NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

# JNSA電子署名WGの活動報告

## - Activity report of JNSA ESWG -

## 【 欧州と日本のトラストサービスの動向 】

### ～ eIDAS規則とEUDIW(欧州IDウォレット)の現状 ～

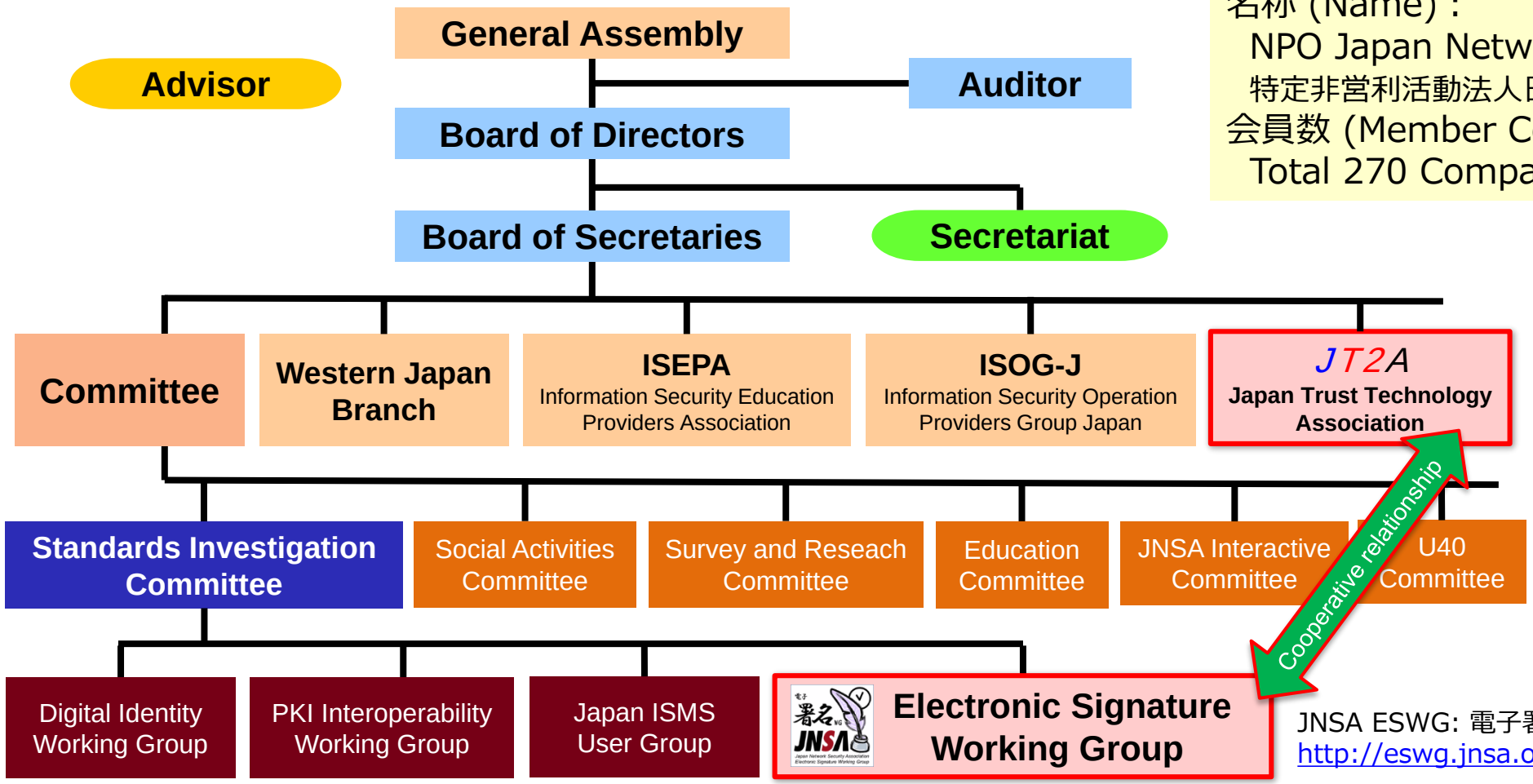
## *JNSA* 標準化部会 電子署名WG

2023/11/15

電子署名WGサブリーダー（有限会社ラング・エッジ） 宮地
ESWG Sub-Leader (LangEdge,Inc.) miyachi@langedge.jp

# NPO Japan Network Security Association






名称 (Name)：
NPO Japan Network Security Association
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
会員数 (Member Comapnies)：
Total 270 Companies (2023-10-19)

JT2A: 日本トラストテクノロジー協議会
http://www.jt2a.org/

JNSA ESWG: 電子署名WG
http://eswg.jnsa.org/

# JNSA: Electronic Signature WG



## JNSA 電子署名WG
JNSA: Electronic Signature Working Group

Leader:
Miyazaki (Mitsubishi Electric)

月１回会合 (Monthly meeting)
情報交換と各種検討
(Information exchange and various considerations)

TC 154: ISO 14533-1/2/3
SC34: ISO/IEC 29500-2, ISO/IEC 26300
JIS (Japanese Industrial Standards), ETSI, ...

