日欧電子署名の法制度の比較

2017年7月4日@日欧インターネットトラストシンポジウム

株式会社コスモス・コーポレイション　濱口　総志

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

eIDAS規則と電子署名法

eIDAS規則における電子署名の定義

eIDAS規則
第３条(10)(11)(12)
「電子署名」とは、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、署名者が署名する為に使用するものをいう
「先進電子署名」とは、第26条で規定される要求事項に適合する電子署名をいう
「適格電子署名」とは、適格電子署名生成装置を利用して生成され、電子署名の為の適格証明書に順ずる先進電子署名をいう

先進電子署名（26条）

署名者に一意的にリンクしている；

署名者を識別することができる；

署名者が、本人単独の管理のもとに、高いレベルの信頼を持って使用することができる電子署名生成データを使って作成されている；

その後のデータへの変更を検知できる方法で署名されたデータにリンクされている。
➡ PKIベースの電子署名

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

eIDAS規則と電子署名法

適格電子証明書

eIDAS規則　第3条　（15）
「電子署名の為の適格証明書」とは、適格トラストサービスプロバイダによって発行され、付属書Ⅰの要求事項を満たす電子署名証明書をいう；

適格トラストサービスプロバイダ
➡設備、本人確認方法及び運営が
eIDAS規則に適合していると監督機関（国）からお墨付きを得ている事業者

eIDAS規則と電子署名法

eIDAS規則における電子署名の定義

eIDAS規則
第３条(10)(11)(12)
「電子署名」
➡電子形式の署名

「先進電子署名」
➡PKIベースの電子署名（デジタル署名）で基準（ETSI規格）を満たすもの

「適格電子署名」
➡適格電子証明書とICカードのような安全な装置を用いた先進電子署名

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

eIDAS規則と電子署名法

日本における電子署名の定義

電子署名及び認証業務に関する法律

第二条

この法律において「電子署名」とは、電磁的記録（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。以下同じ。）に記録することができる情報について行われる措置であって、次の要件のいずれにも該当するものをいう。

一　当該情報が当該措置を行った者の作成に係るものであることを示すためのものであること。

二　当該情報について改変が行われていないかどうかを確認することができるものであること。

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

eIDAS規則と電子署名法

電子署名法における特定認証業務

第二条

2　この法律において「認証業務」とは、自らが行う電子署名についてその業務を利用する者（以下「利用者」という。）その他の者の求めに応じ、当該利用者が電子署名を行ったものであることを確認するために用いられる事項が当該利用者に係るものであることを証明する業務をいう。

3　この法律において「特定認証業務」とは、電子署名のうち、その方式に応じて本人だけが行うことができるものとして主務省令で定める基準に適合するものについて行われる認証業務をいう。

＊PKIベース

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

eIDAS規則と電子署名法

電子署名法における認定認証業務

第四条

特定認証業務を行おうとする者は、主務大臣の認定を受けることができる。

（認定の基準）

一　申請に係る業務の用に供する設備が主務省令で定める基準に適合するものであること。

二　申請に係る業務における利用者の真偽の確認が主務省令で定める方法により行われるものであること。

三　前号に掲げるもののほか、申請に係る業務が主務省令で定める基準に適合する方法により行われるものであること。

認証業務

➡電子署名が署名者によって行われたことを証明するサービス

特定認証業務

➡認証業務の内、PKIベースのサービスで基準（関係指針）を満たすもの

認定認証業務

➡特定認証業務について、主務大臣の認定を受けたサービス

Cosmos

POFESSIONALS OF SAFETY ENGINEERING

eIDAS規則と電子署名法

電子署名の法的効力

eIDAS規則
第25条
電子署名は、それが電子形式である、又は適格電子署名の要求事項を満たさないという理由だけで、法的効力及び法的手続きにおける証拠としての能力を否定されないこと。

適格電子署名は、手書き署名と同等の法的効力をもつこと。

電子署名及び認証業務に関する法律
第三条
電磁的記録であって情報を表すために作成されたもの（公務員が職務上作成したものを除く。）は、当該電磁的記録に記録された情報について本人による電子署名（これを行うために必要な符号及び物件を適正に管理することにより、本人だけが行うことができることとなるものに限る。）が行われているときは、真正に成立したものと推定する。

