

令和6年3月1日  
法務省民事局  
(令和6年8月30日更新)

## 戸籍電子証明書等の提供の求め及び戸籍電子証明書等の提供の方法等に関する技術的基準

戸籍法施行規則（昭和22年司法省令第94号。以下「規則」という。）第79条の2の3第3項に規定する戸籍電子証明書等の提供の求め及び戸籍電子証明書等の提供の方法等に関して法務大臣が定める技術的基準は以下のとおりである。

### 第1 目的

戸籍法（昭和22年法律第224号。以下「法」という。）第120条の3第3項の規定による戸籍電子証明書等の提供の求め及び戸籍電子証明書等の提供（規則第79条の2第1項の戸籍電子証明書等の電磁的記録の方式を含む。以下「戸籍電子証明書の提供等」という。）が円滑かつ安全に行われるよう、電気通信回線を通じた戸籍電子証明書の提供の方法等について、技術的基準及び戸籍情報照会者（規則第79条の2の3第1項の戸籍情報照会者をいう。以下同じ。）の長の実施すべき事項を定めることを目的とする。

### 第2 用語の定義

#### 1 戸籍情報連携システム

法第118条第1項に規定する電子情報処理組織であって、市町村長の使用に係る電子計算機と電気通信回線で接続し、磁気ディスクをもって調製された戸籍又は除かれた戸籍の副本の保存、管理等を行う機能を有し、電気通信回線を通じて戸籍電子証明書の提供等を行う電子情報処理組織

#### 2 戸籍電子証明書連携サーバー

戸籍情報連携システムと戸籍情報照会者の使用に係る電子情報処理組織との間で、電気通信回線を通じた戸籍電子証明書の提供等に必要な処理を行う戸籍情報照会者の長の使用に係る電子計算機

#### 3 ファイアウォール

ネットワークにおいて不正侵入を防御する電子計算機又は同等の機能及び効果を有するソフトウェア

#### 4 データ

戸籍情報照会者の長の使用に係る電子情報処理組織において送信され、記録され、保存され又は提供される情報

## 5 プログラム

戸籍電子証明書連携サーバーに設置し、戸籍情報連携システムと戸籍電子証明書連携サーバーとの間の通信を作動させるための命令を組み合わせたもの

## 6 ファイル

戸籍情報照会者の長の使用に係る電子計算機に内蔵される記憶媒体に記録されているデータ

## 7 ドキュメント

戸籍電子証明書連携サーバーの設計、プログラム作成及び運用に関する記録及び文書

## 8 重要機能室

電子計算機、受電設備、定電圧・定周波電源装置等の設備を設置する室並びにその室の空気調和をする空気調和機及びその付属設備を設置する室

# 第3 体制、規程等の整備

## 1 体制の整備

### (1) 責任体制等の確立

戸籍電子証明書の提供等を円滑かつ安全に実施するとともに、戸籍電子証明書連携サーバーのセキュリティ（正確性、機密性及び継続性を維持することをいう。以下同じ。）を確保するため、戸籍電子証明書連携サーバーの企画、開発及び運用保守に関する責任体制並びに連絡体制を明確にすること。また、防災組織及び防犯組織を整備し、通常時及び非常時の責任体制の確立を図ること。

### (2) 監視及び緊急時連絡体制の整備

戸籍電子証明書連携サーバーの運用に際し、異常な状態を早期に発見し、法務大臣に連絡することができるよう体制の整備を図ること。

## 2 規程等の整備

戸籍電子証明書連携サーバーの企画、開発及び運用保守に関する規程を整備するとともに、戸籍電子証明書連携サーバーに関する設計書、操作手順書、緊急時における作業手順書等を整備し、適切な維持管理に努めること。

