デジタルプラクティス　Vol.9 No.3 (July 2018)

特集招待論文

ディジタル社会のトラストを支える電子署名

小川 博久[1]　宮崎 一哉[2]　佐藤 雅史[3]　宮地 直人[4]　政本 廣志[5]

[1]みずほ情報総研（株）　[2]三菱電機（株）　[3]セコム（株）IS研究所　[4]（有）ラング・エッジ　[5]NTTアドバンステクノロジ（株）

ディジタル社会が進展するとともに，あらゆるモノやサービスが連携していく時代となった．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さることながら，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る．電子署名はデータ改ざん検知や否認防止などのトラストを確立するための技術として従来から活用されているが，近年のデータ利活用の促進に伴い，ますます利用分野が拡大している．さまざまな組織，業界，国境を越えて利活用を円滑に進めるためには，具体的な運用を想定した仕様策定や国際化に向けた相互運用性を踏まえた標準化の取り組みが重要である．本稿では，JNSA電子署名WGで行ってきた長期署名プロファイルの標準化やリモート署名の検討を通じて得られた，電子署名のような基盤技術を標準化・普及促進する際の知見について報告する．

1. トラストと電子署名

昨今のディジタル化の進展とあらゆるモノがネットに接続される状況において，ネットを介して仮想と現実が混在する世界で，何をどのように信頼すべきかは重大な課題である．ディジタルデータの真正性の確保とネット越しの相手（人，モノ，サービス等）の確実な認証，相手の意思の確認（否認防止）は信頼（トラスト）の根幹であり，ディジタル時代の社会システムの基盤機能といえる．

従来から改ざんや否認を防止する技術として，公開鍵暗号基盤（PKI：Public Key Infrastructure）を利用した電子署名技術があるが，広く普及していく上で２つの課題があった（**図1**）．

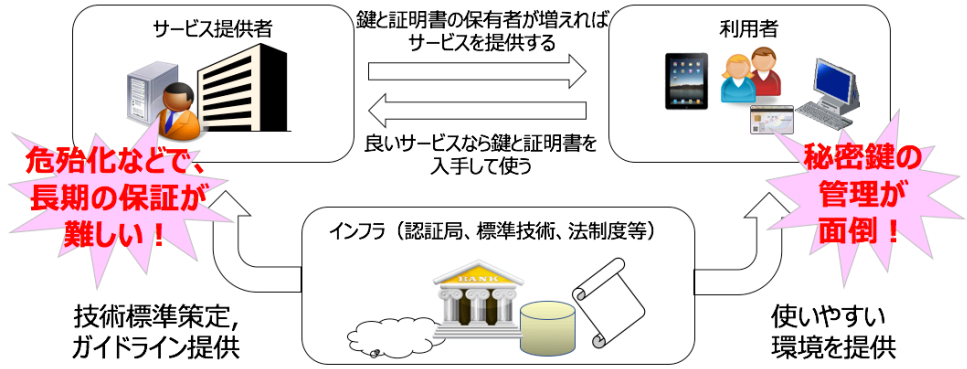

図1　PKI・電子署名普及の課題

1つは，あらゆるものがディジタル化され，保管される状況になると長期間の保証も必要となるが，現代暗号の宿命である暗号危殆化等により，時間が経つと電子署名の効力が失われるという課題である．これに対して，長期に電子署名の有効性を保証する技術として長期署名があるが，実用に供するための基準や標準がまだなかった．

筆者らは，その標準化の検討が進みつつあった欧州のETSI（European Telecommunications Standards Institute）と連携しながら日本ではECOM☆1（電子商取引推進協議会）メンバ（現在はJNSA（日本ネットワークセキュリティ協会）に所属）を中心に長期署名のプロファイル策定と標準化を推進[1], [2]した．その対象は，一般データ用のCAdES，文書やWebデータに適したXML用のXAdES，ポータブル性の高いPDF用のPAdESである．本稿ではこれらの標準化の経緯と取り組みについて，海外との調整状況も含めて述べる．

2つ目の課題は，署名用の秘密鍵の管理方法である．PKIは利用者が安全に秘密鍵を所有していることが大前提であり，ICカード等の耐タンパデバイスに格納することが主流であったが，そのコストや管理の面倒さが普及の阻害要因となっていた．マイナンバーカードの普及が期待されるが，ほかにもさまざまな用途の鍵所有のニーズがある．

このようなニーズに対応する方法の1つが，サーバに鍵を預けて署名をリモートで実施するリモート署名である．筆者らはその活用と普及に向けた取り組みを行ってきた．本稿では，法制度との関係や実現モデルの検討状況について説明する．

本稿は，以下，第2章で長期署名の標準化について，第3章でリモート署名の検討について，第4章で長期署名やリモート署名を業務に取り入れる動きについて紹介する．

2. 長期署名プロファイルの標準化

2.1　活動の経緯

2000年に電子署名法（電子署名および認証業務に関する法律）が制定された際，すでに一部では電子署名が長期にわたる使用に耐えないことが認識され，問題視されていた．具体的には，契約書等の押印文書や署名文書を後々の係争に備えて証拠として保存する観点からの手当てがないという問題であった．電子署名の本来果たすべき機能は，係争が生じたときあるいは説明責任に応える必要のあるときに，「署名者が署名対象にコミットしたこと（署名者が署名対象の内容が示す何らかの約束をしたこと）」を証明することである．それが時間を経過することによりできなくなってしまうという課題があった．

長期にわたる使用時，以下の3つのいずれかの事象が生じた場合，それ以降は電子署名が有効性を失うことになる．①公開鍵証明書の有効期間（長くても5年程度）の超過，②公開鍵証明書の失効（有効期間内でも状況により有効性を喪失），③電子署名で利用されている暗号アルゴリズムの危殆化（技術の進歩により避けられない）．

そこで筆者らは，2000年4月， ECOMの認証・公証WGでこの『電子署名の長期有効性保証の問題』を取り上げ，対策の検討を開始した．調査の結果， ETSI ES 201 733 V1.1.2 "Electronic Signature Formats"を中心にすえて，グローバルな相互運用性確保，妥当性の検証，規格完成に向けた協調，国内への導入のための基盤整備などを目標に活動することとした．このETSI ES 201 733 V1.1.2 はETSIが2000年1月に公開したCMS（Cryptographic Message Syntax）をベースとしたCAdES（CMS Advanced Electronic Signatures）と呼ばれる電子署名規格案である．これは1999年に制定されたEU電子署名指令の中で定義されている「先進電子署名（Advanced Electronic Signatures）」の最初の規格案でもある．

