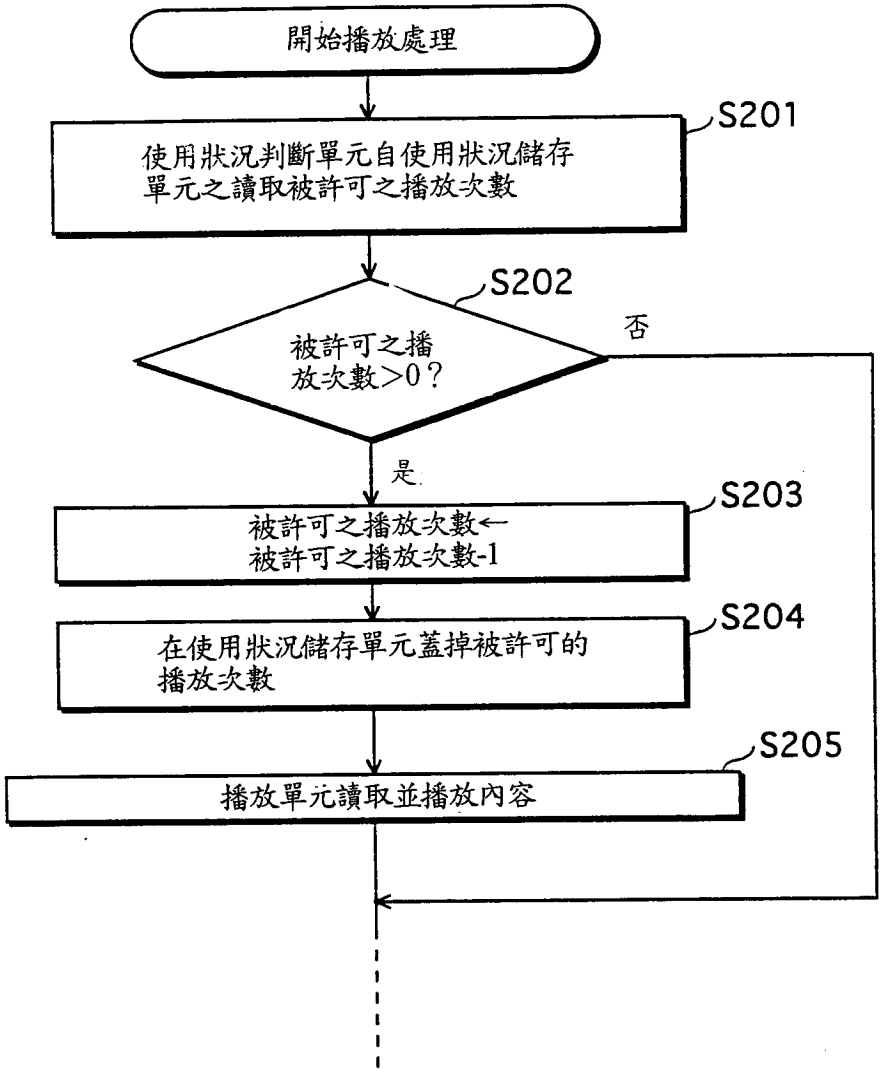

行動電話A(在寫出之際)
300A
獨一資訊A
S151
標題鑰匙
加密
S152
內容
加密
記憶體卡
已加密之標題鑰匙
已加密之內容
外部儲存單元
400
行動電話A(在讀取之際)
300B
獨一資訊A
S153
解密
標題鑰匙
S154
解密
內容
行動電話x(在讀取之際)
300C
獨一資訊 X
S155
解密
標題鑰匙

I308306

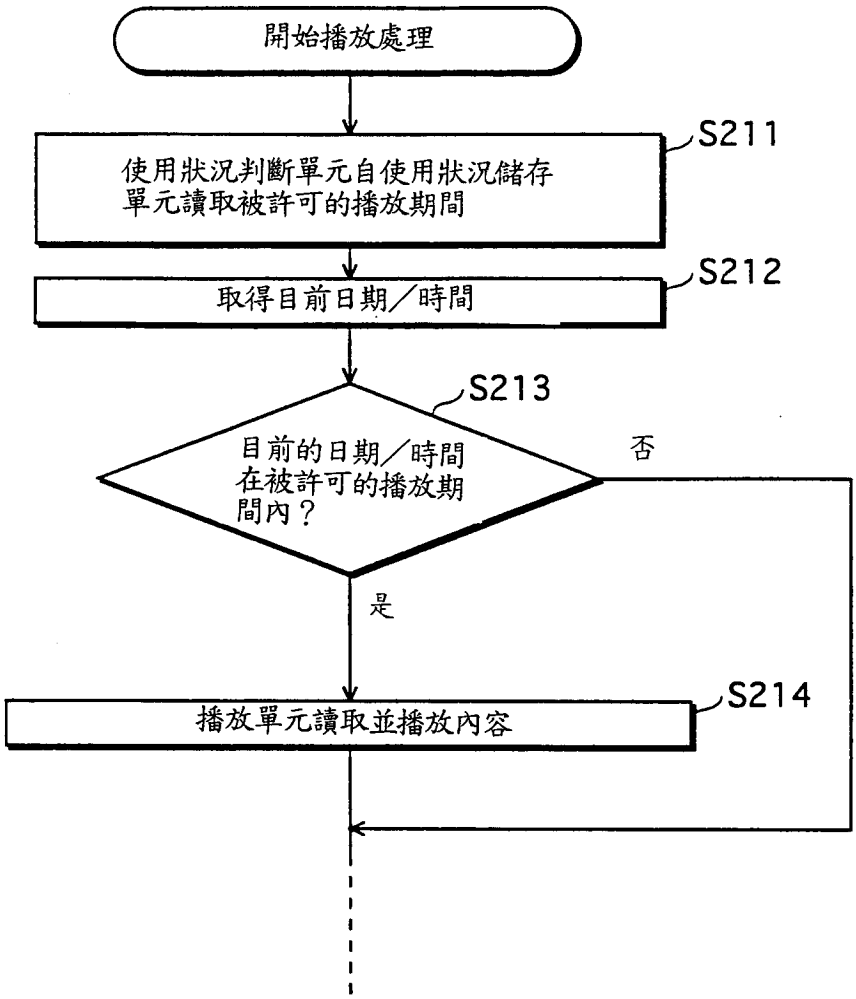

行動電話
300c
367
傳輸接收單元
361
音頻控制單元
362
擴音器
363
輸入單元
365
參克風
364
控制單元
366
內容購買單元
301
內容獲取單元
302
獨一資訊儲存單元
310
獨一資訊
顯示器單元
368
使用狀況儲存單元
305
使用狀況
內部儲存單元
303
內容
601
使用狀況判斷單元
306
播放單元
304
解密單元
(D1)
340
加密單元
(E1)
320
380
讀取單元
350
寫入單元
330
記憶體卡
400
外部儲存單元
410
已加密之內容
602