## 3 人事、教育、研修等

### (1) 要員管理

戸籍電子証明書連携サーバーの企画、開発及び運用保守に必要な職員の配置、交替等の人事管理を適切に行うこと。

### (2) 教育及び研修

戸籍電子証明書連携サーバーの企画、開発及び運用保守を実施する職員に対して戸籍電子証明書連携サーバーのセキュリティ対策についての教育及び研修を実施するための計画を策定し、職員に対する教育及び研修を適切に行うこと。

#### 4 セキュリティ対策

セキュリティ対策に関する情報の収集及び分析を実施するとともに、戸籍電子証明書連携サーバーの企画、開発及び運用保守の各段階におけるセキュリティ対策についての点検又は監査を実施し、その結果に基づき、戸籍電子証明書連携サーバーのセキュリティ対策の改善に努めること。

#### 5 緊急事態発生時の体制等

##### (1) 作動停止等発生時における事務処理体制

ア 戸籍電子証明書連携サーバーの構成機器、関連設備又はソフトウェアの障害等による戸籍電子証明書連携サーバーの全部又は一部の作動停止又は異常作動の発生（以下「作動停止等発生」という。）時の行動計画、法務大臣への連絡方法等について、あらかじめ定めること。

イ アにおいて定めた行動計画、連絡方法等に基づき、適切な対応を行うことができるよう、教育及び研修を行うこと。

ウ 作動停止等発生時には、その旨を速やかに法務大臣に連絡すること。また、戸籍電子証明書連携サーバーの復旧等に必要な措置等を講じ、作動停止等発生の根本原因及び再発防止策について検討を行い、その内容について法務大臣に連絡するとともに、再発防止に努めること。

##### (2) データの漏えいのおそれがある場合又は不正アクセス行為発生時における事務処理体制

ア データの漏えいのおそれがある場合又は不正アクセス行為発生（以下「不正アクセス行為等発生」という。）時の行動計画、法務大臣への連絡方法等についてあらかじめ定めること。

イ アにおいて定めた行動計画、連絡方法等に基づき、適切な対応を行うことができるよう、教育及び研修を行うこと。

ウ 不正アクセス行為等発生時には、その旨を速やかに法務大臣に連絡すること。また、被害状況の把握及び被害の拡大を防止するための措置等必要な対策を講じ、法務大臣に報告すること。さらに、不正アクセス行為等発生の根本原因及び再発防止策について検討を行い、その内容について法務大臣に連絡するとともに、再発防止に努めること。

## 第4 戸籍電子証明書の提供等の方法

### 1 戸籍電子証明書連携サーバー

戸籍電子証明書の提供等は、戸籍情報連携システムと戸籍情報照会者の使用に係る電子情報処理組織とを電気通信回線で接続し、戸籍電子証明書連携サーバーを経由して行うものとする。

## 2 戸籍電子証明書等の電磁的記録の方式

### (1) 戸籍電子証明書等のファイル形式

戸籍電子証明書等のファイル形式は、以下のとおりとする。

#### ア PDF形式

PDF (ISO 32000-1) とする。

また、PDFファイルに記録される画像情報の処理方式は、Flate方式又はCCITTFaxDecode方式とする。

#### イ XML形式

XMLバージョンはXML (XML 1.0、JIS X 4159:2005) とする。

また、XMLスキーマ定義は、以下のとおりとし、スキーマ定義ファイルは、法務大臣から戸籍情報照会者に対して提供するものとする。

XML Schema Definition Language (XSD) 1.1 Part 1: Structure

XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes

### (2) 戸籍電子証明書等の電子署名の方式

戸籍電子証明書等の電子署名の方式は、以下に定めるところによるものとする。

#### ア PDFファイル

PDF Public-Key Digital Signatureファイルとし、アドビ株式会社のPDF Public-Key Digital Signature and Encryption Specification Version 3.2の「2.1 PKCS#7 Signature Format部」に準拠する形式とし、同Formatの設定値を次に定めるところによるものとする。

