eシールに関する総務省の取組と期待

令和5年3月8日

総務省サイバーセキュリティ統括官室

＜本日のアジェンダ＞

１．はじめに　～トラストサービス、eシールのご紹介～

２．eシールに関する総務省の取組

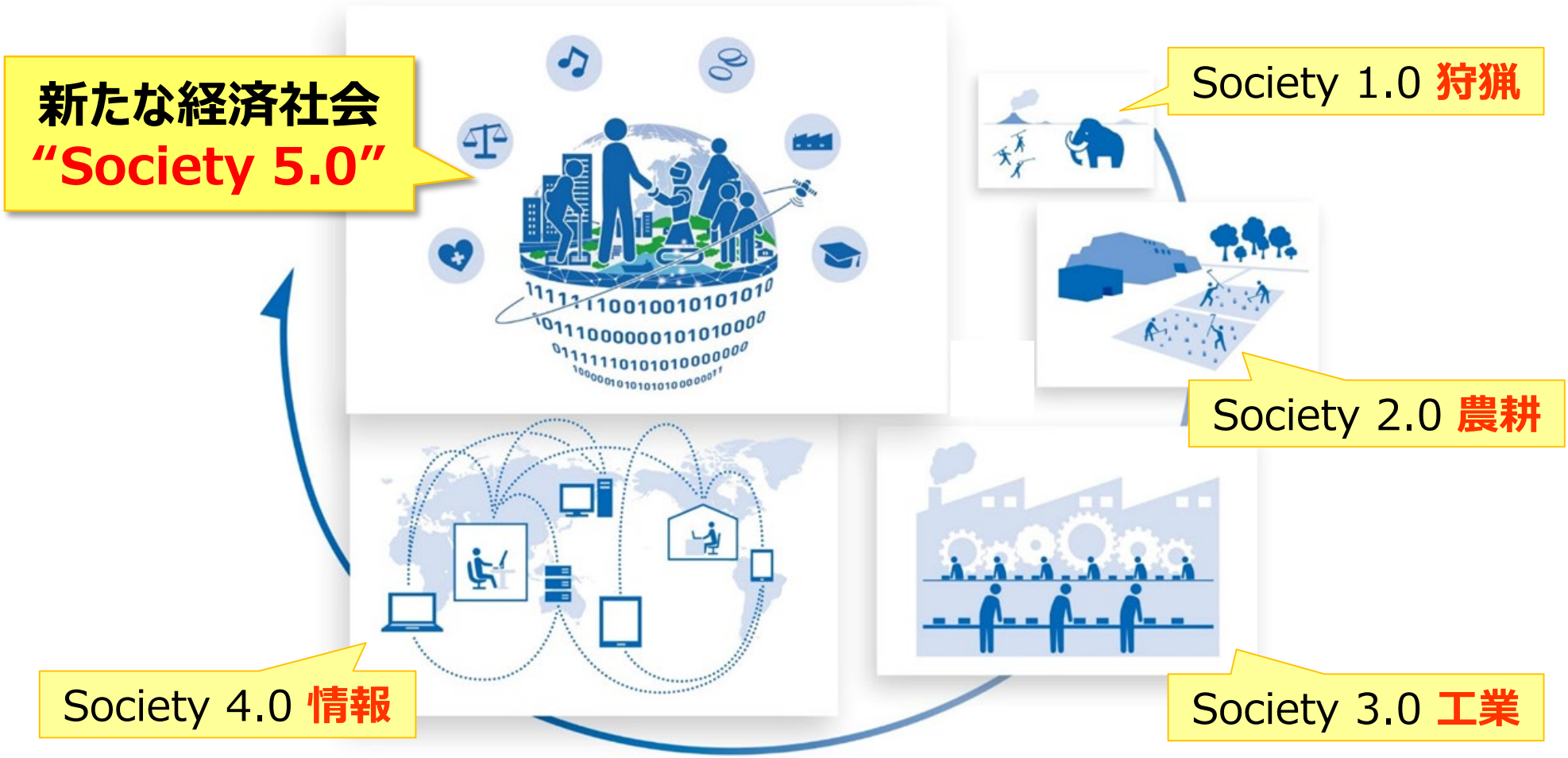
　2-1 「eシールに係る指針」の作成

　2-2 eシールに関する実証実験

３．eシールの今後

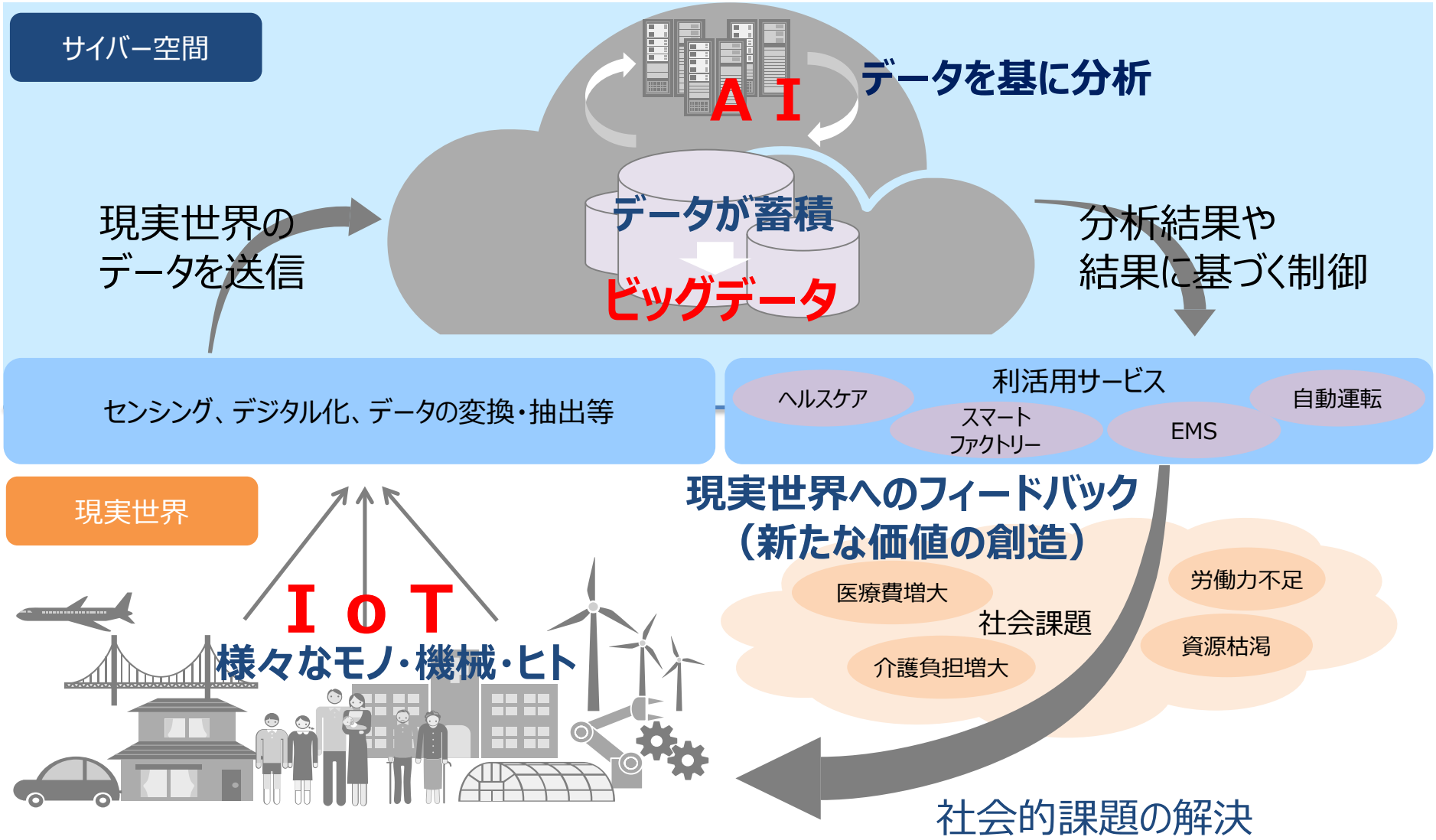
Society 5.0とは

サイバー空間とフィジカル（現実）空間を高度に融合させたシステムにより、
経済発展と社会的課題の解決を両立する、
人間中心の**社会（Society）**

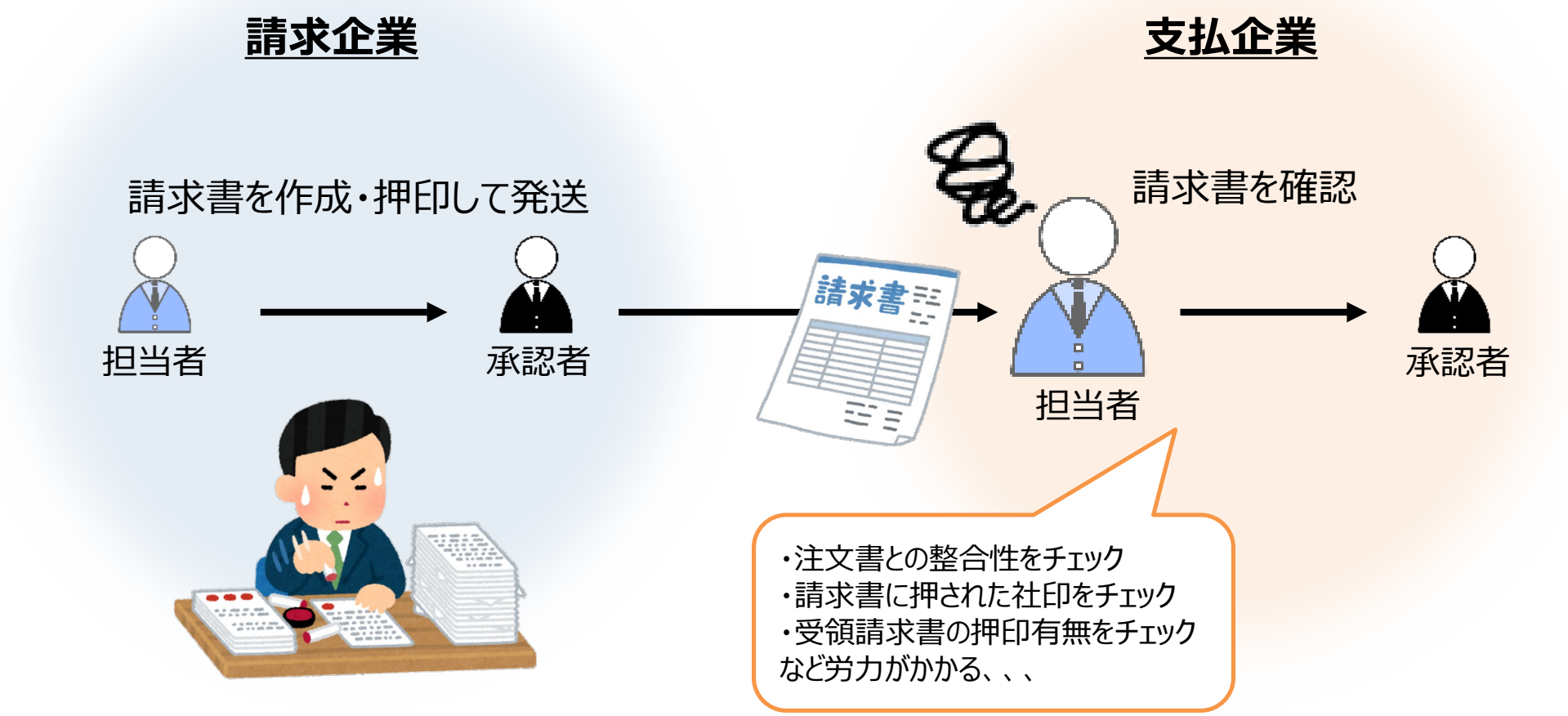


※内閣府資料

Society5.0の到来には、データ主導社会の実現が必要



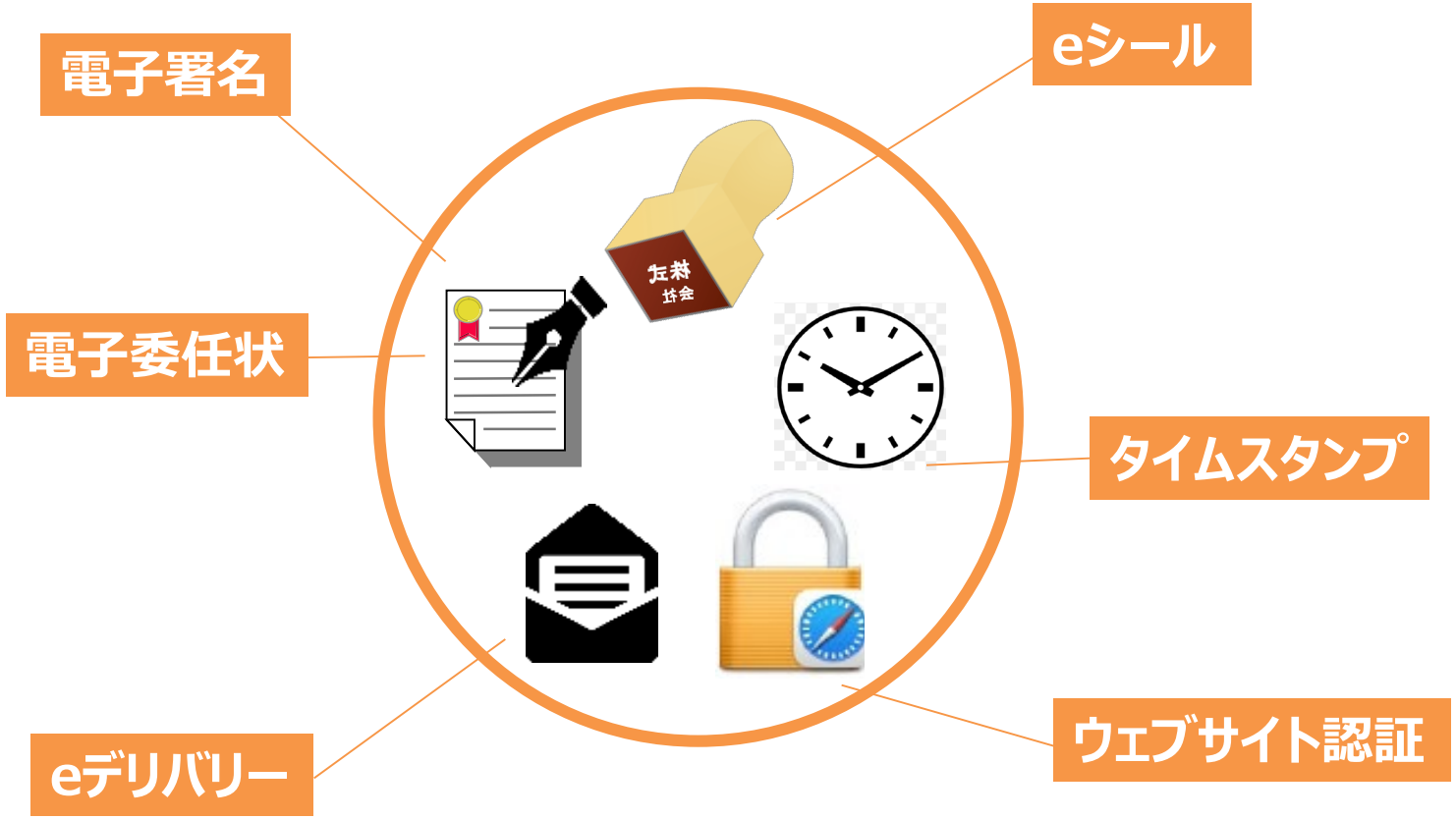
事務処理のデジタル化


請求企業
支払企業
請求書を作成・押印して発送
担当者
承認者
請求書
請求書を確認
担当者
承認者
・注文書との整合性をチェック
・請求書に押された社印をチェック
・受領請求書の押印有無をチェック
など労力がかかる、、、

トラストサービスとは

- ✓ トラストサービスとは、インターネット上で本人であることやデータの正当性を証明することにより、**送信元のなりすましや改ざん等を防止するための仕組み**のこと。
- ✓ 例えば、電子署名、タイムスタンプ、eシール、eデリバリー等がある。

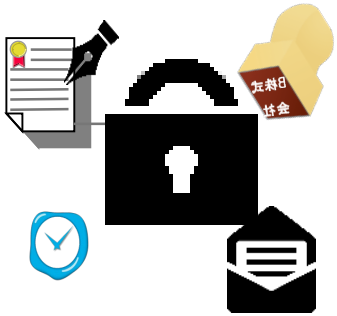
＜トラストサービスの例＞



トラストサービスの重要性（背景）

