

【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 7 部門第 3 区分
【発行日】平成 17 年 8 月 11 日 (2005.8.11)

【公開番号】特開 2005-57701 (P2005-57701A)
【公開日】平成 17 年 3 月 3 日 (2005.3.3)
【年通号数】公開・登録公報 2005-009
【出願番号】特願 2003-289330 (P2003-289330)
【国際特許分類第 7 版】

H 0 4 L 9/14

G 0 6 F 12/14

【F I】

H 0 4 L 9/00 6 4 1

G 0 6 F 12/14 3 2 0 B

【手続補正書】
【提出日】平成 17 年 3 月 16 日 (2005.3.16)
【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】

ネットワーク接続デバイスに対するコンテンツ提供処理を行うコンテンツサーバとしての機能を持つ情報処理装置であり、

暗号化コンテンツと、暗号化コンテンツの復号に適用するコンテンツキーの暗号化データであり、前記ネットワーク接続デバイスとの共有キーとして設定され、適宜更新されるネットワークキーによって暗号化された暗号化コンテンツキーとを格納した記憶部と、

前記記憶部に格納された暗号化コンテンツキーの暗号化キーとして適用中の全ての更新前ネットワークキーを含むネットワークキーを登録、格納したネットワークキーテーブルと、

を有することを特徴とする情報処理装置。

【請求項 2】

前記情報処理装置は、

ネットワークキーの更新処理を条件として、前記記憶部に格納済みの更新前ネットワークキーにより暗号化された暗号化コンテンツキーを、更新後ネットワークキーによる暗号化キーとする鍵架け替え処理を実行することなく前記記憶部に維持する構成であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 3】

前記情報処理装置は、

前記記憶部に格納された暗号化コンテンツの利用処理の発生を条件として、利用処理対象のコンテンツに対応する暗号化コンテンツキーが更新後ネットワークキーと異なる更新前ネットワークキーによる暗号化コンテンツキーとして前記記憶部に格納されている場合に、該暗号化コンテンツキーを、更新後ネットワークキーを適用した暗号化コンテンツキーに更新する鍵架け替え処理を実行する構成を有することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 4】

前記情報処理装置は、

更新後ネットワークキーを格納するカレントネットワークキーメモリを有し、

前記更新後ネットワークキーを適用した暗号化コンテンツキーの前記記憶部に対する格納処理の実行を条件として、前記更新ネットワークキーを前記カレントネットワークキーメモリから前記ネットワークキーテーブルに移動格納する処理を実行する構成を有することを特徴とする請求項 1 に記載の情報処理装置。

【請求項 5】

前記情報処理装置は、

前記ネットワークキーテーブルに新たな更新後ネットワークキーを格納する際に、該ネットワークキーテーブルに格納済みの複数の更新前ネットワークキーから、削除対象ネットワークキーの選択処理を実行し、該削除処理の完了を条件として前記更新後ネットワークキーのネットワークキーテーブルに対する格納処理を実行する構成であることを特徴とする請求項 1 に記載の情報処理装置。

【請求項 6】

暗号化コンテンツと、暗号化コンテンツの復号に適用するコンテンツキーの暗号化データであり、前記ネットワーク接続デバイスとの共有キーとして設定され、適宜更新されるネットワークキーによって暗号化された暗号化コンテンツキーとを記憶部に格納したコンテンツ提供サーバにおけるコンテンツ情報管理方法であり、

前記記憶部に格納された暗号化コンテンツの利用処理の発生を条件として、利用処理対象のコンテンツに対応する暗号化コンテンツキーが更新後ネットワークキーと異なる更新前ネットワークキーによる暗号化コンテンツキーとして前記記憶部に格納されているか否かの判定処理を実行する判定処理ステップと、

前記判定処理ステップにおいて、利用処理対象のコンテンツに対応する暗号化コンテンツキーが更新後ネットワークキーと異なる更新前ネットワークキーによる暗号化コンテンツキーとして前記記憶部に格納されていると判定した場合に、該暗号化コンテンツキーを、更新後ネットワークキーを適用した暗号化コンテンツキーに更新する鍵架け替え処理を実行する鍵架け替え処理ステップと、

を有することを特徴とするコンテンツ情報管理方法。

【請求項 7】

前記コンテンツ情報管理方法は、さらに、

前記記憶部に格納された暗号化コンテンツ、および前記鍵架け替え処理により生成した更新後ネットワークキーを適用した暗号化コンテンツキーを、暗号化コンテンツの利用処理を要求したデバイスに送信するステップを有することを特徴とする請求項 6 に記載のコンテンツ情報管理方法。

【請求項 8】

前記コンテンツ情報管理方法は、さらに、

前記利用処理対象のコンテンツに対応する暗号化コンテンツキーに適用されている更新前ネットワークキーと同一の更新前ネットワークキーを適用した全ての前記記憶部に格納された暗号化コンテンツキーについて、前記更新後ネットワークキーを適用した暗号化コンテンツキーに更新する鍵架け替え処理を実行し、前記更新前ネットワークキーを、前記ネットワークキーテーブルから削除する処理を実行するステップを有することを特徴とする請求項 6 に記載のコンテンツ情報管理方法。

【請求項 9】

前記コンテンツ情報管理方法は、さらに、

前記ネットワークキーテーブルに新たな更新後ネットワークキーを格納する際に、該ネットワークキーテーブルに格納済みの複数の更新前ネットワークキーから、削除対象ネットワークキーの選択処理を実行し、該削除処理の完了を条件として前記更新後ネットワークキーのネットワークキーテーブルに対する格納処理を実行するステップを有することを特徴とする請求項 6 に記載のコンテンツ情報管理方法。

【請求項 10】

暗号化コンテンツと、暗号化コンテンツの復号に適用するコンテンツキーの暗号化データであり、前記ネットワーク接続デバイスとの共有キーとして設定され、適宜更新される

ネットワークキーによって暗号化された暗号化コンテンツキーとを記憶部に格納したコンテンツ提供サーバにおけるコンテンツ情報管理処理を実行するコンピュータ・プログラムであり、

前記記憶部に格納された暗号化コンテンツの利用処理の発生を条件として、利用処理対象のコンテンツに対応する暗号化コンテンツキーが更新後ネットワークキーと異なる更新前ネットワークキーによる暗号化コンテンツキーとして前記記憶部に格納されているか否かの判定処理を実行する判定処理ステップと、

前記判定処理ステップにおいて、利用処理対象のコンテンツに対応する暗号化コンテンツキーが更新後ネットワークキーと異なる更新前ネットワークキーによる暗号化コンテンツキーとして前記記憶部に格納されていると判定した場合に、該暗号化コンテンツキーを、更新後ネットワークキーを適用した暗号化コンテンツキーに更新する鍵架け替え処理を実行する鍵架け替え処理ステップと、

を有することを特徴とするコンピュータ・プログラム。