JNSA

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

電子署名WGの設立について

宮崎　一哉

三菱電機株式会社

2013 年6月7日

発表内容

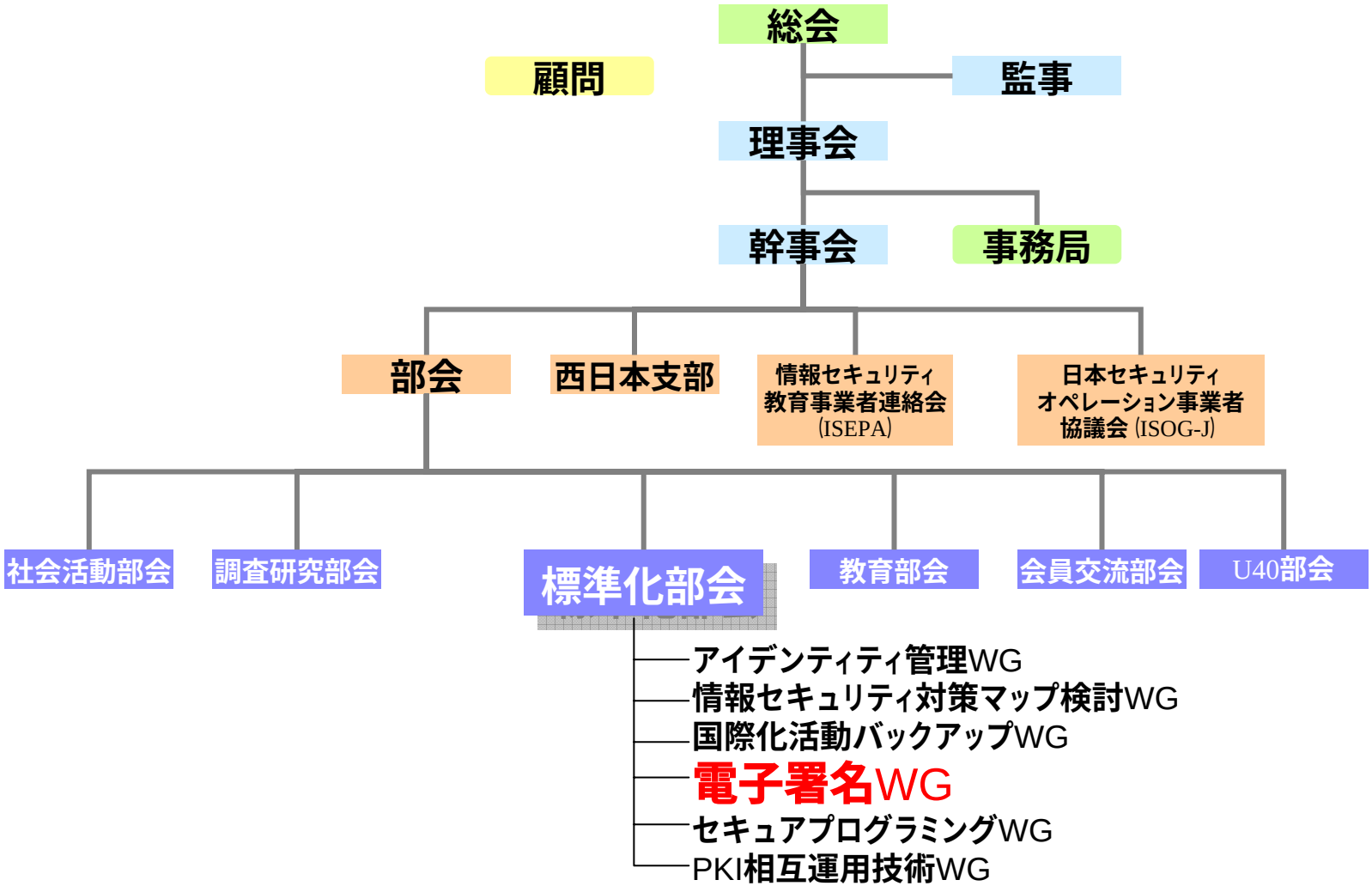
- 電子署名WGの目標
- 電子署名WGの位置付け
- 2013年度活動内容
- 2013年度成果予定
- スケジュール
- メンバ募集の案内

