【講演レポート】JIPDECセミナー

eIDAS2.0 - eIDAS規則の改正案の解説-

株式会社コスモス・コーポレイション　取締役　ITセキュリティ部　責任者
（JIPDEC　客員研究員）濱口　総志　氏

eIDAS2.0の経緯とeIDAS1.0の評価

eIDAS規則は、2014年に批准、その後2016年にトラストサービスに関しての適用が開始されたもので、4年ごとのレビューが定められています。2021年6月にeIDAS2.0が欧州議会に立法提案されたことを受け、本日は主にeIDAS2.0の経緯とその内容についてご説明します。

なお、現時点では草案が示されている段階でeIDAS2.0の批准が決定しているものではありません。

eIDASのレビュー

2016年に適用が開始されたeIDAS規則の中で、レビューに関しても時期や内容が規定されており、第49条において、特に下記６つの項目を含む特定の規則を変更する場合は適切であるか否かを本規則の適用と技術、市場、法的発展により得た経験を考慮して評価することと定められています。

・第6条 ：eIDの相互承認
・第7条：(f) eID通知加盟国によるオンライン認証の可用性保証
・第34条： 適格保存サービス
・第43条： eデリバリーサービスの法的効力
・第44条： 適格eデリバリーサービスの要件
・第45条：ウェブサイト認証の適格証明書の要件

eIDAS2.0 – 経緯

2020年2月、欧州委員会にてeIDASの規則改定が発表され、同年7月、初期影響評価が公開されたと同時にパブコメが開始されました。計53件のフィードバックがあり、2020年末に欧州委員会から何らかの方向性が示されると期待されていましたが、結果としては2021年6月に委員会採択という形でeIDAS2.0が提案されました。現在はeIDAS2.0草案に対するパブコメ（2021年9月2日まで）が募集されており、その後発行から12か月以内に施行される見通しとなっています。

eIDAS1.0の評価

膨大な評価結果の中からいくつか抜粋してご紹介します。

・「eID」

それぞれの国から通知されたeIDスキームを各国のオンラインサービスで受け入れるものですが、通知されたスキームでカバーできたEU市民への普及率は59%に留まる結果となりました。さらに、加盟

国間で互いに評価（3段階）しあうピアレビュー方式を取っていましたが、技術上の判定が難しかったこと、GDPR対応の難しさなどがあり課題が残る結果となりました。

・「トラストサービス」
70%がコスト、時間の削減および行政手続きの簡略化に効果を実感した、という結果が出たものの、[トラストサービスプロバイダ]からは下位規則の不足から生じる加盟国間の不整合（オンラインでの身元確認方法など）等、不平等が生じているという声も聞かれ課題となっています。

・「新たな環境」
分散台帳、ポータブルアイデンティティ、電子アーカイブといった新たな技術の普及により、トラストサービスやeIDAS2.0を拡充していく必要が出てきました。

・「デジタル化」
eIDASがデジタル化に寄与したことは認められていますが、ベーシックな信頼性のみを証明するものであり、実在する自然人または法人であるという事実以上の属性に関しては、信頼性の保証はできていません。セクター（教育、通信、旅行等）によっては属性情報を必要とする場合もあり、その要望にはeIDASだけでは対応できていないという課題もあります。

eIDスキームの推移

eIDのスキームは、2017年Q3に1件通知されて以降、2020年Q3までに計19件（図1）が通知されました。加盟国の中でも19のスキームしかカバーされておらず、これが上で挙げたEU市民への普及率（59%）に表れている形となります。