なお、電子署名のアルゴリズムは、sha256WithRsaEncryptionとする。電子署名の際に用いる電子証明書は、政府認証基盤 (GPKI) の政府共用認証局の発行する法務大臣の官職証明書とする。

|           |                               |
|-----------|-------------------------------|
| キー        | 設定値                           |
| Type      | Sig                           |
| Filter    | [システムの設定する任意の値]               |
| SubFilter | adbe.pkcs7.detached           |
| Name      | Minister of Justice           |
| M         | [電子署名を行った時刻]                  |
| ByteRange | [ハッシュ値の生成に使用した部分のバイト範囲]       |
| Contents  | [PKCS#7署名データ (16進数によるバイナリ形式)] |

#### イ XMLファイル

XML Signature Syntax and Processing Version 2.0に準拠する Enveloped形式の電子署名が付されたファイル形式とする。

また、電子署名のアルゴリズムは、sha256WithRsaEncryptionとする。電子署名の際に用いる電子証明書は、政府認証基盤（GPKI）の政府共用認証局の発行する法務大臣の官職証明書とし、ファイル中には、当該電子証明書を記録するものとする。

## 第5 戸籍電子証明書連携サーバーの環境及び設備

### 1 建物及び重要機能室

#### (1) 建物及び重要機能室の保全等

- ア 戸籍電子証明書連携サーバーを設置する建物及び重要機能室（以下「建物等」という。）は、壁、窓、ドア等が容易に破壊されないよう必要な措置を講ずること。
- イ 建物等への侵入を検知するための措置を講ずること。
- ウ 電力及び電気通信回線の切断等を防止するための措置を講ずること。
- エ 重要機能室の外に設置された関連設備に対する不当な接触の防止について、必要な措置を講ずること。

#### (2) 重要機能室の配置及び構造

- ア 重要機能室の配置及び構造については、セキュリティ対策及び保守を容易に行うことができるよう配慮すること。
- イ 重要機能室は、その場所の表示を行わないなど、できるだけ所在を明らかにしないようにすること。
- ウ 重要機能室は、緊急事態発生の際の連絡設備を設けるなどし、連絡体制を整備すること。
- エ 重要機能室は、他の部屋と区別して専用の部屋とすること。
- オ 電子計算機室は、他の部屋と区分された、施錠可能な専用の部屋とすること。施錠可能な専用の部屋を確保できない場合は、電子計算機及び電気通信関係装置を厳重に固定し、ドキュメントを専用保管庫において施錠保管すること。
- カ 電子計算機室の常時利用する出入口を限定すること等により、侵入の防止を容易に行えるよう配慮すること。

### 2 障害の防止等

戸籍電子証明書連携サーバーの構成機器又は関連設備の各種障害又は損傷の発生を防止するとともに、これらの障害等の発生を検知し、これらの障害等が発生した場合の対策を図るため、必要な設備の整備等について適切な措置を講ずること。

### 3 電気通信回線設備

電気通信回線からのデータの盗取を防止するため、戸籍情報連携システムと戸籍電子証明書連携サーバーを結ぶ電気通信回線は、地方公共団体及び国相互間の通信用に設けた行政専用の回線を使用すること。ただし、同一の電子計算機室にあるなど情報の盗取の防止について必要な措置が講じられていると認められる場合は、この限りでない。

## 第6 戸籍電子証明書連携サーバーの管理

### 1 入退室管理

#### (1) 入退室及び鍵の管理

ア 重要機能室への入室者を限定すること。

イ 重要機能室の出入口の鍵を所定の場所に保管し、その管理は定められた者が行うこと。

ウ 重要機能室への入室者が入室する権限を有することを確認する方法をあらかじめ定めるとともに、重要機能室に入室しようとする者に重要機能室の出入口の鍵を貸与する際に、その者が入室する権限を有することを確認すること。