目標

- 電子署名（含タイムスタンプ）の相互運用性確保のための調査、検討、仕様提案、相互運用性テスト、及び電子署名普及啓発を行う。

⇒ **電子署名に関する拠点**

電子署名WGの位置付け



2013年度活動内容

- テーマ
  - ① 署名検証要件に関する標準作成
  - ② PAdESプロファイルに関する標準作成
  - ③ 署名関連の勉強会
- 活動方法
  - テーマ毎にTFを設置し、個別に会合を実施。
  - 欧州電気通信標準化機構/電子署名基盤技術委員会（ETSI/TC ESI）†、TBF等と連携しつつ、国内で年間10回程度の会合を実施。
  - 合宿1回、懇親会2回を予定。

†JNSAをETSI会員として登録済み

2013年度成果予定（1/2）

① 署名検証要件に関する標準案

- 2012年度作成の初版をベースにETSIに提案し、ETSI標準として成立させる。
- ETSI/TC ESI#38会議（3月12-13日）にて初版をインプット済み。

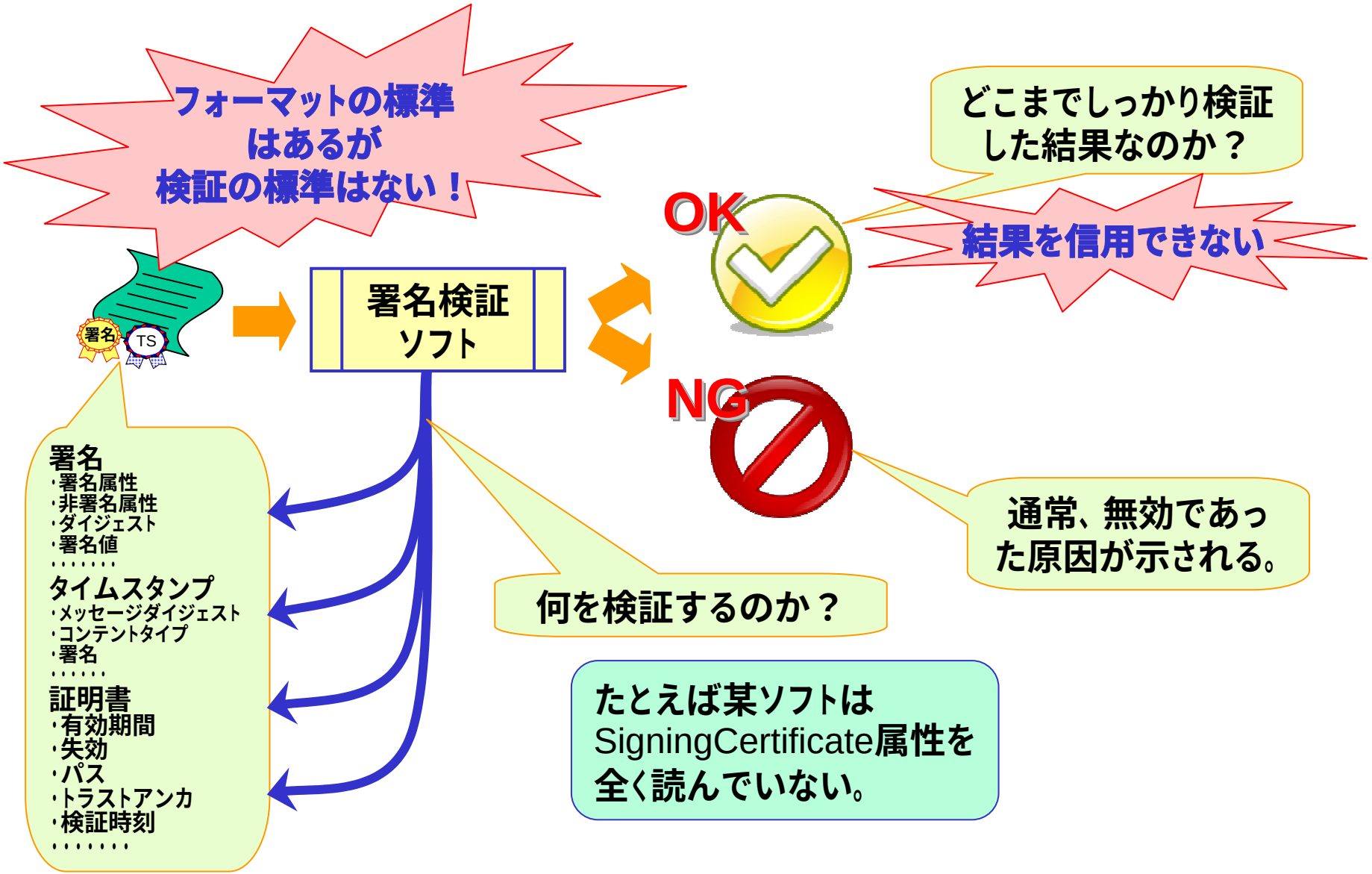
② PAdESプロファイルに関する標準案

- CAdES/XAdESプロファイルに倣い、ETSIと情報交換を行いつつ、まずJIS化に向けたドラフトを作成する。
- JSAの「JIS原案作成公募制度」に応募し、JIS原案作成に着手できるようにする。

