論文

Office Open XMLに対する長期署名の付与

Application of the Long Term Signature to Office Open XML files

山地一禎^{1*}, 片岡俊幸¹, 宮地直人², 曾根原登³

Kazutsuna YAMAJI, Toshiyuki KATAOKA, Naoto MIYACHI, Noboru SONEHARA

1 国立情報学研究所 学術ネットワーク研究開発センター

R & D Center for Academic Networks, National Institute of Informatics

E-mail: yamaji@nii.ac.jp, kataoka@nii.ac.jp

2 有限会社 ラング・エッジ

LangEdge Inc.

E-mail: miyachi@langedge.jp

3 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

E-mail: sonehara@nii.ac.jp

研究成果などの知的財産管理の手段として、電子署名とタイムスタンプ技術を基礎とした長期署名の応用が注目されている。本研究では、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。対象とするフォーマットは、マイクロソフト社のOffice 2007に採用されている、Office Open XML (OOXML)とした。長期署名フォーマットには、XMLで記述されるXAdESを採用した。OOXMLへのXAdESの実装として、標準長期署名と拡張長期署名と呼ぶ二種類の方法を提案した。前者はOOXMLで規定するXML署名のファイルに長期署名に関する記述を含める形式であり、後者は独立したファイルに記述する形式である。双方とも、OOXMLとXAdESの仕様を逸脱するものではない。この二種類の長期署名を、Office 2007が生成するOOXMLファイルに付与するアプリケーションを開発した。長期署名付きファイルをOffice 2007で開いた結果、拡張長期署名はXML署名としての検証には成功するのに対し、標準長期署名は失敗することが確認された。XML長期署名としては、標準長期署名の方がより一般的な実装方法であり、OOXMLにおいて長期署名を付与する書式を明らかにするとともに、Office 2007によるOOXMLの解釈にも対処が必要であることが示唆された。

The long term signature (LTS) is composed of an electronic signature and timestamp and it may be an effective technology for protecting intellectual property. This study describes a method of applying LTSs to files generated by office applications. The targeted files are in Office Open XML (OOXML) and are opened by MS Office 2007. XML LTS is described in XAdES format. Two types of LTS, that

is, standard LTS and expanded LTS, can be used to apply XAdES to OOXML. The standard format involves a LTS description in a XML signature file that is defined by OOXML. The expanded format separates the LTS description from the XML signature file. Both formats satisfy the OOXML and XAdES specifications. As a result of reading two XAdES signature word processing files by using Office 2007, the file with the expanded LTS was recognized as a valid file with an XML signature, whereas the file with the standard LTS was not.

キーワード: 長期署名, 電子署名, タイムスタンプ, 知的財産, 研究ノート

Long-term Electronic Signature, Electronic Signature, Timestamp, Intellectual Property, Lab Notebook.

1 はじめに

国立大学の法人化などを契機に, 大学における知的財産に対する認識が高まってきた[1]. その対象は, 研究成果の帰属や特許取得戦略といったポリシー的な側面のみならず[2], 研究ノートの導入によるリスクマネジメントといった実地的な内容まで多岐にわたる[3]. 一方で, インターネット上におけるデータベースや参加型サイトの普及に伴い, 従来は文献としてのみ公開されていた研究成果が, 現在では様々な段階・形式で公開されるようになってきた[4][5]. しかしながら, そうしたオープンサイエンス的な流れの中では, 知的財産保護に対するシステムのおよびポリシー的な解決策が提示されておらず, そうした問題を解決することは, 今後の普及に向けての重要な課題である.

一方, e-文書法の制定に伴い, 企業内では, 財務・税務関係の法定保存文書を電子的にセキュアに保存するための環境整備が進んでいる. このとき, 文書の作成者や作成時期が紙文書などと電子化した文書が同一であることが確認できること, すなわち, 文書の真正性を担保する

ために, 電子署名とタイムスタンプの付与が求められている[6]. ここで, 電子署名とは, 電子文書の作成者(署名者)が特定でき, その内容の非改ざん性を保障するための行為あるいはシステムのことである. これにより, 電子文書の「誰が」「何を」が保障される. さらに, 「いつ」電子文書が作成されたかを担保する規格がタイムスタンプである. こうした技術は, 事務的な文書保存以外にも, 先使用权を立証し知的財産を確保する目的でも有効利用されている[7]. 最近では, 文書の真正性をより長期的に担保する目的で, 電子署名とタイムスタンプ技術を組み合わせた長期署名が提案されており[8][9], JISにおいても標準化が行われた[10][11].

