マイナンバーカード機能等のスマートフォンへの搭載に係るセキュリティ規定作成業務

調達仕様書

令和６年２月

デジタル庁

目　次

１．件名

マイナンバーカード機能等のスマートフォンへの搭載に係るセキュリティ規定作成業務

２．背景・目的

マイナンバーカードの機能のスマートフォン搭載（以下「スマホ搭載」という）については、「マイナンバー制度及び国と地方のデジタル基盤の抜本的な改善に向けて（国・地方デジタル化指針）」（令和２年 12 月 25 日閣議決定）等に基づき、具体的在り方について検討の上、技術検証・システム構築を行うこととされた。

上記を踏まえ、デジタル庁（以下「当庁」という）において、令和５年５月に Android 端末へのスマホ用電子証明書搭載サービスを開始した。

「デジタル社会の実現に向けた重点計画（令和５年６月９日閣議決定）」においては、今後、スマートフォン用電子証明書について、順次、利用できるサービスの拡大を図るとされている。マイナンバーカード機能等のスマートフォンへの搭載に係る実証事業において、mdoc 発行管理システムを開発するにあたって、mdoc ファイルの認証局・発行局のポリシー及び運用規定をドキュメントとして策定する必要がある。

mdoc 認証局・発行局のポリシー及び運用規定（今回の調達の背景）

本調達は、各種資格者証の情報の格納を可能とする、汎用的な mdoc 発行管理システムにおける、mdoc 認証局・発行局のポリシー及び運用規定に係るセキュリティ規定作成業務を専門の事業者にその業務を請け負わせるものである。

※ mdoc 認証局・発行局のポリシー及び運用規定を CP/CPS という。

CP: Certificate Poricy, CPS: Certification Practice Statement

本文書では、上記 CP/CPS のことを mdoc 認証局・発行局のポリシー及び運用規定に係るセキュリティ規定と表記している。

３．契約期間

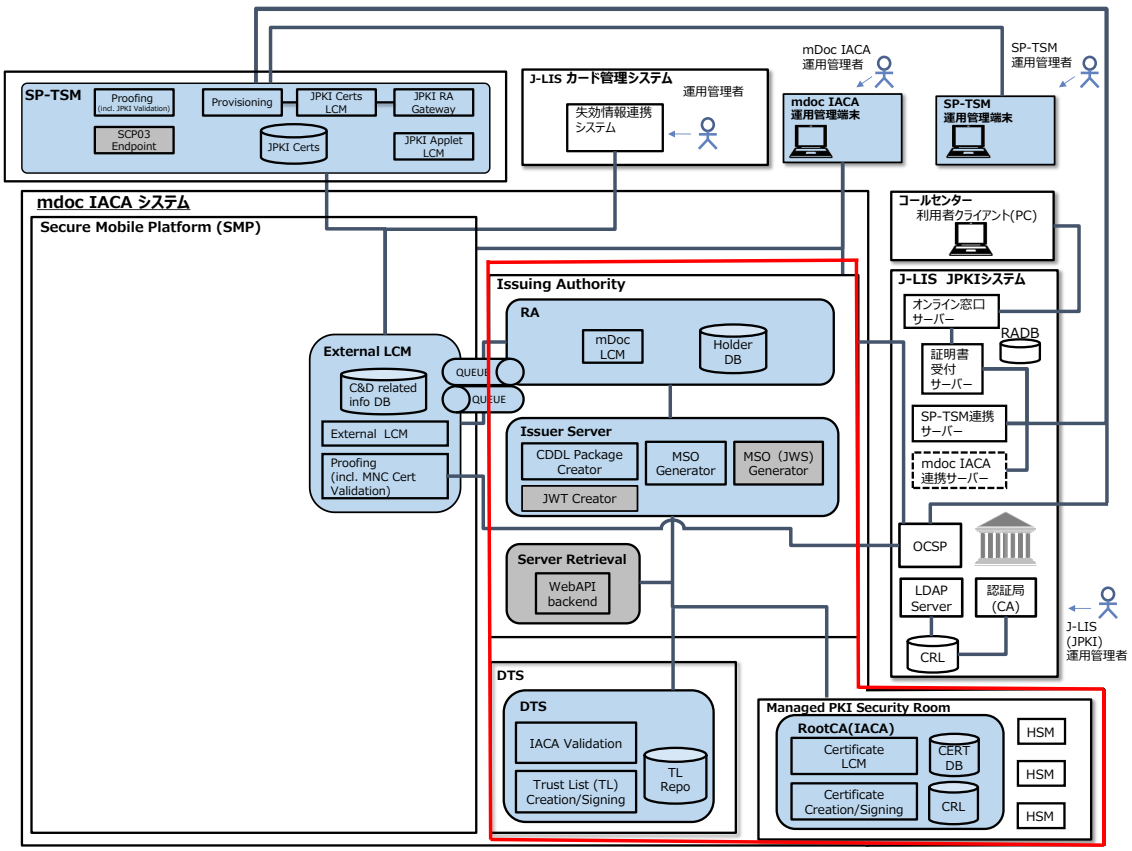
本業務の契約期間は、契約締結日から令和６年 10 月 31 日（木）までとする。

４．業務の概要等

（１）業務の概要

ア　業務の範囲等

本業務で策定する mdoc ファイルの認証局･発行局のポリシー及び運用規定の範囲(概要）を、図表１に示す。CP/CPS の対象となるのは、図表１　業務の範囲（概要）で示す赤線の範囲内の Issuing Authority の RA, Issuer Server(Document Signer), DTS, Managed PKI Security 内にある RootCA, HSM クラスターが対象となる。



図表 1.　業務の範囲（概要）

本 mdocIACA システムは、Managed PKI Security Room に位置する Root CA とガバメントクラウド上に位置する中間 CA である Issuer Server、RA(: Registration Authority 登録局), DTS(* Digital Trust Service)から構成されている。RootCA と Issuer Server 及び DTS の署名用の秘密鍵は、HSM(: Hardware Security Module)クラスターの中でセキュアに保管されている。

Managed PKI Security Room は、Managed PKI ベンダーのオンプレミス環境である。Issuer Server、RA, DTS は、ガバメントクラウド上で構築する。

Issuer Server(Document Signer)の DS 電子証明書は、Root 認証局で電子署名される。また、Issuer Server は、mdoc の MSO(: Mobile Security Object)に電子署名するための認証局である。

Root 認証局は、キーセレモニー後、DS 電子証明書に電子署名後、シャットダウンしエアシャットした状態で保管される。

mdoc ファイルの認証局・発行局のポリシー及び運用規定は、mdoc profile の詳細や図表１の赤線枠で示す mdoc IACA システムを対象としたドキュメントである。

Root 認証局及び中間 CA としての Document Signer、MSO (:Mobile Security Object)の有効期限/再発行の間隔等の運用は、以下のように CP/CPS で規定すること。

