

eシール及びeデリバリーについて

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

概要

1. トラストサービスの法的裏付けについて
2. eシール（電子署名との比較）
 - A) eシールのコード署名における利用シーン
 - B) eシールの実際の利用例 X-Road, PSD2
3. eデリバリーの定義、法的効力
 - A) eデリバリーの利用シーン
 - B) eデリバリーの実際の利用例
 - i. 政府における利用
 - ii. De-Mail、民間における利用
4. 日本における検討に向けた課題と提言

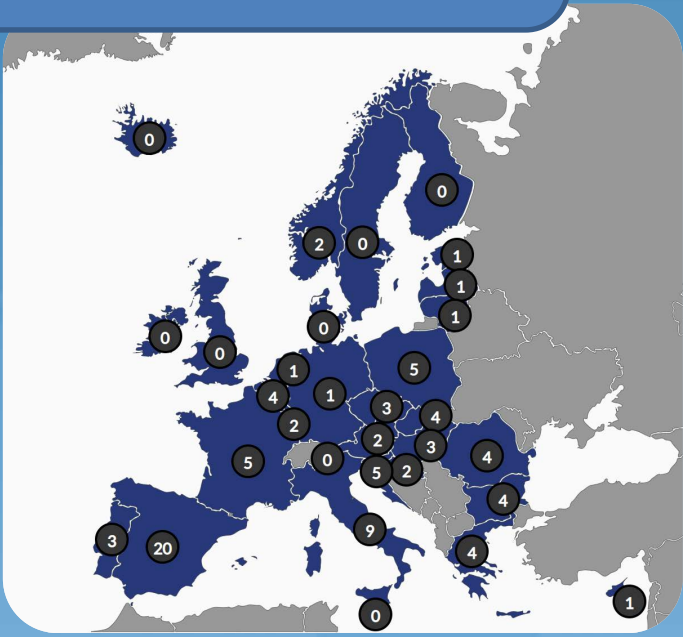
欧州におけるeシール

eシールと電子署名のeIDAS規則における比較

	eシール	電子署名
利用者	法人	自然人
定義	電子データの完全性と起源を保証するもの	署名者が署名として行うもの
法的効力	<p>適格eシール データの起源(origin)と完全性(Integrity)の推定</p> <p>その他のeシール 電子形式である、適格eシールでないという理由で法的効力が否定されない</p>	<p>適格電子署名 手書き署名と同等の法的効力</p> <p>その他の電子署名 電子形式である、適格電子署名でないという理由で法的効力が否定されない</p>
適格性の要件	適格電子証明書 + 適格eシール生成装置 + 先進eシール	適格電子証明書 + 適格電子署名生成装置 + 先進電子署名
利用用途	タイムスタンプ、コード署名、電子インボイス、サーバ/IoT間のデータ交換等	電子契約、電子申請、eTax、S/MIME等

技術的にはeシールと電子署名は同じ仕組み
つまり電子データの作成者と、電子データが改ざんされていないことを保証する仕組み

EUでは電子署名は自然人による行為である定められている。一方で法人にも署名相当の行為のニーズがあるため、新たにeシールが定義された。
例えば:タイムスタンプ、インボイス、コード署名等



eシール用証明書を発行する認証局: 87社 (2019年3月17日時点)
ソース: <https://www.eid.as/fileadmin/eidas-tsp-map/>