これまでに我々は, 学術分野においてアイデアや研究成果の先取権(先使用权)を主張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システムの開発を進めてきた[12]. プレプリントシステムで対象としたのはPDFファイルであったが, より汎用性を高めるためには, 通常の業務で頻繁に使われるオフィス系アプリケーションのファイルフォーマットにも対応することが望まれる. そうした長期署名技術の拡張は, 学術分野

図 1 XAdES 長期署名フォーマット

における知的財産保護の条件を満たしつつ、研究者がインターネットを通じて研究成果を公開する自由度を確保することができる。現在、オフィス系アプリケーションとして多く利用されているものとしては、マイクロソフト社とOpenOffice.orgが提供するものがある[13]。現在では、双方ともにISO化されたXML形式のファイルフォーマットと、XML署名(Xmldsig) [14]による電子署名を採用し、前者はOffice Open XML (OOXML) [15]、後者はOpen Document Format (ODF) [16]で記述される。ODFに関しては、Xmldsigを拡張したXML長期署名(XAdES) [9]の適用が試みられ、実際に、電子署名法に基づく認定認証業務の中で利用されている[17]。一方、よりシェアが高いと考えられるOOXMLに関しては、その長期署名化に関するシステム実装の報告はこれまでなされていない。そこで本研究では、研究成果のセキュアな共有を可能にする基盤技術として、OOXMLの長期署名化を実現することを目的とした。

2 長期署名

図 1は、XAdESによる長期署名フォー

マットを記述したものである[9]。ここで、XAdES-BES (XML Advanced Electronic Signatures - Basic Electronic Signature) の部分が電子署名に該当し、電子文書、署名属性、署名値から構成される。署名値は、電子文書から生成する固定長の疑似乱数であるハッシュ値を、署名者の秘密鍵で暗号化した値である[18]。署名文書の受取者は、このハッシュ値を利用して非改ざん性を検証する。ただし、署名を行った本人は内容を改変することが可能であることから、電子署名に加えて、時間軸での電子文書の存在を保障するタイムスタンプの付与が必要とされる[19]。図 1の場合ではXAdES-T (XAdES with Time) までのフォーマットが、これに該当する[9]。

電子署名やタイムスタンプは、いずれもデジタル署名技術を利用しており、アルゴリズムの脆弱化や鍵漏洩への対応として、有効期限や失効(無効化)機能を有している。すなわち、長期的に証明力を保持できない仕組みとなっており、研究成果のように長期にわたって存在証明と非改ざん証明の保証が必要とされる対象には適していない。これに対処するために提案されたのが長期署名であり、署名の検証に用いた証拠として、認証パ

ス上の全ての公開鍵証明書とその失効情報へのリファレンス（図 1 XAdES-C : XAdES with complete validation data references）と実際の検証情報（図 1 XAdES-X-L : Extended long electronic signatures with time）を付加し、長期署名フォーマット全体にアーカイブタイムスタンプ（図 1 XAdES-A : Archival electronic signatures）を付与する。このとき、XAdES-Cは、ETSI TS 101 903[9]およびJIS プロファイル[11]ともに、その付与を任意としている。本研究では、OOXMLで作成されるコンテンツに対し、XAdESによる長期署名を付与するための方法を提案する。

3 Office Open XML

OOXMLでは、画像などのバイナリデータを除けば他は全てXML記述されており、それらのファイルをZIP形式で圧縮して1つのファイルにまとめる。例えば、Office 2007 Wordで作成したdocx拡張子のZIPファイルを解凍すると、パッケージの内部は以下のようになっている。

- **_rels** (フォルダ)
分散保存されたファイルの関連情報を保存
- **docProps** (フォルダ)
プロパティに関する情報を保存
- **word** (フォルダ)
文書本体およびスタイルに関する情報を保存
- **[Content_Types].xml** (XMLファイル)
含まれる全てのファイルのデータタイプを定義

wordフォルダは、エクセルの場合はxls、パワーポイントの場合はpptフォルダと

なる。こうしたオフィスファイルへの電子署名には、Xmldsigを適用することができ、OOXMLの仕様書内にその方法が記述されている。Xmldsigを付与した場合には、上記のパッケージ構成に対して、

