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 24 年 7 月 20 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年度に、より安全な暗号アルゴリズムへの移行を行う予定である。これに伴い、相互認証先認証局（13認証局）との相互認証更新が予定されている。

現在は、平成25年３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。

---

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

[2] http://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とサーバ証明書等を発行するアプリケーション認証局(「WebTrust for CA[3]」の規準に基づく検証報告書を取得)及び現在構築中のアプリケーション認証局２にわかれる。

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[4]

(政府共用認証局)

・官職認証局 CP/CPS[5]

・アプリケーション認証局 CP/CPS[6]

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[7]」を定め公表している。

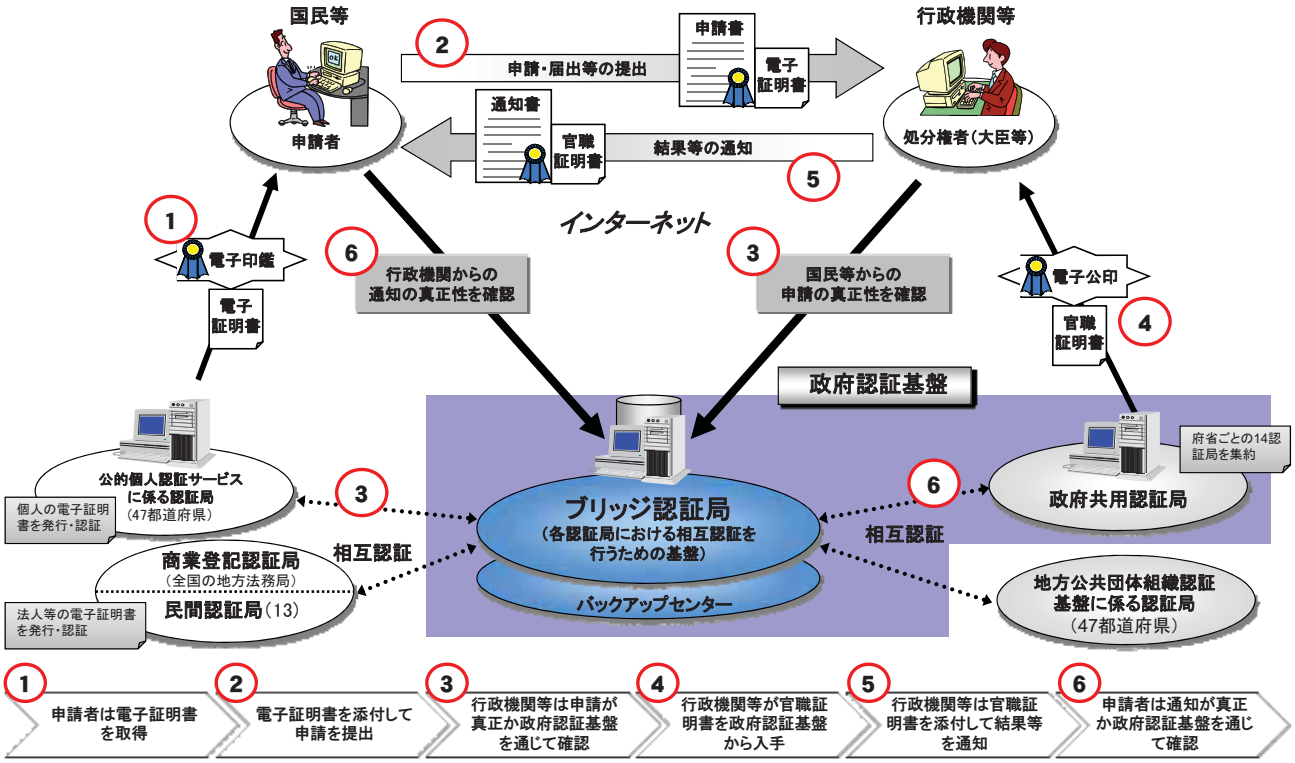


図　２-１　政府認証基盤の概要

---

3 米国公認会計士協会(AICPA)及びカナダ勅許会計士協会(CICA)が定めた認証局についての業界最高水準の基準

4 http://www.gpki.go.jp/bca/cpcps/cpcps.pdf

5 http://www.gpki.go.jp/osca/cpcps/cpcps.pdf

6 http://www.gpki.go.jp/apca/cpcps/cpcps.pdf

7 http://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 170 万件
・府省等が電子証明書を検証する件数　　：月間約 100 万件
・相互認証(接続)している認証局　　：17 認証局（平成 24 年 4 月現在）

(ｳ) 利用者に提供するサービス

政府認証基盤の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。 ・ 相互認証する際の規準である相互認証基準をもとに書類審査及び技術審査を行う。 ・ 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。 ・ 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。 ・ 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。 ・ 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。 ・ 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。 ・ 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、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。 ・ 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（旧霞が関 WAN）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。 ・ 受け付けた情報をもとに証明書を発行する。 ・ 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。 ・ 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。
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。 ・ 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こととし、その業務の詳細内容については、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」を参照とすること。

発行する証明書は最大２万枚/年、相互認証の実施は最大 13 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こと。

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。 常時、運用要員が作業する場所はマスタセンタとする。 ○午前8時30分～午後5時30分まで(休憩時間は別途協議) 運用責任者補佐1名、上級IA操作員2名、一般IA操作員1名 ○午前9時30分～午後6時30分まで(休憩時間は別途協議) 上記以外の運用要員
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	４名以上	
一般IA操作員	２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。 （注）上記運用要員と保守要員との兼務は行わないこと。

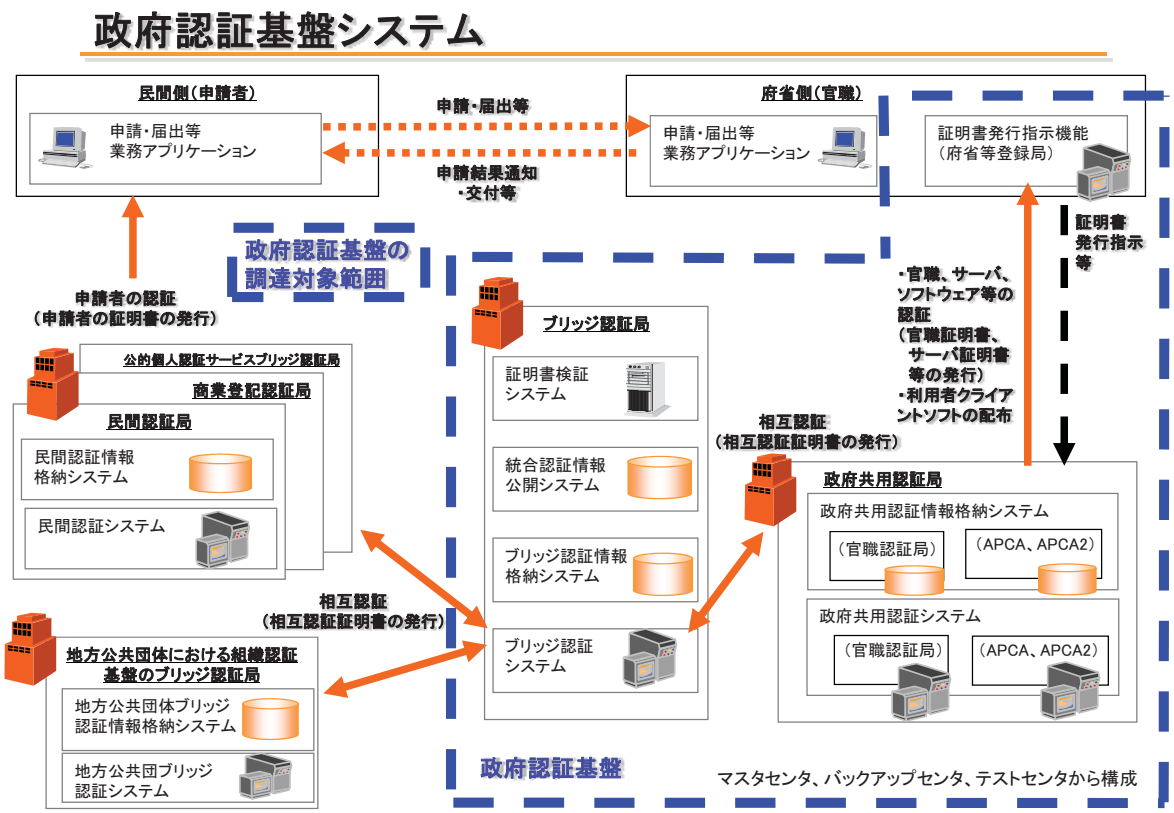


図　2－2　政府認証基盤システムの概要

(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（審査対応、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) アプリケーション認証局に係る認証業務

・自己署名証明書の発行（キーセレモニー）

・テスト環境用証明書の発行（模擬 APCA の EE 証明書）

(d) 失効情報の確認

C 照会対応

(a) LRA

(b) 相互認証先認証局

(c) CA/ブラウザフォーラム等外部組織

(d) 電子申請等アプリケーション

(e) 運営組織側の管理業務支援

D ホームページ作成及び更新

E 外部監査対応

(a) CP/CPS 準拠性監査の対応

(b) WebTrust 検証の対応

F 監査ログ検査

G アーカイブ取得

H アーカイブ可読性確認

I 規程類に関する準拠性監査

J LRA 研修

K 教育・訓練

(a) 危機管理訓練（事業継続計画）

(b) 運用要員教育

L テスト環境の維持

M 書類改定（上位規程、業務規程、業務管理マニュアル）

(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、WebTrust の維持

・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

(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

(d) リリース管理

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) データバックアップに係るテープ交換

(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) 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

㈀ 政府認証基盤の暗号移行対応

A 暗号移行に係る相互認証審査支援

B 暗号移行に係る鍵更新（ブリッジ認証局、官職認証局）

C 暗号移行に係る相互認証取り交し

D 暗号移行に係る証明書の一斉切替（官職認証局）

E 暗号移行に係るアプリケーション認証局２の自己署名証明書の発行

F 暗号移行に係るアプリケーション認証局の廃止

㈁ 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

㈂ 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

㈃ 報告書の作成

A 月次報告書の作成

B 月次報告書の報告

㈄ 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。

・ 主管係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

現行の施設・設備又は請負者の提案する施設・設備で運用すること。

㈠ 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（東京都内）及びバックアップセンタ（東京近郊）の２カ所があり、これらを使用する場合、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及び請負者が保有している設備及び物品は除く。）使用料等（現行月額 16,590,000 円（消費税を含む。）は、請負者の負担とする。

※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) 請負者の提案する施設・設備

請負者の提案する施設・設備で運用する場合、以下の条件を満たすこと。また、機器等の移設・据付・調整･システム設定・テスト等は、請負者の責任と負担において対応すること。

（条件）

・提案施設・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。

・機器の移設に伴う本システムのサービス停止時間は、24 時間（日曜日の 0 時～24 時まで）内とし、回数は４回を限度とする。

(2) 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こと。

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 ｝

(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

(3) 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ついて、仕様書に定める内容について、契約の履行に関し、監督・検査を実施するなどし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、当該指示を受けて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、平成 25 年３月１日以降の本件業務開始以降の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準備行為等に対して、請負者に発生した費用は、請負者の負担とする。

(4) 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、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。）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

