【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成19年8月16日(2007.8.16)

【公開番号】特開2006-18335(P2006-18335A)
【公開日】平成18年1月19日(2006.1.19)
【年通号数】公開・登録公報2006-003
【出願番号】特願2004-192399(P2004-192399)
【国際特許分類】
Ｇ０６Ｆ　21/24　　(2006.01)
Ｈ０４Ｌ　 9/08　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　　５４０Ｃ
Ｇ０６Ｆ　12/14　　５３０Ｃ
Ｈ０４Ｌ　 9/00　　６０１Ｃ
Ｈ０４Ｌ　 9/00　　６０１Ｅ

【手続補正書】
【提出日】平成19年6月29日(2007.6.29)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
外部メモリを接続するためのインタフェースと、
乱数を発生させる乱数発生手段と、
暗号化処理に用いる鍵を生成する鍵生成手段と、
この鍵生成手段によって生成された鍵に基づいて暗号化・復号化を行う暗号化・復号化手段と、
前記インタフェースに接続された外部メモリとの間でデータの読出し、及び書込みを行うデータ処理手段とを備え、
前記鍵生成手段は、前記インタフェースに接続された外部メモリから読み出されたこの外部メモリに固有の識別情報に基づいて第１の鍵を生成し、
前記暗号化・復号化手段は、この第１の鍵を用いて前記乱数発生手段が生成した乱数を暗号化して暗号化乱数を生成し、
前記データ処理手段は、前記暗号化乱数を前記インタフェースに接続された外部メモリに記憶させ、
更に取得したコンテンツを前記インタフェースに接続された外部メモリに記憶させるとき、
前記データ処理手段は、接続された外部メモリから固有の識別情報と暗号化乱数を読出し、
前記鍵生成手段は、読出した識別情報に基づいて第２の鍵を生成し、
前記暗号化・復号化手段は、この第２の鍵を用いて前記暗号化乱数を復号して乱数を生成し、
前記鍵生成手段は、前記暗号化・復号化手段で生成された乱数と前記外部メモリから読出した識別情報とを用いて第３の鍵を生成し、
前記暗号化・復号化手段は、この第３の鍵を用いて外部メモリに記憶させるコンテンツを暗号化するのに用いるコンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、

前記データ処理手段は、この暗号化コンテンツ鍵を前記インタフェースに接続された外部メモリに記憶させること
を特徴とする端末装置。
【請求項２】
前記鍵生成手段は、前記インタフェースに接続された外部メモリとの間で認証処理を実行して外部メモリで生成される鍵と同一の共通鍵を生成し、前記暗号化・復号化手段は、生成された共通鍵を用いて前記暗号化乱数および暗号化コンテンツ鍵を更に暗号化し、前記データ処理手段は、この更に暗号化された暗号化乱数および暗号化コンテンツ鍵を前記インタフェースに接続された外部メモリに記憶させることを特徴とする請求項１に記載の端末装置。
【請求項３】
前記暗号化・復号化手段は、コンテンツを前記インタフェースに接続された外部メモリに記憶させるとき、前記コンテンツ暗号化鍵と入力されたパスワードを、前記第３の鍵を用いて暗号化して暗号化コンテンツ鍵と暗号化パスワードを生成し、前記データ処理手段は、この暗号化コンテンツ鍵と暗号化パスワードを前記インタフェースに接続された外部メモリに記憶させることを特徴とする請求項１に記載の端末装置。
【請求項４】
外部メモリを接続するためのインタフェースと、
乱数を発生させる乱数発生手段と、
暗号化処理に用いる鍵を生成する鍵生成手段と、
この鍵生成手段によって生成された鍵に基づいて暗号化・復号化を行う暗号化・復号化手段と、
前記インタフェースに接続された外部メモリとの間でデータの読出し、及び書込みを行うデータ処理手段とを備え、
コンテンツを前記インタフェースに接続された外部メモリに記憶させる処理を実行する前に、
前記鍵生成手段は、前記インタフェースに接続された外部メモリから読み出したこの外部メモリに固有の識別情報に基づいて第１の鍵を生成し、
前記暗号化・復号化手段は、この第１の鍵を用いて前記乱数発生手段が生成した乱数を暗号化して暗号化乱数を生成し、
前記データ処理手段は、前記暗号化乱数を前記インタフェースに接続された外部メモリに記憶させ、
更に取得したコンテンツを前記インタフェースに接続された外部メモリに記憶させる処理を実行するとき、
前記データ処理手段は、接続された外部メモリから固有の識別情報と暗号化乱数を読出し、
前記鍵生成手段は、読出した識別情報に基づいて第２の鍵を生成し、
前記暗号化・復号化手段は、この第２の鍵を用いて前記暗号化乱数を復号して乱数を生成し、
前記鍵生成手段は、前記暗号化・復号化手段で生成された乱数と前記外部メモリから読出した識別情報とを用いて第３の鍵を生成し、
前記暗号化・復号化手段は、この第３の鍵を用いて外部メモリに記憶させるコンテンツを暗号化するのに用いるコンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、
前記データ処理手段は、この暗号化コンテンツ鍵を前記インタフェースに接続された外部メモリに記憶させること
を特徴とする端末装置。
【請求項５】
前記鍵生成手段は、前記インタフェースに接続された外部メモリとの間で認証処理を実行して外部メモリで生成される鍵と同一の共通鍵を生成し、前記暗号化・復号化手段は、生成された共通鍵を用いて前記暗号化乱数および暗号化コンテンツ鍵を更に暗号化し、前記