- **_xmldsignatures** (フォルダ)
が追加され、必要な情報が保存される。例えば、Office 2007で最初に電子署名を付与した場合には、sig1.xmlというファイルが生成され、Xmldsigの内容が保存される。なお、電子署名ファイルに適用されるスキーマは、OOXMLのものではなく、標準のXmldsigとなる。本研究では、この**_xmldsignatures**に保存される署名情報を対象とし、XML署名(Xmldsig)からXML長期署名(XAdES)へと拡張する方法を提案する。

4 Office Open XMLへの長期署名

4.1 OOXMLによるXmldsigとXAdESによる長期署名フォーマット

ETSI TS 101 903[9]によるXAdESフォーマットと各XML要素の説明を表 1に示す。○マークで示した要素はRFC3275によるXmldsigが必要とされており、●マークで示した要素は長期署名用に追加されたものである。XAdESによる長期署名の場合は、●1と●3の対応からわかるように、署名対象がObject全体(●2)にはならず、SignedProperties(●3)のみとなる。長期署名用のXAdES-A(●4)のように必要に応じて追加されていく内容はUnsignedProperties配下に記述して署名の対象外とすることで、XAdES-BES付与時のハッシュ値の永続性が担保できる構造となっている。

表 1 XAdES 署名の標準的な要素

XML 要素	説明
○ <Signature>	Xmldsig 開始タグ
○ <SignedInfo>	署名対象要素
○ <CanonicalizationMethod/>	署名対象正規化手法指定
○ <SignatureMethod/>	署名アルゴリズム指定
○ <Reference/>	署名対象への URI 指定 1 とオプション
○ :	変換手法指定署名アルゴリズム指定
○ :	署名対象は複数指定可能
●1 <Reference URI="#xades"/>	XAdES 署名対象への URI 指定
○ </SignedInfo>	署名対象要素終了
○ <SignatureValue/>	署名値 (Base64)
○ <KeyInfo/>	署名者の秘密鍵情報
○ <Object>	署名対象内包時のオブジェクト要素
●2 <Object>	長期署名用オブジェクト (必須)
● <QualifyingProperties>	XAdES 要素開始
●3 <SignedProperties Id="xades">	XAdES 署名対象要素
● <SignedSignatureProperties/>	XAdES 署名要素 (例: <SigningTime>等)
● </SignedProperties>	XAdES 署名対象要素終了
● <UnsignedProperties>	XAdES 非署名対象要素
● <UnsignedSignatureProperties>	XAdES 非署名要素
● <SignatureTimeStamp/>	XAdES-T 署名タイムスタンプ要素
● <CertificateValues/>	XAdES-X-L 証明書一覧要素
● <RevocationValues/>	XAdES-X-L 検証情報一覧要素
●4 <ArchiveTimeStamp/>	XAdES-A 保管タイムスタンプ要素
● :	(複数回可能)
● </UnsignedSignatureProperties>	XAdES 非署名要素
● </UnsignedProperties>	XAdES 非署名対象要素終了
● </QualifyingProperties>	XAdES 要素終了
● </Object>	長期署名用オブジェクト終了タグ
○ </Signature>	Xmldsig 終了タグ

OOXMLによるXmldsigの例を表 2に示す。OOXMLでは、Xmldsigにて検証可能なフォーマットとして、△1で示したidPackageObjectで参照されるObject要素 (Package-Specific Object) を記述し、必要に応じて△2で示したidOfficeObjectで参照されるオプション Object 要素 (Application-Specific Object) を記述する。このとき、△1と△3および△2と△4の対応からわかるように、Reference要素で規定される署名の対象はObject全体になる。

4.2 標準長期署名

OOXMLを長期署名化するためには、表 2のXmldsigに表 1の●で示したXAdESの要素を組み込めばよい。表 3に、その記述例を示す。◇1と◇4でPackage-Specific Objectを記述し、◇2と◇5でApplication-Specific Objectを記述することで、OOXMLにおけるXmldsigを構成している。一方、◇3と◇6では、XAdESによる長期署名を構成している。4.1で述べたように署名対象の指定は、Xmldsig

