仕　様　書

１．件名

「スマートモビリティ社会の構築」プロジェクトにおける研究用データ授受用クラウドストレージサービス

２．研究の概要

国立研究開発法人産業技術総合研究所（以下「産総研」という。）デジタルアーキテクチャ研究センターでは、グリーンイノベーション基金事業「スマートモビリティ社会の構築」プロジェクトの一部として、スマートモビリティ社会の構築に寄与するために、各種関連事業者から提供されるデータを安全に管理し、円滑に処理・連携できる基盤の研究開発を行っている。

３．サービスの概要

本件は、各種関連事業者との間で、安全にデータをやり取りするためのクラウドストレージサービスである。

４．サービス基本要件

(1) 導入するクラウドサービスは十分な稼動実績を有し、運用の自動化やサービスの高度化、情報セキュリティの強化、新機能の追加等に積極的かつ継続的な投資が行われていること。
(2) ISO/IEC27001 又はそれに基づく認証を取得しているクラウドサービスプロバイダにより提供されていること。
(3) 導入するクラウドサービスは ISO/IEC27017 又は ISMS クラウドセキュリティ認証制度に基づく認証を取得していること。また、当該認証の証明書等の写しを提出すること。
(4) 「政府情報システムのためのセキュリティ評価制度（以下、「ISMAP」。）」に定める「ISMAP クラウドサービスリスト」に登録されていること。
(5) 導入するクラウドサービスはセキュリティに係る内部統制の保証報告書（SOC 報告書（Service Organization Control Report））を取得していること。
(6) クラウドサービスにおいて個人情報又は発注者における要機密情報を含むコンテンツを配置する場合は、当該クラウドサービスのデータセンター（バックアップセンターを含む。）は国内リージョンに保管すること。
(7) 原則として、情報資産について日本国外への持ち出しを行わないこと。ただ

し、個人情報又は発注者における要機密情報を含むコンテンツ以外の各種アプリケーションで出力されるデータが日本国内のデータセンターに保管することが難しい場合は、適切な暗号化及び利用者の意図に反して復号されないための措置を講じていること。

(8) クラウドサービスの利用契約に関連して生じる一切の紛争は、日本の地方裁判所を専属的合意管轄裁判所とするものであること。

(9) 契約の解釈が日本法に基づくものであること。

(10) 情報資産の所有権がクラウド事業者に移管されるものではないこと。

(11) クラウドサービスの契約を終了する場合、クラウドサービス上に保存された発注者のデータについて、クラウドサービス上において復元できないかたちで抹消されること。

(12) クラウドサービスに係るアクセスログ等の証跡をサービス上に保存し、担当部署が確認できること。なお、証跡は継続利用した場合は最大7年間保存可能であること。

(13) クラウドサービスの稼動は原則として24時間365日であるものとし、稼動率99.9%以上を満たすこと。

(14) 容量は無制限で利用可能であり、容量ひっ迫等により利用不可状態とならないこと。

(15) クラウドサービス上で取り扱う情報について、機密性及び完全性を確保するためのアクセス制御、暗号化及び暗号鍵の保護並びに管理を確実に行うこと。なお、暗号化等に関する技術は、電子政府推奨暗号リストに適合するものとする。

(16) クラウドサービスの利用者が、自らの意思によりクラウドサービス上で取り扱う情報を確実に削除できること。

(17) クラウドストレージサービスでの不具合や調査等が必要な場合、日本語問合せがクラウドサービスを提供する業者に対して可能であること。サポート対応時間は：平日9:00-18:00（土日祝を除く）を含むこと。

