資料２－２

事前旅客情報システム
及び
外国人個人識別情報認証システム

民間競争入札実施要項（案）

警察庁情報通信局情報管理課

目次

事前旅客情報システム及び外国人個人識別情報認証システム　民間競争入札実施要項（案）

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、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、警察庁は、公共サービス改革基本方針（平成 26 年７月 11 日閣議決定）別表において民間競争入札の対象として選定された事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム開発及び保守業務（以下「対象業務」という。）について、公共サービス改革基本方針に従って、民間競争入札実施要項を定めるものとする。

２　対象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業務の質に関する事項

(1) 業務の経緯等

事前旅客情報照合業務及び外国人個人識別情報認証業務は、テロリスト及び不法入国者の上陸阻止、輸入禁制品等の密輸阻止及び指名手配者の逮捕等水際における取締りの徹底を図ることを目的とする業務である。

現在運用している業務システムのハードウェアが平成 30 年度に運用期限を迎えることに伴い、平成 31 年３月に新たな業務システムに更改するため、平成 29 年度及び 30 年度に対象となる「プログラム開発」、「プログラム保守」、「システム構築等」及び「システム賃貸借」を含めた調達を行うこととしている。

(2) 事前旅客情報システム及び外国人個人識別情報認証システムの概要

ア　事前旅客情報システム

事前旅客情報システムは、航空会社から提供される国際線の搭乗者氏名等の旅客情報と関係省庁が保有する要注意者情報を照合し、我が国の安全対策上問題がある旅客等の情報を関係部署に通報するシステムである。

イ　外国人個人識別情報認証システム

外国人個人識別情報認証システムは、入国審査時に提供される外国人の個人識別情報と関係省庁が保有する要注意者の個人識別情報を照合し、我が国の安全対策上問題がある旅客等の情報を関係部署に通報するシステムである。

(3) 対象業務の詳細な内容

対象業務を実施する民間事業者（以下「請負者」という。）が行う業務の内容は「プログラム開発」、「プログラム保守」、「システム構築等」及び「システム賃貸借」であり、それぞれ別添１「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書」、別添２「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム保守仕様書」、別添３「事前旅客情報システム及び外国人個人識別情報認証システム構築等仕様書」及び別添４「事前旅客情報システム及び外国人個人識別

情報認証システム仕様書」に記されているとおりである。

(4) 対象業務の引継ぎ

ア　請負者への引継ぎ

警察庁は、当該引継ぎが円滑に実施されるよう、請負者に対して必要な措置を講ずる。

請負者は、対象業務の開始日までに業務内容を明らかにした書類等により、警察庁から業務の引継ぎを受けるものとする。

イ　請負期間満了時の引継ぎ

警察庁は、当該引継ぎが円滑に実施されるよう、請負者及び次回請負者に対して必要な措置を講ずるとともに、引継ぎが完了したことを確認する。

対象業務の請負期間満了時には、請負者は、次回業務の開始日までに、業務内容を明らかにした書類等により、警察庁を介して、次回請負者に対し、引継ぎを行うものとする。なお、引継ぎに必要となる経費は、請負者の負担となる。

(5) 確保されるべき対象業務の質

ア　対象業務の適切な実施

２(3)の内容をスケジュールを遵守して適切に実施すること。

イ　障害復旧目標時間

警察庁及び情報通信部からシステム（業務）の完全停止を伴う障害の連絡があった場合は、次の時間内を目標に障害を復旧させること。目標時間を超過した場合には、目標時間内の復旧に至らなかった原因を特定し、今後の改善策について資料を提出すること。

- 警察庁（警察庁サーバ、端末等）及び警察本部（端末等）：８時間以内
- 警察署（端末等）：翌官庁執務時間内

ウ　技術者駆けつけ時間

警察庁及び情報通信部から技術者の派遣要請があった場合は、次の時間内に技術者を派遣すること。

- 警察庁（警察庁サーバ、端末等）及び警察本部（端末等）：３時間以内
- 警察署（端末等）：翌官庁執務時間内

エ　障害報告に要する時間

警察庁から連絡を受けた障害について、障害原因や最終対処方法を期限内に書面で報告すること。期限内に報告できない場合は、別途報告日を提示するとともに、必要に応じて中間報告を行うこと。

オ　回答に要する時間

警察庁からの技術的な問い合わせに対し、期限内に回答すること。期限内に回答できない場合は別途回答日を提示するとともに、必要に応じて中間回答を行うこと。

カ　サービスレベルアグリーメント（Service Level Agreement）の締結

対象業務の効率化、品質向上及び円滑化を図るため、上記エ・オに示す期限については、別途サービスレベルアグリーメント（ＳＬＡ）を締結する。

(6) 創意工夫の発揮可能性

対象業務を実施するに当たっては、別添５「総合評価基準」に従い、対象業務の実

施全般に係る質の向上の観点から取り組むべき事項等の提案を行うとともに、改善すべき提案（経費削減に係る提案を含む）の具体的な方法等を示すなどし、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。

(7) 契約の形態及び支払

ア　プログラム開発（別添１）

(ｱ) 契約形態

請負契約

(ｲ) 支払

警察庁は、納入検査に合格し、その引き渡しが行われた後、請負者の適法な支払請求書を受理した日から、30 日以内にその対価を請負者に支払うものとする。

また、警察庁は、納入期限が分割されている場合、特約をすることによって部分払いをすることができる。納入検査の結果、不合格のものについては、警察庁の指示に従い、遅滞なく訂正し、再度検査を受けなければならない。

さらに、警察庁は、自己の都合により、成果物が納入されるまでの間、この契約の一部を解除する場合、既に受領済の成果物があり、これが未納成果物と分離して契約の目的の一部を達するものである時は、その対価を請負者に支払うものとする。

イ　プログラム保守（別添２）

(ｱ) 契約形態

請負契約

(ｲ) 支払

警察庁は、別添２に基づく保守の提供を受けた月から月額で料金を支払うものとする。

警察庁は、この契約による保守期間の当該月を経過した後において請負者の契約履行を確認し、適法な支払請求書を受理した日から 30 日以内に当該料金を請負者に支払うものとする。確認の結果、確保されるべき質が達成されていないと認められる場合、警察庁は、確保されるべき質の達成に必要な限りで、請負者に対して対象業務の実施方法の改善を行うよう指示するものとし、請負者は、当該指示を受けて対象業務の実施方法を改善し、業務改善報告書を速やかに警察庁に提出するものとする。業務改善報告書の提出から 30 日の範囲で、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、警察庁は、支払を行わないことができる。なお、請負費は、対象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。

ウ　システム構築等（別添３）

(ｱ) 契約形態

請負契約

(ｲ) 支払

警察庁は、検査に合格し、その引き渡しが行われた後、請負者の適法な支払請

求書を受理した日から、30 日以内にその対価を請負者に支払うものとする。

また、警察庁は、納入期限が分割されている場合、特約をすることによって部分払いをすることができる。納入検査の結果、不合格のものについては、警察庁の指示に従い、遅滞なく訂正し、再度検査を受けなければならない。

さらに、警察庁は、自己の都合によりこの契約の全部又は一部を解除する場合、既に受領済の成果物があり、これが未納成果物と分離して契約の目的の一部を達するものである時は、その対価を請負者に支払うものとする。

エ　システム賃貸借（別添４）

(ｱ) 契約形態

賃貸借契約

(ｲ) 支払

警察庁は、別添４に基づく機器の使用を開始した月から月額で料金を支払うものとする。

警察庁は、この契約による賃貸借期間の当該月を経過した後において請負者の契約履行を確認し、適法な支払請求書を受理した日から 30 日以内に当該料金を請負者に支払うものとする。確認の結果、確保されるべき質が達成されていないと認められる場合、警察庁は、確保されるべき質の達成に必要な限りで、請負者に対して対象業務の実施方法の改善を行うよう指示するものとし、請負者は、当該指示を受けて対象業務の実施方法を改善し、業務改善報告書を速やかに警察庁に提出するものとする。業務改善報告書の提出から 30 日の範囲で、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、警察庁は、支払を行わないことができる。なお、請負費は、対象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。

(8) 法令変更による増加費及び損害の負担

事業の構成要素が法令等により設定、改定若しくは廃止され、又は契約内容を変更した場合、警察庁と請負者が協議の上、契約金額を変更することができる。

３　実施期間に関する事項

(1) プログラム導入期限

試験環境：平成 30 年９月 28 日まで

運用環境：平成 31 年２月 28 日まで

(2) システム設置期限

平成 31 年２月 28 日までに全ての機器設置を完了すること。

(3) 試験期間

ア　結合テスト（単独試験）：警察庁設置機器のみを用いた試験

平成 30 年 10 月から平成 30 年 11 月までの間

イ　結合テスト（連携試験）：警察システムと外部システムとの間の試験

平成 30 年 10 月から平成 31 年２月までの間

ウ　総合テスト：警察庁設置機器及び都道府県設置の専用端末等を用いた試験

平成 30 年 12 月から平成 31 年１月までの間

(4) 運用開始日

平成 31 年３月１日

(5) システム賃貸借・プログラム保守

平成 31 年３月１日から平成 34 年３月 31 日までの間

4　入札参加資格に関する事項

(1) 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。

(2) 予算決算及び会計令第 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ものは、同条中、特別な理由がある場合に該当する。

(3) 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。

(4) 開札時までに平成 28・29・30 年度内閣府競争参加資格（全省庁統一資格）「物品の製造」又は「物品の販売」及び「役務の提供等」のＡ、Ｂ又はＣの等級に格付けされている者であること。

(5) 法人税並びに消費税及び地方消費税の滞納がないこと。

(6) 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。

(7) 警察庁から「警察庁における物品調達及び工事請負契約等に係る指名停止措置要領」に基づく指名停止の措置を受けている期間中の者でないこと。

(8) 警察当局から、暴力団又は暴力団員が実質的に経営を支配する事業者又はこれに準ずる者として、国発注業務等からの排除要請があり、当該状態が継続している者でないこと。

(9) 単独で対象業務を行うことができない場合、又は単独で実施するより業務上の優位性があると判断する場合は、適正に対象業務を実施できる入札参加グループを結成し、入札に参加することができる。その場合、入札書類提出時までに入札参加グループを結成し、上記(1)～(8)までの入札参加資格の全てを満たす者の中から代表者を定め、他の者は構成員として参加するものとする。

なお、入札参加グループの構成員は、上記(1)～(3)まで及び(5)～(8)までの資格を満たす必要があり、他の入札参加グループの構成員となり、又は単独で参加することはできない。

また、入札参加グループの代表者及び構成員は、入札参加グループ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。

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）

ア　入札公告：官報公告	平成 29 年３月中旬頃
イ　入札説明会	平成 29 年３月下旬頃
ウ　質問受付期限	平成 29 年５月上旬頃
エ　入札書及び企画書提出期限	平成 29 年５月中旬頃

オ　企画書の評価　　平成 29 年５月下旬頃
カ　開札及び落札予定者の決定　　平成 29 年６月上旬頃
キ　契約の締結　　平成 29 年６月下旬頃

(2) 入札書類

民間競争入札に参加する者（以下「入札参加者」という。）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　入札説明書等に関する質問書

入札公告以降、入札説明書の交付を受けた者は、本実施要項の内容や入札に係る事項について、入札説明会後に、警察庁に対して質問を行うことができる。質問は原則として電子メールにより行い、質問内容及び警察庁からの回答は原則として入札説明書の交付を受けたすべての者に公開することとする。ただし、民間事業者の権利や競争上の地位等を害するおそれがあると判断される場合には、質問者の意向を聴取した上で公開しないよう配慮する。

イ　対象業務に係る入札金額を記載した書類

入札参加者は、調達物品の価格のほか、輸送費、保守料等に係る一切に諸経費を含め契約金額を見積もるものとする。

落札決定に当たっては、入札金額の８パーセントに相当する額を加算した金額（当該金額の１円未満の端数がある時は、その端数金額を切り捨てた金額とする。）をもって落札価格とするので、入札者は、消費税に係る課税事業者であるか免税事業者であるかを問わず、見積もった契約金額の 108 分の 100 に相当する金額としなければならない。

ウ　総合評価のための性能、機能、技術等（以下「性能等」という。）に関する書類（以下「企画書」という。）

なお、様式は「総合評価基準」（別添５）の書式に基づき作成する。

エ　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、第４号及び第６号から第９号までの暴力団排除に関する規定（以下「暴力団排除条項」という。）について評価するために必要な書類

オ　平成２８・２９・３０年度内閣府競争参加資格（全省庁統一資格）における資格審査結果通知書の写し

カ　納税証明書

キ　その他入札説明書に記載されている書類

６　請負者を決定するための評価の基準その他の請負者の決定に関する事項

(1) 評価項目等の設定

請負者の決定は、総合評価落札方式によるものとし、提出された企画書の内容が対象業務の目的に合致しており実行可能であるか（技術点の必須項目）、創意工夫が図られ効果的なものであるか（技術点の加点項目）について、警察庁が設ける総合評価委員会において審査を行うとともに、警察庁ＣＩＯ補佐官の決裁を得るものとする。

ア　技術点の必須項目

必須項目は、別添１「事前旅客情報照合業務及び外国人個人識別情報認証業務用

プログラム仕様書」及び別添４「事前旅客情報システム及び外国人個人識別情報認証システム仕様書」に示した要求要件について審査する。

イ　技術点の加点項目

加点項目は、別添５に示す機能及び性能別に警察庁が必要度及び重要度に照らし合わせて設定した要求要件について審査する。

(2) 評価方法（得点の付与方式）

ア　総合評価点

総合評価は、入札者の価格点と当該入札者の申込みに係る技術点の合計をもって行う。

価格点の配分：技術点の配分　＝　１：１

総合評価点　＝　価格点（10,000 点満点）　＋　技術点（10,000 点満点）

イ　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。得点配分の詳細は別添５のとおり。

ウ　技術点

技術点は、基礎点及び加点の得点を合計した値とする。得点配分の詳細は別添５のとおり。

(ｱ) 基礎点（必須項目）

(1)アに示した項目について、要求要件を満たしている場合は合格とし基礎点（8,427 点）を与え、１つでも満たさない場合は不合格とする。

(ｲ) 加点（加点項目）

(1)イに示したものについては、入札者が総合評価基準により行った加点項目に係る提案に対し、加点基準に基づき加点する。加点基準を満たす場合は別添５に記載している配点を与え、満たさない場合は０点とする。

エ　落札者の決定方法

別添１及び別添４の各仕様書に示した全ての要求要件を満たし、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、総合評価点の最も高い者を落札者とする。

ただし、落札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おそれがあって著しく不適当であると認められるときは、予定価格の制限の範囲内の価格をもって申込みがあった他の者のうち、上記の評価点の最も高い者をもって落札者とすることがある。

なお、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、入札者又はその代理人が直接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。

(3) 落札者の決定等の公表

警察庁は、落札者を決定した時は、遅滞なく落札者の氏名又は名称、落札金額、落札者の決定理由及び落札金額を公表する。

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。

(4) 落札者が決定しなかった場合の措置

ア　落札者が決定しなかった場合には、初回の入札において必須項目を全て満たしている者のうち、予定価格の制限に達した入札がない場合には、直ちに再度の入札を行うものとする。これによって落札者となるべき者が決定しない場合は、予算決算及び会計令第 99 条の２の規程に基づき契約を締結することを検討する。

イ　初回の入札において入札参加者がいなかった場合、必須項目を全て満たす入札参加者がいなかった場合、又はアによっても、なお、請負者が決定しなかった場合には、総合評価基準等の入札条件の見直しを行い、再度の公告と入札を行うものとする。

ウ　落札者となるべき者が決定しない場合は、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。

7　対象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

警察庁は、対象業務に関して、以下の情報について別添６「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的の達成の程度

オ　従来の実施方法等

(2) 資料の閲覧

警察庁は、民間競争入札に参加する予定の者から(1)オの「従来の実施方法等」の詳細な情報に関する資料の開示について要望があった場合には、法令、警察庁の規定、機密性等に問題のない範囲で適切に対応するよう努めるものとする。

8　対象業務の請負業者に使用させることができる財産に関する事項

(1) 国有財産の使用

請負者は、対象業務の遂行に必要な施設、設備等として、次に掲げる施設、設備等を適切な管理の下、無償で使用することができる。

ア　対象業務に必要となる電気設備

イ　警察庁と協議し、承認された業務に必要な施設、設備等

(2) 使用制限

ア　請負者は、対象業務の実施及び実施に付随する業務以外の目的で使用し、又は利用してはならない。

イ　請負者は、あらかじめ警察庁と協議した上で、警察庁の業務に支障を来さない範囲内において、施設内に対象業務の実施に必要な設備等を持ち込むことができる。

ウ　請負者は、設備等を設置した場合は、設備等の使用を終了又は中止した後、直ち

に、必要な原状回復を行う。

エ　請負者は、既存の建築物、工作物等に汚損・損傷等を与えないよう十分に注意し、損傷（機器の故障等を含む。）が生じるおそれのある場合は、養生を行う。

万一損傷が生じた場合は、請負者の責任と負担において速やかに復旧するものとする。

9　請負者が、対象業務を実施するに当たり、警察庁長官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業務の適正かつ確実な実施の確保のために請負者が講じるべき措置に関する事項

(1) 報告

ア　請負者は、別添１「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書」、別添２「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム保守仕様書」、別添３「事前旅客情報システム及び外国人個人識別情報認証システム構築等仕様書」及び別添４「事前旅客情報システム及び外国人個人識別情報認証システム仕様書」において報告することとされている事項について、警察庁に報告しなければならない。

イ　警察庁は、請負者による対象業務の適正かつ確実な実施を確保するため必要があると認めるときは、当該請負者に対し、必要な措置をとるべきことを指示し、措置結果について報告を求めることができる。

ウ　上記ア及びイにおける請負者の実施に関して、虚偽の報告をした者、警察庁からの指示に違反した者などについては、法第 55 条及び法第 56 条の罰則が適用される。

(2) 秘密を適正に取り扱うための措置

ア　請負者は、業務に関して知り得た警察庁、都道府県警察及び事前旅客情報システム又は外国人個人識別情報認証システムに関係する省庁の情報について適切な管理をしなければならない。

イ　請負者は対象業務の実施に関して知り得た秘密を漏らし、又は盗用してはならない。対象業務に従事する者（従事していた者を含む。以下同じ。）が秘密を漏らし、又は盗用した場合は、法第 54 条の罰則が適用される。

ウ　対象業務に従事する者は、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す。

エ　請負者は、警察庁の情報セキュリティ規程に基づく情報セキュリティ要求要件を遵守しなければならない。

オ　アからエまでのほか、警察庁は、請負者に対し、対象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取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じるべき措置

ア　知的財産権の取扱い

(ｱ) 対象業務において納入された成果物に関する権利（著作権法（昭和 45 年法律第 48 号）第 21 条から第 28 条に定める全ての権利を含む。）及び所有権は、次の物を除き警察庁が請負者に受領書を交付したときをもって警察庁に移転する。また、

請負者は警察庁に対し、納入成果物に係る著作者人格権（著作権法第 18 条から第 20 条に定める権利をいう。）を行使しないものとする。

a　納入成果物に、請負者が対象業務の契約前から権利を有する著作物（請負者が範囲について警察庁の承認を得たものに限る。）（以下「請負者の既存著作物」という。）が含まれる場合、その請負者の既存著作物

b　納入成果物に、第三者が権利を有する著作物（以下「第三者の既存著作物」という。）が含まれる場合、その第三者の既存著作物

(ｲ) 上記(ｱ) a で示した請負者の既存著作物においては、本システムへ利用する目的の範囲に限り、警察庁は請負者に権利留保された著作物を自由に複製し、改変等し、及びそれらの利用を第三者に許諾することができるものとする。ただし、成果物に第三者の権利が帰属するときはこの限りではないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

(ｳ) 納入成果物に第三者の既存著作物が含まれている場合は、請負者は当該既存著作物の使用に必要な費用の負担及び使用許諾に関する一切の手続を行うものとする。この場合、請負者は使用許諾の内容については、警察庁の承認を得るものとする。

イ　権利義務の帰属等

(ｱ) 対象業務の実施が第三者の特許権、著作権その他の権利と抵触するときは、請負者は、その責任において、必要な措置を講じなくてはならない。

(ｲ) 請負者は、対象業務の実施状況を公表しようとするときは、あらかじめ、警察庁の承認を受けなければならない。

ウ　瑕疵担保責任

警察庁は、納入成果物について納入後１か年以内に瑕疵を発見した場合は、請負者に対して当該瑕疵の修正を請求することができ、請負者は、当該瑕疵を無償で修正するものとする。

エ　再委託

(ｱ) 請負者は、警察庁から委託を受けた対象業務の実施に係る業務を一括して第三者に委託し又は請け負わせてはならない。

(ｲ) 請負者は、対象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５(2)ウの企画書において、再委託する事業の範囲、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その他対象業務の実施方法について記載しなければならない。

(ｳ) 請負者は、委託契約後やむを得ない事情により再委託を行う場合には、委託先・委託金額を明らかにした上で警察庁の承認を得ること。

(ｴ) 請負者は、上記(ｲ)及び(ｳ)により再委託を行う場合は、再委託先に上記(2)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共に、再委託先から必要な報告を徴収すること。

(ｵ) 請負者が再委託先の事業者に業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見なして、請負者が責任を負うものとする。

オ　契約の変更及び解除

(ｱ) 契約の変更

警察庁及び請負者は、対象業務の質の向上、又はその他やむを得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た上で、法第 21 条の手続きを経なければならない。

(ｲ) 契約の解除

警察庁は、請負者が次の各号に該当するときは、当該請負者に対し、委託費の支払いを停止し、又は契約を解除することができる。

なお、上記理由により警察庁が契約を解除したときは、請負者は、違約金として契約金額の 100 分の 10 に相当する金額（対象業務の実施分を除く。）を警察庁に納付するとともに、警察庁との協議に基づき、引継ぎの処理が完了するまでの間、責任をもって当該業務の処理を行わなければならない。

上記違約金の定めは、違約金額を超過する損害額についての損害賠償を妨げるものではない。

a　法第 22 条第１項イからチまで又は同項第２号に該当するとき。

b　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とき。

c　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とき。

d　再委託先等が暴力団又は暴力団関係者と知りながら契約し、又は再委託先等との契約を承認したとき。

e　再委託先等が暴力団若しくは暴力団員が実質的に経営を支配する事業者又はこれに準ずる者に該当することが判明したにも関わらず、直ちに当該再委託先等との契約を解除しないとき、又は再委託先等に対し契約を解除させるための措置を講じないとき。

f　次の各号に該当するとき。

①　仮差押、仮処分、強制執行若しくは競売の申立を受け、手形交換所の取引停止処分若しくは租税公課の滞納処分があり、又はこれらの申立若しくは処分を受けるべき事由を生じた場合。

②　手形、小切手の不渡りを生じ、支払停止の状態に陥り、又は破産、民事再生手続、会社更生手続等の申立を受け、若しくは自ら申し立てた場合。

③　営業停止又は営業免許若しくは営業登録の取消等の行政上の処分を受けた場合。

g　警察庁が行う検査に際し、請負者又はその代理人、使用人等が職務執行を妨げ、又は詐欺その他の不正行為があると認めたとき。

h　自ら又は第三者を利用して次の各号に該当する行為をしたとき。

①　暴力的な要求行為

②　法的な責任を超えた不当な要求行為

③　取引に関して脅迫的な言動をし、又は暴力を用いる行為

④　偽計又は威力を用いて警察庁又はその職員の業務を妨害する行為

⑤　その他前各号に準ずる行為

ｉ　下記カの各号に該当するとき。

カ　私的独占又は不当な取引制限等に伴う違約金

警察庁は、オ(ｲ)の違約金のほか、請負者が次の各号に該当する場合、違約金（損害賠償額の予定）として契約金額の 100 分の 10 に相当する金額を請負者から徴収する。

(ｱ) 本契約に関し、私的独占の禁止及び公正取引の確保に関する法律（昭和 22 年法律第 54 号。次号において「独占禁止法」という。）第３条の規定に違反したことにより、公正取引委員会から、同法第７条の２第１項の規定に基づく課徴金の納付命令（以下「納付命令」という。）を行われ、当該納付命令が確定したとき（確定した当該納付命令が独占禁止法第 63 条第２項の規定により取り消された場合を含む）。

(ｲ) 納付命令又は独占禁止法第７条の規定に基づく排除措置命令（次号において「納付命令又は排除措置命令」という。）において、本契約に関し、独占禁止法第３条の規定に違反する行為の実行としての事業活動があったとされたとき。

(ｳ) 納付命令又は排除措置命令により、請負者に独占禁止法第３条の規定に違反する行為があったとされた期間及び当該違反する行為の対象となった取引分野が示された場合において、本契約が、当該期間（これらの命令に係る事件について、公正取引委員会が請負者に対し納付命令を行い、これが確定したときは、当該納付命令における課徴金の計算の基礎である当該違反する行為の実行期間を除く。）に入札（見積書の提出を含む。）が行われたものであり、かつ、当該取引分野に該当するものであるとき。

(ｴ) 本契約に関し、請負者（法人にあっては、その役員又は使用人を含む。）の刑法（明治 40 年法律第 45 号）第 96 条の６又は独占禁止法第 89 条第１項若しくは第 95 条第１項第１号に規定する刑が確定したとき。

キ　損害賠償

請負者は、請負者の故意又は過失により警察庁に損害を与えたときは、警察庁に対し、その損害について賠償する責任を負う。また、警察庁は、契約の解除及び違約金の徴収をしてもなお損害賠償の請求をすることができる。

なお、警察庁から請負者に損害賠償を請求する場合において、原因を同じくする支払済の違約金がある場合には、当該違約金は原因を同じくする損害賠償について、支払済額とみなす。

ク　不可抗力免責、危険負担

警察庁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又は毀損し、その結果、警察庁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。

ケ　金品等の授受の禁止

請負者は、対象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。

コ　宣伝行為の禁止

請負者及び対象業務に従事する者は、対象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、対象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。

サ　法令の遵守

請負者は、対象業務を実施するに当たり適用を受ける関係法令等を遵守しなくてはならない。

シ　安全衛生

請負者は、対象業務に従事する者の労働安全衛生に関する労務管理については、責任者を定め、関係法令に従って行わなければならない。

ス　記録及び帳簿類の保管

請負者は、対象業務に関して作成した記録及び帳簿類を、対象業務を終了し、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　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、警察庁と請負者との間で協議して解決する。

10　請負者が対象業務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請負者が負うべき責任（国家賠償法の規定により国の行政機関等が当該損害の賠償の責めに任ずる場合における求償に応ずる責任を含む。）に関する事項

(1) 請負者は、対象業務を実施するに当たり、請負者（その者が法人である場合にあっては、役員）又はその被雇用者その他の当該事業に従事する者が、故意又は過失により、第三者に損害を与えたときは、当該第三者に対する賠償の責に任ずるものとする。

この場合において、当該損害の発生について警察庁の責に帰すべき理由が存在するときは、請負者は、警察庁に対し、当該第三者に支払った損害賠償額のうち自ら賠償の責に任ずべき金額を超える部分について求償することができるものとする。

また、警察庁が当該第三者に対する賠償を行ったとき、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警察庁の責に帰すべき理由が存ずる場合は、警察庁が自ら賠償の責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ものとする。

(2) 請負者は、契約に違反し又は故意若しくは重大な過失によって、警察庁に損害を与えたときは、その損害に相当する金額を損害賠償として警察庁に支払わなければならない。

11　対象業務に係る法第７条第８項に規定する評価に関する事項

(1) 調査の時期

総務大臣が行う評価の時期（平成 32 年６月頃を予定）を踏まえ、本対象業務の実施状況を的確に把握するため、平成 32 年２月までに実施状況に関する調査を行うものとする。

(2) 調査方法等

ア　プログラム開発、システム構築等及びシステム賃貸借

納入検査又は検査をもって調査に替える。

イ　プログラム保守及びシステム賃貸借における保守

請負者が月１回行う保守報告をもって調査に替える。保守報告から調査する項目は次のとおり。

(ｱ) 障害復旧時間

(ｲ) 技術者駆けつけ時間

(ｳ) 障害報告の状況

(ｴ) 技術的質問への回答状況

(3) 意見聴取等

警察庁は必要に応じ、請負者から意見の聴取を行うことができるものとする。

(4) 実施状況等の提出時期

警察庁は、平成 32 年４月を目途として、対象業務の実施状況等を総務大臣及び監理委員会へ提出する。

なお、調査報告を総務大臣及び監理委員会に提出するに当たり、警察庁ＣＩＯ補佐官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) 会計検査院への報告等

請負者は、会計検査院法（昭和 22 年法律第 73 号）第 23 条第１項第７号に規定する者に該当することから、会計検査院の検査が必要と認められるときは、同法第 25 条及び法第 26 条により、同院の実地の検査を受けたり、同院から直接又は警察庁を通じて、資料、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。

(2) 監理委員会への報告

請負者は、法第 45 条により、官民競争入札等監理委員会から報告又は資料の提出を求められることがある。

(3) 監督体制

ア　本契約に係る監督は、支出負担行為担当官が、監督職員に命じて、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。

イ　本対象業務の実施状況に係る監督は、警察庁情報通信局情報管理課が行う。

(4) 本請負者の責務

ア　対象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。

別添１

事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書(案)

警 察 庁 情 報 通 信 局
警 情 仕 プ ロ 管 第 ● 号
平 成 ● 年 ● 月 ● 日 制 定

１　調達件名

事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラムに係る設計、開発、導入、調整等

２　品名及び略称

品名及び略称は、表－１のとおりとする。

表－１　品名及び略称

品　　名	略　　称
事前旅客情報照合業務及び 外国人個人識別情報認証業務用プログラム	業務用プログラム
サーバ用プログラム	
抽出系プログラム	抽出プログラム
事前旅客情報照合業務プログラム	APISプログラム
外国人個人識別情報認証業務プログラム	BICSプログラム
端末用プログラム	
専用端末Ａ用プログラム	端末Ａプログラム
専用端末Ｂ用プログラム	端末Ｂプログラム

３　作業の概要

３．１　目的

本仕様書は、事前旅客情報システム及び外国人個人識別情報認証システム（以下「業務システム」という。）において、事前旅客情報照合業務及び外国人個人識別情報認証業務を実施するために構築するプログラムに適用する。

３．２　背景

事前旅客情報照合業務及び外国人個人識別情報認証業務は、テロリスト及び不法入国者の上陸阻止、輸入禁制品等の密輸阻止及び指名手配者の逮捕等水際における取締りの徹底を図ることを目的とする業務である。

現在運用している業務システムのハードウェアが平成30年度に運用期限を迎えることに伴い、平成31年３月に新たな業務システムに更改するため、平成29年度及び30年度に対象となる機器の賃貸借、プログラム開発、構築及び保守作業を含めた調達を行うこととしている。

３．３　用語の定義

3.3.1　警察システム

APIS（警察）及びBICS（警察）の総称をいう。

3.3.2　APIS（警察）

警察庁が事前旅客情報照合業務を運用するために設置するサーバ､端末装置、プログラム等の総称をいう。

3.3.3　BICS（警察）

警察庁が外国人個人識別情報認証業務を運用するために設置するサーバ、端末装置、プログラム等の総称をいう。

3.3.4　外部システム

警察システムと連携する警察庁ホストシステム、警察庁指掌紋システム、アクセス権管理システム及び法務省システムの総称をいう。

3.3.5　警察庁ホストシステム

警察庁に設置される各種業務を行うホストシステムをいう。

3.3.6　警察庁指掌紋システム

関連仕様書の3.7.3項により整備したシステムをいう。

3.3.7　アクセス権管理システム

関連仕様書の3.7.2項により整備したシステムをいう。

3.3.8　法務省システム

APIS（法務省）及びBICS（法務省）の総称をいう。

3.3.9　APIS（法務省）

法務省が事前旅客情報照合業務を運用するために設置する、サーバ、端末装置等の総称をいう。

3.3.10　BICS（法務省）

法務省が外国人個人識別情報認証業務を運用するために設置する、サーバ、端末装置等の総称をいう。

3.3.11　警察BLファイル

警察BLファイル（APIS）及び警察BLファイル（BICS）の総称をいう。

3.3.12　警察BLファイル（APIS）

同種の情報に分類した警察BL（APIS）の集合をいう。

なお、警察BLファイル（APIS）の種別については、警察庁が別途指示する。

3.3.13　警察BL（APIS）

警察庁ホストシステムから取得又は専用端末Ａから端末登録された、事前旅客情報照合業務の照合に用いる情報をいう。1件ごとに取り扱う情報で分類し、該当する警察BLファイル（APIS）にまとめられる。

3.3.14　専用端末Ａ

端末Ａプログラムを運用し、APISプログラム及びBICSプログラムと連携して事前旅客情報照合業務及び外国人個人識別情報認証業務を行う端末装置をいう。警察庁、都道府県警察本部(方面本部を含む）及び警察署等に設置される。

3.3.15　警察BLファイル（BICS）

同種の情報に分類した警察BL（BICS）の集合をいう。

なお、警察BLファイル（BICS）の種別については、警察庁が別途指示する。

3.3.16　警察BL（BICS）

警察庁ホストシステム及び警察庁指掌紋システムから取得又は専用端末Ｂから端末登録された、外国人個人識別情報認証業務の認証に用いる情報をいう。１件ごとに取り扱う情報で分類し、該当する警察BLファイル（BICS）にまとめられる。

3.3.17　専用端末Ｂ

端末Ｂプログラムを運用し、抽出プログラムと連携して外国人個人識別情報認証業務を行う端末装置をいう。警察庁に設置される。

3.3.18　運用連絡通報

利用者に対し運用上の連絡が必要なときに、端末等に表示される連絡内容をいう。

3.3.19　端末等

専用端末、管理端末及び試験端末の総称をいう。

3.3.20　専用端末

専用端末Ａ及び専用端末Ｂの総称をいう。

3.3.21　管理端末

管理端末Ａ及び管理端末Ｂの総称をいう。

3.3.22　管理端末Ａ

APISプログラム及びBICSプログラムの維持管理及び運用状況の監視をするため、警察庁に設置される端末装置をいう。

3.3.23　管理端末Ｂ

抽出プログラムの維持管理及び運用状況の監視をするため、警察庁に設置される端末装置をいう。

3.3.24　試験端末

試験端末Ａ及び試験端末Ｂの総称をいう。

3.3.25　試験端末Ａ

APISプログラム及びBICSプログラムの機能確認及び試験を行うため、警察庁に設置される専用端末Ａをいう。

3.3.26　試験端末Ｂ

抽出プログラムの機能確認及び試験を行うため、警察庁に設置される専用端末Ｂをいう。

3.3.27　警報装置

ランプの点滅、ブザーの鳴動及び音声ファイルの再生を行い、ヒット受信及びシステム異常を知らせる装置をいう。端末等に併設又は都道府県警察本部等の執務室に単独で設置される。

3.3.28　中継サーバ

警察庁ホストシステムの構成機器で、抽出サーバが警察庁ホストシステムで作成したデータの取得を行う装置をいう。

3.3.29　抽出サーバ

主に抽出プログラムの運用を行い、警察庁ホストシステム、警察庁指掌紋シ

ステム、専用端末Ｂ等とデータを送受信し、必要な情報を抽出してデータ交換装置に送信する装置をいう。

3.3.30　専用端末Ｂ等

専用端末Ｂ，試験端末Ｂ及び管理端末Ｂを総称していう。

3.3.31　データ交換装置

ネットワーク間におけるデータの移動を、一方向に制限する装置をいう。警察システムにおいては、抽出サーバから業務サーバへの一方向のみにデータの移動を制限する。

3.3.32　業務サーバ

主にAPISプログラム及びBICSプログラムの運用を行い、データ交換装置、専用端末Ａ等及び法務省システムとデータを送受信し、警察BL（APIS）及び警察BL（BICS）に係る業務処理を行う装置をいう。

3.3.33　専用端末Ａ等

専用端末Ａ、試験端末Ａ及び管理端末Ａを総称していう。

3.3.34　指紋画像情報

警察庁指掌紋システムから取得されたデータをいう。

なお、データの詳細については警察庁が別途指示する。

3.3.35　抽出DB（BICS）

抽出プログラムが管理する、抽出データ及び登録データ（BICS）等を登録するデータベースをいう。

3.3.36　抽出データ

ホスト情報（BICS）から、警察BL（BICS）の登録に必要な情報を抽出したデータをいう。「抽出データ（今回）」「抽出データ（前回）」など、複数の世代に分けて管理する。

3.3.37　ホスト情報（BICS）

ホスト情報から、警察BLファイル（BICS）への登録に必要なファイルに分類したデータをいう。

なお、データの詳細については警察庁が別途指示する。

3.3.38　ホスト情報

警察庁ホストシステムから取得する、複数のファイルで構成されたデータをいう。

なお、ファイルの構成、データの詳細については警察庁が別途指示する。

3.3.39　登録データ（BICS）

警察BL（BICS）のうち、専用端末Ｂから登録され抽出プログラムが管理するデータをいう。

3.3.40　身分事項

氏名、生年月日及び性別で構成する人物に関する情報をいう。

3.3.41　警察BLDB（BICS）

警察BLファイル（BICS）を保存するデータベースをいう。

3.3.42　ユーザ情報

ユーザID、ユーザ名、所属、アクセス権等のユーザに関する情報をいう。

3.3.43　ヒット通知

警察庁の照合条件と法務省ヒット情報（APIS）又は法務省ヒット情報（BICS）が合致した場合に、専用端末Ａ等に強制送付する通知をいう。

3.3.44　法務省ヒット情報（APIS）

旅客情報とAPIS（法務省）が保有するデータベースを照合し、照合条件に合致した場合にAPIS（警察）あてに送付される旅客情報及び当該旅客情報に係るAPIS（法務省）が保有するデータをいう。

3.3.45　旅客情報

国際線の航空機が我が国に到着する前に、航空会社が府省共通ポータルを介して法務省に提供する、当該航空機並びに当該航空機に搭乗している乗客及び乗員に関するデータをいう。

3.3.46　府省共通ポータル

輸出入・港湾等関連手続を処理するために、関係省庁が提供している各種電子申請手続システムを相互に接続・連携を図ることを目的として開発されたシステムをいう。

3.3.47　法務省ヒット情報（BICS）

認証情報とBICS（法務省）が保有するデータベースを照合し、合致した場合にBICS（警察）あてに送付される認証情報及び当該指紋情報に係る法務省システムが保有するデータをいう。

3.3.48　認証情報

外国人から入国審査時に取得する情報をいう。

3.3.49　Webサーバ

主に専用端末Ａに係る業務処理を行う装置をいう。

3.3.50　警察BLDB（APIS）

警察BLファイル（APIS）を保存するデータベースをいう。

3.3.51　ホストコード

ホスト情報に含まれるファイルの一つ。必要な情報を抽出し、構成を変換して警察システムで取り扱う。

3.3.52　競合

異なる警察BLファイル（APIS）に、同一の警察BL（APIS）が重複して登録されていることをいう。また、競合状態にある警察BL（APIS）を登録したデータを、競合情報という。

3.3.53　ヒット情報DB（APIS）

ヒット情報（APIS）を保存するデータベースをいう。

3.3.54　ヒット情報（APIS）

APIS（警察）において、法務省ヒット情報（APIS）と警察BL（APIS）を照合し、照合条件に合致した警察BL（APIS）をいう。

3.3.55　ヒット通知一覧

専用端末Ａ、代行端末及び試験端末Ａで表示する、ヒット情報（APIS）及び法務省ヒット情報（BICS）の一覧をいう。

3.3.56　統一読み

「中国漢字読み方辞典」（編者：千島英一 発行所：教育システム 契約時における最新版）の日本語音読みをいう。

3.3.57　氏名変換

ホスト情報（APIS）の登録情報であるカナ氏名を、英字氏名に変換することをいう。

3.3.58　ホスト情報（APIS）

ホスト情報から、警察BLファイル（APIS）への登録に必要なファイルに分類したデータをいう。

なお、データの詳細については警察庁が別途指示する。

3.3.59　レスポンス

抽出サーバ、業務サーバが端末等からの要求受付完了後又は法務省ヒット情報（APIS）の受信完了後から通報又は回答の送信を開始するまでの時間をいう。

なお、登録等における法務省への送信から回答までの時間については、対象外とする。

3.3.60　現行システム

3.7.4項及び3.7.5項の関連仕様書により調達したソフトウェア及びハードウェアで、事前旅客情報照合業務及び外国人個人識別情報認証業務を現在運用しているシステムをいう。

3.3.61　開発用ソフトウェア

本プログラムの開発に必要となる、ソフトウェア及びツールをいう。

３．４　業務の概要

3.4.1　事前旅客情報照合業務

専用端末Ａから登録及び警察庁ホストシステムから取得した警察BL（APIS）を法務省に提供し、法務省において旅客情報と照合を行い、その照合結果を警察庁及び都道府県警察の関係部署に通報するものである。

3.4.2　外国人個人識別情報認証業務

専用端末Ｂから登録及び警察庁ホストシステム等から取得した警察BL(BICS)を法務省に提供し、法務省において入国審査時に外国人から取得した認証情報と照合し、その照合結果を警察庁及び都道府県警察の関係部署に通報するものである。

３．５　情報システム化の範囲

本作業では、「３．４　業務の概要」で説明した業務内容のうち、法務省システムへの警察BL（APIS）及び警察BL（BICS）の提供から警察庁及び都道府県警察の関係部署への通報等を行う機能を情報システム化の対象範囲とする。

３．６　作業内容・納入成果物

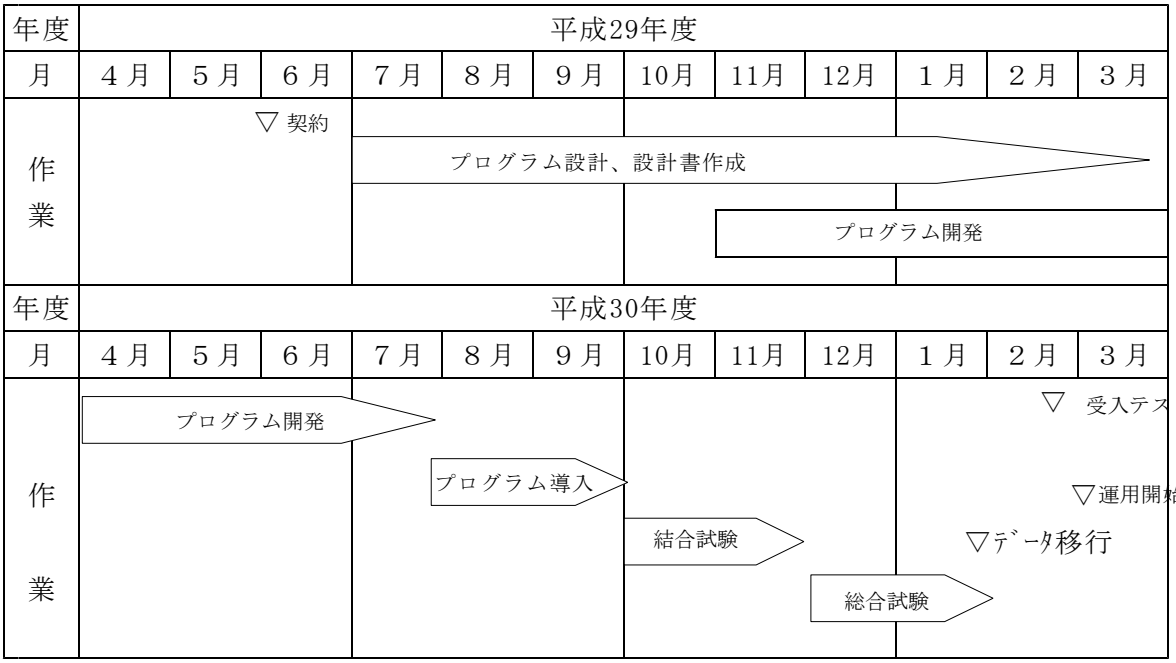
3.6.1　作業内容

本仕様書に基づき、警察システムにおいて正常に動作するプログラムを完成させるために必要となるプログラムの設計、開発、警察システムへの導入及び外部システムとの設定調整等を対象とする。

調達スケジュール（案）を表－２に示す。ただし、スケジュールは概略であ

り、詳細なスケジュールについては、警察庁と協議の上、設計開発実施計画書に記載すること。

表－２　調達スケジュール（案）



3.6.2　納入成果物

納入成果物は、別紙１のとおりとする。

3.6.3　提出資料

提出資料は、別紙２のとおりとする。

３．７　関連仕様書

3.7.1　警情仕形管第●号「事前旅客情報システム及び外国人個人識別情報認証システム仕様書」（平成●年●月●日制定）（以下、「ハードウェア仕様書」という。）

3.7.2　警情仕形管第38号「アクセス権管理システム仕様書」（平成25年２月１日制定）

3.7.3　警情仕形管第42号「指掌紋自動識別システム用照合部仕様書」（平成25年４月25日制定）

3.7.4　警情仕形管第30号「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書」（平成24年２月22日制定）

3.7.5　警情仕形管第40号「事前旅客情報システム及び外国人個人識別情報認証システム仕様書」（平成25年２月８日制定）

４　情報システムの要件

４．１　機能・性能要件

4.1.1　機能要件

(1)　サーバ用プログラムの共通機能は、表－３のとおりとする。

表－３　サーバ用プログラムの共通機能

区　分	項　目	機　　能
アクセス権	種類	次の分類に応じてアクセス権を設定できること。 なお、アクセス権設定の詳細は、警察庁が別途指示する。 (1) ユーザグループ (2) 所属 (3) 警察BLファイル（登録データ（BICS）を含む。）
	範囲	アクセス権に応じて、登録、照会、表示及びファイル入出力等の機能を制御すること。 なお、制御する機能については、警察庁が別途指示する。
入出力制御	印刷出力制御	(1) 画面に表示された各種一覧、詳細データ及び画像が印刷できること。 なお、印刷物の様式については警察庁が別途指示する。 (2) 印刷物の様式は、機能要件で示す機能ごとに設定ができ、容易に改修できること。 (3) 印刷物には、次に示すデータを付加すること。 ア　印刷年月日時分 イ　端末名 ウ　所属名 エ　ユーザ名 (4) 印刷をする際、印刷イメージを生成し、端末等でダウンロードして確認できること。
	ファイル出力制御	(1) 画面に表示された一覧の詳細データを、CSV形式で出力できること。 (2) 出力するデータには、次に示すデータを付加すること。 ア　出力年月日時分 イ　端末名 ウ　所属名 エ　ユーザ名 (3) ファイル出力は、機能要件で示す機能ごとに設定ができること。
	電磁的記録媒体入出力制御	(1) 印刷イメージ及びCSVファイルを電磁的記録媒体に出力できること。 (2) 電磁的記録媒体に出力する場合、出力する電磁的記録媒体及びフォルダの指定ができること。

		(3) 電磁的記録媒体からデータの入力ができること。 (4) 電磁的記録媒体から入力する場合、入力する電磁的記録媒体及びフォルダの指定ができること。
業務管理統計	作成	条件を指定して統計表が作成できること。 なお、統計表の詳細については、警察庁が別途指示する。
	参照	統計参照権限のあるユーザは、統計表を参照できること。
	定期抹消	登録の件数を保存した日から起算して１年以上経過したデータを月単位で抹消できること。
運用連絡通報	通報通知	(1) 運用連絡通報の内容を入力、訂正及び削除ができること。 (2) 通報日時及び通報先を指定し専用端末等に通知できること。 (3) 送信した運用連絡通報を管理できること。 (4) 送信時、端末等に併設する警報装置の動作を制御できること。 なお、警報装置の制御の詳細については、警察庁が別途指示する。
接続状態	表示	(1) 運用環境への端末等の接続状態を、管理端末Ａ又は管理端末Ｂに表示できること。 なお、接続状態の表示の詳細については警察庁が別途指示する。 (2) 試験環境への端末等の接続状態を、管理端末Ａ又は管理端末Ｂに表示できること。 なお、接続状態の表示の詳細については警察庁が別途指示する。
	接続	(1) 運用環境への端末等の接続を開始・停止できること。 (2) 試験環境への端末等の接続を開始・停止できること。
アクセスログ	生成	サーバ用プログラムの機能に対する端末等からのアクセスについて、アクセス開始・終了日時、使用した端末、ユーザ所属(府県、課、係等)、氏名(ユーザを識別する符号を含む。)、各処理の内容、入力項目等のアクセスログを生成すること。また、生成したアクセスログを保存すること。 なお、アクセスログの詳細については警察庁と別途協議すること。
	参照	(1) アクセスログ参照権限のあるユーザは、保存した

		アクセスログを下記の条件を指定して、端末等から参照できること。 ア　アクセス開始・終了日時 イ　ユーザ所属 ウ　端末等 (2) ユーザのアクセス権限に応じて、参照できるアクセスログの項目を設定できること。
	定期抹消	保存した日から起算して５年以上経過したログを日単位で自動抹消できること。
システムログ	生成	業務用プログラムの運用状況、エラー及び障害の発生をシステムログに生成すること。また、生成したシステムログを保存すること。
	参照	システムログを管理端末Ａ又は管理端末Ｂから参照できること。
	定期抹消	保存した日から起算して５年以上経過したログを日単位で自動抹消できること。

(2)　抽出プログラムの機能は、表－４のとおりとする。

表－４　抽出プログラムの機能

区　分	項　目	機　　能
抽出プログラム共通機能	通信制御機能	(1) 専用端末Ｂ等通信制御 専用端末Ｂ等と登録データ（BICS）のデータ通信を制御すること。 (2) 中継サーバ通信制御 中継サーバとホスト情報のデータ通信を制御できること。 (3) 警察庁指掌紋システム通信制御 警察庁指掌紋システムと指紋画像情報のデータ通信を制御できること。 (4) データ交換装置通信制御 データ交換装置とのデータ通信を制御できること。 (5) 冗長構成を用いた業務継続 装置異常時に、冗長構成の機器である抽出サーバを利用して業務の継続ができること。
	入力検査	(1) 専用端末Ｂ等から入力された登録のデータについて、検査をすること。 なお、検査の詳細については、警察庁が別途指示する。 (2) 検査結果を専用端末Ｂ等に表示すること。 なお、表示の詳細については警察庁が別途指示す

		る。
	件数カウント	(1) 登録の件数をカウントすること。 (2) カウントした件数が専用端末Ｂ等に表示できること。 なお、表示の詳細については警察庁が別途指示する。
	処理状況表示	登録の処理状況を専用端末Ｂ等に表示すること。 なお、表示の詳細については警察庁が別途指示する。
	処理確認	処理が完了した場合、その結果を専用端末Ｂ等に表示できること。 なお、結果の表示の詳細については警察庁が別途指示する。
ホスト情報登録	取得	(1) 取得するホスト情報ごとに、中継サーバへの接続先を設定できること。 (2) 中継サーバからホスト情報を取得し、取得後、中継サーバへ当該ホスト情報の削除を指示すること。 (3) 取得したホスト情報から、APIS、BICS及びホストコードのそれぞれで必要なファイルを判別し、それぞれの作業領域にコピーすること。
	抽出（APIS）	(1) APISの作業領域に保存したホスト情報からAPISに必要な情報を抽出し、ホスト情報（APIS）を作成すること。 なお、必要な情報の詳細については警察庁が別途指示する。 (2) ホスト情報及びホスト情報（APIS）は、世代管理を行い、一定期間保存すること。 なお、保存する一定期間については、警察庁が別途指示する。
	抽出（BICS）	(1) BICSの作業領域に保存したホスト情報を検索し、条件を満たすホスト情報を警察システムの文字コードに変換（大文字及び小文字の置換、全角文字及び半角文字の置換等を含む。）ができること。 なお、条件については警察庁が別途指示する。 (2) 変換したホスト情報からBICSに必要な情報を抽出し、ホスト情報（BICS）を作成すること。 なお、必要な情報の詳細については警察庁が別途指示する。
	登録（BICS）	(1) 抽出（BICS)機能で作成したホスト情報（BICS）を抽出DB（BICS）に抽出データ（今回）として登録すること。

		(2) 抽出DB（BICS）に登録されている前回の抽出データ（以下、「抽出データ（前回）」という。）と抽出データ（今回）を比較して差分データを抽出し、抽出DB（BICS）に登録すること。 (3) 抽出DB（BICS）から抽出データ（前回）を削除し、削除後、抽出データ（今回）を抽出データ（前回）に置換すること。 (4) 抽出DB（BICS）に登録されている、前々回の差分データを削除し、前回の差分データを削除待ち状態とすること。
	登録結果通知	(1) 抽出DB（BICS）に差分データが登録できた場合、登録の完了、登録件数、処理日時等を管理端末Ｂに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。 (2) 抽出DB（BICS）に差分データが登録できなかった場合、登録の失敗、処理日時等を管理端末Ｂに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。
	処理時間制限	差分データの登録処理が制限時間を超えた場合、管理端末Ｂへ通知すること。 なお、制限時間及び通知内容の詳細については、警察庁が別途指示する。
指紋画像情報登録	抽出	抽出DB（BICS）から最新の差分データを抽出すること。
	取得	差分データを基に、警察庁指掌紋システムから指紋画像情報を取得すること。
	登録	(1) 警察庁指掌紋システムから取得した指紋画像情報のうち身分事項については、警察システムの文字コードに変換（大文字及び小文字の置き換え、全角文字及び半角文字の置き換え等を含む。）し、抽出DB（BICS）に登録すること。 なお、警察システムの文字コードの詳細については、警察庁が別途指示する。 (2) 警察庁指掌紋システムから取得した指紋画像情報の身分事項と差分データの身分事項を照合し、適合及び不適合の判定を行い、適合した差分データ（以下「適合データ」という。）を抽出DB（BICS）に登録すること。また、判定結果を専用端末Ｂに通知で

		きること。 　なお、適合及び不適合の判定の詳細については、警察庁が別途指示する。 (3) 指紋画像情報が未取得の差分データ及び不適合となった差分データについては、一定期間管理できること。 　なお、管理する一定期間については、警察庁が別途指示する。
	一連番号の生成	抽出DB（BICS）に適合データを登録する際には、１件単位に一連番号を生成すること。 　なお、生成する一連番号の体系については警察庁が別途指示する。
	登録結果通知	(1) 抽出DB（BICS）に適合データが登録できた場合、登録の完了、登録件数、処理日時等を管理端末Ｂに通知すること。 　なお、通知する内容の詳細については、警察庁が別途指示する。 (2) 抽出DB（BICS）に適合データが登録ができなかった場合、登録の失敗、処理日時等を管理端末Ｂに通知すること。 　なお、通知する内容の詳細については、警察庁が別途指示する。
	処理時間制限	適合データの登録処理が制限時間を超えた場合、管理端末Ｂへ通知すること。 　なお、制限時間及び通知内容の詳細については、警察庁が別途指示する。
専用端末Ｂからの登録	登録画像の読込み	(1) スキャナ又は電磁的記録媒体から、画像の読込みができること。 　なお、画像の解像度及び形式等については、警察庁が別途指示する。 (2) 読込んだ登録画像の切り出し処理、解像度変更及び白黒反転等の加工ができること。 　なお、切り出し位置、解像度等、加工の詳細については、警察庁が別途指示する。 (3) 読込んだ画像を、警察庁が別途指示する画像形式の登録画像及び専用端末Ｂで表示できる形式の画像に変換できること。 　なお、専用端末Ｂに表示する形式については、警察庁と別途協議すること。 (4) 変換した画像を、専用端末Ｂ等に表示できること。

	登録	(1) 抽出DB（BICS）に登録する登録データ（BICS）を専用端末Ｂから１件単位で入力できること。 (2) (1)の入力内容について、入力検査の結果に異常が無い場合は、入力内容に基づいて指紋画像情報を取得し、登録データ(BICS)と関連付けること、又は、上記「登録画像の読み込み」で変換した登録画像と関連付けること。 なお、指紋画像情報の取得の詳細については警察庁が別途指示する。 (3) 登録データ(BICS)と、指紋画像情報又は登録画像との関連付けができた場合、抽出DB（BICS）に登録データ（BICS）を新規登録できること。 (4) 入力検査の結果に異常がない場合、抽出DB（BICS）の登録データ（BICS）を訂正登録できること。 (5) 登録データ（BICS）を抽出DB（BICS）に登録する際には、１件単位に一連番号を自動で生成又は入力できること。 なお、生成する一連番号の体系については警察庁が別途指示する。 (6) 登録データ（BICS）の抽出DB（BICS）への登録結果を専用端末Ｂに表示すること。 なお、登録結果の詳細については、警察庁が別途指示する。
	注意喚起	登録データ（BICS）を抽出DB(BICS)に登録する前に、専用端末Ｂに注意喚起を促すメッセージを表示すること。
	定期抹消	(1) 一定期間以上経過した抽出DB（BICS）に登録された登録データ（BICS）を日単位で抽出DB（BICS）から抹消すること。 なお、一定期間の詳細については、警察庁が別途指示する。 (2) 定期抹消した結果を専用端末Ｂ等に表示できること。 なお、表示の詳細については警察庁が別途指示する。
ホスト情報（APIS）及び転送データ（BICS）の転送	転送データ（BICS）の抽出	(1) 抽出DB（BICS）から、転送用に適合データ及び登録データ（BICS）(以下「転送データ（BICS)」という。）を自動抽出すること。 なお、自動抽出方法、抽出時刻、抽出ファイル、抽出項目等については、警察庁が別途指示する。

