

PKI Day 2015

トラストリストと信頼のグローバル化 － 日本版トラストリストの実現に向けて －

2015. 4. 10

セイコーソリューションズ株式会社

村尾 進一

1. はじめに

1-1. EUの取り組み

2. トラストリストの解説

2-1. トラストリストとは

2-2. トラストリストの活用事例

3. 日本における信頼基盤としてのトラストリストの可能性

3-1. 証明書検証の現状

3-2. トラストリスト導入によるBefore/After

3-3. トラストリストのもたらす効果

4. まとめ

4-1. トラストリスト導入に向けた課題

4-2. 最後に

- ① eIDAS規則について
- ② eIDAS規則でのTL設置規定
- ③ 新フレームワーク
- ④ トラストサービス(一覧)

・eIDAS(Electronic identification and trust services)規則

REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014
on **electronic identification and trust services** for electronic transactions
in the internal market and repealing Directive 1999/93/EC

- ・EU電子署名指令(Directive 1999/93/EC)に替わる、EUで定めた電子認証や電子署名を含めたトラストサービスに関する規則(Regulation (EU) N° 910/2014)。

- ・電子認証やトラストサービスを普及させることで、国境を越えた電子取引を安全かつシームレスに実現させることが目的。

- ・トラストサービスとは、「(通常、必ずしもそうとは限らないが、暗号技術を利用し、または機密情報を扱う、)電子取引の安心と信頼を強化する電子サービスの総称」。

ETSI TS 119 612 V1.2.1(2014-04)の用語定義より

②eIDAS規則でのTL設置規定(Article22)

Article 22

Official Journal of the European Union 28.8.2014 から抜粋

Trusted lists

1. Each Member State shall establish, maintain and publish trusted lists, including information related to the qualified trust service providers for which it is responsible, together with information related to the qualified trust services provided by them.

①EU加盟各国に対して、トラストリストの制定を義務付け

2. Member States shall establish, maintain and publish, in a secured manner, the electronically signed or sealed trusted lists referred to in paragraph 1 in a form suitable for automated processing.

②リストの非改ざん性保証対策を義務付け

3. Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificates used to sign or seal the trusted lists and any changes thereto.

③内容変更の、遅滞のないEU委員会への通知を義務付け

4. The Commission shall make available to the public, through a secure channel, the information referred to in paragraph 3 in electronically signed or sealed form suitable for automated processing.

④更新情報の公開(LOTL)を、EU委員会に対して義務付け

5. By 18 September 2015 the Commission shall, by means of implementing acts, specify the information referred to in paragraph 1 and define the technical specifications and formats for trusted lists applicable for the purposes of paragraphs 1 to 4. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 48(2).

⑤技術規格とリストのフォーマットの制定をEU委員会に義務付け(済)

③新フレームワーク

ETSI , CEN, ETSI SR 001 604 「Rationalised Framework for Electronic Signature Standardisation」より

Trust Service Status List Providers

【信頼サービスリストプロバイダ】

TSP supporting eSignature

【認証局、タイムスタンプ局など】

TSP Certs

TSSP

SGSP

SVSP

TSP Application Service Providers

Registered eMail

Data Preservation

Signature Creation & Validation

【高度署名(長期署名)】

CAdES

XAdES

PADES

...

標準化部会
> 電子署名WG

Signature Creation & other related
Devices

【署名デバイス】

SSCD

Other SCDs

Cryptographic Suites

【暗号アルゴリズム】

④トラストサービス(一覧)

No.	トラストサービス
1	適格証明書生成サービス
2	非適格証明書生成サービス
3	タイムスタンプ生成サービス
4	適格タイムスタンプ生成サービス
5	適格署名に対するタイムスタンプ生成サービス (適格証明書生成の一部)
6	適格署名に対するタイムスタンプ生成サービス
7	CRL発行サービス
8	適格証明書のCRL発行サービス
9	OCSP発行サービス
10	適格証明書のOCSP発行サービス
11	RAサービス
12	非PKIベースのRAサービス
13	属性証明書生成サービス

No.	トラストサービス
14	署名ポリシー発行運用サービス
15	国家ルート認証局サービス
16	記録保管サービス
17	書留電子メールサービス
18	電子配送サービス
19	適格電子配送サービス
20	電子署名保管サービス
21	適格電子署名保管サービス
22	アイデンティティ検証サービス
23	鍵預託サービス
24	PIN/パスワードベース身分証明発行サービス
25	トラストリスト発行サービス
26	未定義のトラストサービス

ETSI TS 119 612 V1.2.1(2014-04) 5.1.1 サービスタイプより抜粋

2. トラストリストの解説

2-1. トラストリストとは

2-2. トラストリストの活用事例

- ① EUトラストリストの概要
- ② EUトラストリスト(PDF/XML)
- ③ EUトラストリストの構成
- ④ EUトラストリストにおけるスキーム
- ⑤ EUトラストリストの特徴

① EUトラストリストの概要

1. トラストリストは、以下について記したもの

- ・トラストサービスのための**ルール**
- ・ルールに基づいてサービスを提供する**プロバイダ**
- ・そのプロバイダの**提供サービスとステータス**



まとめて
「スキーム」
と呼びます

2. トラストリストは、**国単位**で設けられている。(各国で制定)

欧州経済地域 (EEA) : EU 28ヶ国 + EFTA加盟国 3ヶ国

3. 規格

- ・ETSI TS 119 612 (V1.2.1)
トラストリスト規格(フォーマットを定義)
- ・ETSI TS 119 403 (V2.1.1)
TSP適合評価 一般要求事項およびガイダンス
(TSPを監査する側に対する要求・監査者の心得・力量等)
- ・etc.

