

OpenXML 長期署名 システム設計書 (概要)

2008年 3月24日版

国立情報学研究所
学術ネットワーク研究開発センター

山地一禎, 片岡俊幸, 曾根原登

■ 目次

■ 目次	1 -
■ 概要	2 -
1. OpenXML 概要	3 -
2. 長期署名概要	4 -
3. ドキュメントフォーマットと長期署名	5 -
4. OpenXML 長期署名	7 -
5. OpenXML 長期署名ツール OOXmlSignTool	8 -
6. 今後の課題	9 -
付録 1. Info-zip のライセンス	10 -
付録 2. zlib のライセンス	11 -

■ 概要

今回の OpenXML 長期署名の開発では Open XML フォーマットに対する XML 署名の解析と長期署名の適用を検討し実際に実装例としてのテスト開発を実施することを目的としている。その為に大きく分けて仕様の調査検討と実装例開発の2つのパートに分けられる。

1) OpenXML 長期署名化の仕様調査検討

ODF 署名の長期署名化は、標準の XML 署名を拡張しただけで対応可能であった。しかし同じ方式を今回の OpenXML に適用したところ、MS-Office2007 において検証エラーになる問題を生じた。これでは本来の目的を達成できない為に、OpenXML 標準の XML 署名ファイルを署名対象として更に2番目の署名として長期署名を付与する方式も検討した。本来の OpenXML 署名ファイルを長期署名化する方式を「標準長期署名」と呼び別途長期署名ファイルを追加する方式を「拡張長期署名」と呼ぶ。また本来の OpenXML 署名を「標準 XML 署名」と呼ぶ。以下に3方式を列挙する。

種類	動作
標準 XML 署名	sig1.xml を生成 (標準の XML 署名)
標準長期署名	sig1.xml を生成 (sig1.xml を長期署名化)
拡張長期署名	sig1.xml (標準の XML 署名) と sig1-xades.xml (長期署名) を生成

2) OpenXML 長期署名化の実装例として署名検証ツールの開発

OpenXML のドキュメントファイルは画像等をバイナリファイルとしてその他のデータを XML ファイルとしてフォルダを含む階層構造になっているものを ZIP 形式により圧縮している。今回の長期署名検証ツール OOXmlSignTool では OpenXML ファイルがセットされるとテンプレフォルダに ZIP 形式を展開した上で署名や検証を行うようにした。プルダウンの指定により前述の3方式の署名に対応し、署名ファイルや展開されたフォルダをボタン操作で簡単に開けるようにした。ただし以下制限がある。

1) 最もシンプルな形式の入力ファイルのみ動作確認で他は未対応
2) 複数 (並列) 署名には未対応
3) 未署名の入力ファイルのみ対応で、再署名等の操作には対応しない
4) タイムスタンプ取得は RFC3161 準拠のみ (SHA-2 には対応)
5) Word 形式 (拡張子 .docx) のみ対応で Excel 等のファイルには未対応

以上の制限はいずれも時間的な問題であり、今後時間をかけて実装を続けていけば対応可能な項目である。今回の実装において技術的な問題点はほぼ解決が出来たか目処が立ったのでは無いかと考えている。

1. OpenXML概要

OpenXMLとは、正確には Office Open XML を略して OOXML と呼ばれる XML を利用したファイルフォーマットである。米 Microsoft 社が MS-Office2007 アプリケーションにおける標準のファイル保存フォーマットとして策定した。仕様は公開されており 2006 年には標準規格 ECMA-376 として認証された。2007 年には ISO にて標準採択の投票が行われたが否決された。Microsoft は引き続き ISO 認証を目指している。

ほぼ同じ内容の競合規格としては、オープンソース陣営の OpenOffice.org が策定した ODF (OpenDocument Format) がある。ODF は OpenOffice.org のワープロや表計算アプリケーションの標準ファイル保存フォーマットとして策定され、2005 年には ISO 認証を得ている。標準化の認定では ODF が OpenXML を一歩リードしていると言える。

OpenXML も ODF も画像等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 つのファイルにする等、基本的な技術仕様はほぼ同じになっている。電子署名に関してもいずれも XML 署名を利用している。

