資料６－１

欧州適格eシールと日本版eシールの期待

総務省：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 第6回 資料

2020年11月6日(金)

GMOグローバルサイン株式会社
漆嶌 賢二

欧州のeシールとは

- 欧州eIDASの電子署名が「自然人」による署名であるのに対し「法人(や組織、部署等)」による原本保証
- 法人や組織による原本保証は、データ、文書、コード、メールなど従来からあるデジタル署名で、特に新しいものではない。

	電子署名	eシール	タイムスタンプ
発行主体	自然人	法人や組織	TSU (デバイス)
目的	自然人が電磁的に記録した情報について、その自然人が作成したことを示す	文書の起源と完全性の確実性を保証し、電子文書等が法人によって発行されたことを示す	電子データがある時刻に存在し、以降改ざんされていないことを示す
署名対象例	電子データ、文書、コード、メール		時刻情報
署名フォーマット	共通 PKCS#7/CMS SignedData/CAdES (ASN.1バイナリ形式)		
	他、XML署名/XAdES、PDF署名/PAdESなど		–
署名者証明書	個人の署名用証明書	組織の署名用証明書	TSA証明書

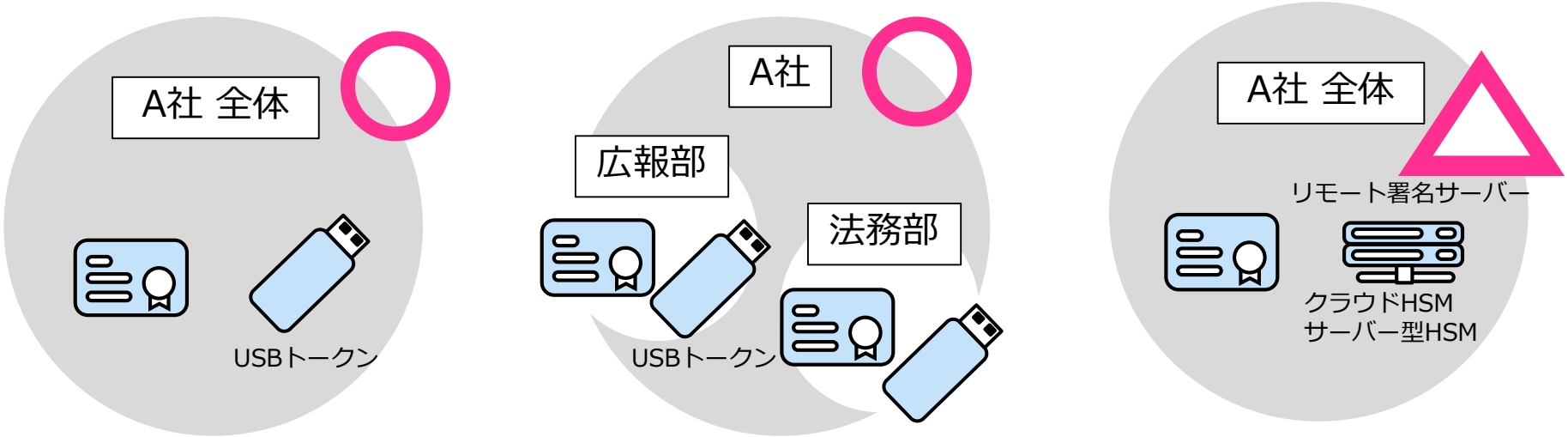
欧州 適格(Qualified)eシール、電子署名とは

- 「適格」であることにより法的な効力を持つ。
- 実は、フォーマットは変わらない。証明書やタイムスタンプの発行者が一定の要件を満たし、認定されているかどうかの違い。

	適格電子署名	適格eシール	適格タイムスタンプ
発行主体	自然人(個人)	法人や組織	TSU (デバイス)
署名フォーマット	先進電子署名フォーマット(AdES)のみ		非適格と同じ
署名者証明書	電子署名用適格証明書	eシール用適格証明書	適格TSP向けのTSA証明書
適格の追加要件	• 厳格な個人、法人、組織の身元確認審査 • 認証局、タイムスタンプ局の審査とEUトラストリスト掲載 • 署名にEU認定された適格署名生成デバイスを使用 (USBトークン、ICカード等)		

GlobalSignにおける Eシール用EU適格証明書の発行範囲と署名デバイス

- 部課レベルで発行は可能だが、執行役員以上の確認が必要
- 現時点ではUSBトークンに発行可能。リモート署名に用いるサーバー用HSM、クラウドHSM向けは計画中



