



総務省におけるeシールの制度化に向けた取組

総務省 サイバーセキュリティ統括官室

1. はじめに

通信インフラの高度化やデジタルサービスの普及・多様化により、我が国のネットワーク上でのデータ流通量が飛躍的に増大している中、電子データを安心・安全に流通できる基盤として、電子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活用が期待される。とりわけ、業務効率化や生産性向上の観点から、企業等が発行する電子データの発行元を証明する「eシール」の活用が期待される。

このような背景から、総務省では2021年6月にeシールに係る技術や運用等に関する一定の基準を示した「eシールに係る指針」を策定したが、国による認定制度など適合性評価の枠組みが存在しないこと等もあり、依然としてeシールの世間的な認知度は高くない状況である。

そこで、eシールの更なる普及を促す観点から、2023年9月から「eシールに係る検討会」（以下、eシール検討会）を開催し議論を進めた結果、2024年4月に総務大臣によるeシールに係る認定制度の創設等を内容とする「最終取りまとめ」を公表するとともに、「eシールに係る指針（第2版）」を公表した。

2. eシールとは

2.1 トラストサービスとは

我が国の「トラストサービス」については、総務省が公表した「プラットフォームサービスに関する研究会トラストサービス検討ワーキンググループ最終取りまとめ」において、「インターネット上における人・組織・データ等の正当性を確認し、改ざんや送信元のなりすまし等を防止する仕組み」と定義されている。

Society5.0の到来や我が国が提唱するDFFT（Data Free Flow with Trust）の実現に向けて、トラストサービスは電子データを安心・安全に流通できる基盤として、重要な役割を担うことが期待されており、「デジタル社会の実現に向けた重点計画」（2023年6月9日閣議決定。以下、重点計画）などの各種政府方針において重要課題と位置付けられている。

2.2 eシールとは

eシールは、企業等が発行する電子データの発行元を証明し、また、電子データに改ざんがないことを証明できるようにするために用いられる。我が国におけるeシールの定義は以下のとおりとする。

「eシール」とは、電磁的記録（電子的方式、磁気的方式その他の知覚によっては認識することができない方式で作られる記録であって、電子計算機による情報処理の用に供されるものをいう。）に記録された情報（以下、電子データ）に付与された又は論理的に関連付けられた電子データであって、次の要件のいずれにも該当するものをいう。

- 一 当該情報の出所又は起源を示すためのものであること。
- 二 当該情報について改変が行われていないかどうか確認することができるものであること。

なお、電子データの発行元となる組織等に紐付く「eシール」は、意思表示という性質から利用者たる自然人との紐付きが強固である電子署名とは異なり、組織内の人事異動に伴ってeシール用の電子証明書を再発行する必要がないことや、意思表示を伴わないため、大量の電子文書等に機械的、自動的にeシールを行うこともできること等のメリットがあるが、eシールが行われた電子文書等にはeシールを行った自然人の意思は顕れていないことに留意する必要がある。

2.3 eシールのユースケース

eシールを用いることで、発行元の組織等の確認や電子文書等の改ざんの有無の確認を簡便に行うことができるようになるため、これまで人手を介して紙で行われていた書類等の企業間のやりとりを電子的に安全に行え、機械的、自動的に処理することもできるようになり、業務効率化や生産性の向上が期待される。

eシールの活用が見込まれる分野としては、企業間取引関係、組織が公開する情報、組織が発出する証明書、官民間のやりとり、監査関係等が考えられる。例えば、組織

が発出する証明書としては、排他的独占業務とされている士業等の資格証明書が該当し、これらはトラストが確保されていることに関して高い信頼性を有することが求められるため、認定を受けたeシール用認証業務によって保証されたeシールの活用が見込まれる。

3. 政府におけるeシールに係る検討経緯

2019年1月から同年11月にかけて総務省で開催された、「プラットフォームサービスに関する研究会」の下の「トラストサービス検討ワーキンググループ」の「最終取りまとめ」での提言を踏まえて、2020年4月から2021年6月にかけて、「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」を開催し、eシールに係る技術や運用等に関する一定の基準を示す「eシールに係る指針」を策定した。

デジタル庁は、2021年11月から2022年6月にかけて、「データ戦略推進ワーキンググループ」の下で「トラストを確保したDX推進サブワーキンググループ」を開催し、トラストを確保したDXの具体的な推進方策について検討が行われた。同サブワーキンググループの「報告書」においては、「eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現に向け、総務省の取組を支援すべきである。」とされた。

上記に基づき、総務省で、2023年4月から同年5月にかけて、我が国におけるeシールサービスの状況等に関する情報提供依頼を行った結果、eシールに関する国の制度が存在しないこと等がeシール普及の阻害要因となっているという課題が明らかとなった。これを踏まえ、eシールに係る認定制度の創設の可否を含めて検討する場として2023年9月に「eシールに係る検討会」を設置した。