eシール - コード署名における利用シーン

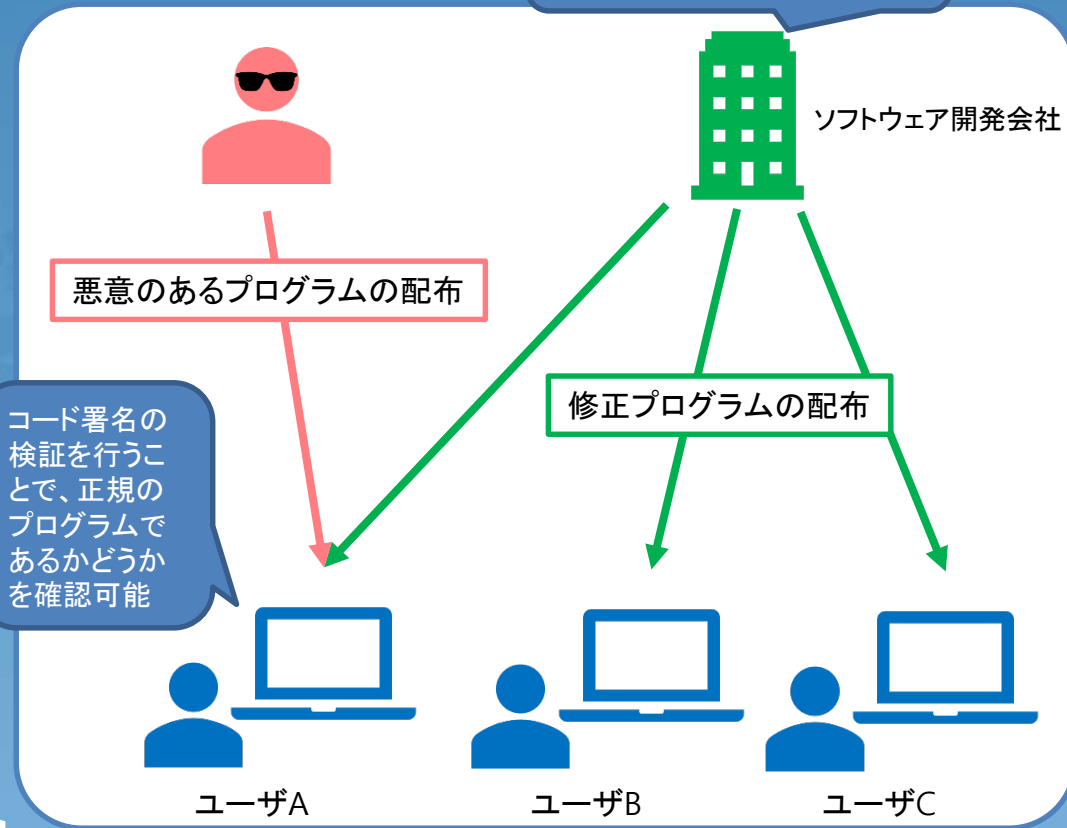
修正プログラムの信頼性を保証する為に、コード署名を実施

コード署名における課題

1. 自然人の電子証明書を利用する場合、担当者毎に電子証明書を管理する必要があり、管理コストが高い
2. 組織、法人の電子証明書を利用する場合、法律

eIDAS規則によって、法人向け電子証明書で電子署名相当であるeシールが可能となり、その法的効力も承認されている。

*コード署名の検証は現在はOS上や、ブラウザによって実施されることが多いが、今後は自動車におけるOTA(Over the Air)によるアップデート等、一般的なOSやブラウザに依らない検証が増加することが予測される。その際の検証方法については今後の検討課題である。