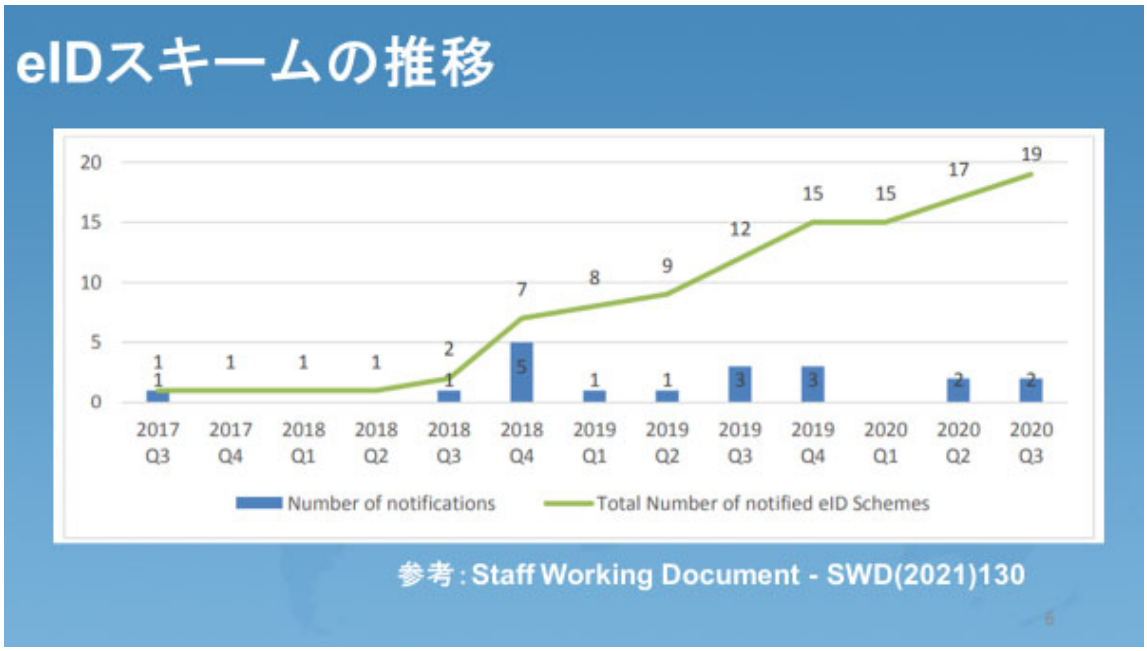

図1.eIDスキームの推移

国境を越えた認証の回数とQTSP（適格トラストサービスプロバイダ）の推移

国境を越えた認証の回数は2017年の917回から2020年の62,761回（図2）まで、右肩上がりで増えているものの欧州委員会が当初想定していた回数には達していません。