OpenXML の電子署名に関しては「Office Open XML - Part2: Open Packaging Conversions (※1)」に仕様の記述がある。ODF の電子署名に関しては仕様としては公開されていないが OpenOffice.org 2.0 より実装はされているので確認は可能な状態にある。OpenOffice.org 2.0 に対応した仕様が ODF 1.2 として公開される予定になっており、これで電子署名の仕様も公開される。現在公開されているのは ODF 1.1 (※2) である。

OpenXML の電子署名を長期保管に適した長期署名化した例は今のところ見当たらない。ODF の電子署名の長期署名化は、既に 2007 年に認証局の 1 つである日本認証サービス株式会社 (JCSI) が証明書の電子申請時に利用した例 (※3) がある。これは国の認定も受けたサービスとなっており、開発は有限会社ラング・エッジが担当をしている。

※1 : 「Office Open XML - Part2: Open Packaging Conversions 」

以下アドレスよりダウンロード可能

http://www.ecma-international.org/news/TC45_current_work/TC45_available_docs.htm

※2 : ODF の仕様書 (注意 : 現在は電子署名未対応の 1.1 まで)

以下アドレスよりダウンロード可能

<http://www.oasis-open.org/specs/index.php#opendocumentv1.1>

※3 : ODF 長期署名実用例

以下アドレスに説明がある

http://www.jcsinc.co.jp/service/a_sign_online.html

2. 長期署名概要

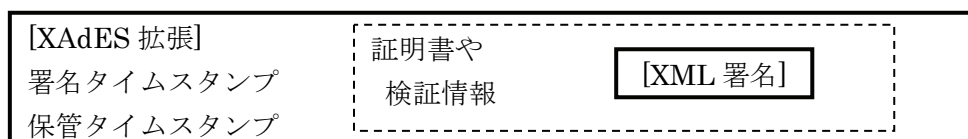
長期署名フォーマットにも種類があるが、現在日本で標準化されているのはタイムスタンプを重ねることで長期保管に対応する XAdES と CAdES が推奨されている。この2種類の長期署名フォーマットは JIS 化作業中でありまもなく認証される予定である。更に XAdES と CAdES は欧州においても ETSI により標準化が完了しており、国際的に通用する仕様となっている。しかしながら米国においては長期署名フォーマットそのものの検討が進んでおらず、米国製ソフトである MS-Office2007 や OpenOffice.org 等のアプリケーションでは長期署名化が進んでいないのが現状となっている。

XAdES と CAdES に機能的な違いはほとんど無く、ベースとなるフォーマットがテキスト形式の XML 署名なのか、バイナリ形式の CMS/PKCS#7 なのかで異なる。この差異によるメリット（利点）とデメリット（欠点）は以下となる。

形式	評価	項目
XML	利点	<ul style="list-style-type: none"> ・近年 XML を採用したドキュメント形式やシステムが増えている ・テキストベースなので可読性が高い ・一般的な XML パーサがあれば専用のライブラリで無くても解析可能
	欠点	<ul style="list-style-type: none"> ・バイナリを含む場合は Base64 化されサイズが大きくなる ・PDF 等レガシーなドキュメントや PKI では CMS 形式が多い ・証明書やタイムスタンプトークン等は CMS 形式のままである
CMS	利点	<ul style="list-style-type: none"> ・PDF 等レガシーなドキュメントや PKI では CMS 形式が多い ・バイナリ形式でありファイルサイズが小さくできる
	欠点	<ul style="list-style-type: none"> ・バイナリ形式の為に可読性が悪く専用パーサが必要 ・XML ベースのドキュメント形式やシステムへの対応が困難

PDF のようにフォーマットの策定が早かったものでは CMS 形式をベースにした方が有利と言え、OpenXML や ODF のように近年策定されたフォーマットでは XML 形式をベースにした方が有利とも言える。両方の形式は競合と言うよりも互いに補うべき存在である。

XAdES の長期署名化は、XML 署名にタイムスタンプや検証情報を追加する事で実現されている。上位互換（XAdES ファイルは XML 署名として検証可能）ではあるが、基本となる署名形式が異なる（XAdES では署名のみでは XAdES-BES 型だがこれには長期署名用のデータが含まれている）為に、署名時において最初から長期署名化を前提にする必要がある。



3. ドキュメントフォーマットと長期署名

現在良く利用されるドキュメントフォーマットは、PDF・OpenXML (MS-Office 文書)・ODF・XPS 等がある。これらは全て電子署名に対応しているが、いずれも長期署名には未対応の状況にある。