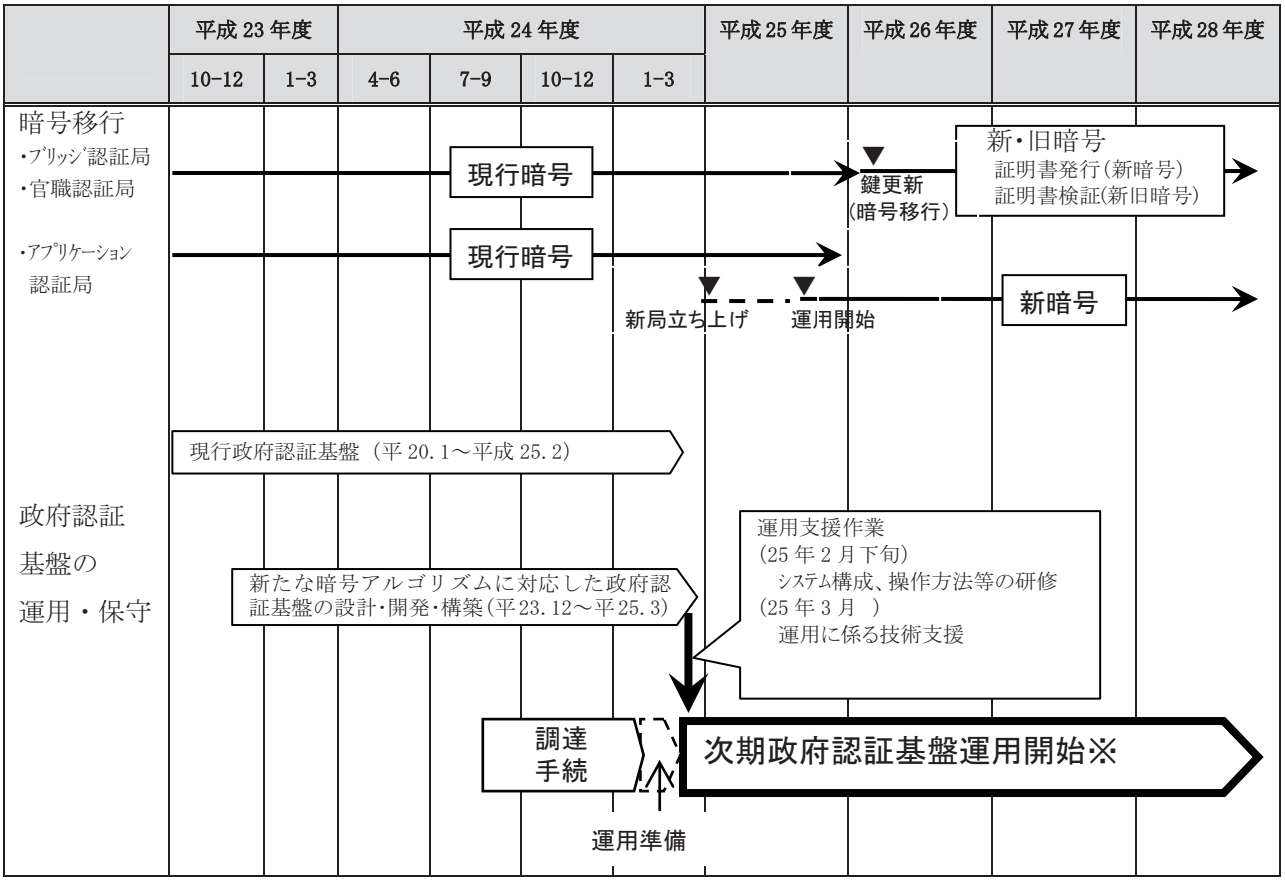
請負契約の契約期間は、平成 25 年３月から平成 29 年２月までとする。

移行指針等に基づく暗号移行については、ブリッジ認証局と官職認証局は、平成 26 年度早期に鍵更新により行う。また、アプリケーション認証局は新局立ち上げ方式により行うこととするが、ブラウザソフトウェアへの同認証局のルート証明書の登録等に期間がかかることなどから、平成 25 年 12 月のサーバ証明書等の発行開始に向け、平成 25 年 3 月から自己署名証明書発行等の準備を行い、平成 25 年４月に新暗号の認証局を立ち上げる。

これらの暗号移行に伴い、平成 26 年度は、相互認証先認証局（平成 24 年度末時点、13 認証局）全ての相互認証の更新等を行うとともに、全ての電子証明書の再発行（約２万枚）を行うこととなる。

なお、現在実施している「新たな暗号アルゴリズムに対応した政府認証基盤の設計・開発・構築等の請負」を請け負っている（社）行政情報システム研究所は、運用支援作業として、本請負者に対し、平成 25 年２月下旬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を実施するとともに、１カ月間（25 年３月）の運用に係る技術支援を行うこととしている。

表　3-1 政府認証基盤の運用・保守スケジュール



※運用・保守期間は平成 25 年３月～平成 29 年２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　平成 22・23・24 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　当省及び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。

キ　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。

ク　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。

ケ　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。

コ　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２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	2012 年(平成 24 年)	11 月中旬
入札説明会		11 月下旬
質問受付期限		12 月中旬
入札書（提案書）提出期限		1 月上旬
入札参加者によるプレゼンテーション	2013 年(平成 25 年)	1 月上旬
提案書の審査		1 月上旬
開札及び落札者の決定		1 月下旬
契約締結		1 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、所定の手続きを経て、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及び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（案)」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 105 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

平成 22・23・24 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出来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わない場合には不要。

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）

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（案）」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（案）」を基本とする。

(1) 評価方法

総合評価落札方式（加算方式）とする。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（2,800 点満点）＋技術点（2,800 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）×2,800 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。（2,800 点満点）

(ｲ)「加点」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、同評価とする事がある。

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項ただし書き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項ただし書き抜粋）
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、落札者を決定するものとする。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、落札者を決定するものとする。

(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、なお、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管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

(1) 開示情報

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、請負業務を実施したとき、又は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は、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こと。

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　瑕疵担保責任

(ｱ) 当省は、成果物の引渡し後に発見された瑕疵について、引渡し後１年間は、請負者に補修を請求できるものとし、補修に必要な費用は、全て請負者の負担とする。

(ｲ) 成果物の瑕疵が請負者の責に帰すべき事由によるものである場合は、当省は、前項の請求に際し、これによって生じた損害の賠償を併せて請求することができる。

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じるべき措置」に規定する事項その他の事項について、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実施させる場合は、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、本業務を改善するため、又は経済情勢の変動、天災地変の発生、関係法令の制定若しくは改廃その他契約の締結の際、予測できなかった著しい変更が生じたことにより本業務を実施することが不適当と認められる場合は、協議により、契約の内容を変更することができる。

カ　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、同額の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。

キ　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。

ク　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。

ケ　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。

コ　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。

サ　請負業務の引継ぎ

(ｱ) 現行請負者からの引継ぎ

請負者は、本業務が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。

シ　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ときは、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、内閣総理大臣が行う評価の時期（平成 28 年５月を予定）を踏まえ、本業務に係る運用が開始される平成 25 年３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、平成 28 年５月を目途として、本業務の実施状況等を内閣総理大臣及び官民競争入札等監理委員会へ提出する。

なお、調査報告を内閣総理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) 本業務の実施状況等の官民競争入札等監理委員会への報告及び公表

当省は、請負者の政府認証基盤の運用・保守業務の実施状況について、毎年度、官民競争入札等監理委員会へ報告するとともに、公表する。

(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 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。

ウ　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に通じて、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きを行うものとする。

政府認証基盤の運用・保守業務民間競争入札実施要項(案)

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 21 年度	平成 22 年度	平成 23 年度
政府認証基盤の運用・保守の請負業務					
	人件費	常勤職員	－	－	－
		非常勤職員	－	－	－
	物件費		－	－	－
	請負費	役務等（運用・保守）	678,720	622,620	622,574
		施設使用料等	199,080	199,080	199,080
計(a)			877,800	821,700	821,654
参考値(b)	減価償却費		－	－	－
	退職給付費用		－	－	－
	間接部門費		－	－	－
(a)＋(b)			877,800	821,700	821,654

（注記事項）

※　請負業務のため、費用の詳細な内訳の開示は受けられない。

・役務等（運用・保守）には、人件費の他、IC カードなどの消耗品、通信費、郵送料が含まれる。

・施設使用料等は、現在借用しているマスタセンタのバックアップセンタの施設使用料と通信回線使用料のこと。

運用業務を見直し、22 年度以降の予算を削減（調達仕様書において運用要員３名を削減）。その結果、22 年度においては、請負額が前年度より 56,100 千円減少している。

2　従来の実施に要した人員

	平成 21 年度	平成 22 年度	平成 23 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（３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（５名以上）	６名（４名以上）	６名（４名以上）
一般 IA 操作員	３名（３名以上）	３名（２名以上）	３名（２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。
・22 年度以降、運用業務を見直し、運用業務従事者の人数に関しては、運用責任者補佐、上級 IA 操作員、一般 IA 操作員の最低人数を 21 年度に比べそれぞれ１名（合計３名）を削減して調達を実施したが、事業者が前年と同様の人数による提案であったため、要員数は変わっていない。

○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。
⇒23 年度については、運用責任者（１名）が適合している。
・上級 IA 操作員、一般 IA 操作員（常駐：上級４名以上、一般２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。
⇒23 年度については、上級 IA 操作員（６名）及び上級 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。
⇒23 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。
⇒23 年度については、８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。
⇒23 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。
⇒23 年度については、５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	→	→	→	→	→	→	→	→	→	→	→	→
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 21～23 年度の主な状況は以下のとおり。

（単位：件）

	平成 21 年度	平成 22 年度	平成 23 年度
相互認証(新規・更新・失効)件数	1	3	2
認証情報公開サービスの利用件数	9,240,454	11,817,524	11,739,609
証明書検証サービスの利用件数	8,083,242	10,280,234	12,403,108
証明書の発行枚数	649	10,795	4,972
問い合わせ対応件数	66	71	66
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）	39	40	39
予防保守件数（上段：脆弱性調査件数）	1,075	1,181	1,304
予防保守件数（下段：ﾊﾟｯﾁ等適用件数）	130	54	55
利用者環境の維持	91	65	31

（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。

・システム運用開始当初（平成 20 年 1 月）に発行した証明書が 3 年間の有効期間を迎え、平成 22 年度から 23 年度にかけて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９式、監視カメラ 20 台、IC カード認証装置 15 台、指紋認証装置７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 39 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）

・現行の施設・設備又は請負者の提案する施設・設備で運用すること。

・現行の施設・設備で運用する場合、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、及び上記、請負者が保有している設備及び物品は除く。）使用料等（現行月額 15,800,000 円（税抜）は、請負者の負担とする。
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×２）：187,500 円

※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。

・請負者の提案する施設・設備で運用する場合、以下の条件を満たすこと。また、現行機器等の移設・据付・調整・システム設定・テスト等は、請負者の責任と負担において対応すること。
（条件）
・提案施設・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。
・現行機器の移設に伴う本システムのサービス停止時間は、24 時間（日曜日の 0 時～24 時まで）内とし、回数は４回を限度とする。

4　従来の実施における目標の達成の程度

SLA 達成率	平成 21 年度		平成 22 年度		平成 23 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)						
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	1回/年以内	0件	1回/年以内	0件	1回/年以内	0件
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	0.00001446	1.0秒以内	0.00003748	1.0秒以内	0.00003629
証明書検証サービス	1.0秒以内	0.18	1.0秒以内	0.20	1.0秒以内	0.19

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（セキュリティ編、ブリッジ CA 編、官職 CA 編、アプリケーション CA 編、
アプリケーション CA２編、ネットワーク編）

・LRA 仕様書（基本設計書、詳細設計書）

・IC カードシステム仕様書

・暗号移行検証環境　構築仕様書

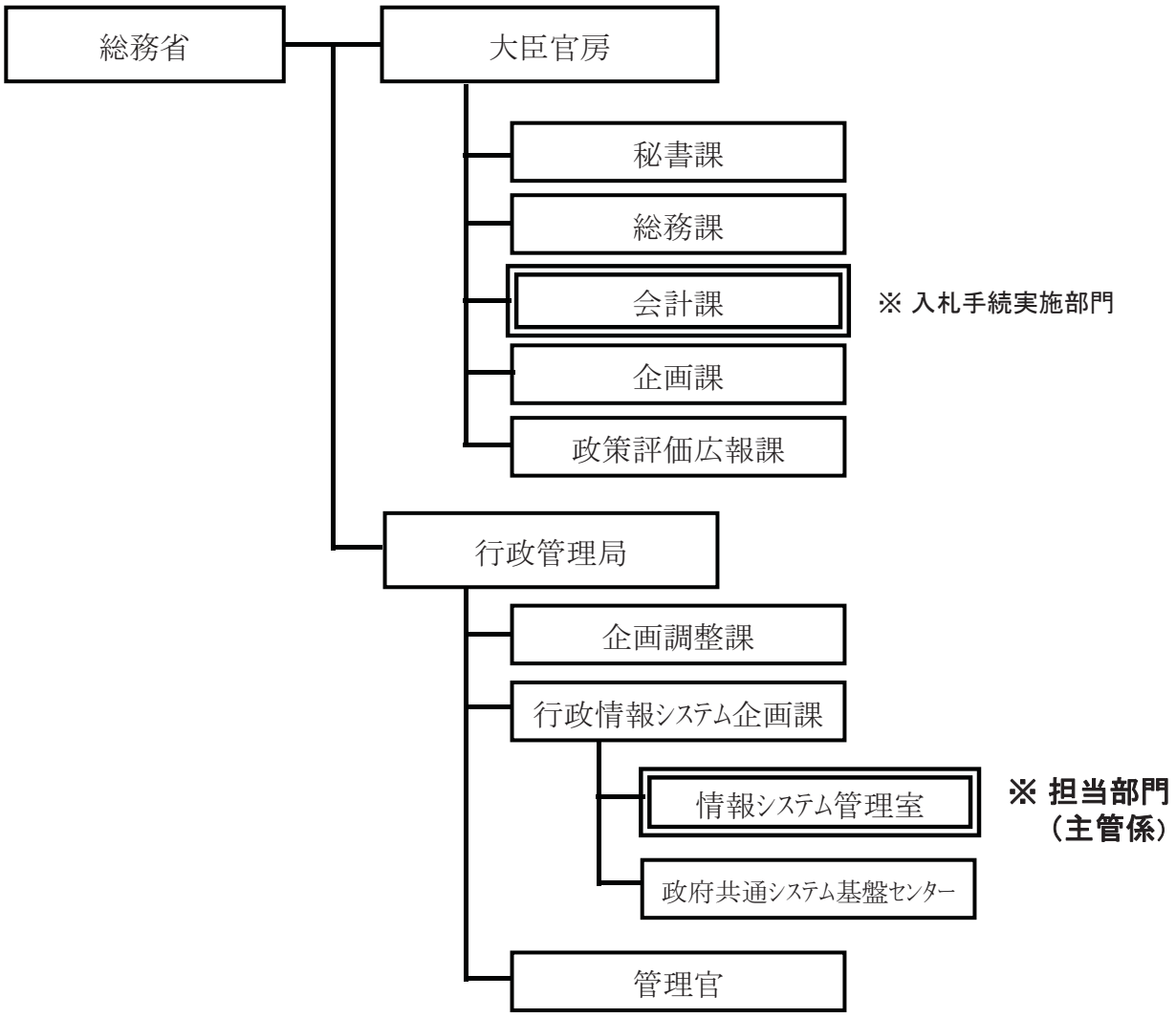
2　１に示す資料のほか、現行の手順書及び３に示す研修資料については、請負者に対し提供を行う。