図表 2.　Root 証明書、DS 電子証明書、MSO の有効期限、再発行の間隔

大区分	中分類	CP/CPS での運用規定内容
Root 認証局	自己署名証明書の有効期限、 新しい署名鍵のための証明書 発行開始期限	最大有効期限　最大５年 発行間隔　　5 年毎 利用期限が切れる１ヶ月前 **5 年毎　(初回のみ 4 年 11 ヶ月毎)**
Document Signer (中間 CA)	DS 電子証明書の有効期限、 新しい署名鍵のための証明書 発行開始期限	最大有効期限　最大３ヶ月 発行間隔　　３ヶ月毎 利用期限が切れる１ヶ月前 **３ヶ月毎（初回のみ２か月後）**
MSO	MSO の有効期限、再発行の間隔	最大有効期限　最大 30 日 発行期間　**30 日毎** (米国 mDL 運用基準)

イ　CP/CPS 記載事項の骨子

- mdoc IACA Root 認証局の鍵の更新

  5 年毎（２回目のみ４年 11 ヶ月後）に Root 認証局の鍵の更新を行なう。
  鍵ペア更新時には、古い公開鍵と新しい公開鍵の認証パスを構築するリンク証明書を発行し、DTS 上で公開する。

- mdoc IACA 中間 CA(Document Signer 認証局)の鍵の更新

  ３ヶ月毎(初回のみ２ヶ月後）に DS 認証局の鍵の更新と DS 証明書の再発行を行なう。鍵ペア更新時には、古い公開鍵と新しい公開鍵の認証パスを構築するリンク証明書を発行し、DTS 上で公開する。

- mdoc IACA MSO(:Mobile Security Object)の更新
  MSO の有効期限は、発行から 30 日とする。
  MSO の有効期限は、 validfrom に発行日付け, validUntil に有効期限の日付けを格納する運用とする。Verifier(検証者）は必ず有効期限内かを確認しなければならない。

補足）選択的情報開示のチェックを行なう際、Verifier(検証者)側は、CP/CPS で MSO の validityInfo の validFrom～ validUntil の有効期限日時内であることのチェックを必ず行なう実装とすることを規定すること。

```
ValidityInfo = {
    "signed" : tdate,
    "validFrom" : tdate,
    "validUntil" : tdate,
    ? "expectedUpdate" : tdate
}
```

図表 3. ISO/IEC18013-5 で規定されている ValidityInfo 構造体

ウ 証明書と失効記録(CRL/ARL)の プロファイルを CP/CPS で規定すること

Root 認証局の自己署名電子証明書と Document Signer 認証局の DS 電子証明書のプロファイルの詳細は、別紙の技術仕様書の中で規定することとし、CP/CPS においては技術仕様書を参照する規定のみ記載すればよい。(技術仕様書は本調達の範囲外とする。)

なお、Root 認証局の自己署名証明書及びリンク証明書には、以下の情報を含めることを CP/CPS で規定すること。また、各証明書及び CRL/ARL は、ISO/IEC18013-5 に準拠した仕様とすることを CP/CPS で規定すること。

- バージョン番号（X.509 証明書フォーマットのバージョン番号）
- シリアル番号（署名用 CA 内で発行済み証明書を識別するための番号）
- 署名アルゴリズム（署名用 CA が当該自己署名証明書へ署名する際に用いた アルゴリズム情報）
- 発行者情報（当該自己署名証明書を発行した機構名が X.500 識別名で記述 - 65 - される）
- 有効期間の開始日（当該自己署名証明書の発行日）
- 有効期間の終了日（発行日の 10 年後）
- 公開鍵（署名用 CA の公開鍵）
- 拡張情報

エ　mdoc のプロファイルを CP/CPS で規定すること

・番号法、公的個人認証法の改正で対応する mdoc のデータ項目については、.JP の日本固有の namespace に格納する。
換言すると物理的なマイナンバーカードに格納されている情報で mdoc に格納する情報は、.JP Namespace に限定する。(Global namespace は利用しない。)

・省令で生年月日の二次的利用（age over ○○、age in years 等）は、mdoc のデータ項目に格納できるようにすることを検討する。その際、Global namespace に格納することを検討する。

CP/CPS の中で、以下を規定すること。

Doctype/Namespace (.JP 関連)

Doctype:　　org.iso.23220.1.jp.mnc

Namespace:　　org.iso.23220.1.jp

図表 4.　マイナンバーカード mdoc データ項目一覧(案)

Data element	Data element identifier	Character set	encoding	例
姓名	full_name	UTF-8	tstr	“山田　太郎”
生年月日	birth_date_unicode	UTF-8	tstr	2000 年 3 月 31 日
現住所	resident_address_unicode	UTF-8	tstr	○県□□市△町◇丁目○番地▽▽号
性別	sex_unicode	UTF-8	tstr	男又は女
市町村コード	local_gov_code		uint	
マイナンバー	individual_number		uint	123456789012
写真	Portrait		bstr	JPEG2000 形式

Global Namespace に格納するデータ項目

図表 5.　マイナンバーカード mdoc データ項目一覧(案)

Data element	Data element identifier	Character set	encoding	例
20 歳以上	age_over_20		boolean	“20 歳以上”
年齢確認	age_in_years		uint	

※1. 年齢確認 age_in_years は、Global Namespace では、必須にはなっていない。

※2. Global Namespace に格納する年齢の関連情報は、.JP Namespace の生年月日の二次的利用のデータ項目に限定する。。

オ　MSO　(Mobile Security Object) のプロファイル

MSO には、以下の情報を含めることを CP/CPS で規定する。

- Version　MSO のバージョン
- Digest Algorithm　ハッシュアルゴリズム
- value Digest　各データ項目のハッシュ値の配列
- device Key information　Device Key の公開鍵
- docType　mdoc で規定されている docType
- ValidityInfo　MSO の有効期間

MSO のプロファイルは、ISO/IEC18013-5 に準拠した仕様とすることを規定すること。

カ　運用規定

運用の詳細は、運用手順書に詳細を規定する。

CP/CPS では、運用に関するセキュリティポリシー等を規定する。

参考文献として、公開されている JPKI の CP/CPS, GPKI の CP/CPS を参照して詳細を記載すること。

キ　mdoc IACA に求められる運用保守の要件

mdoc IACA の中間 CA である Document Signer は、オンプレ環境ではなくガバクラ上に政府系認証局として初めて構築する。従って、入退出管理等、CP/CPS の要件に示したセキュリティ要件を満足できる部屋で、キーセレモニーや DS 証明書等のセットアップができるように運用することが要件となる。

但し、外部公開する CP/CPS には、中間 CA である Document Signer がガバクラ上で構築されていることは公開しない。すなわち外部公開版の CP/CPS と外部に公開しない事項を削ぎ落とした二種類の CP/CPS を用意することが必要である。