- ✓ Society5.0においては、実空間とサイバー空間が高度に融合し、実空間での紙や対面に基づく様々なやりとりを、サイバー空間においても電子的に円滑に実現することが求められる。
- ✓ その実現には、データを安全・安心に流通できる基盤が不可欠であり、データの改ざんや送信元のなりすまし等を防止する仕組みであるトラストサービスの重要性が高まっている。

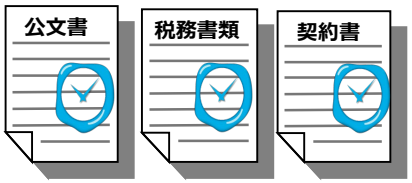
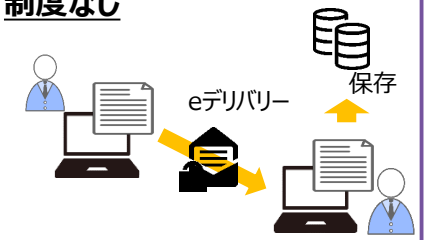
トラストサービスの普及 ⇒ **データの自由な流通が促進** ⇒ **Society5.0の実現！！**



テレワークの利用が広がっている中、トラストサービスは、企業間での契約や請求書・領収書等のやりとりを電子化し、オンラインで完結することで、コロナ後も見据えた業務改革を進めるための基盤として期待されるところ。

トラストサービスに関する総務省の取組

- ✓ トラストサービスについてはデジタル庁や総務省において、民間サービスの信頼性を評価する認定制度や普及啓発に関する取組を実施。
- ✓ 総務省ではデジタル庁による取組の下、タイムスタンプに関する認定制度の運用や、eシールに関する認定制度整備の検討等の取組を実施。

	① 電子署名 ・意思を確認できる仕組み	② タイムスタンプ ・データの存在証明の仕組み	③ eシール ・文書の発行元を確認できる仕組み	④ eデリバリー ・データの送達を保証する仕組み
サービス内容	**国による認定制度あり** 意思に係る文書	**国による認定制度あり**  	**技術上・運用上の基準あり** 事実・情報に係る文書	**制度なし** 