QTSP（適格トラストサービスプロバイダ）数は順調に増えており（図3）、2020年Q３では186件となっています。

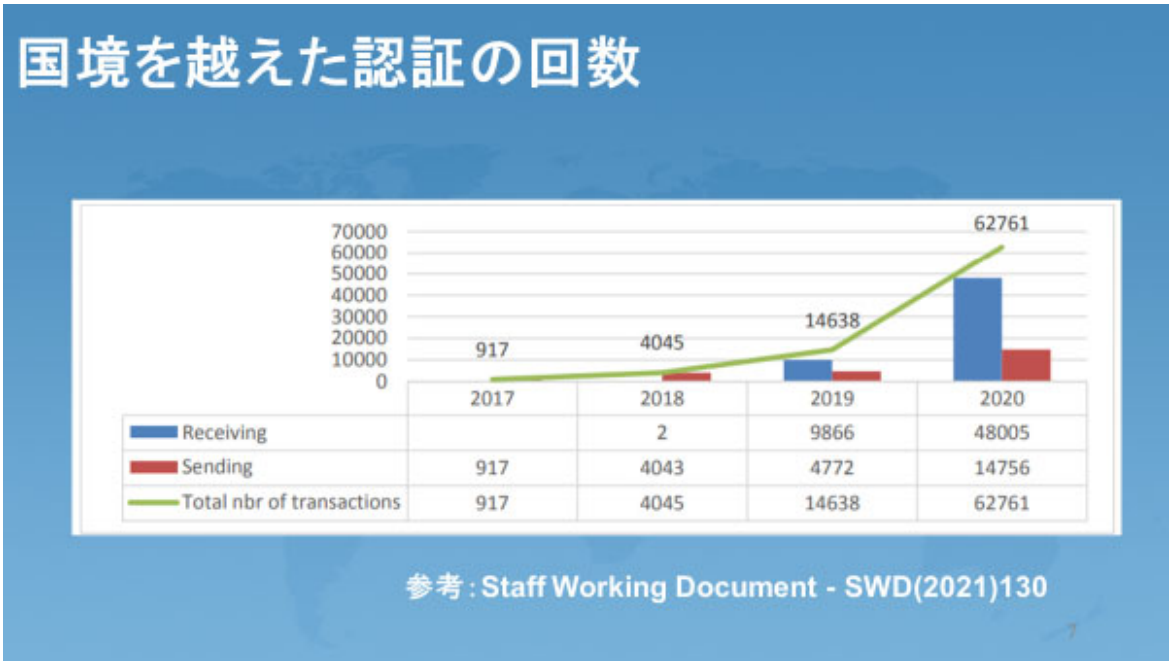

図2.国境を越えた認証の回数

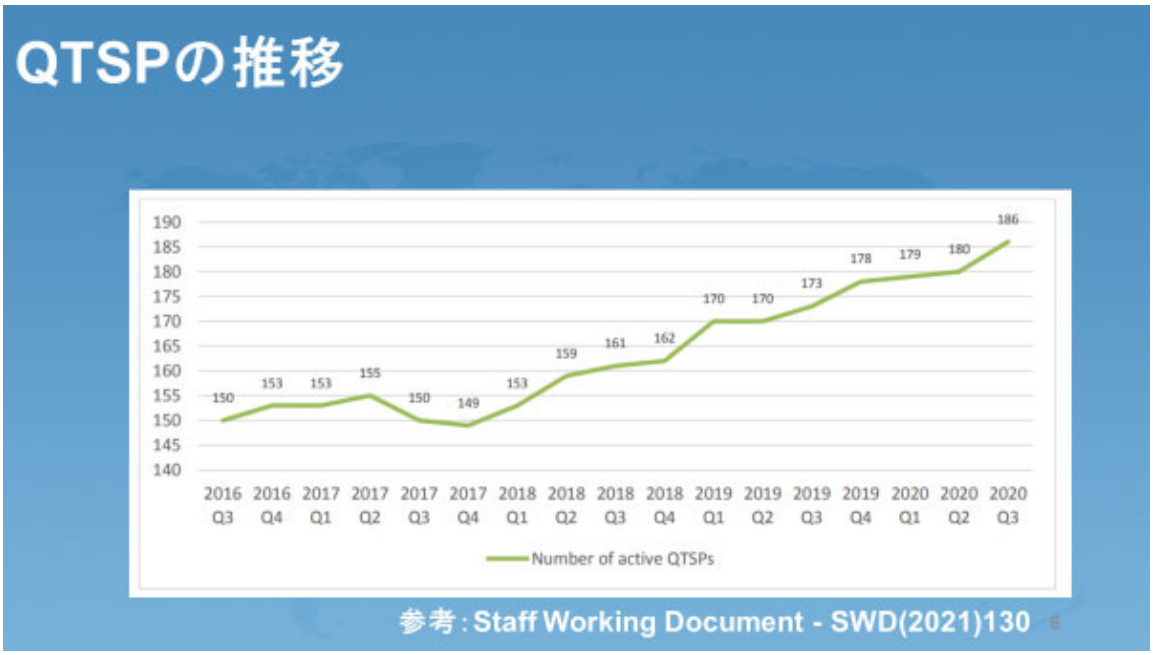

図3.QTSPの推移

改定案の内容　1）EU Digital Identity Wallet

共通インターフェース

加盟国には、希望する全欧州市民、在留者、企業が利用可能なeIDの枠組みを整備し、本規則発効後12か月以内にEU Digital Identity Wallet（以下、EUDIW）を発行することが義務付けられました。

また、個人識別データ及び属性の電子証明は、透明性があり、かつユーザが追跡可能な方法で取得、保管するなどの仕組みを用意する必要があること、適格電子署名のサポート、保証レベルはHighとすることが新たに定められました。ウォレットに証明書や属性証明を発行するTSP（トラストサービスプロバイダ）、QTSP（適格トラストサービスプロバイダ）のための共通のインターフェース（オンライン、オフラインとも）を備える必要もあり、依拠当事者（RP）による識別データおよび属性証明の要求と確認を行うことと明記されています。

