eシール活用セミナー
「eシール解説～実用化に向けて～」解説

JDTF 推進部会
調査研究委員会 委員長
佐藤　雅史（セコム(株)IS研究所）

All Rights Reserved. Copyright © Japan Digital Trust Forum

総務省「eシールに係る指針」（2021年6月）

- https://www.soumu.go.jp/main_content/000756907.pdf
- 本指針は、我が国における e シールの在るべき姿を示すとともに、e シールの信頼性を担保するために証明機関に求めるべき基準を検討するにあたっての参考とすることを目的としたもの

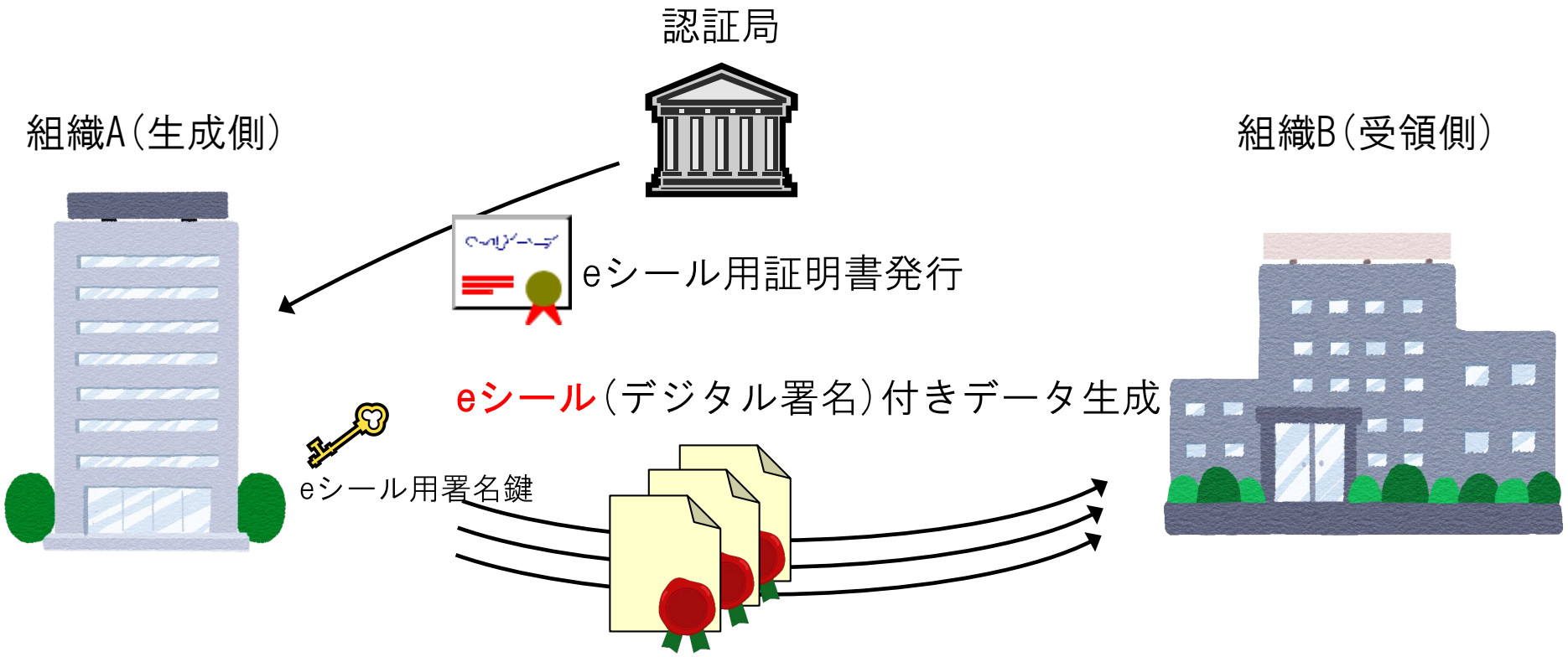
> 1.1 我が国におけるeシールの定義
> 発行元証明の機能を果たす e シールの我が国における定義は、データ戦略タスクフォース第一次とりまとめ で示されている“「事実・情報」：発行元証明 ”を踏まえて、**「電子文書等の発行元の組織等を示す目的で行われる暗号化等の措置であり、当該措置が行われて以降当該文書等が改ざんされていないことを確認する仕組み」**とする。