ク　Root 認証局から DS 証明書セットアップまでの運用手順

詳細は運用手順に記載するが、ここでは、 CP/CPS に関連する運用規定の骨子のみ記載する。

（前提条件）

・Root 認証局は、スタンドアロンで Network 接続しないため、DS 電子証明書への Root 認証局への電子署名は、Managed PKI Security Room の中でなければ電子署名できない。

・DS 電子証明書のセットアップは、mdoc IACA 運用保守ルームからしか行なってはい

けない。

・mdoc IACA 運用保守ルームは、接続検証環境のキーセレモニーまでに準備する必要がある。

ケ　Root 認証局から DS 電子証明書セットアップまでの手順

(1) Managed PKI Security Room の中で、キーセレモニーを行い、Root 認証局を立上げ

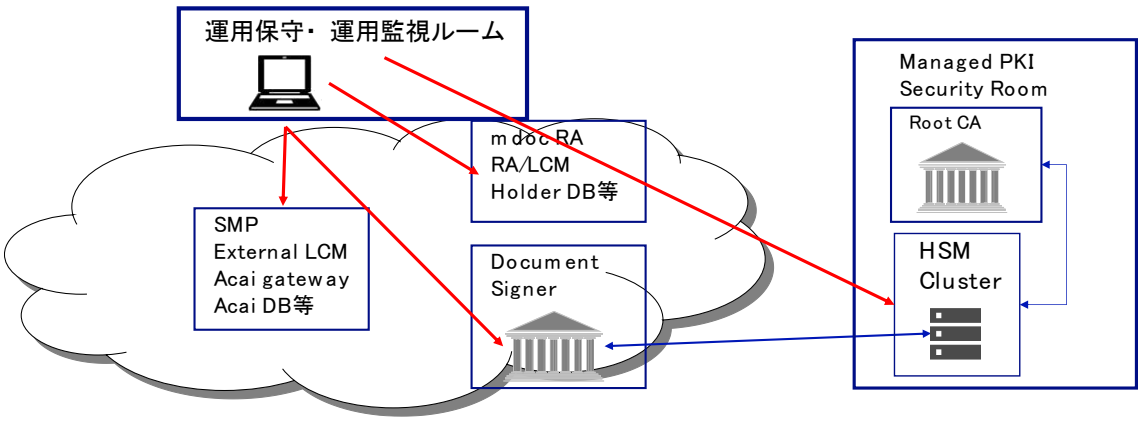
(2) mdoc IACA 運用保守ルームの中で、キーセレモニーを行い、Document Signer 認証局を立上げ

(3) mdoc IACA 運用保守ルームの中で、DS 認証局の CSR を作成
※CSR: Certificate Signing Request

(4) DS 認証局の CSR データを Managed PKI Security に持ち込み、Root 認証局が電子署名した DS 証明書を生成

(5) Root 認証局が電子署名した DS 証明書を mdoc IACA 運用保守ルームに持ち込み、環境のセットアップを行なう。

mdoc IACA の中間 CA である Document Signer は、オンプレ環境ではなくガバクラ上に政府系認証局として初めて構築する。従って、入退出管理等、CP/CPS の要件に示したセキュリティ要件を満足できる部屋で、キーセレモニーや DS 証明書等のセットアップができるように運用することが必須要件となる。そのことを CP/CPS で規定すること。



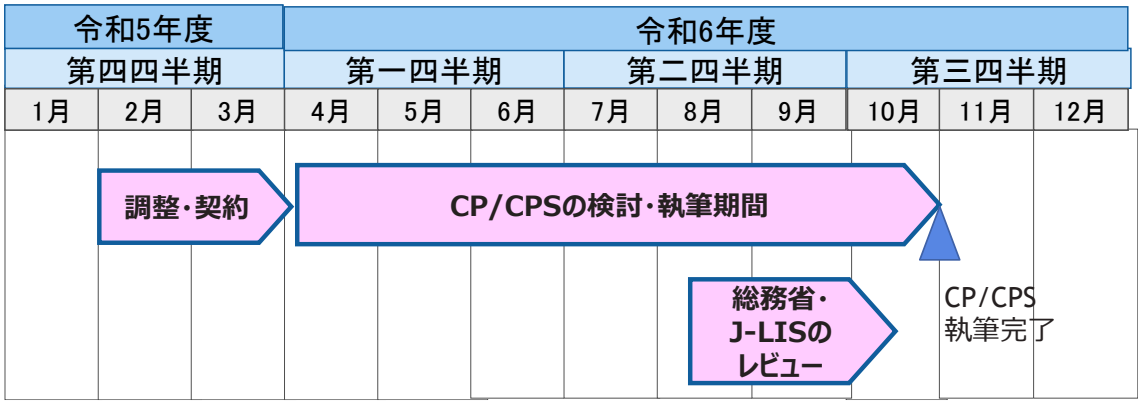
図表 6.　運用保守の要件

（２）**全体スケジュール**

本業務に関連する現時点での全体スケジュール想定を以下に示す。

本スケジュールは、現時点での想定の内容で、今後の検討において変更される可能性がある。

基本的に執筆は、令和６年度の９月末までに完了すること。またレビューは執筆完了分から順次８月～９月末までを総務省、J-LIS を始めとした関係省庁・機関からのレビュー期間とする。レビュー指摘事項を反映する期間及びデジタル庁が最終確認する期間として９月末から 10 月末を想定している。



図表 7.　本業務に関連する全体スケジュール（調整中）

５．作業要件

（１）**実施計画書の作成及び業務管理**

ア　契約締結後速やかに本業務に係る実施計画書を作成し、当庁のレビューを経て、契約締結後１週間以内に当庁の承認を得ること。また、本業務を速やかに開始できるよう、提案書において実施計画書の案を提出すること。

イ　実施計画書には、少なくとも作業体制、スケジュール、成果物、プロジェクト管理方法等を含めること。具体的な記載内容、提出形式等に関しては、当庁と事前に協議し決定すること。

ウ　提出した内容に変更があった場合は、変更の事由が発生したごとに再度提出し、当庁の承認を得ること。

エ　作成した実施計画書に基づき、本業務の進捗、課題等の状況を管理し、当庁に報告すること。報告頻度は隔週から週１回を想定するが、実施計画書の作成時に当庁と協議の上決定すること。

（２）**規定書の作成**

以下のとおり、作業をすること。

ア. 関連ドキュメントの調査結果報告書

（ア）概要

mdoc 認証局・発行局のポリシー及び運用規定を策定するためには、どのような規定を遵守しなければならないかを調査してまとめる。

（イ）作業内容

デジタル庁の指定した以下のドキュメントを調査して、CP/CPS で規定すべきセキュリティ要件の遵守事項をまとめること。

- □ Webtrust for Certificate Authorities
- □ JIPDEC 特定認証業務要件
- □ Network and Certificate System Security Requirement Version1.7
  5, April CA/BROWSER FORUM
- □ Draft ETSI EN 319 411-1 V1.4.0
  Electronic Signatures and Infrastructures Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
- □ RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certificate Practices Framework