		(2) (1) の転送データ（BICS）については、抽出DB（BICS）とは別に保存すること。 (3) 自動抽出のほか、任意の時刻に管理端末Ｂを用いて手動で抽出ができること。 (4) 抽出結果の確認ができること。 なお、抽出結果の確認方法については、警察庁が別途指示する。
	定期抹消	抽出DB（BICS）の定期抹消を行う場合、定期抹消する登録データ（BICS）を抽出DB（BICS）から抽出し、データ交換装置を介して、業務サーバにFTPにより自動転送し、該当する警察BLDB（BICS）を削除登録できること。 なお、定期抹消の詳細については、警察庁が別途指示する。 また、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。
	転送（APIS）	(1) 保存されたホスト情報（APIS）については、データ交換装置を介して、業務サーバにFTPにより自動転送できること。 なお、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。 (2) 自動転送のほか、手動による即時転送及び転送停止ができること。 (3) 転送結果の確認ができること。 なお、転送結果の確認方法については、警察庁が別途指示する。
	転送（BICS）	(1) 抽出した転送データ（BICS）については、データ交換装置を介して、業務サーバにFTPにより自動転送できること。 なお、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。 (2) 自動転送のほか、手動による即時転送及び転送停止ができること。 (3) 転送結果の確認ができること。 なお、転送結果の確認方法については、警察庁が別途指示する。
	表示	(1) ホスト情報（APIS）の転送結果を管理端末Ｂに表示できること。 なお、転送結果の表示の詳細については警察庁が別途指示する。

		(2) 転送データ（BICS）を条件指定して管理端末Ｂに表示できること。 　なお、条件及び表示方法の詳細については警察庁が別途指示する。 (3) 抽出及び転送が正常に終了しなかった場合、異常のあった旨を管理端末Ｂ及び警報装置に通知ができること。 　なお、通知の詳細については警察庁が別途指示する。 (4) 管理端末Ｂから転送に関する履歴が管理できること。
試験	試験環境	(1) 運用環境と同等の機能が確認できる試験環境を構築できること。 　なお、試験環境は業務で使用するものとは別に作成し、運用環境に影響を与えないこと。 (2) 試験環境は専用端末Ｂ等と接続ができること。また、試験接続は、専用端末Ｂ等ごとに設定ができること。 (3) 試験中は、専用端末Ｂ等に試験中であることを明示すること。
接続	警察庁ホストシステムとの接続	運用環境及び試験環境から中継サーバと接続ができること。
	警察庁指掌紋システムとの接続	運用環境及び試験環境から警察庁指掌紋システムの運用環境及び試験環境と接続できること。
メンテナンス	ログ出力設定	専用端末Ｂ等ごと及びアクセス権ごとに、出力できるログの種類及び出力内容を設定できること。 　なお、ログの種類及び出力内容の詳細については警察庁が別途指示する。
	試験環境設定	(1) 専用端末Ｂ等ごとに試験環境に接続する設定ができること。 (2) 試験環境へ接続している専用端末Ｂ等の情報が一覧で表示できること。 　なお、一覧表示の詳細については警察庁が別途指示する。
	登録データ（BICS）等内容確認	(1) 抽出DB（BICS）に登録されている転送データ（BICS）の内容を、日時又は期間を指定して表示できること。 　なお、表示の詳細については警察庁が別途指示す

		る。 (2) 抽出DB（BICS）に登録されている登録データ（BICS）の内容を一連番号又は全てを指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。
	変換テーブル等メンテナンス	(1) コード変換テーブルの更新ができること。 なお、変換テーブルは警察庁からデータを提供することとし、変換が必要なデータ、変換方法、変換タイミング等の詳細については、警察庁が別途指示する。 (2) 運用環境と試験環境で、コードの同期がとれること。
	定期抹消設定	定期抹消において、登録データファイル（BICS）ごとに抹消結果の通知先を設定できること。
	ホスト情報等登録結果	(1) ホスト情報等の登録結果を管理端末Ｂに表示すること。 なお、登録結果の表示の詳細については別途指示する。 (2) ホスト情報等の登録において異常があった場合、その内容を管理端末Ｂに表示すること。
	警察庁ホストシステム間機能の開始・停止設定	(1) ホスト情報の取得の開始・停止を設定できること。 (2) 中継サーバと抽出サーバの接続状況を管理端末Ｂから確認できること。 なお、接続状況の表示の詳細については警察庁が別途指示する。
	警察庁指掌紋システム間機能の開始・停止設定	(1) 指紋画像情報の取得の開始・停止を設定できること。 (2) 警察庁指掌紋システムと抽出サーバ等の接続状況を管理端末Ｂから確認できること。 なお、確認方法については警察庁が別途指示する。
	業務サーバ間機能の開始・停止機能	(1) ホスト情報（APIS）及び転送データ（BICS）の転送の開始・停止を設定できること。 (2) 転送機能の状態を管理端末Ｂから確認できること。 なお、確認方法については警察庁が別途指示する。
ユーザ情報	認証	(1) 専用端末Ｂ等に接続した生体認証装置による生体情報の取得及び送信等を制御できること。 (2) ユーザの認証情報を、端末Ｂプログラムから受信できること。 (3) 受信したユーザの認証情報から、ユーザの照合が

		できること。 (4) 認証が認められた場合、対応するユーザ情報をアクセス権管理システムから取得できること。 (5) 取得したユーザ情報から、抽出プログラムにログインできること。 (6) 取得したユーザ情報から、業務ごとにアクセス権の制御を行うこと。 (7) 認証が認められなかった場合、再度認証を行い、一定回数認証が認められなかった場合には、当該ユーザからの認証要求について、解除するまで受け付けないこと。 なお、受け付けなくなるまでの認証の回数については、警察庁が別途指示する。

(3) APISプログラムの機能は、表－５のとおりとする。

表－５ APISプログラムの機能

区 分	項 目	機 能
APISプログラム共通機能	通信制御機能	(1) APIS（法務省）間通信制御 APIS（法務省）とファイル転送、法務省ヒット情報(APIS) のデータ通信を制御できること。 (2) 専用端末Ａ等通信制御 専用端末Ａ等と登録、照会、回答及びヒット通知のデータ通信を制御すること。 (3) データ交換装置間通信制御 データ交換装置とデータ通信を制御できること。 (4) 冗長構成を用いた業務継続 装置異常時に、冗長構成の機器である業務サーバ、Webサーバを利用して業務の継続ができること。
	入力検査	(1) 専用端末Ａ等から入力された登録及び照会のデータについて検査をすること。 なお、検査の詳細については、警察庁が別途指示する。 (2) 検査結果を専用端末Ａ等に表示すること。
	件数カウント	(1) 登録、照会、回答、ヒット通知の件数をカウントすること。 (2) カウントした件数を専用端末Ａ等に表示できること。 なお、表示の詳細については警察庁が別途指示する。
	処理状況表	登録及び照会の処理状況を専用端末Ａ等に表示する

	示	こと。 なお、表示の詳細については警察庁が別途指示する。
	処理確認	処理が完了した場合、その結果を専用端末Ａ等に表示できること。 なお、表示の詳細については警察庁が別途指示する。
	取扱いデータの種類	データは、日本語のほか、中国語（簡体字、繁体字）及び韓国語（ハングル文字）を扱うことができること。
ホスト情報登録	取得	ホスト情報（APIS）を、抽出サーバからデータ交換装置を介して、FTPにより取得できること。 なお、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。
	登録	(1) ホスト情報（APIS）を警察システムの文字コードに変換(大文字及び小文字の置き換え、全角文字及び半角文字の置き換え等を含む。）すること。 なお、警察システムの文字コードの詳細と変換内容については、警察庁が別途指示する。 (2) 警察BLDB（APIS）に登録されているホスト情報（APIS）を削除、又は差分を抽出し、新たに取得したホスト情報（APIS）又は差分データを警察BLDB（APIS）に登録すること。
	一連番号の生成	警察BLDB（APIS）にホスト情報を登録する際には、１件単位に一連番号を生成すること。 なお、生成する一連番号の体系については警察庁が別途指示する。
	入力データ変換	(1) 氏名の入力データについて、カナ氏名から英字氏名へデータ変換ができること。 (2) 入力されたホストコードを、変換テーブルを用いて必要なデータに変換できること。 なお、変換テーブル及び変換方法については警察庁が別途指示する。
	照合用氏名の生成	ホスト情報（APIS）を警察BLDBに登録する際、警察BLファイル（APIS）ごとの照合・照会条件の設定に基づいた照合用氏名を生成し、ホスト情報（APIS）と共に警察BLDBに登録すること。 なお、生成方法の詳細については警察庁が別途指示する。
	登録結果通知	(1) 警察BLDB（APIS）にホスト情報（APIS）が登録できた場合、登録の完了を管理端末Ａに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。

		(2) 警察BLDB（APIS）にホスト情報（APIS）が登録ができなかった場合、登録の失敗を管理端末Ａに通知すること。 　なお、通知する内容の詳細については、警察庁が別途指示する。
	処理時間制限	ホスト情報の登録処理が制限時間を超えた場合、管理端末Ａへ通知すること。 なお、制限時間及び通知内容の詳細については、警察庁が別途指示する。
専用端末Ａからの登録	端末登録	(1) 端末Ａプログラムで作成した登録用ファイルを読込み、ファイルに保存されたデータの一覧を専用端末Ａに表示すること。 (2) (1)で表示した一覧から、警察BLDB（APIS）に登録するデータを選択できること。 (3) (2)で選択したデータについて、登録先の警察BLファイル（APIS）の種別を指定し、同ファイルと照合すること。 (4) (3)の後に、他の警察BLファイル（APIS）と照合し、競合情報を専用端末Ａに表示すること。 (5) (3)の結果が未登録の場合、警察BLDB（APIS）に警察BL（APIS）を登録すること。 (6) 警察BL（APIS）を警察BLDB（APIS）に登録する際には、１件単位に一連番号を自動で付与すること。 　なお、付与する一連番号の体系については警察庁が別途指示する。 (7) 警察BL（APIS）の警察BLDB（APIS）への登録結果を、専用端末Ａに表示すること。 　なお、登録結果及び表示の詳細については、警察庁が別途指示する。 (8) 登録結果を保存すること。 (9) (8) で保存したデータを専用端末Ａに表示すること。 　なお、表示の詳細については警察庁が別途指示する。 (10) 保存した登録結果は、一定期間経過後に自動で削除すること。 　なお、一定期間の詳細については警察庁が別途指示する。
	訂正・削除登録	(1) 端末Ａプログラムで作成した訂正・削除用ファイルを読込み、ファイルに保存されたデータの一覧を

		表示すること。 なお、表示の詳細については警察庁が別途指示する。 (2) (1)の一覧から、警察BL（APIS）に登録するデータを1件ごと選択できること。 (3) (2)で選択したデータについて、対象となる警察BL（APIS）を警察BLDB（APIS）から取得できること。 (4) (2)で選択したデータと(3)で取得したデータを、専用端末Ａの画面に並列表示すること。 (5) (4)の後、(1)の画面に戻り、表示した一覧から、訂正・削除を実施するデータを選択できること。 (6) (5)で選択した警察BL（APIS)の訂正・削除の処理を実施し、その結果を専用端末Ａに表示すること。 なお、処理結果の詳細については、警察庁が別途指示する。 (7) 訂正・削除の処理結果を、保存すること。 (8) (7) で保存したデータを専用端末Ａに表示すること。 なお、表示の詳細については別途指示する。 (9) 保存した訂正・削除の処理結果は、一定期間経過後に自動で削除すること。 なお、一定期間の詳細については警察庁が別途指示する。
	照合用氏名の生成	警察BL（APIS）を警察BLDB（APIS）に登録する際、警察BLファイル（APIS）ごとの照合・照会条件設定に基づいた照合用氏名を生成し、警察BL（APIS）と共に登録すること。 なお、生成方法の詳細については警察庁が別途指示する。
	注意喚起	警察BL（APIS）を警察BLDB(APIS)に登録する前に、専用端末Ａに注意喚起を促すメッセージを表示すること。
	定期抹消	(1) 警察BLDB（APIS）に登録されてから一定期間以上経過した警察BL（APIS）を、日単位で警察BLDB（APIS）から抹消すること。 なお、一定期間の詳細については、警察庁が別途指示する。 (2) 定期抹消の結果を専用端末Ａに表示できること。 なお、表示の詳細については警察庁が別途指示する。

競合情報	照合	(1) 警察BLDB（APIS）において、登録する警察BL（APIS）を登録対象以外の警察BLファイル（APIS）と照合し、競合の有無を確認すること。 (2) 競合の有無の確認の結果を、端末登録機能(8)の登録結果として登録すること。 (3) 警察BLファイルごとに、照合対象の警察BLファイル（APIS）及び競合通知先の所属を設定できること。
	保存	(1) 照合の結果、他の警察BLファイル（APIS）に競合して登録されていた場合、競合元及び競合先に関する情報を、競合情報として保存すること。 (2) 保存した日から一定期間以上経過した競合情報を、日単位で自動削除すること。 なお、一定期間の詳細については、警察庁が別途指示する。
	表示	保存した競合情報を専用端末Ａに表示できること。
	照会	表示された競合情報が他の警察BLファイル（APIS）と競合しているか照会できること。
警察BL(APIS)照会	即時照会	(1) 警察BLDB（APIS）に照会するデータを、専用端末Ａから１件単位で入力できること。 (2) 照会する警察BLファイルを選択して、以下のア～ウの情報を用いて警察BL（APIS）が照会でできること。 なお、ア～ウの情報の詳細については警察庁が別途指示する。 ア　人定情報 イ　一連番号 ウ　登録所属 (3) 入力検査の結果が正常であった場合、警察BLDB（APIS）に対して照会ができること。 (4) 照会中に処理の中止ができること。 (5) 照会の処理状況が分かること。 なお、処理状況の詳細については警察庁が別途指示する。
	照会結果表示	(1) 照会した結果を専用端末Ａに表示すること。 なお、表示の詳細については警察庁が別途指示する。 (2) 照会した結果をファイルに出力できること。 なお、ファイル形式及びデータレイアウト等の詳細については、警察庁と別途協議すること。 (3) 照会結果が一定件数を超える場合は、画面表示を

		取りやめ、(2)の方法及び件数を分割して、照会結果を出力すること。 なお、一定件数については、警察庁と別途協議すること。
	照会条件設定	警察BLファイル（APIS）ごとに照合・照会条件を設定し、照会できること。 なお、照合・照会条件については警察庁が別途指示する。
警察BL(APIS)の法務省への転送	抽出	(1) 警察BLDB（APIS）から転送用の警察BL（APIS）を自動抽出すること。 なお、自動抽出方法、抽出時期、抽出ファイル、抽出項目等の自動抽出の詳細については、警察庁が別途指示する。 (2) （1）の転送用の警察BL（APIS）について、警察BLDB（APIS）とは別に保存すること。 (3) （1）の転送用の警察BL（APIS）は、一意となる一連番号を生成すること。 なお、生成する一連番号の体系については警察庁が別途指示する。 (4) 任意の時刻に管理端末Ａを用いて手動で抽出ができること。 (5) 管理端末Ａから手動抽出／自動抽出／抽出停止の切替の操作ができること。 (6) 管理端末Ａから抽出する警察BLファイル（APIS）の選択ができること。 (7) 管理端末Ａから抽出する警察BLファイル（APIS）ごとに、抽出する項目の情報が選択できること。 なお、抽出する項目については、警察庁が別途指示する。 (8) 抽出結果を、管理端末Ａで確認できること。 なお、抽出結果の確認方法については、警察庁が別途指示する。 (9) APIS（法務省）への転送済みの警察BL（APIS）ついて、警察BLDBからの再抽出を、管理端末Ａから実施できること。
	定期抹消	警察BLDB（APIS）から警察BL（APIS）の定期抹消を行う場合、当該警察BL（APIS）の削除をAPIS（法務省）に依頼するデータを作成し、送信すること。 なお、作成するデータの詳細については、警察庁が別途指示する。

	検査	警察BLDB（APIS）から転送用の警察BL（APIS）を抽出する際には、抽出する項目を検査すること。 なお、検査の詳細については、別途指示する。
	転送用データへの変換	検査が完了した転送用の警察BL（APIS）は、APIS（法務省）に転送する転送用データに変換すること。 なお、転送用データの詳細については、警察庁が別途指示する。
	転送	(1) 変換した転送用データは、１件ごと又は複数件を一括してAPIS（法務省）に自動転送すること。 (2) APIS（法務省）と転送結果の送達確認ができること。 なお、送達確認の詳細については、警察庁が別途指示する。 (3) 任意の時刻に管理端末Ａを用いて手動で転送を実行できること。 (4) 管理端末Ａから手動転送／自動転送／転送停止の切替の操作ができること。 (5) 転送結果を、管理端末Ａで確認できること。 なお、転送結果の確認方法については、警察庁が別途指示する。 (6) 管理端末Ａから転送に関する履歴を管理できること。
	表示	(1) 転送用データの転送処理過程、転送結果を、管理端末Ａで確認できること。 なお、転送処理過程及び転送結果の詳細については、警察庁が別途指示する。 (2) (1)の確認中に異常が発見された場合には、管理端末Ａ及び警報装置に通知すること。 なお、異常の詳細については、警察庁が別途指示する。 (3) 定期抹消の結果を管理端末Ａに表示できること。 なお、表示の詳細については警察庁が別途指示する。 (4) 転送に関する履歴を管理端末Ａに表示できること。 なお、表示の詳細については警察庁が別途指示する。
照合	受信	APIS（法務省）から法務省ヒット情報（APIS）を自動取得できること。 なお、自動取得の詳細については、警察庁が別途指示する。

	検査	(1) 取得した法務省ヒット情報（APIS）について、検査すること。 　なお、検査の詳細については、警察庁が別途指示する。 (2) (1)の検査の結果、取得した法務省ヒット情報（APIS）に異常がある場合、取得した法務省ヒット情報（APIS）を破棄すると共に、管理端末Ａに通知をすること。 　なお、通知の詳細については、警察庁が別途指示する。
	照合条件による照合	(1) 検査の結果が正常であった法務省ヒット情報（APIS）については、ヒット情報DB（APIS）と自動照合し、合致する情報の有無を確認すること。 (2) (1)の照合の結果、合致する場合、法務省ヒット情報（APIS）を破棄すること。 (3) (1)の照合の結果、合致しない場合、照合・照会条件の設定に従い、警察BLDB（APIS）と照合すること。 　なお、照合・照会条件については警察庁が別途指示する。 (4) (3)の照合の結果から、ヒット通知の必要性の有無を判定すること。 　なお、判定の条件については、警察庁が別途指示する。 (5) (4)の判定の結果を、APIS（法務省）に照合理由依頼通知として通知すること。 　なお、通知の詳細については、警察庁が別途指示する。
ヒット通知	ヒット通知	(1) ヒット通知が必要となったヒット情報（APIS）については、ヒット情報の条件設定に従ってヒット通知先に通知すること。 　なお、ヒット通知先は、法務省ヒット情報（APIS）に該当する警察BL(APIS)において個別に設定された通知先、又は警察BLファイルごとに設定された共通の通知先が設定される。 (2) メインメニュー画面からヒット通知先及びヒット通知の代行先を、専用端末Ａで確認できること。
	警報装置制御	(1) ヒット情報（APIS)の内容に応じ、警報装置を鳴動させること。 　なお、警報装置の鳴動の詳細については、警察庁が別途指示する。

		(2) 警報装置の鳴動を確認すること。 (3) (2)の後、警報装置の鳴動が停止されたことを確認すること。 (4) (2)及び(3)の確認の結果を管理端末Ａに通知すること。 　なお、確認内容の詳細については、警察庁が別途指示する。
	照合結果等表示	(1) 法務省ヒット情報（APIS）の受信結果及び照合結果について、管理端末Ａに表示できること。 　なお、表示内容の詳細については、警察庁が別途指示する。 (2)　照合機能及びヒット通知機能の処理中に異常が見られた場合、管理端末Ａ及び警報装置に通知すること。 　なお、通知内容の詳細については、警察庁が別途指示する。
ヒット情報（APIS）	登録	ヒット情報（APIS）及び法務省ヒット情報（APIS）をヒット情報DB（APIS）へ登録すること。
	ヒット通知一覧	ヒット情報DB（APIS）から、ヒット通知一覧を抽出すること。 　なお、ヒット通知一覧の詳細については、警察庁が別途指示する。
	表示	(1) 業務プログラムにログインすることなく、専用端末Ａでヒット通知一覧を確認できること。また、ヒット通知一覧からヒット情報（APIS）の詳細を確認する場合は、ユーザ認証を行うこと。 　なお、確認方法については、警察庁が別途指示する。 (2) 業務プログラムにログインにしている場合、専用端末Ａで、ヒット通知一覧及びヒット情報（APIS）の詳細を表示できること。 　なお、表示方法及び表示内容の詳細については、警察庁が別途指示する。
	定期抹消	(1) 一定期間以上経過したヒット情報DB（APIS）に登録されたヒット情報（APIS）及び法務省ヒット情報（APIS）を日単位に自動抹消すること。 　なお、一定期間の詳細については、警察庁が別途指示する。 (2) 定期抹消した結果を、専用端末Ａに表示できること

ヒット情報（APIS）照会	即時照会	(1) ヒット情報DB（APIS）に照会するデータを、専用端末Ａから１件単位で入力できること。 　なお、入力するデータの詳細については警察庁が別途指示する。 (2) 入力検査の結果が正常であった場合、ヒット情報DB（APIS）に対して照会ができること。 (3) 照会中に処理の中止ができること。 (4) 照会の処理状況を専用端末Ａに表示できること。 　なお、表示の詳細については警察庁が別途指示する。 (5) 照会した結果を専用端末Ａに表示できること。 　なお、表示の詳細については警察庁の別途指示する。
	日本語、中国語及び韓国語変換	(1) 日本語から中国語（簡体字、繁体字)、ピンイン及び統一読みへの変換ができること。 (2) 中国語（簡体字）から日本語、中国語（繁体字)、ピンイン及び統一読みへの変換ができること。 (3) 中国語（繁体字）から日本語、中国語（簡体字)、ピンイン及び統一読みへの変換ができること。 (4) 日本語から韓国語（ハングル文字）及び韓国語（ローマ字）への変換ができること。 (5) 韓国語（ハングル文字）から日本語及び韓国語（ローマ字）への変換ができること。 (6) 統一読みへの変換テーブルについては、警察庁が官給する、3.3.56 「中国漢字読み方辞典」の電子データをもとに作成すること。 (7) (6)以外の変換テーブルについては、警察庁が保有する変換テーブルをデータで提供する。
ヒット通知の代行	設定	(1) 代行元の専用端末Ａで代行設定することにより、代行先の専用端末Ａにおいてもヒット情報（APIS）が表示されること。 (2) 代行元の専用端末Ａで代行設定することにより、代行先の警報装置の鳴動等を制御できること。 (3) 代行設定及び解除は、手動で設定する方法及び期間、時間及び日付を設定することにより自動で設定する方法で行えること。また、期間にあっては複数設定可能であること。 (4) 代行設定は、全ての所属のユーザーが設定できること。 (5) 管理端末Ａから、全ての専用端末Ａの代行設定期

		間を一括して設定できること。また、専用端末Aは、一括して設定した代行設定期間を変更できること。
	代行表示	(1) 代行元の専用端末A ア　代行中であることを専用端末Aに表示できること。 イ　代行設定を行った所属を、専用端末Aで確認できること。 ウ　ログインすることなく代行状態を確認できること。 エ　確認方法及び表示の詳細については警察庁が別途指示する。 (2) 代行先の専用端末A ア　代行された旨を専用端末Aに表示できること。 イ　代行元の専用端末Aの代行状態に関する所属の情報を専用端末Aに表示できること。 ウ　代行設定が解除された場合、解除された旨を専用端末Aに表示できること。 エ　表示の詳細については警察庁が別途指示する。
	代行先の警報装置制御	代行元の警報装置と同等の制御ができること。
他システムへの照会	準即時照会	(1) 他システムに照会するデータを、専用端末Aから１件単位で入力できること。 (2) 入力検査の結果が正常であった場合、他システムに対して照会に必要なデータが送信できること。 (3) 他システムに対して、一定間隔で受信要求を行い、回答データを受信できること。 なお、受信要求の間隔については、警察庁が別途指示する。 (4) 一定期間以上経過して回答がない場合、照会データを削除できること。 なお、一定期間の詳細については、警察庁が別途指示する。 (5) 管理端末Aから手動により他システムへの照会機能の開始・停止の切替の操作ができること。 (6) 回答データの結果を一定期間保存できること。 なお、一定期間の詳細については、警察庁が別途指示する。 (7) (1)～(5)項に係る他システムの詳細については、警察庁が別途指示する。
	再送	他システムに対して照会に必要なデータを送信して

		から受信要求間隔として設定した時間までに回答データを受信できない場合、照会に必要なデータを自動で再送すること。 なお、他システムの詳細については、警察庁が別途指示する。
	検査	他システムから受信した回答データの各項目について、検査すること。 なお、他システムの詳細及び検査の内容の詳細については、警察庁が別途指示する。
	照会結果表示	(1) 準即時照会 照会した結果を専用端末Aに表示できること。 なお、表示の詳細については警察庁が別途指示する。 (2) 準即時照会の照会過程、処理結果を、管理端末Aで確認できること。 なお、照会過程及び処理結果の詳細については、警察庁が別途指示する。 (3) (2)の確認中に異常が発見された場合には、管理端末A及び警報装置に通知すること。 なお、異常の詳細については、警察庁が別途指示する。
	注意喚起	他システムに照会するデータを送付する前に、専用端末Aに注意喚起を促すメッセージを表示すること。
コード出力	コード出力	国名等のコード変換テーブルをファイルに出力できること。 なお、出力するコードの種類及びファイルの詳細については、警察庁と別途協議すること。
試験	試験環境	(1) 運用環境と同等の機能が確認できる試験環境を構築できること。 なお、試験環境は運用環境で使用するものとは別に作成し、運用環境に影響を与えないこと。 (2) APIS(警察)の単独での試験環境とは別に、APIS(法務省)と接続する試験環境を構築できること。 (3) 試験環境は専用端末A等と接続ができること。また、試験環境と専用端末A等との接続は、個別に設定ができること。 (4) 試験中は専用端末A等に試験中であることを明示すること。
	試験機能	作成した試験データで、APISプログラムの機能が確認できること。

メンテナンス	ログ出力設定	専用端末Ａ等ごと及びアクセス権ごとに、出力できるログの種類並びに出力内容を設定できること。 なお、ログの種類及び出力内容の詳細については警察庁が別途指示する。
	試験環境設定	(1) 専用端末Ａ等ごとに試験環境に接続する設定ができること。 (2) 試験環境へ接続している専用端末Ａ等の情報が一覧で表示できること。 なお、一覧表示の詳細については警察庁が別途指示する。 (3) 試験データ（登録、即時・準即時照会、ヒット通知）の作成及び編集ができること。 (4) 試験データの情報が一覧で表示できること。 なお、一覧表示の詳細については別途指示する。 (5) APIS（警察）の単独試験と、APIS（法務省）との接続試験の切替ができること。 なお、切替方法については、警察庁と協議すること。
	変換テーブル等メンテナンス	(1) 抽出サーバから取得したホスト情報（APIS）及び専用端末Ａから入力した警察BL（APIS）について、変換テーブルを用いて、氏名変換及びコード変換等の必要なデータ変換ができること。 なお、変換テーブルは警察庁からデータを提供することとし、変換が必要なデータ、変換方法及び変換のタイミング等の詳細については、警察庁が別途指示する。 (2) データ変換テーブルの更新ができること。 (3) コードの登録・削除を行った場合、コードの表示・非表示等の挙動及び内部処理について、警察庁と別途協議すること。
	件数制限設定	(1) 各照会の結果ごとに回答するデータの件数及び一括登録可能な件数等の制限ができること。 (2) 件数制限を超えた場合、専用端末Ａ等にメッセージ表示ができること。 (3) 件数制限が変更できること。
	処理時間設定	(1) 登録、照会等に要する処理時間の制限ができること。 (2) 制限時間を超えた場合、処理を中断し、専用端末Ａ等にメッセージ表示ができること。 (3) 制限時間が変更できること。

	受信要求間隔設定	(1) 各機能の受信要求間隔を設定できること。 (2) 受信要求間隔を変更できること。
	定期抹消設定	定期抹消において、警察BLファイル（APIS）ごとに抹消結果の通知先を設定できること。
	競合情報設定	競合情報の照合において、照合対象の警察BLファイル（APIS）及び通知先を設定できること。
	ヒット情報の条件設定	(1) 警察BLファイル（APIS）ごとに、措置、通知先の所属及び通知内容の設定ができること。 なお、設定内容については、警察庁が別途指示する。 (2) 前項で設定したヒット情報の条件について、条件の追加、訂正及び削除ができること。 (3) 通知先の代行設定状態により、ヒット通知を制御する設定ができること。
	照合・照会条件の設定	照合・照会条件の設定及び変更が警察BLファイル（APIS）ごとにできること。 なお、照合・照会条件の詳細については、警察庁が別途指示する。
	ホスト情報等登録結果	(1) 警察BLDB（APIS）にホスト情報等の登録結果を管理端末Ａに表示できること。 (2) 警察BLDB（APIS）にホスト情報等の登録において異常があった場合、その詳細を管理端末Ａに表示できること。
	法務省への警察BL（APIS）転送設定	(1) 警察BLファイル（APIS）ごとに、転送の設定ができること。 なお、設定内容の詳細については警察庁が別途指示する。 (2) 転送結果の確認ができること。 (3) 警察BLファイル（APIS）ごとに、登録、更新及び削除を選択し、警察BL（APIS）が転送できること。
	法務省間機能の開始・停止設定	(1) APIS（法務省）間の機能である警察BL（APIS）転送及び照合結果通知の開始・停止を設定できること。 (2) APIS（法務省）と業務サーバの接続状況を管理端末Ａから確認できること。 なお、接続状況の確認方法については警察庁が別途指示する。
	抽出サーバ間機能の開始・停止設定	(1) 抽出サーバ間の機能であるホスト情報（APIS）の取得の開始・停止を設定できること。 (2) 取得機能の状態を管理端末Ａから確認できること。 なお、確認方法については警察庁が別途指示する。

ユーザ情報	認証	(1) 専用端末Ａ等に接続した生体認証装置による生体情報の取得及び送信等を制御できること。 (2) ユーザの認証情報を、端末Ａプログラムから受信できること。 (3) 受信したユーザの認証情報から、ユーザの照合ができること。 (4) 認証が認められた場合、対応するユーザ情報をWebサーバから取得できること。 (5) 取得したユーザ情報から、APISプログラムにログインできること。 (6) 取得したユーザ情報から、業務ごとにアクセス権の制御を行うこと。 (7) 認証が認められなかった場合、再度認証を行い、一定回数認証が認められなかった場合には、当該ユーザからの認証要求について、解除するまで受け付けないこと。 なお、受け付けなくなるまでの認証の回数については、警察庁が別途指示する。

(4)　BICSプログラムの機能は、表－６のとおりとする。

表－６　BICSプログラムの機能

区　分	項　目	機　　能
BICSプログラム共通機能	通信制御機能	(1) BICS（法務省）間通信制御 BICS（法務省）とファイル転送、法務省ヒット情報（BICS）のデータ通信を制御できること。 (2) 専用端末Ａ等通信制御 専用端末Ａ等と照会、回答、ヒット通知のデータ通信を制御すること。 (3) データ交換装置間通信制御 データ交換装置とデータ通信を制御できること。 (4) 冗長構成を用いた業務継続 装置異常時に、冗長構成の機器である業務サーバ、Webサーバを利用して業務の継続ができること。
	入力検査	(1) 専用端末Ａ等から入力された照会のデータについて、検査すること。 なお、検査の詳細については、警察庁が別途指示する。 (2) 検査結果を専用端末Ａ等に表示すること。 なお、表示の詳細については警察庁が別途指示する。

	件数カウント	(1) 登録、照会、回答、ヒット通知の件数をカウントすること。 (2) カウントした件数を専用端末Ａ等に表示できること。 　なお、表示の詳細については警察庁が別途指示する。
	処理確認	処理が完了した場合、その結果を専用端末Ａ等に表示できること。 なお、表示の詳細については警察庁が別途指示する。
転送データ（BICS）登録	取得	転送データ（BICS）を、抽出サーバからデータ交換装置を介して、FTPにより取得すること。 なお、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。
	登録	(1) 抽出サーバから取得した転送データ（BICS）を警察BLDB（BICS）に登録すること。 (2) 転送データ（BICS）が警察BLDB（BICS）に既に登録済みの場合、警察BLDB（BICS）から登録済みの転送データ（BICS）を削除し、新たに取得した転送データ（BICS）を警察BLDB（BICS）に登録すること。
	登録結果通知	(1) 警察BLDB（BICS）に転送データ（BICS）が登録できた場合、登録の完了、登録件数、処理日時等を管理端末Ａに通知すること。 　なお、通知する内容の詳細については、警察庁が別途指示する。 (2) 警察BLDB（BICS）に転送データ（BICS）が登録できなかった場合、登録の失敗、処理日時等を管理端末Ａに通知すること。 　なお、通知する内容の詳細については、警察庁が別途指示する。
	処理時間制限	転送データ（BICS）の登録処理が制限時間を超えた場合、管理端末Ａへ通知すること。 なお、制限時間及び通知内容の詳細については、警察庁が別途指示する。
警察BL(BICS)の転送	抽出	(1) 警察BLDB（BICS）から転送用の警察BL（BICS）を自動抽出すること。 　なお、自動抽出方法、抽出時期、抽出ファイル、抽出項目等については、警察庁が別途指示する。 (2) 自動抽出した転送用の警察BL（BICS）について、警察BLDB（BICS）とは別に保存できること。 (3) 抽出した転送用の警察BL（BICS）に全体で一意と

		なる一連番号を生成し付与すること。 なお、付与する一連番号の体系については警察庁が別途指示する。 (4) 任意の時刻に管理端末Ａを用いて手動で抽出ができること。 (5) 管理端末Ａから抽出する警察BLファイル（BICS）の選択ができること。 (6) 抽出結果の確認ができること。 なお、抽出結果の確認方法については、警察庁が別途指示する。
	検査	警察BLDB（BICS）から転送用の警察BL（BICS）を抽出する際には、抽出する項目について、必須項目及び任意項目の検査、項目の属性等を検査すること。
	転送用データへの変換	検査が完了した転送用の警察BL（BICS）は、BICS（法務省）に転送するデータに変換すること。 なお、転送用データの詳細については、警察庁が別途指示する。
	転送	(1) 変換した転送用データは、BICS（法務省）に自動転送すること。 (2) BICS（法務省）から転送結果を受信すること。 (3) 任意の時刻に管理端末Ａを用いて手動で転送を実行できること。 (4) 管理端末Ａから手動転送／自動転送／転送停止の切替の操作ができること。 (5) 転送結果を、管理端末Ａで確認ができること。 なお、転送結果の確認方法については、警察庁が別途指示する。 (6) 管理端末Ａから転送に関する履歴が管理できること。
	表示	(1) 転送処理過程、転送結果等については、転送日時、件数等の内容を管理端末Ａに表示できること。また、警察BL（BICS）の転送処理が正常に終了しなかった場合、前記のほか、異常であった旨の通知、警報装置の鳴動等ができること。 なお、転送日時、件数等の詳細については、警察庁が別途指示する。 (2) 転送に関する履歴が管理端末Ａに表示できること。
ヒット受信	ヒットの受信	(1) BICS(法務省)から、ヒット通知にかかる存否確認を自動受信できること。

		なお、存否確認の詳細については警察庁が別途指示する。 (2) 存否確認の内容から、警察BLDB(BICS)を検索すること。 (3) (2)の検索の結果を、BICS(法務省)に通報依頼理由として通知すること。 なお、通知の詳細については、警察庁が別途指示する。 (4) (3)の通知の後に送信される法務省ヒット情報(BICS)を、自動受信できること。 なお、法務省ヒット情報(BICS)の詳細については警察庁が別途指示する。
ヒット通知	ヒット通知	(1) 法務省ヒット情報(BICS)の受信後、ヒット通知先設定に従いヒット通知を行うこと。 (2) メインメニュー画面からヒット通知先及びヒット通知の代行先を、専用端末Aで表示できること。
	照合結果表示	(1) 法務省ヒット情報(BICS)を管理端末Aに表示できること。 なお表示内容の詳細については、警察庁が別途指示する。 (2) ヒット通知機能の処理中に異常が見られた場合、管理端末A及び警報装置に通知すること。 なお、通知内容の詳細については、警察庁が別途指示する。
	警報装置制御	(1) ヒット通知先設定に従って、警報装置を鳴動させること。 なお、警報装置の鳴動の詳細については、警察庁が別途指示する。 (2) 警報装置の鳴動を確認すること。 (3) (2)ののち、警報装置の鳴動が停止されたことを確認すること。 (4) (2)及び(3)の確認の結果を管理端末に通知すること。 なお、確認内容及び通知の詳細については、警察庁が別途指示する。
ヒット通知一覧	登録	法務省ヒット情報(BICS)及び該当する警察BL(BICS)をデータベースに保存すること。
	ヒット通知一覧	法務省ヒット情報(BICS)及び該当する警察BL(BICS)をデータベースから、ヒット通知一覧を抽出すること。 なお、ヒット通知一覧の詳細については、警察庁が

		別途指示する。
	画像変換	専用端末Ａで法務省ヒット情報(BICS)及び該当する警察BL（BICS）の画像を、専用端末Ａで表示できる画像形式に変換すること。 なお、画像形式の詳細については、警察庁が別途指示する。
	表示	(1) 業務プログラムにログインすることなく、専用端末Ａで、ヒット通知一覧を確認できること。また、ヒット通知一覧から法務省ヒット情報(BICS)の詳細を確認する場合は、ユーザ認証を行うこと。 なお、確認内容については、警察庁が別途指示する。 (2) 業務プログラムにログインにしている場合、専用端末Ａで、ヒット通知一覧及び法務省ヒット情報(BICS)の詳細を表示できること。 なお、表示方法及び表示内容の詳細については、警察庁が別途指示する。
ヒット通知の代行	設定	(1) 代行元の専用端末Ａで代行設定することにより、代行先の専用端末Ａにおいてもヒット情報（BICS）が表示されること。 (2) 代行元の専用端末Ａで代行設定することにより、代行先の警報装置の鳴動等を制御できること。 (3) 代行設定及び解除は、手動で設定する方法及び期間、時間及び日付を設定することにより自動で設定する方法で行えること。また、期間にあっては複数設定可能であること。 （4）代行設定は、全ての所属のユーザーが設定できること。 (5) 管理端末Ａから、全ての専用端末Ａの代行設定期間を一括して設定できること。また、専用端末Ａは、一括して設定した代行設定期間を変更できること。
	表示	(1) 代行元の専用端末Ａ ア　代行されている旨を専用端末Ａに表示できること。 イ　代行設定を行った所属について、専用端末Ａで確認ができること。 ウ　ログインすることなく代行状態を確認できること。 エ　確認方法及び表示の詳細については警察庁が別途指示する。

		(2) 代行先の専用端末A ア　代行された旨を専用端末Aに表示できること。 イ　代行元の専用端末Aの代行状態に関する所属の情報を専用端末Aに表示できること。 ウ　代行設定が解除された場合、解除された旨を専用端末Aに表示できること。 エ　表示の詳細については警察庁が別途指示する。
	代行先の警報装置制御	代行元の警報装置と同等の制御ができること。
他システムへの照会	データ取込み	(1) スキャナ又は電磁的記録媒体から、照会画像及び添付画像の読込みができること。 なお、画像の解像度及び形式等については、警察庁が別途指示する。 (2) 読込んだ照会画像の切り出し処理等ができること。 なお、切り出し位置、寸法等については、警察庁が別途指示する。 (3) 読込んだ照会画像を、警察庁が別途指示する画像形式及び専用端末Aで表示できる画像形式に変換できること。 なお、専用端末Aに表示する画像形式については、警察庁と別途協議すること。 (4) 変換した照会画像を、専用端末Aに表示できること。
	照会1	(1) 他システムに照会するデータを専用端末Aから1件単位で入力できること。 なお、入力データの詳細については警察庁が別途指示する。 (2) 入力検査の結果が正常であった場合、他システムに対して照会画像及び照会に必要なデータが送信できること。 (3) 他システムからの回答データの有無を一定間隔で確認し、回答データが受信できること。 (4) 回答データの結果を一定期間保存できること。 なお、一定期間の詳細については、警察庁が別途指示する。 (5) 他システムの詳細については、警察庁が別途指示する。
	照会2	(1) 他システムに照会するデータを専用端末Aから1件単位で入力できること。 なお、入力データの詳細については警察庁が別途

		指示する。 (2) 入力検査の結果が正常であった場合、他システムに対して照会画像、添付画像及び照会に必要なデータが送信できること。 (3) 他システムからの回答データの有無を一定間隔で確認し、回答データが受信できること。 (4) 回答データの結果を一定期間保存できること。 なお、一定期間の詳細については、警察庁が別途指示する。 (5) 他システムの詳細については、警察庁が別途指示する。
	画像変換	専用端末Ａで照会結果を表示する際には、警察庁が別途指示する画像形式を、専用端末Ａで表示できる画像形式に変換すること。 なお、画像形式の詳細については、警察庁が別途指示する。
	表示	(1) 照会した結果を専用端末Ａに表示できること。 なお、表示する画像形式については、警察庁と別途協議すること。 (2) 照会２の結果については、照会結果の印刷ができること。 なお、表示する画像形式については、警察庁と別途協議すること。 (3) 照会過程、処理結果等について、処理日時、端末名、処理件数等の内容を管理端末Ａに表示できること。また、処理が正常に終了しなかった場合、異常であった旨の通知、警報装置の鳴動等ができること。 なお、処理日時、処理件数等の詳細については、警察庁が別途指示する。
	注意喚起	他システムに照会するデータを送付する前に、専用端末Ａに注意喚起を促すメッセージを表示すること。
	アクセスログ参照	アクセス権に応じてアクセスログの参照ができること。
試験	試験環境	(1) 運用環境と同等の機能が確認できる試験環境を構築できること。 なお、試験環境は運用環境で使用するものとは別に作成し、運用環境に影響を与えないこと。 (2) BICS(警察)の単独での試験環境とは別に、BICS(法務省)と接続した試験環境を構築できること。 (3) 試験環境は専用端末Ａ等と接続ができること。ま

		た、試験接続は、専用端末Ａ等ごとに設定ができること。 (4) 試験中は専用端末Ａ等に試験中であることを明示すること。
	試験機能	作成した試験データで、BICSプログラムの機能が確認できること。
メンテナンス	ログ出力設定	専用端末Ａ等ごと及びアクセス権ごとに、出力できるログの種類及び出力内容を設定できること。 なお、ログの種類及び出力内容の詳細については警察庁が別途指示する。
	試験環境設定	(1) 専用端末Ａ等ごとに試験環境に接続する設定ができること。 (2) 試験環境へ接続している専用端末Ａ等の情報が一覧で表示できること。 なお、一覧表示の詳細については警察庁が別途指示する。 (3) 試験データ（照会、ヒット通知）の作成及び編集ができること。 (4) 試験データの情報が一覧で表示できること。 なお、一覧表示の詳細については警察庁が別途指示する。 (5) 運用環境と試験環境でコードの同期がとれること。
	警察BL(BICS)等内容確認	(1) 抽出サーバ（BICS）で登録された転送用の警察BL（BICS）から取得した転送データ（BICS）の内容を、日時又は期間を指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。 (2) 専用端末Ａ等から照会入力された転送用の照会データの内容を、日時又は期間を指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。 (3) 警察BLDB（BICS）に登録されている警察BL（BICS）の内容を、一連番号又は全てを指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。
	変換テーブル等メンテナンス	(1) コード変換テーブルの更新ができること。 なお、変換テーブルは警察庁からデータを提供することとし、変換が必要なデータ、変換方法、変換

		タイミング等の詳細については、警察庁が別途指示する。 (2) 運用環境と試験環境でコードの同期がとれること。
	ヒット通知先設定	警察BLファイル（BICS）ごとのヒット通知先の所属を変更できること。
	法務省間機能の開始・停止設定	(1) BICS（法務省）間の機能である警察BL（BICS）転送及び法務省ヒット通知の開始・停止を設定できること。 (2) BICS（法務省）と業務サーバの接続状況を管理端末Aから確認できること。 なお、接続状況の確認方法については警察庁が別途指示する。
	抽出サーバ間機能の開始・停止設定	(1) 抽出サーバ間の機能である登録データ（BICS）の取得の開始・停止を設定できること。 (2) 取得機能の状態を管理端末Aから確認できること。 なお、状態の確認方法については警察庁が別途指示する。
ユーザ情報	認証	(1) 専用端末A等に接続した生体認証装置による生体情報の取得及び送信等を制御できること。 (2) ユーザの認証情報を、端末Aプログラムから受信できること。 (3) 受信したユーザの認証情報から、ユーザの照合ができること。 (4) 認証が認められた場合、対応するユーザ情報をWebｻｰﾊﾞから取得できること。 (5) 取得したユーザ情報から、BICSプログラムにログインできること。 (6) 取得したユーザ情報から、業務ごとにアクセス権の制御を行うこと。 (7) 認証が認められなかった場合、再度認証を行い、一定回数認証が認められなかった場合には、当該ユーザからの認証要求について、解除するまで受け付けないこと。 なお、受け付けなくなるまでの認証の回数については、警察庁が別途指示する。

(5)　端末Aプログラムの機能は、表－7のとおりとする。

表－7　端末Aプログラムの機能

区　分	項　目	機　　能
共通	通信制御機	APISプログラムの制御下で、登録、照会、回答、ヒ

	能	ット通知のデータ通信を行うこと。
ユーザ管理	管理	(1) ユーザ情報の登録、訂正及び削除を一件単位で入力できること。 (2) ユーザ情報の登録は、電磁的記録媒体により一括して入力できること。 (3) ユーザの新規登録、訂正登録及び削除登録では、ユーザ情報と生体情報を関連付けて登録ができること。 (4) 登録した結果を表示できること。 なお、表示の詳細は警察庁が別途指示する。
	認証	(1) 生体情報又はその他の情報が取得できること。 なお、その他の情報については警察庁と協議すること。 (2) 取得したユーザの生体情報含む認証要求を、Webサーバに送信できること。 (3) (2)の認証要求に応じたアクセス権を取得できること。 (4) (3)で取得したアクセス権に対応した業務プログラムにログインできること。
Web機能	Web機能	(1) 専用端末Ａ等のOSで安定稼働すること。 (2) 業務用プログラムに対応すること。 (3) SSL／TLSにより暗号化し、HTTPSによるデータの送受信が行えること。
APIS登録ツール	端末登録用ファイルの作成	(1) 警察BLファイル（APIS）の種別ごとに入力ができること。 なお、警察BLファイル（APIS）の種別については、警察庁が別途指示する。 (2) 表形式（エクセル形式）のインタフェースにより、項目ごとに警察BL（APIS）の入力ができること。 (3) エクセル形式及びCSV形式のファイルを読込み、(2)のインタフェースにより、警察BL（APIS）の訂正・削除ができること。 (4) 入力検査を行い、検査結果を表示すること。 なお、検査の詳細については、警察庁が別途指示する。 (5) (4)の入力検査が正常であった場合、入力した警察BL（APIS）をAPISプログラムが取り扱う登録用ファイルに変換すること。 なお、変換方法については警察庁と協議して決定すること。

		(6) 複数件の警察BL（APIS）を、一つの登録用ファイルに一括して変換できること。 なお、変換方法については警察庁と協議して決定すること。
	訂正・削除用ファイルの作成	(1) 警察BLファイル（APIS）の種別ごとに入力ができること。 なお、警察BLファイル（APIS）の種別については、警察庁が別途指示する。 (2) 表形式（エクセル形式）のインタフェースにより、項目ごとに警察BL（APIS）の入力ができること。 (3) エクセル形式及びCSV形式のファイルを読込み、項目ごとに警察BL（APIS）の訂正・削除ができること。 (4) 警察BL（APIS）照会で出力した照会結果ファイルの読込み、その内容の表示、編集ができること。 (5) 訂正の場合、項目ごとに訂正ができること。 (6) 削除の場合、一連番号を指定して削除できること。 (7) 入力検査を行い、検査結果を表示すること。 なお、検査の詳細については、警察庁が別途指示する。 (8) (7)の入力検査が正常であった場合、訂正及び削除した警察BL（APIS）をAPISプログラムが取り扱う訂正削除用ファイルに変換すること。 なお、変換方法については警察庁と協議して決定すること。 (9) 複数件の警察BL（APIS）を一つの訂正削除用ファイルに一括して変換できること。 なお、変換方法については警察庁と協議して決定すること。
	ヒット情報の条件の反映	警察BL（APIS）のヒット通知の通知先について、1件単位及び複数件を一括で反映できること。 なお、ヒット通知先の情報については警察庁が別途指示する。
	日本語、中国語及び韓国語変換	(1) 日本語から中国語（簡体字、繁体字）、ピンイン及び統一読みへの変換ができること。 (2) 中国語（簡体字）から日本語、中国語（繁体字）、ピンイン及び統一読みへの変換ができること。 (3) 中国語（繁体字）から日本語、中国語（簡体字）、ピンイン及び統一読みへの変換ができること。 (4) 日本語から韓国語（ハングル文字）及び韓国語（ローマ字）への変換ができること。

		(5) 韓国語（ハングル文字）から日本語及び韓国語（ローマ字）への変換ができること。 (6) 統一読みへの変換テーブルについては、警察庁が官給する、3.3.56「中国語漢字読み方辞典」の電子データをもとに作成すること。 (7) (6)以外の変換テーブルについては、警察庁が保有する変換テーブルをデータで提供する。 (8) 当該機能の一部又は全部を、端末装置以外の機器に持たせる場合には、実現方法について警察庁と協議の上、他のプログラムと相互に影響を与えないこと。
	コード更新	APISプログラムから出力したファイルを取り込むことにより、国名等のコードを更新できること。 なお、更新を行うコードの種類については、警察庁が別途指示する。
セキュリティ	安全対策	(1) 業務起動中、一定時間操作されなかった場合、スクリーンロックができること。また、キーボード操作により、任意にスクリーンロックができること。 (2) スクリーンロックの設定及び解除の時間が設定できること。 (3) スクリーンロック起動中、認証又はキーボード操作により、スクリーンロックが解除できること。 (4) スクリーンロック起動中において、指定した時間内に認証による解除がされない場合又はキーボード操作によりスクリーンロックを解除した場合は、業務を強制終了し、使用中のデータを、専用端末Ａ等の一時使用領域から自動で消去すること。また、強制終了を行う時間は１分単位で設定できること。
	データ消去	業務で使用したデータは、業務用プログラムを終了した時、専用端末Ａ等の一時使用領域から自動で消去すること。

(6)　端末Ｂプログラムの機能は、表－８のとおりとする。

表－８　端末Ｂプログラムの機能

区　分	項　目	機　　能
共通	通信制御機能	抽出プログラムの制御下で、登録のデータ通信を行うこと。
ユーザ情報	管理	(1) 入力された生体情報を、アクセス権管理システムに登録されたユーザ情報と関連付けて登録ができること。

		(2) 登録した結果が表示できること。 なお、表示の詳細は警察庁が別途指示する。
	認証	(1) 生体情報又はその他の情報等、ユーザの認証情報が取得できること。 なお、その他の情報については警察庁と協議すること。 (2) 取得したユーザの認証情報含む認証要求を、抽出サーバに送信できること。 (3) (2)の認証要求に応じたアクセス権を取得できること。 (4) (3)で取得したアクセス権に対応した業務プログラムにログインできること。
Web機能	Web機能	(1) 専用端末Ｂ等のOSで安定稼働すること。 (2) 業務用プログラムに対応すること。 (3) SSL／TLSにより暗号化し、HTTPSによるデータの送受信が行えること。
セキュリティ	安全対策	(1) 業務起動中、一定時間操作されなかった場合、スクリーンロックすること。また、キーボード操作により、任意にスクリーンロックができること。 (2) スクリーンロックの設定及び解除の時間が設定できること。 (3) スクリーンロック起動中、認証又はキーボード操作により、スクリーンロックが解除できること。 (4) スクリーンロック起動中において、指定した時間内に認証による解除がされない場合又はキーボード操作によりスクリーンロックを解除した場合は、業務を強制終了し、使用中のデータを、専用端末Ｂ等の一時使用領域から自動で消去すること。また、強制終了を行う時間は１分単位で設定できること。
	データ消去	業務で使用したデータは、業務用プログラムを終了した時、専用端末Ｂ等の一時使用領域から自動で消去すること。

4.1.2 性能要件

サーバ用プログラムの性能は、表－９のとおりとする。

なお、レスポンスは業務トランザクションが集中する午前６時から午後７時までの間におけるものとする。

表－９ サーバ用プログラムの性能

機　能	項　目	機能概要	レスポンス
事前旅客情	登録	専用端末Ａからの要求により、業務	平均３秒以内／件

報照合業務機能		サーバに新規登録、訂正登録及び削除登録を行い、処理結果を専用端末Ａに送信する。	最大10秒以内／件
	照会（他システムへの照会を除く。）	専用端末Ａからの要求により、業務サーバから回答結果を専用端末Ａに送信する。	平均５秒以内／件 最大60秒以内／件
	ヒット通知	法務省ヒット情報（APIS）を受信し、ヒット通知を専用端末Ａに送信する。	平均60秒以内 最大90秒以内
	ヒット通知一覧	専用端末Ａからの要求により、業務サーバからヒット通知一覧を専用端末に送信する。	平均３秒以内／件 最大10秒以内／件
外国人個人識別情報認証業務機能	登録	専用端末Ｂからの要求により、抽出サーバに新規登録、訂正登録及び削除登録を行い、処理結果を専用端末Ｂに送信する。	平均５秒以内／件 最大10秒以内／件 （警察庁指掌紋システムの処理時間を除く。）
	ヒット通知	法務省ヒット情報（BICS）を受信し、ヒット通知を専用端末Ａに送信する。	平均60秒以内 最大90秒以内
	ヒット通知一覧	専用端末Ａからの要求により、業務サーバからヒット通知一覧を専用端末Ａ等に送信する。	平均３秒以内／件 最大10秒以内／件

4.1.3　マンマシン・インタフェース

(1)　サーバ、端末等間のマンマシン・インタフェースはWebブラウザによるGUIとすること。

(2)　プログラムの処理ができない場合、端末等にメッセージを出力すること。

(3)　WebブラウザからURLを指定してプログラムを呼び出しても業務を行えないこと。

(4)　ツールバー及びメニューの表示を画面ごとに制御し、URLを非表示とすること。

(5)　ウインドウ切替時等にクリップボードをクリアすること。

(6)　ログイン中の各画面において、コピー機能並びにマウスの右クリックを禁止すること。

(7)　ハードコピー機能を禁止すること。

(8)　前項(5)から(7)のほか、業務で使用する操作以外の機能を禁止すること。

(9)　ログイン中のユーザ情報を常に画面に表示できること。

(10)　端末等の電源停止中も、警報装置によるヒット通知の受信ができること。

(11)　項目間の移動は、マウスによる操作に加え、タブ及びショートカットメニューによりキーボードで行えること。

(12) 入力項目に指定桁数のデータを入力した場合、次入力項目にカーソルを移動すること。

なお、指定桁数については、警察庁が別途指示する。

(13) データの誤入力を避けるため、コンボボックス、ラジオボタン、チェックボックス等による選択入力を用いること。

(14) コンボボックス等を使用する場合は、直接入力及び選択入力の両方が実行可能であること。

(15) 入力項目ごとに入力文字種に応じた入力モードに自動切替を行うこと。

(16) 入力したデータを「クリア」ボタンで初期値に戻すことができること。

(17) 入力したデータを画面遷移時に記憶し、前画面に戻った場合にも表示すること。

(18) 一覧表示において、任意の項目をクリックすることにより、その項目をキーとして昇順又は降順に並べかえることができること。

(19) 次の場合、画面上の文字等を区別して表示すること。

ア　使用できるボタン等及び使用できないボタン等

イ　アクセスできるファイル名及びアクセスできないファイル名

ウ　一覧表で選択した項目及び未選択の項目

エ　入力項目の必須及び任意並びに誤入力項目

4.1.4　サーバ、端末等間インタフェース

Webサーバと端末等間のWebインタフェースを用いた通信は、SSL／TLSにより暗号化し、HTTPSによるデータの送受信が行えること。

4.1.5　保守性

(1)　業務ごとに起動・停止ができること。

(2)　警察庁が別途指示する範囲で、業務及び機能ごとの閉塞・解除ができること。

4．2　画面要件

画面遷移、画面イメージ及び入出力仕様については、警察庁が別途指示する。

4．3　帳票要件

警察庁が別途指示する。

4．4　情報・データ要件

警察庁が別途指示する。

4．5　外部インタフェース要件

外部システムとのインタフェース要件については、警察庁が別途指示する。

なお、使用するプロトコルについては、次のとおりである。

4.5.1　APIS（法務省）間

(1)　警察BL（APIS）の転送については、FTP／SMTP／POP3とする。

(2)　警察庁、法務省間の通知等については、SMTP／POP3とする。

4.5.2　BICS（法務省）間

(1)　警察BL（BICS）の転送については、FTP／HTTPとする。

(2)　警察庁、法務省間の通知等については、HTTPとする。

4.5.3　その他の外部システム

(1)　中継サーバ間の転送については、FTPとする。

(2)　警察庁指掌紋システム間の転送については、RCPとする。

(3)　アクセス権管理システム間の転送については、LDAPとする。

(4)　他システム間の照会(APIS)については、SMTP／POP3とする。

(5)　他システム間の照会(BICS)については、FTP／HTTPとする。

5　規模要件

5．1　APIS（警察）業務データ量

APIS（警察）業務データ量(予測最大値)を表－10に示す。

表－10　APIS（警察）業務データ量(予測最大値)

情報・データ名	初期データ (件)	年間件数 (件)	最大データ量 (byte/件)
警察BL（APIS）登録	600,000	25,000	20,000
ヒット情報登録		20,000	25,000
警察BL（APIS）照会		10,000	20,000
ヒット情報照会		25,000	25,000
他システム(APIS)照会		20,000	25,000
照合結果通知受信		150,000	25,000
ヒット通知		60,000	25,000

5．2　BICS（警察）業務データ量

BICS（警察）業務データ量(予測最大値)を表－11に示す。

表－11　BICS（警察）業務データ量(予測最大値)

