【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21年9月3日(2009.9.3)

【公表番号】特表2009-500766(P2009-500766A)
【公表日】平成21年1月8日(2009.1.8)
【年通号数】公開・登録公報2009-001
【出願番号】特願2008-521535(P2008-521535)
【国際特許分類】
Ｇ０６Ｆ　21/24　(2006.01)
Ｈ０４Ｎ　 7/167　(2006.01)
Ｇ０９Ｃ　 1/00　(2006.01)
Ｇ０６Ｆ　12/00　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　12/14　５６０Ａ
Ｈ０４Ｎ　 7/167　Ｚ
Ｇ０９Ｃ　 1/00　６６０Ｄ
Ｇ０６Ｆ　12/00　５３７Ｈ
Ｇ０６Ｆ　12/14　５４０Ａ
Ｇ０６Ｆ　12/14　５４０Ｂ
Ｇ０６Ｆ　12/14　５２０Ｄ

【手続補正書】
【提出日】平成21年7月13日(2009.7.13)
【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】
デジタルコンテンツを保護するコンピューティングシステムであって、
前記デジタルコンテンツを使用できる複数のコンテンツ保護システムを列挙するインクルージョンリストを含む前記デジタルコンテンツを復号化可能な第１コンテンツ保護システムと、
第２コンテンツ保護システムを含むアプリケーションに対して、前記第１コンテンツ保護システムの機能性へのアクセスを提供するリンク可能なライブラリと、
前記第２コンテンツ保護システムが前記インクルージョンリストにあるか否かを判断する手段と
を備えることを特徴とするシステム。
【請求項２】
前記コンテンツ保護システムと前記リンク可能なライブラリとを安全に結合させる手段をさらに備えることを特徴とする請求項１に記載のシステム。
【請求項３】
初期ベクトルを計算する手段であって、前記初期ベクトルは、前記第１コンテンツ保護システムと前記第２コンテンツ保護システムとの間で、共有手段を介して共有される、初期ベクトルを計算する手段をさらに備えることを特徴とする請求項１に記載のシステム。
【請求項４】
前記デジタルコンテンツのチャンクに基づいてソルト値を計算する手段であって、前記ソルト値は、一時暗号化鍵を生成する暗号ハッシュ手段を介して前記初期ベクトルと組み

合わせられる、計算する手段をさらに備えることを特徴とする請求項３に記載のシステム。
【請求項５】
前記一時暗号化鍵を使用して前記チャンクの一時暗号化を行う手段をさらに備えることを特徴とする請求項４に記載のシステム。
【請求項６】
前記第２コンテンツ保護システムに、一時暗号化された前記チャンクと、前記初期ベクトルと、前記ソルト値とを提供する手段をさらに備えることを特徴とする請求項５に記載のシステム。
【請求項７】
デジタルコンテンツを複写する方法であって、
前記デジタルコンテンツを、第１コンテンツ保護システムを介して復号化し、復号化デジタルコンテンツを生成する段階と、
一時暗号化鍵を生成し、前記一時暗号化鍵を使用して前記復号化デジタルコンテンツの一時暗号化を行う段階と、
前記一時暗号化鍵および一時暗号化されたデジタルコンテンツを前記第２コンテンツ保護システムに提供する段階と
を備えることを特徴とする方法。
【請求項８】
前記デジタルコンテンツの前記デジタルコンテンツを使用できる複数のコンテンツ保護システムを列挙するインクルージョンリストをチェックして、前記デジタルコンテンツが前記第２コンテンツ保護システムに複写できるか否かを判断する段階をさらに備えることを特徴とする請求項７に記載の方法。
【請求項９】
前記一時暗号化鍵は、初期ベクトルと、前記デジタルコンテンツのチャンクに基づいて計算されたソルト値とを暗号ハッシュすることにより生成されることを特徴とする請求項７に記載の方法。
【請求項１０】
デジタルコンテンツを保護する方法であって、前記方法は第１コンテンツ保護システムを備え、
前記第１コンテンツシステムは、
初期ベクトルを生成する段階と、
前記デジタルコンテンツのチャンクを復号化する段階と、
前記チャンクに基づいてソルト値を生成する段階と、
前記初期ベクトルと前記ソルト値とを暗号ハッシュして一時鍵を生成する段階と、
前記一時鍵を使用して前記チャンクを暗号化することにより、前記チャンクの一時暗号化を行う段階と
を備えることを特徴とする方法。
【請求項１１】
前記デジタルコンテンツは、前記デジタルコンテンツを使用できる複数のコンテンツ保護システムを列挙するインクルージョンリストを含むことを特徴とする請求項１０に記載の方法。
【請求項１２】
前記初期ベクトルは、乱数であることを特徴とする請求項１０に記載の方法。
【請求項１３】
前記ソルト値は、前記チャンクを使用して計算された数字であることを特徴とする請求項１０に記載の方法。
【請求項１４】
前記一時暗号化は、ストリーム暗号を使用して行われることを特徴とする請求項１０に記載の方法。

【請求項１５】
前記方法は、第２コンテンツ保護システムをさらに備え、前記第２コンテンツ保護システムは、
前記第１コンテンツ保護システムから暗号化初期ベクトルを受信する段階と、
前記初期ベクトルを復号化し、記憶する段階と、
前記第１コンテンツ保護システムから一時暗号化された前記チャンクを受信する段階と、
前記第１コンテンツ保護システムからソルト値を受信する段階と、
前記初期ベクトルと前記ソルト値とを暗号ハッシュして、前記一時鍵の複製を生成する段階と、
前記一時鍵の複製を使用して前記一時暗号化された前記チャンクを復号化する段階と
を備えることを特徴とする請求項１０に記載の方法。
【請求項１６】
前記第２コンテンツ保護システムは、前記デジタルコンテンツが含む前記デジタルコンテンツを使用できる複数のコンテンツ保護システムを列挙するインクルージョンリストに記載されていることを特徴とする請求項１５に記載の方法。
【請求項１７】
前記初期ベクトルは、前記第２コンテンツ保護システムにより提供された公開鍵を使用して、前記第１コンテンツ保護システムにより暗号化されることを特徴とする請求項１５に記載の方法。
【請求項１８】
前記暗号化初期ベクトルは、前記第２コンテンツ保護システムにより提供された秘密鍵を使用して、前記第２コンテンツ保護システムにより復号化されることを特徴とする請求項１５に記載の方法。
【請求項１９】
前記初期ベクトルは、安全な方法で記憶されることを特徴とする請求項１５に記載の方法。
【請求項２０】
前記方法は、コンピュータ可読記録媒体において具現化されることを特徴とする請求項１５に記載の方法。