JNSA ワーキンググループ紹介

JNSA 標準化部会・電子署名ワーキンググループ

電子署名 WG リーダー
三菱電機株式会社　宮崎　一哉

■ はじめに

2013年4月に標準化部会のもとに電子署名WGを立ち上げてから5年が経過しました。その当時の意気込みを思い出しながらこの5年で達成したこと、達成できなかったことを振り返るとともに、電子署名WGコアメンバの溢れる思いから派生的（噴出的?）に設立することとなった日本トラストテクノロジー協議会（JT2A）について紹介します。

■ これまでの活動について

電子署名WGは標準化部会に属する組織であり、その主要な目的は電子署名に関わる標準化です。標準原案作成タスクフォースが標準化を推進するタスクフォースです。この5年間で関わってきた標準のいくつかを表1に掲げます。標準化のためには国内外で開催される標準化会議に出席することはもちろん、電子署名の規格にはETSI/TC ESI(欧州電気通信標準化機構/電子署名基盤技術委員会) が大きな影響力を持っているため、電子署名WGではETSIの会員となり、欧州で開催される電子署名関連の会議に参加して必要な調整を行ってきました。

表1　標準化活動

組　織	規　格	概　要
ISO/TC 154	ISO 14533-3:2017 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)	PAdES（PDF 長期署名）プロファイル規格を策定。発行済み。
ISO/TC 171	ISO 32000-2:2017 Document management -- Portable document format -- Part 2: PDF 2.0	PAdES 規格部分の策定に協力。 発行済み。
	ISO/CD 19005-4 Document management -- Electronic document file format for long-term preservation -- Part 4: Use of ISO 32000-2 (PDF/A-NEXT)	PDF/A-NEXT の長期署名規格部分の提案に協力。委員会原案段階。
ISO/IEC JTC 1/SC 34	ISO/IEC 26300:2015 Open Document Format for Office Applications (OpenDocument) v1.0	OpenDocument の長期署名規格部分の策定に協力。発行済み。
	ISO/IEC 29500 : Part 2: Open Packaging Conventions	Office Open XML の長期署名規格部分の提案に協力。改定準備中。
ISO/TC 215	ISO 17090-4:2014 Health informatics -- Public key infrastructure -- Part 4: Digital Signatures for healthcare documents	医療情報向けの電子署名プロファイル規格策定に協力。現在改定に協力中。

JAHIS（一般社団法人保健医療福祉情報システム工業会）	JAHIS ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.1.1	医療情報向けの電子署名プロファイル規格策定に協力。現在改定に協力中。
	ヘルスケア PKI を利用した医療文書に対する電子署名規格 PAdES 編 Ver.1.0	医療情報向けの PAdES プロファイル規格策定に協力。
	JAHIS 電子処方せん実装ガイド Ver.1.0	電子処方せん向けの XAdES（XML 長期署名）プロファイル規格策定に協力。
JNSA	SHA-1 衝突の実現による電子署名への影響と対策	SHA-1 衝突の発見による電子署名への影響と対策につき、JNSA より公表。
TBF（タイムビジネス協議会）	電子署名検証ガイドライン	タイムビジネス協議会との共同作業により、電子署名の検証に関するガイドラインを作成。
TBC（タイムビジネス認定センター）	「SHA-1 衝突の実現」による時刻認証業務認定事業者が発行するタイムスタンプへの影響について	SHA-1 衝突の発見によるタイムスタンプへの影響に関する公表コメント作成に協力。
Cryptrec	「暗号技術ガイドライン」	暗号技術ガイドラインの SHA-1 の電子署名に関する部分の作成に協力。

また、JAHISやCryptrecなどの他団体からの要請に応じ、標準化に協力してきました。電子署名は決して新しい技術ではありませんが、近年の国際的かつ本格的な利用拡大により更に進化（深化）しており、標準化作業もまだしばらく続くことが予想されます。

