JNSA ワーキンググループ紹介

標準化部会・電子署名ワーキンググループ

三菱電機株式会社
電子署名 WG リーダー　宮崎　一哉

1.はじめに

現在の電子署名WGは2013年4月に発足してはや9年が経過します。(「現在の」といったのは、2003年頃に電子署名検討WGというワーキンググループがあったからです。https://www.jnsa.org/active/press/vol8/3-1WG.pdf)

2014年3月発行のJNSA Press 第37号（https://www.jnsa.org/jnsapress/vol37/5_WG.pdf）及び2018年3月発行のJNSA Press第45号（https://www.jnsa.org/jnsapress/vol45/3_WG-1.pdf）で現電子署名WGを紹介し、今回が3度目の紹介となります。

2000年前後に日本を含めて各国で電子署名法が制定されてから随分と経ちますし、利用する暗号技術も十分に枯れていますが、未だに活動を続けなければならないことには以下のような要因がありそうです。

・主にコロナ禍に起因する仕事環境の変化に伴う電子契約の登場（新しい電子署名の登場）
・EUでのトラストサービスの法制化（eIDAS規則）とそれに伴う標準規格の充実
・我が国が世界に向けて提唱したDFFTでのトラストサービスの重要性への認識の高まり
・DXを始めとしたもろもろの電子化推進でのトラスト技術の必要性

電子署名WGは発足以来、100回以上の定例会議を重ね、テーマによってはアドホック会議も実施しつつ、また合宿で集中討議を行いながら、数々の成果を生み出してきました。本稿では、前回の報告以降、どのような変化があり、どのような検討をし、どのような成果が得られたかを差分を中心に紹介します。

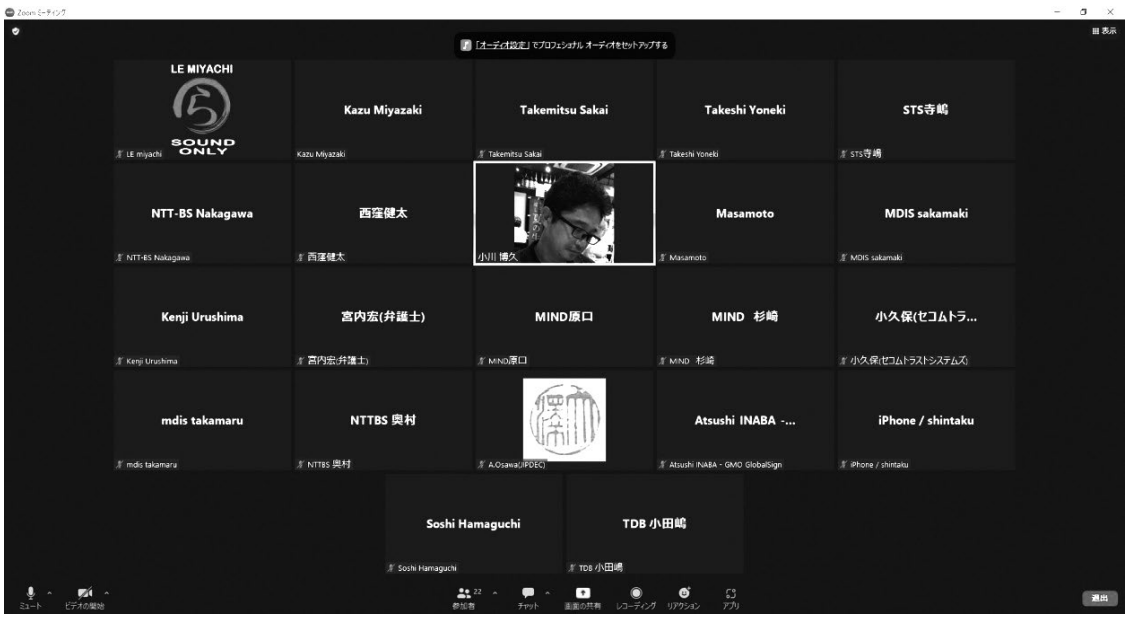

図1　最近の定例会議の様子（リモートばかり、、、）

2.電子署名Q&A

2020年9月16日に公開したこのQ&Aの背景には、電子契約の台頭に伴い、新たな電子署名として、いわゆる立会人型署名（事業者署名型署名）が出現したことがあります。

JNSA ワーキンググループ紹介

電子署名法主務三省（当時：総務省、経済産業省、法務省）から2020年7月と9月の二回にわたり電子契約サービスに関するＱ＆Ａが公開され、その中で立会人型署名（三省Q&Aでは「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う」電子署名と表わされています）に関する見解が示されましたが、電子署名に馴染みのない方にはややハードルが高い内容となっています。このような状況を踏まえ、少しでも多くの方に電子署名に対するご理解を深めていただけますよう、電子署名WGでは「電子署名Q&A」を作成し、公開することといたしました（https://www.jnsa.org/result/e-signature/e-signature-qa/）。