表 2 OOXML における署名例

	<?xml version="1.0" encoding="UTF-8" ?>
	<Signature Id="idPackageSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
	<SignedInfo>
	<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
	<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
△1	<Reference URI="#idPackageObject" Type="http://www.w3.org/2000/09/xmldsig#Object">
	<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
	<DigestValue>\$aDdLivsjfCQLGxtrqC0tWts0914=\$</DigestValue>
	</Reference>
△2	<Reference URI="#idOfficeObject" Type="http://www.w3.org/2000/09/xmldsig#Object">
	<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
	<DigestValue>60B0mxo/DLT80lprfcK9P/ieHGM=</DigestValue>
	</Reference>
	</SignedInfo>
	<SignatureValue>gZDjjpwCkFGZUz9X/O7cq\$6E54f1NehWqz...</SignatureValue>
	<KeyInfo>
	:
	</KeyInfo>
△3	<Object Id="idPackageObject" xmlns:mdssi="http://schemas.openxmlformats.org/package/2006/digital-signature">
	:
	</Object>
△4	<Object Id="idOfficeObject">
	<SignatureProperties>
	<SignatureProperty Id="idOfficeV1Details" Target="#idPackageSignature">
	<SignatureInfoV1 xmlns="http://schemas.microsoft.com/office/2006/digsig">
	:

のようにObject全体ではなく、その子要素のSignedPropertiesに特定している。以上のように、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呼ぶ。

4.3 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、表1の●3からはじまるSignedProperties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。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。表4に、XAdES用ファイルの記述例を示す。□1で示した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。□2で示したReferenceでは、長期署名のためのObjectのSignedProperties (□6)を参照する。SignedInfo以降には、SignatureValue (□3) , KeyInfo (□4)

表 3 標準長期署名の署名例

	<?xml version="1.0" encoding="utf-8" ?>
	<Signature Id="idPackageSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
	<SignedInfo Id="idPackageSignature-Si-3">
	<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
	<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
◇1	<Reference Id="idPackageSignature-Ref-1" URI="# <u>idPackageObject</u> "
	Type="http://www.w3.org/2000/09/xmldsig#Object">
	:
	</Reference>
◇2	<Reference Id="idPackageSignature-Ref-2" URI="# <u>idOfficeObject</u> "
	Type="http://www.w3.org/2000/09/xmldsig#Object">
	:
	</Reference>
◇3	<Reference Id="idPackageSignature-Ref-7" URI="# <u>idPackageSignature-Sp-6</u> "
	Type="http://uri.etsi.org/01903#SignedProperties">
	:
	</Reference>
	</SignedInfo>
	<SignatureValue Id="idPackageSignature-Sv-4">NLGwNiV1vYs...</SignatureValue>
	<KeyInfo Id="idPackageSignature-Key-5">
	:
	</KeyInfo>
◇4	<Object Id=" <u>idPackageObject</u> " xmlns:mdssi="http://schemas.openxmlformats.org/
	package/2006/digital-signature">
	:
	</Object>
◇5	<Object Id=" <u>idOfficeObject</u> ">
	:
	</Object>
	<Object Id="idPackageSignature-XAdES-Object">
	<QualifyingProperties Target="#idPackageSignature" xmlns="http://uri.etsi.org/01903/v1.3.2#">
◇6	<SignedProperties Id=" <u>idPackageSignature-Sp-6</u> ">
	<SignedSignatureProperties>
	:

を記述する。SignatureValueの署名値はXmldsigとして計算したものとは異なり、表 4のファイルが規定する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。XAdESのObject (◇5) には、表 1の●2以降のObjectの内容を記述する。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呼ぶ。

4.4 アプリケーション構築

OOXMLの長期署名フォーマットとして本研究で提案する標準長期署名と拡張長期署名を実際に付与し、本研究で提案している仕様の妥当性を検討するためのアプリケーションを開発した。長期署名