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

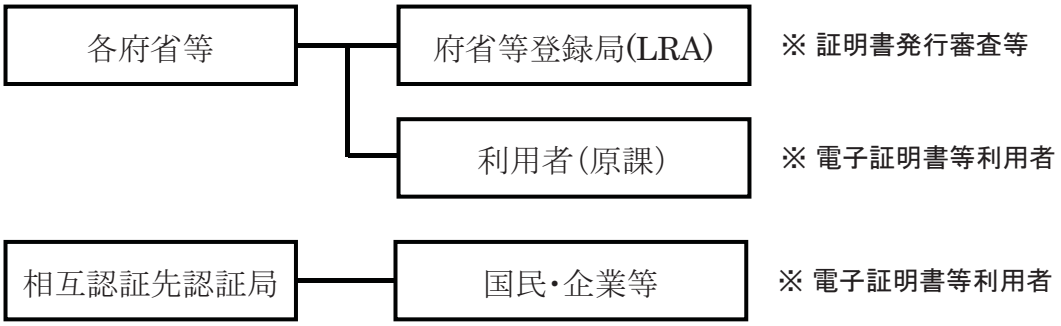
別紙２

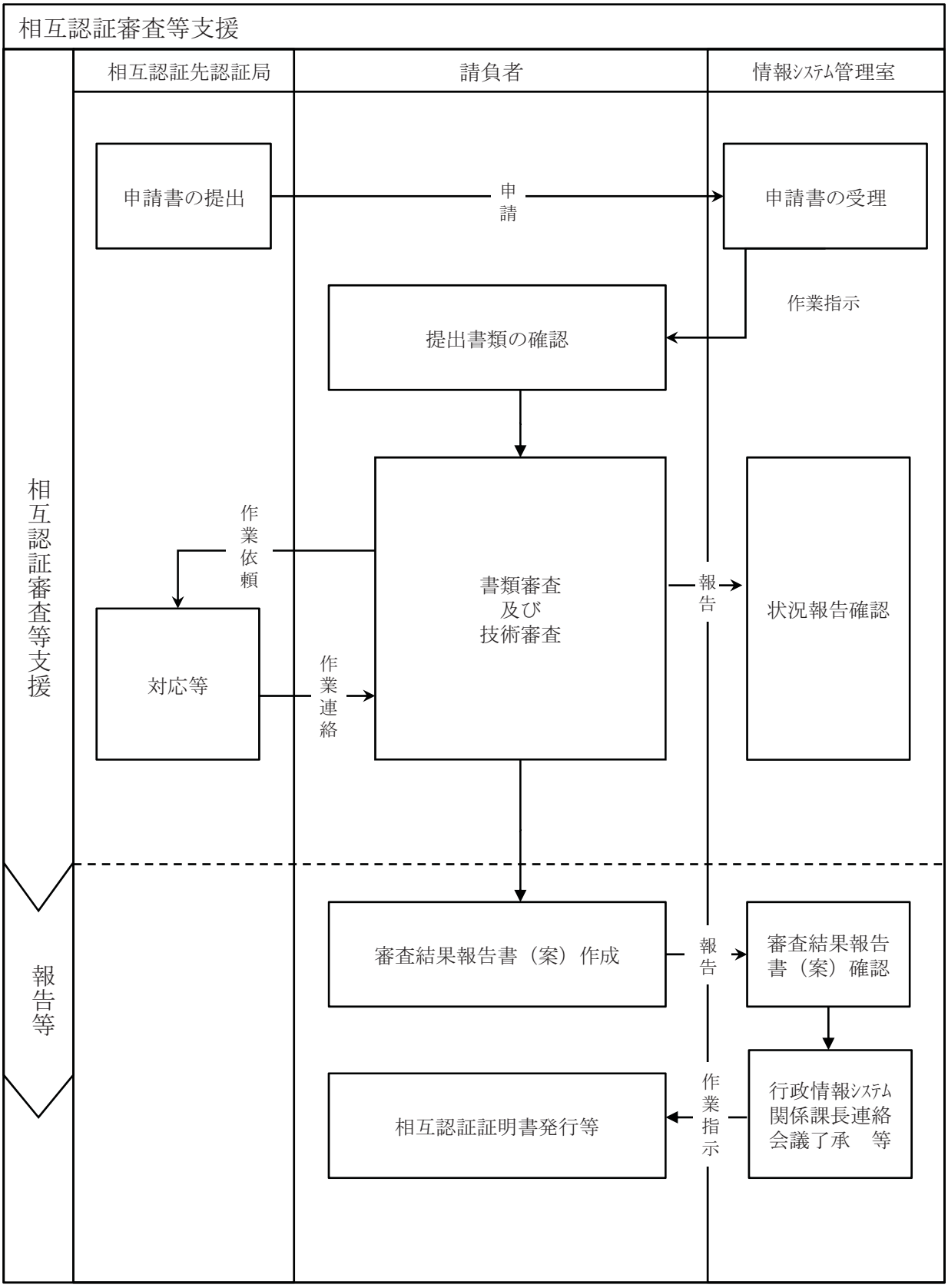
運 用・保 守 業 務 フ ロ ー

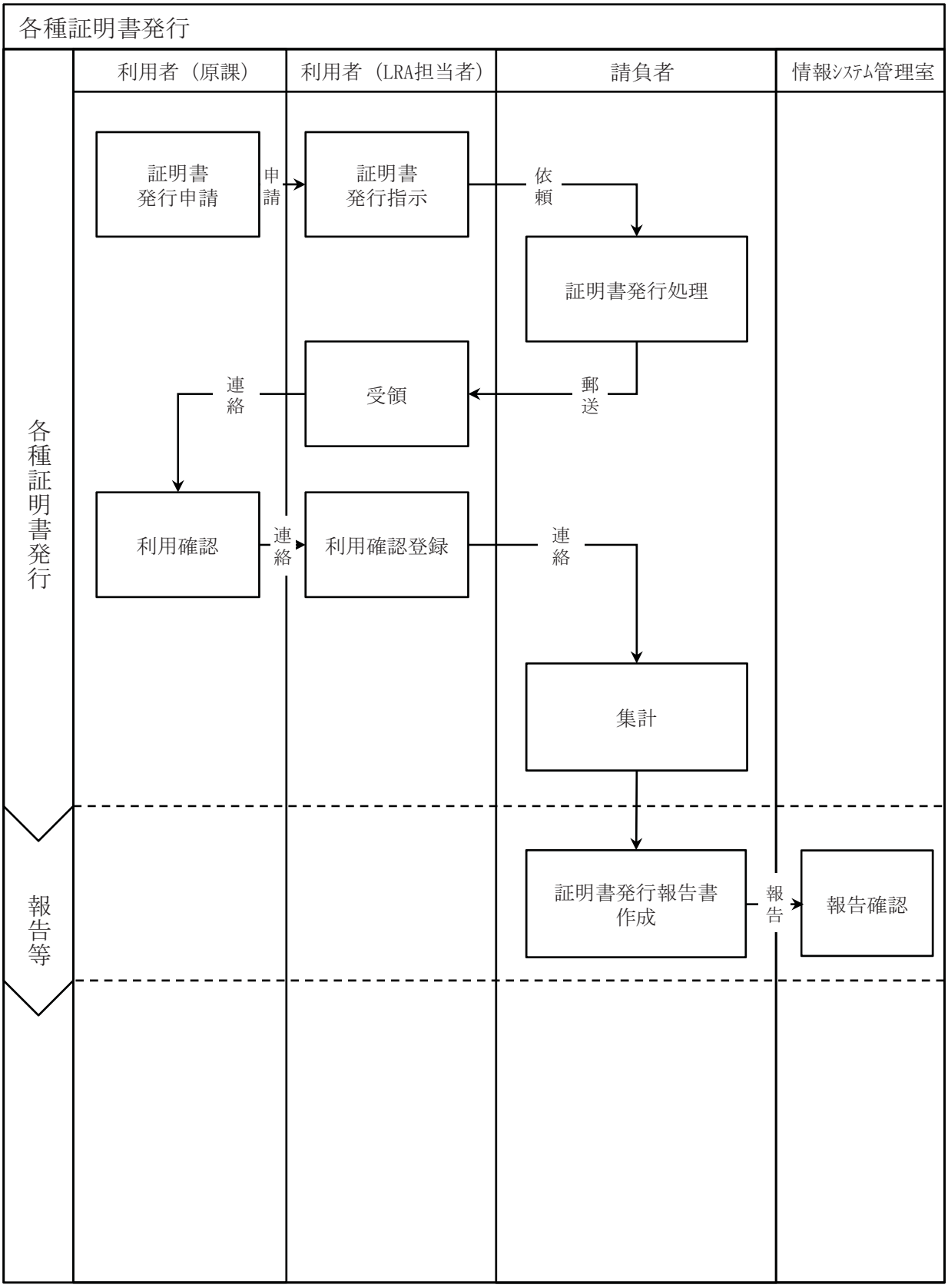
総務省の組織（関係部門）及び利用者は、下図のとおり。
また、運用・保守業務の主な業務フローを次頁以降に示す。

