資料６－２

EUにおけるeシールの基準

株式会社コスモス・コーポレイション
濱口　総志

Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

eIDAS規則におけるeシール

Article 3 定義

'electronic seal' means data in electronic form, which is attached to or logica
lly associated w
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添付又は論理的に関係している電子形式のデータをいう;

'advanced electronic seal' means an electronic seal, which meets the require
ments set out

「先進eシール」とは、第36条で規定する要件を満たすeシールをいう:

'qualified electronic seal' means an advanced electronic seal, which is create
d by a qualifie
ied certificate

「適格eシール」とは、適格eシール生成装置を利用して生成され、eシールの適格証明書に準ずる先進eシールをいう

適格eシール = 先進eシール + 適格証明書 + 適格eシール生成装置

Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

*eIDAS reg. Art. 3 定義 (27)

適格eシール ＝ 先進eシール ＋ 適格証明書 ＋ 適格eシール生成装置

先進eシール

eIDAS reg. Art. 36 先進eシールの要件

eIDAS reg. Art. 37 公的セクターにおけるeシール

委員会実施決定 2015/1506
AdESフォーマット
- ETSI TS 103171(XAdESベースラインプロファイル),
- ETSI TS 103173(CAdESベースラインプロファイル),
- ETSI TS 103172(PAdESベースラインプロファイル),
- ETSI TS 103174(ASiCベースラインプロファイル)

適格証明書

eIDAS reg. Art. 38 eシールの為の適格証明書

eIDAS reg. Annex III eシールの為の適格証明書に対する要件

ETSI EN 319421 適格証明書プロファイル

適格トラストサービスプロバイダが適格証明書を発行する（eIDAS Reg. Art.3）

適格トラストサービスプロバイダ

eIDAS reg. Art. 19 トラストサービスプロバイダに適用されるセキュリティ要件

監督（eIDAS Reg. Art. 20）

適合性評価機関が適格トラストサービスプロバイダを監査(eIDAS reg. Art. 20)
- ETSI EN 319 401 (一般ポリシー要件)
- ETSI EN 319 411-1 (認証局のポリシー要件)
- ETSI EN 319 411-2 (適格証明書を発行する認証局のポリシー要件)

監督機関

eIDAS reg. Art. 17 監督機関

適合性評価機関

Reg. (EC) No 765 /2008 Art. 2

認定機関が適合性評価機関を認定する (Reg. (EC) No765/2008 Art. 3)
- ETSI EN 319 403
- ISO/IEC 17065

認定機関

Reg. (EC) No 765 /2008 Art. 4

適格eシール生成装置

eIDAS reg. Art. 39 適格eシール生成装置

eIDAS reg. Annex II 適格eシール生成装置の要件

適切な機関が適格電子署名生成装置を認証する(eIDAS reg. Art. 30)
委員会実施決定 2016/650
- ISO/IEC 15408
- EN 419 211 (Protection Profiles)