さらに、EU Digital Identity Wallet Trust Markを表示することで、ユーザが利用しているウォレットがEUで認証されたものである事を確認できるようにする必要もあります。

通知と認証

サービス事業者である依拠当事者（RP）は、何の目的で検証するのかを事前に加盟国に通知する必要があり、同時に法的要件への準拠を確実にすることが求められています。

一方、加盟国はサービス事業者に対して共通認証機能を実装しデータの透明性を保証することとされ、技術、運用に係る仕様などの詳細については実施法によって施行から6か月以内に規定する必要があります。

次にEUDIWの認証ですが、認証は製品認証の対象内で、評価・認証のスキームはEUサイバーセキュリティ認証フレームワーク（検討中）を適用することが検討されています。これは、恐らく、アプリで実装されることが想定されており、実際の評価は加盟国の認定を受けた公的・民間機関が行い、認証されたリストは欧州委員会が公開・管理していくことになります。

使用方法

EUDIWは、行政サービスのような公的オンラインサービスのほか、多要素認証など強固なユーザ認証を要求する民間サービスなどでの利用も想定されています。また、「大規模オンラインプラットフォームでは、ユーザからの要請に従ってEUDIWによる認証を受け入れなければならない」と定義されており、例えばAmazonのような大規模プラットフォーマーは、ユーザがEUDIWでの認証を望めば受け入れる必要があります。

コンセプト

EUDIWのアプリ上（図4）に、日本で言えばJPKI（公的個人認証サービス）のような認証要素を入れることができると考えられます。また、免許証情報や医師、弁護士などの資格情報などを用いて認証を行い特定のサービスを利用可能にすることが想定されています。ユーザが単独で、IDや属性情報の管理責任を持つことができるため、ログもセキュアな状態で管理されることになります。