第 10 圖

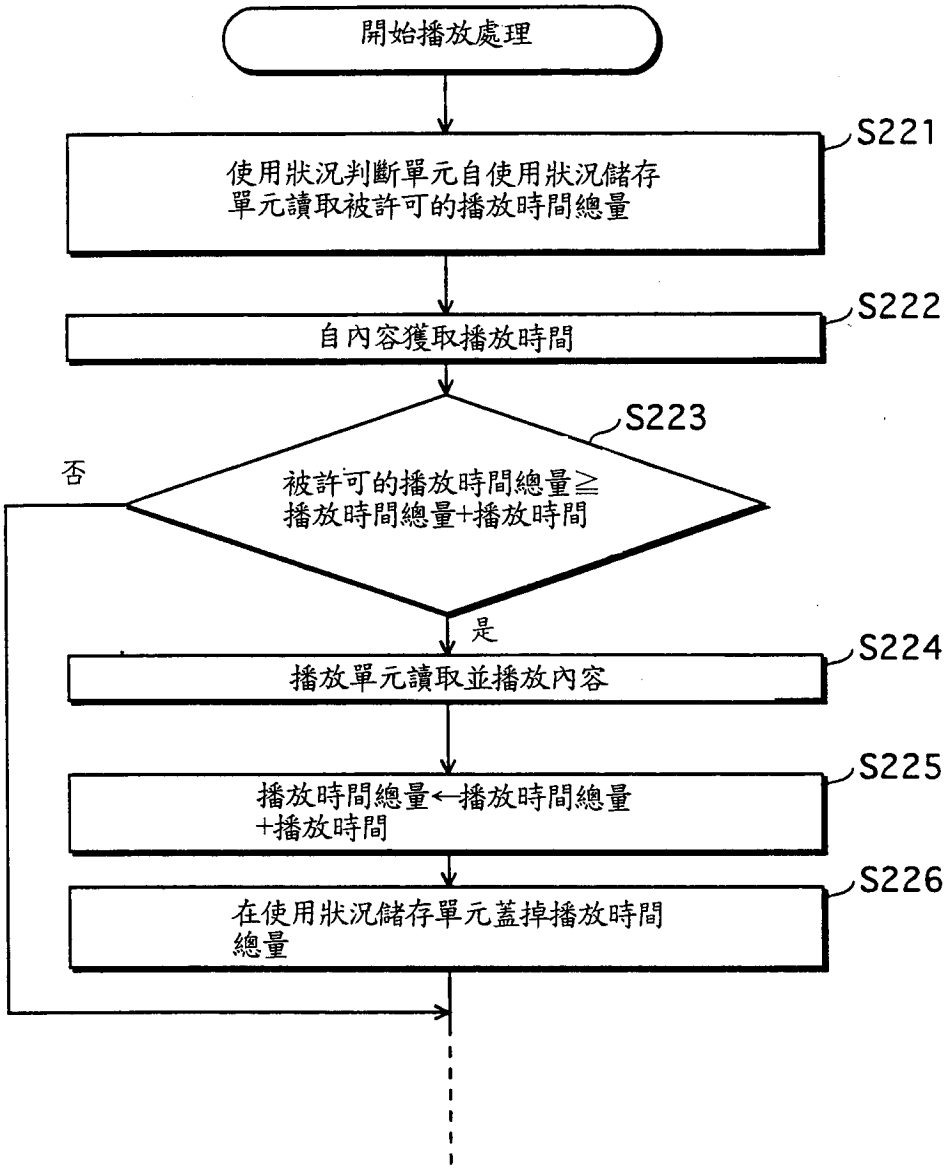
第 11 圖

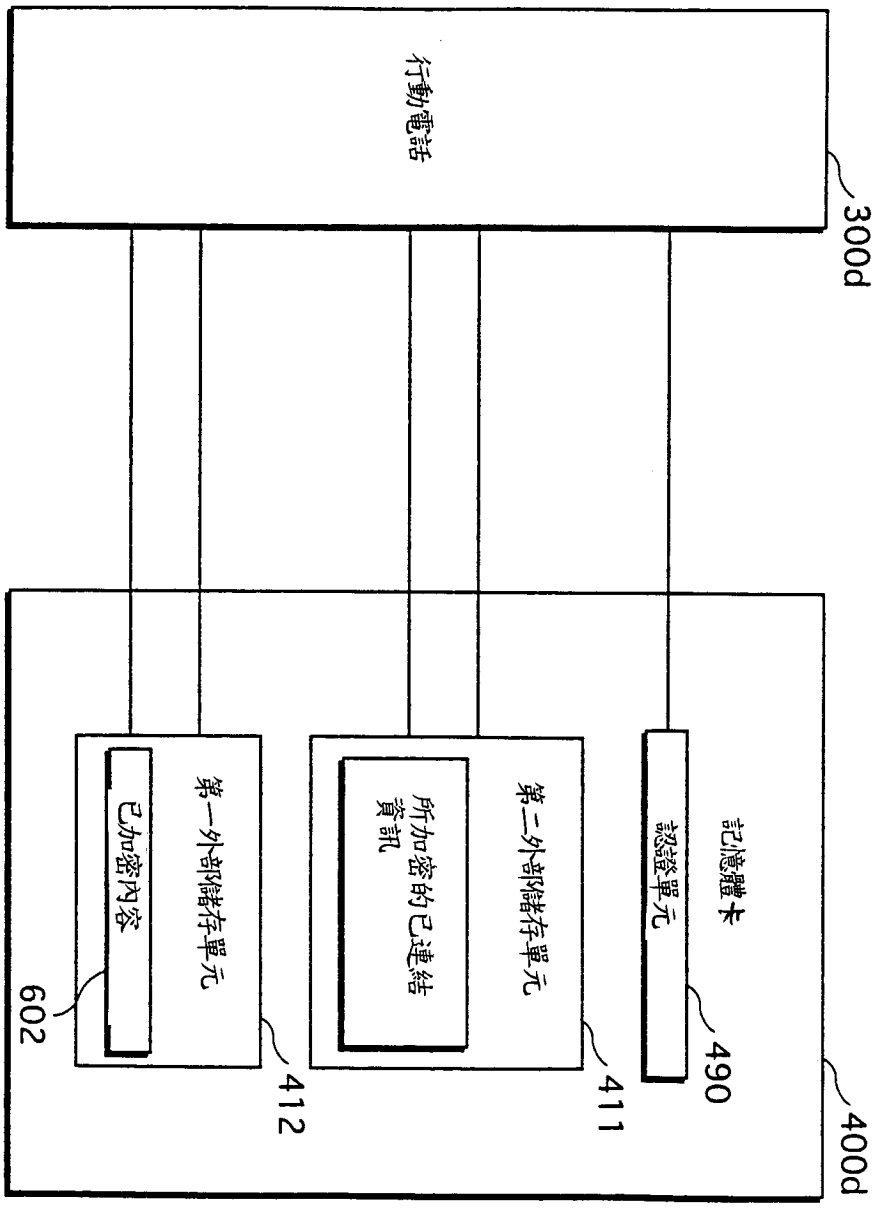

開始播放處理
S201
使用狀況判斷單元自使用狀況儲存單元之讀取被許可之播放次數
S202
被許可之播放次數>0？
否
是
S203
被許可之播放次數←被許可之播放次數-1
S204
在使用狀況儲存單元蓋掉被許可的播放次數
S205
播放單元讀取並播放內容

第 12 圖

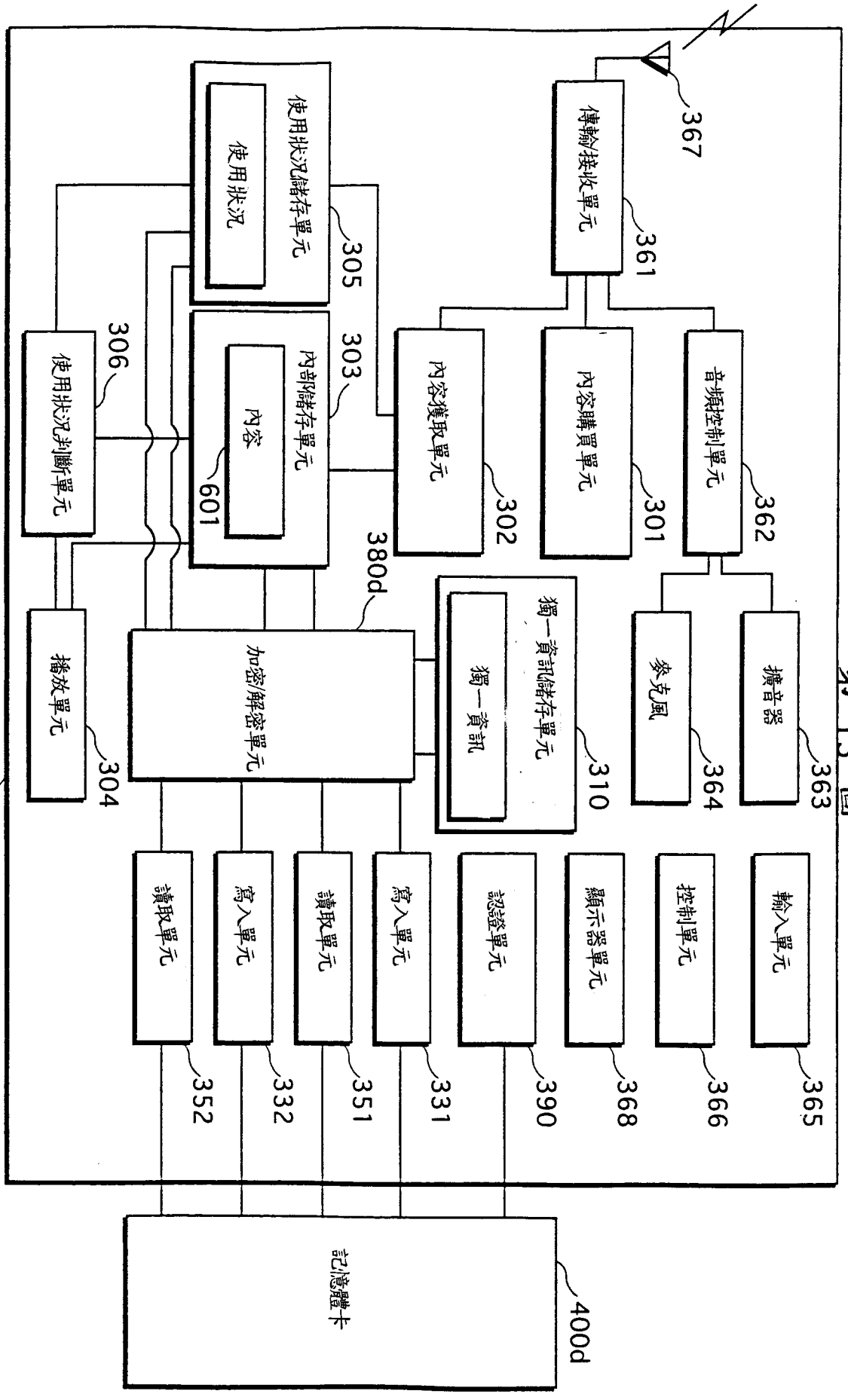

開始播放處理
使用狀況判斷單元自使用狀況儲存單元讀取被許可的播放期間
S211
取得目前日期／時間
S212
目前的日期／時間在被許可的播放期間內？
S213
否
是
播放單元讀取並播放內容
S214

第 13 圖

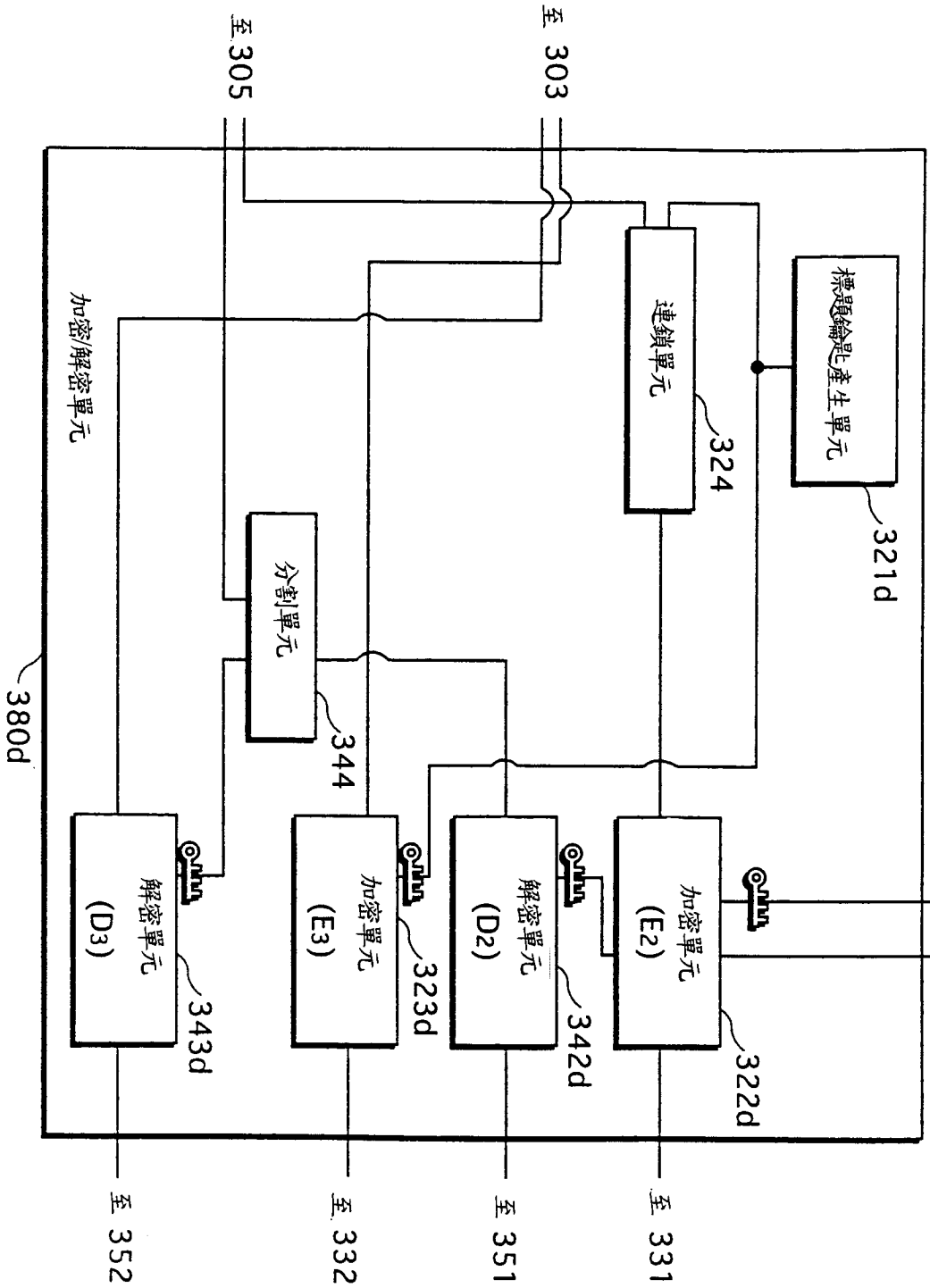

開始播放處理
使用狀況判斷單元自使用狀況儲存單元讀取被許可的播放時間總量
S221
自內容獲取播放時間
S222
被許可的播放時間總量≧播放時間總量+播放時間
S223
否
是
播放單元讀取並播放內容
S224
播放時間總量←播放時間總量+播放時間
S225
在使用狀況儲存單元蓋掉播放時間總量
S226


