A Data Usability Company
アンテナハウス

システム製品活用事例　紹介
・サーバベース・コンバータ（SBC）
・PDF 電子署名モジュール

学認を利用した電子ブック利用基盤の実現

～PDF の証明書による暗号化(DRM)を利用した文書閲覧～

○ はじめに

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が、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、実証実験を行った。実証実験は、**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。成果は公開（http://ebook.nii.ac.jp/）されている。

これまでのクライアント方式による図書館向けのサービスでは、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、暗号化と DRM(Digital Rights Management)を使った、専用のクライアントアプリケーションやウェブによる閲覧制限をかける利用モデルに大別できた。**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、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**があるもの、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**デメリット**があった。いずれのモデルも一長一短あり、容易な運用・利用方法でかつコンテンツを守れる仕組みが望まれている。

国立情報学研究所では、現在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。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している。この学認の仕組みと属性情報を利用した**PDF 暗号化**により DRM を実現することで、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した。これにより認証と連携した、特別な仕組みが必要ない、オフライン時の DRM の仕組みが実現できた。

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き、各クライアント用に証明書(X.509 形式の証明書)と秘密鍵を発行し、証明書に含まれる公開鍵を利用して電子ブックの PDF ファイルを暗号化するプラットフォームを構築した。証明書と秘密鍵は，自動的にクライアントにインストールされる。閲覧時には証明書に紐付いた秘密鍵を保有したクライアントでのみ閲覧が可能となる。**PDF の証明書による暗号化は、ISO 仕様書や PDF Reference にも書かれた PDF の標準仕様であり、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。**

電子ブックの購入と閲覧の手順は、まずサーバサイドにおいて Flash 変換されたコンテンツを閲覧し、ダウンロード要求ボタンがクリックされることで、証明書の発行・インストールを行った後に、暗号化された PDF をダウンロードして閲覧する。ダウンロードされた PDF ファイルは、オフライン状態でも許可されたクライアントでのみ閲覧が可能となる。証明書をコントロールすることで、PDF の閲覧権限のコントロールを実現した。

○ 学術認証フェデレーション（学認）

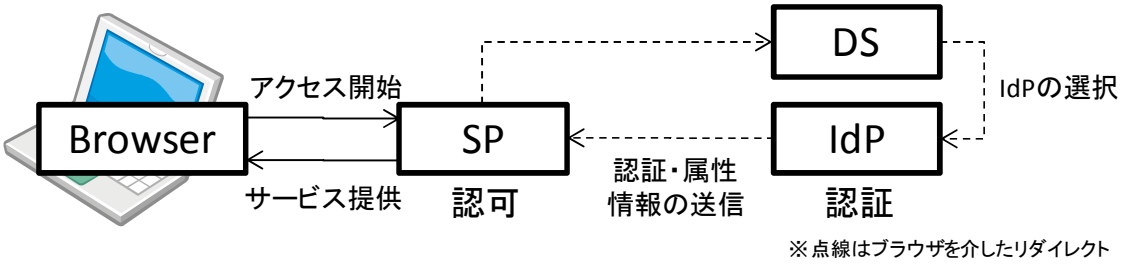

図１　学認における認証プロセスの概略

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。

学認サイト　https://www.gakunin.jp/

○ メンバー属性プロバイダシステム

学認の IdP で利用されている属性により、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、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。

これに対し、メンバー属性プロバイダ : 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。このように認証（IdP）と属性プロバイダ（GakuNin mAP）を分離することで組織間にまたがった属性管理を実現している。

GakuNin mAP　https://map.gakunin.nii.ac.jp/map/

○ 証明書による DRM 方式のメリットとデメリット

※ 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。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。ただし証明書による暗号対応の 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。**

※ 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、証明書と秘密鍵は，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 Adobe 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。