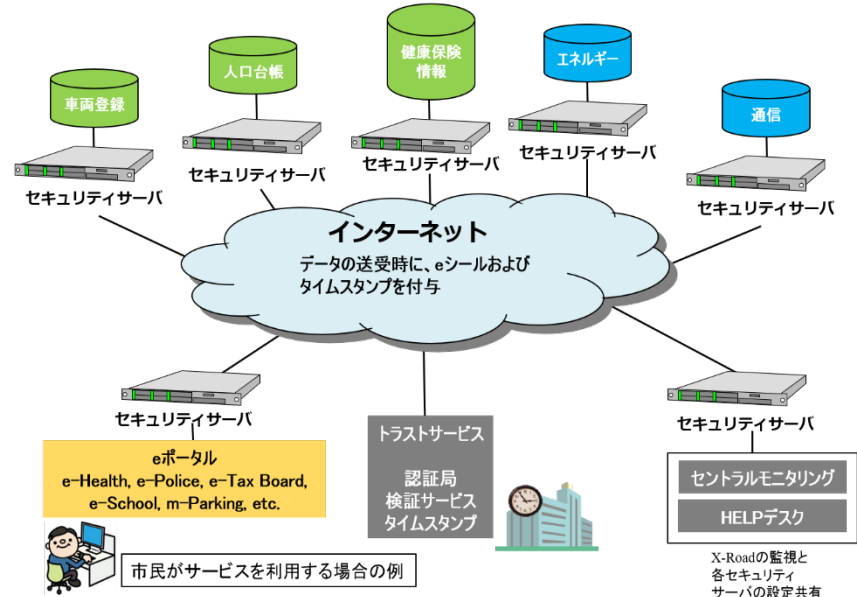
eシールの利用例-X-Road

エストニア、フィンランド、キルギスタンで利用されている官民情報連携基盤X-Roadでは、情報の真正性と完全性確保にeシールが利用されている。

各セキュリティサーバーには、eシール証明書が格納されており、セキュリティサーバーからの情報送信時にeシールを付けている。

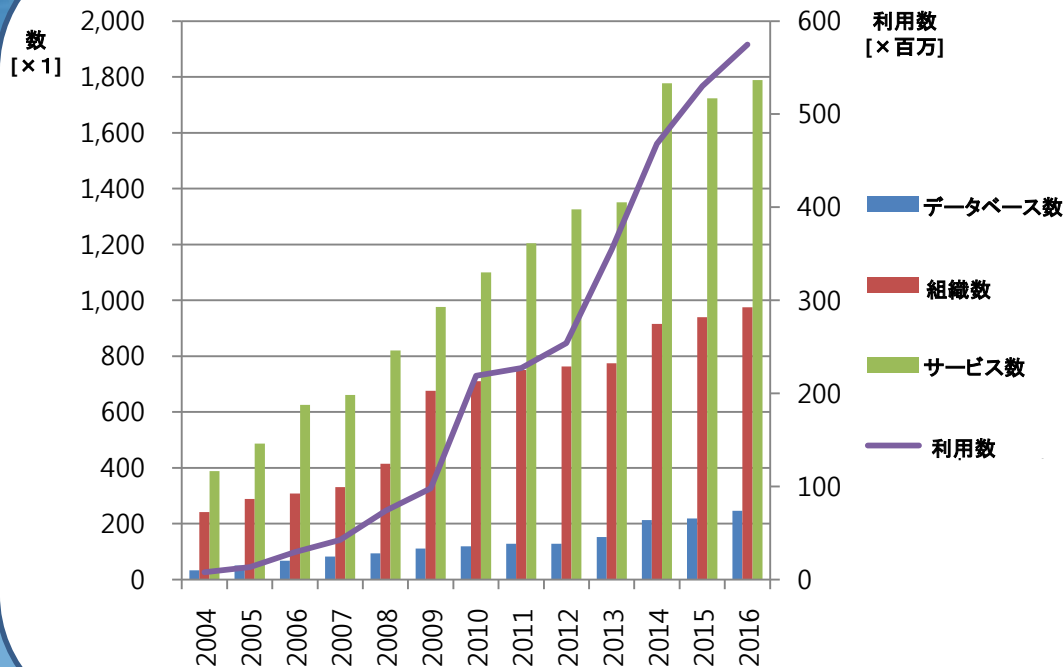
2018年のリクエスト数:
985,878,107件

X-Roadに接続されている組織数:
民間組織:412社
公的機関:258機関



X-Roadの利用数の推移

利用数の統計データは2016年時点で約5億5千万件、2018年は9億8千万件と右肩上がり



2019年2月のサービス利用数TOP5

10,733,277 電子処方箋
9,932,798 従業員登記
7,781,552 電子カルテ
7,257,980 人口統計台帳
4,763,416 交通統計台帳