※太字は本資料によるもの

この指針により、eシールがより具体的に明確化され、今後の活用への期待とともに、活用のための議論の土台が築かれた。

All Rights Reserved. Copyright © Japan Digital Trust Forum

eシールは組織によるデジタル署名



データ発出元の証明、改ざん検知

All Rights Reserved. Copyright © Japan Digital Trust Forum

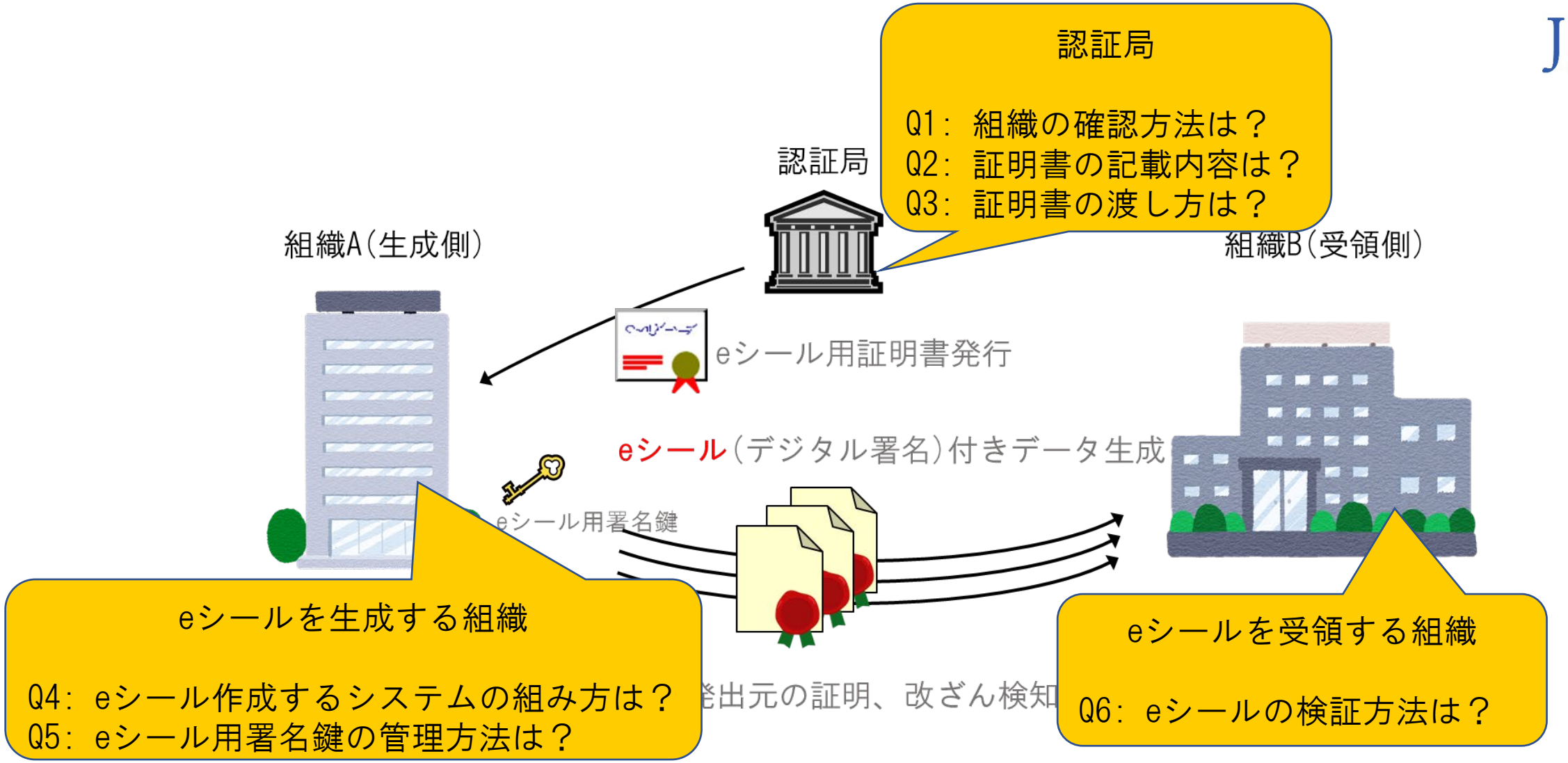
eシールは何に使える？

- 組織間文書
  - 受発注情報、申込書、請求書、領収書、見積書など
- 組織が公開する文書
  - ニュース、プレスリリース、官報、約款、カタログ、取扱説明書など
- 証明書類
  - 保証書、在籍証明、ライセンス（資格）証明
- 組織が管理するシステムから発信されるデータ
  - 例：測定データ、売上データ、統計データ、オープンデータ
- サービス間で交換されるデータ
  - 例：決済サービスの取引データ、eデリバリー（電子配送）サービス

※ユースケースによっては、自然人による電子署名やデバイス用証明書
　との使い分けや併用も考慮に入れる必要がある

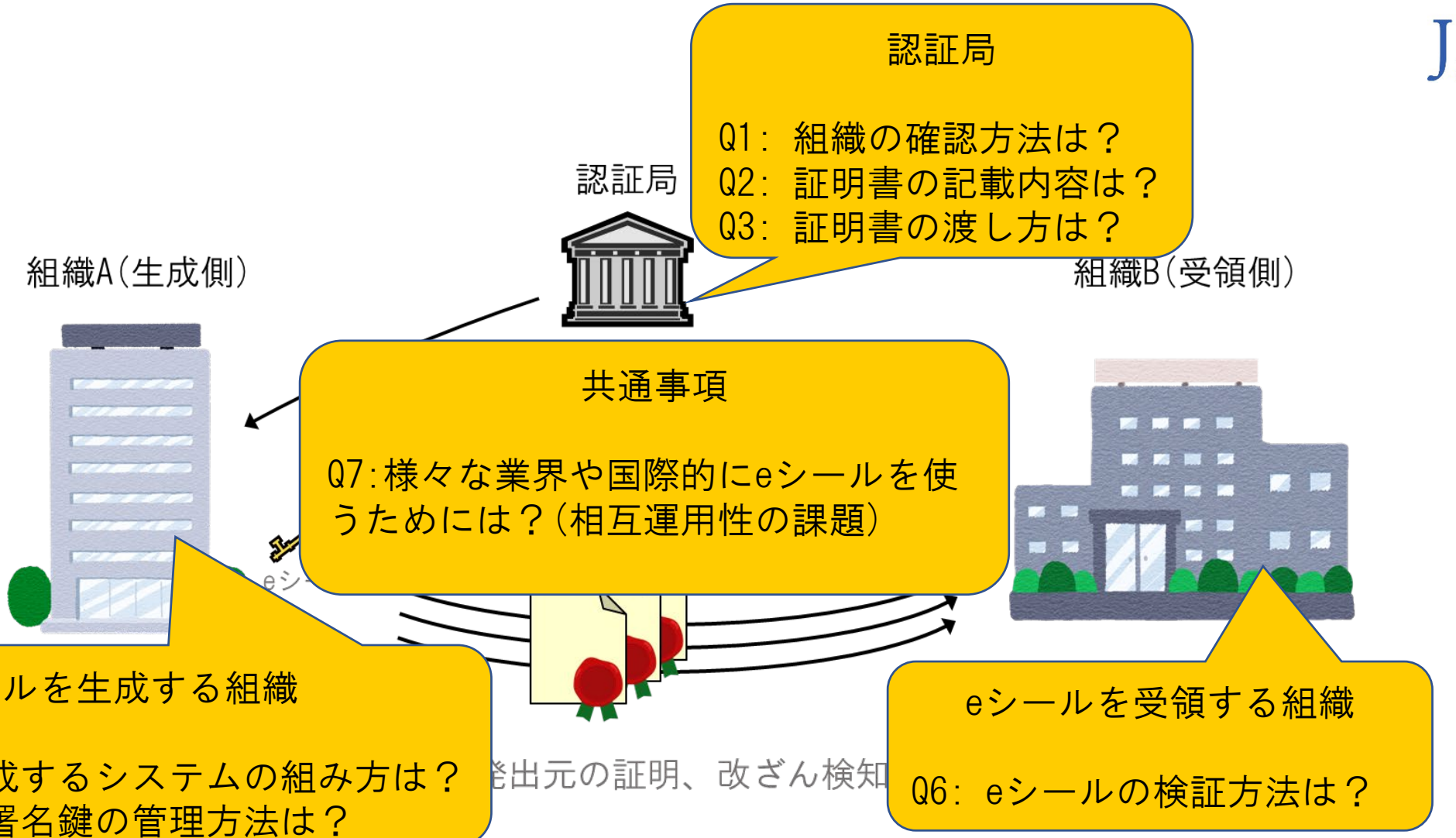
All Rights Reserved. Copyright © Japan Digital Trust Forum

