eシール民間制度検討ワーキンググループ
報告書

2021年3月

一般財団法人日本データ通信協会
eシール民間制度検討ワーキンググループ

公表にあたって

我が国では、総務省のプラットフォームサービスに関する研究会に設置された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（2020 年 2 月）において、初めて e シールに関する制度化について「一定程度国が関与した民間の自主的な仕組みの創設」という方向性が示された。当時総務省の「タイムビジネスの指針」を受けてタイムスタンプに関する民間認定制度を運用していた当協会としては、この経験を活かして、e シールについても同様の認定制度を創設する場合の課題と方針につき情報発信することにより、近い将来社会から要請があった場合、速やかな制度整備に貢献できるよう準備を開始した。

具体的には、総務省における e シールに関する検討（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）に協力する一方で、有識者の協力を得て協会内に e シール民間制度検討ワーキンググループを設置し、民間制度像を明確にすべく議論を重ね、これを一般に公表する前提で 2021 年 3 月に本報告書を取りまとめた。

しかしながら、当時は総務省における検討が継続中で、e シールに係る指針（案）の下に民間制度がどのように位置づけられるか結論は得られておらず、また、2021 年 9 月のデジタル庁設置を控えて、政府としての方向性が見通せない状況のなか、もう暫く報告書公表の機会を窺う判断をしたまま今日に至ったものである。

今般、デジタル庁のトラストを確保した DX 推進サブワーキンググループ最終報告書（案）において、マルチステークホルダーモデルで扱う議題に「リモート署名・e シールの技術基準の検討」が挙げられていることや関連諸団体においても e シールについて活発な議論が展開されていることから、本報告書についても公表の機が熟したものと判断した。

本報告書を関係各所で活用頂ければ幸いである。

2022 年 6 月 23 日

一般財団法人日本データ通信協会
専務理事　髙嶋幹夫

目　次

はじめに

我が国における、実際のビジネスの場面では、既に個人に紐づかない組織名が記載された電子証明書が発行され活用されている。法人取引業務等における様々なデジタルデータに対して組織名の電子署名（以下、eシールと言う）を付すことによるメリットは、当該デジタルデータを受け取った側が、以下を簡便に確認できることである。

○　当該データの発出元企業・組織

○　当該データの改ざん有無

一方で、eシールに関する技術面、設備面、運用面等の基準は無く、信頼性の確保は、eシール用証明書を発行する認証局やeシール付きデータを発行する組織に委ねられている。

また、eシールのようなトラストサービスはデジタル社会を実現する上で必要とされるサービスであるが、自然人の利用する電子署名は「電子署名法[1]」として早くから法整備されているものの、法人等が利用するeシールは制度が未整備である。

こうした状況で暗号技術や公開鍵基盤の知識に疎い組織が、不適切な環境下でeシール用証明書を発行したり、セキュリティ上危険な状態でeシール生成用の秘密鍵を保管したりするなど、安全措置が施されていないeシールが流通し始めると、トラストサービス全体の信頼を揺るがすことにもなりかねない。例えば、eシール用秘密鍵が持ち出されて生成された不正なeシール付き文書と正当な手続きをもって生成されたeシール付文書との識別は不可能である。また、実在の有名企業を騙る偽のeシール用証明書による犯罪なども懸念されるところである。

そこで、2020年2月の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[2]に示された「一定程度国が関与した民間の自主的な仕組みの創設」という方向性を踏まえ、一般財団法人日本データ通信協会（以下「協会」という。）が制度運用主体となることを想定し、一定レベルの基準を満たしたeシールを識別できる制度を創設すべく有識者の協力を得てeシール民間制度検討ワーキンググループ（以下「本WG」という。）を開催し、制度検討を行っ

---

[1]電子署名及び認証業務に関する法律（平成12年法律第102号）
https://elaws.e-gov.go.jp/document?lawid=412AC0000000102

[2] 総務省『プラットフォームサービスに関する研究会最終報告書』別紙（2020年2月）
https://www.soumu.go.jp/main_content/000668595.pdf

た。信頼性の高いeシールの普及に向けて早急に制度を設計し運用開始すべきであるとの認識に立ち、ここに本報告書を取りまとめ、関係者の方々にご報告するものである。

１．制度設計の基本的な考え方

本WGでeシール民間制度の設計を進めるにあたり、考慮すべき各事項について基本的な考え方を以下に示す。

1.1 総務省検討会の示す方向性との整合性

総務省の「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」においては、我が国におけるeシール検討事項について議論されており、eシールの利用用途等にあわせてレベル分けを行うこと等の方向性が示されている。本WGのeシール民間制度設計においては、総務省検討会の検討状況を把握し、示された方向性と整合した制度設計を行うこととする。

1.2 既存のトラストサービス制度との整合性

我が国における既存のトラストサービス制度としては、電子署名（国による法制度）及びタイムスタンプ（協会による民間の認定制度）の認定制度がある。これらの制度の技術方式はデジタル署名方式が主流であり、eシール民間制度もデジタル署名方式を用いることから審査すべき事項には少なからず共通部分があると考えられる。これらの共通部分については、各制度から引用可能な共通基準を策定することが望ましく目指すべきところである。