3.デジタル署名検証ガイドライン

2021年3月31日に作成（4月15日公開）の本ガイドラインは、タイムビジネス協議会（TBF）との共同で2013 年に作成した「電子署名検証ガイドライン」の改定版で、JNSA メールマガジン215号（2021年7月9日配信）でも紹介しています（https://www.jnsa.org/aboutus/jnsaml/ml_bk215.html）。

DXに伴うデジタル化とネットワーク化の進展に伴い、デジタルデータの保証と取り扱う人やサービスの信頼性が、これまで以上に必要とされるようになっています。中でもデータの作成責任とその真正性は、アナログ時代においては「署名」や「押印」によって担保されてきましたが、デジタル時代においては、それに相当する技術として「電子署名」があります。

署名は文書等にそれが付与され、受領者が署名を確認することで文書等の真偽や価値の判断材料となります。しかし、可視データであるアナログの「署名」や「押印」と違い、「電子署名」は機械処理としての「署名検証」が必要であり、検証ツール（ソフトウェア）に依存せざるを得ません。さらに、電子署名は様々な要素から構成されており、その判定には細心の注意を必要とします。その判定基準が検証ツールによって異なると、同じデータに対する判定が異なる結果となり、デジタル化の阻害要因となりかねません。それを防ぐため、電子署名のうち公開鍵暗号技術に基づくデジタル署名について検証のためのガイドラインである「デジタル署名検証ガイドライン」を作成しました（https://www.jnsa.org/result/e-signature/data/e-signature-guideline_v1.0_20210331.pdf）。

4.電子署名保証レベル（要約版）

2001年4月電子署名法が施行された時は「電子署名」とは「公開鍵暗号を利用したデジタル署名と公開鍵インフラ（PKI）」を前提としていました。一方で電子認証によるクラウド利用のサービスが一般化したこともあり、電子署名サービスも多様化し色々な電子署名の技術や方式が使われるようになりました。これは本稿の2章でも述べた立会人型署名の出現が典型例です。

従って現在では単純に「電子署名＝デジタル署名＋PKI」とは言えません。しかし技術や方式が異なる電子署名方式の比較は簡単ではありません。「技術に関する電子署名の保証レベル」を専門家が公平に策定し標準化を行い電子署名利用者が目的に合った選択ができるようになることが重要です。

電子署名ワーキンググループでは新たに保証レベルタスクフォースを発足し電子署名の保証レベルの策定を行いました（https://www.jnsa.org/result/e-signature/2022/index.html）。

最終的にはガイドブックの公開を目指していますが、本資料はその要約版として公開したものです。電子署名サービスの仕様検討時や、電子署名の利用者も自身が利用する電子署名の保証レベルを知る為の参考ガイドとして本資料をご利用ください。

5.標準化活動

電子署名関連の標準化は、データの流通、インタオペラビリティ確保に重要であるとともに、それを主導することで日本の状況にも即した内容となることが期待されます。

電子署名WGではISO/TC 154（行政・商業・工業用書式及び記載項目）において長期署名プロファイルの標準規格化を推進しています。

JNSAは2019年にJIPDEC（日本情報経済社会推進協会）からISO/TC 154の国内審議団体を引継ぎました。長期署名プロファイル国際標準規格であるISO 14533シリーズは電子署名WGメンバーが主導して標準化を行って来ました。現在、ISO 14533シリーズは現在Part1からPart4までの4種類が発行されています。

2021年10月4日には、XAdES長期署名プロファイル国際規格の改定を達成しました。これは、日本（JNSA）が提案しプロジェクトリーダーとして標準化していた、XML署名をベースとしたXAdES長期署名プロファイルの2nd editionへの改定です。今回の改定では最新仕様にすると共に、欧州eIDAS規則仕様との互換性もまとめました。コロナ禍にニーズが高まっている電子（デジタル）署名国際標準規格の最新版となります。

また、ECOM（次世代電子商取引推進協議会）で策定した次の長期署名プロファイルのJIS原案作成もJIPDECから引き継ぐこととなっています。

- JISX5092:2008 CMS利用電子署名（CAdES）の長期署名プロファイル
- JISX5093:2008 XML署名利用電子署名（XAdES）の長期署名プロファイル

6.おわりに

電子署名WGのアクティブメンバーは20名から30名ほどです。月1回の定例会議のほか、頻繁な懇親会や合宿が特長です（コロナ禍の影響でここ数年は実施できませんでしたが、、、）。

今後は、電子署名のJISの改定とPAdES版の作成、電子署名保証レベルに関する報告書の作成、デジタル署名の検証結果を表現する検証レポートの標準案の検討を、進めていく予定です。DXを取り入れて業務展開しつつ信頼性を高めたい方、あるいは、社会のトラストに貢献したい方、ぜひ一緒に活動していきましょう。

なお、電子署名WG及びJT2Aの最近の成果（図2）は次のURLが示すページで紹介していますので、ご活用いただければ幸いです。
https://www.jnsa.org/result/e-signature/

図2　電子署名WG/JT2A　報告書・成果物のページ