「令和８年度 クラウドサービス(特殊車両通行許可等業務支援システム)提供業務　仕様書」へのご意見に対する回答

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
1	9	3.2.1（4）	Red Hat Enterprise Linux 10、Apache 2.4.62 以降、WildFly 35 以降、Java 21、Jakarta EE 10 及び Oracle Database 19c 等を使用すること。	指定された OS、ミドルウェア及びデータベース構成に対する、既存アプリケーションの互換性確認、改修及び動作保証の責任分界をご提示願います。Java 21 及び Jakarta EE 10 への対応、既存ライブラリの更新、非互換機能への対応、DB 接続方式の変更並びにアプリケーション試験で検出された不具合への対応は、アプリケーション開発・保守業者の担当範囲との理解でよいかご教示ください。	ご意見を踏まえ、各関係者の基本的な役割及び障害発生時の責任分界が明確になるよう、仕様書の記載内容を見直します。 なお、本調達において準備するものについては、原則として本調達の受注者が責任を負うものとします。また、障害等の原因が明確でない場合は、関係事業者が連携して原因調査を行い、各契約の範囲及び原因・責任の所在に基づいて費用負担を決定します。
2	15～17	4.1、4.2	受注者は、問い合わせ窓口を設置し、プラットフォーム保守・運用、障害対応等を実施するとともに、機構、アプリケーション開発・保守業者及びクラウドサービス提供事業者等と連携すること。	機構様、アプリケーション開発・保守業者、クラウドサービス提供事業者及び既存システム保守業者と受注者との作業分界・責任分界をご提示願います。特に、OS、ミドルウェア、データベース、ネットワーク、クラウドサービス及びアプリケーションの障害について、一次切り分け後の対応主体、エスカレーション先及び各事業者の費用負担範囲をご教示ください。	ご意見を踏まえ、各関係者の基本的な役割及び障害発生時の責任分界が明確になるよう、仕様書の記載内容を見直します。 なお、本調達において準備するものについては、原則として本調達の受注者が責任を負うものとします。また、障害等の原因が明確でない場合は、関係事業者が連携して原因調査を行い、各契約の範囲及び原因・責任の所在に基づいて費用負担を決定します。
3	16～17	4.2.1 (3)、4.2.3（2）（4）	緊急度が高い場合は時間外対応を行う。また、障害発生時は、原則として 4 時間以内に障害箇所の修復又は暫定措置の実施にあたること。	「原則として 4 時間以内」とする対応について、起算時点及び 4 時間以内に求められる対応状態をご明示願います。受付、調査着手、技術者派遣、暫定措置、サービス復旧及び完全復旧のうち、どの状態を達成条件とするかご教示ください。	起算時点は、受注者がシステムの停止を確認した時点もしくは機構から障害対応の要請を受け付けた時点とします。4 時間以内に求める対応は、原因調査に着手し、修復又は暫定措置の実施により、システムを復旧することを指します。 なお、サービス復旧及び完全復旧までの時間は、障害の内容及び影響範囲により異なるため、受注者は対応状況及び復旧見込みを機構へ随時報告するものとします。
4	18	5.2（2）(3)	令和 9 年 11 月 1 日から本番運用を開始する。アプリケーション開発・保守業者が必要な改修及び動作確認を実施できるよう、令和 9 年 5 月末までにクラウドサービス環境の構築、設定及び接続確認等を行うこと。	令和 9 年 5 月末時点におけるクラウドサービス環境の具体的な完成条件及び引渡条件をご提示願います。 （同日時点までに必要となる構築・設定・試験の範囲をご教示ください） また、令和 9 年 5 月末から 11 月 1 日までの工程、関係事業者との作業順序及び各工程の開始条件・完了条件についてもご提示願います。	令和 9 年 5 月末までにアプリケーション開発・保守業者が必要な改修及び動作確認を実施できるよう、クラウドサービス環境の構築、設定及び接続確認等を行うこととし、そのために必要な部分について、一部引渡しをすることとします。 なお、詳細な工程は、アプリケーション開発・保守業者が未定なため、双方の受注者が決まり次第協議するものとします。