しかしながら、本WGで検討するeシール民間制度設計は早期の実現が必要なものであるため、共通基準の策定までは求めず、既存の電子署名、タイムスタンプの制度と共通する部分について出来る限り制度の一致を図ることとする。

1.3 日本版トラステッドリストを見据えた設計

EUでは、様々なトラストサービスを横断的に検証可能にするトラステッドリスト[3]が運用されており、我が国においても、日本版トラステッドリストについて検討が進められている。eシール民間制度においても、その認定に係るサービスの公表が必要であり既存のトラストサービス制度同様ホームページで公表することが考えられるが、日本版トラステッドリストが運用開始された際には、公表データを移行することを想定し、必要な情報が欠落することがないよう留意し制度設計を行うこととする。

---

[3] 認定されたトラストサービスであることが一意に確認できる情報

1.4 国際通用性の確保

EUでは、eIDAS規則[4]においてトラストサービス全体の横断的な制度が整理され、ETSI等による技術標準等化も進んでおり、各サービスに共通する要件や公表の仕組み等が一元的に運用されている。eシール民間制度の設計にあたっても、国際通用性の確保という観点を持ち、デジュールスタンダードで先行するEUのeIDAS規則やETSIの技術標準等も参考にし、制度設計を行うこととする。

1.5 他団体におけるeシールの検討状況の参照

eシールについては、トラストサービス推進フォーラム[5]、日本トラストテクノロジー協議会[6]及びトラストサービスアーキテクチャ検討委員会[7]等で検討が進められており、これらにおける検討内容を参考にし、制度設計を行うこととする。

1.6 その他（認定という用語の使用）

JIS Q 17000：2005（ISO/IEC 17000：2004）では、「認定（accreditation）」という用語を「適合性評価機関に関し、特定の適合性評価業務を行う能力を公式に実証したことを伝える第三者証明」と定義し、専ら適合性評価機関に対して用いられている。そのため、事業者や業務に対しては「認定」ではなく「認証」が用いられるべきであるが、電子署名法や協会のタイムビジネス信頼・安心認定制度では、適合性評価機関以外の事業者や業務に対して「認定」を用いているため、「認定」の用語を用いることとする。

---

[4] REGULATION (EU) No 910/2014
https://ec.europa.eu/futurium/en/system/files/ged/eidas_regulation.pdf

[5] トラストサービス推進フォーラム
https://www.dekyo.or.jp/tsf/

[6] 特定非営利活動法人日本ネットワークセキュリティ協会　日本トラストテクノロジー協議会
https://www.jnsa.org/result/jt2a/2020/index.html

[7] 内閣府が推進する「戦略的イノベーション創造プログラム」の研究項目のうちトラスト基盤におけるリモート署名やトラステッドリストに関しての仕様策定や実証研究を行う委員会

