

# eシールの国際相互承認を見据えた課題等

eシールに係る検討会(第1回)

令和5年9月6日

慶應義塾大学SFC研究所

上席所員 濱口 総志

# eシールの定義 - 日本とEU

- 日本における定義
  - 電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み
- eIDAS規則における定義
  - “‘electronic seal’ means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter’s origin and integrity (「eシール」とは、データの起源と完全性を保証する為に電子データに付され又は論理的に関係している電子形式のデータをいう)”

# eシールに係る指針とeIDASの比較

eシールに係る指針	eIDAS規則	差異
<b>レベル1</b> eシールの定義（電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み）に合致するもの。	<b>eシール</b> “eIDAS規則3条” データの起源と完全性を保証する為に電子データに付され又は論理的に関係している電子形式のデータ	“措置”と“データ”の違いはあるものの同等と言える
<b>レベル2</b> 技術的には発行元証明として十分機能することが確認できるもの。	<b>先進eシール(Advanced)</b> “eIDAS規則 36条” a) eシールの作成者と一意にリンクされていること b) eシールの作成者を識別できること； c) eシールの作成者が、その管理下で高い信頼性をもってeシールの作成に使用できるeシール作成データを使用して作成される。 d) eシールが関連するデータと、その後のデータの変更が検出できるようにリンクされていること。	同等と言えるか
<b>レベル3</b> 組織等の実在性の確認の方法や認証局における設備のセキュリティ要件等について、十分な水準を満たしたトラストアンカーによって信頼性が担保され、発行元証明として機能することに関し、第三者のお墨付き（将来的には国による認定制度等の要否を検討）があるもの。	<b>適格eシール(Qualified)</b> “eIDAS規則3条” 適格eシール生成装置(QSCD)によって作成され、適格証明書(QC)に基づく先進eシール	日本では証明書の信頼性を要件としており、秘密鍵の保護環境が規定されていない  EUでは、法的効力が推定されるのに対し、日本では法定されていない <sup>3</sup>

# 組織が発行するデータの信頼性を確保する制度に関する 検討会資料との比較

	eシールのレベル	認証局のポリシーレベル	秘密鍵の保護	第三者監査と認証	ステータスの公開方法	監督
eIDAS規則14条の相互承認の範囲	適格eシール (Qualified Electronic Seal)	QCP-I- qscd	QSCD	eIDAS規則におけるQTSPとしての適格性認定	トラステッドリスト	監督機関による 事前 / 事後監督*
レベル3	先進eシール (Advanced Electronic Seal)	QCP-I	—			
レベル2		NCP+ NCP, LCP	セキュア暗号装置 —	ETSI基準に基づく 第三者認証 (任意)	認証機関のWeb (任意の第三者認証を受けた場合)	監督機関による事後監督*
レベル1	eシール (Electronic Seal)	—	—	—	—	監督機関による事後監督*

 : eIDAS規則によって定められている範囲

 : 技術基準が定められている範囲

# eIDAS 2.0でのeシール

- 36条に第2段落が追記
  - 欧州委員会は、この規則の発効後12ヶ月以内に、実施法によって、先進eシール(Advanced)の技術仕様および規格の参照番号を定めるものとする。先進eシールがこれらの仕様および規格を満たしている場合、先進eシールの要求事項への適合が推定されるものとする
  - これまで、先進eシール(Advanced)は法的要件とフォーマット(PAdES, XAdES等)のみが定められていたが、技術基準への適合を以て法的要件の充足が可能になる
- リモートeシールの規定
  - リモート適格eシール生成装置の管理サービス
  - 適格トラストサービスとしてeIDAS規則の評価・認定の枠組みに加わる

