資料１－２

# 政府認証基盤の運用・保守業務
# 民間競争入札実施要項（案）

総務省行政管理局
行政情報システム企画課情報システム管理室

# － 目　次 －

## 1　趣旨

競争の導入による公共サービスの改革に関する法律（平成 18 年法律第 51 号。以下「法」という。）に基づく競争の導入による公共サービスの改革については、公共サービスによる利益を享受する国民の立場に立って、公共サービスの全般について不断の見直しを行い、その実施について、透明かつ公正な競争の下で民間事業者の創意と工夫を適切に反映させることにより、国民のために、より良質かつ低廉な公共サービスを実現することを目指すものである。

上記を踏まえ、総務省は、公共サービス改革基本方針（平成 28 年 6 月 28 日閣議決定）別表で民間競争入札の対象として選定された「政府認証基盤の運用・保守の請負」について、公共サービス改革基本方針に従って、本実施要項を定めるものである。

## ２　政府認証基盤の運用・保守業務の詳細な内容及びその実施に当たり確保されるべき対象公共サービスの質に関する事項

### (1) 政府認証基盤の運用・保守業務の概要

#### ア　政府認証基盤の経緯

政府認証基盤は「ミレニアム・プロジェクト（新しい千年紀プロジェクト）について」(1999年(平成 11 年)12 月 19 日内閣総理大臣決定）に基づき、国民等と行政との間でインターネット等を利用してやり取りされる申請・届出等手続に係る電子文書について、その文書が真にその名義人によって作成され、内容に改ざんがないことを相互に確認できるように整備されたものであり、①処分権者に係る電子署名を行うために用いる電子証明書（以下「官職証明書」という。）等を発行する府省認証局、②府省認証局と国民等に係る電子証明書等を発行する民間認証局等との間の相互認証を行うブリッジ認証局で構成され、平成 13 年４月にその運用を開始した。

その後、「電子政府構築計画」(2003 年(平成 15 年) 7 月 17 日各府省情報化統括責任者（CIO）連絡会議決定。2004 年(平成 16 年) 6 月 14 日一部改定。）において、府省共通業務・システムとして、システムの共通化・一元化等を内容とする最適化計画を策定し、システムの見直しを進めることとされ、平成 17 年３月 31 日に「霞が関 WAN 及び政府認証基盤（共通システム）の最適化計画」1（以下「最適化計画」という。）が各府省情報化統括責任者(CIO)連絡会議において決定された。

この最適化計画に基づき、平成 20 年１月に官職証明書等を一元的に発行する政府共用認証局の運用を開始し、府省等が個別に整備・運用してきた府省認証局（14 認証局）及び最高裁判所認証局を順次廃止して政府共用認証局に集約することにより、最適化効果として年間約 9.6 億円の運用経費の削減を達成した。

また、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針」（平成 20 年４月 22 日 情報セキュリティ政策会議決定2。以下、「移行指針」という。）に基づき、より安全な暗号アルゴリズムへの移行を平成 26 年９月に、より安全な暗号アルゴリズムへの移行を行うとともに、相互認証先認証局との相互認証更新を行った。

一方、アプリケーション認証局に係る認証業務は平成 30 年４月をもって終了し、平成 30 年５月以降、サーバ証明書等について民間認証局から取得する手続を政府認証基盤が取りまとめる業務（サーバ証明書等の発行支援業務）に切り替えた。

現在は、令和４年２月に運用開始する新システムに係るシステムの更新作業を行っているところである。

---

1 https://www.kantei.go.jp/jp/singi/it2/cio/dai13/13siryou1.pdf

2 https://www.nisc.go.jp/active/general/pdf/crypto_p1.pdf

### イ　政府認証基盤の概要

#### (ｱ) 政府認証基盤の構成

政府認証基盤は、図２－１のとおり、ブリッジ認証局と政府共用認証局で構成され、このうち、政府共用認証局は、官職証明書等を発行する官職認証局から構成される。

これらの認証局の運営業務、発行する証明書の用途、運用要員の役割等は、下記の CP/CPS (証明書ポリシ/認証実施規程)に記載し公表している。

・ブリッジ認証局 CP/CPS[3]

（政府共用認証局）

・官職認証局 CP/CPS[4]

また、民間認証局等がブリッジ認証局と相互認証を行うために必要な技術要件については、「政府認証基盤相互運用性仕様書[5]」を定め、公表している。

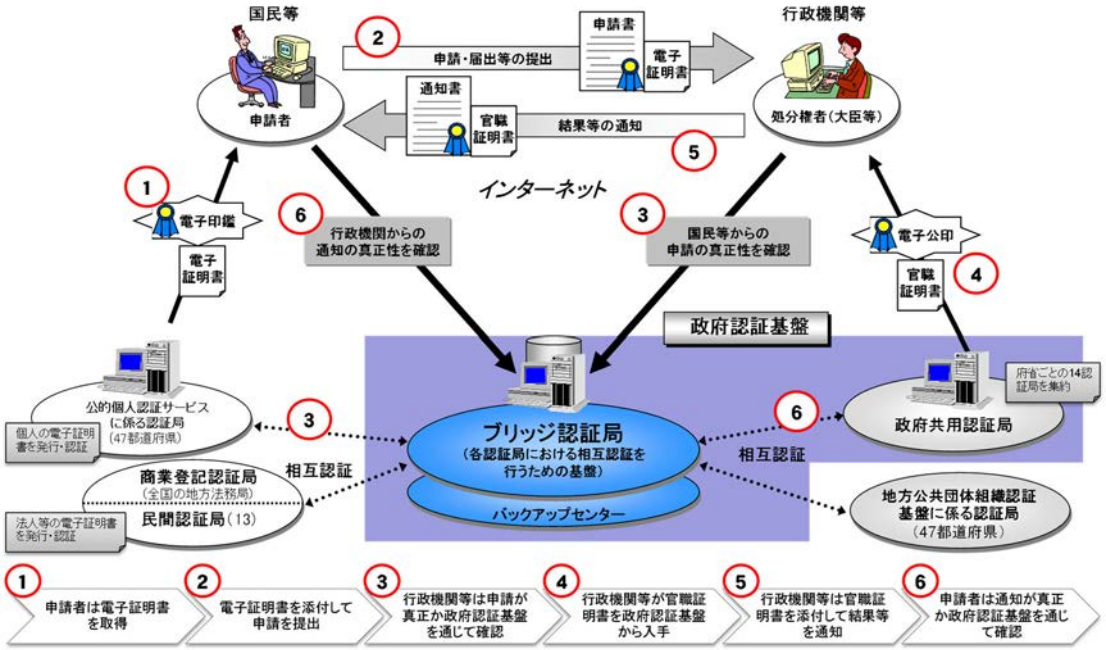



図　２-1　政府認証基盤の概要

[3] https://www.gpki.go.jp/bca/cpcps/cpcps.pdf
[4] https://www.gpki.go.jp/osca/cpcps/cpcps.pdf
[5] https://www.gpki.go.jp/session/CompatibilitySpecifications.pdf

### (ｲ) 政府認証基盤の利用者

政府認証基盤の利用者は、官職証明書等の利用者と検証者に大別される。官職証明書等の利用者は府省等の職員であるが、官職証明書等を検証するのは電子申請等を利用する国民等である。

また、国民等が電子申請等で利用する民間認証局等の電子証明書の検証については、府省等の職員が政府認証基盤を利用して行っている。

これらの利用状況は、下記のとおりである。

・現在、有効な官職証明書等　　：約２万枚
・国民等が官職証明書等を検証する件数　：月間約 115 万件
・府省等が電子証明書を検証する件数　　：月間約 1,330 万件
・相互認証(接続)している認証局 ：13 認証局（令和２年６月現在）

### (ｳ) 利用者に提供するサービス

政府認証基盤が利用者に提供するサービスの業務概要及び実施手順は下表のとおりである。

なお、請負業務内容については、後述「ウ 政府認証基盤の運用・保守業務の内容」に示す。

| サービス | 業務概要及び実施手順 |
|---|---|
| 相互認証 | ・ ブリッジ認証局との相互認証を要望する民間認証局等から申請を受理する。<br>・ 相互認証基準を基に書類審査及び技術審査を行う。<br>・ ブリッジ認証局の意思決定機関である行政情報システム関係課長連絡会議の了承を得る。<br>・ 相互認証証明書を相互に発行することで相互認証を実施する。 |
| 認証情報公開サービスの提供 | ・ 統合認証情報公開システムに対し、ブリッジ認証局、政府共用認証局及び商業登記認証局の失効情報等の認証情報を定期的に登録する。<br>・ 上記以外でブリッジ認証局と相互認証している民間認証局等については、相互認証実施時に失効情報等の認証情報の格納箇所（リフェラル）を登録する。<br>・ 府省等が運用する電子申請等システムからのオンラインでの認証情報提供要求に対し、情報を提供する。 |
| 証明書検証サービスの提供 | ・ 府省等が運用する電子申請等システムからオンラインで証明書の有効性検証要求を受け付ける。<br>・ 受け付けた要求に対し、認証情報公開サービスの情報等を利用し、証明書の有効性を検証する。<br>・ 検証結果を電子申請等システムへオンラインで返答する。 |

| サービス | 業務概要及び実施手順 |
|---|---|
| 証明書の発行指示 | ・ 電子申請等システムの利用者で電子証明書（官職証明書、利用者証明書、暗号化通信用等証明書）を必要とする各府省の職員は、各府省の府省等登録局（LRA）に対し、証明書の発行依頼を行う。<br>・ LRA は政府共用認証局から提供された LRA システムを利用し、政府共通ネットワーク経由で政府共用認証局に対し証明書の発行指示を行う。 |
| 証明書の発行 | ・ 証明書の発行要求を LRA システムから受け付ける。<br>・ 受け付けた情報を基に証明書を発行する。<br>・ 発行した証明書が証明書ファイル形式の場合は、LRA システムに送付し、LRA システムからダウンロード可能とする。<br>・ 発行した証明書が IC カード形式の場合は、IC カードに証明書を格納するとともに、券面に必要事項を印刷する。 |
| 証明書の発行支援 | ・ 電子申請等システムの利用者で電子証明書（サーバ証明書、コード署名証明書、ドキュメント署名証明書）を必要とする各府省の職員は、各府省の府省等登録局（LRA）に対し、証明書の発行依頼を行う。<br>・ LRA は証明書の発行申請書と発行要求データ（CSR）の内容を確認し、政府認証基盤へ送付する。<br>・ 政府認証基盤は受け付けた情報を基に発行事業者（民間）へ証明書発行を指示する。 |
| 利用者クライアントソフト | ・ 政府共用認証局は、発行した IC カードを電子申請等システムの担当者が利用できるようにする利用者クライアントソフトを提供する。<br>・ 各府省の電子申請等システムの担当者は利用者クライアントソフトを PC に導入し、IC カードを利用して電子署名等を行う。 |

ウ　**政府認証基盤の運用・保守業務の内容**

本業務を実施する民間事業者（以下「請負者」という。）が行う業務は、図２－２の調達対象範囲のシステムの運用・保守に係る下記業務を行うことにより、利用者に２(1)イ(ｳ)に示す業務を　安定的に供給する。（詳細は、別添１「政府認証基盤の運用・保守の請負調達仕様書　２（５）作業内容・納入成果物」を参照）

発行する証明書は最大２万枚/年、相互認証の実施は最大 12 件/年であり、システムの維持・監視は、24 時間週 7 日である。運用・保守業務に必要な役割と要員数は、下表のとおりであり、適宜柔軟に業務量に応じた対応ができる体制を整備する。

| 役　割 | 要員数 | 備　　考 |
|---|---|---|
| 運用責任者 | １名 | 「行政機関の休日に関する法律(昭和63年法律第91号)」に規定 |

| 役　割 | 要員数 | 備　　考 |
|---|---|---|
| 運用責任者補佐 | ２名以上 | する行政機関の休日を除く日に作業を行うことを原則とする。<br>常時、運用要員が作業する場所はマスタセンタとする。<br>○午前8時30分～午後5時30分まで(休憩時間は別途協議)<br>運用責任者補佐1名、上級IA操作員1名以上<br>○午前9時30分～午後6時30分まで(休憩時間は別途協議)<br>監視員を除く上記以外の運用要員 |
| ログ検査者 | ２名以上 | |
| 上級IA操作員 | ６名以上 | |
| 一般IA操作員 | ３名以上 | |
| 監視員 | ８名以上 | ２名、２交替又は３交替にて24時間（休憩時間は別途協議） |
| 保守要員 | 特に定めない | 24時間週７日のシステムの維持に必要な要員を登録すること。<br>（注）上記運用要員と保守要員との兼務は行わないこと。 |

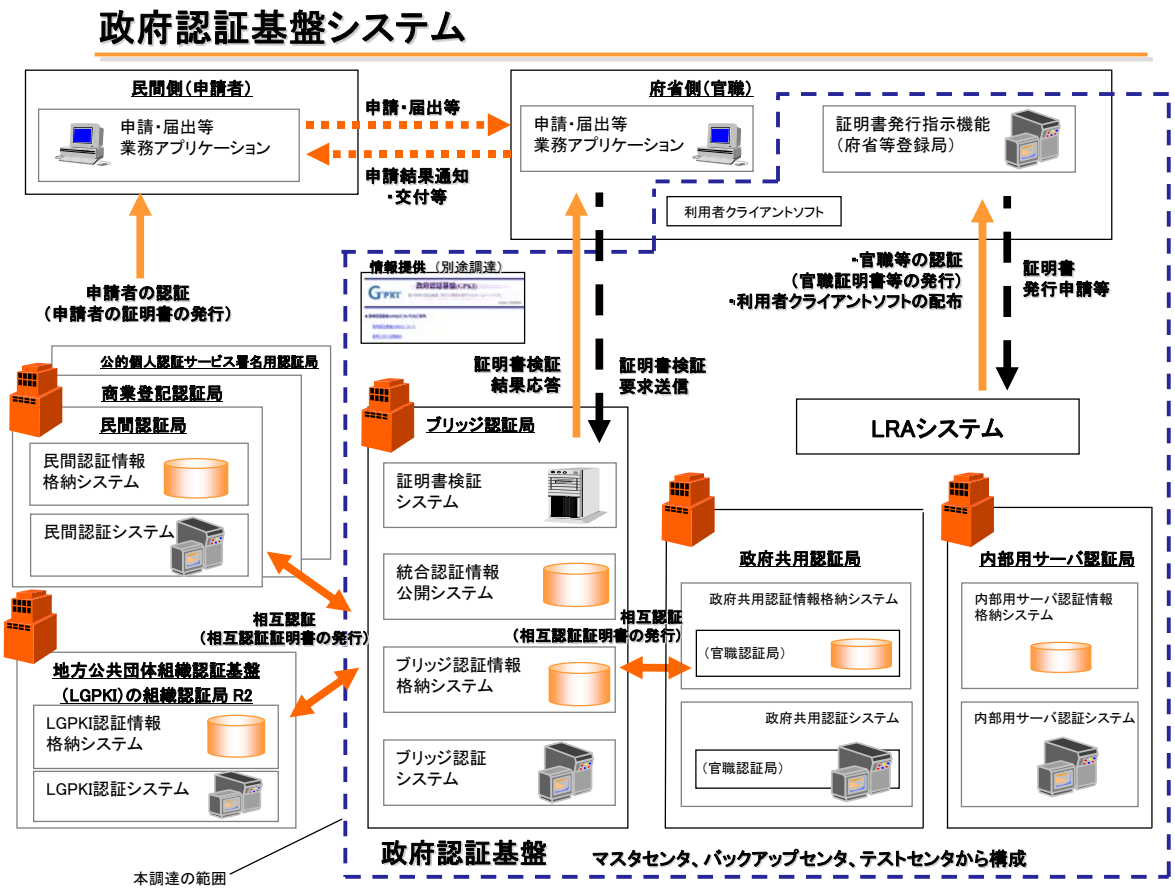



図　2－2　政府認証基盤システムの概要

## (ア) 政府認証基盤の運用・保守計画書の策定

## (イ) 政府認証基盤の認証業務及び運用業務

A ブリッジ認証局に係る認証業務

(a) 自己署名証明書の発行（鍵更新）

(b) 相互認証審査等支援（書類審査）

(c) 相互認証審査等支援（技術審査）

(d) 相互認証証明書の取り交わし

(e) 相互認証証明書の解消（失効）

(f) システム運用関連証明書の発行（リポジトリ複製用証明書、CVS 証明書等）

(g) 監査結果報告書の確認（相互認証先認証局）

(h) テスト環境用証明書の発行（相互認証証明書、模擬民間 CA の EE 証明書）

B 政府共用認証局に係る認証業務

(a) LRA の登録業務（券面情報、ドメイン情報等の更新や休日設定含む。）

(b) 官職認証局に係る認証業務

・自己署名証明書の発行（鍵更新）

・各種証明書発行（IC カード発行業務）

・相互認証業務（取り交わし）

・システム運用関連証明書の発行（リポジトリ複製用証明書、CVS 証明書等）

・テスト環境用証明書の発行（模擬官職 CA の EE 証明書）

(c) 失効情報の確認

C 内部用サーバ認証局に係る認証業務

(a) 自己署名証明書の発行（キーセレモニー）

(b) 内部用サーバ証明書の発行

(c) テスト環境用証明書の発行（模擬 ISCA の EE 証明書）

(d) 失効情報の確認

(e) 内部監査

D 照会対応

(a) LRA

(b) 相互認証先認証局

(c) 電子申請等アプリケーション

(d) 運営組織側の管理業務支援

E ホームページ作成及び更新

F 外部監査対応

(a) CP/CPS 準拠性監査の対応

G 監査ログ検査

(a) 監査ログ検査（マスタセンタ）

(b) 監査ログ検査（バックアップセンタ）

H アーカイブ取得

I アーカイブ可読性確認

J 規程類に関する準拠性監査

K LRA 研修

L 教育・訓練

(a) 危機管理訓練（事業継続計画）

(b) 運用要員教育

M テスト環境の維持

N 書類改定（上位規程、業務規程、業務管理マニュアル）

O サーバ証明書等の発行支援

(a) サーバ証明書の発行支援

(b) コード署名証明書の発行支援

(c) ドキュメント署名証明書の発行支援

(ｳ) 政府認証基盤システムの運用業務

A 運用・保守管理業務

(a) セキュリティ管理

・セキュリティ実施手順書

・ウィルスパターンファイルの適用

・ファイアウォールアクセス制御管理

・セキュリティ情報の収集

・脆弱性診断

(b) インシデント管理

・障害記録書起票

・障害管理（フォローアップ）

(c) 変更管理

・アカウント情報の管理（アカウントレビュー含む。）

・ファイアウォールのアクセス制御定期確認

・ハードウェアの棚卸し確認

・ソフトウェアの棚卸し確認

・書類・媒体の廃棄

(d) リリース管理

・作業計画書、報告書の確認

B 監視業務

(a) 機器の稼働状況監視

(b) 不正アクセス監視

(c) 定常処理の結果確認

C 定常業務

(a) バックアップデータ管理
(b) フルバックアップの取得
(c) リソース使用状況の情報取得及び集計
(d) パスワード変更管理
(e) アクセス件数等統計処理の収集及び集計（CVS、公開リポジトリ）
(f) CA 秘密鍵可読性確認
(g) CVS 秘密鍵可読性確認

D 非定常業務
(a) システムの障害対応
(a) 障害対応時のマシン室立会い
(b) 書類改定（システム運用マニュアル、操作マニュアル）
(c) 機器等更改に伴うデータ移行

㈡政府認証基盤システムの保守業務
A システム保守管理
B システム障害保守
C システム予防保守
D 利用者環境の維持

㈢ 認証局施設・設備の管理業務
A 施設・室に関する管理
B 設備、備品等に関する管理

㈣ 報告書の作成
A 月次報告書の作成
B 月次報告書の報告

㈤ その他
・ 運用要員及び保守要員は、夜間・休日を問わず緊急時の連絡及び召集に対応するため、携帯電話等（請負者が手配し通話料・通信料を負担）を常備して常に連絡が取れること。
・ 行政管理局行政情報システム企画課情報システム管理室政府認証基盤担当（以下「主管係」という。）が要員への連絡に必要な携帯電話等３台以上を請負者の負担で用意すること。
・ 運用及び保守に必要な消耗品等は請負者が準備すること。
・ 主管係及び利用機関等への連絡等に必要な通信運搬費は請負者が負担すること。

**エ　運用施設・設備要件**

施設・設備の要件は、認証業務に係る機器等の稼働に直接影響を与えない監視室及び事務室を

除き、耐震性について震度６強以上の地震に耐えられる免震構造の建物とし、少なくとも現行のテストセンタを含むマスタセンタ（東京都内）を新たな施設・設備に移設すること。

**(ｱ) 現行の施設・設備**

現行の施設については、テストセンタを含むマスタセンタ及びバックアップセンタ（東京近郊）の２カ所があり、施設使用料、通信回線（インターネットとマスタセンタ間、インターネットとバックアップセンタ間の通信費及びプロバイダ契約料。請負者が保有している設備、物品及び政府共通ネットワークの接続料は除く。）使用料（現行月額 17,380,000 円（消費税を含む。））は、請負者の負担である。

※施設・設備の詳細については、別途、閲覧に供する「現行の施設・設備の詳細」資料を参照。

**(ｲ) 新たな施設・設備**

以下の条件を満たす新たな施設・設備を提案することとし、施設使用料、通信回線使用料等は現行月額を上限とすること。また、機器等の移設・据付・調整･システム設定・テスト等への対応は、請負者の責任と負担において行うこと。

（条件）

・新たな施設・設備は、別添資料３「政府認証基盤　施設・設備の詳細仕様」を満たしていること。

・移設に伴う本システムのサービス停止時間（新旧システムの切替えに伴うもの）については、システム更改の請負者と連携して 24 時間内とし、回数は４回を限度とすること。

**(ｳ) 請負者の責任分界**

請負者は施設･設備を提供するとともに、「政府認証基盤の運用･保守の請負」調達仕様書（案）で規定された作業内容の業務を実施すること。

なお、請負者に関連するステークホルダ（総務省及び各府省は除く）とその責任分界は以下のとおりである。

| 項番 | 関連ステークホルダ | 調達件名 | 責任分界（費用負担含む） |
|---|---|---|---|
| 1 | システム更改の請負者 | 「政府認証基盤のシステム更改のための設計・開発・構築等の請負」 | システム移行を含めたシステム設計、開発及び構築 |
| 2 | 機器業者（機器等の借入業者） | 「政府認証基盤のシステム更改のための機器等の借入」 | 機器等の設定・調整・単体テスト、据付・設置、及び機器等の保守を含めた機器等の提供 |
| 3 | 現行システムの運用･保守の請負者 | 平成 28 年度調達の「政府認証基盤の運用･保守の請負」 | 項番１「システム更改の請負者」が行うシステム移行時のマシン室立合い、及び現行システムの運用・保守 |

### ⑵ 確保されるべき対象業務の質

本業務は、政府認証基盤利用者への継続的かつ安定的なサービスの円滑な提供に資するものである必要がある。このような観点から、２(1)ウに示した業務内容を実施するに当たり、請負者が確保すべき対象業務の質は、次のとおりとする。

#### ア　業務の内容

「２(1)ウ政府認証基盤の運用・保守業務の内容」に示す業務を適切に実施する。

#### イ　政府認証基盤のサービスレベル

政府認証基盤が府省等の職員、国民等に提供するサービスとしては、

①認証情報公開サービス（リポジトリの提供サービス）

②証明書検証サービス（政府共用証明書検証サーバの提供サービス）

③証明書の発行サービス（LRA システムの提供サービス）

があり、これらのサービスの稼働率、障害件数（サービス停止を伴うもの）、障害復旧時間、応答時間については、次のとおりとする。

（詳細は別添１「政府認証基盤の運用・保守の請負調達仕様書５(1)信頼性要件」を参照）

##### ㋐ サービスの稼働率

サービスの稼働率(%)は、

①認証情報公開サービス、②証明書検証サービス　　99.99%以上

③証明書の発行サービス　　99.9%以上

とし、この稼働率は以下の算式で計算する。

（計算式）稼働率(%) ＝ ｛（稼働時間 － サービス停止時間）÷ 稼働時間 ｝× 100

##### ㋑ 障害件数（サービス停止を伴うもの）

サービス停止を伴う障害件数は、いずれのサービスも年１回以内とする。

##### ㋒ 障害復旧時間

サービス停止を確認してから復旧するまでの障害復旧時間は、

①認証情報公開サービス、②証明書検証サービス　　１時間以内

③証明書の発行サービス　　８時間以内　とする。

##### ㋓ 応答時間（平均値）

府省等が運用する電子申請等システムからオンラインでの認証情報提供要求及び証明書の有効性検証要求に対する応答時間（平均値）は、1.0 秒以内とし、これらの応答時間は以下の算式で計算する。

（計算式）応答時間 平均値(s) ＝ 応答時間の合計値 ÷ 要求件数

### ⑶ 創意工夫の発揮可能性

本業務を実施するに当たっては、以下の観点から請負者の創意工夫を反映し、公共サービスの質の向上（包括的な質の向上、効率化の向上、経費の削減等）に努めるものとする。

(ｱ) 政府認証基盤の運用・保守業務全般に対する提案

請負者は、別添３「政府認証基盤の運用・保守の請負　総合評価基準書（案)」に従い、政府認証基盤の運用・保守業務の実施全般に係るセキュリティ又は品質の向上の観点から取り組むべき事項等の提案を行うこととする。

(ｲ) 事業内容に対する改善提案

請負者は、事業内容に対し、改善すべき提案（コスト削減に係る提案を含む）がある場合は、別添３「政府認証基盤の運用・保守の請負　総合評価基準書（案)」に従い、具体的な方法等を示すとともに、従来の実施状況と同等以上の質が確保できる根拠等を提案すること。

### (4) 請負費用の支払方法

契約の形態は、業務請負契約とする。

当省は、業務請負契約に基づき請負者が実施する本業務に関し、監督・検査を実施するなどして仕様書に定める内容について適正に実施されていることを確認した上で、適法な支払請求書を受理した日から起算して 30 日以内に毎月支払うものとする。確認の結果、確保されるべき対象業務の質が達成されていないと認められる場合、当省は、確保されるべき対象業務の質の達成に必要な限りで、請負者に対して本業務の実施方法の改善を行うよう指示することができる。

請負者は、当該指示を受けた場合、業務の実施方法を改善し、業務改善報告書を当省に提出するものとする。業務改善報告書の内容が、確保されるべき対象業務の質が達成可能なものであると認められるまで、当省は、請負費の支払を行わないことができる。

なお、請負費は、令和３年９月末までの新たな施設の確保（必要な耐震化工事を含む。）、同年 10 月から令和４年１月末までの運用準備（機器等の据付・調整・システム設定・テスト、マニュアル整備等を含む。）、及び、令和４年２月１日以降の運用・保守サービス提供に対して支払われるものであり、請負者が行う引継ぎや一般的に行われる業務準備行為に対して、請負者に発生した費用は、請負者の負担とする。

### (5) 法令変更による増加費用及び損害の負担

法令の変更により事業者に生じた合理的な増加費用及び損害は、(ｱ)から(ｳ)に該当する場合には当省が負担し、それ以外の法令変更については請負者が負担する。

(ｱ) 本業務に類型的又は特別に影響を及ぼす法令変更及び税制度の新設

(ｲ) 消費税その他類似の税制度の新設・変更（税率の変更含む）

(ｳ) 上記(ｱ)及び(ｲ)のほか、法人税その他類似の税制度の新設・変更以外の税制度の新設・変更（税率の変更含む）

### (6) 管理・運営業務の確実な実施を担保する観点から、ペナルティ的な減額措置を定める場合

本件契約については、サービスレベルアグリーメント（SLA）を導入する。請負者は、別途指定するサービスレベル要件を満たすサービスの提供が可能となる運用・保守体制をとる。本件調達範囲の業務に起因して SLA が達成されなかった場合、月額役務経費に相当する金額の５％を減額して支払うものとする。ただし、請負者の責めに帰すべき理由により正常稼働率が基準を下回った場合に限る。なお、サービス提供時間及び正常稼働時間の実績値は、仕様書に基づき請負者が作成し、主管係に提出した各種報告書の記載内容を踏まえて、当省が判断するものとする。

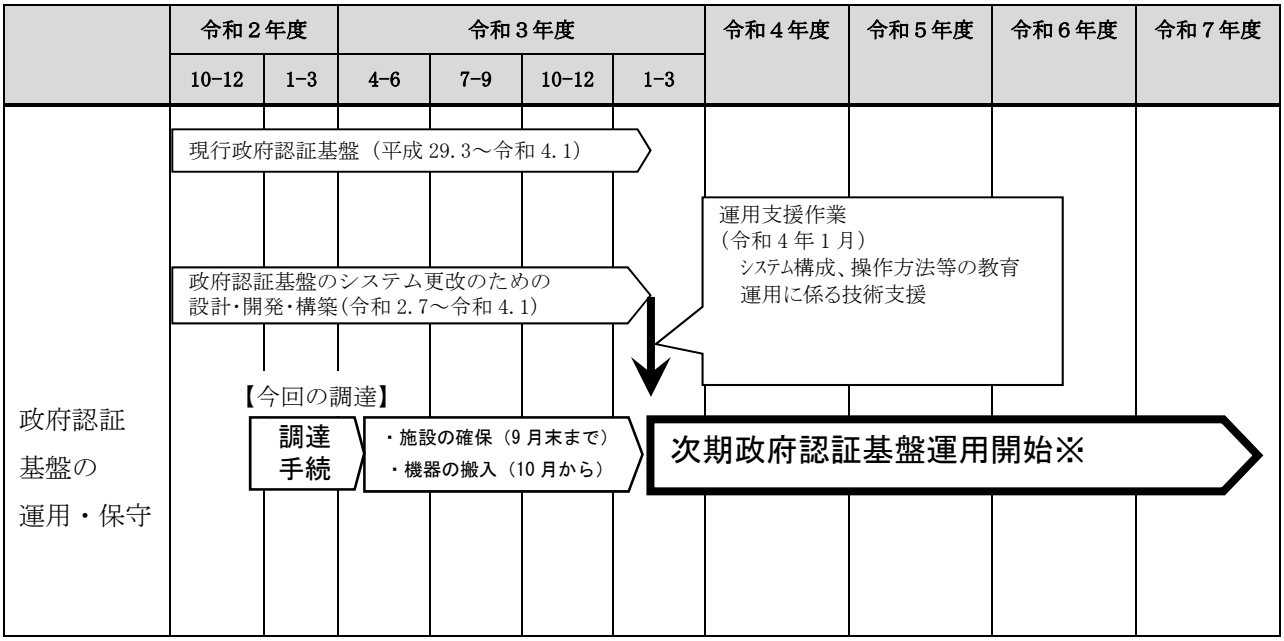
## ３　実施期間に関する事項等

請負契約の契約期間は、令和３年４月から令和８年１月までとする。

なお、現在実施している「政府認証基盤のシステム更改のための設計・開発・構築等の請負」を請け負っている（一社）行政情報システム研究所、日本電気（株）、（株）日立製作所、セコムトラストシステムズ（株）の４社（共同提案）は、運用支援作業として、本請負者に対し、令和４年１月に政府認証基盤のシステム構成、システム操作方法等の教育と、運用に係る技術支援を行う。

また、政府認証基盤の運用の業務引継については、令和３年４月以降、現行の運用・保守の請負者が随時行うものとする。

表　3-1 政府認証基盤の運用・保守スケジュール




※運用・保守期間は令和４年２月～令和８年１月まで。

## 4　入札参加資格に関する事項

### (1) 入札参加資格

ア　法第 15 条において準用する法第 10 条各号（第 11 号を除く。）に該当する者でないこと。

イ　予算　決算及び会計令（昭和 22 年勅令第 165 号）第 70 条の規定に該当しない者であること。なお、未成年者、被保佐人又は被補助人であって、契約締結のために必要な同意を得ている者は、同条中、特別な理由がある場合に該当する。

ウ　予算決算及び会計令第 71 条の規定に該当しない者であること。

エ　令和元・２・３年度総務省競争参加資格（全省庁統一資格）「役務の提供等」Ａ、Ｂ又はＣ等級に格付けされ、関東・甲信越地域の競争参加資格を有する者であること（「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）。

オ　法人税並びに消費税及び地方消費税の滞納がないこと。

カ　労働保険、厚生年金保険等の適用を受けている場合、保険料等の滞納がないこと。

キ　当省又は他府省等における物品等の契約に係る指名停止措置要領に基づく指名停止を受けている期間中でないこと。

ク　調査研究や各工程の調達仕様書の作成に直接関与した事業者及びその関連事業者（財務諸表等の用語、様式及び作成方法に関する規則（昭和 38 年大蔵省令第 59 号）第８条に規定する親会社及び子会社、同一の親会社をもつ会社並びに委託先事業者等の緊密な利害関係を有する事業者をいう。）でないこと。

ケ　調達計画書及び調達仕様書の妥当性確認並びに入札事業者の審査に関する業務を行うCIO補佐官及びその支援スタッフ等の属する又は過去２年間に属していた事業者でないこと。または、CIO補佐官等がその職を辞職した後に所属する事業者の所属部門（辞職後の期間が２年に満たない場合に限る。）でないこと。

コ　単独で対象業務を行えない場合は、適正な業務を遂行できる共同事業体（対象業務を共同して行うことを目的として複数の民間事業者により構成される組織をいう。以下同じ。）として参加することができる。その場合、入札書類提出時までに共同事業体を構成し、代表者を決め、他の者は構成員として参加するものとする。また、共同事業体の構成員は、他の共同体の構成員となり、又は、単独で参加することはできない。なお、共同事業体の代表者及び構成員は、共同事業体の結成に関する協定書（又はこれに類する書類）を作成し、提出すること。

サ　本業務を実施する部門は、ISO27001 又は同等の認証を取得していること。

### (2) 競争参加資格申請書の入手方法等

競争参加資格を有しない者で、本入札に参加を希望する者は、所定の資格審査申請書を入手し、速やかに資格審査申請を行わなければならない。

【申請書の提出先】総務省大臣官房会計課契約第１係 電話 03-5253-5132

## ５　入札に参加する者の募集に関する事項

### (1) 入札手続（スケジュール）

| | |
|---|---|
| 入札公示：官報公示 | 2021 年(令和３年) １月下旬 |
| 入札説明会 | ２月中旬 |
| 質問受付期限 | ２月中旬 |
| 入札書（提案書）提出期限 | ３月上旬 |
| 提案書の審査 | ４月上旬 |
| 開札及び落札者の決定 | ４月下旬 |
| 契約締結 | ４月下旬 |

なお、従来の当該業務の調達仕様書、提出書類、各設計書等については、民間競争入札に参加する予定の者から要望があった場合、所定の手続を経て、閲覧可能である。

### (2) 入札書類

入札参加者は、次に掲げる書類を別に定める入札説明書に記載された期日までに、記載された方法により提出すること。

ア　提案書

別添３の別紙「総合評価対応表」に示した各要求項目について具体的な提案（創意工夫を含む。）を行い、各要求項目を満たすことができることを証明する書類

イ　下見積書

人件費の単価証明書及び物件費の価格証明書を含んだ下見積書

ただし、契約後に発生する経費のみとする。

ウ　入札書

入札金額（契約期間内の全ての請負業務に対する報酬の総額の 110 分の 100 に相当する金額）を記載した書類

エ　委任状

代理人に委任したことを証明する書類

ただし、代理人による入札を行う場合に限る。

オ　競争参加資格審査結果通知書の写し

令和元・２・３年度総務省競争参加資格（全省庁統一資格）「役務の提供等」Ａ、Ｂ又はＣ等級に格付けされ、関東・甲信越地域の競争参加資格を有する者であること（「役務の提供等」の営業品目「ソフトウェア開発」、「情報処理」又は「その他」に登録している者であること。）を証明する審査結果通知書の写し

ただし、電子入札システムにより入札を行う場合は不要。

カ　理由書

電子入札システムにより入札を行うことができない旨の理由を示した書類

ただし、電子入札システムによる入札を行う場合は不要。

キ　法第 15 条において準用する法第 10 条に規定する欠格事由のうち、暴力団排除に関する規程について評価するために必要な書類

ク　法人税並びに消費税及び地方消費税の納税証明書（直近のもの）

社会保険料納入確認書等（直近のもの）

ケ　主たる事業概要、従業員数、事業所の所在地、代表者略歴、主要株主構成、他の者との間で競争の導入による公共サービス改革に関する法律施行令（平成 18 年政令第 228 号）第３条に規定する特定支配関係にある場合は、その者に関する当該情報

コ　共同事業体による参加の場合は、共同事業体内部の役割分担について定めた協定書又はこれに類する書類

## ６　政府認証基盤の運用・保守請負業務を実施する者を決定するための評価の基準その他の政府認証基盤の運用・保守請負業務を実施する者の決定に関する事項

以下に請負者の決定に関する事項を示す。なお、詳細は別添２「政府認証基盤の運用・保守の請負提案書作成要領」及び別添３「政府認証基盤の運用・保守の請負総合評価基準書」を参照とする。

(1) 評価方法

本業務を実施する者の決定は、総合評価落札方式によるものとする。なお、技術の評価に当たっては、入札プロセスの中立性、公正性等を確保するため、当省の CIO 補佐官に意見を聴くものとする。

また、総合評価は、価格点（入札価格の得点）に技術点（提案書による加点）を加えて得た数値（以下「総合評価点」という。）をもって行う。

総合評価点＝価格点（3,200 点満点）＋技術点（3,200 点満点）

(2) 決定方法

提出された提案書に記述された内容が、仕様書に定める要求要件のうち、必須とされた項目について全て満たしている場合は「合格」とし、一つでも満たすことができない項目がある場合は「不合格」とする。

(3) 総合評価点

ア　価格点

価格点は、入札価格を予定価格で除して得た値を１から減じて得た値に入札価格に対する得点配分を乗じて得た値とする。

価格点＝（１－入札価格÷予定価格）×3,200 点

イ　技術点

技術点の評価方法は以下のとおりとする。

(ｱ) 上記（2）における合否の判定により「合格」となった提案書に対して、別添３の別紙「総合評価対応表」に示す各加点項目について評価観点に基づき評価を行い「加点」を与える。（3,200 点満点）

(ｲ) 「加点」については別添３の別紙「総合評価対応表」で示す各加点項目をその重要度に応じ２種類の評価タイプ（最重要、重要）に区分し、提案内容の優劣について下表に基づき相対評価を行い、加点を与える。ただし、評価結果が全く同等で優劣を付けがたい場合には、同評価とすることがある。

| 相対的評価 | 最重要 | 重要 |
|---|---|---|
| (A) 相対的にかなり優れている | 400 点 | 200 点 |
| (B) 相対的に優れている | 300 点 | 150 点 |
| (C) 相対的に平均である | 200 点 | 100 点 |
| (D) 相対的に劣っている | 150 点 | 75 点 |

| | | |
|---|---|---|
| (E)相対的にかなり劣っている | 100 点 | 50 点 |

(ｳ)「加点」の合計点を「技術点」とする。

(4) 落札者の決定

ア　落札者の決定方法

(ｱ) 入札者の入札価格が予算決算及び会計令第 79 条の規定に基づいて作成された予定価格の制限の範囲内であり、かつ、「６(1)評価方法」によって得られた数値の最も高い者を落札者とする。ただし、予算決算及び会計令第 84 条の規定に該当する場合は、予算決算及び会計令第 85 条の基準（予定価格に 10 分の６を乗じて得た額）を適用するので、基準に該当する入札が行われた場合は入札の結果を保留する。この場合、入札参加者は当省の行う事情聴取等の調査に協力しなければならない。

(ｲ) 調査の結果、会計法（昭和 22 年法律第 35 号）第 29 条の６第１項ただし書の規定に該当すると認められるときは、その定めるところにより、予定価格の制限の範囲内で次順位の者を落札者とすることがある。

（会計法第 29 条の６第１項ただし書抜粋）
相手方となるべき者の申込みに係る価格によっては、その者により当該契約の内容に適合した履行がされないおそれがあると認められるとき、又はその者と契約を締結することが公正な取引の秩序を乱すこととなるおそれがあって著しく不適当であると認められるとき

(ｳ) 落札者となるべき者が２人以上あるときは、直ちに当該入札者にくじを引かせ、落札者を決定する。また、入札者又は代理人がくじを引くことができないときは、入札執行事務に関係のない職員がこれに代わってくじを引き、落札者を決定する。

(ｴ) 契約担当官等は、落札者を決定したときに入札者にその氏名（法人の場合はその名称）及び金額を口頭で通知する。ただし、上記(ｲ)により落札者を決定する場合には別に書面で通知する。また、落札できなかった入札者は、落札の相対的な利点に関する情報（当該入札者と落札者のそれぞれの入札価格及び性能等の得点）の提供を要請することができる。

イ　落札決定の取消し

次の各号のいずれかに該当するときは、落札者の決定を取り消す。ただし、契約担当官等が、正当な理由があると認めたときはこの限りでない。

(ｱ) 落札者が、契約担当官等から求められたにもかかわらず契約書の取り交わしを行わない場合

(ｲ) 入札書の内訳金額と合計金額が符合しない場合

落札後、入札者に内訳書を記載させる場合があるので、内訳金額が合計金額と符合しないときは、合計金額で入札したものとみなす。この場合で、入札者は内訳金額の補正を求められたときは、直ちに合計金額に基づいてこれを補正しなければならない。

ウ　落札者が決定しなかった場合の措置

初回の入札において入札参加者がなかった場合、必須項目を全て満たす入札参加者がなかった場合又は再度の入札を行っても落札者が決定しなかった場合、原則として、入札条件等を見直した後、再度公告を行う。