イ. mdoc 認証局・発行局のポリシー及び運用規定（CP/CPS）の作成

（ア）目次案の作成

上記関連ドキュメントの調査結果報告書をベースとして、mdoc 認証局・発行局のポリシー及び運用規定の目次案と各目次案に記載する内容の参照先と各目次案の項目毎に記載する内容の概要をまとめる。(WebTrust, 特定認証業務,CABForum の各規定等を参照して、概要を記述する。手戻りを防止するために記載内容の骨子をデジタル庁の担当者と合意後に詳細内容の執筆を始めること。)

（イ） 詳細規定の執筆

上記(ア)でデジタル庁と合意した目次案に基づいて、詳細内容を執筆する。執筆した内容に関しては、適宜、デジタル庁担当社のレビュー確認を受けること。

６．納入成果物の範囲、納品期日等

（１）納入成果物

受注者は、下表に示す納入成果物について納入予定日までに納入すること。納期につ

いては、実施計画書の作成時に当庁と協議の上決定すること。

図表 8.　納入成果物一覧

項番	成果物	内容	納期（想定）
1	実施計画書	本業務の実施計画。 作業概要、作業体制、スケジュール、成果物等を定めた文書。	契約締結後１週間以内
2	レビュー結果報告書	実証事業者が提出する成果物に対して、デジタル庁がレビューした指摘事項に関して反映した結果を記載した文書。	各成果物が提出された後、１週間以内を目処（詳細は都度協議）
3	mdoc 認証局・発行局のポリシー及び運用規定（全体詳細版）	mdoc 認証局・発行局のポリシー及び運用規定の詳細をまとめた文書 各詳細項目毎に参考文献の参照先と内容を記載すること	最終納品物 令和６年 10 月 31 日
4	mdoc 認証局・発行局のポリシー及び運用規定（外部公開用）	ガバクラ上での中間 CA の運用等、公開できない事項を削ぎ落とした外部公開版 必要最小限の事項に留める。	最終納品物 令和６年 10 月 31 日
5	定例会議事録	本業務で受注者が主催した会議の議事録。	各会議完了後 ３営業日以内。 また、議事録全体を令和６年 10 月 31 日までに納品

（２）納品方法

ア　受注者は、全ての納入成果物について、事前に当庁のレビュー及び承認を受けてから、納期までに納品すること。そのため、実施計画書に記載するスケジュールでは、当庁のレビュー及び指摘対応に要する期間を明示すること。

イ　受注者は、全ての納入成果物について、本業務の完了時に最新版を改めて提出すること。

ウ　受注者は、全ての納入成果物について、全て日本語で作成すること。ただし、情報処理に関する用語等、日本国においても英字で表記されることが一般的な文言については、英字のまま記載しても構わない。なお、用字・用語・記述符号の表記については、「公用文作成の考え方（令和４年１月 11 日内閣官房長官通知）」を参考にすること。また、情報処理に関する用語の表記については、日本産業規格（JIS）の規定を参考にすること。

エ　受注者は、全ての納入成果物について、原則として電子データで作成すること。納入形態の詳細（電子媒体のファイル形式等も含む。）については、当庁と協議の上、決定すること。

オ　受注者は、納入成果物のうちプログラム等を除くドキュメント類について、当庁での確認を可能とするため、原則として Microsoft Word、Excel、PowerPoint 形式等の当庁において閲覧・編集可能なファイル形式及び PDF 形式（ただし、PDF 形式は

納入後に加除訂正等のない成果物に限る。）で作成すること。また、当庁が他の形式による提出を求める場合は、協議の上対応方針を決定すること。

カ　受注者は、納入成果物の作成に当たり、ドキュメントに図表や写真を貼り付けている場合は、図表や写真のデータはアウトライン化・画像化せず、取り出せるデータとして埋込む又は別データとして格納すること。

キ　受注者は、成果物が外部に不正に使用されたり、納品過程において改ざんされたりすることのないよう、安全な納品方法を提案し、成果物の情報セキュリティの確保に留意すること。

ク　受注者は、電磁的記録媒体により納品する場合、不正プログラム対策ソフトウェアによる確認を行うなどして、成果物に不正プログラムが混入することのないよう適切に対処すること。

ケ　受注者は、提出した成果物に対して当庁の検査を受けること。検査の結果、納入成果物の全部又は一部が不合格となった場合は、必要な対応を行った後、指定した期日までに改めて納品すること。

（３）納品場所

原則として、成果物は次の場所において引渡しを行うこと。ただし、当庁が納品場所を別途指示する場合はこの限りではない。

〒102-0094

東京都千代田区紀尾井町 1-3　東京ガーデンテラス紀尾井町 19 階

デジタル庁　国民向けサービスグループ　マイナンバーカード担当

（TEL：03-4477-6775、E-Mail：mynumber_smartphone@digital.go.jp）

７．作業の実施体制・方法に関する事項

７．１　作業体制に求める要件

受注者の作業体制に求める要件について、以下に示す。

（１）作業体制の要件

ア　本業務の遂行に必要な専門知識・経験を有する要員が確保され、本調査の遂行について確実に実施される体制が整備されていること。それが確認できる実施体制図等を提出すること。

イ　受注者の作業体制として、本業務を統括する実施責任者（プロジェクトマネージャ）及び作業担当者を配置すること。実施責任者は本業務に関する実質的な責任と権限を有すること。

ウ　受注者において情報セキュリティ対策を確実かつ継続的に実施するための責任

者を定め、個別の対策の実施・点検・改善等を行う体制を整備し、本調達に係る業務の着手に先立ち、その概要を示す資料を提示すること。契約期間中、整備した情報セキュリティを確保するための体制を維持すること。

（２）業務実施者の適格性の確保等

ア　受注者は、契約を履行する業務に従事する個人（以下「業務従事者」という。）として、本件業務を実施するに当たって必要な経験、資格、業績等を有する者を確保すること。

イ　業務従事者は、履行に必要若しくは有用な、又は背景となる経歴、知見、語学（母語及び外国語能力）、文化的背景（国籍等）を有すること。

（３）情報保全の履行体制

ア　受注者は、この契約の履行に際し知り得た保護すべき情報（契約を履行する一環として受注者が収集、整理、作成等した情報であって、当庁が保護を要さないと確認したものを除く。）及びその他の非公知の情報（当庁から提供した情報を含む。以下「保護すべき情報等」という。）について、適切に管理するものとする。

