|  |
| --- |
|  |
| カードAP搭載事務取扱要領　（記載例） |
|  |
| 令和　年　月　日 |
| 株式会社○○○○ |
|  |

[１ 目的 1](#_Toc26365900)

[２ 対象業務 1](#_Toc26365901)

[３ 役員等の基準および複数利用の有無 1](#_Toc26365902)

[3.1 役員等の基準 1](#_Toc26365903)

[3.2 複数での利用の有無 1](#_Toc26365904)

[４ 本業務で利用するアプリケーション等の基準 1](#_Toc26365905)

[4.1 カードAPの基準 1](#_Toc26365906)

[4.2 カードAPの搭載等を行うシステムの基準 2](#_Toc26365907)

[4.3 カードAPの搭載等を行うシステムと端末機の通信の基準 2](#_Toc26365908)

[4.4 端末機の基準 3](#_Toc26365909)

[５ 本業務の手順および基準 4](#_Toc26365910)

[5.1 規定等の整備 4](#_Toc26365911)

[5.2 業務の委託 7](#_Toc26365912)

[5.3 内閣総理大臣及び総務大臣に対する報告 7](#_Toc26365913)

[5.4 その他 7](#_Toc26365914)

# 目的

この要領は、「通知カード及び個人番号カードに関する技術的基準（平成27年総務省告示第314号）」（以下「技術的基準」という。）に基づき、カードAPの搭載等の業務（以下「本業務」という。）を実施するにあたり、必要な事項を定めるものとする。

# 対象業務

カードAPの搭載等に係る業務は、カードAPを利用して提供するサービス全てをさすものとする。

# 役員等の基準および複数利用の有無

## 役員等の基準

役員および本業務を統括する者は、次の者（①かつ②）ではないことについて、誓約書で宣言することとする。

①行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）、暴力団員による不当な行為の防止等に関する法律（平成３年法律第77号）若しくはこれに相当する外国の法令に違反し、又は刑法（明治40年法律第45号）若しくは暴力行為等処罰に関する法律（大正15年法律第60号）の罪を犯し、

②罰金の刑に処せられ、その刑の執行を終わり、又はその刑の執行を受けることがなくなった日から５年を経過しない者

## 複数での利用の有無

本業務は、複数利用は行わないこととする。（※複数で利用する場合は、利用事業者ごとに3.1役員等の基準を満たす旨の誓約書および利用事業者一覧表を本申請の代表事業者がとりまとめた上で提出すること。）

# 本業務で利用するアプリケーション等の基準

## カードAPの基準

カードAPは、○○（機構から提供を受ける機構の所有に係るアプリケーション（標準カードAP）又は民間事業者からデータの提供を受け機構が作成したアプリケーション（独自カードAP）のいずれかを選択して記入）を採用し、○○サービスを提供することとする。なお、カードAPタイプは○○（標準カードAPの場合、記入）とする。

## カードAPの搭載等を行うシステムの基準

カードAPの搭載等を行うシステムは、地方公共団体情報システム機構（以下、「機構」という。）が整備する「マイナンバーカードアプリケーション搭載システム（以下「カードAP搭載システム」という。）」を利用する。システムの利用形態は、機構の提供するクラウドサービスを利用する形態とする。

*システム構成図等を表記*

## カードAPの搭載等を行うシステムと端末機の通信の基準

カードAPの搭載等を行うシステムと端末機の通信においては、機構がクラウドサービスで提供するセキュリティ対策により、以下の項目について対策を講じることで情報セキュリティを確保する。

#### 通信の制御

カードAP搭載システムと端末機の通信経路中に、有人監視または自動発報による監視が可能なファイアウォールを構築し、暗号化通信以外での接続はすべて拒否され、アクセス可能なサーバおよびポートも必要最小限の設定となっている。

#### 通信データの盗取の防止

カードAP搭載システムと端末機をつなぐ回線は、IP-VPNとし、不特定多数の公衆からアクセスできないようにする。

#### 通信データの暗号化

カードAP搭載システムと端末機の間で行う通信はすべて暗号化(SSL)しており、特に重要な通信(マイナンバーカードとの鍵交換等)の処理については、さらに通信でやり取りをするデータを暗号化処理している。