情報・データ名	初期データ (件)	年間件数 (件)	最大データ量 (byte/件)
警察BL（BICS）登録	30,000	5,000	1,000(文字情報) 5,000,000(画像情報)
他システム（BICS）への照会１		25,000	1,000(文字情報) 5,000,000(画像情報)
他システム（BICS）照会回答１		25,000	1,000(文字情報) 5,000,000(画像情報)
他システム（BICS）への照会２		15,000	1,000(文字情報) 5,000,000(照会情報) 300,000(添付画像)
他システム（BICS）照会回答２		15,000	1,000(文字情報) 5,000,000(画像情報)
ヒット通知		50	3,000(文字情報) 1,000,000(画像情報)

５．３　アクセス数

現行システムから算出したアクセス数（概算値）の一覧を表- 12に示す。

表- 12　APIS（警察）及びBICS（警察）におけるアクセス数（概算値）

業務の区分	アクセス数	
	平均(件／日)	総数(件／年)
APIS（警察）	400	150,000
BICS（警察）（登録）	10	3,500
BICS（警察）（照会、ヒット）	10	3,500

５．４　端末台数

専用端末Ａ等　96台

専用端末Ｂ等　５台

５．５　利用者数

専用端末Ａ等　4,000名

専用端末Ｂ等　100名

５．６　現行システムの構成、性能及び機能

関連仕様書を参照すること。

6　信頼性等要件

６．１　信頼性要件

6.1.1　可用性

ソースコードを変更することなくパラメータによるプログラムの設定変更が可能なコーディング、冗長構成の機器による運用、その他業務の継続運用に影響を与えない手法により、可用性を確保したプログラム設計を行うこと。

6.1.2　完全性

取り扱うデータに応じた記憶領域の確保その他データ処理時におけるデータ欠損発生を防止する手法により､完全性を確保するプログラム設計を行うこと。

6.1.3　機密性

既知の脆弱性を用いないコーディング、各処理ごとのモジュール化その他のデータ漏えいにつながる脆弱性の発生を防止する手法により、高い機密性を確保するプログラム設計を行うこと。

６．２　拡張性要件

6.2.1　データの追加及び変更並びに機能の追加及び変更に容易に対応できるよう、設計・開発に当たること。

6.2.2　警察BLDB（APIS)、警察BLDB（BICS)、抽出DB（BICS）及びヒット情報DB（APIS）で取り扱うデータ項目の追加及び削除並びに参照するデータベースの追加及び削除が容易にできるよう、設計・開発を行うこと。

6.2.3　画面の追加・修正に容易に対応できるよう、設計・開発を行うこと。

6.2.4　旅客情報のデータ項目の追加等、法務省システムの拡張性に容易に対応できるよう、設計・開発を行うこと。

６．３　システム中立性要件

特定の事業者にしか取り扱うことができない製品や技術に依存せず、他事業者が、システムの改修を引き継ぐことが可能であること。

６．４　事業継続性要件

4.1.5項参照。

7　情報セキュリティ要件

権限要件は以下のとおりとする。

７．１　警察庁が別途指示する利用者ごとに付与する権限に基づき、機能別、ファイル別に情報システムに対するアクセスを制御できること。

７．２　ログの管理等の情報セキュリティの機能により、情報の漏えい、改ざん、消去の防止及び情報システムのセキュリティ確保ができること。

8　情報システム稼働環境

８．１　全体構成

ハードウェア仕様書を参照すること。

８．２　ハードウェア構成

警察庁がハードウェア仕様書で調達する機器の構成並びに構成機器の機能及び性能の詳細について、契約後に速やかに警察庁と協議を行い、決定すること。ただし、６．３項に示すシステム中立性要件を損なわないこと。

８．３　ソフトウェア構成

各装置のOS・ミドルウェアは、ハードウェア仕様書を参照すること。

８．４　ネットワーク環境

8.4.1　通信プロトコル

TCP／IPとする。

8.4.2　IPアドレス体系

警察庁が別途指示する。

８．５　アクセシビリティ要件

4.1.3項参照。

9　テスト要件定義

９．１　テスト要件

9.1.1　警察庁と協議を行い、「政府情報システムの整備及び管理に関する標準ガイドライン」（平成26年12月３日各府省情報化統括責任者（CIO）連絡会議決定）（以下「ガイドライン」という。）に基づき、契約業者が社内環境において実施する単体・結合テスト（以下「契約業者単体・結合テスト」という。）及び警察庁環境において実施する総合テスト（以下「契約業者総合テスト」という。）のテスト計画書を作成し、警察庁の承認を得ること。

9.1.2　テスト計画書に基づき、テストを行い、各テストの実施結果を報告すること。なお、契約業者単体・結合テスト及び契約業者総合テストに必要なデータは、

契約業者が準備すること。

9.1.3　警察庁が行う結合テスト及び総合テスト（以下「受入テスト」という。）については、次のとおり実施する。

(1)　結合テスト

ア　警察庁設置機器のみを用いた警察システムの単独試験及び警察システムと外部システムとの連携試験を行う。

イ　結合テストに必要なデータは、警察庁が準備する。

ウ　単独試験は、平成30年10月から11月までの間に実施する。

エ　連携試験は、平成30年10月から平成31年２月までの間に実施し、テスト期間中に、外部システムごとの連携試験を数回行う。

なお、法務省システムとの連携試験にあっては、一部テストを夜間深夜時間帯に実施する。

(2)　総合テスト

ア　警察庁設置機器及び都道府県設置の専用端末等を用いた、警察システムのテストを行う。

イ　法務省システムと連携したテストは行わない。

ウ　総合テストに必要なデータは、警察庁が準備する。

エ　平成30年12月から平成31年1月までの間、週２回のテストを行う。

9.1.4　契約業者は警察庁と協議を行い、ガイドラインに準じた受入テストのテスト計画書及びテスト仕様書を作成し、警察庁が実施する受入テストを支援すること。また、支援結果を報告すること。

9.1.5　受入テスト中、業務用プログラムに不具合が発生した場合、以下の作業を実施し、結果を報告すること。

(1)　原因調査

(2)　不具合の修正及び修正済み業務用プログラムのインストール

(3)　運用環境及び試験環境における動作試験

9.1.6　テスト実施方法については、表- 13のとおりとする。

表- 13　テスト実施方法

テスト名	実施方法		テスト環境	テスト方法	テストデータの準備
	警察庁	契約業者			
契約業者単体・結合テスト	－	実施	社内環境	・機能テスト ・異常系テスト	契約業者
契約業者総合テスト	協力	実施	運用環境 試験環境	・機能テスト ・異常系テスト ・機能間連携テスト	契約業者
受入テ　結合テスト	実施	支援	運用環境 試験環境	・機能テスト ・異常系テスト ・機能間連携テスト	警察庁

スト	総合テスト	実施	支援	運用環境	・機能テスト ・異常系テスト ・機能間連携テスト	警察庁

9．2　検査

9.2.1　検査は、納入成果物、機能要件及び性能要件について行う。

なお、検査方法及び検査内容については、警察庁と協議すること。

9.2.2　検査は、警察庁と協議の上定める場所において、警察庁検査官が立会いの上行う。

なお、検査方法及び検査内容により、警察庁の設備以外に機器が必要となった場合には、契約業者が準備すること。

9.2.3　検査中に、本仕様書の規定に関して解釈上の疑義が生じた場合は、警察庁検査官の指示に従うこと。

10　移行要件定義

10．1　移行に係る要件

10.1.1　移行実施計画の作成

警察庁と協議を行い、ガイドラインに基づき、新システムへの移行スケジュール、移行方法及び移行後の検証方法を記載した移行計画書を作成し、警察庁の承認を得ること。

なお、現行システムから運用環境への移行作業及び移行後の検証作業は警察庁が実施する。

10.1.2　移行スケジュール

移行は、警察庁結合テスト前、警察庁総合テスト前及び運用開始前の３回とする。

10.1.3　移行方法及び検証方法

警察庁が現行システムから抽出したデータについて、運用環境に移行するツール、移行作業及び検証作業に必要な手順書を作成すること。また、警察庁が実施する移行作業及び検証作業に関して、当該ツールの使用方法の教示など技術的支援を行うこと。

なお、抽出したデータのレイアウトは、警察庁が別途指示する。

10．2　教育に係る要件

警察庁が指示する教育訓練の計画に従い、以下のとおり教育訓練を行い、その結果を報告すること。

10.2.1　開発用ソフトウェアの操作について､以下のとおり教育訓練を実施すること。

(1)　実施方法は集合教育訓練とし、警察庁が指示する東京都23区内の場所において、警察庁に設置された試験端末で実施すること。

(2)　教育訓練は、開発用ソフトウェアの操作について、１日間実施することとし、対象者は警察庁職員約５人とする。

(3)　教育訓練に必要な教材は、契約業者が準備すること。

11　運用要件定義

11．1　情報システムの操作・監視等要件

運用形態は、24時間連続運転稼働とする。

11．2　データ管理要件

13.2.5項参照。

11．3　運用施設・設備要件

システムの設置場所及びその構造、入退室の方法、空調設備、消防設備並びに電力供給設備については、警察庁が別途指示する。

12　保守要件定義

12．1　ソフトウェア保守要件

別途契約を結ぶ。

12．2　ハードウェア保守要件

ハードウェア仕様書を参照すること。

13　作業の体制及び方法

13．1　作業体制

13.1.1　設計・開発実施計画

契約後、警察庁と協議を行い、速やかにガイドラインに基づく作業概要、作業体制、スケジュール、成果物、開発形態・開発手法・開発環境・開発ツール等及びその他に関する事項を記載した設計・開発実施計画書並びにその附属文書であるWBS（Work Breakdown Structure）を作成し、警察庁の承認を得ること。

なお、WBSは作業項目、作業内容及びスケジュールをより詳細に階層化し、担当者等を記載すること。

13.1.2　設計・開発実施要領

契約後、警察庁と協議を行い、速やかにガイドラインに基づくコミュニケーション管理、体制管理、工程管理、品質管理、リスク管理、課題管理、システム構成管理、変更管理及び情報セキュリティ対策に関する事項を記載した設計・開発実施要領を作成し、警察庁の承認を得ること。

13.1.3　体制管理及び品質管理

(1)　本プログラムの設計、開発、テスト及び3.7.1項の関連仕様書により調達するシステムへの導入の各工程において、警察庁の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。

(2)　警察庁の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。第三者機関による品質保証体制を証明する書類等が提出可能な

場合は提出すること。

(3) 本プログラムに警察庁の意図しない変更が行われるなどの不正が見つかった時に、追跡調査や立ち入り検査など、警察庁と連携して原因を調査し、排除するための手順及び体制を整備すること。また、当該手順及び体制が妥当であることを証明するための書類を提出すること。

13.1.4 リスク管理、課題管理及び変更管理

リスク管理簿を作成し、本プログラムの設計・開発における作業を阻害する可能性のあるリスクを適切に管理すること。また、設計・開発において解決すべき問題及び変更内容についても適切に管理・記録すること。

13.1.5 進捗報告等

設計・開発実施計画書及び設計・開発実施要領に基づき設計・開発を行い、原則月２回行う予定の警察庁との定例会議において､その結果を報告すること。また、警察庁と協議を行い、ガイドラインに基づく次の書類を作成し、警察庁に提出すること。

なお、定例会議が行われない場合においても、進捗報告に関する書類は提出すること。

(1) EVM進捗管理表を作成し、定例会議に提出すること。

(2) 前月の進捗状況表、EVM（Earned Value Management）推移グラフ及び進捗状況分析図を作成し、月初めの定例会議に提出すること。

(3) ODB登録用シートに必要事項を記載し、設計・開発実施要領において定める時期に提出すること。

なお、ODB登録用シートの詳細については、警察庁が別途指示する。

(4) 警察庁の求めに応じ、作業の進捗状況等について中間報告を行うこと。

(5) 警察庁と協議した場合は、速やかに議事録を作成し、警察庁の承認を得ること。

13. 2 開発方法

13.2.1 次に示す設計書等は、警察庁と仕様の詳細について調整の上作成し、警察庁の承認を得ること。

(1) プログラム設計書

(2) マスタ移行設計書

(3) 開発環境

(4) 警察庁が指示する以外の通信プロトコル及びアプリケーションレベルの通信インタフェース

13.2.2 次に示す事項は、利用に当たり警察庁と協議し、警察庁の承認を得ること。

(1) 既存開発済み部品の利用

(2) パッケージソフトウェアの利用

(3) 既存納入成果物の利用

13.2.3 本プログラムの作成に当たって次の事項に留意すること。

(1) ソースプログラムには、適宜日本語でコメントを付加すること。

(2) ソースプログラムは、ステートメント（文）の意味に沿った字下げを行う

こと。

(3)　変数等の命名規則を統一すること。

(4)　処理ごとにモジュール化すること。

(5)　データの検査項目は外部パラメータ化し、コードの追加、訂正及び削除時にソースプログラムの変更、再コンパイルの必要がないようにすること。

なお、外部パラメータ化できない項目は事前に警察庁の承認を得ること。

(6)　利用する各種コードは外部パラメータ化し、コードの追加、訂正及び削除時にソースプログラムの変更、再コンパイルの必要がないようにすること。

なお､外部パラメータ化できないコードは事前に警察庁の承認を得ること。

(7)　期間指定、指定日付等の日付に関する定義及び和暦西暦間の対応は外部パラメータ化し、定義の追加、訂正及び削除時にソースプログラムの変更、再コンパイルの必要がないようにすること。

なお、外部パラメータ化できない項目は事前に警察庁の承認を得ること。

(8)　業務ごとにマルチプロセス化すること。

(9)　システム及び業務の運用に影響することなく、プログラムや各種設定の変更が容易にできること。

13.2.4　開発言語等

原則として、Java及びC言語を使用して開発を行うこと。

なお、開発言語及び開発環境については、事前に警察庁の承認を得ること。

13.2.5　データベース

(1)　データのバックアップ及び障害時の復旧においては、データの完全性を確保すること。

(2)　データベースバックアップは、業務を停止せずに行えること。

(3)　ディスクの使用容量については、必要最低限にとどめ数値的な根拠を明確にして設計すること。

(4)　業務で使用するものとは別に試験で使用するデータベースを設けること。

13.2.6　文字コード

使用する文字コードについては、警察庁が別途指示する。また、文字コードの変換が必要な場合には、相互に変換できること。

13.2.7　各種設定変更は、システム及び運用に影響することなく、随時及び容易にできるようにすること。

13．３　導入

13.3.1　本プログラムの導入に当たっては、外部システムの運用に影響を与えることなく構築及び運用ができること。

13.3.2　納入成果物は、平成31年２月28日（木）までに納入すること。

なお、詳細については、警察庁と協議すること。

13.3.3　警察システムの試験環境への業務用プログラムのインストール､必要な設定、調整及びテストについては、平成30年９月28日（金）までに完了すること。

13.3.4　警察システムの運用環境への業務用プログラムのインストール､必要な設定、調整及びテストについては、平成31年２月28日（木）までに完了すること。

13.3.5　13.3.4項に関する全ての設定及び調整が終了し、テストに合格した後、警察庁が別途指示する電磁的記録媒体に警察システムにおける業務用プログラムのバックアップを行い、警察庁に提出すること。

なお、当該作業の実施は、本調達に係る作業範囲に含まれるものとする。また、バックアップの取得時期は警察庁と協議し、バックアップ用の電磁的記録媒体は契約業者が準備すること。

13.3.6　開発用ソフトウェアのインストール、必要な設定及び調整については、警察庁と協議の上、平成31年１月31日までに完了すること。

13.3.7　作業に係る日程の詳細については、警察庁と協議すること。

13.3.8　本作業の実施結果については、報告書を提出すること。

なお、報告書の詳細については、警察庁と協議すること。

13．４　瑕疵担保責任

警察庁は、納入成果物について納入後１か年以内に瑕疵を発見した場合は、契約業者に対して当該瑕疵の修正を請求することができ、契約業者は、当該瑕疵を無償で修正するものとする。

14　特記事項

14．１　知的財産権の取扱い

14.1.1　本調達において納入された成果物に関する権利（著作権法（昭和45年法律第48号）第21条から第28条に定める全ての権利を含む。）及び所有権は、次の物を除き警察庁が契約業者に受領書を交付したときをもって警察庁に移転する。また、契約業者は警察庁に対し、納入成果物に係る著作者人格権（著作権法第18条から第20条に定める権利をいう。）を行使しないものとする。

(1)　納入成果物に、契約業者が本調達の契約前から権利を有する著作物（契約業者が範囲について警察庁の承認を得たものに限る。）（以下「契約業者の既存著作物」という。）が含まれる場合、その契約業者の既存著作物

(2)　納入成果物に、第三者が権利を有する著作物（以下「第三者の既存著作物」という。）が含まれる場合、その第三者の既存著作物

14.1.2　14.1.1(1)項で示した契約業者の既存著作物においては、本システムへ利用する目的の範囲に限り、警察庁は契約業者に権利留保された著作物を自由に複製し、及びそれらの利用を第三者に許諾することができるものとする。ただし、成果物に第三者の権利が帰属するときはこの限りではないものとし、この場合には、複製等ができる範囲やその方法等について協議するものとする。

14.1.3　納入成果物に第三者の既存著作物が含まれている場合は、契約業者は当該既存著作物の使用に必要な費用の負担及び使用許諾に関する一切の手続を行うものとする。この場合、契約業者は使用許諾の内容については、警察庁の承認を得るものとする。

14．２　外部システムとの設定調整等

「13．３　導入」において、警察システムと各外部システム間の接続に係る設定、調整及び試験ついては、警察庁及び各外部システムの担当者と連携して行う

こと。

なお、実施の詳細について、警察庁及び各外部システムの担当者と協議すること。

14．３　その他

14.3.1　納入成果物が他者の権利を侵害していないこと。

14.3.2　プログラムの設計、開発、導入及び調整等に当たり、府省共通ポータル及び法務省システムの間で確認すべき事項等が生じた場合には、全て警察庁と協議すること。

14.3.3　プログラム開発及び試験に必要な機器、ソフトウェア及びテストデータは契約業者において準備すること。

14.3.4　プログラム開発に必要なソフトウェアのサポート契約は契約業者において行うこと。

14.3.5　本仕様書の内容について疑義があるときは、警察庁の指示又は承認を得ること。

14.3.6　警察庁が別途指示する事項については、入札公告期間中に閲覧可能であるため、警察庁に問い合わせること。

14.3.7　プログラムに関して変更が必要となった場合は、警察庁と協議の上対応し、試験を行うこと。

なお、プログラムの変更及び変更後の試験を行った場合は、変更内容、試験結果等を記載した書面を２部提出するとともに、該当する資料及び電磁的記録媒体の変更を行うこと。

14.3.8　納入時に、納入報告書を作成し、提出すること。

14.3.9　全ての作業完了後、完了報告書を提出すること。

なお、完了報告書の詳細については、警察庁と協議すること。

14.3.10　警察庁に提出する資料及び納品物については、日本語に対応していること。

15　妥当性証明

本調達仕様書の妥当性について証す。

警察庁情報通信局情報管理課長（警察庁CIO補佐官）　　降簱　喜和男

１　納入成果物

納入成果物は以下のとおり。

分類	品名	数量	構成
サーバ用プログラム	抽出プログラム	1式	２項「納入成果物の構成（サーバ用プログラム）」のとおり
	APISプログラム	1式	２項「納入成果物の構成（サーバ用プログラム）」のとおり
	BICSプログラム	1式	２項「納入成果物の構成（サーバ用プログラム）」のとおり
端末用プログラム	端末Ａ用プログラム	1式	３項「納入成果物の構成（端末用プログラム）」のとおり
	端末Ｂ用プログラム	1式	３項「納入成果物の構成（端末用プログラム）」のとおり

２　納入成果物の構成（サーバ用プログラム）

サーバ用プログラムの構成の詳細については、以下のとおり。

区分	品　　目	数量	納入方法	記　　事
本体	プログラム	1式	電磁的記録媒体	
添付品	プログラムインストール用品	1式	電磁的記録媒体	(1) プログラムの名称、バージョン及び製造番号を明記すること。 (2) プログラムのソースファイルを含む内容とすること。
	プログラム設計書	1式	書面及び 電磁的記録媒体	次の記述を含む内容とすること。 (1) 機能設計 (2) 環境条件 (3) ユーザインタフェース設計（画面設計、帳票設計、電磁的記録媒体入出力レイアウト） (4) データベース設計 (5) コード設計 (6) 外部インタフェース設計
	プログラム仕様書	1式	書面及び 電磁的記録媒体	プログラム詳細設計を含む内容とすること。
	プログラムリスト	1式	書面及び 電磁的記録媒体	(1) バージョンを明記すること。 (2) モジュール一覧表を含む内容とすること。 (3) ステップ数とその算出基準を含む内容とすること。 (4) ファンクションポイントとその算出基準を含む内容とすること。
	システム構築手順書	1式	書面及び 電磁的記録媒体	次の記述を含む内容とすること。 (1) インストール手順 (2) バックアップ手順 (3) リストア手順
	プログラム操作説明書	1式	書面及び 電磁的記録媒体	次の記述を含む内容とすること。 (1) プロセスフローチャート (2) オペレーションフローチャート (3) メッセージ一覧表 (4) 外部パラメータの変更手順 (5) ハードウェア定期点検時のジョブ保留、スキップ、ジョブ保留解除等手順 (6) データ移行及び検証作業手順
	端末操作説明書	1式	書面及び 電磁的記録媒体	

※電磁的記録媒体の種類、規格及び保存するファイル形式については、警察庁と協議すること。

３　納入成果物の構成（端末用プログラム）

端末用プログラムの構成の詳細は以下のとおり。

区分	品　　目	数量	納入方法	記　　事
本体	プログラム	1式	電磁的記録媒体	
添付品	プログラムインストール用品	1式	電磁的記録媒体	(1) プログラムの名称、バージョン及び製造番号を明記すること。 (2) プログラムのソースファイルを含む内容とすること。
	プログラム設計書	1式	書面及び 電磁的記録媒体	次の記述を含む内容とすること。 (1) 機能設計 (2) 環境条件 (3) 外部インタフェース設計
	プログラム仕様書	1式	書面及び 電磁的記録媒体	プログラム詳細設計を含む内容とすること。
	プログラムリスト	1式	書面及び 電磁的記録媒体	(1) バージョンを明記すること。 (2) モジュール一覧表を含む内容とすること。 (3) ステップ数とその算出基準を含む内容とすること。 (4) ファンクションポイントとその算出基準を含む内容とすること。
	証明関係仕様書	１式	書面及び 電磁的記録媒体	
	システム構築手順書	1式	書面及び 電磁的記録媒体	次の記述を含む内容とすること。 (1) インストール手順 (2) バックアップ手順 (3) リストア手順
	プログラム操作説明書	1式	書面及び 電磁的記録媒体	次の記述を含む内容とすること。 (1) プロセスフローチャート (2) オペレーションフローチャート (3) メッセージ一覧表
	端末操作説明書 （警察庁用）	※式	書面及び 電磁的記録媒体	配分数は別途指示する。
	端末操作説明書 （都道府県警察用）	※式	書面及び 電磁的記録媒体	配分数は別途指示する。
	端末操作説明書 （管理端末・試験端末用）	※式	書面及び 電磁的記録媒体	配分数は別途指示する。

※電磁的記録媒体の種類、規格及び保存するファイル形式については、警察庁と協議すること。

別紙 2

事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書
提出資料等一覧

No	提出資料等		提出予定	
			時期	方法
1	テスト要件	契約業者単体・結合テスト計画書	テストの10営業日前まで	書面
2		契約業者総合テスト計画書	テストの10営業日前まで	書面
3		テスト結果報告書	テスト終了後、5営業日以内	書面
4		受入テスト計画書	受入テストの10営業日前まで	書面
5		受入テスト仕様書	受入テストの10営業日前まで	書面
6		受入テスト支援結果報告書	受入テスト終了後、5営業日以内	書面
7		不具合発生時の作業報告	作業終了後、5営業日以内	書面
8	教育訓練	教育訓練計画書	教育訓練実施の10営業日前まで	書面
9		教育訓練結果報告書	教育訓練実施後、5営業日以内	書面
10	ガイドライン関係	設計・開発実施計画	第1回定例会議終了後、30日以内	書面
11		WBS		書面
12		設計・開発実施要領		書面
13		設計・開発結果報告書	定例会議の開催ごと	書面
14		EVM進捗管理表	定例会議の開催ごと	書面

No	提出資料等		提出予定	
			時期	方法
15	ガイドライン関係	進捗状況表	月初めの定例会議ごと	書面
16		EVM推移グラフ		書面
17		進捗状況分析図		書面
18		移行計画書	移行に係る協議後、30日以内	書面
19		ODB登録用シート	設計・開発実施要領に定める時期まで	書面
20		中間報告書	協議して決定	書面
21		議事録	協議後、5営業日以内	書面
22	承認図書	プログラム設計書	協議して決定	書面
23		マスタ移行設計書		書面
24		開発環境		書面
25		警察庁が指示する以外の通信プロトコル及びアプリケーションレベルの通信インタフェース		書面
26	バックアップ		協議して決定	電磁的記録媒体
27	導入作業実施結果報告書		導入作業実施後、5営業日以内	書面
28	プログラム変更内容及び試験結果		試験実施後、5営業日以内	書面及び 電磁的記録媒体
29	納入報告書		納入時	書面
30	完了報告書		契約履行期限まで	書面

別添２

事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム保守仕様書（案）

警察庁情報通信局情報管理課
平 成 ● 年 ● 月 ● 日 制 定

１　概要

事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラムの保守及び連携する外部システムの更改に伴う接続変更の対応を委託するものである。

２　関連仕様書

２．１　警情仕プロ管第●号「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書」（平成●年●月●日制定）

２．２　警情仕形管第●号「事前旅客情報システム及び外国人個人識別情報認証システム仕様書」（平成●年●月●日制定）

２．３　警情仕形管第38号「アクセス権管理システム仕様書」（平成25年２月１日制定）

２．４　警情仕形管第42号「指掌紋自動識別システム用照合部仕様書」（平成25年４月25日制定）

３　委託期間

平成31年３月１日から平成34年３月31日までとする。

４　対象

事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム

５　対象の運用場所

５．１　サーバ用プログラム

警察庁（東京都23区内の庁舎）

５．２　端末用プログラム

(1)　警察庁（中央合同庁舎２号館及び東京都23区内の庁舎）

(2)　都道府県警察本部（方面本部を含む。）

(3)　警察署等

６　用語の定義

６．１　業務用プログラム

２．１項の関連仕様書により調達したプログラムをいう。

６．２　警察システム

２．２項の関連仕様書により調達したシステムをいう。

６．３　外部システム

警察システムと接続し、業務用プログラムの運用に必要なデータの送受信を行う外部のシステム。２．１項の関連仕様書における警察庁指掌紋システム、アクセス権管理システム及び警察庁ホストシステム並びに法務省システムを指す。

６．４　情報通信部

関東管区警察局情報通信部、東京都警察情報通信部、北海道警察情報通信部及び各府県（方面を含む。）情報通信部を指す。

６．５　ガイドライン

「政府情報システムの整備及び管理に関する標準ガイドライン」（平成26年12月３日付け各府省情報化統括責任者（CIO）連絡会議決定）をいう。

7　委託内容

７．１　保守

7.1.1　障害対応

(1)　契約業者は、24時間対応可能な障害受付ができる窓口を準備すること。

なお、準備する窓口については、２．２項の関連仕様書で定める障害受付窓口と共通とすること。

(2)　警察庁及び情報通信部からの連絡を受けたときには速やかに切り分け作業を行い、障害が発見された場合には、復旧作業を行うこと。また、障害原因を究明し、書面で警察庁に報告すること。

なお、情報通信部からの連絡内容が障害であった場合、警察庁に速やかに報告すること。

(3)　警察庁から技術者の派遣要請があった場合は、３時間以内に技術者の派遣をすること。

(4)　切り分け作業中、業務プログラムに不具合が発見された場合は、不具合を修正するプログラム改修を行うこと。

(5)　不具合を修正するプログラム改修では、運用環境への実施前に、警察庁の試験環境において不具合を修正するプログラムの検証を行うこと。また、作業実施中及び作業実施後において、２．１項の関連仕様書で規定する仕様を満たすことを確認すること。

(6)　(5)項の検証において、異常が見られなかった場合は、運用環境に不具合を修正するプログラム適用を実施すること。

なお、作業完了後、速やかに関連資料の訂正を行い、プログラム改修の作業に利用したインストール媒体とともに、警察庁に提出すること。

7.1.2　ソフトウェアパッチ対応（業務用プログラム）

(1)　業務用プログラムの稼働に必要なミドルウェア及びアプリケーション等のパッケージプログラムについて、それらの開発業者よりパッチのリリースが発表された場合は、速やかに警察庁に報告し、その指示に従うこと。

なお、警察庁に報告したパッチの種類及びその対応について履歴を資料管理し、変更があった場合は警察庁へ最新版の資料を提出すること。

(2)　(1)項で示すパッチを運用環境の業務用プログラムに適用する前に、試験

環境にパッチを適用した上で業務用プログラムの動作検証を行い、不具合発生の有無を確認すること。

(3)　(2)項の検証において、業務用プログラムに不具合が発見されなかった場合は、警察庁に報告した上で、速やかにパッチの適用を行うこと。また、適用作業の結果を報告すること。

(4)　(2)項の検証において、業務用プログラムに不具合が発見された場合は、警察庁に報告した上で、不具合を修正するプログラム改修を行うこと。

(5)　不具合を修正するプログラム改修では、運用環境への実施前に、警察庁の試験環境において不具合を修正するプログラムの検証を行うこと。また、作業実施中及び作業実施後において、２．１項の関連仕様書が示す仕様を満たすことを確認すること。

(6)　(5)項の検証において、異常が見られなかった場合は、運用環境に不具合を修正するプログラム適用を実施すること。また、関連資料の訂正を行い、警察庁に提出すること。

7.1.3　ソフトウェアパッチ対応（警察システム）

(1)　警察システムが調達したOS、パッケージプログラム及びドライバー等のソフトウェアのうち業務用プログラムの稼働に必要なソフトウェアについて、それらの開発業者よりパッチのリリースが発表された場合は、速やかに警察庁に報告し、その指示に従うこと。

　なお、警察庁に報告したパッチの種類及びその対応について履歴を資料管理し、変更があった場合は警察庁へ最新版の資料を提出すること。

(2)　(1)項で示すパッチを運用環境の警察システムに適用する前に、警察システム担当者が試験環境にパッチを適用するので、警察システム担当者と協力して業務用プログラムの動作検証を行い､不具合発生の有無を確認すること。

(3)　(2)項の検証において、業務用プログラムに不具合が発見されなかった場合は、警察庁に報告すること。

(4)　(2)項の検証において、業務用プログラムに不具合が発見された場合は、警察庁に報告した上で、不具合を修正するプログラム改修を行うこと。

(5)　不具合を修正するプログラム改修では、運用環境への実施前に、警察庁の試験環境において不具合を修正するプログラムの検証を行うこと。また、作業実施中及び作業実施後において、２．１項の関連仕様書が示す仕様を満たすことを確認すること。

(6)　(5)項の検証において、異常が見られなかった場合は、運用環境に不具合を修正するプログラム適用を実施すること。また、関連資料の訂正を行い、警察庁に提出すること。

7.1.4　プログラム改修後の対応

(1)　プログラム改修後、サーバ用プログラムのバックアップを行うこと。

(2)　不具合を修正するプログラムのインストール媒体及びインストール手順書を警察庁に提出すること。

　なお、インストール媒体に記録する内容及び作成する時期については、警

察庁と協議すること。

7.1.5　契約業者は、官庁執務時間内（９時30分から18時15分）の技術的な質問に対応できる連絡窓口を設置すること。

７．２　外部システム更改の対応

7.2.1　外部システムの更改に伴う業務用プログラムの接続に必要なIPアドレス等の設定情報の変更及び試験について、警察庁及び外部システムの担当者と協議を行うこと。

7.2.2　協議後、作業計画、作業手順書、試験計画及び試験手順書を提出し、警察庁の承認を得ること。

7.2.3　変更作業は、警察庁及び外部システムの担当者と連携して実施すること。

7.2.4　試験は、警察庁及び外部システムの担当者と連携して実施すること。

なお、試験データについては、警察庁と協力して作成すること。

7.2.5　外部システムの更改の次期については、警察庁が別途指示する。

なお、外部システムの更改は、委託期間中、外部システムごとに一回ずつ計画している。

７．３　保守に関する留意事項

上記の７．１項及び７．２項の作業について、一部作業は、夜間深夜時間帯及び警察システムを停止する定期点検時に実施する。

８　特記事項

８．１　保秘に関する遵守事項

8.1.1　本契約により知り得た情報は、他者に漏らしてはならない。

8.1.2　警察庁から秘密の保全状況について検査通知があった場合には、これを受けること。

８．２　提出書類

8.2.1　体制表及び技術者名簿

契約締結後、速やかに体制表及び技術者名簿（以下、「体制表等」という。）を警察庁に提出すること。

なお、体制表等の内容に変更が生じた場合は、その都度提出すること。

8.2.2　誓約書及び管理規程

契約締結後、速やかに保秘に関する遵守事項について、秘密の保全に関する誓約書及び具体的な管理規程を警察庁に提出すること。

8.2.3　月次報告書

７項に掲げる保守の実施状況を記した報告書を毎月作成し、警察庁に提出すること。

なお、報告内容、報告方法及び報告時期については警察庁と協議すること。

8.2.4　作業申請書

７項に掲げる内容について、計画的に実施する作業については、作業を実施する５営業日前までに作業計画及び作業手順をまとめた作業申請書を提出し、警察庁の承認を得ること。

なお、申請書に記載する内容の詳細については、警察庁と協議すること。

8.2.5　作業報告書

７項に掲げる内容について作業を実施した際には、実施した作業内容を記した報告書を作成し、その都度警察庁に提出すること。

なお、報告書に記載する内容については警察庁と協議すること。

8.2.6　ODB登録用シート

ガイドラインに基づき、警察庁が別途指示するODB登録用シートを作成し、警察庁に提出すること。

8.2.7　課題管理表

保守において解決すべき問題について、発生時の対応及び管理手法について記載し、更新がある度に警察庁に提出すること。

８．３　引継ぎ等

8.3.1　委託期間中にプログラム改修が実施される場合の措置

委託期間中にプログラム改修が実施される場合は、プログラム改修後の保守について警察庁と別途協議を行うものする。

8.3.2　システム更改等に係る引継ぎ

事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラムに係るシステム更改等により、新たにプログラム開発又はプログラム保守を担当することになる事業者に対して作業経緯や残存課題等の引継ぎを行うため、必要な各種資料を整理し、引継書を作成し、警察庁へ提出すること。また、システム更改等に係る移行作業において、運用環境で保有するデータを出力するためのツールを作成すること。

別添３

事前旅客情報システム及び外国人個人識別情報認証システム構築等仕様書（案）

警察庁情報通信局情報管理課
平 成 ○ 年 ○ 月 ○ 日

１　概要

本仕様書は、事前旅客情報システム及び外国人個人識別情報認証システムの設計、構築、試験及び運用に必要な教育訓練にかかる全ての作業に適用する。

２　作業場所

警察庁が別途指示する、東京都23区内の警察庁庁舎(2か所)、各都道府県警察本部（方面本部を含む。）及び警察署等とする。

３　履行期限

平成31年２月28日（木）までに全ての作業を完了すること。

４　関連仕様書

４．１　警情仕プロ管第●号「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書」（平成28年●月●日制定）

４．２　警情仕形管第●号「事前旅客情報システム及び外国人個人識別情報認証システム仕様書」（平成28年●月●日制定）

４．３　警情仕形管第38号「アクセス権管理システム仕様書」（平成25年２月１日制定）

４．４　警情仕形管第42号「指掌紋自動識別システム用照合部仕様書」（平成25年４月25日制定）

５　用語の定義

５．１　業務用プログラム

４．１項の関連仕様書により調達したプログラムをいう。

５．２　警察システム

４．２項の関連仕様書により調達したシステムをいう。

５．３　設置機器

警察システムを構成する機器のうち、別紙「構成品一覧」に示す機器をいう。

５．４　機械室等設置機器

設置機器のうち、機械室及び監視室に設置する機器をいう。詳細については別紙「構成品一覧」に示す。

５．５　専用端末等

設置機器のうち、作業場所の各拠点に設置する機器をいう。詳細については別紙「構成品一覧」に示す。

５．６　外部システム

４．１項の関連仕様書により定義する、警察システムと連携するシステムの総

称をいう。

５．７　情報通信部

関東管区警察局情報通信部、東京都警察情報通信部、北海道警察情報通信部及び各府県（方面を含む。）情報通信部を指す。

５．８　ガイドライン

「政府情報システムの整備及び管理に関する標準ガイドライン」（平成26年12月３日各府省情報化統括責任者（CIO）連絡会議決定）をいう。

６　作業内容

６．１　設計・開発実施計画、実施要領の作成

6.1.1　契約後、警察庁と協議を行い、ガイドラインに基づく設計・開発実施計画及び設計・開発実施要領の案を速やかに作成し、警察庁に提出すること。実施計画書及び実施要領には以下の項目を記載すること。また実施計画書の附属文書としてWBS(WorkBreakdownStructure)も併せて作成すること。

(1)　実施計画書

作業概要、作業体制、スケジュール、成果物、開発形態・開発手法・開発環境・開発ツールについて記載すること。

(2)　WBS

作業項目、作業内容及びスケジュールをより詳細に階層化し、担当者等を記載すること。

(3)　実施要領

コミュニケーション管理、体制管理、品質管理、工程管理、リスク管理、課題管理、システム構成管理、変更管理及び情報セキュリティ対策について記載すること。

6.1.2　実施要領の各項目について以下の要件を満たすよう作成すること。

(1)　コミュニケーション管理

警察庁と協議した場合は、速やかに議事録を作成し、警察庁の承認を得ること。

(2)　体制管理及び品質管理

ア　警察システムの設計、開発、テスト及び４．１項の関連仕様書により調達するプログラムの導入の各工程において、警察庁の意図しない変更や機密情報の窃取等が行われないことを保証する管理が、一貫した品質保証体制の下でなされていること。

イ　警察庁の意図しない変更や機密情報の窃取等が行われないことを保証するための具体的な管理手順や品質保証体制を証明する書類（例えば、品質保証体制の責任者や各担当者がアクセス可能な範囲等を示した管理体制図）を提出すること。第三者機関による品質保証体制を証明する書類等が提出可能な場合は提出すること。

ウ　警察システムに警察庁の意図しない変更が行われるなどの不正が見つかった時に、追跡調査や立ち入り検査など、警察庁と連携して原因を調査し、

排除するための手順及び体制を整備すること。また、当該手順及び体制が妥当であることを証明するための書類を提出すること。

(3) 工程管理

設計・開発実施計画書及び設計・開発実施要領に基づき設計・開発を行い、原則月２回行う予定の警察庁との定例会議において、その結果を報告すること。また、警察庁と協議を行い、ガイドラインに基づく次の書類を作成し、警察庁に提出すること。

なお、定例会議が行われない場合においても、進捗報告に関する書類は提出すること。

ア EVM（Earned Value Management）進捗管理表を作成し、定例会議に提出すること。

イ 前月の進捗状況表、EVM推移グラフ及び進捗状況分析図を作成し、月初めの定例会議に提出すること。

ウ ガイドラインに基づく政府情報システム管理データベース（Official information systemtotal management Database）（以下「ODB」という。）に警察庁が登録を行うので、登録用シートに必要事項を記載し、設計・開発実施要領において定める時期に提出すること。

なお、ODB登録用シートの詳細については、警察庁が別途指示する。

エ 警察庁の求めに応じ、作業の進捗状況等について中間報告を行うこと。

(4) リスク管理、課題管理及び変更管理

リスク管理簿を作成し、警察システムの設計・開発における作業を阻害する可能性のあるリスクを適切に管理すること。また、設計・開発において解決すべき問題及び変更内容についても適切に管理・記録すること。

６．２ 仕様要件の確定及び設計

6.2.1 ４．２項の関連仕様書の各機器における機能及び性能の承認事項について、警察庁と協議を行い、承認を得て仕様要件を確定すること。

6.2.2 設計・開発実施計画書、実施要領及び確定した仕様要件に基づき、設計を行うこと。また、基本設計書及び詳細設計書を警察庁に提出し承認を得ること。

６．３ 構築

6.3.1 搬入

(1) 設置機器の搬入場所及び搬入場所別の配分数量については、警察庁が別途指示する。

(2) 機械室等設置機器の搬入方法及び搬入日程の詳細については、警察庁と協議して決定すること。

(3) 専用端末等の搬入方法及び搬入日程の詳細については、搬入先の拠点を担当する情報通信部と協議して決定すること。

(4) 専用端末等の搬入日程を取りまとめ、警察庁に報告すること。

6.3.2 設置

(1) 機械室等設置機器

ア 設置

警察庁が承認した設置図面等に従い、設置を行うこと。

イ　ケーブルの敷設及び接続

(ｱ)　電源ケーブル

a　設置機器の電源供給に必要な電源ケーブルを、既設分電盤（AC200Ｖ又はAC100Ｖ）から設置機器の設置箇所まで敷設し、必要な口数を有するコンセントを取り付け、設置機器と接続すること。

b　接地が必要な機器については、接地用のケーブルを敷設し、接続すること。

(ｲ)　通信ケーブル

a　設置機器の間を接続するために必要なLANケーブル、ファイバチャネルケーブル等を敷設し、接続すること。

b　L3SW、ハブＩと既設ネットワーク機器を接続するために必要なLANケーブルを敷設し、接続すること。

(ｳ)　FM受信ケーブル

時刻同期装置のFMラジオ受信に必要な同軸ケーブルを既設端子板（FJ接栓）から時刻同期装置の設置箇所まで敷設し、契約業者が準備するFM端子用分配器（３分配）１個を使用して接続すること。

ウ　フロアパネルの加工

設置機器の固定又はケーブル立ち上げのため、必要に応じてフロアパネルに開口部を設けるなど加工を施すこと。

フロアパネルの仕様は、以下のとおりとする。

・パネル素材　：ケイ酸カルシウム板(ニチアス(株))
・パネル種類　：M300A-0-Pタイル(Ｐタイル一体貼りタイプ)
・サイズ　　：500㎜×500㎜
・厚さ　　：25.5㎜

(2)　専用端末等

ア　専用端末等は搬入先の情報通信部の指示に従い設置すること。

イ　情報通信部が別途用意する、LANケーブル及び電源に接続すること。

ウ　警報装置については、LANケーブル及び電源ケーブルの脱落防止対策を施すこと。

(3)　留意事項

ア　荷重

機械室等設置機器は、免震床にかかる荷重が次の規格値を超えないように配置すること。なお、荷重が規格値を超えるおそれがある場合は、荷重を分散させる措置を行うこと。

・フロアパネル（500㎜×500㎜）１枚あたりにかかる荷重が2,000Ｎ以下
・フロアパネル２枚×２枚（１㎡）あたりにかかる荷重が4,900Ｎ以下
・フロアパネル８枚×６枚（12㎡）あたりにかかる荷重が16,600Ｎ以下

イ　転倒防止

機器の高さ、重量等を勘案し、転倒のおそれがある機器については、堅

固に固定等を行い、転倒を防止するよう措置すること。

ウ　落下防止

操作卓に設置する機器は、耐震用具等を用いて操作卓に固定し、落下を防止するよう措置すること。

6.3.3　導入及び調整

設置機器について、運用開始までの間に、以下の導入、調整等を行うこと。

(1)　設置機器の構成品に含まれるソフトウェアについて、警察庁と協議の上、インストール、設定、調整及び試験を行うこと。

(2)　設置機器の内蔵HDDのパーティション割当て、各ストレージのHDD等の割り当て及び各サーバのメモリ割り当てについては、警察庁と協議を行い、承認を得て設定すること。

(3)　業務用プログラムの開発事業者が、業務用プログラムのインストール、設定及び試験を行うので、協力すること。

(4)　業務用プログラムの安定稼働に必要なソフトウェアの調整、設定項目については、警察庁又は業務用プログラム開発担当者から受領し、妥当性の検証後、警察庁の承認を得た後に作業を行うこと。

(5)　機械室等設置機器と外部システムとの接続に関し、警察庁が別途指示する要件に基づき設定、調整及び試験を行うこと。

なお、当該作業の実施にあたっては、警察庁及び外部システムの担当者と協議を行い、詳細を決定した上で実施すること。

(6)　全ての設定及び試験が終了した時点で、契約業者が準備する電磁的記録媒体にバックアップを行い、作業を担当した警察庁又は情報通信部に提出すること。

なお、提出するバックアップは、リカバリ実施の際にソフトウェアの設定変更等の追加作業を必要としない状態であること。

(7)　設置機器の構成品に含まれるソフトウェアについて、導入から運用開始までの間に、その開発業者から修正プログラムがリリースされた場合には、速やかに警察庁に報告し、その指示に従うこと。

６．４　試験

４．１項の関連仕様書の9.1.3項で示す、警察庁が実施する業務用プログラムのテスト（以下「受入テスト」という。）について、次の通り対応すること。

6.4.1　受入テストにおいて、警察システムの設定及び調整の変更が必要となった場合は、警察庁と協議して承認を得た後、実施すること。

6.4.2　受入テストの実施中は、支援体制を確保すること。

６．５　教育訓練

警察庁が指示する教育訓練の計画に従い、警察システムの運用管理、監視方法について、次のとおり教育訓練を行い、その結果を報告すること。

なお、実施時期、実施方法等の詳細については、事前に警察庁と協議すること。

6.5.1　警察システムの運用管理及び監視方法に係る教育訓練を、約30人に対し４日程度に分けて平成●年●月●日までに実施すること。

6.5.2　教育訓練に必要な機器及び教材は、契約業者が準備すること。
　　なお、警察庁と協議し、納品する機器を活用することは可能とする。
6.5.3　教育訓練の実施場所は、警察庁が別途指示する東京都23区内の警察庁庁舎とする。

6．6　その他

6.6.1　情報通信部の担当者及び連絡先については、警察庁が別途指示する。
6.6.2　作業時間は、原則として搬入場所における警察庁又は情報通信部の執務時間とし、執務時間外に作業を行う必要がある場合は、事前に警察庁または情報通信部の承認を得ること。
　　なお、警察庁の執務時間は午前9時半から18時15分までとし、情報通信部の執務時間については、情報通信部に確認すること。
6.6.3　搬入場所ごと個別に必要となる調整事項については、該当する警察庁又は情報通信部と行うこと。
6.6.4　作業に必要な資機材は、契約業者において全て用意すること。
6.6.5　6.3.3(5)項について、一部作業を夜間深夜時間帯に実施する場合がある。

7　一般的共通事項

7．1　遵守事項

7.1.1　作業に当たっては、本仕様書、関係法規等を遵守の上、確実堅固・美観に留意して行うこと。
7.1.2　作業に当たっては、既設物等に損傷を与えないよう十分な養生を行い、損傷を与えないよう留意すること。
7.1.3　作業中に、既設物等に損傷を与えたとき、また、作業従事者及び第三者に対して損害を及ぼしたときは、速やかに警察庁に報告するとともに、契約業者はその補償を行うこと。
7.1.4　仕様書に明記されていない事項であっても、構造上必要な作業は、警察庁又は情報通信部の指示により契約業者の負担において行うこと。
7.1.5　作業中知り得た情報は、他に漏えいしないこと。

7．2　作業責任者及び作業従事者

7.2.1　契約業者は、作業責任者を定め、作業中は、常に現場に派遣し、警察庁又は情報通信部との連絡及び作業全般の責に当たらせること。
7.2.2　作業責任者及び作業従事者は、腕章及び契約業者の社章をつけること。

7．3　作業場所の管理

7.3.1　作業中は、火災、盗難、その他事故が起こらないよう十分注意し、常に資機材の整理を行うこと。
7.3.2　作業により生じた廃材等は、契約業者が関係法令等に基づいて適切かつ速やかに処理すること。
7.3.3　作業従事者の規律は厳重に保持すること。
7.3.4　その他必要な事項は、警察庁又は情報通信部の指示に従うこと。

7．4　作業の確認等

作業完了後、容易に目視確認等が出来ない箇所は、作業の過程において警察庁又は情報通信部の確認又は立会いを受けること。

7．5　作業計画の変更

作業日程、作業方法等について変更する必要がある場合は、事前に作業を担当する警察庁又は情報通信部の承認を得た上で実施すること。

7．6　本仕様書の解釈について疑義が生じたときは、速やかに警察庁に連絡して指示を受けること。

8　提出書類

ガイドラインに係る提出書類とは別に、次に指示する書類を提出すること。

8．1　機械室等設置機器

8.1.1　契約締結後、速やかに次の書類を警察庁に提出すること。

なお、変更が生じた場合は、事前に警察庁の承認を得ること。

(1)　従事者名簿

作業責任者及び作業従事者の名簿を作成し、1部提出すること。

(2)　作業計画表

作業計画表を作成し、1部提出すること。

(3)　設置図面

サーバ等機器のラック搭載レイアウト、フロア配置、ケーブル敷設ルート、転倒防止措置等の詳細について記載した書類を作成し、警察庁の承認を得た後、1部提出すること。

8.1.2　作業日ごとに次の書類を警察庁に提出すること。

(1)　作業予定表

6.3.2(1)項の作業における作業日ごとの作業予定内容等を記載した書類を作成し、作業日の2日前までに1部提出すること。

(2)　作業報告書

6.3.2(1)項の作業における作業日ごとに実施した作業内容等を記載した書類を作成し、1部提出すること。

8.1.3　作業完了後、速やかに次の書類を警察庁に提出すること。

(1)　実施結果報告書

6項の各作業の作業実施結果について、実施結果報告書を作成し、1部提出すること。

(2)　作業完了報告書

全ての作業完了後、作業完了報告書を作成し、1部提出すること。

(3)　作業写真

6.3.2(1)項の作業における作業写真を、冊子で1部提出すること。

(4)　完成図書

6.3.2(1)項の作業完了後の設置及び搭載レイアウト、ケーブル敷設ルート、転倒防止措置等を記載した図面を作成し、冊子及び電磁的記録媒体で、各1部提出すること。

なお、ウ項の作業写真の編冊も可とする。

(5)　(4)項の電磁的記録媒体は、契約業者で準備すること。

なお、電磁的記録媒体の種類については、警察庁と協議すること。

8.1.4　詳細は、警察庁と協議すること。

8．2　専用端末等

8.2.1　全ての専用端末に対して6.3.1項から6.3.3項までの作業が完了した後に、警察庁にその旨の報告をすること。

8.2.2　警察庁の求めに応じ、6.3.1項から6.3.3項までの作業経過を報告すること。

8.2.3　情報通信部より６．３項の作業実施に係る書類の提出を求められた場合は、情報通信部と調整した上で書類を提出すること。

9　検査

(1)　作業完了後、６項の作業内容について警察庁検査官が検査を行う。

(2)　検査で不合格となったものは、警察庁検査官の指示に基づき所要の作業を行い、再検査を行う。

(3)　検査に必要な準備は、すべて契約業者が行うこと。

(4)　検査中に疑義が生じたときは、警察庁検査官の指示に従うこと。

別添４

事前旅客情報システム及び外国人個人識別情報認証システム仕様書(案)

警 察 庁 情 報 通 信 局
警 情 仕 形 管 第 ● 号
平 成 ● 年 ● 月 ● 日 制 定

１　調達件名

事前旅客情報システム及び外国人個人識別情報認証システムに係る整備

２　品名及び略称

品名及び略称は、表－１のとおりとする。

表－１　　品名及び略称

品　　名	略　　称
事前旅客情報システム及び外国人個人識別情報認証システム	
JB18-LB11形負荷分散装置	負荷分散装置
JB18-WD11形Web/AP・Dirサーバ	Webサーバ
JB18-BU11形業務・DBサーバ	業務サーバ
JB18-EX21形抽出サーバ	抽出サーバ
JB18-MO21形監視・配信サーバA	監視サーバA
JB18-MD21形監視・配信サーバB	監視サーバB
JB18-BA21形バックアップサーバ	バックアップサーバ
JB18-ST21形ストレージ装置A	ストレージA
JB18-ST21形ストレージ装置B	ストレージB
JB18-DX21形データ交換装置	データ交換装置
JB18-TI21形時刻同期装置	時刻同期装置
JB18-FW21形ファイアウォール	FW
JB18-WD31形試験Web/AP・Dirサーバ	試験Webサーバ
JB18-BU31形試験業務・DBサーバ	試験業務サーバ
JB18-PC11形専用端末装置A	専用端末A
JB18-PC11形専用端末装置B	専用端末B
JB18-PC21形管理・監視端末装置A	管理端末A
JB18-PC21形管理・監視端末装置B	管理端末B
JB18-PC31形コンソール端末装置A	コンソール端末A
JB18-PC31形コンソール端末装置B	コンソール端末B
JB18-PC41形試験専用端末装置A	試験端末A
JB18-PC41形試験専用端末装置B	試験端末B
JB18-WD11形警報装置	警報装置
JB18-SC11形画像読取装置	スキャナ
JB18-PR11形印字装置	印字装置

	レイヤ３スイッチ	L3SW
	スイッチングハブⅠ	ハブⅠ
	ラック	ラック

３　作業の概要

３．１　目的

本仕様書は、事前旅客情報システム及び外国人個人識別情報認証システム（以下「業務システム」という。）において、事前旅客情報照合業務及び外国人個人識別情報認証業務を実施するために構築するハードウェアに適用する。

３．２　背景

事前旅客情報照合業務及び外国人個人識別情報認証業務は、テロリスト及び不法入国者の上陸阻止、輸入禁制品等の密輸阻止及び指名手配者の逮捕等水際における取締りの徹底を図ることを目的とする業務である。

現在運用している業務システムのハードウェアが平成30年度に運用期限を迎えることに伴い、平成31年３月に新たな業務システムに更改するため、平成29年度及び30年度に対象となる機器の賃貸借、プログラム開発、構築及び保守作業を含めた調達を行うこととしている。

３．３　用語の定義

3.3.1　クラスタ構成

複数台のサーバを接続して、いずれかのサーバが故障しても別のサーバが業務を引き継ぎ、業務を停止させることなく継続できるシステム構成をいう。

3.3.2　アクティブ／スタンバイ型

稼働系サーバと待機系サーバで構成され、稼働系サーバが故障したときは、待機系サーバがその処理を引き継ぐ方式をいう。

3.3.3　アクティブ／アクティブ型

稼働系サーバと稼働系サーバで構成され、片方の稼働系サーバが故障したとき、もう片方の稼働系サーバが故障した稼働系サーバの処理も行う方式をいう。

3.3.4　ホットスペアディスク

ホットスペアとは、HDDの故障に備えて、あらかじめ予備のHDDを通電状態で待機させておき、RAIDを構成するHDDが故障したときに、自動的に故障したHDDを論理的に切離し、予備のHDDをRAIDに組み込むことをいう。このホットスペアに使用するための予備のHDDのことをホットスペアディスクという。

3.3.5　業務サーバ等

警察庁に設置するWebサーバ、業務サーバ、監視サーバＡ、バックアップサーバ、試験Webサーバ及び試験業務サーバをいう。

3.3.6　抽出サーバ等

警察庁に設置する抽出サーバ及び監視サーバＢをいう。

3.3.7　警察庁サーバ

業務サーバ等及び抽出サーバ等をいう。

3.3.8　各ストレージ

ストレージA及びストレージBをいう。

3.3.9　専用端末

専用端末A及び専用端末Bをいう。

3.3.10　管理端末

管理端末A及び管理端末Bをいう。

3.3.11　コンソール端末

コンソール端末A及びコンソール端末Bをいう。

3.3.12　試験端末

試験端末A及び試験端末Bをいう。

3.3.13　専用端末A等

専用端末A、試験端末A、管理端末A及びコンソール端末Aをいう。

3.3.14　専用端末B等

専用端末B、試験端末B、管理端末B及びコンソール端末Bをいう。

3.3.15　各端末

専用端末、管理端末、コンソール端末及び試験端末をいう。

3.3.16　各スイッチ

L3SW及びハブⅠを総称していう。

3.3.17　警察庁ホストシステム

警察庁に設置される各種業務を行うシステムをいう。

3.3.18　警察庁指掌紋システム

警察庁に設置される指掌紋に関する業務を行うシステムをいう。

3.3.19　アクセス権管理システム

警察庁に設置される利用者のアクセス権を一元管理するシステムをいう。

3.3.20　法務省システム

法務省が運用しているシステムをいう。

3.3.21　外部回線

警察機関の管理が及ばない電子計算機が論理的に接続され、当該電子計算機の通信に利用されるインターネットその他の電気通信回線をいう。

3.3.22　複製ボリューム

データベースを記録したボリュームの複製をいう。

3.3.23　業務用プログラム

3.7.1項の関連仕様書により調達するプログラムをいう。

３．４　業務の概要

3.7.1項の関連仕様書のとおり。

３．５　情報システム化の範囲

「３．４　業務の概要」に示すもののうち、本システムにて行う処理機能を情報システム化の対象範囲とする。

３．６　作業内容・納入物

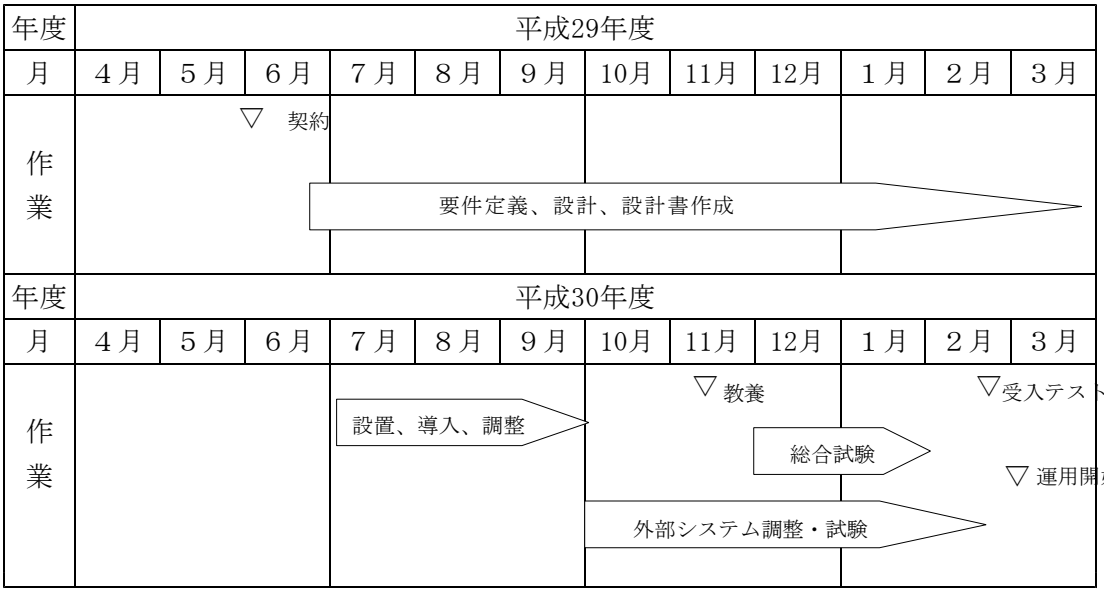
3.6.1　作業内容

本システムの調達を行い、整備後の保守を行う。整備に伴う要件定義、設計、

設置、導入等は別途契約を結ぶ。

調達スケジュール（案）を表－２に示す。ただし、スケジュールは概略であり、詳細なスケジュールについては、警察庁と協議の上、設計開発実施計画書に記載すること。

表－２　調達スケジュール（案）



3.6.2　納入物

納入物は、表- ３のとおりとする。また、提出が必要となる提出書類及び提出期限については、別紙１のとおりとする。

表- ３　　納入物

品名（略称）	数量	単位
負荷分散装置	1	式
Webサーバ	1	式
業務サーバ	1	式
抽出サーバ	1	式
監視サーバA	1	式
監視サーバB	1	式
バックアップサーバ	1	式
ストレージA	1	式
ストレージB	1	式
データ交換装置	1	式
時刻同期装置	2	式
FW	1	式
試験Webサーバ	1	式
試験業務サーバ	1	式
専用端末A	94	式
専用端末B	3	式