行動電話
300d
記憶體卡
認證單元
490
第二外部儲存單元
所加密的已連結資訊
411
第一外部儲存單元
已加密內容
602
412
400d

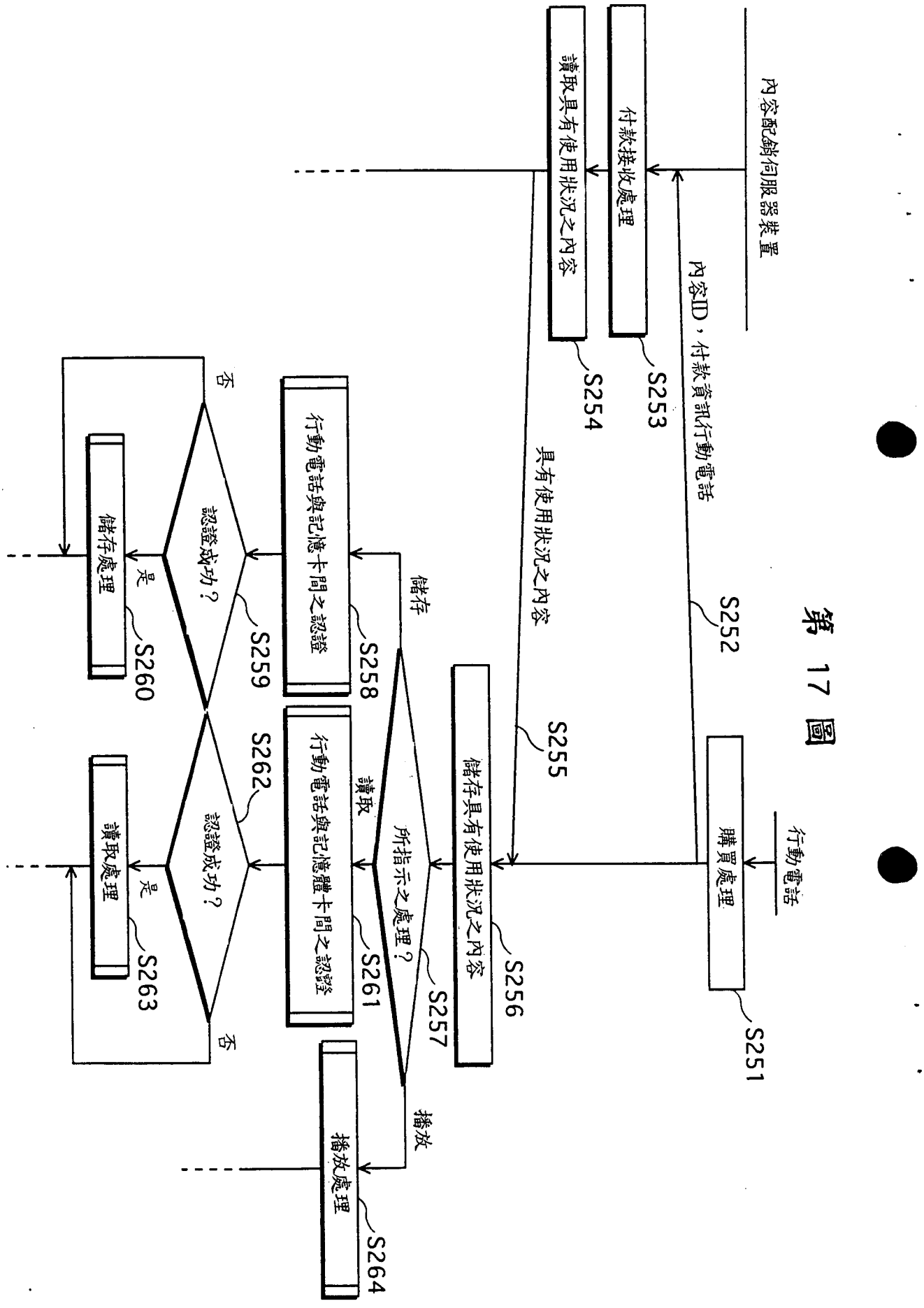
第 14 圖


367
傳輸接收單元
361
使用狀況儲存單元
使用狀況
305
內部儲存單元
內容
601
303
使用狀況判斷單元
306
播放單元
304
300d
音頻控制單元
362
內容購買單元
301
內容獲取單元
302
380d
加密/解密單元
獨一資訊儲存單元
獨一資訊
310
擴音器
363
麥克風
364
輸入單元
365
控制單元
366
顯示器單元
368
認證單元
390
寫入單元
331
讀取單元
351
寫入單元
332
讀取單元
352
記憶體卡
400d

第 15 圖

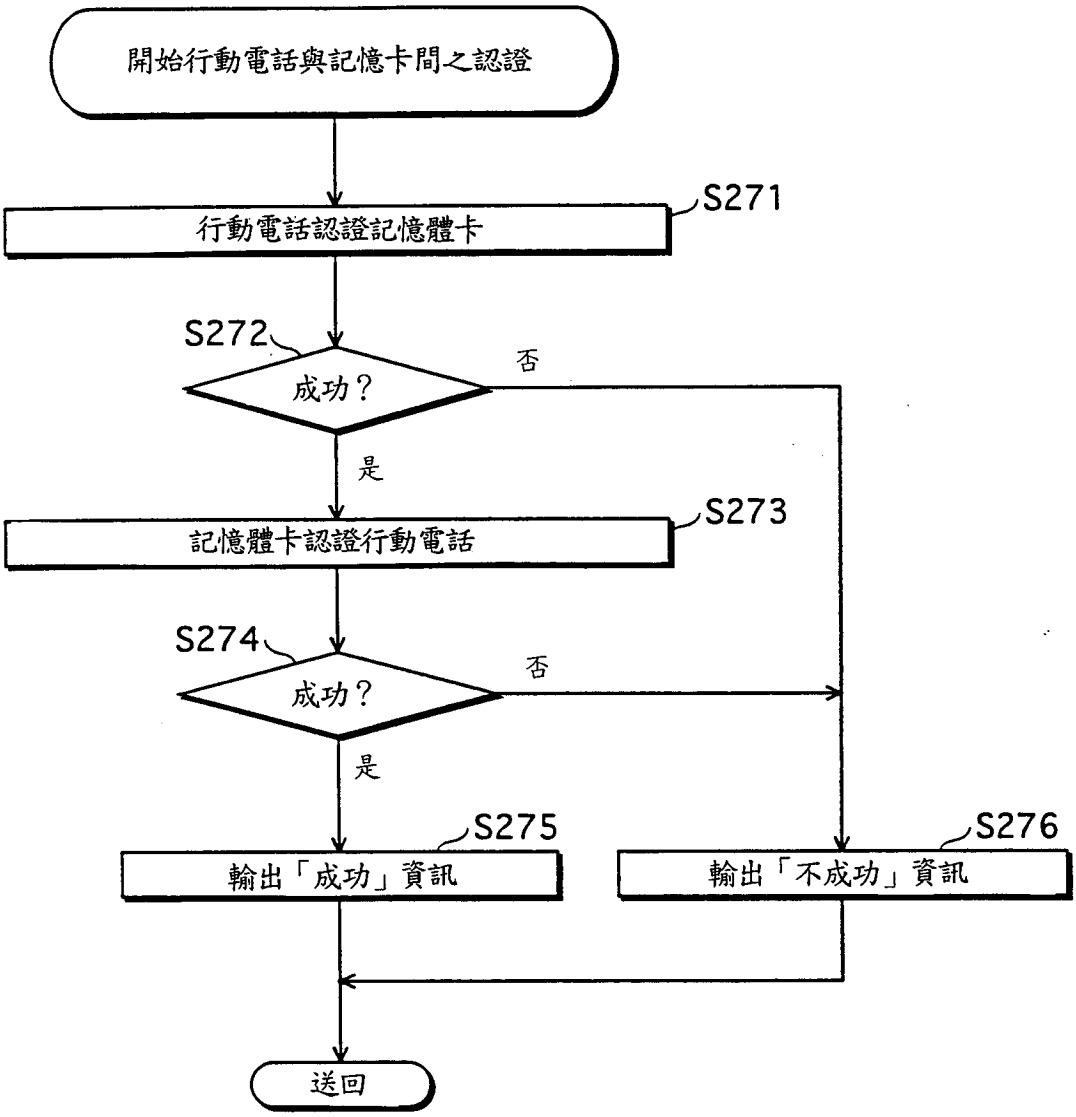

至 303
至 305
標頭鑰匙產生單元
321d
連鎖單元
324
加密解密單元
分割單元
344
380d
加密單元
(E2)
322d
解密單元
(D2)
342d
加密單元
(E3)
323d
解密單元
(D3)
343d
310
至 331
至 351
至 332
至 352

第 16 圖

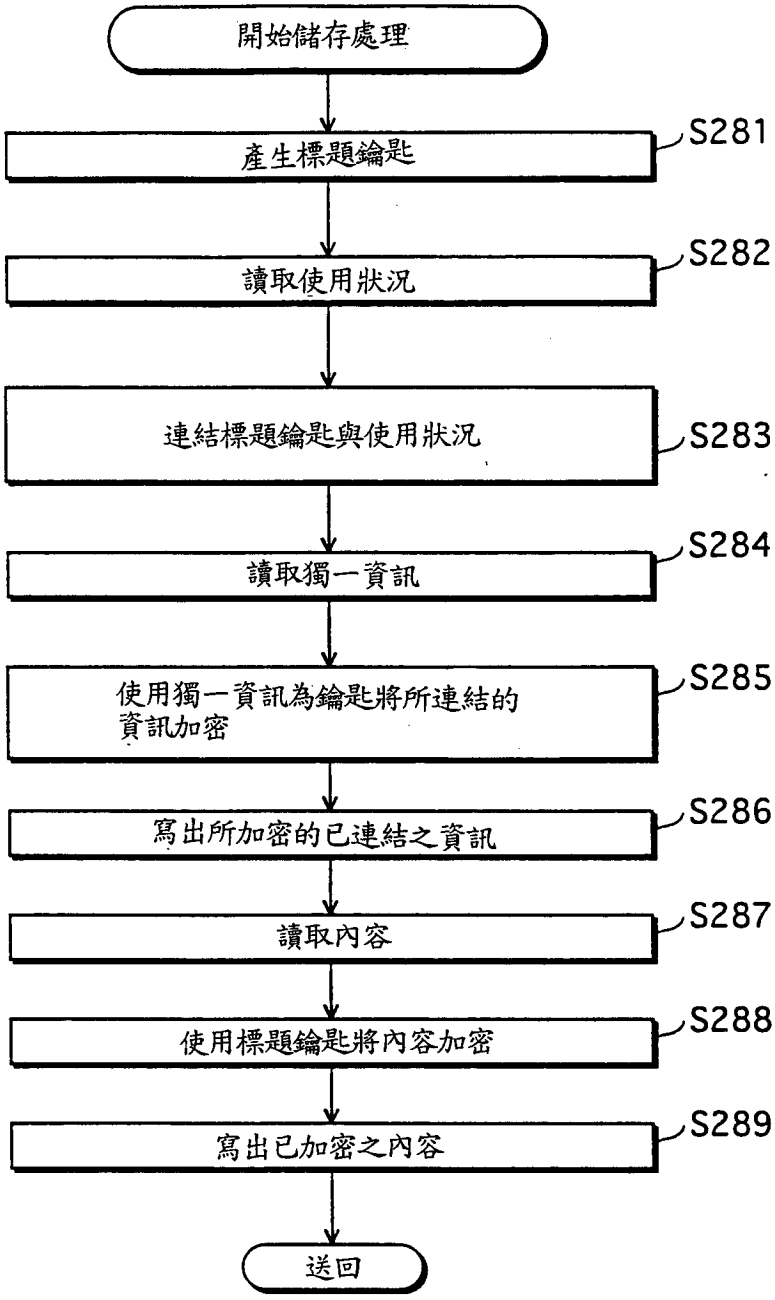

內容配銷伺服器裝置
行動電話
購買處理
S251
內容ID，付款資訊行動電話
S252
付款接收處理
S253
讀取具有使用狀況之內容
S254
具有使用狀況之內容
儲存具有使用狀況之內容
S255
S256
儲存
所指示之處理？
S257
讀取
播放
播放處理
S264
行動電話與記憶卡間之認證
S258
行動電話與記憶體卡間之認證
S261
認證成功？
S259
否
是
儲存處理
S260
認證成功？
S262
否
是
讀取處理
S263