JSA：一般財団法人日本規格協会

①署名検証要件に関するETSI標準

署名検証の問題点



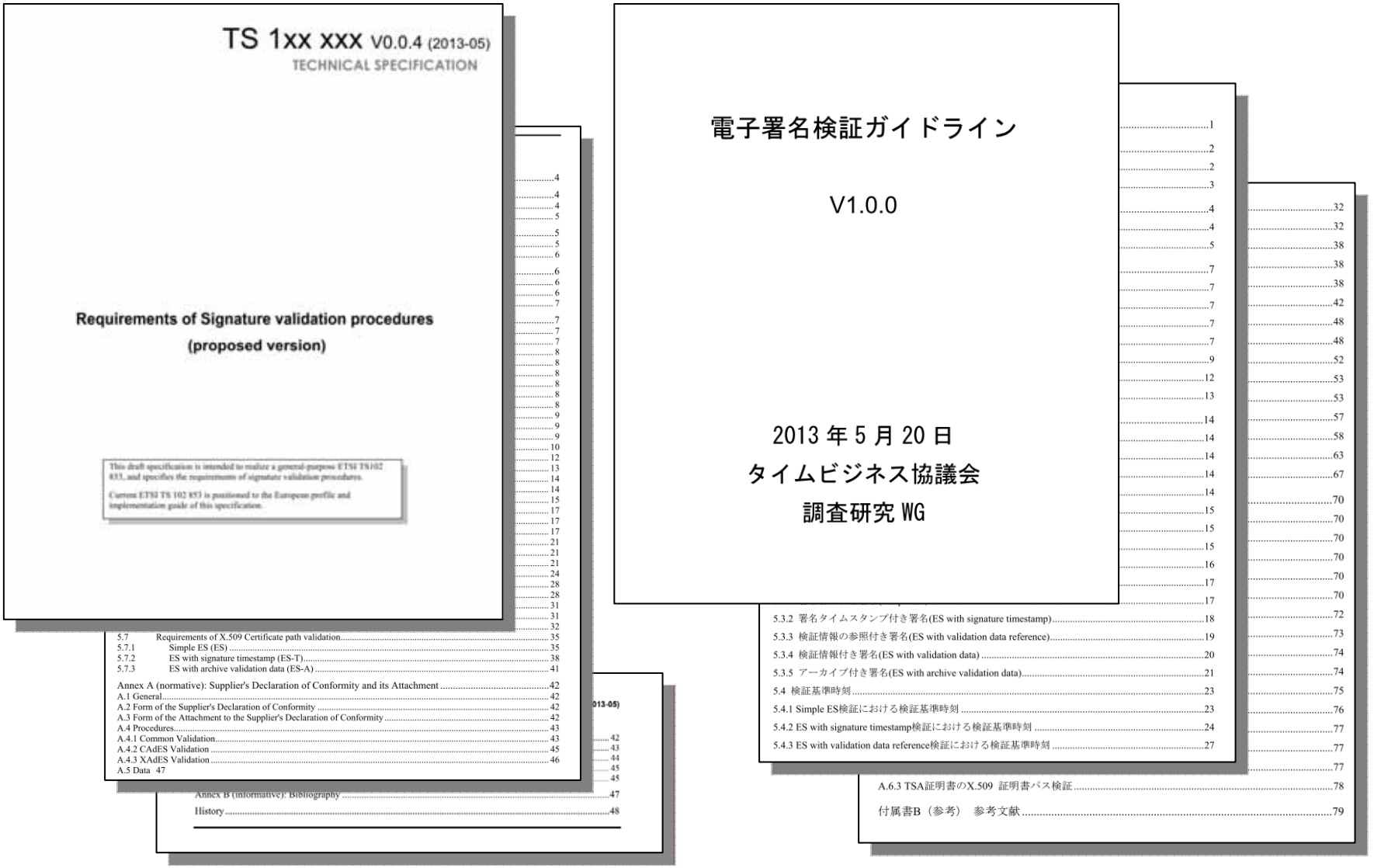
署名検証標準規格の意義

- 署名検証における検証項目や要件を定義
- 検証結果の出力内容を定義
- 検証ソフトウェアの検証範囲を明示できる枠組み（適合宣言書）を提供

⇒実装者にとって、実装方法がわかる。
⇒調達者・利用者にとって、検証範囲がわかる。

⇒安全・安心な署名検証ソフト

署名検証標準規格の作成状況



2013年度成果予定 (1/2)

① 署名検証要件に関する標準案

- 2012年度作成の初版をベースにETSIに提案し、ETSI標準として成立させる。
- ETSI/TC ESI#38会議（3月12-13日）にて初版をインプット済み。

② PAdESプロファイルに関する標準案

- CAdES/XAdESプロファイルに倣い、ETSIと情報交換を行いつつ、まずJIS化に向けたドラフトを作成する。
- JSAの「JIS原案作成公募制度」に応募し、JIS原案作成に着手できるようにする。

JSA：一般財団法人日本規格協会

②PAdESプロファイルに関するJISドラフト

PAdESプロファイルの位置付け

JNSA

CAdES
(CMS Advanced Electronic Signature)

バイナリデータ形式 (ASN.1) **のフォーマット**

関連する代表的な規格

- ETSI TS 101 733
- RFC 5126 (IETF)

ECOM/eRAP**が原案作成**

- JIS X 5092:2008
- ISO 14533-1

XAdES
(XML Advanced Electronic Signature)

XML**形式のフォーマット**

関連する代表的な規格

- ETSI TS 101 903

ECOM/eRAP**が原案作成**

- JIS X 5093:2008
- ISO 14533-2

相互運用性を確保した
長期保存のためのプロファイル

PAdES
(PDF Advanced Electronic Signature)

PDF**形式のフォーマット**

関連する代表的な規格

- ETSI TS 102 778
- ISO 32000-2(draft)