2.2　CAdES

本節では，長期署名フォーマットCAdESに対するプロファイルの標準化に至る経緯とそこから得られた知見について述べる．

CAdESは，XAdES，PAdESに先立ち最も早く出現した長期署名フォーマットである．バイナリ形式の暗号メッセージフォーマット規格であるCMSで定義された署名データ形式（Signed-data）を拡張したものである．2000年初頭に最初の規格案が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）より発行された．現在では改定が進み，EU（欧州連合）のeIDAS規則（Electronic Identification and Trust Services Regulation 910/2014/EC）で規定された電子署名形式の一端を担うべく，欧州規格として制定されている．

2.2.1　長期署名フォーマットの基本的考え方

前述の問題①～③が生じても当初の電子署名が有効性を失っていないことを確認できるようにするため，CAdESでは，CMSの署名データ形式（Signed-data）のオプション領域に，署名タイムスタンプ，署名検証情報，アーカイブタイムスタンプを追加する [3]（**図2**）．署名タイムスタンプは署名生成時刻（正確には存在時刻）を証明するためのタイムスタンプである．署名検証情報とは，署名生成時刻における署名者証明書からルート証明書までの認証パスと各々の失効情報を指す．アーカイブタイムスタンプは，それらのデータに署名対象文書と署名タイムスタンプ，および署名検証情報を含む電子署名データの全体を保護するためのタイムスタンプである．

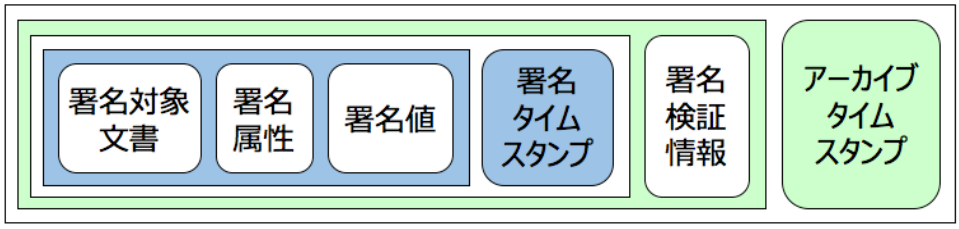

図2　長期署名フォーマットのイメージ

これら3つの情報を追加する考え方はXAdES，PAdESでも同様である．

2.2.2　リモートプラグテストによる相互運用性試験の改善

CAdES等の長期署名フォーマットは複雑であり，フォーマットの生成処理や検証処理の実装には困難を伴う．フォーマット仕様の妥当性確認や標準仕様ドキュメントの曖昧性を排除するために，ETSIではほぼ毎年プラグテストと呼ばれる相互運用性試験を実施している．日本でも仕様確認のため参加を模索したが，当時は欧州の開催国に機材を持ち込み，対面で試験を実施しており，参加は容易ではなかった．

そこでECOMでは，試験データや各機関で生成したデータをインターネットを介して交換することによる「リモートプラグテスト」を2005年と2007年に実施した．結果は良好であり，従来の対面によるプラグテストと遜色のない成果を得ることができた．

さらにECOMはリモートプラグテストで得られた標準仕様のあいまい性や不具合等の知見により，ETSIにアーカイブタイムスタンプの相互運用性の問題を指摘し，後のアーカイブタイムスタンプV2仕様への改訂に繋げることができた．これにより相互運用性の問題は解消され，日本ではV2ベースでの運用が広がった．またリモートプラグテストの手法についても紹介したことにより，ETSIでは2008年より対面ではなく遠隔でのプラグテストを実施するようになった．

2.2.3　長期署名プロファイルの標準化

日本では，必須ではない多数のパラメータの中から電子署名データの長期有効性保証を確保するために最低限必要なパラメータのセットを選定することにより，『プロファイル』として規格化することとした．前述の通り，複雑な仕様を持つフォーマットであるが，ユースケースを特定することにより，生成においても検証においてもすべての仕様を実装する必要はなくなる．この取り組みについて以下で説明する．

プロファイル標準化は2005年から10年をかけて策定を進めた．まず，ECOMでのリモートプラグテストの結果を反映し，2005年にECOM長期署名プロファイルを策定した．その後，2005年のe-文書法制定に伴い，長期署名の必要性が高まるとの見通しから，JIS化を目指し，2008年にJIS X 5092（CAdES）およびJIS X 5093（XAdES）を制定，2012年にはそれぞれISO 14533-1および14533-2として制定した．ISO 14533-1は2014年に改版されている．

プロファイルの策定にあたっては，オリジナル規格を所管するETSIとの調整が欠かせない．プロファイルとしては，オリジナルが必須の場合はそれを継承し，オプションの場合はそれを必須とするか，使用禁止とするか，オプションとして残すかを定義するのが基本である．

我々は，電子署名を長期にわたって検証可能とするために，セキュリティの観点から必要なもののみを必須として残し，それ以外は極力オプションあるいは使用禁止とする考えで臨んだ．

EUからの要請で，不要と思われるパラメータがオリジナルでは必須となるケースもあった．一例を挙げると，電子署名フォーマットの署名時刻（SigningTime）という署名対象データをオリジナル規格では必須としている．この値は通常，電子署名を生成するPCの時計の示す時刻が格納されるもので，署名者により自由に変更ができ，信頼のできない時刻である．この問題はPAdESプロファイルの策定においても生じた．対処を含め同様な経緯をたどったため，詳細は2.4.2節に記す．

このプロファイル規格制定により，実装の容易化と相互運用性の確保が進んだ．プロファイルはオリジナル仕様のサブセットであることから，実装を要する範囲は縮小される．また規格制定により，仕様の解釈のぶれは抑えられ，実装も容易となる．結果として相互運用性の確保もよりスムーズになる．実際，相互運用性を重視する医療情報分野では，ISO 14533シリーズにさらに

制約を加えたプロファイルとしてISO 17090-4: Health informatics -- Public key infrastructure -- Part 4: Digital Signatures for healthcare documentsを2014年に制定している．