文書形式	署名	概要
PDF	CMS	Adobe が策定し 2008 年に ISO 認証された。 電子署名は PKCS#7 形式であり外観を持つことも出来る。 長期署名に関して ECOM で検討されているが幾つか問題がある。
OpenXML	XML	Microsoft が策定し ECMA 認証された。ISO 認証はまだ。 電子署名は XML 署名に独自仕様を加えた形式である。 外観を持つことが出来る。
ODF	XML	OpenOffice.org が策定し 2005 年に ISO 認証された。 電子署名はほぼ XML 署名のままである。 外観は現在は持つことが出来ない。
XPS	XML	Microsoft が策定し、一般に PDF 対抗と言われている。 標準化作業はまだだが今後の普及は見込まれる。 電子署名は XML 署名のようだが現在はまだ未調査。 基本的な構造は OpenXML とかなり共通化されている。 外観の可否に関しても不明。

1) PDF 長期署名の現状

PDF は配布フォーマットとして最も普及していると言える。ビューワとしての Adobe Reader の普及率もほぼ 100%と言えるし、MacOS-X 等のマルチプラットフォームでも扱える。長期署名化に関しては ECOM 参加企業より PDS/A を長期署名化する案が提出されているが、以下の問題をかかえている。

- ・ PDF/A では添付ファイルが認められていないが ECOM 案では添付ファイルを利用。
→ 将来的に PDF/A で添付ファイルが認められれば解決する。

2) ODF 長期署名の現状

ODF は OpenOffice.org くらいしかネイティブ対応していないが、MS-Office 用のプラグイン等は Microsoft から提供されている。長期署名は単に標準の XML 署名を長期署名化するだけで良い。ODF 用には署名日時用に独自の Obejct 要素の追加が必要だが長期署名と競合することは無い。

3) OpenXML 長期署名

今回の調査と開発目的が OpenXML の長期署名化であった。調査の結果 ODF 同様に標

準の XML 署名の長期署名化に関して仕様自体の策定は可能だが、MS-Office2007 においては検証エラーになってしまうことが判明した。Microsoft が MS-Office2007 の仕様を変更してくればこの標準的な長期署名で対応が可能となる。現状では標準の XML 署名のファイルを署名対象として新たに拡張の長期署名ファイルを作成する事で、OpenXML を長期署名化させる方法が現実的であろう。詳しくは次章以降で解説。

4) XPS 長期署名

詳しく調査は必要だが、XPS も XML 署名により電子署名が可能になっている。構造も OpenXML とほぼ同じであり、OpenXML と同様の方法により長期署名化は可能である可能性が高い。しかしまだ未調査の段階であり、一般的にも検討されていないようである。

4. OpenXML長期署名

XML 署名された既存の XML 署名ファイルを後から長期署名 (XAdES) 化することは出来ない。署名時から長期署名用に署名付与して XAdES-BES 形式にしておく必要がある。

OpenXML を採用している Office2007 や、ODF を採用している OpenOffice.org では標準の署名形式が XML 署名である。しかしながら XAdES 形式の長期署名を付与するには標準の署名機能を使わずに、別途署名時に長期署名形式の XAdES-BES を作成する必要がある。生成された長期署名ファイルは XML 署名として検証が可能なので基本的には Office2007 や OpenOffice.org のアプリケーションでの検証も可能であるはずである。

ただし OpenXML が XML 署名を採用しているからと言っても独自に拡張されている。調査した結果、OpenXML においては必須の Object 要素 (Package-Specific Object : Id は "idPackageObject" 固定) と、オプションの Object 要素 (Application-Specific Object) を標準の XML 署名に対して追加すれば良い事が判明している。

長期署名対応とするにはこの 2 種類 OpenXML 用の Object 要素に加えて長期署名用 Object 要素を追加する必要がある。長期署名用 Object 要素を追加して MS-Office2007 が検証を通して見たところ MS-Office2007 では長期署名仕様の XML 署名ファイルの検証は通らなかった。

ECMA による ISO に対する OpenXML の仕様書 (Final Draft) では「Part2: Open Packaging Conventions」の「1 2 . Digital Signature」では OpenXML 独自の Package-Specific と Application-Specific が指定可能とあるものの、他のタイプの Object 要素に関しては何も記載が無い (駄目だとも書いてない)。少なくとも MS-Office2007 で長期署名 Object が許されないと OpenXML ではそのままの形式での長期署名 (XAdES) 化は困難だと言える。