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

日欧電子署名の定義の比較

EU

適格電子署名
➡適格証明書＋適格署名生成装置
＋先進電子署名

先進電子署名
➡PKIベースの電子署名
（デジタル署名）で基準
（ETSI規格）を満たすもの

電子署名
➡電子形式の署名

日本

認定認証業務で発行される電子証明書に基づいた電子署名

特定認証業務で発行される電子証明書に基づいた電子署名

電子署名
➡電子形式の署名

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

製品評価制度

eIDAS規則対応の為の製品評価

HSM及び適格電子署名生成装置
➡CC EAL4+及びProtection Profile
　＊FIPS 140-2?

コモンクライテリア評価／認証の課題
➡CCRAの相互承認はEAL2まで

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

認定制度の比較

適格トラストサービスプロバイダ
➡24ヶ月毎の認定と認定更新
➡認定基準：ETSI EN規格及びeIDAS規則
➡認定結果はトラストリストによって公開

認定認証事業者
➡1年毎の認定更新
➡認定基準:施行規則／指針
➡認定結果は官報によって公開

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

監督制度

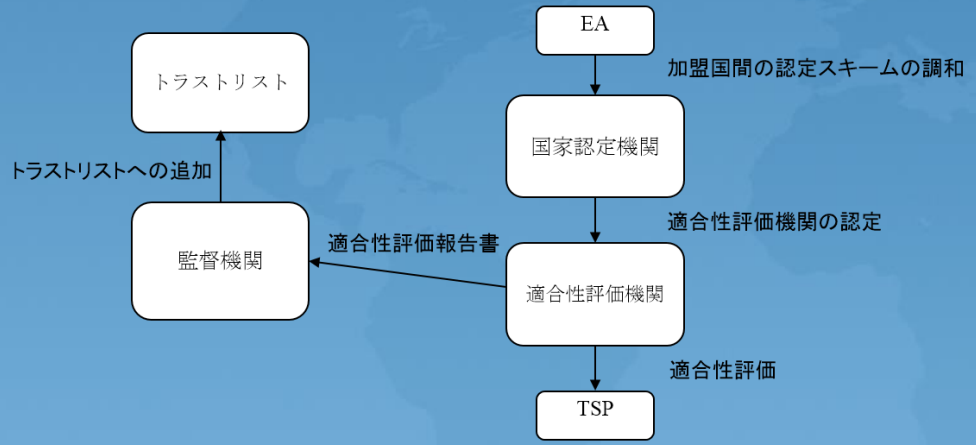
トラストサービスプロバイダの監督

適格トラストサービスプロバイダ≒認定認証事業者

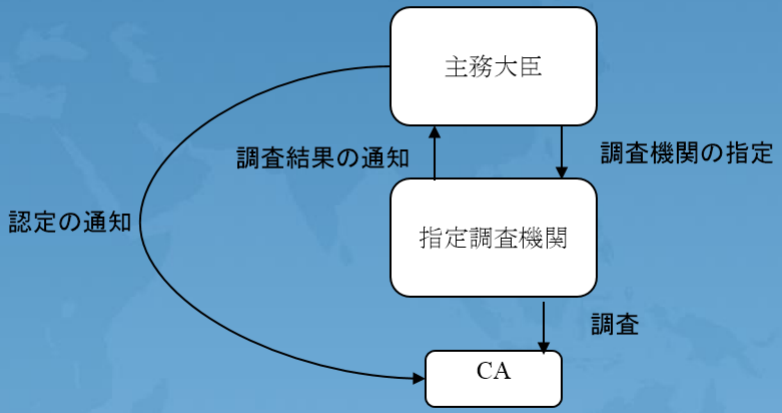
EUでは適格でないトラストサービスプロバイダも監督対象

認定制度の比較

EU



日本



Cosmos
POFESSIONALS OF SAFETY ENGINEERING

認定基準の比較

EN 319 401, 411-1,-2と施行規則／指針の要求比較

EN 319 411-1,2	施行規則	指針
5 認証業務運用規定及び証明書ポリシーに関する一般規定		
6 トラストサービスプロバイダの運用	1. 業務の用に供する設備の基準	1.1 認証設備室への入出場を管理するために必要な措置