２．eシールに係る指針

以下、eシールの利活用に関わる現状を踏まえ、公開鍵基盤を用いた民間の自主的な仕組みを設計するにあたり基本的な事項を示す。

2.1 eシールのイメージ

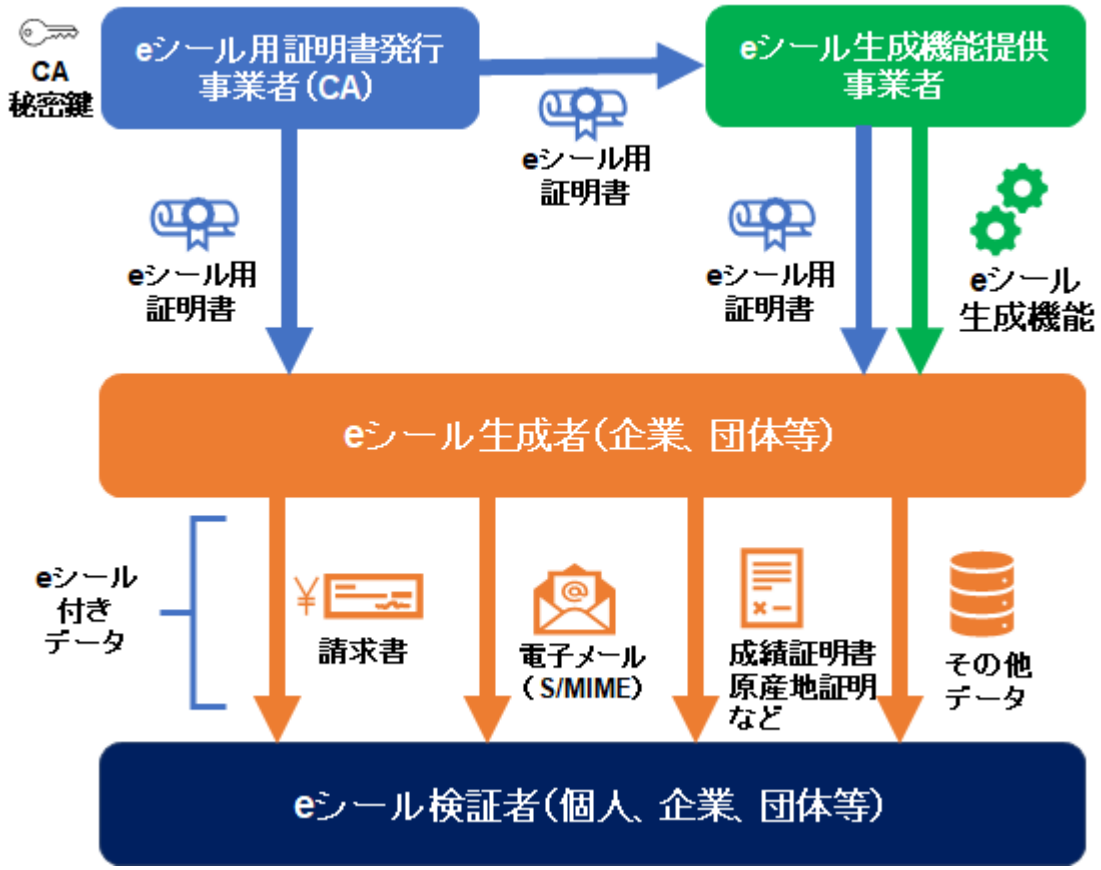

図１　eシールのイメージ

2.2 定義

- eシール
  - デジタルデータの発出元企業・団体等を示す目的で生成されたものであり、eシールが生成されて以降、当該文書が改ざんされていないことを確認することが可能な仕組み。技術的には、組織名義で発行された公開鍵証明書（後述するeシール用証明書）に対応する秘密鍵によりeシール対象データのハッシュ値に対して暗号化を行ったもので、デジタル署名技術を用いて作成される。

・ eシール付きデータ
  - 対象となるデジタルデータにeシールを付与したもの。
    （ex.図1の請求書、電子メール、成績証明書、原産地証明など）

・ eシール用証明書
  - eシールの有効性を確認（検証）するためのデジタルデータ（公開鍵等）と企業・団体等のeシール生成者との結合を十分に保証し、eシール生成者を確認可能とするデジタルデータ。

・ eシール生成鍵（秘密鍵）
  - 公開鍵暗号方式における鍵の対の一方であって、eシールを生成するために用いられる鍵。

・ CA秘密鍵
  - 公開鍵暗号方式における鍵の対の一方であって、eシール用証明書及び失効リストに付与するデジタル署名を生成するための秘密鍵。これとペアとなる公開鍵が格納されたCA証明書によりｅシール用証明書の正当性が検証できる。

・ eシール生成装置
  - eシール生成鍵を設置・保管し、eシールの生成を行う装置。

・ eシール生成機能
  - eシール生成者の正当な権限を有する者の指示に基づき、eシール生成装置を用いてeシールの生成を行う機能。

・ eシール用証明書発行事業者（CA）
  - eシール生成者にeシール用証明書を発行する事業者。

・ eシール生成機能提供事業者
  - eシール生成機能をeシール生成者に提供する事業者。

・ eシール生成者
  - eシール生成鍵（秘密鍵）を使ってeシールの対象となるデジタルデータに対してeシールを生成する主体。 eシール用証明書のサブジェクトに記載された企業・団体等。

・ eシール検証鍵（公開鍵）
  - 公開鍵暗号方式における鍵の対の一方であって、eシールの有効性を確認するために用いられるもの。

・ eシール検証者
  - eシール検証鍵（公開鍵）を使ってeシール付きデータに付されたeシールの有効性を確認する者。

・ 検証
  - eシール用証明書を用いて、eシール検証者が受領したeシールが有効であることを確認することをいう。eシールの有効性を確認することで、eシールが付されたデータがeシール用証明書に記された組織から発出されたものであり、eシールの付与後、改ざんされていないことが確認できる。

2.3 eシール関係業務に求められる事項

2.3.1 eシール用証明書発行業務

(1) 運用

ア 業務の適切な許諾管理

業務の重要度に応じて、eシール用証明書の作成又は管理に用いる電子計算機その他、認定制度により認定された設備（以下「認定業務用設備」という。）が設置された室（以下「認定業務用設備室」という。）への入室及び操作に関する許諾管理が適切に行われていること。

イ CA秘密鍵の漏えい防止策等

複数の者によるCA秘密鍵の作成及び管理その他当該CA秘密鍵の漏えいを防止するために必要な措置が講じられていること。

ウ 認定業務の実施規程の策定、当該規程の公開

業務の実施に係るポリシ及び運用実施規程を適切に定め、利用者、検証者その他の者が当該規程を容易に閲覧することができるようにすること。業務に係る運用は、重要なサーバ等の施錠管理、入退室管理・記録の保管、警報設置状況、アクセス権限管理、内部牽制状況、不正アクセス防止措置、設備運用保守記録等がなされていること。

エ eシール生成鍵等の安全な配信（配送）

（ア）eシール生成鍵をeシール用証明書発行事業者が作成する場合

eシール用証明書発行事業者がeシール生成に用いる秘密鍵を安全かつ確実にeシール生成者に渡すことができる方法により交付し、又は送付し、かつ、当該秘密鍵及びその複製を直ちに消去すること。

（イ）eシール生成鍵をeシール生成者が作成する場合

eシール生成者またはeシール生成者から委託を受けたeシール生成機能提供事業者がeシール生成に用いる秘密鍵を作成する場合において、当該秘密鍵に対応するeシール検証鍵をeシール用証明書発行事業者が電気通信回線を通じて