総務省の取組	■令和３年９月１日のデジタル庁設置に伴い、電子署名法は同庁に移管。	■令和３年４月より総務大臣による認定制度が開始。民間認定制度からの円滑な移行を支援。 ■令和４年度税制改正で、電子帳簿等保存制度の中に、総務大臣による認定制度に基づくタイムスタンプの付与を位置づけた。	■令和３年６月、eシールに係る技術上・運用上の基準等を整理した「eシールに係る指針」を公表。 ■デジタル庁において取りまとめた「トラストを確保したDX推進SWG報告書」（令和4年７月）を踏まえ、今後eシールの信頼性評価等に係る取組を実施予定。	■令和３年度、eデリバリーの日本での導入に当たっての法的・技術的課題について調査を実施。 ■今後、eデリバリーの海外での活用事例等を含めて、調査を継続予定。

トラストサービスを巡る状況（欧州との比較）

○　国際的な電子取引等に伴うデータ流通を信頼できるものとするためにも、我が国におけるトラストサービスの枠組みについて検討するにあたっては、**諸外国の制度との整合性等についても留意**していくことが必要。

【日本】

	ヒト	組織	モノ
送信元の確認	電子署名 【電子署名法】	eシール 【eシールに係る指針】	
非改ざんの確認	タイムスタンプ 【時刻認証業務の認定に関する規程】＊		

＊　令和２年度までは民間の認定スキームのみ　⇒　令和３年度より国による認定制度の創設

【ＥＵ】

	ヒト	組織	モノ
送信元の確認	【ｅＩＤＡＳ規則＊】 電子署名	eシール	ウェブサイト認証
非改ざんの確認	eデリバリー タイムスタンプ		

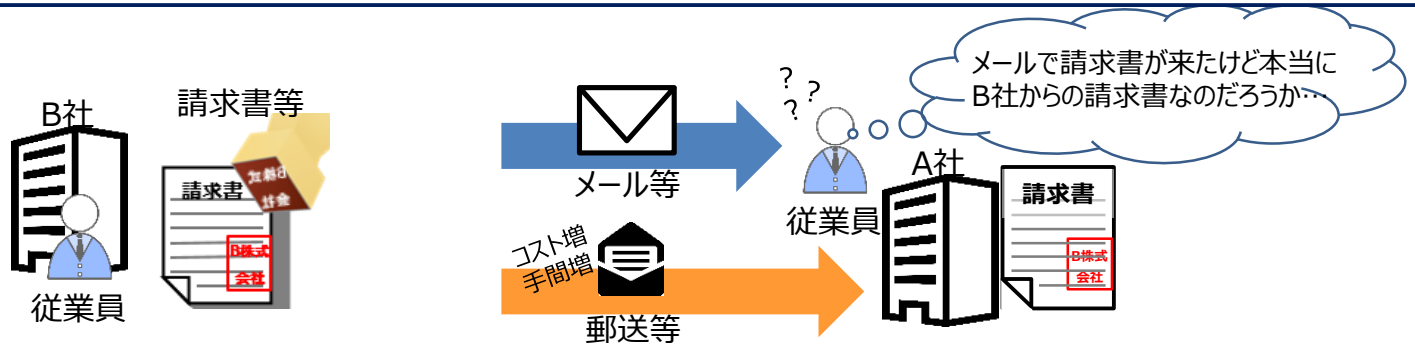
＊　EUでは、電子取引における確実性を確保し、市民、企業の経済活動の効率化を促進するため、2016年７月にeIDAS※規則を発効し、トラストサービスに関して包括的に規定。

