データ交換共通認証局 証明書ポリシー

V1.0.0

インターネットEDI普及推進協議会

Japan internet EDI Association (JiEDIA)

目　次

1. はじめに

1.1. 概要

本書は「データ交換共通認証局　証明書ポリシー」(以下、「本ポリシー」と記する）である。本ポリシーは、法人や個人事業主がインターネット等のネットワークを利用したデータ交換を安全に行うために利用する証明書を発行するサービスを提供する認証局が最低限守るべき事項を定めている。

上記用途のための証明書を発行する認証局は本ポリシーに従い、さらに別途定められた手続きにより認証局を認定する機関（以下、「認定機関」と記する）により認定を取得する必要がある。当該認定を受けたそれぞれの認証局のことを「データ交換共通認証局データ交換共通認証局」と呼ぶ。

また、各データ交換共通認証局は、本ポリシーを基準にして、個々の認証業務の実態に即して認証業務実施規程（Certificate Practice Statement、以下「CPS」と記する）作成しなければならない。

各 CPS では、本ポリシーにおいて要件が定められている項目についてはそれに準拠した内容が規定されていなければならない。本ポリシーにおいて「規定しない」と記載されている項目については内容が規定されている必要はない。

また、本ポリシーにおいて「各データ交換共通認証局が定める」と記載されている内容については、各データ交換共通認証局が個々の業務内容に即して明確に実施内容を規定しなければならない。当該規定内容については各 CPS に記載されることが望ましいが、各データ交換共通認証局の判断により、各 CPS 上には記載しないことも認められる。

なお、本ポリシーは IETF が作成した RFC3647(Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Framework）において定めている章・節・項の構成に従って記述されている。

本ポリシーでは、各データ交換共通認証局が発行した証明書の相互利用については依拠当事者が各データ交換共通認証局を全て信頼することによって実現されることを前提としている。ただし、将来において各データ交換共通認証局が発行した証明書の相互利用性の確保は、他の手段にて実現される可能性がある。このため、各データ交換共通認証局はこれに留意しなければならない。

本書の内容は逐次改定を加える予定である。本書を引用する場合は、
「出典：データ交換共通認証局 証明書ポリシー VX.X.X（インターネット EDI 普及推進協議会)」と出典を明記していただきたい。

1.2. 文書の名前と識別

本書の名称は「データ交換共通認証局　証明書ポリシー」である。本ポリシーに対して OID の割り当ては行わない。

1.3. PKI の関係者

1.3.1. 認証局

認証局とは、認証局秘密鍵を安全に管理し、利用者からの証明書の発行や失効に関わる申請を審査し、証明書の発行、失効等を行う機関である。認証局の業務は大きく分けて、認証局秘密鍵の管理を行い、証明書の発行や CRL の発行を行う業務と、利用者から提出された書類等を確認し、証明書の発行や失効に関わる審査を行う業務に分けられる。

また、各認証局は、2 章において規定されている通りに情報の公開場所としてリポジトリを提供しなければならない。

なお、各データ交換共通認証局は PKI の階層構造として、複数段の階層構造を採用することが出来る。ただし、階層構造の頂点をなすルート認証局より利用者の証明書を発行する認証局までの全ての認証局は単一の組織により運営されなければならない。また、データ交換共通認証局として認定の対象となるのは単一の組織が提供する業務についてである（ただし、業務の一部を他の組織に委託することは認められる)。

また、将来において各データ交換共通認証局の上位に位置づけられる認証局が構築される可能性がある。このため、各データ交換共通認証局はそれを妨げる技術仕様はまたは運用ポリシーを設定してはならない。

1.3.2. 登録局

登録局とは、利用者から提出した書類等を確認し、証明書の発行や失効に関わる審査を行う業務である。本ポリシーにおいて、登録局とは認証局内の業務の一部を指し示すものとする。

1.3.3. 利用者

利用者とは各データ交換共通認証局により証明書の発行を受け、利用を行うものである。各データ交換共通認証局は、データ交換に関わりを有しているものの中で、以下のものの全てまたはその一部に対して証明書を発行する。

(1) 法人（個人で事業を行っており、かつ法人登記を行っている者も含むものとする）
(2) 法人の従業者（役員、社員、契約社員等を含む）
(3) 法人が所有するサーバまたはシステム（の管理者）
(4) 個人事業主（法人登記を行っていない事業者のみを指すものとする）
(5) 個人事業主が所有するサーバまたはシステム（の管理者）

1.3.4. 依拠当事者

依拠当事者とは、各データ交換共通認証局が発行した証明書に依拠して以下の行為を行うものである。

- 利用者が作成した電子署名を証明書内の公開鍵を利用して検証行う
- 利用者から提示された証明書により利用者の認証を行う
- 利用者に対して証明書内の公開鍵を利用して暗号化されたデータを送信する

なお、各データ交換共通認証局はデータ交換の目的において広くサービスを提供するために依拠当事者の範囲に関する制限を定めてはならない。

1.3.5. 他の参加者

規定しない。

1.4. 証明書の利用方法

1.4.1. 適切な証明書の利用

各データ交換共通認証局が発行する証明書の利用用途は以下の範囲に制限される。

- データ交換用途のメッセージ署名・暗号化
- データ交換用途の SSL サーバ認証・暗号化
- データ交換用途の SSL クライアント認証

1.4.2. 禁止される証明書の利用

利用者は如何なる理由によっても、1.4.1 項で規定された証明書の利用用途以外に証明書を利用してはならない。

1.5. ポリシー管理

1.5.1. 文書を管理する組織

本ポリシーの管理組織（以下、「本ポリシー管理組織」と記する）は、認定機関とする。

1.5.2. 連絡窓口

本ポリシーに関する問い合わせの窓口は以下のとおりとする。

https://・・・・・・・・・・【認定機関が運営する Web サイトの URL】

また各データ交換共通認証局の問い合わせ窓口は、各データ交換共通認証局が定める CPS に掲載場所を記載するものとする。

1.5.3. CPS のポリシー適合性を決定する者

各 CPS が本ポリシーに適合していることの判断は認定機関が行うものとする。

1.5.4. CPS 承認手続

各 CPS の作成及び承認手続きは各データ交換共通認証局によって定められる。ただし、

1.5.3 項で規定されている通りに、認定機関の判断により各 CPS が本ポリシーに準拠していないとみなされる場合がある。

1.6. 定義と略語

本報告書の付録を参照のこと。

2. 公開とリポジトリの責任

2.1. リポジトリ

各データ交換共通認証局は、依拠当事者等が CRL（利用者の証明書を対象としたものを指す。以下同様）を参照できるために、インターネット上にリポジトリを公開しなければならない。リポジトリは、常時アクセス可能でなけければならないが、保守等の理由によっては一時的に停止することは認められる。