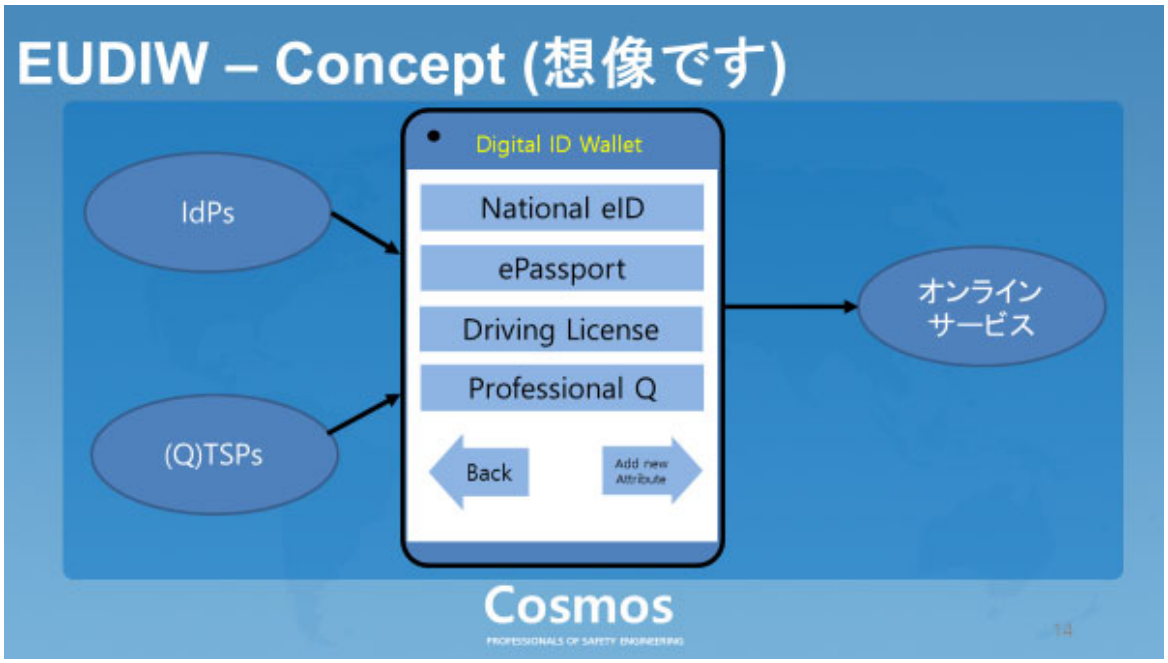

図4. EUDIW－コンセプト

改定案の内容　2）対象となるトラストサービスの拡充

これまでeIDAS1.0で定義されていた、電子署名のための証明書やタイムスタンプ、eシールの保存、Webサイト認証等に加え以下５つのトラストサービスが新たに定義されました。

電子アーカイブ

QTSPのみが適格サービスの提供が可能で、保存期間中は電子データまたは文書の完全性、出所の正確性、法的特性を保証するために電子データまたは文書の受領、保存、削除、送信を保証するサービスを指します。

電子台帳（分散台帳、ブロックチェーン）

電子台帳の法的効果を承認するとともに、適格電子台帳であれば含まれるデータの一意性および真正性の推定を享受でき、台帳内で時系列的な順序付けの推定を受けることができるとしています。

属性の電子証明

属性の認証を許可する電子形式の証明を意味するもので、付属書Vを満たすことが条件となっています。付属書Ｖはeシールや電子署名のための適格証明書の要件と酷似した内容となっており、適格電子属性証明は紙媒体で発行された証明書と同等の法的効力を有すると定められています。

適格電子属性証明に含む必要がある情報

適格電子属性証明に含む必要がある情報としては以下のようなものがあります。

1. 住所（Address）
2. 年齢（Age）
3. 性別（Gender）
4. 民法上の身分（Civil status）
5. 家族構成（Family composition）
6. 国籍（Nationality）
7. 資格（Educational qualifications, titles and licenses）
8. 専門的な資格、許可（Professional qualifications, titles and licenses）
9. 公的な資格、許可（Public permits and licenses）
10. 財政情報（Financial and company data）

リモート(Q)SCD管理（リモート署名・シール）

適格電子署名（シール）に関しては、QTSPがサービスを提供することとされています。QSCDの認証の有効期限は5年、ただし2年ごとの脆弱性評価が条件となっています。

改定案の内容　3）ブラウザ対応

第45条において、ブラウザは、QWAC（認定Web認証用証明書）を認識しなければならないと新たに明記されました。

改定案の内容　4）下位規則の整備

eIDAS1.0では、法的要件等の明確化に対して下位規則を定めたうえで技術基準等を参照していますが、残念ながらすべての要件に対する下位規則は定められていませんでした。しかし今回のeIDAS 2.0では、欧州委員会は法律によって下位規則を整備しなければならないと定められ（図5）、欧州のQTSPにも朗報となっています。ただし示された整備基準一覧の中でも唯一、「電子台帳の基準」に関しては下位規則の整備が義務付けられておらず、トラストサービスとして規定に盛り込んだものの欧州委員会は１～２年以内の整備は難しいと判断したものと考えられます。

図5. 下位規則の整備

以上

株式会社コスモス・コーポレイション　取締役　ITセキュリティ部責任者
（JIPDEC　客員研究員）　濱口　総志 氏

・2007年4月 コスモス・コーポレイションに入社。
・2008年9月よりドイツTUEV Nord AGグループにて1年3ヶ月間の研修を受講。
TUEV Informationstechnik GmbHではCommon Criteria評価に従事。
・2011年4月よりTUEV Informationstechnik GmbHの日本現地パートナーとして、認証局・タイムスタンプ局のマネジメントシステムの認定業務、セミナー、調査等を担当。
・2013年4月よりJIPDEC客員研究員として、JCAN証明書の普及に関する業務に携わる。

本内容は、2021年7月13日に開催されたJIPDECセミナー「デジタル社会を支えるトラスト基盤の構築」講演内容を取りまとめたものです。