イ　保護すべき情報等の取扱いについては、次の履行体制を確保し、これを変更した場合には、遅滞なく当庁に通知するものとする。

(ア)当庁が保護を要さないと確認するまでは保護すべき情報として取り扱う履行体制

(イ)当庁の同意を得て指定した取扱者以外の者に取扱わせない履行体制

(ウ)当庁が許可した場合を除き、受注者に係る親会社や受注者に対して指導、監督、業務支援、助言、監査等を行う者を含む一切の受注者以外の者に対して伝達又は漏えいさせない履行体制

ウ　契約の履行中、履行後を問わず情報の漏洩等の事故や疑い、将来的な懸念の指摘があったときは、直ちに必要な措置等を講ずるとともに、当庁に報告すること。また、当庁から求められた場合は、情報の管理の履行状況等を報告するとともに、デジタル庁による調査が行われる場合は、これに協力すること。

７．２　作業要員に求める資格等の要件

受注者の作業要員に求める要件について、以下に示す。

ア　実施責任者は、情報システムの企画等の業務におけるプロジェクト管理経験を５年以上有すること。

イ　実施責任者は、プロジェクトマネジメントの知見を有する者として、プロジェクトマネジメント協会（PMI）が認定する「プロジェクトマネジメントプロフェッショナル（PMP)」又は情報処理の推進に関する法律（昭和 45 年法律第 90 号）に

基づく「情報処理技術者試験（プロジェクトマネージャ）」の資格を有すること。

ウ　実施責任者及び主要な作業担当者は、住民基本台帳カード、マイナンバーカード又は公的個人認証サービスに関連する情報システムにおける企画等業務の経験を有すること。

７．３　作業場所

本業務の実施に必要な作業場所、備品、消耗品等については、全て受注者の責任において用意し、事前に当庁の承認を得ること。作業場所に変更が生じた場合も、事前に当庁の承認を得ること。

７．４　作業の管理に関する要領

本業務の作業の管理に当たっては、実施計画書の作成時に、必要となる管理要領を作成すること。当該管理要領に基づき、作業の管理及び当庁への報告を実施すること。

８．作業の実施に当たっての遵守事項

８．１　機密保持、資料の取扱い

ア　受注者は、「政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）」、「デジタル庁情報セキュリティポリシー」等に規定されているセキュリティ要件（本業務の遂行に関係するものに限る。）に準拠すること。また、契約期間内に当該規定の改定があった場合、本システムへの影響について確認するとともに、必要に応じて当庁と協議の上対応方針を決定すること。

イ　受注者は、本業務に関してデジタル庁が開示した情報（公知の情報等を除く。以下同じ。）、契約履行過程で生じた納入成果物に関する情報、その他当該業務の実施において知り得た情報について、本業務の目的以外に使用または第三者に開示若しくは漏洩してはならないものとし、そのために必要な措置を講ずること。当該情報を本業務以外の目的に使用または第三者に開示する必要がある場合、事前に当庁の承認を得ること。

ウ　受注者は、本業務の遂行における情報セキュリティ対策の履行が不十分である可能性を当庁が認める場合には、当庁の求めに応じ協議を行い、合意した対応を取ること。

エ　受注者は、本調達に係る業務の実施のためにデジタル庁から提供する情報及び当該業務の実施において知り得た情報について、以下の事項を遵守すること。ただし、既に公知である情報については、この限りではない。

（ア）本調達に係る業務にのみ使用し、他の目的には使用しないこと。

（イ）本調達に係る業務を行う者以外には機密とすること。

オ　受注者は、本業務で取り扱う情報について、本調達仕様書の別添１「情報保護・管理要領」を遵守し、十分な管理を行うこと。なお、本業務の一部を第三者に再委託する場合についても同様とする。

カ　受注者は、本業務の実施に当たり、受注者が所有する情報システム等において不正なアクセスが行われていないかを確認するため、必要に応じて業務に使用するツールの操作ログや開発中のプログラムへのアクセスログ等を監査証跡として取得すること。また、必要に応じて監査証跡を分析の上、その結果について当庁へ報告すること。不正なアクセス又はそのおそれが確認された場合には、速やかに当庁に報告すること。

キ　受注者は、本調達に係る業務の実施のために取得し、処理する要機密情報を、全て国内法が適用される場所に保存すること。

ク　受注者は、本調達に係る業務の遂行において情報セキュリティが侵害された場合及びそのおそれがある場合に備え、事前に連絡体制を策定するとともに、証跡（ログ、機器など事象の精査に必要なもの）の取得・分析が可能な体制を整備し、当庁に提示すること。また、本調達に係る業務の遂行において情報セキュリティが侵害された場合又はそのおそれがある場合には、速やかに当庁に報告するとともに、必要な対応を実施すること。

ケ　受注者は、当庁から、本調達に係る業務の遂行における情報セキュリティ対策の履行状況に関する以下の事項の報告を求められた場合は、速やかに回答すること。

(ア)本仕様において求める情報セキュリティ対策の実績

(イ)受注者に取り扱わせるデジタル庁の情報の機密保持等に係る管理状況

８．２　サプライチェーン・リスクの低減

ア　受注者は、本調達で納入する機器等がある場合、不正な変更が加えられた機器等を調達することを防止するため、当該機器等の製造企業、製造国及び技術提供企業が確認できる書面を提出すること。また、当庁が要求する項目以外の付加装置やプログラム等が当該機器等に含まれている場合において、機密情報や個人情報を収集する機能を具備し、これらの情報が窃取・漏えいされるおそれがあるときも同様に、当該機器等を製造企業、製造国及び技術提供企業が確認できる書面を提出すること。

イ　受注者は、納入した機器等に不正な変更が発見された場合の対応として、デジタル庁と連携を図りながら製造元への問合せや調査依頼等、不正な変更が加えられた理由や原因等の調査に必要な対応を実施すること。また、当庁が要求する項目以外の付加装置やプログラム等が当該機器等に含まれている場合において、機密情報や個人情報を収集する機能を具備し、これらの情報が窃取・漏えいされ

るおそれがあるときも同様に、デジタル庁と連携を図りながら製造元への問合せや調査依頼等、不正な変更が加えられた理由や原因等の調査に必要な対応を実施すること。

８．３　遵守する法令等

（１）法令等の遵守

受注者は、本業務の実施に当たり、以下の法令等を遵守すること。

ア　民法（明治 29 年法律第 89 号）
イ　刑法（明治 40 年法律第 45 号）
ウ　私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号）
エ　著作権法（昭和 45 年法律第 48 号）
オ　不正アクセス行為の禁止等に関する法律（平成 11 年法律 128 号）
カ　行政機関の保有する個人情報の保護に関する法律（平成 15 年法律第 58 号）
キ　電子署名等に係る地方公共団体情報システム機構の認証業務に関する法律（平成 14 年法律第 153 号）
ク　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）

（２）その他文書への準拠

受注者は、本業務について、以下の文書等に基づき実施すること。契約期間内に当該文書等の改定があった場合、本業務への影響について確認するとともに、必要に応じて当庁と協議の上対応方針を決定すること。