電子署名WGは、電子署名関連の普及啓発も大きな目的の一つとしており、スキルアップタスクフォースがこれを担当しています。これまで、表2に掲げるような活動を行ってきました。電子署名やそのベースとなるPKIは実装・運用ともに複雑であり、暗号はもちろん、ソフトウェアだけでなくハードウェアの知識を要する場合もあるため、特に若手に対する啓発活動が極めて重要だと認識しています。先進技術に関する勉強会だけでなく、基礎的な技術についても勉強できるような機会を設けようと考えています。

表2　普及啓発活動

形　式	概　要
勉強会	JNSA 内外、国内外の専門家を招き、周辺技術も含む話題の技術の最新動向などの詳細を講義
PKI Day	PKI 相互運用技術 WG との共催で、PKI を様々な観点から捉え、有識者による講演会を実施
定例講演会	毎年春秋の 2 回、電子署名に関連したテーマを設けた基調講演と LT（ライトニングトーク）を実施
ハンズオン	PKI や電子署名のプログラムに実際に触れての基礎から最先端までの実習型の勉強会
ホームページ、フェイスブック	電子署名 WG 関連イベントの通知・紹介や、過去の講演資料等を公開
リンク集	電子署名に関わる主要な情報へのリンク集の提供（図 1）
合宿	定例会議ではできないような深い議論や周辺テーマについての議論をじっくりと実施

JNSA ワーキンググループ紹介

図1 電子署名関連リンク集（http://esig.jnsa.org/portal-search/）　※近日公開予定

■ JT2Aについて

デジタル社会が進展し、あらゆるモノやサービスが連携していく時代となりました。このような社会変革の中で、自身の組織やサービスに対するセキュリティの向上はもちろん、連携を前提とした接続先やデータに対するトラスト（信頼）の重要性が増大しています。電子署名は実在証明やデータ改ざん検知などのトラストを確立するための技術として電子署名WGでテーマアップしていますが、本人や機器等の認証技術や近年話題となっているブロックチェーン、EUのeIDAS規則で定義されたトラステッドリストなど、デジタル社会上でトラストを実現できそうな技術は電子署名に留まりません。電子署名を超えたより幅広い仕組みについて、セキュリティベンダーのみでなくユーザーを含めて利用面からも検討ができないか、との思いが複数のメンバの間に募った結果、新たな組織として日本トラストテクノロジー協議会（JT2A）を設立することとしました（図2）。

JT2Aは、この6月に開催されるJNSA2018年度総会での承認を受け、JNSA傘下にて正式に発足します（http://www.jnsa.org/aboutus/04.html の組織図をご覧ください）。代表として慶應義塾大学の手塚教授に、副代表としてセコム株式会社/PKI相互運用技術WGリーダーの松本様氏に就任頂きます。運営委員長には当協議会発足の第一の功労者であるみずほ情報総研株式会社/電子署名WGサブリーダーの小川氏が就任します。

図2　JT2Aホームページ（http://www.jt2a.org/）

■今後の活動について

電子署名WGでは、今後も標準化と普及啓発を軸に活動を続けていきます。表1に「電子署名検証ガイドライン」を掲げましたが、これは極めて重要で、標準規格にまで完成度を高める必要を感じています。電子署名フォーマットの標準に沿ったデータの生成はできても、それを正しく検証したり、検証結果を誤解の無いように表示したり、といった基準が曖昧では、それこそトラストを形成することはできません。現に検証プログラムによって検証の結果が異なるケースも見られます。ETSI/TC ESIでも2012年頃から規格化を進めているものの、まだフィックスできていないほど困難な作業ですが、2018年度は是非取り組もうと思います。このほか、既存の標準規格の見直しや情報提供のためのホームページや電子署名に参考となるツールの充実化にも取り組みます。

JT2Aでは、リモート署名ガイドラインの作成と「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の改定を2018年度の目標とし、それぞれタスクフォースを設定して取り組むこととしています。前者はマイナンバーカードの有効活用や安全な電子契約サービスを提供することにつながりますし、後者は必要とするトラストを実現するために、どのようなレベルの電子署名や認証を実現する必要があるかの指針となります。

電子署名WG及びJT2AはJNSA会員であればどなたでも参加できます。JT2Aではユーザー企業向けの会員枠も設定予定です。ご興味を感じられた方は是非ご参加ください。