適切な機関

eIDAS reg. Art. 30 適格電子署名生成装置の認証

加盟国は適切な機関を指定する（eIDAS reg. Art. 30）

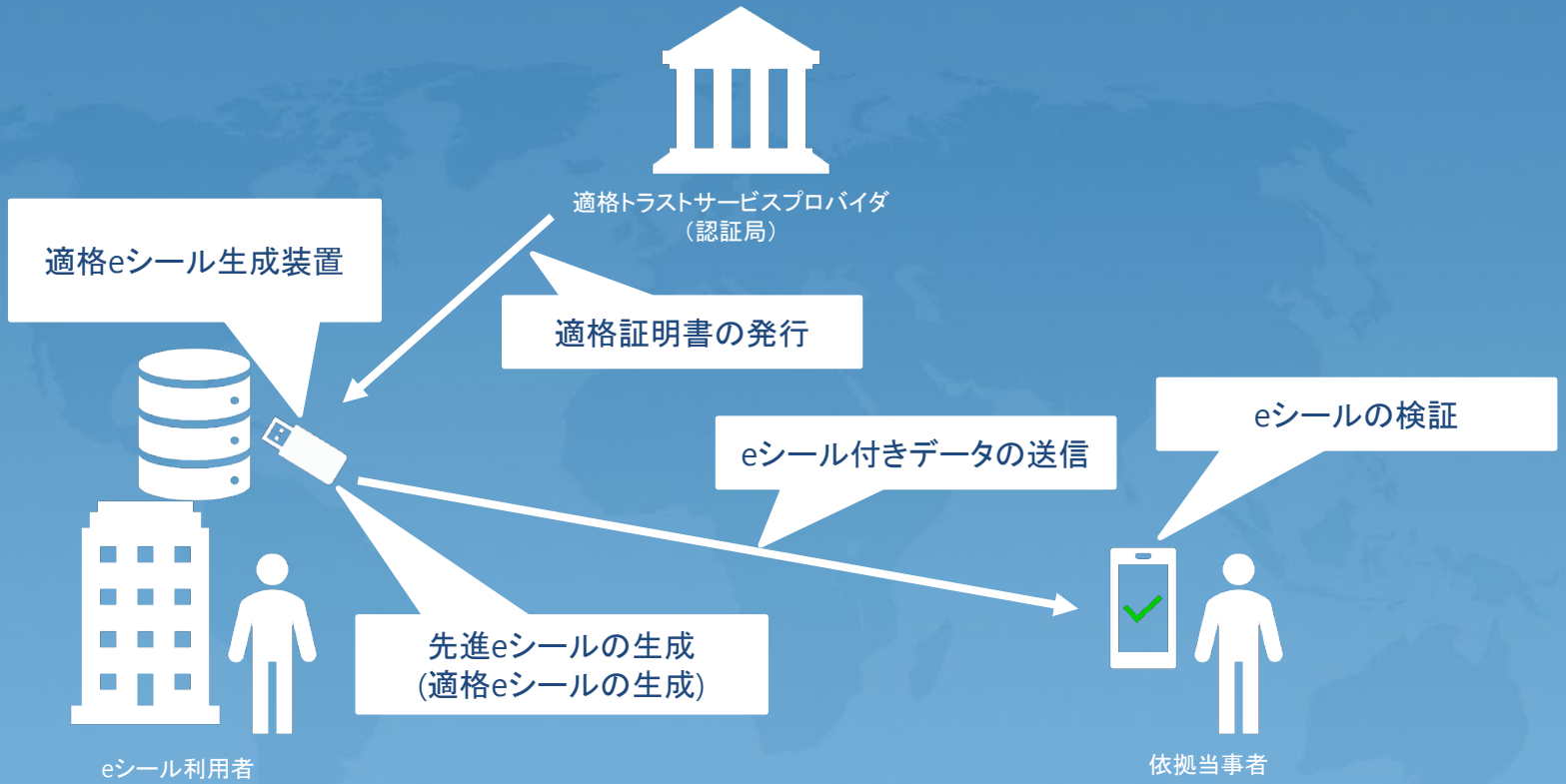
加盟国

eIDAS reg. Art. 31 認証された適格電子署名生成装置リストの公開

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

*eIDAS reg. Art. 3 定義 (27)

適格eシール ＝ 先進eシール ＋ 適格証明書 ＋ 適格eシール生成装置



Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

先進eシール（Advanced Electronic Seal）

先進eシール

eIDAS reg. Art. 36 先進eシールの要件

eIDAS reg. Art. 37 公的セクターにおけるeシール

委員会実施決定 2015/1506
AdESフォーマット
- ETSI TS 103171(XAdESベースラインプロファイル),
- ETSI TS 103173(CAdESベースラインプロファイル),
- ETSI TS 103172(PAdESベースラインプロファイル),
- ETSI TS 103174(ASiCベースラインプロファイル)