5	18	5.2（7）(8)	仕様書に明記されていない事項であっても、システムの正常稼働に必要なサービス、調整作業等は受注者の責任において実施すること。アプリケーション開発・保守業者との調整等も本調達範囲とする。	「本システムが正常稼働するために必要なサービス、調整作業等」について、想定される作業範囲及び完了条件をご明示願います。契約締結後に、事前に提示されていない要件、現行環境の制約又は追加作業が判明した場合には、影響内容を確認のうえ、費用、納期及び契約内容の変更について協議するとの理解でよいかご教示ください。	本項は、仕様書に明示された業務を正常に履行するために通常必要となる付随的な作業及び調整を対象とするものであって、これに伴うアプリケーション開発・保守業者との調整に要する費用は、設計変更の対象としません。ただし、追加の改修に要する費用については、設計変更の対象とします。
6	18～19	5.2、5.3	受注者は、事前稼働検証、各種ソフトウェアのインストール、環境設定、動作確認、設計・構築及び導入作業等を行うこと。	各試験工程について、受注者、機構及びアプリケーション開発・保守業者の実施範囲をご提示願います。 試験環境、試験データ、合格基準、証跡並びに不具合発生時の対応分界をご明示ください。	各関係者の基本的な役割及び不具合等発生時の対応分界が明確になるよう、仕様書の記載内容を見直します。 なお、本調達において準備するものは本調達内で正常に稼働することを確認します。また、不具合等の原因が明確でない場合は、関係事業者が連携して原因調査を行うものとします。
7	18～19	5.2（6）（11）（13）、 5.3	受注者は、機構及び関係事業者と調整のうえ、環境設定、導入及び検証等を行うこと。必要な詳細設定情報は契約締結後に機構より提示する。	詳細設定情報は契約後速やかにご提供いただけるとの理解でよいかご教示ください。	契約締結後、機構、本調達の受注者及び関係事業者による打合せを速やかに実施し、本業務の設計・構築に必要な詳細設定情報を提示します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
8	-	-	第３章 開発するシステムの要件 ８．信頼性要件	バックアップについて、関連するシステム要件との整合も踏まえ、対象データ、取得方式、取得頻度、保存世代及び復旧方法等の要件をご確認いただけないでしょうか。	ご意見を踏まえ、関連するシステム要件との整合を確認し、バックアップの対象、取得方式、取得頻度、保存世代、保存場所、復旧方法、RTO 及び RPO が明確になるよう仕様書を見直します。
9	3	図２－１特車システム概要図 p ※２	バックアップ用ストレージ内の搬出可能とは、業務ファイルバックアップなどを機構オフィス環境にコピーまたはダウンロード可能であることを示す。	バックアップ方式を特定の構成に限定しない観点から、クラウドサービスが提供するバックアップ機能等により必要なバックアップおよび復旧が可能な場合には、バックアップデータの機構オフィス環境への搬出を必須としない要件に見直していただけないでしょうか。 要件を緩和いただくことにより、バックアップ用サーバの管理やコストを抑えることが可能でございます。	ご意見を踏まえ、仕様書の記載内容を検討します。
10	7	3.2.1(2)	Web サーバ、オンライン申請 AP サーバ、違反・取締 AP サーバ、特車許可 AP サーバ、情報授受サーバについては可用性が 99.99%以上であること[葉友 3.1]をサービスレベルに関する規約等に明記されていること。	許可証ダウンロードサーバも対象になると思いますので、追記いただくようお願いいたします。 また、情報授受サーバおよび許可証ダウンロードサーバについては、採用可能なクラウドサービスおよび構成の選択肢を広げる観点から、可用性の要件を「99.5%以上」に緩和いただけないでしょうか。	ご意見を踏まえ、仕様書の記載内容を検討します。
11	8	表３－１サーバ仕様概要	バックアップサーバ	採用可能なクラウドサービスおよび構成の選択肢を広げる観点から、バックアップ方式を特定のサーバ構成に限定せず、クラウドサービスが提供するバックアップサービスの利用も可能となるよう要件の見直しをお願いいたします。バックアップについて専用サーバの構築を前提とした場合、当該サーバの管理・運用およびセキュリティ対策が別途必要となります。バックアップサービスの利用も可能とする場合、管理・運用不可の軽減およびクラウド環境に適した効率的な運用が可能になると考えます。	ご意見を踏まえ、仕様書の記載内容を検討します。