6.1 公開及び保管の責任	2 利用者の真偽の確認の方法	1.2 認証業務用設備への不正なアクセス等を防止するために必要な措置
6.2 識別及び認証	3 その他の業務の方法	1.3 正当な権限を有しない者による認証業務用設備の作動を防止するための措置等
6.3 証明書のライフサイクル運用要件	4 帳簿書類	1.4 発行者署名符号の生成管理に使用する暗号装置
6.4 施設、管理、及び運用管理		1.5 認証業務用設備等の災害の被害を防止するために必要な措置
6.5 技術的セキュリティマネジメント		
6.6 証明書、CRL、及びOSCPプロファイル		2.1 認証業務の利用申込み等
6.7 適合性の監査及びその他の評価		2.2 利用者の真偽の確認方法等
6.8 その他の事業及び法的事項		
6.9 その他の規定		3.1 利用申込者に対する説明事項
		3.2 利用申込書等の記載事項等
		3.3 利用者署名符号及び利用者識別符号の生成等
		3.4 電子証明書に係る事項
		3.5 認定認証業務と他の業務との誤認を防止するための措置
EN 319 401		3.6 電子証明書への属性の記録
5 リスクアセスメント		3.7 署名検証者への情報提供
6 ポリシー及び運用		3.8 電子証明書の失効に係る事項
6.1 トラストサービス運用規定		3.9 認証業務の実施に関する規程
6.2 契約条件		3.10 認証業務の廃止
6.3 情報セキュリティポリシー		3.11 電子証明書名義人への情報の開示
7 TSPの管理及び運営		3.12 認証業務実施のための組織及び体制等
7.1 内部組織		3.13 認証業務用設備の操作等に関する許諾等
7.2 人的資源		3.14 発行者署名符号の漏えいを防止するために必要な措置
7.3 資産管理		
7.4 アクセスコントロール		4.1 認証業務利用申込に関する帳簿書類関係
7.5 暗号管理		4.2 電子証明書の失効に関する帳簿書類関係
7.6 物理および環境セキュリティ		4.3 認証事業者の組織管理に関する帳簿書類関係
7.7 運用セキュリティ		4.4 設備及び安全対策措置に関する帳簿書類関係
7.8 ネットワークセキュリティ		
7.9 インシデント管理		
7.10 証拠の収集		
7.11 事業継続マネジメント		
7.12 TSPの終了および終了計画		
7.13 コンプライアンス		