2.2.4　CAdES標準化活動により得られた知見

この活動を通じて得られた知見としては，標準化は，傍観していると日本では受け入れがたい規格ができてしまう恐れがあり，常に積極的な発信が必要だということが挙げられる．標準化活動は実装や運用に長じた者が行うとは限らず，実際の利用にあたって支障をきたす恐れがある．また，ETSIにはEUの事情を反映するミッションが与えられており，欧州規格のISO化によりEU外での利用や相互運用性が制限される可能性もある．電子署名分野においては日本からの貢献についてはETSI側も認識しており，妥協点を見出すことができたが，これからも対等に交渉できるよう発信し続けることが重要である．

> 後を追うだけではだめ．標準化活動には積極的に参加しよう！

2.3　XAdES

本節ではXAdES（XML Advanced Electronic Signatures）の標準化にあたり，長期署名の専門家が少ないPDFやオフィス等の文書仕様を扱うドキュメント分野に対して，複数の仕様間の矛盾点を整理し，対策を講じていった取り組みについて述べる．

XAdESはXML（Extensible Markup Language）形式の長期署名である．ベースはW3C勧告のXML署名（XMLDSig）であり，ETSI ESIにより拡張され標準化された．長期署名としての基本的な考え方はCAdESとほぼ同じであるが，署名対象の指定方法と署名対象の広さに特徴がある．署名対象の指定方法では，複数の署名対象ごとにハッシュ値を持ち，個別に改ざん検知が可能であり，Detached（外部参照）・Enveloped（外包：署名埋め込み）・Enveloping（内包：データ埋め込み）の3種類から選択できる．また署名対象はXML以外に画像等の任意バイナリデータの指定も可能である．これら署名対象に対する柔軟性がXML署名とXAdESの最大の利点である．

2.3.1　XML系標準化の経緯

テキストベースのデータ記述言語として使われているXMLは通信やWeb系APIにおいて多く使われている．近年ではドキュメント分野においても多く利用されている．ドキュメント編集時にアプリケーションとして，MS-Word/MS-Excel/MS-PowerPoint ☆2がよく使われているが，これらのMS-Office系で使われているドキュメントフォーマットはOOXML（Office Open XML）であり，XMLデータをZIP圧縮した形式を採用している．同様なドキュメントフォーマットとしてODF（OpenDocument Format）やEPUB（Electronic PUBlication）があるが，XMLデータをZIP圧縮したフォーマットである点は共通である．ドキュメントには改ざん防止や否認防止等の目的による署名ニーズがあり，OOXML/ODF/EPUB等のXML系ドキュメントでは署名フォーマットとしていずれもXML署名が採用されている．

これらXMLベースのドキュメントを標準化しているのがISOのJTC1 SC34である．SC34では近年XML署名からXAdESへの移行検討が行われてきたが，JNSAは長期署名に関するサポートをするためにSC34のリエゾンとして活動してきた．XAdESの利用に関しては，OOXMLは現在作業中，ODFは採用済み，EPUBは検討中となっている．

2.3.2　OOXMLへのXAdES採用

OOXMLでXAdESを採用するには，MS-Office既存仕様との互換性の点で課題が残っている．この経緯と解決状況を以下で説明する．

OOXMLはMS-Officeが採用しているドキュメントフォーマットである．実は最大の問題はOOXML標準化においてXAdESが採用される前に，MS-Officeにおいて独自にOOXMLへのXAdES実装が行われた点であった．残念なことにいくつかの点で長期署名として間違いではないが一般的ではない実装がされ，世の中に一般的ではない形式のXAdESを利用したMS-Office文書が大量に存在してしまうことになった．

このためにSC34において既存ドキュメントとの互換性も考慮する必要が生じた．議論は紆余曲折があったが最終的に，新仕様ではXAdESの一般的な仕様を取り入れるとともにZIP中のXML署名ファイル名を分けて，新旧XAdESが共存できる仕様にまとまりつつある．強引に過去との互換性を持たせるよりも新旧両方の仕様を併存する道を選んだのである．標準化仕様において過去仕様との互換性は非常に重要なポイントである．

XAdESの元仕様を策定しているETSIにおいて過去何度かXAdES仕様に対応するバージョンアップが行われてきたが，過去仕様との互換性という意味では仕様重複の問題がある．

CAdESの項でも述べたがオプションであったSigningTime要素が必須になる等のEU（欧州連合）としての要望が取り入れられた．またETSIのXAdES最新仕様では，署名対象に対するMimeType要素も必須項目となった．OOXMLはETSIのXAdES仕様を参照しようとしていたため，ETSIの最新仕様を参照するとSigningTimeやMimeType等の必須要素を含まなければならない状況にある．しかしOOXMLではSigningTimeもMimeTypeも別の方法ですでに管理されており，新XAdES仕様と重複してしまう．SC34では現在この対策を検討中である．

2.3.3　XAdESバージョン間の整合性

XAdESの標準化に関しては，バージョン間の整合性について，現在3つの課題がある．1つはXAdESは他の標準から参照されるコア仕様であるが欧州ローカルな標準化団体が管理していることにより国際的な同意なしに仕様が更新される課題，2つ目は仕様改定時にバージョンを上げ損ねたことによる版判定の不備，もう1つは古いバージョンが放置されて過去仕様との整合性を保つことが困難になることである．

ETSIのXAdESは他の標準から参照されるコア仕様であるが，これをETSIという欧州ローカルな標準化団体が管理していることによるリスクが顕在化している．

XAdESプロファイルの国際標準のISO 14533-2は，コア仕様としてETSIのXAdES仕様を参照している．本来はXAdESのコア仕様も国際的なISOで管理されることにより，国際的な同意を経た上で更新すべきである．現在ISO 14533-2の改定を計画しており，日本として欧州ローカルなコア仕様による課題をどうするか検討中である．

ETSIの仕様にはTS（Technical Specification），EN（European Norm，European Standard）等のいくつかの種類がある．TS仕様はETSIで決めることができるが，EN仕様にはEUの要望が強く反映される．元々XAdESの仕様はETSI TS 101 903として，V1.1→V1.2→V1.3→V1.4と進化してきた．XAdESのバージョンはXML名前空間にも利用される重要要素である．MimeType要素が追加されたのはXAdESがEN仕様となったETSI EN 319 132で，本来新しい要素を追加するのであればバージョンを進めV1.5とすべきであった．しかし

