令和８年度新潟県企業誘致支援クラウドサービス提供業務仕様書

令和８年４月１日

１　業務名

令和８年度新潟県企業誘致支援クラウドサービス提供業務

２　業務の背景・目的

企業誘致を進めるにあたっては、目まぐるしく変わる社会経済の情勢に迅速に対応し、柔軟な企業選定をした上で働きかけを行うことが必要となっている。

このため、多様な企業情報を基に、本県経済の活性化に寄与し且つ本県への立地が見込まれる企業を抽出すると同時に、反社会的勢力との関連がある企業や倒産可能性の高い企業等を選別しリスクを回避することを目的として、クラウド型企業データベースを導入することとする。

３　契約期間

契約締結の日から令和９年３月 31 日（水）まで

４　業務の概要

（１）概要

オンラインにより、任意に調査対象に指定した企業等に関する情報を提供するほか、対象企業の訪問記録、企業担当者の名刺情報管理サービス等を提供するものとする。

５　要件

（１）機能要件

ア　企業及び拠点データ

・国内に拠点のある法人の拠点データ（本社及び事業所）を網羅していること。

・データについては網羅的に登記簿の購入や行政機関への開示請求、官公庁や自治体の公開情報等を用いて調査を行い、中小・零細企業まで調査を行っていること。

・倒産や閉鎖した法人や拠点の情報等について、登記簿情報との照合を行うなどし、実態に近い状態に更新されていること。

イ　企業の基本情報

以下の項目について日々調査を行い、提供ができること。

①　企業名
②　本社所在地
③　拠点名（拠点を持つ企業の場合のみ）
④　拠点所在地（拠点を持つ企業の場合のみ）
⑤　代表者名
⑥　役員名
⑦　業種分類
⑧　事業内容
⑨　資本金額/売上高/従業員数/利益（実数値ではなくレンジ表記でも可）

ウ　グループ企業や本支店関係の情報

・親会社・子会社・関連会社等の企業グループ階層構造について、多くの階層（子会社だけでなく孫会社・ひ孫会社等まで）を提供できること。

・本社及び事業所の関係を提供できること。

エ　部署、人事異動、ニュース情報

・各種公開情報をもとにした企業の部署情報、人事異動、ニュースの情報を提供できること。

・部署情報については部署名に加えて部署直通番号も提供できること。

オ　反社・財務・評判等を統合した網羅的なリスク情報

反社会的勢力との繋がり、財務健全性、行政処分歴、実在性、風評等の網羅的なリスクを企業検索時点で即時に確認ができ、フィルタリング・除外が可能であること。

カ　ウェブ行動ログによるインテントデータ

・企業のインターネット上の行動履歴をもとにインテント（興味・関心情報）を特定し、可視化できること。

・県の運営するサイトへのアクセスや県の指定するキーワードに興味を持つ企業を抽出できること。

・当該データ収集の際は、プライバシーやセキュリティに配慮し、同意のない個人情報の収集や、Cookie による収集は行っていないこと。

キ　企業リスト抽出機能

・上記「イ」「ウ」「オ」「カ」の各情報を掛け合わせてリスト抽出が可能であること。

・リストの抽出は、県が適時、Excel（.xlsx）形式でダウンロードが可能であること。

ク　名刺管理

企業担当者の名刺情報を管理できること。

ケ　訪問記録管理

企業とのやり取りを記録できること。

コ　利用可能人数

20 名以上の利用が可能であり、必要に応じて人数の拡大が可能であること。

（２）非機能要件

ア　セキュリティ対策

以下のセキュリティ対策が講じられていること。

① アカウント管理

クラウドサービス利用のために作成したアカウントの随時削除等が行えること。

② アクセス制御

利用者ごとにアカウントを割り当てられ、必要に応じてアクセス権限を個別に設定できること。

③ データ保存場所

当該クラウドサービスで利用するデータセンターの設置場所が、国内であり、日本の裁判管轄、法令が適用されること。

④ データの暗号化

クラウドサービス利用における通信及びクラウドサービス上に蓄積する全てのデータについて、暗号技術検討会及び関連委員会（CRYPTREC）により安全性及び実装性能が確認された「電子政府推奨暗号リスト」に掲載される暗号アルゴリズムを用

いて暗号化されること。

⑤ 暗号化に用いる暗号鍵

鍵の生成から廃棄に至るまでのライフサイクルにおいて、適切なセキュリティ対策を講じた管理を行うこと。

⑥ データの消去

クラウドサービスの利用終了時に、暗号鍵の抹消によるデータの暗号化消去（Cryptographic Erase）を行い、暗号化/鍵消去ログ等により消去の実施記録に係る証跡ないし消去の実施を証明する書面を提出できること。

⑦ ログの取得

・不正検知に必要なログ（ログイン/ログアウト履歴（成功/失敗）、操作ログ、セキュリティ機器の検知ログ、データベースログ、アプリケーションログ等）を取得し、90 日間以上保存できること。