管理端末A	2	式
管理端末B	2	式
コンソール端末A	1	式
コンソール端末B	1	式
試験端末A	1	式
試験端末B	1	式
警報装置	377	式
スキャナ	59	式
印字装置	101	式
L3SW	6	式
ハブⅠ	1	式
ラック	1	式

３．７　関連仕様書

3.7.1　警情仕プロ管第●号「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書」（平成●年●月●日制定）（以下「プログラム仕様書」という。）

3.7.2　警情仕形管第42号「指掌紋自動識別システム用照合部仕様書」（平成25年４月25日制定）

3.7.3　警情仕形管第38号「アクセス権管理システム仕様書」（平成25年２月１日制定）

3.7.4　警情仕形管第30号「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書」（平成24年２月22日制定）

3.7.5　警情仕形管第40号「事前旅客情報システム及び外国人個人識別情報認証システム仕様書」（平成25年２月８日制定）

３．８　注意事項

警察庁サーバ、各ストレージ、データ交換装置、時刻同期装置、各端末、スキャナ、警報装置及び印字装置については、国等による環境物品等の調達の推進等に関する法律（平成12年法律第100号）第６条第１項の規定に基づく、環境物品等の調達の推進に関する基本方針で最新の基準を満たしていること。

４　情報システムの要件

情報システムの要件については、次のとおりとする。

４．１　機能・性能要件

4.1.1　負荷分散装置の機能及び性能は、表－４のとおりとする。

表－４　負荷分散装置の機能及び性能

品目	項目	機能及び性能
本体部	ロードバランス機能	Webサーバに対して、ラウンドロビン、最小コネクション又は最速応答によりロードバランス機能を有すること。
	セッション	URL、Cookie、SSL Session ID又は送信元IPアドレスによ

	維持機能	り、一定期間Webサーバにリクエストを割り振り続ける機能を有すること。
	ヘルスチェック機能	pingチェック､ポートチェック又はコンテンツチェック(HTTPに対するPOSTリクエストによる応答文字列の確認等)により、Webサーバの動作を確認する機能を有すること。
	スパニングツリー機能	ネットワークにおいて、データが永遠に循環するのを防止する機能を有すること。
	VLAN機能	物理的な接続形態とは別に、MACアドレス、IPアドレス、利用するプロトコルのいずれかに応じて、32以上の仮想的なグループが設定できること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを５個以上有すること。 (2) ネットワークは冗長構成ができること。
	管理コンソール機能	Webブラウザを使用し、負荷分散装置の管理に係る操作ができること。
	ネットワーク管理	監視サーバＡのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	コンソールインタフェース	コンソール端末と接続可能なポートを有すること。
	時刻同期	１日１回以上、監視サーバＡと自動及び手動で時刻同期ができること。
その他		アクティブ／スタンバイ型の冗長構成とし、冗長側機器への切替が任意にできること。

4.1.2 Webサーバの機能及び性能は、 表- ５のとおりとする。

表- ５ Webサーバの機能及び性能

品目	項目	機能及び性能
本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。
	メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。 (2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。 (3) 運用期間中、交換又は増設による拡張の必要がない、

		十分な容量を有すること。 (4) サーバを停止せずに、HDDの交換ができること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを５個以上有すること。 (2) ネットワークは冗長構成ができること。
	電源ユニット	冗長構成であること。
バックアップ部		(1) RDX媒体を扱うことができること。 (2) １回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。
ソフトウェア	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。 (2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。 (3) 日本語に対応すること。
	Web機能	(1) Apache HTTP Serverを搭載すること。 (2) アクティブ／アクティブ型のWebサーバを構築できること。
	ディレクトリサービス	(1) 業務用プログラムの要求受け、必要なユーザ情報を送信できること。 (2) 日本語に対応すること。 (3) SSLオプションを搭載すること。 (4) 5,000ユーザ以上を登録できること。 (5) ディレクトリサーバについては、アクティブ/アクティブ型の冗長構成とし、レプリケーション機能を有すること。 (6) ユーザ情報を管理する、GUIによるインターフェースを有すること。 (7) アクセス権管理システムが採用するユーザーインターフェースと互換性を有すること。
	プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。
	バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。 (2) サーバを停止せずに、内蔵HDDのバックアップができること。
	運用管理	(1) 本装置の本体部及びバックアップ部の稼働状況を監視し、監視サーバＡの運用管理ソフトウェアに通知できる

		こと。 (2) 監視サーバＡの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携しジョブを実行できること。
	ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア　ログイン及びログアウト履歴 イ　システムログ ウ　アプリケーションログ エ　セキュリティログ オ　データベースへのアクセスログ (2) 監視サーバＡのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。 (3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること
	ネットワーク管理	監視サーバＡのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) 監視サーバＡからウイルス対策ソフトウェアの更新データを受信できること。 (4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。
	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。

4.1.3　業務サーバの機能及び性能は、表- ６のとおりとする。

表- ６　業務サーバの機能及び性能

品目	項目	機能及び性能
本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。
	メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。

		(2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。 (3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。 (4) サーバを停止せずに、HDDの交換ができること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを４個以上有すること。 (2) ネットワークは冗長構成ができること。 (3) ストレージＡへ接続するためのファイバチャネルポートを有すること。 (4) ストレージＡへの接続は冗長構成とし、各々のディスクコントローラで接続できること。 (5) 冗長構成としたファイバチャネルについては、障害による自動閉塞機能及び自動切替機能を有すること。
	電源ユニット	冗長構成であること。
バックアップ部		(1) RDX媒体を扱うことができること。 (2) １回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。
ソフトウェア	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。 (2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。 (3) 日本語に対応すること。
	データベース管理	次の機能を有するソフトウェアを搭載すること。 (1) 別途調達する業務用プログラムが、SQL及びストアドプロシージャの実行及び結果の取得ができること。 (2) 複数のデータベースサーバから、同一のデータベースにアクセス可能なこと。 (3) アクティブ/アクティブ型のクラスタ構成に対応できること。 (4) データベースの性能情報、運用状況の統計を作成でき、分析できること。
	クラスタ	(1) アクティブ／アクティブ型のクラスタ構成であること。 (2) データベースのデータを同一の内容に保つこと。 (3) クラスタ構成の構築及び運用保守を行うために必要な

	次の機能を有すること。 ア　管理端末Ａ及びコンソール端末ＡからGUI又はWebブラウザを使用し、クラスタの設定変更ができること。 イ　管理端末Ａ及びコンソール端末ＡからGUI又はWebブラウザを使用し、クラスタ、ノード及びアプリケーションの起動及び停止が容易にできること。 (4) 管理端末Ａ及びコンソール端末Ａから系の切替えを任意にできること。
プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。
バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。 (2) サーバを停止せずに、内蔵HDDのバックアップができること。
運用管理	(1) 本装置の本体部及びバックアップ部の稼働状況を監視し、監視サーバＡの運用管理ソフトウェアに通知できること。 (2) 監視サーバＡの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携しジョブを実行できること。
ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア　ログイン及びログアウト履歴 イ　システムログ ウ　アプリケーションログ エ　セキュリティログ オ　データベースへのアクセスログ (2) 監視サーバＡのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。 (3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること
ネットワーク管理	監視サーバＡのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) 監視サーバＡからウイルス対策ソフトウェアの更新データを受信できること。 (4) ウイルス対策ソフトウェアの更新データを自動及び手

		動で更新できること。
	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。

4.1.4　抽出サーバの機能及び性能は、表- ７のとおりとする。

表- ７　抽出サーバの機能及び性能

品目	項目	機能及び性能
本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。
	メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。 (2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。 (3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。 (4) サーバを停止せずに、HDDの交換ができること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを８個以上有すること。 (2) ネットワークは冗長構成ができること。 (3) ストレージＢに接続するためのファイバチャネルポートをすること。 (4) 待機系サーバにあっては、ストレージＢに接続するためのファイバチャネルポートとは別に、テープライブラリに接続するためのファイバチャネルポートを有すること。 (5) ストレージＢへの接続は冗長構成とし、各々のディスクコントローラで接続できること。 (6) 冗長化したファイバチャネルは、障害による自動閉塞機能及び自動切替機能を有すること。
	電源ユニット	冗長構成であること。
バックアップ部		(1) RDX媒体を扱うことができること。 (2) １回のバックアップ作業で、交換することなく単一の

		電磁的記録媒体でシステムバックアップを採取できること。
テープライブラリ部	テープライブラリ	(1) テープスロット数が20個以上であること。 (2) ライブラリ容量が30Tバイト（非圧縮）以上であること。 (3) 本体部とファイバチャネルにより接続できること。
	テープドライブ	(1) LTO5以上に対応したものを２台以上搭載すること。 (2) １台当たりのデータ転送速度は、最大140Mバイト/秒以上(非圧縮)であること。 (3) 暗号化については、次のとおりとする。 ア　警察庁が別途指示する政府推奨の暗号アルゴリズムにより暗号化した上で、電磁的記録媒体に記録できること。また、任意の周期で暗号鍵を変更できること。 イ　暗号化に使用した暗号鍵を電磁的記録媒体に記録できること。 ウ　暗号鍵生成のログが採取でき、暗号鍵を作成した年月日時分秒を確認できること。
ソフトウェア１	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。 (2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。 (3) 日本語に対応すること。
	Web機能	(1) Apache HTTP Serverを搭載すること。 (2) アクティブ／スタンバイ型のWebサーバを構築できること。
	データベース管理	次の機能を有するソフトウェアを搭載すること。 (1) 別途調達する業務用プログラムが、SQL及びストアドプロシージャの実行及び結果の取得ができること。 (2) 複数のデータベースサーバから、同一のデータベースにアクセス可能なこと。 (3) アクティブ/スタンバイ型のクラスタ構成に対応できること。 (4) データベースの性能情報、運用状況の統計を作成でき、分析できること。
	クラスタ	(1) アクティブ／スタンバイ型のクラスタ構成であること。 (2) データベースのデータを同一の内容に保つこと。 (3) クラスタ構成の構築及び運用保守を行うために必要な次の機能を有すること。 ア　管理端末Ｂ及びコンソール端末ＢからGUI又はWebブラウザを使用し、クラスタの設定変更ができること。

	イ　管理端末Ｂ及びコンソール端末ＢからGUI又はWebブラウザを使用し、クラスタ、ノード及びアプリケーションの起動及び停止が容易にできること。 (4) 管理端末Ｂ及びコンソール端末Ｂから系の切替えを任意にできること。
プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。
バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。 (2) サーバを停止せずに、内蔵HDDのバックアップができること。
運用管理	(1) 本装置の本体部、バックアップ部及びテープライブラリ部の稼働状況を監視し、監視サーバＢの運用管理ソフトウェアに通知できること。 (2) 監視サーバＢの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携し、ジョブを実行できること。
ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア　ログイン及びログアウト履歴 イ　システムログ ウ　アプリケーションログ エ　セキュリティログ オ　ユーザ認証ログ カ　データベースへのアクセスログ (2) 監視サーバＢのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。 (3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。
ネットワーク管理	監視サーバＢのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2)　ファイルアクセス時に自動でウイルスチェックができること。 (3) 監視サーバＢからウイルス対策ソフトウェアの更新データを受信できること。 (4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。

	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。
ソフトウェア２	データレプリケーション	(1) ストレージＢ内で、データベースを記録したボリュームの複製が作成できること。 (2) 業務に影響することなく、ストレージＢ内で複製ボリュームの作成及び切離しができること。 (3) 待機系サーバへ機能を搭載すること。
	バックアップ２	(1) 監視サーバＢに収集されたログをテープライブラリ部の電磁的記録媒体にバックアップし、累積して管理できること。 (2) 業務に影響することなく、ストレージＢのデータベースをバックアップ及びリストアするため、次の機能を有すること。 ア バックアップ (ｱ) 監視サーバＢの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携し、定められた時刻に自動及び任意の時刻に手動で、ストレージＢの複製ボリュームをオンラインから切離し、対象データをテープライブラリ部の電磁的記録媒体にバックアップができること。 (ｲ) バックアップデータは、日付、時刻及びバックアップの対象データを一意に識別できる名称で管理できること。 (ｳ) バックアップデータは、１世代当たり正・副とし、３世代の管理ができること。 イ リストア (ｱ) オンラインから切り離された複製ボリューム並びにデータの更新、追加、削除のログ及びその他必要な情報から、データベースを障害発生直前の状態までリストアできること。 (ｲ) (ｱ)によりリストアできない場合、テープライブラリ部の電磁的記録媒体に保存されたバックアップデータ及びその他必要な情報から、データベースをバックアップ取得時の状態までリストアできること。 (ｳ) データベースのリストアは、(2)ア(ｲ)の名称を指定してできること。 (3) 管理端末ＢからGUI又はWebブラウザにより、バックアップ２の設定及び監視ができること。 (4) 待機系サーバへ機能を搭載すること。

4.1.5　監視サーバＡの機能及び性能は、表- ８のとおりとする。

表- ８　監視サーバＡの機能及び性能

品目	項目	機能及び性能
本体部	CPU	本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる処理能力を有すること。
	メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。 (2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。 (3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。 (4) サーバを停止せずに、HDDの交換ができること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを５個以上有すること。 (2) ネットワークは冗長構成ができること。 (3) 共有ディスク装置へ接続するためのファイバチャネルポートを有すること。 (4) 共有ディスク装置への接続は冗長構成とし、各々のディスクコントローラで接続できること。 (5) 冗長構成としたファイバチャネルについては、障害による自動閉塞機能及び自動切替機能を有すること。
	電源ユニット	冗長構成であること。
コンソール部	ディスプレイ	(1) 解像度は1,024×768ドット以上であること。 (2) 表示色は、65,536色以上であること。
	キーボード	JIS規格キー配列に準拠していること。
	マウス	(1) ２ボタン式以上の光学式又はレーザー式であること。 (2) ホイール等によりマウスを移動せずに画面のスクロールができること。
	KVMスイッチ	(1) ディスプレイ、キーボード及びマウスを接続できること。 (2) クラスタ構成された本サーバ２台を接続し、切替えで

		きること。
バックアップ部		(1)　RDX媒体を扱うことができること。 (2)　１回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。
共有ディスク部	共有ディスク装置	(1) RAID1、RAID5又はRAID6の冗長構成とし、RAID構成後の実記憶容量については、警察庁と協議すること。 (2) (1)で決定した実記憶容量とは別に、HDD又はエンクロージャー等の増設により、取り扱う容量の拡張ができること。 (3) サーバを停止せずに、HDDの交換ができること。 (4) 本体部とは、ファイバチャネルで接続できること。
ソフトウェア	OS	(1) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。 (2) 日本語に対応すること。
	クラスタ	(1) アクティブ／スタンバイ型のクラスタ構成であること。 (2) クラスタ構成の構築及び運用保守を行うために必要な次の機能を有すること。 ア　GUI又はWebブラウザを使用し、クラスタの設定変更ができること。 イ　GUI又はWebブラウザを使用し、クラスタ、ノード及びアプリケーションの起動及び停止ができること。 (3) 系の切替えを任意にできること。
	バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。 (2) サーバを停止せずに、内蔵HDDのバックアップができること。
	統合監視	(1) 業務統合監視機能 GUI又はWebブラウザによる統合監視機能を有し、監視目的別に業務状況(運用管理、ログ管理、ネットワーク管理、ストレージ管理及び性能管理)を監視することができること。また、監視画面から各機能の監視画面に遷移し、階層を掘り下げることにより障害箇所を特定できること。 (2) コマンド制御機能 コマンドを業務サーバ等(監視サーバＡを除く。)へ発行できること。また、発行したコマンド及び受信メッセージの履歴を照会できること。 (3) メッセージ監視機能 業務サーバ等（監視サーバＡを除く。）から通知されたメッセージについて、メッセージごとに内容説明や処置方法を任意に定義できること。また、日本語で表示及

	び印字できること。 (4) 警報装置の制御 　メッセージの内容に応じて、管理端末Ａに付帯する警報装置の制御ができること。 (5) 管理端末Ａへの通知 　業務サーバ等（監視サーバを除く。）から通知されたメッセージは、管理端末Ａの統合監視ソフトウェアへ通知できること。
ストレージ管理	ストレージＡの管理機能として、次の機能を有すること。 (1) ディスクアレイ構成情報（HDDの物理名称、エンクロージャ、プール及び制御装置に係る情報）をGUI又はWebブラウザで表示できること。 (2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。 (3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。 (4) ストレージＡのディスクアレイ及びネットワークの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報に反映できること。
性能管理	(1) 次の項目について、業務サーバ等の性能状態監視及び管理ができること。 ア　内蔵HDD利用率 イ　CPU利用率 ウ　メモリ利用率 (2) GUI又はWebブラウザによる業務サーバ及び試験業務サーバのRDBMS（Relational DataBase Management System）管理機能を有すること。
運用管理	(1) ジョブスケジューリング機能を有すること。 (2) 業務サーバ等、各スイッチ、各端末及び警報装置の稼働状況を監視し、統合監視ソフトウェアへ通知できること。 (3) ジョブスケジューリング機能と連携し、業務サーバ等のジョブの実行及び管理ができること。
ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 　なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア　ログイン及びログアウト履歴 イ　システムログ

		ウ　アプリケーションログ エ　セキュリティログ (2) 業務サーバ等及びデータ交換装置のログを収集し共有ディスク装置へ保存すると共に、区分(システムログ、アプリケーションログ、セキュリティログ等)、発生時間、発生装置、キーワード等により、抽出、分析及び出力ができること。 (3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。
	ネットワーク管理	業務サーバ等（監視サーバＡを除く。)、負荷分散装置、ストレージA及び各スイッチのMIB情報を収集する機能を有すること。
	端末リモート操作サーバ	専用端末Ａ及び試験端末Ａの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末Ａ及び試験端末ＡのOSへのログイン操作ができること。 (2) 専用端末Ａ及び試験端末Ａと監視サーバＡ間でクリップボードの情報を共有できること。 (3) 専用端末Ａ及び試験端末Ａと監視サーバＡ間でファイルの送受信ができること。
	ソフトウェア配信サーバ	(1) 専用端末Ａ等にインストールされたソフトウェア配信クライアントソフトウェアに対し、自動及び手動でソフトウェア及びソフトウェアのパッチを配信、適用ができること。このとき、配信開始時刻、転送速度制限、分割配信及び同時配信端末数の設定ができること。 (2) GUI又はWebブラウザによる管理コンソール機能を有し、スケジュール機能によりソフトウェアをインストールする時刻及び手順を一括、グループ別及び個別で設定できること。また、専用端末Ａ等に対して次の動作が設定できること。 ア　端末の強制再起動及び強制シャットダウン イ　インストール時及び終了時の端末の権限設定の変更 ウ　インストール失敗時の動作設定 (3) (2)で設定したスケジュールは、設定情報として内蔵HDDに保存できること。また、保存した設定情報をスケジュールに反映できること。 (4) 専用端末Ａ等からインストールの進行状況を自動及び手動で受信し、管理コンソール機能で表示でき、ログとして出力できること。 (5) 管理コンソール機能は、管理者権限が与えられた者の

		みが操作できるようアクセス権設定ができること。 (6) 待機系サーバへ機能を搭載すること。
	証跡収集	(1) 専用端末Ａ等が生成した証跡を収集し、管理できること。 (2) 専用端末Ａ等の要求により収集した証跡を送信し、検証ができること。
	定義ファイル配信	(1) 業務サーバ等、専用端末Ａ等及びデータ交換装置に対して、待機系サーバから配信先ごとのウイルス対策ソフトに対応するウイルス対策ソフトウェアの更新データを配信すること。 (2) ウイルス対策ソフトベンダーが提供する最新のウイルス対策ソフトウェアの更新データを取得できること。 ウイルス対策ソフトウェアの更新データの取得方法については、警察庁と別途協議すること。
	ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。
	時刻同期	(1) １日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。 (2) 専用端末Ａ等及び各スイッチの時刻修正ができること。

4.1.6 監視サーバＢの機能及び性能は、表- ９のとおりとする。

表- ９ 監視サーバＢの機能及び性能

品目	項目	機能及び性能
本体部	CPU	本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる処理能力を有すること。
	メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。 (2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。 (3) 運用期間中、交換又は増設による拡張の必要がない、

		十分な容量を有すること。 (4) サーバを停止せずに、HDDの交換ができること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを５個以上有すること。 (2) ネットワークは冗長構成ができること。 (3) 共有ディスク装置へ接続するためのファイバチャネルポートを有すること。 (4) 共有ディスク装置への接続は冗長構成とし、各々のディスクコントローラで接続できること。 (5) 冗長構成としたファイバチャネルについては、障害による自動閉塞機能及び自動切替機能を有すること。
	電源ユニット	冗長構成であること。
コンソール部	ディスプレイ	(1) 解像度は1,024×768ドット以上であること。 (2) 表示色は、65,536色以上であること。
	キーボード	JIS規格キー配列に準拠していること。
	マウス	(1) ２ボタン式以上の光学式又はレーザー式であること。 (2) ホイール等によりマウスを移動せずに画面のスクロールができること。
	KVMスイッチ	(1) ディスプレイ、キーボード及びマウスを接続できること。 (2) クラスタ構成された本サーバ２台を接続し、切替えできること。
バックアップ部		(1) RDX媒体を扱うことができること。 (2) １回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。
共有ディスク部	共有ディスク装置	(1) RAID1、RAID5又はRAID6の冗長構成とし、RAID構成後の実記憶容量については、警察庁と協議すること。 (2) (1)で決定した実記憶容量とは別に、HDD又はエンクロージャー等の増設により、取り扱う容量の拡張ができること。 (3) サーバを停止せずに、HDDの交換ができること。 (4) 本体部とは、ファイバチャネルで接続できること。
ソフトウェア	OS	(1) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。 (2) 日本語に対応すること
	クラスタ	(1) アクティブ／スタンバイ型のクラスタ構成であること。

		(2) クラスタ構成の構築及び運用保守を行うために必要な次の機能を有すること。 ア　GUI又はWebブラウザを使用し、クラスタの設定変更ができること。 イ　GUI又はWebブラウザを使用し、クラスタ、ノード及びアプリケーションの起動及び停止ができること。 (3) 系の切替えを任意にできること。
	バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。 (2) サーバを停止せずに、内蔵HDDのバックアップができること。
	統合監視	(1) 業務統合監視機能 GUI又はWebブラウザによる統合監視機能を有し、監視目的別に業務状況(運用管理、ログ管理、ネットワーク管理、ストレージ管理及び性能管理)を監視することができること。また、監視画面から各機能の監視画面に遷移し、階層を掘り下げることにより障害箇所を特定できること。 (2) コマンド制御機能 コマンドを抽出サーバへ発行できること。また、発行したコマンド及び受信メッセージの履歴を照会できること。 (3) メッセージ監視機能 抽出サーバから通知されたメッセージについて、メッセージごとに内容説明や処置方法を任意に定義できること。また、日本語で表示及び印字できること。 (4)　警報装置の制御 メッセージの内容に応じて、管理端末Ｂに付帯する警報装置の制御ができること。 (5) 抽出サーバから通知されたメッセージは、管理端末Ｂの統合監視ソフトウェアへ通知できること。
	ストレージ管理	ストレージＢの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報（HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報）をGUI又はWebブラウザで表示できること。 (2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。 (3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。 (4) メッセージにより、ストレージＢのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情

	報を反映できること。
性能管理	(1) 次の項目について、抽出サーバ等の性能状態監視及び管理ができること。 ア　内蔵HDD利用率 イ　CPU利用率 ウ　メモリ利用率 (2) GUI又はWebブラウザによる抽出サーバのRDBMS管理機能を有すること。
運用管理	(1) ジョブスケジューリング機能を有すること。 (2) 抽出サーバ等、各スイッチ、専用端末Ｂ等及び警報装置の稼働状況を監視し、統合監視ソフトウェアに通知できること。 (3) ジョブスケジューリング機能と連携し、抽出サーバ等のジョブの実行及び管理ができること。
ログ管理	(1) 次の各項目のログを本体部の内蔵HDDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア　ログイン及びログアウト履歴 イ　システムログ ウ　アプリケーションログ エ　セキュリティログ (2) 抽出サーバ等及びデータ交換装置のログを収集し共有ディスク装置へ保存すると共に、区分(システムログ、アプリケーションログ、セキュリティログ等)、発生時間、発生装置、キーワード等により、抽出、分析及び出力ができること。 (3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。
ネットワーク管理	抽出サーバ、ストレージＢ、各スイッチのMIB情報を収集する機能を有すること。
端末リモート操作サーバ	専用端末Ｂ及び試験端末Ｂの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末Ｂ及び試験端末ＢのOSへのログイン操作ができること。 (2) 専用端末Ｂ及び試験端末Ｂと監視サーバＢ間でクリップボードの情報を共有できること。 (3) 専用端末Ｂ及び試験端末Ｂと監視サーバＢ間でファイルの送受信ができること。
ソフトウェ	(1) 専用端末Ｂ等にインストールされたソフトウェア配信

	ア配信サーバ	クライアントソフトウェアに対して自動及び手動でソフトウェア及びソフトウェアのパッチを配信、適用ができること。このとき、配信開始時刻、転送速度制限、分割配信及び同時配信端末数の設定ができること。 (2) GUI又はWebブラウザによる管理コンソール機能を有し、スケジュール機能によりソフトウェアをインストールする時刻及び手順を一括、グループ別及び個別で設定できること。また、専用端末Ｂ等に対して次の動作が設定できること。 ア　端末の強制再起動及び強制シャットダウン イ　インストール時及び終了時の端末の権限設定の変更 ウ　インストール失敗時の動作設定 (3) (2)で設定したスケジュールは、設定情報として内蔵HDDに保存できること。また、保存した設定情報をスケジュールに反映できること。 (4) 専用端末Ｂ等からインストールの進行状況を自動及び手動で受信し、管理コンソール機能で表示でき、ログとして出力できること。 (5) 管理コンソール機能は、管理者権限が与えられた者のみが操作できるようアクセス権設定ができること。 (6) 待機系サーバへ機能を搭載すること。
	証跡収集	(1) 専用端末Ｂ等が生成した証跡を収集し、管理できること。 (2) 専用端末Ｂ等の要求により収集した証跡を送信し、検証ができること。
	定義ファイル配信	(1) 抽出サーバ等、専用端末Ｂ等及びデータ交換装置に対して、待機系サーバから配信先ごとのウイルス対策ソフトに対応するウイルス対策ソフトウェアの更新データを配信すること。 (2) ウイルス対策ソフトベンダーが提供する最新のウイルス定義ファイルを取得できること。 ウイルス対策ソフトウェアの更新データの取得方法については、警察庁と別途協議すること。
	ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。
	時刻同期	(1) １日１回以上、時刻同期装置と自動及び手動で時刻同

		期ができること。 (2) 専用端末Ｂ等及び各スイッチの時刻修正ができること。

4.1.7 バックアップサーバの機能及び性能は、 表- 10のとおりとする。

表- 10 バックアップサーバの機能及び性能

品目	項目	機能及び性能
本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。
	メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。 (2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。 (3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。 (4) サーバを停止せずに、HDDの交換ができること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを３個以上有すること。 (2) ネットワークは冗長構成ができること。 (3) ストレージＡ及びテープライブラリに接続するためのファイバチャネルポートを有すること。 (4) ストレージＡへの接続は冗長構成とし、各々のディスクコントローラで接続できること。 (5) 冗長構成としたファイバチャネルポートは、障害による自動閉塞機能、自動切替機能を有すること。
	電源ユニット	冗長構成であること。
バックアップ部		(1) RDX媒体を扱うことができること。 (2) １回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。
テープライブラリ部	テープライブラリ	(1) テープスロット数が20個以上であること。 (2) ライブラリ容量が30Ｔバイト（非圧縮）以上であること。

		(3) 本体部とファイバチャネルにより接続できること。
	テープドライブ	(1) LT05以上に対応したものを２台以上搭載すること。 (2) １台当たりのデータ転送速度は、最大140Mバイト/秒以上（非圧縮）であること。 (3) 暗号化については、次のとおりとする。 ア　警察庁が別途指示する政府推奨の暗号アルゴリズムにより暗号化した上で、電磁的記録媒体に記録できること。また、任意の周期で暗号鍵を変更できること。 イ　暗号化に使用した暗号鍵を電磁的記録媒体に記録できること。 ウ　暗号鍵生成のログが採取でき、暗号鍵を作成した年月日時分秒を確認できること。
ソフトウェア	OS	(1) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。 (2) 日本語に対応すること。
	プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。
	運用管理	(1) 本装置の本体部、バックアップ部及びテープライブラリ部の稼働状況を監視し、監視サーバＡの運用管理ソフトウェアに通知できること。 (2) 監視サーバＡの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携し、ジョブを実行できること。
	ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア　ログイン及びログアウト履歴 イ　システムログ ウ　アプリケーションログ エ　セキュリティログ (2) 監視サーバＡのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。 (3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。
	ネットワーク管理	監視サーバＡのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	データレプリケーション	(1) ストレージＡ内で、データベースを記録したボリュームの複製が作成できること。 (2) 業務に影響することなく、ストレージＡ内で複製ボリ

	ュームの作成及び切離しができること。
バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。 (2) サーバを停止せずに、内蔵HDDのバックアップができること。 (3) 監視サーバＡに収集されたログをテープライブラリ部の電磁的記録媒体にバックアップし、累積して管理できること。 (4) 業務に影響することなく、ストレージＡのデータベースをバックアップ及びリストアするため、次の機能を有すること。 ア　バックアップ (ｱ)　監視サーバＡの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携し、定められた時刻に自動及び任意の時刻に手動で、ストレージＡの複製ボリュームをオンラインから切離し、対象データをテープライブラリ部の電磁的記録媒体にバックアップできること。 (ｲ) バックアップデータは、日付、時刻及びバックアップの対象データを一意に識別できる名称で管理できること。 (ｳ) バックアップは、１世代当たり正・副とし、３世代の管理ができること。 イ　リストア (ｱ) オンラインから切離された複製ボリューム並びにデータの更新、追加、削除のログ及びその他必要な情報から、データベースを障害発生直前の状態までリストアできること。 (ｲ) (ｱ)によりリストアできない場合、テープライブラリ部の電磁的記録媒体に保存されたバックアップデータ及びその他必要な情報から、データベースをバックアップ取得時の状態までリストアできること。 (ｳ) データベースのリストアは、(4)ア(ｲ)の名称を指定してできること。 (5) 管理端末ＡからGUI又はWebブラウザにより、バックアップの設定及び監視ができること。
ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) ウイルス対策ソフトウェアの更新データを自動及び手

		動で更新できること。
	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。

4.1.8 ストレージＡの機能及び性能は、表- 11のとおりとする。

表- 11 ストレージＡの機能及び性能

品目	項目	機能及び性能
本体部	ディスクアレイ	(1) RAID1、RAID5又はRAID6の冗長構成とする。RAID構成後の実記憶容量については、警察庁の承認を得ること。 (2) (1)で決定した実記憶容量とは別に、HDD又はエンクロージャー等の増設により、取り扱う容量の拡張ができること。 (3) HDDのインタフェースは、SAS(Serial Attached SCSI)であること。 (4) 装置を停止せずにHDDの交換ができること。また、HDD障害時にホットスペアディスクを使用してRAID構成を自動で復旧できること。 (5) ホットスペアディスクを２個以上有すること。 なお、ホットスペアディスク２個以上の容量に相当するホットスペア専用の領域を、HDDに分散して有することも可とする。 (6) バックアップサーバと連携し、複製ボリュームの作成及び切離しができること。 (7) バックアップサーバと連携し、正常に一元バックアップできること。 (8) 本体部間でミラーリングができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを２個以上有すること。 (2) 業務サーバ、バックアップサーバ及び試験業務サーバを接続するため、ファイバチャネルポートを必要数搭載すること。 なお、接続に当たって、ファイバチャネルスイッチの利用も可とする。 (3) 業務サーバ、バックアップサーバ及び試験業務サーバへの接続は冗長構成とし、各々のディスクコントローラで接続できること。
	ネットワーク管理	監視サーバＡのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	電源ユニット	冗長構成であること。

	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。

4.1.9　ストレージＢの機能及び性能は、表- 12のとおりとする。

表- 12　ストレージＢの機能及び性能

品目	項目	機能及び性能
本体部	ディスクアレイ	(1) RAID1、RAID5又はRAID6の冗長構成とする。RAID構成後の実記憶容量については、警察庁の承認を得ること。 (2) (1)で決定した実記憶容量とは別に、HDD又はエンクロージャー等の増設により、取り扱う容量の拡張ができること。 (3) HDDのインタフェースは、SASであること。 (4) 装置を停止せずにHDDの交換ができること。また、HDD障害時にホットスペアディスクを使用してRAID構成を自動で復旧できること。 (5) ホットスペアディスクを２個以上有すること。なお、ホットスペアディスク２個以上の容量に相当するホットスペア専用の領域を、HDDに分散して有することも可とする。 (6) 抽出サーバと連携し、複製ボリュームの作成及び切離しができること。 (7) 抽出サーバと連携し、正常に一元バックアップできること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを２個以上有すること。 (2) 抽出サーバを接続するため、ファイバチャネルポートを必要数搭載すること。 なお、接続に当たって、ファイバチャネルスイッチの利用も可とする。 (3) 抽出サーバへの接続は冗長構成とし、各々のディスクコントローラで接続できること。
	ネットワーク管理	監視サーバＢのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	電源ユニット	冗長構成であること。
	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。

4.1.10　データ交換装置の機能及び性能は、表- 13のとおりとする。

表- 13　データ交換装置の機能及び性能

品目	項目	機能及び性能
本体部	データ交換機能	(1) 抽出サーバからFTPによりファイルを受信できること。 (2) 受信したファイルを、抽出サーバ等のネットワークから業務サーバ等のネットワークへの片方向に制限した転送ができること。 (3) 受信したファイルを業務サーバ及び試験業務サーバへFTPにより送信できること。 (4) 抽出サーバ等のネットワークと業務サーバ等のネットワーク間は、TCP/IPによるコネクションを確立しないこと。 (5) 抽出サーバ等のネットワークと業務サーバ等のネットワークがデータ交換を行う記録媒体には、抽出サーバ等のネットワークと業務サーバ等のネットワークから独立した制御系のコントロールにより、同時に接続できないこと。 (6) 抽出サーバ等のネットワークと業務サーバ等のネットワークがデータ交換を行う記録媒体には、アクセス制御により本装置以外からアクセスができないこと。 (7) データ交換の時間、間隔、回数等を任意に設定できること。 (8) 転送が完了した記録媒体上のファイルは、自動及び手動で削除できること。 (9) 転送容量として900Mバイト以上を１回の処理で転送できること。
	ネットワークインタフェース	(1) 抽出サーバ等のネットワークに1000BASE-T以上に対応するポートを２個以上有すること。 (2) 業務サーバ等のネットワークに1000BASE-T以上に対応するポートを２個以上有すること。 (3) ネットワークは冗長構成ができること。
	電源ユニット	冗長構成であること。
	運用管理	本装置の稼働状況を監視し、監視サーバＡ及び監視サーバＢの運用管理ソフトウェアに通知できること。
	ログ管理	(1) 次の各項目のログを、電磁的記録媒体に保存できること。 ア　ファイルの受信及び送信履歴 イ　システムメッセージ なお、ログの記録可能容量は30Mバイト以上とする。 (2) 監視サーバＡ及び監視サーバＢのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。

		(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。
	ネットワーク管理	監視サーバA及び監視サーバBのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。
	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。
その他		任意の時点で、システムファイルを電磁的記録媒体へバックアップができること。

4.1.11　時刻同期装置の機能及び性能は、表- 14のとおりとする。

表- 14　時刻同期装置の機能及び性能

品目	項目	機能及び性能
本体部	時刻同期機能	(1) FMラジオの時報を受信し、１日１回以上、内蔵時計の時刻修正を自動で行えること。 (2) 時刻修正の最大誤差は、日差±100ms以内であること。 (3) 時刻情報伝送プロトコルは、SNTP(Simple NetWork Time Protocol)及びNTP(Network Time Protocol)とし、警察庁サーバ、各ストレージ及び各スイッチの時刻修正ができること。 (4) うるう秒対応が自動又は手動で行えること。
	ネットワークインタフェース	100BASE-TX以上に対応するポートを有すること。

4.1.12　FWの機能及び性能は、表- 15のとおりとする。

表- 15　FWの機能及び性能

品目	項目	機能及び性能
本体部	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを２個以上有すること。 (2) ネットワークの冗長構成ができること。
	FW	(1) 最大スループットは、400Mbit/s以上であること。 (2) パケットフィルタリング機能を有すること。 (3) ISO/IEC 15408評価保証レベルにおいてCommonCriteria

		EAL3以上を取得していること。 (4) ステートフルインスペクション方式又はアプリケーションゲートウェイ方式であること。 (5) 特定の機器に対してアクセス制御できること。 (6) 最大同時セッション数は100,000以上であること。 (7) DynamicNAT、DynamicPAT及びStaticNATを有すること。 (8) アクティブ／スタンバイ型のクラスタ構成による冗長化ができること。
	管理コンソール機能	(1) GUI又はWebブラウザ画面を使用した管理、設定及び監視ができること。 (2) アクセスログを保存できること。 なお、保存する容量は、30Ｇバイト以上有すること。 (3) (1)及び(2)については、専用の端末装置等を利用することも可とする。
	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。

4.1.13　試験Webサーバの機能及び性能は、 表- 16のとおりとする。

表- 16　試験Webサーバの機能及び性能

品目	項目	機能及び性能
本体部	CPU	Webサーバに準ずる処理能力を有すること。
	メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。 (2) RAID構成後、本機器の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。 (3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。 (4) サーバを停止せずに、HDDの交換ができること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを５個以上有すること。 (2) ネットワークは冗長構成ができること。
	電源ユニット	冗長構成であること。

バックアップ部		(1) RDX媒体を扱うことができること。 (2) １回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。
ソフトウェア	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。 (2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。 (3) 日本語に対応すること。
	ディレクトリサービス	(1) 業務用プログラムの要求受け、必要なユーザ情報を送信できること。 (2) 日本語に対応すること。 (3) SSLオプションを搭載すること。 (4) 500ユーザ以上を登録できること。 (5) ユーザ情報を管理する、GUIによるインターフェースを有すること。 (6) アクセス権管理システムが採用するユーザーインターフェースと互換性を有すること。
	プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。
	バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。 (2) サーバを停止せずに、内蔵HDDのバックアップができること。
	運用管理	(1) 本装置の本体部及びバックアップ部の稼働状況を監視し、監視サーバＡの運用管理ソフトウェアに通知できること。 (2) 監視サーバＡの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携しジョブを実行できること。
	ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア　ログイン及びログアウト履歴 イ　システムログ ウ　アプリケーションログ エ　セキュリティログ オ　データベースへのアクセスログ (2) 監視サーバＡのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。 (3) 保存されたログは、管理者権限を与えられた者のみが

		閲覧できるよう閲覧権限を設定できること。
	ネットワーク管理	監視サーバＡのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) 監視サーバＡからウイルス対策ソフトウェアの更新データを受信できること。 (4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。
	時刻同期	１日１回以上、時刻同期装置と自動及び手動で時刻同期ができること。

4.1.14　試験業務サーバの機能及び性能は、表- 17のとおりとする。

表- 17　試験業務サーバの機能及び性能

品目	項目	機能及び性能
本体部	CPU	業務サーバに準ずる処理能力を有すること。
	メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。 (2) RAID構成後、本機器の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。 (3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。 (4) サーバを停止せずに、HDDの交換ができること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。
	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを３個以上有すること。 (2) ネットワークは冗長構成ができること。 (3) ストレージＡへ接続するためのファイバチャネルポートを４個以上有すること。 (4) ストレージＡへの接続は冗長構成とし、各々のディスクコントローラで接続できること。 (5) 冗長構成としたファイバチャネルについては、障害に

		よる自動閉塞機能及び自動切替機能を有すること。
	電源ユニット	冗長構成であること。
バックアップ部		(1) RDX媒体を扱うことができること。 (2) １回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。
ソフトウェア	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。 (2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。 (3) 日本語に対応すること。
	データベース管理	次の機能を有するソフトウェアを搭載すること。 (1) 別途調達する業務用プログラムが、SQL及びストアドプロシージャの実行及び結果の取得ができること。 (2) 複数のデータベースサーバから、同一のデータベースにアクセス可能なこと。 (3) データベースの性能情報、運用状況の統計を作成でき、分析できること。
	プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。
	バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。 (2) サーバを停止せずに、内蔵HDDのバックアップができること。
	運用管理	(1) 本装置の本体部及びバックアップ部の稼働状況を監視し、監視サーバＡの運用管理ソフトウェアに通知できること。 (2) 監視サーバＡの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携しジョブを実行できること。
	ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア　ログイン及びログアウト履歴 イ　システムログ ウ　アプリケーションログ エ　セキュリティログ オ　データベースへのアクセスログ (2) 監視サーバＡのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。

		(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。
	ネットワーク管理	監視サーバAのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) 監視サーバAからウイルス対策ソフトウェアの更新データを受信できること。 (4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。
	時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。

4.1.15 各端末の共通の機能及び性能は、表- 18のとおりとする。

表- 18 各端末の共通の機能及び性能

品目	項目	機能及び性能
ソフトウェア	バックアップ	OSがインストールされたドライブのバックアップができ、内蔵HDD交換後にバックアップ取得時の状態まで復旧できるリカバリ媒体を作成できること。
	ソフトウェア配信クライアント	(1) 監視サーバA又は監視サーバBのソフトウェア配信サーバソフトウェアからの要求により、自動及び手動でソフトウェア及びソフトウェアのパッチを監視サーバA又は監視サーバBからダウンロードできること。 (2) 手動及び監視サーバA又は監視サーバBのソフトウェア配信サーバソフトウェアが指定したスケジュールにより自動でソフトウェア及びソフトウェアのパッチをインストールし、必要に応じて自動で再起動ができること。 (3) インストール結果並びにハードウェア及びソフトウェアのシステム状況を自動及び監視サーバA又は監視サーバBの要求に応じて通知できること。 (4) ソフトウェアのインストール時は必要に応じて管理者権限で実行できること。 (5) インストール失敗時には失敗した時点及び最初から再インストールする機能を有すること。
	内蔵HDD暗号化	警察庁が別途指示する政府推奨の暗号化方式を使用すること。
	外部記録媒体暗号化	(1) 外部記録媒体へ情報を書き込む際は、自動的に情報を暗号化できること。また、外部記録媒体から暗号化され

		た情報を読み込む際に自動的に情報を復号できること。 なお、暗号化に用いる暗号鍵の更新は管理者権限を有する者のみが行えること。 (2) (1)の機能を用いない場合に備え、パスワードを用いて情報を暗号化及び平文による記録ができること。また、復号に用いるプログラムを配布できること。 (3) 警察庁が別途指示する政府推奨の暗号化方式を用いること。
	外部記録媒体利用制限	(1) 事前に許可された外部記録媒体以外の利用を制限できること。 (2) USB機器（USBメモリを含む。）について、ベンダID、プロダクトID及びシリアルナンバ等の情報を用いることにより、個別に使用の可否を制御する機能を有すること。 (3) 外部記録媒体の利用の許可を与える権限を有するユーザは、ユーザID、端末装置、期間（日時)、許可の種別（平文又は暗号文の別）の条件を指定の上、外部記録媒体の利用の可否を変更できること。また、設定時にコメントを付加できること。 (4) 光学ディスクドライブの使用可否について制限できる機能を有すること。
	証跡収集検証	(1) 外部記録媒体に対するファイル操作について、証跡の収集が行えること。 なお、証跡からファイル操作の年月日時分秒、ユーザID、ファイル名、ファイルサイズ及び平文又は暗号文の別を把握できること。 (2) (1)で収集した証跡を、監視サーバＡ又は監視サーバＢに送信できること。また、検証を行う際、監視サーバＡ又は監視サーバＢに送信した証跡を取得できること。 (3) (1)の証跡について、事前に指定されたユーザが検証できること。 (4) 外部記録媒体の利用の許可に係る証跡の収集が行えること。 なお、証跡から利用を許可した年月日時分秒、許可が終了する年月日時分秒、許可の内容（平文、暗号文の別)、許可をしたユーザID、許可を受けたユーザID及びコメントについて把握できること。 (5) (4)で収集した証跡を、監視サーバＡ又は監視サーバＢに送信できること。また、検証を行う際、監視サーバＡ又は監視サーバＢに送信した証跡を取得できること。 (6) (4)の証跡について、事前に指定されたユーザが検証で

		きること。
	ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。 (2) ファイルアクセス時に自動でウイルスチェックができること。 (3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。
	時刻同期	(1) OS起動時に、監視サーバＡ又は監視サーバＢと自動で時刻同期ができること。 (2) 起動中については、前回調整時から24時間に１回以上、監視サーバＡ又は監視サーバＢと自動で時刻同期ができること。また、任意の時点で手動による時刻同期ができること。

4.1.16　専用端末Ａ及び試験端末Ａの機能及び性能は、表- 19のとおりとする。

表- 19　業務端末Ａ及び試験端末Ａの機能及び性能

品目	項目	機能及び性能
本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。
	メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。 (2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。
	ネットワークインタフェース	10BASE-T/100BASE-TX/1000BASE-Tに対応するポートを有すること。
	USBインタフェース	(1) USB3.0以上に対応するポートを有すること。 (2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを１ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。

	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。 (2) 表示色は、1,677万色以上であること。
	キーボード	JIS規格キー配列に準拠していること。
	マウス	(1) ２ボタン式以上の光学式又はレーザー式であること。 (2) ホイール等によりマウスを移動せずに画面のスクロールができること。
	バッテリ	(1) パック方式で、交換可能な内蔵バッテリであること。 (2) バッテリ稼働時間は、社団法人電子情報技術産業協会「JEITAバッテリ動作時間測定法(Ver1.0)」準拠において、カタログ値で１時間以上であること。
認証部	生体認証ユニット	(1) USBにより、本体部と接続できること。 (2) 非接触型の読み取り装置であること。 (3) 他人許容率0.0002%以下かつ本人拒否率0.05%以下であること。 (4) 業務用プログラムと連携して、生体認証ができること。
ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。
	アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 業務用プログラムが作成する帳票を、表示及び印刷できること。 (2) 業務用プログラム起動中、日本語から繁体字及び簡体字に入力の切替ができること。 (3) 業務用プログラム起動中、日本語からハングルに入力の切替ができること。
	端末リモート操作クライアント	(1) 監視サーバA、管理端末A及びコンソール端末Aの端末リモート操作サーバソフトウェアからリモート操作を受け付けること。 (2) OS起動時にユーザーの操作とは無関係にバックグラウンドで自動的に開始できること。

4.1.17　専用端末Ｂ及び試験端末Ｂの機能及び性能は、表- 20のとおりとする。

表- 20　専用端末Ｂ及び試験端末Ｂの機能及び性能

品目	項目	機能及び性能
本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。
	メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。

		(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。 (2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。
	ネットワークインタフェース	10BASE-T/100BASE-TX/1000BASE-Tに対応するポートを有すること。
	USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。 (2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを１ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。
	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。 (2) 表示色は、1,677万色以上であること。
	キーボード	JIS規格キー配列に準拠していること。
	マウス	(1) ２ボタン式以上の光学式又はレーザー式であること。 (2) ホイール等によりマウスを移動せずに画面のスクロールができること。
	バッテリ	(1) パック方式で、交換可能な内蔵バッテリであること。 (2) バッテリ稼働時間は、社団法人電子情報技術産業協会「JEITAバッテリ動作時間測定法(Ver1.0)」準拠において、カタログ値で１時間以上であること。
認証部	生体認証ユニット	(1) USBにより、本体部と接続できること。 (2) 非接触型の読み取り装置であること。 (3) 他人許容率0.0002%以下かつ本人拒否率0.05%以下であること。 (4) 業務用プログラムと連携して、生体認証ができること。
ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。
	アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 ・ 業務用プログラムが作成する帳票を、表示及び印刷できること。

	端末リモート操作クライアント	(1) 監視サーバB、管理端末B及びコンソール端末Bの端末リモート操作サーバソフトウェアからリモート操作を受け付けること。 (2) OS起動時にユーザーの操作とは無関係にバックグラウンドで自動的に開始できること。

4.1.18　管理端末Aの機能及び性能は、表- 21のとおりとする。

表- 21　管理端末Aの機能及び性能

品目	項目	機能及び性能
本体部	CPU	(1) 統合監視、ストレージ管理及び運用管理のソフトウェアが同時に起動できること。 (2) 同時に14個のWebブラウザ及びXサーバを起動して、安定稼働ができること。 (3) (1)、(2)を同時に起動しながら、業務プログラムがプログラム仕様書の性能要件を満たす処理能力を有すること。
	メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。 (2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。
	光学ドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。
	ネットワークインタフェース	1000BASE-T以上に対応するポートを２個以上有すること。
	USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。 (2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを１ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。
表示部	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。 (2) 表示色は、1,677万色以上であること。
操作部	キーボード	JIS規格キー配列に準拠していること。

	マウス	(1) ２ボタン式以上の光学式又はレーザー式であること。 (2) ホイール等によりマウスを移動せずに画面のスクロールができること。
認証部	生体認証ユニット	(1) USBにより、本体部と接続できること。 (2) 非接触型の読み取り装置であること。 (3) 他人許容率0.0002%以下かつ本人拒否率0.05%以下であること。 (4) 業務用プログラムと連携して、生体認証ができること。
ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。
	警報装置制御	警報装置の音声ファイルの再生、ブザーの鳴動及び表示灯の点滅を制御できること。
	Webブラウザ	WebGUIを使用して設定等作業を行う機器及びソフトウェアの仕様を満たすこと。
	アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 警察庁が指示する形式のファイルを入出力できる表計算ソフト (2) 業務サーバ等が使用する文字コードに対応するテキストエディタ (3) 業務用プログラムが作成する帳票を、表示及び印刷できる画像表示ソフト
	ファイル圧縮展開	(1) CAB形式、ZIP形式及びTAR形式で複数ファイル及びディレクトリを圧縮して１つのファイルに格納できること。 (2) CAB形式、ZIP形式、TAR形式及びZ形式のファイルを展開できること。 (3) CAB形式及びZIP形式の自己解凍型圧縮ファイルが作成できること。 (4) GUIにより操作ができること。
	ユーザ管理	(1) Webサーバ及び試験Webサーバのディレクトリサービスと連携して、ユーザ情報の登録・削除・編集・検索がGUI又はWebブラウザで行えること。 (2) ユーザ情報の登録は一括で行えること。 (3) ユーザ情報をGUI又はWebブラウザの操作でファイル出力できること。 (4) ユーザ情報の操作ログをGUI又はWebブラウザの操作で出力できること。
	Xサーバ	(1) X11R7以上に対応すること。 (2) 日本語に対応すること。

		(3) 業務サーバ等のOSに対応すること。
	統合監視	(1) 業務統合監視機能 監視サーバＡの統合監視ソフトウェアと連携し、監視目的別に業務状況(運用管理、ログ管理、ネットワーク管理､ストレージ管理及び性能管理)を監視することができ、かつ、監視画面から各機能の監視画面に遷移し、階層を掘り下げることにより障害箇所を特定できること。 (2) コマンド制御機能 コマンドを業務サーバ等へ発行できること。また、発行したコマンド及び受信メッセージの履歴を照会できること。 (3) メッセージ監視機能 監視サーバＡから通知されたメッセージについて、メッセージごとに内容説明や処置方法を日本語で表示及び印字できること。
	ストレージ管理	ストレージＡの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報（HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報）をGUI又はWebブラウザで表示できること。 (2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。 (3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。 (4) メッセージにより、ストレージＡのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。
	運用管理	監視サーバＡの運用管理ソフトウェアと連携し、外部サーバのジョブの実行及び管理ができること。
	端末リモート操作サーバ	専用端末Ａ及び試験端末Ａの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末Ａ及び専用端末ＡのOSへのログイン操作ができること。 (2) 専用端末Ａ及び試験端末Ａと管理端末Ａ間でクリップボードの情報を共有できること。 (3) 専用端末Ａ及び試験端末Ａと管理端末Ａ間でファイルの送受信ができること。

4.1.19　管理端末Ｂの機能及び性能は、表- 22のとおりとする。

表- 22　管理端末Ｂの機能及び性能

品目	項目	機能及び性能
本体部	CPU	(1) 統合監視、ストレージ管理及び運用管理のソフトウェアが同時に起動できること。 (2) 同時に８個のWebブラウザ及びXサーバを起動して、安定稼働ができること。 (3) (1)、(2)を同時に起動しながら、業務プログラムがプログラム仕様書の性能要件を満たす処理能力を有すること。
	メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。 (2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。
	ネットワークインタフェース	1000BASE-T以上に対応するポートを２個以上有すること。
	USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。 (2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを１ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。
表示部	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。 (2) 表示色は、1,677万色以上であること。
操作部	キーボード	JIS規格キー配列に準拠していること。
	マウス	(1) ２ボタン式以上の光学式又はレーザー式であること。 (2) ホイール等によりマウスを移動せずに画面のスクロールができること。
認証部	生体認証ユニット	(1) USBにより、本体部と接続できること。 (2) 非接触型の読み取り装置であること。 (3) 他人許容率0.0002%以下かつ本人拒否率0.05%以下であること。 (4) 業務用プログラムと連携して、生体認証ができること。

ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。
	警報装置制御	警報装置の音声ファイルの再生、ブザーの鳴動及び表示灯の点滅を制御できること。
	Webブラウザ	(1) 日本語に対応すること。 (2) WebGUIを使用して設定等作業を行う機器及びソフトウェアの仕様を満たすこと。
	アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 警察庁が指示する形式のファイルを入出力できる表計算ソフト (2) 抽出サーバ等が使用する文字コードに対応するテキストエディタ (3) 業務用プログラムが作成する帳票を、表示及び印刷できる画像表示ソフト
	ファイル圧縮展開	(1) CAB形式、ZIP形式及びTAR形式で複数ファイル及びディレクトリを圧縮して１つのファイルに格納できること。 (2) CAB形式、ZIP形式、TAR形式及びZ形式のファイルを展開できること。 (3) CAB形式及びZIP形式の自己解凍型圧縮ファイルが作成できること。 (4) GUIにより操作ができること。
	Xサーバ	(1) X11R7以上に対応すること。 (2) 日本語に対応すること。 (3) 抽出サーバ等のOSに対応すること。
	統合監視	(1) 業務統合監視機能 監視サーバＢの統合監視ソフトウェアと連携し、監視目的別に業務状況（運用管理、ログ管理、ネットワーク管理、ストレージ管理及び性能管理）を監視することができ、かつ、監視画面から各機能の監視画面に遷移し、階層を掘り下げることにより障害箇所を特定できること。 (2) コマンド制御機能 コマンドを抽出サーバ等へ発行できること。また、発行したコマンド及び受信メッセージの履歴を照会できること。 (3) メッセージ監視機能 監視サーバＢから通知されたメッセージについて、メッセージごとに内容説明や処置方法を日本語で表示及び印字できること。

	ストレージ管理	ストレージＢの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報（HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報）をGUI又はWebブラウザで表示できること。 (2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。 (3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。 (4) メッセージにより、ストレージＢのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。
	運用管理	監視サーバＢの運用管理ソフトウェアと連携し、内部サーバのジョブの実行及び管理ができること。
	端末リモート操作サーバ	専用端末Ｂ及び試験端末Ｂの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末Ｂ及び試験端末ＢのOSへのログイン操作ができること。 (2) 専用端末Ｂ及び試験端末Ｂと管理端末Ｂ間でクリップボードの情報を共有できること。 (3) 専用端末Ｂ及び試験端末Ｂと管理端末Ｂ間でファイルの送受信ができること。

4.1.20　コンソール端末Ａの機能及び性能は、表- 23のとおりとする。

表- 23　コンソール端末Ａの機能及び性能

品目	項目	機能及び性能
本体部	CPU	同時に14個のWebブラウザ及びXサーバを起動して、安定稼働ができること。
	メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。 なお、Webブラウザ及びXサーバは、同時に14個を起動できること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。 (2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。