GlobalSign eシール用EU適格証明書の発行の流れ(概要)

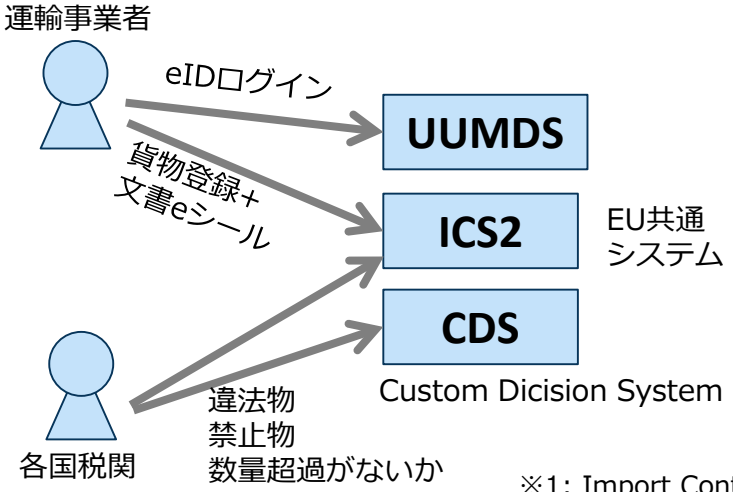
- eシール用適格証明書の発行はEV SSL証明書発行と同等の審査
- 第三者検証者(公証人,弁護士,公認会計士)による対面確認と署名

① 弊社欧州サイトにてアカウント作成と申込み
② 登記情報を第三者データベースで確認
③ 組織の正式代表者(執行役員以上)による承認の確認
④ 同意書(組織代表者、鍵(トークン)の管理、失効申請義務等)
⑤ 正式代表者の第三者検証者による本人確認、同意書確認と署名
⑥ 第三者検証者の確認 (弁護士の場合、日弁連サイト経由で確認)
⑦ 秘密鍵、証明書格納用のEU認定済(QSCD)USBトークンを送付
⑧ 証明書ダウンロードURLを送付
⑨ USBトークン内鍵生成と証明書の発行、格納

注意：現在、日本の組織に対する適格証明書発行は正式なサービス化はされていません。

利用例：貨物・郵便のオンライン税関手続き

- EC加盟国の航空郵便、航空・船舶・鉄道・道路による貨物の税関手続きのオンライン化プロジェクト ICS2※1(Import Control System2)
- EU加盟国で入札開始、運輸事業者がシステム化対応、eシールが要件
- 認証、署名には共通システムUUM&DS※2を使用
- なお、日本にはNACCS※3という独自のシステムがあるが、他のシステムと互換性のないシステムとなっていることが課題



出典: http://ec.europa.eu/ICS2

※1: Import Control System 2 http://ec.europa.eu/ICS2
※2: Uniform User Management & Digital Signature
※3: NACCS　https://www.naccs.jp/

GlobalSign eシール用EU適格証明書顧客の業種(抜粋)と傾向 (2020年9月時点)

- 始まって間もなく欧州中心だが、アジア圏もあり、業種に偏りは無い
- 電子調達(インボイスを含む)や公式な文書の発行元保証に使われている
- 政府調達の応札要件で導入頂くケースも数件ある

業種	地域	事業内容
輸送	欧州	国際配送サービスの現地法人
輸送	欧州	空港、駅の荷物サービス
ITサービス	欧州	ブロックチェーンセキュリティ
バイオ	欧州	ゲノム技術研究開発
ITサービス	欧州	電子契約サービス
金融	欧州	金融系サービス
重要インフラ	アジア	原子力/火力/風力/水力発電プラント
サービス・製造	アジア	児童向けプログラミング教育、教材
団体	アジア	(JIPDEC様) 登録証、見積請求書、報告書等
サービス	欧州	(GlobalSign) テスト・評価用

日本版eシール制度への期待(1)
日本認定eシールを諸外国含め機械的に表示区別できること

- 欧州eIDASの適格eシールは表示の要求事項がある
- 表示区別により日本認定eシールの市場価値を高める
- 表示のために2つの要件への対応が必要

欧州eIDAS規則 910/2014 Annex 3 eシール用適格証明書の要件
(a) 少なくとも自動処理に適した形式で、その証明書がeシール用適格証明書として発行されたという表示を行う。
(j) eシール検証データに関連付けれらたeシール生成データが適格eシール生成デバイスの中にある場合、少なくとも、自動処理に適した形式で、これを適切に表示する。