※　electronic Identification and Authentication Services

eシールとは

- eシールとは、電子文書の発信元の組織を示す目的で行われる暗号化等の措置（技術的には電子署名と同じ仕組み）。
- 個人名の電子署名とは異なり、**使用する個人の本人確認が不要**であり、領収書や請求書等の経理関係書類等のような**迅速かつ大量に処理するような場面**において、**簡便にデータの発行元を保証することが可能**。
- eシールの活用により、**データ発行元の組織を簡便に確認**できるようになり、これまで紙で行われていた**書類等の企業間のやり取りを電子的に安全に行える**ようになり、従来の郵送の手間やコストの削減による業務効率化や生産性向上が期待される。

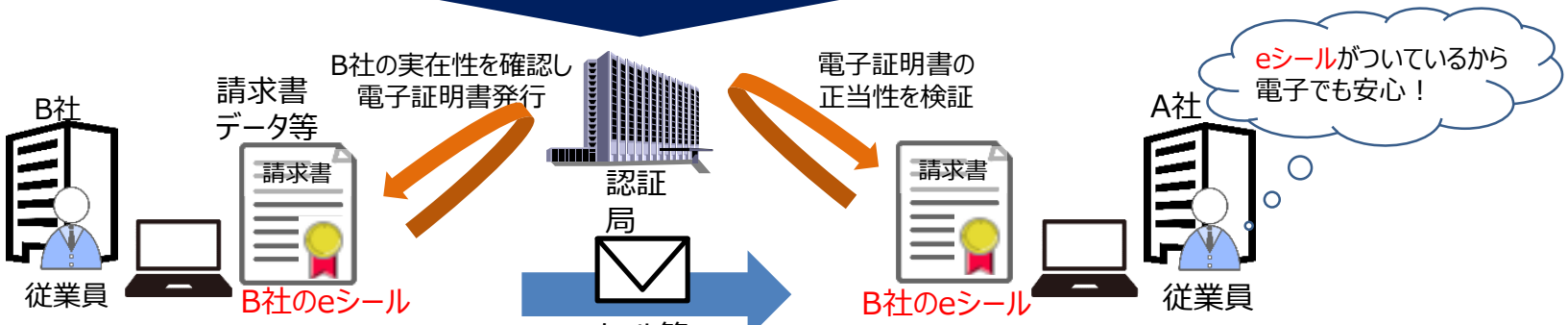
従来



B社は請求書等に会社印（角印等）を押印し、取引先（A社）に送付

請求書等を受け取ったA社は、B社の角印を確認し、請求書等の発行元がB社であることを確認

eシール



B社は請求書等のデータにB社のeシール（電子証明書は認証局が発行）を行い、メール等でA社に電子的に送付

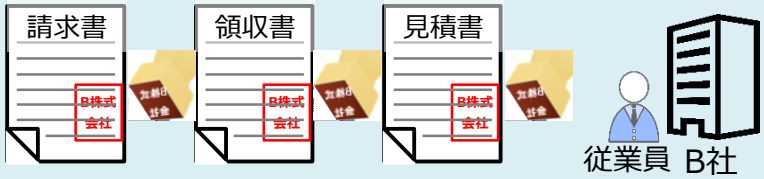
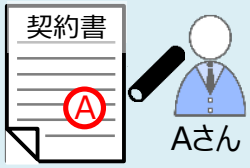
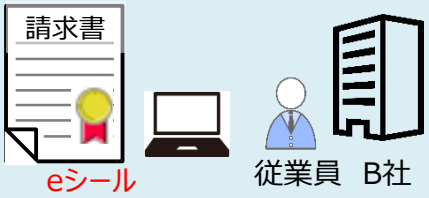
請求書等のデータを受け取ったA社は、データに行われたB社のeシールを確認（検証）し、請求書等データの発行元がB社であることを確認

eシールと電子署名の異同

eシール		電子署名
発行元の組織等	証明の対象	発行者個人
発行元の証明にとどまる場面 ex) 請求書、領収書など	使用場面	自然人としての意思表示が必要とされる用途 例）電子契約、電子申請など
無し	制度の有無	有り(電子署名法)
✓ 電子文書等への暗号化の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 ✓ 発行元を証明する機能	担保できるもの	✓ 電子文書等への暗号化の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 ✓ 本人が電子文書を作成したこと ✓ 当該文書に示された意思表示が当該本人によるものであること

eシールのメリット

- 電子署名は個人に紐づくため、人事異動等の際に新たな電子証明書の取得が必要。他方、eシールは組織に紐づくものであり、使用する個人の本人確認が不要であることから、異動等の際に再発行手続きが不要。
- 個人の意思表示のために用いられる電子署名と異なり、eシールは対象となる電子文書に機械的に迅速・大量に付すことができることから、eシールの使用により業務効率化が期待される。
- トラストサービス検討ＷＧ最終取りまとめでは、経理関係業務等においてeシール等の導入により、大企業1社あたりで、10.2万時間/月⇒5.1万時間/月の業務効率化の余地が期待できるとの試算が示された。

	組織が発行する文書 （経理関係書類 等）	個人が発行する文書 （重要な契約書 等）
実空間	 **組織に紐付く角印を押印**	 **（権限を有する代表者からの契約行為の委任に基づき）** **個人印・代表者印を押印**
サイバー空間	 **eシールを付与**	 **電子署名（＋電子委任状）を付与**