### 標準化TF
Standardization Task Force

Leader:
Sato (SECOM)

デジタル署名検証ガイドライン
Digital Signature Verification Guidelines

### 署名検証TF
Signatures Verification Task Force

Leader:
Masamoto (JNSA)

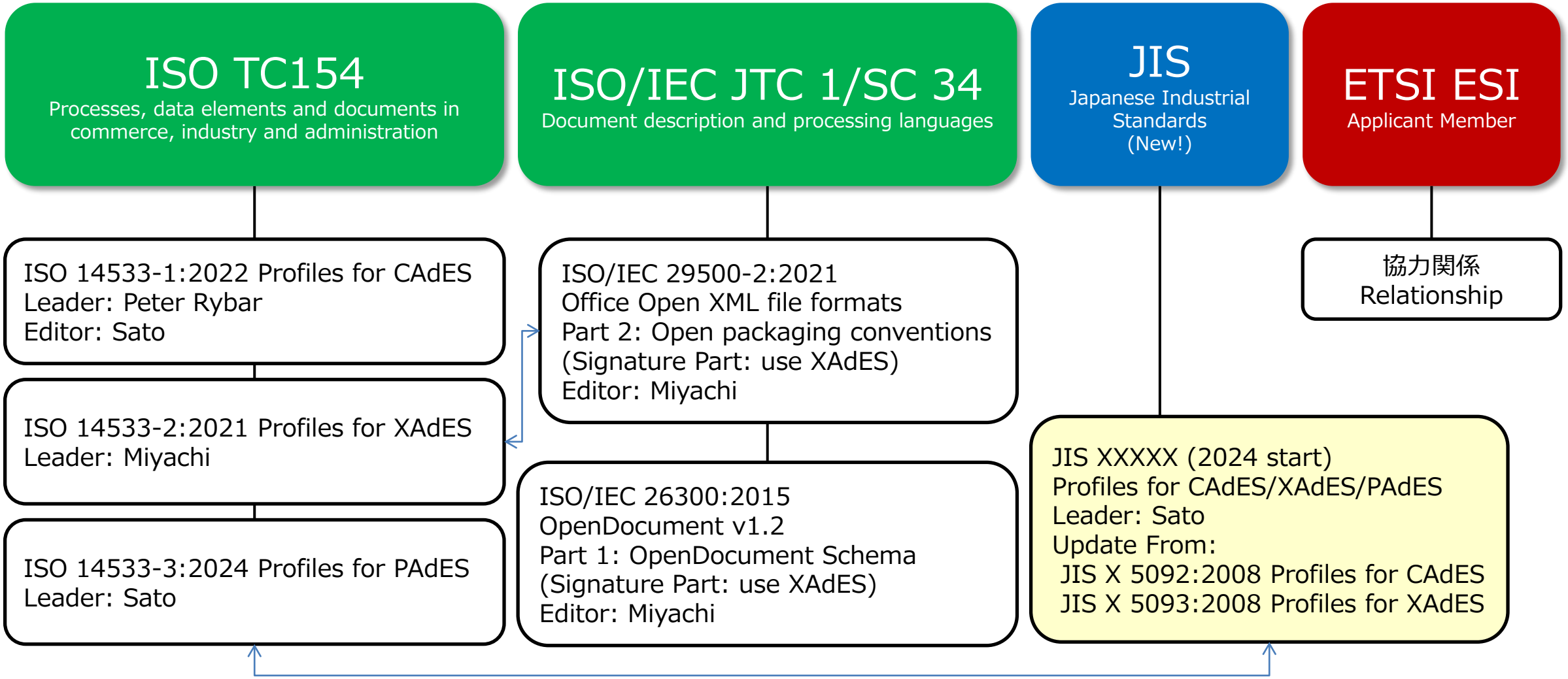
署名保証ガイドライン
Signature Assurance Guidelines

### 保証レベルTF
Assurance Level Task Force

Leader:
Miyachi (LangEdge)

# JNSA ESWG: Standardization TF





# JNSA ESWG: Signatures Verification TF



1. 「デジタル署名検証ガイドライン」を作成し2021年に公開。
   - Created “Digital Signature Verification Guidelines” and released at 2021.
   - https://www.jnsa.org/result/e-signature/2021/
2. 長期署名フォーマットCAdES/XAdES/PAdESに対応。
   - Supports long-term signature formats CAdES/XAdES/PAdES.
3. 検証項目を整理したチェックリスト方式になっている。
   - Explains the verification items by checklist.
4. 現在「トラストのためのデジタル署名検証 解説書」を作成中。
   - Currently writing “Guide to digital signature verification for trust.".