○ 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 2 に示す。SAML で認証連携を行い、IdP や GakuNin mAP(メンバー属性プロバイダ)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 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。汎用リポジトリシステム WEKO では**アンテナハウス社のサーバベース・コンバータ（SBC）を利用してコンテンツを Flash 変換して，専用の Flash ビューアを使ってプレビューに利用している。**

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（アンテナハウス社の PDF 電子署名モジ**

ュール）の都合により 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。DRM の仕組みはラング・エッジ社が開発を担当した。

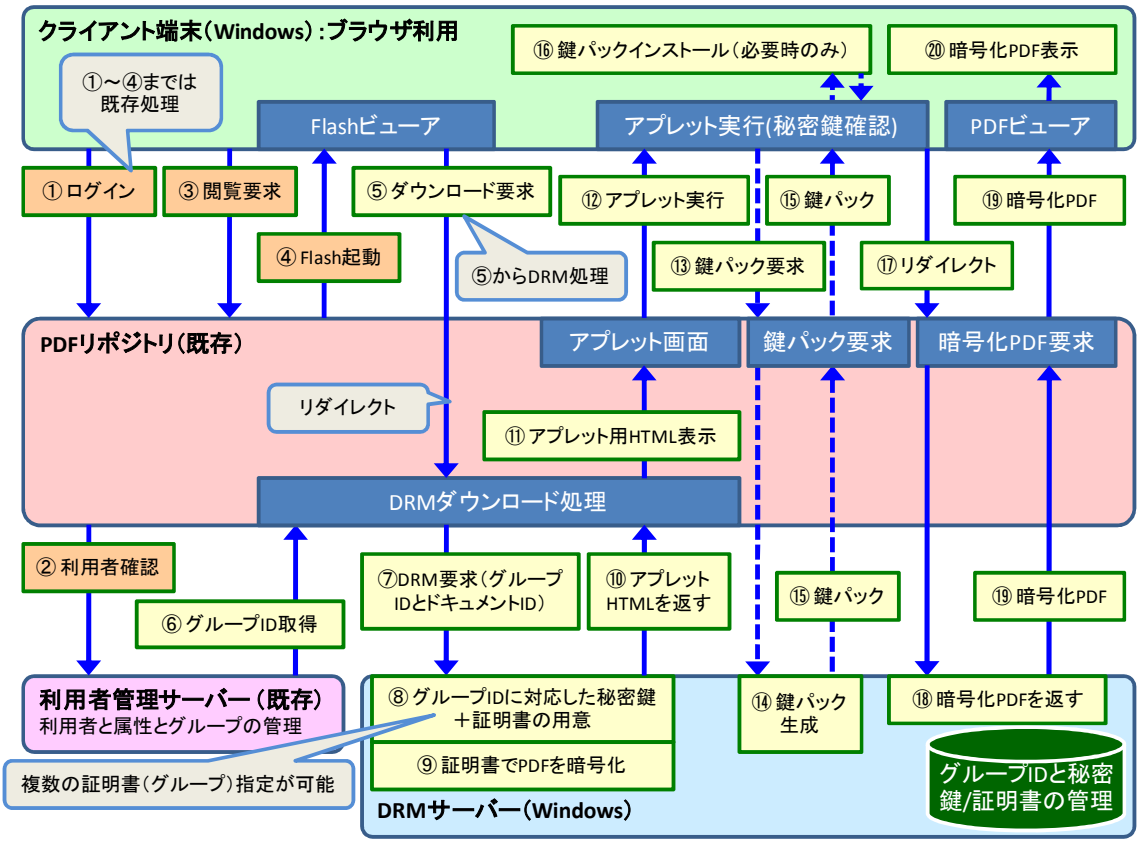

図２：システム構成図と処理の流れ

○ 利用時の画面遷移例

実験では、実際に図 2 に示した全てのシステムを構成し、証明書を用いた DRM 機能の動作実証を行った。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。実際の利用時の画面遷移例を図 3 に示す。