EN仕様になったときにV1.4のままとなっており，これではXML名前空間によって仕様バージョンの判定が行えない．JNSAとして早く気がつけばコメントできたかもしれなかったのは心残りである．

古いXAdESコア仕様の放置も課題の1つである．XAdESコア仕様としてはW3CにおいてもXAdES Noteとして2003年に公開されているがバージョンがV1.1という最初の仕様のまま更新されていないために使い物にはならない．いくつかの標準化にて古いW3CのXAdES仕様を参照しようとしていた例があった．W3Cにおいて，XML署名はメンテナンスされバージョンアップされているが，XAdESは古い仕様のまま放置されているために，世の中で多く使われている実装にて検証できないという問題を生じている．一般的にV1.3以降の検証を前提にしている実装が多い．ほかにもXAdESプロファイルのISO 14533-2は2010年のTS仕様V1.4をベースとし，JISのXAdESプロファイルJIS X5093:2008は2006年TS仕様V1.3をベースにしている．（**表1**）．

表1　XAdES仕様のバージョン

仕様名	Ver	Year	補足
ETSI TS 101 903	V1.1	2002	TS 仕様 初版
W3C XAdES Note	V1.1	2003	放置のコア仕様
ETSI TS 101 903	V1.3	2006	TS 仕様 更新版
JIS X5093:2008	V1.3	2008	日本プロファイル 2006 年 TS 仕様参照
ETSI TS 101 903	V1.4	2010	TS 仕様 最終版 今後保守されない
ISO 14533-2:2012	V1.4	2012	国際プロファイル 2010 年 TS 仕様参照
ETSI EN 319 132	V1.4+	2016	TS 仕様 後継版 V1.4 から拡張あり

今後これらのベースをETSI EN仕様のV1.4+とどう整合性をとっていくのかが課題である．

2.3.4　XAdES標準化活動により得られた知見

この活動で得られた知見として，以下の2点が挙げられる．1つ目は，標準仕様は制定されて終わりではなく，広く使われるためには制定後のメンテナンスが重要だということである．すでに一般的ではないV1.1仕様のまま放置されているW3C XAdES Note V1.1 や，V1.3のままの JIS X5093:2008 の改定は課題である．2つ目は，ほかから参照されるコア仕様は，ローカル仕様ではなくISO等の国際標準とすべきということである．実際，コア仕様であるETSI TS 101 903 V1.4 は，その改定もEUに依存している状況にある．

> 標準化は策定して終わりでなくメンテナンスの始まり！

2.4　PAdES

本節では，PDF（Portable Document Format）署名の長期署名化に際して，PDF特有の仕様に起因する問題や，製品化が急速に進み始める状況下で実装に影響する課題を検討していったこと，また欧州規格とISOの規格が並立する中でCAdESのときと同様に日欧の見解の相違が再発し，妥協点を探った状況について述べる．

PAdES（PDF Advanced Electronic Signature）はPDFに適用でき，長期署名への展開も可能な電子署名規格である．最新動向としては2016年にETSI EN 319 142（PAdESの欧州規格）が，2017年にはPAdES仕様を取り込んだISO 32000-2 （PDF2.0）とJNSAが推進したISO 14533-3（PAdESの長期署名プロファイル）が発行された．

PDFは画面や印刷の構図も含めた定義が可能なフォーマットで，人が読むことを想定とした文書や契約書にも向いた主流のフォーマットといえる．PDFの標準的なビューアを用いて契約書などへ電子署名の付与や閲覧をしたいという要望があった．そこで，Adobe社ではPDF 1.3仕様で電子署名をサポートし，それに対応した製品の提供を行ってきた．PDF仕様は元々はAdobe社が管理する規格であったが，2008年頃にISOの管理下となり現在に至っている．PDF仕様のISO規格は2008年にISO 32000-1として発行された．このISO 規格はPDF 1.7仕様に基づいており，上で述べた電子署名仕様も含まれている．この電子署名は通称PDF署名とも呼ばれている．

2.4.1　PDF署名の長期署名化への取り組み

当時の日本では長期署名プロファイルのJIS規格策定に至る議論が進められていたが，その議論の中でPDF署名を長期署名に展開する際の技術的問題が明らかになった．

それは，署名を無効化してしまう恐れがあることと，署名データのサイズの見積りが難しいことである．長期署名は電子署名を生成して時間を経た後，検証に必要な失効情報やタイムスタンプを追加する仕組みとなっている．一方，PDFに署名データが格納される領域は**図3**に示したように，文書データの内容が記された領域と，更新情報やPDF構成情報への参照を格納した領域との間に位置するようになっている．このため，PDF署名をそのまま長期署名化を行うと，元の領域が壊れて署名が無効化してしまう恐れがある．また，署名データのサイズは長期署名の延長処理を繰り返す回数や格納する失効情報の大きさなどにより，署名前に見積りにくい問題もある．