COSMOS

PROFESSIONALS OF SAFETY ENGINEERING

*平成29年度 タイムスタンプや電子署名等のトラストサービスの
利用動向に関する調査報告より

X-Roadで実現されている電子処方箋

X-Roadにおける課題

X-Road上の官民情報システム連携には、互いに信頼できるシステムであることが前提条件となる。

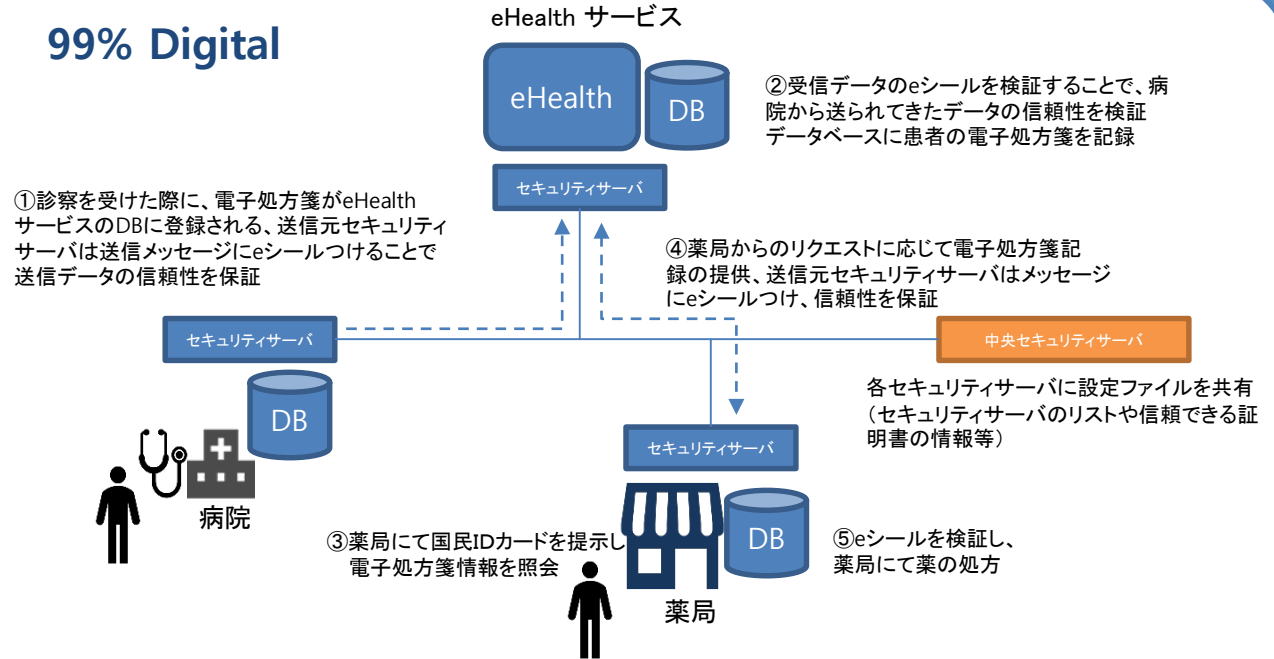
その信頼性の証拠として送信メッセージにeシールが利用されている。

eシール付きのメッセージは、受信側で証拠としてタイムスタンプを付けて保存している。

また、eシールは電子署名と異なり生成者の同意を必要としないため、**自動処理**が可能。

X-Road上の実際のトラフィックの95%は人が介在していない。

99% Digital



Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

決済サービス指令 (PSD2)

1. 欧米における法制度の全体像

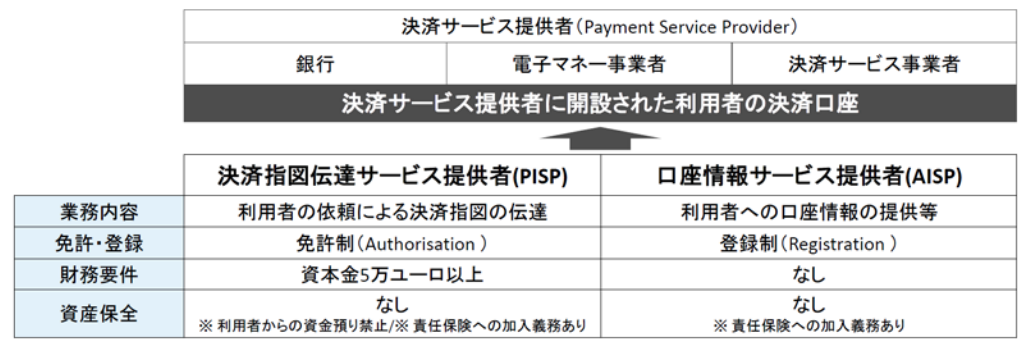
PSD2は銀行のAPIをオープン化し、利用者から委託の受けた中間事業者が銀行APIにアクセスできるようにすることで金融サービスにおけるイノベーションを促進することが狙い。

口座情報サービス提供者は利用者の同意を得て複数の口座情報へアクセスすることで、より高度な分析が可能になる。

決済指図伝達サービス提供者も、利用者の同意に基づき、銀行口座に決済指示を出せることになり、金融機関以外の事業者の参入がより容易になり、市場の刺激となる。

一方で、これらの中間事業者についても登録性となっており、加盟国の金融当局から認可番号を取得する必要がある。

- PSD2は、以下の業について、新たに規制の枠組みを整備。
 - ① 決済指図伝達サービス提供者 (PISP: Payment Initiation Service Provider) : 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 (第4条第15項)
 - ② 口座情報サービス提供者 (AISP: Account Information Service Provider) : 利用者が、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1つ又は複数の決済口座の情報を統合して提供するオンラインサービス (第4条第16項)



- また、これに関連して、
 - ① 無権限取引や決済の実行に瑕疵があった場合の中間的業者と銀行等の損失分担ルールや、
 - ② 不正取引等の場合には、銀行等は、中間的業者からのアクセスを拒否できるといった規定を設ける一方、そうした場合以外では、銀行等が顧客による中間的業者経由の決済指図に応じるよう求めるとともに、銀行等による中間的業者の不当な取扱いを禁止するなど、オープンAPIの取組みと統合的な規定が整備されている。

PSD2(決済サービス指令)