eシールのユースケース

契約に紐付いて発生する書類（領収書、請求書、見積書等）

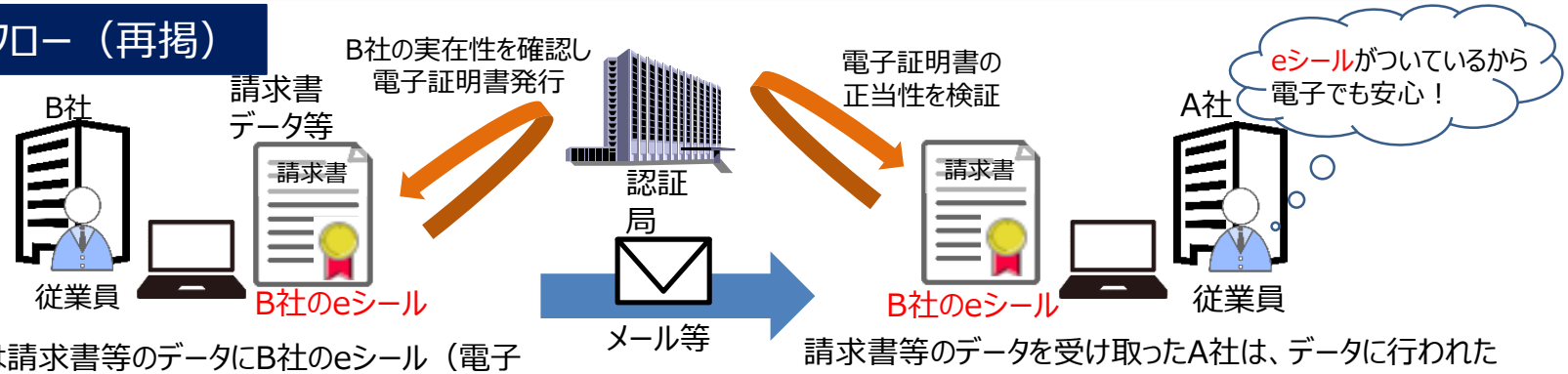
現状は…

- 押印や振込先口座番号等のチェックにより請求書の真正性を一つずつ確認している。
- 発行元や非改ざん性を保証する手段がない。

eシール導入で…

- 発行元の確認や非改ざん性を即座にデジタルで完結することが可能。
- 紙での保存コストや紛失リスクがなくなる。

eシール導入後のフロー（再掲）



B社は請求書等のデータにB社のeシール（電子証明書は認証局が発行）を行い、メール等でA社に電子的に送付

請求書等のデータを受け取ったA社は、データに行われたB社のeシールを確認（検証）し、請求書等データの発行元がB社であることを確認

eシールのユースケース

想定されるその他のユースケース例

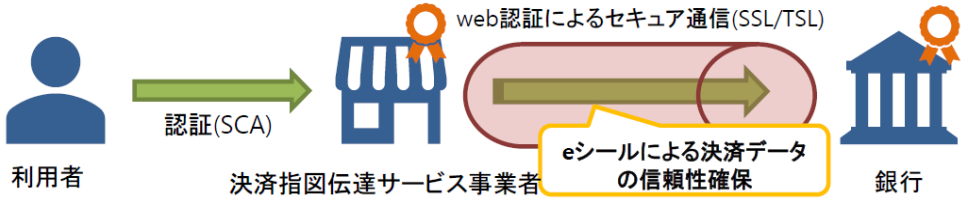
- 組織が公開する情報（決算短信、ニュースリリース 等）
- 組織が発出する証明書（レポート、在職証明書、保証書 等）
- 監査手続において、外部証跡を入手及び確認する必要のある資料
- 行政と民間との間でやり取りされる証明書・報告書

eシールのユースケース

○ EUでは、eIDAS規則に基づくeシールの普及が進みつつあり、中でも電子決済サービス等をはじめとする金融サービスや、ヘルスケア等の情報システム間のデータ交換等において、その主体及び送信情報の信頼性を確認する目的での活用が進んでいる。

例1：決済サービスでの活用

- PSD2（欧州決済サービス指令）において、2020年12月より、各種決済サービス提供者は、当該組織の正当性を確認するために認定eシール又はWEB認証を用いることが義務づけられた。
- 例えば、決済指図伝達サービス事業者※が銀行等の決済サービス提供者に利用者の情報を送付する際、当該事業者のeシールを付与するか、WEB認証によるセキュア通信を介した通信を行うことで、その決済データの信頼性を確保する必要がある。

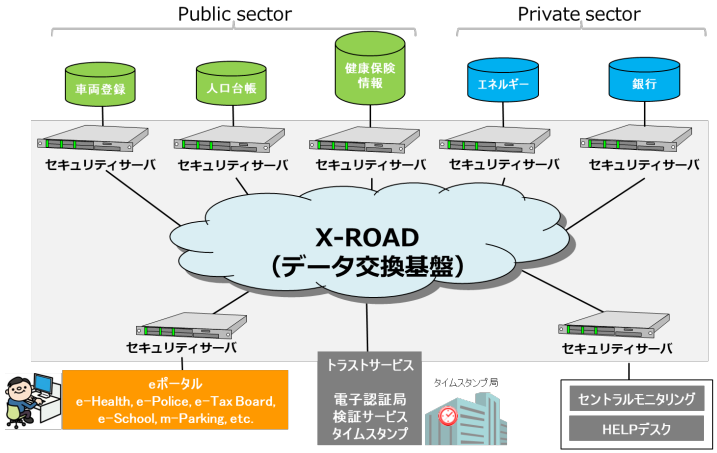


※ 利用者の依頼により、他の決済サービス提供者（銀行、電子マネー事業者、決済サービス事業者）に開設されている利用者の決済口座に係る決済指図を伝達するサービス事業者

例2：官民情報連携基盤 X-Road

- エストニアやフィンランド等で利用されている官民情報連携基盤「X-Road」は、住民登録、健康保険、金融関連情報の共有等に活用されており、データの送信時にeシール、受信時にタイムスタンプを付与することで、その情報の信頼性を担保している。
- 中でも、X-Roadシステムを用いた電子処方箋サービス（eHealthサービス）においては、各主体のeシールの付与により、病院、薬局等が、信頼性を担保した形で患者の診療情報を共有することが可能となっているため、患者は国民IDの提示のみで、薬局での薬の処方を受けることができる。

（イメージ） :X-ROADシステム



※ X-Roadでは、各情報システムがX-Roadへ接続するための条件やポリシー及び情報システムとセキュリティサーバ間のプロトコル等まで規定されている。

＜本日のアジェンダ＞

１．はじめに　～トラストサービス、eシールのご紹介～

２．eシールに関する総務省の取組

2-1 「eシールに係る指針」の作成

2-2 eシールに関する実証実験

３．eシールの今後

eシールに関するこれまでの取組

- ✓ 総務省やデジタル庁が立ち上げたWGなどにおいて、 eシールに関する検討を実施
- ✓ 総務省ではデジタル庁による取組の下、タイムスタンプに関する認定制度の運用や、eシールに関する認定制度整備の検討等の取組を実施。

2019.1

「トラストサービス検討WG」

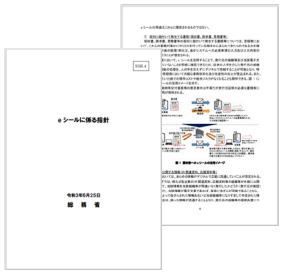
2020.4

■「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」

■eシールに関する実証実験

2021.6

「eシールに係る指針」を策定・公表



2022.7

デジタル庁にて「トラストを確保したDX推進SWG報告書」を策定・公表

「eシールに係る指針」について

- ✓ 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。
- ✓ eシールに関するより詳細な検討や制度設計については、本指針を踏まえつつも、デジタル庁でのトラストサービスの基盤となる枠組みの検討の中で具体化される見込み。

「eシールに係る指針」（令和３年６月25日公表）

第１章　eシールとは

１．１　我が国におけるeシールの定義

１．２　eシールと電子署名の異同

１．３　eシールのユースケース

１．４　eシールの仕組み

１．５　eシールの方式（ローカル/リモート）

第２章　我が国におけるeシールの在り方

２．１　eシールの分類

２．２　eシール用電子証明書の発行対象となる組織等の範囲

２．３　組織等の実在性・申請意思の確認の方法

２．４　eシール用電子証明書のフォーマット及び記載事項

２．５　認証局/利用者の秘密鍵の管理に係る基準

２．６　eシールを大量に行う際の処理

２．７　リモートeシールにおける認証

２．８　利用者におけるeシール用電子証明書の失効要求

eシールの分類

検討事項

- eシールの用途等にあわせて、レベル感を分けて検討することが必要か。

方向性

- 我が国におけるeシールは以下のようにレベル分けを行う。

レベル3：レベル2に加えて、十分な水準※1を満たしたトラストアンカー※2によって信頼性が担保されたeシール（発行元証明として機能することに関し、第三者によるお墨付き（将来的には国による認定制度等の要否を検討）があるものを想定）