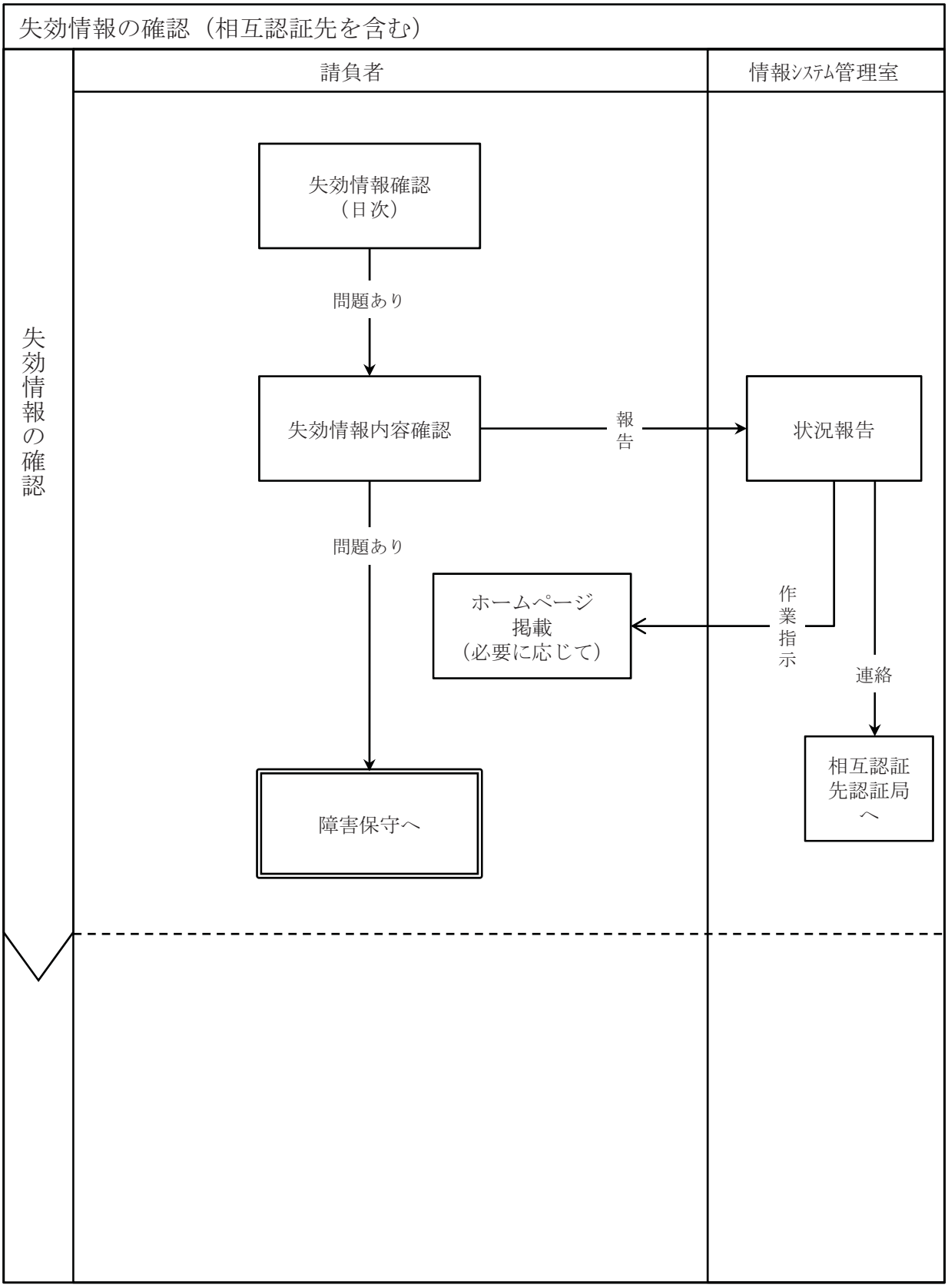


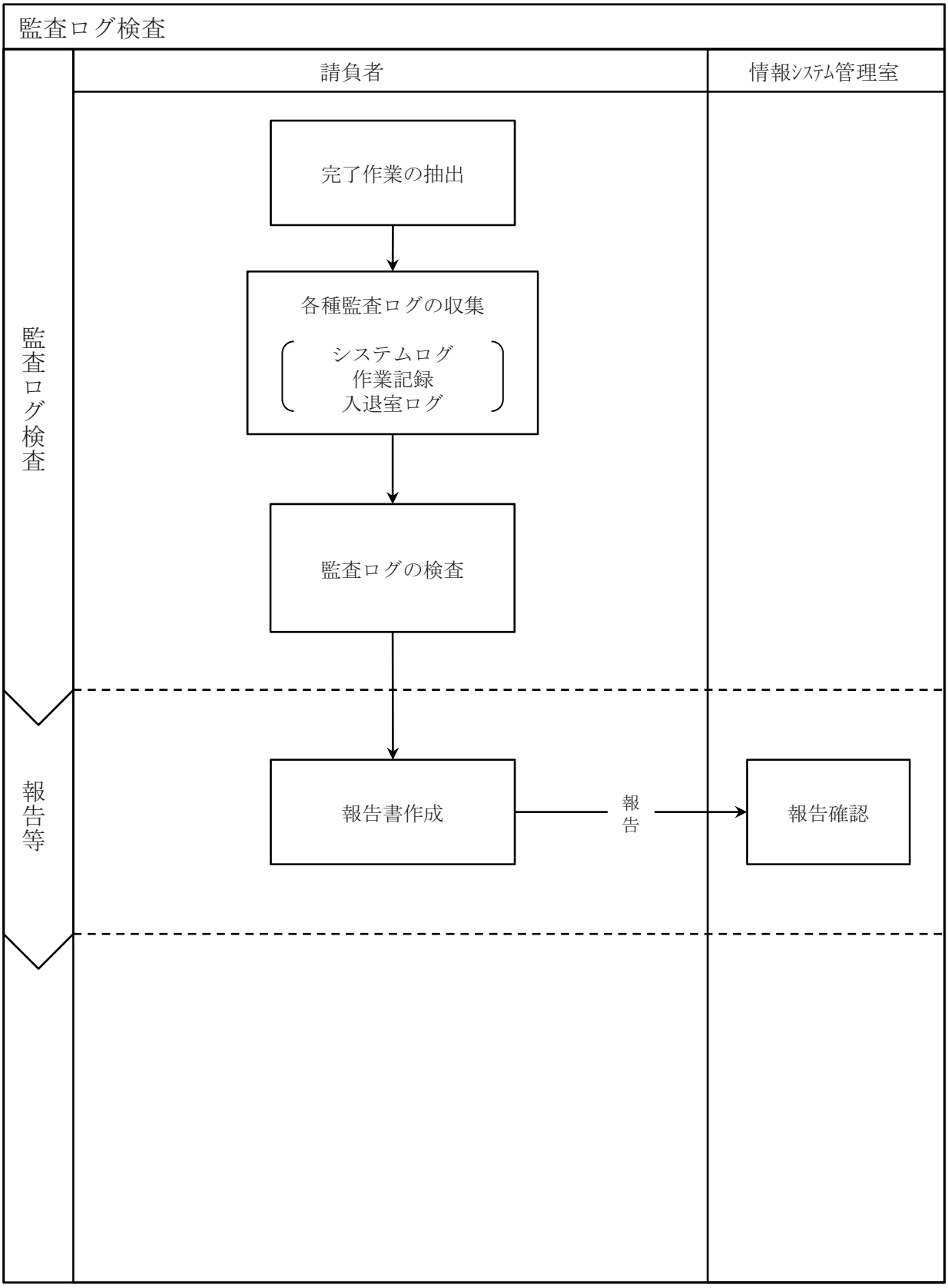
【 利用者 】

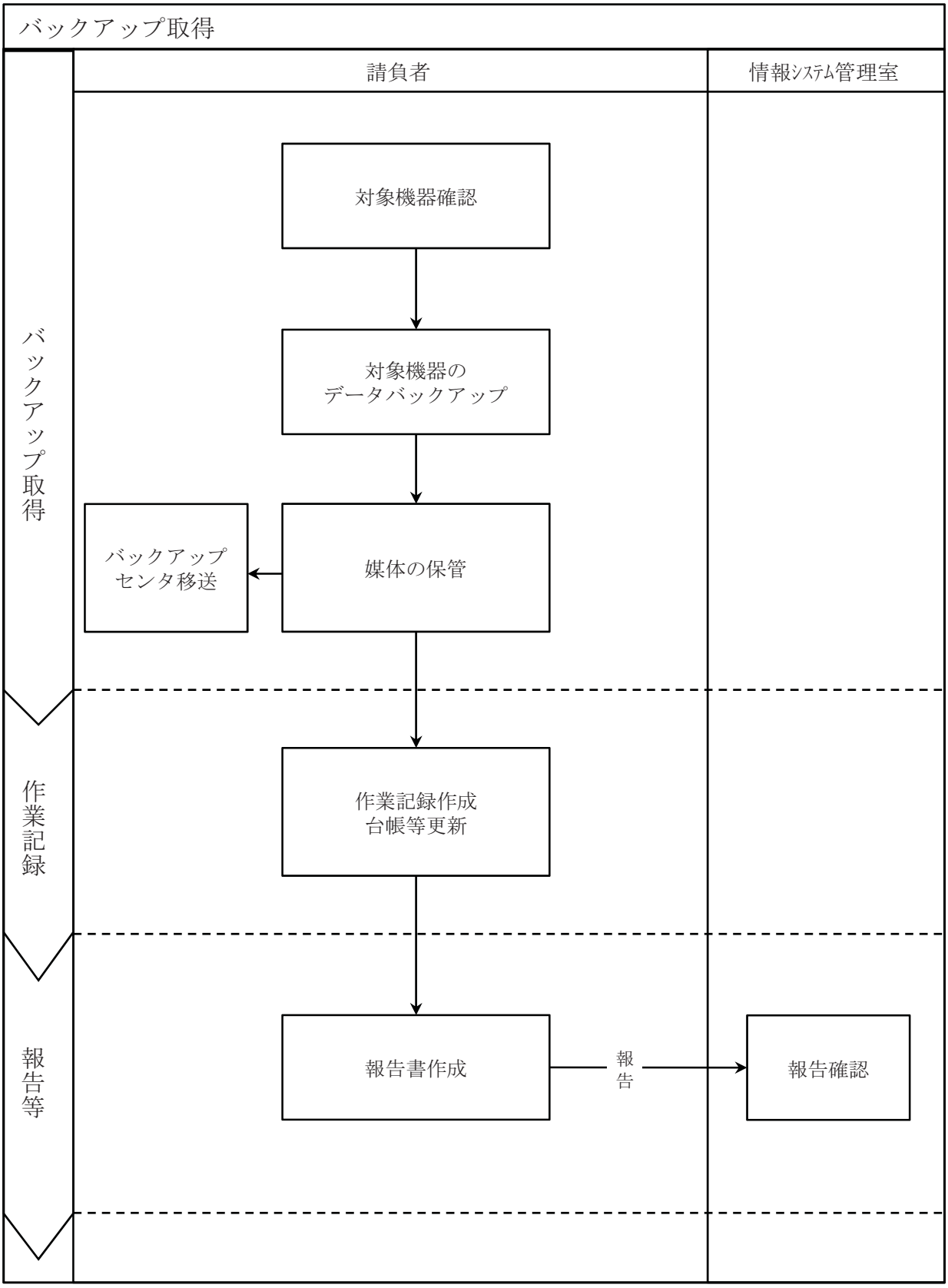


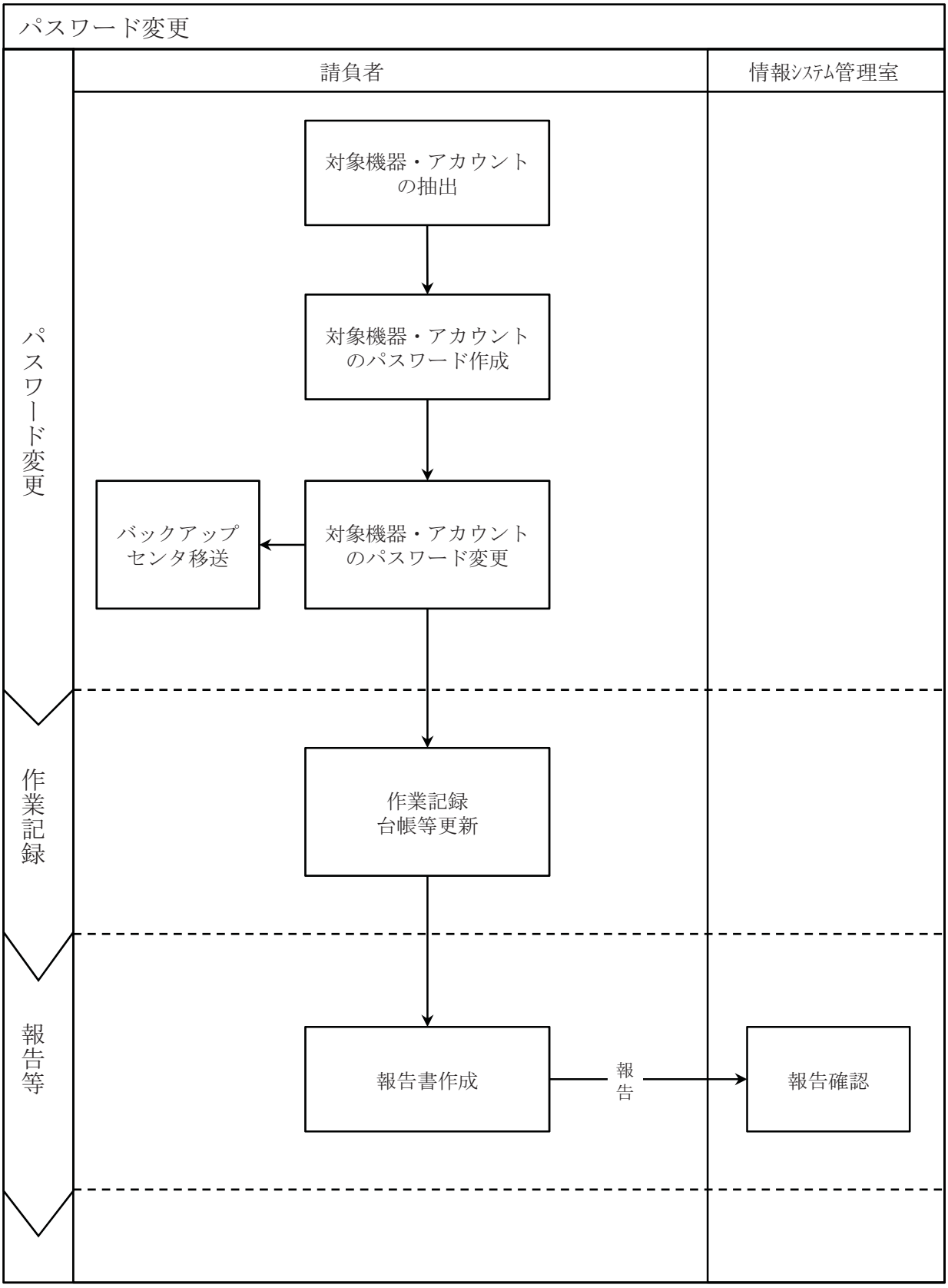

相互認証審査等支援
相互認証先認証局
請負者
情報ｼｽﾃﾑ管理室
申請書の提出
申請
申請書の受理
作業指示
提出書類の確認
相互認証審査等支援
作業依頼
書類審査
及び
技術審査
報告
状況報告確認
対応等
作業連絡
報告等
審査結果報告書（案）作成
報告
審査結果報告書（案）確認
行政情報ｼｽﾃﾑ関係課長連絡会議了承　等
相互認証証明書発行等
作業指示