2.2. 証明情報の公開

各データ交換共通認証局はリポジトリ上において以下の情報を公開しなければならない。

- 各 CPS
- 利用者規約
- 依拠当事者規約
- 認証局証明書（ルート認証局より利用者の証明書を発行する認証局までの全ての認証局を含む）
- CRL

2.3. 公開の時期、及び頻度

各 CPS、利用者規約及び依拠当事者規約は更新された場合、直ちに公開されなければならない。認証局証明書は発行された都度、直ちに公開されなければならない。CRL は 4.9.7 項で規定された頻度で更新され、更新後直ちに公開されなければならない。

2.4. リポジトリへのアクセス管理

各データ交換共通認証局が提供するリポジトリの情報の参照については、利用者及び依拠当事者の利用を阻害しないために、制限が行われてはならない。また、リポジトリへの情報の追加、変更については、各データ交換共通認証局内の正しい権限を持つ者のみが実施可能とするような対策が講じられなければならない。

3. 識別と認証

3.1. 名前決定

3.1.1. 名前の種類

各データ交換共通認証局が発行する証明書のサブジェクト名は X.500 の Distinguished Name の形式に従わなければならない。

3.1.2. 名前が意味を持つことの必要性

各データ交換共通認証局のルート認証局から利用者の証明書を発行する認証局の名称は各データ交換共通認証局が定める。ただし、各認証局の始めの OrganizaionalUnitName には「CA for manufatures-distributors-retailers」の値を設定することを推奨する。

利用者の証明書に記載される利用者の名称は以下の通りとする。

表 1　法人の証明書

No.	項目	設定	仕様
1	ContryName	◎	"JP"が設定される
2	OrganizationName	◎	法人の英語名称が記載される
3	CommonName	◎	法人の英語名称が記載される
4	その他	△	各データ交換共通認証局が定める

（◎は必須、○は推奨、△は任意、×は不可を表す。）

表 2　法人の従業者の証明書

No.	項目	設定	仕様
1	ContryName	◎	"JP"が設定される
2	OrganizationName	◎	法人の英語名称が記載される
3	OrganizationalUnitName	○	従業者が所属する部署の英語名称が記載される
4	CommonName	◎	従業者の名称のヘボン式ローマ字表記または英語表記が記載される
5	その他	△	各データ交換共通認証局が定める

（◎は必須、○は推奨、△は任意、×は不可を表す。）

表 3　法人が所有するサーバまたはシステムの証明書

No.	項目	設定	仕様
1	ContryName	◎	"JP"が設定される
2	OrganizationName	◎	法人の英語名称が記載される
3	OrganizationalUnitName	○	サーバまたはシステムを管理する部署の英語名称が記載される。
4	CommonName	◎	サーバまたはシステムの FQDN 名又はシステム名称が記載される
5	その他	△	各データ交換共通認証局が定める

（◎は必須、○は推奨、△は任意、×は不可を表す。）

表 4　個人事業主の証明書

No.	項目	設定	仕様
1	ContryName	◎	"JP"が設定される
2	OrganizationName	◎	"Natural Person"が設定される
3	CommonName	◎	個人事業主の名称のヘボン式ローマ字表記または英語表記が記載される
4	その他	△	各データ交換共通認証局が定める

（◎は必須、○は推奨、△は任意、×は不可を表す。）

表 5　個人事業主が所有するサーバまたはシステムの証明書

No.	項目	設定	仕様
1	ContryName	◎	"JP"が設定される
2	OrganizationName	◎	"Natural Person"が設定される
3	OrganizationalUnitName	◎	個人事業主の名称のヘボン式ローマ字表記または英語表記が記載される
4	CommonName	◎	サーバまたはシステムの FQDN 名又はシステム名称が記載される。
5	その他	△	各データ交換共通認証局が定める

（◎は必須、○は推奨、△は任意、×は不可を表す。）

3.1.3. 利用者の匿名性、または仮名性

規定しない。

3.1.4. 種々の名前形式を変換するための規則

各データ交換共通認証局が定める。

3.1.5. 名前の一意性

各データ交換共通認証局は自身が発行する証明書に関して、利用者の名称の一意性の確保を行わなければならない。

3.1.6. 認識、認証、及び商標の役割

各データ交換共通認証局が定める。

3.2. 初回の本人性確認

3.2.1. 秘密鍵の所持を証明する方法

各データ交換共通認証局は、証明書の発行に先立ち利用者より PKCS#10 形式を受領する等により、利用者が証明書に記載される公開鍵と対応する秘密鍵を所有していることの確認を行わなければならない。各データ交換共通認証局が利用者の秘密鍵を生成する場合を除く。

3.2.2. 組織の本人性の認証

各データ交換共通認証局は法人の証明書、法人の従業者の証明書、法人が所有するサーバ又はシステムの証明書を発行する際に、以下のいずれかの方法または認定機関が承認するこれらに準ずる方法により各証明書発行対象者に関係する法人の認証を行わなければならない。

- 商業登記簿謄本、法人印の印鑑証明書、及び法人印による押印がなされた証明書申請書の確認
- 民間調査会社が割り当てる企業コード＋公開情報を利用した電話による当該法人に対する申請の意思の確認

また、FQDN 名を含む証明書については whois 検索またはその他の確実な方法により、当該 FQDN を当該法人が利用する権利を有していることの確認を行わなければならない。

なお、EPC の用途で法人が利用する証明書については上記の認証と同様の手続きを行うものとする。

3.2.3. 個人の本人性の認証

各データ交換共通認証局は個人事業主の証明書、個人事業主が管理するサーバ又はシステムの証明書を発行する際に、以下の方法または認定機関が承認するこれに準ずる方法に

より個人事業主個人の認証を行わなければならない。

- 個人印の印鑑登録証明書、及び個人印による押印がなされた証明書申請書の確認

また、FQDN 名を含む証明書については whois 検索またはその他の確実な方法により、当該 FQDN を当該個人事業主が利用することの権利を有していることの確認を行わなければならない。

なお、EPC の用途で個人事業主が利用する証明書については上記の認証と同様の手続きを行うものとする。

3.2.4. 確認しない利用者の情報

規定しない。

3.2.5. 権限の正当性確認

規定しない。

3.2.6. 相互運用の基準

規定しない。

3.3. 鍵更新申請時の本人性確認と認証

3.3.1. 証明書の更新時の本人性確認と認証

各データ交換共通認証局は、通常の証明書の更新時には、証明書の初回発行と同様の利用者に対する認証を行う。利用者からの電子署名を確認する等、初回発行と異なる方法により更新に関する申請が利用者から行われていることの確認を行う場合、併せて初回申請と同等の利用者の実在性確認を行わなければならない。