eシールを活用するためには？



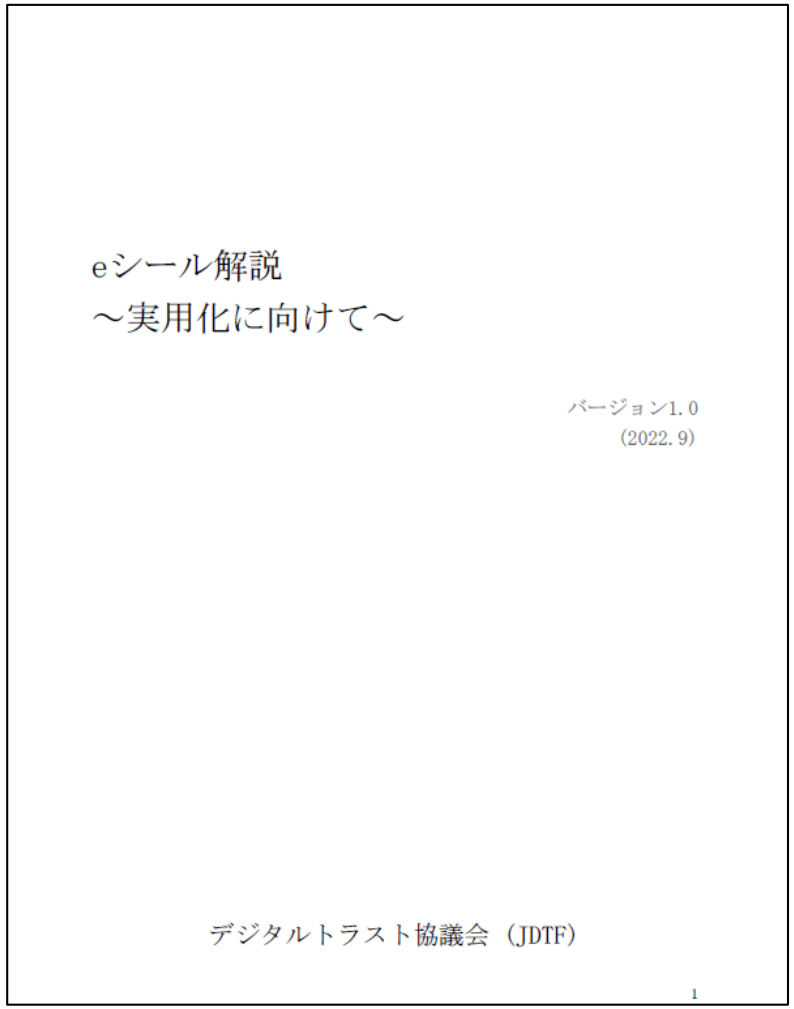
All Rights Reserved. Copyright © Japan Digital Trust Forum

eシールを活用するためには？



All Rights Reserved. Copyright © Japan Digital Trust Forum

「eシール解説～実用化に向けて～」


eシール解説
～実用化に向けて～

バージョン1.0
(2022.9)

デジタルトラスト協議会（JDTF）

1

- JDTF調査研究員会にて作成。
- バージョン1.0を2022年９月に公開。
- すでに様々な標準規格が構築されているPKIをベースとしたeシールに特化。
- 実用化や相互運用性確保のための課題や論点を整理。
- 総務省の指針と関係しながらも、独立した位置づけ。
- https://jdtf.or.jp/report/whitepaper/から入手可能。

All Rights Reserved. Copyright © Japan Digital Trust Forum

eシール解説の全体

目次

All Rights Reserved. Copyright © Japan Digital Trust Forum

eシール解説の全体

eシールを生成する組織

Q4: eシール作成するシステムの組み方は？

4. eシ
5. 本書 ールのスコープ
6. eシー ケース例
7. eシール ムモデル
7.1 本章の概
7.2 eシール用 書の発行対象
のバリエー ョン
7.3 システム構成例の分類
7.4 組織内運用
7.4.1 媒体管理型
7.4.2 サーバー管理型
7.4.3 システム組込み型
7.5 リモートeシールサービス
7.6 機器組込み

eシールを受領する組織

Q6: eシールの検証方法は？
（考え方のみ記述）

認証局

Q1: 組織の確認方法は？
Q2: 証明書の記載内容は？
Q3: 証明書の渡し方は？

eシールを実用化するための課題
本章の概要
eシールの保証レベルの考え方
eシール用証明書の発行に関する課題 案
8.3.1 本節について
8.3.2 組織や代表者等の確認方法
8.3.3 証明書の記載事項に関する論点
8.3.3.2 証明書の記載事項を検討する際の留意点
8.3.3.3 QCStatementsの運用方法について
8.3.4 eシール用証明書等の受け渡し方法に関する論点
8.4 eシール署名鍵の管理について
8.4.1 eシール署名鍵生成
8.4.2 eシール署名鍵管理における運用上の課題
8.4.2.1 eシール署名鍵管理の考え方
8.4.2.2 eシール署名鍵の管理や利用について
8.4.2.2 eシール用証明書の失効とeシール署名鍵の廃棄について
8.5 eシールの国際相互承認
8.5.1 本節について
8.5.2 国際相互承認の必要性
8.5.3 国際相互承認のために必要な項目
8.5.4 国際的な相互運用への配慮
8.6 eシールの実用化に向けた制度等の全般に関わる課題