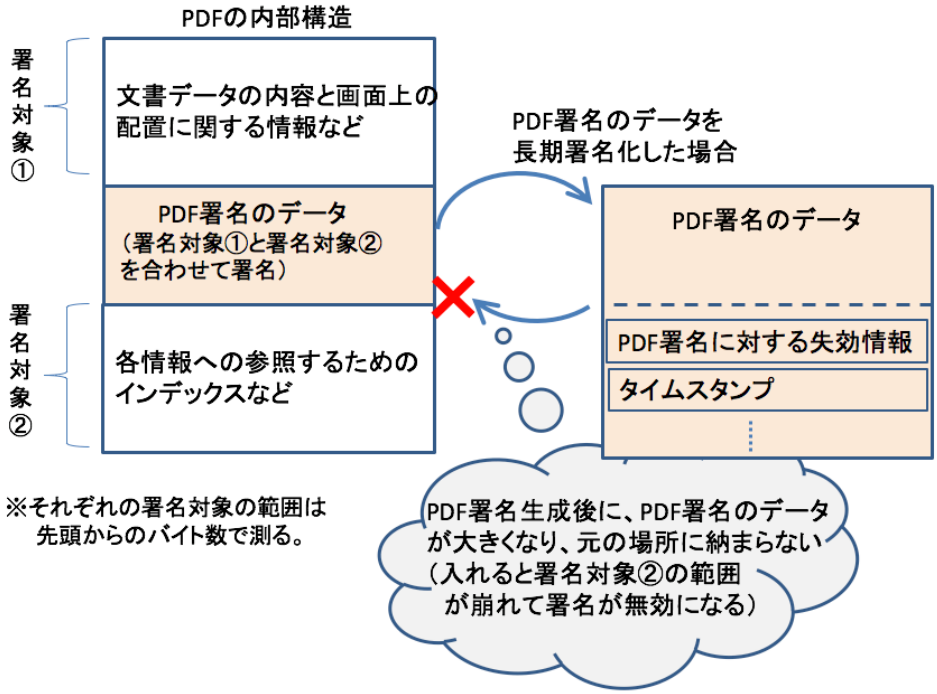

図3　PDF署名の特徴

ECOMではこの問題と解決案をまとめ，当時この問題を認識していなかったETSIにも伝えた結果，Adobe社の専門家も交えた議論に発展した．最終的には日本から提出した案ではなくPDF自体の仕様変更も含めた別の提案（これがPAdESである）が採用されたが，PAdESの起点となったことには大きな意味があった．

2.4.2　PAdESプロファイル標準化の課題と対応

2009年にETSI TS 102 778としてPAdESが発行され，2010年に入ると各社からPAdESに対応した製品も出始めてきた．PAdESが利用され始めるにつれ，また別の課題も見え始めてきた．

ETSI TS 102 778はさまざまな利用を想定し，基本的な要素群の定義に言及をとどめていたが，各要素の使い方や組み合わせ方は厳格に定めていないため，実装者の考え方や使い方によってさまざまな形態のデータが発生し相互運用に問題が起こる恐れがある．たとえば，人による電子署名なしにタイムスタンプだけを適用することは認められるのか，署名・証明書や失効情報の格納・タイムスタンプ付与などを適切な順番で適用していない長期署名の検証をどうすべきか，といった問題である．

長期署名を適切に実施し相互運用性を確保するためには，各要素の使い方のルール作り（すなわち，PAdESに対するプロファイル）が重要である．この仕様作りについてECOMの専門家が議論を重ね，2013年には活動の拠点をJNSAに移し，2014年に経済産業省の国際標準化事業でISO化（ISO 14533-3）を推進していくこととなった．

一方，海外でも2つの動きがあった．1つはPDF2.0 （ISO 32000-2）策定のプロジェクトであり，PDF2.0としてETSI TS 102 778のPAdES仕様が組み込まれることとなった．2つ目はETSIの標準規格の再構築作業である．当時のETSI/ESIはEUのeIDAS規則にかかわる活動に注力しており，EC指令460（mandate460:2009/12）に従い，電子署名に関してもこれまでの規格（TS）を整理統合し，より影響力を持つ欧州規格（EN）へ格上げ，さらにISO化を目指す方針に転換した．

国内と海外の動きの中で，日本が主導する長期署名プロファイルのISOとの整合化が再び問題となり， JNSAとETSI/ESIの代表者を交えてISO 14533-3も含め国際標準化に向けた協議を行った．

これまではETSI TS 102 788が技術仕様のベースとしてあり，EU内での利用を想定したプロファイルは独立した ETSI TS 103 172という規格があった．日本が推進する長期署名プロファイルもそれと独立し併用もできるプロファイルとして位置づけることができた（**図4左**）．しかし，ENへの再構築作業によって，ETSI TS 102 778とETSI TS 103 172はEN 319 142という規格に統合されることなった．さらに，EU向けプロファイルを前提に規格が構築されることになった．つまり，EU向けプロファイルがベース仕様になったようなものである．

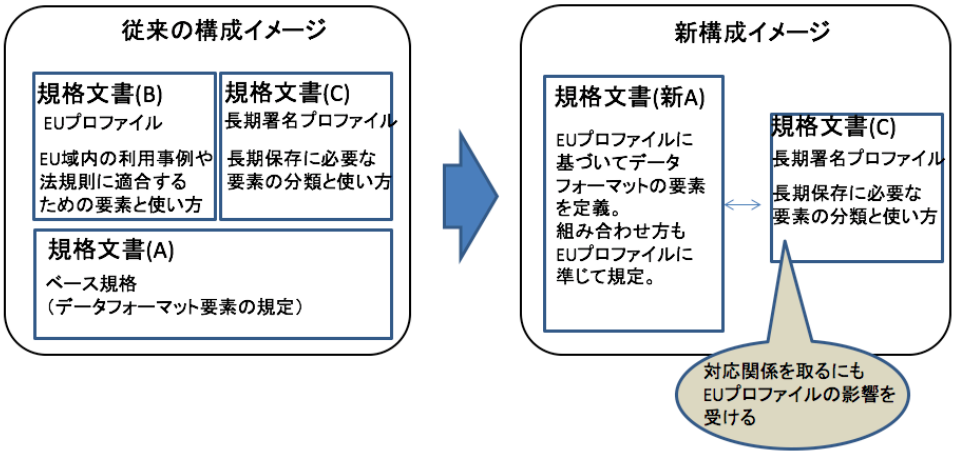

図4　PAdES規格の変遷

この余波を受けた議論の1つの例がSigningTime属性（PAdESではM属性）の問題である．SigningTimeはCAdESの項で述べた通り，必ずしも信頼のおけない時刻であり，この時刻を基準に検証を実施すると不正な署名を受け入れてしまう恐れがある．このような脅威への懸念から日本ではSigningTimeは使用せず，信頼できる第三者機関のタイムスタンプ時刻を使用するように示してきた．これまでのベース仕様ではSigningTimeは必須ではなかったが，EUプロファイルでは必須とされており，EN 319 142ではベース仕様として必須の要件に含まれるため，ISO 14533-3においても必須に変更するよう要求された．ETSIの主張の背景には，各国で築き上げられた既存の制度や仕組みの存在があるのではないかと思われる．この点については，JNSAとETSIで意見が平行した状態が続いたが，最終的には検証に使わないことを前提に必須とする形で妥結した．