① DFFTの観点から国際相互運用性のある日本認定eシール用証明書	• 国際標準 RFC 3739 適格証明書プロファイルを使用する • 組織の特定に国で登録される法人番号(13桁)等を用いる。国内事務所を支店登記する法人番号のない外国法人の扱い等の検討。 • 日本認定eシール、日本認定eシール用デバイスを示すオブジェクト識別子(OID)をJIS等で定義
② 認定の有無が機械判読可能なこと	• XML等の構造化フォーマットによるデジタル署名つき日本認定トラストリストの公開

(参考)
eシール用EU適格証明書(QC)の各社X.509証明書プロファイル比較

- (自然人)電子署名用EU適格証明書と大きくは変わらない
- 証明書ポリシ、QCステートメント拡張の内容が異なる
- 文書署名専用

用語
QES: 適格電子署名
QSCD: 適格セキュア署名生成デバイス
QC: 適格証明書
ETSI: 欧州通信規格協会

業種	GS QES用	GS eシール用	A社 eシール用	B社 eシール用
主体者名の特徴	氏名又は仮名	organizationalIdentifierに加盟国VAT番号 ※1	organizationalIdentifierに加盟国VAT番号	organizationalIdentifierに加盟国VAT番号
鍵使用目的	否認防止のみ	否認防止のみ	否認防止のみ	否認防止のみ
証明書ポリシ	ETSI自然人QSCD GS QC自然人	ETSI法人QSCD GS QC法人	ETSI法人 A社QC法人	ETSI法人QSCD B社QC法人
QCステートメント	ETSI QC準拠 ETSI QC SSCD使用 ETSI QC種別=ESign	ETSI QC準拠 ETSI QC SSCD使用 ETSI QC種別=eシール	ETSI QC準拠 – ETSI QC種別=eシール	ETSI QC準拠 ETSI QC SSCD使用 ETSI QC種別=eシール
拡張鍵使用目的	Acrobat認証文書 (MS)文書署名者	Acrobat認証文書 (MS)文書署名者	–	–

※1: VAT番号(例：VATBE-12345678)が無い場合、国で登録された法人の識別番号が必要となり、日本の場合、「会社法人等番号(12桁)」を確認し「NTRJP-番号12桁」を記載

