Vol.2011-IFAT-104 No.5
2011/11/22

電子ブックのグループ閲覧を可能にする PKI を活用した DRM 機能の実装

山地一禎[†] 中村素典[†] 西村 健[†] 大谷 誠[†] 曽根原 登[††]

大学では，全学的な図書館だけなく，キャンパス，学部，研究室など様々なレベルで図書が購入され共有されている．こうした利用形態を電子ブックの利用においても実現することは，その利用促進に向けての重要な鍵となる．電子ブックの閲覧方式には，ウェブブラウザを利用するサーバサイド方式と，コンテンツをダウンロードして利用するクライアント方式に大別できる．本研究では，後者のクライアント方式において，電子ブックの閲覧を所属レベルで制御可能な方法を提案した．所属情報には，学認において，大学の認証システムから送信される属性と，メンバー属性プロバイダから送信させる属性を利用した．この属性情報に基づいたクライアント証明書を発行し，電子ブックの PDF ファイルを暗号化するプラットフォームを構築した．PDF の標準仕様活用した DRM 機能により，特殊なアプリケーションを用意することなく，普段利用している PDF ビューアを用いて，電子ブックのセキュアなグループ閲覧を実現することに成功した．

Development of PKI based DRM enabling eBook sharing within authenticated groups.

Kazutsuna Yamaji[†], Motonori Nakamura[†], Takeshi Nishimura[†], Makoto Ohtani and Noboru Sonehara[††]

In universities, books are purchased and shared by the variety of organizations such as individual labs or departments, or the broader campus, in addition to the main campus library. Students and researchers benefit when the e-book platform allows access to materials for the right campus members from the right organizations. In general, there are two ways to read an e-book. One, the server side method, utilizes a web browser. The other, the client method, requires specific e-book reader applications. This study focuses on the latter client method and proposes a way to control e-book access depending on the different affiliation levels. The system developed in this study is based on the academic access management federation, GakuNin. Attributes from university IdP's and other GakuNin member attribute providers are employed as trusted user data. The PDF file that contains the e-book is encrypted using a client certificate, for which the corresponding private key is available only to users with the proper membership in the right campus organization. The system is entirely standards-based, so there is no need for modification of the client or installation of a new application.

1. はじめに

現在ではいくつかの大学図書館において, NetLibrary 1)や ebrary 2)などの電子ブックプラットフォームの利用が進んでいる．図書館向けのサービスは，従来の電子ジャーナルのようにダウンロードしたファイルに閲覧制限をかけない利用モデルと，特殊なクライアントアプリケーションやウェブによる閲覧で閲覧制限をかける利用モデルに大別できる．前者は，利用者にとっては便利である反面，大学等で利用される単価の高い学術書や専門書を提供する出版社にとっては，不正利用に対するリスクが高い．これに対し後者の利用モデルは，アクセス制御のための特別な運用・利用方法を必要とするものの，出版社が安心してコンテンツを提供できるというメリットがある．

大学では，全学的な図書館だけなく，キャンパス，学部，研究室など様々なレベルで図書が購入され, 共有されている. こうした所属レベルで購入された従来の図書は，購入者の優先利用の権利を維持しつつ，できるだけ多くの利用者が参照できるよう幅広く融通し合う形で運用が行われており，そのための図書の蔵書管理を行うことが図書館の役割の一つである．一方，電子ブックの流通プラットフォームは，大学全体としての機関契約と機関認証をするにとどまり，これまで紙媒体で実現できていた異なる所属レベルでの利用モデルさえも反映できていない．これは，電子ブックプラットフォームのアクセス制御が, 従来ながらの IP アドレスによる認証という非常に大まかな認証レベルにとどまっていることに起因する 3)．こうしたアクセス制御機能の不足は，利用者にとって電子ブック利用の不便さを強調し，大学における電子ブックの契約ならびに利用促進に対し，大きなマイナス要因となる．電子ブック利用を促進するためには，キャンパス，学部，学科，研究室，さらには機関をまたがった研究プロジェクト等，利用者の様々な粒度の所属レベルに応じて電子ブックへのアクセス権を柔軟にコントロールできる，新しい認証・認可技術の実現と導入が重要な要素となるものと考えられる．