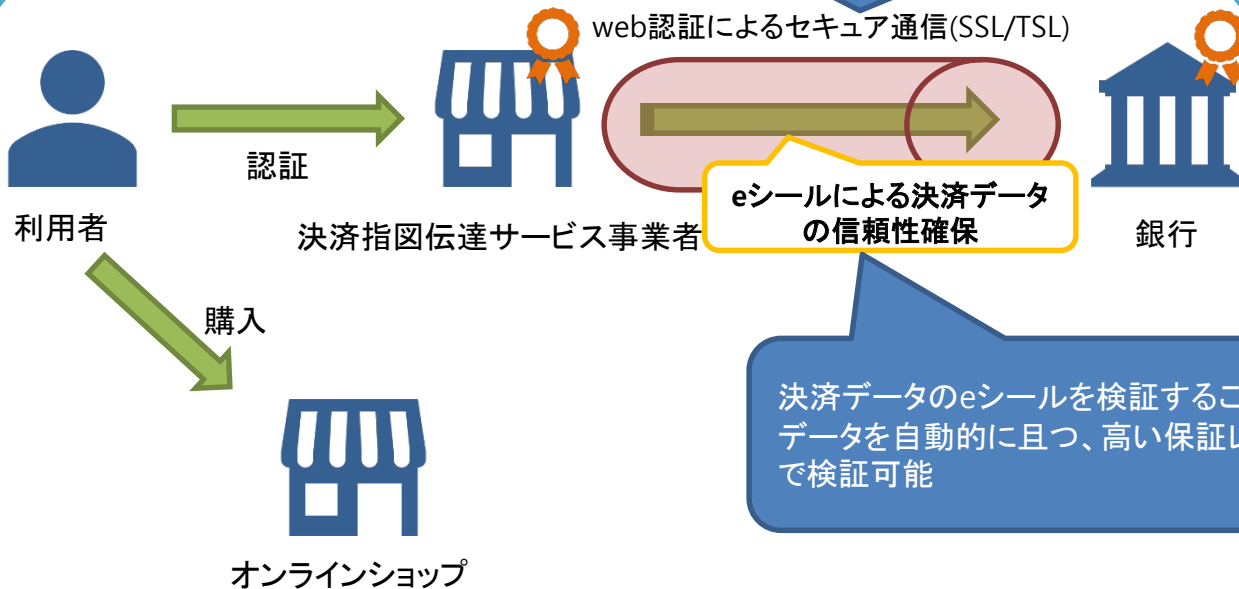
Web認証証明書に規制当局からの認可番号を追記することで、認可された事業者であることを自動的に認証可能

PSD2における課題

決済指図伝達サービス事業者は銀行と直接契約関係にないので、通信時に銀行に対して認可された事業者であることを認めてもらう必要がある。

決済指図伝達サービスには、ヒトの介在が少なく、自動処理可能な形の信頼性構築が必要。

証拠能力の高い方法で決済データを保管することが必要。



決済データのeシールを検証することでデータを自動的に且つ、高い保証レベルで検証可能

欧州におけるeデリバリー

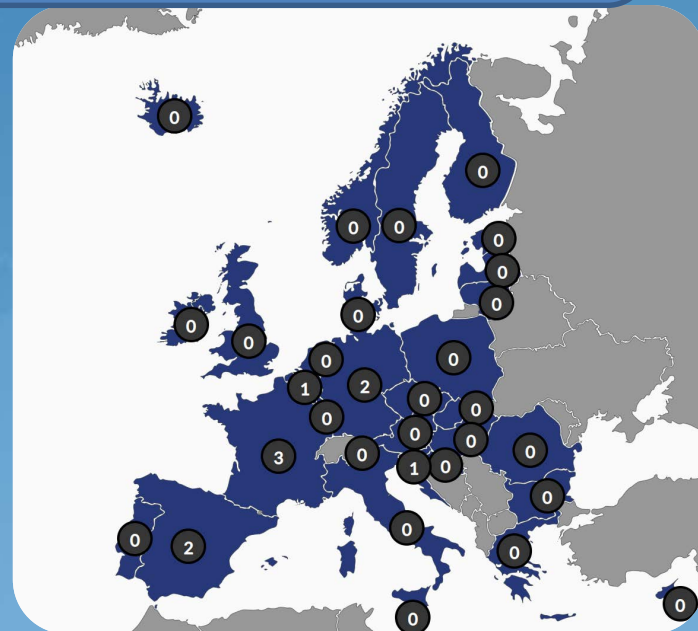
eIDAS規則以前からeデリバリーサービスは既に存在していた(ドイツ、チェコ等)が、法律が存在しない国もあり、また、国境を越えたサービスの提供の為にはeIDAS規則で法的効力を認める必要があった

eデリバリーの定義:

「eデリバリーサービス」とは電子手段により第三者間でデータを送受信し、送信されたデータの取扱いに関する証拠を提供するサービスを言う。取扱いに関する証拠データの送受信を含み、そのデータを損失リスクや窃盗、不正な変更から守るものである