2.4.3　PAdES標準化活動により得られた知見

この活動で得られた重要な知見は，規格が必ずしも技術のみでは決まらないということである．電子署名の特徴的な側面といえるが，ETSI側は，電子署名を法制度や社会，慣習などを含めた視点で捉えており，従来の考え方を簡単に変えることはしない．これは電子署名に限らず，技術が社会生活とより一体となっていく時代において，何をトラストの根幹と捉えるかという点で重要な示唆であると思われる．

> 標準化作業は文化のすり合わせ．背景の相互理解が欠かせない

3. リモート署名

電子署名普及のネックとなる秘密鍵（以後，署名鍵と記載する場合もある）管理について，有力な対策がリモート署名である．本節では，その実現にあたって鍵の管理方法や処理の要件について，法制度との関係や，モデル化によるリスク評価を行い，検討してきた経緯について述べる．

3.1 リモート署名の概要と課題

電子署名は従来，署名者の環境において署名鍵を用いて署名していたが，署名鍵をサーバに安全に保管し，利用者の指示に基づきサーバで署名を行う方式が，リモート署名（類似の概念としてサーバ署名，クラウド署名もある）である（**図5**）．一般利用者の管理負担を軽減するとともに，時間や場所の制約を受けずに利用できるマルチデバイス対応を可能として，署名利用の拡大に繋がることが期待されている．

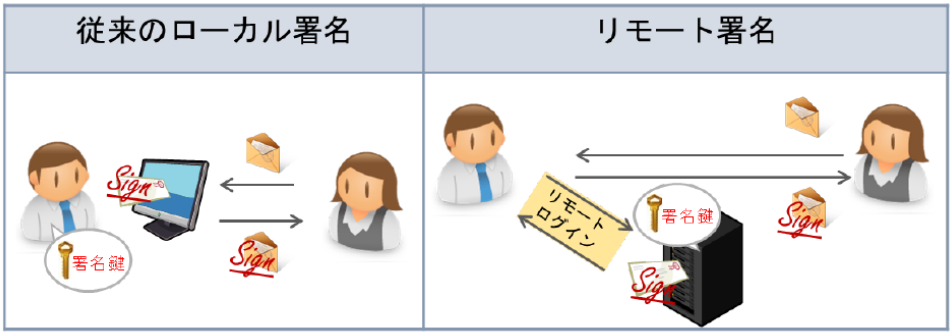

図5　ローカル署名とリモート署名の相違概要

一方，日本における電子署名の法的効力は，ローカル署名のみが想定された時代の『電子署名および認証業務に関する法律（平成12年法律第102号）』（いわゆる電子署名法）に依拠しており，リモート署名との整合性は課題であった．また，リモートで利用する際のセキュリティ要件の整理も必要である．

3.2 法制度とリモート署名の整合性

本節では1つ目の課題である日本の電子署名法とリモート署名との整合性の取り組みについて述べる．

3.2.1 欧州のeIDAS規則

欧州では，ディジタルアイデンティティに関する規則（Regulation）を規定し，技術要件や管理・運用規定およびそれらを監査するフレームワークが構築されている．リモート署名分野においては，Security Requirements for Trustworthy Systems Supporting Server Signing をEN 419 241-1で規定し，Cryptographic Moduleと一部の機能をEN 419 241-2，EN 419 221-5で規定し，これらのセキュリティ要件は，PP 419 241-2，PP 419 221-5で定めている（一部改訂中および作成中も含む）．**図6**にETSIの公開情報[4][5]を基にリモート署名の構成と関連規定の関係を示す．

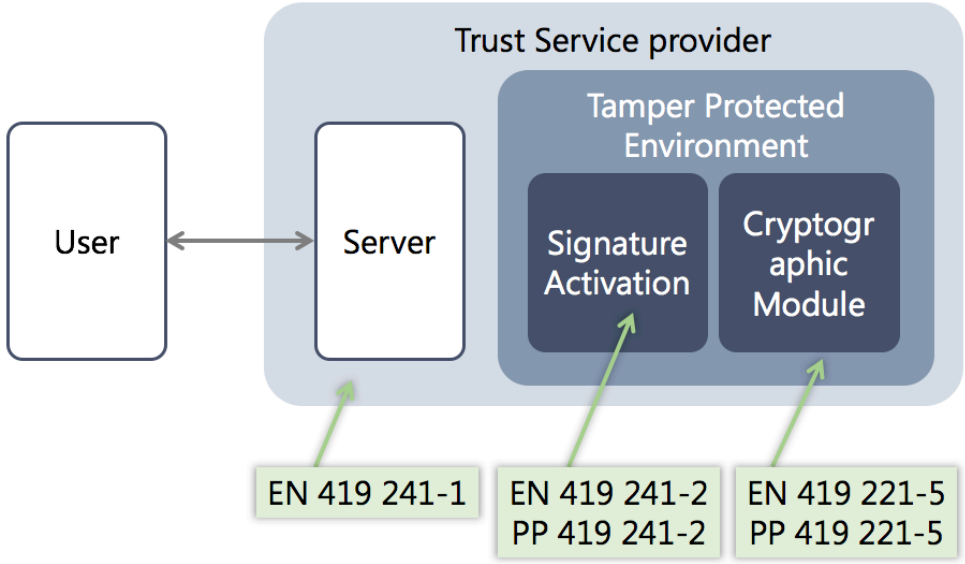

図6　欧州eIDAS検討の構成概要

3.2.2　日本の電子署名法

日本の電子署名法では，第3条で「本人による電子署名」であることを真正な署名と推定する要件とし，施行規則 第6条の三で署名鍵を本人に「安全かつ確実に」渡すことを定めている．つまり利用者（署名者）本人の確認と登録，および署名鍵の発行と配送を規定しているが，署名者の鍵管理状態や，署名鍵の利用時（署名時）の要件について詳細な記載はない．

3.2.3　電子署名法とリモート署名の整合性検討

この状況を受けて，筆者らを含む電子署名法研究会[6] では2015年から，日本の電子署名法とリモート署名との整合性について検討してきた．結論として「本人による電子署名」とは何かを明らかにすることはできないが，同法では，署名者の本人確認と署名者に対して適切に署名鍵を配布することを定めているため，後は署名者本人しか利用できない管理状態と署名者本人が署名する意思によって署名したことを示す必要があると考えられる．これらの事実を示すための技術的要件について整理することとなった．その結果，署名要求のための安全な通信路，署名者本人が安全に保管している署名鍵の活性化情報，署名者本人の署名意思に基づき電子署名が行われたことを担保するための一連のログの記録などが，本人による電子署名であることの重要な要件となると整理した[7]．