12	8	3.2.1(3)③	データ通信用インタフェースは、次の仕様を満たすこと。 ・電源は冗長化されていること。	クラウドサービスを利用する場合、電源設備についてはクラウドサービス提供事業者が管理するデータセンター設備として冗長化等の可用性対策が講じられており、受注者が個別に物理的な電源構成を指定・管理するものではありません。 このため、「電源は冗長化されていること」とする要件について、クラウドサービス提供事業者が提供する冗長化された電源設備その他これと同等以上の可用性を確保する仕組みにより満たすことを可能とするよう、要件の見直しをお願いいたします。	ご意見を踏まえ、仕様書の記載内容を見直します。
13	10	3.2.2(2)	本番用 DB サーバをクラウドサービスによるデータベース機能とした場合は、テスト用にも最小構成の同様のデータベース機能を構築するものとする。本番用 DB サーバを実サーバ、もしくは仮想サーバで実現した場合はテスト用サーバの DBMS は Oracle の OTN 開発者ライセンス等の無償版を使用するものとする。	テスト環境における OTN ライセンスの利用可否について販売代理店へ確認したところ、貴機構から Oracle 社へ直接確認する必要がある旨の回答がございました。既にご確認済みの場合は恐縮ですが、テスト環境において OTN ライセンスが利用可能であるか、Oracle 社へご確認をお願いいたします。	ご意見を踏まえ、仕様書の記載内容を検討します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
14	10	3.2.2(3)	SSL/TLS 証明書は自己証明書とする。	テスト用サーバの SSL 証明書は、自己証明書ではなく第三者認証局による証明書への変更をお願いいたします。	ご意見を踏まえ、仕様書の記載内容を見直します。
15	11	3.3.1 (3)	(3) USB トークン 下記基準を満たす USB トークンにクライアント証明書をインストールして納品すること。 ① USB トークンは 250 個 ② Windows11 で管理者権限によるドライバインストールなど、特別な設定なしに使用可能なこと。	利用者への影響を抑えるため、利用者向け手順書の作成、切替期間中の問合せ対応を受注者の作業範囲として明記することを提案いたします。	ご意見を踏まえ、仕様書の記載内容を見直します。
16	12	3.3.4	クライアント端末からインターネット回線を利用し、SSL-VPN 接続により本システム環境へ接続可能とすること。 (1)処理能力 1 ポートあたり 100Mbps 以上の処理能力を有すること。 (2)セキュリティ機能仕様 ①IPS、WAF に相当するセキュリティ機能があること。 ②3 カ月間の通信ログを取得、保管できること。また、ログ監視運用に必要な表示機能を備えていること。 ③クライアント認証は、PC 端末の固有情報を利用する機体認証及びパスワード等の複数要素により認証する仕組みとすること。	SSL-VPN は仕組み上、潜在する脆弱性が多く顕在化も頻発するようになったため、ネットワーク機器の主要ベンダーにおいても機能の廃止に向けた対応がとられています。 SSL-VPN におけるセキュリティ上のリスクを考慮し、本要件の削除をお願いいたします。 より適切なセキュリティ対策の採用を可能にするため、SSL-VPN に方式を限定せず、必要なセキュリティ水準を満たす接続方式を選択可能となるよう要件の見直しをお願いいたします。	ご意見を踏まえ、仕様書の記載内容を見直します。
17	13	3.5（7）関連：4.2.2 （5）②、別添 1	（7）セキュリティ ②下記事象等、システムセキュリティに対する脅威、実害を検知できること。月次での状況報告を行うこと。 (a)不正アクセスのアタック、成功の種類、数（※成功の場合はリアルタイムで対処） (b)システムへの攻撃の可能性のある事象（例、海外からアクセス試行等） (c)システムから機構、会社、国システム以外へのデータ送信と考えられる通信	現行の仕様ではセキュリティ上の脅威を検知し、月次で報告することが求められています。ただし、保守窓口の受付時間は平日 9:00～18:00 です。このため、夜間や休日に攻撃を受けた場合、検知してから分析・対応を始めるまでに時間が掛かる恐れがあります。