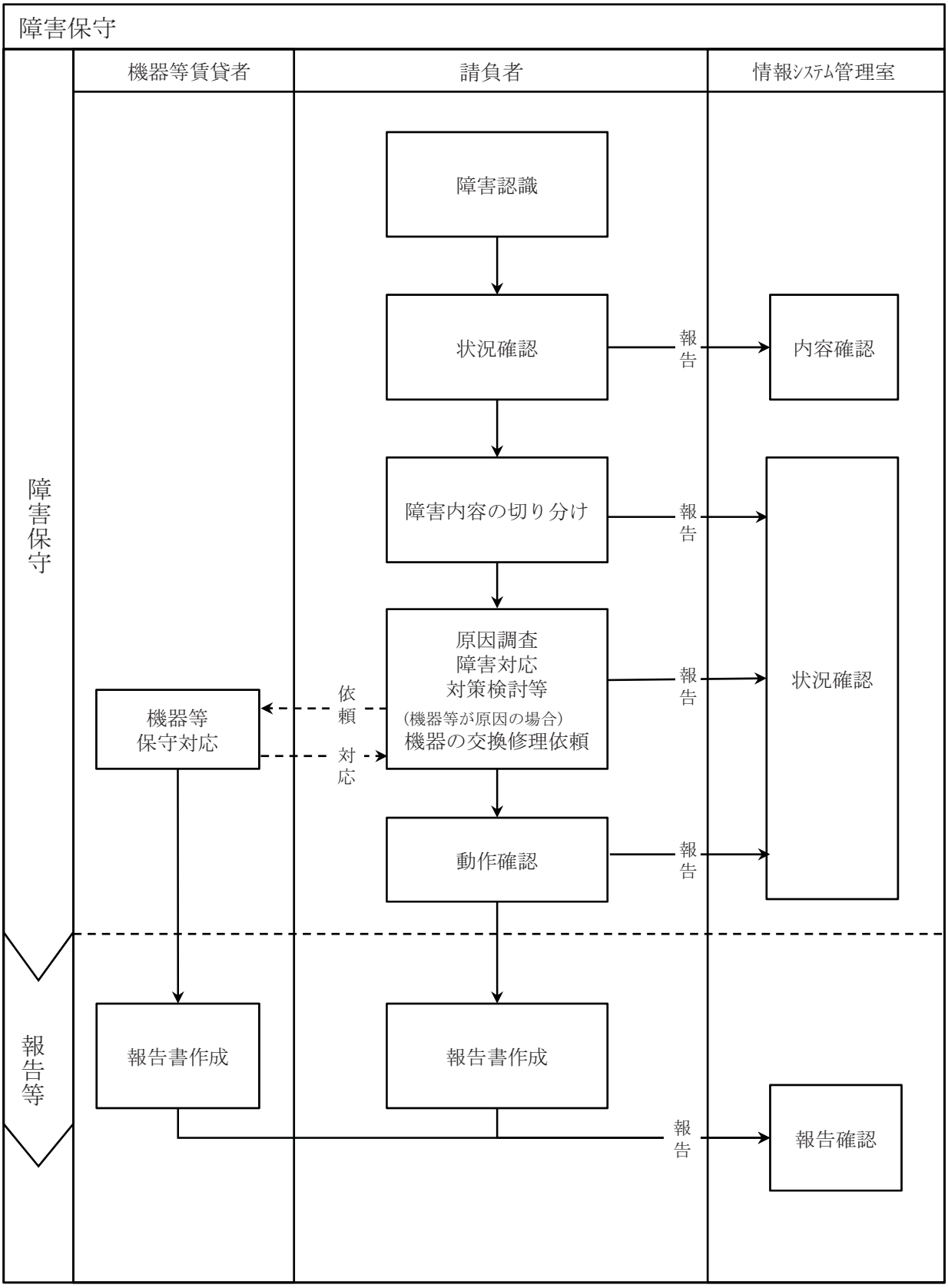

各種証明書発行
利用者（原課）
利用者（LRA担当者）
請負者
情報ｼｽﾃﾑ管理室
各種証明書発行
報告等
証明書
発行申請
申請
証明書
発行指示
依頼
証明書発行処理
連絡
受領
郵送
利用確認
連絡
利用確認登録
連絡
集計
証明書発行報告書
作成
報告
報告確認

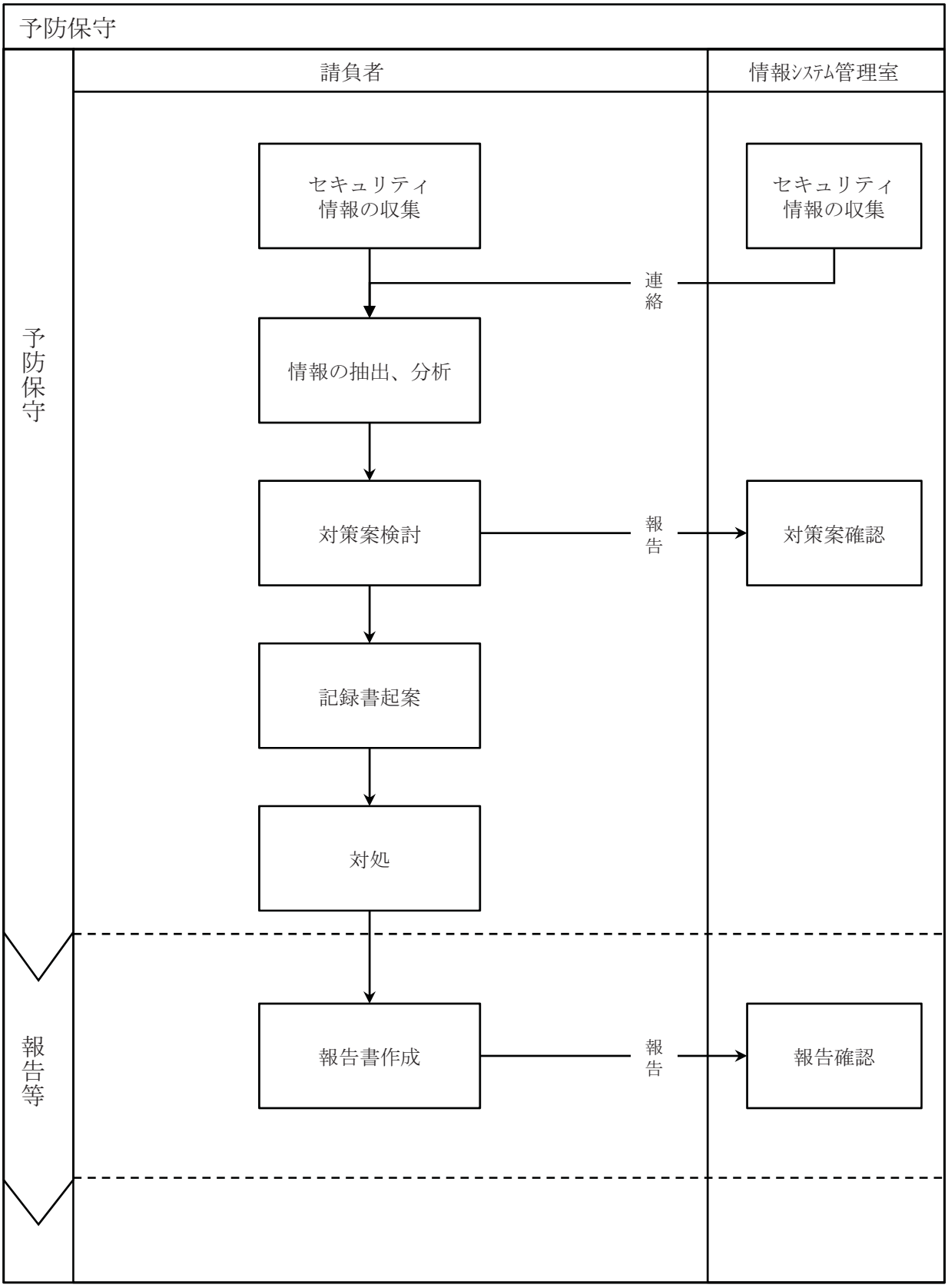

失効情報の確認（相互認証先を含む）
失効情報の確認
請負者
情報ｼｽﾃﾑ管理室
失効情報確認
（日次）
問題あり
失効情報内容確認
報告
状況報告
問題あり
ホームページ
掲載
（必要に応じて）
作業指示
連絡
相互認証
先認証局
へ
障害保守へ

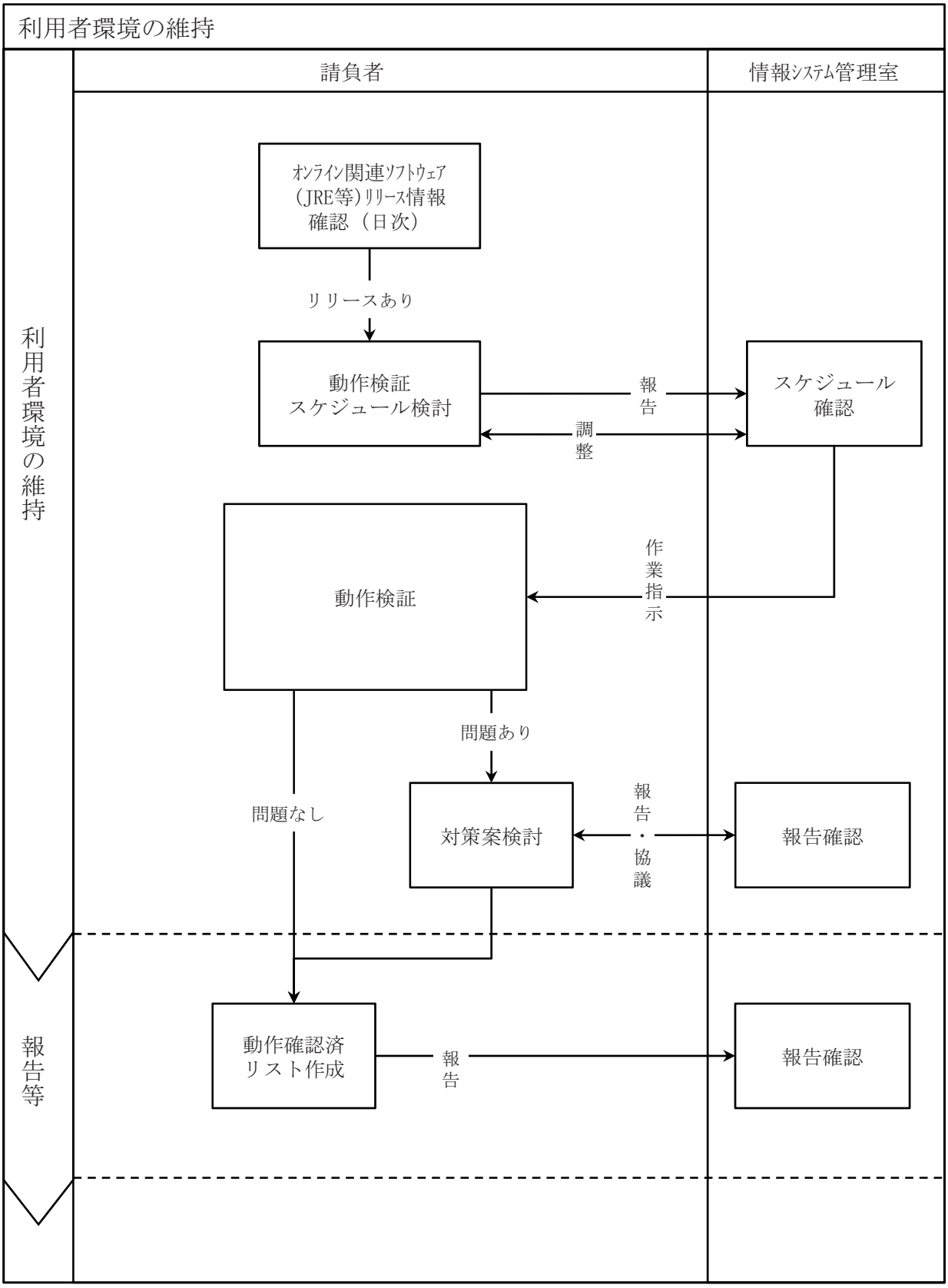

監査ログ検査
請負者
情報ｼｽﾃﾑ管理室
監査ログ検査
完了作業の抽出
各種監査ログの収集
システムログ
作業記録
入退室ログ
監査ログの検査
報告等
報告書作成
報告
報告確認


バックアップ取得
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
対象機器の
データバックアップ
媒体の保管
バックアップ
センタ移送
作業記録作成
台帳等更新
報告書作成
報告
報告確認


パスワード変更
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
報告確認


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
報告
内容確認
障害内容の切り分け
報告
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
報告
状況確認
依頼
対応
機器等
保守対応
動作確認
報告
報告書作成
報告書作成
報告
報告確認


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
連絡
情報の抽出、分析
対策案検討
報告
対策案確認
記録書起案
対処
報告等
報告書作成
報告
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）
リリースあり
動作検証
スケジュール検討
報告
調整
スケジュール確認
動作検証
作業指示
問題あり
問題なし
対策案検討
報告・協議
報告確認
報告等
動作確認済リスト作成
報告
報告確認

別添1

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 年度に、より安全な暗号アルゴリズムへの移行を行う予定である。これに伴い、相互認証先認証局（13 認証局）との相互認証更新が予定されている。

本件は、システム更改により平成 25 年３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

・アプリケーション認証局（アプリケーション CA、AP 認証局、APCA）

各府省が運営しているWebサーバ等で必要とする、コード署名証明書及びドキュメント署名証明書を発行する CA で、政府共用認証局を構成する CA の一つ。

・アプリケーション認証局2（アプリケーション CA2、AP 認証局2、APCA2）

新たな暗号アルゴリズムに対応したアプリケーション認証局。

・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電子的な文書。行政機関等の CA が官職証明書を発行する。