ア　デジタル・ガバメント推進標準ガイドライン（令和 5 年 3 月 31 日デジタル社会推進会議幹事会決定）
イ　政府機関等のサイバーセキュリティ対策のための統一基準群（令和５年度版）（令和 5 年 7 月 4 日サイバーセキュリティ戦略本部決定）
ウ　デジタル庁情報セキュリティポリシー（令和 4 年 10 月 21 日デジタル監決定）
エ　調達等における情報セキュリティ対策手順書（令和 3 年 9 月 1 日改定、統括情報セキュリティ責任者）

９．成果物の取扱いに関する事項

９．１　知的財産権の帰属

ア　本業務における成果物の原著作権及び二次的著作物の著作権（著作権法第 21 条から第 28 条までに定める全ての権利を含む。）は、受注者が本調達の実施の従前から権利を保有していた等の明確な理由によりあらかじめ提案書にて権利譲渡

不可能と示されたもの以外は、全てデジタル庁に帰属するものとする。

イ　デジタル庁は、成果物について、第三者に権利が帰属する場合を除き、自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるとともに、任意に開示できるものとする。

ウ　納品される成果物に第三者が権利を有する著作物（以下「既存著作物等」という。）が含まれる場合には、受注者は、当該既存著作物等の使用に必要な費用の負担及び使用許諾契約等に関わる一切の手続を行うこと。この場合、本業務の受注者は、当該既存著作物の内容について事前にデジタル庁の承認を得ることとし、デジタル庁は、既存著作物等について当該許諾条件の範囲で使用するものとする。なお、本仕様に基づく作業に関し、第三者との間に著作権に係る権利侵害の紛争の原因が専らデジタル庁の責めに帰す場合を除き、受注者の責任及び負担において一切を処理すること。この場合、デジタル庁は係る紛争等の事実を知ったときは、受注者に通知し、必要な範囲で訴訟上の防衛を受注者に委ねる等の協力措置を講じるものとする。

エ　本件の成果物に係る所有権は、デジタル庁から受注者に対価が完済されたとき、受注者からデジタル庁に移転するものとする。

オ　受注者はデジタル庁に対し、一切の著作者人格権を行使しないものとし、また、第三者をして行使させないものとする。また、受注者が本受託業務の実施の過程で生じた納入成果物に係る著作権を自ら使用し又は第三者をして使用させる場合は、デジタル庁と別途協議するものとする。

カ　受注者は使用する画像、デザイン、表現等に関して他者の著作権を侵害する行為に十分配慮し、これを行わないこと。

９．２　契約不適合責任

ア　受注者は、本調達について検収を行った日を起算日として１年間、成果物に対する契約不適合責任を負うものとする。ただし、契約不適合が受注者の故意又は重大な過失に基づく場合は、当該期間の経過後であっても受注者はその責任を負うものとする。

イ　本業務における成果物等について、種類、品質又は数量が契約書、本調達仕様書その他合意された要件の内容に適合しないもの（以下「不適合」という。）である場合、その不適合がデジタル庁の責に帰すべき事由による場合を除き、受注者は、自己の費用で、デジタル庁の選択に従い、その修補、代替物の引渡し又は不足分の引渡しによる履行の追完（以下、手段を問わず総称して「履行の追完」という。）をすること。なお、受注者は如何なる場合であっても、デジタル庁の選択と異なる方法で履行の追完をする場合は、デジタル庁の事前の承諾を受けること。

ウ　受注者は、その具体的な履行の追完の実施方法、完了時期、実施により発生する諸制限事項について、デジタル庁と協議し、承諾を得てから履行の追完を実施するものとし、完了時には、その結果についてデジタル庁の承諾を受けること。

エ　受注者がデジタル庁から相当の期間を定めた履行の追完の催告を受けたにもかかわらず、その期限内に履行の追完を実施しない場合、デジタル庁は、その不適合の程度に応じて代金の減額を請求することができる。ただし、次に掲げる場合、受注者に対して履行の追完の催告なく、直ちに代金の減額を請求することができる。

(ア)履行の追完が不能であるとき。

(イ)受注者が履行の追完を拒絶する意思を明確に表示したとき。

(ウ)本業務の性質又は契約書等の内容により、特定の日時又は一定の期間内に履行をしなければ契約をした目的を達することができない場合において、受注者が履行の追完をしないでその時期を経過したとき。

(エ)前 3 号に掲げる場合のほか、前項の催告をしても履行の追完を受ける見込みがないことが明らかであるとき。

９．３　検収

ア　受注者は、納入成果物等について、納品期日までに当庁に内容の説明を実施して検収を受けること。

イ　検収の結果、成果物等に不備又は誤り等が見つかった場合には、直ちに必要な修正、改修、交換等を行い、変更点について当庁に説明を行った上で、指定された日時までに再度納品すること。

１０．入札参加資格に関する事項

１０．１　入札参加要件

（１）本業務の遂行に必要な専門知識・経験を有する要員が確保され、関係者の協力のもと、本業務の遂行について確実に実施される体制が整備されていること。外部の有識者等の氏名等を含め、体制全体が確認できる実施体制図を提出すること。

（２）本業務の遂行に必要な専門知識・経験を有する要員が確保されているほか、スマートフォン・IC カードリーダの製造事業者や携帯事業者等の関係事業者との関係性が構築されている等、本業務を確実に遂行可能な体制となっていること。

（３）官公庁又はその他組織において、類似の業務等を実施した実績を有すること。

（４）納入期限までに本業務を完了するための合理的な計画を策定していること。

（５）「マイナンバーカードの機能のスマートフォン搭載に関する検討会」における検討状況を踏まえた提案を行っていること。同検討会については、以下のＵＲＬを参照の

こと。
https://www.digital.go.jp/councils/smartphone-mynumbercard/

（６）複数事業者による共同入札を実施する場合は、以下に示す全ての要件を満たすこと。

ア　複数の事業者が共同入札する場合、その中から全体の意思決定、運営管理等に責任を持つ共同入札の代表者を定めるとともに、本代表者が本調達に対する入札を行うこと。

イ　共同入札を構成する事業者間においては、その結成、運営等について協定を締結し、業務の遂行に当たっては、代表者を中心に、各事業者が協力して行うこと。事業者間の調整事項、トラブル等の発生に際しては、その当事者となる当該事業者間で解決すること。また、解散後の契約不適合責任に関しても協定の内容に含めること。

ウ　共同入札を構成する全ての事業者は、本入札への単独提案又は他の共同入札への参加を行っていないこと。

エ　共同入札を構成する全ての事業者は、公的な資格や認証等の取得を除く全ての応札条件を満たすこと。

１０．２　入札制限

本調達は、「デジタル庁における入札制限等に関する規程」に従い、入札の制限を行う。

https://www.digital.go.jp/assets/contents/node/basic_page/field_ref_resources/c5d7192e-22e0-4810-8afd-ce83c50af6a4/20220309_policies_procurement_doc_01_1.pdf