国立情報学研究所では，全国的な最先端学術情報基盤整備の一環として，学術認証フェデレーション「学認：GakuNin」の構築に取り組んでいる 4)．学認に参加することにより，学術向け Web サービスに、大学の認証情報を利用してログインすることができる．さらに，学認では認証時に所属情報など，ユーザに関する属性情報をサービス側に提示できる仕組みも提供する．この仕組みを利用することで，Web サービス側では，大学の認証システムから受け取ったユーザの属性情報に基づいてアクセス制御を実現することができる．これまでに我々は，学認における属性をさらに柔軟に扱う

[†] 国立情報学研究所　学術ネットワーク研究開発センター
Research and Development Center for Academic Networks, National Institute of Informatics
[††] 国立情報学研究所　情報社会相関研究系
Information and Society Research Division, National Institute of Informatics

ことができる，メンバ属性プロバイダシステムを構築してきた 5)．このシステムから送信される属性情報を活用することで，紙媒体で実現できていた異なる所属レベルでの利用モデルを，電子ブックプラットフォームにおいても実現することが原理的に可能となる．さらに，これまで困難であった大学横断型のグループによる電子ブックの購入や閲覧にも活用することが可能となる．ただし，そうした認可判断が簡便に行えるのは，Web ベース上で電子ブックを閲覧する場合に限られていた．電子ブックデータをダウンロードして閲覧するには，メンバ属性プロバイダシステムから送信される属性情報を，オフラインにおけるアクセス制御，すなわち，Digital Rights Management（DRM）機能と連携させる必要がある．そこで本研究では，学認におけるメンバ属性プロバイダシステムからの属性情報を活用した DRM システムを開発することで、この問題を解決することを目的とする．

2. 学術認証フェデレーションとメンバ属性プロバイダシステム

2.1 学術認証フェデレーションの仕組みと属性

学認は，図 1 に示したように，ID を管理する ID プロバイダ（IdP），サービスを提供するサービスプロバイダ（SP），エンドユーザに対して利用する IdP の選択画面を提示するディスカバリサービス（DS）と呼ばれるシステムから構成される．多くの場合，IdP は，大学や研究機関といった学術機関により構築・運用されている．SP は，商用出版社が提供する電子ジャーナルなどを主として，大学が提供する e-learning サイトや研究者コミュニティが提供するデータベースなど，その種類は多岐にわたる．認証や属性交換のプロトコルとしては，SAML (Security Assertion Markup Language) 2.0 6)を採用している．SAML による通信を実現するための IdP や SP としては，米国 Internet2 が開発したミドルウエア Shibboleth 7)を主として使用する．

認証を受けるためには，まず，SP でのログインのリンク先として設定されている DS において，ユーザの所属機関の IdP を選択する．IdP での認証が完了すると，IdP は，SP に対して認証の結果と SP が必要とする属性を送信する．SP はこの属性情報に応じてユーザのアクセスレベルを設定し，サービスを提供する．従来，学術認証フェデレーションで推奨されている属性は，表 1 に示す 16 種類である 8)．

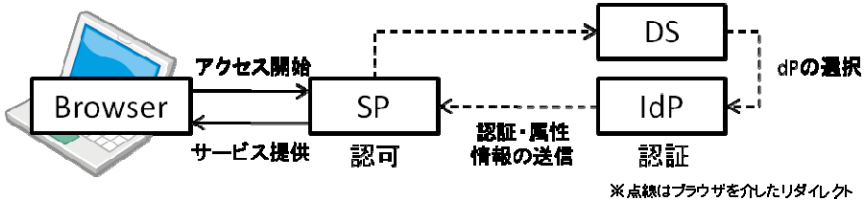

図 1 学認における認証プロセスの概略

表 1 学認で利用されている属性一覧 8)

1	mail	電子メールアドレス
2	sn	氏名（姓）の英語表記
3	o	組織名称を英語表記
4	ou	組織内所属名称を英語表記
5	givenName	氏名（名）を英語表記
6	displayName	表示名の英語表記
7	eduPersonAffiliation	利用者が所属する組織内での職種
8	eduPersonPrincipalName	フェデレーション内で一意な，かつ，永続的な利用者識別子
9	eduPersonEntitlement	特定のアプリケーションを利用する資格情報
10	eduPersonScopedAffiliation	利用者が所属する組織内での職種のスコープ付き表記
11	eduPersonTargetedID	フェ デレーション内で一意な，かつ，SP サイト毎に異なる利用者識別子
12	jasn	氏名（姓）の日本語表記
13	jaGivenName	氏名（名）を日本語表記
14	jaDisplayName	表示名の日本語表記
15	jao	組織名称を日本語表記
16	jaou	組織内所属名称を日本語表記