## 端末機の基準

カードAP搭載システムを利用する端末機は、以下の対策を講じることで情報セキュリティを確保する。

#### 専用の端末機の準備

#### 端末機は、本業務専用に設置しその他の用途では利用しないこととする。

#### コンピュータウィルス等の不正プログラムへの対策

#### コンピュータウィルス等の不正プログラムが混入しないよう、以下の措置を講じる。

##### 端末機のOSは○○（セキュリティパッチ適用の頻度を記入）でセキュリティパッチを適用し、最新の状態にする。その他、緊急でセキュリティパッチを適用する場合がある。

##### 端末機にはウィルス対策ソフトをインストールするとともに、○○（パターンファイル最新化の頻度を記入）でパターンファイル（ウィルス定義ファイル）を適用する。

##### 端末機はインターネットに接続しないこととし、OSセキュリティパッチおよびウィルス対策ソフトのパターンファイルは、インターネットには接続しない方法により端末機に適用することとする。

##### ウィルス対策ソフトにより不正プログラムの混入を監視し、混入されていた場合は駆除できるようにする。

#### 端末機の盗取への対策

#### 端末機は、入室ができる者が限定され、かつ入退室記録が管理できる場所に設置するとともに盗難防止ワイヤー取り付ける等、盗取および不正操作を防ぐ。

#### 端末機を管理する者の任命

#### 端末機のセキュリティ設定、カードAP搭載システムの操作者（オペレータ）管理などの管理業務を行う端末機管理責任者、マイナンバーカードへのアプリケーションの搭載などを行う端末機操作権限保持者は、業務統括責任者が選任することとし、該当者の名簿を作成・管理する。

#### 端末機へのアクセス権限

#### カードAP搭載システムへのログインは、生体認証（指紋、手の静脈など）による認証を必要とする。なお、身体の障がい等、やむを得ない事情により、生体情報による認証が行えない者は、該当者の申請によりパスワードによる認証もできることとする。

#### 操作履歴の記録

#### 端末機OSのイベントログ、生体認証システムおよびパスワードによるログイン履歴を記録できるようにする。また、不正ログインがないか、操作ログを●●に１回確認を行うこととする。

# 本業務の手順および基準

## 規定等の整備

#### 業務の手順

業務従事者の業務手順は〇〇（別途定めるアプリケーション登録手順書等）に定めることとし、変更が生じた場合は、軽微なものを除き事前にデジタル庁及び総務省担当部署と協議し、遅滞なくこれを事務取扱要領等に反映し、必要に応じて資料等を提出することとする。

#### 業務従事者の責任および権限並びに指揮命令系統

業務従事者の責任および権限は以下のとおりとし（必要に応じて追加及び修正可）、本業務従事者はすべて当社役社員とする。また、指揮命令系統を含む組織体制図は、〇〇（別途定める指揮命令系統を含む組織体制図等）に定める。

責任および権限並びに指揮命令系統を変更する場合は、遅滞なく関連する事務取扱要領等を改訂する。

##### 業務統括責任者

業務統括責任者は本業務における最高責任者で、本業務を統括し、技術的基準に基づく確実な実施および運用に関する責任および権限を持ち、○○（別途定める業務一覧等）に定めた業務を行う。

なお、業務統括責任者は○○（選任元を記入すること）から選任するものとし、「行政手続における特定の個人を識別するための番号の利用等に関する法律（平成25年法律第27号）、暴力団員による不当な行為の防止等に関する法律（平成３年法律第77号）若しくはこれに相当する外国の法令に違反し、又は刑法（明治40年法律第45号）若しくは暴力行為等処罰に関する法律（大正15年法律第60号）の罪を犯し、罰金の刑に処せられ、その刑の執行を終わり、又はその刑の執行を受けることがなくなった日から５年を経過しない者」ではない者とする。