受信する方法によるときは、あらかじめ、eシール生成者と一意に紐づく方法により安全かつ確実に受信すること。

(2) 証明書の失効

ア　失効要求の処理

失効要求を受領後24時間以内に証明書の失効状況を公開すること。

(3) 設備

ア　入退室管理

認定業務用設備は、入出場を管理するために業務の重要度に応じて必要な措置が講じられている場所に設置されていること。

イ　不正アクセス防止

認定業務用設備は、電気通信回線を通じた不正なアクセス等を防止するために必要な措置が講じられていること。

ウ　不正操作防止

認定業務用設備は、正当な権限を有しない者によって作動させられることを防止するための措置が講じられ、かつ、当該認定業務用設備の動作を記録する機能を有していること。

エ　CA秘密鍵を適切に管理する装置

認定業務用設備のうちCA秘密鍵を作成、管理する装置は、当該CA秘密鍵の漏えいを防止するために必要な耐タンパー機能等を有する専用の装置であること。

オ　災害被害の防止

認定業務用設備及び(1)の措置を講じるために必要な装置は、停電、地震、火災及び水害その他の災害の被害を容易に受けないように業務の重要度に応じて必要な措置が講じられていること。

業務に係る設備は、施設自体の耐震、耐火、水害防止措置、電気設備の無停電対策や瞬停対策、自火報、消火装置の設置、温湿度管理がなされていること。

(4) 帳簿書類又は記録の作成及び保存

ア　認定事業者は、業務に関する以下の帳簿書類又は記録を作成し、保存すること。

（ア）利用の申込みに関する帳簿書類

（イ）eシール用証明書の失効に関する帳簿書類

（ウ）eシール用証明書の申込や失効に関するeシール生成者（申請者含む）本人からの開示請求書類

（エ）組織管理に関する帳簿書類(規定や監査等)

（オ）設備及び安全対策措置に関する帳簿書類

（カ）eシール生成鍵等の受領等に関する記録

イ　上記（ア）から（カ）の帳簿書類又は記録は、当該帳簿書類に係るeシール用証明書の有効期間の満了日から十年間保存すること。

ウ　上記（ア）から（カ）の帳簿書類は、電磁的方法により保存することができること。

(5) セキュリティ対策

ア　役割・組織の管理

（ア）管理者種別と権限分離

少なくとも次の①～④の役割を担う責任者を任命すること。

① セキュリティ統括責任者（Security Officers）：
セキュリティポリシの確実な実施に対する責任を有し、セキュリティ関連情報を管理する者。

② システム管理者（System Administrators）：
eシール用証明書発行業務関連システムのインストール、設定及びメンテナンスの権限を有する者。セキュリティ関連情報へのアクセス権はない。

③ システム運用担当者（System Operators）：
eシール用証明書発行業務の運用に関する責任を有し、システムバックアップ及びリカバリの権限を有する者。

④ システム監査者（System Auditors）：
システム運用がセキュリティポリシに従った運用であるか監査し、其の為にアーカイブや監査ログを確認する権限を有する者。

⑤ 権限分離：
全ての特権をもつ役割を一人で担わないこと。また、一人で二つ以上の特権を持つ役割を担わないこと。

（イ）システム運用

eシール用証明書発行業務を運営する事業者は運営管理が適切で安全であることを保証するため以下を実施すること。

① システム故障リスクの最小化
② ウィルス及び悪意のあるソフトウェアからの保護
③ 「（ア）管理者種別と権限分離」の4つの責任者の役割及び、以下の事項を含む規程文書の提供。
- インストールガイダンス
- 管理ガイダンス
- ユーザガイダンス

イ　サーバ等の時刻同期

eシール用証明書発行業務が標準時刻に適切に同期していること。

ウ　システム及び機密性の高い残存情報へのアクセスコントロール

（ア）特定のユーザだけがアクセスを許可されたシステム及びユーザオブジェクトに対し、アクセスコントロールを実施すること。

（イ）機密性の高い残存情報へのアクセスコントロールを実施すること。

エ　監査データの完全性及びイベントログの記録

（ア）少なくとも以下のイベントを記録すること。

① eシール生成鍵管理イベント（生成、使用及び破壊）

② 監査データ生成機能の開始及び停止

③ 監査パラメータの変更

（イ）監査データの完全性を保証すること。

（ウ）監査データの完全性を検証する機能を提供すること。

オ　アーカイブ

（ア）外部メディア

外部メディアでのアーカイブ生成の能力をもつこと。保存及び情報提供の観点から適切な外部メディアを選択すること。

（イ）アーカイブ対象

すべての監査ログをアーカイブすること。

（ウ）各アーカイブエントリ

① 各アーカイブエントリにはアーカイブの時刻を含むこと。

② アーカイブには、ユーザパスワードなどの機密性の高いセキュリティパラメータを含まないこと。

（エ）アーカイブデータの完全性

① アーカイブにおけるエントリの不正変更が行われないよう防止すること。

② 不正変更を検知するために、完全性を検証するメカニズムを実行すること。

カ　バックアップ・リカバリ

（ア）バックアップ情報の完全性及び機密性

① バックアップ情報の完全性の検証を可能にするメカニズムによる変更からバックアップを保護すること。

② 高感度のセキュリティパラメータ及びその他機密情報は、機密性及び完全性を確保するために保護された形で保管すること。

（イ）リカバリ

① バックアップからシステムの状態を復元できる回復機能をもつこと。

② 十分な特権を持つ役割にリンクしているユーザは、要求に応じてバックアップからの回復機能を起動することができること。

キ　CRYPTREC[8]暗号リストのうち電子政府推奨暗号リストに記載された暗号技術の利用

(6) 運営組織のセキュリティ対策

組織のセキュリティ対策及び運営に関しては、主にISO/IEC27002（JIS Q 27002）の「6情報セキュリティのための組織」に規定する管理策の推奨基準を適用すること。