順次 **EN** 規格に移行中

ETSI TS 119 403 V1.1.1 (2012-03) から抜粋

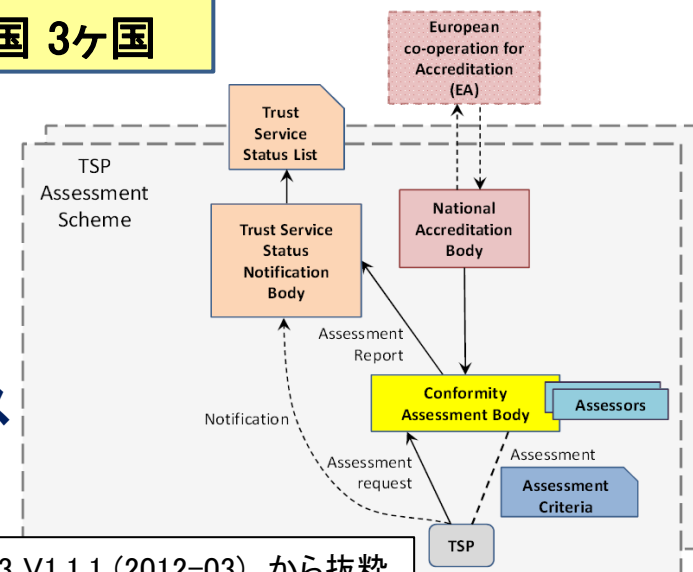


Figure 1: Model for Trust Service provider Conformity Assessment
トラストサービスプロバイダに対する評価モデル

②EUトラストリスト(PDF)

Member State	download links	Next Update
 Austria Österreich	  	22/06/2015
 Belgium Belgique/België	  	03/07/2015
 Bulgaria България	  	30/07/2015
 Cyprus Κύπρος/Cıbrıs	  	02/04/2015
 Czech Republic Česká republika	  	10/07/2015
 Germany Deutschland	 	05/08/2015
 Denmark Danmark	  	15/03/2015
 Estonia Eesti	  	11/09/2015
 Greece Ελλάδα	 	19/08/2015
 Spain España	  	31/08/2015

<http://www.polysys.eu/tledit/Download/>より抜粋

BG:ブルガリアのトラストリスト(PDF)



Веселин
Божков
Божков

Digitally signed by Веселин
Божков Божков
DN: c=BG, postalCode=1000,
l=Sofia, ou=Chairman, street=6
Gurko str, email=vbozhkov@crc.
bg, dc=crc-members-ca,
o=Communications Regulation
Commission, cn=Веселин
Божков Божков
Date: 2015.01.30 13:44:52
+02'00'

БЪЛГАРИЯ (BULGARIA) : Trusted List

Tsl Id: TSL-BG

Valid until nextUpdate value: 2015-07-29T22:00:00Z

TSL signed on: 2015-01-30T11:41:50Z

PDF generated on: Fri Jan 30 12:49:16 CET 2015

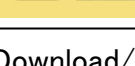
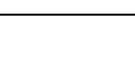
БЪЛГАРИЯ (BULGARIA) - Trusted List ID: TSL-BG

Page 1

②EUトラストリスト(XML)

BG: ブルガリアのトラストリスト(XML)

```
<?xml version="1.0" encoding="UTF-8"?>
- <TrustServiceStatusList TSLTag="http://uri.etsi.org/19612/TSLTag" Id="TSL-BG" xmlns:ns5="http://uri.etsi.org/TrstSvc/SvcInfoExt/eSigDir-1999-93-EC-
TrustedList/#" xmlns:ns4="http://uri.etsi.org/01903/v1.3.2#" xmlns:ns3="http://uri.etsi.org/02231/v2/additionaltypes#"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#" xmlns="http://uri.etsi.org/02231/v2#">
- <SchemeInformation>
  <TSLVersionIdentifier>4</TSLVersionIdentifier>
  <TSLSequenceNumber>7</TSLSequenceNumber>
  <TSLType>http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUGeneric</TSLType>
- <SchemeOperatorName>
  <Name xml:lang="en">Communications Regulation Commission</Name>
  <Name xml:lang="bg">Комисия за регулиране на съобщенията</Name>
</SchemeOperatorName>
- <SchemeOperatorAddress>
  <PostalAddresses>
    <PostalAddress xml:lang="en">
      <StreetAddress>6 Gurko Str.</StreetAddress>
      <Locality>Sofia</Locality>
      <PostalCode>1000</PostalCode>
      <CountryName>BG</CountryName>
    </PostalAddress>
    <PostalAddress xml:lang="bg">
      <StreetAddress>ул. Гурко № 6</StreetAddress>
      <Locality>София</Locality>
      <PostalCode>1000</PostalCode>
      <CountryName>BG</CountryName>
    </PostalAddress>
  </PostalAddresses>
  <ElectronicAddress>
    <URI xml:lang="en">http://www.crc.bg/index.php?lang=en</URI>
    <URI xml:lang="en">mailto:info@crc.bg</URI>
  </ElectronicAddress>
</SchemeOperatorAddress>
- <SchemeName>
  <Name xml:lang="en">BG:Supervision/Accreditation Status List of certification services from Certification Service Providers, which are
supervised/accredited by the referenced Scheme Operator's Member State for compliance with the relevant provisions laid down in Directive
1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.</Name>
  <Name xml:lang="bg">BG: Списък на състоянието на надзор/акредитация на удостоверителните услуги, предлагани от доставчици на
удостоверителни услуги, които са под надзор/акредитация в Република България по отношение на съответствието им с разпоредбите на
Директива1999/93/EO на Европейския парламент и на Съвета от 13 декември 1999 г. относно правната рамка на Общността за електронните
подписи.</Name>
</SchemeName>
</SchemeInformation>
</TrustServiceStatusList>
```

	Austria		19/08/2015	19/02/2015	15	Hellenic Telecommunications and Post Commission - EETT
	Belgium		31/08/2015	02/03/2015	26	MINISTRY OF INDUSTRY ENERGY AND TOURISM
	Bulgaria					
	Czech Republic					
	Denmark					
	Germany					
	Greece					
	Spain					
	France					
	Italy					
	Netherlands					
	Portugal					
	Romania					
	Slovakia					
	Slovenia					
	Sweden					
	Switzerland					
	United Kingdom					

<http://www.polysys.eu/tledit/Download/>より抜粋

②EUトラストリスト(XML)

UK: イギリスのトラストリスト(XML)

```
<ListIssueDateTime>2015-02-27T00:00:00Z</ListIssueDateTime>
- <NextUpdate>
  <dateTime>2015-03-30T23:00:00Z</dateTime>
</NextUpdate>
- <DistributionPoints>
  <URI>http://www.tscheme.org/UK_TSL/index.html</URI>
</DistributionPoints>
</SchemeInformation>
```