##### 端末機管理責任者

端末機管理責任者は本業務に利用する端末機の管理に関する権限を持ち、○○（別途定める業務一覧等）に定めた業務を行う。

なお、端末機管理責任者は端末機操作権限保持者を兼ねることはできない。

##### 端末機操作権限保持者

端末機操作権限保持者は本業務に利用する端末機の操作に関する権限を持ち、○○（別途定める業務一覧等）に定めた業務を行う。

なお、端末機操作権限保持者は端末機管理責任者を兼ねることはできない。

##### 各部門の長

各部門の長は自らの部門に所属する者に対し、○○（別途定める業務一覧等）に定めた業務を行う。

##### サービス利用者

サービス利用者は、○○（別途定める業務一覧に記載されているサービス利用者の業務範囲を記入すること）とし、○○（別途定める業務一覧等）に定めた業務を行う。

#### 本業務の委託の有無

本業務は他に委託を行わないこととする。（※委託を行う場合は、業務委託に係る手続き及び委託業務の内容の明確化、委託元の指示の遵守及び責任分担保証等の明確化並びに業務が適切に行われていることの管理等について記載を行うこと。）

#### 本業務に対する監査

##### 業務監査責任者

業務監査責任者は本業務に対する監査を統括する権限を持ち、○○（別途定める業務一覧等）に定めた業務を行う。

なお、業務監査責任者は、○○（役職名等）とし、業務監査責任者は業務統括責任者を兼ねることはできない。

##### 業務監査受任者

業務監査受任者は業務監査責任者から指示を受けて監査を実施することとし、○○（別途定める業務一覧等）に定めた業務を行う。

なお、業務監査受任者は、業務監査責任者が選任する。

##### 被監査者

被監査者は、業務統括責任者とする。

##### 監査基準

監査基準は業務監査責任者が定める〇〇（別途定める業務監査基準書等）に準じることとする。

##### 監査計画

監査計画は事前に業務監査受任者が〇〇（別途定める業務監査計画書等）を作成の上、業務監査責任者の確認を受けることとする。

なお、監査は定期的（頻度を記入。例：年次）に実施することとし、（例：毎年○月○日から○月○日までの）本業務実施状況を監査することとする。

##### 監査の実施

監査あたっては業務監査受任者が業務監査計画書に従い、業務監査基準書に基づいて○○（別途定めるアプリケーション登録手順書等）に規定される業務が適正に運営されていることを確認することとする。

なお、業務統括責任者は、端末機管理責任者および端末機操作権限保持者、その他必要に応じてその他関係者(サービス利用者等)を同席させることができることとする。

##### 監査結果の評価および対策

監査実施後には「監査報告書」を作成し、監査結果により設備や事務取扱要領等の見直しが必要な場合は見直しを実施し、事務取扱要領の改版を行う。

また、セキュリティ対策技術の最新動向を踏まえた設備、事務取扱要領等の見直しについては、「カードAPの搭載等の業務手順に関する規定」にて端末機管理責任者の通常業務としており、監査時に当該業務が適切に実施されているかを確認している。

#### 業務に係る記述に関し充分な知識および経験を有する者の配置

業務統括責任者および端末機管理責任者は、マイナンバーカードやカードAP搭載システム等に加え、一般的な個人情報保護等に関する十分な知識及び経験を有する者が従事する。

#### 業務の実施に際し知り得た情報の漏えいおよび目的外利用の防止並びに業務に係る帳簿書類の記載内容の漏えい、滅失又は毀損の防止のために必要な措置

業務に係る帳簿書類は、ファイリングした上で施錠可能な場所に保管し、鍵は端末機管理責任者もしくは端末機管理責任者が認めた者が管理することとする。帳簿書類の複製に際しては端末機管理責任者が立ち会うこととし、捺印する等により複製資料であることが容易に判別できる対策を講ずる。

#### 危機管理

災害等により端末機の破損および端末機とカードAP搭載システムを接続する電気通信回線の途絶などが生じた場合、代替機器の構築および回線業者に対する通信復旧依頼を実施し、速やかに業務を再開できるようにする。

#### 業務に係る教育訓練

##### 教育訓練実施者・対象者

教育訓練実施者は、業務統括責任者もしくは業務統括責任者から委任された者とする。教育訓練対象者は、本業務に従事する者のうちから、教育訓練実施者が決定することとする。