ア　特に重要な職務権限の分離

eシール用証明書発行業務とeシール生成機能提供業務の両方を行う事業者においては、eシール用証明書発行業務に関わる者とeシール生成機能提供業務に関わる者との職務権限の分離を行うこと。

イ　事業継続のための管理方法の規定化

情報システムの重大な故障、自然災害、またはセキュリティ事故等における、eシール生成者・検証者への影響を最小限に抑えたBCPを事前に定め規定化すること。

ウ　サービスポリシの公表

eシールの利用分野は、電子商取引、電子契約、電子申請など様々であるが、事業者はその利用分野の個別法への準拠性を明確にしたサービスポリシを公開すること。

(7) 組織等の確認

ア　実在性確認

eシール生成者の企業・団体等の実在性を確認すること。

想定される具体的確認事項

- 商業登記上の確認
- 物理的確認
- 運営上の確認

イ　申請者の身元確認

eシール用証明書の発行について申請しようとする者（申請者）がeシール生成者（企業・組織等）の代表者であるか、または代表者から委任を受けた者であるか、その真偽の確認を行うこと。

---

[8] Cryptography Research and Evaluation Committees の略。電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。総務省及び経済産業省が共同で運営する暗号技術検討会と、国立研究開発法人情報通信研究機構（NICT）及び独立行政法人情報処理推進機構（IPA）が共同で運営する暗号技術評価委員会及び、暗号技術活用委員会で構成。
https://www.cryptrec.go.jp/

ウ　申請意思確認

eシール用証明書の発行申請に関し、eシール生成者（企業・団体等）における意思決定に基づくものであることを記名及び押印された提出物又は公開鍵証明書で検証可能な電子署名による方法で確認すること。

(8) 財務

損害に対するリスクを勘案し、財源の維持や適切な保険への加入により十分に備えること。

(9) 証明書プロファイル

以下の必須項目を含めた、eシール用証明書のプロファイルを定めた証明書ポリシを公開すること。

- 当該eシール用証明書の発行者の名称及び発行番号
- 当該eシール用証明書の発行日及び有効期間の満了日
- 当該eシール用証明書の利用組織の名称、および識別子（一意に特定できるものに限る）
- 当該eシール用証明書に係る利用者署名検証符号及び当該利用者署名検証符号に係るアルゴリズムの識別子

(10)業務廃止

業務廃止後も法的手続きにおける証拠資料の提供及び証明書の検証可能性を維持する目的で適切な期間、記録を保持し、かつ記録へのアクセスが可能となる方法を含む終了計画を策定し、維持すること。

2.3.2 eシール生成機能提供業務

(1) 運用

ア　業務の適切な許諾管理

業務の重要度に応じて、eシールの付与又は管理に用いる電子計算機その他設備（以下「eシール生成機能提供業務用設備」という。）を設置した室への入室及び操作に関する許諾管理が適切に行われていること。

イ　eシール生成鍵の安全な管理

eシール生成鍵の安全な生成又は受信、eシール生成鍵利用者とeシール生成鍵の確実な紐付け、eシール生成鍵の漏えい防止等に必要な措置が講じられていること。

ウ　認定業務の実施規程の策定、当該規程の公開

「2.3.1 (1)ウ」と同じ

エ　eシール生成者の認証のための情報の安全な配信（配送）

eシール生成者を初回に認証するための認証クレデンシャルを発行し安全にeシール生成者に配信すること。

(2) 設備

ア　入退室管理

「2.3.1 (2) ア」と同じ。

イ　不正アクセス防止

「2.3.1 (2) イ」と同じ。

ウ　不正操作防止

「2.3.1 (2) ウ」と同じ。

エ　eシール生成鍵の適切に管理する装置

eシール生成機能提供業務用設備のうちeシール生成装置は、当該eシール生成鍵の漏えいを防止するために必要な耐タンパー機能等を有する専用の装置であること。

オ　災害被害の防止

eシール生成機能提供業務用設備及びアの措置を講じるために必要な装置は、停電、地震、火災及び水害その他の災害の被害を容易に受けないように業務の重要度に応じて必要な措置が講じられていること。

(3) 帳簿書類又は記録の作成及び保存

ア　業務に関する以下の帳簿書類又は記録を作成し、保存すること。

（ア）利用の申込みに関する帳簿書類

（イ）組織管理に関する帳簿書類(規定や監査等)