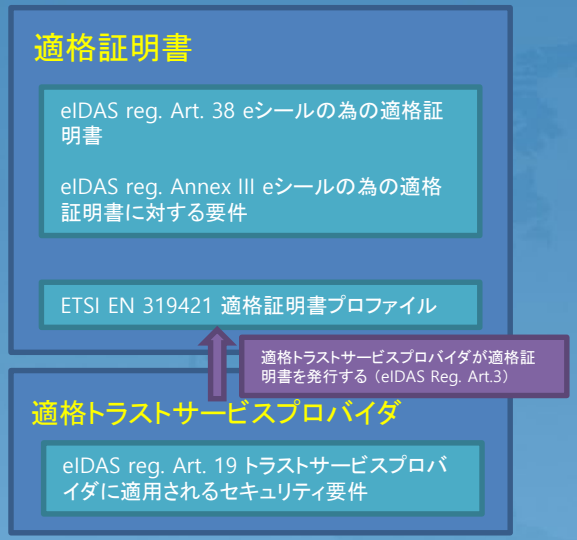
36条　先進eシールの要件

(a)シール生成者に一意にリンクしている
(b)シールの生成者を識別できる
(c)シールの生成者が本人による管理のもとに、高いレベルの信頼を持って、eシール生成に使用することができる、eシール生成データを使って生成されている
(d)改ざん検知が可能である

37条　公的セクターにおけるeシール

-加盟国が公的セクターにおいて先進eシールを要求する場合、実施法で定められるフォーマットの先進eシール、適格証明書に基づく先進eシール及び適格eシールを認めること
-適格証明書に基づく先進eシールを要求する場合、実施法で定められるフォーマットの適格証明書に基づく先進eシール及び適格eシールを認めること
-適格eシール以上のeシールを要求しないこと

eシールの適格証明書



eIDAS Annex III（欧州特有の要件のみ抜粋）
-適格証明書であることの識別子(QC Statement)
-eシール生成者の情報（名称と公的な登録番号）
-適格eシール生成装置の利用を示す情報

ETSI EN 319421
-証明書のSubject
CountryName, organizationName(公的記録に紐づく完全な名称), organizationIdentifier, commonName(通称)
-organizationIdentifier
XXXYY-ZZZZZZZZZ

項目	
XXX	どのスキームの法人番号であるかを示す情報(VAT, NTR, LEI, PSD等)、ローカルスキームの場合2文字+:(XX:)
YY	国コード（ISO3166）, LEIの場合XGとする
ZZZZZ	識別番号
例	VATBE-0876866142, NTRJP-8190001006631

Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

eシールの適格証明書

適格証明書

eIDAS reg. Art. 38 eシールの為の適格証明書

eIDAS reg. Annex III eシールの為の適格証明書に対する要件

ETSI EN 319421 適格証明書プロファイル

適格トラストサービスプロバイダが適格証明書を発行する（eIDAS Reg. Art.3）

適格トラストサービスプロバイダ

eIDAS reg. Art. 19 トラストサービスプロバイダに適用されるセキュリティ要件

フィールド名	値（サンプル）
バージョン	V3
シリアルナンバー	WWWWWWWWW
署名アルゴリズム	sha256RSA/sha512RSA
署名ハッシュアルゴリズム	sha256/sha512
発行者	QCA XXXX
有効期限の開始時刻	Monday, January 5, 2020 5:00:00 PM
有効期限の終了時刻	Thursday, January 5, 2020 5:00:00 PM
サブジェクト	CN = Cosmos Corporation O = Cosmos Corporation OID = NTRJP-8190001006631
公開鍵	RSA (2048bit)
公開鍵パラメータ	05 00
認証機関アクセス情報	[1]CA証明書のURL [2]OCSPのURL
サブジェクト鍵識別子	YYYYYYYYYY
QCステートメント	id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD. id-etsi-qct-eseal
証明書ポリシー	[1]0.4.0.194112.1.1/0.4.0.194112.1.3 [2] http://xxxxxxxxxxxxxx

