



eIDAS規則の概要と EUにおける属性認証について

2016/03/09

株式会社コスモス・コーポレイション

ITセキュリティ部 濱口 総志



自己紹介

株式会社コスモス・コーポレーション

製品安全／EMC／医療機器評価・認証

TUViT GmbHの日本代理店

ETSI認証／データセンタ監査／コモンクライテリア評価／調査

一般財団法人 日本情報経済社会推進協会

客員研究員

東京工科大学 手塚 悟 研究室



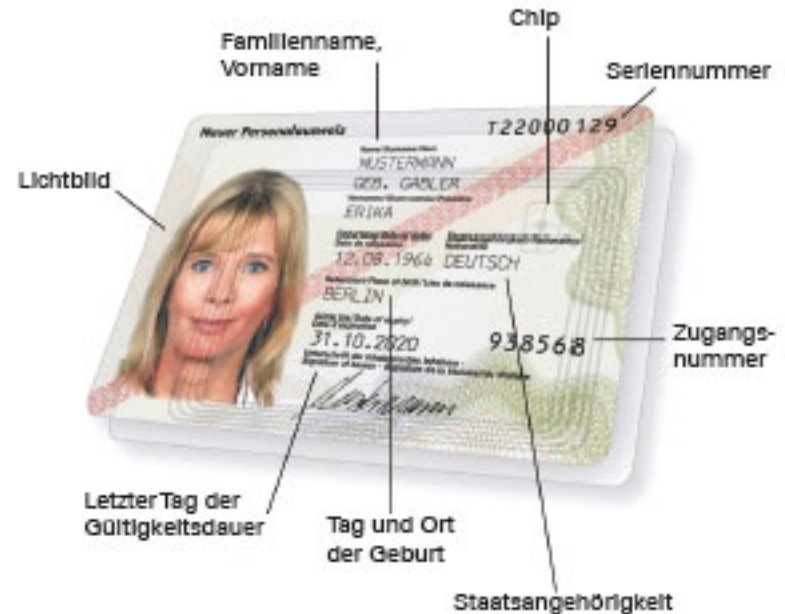
電子署名指令とeIDAS規則

	電子署名指令	eIDAS規則
目的	<p>電子署名の利用促進と、法的承認への寄与</p> <p>特定認証サービスに関する法的枠組みを構築することで、EU域内市場の適切な機能を確保</p>	<p>eIDとトラストサービスの適切なセキュリティレベルの実現による域内市場の適切な機能を保証</p> <p>eIDの相互認証の為の条件を定め、また、トラストサービスの法的枠組みを確立する</p>
範囲	電子署名	eID及びTS(電子署名、eシール、タイムスタンプ、eデリバリ、検証サービス、長期保存、WEB認証)
効力	指令に基づいて加盟国が法整備	加盟国に直接適応

eID＝オンラインで本人確認を実現する機能（e.g ドイツ新国民IDカード（Der Neue Personalausweis）のeID機能）

- eIDの保証レベル

- Low
- Substantial
- High
 - 詳細はIR 2015/1502



出典 Bundesministerium des innern

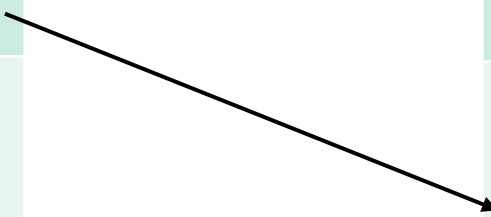


eIDの相互承認の条件 (例)



スキーム	LoA
eID	High
公共サービスが求める 認証の保証 レベル	High

スキーム	LoA
eID	Substantial
公共サービスが求める 認証の保証 レベル	Substantial





「トラストサービス」とは、下記により構成される、通常は報酬の為に提供される電子サービスをいう：

1. 電子署名、電子シール、又は電子タイムスタンプ、電子登録配布サービス及びこれらのサービスに関連する証明書の生成、検証、照合、または、
2. ウェブサイト認証の為に証明書の生成、検証、照合；または、
3. これらのサービスに関連する電子署名、シール、又は証明書の保存；



