L-001

マイナンバーカードを用いた Office Open XML ファイルに対する署名と検証スキーム
Signature and Verification Scheme for Office Open XML Files Using My Number Card

先名健一†
Ken-ichi Sakina

1. まえがき

ネットワークや AI などのソフトウェア技術の進化に伴い、デジタルデータの存在感は増すばかりであるが、デジタルデータは編集が容易なため、その原本性を保証する技術は極めて重要である．中でも、公開鍵基盤(PKI)は、インターネットや電子ファイルの信頼性を担保するのに不可欠な技術であり、その PKI の中核をなすのが電子証明書とデジタル署名である．しかし、電子証明書の発行を民間の電子証明書事業者に依頼すると、発行や運用（失効、更新等）に高いコストがかかるのが現状である．

上記のコスト改善にマイナンバーカードの活用は有効である．マイナバーカードは、地方公共団体情報システム機構（J-LIS）が発行しており、その IC チップには J-LIS をトラストアンカーとする電子証明書が格納されている[1]．この電子証明書は公的に保証されているものであり、これを利用することは企業に大幅なコスト軽減をもたらす[2]．また、個人ユーザにおいても中間業者を介さない個人同士の契約等が可能になる．

一般に、MS Office や Open Office などの電子ファイル（以降、ファイル）において、署名対象は署名者自身か、或いは、ドキュメント全体かである．前者は、通常、ファイルに組み込まれている機能を利用するもので、署名者アカウントと紐づいた電子証明書をファイルに付与することで署名者の真正性を担保する．また後者は、電子証明書による署名をファイルに紐づけてセット にしたものを使う(例えば、ファイルと署名値を含む XML ファイル等を格納したフォルダ)．しかし、前者はドキュメントの真正性を保証するものではないし、後者はファイルと署名を一体化できない、などの課題がある．また、現行の提供サービスでは、両者とも厳格に真正性を保証するには正規の電子証明書が必要で、そのための導入/運用コストが発生する．

本論文で提案するスキームは、上記の課題を解決するもので、署名対象のファイルとデジタル署名を一体化したファイル「署名入りファイル」の生成と、マイナンバーカードの電子証明書を利用することにより、商業ベースの PKI に依存しない公的なトラストチェーンの構築を実現するものである．技術的には、マイナンバーカードのカード AP ライブラリと Java API を用い、Office Open XML(以下、OOXML)ファイルに対して署名/検証するスキームである．

2. マイナンバーカードを用いた署名/検証スキーム

OOXML 形式は、MS Office2007 以降の Office アプリケーションなどに採用されているファイル形式である．この形式で作成されたファイルは、複数の XML 文書や画像ファイルから構成されたドキュメントを ZIP 圧縮によりパッケージ化したものである．この節では、OOXML 形式のファイルとして MS Word ファイルを選び、マイナンバーカードを利用した署名/検証スキームの提案と、その応用について述べる．

† 合同会社 QR テクノロジー　QRTechnology, LLC
e-mail: sakina@qr-technology.matrix.jp

2.1 MS Word のパッケージ構造

図 1 は、提案スキームの実験に用いた MS Word ドキュメントのパッケージ構造である．図 1 に示すように、word/media ディレクトリには 2 つの画像(Image1, Image3)と 1 つの動画(Image2)が格納されている．ここで、試験的に、この Word ドキュメントに 1 つの画像を挿入すると、このディレクトリには、Image1~Image4 の 4 つ動画像ファイルが格納される．このようなパッケージ構造の性質を利用することで、Word ドキュメントとデジタル署名を一体化した署名入り Word ファイルの生成が可能となる．

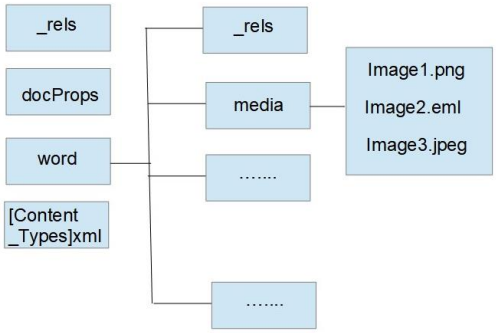

図 1　Word のパッケージ構造

2.2 マイナンバーカードの電子証明書

マイナンバーカードは J-LIS が発行しており、カードの IC チップには標準で 2 つの電子証明書、即ち、署名用電子証明書と利用者証明用電子証明書が搭載されている．前者は、電子文書に署名する際に利用するもので、DER 形式で秘密鍵と公開鍵（RSA2048 bits）及び基本 4 情報（氏名、性別、生年月日、住所）などが格納されている[1]．また、後者は、マイナンバーカード利用者の本人確認などに利用される．

2.3 署名/検証スキーム

ここでは、図 1 の構造をもつ MS Word ファイルを対象に署名/検証スキームを説明するが、OOXML 形式のファイルであれば同様のスキームで署名/検証が可能である．なお、以下では、Word ドキュメントはテキスト部分（メタデータを含む）と動画像部分から構成されているものとする．

(ⅰ) Word ファイルへのデジタル署名

署名は、マイナンバーカード内に搭載されているカード AP ライブラリを利用する．署名アルゴリズムとして、SHA256RSA が採用されている．

次の手順で「署名入り Word ファイル」を生成する．

① テキスト部分の最終行以降の任意の位置に、署名者名、住所、日時等を含む署名欄を作成する．

② Word ドキュメントのテキスト部分と動画像部分(Imege1~Image3)のハッシュ値を求める．
③ ②で求めたハッシュ値をもとに、カード AP ライブラリを利用して 2048 ビットの RSA デジタル署名値を算出する．
④ IC チップから署名用電子署名書を取り出し PEM 形式に変換する．
⑤ 上記で取得した電子証明書とデジタル署名値をそれぞれ QR コードに変換した後、それらを署名欄に挿入して（図２）、署名入り Word ファイルを生成する．

