様式 C-19

科学研究費補助金研究成果報告書

平成２３年６月１７日現在

機関番号：62615
研究種目：若手研究（B）
研究期間：2008～2010
課題番号：20700103
研究課題名（和文）知的財産保護を考慮した学術コンテンツ流通システムに関する研究

研究課題名（英文）A study on academic contents sharing system considering intellectual property protection.

研究代表者
山地　一禎（KAZUTSUNA YAMAJI）
国立情報学研究所・学術ネットワーク研究開発センター・准教授
研究者番号：50373379

研究成果の概要（和文）：現在では、論文だけでなく、様々な形式による研究成果の公開が普及している。本研究では、長期署名技術を活用し、そうした成果物を知的財産保護の観点からも安心して公開できる環境の整備に取り組んだ。まずは、リポジトリから公開される PDF に長期署名を付与する統合環境を開発した。次に、PDF に加えて、オフィス系アプリケーションで利用されている、Open Office XML フォーマットに長期署名を付与する方法を提案した。これにより、長期署名による学術コンテンツの内容証明モデルの、基礎基盤の構築に成功した。

研究成果の概要（英文）：In the recent Internet society, research result is published not only by the academic paper but also different methods and formats. This study proposes a secure and safe environment which allow us to publicize our intellectual property by ensuring the electronic signature. An electronic signing system was developed, then it was integrated to a repository system. In addition to the PDF format, long-term signature methods for Open Office XML format were developed. Based on these results, this study proposed the academic contents certificate model by using long-term electronic signature.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2008 年度	1,600,000	480,000	2,080,000
2009 年度	1,500,000	450,000	1,950,000
2010 年度	300,000	90,000	390,000
年度			
年度			
総　計	3,400,000	1020,000	4,420,000

研究分野：総合領域
科研費の分科・細目：情報学・メディア情報学・データベース
キーワード：アーカイブ，コンテンツ保護，長期署名，リポジトリ，電子署名，タイムスタンプ，知的財産，学術情報流通

１．研究開始当初の背景

インターネット社会における Web2.0 的なサービスの徹底活用、それに伴う情報量の爆発に比べて、研究者や教育者からの情報発信量は発展途上である。従来は、論文を書くことが研究者の主たる情報発信の手段であったが、社会的な要求も徐々に変わりつつある。高額な研究費から創出される成果を論文のみで表現するのではなく、研究者間でのデータシェアリングや納税者に対する説明責任を果たすことによって、成果を還元・循環させるべきという理念が波及しつつある。

例えば、ニューロインフォマティクスと呼ばれる分野では、脳・神経系に関する研究成果の統合・共有を実現するために、データベースによる知識共有環境の構築を推進して

いる。また、大学図書館を中心に進められている機関リポジトリにおいても、研究活動により密接に関連して、非文献コンテンツを扱うリポジトリの構築もみられる。こうしたインターネットを主体とした学術コンテンツの共有・蓄積・流通は、今後様々な分野で展開されることが予想されるが、研究者が安心・安全に、かつ、積極的に参加するインセンティブを創出するための基盤の整備が重要な課題である。

２．研究の目的

本研究では、知的財産保護の観点から利用が進められている電子署名とタイムスタンプ技術を学術コンテンツ流通分野に応用することで、研究成果物を安心して公開できるセキュアな環境の整備に取り組む。最近では、最終的な論文より以前に、様々なレベルやフォーマットによる研究成果の公開が試みられている。

本研究では、第一ステップとして、研究成果の先取性を確保するために、論文として投稿する以前に公開するプレプリントを対象とする。従来であれば印刷物として発行されていたプレプリントであるが、電子化が進んだ結果、「誰が」「何を」「いつ」公開したものであるかを共通のフォーマットで電子的に明示でき、研究成果のオリジナリティを保証できることが知的財産保護の観点からも望まれている。こうした問題に対して本研究では、電子署名およびタイムスタンプから構成される長期署名技術を導入し、署名から検証までを実現する統合環境システムを構築することにより、学術コンテンツの内容証明モデルを確立する。