電子署名とeシール

	電子署名	eシール
定義	<p>「電子署名」と、電子データに添付されている又は論理的に関係している電子形式のデータであり、署名者が署名として使うものをいう</p> <p>*署名者=自然人(定義9参照)</p>	<p>「電子シール」とは、電子データに添付又は論理的に関係している電子形式のデータであり、元の電子データの起源と完全性を保証するものをいう</p> <p>eシール生成者=法人</p>
法的効力	<p>適格電子署名＝手書き署名と同等</p> <p>適格以外の電子署名：適格証明書を使用しない電子署名の法的有効性は否定されない。適格証明書を使用した電子署名は手書き署名と同等とみなす</p>	<p>適格eシール：リンクするデータの完全性及び起源の正確性の推定を享有できる。</p> <p>適格以外のeシール：eシールは、その法的効力及び法的手続きにおける証拠としての能力を、それが電子形式である、又は適格eシールの要求事項を満たさないという理由だけで否定されるものではない</p>
証明書の定義	<p>「電子署名証明書」とは、電子署名検証データと自然人を関連付け、少なくともその人物氏名、又は仮名を確認する電子証明書をいう</p>	<p>「電子シール証明書」とは、電子シール検証データと法人を関連付け、その法人名称を確認する電子証明書をいう</p>



法的有効性について

eIDAS規則では、電子署名の法的有効性について、手書き署名と同等と規定している。

手書き署名の法的有効性や、実際（電子でない）のシールの法的有効性は、加盟国の国内法に依存する。

以下はeIDAS規則の和訳

序文(49): 本規則は、電子署名が、電子形式であること、あるいは適格電子署名の要求を満たしていないことが理由で法的効果を拒否されるべきではないという原則を確立する。ただし、**適格電子署名が自筆署名と同等の法的効力をもたせるべきであるという本規則で規定される要求事項を除き、電子署名の法的効果を定義するのは国内法である。**

序文(59): 電子シールは電子文書が法人により発行されたことの証拠となり、文書の発行元と完全性を保証するものである。



- 法人の文書
 - 請求書、ホワイトペーパー、テストレポート、
- ソフトウェアコード、サーバ
 - パッチファイル、アップデート
- ログファイル等
- デバイスorアプリケーション
 - カメラ、医療機器、スマホ上のアプリケーション等



電子登録配送サービス (e Registered Delivery)

<定義>

「電子登録配布サービス」とは、電子手段により第三者間でデータを送信することを可能にし、データの送受信の証拠を含む送信されたデータの取扱に関する証拠を提供し、送信されたデータの損失、破損や窃盗、損害、又は不正な変更のリスクから守るものをいう;