9. おわりに
付録A：EUにおけるeシール用証明書の記載項目に関する特記事項
A.1 QCStatements拡張の要素
A.2 組織識別子(organizationIdentifier)の値
A.3 LEI拡張について

eシールを生成する組織

Q5: eシール用署名鍵の管理方法は？

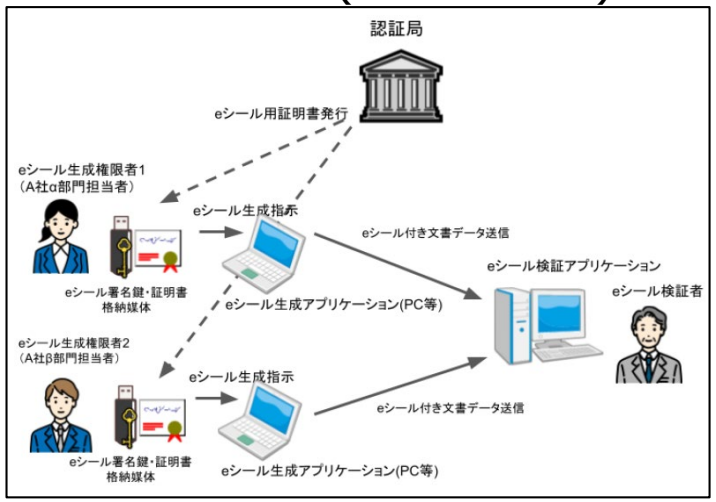
共通事項

Q7:様々な業界や国際的にeシールを使うためには？(相互運用性の課題)
※証明書の記載内容等の他の項目にも影響。

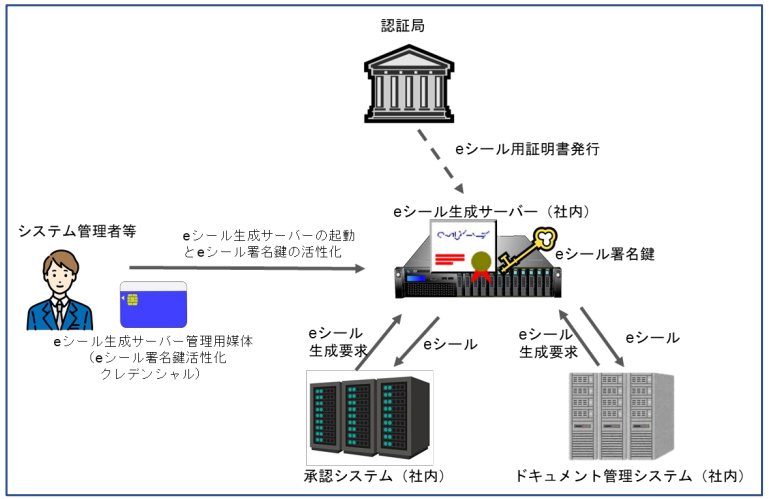
All Rights Reserved. Copyright © Japan Digital Trust Forum

eシールの様々な導入方法

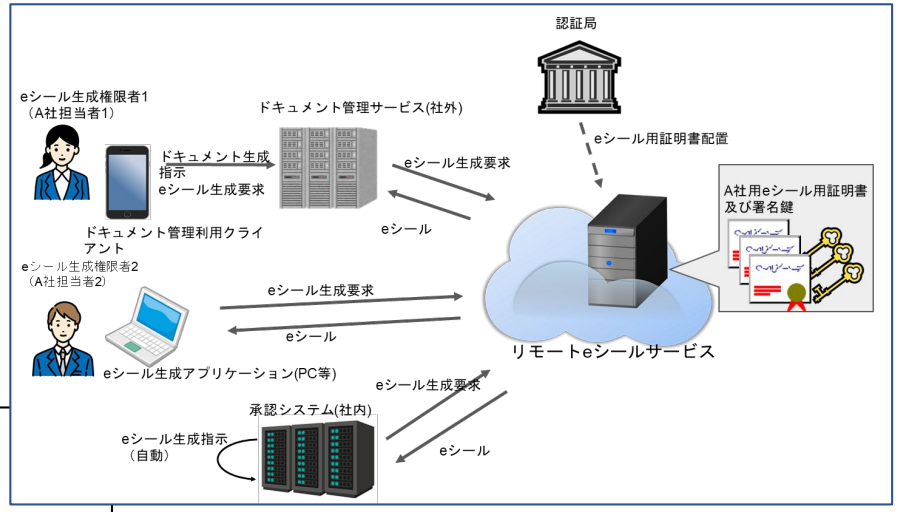
組織内運用(媒体管理型)



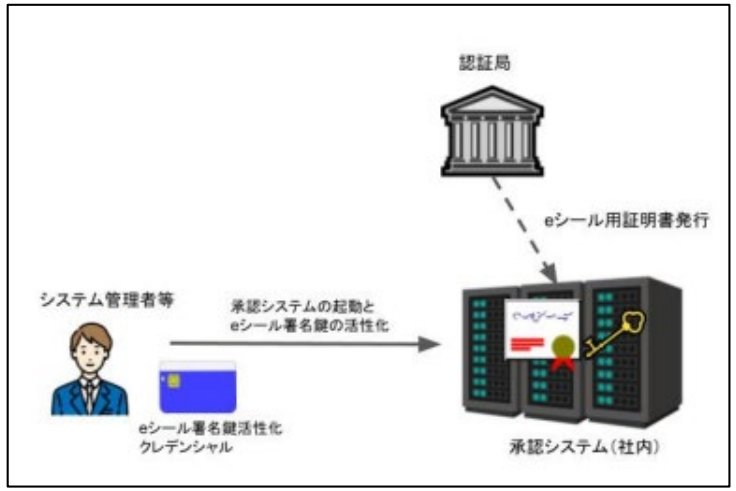
組織内運用(サーバー管理型)



