

ライトニングトーク:

標準化どうでしょう

JNSA 電子署名WG秋祭り
オクトーバーフェスト

宮地(miyachi@langedge.jp)

2016年10月26日

どんな標準規格団体知っていますか？

International Organization for Standardization

Internet Engineering Task Force

M2M/IoT
one M2M

世界

オンライン認証
fido alliance

W3C
WORLD WIDE WEB
consortium

ETSI

World Class Standards
ローカル

デファクト標準
RSA
PKCS
Public-Key Cryptography Standards

日本
JIS規格

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

ISO/IETF/W3Cを比較してみる

組織	メンバー	規格例	個人的感想
ISO	加盟国 (162) 各国 1 組織 が参加可能 [TC毎に活動]	ISO 32000 - PDF ISO 14533 - AdESプロファイル	各段階で決められた賛成票が必要であり、標準化までに比較的時間がかかる。各国の専門家が国を代表して参加するので政治的な面もある。日本語化されてJISになるケースも多い。
IETF	MLに参加 誰(個人)でも 参加可能 [年3回会議]	RFC 3161 - TimeStamp RFC 5280 - X.509/PKI	誰でもプロポーザルが出せるがMLで多くの賛同を得る必要がある。成立までの時間が比較的短い。日本からも多くの人に参加している。PKCS等のRFCとして再定義も多い。
W3C	企業会員 (400弱) 個人参加は 認められない	W3C XML-DSig 勧告	XML/HTML系がメイン。参加が企業会員のための為に各企業の要望が色濃く反映される傾向がある。署名系ではXML署名のオリジナル規格が議論されている。

例えばXAdES標準ってどうなっている？

仕様	名前空間	最新版	状況
ETSI EN 319 132-1&2 [ETSI TS 101 903] (元仕様 + 欧州プロファイル)	v1.4.1	2016	オリジナル (最新版)
ISO 14533-2:2012 (国際プロファイル)	v1.4.1	2012	EN未対応
JIS X5093:2008 (日本プロファイル)	v1.3.2	2008	更新検討中
W3C XAdES Note (参照では無く仕様そのもの)	v1.1.1	2003	放置プレイ？

参照先のオリジナルが更新された場合の対応には問題がありそう。特に危険なのが「**放置プレイ**」！

標準化に参加するとどんな**メリット**があるの？

日本の為だよね！

☞ なんだけど、会社のOK貰えないw

やっても儲からないからやらない…

☞ これはこれまでの戦略的なミス…

作業時間や拘束時間が多…

☞ それはそーなんですが(^^;

;) ㍻) あれ？ デメリットばかり？ ？

標準化活動のあるべき姿

正しく標準化活動
すればメリットはある!

会社・組織として

A1. 国際的な競争力の強化！

A2. 戦略的に新たなマーケットの創出！

A3. 先駆けた商品化で先行者利益！

個人・技術者として

B1. 新しい技術を学んで専門家に！

B2. 業界内の人脈とパイプができる！

B3. パブリックな貢献活動ができる！

標準化活動のすゝめ

JNSA電子署名WGは「**標準化部会**」！

ISOや**JIS**を中心に活動していますが、**IETF**等の活動もやらない訳ではない！

電子文書のセキュリティの**新たなマーケット**
(市場) を一緒に作りませんか？

電子署名分野以外にも**興味がある分野**
があれば是非**標準化活動に参加しよう**！