第 17 圖

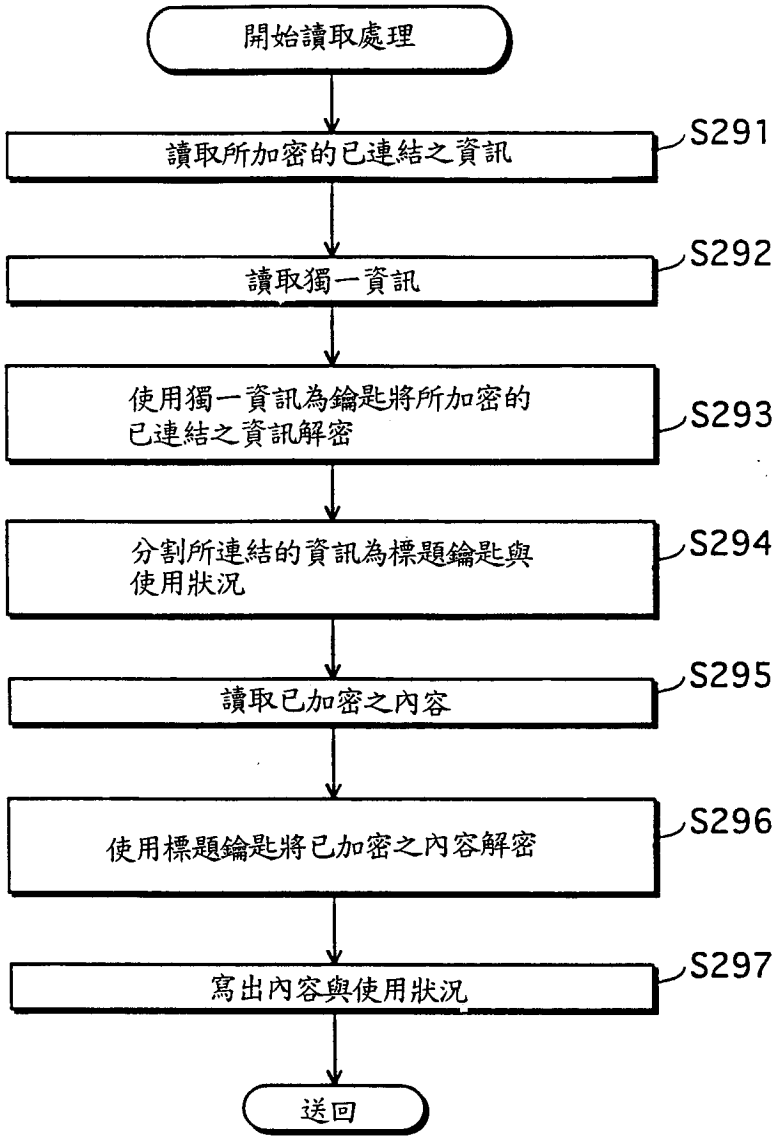
第 18 圖


開始行動電話與記憶卡間之認證
S271
行動電話認證記憶體卡
S272
成功？
否
是
S273
記憶體卡認證行動電話
S274
成功？
否
是
S275
輸出「成功」資訊
S276
輸出「不成功」資訊
送回

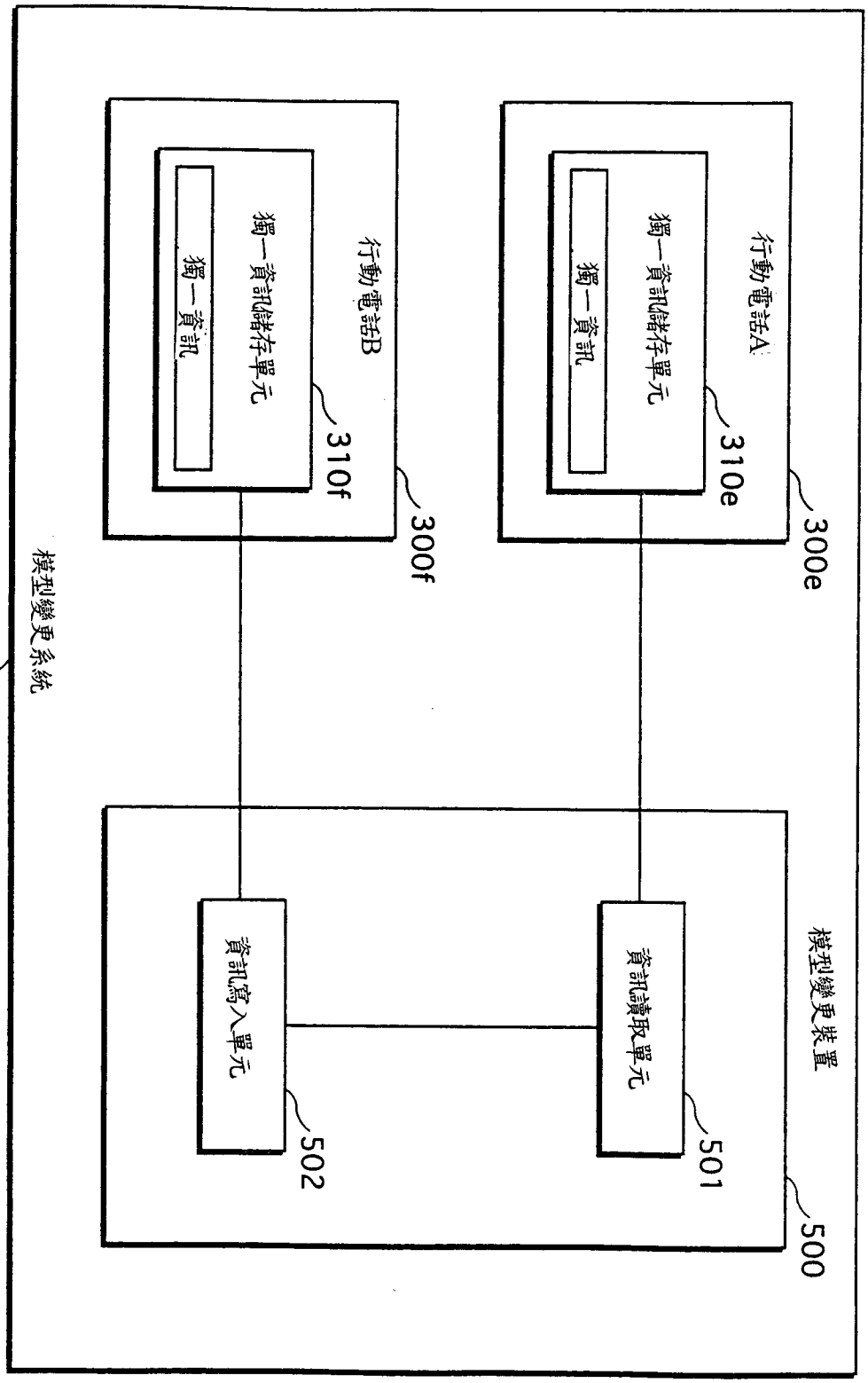
第 19 圖


開始儲存處理
產生標題鑰匙
S281
讀取使用狀況
S282
連結標題鑰匙與使用狀況
S283
讀取獨一資訊
S284
使用獨一資訊為鑰匙將所連結的資訊加密
S285
寫出所加密的已連結之資訊
S286
讀取內容
S287
使用標題鑰匙將內容加密
S288
寫出已加密之內容
S289
送回

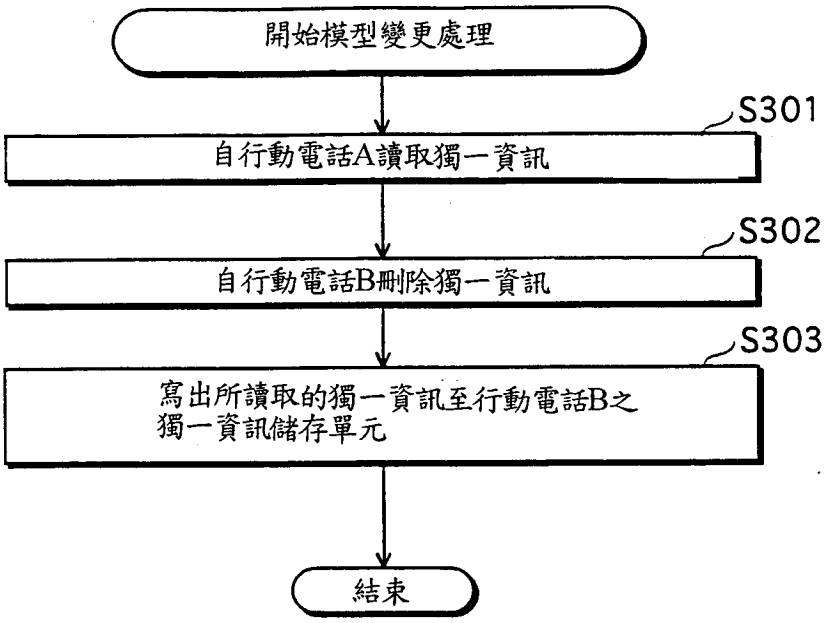
第 20 圖


開始讀取處理
讀取所加密的已連結之資訊
S291
讀取獨一資訊
S292
使用獨一資訊為鑰匙將所加密的已連結之資訊解密
S293
分割所連結的資訊為標題鑰匙與使用狀況
S294
讀取已加密之內容
S295
使用標題鑰匙將已加密之內容解密
S296
寫出內容與使用狀況
S297
送回