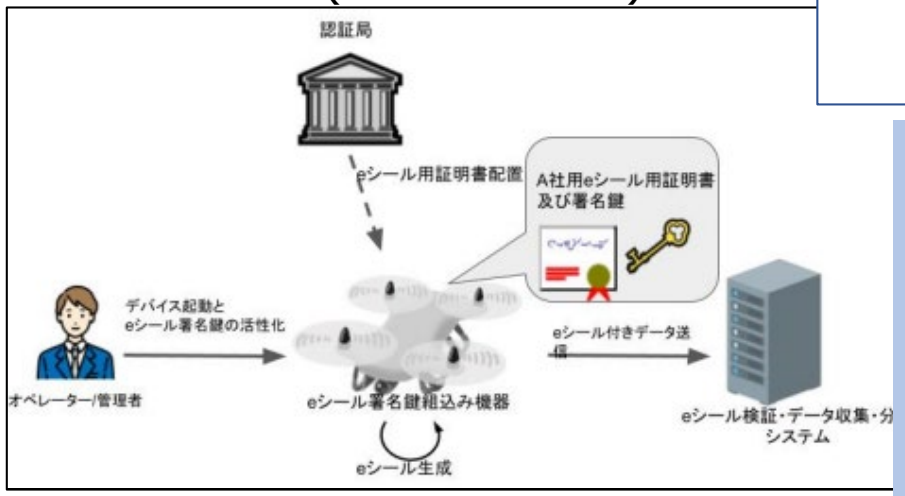
リモートeシールサービス(第三者サービス)の利用



組織内運用(システム組込み型)



組織内運用(機器組込み型)



導入方法に応じた構築・運用時の考え方を整理

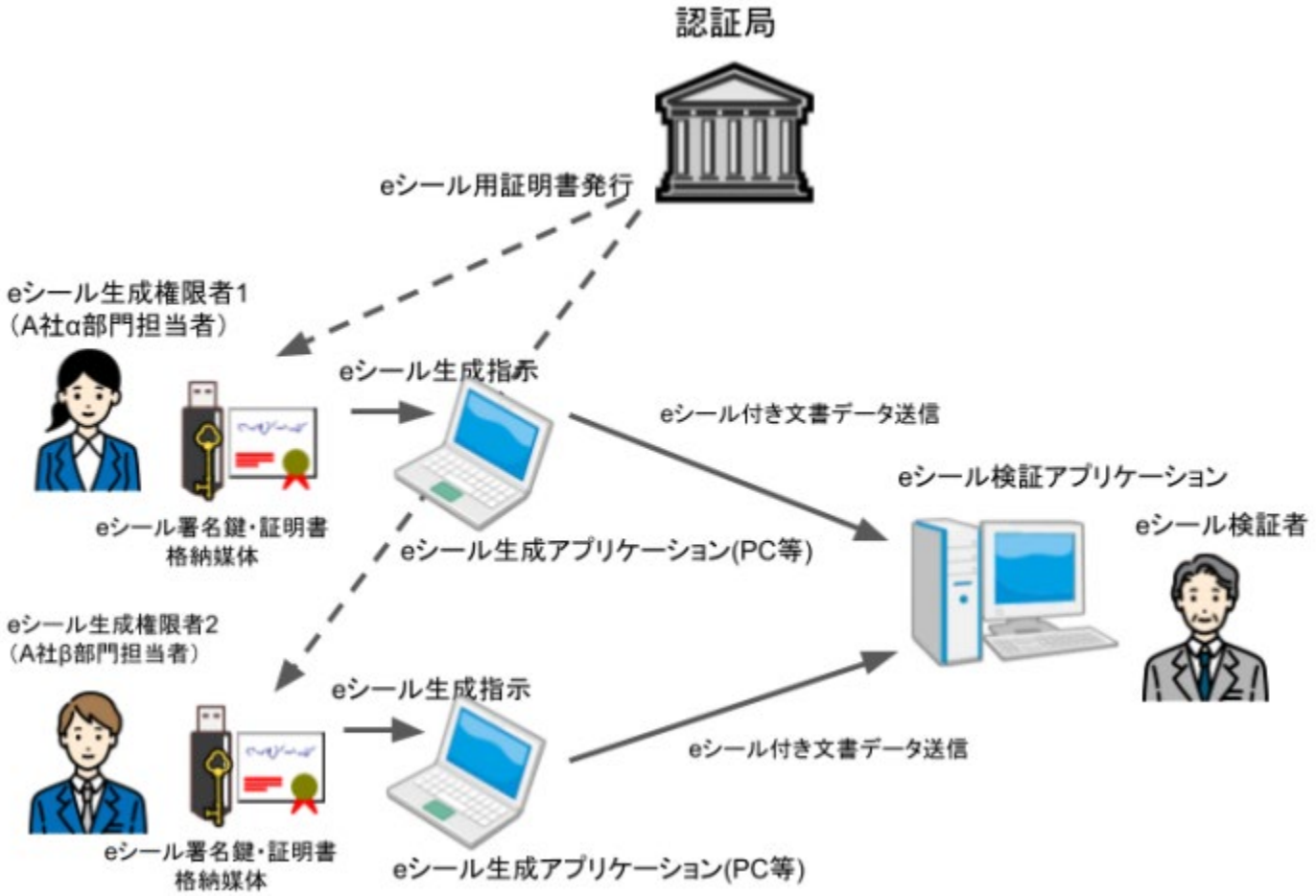
- eシールの生成に必要な署名鍵の管理
- eシールの生成方法(プロセス)の考え方
- 署名鍵の管理における留意点
- 認証局からの証明書発行・受け渡し方法の考え方