表 4 拡張長期署名の長期署名部記述例

	<?xml version="1.0" encoding="UTF-8" ?>
	<Signature Id="idXadesSignature" xmlns="http://www.w3.org/2000/09/xmldsig#">
	<SignedInfo Id="idXadesSignature-Si-2">
	<CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
	<SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
□1	<Reference Id="idXadesSignature-Ref-1" URI="_xmldsignatures/sig1.xml">
	<Transforms>
	<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
	</Transforms>
	<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
	<DigestValue>IAGQ8Mz2NchhdS/cCPiNsFoHw7w=</DigestValue>
	</Reference>
□2	<Reference Id="idXadesSignature-Ref-6" URI="# <u>idXadesSignature-Sp-5</u> "
	Type="http://uri.etsi.org/01903#SignedProperties">
	<Transforms>
	<Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315" />
	</Transforms>
	<DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
	<DigestValue>wlPeYDJJXmFolW8N+ohgaUQtE+8=</DigestValue>
	</Reference>
	</SignedInfo>
□3	<SignatureValue Id="idXadesSignature-Sv-3">enf7MqAWThKHpLbrue+cMIL8uP...
	</SignatureValue>
□4	<KeyInfo Id="idXadesSignature-Key-4">
	:
	</KeyInfo>
□5	<Object Id="idXadesSignature-XAdES-Object">
	<QualifyingProperties Target="#idXadesSignature" xmlns="http://uri.etsi.org/01903/v1.3.2#">
□6	<SignedProperties Id=" <u>idXadesSignature-Sp-5</u> ">
	:

は、XAdES-Cを含めない、XAdES-BES、XAdES-T、XAdES-X-L、XAdES-Aで構成した。任意の電子証明書およびタイムスタンプ局を利用して、XAdESによる長期署名が付与できるシステムとするために、以下の機能を実装した。

- Windows証明書ストアからの証明書選択機能
- タイムスタンプ局指定機能
- 長期署名付与機能
(標準長期署名、拡張長期署名を選択可能)

- 保管タイムスタンプの追加機能
- 長期署名検証機能
(Xmldsig, XAdESのスキーマ検証を含む)

これらの機能を、Microsoft Visual C++を利用し、Xmldsig付与に関する研究開発でもしばしば利用されている .NET Framework[20][21]上で動作するアプリケーションとして開発した。XAdESに関する基本的な処理は、Le-XAdESを利用した[22]。ZIP圧縮の処理には、zlib[23]とInfo-ZIP[24]を利用した。開発したアプリ

図 2 XML 長期署名付与アプリケーションのスクリーンショット

ケーションのスクリーンショットを図 2 に示す。長期署名では、図 1 における XAdES-BES, XAdES-T, XAdES-A が検証の対象となるが、本アプリケーションにおいても、以下のように各内容が個別に検証されるように構築した。XAdES-A に関しては、全ての世代のタイムスタンプが検証されるようにした。

- Xmldsig の検証 (XAdES-BES)
- 署名タイムスタンプの検証 (XAdES-T)
- 全世代のアーカイブタイムスタンプの検証 (XAdES-A)

5 評価と考察

OOXML は標準化された仕様であるが、

現在のところ、技術開発のために汎用的に利用されている検証ツールは存在しない。そこで本研究では、Office 2007 Word を利用し、ベースとなる文書ファイルの作成、および、電子署名に関する動作確認を行った。まず、Office 2007 Word で文書ファイルを作成した後に、開発したアプリケーションで標準長期署名および拡張長期署名を付与し、どちらも Xmldsig および XAdES として正常に検証できることを確認した (図 2 中赤矢印)。電子証明書¹と時刻認証局²には、第三者機関が提供するサービスを利用した。

¹ 日本ベリサイン株式会社 Class2 スタンダード

² アマノタイムビジネス株式会社 AMANO Time Stamp Service Type-Free-A

図 3 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

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3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が、Office 2007の応答としてはエラーとなる。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ことがわかる。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、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。