なお、再度の入札によっても落札者となるべき者が決定しない場合又は本業務の実施に必要な期間が確保できないなどやむを得ない場合は、自ら実施する等とし、その理由を官民競争入札等監理委員会に報告するとともに、公表するものとする。

## 7　政府認証基盤の運用・保守請負業務に関する従来の実施状況に関する情報の開示に関する事項

対象業務に関して、以下の情報は別紙１「従来の実施状況に関する情報の開示」のとおり開示する。

ア　従来の実施に要した経費

イ　従来の実施に要した人員

ウ　従来の実施に要した施設及び設備

エ　従来の実施における目標の達成の程度

オ　従来の実施方法等

## 8　政府認証基盤の運用・保守業務請負者に使用させることができる国有財産に関する事項

特になし。

## ９　公共サービス実施請負者が、対象公共サービスを実施するに当たり、総務省に対して報告すべき事項、秘密を適正に取り扱うために必要な措置その他の対象公共サービスの適正かつ確実な実施の確保のために契約により公共サービス実施請負者が講ずるべき措置に関する事項

### (1) 請負者が当省に報告すべき事項、当省の指示により講ずるべき措置

ア　報告等

(ｱ) 請負者は、仕様書に規定する業務を実施したときは、当該仕様書に基づく各種報告書を当省に提出しなければならない。

(ｲ) 請負者は、請負業務の完了に影響を及ぼす重要な事項の変更が生じたときは、直ちに当省に報告するものとし、当省と請負者が協議するものとする。

(ｳ) 請負者は、契約期間中において、(ｲ)以外であっても、必要に応じて当省から報告を求められた場合は、適宜、報告を行うものとする。

イ　調査

(ｱ) 当省は、請負業務の適正かつ確実な実施を確保するために必要があると認めるときは、法第26条第１項の規定に基づき、請負者に対し必要な報告を求め、又は当省の職員が事務所に立ち入り、当該業務の実施の状況若しくは記録、帳簿書類その他の物件を検査し、又は関係者に質問することができる。

(ｲ) 立入検査をする当省の職員は、検査等を行う際には、当該検査が法第 26 条第１項の規定に基づくものであることを請負者に明示するとともに、その身分を示す証明書を携帯し、関係者に提示するものとする。

ウ　指示

当省は、請負業務の適正かつ確実な実施を確保するために必要と認めるときは、請負者に対し、必要な措置を採るべきことを指示することができる。

### (2) 秘密を適正に取り扱うための措置

ア　請負者は、本業務の実施に際して知り得た当省の情報を、第三者に漏らし、盗用し、又は請負業務以外の目的のために利用してはならない。これらの第三者が秘密を漏らし、又は盗用した場合は、法第54条の規定により罰則の適用がある。

イ　請負者は、本業務の実施に際して得られた情報処理に関する利用技術（アイデア又はノウハウ）については、請負者からの文書による申出を当省が認めた場合に限り、第三者へ開示できるものとする。

ウ　請負者は、当省から提供された個人情報及び業務上知り得た個人情報について、個人情報の保護に関する法律（平成15年法律第57号）の規定に基づき、適切な管理を行わなくてはならない。また、当該個人情報については、本業務以外の目的のために利用してはならない。

エ　請負者は、当省の情報セキュリティに関する規程等に基づき、個人情報等を取り扱う場合、①情報の複製等の制限、②情報の漏えい等の事案の発生時における対応、③請負業務終了時の情報の消去・廃棄（復元不可能とすること。）及び返却、④内部管理体制の確立、⑤情報セキュリティの運用状況の検査に応じる義務、⑥請負者の事業責任者及び請負業務に従事する者全てに対して

の守秘義務及び情報セキュリティ要求事項を遵守しなければならない。

オ　アからエまでのほか、当省は、請負者に対し、本業務の適正かつ確実な実施に必要な限りで、秘密を適正に取り扱うために必要な措置を採るべきことを指示することができる。

### (3) 契約に基づき請負者が講ずるべき措置

ア　請負業務の開始

請負者は、本業務の開始日から確実に業務を開始する。

イ　権利の譲渡

請負者は、債務の履行を第三者に引き受けさせ、又は契約から生じる一切の権利若しくは義務を第三者に譲渡し、承継せしめ、若しくは担保に供してはならない。ただし、書面による当省の事前の承認を得たときは、この限りではない。

ウ　契約不適合責任

(ｱ) 当省は、請負者に対し、引き渡された成果物が種類又は品質に関して契約の内容に適合しないものである場合（その不適合が当省の指示によ って生じた場合を除き、請負者が当該指示が不適当であることを知りながら、又は過失により知らずに告げなかった場合を含む。）において、その不適合を当省が知った時から起算して１年以内にその旨の通知を行ったときは、その成果物に対する修補等による履行の追完を請求することができる。ただし、請負者は、当省に不相当な負担を課するものでないときは、当省が請求した方法と異なる方法による履行の追完をすることができる。

(ｲ) (ｱ)の場合において、当省が相当の期間を定めて履行の追完の催告をし、その期間内に履行の追完がないときは、当省は、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。

(ｳ) (ｱ)又は(ｲ)の場合において、当省は、損害賠償を請求することができる。

(ｴ) ただし、上記(ｱ)ないし(ｳ)の具体的な取決め内容については、必要に応じて契約締結時の協議事項とする。

エ　再委託

(ｱ) 請負者は、本業務の実施に当たり、その全部を一括して再委託してはならない。

(ｲ) 請負者は、本業務の実施に当たり、その一部について再委託を行う場合には、原則として、あらかじめ機能証明書において、再委託先に委託する業務の範囲、再委託を行うことの合理性及び必要性、再委託先の履行能力並びに報告徴収、個人情報の管理その他運営管理の方法（以下「再委託先等」という。）について記載しなければならない。

(ｳ) 請負者は、契約締結後やむを得ない事情により再委託を行う場合には、再委託先等を明らかにした上で、当省の承認を受けなければならない。

(ｴ) 請負者は、(ｲ)又は(ｳ)により再委託を行う場合には、請負者が当省に対して負う義務を適切に履行するため、再委託先の事業者に対し前項「(2)秘密を適正に取り扱うために必要な措置」及び本項「(3)契約に基づき請負者が講ずるべき措置」に規定する事項等について、必要な措置を講じさせるとともに、再委託先から必要な報告を聴取することとする。

(ｵ) (ｲ)から(ｴ)までに基づき、請負者が再委託先の事業者に義務を履行させる場合は、全て請負者の責任において行うものとし、再委託先の事業者の責に帰すべき事由については、請負者の

責に帰すべき事由とみなして、請負者が責任を負うものとする。

オ　契約内容の変更

当省及び請負者は、本業務の質の確保の推進、またはその他やむをえない事由により本契約の内容を変更しようとする場合は、あらかじめ変更の理由を提出し、それぞれの相手方の承認を受けるとともに法第 21 条の規定に基づく手続を適切に行わなければならない。

カ　機器更新等の際における民間事業者への措置

当省は、次のいずれかに該当するときは、請負者にその旨を通知するとともに、請負者と協議の上、契約を変更することができる。

(ｱ) ハードウェアの更新、撤去又は新設、サポート期限が切れるソフトウェアの更新等に伴い運用管理対象機器の一部に変更が生じるとき

(ｲ) セキュリティ対策の強化等により業務内容に変更が生じるとき

(ｳ) 当省の組織変更や人員増減に伴うシステム利用者数の変動等により業務量に変動が生じるとき

キ　契約の解除

当省は、請負者が次のいずれかに該当するときは、請負者に対し請負費の支払を停止し、又は契約を解除若しくは変更することができる。この場合、請負者は当省に対して、請負費の総価の 100 分の 10 に相当する金額を違約金として支払わなければならない。その場合の算定方法については、当省の定めるところによる。ただし、同額を超過する増加費用及び損害が発生したときは、超過分の請求を妨げるものではない。

また、請負者は、当省との協議に基づき、本業務の処理が完了するまでの間、責任を持って当該処理を行わなければならない。

(ｱ) 法第 22 条第１項イからチまで又は同項第２号の規定に該当するとき。

(ｲ) 暴力団員を、業務を統括する者又は従業員としていることが明らかになった場合。

(ｳ) 暴力団員と社会的に非難されるべき関係を有していることが明らかになった場合。

(ｴ) 再委託先が、暴力団若しくは暴力団員により実質的に経営を支配される事業を行う者又はこれに準ずる者に該当する旨の通知を、警察当局から受けたとき。

(ｵ) 再委託先が暴力団又は暴力団関係者と知りながらそれを容認して再委託契約を継続させているとき。

ク　談合等不正行為

請負者は、談合等の不正行為に関して、当省が定める「談合等の不正行為に関する特約条項」に従うものとする。

ケ　損害賠償

請負者は、請負者の故意又は過失により当省に損害を与えたときは、当省に対し、その損害について賠償する責任を負う。

コ　不可抗力免責、危険負担

当省及び請負者の責に帰すことのできない事由により契約期間中に物件が滅失し、又は毀損し、その結果、当省が物件を使用することができなくなったときは、請負者は、当該事由が生じた日の翌日以後の契約期間に係る代金の支払を請求することができない。

サ　金品等の授受の禁止

請負者は、本業務の実施において、金品等を受け取ること、又は、与えることをしてはならない。

シ　宣伝行為の禁止

請負者及び本業務に従事する者は、本業務の実施に当たっては、自ら行う業務の宣伝を行ってはならない。また、本業務の実施をもって、第三者に対し誤解を与えるような行為をしてはならない。

ス　記録及び帳簿類の保管

請負者は、本業務に関して作成した記録及び帳簿類を、本業務を終了し、又は中止した日の属する年度の翌年度から起算して５年間、保管しなければならない。

セ　請負業務の引継ぎ

(ｱ) 現行請負者からの引継ぎ

請負者は、本業務を適正かつ円滑にできるよう現行請負者から本業務の開始日までに運用管理手順書等を使用して必要な事務引継ぎを受けなければならない。

また、当省は、当該事務引継ぎが円滑に実施されるよう、現行請負者及び請負者に対して必要な協力を行うものとする。

なお、その際の事務引継ぎに必要となる経費は、現行請負者の負担となる。

(ｲ) 請負期間満了の際、業者変更が生じた場合の引継ぎ

本業務の期間満了の際、業者変更が生じた場合は、請負者は、次回の請負者に対し、当該業務の開始日までに運用管理手順書等を使用し必要な事務引継ぎを行わなければならない。

なお、その際の事務引継ぎに必要となる請負者に発生した経費は、請負者の負担となる。

ソ　契約の解釈

契約に定めのない事項及び契約に関して生じた疑義は、当省と請負者との間で協議して解決する。

## 10　公共サービス実施請負者が対象公共サービスを実施するに当たり、第三者に損害を加えた場合において、その損害の賠償に関し契約により当該公共サービス実施請負者が負うべき責任に関する事項

本業務を実施するに当たり、請負者又はその他本業務に従事する者が、故意又は過失により、本業務の受益者等の第三者に損害を加えた場合は、次のとおりとする。

(1) 当省が国家賠償法（昭和 22 年法律第 125 号）第１条第１項等の規定に基づき当該第三者に対する賠償を行ったときは、当省は請負者に対し、当該第三者に支払った損害賠償額（当該損害の発生について当省の責めに帰すべき理由が存する場合は、当省が自ら賠償の責めに任ずべき金額を超える部分に限る。）について求償することができる。

(2) 請負者が民法（明治 29 年法律第 89 号）第 709 条等の規定に基づき当該第三者に対する賠償を行った場合であって、当該損害の発生について当省の責めに帰すべき理由が存する場合は、請負者は当省に対し、当該第三者に支払った損害賠償額のうち自ら賠償の責めに任ずべき金額を超える部分を求償することができる。

## 11　政府認証基盤の運用・保守に係る法第７条第８項に規定する評価に関する事項

(1) 本業務の実施状況に関する調査の時期

当省は、本業務の実施状況について、総務大臣が行う評価の時期（令和６年１月を予定）を踏まえ、本業務に係る運用が開始される令和４年２月以降、各年度末時点における状況を調査する。

(2) 調査項目及び実施方法

ア　業務の内容

業務報告書及び各種提出書類により調査

イ　政府認証基盤のサービス稼働率

業務報告書等により調査

ウ　障害件数

業務報告書等により調査

エ　障害復旧時間

業務報告書等により調査

オ　応答時間

業務報告書等により調査

(3) 意見聴取等

当省は、必要に応じ、民間事業者から意見の聴取を行うことができるものとする。

また、当省は、令和６年１月を目途として、本業務の実施状況等を総務大臣及び官民競争入札等監理委員会へ提出する。

なお、調査報告を総務大臣及び官民競争入札等監理委員会に提出するに当たり、CIO 補佐官及び外部有識者の意見を聴くものとする。

## 12　その他業務の実施に関し必要な事項

(1) 本業務の運用管理業務の実施状況等の監理委員会への報告

当省は、法第 26 条及び第 27 条に基づく報告徴収、立入検査、指示等を行った場合には、その都度、措置の内容及び理由並びに結果の概要を監理委員会へ報告することとする。

(2) 総務省の監督体制

本契約に係る監督は、主管係自ら立会い、指示その他の適切な方法によって行うものとする。

本業務の実施状況に係る監督は以下のとおり。

監督職員：総務省行政管理局行政情報システム企画課情報システム管理室認証基盤企画係長

検査職員：総務省行政管理局行政情報システム企画課情報システム管理室課長補佐

(3) 請負者の責務

ア　本業務に従事する請負者は、刑法（明治 40 年法律第 45 号）その他の罰則の適用については、法令により公務に従事する職員とみなされる。

イ　請負者は、法第 54 条の規定に該当する場合は、1 年以下の懲役又は 50 万円以下の罰金に処される。

ウ　請負者は、法第 55 条の規定に該当する場合は、30 万円以下の罰金に処されることとなる。なお、法第 56 条の規定により、法人の代表者又は法人若しくは人の代理人、使用人その他の従業者が、その法人又は人の業務に関し、法第 55 条の規定に違反したときは、行為者を罰するほか、その法人又は人に対して同条の刑を科する。

エ　請負者は、会計検査院法（昭和 22 年法律第 73 条）第 23 条第 1 項第 7 号に規定する者に該当することから、会計検査院が必要と認めるときには、同法第 25 条及び第 26 条の規定により、同院の実地の検査を受けたり、同院から直接又は当省を通じて、資料又は報告等の提出を求められたり、質問を受けたりすることがある。

(4) 著作権

ア　請負者は、本業務の目的として作成される成果物に関し、著作権法（昭和 45 年法律 48 号）第 27 条及び第 28 条を含む著作権の全てを当省に無償で譲渡するものとする。

イ　請負者は、成果物に関する著作者人格権（著作権法第 18 条から第 20 条までに規定された権利をいう。）を行使しないものとする。ただし、当省が承認した場合は、この限りではない。

ウ　ア及びイにかかわらず、成果物に請負者が既に著作権を保有しているもの（以下「請負者著作物」という。）が組み込まれている場合は、当該請負者著作物の著作権についてのみ、請負者に帰属する。

エ　提出される成果物に第三者が権利を有する著作物が含まれる場合には、請負者が当該著作物の使用に必要な費用の負担及び使用許諾契約等に係る一切の手続を行うものとする。

# 政府認証基盤の運用・保守業務

## 資料目次

別紙１

# 従来の実施状況に関する情報の開示

１　従来の実施に要した経費　（単位：千円）

| | | 平成 29 年度 | 平成 30 年度 | 令和元年度 |
|---|---|---|---|---|
| 政府認証基盤の運用・保守の請負業務 | | | | |
| 請負費 | 役務等（運用・保守） | 574,058 | 522,211 | 522,393 |
| | センター運用 | 382,042 | 382,042 | 382,042 |
| | システム保守等 | 189,574 | 118,294 | 116,710 |
| | 消耗品等 | 1,690 | 1,690 | 1,690 |
| | 通信費 | 422 | 422 | 422 |
| | 郵送料等 | 330 | 330 | 330 |
| | 証明書取得費 | 0 | 19,433 | 21,199 |
| | 施設使用料等 | 208,560 | 208,560 | 208,560 |
| | マスタセンター | 129,360 | 129,360 | 129,360 |
| | バックアップセンター | 79,200 | 79,200 | 79,200 |
| | 調整費 | ▲14,532 | ▲2,021 | ▲2,203 |
| | 小計 | 768.086 | 728,750 | 728,750 |
| | 消費税 | 61,447 | 58,300 | 65,587 |
| 計 | | 829,533 | 787,050 | 794,337 |

（注記事項）

※　施設使用料等は、マスタセンタ及びバックアップセンタの施設使用料と通信回線使用料が含まれる。

※　平成 29 年度において、利用者環境を構成する JRE のメジャーバージョンアップに伴い、JRE に依存しない利用者クライアントソフトへの変更、及び利用者クライアントソフトの動作検証の環境の構築、動作検証を行ったため一時的に役務等請負費（システム保守等）が増大したが、それ以降は同じ水準を維持している。

2　従来の実施に要した人員

| | 平成 29 年度 | 平成 30 年度 | 令和元年度 |
|---|---|---|---|
| (受託者における運用業務従事者) | | | |
| 運用責任者 | １名（１名） | １名（１名） | １名（１名） |
| 運用責任者補佐 | ３名（２名以上） | ３名（２名以上） | ３名（２名以上） |
| ログ検査者 | ２名（２名以上） | ２名（２名以上） | ２名（２名以上） |
| 上級 IA 操作員 | ６名（６名以上） | ６名（６名以上） | ６名（６名以上） |
| 一般 IA 操作員 | ３名（３名以上） | ３名（３名以上） | ３名（３名以上） |
| 監視員 | ８名（８名以上） | ８名（８名以上） | ８名（８名以上） |
| 保守要員（登録人数） | １３ | １３ | １３ |

(注)・上表括弧内の人数は、調達仕様書において求める人数。

○運用業務従事者に求められる知識・経験等
・運用責任者、運用責任者補佐、ログ検査者（常駐：責任者１名、責任者補佐２名以上、ログ検査者２名以上）
　行政機関の認証局又は電子署名法に基づく特定認証業務の認定を受けた認証局（以下、「特定認証局」という。）における運用責任者相当の運用を行った者を含めること。
　⇒令和元年度については、運用責任者相当（４名）が適合している。
・上級 IA 操作員、一般 IA 操作員（常駐：上級６名以上、一般３名以上）
　行政機関の認証局又は特定認証局の操作員としての運用を行った者を含めること。
　⇒令和元年度については、上級 IA 操作員（６名）及び一般 IA 操作員（３名）が適合している。
・監視員（８名、交替制により 24 時間週７日、常時２名が監視を行う。）
　行政機関の認証局又は特定認証局の監視員としての運用を行った者を含めること。
　⇒令和元年度については、監視員（８名）が適合している。
・スキル
　ITIL V3(Information Technology Infrastructure Library Version3)について広範な知識を有していること。
　ITIL Foundation 認定資格者又は経済産業大臣認定の情報処理技術者試験の IT サービスマネージャ試験、システム監査技術者試験、プロジェクトマネージャ試験の合格者であることが望ましい。
　⇒令和元年度については、５名が適合している。

○運用業務従事者の作業時間等
・作業実施日
　「行政機関の休日に関する法律（昭和 63 年法律第 91 号)」に規定する行政機関の休日を除く日。
　ただし、主管係から業務上の指示（システム保守等）があるときは、これに従うこと。
　なお、監視業務については、作業実施期間における全日とする。
・作業時間
　運用責任者補佐１名、上級 IA 操作員２名及び一般 IA 操作員１名
　　午前 8 時 30 分から午後 5 時 30 分まで（休憩時間は別途協議）
　監視員
　　２名、２交替又は３交替にて 24 時間（休憩時間は別途協議）
　上記以外の運用業務従事者
　　午前 9 時 30 分から午後 6 時 30 分まで（休憩時間は別途協議）

○保守業務従事者に求められる知識・経験等
・要員数については特に定めないが、政府認証基盤を構成するシステムについて障害保守、予防保守等の対応を迅速かつ恒常的に行える体制を組むこと。
・行政機関の認証局又は特定認証局の保守を行った者を含めること。
　⇒令和元年度については、13 名が適合している。
・主要なメンバとして情報セキュリティスペシャリスト試験、テクニカルエンジニア（情報セキュリティ）試験の合格者又は IT スキル標準の IT スペシャリスト職種（専門分野セキュリティ）のレベル４以上の者、若しくは同等の能力を有する者を含むことが望ましい。
　⇒令和元年度については、８名が適合している。

○その他
・運用業務従事者及び保守業務従事者のバックアップ体制をとること。
・運用業務従事者及び保守業務従事者は、夜間・休日を問わず緊急時の連絡及び召集に対応するため、携帯電話等（請負者が手配し通話料・通信料を負担）を常備して常に連絡がとれること。

（業務の繁閑の状況とその対応）

年間の主な作業スケジュールは下表のとおり

| 主な作業項目 | 4月 | 5月 | 6月 | 7月 | 8月 | 9月 | 10月 | 11月 | 12月 | 1月 | 2月 | 3月 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 運用計画 | ● | | | | 随時、見直し | | | | | | | |
| 認証業務 | | | | | | | | | | | | |
| 相互認証審査等支援 | | | | | | | | | | | | |
| 各種証明書発行等 | | | | | | | | | | | | |
| 失効情報の確認（相互認証先を含む） | | | | | | | | | | | | |
| 照会対応(相互認証先等) | | | | | | | | | | | | |
| 外部監査対応 | | 事前準備 | | | 実地監査 | | | | 監査結果への対応 | | | |
| 監査ログ検査 | | | | | | | | | | | | |
| アーカイブ取得及び可読性確認 | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| ＬＲＡ研修 | | ● | | | | | ● | | | | | |
| 教育・訓練 | | | | | 訓練計画策定 | | | ● 危機管理訓練 | | | セｷｭﾘﾃｨ教育 | |
| システムの運用 | | | | | | | | | | | | |
| システム構成管理 | | | | | | | | | | | | |
| （設定値、ﾊﾞｰｼﾞｮﾝ情報、ﾊﾟｯﾁ適用状況等） | | | | | | | | | | | | |
| 稼働状況監視､不正アクセス監視（24時間） | | | | | | | | | | | | |
| ﾃﾞｰﾀ等ﾊﾞｯｸｱｯﾌﾟ（日次） | | | | | | | | | | | | |
| ﾊﾞｯｸｱｯﾌﾟﾃﾞｰﾀ移送 | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |
| パスワード変更管理 | | | | | | | | | | | | |
| ＣＡ秘密鍵可読性確認 | | | | | | | | | | | | ● |
| システムの保守 | | | | | | | | | | | | |
| 障害保守 | | | | | | | | | | | | |
| 予防保守 | | | | | | | | | | | | |
| 利用者環境の維持 | | | | | | | | | | | | |
| 認証局施設・設備の管理 | | | | | | | | | | | | |
| 入退室管理 | | | | | | | | | | | | |
| 報告書の作成 | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● |

平成 29～令和元年度の主な状況は以下のとおり。

（単位：件）

| | 平成 29 年度 | 平成 30 年度 | 令和元年度 |
|---|---|---|---|
| 相互認証(新規・更新・失効)件数 | 1 | 8 | 9 |
| 認証情報公開サービスの利用件数 | 14,022,265 | 12,327,793 | 13,810,882 |
| 証明書検証サービスの利用件数 | 67,686,516 | 120,568,246 | 159,692,871 |
| 証明書の発行枚数 | 1,163 | 1,922 | 13,189 |
| 問合せ対応件数 | 59 | 87 | 124 |
| サービス停止を伴う重大な障害保守件数 | 0 | 0 | 0 |
| その他の障害保守件数（注） | 13 | 2 | 4 |
| 予防保守件数（上段：脆弱性調査件数） | 2,062 | 1,783 | 1,982 |
| 予防保守件数（下段：ﾊﾟｯﾁ等適用件数） | 6 | 6 | 0 |
| 利用者環境の維持 | 19 | 21 | 11 |

（注）

- 年度内に発生した障害件数であり、対応に期間を要し翌年度に完了したものについても、発生年度に記載。
- 平成 30 年度、令和元年度には、システム運用開始当初（平成 20 年 1 月）から 3 世代後に発行した証明書の有効期間を迎えたため、再発行があったため、当該年度の発行件数が増えている。

3　従来の実施に要した施設及び設備

（マスタセンタ）
【施設】
使用場所：東京都内

※マスタセンタには、事務室、監視室及びテストセンタがあり、常時、運用要員が作業する場所となる。
また、バックアップセンタの稼働監視等はマスタセンタの監視室からの遠隔監視により行っている。

【設備及び主な物品】
請負者所有：
空調装置７式、監視カメラ 24 台、IC カード認証装置 15 台、生体認証装置９台、ラック架台 53 台、ラック 14 台、消火装置 17 台、金庫 11 台、机 47 台、椅子 37 脚、会議用テーブル８台、ロッカー２台、災害時優先電話２台、ファックス１台、ホワイトボード１台

（バックアップセンタ）
【施設】
使用場所：東京近郊

（注記事項）

以下の条件を満たす新たな施設・設備を提案することとし、施設使用料、通信回線使用料等は現行月額を上限とすること。また、機器等の移設・据付・調整･システム設定・テスト等への対応は、請負者の責任と負担において行うこと。

（条件）
- 新たな施設・設備は、別添資料３「政府認証基盤　施設・設備の詳細仕様」を満たしていること。
- 移設に伴う本システムのサービス停止時間（新旧システムの切替えに伴うもの）については、システム更改の請負者と連携して 24 時間内とし、回数は４回を限度とすること。

※施設・設備の詳細については、別途、閲覧に供する「現行の施設・設備の詳細」資料を参照。

4　従来の実施における目標の達成の程度

| SLA 達成率 | 平成 29 年度 | | 平成 30 年度 | | 令和元年度 | |
|---|---|---|---|---|---|---|
| | 目標 | 実績 | 目標 | 実績 | 目標 | 実績 |
| | | | | | | |
| サービスの稼働率 | | | | | | |
| 認証情報公開サービス | 99.99%以上 | 100.00% | 99.99%以上 | 100.00% | 99.99%以上 | 100.00% |
| 証明書検証サービス | 99.99%以上 | 100.00% | 99.99%以上 | 100.00% | 99.99%以上 | 100.00% |
| 証明書の発行サービス | 99.9%以上 | 100.00% | 99.9%以上 | 100.00% | 99.9%以上 | 100.00% |
| 障害件数(サービス停止を伴うもの) | 1回/年以内 | 0件 | 1回/年以内 | 0件 | 1回/年以内 | 0件 |
| 認証情報公開サービス | 1回/年以内 | 0件 | 1回/年以内 | 0件 | 1回/年以内 | 0件 |
| 証明書検証サービス | 1回/年以内 | 0件 | 1回/年以内 | 0件 | 1回/年以内 | 0件 |
| 証明書の発行サービス | | | | | | |
| 障害復旧時間 | | | | | | |
| 認証情報公開サービス | 1時間以内 | － | 1時間以内 | － | 1時間以内 | － |
| 証明書検証サービス | 1時間以内 | － | 1時間以内 | － | 1時間以内 | － |
| 証明書の発行サービス | 8時間以内 | － | 8時間以内 | － | 8時間以内 | － |
| 応答時間(平均値(秒)) | | | | | | |
| 認証情報公開サービス | 1.0秒以内 | 0.00001256 | 1.0秒以内 | 0.00000571 | 1.0秒以内 | 0.00000485 |
| 証明書検証サービス | 1.0秒以内 | 0.0041 | 1.0秒以内 | 0.039 | 1.0秒以内 | 0.04 |

5　従来の実施方法等

従来の実施方法（業務フロー図等）

別紙２のとおり

（注記事項）

1　政府認証基盤の運用・保守の対象となるシステムの詳細は、別途閲覧に供する以下の仕様書等を参照。

・構築仕様書（ブリッジ CA 編、官職 CA 編、内部用サーバ CA 編、ネットワーク編）

・LRA システム基本設計書

・IC カードシステム仕様書

・政府認証基盤 業務管理マニュアル

・政府認証基盤 システム運用マニュアル

・LRA 業務管理・システム運用マニュアル

・証明書申請の手引き

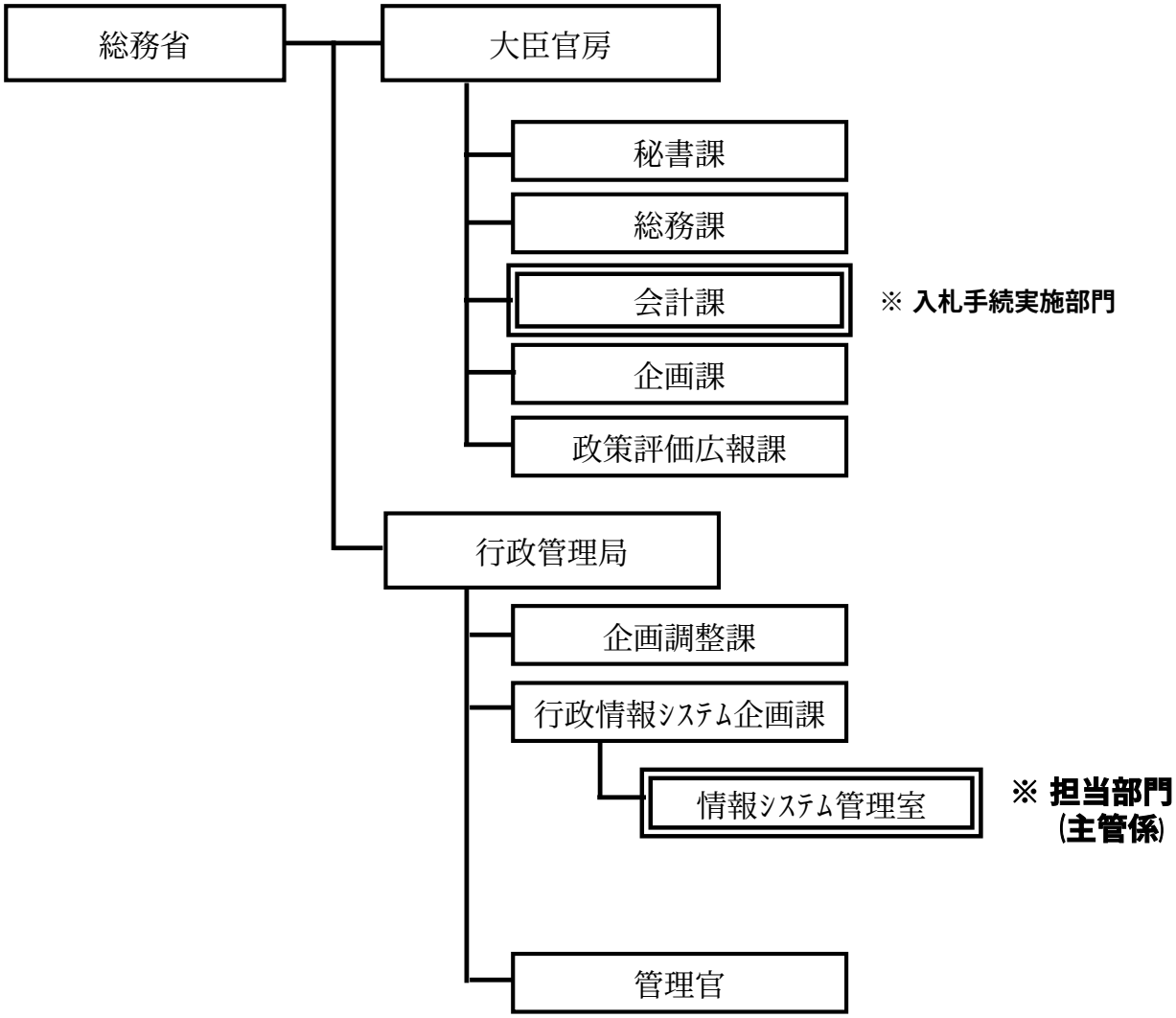
・現行の施設・設備の詳細

2　１に示す資料のほか、現行の手順書及び３に示す研修資料については、請負者に対し提供を行う。

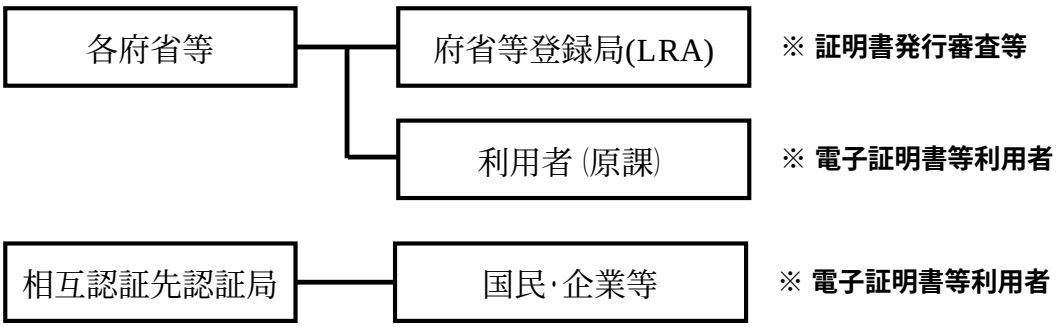
3　現行政府認証基盤において、各府省等 LRA 要員への研修については、年２回の研修を実施

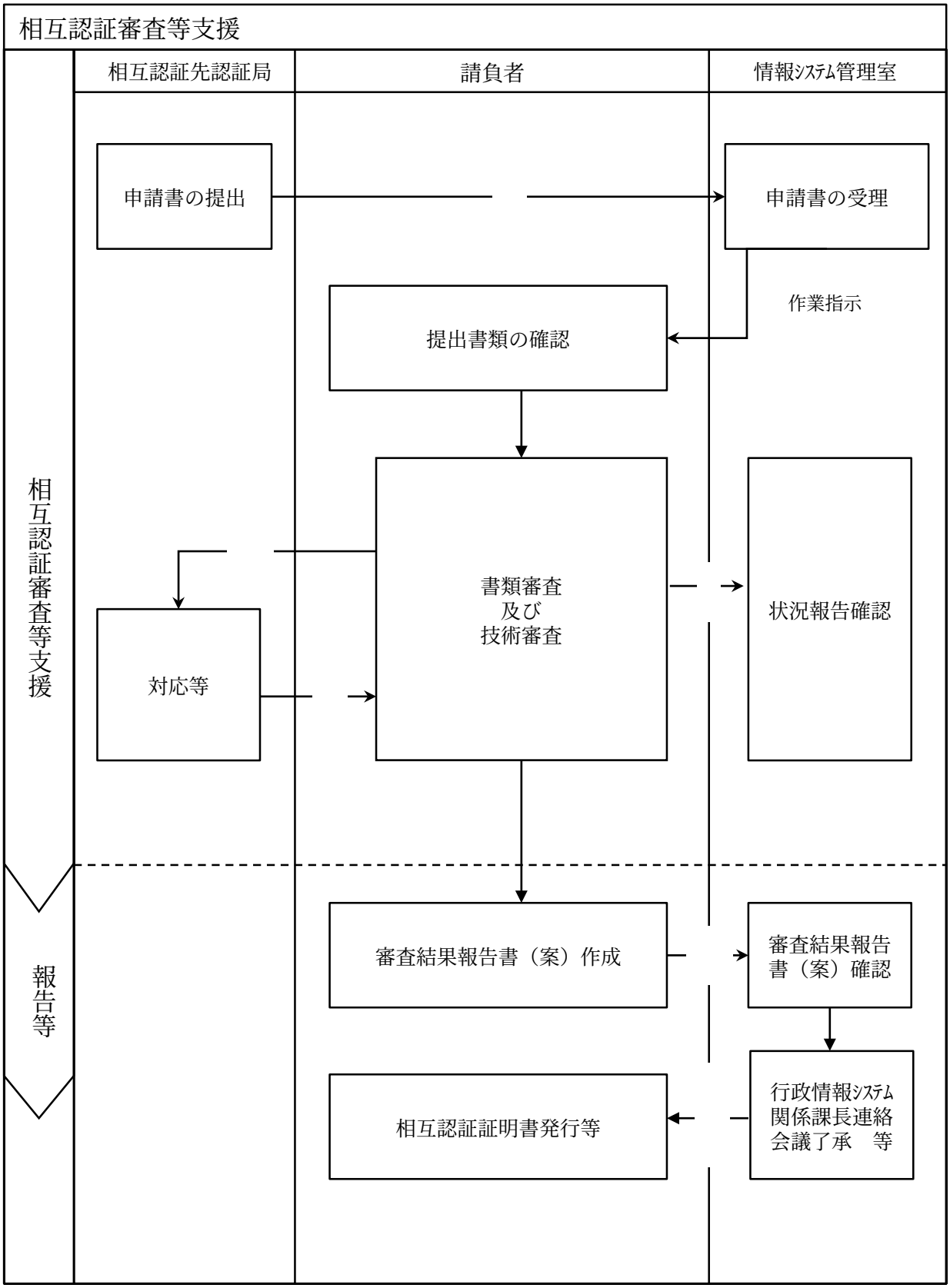
# 運 用・保 守 業 務 フ ロ ー

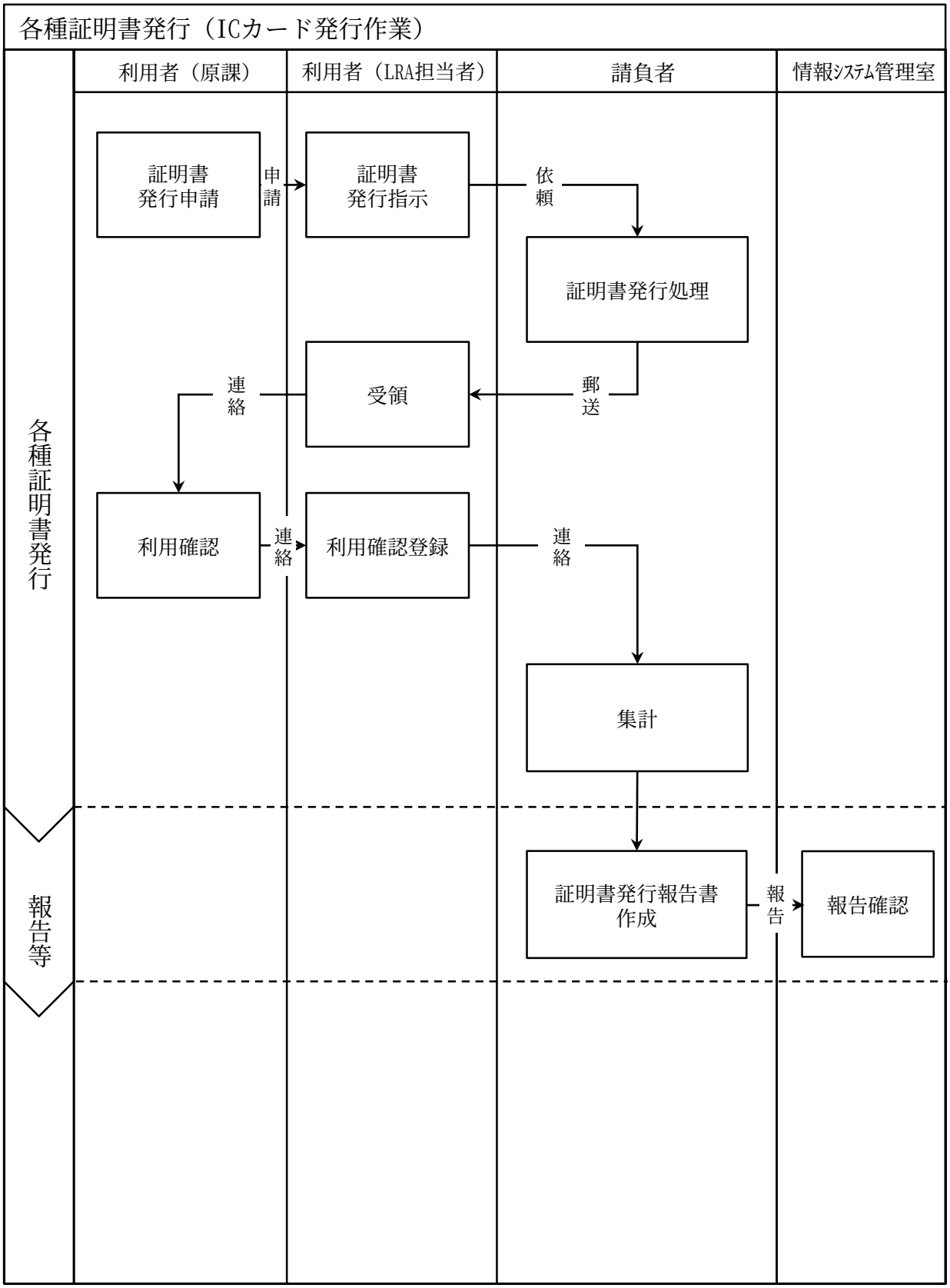
総務省の組織(関係部門)及び利用者は、下図のとおり。
また、運用・保守業務の主な業務フローを次頁以降に示す。