2.2 メンバー属性プロバイダシステム

表 1 における 4 の ou，その日本語表記である 16 の jaou を利用すると，利用者の所属に関する情報を細かく記述することが可能である．しかしながら，そうしたユーザ属性を IdP で管理している例は少ない．これは，一般的に 1 組織に 1 つの IdP では，学科等のより細やかな分類が集約的に管理されていないことが原因として考えられる．あるいは，大学内において，細分化したグループを管理する管理主体が，IdP の管理主体と異なることにより，IdP の属性として提供されていないという原因も考えられる 4)．これに対し，メンバ属性プロバイダ：GakuNin mAP では，IdP での情報管理とは独立に，管理主体によるグループ属性の付与を可能にする．大学内における研究室などを 1 つのグループとみなせば，大学の IdP から提供されていない異なるレベルの所属情報を，GakuNin mAP を用いて SP に提供することができる．また，大学内に限らず，機関を横断した構成員から成るグループ属性を，GakuNin mAP から提供することも可能である．

GakuNin mAP では，図 1 に示す通常の IdP と SP による認証時に，利用者の ID を属性として送信することを前提とする．ID には，表 1 における 8 の eduPersonPrincipalName を利用する．その利用者 ID を用いて，バックチャネルと呼ぶブラウザを介さない直接通信により SP から GakuNin mAP に通信し，isMemberOf として表現されるメンバ属性を送受信する．バックチャネルによる属性要求機能は，最近の Shibboleth ソフトウエアでは標準で実装されているため，比較的容易に SP 側で GakuNin mAP に対応することが可能である 9)．

GakuNin mAP の概念図を図 2 に示す．GakuNin mAP では，グループの階層化を表現することができる．電子ジャーナルや電子ブックといった，出版社等との契約に基づく認可判断が必要な場合，様々な契約形態をグループ管理上に反映させる必要がある．例えば，複数の大学の学部等の組織同士がコンソーシアムという形でつながり，コンソーシアムが主体となって出版社と契約を結ぶような形態を考えたとすると，コンソーシアムはサービスを提供する SP 側というより大学，つまり ID を管理する IdP 側の組織であり，SP に対してはコンソーシアムという一つのグループとして見せることが合理的である．各学部がそれぞれ独立したグループとして表現されるとすると，その上位グループとしてコンソーシアムに対応するメタグループを定義することができると都合が良い．すなわち，2 階層のグループ構造が構成されることになる．図 2 におけるメタグループ M がコンソーシアムに対応するグループとなる．SP と SP グループとの紐付けは当該 SP 管理者のみが可能となっており，契約に基づいたグループの管理・許可を SP 側でコントロールできる仕組みが提供されている．