エ 重要機能室への入退室については、入退室管理台帳により適切に管理すること。

#### (2) 搬出入物品の確認

重要機能室へ物品を搬出入する際、重要機能室に入室する権限を有する職員に当該物品の内容を確認させること。

#### (3) 重要機能室の管理

戸籍電子証明書連携サーバーの構成機器及び関連設備等の盗難、損壊等を防止するため、重要機能室に入室する権限を有する者が不在となる場合の重要機能室の施錠等、必要な措置を講ずること。

### 2 戸籍電子証明書連携サーバーの通信制御等

#### (1) アクセス権限の限定

戸籍電子証明書連携サーバーの運用保守を実施する職員等に対してのみ、電子計算機、端末機、電気通信関係装置、電気通信回線、ファイル等に関し、必要なアクセス権限を付与すること。

#### (2) ファイアウォールによる通信制御

電気通信回線に接続する電子計算機若しくは電気通信関係装置における不正行為又は電子計算機若しくは電気通信関係装置への不正アクセス行為に対して戸籍電子証明書連携サーバーを保護するため、戸籍電子証明書連携サーバーと戸籍情報連携システムとの間にファイアウォールを

設置し、通信制御を行うこと。ただし、同一の電子計算機室にあるなど、通信制御を行う必要がないと認められる場合は、この限りでない。

(3) 電気通信関係装置の管理

エラー及び不正行為により電気通信関係装置の不当な運用が行われないうようにするため、電気通信関係装置の管理に当たっては厳重な確認を行うなど、管理権限がある者以外の者による操作を防止するための措置を講ずること。

(4) 通信相手相互の認証

戸籍電子証明書連携サーバーと戸籍情報連携システムとの間の通信については、通信相手相互の認証を行うこと。ただし、同一の電子計算機室にあるなど、通信相手の認証を行う必要がないと認められる場合は、この限りでない。

(5) データの暗号化

戸籍電子証明書連携サーバーと戸籍情報連携システムとの間の通信については、交換するデータの暗号化を実施すること。ただし、同一の電子計算機室にあるなど、通信の暗号化を行う必要がないと認められる場合は、この限りでない。

(6) 秘密鍵の厳重な管理

通信相手の認証及び通信の暗号化を行うために必要な秘密鍵を厳重に保護し、外部に漏えいすることを防止するための措置を講ずること。

(7) 時刻の正確性確保

不正行為の追跡、セキュリティを侵害された場合における証跡の解析等を容易にするため、重要機能室内の機器を正確な時刻に同期するための必要な措置を講ずること。

(8) 帯域の確保

戸籍電子証明書連携サーバーと戸籍情報連携システムとの接続に係る電気通信回線の通信について、情報提供等事務の処理が遅滞なく実施できるよう必要な帯域を確保すること。

(9) 戸籍情報連携システムと戸籍電子証明書連携サーバーとの間のデータ送信方法

大量のデータを送信する場合において、送信処理が途中で中断しても再送信が可能な仕組みを備えること。

3 構成機器及び関連設備等の管理

(1) 管理方法の明確化

ア 戸籍電子証明書連携サーバーに機器を接続するための手続、方法等を定めるとともに構成機器及び関連設備等の管理方法を明確にするこ

と。

イ 使用する戸籍電子証明書連携サーバーの構成機器、数量等を体系的かつ一元的に記録管理し、現況と一致させること。また、この記録管理された内容を関係職員に周知し、記録管理している戸籍電子証明書連携サーバーの構成機器以外のものを使用しないこと。

(2) 保守の実施

戸籍電子証明書連携サーバーの構成機器及び関連設備の保守を定期的に又は随時に、実施すること。また、保守の実施に当たっては、エラー及び不正行為を防止し、データを保護するため、必要な措置を講ずること。