United
Kingdom



31/03/2015 27/02/2015

6

tScheme Limited

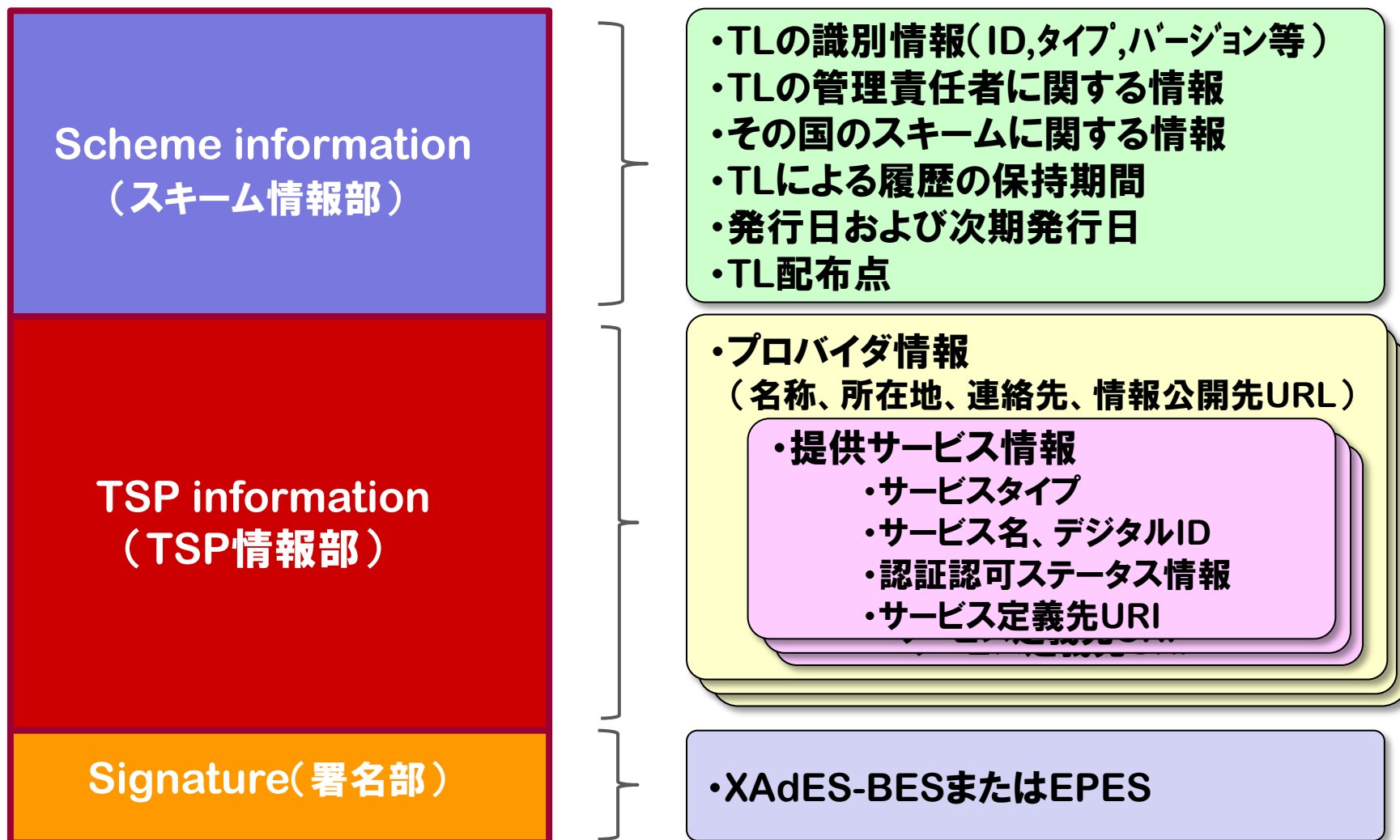
Generated by TLEdit server on 09 Apr 2015 15:07:21 CEST

<http://www.polysys.eu/tledit/Download/>より抜粋

2015/4/10現在
イギリスのTLは**期限切れ**のまま
(通常: 次回更新は6カ月後)
イギリスのTSPは**0件** (フランス:TSP: 16件 TS: 98件)

③ EUトラストリストの構成

トラストリストは、主に以下の3つのパートからなる。



④EUTラストリストにおけるスキーム **JNSA**

EUTラストリストにおけるスキームを構成する要素

- ◆提供するサービスの種類
 - 提供するサービスの格付けの表明
 - 上記格付けの、ETSI標準(QC／PKC等)との対応関係
- ◆基づく当該国の法律についての表明
- ◆審査認定機関についての規定
- ◆告知機関についての規定
- ◆認定認可手続きに関する規定
- ◆ラストリスト公開先URL

など

- ◆スキームオペレータ(上記スキームの管理責任者)
特にラストリストのスキームオペレータを**TLSO**と呼ぶ

法律と運用と技術規格の整合性が取られている

④ EUトラストリストにおけるスキーム

スキーム記述(フランスTLから)

TSL Scheme Information

Scheme Operator Name:

General Secretariat for the Modernisation of Public Action

Scheme Name:

FR:Supervision/Accreditation Status List of certification services [from Certification Service Providers, which are supervised/accredited by the referenced Scheme Operator's Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.](#)

Scheme Information URI:

<http://references.modernisation.gouv.fr/en>

公共活動近代化事務局(SGMAP)
行政手続きの合理化・公共データの共有化がミッション

この部分は
「お決まり。」

ここにその国のスキームが
掲載されている

⑤ EUトラストリストの特徴

●相互運用のための機構

- ・TSLタイプ(各国のトラストリストを各社の検証アプリ共通的にハンドリングするための識別情報)

※CC: 国名を示す2文字コード

EU共通:	http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUgeneric
非EU国/組織:	http://uri.etsi.org/TrstSvc/TrustedList/TSLType/CClist

- ・スキームタイプ/コミュニティ/ルール(相互運用の範囲)

EU共通:	http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon
EU各国:	http://uri.etsi.org/TrstSvc/TrustedList/schemerules/CC