# eシールの欧州における利用例①

## TRACES(TRAde Control and Export System)

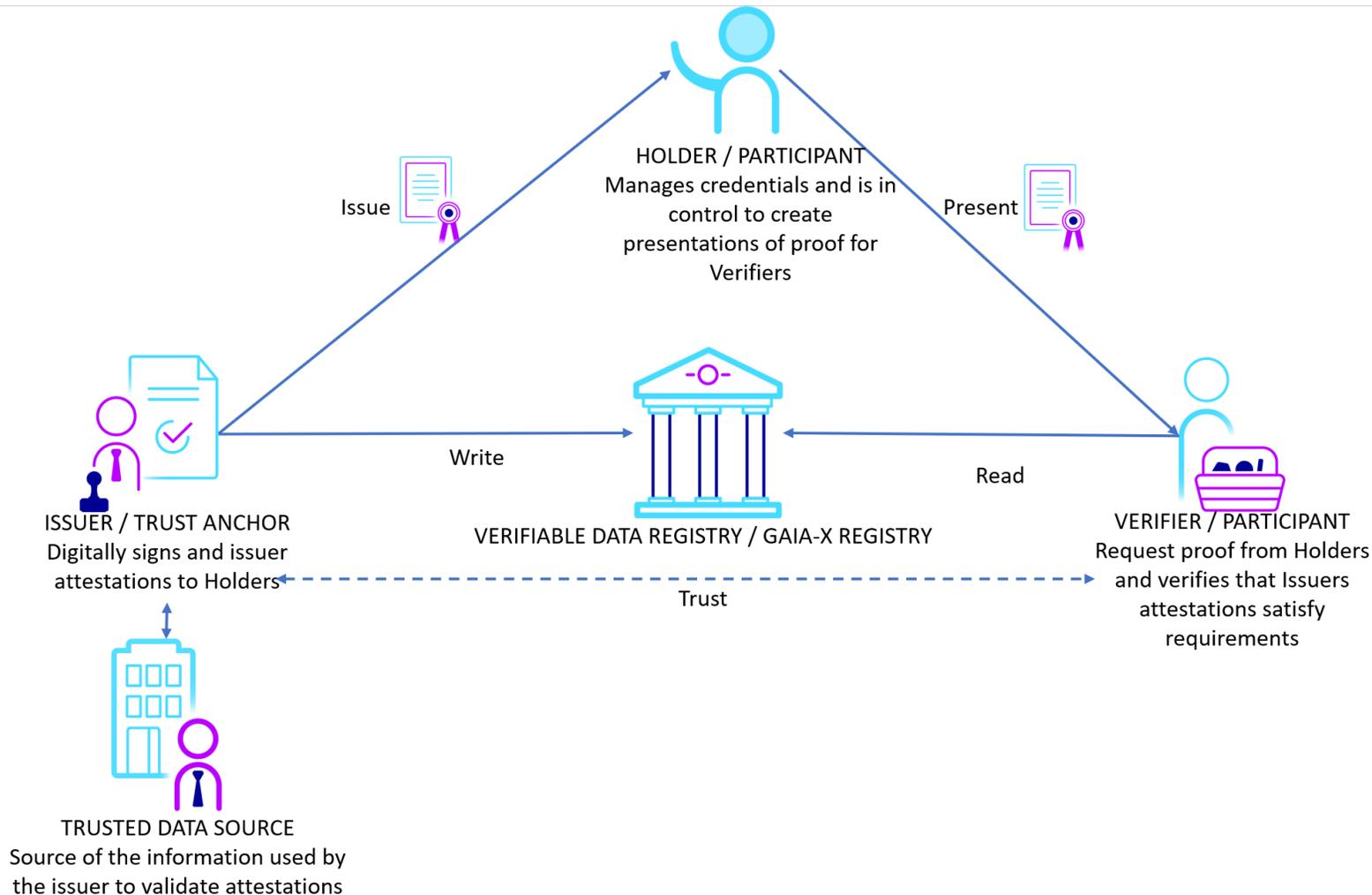
- 2022年3月、欧州委員会はDG SANTEおよびDG AGRIと共同で新たな協定に調印し、欧州連合（EU）に輸入されるすべての商品は、適格トラストサービスプロバイダ（QTSP）が発行する安全衛生デジタルシール証明書でシールされることを定めた。
- 欧州委員会が提供するオンラインプラットフォームであるTRACESシステムは、動物、動物製品、非動物由来の食品および飼料、植物のEU域内への輸入、動物および特定の動物製品のEU域内貿易およびEU域内への輸出に必要な衛生・植物検疫証明に使用される。