昨今の情勢を鑑み、攻撃を受けたときの影響が大きく、専門の監視体制で早く検知し、すぐに初動対応できることが重要と考えます。 つきましては、以下を仕様に追記することを提案いたします。 ①SOC（Security Operation Center）サービスを導入し、サーバ・ネットワーク機器などのログやアラートを 24 時間 365 日監視・分析すること。 ②SOC サービスは、情報処理推進機構（IPA）の「情報セキュリ	ご意見を踏まえ、仕様書の記載内容を検討します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			(d)保守業者のみ可能なサーバへのサインイン（成功・失敗）アカウント、数 (e)データベースの異常な読み出し(f)不正プログラムの検知、駆除等の状況 ③通常とは異なる危険な状態の場合、アラートを発すること	ティサービス基準適合サービスリスト」の「セキュリティ監視・運用サービス」に登録された事業者から選ぶこと。 ③別添 1 に「SOC サービス」の項目を追加すること。	
18	14	3.6（2）関連：4.2.2（3）、別添 1	（2）本調達に係る情報システムの構成における以下の脆弱性対策を実施すること。 ① 脆弱性対策を行うとした機器及びソフトウェアについて、公表されている脆弱性情報及び公表される脆弱性情報を把握すること。 ② 把握した脆弱性情報について、対処の要否、可否を判断すること。対処したものに関して対処方法、対処しなかったものに関してその理由、代替措置及び影響を納品時に機構に報告すること。	現行の仕様で求められている脆弱性対策は、公表された脆弱性情報を集め、対処が必要かどうかを判断することにとどまっています。実際に構築した環境に脆弱性が残っていないかを検査で確かめる要件はありません。 つきましては、以下を仕様に追記することを提案いたします。 ①サービス開始前に、インターネットに公開するサーバやネットワーク機器（ファイアウォール、WAF など）を対象として、脆弱性診断を行うこと。 ②脆弱性が見つかった場合は対処し、再診断などで最終的に脆弱性が残っていないことを確認して、機構に報告すること。 ③サービス開始後も、環境の変更や OS・ミドルウェアの更新による影響をふまえ、定期的に（例：年 1 回）診断を行うこと。ただし、過去 1 年以内に同じ検査を行っている場合は、その結果で代えられるものとすること。 ④別添 1 に「脆弱性診断」の項目を追加すること。	ご意見を踏まえ、仕様書の記載内容を見直します。
19	15	4.1.(3)	受注者は、保守対応における責任体制を明確にするため、担当者名を明記した保守体制図及び平常時・障害時における受付窓口・担当者名・連絡先等を明記した連絡体制図を提出することとし、対応時間外に機構から要請する場合の連絡体制図には、クラウドサービス提供事業者の受付窓口・担当者名・連絡先等も明記するものとする。なお、体制を変更する必要が生じた場合には、変更内容を記載した書面をもって報告し、機構の確認を得ること。	クラウドサービス提供事業者の受付窓口・担当者名・連絡先等を機構向けの連絡体制図に記載する要件について、削除いただきたくお願いいたします。 クラウドサービスを利用する場合、クラウドサービス提供事業者はクラウド基盤を提供・管理する立場であり、受注者が当該基盤上に構築したシステムの個別構成や設定内容、障害発生時の状況等をすべて把握しているものではありません。 このため、障害発生時には、本システムの構成及び運用状況を把握している受注者が一次窓口となって原因の切り分けを行い、クラウド基盤に起因する可能性がある場合には、受注者からクラウドサービス提供事業者へ必要 な技術情報を付して問い合わせを行う体制とすることが、迅速かつ適切な障害対応につながると考えます。	ご意見を踏まえ、仕様書の記載内容を見直します。