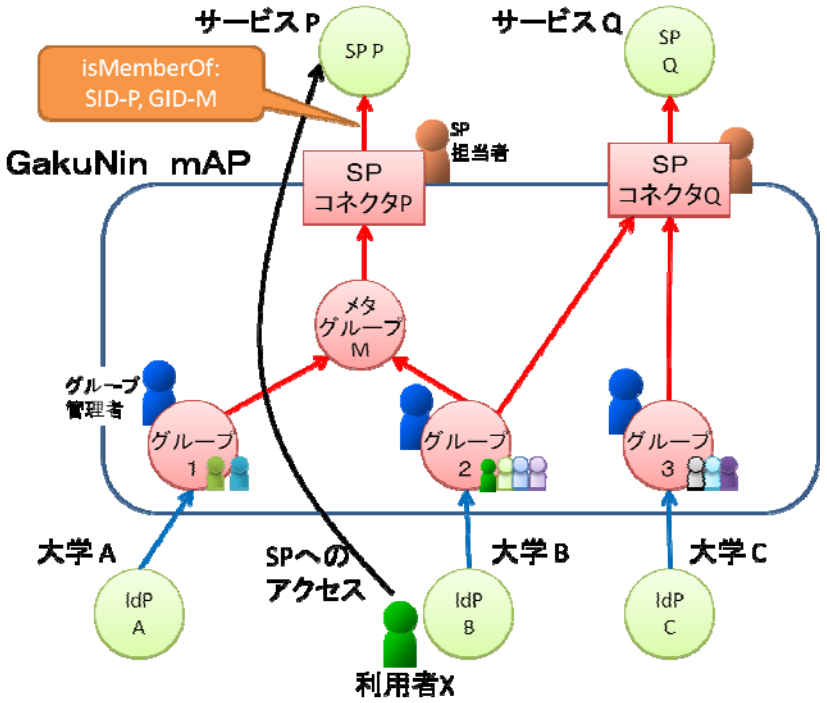

図 2 GakuNin mAP 概念図

GakuNin mAP から送信される属性を利用することで，ウェブブラウザを利用するサーバサイド方式による電子ブックの閲覧に関しては，容易に利用者の所属レベル，すなわち，契約状態に基づいた柔軟なアクセス制御を行うことができる．一方，コンテンツをダウンロードして利用するクライアント方式では，アクセス制御の鍵となるグループ属性の情報を，何らかの方法でクライアント側に取得し，それを用いた DRM を実現する必要がある．

3. PKI を活用した DRM 機能

一般的に，DRM に関する技術としては，不正コピーを防止するコピーガード技術や，コンテンツの流通自体を管理する技術も含まれるが 10)，ここでは，電子ブック利用のためのコンテンツ保護に関する DRM 技術を検討する．コンテンツを保護する方法としては，基本的には，暗号化と復号の組み合わせによりシステムが実現される．暗号化されたコンテンツを復号するための鍵は，クライアントとなるアプリケーションやデバイスに組み込まれて利用される．近年の電子ブックの展開は，DRM の導入の必要性も含めてデバイス主導型で進められてきたが 11)，利用の即時性や利便性などを考慮すると，特別な電子ブックリーダを必要とせずにコンテンツを閲覧できることは，電子ブックの普及において重要な要素の一つとなる．そこで本研究では，広く閲覧アプリケーションが普及している PDF リーダにおいて，プラグイン等の特別な付加機能を導入することなく DRM として利用できる PKI を用いた暗号化に注目し，GakuNin mAP から送信されるグループ属性と連動させるシステムの構築に取り組んだ．

3.1 PKI を利用する DRM のメリットとデメリット

本研究では，PDF ファイルを X.509 証明書の公開鍵を使って暗号化することで，秘密鍵がインストールされた端末でのみ閲覧可能な PDF ファイルを生成し，DRM 機能を実現する．この方法のメリットとデメリットをまとめると，以下のようになる．

3.1.1 PKI による DRM 方式のメリット

- 一般の DRM システムでは，ドキュメントの閲覧鍵はクライアント上の独自領域またはサーバに格納される．この DRM の仕組みが分かることにより閲覧鍵のコピーが可能となるために，一般の DRM システムでは詳細仕様は公開されていない．すなわち，独自の仕組みを構築する必要がある．これに対し，証明書ベースの DRM システムでは Windows 環境においては標準で管理されている証明書と秘密鍵（閲覧鍵）を利用し，秘密鍵の保管については Windows 標準の証明書ストアの機能で実現できる．従って，仕組みを秘密にする必要がない．
- PDF では，証明書ベースの暗号化の仕組みが標準化されている 12)．最も普及している PDF ビューアである Adobe 社の Acrobat や Reader が，標準パッケージで対応しており，DRM のビューアとして利用できる．
- 一般の DRM システムを Acrobat や Reader で使う場合には独自のプラグインを提供する必要があり，ライセンスの問題を解決する必要がある．一方，上記の利点で述べたように証明書ベースの DRM システムでは標準機能を利用するだけなので，ライセンス的な問題が発生せず手軽に利用できる．
- PDF の暗号化は標準仕様であるためにクライアントとして Windows 以外の環境へ展開できる可能性がある．ただし，PKI 暗号対応の PDF ビューアが必要である．
- 証明書と秘密鍵のペアを個人ではなく，組織やグループ単位で関連付けることで，研究室や組織単位内でのみ閲覧可能なドキュメントが実現できる．
- 複数の秘密鍵指定による暗号化と，個別の権限指定も可能である．同じ暗号化 PDF ファイルを複数人で共有し，異なる権限で閲覧可能なドキュメントが実現できる．