参照：<https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=542277930>

# eシールの欧州における利用例②

## GAIA-Xとeシール

参照：<https://gaia-x.eu/>

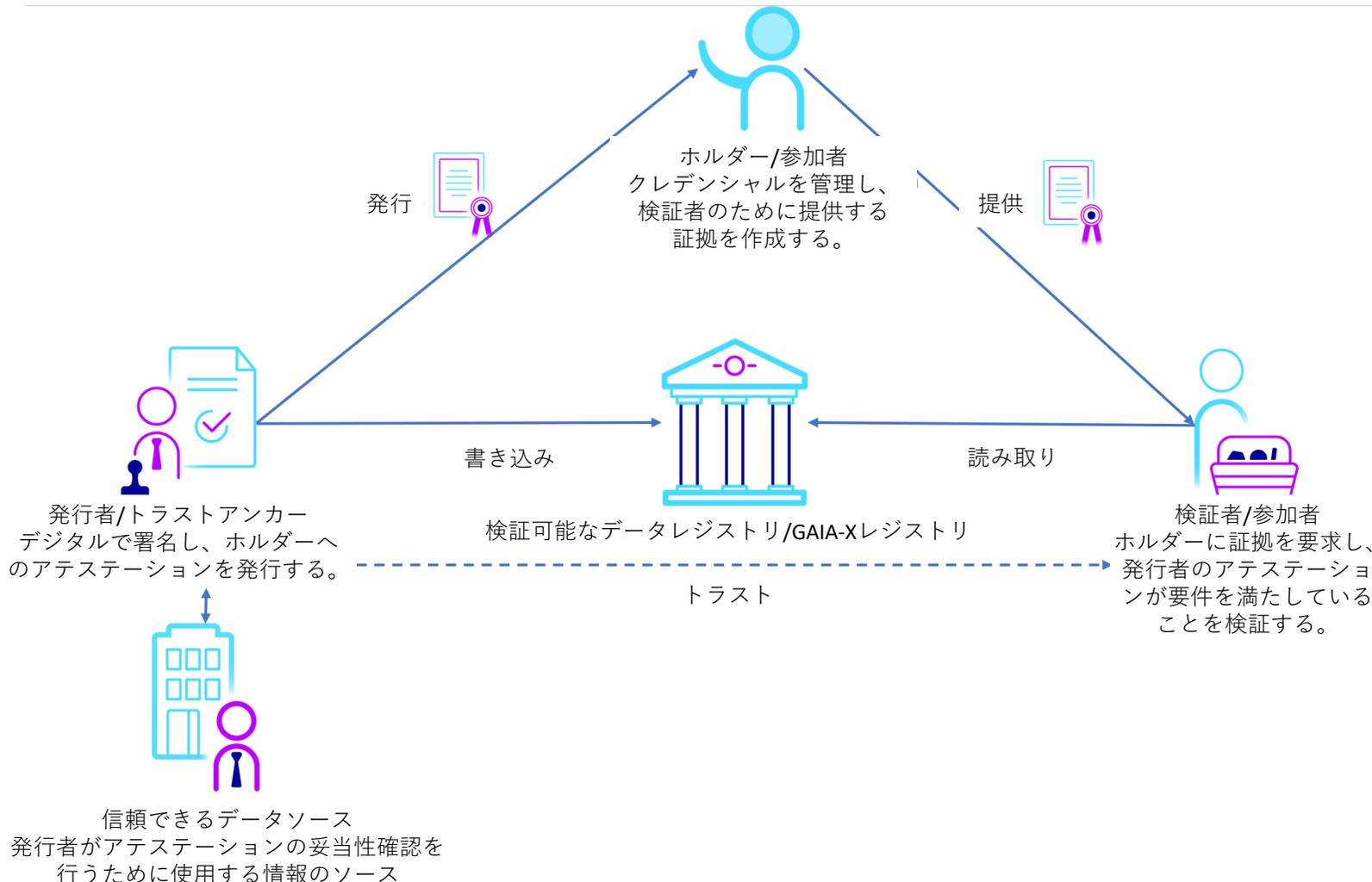


Name	Defined as
State	The Trust Service Providers (TSP) must be a state validated identity issuers or EV SSL issuers. <ul style="list-style-type: none"> <li>- For participant, if the legalAddress.country is in EEA, valid state identity issuers are <b>eiDAS</b> ones.</li> <li>- <b>Gaia-X</b> Association may also be a valid TSP for Gaia-X Association members.</li> </ul>
eiDAS	Issuers of Qualified Certificate for Electronic Signature as defined in eIDAS <a href="#">Regulation (EU) No 910/2014</a> (homepage: <a href="https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home">https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home</a> ) (machine: <a href="https://ec.europa.eu/tools/lotl/eu-lotl.xml">https://ec.europa.eu/tools/lotl/eu-lotl.xml</a> )
EV SSL	Extended Validation (EV) Secure Sockets Layer (SSL) certificate issuers are considered to be temporarily valid Trust Service Providers. (homepage: <a href="https://wiki.mozilla.org/CA/Included_Certificates">https://wiki.mozilla.org/CA/Included_Certificates</a> ) (machine: <a href="https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReportPEMCSV">https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReportPEMCSV</a> )
registration NumberIssuer	During the pilot phase, the Gaia-X Association nominated itself as a valid Trust Anchor under <a href="https://notary.gaia-x.eu">https://notary.gaia-x.eu</a>

# eシールの欧州における利用例② (和訳)

## GAIA-Xとeシール

参照：<https://gaia-x.eu/>



名前	定義