第二ステップとしては、そのモデルをより拡張することを目的として、研究の過程で頻繁に利用される、オフィス系アプリケーションに対応した長期署名の付与方法を提案する。具体的には、マイクロソフト社の Office 2007 にも採用されている, Office Open XML（OOXML）フォーマットに対する、長期署名の付与技術を開発すると共に、その有効性について検証する。

３．研究の方法

（１）プレプリントへの長期署名付与および検証システムの構築

本研究では、その準備段階から開発を進めている長期署名付与システムを活用する。このシステムでは、プレプリントの分野でも一般的に利用されている PDF ファイルに長期署名を付与する機能を有する。そのエンジンとしては、RFC3126 に準拠し、かつ、１つの PDF ファイル（プレプリントファイル）内に長期署名を付与できる機能を採用した。これに加えて、本研究では、PAdES（PDF Advanced Electronic Signatures：ETSI TS 102 778）を利用したドキュメントタイムスタンプの利用についても検証を進めた。プレプリントサーバとしては、英国サウサンプトン大学で開発されている、EPrints Version 3 を利用した。

長期署名統合環境として新たに開発する検証サービスのエンジンには、上記の長期署名サーバを利用した。長期署名サーバが外部と通信ができるように、 XML ベースのメッセージ交換プロトコルである SOAP を利用したインターフェースを提供するための、拡張開発を行った。PDF は，Base64 エンコードして SOAP の BODY 内の<pdf>タグ内に挿入する。この PDF に対し、p1：証明書効力（CRL との照合）、p2：有効期限、p3：証明書信頼性（CTL との照合）、p4：文書変更可能性、p5：総合判定結果、の 5 つの項目が検証され、ウェブ上に結果が表示される。図 1 は、長期署名検証サーバ（学術長期署名検証サービス）に各種ファイルを入力した結果の一例である。

（２）OOXML に対する長期署名の付与

①標準長期署名

OOXML を長期署名化するためには、通常の XML 署名（Xmldsig）に XML 長期署名（XAdES）の要素を組み込む必要がある。まず、Package-Specific Object と Application-Specific Object の記述の対を構成することで、OOXML における Xmldsig を実現する。一方、XAdES による長期署名は、署名対象の指定を Xmldsig のように Object 全体にするのではなく、その子要素の SignedProperties に特定する。これにより、一般的な方法として、Xmldsig と XAdES の記述を単一のファイルで記述する方法を標準長期署名として提案する。

②拡張長期署名

Office 2007 では Xmldsig を付与することができるため、この記述とはできる限り干渉しないように、長期署名を付与する方法が考えられる。XAdES による電子署名部分、すなわち XAdES-BES では、 Signed-Properties の内容もハッシュ値の計算対象となる。したがって、本文が同じ場合でも Xmldsig と XAdES-BES では署名値が異なることになる。そこで、Office 2007 による Xmldsig はそのまま保存し、XAdES に関わる内容を独自のファイルに保存する実装方式を提案する。SignedInfo 内の Reference では、Xmldsig のみを記述した署名ファイルを URI として指定する。また、長期署名のための Object の SignedProperties を参照する Reference も用意する。SignedInfo 以降には、SignatureValue と KeyInfo を記述する。SignatureValue の署名値は Xmldsig として