- ETSI TS 119 102-1 Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation -> 「Corresponds to Validation section」
- ETSI TS 119 102-1 is explanation of the verification process, not a checklist.
- Interested in the consistency with Part 2: Signature Validation Report.

# SVTF: Digital Signature Verification Guidelines



目次：



Index:

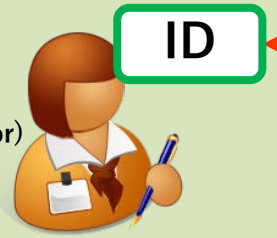
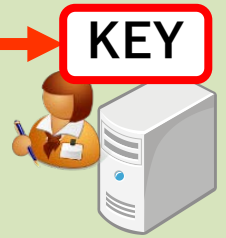
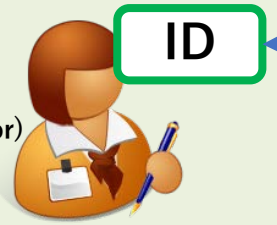
# JNSA ESWG: Assurance Level TF



1. 日本にはeIDASのようなトラストのレギュレーションは無い。
   - No regulations regarding Trusts in Japan like eIDAS.
2. 日本では様々なタイプの電子署名が使われている。
   - Various Types of Electronic Signatures are used in Japan.
3. 保証レベルにより各種タイプの電子署名を比較する。
   - Compare various types of Electronic Signatures based by Assurance Level.
4. デジタルIDの世界には NIST SP 800-63 と言う保証レベルがある。
   - Digital Identity has an Assurance Level of NIST SP 800-63.
5. 本TFでは電子署名の保証レベルを整理してまとめる予定である。
   - This TF summarize the Assurance Levels of Electronic Signatures with reference to NIST SP 800-63.
6. 「署名保証ガイドライン（JNSA SAG:2024）」を2024年にリリースする予定である。
   - "Signature Assurance Guidelines" are scheduled to be released in 2024.

# ALTF: Type of Electronic Signatures



| | ID: Digital Identy | KEY: Digital Signature | Proof of Signature Evidence |
|---|---|---|---|
| (EU) (JP) (US) Type1: Local Sign | (not used) | Signer (IC card etc)   | Digital Signature Data by Signer (AdES formats, JWS, etc) |
| (US) (JP) Type2: Auth Record Sign | Signer (Authenticator)   | (not used) | Digital Identity Record Data by Auth (Access logs, Assertion, id_token, etc) |
| (EU) (JP) Type3: Remote Sign | Signer (Authenticator)   | binding   Server (HSM) | Digital Signature Data by Signer (AdES formats, JWS, etc) + Digital Identity Record Data by Auth (Access logs, Assertion, id_token, etc) |
| (JP) (US) Type4: Provider Sign | Signer (Authenticator)   | approve   Provider (HSM) | Digital Signature Data by Provider (AdES formats, JWS, etc) + Digital Identity Record Data by Auth (Access logs, Assertion, id_token, etc) |

# ALTF: Signature Assurance Guidelines (draft)



| レイヤー | 署名（JNSA SAG） | 認証（NIST SP 800-63） |
|---|---|---|
| **ABOUT（概要）** | **Signature Assurance Guidelines**<br>**署名保証ガイドライン**<br>**JNSA SAG:2024** | **Digital Identity Guidelines**<br>**デジタルIDガイドライン**<br>**NIST SP 800-63** |
| **IDENTITY（身元）** | **Enrollment and Identity Proofing**<br>**本人確認保証レベル - JNSA SAG-A**<br>IAL: Identity Assurance Level<br>（Refere to NIST SP 800-63A IAL） | **Enrollment and Identity Proofing**<br>**本人確認保証レベル - SP 800-63A**<br>IAL: Identity Assurance Level<br>登録時の本人の身元確認の保証レベル |
| **PROCESS（プロセス）** | **Signing Process and Authorization**<br>**署名プロセス保証レベル - JNSA SAG-B**<br>SPAL: Signing Process Assurance Level<br>署名時のプロセス保証レベル (use AAL) | **Authentication and Lifecycle Management**<br>**当人認証保証レベル - SP 800-63B**<br>AAL: Authenticator Assurance Level<br>認証時のプロセス保証レベル |
| **DATA（データ）** | **Signed Data Verification**<br>**署名データ保証レベル - JNSA SAG-C**<br>SDAL: Signed Data Assurance Level<br>署名対象データの保証レベル | **Federation and Assertions**<br>**携情報保証レベル - SP 800-63C**<br>FAL: Federation Assurance Level<br>連携時のデータ保証レベル |
| **POLICY（ポリシー）** | **Service Operation and Policy**<br>**サービス運用保証レベル - JNSA SAG-D**<br>SOAL: Service Operational Assurance Level<br>運用や認定・監査のポリシー保証レベル | |