3.3.2. 証明書の再発行時の本人性確認と認証

各データ交換共通認証局は、何らか事由によって利用者の証明書を失効した後に、証明書の再発行を行う場合は、初回発行時と同様の利用者に対する認証を行わなければならない。

3.4. 失効申請時の本人性確認と認証

利用者より証明書の失効申請が行われた場合、各データ交換共通認証局は以下のような方法により当該申請が、証明書を所有しているものによって行われていることを確認しなければならない。

- 利用者が事前に登録している失効用のパスワードを確認する
- 利用者より証明書で証明されている公開鍵に対応する秘密鍵による電子署名を受領す

る

- 各業界共通認証局が管理している利用者の電話番号を利用した、利用者の失効意思の確認
- その他、失効の申請者が利用者本人であることを確認する方法

4. 証明書のライフサイクルに対する運用上の要件

4.1. 証明書申請

4.1.1. 証明書申請を提出することができる者

各データ交換共通認証局に証明書の申請を行えるのは以下の者とする。

- データ交換を業務に必要とする法人の従業者
- データ交換を業務に必要とする個人事業主

4.1.2. 登録手続き、及び責任

各データ交換共通認証局に証明書の申請を行うものは、各データ交換共通認証局によって指定された書類及び電子データを準備し、各データ交換共通認証局に指定された方法によって当該書類及び電子データを送付しなければならない。

4.2. 証明書申請の処理手順

4.2.1. 本人性確認と認証機能の実行

各データ交換共通認証局は法人及び法人内の個人に対して証明書を発行する場合は 3.2.2 項で規定された内容にしたがって法人の認証を行わなければならない。また、各データ交換共通認証局は個人事業主に対して証明書を発行する場合は 3.2.3 項で規定された内容に従って個人事業主の認証を行わなければならない。

4.2.2. 証明書申請の承認、または却下

各データ交換共通認証局は 4.2.1 項で規定された手続において、書類の不備、本人性の確認時における疑義、及びその他の懸念が生じた場合などは、申請を許可してはならない。

4.2.3. 証明書申請の処理に要する時間

各データ交換共通認証局が定める。

4.3. 証明書発行

4.3.1. 証明書の発行過程における認証局、及び登録局の行為

各データ交換共通認証局は 4.2 節で規定された証明書申請により証明書の発行が認められた場合、速やかに証明書を発行しなければならない。

4.3.2. 利用者に対する証明書発行通知

各データ交換共通認証局が定める。

4.4.　証明書の受領

4.4.1. 証明書の受領確認の行為

利用者は各データ交換共通認証局より証明書を受領した場合、証明書の記載内容を確認し、記載内容に誤りが含まれていないことの確認を行わなければならない。利用者は、証明書の記載内容に誤りが含まれていた場合、当該事実を各データ交換共通認証局に通知しなければならない。

4.4.2. 認証局による証明書の公開

各データ交換共通認証局が定める。

4.4.3. 他のエンティティに対する認証局の証明書発行通知

規定しない。

4.5.　鍵ペアと証明書の用途

4.5.1. 利用者による秘密鍵、及び証明書の使用

利用者の秘密鍵及び証明書は 1.4.1 項で規定された証明書の利用用途に即して利用されなければならない。

4.5.2. 依拠当事者による公開鍵、及び証明書の使用

依拠当事者は 1.4.1 項で規定された証明書の利用用途に即した場合のみ依拠することができる。

4.6.　証明書の更新

各データ交換共通認証局では鍵の更新を伴わない証明書の更新は実施しない。

4.7.　証明書の鍵更新

4.7.1. 鍵の更新を伴う証明書の更新の場合

鍵の更新を伴う証明書の更新は以下の場合行われる。

- 失効されていない利用者の証明書の有効期限が満了する場合

4.7.2. 新しい公開鍵の証明書の申請を行うことができる者

鍵の更新を伴う証明書の更新に関する申請は以下の者が行える。

- 利用者
- 各データ交換共通認証局が認めた者

4.7.3. 証明書の鍵更新申請の処理

各データ交換共通認証局は、鍵の更新を伴う証明書の更新時には、証明書の初回発行と同様の利用者に対する認証を行うか、または利用者からの電子署名を確認することで更新に関する申請が利用者から行われていることの確認を行わなければならない。

4.7.4. 利用者に対する新しい証明書の通知

各データ交換共通認証局が定める。

4.7.5. 鍵更新された証明書の受領確認の行為

利用者は各データ交換共通認証局より証明書を受領した場合、証明書の記載内容を確認し、記載内容に誤りが含まれていないことの確認を行わなければならない。利用者は、証明書の記載内容に誤りが含まれていた場合、当該事実を各データ交換共通認証局に通知しなければならない。

4.7.6. 認証局による鍵更新済みの証明書の公開

各データ交換共通認証局が定める。

4.7.7. 他のエンティティに対する認証局の証明書発行通知

規定しない。

4.8. 証明書の変更

各データ交換共通認証局では証明書の変更は実施しない。

4.9. 証明書の失効と一時停止

4.9.1. 証明書失効の場合

各データ交換共通認証局が発行した証明書は以下の場合失効される。

- 利用者の秘密鍵が危殆化した、または危殆化した恐れがある場合
- 利用者が証明書の利用を取りやめる場合
- 証明書で記載されている情報に変更があった場合
- 各データ交換共通認証局が必要と認めた場合

4.9.2. 証明書失効を申請することができる者

各データ交換共通認証局が発行した証明書の失効に関わる申請を行えるのは以下の者とする。

- 利用者
- 利用者と同じ法人の従業者

- 各データ交換共通認証局

4.9.3. 失効申請手続き

利用者の申請に基づく証明書の失効を実施する場合は、各データ交換共通認証局は、3.4節で規定された認証方法に基づき、証明書の失効を申請した者が利用者かまたは利用者と同じ法人に所属するものであることの認証を行わなければならない。

各データ交換共通認証局の申請に基づく証明書の失効を実施する場合の手続は、各データ交換共通認証局が定める。

4.9.4. 失効申請の猶予期間

利用者は 4.9.1 項で規定された失効事由に該当した場合、速やかに各データ交換共通認証局によって定められた失効手続きを行わなければならない。

4.9.5. 認証局が失効申請を処理しなければならない期間

各データ交換共通認証局が定める。

4.9.6. 依拠当事者の失効確認の要求

依拠当事者は各データ交換共通認証局が発行した証明書に依拠する前に当該証明書を発行した各データ交換共通認証局の最新の CRL を確認し、当該証明書が失効されていないことの確認を行わなければならない。