（ウ）設備及び安全対策措置に関する帳簿書類

（エ）eシール生成者を初回に認証するための認証クレデンシャルの送受信等に関する記録

イ　上記の帳簿書類又は記録は、当該帳簿書類に係る利用の終了日から十年間保存すること。

ウ　上記（ア）から（エ）の帳簿書類又は記録は、電磁的方法により保存することができる。

(4) セキュリティ対策

ア　役割・組織の管理

「2.3.1　(4) ア」と同じ。

イ　サーバ等の時刻同期

「2.3.1　(4) （イ）イ」と同じ。

ウ　許可されたユーザの識別及び認証と認証の失敗の管理

（ア）サービスは各ユーザの利用の際に識別と認証を実施すること。

ログアウト後の再認証を必須とすること。

認証データの組み合わせを使用する場合、容易に予測できないものであること。

特権ユーザについては、有効なセッションの時間を定義し、一定時間以上の経過によってセッションを停止する等の措置を取り、セッション乗っ取りのリスクを低減すること。

（イ）認証の失敗

ユーザ認証エラーの回数を管理し、限度を超えたユーザ認証エラーが発生した場合、定期間或いは管理者によるアンロックが行われるまで、同一ユーザによるユーザ認証を認めないこと。

エ　システム及び機密性の高い残存情報へのアクセスコントロール

「2.3.1（4）ウ」と同じ。

オ　監査データの完全性及びイベントログの記録

（ア）少なくとも以下のイベントを記録すること。

① eシール生成鍵管理イベント（生成、使用及び破壊）
② ユーザ署名イベント（署名者の署名鍵を使った正常な署名及び署名対象データと認証データ等による署名リクエスト管理）
③ 署名制御用のプロトコル中のユーザ認証
④ 署名者の署名鍵活性化データの管理
⑤ 監査データ生成機能の開始及び停止
⑥ 監査パラメータの変更