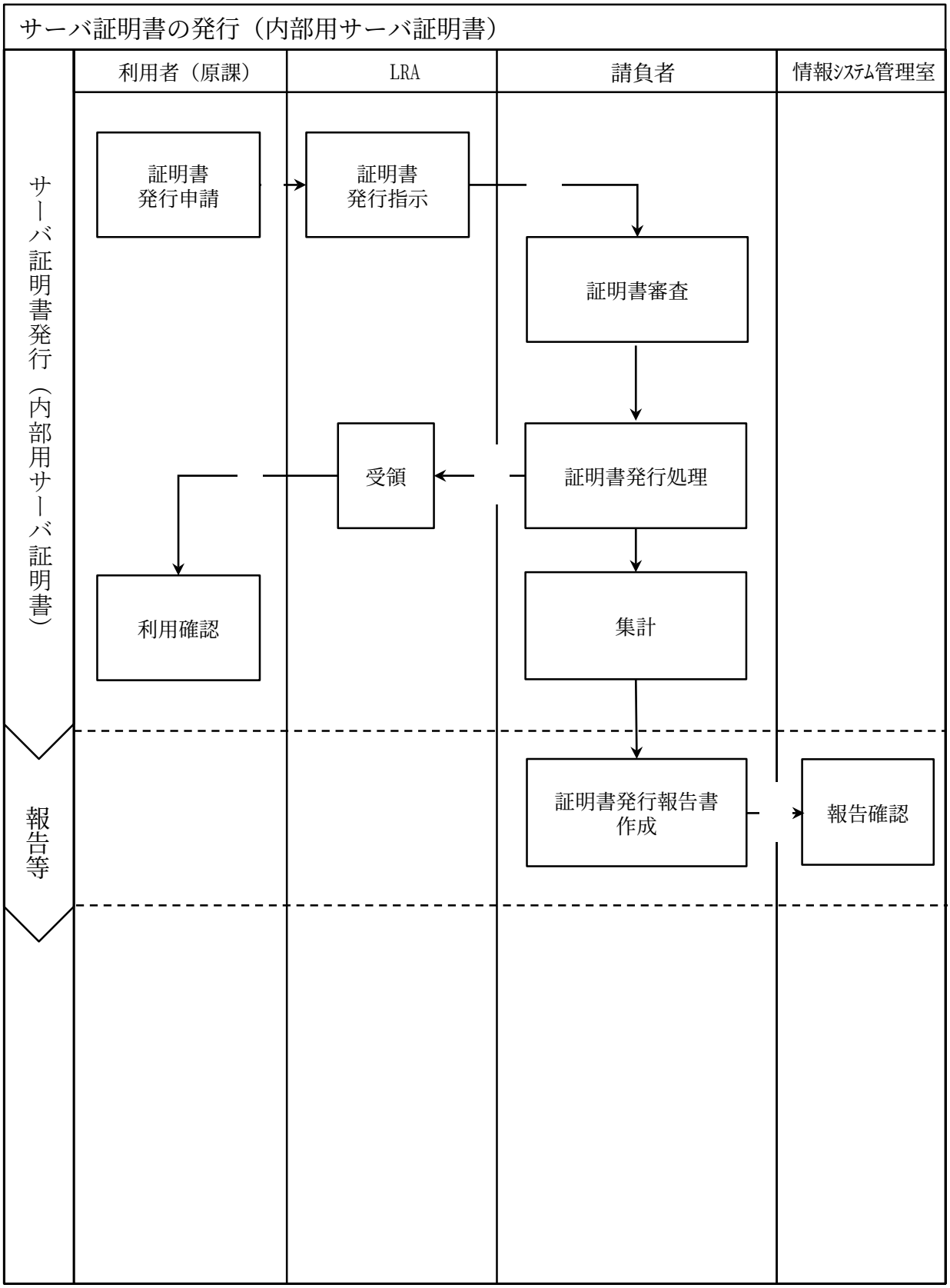



## 【 利用者 】

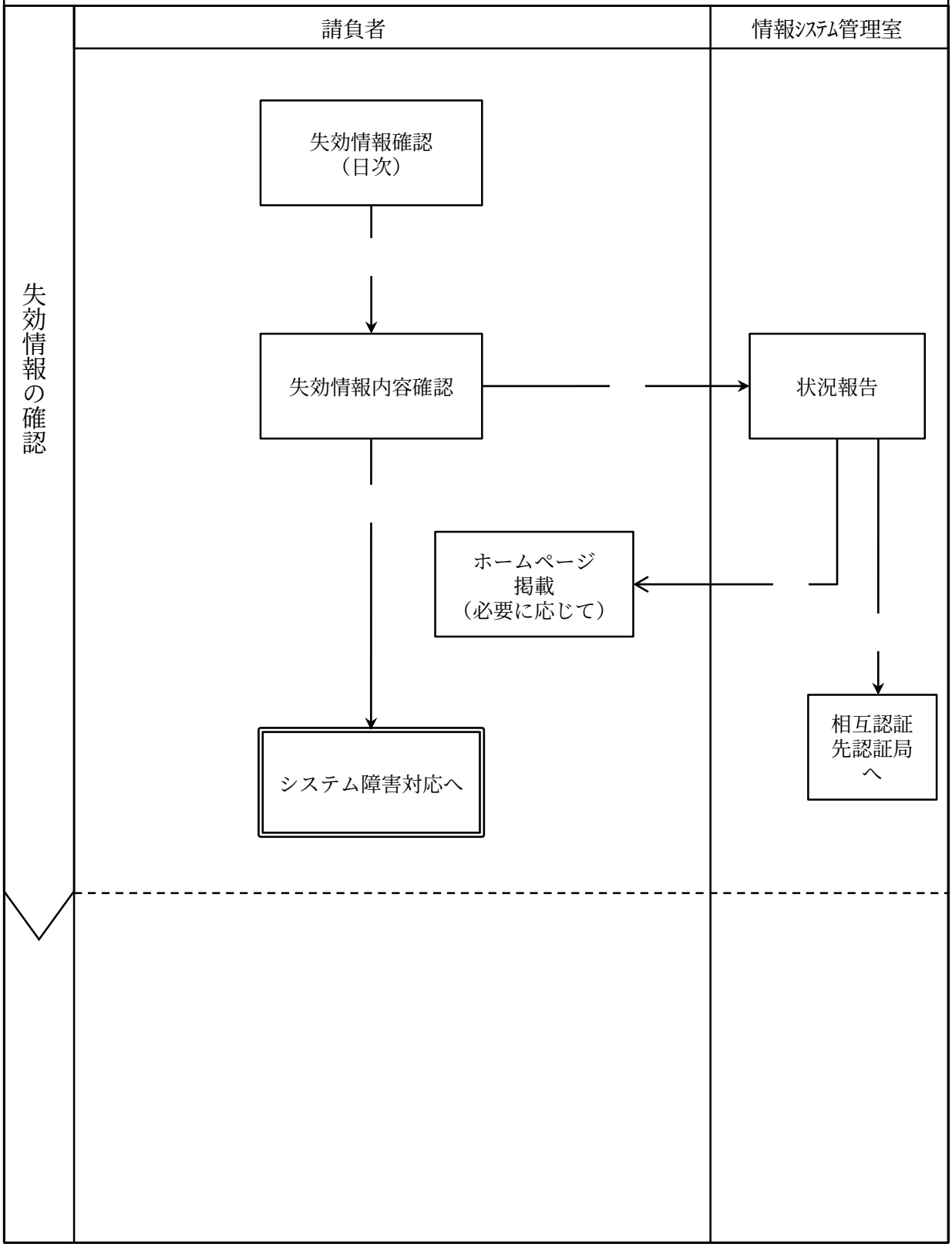


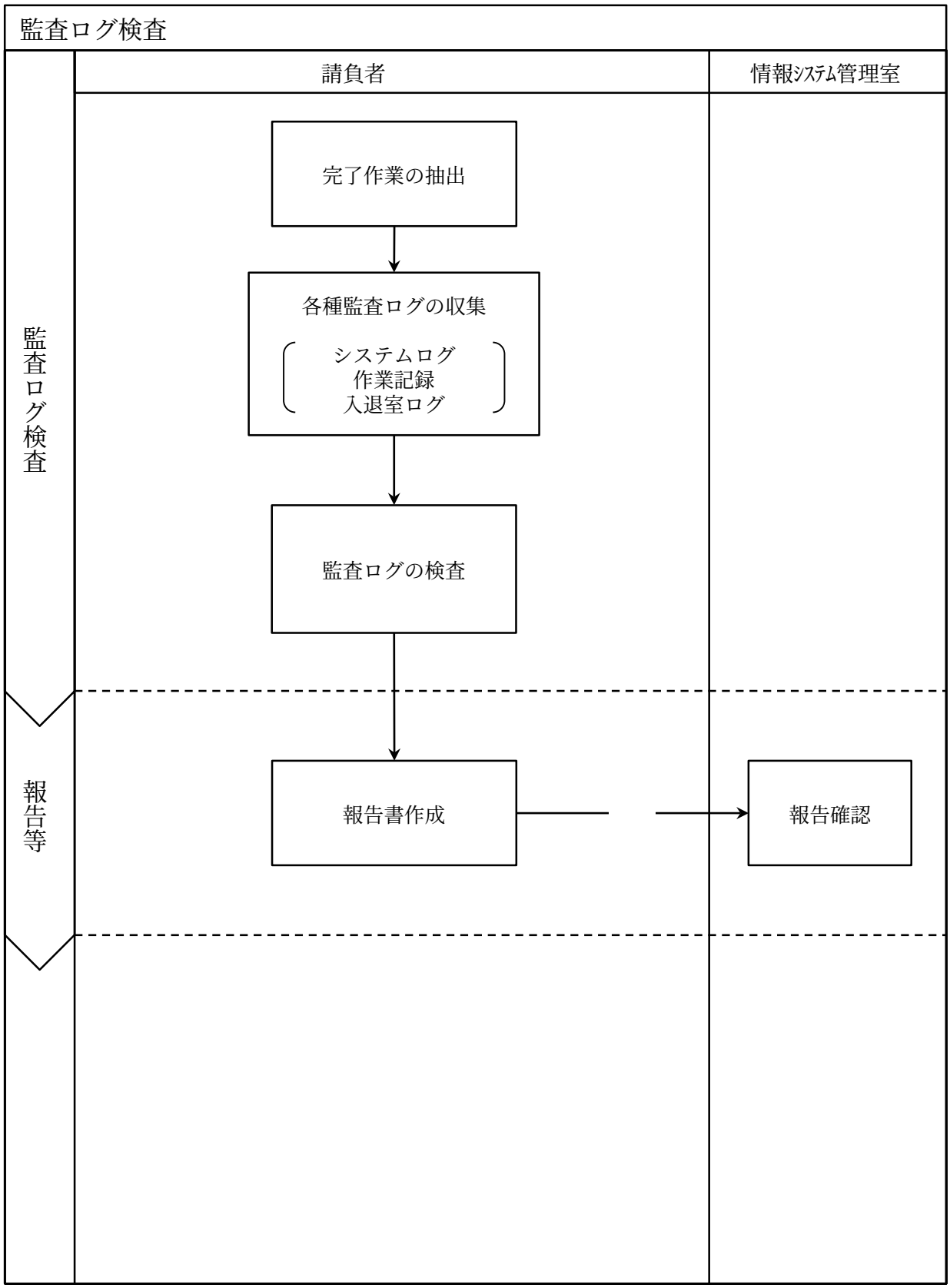

相互認証審査等支援
相互認証先認証局
請負者
情報ｼｽﾃﾑ管理室
申請書の提出
申請書の受理
作業指示
提出書類の確認
書類審査
及び
技術審査
状況報告確認
対応等
相互認証審査等支援
報告等
審査結果報告書（案）作成
審査結果報告書（案）確認
行政情報ｼｽﾃﾑ関係課長連絡会議了承　等
相互認証証明書発行等

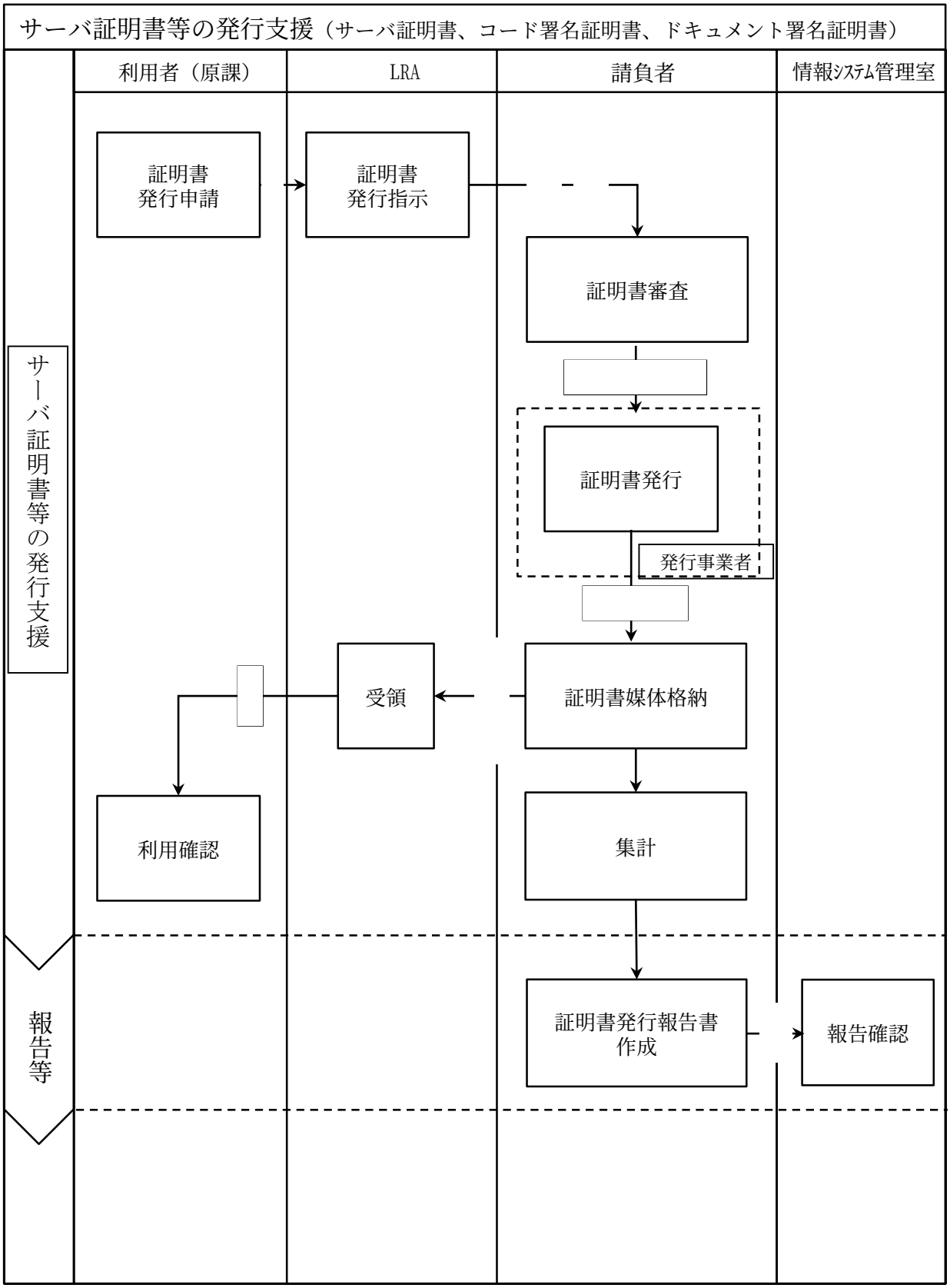

各種証明書発行（ICカード発行作業）
利用者（原課）
利用者（LRA担当者）
請負者
情報ｼｽﾃﾑ管理室
各種証明書発行
報告等
証明書
発行申請
申
請
証明書
発行指示
依
頼
証明書発行処理
受領
郵
送
連
絡
利用確認
連
絡
利用確認登録
連
絡
集計
証明書発行報告書
作成
報
告
報告確認

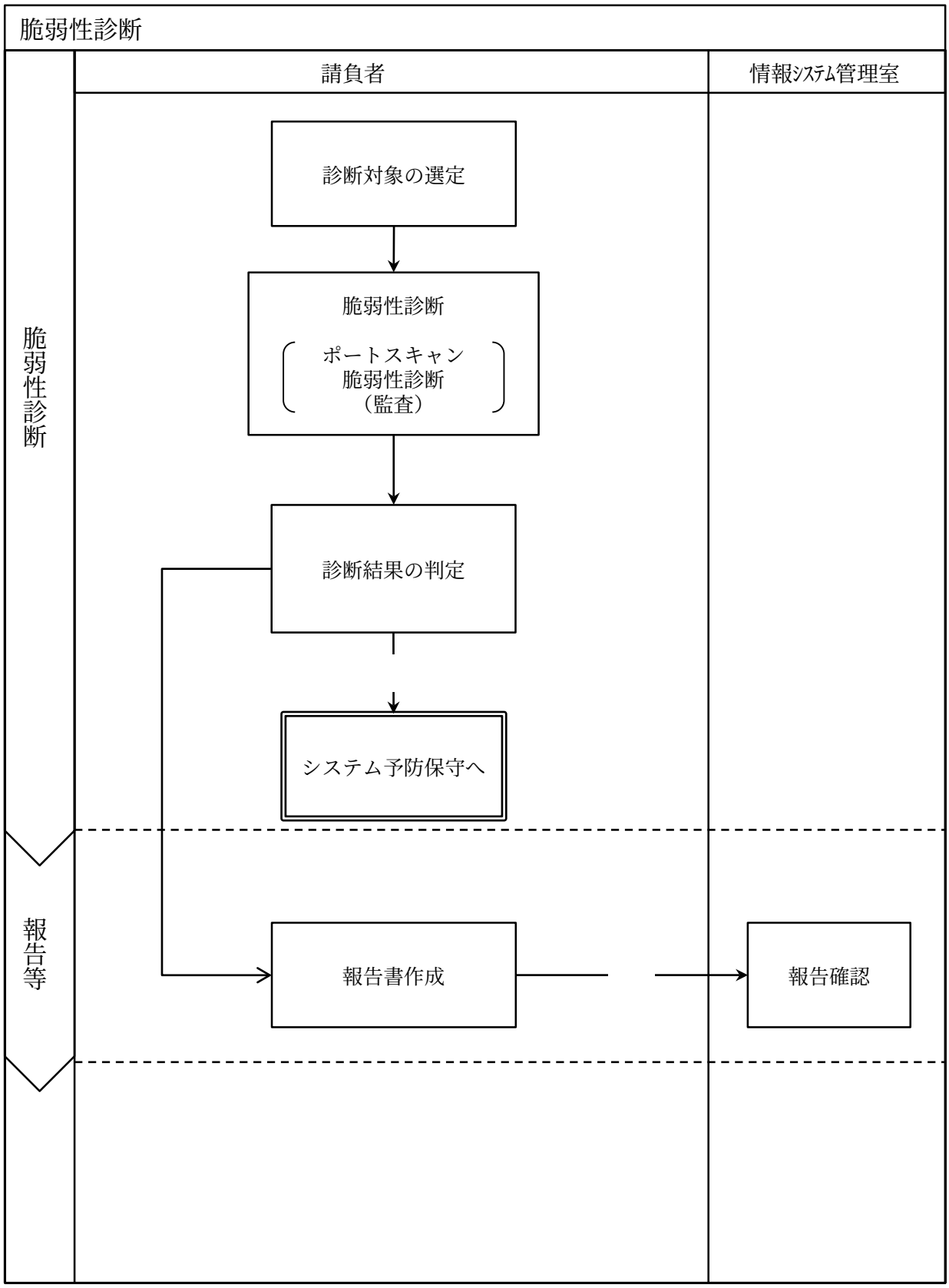

サーバ証明書の発行（内部用サーバ証明書）
利用者（原課）
LRA
請負者
情報ｼｽﾃﾑ管理室
サーバ証明書発行（内部用サーバ証明書）
証明書
発行申請
証明書
発行指示
証明書審査
受領
証明書発行処理
利用確認
集計
報告等
証明書発行報告書
作成
報告確認

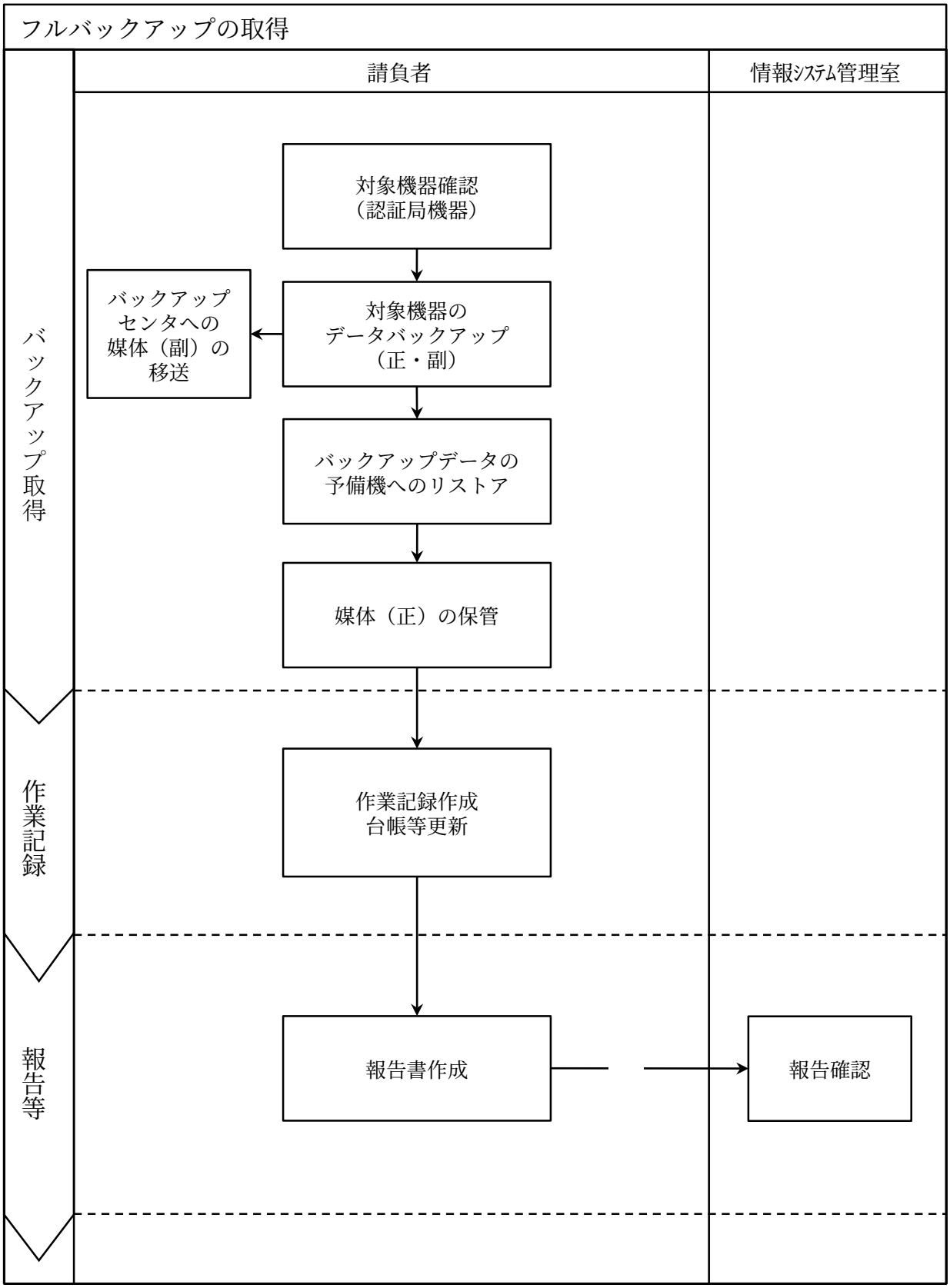
失効情報の確認（相互認証先を含む。）

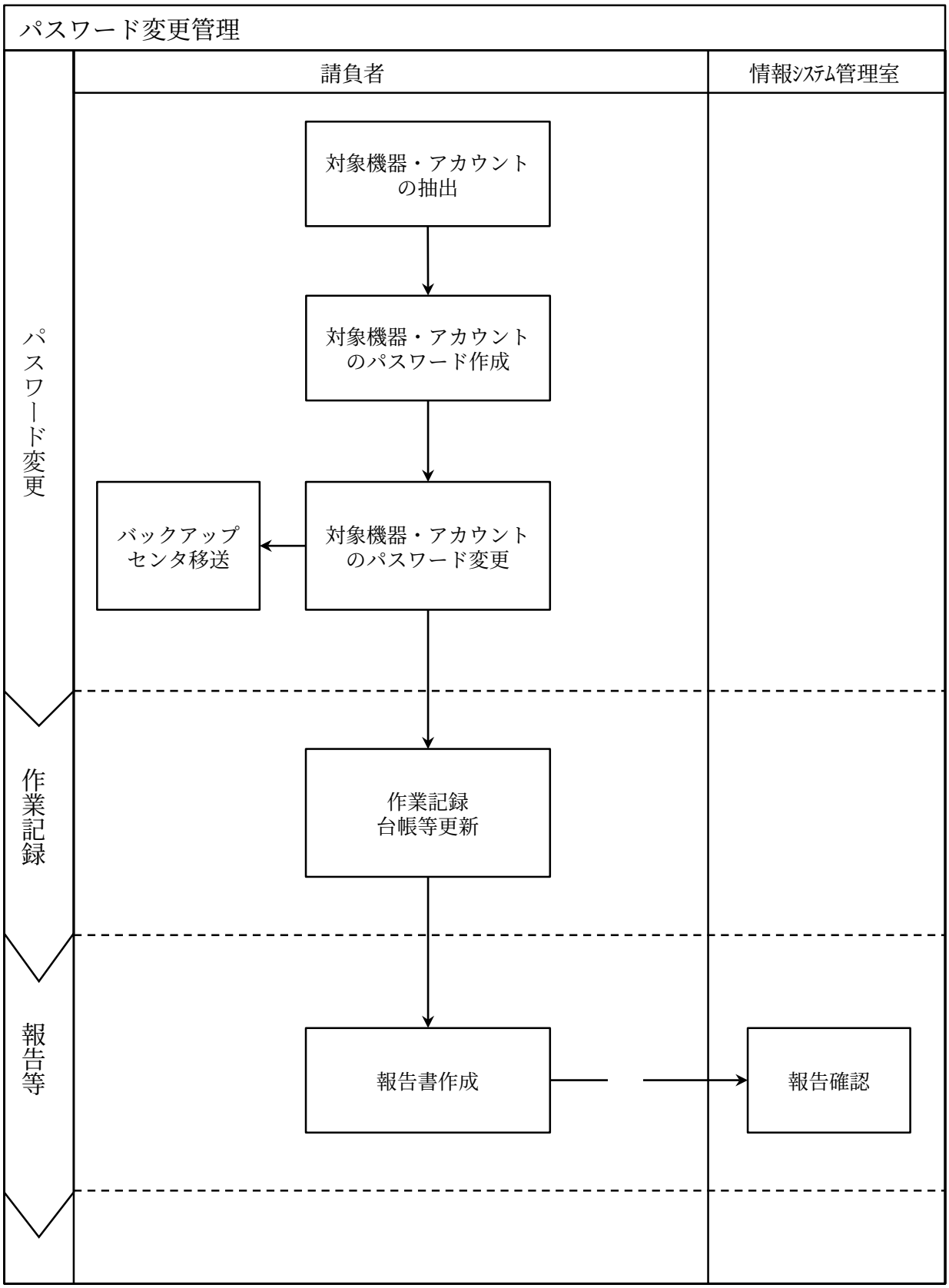


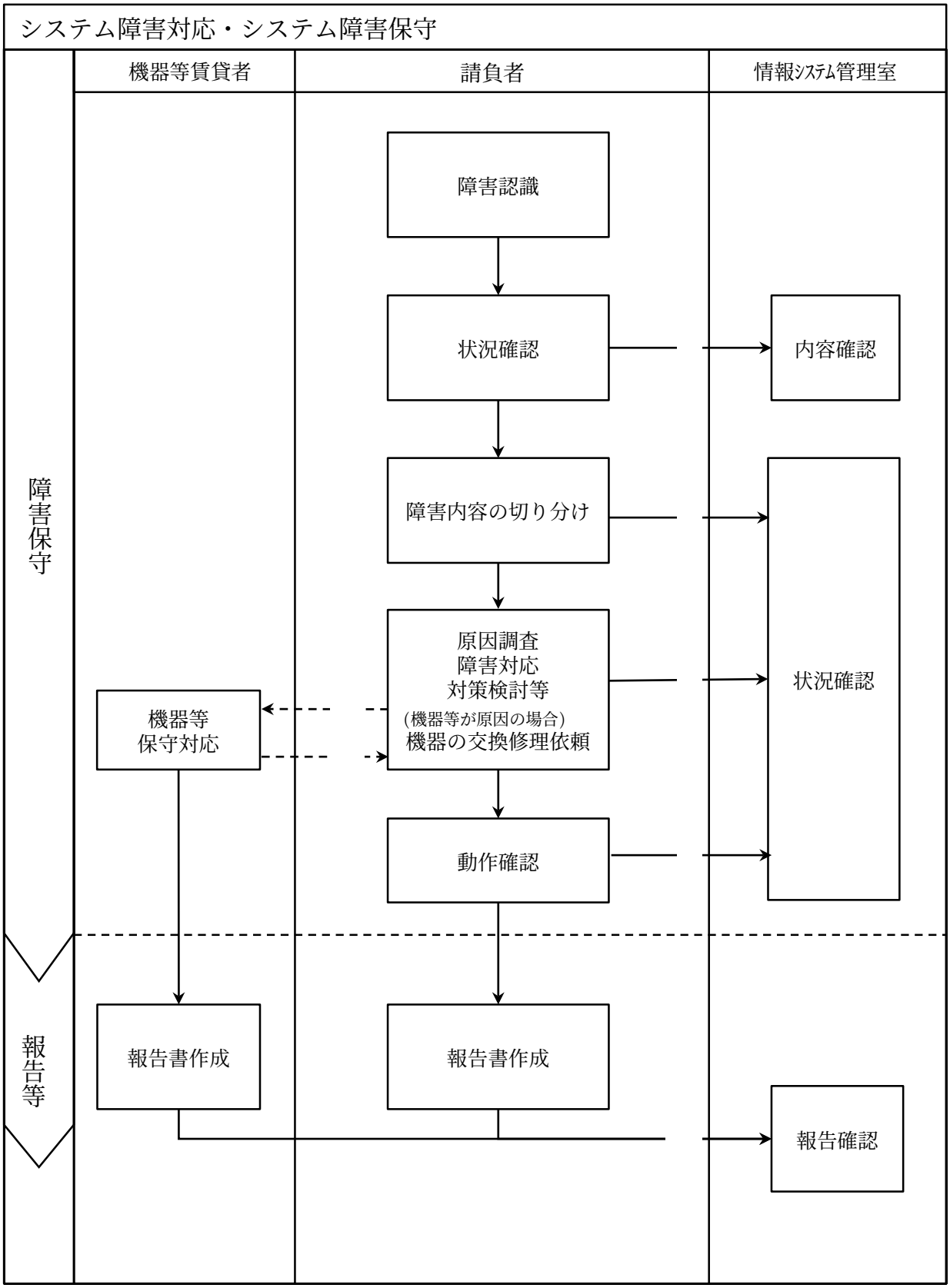

監査ログ検査
請負者
情報ｼｽﾃﾑ管理室
監査ログ検査
完了作業の抽出
各種監査ログの収集
システムログ
作業記録
入退室ログ
監査ログの検査
報告等
報告書作成
報告確認

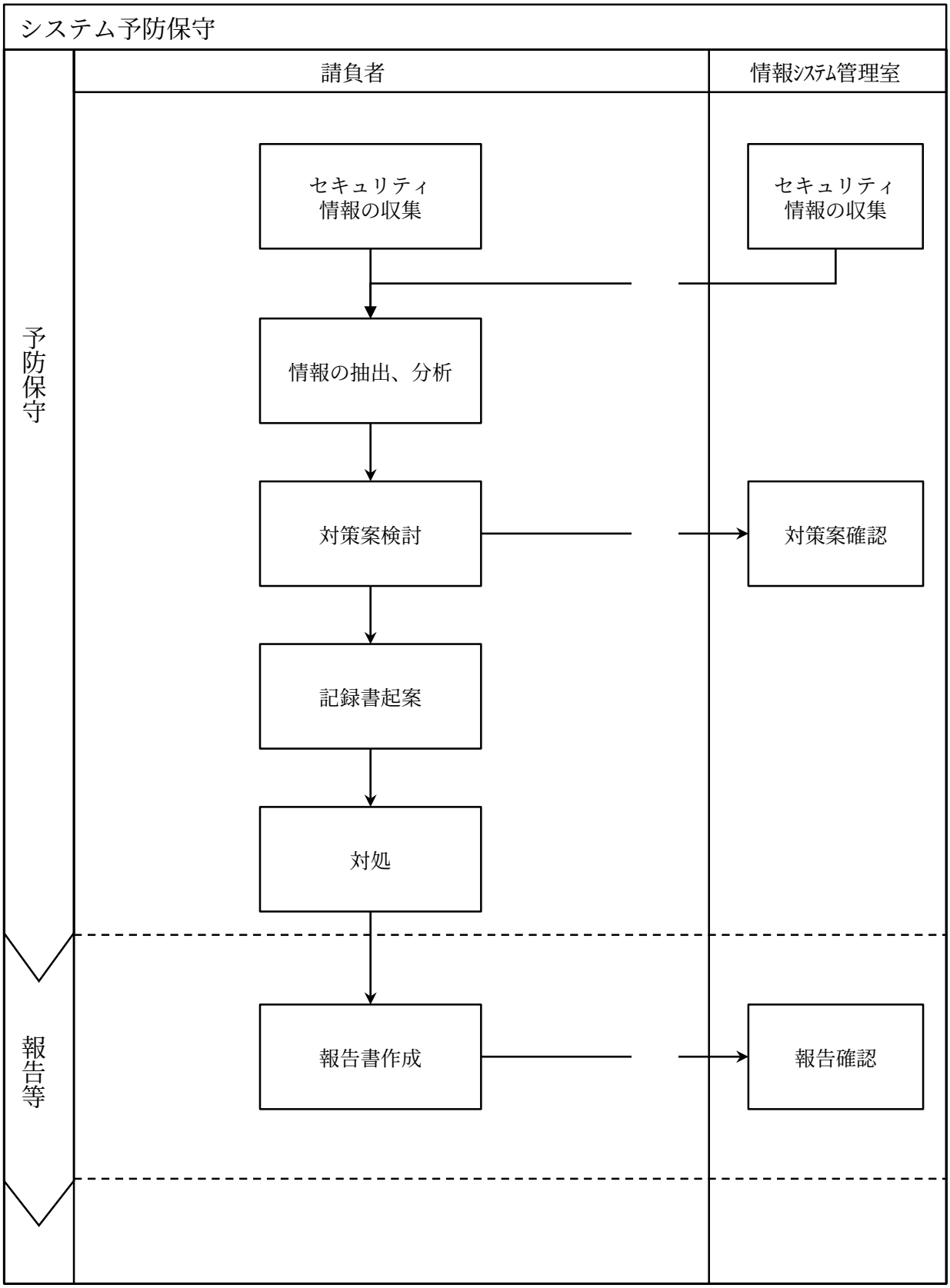

サーバ証明書等の発行支援（サーバ証明書、コード署名証明書、ドキュメント署名証明書）
利用者（原課）
LRA
請負者
情報ｼｽﾃﾑ管理室
サーバ証明書等の発行支援
証明書
発行申請
証明書
発行指示
証明書審査
証明書発行
発行事業者
受領
証明書媒体格納
利用確認
集計
報告等
証明書発行報告書
作成
報告確認

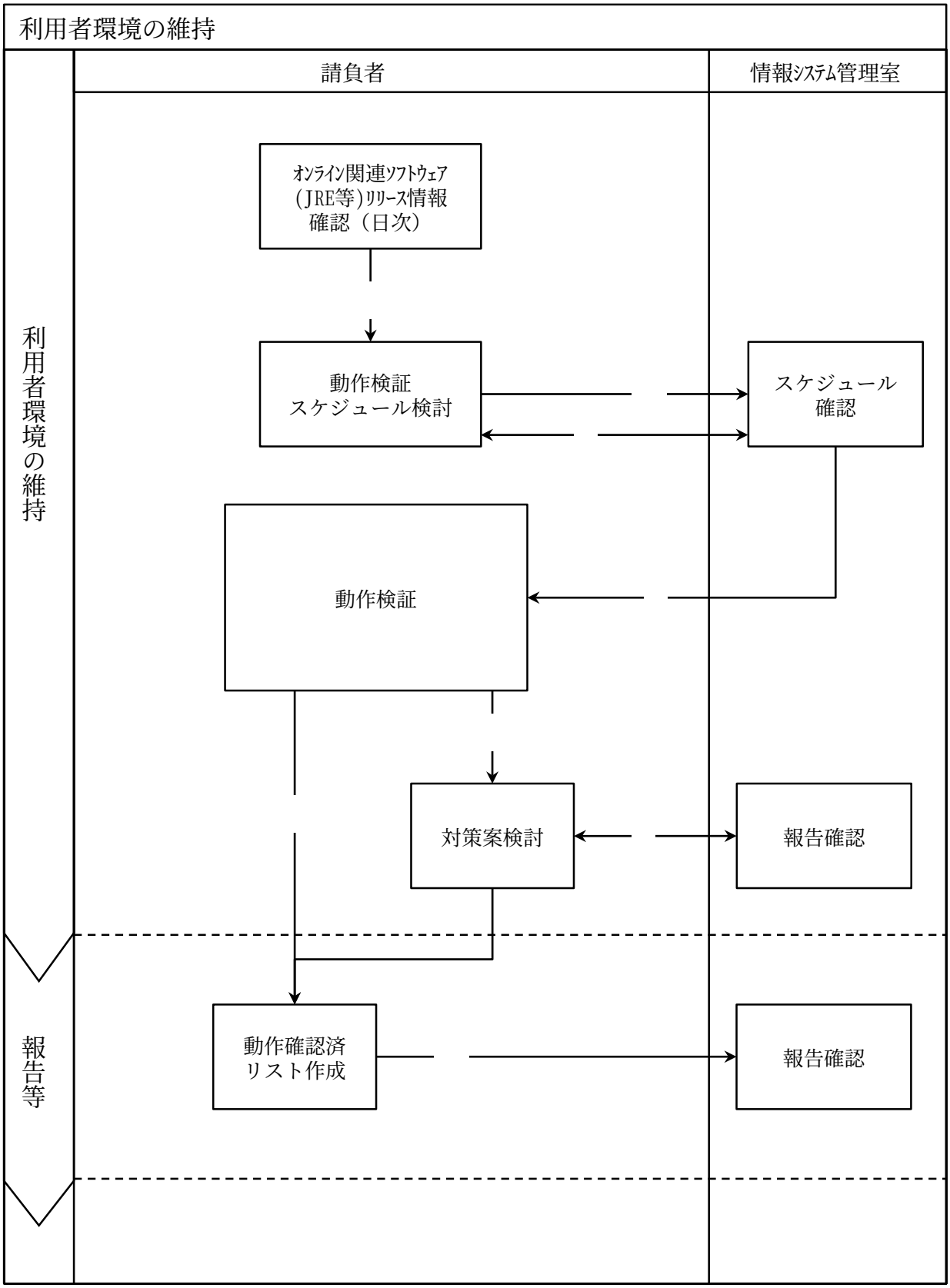

脆弱性診断
請負者
情報ｼｽﾃﾑ管理室
脆弱性診断
診断対象の選定
脆弱性診断
ポートスキャン
脆弱性診断
（監査）
診断結果の判定
システム予防保守へ
報告等
報告書作成
報告確認


フルバックアップの取得
請負者
情報ｼｽﾃﾑ管理室
バックアップ取得
作業記録
報告等
対象機器確認
（認証局機器）
対象機器の
データバックアップ
（正・副）
バックアップ
センタへの
媒体（副）の
移送
バックアップデータの
予備機へのリストア
媒体（正）の保管
作業記録作成
台帳等更新
報告書作成
報告確認


パスワード変更管理
請負者
情報ｼｽﾃﾑ管理室
パスワード変更
作業記録
報告等
対象機器・アカウントの抽出
対象機器・アカウントのパスワード作成
対象機器・アカウントのパスワード変更
バックアップセンタ移送
作業記録台帳等更新
報告書作成
報告確認


システム障害対応・システム障害保守
機器等賃貸者
請負者
情報ｼｽﾃﾑ管理室
障害保守
報告等
障害認識
状況確認
内容確認
障害内容の切り分け
原因調査
障害対応
対策検討等
(機器等が原因の場合)
機器の交換修理依頼
状況確認
機器等
保守対応
動作確認
報告書作成
報告書作成
報告確認


システム予防保守
請負者
情報ｼｽﾃﾑ管理室
予防保守
セキュリティ情報の収集
セキュリティ情報の収集
情報の抽出、分析
対策案検討
対策案確認
記録書起案
対処
報告等
報告書作成
報告確認


利用者環境の維持
請負者
情報ｼｽﾃﾑ管理室
利用者環境の維持
ｵﾝﾗｲﾝ関連ｿﾌﾄｳｪｱ
(JRE等)ﾘﾘｰｽ情報
確認（日次）
動作検証
スケジュール検討
スケジュール
確認
動作検証
対策案検討
報告確認
報告等
動作確認済
リスト作成
報告確認

# 政府認証基盤の運用・保守の請負

(Operation, Management and Maintenance of the Government Public Key Infrastructure)

# 調達仕様書(案)

総務省

## 1 調達件名

「政府認証基盤の運用・保守の請負」

Operation, Management and Maintenance of the Government Public Key Infrastructure

## 2 作業の概要

（１）目的

政府認証基盤は「ミレニアム・プロジェクト（新しい千年紀プロジェクト）について」（1999年(平成 11 年)12 月 19 日内閣総理大臣決定）に基づき、国民等と行政との間でインターネット等を利用してやり取りされる申請・届出等手続に係る電子文書について、その文書が真にその名義人によって作成され、内容に改ざんがないことを相互に確認できるように整備されたものであり、①処分権者に係る電子署名を行うために用いる電子証明書（以下「官職証明書」という。）等を発行する府省認証局、②府省認証局と国民等に係る電子証明書等を発行する民間認証局等との間の相互認証を行うブリッジ認証局で構成され、平成 13 年 4 月にその運用を開始した。