4.9.7. 証明書失効リストの発行頻度

各データ交換共通認証局は少なくとも 1 日に１度の頻度で CRL を発行しなければならない。

4.9.8. 証明書失効リストの発行最大遅延時間

規定しない。

4.9.9. オンラインでの失効/ステータス確認の適用性

規定しない。

4.9.10. オンラインでの失効/ステータス確認を行うための要件

規定しない。

4.9.11. 利用可能な失効通知の他の形式

規定しない。

4.9.12. 鍵更新の危殆化に対する特別要件

各データ交換共通認証局は自身の秘密鍵が危殆化した場合は、直ちに関係者に当該事実を通知しなければならない。

利用者が自身の秘密鍵が危殆化した場合は、速やかに証明書を発行した各データ交換共通認証局に通知しなければならず、また指定された証明書の失効等に関わる手続きを行わなければならない。

4.9.13. 証明書の一時停止の場合

規定しない。

4.9.14. 証明書の一時停止を申請することができる者

規定しない。

4.9.15. 証明書の一時停止申請手続き

規定しない。

4.9.16. 一時停止を継続することができる期間

規定しない。

4.10. 証明書のステータス確認サービス

規定しない。

4.11. 利用の終了

利用者が何らかの事由により証明書の利用を終了する場合は、少なくとも 4.9 項で規定した、証明書の失効手続きを行わなければならない。

4.12. キーエスクローと鍵回復

規定しない。

5. 設備上、運営上、運用上の管理

5.1. 物理的管理

5.1.1. 立地場所、及び構造

各データ交換共通認証局内において認証局秘密鍵の管理・利用が行われる施設（以下、「認証局秘密鍵管理施設」と記する）の所在は、必要な関係者以外には公表されてはならない。また、認証局秘密鍵管理施設はその構造上、洪水・地震等の天災に対する対応が行われていなければならない。

5.1.2. 物理的アクセス

認証局秘密鍵管理施設において、生体認証等を利用した厳格な個人による入退室管理が行われていなければならない。また、特に重要な部屋については正当な権限を有する複数人以上の立会いがなければ入室が不可能となるような仕組みが講じられなければならない。

各流業界共通認証局内において登録局の業務を行う施設（以下、「登録局施設」と記する）においては適切な入退室管理が行われていなければならない。

5.1.3. 電源、及び空調

認証局秘密鍵管理施設において利用される重要な機器には停電に対する対策が講じられていなければならない。また、認証局秘密鍵管理施設において利用される重要な機器が適切な動作するように空調設備が整備されていなければならない。

5.1.4. 水害対策

認証局秘密鍵管理施設において利用される重要な機器には、漏水等の対策が行われていなければならない。

5.1.5. 火災防止、及び火災保護対策

認証局秘密鍵管理施設は、適切な耐火構造が採用されていなければならない。また、認証局秘密鍵管理施設は、適切な消化設備が備えられていなければならない。

5.1.6. 媒体保管場所

各データ交換共通認証局内で記録され保管される記録媒体は施錠可能な保管場所に保管されなければならない。また当該保管場所については適切な搬入出管理が行われていなければならない。

5.1.7. 廃棄処理

各データ交換共通認証局内で廃棄処理を行う書類・記録媒体については、所定の手続きにより適切に廃棄処理が行われていなければならない。

5.1.8. 施設外のバックアップ

規定しない。

5.2. 手続き的管理

5.2.1. 信頼すべき役割

各データ交換共通認証局が定める。

5.2.2. 職務ごとに必要とされる人数

各データ交換共通認証局では、認証局秘密鍵の管理を行う役割は必ず複数以上の者を任命し、一人の管理者の権限のみでは、認証局秘密鍵の利用が行えないようにするための相互牽制の仕組みが講じられなければならない。

また、利用者から提出された書類等の審査については、ダブルチェックを義務づける等により一人の担当者の作業では審査が完了しないための仕組みを講じなければならない。

5.2.3. 個々の役割に対する本人性確認と認証

各データ交換共通認証局では、認証局内の各要員が業務を実施するよりも前に、適切な本人性の確認が行われなければならない。

5.2.4. 職務分割が必要となる役割

各データ交換共通認証局が定める。

5.3. 人事的管理

5.3.1. 資格、経験及び身分の要件

各データ交換共通認証局が定める。

5.3.2. 経歴の調査手続き

規定しない。

5.3.3. 研修要件

各データ交換共通認証局は、認証業務を担う要員に対し、業務を遂行する上で必要となる知識を習得させる研修を適切に行わなければならない。

5.3.4. 再研修の頻度及び要件

規定しない。

5.3.5. 職務のローテーションの頻度及び要件

規定しない。

5.3.6. 認められていない行動に対する制裁

規定しない。

5.3.7. 独立した契約者の要件

規定しない。

5.3.8. 要員に提供する資料

規定しない。

5.4. 監査ログの手続き

5.4.1. 記録されるイベントの種類

各データ交換共通認証局では最低限以下のイベントに関してログを保管しなければならない。

- 認証局秘密鍵の操作
- 認証局秘密鍵が保管される部屋の入退室
- 認証局の重要なシステムが保管される部屋の入退室
- 証明書の発行
- 証明書の失効
- CRL の発行

5.4.2. 監査ログを処理する頻度

各データ交換共通認証局が定める。

5.4.3. 監査ログを保持する期間

各データ交換共通認証局は取得した監査ログを少なくとも１ヶ月以上の期間は読み取りが容易な場所に保持しなければならない。

5.4.4. 監査ログの保護

各データ交換共通認証局は正当な権限を有する者のみが監査ログにアクセス可能になるように適切な保護措置を講じなければならない。

5.4.5. 監査ログのバックアップ手続き

各データ交換共通認証局が定める。

5.4.6. 監査ログの収集システム

規定しない。

5.4.7. イベントを起こしたサブジェクトへの通知

規定しない。

5.4.8. 脆弱性評価

規定しない。

5.5. 記録のアーカイブ

5.5.1. アーカイブされる記録の種類

各データ交換共通認証局では最低限以下の書類・電子データを保存しなければならない。

(1) 証明書の初回発行に関する記録
- 利用者が提出した書類
- 各データ交換共通認証局内での審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）

(2) 証明書の更新に関する記録
- 利用者が提出した書類
- 各データ交換共通認証局内での審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）

(3) 証明書の失効に関する記録
- 利用者が提出した書類
- 各データ交換共通認証局内での審査記録（審査結果、審査日時、審査担当者、承認者に関する情報等）

(4) 認証局秘密鍵の操作に関する記録

(5) 各データ交換共通認証局の組織の維持管理に関する記録
- 認証局の体制図及びこれに準ずる書類
- 認証局に関連する規程類（各 CPS、利用者規約、依拠当事者規約等）

