電子署名 WG

WG リーダー　三菱電機株式会社　宮崎　一哉
WG サブリーダー　セコム株式会社　佐藤　雅史
WG サブリーダー　有限会社ラング・エッジ　宮地　直人

■ 電子署名とは

電子署名は電子データの改ざんを検知し、電子データの作成者の身元を証明することで電子データの真正性を担保する仕組みです。電子署名を用いることで、安全に電子データをやりとりすることが可能になります。電子署名フォーマットの標準規格が定められており、これを用いることで異なるシステム間の連携や移行を容易に行えます。この電子署名の標準規格では PKI（公開鍵暗号基盤）の仕組みを用いますが、電子署名付電子データを長期保存する場合には、電子証明書の有効期限切れや暗号アルゴリズムの脆弱化によって有効性が維持できない問題があります。タイムスタンプ技術を用いてこの問題を解決するのが長期署名と呼ばれる仕組みです。現在、標準化されている CAdES（CMS Advanced Electronic Signature）、XAdES（XML Advanced Electronic Signature）、PAdES（PDF Advanced Electronic Signature）といった電子署名規格は長期署名に対応しています。この仕組みによって、電子データの作成者や保管者が第三者に対しても電子データの真正性を証明することができるため、システムの監査や係争時等における証拠提示においても有用です。

■ 電子署名 WG の目的

ここ数年、標的型攻撃や不正なデータ改ざんなどの事件、電子データによる知的財産や営業秘密等の保護への要求など、電子データの真正性に対する社会的なニーズの高まりを感じます。電子データの安全な配布や保管を実現するための社会基盤の整備が求められますが、この中核となるのが電子署名技術といえます。電子署名は電子署名フォーマットや、電子証明書と認証局、タイムスタンプ技術とタイムスタンプ局、電子署名を生成するデバイスなど様々な要素が一体となって実現できるものですので、全体像を俯瞰し整合性の取れた取り組みが必要です。欧州では既にそのような基盤整備を進めていますが、これまで日本では全体像を把握し検討を行う場もない状況にありました。このような状況を打開するため、電子署名に関連するあらゆる情報の収集、電子署名の相互運用のための基盤整備（調査、検討、仕様提案など）、普及促進のための啓発活動などを行う場として電子署名 WG を発足しました。

■ 電子署名 WG の体制と活動内容

電子署名 WG には現在以下の 3 つのタスクフォースを立ち上げています。

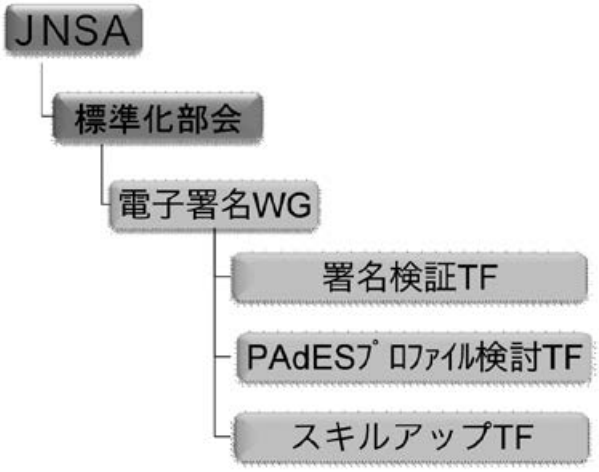

図 1 ：電子署名 WG 体制図

・署名検証タスクフォース

電子署名フォーマットの規格には構文の定義と各フィールドの使用方法などが記述されていますが、その電子署名フォーマットをどのように検証して正しい電子署名であると判定するかという明確な要件は示されていません。そのため、同じ電子署名のデータであっても、検証を行うアプリケーションが異なると、異なる結果が表示されうるという相

JNSA ワーキンググループ紹介

互運用上の問題がありました。この問題を解決するために、検証項目の洗い出しと検証方法、判定条件などを明確にした検証要件規格の定義を行っています。

・PAdES プロファイル検討タスクフォース

PDF に長期署名対応の電子署名データを格納する仕組みとして PAdES が欧州の標準化団体 ETSI（欧州電気通信標準化機構）にて規格化されており、この規格を取り込んだ PDF の ISO 規格（ISO 32000-2）の策定が現在進められています。この PAdES 規格は電子署名やタイムスタンプ、それらを検証するための証明書などを格納するフィールドが定義されているのみで、それらの要素をどのように組み合わせて使用すればよいかというルールは示されていません。そのため、PAdES 対応アプリケーションと言っても、例えば、長期署名（電子署名およびタイムスタンプ）に対応したもの、電子署名のみでタイムスタンプには対応していないもの、タイムスタンプのみに対応したものなど、様々な方式に分かれ相互運用に問題が生じます。本タスクフォースでは相互運用性を確保し長期署名を実現するための要件定義を行うプロファイル規格を作成し、国際標準化を目指しています。

・スキルアップタスクフォース

電子署名の技術者の育成やスキルアップ、電子署名に関連する様々な情報収集と共有などを行っています。また新しい電子署名の技術や利用について先行して調査研究を行い、次の標準化項目を検討します。WG や JNSA メンバー外からも講師を招いた勉強会も実施しており、今年度は、電子署名入門、クラウド環境下における HSM（Hardware Security Module）、PKI を使用しない電子署名サービスなどのテーマで勉強会を行いました。次年度は公開可能なサーバを利用した実証実験や試験環境の構築を目指し、JNSA メンバー外の一般技術者を対象とした勉強会やハンズオンも実施したいと考えています。

■ ETSI 会議への参加

電子署名 WG 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）と連携して標準化活動を行っています。2013 年 9 月に ESI 第 40 回会議（スペイン）、2014 年 2 月に ESI 第 42 回会議（オーストリア）に参加し、署名検証タスクフォースと PAdES プロファイル検討タスクフォースの活動成果の紹介と議論を行うと共に欧州の最新動向

ETSI/TC ESI 第 42 回会議

の情報を収集しました。欧州でも電子署名検証に関する規格の策定を進めておりますが、署名検証タスクフォースが作成した規格案とはコンセプトが異なるため、両者の整合性が議論の争点となっています。PAdES プロファイル検討タスクフォースが作成したプロファイル原案については、国際標準化に向けて ETSI/TC ESI と調整していくことになりました。また、PAdES プロファイル原案作過程において判明した PAdES のベース規格自体の問題点を指摘しましたが、現在もベース規格の修正の必要性について議論が続いています。

現在、欧州では 1999 年に発足した電子署名指令（各国電子署名法の指針）を改訂し、強制力を持った電子署名規則を発行するための準備に注力しています。その一環として ETSI/TC ESI では電子署名規則に基づいて電子署名の技術標準フレームワークの見直しを行っています。技術標準フレームワークには、従来の電子署名規格、署名生成デバイスの要件定義、認証局やタイムスタンプ局に関する要件定義に加え、電子署名に用いる推奨暗号リストの作成、信頼できるサービス（Trusted Service Provider）に関する要件定義、信頼できるサービスのリスト作成なども含まれています。信頼できるサービスには従来の認証局やタイムスタンプ局だけでなく、電子署名を用いた安全な電子データ配信サービスや保管サービスなども含まれており、幅広い視点で基盤構築を行おうとしていることがわかります。

■ 電子署名 WG の Facebook ページ

電子署名 WG の活動予定やイベント告知等を行う Facebook ページを公開しています。

https://www.facebook.com/eswg.jnsa.org

電子署名 WG