オープン型電子出版 DRM 仕様案

1. 用語定義

使用する用語の定義を表 1 にまとめる。

表 1 オープン型電子出版 DRM 仕様案に関する用語定義

用語	定義
本システム	本実験で使用する DRM システム。DRM サーバと UI 内のモジュールで構成される。
DRM サーバ	本実験で使用する DRM サーバ。コンテンツを暗号化し、鍵を保管し、DRM 権限を管理する。
UI	コンテンツの閲覧用のアプリケーション。デバイス上で動作する。
コンテンツ	DRM で管理・保護する対象のデータ。主に電子出版を想定する。
ユーザー	ライセンスを保持する主体。所有しているデバイス上で UI を起動し、コンテンツを閲覧する。
デバイス	ユーザーが所有している PC、モバイル端末等。1 ユーザーが複数のデバイスを保持し、使用することを想定している。
ライセンス	ユーザーが保持している、コンテンツに対する権利。この権利を元に DRM 権限が設定される。

2. 想定するシステム構成

- DRM サーバ： 本システムのサーバ。コンテンツを暗号化し、暗号化鍵を保持し、DRM 権限を管理する。
- コンテンツサーバ： 外部のサーバ。コンテンツデータを保持する。
- デバイス： ユーザーが使用するデバイス。本システムの DRM モジュールが組み込まれた UI がインストールされている。

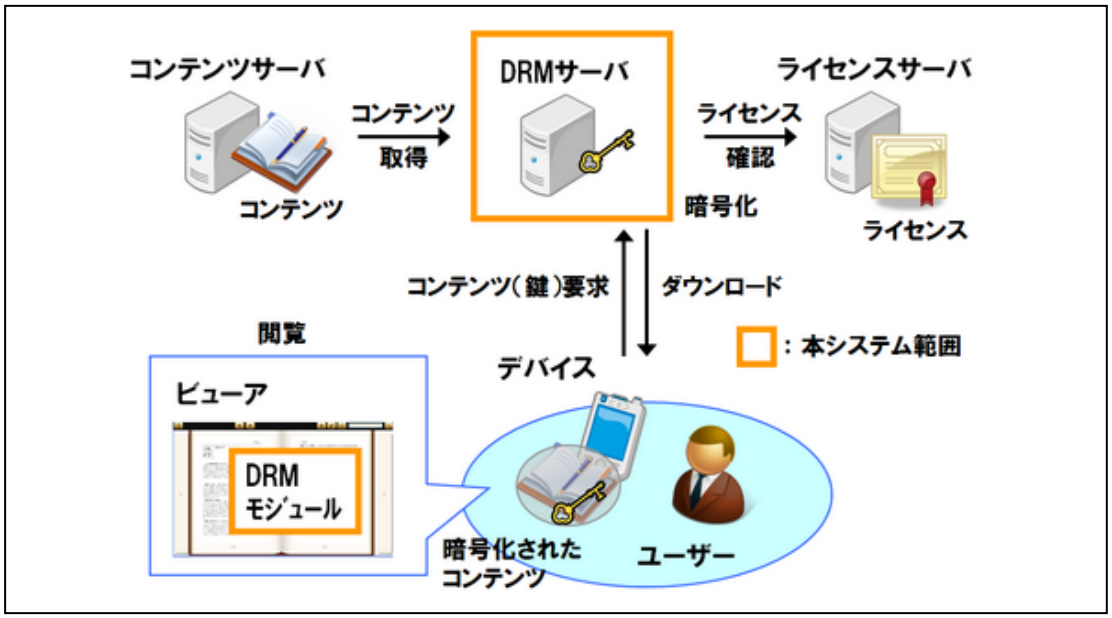

図 1 想定するシステム構成図

ユーザーがサーバからコンテンツをダウンロードして閲覧する場合、以下の処理が必要となる。

① ユーザーは、自分のデバイスでサーバにコンテンツ要求を送信する。
② DRM サーバは、要求されたコンテンツが要求したユーザー、デバイスで閲覧可能な場合、コンテンツのデータをコンテンツサーバより取得する。
③ DRM サーバにて、取得したコンテンツのデータを暗号化する。
④ デバイスにて、DRM サーバより暗号化されたコンテンツをダウンロードする。
⑤ DRM モジュールが組み込まれた UI にて、暗号化されたコンテンツを復号し閲覧する。

ユーザーが別の手段で取得した、暗号化されたコンテンツを閲覧する場合、以下の処理が必要となる。

① ユーザーは、自分のデバイスでサーバにコンテンツの復号鍵を送信する。
② DRM サーバは、要求されたコンテンツが要求したユーザー、デバイスで閲覧可能な場合、コンテンツの復号鍵を暗号化して用意する。
③ デバイスにて、DRM サーバより暗号化されたコンテンツの復号鍵をダウンロードする。
④ DRM モジュールが組み込まれた UI にて、暗号化されたコンテンツを復号し閲覧する。