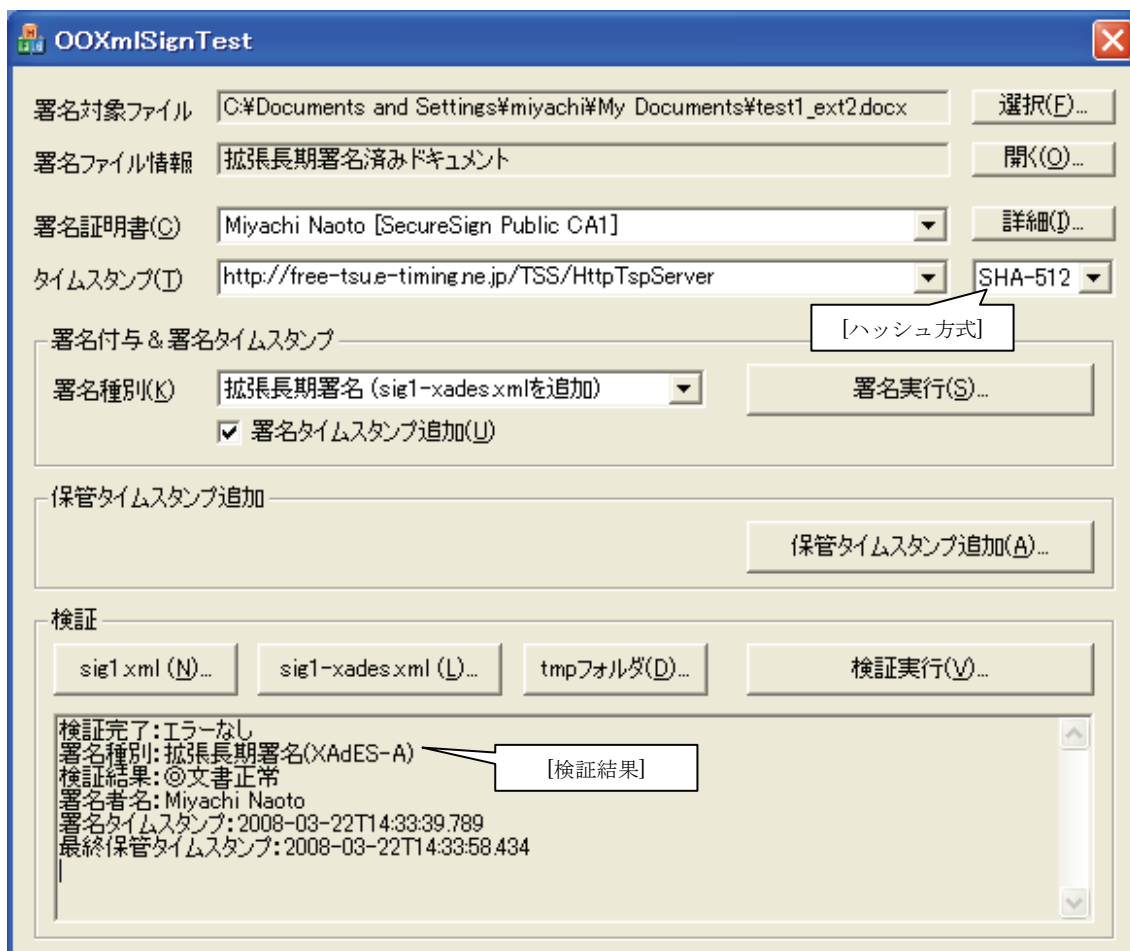
OpenXML の長期署名 (XAdES) 化が現在は実現できない状況にある。この場合に対応可能な方針としては以下の 2 通りが考えられる。

1) Microsoft に交渉して長期署名 Object を OpenXML の仕様に追加して貰う
2) OpenXML 標準の署名ファイルに対して別途長期署名を付与する

今回の開発では上記 2 種類のいずれの方法でも署名と検証を可能としておき、デフォルトの設定では 2) の別途長期署名ファイルを生成する方法を採用する方針となった。