(18) クラウドストレージサービスの稼働状況を確認できるステータスサイトが整備されていること。

５．サービス機能要件

５．１．クラウドストレージサービス機能

(1) クラウドストレージにファイルを配置した状態で組織内外の送信者・受信者が双方向で大容量ファイル等のコンテンツ共有が可能であること。

(2) クラウドストレージサービスの利用において、API連携が可能となるインタフェースを有していること。APIリファレンスは一般公開されており、独自

の作り込み等による開発事業者依存となる部分を最小限とすること。また、UI エレメントの組み込みも可能とすること。

(3) クラウドストレージの利用において、JSON ウェブトークン(JWT)、クライアント資格情報、OAuth2.0 による認証が行えること。

(4) API コール数は月間 175,000API コールを上限とすること。

(5) API 連携を実施するアプリケーションユーザは 100 ユーザを上限とする。また 1 アプリケーションユーザあたり月間 1TB の転送量を上限とすること。

(6) 利用実績を確認するために API コール数を確認できるレポート機能を有していること。

(7) 1 ファイル当たり 50GB までアップロード可能であること。

(8) 同一ファイルのバージョン管理は、無制限に過去に遡り確認が可能であること。

(9) クラウドストレージサービスの機能としてバックアップ／レプリケーションがリアルタイムで遠隔地のバックアップサイトに保管され、被災等でメインサイトが使用できなくなった際は、遠隔地のバックアップサイトに切替わり利用継続が可能であること。なお、メインサイト、バックアップサイトは可用性の観点より複数社のクラウドサービス基盤を利用していること。

(10) クラウドストレージサービスに保存されたデータは CRYPTREC 暗号化リスト（電子政府推奨暗号リスト）に記載された技術で暗号化されていること。

(11) 通信経路は暗号化されていること。

(12) ファイルがアップロードされたタイミングで全てのファイルにウイルスチェックが自動で実施されること。ウイルスを検知した場合は、管理者及び所有者に通知すること。

(13) 不注意な操作や悪意のある操作による、不適切な設定をガードする機能を有すること。

(14) 通常利用では発生し得ない不審・異常な操作を検知する機能を有すること。

５．２．管理者機能

(1) 管理者アカウントを、最低 20 アカウント提供すること。

(2) 管理者が利用するクラウドストレージサービスのインタフェースとして Web ブラウザ（Microsoft Edge 等）を提供すること。サポートしている Web ブラウザは最新を含め過去 2 バージョンまで対応していること。

(3) 外部組織にアクセス権を付与するフォルダおよびその利用状況を確認可能なレポート機能を提供すること。

(4) 外部組織の利用状況を把握する上で、以下レポートが表示・出力可能であること。なお、各種ログはアーカイブせず最大 7 年間はクラウドストレージ

サービス内で保管するものとし、管理者によるログ出力の停止や削除の操作ができないこと。

・セキュリティログ
　クラウドストレージサービス上で取得可能なすべての管理セキュリティ関連設定のログ
・フォルダとファイル
　クラウドストレージサービス上で取得可能な全てのフォルダとファイルに関する情報の現在のスナップショット
・ファイル共有
　クラウドストレージ上で共有されたファイルのユーザ権限の現在のスナップショット
・クラウドストレージ上で取得可能なすべての共有リンクに関する情報の現在のスナップショット
・外部とのファイル共有
　社外でファイルの共有を行っている管理対象ユーザに関する詳細

(5) 外部組織に対しても細かなアクセス権コントロールが行えるようなアクセス権付与が可能であり、利用者に応じた操作制限が可能であること。

５．３．システム移行支援要件

2024 年度は Box 社のクラウドストレージサービスを利用していた。Box 社のクラウドストレージサービスと異なるサービスとなる場合、以下のスコープに応じたシステム移行支援を実施すること。支援は日本語でのコミュニケーションを前提とする。なお、サービス本番環境の各種設定や操作等は産総研にて実施する。

(1) Kickoff Meeting の開催（最大 1h×2 回）
(2) 基本設定の要件確認と設定案の作成（週 1 回の打合せ：最大 1.5 ヶ月間）
(3) セキュリティに関するオプション機能の要件確認と設定方法等の説明（週 1 回の打合せ：最大 1 ヶ月間）
(4) API コール等の連携開発に関する手順及びクラウドストレージサービスの制約や利用方式等に関する説明（週 1 回の打合せ：最大 1 ヶ月間）
(5) ストレージサービスに対し利用者が Linux のコマンドラインやスクリプトから、非対話的にデータをアップロード可能な連携ツールを令和 6 年度に開発した。該当の連携ツールを新サービスの API に利用する場合の関連する API その他のサービスの制約や利用方法等に関する説明（週 1 回の打合せ：最大 1 ヶ月間）
(6) 基本設定やオプション機能、API 連携を進めていく上での QA 対応（最大月