20	16	4.2.1(3)	受付時間外の対応については、本調達に含まないものとするが、障害・故障の重要度、緊急度が大きいと判断し、機構から要請した場合は、時間外の対応を行うものとする。時間外の対応を行った場合は、対応実績を機構に報告する	「受付時間外の対応については、本調達に含まない」とされている一方、「機構から要請した場合は、時間外の対応を行うものとする」（4.1.(3)）とされております。 時間外の対応を必須とした場合、受注者は受付時間外においても連絡を受理し、必要な要員を確保して対応を開始できる体制を継	ご意見を踏まえ検討しましたが、昨今のセキュリティ環境の変化により緊急時の対応の重要性が高まっていることから、受付時間外の対応に関する本項の記載は原案どおりとします。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			ものとし、実績に応じて精算することとする。	続的に維持する必要があり、実質的に時間外の待機・対応体制を求める要件となります。 このような体制を必須とする場合には、時間外対応に必要な要員及び連絡・エスカレーション体制をあらかじめ確保する必要があることから、「受付時間外の対応は本調達に含まない」とする前提との整合を図る必要があると考えます。 つきましては受付時間外に機構から緊急の要請があった場合については、受注者が対応可能な範囲でのベストエフォート対応とし、時間外における連絡の受理及び対応の実施を保証するものではない旨を明記いただきたくお願いいたします。 なお、時間外に対応できない場合又は詳細な調査・作業が必要となる場合については、翌営業日の受付開始後、速やかに対応を行うものとすることをご検討いただけないでしょうか。 (案) 受付時間外の対応については本調達に含まないものとする。ただし、障害・故障の重要度、緊急度が大きいと機構が判断した場合は、受注者に緊急連絡を行うことができるものとし、受注者は対応可能な範囲でベストエフートによる対応を行うものとする。なお、受付時間外における連絡の受理及び対応の実施を保証するものではなく、詳細な調査・作業等が必要な場合は、原則として翌営業日の受付開始後、速やかに対応するものとする。	
21	16	4.2.1（7） 関連：2.3（１）、 3.1④ホ)、3.2.1 表 3-1、3.4 (3)、別添 1	管理者権限は個人単位で付与することとし、共用 ID の利用は禁止する。権限付与及び変更は承認手続に基づき実施し、少なくとも年 1 回以上棚卸しを行うこと。管理者操作については操作ログを取得し、監査可能な状態を維持すること。	本項では、管理者の操作ログを取得し、監査できる状態を保つことが求められています。一方、2.3 及び表 3-1 のサーバ構成には、ログを集めて保管するためのサーバや機能がありません。 つきましては、以下を仕様に追記していただくようお願いいたします。 ①2.3 (1)、表 3-1 及び別添 1 に「ログ管理サーバ（Syslog サーバ）1 式（又は同等のクラウドサービスのログ管理機能)」を追加すること。 ②各サーバ、ネットワーク機器及びクラウド管理基盤の管理者操作ログ・認証ログを、このログ管理サーバに集めて保管すること。 ③集めたログは、管理者でも書き換えや削除ができないよう、アクセス制御などで改ざんを防ぐこと。 ④ログの保存期間は〇ヶ月とすること ⑤全サーバ・機器の時刻を NTP でそろえ、ログ同士を突き合わせられるようにすること。	ご意見を踏まえ、仕様書の記載内容を見直します。
22	18	5.2.(3)	受注者は、アプリケーション開発・保守業者が必要な改修作業及び動作確認を支障なく実施できるよう、令和 9 年 5 月末までにクラウドサービス環境の構築、設定及び接続確認その他の必要な	「令和 9 年 5 月末までにクラウドサービス環境の構築、設定および接続確認その他の必要な支援を行うこと。」とございますが、開札から構築期限までの期間を踏まえて実現可否を検討させていただきたいため、開札時期を明記いただきたくお願いいたします。	開札時期につきましては、入札公告においてお示しします。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
			支援を行うこと。なお、受注者の責めに帰すことができない事由により、同期限までに当該作業を完了することが困難となった場合は、速やかに監督員と協議すること。		
23	19	5.3（10）	本調達システムが、機構の指示によらず既存のクラウド基盤から他のクラウド基盤に移行する等により既存環境の再構築が必要となる場合、受注者は、既存環境の再現に必要なサーバ・ネットワーク等の再構築及び既存アプリケーション（別途調達）の再設定・データ移行・総合テスト等その他一切の作業を受注者の費用負担と責任において実施するものとする。	以下要件変更をお願いいたします。 ①契約したクラウドサービスが運用期間中にサービス終了となり別の環境構築を行う場合などに発生する経費は現時点では費用算出ができないため別途調達とする要件へ変更いただきたくお願いいたします。 ②既存アプリケーション（別途調達）の再設定・データ移行・総合テスト等の費用は、アプリケーション開発業者でしか対応できないため別途調達とする要件へ変更いただきたくお願いいたします。	ご意見を踏まえ検討しましたが、本項の記載は原案どおりとします。