その後、「電子政府構築計画」（2003 年(平成 15 年)7月 17 日各府省情報化統括責任者（CIO）連絡会議決定。2004 年(平成 16 年)6月 14 日一部改定。）において、府省共通業務・システムとして、システムの共通化・一元化等を内容とする最適化計画を策定し、システムの見直しを進めることとされ、平成 17 年3月 31 日に「霞が関 WAN 及び政府認証基盤（共通システム）の最適化計画」[1]（以下「最適化計画」という。）が各府省情報化統括責任者(CIO)連絡会議決定)で決定された。

この最適化計画に基づき、平成 20 年 1 月に官職証明書等を一元的に発行する政府共用認証局の運用を開始し、府省等が個別に整備・運用してきた府省認証局（14 認証局）及び最高裁判所認証局を順次廃止して政府共用認証局に集約することにより、最適化効果として年間約 9.6 億円の運用経費の削減を達成した。

また、「政府機関の情報システムにおいて使用されている暗号アルゴリズム SHA-1 及び RSA1024 に係る移行指針（平成 20 年4月 22 日 情報セキュリティ政策会議決定）[2]（以下、「移行指針」という。）」に基づき、平成 26 年9月に、より安全な暗号アルゴリズムへの移行を行うとともに、相互認証先認証局との相互認証更新を行った。

一方、アプリケーション認証局に係る認証業務は平成 30 年4月をもって終了し、平成 30 年5月以降、サーバ証明書等について民間認証局から取得する手続を政府認証基盤が取りまとめる業務（サーバ証明書等の発行支援業務）に切り替えた。

本件は、システム更改により令和4年2月から運用開始する新システムを用いた政府認証基盤の業務・システムについて、24 時間週7日安全かつ確実に稼働させるための運用及び保守を調達するものである。

---

[1] http://www.kantei.go.jp/jp/singi/it2/cio/dai13/13siryou1.pdf

[2] http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf

（２） 用語の定義

・ 官職証明書

ある公開鍵が、記載された官職のものであることを保証する公開鍵証明書。政府共用認証局の官職認証局が発行する。

・ 官職認証局（官職 CA、OSCA）

申請・届出等手続における行政機関等側の官職証明書等を発行する認証局で、政府共用認証局を構成する認証局の一つ。

・ コード署名証明書

インターネットを利用して、ソフトウェアを安全に配布するために用いる公開鍵証明書。コード署名証明書により配布元をなりすまされたり、プログラムが改ざんされていないことを保証することができる。

・ サーバ証明書

クライアント、サーバ間で安全な通信を行うために、そのサーバが信頼できるものであることを証明した公開鍵証明書。

・ 自己署名証明書

発行者名と主体者名が同一であり、自認証局の公開鍵に対して、自認証局の対応する秘密鍵で署名した公開鍵証明書。自認証局の公開鍵の正当性を保証する。

・証明書検証システム

申請・届出等手続における行政機関等側が公開鍵証明書の有効性を検証するためのシステム。CVS（政府共用証明書検証サーバ）によって構成されるシステム。

・ 政府共用認証局（政府共用 CA）

申請・届出等手続における行政機関等側の官職証明書等を発行する認証局。官職認証局によって構成される。

・ 政府共用認証システム

政府共用認証局の鍵の生成・管理、証明書の発行等を行うシステム。

・ 政府共用認証情報格納システム

政府共用認証局の認証情報を、公開に先立って格納するシステム。

・ 相互認証証明書

2つの異なる認証ドメインの認証局がお互いを認証したことを示すために、相互に発行する証明書。政府認証基盤（ブリッジ認証局）では、政府共用認証局の官職認証局、民間認証局又は商業登記認証局との間で相互認証証明書が発行される。

・統合認証情報公開システム

政府認証基盤を構成するブリッジ認証局、政府共用認証局及び商業登記認証局から発行された証明書及び失効情報（CRL/ARL）を各々の認証情報格納システムから集約し、統合されたリポジトリとして認証情報を公表するためのシステム。

・ ドキュメント署名証明書

インターネットを利用して、PDF ファイルの電子ドキュメントを安全に配布するために用いる公開鍵証明書。ドキュメント署名証明書により配布元をなりすまされたり、電子ドキュメントが改ざんされていないことを保証することができる。

・ 内部用サーバ証明書

クライアント、サーバ間で安全な通信を行うために、そのサーバが信頼できるものであることを証明した公開鍵証明書。各府省が運営している Web サーバのうち各府省の内部ネットワークまたは政府共通ネットワークで使用される Web サーバに対して発行するもの。

・ 内部用サーバ認証局（内部用サーバ CA、ISCA）

各府省が運営している業務システム等で必要とする内部用のサーバ証明書を発行する認証局。政府認証基盤を構成する認証局ではないが、同施設内に設置していることから、政府認証基盤を構成する認証局と同様の認証業務及び運用業務を行う。

・認証システム

認証局において公開鍵証明書の発行、失効、鍵管理を行うシステム。政府認証基盤は、ブリッジ認証局のブリッジ認証システム、政府共用認証局の政府共用認証システムを有する。

・認証情報

認証局から発行された証明書とその失効情報（CRL/ARL）のこと。GPKI では自己署名証明書、リンク証明書、相互認証証明書及びそれらの失効情報を総じて認証情報を呼ぶ。

・認証情報公開システム

発行された証明書及び失効情報（CRL/ARL）を格納しリポジトリを公表するためのシステム。政府認証基盤においては、公開鍵証明書の発行、失効、鍵管理を行うシステムを認証システムと呼ぶが、リポジトリを公表するシステムを認証情報公開システムと呼ぶ。

・ 府省等登録局（LRA：Local Registration Authority）

府省等内における証明書利用者からの証明書の発行、更新及び失効申請の受付と審査を行う、府省等単位で設置される組織。

・ ブリッジ認証局（ブリッジ CA、BCA）

政府共用認証局の官職認証局及び民間認証局との間に相互認証証明書を発行して、認証基盤の要としての役割を果たす認証局。

・ ブリッジ認証システム

ブリッジ認証局の鍵の生成・管理、証明書の発行等を行うシステム。

・ブリッジ認証情報格納システム

ブリッジ認証局の認証情報を、公開に先立って格納するシステム。

・ リポジトリ

証明書及び CRL/ARL を格納し公表するデータベース。政府認証基盤ではディレクトリサーバを使用する。

・ 利用者証明書

ある公開鍵が、記載された官職等のものであることを保証する公開鍵証明書。政府共用 CA の官職 CA が発行する。

・ リンク証明書

認証局の鍵更新に伴い同時に存在することとなる新しい鍵ペアと古い鍵ペアの関係を保証するための証明書。発行者名及び主体者名は同じだが、新しい証明書の利用者に対しては新しい世代の鍵で古い世代の鍵を署名した証明書によって、古い証明書の利用者に対しては古い世代の鍵で新しい世代の鍵を署名した証明書によってその関係を示す。

・ CA（Certification Authority）

認証局。

・ CP（Certificate Policy）

証明書ポリシ。

・ CPS（Certification Practice Statement）

認証実施規程。

・ CRL/ARL（Certificate Revocation List / Authority Revocation List）

証明書の失効リスト。

・ CVS（政府共用証明書検証サーバ）

認証パスの検索、証明書，失効情報の取得を行い、公開鍵証明書の有効性を検証するサーバ。

・ GPKI（Government Public Key Infrastructure:政府認証基盤）

国民等と行政機関との間でインターネット等を利用してやり取りされる申請・届出等手続に係る電子文書について、その文書が真にその名義人によって作成され、内容に改変がないことを相互に確認できるようにするための仕組み。

・ HSM（Hardware Security Module：ハードウェアセキュリティモジュール）

ハードウェアによる秘密鍵の管理装置。

・JPKI（公的個人認証サービス）

インターネットを通じて安全・確実な行政手続き等を行うために、他人によるなりすまし申請や電子データが通信途中で改ざんされていないことを確認するための機能を全国どこに住んでいる人に対しても提供するもの。この公的個人認証サービスを利用することで、自宅や職場などのパソコンから様々な行政手続き等を行うことができる。

・ OCSP（Online Certificate Status Protocol）レスポンダ

署名検証者からの検証要求に対し、証明書の有効性を確認し、その結果を返す仕組み。

・LRA（Local Registration Authority）システム

府省等登録局が政府共通ネットワーク経由で政府共用認証局の証明書発行・失効指示を行うためのシステム。LRA システムは府省等側の機能である府省 LRA と政府共用認証局側の機能から構成される。

・ WebTrust for BR

認証事業者と米国のウェブブラウザベンダ等から構成される団体であるCA/ブラウザフォーラムが、SSL 証明書の発行・管理を行う認証局に求められる要件として策定したガイドラインの一つ。

・ WebTrust for CA

米国公認会計士協会（AICPA）及びカナダ勅許会計士協会（CICA）が定めた、認証局の信頼性を保証する制度。

（３） 業務の概要

業務分野:

認証業務

業務内容:

政府認証基盤のブリッジ認証局及び政府共用認証局の維持・運営に係る一連の運用を実施する。業務の概要及び要員の定義は、それぞれの CP/CPS に記載し公表している。

利用者特性:

政府認証基盤の利用者は、証明書利用者と証明書検証者に大別され、それぞれの利用者は府省等の職員及び電子申請等を利用する国民等である。このため、運用に起因したシステム障害の際には、社会的影響が大きなものとなるので、適宜迅速なる判断・対処をもって確実に遂行していくことが必要である。

業務量:

過去の実績においては、発行する証明書は最大2万枚／年、相互認証の実施は最大12 件／年であり、システムの維持及び監視は、24 時間週7日である。ただし、同業務量においては、増加するケースも想定されるため、適宜柔軟に業務量に応じた対応ができるよう体制を構築し取り組む必要がある。

利用者に提供するサービス:

利用者に提供するサービスに係る業務概要及び実施手順は、以下のとおり。

請負業務内容については、「（5）作業内容・納入成果物 ア 作業内容」に示す。

| サービス | 業務概要及び実施手順 |
|---|---|
| 相互認証 | ・ ブリッジ認証局との相互認証を要望する民間認証局等から申請を受理する。<br>・ 相互認証基準を基に書類審査及び技術審査を行う。<br>・ ブリッジ認証局の意思決定機関である行政情報システム関 |

| サービス | 業務概要及び実施手順 |
| --- | --- |
| | 係課長連絡会議の了承を得る。<br>・ 相互認証証明書を相互に発行することで相互認証を実施する。 |
| 認証情報公開サービスの提供 | ・ 統合認証情報公開システムに対し、ブリッジ認証局、政府共用認証局及び商業登記認証局の失効情報等の認証情報を定期的に登録する。<br>・ 上記以外でブリッジ認証局と相互認証している民間認証局等については、相互認証実施時に失効情報等の認証情報の格納箇所(リフェラル)を登録する。<br>・ 府省等が運用する電子申請等システムからのオンラインでの認証情報提供要求に対し、情報を提供する。<br>・ 令和元年度のアクセス件数は、約 1,381 万件。 |
| 証明書検証サービスの提供 | ・ 府省等が運用する電子申請等システムからオンラインで証明書の有効性検証要求を受け付ける。<br>・ 受け付けた要求に対し、認証情報公開サービスの情報等を利用し証明書の有効性を検証する。<br>・ 検証結果を電子申請等システムへオンラインで返答する。<br>・ 令和元年度のアクセス件数は、約 1 億 5,969 万件。 |
| 証明書の発行指示 | ・ 電子申請等システムの利用者で電子証明書(官職証明書、利用者証明書、内部用サーバ証明書)を必要とする各府省の職員は、各府省の府省等登録局(LRA)に対し、証明書の発行依頼を行う。<br>・ LRA は政府共用認証局から提供された LRA システムを利用し、政府共通ネットワーク経由で政府共用認証局に対し証明書の発行指示を行う。 |
| 証明書の発行 | ・ 証明書の発行要求を LRA システムから受け付ける。<br>・ 受け付けた情報を基に証明書を発行する。<br>・ 発行した証明書が証明書ファイル形式の場合は、LRA システムに送付し、LRA システムからダウンロード可能とする。<br>・ 発行した証明書が IC カード形式の場合は、IC カードに証明書を格納するとともに、券面に必要事項を印刷する。 |
| 証明書の発行支援 | ・ 電子申請等システムの利用者で電子証明書(サーバ証明書、コード署名証明書、ドキュメント署名証明書)を必要とする各府省の職員は、各府省の府省等登録局(LRA)に対し、証明書の発行依頼を行う。<br>・ LRA は証明書の発行申請書と発行要求データ(CSR)の内 |

| サービス | 業務概要及び実施手順 |
| --- | --- |
| | 容を確認し、政府認証基盤へ送付する。<br>・ 政府認証基盤は受け付けた情報を基に発行事業者（民間）へ証明書発行を指示する。 |
| 利用者クライアントソフト | ・ 政府共用認証局は、発行したICカード形式の証明書を電子申請等システムの担当者が利用できるようにする利用者クライアントソフトを提供する。<br>・ 各府省の電子申請等システムの担当者は利用者クライアントソフトをPCに導入し、ICカード形式の証明書を利用して電子署名等を行う。 |

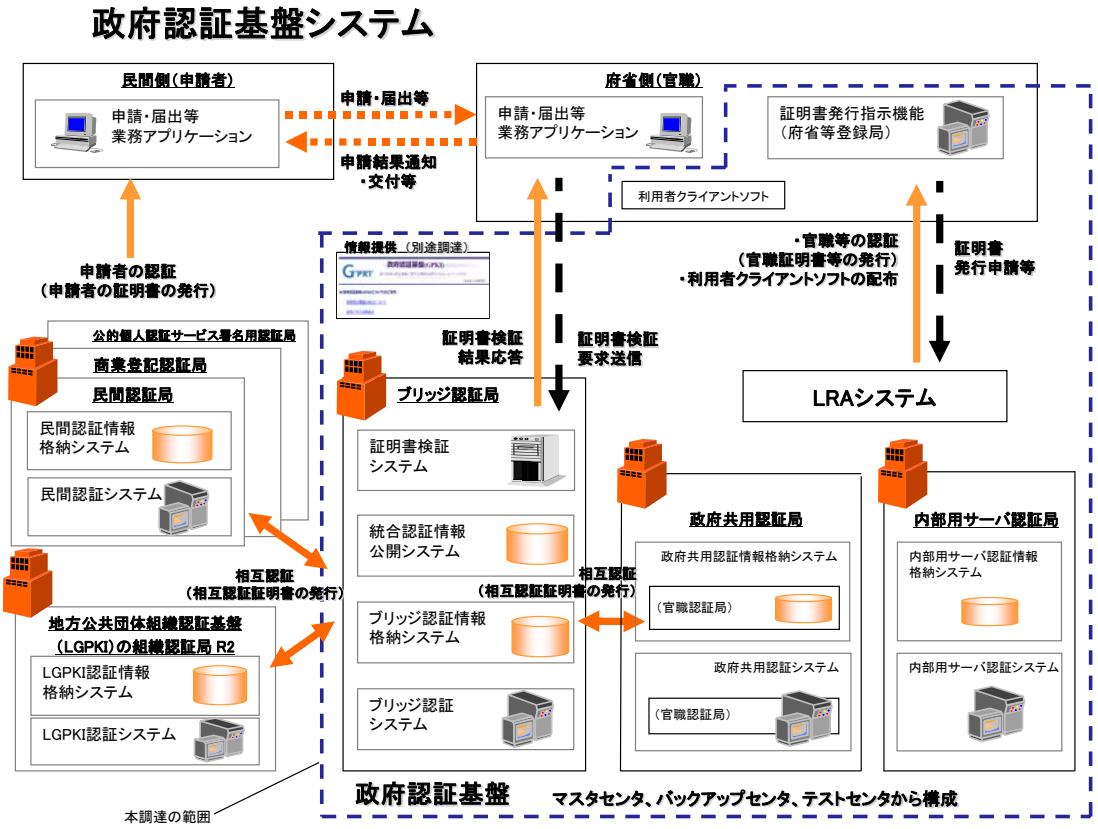
成果指標・目標：

「5　信頼性等要件　（1）信頼性要件」を参照のこと。

（４）運用・保守業務の範囲

本調達の範囲は、下図の「政府認証基盤の調達対象範囲」に係る運用及び保守並びに後述「８　運用要件　(3)運用施設・設備要件」に定める施設・設備である。

なお、政府認証基盤の機器等については、別調達としている。



（５） 作業内容・納入成果物

ア 作業内容

本契約における作業内容を以下に示す。

（ア）政府認証基盤の運用・保守実施計画書の策定

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 運用・保守実施計画書の策定 | ・本契約期間における運用及び保守に係る実施計画書を策定し、行政管理局行政情報システム企画課情報システム管理室政府認証基盤担当（以下「主管係」という。）の承認を得る。<br>・計画書に変更の必要があった場合には、その都度、改定等を行う。 | 契約後早期 |

（イ）政府認証基盤の認証業務及び運用業務

A ブリッジ認証局に係る認証業務

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 自己署名証明書の発行（鍵更新） | ・作業スケジュール及び手順書を作成して、テスト環境を使用したリハーサルを実施する。<br>・IA 鍵管理者（主管係）が実施する鍵生成を支援するとともに、自己署名証明書及びリンク証明書の発行作業を行う。<br>・生成した鍵のバックアップを取得し、マスタセンタへの保管、バックアップセンタへの別地保管を行う。<br>・実施した結果を主管係に報告する。 | ５年に１度<br>（令和6年度予定） |
| 相互認証審査等支援（書類審査） | ・相互認証先認証局から相互認証更新等の申請があった場合、当該認証局が希望する時期に沿うように審査スケジュールを調整する。<br>・当該認証局の CP/CPS や事務取扱要領等から、相互認証基準（運用基準）を満たしていること | 随時<br><br>相手認証局の数：13 認証局 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| | を、あらかじめ定められた審査基準に基づき審査する。<br>・確認したい事項等がある場合には、確認事項一覧としてとりまとめ、主管係に事前相談の上、当該認証局に照会をかけ、回答を得る。<br>・審査結果は、審査結果報告書（案）としてとりまとめ、主管係に報告する。 | 証明書の有効期間：5年 |
| 相互認証審査等支援（技術審査） | ・相互認証先認証局から相互認証更新等の申請があった場合、当該認証局が希望する時期に沿うように審査スケジュールを調整する。<br>・当該認証局が、相互認証基準（技術基準）を満たしていることを確認するためのテスト仕様書、実施手順書を設計・作成する。<br>・作成したテスト仕様書、実施手順書に基づき、テスト環境を用いて審査する。<br>・発行した証明書のプロファイル確認や検証結果を審査結果報告書（案）としてとりまとめ、主管係に報告する。 | 随時<br><br>相手認証局の数：13 認証局<br><br>証明書の有効期間：5年 |
| 相互認証証明書の取り交わし | ・相互認証審査が完了したのち、主管係の指示の下、相互認証の更新等を希望する認証局と取り交わしスケジュールを調整する。<br>・取り交わし手順書を作成して、ブリッジ認証局側と当該認証局で作業内容や作業時間等を調整する。<br>・『相互運用性仕様書 4.3.1.相互認証証明書の発行』で定められた手順に基づき、相互認証証明書の取り交わしを行う。<br>・発行した相互認証証明書をリポジトリに登録する。<br>・実施した結果を主管係に報告する。 | 随時<br><br>相手認証局の数：13 認証局<br><br>証明書の有効期間：5 年 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 相互認証証明書の解消（失効） | ・相互認証先認証局から相互認証失効の申請があった場合、主管係の指示の下、当該認証局と失効日時を調整する。<br>・失効手順書を作成して、ブリッジ認証局側と当該認証局で作業内容や作業時間等を調整する。<br>・作成した手順書に従い、相互認証証明書を失効する。<br>・実施した結果を主管係に報告する。 | 随時 |
| システム運用関連証明書の発行（リポジトリ複製用証明書、CVS 証明書等） | ・作業スケジュール及び手順書を作成して、テスト環境を使用したリハーサルを行う。<br>・手順書に従い、リポジトリ複製用証明書、CVS 証明書、証明書検証サーバ用 SSL 証明書等のシステム運用関連証明書の証明書発行要求を発行する。<br>・官職認証局側で発行したリポジトリ複製用証明書、CVS 証明書、証明書検証サーバ用 SSL 証明書等のシステム運用関連証明書を各サーバに登録する。<br>・実施した結果を主管係に報告する。 | 随時<br><br>各証明の有効期限：5 年 |
| 監査結果報告書の確認（相互認証先認証局） | ・主管係から相互認証先認証局の監査結果報告書を受領して、監査期間、監査人の情報、指摘事項等の内容を確認する。<br>・指摘事項に対しては、鍵の危殆化等の重大な事故が発生していないか、是正措置が適切に講じられているか等、相互認証基準を満たす運用を行っているか確認する。<br>・不明点等が生じた場合には、主管係に事前相談の上、相互認証先認証局に照会をかけ、回答を得る。<br>・実施した結果を主管係に報告する。 | 随時<br><br>相互認証局の数：13 認証局 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| テスト環境用証明書の発行（相互認証証明書、模擬民間 CA の EE 証明書） | ・相互認証を希望する認証局及び各府省からの要望に応じ、テスト環境における相互認証証明書や EE 証明書を発行する。 | 随時<br><br>29 年 3 月～令和 2 年 2 月実績 19 件 |

B 政府共用認証局に係る認証業務

(a) LRAの登録業務

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| LRA の登録業務（券面情報、ドメイン情報等の更新や休日設定含む） | ・主管係から LRA 変更申請書を受領する。<br>・LRA 変更申請書に基づき、登録情報（券面情報、ドメイン情報等）の登録、更新及び削除を手順書に基づき実施する。<br>・また、年次で LRA システムに対して、休日の設定を行う。 | 随時<br><br>29 年 3 月～令和 2 年 2 月実績 143 件 |

(b) 官職認証局に係る認証業務

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 自己署名証明書の発行（鍵更新） | ・作業スケジュール及び手順書を作成して、テスト環境を使用したリハーサルを実施する。<br>・IA 鍵管理者が実施する鍵生成を支援するとともに、自己署名証明書及びリンク証明書の発行作業を行う。<br>・生成した鍵のバックアップを取得し、マスタセンタへの保管、バックアップセンタへの別地保管を行う。<br>・実施した結果を主管係に報告する。 | ５年に１度（令和6年度予定） |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 各種証明書発行（IC カード発行業務） | ・各 LRA からの証明書発行申請を受け、手順書に基づき官職証明書、利用者証明書及び LRA システムへのログイン用カードを発行する。<br>・発行した証明書（IC カード）を封入・封印の上、申請元 LRA へ配達証明により郵送する。 | 日次<br><br>29 年 3 月～令和 2 年 2 月実績 15,838 枚 |
| 相互認証業務（取り交わし） | ・取り交わし手順書を作成して、作業内容や作業時間等を設定して、主管係の承認を得る。<br>・『相互運用性仕様書 4.3.1.相互認証証明書の発行』で定められた手順に基づき、相互認証証明書の取り交わしを行う。<br>・発行した相互認証証明書をリポジトリに登録する。<br>・実施した結果を主管係に報告する。 | ５年に1度<br>（令和6年度予定） |
| システム運用関連証明書の発行（リポジトリ複製用、CVS 証明書等） | ・作業スケジュール及び手順書を作成して、テスト環境を使用したリハーサルを行う。<br>・手順書に従い、リポジトリ複製用証明書、CVS 証明書、証明書検証サーバ用 SSL 証明書等のシステム運用関連証明書を発行する。<br>・実施した結果を主管係に報告する。 | 随時<br><br>各証明書の有効期間：５年 |
| テスト環境用証明書の発行（模擬官職 CA の EE 証明書） | ・相互認証先認証局及び各府省からの要望に応じ、テスト環境における官職証明書や利用者証明書を発行する。 | 随時<br><br>29 年 3 月～令和 2 年 2 月実績 1,066 枚 |

(c) 失効情報の確認

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 失効情報の確認 | ・日々発行される失効情報がリポジトリ上に適切に掲載されていることを定期的に確認する。<br>・適切な失効情報となっていない場合には、主管係に報告する。<br>・相互認証先認証局で失効情報の不備がある場合には、主管係に報告する。<br>・問題ある失効情報の場合には、主管係の指示の下、必要に応じて GPKI ホームページに障害情報として掲載する。<br>・また、失効情報の失効事由が鍵の危殆化によるものか確認し、あった場合には主管係に報告する。 | 日次 |

C 内部用サーバ認証局に係る認証業務

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 自己署名証明書の発行（キーセレモニー） | ・作業スケジュール及びキーセレモニースクリプト（手順書）を作成して、テスト環境を使用したリハーサルを実施する。<br>・作成したキーセレモニースクリプト（手順書）に基づき、サーバ機器を受け入れて、OS、ソフトウェアのインストールから、IA 鍵管理者（主管係）立会いの下、自己署名証明書の発行を行う。<br>・システムフルバックアップを行い、バックアップセンタへの別地保管を行う。<br>・実施した結果を主管係に報告する。 | 設立時<br>（28 年に発行済であり、通常作業としての予定なし。ただし、CA 秘密鍵の危殆化等が発生した場合は、再度作業を行う可能性あり） |
| 内部用サーバ証明書の発行 | ・各府省等 LRA から証明書発行申請書及び証明書発行要求（CSR）を受け取り、予め決められた受付処理を行う。 | 随時 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| | ・証明書発行申請書に基づき、内部用サーバの実在性に係る審査を行う。必要に応じて申請者に意思確認等を行う。<br>・審査完了後、所定の端末からLRAシステムにアクセスし、証明書発行要求（CSR）を基にサーバ証明書の発行指示を行う。<br>・発行したサーバ証明書を各府省等LRAに引き渡す。 | |
| テスト環境用証明書の発行（模擬ISCAのEE証明書） | ・各府省からの要望に応じ、テスト環境における内部用サーバ証明書を発行する。 | 随時 |
| 失効情報の確認 | ・日々発行される失効情報がリポジトリ上に適切に掲載されていることを定期的に確認する。<br>・適切な失効情報となっていない場合には、主管係に報告する。<br>・問題ある失効情報の場合には、主管係の指示の下、必要に応じてGPKIホームページに障害情報として掲載する。<br>・また、失効情報の失効事由が鍵の危殆化によるものか確認し、あった場合には主管係に報告する。 | 日次 |
| 内部監査 | ・内部用サーバ認証局のCP/CPS準拠性に対し、確認するための監査規準を作成する。<br>・監査規準を基に作業記録や台帳等からCP/CPSに準拠した運用がされているか監査する。<br>・監査結果を監査結果報告書としてとりまとめ、主管係に報告する。 | 年次 |

D 照会対応

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| LRA<br>相互認証先認証局<br>電子申請等アプリケーション<br>運営組織側の管理業務支援 | ・各照会元からの問い合わせ（メールや電話）に対し、内容確認をした上で、運用面や技術面の調査等を行う。<br>・調査結果等を基に回答案を作成して、主管係の承認を得る。<br>・主管係による回答案の確認後、照会元に回答を行う。 | 随時 |

E ホームページ作成及び更新

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| ホームページ作成及び更新 | ・主管係等からの依頼（メール等）により、政府認証基盤ホームページ（http://www.gpki.go.jp/）に掲載されているhtmlファイルの作成、変更及び結果確認を行う。<br>・本システムに関する機器、施設、設備等の障害発生時は、必要に応じて当該ホームページに障害内容を掲載する。<br>・相互認証先認証局で障害等が生じた場合には、その状況を当該ホームページに掲載する。<br>・作成及び変更の範囲は静的コンテンツとし、画像を含むすべてのhtml等コンテンツとする。<br>・作成等にあたっては、複数の異なるブラウザを用いて、表示上の問題がないことを確認する。 | 随時<br>29年3月～令和2年2月<br>実績<br>28件 |

F 外部監査対応

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| CP/CPS 準拠性監査の対応 | ・ブリッジ認証局、官職認証局、内部用サーバ認証局の CP/CPS 準拠性に対し、主管係からの指示の下、監査人と監査スケジュールの調整を行う。<br>・監査人からの依頼に基づき、規程類や作業記録等の資料提供依頼に対して、必要に応じて内容を説明する。<br>・監査人からの指摘があった場合は、指摘事項に対してシステムや運用面の改善を図る。 | 年次 |

G 監査ログ検査

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 監査ログ検査（マスタセンタ） | ・各サーバのログイン情報やシステムログ（操作ログ）等を参照して、操作状況を確認する。<br>・操作の記録が見つかった場合には、作業記録から運用責任者からの指示に基づく操作かどうか確認するとともに入退出記録により、各室の入退出記録とのつき合わせを行う。<br>・サーバ機器や端末等のイベントログ、セキュリティログ等を確認して、異常なエラーや警告がないか確認し、ある場合は原因を調査する。<br>・不適切な操作やシステムに対する異常なエラー等が発見された場合には、主管係に報告する。 | 週次 |
| 監査ログ検査（バックアップセンタ） | | 四半期 |

H アーカイブ取得

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| アーカイブの取得 | ・手順に基づき、対象サーバ機器のアーカイブを2式取得する。<br>・アーカイブ媒体の定められた保管場所で管理を行うとともに、アーカイブ媒体一式をバックアップセンタに別地保管する。 | 月次 |

I アーカイブ可読性確認

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| アーカイブの可読性確認 | ・取得したアーカイブ媒体及び各府省認証局閉局時に預かっているアーカイブ媒体について、可読性確認用の端末を用いて、読み込みエラーがなく完了したことを確認する。<br>・なお、定期的に保管期限が切れたアーカイブ媒体を初期化の上、廃棄する。 | 年次<br>29年3月～<br>令和2年2月<br>合計:690枚 |

J 規程類に関する準拠性監査

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 規程類に関する準拠性監査 | ・上位規程(総務省情報セキュリティポリシー等)が変更されているか確認し、変更がある場合には、業務規程及び業務管理マニュアルの内容に不足がないか確認する。<br>・記録書や台帳類を基に、業務規程及び業務管理マニュアルの内容に沿った運用をしているかサンプリングにより確認する。<br>・適切ではない運用をしている場合には、重要度に応じて主管係に報告するとともに、運用の改善を図る。 | 年次 |

K LRA研修

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| LRA 研修 | ・各府省等 LRA 要員向けに教育教材（GPKI の概要、LRA の業務概要、IC カード概要、操作演習資料）を作成する。<br>・研修場所の環境に対して、操作演習ができるようにソフトウェアのセットアップを事前に実施するとともに、研修当日に使用する申請データを作成する。<br>・各教育教材に従って、各府省等 LRA 要員向けに説明する。<br>・研修後に各府省等 LRA 要員から意見や改善提案等があった場合は、次回の LRA 研修に反映するよう教育教材等を改定する。 | 年2回 |

L 教育・訓練

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 危機管理訓練（事業継続計画） | ・予め想定された危機に対して、マニュアルで示されている対応手順が適切であるかどうかを、訓練の実施を通して有効性を確認する。また、マニュアルに示されていない危機であっても、必要に応じて訓練を実施し、必要性を確認する。<br>・加えて、災害が発生して、公共交通機関が不通である場合を想定して、自宅から各センターに参集して、システムの稼働状況を確認する訓練を行う。<br>・有効性及び必要性を確認した結果、マニュアル等の不備や課題がある場合には、適宜マニュアルの作成及び修正を行う。<br>・実施した結果を主管係に報告する。 | 年次 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 運用要員教育 | ・認証局の要員へのセキュリティに関する意識を向上させるための教育・研修に関する方針・計画の策定を行う。<br>・運用要員教育に使用する教育教材（情報セキュリティ対策、緊急時の一次対処）を作成して全運用員に対して実施するとともに、１年間の業務に携わった振り返りとして自己点検を実施する。<br>・自己点検の内容を基に、運用責任者は面談を行い、主管係に教育実施結果を報告する。 | 年次 |

M テスト環境の維持

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| テスト環境の維持 | ・テスト環境の利用を希望する組織の要望に応じて、リフェラルの設定等の環境を整備する。<br>・また、必要に応じて利用時間外は物理的にインターネットから遮断する。 | 随時 |

N 書類改定（上位規程、業務規程、業務管理マニュアル）

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 書類改定（上位規程、業務規程、業務管理マニュアル） | ・監査人からの指摘事項やシステム変更を契機として、必要に応じて CP/CPS、相互認証基準、相互運用性仕様書等の修正案を作成し、主管係の了承を得る。<br>・各種規程・マニュアルの変更に伴い、各種様式の変更が必要な場合は、併せて修正する。 | 随時 |

○ サーバ証明書等の発行支援

請負事業者は、WebTrust for CA及びWebTrust for BRの認定を取得した発行事業者（民間）からサーバ証明書、コード署名証明書、ドキュメント署名証明書の発行を受ける発行支援の作業を行うこと。

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| サーバ証明書の発行支援 | ・各府省等 LRA から証明書発行申請書及び証明書発行要求（CSR）を受け取り、予め決められた受付処理を行う。<br>・証明書発行申請書に基づき、サーバの実在性に係る審査を行う。必要に応じて申請者に意思確認等を行う。<br>・審査完了後、所定の端末から発行事業者（民間）が提供する発行管理システムにアクセスし、証明書発行申請書及び証明書発行要求（CSR）に基づくサーバ証明書の発行申請を行う。<br>・発行事業者で発行されたサーバ証明書を発行管理システムからダウンロード等で取得し、各府省等 LRA に引き渡す。 | 随時 |
| コード署名証明書の発行支援 | ・各府省等 LRA から証明書発行申請書及び証明書発行要求（CSR）を受け取り、予め決められた受付処理を行う。<br>・証明書発行申請書に基づき、組織の実在性に係る審査を行う。必要に応じて申請者に意思確認等を行う。<br>・審査完了後、所定の端末から発行事業者（民間）が提供する発行管理窓口へ、証明書発行申請書及び証明書発行要求（CSR）に基づくコード署名証明書の発行申請を行う。<br>・発行事業者で発行されたコード署名証明書を安全にダウンロード等で取得し、各府省等 LRA に引き渡す。 | 随時 |
| ドキュメント署名証明書の発行支援 | ・各府省等 LRA から証明書発行申請書及び証明書発行要求（CSR）を受け取り、予め決められた受付処理を行う。<br>・証明書発行申請書に基づき、組織の実在性に係る審査を行う。必要に応じて申請者に意思確認 | 随時 |

| 作業項目 | 作業内容 | 頻度・タイミング |
| --- | --- | --- |
| | 等を行う。<br>・審査完了後、所定の端末から発行事業者（民間）が提供する発行管理システムにアクセスし、証明書発行申請書及び証明書発行要求（CSR）に基づくドキュメント署名証明書の発行申請を行う。<br>・発行事業者で発行されたドキュメント署名証明書を発行管理システムからダウンロード等で取得し、各府省等 LRA に引き渡す。 | |

（ウ） 政府認証基盤システムの運用業務

A 運用・保守管理業務

(a) セキュリティ管理

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| セキュリティ実施手順書 | ・総務省情報セキュリティポリシー、情報セキュリティ技術の進歩及びその他リスクの変化に対して、現状の運用やシステムの対応状況を分析して評価する。<br>・本評価により各種規程・マニュアルの変更が必要な場合には、主管係と調整の上、変更作業を実施する。 | 年次 |
| ウィルスパターンファイルの適用 | ・システムで使用しているウィルス対策ソフトウェアのパターンファイルが更新されている場合には、速やかに入手してテスト環境で動作を確認する。<br>・動作を確認した後、マスタセンタ及びバックアップセンタの各本番機器に適用する。 | 月次 |
| ファイアウォールアクセス制御管理 | ・証明書検証サーバ及び LRA システムに接続する各府省から、アクセス元の追加／削除等の依頼が発生した場合には、依頼内容に問題がないことを確認し、アクセス制御の変更作業を行う。 | 随時 |
| セキュリティ情報の収集 | ・市販されている脆弱性情報等を定期的に収集し、対象となるセキュリティ情報をシステム予防保守に引き渡す。<br>・脆弱性情報を保管管理する。 | 日次 |
| 脆弱性診断 | ・本システムが使用している OS 及びソフトウェア | 四半期<br>随時 |

| 作業項目 | 作業内容 | 頻度・タイミング |
|---|---|---|
| | に対して、脆弱性検査ツール等を使用して擬似攻撃を行うことで脆弱性の有無を診断する。<br>・セキュリティ診断に際しては、インターネット経由及び内部ネットワーク経由の 2 種類の方法で行う。<br>・診断結果を報告書にとりまとめ、システム予防保守に引き渡し、システム予防保守完了後、必要に応じて、再度セキュリティ診断を行う。<br>・診断結果の報告書を保管管理する。 | |

(b) インシデント管理

| 作業項目 | 作業内容 | 頻度・タイミング |
|---|---|---|
| 障害記録書起票 | ・システムに障害が発生した場合や、システム予防保守で対策が必要と判断された場合には、障害記録書を起票する。<br>・月次報告書の資料となる障害・案件一覧を作成する。 | 随時 |
| 障害管理（フォローアップ） | ・障害記録書で起票した案件について、定期的にフォローアップして対応状況を管理する。<br>・月次報告書の資料となる障害・案件一覧を更新する。 | 月次 |

(c) 変更管理

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| アカウント情報の管理(アカウントレビュー含む) | ・アカウント情報に関する管理台帳の内容を確認する。<br>・管理台帳の内容と各サーバ機器のアカウント設定内容の突き合わせを行い、誤りがないか確認する。<br>・また、新しい運用員が着任した時や離任した時には、管理台帳の更新を行う。 | 四半期 |
| ファイアウォールのアクセス制御定期確認 | ・ファイアウォール機器の設定内容を確認して、設計書(設定書)の内容と突き合わせを行い、誤りがないか確認する。<br>・また、ファイアウォールのアクセス制御だけではなくGPKIドメインのWhoisデータベース情報も対象として定期確認を行う。 | 半期 |
| ハードウェアの棚卸し確認 | ・ハードウェア管理台帳の内容を基に、設置しているハードウェアの状況を確認し、台帳の記載誤りや、ハードウェアの欠損等がないか確認する。 | 年次 |
| ソフトウェアの棚卸し確認 | ・ソフトウェア管理台帳の内容を基に、保管しているソフトウェア媒体を確認し、台帳の記載誤りや、ソフトウェア媒体の欠損等がないか確認する。<br>・ソフトウェア管理台帳の内容を基に、導入ソフトウェアに過不足等がないか、導入しているソフトウェアのバージョンに誤りがないか確認する。 | 年次 |
| 書類・媒体の廃棄 | ・保管期間の過ぎた書類やバックアップ等の媒体を抽出する。 | 年次 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| | ・抽出した書類やバックアップ等の媒体は、復元不可能な状態とし、廃棄する。（書類はシュレッダ、バックアップ等の媒体は裁断等を行う。） | |

(d) リリース管理

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 作業計画書、報告書の確認 | ・システム障害保守及び予防保守で、必要な業務資源（プログラム、アプリケーションのパラメータファイル、DB の設定等）に対して修正、検証、適用等を行う際に、事前にシステム保守で作成される作業計画書の内容を確認する。<br>・システム保守で作成される作業報告書の内容を確認して、定期的な報告会で主管係に最終的な報告をする。 | 随時 |

B 監視業務

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 機器の稼働状況監視 | ・監視装置が通知するアラート情報を監視し、予め定める手順に従い、対処する。<br>・また、休日・夜間の相互認証先認証局からの連絡窓口となり、連絡を行う。 | 24 時間 |
| 不正アクセス監視 | ・監視装置が通知する不正アクセス情報を監視し、予め定める手順に従い、対処する。<br>・不正アクセス等の状況とりまとめを日次行う。 | 24 時間 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| 定常処理の結果確認 | ・システムとして自動化されているバッチ処理等の結果を確認して、問題がある場合には、予め定める手順に従い、連絡・対処・報告を行う。重要度監視業務に関する報告書を作成する。<br>・また、各サーバの日次バックアップ結果の確認やLRAシステム申請処理件数の確認を日次で行う。 | 日次<br><br>確認件数:約30項目／日 |

C 定常業務

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| バックアップデータに係る管理（マスタセンタ） | ・バックアップデータの管理台帳から日次でデータバックアップを取得している対象機器を確認する。<br>・世代管理されているバックアップのデータのうち、対象となる機器全てについて、バックアップのデータが取得できていること、及び世代管理が正しく行われていることをNASの動作ログ、バックアップデータの格納状態によって確認する。<br>・バックアップデータの管理台帳を更新する。 | 週次 |
| バックアップデータに係る管理（バックアップセンタ） | | 月次 |
| フルバックアップの取得 | ・認証局システムの機器を対象として、月次でフルバックアップデータを正・副2式取得する。<br>・取得したフルバックアップデータ（正）を予備機にリストアし、フルバックアップデータ（副）は、バックアップセンタに移送した上で予備機にリストアする。<br>・取得したフルバックアップデータを保管管理し、管理台帳を更新する。 | 月次 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| リソース使用状況の情報取得及び集計 | ・LRA 申請受付サーバ、リポジトリサーバ及び証明書検証サーバに関するリソースの使用状況を収集及び集計して、サーバ機器の増設及び増強の必要性を分析する。<br>・政府共通ネットワーク及びインターネットの回線使用状況についても、収集及び集計し、回線増強の必要性を分析する。 | 週次 |
| パスワード変更管理 | ・管理台帳から、定められた変更周期を踏まえ、パスワード変更となるアカウントを抽出する。<br>・抽出したアカウントに対して、パスワードの管理票を作成する。<br>・パスワードの管理票に基づき、実施者と確認者の複数人によりパスワードを変更し、管理台帳を更新する。<br>・変更したパスワードを封入・封印の上、あらかじめ定められた場所に保管する。 | 週次 |
| アクセス件数等統計処理の収集及び集計（CVS、公開リポジトリ） | ・リポジトリサーバや証明書検証サーバで保管されている各種ログ情報等を収集して、それぞれのサーバに対するアクセス件数を集計する。<br>・また、障害等発生時には、必要に応じてトラブルシューティングのための解析を行う。 | 月次 |
| CA 秘密鍵の可読性確認支援 | ・保管管理されている CA 秘密鍵のバックアップ媒体に対して、可読性を確認する。<br>・なお、可読性確認の操作は IA 鍵管理者（主管係）で実施するため、当該作業の支援を行う。 | 年次 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| CVS 秘密鍵の可読性確認 | ・保管管理されている CVS 秘密鍵のバックアップ媒体に対して、可読性を確認する。 | 年次 |