<法的有効性>

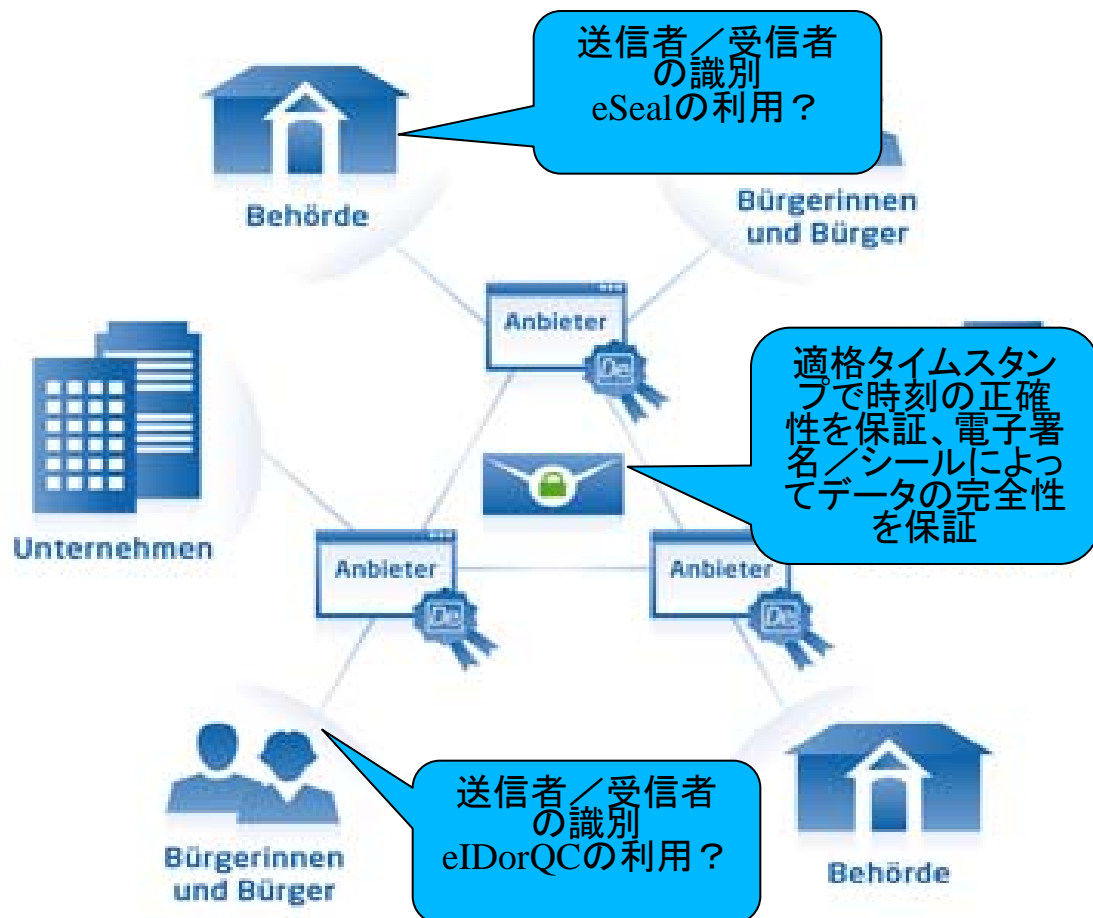
適格電子登録配布サービスを利用して送受信されたデータは、識別された送信者により送信され、識別されたデータの宛先で受信されるデータの完全性と、適格電子登録配布サービスで示されたデータの送受信の日時の正確性を、法的に推定することが出来るものとする。

送受信者の識別＋データの完全性、送受信日時の正確性を保証

誰が、何を何時送り、誰が何を何時受信したか



e.g. De-Mail



ドイツでは2011年5月にDe-Mail法(De-Mail Act)が発効され政府機関と市民や民間企業間のセキュアな電子通信の要求事項が定められた

現在、ドイツ連邦情セキュリティ庁(BSI)よりDe-Mailサービス事業者としての認定を受けサービスを提供している事業者は、1&1 De-Mail GmbH, Mentana Claimsoft GmbH, T-systems International GmbH及びTelecom Deutschland GmbHの4社である。

出典 Bundesministerium des innern

Timeline

2014

2015

2016

2017

2018

2019

17.09.2014
**Entry into
force of the
eIDAS
Regulation**

eID

29/09/2015
Voluntary cross-border recognition

29/09/2018
**Mandatory cross-
border recognition**

**Trust
services**

**eSignature Directive
rules**

1.07.2016
**Date of application of eIDAS rules for trust
services**

出典: 6th TSP Compliance Info-Day



第28条(第38条、eシール)

3. 電子署名の(eシール)適格証明書は、非強制の追加の特定の属性を含むことができる。この属性は、適格電子署名の相互運用性や承認に影響しないこと。



(2) At an applicant's request the certification authority shall include in the signature key **certificate or an attribute certificate** information relating to **his authority to represent a third party** and to **his professional admission to practice or other type of admission** insofar as reliable proof is furnished of the consent by the third party to the inclusion of the authority of representation or of the admission.



独 Elektronischer Heilberufsausweis(eHBA) (electronic Health Professional Card)

- Medisign GmbH(ドイツのQTSP)が医師の電子身分証(eHBA)を発行
 - e-Apothekerausweis(薬剤師)
 - e-Arzttausweis(医師)
 - e-Zahnarzttausweis(歯科医師)
 - e-Psychotherapeutenausweis(心理療法士)
 - eHBAの機能
 - 電子処方箋
 - 電子医療記録
 - 電子健康カードへの書き込み
 - 適格証明書を格納
- 医師等の資格情報は各医師会(Kammer)に依拠する。Kammer = 協会



- Bundesnotarkammer
 - 適格証明書、タイムスタンプ
 - 署名カードの発行
 - 公証人、廷吏 (Bailiffs)、弁護士
 - 公証人会、弁護士会、裁判所に属性の確認