（イ）ユーザ署名イベントには、署名鍵に関連付けられた公開鍵証明書に関する情報を含むこと。

（ウ）監査データの完全性の保証すること。

（エ）監査データの完全性を検証する機能を提供すること。

カ　アーカイブ

「2.3.1（4）　オ」と同じ。

キ　バックアップ・リカバリ

「2.3.1（4）　カ」と同じ。

ク　CRYPTREC暗号リストのうち電子政府推奨暗号リストに記載された暗号技術の利用

(5) 運営組織のセキュリティ対策

「2.3.1（5）」と同じ。

(6) eシール生成者の正当な権限を有する者の認証及び認可

eシール生成鍵に対応するeシール用証明書の名義法人が当該鍵を利用する法人と同一であることを保証し、当該eシール生成鍵とeシール検証鍵を紐づけて管理すること。

ア　eシール生成者の正当な権限を有するものの確実な認証

eシール生成者が秘密鍵とeシール用証明書を利用する際のアカウント登録の当人認証を安全かつ確実に行うこと。

イ　正当なeシール生成者の指示のみによるeシール生成の実施

eシール生成を行う際は正当なeシール生成者以外が秘密鍵を利用できないよう対策を講じること。

ウ　eシール生成鍵の活性化情報による鍵認可の実施

eシール生成の際にはeシール生成装置に対してeシール生成者が直接、秘密鍵への認可情報入力をすること。

2.3.3 eシールのレベル分けと認定制度

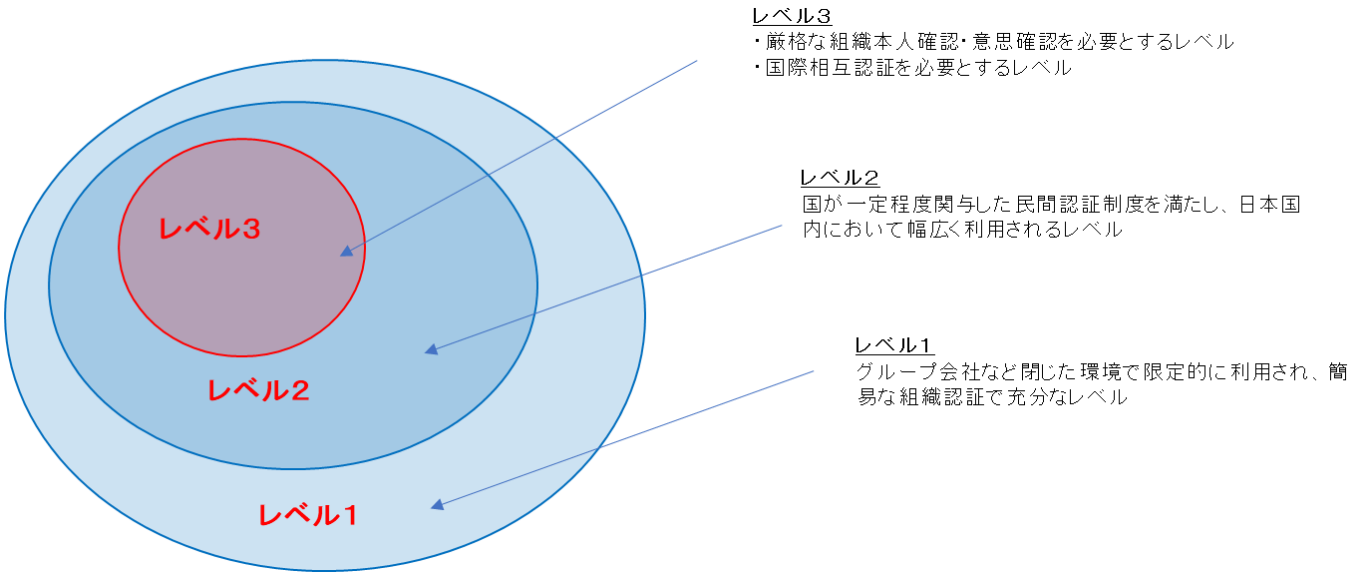

図2　レベル別の認定制度

（出典：トラストサービス推進フォーラム　調査研究WG　「eシール解説」より作図）

「2.3 eシール関係業務に求められる事項」において、eシール用証明書発行業務及びeシール生成機能提供業務の運用面、設備面、その他の要求事項を示した。認定制度の設計においては、それぞれの要求事項についてどのようなレベルを求めるかを決定することとなる。各要求事項のレベルを高く設定すれば、認定事業者の負担は大きくなり利用者（eシール生成者）が負担するコストも大きくなる。一方、各要求事項のレベルを低く設定すれば、eシールの信頼性に関するリスク（不正なeシール生成等）が高まるため、各要求事項のレベル設定は制度設計の要諦である。eシールの利用用途が多様であることを鑑みると、単一のレベルではなく複数のレベルの認定設定を行うことが合理的である。

eシールについての議論を深めているトラストサービス推進フォーラムにおいても、以下の通り利用用途による三段階のレベルを設けて検討を行っている。

- レベル３：厳格な組織本人確認・意思確認を必要とするレベル。国際相互承認を必要とするレベル。
- レベル２：国が一定程度関与した民間認証制度を満たし、日本国内において幅広く利用されるレベル。

・　レベル１：グループ会社など閉じた環境で限定的に利用され、簡易な組織認証で十分なレベル。

このレベル分けの例では、レベル３は国際相互承認を必要とすることから、認定制度に関しても国の制度であることが望ましく、レベル２及びレベル１は民間制度でも対応可能と考えられる。なお、レベル１については「グループ会社など閉じた環境で限定的」な利用であり、敢えて認定制度の対象とする必要はないものと思われる。

３．認定制度の基本設計

協会が新たに創設する認定制度は、国際相互承認を念頭に置きながらもまずはレベル2とし、日本国内において幅広く利用されるeシール民間認定制度を目指す。なお、2023年に開始される電子インボイス制度でのeシール利用も想定し、eシール生成主体の範囲は、法人及び適格請求書発行事業者の登録を受けた個人事業主とするが、登録事業者の公表開始時期によっては法人のみを対象として制度を創設することも考えられる。また、権利能力なき社団・財団やIoT機器のようなデバイスについては、それらのeシール生成主体によるeシールの必要性を踏まえ追加検討することとする。

3.1 認定対象

・　「eシール用証明書発行業務」及び「eシール生成機能提供業務」

eシール用証明書を発行するCAの公開鍵証明書はeシールを検証する際のトラストアンカーとなりうるものであるため、「eシール用証明書発行業務」を認定対象とする。また、eシール生成機能を外部に委託するケースも多く、認証局（CA）から独立分離した認定対象の業務として位置付けるべきとの考え方もあるため「eシール生成機能提供業務」も認定対象とする。

3.2 技術方式

・　「eシール生成者に対して発行された公開鍵証明書によるデジタル署名方式」とする。

国際的に採用されている方式は、eシール生成者に対して発行された公開鍵証明書によるデジタル署名方式であり、まずはデジタル署名方式で制度を開始する。また、デジタル署名方式以外の新たな技術方式によるeシールが実用に供される必要がある場合には、その技術に関する評価を行う。

3.3 審査基準

・ 適合性評価のための「eシール用証明書発行業務審査基準」及び「eシール生成機能提供業務審査基準」を策定。

eシール用証明書発行業務の審査基準については、指針の「2.3.1　eシール用証明書発行業務」の通りとする。また。eシール生成機能提供業務の審査基準については、指針の「2.3.2　eシール生成機能提供業務」の通りとする。

3.4 認定

・ 審査基準に照らし適合性を評価することにより認定。

審査機関は審査の結果に基づき、認定又はその否認の決定をし、その内容を申請者に通知する。

有効期間の更新時には、再度適合性評価のための審査を行い、認定又はその否認の決定をし、その内容を申請者に通知する。

なお、マネジメントシステムの変更を伴うような変更の認定（軽微な変更を除く）等については、２年間の有効期間内の１年の監査（３．６「監査報告」参照）で認定対象業務の確認を行うこととする。

3.5 認定の有効期間

・ 認定日より2年。

参照事例：

EU及び協会のタイムビジネス信頼・安心認定制度の認定の有効期間は2年であり特段の問題も生じていない。電子署名法の認定の有効期間は1年であるが、事業者や審査機関の負担や、事務手続きの煩雑さもあり、現段階では、2年間を採用する。

3.6 監査報告

・ 認定事業者は、年一回以上の監査（内部監査も可とする）を行い、当該監査の結果を審査機関に報告。

参照事例：

協会のタイムビジネス信頼・安心認定制度は、一年に一回の監査結果の報告を義務とし、必要に応じその内容に関し事業者へ確認することで適合性の維持

の確認を行っている。一方、EUでは認定の有効期間（2年）の中間の年において適合性評価機関によるサーベイランス監査を実施、報告義務はないものの事業者における内部監査も実施されている。結果、2年の認定の有効期間内に、3回の適合性の維持を確認する機会がある。今後、国際通用性確保に向けて、必要に応じ制度の見直しを行うこととする。