3.1.2 PKI による DRM 方式のデメリット

- 証明書に関連付けられる秘密鍵（閲覧鍵）は Windows 標準の証明書ストアの場合にはエクスポート（取り出し）を不可能にすることができるが，MacOS-X のキーチェーン等ではエクスポートが可能である．したがって，Windows 以外の MacOS-X やスマートフォンでは秘密鍵の管理方法を別途検討する必要がある．
- 証明書と秘密鍵の管理自体は Windows 標準の証明書ストアで行なえるが，証明書と秘密鍵をブラウザを介して簡便に導入する仕組みを用意する必要がある（本研究では Java アプレットを利用）．証明書ストアにアクセスするためには，ブラウザの管理者権限が必要になる．
- 証明書には有効期限が設定されているが，現状で Acrobat や Reader ではこの期限は利用されていない．このために，ドキュメントの利用期限は別途方式を考える必要がある．例えばサーバと連携して証明書と秘密鍵を削除する仕組みが必要となる．

3.2 システム構成と処理の流れ

システム構成図と DRM 処理の流れを図 3 に示す．SAML で認証連携を行い，IdP や GakuNin mAP から属性を取得する SP の機能は，Shibboleth SP Ver.2.4 を利用した．リポジトリ部には，汎用リポジトリシステム WEKO Ver.1.6 13) を使用し，本研究で開発した DRM サーバとの通信やブラウザへのアプレットの提供ができるようにカスタマイズした．

システムは，秘密鍵と証明書（公開鍵）の生成と管理および PDF ファイルの暗号化を行なう DRM サーバと，秘密鍵を閲覧端末にインストールする DRM クライアントで構成される．DRM サーバは，利用するライブラリ（アンテナハウス製 PDF 電子署名モジュール 14) ）の制限により Windows サーバを利用した．DRM クライアントは，エンドユーザの利用するクライアントの端末にはインストールせずに利用可能とするために Java のアプレットを採用した．