	光学ドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。
	ネットワークインタフェース	1000BASE-T以上に対応するポートを２個以上有すること。
	USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。 (2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを１ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。
表示部	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。 (2) 表示色は、1,677万色以上であること。
操作部	キーボード	JIS規格キー配列に準拠していること。
	マウス	(1) ２ボタン式以上の光学式又はレーザー式であること。 (2) ホイール等によりマウスを移動せずに画面のスクロールができること。
ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。
	Webブラウザ	(1) 日本語に対応すること。 (2) WebGUIを使用して設定等作業を行う機器及びソフトウェアの仕様を満たすこと。
	アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 警察庁が指示する形式のファイルを入出力できる表計算ソフト (2) 業務サーバ等が使用する文字コードに対応するテキストエディタ (3) 30Mバイト以上ログファイルを取り扱えられるテキストエディタ
	Xサーバ	(1) X11R7以上に対応すること。 (2) 日本語に対応すること。 (3) 業務サーバ等のOSに対応すること。
	ストレージ管理	ストレージAの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報（HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報）をGUI又はWebブラウザで表示できること。 (2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。

		(3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。 (4) メッセージにより、ストレージAのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。
	端末リモート操作サーバ	専用端末A及び試験端末Aの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末A及び試験端末AのOSへのログイン操作ができること。 (2) 専用端末A及び試験端末Aとコンソール端末A間でクリップボードの情報を共有できること。 (3) 専用端末A及び試験端末Aとコンソール端末A間でファイルの送受信ができること。

4.1.21　コンソール端末Bの機能及び性能は、表- 24のとおりとする。

表- 24　コンソール端末Bの機能及び性能

品目	項目	機能及び性能
本体部	CPU	同時に8個のWebブラウザ及びXサーバを起動して、安定稼働ができること。
	メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。 なお、Webブラウザ及びXサーバは、同時に8個を起動できること。 (2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。
	内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。 (2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。
	光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。
	ネットワークインタフェース	1000BASE-T以上に対応するポートを2個以上有すること。
	USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。 (2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを1ポート以

		上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。
表示部	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。 (2) 表示色は、1,677万色以上であること。
操作部	キーボード	JIS規格キー配列に準拠していること。
	マウス	(1) ２ボタン式以上の光学式又はレーザー式であること。 (2) ホイール等によりマウスを移動せずに画面のスクロールができること。
ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。
	Webブラウザ	(1) 日本語に対応すること。 (2) WebGUIを使用して設定等作業を行う機器及びソフトウェアの仕様を満たすこと。
	アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 警察庁が指示する形式のファイルを入出力できる表計算ソフト (2) 抽出サーバ等が使用する文字コードに対応するテキストエディタ (3) 30Mバイト以上ログファイルを取り扱えられるテキストエディタ
	Xサーバ	(1) X11R7以上に対応すること。 (2) 日本語に対応すること。 (3) 抽出サーバ等のOSに対応すること。
	ストレージ管理	ストレージＢの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報（HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報）をGUI又はWebブラウザで表示できること。 (2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。 (3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。 (4) メッセージにより、ストレージＢのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。
	端末リモート操作サー	専用端末Ｂ及び試験端末Ｂの端末リモート操作クイアントソフトウェアと連携して次の操作ができること。

	バ	(1) 専用端末Ｂ及び試験端末ＢのOSへのログイン操作ができること。 (2) 専用端末Ｂ及び試験端末Ｂとコンソール端末Ｂ間でクリップボードの情報を共有できること。 (3) 専用端末Ｂ及び試験端末Ｂとコンソール端末Ｂ間でファイルの送受信ができること。

4.1.22　警報装置の機能及び性能は、表- 25のとおりとする。

表- 25　警報装置の機能及び性能

品目	項目	機能及び性能
本体部	基本機能	(1) 音声ファイルの再生、ブザーの鳴動及び表示灯の点滅を、警察庁サーバ及び端末等から制御できること。 なお、再生、鳴動及び点滅パターンについては、警察庁と協議すること。 (2) 警察庁サーバから要求により、鳴動及び点滅の状態を回答できること。 (3) 20個以上の音声ファイルが登録でき、再生できること。 (4) 音量調整ができること。 (5) ボタンの操作により、点滅、鳴動及び再生を停止できること。 (6) 表示灯は、赤、黄及び緑の３色とすること。
	ネットワークインターフェース	10BASE-T/100BASE-TX以上に対応するポートを有し、ネットワーク接続ができること。
	時刻同期	24時間に１回以上、監視サーバＡ又は監視サーバＢと自動で時刻同期ができること。

4.1.23　スキャナの機能及び性能は、表- 26のとおりとする。

表- 26　スキャナの機能及び性能

品目	項目	機能及び性能
本体部	基本機能	(1) カラー読み取りができること。 (2) 最大読取原稿サイズは、A4サイズであること。 (3) 最高光学解像度は、1,200×1,200dpi以上であること。 (4) 読取速度は、A4原稿モノクロで読取解像度が600dpiの場合５ms/line以上であること。また、A4原稿カラーで読取解像度が600dpiの場合５ms/line以上であること。 (5) USB2.0以上に対応するインタフェースで、専用端末及び試験端末に接続できること。 (6) TWAIN対応であること。

4.1.24　印字装置の機能及び性能は、表- 27のとおりとする。

表- 27　印字装置の機能及び性能

品目	項目	機能及び性能
本体部	基本機能	(1) レーザープリンタ(モノクロ)であること。 (2) 各端末からTCP/IPを利用して印字できること。 (3) 用紙は、普通紙単票のA4サイズに対応すること。 (4) 解像度が600×600dpi以上で印字できること。 (5) A4で20枚/分以上の印字速度であること。 (6) 200枚以上の自動給紙が可能なカセットを有すること。
	ネットワークインターフェース	(1) 10BASE-T/100BASE-TXに対応するポートを有すること。 (2) 無線LAN機能を標準で搭載している場合は、 無線LAN機能を停止できること。 なお、利用者による設定変更ができないこと。
	その他	電磁的記録媒体への入出力機能を有しないこと。

4.1.25　L3SWの機能及び性能は、表- 28のとおりとする。

表- 28　L3SWの機能及び性能

品目	項目	機能及び性能
本体部	基本機能	(1) 24Gbit/s以上のスイッチング容量を有すること。 (2) レイヤ２及びレイヤ３におけるスイッチング処理能力が12Mパケット/s以上であること。 (3) 各ポート単位にスイッチング、ルーティングができること。 (4) 各ポートの稼働状態を表示するLEDを有すること。 (5) RFC2338に準拠したVRRP(Virtual Router Redundancy Protocol)機能又はHSRP(HotStandby Router Protocol)機能を有すること。 (6) ルーティングプロトコルはRIP(Routing Infomation Protocol)ver1、RIPver2及びOSPF(Open Shortest Path First)が使用できること。 (7) RIP、OSPF間において相互の情報交換ができること。 (8) 静的な経路設定ができること。 (9) MACアドレス、IPアドレス及びTCP/UDPポート番号によるフィルタリングができること。 (10) ポートベースVLAN機能を有すること。 (11) IEEE802.1qに準拠したVLANタギング機能を有すること。 (12) IEEE802.1dに準拠したスパニングツリー機能を有し、VLAN単位に動作すること。 (13) IEEE802.3adに準拠したリンクアグリゲーション機能

		を有すること。 (14) IPアドレス、論理ポート等により、データ入出力の可否を制御できること。
	ネットワークインタフェース	(1) 1000BASE-T以上のポートを24個以上有すること。 (2) ネットワークは冗長構成とし、切替えが任意にできること。
	ネットワーク管理	(1) 監視サーバＡ又は監視サーバＢのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。 (2) RMON (Remote Network Monitoring) に対応すること。
	時刻同期	１日１回以上、時刻同期装置又は監視サーバＡと自動及び手動で時刻同期ができること。
	電源ユニット	冗長構成であること。
	バックアップ	(1) 装置内の各モジュールの構成情報データ及びソフトウェアを電磁的記録媒体に保持し、電源のオン／オフ時及び各モジュール交換後の再設定が不要であること。 (2) 各設定情報をファイルに保存及び読み込みができること。

4.1.26　ハブＩの機能及び性能は、表- 29のとおりとする。

表- 29　ハブＩの機能及び性能

品目	項目	機能及び性能
本体部	ネットワークインタフェース	(1) 16Gbit/s以上のスイッチング容量を有すること。 (2) 1000BASE-T以上に対応する自動認識ポートを16個以上有すること。 (3) ネットワークは冗長構成ができること。 (4) ストア及びフォワード方式によるパケットスイッチング機能を有すること。 (5) 各ポートの稼働状態を表示するLEDを有すること。 (6) ８グループ以上設定可能なVLAN機能を有すること。 (7) VLAN単位ごとに、IEEE802.1dに準拠したスパニングツリー機能を有すること。 (8) IEEE802.3adに準拠したリンクアグリゲーション機能を有すること。
	ネットワーク管理	監視サーバＡ又は監視サーバＢのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。
	時刻同期	１日１回以上、時刻同期装置又は監視サーバＡと自動及び手動で時刻同期ができること。

４．２　外部インタフェース要件

警察庁サーバにおいて、下記の通信プロトコル用いた通信機能を有すること。

4.2.1　Webサーバ及び試験Webサーバ

HTTPS、LDAP

4.2.2　業務サーバ及び試験業務サーバ

FTP、SMTP、POP3、HTTP

4.2.3　抽出サーバ

FTP、RCP、HTTPS、LDAPv3

4.2.4　データ交換装置

FTP

５　規模要件

５．１　警察庁サーバ、負荷分散装置、データ交換装置、各ストレージ、FW、時刻同期装置、各端末、警報装置、スキャナ、印字装置、各スイッチ及びラックは、東京都23区内の警察庁が別途指示する場所に設置する。

５．２　専用端末、警報装置、スキャナ及び印字装置は、警察庁及び都道府県警察にそれぞれ１台以上を警察庁が別途指示する場所に設置する。

６　信頼性等要件

６．１　信頼性要件

6.1.1　可用性

(1)　警察庁サーバ（バックアップサーバを除く。）は、クラスタ構成又は冗長構成とすること。また、負荷分散装置、FW及び各スイッチ（端末を接続するものを除く。）についても複数台構成とすること。

(2)　警察庁サーバ及び各ストレージは、稼働中にHDD及び電源ユニットの部品を交換できること。

(3)　ネットワークは冗長構成とし、任意に切替えができること。

(4)　クラスタ構成又は冗長構成としているハードウェアの障害時においても、業務の継続運用ができること。

(5)　警察庁サーバのネットワークインタフェースは、単一障害点（Single Pointof Failure）のないハードウェア構成とすること。ただし、コンソール端末及びテープライブラリと接続するものを除く。

(6)　本システムで調達する機器のうち５．１項で指定する機器については、２系統ある電源の片系統が電源設備点検等で供給できない場合にも、電源ユニットの冗長化や無瞬断切替装置等により業務の継続運用ができること。

(7) 稼働率は、システムの稼働により業務が正常に動作している時間の割合をいい、クラスタ構成等のハードウェア障害時において、業務が継続運用できる場合は稼働しているものとし、また、計画停止など契約業者の責に依らない停止は考慮しないものとする。

本システムにおいては、目標稼働率をWebサーバ、業務サーバ、ストレージA及び負荷分散装置並びに付随する各スイッチで運用する業務に適用する。

なお、本仕様書で構築するシステムが目標とする稼働率（目標とする稼働率）を表- 30に示す。

表- 30　システムの稼働率

システム名	目標とする稼働率
事前旅客情報システム及び 外国人個人識別情報認証システム	99.99%

6.1.2　完全性

(1)　警察庁サーバ及び各ストレージのデータについては、バックアップサーバと連携し自動的にバックアップが取得できること。また、取得したバックアップを用いて、バックアップ取得時の状態に復元ができること。

(2)　データベース破損時には、データの更新、追加、削除のログ及びその他必要な情報により、直前の状態に復元ができること。

(3)　警察庁サーバについて、任意のタイミングでバックアップの取得ができ、取得したバックアップを用いて、バックアップ取得時の状態に復元ができること。

(4)　FW及び各スイッチについて、任意のタイミングで設定ファイルの取得ができ、取得した設定ファイルを用いて、設定ファイル取得時の状態に復元ができること。

(5)　各端末について、内蔵HDDのバックアップが取得でき、取得したバックアップを用いて、バックアップ取得時の状態に復元ができること。

6.1.3　機密性

(1)　警察庁サーバ、負荷分散装置、データ交換装置、各ストレージ、FW、時刻同期装置、各スイッチ及び各端末のソフトウェアにおいてパッチが必要となった場合は、速やかに警察庁に報告し、その指示に従い対応すること。

(2)　バックアップサーバのテープライブラリ部において、電磁的記録媒体へデータの書き込みを行う際は、暗号化すること。

(3)　各端末から外部記録媒体へデータの書き込みを行う際は､暗号化すること。

(4)　各端末の内蔵HDDは、全体を暗号化できること。

6．2　拡張性要件

将来の業務追加及びデータ増加に伴う容量、処理速度等に対応できるよう装置の拡張性を確保すること。

6．3　システム中立性要件

特定の事業者にしか取り扱うことができない製品や技術に依存しないこと。

6．4　事業継続性要件

6.1.1項参照。

7　情報セキュリティ要件

7．1　権限要件

7.1.1　警察庁サーバ、各ストレージ及び各スイッチのソフトウェア等の構成品について、管理者権限、保守ユーザ権限及び業務ユーザ権限を設定できること。

なお、権限設定を行う構成品及び権限内容について、警察庁と協議すること。

7.1.2　各端末のOS及び内蔵HDD暗号化ソフトウェアについては、管理者権限及び一般ユーザ権限を設定できること。

7．2　ウイルス定義ファイルの更新

ウイルス対策については、監視サーバＡ又は監視サーバＢから警察庁サーバ、データ交換装置及び各端末にウイルス対策ソフトウェアの更新データを随時配信し、ウイルス定義ファイル及びウイルス検索エンジン等を更新できること。

8　情報システム稼働環境

8．1　使用条件

8.1.1　本システムは、次の使用条件で異常なく動作すること。

温　　度　　10~32℃

湿　　度　　30~80％（結露しない状態）

電源電圧　　ア　警察庁サーバ、各ストレージ及びデータ交換装置は、ＡＣ200~220Ｖ（50／60Hz）又はＡＣ100~110Ｖ（50／60Hz）とする。

イ　負荷分散装置、FW、時刻同期装置、各端末、警報装置、スキャナ、印字装置及び各スイッチは、ＡＣ100~110Ｖ（50／60Hz）とする。

8.1.2　本システムは、24時間連続運用に耐えられる設計であること。

8.1.3　警察庁サーバ、各ストレージ、各スイッチ及びデータ交換装置は、帯電防止対策及び電源投入・切断に関する保護対策が十分にとられていること。

8．2　全体構成

警察庁が想定する全体構成については、別紙２「ハードウェア構成図」のとおり。

8．3　ハードウェア構成

8.3.1　ハードウェア構成

(1)　共通事項

ア　同一品名の機器は同一機種とする。

イ　本システムの構築に当たっては別紙２「ハードウェア構成図」を参考とし、必要なネットワーク機器等を全て準備すること。

ウ　構成機器構築説明書については、各機器のホスト名、IPアドレス、ユーザアカウント、ネットワーク構成図、OSインストール時の設定情報、システム構築に係る情報とする。

(2)　クラスタ構成を組むサーバにあっては、１台のサーバ内でCPU、メモリ等の資源を物理的に複数に分割する、または仮想化技術により、複数のアプリ

ケーションのパフォーマンスを低下させることなく異なるサーバの機能を同時に稼働させる構成も可とする。

(3) 負荷分散装置の構成及び構造は、表- 31のとおりとする。

表- 31 負荷分散装置の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	2	式	ラックに搭載できること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

(4) Webサーバの構成及び構造は、表- 32のとおりとする。

表- 32 Webサーバの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	2	式	(1) クラスタ構成であること。 (2) ラックに搭載できること。
	バックアップ部	2	式	ラックに搭載できること。
	ソフトウェア	2	式	
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	
	バックアップ手順書	1	式	
	リストア手順書	1	式	

(5) 業務サーバの構成及び構造は、表- 33のとおりとする。

表- 33 業務サーバの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	2	式	(1) クラスタ構成であること。 (2) ラックに搭載できること。
	バックアップ部	2	式	ラックに搭載できること。
	ソフトウェア	2	式	
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。

	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	
	バックアップ手順書	1	式	
	リストア手順書	1	式	

(6)　抽出サーバの構成及び構造は、表- 34のとおりとする。

表- 34　抽出サーバの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	2	式	(1) クラスタ構成であること。 (2) ラックに搭載できること。
	バックアップ部	2	式	ラックに搭載できること。
	テープライブラリ部	1	式	ラックに搭載できること。
	ソフトウェア１	2	式	
	ソフトウェア２	1	式	
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	
	バックアップ手順書	1	式	
	リストア手順書	1	式	

(7)　監視サーバＡ及び監視サーバＢの構成及び構造は、表- 35とおりとする。

表- 35　監視サーバＡ及監視サーバＢの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	2	式	(1) クラスタ構成であること。 (2) ラックに搭載できること。
	コンソール部	1	式	(1) ラックに搭載できること。 (2) 15型以上のTFTカラー液晶ディスプレイであること。
	バックアップ部	2	式	ラックに搭載できること。
	ソフトウェア	2	式	
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	

	バックアップ手順書	1	式	
	リストア手順書	1	式	

(8)　バックアップサーバの構成及び構造は、表- 36とおりとする。

表- 36　バックアップサーバの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	ラックに搭載できること。
	バックアップ部	1	式	ラックに搭載できること。
	テープライブラリ部	1	式	ラックに搭載できること。
	ソフトウェア	1	式	
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	
	バックアップ手順書	1	式	
	リストア手順書	1	式	

(9)　ストレージＡの構成及び構造は、表- 37とおりとする。

表- 37　ストレージＡの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	2	式	ラックに搭載できること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

(10)　ストレージＢの構成及び構造は、表- 38とおりとする。

表- 38　びストレージＢの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	ラックに搭載できること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

(11)　データ交換装置の構成及び構造は、表- 39とおりとする。

表- 39　データ交換装置の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	ラックに搭載できること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

(12)　時刻同期装置の構成及び構造は、表- 40とおりとする。

表- 40　時刻同期装置の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	ラックに搭載できること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

(13)　FWの構成及び構造は、表- 41とおりとする。

表- 41　FWの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	2	式	ラックに搭載できること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

(14)　試験Webサーバの構成及び構造は、表- 42のとおりとする。

表- 42　試験Webサーバの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	ラックに搭載できること。
	バックアップ部	1	式	ラックに搭載できること。
	ソフトウェア	1	式	
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

	インストール手順書	1	式	
	バックアップ手順書	1	式	
	リストア手順書	1	式	

(15)　試験業務サーバの構成及び構造は、表- 43のとおりとする。

表- 43　試験業務サーバの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	ラックに搭載できること。
	バックアップ部	1	式	ラックに搭載できること。
	ソフトウェア	1	式	
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	
	バックアップ手順書	1	式	
	リストア手順書	1	式	

(16)　専用端末の構成及び構造は、　表- 44のとおりとする。

表- 44　専用端末の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) ノート型であること。 (2) 15型以上のカラー液晶ディスプレイであること。 (3) 盗難防止用セキュリティスロットを有すること。 (4) 質量は、５kg以下であること。また、最大消費電力は、100W以下であること。 (5) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 なお、２極接地極付プラグを有する場合は、２極に変換できるプラグを付属すること。
	認証部	1	式	USB接続であること。
	ソフトウェア	1	式	
付属品	接続ケーブル	1	式	機器の接続に必要なケーブ

				ルを付属すること。
	セキュリティワイヤー	1	式	(1) 錠を有し、鍵は２個以上有すること。 (2) 錠は、本体部の盗難防止用セキュリティスロットに取り付けることができること。 (3) ワイヤーの太さは、4.0㎜以上であること。また、長さは、1.5m以上2.5m以下であること。 (4) マウスを盗難防止の目的で取り付けられる構造であること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	
	OAタップ	1	式	(1) 構成機器を収容する口数及び容量を有すること。 (2) 長さは３m以上であること。 (3) 磁石、両面テープ又はネジにより固定できること。 (4) 電源コンセントの形状は、２極コンセント又は２極接地極付コンセントであること。 なお、２極接地極付コンセントを有する場合は、２極に変換できるプラグを付属すること。

(17) 試験端末の構成及び構造は、 表- 45のとおりとする。

表- 45 試験端末の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) ノート型であること。 (2) 15型以上のカラー液晶ディスプレイであること。 (3) 盗難防止用セキュリティ

				スロットを有すること。 (4) 質量は、５kg以下であること。また、最大消費電力は、100W以下であること。 (5) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 なお、２極接地極付プラグを有する場合は、２極に変換できるプラグを付属すること。
	認証部	1	式	USB接続であること。
	ソフトウェア	1	式	
	操作卓	1	式	(1) 次の機器が搭載できる必要最小限のサイズであること。 ア　本体部 イ　認証部 ウ　警報装置 エ　スキャナ (2) OAチェア付きであること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
	セキュリティワイヤー	1	式	(1) 錠を有し、鍵は２個以上有すること。 (2) 錠は、本体部の盗難防止用セキュリティスロットに取り付けることができること。 (3) ワイヤーの太さは、4.0mm以上であること。また、長さは、1.5m以上2.5m以下であること。 (4) マウスを盗難防止の目的で取り付けられる構造であること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	

	OAタップ	1	式	(1) 構成機器を収容する口数及び容量を有すること。 (2) 長さは３ｍ以上であること。 (3) 磁石、両面テープ又はネジにより固定できること。 (4) 電源コンセントの形状は、２極コンセント又は２極接地極付コンセントであること。 なお、２極接地極付コンセントを有する場合は、２極に変換できるプラグを付属すること。

(18) 管理端末の構成及び構造は、表- 46のとおりとする。

表- 46 管理端末の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) デスクトップ型であること。 (2) 盗難防止用セキュリティスロットを有すること。 (3) 質量は、10kg以下であること。また、最大消費電力は、300W以下であること。 (4) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 なお、２極接地極付プラグを有する場合は、２極に変換できるプラグを付属すること。
	表示部	1	式	(1) 19型以上のカラー液晶ディスプレイであること。 (2) 質量は、10kg以下であること。また、最大消費電力は、150W以下であること。 (3) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。

				なお、２極接地極付プラグを有する場合は、２極に変換できるプラグを付属すること。
	操作部	1	式	
	認証部	1	式	USB接続であること。
	ソフトウェア	1	式	
	操作卓	1	式	(1) 次の機器が搭載できる必要最小限のサイズであること。 ア　本体部 イ　表示部 ウ　操作部 エ　認証部 オ　警報装置 カ　印字装置 (2) OAチェア付きであること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
	セキュリティワイヤー	1	式	(1) 錠を有し、鍵は２個以上有すること。 (2) 錠は、本体部の盗難防止用セキュリティスロットに取り付けることができること。 (3) ワイヤーの太さは、4.0mm以上であること。また、長さは、1.5m以上2.5m以下であること。 (4) マウスを盗難防止の目的で取り付けられる構造であること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	
	OAタップ	1	式	(1) 操作卓に搭載する装置を収容する口数及び容量を有すること。 (2) 長さは３m以上であるこ

				と。 (3) 磁石、両面テープ又はネジにより操作卓に固定できること。 (4) 電源コンセントの形状は、２極コンセント又は２極接地極付コンセントであること。 　なお、２極接地極付コンセントを有する場合は、２極に変換できるプラグを付属すること。

(19)　コンソール端末の構成及び構造は、表- 47のとおりとする。

表- 47　コンソール端末の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) デスクトップ型であること。 (2) 盗難防止用セキュリティスロットを有すること。 (3) 質量は、10kg以下であること。また、最大消費電力は、300W以下であること。 (4) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 　なお、２極接地極付プラグを有する場合は、２極に変換できるプラグを付属すること。
	表示部	1	式	(1) 19型以上のカラー液晶ディスプレイであること。 (2) 質量は、10kg以下であること。また、最大消費電力は、150W以下であること。 (3) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 　なお、２極接地極付プラグを有する場合は、２極に

				変換できるプラグを付属すること。
	操作部	1	式	
	ソフトウェア	1	式	
	操作卓	1	式	(1) 次の機器が搭載できる必要最小限のサイズであること。 ア　本体部 イ　表示部 ウ　操作部 (2) OAチェア付きであること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
	セキュリティワイヤー	1	式	(1) 錠を有し、鍵は２個以上有すること。 (2) 錠は、本体部の盗難防止用セキュリティスロットに取り付けることができること。 (3) ワイヤーの太さは、4.0mm以上であること。また、長さは、1.5m以上2.5m以下であること。 (4) マウスを盗難防止の目的で取り付けられる構造であること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	
	インストール手順書	1	式	
	OAタップ	1	式	(1) 操作卓に搭載する装置を収容する口数及び容量を有すること。 (2) 長さは３m以上であること。 (3) 磁石、両面テープ又はネジにより操作卓に固定できること。 (4) 電源コンセントの形状は、２極コンセント又は２極接

				地極付コンセントであること。 　なお、２極接地極付コンセントを有する場合は、２極に変換できるプラグを付属すること。

⑳　警報装置の構成及び構造は、 表− 48のとおりとする。

表− 48　警報装置の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) 質量は、1.5kg以下であること。また、最大消費電力は、30W以下であること。 (2) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 　なお、２極接地極付プラグを有する場合は、２極に変換できるプラグを付属すること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

㉑　スキャナの構成及び構造は、 表− 49のとおりとする。

表− 49　スキャナの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) フラットベッド型であること。 (2) USB接続であること。 (3) 質量は、５kg以下であること。また、最大消費電力は、110W以下であること。 (4) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 　なお、２極接地極付プラグを有する場合は、２極に

				変換できるプラグを付属すること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

㉒ 印字装置の構成及び構造は、 表- 50のとおりとする。

表- 50 印字装置の構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) 管理端末A及び管理端末Bの操作卓に搭載できること。 (2) 質量は、10kg以下であること。また、最大消費電力は､1,000W以下であること。 (3) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 なお、２極接地極付プラグを有する場合は、２極に変換できるプラグを付属こと。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	カートリッジ	1	式	
	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

㉓ L3SWの構成及び構造は、 表- 51のとおりとする。

表- 51 L3SWの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	ラックに搭載できること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

⑵4　ハブⅠの構成及び構造は、表− 52のとおりとする。

表− 52　ハブⅠの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) 必要数を準備すること。 (2) ラックに搭載できること。 (3) 管理端末Ａ及び管理端末Ｂの操作卓に搭載できること。 (4) 電源プラグの形状は、２極プラグ又は２極接地極付プラグであること。 なお、２極接地極付プラグを有する場合は、２極に変換できるプラグを付属すること。
付属品	接続ケーブル	1	式	機器の接続に必要なケーブルを付属すること。
添付品	試験成績書	1	式	日本語であること。
	構成機器操作説明書	1	式	
	構成機器構築説明書	1	式	

⑵5　ラックの構成及び構造は、 表− 53のとおりとする。

表− 53　ラックの構成及び構造

区分	品目	数量	単位	記事
本体	本体部	1	式	(1) 必要数を準備すること。 (2) 前面部及び背面部ともに施錠できること。 (3) ラック単体は、幅650㎜以下、奥行き1,150㎜以下、高さ2,050㎜以下であること。 (4) 搭載する機器で必要な口数を有するラック電源を有すること。 (5) EIA規格に準拠すること。

8.3.2　その他

(1)　添付品（OAタップを除く。）については、書面で１部及び電磁的記録媒体で２部、警察庁に提出すること。

なお、配分数及び配分先については警察庁が別途指示する。

(2) (1)の電磁的記録媒体の種類及びに記録するファイルの種類については、警察庁と別途協議すること。

８．４　ソフトウェア構成

8.4.1　ソフトウェア構成

「４．１　機能・性能要件」における各構成機器の項目のソフトウェアに示すとおりである。

本仕様書で調達するソフトウェアについては、契約時における最新のバージョンを搭載すること。なお、業務用プログラムの開発期間中に新しいバージョンがリリースされた場合には、対応について警察庁と協議すること。

8.4.2　ライセンス

(1) 契約業者は、調達するソフトウェアのライセンスのうち、ウイルス対策ソフトについて、ガバメントライセンスを利用してよいものとする。

なお、詳細については警察庁が別途指示する。

(2) Microsoft 社製ソフトウェアのライセンスについては、警察庁がMicrosoft Professional Desktopを準備する。OSについては、別途指示を参照すること。

(3) 調達したソフトウェアのライセンス一覧については、書面及び電磁的記録媒体で警察庁に報告すること。

なお、報告の詳細事項については、警察庁と協議の上、決定すること。

(4) ライセンスの認証に外部回線を必要としないこと。

８．５　ネットワーク環境

本システムの通信プロトコルは、TCP/IPとする。

9　テスト要件定義

９．１　検査

9.1.1　検査は、構成、構造、機能及び性能について行う。また、３．８項については、基準を満足することを証明する技術資料に基づいて行う書面による検査とする。

なお、検査方法、検査内容については、警察庁と協議すること。

9.1.2　検査は、警察庁と協議の上定める場所において、警察庁検査官が立会いの上行う。

9.1.3　検査中に、本仕様書の規定に関して解釈上の疑義が生じた場合は、警察庁検査官の指示に従うこと。

10　移行要件定義

10．１　教育に係る要件

別途契約を結ぶ。

11　運用要件定義

11．１　情報システムの操作・監視等要件

11.1.1　運用形態は24時間連続運転稼働とする。

11.1.2　管理端末及びコンソール端末から操作及び監視する。

11.1.3　試験端末から業務確認できること。

11．２　データ管理要件

バックアップサーバ及び抽出サーバにおいてバックアップした電磁的記録媒体は、世代管理ができること。

11．３　運用施設・設備要件

11.3.1　床面は、フリーアクセスである。

11.3.2　床荷重の規格値は以下のとおりである。荷重が規格値を超えるおそれがある場合は、荷重を分散させる措置を行うこと。

(1)　フロアパネル（500㎜×500㎜）１枚あたりにかかる荷重が2,000Ｎ以下

(2)　フロアパネル２枚×２枚（１㎡）あたりにかかる荷重が4,900Ｎ以下

(3)　フロアパネル８枚×６枚（12㎡）あたりにかかる荷重が16,600Ｎ以下

11.3.3　導入する機器の発熱量が、170,000kJ/h以下であること。

12　保守要件定義

ソフトウェア及びハードウェア保守要件

12．１　保守体制

12.1.1　本仕様書で調達するソフトウェア及びハードウェアについては、障害連絡窓口を持ち、警察庁又は、関東管区警察局情報通信部、東京都警察情報通信部、北海道警察情報通信部及び各府県（方面を含む。）情報通信部（以下「情報通信部」という。）からの障害連絡を受け付けた場合は、速やかに復旧作業を行い、技術者の派遣要請があった場合は、技術者の派遣をすること。

なお、機器ごとの障害連絡窓口の受付時間及び技術者の駆けつけまでの時間は表- 54のとおりとする。

12.1.2　警察庁及び情報通信部の執務時間内は、技術的な質問に対応できる連絡窓口を有すること。

なお、連絡窓口の対応時間は、表- 54のとおりとする。

表- 54　障害等対応時間

	警察庁 (警察庁サーバ)	警察庁 (端末等)	警察本部 (端末等)	警察署 (端末等)
障害連絡窓口の 受付時間	24時間 365日	24時間 365日	24時間 365日	官庁執務時間 (8:30～17:15)
技術者の駆けつけ 時間	３時間以内	３時間以内	３時間以内	翌官庁執務時間
技術的な質問に 対応できる連絡窓口	官庁執務時間 (8:30～18:15)			

12.1.3　障害受付窓口及び体制を記した資料並びに技術的な質問に対応できる連絡窓口及び体制を記した資料を、警察庁に２部提出すること。

なお、準備する窓口ついては、プログラム仕様書において別途契約するプログラム保守契約が定める障害受付窓口と共通とすること。

12.1.4　障害復旧作業時間は、障害の通知を受けてから障害が復旧するまでの時間とし､障害状況ごとに設定した障害復旧までの目標時間は表- 55のとおりとする。

なお、目標復旧時間を超過した場合には、目標復旧時間内の復旧に至らなかった原因を特定し、今後の改善策について資料を提出すること。

表- 55　障害復旧目標時間

障害レベル	障害状況	警察庁（警察庁サーバ）	警察庁（端末等）	警察本部（端末等）	警察署（端末等）
4	システム(業務）の完全停止を伴う障害	８時間以内	８時間以内	８時間以内	翌官庁執務時間終了まで
3	運用制限等の業務への影響を生じる障害	８時間以内	８時間以内	８時間以内	翌官庁執務時間終了まで
2	運用制限等にまで至らない程度の障害	翌官庁執務時間終了まで	翌官庁執務時間終了まで	翌官庁執務時間終了まで	翌官庁執務時間終了まで
1	その他の障害	翌官庁執務時間終了まで	翌官庁執務時間終了まで	翌官庁執務時間終了まで	翌官庁執務時間終了まで

※官庁執務時間は9:30～18:15とする。

12.1.5　障害によりHDDを交換する場合、不良となったHDDのデータは、速やかに警察職員立会いの下、契約業者の準備するデータ消去機能を有する装置あるいはツールで消去し、データ消去を確認後、HDDを搬出すること。（この場合のデータ消去とは、NSA方式、NATO方式、DoD方式、Gutmann方式等に準じたパターンで上書きすることをいう。）また、契約業者の準備するデータ消去機能を有する装置又はツールについては、事前に警察庁の承認を得ること。

なお、HDDのデータ消去が困難な場合には、警察職員立会いの下、契約業者の準備するHDD破壊装置等でHDDを再利用できない状態にした上で搬出すること。

12.1.6　本仕様書で調達されたソフトウェアについてパッチが必要な場合は、速やかに警察庁に報告し、その指示に従い適用すること。

12.1.7　専用端末及び試験端末の本体部のバッテリが必要な性能を満たさなくなった場合には、速やかに交換すること。

12.1.8　12.1.1項から12.1.7項までに基づき保守を実施し、その実施状況について警察庁に報告書を提出すること。また、報告内容、報告方法及び報告時期については、警察庁と協議すること。

なお、障害発生時等、警察庁が必要に応じ報告を求めた場合は、速やかに報告書を提出すること。

12.1.9　警察庁ホストシステム、警察庁指掌紋システム、アクセス権管理システム及び法務省システムの更改に伴う本システムの設定変更を行い、安定稼働確認及び性能確認を行うこと。

なお、警察庁ホストシステム、警察庁指掌紋システム、アクセス権管理システム及び法務省システムの更改の時期及び作業の詳細については、別途指示する。

12．２　定期点検

東京都23区内の警察庁が別途指示する場所に設置する機器について、機器ごとに年１回以上の定期点検(点検、清掃、バックアップ及び消耗品交換)を実施し、警察庁に報告書を提出すること。定期点検実施後は、システムの安定稼働確認及び性能確認を行うこと。また、警察庁の指示する不具合等に対する設定及び調整を行うこと。

なお、点検の対象機器、定期点検の実施時期及び作業項目の詳細については、警察庁と協議すること。

13　作業の体制及び方法

13．１　作業体制

契約業者は、本仕様書で調達されたソフトウェア及びハードウェアの保守について、警察庁が「政府情報システムの整備及び管理に関する標準ガイドライン」（平成26年12月３日各府省情報化統括責任者（CIO）連絡会議決定）（以下「ガイドライン」という。）に基づく保守作業計画及び保守実施要領を作成するので、警察庁の求めに応じ資料を作成し提出すること。

13．２　導入

13.2.1　搬入等

別途契約を結ぶ。

13.2.2　協議

契約後、速やかに以下の協議を行い、資料を提出すること。

(1)　ハードウェア構成の詳細

(2)　納入機器の構成品の詳細

(3)　納入機器の性能及び機能の詳細

(4)　納入機器の発熱量計算書、重量計算書、電源容量計算書、電源コンセント形状及び数量

(5)　ラックのサイズ、数量及び機器実装図

(6)　各端末における本体のサイズ、数量及び機器搭載図

13.2.3　調整等

別途契約を結ぶ。

14　特記事項

14．１　ODB登録用シートの作成

本仕様書で調達された情報システムに係る詳細事項については、ガイドラインに基づき政府情報システム管理データベース（Official information system total management Database）（以下「ODB」という。）に警察庁が登録するので、契約業者はODB登録用シートを作成し、提出すること。

なお、詳細については、警察庁が別途指示する。

14．２　警察庁が別途指示する事項、並びに警察庁が3.7.5項で整備した機器に係る性能及び利用状況については、入札公告期間中に閲覧可能であるため、警察庁に問い合わせること。

14．３　納入物が他者の権利を侵害していないこと。

14．４　契約の履行終了又は解除により納入物の返還が必要となった場合、添付品については、警察庁において処分することとする。

14．５　全ての作業完了後、完了報告書を提出すること。

なお、完了報告書に係る詳細については、警察庁と協議すること。

15　妥当性証明

本調達仕様書の妥当性について証す。

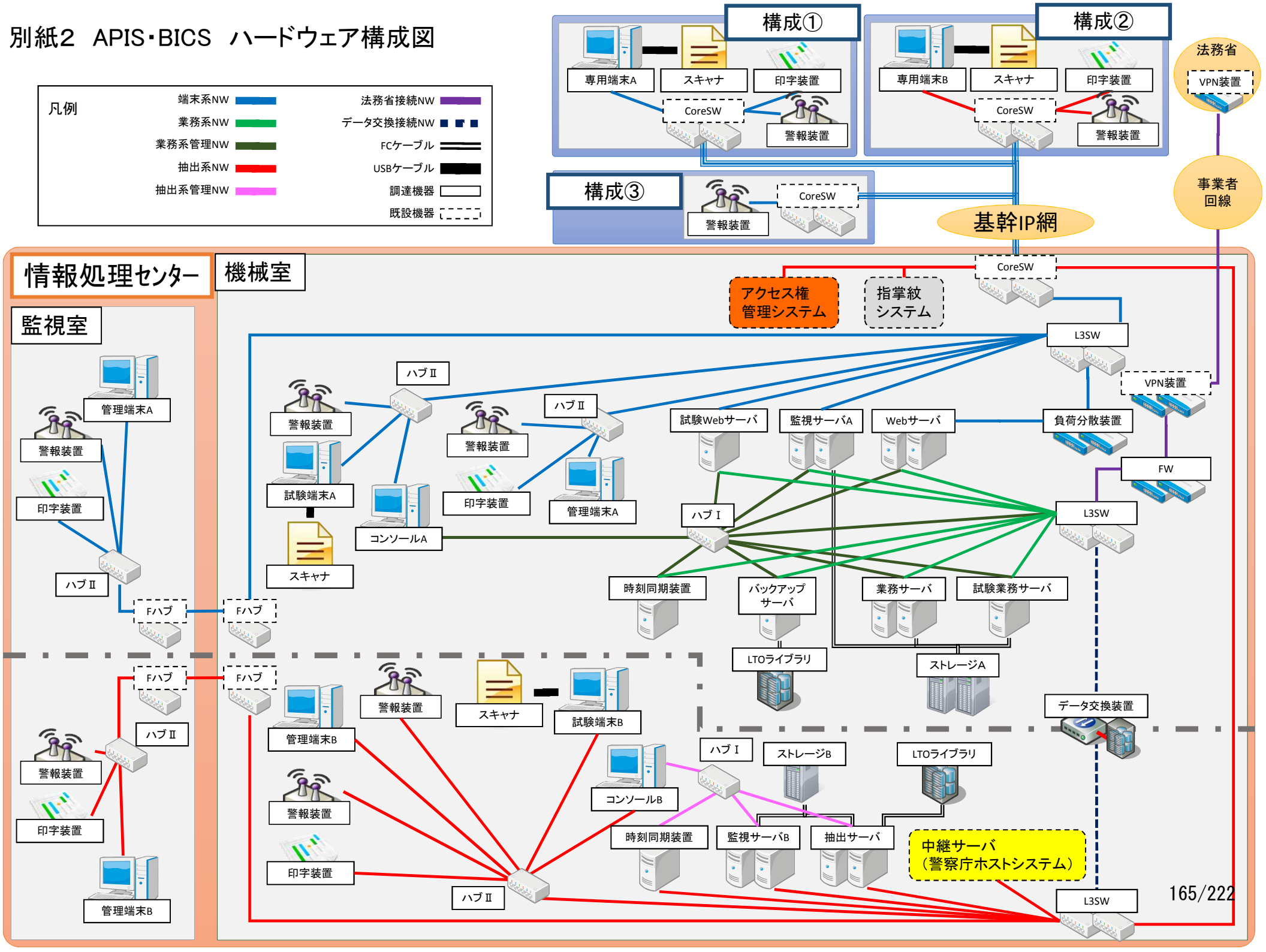
警察庁情報通信局情報管理課長（警察庁CIO補佐官）　　降簱　喜和男

別紙1

事前旅客情報システム及び外国人個人識別情報認証システム仕様書　提出資料等一覧

No	提出資料等		提出予定	
			時期	方法
1	ハードウェアの構成の詳細	ハードウェアの構成の詳細等	協議して決定	書面
2	ソフトウェアの構成	ソフトウェアライセンスの一覧	納入時	書面、電磁的記録媒体
3	保守	障害受付窓口及び体制を記した資料	平成31年1月31日まで	書面
4		技術的な質問に対応できる連絡窓口及び体制を記した資料	平成31年1月31日まで	書面
5		障害回復後の改善策	障害復旧後、10営業日以内	書面
6		保守に関する報告	実施後、5営業日以内	書面
7		ソフトウェアパッチ	必要な場合、協議して決定	書面
8		定期点検実施報告	実施後、5営業日以内	書面
9	ガイドライン関係	保守実施計画作成に係る資料	協議して決定	書面
10		保守実施要領作成に係る資料	協議して決定	書面
11		ODB登録用シート	保守実施要領に定める時期まで	書面
12	完了報告書		契約履行期限まで	書面

別紙2　APIS･BICS　ハードウェア構成図



別添５

「事前旅客情報システム及び外国人個人識別情報認証システム」
「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム」

総合評価基準

平成28年８月

警察庁

１　はじめに

本総合評価基準は、「事前旅客情報システム及び外国人個人識別情報認証システム」及び「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム」について提供される要求仕様の総合評価について示したものである。

２　性能等の評価に係る要求要件等について

(1)　必須項目

必須条件については、別冊「事前旅客情報システム及び外国人個人識別情報認証システム仕様書」及び「事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書」に示したもののほか、本総合評価基準における評価内容の区分のうち「必須項目」として示したものについては、最低限の要求要件を設定したものであり、この要求要件を全て満たしている場合は基礎点を与え、満たさない場合は不合格とする。

(2)　加点項目

本総合評価基準における評価内容の区分のうち、加点項目として示したものについては、警察庁が必要度、重要度に照らし合わせて設定したものであり、この要求要件を満たした提案について加点するものとする。

３　得点の付与方式について

(1)　入札価格の得点（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。

なお、入札価格に対する得点配分と性能等の得点配分は等しいものとする。

(2)　性能等の得点（技術点）

基礎点及び加点の得点を合計した値とする。

ア　基礎点

本総合評価基準における評価内容の区分のうち、必須項目として示したものについて、最低限の要求要件を満たしている場合に基礎点を付与する。

イ　加点

本総合評価基準における評価内容の区分のうち、加点項目として示したものについては、入札者が本総合評価基準表により行った加点項目に係る提案に対し、加点基準に基づき加点する。

４　落札方式について

(1)　入札については、予定価格の制限範囲の応札について有効とする。

(2)　総合評価は、入札者の価格点と当該入札者の申込みに係る技術点の合計をもって行い、該当数値の最も高いものを落札者とする。

(3)　上記(2)の数値の最も高いものが２者以上ある時は、くじ引きにより落札者を決定する。

５　得点配分

各項目における得点配分の一覧を示す。入札価格に対する得点配分と性能等の得点配分の比率は１：１とする。（記載の数値は１：１で算出した得点である。）

項目	入札価格に対する得点配分	性能等の得点配分		
		基礎点	加点	計
事前旅客情報システム及び外国人個人識別情報認証システム	6,912	6,883 (10,000)	29 (42)	6,912 (10,042)
事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム	3,088	1,544 (1,560)	1,544 (1,560)	3,088 (3,120)
総計	10,000	8,427	1,573	10,000

※ 性能等の得点は、下段の括弧内の満点に対する得点比率を、上段の満点に対する比率に換算したものとする。

必須項目

1 総合

区分	詳細内容				配点	根拠資料番号	備考	得点
必須項目	使用条件			仕様書に示す条件を満足すること。	基礎点			
	ハードウェア構成			仕様書に示す構成及び構造であること。				

2 負荷分散装置

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	負荷分散装置	本体部	ロードバランス機能	Webサーバに対して、ラウンドロビン、最小コネクション又は最速応答によりロードバランス機能を有すること。	基礎点			
			セッション維持機能	URL、Cookie、SSL Session ID又は送信元IPアドレスにより、一定期間Webサーバにリクエストを割り振り続ける機能を有すること。				
			ヘルスチェック機能	pingチェック、ポートチェック又はコンテンツチェック(HTTPに対するPOSTリクエストによる応答文字列の確認等)により、Webサーバの動作を確認する機能を有すること。				
			スパニングツリー機能	ネットワークにおいて、データが永遠に循環するのを防止する機能を有すること。				
			VLAN機能	物理的な接続形態とは別に、MACアドレス、IPアドレス、利用するプロトコルのいずれかに応じて、32以上の仮想的なグループが設定できること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを5個以上有すること。				
				(2) ネットワークは冗長構成ができること。				
			管理コンソール機能	Webブラウザを使用し、負荷分散装置の管理に係る操作ができること。				
			ネットワーク管理	監視サーバAのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			コンソールインタフェース	コンソール用ポートを有すること。				
			時刻同期	1日1回以上、監視サーバAと自動及び手動で時刻同期ができること。				
		その他		アクティブ／スタンバイ型の冗長構成とし、冗長側機器への切替が任意にできること。				

3 Webサーバ

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	Webサーバ	本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。	基礎点			
			メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。				
				(2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。				
				(3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
				(4) サーバを停止せずに、HDDの交換ができること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを5個以上有すること。				
				(2) ネットワークは冗長構成ができること。				
			電源ユニット	冗長構成であること。				
		バックアップ部		(1) RDX媒体を扱うことができること。				
				(2) 1回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。				
		ソフトウェア	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。				
				(2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。				
				(3) 日本語に対応すること。				
			Web機能	(1) Apache HTTP Serverを搭載すること。				
				(2) アクティブ／アクティブ型のWebサーバを構築できること。				

			ディレクトリサービス	(1) 業務用プログラムの要求受け、必要なユーザ情報を送信できること。				
				(2) 日本語に対応すること。				
				(3) SSLオプションを搭載すること。				
				(4) 5,000ユーザ以上を登録できること。				
				(5) ディレクトリサーバについては、アクティブ/アクティブ型の冗長構成とし、レプリケーション機能を有すること。				
				(6) ユーザ情報を管理する、GUIによるインターフェースを有すること。				
				(7) アクセス権管理システムが採用するユーザーインターフェースと互換性を有すること。				
			プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。				
			バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。				
				(2) サーバを停止せずに、内蔵HDDのバックアップができること。				
			運用管理	(1) 本装置の本体部及びバックアップ部の稼働状況を監視し、監視サーバAの運用管理ソフトウェアに通知できること。				
				(2) 監視サーバAの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携しジョブを実行できること。				
			ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア ログイン及びログアウト履歴 イ システムログ ウ アプリケーションログ エ セキュリティログ オ データベースへのアクセスログ				
				(2) 監視サーバAのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。				
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。				
			ネットワーク管理	監視サーバAのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) 監視サーバAからウイルス対策ソフトウェアの更新データを受信できること。				
				(4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				

4 業務サーバ

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	業務サーバ	本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。	基礎点			
			メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。				
				(2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。				
				(3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
				(4) サーバを停止せずに、HDDの交換ができること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを4個以上有すること。				
				(2) ネットワークは冗長構成ができること。				
				(3) ストレージAへ接続するためのファイバチャネルポートを有すること。				
				(4) ストレージAへの接続は冗長構成とし、各々のディスクコントローラで接続できること。				

				(5) 冗長構成としたファイバチャネルについては、障害による自動閉塞機能及び自動切替機能を有すること。				
			電源ユニット	冗長構成であること。				
		バックアップ部		(1) RDX媒体を扱うことができること。				
				(2) 1回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。				
		ソフトウェア	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。				
				(2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。				
				(3) 日本語に対応すること。				
			データベース管理	次の機能を有するソフトウェアを搭載すること。 (1) 別途調達する業務用プログラムが、SQL及びストアドプロシージャの実行及び結果の取得ができること。				
				(2) 複数のデータベースサーバから、同一のデータベースにアクセス可能なこと。				
				(3) アクティブ/アクティブ型のクラスタ構成に対応できること。				
				(4) データベースの性能情報、運用状況の統計を作成でき、分析できること。				
			クラスタ	(1) アクティブ／アクティブ型のクラスタ構成であること。				
				(2) データベースのデータを同一の内容に保つこと。				
				(3) クラスタ構成の構築及び運用保守を行うために必要な次の機能を有すること。 ア 管理端末A及びコンソール端末AからGUI又はWeb ブラウザを使用し、クラスタの設定変更ができること。 イ 管理端末A及びコンソール端末AからGUI又はWebブラウザを使用し、クラスタ、ノード及びアプリケーションの起動及び停止が容易にできること。				
				(4) 管理端末A及びコンソール端末Aから系の切替えを任意にできること。				
			プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。				
			バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。				
				(2) サーバを停止せずに、内蔵HDDのバックアップができること。				
			運用管理	(1) 本装置の本体部及びバックアップ部の稼働状況を監視し、監視サーバAの運用管理ソフトウェアに通知できること。				
				(2) 監視サーバAの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携しジョブを実行できること。				
			ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア ログイン及びログアウト履歴 イ システムログ ウ アプリケーションログ エ セキュリティログ オ データベースへのアクセスログ				
				(2) 監視サーバAのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。				
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること				
			ネットワーク管理	監視サーバAのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) 監視サーバAからウイルス対策ソフトウェアの更新データを受信できること。				
				(4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				

5 抽出サーバ

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	抽出サーバ	本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。	基礎点			
			メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。				

				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。			
			内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。			
				(2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。			
				(3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。			
				(4) サーバを停止せずに、HDDの交換ができること。			
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。			
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを8個以上有すること。			
				(2) ネットワークは冗長構成ができること。			
				(3) ストレージBに接続するためのファイバチャネルポートをすること。			
				(4) 待機系サーバにあっては、ストレージBに接続するためのファイバチャネルポートとは別に、テープライブラリに接続するためのファイバチャネルポートを有すること。			
				(5) ストレージBへの接続は冗長構成とし、各々のディスクコントローラで接続できること。			
				(6) 冗長化したファイバチャネルは、障害による自動閉塞機能及び自動切替機能を有すること。			
			電源ユニット	冗長構成であること。			
		バックアップ部		(1) RDX媒体を扱うことができること。			
				(2) 1回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。			
		テープライブラリ部	テープライブラリ	(1) テープスロット数が20個以上であること。			
				(2) ライブラリ容量が30Tバイト(非圧縮)以上であること。			
				(3) 本体部とファイバチャネルにより接続できること。			
			テープドライブ	(1) LTO5以上に対応したものを2台以上搭載すること。			
				(2) 1台当たりのデータ転送速度は、最大140Mバイト/秒以上(非圧縮)であること。。			
				(3) 暗号化については、次のとおりとする。 ア 警察庁が別途指示する政府推奨の暗号アルゴリズムにより暗号化した上で、電磁的記録媒体に記録できること。 また、任意の周期で暗号鍵を変更できること。 イ 暗号化に使用した暗号鍵を電磁的記録媒体に記録できること。 ウ 暗号鍵生成のログが採取でき、暗号鍵を作成した年月日時分秒を確認できること。			
		ソフトウェア1	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。			
				(2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。			
				(3) 日本語に対応すること。			
			Web機能	(1) Apache HTTP Serverを搭載すること。			
				(2) アクティブ／スタンバイ型のWebサーバを構築できること。			
			データベース管理	次の機能を有するソフトウェアを搭載すること。 (1) 別途調達する業務用プログラムが、SQL及びストアドプロシージャの実行及び結果の取得ができること。			
				(2) 複数のデータベースサーバから、同一のデータベースにアクセス可能なこと。			
				(3) アクティブ/スタンバイ型のクラスタ構成に対応できること。			
				(4) データベースの性能情報、運用状況の統計を作成でき、分析できること。			
			クラスタ	(1) アクティブ／スタンバイ型のクラスタ構成であること。			
				(2) データベースのデータを同一の内容に保つこと。			

				(3) クラスタ構成の構築及び運用保守を行うために必要な次の機能を有すること。 ア 管理端末B及びコンソール端末BからGUI又はWebブラウザを使用し、クラスタの設定変更ができること。 イ 管理端末B及びコンソール端末BからGUI又はWebブラウザを使用し、クラスタ、ノード及びアプリケーションの起動及び停止が容易にできること。				
				(4) 管理端末B及びコンソール端末Bから系の切替えを任意にできること。				
			プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。				
			バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。				
				(2) サーバを停止せずに、内蔵HDDのバックアップができること。				
			運用管理	(1) 本装置の本体部、バックアップ部及びテープライブラリ部の稼働状況を監視し、監視サーバBの運用管理ソフトウェアに通知できること。				
				(2) 監視サーバBの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携し、ジョブを実行できること。				
			ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア ログイン及びログアウト履歴 イ システムログ ウ アプリケーションログ エ セキュリティログ オ ユーザ認証ログ カ データベースへのアクセスログ				
				(2) 監視サーバBのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。				
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。				
			ネットワーク管理	監視サーバBのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) 監視サーバBからウイルス対策ソフトウェアの更新データを受信できること。				
				(4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				
		ソフトウェア2	データレプリケーション	(1) ストレージB内で、データベースを記録したボリュームの複製が作成できること。				
				(2) 業務に影響することなく、ストレージB内で複製ボリュームの作成及び切離しができること。				
				(3) 待機系サーバへ機能を搭載すること。				
			バックアップ2	(1) 監視サーバBに収集されたログをテープライブラリ部の電磁的記録媒体にバックアップし、累積して管理できること。				
				(2) 業務に影響することなく、ストレージBのデータベースをバックアップ及びリストアするため、次の機能を有すること。 ア バックアップ (ア) 監視サーバBの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携し、定められた時刻に自動及び任意の時刻に手動で、ストレージBの複製ボリュームをオンラインから切離し、対象データをテープライブラリ部の電磁的記録媒体にバックアップができること。				
				(イ) バックアップデータは、日付、時刻及びバックアップの対象データを一意に識別できる名称で管理できること。				
				(ウ) バックアップデータは、1世代当たり正・副とし、3世代の管理ができること。				
				イ リストア (ア) オンラインから切り離された複製ボリューム並びにデータの更新、追加、削除のログ及びその他必要な情報から、データベースを障害発生直前の状態までリストアできること。				
				(イ) (ア)によりリストアできない場合、テープライブラリ部の電磁的記録媒体に保存されたバックアップデータ及びその他 必要な情報から、データベースをバックアップ取得時の状態までリストアできること。				
				(ウ) データベースのリストアは、(2)ア(イ)の名称を指定してできること。				
				(3) 管理端末BからGUI又はWebブラウザにより、バックアップ2の設定及び監視ができること。				
				(4) 待機系サーバへ機能を搭載すること。				

6 監視サーバA

区分	機器名	詳細内容	配点	根拠資料番号	備考	得点

必須項目	監視サーバA	本体部	CPU	本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる処理能力を有すること。	基礎点			
			メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。				
				(2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。				
				(3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
				(4) サーバを停止せずに、HDDの交換ができること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを5個以上有すること。				
				(2) ネットワークは冗長構成ができること。				
				(3) 共有ディスク装置へ接続するためのファイバチャネルポートを有すること。				
				(4) 共有ディスク装置への接続は冗長構成とし、各々のディスクコントローラで接続できること。				
				(5) 冗長構成としたファイバチャネルについては、障害による自動閉塞機能及び自動切替機能を有すること。				
			電源ユニット	冗長構成であること。				
		コンソール部	ディスプレイ	(1) 解像度は1,024×768ドット以上であること。				
				(2) 表示色は、65,536色以上であること。				
			キーボード	JIS規格キー配列に準拠していること。				
			マウス	(1) 2ボタン式以上の光学式又はレーザー式であること。				
				(2) ホイール等によりマウスを移動せずに画面のスクロールができること。				
			KVMスイッチ	(1) ディスプレイ、キーボード及びマウスを接続できること。				
				(2) クラスタ構成された本サーバ2台を接続し、切替えできること。				
		バックアップ部		(1) RDX媒体を扱うことができること。				
				(2) 1回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。				
		共有ディスク部	共有ディスク装置	(1) RAID1、RAID5又はRAID6の冗長構成とし、RAID構成後の実記憶容量については、警察庁と協議すること。				
				(2) (1)で決定した実記憶容量とは別に、HDD又はエンクロージャー等の増設により、取り扱う容量の拡張ができること。				
				(3) サーバを停止せずに、HDDの交換ができること。				
				(4) 本体部とは、ファイバチャネルで接続できること。				
		ソフトウェア	OS	(1) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。				
				(2) 日本語に対応すること。				
			クラスタ	(1) アクティブ／スタンバイ型のクラスタ構成であること。				
				(2) クラスタ構成の構築及び運用保守を行うために必要な次の機能を有すること。 ア GUI又はWebブラウザを使用し、クラスタの設定変更ができること。 イ GUI又はWebブラウザを使用し、クラスタ、ノード及びアプリケーションの起動及び停止ができること。				
				(3) 系の切替えを任意にできること。				
			バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。				
				(2) サーバを停止せずに、内蔵HDDのバックアップができること。				