3.7 事故報告

・ 認定事業者は、eシールの信頼性又は安心性を損なうおそれがある緊急事態発生時に審査機関へ報告。

認定事業者は、eシールの信頼性又は安心性を損なうおそれがある緊急事態が発生又は発覚した場合には、速やかにその旨を通知するとともに、必要な対処を行い、その経過を報告。

3.8 業務廃止又は一時停止の届出及び終了計画等の届出

・ 認定事業者は、休廃止を行おうとする場合には、審査機関に事前に終了計画（再開計画）を届出。

・

認定業務を廃止するにあたっては、eシール生成者がこれまでに発行したeシールの信頼性や検証に影響を与えないようにすること、今後のeシール発行について他の認定事業者の業務へ移行する十分な期間を確保するなどの必要がある。ついては、業務廃止の届出の際には、終了計画の策定と提出を要件とし、eシール生成者が安心して業務（サービス）を継続できるようにすることが望ましい。

3.9 適合性評価に関する第三者の関与

・ 適合性評価に関する検討やその判断について外部有識者から構成される委員会等へ諮問。

協会はタイムビジネス信頼・安心認定制度を15年にわたり運用している。この制度においては、有識者により構成する二つの組織、制度諮問委員会及び認定審査会を設置し、認定するか否かの技術面の妥当性の判断や制度運営面の検討体制を整え、課題検討にあたっての助言等を得てきた。認定制度の企画立案及び運用に関する重要事項について審議する制度諮問委員会は、公共の福祉に関し公正な判断をすることができ、電気通信に関する広い経験と知識を有する委員で構成されている。また、認定審査会は、時刻配信・時刻同期、公開鍵基

盤、暗号技術、システム監査等の専門知識を有した委員で構成しており、事業者から認定の申請があった場合には必ず審査会の判断を仰ぐ仕組みとなっており、民間制度における認定の公平性、恣意性の排除や水準の維持に寄与している。

3.10 認定を受けた業務の公表（トラステッドリストへの移行を前提とする）

・ 審査機関は、ウェブページに事業者名や認定業務で用いる公開鍵証明書等を公開。なお、日本版トラステッドリストの仕様等が確定した後、公表方法を移行することを前提とする。

認定を受けた業務の公表については、マシンリーダブルな形式を基本とし、そこからヒューマンリーダブルな表示等が出来ることが望ましい。また、過去に認定を受けていた事業者の廃業後であっても、「かつて認定を受けていた」という事実を有効期間も含めて確認できる仕組みが望まれる（EUで運用されているトラステッドリストのようなものが具体的な手段として考えられる）。

3.11 認定マーク

・ 認定を受けた業務に対し、認定番号等が付されたマークを付与。

将来的には、EUのトラストマークのように、トラストサービス横断的な共通のマークとの統合も視野に制定する。

おわりに

民間制度をスタートさせる前提として、我々は指針を定め基本設計を取りまとめた。今後、総務省において大枠（指針）を定め公表されるものと想定しているが、民間制度を早期に立ち上げるべく、この国の指針を踏まえ基本設計の修正、詳細な制度設計を引き続き行っていく。

【参考】　eシールのユースケース

eシールは、具体的なユースケースや効果についてトラストサービス推進フォーラムのeシール認証制度検討SWGが取り纏めた成果の抜粋を参考資料として提示する。
eシール付与対象へのレベル分け判断については、今後検討必要。

(1) 対外取引
（販売部門）
・領収書
・見積書
・納品書
・請求書
（調達部門）
・受領書

(2) 行政機関への申請
・源泉徴収票、労働基準監督署への提出資料等

(3) 対外情報公開・発信
・IR関連資料（BS/PL、有価証券方向書、決算短信、決算公告等）
・広報資料（ニュースリリース、調査レポート等）
・金融関連資料（運用報告書、目論見書等）

(4) 品質証明、認定書
（自己宣言）
・適合性宣言書、マニュアル等
（第三者証明）
・原産地証明、認定登録書資格証明書（排他的独占業務とされている士業等）等

(5) 顧客等への証明書
・保険証券
・資格証明書（排他的独占業務とされている士業等）等
・卒業証明書
・修了証明書
・在職証明書
・控除証明書等

(6) クラウド環境等における連携データの信頼性証明
・企業Aから企業Bに連携されたデータ
・企業Aから行政機関に連携されたデータ

「eシール民間制度検討ワーキンググループ」構成員等

（敬称略・五十音順）

構成員

江頭英一	株式会社コンストラクション・イーシー・ドットコム
小田嶋昭浩	株式会社帝国データバンク
柴田孝一	セイコーソリューションズ株式会社
西山晃	セコムトラストシステムズ株式会社
濱口総志	株式会社コスモス・コーポレイション
宮崎一哉	三菱電機株式会社

事務局（一般財団法人日本データ通信協会）

林　信秀	情報通信セキュリティ本部長
伊地知　理	
齋藤　久	
田中　裕	