24	20	6.1.（2）	本調達に係る業務を行う事業者は、事業者組織全体のセキュリティを確保するとともに、機構から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。また、本業務の実施予定部門が JIS Q 27001（ISO/IEC27001）又はプライバシーマーク制度の認証を取得して　おり、情報セキュリティ管理を的確に行う体制が整備されていることを証明すること。	ISO/IEC27001 とプライバシーマークは、どちらも情報を守るための制度ですが、守る対象と目的が異なります。 本システムでは両方の観点が必要となるため、どちらか一方ではなく両方の取得を求めることが適切です。以下の仕様案を検討いただけないでしょうか。 本調達に係る業務を行う事業者は、事業者組織全体のセキュリティを確保するとともに、機構から求められた当該業務の実施において情報セキュリティを確保するための体制を整備すること。また、以下のいずれも満たし、情報セキュリティ管理及び個人情報保護を的確に行う体制が整備されていることを証明すること。 ①本業務の実施予定部門が、（一財）日本情報経済社会推進協会により認定された審査登録機関による JIS Q 27001（ISO/IEC27001）の認証を取得していること。 ②プライバシーマーク制度の認証により、プライバシーマーク使用許諾を受けていること。	ご意見を踏まえ、仕様書の記載内容を見直します。
25	21	6.1.（3）	過去 5 年以内に、本業務で提供するクラウドサービスと同等の環境を 6 か月以上提供した経験を有すること。	本システムは、道路法に基づく特殊車両通行許可という行政処分の事務を支える基盤と認識しております。国のシステムとも接続し、申請者の情報を扱います。このため、システムが停止したり情報が漏えいしたりした場合、機構の業務にとどまらず、物流事業者などの申請者や関係機関にまで影響が及ぶと考えます。こうした点から、受注者の要件は「同等のクラウド環境を提供した経験」だけでは足りず、以下の観点で履行能力を確認する必要があると考えます。 過去 5 年以内に、独立行政法人、国立大学法人、公立大学法人又は国・地方公共団体（以下「公的機関」という。）を発注者とし、ISMAP クラウドサービスリストに登録された今回提案するクラウドサービスを用いた情報システム基盤の構築及び運用保	ご意見を踏まえ、仕様書の記載内容を検討します。

No.	ページ	項目番号	仕様書記載内容	ご意見	回答
				守業務を、元請（発注者と直接契約した者）として 5 件以上受注し、履行した実績を有すること。なお、実績を証明する書類（契約書の写し等）を提出すること。	
26	22	7.2.(5)	受注者は、本調達に係る業務の遂行において、定期的に情報セキュリティ対策の履行状況を機構に報告するとともに、情報セキュリティが侵害され、又はそのおそれがある事象を認知した場合は、認知後速やかに、遅くとも機構が別途指定する時間以内に機構へ第一報を行うこと。第一報には、発生又は認知日時、対象システム、検知事象、影響範囲、初動対応、証拠保全状況及び今後の対応予定を含めること。 なお、当該事象には、受注者に提供し、又は受注者によるアクセスを認める機構の情報の外部への漏えい、目的外利用、受注者による機構のその他の情報への不適切なアクセスその他情報セキュリティ上の影響が疑われる事象を含むものとする。また、被害の程度を把握するため、受注者は、関係するログ、通信記録、操作記録その他必要な記録類を契約終了時まで保存し、機構の求めに応じて、成果物とともに機構に引き渡すこと。	「情報セキュリティが侵害され、又はそのおそれがある事象を認知した場合の第一報の期限」については、事象の内容や対応体制等により実現可能な時間が異なることから、「機構が別途指定する時間以内」ではなく、「具体的な報告期限については契約後に機構と受注者で協議のうえ定める」のように要件の見直しをお願いいたします。	ご意見を踏まえ、仕様書の記載内容を検討します。