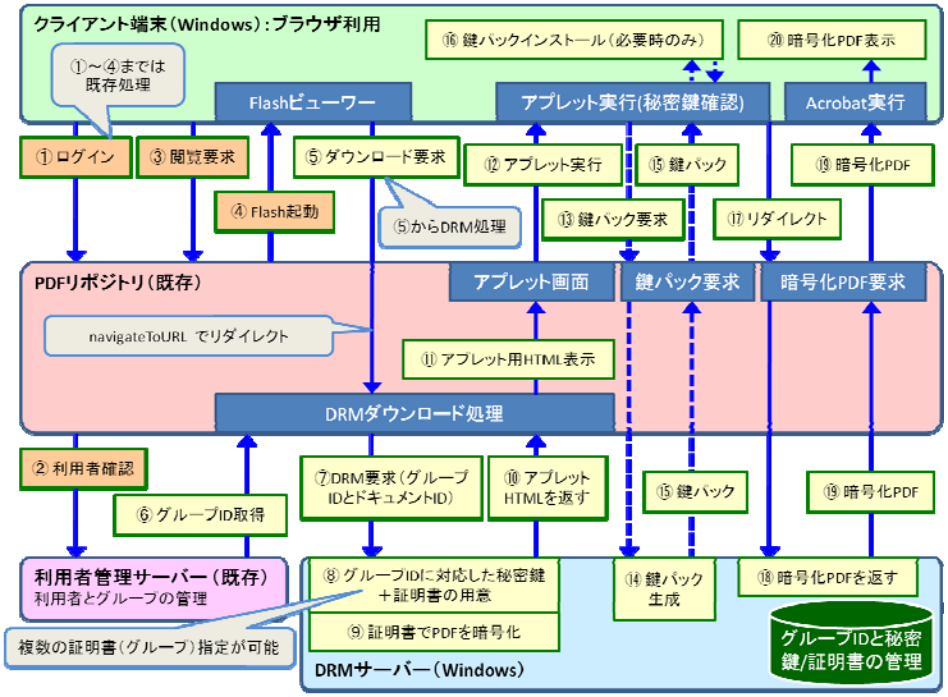

図 3 システム構成図と DRM 処理の流れ

表 2 DRM 処理における各ステップの説明

No.	機能	補足
①	ログイン	既存のログイン処理 1
②	利用者確認	既存のログイン処理 2
③	閲覧要求	既存の閲覧処理 1
④	Flash 起動	既存の閲覧処理 2
⑤	ダウンロード要求	Flash で「ダウンロード」ボタンをクリック リダイレクト処理により DRM ダウンロード処理を起動
⑥	グループ ID 取得	利用者の所属するグループ ID を取得する
⑦	グループ ID とドキュメント ID を指定し DRM 要求	グループ ID（複数指定可能）とドキュメント ID（1 つのみ）を指定して DRM サーバに暗号化要求を行う
⑧	グループ ID に対応した秘密鍵＋証明書の用意	DRM サーバはまずグループ ID に対応した秘密鍵＋証明書が生成済みかどうかチェック 未生成なら生成して DB（今回はファイル名を使った簡易なもの）に登録する
⑨	グループ ID に対応した証明書で PDF を暗号化	グループ ID に対応した証明書（公開鍵）を使って（複数指定可能）PDF 1 つを暗号化して一時ファイルとして出力
⑩	アプレット HTML を返す	鍵情報とセッション ID を含んだアプレット HTML を返す
⑪	アプレット HTML 表示	取得したアプレット HTML をクライアントに表示させる
⑫	アプレットの実行	クライアントのブラウザに表示された HTML よりアプレットを実行され、未インストールの鍵があれば⑬に無ければ⑰へ
⑬	鍵パックの要求（必要時）	未インストール鍵のグループ ID で要求
⑭	鍵パック生成（必要時）	要求グループ ID 独自形式の鍵パック（PKCS# 12 形式の秘密鍵＋証明書）にまとめる
⑮	鍵パック（必要時）	⑭で生成した鍵パックをアプレットに返す
⑯	鍵パックインストール（必要時）	入手した鍵パックをインストール
⑰	リダイレクト	セッション ID により PDF 要求 URL へ移動
⑱	暗号化 PDF を返す	セッション ID で暗号化済みの PDF を返し、PDF は不要になるので削除する
⑲	暗号化 PDF	⑱の暗号化済み PDF をクライアントに返す
⑳	暗号化 PDF 表示	ブラウザにダウンロードされ、Arobat や Reader で開いた際にインストールされた秘密鍵でファイルを開く

表 2 に，DRM 処理における各ステップの詳細説明を示す．ここで，⑧⑨⑭⑮⑱⑲が DRM サーバの処理となり，⑫⑬⑯⑰がクライアントのアプレットの処理となる．

3.3 実証実験

実験では，実際に図 3 に示した全てのシステムを構成し，PKI を用いた DRM 機能の動作実証を行った．図中①～④の操作を通して，以下の一連のフローが正常に動作することを確認できた．また，秘密鍵がインストールされていない PC 上では，同 PDF が復号できないことも同時に確認した．

1. GakuNin mAP から取得した isMemberOf 属性に基づいて X.509 証明書を作成
2. 作成した証明書の秘密鍵を Java アプレットを用いて Windows の証明書ストアにインストール
3. 公開鍵で暗号化した PDF をダウンロード
4. 秘密鍵がインストールされた PC 上で暗号化された PDF を復号し閲覧