1. Flash 変換された電子ブックの Flash ビューアによるプレビューとダウンロード開始
2. GakuNin から取得した所属属性に基づいて X.509 証明書と秘密鍵を生成し、Java アプレットを用いて Windows 証明書ストアにインストール
3. リダイレクトにより、証明書（公開鍵）で暗号化した PDF ファイルをダウンロード
4. 証明書と秘密鍵がインストールされた PC 上で暗号化された PDF を復号し閲覧可能

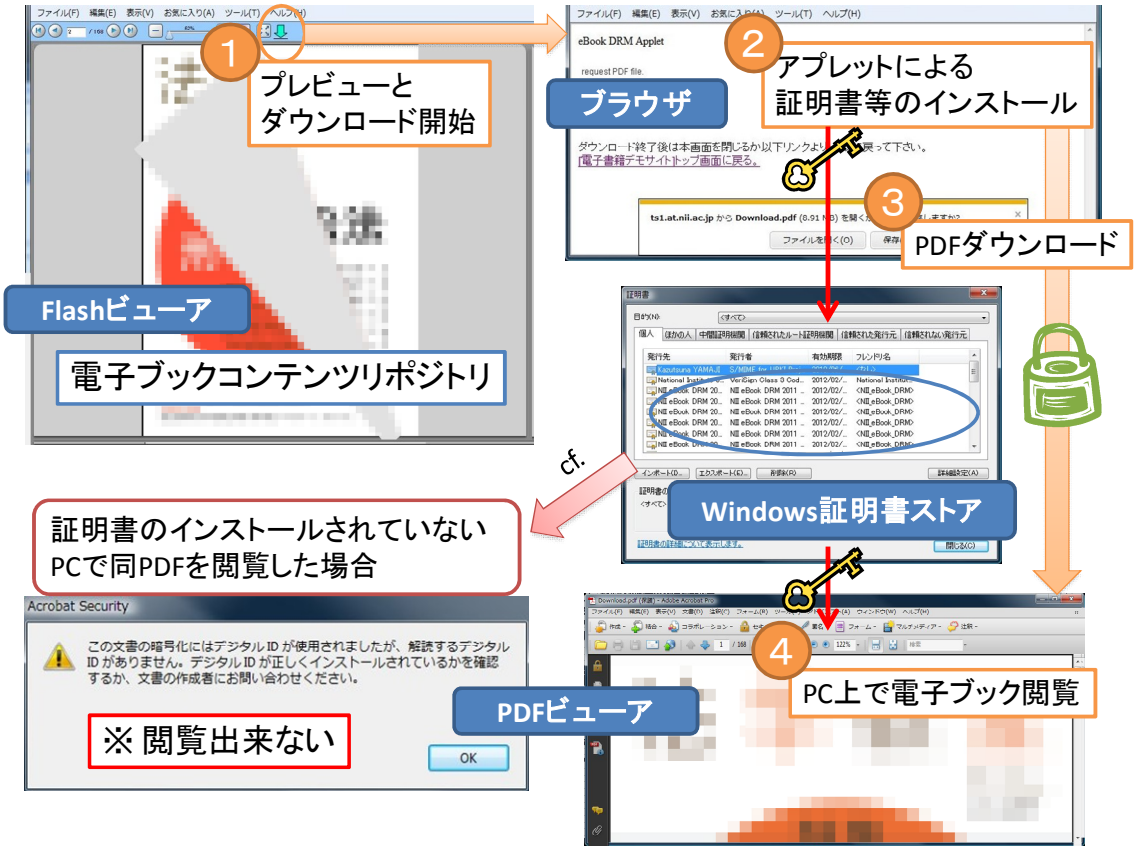

図３：利用時の画面遷移例

○ 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 PDF の 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い、その有効性を確認した。今後は、Windows 以外の MacOS-X やスマートフォンやタブレット端末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、証明書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。

国立情報学研究所
学術ネットワーク研究開発センター
やまじ　かずつな
准教授　山地　一禎