１１．再委託に関する事項

１１．１　再委託の制限及び再委託を認める場合の条件

ア　受注者は、本業務の全部又は主たる部分を再委託してはならない。ただし、本業務の一部に限り、後述する「０１１．２　承認手続」に示す手続に従いデジタル庁の承認を得た場合のみ、再委託を認めるものとする。

イ　受注者は、本業務の実施責任者（プロジェクトマネージャ）を再委託先事業者の社員や契約社員とすることはできない。

ウ　再委託先の業務従事者は原則として再委託先の社員とし、社員以外の者が従事する場合は、当該者の身元を保証するとともに、身元を明らかにする書面をデジタル庁に提出し、デジタル庁の承認を受けるものとする。

エ　受注者は、再委託先の行為について、一切の責任を負うものとする。

オ　受注者は、情報セキュリティ、機密保持、知的財産権、その他遵守事項について、本調達仕様書が定める受注者の責務を再委託先にも負うよう、必要な処置を実施すること。

カ　受注者は、「１０．２　入札制限」に掲げる事業者に再委託を行わないこと。

１１．２　承認手続

ア　本業務の実施の一部を再委託する場合には、あらかじめ再委託の相手方の商号又は名称及び住所並びに再委託を行う業務の範囲、再委託の必要性、契約金額、資本関係・役員等の情報、業務の実施場所、作業要員の所属・専門性（情報セキュリティに係る資格・研修実績等）・実績・国籍等について記載した再委託等承認申請書（所定様式あり）をデジタル庁に提出し、承認を受けること。

イ　再委託の相手方の変更等を行う必要が生じた場合も、前項と同様に再委託等承認申請書をデジタル庁に提出し、承認を受けること。

ウ　再委託の相手方が更に委託を行うなど複数の段階で再委託が行われる場合（以下「再々委託」という。）についても、前項と同様に再委託等承認申請書をデジタル庁に提出し、承認を受けること。

１１．３　再委託先の契約違反等

再委託先において、本調達仕様書に定める事項に関する義務違反又は義務を怠った場合には、受注者が一切の責任を負うとともに、デジタル庁は、当該再委託先への再委託の中止を請求することができる。

１２．その他特記事項

本業務に関連するその他特記事項について、以下に示す。

ア　応札を前提とする者は、提案書提出期限の 10 営業日前（土曜、日曜、祝日を含まない。）までに必ず関連資料を参照し、本業務の範囲の確認と想定業務量を確認した上で提案書を作成すること。関連資料を参照する場合は事前に閲覧の申し入れを行い、閲覧時の遵守事項に係る誓約書を提出すること。関連資料を閲覧した結果、本調達に応札しない場合は、提案書提出期限の 2 営業日前（土曜、日曜、祝日を含まない。）までに、必ず当庁に応札しない旨を連絡すること。

イ　本調達事業者は、標準ガイドラインに基づき、契約金額の内訳を記載した情報資産管理標準シートを契約締結後速やかに提出すること。

ウ　本業務を実施する上で必要と判断する諸経費については、受注者が関係者と調整し、予め見積りに含めること。

エ　本仕様書の内容及び解釈等について不明な個所がある場合、その他特に必要がある場合は、事前に当庁と協議し、決定、解決すること。この場合、当該協議に関する議事録を作成し、当庁の確認を受けること。

オ　本業務受注後に、本調達仕様書の内容の一部について変更を行おうとする場合、その変更の内容、理由等を明記した書面をもってデジタル庁に申し入れを行うこと。

双方の協議において、その変更内容が軽微（委託料、納期に影響を及ぼさない）かつ許容できると判断された場合は、変更の内容、理由等を明記した書面に双方が記名捺印することによって変更を確定する。

カ　本業務に係る費用は、業務完了後、契約書に定めるところにより支払うものとする。

以上

別添１

情報保護・管理要領

（１）目的

本契約に係る作業において取り扱う各種情報について、適正な保護・管理方策について明確にすることを目的とする。

（２）適用範囲

本契約に係る作業で取り扱う当庁が交付又は使用を許可した全ての情報（電子データ、印刷された情報を含む。）を対象とする。

（３）本契約を受託する者が遵守すべき事項

請負者は、本契約の履行に関して、以下の項目を全て遵守すること。

ア．作業開始前の遵守事項

請負者は以下の(1)から(5)までの各項目に定める事項を定め、その結果を取りまとめた「情報管理計画書」を作成し、契約締結後１週間を目途に遅滞なく当庁の承認を受けること。また、役務内容を一部再委託する場合は、(6)に定める事項に必要な情報を当庁に提供し、当庁の承認を受けること。

(1) 情報取扱者等の指定

「適用範囲」に定める情報を取り扱う者（以下、「情報取扱者」という。）を指定すること。また、情報取扱者のうち、情報取扱者を統括する立場にある者一名を情報取扱責任者として指定すること。なお、情報取扱者及び情報取扱責任者（以下、「情報取扱者等」という。）は、守秘義務等の情報の取り扱いに関する社内教育又はこれに準ずる講習等（以下、「社内情報セキュリティ教育」という。）を受講した者とすること。

なお、「情報管理計画書」には、上記に従って指定した情報取扱者等の所属、役職、氏名及び社内情報セキュリティ教育の受講状況を明記すること。

(2) 情報取扱者等への教育・周知の計画策定

情報取扱者等を対象に実施する本契約での各情報の取り扱いや漏えい防止等の教育・周知に関する計画を策定すること。

(3) 情報の取り扱いに関する計画策定

本契約の作業に係る情報の取り扱いに関し、情報の保存、運搬、複製及び破棄において実施する措置を情報セキュリティ確保の観点から定めること。また、情報の

保管場所を変更する場合における取り扱いについても定めること。

上記の情報の取り扱いに関して定める措置には、以下に示す措置を含めること。

- 本契約の作業に係る情報を取り扱うサーバ、PC、モバイル端末について、脅威に関する最新の情報を踏まえた不正プログラム対策及び脆弱性対策を行うこと。
- デジタル庁が「要保護情報」に指定した情報の取り扱いに、デジタル庁又は請負者のいずれかの管理下にない情報システム等（作業従事者の個人所有物であるPC及びモバイル端末を含む）を用いることを原則として禁止し、必要がある場合は当庁の許可を得て用いること。
- デジタル庁が「要保護情報」に指定した情報の保存に、デジタル庁又は請負者のいずれかの管理下にない情報システム等又は電磁的記録媒体（作業従事者が私的に契約しているサービス及び作業従事者の個人所有物である電磁的記録媒体を含む。）を用いることを原則として禁止し、必要がある場合は当庁の許可を得て用いること。
- デジタル庁が「要保護情報」に指定した情報を電子メールにて送信する場合には、暗号化を行うこと。