送受信者の識別とデータの送受信日時 of 正確性、送受信データの完全性を保証する(ハッシュ値を保存)

eデリバリーサービスを提供している事業者数:9社



eデリバリーを提供している事業者

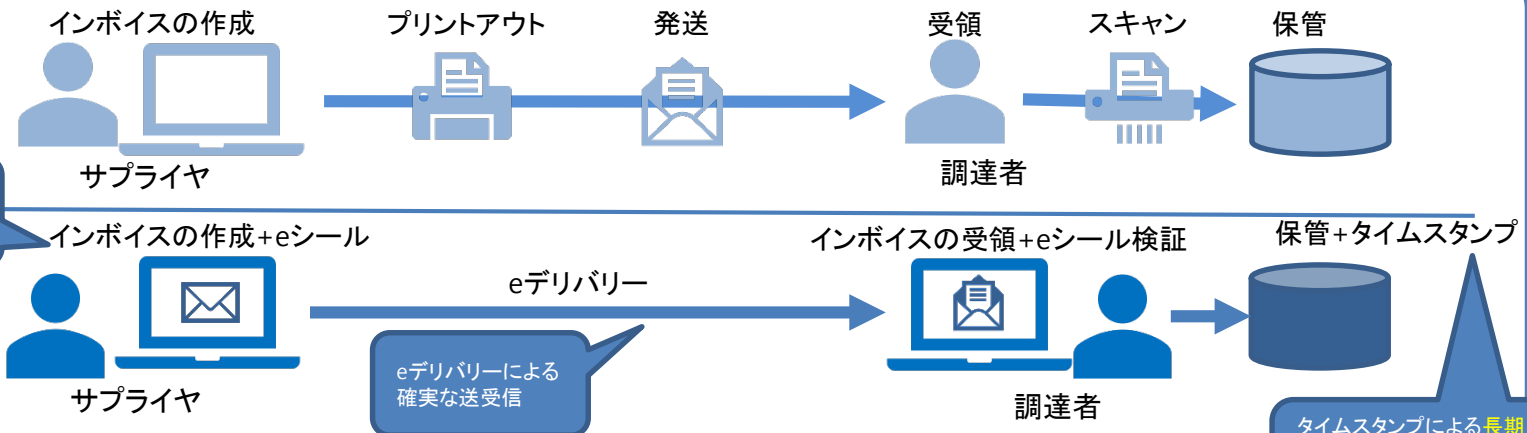
事業者名	説明
Connect Solutions	ベルギーのサービスプロバイダ eデリバリーサービスとして“Aangetekende.email™”を提供
1&1 De-Mail GmbH	ドイツの3つの個人ユーザ向けDe-Mailプロバイダの1つ この他、Deutsche Telekom、Mentana-Claimssoft GmbH がある
Deutsche Post AG	ドイツに拠点を置く多国籍企業、約220か国の郵便・物流を担っている
EDICOM CAPITAL, S.L.	世界的規模でサービスを提供しているサービスプロバイダ EDIテクノロジー(Electronic Data Interchange)またはe-Invoicingによる企業間のデータ転送のためのプラットフォーム開発を行っている
LLEIDANETWORKS SERVEIS T ELEMATICS, S.A.	スペインのインターネットアクセスサービスプロバイダ 電子通知、契約プロセスでの認証等のデータ検証ソリューションを提供
AR24	フランスで最初のeIDAS認定メールサービスプロバイダ
Equisign	フランスのデジタルセキュリティを専門とするソフトウェア企業 製品の1つとして、“LetReco(電子書留)”を提供
TESSI DOCUMENTS SERVICES	フランスのサービスプロバイダ 電子署名サービス “Tessi SIGN”を提供
EIUS d.o.o.	スロバニアのサービスプロバイダ eデリバリーサービスとして“VEP.si”を提供

eシール及びeデリバリー - 電子インボイスにおける利用シーン

電子インボイスの課題
保管されたインボイスは監査対象となり、**起源と完全性**に加えて**可読性**、
特に監査効率を考慮すると**機械可読性が重要**となる。

欧州ではインボイスのデータモデルの標準化が進んでいる。
2015年の欧州全体でのインボイス数：**約350億**(凡そ半分がB2B/B2G/G2B)*

eシールでインボイスの**起源と完全性**を保証



タイムスタンプによる**長期保存**(保管期間終了時までの**起源、完全性、可読性の保証**)