本人だけが署名を行うことができるという点について，欧州の規格と日本の事例を整理する必要があった．欧州のCEN/TS 419241:2014では，署名者自らのコントロールのもとで署名鍵を利用していることを保証するレベルとして，Sole Control Levelを定めている．Sole Control Level 1は，リモート署名を利用する署名者の認証をシステム環境（アプリケーション）で行い，Sole Control Level 2は，署名者の認証を署名生成装置（HSM（Hardware Security Module）を想定）で行う必要がある．

一方，日本では，実稼働中の電子契約などで利用しているリモート署名に，さまざまなケースがあり，この2つのレベルや定義に集約できない．実稼働中のものをどのように整理していくかは今後の課題である．たとえばSole Control Level 2を適用する場合には，HSMの処理能力やコストの観点から，サービス提供者が円滑にHSMを導入できるか等の問題があり得る．

3.3　リモート署名のモデルの検討

この節では2つ目の課題であるリモートで安全に利用する際のセキュリティ要件の整理の取り組みについて説明する.

3.3.1 リモート署名のプレイヤとフェーズ

電子署名法研究会では，リモート署名の各フェーズのセキュリティ要件を規定するため，リモート署名のモデルと構成について検討した．プレイヤとフェーズごとに必要な処理を抽出し，リスク分析を行って処理内容を詳細化した[7]（**図7**）.

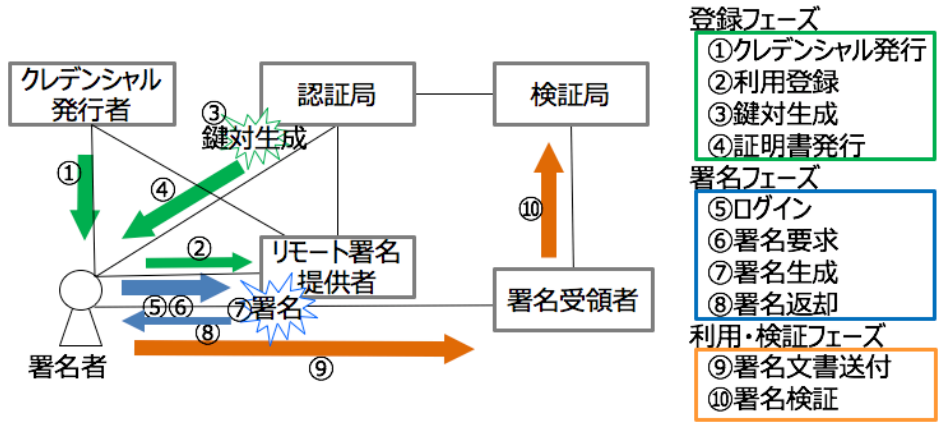

図7　リモート署名のモデルと処理パターン例

3.3.2 ガイドライン化

上記のモデルにおいて，プレイヤの構成や処理のパターンはさまざまなケースが考えられるため，さらに詳細な検討が必要である．また，署名鍵活性化のタイミングや署名結果の確認方法など，さらに検討すべき事項も明らかにした.

これらの検討および諸外国の動向を踏まえ，電子署名法研究会では，より具体的な検討を行いガイドラインを作成すべきであるとしている．そのためには，電子署名および認証業務の有識者だけではなく，リモート署名提供事業者や利用者等を含んだマルチステークホルダで引き続き検討する必要がある.

3.4 リモート署名の検討で得られた知見

この活動で得られた知見としては，電子契約等のように実運用段階に入っているサービスが存在する場合には，3.2.3項で示した通り，リモート署名提供事業者の実稼働中システムが満たしている要件，リモート署名利用者の要求事項等も含めて調査検討する必要があるため，事業者や利用者を含んだマルチステークホルダによる検討が必須ということである．また，国際的な取引を考慮すると，各国の基準（基準には法令に基づく仕様や技術的およびセキュリティ面での要件も含む）を踏まえた検討が必要であり，特に利用者にとっては，特定の国の状況に左右されないよう基準を定め，ガイドラインを整備することが重要である.

基準や標準の作成は海外状況を踏まえながらマルチステークホルダで

4. 電子署名の適用事例

長期署名やリモート署名の標準化と普及の取り組みを受けて，これらを活用して業務に取り入れる動きが進みつつある．本章ではその動向について紹介する．

医療分野では，診療録や紹介状等の電子化にあたり，従来，医師の署名や押印が必要な文書に対してはその医師の電子署名を付与することが要件とされている（医療情報システムの安全管理に関するガイドライン[8]）．また，電子処方せん運用ガイドライン[9] の発行に伴い2016年4月に解禁された電子処方せんでは，医療機関と薬局の間で処方せんASPサーバを介して電子処方せんが交換されるが，その際には医師および薬剤師の電子署名が多重に付与されるような標準的な形式が決められている．いずれの文書も省令等によって定められた期間の保存が必要となる場合があり，タイムスタンプを伴う長期署名形式が求められる．

ほかにも電子署名がさまざまな分野で利用され始めている[10]．たとえば建築分野においては，建築設計図書を電子的に保存する場合や建築確認審査を電子申請により実施する場合，電子署名が求められる．前者では，設計を行った建築士の電子署名が，後者では申請者（建築主または代理者）と建築士の電子署名が必要となる．申請書や設計図書は15年の保存義務があるため，長期署名を利用する必要がある．

また，電子契約[11]と銘打ったサービスが多数出現している．電子契約サービスは，契約成立の事実を事後に証明するために必要な証拠を提供するサービスであるが，電子署名を利用するものとそうでないものが存在する．電子署名を利用しないサービスでは，契約者の認証と操作に関する証跡と対象の契約書をサーバが保持し，それを契約成立の証拠とする必要があるが，電子署名を利用する場合は電子署名法で定められた要件を満たす電子署名を用いることにより契約者の意思が推定可能となるため，電子署名そのものが契約成立の証拠となる．前者は証跡の偽造がないことを証明することが困難であったり，サービスが廃業してしまうとそれ以降証拠の提示が困難となったりする一方，後者は電子署名という証拠情報が契約書自体に含まれるため，サーバに依存することなく正当性を証明しやすくなる．リモート署名の実現により，ますます電子署名の利用の幅は広がることであろう．