・官職認証局（官職 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 CA で、政府共用認証局を構成する CA 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したり、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 CA の公開鍵に対して、自 CA の対応する秘密鍵で署名した公開鍵証明書。自 CA の公開鍵の正当性を保証する。

・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 CA。各府省単位に構成される府省認証局を集約した認証局。官職 CA とアプリケーション CA から構成される。

・相互認証証明書

2つの異なる認証ドメインの CA 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。GPKI では、政府共用 CA の官職 CA、民間 CA 又は商業登記 CA とBCA の間で相互認証証明書が発行される。

・ドキュメント署名証明書

インターネット等を利用して、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したり、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。

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

府省等単位で設置される組織で「府省等登録局」のこと。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。

・ブリッジ認証局（ブリッジ CA、BCA）

政府共用 CA の官職 CA 及び民間 CA 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 CA。

・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。GPKI 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電子的な文書。政府共用 CA の官職 CA が発行する。

・リンク証明書

CA の鍵更新に伴い同時に存在することとなる新しい CA 鍵ペアと古い CA 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、新しい世代の鍵で古い世代の鍵を署名した証明書、古い世代の鍵で新しい世代の鍵を署名した証明書を示す。

・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（Authority Revocation List/ Certificate Revocation List）
証明書の失効リスト。

・ CVS（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。

・ 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 13 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。 ・ 相互認証する際の規準である相互認証基準をもとに書類審査及び技術審査を行う。 ・ 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。 ・ 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。 ・ 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。 ・ 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。 ・ 平成 23 年度のアクセス件数は、約 1,174 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。 ・ 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。 ・ 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。 ・ 平成 23 年度のアクセス件数は、約 1,240 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、サーバ証明書、コード署名証明書及び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。

サービス	業務概要及び実施手順
	・ 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（旧霞が関 WAN）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。 ・ 受け付けた情報をもとに証明書を発行する。 ・ 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。 ・ 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。
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。 ・ 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。

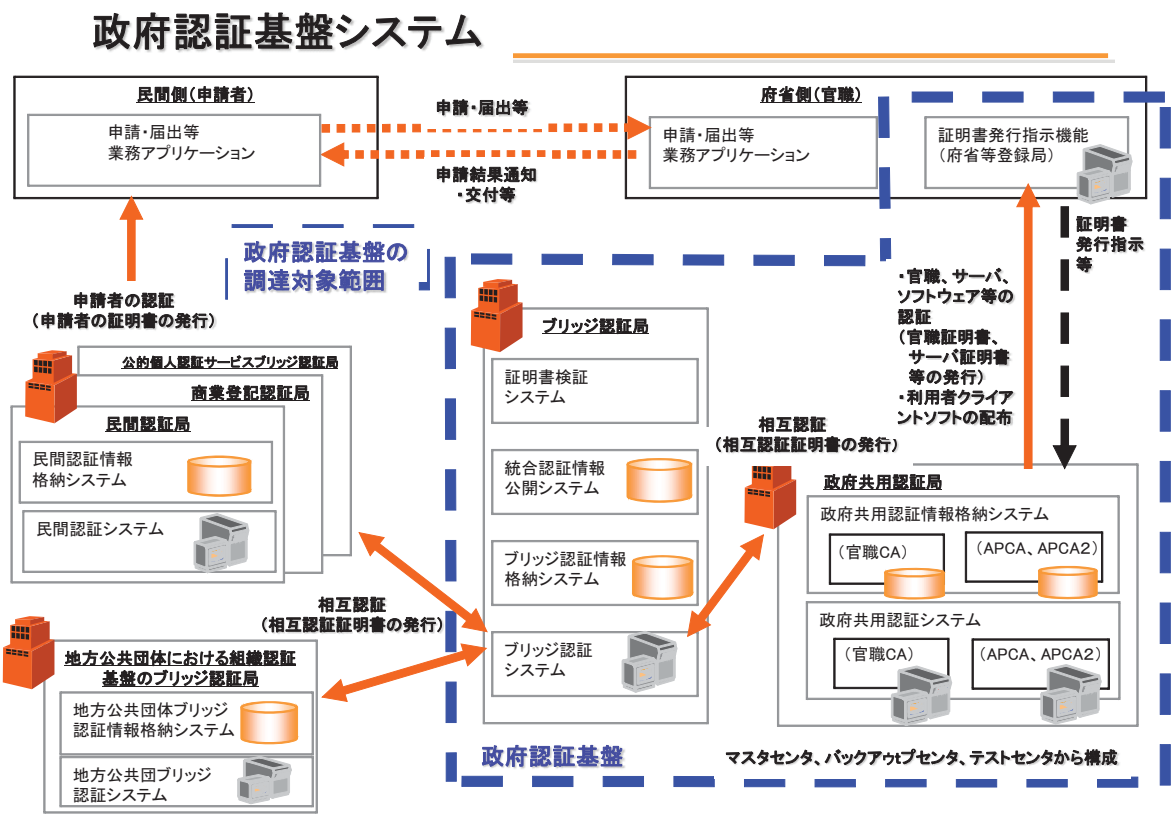
成果指標・目標：

「5　信頼性等要件　（1）信頼性要件」を参照のこと。

（4）調達の範囲

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。 ・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。 ・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。 ・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。 ・実施した結果を主管係に報告する。	5年に1度 （26 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。 ・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 相手認証局の数：13 認証局

	を、あらかじめ定められた審査基準に基づき審査する。 ・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。 ・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。 ・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、あらかじめ定められた実施手順に基づき、テスト環境を用いて審査する。 ・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 相手認証局の数：13 認証局 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、主管係の指示のもと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。 ・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。 ・『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。 ・発行した相互認証証明書をリポジトリに登録する。 ・実施した結果を主管係に報告する。	随時 相手認証局の数：13 認証局 証明書の有効期間：5年

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、主管係の指示のもと当該認証局と失効日時を調整する。 ・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。 ・作成した手順書に従い、相互認証証明書を失効する。 ・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。・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。 ・官職認証局側で発行した当該証明書をリポジトリに登録する。 ・実施した結果を主管係に報告する。	随時 各証明の有効期限：3年（暗号移行後は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。 ・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。 ・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。 ・実施した結果を主管係に報告する。	随時 相互認証局の数：13 認証局
テスト環境用証明書の発行（相互認	・相互認証を希望する認証局及び各府省からの	随時

証証明書、模擬民間 CA の EE 証明書）	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。	23 年度実績 6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。 ・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。 ・また、年次で LRA システムに対して、休日の設定を行う。	随時 23 年度実績 6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。・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。 ・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。 ・実施した結果を主管係に報告する。	5年に1度 （26 年度予定）
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。 ・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 23 年度実績 4,729 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。 ・『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。 ・発行した相互認証証明書をリポジトリに登録する。 ・実施した結果を主管係に報告する。	5年に1度
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。・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。 ・実施した結果を主管係に報告する。	随時 各証明書の有効期間：3年（暗号移行後は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 23 年度実績 146 枚

(c) アプリケーション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）	・予め作成されているキーセレモニースクリプト（手順書）に基づき、サーバ機器や HSM 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）が実施する鍵生成を支援するとともに、自己署名証明書の発行を行う。 ・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。	設立時 （25 年3月予定）
テスト環境用証明書の発行（模擬 APCA 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サーバ証明書やコード署名証明書等を発行する。	随時 23 年度実績 6枚

(d) 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。 ・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。 ・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。 ・問題ある失効情報の場合には、主管係の指示のもと、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。 ・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 照会対応

作業項目	作業内容	頻度・ﾀｲﾐﾝｸﾞ
LRA 相互認証先認証局 CA/ブラウザフォーラム等外部組織 電子申請等アプリケーション 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、内容確認をしたうえで、運用面や技術面の調査等を行う。 ・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。 ・主管係による回答案の確認後、照会元に回答を行う。	随時 23 年度実績 71 件

D 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。 ・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。 ・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。 ・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。 ・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 23 年度実績 12 件

E 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、アプリケーション認証局及びアプリケーション認証局2の CP/CPS 準拠性に対し、主管係からの指示のもと、監査人と監査スケジュールの調整を行う。 ・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。 ・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
WebTrust 検証の対応	・アプリケーション認証局及びアプリケーション認証局2の WebTrust for CA 2.0 検証に対し、主管係からの指示のもと、監査人と監査スケジュールの調整を行う。 ・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。 ・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

F 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。 ・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。 ・不適切な操作が実施されていた場合には、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

G 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。 ・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

H 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。 ・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 合計：2,000枚 増加分：400枚／年

I 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。 ・記録書や台帳類をもとに、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。 ・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

J 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。 ・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	年2回

	とともに、研修当日に使用する申請データを作成する。 ・各教育教材に従って、各府省等 LRA 要員向けに説明する。	

K 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。 ・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。 ・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。	年次
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、 ・運用要員教育に使用する教育教材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。 ・自己点検の内容をもとに、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

L 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。 ・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

M 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。 ・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、あわせて修正する。	随時

（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、WebTrustの維持	・総務省情報セキュリティポリシー、WebTrust for CA（認証局のための WebTrust 規準）、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。 ・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。 ・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。 ・脆弱性情報を保管管理する。	日次

(b) インシデント管理

作業項目	作業内容	頻度・ﾀｲﾐﾝｸﾞ
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。 ・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。 ・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。 ・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。 ・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。	年次
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。 ・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

(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。 ・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。 ・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。 ・不正アクセス等の状況とりまとめを日次行う。	24 時間
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。 ・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 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
データバックアップに係るテープ交換（マスタセンタ）	・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。 ・世代管理されているテープ媒体のうち、対象となるテープ媒体を確認する。 ・対象機器において装填されているテープ媒体（LTO テープ）を取り出し、新たなバックアップ用のテープ媒体を装置に装填する。 ・取り出した媒体を定められた場所に保管管理し、管理台帳を更新する。	週次
データバックアップに係るテープ交換（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。 ・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うえで予備機にリストアする。 ・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
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。 ・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。 ・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。 ・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。 ・変更したパスワードを封入・封印のうえ、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。 ・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。 ・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
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
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。 ・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	・平成29年3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、アプリケーション認証局2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作業を実施する。	機器等の更改時

（エ） 政府認証基盤の暗号移行対応

作業項目	作業内容	頻度・ﾀｲﾐﾝｸﾞ
暗号移行に係る相互認証審査支援	新たな暗号アルゴリズムでの相互認証を希望する全認証局に対して、相互認証審査支援（書類審査及び技術審査）を行う。（相互認証先認証局である 13 の認証局を約1年間で実施）	25 年度
暗号移行に係る鍵更新（ブリッジ認証	「政府機関の情報システムにおいて使用されて	26 年度

局、官職認証局）	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）」に基づき、ブリッジ認証局及び官職認証局において、平成 26 年度早期に鍵更新方式による新たな暗号アルゴリズムに移行する。（ブリッジ認証局及び官職認証局を対象として、2～4日程度の作業を想定） また、各 LRA に対して、各種証明書の発行申請をするためのログイン用 IC カードを発行して、手交により配付する。	
暗号移行に係る相互認証取り交し	暗号移行に係る鍵更新後、相互認証審査を行った相互認証先認証局と新たな暗号アルゴリズムで相互認証証明書を発行して、リポジトリに登録する。（相互認証先認証局である 13 の認証局を約2か月で実施）	26 年度
暗号移行に係る証明書の一斉切替（官職認証局）	各府省で使用している官職証明書及び利用者証明書を新たな暗号アルゴリズムによる IC カードへ切り替える。（平成 26 年度早期から発行を開始し、約 20,000 枚を約6か月間で発行） また、暗号移行直前（平成 25 年度後半から 26 年度早期までの期間）に、有効期間が満了する証明書が大量にあることから、短期間の間に旧暗号の IC カードを発行する可能性がある。（最大で約 9,000 枚の発行を想定）	25 年度 及び 26 年度
暗号移行に係るアプリケーション認証局2の自己署名証明書の発行	平成 25 年3月頃にアプリケーション認証局2（root）における自己署名証明書の発行（キーセレモニー）を、25 年 11 月頃にアプリケーション認証局2（sub）における自己署名証明書の発行（キーセレモニー）を行う。（それぞれ3～4日の作業） なお、各府省は 25 年 12 月までに、暗号アルゴ	24 年度 及び 25 年度

	リズムに対応したサーバ証明書、コード署名証明書及びドキュメント署名証明書へ全て切り替える予定である。	
暗号移行に係るアプリケーション認証局の廃止	平成 26 年 1 月頃に、自己署名証明書の失効、アーカイブデータの取得及び HSM の初期化を含む CA 秘密鍵の破棄等の廃止作業を行う。（3～4日の作業）	25 年度

（オ） 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、問題の切り分け、応急措置、情報収集、主管係・機器ベンダへの連絡・調整、修復後の確認等を行う。 ・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。 ・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。 ・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 23 年度実績 39 件

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。 ・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。 ・作業完了の後、作業報告書の作成を行う。 ・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 23年度実績 調査:1,304件 適用:55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。 ・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。 ・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。 ・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 23年度実績 31件