国 (State)	<p>トラストサービスプロバイダ (TSP) は、有効な身元発行者又はEV SSL発行者でなければならない。</p> <ul style="list-style-type: none"> <li>- 参加者について、LegalAddress.countryがEEAに存在する場合、有効な状態の身元発行者はeIDASのものである。</li> <li>- Gaia-X Associationは、Gaia-X Associationメンバーにとって有効なTSPである場合もある。</li> </ul>
eIDAS	<p>eIDAS規則 (EU) No 910/2014に定義される電子署名用適格証明書の発行者。</p> <p>(homepage: <a href="https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home">https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home</a>)</p> <p>(machine: <a href="https://ec.europa.eu/tools/lotl/eu-lotl.xml">https://ec.europa.eu/tools/lotl/eu-lotl.xml</a>)</p>
EV SSL	<p>Extended Validation (EV) Secure Sockets Layer (SSL)証明書発行者は、一時的に有効なトラストサービスプロバイダとみなされる。</p> <p>(homepage: <a href="https://wiki.mozilla.org/CA/Included_Certificates">https://wiki.mozilla.org/CA/Included_Certificates</a>)</p> <p>(machine: <a href="https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReportPEMCSV">https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReportPEMCSV</a>)</p>
登録番号発行者 (registrationNumberIssuer)	<p>実証段階においては、GaiaX Associationは、<a href="https://notary.gaia-x.eu">https://notary.gaia-x.eu</a>の有効なトラストアンカーとして自らを指名した。</p>

# eシール利用のトレンド

- 自動処理
- リモートeシール
- 文書からデータへ

# 相互承認

## 第14条 国際的側面

1. 第三国に設立されたトラストサービスプロバイダが提供するトラストサービスは、当該第三国のトラストサービスが、EUと当該第三国またはTFEU第218条に基づく国際機関との間で締結された協定に基づいて承認されている場合、EUに設立された適格トラストサービスプロバイダが提供する適格トラストサービスと法的に同等であると認められる。
2. 第1項で言及される協定は、特に以下を確保するものとする：
  - (a) 協定が締結された第三国又は国際機関のトラストサービスプロバイダ及びその提供するトラストサービスによって、EUに設立された適格トラストサービスプロバイダ及びその提供する適格トラストサービスに適用される要件が満たされること；
  - (b) 域内に設立された適格トラストサービスプロバイダが提供する適格トラストサービスが、協定が締結された第三国又は国際機関のトラストサービスプロバイダが提供するトラストサービスと法的に同等であると認められること。