主な用途例：国際取引等における証憑類、法的に保存義務が課されているデータ、排他的独占業務とされている士業の証明書等

レベル2：一定の技術基準を満たすeシール（技術的には発行元証明として十分機能することが確認できるもの）

主な用途例：行政手続における提出書類※3、民民の契約に関連する書類、IR関連資料等の公開情報等

レベル1：裸のeシール（eシールの定義には合致するが、レベル2の要件を満たす保証がないもの）

主な用途例：民民における企業間で日常的にやり取りされる電子データ全般、発行元を担保したい情報等

注） eシールのレベルを判別するための呼称については将来決定することが必要。

今後、eシールは発行元証明として様々なユースケースでの使用が期待される。

例えば、国際取引等における証憑類に使用する場面においては、当該eシールについて国際的な整合性を求められることが想定され、行政手続における提出書類等に使用する場面においては、当該eシールが一定の水準を満たしていることを求められることが想定される。

一方、eシールの普及・利用拡大の観点では、例えば、日常的に企業間でやりとりする資料等にeシールを行ったり、個人事業主や中堅・中小企業等においてeシールを活用する場面においては、低コストで簡便に利用できるeシールのニーズも想定される。

また、EUにおいては、eシール、先進eシール、適格eシールと3つのeシールが定められており、用途やeシールの効力に応じてそれぞれのeシールが使い分けられている。

これらに鑑みて、我が国におけるeシールは、**用途や活用場面に応じてレベル分けを行い、利用者自身である程度選択的にeシールを利用できるようなフレームワークにすることが適切**だと考えられる。

※1 組織等の実在性確認の方法、電子証明書のフォーマット、認証局におけるセキュリティ要件等の一定の水準

※2 インターネットなどで行われる、電子的な認証の手続きのために置かれる基点。信頼性の起点となる認証局を想定。

※3 用途によっては、レベル3が必要となるケースも考えられる

eシールの分類

【参考】各ユースケースとeシールのレベルとの関係性の一例

発出元証明による信頼性担保の必要性（高 ↔ 低）

	分類① 契約関係	分類② 組織が公開する情報	分類③ 組織が発出する証明書	分類④ 官民間のやりとり	分類⑤ 監査関係	分類⑥ その他
レベル３		• 気象データ • IR関連資料	• 資格証明書（排他的独占業務とされている士業等）等 • 商工会議所が発行する貿易関係書類 • 健康診断結果証明書	• 法令上保存義務のある書類（国税関係等） • 国への各種申請書類等	• 監査の合格証明書 • 残高証明書	
レベル２	• 領収書 • 請求書 • 【契約書】 • 見積書 • 納品書 • 受領書	• 広報資料 • 【会社法に定める議事録】 • デジタル名刺	• 生産者証明書 • 在学、卒業証明書 • 機器測定データ • 機器の保証書、ライセンス証書	• 請負、委託業務の成果物		
		• 企業間でやりとりされる一般的なデータ	• 加工証明書		• 企業文書	• 情報連携基盤・クラウド環境等でやり取りされるデータ
レベル１						

【 】内は、本来、意思表示を目的とする“電子署名”が馴染むと考えられるユースケース

主に機械的に大量に発行するものにeシールの活用が期待

eシール用電子証明書の発行対象となる組織等の範囲

検討事項

- eシール用電子証明書の発行対象となる組織等の範囲は以下のどこまでを含めることが適切か。
  - 法人、個人事業主、権利能力なき社団・財団、その他の団体等の組織
  - 事業所・営業所・支店・部門等の組織内の細かい単位
  - その他（組織に所属する個人、機器等）

方向性

- **eシール用電子証明書の発行対象は、法人 、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等の組織**とする。
- それよりも粒度の細かい、**事業所・営業所・支店・部門単位や、**担当者（意思表示を伴わない個人）**、機器については、電子証明書の任意のフィールドである拡張領域に記載**することができることとする。

eシール用電子証明書の発行対象については、対象とする組織自体の範囲や組織内のより細かい区分を含むかどうか等について検討が必要となる。

対象とする組織自体の範囲については、 eシールの普及・利用拡大の観点から、発行対象の実在性を認証局が確認できることを前提に、法人に限定せず幅広い対象を含めることが適当だと考えられる。

他方、発行対象として組織内の事業所等を含むかどうかについては、含めることに対するニーズもあるが、**認証局においてその実在性等を確認することが極めて困難である**（確認できる内容に限界があり、信頼性にも課題がある）ことや、**当該発行対象自体に変更（例えば、事業所統合・廃止や部署名の変更等）が生じた場合、その都度電子証明書の再発行が必要となることが想定され、利便性が著しく低下してしまう可能性がある**といった課題があげられる。

なお、EUにおいては、発行対象は法人であり、事業所や営業所といった細かい単位や機器等については、電子証明書の任意のフィールドである拡張領域に記載可能になっている。

これらを踏まえて、 eシール用電子証明書の発行対象は、法人 、個人（主に個人事業主を想定）、権利能力なき社団・財団、その他任意の団体等の組織とし、**事業所や営業所といった細かい単位や組織に所属する個人や機器等については、電子証明書の任意のフィールドである拡張領域に記載することができることとすることが適切**だと考えられる。

組織等の実在性・申請意思の確認の方法

検討事項

- レベル３のeシール用電子証明書の発行の際には、どのような手続・手段で確認することが必要か。

方向性

- 組織等の**実在性の確認については、登記事項証明書や第三者機関データベース等で行い、申請意思については、電子署名、押印、署名等で行うことが必要**。ただし、当該申請者（電子署名、押印、署名等をした者）が間違いなく当該組織の代表者又は代表者から委任を受けた者（委任状等によって委任を受けていることを確認できる場合に限る。）であることを確認できることが必要。
- **レベル３のeシール**の電子証明書の発行にあっては、**組織等の実在性の確認に用いるエビデンスが公的な情報に裏付けられたもの**であることが必要。

eシールは発行元証明であることから、架空の組織等のeシールやなりすましのeシールの流通を防止するため、eシール用電子証明書を発行する際には、発行対象の組織等が間違いなく実在していること（実在性）を確認し、かつ、発行申請が間違いなく当該組織に在籍する適切な権限を有した者（法人であれば代表者）によって行われたこと（申請意思）を確認する必要があると考えられる。

実在性の確認については、客観的に判断可能な情報である登記事項証明書や第三者機関が管理するデータベース等による確認が想定され、申請意思の確認については、当該組織等に在籍する適切な権限を有した者による電子署名や押印、署名等による確認が想定される。（詳細はP16参照）

ただし、レベル３のeシール用電子証明書の発行にあっては、十分な水準を満たした組織等の実在性の確認を行う必要があるため、実在性の確認は商業登記情報等の公的な機関が管理する情報に裏付けられたものであることを求めることが適切だと考えられる。なお、将来的には、データ戦略タスクフォース等他の検討の場で議論されているベースレジストリを活用して実在性の確認が行われることが望ましいと考えられる。

eシール用電子証明書の記載事項等

検討事項

- eシール用電子証明書に記載すべき事項として何が考えられるか。
- eシール用電子証明書のフォーマットはどうあるべきか。
- eシールのレベルに応じて記載事項を検討する必要があるか。

方向性

- **レベル２及びレベル３のeシール用電子証明書のフォーマットはITU-T X.509**を使用する。
- 電子証明書には、**発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子、有効期間、公開鍵、署名アルゴリズム、eシール用電子証明書の発行者、eシールのレベルを判別可能な情報、その他属性情報（営業所、事業所、機器等）等を記載**することとする。なお、レベル２で第三者（当該eシールサービスについて技術基準等を満たしているか否かの評価を行う機関）による評価を受けている場合は、評価を行った当該第三者機関を拡張領域に記載することを可能とする（レベル３の場合は、制度上明確化された認定主体であるため記載は自由）。レベル３、レベル２に関わらず、記載項目は変わらない。