など

All Rights Reserved. Copyright © Japan Digital Trust Forum

eシール導入方法の例～組織内運用（媒体管理型）～

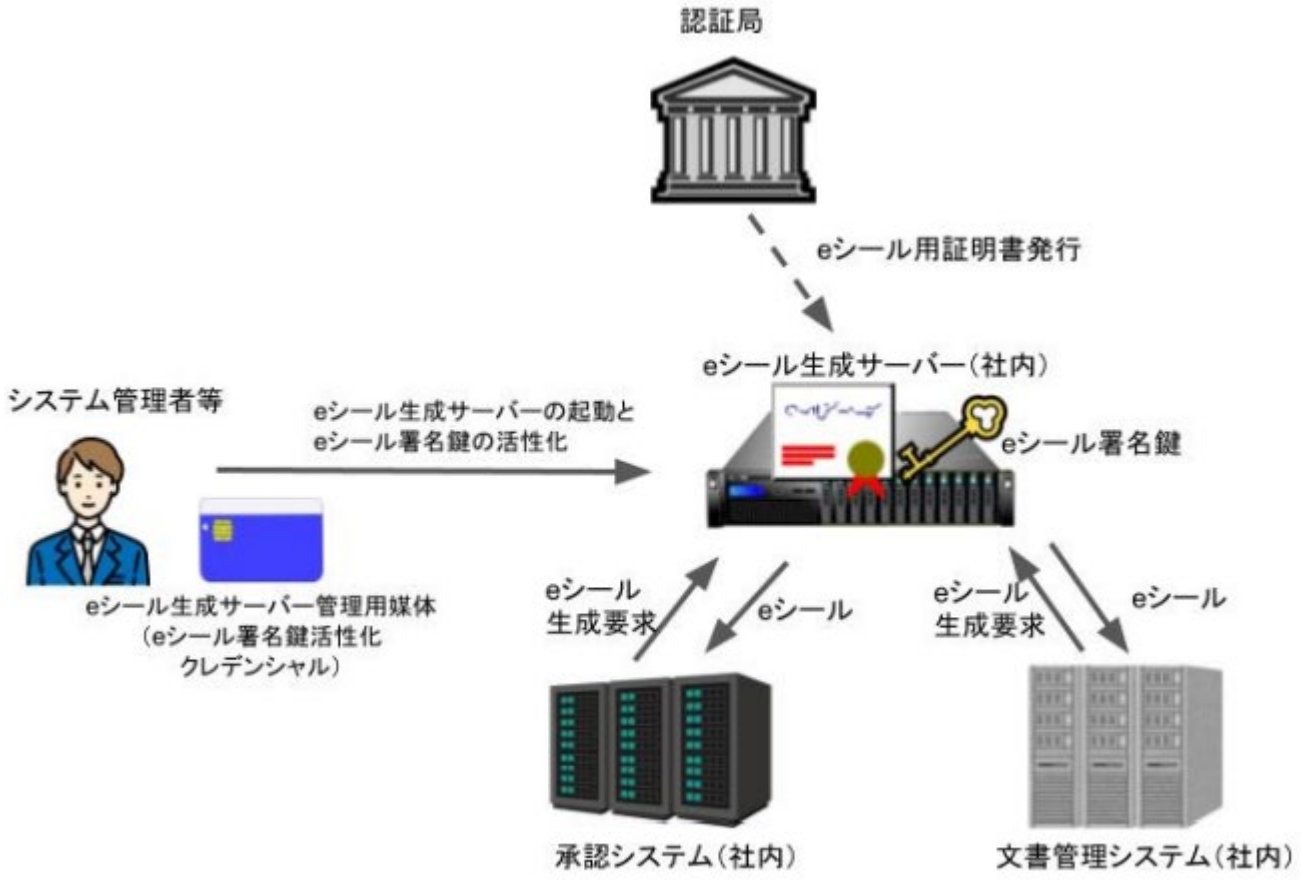
組織内担当者がeシール作成操作を行うケース



All Rights Reserved. Copyright © Japan Digital Trust Forum

eシール導入方法の例～組織内運用（サーバー管理型）～

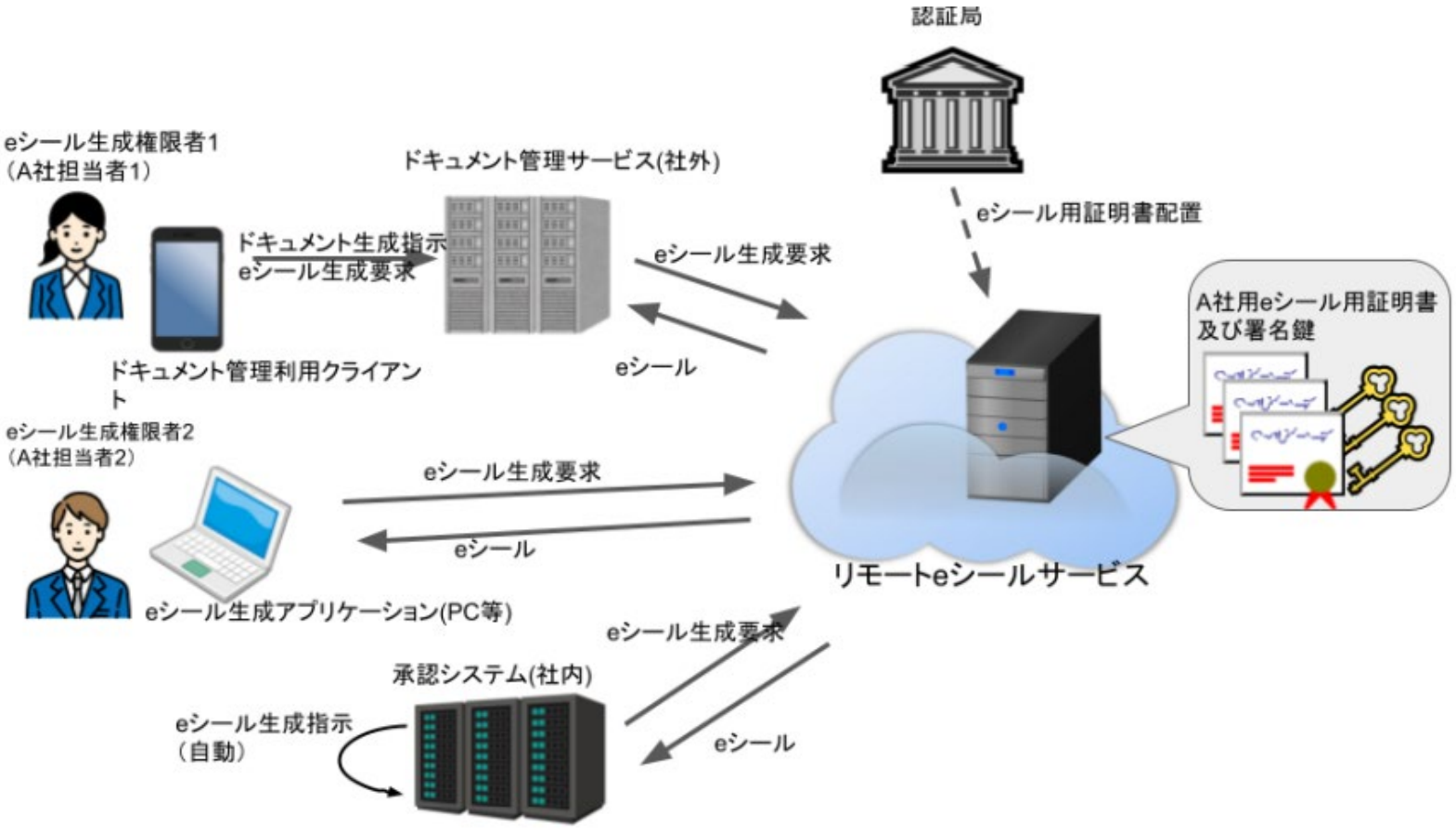
組織内システムと連動したeシール作成を行うケース



All Rights Reserved. Copyright © Japan Digital Trust Forum

eシール導入方法の例～リモートeシールサービス～

第三者のサービスを利用したeシール作成を行うケース



All Rights Reserved. Copyright © Japan Digital Trust Forum

eシール検証の考え方

- eシール解説では検証の考え方のみ簡潔に記している。
- 検証方法は従来の電子署名(PKIのデジタル署名)の基本と同様に考えられる。
  - eシール用証明書はX.509証明書
  - eシールのフォーマットは従来のデジタル署名(長期署名)フォーマットが適用可能
  - 参考：JNSA デジタル署名検証ガイドライン https://www.jnsa.org/result/e-signature/2021/index.html
- 「従来のデジタル署名の検証」＋「eシール固有の要素(証明書の記載事項など)の確認」が基本となる。

All Rights Reserved. Copyright © Japan Digital Trust Forum

相互運用性を確保するためには？

- ユースケースによりeシールに要求されるレベル（確実性など）も異なる⇒保証レベルの考え方
- 認証局のレベル
  - 組織の確認方法の度合い
  - 証明書の受け渡し方法
  - 認証局のセキュリティ（運用体制、施設・設備、証明書発行用署名鍵の管理）
- eシール用署名鍵管理方法のレベル
  - 鍵管理媒体、運用方法、鍵廃棄や証明書の失効申請。
  - リモートeシールサービスにおける鍵管理
- 保証レベルに応じたeシール用証明書の記載内容

※上記を検討するにあたり、制度や標準規格など国際動向にも目を配ることが大切

All Rights Reserved. Copyright © Japan Digital Trust Forum

eシール解説における保証レベル案

PKIのデジタル署名によりeシールを実現するための保証レベルを想定
(総務省の指針ではより広い定義での保証レベルを規定)

表8-1　eシールの保証レベルの考え方

	レベル1	レベル2	レベル3