同じ位置付けのものがない！

②PAdESプロファイルに関するJISドラフト

PAdESプロファイルの考え方

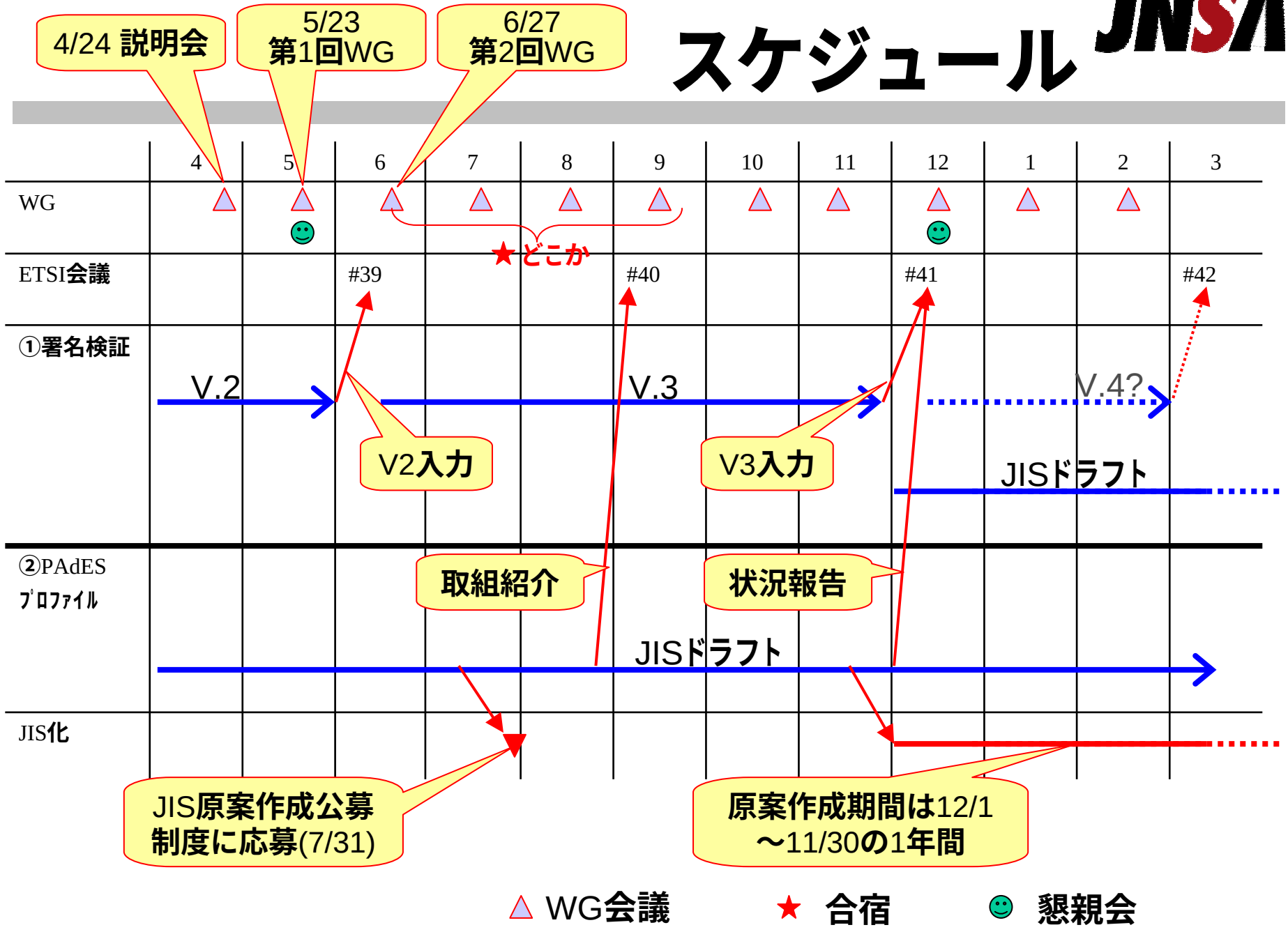
- PAdES(PDF Advanced Electronic Signature)
  - ベース規格 ETSI TS 102 778 Part1～Part6
  - 現在策定作業中のPDF規格(ISO 32000-2)に取り入れられる予定。
- PAdESの主な特徴と問題点
  - 従来のPKCS#7ベースのPDF署名(PAdES Basic)に加え、CAdESを用いたPAdES Enhancedを定義している。
  - 検証に必要な証明書や失効情報を格納するためにDSSというPDFの要素を定義している。
  - PDFに適用するタイムスタンプ（ドキュメントタイムスタンプ）を定義している。
  - 問題点：DSSや署名、ドキュメントタイムスタンプ等の様々な要素の組み合わせの自由度が高い一方で、様々なパターンに応じた利用方法（生成・検証）が示されておらず、相互運用性の問題が生じる。
- PAdESプロファイルの考え方
  - 長期保存可能なPAdESを実現するうえで必要な各要素の利用方法（生成・検証）を定める。