レベル２及びレベル３のeシール用電子証明書のフォーマットについては、国内の類似制度（電子署名法における認定認証業務の電子証明書、商業登記電子証明書）や国際的な整合性に鑑みて、ITU-T X.509を使用することが適切だと考えられる。

eシール用電子証明書に記載すべき事項としては、発行元を示すための組織等の公式名称、当該組織等を一意に特定可能な識別子をはじめとして、電子証明書の有効期間、公開鍵、署名アルゴリズム等があげられる。

また、レベル２のeシールについては、例えば第三者による評価を受けたeシールが今後登場することも想定されるが、レベル３のeシールは認定主体が制度上明確である一方、レベル２のeシールはそもそも制度上の位置づけが明確でないため、当該eシール用電子証明書の検証時に当該eシールが第三者（当該eシールサービスについて技術基準等を満たしているか否かの評価を行う機関）による評価を受けたeシールであることが判別できるように拡張領域に記載することを認めることが信頼性確保の観点からは適切だと考えられる。

eシール用電子証明書の記載事項等

【参考】eシール用電子証明書（ITU-T X.509）の記載の一例

	フィールド名	値（サンプル）
基本領域	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	発行者を識別する情報
	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, 2022 5:00:00 PM
	サブジェクト	発行対象となる組織等の公式名称、当該組織等を一意に特定可能な識別子等
	公開鍵	RSA (2048bit)
	公開鍵パラメータ	05 00 …
拡張領域	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	eシールのレベルを判別可能な情報等
	証明書ポリシー	[1]0.4.0.194112.1.1/0.4.0.194112.1.3 [2] http://xxxxxxxxxxxxxx
	サブジェクト別名	「事業所・営業所・支店・部門名、担当者、機器」や「組織等の和文商号」等
	CRL配布ポイント	http://xxxxxxxxxxxxxxxxCA.crl
	基本制約	Subject Type = End Entity
	鍵使用目的	Non-Repudiation (40)

eシールを大量に行う際の処理

検討事項

- レベル３のeシールにおいて、複数の対象データに一括でeシールを行うことを認めるか。

方向性

- レベル３のeシールにおいて、複数の対象データに一括でeシールを行うことを認めることが適当。

eシールにおいては、**業務効率化の観点から、**ローカル/リモート方式に限らず機械的に**複数の対象データ（例えば領収書等）に対して一括でeシールを行うことに対するニーズがある。**

一括処理について、我が国における**実空間での手続では、複数の対象文書（例えば委嘱状等）に対して、まとめて処理（決裁・押印）することは一般的に実施されている。**

また、EUの適格eシールにおいては、ローカルeシールについては特段の規定がないが、リモートeシールについてはCENの技術基準において、複数の対象データに一括で署名（eシール）指示することが認められている。

eシールの普及・利用促進の観点や国内における実運用、EUの制度を踏まえ、そもそもeシールは意思表示を伴わず、発行元証明にとどまるということに鑑みて、レベル３のeシールであっても、複数の対象データに一括でeシール行うことを認めることが適当だと考えられる。

ただし、一括でeシールを行う際には、当然利用者が指定したデータのみにeシールが行われることが求められることから、利用者が対象データに対してeシールを行う指示を行って以降、他のデータが紛れ込むことがないことはeシールサービス側で担保する必要がある。

＜本日のアジェンダ＞

１．はじめに　～トラストサービス、eシールのご紹介～

２．eシールに関する総務省の取組

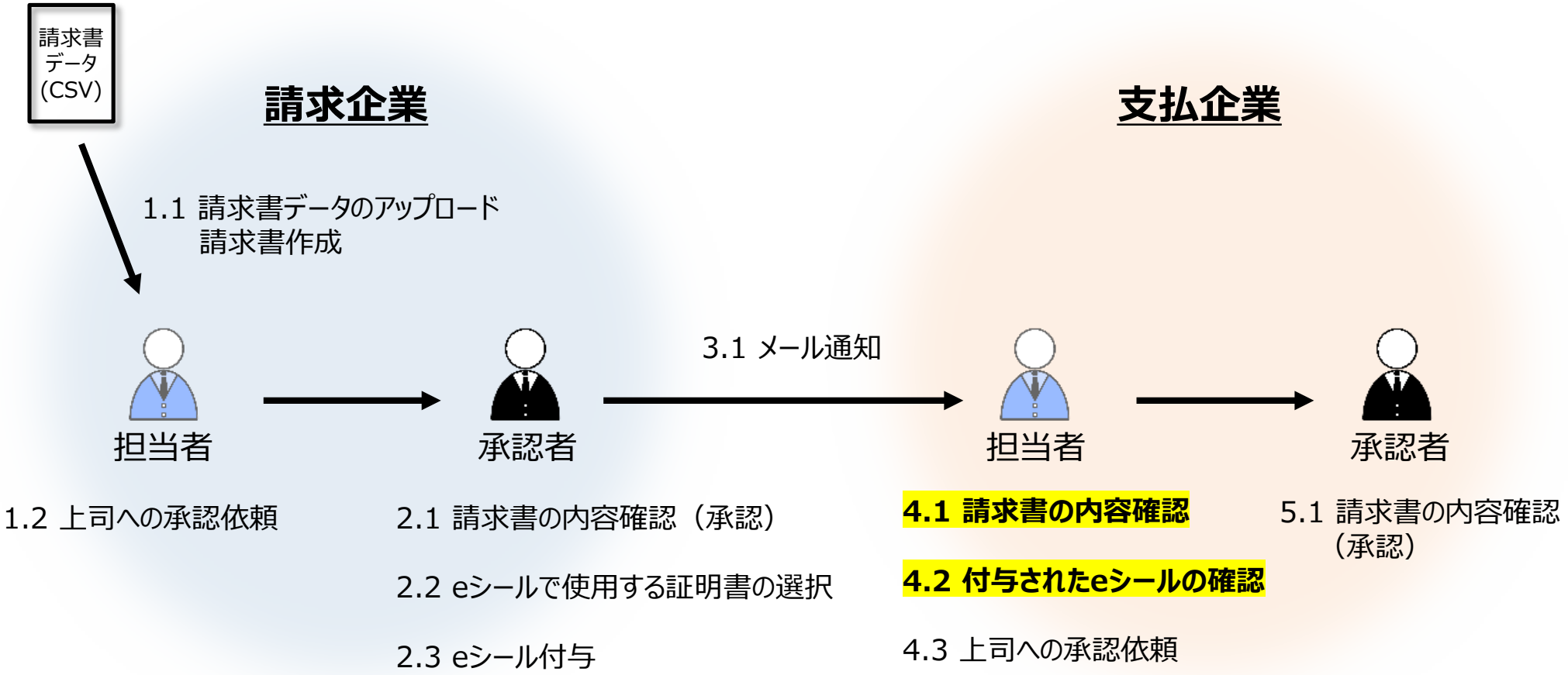
2-1 「eシールに係る指針」の作成

2-2　eシールに関する実証実験

３．eシールの今後

eシールに関する実証実験

- 2020年、総務省においてeシールに関する実証実験を実施
- 実験内容は、企業間の商取引で行われる「請求（支払通知）プロセス」において、電子化された請求書にeシールを付与して請求書の発行企業および受領企業における業務効率化の効果を調査するもの。



eシールに関する実証実験

- 企業における請求書の真正性確認について、eシールを導入した場合の実証実験を実施したところ、98.90%から99.97%という圧倒的な工数削減率となった。
- 業種や規模に関係なく大幅な工数削減が見込まれ、請求書業務へのeシールの適用が有効なものと考えられる。