署名：K Sakina 2024-5 月-01

図２　署名入り Word ファイルの署名部分
（電子証明書に対応する QR コードは不可視になっている）

署名入り Word ファイルのパッケージ構造を図 3 に示す．図 3 から分かるように、word/media ディレクトリには、Image1.png, Image2.eml, Image3.jpeg. Image4.png, Image5.png の５個のファイルが存在している．このうち、Image4.png と Image5.png は、それぞれ電子証明書とデジタル署名値に対応する QR コードである．

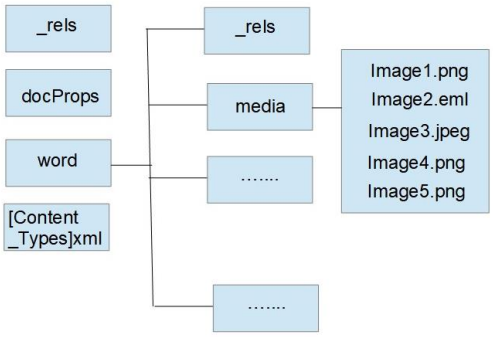

図３　署名入り Word ファイルのパッケージ構造

(ⅱ) デジタル署名の検証
一般に、検証者は署名者と異なることから、ここでは、検証にカード AP ライブラリは使用せず、Java の標準ライブラリを用いる．
次の手順でデジタル署名を検証する．
① 署名入り Word ファイルのテキスト部分と QR コードを除いた動画像部分(Imege1~Image3)のハッシュ値を求める．
② ２つの QR コード（Image4、Image5）から電子証明書とデジタル署名値を取り出す．
③ ①と②及び Java のインターフェース Certificate を用いて、デジタル署名の検証を行う．検証結果が OK であれば、署名入り Word ファイルの真正性が確認される．

2.4 提案スキームの特徴

通常の公開鍵技術では、ファイルにデジタル署名すると、ファイルとは別に XML 署名（デジタル署名の XML 形式）と電子証明書がセットで付与されるが、ファイルは署名データと一体化されていない．提案スキームでは、電子証明書とデジタル署名を画像（QR コード）としてファイルに埋め込むことでファイルの一体化を実現している．この一体化は、次に述べるような複数人による署名/検証を可能にする．

2.5 ユーザ同士の電子契約

ここでは、提案スキームの応用として、2 者間で交わす電子契約書への署名/検証について述べるが、N者間($N = 2,3,\cdots$)の署名/検証も可能である．また、署名者と検証者は共に既述の署名/検証スキームを実装した署名/検証アプリケーションを所有しているものと仮定する．
いま甲乙の２者で交わす署名について考える．最初に、署名フォーム(図４から QR コードを除いたもの)を含む電子契約書を両者で共有する．次に、甲（乙）は既述の署名スキームに従って署名した電子契約書を乙(甲)に送付し、乙（甲）は受信した電子契約書に署名を追加する（図４）．
甲または乙の署名の検証では、既述の検証スキームに従い検証する．ただし、必要に応じて民間認定業社等を介して J-LIS にアクセスし、電子証明書の有効性を確認する．
上記のような契約方式は、第三者を介さない公的に保証されたユーザ同士の契約を可能にする．この応用例から分かるように、提案スキームを実装したアプリケーションは、P2P(Peer to Peer)ネットワークと相性がよく、非中央集権型のアプリケーションとみなすことができる．

（甲）住所　○○県○○市○○町○丁目○番地
氏名　○○　　○○

（乙）住所　○○県○○市○○町○丁目○番地
氏名　○○　　○○

図４　契約書の署名部分

3. 今後の展望

昨年、筆者は、誤り訂正符号と楕円曲線デジタル署名アルゴリズム(ECDSA)を混合したアルゴリズム（以下、EC-ECDSA）を提案した[3]．EC-ECDSA による署名(EC-ECDSA 署名)を用いると、ファイルの形式に関係なく、Open Office、画像、PDF など、殆どすべてのファイルへの署名が可能で、しかもファイルと EC-ECDSA 署名は一体化している． ただし、EC-ECDSA 署名は、上記のような２者間の電子契約には対応できない．
今回提案のマイナンバーカードを用いた手法を EC-ECDSA 署名に適用すると、J-LIS を基点とする公的に保証されたトラストチェーンにより、ファイル形式に関係なく、どのようなファイルに対しても、その真正性は公的に担保されたものになる．今後は、マイナンバーカードと EC-ECDSA 署名を組み合わせた署名アルゴリズムとその応用について研究を進める予定である．

参考文献

[1]J-LIS，“利用者クライアントソフトに係る技術仕様について”,
https://www.j-lis.go.jp/jpki/procedure/procedure1_2_3.html
[2] 西村幸浩, 小野津宗之, 志賀正裕, “マイナンバーカードの技術仕様と利活用方式”, FUJITSU.68,4,pp.59-65(2017)
[3]先名健一, “ 誤り訂正符号とデジタル署名を用いた斬新な画像認証スキーム”, 信学技報, vol. 123, no. 134, EMM2023-28, pp. 91-96,