5.5.2. アーカイブ保持期間

各データ交換共通認証局では、5.5.1 項で規定された保存すべき書類・電子データを最低限以下の期間の間は保管しなければならない。

(1) 証明書の初回発行に関する記録・・・当該証明書の有効期間が満了してから 3 年間

(2) 証明書の更新に関する記録・・・当該証明書の有効期間が満了してから 3 年間

(3) 証明書の失効に関する記録・・・当該証明書の有効期間が満了してから 3 年間

(4) 認証局秘密鍵の操作に関する記録・・・当該認証局秘密鍵が利用されている限り
(5) 各データ交換共通認証局の組織の維持管理に関する記録・・・改訂後より 10 年間

5.5.3. アーカイブの保護
各データ交換共通認証局は保管された書類・電子データが、不正に改ざん、紛失、劣化しないための保護措置を講じなければならない。

5.5.4. アーカイブのバックアップ手続き
各データ交換共通認証局が定める。

5.5.5. 記録にタイムスタンプを付ける要件
規定しない。

5.5.6. アーカイブ収集システム
規定しない。

5.5.7. アーカイブの情報を入手し検証する手続
規定しない。

5.6. 鍵の切り替え
規定しない。

5.7. 危殆化、及び災害からの復旧
5.7.1. 事故、及び危殆化の取り扱い手続き
各データ交換共通認証局は以下のインシデントに対し、迅速な復旧作業を実施するために、関係する要員に必要な教育及び訓練を行わなければならない。

- 認証局秘密鍵の危殆化
- 認証局内で利用しているシステムの障害

5.7.2. コンピュータの資源、ソフトウェア、またはデータが破損した場合
各データ交換共通認証局は、自身のシステム内において、ハードウェア、ソフトウェアまたはデータの破壊が生じた場合は、可能な限り速やかにバックアップ機、バックアップデータ等を用いて復旧作業を行い、速やかな業務再開に努めなければならない。

5.7.3. エンティティの秘密鍵が危殆化した場合の手続き
各データ交換共通認証局が定める。

5.7.4. 災害後の事業継続能力

各データ交換共通認証局は、災害などの不測の事態が発生した際に速やかに復旧作業が実施できるように、予め復旧手順書の作成等の措置を講じなければならない。

5.8. 認証局、または登録局の終了

各データ交換共通認証局が、業務を終了する場合は、業務を終了する3ヶ月以上前に利用者に対して通知を行うべく努めなければならない。また、各データ交換共通認証局が保管する記録等に関して、継続保管又は廃棄に関する取り決めを行い、必要に応じて当該処置内容を利用者に通知しなければならない。

各データ交換共通認証局は、業務を終了するその際には自身が発行した有効な利用者の証明書を全て失効しなければならない。

6. 技術的セキュリティ管理

6.1. 鍵ペアの生成、及びインストール

6.1.1. 鍵ペアの生成

認証局秘密鍵は、FIPS140-1 レベル 3 相当以上の暗号モジュール上で生成されなければならない。また当該作業は正当な権限を有する複数の者の立会いの上で実施されなければならない。

利用者の秘密鍵の生成は、利用者自身が行うこと、あるいは各データ交換共通認証局が行うことの両方が認められる。

各データ交換共通認証局が利用者の秘密鍵を作成する場合は、当該秘密鍵の紛失、盗難、改ざん、不正な開示、無権限での使用等が行われないようにしなければならない。

6.1.2. 利用者に対する秘密鍵の配送

各データ交換共通認証局が利用者の秘密鍵を生成する場合は、各データ交換共通認証局は、当該秘密鍵を安全な方法により利用者に配送しなければならない。また、各データ交換共通認証局は、利用者への秘密鍵の配送手続きが完了後に自身が管理する装置等に記録されていた利用者の秘密鍵を確実に削除しなければならない。

6.1.3. 認証局に対する利用者の公開鍵

利用者の公開鍵は、SSL 等を利用した安全な方法にて各データ交換共通認証局に配送されなければならない。

6.1.4. 依拠当事者に対する認証局の公開鍵の交付

各データ交換共通認証局は、安全に自身の認証局証明書を依拠当事者に対して配布するための仕組みを講じなければならない。

6.1.5. 鍵サイズ

各データ交換共通認証局はその全ての階層構造中の認証局について、2,048 ビット以上の鍵長の RSA 暗号鍵アルゴリズムを使用しなければならない（ただし、別途認められた場合は除く）。

利用者は 1,024 ビット以上[1]の鍵長の RSA 暗号アルゴリズムを使用しなければならない

6.1.6. 公開鍵のパラメータの生成、及び品質検査

規定しない。

---

[1] EPC に関する標準（「EPCglobal Certficate Profile Ratified Specification 1.0」2006 年 3 月 8 日 EPCglobal Inc.）では、西暦 2010 年以降においては 2,048 ビット以上の鍵の利用が推奨されているので、各データ交換共通認証局はこれに留意しなければならない

6.1.7. 鍵用途の目的

各データ交換共通認証局内のルート認証局及び中間認証局の証明書の keyUsage の値には keyCertSign と keyCertSign の値が設定される。これらの設定値は、ルート認証局及び中間認証局の秘密鍵が、下位の認証局または利用者の証明書への署名もしくは、それらに対する失効情報（ARL または CRL）の署名に利用されることを意味する。

利用者の証明書の keyUsage の値は各データ交換共通認証局が定める。

6.2. 秘密鍵の保護、及び暗号モジュール技術の管理

6.2.1. 暗号モジュールの標準と管理

各データ交換共通認証局の認証局秘密鍵は FIPS 140-1 レベル 3 相当以上の機能を有する暗号モジュール内で管理されなければならない。

各データ交換共通認証局が利用者の秘密鍵を作成する場合の要件については各データ交換共通認証局が定める。

6.2.2. 秘密鍵の複数人管理

各データ交換共通認証局の認証局秘密鍵は正当な権限を有する複数の者によって管理が行われ、一人の管理者の権限のみでは、認証局秘密鍵の利用が行えないようにするための相互牽制の仕組みが講じられなければならない。

6.2.3. 秘密鍵の預託

規定しない。

6.2.4. 秘密鍵のバックアップ

各データ交換共通認証局の認証局秘密鍵については、各データ交換共通認証局が定める。なお、各データ交換共通認証局は、利用者の秘密鍵を生成し、さらに当該秘密鍵のバックアップデータを取得していた場合は、利用者への秘密鍵の配送手続きが完了後に、当該バックアップデータも確実に削除しなければならない。また、利用者への秘密鍵の配送が終了した後は、利用者より秘密鍵のバックアップデータを受領してはならない。