4. 国によるeシールに係る認定制度の創設

重点計画においては、「eシールの民間サービスの信頼性を評価する基準策定及び適合性評価の実現にも取り組む」こととされており、「eシールの民間サービスの信頼性を評価する基準策定」については、2021年6月に策定された「eシールに係る指針」において技術や運用等に関する一定の基準が既に示されている。他方、重点計画に記載された方針のうち、「適合性評価の実現」については、現状として国による適合性評価の枠組みが存在していない状況である。こうした状況を受け、eシール検討会での議論では、国による適合性評価の枠組みとして、総務大臣によるeシールに係る認定制度を創設することが適当であるとの結論を得た。

トラストサービスについて総務大臣による認定制度を設けた前例として、タイムスタンプに係る認定制度が挙げられ、同制度は総務省告示によって制度を設けている。同制度も参考にしながら、「eシール用認証業務（eシールを生成する組織等を認証する業務をいう。以下同じ。）」を認定の対象として、eシールに係る認定制度の創設に向けた議論を進めた。

5. eシールに係る検討会における個別論点と方向性

5.1 eシールの分類

eシールは、発行元証明の信頼性を担保するための水準に応じて、保証レベルの段階を分けることができる。eシールの用途に応じ、①総務大臣による認定を受けたeシール用認証業務によって保証されていないが、より低コスト・簡易な手続で大量発行されるeシールに期待される保証レベル（例：企業間で日常的にやり取りされる電子データ等に活用）と、②総務大臣による認定を受けたeシール用認証業務によって保証され、eシールが付された電子データの出所・起源や完全性について高い信頼が期待されるレベル（例：排他的独占業務とされている士業等の資格証明書等に活用）の2段階に分ける形で整理することとした。

なお、上記の整理は、総務大臣の認定制度に着目したものであり、これ以外に、認証局のeシール用認証業務の信頼性を確保するための民間団体が自主的に行う取組を妨げるものではない点に留意が必要である。

5.2 eシール用電子証明書の発行対象となる組織等の範囲

eシール用電子証明書の発行対象となる組織等を一意に識別できる識別子を設け、eシール用電子証明書に当該識別子を格納する必要がある。eシール検討会では、当該識別子として、国際的に使用されているプレフィクス（接頭辞）と公的機関が発行する既存の番号体系を組み合わせるという提案がなされ、既存の番号体系「法人番号」を用いて組織識別子を構成することとした。なお、認定を受けたeシール用認証業務によって発行されたeシール用電子証明書には、公的機関が発行する番号体系を用いた組織識別子を少なくとも1つ記載することを要件とするが、取引主体識別子（Legal Entity Identifier：LEI）や民間企業コードを用いた組織識別子を追加で記載することを可能とした。

また、「個人事業主」については、eシール用電子証明書を発行する認証局において同姓同名の個人事業主を一意に



特定できる公的番号体系が存在しないことから、引き続きの検討課題と整理した。

5.3 eシール生成者の実在性・申請意思の確認の方法

組織等の実在性・申請意思を確認して証明書を発行する点で、eシール用電子証明書と類似の証明書として、EV (Extended Validation) 証明書がある。同証明書における組織の実在性確認は、CA/Browser Forumのガイドライン等に従って、①法的な存在の確認、②物理的な存在の確認、③運営的な存在の確認の3点が必要とされており、eシール用電子証明書も同様に整理することが適当とされた。

5.4 eシール用電子証明書のフォーマット及び記載事項

eシール用電子証明書のフォーマットは「ITU-T X.509」を使用することとした上で、eシール用電子証明書への記載事項については「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、保証レベルを判別可能な情報、その他属性情報（営業所、事業所等）等」と整理された。特に、「電子署名」用電子証明書と「eシール」用電子証明書を機械判読可能な形で区別できる必要があるため、国際相互運用性の観点も考慮して、共通証明書ポリシー OID体系を整備することが適当であるとされた。

5.5 認証局の秘密鍵の管理に係る基準

認証局の秘密鍵は、認証局が発行する電子証明書及び証明書失効リストに署名する際に使用される。当該秘密鍵の管理に係る基準については、基本的には電子署名法の規定を準用することとし、実施要項等において細部を検討するに当たっては、タイムスタンプの認定制度等も参考にすることが望ましいとした。

その上で、HSM (Hardware Security Module) の技術基準として満たすべきFIPSの規格をはじめ、技術・設備・運用基準については、技術の進展等に応じて変化していくため、国際動向等も踏まえて機動的に見直しができることが適当であるとされた。

5.6 eシール生成者の秘密鍵の管理に係る基準

eシール生成者側の秘密鍵の管理については、認証局からeシール生成者に対して秘密鍵の管理の重要性等を説明することとした上で、eシール生成者の秘密鍵の管理の責任

はeシール生成者自身にあるとすることが適当であるとされた。

5.7 eシールを大量に生成する際の処理

機械的・自動的に複数の対象電子文書等に対して一括でeシールを付与するニーズが想定されるため、認定を受けたeシール用認証業務によって保証されたeシールについても、複数の対象データに一括でeシールを付すことを認めることとした。