標準長期署名におけるOffice 2007の応答のエラーの原因に関しては、以下の理由が考えられる。まず、OOXMLの電子署名に適用されるスキーマはXmldsigであり、本研究で開発したアプリケーションにおいて電子署名値とスキーマの検証には成功しており、有効なXmldsigが付与されていると評価できる。従って、Office 2007においてもXmldsigとしての検証に成功することが期待されるが、実際にはエラーとなる。OOXMLの仕様書では、SignedInfo 要素 には、Package-Specific ObjectとApplication-Specific Object要素へのReferenceが指定可能であるが、それ以外のReferenceの指定に関する制約は書かれていない。しかしながら、図3の結果より、Office 2007の動作としては、Package-Specific Object と Application-Specific Object要素以外のReferenceは受け付けないと推定される。これはXmldsigの仕様やスキーマにも記述されていない制限である。こうした動作が、Office 2007の実装上の不備に起因するものなのか、仕様上のものなのかは、現在のソフトウェア流通メカニズムでは判別することが困難である。ただし、ここで得られた結果を基に、標準長期署名のような形式でOOXMLに対して長期署名を付与するためには、Object要素だけではなく、その下位に位置するSignedProperties要素(表3◇3)に対しても、Referenceを許可するようにOOXMLの仕様を厳密化する必要がある。

本研究では、OOXMLの仕様から派生する長期署名方法として標準長期署名と拡張長期署名を提案した。これらの方法とは別に、OOXMLの仕様とは全く別に

長期署名を付与することも可能である。すなわち、標準長期署名により作成されるファイルを、OOXMLが解釈できない場所あるいはファイル名で保存すればよい。この長期署名の付与方法を独立長期署名と呼ぶことにする。標準長期署名、拡張長期署名および独立長期署名は、それぞれXAdESにより定義される長期署名フォーマットから逸脱するものではない。以下では、各方式の得失について考察する。

拡張長期署名は、表 4中□1で示したようにXmldsigに対するリンクをもつことになる。したがって、Xmldsigに利用された電子署名が長期署名に利用されたものと等しい場合には、表 4のXAdESファイルの中でその検証情報(図 1のXAdES-CとXAdES-X-T)を保存することができる。しかしながら、双方の電子署名が異なる場合には、その検証情報を保持することができないという制約がある。

OOXMLに従う仕様としては、署名情報を1つのファイルに保存する標準長期署名がXAdESの表現として最も標準的である。拡張長期署名は、XmldsigとXAdESを共存させるという点で冗長性があるが、現状のOOXMLの仕様の拡張版と捉えることができる。一方、独立長期署名は、OOXMLの仕様とは関連性がない。

Office 2007がXmldsigとして正常に認識できるのは、拡張長期署名だけである。標準長期署名は、図 3(a)に示したように、Xmldsigとしてはエラーとなる。独立長期署名は、OOXMLの仕様から逸脱することを目的とした方法であるため、Office 2007のXmldsigとしては、評価の対象外と

なる。独立長期署名では、Office 2007の既存の機能としては、いかなる署名も付与されていないと認識されることになる。

以上の比較により、Office 2007の改良が可能であれば、OOXMLの長期署名方法としては標準長期署名が最も優れた方法であると考えられる。ただし、既存のOffice 2007ユーザの利便性を考慮すると、現状では、拡張長期署名の利用が優位なケースも考えられる。

6 おわりに

本研究では、オフィス系アプリケーションのためのISO標準フォーマットである、OOXMLへの長期署名方式について検討した。OOXMLから派生する方法として、標準長期署名と拡張長期署名を提案し、それぞれの特徴について評価した。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[25]。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。また、本研究の一部をワーキンググループにて報告した次世代電子商取引推進協議会では、その内容が高く評価されており[26]、OOXMLに対する長期署名方法の標準化という側面からも、今後、産学連携により本研究の成果を展開していく予定である。

参考文献

- [1] Shimada, R.: “Intellectual Property Management of National University Corporations Shift to Institutional Ownership and its New Challenges” Vol.1, No.1, 37-45, 2005.
- [2] 青山紘一: 「研究成果の帰属と補償 (下) —大学・公的研究機関における研究成果の帰属と管理—」, 情報管理, Vol.45, No.12, 845-857, 2003.
- [3] 妹尾堅一郎: 「研究ノートのリスクマネジメント」, 研究・技術計画学会, Vol.21, No.2, 435-438, 2006.
- [4] 西村美咲, 横井茂樹, 安田孝美: 「研究室の情報共有・公開を支援するCMSを基盤としたWebシステムの構築」, 情報処理学会研究報告, Vol. IS-103, No.4, 23-28, 2008.
- [5] Yamaji, K., Sakai, H., Okumura, Y. and Usui, S.: “Customizable neuroinformatics database system: XooNIps and its