（カ） 認証局施設・設備の管理業務

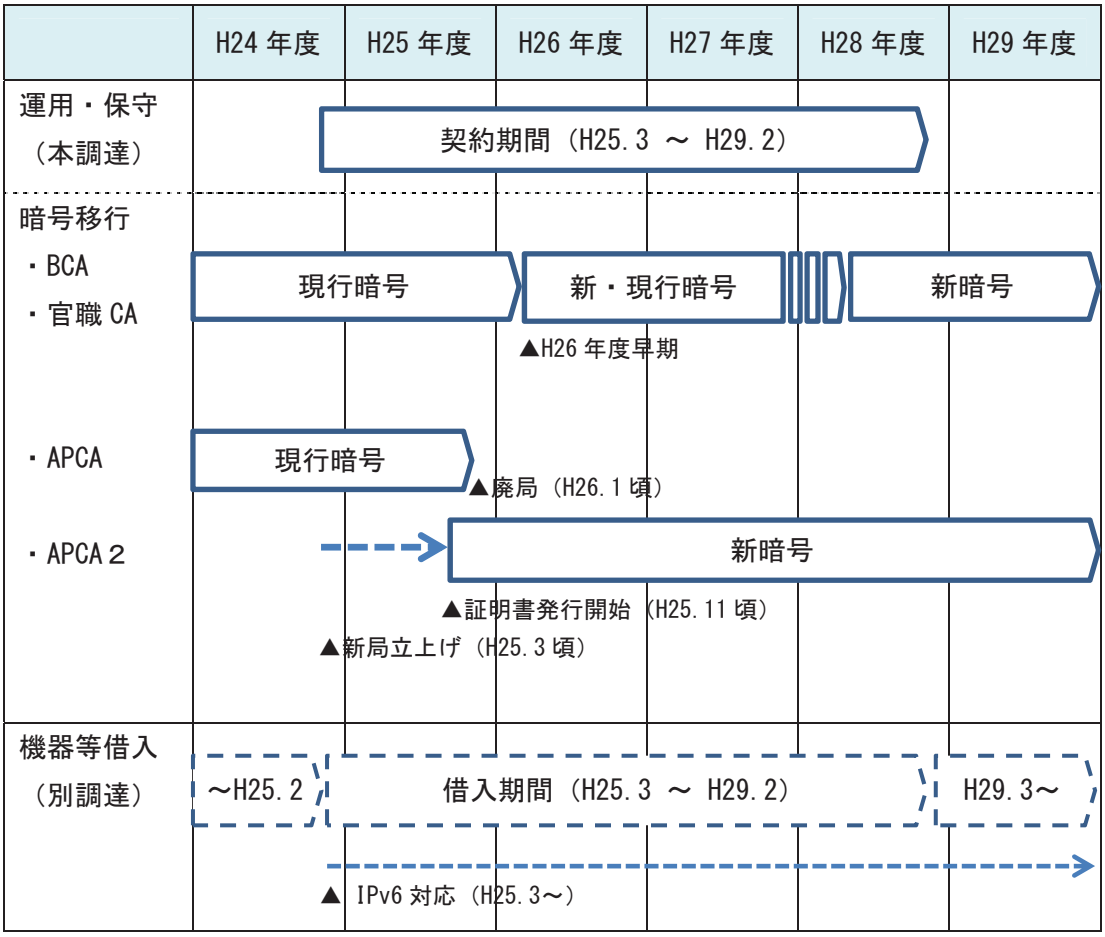
作業項目	作業内容	頻度・タイミング
施設・室に関する管理	・運用要員等の変更がある場合に、各室（セキュア室、関連サーバ室、操作室、ネットワーク室、監視室、事務室、テストセンタ及びバックアップセンタ各室）への入室に対する生体認証の登録、変更及び削除作業を行う。 ・定期的に登録されている入室権限に誤りがないことを確認する。 ・各室で保存されている入退室記録等を定期的（マスタセンタ：週次、バックアップセンタ：月次）に記録媒体に移動して、保管・管理する。 ・施設で障害が発生した場合には、主管係への報告した上で、問題の切り分け、応急措置、情報収集及び修復作業を行う。	随時
設備、備品等に関する管理（回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

（キ）報告書の作成

作業項目	作業内容	頻度・ﾀｲﾐﾝｸﾞ
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。 ・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。 ・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

平成 25 年3月1日(金)から平成 29 年2月 28 日(火)まで。



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

次の文書の書面及び電子データ（CD-R）（各一式）を納入する。

納入成果物	納入期限
・実施計画書 （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）	平成 25 年3月8日
・運用状況報告書 （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 （障害・案件一覧、個別障害対応報告書　等） ・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 ・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、最終版を平成 29 年2月 28 日に納入

3 情報システムの概要

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する。

ブリッジ認証局は、政府共用認証局、公的個人認証サービス、地方公共団体組織認証基盤、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を発行する。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、政府認証基盤における統合リポジトリで公開する。

政府共用認証局は、官職認証局、AP 認証局及び AP 認証局2から構成され、各府省等の LRA 担当者が政府共通ネットワーク経由で証明書の発行・失効を指示する機能として LRA システムを持つ。

官職認証局は、申請・届出等手続における各府省の官職証明書及び利用者証明書を発行する。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、住民基本台帳カードを参考とした仕様とする。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。

AP 認証局及び AP 認証局2は、各府省が運営している Web サーバ等で必要とするサーバ証明書やコード署名証明書、ドキュメント署名証明書を発行する。また、AP 認証局では、「WebTrust for CA」の認定を取得している。「WebTrust for CA」の認定を維持するために毎年度の定期的な検証が必要であり、要件は「認証局のための WebTrust プログラムバージョン 2.0」に規定されている。

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）は原則として府省ごとに設置される（平成 24 年4月現在、21 府省等が設置）。

本件の対象となる情報システムの詳細は、別添資料1「政府認証基盤 暗号アルゴリズム移行に係る相互運用要件（平成 21 年3月 30 日 平成 24 年3月 23 日改定 共通システム専門部会了承）」及び別途閲覧に供する以下の仕様書を参照。

- 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（アプリケーションCA編）
- 構築仕様書（アプリケーションCA2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
- 暗号移行検証環境 構築仕様書

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

4 規模・性能の概要

（1）規模

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。

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	ブリッジ CA システム					政府共用 CA システム		
			計	MC	BC	TC	JM	計	MC	BC
1. サーバ										
(1)	CA/ディレクトリサーバ(BCA)	6	6	2	1	3	0	0	0	0
(2)	CA/ディレクトリサーバ(官職 CA)	3	0	0	0	0	0	3	2	1
(3)	CA/ディレクトリサーバ(アプリケーション CA)	6	3	0	0	3	0	3	2	1
(4)	CA/ディレクトリサーバ(民間) AP テスト用	2	2	0	0	2	0	0	0	0
(5)	CA/ディレクトリサーバ(府省兼汎用) AP テスト用	1	1	0	0	1	0	0	0	0
(6)	OCSP サーバ AP テスト用	3	3	0	0	3	0	0	0	0
(7)	統合リポジトリサーバ	7	7	2	2	3	0	0	0	0
(8)	公開リポジトリサーバ(A)	8	8	4	2	2	0	0	0	0
(9)	公開リポジトリサーバ(B)	5	5	2	2	1	0	0	0	0
(10)	ディスクアレイ装置(A)	8	8	4	2	2	0	0	0	0
(11)	ディスクアレイ装置(B)	3	1	0	0	1	0	2	1	1
(12)	政府共用証明書検証サーバ(A)	9	9	4	1	4	0	0	0	0
(13)	政府共用証明書検証サーバ(B)	3	3	1	1	1	0	0	0	0
(14)	申請管理 DB サーバ	8	3	0	0	3	0	5	3	2

（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	ブリッジ CA システム				政府共用 CA システム		
			計	MC	BC	TC	JM	計	MC	BC
(15)	申請管理サーバ	5	2	0	0	2	0	3	2	1
(16)	申請受付サーバ	5	2	0	0	2	0	3	2	1
(17)	DNS サーバ	4	4	2	1	1	0	0	0	0
(18)	FTP サーバ	3	1	0	0	1	0	2	0	2
(19)	ログ収集サーバ	2	2	2	0	0	0	0	0	0
(20)	ファイアウォール管理サーバ	4	4	2	1	1	0	0	0	0
(21)	可読性チェックサーバ	2	2	1	1	0	0	0	0	0
(22)	監視サーバ	6	6	2	2	2	0	0	0	0
(23)	ファイルサーバ	1	1	0	0	0	1	0	0	0
2. 端末										
(1)	CA 操作端末（BCA）	5	5	2	1	2	0	0	0	0
(2)	CA 操作端末（政府共用 CA）	5	2	0	0	2	0	3	2	1
(3)	CA 操作端末(民間/府省兼汎用) AP テスト用	2	2	0	0	2	0	0	0	0
(4)	運用操作員登録端末	3	3	2	1	0	0	0	0	0
(5)	証明書検証サーバ操作端末	4	4	2	1	1	0	0	0	0
(6)	証明書検証サーバ監視端末	4	4	2	1	1	0	0	0	0
(7)	FTP 端末	5	1	0	0	1	0	4	4	0
(8)	SSH 端末	4	4	2	1	1	0	0	0	0
(9)	監視端末	3	3	2	0	1	0	0	0	0
(10)	アラート解析レスポンス測定端末	1	1	1	0	0	0	0	0	0
(11)	ファイアウォール設定端末	9	9	6	3	0	0	0	0	0
(12)	ﾌｧｲｱｳｫｰﾙ操作端末兼ﾈｯﾄﾜｰｸﾍﾞｰｽ IDS 監視端末	4	4	2	1	1	0	0	0	0
(13)	エンドエンティティ端末(A)	2	2	0	0	2	0	0	0	0
(14)	エンドエンティティ端末(B)	1	1	0	0	1	0	0	0	0
(15)	エンドエンティティ端末(C)	1	1	0	0	1	0	0	0	0
(16)	運用員用端末	23	23	0	0	0	23	0	0	0
3. IC カード関連機器										
(1)	IC カード発行機	4	1	0	0	1	0	3	2	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	ブリッジ CA システム					政府共用 CA システム		
			計	MC	BC	TC	JM	計	MC	BC
(2)	IC カード関連ソフト開発機	1	1	0	0	1	0	0	0	0
(3)	GPKI-AP 製造番号生成端末	1	1	0	0	1	0	0	0	0
4. ネットワーク機器										
(1)	L2 スイッチ(A)	21	14	6	5	3	0	7	6	1
(2)	L2 スイッチ(B)	8	7	6	0	1	0	1	0	1
(3)	L2 スイッチ(C)	5	5	3	1	1	0	0	0	0
(4)	L2 スイッチ(D)	6	3	3	0	0	0	3	2	1
(5)	事務室 L2 スイッチ	1	1	0	0	0	1	0	0	0
(6)	L3 スイッチ（A）	6	6	3	2	1	0	0	0	0
(7)	L3 スイッチ（B）	2	2	0	2	0	0	0	0	0
(8)	事務室 L3 スイッチ	1	1	0	0	0	1	0	0	0
(9)	センタ間接続ルータ	4	4	2	2	0	0	0	0	0
(10)	VPN 装置	16	10	2	2	2	0	6	4	2
(11)	負荷分散装置(A)	5	5	2	2	1	0	0	0	0
(12)	負荷分散装置(B)	4	4	2	2	0	0	0	0	0
(13)	ファイアウォール(A)	4	4	2	2	0	0	0	0	0
(14)	ファイアウォール(B)	11	11	6	3	2	0	0	0	0
(15)	ファイアウォール(C)	6	6	4	2	0	0	0	0	0
(16)	ファイアウォール（事務システム）	1	1	0	0	0	1	0	0	0
(17)	ネットワークベース IDS(A)	2	2	2	0	0	0	0	0	0
(18)	ネットワークベース IDS(B)	2	2	0	1	1	0	0	0	0
(19)	事務システム回線等	1	1	0	0	0	1	0	0	0
5. その他										
(1)	ネットワーク型ディスク装置	2	2	0	0	0	2	0	0	0
(2)	ディスククラッシャ	2	2	1	1	0	0	0	0	0
(3)	シュレッダ	1	1	0	0	0	1	0	0	0
(4)	マルチシュレッダ	2	2	1	1	0	0	0	0	0
(5)	CD/DVD データ書込みレーベル印刷機	1	1	0	0	1	0	0	0	0
(6)	プリンタ	11	6	5	0	1	0	5	2	3
(7)	カラープリンタ・コピー・FAX 複合機	1	1	0	0	0	1	0	0	0

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（アプリケーションCA編）
- 構築仕様書（アプリケーションCA2編）
- 構築仕様書（ネットワーク編）
- 暗号移行検証環境　構築仕様書

（2）性能

「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}
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}
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}
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 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}
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}
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}
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 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}
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 障害復旧時間(H)＝（障害復旧日時-障害確認日時）
11		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。（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}
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}
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}
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 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}
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 障害復旧時間(H)＝(障害復旧日時－障害確認日時)
11		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。 （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。 （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｝ 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 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。 （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、官職認証局及びアプリケーション認証局それぞれの 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。

- 統合リポジトリ及び 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
アプリケーション認証局 CP/CPS　http://www.gpki.go.jp/apca/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、別途閲覧に供する以下の資料を参照。