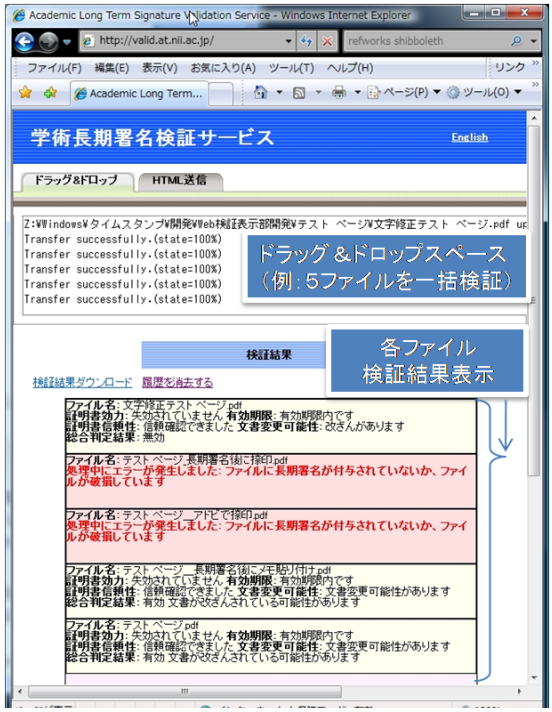

図 1　長期署名検証サーバとその利用例

計算したものとは異なり、XAdES-BES として、長期署名の SignedProperties を署名対象に加えて計算した署名値とする。 KeyInfo は、Xmldsig と同じものを利用する。以上に従い、Xmldsig とは分離したファイルで XAdES による長期署名を行う方法を拡張長期署名として提案する。

４．研究成果

（1）プレプリントへの長期署名付与および検証システムの構築

本研究における第一ステップでは、研究成果の先取権を獲得する目的で発行されるプレプリントに対し長期署名を付与することで、ボーンディジタル時代における学術コンテンツの内容証明統合環境を構築した。

PAdES では、ドキュメントタイムスタンプと呼ばれるアーカイブタイムスタンプの更新により、長期署名が実現される。PAdES におけるドキュメントタイムスタンプの単独付与をオプションとして組み込み、生成された PDF を Adobe 社 Acrobat で表示した結果、サブフィルターにおける ETSI.RFC3161 が未対応であるために検証が実行不可であること、また、タイムスタンプトークンは PKCS7 として単純に検証できず検証に失敗することが明らかとなった。前者は、対応した検証ハンドラを検索する際に生じる問題である。一致する検証ハンドラがない場合に、標準の署名ハンドラを利用することで、この問題は可決される。後者の原因としては、署名対象が正しいかどうかの判定時のエラーが挙げられる。ドキュメントタイムスタンプの単独付与 PDF を扱う際には、検証時におけるこうした点に留意する必要があることが示唆された。

検証サーバでは、フォーム内にファイルをドラッグ＆ドロップするだけで、ファイルをアップロードできるユーザインターフェースを装備した。複数のファイルを同時にドラッグ＆ドロップすることも可能であり、一般的なファイルのアップロード操作と比較すると、検証作業の簡便性が飛躍的に向上した。

本研究では、プレプリントを対象としたが、機関リポジトリなどからのコンテンツサービスにおいても、同様のモデルが適用可能である。機関リポジトリでは、国内外を問わず灰色文献を扱うケースが多く、ブランド力のある出版社から膨大に発信されるコンテンツとは対比的である。こうした灰色文献こそ、本研究で開発したシステムにより信頼性を担保することが、今後、重要になるものと考えられる。そうしたコンテンツへの適用により、印刷物を発行しその内容証明を行ったように、PDF の「誰が」「何を」「いつ」を保証できる本研究の成果は、今後の学術コンテンツ流通のあり方を大きく変化させる可能性がある。

（2）OOXML に対する長期署名の付与

各長期署名を付与したファイルを Office 2007 Word で開いた結果を図 2 に示す。これより、標準長期署名は、本研究で開発したアプリケーションでの検証には成功することは確認しているが、Office 2007 の応答としてはエラーとなることがわかる。これに対し、拡張長期署名は、Office 2007 においても有効な Xmldsig として認識されている。また、OOXML は複数の XML ファイルを ZIP 形式で圧縮した構造となっているが、Office 2007 では構造の詳細なチェックはせずに、拡張長期署名で XAdES を追加したファイルの添付も許容されている。このとき、検証の対象となるのは、XAdES を含まない Xmldsig の部分である。すなわち、 Office 2007 においても、拡張長期署名では、署名値は正しく本文は改ざんされていないことが確認できる。現状の OOXML の仕様は、Xmldsig を付与することにのみ対応しているが、本研究の成果は、OOXML において XAdES を実装する上での仕様拡張の方向性を与えるものである。また、OOXML の仕様を逸脱しないと考えられる標準長期署名が、Office 2007 では Xmldsig としてエラーになることから、OOXML の厳密化の必要性、あるいは、Office 2007 の改善点が示唆された。