その他の属性情報を証明書に記載することも認められている。（eIDAS reg. Art. 38）
正し、適格トラストサービスプロバイダ（認証局）はその属性情報を確認しなければならず、また、追加の属性情報についてはeIDAS規則が定める加盟国間の相互承認の範囲外となる。

eシールの適格証明書

適格証明書

eIDAS reg. Art. 38 eシールの為の適格証明書

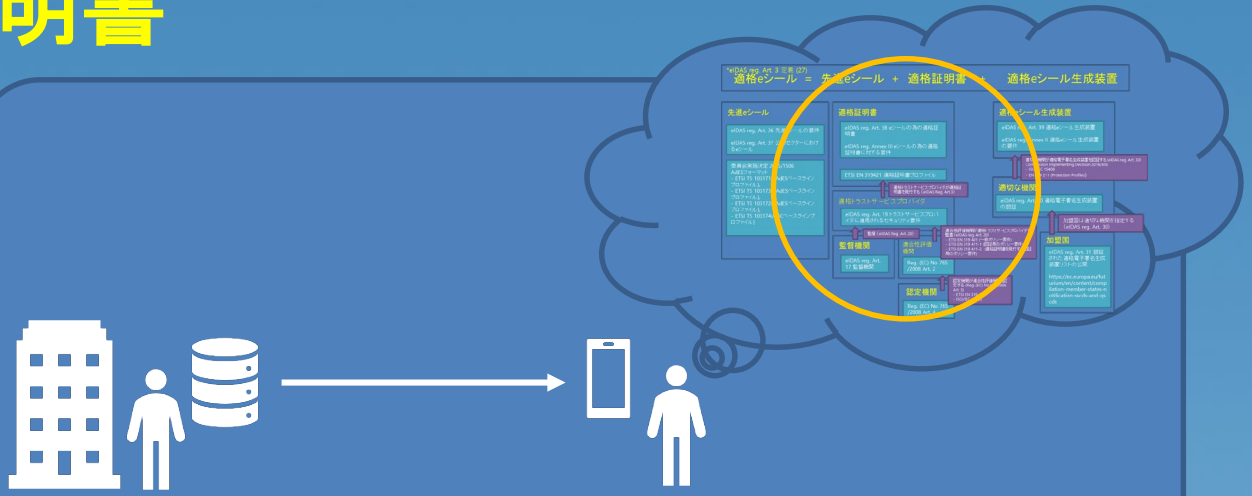