6.2.5. 秘密鍵のアーカイブ

規定しない。

6.2.6. 秘密鍵の暗号モジュールへの移動

規定しない。

6.2.7. 暗号モジュール内での秘密鍵保存

各データ交換共通認証局の認証局秘密鍵は、暗号モジュール内で容易に読み取りが出来ない状態にて保管されなければならない。

6.2.8. 秘密鍵の活性化方法

各データ交換共通認証局の認証局秘密鍵は正当な権限を有する複数の者の関与が無ければ活性化されないような仕組みが講じられなければならない。

6.2.9. 秘密鍵の非活性化方法

規定しない。

6.2.10. 秘密鍵の破棄方法

各データ交換共通認証局の認証局秘密鍵が廃棄される必要がある場合は、認証局秘密鍵は確実に廃棄処理されなければならない。

利用者の秘密鍵が廃棄される必要がある場合は、利用者の秘密鍵は確実に廃棄処理されなければならない。

6.2.11. 暗号モジュールの評価

各データ交換共通認証局の認証局秘密鍵を格納する暗号モジュールは FIPS 140-1 レベル 3 以上の機能を有していなければならない。

各データ交換共通認証局が利用者の秘密鍵を作成する場合の要件については各データ交換共通認証局が定める。

6.3. その他の鍵ペア管理

6.3.1. 公開鍵のアーカイブ

各データ交換共通認証局は、自身が発行した全ての証明書を、証明書の有効期間の満了後、3 年間はアーカイブしなければならない。

6.3.2. 証明書の運用上の期間、及び鍵ペアの使用期間

各データ交換共通認証局のその全ての階層構造中の認証局証明書の有効期間及び認証局秘密鍵の利用期間は、最大で 20 年とする。利用者証明書の有効期間及び利用者の秘密鍵の利用期間は最大で 3 年 2 ヶ月とする。

6.4. 活性化データ

6.4.1. 活性化データの生成、及び設定

各データ交換共通認証局の認証局秘密鍵の活性化データは、正当な権限を有する複数の

人物の関与のもと、生成及び設定がなされなければならない。
各データ交換共通認証局が利用者の活性化データを作成する場合は、正当な権限を有する複数の人物の関与のもと、生成及び設定がなされなければならない。
利用者が自身の活性化データを生成する場合については、各データ交換共通認証局が定める。

6.4.2. 活性化データの保護
各データ交換共通認証局の認証局秘密鍵の活性化データは、正当な権限を有する複数の人物により、相互牽制のもとに管理されなければならない。
各データ交換共通認証局が利用者の秘密鍵を作成する場合、利用者への秘密鍵の配送が行われるまでは、秘密鍵の活性化データは正当な権限を有する複数の人物により、相互牽制のもとに管理されなければならない。また、当該活性化データは安全な方法にて利用者に配送されなければならない。また、各データ交換共通認証局は利用者に活性化データの配送手続きが完了後に、自身が管理する装置等に記録されていた利用者の活性化データを確実に削除しなければならない。
利用者は、自身で活性化データを作成した、または各データ交換共通認証局より活性化データを受領した以降は、当該活性化データを安全に保管しなければならない。

6.4.3. 活性化データの他の考慮点
規定しない。

6.5. コンピュータのセキュリティ管理
各データ交換共通認証局は広く認められたセキュリティ規格（「JIS Q 27002:2006 情報セキュリティマネジメントの実践のための規範」）等の規格で求められているコンピュータセキュリティ管理に関する要件を参考にし、それと同等の水準のコンピュータのセキュリティ確保に努めなければならない。

6.6. ライフサイクルの技術上の管理
各データ交換共通認証局は広く認められたセキュリティ規格（「JIS Q 27002:2006 情報セキュリティマネジメントの実践のための規範」）等の規格で求められているシステム保守に関する要件を参考にし、それと同等の水準のシステム保守の維持に努めなければならない。

6.7. ネットワークセキュリティ管理
各データ交換共通認証局は広く認められたセキュリティ規格（「JIS Q 27002:2006 情報セキュリティマネジメントの実践のための規範」）等の規格で求められているネットワーク

セキュリティ確保に関する要件を参考にし、それと同等の水準のネットワークセキュリティの維持に努めなければならない。

6.8. タイムスタンプ

各データ交換共通認証局は、5.4.1 項及び 5.5.1 項で保存すると規定した書類・電子データには日時情報を付与しなければならない（一部日付情報のみで可)。ただし、当該時刻情報に関して暗号技術によるタイムスタンプを付与することによる保護を行う必要はない。

7. 証明書、CRL、及び OCSP のプロファイル

7.1. 証明書のプロファイル

本節では各データ交換共通認証局が発行する証明書プロファイルについて規定する。

7.1.1. バージョン番号

各データ交換共通認証局が発行する証明書のバージョンは 3 とする。

7.1.2. 証明書の拡張

各データ交換共通認証局の認証局証明書(ルート認証局証明書、中間認証局証明書のみを指す。相互認証証明書及びリンク証明書は規定しない) の拡張領域は表 6 の通りとする。

表 6　認証局証明書の拡張領域

No.	フィールド	設定	クリティカル	仕様
1	authorityKeyIdentifier	△	FALSE	各データ交換共通認証局が定める
2	subjectKeyIdntifier	△	FALSE	各データ交換共通認証局が定める
3	keyUsage	◎	TRUE または FALSE	cRLSign,keyCertSign とする
4	extendedKeyUsage	△	FALSE	各データ交換共通認証局が定める
5	privateKeyUsagePeriod	×	-	-
6	certificatePolicies	△	FALSE	各データ交換共通認証局が定める
7	policyMapping	×	-	-
8	subjectAltName	△	FALSE	各データ交換共通認証局が定める
9	issuerAltName	△	FALSE	各データ交換共通認証局が定める
10	basicConstraints	◎	TRUE または FALSE	cA=TURE とする pathLenConstraint には値を設定しなければならない
11	nameConstraints	×	-	-
12	policyConstraints	×	-	-
13	cRLDistributionPoints	△	FALSE	各データ交換共通認証局が定める
15	subjectDirectoryAttributes	×	-	-
16	authorityInfoAccess	△	FALSE	各データ交換共通認証局が定める

(◎は必須、○は推奨、△は任意、×は不可を表す。)