- application to the pupil platform”,
Computers in biology and medicine,
Vol.37, No.7, 1036-1041, 2006.
- [6] 石島正勝: 「情報の権限付与と共有範囲を考える」, 情報の科学と技術,
Vol.56, No.1, 19-24, 2006.
- [7] 池畠裕介: 「先使用権制度の円滑な利用に関する調査研究」, 知財研紀要,
Vol.16, No.11, 1-8, 2007.
- [8] Pinkas, D., Ross, J. and Pope, N.: “Electronic Signature Formats for Long Term Electronic Signatures”, IETF RFC3126, 2001.
- [9] European Telecommunications Standards Institute: “XML Advanced Electronic Signatures (XAdES)”, ETSI TS 101 903 v1.3.2, ETSI, 2006.
- [10] 日本工業規格: “CMS利用電子署名 (CAAdES)の長期署名プロファイル”, JISX5092, 2008.
- [11] 日本工業規格: “XML署名利用電子署名 (XAdES)の長期署名プロファイル”, JISX5093, 2008.
- [12] 山地一禎, 片岡俊幸, 曾根原登, 行木孝夫: 「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, Vol.18, No.3, 240-248, 2008.
- [13] Kosek, J.: “From the Office Document Format Battlefield”, IT Professional, Vol.10, No.3, 51-55, 2008.
- [14] Eastlake, D., Reagle, J. and Solo, D.: “XML-Signature Syntax and Processing”, IETF RFC3275, 2002.
- [15] International Organization for Standardization: “Information technology - Document description and processing languages - Office Open XML File Formats”, ISO/IEC 29500, 2008.
- [16] International Organization for Standardization: “Document Format for Office Applications (OpenDocument)”, v1.0, ISO/IEC 26300, 2006.
- [17] 本間史夫: 「証明書電子更新サービス」, PKI-Jジャーナル, Vol. 2007最終号, 103-104, 2007.
- [18] Housley, R.: “Cryptographic Message Syntax”, IETF RFC3852, 2004.
- [19] Adams, C., Cain, P., Pinkas, D. and Zuccherato, R.: “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)”, IETF RFC3161, 2001.
- [20] Bull L., and Squire D. M.: “XML Signature Extensibility Using Custom Transforms”, Lecture Notes in Computer Science, Vol.3306, pp.102-112, 2004.
- [21] Mahmud M.: “A Study on Data Security in the Microsoft .NET Platform”, Proc. National Conference on Cryptography and Information Security, NCCIS 2006, pp.45-49, 2006.
- [22] 宮地直人: “Le-XAdESライブラリ, 有限会社ラング・エッジ”, 入手先 <http://www.langedge.jp/pub/LeXAdES/>, 参照2009-04-07.
- [23] Roelofs, G., Gailly, J. and Adler, M.: “zlib software”, available from <http://zlib.net>, accessed 2009-04-07
- [24] Adler, M., Bush, J., Davis, K., Denker, H., Dubois, J., Gailly, J., Goatley, H., Gordon, E., Gorman, I., Herborth, C., Haase, D., Hartwig, G.,

Heath, R., Hudson, J., Kienitz, P.,
Kirschbaum, D., Lee, J., Linden, O.,
Mandrighenko, I., Miller, S., Monesi, S.,
Owens, K., Petrov, G., Roelofs, G.,
Rommel, K., Salisbury, S., Smith D.,
Schweda, S., Spieler, C., Truta, C.,
Verheijen, A., Behren, P., Wales R. and
White, M.: “Info-ZIP”, available from
<http://www.info-zip.org>, accessed
2009-04-07.

[25] Brunger-Weilandt, S.: “E-Science -
Advancing new ways of scientific
communication”, Information Services
and Use, Vol.27, No.4, 161-166, 2007.

[26] 次世代電子商取引推進協議会: “電子
署名普及に関する活動報告2008”, 入
手先
<http://www.ecom.jp/results/h20seika/H20results-14.pdf>, 参照2009-10-06.

(2009年4月9日受付)
(2009年12月18日採択)
(2009年12月22日オンライン公開)