eIDAS reg. Annex III eシールの為の適格証明書に対する要件

ETSI EN 319421 適格証明書プロファイル

適格トラストサービスプロバイダが適格証明書を発行する（eIDAS Reg. Art.3）

適格トラストサービスプロバイダ

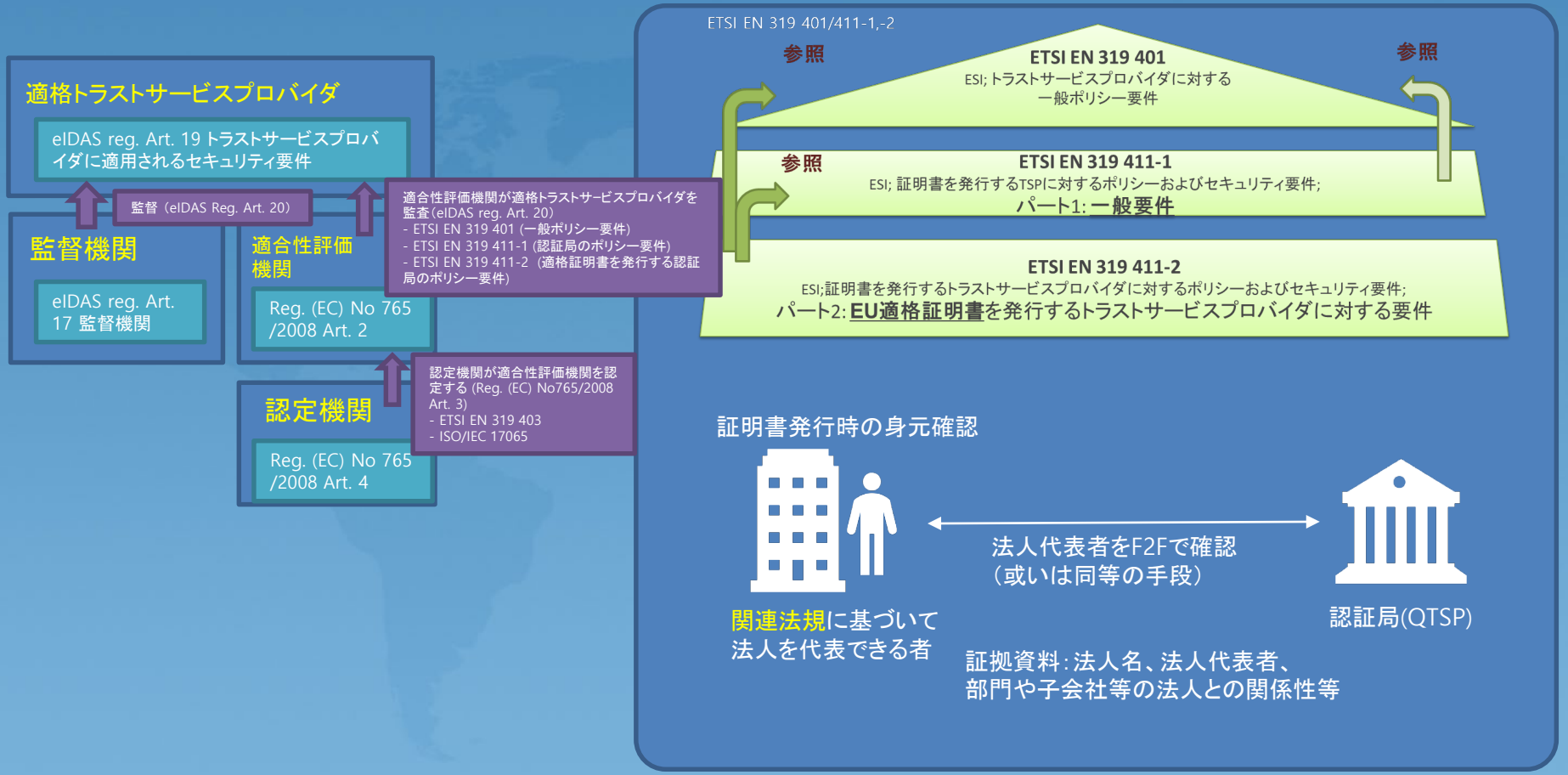
eIDAS reg. Art. 19 トラストサービスプロバイダに適用されるセキュリティ要件