レベル概要	発行元証明に必要とされる最低限の組織確認が行われるレベル。	国並びに国に準ずる機関又は中立・公正な機関が作成した基準に基づく適合性評価を受けたレベル。 日本国内において幅広く利用される。	国際相互承認の対象となる適合性評価を受けたレベル。 厳格な組織確認を必要とする。

All Rights Reserved. Copyright © Japan Digital Trust Forum

組織確認のレベル案(法的実在確認)

	組織確認レベル１	組織確認レベル２	組織確認レベル3
対象例 （レベルが上がる毎に範囲が狭い）	レベル2の対象に加え ・登記されていない組織（任意団体、管理組合など） ・個人事業主	レベル3の対象に加え ・開業届を確認できる個人事業主 ・適格請求書発行事業者登録番号を確認できる事業者	・法人番号を確認できる組織
法的実在確認	―	商業登記されていることを確認 ＜確認事項＞ 以下のいずれかの方法によるものとする。 1. 組織の商業登記簿謄本（もしくは抄本）の提出を求める方法、もしくは民間企業概要データベース（商業登記簿を確認しているものに限る）を参照する方法 2. 法人の代表者の電子署名の有効性を検証する方法（商業登記法第12条の2第1項、同第3項の規定で証明されるものに限定） 3. 組織属性を格納した証明書による電子署名の有効性を検証する方法（電子署名法第4条に基づく認定認証事業者の発行に限定） レベル2で個人事業主の場合は以下全てを確認 1. 利用申込書等に屋号を記載のうえ、当該個人事業主の実印を押印し印鑑登録証明書を添付 2. 利用申込書等に記載の屋号と開業届の屋号を確認 3. 適格請求書発行事業者登録番号を保持している場合は当該番号を利用申込書に記載し、国税庁適格請求書発行事業者公表サイトで確認	

All Rights Reserved. Copyright © Japan Digital Trust Forum

組織確認のレベル案(物理的実在確認・組織の運営確認)

	組織確認レベル１	組織確認レベル２	組織確認レベル3
対象例 （レベルが上がる毎に範囲が狭い）	レベル2の対象に加え ・登記されていない組織（任意団体、管理組合など） ・個人事業主	レベル3の対象に加え ・開業届を確認できる個人事業主 ・適格請求書発行事業者登録番号を確認できる事業者	・法人番号を確認できる組織
物理的実在確認	–	申請された住所が登記簿やQIISで確認できる住所であることを確認。 QIIS：CA/Browser Forumで用語定義されている認定された独立した組織情報ソース(例.帝国データバンク、東京商工リサーチ)。	
組織の運営確認	–	設立から3年以上経過しているか、QIISに登録があるかの確認。 又は弁護士意見書などを確認。 ＜個別実施事項＞ 1.法人番号を証明書に格納する際には、「証明書に格納された属性情報の信頼性と利用に関するガイドライン」の認証方法に基づく。 2.英文商号は、定款に記載がある場合は提出を求める(定めがない場合自己申告に基づく) 3.QIIS(商業登記簿を確認しているものに限る)を参照して当該民間企業が管理する企業コードを証明書に格納する場合は、オンラインで企業コードを確認する。	