D 非定常業務

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| システム障害対応 | ・本システムの障害発生時には、問題の切り分け、応急措置、情報収集、主管係・システム保守員・機器ベンダへの連絡・調整、修復後の確認等を行う。<br>・応急措置を行うにあたって、システム保守員が必要な場合は、システム保守員と連携して作業を行う。<br>・システムの障害発生時には、現象を把握して、利用者への影響範囲を最小化するための暫定的な一時対処を行う。<br>・必要に応じて、利用者への影響度合いを確認するため、アクセス元の解析等を行う。 | 随時<br><br>29 年 3 月～<br>令和 2 年 2 月<br>実績<br>18 件 |
| 障害対応時のマシン室立会い | ・システム障害保守及び予防保守によるマシン室での作業が発生する時には、運用権限のある運用員がマシン室への入退室、作業の立会い等の作業監督を行い、主管係に作業開始／終了を報告する。 | 随時 |
| 書類改定（システム運用マニュアル、操作マニュアル） | ・運用やシステムが変更となり、システム運用マニュアル及び操作マニュアルに修正が必要な場合は、対象マニュアルの修正案を作成し、主管係の了承を得る。<br>・また、各種様式の変更が必要な場合は、あわせて修正する。 | 随時 |
| 機器等更改に伴うデータ移行 | ・令和4年2月に機器等の更改を予定しているため、現行運用で使用しているブリッジ認証局、官職認証局の CA 秘密鍵及び認証局データを新しい機器上で継続的に稼働できるようにデータ移行 | 機器等の更改時 |

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| | 作業を実施する。 | |
| 保守交換済み旧HDD 等記憶媒体管理 | ・システム障害保守及び予防保守によって交換を行った旧 HDD 等記憶媒体に格納されていた情報を復元できないように情報消去し、作業記録に記録する。<br>・情報消去した旧 HDD を保管管理台帳に記録し、契約期間中は施錠可能な保管庫に保管する。<br>・旧 HDD 等記録媒体の保管状況を年1回確認する。 | 随時 |

（エ） 政府認証基盤システムの保守業務

| 作業項目 | 作業内容 | 頻度・ﾀｲﾐﾝｸﾞ |
|---|---|---|
| システム保守管理 | ・「インシデント管理（障害、問い合わせへの対応内容等の管理）」、「変更管理（システムに変更が生じる場合の変更手順等の管理）」及び「リリース管理（システムの本番環境に変更を加えたアプリケーションを適用する場合の手順等の管理）」を除く、システム保守として必要となる管理を行い、定期・不定期に主管係に報告を行う。 | 随時 |
| システム障害保守 | ・本システムの障害発生時には、運用員からの連絡を受け、システムの障害原因の調査を行い、必要な業務資源（プログラム、アプリケーションのパラメータファイル、DB の設定等）に対して修正、検証、適用等の本格的な対処を行う。<br>・必要に応じて、利用者への影響度合いを確認するため、アクセス元の解析等を行う。 | 随時<br>29 年 3 月～令和 2 年 2 月<br>実績<br>18 件 |

| 作業項目 | 作業内容 | 頻度・<br>ﾀｲﾐﾝｸﾞ |
|---|---|---|
| システム予防保守 | ・「4 規模・性能要件 (1) 規模要件 表4-1機器一覧」に掲載している機器を構成するソフトウェアの管理とそれらに対する脆弱性情報を定期的に収集し、脆弱性の有無について主管係に報告する。<br>・脆弱性が確認された場合、対応の要否を判断するための支援を主管係に対して行う。対応を必要と判断した場合、作業手順の検討と付随する準備、調整及びソフトウェアの適用作業を行う。<br>・作業完了の後、作業報告書の作成を行う。<br>・なお、本作業の実施に当たり、作業対象のソフトウェア以外のソフトウェアに変更等影響が発生する場合、別途主管係と協議を行う。 | 随時<br><br>29 年 3 月～<br>令和 2 年 2 月<br>実績<br>調査:5,821 件<br>適用:31 件 |
| 利用者環境の維持 | ・利用者環境を構成する OS、ブラウザ及び JRE のマイナーバージョンアップに伴う検証を必要に応じて行う。<br>・マイナーバージョンアップ情報を収集して、リリースされている場合には、動作検証スケジュールを作成し、主管係に報告する。<br>・動作検証の環境を構築して動作検証を行い、問題がない場合には、動作確認リストを更新し主管係に報告する。動作検証の結果に問題がある場合には、対応策を検討して別途主管係と協議する。<br>・なお、マイナーバージョンアップに伴い、政府認証基盤で独自に開発したソフトウェア、「4 規模・性能要件 (1) 規模要件 表4-1機器一覧」に掲載している機器を構成するソフトウェアに変更が必要となる場合は、別途主管係と協議を行う。 | 随時<br><br>29 年 3 月～<br>令和 2 年 2 月<br>実績<br>55 件 |
| | ・LRA 端末環境について OS、ブラウザのマイナー | 月次 |

| 作業項目 | 作業内容 | 頻度・タイミング |
| --- | --- | --- |
| | バージョンアップに伴う動作確認を定期的に行う。<br>・OS、ブラウザのマイナーバージョンアップ情報を収集して、リリースされている場合には、動作確認を行う旨を主管係に報告し、動作確認を行う。<br>・動作確認の結果を主管係に報告する。<br>・なお、マイナーバージョンアップに伴い、政府認証基盤で独自に開発した LRA システムのソフトウェア、「4 規模・性能要件 (1) 規模要件 表4-1 機器一覧」に掲載している機器に変更が必要となる場合は、別途主管係と協議を行う。 | |

（オ） 認証局施設・設備の管理業務

| 作業項目 | 作業内容 | 頻度・タイミング |
| --- | --- | --- |
| 施設・室に関する管理 | ・運用要員等の変更がある場合に、各室（セキュア室、関連サーバ室、操作室、ネットワーク室、監視室、事務室、テストセンタ及びバックアップセンタ各室）への入室に対する生体認証の登録、変更及び削除作業を行う。<br>・定期的に登録されている入室権限に誤りがないことを確認する。<br>・各室で保存されている入退室記録等を定期的（マスタセンタ：週次、バックアップセンタ：月次）に記録媒体に移動して、保管・管理する。<br>・施設で障害が発生した場合には、主管係へ報告した上で、問題の切り分け、応急措置、情報収集及び修復作業を行う。 | 随時 |
| 設備、備品等に関する管理（回線、電気設備、空調設備等） | ・生体認証装置、ガス消化システム、消防施設、湿度調整器、全熱交換機、空調機等について、維持・管理を行うとともに、必要に応じ、これらの | 随時 |

| 作業項目 | 作業内容 | 頻度・タイミング |
|---|---|---|
| | 定期的な点検を行う。<br>・金庫や保管庫で管理しているパスワード等の保管物や、ハードウェア、ソフトウェア等の備品を適切に保管し、定期的（年次）に棚卸しを行う。<br>・金庫、保管庫等の物理鍵を適切に保管し、定期的（年次）に棚卸しを行う。<br>・施設内の設備で障害が発生した場合には、主管係へ報告した上で、問題の切り分け、応急措置、情報収集及び修復作業を行う。 | |

（カ） 報告書の作成

| 作業項目 | 作業内容 | 頻度・タイミング |
|---|---|---|
| 月次報告書の作成 | ・本システムの運用状況、作業状況、障害発生対応状況等を、定められた報告書としてとりまとめる。<br>・報告書の種類は、進捗管理報告書、運用報告書、課題管理台帳、タスクチャート、アクセス状況一覧、監視報告書、相互認証状況一覧、CVS・リポジトリアクセス状況、月間作業一覧、月間作業スケジュール、年間作業一覧、サービス指標実績値、ヘルプデスク運用状況、教育訓練実施状況、障害・案件一覧及び個別障害対応報告書から構成する。<br>・報告書の作成に当たっては、別途調達される機器等の借入業者と定期的に会議を設けて、障害発生の対応状況の確認を行う。 | 月次 |
| 月次報告書の報告 | ・作成した運用状況、作業状況、障害発生対応状況等の各種報告書を用いて、主管係に運用状況等の報告を行う。 | 月次 |

イ　作業実施期間

令和4年2月1日（火）から令和8年1月 31 日（土）まで。

ただし、令和3年 10 月1日（金）から令和4年1月 31 日（月）までは、運用を行う施設・設備の移設及びシステム更改への対応等、運用準備を行うこと。

施設・設備の移設及びシステム更改への対応については、「8 運用要件定義 （3）運用施設・設備要件」を参照。

ウ　作業実施日

「行政機関の休日に関する法律（昭和 63 年法律第 91 号）」に規定する行政機関の休日を除く日。

ただし、主管係から業務上の指示があるときは、これに従うこと。

なお、監視業務については、作業実施期間における全日とする。

エ　作業時間

（ア） 運用要員

- 運用責任者補佐1名、上級 IA 操作員1名以上
  午前8時 30 分から午後5時 30 分まで（休憩時間は別途協議）
- 上記以外の運用要員
  午前9時 30 分から午後6時 30 分まで（休憩時間は別途協議）
- 監視員
  2名、2交代又は3交代にて 24 時間（休憩時間は別途協議）
- 上記以外の運用要員
  午前9時 30 分から午後6時 30 分まで（休憩時間は別途協議）

（イ） 保守要員

「5 信頼性等要件 （1）信頼性要件」に示すサービスの停止を伴う場合、24 時間週7日対応とする。

なお、上記以外は、原則午前9時 30 分から午後6時 30 分まで（休憩時間は別途協議）とする。

ただし、主管係から業務上の指示があるときは、これに従うこと。

オ　納入成果物

次の文書の電子データ（CD-R）（PDF 形式を含む各一式）を納入する。

| 納入成果物 | 納入期限 |
|---|---|
| ・実施計画書<br>（本請負業務に係るスケジュール、体制、管理方針等の計画書） | 令和4年2月 10 日 |
| ・運用状況報告書<br>（進捗管理報告書、運用報告書、課題管理台帳、タスクチャート、アクセス状況一覧、監視報告書、相互認証状況一覧、CVS・リポジトリアクセス状況、月間作業一覧、月間作業スケジュール、年間作業一覧、サービス指標実績値、ヘルプデスク運用状況、教育訓練実施状況　等） | 月ごとに報告書を作成し、翌月の第２木曜日までに納入（計画等については、適宜見直しを行う） |
| ・障害発生対応状況報告書<br>（障害・案件一覧、個別障害対応報告書　等）<br>・予防保守等に係る調査報告書 | 月ごとに報告書を作成し、翌月の第２木曜日までに納入 |
| ・保守作業計画書<br>・保守作業報告書 | 作業前に保守作業計画書を作成し、月ごとの保守作業報告書を翌月の第２木曜日までに納入 |
| ・各種規程・マニュアル等ドキュメント（更新履歴書含む）の最新版 | 修正の都度速やかに納入し、最終版を令和８年１月 30 日に納入 |

## 3 情報システムの要件

政府認証基盤は、ブリッジ認証局と政府共用認証局から構成され、マスタセンタ、バックアップセンタ及びテストセンタに配置されている。

### （１） ブリッジ認証局

ブリッジ認証局は、ブリッジ認証システム、リポジトリ（ブリッジ認証情報格納システム、統合認証情報公開システム）、証明書検証システム等から構成されている。

また、ブリッジ認証局は、官職認証局、公的個人認証サービス（JPKI）、地方公共団体組織認証基盤（LGPKI）、商業登記認証局及び民間認証局と取り交わす相互認証証明書の発行を行っている。

リポジトリは、ブリッジ認証局に関する認証情報（自己署名証明書、リンク証明書、相互認証証明書（ペア）及び証明書失効情報）は、インターネット向け及び政府共通ネットワーク向けに公開を行っている。

証明書検証システムは、官職認証局をトラストアンカとする署名検証者に対して、政府共用証明書検証サーバによる証明書検証機能の提供を行っている。

### （２） 政府共用認証局

政府共用認証局は、LRA システム及び IC カードシステムを含む政府共用認証システム及び政府共用認証情報格納システム等から構成されている。

さらに、政府共用認証局は、官職認証局から構成されている。

官職認証局は、電子申請・届出等の手続に利用する各府省の官職証明書、利用者証明書、情報提供ネットワークで使用する暗号通信用等証明書及び政府共用証明書検証サーバに対して証明書を発行している。

官職認証局から発行する官職証明書又は利用者証明書の IC カードは、「公的分野における連携 IC カードの実現に向けた基本的考え方」（平成 13 年7月 27 日 公的分野における IC カードの普及に関する関係府省連絡会議）[3]等を踏まえた仕様とする。カードインタフェースは、非接触・接触両インタフェースを有するコンビ型を必須とする。

また、政府共用認証局を構成する認証局ではないが、各府省が運営している業務システム等で必要とする内部用のサーバ証明書を発行するための内部用サーバ認証局がある。内部用サーバ認証局は、政府認証基盤を構成する認証局と同様の認証業務及び運用業務を行う。

LRA システムは、府省等登録局（LRA）に所属する職員のみ利用可能とする。府省等登録局（LRA）は令和2年4月現在、26 府省等が設置されており、官職認証局が発行する官職証明書、利用者証明書及び暗号化通信用等証明書の発行申請、及び内部用サーバ CA が発行する内部用サーバ証明書の発行申請を行う。

なお、平成30年4月をもって終了したアプリケーション認証局に係る認証業務は、平成30 年5月以降民間の発行事業者から証明書等を政府認証基盤が取りまとめて取得する

[3] http://www.kantei.go.jp/jp/singi/it2/others/kihon.pdf

業務に変更し、サーバ証明書、コード署名証明書、ドキュメント署名証明書の発行支援業務に切り替えを行った。

本件の対象となる情報システムの詳細は、別途閲覧に供する以下の仕様書及び参照資料1「政府認証基盤　セキュリティ要件」を参照。

- 構築仕様書（ブリッジCA編）
- 構築仕様書（官職CA編）
- 構築仕様書（内部用サーバCA編）
- 構築仕様書（ネットワーク編）
- LRAシステム基本設計書
- ICカードシステム仕様書
- LRA業務管理・システム運用マニュアル
- 証明書申請の手引き

## 4 規模・性能要件

### （１）規模要件

政府認証基盤は、マスタセンタ、バックアップセンタ及びテストセンタから構成する。

政府認証基盤では、インターネットや政府共通ネットワークに向けて、証明書の発行、証明書情報の公開及び証明書の検証に係わるサービスを提供する。マスタセンタには、これらを実現する上で必要となる機能をすべて設置している。これに対してバックアップセンタは、マスタセンタの予期せぬ障害に備え、性能、可用性を除き、サービス継続を行うためのみに必要な機能を保有する。

また、テストセンタは、本番環境のシステムの維持、相互認証の際の接続試験、証明書を利用したアプリケーションの評価テスト等を行うため、必要に応じて、インターネットや政府共通ネットワークに向けて、テスト環境を提供する機能を保有する。

システム更改の対象としている現行のシステムの機器一覧を「表4−1　機器一覧」に示す。

表 4-1 機器一覧

（凡例　MC：マスタセンタ、BC:バックアップセンタ、TC：テストセンタ、JM：事務システム）

| | 機器名 | 数量 | | | | |
|---|---|---|---|---|---|---|
| | | 合計 | 設置場所 | | | |
| | | | MC | BC | TC | JM |
| １．サーバ | | | | | | |
| (1) | CA/ディレクトリサーバ(BCA) | 4 | 2 | 1 | 1 | 0 |
| (2) | CA/ディレクトリサーバ(官職 CA) | 4 | 2 | 1 | 1 | 0 |
| (3) | CA/ディレクトリサーバ(内部用サーバ CA) | 1 | 1 | 0 | 0 | 0 |
| (4) | CA/ディレクトリサーバ(民間) | 1 | 0 | 0 | 1 | 0 |
| (5) | ハードウェアセキュリティモジュール(A) | 4 | 2 | 1 | 1 | 0 |
| (6) | ハードウェアセキュリティモジュール(B) | 4 | 2 | 1 | 1 | 0 |
| (7) | ハードウェアセキュリティモジュール(C) | 6 | 4 | 1 | 1 | 0 |
| (8) | 統合リポジトリサーバ | 6 | 2 | 2 | 2 | 0 |
| (9) | 公開リポジトリサーバ | 8 | 4 | 2 | 2 | 0 |
| (10) | ディスクアレイ装置(A) | 8 | 4 | 2 | 2 | 0 |
| (11) | ディスクアレイ装置(B) | 3 | 1 | 1 | 1 | 0 |
| (12) | 政府共用証明書検証サーバ | 6 | 4 | 1 | 1 | 0 |
| (13) | 申請管理 DB サーバ | 6 | 2 | 2 | 2 | 0 |
| (14) | 申請管理サーバ | 3 | 1 | 1 | 1 | 0 |
| (15) | 申請受付サーバ | 4 | 2 | 1 | 1 | 0 |
| (16) | DNS サーバ | 4 | 2 | 1 | 1 | 0 |
| (17) | FTP サーバ | 3 | 0 | 2 | 1 | 0 |
| (18) | ログ収集サーバ | 2 | 2 | 0 | 0 | 0 |
| (19) | ファイアウォール管理サーバ | 7 | 3 | 2 | 2 | 0 |
| (20) | 監視サーバ | 6 | 2 | 2 | 2 | 0 |
| (21) | ファイルサーバ | 1 | 0 | 0 | 0 | 1 |
| ２．端末 | | | | | | |
| (1) | CA 操作端末(BCA) | 4 | 2 | 1 | 1 | 0 |
| (2) | CA 操作端末(政府共用 CA) | 2 | 1 | 1 | 0 | 0 |
| (3) | CA 操作端末(民間) | 1 | 0 | 0 | 1 | 0 |
| (4) | 運用操作員登録端末 | 3 | 2 | 1 | 0 | 0 |
| (5) | 証明書検証サーバ操作端末 | 4 | 2 | 1 | 1 | 0 |
| (6) | FTP 端末 | 4 | 3 | 0 | 1 | 0 |
| (7) | SSH 端末 | 3 | 1 | 1 | 1 | 0 |
| (8) | 監視端末 | 3 | 2 | 0 | 1 | 0 |

（凡例　MC：マスタセンタ、BC:バックアップセンタ、TC：テストセンタ、JM：事務システム）

| | 機器名 | 数量 | | | | |
|---|---|---|---|---|---|---|
| | | 合計 | 設置場所 | | | |
| | | | MC | BC | TC | JM |
| (9) | アラート解析レスポンス測定端末 | 2 | 2 | 0 | 0 | 0 |
| (10) | ファイアウォール設定端末 | 6 | 4 | 2 | 0 | 0 |
| (11) | ファイアウォール操作端末兼ネットワークベース IDS 監視端末 | 4 | 2 | 1 | 1 | 0 |
| (12) | エンドエンティティ端末(A) | 1 | 0 | 0 | 1 | 0 |
| (13) | エンドエンティティ端末(B) | 1 | 0 | 0 | 1 | 0 |
| (14) | 運用員用端末(A) | 20 | 0 | 0 | 0 | 20 |
| (15) | 運用員用端末(B) | 1 | 0 | 0 | 0 | 1 |
| (16) | 運用員用端末(C) | 1 | 0 | 0 | 0 | 1 |
| ３．IC カード関連機器 | | | | | | |
| (1) | IC カード発行機 | 4 | 2 | 1 | 1 | 0 |
| (2) | IC カード関連ソフト開発機 | 1 | 0 | 0 | 1 | 0 |
| (3) | IC カード確認端末 | 1 | 0 | 0 | 1 | 0 |
| ４．ネットワーク | | | | | | |
| (1) | L2 スイッチ(A) | 16 | 10 | 4 | 2 | 0 |
| (2) | L2 スイッチ(B) | 23 | 14 | 8 | 1 | 0 |
| (3) | L2 スイッチ(C) | 1 | 0 | 0 | 1 | 0 |
| (4) | 事務室 L2 スイッチ | 2 | 0 | 0 | 0 | 2 |
| (5) | L3 スイッチ | 5 | 3 | 1 | 1 | 0 |
| (6) | 事務室 L3 スイッチ | 1 | 0 | 0 | 0 | 1 |
| (7) | VPN 装置 | 9 | 4 | 2 | 3 | 0 |
| (8) | 負荷分散装置 | 5 | 2 | 1 | 2 | 0 |
| (9) | ファイアウォール(A) | 13 | 8 | 3 | 2 | 0 |
| (10) | ファイアウォール(B) | 4 | 2 | 1 | 1 | 0 |
| (11) | ファイアウォール(事務システム) | 1 | 0 | 0 | 0 | 1 |
| (12) | ネットワークベース IDS(A) | 2 | 2 | 0 | 0 | 0 |
| (13) | ネットワークベース IDS(B) | 2 | 0 | 1 | 1 | 0 |
| (14) | ルータ(A) | 4 | 3 | 1 | 0 | 0 |
| (15) | ルータ(B) | 4 | 3 | 1 | 0 | 0 |
| (16) | ブリッジ接続装置 | 2 | 0 | 0 | 2 | 0 |
| (17) | 事務システム回線等 | 1 | 0 | 0 | 0 | 1 |

（凡例　MC：マスタセンタ、BC:バックアップセンタ、TC：テストセンタ、JM：事務システム）

| | 機器名 | 数量 | | | | |
|---|---|---|---|---|---|---|
| | | 合計 | 設置場所 | | | |
| | | | MC | BC | TC | JM |
| ５．その他 | | | | | | |
| (1) | ディスククラッシャ | 2 | 0 | 1 | 1 | 0 |
| (2) | シュレッダ | 1 | 0 | 0 | 0 | 1 |
| (3) | マルチシュレッダ | 2 | 0 | 1 | 0 | 1 |
| (4) | プリンタ | 11 | 5 | 4 | 2 | 0 |
| (5) | カラープリンタ・コピー複合機 | 1 | 0 | 0 | 0 | 1 |
| (6) | IC カード | 20,000 | | | | |

詳細は、別途閲覧に供する以下の資料を参照。

- 構築仕様書（ブリッジCA編）
- 構築仕様書（官職CA編）
- 構築仕様書（内部用サーバCA編）
- 構築仕様書（ネットワーク編）

（２）性能要件

「５ 信頼性等要件 （1）信頼性要件」の評価項目と目標値 の応答時間を参照。

## 5 信頼性等要件

### （１）信頼性要件

政府認証基盤では SLA(Service Level Agreement)を導入し、政府認証基盤のサービスの内容、範囲、提供状況を測定・分析可能な単位で明確に規定し、目指すべき目標値の達成状況を管理することで、サービス品質の確保及び維持・改善を行っている。

国民等、府省等利用機関に向けた各サービスに関するサービスレベルの評価項目及び目標値は、表5-1、表5-2及び表5-3のとおりであるが、本調達における SLA の対象は、運用・保守に係る作業及び施設・設備に起因した場合とする。

表5-1 国民等向けサービスの評価項目と目標値
（インターネット経由での提供）

| No | サービス名 | サービス条件 | サービスレベル | | 評価又は測定方法 |
|---|---|---|---|---|---|
| | | | 評価項目 | 目標値 | |
| 1 | リポジトリの提供サービス | 有効な証明書失効情報(CRL/ARL)を計画された稼働時間に渡り提供すること。 | サービスの稼働率(%) | 99.99%以上 | 稼働率(%)＝{(稼働時間－サービス停止時間)÷稼働時間}×100 |
| 2 | | 有効な自己署名証明書及びリンク証明書を計画された稼働時間に渡り提供すること。 | サービスの稼働率(%) | 99.99%以上 | 稼働率(%)＝{(稼働時間－サービス停止時間)÷稼働時間}×100 |
| 3 | | 有効な相互認証証明書ペアを計画された稼働時間に渡り提供すること。 | サービスの稼働率(%) | 99.99%以上 | 稼働率(%)＝{(稼働時間－サービス停止時間)÷稼働時間}×100 |
| 4 | | 障害件数が目標値以下であること。 | 障害件数 | 1 回/年以内 | サービス停止件数 |
| 5 | | あらかじめ定めた期限までにサービスが復旧すること。 | 障害復旧時間 | 1時間以内 | サービス停止を確認してから復旧するまでの時間<br>障害復旧時間(H)＝(障害復旧日時－障害確認日時) |
| 6 | | LDAP の検索要求がサーバプロセスに到着してから応答を返却するまでの時間が定められた時間内であること。 | 応答時間（平均値） | 1.0 秒以内 | 応答時間 平均値(s) ＝応答時間の合計値÷要求件数 |
| 7 | | サービス停止を確認してから通知までの時間が定められていること。 | 障害通知時間 | 1時間以内 | 障害通知時間(H)＝(障害通知日時－障害確認日時) |

災害、外部ネットワーク障害等の要因による停止及び計画停止は除く。

表5-2 府省等利用機関向けサービスの評価項目と目標値

（インターネット経由での提供）

| No | サービス名 | サービス条件 | サービスレベル | | 評価又は測定方法 |
|---|---|---|---|---|---|
| | | | 評価項目 | 目標値 | |
| 1 | リポジトリの提供サービス | 有効な証明書失効情報（CRL/ARL）を計画された稼働時間に渡り提供すること。 | サービスの稼働率（%） | 99.99%以上 | 稼働率（%）＝{（稼働時間－サービス停止時間）÷稼働時間}×100 |
| 2 | | 有効な自己署名証明書及びリンク証明書を計画された稼働時間に渡り提供すること。 | サービスの稼働率（%） | 99.99%以上 | 稼働率（%）＝{（稼働時間－サービス停止時間）÷稼働時間}×100 |
| 3 | | 有効な相互認証証明書ペアを計画された稼働時間に渡り提供すること。 | サービスの稼働率（%） | 99.99%以上 | 稼働率（%）＝{（稼働時間－サービス停止時間）÷稼働時間}×100 |
| 4 | | 障害件数が目標値以下であること。 | 障害件数 | 1 回／年以内 | サービス停止件数 |
| 5 | | あらかじめ定めた期限までにサービスが復旧すること。 | 障害復旧時間 | 1時間以内 | サービス停止を確認してから復旧するまでの時間<br>障害復旧時間(H)＝（障害復旧日時－障害確認日時） |
| 6 | | LDAP の検索要求がサーバプロセスに到着してから応答を返却するまでの時間が定められた時間内であること。 | 応答時間（平均値） | 1.0 秒以内 | 応答時間 平均値(s) =応答時間の合計値÷要求件数 |
| 7 | | サービス停止を確認してから通知までの時間が定められていること。 | 障害通知時間 | 1時間以内 | 障害通知時間(H)＝（障害通知日時-障害確認日時） |
| 8 | 政府共用証明書検証サーバの提供サービス | 計画された稼働時間に渡り証明書検証サービスを提供すること。 | サービスの稼働率（%） | 99.99%以上 | 稼働率（%）={（稼働時間-停止時間）÷稼働時間}×100 |
| 9 | | 障害件数が目標値以下であること。 | 障害件数 | 1 回／年以内 | サービス停止件数 |
| 10 | | あらかじめ定めた期限までにサービスが復旧すること。 | 障害復旧時間 | 1時間以内 | サービス停止を確認してから復旧するまでの時間<br>障害復旧時間(H)＝（障害復旧日時-障害確認日時） |
| 11 | | 政府共用証明書検証サーバの検証要求がサーバプロセスに到着してから応答を返却するまでの時間が定められた時間内であること。<br>（政府共用証明書検証サーバが制御できない外部サーバの処理時間及びネットワークの遅延時間は応答時間に含めない。） | 応答時間（平均値） | 1.0 秒以内 | 応答時間 平均値(s)＝応答時間の合計(s)÷要求件数(件) |
| 12 | | サービス停止を確認してから通知までの時間が定められていること。 | 障害通知時間 | 1時間以内 | 障害通知時間(H)＝（障害通知日時－障害確認日時） |

災害、外部ネットワーク障害等の要因による停止及び計画停止は除く。

表5-3 府省等利用機関向けサービスの評価項目と目標値

（政府共通ネットワーク経由での提供）

| No | サービス名 | サービス条件 | サービスレベル | | 評価又は測定方法 |
|---|---|---|---|---|---|
| | | | 評価項目 | 目標値 | |
| 1 | リポジトリの提供サービス | 有効な証明書失効情報(CRL/ARL)を計画された稼働時間に渡り提供すること。 | サービスの稼働率(%) | 99.99%以上 | 稼働率(%)={(稼働時間－サービス停止時間)÷稼働時間}×100 |
| 2 | | 有効な自己署名証明書及びリンク証明書を計画された稼働時間に渡り提供すること。 | サービスの稼働率(%) | 99.99%以上 | 稼働率(%)={(稼働時間－サービス停止時間)÷稼働時間}×100 |
| 3 | | 有効な相互認証証明書ペアを計画された稼働時間に渡り提供すること。 | サービスの稼働率(%) | 99.99%以上 | 稼働率(%)={(稼働時間－サービス停止時間)÷稼働時間}×100 |
| 4 | | 障害件数が目標値以下であること。 | 障害件数 | 1 回/年以内 | サービス停止件数 |
| 5 | | あらかじめ定めた期限までにサービスが復旧すること。 | 障害復旧時間 | 1時間以内 | サービス停止を確認してから復旧するまでの時間<br>障害復旧時間(H)＝(障害復旧日時－障害確認日時) |
| 6 | | LDAP の検索要求がサーバプロセスに到着してから応答を返却するまでの時間が定められた時間内であること。 | 応答時間（平均値） | 1.0 秒以内 | 応答時間 平均値(s) = 応答時間の合計値÷要求件数 |
| 7 | | サービス停止を確認してから通知までの時間が定められていること。 | 障害通知時間 | 1時間以内 | 障害通知時間(H)＝(障害通知日時-障害確認日時) |
| 8 | 政府共用証明書検証サーバの提供サービス | 計画された稼働時間に渡り証明書検証サービスを提供すること。 | サービスの稼働率(%) | 99.99%以上 | 稼働率(%)={(稼働時間-停止時間)÷稼働時間}×100 |
| 9 | | 障害件数が目標値以下であること。 | 障害件数 | 1 回/年以内 | サービス停止件数 |
| 10 | | あらかじめ定めた期限までにサービスが復旧すること。 | 障害復旧時間 | 1時間以内 | サービス停止を確認してから復旧するまでの時間<br>障害復旧時間(H)＝(障害復旧日時－障害確認日時) |
| 11 | | 政府共用証明書検証サーバの検証要求がサーバプロセスに到着してから応答を返却するまでの時間が定められた時間内であること。<br>（政府共用証明書検証サーバが制御できない外部サーバの処理時間及びネットワークの遅延時間は応答時間に含めない。） | 応答時間（平均値） | 1.0 秒以内 | 応答時間 平均値(s)＝応答時間の合計(s)÷要求件数(件) |
| 12 | | サービス停止を確認してから通知までの時間が定められていること。 | 障害通知時間 | 1時間以内 | 障害通知時間(H)＝(障害通知日時-障害確認日時) |

| No | サービス名 | サービス条件 | サービスレベル | | 評価又は測定方法 |
|---|---|---|---|---|---|
| | | | 評価項目 | 目標値 | |
| 13 | LRA システムの提供サービス | 計画された稼働時間に渡り証明書発行・失効指示の受付が可能であること。<br>（業務プロセスのソフトウェアに起因する障害は除く） | サービスの稼働率（%） | 99.9%以上 | 稼働率（%）=｛（稼働時間−サービス停止時間）÷稼働時間｝×100<br>サービス提供時間：9 時 30 分～18 時 30 分（土曜、日曜、祝祭日、年末年始を除く） |
| 14 | | 障害件数が目標値以下であること。 | 障害件数 | 1 回／年以内 | サービス停止件数 |
| 15 | | あらかじめ定めた期限までにサービスが復旧すること。 | 障害復旧時間 | 8 時間以内 | サービス停止を確認してから復旧するまでの時間<br>障害復旧時間(H)＝（障害復旧日時−障害確認日時） |
| 16 | | 指示内容の形式検査後、受付が完了した発行・失効指示は損失することなく処理を行うこと。<br>（業務プロセスのソフトウェアに起因する障害は除く） | 損失件数 | 0 件 | 損失件数 |
| 17 | | サービス停止を確認してから通知までの時間が定められていること。 | 障害通知時間 | 1時間以内 | 障害通知時間(H)＝（障害通知日時−障害確認日時） |

災害、外部ネットワーク障害等の要因による停止及び計画停止は除く。

（２）事業継続性要件

政府認証基盤は、ブリッジ認証局、官職認証局それぞれの CP/CPS[4]に災害時の事業継続性要件を定めている。

災害等により認証局の設備が被害を受けた場合は、バックアップセンタにおいてバックアップデータを用いて運用を行う。バックアップセンタは、マスタセンタから適切な距離の場所に設置する。災害時の業務方針は以下のとおりである。

・リポジトリ及び Web による CRL/ARL の公表を最優先として、公表停止から 48 時間以内に公表を再開する。

・ 緊急を要する証明書発行及び失効業務は、業務停止より 96 時間以内に再開する。

・ 通常業務は、マスタセンタの認証局の設備及びセキュリティが完全に復旧されたことを確認後に再開する。

なお、事業継続に係る具体的な作業内容は、別途閲覧に供する以下の資料を参照。

・ 政府認証基盤 業務管理マニュアル － 危機管理マニュアル

[4] ブリッジ認証局 CP/CPS http://www.gpki.go.jp/bca/cpcps/cpcps.pdf
官職認証局 CP/CPS http://www.gpki.go.jp/osca/cpcps/cpcps.pdf

## ６ 情報セキュリティ要件

### （１）権限要件

今回調達する運用要員の役割ごとの権限要件については、別途閲覧に供する以下の資料を参照。

・ 政府認証基盤 業務管理マニュアル － 運用権限管理マニュアル

### （２）情報セキュリティ対策

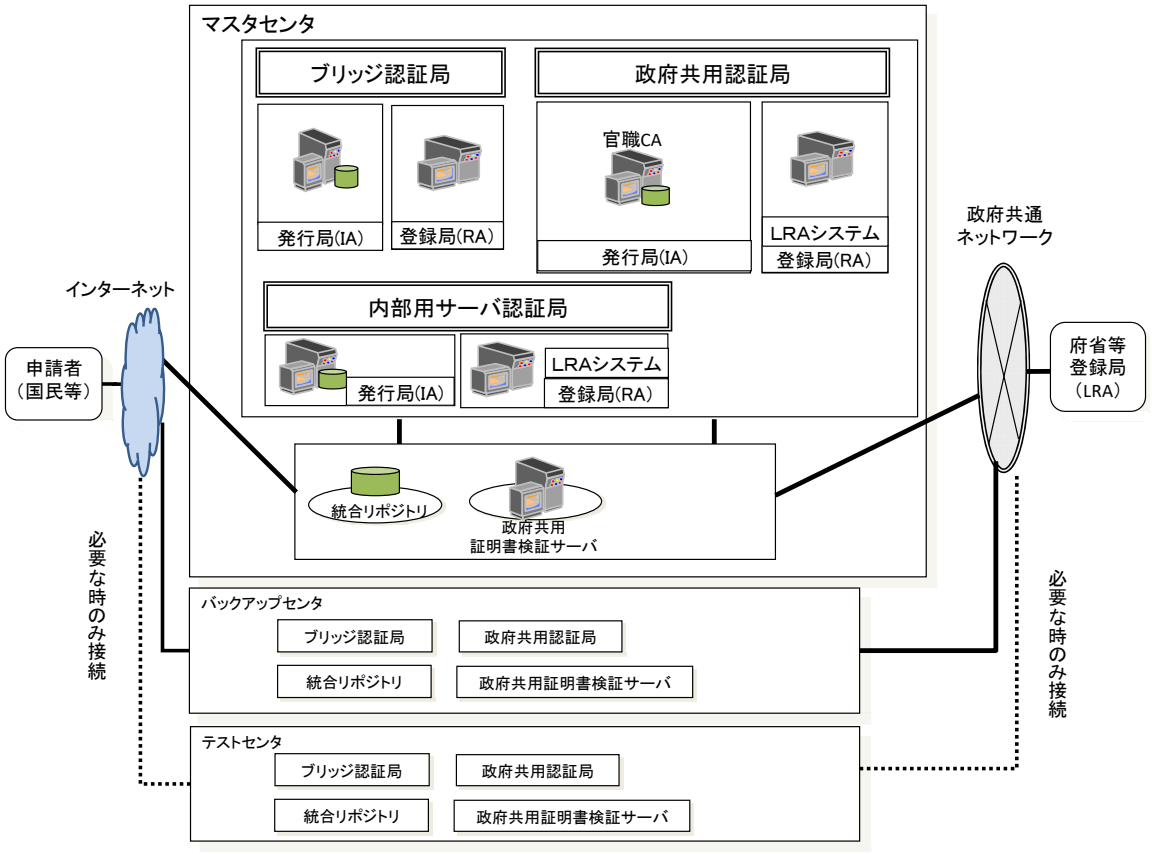
具体的な情報セキュリティ対策は、参照資料1「政府認証基盤 セキュリティ要件」及び別途閲覧に供する以下の資料を参照。

・ 政府認証基盤 情報セキュリティ実施手順書

なお、主管係が必要と認める際には、情報セキュリティ監査を受け入れること。

## 7 情報システム稼動環境

政府認証基盤を構成するシステム概要を下図に示す。




なお、全体構成、ハードウェア構成、ソフトウェア構成及びネットワーク構成の詳細は別途閲覧に供する以下の資料を参照。

- 構築仕様書（ブリッジCA編）
- 構築仕様書（官職CA編）
- 構築仕様書（内部用サーバCA編）
- 構築仕様書（ネットワーク編）
- LRAシステム基本設計書
- ICカードシステム仕様書

## 8 運用要件定義

### （１）システム操作・監視等要件

政府認証基盤を構成するシステムの操作及び監視に係る要件は、別途閲覧に供する以下の資料を参照。

- 政府認証基盤 システム運用マニュアル

なお、システム監視に関する特記事項は以下のとおり。

- 24時間週7日、監視を行うこと。
- 監視員は、2名が常時マスタセンタにて監視業務にあたるものとし、休憩時にも最低1名は、監視業務を継続していること。
- 監視業務における対処履歴を、電子データに記録すること。
- 指示事項に対しては、都度、監視員全員に、周知が完了したことを示す報告書を提出すること。

### （２）データ管理要件

運用要員は、システムで取得された認証業務及び監視業務に係るバックアップ及びアーカイブのデータ管理を実施する。認証業務の具体的なデータ管理要件は別途閲覧に供する以下の資料を参照。

- 政府認証基盤 システム運用マニュアル

### （３）運用施設・設備要件

施設・設備の要件は、認証業務に係る機器等の稼働に直接影響を与えない監視室及び事務室を除き、耐震性について震度6強以上の地震に耐えられる免震構造の建物とし、少なくとも現行のテストセンタを含むマスタセンタ（東京都内）を新たな施設・設備に移設すること。

ア 現行の施設・設備

現行の施設・設備については、マスタセンタ及びバックアップセンタ（東京近郊）の2カ所があり、施設使用料及び通信回線（インターネットとマスタセンタ間、インターネットとバックアップセンタ間の通信費及びプロバイダ契約料。請負者が所有している設備、物品及び政府共通ネットワークの接続料は除く）使用料（月額 17,380,000 円（税込み））は、請負業者の負担である。

なお、使用料の内訳は次のとおり。

【マスタセンタ】

施設使用料：9,421,100 円

通信回線使用料（インターネット回線　10Mbps×３）：378,900 円

【バックアップセンタ】

施設使用料：5,812,500 円

通信回線使用料（インターネット回線　1Mbps×1）：187,500 円

上記に含まれない次の設備等については、請負業者の負担である。

空調装置7式、監視カメラ 24 台、IC カード認証装置 15 台、生体認証装置9台、ラック架台 53 台、ラック 14 台、消火装置 17 台、金庫 11 台　等

現行の施設・設備の詳細については、別途閲覧に供する「現行の施設・設備の詳細」資料を参照。

イ　新たな施設・設備

以下の条件を満たす新たな施設・設備を提案することとし、施設使用料、通信回線使用料等は現行の月額を上限とすること。

また、機器等の移設・据付・調整・システム設定・テスト等への対応は、請負業者の責任と負担において行うこと。

- 新たな施設・設備は、参照資料2「政府認証基盤　施設・設備の詳細仕様」を満たしていること。
- 移設に伴う本システムのサービス停止時間（新旧システムの切替えを伴うもの）については、システム更改の請負者と連携して24時間内とし、回数は4回を限度とする。