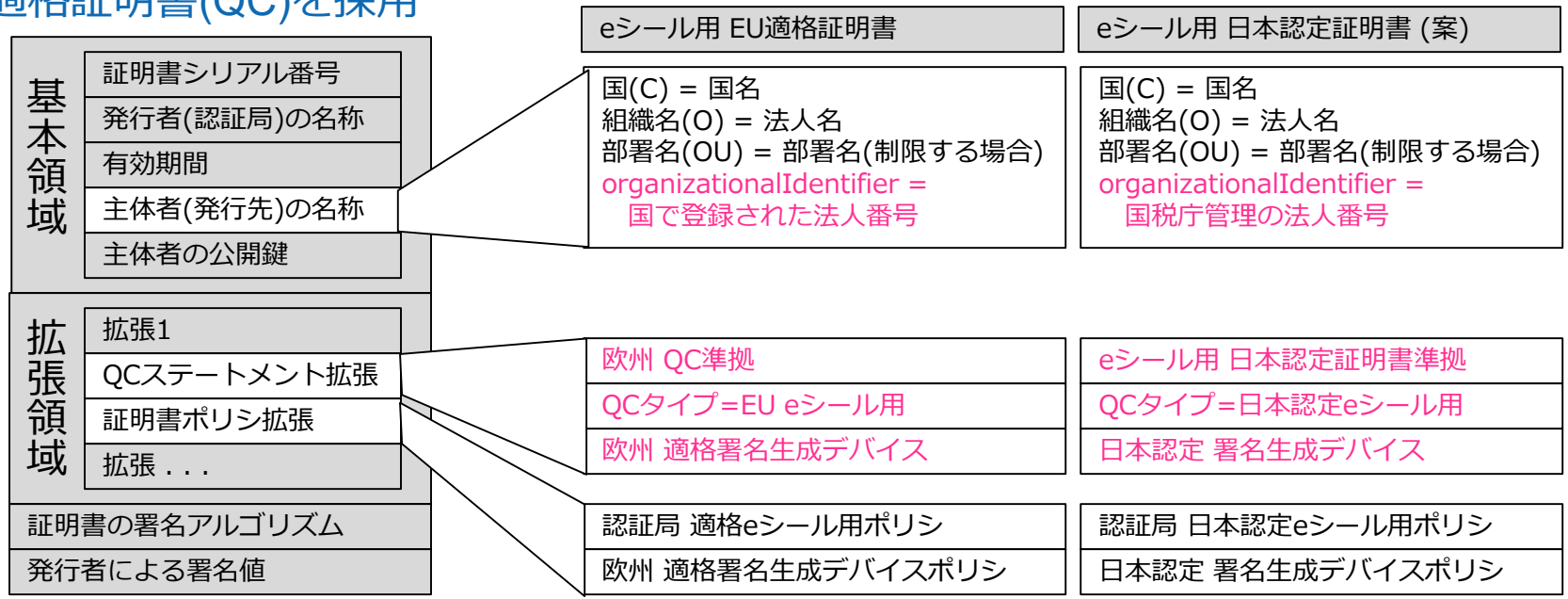
(参考)
日本版eシール用証明書の実装方法の比較

- 日本版eシール用証明書フォーマットの実装方法として3通りを比較
- 電子的に区別を容易にするならば、QCが最も実現が容易で相互運用性が高い

フォーマット	長所	短所
QC利用	• 日本認定eシールか区別が容易 • 製品調達が容易 • 国際相互運用性が高い • 標準化はOIDだけでよい	• QC OID標準化が必要
日本独自拡張	• 日本認定eシールか区別が容易	• ベンダーロックオン • 広範囲の標準化(拡張形式+OID)が必要 • 製品調達が限定的 • 国際相互運用性に課題
日本認定eシール証明書か区別する共通情報を入れない	• 標準化がほぼ不要(ガイドラインレベルで十分か？)	• 日本認定eシールかどうかの区別がつかない、つきにくい • 証明書の記載内容が認証ベンダーでばらつく • 区別不能でeシール自体の市場価値の損失

(参考)
デジタル証明書、適格証明書の構造と日本認定(案)

- SSLサーバー、PDF署名、S/MIMEメール、認証局に使われるデジタル証明書はITU-T X.509、RFC 5280で国際標準化された共通の証明書フォーマットを採用
- 欧州eIDAS eシール用や電子署名用の証明書はRFC5280ををベースにしたRFC 3739 適格証明書(QC)を採用



日本版eシール制度への期待(2)
日本認定eシールを要件とする制度、ガイドライン、調達の拡充

■既存の電子署名、タイムスタンプを要件とする法律・ガイドラインの見直し

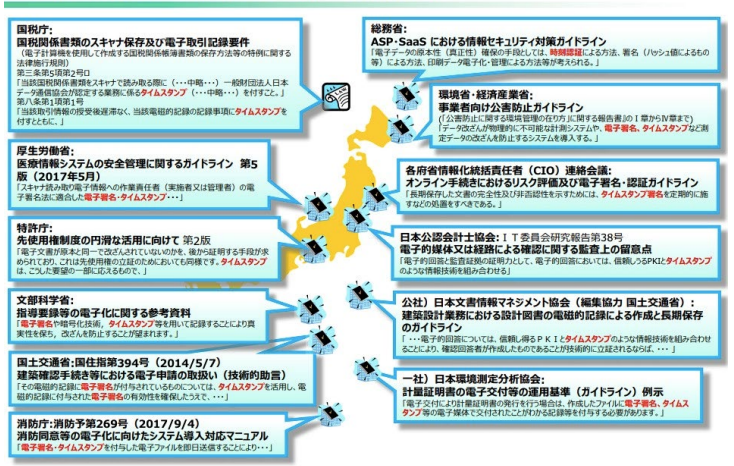
見直すケース

- プライバシー保護の観点から電子署名で担当者を明示することが適切でない場合
- 機械処理のためにタイムスタンプでは文書発行元の保証が十分でない場合

■電子化、機械処理の観点から組織によるデータの確実な保証を必要とする新しい制度、ガイドライン、調達の拡充

- ➢ これまで、担当者名がデジタル署名として残ることに抵抗があり、電子化が進まなかった分野への導入
- ➢ 欧州 適格eシールの利用事例を積極的に取り入れる

タイムスタンプに関する法律・ガイドライン



出典:日本データ通信協会 認定タイムスタンプを利用する事業者に関する登録制度より
www.dekyo.or.jp/touroku

GMOグローバルサイン株式会社

〒150-0043

東京都渋谷区道玄坂1-2-3　渋谷フクラス

https://jp.globalsign.com/