All Rights Reserved. Copyright © Japan Digital Trust Forum

組織確認のレベル案

	組織確認レベル１	組織確認レベル２	組織確認レベル3
組織代表者の申請意思確認	レベル2に準じた方法を採用する。求められるレベルに基づき、例えば、以下のような方法が考えられる。 ・「在職証明」の提出 ・民間企業概要データベース(商業登記簿を確認しているものに限る)を参照した法人電話番号への電話による代表者の在職確認 ・電話帳、電話会社発行の請求書などで確認できる電話番号	以下のいずれかの方法によるものとする。 1. 書類申請 代表者印が押印された発行申請書、および印鑑証明書の提出が必要 個人事業主の場合は利用申込書等に屋号を記載のうえ、当該個人事業主の実印を押印し、開業届および印鑑登録証明書を添付 2. 電子申請(その1) 法人代表者の電子署名(商業登記法第12条の2第1項及び第3項の規定により証明されるものに限る)の付与が必要 3. 電子申請(その2) 法人代表者から委任を受けた者の電子署名(電子委任状の普及の促進に関する法律第5条第1項の認定を受けた電子委任状取扱事業者が発行したもので署名検証できるものに限る)の付与が必要(電子委任状が電子署名法の認定認証業務以外の場合は委任を受けた者の本人性を確認するため、別途住民票の提出を求める) 4. 電子申請(その3) 法人の代表者の電子署名(電子委任状の普及の促進に関する法律第５条第１項の認定を受けた電子委任状取扱事業者が発行したもので、代表者であることの確認、および署名検証できるものに限る)の付与が必要 5. 代表者のマイナンバーカードに格納された署名用証明書による電子署名(「第三者機関が管理するデータベース(商業登記情報等の公的な機関が管理する情報と照合されたものに限る。)に登録されている代表者の住所の一致の確認」が必要)	レベル2に加え、厳密な身元確認を求める。詳細は、以下の＜A＞＜B＞＜C＞を全て実施する。 ＜A＞ いずれかの方法によるものとする。 1. 書類申請 代表者印が押印された発行申請書、および印鑑証明書の提出が必要 2. 電子申請(その1) 法人の代表者の電子署名(商業登記法第12条の2第1項及び第3項の規定により証明されるものに限る)の付与が必要 3. 電子申請(その2) 法人代表者から委任を受けた者の電子署名(電子委任状の普及の促進に関する法律第5条第1項の認定を受けた電子委任状取扱事業者が発行したもので検証できるものに限る)の付与が必要(電子委任状が電子署名法の認定認証業務以外の場合は委任を受けた者の本人性を確認するため、別途住民票の提出を求める) 4. 電子申請(その3) 法人の代表者の電子署名(電子委任状の普及の促進に関する法律第5条第1項の認定を受けた電子委任状取扱事業者が発行したもので、代表者であることの確認、および署名検証できるものに限る)の付与が必要 ＜B＞ 必要書類(写し)の提出を求める ＜C＞ 代表者等の写真付き身分証明書を持参のうえ、対面(もしくはビデオによる対面)による認証を実施し、認証結果を保存する。 または第三者検証者(弁護士など)による身元確認を実施し確認結果書類(第三者検証者の署名を求める)を保存する。

All Rights Reserved. Copyright © Japan Digital Trust Forum

証明書記載事項(証明書プロファイル)案

- 詳細はeシール解説をご覧ください。以下は識別名の箇所のみ抜粋。

領域名	要求レベル	属性	値の例	説明
issuer 発行者名 (必須)	必須	C	JP	PrintableStringを使用
	任意	ST	Tokyo	・UTF8StringまたはPrintableStringを使用 ・organizationIdentifierに格納される値は8.6の「組織等の識別子や表記に関する課題」を参照のこと ・左記属性タイプ以外の格納も可能とする(任意)
	任意	L	Chiyoda-ku	
	必須	O	xxx, LTD.	
	必須	CN	xxxCA for eSeal	
	任意	OU	xxxCA	
	任意	organization Identifier	NTRJP-987654321098	
subject 主体者名 (必須)	必須	C	JP	PrintableStringで記述
	任意	ST (※2)	Tokyo	・UTF8StringまたはPrintableStringを使用 ・organizationIdentifierの例示は会社法人等番号を記載 ・organizationIdentifierに格納される値は8.6の「組織等の識別子や表記に関する課題」を参照のこと ・左記属性タイプ以外の格納も可能とする(任意) ・主体者の名称、住所はシステムや国際的な相互運用性の観点から英名、半角英数字記号を使用する。和名はsubjectAltNameに記載する。
	任意	L (※2)	Shinjuku-ku	
	必須	O (※1)	YYYYYY, LTD.	
	必須	CN (※1)	YYY	
	任意	OU	ZZ Division	
	必須	organization Identifier	NTRJP-1234567890123	

以下の検討課題がある。

- eシール用証明書とその他の証明書(例:組織代表者向け証明書)との区別
- 保証レベルごとの区別

現在、JDTFにて、より詳細な検討に進展中。

All Rights Reserved. Copyright © Japan Digital Trust Forum

その他の項目

- リモートeシールサービスの運用方法の考え方
  - リモート署名サービスとの相違点
- 適合性評価等の制度に関する考え方
- 信頼点（トラストアンカー）に関わる整備
- 国際相互承認における課題
- 制度等全般にかかわる課題
  - 利用者・組織が安心して利用できる枠組み・認証制度
  - 利用を支援するガイドライン、標準化、実装ガイド、検証環境
  - 組織等の識別子や表記の相互運用を確保するための登録制度

All Rights Reserved. Copyright © Japan Digital Trust Forum

デジタル社会の発展に向けて

- eシールは組織から発出するデータの真正性(発出元組織の実在性、非改ざん性)を担保するもの。
- データによる検証可能性は、組織間のサービスやシステムが連携するデジタル社会で特に重要なものと考えられる。
- eシール解説ではPKIのデジタル署名によるeシールにフォーカスし、実装上の課題、相互運用性の課題を洗い出し、全体像を俯瞰している。
- 今後もより詳細な検討が進み、eシールに関わる基盤が強化され、実用化が促進し、新たなデジタル社会の発展に寄与すると期待している。

All Rights Reserved. Copyright © Japan Digital Trust Forum

ご清聴ありがとうございました

All Rights Reserved. Copyright © Japan Digital Trust Forum