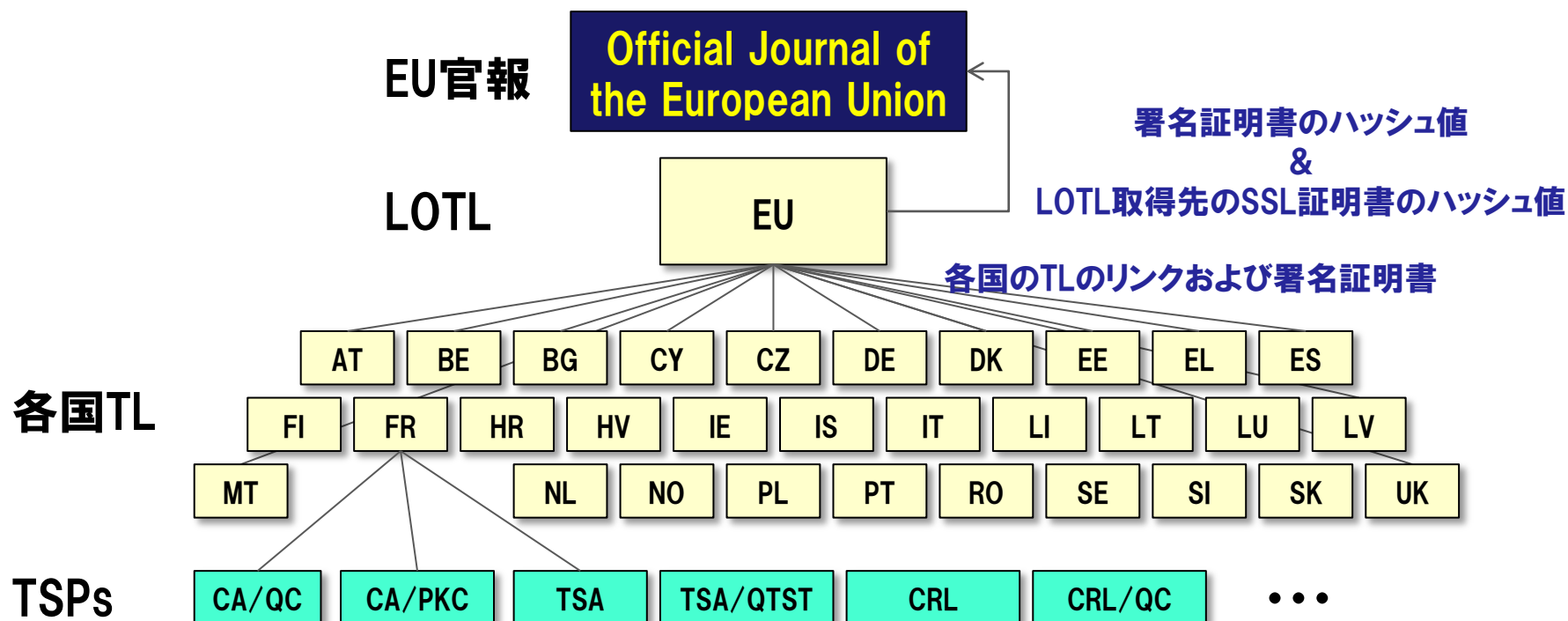
- ・他のTLへのポインタ(相互運用国のリストのポインタ。
EU加盟国の場合はここへLOTLを適用し、
メンテ負担を集約 & 軽減)

公開先:	https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml
TSLタイプ:	http://uri.etsi.org/TrstSvc/TrustedList/TSLType/EUlistofthelists
コミュニティ:	http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUlistofthelists

⑤EUトラストリストの特徴

●リストオブトラストリスト(LOTL)

各国のトラストリストへのポインタおよび識別情報(トラストリストへの署名証明書)が記載されたトラストリストの上位リスト



LOTLを安全に取得・検証することで
リンクされる各国TLを安全に検証することができる

⑤ EUトラストリストの特徴

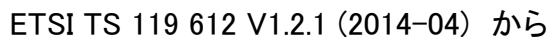
● リストオブトラストリスト(LOTL)のトラストアンカー

• Official Journal of the European Union(EU官報)に掲載される
European Commissionの署名証明書のハッシュ値リスト

21.3.2015	EN	Official Journal of the European Union	C 95/15
Information related to data on Member States' trusted lists as notified under Commission Decision 2009/767/EC, as amended (2015/C 95/05) Pursuant to Article 2(4) of Commission Decision 2009/767/EC⁽¹⁾, as amended by Commission Decision 2010/425/EU⁽²⁾ and Commission Implementing Decision 2013/662/EU⁽³⁾, the European Commission makes available to all Member States, through a secure channel to an authenticated web server, the information notified by Member States under Article 2(3) of the Decision, both in a human readable form and in a signed machine processable form. The information notified by Member States is available at the following URLs: — https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml for a signed xml machine processable version, - and — https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-hr.pdf for a human readable version. 3. Digest value for the third certificate, valid until 16 November 2015: — SHA-256 digest (Hex) value: 5d 39 e8 f1 16 69 50 e9 97 38 32 ad 26 6f 06 74 2c c4 a9 48 48 69 df 61 ef cb 84 9d b2 fc 60 4a — SHA-1 digest (Hex) value: a8 4e 18 97 24 1f 85 c5 55 d0 3f 48 f5 a1 95 d6 3c 6a a6 5b			