*ソース：<https://www.billentis.com/>

EU加盟国政府におけるeデリバリーの利用数

eデリバリー 2015年Q3以降 凡そ2億件の文書が交換されている

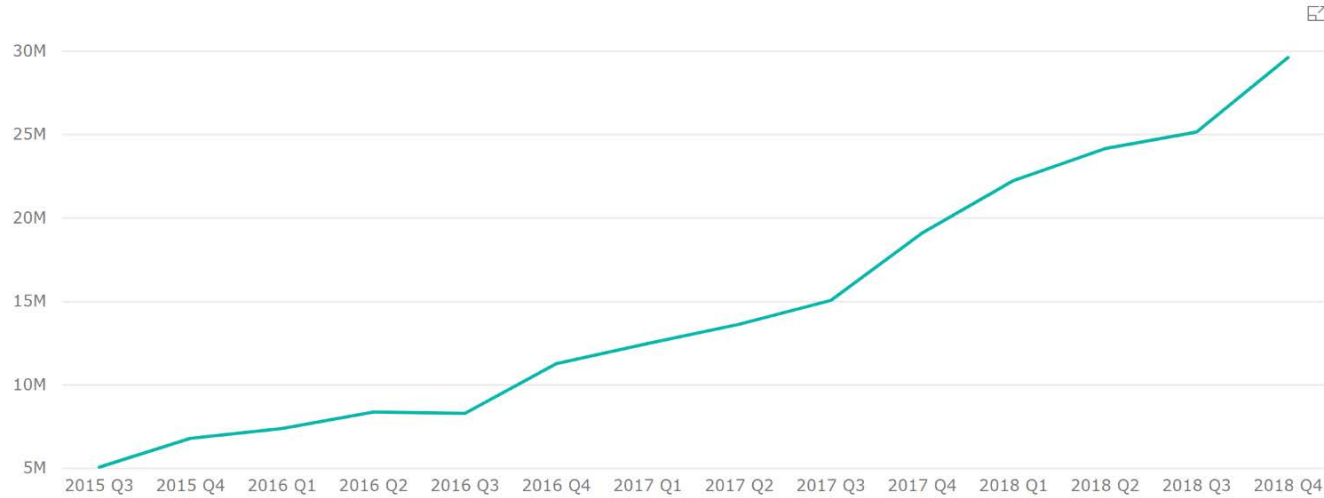
各加盟国は以下のプロジェクトにおいて、eデリバリーを利用し、文書交換を行っている。

右の統計データは下記プロジェクトの統計データの合算である。

- BRIS (Business Registers Interconnection System: 事業者登録相互接続システム)
- EESSI (Electronic Exchange of Social Security Information: 社会保障情報の電子交換)
- ENTSOG (European Network of Transmission System Operators for Gas: 欧州ガス輸送システム事業者ネットワーク)
- EU Common Entry Gate: たばこ製品に関する情報提供のためのEU共通エントリーゲート)
- Me-CODEX (Maintenance of e-Justice Communication via Online Data Exchange: EUの法的手段のアクセス改善などを目的としたオンラインデータ交換によるコミュニケーションの維持)
- OpenPEPPOL (Open Pan-European Public Procurement OnLine: オープンな汎ヨーロッパ公調達オンライン)

Evolution of the total number of exchanged documents

This chart shows the evolution of the total number of exchanged documents.



Cosmos

PROFESSIONALS OF SAFETY ENGINEERING

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Uptake+-+view+eDelivery+-+Access+Points>