3. 提供する機能

以下は、本システムが DRM サーバと UI 内のモジュールの連携によって提供する機能である。

（1） デバイス管理

ユーザーの使用するデバイスを管理し、デバイスごとにコンテンツの利用権限を管理する。

UI でのデバイス登録処理により、その UI が動作しているデバイスが、ユーザーに紐付いて登録される。

サービスによって１ユーザーで登録できるデバイスの最大台数を制限できる。

（2） コピープロテクト

コンテンツを暗号化することで、コンテンツのコピー対策を行う。

以下の３段階の強度を、コンテンツごとに設定できる。

- 強度１： コンテンツごとに異なる鍵で暗号化を行う。
  コンテンツを別のユーザーにコピーしても、UI があれば閲覧できる。
- 強度２： コンテンツごと、ユーザーごとに異なる鍵で暗号化を行う。
  同じユーザーであれば、コンテンツを別のデバイスに共有しても閲覧できる。
- 強度３： コンテンツごと、ユーザーごと、デバイスごとに異なる鍵で暗号化を行う。
  同じユーザーであっても、コンテンツを別のデバイスにコピーして使用できない。

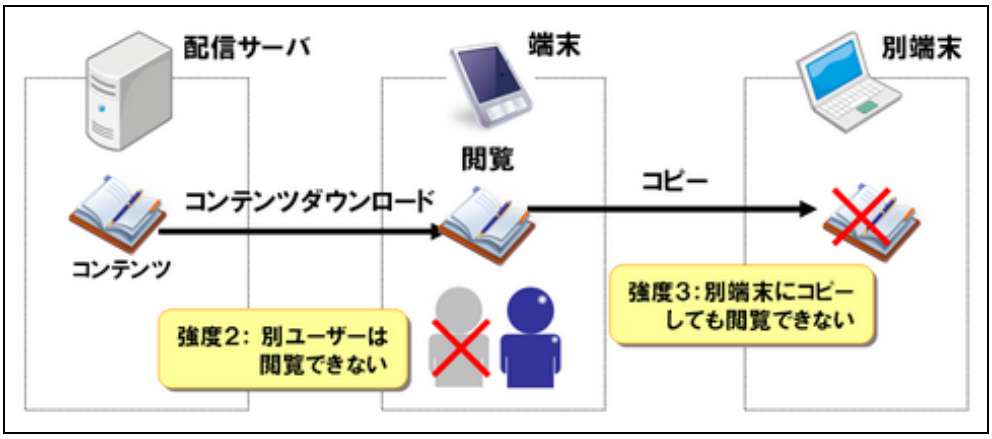

図 2 コピープロテクトの強度

（3） 権限設定

以下の権限が設定可能である。

- アクティベーション・オフライン閲覧

  次の 3 つから選択して設定可能。

・ オンラインのみ閲覧可能

・ オフラインで閲覧可能・要アクティベーション（アクティベーション期間の設定が可能）

  - 一定期間ごとにオンライン状態でサーバにライセンスの確認（＝アクティベーション）を行う必要がある。
  - コンテンツごとにアクティベーション期間を設定し、前回のアクティベーションからその期間以上経過すると、オフラインでの閲覧ができなくなる。

・ オフラインで閲覧可能・アクティベーション不要

- 閲覧期限

・ 制限あり（期間の設定が可能）

  制限を過ぎたコンテンツは閲覧できなくなる。UI 側で自動削除することも可能。

・ 制限なし

- 利用数制限

  システム全体でのライセンス発行数を制限する。図書館システム等で使用。

- 機能制限

・ テキスト・画像等のコピー（キャプチャ）

  コンテンツ内のテキスト、画像、表などのクリップボードへのコピーを制限する。

  - 可能
  - 禁止

・ 印刷

  コンテンツの紙への印刷を制限する。

  - 可能
  - 禁止

・ 自動読上げ（TTS）機能

  - 可能
  - 禁止

（4） コンテンツの認証

本システムでは、電子署名を使用し、コンテンツが本システムによって生成された真正のコンテンツであることを確認できる。

以下の改ざんの検知が可能である。

- コンテンツの中身の改ざん
- メタデータの改ざん
- メタデータとコンテンツの対応の改ざん

（5） ログ送信

以下のログを、UI から DRM サーバに送信する。

- コンテンツダウンロード完了ログ： コンテンツのダウンロードが完了した場合に送信する。
- コンテンツ表示ログ： コンテンツが正しく復号された場合に、その旨を送信する。
  ダウンロード後 1 回のみなど、頻度を設定可能。
- コンテンツ削除ログ： 期限切れのコンテンツを削除した場合に、その旨を送信する。

4. UIとの連携について

本 DRM モジュールは、そのオープンな仕様上、DRM モジュールのみではその機能が完結できず、以下の機能について、UI 側で対応する必要がある。

- 期限切れコンテンツの削除
  期限が切れたコンテンツを、ローカルストレージから削除し、削除したことを DRM モジュールに通知する。
- テキストコピー権限
  テキストコピー可能かを、DRM モジュールに問い合わせ、その結果によって機能の可否を切り替える。
- 印刷権限
  印刷可能かを、DRM モジュールに問い合わせ、その結果によって機能の可否を切り替える。

5. 使用する暗号技術

CRYPTRECの「電子政府推奨暗号リスト[1]」に準ずる、以下の技術を使用する。

- 暗号化：AES 暗号
- 電子署名：鍵長 2048 ビットの RSA 暗号
- ハッシュ関数：SHA256

[1] http://www.cryptrec.go.jp/list.html