また、各データ交換共通認証局が発行する利用者の証明書の拡張領域は表 7 の通りとする。

表 7　利用者の証明書の拡張領域

No.	フィールド	設定	クリティカル	仕様
1	authorityKeyIdentifier	△	FALSE	各データ交換共通認証局が定める
2	subjectKeyIdntifier	△	FALSE	各データ交換共通認証局が定める
3	keyUsage	◎	TRUE または FALSE	digitalSignature,keyEncipherment,dataEncipherment とする
4	extendedKeyUsage	△	FALSE	各データ交換共通認証局が定める
5	privateKeyUsagePeriod	×	-	-
6	certificatePolicies	△	FALSE	各データ交換共通認証局が定める
7	policyMapping	×	-	-
8	subjectAltName	△	FALSE	各データ交換共通認証局が定める
9	issuerAltName	△	FALSE	各データ交換共通認証局が定める
10	basicConstraints	△	FALSE	各データ交換共通認証局が定める
11	nameConstraints	×	-	-
12	policyConstraints	×	-	-
13	cRLDistributionPoints	◎	FALSE	CRL を配布する URI を記載する
14	subjectDirectoryAttributes	×	-	-
15	authorityInfoAccess	△	FALSE	各データ交換共通認証局が定める

（◎は必須、○は推奨、△は任意、×は不可を表す。）

7.1.3. アルゴリズムオブジェクト識別子

本項では、証明書への署名形式と証明書で証明される公開鍵の形式を規定する。基本領域のsignatureフィールドには sha256WithRSAEncryption (1.2.840.113549.1.1.11)、sha384WithRSAEncryption (1.2.840.113549.1.1.12)、sha512WithRSAEncryption (1.2.840.113549.1.1.13)、およびsha224WithRSAEncryption (1.2.840.113549.1.1.14) のいずれかが設定されなければならない。また、基本領域のsubjectPublicKeyInfフィールドにはrsaEncryption(1.2.840.113549.1.1.1)が設定されなければならない。

7.1.4. 名前の形式

各データ交換共通認証局及び利用者の名称は 3.1.2 項の内容に従う。また、issuer 及び

subject のデータ型は全て Printable String でなければならない。

7.1.5. 名前制約(nameConstraints フィールド)
使用してはならない。

7.1.6. 証明書ポリシーのオブジェクト識別子（certificatePolicies フィールドの一部）
各データ交換共通認証局が定める。

7.1.7. ポリシー制約拡張（policyConstraints フィールド）
使用してはならない。

7.1.8. ポリシー修飾子の構文及び意味（certificatePolicies フィールドの一部）
各データ交換共通認証局が定める。

7.1.9. クリティカルな証明書ポリシー拡張に対する処理の意味
各データ交換共通認証局が定める。

7.2. CRL のプロファイル

各データ交換共通認証局が発行する利用者の証明書の CRL は表 8 のフォーマットを満たさなければならない。ARL については規定しない。

表 8　CRL プロファイル

No.	領域名	フィールド		設定	クリティカル	仕様
1	CRL 基本領域	version		-		バージョン２を利用
2		signature		-		sha1withRSAEncryption
3		issuer		-		CRL を発行する認証局の名称が記載される（証明書を発行した認証局のみ）
4		thisUpdate		-		CRL 発行日時
5		nextUpdate		◎		thisUpdate より 10 日以内
6		revokedCertificates		-		
7			userCertificate	-		失効した証明書のシリアル番号
8			revocationDate	-		失効した証明書の日時
9			crlEntryExtensions (No.11~No.14)	△		
10		crlExtensions (No.15~20)		△		各データ交換共通認証局が定める
11	CRL エントリ拡張領域	reasonCode		△	FALSE	各データ交換共通認証局が定める
12		holdInstructionCode		×	-	-
13		invalidityDate		△	-	-
14		certificateIssuer		×	-	-
15	CRL 拡張領域	authorityKeyIdentifier		△	FALSE	各データ交換共通認証局が定める
16		issuerAltName		△	FALSE	各データ交換共通認証局が定める
17		cRLNumber		△	FALSE	各データ交換共通認証局が定める
18		deltaCRLIndicator		×	-	-
19		issueingDistributionPoint		△	FALSE	各データ交換共通認証局が定める
20		freshesCRL		×	-	-

（◎は必須、○は推奨、△は任意、×は不可を表す。）

＊No.6 から No.9 までの値は失効された証明書ごとの情報が記載される。

7.3. OCSP のプロファイル

規定しない。

8. 準拠性監査とその他の評価

8.1. 監査の頻度あるいは条件

各データ交換共通認証局は、本ポリシー及び各 CPS に準拠して業務を行っていることを確実にするために、必要に応じて監査を行わなければならない。ただし、利用者の識別及び書類の審査を行う業務については少なくとも 1 年に１度以上の監査を行わなければななら ない。

8.2. 監査人の要件

監査人は、監査に関する知識を有し、かつ認証業務に関する知識を有していなければなら ない。

8.3. 監査人と非監査人の関係

監査人は、外部の監査法人等に所属する者、あるいは監査対象と同じ組織に所属する者も認められる。ただし、監査対象と同じ組織に所属する者が監査人に任命される場合は、監査対象業務の運用に直接携わっている者であってはならない。

8.4. 監査の対象

準拠性監査の目的は各データ交換共通認証局が、本ポリシー及び各 CPS に準拠して業務を実施していることの確認のために実施される。監査の対象としては、発行業務、更新業務、失効業務が含まれるが、これに限定されない。

8.5. 監査指摘事項への対応

監査の結果、各データ交換共通認証局の業務が本ポリシーに反していることが判明した場合は、各データ交換共通認証局は当該事項の是正をただちに行わなければならない。また、当該是正処置について認定機関に報告を行わなければならない。それ以外の監査指摘事項については各データ交換共通認証局の判断により必要な是正処置を行わなければならない。

8.6. 監査結果の開示

各データ交換共通認証局は監査結果を外部に公開する必要はない。ただし、認定機関より準拠性に関する照会を求められた場合は、監査指摘事項の有無やその対応状況について報告を行わなければならない。

9. 他の業務上の問題、及び法的問題

9.1. 料金

9.1.1. 証明書の発行及び証明書の更新に関わる手数料

各データ交換共通認証局が定める。

9.1.2. 証明書の参照に関わる手数料

各データ交換共通認証局は、依拠当事者等が自身が発行した証明書をリポジトリ等より参照することことに関して手数料を入手してはならない。

9.1.3. 失効情報の参照に関わる手数料

各データ交換共通認証局は、依拠当事者等が、自身が発行した証明書の失効情報をリポジトリ等より参照することに関して手数料を入手してはならない。

9.1.4. 他のサービスに関する利用料金

規定しない。

9.1.5. 返金制度

規定しない。

9.2. 財務的責任

9.2.1. 保険の範囲

規定しない。

9.2.2. 他の資産

各データ交換共通認証局は、認証業務を健全に実施するために、十分な財務的健全性を有していなければならない。

9.2.3. 拡張された保証の範囲

規定しない。

9.3. 業務情報の機密性

9.3.1. 機密として扱う情報の範囲

9.3.2 項の記載内容と矛盾しない範囲において、各データ交換共通認証局が定める。

9.3.2. 機密として扱わない情報

各データ交換共通認証局は以下の情報を機密として取り扱ってはならない。

(1) 各 CPS
(2) 利用者規約
(3) 依拠当事者規約
(4) 自身が発行した証明書、及び証明書に記載されている情報
(5) CRL、及び CRL に記載されている情報