			統合監視	(1) 業務統合監視機能 GUI又はWebブラウザによる統合監視機能を有し、監視目的別に業務状況(運用管理、ログ管理、ネットワーク管理、ストレージ管理及び性能管理)を監視することができること。また、監視画面から各機能の監視画面に遷移し、階層を掘り下げることにより障害箇所を特定できること。			
				(2) コマンド制御機能 コマンドを業務サーバ等(監視サーバAを除く。)へ発行できること。また、発行したコマンド及び受信メッセージの履歴を照会できること。			
				(3) メッセージ監視機能 業務サーバ等(監視サーバAを除く。)から通知されたメッセージについて、メッセージごとに内容説明や処置方法を任意に定義できること。また、日本語で表示及び印字できること。			
				(4) 警報装置の制御 メッセージの内容に応じて、管理端末Aに付帯する警報装置の制御ができること。			
				(5) 管理端末Aへの通知 業務サーバ等(監視サーバを除く。)から通知されたメッセージは、管理端末Aの統合監視ソフトウェアへ通知できること。			
			ストレージ管理	ストレージAの管理機能として、次の機能を有すること。 (1) ディスクアレイ構成情報(HDDの物理名称、エンクロージャ、プール及び制御装置に係る情報)をGUI又はWebブラウザで表示できること。			
				(2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。			
				(3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。			
				(4) ストレージAのディスクアレイ及びネットワークの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報に反映できること。			
			性能管理	(1) 次の項目について、業務サーバ等の性能状態監視及び管理ができること。 ア 内蔵HDD利用率 イ CPU利用率 ウ メモリ利用率			
				(2) GUI又はWebブラウザによる業務サーバ及び試験業務サーバのRDBMS(Relational DataBase Management System)管理機能を有すること。			
			運用管理	(1) ジョブスケジューリング機能を有すること。			
				(2) 業務サーバ等、各スイッチ、各端末及び警報装置の稼働状況を監視し、統合監視ソフトウェアへ通知できること。			
				(3) ジョブスケジューリング機能と連携し、業務サーバ等のジョブの実行及び管理ができること。			
			ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア ログイン及びログアウト履歴 イ システムログ ウ アプリケーションログ エ セキュリティログ			
				(2) 業務サーバ等及びデータ交換装置のログを収集し共有ディスク装置へ保存すると共に、区分(システムログ、アプリケーションログ、セキュリティログ等)、発生時間、発生装置、キーワード等により、抽出、分析及び出力ができること。			
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。			
			ネットワーク管理	業務サーバ等(監視サーバAを除く。)、負荷分散装置、ストレージA及び各スイッチのMIB情報を収集する機能を有すること。			
			端末リモート操作サーバ	専用端末A及び試験端末Aの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末A及び試験端末AのOSへのログイン操作ができること。			
				(2) 専用端末A及び試験端末Aと監視サーバA間でクリップボードの情報を共有できること。			
				(3) 専用端末A及び試験端末Aと監視サーバA間でファイルの送受信ができること。			
			ソフトウェア配信サーバ	(1) 専用端末A等にインストールされたソフトウェア配信クライアントソフトウェアに対し、自動及び手動でソフトウェア及びソフトウェアのパッチを配信、適用ができること。このとき、配信開始時刻、転送速度制限、分割配信及び同時配信端末数の設定ができること。			
				(2) GUI又はWebブラウザによる管理コンソール機能を有し、スケジュール機能によりソフトウェアをインストールする時刻及び手順を一括、グループ別及び個別で設定できること。また、専用端末A等に対して次の動作が設定できること。 ア 端末の強制再起動及び強制シャットダウン イ インストール時及び終了時の端末の権限設定の変更 ウ インストール失敗時の動作設定			
				(3) (2)で設定したスケジュールは、設定情報として内蔵HDDに保存できること。また、保存した設定情報をスケジュールに反映できること。			
				(4) 専用端末A等からインストールの進行状況を自動及び手動で受信し、管理コンソール機能で表示でき、ログとして出力できること。			
				(5) 管理コンソール機能は、管理者権限が与えられた者のみが操作できるようアクセス権設定ができること。			

				(6) 待機系サーバへ機能を搭載すること。				
			証跡収集	(1) 専用端末A等が生成した証跡を収集し、管理できること。				
				(2) 専用端末A等の要求により収集した証跡を送信し、検証ができること。				
			定義ファイル配信	(1) 業務サーバ等、専用端末A等及びデータ交換装置に対して、待機系サーバから配信先ごとのウイルス対策ソフトに対応するウイルス対策ソフトウェアの更新データを配信すること。				
				(2) ウイルス対策ソフトベンダーが提供する最新のウイルス対策ソフトウェアの更新データを取得できること。 ウイルス対策ソフトウェアの更新データの取得方法については、警察庁と別途協議すること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	(1) 1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				
				(2) 専用端末A等及び各スイッチの時刻修正ができること。				

7 監視サーバB

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	監視サーバB	本体部	CPU	本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる処理能力を有すること。	基礎点			
			メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。				
				(2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。				
				(3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
				(4) サーバを停止せずに、HDDの交換ができること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを5個以上有すること。				
				(2) ネットワークは冗長構成ができること。				
				(3) 共有ディスク装置へ接続するためのファイバチャネルポートを有すること。				
				(4) 共有ディスク装置への接続は冗長構成とし、各々のディスクコントローラで接続できること。				
				(5) 冗長構成としたファイバチャネルについては、障害による自動閉塞機能及び自動切替機能を有すること。				
			電源ユニット	冗長構成であること。				
		コンソール部	ディスプレイ	(1) 解像度は1,024×768ドット以上であること。				
				(2) 表示色は、65,536色以上であること。				
			キーボード	JIS規格キー配列に準拠していること。				
			マウス	(1) 2ボタン式以上の光学式又はレーザー式であること。				
				(2) ホイール等によりマウスを移動せずに画面のスクロールができること。				
			KVMスイッチ	(1) ディスプレイ、キーボード及びマウスを接続できること。				
				(2) クラスタ構成された本サーバ2台を接続し、切替えできること。				
		バックアップ部		(1) RDX媒体を扱うことができること。				
				(2) 1回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。				
		共有ディスク部	共有ディスク装置	(1) RAID1、RAID5又はRAID6の冗長構成とし、RAID構成後の実記憶容量については、警察庁と協議すること。				

				(2) (1)で決定した実記憶容量とは別に、HDD又はエンクロージャー等の増設により、取り扱う容量の拡張ができること。			
				(3) サーバを停止せずに、HDDの交換ができること。			
				(4) 本体部とは、ファイバチャネルで接続できること。			
		ソフトウェア	OS	(1) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。			
				(2) 日本語に対応すること			
			クラスタ	(1) アクティブ／スタンバイ型のクラスタ構成であること。			
				(2) クラスタ構成の構築及び運用保守を行うために必要な次の機能を有すること。 ア GUI又はWebブラウザを使用し、クラスタの設定変更ができること。 イ GUI又はWebブラウザを使用し、クラスタ、ノード及びアプリケーションの起動及び停止ができること。			
				(3) 系の切替えを任意にできること。			
			バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。			
				(2) サーバを停止せずに、内蔵HDDのバックアップができること。			
			統合監視	(1) 業務統合監視機能 GUI又はWebブラウザによる統合監視機能を有し、監視目的別に業務状況(運用管理、ログ管理、ネットワーク管理、ストレージ管理及び性能管理)を監視することができること。また、監視画面から各機能の監視画面に遷移し、階層を掘り下げることにより障害箇所を特定できること。			
				(2) コマンド制御機能 コマンドを抽出サーバへ発行できること。また、発行したコマンド及び受信メッセージの履歴を照会できること。			
				(3) メッセージ監視機能 抽出サーバから通知されたメッセージについて、メッセージごとに内容説明や処置方法を任意に定義できること。また、日本語で表示及び印字できること。			
				(4) 警報装置の制御 メッセージの内容に応じて、管理端末Bに付帯する警報装置の制御ができること。			
				(5) 抽出サーバから通知されたメッセージは、管理端末Bの統合監視ソフトウェアへ通知できること。			
			ストレージ管理	ストレージBの管理機能として、次の機能を有すること。 (1) ディスクアレイ構成情報(HDDの物理名称、エンクロージャ、プール及び制御装置に係る情報)をGUI又はWebブラウザで表示できること。			
				(2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。			
				(3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。			
				(4) メッセージにより、ストレージBのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。			
			性能管理	(1) 次の項目について、抽出サーバ等の性能状態監視及び管理ができること。 ア 内蔵HDD利用率 イ CPU利用率 ウ メモリ利用率			
				(2) GUI又はWebブラウザによる抽出サーバのRDBMS管理機能を有すること。			
			運用管理	(1) ジョブスケジューリング機能を有すること。			
				(2) 抽出サーバ等、各スイッチ、専用端末B等及び警報装置の稼働状況を監視し、統合監視ソフトウェアに通知できること。			
				(3) ジョブスケジューリング機能と連携し、抽出サーバ等のジョブの実行及び管理ができること。			
			ログ管理	(1) 次の各項目のログを本体部の内蔵HDDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア ログイン及びログアウト履歴 イ システムログ ウ アプリケーションログ エ セキュリティログ			
				(2) 抽出サーバ等及びデータ交換装置のログを収集し共有ディスク装置へ保存すると共に、区分(システムログ、アプリケーションログ、セキュリティログ等)、発生時間、発生装置、キーワード等により、抽出、分析及び出力ができること。			
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。			
			ネットワーク管理	抽出サーバ、ストレージB、各スイッチのMIB情報を収集する機能を有すること。			

			端末リモート操作サーバ	専用端末B及び試験端末Bの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末B及び試験端末BのOSへのログイン操作ができること。				
				(2) 専用端末B及び試験端末Bと監視サーバB間でクリップボードの情報を共有できること。				
				(3) 専用端末B及び試験端末Bと監視サーバB間でファイルの送受信ができること。				
			ソフトウェア配信サーバ	(1) 専用端末B等にインストールされたソフトウェア配信クライアントソフトウェアに対して自動及び手動でソフトウェア及びソフトウェアのパッチを配信、適用ができること。このとき、配信開始時刻、転送速度制限、分割配信及び同時配信端末数の設定ができること。				
				(2) GUI又はWebブラウザによる管理コンソール機能を有し、スケジュール機能によりソフトウェアをインストールする時刻及び手順を一括、グループ別及び個別で設定できること。また、専用端末B等に対して次の動作が設定できること。 ア 端末の強制再起動及び強制シャットダウン イ インストール時及び終了時の端末の権限設定の変更 ウ インストール失敗時の動作設定				
				(3) (2)で設定したスケジュールは、設定情報として内蔵HDDに保存できること。また、保存した設定情報をスケジュールに反映できること。				
				(4) 専用端末B等からインストールの進行状況を自動及び手動で受信し、管理コンソール機能で表示でき、ログとして出力できること。				
				(5) 管理コンソール機能は、管理者権限が与えられた者のみが操作できるようアクセス権設定ができること。				
				(6) 待機系サーバへ機能を搭載すること。				
			証跡収集	(1) 専用端末B等が生成した証跡を収集し、管理できること。				
				(2) 専用端末B等の要求により収集した証跡を送信し、検証ができること。				
			定義ファイル配信	(1) 抽出サーバ等、専用端末B等及びデータ交換装置に対して、待機系サーバから配信先ごとのウイルス対策ソフトに対応するウイルス対策ソフトウェアの更新データを配信すること。				
				(2) ウイルス対策ソフトベンダーが提供する最新のウイルス定義ファイルを取得できること。 ウイルス対策ソフトウェアの更新データの取得方法については、警察庁と別途協議すること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	(1) 1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				
				(2) 専用端末B等及び各スイッチの時刻修正ができること。				

8 バックアップサーバ

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	バックアップサーバ	本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。	基礎点			
			メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。				
				(2) RAID構成後、本装置の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。				
				(3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
				(4) サーバを停止せずに、HDDの交換ができること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを3個以上有すること。				
				(2) ネットワークは冗長構成ができること。				
				(3) ストレージA及びテープライブラリに接続するためのファイバチャネルポートを有すること。				
				(4) ストレージAへの接続は冗長構成とし、各々のディスクコントローラで接続できること。				
				(5) 冗長構成としたファイバチャネルポートは、障害による自動閉塞機能、自動切替機能を有すること。				

			電源ユニット	冗長構成であること。			
		バックアップ部		(1) RDX媒体を扱うことができること。			
				(2) 1回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。			
		テープライブラリ部	テープライブラリ	(1) テープスロット数が20個以上であること。			
				(2) ライブラリ容量が30Tバイト(非圧縮)以上であること。			
				(3) 本体部とファイバチャネルにより接続できること。			
			テープドライブ	(1) LTO5以上に対応したものを2台以上搭載すること。			
				(2) 1台当たりのデータ転送速度は、最大140Mバイト/秒以上(非圧縮)であること。			
				(3) 暗号化については、次のとおりとする。 ア 警察庁が別途指示する政府推奨の暗号アルゴリズムにより暗号化した上で、電磁的記録媒体に記録できること。 また、任意の周期で暗号鍵を変更できること。 イ 暗号化に使用した暗号鍵を電磁的記録媒体に記録できること。 ウ 暗号鍵生成のログが採取でき、暗号鍵を作成した年月日時分秒を確認できること。			
		ソフトウェア	OS	(1) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。			
				(2) 日本語に対応すること。			
			プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。			
			運用管理	(1) 本装置の本体部、バックアップ部及びテープライブラリ部の稼働状況を監視し、監視サーバAの運用管理ソフトウェアに通知できること。			
				(2) 監視サーバAの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携し、ジョブを実行できること。			
			ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア ログイン及びログアウト履歴 イ システムログ ウ アプリケーションログ エ セキュリティログ			
				(2) 監視サーバAのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。			
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。			
			ネットワーク管理	監視サーバAのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。			
			データレプリケーション	(1) ストレージA内で、データベースを記録したボリュームの複製が作成できること。			
				(2) 業務に影響することなく、ストレージA内で複製ボリュームの作成及び切離しができること。			
			バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。			
				(2) サーバを停止せずに、内蔵HDDのバックアップができること。			
				(3) 監視サーバAに収集されたログをテープライブラリ部の電磁的記録媒体にバックアップし、累積して管理できること。			
				(4) 業務に影響することなく、ストレージAのデータベースをバックアップ及びリストアするため、次の機能を有すること。 ア バックアップ (ア) 監視サーバAの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携し、定められた時刻に自動及び任意の時刻に手動で、ストレージAの複製ボリュームをオンラインから切離し、対象データをテープライブラリ部の電磁的記録媒体にバックアップできること。			
				(イ) バックアップデータは、日付、時刻及びバックアップの対象データを一意に識別できる名称で管理できること。			
				(ウ) バックアップは、1世代当たり正・副とし、3世代の管理ができること。			
				イ リストア (ア) オンラインから切り離された複製ボリューム並びにデータの更新、追加、削除のログ及びその他必要な情報から、データベースを障害発生直前の状態までリストアできること。			
				(イ) (ア)によりリストアできない場合、テープライブラリ部の電磁的記録媒体に保存されたバックアップデータ及びその他必要な情報から、データベースをバックアップ取得時の状態までリストアできること。			
				(ウ) データベースのリストアは、(4)ア(イ)の名称を指定してできること。			
				(5) 管理端末AからGUI又はWebブラウザにより、バックアップの設定及び監視ができること。			

			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				

9 ストレージA

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	ストレージA	本体部	ディスクアレイ	(1) RAID1、RAID5又はRAID6の冗長構成とする。RAID構成後の実記憶容量については、警察庁の承認を得ること。	基礎点			
				(2) (1)で決定した実記憶容量とは別に、HDD又はエンクロージャー等の増設により、取り扱う容量の拡張ができること。				
				(3) HDDのインタフェースは、SAS(Serial Attached SCSI)であること。				
				(4) 装置を停止せずにHDDの交換ができること。また、HDD障害時にホットスペアディスクを使用してRAID構成を自動で復旧できること。				
				(5) ホットスペアディスクを2個以上有すること。 なお、ホットスペアディスク2個以上の容量に相当するホットスペア専用の領域を、HDDに分散して有することも可とする。				
				(6) バックアップサーバと連携し、複製ボリュームの作成及び切離しができること。				
				(7) バックアップサーバと連携し、正常に一元バックアップできること。				
				(8) 本体部間でミラーリングができること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを2個以上有すること。				
				(2) 業務サーバ、バックアップサーバ及び試験業務サーバを接続するため、ファイバチャネルポートを必要数搭載すること。 なお、接続に当たって、ファイバチャネルスイッチの利用も可と				
				(3) 業務サーバ、バックアップサーバ及び試験業務サーバへの接続は冗長構成とし、各々のディスクコントローラで接続できること。				
			ネットワーク管理	監視サーバAのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			電源ユニット	冗長構成であること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				

10 ストレージB

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	ストレージB	本体部	ディスクアレイ	(1) RAID1、RAID5又はRAID6の冗長構成とする。RAID構成後の実記憶容量については、警察庁の承認を得ること。	基礎点			
				(2) (1)で決定した実記憶容量とは別に、HDD又はエンクロージャー等の増設により、取り扱う容量の拡張ができること。				
				(3) HDDのインタフェースは、SASであること。				
				(4) 装置を停止せずにHDDの交換ができること。また、HDD障害時にホットスペアディスクを使用してRAID構成を自動で復旧できること。				
				(5) ホットスペアディスクを2個以上有すること。なお、ホットスペアディスク2個以上の容量に相当するホットスペア専用の領域を、HDDに分散して有することも可とす				
				(6) 抽出サーバと連携し、複製ボリュームの作成及び切離しができること。				
				(7) 抽出サーバと連携し、正常に一元バックアップできること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを2個以上有すること。				
				(2) 抽出サーバを接続するため、ファイバチャネルポートを必要数搭載すること。 なお、接続に当たって、ファイバチャネルスイッチの利用も可と				
				(3) 抽出サーバへの接続は冗長構成とし、各々のディスクコントローラで接続できること。				
			ネットワーク管理	監視サーバBのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			電源ユニット	冗長構成であること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				

11 データ交換装置

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	データ交換装置	本体部	データ交換機能	(1) 抽出サーバからFTPによりファイルを受信できること。	基礎点			
				(2) 受信したファイルを、抽出サーバ等のネットワークから業務サーバ等のネットワークへの片方向に制限した転送ができること。				

				(3) 受信したファイルを業務サーバ及び試験業務サーバへFTPにより送信できること。				
				(4) 抽出サーバ等のネットワークと業務サーバ等のネットワーク間は、TCP/IPによるコネクションを確立しないこと。				
				(5) 抽出サーバ等のネットワークと業務サーバ等のネットワークがデータ交換を行う記録媒体には、抽出サーバ等のネットワークと業務サーバ等のネットワークから独立した制御系のコントロールにより、同時に接続できないこと。				
				(6) 抽出サーバ等のネットワークと業務サーバ等のネットワークがデータ交換を行う記録媒体には、アクセス制御により本装置以外からアクセスができないこと。				
				(7) データ交換の時間、間隔、回数等を任意に設定できること。				
				(8) 転送が完了した記録媒体上のファイルは、自動及び手動で削除できること。				
				(9) 転送容量として900Mバイト以上を1回の処理で転送できること。				
			ネットワークインタフェース	(1) 抽出サーバ等のネットワークに1000BASE-T以上に対応するポートを2個以上有すること。				
				(2) 業務サーバ等のネットワークに1000BASE-T以上に対応するポートを2個以上有すること。				
				(3) ネットワークは冗長構成ができること。				
			電源ユニット	冗長構成であること。				
			運用管理	本装置の稼働状況を監視し、監視サーバA及び監視サーバBの運用管理ソフトウェアに通知できること。				
			ログ管理	(1) 次の各項目のログを、電磁的記録媒体に保存できること。 ア ファイルの受信及び送信履歴 イ システムメッセージ なお、ログの記録可能容量は30Mバイト以上とする。				
				(2) 監視サーバA及び監視サーバBのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。				
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。				
			ネットワーク管理	監視サーバA及び監視サーバBのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				
		その他		任意の時点で、システムファイルを電磁的記録媒体へバックアップができること。				

12 時刻同期装置

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	時刻同期装置	本体部	時刻同期機能	(1) FMラジオの時報を受信し、1日1回以上、内蔵時計の時刻修正を自動で行えること。	基礎点			
				(2) 時刻修正の最大誤差は、日差±100ms以内であること。				
				(3) 時刻情報伝送プロトコルは、SNTP(Simple NetWork Time Protocol)及びNTP(Network Time Protocol)とし、警察庁サーバ、各ストレージ及び各スイッチの時刻修正ができること。				
				(4) うるう秒対応が自動又は手動で行えること。				
			ネットワークインタフェース	100BASE-TX以上に対応するポートを有すること。				

13 FW

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	FW	本体部	ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを2個以上有すること。	基礎点			
				(2) ネットワークの冗長構成ができること。				
			FW	(1) 最大スループットは、400Mbit/s以上であること。				
				(2) パケットフィルタリング機能を有すること。				
				(3) ISO/IEC 15408評価保証レベルにおいてCommonCriteria EAL3以上を取得していること。				
				(4) ステートフルインスペクション方式又はアプリケーションゲートウェイ方式であること。				
				(5) 特定の機器に対してアクセス制御できること。				

				(6) 最大同時セッション数は100,000以上であること。				
				(7) DynamicNAT、DynamicPAT及びStaticNATを有すること。				
				(8) アクティブ／スタンバイ型のクラスタ構成による冗長化ができること。				
			管理コンソール機能	(1) GUI又はWebブラウザ画面を使用した管理、設定及び監視ができること。				
				(2) アクセスログを保存できること。 なお、保存する容量は、30Gバイト以上有すること。				
				(3) (1)及び(2)については、専用の端末装置等を利用することも可とする。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				

14 試験Webサーバ

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	試験Webサーバ	本体部	CPU	Webサーバに準ずる処理能力を有すること。	基礎点			
			メモリ	(1) 本装置の構成品に含まれるソフトウェア及び業務用プログラムを起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。				
				(2) RAID構成後、本機器の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。				
				(3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
				(4) サーバを停止せずに、HDDの交換ができること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを5個以上有すること。				
				(2) ネットワークは冗長構成ができること。				
			電源ユニット	冗長構成であること。				
		バックアップ部		(1) RDX媒体を扱うことができること。				
				(2) 1回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。				
		ソフトウェア	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。				
				(2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。				
				(3) 日本語に対応すること。				
			ディレクトリサービス	(1) 業務用プログラムの要求受け、必要なユーザ情報を送信できること。				
				(2) 日本語に対応すること。				
				(3) SSLオプションを搭載すること。				
				(4) 500ユーザ以上を登録できること。				
				(5) ユーザ情報を管理する、GUIによるインターフェースを有すること。				
				(6) アクセス権管理システムが採用するユーザーインターフェースと互換性を有すること。				
			プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。				
			バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。				
				(2) サーバを停止せずに、内蔵HDDのバックアップができること。				
			運用管理	(1) 本装置の本体部及びバックアップ部の稼働状況を監視し、監視サーバAの運用管理ソフトウェアに通知できること。と。				
				(2) 監視サーバAの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携しジョブを実行できること。				

			ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア ログイン及びログアウト履歴 イ システムログ ウ アプリケーションログ エ セキュリティログ オ データベースへのアクセスログ				
				(2) 監視サーバAのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。				
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。				
			ネットワーク管理	監視サーバAのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) 監視サーバAからウイルス対策ソフトウェアの更新データを受信できること。				
				(4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				

15 試験業務サーバ

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	試験業務サーバ	本体部	CPU	業務サーバに準ずる処理能力を有すること。	基礎点			
			メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動して、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) RAID1、RAID5又はRAID6の冗長構成とする。				
				(2) RAID構成後、本機器の構成品に含まれるソフトウェア及び業務用プログラムを全てインストールして安定稼働できる実記憶容量を選定し、警察庁の承認を得ること。				
				(3) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
				(4) サーバを停止せずに、HDDの交換ができること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込ができること。				
			ネットワークインタフェース	(1) 1000BASE-T以上に対応するポートを3個以上有すること。				
				(2) ネットワークは冗長構成ができること。				
				(3) ストレージAへ接続するためのファイバチャネルポートを4個以上有すること。				
				(4) ストレージAへの接続は冗長構成とし、各々のディスクコントローラで接続できること。				
				(5) 冗長構成としたファイバチャネルについては、障害による自動閉塞機能及び自動切替機能を有すること。				
			電源ユニット	冗長構成であること。				
		バックアップ部		(1) RDX媒体を扱うことができること。				
				(2) 1回のバックアップ作業で、交換することなく単一の電磁的記録媒体でシステムバックアップを採取できること。				
		ソフトウェア	OS	(1) Redhat Enterprise Linux 7(64bit)又はこれと同等のものを搭載すること。				
				(2) 本装置の構成品に含まれる機器及びソフトウェア並びに業務用プログラムの全てが安定稼働すること。				
				(3) 日本語に対応すること。				
			データベース管理	次の機能を有するソフトウェアを搭載すること。 (1) 別途調達する業務用プログラムが、SQL及びストアドプロシージャの実行及び結果の取得ができること。				
				(2) 複数のデータベースサーバから、同一のデータベースにアクセス可能なこと。				
				(3) データベースの性能情報、運用状況の統計を作成でき、分析できること。				
			プロセス監視	プロセスを監視し、意図しないプロセス消滅時に自動的にプロセスの再起動ができること。				
			バックアップ	(1) 任意の時点で、内蔵HDDのバックアップができること。				

				(2) サーバを停止せずに、内蔵HDDのバックアップができること。				
			運用管理	(1) 本装置の本体部及びバックアップ部の稼働状況を監視し、監視サーバAの運用管理ソフトウェアに通知できること。				
				(2) 監視サーバAの運用管理ソフトウェアにおけるジョブスケジューリング機能と連携しジョブを実行できること。				
			ログ管理	(1) 次の各項目のログを本体部の内蔵HDDに保存できること。 なお、ログの詳細内容及び保存期間は警察庁と協議の上、決定すること。 ア ログイン及びログアウト履歴 イ システムログ ウ アプリケーションログ エ セキュリティログ オ データベースへのアクセスログ				
				(2) 監視サーバAのログ管理ソフトウェアからの要求に対して、保存したログを送出できること。				
				(3) 保存されたログは、管理者権限を与えられた者のみが閲覧できるよう閲覧権限を設定できること。				
			ネットワーク管理	監視サーバAのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) 監視サーバAからウイルス対策ソフトウェアの更新データを受信できること。				
				(4) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	1日1回以上、時刻同期装置と自動及び手動で時刻同期ができること。				

16 各端末(共通)

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	各端末(共通)	ソフトウェア	バックアップ	OSがインストールされたドライブのバックアップができ、内蔵HDD交換後にバックアップ取得時の状態まで復旧できるリカバリ媒体を作成できること。	基礎点			
			ソフトウェア配信クライアント	(1) 監視サーバA又は監視サーバBのソフトウェア配信サーバソフトウェアからの要求により、自動及び手動でソフトウェア及びソフトウェアのパッチを監視サーバA又は監視サーバBからダウンロードできること。				
				(2) 手動及び監視サーバA又は監視サーバBのソフトウェア配信サーバソフトウェアが指定したスケジュールにより自動でソフトウェア及びソフトウェアのパッチをインストールし、必要に応じて自動で再起動ができること。				
				(3) インストール結果並びにハードウェア及びソフトウェアのシステム状況を自動及び監視サーバA又は監視サーバBの要求に応じて通知できること。				
				(4) ソフトウェアのインストール時は必要に応じて管理者権限で実行できること。				
				(5) インストール失敗時には失敗した時点及び最初から再インストールする機能を有すること。				
			内蔵HDD暗号化	警察庁が別途指示する暗号化方式を使用すること。				
			外部記録媒体暗号化	(1) 外部記録媒体へ情報を書き込む際は、自動的に情報を暗号化できること。また、外部記録媒体から暗号化された情報を読み込む際に自動的に情報を復号できること。 なお、暗号化に用いる暗号鍵の更新は管理者権限を有する者のみが行えること。				
				(2) (1)の機能を用いない場合に備え、パスワードを用いて情報を暗号化及び平文による記録ができること。また、復号に用いるプログラムを配布できること。				
				(3) 警察庁が別途指示する暗号化方式を用いること。				
			外部記録媒体利用制限	(1) 事前に許可された外部記録媒体以外の利用を制限できること。				
				(2) USB機器(USBメモリを含む。)について、ベンダID、プロダクトID及びシリアルナンバ等の情報を用いることにより、個別に使用の可否を制御する機能を有すること。				
				(3) 外部記録媒体の利用の許可を与える権限を有するユーザは、ユーザID、端末装置、期間(日時)、許可の種別(平文又は暗号文の別)の条件を指定の上、外部記録媒体の利用の可否を変更できること。また、設定時にコメントを付加できること。				
				(4) 光学ディスクドライブの使用可否について制限できる機能を有すること。				
			証跡収集検証	(1) 外部記録媒体に対するファイル操作について、証跡の収集が行えること。 なお、証跡からファイル操作の年月日時分秒、ユーザID、ファイル名、ファイルサイズ及び平文又は暗号文の別を把握できること。				

				(2) (1)で収集した証跡を、監視サーバA又は監視サーバBに送信できること。また、検証を行う際、監視サーバA又は監視サーバBに送信した証跡を取得できること。				
				(3) (1)の証跡について、事前に指定されたユーザが検証できること。				
				(4) 外部記録媒体の利用の許可に係る証跡の収集が行えること。 なお、証跡から利用を許可した年月日時分秒、許可が終了する年月日時分秒、許可の内容(平文、暗号文の別)、許可をしたユーザID、許可を受けたユーザID及びコメントについて把握できること。				
				(5) (4)で収集した証跡を、監視サーバA又は監視サーバBに送信できること。また、検証を行う際、監視サーバA又は監視サーバBに送信した証跡を取得できること。				
				(6) (4)の証跡について、事前に指定されたユーザが検証できること。				
			ウイルス対策	(1) 保存されたファイルに対して、定められた時刻に自動及び任意の時刻に手動でウイルスチェックができること。				
				(2) ファイルアクセス時に自動でウイルスチェックができること。				
				(3) ウイルス対策ソフトウェアの更新データを自動及び手動で更新できること。				
			時刻同期	(1) OS起動時に、監視サーバA又は監視サーバBと自動で時刻同期ができること。				
				(2) 起動中については、前回調整時から24時間に1回以上、監視サーバA又は監視サーバBと自動で時刻同期ができること。また、任意の時点で手動による時刻同期ができること。				

17 専用端末A及び試験端末A

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	専用端末A及び試験端末A	本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。	基礎点			
			メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。				
			ネットワークインタフェース	10BASE-T/100BASE-TX/1000BASE-Tに対応するポートを有すること。				
			USBインタフェース	(1) USB3.0以上に対応するポートを有すること。				
				(2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを1ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。				
			ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。				
				(2) 表示色は、1,677万色以上であること。				
			キーボード	JIS規格キー配列に準拠していること。				
			マウス	(1) 2ボタン式以上の光学式又はレーザー式であること。				
				(2) ホイール等によりマウスを移動せずに画面のスクロールができること。				
			バッテリ	(1) パック方式で、交換可能な内蔵バッテリであること。				
				(2) バッテリ稼働時間は、社団法人電子情報技術産業協会「JEITA バッテリ動作時間測定法(Ver1.0)」準拠において、カタログ値で1時間以上であること。				
		認証部	生体認証ユニット	(1) USBにより、本体部と接続できること。				
				(2) 非接触型の読み取り装置であること。				
				(3) 他人許容率0.0002%以下かつ本人拒否率0.05%以下であること。				
				(4) 業務用プログラムと連携して、生体認証ができること。				
		ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。				
			アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 業務用プログラムが作成する帳票を、表示及び印刷できること。				
				(2) 業務用プログラム起動中、日本語から繁体字及び簡体字に入力の切替ができること。				
				(3) 業務用プログラム起動中、日本語からハングルに入力の切替ができること。				

			端末リモート操作クライアント	(1) 監視サーバA、管理端末A及びコンソール端末Aの端末リモート操作サーバソフトウェアからリモート操作を受け付けること。				
				(2) OS起動時にユーザーの操作とは無関係にバックグラウンドで自動的に開始できること。				

18 専用端末B及び試験端末B

区分	機器名			詳細内容	配点	根拠資料番号	備考	得点
必須項目	専用端末B及び試験端末B	本体部	CPU	プログラム仕様書の性能要件を満たす処理能力を有すること。	基礎点			
			メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。				
			ネットワークインタフェース	10BASE-T/100BASE-TX/1000BASE-Tに対応するポートを有すること。				
			USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。				
				(2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを1ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。				
			ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。				
				(2) 表示色は、1,677万色以上であること。				
			キーボード	JIS規格キー配列に準拠していること。				
			マウス	(1) 2ボタン式以上の光学式又はレーザー式であること。				
				(2) ホイール等によりマウスを移動せずに画面のスクロールができること。				
			バッテリ	(1) パック方式で、交換可能な内蔵バッテリであること。				
				(2) バッテリ稼働時間は、社団法人電子情報技術産業協会「JEITA バッテリ動作時間測定法(Ver1.0)」準拠において、カタログ値で1時間以上であること。				
		認証部	生体認証ユニット	(1) USBにより、本体部と接続できること。				
				(2) 非接触型の読み取り装置であること。				
				(3) 他人許容率0.0002%以下かつ本人拒否率0.05%以下であること。				
				(4) 業務用プログラムと連携して、生体認証ができること。				
		ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。				
			アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 ・業務用プログラムが作成する帳票を、表示及び印刷できること。				
			端末リモート操作クライアント	(1) 監視サーバB、管理端末B及びコンソール端末Bの端末リモート操作サーバソフトウェアからリモート操作を受け付けること。				
				(2) OS起動時にユーザーの操作とは無関係にバックグラウンドで自動的に開始できること。				

19 管理端末A

区分	機器名			詳細内容	配点	根拠資料番号	備考	得点
必須項目	管理端末A	本体部	CPU	(1) 統合監視、ストレージ管理及び運用管理のソフトウェアが同時に起動できること。	基礎点			
				(2) 同時に14個のWebブラウザ及びXサーバを起動して、安定稼働ができること。				
				(3) (1)、(2)を同時に起動しながら、業務用プログラムがプログラム仕様書の性能要件を満たす処理能力を有すること。				
			メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。				

			ネットワークインタフェース	1000BASE-T以上に対応するポートを2個以上有すること。			
			USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。			
				(2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを1ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。			
		表示部	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。			
				(2) 表示色は、1,677万色以上であること。			
		操作部	キーボード	JIS規格キー配列に準拠していること。			
			マウス	(1) 2ボタン式以上の光学式又はレーザー式であること。			
				(2) ホイール等によりマウスを移動せずに画面のスクロールができること。			
		認証部	生体認証ユニット	(1) USBにより、本体部と接続できること。			
				(2) 非接触型の読み取り装置であること。			
				(3) 他人許容率0.0002%以下かつ本人拒否率0.05%以下であること。			
				(4) 業務用プログラムと連携して、生体認証ができること。			
		ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。			
			警報装置制御	警報装置の音声ファイルの再生、ブザーの鳴動及び表示灯の点滅を制御できること。			
			Webブラウザ	WebGUIを使用して設定等作業を行う機器及びソフトウェアの仕様を満たすこと。			
			アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 警察庁が指示する形式のファイルを入出力できる表計算ソフト			
				(2) 業務サーバ等が使用する文字コードに対応するテキストエディタ			
				(3) 業務用プログラムが作成する帳票を、表示及び印刷できる画像表示ソフト			
			ファイル圧縮展開	(1) CAB形式、ZIP形式及びTAR形式で複数ファイル及びディレクトリを圧縮して1つのファイルに格納できること。			
				(2) CAB形式、ZIP形式、TAR形式及びZ形式のファイルを展開できること。			
				(3) CAB形式及びZIP形式の自己解凍型圧縮ファイルが作成できること。			
				(4) GUIにより操作ができること。			
			ユーザ管理	(1) Webサーバ及び試験Webサーバのディレクトリサービスと連携して、ユーザ情報の登録・削除・編集・検索がGUI又はWebブラウザで行えること。			
				(2) ユーザ情報の登録は一括で行えること。			
				(3) ユーザ情報をGUI又はWebブラウザの操作でファイル出力できること。			
				(4) ユーザ情報の操作ログをGUI又はWebブラウザの操作で出力できること。			
			Xサーバ	(1) X11R7以上に対応すること。			
				(2) 日本語に対応すること。			
				(3) 業務サーバ等のOSに対応すること。			
			統合監視	(1) 業務統合監視機能 監視サーバAの統合監視ソフトウェアと連携し、監視目的別に業務状況(運用管理、ログ管理、ネットワーク管理、ストレージ管理及び性能管理)を監視することができ、かつ、監視画面から各機能の監視画面に遷移し、階層を掘り下げることにより障害箇所を特定できること。			
				(2) コマンド制御機能 コマンドを業務サーバ等へ発行できること。また、発行したコマンド及び受信メッセージの履歴を照会できること。			
				(3) メッセージ監視機能 監視サーバAから通知されたメッセージについて、メッセージごとに内容説明や処置方法を日本語で表示及び印字できること。			
			ストレージ管理	ストレージAの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報(HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報)をGUI又はWebブラウザで表示できること。			
				(2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。			
				(3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。			

				(4) メッセージにより、ストレージAのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。				
			運用管理	監視サーバAの運用管理ソフトウェアと連携し、外部サーバのジョブの実行及び管理ができること。				
			端末リモート操作サーバ	専用端末A及び試験端末Aの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末A及び専用端末AのOSへのログイン操作ができること。				
				(2) 専用端末A及び試験端末Aと管理端末A間でクリップボードの情報を共有できること。				
				(3) 専用端末A及び試験端末Aと管理端末A間でファイルの送受信ができること。				

20 管理端末B

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	管理端末B	本体部	CPU	(1) 統合監視、ストレージ管理及び運用管理のソフトウェアが同時に起動できること。	基礎点			
				(2) 同時に8個のWebブラウザ及びXサーバを起動して、安定稼働ができること。				
				(3) (1)、(2)を同時に起動しながら、業務用プログラムがプログラム仕様書の性能要件を満たす処理能力を有すること。				
			メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。				
			ネットワークインタフェース	1000BASE-T以上に対応するポートを2個以上有すること。				
			USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。				
				(2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを1ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。				
		表示部	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。				
				(2) 表示色は、1,677万色以上であること。				
		操作部	キーボード	JIS規格キー配列に準拠していること。				
			マウス	(1) 2ボタン式以上の光学式又はレーザー式であること。				
				(2) ホイール等によりマウスを移動せずに画面のスクロールができること。				
		認証部	生体認証ユニット	(1) USBにより、本体部と接続できること。				
				(2) 非接触型の読み取り装置であること。				
				(3) 他人許容率0.0002%以下かつ本人拒否率0.05%以下であること。				
				(4) 業務用プログラムと連携して、生体認証ができること。				
		ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。				
			警報装置制御	警報装置の音声ファイルの再生、ブザーの鳴動及び表示灯の点滅を制御できること。				
			Webブラウザ	(1) 日本語に対応すること。				
				(2) WebGUIを使用して設定等作業を行う機器及びソフトウェアの仕様を満たすこと。				
			アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 警察庁が指示する形式のファイルを入出力できる表計算ソフト				
				(2) 抽出サーバ等が使用する文字コードに対応するテキストエディタ				
				(3) 業務用プログラムが作成する帳票を、表示及び印刷できる画像表示ソフト				
			ファイル圧縮展開	(1) CAB形式、ZIP形式及びTAR形式で複数ファイル及びディレクトリを圧縮して1つのファイルに格納できること。				
				(2) CAB形式、ZIP形式、TAR形式及びZ形式のファイルを展開できること。				
				(3) CAB形式及びZIP形式の自己解凍型圧縮ファイルが作成できること。				

				(4) GUIにより操作ができること。				
			Xサーバ	(1) X11R7以上に対応すること。				
				(2) 日本語に対応すること。				
				(3) 抽出サーバ等のOSに対応すること。				
			統合監視	(1) 業務統合監視機能 監視サーバBの統合監視ソフトウェアと連携し、監視目的別に業務状況(運用管理、ログ管理、ネットワーク管理、ストレージ管理及び性能管理)を監視することができ、かつ、監視画面から各機能の監視画面に遷移し、階層を掘り下げることにより障害箇所を特定できること。				
				(2) コマンド制御機能 コマンドを抽出サーバ等へ発行できること。また、発行したコマンド及び受信メッセージの履歴を照会できること。				
				(3) メッセージ監視機能 監視サーバBから通知されたメッセージについて、メッセージごとに内容説明や処置方法を日本語で表示及び印字できること。				
			ストレージ管理	ストレージBの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報(HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報)をGUI又はWebブラウザで表示できること。				
				(2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。				
				(3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。				
				(4) メッセージにより、ストレージBのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。				
			運用管理	監視サーバBの運用管理ソフトウェアと連携し、内部サーバのジョブの実行及び管理ができること。				
			端末リモート操作サーバ	専用端末B及び試験端末Bの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末B及び試験端末BのOSへのログイン操作ができること。				
				(2) 専用端末B及び試験端末Bと管理端末B間でクリップボードの情報を共有できること。				
				(3) 専用端末B及び試験端末Bと管理端末B間でファイルの送受信ができること。				

21 コンソール端末A

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	コンソール端末A	本体部	CPU	同時に14個のWebブラウザ及びXサーバを起動して、安定稼働ができること。	基礎点			
			メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。				
			ネットワークインタフェース	1000BASE-T以上に対応するポートを2個以上有すること。				
			USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。				
				(2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを1ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。				
		表示部	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。				
				(2) 表示色は、1,677万色以上であること。				
		操作部	キーボード	JIS規格キー配列に準拠していること。				
			マウス	(1) 2ボタン式以上の光学式又はレーザー式であること。				
				(2) ホイール等によりマウスを移動せずに画面のスクロールができること。				
		ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。				
			Webブラウザ	(1) 日本語に対応すること。				
				(2) WebGUIを使用して設定等作業を行う機器及びソフトウェアの仕様を満たすこと。				
			アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 警察庁が指示する形式のファイルを入出力できる表計算ソフト				

				(2) 業務サーバ等が使用する文字コードに対応するテキストエディタ				
				(3) 30Mバイト以上ログファイルを取り扱えられるテキストエディタ				
			Xサーバ	(1) X11R7以上に対応すること。。				
				(2) 日本語に対応すること。				
				(3) 業務サーバ等のOSに対応すること。				
			ストレージ管理	ストレージAの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報(HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報)をGUI又はWebブラウザで表示できること。				
				(2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。				
				(3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。				
				(4) メッセージにより、ストレージAのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。				
			端末リモート操作サーバ	専用端末A及び試験端末Aの端末リモート操作クライアントソフトウェアと連携して次の操作ができること。 (1) 専用端末A及び試験端末AのOSへのログイン操作ができること。				
				(2) 専用端末A及び試験端末Aとコンソール端末A間でクリップボードの情報を共有できること。				
				(3) 専用端末A及び試験端末Aとコンソール端末A間でファイルの送受信ができること。				

22 コンソール端末B

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	コンソール端末A	本体部	CPU	同時に8個のWebブラウザ及びXサーバを起動して、安定稼働ができること。	基礎点			
			メモリ	(1) 本機器の構成品に含まれるソフトウェア及び業務用プログラムを全て起動し、安定稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) メモリの増設又は交換により、(1)を満たす容量から拡張した容量を取り扱えること。				
			内蔵HDD	(1) ソフトウェア及び業務用プログラムをインストールし、安定して稼働できる容量を選定し、警察庁の承認を得ること。				
				(2) 運用期間中、交換又は増設による拡張の必要がない、十分な容量を有すること。				
			光学ディスクドライブ	DVD規格及びCD規格の媒体の読込及び書込ができること。				
			ネットワークインタフェース	1000BASE-T以上に対応するポートを2個以上有すること。				
			USBインタフェース	(1) USB3.0以上に対応するインターフェースを有すること。				
				(2) 本体部に接続する必要がある機器を全て接続できる数に加え、USB3.0以上に対応する空きポートを1ポート以上有すること。 なお、USBハブにより必要なポート数を確保することも可とする。				
		表示部	ディスプレイ	(1) 解像度は、1,280×1,024ドット以上であること。				
				(2) 表示色は、1,677万色以上であること。				
		操作部	キーボード	JIS規格キー配列に準拠していること。				
			マウス	(1) 2ボタン式以上の光学式又はレーザー式であること。				
				(2) ホイール等によりマウスを移動せずに画面のスクロールができること。				
		ソフトウェア	OS	Microsoft Windows10を搭載し、日本語に対応すること。 なお、エディション等の詳細については、警察庁が別途指示する。				
			Webブラウザ	(1) 日本語に対応すること。				
				(2) WebGUIを使用して設定等作業を行う機器及びソフトウェアの仕様を満たすこと。				
			アプリケーション	次の機能を有し、日本語に対応するソフトウェアを搭載すること。 (1) 警察庁が指示する形式のファイルを入出力できる表計算ソフト				
				(2) 抽出サーバ等が使用する文字コードに対応するテキストエディタ				
				(3) 30Mバイト以上ログファイルを取り扱えられるテキストエディタ				
			Xサーバ	(1) X11R7以上に対応すること。				
				(2) 日本語に対応すること。				

				(3) 抽出サーバ等のOSに対応すること。				
			ストレージ管理	ストレージBの管理機能として次の機能を有すること。 (1) ディスクアレイの構成情報(HDDの物理名称、エンクロージャ、プール及び制御装置にかかる情報)をGUI又はWebブラウザで表示できること。				
				(2) ディスクアレイに対する監視の開始及び停止が自動及び手動で操作できること。				
				(3) ディスクアレイに対し、ディスクアレイ名及び論理ディスク名の設定ができること。				
				(4) メッセージにより、ストレージBのディスクアレイの状態をGUI又はWebブラウザ画面上で監視できること。また、構成の変更が生じた場合は、ディスクアレイ構成情報を反映できること。				
			端末リモート操作サーバ	専用端末B及び試験端末Bの端末リモート操作クイアントソフトウェアと連携して次の操作ができること。 (1) 専用端末B及び試験端末BのOSへのログイン操作ができること。				
				(2) 専用端末B及び試験端末Bとコンソール端末B間でクリップボードの情報を共有できること。				
				(3) 専用端末B及び試験端末Bとコンソール端末B間でファイルの送受信ができること。				

23 警報装置

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	警報装置	本体部	基本機能	(1) 音声ファイルの再生、ブザーの鳴動及び表示灯の点滅を、警察庁サーバ及び端末等から制御できること。 なお、再生、鳴動及び点滅パターンについては、警察庁と協議すること。	基礎点			
				(2) 警察庁サーバから要求により、鳴動及び点滅の状態を回答できること。				
				(3) 20個以上の音声ファイルが登録でき、再生できること。				
				(4) 音量調整ができること。				
				(5) ボタンの操作により、点滅、鳴動及び再生を停止できること。				
				(6) 表示灯は、赤、黄及び緑の3色とすること。				
			ネットワークインタフェース	10BASE-T/100BASE-TX以上に対応するポートを有し、ネットワーク接続ができること。				
			時刻同期	24時間に1回以上、監視サーバA又は監視サーバBと自動で時刻同期ができること。				

24 スキャナ

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	スキャナ	本体部	基本機能	(1) カラー読み取りができること。	基礎点			
				(2) 最大読取原稿サイズは、A4サイズであること。				
				(3) 最高光学解像度は、1,200×1,200dpi以上であること。				
				(4) 読取速度は、A4原稿モノクロで読取解像度が600dpiの場合5ms/line以上であること。また、A4原稿カラーで読取解像度が600dpiの場合5ms/line以上であること。				
				(5) USB2.0以上に対応するインタフェースで、専用端末及び試験端末に接続できること。				
				(6) TWAIN対応であること。				

25 印字装置

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	印字装置	本体部	基本機能	(1) レーザープリンタ(モノクロ)であること。	基礎点			
				(2) 各端末からTCP/IPを利用して印字できること。				
				(3) 用紙は、普通紙単票のA4サイズに対応すること。				
				(4) 解像度が600×600dpi以上で印字できること。				
				(5) A4で20枚/分以上の印字速度であること。				
				(6) 200枚以上の自動給紙が可能なカセットを有すること。				
			ネットワークインタフェース	(1) 10BASE-T/100BASE-TXに対応するポートを有すること。				
				(2) 無線LAN機能を標準で搭載している場合は、無線LAN機能を停止できること。 なお、利用者による設定変更ができないこと。				
			その他	電磁的記録媒体への入出力機能を有しないこと。				

26 L3SW

区分	機器名	詳細内容	配点	根拠資料番号	備考	得点

必須項目	L3SW	本体部	基本機能	(1) 24Gbit/s以上のスイッチング容量を有すること。	基礎点			
				(2) レイヤ2及びレイヤ3におけるスイッチング処理能力が12Mパケット/s以上であること。				
				(3) 各ポート単位にスイッチング、ルーティングができること。				
				(4) 各ポートの稼働状態を表示するLEDを有すること。				
				(5) RFC2338に準拠したVRRP(Virtual Router Redundancy Protocol)機能又はHSRP(HotStandby Router Protocol)機能を有すること。				
				(6) ルーティングプロトコルはRIP(Routing Infomation Protocol)ver1、RIPver2及びOSPF(Open Shortest Path First)が使用できること。				
				(7) RIP、OSPF間において相互の情報交換ができること。				
				(8) 静的な経路設定ができること。				
				(9) MACアドレス、IPアドレス及びTCP/UDPポート番号によるフィルタリングができること。				
				(10) ポートベースVLAN機能を有すること。				
				(11) IEEE802.1qに準拠したVLANタギング機能を有すること。				
				(12) IEEE802.1dに準拠したスパニングツリー機能を有し、VLAN単位に動作すること。				
				(13) IEEE802.3adに準拠したリンクアグリゲーション機能を有すること。				
				(14) IPアドレス、論理ポート等により、データ入出力の可否を制御できること。				
			ネットワークインタフェース	(1) 1000BASE-T以上のポートを24個以上有すること。				
				(2) ネットワークは冗長構成とし、切替えが任意にできること。				
			ネットワーク管理	(1) 監視サーバA又は監視サーバBのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
				(2) RMON(Remote Network Monitoring)に対応すること。				
			時刻同期	1日1回以上、時刻同期装置又は監視サーバAと自動及び手動で時刻同期ができること。				
			電源ユニット	冗長構成であること。				
			バックアップ	(1) 装置内の各モジュールの構成情報データ及びソフトウェアを電磁的記録媒体に保持し、電源のオン／オフ時及び各モジュール交換後の再設定が不要であること。				
				(2) 各設定情報をファイルに保存及び読み込みができること。				

27 ハブⅠ

区分	機器名	詳細内容			配点	根拠資料番号	備考	得点
必須項目	ハブⅠ	本体部	ネットワークインタフェース	(1) 16Gbit/s以上のスイッチング容量を有すること。	基礎点			
				(2) 1000BASE-T以上に対応する自動認識ポートを16個以上有すること。				
				(3) ネットワークは冗長構成ができること。				
				(4) ストア及びフォワード方式によるパケットスイッチング機能を有すること。				
				(5) 各ポートの稼働状態を表示するLEDを有すること。				
				(6) 8グループ以上設定可能なVLAN機能を有すること。				
				(7) VLAN単位ごとに、IEEE802.1dに準拠したスパニングツリー機能を有すること。				
				(8) IEEE802.3adに準拠したリンクアグリゲーション機能を有すること。				
			ネットワーク管理	監視サーバA又は監視サーバBのネットワーク管理ソフトウェアからの要求に対して、MIB情報を回答する機能を有すること。				
			時刻同期	1日1回以上、時刻同期装置又は監視サーバAと自動及び手動で時刻同期ができること。				

最高点	基礎点	10,000	総合得点	基礎点	
	加点	42		加点	
	合計点	10,042		合計点	

事前旅客情報システム及び外国人個人識別情報認証システム

加点項目

区分・機器名等				評価基準(必須)	加点基準	配点	提案内容	根拠資料番号	得点
加点項目	保守体制	官庁執務時間内における障害対応までの時間	警察庁、各管区警察局及び都道府県警察	警察庁から技術者の派遣要請があった場合は、3時間以内に技術者を派遣すること。 ただし、警察庁及び都道府県警察本部（方面本部を含む）設置の機器を対象とし、警察署等設置機器は除く。	警察庁から技術者の派遣要請があった場合は、2時間以内に技術者を派遣すること。 ただし、警察庁及び都道府県警察本部（方面本部を含む）設置の機器を対象とし、警察署等設置機器は除く。	42			

最高点	基礎点	10,000	総合得点	基礎点	
	加点	42		加点	
	合計点	10,042		合計点	

事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム

必須項目

1．1 総合

区　分	機能名	詳　細　内　容	配　点	根拠資料番号	備考	得　点
必須項目	設計条件	仕様書に示す条件を満足すること。	基礎点			

1．2 サーバ用プログラムの共通機能

区　分	機能名	詳　細　内　容		配　点	根拠資料番号	備考	得　点
必須項目	アクセス権	種類	次の分類に応じてアクセス権を設定できること。 なお、アクセス権設定の詳細は、警察庁が別途指示する。 (1) ユーザグループ (2) 所属 (3) 警察BLファイル(登録データ(BICS)を含む。)	基礎点			
		範囲	アクセス権に応じて、登録、照会、表示及びファイル入出力等の機能を制御すること。 なお、制御する機能については、警察庁が別途指示する。				
	入出力制御	印刷物の様式は、機能要件で示す機能ごとに設定ができ、容易に改修できること。	(1) 画面に表示された各種一覧、詳細データ及び画像が印刷できること。 なお、印刷物の様式については警察庁が別途指示する。				
			(2) 印刷物の様式は、機能要件で示す機能ごとに設定ができ、容易に改修できること。				
			(3) 印刷物には、次に示すデータを付加すること。 ア 印刷年月日時分 イ 端末名 ウ 所属名 エ ユーザ名				
			(4) 印刷をする際、印刷イメージを生成し、端末等でダウンロードして確認できること。				
		ファイル出力制御	(1) 画面に表示された一覧の詳細データを、CSV形式で出力できること。				
			(2) 出力するデータには、次に示すデータを付加すること。 ア 出力年月日時分 イ 端末名 ウ 所属名 エ ユーザ名				
			(3) ファイル出力は、機能要件で示す機能ごとに設定ができること。				
		電磁的記録媒体入出力制御	(1) 印刷イメージ及びCSVファイルを電磁的記録媒体に出力できること。				
			(2) 電磁的記録媒体に出力する場合、出力する電磁的記録媒体及びフォルダの指定ができること。				
			(3) 電磁的記録媒体からデータの入力ができること。				
			(4) 電磁的記録媒体から入力する場合、入力する電磁的記録媒体及びフォルダの指定ができること。				
	業務管理統計	作成	条件を指定して統計表が作成できること。 なお、統計表の詳細については、警察庁が別途指示する。				
		参照	統計参照権限のあるユーザは、統計表を参照できること。				
		定期抹消	登録の件数を保存した日から起算して1年以上経過したデータを月単位で抹消できること。				
	運用連絡通報	通報通知	(1) 運用連絡通報の内容を入力、訂正及び削除ができること。				
			(2) 通報日時及び通報先を指定し専用端末等に通知できること。				
			(3) 送信した運用連絡通報を管理できること。				
			(4) 送信時、端末等に併設する警報装置の動作を制御できること。 なお、警報装置の制御の詳細については、警察庁が別途指示する。				
	接続状態	表示	(1) 運用環境への端末等の接続状態を、管理端末A又は管理端末Bに表示できること。 なお、接続状態の表示の詳細については警察庁が別途指示する。				
			(2) 試験環境への端末等の接続状態を、管理端末A又は管理端末Bに表示できること。 なお、接続状態の表示の詳細については警察庁が別途指示する。				
		接続	(1) 運用環境への端末等の接続を開始・停止できること。				
			(2) 試験環境への端末等の接続を開始・停止できること。				
	アクセスログ	生成	サーバ用プログラムの機能に対する端末等からのアクセスについて、アクセス開始・終了日時、使用した端末、ユーザ所属(府県、課、係等)、氏名(ユーザを識別する符号を含む。)、各処理の内容、入力項目等のアクセスログを生成すること。また、生成したアクセスログを保存できること。 なお、アクセスログの詳細については警察庁と別途協議すること。				
		参照	(1) アクセスログ参照権限のあるユーザは、保存したアクセスログを下記の条件を指定して、端末等から参照できること。 ア アクセス開始・終了日時 イ ユーザ所属 ウ 端末等				
			(2) ユーザのアクセス権限に応じて、参照できるアクセスログの項目を設定できること。				
		定期抹消	保存した日から起算して5年以上経過したログを日単位で自動抹消できること。				
	システムログ	生成	業務用プログラムの運用状況、エラー及び障害の発生をシステムログに生成すること。また、生成したシステムログを保存すること。				
		参照	システムログを管理端末A又は管理端末Bから参照できること。				
		定期抹消	保存した日から起算して5年以上経過したログを日単位で自動抹消できること。				