## 9 保守要件定義

対象となるシステムは、ブリッジ認証局システム、政府共用認証局システム（独自に開発したアプリケーション含む）及び内部用サーバ認証局とすること。

システム変更を伴うシステム保守については、システム変更を本番環境に適用する前に必ずテストセンタのテスト環境において評価を実施すること。

システム保守は、業務停止を伴わないこと。業務を停止する場合は、夜間若しくは休日等の利用者の利用時間外に実施すること。

## 10 作業の体制及び方法

### （１）作業体制

ア　運用要員数の要件

今回調達する運用要員の役割と要員数を表 10-1 に示す。役割の兼務は運用責任者補佐とログ検査者についてのみ可能とする。

表 10-1 運用要員の役割と要員数

| 役割 | 要員数 |
|---|---|
| 運用責任者 | 1名 |
| 運用責任者補佐 | 2名以上 |
| ログ検査者 | 2名以上 |
| 上級IA操作員 | 6名以上 |
| 一般IA操作員 | 3名以上 |
| 監視員 | 8名以上 |
| 計 | 22名以上 |

イ　運用要員の経験、業務知識及びスキル等

（ア）認証局の運用実績

運用要員には、以下の運用実績を有する者を含めること。

- 行政機関の認証局又は電子署名法に基づく特定認証業務の認定を受けた認証局（以下、「特定認証局」という。）における運用責任者相当の運用
- 行政機関の認証局又は特定認証局における操作員としての運用
- 行政機関の認証局又は特定認証局における監視員としての運用

（イ）スキル

ITIL Foundation 認定資格者又は経済産業大臣認定の情報処理技術者試験のITサービスマネージャ試験、システム監査技術者試験、プロジェクトマネージャ試験いずれかの合格者であることが望ましい。

ウ　システム保守要員数の要件

システム保守要員数については、特に定めない。ただし、政府認証基盤を構成するシステムについて障害保守、予防保守等の対応を迅速かつ恒常的に行える体制を組むこと。

エ　システム保守要員の経験、業務知識及びスキル等

（ア） 認証局の保守実績

システム保守要員には、以下の保守実績を有する者を含めること。

- 行政機関の認証局又は特定認証局

（イ） スキル

主要なメンバとして、情報セキュリティスペシャリスト試験、テクニカルエンジニア（情報セキュリティ）試験いずれかの合格者又はITスキル標準のITスペシャリスト職種（専門分野セキュリティ）のレベル4以上の者、若しくは同等の能力を有する者を含むことが望ましい。

オ　その他

請負業者は、作業時期・内容等について主管係が承認した場合は、請負業者が指定する場所（運用要員の自宅を含む。）でリモート環境により作業を行うことができる。

なお、感染症対策として、業務のうち主管係との連絡調整などについてリモート環境で行うことや、主管係の承認のもと勤務体制を変更することなど、合理的な対策を可能な限り行うものとする。

（２） 導入

ア　作業実施場所

作業実施場所は、テストセンタを含むマスタセンタ（新たな施設・設備）及びバックアップセンタ（東京近郊）の2カ所となる。常時、運用要員が作業する場所は、マスタセンタとなる。

イ　業務引継

請負開始前までに、請負業者の負担において現請負先等から業務内容等について詳細に引継ぎ、令和4年2月1日から現行と同等のサービスを提供すること。

また、請負終了前においても、令和8年2月以降の請負先が現行と同等のサービスを提供できるよう、業務内容等について詳細に引継ぐこと。

ウ　その他

- 運用要員及び保守要員のバックアップ体制をとること。
- 運用要員と保守要員の兼務は行わないこと。
- 運用要員及び保守要員は、夜間・休日を問わず緊急時の連絡及び召集に対応するため、携帯電話等（請負業者が手配し通話料・通信料を負担）を常備して常に連絡が取れること。

また、主管係が要員への連絡に必要な携帯電話等2台以上を請負業者の負担において手配し、通話料・通信料も負担すること。

- 本件調達については、サービスレベルアグリーメント（SLA）を導入する。請負業者は、別途指定するサービスレベル要件を満たすサービスの提供が可能となる体制をとること。本件調達範囲の業務に起因してSLAが達成されなかった場合、月額役務経費に相当する金額の5%を減額する。
- 運用及び保守に必要な消耗品等は請負業者が準備すること。消耗品の仕様等の詳細は別途閲覧に供する「消耗品一覧」資料を参照。
- サーバ証明書等の発行支援の業務において、証明書の取得に係る費用は請負業者が負担すること。
- 主管係及び利用機関等への連絡等に必要な通信運搬費は請負業者が負担すること。
- 主管係の指示に従い業務を実施すること。
- 主管係において、要員が適切に業務を実施できないと判断した場合、請負業者は速やかに対応すること。

## １１ 特記事項

（１）情報セキュリティ確保及び秘密保持

本件業務を請負う者は、取り扱う情報に関して、以下の事項を遵守すること。

ア　情報セキュリティ実施手順の作成

請負業者は、請負った情報システムについて、別途閲覧に供する総務省情報セキュリティポリシーを踏まえ、次に掲げる事項の具体的な内容を盛り込んだ情報セキュリティ実施手順書（以下「実施手順書」という。）を作成し、主管係の承認を得ること。

（ア）システム運用管理者、システム運用担当者を明確にした情報セキュリティ管理体制及び緊急時における連絡体制

（イ）管理区域への入退室等の物理的セキュリティ対策

（ウ）パスワード管理、要員の教育計画等の人的セキュリティ対策

（エ）アクセス制御等の技術的セキュリティ対策

（オ）各セキュリティ対策の確保状況に関する報告内容、報告方法等

（カ）緊急時の対応に必要な事項

（キ）その他、情報システム管理者が必要と認めた事項

イ　実施手順書等の遵守

請負業者は、実施手順書及び参照資料3「秘密情報保護・管理要領」を遵守し、実施手順書違反等があった場合は直ちに主管係へ報告し、指示を受けること。

ウ　セキュリティ情報の収集

請負業者は、請負った情報システムのセキュリティに関連する最新情報を常に収集し、主管係へ報告するとともに、主管係の指示に基づき必要な措置を行うこと。

エ　委託契約

請負業者は、請負った情報システムの整備・運用に当たって他の事業者と委託契約を行う場合は、主管係の承認を得ること。承認等必要な手続については、契約書に従うこと。

オ　身元保証

請負業者は、各要員の在籍証明書、業務経歴書及び秘密保持管理証明書を提出すること。

また、他の事業者と委託契約を行う場合は、当該事業者の在籍証明書及び秘密保持管理証明書とともに、請負業者がこれを保障する証明書を提出すること。

カ　運用・保守に支障をきたす事案の発生時等における対処

請負業者は、請負った情報システムの運用・保守に支障をきたす事案が発生したとき、又は発生する恐れがあると推定されるときは、主管係に対して直ちに連絡し、対応措置について指示を受けること。

（２） 法令等の遵守

業務の遂行において使用する情報資産について、次の法律その他の法令等を遵守し、これに従わなければならない。また、関連するガイドライン等も同様とする。

・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）
・著作権法（昭和 45 年法律第 48 号）
・不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）
・電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成 14 年総務省告示第 334 号）

（３） 知的財産権

ア　本契約履行過程で生じた成果物に関し、著作権法第27条及び28条に定める権利を含むすべての著作権を総務省に譲渡し、総務省は独占的に使用するものとする。
なお、請負業者は総務省に対し、一切の著作者人格権を行使しないこととし、また、第三者をして行使させないものとする。
また、請負業者が本契約の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、総務省と別途協議するものとする。

イ　成果物に第三者が権利を有する著作物が含まれている場合は、総務省が特に使用を指示した場合を除き、請負業者は当該著作物の使用に関して費用の負担を含む一切の手続を行うものとする。なお、この場合、請負業者は当該著作物の使用許諾条件につき、主管係の了承を得ること。

ウ　本件業務の作業に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合、当該紛争の原因が専ら総務省の責めに帰す場合を除き、請負業者は自らの責任と負担において一切を処理すること。なお、総務省は紛争等の事実を知ったときは、速やかに請負業者に通知することとする。

（４） その他

ア　本件調達に係る業務の実施予定組織・部門がISO27001又は同等の認証を取得していること。

イ　運用業務において必要とする当該仕様書に記載のない要件が発生した際には、対処に関する協議を別途行うものとする。

ウ　LRAからの証明書発行申請に基づき、サーバ証明書、コード署名証明書、ドキュメント署名証明書を発行事業者（民間）から取得するサーバ証明書等の発行支援を行うこと。
契約期間中、発行事業者から取得する証明書は、最大の有効枚数を以下と想定する。

- サーバ証明書・・・1,000枚
- コード署名証明書・・・100枚
- ドキュメント署名証明書・・・30枚

≪本調達仕様書に関する問い合わせ先≫

総務省行政管理局行政情報システム企画課情報システム管理室
（政府認証基盤担当）
電話：03-5253-6078
電子メール：gpki2@soumu.go.jp

参照資料1

# 政府認証基盤　セキュリティ要件

目次

# 1. セキュリティ要件

## 1.1 前提条件

政府認証基盤のセキュリティ要件の前提条件は次のとおりである。

WebTrust for CA 基準相当とすること。
「総務省情報セキュリティポリシー」（以下「情報セキュリティポリシー」という。）に準拠すること。
リスク分析を実施し、その結果、必要と認められた対策をセキュリティ対策として定義すること。

なお、WebTrust for CA は次に示す 3 つの原則から構成されているが、原則 1 は CP/CPS 等での開示に関するものであるため、セキュリティ要件の検討対象外とする。

原則 1　CA ビジネス実務の開示
原則 2　サービスインテグリティ
原則 3　CA 環境の内部統制

## 1.2 リスク分析

### 1.2.1 リスク分析手法

**(1) 情報資産の調査**

政府認証基盤における保護すべき情報資産として、どのようなものが存在するか調査した。なお、情報資産としての性質（用途等）、ライフサイクルが類似しており、かつその重要性が同等と考えられる情報資産については、個別に列記せず、総称することとした。具体的には、「作業指図書兼作業記録書」、「作業申請書」、各種管理台帳等は、個別の情報資産としては取り扱わず、「作業記録帳票」として総称した。

**(2) 重要性の分類**

情報資産について、機密性、完全性、可用性の 3 つの側面から重要性を検討し、分類した。

(a) 重要性の 3 つの側面

機密性・・・情報に関して正当な権限を持った者だけが、情報にアクセスできることの重要性。
完全性・・・情報に関して破壊、改ざん又は消去されていないことの重要性。
可用性・・・情報に関して正当な権限を持った者が、必要時に中断することなく、情報にアクセスできることの重要性。
（出典：サイバーセキュリティ 2019[1]）

(b) 重要性の分類

（機密性）
機密性 3：
行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報。
機密性 2：
行政事務で取り扱う情報のうち、不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性 3 情報」以外の情報。
機密性 1：
機密性 2 情報又は機密性 3 情報以外の情報。

（完全性）
完全性 2：
行政事務で取り扱う情報のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障

[1] サイバーセキュリティ 2019（令和元年 5 月 23 日　サイバーセキュリティ戦略本部）

（軽微なものを除く。）を及ぼすおそれがある情報。

完全性１：

完全性２情報以外の情報。

（可用性）

可用性２：

行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報。

可用性１：

可用性２情報以外の情報。

（出典：情報セキュリティポリシー）

以下の表に情報資産とその重要性を示す。

情報資産の「名称」欄に、複数の情報資産の総称を記載した場合は、「詳細」欄にその内訳を記載した。また、情報資産に個人情報（氏名だけでなく、所属・連絡先等を含む場合に限る）が含まれる場合は、「個人情報」欄に「○」を記載した。特に該当がない場合は「－」と記載している。

なお、可用性に関する重要性は、利用不可能となることによる影響に基づき評価した。

**表 1.2-1　情報資産一覧**

| 項番 | 情報資産 | | 個人情報 | 重要性 | | |
|---|---|---|---|---|---|---|
| | 名称 | 詳細 | | 機密性 | 完全性 | 可用性 |
| 1 | 認証局（以下、CA という。）秘密鍵 | － | － | 3 | 2 | 2 |
| 2 | 自己署名証明書（CA 公開鍵） | － | － | 1 | 2 | 2 |
| 3 | 相互認証証明書 | － | － | 1 | 2 | 2 |
| 4 | エンドエンティティ（以下、EE という。）秘密鍵（CA が代理生成する場合） | － | － | 3 | 2 | 2 |
| 5 | EE 証明書（EE 公開鍵） | － | － | 1 | 2 | 2 |
| 6 | 政府共用証明書検証サーバ（以下、CVS という。）秘密鍵 | － | － | 3 | 2 | 2 |
| 7 | CVS 証明書（CVS 公開鍵） | － | － | 1 | 2 | 2 |
| 8 | CRL/ARL | － | － | 1 | 2 | 2 |
| 9 | 府省等登録局（以下、LRA という。）の要員登録・変更申請書類 | － | ○ | 3 | 2 | 1 |
| 10 | LRA システムログインカード | － | － | 3 | 2 | 1 |
| 11 | EE 証明書申請書類 | 発行申請書、失効申請書等 | ○ | 3 | 2 | 1 |
| 12 | EE 証明書受領書（LRA から政府共用認証局に提出されるもの） | － | ○ | 3 | 2 | 1 |
| 13 | EE 証明書受領書（証明書利用者から LRA に提出されるもの） | － | ○ | 3 | 2 | 1 |

| 項番 | 情報資産 | | 個人情報 | 重要性 | | |
|---|---|---|---|---|---|---|
| | 名称 | 詳細 | | 機密性 | 完全性 | 可用性 |
| 14 | 監査ログ | CA 監査ログ、LRA 監査ログ等 | － | 3 | 2 | 1 |
| 15 | アーカイブ | CA アーカイブ、LRA アーカイブ等 | － | 3 | 2 | 1 |
| 16 | システムデータ、アプリケーションデータ | CA、LRA、CVS、リポジトリ等各種サーバのデータ、設定値 | － | 3 | 2 | 2 |
| 17 | パスワード、PIN | － | － | 3 | 2 | 2 |
| 18 | 入退室ログ | － | － | 3 | 2 | 1 |
| 19 | 作業記録帳票 | 作業指図書兼作業記録書、作業申請書、各種管理台帳、障害調査記録書、日次報告書、要員への教育記録等 | － | 3 | 1 | 1 |
| 20 | 業務連絡書 | － | － | 3 | 1 | 1 |
| 21 | 入室申請書 | － | ○ | 3 | 1 | 1 |
| 22 | 設計・開発文書 | システム構築納品物、コンフィグレーションシート等 | － | 3 | 2 | 1 |
| 23 | 準拠性監査報告書 | － | － | 3 | 2 | 1 |
| 24 | LRA の内部監査結果 | － | － | 3 | 2 | 1 |
| 25 | 緊急連絡先 | ブリッジ認証局、政府共用認証局、相互認証先、委託先等の緊急連絡先 | ○ | 3 | 2 | 2 |
| 26 | 会議資料、議事録 | 運用報告会資料、連絡会議資料、議事録 | － | 3 | 1 | 1 |
| 27 | 契約書等 | 委託先契約書、仕様書 | － | 3 | 2 | 1 |
| 28 | CP/CPS(CP:証明書ポリシー、CPS:認証局運用規程) | ブリッジ認証局 CP/CPS、官職認証局 CP/CPS | － | 1 | 2 | 1 |
| 29 | 運用マニュアル | 情報セキュリティ実施手順書、システム運用マニュアル、業務管理マニュアル、操作手順書等 | － | 3 | 2 | 2 |

### (3) リスク評価

情報資産について、次の観点からリスクを評価した。

(a) 脅威の調査

次に示す情報資産のライフサイクルを踏まえ、情報資産に対する脅威（漏洩、改ざん、利用不能）を調査した。

作成・入手
利用
保存
移送
提供
消去

(b) 脅威の発生頻度の評価

脅威に対する現状対応策を踏まえ、次の観点から脅威の発生頻度を評価した。

A：かなりの頻度で発生する。
B：時々発生する。
C：偶発的に発生する。
D：ほとんど発生しない。

(c) リスクの評価

情報資産の重要性と、脅威の発生頻度に基づき、次の算式でリスクの大きさを評価した。4 が最もリスクが大きく、1 が最もリスクが小さいものとし、1 を許容可能なものとした。

表 1.2-2　リスクの大きさ

| | | 重要性（被害の大きさ） | | |
|---|---|---|---|---|
| | | 上段：機密性、下段：完全性・可用性 | | |
| | | 3 | 2 | 1 |
| | | 2 | 1 | 該当なし |
| 発生頻度 | A | 4 | 3 | 1 |
| | B | 3 | 2 | 1 |
| | C | 2 | 1 | 1 |
| | D | 1 | 1 | 1 |

### (4) リスク再評価

リスクを評価した結果、2 以上（許容不可能）となったものについて、追加対応策を検討し、それを踏まえて脅威の発生頻度及びリスクの大きさを再評価した。また、リスクを許容可能な水準まで低減するために必要と認めた追加対応策は、セキュリティ対策に反映した。

## 1.3 セキュリティ対策

セキュリティ対策の検討を行った結果を、以下に示す。

### 1.3.1 セキュリティ対策（WebTrust for CA 原則 2）

WebTrust for CA 原則 2 における規準(Criteria)のうち政府共用認証局に該当するものをセキュリティ目標とし、コントロール例（Illustrative Controls）のうち政府共用認証局に該当するもの及びリスク分析の結果、必要と判断された対策を、セキュリティ対策として表 1.3-1 のとおり実施する。

なお、ブリッジ認証局についても該当する箇所はこれに準じる。

表 1.3-1 セキュリティ対策（WebTrust for CA 原則 2）

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| 2 サービスインテグリティ<br>2.1 鍵ライフサイクル統制<br>2.1.1 CA 鍵生成 | | |
| 政府共用認証局は、CA 鍵ペアを業界標準に従い生成するという合理的な保証を提供する内部統制を保持する | 1 | FIPS140-1 レベル 3 又は 140-2 レベル 3 以上のセキュリティレベルの認定を得たハードウェアセキュリティモジュール（以下「CA-HSM」という。）内部において、CA 鍵生成を実施すること |
| | 2 | CA 鍵生成は、適切に承認された要員によるデュアルコントロールを要すること |
| | 3 | CA 鍵生成は、鍵を使用する CA-HSM そのものにおいて実施すること |
| | 4 | CA 鍵生成においては、ANSI X9 もしくは ISO 規格に規定する乱数生成方法(RNG)、あるいは疑似乱数生成方法(PRNG)を利用すること |
| | 5 | CA 鍵生成においては、ANSI X9 もしくは ISO 規格に規定する素数生成方法を利用すること |
| | 6 | CA 鍵生成においては、ANSI X9 あるいは ISO 規格に規定する鍵生成アルゴリズムを利用すること |
| | 7 | CA 鍵生成においては、CP/CPS に規定する鍵長で鍵生成を行うこと |
| | 8 | 鍵生成に利用するハードウェア及びソフトウェアの完全性、ハードウェア及びソフトウェアに対するインターフェイスを、利用に先立ちテストすること |
| 2.1.2 CA 鍵格納、バックアップ、復旧 | | |
| 政府共用認証局は、CA 秘密鍵の機密性、完全性を維持するという合理的な保証を提供する内部統制を保持する | 9 | FIPS140-1 レベル 3 又は 140-2 レベル 3 以上のセキュリティレベルの認定を得た CA-HSM 内部に、CA 秘密鍵を格納すること |
| | 10 | CA 秘密鍵は、オフライン処理、バックアップ及び復旧を実施するために、CA-HSM から安全な保管場所に移される場合を除いては、同一の CA-HSM 内部で生成、使用され、CA-HSM の外部には取り出さないこと |
| | 11 | オフライン処理、バックアップ及び復旧を実施するために、CA 秘密鍵を CA-HSM から安全な記憶媒体にコピーする場合、下記手法のいずれかを含む、安全な鍵管理手法を利用すること<br><br>a. デュアルコントロールにより暗号化する<br>b. デュアルコントロール及び知識/所有権分割により、暗号化された鍵の断片とする<br>c. デュアルコントロールにより、鍵を持ち運ぶための機器等、安全な暗号モジュールにコピーする |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| | 12 | CA 秘密鍵は、物理的に安全な環境で、デュアルコントロールを用い、適切に承認された要員により、バックアップ、格納及び復旧されること |
| | 13 | CA 秘密鍵をバックアップする場合、CA 秘密鍵のバックアップコピーは、実運用におけるものと同等、あるいはそれ以上のセキュリティレベルにより管理すること |
| | 14 | CA 秘密鍵をバックアップする場合、CA 秘密鍵の復旧は、デュアルコントロールを用い、バックアップと同様に安全な方法で行うこと |
| 2.1.3　CA 公開鍵配布 | | |
| 政府共用認証局は、初期配付及びそれ以降の配付において、CA 公開鍵及びそれに関連するパラメータの完全性と信頼性を維持するという合理的な保証を提供する内部統制を保持する | 15 | CA 公開鍵の初期配布において、配布する CA 公開鍵の改ざんを検知できる仕組みを提供すること<br>例えば、オフライン、SSL 等、安全な方法での自己署名証明書及びそのフィンガープリントの提供等 |
| | 16 | CA 公開鍵の初期配布は CP/CPS に規定するとおり、管理すること |
| | 17 | CA 公開鍵の初期配布は、安全な方法により行うこと |
| | 18 | CA 公開鍵は、定期的に更新すること |
| | 19 | CA 公開鍵の初期配布以降の配布方法は CP/CPS に規定するとおり、管理すること |
| | 20 | 証明書利用者、証明書検証者が既に認証された CA 公開鍵のコピーを所有する場合、新たな CA 公開鍵の配布は、安全な方法により行うこと |
| 2.1.4　CA 鍵預託（オプション） | | |
| 2.1.5　鍵使用目的 | | |
| 政府共用認証局は、CA 鍵を予定した機能および場所に限定して利用するという合理的な保証を提供する内部統制を保持する | 21 | CA 秘密鍵の活性化は、マルチパーティコントロール（つまり、m of n）により実施すること |
| | 22 | CA 秘密鍵の活性化は多因子認証を利用すること |
| | 23 | CA 鍵ペアの有効期間が終了した場合、CA 秘密鍵の危殆化が発覚した場合、あるいはそのおそれがある場合は、CA 鍵ペアの利用を終了すること |
| 2.1.6　CA 鍵の破棄 | | |
| 政府共用認証局は、鍵ペアライフサイクル終了時に、CA 鍵を完全に破棄するという合理的な保証を提供する内部統制を保持する | 24 | CA 秘密鍵の破棄に対する承認及び CA 秘密鍵の破棄方法（例えば、トークンの破壊や鍵の上書き等）を、制限すること |
| | 25 | CA 鍵ペアライフサイクル終了時に、CA 秘密鍵に関するあらゆるコピー及び断片を破棄すること |
| | 26 | 利用中の CA-HSM を、サービスから恒久的に取り除くことが予定されている場合、CA-HSM に格納された全ての CA 秘密鍵（これまでに暗号的な目的で利用された、或いは利用された可能性があるもの）を破棄すること |
| | 27 | CA-HSM をサービスから恒久的に取り除く場合、CA-HSM が保管し、これまでに暗号目的で利用があったあらゆる鍵を CA-HSM から消去すること |
| | 28 | CA-HSM を恒久的にサービスから取り除く場合であり、CA-HSM をタンパー検知筐体に収容していた場合は、筐体を破壊すること |
| 2.1.7　CA 鍵アーカイブ | | |
| 政府共用認証局は、アーカイブされた CA 鍵の機密性を維持し、決して実運用に戻さないという合理的な保証を提供する内部統制を保持する | 29 | CA 秘密鍵のアーカイブは行わないこと<br>また、アーカイブされた CA 公開鍵は、実運用におけるものと同等あるいはそれ以上のセキュリティレベルで管理すること |
| | 30 | アーカイブされた CA 公開鍵は、アーカイブ期間が終了した時点で、物理的に安全な場所において、デュアルコントロールにより破棄すること |
| | 31 | アーカイブされた CA 公開鍵を、決して実運用に戻さないこと |
| | 32 | アーカイブされた CA 公開鍵は、技術的に可能な限り短時間で復旧すること |
| | 33 | アーカイブ期間を終了した時点で適切に破棄しているかを確認するために、アーカイブされた CA 公開鍵を定期的に検査すること |
| 2.1.8　CA 暗号装置ライフサイクル管理 | | |
| 政府共用認証局は、CA-HSM へのアクセスを適切に | 34 | CA-HSM が製造業者からタンパー検知梱包を利用し、かつ配達記録がされる方法により配送されることを、方針および手続に定めること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| 承認された要員のみに制限するという合理的な保証を提供する内部統制を保持する | 35 | 製造業者から CA-HSM が入荷した時点で、封印が破損していないか確認するため、承認された CA 要員がタンパー検知梱包を検査すること |
| | 36 | 不正を防止するため、CA-HSM は、承認された要員のみにアクセス制御され、次のような条件を満たす安全な場所に設置すること<br>a. 機器毎の出所、入荷、状態、搬出、宛先を管理する機材管理手続<br>b. 承認された要員のみに物理的アクセスを制限するアクセスコントロール手続<br>c. CA 設備および装置保管庫（例えば金庫等）に対するあらゆるアクセス成功及び失敗のイベント履歴への記録<br>d. 異常事態、セキュリティ侵害を取扱い、調査・報告するための事故対応手続<br>e. コントロールの有効性を検証する監査手続 |
| | 37 | CA-HSM は、耐タンパー筐体に収容すること |
| | 38 | CA-HSM の取り扱いは、2 名以上の信頼できる従業員の立会の下で実施すること |
| | 39 | CA-HSM の設置は、2 名以上の信頼できる従業員の立会の下で実施すること |
| | 40 | 運用環境からの CA-HSM 撤去は、2 名以上の信頼できる従業員の立会の下で実施すること |
| | 41 | CA-HSM を新たなハードウェア、ファームウェア、ソフトウェア等により修理あるいは保守点検する場合は、2 名以上の信頼できる従業員の立会の下で実施すること |
| | 42 | 修理あるいは保守点検を行う場所は、機材管理を行い、承認された要員のみに入退室を制限すること |
| | 43 | CA-HSM を解体し、恒久的に運用環境から撤去する場合は、2 名以上の信頼できる従業員の立会の下で実施すること |
| 政府共用認証局は、CA-HSM が正常に機能しているという合理的な保証を提供する内部統制を保持する | 44 | 製造業者から CA-HSM が入荷した時点で、受入検査およびファームウェア設定確認を実施すること |
| | 45 | 修理あるいは保守点検に出した CA-HSM が戻った時点で、受入検査およびファームウェア設定確認を実施すること |
| | 46 | CA-HSM 及び CA-HSM に対するインターフェイスの完全性を、利用に先立ちテストすること |
| | 47 | CA-HSM が正しく稼働しているか、定期的に確認すること |
| | 48 | CA-HSM の障害分析時に、CA-HSM の診断を実施する場合は、2 名以上の信頼できる従業員の立会の下で実施する |
| 2.1.9　CA が提供する証明書利用者管理サービス（オプション） | | |
| 2.2　証明書ライフサイクル統制<br>2.2.1　証明書利用者登録 | | |
| 政府共用認証局は、証明書利用者を適切に識別・認証するという合理的な保証を提供する内部統制を保持する | 49 | 政府共用認証局は、府省等登録局が証明書申請者の真偽を審査していることを、審査するか、または要求すること |
| | 50 | 政府共用認証局は証明書申請者に対し、適切な証明書申請情報を、府省等登録局または政府共用認証局に対し準備及び提出するよう要求すること |
| | 51 | 政府共用認証局は、府省等登録局が証明書申請者の権限を審査することを、審査するか、または要求すること |
| | 52 | 政府共用認証局は、証明書申請者が提出した証明書申請情報の正確性を、府省等登録局が審査することを、審査するか、または要求すること |
| | 53 | 政府共用認証局は府省等登録局の真偽を確認すること |
| | 54 | 政府共用認証局は府省等登録局を認可すること |
| 政府共用認証局は、証明書利用者の証明書発行申 | 55 | 政府共用認証局は、証明書申請者に対し、適切な証明書申請情報を準備し、府省等登録局または政府共用認証局に提出するよう要求すること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| 請が正確、承認済かつ完全であるという合理的な保証を提供する内部統制を保持する | 56 | 証明書利用者にて鍵ペアを生成する場合、政府共用認証局は証明書申請者に、公開鍵を署名したメッセージに含めて府省等登録局または政府共用認証局に提出するよう要求すること。<br>下記を実施するため、政府共用認証局は証明書申請者に、登録要求に含まれる公開鍵に対応する秘密鍵を用いて登録要求に電子署名することを要求すること。<br>a. 証明書申請における誤謬（誤り等）を発見可能とするため<br>b. 登録される公開鍵と対を成す秘密鍵を所持することを証明するため<br>ただし、政府共用認証局にて証明書利用者の鍵ペアを生成する場合は、この限りではない。 |
| | 57 | 証明書利用者にて鍵ペアを生成する場合、政府共用認証局は、証明書申請に含まれる公開鍵を用いて、証明書申請の電子署名を検証すること<br>ただし、政府共用認証局にて証明書利用者の鍵ペアを生成する場合は、この限りではない。 |
| | 58 | 政府共用認証局は、府省等登録局が政府共用認証局に証明書申請情報を提出する際、当該申請情報を府省等登録局が署名したメッセージ（証明書要求）に含めるか、または同等の安全性が確保できる方法により、政府共用認証局に提出するよう要求すること |
| | 59 | 政府共用認証局は、証明書申請の過程における府省等登録局の責任範囲について、府省等登録局自身で安全性を確保するよう、府省等登録局に要求すること |
| | 60 | 政府共用認証局は府省等登録局における活動をイベント履歴に記録するよう、府省等登録局に要求すること |
| | 61 | 政府共用認証局は府省等登録局から提出された証明書申請情報の信頼性を審査すること |
| | 62 | 政府共用認証局は、府省等登録局から提出された証明書申請情報について、府省等登録局の署名確認、または同等の安全性が確保できる方法による確認を行うこと |
| | 63 | 政府共用認証局あるいは府省等登録局は、証明書申請情報に誤謬あるいは脱落がないか審査すること |
| | 64 | 政府共用認証局は、証明書申請情報に記載された識別名が、政府共用認証局において一意であるかを審査すること |
| | 65 | 政府共用認証局は、その真偽が確認された証明書申請者からの証明書発行申請のみを受け付けること |
| | 66 | 政府共用認証局は、公開鍵の重複を発見した場合、証明書申請を拒否し、元々の証明書を失効すること |
| 2.2.2　証明書更改（オプション） | | |
| 2.2.3　証明書更新 | | |
| 政府共用認証局は、証明書更新申請が正確、承認済かつ完全であるという合理的な保証を提供する内部統制を保持する | 67 | 政府共用認証局あるいは府省等登録局が、更新すべき証明書を識別可能とするため、証明書利用者の更新申請は、更新すべき証明書を識別するために必要な情報を含んでいること |
| | 68 | 政府共用認証局または府省等登録局は、証明書更新申請を処理し、証明書申請者の真偽を確認するとともに、更新すべき証明書を識別すること |
| | 69 | 政府共用認証局または府省等登録局は、証明書更新申請の署名を検証すること |
| | 70 | 政府共用認証局または府省等登録局は、更新すべき証明書が実在し、かつ有効であることを確認すること |
| | 71 | 政府共用認証局または府省等登録局は、証明書更新申請が CP/CPS に規定する要件を満たしているか確認すること |
| | 72 | 政府共用認証局は府省等登録局に対し、証明書更新申請を府省等登録局が署名したメッセージに含めるか、または同等の安全性が確保できる方法により、政府共用認証局に提出することを要求すること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| | 73 | 政府共用認証局は、証明書更新申請の過程における府省等登録局の責任範囲について、府省等登録局自身で安全性を確保するよう、府省等登録局に要求すること |
| | 74 | 政府共用認証局は府省等登録局における活動をイベント履歴に記録するよう、府省等登録局に要求すること |
| | 75 | 政府共用認証局は府省等登録局から提出された証明書申請情報の信頼性を審査すること |
| | 76 | 政府共用認証局は、府省等登録局から提出された証明書更新申請について、府省等登録局の署名確認、または同等の安全性が確保できる方法による確認を行うこと |
| | 77 | 政府共用認証局あるいは府省等登録局は、証明書更新申請に誤謬あるいは脱落がないか審査すること |
| | 78 | 政府共用認証局あるいは府省等登録局は、証明書利用者に対し、有効期限終了に先立ち証明書更新が必要であることを通知すること |
| | 79 | 更新する証明書の生成および発行に先立ち、政府共用認証局または府省等登録局は下記を確認すること<br>a. 提出された証明書更新申請の署名<br>b. 更新するべき証明書の実在および有効性<br>c. 証明書更新申請（有効期間延長を含む）が CP/CPS に規定する要件に適合すること |
| 政府共用認証局は、失効或いは有効期限切れを原因とする証明書更新申請が正確、承認済かつ完全であるという合理的な保証を提供する内部統制を保持する | 80 | 証明書利用者の既存証明書が有効期間満了あるいは失効した場合の証明書再発行は、初期登録の手続に基づき行うこと |
| 2.2.4　証明書発行 | | |
| 政府共用認証局は、新規発行及び更新時の証明書生成・発行を CP/CPS に従い実施するという合理的な保証を提供する内部統制を保持する | 81 | 政府共用認証局は、適切な証明書フォーマットを用いて証明書を生成すること |
| | 82 | 政府共用認証局は、X.509 に従って証明書を生成すること |
| | 83 | X.509 に従って有効期間を設定すること |
| | 84 | X.509 に従って拡張領域を設定すること |
| | 85 | X.509 に従って鍵使用目的拡張領域を設定すること |
| | 86 | 政府共用認証局は、証明書利用者の証明書に、CA 秘密鍵を用いて署名すること |
| | 87 | 政府共用認証局は、証明書利用者に対し、証明書受領後、速やかに証明書の内容を確認するとともに、問題があった場合は、速やかに失効及び再発行申請するよう要求すること |
| | 88 | 政府共用認証局は、証明書利用者に証明書を発行した際、当該証明書に係る証明書申請情報を提出した府省等登録局に対し、発行の事実を通知すること |
| | 89 | 証明書鍵更新時に、所定の手続に従い、証明書鍵更新申請を承認した場合に限り、政府共用認証局は新しい証明書を生成し、署名すること |
| | 90 | 証明書を発行した時点で、政府共用認証局は証明書利用者に対し、個別に発行の事実を通知すること |
| 2.2.5　証明書配布 | | |
| 政府共用認証局は、CP/CPS に従い、証明書発行時に、証明書利用者及び証明書検証者が完全かつ正確な証明書を利用できるという合理的な保証 | 91 | 政府共用認証局は、発行した証明書のうち、証明書検証者への提供が必要なものについては、リポジトリを用いて証明書検証者に提供すること |
| | 92 | 政府共用認証局は、証明書発行時に、リポジトリあるいはその他の証明書配布手段を用いて証明書を配布する |
| | 93 | 承認された CA 要員だけがリポジトリあるいはその他の証明書配布手段を管理すること |
| | 94 | リポジトリあるいはその他の証明書配布手段の性能を監視・管理すること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| を提供する内部統制を保持する | 95 | リポジトリあるいはその他の証明書配布手段の完全性を維持すること |
| 2.2.6　証明書失効 | | |
| 政府共用認証局は、承認された、かつ有効な証明書失効申請に基づいて、証明書を失効するという合理的な保証を提供する内部統制を保持する | 96 | 政府共用認証局は、下記に関する安全かつ承認された失効を促進するための緊急連絡手段を提供すること<br>a. 1 以上のエンティティに係わる 1 以上の証明書<br>b. 政府共用認証局が証明書生成に用いた単一の公開鍵/秘密鍵ペアにより、政府共用認証局が発行した証明書全て<br>c. 使用した公開鍵/秘密鍵ペアにかかわらず、政府共用認証局が発行した証明書全て |
| | 97 | 政府共用認証局は、府省等登録局が証明書失効申請者を識別・認証していることを審査するか、または要求すること |
| | 98 | 政府共用認証局は、府省等登録局が証明書失効申請を受理した場合、認可された方法で当該失効申請を政府共用認証局に提出するよう、府省等登録局に要求すること |
| | 99 | 政府共用認証局は、府省等登録局が証明書失効申請を受理し、政府共用認証局に提出した場合、府省等登録局に対し証明書失効を通知すること |
| | 100 | 政府共用認証局は、証明書失効時に証明書失効リスト(Certificate Revocation List：CRL)を更新すること |
| | 101 | 政府共用認証局は、全ての証明書失効申請及びそれらの結果をイベント履歴に記録すること |
| | 102 | 政府共用認証局または府省等登録局は、失効した証明書の証明書利用者に対し、証明書失効を通知すること |
| 2.2.7　証明書一時停止（オプション） | | |
| 2.2.8　証明書状態情報処理 | | |
| 政府共用認証局は、最新、完全、かつ正確な証明書状態情報（CRL およびその他の証明書状態機構を含む）を証明書利用者および証明書検証者が利用可能であるという合理的な保証を提供する内部統制を保持する | 103 | CRL/ARL を全ての関係者に提供すること |
| | 104 | 政府共用認証局は、リポジトリを用いて CRL/ARL を証明書検証者に提供すること |
| | 105 | 関係者が CRL/ARL の完全性及び発行日を確認できるように、政府共用認証局は発行する CRL/ARL に電子署名すること |
| | 106 | 政府共用認証局は、前回発行から変更が無い場合であっても定期的に CRL/ARL を発行すること |
| | 107 | 少なくとも、失効した証明書の有効期間が満了するまでは、失効済証明書を特定するエントリを CRL/ARL に登録すること |
| | 108 | CRL/ARL をアーカイブすること |
| | 109 | 政府共用認証局は発行する CRL/ARL に単調増加する通し番号（例えば、1、2、3...）を付番すること |
| | 110 | CRL/ARL には、政府共用認証局が発行した失効済かつ有効期間を満了していない全ての証明書に対応するエントリを登録すること |
| | 111 | 政府共用認証局は、古い CRL/ARL を適切な期間に渡り保管すること |
| | 112 | 政府共用認証局は、証明書の有効期間満了、失効にかかわらず、証明書のコピーを適切な期間に渡り保管すること |
| 2.2.9　IC カードライフサイクル管理（オプション） | | |

## 1.3.2 セキュリティ対策（WebTrust for CA 原則 3）

WebTrust for CA 原則 3 における規準(Criteria)のうち政府共用認証局に該当するものをセキュリティ目標とし、コントロール例（Illustrative Controls）のうち政府共用認証局に該当するもの及びリスク分析の結果、必要と判断された対策を、セキュリティ対策として表 1.3-2 のとおり実施する。