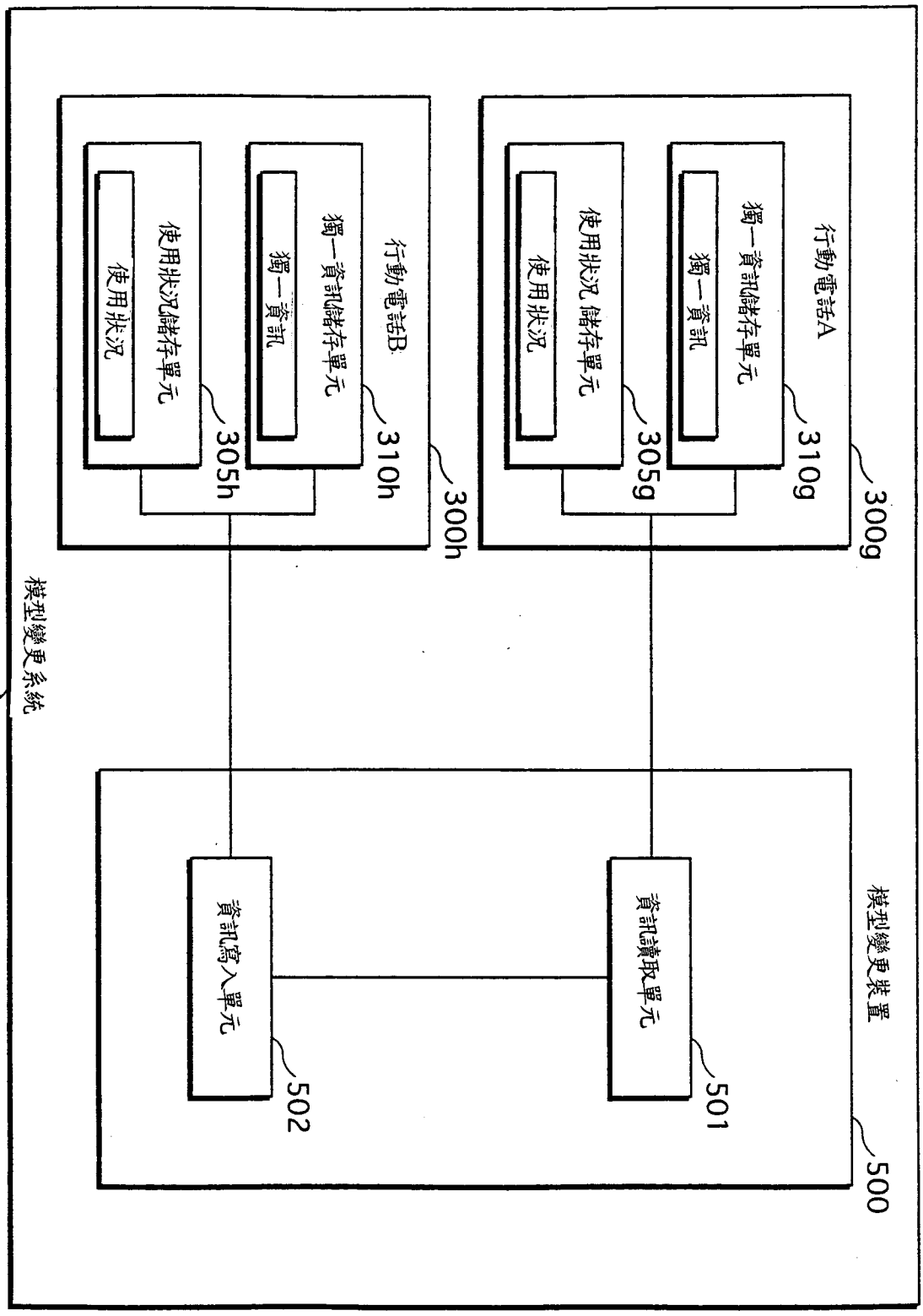
第 21 圖

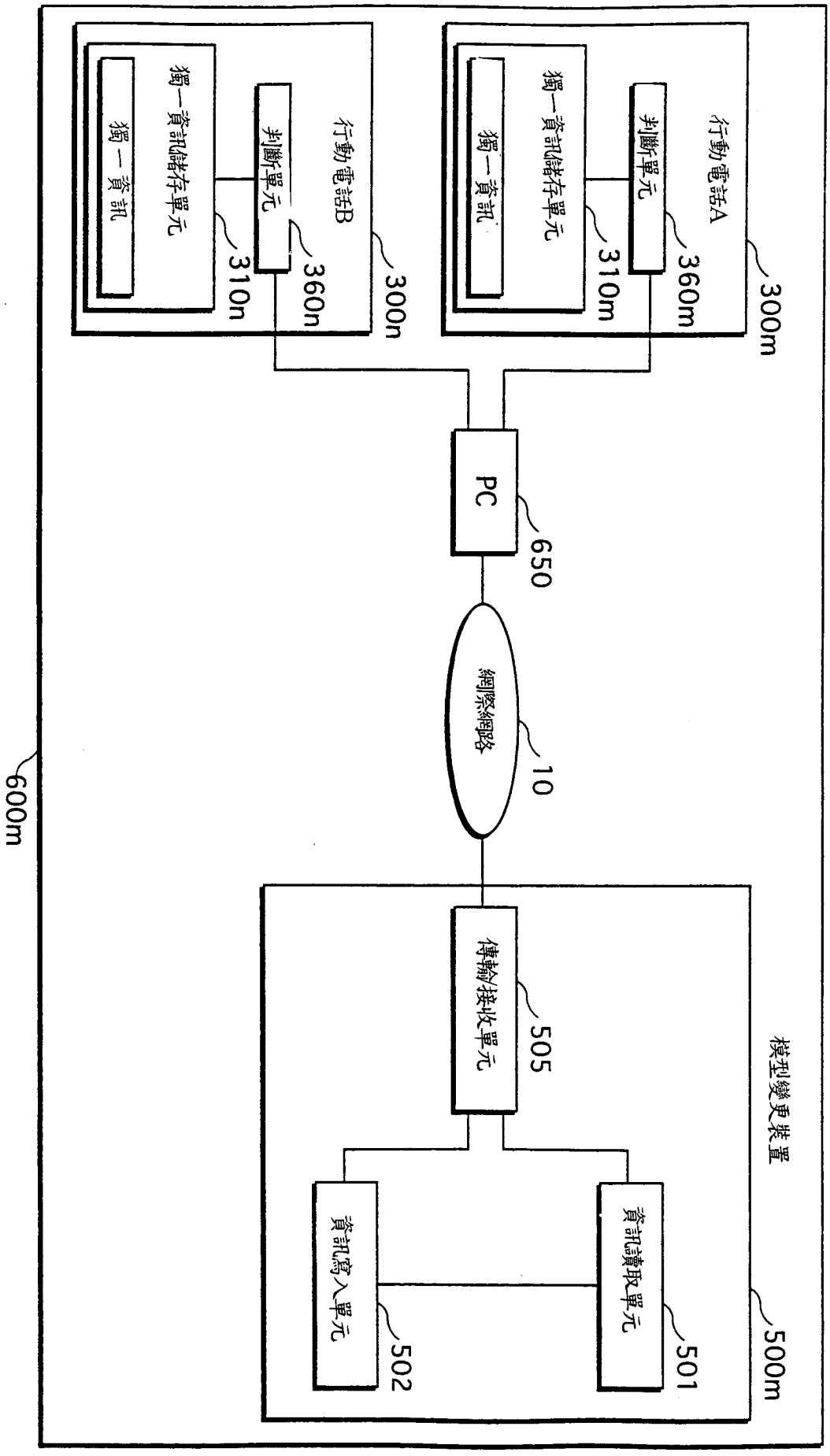

模型變更系統
600e
行動電話A
300e
獨一資訊儲存單元
310e
獨一資訊
行動電話B
300f
獨一資訊儲存單元
310f
獨一資訊
模型變更裝置
500
資訊讀取單元
501
資訊寫入單元
502