参加企業		現行業務		電子化後	
企業	業種	通数	工数	工数	工数削減率
A社	情報サービス	10000 (枚/月)	720.0 (h/月)	1.9 (h/月)	99.73%
B社	情報サービス	2500 (枚/月)	1014.0 (h/月)	0.5 (h/月)	99.95%
C社	金融	350 (枚/月)	5.8 (h/月)	0.1 (h/月)	98.27%
D社	食品卸	15000 (枚/月)	回答なし	2.9 (h/月)	–
E社	製造業	10000 (枚/月)	回答なし	1.9 (h/月)	–
F社	情報サービス	3000 (枚/月)	52.8 (h/月)	0.6 (h/月)	98.90%
G社	リース	40 (枚/月)	30.0 (h/月)	0.1 (h/月)	99.77%
H社	情報サービス	–	–	–	–

総務省令和2年度調査委託事業における調査結果

＜本日のアジェンダ＞

１．はじめに　～トラストサービス、eシールのご紹介～

２．eシールに関する総務省の取組

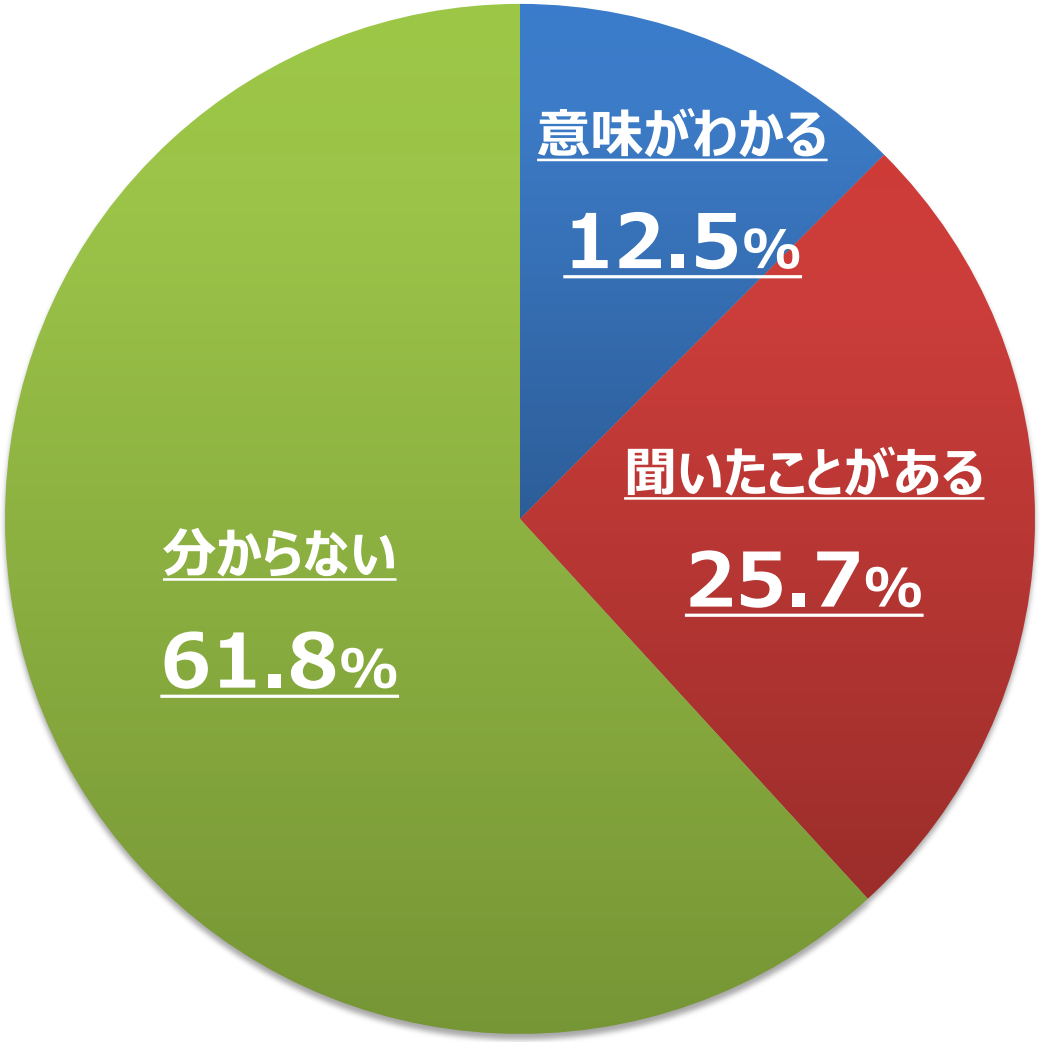
　2-1 「eシールに係る指針」の作成

　2-2 eシールに関する実証実験

３．eシールの今後

eシールの今後

eシールの認知状況



総務省令和3年度調査委託事業における調査結果

eシールの分類（再掲）

検討事項

- eシールの用途等にあわせて、レベル感を分けて検討することが必要か。

方向性

- 我が国におけるeシールは以下のようにレベル分けを行う。

レベル３： レベル２に加えて、十分な水準※1を満たしたトラストアンカー※2によって信頼性が担保されたeシール（発行元証明として機能することに関し、第三者によるお墨付き（将来的には国による認定制度等の要否を検討）があるものを想定）

主な用途例：国際取引等における証憑類、法的に保存義務が課されているデータ、排他的独占業務とされている士業の証明書等

レベル２： 一定の技術基準を満たすeシール（技術的には発行元証明として十分機能することが確認できるもの）

主な用途例：行政手続における提出書類※3、民民の契約に関連する書類、IR関連資料等の公開情報等

レベル１： 裸のeシール（eシールの定義には合致するが、レベル２の要件を満たす保証がないもの）

主な用途例：民民における企業間で日常的にやり取りされる電子データ全般、発行元を担保したい情報等

注） eシールのレベルを判別するための呼称については将来決定することが必要。

今後、eシールは発行元証明として様々なユースケースでの使用が期待される。

例えば、国際取引等における証憑類に使用する場面においては、当該eシールについて国際的な整合性を求められることが想定され、行政手続における提出書類等に使用する場面においては、当該eシールが一定の水準を満たしていることを求められることが想定される。

一方、eシールの普及・利用拡大の観点では、例えば、日常的に企業間でやりとりする資料等にeシールを行ったり、個人事業主や中堅・中小企業等においてeシールを活用する場面においては、低コストで簡便に利用できるeシールのニーズも想定される。

また、EUにおいては、eシール、先進eシール、適格eシールと３つのeシールが定められており、用途やeシールの効力に応じてそれぞれのeシールが使い分けられている。

これらに鑑みて、我が国におけるeシールは、**用途や活用場面に応じてレベル分けを行い、利用者自身である程度選択的にeシールを利用できるようなフレームワークにすることが適切**だと考えられる。

※１ 組織等の実在性確認の方法、電子証明書のフォーマット、認証局におけるセキュリティ要件等の一定の水準

※２ インターネットなどで行われる、電子的な認証の手続きのために置かれる基点。信頼性の起点となる認証局を想定。

※３ 用途によっては、レベル３が必要となるケースも考えられる

ご静聴ありがとうございました。

総務省

Ministry of Internal Affairs and Communications