  - ベース規格へ反映すべき事項はETSIやISOに提言する。

2013年度成果予定 (2/2)

③ 署名関連の勉強会

- オープンソースプロジェクト FreeXAdES
- Java6以降標準提供された XMLSignature クラスを拡張して実装
- 成果物はMITやGPLのライセンスで公開
- 2ヶ月に1回程度の勉強会を開催し少しずつ実装を進める

スケジュール


4/24 説明会
5/23
第1回WG
6/27
第2回WG
4
5
6
7
8
9
10
11
12
1
2
3
WG
ETSI会議
#39
#40
#41
#42
★どこか
①署名検証
V.2
V.3
V.4?
V2入力
V3入力
JISドラフト
②PAdES
ﾌﾟﾛﾌｧｲﾙ
取組紹介
状況報告
JISドラフト
JIS化
JIS原案作成公募
制度に応募(7/31)
原案作成期間は12/1
～11/30の1年間
WG会議
合宿
懇親会

電子署名WGメンバ募集

電子署名WGに登録を希望する方は下記にご連絡ください。（現在の登録者数：約30名）

NPO **日本ネットワークセキュリティ協会**

事務局宛

<E-Mail>office@jnsa.org

※件名を「電子署名WG登録希望」としてください。

※MLに登録するメールアドレスをお知らせください。