第 22 圖

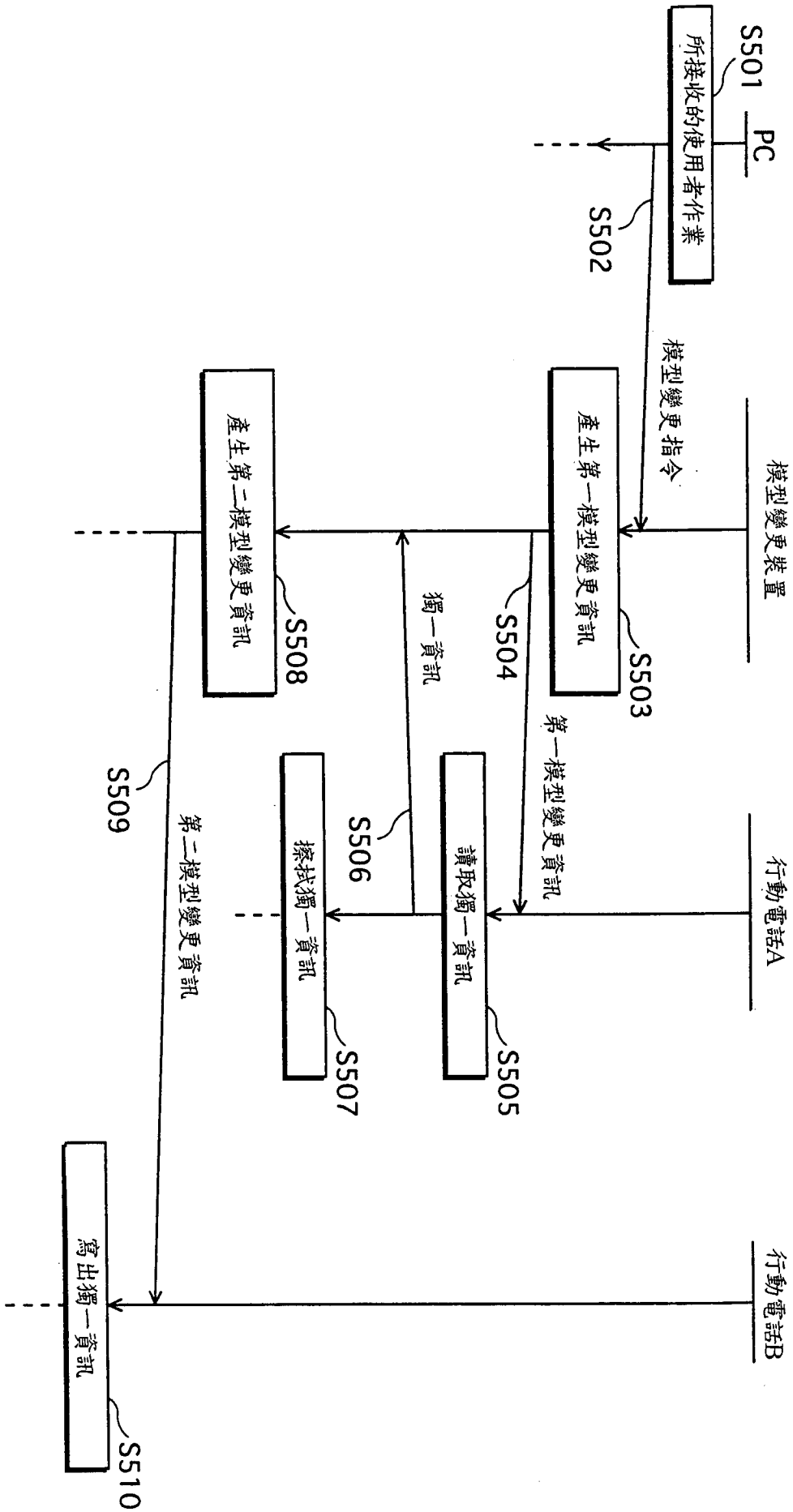

開始模型變更處理
S301
自行動電話A讀取獨一資訊
S302
自行動電話B刪除獨一資訊
S303
寫出所讀取的獨一資訊至行動電話B之
獨一資訊儲存單元
結束

第 23 圖

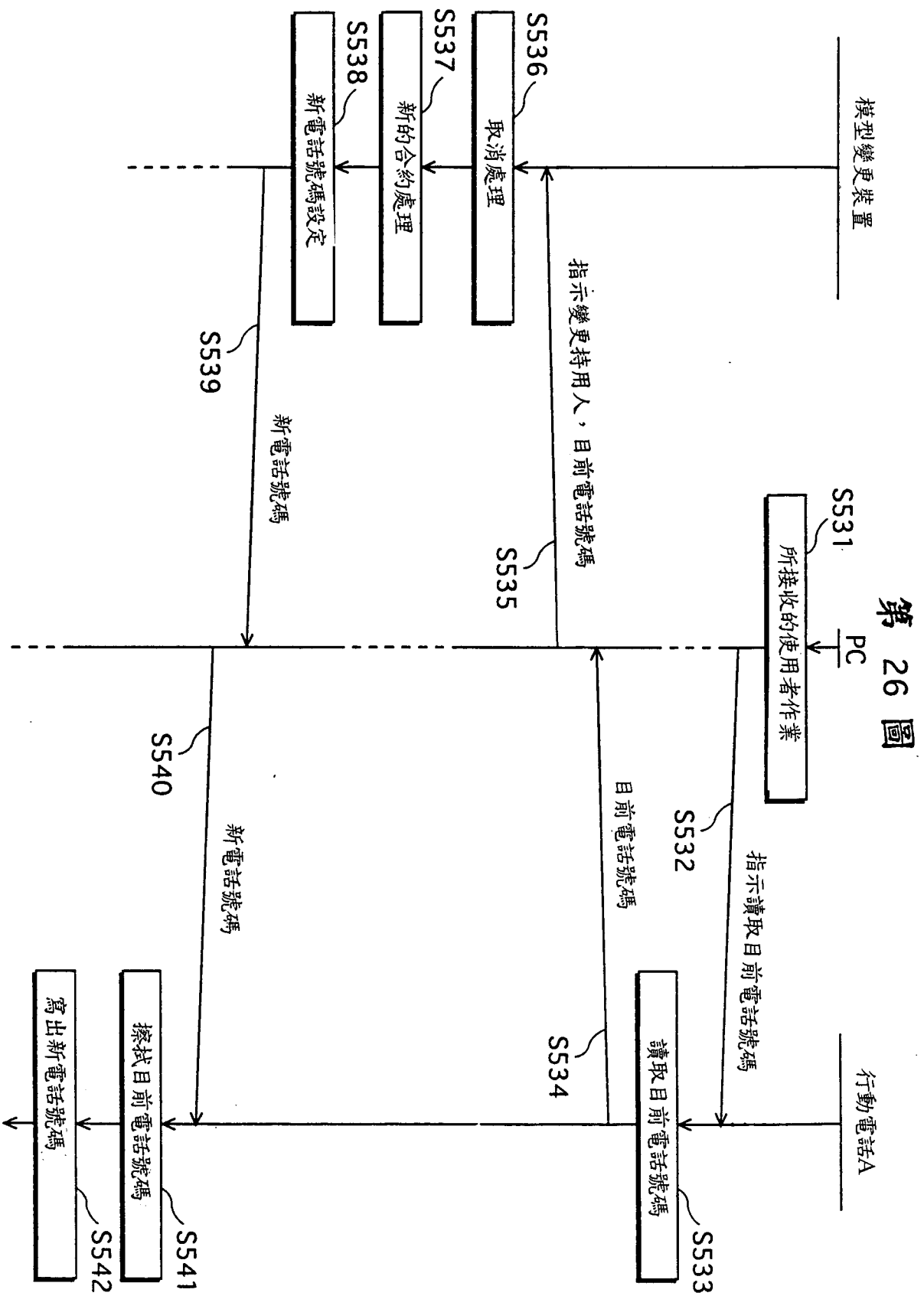

模型變更系統
600g
行動電話A
300g
獨一資訊儲存單元
310g
獨一資訊
使用狀況 儲存單元
305g
使用狀況
行動電話B
300h
獨一資訊儲存單元
310h
獨一資訊
使用狀況儲存單元
305h
使用狀況
模型變更裝置
500
資訊讀取單元
501
資訊寫入單元
502


600m
行動電話A
300m
判斷單元
360m
獨一資訊儲存單元
310m
獨一資訊
行動電話B
300n
判斷單元
360n
獨一資訊儲存單元
310n
獨一資訊
PC
650
網際網路
10
模型變更裝置
500m
傳輸接收單元
505
資訊讀取單元
501
資訊寫入單元
502

第 24 圖

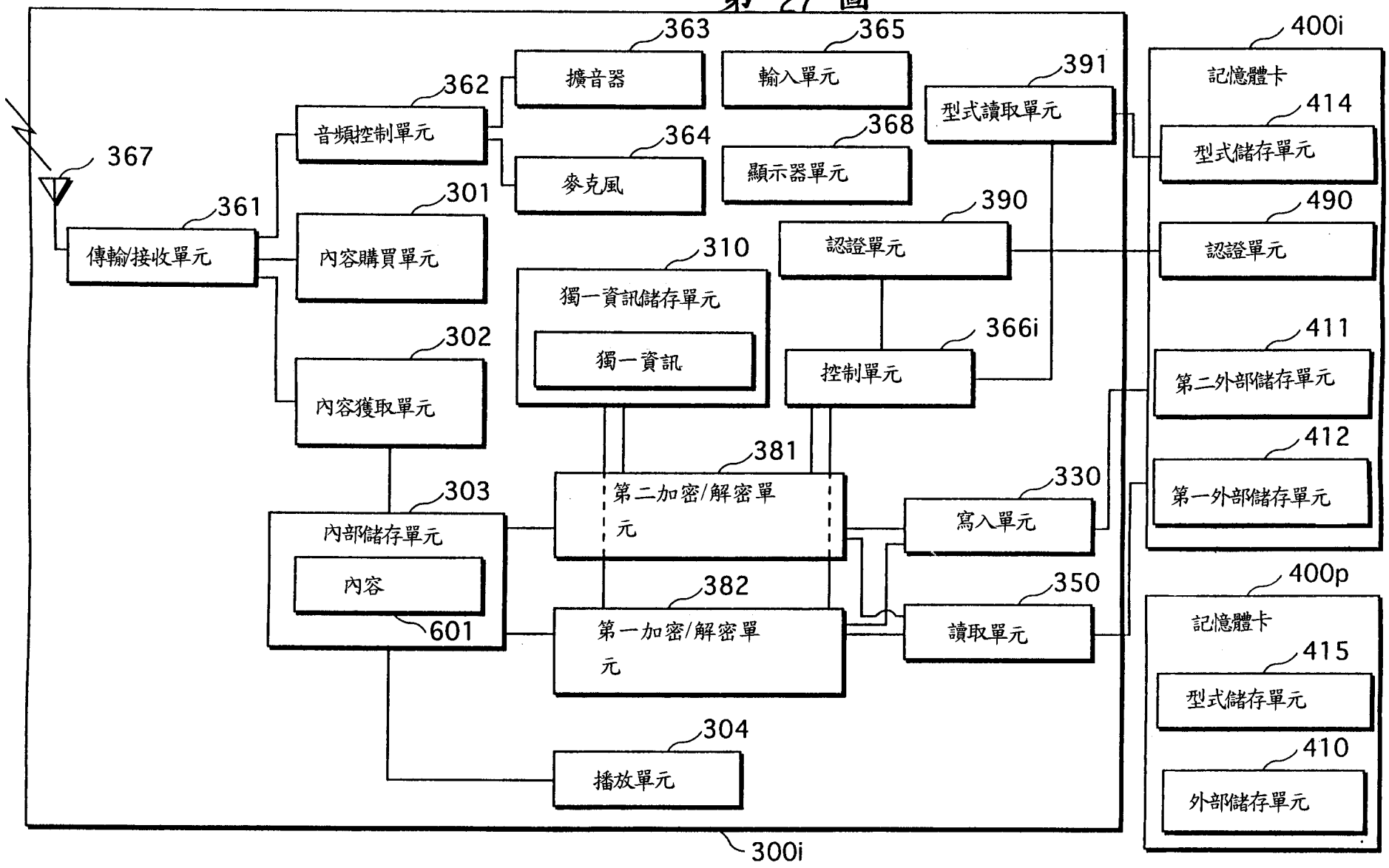

PC
所接收的使用者作業
S501
S502
模型變更指令
模型變更裝置
產生第一模型變更資訊
S503
S504
第一模型變更資訊
行動電話A
讀取獨一資訊
S505
獨一資訊
擦拭獨一資訊
S506
S507
產生第二模型變更資訊
S508
S509
第二模型變更資訊
行動電話B
寫出獨一資訊
S510

第 25 圖

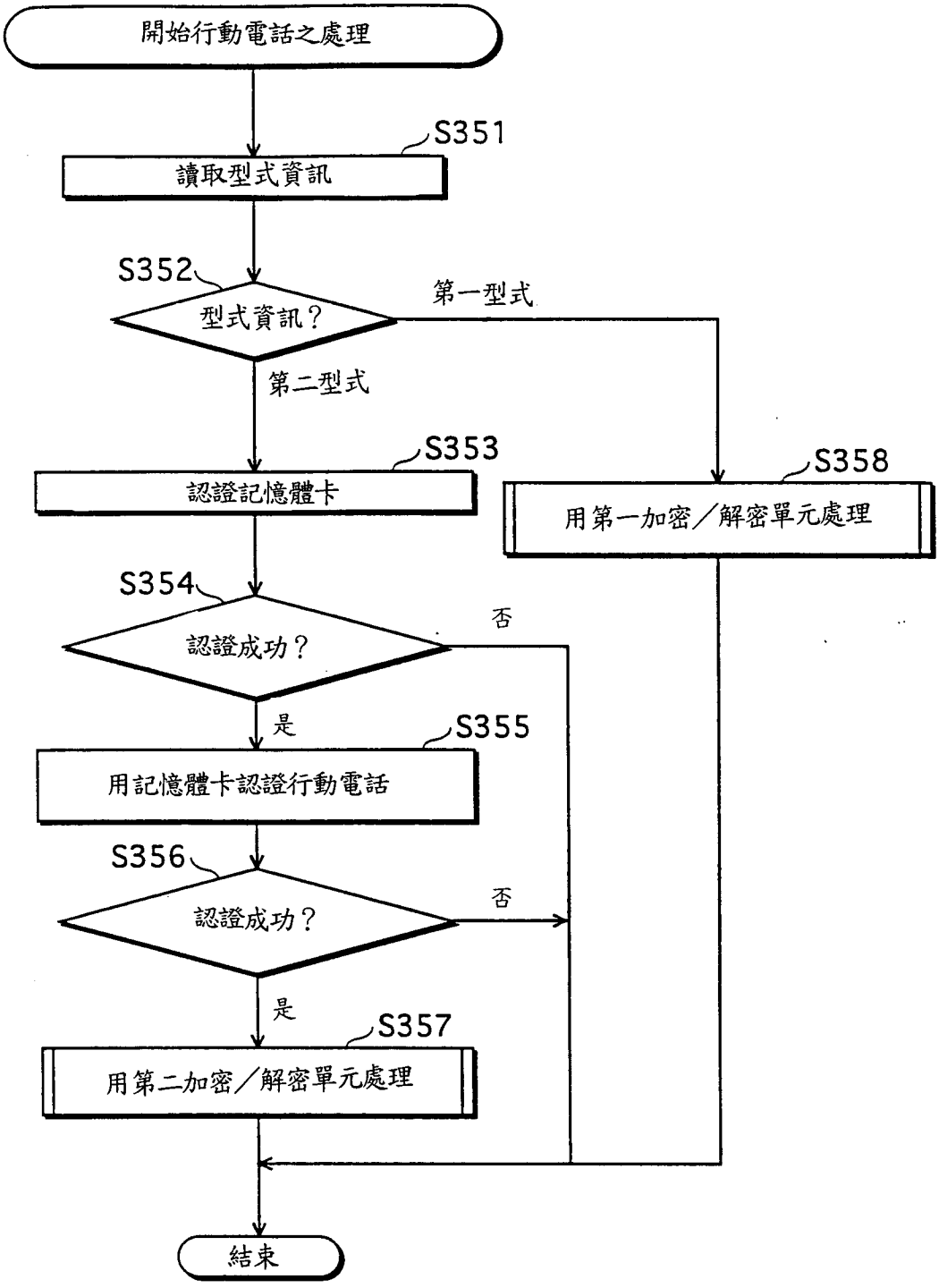

模型變更裝置
PC
行動電話A
S531
所接收的使用者作業
指示讀取目前電話號碼
S532
讀取目前電話號碼
S533
目前電話號碼
S534
指示變更持用人，目前電話號碼
S535
取消處理
S536
新的合約處理
S537
新電話號碼設定
S538
新電話號碼
S539
新電話號碼
S540
擦拭目前電話號碼
S541
寫出新電話號碼
S542

第 26 圖

第 27 圖


363
擴音器
365
輸入單元
391
型式讀取單元
400i
記憶體卡
362
音頻控制單元
414
型式儲存單元
367
364
麥克風
368
顯示器單元
361
傳輸/接收單元
301
內容購買單元
390
認證單元
490
認證單元
310
獨一資訊儲存單元
獨一資訊
366i
控制單元
411
第二外部儲存單元
302
內容獲取單元
412
第一外部儲存單元
381
第二加密/解密單元
330
寫入單元
303
內部儲存單元
內容
601
382
第一加密/解密單元
350
讀取單元
400p
記憶體卡
415
型式儲存單元
410
外部儲存單元
304
播放單元
300i