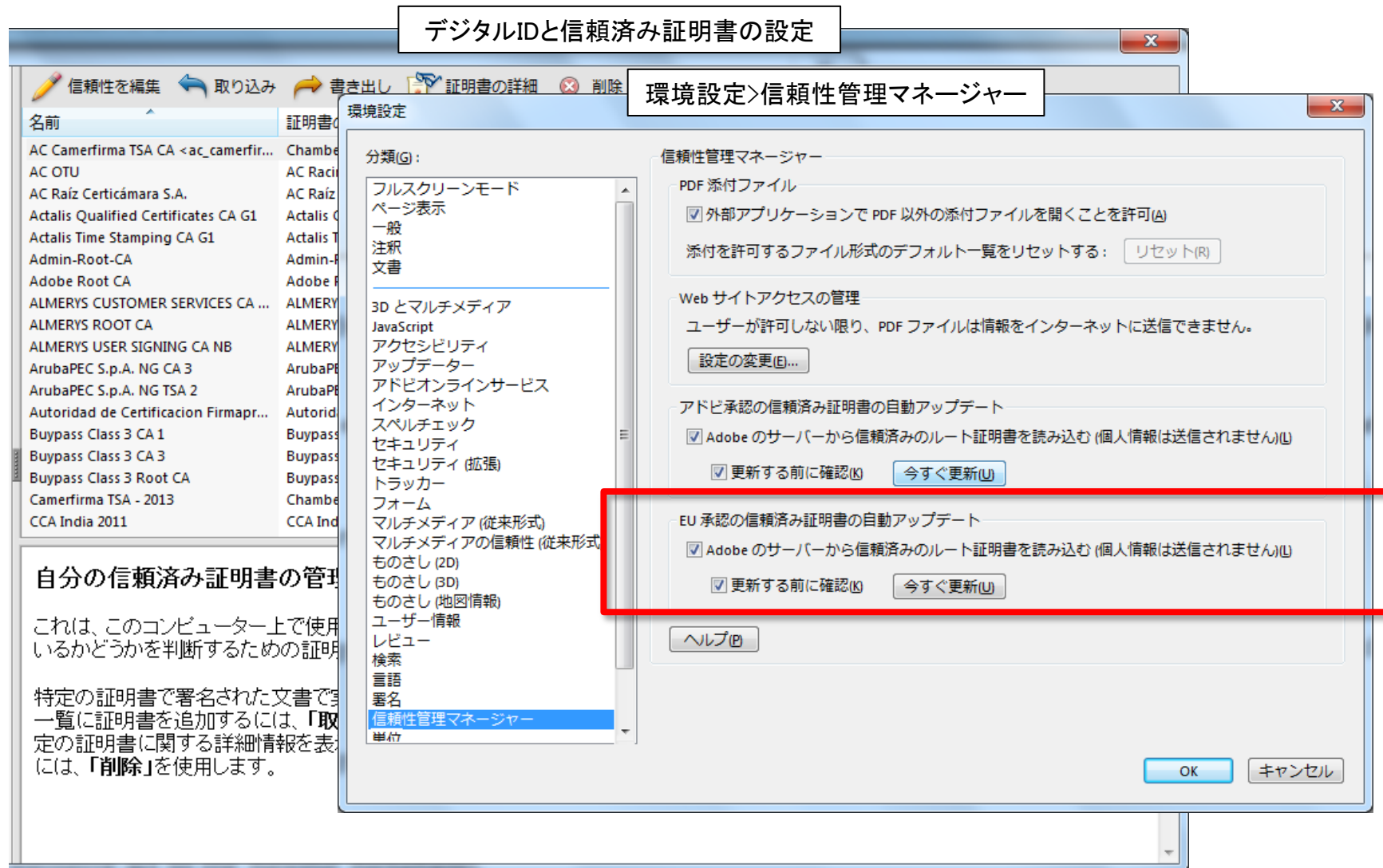
[http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1427848559233&uri=CELEX:52015XC0321\(03\)](http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1427848559233&uri=CELEX:52015XC0321(03))

- ・認定取得前から掲載
- ・廃業／停止したサービスも掲載
- ・ステータス認定履歴情報部で前ステータスも確認可
- ・移管先情報も記載可で廃業や移管にも対応



2-2. トラストリストの活用事例

Adobe Reader XI (v11.0.10) における実装事例



3. 日本における信頼基盤としての のトラストリストの可能性



3－1. 証明書検証の現状

3－2. トラストリスト導入によるBefore/After

3－3. トラストリストのもたらす効果(可能性)

証明書リストを信頼する仕組みの現状は？

PKI対応アプリが提供する証明書リストを**信用**している
→アプリ提供者が定める**証明書登録基準**を信頼している

(例)マイクロソフトの「ルート証明書プログラム」より

[<https://technet.microsoft.com/ja-jp/library/cc751157.aspx>]

- WebTrust (CA/Browser Forumでガイドラインを策定)
- ETSI TS 101 456 v1.2.1 またはそれ以降
- ETSI TS 102 042 v1.2.1 またはそれ以降
- 政府CA (WebTrust For CAs, ETSI TS 102 042, ETSI 101 456, ISO 21188
と同等であること)

国内では

どちらかというとブラウザで電子商取引を行う際の
電子証明書を利用した**サーバ認証**と**通信の安全性確保**や
コードサインによるアプリの**発行元証明**がメイン！
電子署名では有効に利用されていない！？

個別PKI対応**アプリに依存する**証明書リストの課題

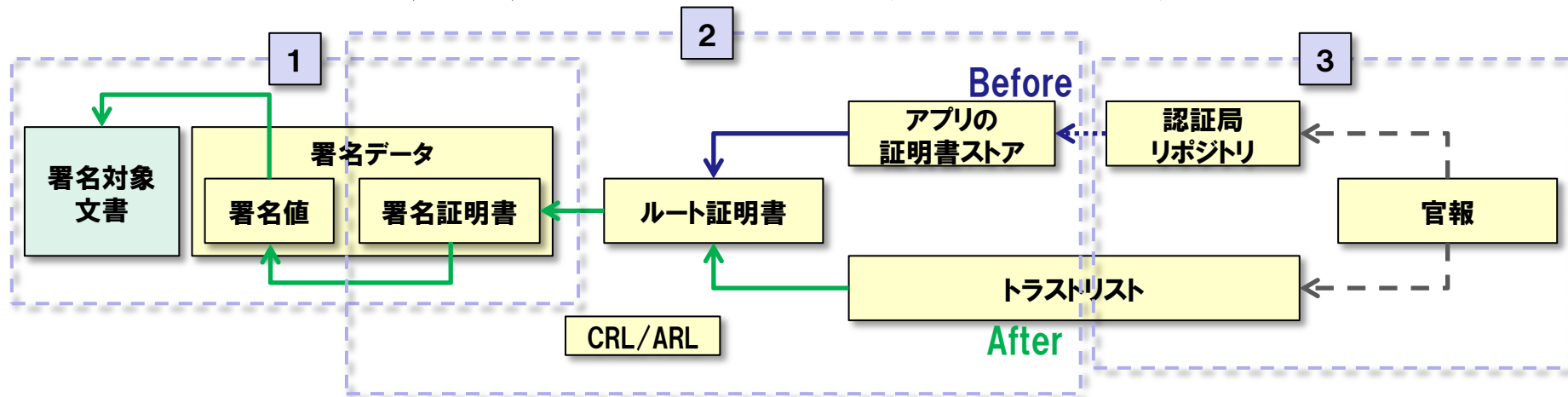
- ①信頼点がアプリ提供元(提供元企業に依存)
- ②相互運用性(アプリによって証明書リストが異なる)
- ③レベル合わせ(アプリによって検証レベルが違う)
- ④長期経過後(過去の時点の履歴がない)
- ⑤自動処理できない(更新方法がアプリに依存)