5. OpenXML長期署名ツール OOXmlSignTool

OpenXML 長期署名を確認するツールとして OOXmlSignTool を開発した。



署名種別の指定により、「標準 XML 署名」「標準長期署名」「拡張長期署名」の各方式により署名の付与が可能。保管タイムスタンプは「標準長期署名」「拡張長期署名」に対してのみ可能となる。OOXmlSignTool を開発するにあたり、以下の第 3 者が著作権を持つソフトウェアを利用している。Le-XAdES ライブラリは今回開発の目的に限り無償貸与されている。OpenXML 長期署名は Le-XAdES ライブラリの拡張プロジェクトとして開発されている。Info-zip で ZIP 圧縮も可能だが OpenXML の一部ファイルが特殊文字を使っている為に対応できず、ZIP 圧縮のみ zlib を使った。

名称	ライセンス	目的	アドレス
Le-XAdES	無償貸与	長期署名と ASN.1 解析他	http://www.langedge.jp/
Info-zip	BSD ライク	ZIP 展開	http://www.info-zip.org/
zlib	Free	ZIP 圧縮	http://zlib.net/

6. 今後の課題

以下に今後の課題と考えられる項目を列挙する。

1) MS-Office における長期署名の容認

「標準長期署名」形式の署名は現在の MS-Office2007 では検証エラーとなってしまいう問題が残っている。これは Microsoft 社が対応してくれないと解決しない問題であり、今後問合せや修正の要請をすることは意味があるだろう。ODF では長期署名化できている点は依頼する場合に有利に働く可能性がある。

2) より複雑なドキュメントへの対応

時間的な問題もあり、今回の実装では基本的でシンプルなドキュメントにのみ対応している。実用的なレベルにするには OpenXML の仕様をもっと細かくチェックすることでより複雑なドキュメント形式への対応作業が必要であろう。

3) 複数署名や再署名への対応

OpenXML では並列署名としての複数署名に対応している。最初の署名は sig1.xml ファイルに保存され、2 番目は sig2.xml に保存される。以下 sigN.xml として N 番目の署名ファイルが作成される。これに対応するのは比較的容易であるが今回は時間的な問題で対応を見送った。また署名済みの場合に再署名を行う機能等も同様に未実装である。

4) 利用可能にする為の作業

実際に利用されるシーンを考慮すると、例えば MS-Office へのプラグインによる機能を提供する等の検討が必要になるだろう。またインストールキットの用意も必要である。他にも品質を高める為のテスト期間も月単位で必要になると予想される。

5) OpenXML のワープロ (Word) 以外の形式への対応

表計算 (Excel) やプレゼンテーション (PowerPoint) 形式に対しても長期署名が可能になるように対応フォーマットを増やす必要があるだろう。

今回の開発において OpenXML 長期署名化に関する基本的な要素技術の蓄積は行えたと考えている。今後はこれをより具体的に作る作業が必要であろう。

付録 1. Info-zipのライセンス

This is version 2007-Mar-4 of the Info-ZIP license. The definitive version of this document should be available at <ftp://ftp.info-zip.org/pub/infozip/license.html> indefinitely and a copy at <http://www.info-zip.org/pub/infozip/license.html>.

Copyright (c) 1990-2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, "Info-ZIP" is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White.

This software is provided "as is," without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the above disclaimer and the following restrictions:

1. Redistributions of source code (in whole or in part) must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions—including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP—must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases—including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names "Info-ZIP," "Zip," "UnZip," "UnZipSFX," "WiZ," "Pocket UnZip," "Pocket Zip," and "MacZip" for its own source and binary releases.

付録2. zlibのライセンス

```
/* zlib.h -- interface of the 'zlib' general purpose compression library
   version 1.2.3, July 18th, 2005

   Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

   This software is provided 'as-is', without any express or implied
   warranty. In no event will the authors be held liable for any damages
   arising from the use of this software.

   Permission is granted to anyone to use this software for any purpose,
   including commercial applications, and to alter it and redistribute it
   freely, subject to the following restrictions:

   1. The origin of this software must not be misrepresented; you must not
      claim that you wrote the original software. If you use this software
      in a product, an acknowledgment in the product documentation would be
      appreciated but is not required.
   2. Altered source versions must be plainly marked as such, and must not be
      misrepresented as being the original software.
   3. This notice may not be removed or altered from any source distribution.

   Jean-loup Gailly jloup@gzip.org
   Mark Adler madler@alumni.caltech.edu

*/
```