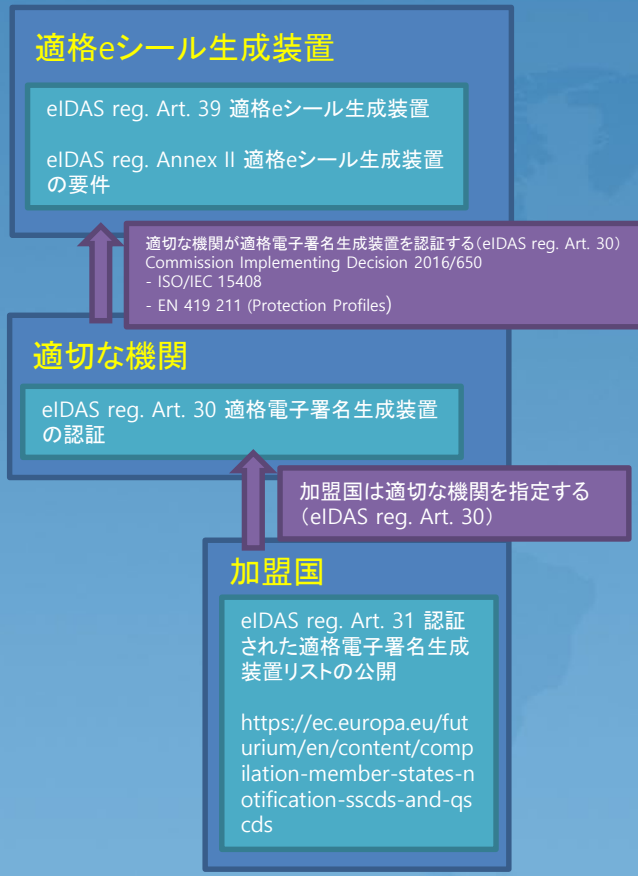
eシール付きデータの受信者はeシールをトラステッドリストと合わせて検証することで、eシールが適格eシールの条件を満たしていることが自動的に判別できる。

- 先進eシールであるか ➡ デジタル署名の検証
- eシール用の適格証明書であるか ➡ id-etsi-qcs-QcCompliance / id-etsi-qct-eseal
- 適格証明書が適格トラストサービスプロバイダから発行されているか
  ➡ 発行者をトラステッドリストで検証
- 適格eシール生成装置が利用されているか ➡ id-etsi-qcs-QcSSCD

適格トラストサービスプロバイダ



適格eシール生成装置



- ISO/IEC 15408 コモンクライテリア

IT製品やシステムがセキュリティの観点で適切に設計され、正しく実装されていることを評価する為の国際規格。

セキュリティ評価のフレームワークであり、満たさなければならないセキュリティ要件そのものは規定していない。
世界20か国以上の政府調達基準として採用されている。

- プロテクションプロファイル

IT製品やシステムが満たすべき要求仕様を調達者の視点で定めたもの。

- 評価保証レベル(EAL)

セキュリティ保証要件のパッケージであり、EAL1～7の7段階ある。
保証要件＝実際の評価作業

https://www.ipa.go.jp/security/jisec/cc/documents/CCPART3V3.1R5-J1.0.pdf

適格eシール生成装置

適格eシール生成装置

eIDAS reg. Art. 39 適格eシール生成装置

eIDAS reg. Annex II 適格eシール生成装置の要件

適切な機関が適格電子署名生成装置を認証する(eIDAS reg. Art. 30)
Commission Implementing Decision 2016/650
- ISO/IEC 15408
- EN 419 211 (Protection Profiles)

適切な機関

eIDAS reg. Art. 30 適格電子署名生成装置の認証

加盟国は適切な機関を指定する(eIDAS reg. Art. 30)

加盟国

eIDAS reg. Art. 31 認証された適格電子署名生成装置リストの公開

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

EN 419 211 プロテクションプロファイル
EAL4+(AVA_VAN.5, ALC_DVS.2)

保証クラス	保証ファミリ	評価保証レベル別の保証コンポーネント						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
開発	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
ガイダンス文書	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
ライフサイクルサポート	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
セキュリティターゲット評価	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASE_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
テスト	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
脆弱性評定	AVA_VAN	1	2	2	3	4	5	5

https://www.ipa.go.jp/security/jisec/cc/documents/CCPART3V3.1R5-J1.0.pdf

適格eシール生成装置

EN 419 211 プロテクションプロファイル*
EAL4+(AVA_VAN.5, ALC_DVS.2)
セキュリティ機能

- 鍵生成／保護
- 暗号機能
- 鍵のエクスポート
- 認証機能(ユーザ、署名要求)
- データ保護(ハッシュ値)
- アクセスコントロール
- 監査証跡

*eIDAS reg. Art. 3 定義 (27)