データ処理手段は、この更に暗号化された暗号化乱数および暗号化コンテンツ鍵を前記インタフェースに接続された外部メモリに記憶させることを特徴とする請求項４に記載の端末装置。
【請求項６】
前記暗号化・復号化手段は、コンテンツを前記インタフェースに接続された外部メモリに記憶させるとき、前記コンテンツ暗号化鍵と入力されたパスワードを、前記第３の鍵を用いて暗号化して暗号化コンテンツ鍵と暗号化パスワードを生成し、前記データ処理手段は、この暗号化コンテンツ鍵と暗号化パスワードを前記インタフェースに接続された外部メモリに記憶させることを特徴とする請求項４に記載の端末装置。
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正の内容】
【発明の名称】端末装置
【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正の内容】
【０００１】
本発明は、外部メモリを接続可能で、この外部メモリにコンテンツを記憶する機能を備えた端末装置に関する。
【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正の内容】
【００１０】
本発明は上記問題点を解決するためになされたものであり、ユーザの操作を必要とせずにＡＩＤを用いたバインドを可能とする端末装置を提供することを目的とする。
【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正の内容】
【００１１】
本発明の端末装置は、外部メモリを接続するためのインタフェースと、乱数を発生させる乱数発生手段と、暗号化処理に用いる鍵を生成する鍵生成手段と、この鍵生成手段によって生成された鍵に基づいて暗号化・復号化を行う暗号化・復号化手段と、前記インタフェースに接続された外部メモリとの間でデータの読出し、及び書込みを行うデータ処理手段とを備え、前記鍵生成手段は、前記インタフェースに接続された外部メモリから読み出されたこの外部メモリに固有の識別情報に基づいて第１の鍵を生成し、前記暗号化・復号化手段は、この第１の鍵を用いて前記乱数発生手段が生成した乱数を暗号化して暗号化乱数を生成し、前記データ処理手段は、前記暗号化乱数を前記インタフェースに接続された外部メモリに記憶させ、更に取得したコンテンツを前記インタフェースに接続された外部メモリに記憶させるとき、前記データ処理手段は、接続された外部メモリから固有の識別情報と暗号化乱数を読出し、前記鍵生成手段は、読出した識別情報に基づいて第２の鍵を生成し、前記暗号化・復号化手段は、この第２の鍵を用いて前記暗号化乱数を復号して乱数を生成し、前記鍵生成手段は、前記暗号化・復号化手段で生成された乱数と前記外部メ

モリから読出した識別情報とを用いて第３の鍵を生成し、前記暗号化・復号化手段は、この第３の鍵を用いて外部メモリに記憶させるコンテンツを暗号化するのに用いるコンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、前記データ処理手段は、この暗号化コンテンツ鍵を前記インタフェースに接続された外部メモリに記憶させることを特徴とする。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】削除
【補正の内容】
【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】削除
【補正の内容】
【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】変更
【補正の内容】
【００１４】
本発明によれば、コンテンツの秘密管理を強化するためのＡＩＤの値を直接操作せずに実現することを可能とした端末装置を提供することができる。