(3) 稼動状況の監視

緊急事態や障害を早期に発見するため、戸籍電子証明書連携サーバーの構成機器の稼動状況を監視すること。

(4) 不正プログラムの混入の検知等

戸籍電子証明書連携サーバーにコンピュータウイルス等の不正プログラムが混入されていないかどうかを監視する措置を講じ、混入されていた場合には駆除する措置を講ずること。また、コンピュータウイルス等の不正プログラムが発見された場合の必要な措置を定め、戸籍電子証明書連携サーバーを運用する職員に周知すること。

4 ファイル、ドキュメント等の管理

(1) ファイル及びドキュメントの取扱い及び管理

ア ファイル及びドキュメントについては、定められた場所に保管すること、受渡し及び保管に関し必要な事項を記録すること、使用、複写、消去及び廃棄は責任者の承認を得て行うとともに、その記録を作成すること等、これらの取扱い及び管理の方法を明確にすること。

イ ファイル、プログラム及びドキュメントの内容については、最新の状態にしておくこと。

ウ ファイル、プログラム及びドキュメントを変更した場合については、変更者及び版数の管理を行うこと。

エ プログラムの改ざん、消去等を防止するために、プログラムの登録及び抹消は、責任者の指示又は承認を受けた者が行うこと。

オ ファイル、プログラム及びドキュメントを廃棄する場合には、消磁、破碎、溶解等の措置を講ずること。

(2) 帳票の管理

ア 重要な印字済みの帳票の受渡し及び廃棄の方法を定めること。

イ 事務室の出力装置から出力する場合のデータの漏えいを防止するため必要な措置を講ずること。

(3) 提供プログラムの管理

戸籍電子証明書連携サーバーに設置するプログラムのうち、法務大臣が提供するものがある場合、当該プログラム、当該プログラムに係るドキュメント等について、適切に管理すること。また、これらについて、法務大臣から返却又は廃棄を求められたときは、これに応じること。

5 障害時等の対応

(1) 障害の早期発見

戸籍電子証明書連携サーバーの障害箇所を発見するための機能を整備すること。

(2) 早期回復のための代替機能等の整備

ア 重要なファイルについては、他の磁気ディスクに複製することとし、必要に応じ、複製された磁気ディスクと当該ファイルを記録した磁気ディスクとは別に保管すること。

イ 障害が発生した場合に、複製された重要なファイル等を基に速やかに戸籍電子証明書連携サーバーを回復させるための機能を整備すること。

(3) 不正アクセスの早期発見

不正アクセスを早期に発見するための機能を整備すること。

(4) 不正アクセスが判明した場合の対応

不正アクセスが判明した場合、被害状況の把握、被害拡大を防止するための措置等必要な措置を講ずること。

6 委託等を行う場合の措置

(1) 委託先事業者等の社会的信用等の確認

戸籍電子証明書連携サーバーの運用保守等について、委託を行う場合には、委託先事業者等の社会的信用と能力を確認すること。

(2) 委託先事業者等に対する監督

委託先事業者等に対し、必要なセキュリティ対策を実施させるとともに、適切な監督を行うこと。また、委託先事業者等による不正行為を防止するため、必要な措置を講ずること。

(3) 再委託の制限等

委託業務の一部を第三者に再委託する場合の制限、事前申請及び承認に関する事項を委託先事業者等とあらかじめ取り決めること。

(4) 秘密保持に関する措置

委託先事業者等から、その従事者に係る秘密保持に関する誓約書を提出させる等の措置を講ずること。

第7 戸籍情報連携システムへの接続等における留意事項

新たに戸籍情報連携システムと接続し、戸籍電子証明書の提供等事務を開始しようとするときは、あらかじめ法務大臣と必要な調整を行うこと。

第8 戸籍電子証明書の提供等事務に関し法務大臣が定める事項

1 法務大臣が定める仕様

インターフェイス仕様については、法務大臣が定めるものとする。

2 その他法務大臣が定める事項

ここに定めるもののほか、戸籍電子証明書の提供等事務に関し必要な事項は、法務大臣が定めるものとする。