第 28 圖


開始行動電話之處理
S351
讀取型式資訊
S352
型式資訊？
第一型式
第二型式
S353
認證記憶體卡
S358
用第一加密／解密單元處理
S354
認證成功？
否
是
S355
用記憶體卡認證行動電話
S356
認證成功？
否
是
S357
用第二加密／解密單元處理
結束

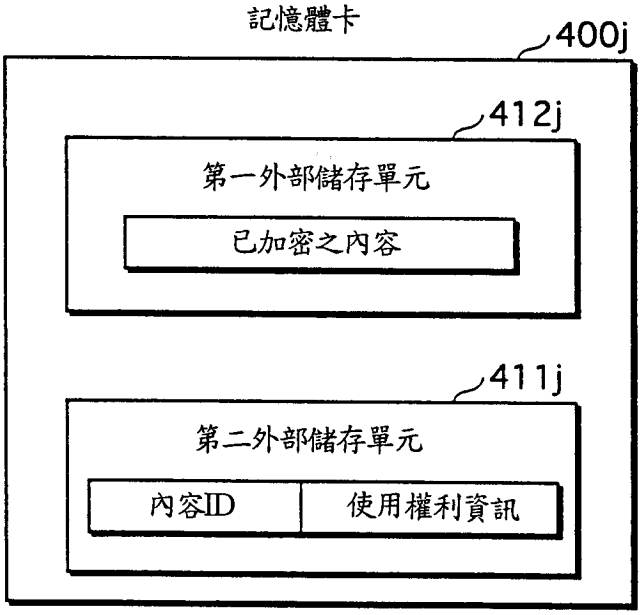
第 29 圖

權利資訊表

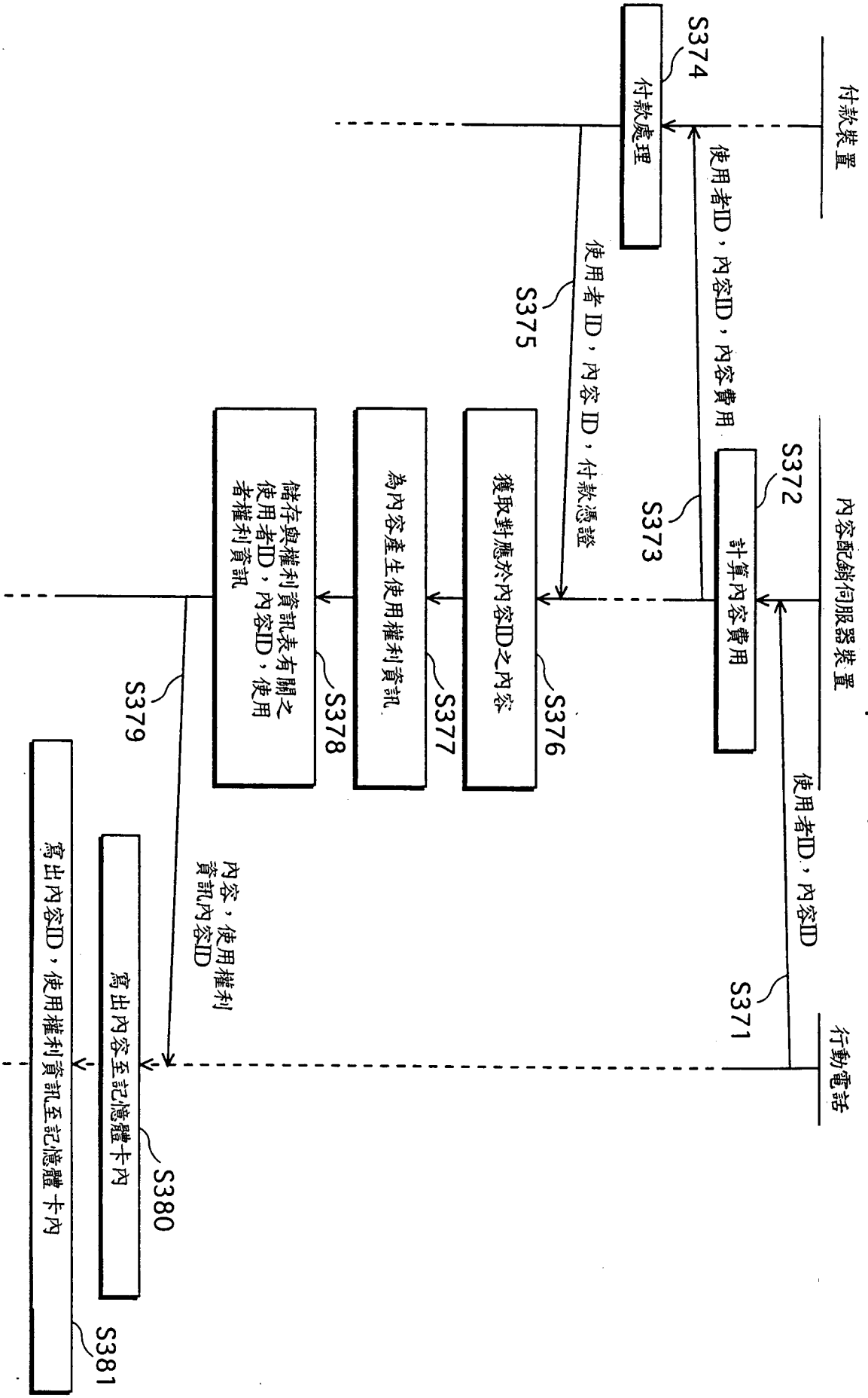
610

使用者ID	內容ID	使用權利資訊
A0001	C0001	AF1425…
B0002	C0002	CE5D369…
⋮	⋮	⋮

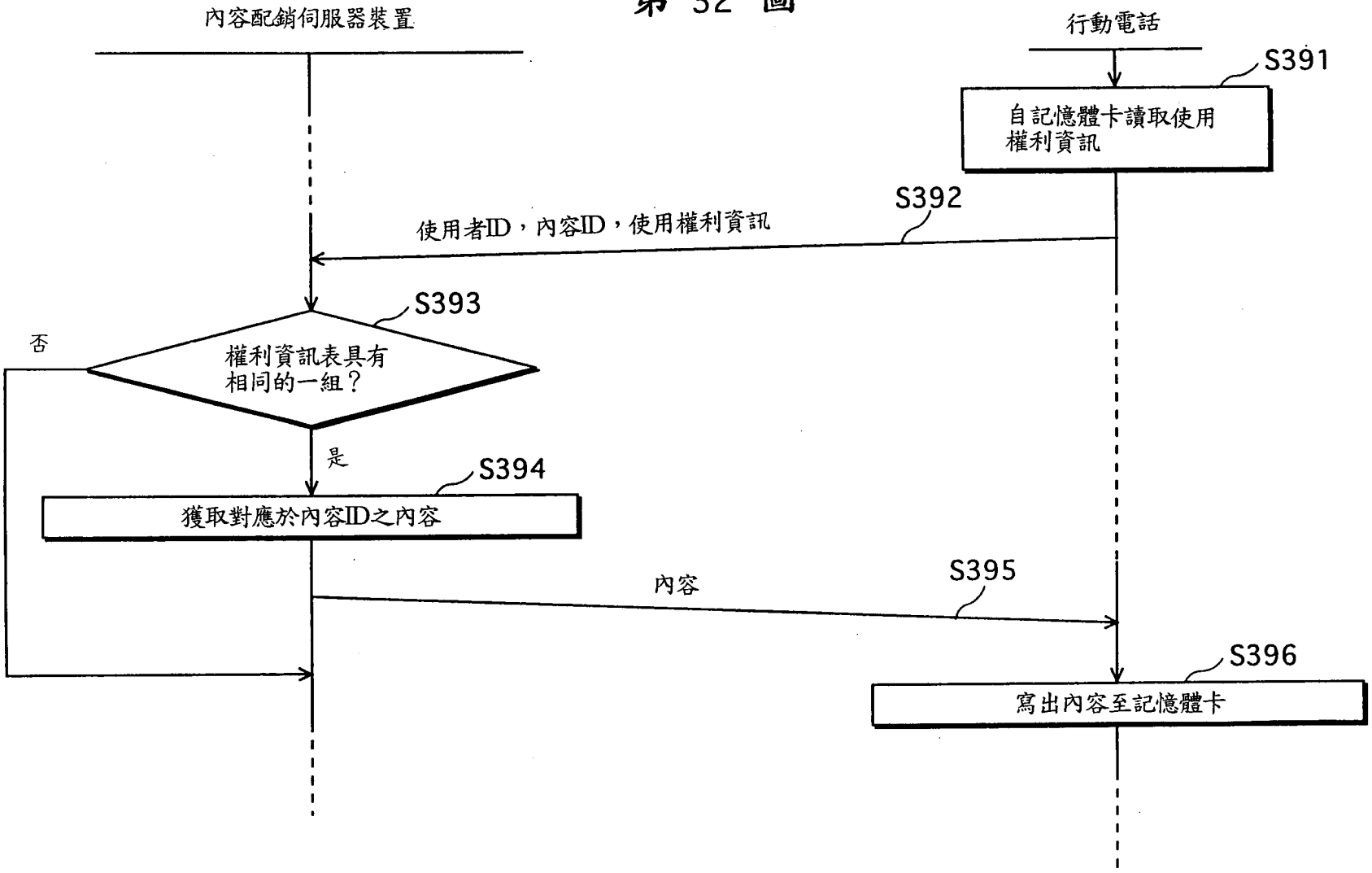
第 30 圖



第 31 圖


付款裝置
內容配銷伺服器裝置
行動電話
使用者ID，內容ID
S371
S372
計算內容費用
使用者ID，內容費用
S373
S374
付款處理
使用者 ID，內容 ID，付款憑證
S375
獲取對應於內容ID之內容
S376
為內容產生使用權利資訊
S377
儲存與權利資訊表有關之使用者ID，內容ID，使用者權利資訊
S378
S379
內容，使用權利資訊內容ID
寫出內容至記憶體卡內
S380
寫出內容ID，使用權利資訊至記憶體卡內
S381