10h/最大 3 ヶ月間）
(7) 上記(1)～(5)の機能説明や利用方法等に関する資料の提供
(8) 導入支援作業完了後に報告書を提出

※上記支援の対応時間や打合せの方式については契約後に調整する。また、連携ツールの詳細については契約後に仕様を開示する。

６．クラウドストレージサービスの履行期間
1 年

７．納品確認試験
受注者が提案した製品が、仕様書を満たす条件の下で、正常に使用できることを確認し、その結果を納品確認試験成績書として提出すること。

８．納入物品
(1) クラウドストレージサービス　一式
(2) サービス利用ライセンス証書（電子媒体）　一式
(3) 納品確認試験成績書（電子媒体）　1 部
(4) システム移行支援要件における提供資料一覧（電子媒体）　1 部
(5) 導入支援作業完了報告書　1 部
※電子媒体は、磁気記録媒体を使用せず、メール等で納入すること。
※項番　(3)～(5)は 2024 年度に使用した Box 社のクラウドストレージサービスと異なるサービスとなる場合に必要とする。

９．納入の完了
本装置は、「８．納入物品」に記載された納入物品が過不足なく納入され、仕様書を満たしていることを確認して、納入の完了とする。

１０．納入期限及び納入場所、履行期間
・５．１．クラウドストレージサービス機能、５．２．管理者機能について
納入期限：２０２５年４月１日
納入場所：東京都江東区青海２－４－７
国立研究開発法人産業技術総合研究所
デジタルアーキテクチャ研究センター
臨海副都心センター別館 7 階 07207 室
履行期間：２０２５年４月１日～２０２６年３月３１日

・５．３．導入支援要件について

納入期限：２０２５年８月３０日

納入場所：東京都江東区青海２－４－７

国立研究開発法人産業技術総合研究所

デジタルアーキテクチャ研究センター

臨海副都心センター別館 7 階 07207 室

※５．３．は 2024 年度に使用した Box 社のクラウドストレージサービスと異なるサービスとなる場合に該当する。

１１．付帯事項

⑴ 本仕様書の技術的内容及び知り得た情報に関しては、守秘義務を負うものとする。

⑵ 本仕様書の技術的内容に関する質問等については、調達請求者と協議すること。また、本仕様書に定めのない事項及び疑義が生じた場合は、調達担当者と協議のうえ決定する。

⑶ サプライチェーン・リスクに対応するため、別紙に記載する事項に従って契約を履行しなければならない。

以上

別紙

サプライチェーン・リスク対応に係る特記事項

１．サプライチェーン・リスクへの対応

受注者は、機器等の意図的な不正改造及び情報システム又はソフトウェアに不正なプログラムを埋め込むなど、国立研究開発法人産業技術総合研究所（以下、「産総研」という。）の意図しない変更が加えられたときに生じ得る情報の漏えい若しくは破壊又は機能の不正な停止、暴走その他の障害等の情報セキュリティ上のリスク（以下「サプライチェーン・リスク」という。）に対応するため、受注者は「IT 調達に係る国の物品等又は役務の調達方針及び調達手続に関する申合せ」（平成 30 年 12 月 10 日関係省庁申合せ）に基づく対応を図らねばならない。

２．意図しない変更に対する対策

①受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得るべきソースコード、プログラム等（以下「ソースコード等」という。）の埋込み又は組込みその他産総研担当者の意図しない変更を行ってはならない。