eデリバリーの例: De-Mail

・2011年のDe-Mail法に基づくサービス

・現在適格eデリバリーサービスとして認定されている。

利用組織数: 1916組織

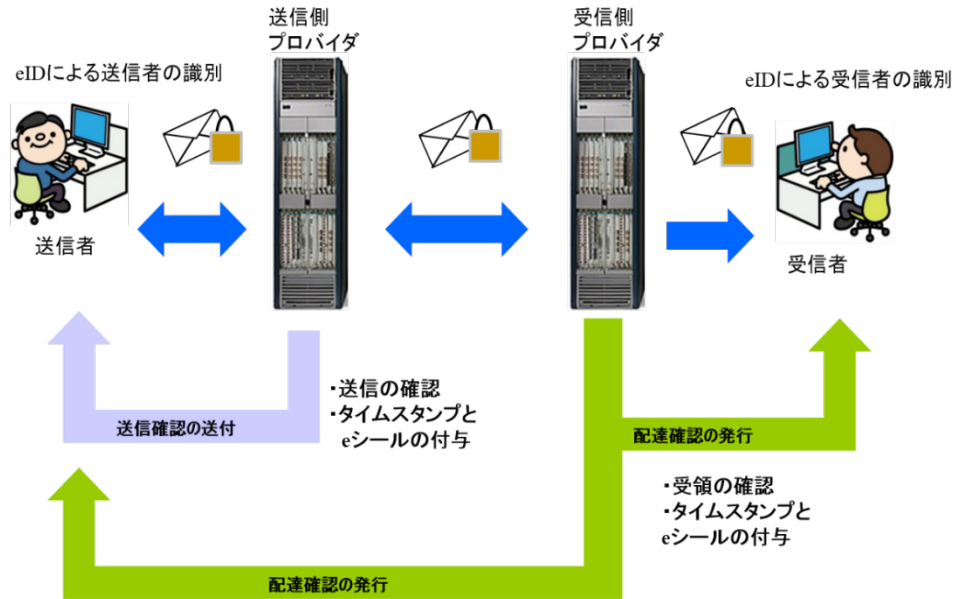
総アカウント数: 約100万アカウント

B2Gのユースケース

- ・不動産事業者の許可申請
- ・商業登記申請
- ・会社の設立申請

C2Gのユースケースとして

- ・住宅給付申請
- ・税額の査定申請
- ・廃棄物申請
- ・車両登録
- ・ドッグライセンス申請
- ・教育支援申請



De-Mailの利用例

ERGO社

欧州最大の保険グループ企業

保険契約事項に係る連絡をDe-Mailで実現

ERGO



HEINZ VON HEIDEN社

ドイツの建築会社

建築計画における迅速なコミュニケーションの実現

見積書、契約書、修正依頼書等をDe-Mailで交換



Allianz社

ドイツミュンヘンに本社を置く世界有数の金融グループ

生命保険、健康保険及び株主総会に係る連絡をDe-Mailによって実現



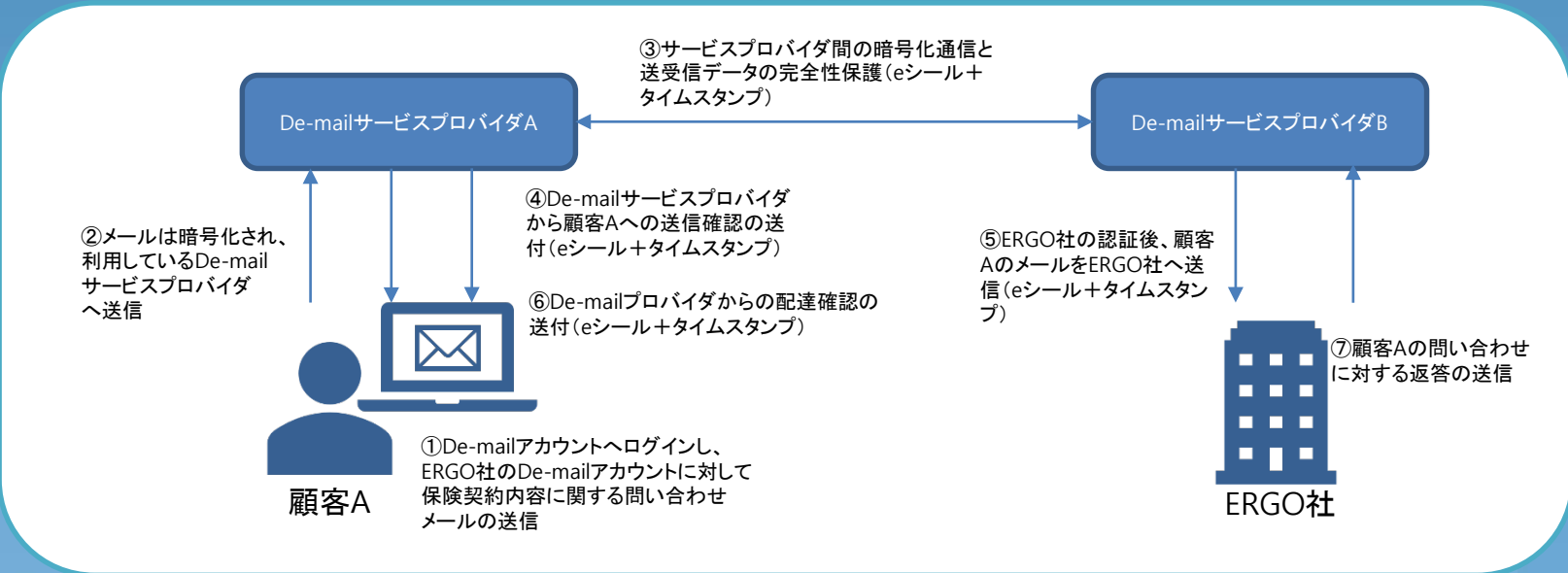
利用民間企業数141社

ソース:<https://www.de-mail.info/>

De-Mailの利用例 ERGO社

顧客の契約情報については、機微な情報であり本人確認が取れなければ返答すべきでないが、De-mailによって送信者（顧客A）が特定されており、かつ返答が確実に顧客Aに到達することが保証されているので、機微な情報であってもメールベースでのやり取りが可能になる。

eデリバリーは、電子署名、eシール、タイムスタンプといった技術の組み合わせで提供されるが、eデリバリーサービス提供者自身の信頼性の保証も考慮する必要がある。



日本におけるeシール、eデリバリーに対する課題と提言

1. Society5.0の目指す世界では、IoT/サーバ間の信頼性構築がより重要となるので自動生成可能、機械可読可能なeシールの仕組みを考える必要がある。
2. 1. に関連して、ブラウザやOSに依らないeシールの検証方法についても考慮すべきである。
3. 我が国において法人の署名行為が認められるか否かは不明瞭である。
4. 認証局およびタイムスタンプ局の信頼性保証に加えて、eデリバリーのサービス提供者の信頼性保証も検討するべきである。