5.8 リモートeシール方式

リモートeシール方式とは、eシール生成者の秘密鍵を自身で管理するのではなく、リモートeシールサービス提供事業者に管理を委ねる方式のことをいう。本方式については、複数の電子データにシステム上で大量にeシールを付すことが可能であること等の観点で、リモート署名と差異はあるものの、両者が技術的に共通する部分が多いことから、リモート署名における検討を踏まえてリモートeシールについて検討を進める必要がある。リモート署名については、現在、デジタル庁において、リモート署名生成事業者に係る論点を含めて議論を進めているところであり、eシールの認定制度を検討していく上でも、これらの議論を注視する必要がある。したがって、「リモートeシールサービス提供事業者」に係る規律については、引き続きの検討課題とした。

5.9 eシール用電子証明書の失効要求

eシール生成者の秘密鍵が危殆化したり、eシール用電子証明書の発行対象組織等の統廃合が発生したりした場合は、適切なタイミングでの当該eシール用電子証明書の失効が求められる。特に、eシール生成者の秘密鍵の危殆化については、第三者によるなりすまし等の悪用のおそれがあることから、当該秘密鍵に係るeシール用電子証明書は、可及的速やかに失効される必要がある。

電子署名法に基づく認定認証業務においては、認証局側から電子証明書を失効可能な場合として、「電子証明書に記録された事項に事実と異なるものが発見されたとき」、「利用者署名符号が危殆化したおそれがあるとき」等が挙げられており、eシールについても、同様の場合には、認証局側からeシール用電子証明書を失効可能とした。

6. 「eシールに係る指針」の改訂

「eシールに係る指針」は3章で示したとおり「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」での議論を踏まえ、2021年6月に我が国におけるeシールの在るべき姿を示すことによって、eシール用認証業務を提供する認証局をはじめとする関係者が参考にすべき技術・運用上の基準を示すことを目的として策定された。eシール検討会で示された方向性を受け、5章のとおり、「eシールに係る指針（第2版）」を策定した。

7. 今後に向けた検討課題

7.1 認定制度の運用開始までに議論すべき主な事項

eシールに係る認定制度の創設に向けては、2024年度中に実施要項等の関係規程の検討を行うこととするが、eシール検討会における議論を踏まえ、①技術・設備・運用の基準策定、②電子署名法の認定制度等を用いた適合性評価等の効率化、③CP/CPSに最低限記載すべき事項の整理、④共通証明書ポリシー OID体系の整備、について検討を行う。

7.2 eシールの普及に向けた取組

eシールを社会に広く普及させる上では、eシールを付す者が、自らの経営判断によりeシールの活用を選択する必要があり、そのためには、

- ① eシールを活用した形でのデジタル化が進むことによって削減される人件費等のコストが、eシールを利用するために必要となるコストを上回るとともに、
- ② eシールを活用することで、上記の定量的な効果に加え、安心・安全な形でデータ流通を促進することが可能となること、

について認識を広めてもらうための周知啓発が重要である。

その際、「eシールの保証レベル」の考え方を基に、eシールを付すことによって確保される信頼性のレベルと、それを実現するために必要なコストの関係に対する理解を広めていくことが必要である。また、eシールの有効性を社会に

浸透させていくためには、eシールを受領した側が適切に検証できることが前提となるため、eシールをはじめとするトラストサービスに関するリテラシーを向上させていくことも必要となる。

7.3 国際間のデータ流通におけるeシール活用の可能性

eシール検討会においては、総務大臣によるeシールに係る認定制度の創設は大きな一歩だとしつつも、欧米等における状況も参考にしながら、我が国における包括的なトラスト基盤の構築の要否や認定に係る公表方法等を含めて、戦略的に制度設計等を検討していく必要があることが指摘された。国際間のデータ流通におけるトラストサービスの活用は、国際データ連携基盤以外も含め我が国が提唱するDFFT等とも整合的であり、デジタル庁及び総務省においては、国際的な基準・規格等も踏まえながら戦略的に検討を進める必要がある。

8. おわりに

2023年4月29日及び30日に群馬県高崎市で開催された「G7群馬高崎デジタル・技術大臣会合」において、「越境データ流通と信頼性のある自由なデータ流通（DFFT）の推進」が議論されるなど、安心・安全が確保された形でデータ流通を促進していくことは、デジタル化の進展に欠かせない視点となっている。

我が国において、「eシール」をはじめとする「トラストサービス」が十分に活用されているとは言い難い状況にある中、「総務大臣によるeシールに係る認定制度」の創設は、我が国において安心・安全なデータ流通基盤を構築する上で、大きな一歩と言える。

今後、認定制度の創設に向けた議論を具体化していくこととなるが、デジタル庁及び総務省においては、引き続き緊密な連携を取りながら、我が国のトラストサービスの在り方を大局的な視点から検討していくことが期待される。

ITUが注目しているホットトピックス

ITUのホームページでは、その時々ホットトピックスを“NEWS AND VIEWS”として掲載しています。まさに開催中の会合における合意事項、ITUが公開しているICT関連ツールキットの紹介等、旬なテーマを知ることができます。ぜひご覧ください。

<https://www.itu.int/en/Pages/default.aspx>