②受注者は、本業務の履行に際して、サプライチェーン・リスクが潜在すると知り、又は知り得るべきソースコード等の埋込み又は組込みその他産総研担当者の意図しない変更が行われないように相応の注意をもって管理しなければならない。

③受注者は、本業務の履行に際して、情報の窃取等により研究所の業務を妨害しようとする第三者から不当な影響を受けるおそれのある者が開発、設計又は製作したソースコード等（受注者がその存在を認知し、かつ、サプライチェーン・リスクが潜在すると知り、又は知り得るべきものに限り、主要国において広く普遍的に受け入れられているものを除く。）を直接又は間接に導入し、又は組み込む場合には、これによってサプライチェーン・リスクを有意に増大しないことを調査、試験その他の任意の方法により確認又は判定するものとする。

３．サプライチェーン・リスクにかかる調査の受入れ体制

①受注者は、本業務に産総研担当者の意図しない変更が行われるなど不正が見つかったときは、追跡調査や立入検査等、産総研と連携して原因を調査し、サプライチェーン・リスクを排除するための手順及び体制を整備し、当該手順及び体制を示した書面を産総研担当者に提出しなければならない。

４．サプライチェーン・リスクを低減するための対策

①受注者は、サプライチェーン・リスクを低減する対策として、本業務の設計、構築、運用・保守の各工程における不正行為の有無について定期的または必要に応じて監査を行う体制を整備するとともに、本業務により産総研に納入する納入物品に対して意図しな

い変更が行われるリスクを回避するための試験を行わなければならない。当該試験の項目は、情報セキュリティ技術の趨勢、対象の情報システムの特性等を踏まえ、受注者において適切に設定するものとする。

②機器の納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、４．①の対応は不要。

５．受注者の業務責任者

①受注者は、本業務の履行に従事する業務責任者及び業務従事者（契約社員、派遣社員等の雇用形態を問わず、本業務の履行に従事する全ての従業員をいう。以下同じ。）を必要最低限の範囲に限るものとする。

②機器納入であり、かつ、設計、構築、運用・保守の各工程が存在しない場合は、５．①の対応は不要。

６．再委託

6.1 本業務の第三者への委託の制限

受注者は、産総研の許可なく、本業務の一部又は全部を第三者（再委託先）に請け負わせてはならない。ただし、6.2 に定める事項を遵守する場合はこの限りではない。

6.2 第三者への委託に係る要件

①受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託先の事業者名、住所、再委託対象とする業務の範囲、再委託する必要性について記載した承認申請書を、委託元である産総研に提出し、書面による事前承認を受けなければならない。

②受注者は、本業務の一部又は全部を第三者に再委託するときは、再委託した業務に伴う再委託者の行為について、全ての責任を負わなければならない。

③受注者は、知的財産権、情報セキュリティ（機密保持を含む。）及びガバナンス等に関して、本仕様書が定める受注者の責務を再委託先も負うよう、必要な処置を実施し、その内容について委託元である産総研の承認を得なければならない。

④受注者は、受注者がこの仕様書の定めを遵守するために必要な事項について本仕様書を準用して、再委託者と約定しなければならない。

⑤受注者は、前号に掲げる情報の提供に加えて、再委託先において本委託事業に関わる要員の所属、専門性（情報セキュリティに係る資格・研修実績等）、実績及び国籍についての情報を委託元である産総研へ提出すること。

⑥受注者は、再委託先において、産総研の意図しない変更が加えられないための管理体制について委託元である産総研に報告し、許可又は確認（立入調査）を得ること。

７．その他

①提出された資料等により産総研担当者に報告された内容について、サプライチェーン・

リスクが懸念され、これを低減するための措置を講じる必要があると認められる場合に、調達担当者は受注者に是正を求めることがあり、受注者は相当の理由があると認められるときを除きこれに応じなければならない。

②産総研は、受注者の責めに帰すべき事由により、本情報システムに産総研担当者の意図しない変更が行われるなど不正が見つかった場合は、契約条項に定める契約の解除及び違約金の規定を適用し、本業務契約の全部又は一部を解除することができる。