インターネット上に流通する研究成果としては、これまでは PDF フォーマットで公開される文献が中心であった。今後は、その

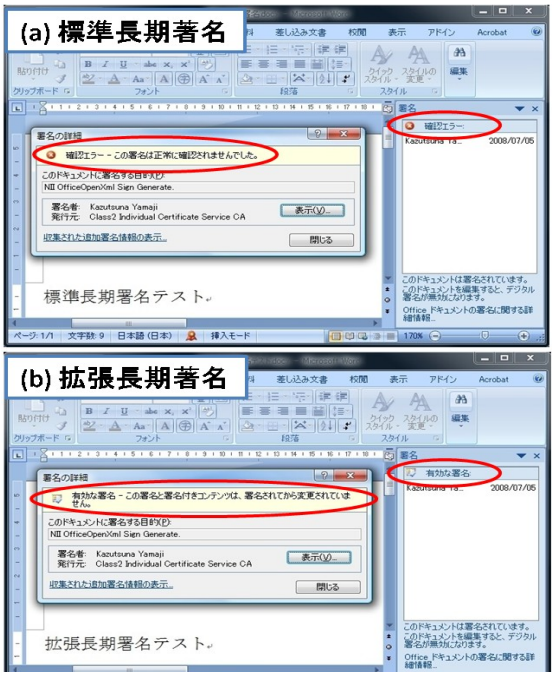

図 2　Office 2007 Word ファイルに対する標準および拡張長期署名付与結果

モデルを軸として、文献に関連する補遺的なコンテンツを、多様なフォーマットで配信するためのインターネット上のサービスやコミュニティの育成が進んでくると予想される。本研究の成果は、そうした状況においても、コンテンツの流通を妨げることなく知的財産保護を確保するための、基盤技術を提供するものである。今後は，長期署名付きコンテンツの流通と、その情報を利用したサービスについて検討を更に進め，よりリッチな学術成果共有社会の育成に寄与したいと考えている。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

1. 山地一禎, 片岡俊幸, 行木孝夫, 曽根原登, プレプリントへの長期署名付与および検証システムの構築, 情報知識学会誌, 18(3), pp.240-248, 2008 年［査読有］
2. 山地一禎, 片岡俊幸, 宮地直人, 曽根原登, Office Open XML に対する長期署名の付与, 情報知識学会誌, 20(1), pp.1-14, 2010 年［査読有］

〔学会発表〕（計 8 件）

1. Yamaji, K., Aoyama, T. and Takeda, H., Repository System WEKO associated with Flash Converter, The 5th International Conference on Open Repositories, 2010-07-06, Madrid
2. 山地一禎, Shibboleth 電子認証連携と学術コンテンツ流通技術, 第 14 回 ISS スクエア水平ワークショップ, 2010-03-26, 神奈川
3. 山地一禎, オープンサイエンスによる学術メディアとコンテンツの多様化, インターンシップ・インテリジェンス教育推進シンポジウム, 2009-07-13, 福岡
4. Yamaji, K., Aoyama, T., Takeda, H., WEKO: A New Repository System as a Function of Content Management System, The 4th International Conference on Open Repositories, 2009-05-19, Atlanta
5. 山地一禎, 青山俊弘, 武田英明, 学術資源共有基盤 WEKO の開発, 第 36 回ディジタル図書館ワークショップ, 2009-03-10, 東京
6. 山地一禎, 学術分野における知的財産管理とタイムスタンプ, タイムビジネス協議会「タイムスタンプが支える知的財産管理の最前線」, 2008-09-29, 東京
7. Yamaji, K., Kataoka, T., Sonehara, N., Namiki, T., Time Stamping Preprint Server Environment using EPrints 3, Third International Conference on Open Repositories 2008, 2008-04-04, Southampton
8. 山地一禎, 学術コンテンツ流通におけるタイムスタンプの活用, 日本社会情報学会(JASI)第 111 回研究会, 2008-02-16, 東京

〔その他〕
ホームページ等
http://www.at.nii.ac.jp/

６．研究組織
(1)研究代表者
山地　一禎（KAZUTSUNA YAMAJI）
国立情報学研究所・学術ネットワーク研究開発センター・准教授
研究者番号：50373379