なお、ブリッジ認証局についても該当する箇所はこれに準じる。

**表 1.3-2 セキュリティ対策（WebTrust for CA 原則 3）**

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| 3 CA 環境の内部統制<br>3.1 CP/CPS マネジメント | | |
| 政府共用認証局は、CP/CPS の有効性の維持を合理的に保証する内部統制を保持する | 1 | 政府共用認証局は、CP/CPS を規定し、かつ、承認する最終的な権限及び責任を持つポリシー管理機関を持つこと |
| | 2 | ポリシー管理機関(もしくはそれと同等の機関)は、業務に関するリスクを評価し、以下に関して該当する CP 或いは CPS に含まれるべきセキュリティ要件及び業務手続きを決定すること<br>a)鍵ライフサイクル管理<br>b)証明書ライフサイクル管理<br>c)CA 環境の内部統制 |
| | 3 | 政府共用認証局の CP/CPS は、CP/CPS を保持していくための責任も含め、明確化したレビュー手続きにしたがい、承認、かつ、修正されること |
| | 4 | 政府共用認証局は、CP/CPS を全ての証明書利用者及び証明書検証者に利用可能にすること |
| | 5 | 政府共用認証局は、CP/CPS の改訂版を証明書利用者及び証明書検証者に利用可能にすること |
| | 6 | CP が政府共用認証局の CPS にサポートされているということを保証するための明確化されたレビュー手続きが存在すること |
| 3.2 セキュリティマネジメント | | |
| 政府共用認証局は、外部委託業者等によりアクセスされる政府共用認証局の施設、システム、情報資産のセキュリティを維持することを合理的に保証する内部統制を保持する | 7 | 施設内契約業者、取引業者、またジョイントベンチャー等の第三者による政府共用認証局施設、システムへの物理的・論理的アクセスの管理手続を整備すること |
| | 8 | 政府共用認証局の施設、システムに第三者がアクセスする業務上の必要性が生じた場合、セキュリティへの影響及びコントロール要件を決定するためのリスク評価を実施すること |
| | 9 | 第三者による政府共用認証局の施設、システムへのアクセスに関する取り決めは、必要な全てのセキュリティ要件を含んだ正式な契約に基づくこと |
| 政府共用認証局は、政府共用認証局の業務を外部委託する場合、情報のセキュリティを確保することを合理的保証する内部統制を保持する | 10 | システム、ネットワーク及び/又はデスクトップ環境において、管理及び管理手続の全部又は一部を外部委託する場合、政府共用認証局のセキュリティ要求事項は、当事者間で合意される契約書に記述されること |
| | 11 | 政府共用認証局は、政府共用認証局の役割やそれぞれの機能の一部を委託する場合も、CP/CPS の定義及び維持、並びに政府共用認証局が実施する機能の完遂に対する最終的な責任を負うこと |
| 3.3 資産の分類と管理 | | |
| 政府共用認証局は、政府共用認証局の資産や情報に対して、適切な保護レベルを維持することを合 | 12 | 政府共用認証局の全ての主要な情報資産に対して、管理責任者が特定され、管理責任者には適切な管理手続を維持するための責任が割り当てられること |
| | 13 | 重要な政府共用認証局の情報資産の目録が維持されること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| 理的に保証する内部統制を保持する | 14 | 政府共用認証局は、情報共有、又は情報制限に関する業務上の必要性及びそのような必要性に伴う業務上の影響を考慮した情報分類や管理手続を実施すること |
| | 15 | 政府共用認証局が採用した分類体系に従って、情報のラベリングや取扱いが実施されていることを保証する手続を整備すること |
| 3.4　人事セキュリティ | | |
| 政府共用認証局に関する人事及び人事採用は、業務の信頼性を維持することを合理的に保証する内部統制を保持する | 16 | 情報セキュリティの役割及び責任は、職務定義書のなかに明文化すること |
| | 17 | 政府共用認証局の要員（警備スタッフ等の要員含む）の採用において、選別手続等を明文化すること |
| | 18 | 政府共用認証局の要員は、雇用条件の一部として、機密保持誓約書を締結すること |
| | 19 | 政府共用認証局の全ての職員、（関係する場合には）第三者に対して、関連する情報セキュリティ実施手順書、手続について教育を実施すること<br>教育手続には、次の事項を含めること<br>a)役割毎の教育要件と教育手続<br>b)役割毎の再教育期間と再教育手続 |
| | 20 | 鍵管理や証明書管理に従事する政府共用認証局の要員の継続的な信頼性維持のため、定期的なレビューを行うこと |
| | 21 | 情報セキュリティ実施手順書及び手続に違反した政府共用認証局の要員に対する正式な懲戒手続を整備し、実施すること<br>政府共用認証局の方針及び手続では、未承認の行為、未承認の権限の使用、そして未承認のシステムの使用を行なった要員に対する処罰を明文化すること |
| | 22 | 政府共用認証局の要員が退職する際には、情報セキュリティが侵害されないように適切かつ迅速な対応を実施すること |
| 3.5　物理的及び環境的セキュリティ | | |
| 政府共用認証局の施設･設備へのアクセスを承認された個人に制限し、施設・設備を環境面の脅威から保護することを合理的に保証する内部統制を保持する | 23 | 建物や政府共用認証局の施設の周辺にセキュリティ境界(つまり、物理的バリア)を明確に定義し、構築することにより、政府共用認証局は物理的に保護されること |
| | 24 | 政府共用認証局の施設を含む建物やサイトの境界は、物理的に安全であること(簡単に侵入できないように境界には隙間をなくすこと) |
| | 25 | 政府共用認証局の業務を行う建物、又は室へのアクセスを、承認された個人に制限するために、受付やその他の物理的アクセス制御を整備すること |
| | 26 | 承認されていない立ち入りや環境面での汚染を防ぐために、適切に物理的バリア（例えば、二重天井や二重床に対して、実際の天井から実際の床まで拡張された物理的バリア）を設けていること |
| | 27 | 政府共用認証局の施設の周辺におけるセキュリティ境界に設置された防火扉は、警報システムが稼働しており、しっかりと閉められていること |
| | 28 | 政府共用認証局の施設のある建物及び政府共用認証局の施設自体の全ての外部扉を網羅するように、侵入者検知システムを整備し、定期的に動作確認を行うこと |
| | 29 | 政府共用認証局の施設では、無人の際には警報システムを稼働させること |
| | 30 | 政府共用認証局の施設は、物理的に施錠され、無人の際には定期的にチェックがされること |
| | 31 | 安全性の理由からと悪意のある行為を防ぐため、政府共用認証局の施設においては、監督されていない作業は禁止すること |
| | 32 | 政府共用認証局の要員は、部外者を識別する手段を整備し、部外者を見かけた際には身元確認を行うこと |
| | 33 | 政府共用認証局施設へのアクセスは、入退室管理システムにより承認された者のみに制限すること |
| | 34 | 政府共用認証局施設の入退室ログを記録すること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| | 35 | 政府共用認証局施設への訪問者を管理し、入退室日時を記録すること |
| | 36 | サポートサービス業務を行う第三者の政府共用認証局の施設へのアクセスは、必要な場合のみに制限され、そのようなアクセスは承認・モニタされること |
| | 37 | 政府共用認証局施設へのアクセス権は、定期的にレビューされ、更新されること |
| 政府共用認証局は、資産の損失、損害、危殆化、業務の中断を最小限におさえることを合理的に保証する内部統制を保持する | 38 | 政府共用認証局の機器類は、環境の脅威や未承認のアクセスなどのリスクを低減するように、配置され、保護されること |
| | 39 | 政府共用認証局の機器類は、電力の供給停止及びその他の電源異常などから保護されること |
| | 40 | データを伝送するものや政府共用認証局のサービスを支える、電力ケーブル及び通信ケーブルは、妨害や損害から保護されること |
| | 41 | 政府共用認証局の機器類は、可用性及び完全性を保証するために製造業者の説明書やその他の文書化された手続に従い、維持されること |
| | 42 | 記憶媒体を含む全ての機器類は、廃棄・再利用される前に重要な情報が含まれていないかを確認するために検査されること。また、重要な情報を含んだ記憶媒体は、廃棄・再利用する前に物理的に破壊するか、完全に上書きをされること |
| 政府共用認証局は、情報や情報プロセスのための施設･設備を損失や盗難から保護することを合理的に保証する内部統制を保持する | 43 | 取扱いに注意を要する情報や重要な業務情報は、必要ではない時、また、政府共用認証局施設を立ち退く際には、施錠されること |
| | 44 | パーソナルコンピュータやワークステーションは、一時離席時には、ログオンした状態で放置されないこと、及び使用されていない時は、キーロック、パスワード、又は、その他のコントロールで保護されること |
| | 45 | 政府共用認証局に所有権がある機器類、情報、ソフトウェアは、承認なしで政府共用認証局の施設外に持ち出さないこと |
| 3.6　業務マネジメント | | |
| 政府共用認証局は、情報処理設備に関する業務を正確かつ安全に実施することを合理的に保証する内部統制を保持する | 46 | 政府共用認証局の業務手続は、明文化し、維持すること |
| | 47 | 政府共用認証局の機器類、ソフトウェア、及び業務手続を変更する際の正式な管理手続及び管理責任を明確にすること |
| | 48 | 情報またはサービスに関する未承認の修正や誤用の機会を低減するため、職務や管理責任領域を分離すること |
| | 49 | 開発・テスト環境は、本番環境と分離すること |
| | 50 | 外部の施設管理サービスを利用する場合には、事前にリスクを識別し、必要なコントロールを業者との間で合意し、契約に含めること |
| 政府共用認証局は、システム障害のリスクを最小限におさえることを合理的に保証する内部統制を保持する | 51 | キャパシティ需要は監視され、適切な処理能力と記憶容量の利用を確実にするために、将来のキャパシティ要件を決定すること |
| | 52 | 新規の情報システム、更新および新バージョンの導入に関する受入基準は確立され、受入前に適切なシステムの検査を実施すること |
| 政府共用認証局は、システムや情報の完全性をコンピュータウイルスや悪意のあるソフトウェアから保護することを合理的に保証する内部統制を保持する | 53 | コンピュータウイルスや悪意のあるソフトウェアから保護するための検知・防止のコントロール、及び適切に利用者に認知させる手続を導入すること |
| 政府共用認証局は、セキュリティに関する侵害、機能不全による損害を、事故報告と対応手続きによって最小限におさえる | 54 | 事故報告を受けた時に取るべき行動を明記した事故対応手続とともに、正式な報告手続が存在し、遵守されること |
| | 55 | 政府共用認証局システムの利用者は、システム又はサービスに関する弱点・脅威が、発見もしくは疑われた場合には記録を取り、定められた報告先に報告すること |
| | 56 | ソフトウェアの不具合に関する報告手続は明文化され、遵守されること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| ことを合理的に保証する内部統制を保持する | 57 | 欠陥が報告され、改善が行われることを保証する手続を明文化され、遵守されること |
| | 58 | インシデントや機能不全の種類、大きさ、及びコストは、計量化され、モニタされること |
| | 59 | セキュリティ事件・事故に対して、迅速、効果的、かつ、整然とした対処の実施を保証するために、事件・事故管理の管理責任及び手続が確立され、遵守されること |
| 政府共用認証局は、損害、盗難、未承認のアクセスから情報媒体を保護するため、情報媒体を安全に取扱うという合理的な保証を提供する内部統制を保持する | 60 | 取外し可能な記憶媒体の管理に関する手続には、次の事項を含めること<br>a)不必要になった場合、取り除かれるべきである再利用可能な媒体の中身は消去される<br>b)媒体を破棄する場合には、承認を必要とし、監査証跡を確保するために破棄記録は保管される<br>c)全ての媒体は、製造者の仕様書の基づき、安全かつセキュリティが確保された環境で保存される |
| | 61 | 媒体は必要でなくなった時には、安全かつ適切に廃棄されること |
| | 62 | 承認されていない開示もしくは誤用から情報を保護するため、情報の取扱いまたは保存に関する手続が確立され、遵守されること |
| | 63 | システムに関する文書は、承認されていないアクセスから保護すること |
| 3.7　システムアクセス制御 | | |
| 政府共用認証局は、システムに対して、承認された要員に対してのみアクセスを許可することを合理的に保証する内部統制を保持する<br><br>ユーザアクセス制御 | 64 | アクセス制御ポリシーにおいて、アクセス制御に対する業務要件は定義され、明文化されること<br>また、最低限、次の事項が含まれること<br>a)役割と対応するアクセス許可<br>b)各ユーザの認証・識別手続き<br>c)職務の分離<br>d)特定の認証局業務を遂行するために必要な人員数 |
| | 65 | 政府共用認証局のシステムやサービスへのアクセス権限を与える正式なユーザ登録及び登録削除の手続が確立され、遵守されること |
| | 66 | 特権の割当てや使用は、制限され、管理されること |
| | 67 | パスワードの配付は、正式な管理手続を通して管理されること |
| | 68 | ユーザのアクセス権限は、一定期間毎にレビューされること |
| | 69 | ユーザは、パスワードの選択や使用に関して、明確化された方針や手続に従うこと |
| | 70 | ユーザは、一時的に使用されていない機器類を適切に保護すること |
| ネットワークアクセス制御 | 71 | ユーザは、使用が許可されているサービスに限り、直接のアクセスが許可されること |
| | 72 | ユーザが利用する端末からサーバ等の提供するサービスへの経路は制御されること |
| | 73 | 遠隔地からの利用者のアクセスには、認証を行うこと |
| | 74 | 遠隔地のシステムへの接続には、認証を行うこと |
| | 75 | 診断ポートへのアクセスは、安全に管理されること |
| | 76 | 第三者による外部ネットワークドメインからCAの内部ネットワークドメインを守るためのコントロールがあること<br>（例えばファイアウォール） |
| | 77 | 政府共用認証局のアクセス制御ポリシーに従って、ユーザが利用可能なサービス(例えばHTTP、FTP)を制限すること |
| | 78 | コンピュータ接続や情報の流れが、組織の業務アプリケーションのアクセス制御ポリシーに違反していないということを保証するルーティングコントロールがあること |
| | 79 | 政府共用認証局が利用している全てのネットワークサービスのセキュリティ特質は、政府共用認証局により明文化されること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| オペレーティングシステムアクセス制御 | 80 | 特定の場所及び持ち運びできる機器類への接続を認証するために、自動端末識別を行うこと |
| | 81 | 政府共用認証局システムへの接続は、セキュアなログオンプロセスを利用すること |
| | 82 | 全てのユーザは、その活動の責任を後で追跡できるように、個人ごとに一意な識別子（ユーザ ID）を保有すること |
| | 83 | パスワード管理システムは、パスワードの品質を保証するために、効果的な対話型の機能を提供すること |
| | 84 | システムユーティリティプログラムの利用は、制限され、厳格に管理されること |
| | 85 | 政府共用認証局システムで使用する端末は、承認されていない者の利用を防ぐために、未使用の一定時間後にタイムアウトすること |
| | 86 | リスクの高いアプリケーション（府省等登録局のシステムを含む）に対して、接続時間の制限による追加のコントロールを提供すること |
| アプリケーションアクセス制御 | 87 | 情報やアプリケーションシステム機能へのアクセスは、アクセス制御ポリシーに従い、制限されること |
| | 88 | 重要なシステムは、専用の(隔離された)コンピュータ環境を必要とすること |
| 3.8　システム開発と保守 | | |
| 政府共用認証局は、システムの完全性を維持するために、適切な承認が行なわれた上でシステム開発及び保守を行うことを合理的に保証する内部統制を保持する | 89 | 新規及び既存システムの改善のための業務要件には、コントロールに関する要件が明文化されること |
| | 90 | 運用システム上でソフトウェアを導入する際の変更管理手続は明文化され、遵守されること |
| | 91 | 予定されたソフトウェアのリリースや修正のための変更管理手続が明文化され、遵守されること |
| | 92 | 緊急のソフトウェア修正のための変更管理手続が明文化され、遵守されること |
| | 93 | テストデータは、保護され、管理されること |
| | 94 | プログラムソースライブラリへのアクセスに対する厳格なコントロールが維持されること |
| | 95 | 情報システムの改悪によるリスクを最小化するため、変更は正式な変更管理手続の実施により厳格に管理すること |
| | 96 | OS の変更が発生した際には、アプリケーションシステムのレビュー及びテストを実施すること |
| | 97 | パッケージソフトウェアの変更は極力行わないようにし，絶対に必要な変更は厳しく管理すること |
| | 98 | 隠れチャネル及びトロイの木馬の危険性から保護するために、ソフトウェアの購入、使用及び修正を管理し、検査すること |
| | 99 | 委託先によるソフトウェア開発は安全に管理されること |
| 3.9　事業継続管理 | | |
| 政府共用認証局は、災害時における、業務の継続性を確保することを合理的に保証する内部統制を保持する | 100 | 政府共用認証局は、事業継続計画の作成及び維持のための管理手続を整備すること |
| | 101 | 政府共用認証局は、適切なリスク評価に基づき、事業継続計画を作成すること |
| | 102 | 政府共用認証局は、重要な業務の障害、もしくは機能停止時、速やかに運用を維持もしくは復旧させるための事業継続計画を作成すること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| | 103 | 事業継続計画には、次の事項を含むこと<br>a)計画を発動するための条件<br>b)緊急時の手続き<br>c)フォールバック手続き<br>d)回復手続き<br>e)保守計画<br>f)意識付けと教育のための要件<br>g)各要員の責任 |
| | 104 | 事業継続計画は、最新かつ有効なものであるという保証を得るため、定期的にテストを実施すること |
| | 105 | 事業継続計画は、定期的な見直しにより保持され、継続的な有効性を保証するために更新を実施すること |
| | 106 | 事業継続計画では、許容可能なシステム停止時間、システム復旧時間及び平均故障時間を明確にすること |
| | 107 | 政府共用認証局の事業継続計画は、ハードウェア、ソフトウェア及び鍵等の政府共用認証局システムの全ての重要な構成要素に関して、それらの構成要素の 1 つまたはそれ以上に障害が発生した場合の災害復旧手続を含むこと |
| | 108 | 政府共用認証局の事業継続計画は、電算リソース、ソフトウェア、データが改ざんされた、又は改ざんされたおそれがある場合に使用される復旧手続を記述すること |
| | 109 | 自然災害、又はその他の災害の後で、現所在地もしくは遠隔ホットサイトに安全な環境が再構築されるまでの間に施設を安全に維持する手続が、政府共用認証局の事業継続計画には含まれること |
| | 110 | 重要な業務情報やソフトウェアは定められた手順に従ってバックアップが取得されること。これらのバックアップの情報セキュリティ要件は、バックアップ元の情報に対するコントロールと一致させること |
| | 111 | フォールバック装置とバックアップ媒体は、メインサイトの災害からの損害を避けるため、十分に安全な距離をおいた場所に設置すること |
| 政府共用認証局は、署名用秘密鍵の危殆化が生じた際に業務の継続性を確保することを合理的に保証する内部統制を保持する | 112 | 政府共用認証局の事業継続計画は、政府共用認証局の秘密鍵の危殆化、もしくはその疑いがあるものを災害として扱うこと |
| | 113 | 政府共用認証局の秘密鍵の危殆化もしくはその疑いがある場合、災害復旧手続には政府共用認証局秘密鍵により署名された全ての証明書失効と再発行を含むこと |
| | 114 | 政府共用認証局秘密鍵が危殆化し、公開鍵を失効する際に実施される復旧手続には、次の事項を含むこと a)どのように安全な環境が再構築されるか b)どのように政府共用認証局の古い公開鍵は失効されるか c)どのように政府共用認証局の新しい公開鍵はユーザに配付されるか d)どのように主体者は再度認証されるか |
| | 115 | 政府共用認証局の秘密鍵を更新しなければならない場合、次の安全かつ認証された失効のため手続を定めること<br><br>a)古い政府共用認証局の公開鍵<br>b)危殆化した秘密鍵に基づいて政府共用認証局により発行された全ての証明書 |
| | 116 | 鍵の危殆化に関する政府共用認証局の事業継続計画には、誰に報告し、システムソフトウェア、ハードウェア、共通鍵、非対称鍵、以前に生成された署名及び暗号データに対して、どんな行動を取るかが定められていること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| 政府共用認証局は、業務終了による利用者や証明書検証者への潜在的な中断を最小限におさえることを合理的に保証する内部統制を保持する | 117 | 政府共用認証局は、業務終了のための手続、影響を受けるエンティティへの通知手続、関連する政府共用認証局記録のアーカイブを管理者に転送する手続を整備すること |
| 3.10　監視と準拠 | | |
| 政府共用認証局は、法的要件に対する準拠性を確保することを合理的に保証する内部統制を保持する | 118 | 政府共用認証局のシステムについて、すべての関連する法令、規制及び契約上の要求事項を、明確に定め、文書化すること |
| | 119 | 知的所有権がある物件を使用する場合及び所有権があるソフトウェアを使用する場合は、法的制限事項に適合するように適切な手続を実行すること |
| | 120 | 組織の重要な記録は、損失、破壊、改ざんから保護されること |
| | 121 | 関連する法令等に従って個人情報を保護するためのコントロールを整備すること |
| | 122 | 情報処理施設の使用には管理者の認可を要するものとし、そのような施設の誤用を防ぐためのコントロールを整備すること |
| | 123 | 国家間の合意、法令、規制、及び暗号管理策へのアクセス、又は暗号管理策の使用を管理するその他の規制に対する準拠を保証する管理策が存在すること |
| | 124 | 政府共用認証局の機密に関する方針と手続きには次の事項を明記すること<br>a)政府共用認証局、もしくは府省等登録局により機密情報として扱われるべき情報の種類<br>b)機密情報ではないと考えられる情報の種類<br>c)証明書の失効、或いは一時停止の理由を知らされるべき権利のある人<br>d)法的強制力のある機関への情報のリリースに関するポリシー<br>e)民事上の開示の一環として明かされうる情報<br>f)政府共用認証局もしくは、府省等登録局が、所有者のリクエストにより情報の開示をする条件<br>g)機密性のある情報が開示されうるその他の状況 |
| 政府共用認証局は、情報セキュリティ実施手順書や手続きへの準拠を維持することを合理的に保証する内部統制を保持す | 125 | 管理者は、自分の責任範囲におけるすべてのセキュリティ手続が正確に実施されていることを保証すること |
| | 126 | 政府共用認証局の業務は、セキュリティポリシーや基準への準拠を保証するために定期的なレビューを実施すること |
| | 127 | 政府共用認証局のシステムは、セキュリティの実行基準への準拠性を定期的に検査すること |
| 政府共用認証局は、システム監査プロセスの有効性を維持し、システム監査への（もしくは、システム監査からの）影響を最小限におさえることを合理的に保証する内部統制を保持する | 128 | 運用システムの監査は、業務プロセスへの妨げとなるリスクを最小化するなどのため、計画され、同意されること |
| | 129 | システム監査ツールへのアクセスは、不正使用や危殆化を防ぐために保護すること |
| 政府共用認証局は、未承認のシステム利用を発見することを合理的に保証する内部統制を保持する | 130 | 政府共用認証局システムの使用を監視する手続を確立し、監視活動の結果を定期的にレビューすること |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| 3.11　事業の記録 | | |
| 政府共用認証局は、環境、鍵管理、証明書管理に関する事象を正確かつ完全に記録することを合理的に保証する内部統制を保持する | 131 | 政府共用認証局は、事象の記録をシステム的に、もしくは手動で適切に作成すること |
| | 132 | 全ての事象の記録には、次の事項を含むこと<br>a)記録時の日付と時間<br>b)記録のシリアルナンバーとシーケンシャルナンバー（自動採番のため）<br>c)記録の種類<br>d)記録のソース<br>e)事象の記録を作成したエンティティの特定 |
| | 133 | 政府共用認証局は、次の鍵ライフサイクル管理に関する事項に関して記録を取ること<br>a)政府共用認証局の鍵生成<br>b)政府共用認証局の鍵バックアップ<br>c)政府共用認証局の鍵保管<br>d)政府共用認証局の鍵回復<br>e)政府共用認証局鍵使用<br>f)政府共用認証局の鍵アーカイブ<br>g)鍵に関する情報のサービスから鍵の取り出し<br>h)政府共用認証局の鍵廃棄<br>i)鍵管理業務を承認しているエンティティの特定<br>j)鍵に関する情報（例えば、鍵の構成要素、持ち運びのできる装置、媒体に保存された鍵など）を取り扱うエンティティの特定<br>k)鍵や鍵を保存した装置もしくは媒体の保管<br>l)秘密鍵の危殆化 |
| | 134 | 政府共用認証局は、次の証明書ライフサイクル管理に関した記録を取ること<br>a)証明書の依頼の受取―証明書発行依頼、更新依頼、鍵更新依頼<br>b)証明書のための公開鍵の提出<br>c)エンティティの属性変更<br>d)証明書の作成<br>e)政府共用認証局の公開鍵の配布<br>f)証明書失効依頼<br>g)証明書失効リストの作成と発行<br>h)証明書の期限切れに伴う行動 |
| | 135 | 政府共用認証局は、次の暗号装置ライフサイクル管理に関して記録を取ること a)装置の受入れ b)保管庫からの出し入れ c)装置の使用 d)装置の撤去 e)サービスや修正のための装置の指定 f)装置の廃棄 |
| | 136 | 政府共用認証局は、次の証明書発行申請情報について記録を取ること（もしくは、府省等登録局に記録を取るように要請すること）<br>a)申請者を示す人物照合のための文書<br>b)特有の人物照合のデータ、数字、それらの組み合わせ<br>c)申請書と人物特定文書のコピーの保管場所<br>d)申請書を受入れるエンティティの特定<br>e)（ある場合には）人物特定文書の正当性を確認する方法<br>f)証明書申請を提出した府省等登録局 |

| セキュリティ目標 | 項番 | セキュリティ対策 |
|---|---|---|
| | 137 | 政府共用認証局は、次のセキュリティの重要な出来事について記録を取ること<br>a)事象の記録に含まれたセキュリティ重要ファイルや記録に関する読込み及び書き出し<br>b)重要なセキュリティデータの削除<br>c)セキュリティプロフィールの変更<br>d)本人識別と本人認証手法の利用<br>（成功及び失敗の記録を含み、失敗には複合的な認証の不成功も含む）<br>e)システムクラッシュ、ハードウェアの故障、又は、その他の機能不全<br>f)コンピュータオペレータ、システムアドミニストレータ、システムセキュリティ管理者の行為<br>g)エンティティの属性変更<br>h)暗号化・人物認証プロセスもしくは手続きをバイパスするための決定<br>i)政府共用認証局システムやその他の構成要素へのアクセス |
| | 138 | 事象の記録には、いかなる秘密鍵の平文テキストも記録しないこと |
| | 139 | 政府共用認証局システムの時間は、正確な記録のために同期されること |
| 政府共用認証局は、現在のもしくは保存されている事象の記録の機密性と完全性を維持することを合理的に保証する内部統制を保持する | 140 | 現在及びアーカイブされた事象の記録は、未承認の修正や廃棄から保護すること |
| | 141 | 現在及びアーカイブされた事象の記録は、修正や置換から保護すること |
| | 142 | 事象の記録の署名に使われる秘密鍵は、他の目的では使わないこと |
| 政府共用認証局は、開示された業務規定に従い、事象の記録の正確性及び機密性を確保することを合理的に保証する内部統制を保持する | 143 | 政府共用認証局は、定期的に事象の記録をアーカイブすること |
| | 144 | 事象の記録の適切な保管期間を決めるためにリスク評価を実施すること |
| | 145 | 政府共用認証局は、あらかじめ決められた期間、安全なオフサイトに、事象の記録を保存すること |
| 事象の記録は、適切な責任者に定期的にレビューされるということを合理的に保証する内部統制を保持する | 146 | 現在及びアーカイブされた事象の記録は、正当な業務のため、又は、セキュリティ上の理由のために、承認された者以外は検索できないようにすること |
| | 147 | 事象の記録は、定期的にレビューすること |
| | 148 | 現在及びアーカイブされた事象の記録のレビューは、事象の記録の完全性の確認、例外、未承認及び疑わしい行為の特定とフォローアップを含むこと |

### 1.3.3 セキュリティ要件（情報セキュリティポリシー）

情報セキュリティポリシーに従って、セキュリティ対策を実施する。

## 1.4 個人情報保護対策

### 1.4.1 政府認証基盤において取り扱う個人情報

政府認証基盤において取り扱う個人情報としては、次に示す個人に関する情報が存在する。いずれも内容は氏名、所属、役職、所属組織の連絡先（住所､電話番号､FAX 番号）であり、携帯電話番号が含まれる場合がある。

政府認証基盤、府省等登録局（LRA）の要員
証明書利用者及び申請者
保守員、監査人及びその他委託先の従業員

### 1.4.2 個人情報保護対策

個人情報の取得、利用、提供、開示、訂正及び利用停止は、「行政機関の保有する個人情報の保護に関する法律（平成十五年五月三十日法律第五十八号）」及び「行政機関の保有する個人情報の保護に関する法律施行令（平成十五年十二月二十五日政令第五百四十八号）」に基づき、適切に行う。

また、個人情報は要機密情報として格付し、漏えい、滅失又はき損を防止する措置を講じる。

参照資料２

# 政 府 認 証 基 盤

# 施設･設備の詳細仕様

## １　建物の要求要件仕様

政府認証基盤を設置する建物（以下「建物」という。）は、財団法人日本品質保証機構の行う「情報処理サービス業情報システム安全対策実施事業所認定第４条第１項第１号に掲げる事項に係わる安全対策に関する検査」又は「情報セキュリティマネジメントシステム（ＩＳＭＳ）適合性評価制度」に合格し、同機構の発行する安全対策事業所認定を取得していること、もしくはそれと同等の安全対策が実現されていることを証明すること。ISO27001（ISMS）、ISO22301（BCMS）、JISQ15001（Pマーク）の認証を受けていること。また、「電子署名及び認証業務に関する法律に基づく特定認証業務の認定に係る指針（平成１３年総務省 法務省 経済産業省告示第２号）」の第四条から第七条までの条項を満たしていること。

さらに、建物は次の条件を満足していること。

Ａ　立地

マスタセンタは、中央合同庁舎第 2 号館（東京都千代田区 2-1-2）から直線距離で 30km 圏内であり、公共交通機関（タクシーを除く。）及び徒歩を利用しておおよそ 60 分以内で到着できる場所であること。

東京都道318号環状七号線よりも外側(東京都地域防災計画において大震災時に流入禁止区域として指定されている地域よりも外側)であること。

公共交通機関による複数のアクセス経路が確保できること。

バックアップセンタは、マスタセンタと同時被災しない場所であるとともに、業務継続性を考慮した場所に設置すること。

Ｂ　耐震性

政府認証基盤関連設備（以下「認証設備」という。）を設置する室（以下「認証設備室」という。）は、震度６強以上の地震に耐えられる免震構造の建物であること。

現行建築基準法に基づいた耐震・防振等の構造上の安全性を配慮した設計・施工が行われていること。旧建築基準法に基づき設計・施工されている場合には、耐震安全診断を行い、現行建築基準法に基づいた耐震･防振等の構造上の安全性を確保するための補強が行われていること。

データセンターを利用する場合、日本データセンター協会が定めている「データセンタ

ーファシリティスタンダード（データセンターファシリティスタンダードの概要(日本データセンター協会　2010年10月18日）（ https://www.jdcc.or.jp/pdf/facility.pdf ）基準項目一覧表）」の分類「建物（B）」のティア４の項目を満たすこと。

なお、認証業務に係る機器等の稼働に直接影響を与えない監視室及び事務室が入る建物については、耐震構造なども可とする。

C　火災予防

建物は、揮発物等爆発の危険性が高いものを取り扱う施設からはなれた火災の被害を受けるおそれの少ない場所に設置されていること。また、隣接建物から離れているなど延焼の危険性が低い場所に設置されていること。

D　水害予防

建物は、海、湖、河川からはなれた水害のおそれの少ない場所に設置されていること。また、建物設置場所は、過去５０年間において津波、高潮、集中豪雨等による水害が発生したことがないこと。さらに建物の全ての開口部は地面より高くなっていること。
これらの条件が満たされない場合は、建物が水害の影響を受ける恐れのないよう必要な措置を行うこと。

E　落雷被害予防

建物は、標高２００ｍ未満の地域等の落雷の被害を受けるおそれの少ない場所に設置されていること。

また、避雷設備が設置され、雷サージによる電気設備機器の破損を防止できるような構造になっていること。

F　電磁波被害予防

建物は、マイクロ回線、レーダー施設、送電線、強電実験室等から５０ｍ以上はなれているなど、電界及び磁界の被害を受けるおそれの少ない場所に設置されていること。

これらの条件が満たされない場合は、認証設備室の全体を遮蔽して電磁波の影響を受けないようにすること。また、電源線、通信回線の出入口にノイズフィルターを設置し、あるいは電源線にシールド付ケーブルを使用し、ノイズによる影響を防止すること。

G　空気汚染・塩害被害予防

建物は、空気汚染及び塩害による被害を受けるおそれの少ない場所に設置されていること。

この条件が満たされない場合は、認証設備室が空気汚染及び塩害による被害を受けないよう必要な措置を行うこと。

H　出入口の設置位置

建物の出入り口には、無権限者の立入りが不可能なセキュリティ対策が講じられていること。

認証設備室への入室者はあらかじめ登録された者からの事前申請によるものとし、

２４時間３６５日有人による本人確認を行うこと。

I　災害発生時の避難対策

(a) 非常口の設置

非常口が適切な位置に設置されていること。非常口は、建物内のどの場所からでも二方向に避難できる位置に設置され、災害時の避難及び救助活動が円滑に行えること。

(b) 非常照明設備の設置

非常照明設備が設置され、災害時の避難誘導を安全かつ迅速に行えること。また、建物内のどの位置からでも判別できるように、避難口誘導灯及び誘導標識判別が設置されていること。電源は常用電源が断たれた場合のために、自動的に切り替わる予備電源が設置されていること。

## 2　認証設備室の要求要件仕様

（1）　施設規模要件仕様

次のような施設規模の認証設備室を提供すること。

| 室名 | マスタセンタ<br>最低限の広さ | バックアップセンタ<br>最低限の広さ |
|---|---|---|
| 室扉のある廊下 | 適宜 | 適宜 |
| セキュア室前室<br>セキュア室 | 20 ㎡ | 20 ㎡ |
| オペレーション室 | 10 ㎡ | 10 ㎡ |
| 関連サーバ室 | 35 ㎡ | 35 ㎡ |
| テストセンタ室 | 40 ㎡ | ― |

また、マスタセンタには次のような監視室および事務室を提供すること。

| 室名 | 最低限の広さ |
|---|---|
| 監視室 | 40 ㎡ |
| 事務室 | 150 ㎡ |

セキュリティレベル要件は、別途閲覧に供するセキュリティレベル要件を参照。

（2）　施設設備要求要件仕様

認証設備室は、次のような要件を満足するものであること。

A　床・天井の構造

認証設備室の床面及び天井には、以下の措置が講じられていること。

・床荷重設計は、１０００kg/㎡以上とすること。
ただし、架台により荷重分散する場合は、５００kg/㎡以上とする。

・床面はフリーアクセス床とすること。

・フリーアクセス床は、地震発生時に破損しない構造とし、落ち込み等による機器類及び人身の被害を防止されていること。

・床面には認証設備室に設置する機器について移動・転倒防止の措置を施すことができること。

・フリーアクセス床の主要部分(床パネル、支柱、ジョイント等)には不燃材が使用されていること。

B　漏水対策

認証設備室は、最上階等天井からの漏水等のおそれがある場所に設置されていないこと。漏水等のおそれがある場合は、天井部分からの漏水を防止する措置が講じられているとともに、漏水検知器の設置など機器に対する漏水対策が講じられていること。

C　遮光措置

認証設備室は、建物の外部から直接光が入らない構造とすること。

D　避難及び保守空間の確保

認証設備室の各室には、それぞれ避難及び保守のための空間が確保されていること。

E　電話機の設置

認証設備室の各室（廊下を除く。）には、それぞれ 1 台以上の電話機が設置されていること。

F　火災対策

(a) 耐火性能

認証設備室は、建築基準法に規定する耐火性能を満たしていること。

(b) 延焼防止措置

認証設備室は、専用の防火区画とし、火災の延焼を防ぐ措置が取られていること。

(c) 内装等

認証設備室の内装（壁・床・天井）、各種間仕切壁には、不燃材が使用されていること。ただし、床表面が不燃材でない場合には、防炎処理が施されていること。

防火区画壁を貫通する配管は、両側を不燃材で被覆されていること。

防火区画の扉は甲種防火仕様の鉄扉又はこれと同等以上の強度を有すること。

(d) 消火設備

認証設備室には、窒素、ハロン等による機器等への影響がない消火設備が設置されていること。また、消火設備は次の仕様を満たしていること。

・消火剤の噴出は、防火区画毎に独立して行うこと。また、室の天井がシステム天井の場合には、消火ガス噴出による天井の破損を回避するために、消火時には天井裏にも適切な量の消火ガスを噴出し天井上下間の気圧差を緩和すること。

・消火器は熱感知センサー・煙感知センサーの両方が同時に感知しないと噴出しないように設定されていること。また、消火剤の噴出の制御を可能とすること。

(e) その他

認証設備室には、次の設備が設置されていること。

・熱感知器・煙感知器を用いた自動火災報知設備

・温度・湿度を監視できる設備

・火災時の煙や消火ガスを排出するための排煙設備

・早期に火災を検知できる超高感度煙検知システム

G　損傷対策

認証設備室の内装には、機器等に対する損傷防止の措置が講じられていること。また、室内の照明器具には落下及び損傷防止の措置が講じられていること。

H　セキュリティ対策

(a) 監視カメラ

認証設備室には、監視カメラが設置され、不正な侵入及び室内における不正行為の有無が２４時間監視及び録画されていること。また、監視カメラの設置位置については、室内の撮影において死角がないこと。

(b)　モニタ・録画装置

監視カメラ用のモニタ・録画装置は、認証設備室以外のセキュリティ管理された室に設置されていること。また、録画した媒体は１ヶ月間保管されていること。

(c)　入退室管理

認証設備室の各出入口には入退室管理を行う設備が設置され、入退室の状況が常に次に示す機能を有する入退室管理システムにより把握されていること。

・個人識別機能（暗証番号、個人認証カード、生体認証）

・アクセス者、日時、鍵区分、不正アクセスの記録機能

・扉の自動施錠・解錠機能

なお、入退室管理システムの設定、制御等を行う機器は、認証設備室以外のセキュリティ管理された室に設置されていること。

(d) 扉の強度

認証設備室の扉、枠、錠は、甲種防火仕様の鉄扉又はこれと同等以上の強度を有すること。

(e)その他

認証設備室には、外部に直接面した窓、扉等が設置されていないこと。

## ３　空調設備仕様

空調設備は、次のような条件等を満足するものであること。

A　空調設備の性能

温度が２０℃から２６℃まで、湿度が３０％から７０％までにそれぞれ保たれていること。

B　塵埃除去フィルタ

汚染物質及び塩分等の室内に対する浸入を防止するために、空調設備には塵埃除去フィルタが設置されていること。また、塩害のおそれがある場合は塩分除去装置が設置されていること。

C　監視

空調設備が設置された室については、温度及び湿度並びに空調設備の作動状況の常時検知･監視が行われていること。また、監視記録は３年間保管されていること。

D　火災対策

空調設備の配管・ダクト類は、圧力の変動や火災による機器の損傷を防止するため耐圧性、耐火性に優れた材質を使用し、さらに不燃材で被覆していること。また、フィルタに使用する断熱材も不燃性とし、火災時の煙や有毒ガスから人命の保護を図るとともに、設備の損傷を防止していること。

E　地震対策

空調設備を設置する場合は、地震による被害を防止するため、架台を建物床スラブに固定すること。

E　漏水対策

空調設備の水漏れ防止措置を講じるとともに、漏水のおそれがある場所には漏水感知機等が設置されていること。また、空調設備の配水管が壁を貫通する場合は、設備設置室の直前に止水弁を設置し、開閉方向の表示及び常時開又は常時閉の表示がされていること。

G　防犯対策

空調設備の室内機は防犯設備を完備した室内に設置され、室外機は施錠管理された区画に設置されていること。

H　冗長性

空調機の予備機を有すること。

## 4　電気設備仕様

認証設備のうち、マスタセンタには、常時１５０ＫＶＡ以上、バックアップセンタには、常時１００ＫＶＡ以上の電力が供給されること。また、電力系統の事故や電気設備自体の故障により、電気の瞬断、瞬時電圧低下、電圧変動、周波数変動、停電が発生した場合でも、無停電で良質な電力を供給できるよう、次のような対策が講じられていること。

A　予備電力供給

(a) 予備線

電力会社からの引き込み線は本線及び予備線の２系統を備え、大規模停電時においても認証設備への電力供給が停止しないようになっていること。

(b) 自家発電

停電時でも認証設備が正常に機能するような能力を有する自家発電設備及びＵＰＳ等の無停電電源装置を冗長構成にて適切に設置していること。また、これらの性能は建築基準法、消防法に準拠していること。

自家発電設備に対し、災害時優先補給契約(優先的に燃料供給が受けられる契約）を燃料供給会社と結んでいること。

B　電圧変動防止対策

認証設備に電力を供給する電源変圧器は、それ以外の回路（エレベータ等）に接続していないこと。また、電源変圧器の容量は、負荷全体の１０％程度の余裕が確保されていること。

C　分電盤の防犯対策

認証設備に使用する分電盤は、それ以外の回路に接続していないこと。また、この分電

盤は認証設備室内に設置され、適切な操作性及び保守性が確保されていること。

D　事故防止対策

電気設備について年一回の法定点検が実施されていること。また、電力供給を停止しないで法定点検が実施できていること。

E　地震対策

次のような地震対策が講じられていること。

・重量物(変圧器、自家発電機、ＵＰＳ等)は建物構造体に固定すること。

・蓄電池は架台を強化し建物構造体に固定すること。

・軽量機器(分電盤等)は、床又は壁に固定すること。

・配線用の室内ケーブルの長さには十分余裕を確保し、ケーブルと機器・設備の接続点を固定すること。

F　落雷対策

配電線等から侵入する雷サージによる電気設備機器の破損を防止するため、次のような対策が講じられていること。

・高圧電路には避雷器を設置すること。

・低圧電路には避雷器、電源保護用保安器又は異常電圧吸収装置を設置すること。

G　その他の防災対策

その他の防災対策として以下の対策が講じられていること。

分電盤の主回路には、地絡を検知し警報を発する装置又は自動遮断する装置を設置すること。

過電流遮断器及び漏電遮断器は、当該回路の電源側に設置されているものと同期する様に設計し、回路で事故が発生した際の停電範囲を最小限にすること。

電気設備室から分電盤までの配線には、防火、防犯、ノイズ防止等の措置を講じること。

H　防犯対策

電気設備の室内機は防犯機能を完備した電気設備室内に設置され、室外機は施錠管理された区画に設置されていること。

## ５　サーバラック設備仕様

認証設備室に設置するサーバラックは、耐震性を考慮した設計であるとともに、次の耐震措置が講じられていること。

荷重条件（水平方向 1.0〔G〕鉛直方向 0.5〔G〕）において安全率 1.2 以上が確保されていること。

・引抜力、せん断力において「M12」以上床固定用ボルトが使用されていること。

・ラックは建物床スラブに固定されていること。

## ６　通信回線設備仕様

マスタセンタのインターネット接続は、複数の通信業者が提供する１０Ｍｂｐｓ保障の帯域を最低２回線及び、１０Ｍｂｐｓの回線を最低１回線準備すること。

バックアップセンタは、１Ｍｂｐｓの回線を最低２回線準備すること。

インターネット接続機器及びその回線は請負業者が準備し、セキュリティレベル及びサービスレベルを協議し、保障すること。

マスタセンタとバックアップセンタ間は政府共通ネットワーク[i]を利用するため、両センタは政府共通ネットワーク回線の引き込みが可能であること。

政府共通ネットワークの接続機器及びその回線は、政府共通ネットワークで用意するが、回線引き込みに係る経費については、請負事業者が負担すること。

建物への引き込み経路及び建物内のネットワーク経路(MDF室、IDF室等を含む。)は、冗長性を確保するため複数経路となっていること。

## ７　その他の条件

・建物及び認証設備室は、入室権限を有する者が必要に応じ２４時間３６５日随時入室できること。

[i] 政府共通ネットワークとは、府省等を接続する政府内の専用ネットワークである。

参照資料3

# 秘密情報保護・管理要領

第１　目的

　請負業務において請負業者が取扱う秘密情報について、その適正な保護・管理のための取扱いを明確に定めることを目的とする。

第２　適用範囲

１.請負業務の実施に当たって請負業者が取扱う書面､電磁的記録等のすべての情報のうち、主管係が秘密情報であることを明確にしたものを対象とする。

２.前項の規定にかかわらず､次の各号の一に該当することを請負業者が証明する情報については、本要領における秘密情報として取り扱わないものとする。

⑴ 開示の時に、既に公知であった情報または既に受託事業者が保有していた情報。

⑵ 開示後、受託事業者の責によらず公知となった情報。

⑶ 受託事業者が、秘密保持義務を負うことなく、第三者から適法に入手した情報。

⑷ 受託事業者が独自に開発したパッケージソフトウェア。

第３　請負業者が遵守すべき事項

１　一般的遵守事項

（１）秘密保持

　請負業者は､主管係の承諾を得ることなく秘密情報をいかなる第三者に対しても開示、又は漏えいしないこと。

（２）善管注意義務

　請負業者は、秘密保持義務を遵守するため、善良なる管理者の注意をもって秘密情報を管理すること。

（３）目的外使用の禁止

　請負業者は、主管係の承諾を得ることなく、秘密情報を請負業務以外の目的に一切使用しないこと。

２　請負作業開始前の遵守事項

（１）秘密情報取扱者等の指定

　請負業者は、秘密情報を取扱う者（以下「秘密情報取扱者」という。)、及び秘密情報取扱者を統括する者であり情報システムに精通した課長相当職以上の者（以下「秘密情報取扱責任者」という。）を指定し、その所属、役職及び氏名等を記載した名簿を作成すること。