9.3.3. 機密として扱う情報を保護する責任

各データ交換共通認証局は、認証業務を実施する上で入手した情報を、認証業務を実施する上で必要とする場合を除いて、利用してはならない。

9.4. 個人情報のプライバシー保護

各データ交換共通認証局は自身が準拠する個人情報保護方針を公開し、当該方針に従って個人情報の保護を行わなければならない。

9.5. 知的財産権

本ポリシーの知的財産権は本ポリシー管理組織に帰属する。各データ交換共通認証局に関わるその他の規程等の知的財産権は各データ交換共通認証局が定める。

9.6. 表明保証

9.6.1. 認証局の表明保証

- 各 CPS に関して

  各データ交換共通認証局は各 CPS に従うこと。

9.6.2. 利用者の表明保証

利用者は以下の事項を実施又は遵守することを保証しなければならない。なお、各データ交換共通認証局は以下の保証事項を明確に利用者に理解させるために利用者規約を作成し、これを公開しなければならない。

- 証明書の申請に関して

  利用者は証明書の発行・更新・再発行時に各データ交換共通認証局に対して虚偽なく正確な内容の申請を行うこと。
- 証明書に記載されている内容に関して

  利用者は証明書を受領した際に、証明書に自身が申請した内容と異なる情報が含まれてことの確認を行うこと。また、証明書に記載されている内容に変更が生じた場合は速やかに各データ交換共通認証局により指定された手続きを行うこと。
- 鍵の管理に関して

  利用者は自身の秘密鍵を、紛失、改ざん又は盗難から保護するために適切な措置を講

じること。

- 各 CPS に関して

  利用者は各 CPS 及び利用者規約に従うこと。

9.6.3. 依拠当事者の表明保証

依拠当事者は以下の事項を実施又は遵守することを保証しなければならない。なお、各データ交換共通認証局は以下の保証事項を明確に依拠当事者に理解させるために依拠当事者規約を作成し、これを公開しなければならない。

- 証明書の検証に関して

  依拠当事者は証明書に依拠する前に、定められた手続きに従い、証明書の有効性の検証を行うこと。

- 認証局証明書の入手

  依拠当事者は各データ交換共通認証局及び認定機関によって指定された方法により誤り無く認証局証明書の入手を行うこと。

- 各 CPS に関して

  依拠当事者は各 CPS 及び依拠当事者規約に従うこと。

9.7. 無保証

各データ交換共通認証局は、9.6.1 項で規定された内容以上の保証は行わない。また、9.16.5 項で規定された内容に従って保証事項に関して免責される場合がある。

9.8. 責任の制限

各データ交換共通認証局の責任は、本ポリシー及び各 CPS に定められた要件を果たさなかった場合に限定される。また、損害賠償の際に各データ交換共通認証局が支払うべき金額は別段の定めにより制限される場合がある。

9.9. 補償

本ポリシーで規定された責任を果たさなかったことにより、各データ交換共通認証局が関係者に損害を与えた場合は、各データ交換共通認証局は損害を賠償する責任を有する。ただし、各データ交換共通認証局の責に帰さない理由により生じた損害については、各データ交換共通認証局は賠償を行う責任を有さない。

9.10. 有効期間と終了

9.10.1. 有効期間

本ポリシーは、認定機関に承認されたことにより有効化される。また、9.10.2 項で定める期間までは有効である。

9.10.2. 終了

本ポリシーは、認定機関が必要と認めた場合、無効化されることがある。

9.10.3. 終了の効果と効果継続

本ポリシーが無効化された場合であっても、9.3 節、9.4 節及び 9.5 節に関する規定は効力を継続するものとする。

9.11. 関係者間の個別通知と連絡

各データ交換共通認証局が定める。

9.12. 改訂

9.12.1. 改訂手続き

本ポリシーは、認定機関が必要と判断する場合は、改訂が行われる。

9.12.2. 通知方法、及び期間

認定機関が本ポリシーの改訂が必要と判断した場合は以下の手続きがとられる。

- 認定機関が軽微と判断する本ポリシーの変更

  改訂されたガイドラインが情報公開用サイトに掲載された段階で有効化される。
- 認定機関が軽微でないと判断する本ポリシーの変更

  改訂されたガイドラインを情報公開用サイトに掲載し、30 日間の猶予期間を経た後に当該ガイドラインは有効化される。なお、当該猶予期間内において関係者は認定機関に対して、コメント等を提出することができる。

9.12.3. オブジェクト識別子が変更されなければならない場合

規定しない。

9.13. 紛争解決手続き

各データ交換共通認証局が定める。

9.14. 準拠法

本ポリシーは、日本国内法規に準拠している。また、各データ交換共通認証局と関係者の間で係争が発生した場合は日本国内法規を準拠法とする。

9.15. 適用法の遵守

本ポリシーの運用にあたり、日本国内法規に抵触する可能性がある場合は、日本国内法規

が優先される。

9.16. 雑則

9.16.1. 完全合意条項

本ポリシーは、口頭で変更、追加、削除、または終了させることはできない。

9.16.2. 権利譲渡条項

関係者は、本ポリシーに定める権利義務を、如何なる担保にも供してはならない。なお、本ポリシーに反しない限りにおいて、各データ交換共通認証局がその業務の一部を第三者に委託することは認められる。

9.16.3. 分離条項

本ポリシーの一部または複数の条項が、何らかの事情によって無効化されたとしても、本ポリシーの他の条項の有効性は失われないものとする。

9.16.4. 強制執行条項

規定しない。

9.16.5. 不可抗力条項

以下の事象に起因する損害については、各データ交換共通認証局は免責される。

- 天変地異、地震、噴火、台風、洪水、雷、火災等などの災害
- 戦争、テロ行為、市民暴動等の不可抗力

9.17. その他の条項

規定しない。

改訂の要約

・V1.0.0（2019 年 7 月公開）作成

-流通システム標準普及推進協議会より認定業務を引き継ぐにあたり新規作成

データ交換共通認証局　証明書ポリシー

2019 年 7 月　発行

インターネット EDI 普及推進協議会
Japan internet EDI Association (JiEDIA)

本資料に関する問い合わせは、下記までお願いします。

JiEDIA 事務局：一般社団法人 情報サービス産業協会
https://www.jisa.or.jp/tabid/2821/Default.aspx

〒101-0047
東京都千代田区内神田 2-3-4
S-GATE 大手町北 6F
TEL：03-5289-7651（代表）
FAX：03-5289-7653