3-2. トラストリスト導入によるBefore/After **JNSA**

1. 署名検証フローのBefore/After

手順	検証項目（概要）	Before	After
1	（署名証明書を利用して） 署名値の検証	（従来通り）	（従来通り）
2	署名証明書の検証	—	—
	1 署名証明書からルート証明書 までの認証パスの検証	事前にアプリの証明書ストアにルート証明書を登録	トラストリストにより 自動化 （ルート証明書の識別）
	2 認証パス上の各証明書の 失効確認（失効情報、有効期限）	（従来通り）	（従来通り） （※）
3	ルート証明書のステータス確認 （トラストアンカーとしての検証）	リポジトリおよび 官報 を確認	トラストリストにより 自動化 （ステータス・格付け確認）

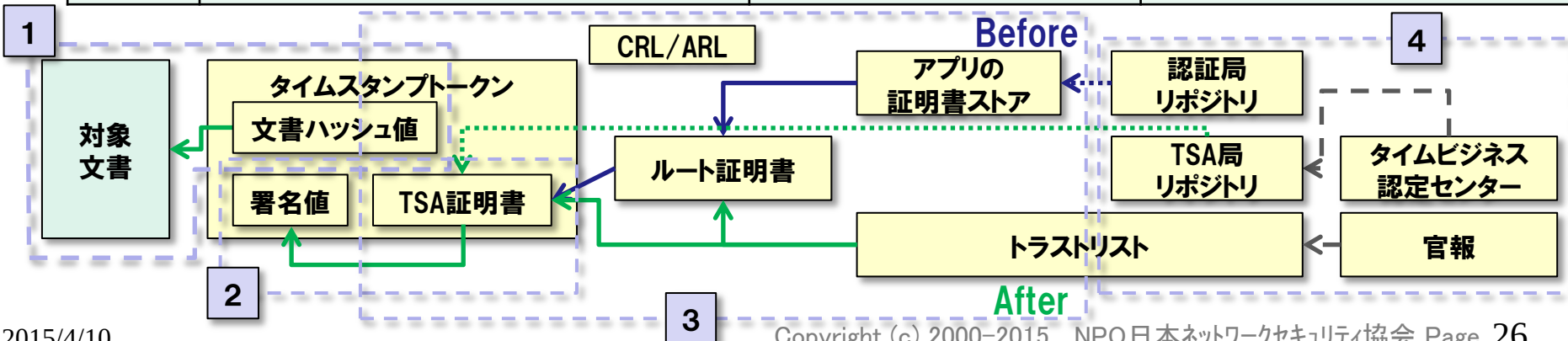
※：失効情報発行をCRL/OCSP/LDAPに関するTSPが行う場合はその検証も実施する



3-2. トラストリスト導入によるBefore/After JNSA

2. タイムスタンプ検証フローのBefore/After

手順	検証項目（概要）	Before	After
1	文書ハッシュ値の検証	（従来通り）	（従来通り）
2	（TSA証明書を利用して）タイムスタンプトークンの署名値の検証	（従来通り）	（従来通り）
3	TSA証明書の検証	—	—
1	TSA証明書からルート証明書までの認証パスの検証	証明書ストアを信頼（WebTrust）	トラストリストにより自動化（ルート証明書の識別とステータス・格付け確認）
	認証パス上の各証明書の失効確認（失効情報、有効期限）	（従来通り）	（従来通り）
4	TSA局のステータス確認（トラストアンカーとしての検証）	認定センターのHPを確認 ※TSA証明書との関係は現状わからない	トラストリストにより自動化（TSA証明書の識別とステータス・格付け確認）



3-3. トラストリストのもたらす効果(可能性) **JNSA**

- 1. 現行の国内各種認証局サービス、タイムスタンプサービスの枠組みを再整理できる。**
- 2. プロバイダ廃業後での、ユーザでの証明書／TST検証の厳密性が向上する。**
- 3. 諸外国(特にEU各国)との相互運用が可能になる。**

3-3. トラストリストのもたらす効果(可能性)

1. 現行の国内各種認証局サービス、タイムスタンプサービスの枠組みを再整理できる。

	種別	根拠法・制度等	認定主体		審査・監査機関
1	GPKI	政府認証基盤(総務省)	官職CA	—	
			AppCA	WebTrust	WebTrust審査機関
2	LGPKI	地方公共団体組織認証基盤(総合行政ネットワーク運営協議会)	組織CA	—	
			AppCA	WebTrust	WebTrust審査機関
3	JPKI	電子署名に係る地方公共団体の認証業務に関する法律(総務省)	—		
4	認定認証業務	電子署名法(法務省・経産省・総務省)	主務大臣		電子署名・認証センター(JIPDEC)
5	タイムスタンプ (時刻認証業務)	タイムビジネスに係る指針(総務省) タイムビジネス信頼・安心認定制度(JADAC)	タイムビジネス認定センター(JADAC)		
6	商業登記 (電子認証登記所)	商業登記に基づく電子認証制度(法務省)	—		
7	HPKI	保健医療福祉分野の公開鍵基盤(厚生省)	厚生省		準拠性監査報告書による
8	その他 (特定認証業務等)	・電子署名法(法務省・経産省・総務省)	・WebTrust for CA ・ETSI		

3-3. トラストリストのもたらす効果(可能性)