1．3 抽出プログラムの機能

区　分	機能名	詳　細　内　容		配　点	根拠資料番号	備考	得　点
必須項目	抽出プログラム共通機能	通信制御機能	(1) 専用端末B等通信制御 専用端末B等と登録データ(BICS)のデータ通信を制御すること。	基礎点			
			(2)　中継サーバ通信制御 中継サーバとホスト情報のデータ通信を制御できること。				
			(3)　警察庁指掌紋システム通信制御 警察庁指掌紋システムと指紋画像情報のデータ通信を制御できること。				
			(4)　データ交換装置通信制御 データ交換装置とのデータ通信を制御できること。				
			(5)　冗長構成を用いた業務継続 装置異常時に、冗長構成の機器である抽出サーバを利用して業務の継続ができること。				
		入力検査	(1)　専用端末B等から入力された登録のデータについて、検査をすること。 なお、検査の詳細については、警察庁が別途指示する。				
			(2)　検査結果を専用端末B等に表示すること。 なお、表示の詳細については警察庁が別途指示する。				
		件数カウント	(1)　登録の件数をカウントすること。				
			(2)　カウントした件数が専用端末B等に表示できること。 なお、表示の詳細については警察庁が別途指示する。				
		処理状況表示	登録の処理状況を専用端末B等に表示すること。 なお、表示の詳細については警察庁が別途指示する。				
		処理確認	処理が完了した場合、その結果を専用端末B等に表示できること。 なお、結果の表示の詳細については警察庁が別途指示する。				
	ホスト情報登録	取得	(1)　取得するホスト情報ごとに、中継サーバへの接続先を設定できること。				
			(2)　中継サーバからホスト情報を取得し、取得後、中継サーバへ当該ホスト情報の削除を指示すること。				
			(3)　取得したホスト情報から、APIS、BICS及びホストコードのそれぞれで必要なファイルを判別し、それぞれの作業領域にコピーすること。				
		抽出(APIS)	(1)　APISの作業領域に保存したホスト情報からAPISに必要な情報を抽出し、ホスト情報(APIS)を作成すること。 なお、必要な情報の詳細については警察庁が別途指示する。				
			(2)　ホスト情報及びホスト情報(APIS)は、世代管理を行い、一定期間保存すること。 なお、保存する一定期間については、警察庁が別途指示する。				
		抽出(BICS)	(1)　BICSの作業領域に保存したホスト情報を検索し、条件を満たすホスト情報を警察システムの文字コードに変換(大文字及び小文字の置換、全角文字及び半角文字の置換等を含む。)ができること。 なお、条件については警察庁が別途指示する。				
			(2)　変換したホスト情報からBICSに必要な情報を抽出し、ホスト情報(BICS)を作成すること。 なお、必要な情報の詳細については警察庁が別途指示する。				
		登録(BICS)	(1)　抽出(BICS)機能で作成したホスト情報(BICS)を抽出DB(BICS)に抽出データ(今回)として登録すること。				
			(2)　抽出DB(BICS)に登録されている前回の抽出データ(以下、「抽出データ(前回)」という。)と抽出データ(今回)を比較して差分データを抽出し、抽出DB(BICS)に登録すること。				
			(3)　抽出DB(BICS)から抽出データ(前回)を削除し、削除後、抽出データ(今回)を抽出データ(前回)に置換すること。				
			(4)　抽出DB(BICS)に登録されている、前々回の差分データを削除し、前回の差分データを削除待ち状態とすること。				
		登録結果通知	(1)　抽出DB(BICS)に差分データが登録できた場合、登録の完了、登録件数、処理日時等を管理端末Bに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。				
			(2)　抽出DB(BICS)に差分データが登録できなかった場合、登録の失敗、処理日時等を管理端末Bに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。				
		処理時間制限	差分データの登録処理が制限時間を超えた場合、管理端末Bへ通知すること。 なお、制限時間及び通知内容の詳細については、警察庁が別途指示する。				
	指紋画像情報登録	抽出	抽出DB(BICS)から最新の差分データを抽出すること。				
		取得	差分データを基に、警察庁指掌紋システムから指紋画像情報を取得すること。				
		登録	(1)　警察庁指掌紋システムから取得した指紋画像情報のうち身分事項については、警察システムの文字コードに変換(大文字及び小文字の置き換え、全角文字及び半角文字の置き換え等を含む。)し、抽出DB(BICS)に登録すること。 なお、警察システムの文字コードの詳細については、警察庁が別途指示する。				
			(2)　警察庁指掌紋システムから取得した指紋画像情報の身分事項と差分データの身分事項を照合し、適合及び不適合の判定を行い、適合した差分データ(以下「適合データ」という。)を抽出DB(BICS)に登録すること。また、判定結果を専用端末Bに通知できること。 なお、適合及び不適合の判定の詳細については、警察庁が別途指示する。				
			(3)　指紋画像情報が未取得の差分データ及び不適合となった差分データについては、一定期間管理できること。 なお、管理する一定期間については、警察庁が別途指示する。				
		一連番号の生成	抽出DB(BICS)に適合データを登録する際には、1件単位に一連番号を生成すること。 なお、生成する一連番号の体系については警察庁が別途指示する。				
		登録結果通知	(1)　抽出DB(BICS)に適合データが登録できた場合、登録の完了、登録件数、処理日時等を管理端末Bに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。				
			(2)　抽出DB(BICS)に適合データが登録ができなかった場合、登録の失敗、処理日時等を管理端末Bに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。				

	処理時間制限	適合データの登録処理が制限時間を超えた場合、管理端末Bへ通知すること。 なお、制限時間及び通知内容の詳細については、警察庁が別途指示する。			
専用端末Bからの登録	登録画像の読込み	(1) スキャナ又は電磁的記録媒体から、画像の読込みができること。 なお、画像の解像度及び形式等については、警察庁が別途指示する。			
		(2) 読込んだ登録画像の切り出し処理、解像度変更及び白黒反転等の加工ができること。 なお、切り出し位置、解像度等、加工の詳細については、警察庁が別途指示する。			
		(3) 読込んだ画像を、警察庁が別途指示する画像形式の登録画像及び専用端末Bで表示できる形式の画像に変換できること。 なお、専用端末Bに表示する形式については、警察庁と別途協議すること。			
		(4) 変換した画像を、専用端末B等に表示できること。			
	登録	(1) 抽出DB(BICS)に登録する登録データ(BICS)を専用端末Bから1件単位で入力できること。			
		(2) (1)の入力内容について、入力検査の結果に異常が無い場合は、入力内容に基づいて指紋画像情報を取得し、登録データ(BICS)と関連付けること、又は、上記「登録画像の読み込み」で変換した登録画像と関連付けること。 なお、指紋画像情報の取得の詳細については警察庁が別途指示する。			
		(3) 登録データ(BICS)と、指紋画像情報又は登録画像との関連付けができた場合、抽出DB(BICS)に登録データ(BICS)を新規登録できること。			
		(4) 入力検査の結果に異常がない場合、抽出DB(BICS)の登録データ(BICS)を訂正登録できること。			
		(5) 登録データ(BICS)を抽出DB(BICS)に登録する際には、1件単位に一連番号を自動で生成又は入力できること。 なお、生成する一連番号の体系については警察庁が別途指示する。			
		(6) 登録データ(BICS)の抽出DB(BICS)への登録結果を専用端末Bに表示すること。 なお、登録結果の詳細については、警察庁が別途指示する。			
	注意喚起	登録データ(BICS)を抽出DB(BICS)に登録送付する前に、専用端末Bに注意喚起を促すメッセージを表示すること。			
	定期抹消	(1) 一定期間以上経過した抽出DB(BICS)に登録された登録データ(BICS)を日単位で抽出DB(BICS)から抹消すること。 なお、一定期間の詳細については、警察庁が別途指示する。			
		(2) 定期抹消した結果を専用端末B等に表示できること。 なお、表示の詳細については警察庁が別途指示する。			
ホスト情報(APIS)及び転送データ(BICS)の転送	転送データ(BICS)の抽出	(1) 抽出DB(BICS)から、転送用に適合データ及び登録データ(BICS)(以下「転送データ(BICS)」という。)を自動抽出すること。 なお、自動抽出方法、抽出時刻、抽出ファイル、抽出項目等については、警察庁が別途指示する。			
		(2) (1)の転送データ(BICS)については、抽出DB(BICS)とは別に保存すること。			
		(3) 自動抽出のほか、任意の時刻に管理端末Bを用いて手動で抽出ができること。			
		(4) 抽出結果の確認ができること。 なお、抽出結果の確認方法については、警察庁が別途指示する。			
	定期抹消	抽出DB(BICS)の定期抹消を行う場合、定期抹消する登録データ(BICS)を抽出DB(BICS)から抽出し、データ交換装置を介して、業務サーバにFTPにより自動転送し、該当する警察BLDB(BICS)を削除登録できること。 なお、定期抹消の詳細については、警察庁が別途指示する。また、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。			
	転送(APIS)	(1) 保存されたホスト情報(APIS)については、データ交換装置を介して、業務サーバにFTPにより自動転送できること。 なお、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。			
		(2) 自動転送のほか、手動による即時転送及び転送停止ができること。			
		(3) 転送結果の確認ができること。 なお、転送結果の確認方法については、警察庁が別途指示する。			
	転送(BICS)	(1) 抽出した転送データ(BICS)については、データ交換装置を介して、業務サーバにFTPにより自動転送できること。 なお、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。			
		(2) 自動転送のほか、手動による即時転送及び転送停止ができること。			
		(3) 転送結果の確認ができること。 なお、転送結果の確認方法については、警察庁が別途指示する。			
	表示	(1) ホスト情報(APIS)の転送結果を管理端末Bに表示できること。 なお、転送結果の表示の詳細については警察庁が別途指示する。			
		(2) 転送データ(BICS)を条件指定して管理端末Bに表示できること。 なお、条件及び表示方法の詳細については警察庁が別途指示する。			
		(3) 抽出及び転送が正常に終了しなかった場合、異常のあった旨を管理端末B及び警報装置に通知ができること。 なお、通知の詳細については警察庁が別途指示する。			
		(4) 管理端末Bから転送に関する履歴が管理できること。			
試験	試験環境	(1) 運用環境と同等の機能が確認できる試験環境を構築できること。 なお、試験環境は業務で使用するものとは別に作成し、運用環境に影響を与えないこと。			
		(2) 試験環境は専用端末B等と接続ができること。また、試験接続は、専用端末B等ごとに設定ができること。			
		(3) 試験中は、専用端末B等に試験中であることを明示すること。			
接続	警察庁ホストシステムとの接続	運用環境及び試験環境から中継サーバと接続ができること。			
	警察庁指掌紋システムとの接続	運用環境及び試験環境から警察庁指掌紋システムの運用環境及び試験環境と接続できること。			

	メンテナンス	ログ出力設定	専用端末B等ごと及びアクセス権ごとに、出力できるログの種類及び出力内容を設定できること。 なお、ログの種類及び出力内容の詳細については警察庁が別途指示する。			
		試験環境設定	(1) 専用端末B等ごとに試験環境に接続する設定ができること。			
			(2) 試験環境へ接続している専用端末B等の情報が一覧で表示できること。 なお、一覧表示の詳細については警察庁が別途指示する。			
		登録データ(BICS)等内容確認	(1) 抽出DB(BICS)に登録されている転送データ(BICS)の内容を、日時又は期間を指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。			
			(2) 抽出DB(BICS)に登録されている登録データ(BICS)の内容を一連番号又は全てを指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。			
		変換テーブル等メンテナンス	(1) コード変換テーブルの更新ができること。 なお、変換テーブルは警察庁からデータを提供することとし、変換が必要なデータ、変換方法、変換タイミング等の詳細については、警察庁が別途指示する。			
			(2) 運用環境と試験環境で、コードの同期がとれること。			
		定期抹消設定	定期抹消において、登録データファイル(BICS)ごとに抹消結果の通知先を設定できること。			
		ホスト情報等登録結果	(1) ホスト情報等の登録結果を管理端末Bに表示すること。 なお、登録結果の表示の詳細については別途指示する。			
			(2) ホスト情報等の登録において異常があった場合、その内容を管理端末Bに表示すること。			
		警察庁ホストシステム間機能の開始・停止設定	(1) ホスト情報の取得の開始・停止を設定できること。			
			(2) 中継サーバと抽出サーバの接続状況を管理端末Bから確認できること。 なお、接続状況の表示の詳細については警察庁が別途指示する。			
		警察庁指掌紋システム間機能の開始・停止設定	(1) 指紋画像情報の取得の開始・停止を設定できること。			
			(2) 警察庁指掌紋システムと抽出サーバ等の接続状況を管理端末Bから確認できること。 なお、確認方法については警察庁が別途指示する。			
		業務サーバ間機能の開始・停止機能	(1) ホスト情報(APIS)及び転送データ(BICS)の転送の開始・停止を設定できること。			
			(2) 転送機能の状態を管理端末Bから確認できること。 なお、確認方法については警察庁が別途指示する。			
	ユーザ情報	認証	(1) 専用端末B等に接続した生体認証装置による生体情報の取得及び送信等を制御できること。			
			(2) ユーザの認証情報を、端末Bプログラムから受信できること。			
			(3) 受信したユーザの認証情報から、ユーザの照合ができること。			
			(4) 認証が認められた場合、対応するユーザ情報をアクセス権管理システムから取得できること。			
			(5) 取得したユーザ情報から、抽出プログラムにログインできること。			
			(6) 取得したユーザ情報から、業務ごとにアクセス権の制御を行うこと。			
			(7) 認証が認められなかった場合、再度認証を行い、一定回数認証が認められなかった場合には、当該ユーザからの認証要求を解除するまでの間、受け付けないこと。 なお、受け付けなくなるまでの認証の回数については、警察庁が別途指示する。			

1．4 APISプログラムの機能

区　分	機能名	詳　細　内　容		配　点	根拠資料番号	備考	得　点
必須項目	APISプログラム共通機能	通信制御機能	(1) APIS(法務省)間通信制御 APIS(法務省)とファイル転送、法務省ヒット情報(APIS)のデータ通信を制御できること。	基礎点			
			(2) 専用端末A等通信制御 専用端末A等と登録、照会、回答及びヒット通知のデータ通信を制御すること。				
			(3) データ交換装置間通信制御 データ交換装置とデータ通信を制御できること。				
			(4) 冗長構成を用いた業務継続 装置異常時に、冗長構成の機器である業務サーバ、Webサーバを利用して業務の継続ができること。				
		入力検査	(1) 専用端末A等から入力された登録及び照会のデータについて検査をすること。 なお、検査の詳細については、警察庁が別途指示する。				
			(2) 検査結果を専用端末A等に表示すること。				
		件数カウント	(1) 登録、照会、回答、ヒット通知等の件数をカウントすること。				
			(2) カウントした件数を専用端末A等に表示できること。 なお、表示の詳細については警察庁が別途指示する。				
		処理状況表示	登録及び照会の処理状況を専用端末A等に表示すること。 なお、表示の詳細については警察庁が別途指示する。				
		処理確認	処理が完了した場合、その結果を専用端末A等に表示できること。 なお、表示の詳細については警察庁が別途指示する。				
		取扱いデータの種類	データは、日本語のほか、中国語(簡体字、繁体字)及び韓国語(ハングル文字)を扱うことができること。				
	ホスト情報登録	取得	ホスト情報(APIS)を、抽出サーバからデータ交換装置を介して、FTPにより取得できること。 なお、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。				

		登録	(1) ホスト情報(APIS)を警察システムの文字コードに変換(大文字及び小文字の置き換え、全角文字及び半角文字の置き換え等を含む。)すること。 なお、警察システムの文字コードの詳細と変換内容については、警察庁が別途指示する。			
			(2) 警察BLDB(APIS)に登録されているホスト情報(APIS)を削除、又は差分を抽出し、新たに取得したホスト情報(APIS)又は差分データを警察BLDB(APIS)に登録すること。			
		一連番号の生成	警察BLDB(APIS)にホスト情報を登録する際には、1件単位に一連番号を生成すること。 なお、生成する一連番号の体系については警察庁が別途指示する。			
		入力データ変換	(1) 氏名の入力データについて、カナ氏名から英字氏名へデータ変換ができること。			
			(2) 入力されたホストコードを、変換テーブルを用いて必要なデータに変換できること。 なお、変換テーブル及び変換方法については警察庁が別途指示する。			
		照合用氏名の生成	ホスト情報(APIS)を警察BLDBに登録する際、警察BLファイル(APIS)ごとの照合・照会条件の設定に基づいた照合用氏名を生成し、ホスト情報(APIS)と共に警察BLDBに登録すること。 なお、生成方法の詳細については警察庁が別途指示する。			
		登録結果通知	(1) 警察BLDB(APIS)にホスト情報(APIS)が登録できた場合、登録の完了を管理端末Aに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。			
			(2) 警察BLDB(APIS)にホスト情報(APIS)が登録ができなかった場合、登録の失敗を管理端末Aに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。			
		処理時間制限	ホスト情報の登録処理が制限時間を超えた場合、管理端末Aへ通知すること。 なお、制限時間及び通知内容の詳細については、警察庁が別途指示する。			
	専用端末Aからの登録	端末登録	(1) 端末Aプログラムで作成した登録用ファイルを読込み、ファイルに保存されたデータの一覧を専用端末Aに表示すること。			
			(2) (1)で表示した一覧から、警察BLDB(APIS)に登録するデータを選択できること。			
			(3) (2)で選択したデータについて、登録先の警察BLファイル(APIS)の種別を指定し、同ファイルと照合すること。			
			(4) (3)の後に、他の警察BLファイル(APIS)と照合し、競合情報を専用端末Aに表示すること。			
			(5) (3)の結果が未登録の場合、警察BLDB(APIS)に警察BL(APIS)を登録すること。			
			(6) 警察BL(APIS)を警察BLDB(APIS)に登録する際には、1件単位に一連番号を自動で付与すること。 なお、付与する一連番号の体系については警察庁が別途指示する。			
			(7) 警察BL(APIS)の警察BLDB(APIS)への登録結果を、専用端末Aに表示すること。 なお、登録結果及び表示の詳細については、警察庁が別途指示する。			
			(8) 登録結果を保存すること。			
			(9) (8)で保存したデータを専用端末Aに表示すること。 なお表示の詳細については警察庁が別途指示する。			
			(10) 保存した登録結果は、一定期間経過後に自動で削除すること。 なお、一定期間の詳細については警察庁が別途指示する。			
		訂正・削除登録	(1) 端末Aプログラムで作成した訂正・削除用ファイルを読込み、ファイルに保存されたデータの一覧を表示すること。 なお、表示の詳細については警察庁が別途指示する。			
			(2) (1)の一覧から、警察BL(APIS)に登録するデータを1件ごと選択できること。			
			(3) (2)で選択したデータについて対象となる警察BL(APIS)を警察BLDB(APIS)から取得できること。			
			(4) (2)で選択したデータと(3)で取得したデータを、専用端末Aの画面に並列表示すること。			
			(5) (4)の後、(1)の画面に戻り、表示した一覧から、訂正・削除を実施するデータを選択できること。			
			(6) (5)で選択した警察BL(APIS)の訂正・削除の処理を実施し、その結果を専用端末Aに表示すること。 なお、処理結果の詳細については、警察庁が別途指示する。			
			(7) 訂正・削除の処理結果を、保存すること。			
			(8) (7)で保存したデータを専用端末Aに表示すること。 なお表示の詳細については別途指示する。			
			(9) 保存した訂正・削除の処理結果は、一定期間経過後に自動で削除すること。 なお、一定期間の詳細については警察庁が別途指示する。			
		照合用氏名の生成	警察BL(APIS)を警察BLDB(APIS)に登録する際、警察BLファイル(APIS)ごとの照合・照会条件設定に基づいた照合用氏名を生成し、警察BL(APIS)と共に登録すること。 なお、生成方法の詳細については警察庁が別途指示する。			
		注意喚起	警察BL(APIS)を警察BLDB(APIS)に登録する前に、専用端末Aに注意喚起を促すメッセージを表示すること。			
		定期抹消	(1) 警察BLDB(APIS)に登録されてから一定期間以上経過した警察BL(APIS)を、日単位で警察BLDB(APIS)から抹消すること。 なお、一定期間の詳細については、警察庁が別途指示する。			
			(2) 定期抹消の結果を専用端末Aに表示できること。 なお、表示の詳細については警察庁が別途指示する。			

競合情報	照合	(1) 警察BLDB(APIS)において、登録する警察BL(APIS)を登録対象以外の警察BLファイル(APIS)と照合し、競合の有無を確認すること。			
		(2) 競合の有無の確認の結果を、端末登録機能(8)の登録結果として登録すること。			
		(3) 警察BLファイルごとに、照合対象の警察BLファイル(APIS)及び競合通知先の所属を設定できること。			
	保存	(1) 照合の結果、他の警察BLファイル(APIS)に競合して登録されていた場合、競合元及び競合先に関する情報を、競合情報として保存すること。			
		(2) 保存した日から一定期間以上経過した競合情報を、日単位で自動削除すること。 なお、一定期間の詳細については、警察庁が別途指示する。			
	表示	保存した競合情報を専用端末Aに表示できること。			
	照会	表示された競合情報が他の警察BLファイル(APIS)と競合しているか照会できること。			
警察BL(APIS)照会	即時照会	(1) 警察BLDB(APIS)に照会するデータを、専用端末Aから1件単位で入力できること。			
		(2) 照会する警察BLファイルを選択して、以下のア～ウの情報を用いて警察BL(APIS)が照会できること。 なお、ア～ウの情報の詳細については警察庁が別途指示する。 ア 人定情報 イ 一連番号 ウ 登録所属			
		(3) 入力検査の結果が正常であった場合、警察BLDB(APIS)に対して照会ができること。			
		(4) 照会中に処理の中止ができること。			
		(5) 照会の処理状況が分かること。 なお、処理状況の詳細については警察庁が別途指示する。			
	照会結果表示	(1) 照会した結果を専用端末Aに表示すること。 なお、表示の詳細については警察庁が別途指示する。			
		(2) 照会した結果をファイルに出力できること。 なお、ファイル形式及びデータレイアウト等の詳細については、警察庁と別途協議すること。			
		(3) 照会結果が一定件数を超える場合は、画面表示を取りやめ、(2)の方法及び件数を分割して、照会結果を出力すること。 なお、一定件数については、警察庁と別途協議すること。			
	照会条件設定	警察BLファイル(APIS)ごとに照合・照会条件を設定し、照会できること。 なお、照合・照会条件については警察庁が別途指示する。			
警察BL(APIS)の法務省への転送	抽出	(1) 警察BLDB(APIS)から転送用の警察BL(APIS)を自動抽出すること。 なお、自動抽出方法、抽出時期、抽出ファイル、抽出項目等の自動抽出の詳細については、警察庁が別途指示する。			
		(2) (1)の転送用の警察BL(APIS)について、警察BLDB(APIS)とは別に保存すること。			
		(3) (1)の転送用の警察BL(APIS)は、一意となる一連番号を生成すること。 なお、生成する一連番号の体系については警察庁が別途指示する。			
		(4) 任意の時刻に管理端末Aを用いて手動で抽出ができること。			
		(5) 管理端末Aから手動抽出／自動抽出／抽出停止の切替の操作ができること。			
		(6) 管理端末Aから抽出する警察BLファイル(APIS)の選択ができること。			
		(7) 管理端末Aから抽出する警察BLファイル(APIS)ごとに、抽出する項目の情報が選択できること。 なお、抽出する項目については、警察庁が別途指示する。			
		(8) 抽出結果を、管理端末Aで確認できること。 なお、抽出結果の確認方法については、警察庁が別途指示する。			
		(9) APIS(法務省)への転送済みの警察BL(APIS)ついて、警察BLDBからの再抽出を、管理端末Aから実施できること。			
	定期抹消	警察BLDB(APIS)から警察BL(APIS)の定期抹消を行う場合、当該警察BL(APIS)の削除をAPIS(法務省)に依頼するデータを作成し、送信すること。 なお、作成するデータの詳細については、警察庁が別途指示する。			
	検査	警察BLDB(APIS)から転送用の警察BL(APIS)を抽出する際には、抽出する項目を検査すること。 なお、検査の詳細については、別途指示する。			
	転送用データへの変換	検査が完了した転送用の警察BL(APIS)は、APIS(法務省)に転送する転送用データに変換すること。 なお、転送用データの詳細については、警察庁が別途指示する。			
	転送	(1) 変換した転送用データは、1件ごと又は複数件を一括してAPIS(法務省)に自動転送すること。			
		(2) APIS(法務省)と転送結果の送達確認ができること。 なお、送達確認の詳細については、警察庁が別途指示する。			
		(3) 任意の時刻に管理端末Aを用いて手動で転送を実行できること。			
		(4) 管理端末Aから手動転送／自動転送／転送停止の切替の操作ができること。			
		(5) 転送結果を、管理端末Aで確認できること。 なお、転送結果の確認方法については、警察庁が別途指示する。			
		(6) 管理端末Aから転送に関する履歴を管理できること。			

	表示	(1) 転送用データの転送処理過程、転送結果を、管理端末Aで確認できること。 なお、転送処理過程及び転送結果の詳細については、警察庁が別途指示する。			
		(2) (1)の確認中に異常が発見された場合には、管理端末A及び警報装置に通知すること。 なお、異常の詳細については、警察庁が別途指示する。			
		(3) 定期抹消の結果を管理端末Aに表示できること。 なお、表示の詳細については警察庁が別途指示する。			
		(4) 転送に関する履歴を管理端末Aに表示できること。 なお、表示の詳細については警察庁が別途指示する。			
照合	受信	APIS(法務省)から法務省ヒット情報(APIS)を自動取得できること。 なお、自動取得の詳細については、警察庁が別途指示する。			
	検査	(1) 取得した法務省ヒット情報(APIS)について、検査すること。 なお、検査の詳細については、警察庁が別途指示する。			
		(2) (1)の検査の結果、取得した法務省ヒット情報(APIS)に異常がある場合、取得した法務省ヒット情報(APIS)を破棄すると共に、管理端末Aに通知をすること。 なお、通知の詳細については、警察庁が別途指示する。			
	照合条件による照合	(1) 検査の結果が正常であった法務省ヒット情報(APIS)については、ヒット情報DB(APIS)と自動照合し、合致する情報の有無を確認すること。			
		(2) (1)の照合の結果、合致する場合、法務省ヒット情報(APIS)を破棄すること。			
		(3) (1)の照合の結果、合致しない場合、照合・照会条件の設定に従い、警察BLDB(APIS)と照合すること。 なお、照合・照会条件については警察庁が別途指示する。			
		(4) (3)の照合の結果から、ヒット通知の必要性の有無を判定すること。 なお、判定の条件については、警察庁が別途指示する。			
		(5) (4)の判定の結果を、APIS(法務省)に照合理由依頼通知として通知すること。 なお、通知の詳細については、警察庁が別途指示する。			
ヒット通知	ヒット通知	(1) ヒット通知が必要となったヒット情報(APIS)については、ヒット情報の条件設定に従ってヒット通知先に通知すること。ヒット通知先は、法務省ヒット情報(APIS)に該当する警察BL(APIS)において個別に設定された通知先、又は警察BLファイルごとに設定された共通の通知先が設定される。			
		(2) メインメニュー画面からヒット通知先及びヒット通知の代行先を、専用端末Aで確認できること。			
	警報装置制御	(1) ヒット情報(APIS)の内容に応じ、警報装置を鳴動させること。 なお、警報装置の鳴動の詳細については、警察庁が別途指示する。			
		(2) 警報装置の鳴動を確認すること。			
		(3) (2)の後、警報装置の鳴動が停止されたことを確認すること。			
		(4) (2)及び(3)の確認の結果を管理端末Aに通知すること。 なお、確認内容の詳細については、警察庁が別途指示する。			
	照合結果等表示	(1) 法務省ヒット情報(APIS)の受信結果及び照合結果について、管理端末Aに表示できること。 なお、表示内容の詳細については、警察庁が別途指示する。			
		(2) 照合機能及びヒット通知機能の処理中に異常が見られた場合、管理端末A及び警報装置に通知すること。 なお、通知内容の詳細については、警察庁が別途指示する。			
ヒット情報(APIS)	登録	ヒット情報(APIS)及び法務省ヒット情報(APIS)をヒット情報DB(APIS)へ登録すること。			
	ヒット通知一覧	ヒット情報DB(APIS)から、ヒット通知一覧を抽出すること。 なお、ヒット通知一覧の詳細については、警察庁が別途指示する。			
	表示	(1) 業務プログラムにログインすることなく、専用端末Aでヒット通知一覧を確認できること。また、ヒット通知一覧からヒット情報(APIS)の詳細を確認する場合は、ユーザ認証を行うこと。 なお、確認方法については、警察庁が別途指示する。			
		(2) 業務プログラムにログインにしている場合、専用端末Aで、ヒット通知一覧及びヒット情報(APIS)の詳細を表示できること。 なお、表示方法及び表示内容の詳細については、警察庁が別途指示する。			
	定期抹消	(1) 一定期間以上経過したヒット情報DB(APIS)に登録されたヒット情報(APIS)及び法務省ヒット情報(APIS)を日単位に自動抹消すること。 なお、一定期間の詳細については、警察庁が別途指示する。			
		(2) 定期抹消した結果を、専用端末Aに表示できること			
ヒット情報(APIS)照会	即時照会	(1) ヒット情報DB(APIS)に照会するデータを、専用端末Aから1件単位で入力できること。入力するデータの詳細については警察庁が別途指示する。			
		(2) 入力検査の結果が正常であった場合、ヒット情報DB(APIS)に対して照会ができること。			
		(3) 照会中に処理の中止ができること。			
		(4) 照会の処理状況を専用端末Aに表示できること。 なお、表示の詳細については警察庁が別途指示する。			
		(5) 照会した結果を専用端末Aに表示できること。 なお、表示の詳細については警察庁の別途指示する。			
	日本語、中国語及び韓国語変換	(1) 日本語から中国語(簡体字、繁体字)、ピンイン及び統一読みへの変換ができること。			
		(2) 中国語(簡体字)から日本語、中国語(繁体字)、ピンイン及び統一読みへの変換ができること。			
		(3) 中国語(繁体字)から日本語、中国語(簡体字)、 ピンイン及び統一読みへの変換ができること。			

		(4) 日本語から韓国語(ハングル文字)及び韓国語(ローマ字)への変換ができること。			
		(5) 韓国語(ハングル文字)から日本語及び韓国語(ローマ字)への変換ができること。			
		(6) 統一読みへの変換テーブルについては、警察庁が官給する、3.3.56「中国語漢字読み方辞典」の電子データをもとに作成すること。			
		(7) (6)以外の変換テーブルについては、警察庁が保有する変換テーブルをデータで提供する。			
ヒット通知の代行	設定	(1) 代行元の専用端末Aで代行設定することにより、代行先の専用端末Aにおいてもヒット情報(APIS)が表示されること。			
		(2) 代行元の専用端末Aで代行設定することにより、代行先の警報装置の鳴動等を制御できること。			
		(3) 代行設定及び解除は、手動で設定する方法及び期間、時間及び日付を設定することにより自動で設定する方法で行えること。また、期間にあっては複数設定可能であること。			
		(4) 代行設定は、全ての所属のユーザーが設定できること。			
		(5) 管理端末Aから、全ての専用端末Aの代行設定期間を一括して設定できること。また、専用端末Aは、一括して設定した代行設定期間を変更できること。			
	代行表示	(1) 代行元の専用端末A ア 代行中であることを専用端末Aに表示できること。			
		イ 代行設定を行った所属を、専用端末Aで確認できること。			
		ウ ログインすることなく代行状態を確認できること。			
		(2) 代行先の専用端末A ア 代行された旨を専用端末Aに表示できること。			
		イ 代行元の専用端末Aの代行状態に関する所属の情報を専用端末Aに表示できること。			
		ウ 代行設定が解除された場合、解除された旨を専用端末Aに表示できること。			
	代行先の警報装置制御	代行元の警報装置と同等の制御ができること。			
他システムへの照会	準即時照会	(1) 他システムに照会するデータを、専用端末Aから1件単位で入力できること。			
		(2) 入力検査の結果が正常であった場合、他システムに対して照会に必要なデータが送信できること。			
		(3) 他システムに対して、一定間隔で受信要求を行い、回答データを受信できること。 なお、受信要求の間隔については、警察庁が別途指示する。			
		(4) 一定期間以上経過して回答がない場合、照会データを削除できること。 なお、一定期間の詳細については、警察庁が別途指示する。			
		(5) 管理端末Aから手動により他システムへの照会機能の開始・停止の切替の操作ができること。			
		(6) 回答データの結果を一定期間保存できること。 なお、一定期間の詳細については、警察庁が別途指示する。			
		(7) (1)～(5)項に係る他システムの詳細については、警察庁が別途指示する。			
	再送	他システムに対して照会に必要なデータを送信してから受信要求間隔として設定した時間までに回答データを受信できない場合、照会に必要なデータを自動で再送すること。 なお、他システムの詳細については、警察庁が別途指示する。			
	検査	他システムから受信した回答データの各項目について、検査すること。 なお、他システムの詳細及び検査の内容の詳細については、警察庁が別途指示する。			
	照会結果表示	(1) 準即時照会 照会した結果を専用端末Aに表示できること。 なお、表示の詳細については警察庁が別途指示する。			
		(2) 準即時照会の照会過程、処理結果を、管理端末Aで確認できること。 なお、照会過程及び処理結果の詳細については、警察庁が別途指示する。			
		(3) (2)の確認中に異常が発見された場合には、管理端末A及び警報装置に通知すること。 なお、異常の詳細については、警察庁が別途指示する。			
	注意喚起	他システムに照会するデータを送付する前に、専用端末Aに注意喚起を促すメッセージを表示すること。			
コード出力	コード出力	国名等のコード変換テーブルをファイルに出力できること。 なお、出力するコードの種類及びファイルの詳細については、警察庁と別途協議すること。			
試験	試験環境	(1) 運用環境と同等の機能が確認できる試験環境を構築できること。 なお、試験環境は運用環境で使用するものとは別に作成し、運用環境に影響を与えないこと。			
		(2) APIS(警察)の単独での試験環境とは別に、APIS(法務省)と接続する試験環境を構築できること。			
		(3) 試験環境は専用端末A等と接続ができること。また、試験環境と専用端末A等との接続は、個別に設定ができること。			
		(4) 試験中は専用端末A等に試験中であることを明示すること。			
	試験機能	作成した試験データで、APISプログラムの機能が確認できること。			

メンテナンス	ログ出力設定	専用端末A等ごと及びアクセス権ごとに、出力できるログの種類並びに出力内容を設定できること。 なお、ログの種類及び出力内容の詳細については警察庁が別途指示する。			
	試験環境設定	(1) 専用端末A等ごとに試験環境に接続する設定ができること。			
		(2) 試験環境へ接続している専用端末A等の情報が一覧で表示できること。 なお、一覧表示の詳細については警察庁が別途指示する。			
		(3) 試験データ(登録、即時・準即時照会、ヒット通知)の作成及び編集ができること。			
		(4) 試験データの情報が一覧で表示できること。 なお、一覧表示の詳細については警察庁が別途指示する。			
		(5) APIS(警察)の単独試験と、APIS(法務省)との接続試験の切替ができること。 なお、切替方法については、警察庁と協議すること。			
	変換テーブル等メンテナンス	(1) 抽出サーバから取得したホスト情報(APIS)及び専用端末Aから入力した警察BL(APIS)について、変換テーブルを用いて、氏名変換及びコード変換等の必要なデータ変換ができること。 なお、変換テーブルは警察庁からデータを提供することとし、変換が必要なデータ、変換方法及び変換のタイミング等の詳細については、警察庁が別途指示する。			
		(2) データ変換テーブルの更新ができること。			
		(3) コードの登録・削除を行った場合、コードの表示・非表示等の挙動及び内部処理について、警察庁と別途協議すること。			
	件数制限設定	(1) 各照会の結果ごとに回答するデータの件数及び一括登録可能な件数等の制限ができること。			
		(2) 件数制限を超えた場合、専用端末A等にメッセージ表示ができること。			
		(3) 件数制限が変更できること。			
	処理時間設定	(1) 登録、照会等に要する処理時間の制限ができること。			
		(2) 制限時間を超えた場合、処理を中断し、専用端末A等にメッセージ表示ができること。			
		(3) 制限時間が変更できること。			
	受信要求間隔設定	(1) 各機能の受信要求間隔を設定できること。			
		(2) 受信要求間隔を変更できること。			
	定期抹消設定	定期抹消において、警察BLファイル(APIS)ごとに抹消結果の通知先を設定できること。			
	競合情報設定	競合情報の照合において、照合対象の警察BLファイル(APIS)及び通知先を設定できること。			
	ヒット情報の条件設定	(1) 警察BLファイル(APIS)ごとに、措置、通知先の所属及び通知内容の設定ができること。 なお、設定内容については、警察庁が別途指示する。			
		(2) 前項で設定したヒット情報の条件について、条件の追加、訂正及び削除ができること。			
		(3) 通知先の代行設定状態により、ヒット通知を制御する設定ができること。			
	照合・照会条件の設定	照合・照会条件の設定及び変更が警察BLファイル(APIS)ごとにできること。 なお、照合・照会条件の詳細については、警察庁が別途指示する。			
	ホスト情報等登録結果	(1) 警察BLDB(APIS)にホスト情報等の登録結果を管理端末Aに表示できること。			
		(2) 警察BLDB(APIS)にホスト情報等の登録において異常があった場合、その詳細を管理端末Aに表示できること。			
	法務省への警察BL(APIS)転送設定	(1) 警察BLファイル(APIS)ごとに、転送の設定ができること。 なお、設定内容の詳細については警察庁が別途指示する。			
		(2) 転送結果の確認ができること。			
		(3) 警察BLファイル(APIS)ごとに、登録、更新及び削除を選択し、警察BL(APIS)が転送できること。			
	法務省間機能の開始・停止設定	(1) APIS(法務省)間の機能である警察BL(APIS)転送及び照合結果通知の開始・停止を設定できること。			
		(2) APIS(法務省)と業務サーバの接続状況を管理端末Aから確認できること。 なお、接続状況の確認方法については警察庁が別途指示する。			
	抽出サーバ間機能の開始・停止設定	(1) 抽出サーバ間の機能であるホスト情報(APIS)の取得の開始・停止を設定できること。			
		(2) 取得機能の状態を管理端末Aから確認できること。 なお、確認方法については警察庁が別途指示する。			
ユーザ情報	認証	(1) 専用端末A等に接続した生体認証装置による生体情報の取得及び送信等を制御できること。			
		(2) ユーザの認証情報を、端末Aプログラムから受信できること。			
		(3) 受信したユーザの認証情報から、ユーザの照合ができること。			
		(4) 認証が認められた場合、対応するユーザ情報をWebサーバから取得できること。			
		(5) 取得したユーザ情報から、APISプログラムにログインできること。			
		(6) 取得したユーザ情報から、業務ごとにアクセス権の制御を行うこと。			

			(7) 認証が認められなかった場合、再度認証を行い、一定回数認証が認められなかった場合には、当該ユーザからの認証要求を解除するまでの間、受け付けないこと。 なお、受け付けなくなるまでの認証の回数については、警察庁が別途指示する。				

1．5 BICSプログラムの機能

区　分	機能名	詳　細　内　容		配　点	根拠資料番号	備考	得　点
必須項目	BICSプログラム共通機能	通信制御機能	(1) BICS(法務省)間通信制御 BICS(法務省)とファイル転送、法務省ヒット情報(BICS)のデータ通信を制御できること。	基礎点			
			(2) 専用端末A等通信制御 専用端末A等と照会、回答、ヒット通知のデータ通信を制御すること。				
			(3) データ交換装置間通信制御 データ交換装置とデータ通信を制御できること。				
			(4) 冗長構成を用いた業務継続 装置異常時に、冗長構成の機器である業務サーバ、Webサーバを利用して業務の継続ができること。				
		入力検査	(1) 専用端末A等から入力された照会のデータについて、検査、項目の属性等を検査すること。 なお、検査の詳細については、警察庁が別途指示する。				
			(2) 検査結果を専用端末A等に表示すること。 なお、表示の詳細については警察庁が別途指示する。				
		件数カウント	(1) 登録、照会、回答、ヒット通知の件数をカウントすること。				
			(2) カウントした件数を専用端末A等に表示できること。 なお、表示の詳細については警察庁が別途指示する。				
		処理確認	処理が完了した場合、その結果を専用端末A等に表示できること。 なお、表示の詳細については警察庁が別途指示する。				
	転送データ(BICS)登録	取得	転送データ(BICS)を、抽出サーバからデータ交換装置を介して、FTPにより取得すること。 なお、自動転送にFTP以外のプロトコルを用いることも可とするが、警察庁の承認を得ること。				
		登録	(1) 抽出サーバから取得した転送データ(BICS)を警察BLDB(BICS)に登録すること。				
			(2) 転送データ(BICS)が警察BLDB(BICS)に既に登録済みの場合、警察BLDB(BICS)から登録済みの転送データ(BICS)を削除し、新たに取得した転送データ(BICS)を警察BLDB(BICS)に登録すること。				
		登録結果通知	(1) 警察BLDB(BICS)に転送データ(BICS)が登録できた場合、登録の完了、登録件数、処理日時等を管理端末Aに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。				
			(2) 警察BLDB(BICS)に転送データ(BICS)が登録できなかった場合、登録の失敗、処理日時等を管理端末Aに通知すること。 なお、通知する内容の詳細については、警察庁が別途指示する。				
		処理時間制限	転送データ(BICS)の登録処理が制限時間を超えた場合、管理端末Aへ通知すること。 なお、制限時間及び通知内容の詳細については、警察庁が別途指示する。				
	警察BL(BICS)の転送	抽出	(1) 警察BLDB(BICS)から転送用の警察BL(BICS)を自動抽出すること。 なお、自動抽出方法、抽出時期、抽出ファイル、抽出項目等については、警察庁が別途指示する。				
			(2) 自動抽出した転送用の警察BL(BICS)について、警察BLDB(BICS)とは別に保存できること。				
			(3) 抽出した転送用の警察BL(BICS)に全体で一意となる一連番号を生成し付与すること。 なお、付与する一連番号の体系については警察庁が別途指示する。				
			(4) 任意の時刻に管理端末Aを用いて手動で抽出ができること。				
			(5) 管理端末Aから抽出する警察BLファイル(BICS)の選択ができること。				
			(6) 抽出結果の確認ができること。 なお、抽出結果の確認方法については、警察庁が別途指示する。				
		検査	警察BLDB(BICS)から転送用の警察BL(BICS)を抽出する際には、抽出する項目について、必須項目及び任意項目の検査、項目の属性等を検査すること。				
		転送用データへの変換	検査が完了した転送用の警察BL(BICS)は、BICS(法務省)に転送するデータに変換すること。 なお、転送用データの詳細については、警察庁が別途指示する。				
		転送	(1) 変換した転送用データは、BICS(法務省)に自動転送すること。				
			(2) BICS(法務省)から転送結果を受信すること。				
			(3) 任意の時刻に管理端末Aを用いて手動で転送を実行できること。				
			(4) 管理端末Aから手動転送／自動転送／転送停止の切替の操作ができること。				
			(5) 転送結果を、管理端末Aで確認ができること。 なお、転送結果の確認方法については、警察庁が別途指示する。				
			(6) 管理端末Aから転送に関する履歴が管理できること。				
		表示	(1) 転送処理過程、転送結果等については、転送日時、件数等の内容を管理端末Aに表示できること。また、警察BL(BICS)の転送処理が正常に終了しなかった場合、前記のほか、異常であった旨の通知、警報装置の鳴動等ができること。 なお、転送日時、件数等の詳細については、警察庁が別途指示する。				
			(2) 転送に関する履歴が管理端末Aに表示できること。				
	ヒット受信	ヒットの受信	(1) BICS(法務省)から、ヒット通知にかかる存否確認を自動受信できること。 なお、存否確認の詳細については警察庁が別途指示する。				
			(2) 存否確認の内容から、警察BLDB(BICS)を検索すること。				

		(3) (2)の検索の結果を、BICS(法務省)に通報依頼理由として通知すること。 なお、通知の詳細については、警察庁が別途指示する。			
		(4) (3)の通知の後に送信される法務省ヒット情報(BICS)を、自動受信できること。 なお、法務省ヒット情報(BICS)の詳細については警察庁が別途指示する。			
ヒット通知	ヒット通知	(1) 法務省ヒット情報(BICS)の受信後、ヒット通知先設定に従いヒット通知を行うこと。			
		(2) メインメニュー画面からヒット通知先及びヒット通知の代行先を、専用端末Aで表示できること。			
	照合結果表示	(1) 法務省ヒット情報(BICS)を管理端末Aに表示できること。 なお表示内容の詳細については、警察庁が別途指示する。			
		(2) ヒット通知機能の処理中に異常が見られた場合、管理端末A及び警報装置に通知すること。 なお、通知内容の詳細については、警察庁が別途指示する。			
	警報装置制御	(1) ヒット通知先設定に従って、警報装置を鳴動させること。 なお、警報装置の鳴動の詳細については、警察庁が別途指示する。			
		(2) 警報装置の鳴動を確認すること。			
		(3) (2)ののち、警報装置の鳴動が停止されたことを確認すること。			
		(4) (2)及び(3)の確認の結果を管理端末に通知すること。 なお、確認内容及び通知の詳細については、警察庁が別途指示する。			
ヒット通知一覧	登録	法務省ヒット情報(BICS)及び該当する警察BL(BICS)をデータベースに保存すること。			
	ヒット通知一覧	法務省ヒット情報(BICS)及び該当する警察BL(BICS)をデータベースから、ヒット通知一覧を抽出すること。 なお、ヒット通知一覧の詳細については、警察庁が別途指示する。			
	画像変換	専用端末Aで法務省ヒット情報(BICS)及び該当する警察BL(BICS)の画像を、専用端末Aで表示できる画像形式に変換すること。 なお、画像形式の詳細については、警察庁が別途指示する。			
	表示	(1) 業務プログラムにログインすることなく、専用端末Aで、ヒット通知一覧を確認できること。また、ヒット通知一覧から法務省ヒット情報(BICS)の詳細を確認する場合は、ユーザ認証を行うこと。 なお、確認内容については、警察庁が別途指示する。			
		(2) 業務プログラムにログインにしている場合、専用端末Aで、ヒット通知一覧及び法務省ヒット情報(BICS)の詳細を表示できること。 なお、表示方法及び表示内容の詳細については、警察庁が別途指示する。			
ヒット通知の代行	設定	(1) 代行元の専用端末Aで代行設定することにより、代行先の専用端末Aにおいてもヒット情報(BICS)が表示されること。			
		(2) 代行元の専用端末Aで代行設定することにより、代行先の警報装置の鳴動等を制御できること。			
		(3) 代行設定及び解除は、手動で設定する方法及び期間、時間及び日付を設定することにより自動で設定する方法で行えること。また、期間にあっては複数設定可能であること。			
		(4) 代行設定は、全ての所属のユーザーが設定できること。			
		(5) 管理端末Aから、全ての専用端末Aの代行設定期間を一括して設定できること。また、専用端末Aは、一括して設定した代行設定期間を変更できること。			
	表示	(1) 代行元の専用端末A ア 代行されている旨を専用端末Aに表示できること。			
		イ 代行設定を行った所属について、専用端末Aで確認ができること。			
		ウ ログインすることなく代行状態を確認できること。			
		(2) 代行先の専用端末A ア 代行された旨を専用端末Aに表示できること。			
		イ 代行元の専用端末Aの代行状態に関する所属の情報を専用端末Aに表示できること。			
		ウ 代行設定が解除された場合、解除された旨を専用端末Aに表示できること。			
	代行先の警報装置制御	代行元の警報装置と同等の制御ができること。			
他システムへの照会	データ取込み	(1) スキャナ又は電磁的記録媒体から、照会画像及び添付画像の読込みができること。 なお、画像の解像度及び形式等については、警察庁が別途指示する。			
		(2) 読込んだ照会画像の切り出し処理等ができること。 なお、切り出し位置、寸法等については、警察庁が別途指示する。			
		(3) 読込んだ照会画像を、警察庁が別途指示する画像形式及び専用端末Aで表示できる画像形式に変換できること。 なお、専用端末Aに表示する画像形式については、警察庁と別途協議すること。			
		(4) 変換した照会画像を、専用端末Aに表示できること。			
	照会1	(1) 他システムに照会するデータを専用端末Aから1件単位で入力できること。 なお、入力データの詳細については警察庁が別途指示する。			
		(2) 入力検査の結果が正常であった場合、他システムに対して照会画像及び照会に必要なデータが送信できること。			
		(3) 他システムからの回答データの有無を一定間隔で確認し、回答データが受信できること。			
		(4) 回答データの結果を一定期間保存できること。 なお、一定期間の詳細については、警察庁が別途指示する。			
		(5) 他システムの詳細については、警察庁が別途指示する。			

		照会2	(1) 他システムに照会するデータを専用端末Aから1件単位で入力できること。 なお、入力データの詳細については警察庁が別途指示する。			
			(2) 入力検査の結果が正常であった場合、他システムに対して照会画像、添付画像及び照会に必要なデータが送信できること。			
			(3) 他システムからの回答データの有無を一定間隔で確認し、回答データが受信できること。			
			(4) 回答データの結果を一定期間保存できること。 なお、一定期間の詳細については、警察庁が別途指示する。			
			(5) 他システムの詳細については、警察庁が別途指示する。			
		画像変換	専用端末Aで照会結果を表示する際には、警察庁が別途指示する画像形式を、専用端末Aで表示できる画像形式に変換すること。 なお、画像形式の詳細については、警察庁が別途指示する。			
		表示	(1) 照会した結果を専用端末Aに表示できること。 なお、表示する画像形式については、警察庁と別途協議すること。			
			(2) 照会2の結果については、照会結果の印刷ができること。 なお、表示する画像形式については、警察庁と別途協議すること。			
			(3) 照会過程、処理結果等について、処理日時、端末名、処理件数等の内容を管理端末Aに表示できること。また、処理が正常に終了しなかった場合、異常であった旨の通知、警報装置の鳴動等ができること。 なお、処理日時、処理件数等の詳細については、警察庁が別途指示する。			
		注意喚起	他システムに照会するデータを送付する前に、専用端末Aに注意喚起を促すメッセージを表示すること。			
		アクセスログ参照	アクセス権に応じてアクセスログの参照ができること。			
	試験	試験環境	(1) 運用環境と同等の機能が確認できる試験環境を構築できること。 なお、試験環境は運用環境で使用するものとは別に作成し、運用環境に影響を与えないこと。			
			(2) BICS(警察)の単独での試験環境とは別に、BICS(法務省)と接続した試験環境を構築できること。			
			(3) 試験環境は専用端末A等と接続ができること。また、試験接続は、専用端末A等ごとに設定ができること。			
			(4) 試験中は専用端末A等に試験中であることを明示すること。			
		試験機能	作成した試験データで、BICSプログラムの機能が確認できること。			
	メンテナンス	ログ出力設定	専用端末A等ごと及びアクセス権ごとに、出力できるログの種類及び出力内容を設定できること。 なお、ログの種類及び出力内容の詳細については警察庁が別途指示する。			
		試験環境設定	(1) 専用端末A等ごとに試験環境に接続する設定ができること。			
			(2) 試験環境へ接続している専用端末A等の情報が一覧で表示できること。 なお、一覧表示の詳細については警察庁が別途指示する。			
			(3) 試験データ(照会、ヒット通知)の作成及び編集ができること。			
			(4) 試験データの情報が一覧で表示できること。 なお、一覧表示の詳細については警察庁が別途指示する。			
			(5) 運用環境と試験環境でコードの同期がとれること。			
		警察BL(BICS)等内容確認	(1) 抽出サーバ(BICS)で登録された転送用の警察BL(BICS)から取得した転送データ(BICS)の内容を、日時又は期間を指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。			
			(2) 専用端末A等から照会入力された転送用の照会データの内容を、日時又は期間を指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。			
			(3) 警察BLDB(BICS)に登録されている警察BL(BICS)の内容を、一連番号又は全てを指定して表示できること。 なお、表示の詳細については警察庁が別途指示する。			
		変換テーブル等メンテナンス	(1) コード変換テーブルの更新ができること。 なお、変換テーブルは警察庁からデータを提供することとし、変換が必要なデータ、変換方法、変換タイミング等の詳細については、警察庁が別途指示する。			
			(2) 運用環境と試験環境でコードの同期がとれること。			
		ヒット通知先設定	警察BLファイル(BICS)ごとのヒット通知先の所属を変更できること。			
		法務省間機能の開始・停止設定	(1) BICS(法務省)間の機能である警察BL(BICS)転送及び法務省ヒット通知の開始・停止を設定できること。			
			(2) BICS(法務省)と業務サーバの接続状況を管理端末Aから確認できること。 なお、接続状況の確認方法については警察庁が別途指示する。			
		抽出サーバ間機能の開始・停止設定	(1) 抽出サーバ間の機能である登録データ(BICS)の取得の開始・停止を設定できること。			
			(2) 取得機能の状態を管理端末Aから確認できること。 なお、状態の確認方法については警察庁が別途指示する。			
	ユーザ情報	認証	(1) 専用端末A等に接続した生体認証装置による生体情報の取得及び送信等を制御できること。			
			(2) ユーザの認証情報を、端末Aプログラムから受信できること。			
			(3) 受信したユーザの認証情報から、ユーザの照合ができること。			
			(4) 認証が認められた場合、対応するユーザ情報をWebｻｰﾊﾞから取得できること。			
			(5) 取得したユーザ情報から、BICSプログラムにログインできること。			
			(6) 取得したユーザ情報から、業務ごとにアクセス権の制御を行うこと。			

			(7) 認証が認められなかった場合、再度認証を行い、一定回数認証が認められなかった場合には、当該ユーザからの認証要求を解除するまでの間、受け付けないこと。 なお、受け付けなくなるまでの認証の回数については、警察庁が別途指示する。				

1．6 端末Aプログラムの機能

区　分	機能名		詳　細　内　容	配　点	根拠資料番号	備考	得　点
必須項目	共通	通信制御機能	APISプログラムの制御下で、登録、照会、回答、ヒット通知のデータ通信を行うこと。	基礎点			
	ユーザ管理	管理	(1)　ユーザ情報の登録、訂正及び削除を一件単位で入力できること。				
			(2)　ユーザ情報の登録は、電磁的記録媒体により一括して入力できること。				
			(3)　ユーザの新規登録、訂正登録及び削除登録では、ユーザ情報と生体情報を関連付けて登録ができること。				
			(4)　登録した結果を表示できること。 なお、表示の詳細は警察庁が別途指示する。				
		認証	(1)　生体情報又はその他の情報が取得できること。 なお、その他の情報については警察庁と協議すること。				
			(2)　取得したユーザの生体情報含む認証要求を、Webサーバに送信できること。				
			(3)　(2)の認証要求に応じたアクセス権を取得できること。				
			(4)　(3)で取得したアクセス権に対応した業務プログラムにログインできること。				
	Web機能	Web機能	(1)　専用端末A等のOSで安定稼働すること。				
			(2)　業務用プログラムに対応すること。				
			(3)　SSL／TLSにより暗号化し、HTTPSによるデータの送受信が行えること。				
	APIS登録ツール	端末登録用ファイルの作成	(1)　警察BLファイル（APIS）の種別ごとに入力ができること。 なお、警察BLファイル（APIS）の種別については、警察庁が別途指示する。				
			(2)　表形式（エクセル形式）のインタフェースにより、項目ごとに警察BL（APIS）の入力ができること。				
			(3)　エクセル形式及びCSV形式のファイルを読込み、(2)のインタフェースにより、警察BL（APIS）の訂正・削除ができること。				
			(4)　入力検査を行い、検査結果を表示すること。 なお、検査の詳細については、警察庁が別途指示する。				
			(5)　(4)の入力検査が正常であった場合、入力した警察BL（APIS）をAPISプログラムが取り扱う登録用ファイルに変換すること。 なお、変換方法については警察庁と協議して決定すること。				
			(6)　複数件の警察BL（APIS）を、一つの登録用ファイルに一括して変換できること。 なお、変換方法については警察庁と協議して決定すること。				
		訂正・削除用ファイルの作成	(1)　警察BLファイル（APIS）の種別ごとに入力ができること。 なお、警察BLファイル（APIS）の種別については、警察庁が別途指示する。				
			(2)　表形式（エクセル形式）のインタフェースにより、項目ごとに警察BL（APIS）の入力ができること。				
			(3)　エクセル形式及びCSV形式のファイルを読込み、項目ごとに警察BL（APIS）の訂正・削除ができること。				
			(4)　警察BL（APIS）照会で出力した照会結果ファイルの読込み、その内容の表示、編集ができること。				
			(5)　訂正の場合、項目ごとに訂正ができること。				
			(6)　削除の場合、一連番号を指定して削除できること。				
			(7)　入力検査を行い、検査結果を表示すること。 なお、検査の詳細については、警察庁が別途指示する。				
			(8)　(7)の入力検査が正常であった場合、訂正及び削除した警察BL（APIS）をAPISプログラムが取り扱う訂正削除用ファイルに変換すること。 なお、変換方法については警察庁と協議して決定すること。				
			(9)　複数件の警察BL（APIS）を一つの訂正削除用ファイルに一括して変換できること。 なお、変換方法については警察庁と協議して決定すること。				
		ヒット情報の条件の反映	警察BL（APIS）のヒット通知の通知先について、1件単位及び複数件を一括で反映できること。 なお、ヒット通知先の情報については警察庁が別途指示する。				
		日本語、中国語及び韓国語変換	(1)　日本語から中国語（簡体字、繁体字）、ピンイン及び統一読みへの変換ができること。				
			(2)　中国語（簡体字）から日本語、中国語（繁体字）、ピンイン及び統一読みへの変換ができること。				
			(3)　中国語（繁体字）から日本語、中国語（簡体字）、 ピンイン及び統一読みへの変換ができること。				
			(4)　日本語から韓国語（ハングル文字）及び韓国語（ローマ字）への変換ができること。				
			(5)　韓国語（ハングル文字）から日本語及び韓国語（ローマ字）への変換ができること。				
			(6)　統一読みへの変換テーブルについては、警察庁が官給する、3.3.56「中国語漢字読み方辞典」の電子データをもとに作成すること。				
			(7)　(6)以外の変換テーブルについては、警察庁が保有する変換テーブルをデータで提供する。				
			(8)　当該機能の一部又は全部を、端末装置以外の機器に持たせる場合には、実現方法について警察庁と協議の上、他のプログラムと相互に影響を与えないこと。				
		コード更新	APISプログラムから出力したファイルを取り込むことにより、国名等のコードを更新できること。 なお、更新を行うコードの種類については、警察庁が別途指示する。				