適格eシール ＝ 先進eシール ＋ 適格証明書 ＋

日本の電子署名法では利用者の秘密鍵をセキュアな装置で運用する要件はない

特定認証業務に基づく電子署名と同等

先進eシール

eIDAS reg. Art. 36 先進eシールの要件

eIDAS reg. Art. 37 公的セクターにおけるeシール

委員会実施決定 2015/1506
AdESフォーマット
- ETSI TS 103171(XAdESベースラインプロファイル),
- ETSI TS 103173(CAdESベースラインプロファイル),
- ETSI TS 103172(PAdESベースラインプロファイル),
- ETSI TS 103174(ASiCベースラインプロファイル)

技術基準は整備されていない

適格証明書

eIDAS reg. Art. 38 eシールの為の適格証明書

eIDAS reg. Annex III eシールの為の適格証明書に対する要件

ETSI EN 319421 適格証明書プロファイル

適格トラストサービスプロバイダが適格証明書を発行する（eIDAS Reg. Art.3）

法人の確認方法については規定が必要

適格トラストサービスプロバイダ

eIDAS reg. Art. 19 トラストサービスプロバイダに適用されるセキュリティ要件

監督（eIDAS Reg. Art. 20）

適合性評価機関が適格トラストサービスプロバイダを監査（eIDAS reg. Art. 20）
- ETSI EN 319 401 (一般ポリシー要件)
- ETSI EN 319 411-1 (認証局のポリシー要件)
- ETSI EN 319 411-2 (適格証明書を発行する認証局のポリシー要件)

監督機関

eIDAS reg. Art. 17 監督機関

適合性評価機関

Reg. (EC) No 765 /2008 Art. 2

認定機関

Reg. (EC) No 765 /2008 Art. 4

認定機関が適合性評価機関を認定する (Reg. (EC) No765/2008 Art. 3)
- ETSI EN 319 403
- ISO/IEC 17065

適格eシール生成装置

eIDAS reg. Art. 39 適格eシール生成装置

eIDAS reg. Annex II 適格eシール生成装置の要件

適切な機関が適格電子署名生成装置を認証する（eIDAS reg. Art. 30）
Commission Implementing Decision 2016/650
- ISO/IEC 15408
- EN 419 211 (Protection Profiles)

適切な機関

eIDAS reg. Art. 30 適格電子署名生成装置の認証

加盟国は適切な機関を指定する（eIDAS reg. Art. 30）

加盟国

eIDAS reg. Art. 31 認証された適格電子署名生成装置リストの公開

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

電子署名法でカバーされている領域

ご清聴ありがとうございました

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
E-Mail：s.hamaguchi@cosmos-corp.com
http://www.safetyweb.co.jp/

Cosmos
PROFESSIONALS OF SAFETY ENGINEERING

補足資料

Assurance Class	Assurance Components	
ADV: Development	ADV_ARC	Security Architecture
	ADV_FSP	Functional Specification
	ADV_IMP	Implementation representation
	ADV_INT	TSF Internal
	ADV_TDS	TOE Design
AGD: Guidance	AGD_OPE	Operation Procedure
	AGD_PRE	Preparative Procedure
ALC: Life-Cycle Support	ALC_CMC	CM Capabilities
	ALC_CMS	CM Scope
	ALC_DEL	Delivery
	ALC_DVS	Development Security
	ALC_FLR	Flaw remediation
	ALC_LCD	Life-cycle definition
	ALC_TAT	Tools and Techniques
ASE: Security Target Evaluation	ASE_CCL	Conformance Claim
	ASE_ECD	Extended Component Definition
	ASE_INT	ST Introduction
	ASE_OBJ	Security Objectives
	ASE_REQ	Security Requirements
	ASE_SPD	Security Problem Definition
	ASE_TSS	TOE Summary Specification
ATE: Tests	ATE_COV	Coverage
	ATE_DPT	Depth
	ATE_FUN	Functional tests
	ATE_IND	Independent testing
AVA: Vulnerability Assessment	AVA_VAN	Vulnerability analysis