　なお、秘密情報取扱者及び秘密情報取扱責任者（以下「秘密情報取扱者等」という。）

は、秘密情報の取扱いに関する社内教育等を受講した者とし、その受講実績も併せて名簿に記載すること。

（２）秘密情報取扱者等への教育・周知

請負業者は、本要領の内容に関して、秘密情報取扱者等に対する教育・周知を行うこと。

（３）秘密情報に関する規定の策定

ア　秘密情報の複製等における取扱方法

請負業者は、秘密情報の複製、破棄、保管場所の変更等の取扱方法を定めること。

イ　秘密情報漏えい等発生時における対応方法

請負業者は、秘密情報の漏えい等が発生した場合の対応方法を定めること。

３　請負作業時における遵守事項

（１）秘密情報管理簿の作成

請負業者は、秘密情報について、記録媒体、授受方法、保管場所、保管方法、使用場所、使用目的等取扱方法を明確に示した「秘密情報管理簿」を作成すること。

（２）業務指図書の作成

請負業者は、秘密情報取扱者等が行う作業について、作業者氏名、作業時間、作業内容、秘密情報の持ち出しの有無等を記載した業務指図書を作成し、これに基づき作業を実施させること。

（３）作業結果の確認

請負業者は、業務指図書に基づく作業が終了した場合、当該作業の実績を業務指図書に記載することにより、秘密情報取扱者等が行った作業の結果を確認すること。

（４）作業結果の報告

請負業者は、秘密情報取扱者等が行った作業の結果について主管係に報告すること。

（５）秘密情報漏えい等発生時の対応

請負業者は、秘密情報の漏えい等が発生した場合は、以下により対応すること。

ア　発生状況報告

秘密情報の漏えい等の発生日時、場所等の発生状況を、直ちに主管係に報告すること。

イ　対応措置

主管係の指示に基づき、直ちに対応措置を実施すること。

ウ　報告書の提出

主管係が指定する期日までに、発生原因、対応措置及びその結果等についての具体的内容を記載した報告書を作成し、提出すること。

エ　再発防止措置の実施

上記ア～ウ対応後、再発防止策を検討し、主管係の指示に基づき、速やかに再発防止のための措置を実施すること。

オ　その他

上記ア～エのほか主管係が指示した事項を実施すること。

4　請負作業完了時の遵守事項

（１）返却等処理

請負業者は、請負作業完了時において、上記３－（１）で作成した「秘密情報管理簿」に記載されている情報について、主管係の指示に基づき、返却、消去、廃棄等の処理を行うこと。

なお、その処理に係る方法、日時、場所、立会い者、作業責任者等について、事前に主管係の承認を得たうえで処理を行うこと。

（２）措置後の報告

請負業者は、上記（１）に基づく処理終了後、その結果を「秘密情報管理簿」に記載し、主管係に提出すること。

（３）その他

受託作業完了以前における契約の解除または、契約期間中に情報の返却、消去、廃棄等に合意した場合は、上記（１）、（２）と同様の手続きを行うこと。

なお、本要領は、契約の完了または解除後においても５年間は有効とする。

別添2

# 政府認証基盤の運用・保守の請負

# 提案書作成要領（案）

総務省

政府認証基盤の運用・保守の請負において、入札を希望する者は、本提案書作成要領に基づき、以下の内容を記載した提案書を作成し、必要部数を締切日までに提出しなければならない。

１．提案書の作成

(1)　様式

ア　使用言語

日本語とする。

イ　用紙サイズ等

日本工業規格(JIS)A 列 4 番で縦置き、横書きを原則とする。図表については、必要に応じて A 列 3 番縦書き・横書きを使用することができる。

ウ　データ形式

ドキュメント類を電子媒体に保存する形式は、Microsoft Word、Excel、Power Point 又は PDF 形式とする。ただし、提出書類を評価する者（総務省行政管理局行政情報システム企画課、以下「主管係」という。）が別途形式を定めて提出を求めた場合はこの限りではない。

エ　作成数量

提案書及び関連資料　　２部（正副）

上記提案書等を格納した電子媒体　　２部（正副）

（電子媒体は、供給者が用意するＣＤ－Ｒ等とする。）

(2)　留意事項

ア　主管係が特段の専門知識及び商品に関する一切の知識を有することなく、提出書類の評価が可能となるような提案書を作成すること。

イ　上記アについて、主管係が不備と判断した場合、提案書を評価しない場合があるので留意すること。

(3)　提案書の記載方法

総合評価基準書の別紙１「総合評価対応表」に掲げる事項に対する実現方法について、具体的に提案・記述するとともに、下記の事項を必ず含めること。また、総合評価対応表における各評価項目の内容と対応が取れるように作成すること。

ア　作業体制図

運用及び保守のそれぞれに係る作業体制図を作成し、各要員の具体的な経験、スキル及び人数を記述すること。また、調達仕様書で要員と組織に求めている資格等について、認定書の写しを提出すること。

イ　作業計画書

「調達仕様書」の契約期間における作業計画を作成すること。

ウ　納入計画書

納入成果物の作成方針を作成すること。なお、納入成果物に含まれる報告書については、具体的な内容について記述すること。

２．提案書の内容説明

提案書提出後、提案の内容について主管係が説明を求めた場合は、指定する日時に説明を行うこと。

３．既存資料の閲覧

(1) 閲覧対象資料

提案書を提出するに当たっては、既存資料の閲覧を行わなければならない。本調達に係る閲覧資料は、以下のとおり。なお、閲覧は、入札することを前提に、付録１の誓約書を提出した者に限る。

ア　構築仕様書（ブリッジ CA 編）
イ　構築仕様書（官職 CA 編）
ウ　構築仕様書（内部用サーバ CA 編）
エ　構築仕様書（ネットワーク編）
オ　LRA システム基本設計書
カ　IC カードシステム仕様書
キ　政府認証基盤 業務管理マニュアル
ク　政府認証基盤 システム運用マニュアル
ケ　LRA 業務管理・システム運用マニュアル
コ　証明書申請の手引き
サ　現行の施設・設備の詳細

(2) 閲覧方法

閲覧を希望する者は、本調達仕様書が公開されてから提案書提出期限までの期間（土日・祝祭日を除く午前 8 時 30 分から午後 6 時 15 分まで)、事前連絡の上、閲覧すること。

なお、閲覧の際には、付録１の誓約書を提出すること。

【閲覧場所】

〒100-8926　東京都千代田区霞が関 2－1－2　中央合同庁舎第 2 号館
総務省行政管理局行政情報システム企画課情報システム管理室

４．本件についての照会先

総務省行政管理局　行政情報システム企画課
情報システム管理室　政府認証基盤担当
〒100-8926　東京都千代田区霞が関２－１－２　中央合同庁舎第２号館
TEL：03-5253-6078（直通）
E-mail：gpki@soumu.go.jp

付録１

# 誓　　約　　書

令和　　年　　月　　日

総務省
　行政管理局行政情報システム企画課
　情報システム管理室長　あて

会社名
代表者氏名　　社印
電話番号

　政府認証基盤の既存資料の閲覧を行うことについて、下記の条件を遵守することを誓約します。

記

1. 閲覧に際しては、セキュリティ上の支障等がない限り、閲覧者が用意した機器等による記録も可とする。
2. 閲覧して得た情報は、提案書作成のためのみに利用し、いかなる理由においてもその他に利用しない。
3. 閲覧して得た情報は、提案書作成の関係者以外に洩らさない。
4. 閲覧中の立会い及び監視カメラでの撮影に同意する。

以上

別添３

# 政府認証基盤の運用・保守の請負

## 総合評価基準書（案）

総務省

本総合評価基準書は、「政府認証基盤の運用・保守の請負」に関する総合評価について定めたものであり、評価の手続及び採点方法は次のとおりである。

1　評価の手続

（1）必須の要求要件の確認

提出された提案書に記述された内容が、仕様書に定める要求要件のうち、総合評価基準（別紙「総合評価対応表」）において必須とされた項目について全て満たしている場合は「合格」とし、一つでも満たすことができない場合は「不合格」とする。

（2）評価方法

① 総合評価は、技術点（提案書による得点）に価格点（入札価格の得点）を加えて得た数値をもって行う。

総合評価点　＝技術点（3,200 点満点）＋価格点（3,200 点満点）

② 技術点は、次の評価方法により評価した値とする。

ア　上記１（１）における合否の判定により「合格」となった提案書に対して、別紙「総合評価対応表」に示す各加点項目について評価観点に基づき評価を行い「加点」を与える。（3,200 点満点）

イ　「加点」は別紙「総合評価対応表」で示す各加点項目をその重要度に応じ２種類の評価タイプ（最重要、重要）に区分し、提案内容の優劣について「２ 採点方式」に基づき相対評価を行い、加点を与える。ただし、評価結果が全く同等で優劣を付けがたい場合には、同評価とする事がある。

ウ　「加点」の合計点を「技術点」とする。

技術点（3,200 点満点）＝加点（3,200 点満点）

③ 価格点は、入札価格を予定価格で除して得た値を一から減じて得た値に入札価格に対する得点配分を乗じて得た値とする。

価格点＝（１－入札価格÷予定価格）×3,200 点

２　採点方法

得点は別紙「総合評価対応表」で示す各加点項目の重要度により、「最重要」、「重要」の２つの評価タイプに分けるものとする。それぞれの評価タイプごとに、以下の５段階の配点を行う。

| 相対的評価 | 最重要 | 重要 |
|---|---|---|
| (A)相対的にかなり優れている | 400 点 | 200 点 |
| (B)相対的に優れている | 300 点 | 150 点 |
| (C)相対的に平均である | 200 点 | 100 点 |
| (D)相対的に劣っている | 150 点 | 75 点 |
| (E)相対的にかなり劣っている | 100 点 | 50 点 |

（参考）相対的評価の例

ア　応札者（甲、乙）の評価が、第１順位＝甲、第２順位＝乙の場合は、甲にＢ評価、乙にＤ評価を与える。

イ　応札者（甲、乙、丙）の評価が、第１順位＝甲、第２順位＝乙、第３順位＝丙の場合は、甲にＢ評価、乙にＣ評価、丙にＤ評価を与える。

ウ　応札者（甲、乙、丙、丁）の評価が、第１順位＝甲、乙、第２順位＝丙、第３順位＝丁の場合は、甲と乙にＢ評価、丙にＣ評価、丁にＤ評価を与える。

エ　応札者（甲、乙、丙、丁）の評価が、第１順位＝甲、第２順位＝乙、第３順位＝丙、第４順位＝丁の場合は、甲にＡ評価、乙にＢ評価、丙にＤ評価、丁にＥ評価を与える。

オ　応札者（甲、乙、丙、丁、戊）の評価が、第１順位＝甲、第２順位＝乙、第３順位＝丙、第４順位＝丁、第５順位＝戊の場合は、甲にＡ評価、乙にＢ評価、丙にＣ評価、丁にＤ評価、戊にＥ評価を与える。

カ　応札者が一社の場合、Ｃ評価を与える。

別紙

# 総合評価対応表

| 調達仕様書対応内容 | | 必須項目 | | 加点項目 | | | |
|---|---|---|---|---|---|---|---|
| | | 評価観点 | 判定 | 加点番号 | 評価観点 | 評価基準 区分 | 評価基準 配点 |
| 1. 調達件名 | | | | | | | |
| | － | － | － | | | | |
| 2. 作業の概要 | | | | | | | |
| (5)作業内容<br>・納入成果物<br><br>ア 作業内容 | (ア)政府認証基盤の運用・保守実施計画書の策定 | 左記要件に係る具体的な実施方針が記載されていること。 | | 加1 | プロジェクトを実施するに当たり、主管課への報告、機器等事業者との連携、障害発生時の対応、ドキュメント類の管理、課題管理等の方針が優れていること。 | 重要 | 200 |
| | (イ)政府認証基盤の認証業務及び運用業務<br>A ブリッジ認証局に係る認証業務<br>B 政府共用認証局に係る認証業務<br>C 内部用サーバ認証局に係る認証業務<br>D 照会対応<br>E ホームページ作成及び更新<br>F 外部監査対応<br>G 監査ログ検査<br>H アーカイブ取得<br>I アーカイブ可読性確認<br>J 規程類に関する準拠性監査<br>K LRA研修<br>L 教育・訓練<br>M テスト環境の維持<br>N 書類改定(上位規程、業務規程、業務管理マニュアル)<br>O サーバ証明書等の発行支援 | 左記要件に係る具体的な実施内容が記載されていること。 | | 加2 | 認証業務及び運用業務に関し、セキュリティ又は品質を更に向上させるための手段や、従来の品質が確保できる根拠等を含めた作業効率を向上させるための改善事項(コスト削減に係る提案を含む)が提案されていること。また、政府共用認証局に係る認証業務と内部用サーバ認証局に係る認証業務を正確に理解した取り組み方針が提案されていること。 | 最重要 | 400 |
| | (ウ) 政府認証基盤システムの運用業務<br>A 運用・保守管理業務<br>B 監視業務<br>C 定常業務<br>D 非定常業務 | 左記要件に係る具体的な実施内容が記載されていること。 | | 加3 | システム運用業務に関し、セキュリティ又は品質を更に向上させるための手段や、従来の品質が確保できる根拠等を含めた作業効率を向上させるための改善事項(コスト削減に係る提案を含む)が提案されていること。 | 重要 | 200 |
| | (エ) 政府認証基盤システムの保守業務<br>・システム保守管理<br>・システム障害保守<br>・システム予防保守<br>・利用者環境の維持 | 左記要件に係る具体的な実施内容が記載されていること。 | | 加4 | システム保守業務に関し、セキュリティ又は品質を更に向上させるための手段や、従来の品質が確保できる根拠等を含めた作業効率を向上させるための改善事項(コスト削減に係る提案を含む)が提案されていること。 | 重要 | 200 |
| | (オ) 認証局施設・設備の管理業務<br>・施設・室に関する管理<br>・設備、備品等に関する管理(回線、電気設備、空調設備等) | 左記要件に係る具体的な実施内容が記載されていること。 | | | | | |
| | (カ) 報告書の作成<br>・月次報告書の作成<br>・月次報告書の報告 | 左記要件に係る具体的な実施内容が記載されていること。 | | | | | |
| | イ 作業実施期間<br><br>令和4年2月1日(火)から令和8年1月31日(土)まで。<br><br>ただし、令和3年10月1日(金)から令和4年1月31日(月)までは、運用を行う施設・設備の移設及びシステム更改への対応等、運用準備を行うこと。<br>施設・設備の移設及びシステム更改への対応については、「8 運用要件定義(3)運用施設・設備要件」を参照。<br><br>ウ 作業実施日<br><br>「行政機関の休日に関する法律(昭和63年法律第91号)」に規定する行政機関の休日を除く日。<br>ただし、主管係から業務上の指示があるときは、これに従うこと。<br>なお、監視業務については、作業実施期間における全日とする。 | 作業計画書において、契約期間中の作業スケジュールが記載されていること。 | | | | | |
| (5)作業内容<br>・納入成果物<br><br>イ 作業実施期間<br><br>～<br><br>オ 納入成果物 | エ 作業時間<br><br>(ア)運用要員<br>・運用責任者補佐1名、上級IA操作員1名以上<br>午前8時30分から午後5時30分まで(休憩時間は別途協議)<br>・監視員<br>2名、2交代又は3交代にて24時間(休憩時間は別途協議)<br>・上記以外の運用要員<br>午前9時30分から午後6時30分まで(休憩時間は別途協議)<br><br>(イ)保守要員<br>「5 信頼性等要件 (1)信頼性要件」に示すサービスの停止を伴う場合、24時間週7日対応とする。<br>なお、上記以外は、原則午前9時30分から午後6時30分まで(休憩時間は別途協議)とする。<br><br>ただし、主管係から業務上の指示があるときは、これに従うこと。 | 作業体制図が左記要件を実現できる体制であること。 | | | | | |
| | オ 納入成果物<br><br>次の文書の電子データ(CD-R)(PDF形式を含む各一式)を納入する。<br>・実施計画書<br>(本請負業務に係るスケジュール、体制、管理方針等の計画書)<br>・運用状況報告書<br>(進捗管理報告書、運用報告書、課題管理台帳、タスクチャート、アクセス状況一覧、監視報告書、相互認証状況一覧、CVS・リポジトリアクセス状況、月間作業一覧、月間作業スケジュール、年間作業一覧、サービス指標実績値、ヘルプデスク運用状況、教育訓練実施状況 等)<br>・障害発生対応状況報告書<br>(障害・案件一覧、個別障害対応報告書 等)<br>・予防保守等に係る調査報告書<br>・保守作業計画書<br>・保守作業報告書<br>・各種規程・マニュアル等ドキュメント(更新履歴書含む)の最新版 | 納入計画書において、納入成果物の作成方針が記載されており、納入成果物に含まれる報告書の具体的な内容が記載されていること。 | | | | | |

別紙

# 総合評価対応表

| 調達仕様書対応内容 | | 必須項目 | | 加点項目 | | | |
|---|---|---|---|---|---|---|---|
| | | 評価観点 | 判定 | 加点番号 | 評価観点 | 評価基準 区分 | 評価基準 配点 |
| 3. 情報システムの要件 | | | | | | | |
| | 政府認証基盤は、ブリッジ認証局と政府共用認証局から構成され、マスタセンタ、バックアップセンタ及びテストセンタに配置されている。<br><br>(1)ブリッジ認証局<br>ブリッジ認証局は、ブリッジ認証システム、リポジトリ(ブリッジ認証情報格納システム、統合認証情報公開システム)、証明書検証システム等から構成されている。<br>また、ブリッジ認証局は、官職認証局、公的個人認証サービス(JPKI)、地方公共団体組織認証基盤(LGPKI)、商業登記認証局及び民間認証局と取り交わす相互認証証明書の発行を行っている。<br>リポジトリは、ブリッジ認証局に関する認証情報(自己署名証明書、リンク証明書、相互認証証明書(ペア)及び証明書失効情報)は、インターネット向け及び政府共通ネットワーク向けに公開を行っている。<br>証明書検証システムは、官職認証局をトラストアンカとする署名検証者に対して、政府共用証明書検証サーバによる証明書検証機能の提供を行っている。<br><br>(2)政府共用認証局<br>政府共用認証局は、LRAシステム及びICカードシステムを含む政府共用認証システム及び政府共用認証情報格納システム等から構成されている。<br>さらに、政府共用認証局は、官職認証局から構成されている。<br>官職認証局は、電子申請・届出等の手続に利用する各府省の官職証明書、利用者証明書、情報提供ネットワークで使用する暗号通信用等証明書及び政府共用証明書検証サーバに対して証明書を発行している。<br>官職認証局から発行する官職証明書又は利用者証明書のICカードは、「公的分野における連携ICカードの実現に向けた基本的考え方」(平成13年7月27日公的分野におけるICカードの普及に関する関係府省連絡会議)等を踏まえた仕様とする。カードインタフェースは、非接触・接触両インタフェースを有するコンビ型を必須とする。<br><br>また、政府共用認証局を構成する認証局ではないが、各府省が運営している業務システム等で必要とする内部用のサーバ証明書を発行するための内部用サーバ認証局がある。内部用サーバ認証局は、政府認証基盤を構成する認証局と同様の認証業務及び運用業務を行う。<br><br>LRAシステムは、府省等登録局(LRA)に所属する職員のみ利用可能とする。府省等登録局(LRA)は令和2年4月現在、26府省等が設置されており、官職認証局が発行する官職証明書、利用者証明書及び暗号化通信用等証明書の発行申請、及び内部用サーバCAが発行する内部用サーバ証明書の発行申請を行う。<br><br>なお、平成30年4月をもって終了したアプリケーション認証局に係る認証業務は、平成30年5月以降、民間の発行事業者から証明書等を政府認証基盤が取りまとめて取得する業務に変更し、サーバ証明書、コード署名証明書、ドキュメント署名証明書の発行支援業務に切り替えを行った。<br><br>本件の対象となる情報システムの詳細は、別途閲覧に供する以下の仕様書及び参照資料1「政府認証基盤 セキュリティ要件」を参照。<br><br>・構築仕様書(ブリッジCA編)<br>・構築仕様書(官職CA編)<br>・構築仕様書(内部用サーバCA編)<br>・構築仕様書(ネットワーク編)<br>・LRAシステム基本設計書<br>・ICカードシステム仕様書<br>・LRA業務管理・システム運用マニュアル<br>・証明書申請の手引き | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | 加5 | ブリッジ認証局に係る認証業務の相互認証審査等支援に関し、相互認証先認証局との調整、事前準備、審査支援、結果のとりまとめ作業を通じて、相互認証先認証局との相互認証を確実に行える取り組み方針が提案されていること。 | 重要 | 200 |
| 4. 規模・性能要件 | | | | | | | |
| (1)規模要件 | 政府認証基盤は、マスタセンタ、バックアップセンタ及びテストセンタから構成する。<br>政府認証基盤では、インターネットや政府共通ネットワークに向けて、証明書の発行、証明書情報の公開及び証明書の検証に係わるサービスを提供する。マスタセンタには、これらを実現する上で必要となる機能をすべて設置している。これに対してバックアップセンタは、マスタセンタの予期せぬ障害に備え、性能、可用性を除き、サービス継続を行うためのみに必要な機能を保有する。<br>また、テストセンタは、本番環境のシステムの維持、相互認証の際の接続試験、証明書を利用したアプリケーションの評価テスト等を行うため、必要に応じて、インターネットや政府共通ネットワークに向けて、テスト環境を提供する機能を保有する。<br>システム更改の対象としている現行のシステムの機器一覧を「表4－1　機器一覧」に示す。<br><br>詳細は、別途閲覧に供する以下の資料を参照。<br>・構築仕様書(ブリッジCA編)<br>・構築仕様書(官職CA編)<br>・構築仕様書(内部用サーバCA編)<br>・構築仕様書(ネットワーク編) | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | |
| (2)性能要件 | 「5　信頼性等要件　(1)信頼性要件」の評価項目と目標値 の応答時間を参照。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | |
| 5. 信頼性等要件 | | | | | | | |
| (1)信頼性要件 | 政府認証基盤ではSLA(Service Level Agreement)を導入し、政府認証基盤のサービスの内容、範囲、提供状況を測定・分析可能な単位で明確に規定し、目指すべき目標値の達成状況を管理することで、サービス品質の確保及び維持・改善を行っている。<br>国民等、府省等利用機関に向けた各サービスに関するサービスレベルの評価項目及び目標値は、表5－1、表5－2及び表5－3のとおりであるが、本調達におけるSLAの対象は、運用・保守に係る作業及び施設・設備に起因した場合とする。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | |

別紙

# 総合評価対応表

| 調達仕様書対応内容 | | | 必須項目 | | 加点項目 | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 評価観点 | 判定 | 加点番号 | 評価観点 | 評価基準 | |
| | | | | | | | 区分 | 配点 |
| | (2)事業継続性要件 | 政府認証基盤は、ブリッジ認証局、官職認証局それぞれのCP/CPS に災害時の事業継続性要件を定めている。<br>災害等により認証局の設備が被害を受けた場合は、バックアップセンタにおいてバックアップデータを用いて運用を行う。バックアップセンタは、マスタセンタから適切な距離の場所に設置する。災害時の業務方針は以下のとおりである。<br>・リポジトリ及びWeb によるCRL/ARLの公表を最優先として、公表停止から48時間以内に公表を再開する。<br>・緊急を要する証明書発行及び失効業務は、業務停止より96時間以内に再開する。<br>・通常業務は、マスタセンタの認証局の設備及びセキュリティが完全に復旧されたことを確認後に再開する。<br><br>なお、事業継続に係る具体的な作業内容は、別途閲覧に供する以下の資料を参照。<br>・政府認証基盤　業務管理マニュアル － 危機管理マニュアル | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | 加6 | 事業継続性要件に関し、災害等により認証局の設備が被害を受けた場合を想定した対応方針が示されていること。 | 最重要 | 400 |

別紙

# 総合評価対応表

| 調達仕様書対応内容 | | | 必須項目 | | 加点項目 | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 評価観点 | 判定 | 加点番号 | 評価観点 | 評価基準 区分 | 評価基準 配点 |
| 6. 情報セキュリティ要件 | | | | | | | | |
| | (1)権限要件 | 今回調達する運用要員の役割ごとの権限要件については、別途閲覧に供する以下の資料を参照。<br>・政府認証基盤　業務管理マニュアル － 運用権限管理マニュアル | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | 加7 | 契約期間中の運用・保守業務の実施にあたり、新たな施設・設備における運用要員への権限付与と権限分離、及びサーバ機器等の主体認証情報の管理について、内部統制が有効となる方法、実施方針が具体的に示されていること。 | 重要 | 200 |
| | (2)情報セキュリティ対策 | 具体的な情報セキュリティ対策は、参照資料1「政府認証基盤　セキュリティ要件」及び別途閲覧に供する以下の資料を参照。<br>・政府認証基盤　情報セキュリティ実施手順書<br><br>なお、主管係が必要と認める際には、情報セキュリティ監査を受け入れること。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |
| 7. 情報システム稼働環境 | | | | | | | | |
| | | － | － | － | | | | |
| 8.運用要件定義 | | | | | | | | |
| | (1)システム操作・監視等要件 | 政府認証基盤を構成するシステムの操作及び監視に係る要件は、別途閲覧に供する以下の資料を参照。<br>・政府認証基盤 システム運用マニュアル<br><br>なお、システム監視に関する特記事項は以下のとおり。<br>・24時間週7日、監視を行うこと。<br>・監視員は、2名が常時マスタセンタにて監視業務にあたるものとし、休憩時にも最低1名は、監視業務を継続していること。<br>・監視業務における対処履歴を、電子データに記録すること。<br>・指示事項に対しては、都度、監視員全員に、周知が完了したことを示す報告書を提出すること。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |
| | (2)データ管理要件 | 運用要員は、システムで取得された認証業務及び監視業務に係るバックアップ及びアーカイブのデータ管理を実施する。認証業務の具体的なデータ管理要件は別途閲覧に供する以下の資料を参照。<br>・政府認証基盤　システム運用マニュアル | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |
| | (3)運用施設・設備要件 | 施設・設備の要件は、認証業務に係る機器等の稼働に直接影響を与えない監視室及び事務室を除き、耐震性について震度6強以上の地震に耐えられる免震構造の建物とし、少なくとも現行のテストセンタを含むマスタセンタ（東京都内）を新たな施設・設備に移設すること。<br><br>ア　現行の施設・設備<br><br>現行の施設・設備については、マスタセンタ及びバックアップセンタ（東京近郊）の2カ所があり、施設使用料及び通信回線（インターネットとマスタセンタ間、インターネットとバックアップセンタ間の通信費及びプロバイダ契約料。請負者が所有している設備、物品及び政府共通ネットワークの接続料は除く）使用料（月額15,800,000円（税抜き））は、請負業者の負担である。<br><br>（略）<br><br>上記に含まれない次の設備等については、請負業者の負担である。<br><br>空調装置7式、監視カメラ24台、ICカード認証装置15台、生体認証装置9台、ラック架台53台、ラック14台、消火装置17台、金庫11台　等<br><br>現行の施設・設備の詳細については、別途閲覧に供する「現行の施設・設備の詳細」資料を参照。<br><br>イ　新たな施設・設備<br><br>以下の条件を満たす新たな施設・設備を提案することとし、施設使用料、通信回線使用料等は現行の月額を上限とすること。<br>また、機器等の移設・据付・調整・システム設定・テスト等への対応は、請負業者の責任と負担において行うこと。<br>・新たな施設・設備は、参照資料2「政府認証基盤 施設・設備の詳細仕様」を満たしていること。<br>・移設に伴う本システムのサービス停止時間（新旧システムの切替えを伴うもの）については、システム更改の請負者と連携して24時間内とし、回数は4回を限度とする。 | 新たな施設・設備における認証設備室のレイアウト、及び監視カメラ、認証装置等設備の配置が具体的に記載されていること。<br>また、新たな施設・設備へのシステムの移設について具体的な手順、スケジュールが記載されていること。 | | | | | |
| 9. 保守要件定義 | | | | | | | | |
| | | 対象となるシステムは、ブリッジ認証局システム、政府共用認証局システム（独自に開発したアプリケーション含む）及び内部用サーバ認証局とすること。<br>システム変更を伴うシステム保守については、システム変更を本番環境に適用する前に必ずテストセンタのテスト環境において評価を実施すること。<br>システム保守は、業務停止を伴わないこと。業務を停止する場合は、夜間若しくは休日等の利用者の利用時間外に実施すること。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |

# 総合評価対応表

| 調達仕様書対応内容 | | | 必須項目 | | 加点項目 | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 評価観点 | 判定 | 加点番号 | 評価観点 | 評価基準 区分 | 評価基準 配点 |
| 10. 作業の体制及び方法 | | | | | | | | |
| | (1)作業体制 | ア　運用要員数の要件<br><br>今回調達する運用要員の役割と要員数を表10－1に示す。役割の兼務は運用責任者補佐とログ検査者についてのみ可能とする。<br><br>運用責任者 1名<br>運用責任者補佐 2名以上<br>ログ検査者 2名以上<br>上級IA操作員 6名以上<br>一般IA操作員 3名以上<br>監視員 8名以上<br>計 22名以上 | 作業体制図において、必要以上の運用要員数が確保されていること。 | | 加8 | 提案する運用要員数について、要員数の考え方が示されていること。また、バックアップ体制も含め、柔軟な要員対応が可能であること。 | 最重要 | 400 |
| | | イ　運用要員の経験、業務知識及びスキル等<br><br>(ア) 認証局の運用実績<br>運用要員には、以下の運用実績を有する者を含めること。<br>・行政機関の認証局又は電子署名法に基づく特定認証業務の認定を受けた認証局（以下、「特定認証局」という。）における運用責任者相当の運用<br>・行政機関の認証局又は特定認証局における操作員としての運用<br>・行政機関の認証局又は特定認証局における監視員としての運用 | 作業体制図において、左記要件の運用実績を有する者を配置していること。 | | | | | |
| | | (イ) スキル<br>ITIL Foundation 認定資格者又は経済産業大臣認定の情報処理技術者試験のITサービスマネージャ試験、システム監査技術者試験、プロジェクトマネージャ試験いずれかの合格者であることが望ましい。 | － | － | | | | |
| | | ウ　システム保守要員数の要件<br><br>システム保守要員数については、特に定めない。ただし、政府認証基盤を構成するシステムについて障害保守、予防保守等の対応を迅速かつ恒常的に行える体制を組むこと。 | 作業体制図において、保守要員の体制が確保されていること。 | | 加9 | 提案する保守要員数について、要員数の考え方が示されていること。また、バックアップ体制も含め、柔軟な要員対応が可能であること。 | 重要 | 200 |
| | | エ　システム保守要員の経験、業務知識及びスキル等<br><br>(ア) 認証局の保守実績<br>システム保守要員には、以下の保守実績を有する者を含めること。<br>・行政機関の認証局又は特定認証局 | 作業体制図において、左記要件の保守実績を有する者を配置していること。 | | | | | |
| | | (イ) スキル<br>主要なメンバとして、情報セキュリティスペシャリスト試験、テクニカルエンジニア（情報セキュリティ）試験いずれかの合格者又はITスキル標準のITスペシャリスト職種（専門分野セキュリティ）のレベル4以上の者、若しくは同等の能力を有する者を含むことが望ましい。 | － | － | | | | |
| | | オ　その他<br>請負者は、作業時期・内容等について当省が承認した場合は、請負者が指定する場所（運用要員の自宅を含む。）でリモート環境により作業を行うことできる。<br>なお、感染症対策として、業務のうち当省との連絡調整などについてリモート環境で行うことや、当省の承認の下で勤務体制を変更することなど、合理的な対策を可能な限り行うものとする。 | － | － | 加10 | 具体的な手法や体制の考え方が示されていること。 | 重要 | 200 |
| | (2)導入 | ア　作業実施場所<br><br>作業実施場所は、テストセンタを含むマスタセンタ（新たな施設・設備）及びバックアップセンタ（東京近郊）の2カ所となる。常時、運用要員が作業する場所は、マスタセンタとなる。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |
| | | イ　業務引継<br><br>請負開始前までに、請負業者の負担において現請負先等から業務内容等について詳細に引継ぎ、令和4年2月1日から現行と同等のサービスを提供すること。<br>また、請負終了前においても、令和8年2月以降の請負先が現行と同等のサービスを提供できるよう、業務内容等について詳細に引継ぐこと。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |
| | | ウ　その他<br><br>・運用要員及び保守要員のバックアップ体制をとること。<br>・運用要員と保守要員の兼務は行わないこと。<br>・運用要員及び保守要員は、夜間・休日を問わず緊急時の連絡及び召集に対応するため、携帯電話等（請負業者が手配し通話料・通信料を負担）を常備して常に連絡が取れること。<br>また、主管係が要員への連絡に必要な携帯電話等2台以上を請負業者の負担において手配し、通話料・通信料も負担すること。 | | | | | | |

# 総合評価対応表

| 調達仕様書対応内容 | | | 必須項目 | | 加点項目 | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 評価観点 | 判定 | 加点番号 | 評価観点 | 評価基準 区分 | 評価基準 配点 |
| | | ・本件調達については、サービスレベルアグリーメント(SLA)を導入する。請負業者は、別途指定するサービスレベル要件を満たすサービスの提供が可能となる体制をとること。本件調達範囲の業務に起因してSLAが達成されなかった場合、月額役務経費に相当する金額の5%を減額する。<br>・運用及び保守に必要な消耗品等は請負業者が準備すること。消耗品の仕様等の詳細は別途閲覧に供する「消耗品一覧」資料を参照。<br>・サーバ証明書等の発行支援の業務において、証明書の取得に係る費用は請負業者が負担すること。<br>・主管係及び利用機関等への連絡等に必要な通信運搬費は請負業者が負担すること。<br>・主管係の指示に従い業務を実施すること。<br>・主管係において、要員が適切に業務を実施できないと判断した場合、請負業者は速やかに対応すること。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | 加11 | 運用・保守の観点から、サービスレベル遵守ための具体的な施策が提案されていること。 | 最重要 | 400 |

別紙

# 総合評価対応表

| 調達仕様書対応内容 | | | 必須項目 | | 加点項目 | | | |
|---|---|---|---|---|---|---|---|---|
| | | | 評価観点 | 判定 | 加点番号 | 評価観点 | 評価基準 区分 | 評価基準 配点 |
| 11. 特記事項 | | | | | | | | |
| | (1)情報セキュリティ確保及び秘密保持 | 本件業務を請負う者は、取り扱う情報に関して、以下の事項を遵守すること。<br><br>ア　情報セキュリティ実施手順の作成<br>請負業者は、請負った情報システムについて、別途閲覧に供する総務省情報セキュリティポリシーを踏まえ、次に掲げる事項の具体的な内容を盛り込んだ情報セキュリティ実施手順書（以下「実施手順書」という。）を作成し、主管係の承認を得ること。<br>（ア） システム運用管理者、システム運用担当者を明確にした情報セキュリティ管理体制及び緊急時における連絡体制<br>（イ） 管理区域への入退室等の物理的セキュリティ対策<br>（ウ） パスワード管理、要員の教育計画等の人的セキュリティ対策<br>（エ） アクセス制御等の技術的セキュリティ対策<br>（オ） 各セキュリティ対策の確保状況に関する報告内容、報告方法等<br>（カ） 緊急時の対応に必要な事項<br>（キ） その他、情報システム管理者が必要と認めた事項<br><br>イ　実施手順書等の遵守<br>請負業者は、実施手順書及び参照資料3「秘密情報保護・管理要領」を遵守し、実施手順書違反等があった場合は直ちに主管係へ報告し、指示を受けること。<br><br>ウ　セキュリティ情報の収集<br>請負業者は、請負った情報システムのセキュリティに関連する最新情報を常に収集し、主管係へ報告するとともに、主管係の指示に基づき必要な措置を行うこと。<br><br>エ　委託契約<br>請負業者は、請負った情報システムの整備・運用に当たって他の事業者と委託契約を行う場合は、主管係の承認を得ること。承認等必要な手続については、契約書に従うこと。<br><br>オ　身元保証<br>請負業者は、各要員の在籍証明書、業務経歴書及び秘密保持管理証明書を提出すること。<br>また、他の事業者と委託契約を行う場合は、当該事業者の在籍証明書及び秘密保持管理証明書とともに、請負業者がこれを保障する証明書を提出すること。<br><br>カ　運用・保守に支障をきたす事案の発生時等における対処<br>請負業者は、請負った情報システムの運用・保守に支障をきたす事案が発生したとき、又は発生する恐れがあると推定されるときは、主管係に対して直ちに連絡し、対応措置について指示を受けること。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |
| | (2)法令等の遵守 | 業務の遂行において使用する情報資産について、次の法律その他の法令等を遵守し、これに従わなければならない。また、関連するガイドライン等も同様とする。<br>・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）<br>・著作権法（昭和45年法律第48号）<br>・不正アクセス行為の禁止等に関する法律（平成11年法律第128号）<br>・電気通信回線を通じた送信又は磁気ディスクの送付の方法並びに磁気ディスクへの記録及びその保存の方法に関する技術的基準（平成14年総務省告示第334号） | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |
| | (3)知的財産権 | ア　本契約履行過程で生じた成果物に関し、著作権法第27条及び28条に定める権利を含むすべての著作権を総務省に譲渡し、総務省は独占的に使用するものとする。<br>なお、請負業者は総務省に対し、一切の著作者人格権を行使しないこととし、また、第三者をして行使させないものとする。<br>また、請負業者が本契約の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、総務省と別途協議するものとする。<br><br>イ　成果物に第三者が権利を有する著作物が含まれている場合は、総務省が特に使用を指示した場合を除き、請負業者は当該著作物の使用に関して費用の負担を含む一切の手続を行うものとする。なお、この場合、請負業者は当該著作物の使用許諾条件につき、主管係の了承を得ること。<br><br>ウ　本件業務の作業に関し、第三者との間で著作権に係る権利侵害の紛争等が生じた場合、当該紛争の原因が専ら総務省の責めに帰す場合を除き、請負業者は自らの責任と負担において一切を処理すること。なお、総務省は紛争等の事実を知ったときは、速やかに請負業者に通知することとする。 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されていること。 | | | | | |
| | (4)その他 | ア　本件調達に係る業務の実施予定組織・部門がISO27001又は同等の認証を取得していること。<br><br>イ　運用業務において必要とする当該仕様書に記載のない要件が発生した際には、対処に関する協議を別途行うものとする。<br><br>ウ　LRAからの証明書発行申請に基づき、サーバ証明書、コード署名証明書、ドキュメント署名証明書を発行事業者（民間）から取得するサーバ証明書等の発行支援を行うこと。<br>　契約期間中、発行事業者から取得する証明書は、最大の有効枚数を以下と想定する。<br>・サーバ証明書・・・1,000枚<br>・コード署名証明書・・・100枚<br>・ドキュメント署名証明書・・・30枚 | 左記要件を理解し、これを実現するための具体的な実施方針が記載されているとともに、実施予定組織・部門がISO27001又は同等の認証を取得していること。 | | | | | |
| 14. ワークライフバランス（複数の認定等に該当する場合は、最も配点が高い区分により加点を行うものとする。） | | | | | | | | |
| | 女性活躍推進法に基づく認定 | | | | 加12 | 第一段階目<br>※労働時間等の働き方に係る基準は満たすことが必要。 | 重要 | 75 |
| | | | | | | 第二段階目<br>※労働時間等の働き方に係る基準は満たすことが必要。 | | 100 |
| | | | | | | 第三段階目 | | 150 |
| | | | | | | プラチナえるぼし | | 200 |
| | | | | | | 行動計画<br>※ 女性活躍推進法に基づく一般事業主行動計画の策定義務がない事業主（常時雇用する労働者の数が300人以下のもの）に限る（計画期間が満了していない行動計画を策定している場合のみ）。 | | 50 |

別紙

# 総合評価対応表

| 調達仕様書対応内容 | 必須項目 | | 加点項目 | | | |
|---|---|---|---|---|---|---|
| | 評価観点 | 判定 | 加点番号 | 評価観点 | 評価基準 区分 | 評価基準 配点 |
| 次世代育成支援法に基づく認定（くるみん企業、プラチナくるみん企業） | | | | くるみん企業（旧基準） | | 100 |
| | | | | くるみん企業（新基準） | | 150 |
| | | | | プラチナくるみん企業 | | 200 |
| 若者雇用促進法に基づく認定（ユースエール企業） | | | | ユースエール企業 | | 200 |