1. 現行の国内各種認証局サービス、タイムスタンプサービスの枠組みを再整理できる。

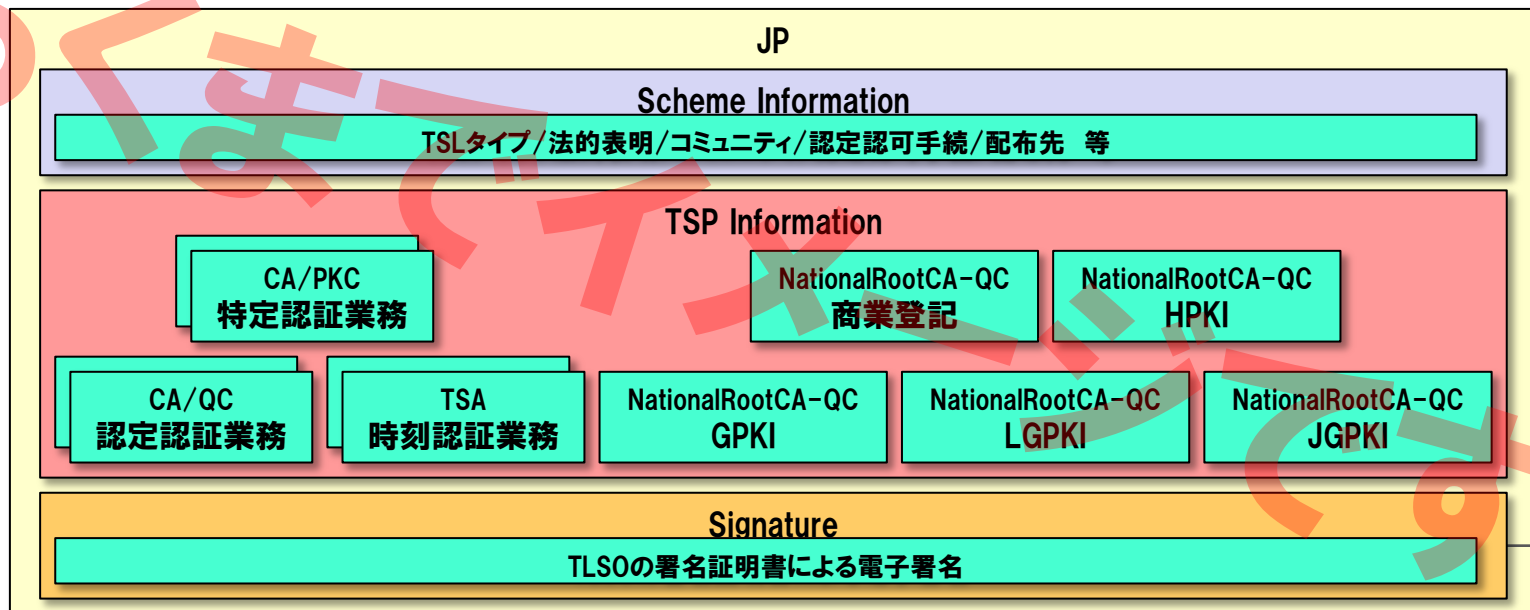
JP官報

官報
(独立行政法人国立印刷局)