##### 教育訓練内容・実施時期

カードAPの搭載等の〇〇（別途定めるアプリケーション登録手順書等）に定めた業務内容および対象事務の利用方法にかかる教育を行う。

教育訓練は○○（頻度を記入すること。例：年次）で実施することとする。

## 業務の委託

（業務の委託がある場合に記載する。）

委託契約内容や委託先事業者のセキュリティ対策等について記載する。

## 内閣総理大臣及び総務大臣に対する報告

業務の監査結果及びカードAPの搭載等の件数は、毎年1回、「条例等利用アプリケーションの搭載等の業務に係る報告書」に基づき業務監査責任者が報告することとする。

## その他

以下の、技術的基準第9個人番号カードの条例等利用領域等の利用を遵守する

|  |
| --- |
| **第９　個人番号カードの条例等利用領域等の利用**  **１　法第18条の条例等に規定する事務以外の事務の処理への利用の禁止等**  **(1) 法第18条の条例等に規定する事務以外の事務の処理への利用の禁止**  個人番号カードの半導体集積回路に、住民基本台帳ネットワークシステムに係るアプリケーション、券面事項確認アプリケーション、券面事項入力補助アプリケーション、公的個人認証サービスアプリケーション又は条例等利用アプリケーション以外のアプリケーションを搭載してはならないこと。また、個人番号カードに貼り付けた磁気テープを利用する場合その他の電磁的方法により必要な事項を記録して利用する場合においても、法第18条の条例等に規定する事務以外の事務の処理に利用してはならないこと。  **(2) 条例等利用領域管理システム等の導入**  個人番号カードの半導体集積回路を法第18条の条例等に規定する事務の処理に利用する場合は、法第18条各号に掲げる者は、条例等利用領域に条例等利用アプリケーションのみを安全かつ確実に搭載する等の運用及び管理を行うシステム等を導入すること。また、当該システム等は、法第17条第３項に規定する措置を講じた個人番号カードの半導体集積回路に、条例等利用アプリケーションを搭載できるものとすること。  **２　個人番号カードの領域間の独立性の確保**  **(1) 基本利用領域等と条例等利用領域間の独立性の確保**  個人番号カードの半導体集積回路を法第18条の条例等に規定する事務の処理に利用する場合は、住民基本台帳ネットワークシステム又は券面事項確認アプリケーション、券面事項入力補助アプリケーション若しくは公的個人認証サービスアプリケーションに係るシステムが条例等利用領域に情報を記録し、又は当該領域の情報を読み取ることができない措置を講ずること。  また、条例等利用アプリケーションに係るシステムが基本利用領域、券面事項確認利用領域、券面事項入力補助領域又は公的個人認証サービス利用領域に情報を記録し、又は公的個人認証サービス利用領域に記録された情報を読み取ることができない措置を講ずること。  **(2) 複数の条例等利用領域間の独立性の確保**  個人番号カードの半導体集積回路を複数の法第18条の条例等に規定する事務の処理に利用する場合は、それぞれの条例等利用アプリケーションに係るシステムがそれぞれの条例等利用領域以外の領域に情報を記録し、又は当該領域に記録された情報を読み取ることができない措置を講ずること。  **３　条例等利用アプリケーションにおける個人情報の保護**  **(1) 法第18条の条例等に規定する事務の処理に応じた個人情報保護措置の実施**  個人番号カードの半導体集積回路を法第18条の条例等に規定する事務の処理に利用する場合は、暗証番号、発行前の不正使用を防止するための情報、相互認証を行うための情報又はアクセス権限の制御その他の個人情報の適切な管理のために必要な措置を講ずること。  **(2) 必要最小限の個人情報の記録**  個人番号カードの条例等利用領域内には、特に必要性が認められる場合を除き、条例等利用アプリケーションに係るシステムへアクセスするための利用者番号等以外の個人情報を記録しないこと。この場合において、当該利用者番号等には、住民票コードを使用しないこと。  **(3) 希望するアプリケーションの搭載等**  法第18条第２号に掲げる者は、条例等利用アプリケーションの全部又は一部の個人番号カードへの搭載を希望する者に限って、当該アプリケーションを当該希望する者の個人番号カードに搭載するほか、個人番号カードに貼り付けた磁気テープ等を利用する場合においても、個人番号カードに貼り付けた磁気テープ等の利用を希望する者に限ってその利用を行うこと。また、法第18条第１号に規定する市町村の機関は、同条の規定により個人番号カードを利用する場合には、利用を希望する者に限ってその利用を行うこと。 |

|  |  |  |
| --- | --- | --- |
| 改訂日 | 版数 | 改訂内容 |
| yyyy/mm/dd | 第1.0版 | 制定 |
|  |  |  |
|  |  |  |
|  |  |  |