# 相互承認 eIDAS 2.0での修正

## 第14条 国際的側面

1. 欧州委員会は、第48条(2)に従い、その領域内に設立されたトラストサービスプロバイダ及びその提供するトラストサービスに適用される第三国の要件が、域内に設立された適格トラストサービスプロバイダ及びその提供する適格トラストサービスに適用される要件と同等であるとみなすことができる条件を定めた実施法を採択することができる。
2. 欧州委員会が第1項に基づく実施法を採択した場合、または条約第218条に従ってトラストサービスの相互承認に関する国際協定を締結した場合、当該第三国に設立されたプロバイダーが提供するトラストサービスは、域内に設立された適格トラストサービスプロバイダーが提供する適格トラストサービスと同等であるとみなされるものとする；

# 相互承認に向けたEUの動向

- TC AdES LTOL
  - EU-第三国間の先進レベルでの相互運用性の為のトラステッドリスト
  - 2023年3月、ウクライナのトラステッドリストが追加
  - eIDAS2.0 36条の追記と併せて、先進eシール（及び電子署名）の評価制度となるか
- EU LOTL
  - Art.14の相互承認はこれまで実績なし
  - ウクライナからの相互承認の申し入れを受けた結果、TC AdES LTOLが作られた

Third Countries Trusted List Browser

The European Commission maintains and publishes a Third Countries AdES List Of The Lists (TC AdES LOTL) containing information notified by the Third Countries and referencing the Third Countries trusted lists to facilitate the technical validation of electronic signatures or seals created in those Third Countries as meeting the requirements of (EU) advanced electronic signatures or seals in accordance with Regulation (EU) No 910/2014.

The effective verification of such a compliance is entirely left to the responsibility of the relying parties. This list shall under no circumstances be used in the context of recognition in accordance with Article 14(1) of Regulation (EU) No 910/2014.

The European Commission, through the DIGITAL programme, provides this tool for anyone to browse the TC AdES LOTL and the national Third Countries Trusted Lists referenced within.

The signature applicability rules (the validation policy) for the electronic signatures and seals supported by certificates issued by trust service providers established in the Third Countries referenced in the TC AdES LOTL can be downloaded by clicking on the button below.

[Download signature applicability rules](#)

---

Trusted Lists

 Ukraine Issue date 2023-08-17	...
 TC AdES LOTL Issue date 2023-03-23	...

<https://eidas.ec.europa.eu/efda/tl-browser/#/screen/tc-tl>

# 相互承認に向けた課題

比較項目	EUの現状	日本の現状	課題
法的効力	適格eシールであれば、データの起源と完全性が推定される	規定なし	<ul style="list-style-type: none"> <li>eシールの法的効力が定められていない</li> </ul>
秘密鍵の保護環境	適格eシール生成装置(QSCD)の義務化	規程なし	<ul style="list-style-type: none"> <li>秘密鍵の保護環境が定められていない日本のeシールはレベル3であっても適格eシールと同等とされない可能性がある(eIDAS規則において相互承認(Mutual Recognition)は、適格トラストサービスについて定められている)             <ul style="list-style-type: none"> <li>a. eシールの指針にもある様に、少なくとも秘密鍵がセキュアトークンで保護されていることを検証時に確認できる仕組みが必要か</li> </ul> </li> </ul>
検証基盤	トラステッドリスト	ブリッジ認証局	<ul style="list-style-type: none"> <li>相互運用性に課題</li> <li>ブリッジモデルでは過去に遡って検証できない</li> </ul>
技術基準	欧州標準化団体による標準化	eシールに係る指針(総務省) eシール解説(JDTF)	<ul style="list-style-type: none"> <li>技術基準群の開発/維持に関する枠組みがない</li> </ul>
リモートeシール	eIDAS2.0で法定	Jリモート署名ガイド(JT2A)	<ul style="list-style-type: none"> <li>リモートeシールに関する公的な裏付けがない</li> </ul>