署名証明書のハッシュ値
&

TL取得先のSSL証明書のハッシュ値

TL

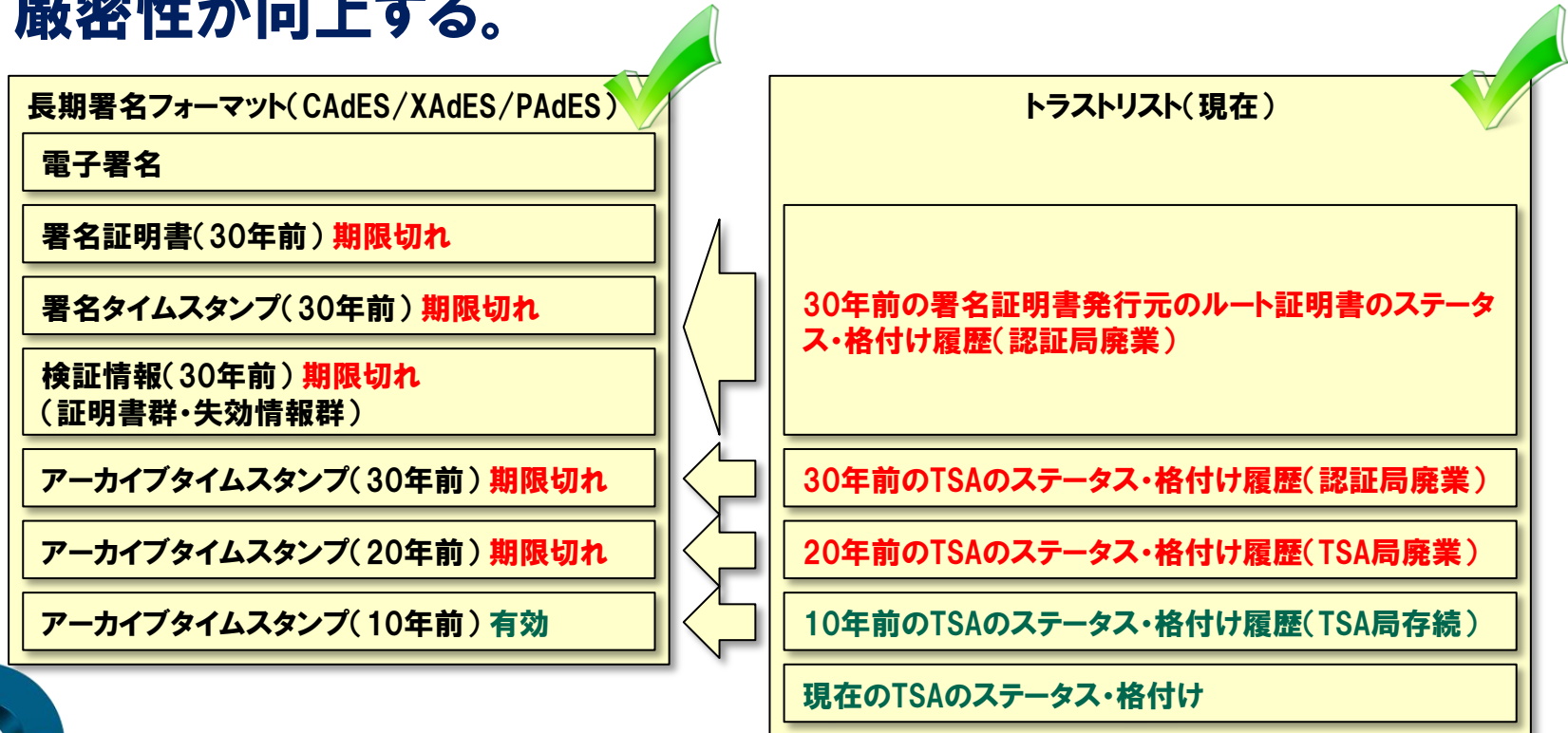


- ・審査認定の国内共通化、EUとの共通化
- ・管理監督機関の国内一本化 …等々

が実現できれば！！

3-3. トラストリストのもたらす効果(可能性) **JNSA**

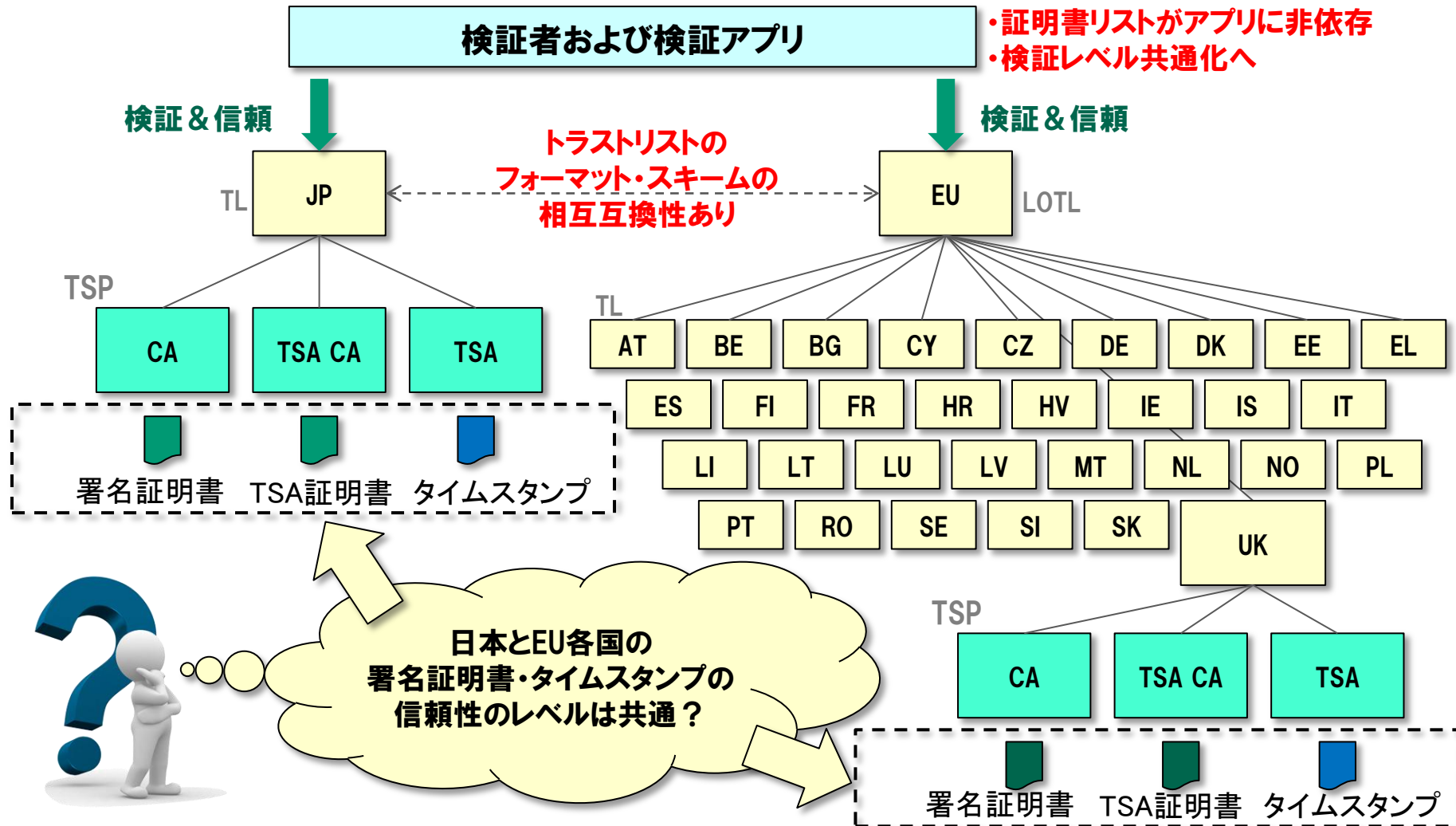
2. プロバイダ廃業後での、ユーザでの証明書／TST検証の 厳密性が向上する。



長期署名フォーマット上は有効だけれども、
いくつか認証局もTSA局も既に廃業しているし、
過去の運用状況等、
本当に大丈夫だったのだろうか？

3-3. トラストリストのもたらす効果(可能性)

3. 諸外国(特にEU各国)との相互運用が可能になる。



- ・証明書リストがアプリに非依存
- ・検証レベル共通化へ

4-1. トラストリスト導入に向けた課題

4-2. 最後に

1. 日本のトラストサービスに関するスキーム作り

- ・法制度化

- 現行法での対応付けおよび新規の制定や改定

- ・認定制度／監査制度の枠組みの整理・統一

- ・トラストサービスの規定

- トラストサービスに含めるべき現行サービスの選定

- 現行JIS規格との対応付けおよび新規の制定や改定

2. 他国との相互運用のための、ETSI標準の精査

- ・現行TL仕様が、日本を含むEU圏外国との相互運用に適用可能かを調査・検討. 必要があればETSIへ提案.

3. トラストリストのインプリメンテーション

- ・TL試作評価実験

- 署名／タイムスタンプの検証アプリへの組み込み実験

1. 日本版トラストサービス・トラストリストの実現に向けて

- ・実現に向けては幾多のハードル(特に法制度・審査認定共通化・監督機関)
- ・幸い他団体でもトラストリストに関する活動が活発化
- ・ぜひ他団体と連携して進めていきたい

2. 2015年度のJNSA 電子署名WGのテーマとして eIDASやトラストリストに取り組んで参ります。

ご清聴ありがとうございました。