5. まとめ

本稿では，CAdES，XAdES，PAdESなどにおける長期署名の標準化の取り組みについて述べた．標準化は各国・地域の状況を踏まえた調整となるため，積極的に取り組むことや相互理解が重要であること，また標準化後のメンテナンスが重要であることの知見について述べた．またリモート署名の活用と普及に向けた取り組みについて述べた．実運用段階に入ったサービスが存在する場合，既存の法制度との関係整理と，事業者や利用者を含んだマルチステークホルダによる検討が必須ということについて述べた．

PKIのようなインフラ技術の仕様策定にあたっては，国際的な相互運用性の考慮，業務利用に即した実用性・互換性の配慮が欠かせない．さらにこれを普及定着させるためには，法令や政省令，施行規則への反映，ガイドラインや業界標準の策定も必要である．また，国際連携のための調整や，各種業界団体との調整のためにも，独立した非営利的な活動が重要である．実際，医療業界での電子署名の適用検討などにおいて，業界標準策定への協力依頼に対応している．

今後，ディジタル社会のトラストを支える新しい技術が次々出てくると想定されるが，その技術の見極め，相互運用のための規定，適用・普及のための活動を，昨年度立ち上げた日本トラストテクノロジー協議会（Japan Trust Technology Association （JT2A））において継続し

ていく．欧州ではEUの下で標準化団体が組織されていたり，アメリカを中心とした巨大グローバル企業なども独自にデファクト標準を推進しているが，日本ではこのような非営利のボランティアに頼らざるを得ないのが現状であり，今後の日本が技術立国としての地位を確立していく上での課題といえよう．

謝辞　本稿の記載内容は，旧ECOMの電子署名関連のWG，JNSAの電子署名WGの主な活動成果をまとめたものであり，各WGに参加し活動された皆様に深く感謝いたします．

参考文献

1）漆嶌賢二：長期署名フォーマットの標準化と日欧相互運用実験，
http://www.jnsa.org/seminar/2007/070625/data/06_urushima.pdf
2）木村道弘：最近の欧州PKI事情，
http://www.jnsa.org/seminar/pki-day/2011/data/05_kimura.pdf
3）電子署名検証ガイドライン，タイムビジネス協議会・調査研究WG（2013年6月5日），
https://www.dekyo.or.jp/tbf/data/seika/densiguideline.pdf
4）Pope，N.：UPDATE ON STANDARDISATION UNDER eIDAS，
https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/Downloads/9-CA-Day-2017/pope-thales.pdf
5）Kjaersgaard，J.：Server Signing QSCD Protection Profile，
https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/Downloads/9-CA-Day-2017/kjaersgaard-cryptomathic.pdf
6）経済産業省：電子署名法研究会（平成27年度第1回），議事要旨，
http://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/h27_01_giji.html
7）経済産業省：電子署名法研究会（平成28年度第4回），配布資料（報告書），
http://www.meti.go.jp/committee/kenkyukai/shoujo/denshishomeihou/h28_04_haifu.html
8）厚生労働省：医療情報システムの安全管理に関するガイドライン第5版（平成29年5月），
http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000166260.pdf
9）厚生労働省：電子処方せんの運用ガイドライン（平成28年3月31日）
http://www.mhlw.go.jp/file/05-Shingikai-12601000-Seisakutoukatsukan-Sanjikanshitsu_Shakaihoshoutantou/0000119545_2.pdf
10）タイムビジネス協議会：電子署名および認証業務等利用促進セミナー ～電子署名・認証，タイムスタンプの国内外の動向および国内先進ユーザ事例紹介～，
https://www.dekyo.or.jp/tbf/contents/seminar/semi14.html
11）宮内宏 編著：電子契約の教科書～基礎から導入事例まで～，日本法令．

脚注

☆1　Electronic Commerce Promotion Council of Japan（2000年4月発足，2005年より次世代電子商取引推進協議会．2010年3月解散）
☆ 2　MS-Word/MS-Excel/MS-PowerPoint/MS-Office は米国Microsoft Corporationの米国およびその他の国における登録商標または商標です．

小川博久（非会員）ogawa@jt2a.org

2008年にみずほ情報総研（株）に入社．情報セキュリティ技術に関する調査および研究開発業務に従事．特定非営利活動法人日本ネットワークセキュリティ協会（JNSA）電子署名WGサブリーダー，日本トラストテクノロジー協議会（JT2A）運営委員長．

宮崎一哉（正会員）Miyazaki.Kazuya@dh.MitsubishiElectric.co.jp
1984年東京工業大学総合理工学研究科修了．同年三菱電機（株）に入社，研究所にて分散システム，情報セキュリティの研究，生産技術本部にて記録管理の普及に従事．JNSA電子署名WGリーダー，JT2A運営委員，タイムビジネス推進協議会副会長，ARMA International東京支部理事．

佐藤雅史（正会員）masas-sato@secom.co.jp
セコム（株） IS研究所 主任研究員．情報セキュリティ分野の調査・研究に従事し，特に電子認証や電子署名の分野を専門とする．JNSA電子署名WGやJAHIS HPKI署名規格作成WG等にて標準化活動に従事．JNSA電子署名WGサブリーダー，JT2A運営委員．

宮地直人（非会員）miyachi@langedge.jp
JNSA電子署名WGサブリーダーとして電子署名関連の標準化活動や普及啓蒙活動に従事．有限会社ラング・エッジのプログラマとしてドキュメントとPKIのソフトウェア開発に従事．1983年大阪電子通信大学工学部応用電子工学科卒業．電子情報通信学会会員．JT2A運営委員．

政本廣志（正会員）hiroshi.masamoto@ntt-at.co.jp
神戸大学大学院電子工学専攻を修了後，NTT研究所にて通信処理，PKI技術の研究開発などに従事．2010年よりNTTアドバンステクノロジにてSI系の事業を担当．JNSA電子署名WG，JT2A運営委員．

投稿受付：2018年2月15日
採録決定：2018年5月31日
編集担当：北村操代（三菱電機（株））