(4) 作業場所の情報セキュリティ確保のための措置の決定

デジタル庁又はデジタル庁が指定する場所以外の作業場所において本契約に係る作業を行う場合は、情報に係るセキュリティ確保のために、作業場所の環境、作業に使用する情報システム等に講ずる措置を定めること。

上記の情報に係るセキュリティ確保のために定める措置には、以下に示す措置を含めること。

- デジタル庁の情報システムにアクセス（一般向けに提供されているウェブページへのアクセスを除く。）する作業は、請負者の管理下にあり、部外者の立入りが制限された場所において行うこと。
- 本契約の作業に係る情報を取り扱うPC、モバイル端末等について、盗難、紛失、表示画面ののぞき見等による情報漏えいを防ぐための措置を講ずること。また、それらの措置を講じていないPC、モバイル端末等を用いた作業を制限すること。

(5) 情報セキュリティが侵害された又はそのおそれがある場合の対処手順等の策定

本契約に係る業務の遂行において情報セキュリティが侵害された又はそのおそれがある場合に備え、事前に連絡体制を整備し、当庁に提示すること。

本契約に係る業務の遂行において情報セキュリティが侵害された場合又はそのおそれがある場合の対処手順を定めること。対処手順には、以下に示す対処を含め

ること。

- 作業中に、情報セキュリティが侵害された又はそのおそれがあると判断した場合には、直ちに、当庁に、口頭にてその旨第一報を入れること。当庁への第一報は、情報セキュリティインシデントの発生を認知してから速やかに行われるように留意して行うこと。
- 当該第一報が行われた後、発生した日時、場所、発生した事由、関係する請負者の作業者を明らかにし、速やかに当庁に報告すること。また、当該報告の内容を記載した書面を遅延なく当庁に提出すること。
- 当庁の指示に基づき、対応措置を実施すること。
- 当庁が指定する期日までに、発生した事態の具体的内容、原因、実施した対応措置を内容とする報告書を作成の上、当庁に提出すること。
- 再発を防止するための措置内容を策定し、当庁の承認を得た後、速やかにその措置を実施すること。

本契約の業務が国の安全に関する重要な情報の取り扱いを含む場合は、上記に加えて、以下に示す対処を対処手順に含めること。

- 情報セキュリティの侵害による被害の程度を把握するために必要となる記録類を作成又は取得すること。これらの記録類は契約終了時まで保存すること。
- デジタル庁の求めに応じてこれらの記録類をデジタル庁に引き渡すこと。

なお、ここでいう「情報セキュリティが侵害された又はそのおそれがある場合」には、以下の事象を含む。

- 不正プログラムへの感染（受託者におけるものを含む。）
- サービス不能攻撃によるシステムの停止（受託者におけるものを含む。）
- 情報システムへの不正アクセス（受託者におけるものを含む。）
- 書面又は外部電磁的記録媒体の盗難又は紛失（受託者におけるものを含む。）
- 要機密情報の流出・漏えい・改ざん（受託者におけるものを含む。）
- 異常処理等、予期せぬ長時間のシステム停止（受託者におけるものを含む。）
- デジタル庁が受託者に提供した又は受託者にアクセスを認めたデジタル庁の情報の目的外利用又は漏えい
- アクセスを許可していないデジタル庁の情報への受託者によるアクセス
- 意図しない不正な変更等が発見された場合

(6) 再委託に係る情報セキュリティの確保

事前に当庁の承認を得たうえで、本契約の役務内容を一部再委託する場合、請負者自体が業務を実施する場合に求められる水準と同一水準の情報セキュリティ対

策を再委託先においても確保させる必要があり、再委託先における情報セキュリティの十分な確保を請負者が担保するとともに、再委託先の情報セキュリティ対策の実施状況を確認するために必要な情報を当庁に提供し、当庁の承認を受けること。

イ．請負作業中の遵守事項

(1)「情報管理計画書」に基づく情報セキュリティ確保

「情報管理計画書」に記載した、情報取扱者等への教育・周知、情報の取り扱い及び作業場所等の情報セキュリティ確保のための措置を実施すること。

(2)「情報管理簿」の作成

当庁から貸与を受けた各種ドキュメント、電子データ類について、授受方法、保管場所、保管方法、作業場所、使用目的等を含む取扱方法を明確にするため、「情報管理簿」を作成すること。

(3)「情報管理計画書」の変更に関する報告

本契約に基づく請負作業中に、作業開始前に提出した「情報管理計画書」の内容と異なる措置を実施する場合は、以下の手続を行うこと。

（ア） 情報取扱者等の異動を行う場合は、事前にその旨を当庁に報告し承認を得ること。また、承認された異動の内容を記録し保存すること。

（イ） 「情報管理計画書」に記載した情報取扱者等に対する教育・周知の計画を変更する場合は、当該個所を変更した「情報管理計画書」を当庁に提出し承認を得ること。

（ウ） 「情報管理計画書」に記載した情報の取り扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置を変更する場合は、当該箇所を変更した「情報管理計画書」を当庁に提出し、承認を得ること。

（エ） 一時的に「情報管理計画書」に記載した情報の取り扱いに関する計画又は作業場所等の情報セキュリティ確保のための措置とは異なる措置を実施する場合は、原則として事前にその旨を当庁に報告し承認を得ること。

(4) 作業場所への監査の受入れ

デジタル庁以外の作業場所において本契約に係る作業を行っている場合に、当庁がその施設及び設備に関し、請負者が「情報管理計画書」に記載した作業場所等の情報セキュリティ確保のため措置が実施されていることを監査する旨申し出た

ときは、これを受け入れること。

(5) 情報セキュリティ対策の履行が不十分であった場合の対応

本契約に係る作業における情報セキュリティ対策の履行が不十分であると当庁が判断した場合、当庁と協議の上、必要な是正措置を講ずること。また、是正措置の内容を「情報管理計画書」に反映させること。

ウ. 請負作業完了時の遵守事項

(1) 情報返却等処理

本契約に係る作業完了時に上記イ(2)で作成した「情報管理簿」に記載されている全ての情報について、返却、消去、廃棄等の処理を行うこと。

なお、その処理について方法、日時、場所、立会人、作業責任者等の事項を網羅した「情報返却等計画書」を事前に当庁に提出し、承認を得ること。

処理の終了後、その結果を記載した「情報管理簿」を当庁に提出すること。

(2) 情報セキュリティ侵害の被害に関する記録類の引渡し

本契約の業務が国の安全に関する重要な情報の取り扱いを含む場合であって、業務遂行中に情報セキュリティが侵害された又はそのおそれがある事象が発生した場合、ア(5)に基づいて取得し保存している記録類を引き渡すこと。

以上