認定基準の比較

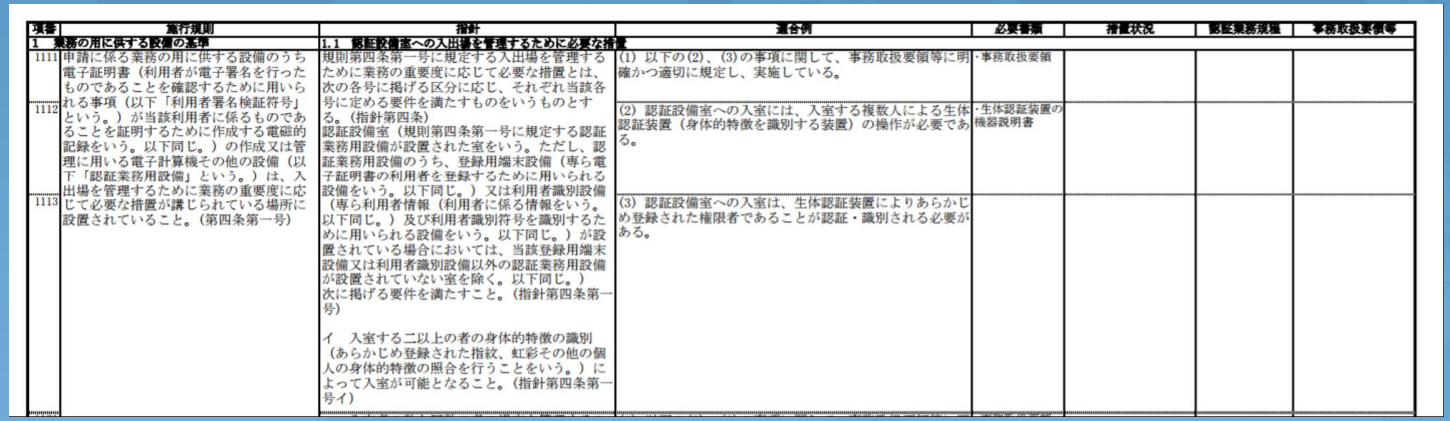
ETSI EN規格の特徴

- マネジメントシステムベース（27002）
  - リスクアセスメント
  - プロセスのデモンストレーション
- 財務上の要求
- 要員のバックグラウンドチェック
- 懲罰
- 廃局時の要求
- CA/Bフォーラムの要求

認定基準の比較

施行規則／指針の特徴

- 適合例の明示



項番	施行規則	指針	適合例	必要書類	措置状況	認証業務規程	事務取扱要領等
1	業務の用に供する設備の基準	1.1 認証設備室への入出場を管理するために必要な措置					
1111	申請に係る業務の用に供する設備のうち電子証明書（利用者が電子署名を行ったものであることを確認するために用いられる事項（以下「利用者署名検証符号」という。）が当該利用者に係るものであることを証明するために作成する電磁的記録をいう。以下同じ。）の作成又は管理に用いる電子計算機その他の設備（以下「認証業務用設備」という。）は、入出場を管理するために業務の重要度に応じて必要な措置が講じられている場所に設置されていること。（第四条第一号）	規則第四条第一号に規定する入出場を管理するために業務の重要度に応じて必要な措置とは、次の各号に掲げる区分に応じ、それぞれ当該各号に定める要件を満たすものをいうものとする。（指針第四条） 認証設備室（規則第四条第一号に規定する認証業務用設備が設置された室をいう。ただし、認証業務用設備のうち、登録用端末設備（専ら電子証明書の利用者を登録するために用いられる設備をいう。以下同じ。）又は利用者識別設備（専ら利用者情報（利用者に係る情報をいう。以下同じ。）及び利用者識別符号を識別するために用いられる設備をいう。以下同じ。）が設置されている場合においては、当該登録用端末設備又は利用者識別設備以外の認証業務用設備が設置されていない室を除く。以下同じ。） 次に掲げる要件を満たすこと。（指針第四条第一号） イ　入室する二以上の者の身体的特徴の識別（あらかじめ登録された指紋、虹彩その他の個人の身体的特徴の照合を行うことをいう。）によって入室が可能となること。（指針第四条第一号イ）	(1) 以下の(2)、(3)の事項に関して、事務取扱要領等に明確かつ適切に規定し、実施している。	・事務取扱要領			
1112			(2) 認証設備室への入室には、入室する複数人による生体認証装置（身体的特徴を識別する装置）の操作が必要である。	・生体認証装置の機器説明書			
1113			(3) 認証設備室への入室は、生体認証装置によりあらかじめ登録された権限者であることが認証・識別される必要がある。				

- 暗号モジュールに対する詳細な要求
- サンプルチェック

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

まとめ

日欧電子署名の法制度のギャップ

1．適格電子署名生成装置
EUでは適格電署名には適格電子署名生成装置の利用が必須
日本では、鍵管理は、署名者の自己責任
➡リモート署名の可能性
便利だけでなく、よりセキュアに

2. HSM及び署名生成装置の製品評価

3．トラストリスト
複数の制度間の相互運用／承認の為のトラストリスト或はブリッジ認証局

4．認定基準のギャップ
文化の違い、IETF RFC3647との整合性

5．タイムスタンプ等の他のトラストサービス

Cosmos
POFESSIONALS OF SAFETY ENGINEERING

ご清聴ありがとうございました

ご質問等御座いましたら、

コスモス・コーポレイション
ITセキュリティ課
濱口 総志
s.hamaguchi@cosmos-corp.com
までご連絡ください。

Cosmos
POFESSIONALS OF SAFETY ENGINEERING