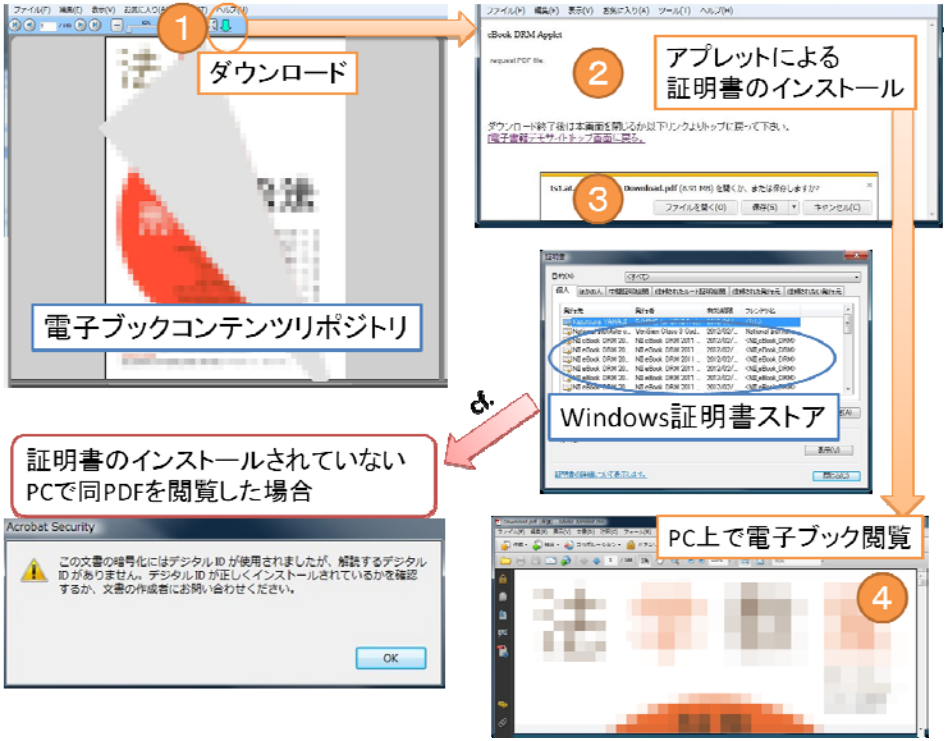

図 4 利用時の画面遷移例

4. おわりに

本研究では，様々な所属レベルで購入された電子ブックのコンテンツ保護を実現し，かつ，簡便に利用できる DRM システムの構築に取り組み，実験にてその利用フローの検証を行った．今後は，Windows 以外の MacOS-X やスマートフォンにおける秘密鍵の管理方法や有効期限に対する検討を更に進める予定である．今回は，PKI を用いた暗号化技術を，電子ブックの PDF ファイルに対する DRM 機能として実装したが，こうした技術は，より一般的にグループ間で共有されるコンテンツの保護にも派生的に利用することができる．現在，GakuNin mAP に接続されている Web アプリケーションには，wiki，メーリングリスト，スケジュール調整やファイル共有などのコラボレーションツールがある．その中でも，コンテンツをクライアント PC に保存する利用形態では，本研究で採用したグループに対する証明書を利用する方法が活用できる可能性がある．例えば，メーリングリストやファイル共有などでは，コンテンツ保護のための暗号化技術として採用できるものと考えられる．最近では，研究を進める過程において，研究者間でのデータ共有などが積極的に進められている．GakuNin mAP は，こうしたコラボレーションを円滑に行うための基礎基盤である．その際に，共有される研究・教育コンテンツをセキュアに保護する技術としても，グループ属性に対する証明書を最大限に活用し，本研究の成果の更なる展開として，検討を進めていきたいと考えている．

謝辞 本研究は，総務省「新 ICT 利活用サービス創出支援事業」における「研究・教育機関における電子ブック利用拡大のための環境整備」の一環として実施されたものである．関係各位に感謝する．

参考文献

1) NetLibrary, http://www.netlibrary.com/, 2011-10-04 last accessed.
2) ebrary, http://www.ebrary.com/, 2011-10-04 last accessed.
3) 野田英明，吉田幸苗，井上敏宏，片岡 真，阿蘇品治夫: Shibboleth 認証で変わる学術情報アクセス，カレントアウェアネス, Vol. 307, pp.407 (2011)
4) 学術認証フェデレーション：学認 GakuNin, http://www.gakunin.jp/, 2011-10-04 last accessed.
5) 西村 健，中村素典，井上 仁，山地一禎，曽根原 登: 電子書籍閲覧における組織横断型認証のためのグループ管理，情報処理学会研究報告, Vol.2011-IFAT-102, No.5, pp.1-6 (2011)
6) Security Assertion Markup Language (SAML) V2.0, http://saml.xml.org/saml-specifications, 2011-10-05 last accessed.
7) Shibboleth, http://shibboleth.internet2.edu/, 2011-10-04 last accessed.
8) 学術認証フェデレーション システム運用基準 (Ver.1.2), https://www.gakunin.jp/docs/files/GakuNin_System_SpecV1.2.pdf, 2011-10-06 last accessed.
9) SimpleAggregationAttributeResolver, https://wiki.shibboleth.net/confluence/display/SHIB2/NativeSPAttributeResolver#NativeSPAttributeResolver-SimpleAggregationAttributeResolver(Version2.2andAbove), 2011-10-04 last accessed.
10) 関 亜紀子，飯田 陽一: 安全性と利便性からみた DRM 方式の比較評価に関する一考察, Vol. 2011-EIP-51, No.7, pp.1-7 (2011)
11) 藤原隆弘，西 啓: デバイスが変える電子書籍の流通と利用者の行動，情報管理, Vol.54, No.2, pp.63-72 (2011)
12) Document management -- Portable document format -- Part 1: PDF 1.7, http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502, 2011-10-05 last accessed.
13) 山地一禎，青山俊弘，武田英明: 学術資源共有基盤 WEKO の開発，ディジタル図書館, Vol.36, pp.51-61 (2009)
14) アンテナハウス社 PDF 電子署名モジュール, http://www.antenna.co.jp/psg/, 2011-10-04 last accessed.