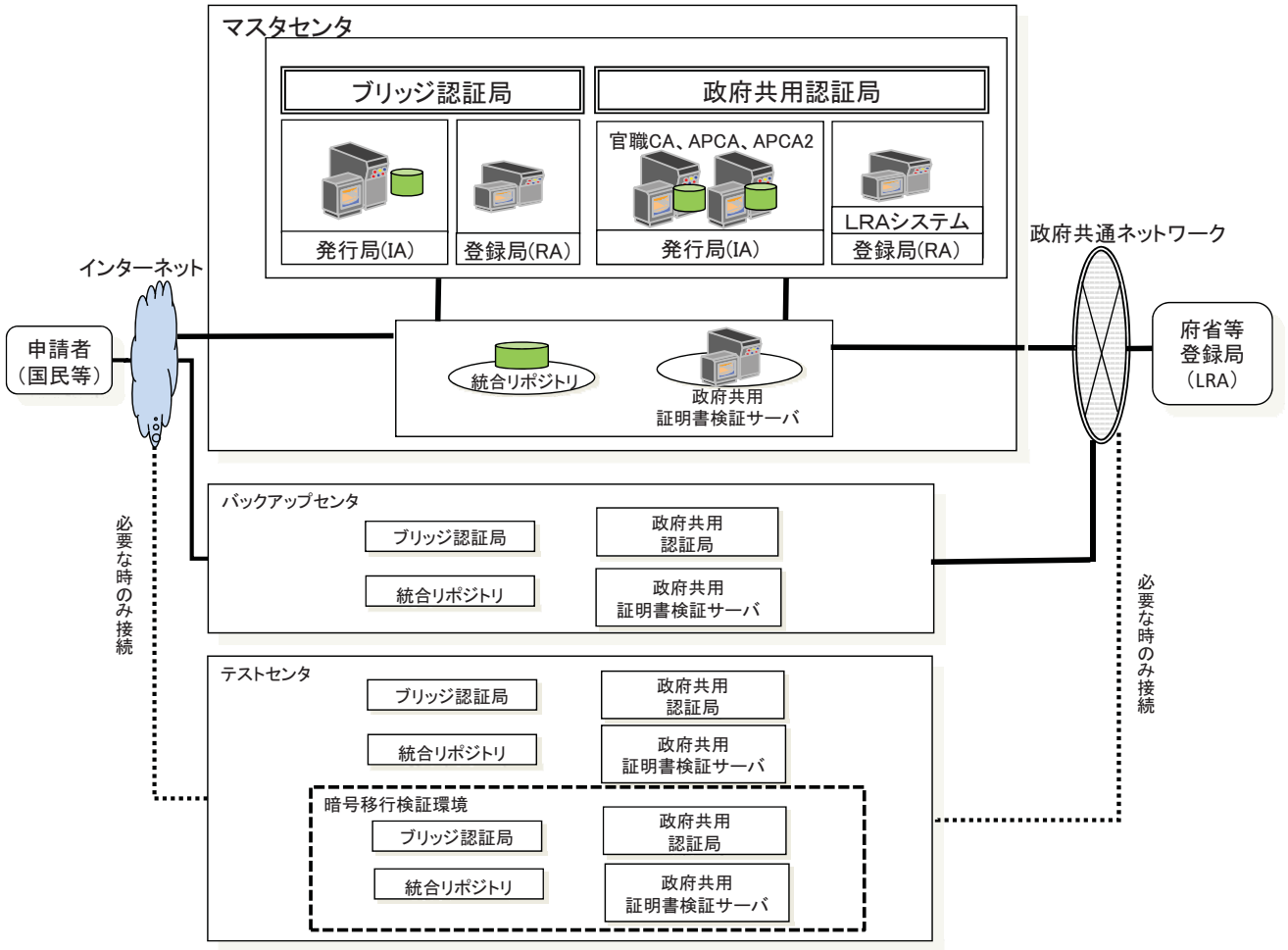
- 構築仕様書（セキュリティ編）

特に、政府共用認証局のセキュリティ対策については、別添資料2「政府共用認証　セキュリティ要件」を遵守すること。

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（アプリケーションCA編）
- 構築仕様書（アプリケーションCA2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
- 暗号移行検証環境　構築仕様書

8 運用要件

（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、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取得を実施する。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

現行の施設・設備又は請負業者の提案する施設・設備で運用すること。

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（東京都内）及びバックアップセンタ（東京近郊）の2カ所があり、これらを使用する場合、施設使用料及び通信回線使用料（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・プロバイダ契約費。政府共通ネットワークの接続料は除く）は、請負業者の負担（月額 15,800,000 円（税抜））とする。

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×2）：187,500 円

上記に含まれない次の設備等については、請負業者が準備すること。

空調装置9式、監視カメラ 20 台、IC カード認証装置 15 台、指紋認証装置7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　請負業者の提案する施設・設備

以下の条件を満たすことを前提に請負業者の提案する施設・設備での運用を可とする。

ただし、機器等の移設・据付・調整・システム設定・テスト等は請負業者の責任と負担において対応すること。

- 提案施設・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。
- 機器等の移設に伴う本システムのサービス停止時間は、24時間（日曜日の0時から24時まで）内とし、回数は4回を限度とする。

9 保守要件

対象となるシステムは、ブリッジ認証局システム及び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）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 運用要員の一覧に示す。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 運用要員の一覧

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	4名以上
一般IA操作員	2名以上
監視員	8名以上
計	19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。

（2）導入

ア　作業実施場所

現行の施設・設備を利用する場合、作業実施場所は、マスタセンタ（東京都内）及びバックアップセンタ（東京近郊）の2カ所となるが、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、平成 25 年3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、平成 29 年3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3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、「5　信頼性等要件　（1）信頼性要件」の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。

・ 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、実施手順書及び別添資料4「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　AP認証局の自己署名証明書（ルート証明書）自動配付にあたりマイクロソフト社との合意書において、運用業務の範囲に該当する事項を遵守すること。
詳細は、別途閲覧に供する以下の資料を参照。

・MICROSOFT WINDOWS CERTIFICATION AUTHORITY AGREEMENT

イ　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。

ウ　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。

12 妥当性証明

確認者：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
澤田　稔一

≪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

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、PowerPoint 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。

エ　移設計画書

　現行の施設・設備を利用せず請負業者が提案する施設・設備を利用する場合には、システム移設に係る具体的な方法、スケジュール等を記述すること。

オ　暗号移行計画書

　暗号移行の作業（相互認証の更新、CA 鍵更新、証明書切替等）に係る具体的な体制、スケジュール、方法等を記述すること。

２．提案書の内容説明

　提案書提出後、主管係指定する日時等において、その内容について説明を行うこと。

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（アプリケーション CA 編）
エ　構築仕様書（アプリケーション CA２編）
オ　構築仕様書（ネットワーク編）
カ　構築仕様書（セキュリティ編）
キ　LRA システム基本設計書
ク　IC カードシステム仕様書
ケ　暗号移行検証環境　構築仕様書
コ　政府認証基盤 業務管理マニュアル
サ　政府認証基盤 システム運用マニュアル
シ　現行の施設・設備の詳細
ス　消耗品一覧
セ　総務省情報セキュリティポリシー
ソ　MICROSOFT WINDOWS CERTIFICATION AUTHORITY AGREEMENT

(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

平成　　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、下記の事項を遵守することを誓約します。

記

1. 総務省の情報セキュリティに関する規定等を遵守し、総務省が開示した情報（公知の情報等を除く）を本件調達の目的以外に使用、又は第三者に開示、若しくは漏洩しないものとし、そのために必要な措置を講ずることを約束する。

2. 上記 1.に違反して、情報の開示、漏えい若しくは使用した場合、法的な責任を負うものであることを確認し、これにより総務省が被った一切の損害を賠償することを約束する。

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（2,800 点満点）＋価格点（2,800 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。（2,800 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（2,800 点満点）＝加点（2,800 点満点）

③ 価格点は、入札価格が予定価格の制限の範囲内であることを条件とし、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）×2,800 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（案）

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 ・納品成果物 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。	最重要	400
	(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 B 政府共用認証局に係る認証業務 C 照会対応 D ホームページ作成及び更新 E 外部監査対応 F 監査ログ検査 G アーカイブ取得 H アーカイブ可読性確認 I 規程類に関する準拠性監査 J LRA研修 K 教育・訓練 L テスト環境の維持 M 書類改定（上位規程、業務規程、業務管理マニュアル）	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が提案されていること。	重要	200
	(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 B 監視業務 C 定常業務 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が提案されていること。	重要	200
	(エ) 政府認証基盤の暗号移行対応 ・暗号移行に係る相互認証審査支援 ・暗号移行に係る鍵更新（ブリッジ認証局、官職認証局） ・暗号移行に係る相互認証取り交し ・暗号移行に係る証明書の一斉切替（官職認証局） ・暗号移行に係るアプリケーション認証局2の自己署名証明書の発行 ・暗号移行に係るアプリケーション認証局の廃止	暗号移行計画書において、暗号移行に係る各作業の具体的な体制、スケジュール、方法等が記載されてること。		加4	暗号移行作業に関する事前準備、相互認証先認証局との調整、各府省への支援、リスク管理等を考慮し、暗号移行を確実に行える提案がされていること。	最重要	400
	(オ) 政府認証基盤システムの保守業務 ・システム保守管理 ・システム障害保守 ・システム予防保守 ・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5	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が提案されていること。	重要	200
	(カ) 認証局施設・設備の管理業務 ・施設・室に関する管理 ・設備、備品等に関する管理	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。					
	(キ) 報告書の作成 ・月次報告書の作成 ・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。					
(5)作業内容 ・納品成果物 イ 作業実施期間 ～ オ 納入成果物	イ 作業実施期間 平成25年3月1日（金）から平成29年2月28日（火）まで。 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。	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。					
	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。	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 次の文書の書面及び電子データ（CD-R）（各一式）を納入する。 ・実施計画書 （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） ・運用状況報告書 （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） ・障害発生対応状況報告書 （障害・案件一覧、個別障害対応報告書 等） ・予防保守等に係る調査報告書 ・保守作業計画書 ・保守作業報告書 ・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。					
3. 情報システムの要件							
	－	－	－				
4. 規模・性能要件							
	－	－	－				
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。	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	運用・保守の観点から、サービスレベル遵守及び事業継続性のための具体的な施策が提案されていること。	最重要	400
(2)事業継続性要件	政府認証基盤は、ブリッジ認証局、官職認証局及びアプリケーション認証局それぞれのCP/CPSに災害時の事業継続性要件を定めている。 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。 ・ 統合リポジトリ及び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						

別紙

総合評価対応表（案）

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。 ・ 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。					
(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、別途閲覧に供する以下の資料を参照。 ・ 構築仕様書（セキュリティ編） 特に、政府共用認証局のセキュリティ対策については、別添資料2「政府共用認証 セキュリティ要件」を遵守すること。 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。 ・ 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。	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、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取得を実施する。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	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	現行の施設・設備又は請負業者の提案する施設・設備で運用すること。 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（東京都内）及びバックアップセンタ（東京近郊）の2カ所があり、これらを使用する場合、施設使用料及び通信回線使用料（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・プロバイダ契約費。政府共通ネットワークの接続料は除く）は、請負業者の負担（月額16,590,000円（消費税を含む））とする。 上記に含まれない次の設備等については、請負業者が準備すること。 空調装置9式、監視カメラ20台、ICカード認証装置15台、指紋認証装置7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 請負業者の提案する施設・設備 以下の条件を満たすことを前提に請負業者の提案する施設・設備での運用を可とする。 ただし、機器等の移設・据付・調整・システム設定・テスト等は請負業者の責任と負担において対応すること。 ・ 提案施設・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。 ・ 機器等の移設に伴う本システムのサービス停止時間は、24時間（日曜日の0時から24時まで）内とし、回数は4回を限度とする。	現行の施設・設備以外を利用する場合は、移設計画書において、左記要件を満たしたシステム移設に係る具体的な方法、スケジュール等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及び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）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。	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。					
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以下に示す。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。 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 4名以上 一般IA操作員 2名以上 監視員 8名以上 計 19名以上	作業体制図において、必要な運用要員数が確保されていること。		加7	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 (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	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 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。	－	－	加8	左記に示すスキルを有する要員を配置していること。	重要	200
	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。	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 (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	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 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。	－	－	加10	左記に示すスキルを有する要員を配置していること。	重要	200

別紙

総合評価対応表（案）

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
	(2)導入	ア 作業実施場所 現行の施設・設備を利用する場合、作業実施場所は、マスタセンタ（東京都内）及びバックアップセンタ（東京近郊）の2カ所となるが、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 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、平成25年3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、平成29年3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 ・ 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3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、「5 信頼性等要件 （1）信頼性要件」の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。 ・ 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。	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。					
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、実施手順書及び別添資料4「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。	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。 ・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）	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。 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。	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 AP認証局の自己署名証明書（ルート証明書）自動配付にあたりマイクロソフト社との合意書において、運用業務の範囲に該当する事項を遵守すること。 詳細は、別途閲覧に供する以下の資料を参照。 ・MICROSOFT WINDOWS CERTIFICATION AUTORITY AGREEMENT イ 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。 ウ 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。	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。					