第 32 圖

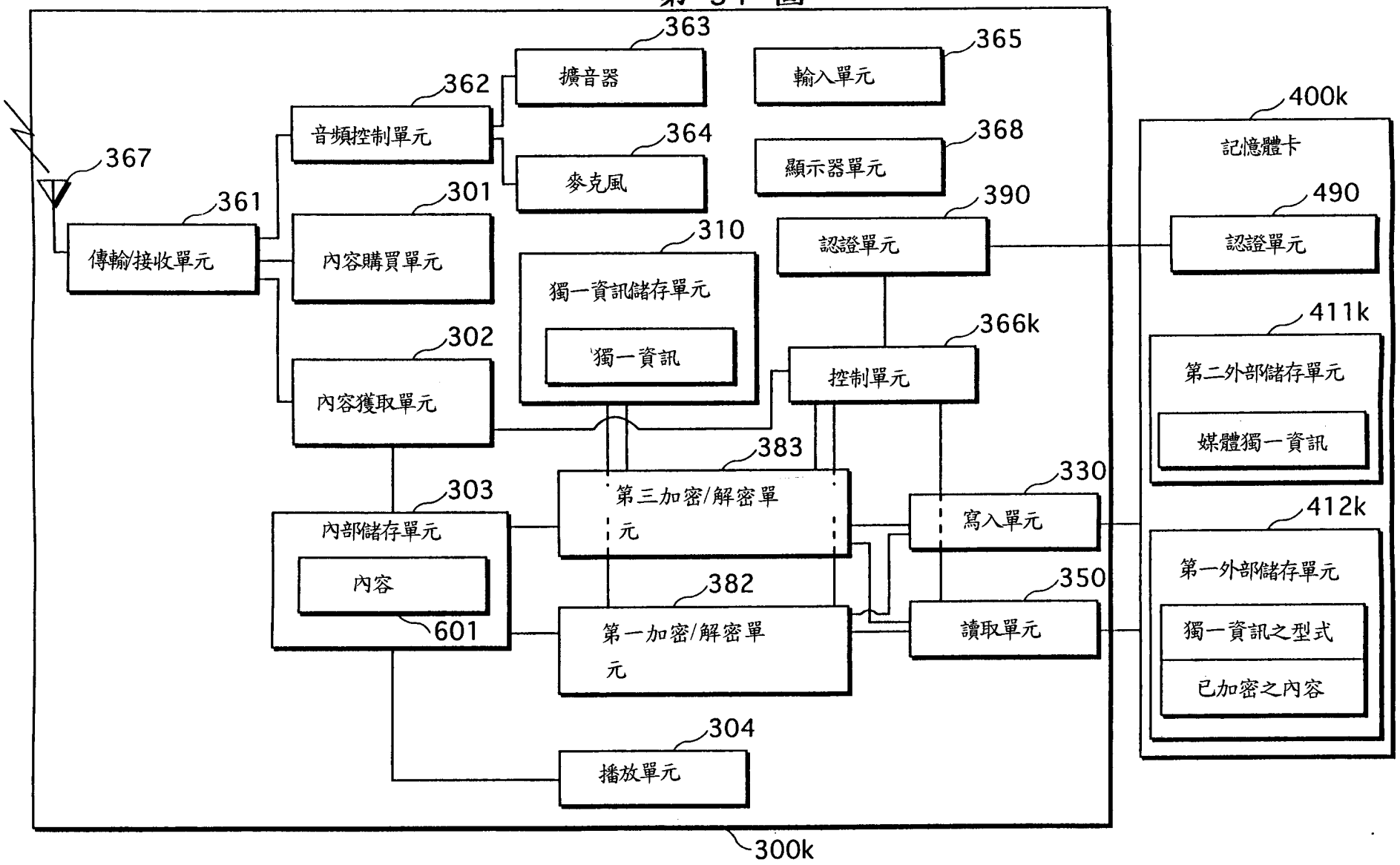

內容配銷伺服器裝置
行動電話
S391
自記憶體卡讀取使用權利資訊
S392
使用者ID，內容ID，使用權利資訊
S393
權利資訊表具有相同的一組？
否
是
S394
獲取對應於內容ID之內容
內容
S395
S396
寫出內容至記憶體卡

第 33 圖

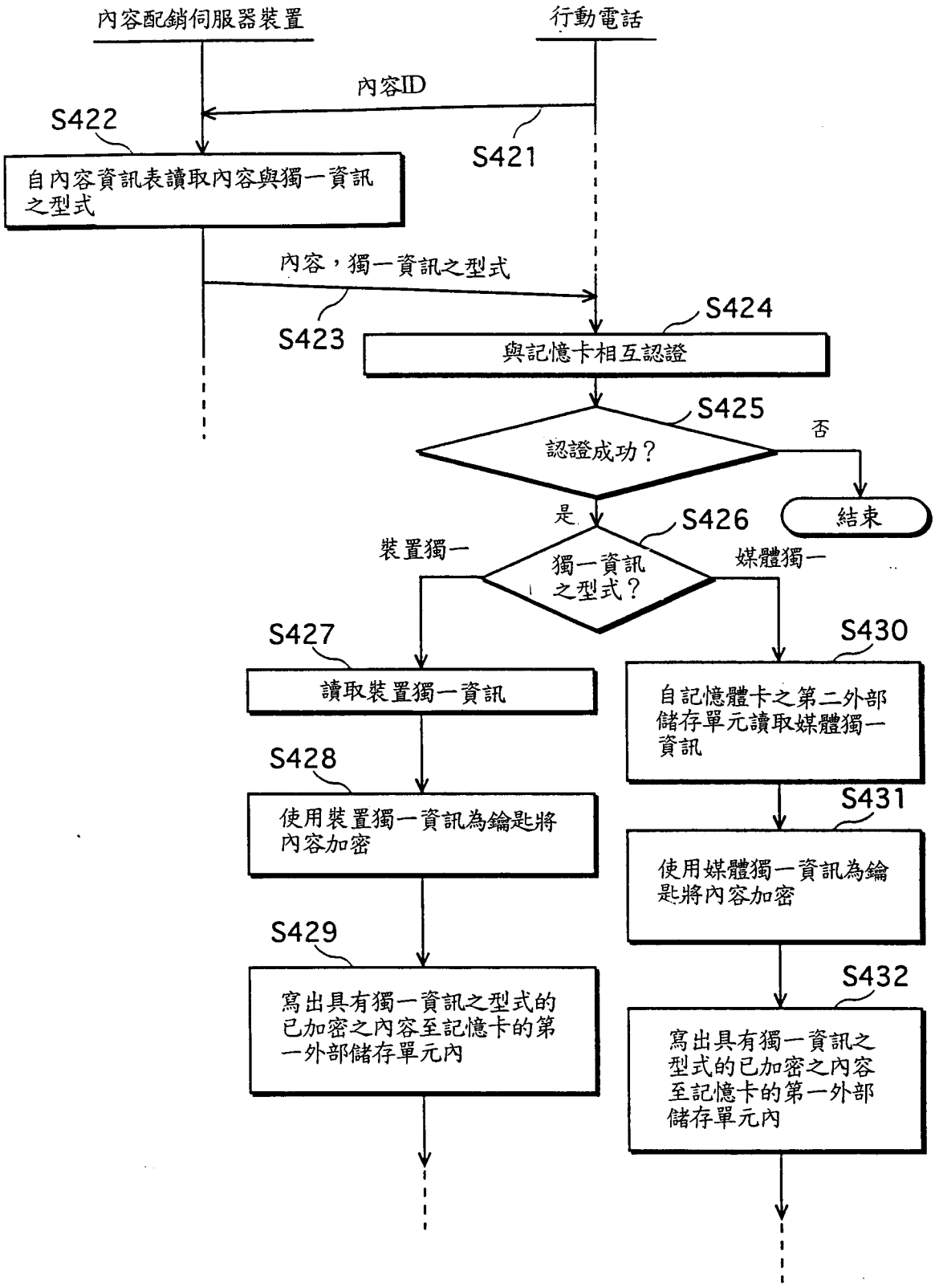
內容資訊表 620

內容ID	內容	獨一資訊之型式
C0001	音樂資訊	媒體獨一
C0002	音樂資訊	裝置獨一
⋮	⋮	⋮

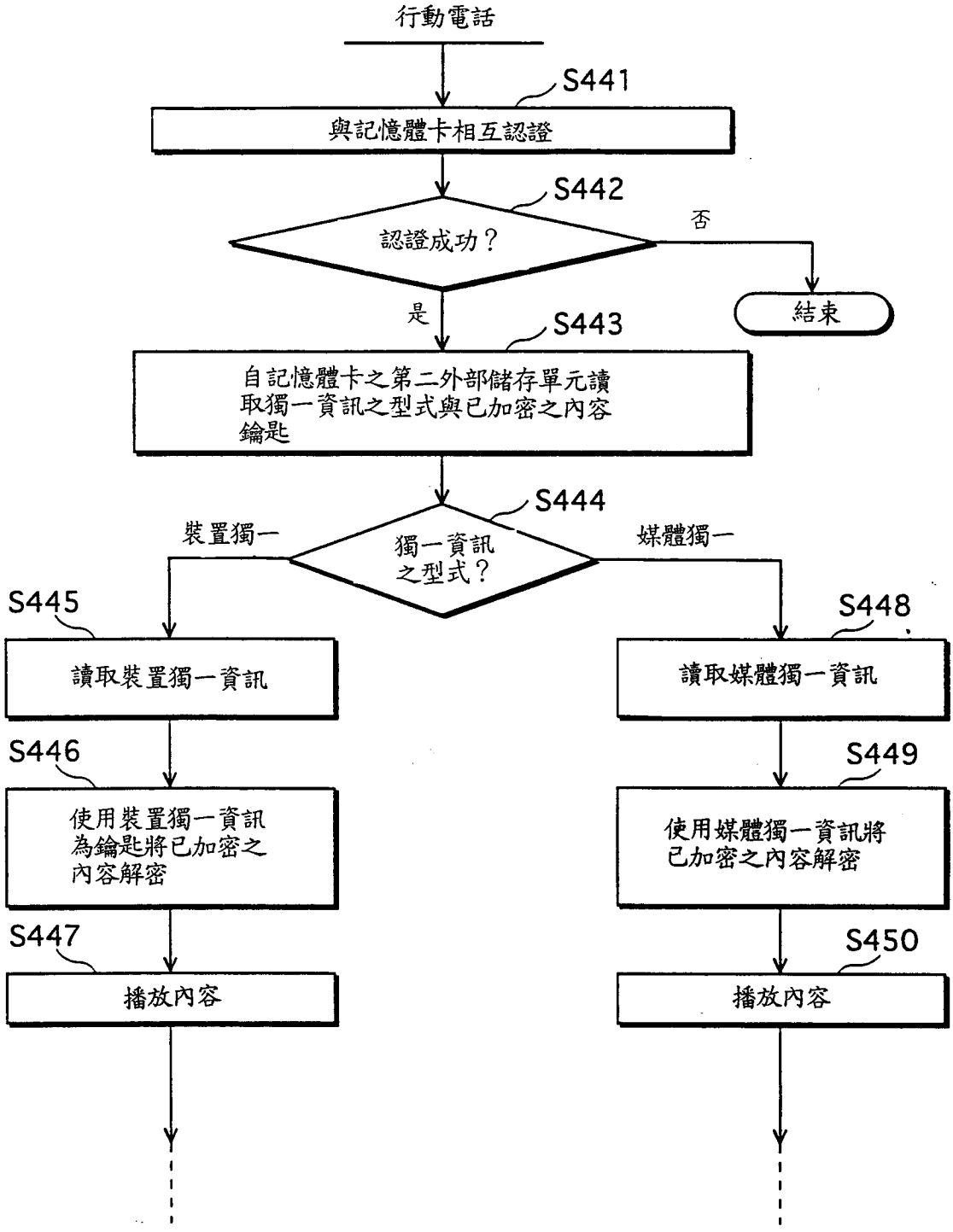
第 34 圖



第 35 圖


內容配銷伺服器裝置
行動電話
內容ID
S422
S421
自內容資訊表讀取內容與獨一資訊之型式
內容，獨一資訊之型式
S423
S424
與記憶卡相互認證
S425
認證成功？
否
結束
是
S426
獨一資訊之型式？
裝置獨一
媒體獨一
S427
讀取裝置獨一資訊
S428
使用裝置獨一資訊為鑰匙將內容加密
S429
寫出具有獨一資訊之型式的已加密之內容至記憶卡的第一外部儲存單元內
S430
自記憶體卡之第二外部儲存單元讀取媒體獨一資訊
S431
使用媒體獨一資訊為鑰匙將內容加密
S432
寫出具有獨一資訊之型式的已加密之內容至記憶卡的第一外部儲存單元內

第 36 圖


行動電話
S441
與記憶體卡相互認證
S442
認證成功？
否
結束
是
S443
自記憶體卡之第二外部儲存單元讀取獨一資訊之型式與已加密之內容鑰匙
S444
獨一資訊之型式？
裝置獨一
媒體獨一
S445
讀取裝置獨一資訊
S446
使用裝置獨一資訊為鑰匙將已加密之內容解密
S447
播放內容
S448
讀取媒體獨一資訊
S449
使用媒體獨一資訊將已加密之內容解密
S450
播放內容