	セキュリティ	安全対策	(1)　業務起動中、一定時間操作されなかった場合、スクリーンロックができること。また、キーボード操作により、任意にスクリーンロックができること。				
			(2)　スクリーンロックの設定及び解除の時間が設定できること。				
			(3)　スクリーンロック起動中、認証又はキーボード操作により、スクリーンロックが解除できること。				
			(4)　スクリーンロック起動中において、指定した時間内に認証による解除がされない場合又はキーボード操作によりスクリーンロックを解除した場合は、業務を強制終了し、使用中のデータを、専用端末A等の一時使用領域から自動で消去すること。また、強制終了を行う時間は1分単位で設定できること。				
		データ消去	業務で使用したデータは、業務用プログラムを終了した時、専用端末A等の一時使用領域から自動で消去すること。				

1．7　端末Bプログラムの機能

区　分	機能名	詳　細　内　容		配　点	根拠資料番号	備考	得　点
必須項目	共通	通信制御機能	抽出プログラムの制御下で、登録のデータ通信を行うこと。	基礎点			
			(1)　入力された生体情報を、アクセス権管理システムに登録されたユーザ情報と関連付けて登録ができること。				
			(2)　登録した結果が表示できること。 なお、表示の詳細は警察庁が別途指示する。				
		認証	(1)　生体情報又はその他の情報等、ユーザの認証情報が取得できること。 なお、その他の情報については警察庁と協議すること。				
			(2)　取得したユーザの認証情報含む認証要求を、抽出サーバに送信できること。				
			(3)　(2)の認証要求に応じたアクセス権を取得できること。				
			(4)　(3)で取得したアクセス権に対応した業務プログラムにログインできること。				
	Web機能	Web機能	(1)　専用端末B等のOSで安定稼働すること。				
			(2)　業務用プログラムに対応すること。				
			(3)　SSL／TLSにより暗号化し、HTTPSによるデータの送受信が行えること。				
	セキュリティ	安全対策	(1)　業務起動中、一定時間操作されなかった場合、スクリーンロックすること。また、キーボード操作により、任意にスクリーンロックができること。				
			(2)　スクリーンロックの設定及び解除の時間が設定できること。				
			(3)　スクリーンロック起動中、認証又はキーボード操作により、スクリーンロックが解除できること。				
			(4)　スクリーンロック起動中において、指定した時間内に認証による解除がされない場合又はキーボード操作によりスクリーンロックを解除した場合は、業務を強制終了し、使用中のデータを、専用端末B等の一時使用領域から自動で消去すること。また、強制終了を行う時間は1分単位で設定できること。				
		データ消去	業務で使用したデータは、業務用プログラムを終了した時、専用端末B等の一時使用領域から自動で消去すること。				

最高点			総合得点		
	基礎点	1,560		基礎点	
	加点	1,560		加点	
	合計点	3,120		合計点	

加点項目

区分・機能名等				評価基準(必須)	加点基準	配点	提案内容	根拠資料番号	得点
加点項目	サーバ用プログラムの機能	アクセス権	・種類 ・範囲	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		入出力制御	・印刷出力制御 ・ファイル出力制御 ・電磁的記録媒体入出力制御	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		業務管理等系	・作成 ・参照 ・定期抹消	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		運用連絡通報	通報通知	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		接続状態	・表示 ・接続	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		アクセスログ	・生成 ・参照 ・定期抹消	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		システムログ	・生成 ・参照 ・定期抹消	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	抽出プログラムの機能	抽出プログラム共通機能	・通信制御機能 ・入力検査 ・件数カウント ・処理状況表示 ・処理確認	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		ホスト情報登録	・取得 ・抽出(APIS) ・抽出(BICS) ・登録(BICS) ・登録結果通知 ・処理時間制限	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		指紋画像情報登録	・抽出 ・取得 ・登録 ・一連番号の生成 ・登録結果通知 ・処理時間制限	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		専用端末Bからの登録	・登録画像の読込み ・登録 ・注意喚起 ・定期抹消	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		ホスト情報(APIS)及び転送データ(BICS)の転送	・転送データ(BICS)の抽出 ・定期抹消 ・転送(APIS) ・転送(BICS) ・表示	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		試験	・試験環境	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		接続	・警察庁ホストシステムとの接続 ・警察庁指掌紋システムとの接続	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		メンテナンス	・ログ出力設定 ・試験環境設定 ・登録データ(BICS)等内容確認 ・変換テーブル等メンテナンス ・定期抹消設定 ・ホスト情報等登録結果 ・警察庁ホストシステム間機能の開始・停止設定 ・警察庁指掌紋システム間機能の開始・停止設定 ・業務サーバ間機能の開始・停止機能	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		ユーザ情報	・認証	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	APISプログラムの機能	APISプログラム共通機能	・通信制御機能 ・入力検査 ・件数カウント ・処理状況表示 ・処理確認 ・取扱いデータの種類	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		ホスト情報登録	・取得 ・登録 ・一連番号の生成 ・入力データ変換 ・照合用氏名の生成 ・登録結果通知 ・処理時間制限	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		専用端末Aからの登録	・端末登録 ・訂正・削除登録 ・照合用氏名の生成 ・注意喚起 ・定期抹消	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			

加点項目

区分・機能名等			評価基準（必須）	加点基準	配点	提案内容	根拠資料番号	得点
	競合情報	・照合 ・保存 ・表示 ・照会	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	警察BL(APIS)照会	・即時照会 ・照会結果表示 ・照会条件設定	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	警察BL(APIS)の法務省への転送	・抽出 ・定期抹消 ・検査 ・転送用データへの変換 ・転送 ・表示	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	照合	・受信 ・検査 ・照合条件による照合	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	ヒット通知	・ヒット通知 ・警報装置制御 ・照合結果等表示	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	ヒット情報（APIS）	・登録 ・ヒット通知一覧 ・表示 ・定期抹消	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	ヒット情報（APIS）照会	・即時照会 ・日本語、中国語及び韓国語変換	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	ヒット通知の代行	・設定 ・代行表示 ・代行先の警報装置制御	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	他システムへの照会	・準即時照会 ・再送 ・検査 ・照会結果表示 ・注意喚起	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	コード出力	・コード出力	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	試験	・試験環境 ・試験機能	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	メンテナンス	・ログ出力設定 ・試験環境設定 ・変換テーブル等メンテナンス ・件数制限設定 ・処理時間設定 ・受信要求間隔設定 ・定期抹消設定 ・競合情報設定 ・ヒット情報の条件設定 ・照合・照会条件の設定 ・ホスト情報等登録結果 ・法務省への警察BL（APIS）転送設定 ・法務省間機能の開始・停止設定 ・抽出サーバ間機能の開始・停止設定	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	ユーザ情報	・認証	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
BICSプログラムの機能	BICSプログラム共通機能	・通信制御機能 ・入力検査 ・件数カウント ・処理確認	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	転送データ（BICS）登録	・取得 ・登録 ・登録結果通知 ・処理時間制限	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	警察BL(BICS)の転送	・抽出 ・検査 ・転送用データへの変換 ・転送 ・表示	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	ヒット受信	ヒット受信	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	ヒット通知	・ヒット通知 ・照合結果表示 ・警報装置制御	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
				② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	ヒット通知一覧	・登録 ・ヒット通知一覧 ・画像変換 ・表示	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			

加点項目

区分・機能名等				評価基準（必須）	加点基準	配点	提案内容	根拠資料番号	得点
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		ヒット通知の代行	・設定 ・表示 ・代行先の警報装置制御	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		他システムへの照会	・データ取込み ・照会1 ・照会2 ・画像変換 ・表示 ・注意喚起 ・アクセスログ参照	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		試験	・試験環境 ・試験機能	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		メンテナンス	・ログ出力設定 ・試験環境設定 ・警察BL(BICS)等内容確認 ・変換テーブル等メンテナンス ・ヒット通知設定 ・法務省間機能の開始・停止設定 ・抽出サーバ間機能の開始・停止設定	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		ユーザ情報	・認証	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	端末Aプログラムの機能	共通	通信制御機能	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		ユーザ管理	・管理 ・認証	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		Web機能	Web機能	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		APIS登録ツール	・端末登録用ファイルの作成 ・訂正・削除用ファイルの作成 ・ヒット情報の条件の反映 ・日本語、中国語及び韓国語変換 ・コード更新	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		セキュリティ	・安全対策 ・データ消去	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
	端末Bプログラムの機能	共通	通信制御機能	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		ユーザ管理	・管理 ・認証	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		Web機能	Web機能	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			
		セキュリティ	・安全対策 ・データ消去	当該機能について、具体的かつ明確に提案されている。	① 処理フローや処理イメージがあり、具体的な提案がされている。	20			
					② 複数社から提案がある場合は、他社に比べて最も優れた具体的な提案がある。	10			

（注） 加点基準は次のとおりとする。
1．加点については、入力補助機能の付与や文字・背景の配色の工夫等、システムの操作性・利便性のほか、保守性等を向上させる効果が認められる提案を対象とする。
2．②の加点は、①を満たす社が複数ある場合に、その中の社に対して行う。
3．②の加点は、最大１社のみとする。

最高点			総合得点		
	基礎点	1,560		基礎点	
	加点	1,560		加点	
	合計点	3,120		合計点	

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24年度	平成25年度	平成26年度	平成27年度	平成28年度	平成29年度
	人件費	常勤職員	ー	ー	ー	ー	ー	ー
		非常勤職員	ー	ー	ー	ー	ー	ー
	物件費		ー	ー	ー	ー	ー	ー
	請負費等	プログラム開発	65,972	26,429	ー	ー	ー	ー
		プログラム保守	ー	ー	ー	ー	ー	ー
		システム設置工事	ー	7,559	ー	ー	ー	ー
		システム賃貸借	ー	21,235	262,098	262,098	262,098	240,256
計(a)			65,972	55,222	262,098	262,098	262,098	240,256
参考値(b)	減価償却費		ー	ー	ー	ー	ー	ー
	退職給付費用		ー	ー	ー	ー	ー	ー
	間接部門費		ー	ー	ー	ー	ー	ー
(a)＋(b)			65,972	55,222	262,098	262,098	262,098	240,256

（注記事項）
支払い金額は、一般競争入札の落札額である。
システム賃貸借の経費については、平成26年３月から平成30年２月の分となっており、平成30年３月から平成31年２月の分については契約を延長する。
なお、プログラム瑕疵対応の経費は、プログラム開発の経費に含まれている。

2 従来の実施に要した人員

	平成24年度	平成25年度	平成26年度	平成27年度	平成28年度	平成29年度
常勤職員	ー	ー	ー	ー	ー	ー
非常勤職員	ー	ー	ー	ー	ー	ー

入札対象である事業の全部を外部委託し実施しているため、記載事項無し。

受託者における業務従事者

	平成24年度	平成25年度	平成26年度	平成27年度	平成28年度	平成29年度
プログラム開発	4,484（人日）		ー	ー	ー	ー
プログラム瑕疵対応	ー	3（人）	3（人）	3（人）	3（人）	ー
システム担当（統括責任者、システム担当責任者、プロジェクトリーダ、サブリーダ及びハードウェア担当責任者）	-	5（人）	5（人）	5（人）	5（人）	-

（注記事項）
プログラム開発は、EVMの積算による投入実績値（AC）累計（人日）の値を入れている。
なお、プログラム開発にの契約から納入期限まで1年8か月程度であった。

システム担当は、障害時の対応、定期点検、パッケージソフトウェアのバージョンアップ等を実施している。
障害の対応件数：4のとおり
定期点検の実施数：サーバ類に関しては年2回の定期点検日を定め、機器毎に年1回の実施としている
パッケージソフトウェアのバージョンアップ：必要の都度

プログラム瑕疵対応は、現行請負者がプログラム瑕疵対応担当者（専属ではない）として確保している人数を記載している。
なお、プログラム瑕疵対応は、発見されたプログラムの瑕疵に関する修正を実施している。
瑕疵対応件数：4のとおり

3 従来の実施に要した施設及び設備

【施設】
警察庁が指示した東京都23区内の場所
【設備】
電気設備、机、椅子

4 従来の実施における目的の達成の程度

保守フェーズにおけるサービスレベル合意書は以下のとおりである。

サービスレベル管理項目	管理指標	合意内容及び保証値
回答に要する時間	警察庁執務時間内の問合せは、当日を1営業日とする。	技術的な問合せは5営業日以内の回答とする。期限内に回答ができない場合は別途回答日を提示する。また、必要に応じて中間回答を実施する。
問題解決に要する時間	問題ごとに警察庁と受託者において協議の上、問題解決日を決定する。	問題解決日までに解決する。
保守要領の遵守	仕様書に従い保守を行う。	仕様書「12　保守要件定義」に従って保守を行いその実施状況を報告書として提出する。障害発生時等、警察庁から報告を求められた場合は、速やかに報告書を提出する。
運用時間帯	本システムの運用時間。	24時間運用とする。
障害報告時間	警察庁執務時間内に障害連絡を受けた場合、その当日を1営業日とする。	5営業日以内までに報告する。期限までに障害原因や最終対処方法が特定できない場合は、別途報告日を提示する。また、必要に応じて中間報告を実施する。業務に影響がある障害の場合又は警察庁から議事録作成を要望があった場合は速やかに報告する。なお、障害報告に際し警察庁から議事録作成を要請された場合は、契約責任者が承認欄に押印の上5営業日以内までに議事録を提出する。
障害受付・連絡窓口対応時間帯	連絡を受け付ける時間。	障害連絡窓口は24時間対応とする。技術的な質問等に対応できる連絡窓口は警察庁執務時間内の対応とする。
技術的な質問等の問合せ件数	対応時間内における問合せ件数の制限。	対応時間帯については問合せ件数を無制限とする。
保守対応時間帯	障害対応を行う時間。	24時間対応とする。
保守要員到着時間	警察庁又は情報通信部から障害連絡窓口に保守要員の派遣要請があってから到着するまでの許容時間。	3時間以内のできる限り早期に技術者を派遣する。
	警察庁又は情報通信部から障害連絡窓口に警察署等への保守要員の派遣要請があってから到着するまでの許容時間。	6時間以内のできる限り早期に技術者を派遣する。
保守報告	月の保守報告の回数。	月1回、定例保守報告資料を提出する。
セキュリティパッチ更新頻度	OS等のセキュリティホールを修正するパッチを適用する頻度。	セキュリティパッチ等が必要な場合は、速やかに警察庁に連絡し、その指示に従い作業を行う。
ウイルスチェックポリシー更新頻度	―	ウイルスチェックは、設定した時刻に自動及び任意の時刻に手動でウイルスの検索・検知・駆除を行う。

なお、障害対応件数は以下のとおりである。

障害対応件数		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
平成25年度	警察庁	―	―	―	―	―	―	―	―	―	―	―	10	10
	都道府県警察	―	―	―	―	―	―	―	―	―	―	―	0	0
平成26年度	警察庁	4	6	3	1	2	1	1	2	1	1	1	0	23
	都道府県警察	0	1	1	0	0	2	0	1	0	1	1	0	7
平成27年度	警察庁	0	4	1	2	3	3	4	2	2	2	0	2	25
	都道府県警察	0	1	0	0	0	3	0	0	1	0	0	2	7
平成28年度	警察庁	9	2	1	―	―	―	―	―	―	―	―	―	12
	都道府県警察	0	1	1	―	―	―	―	―	―	―	―	―	2

（注記事項）
サービスレベル合意書において記されている内容（障害報告に要する時間、回答に要する時間及び技術者駆けつけ時間を含む）は、遵守されていた。
障害復旧目標時間については、従来設定していない。

瑕疵対応件数（発生年月基準）		4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	計
平成25年度	プログラム	―	―	―	―	―	―	―	―	―	―	―	0	0
平成26年度	プログラム	1	2	0	1	0	1	0	0	1	0	0	0	6
平成27年度	プログラム	0	0	1	0	0	0	0	0	1	0	1	0	3
平成28年度	プログラム	0	0	0	―	―	―	―	―	―	―	―	―	0

（注記事項）
プログラムの障害（瑕疵担保）に関しては、仕様書、契約書に記載されている事項について遵守されていた。
技術者駆けつけ時間については、従来設定及び測定していない。
障害報告に要する時間については、従来設定及び測定していない。
回答に要する時間については、従来設定及び測定していない。

5 従来の実施方法等

従来の実施方法（業務フロー図等）

5.1 障害対応
5.2 技術的な質問窓口対応
5.3 HDD交換
5.4 パッチ適用
5.5 バッテリ交換
5.6 警察庁指掌紋システム、法務省システムの更改に伴う本システムの設定変更
5.7 定期点検
別紙1のとおり
（警察庁内の体制）

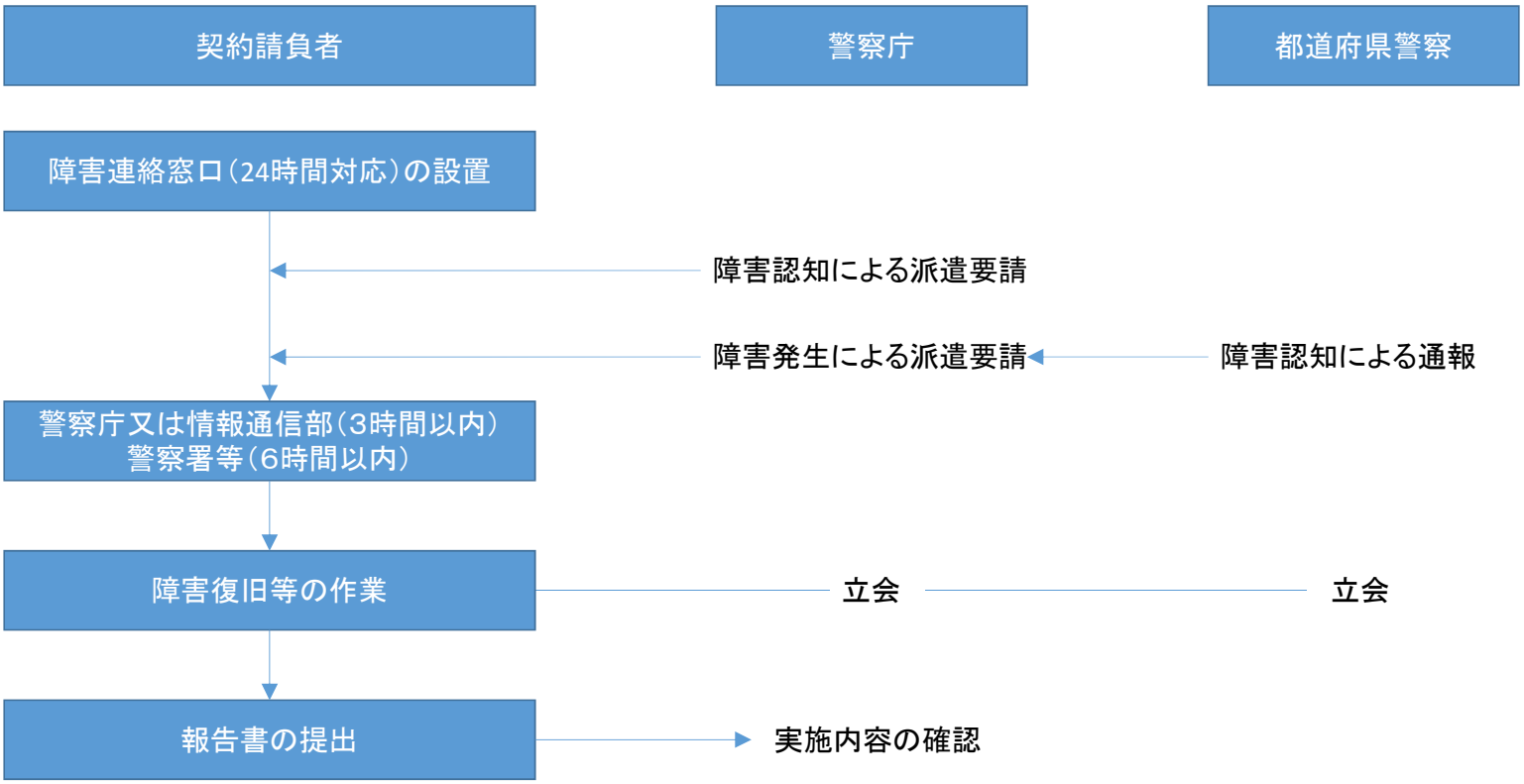
5.8 警察庁の体制
別紙1のとおり

	開示する資料は別紙2のとおり

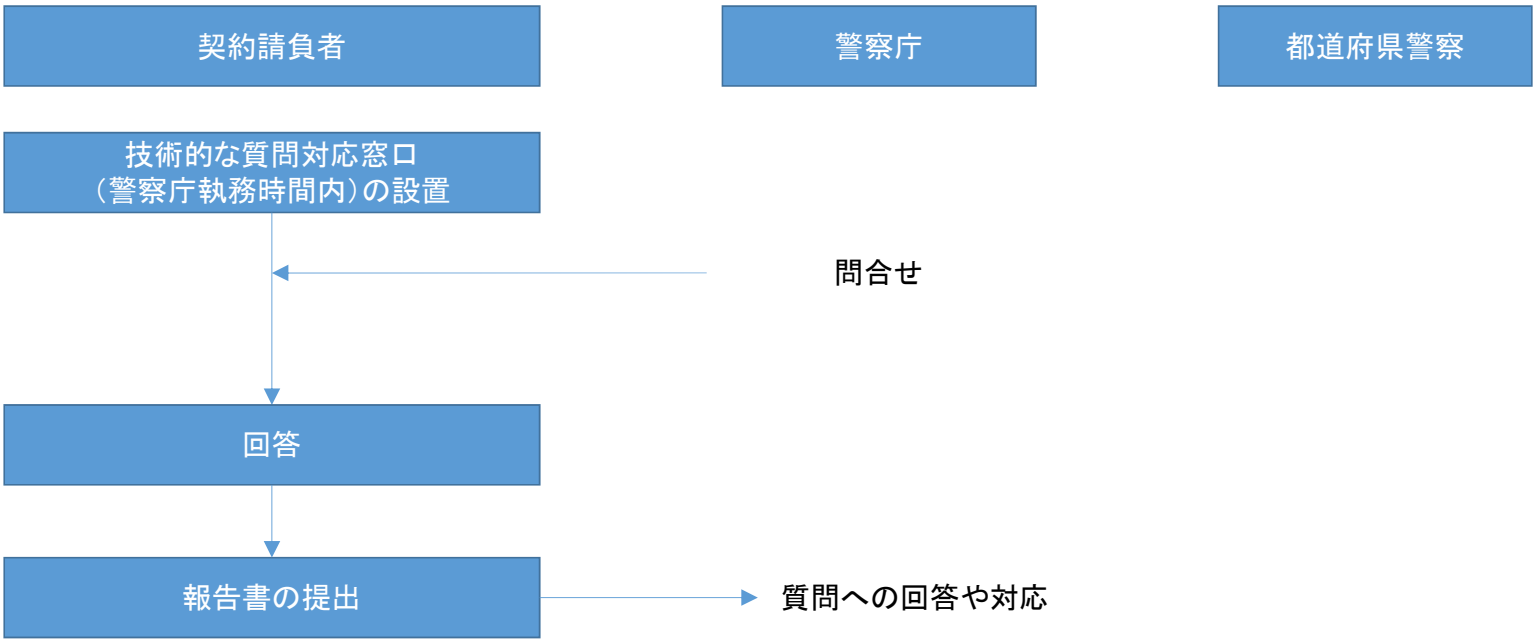
5　従来の実施方法

APISBICSの保守の業務フロー

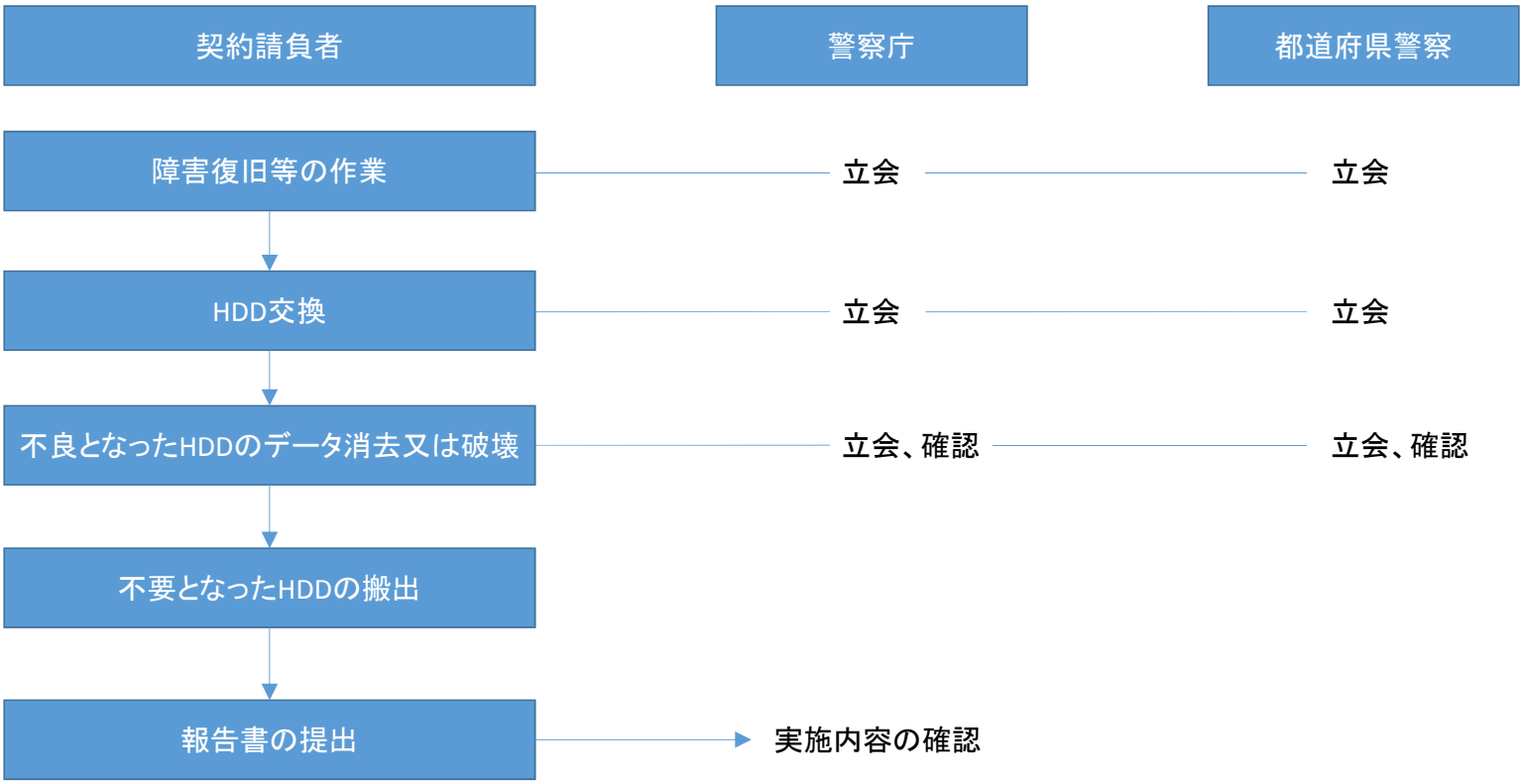
1　障害対応



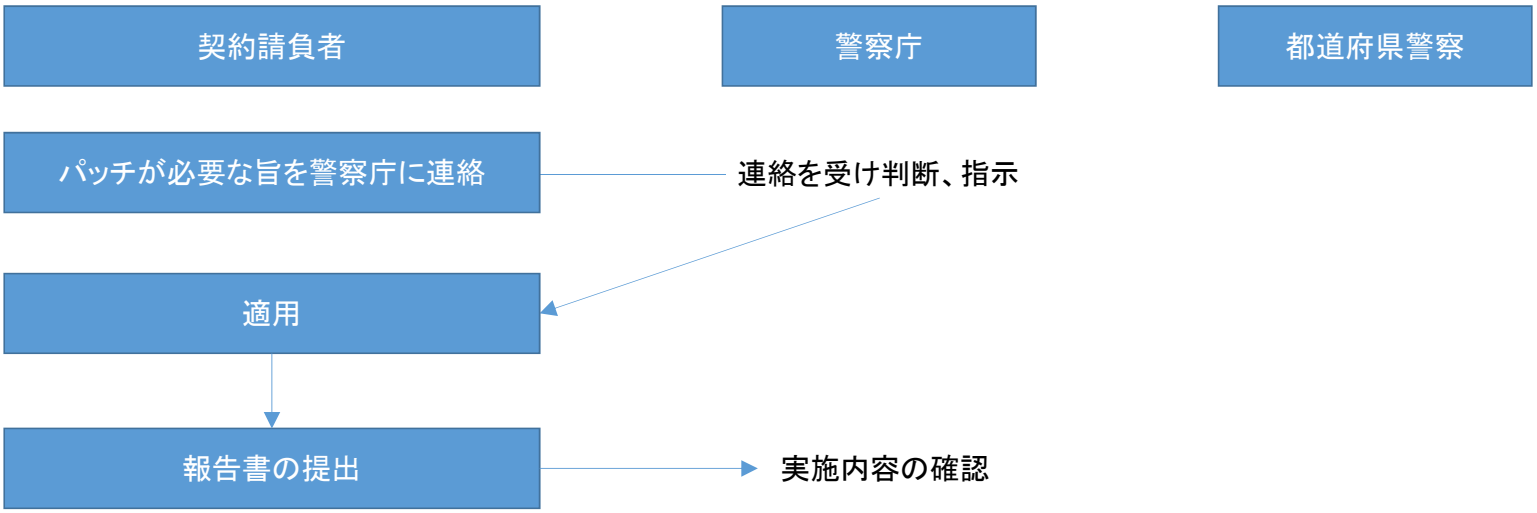
2　技術的な質問対応窓口



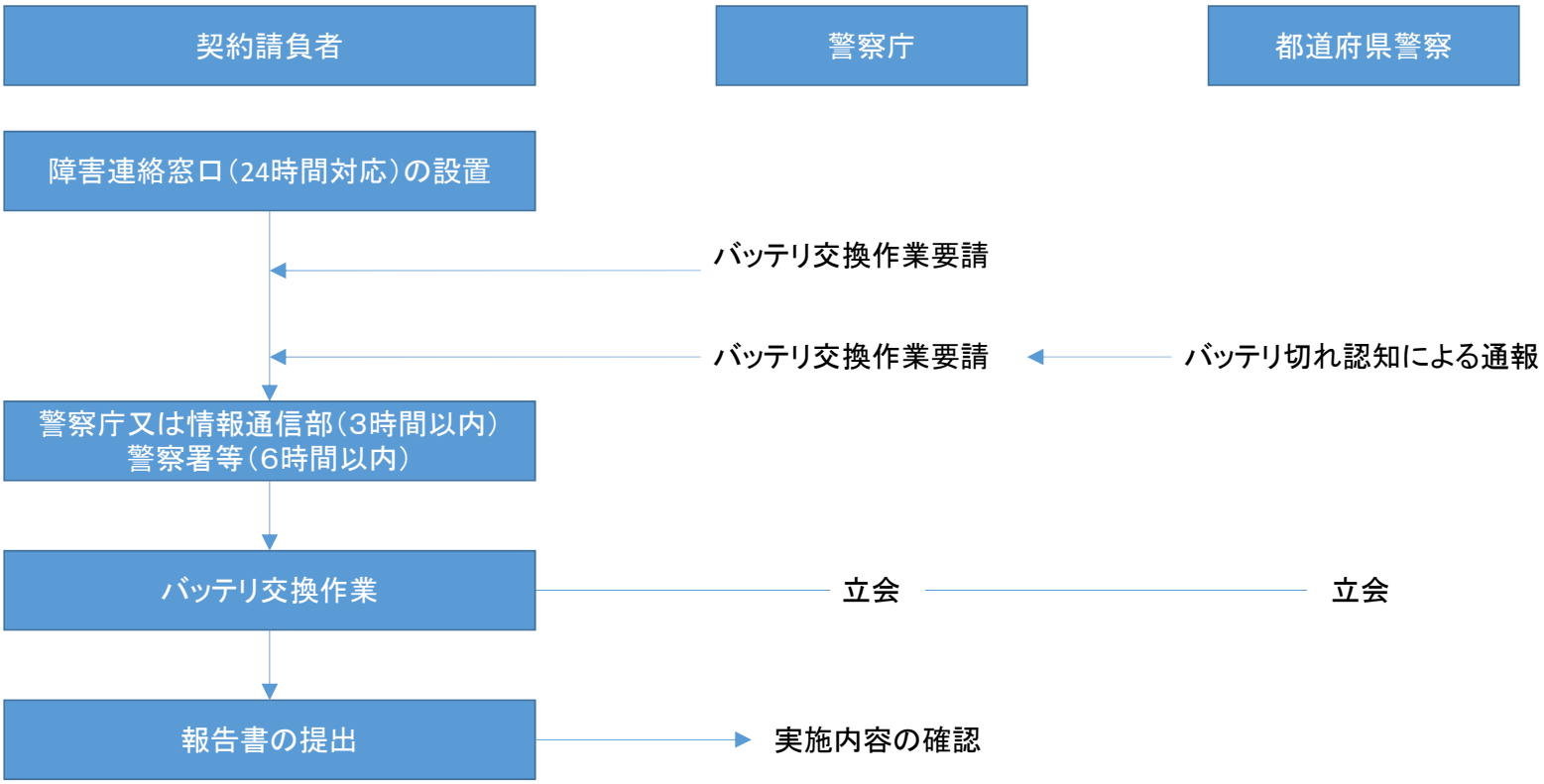
3　HDD交換



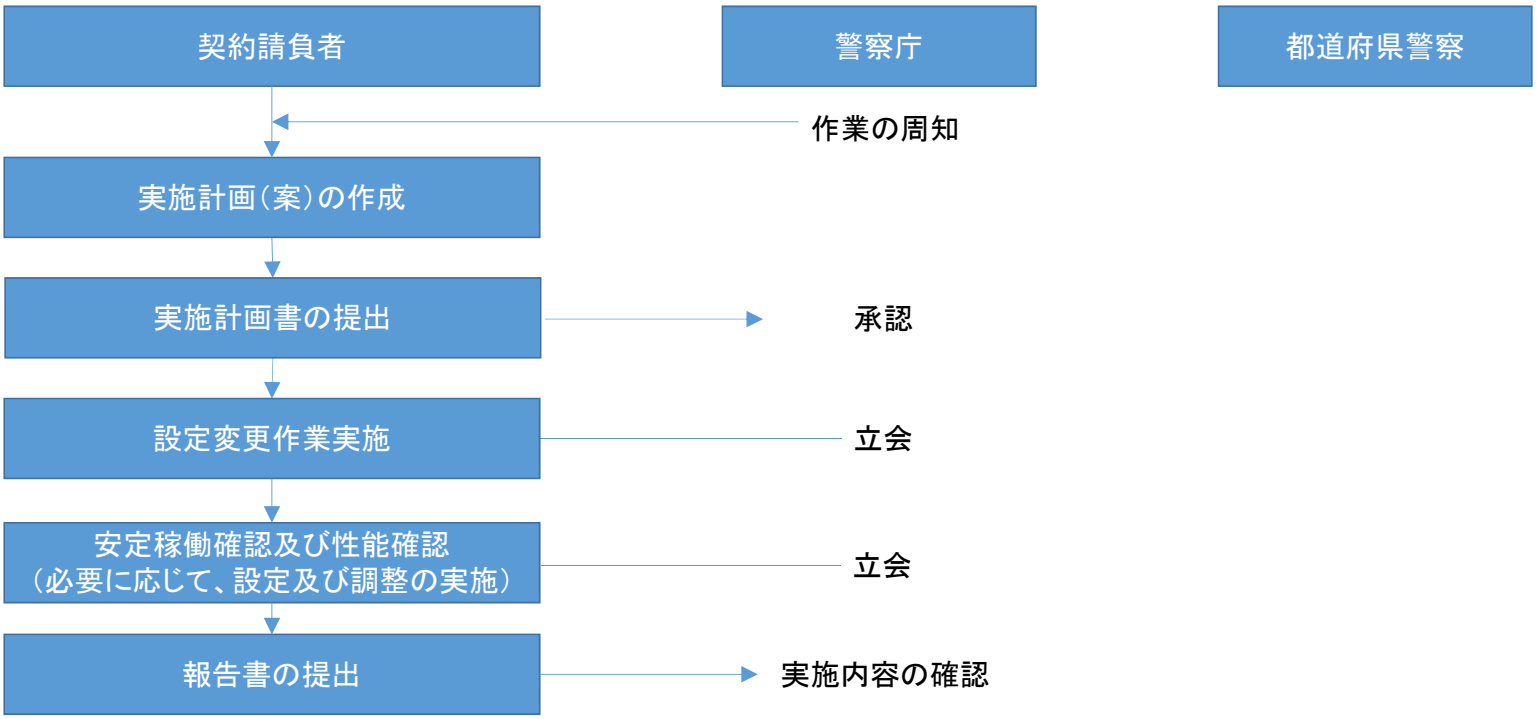
4　パッチ適用



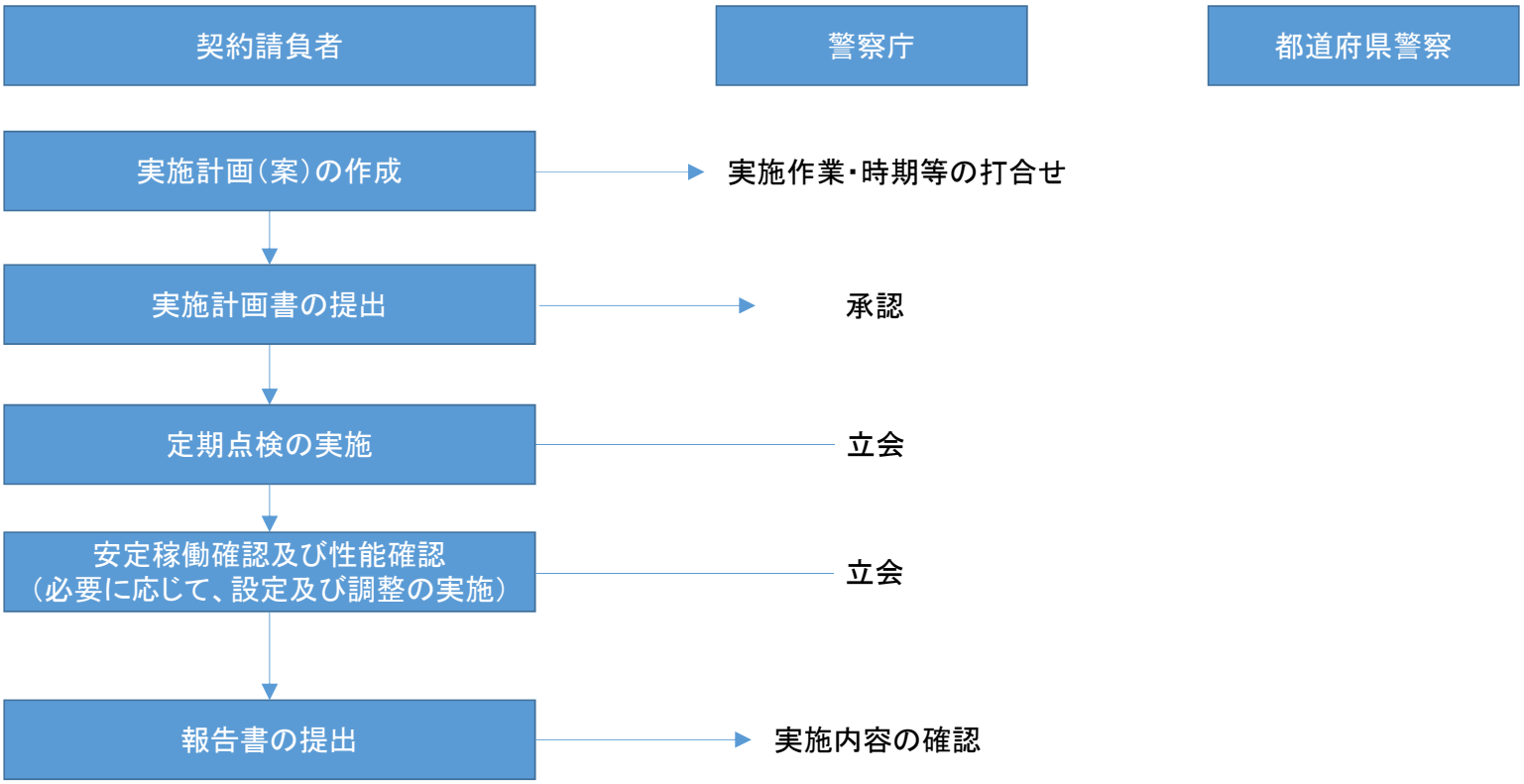
5　バッテリ交換



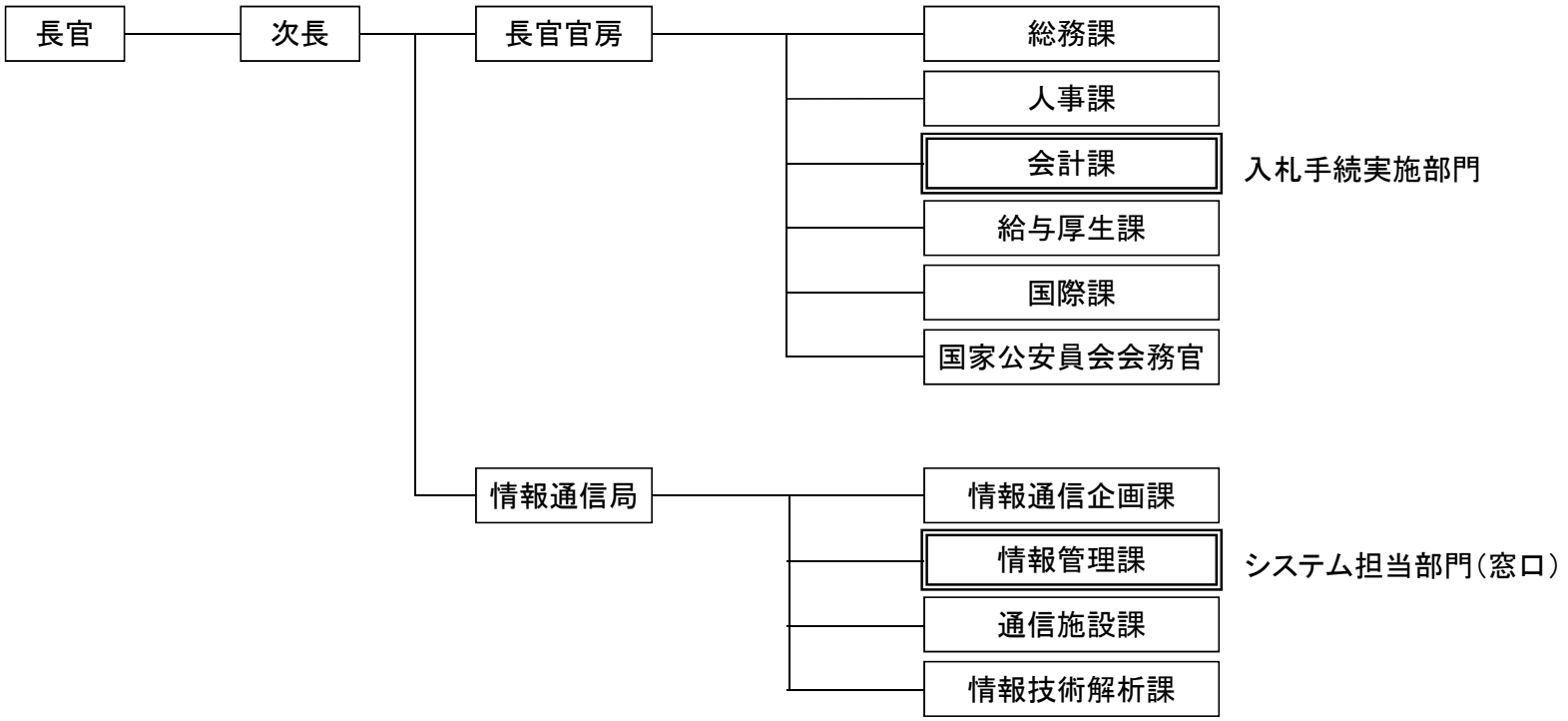
6　指掌紋システム、法務省システムの更改に伴う設定変更、確認等



7　定期点検



8　警察庁の体制


長官
次長
長官官房
総務課
人事課
会計課
入札手続実施部門
給与厚生課
国際課
国家公安員会会務官
情報通信局
情報通信企画課
情報管理課
システム担当部門(窓口)
通信施設課
情報技術解析課

開示する資料

1. 詳細な情報に関する資料
   プログラム設計書、プログラム仕様書、プログラムリスト、プログラム操作説明書、端末操作説明書、システム仕様書、システムの性能及び利用状況

2. 関連仕様書
   現行のアクセス権管理システム仕様書及び現行の指掌紋自動識別システム用照合部仕様書

3. 別添1及び別添4の別途指示
   （1） 事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書 別途指示事項

通番	業務機能	区分	項目	機能
1	警察BLファイル（APIS）	3.3用語の定義		
2	警察BLファイル（BICS）	3.3用語の定義		
3	指紋画像情報	3.3用語の定義		
4	ホスト情報（BICS）	3.3用語の定義		
5	ホスト情報	3.3用語の定義		
6	ホスト情報（APIS）	3.3用語の定義		
7	表－3 サーバ用プログラムの共通機能	アクセス権	種類	アクセス権設定の詳細
8			範囲	制御する機能
9		印刷出力制御	印刷出力制御	印刷物の様式
10		業務管理統計	作成	統計表の詳細
11		運用連絡通報	通報通知	警報装置の制御の詳細
12		接続状態	表示	接続状態表示の詳細
13		アクセスログ	生成	アクセスログの詳細
14	表－4 抽出プログラムの機能	抽出プログラムの共通機能	入力検査	検査の詳細
15			件数カウント	表示の詳細
16			処理状況表示	表示の詳細
17			処理確認	結果の表示の詳細
18		ホスト情報登録	抽出（APIS）	必要な情報の詳細
19			抽出（APIS）	保存する一定期間
20			抽出（BICS）	条件を満たすホスト情報
21			抽出（BICS）	必要な情報の詳細
22			登録結果通知	通知する内容の詳細
23			登録結果通知	通知する内容の詳細
24			処理時間制限	制限時間及び通知内容の詳細
25		指紋画像情報登録	登録	(1) 警察システムの文字コードの詳細
26				(2) 適合及び不適合の判定の詳細
27				(3)管理する一定期間
28			一連番号の生成	付与する一連番号の体系
29			登録結果通知	(1) 通知する内容の詳細
30				(2) 通知する内容の詳細
31			処理時間制限	制限時間及び通知内容の詳細
32		業務端末B等からの登録	登録画像の読込み	(1)画像の解像度及び形式等
33				(2)切り出し位置、解像度等、加工の詳細
34				(3)画像形式
35			登録	(2) 指紋画像情報の取得の詳細
36				(6) 登録結果の詳細
37			定期抹消	(1) 一定期間の詳細
38		ホスト情報（APIS）及び転送データ(BICS)の転送	抽出	(1) 自動抽出方法、抽出時刻、抽出ファイル、抽出項目等
39				(5) 抽出結果の確認方法
40			定期抹消	定期末梢の詳細
41			転送（APIS）	(3) 転送結果の確認方法
42			転送（BICS）	(3) 転送結果の確認方法
43			表示	(1)転送結果の表示の詳細
44				(2)条件及び表示方法の詳細
45				(3)通知の詳細
46		メンテナンス	ログ出力設定	ログの種類及び出力内容の詳細
47			試験環境設定	一覧表示の詳細
48			登録データ（BICS）等内容確認	(1)表示の詳細
49				(2)表示の詳細
50			変換テーブル等メンテナンス	(1)変換が必要なデータ、変換方法、変換タイミング等の詳細
51			ホスト情報等登録結果	（1）登録結果の表示の詳細
52			警察庁ホストシステム間機能の開始・停止設定	(2)接続状況の表示の詳細
53			警察庁指掌紋システム間機能の開始・停止設定	(2)接続状況の表示の詳細
54			業務サーバ間機能の開始・停止機能	(2)状態表示の詳細
55		ユーザ情報	認証	再認証の回数
56	表－5 APISプログラム機能	APISプログラム共通機能	入力検査	(1)検査の詳細
57			件数カウント	(2)表示の詳細
58			処理状況表示	結果の表示の詳細
59		ホスト情報登録	登録	(1) 警察システムの文字コードの詳細と変換内容
60			一連番号の生成	付与する一連番号の体系
61			入力データ変換	(2)変換テーブル及び変換方法
62			照合用氏名の生成	生成方法の詳細
63			登録結果通知	(1) 通知する内容の詳細
64				(2) 通知する内容の詳細
65			処理時間制限	制限時間及び通知内容の詳細
66		業務端末A等からの登録	端末登録	(6)付与する一連番号の体系
67				(7)登録結果及び表示の詳細
68				(9)表示の詳細
69				(10)一定期間の詳細
70			訂正・削除登録	(6)処理結果の詳細
71				(8)表示の詳細
72				(9)一定期間の詳細
73			照合用氏名の生成	生成方法の詳細
74			定期抹消	(1)一定期間の詳細
75				(2)表示の詳細
76		競合情報	保存	(2) 一定期間の詳細
77		警察BL(APIS)照会	即時照会	(2)ア～ウの情報の詳細
78				(5)処理状況の詳細
79			照会結果表示	(1)表示の詳細
80			照会条件設定	照合・照会条件
81		警察BL(APIS)の法務省への転送	抽出	(1) 自動抽出方法、抽出時期、抽出ファイル、抽出項目等
82				(3)付与する一連番号の体系

（1） 事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書 別途指示事項

通番	業務機能	区分	項目	機能
83				(7)抽出する項目
84				(9) 抽出結果の確認方法
85			定期抹消	作成するデータの詳細
86			検査	検査の詳細
87			転送フォーマットへの変換	フォーマット(形式)の詳細
88			転送	(2)送達確認の詳細
89				(6) 転送結果の確認方法
90			表示	(1) 転送日時、警察BLファイル(AIPS)名、件数等の詳細
91				(2)異常の詳細
92				(3)表示の詳細　(定期抹消の結果)
93				(4)表示の詳細　(転送の履歴)
94		照合	受信	自動取得の詳細
95			検査	(1)検査の詳細
96				(2)通知の詳細
97			照合条件による照合	(3) 照合結果の確認方法
98				(4)判定の条件
99				(5)通知の詳細
100		ヒット通知	警報装置制御	(1)警報装置の鳴動の詳細
101				(2)確認内容の詳細
102			照合結果等表示	(1)表示内容の詳細
103				(2)通知内容の詳細
104		ヒット情報(APIS)	ヒット通知一覧	ヒット通知一覧の詳細
105			表示	(1)表示内容の詳細
106				(2)表示方法及び表示内容の詳細
107			定期抹消	一定期間の詳細
108		ヒット情報(APIS)照会	即時照会	(1)入力するデータの詳細
109				(4)表示の詳細
110				(5)表示の詳細
111		ヒット通知の代行	代行表示	(1)ｴ表示の詳細
112				(2)ｴ表示の詳細
113		他ｼｽﾃﾑへの照会	準即時照会	(3) 受信要求の間隔
114				(4) 一定期間の詳細
115				(6) 一定期間の詳細
116				(7)他ｼｽﾃﾑの詳細
117			再送	他システムの詳細
118			検査	他システムの詳細及び検査の内容
119			照会結果表示	(2) 照会過程及び処理結果の詳細
120				(3)異常の詳細
121		メンテナンス	ログ出力設定	ログの種類及び出力内容の詳細
122			試験環境設定	(2)一覧表示の詳細
123				(3)一覧表示の詳細
124			変換テーブル等メンテナンス	(1)変換が必要なデータ、変換方法及び変換のタイミング等の詳細
125			ヒット情報の条件設定	(1)設定内容
126			照合・照会の条件設定	照合・照会条件の詳細
127			法務省への警察BL(APIS)転送設定	(1)設定内容の詳細
128			法務省間機能の開始・停止設定	(2)接続状況の表示の詳細
129			抽出サーバ間機能の開始・停止設定	(2)表示の詳細
130		ユーザ情報	認証	再認証の回数
131	表－6 BICSプログラムの機能	BICSプログラム共通機能	入力検査	(1)検査の詳細
132				(2)表示の詳細
133			件数カウント	(2)表示の詳細
134			処理確認	結果の表示の詳細
135		転送データ(BICS)登録	登録結果通知	(1) 通知する内容の詳細
136				(2) 通知する内容の詳細
137			処理時間制限	制限時間及び通知内容の詳細
138		警察BL(BICS)の転送	抽出	(1) 自動抽出方法、抽出時期、抽出ファイル、抽出項目等
139				(3)付与する一連番号の体系
140				(7) 抽出結果の確認方法
141			転送用データへの変換	転送用データの詳細
142			転送	(5) 転送結果の確認方法
143			表示	(1) 転送日時、件数等の詳細
144		ヒット受信	ヒットの受信	(1)存否確認の詳細
145				(3) 通知の詳細
146				(4)法務省ヒット情報(BICS)の詳細
147		ヒット通知	ヒット通知	(1)表示内容の詳細
148				(2)通知内容の詳細
149			警報装置制御	(1)警報装置の鳴動の詳細
150				(4)確認内容及び通知の詳細
151		ヒット通知一覧	ヒット通知一覧	ヒット通知一覧の詳細
152			画像変換	画像形式の詳細
153			表示	(1)表示内容の詳細
154				(2)表示方法及び表示内容の詳細
155		ヒット通知の代行	表示	(1)ｴ表示の詳細
156				(2)ｴ表示の詳細
157		他ｼｽﾃﾑへの照会	データ取込み	(1)画像の解像度及び形式等
158				(2)切出し位置、寸法等
159				(3)画像形式
160			照会1	(1)入力ﾃﾞｰﾀの詳細
161				(4)一定期間の詳細
162				(5)他ｼｽﾃﾑの詳細
163			照会2	(1)入力ﾃﾞｰﾀの詳細
164				(4)一定期間の詳細
165				(5)他ｼｽﾃﾑの詳細
166			画像変換	画像形式の詳細
167			表示	(3) 処理日時、処理件数等の詳細
168		メンテナンス	ログ出力設定	ログの種類及び出力内容の詳細
169			試験環境設定	(2)一覧表示の詳細
170				(4)一覧表示の詳細
171			警察BL(BICS)等内容確認	(1)表示の詳細
172				(2)表示の詳細
173				(3)表示の詳細
174			変換テーブル等メンテナンス	変換が必要なデータ、変換方法、変換タイミング等の詳細
175			法務省間機能の開始・停止設定	(2)接続状況の表示の詳細
176			抽出サーバ間機能の開始・停止設定	(2)状態表示の詳細
177		ユーザ情報	認証	再認証の回数

（1） 事前旅客情報照合業務及び外国人個人識別情報認証業務用プログラム仕様書 別途指示事項

通番	業務機能	区分	項目	機能
178	表－7 端末Aプログラムの機能	ユーザ管理	管理	表示の詳細
179		APIS登録ツール	端末登録用ファイルの作成	(1)警察BLファイル（APIS）の種別
180				(4)検査の詳細
181			訂正・削除登録	(1)警察BLファイル（APIS）の種別
182				(7)検査の詳細
183			ヒット情報の条件の反映	ヒット通知先の情報
184			コード更新	更新を行うコードの種類
185	情報システムの要件	機能・性能要件	マンマシン・インタフェース	(12) 指定桁数
186			保守性	(2) 機能の閉塞を設定・解除する範囲
187		画面要件		画面遷移、画面イメージ及び入出力仕様
188		帳票要件		帳票要件
189		情報・データ要件		情報・データ要件
190		外部インターフェース要件		外部システムとのインターフェース要件
191	情報セキュリテイ要件	権限要件		利用者ごとに付与する権限
192	情報システム稼働環境	ソフトウェア構成		IPアドレス体系
193	運用要件定義	運用施設・設備要件		システムの設置場所及びその構造、入退室の方法、空調設備、消防設備並びに電力供給設備
194	移行要件定義	移行に係る要件	移行方法及び検証方法	抽出したデータのレイアウト
195	作業の体制及び方法	進捗報告等		ODB登録用シートの詳細
196		文字コード		使用する文字コード
197		導入		提出する電磁的記録媒体の種類

（2） 事前旅客情報システム及び外国人個人識別情報認証システム仕様書 別途指示一覧

通番	業務機能	区分	項目	機能
1	表－7 抽出サーバの機能及び性能	テープライブラリ部	テープドライブ	(3)暗号アルゴリズムによる暗号化
2	表－10 バックアップサーバの機能及び性能	テープライブラリ部	テープドライブ	(3)暗号アルゴリズムによる暗号化
3	表－18 各端末の共通の機能及び性能	ソフトウェア	内蔵HDD暗号化	暗号化方式
4	表－18 各端末の共通の機能及び性能	ソフトウェア	外部記録媒体暗号化	(3)暗号化方式
5	表－19 業務端末A及び試験端末Aの機能及び性能	ソフトウェア	OS	エディション等の詳細
6	表－20 業務端末B及び試験端末Bの機能及び性能	ソフトウェア	OS	エディション等の詳細
7	表－21 管理端末Aの機能及び性能	ソフトウェア	OS	エディション等の詳細
8	表－22 管理端末Bの機能及び性能	ソフトウェア	OS	エディション等の詳細
9	表－23 コンソール端末Aの機能及び性能	ソフトウェア	OS	エディション等の詳細
10	表－21 コンソール端末Bの機能及び性能	ソフトウェア	OS	エディション等の詳細
11	規模要件			東京23区内の場所
12	規模要件			警察庁及び都道府県警察の設置する場所
13	その他	添付品		
14	ソフトウェア構成	ソフトウェア構成	ライセンス	(1)利用してもよいガバメントライセンス
15	保守要件定義	保守体制		警察庁ホストシステム、警察庁指掌紋システム、アクセス権管理システム及び法務省システムの更改の時期及び作業の詳細