・時刻同期の方法が確立され、取得するログの時刻及びタイムゾーンが統一されていること。

イ　サービスレベル合意書（SLA: Service Level Agreement）

以下のサービスレベル設定基準を基に、県と協議の上、稼働時までにサービスレベル合意書（SLA: Service Level Agreement）を締結すること。

① サービス稼働率

月間稼働率　99.5%以上

※月間稼働率は、1 か月の総時間から計画停止時間及び 当県起因の停止時間を除外した時間を分母とし、当該月において正常に利用可能であった時間の割合とする。

② 目標復旧時間

24 時間以内

③ 目標復旧レベル

直近 24 時間以内に取得された バックアップデータを用いた復旧とする。

④ バックアップレベル

○ 世代管理

バックアップは日次で取得し、７世代以上保存すること。

○ 保管方法

バックアップデータは本番環境と分離した領域に保存し、単一障害点を回避する構成とすること。

⑤ 計画停止に関する事前通知方法

原則、メールにて１週間より前に通知することとし、緊急やむを得ない場合は、事前通知を行わず 速やかに事後報告を行うものとする。

⑥ 障害発生時の報告時間

検知から１時間以内に報告

⑦ 情報セキュリティインシデント発生時の体制

インシデント対応体制、エスカレーション経路、連絡先は文書化し、事前に県に提示すること。

⑧ 情報セキュリティ対策の履行が不十分な場合の対処方法

・事案の発生を確認した際には、速やかに県へ報告し、その際に、見込まれるサービ

ス停止時間等を伝達すること。
・再発防止策（機構的、人的、制度的）も調査結果により策定し、通知を実施すること。
・締結する SLA は、天災、第三者による不正行為、利用者環境に起因する障害等、サービス提供者の責に帰さない事由については適用しないこと。
・SLA 未達であっても直ちにペナルティを負うものではなく、SLA 未達時は速やかにその原因を分析し、県へ報告するとともに、必要な是正措置及び再発防止策を講じるものとすること。
・是正措置を講じてもなお改善が認められない場合には、本契約の継続について協議を行うことができること。

（３）運用・管理要件

ア　サポート体制

サービス利用中の問い合わせに対し、祝日を除く平日 10:00～17:00 の間は日本語対応可能な一元的なサポート窓口を設置すること。

イ　管理体制

・クラウドサービスの開発及び運用において、県の意図しない変更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。また、当該品質保証体制が書類等で確認できること。
・クラウドサービスにおいて、県の意図しない変更が行われるなどの不正が見付かったときに、追跡調査や立入検査等、県とクラウドサービス提供者が連携して原因を調査・排除できる体制を整備していること。また、当該体制が書類等で確認できること。
※なお、クラウドサービス利用者全体の使用率が低い等の理由から変更を加えるなど、合理的な理由による変更については県の意図しない変更に含まれないものとする。

ウ　役割分担

利用者とクラウドサービス提供者との役割及び責任の共有及び分担が明確であり、文書化できること。

エ　マニュアル提供

操作マニュアル及び FAQ の作成及び提供、またはウェブサイト上への操作マニュアルと同等の機能及び FAQ の掲載により、県がいつでも閲覧可能な状態とすること。

オ　操作研修

・導入時に初回の操作説明会を実施できること。
・その後もユーザーの習熟状況に合わせた操作説明やサービス活用に向けたフォローを実施できること。

（４）セキュリティ・ガバナンス要件

ア　セキュリティ認証制度による認証取得

以下のいずれかの認証を取得していること
① 政府情報システムのためのセキュリティ評価制度（ISMAP）
② 米国連邦政府によるリスク及び認証管理プログラム（FedRAMP）
③ ISO/IEC 27017 に基づく、ISMS（情報セキュリティマネジメントシステム）クラウドセキュリティ認証
④ JASA クラウドセキュリティ推進協議会（JCISPA）が定めるクラウド情報セキュリティ管理基準に基づく CS マーク ゴールド認証の取得

イ　監査フレームワークに基づく監査報告書

以下のいずれかの監査報告書の内容から当該クラウドサービス提供者の信頼性が十分であることが総合的・客観的に評価判断できること。

① 日本公認会計士協会（JICPA）が定める保証業務実務指針 3850「情報セキュリティ等に関する受託業務の Trust に係る内部統制の保証報告書に関する実務指針」に基づく監査報告書

② 米国公認会計士協会（AICPA）が定める基準に基づき評価された SOC 2/SOC 3（System and Organization Control）Type I 及び Type II 報告書

（５）契約・調達条件

ア　目的外利用

クラウドサービスの利用を通じて県が取り扱う情報資産について、クラウドサービス提供者による目的外利用がされないこと。

イ　契約形態

画一的な約款や規約等への同意のみで利用可能となるクラウドサービスではなく、個別契約等に基づく利用が可能であること。

ウ　個人情報等の取得・保護・管理

・サービス提供者は、本業務の実施上知り得た情報については、秘密を保持するとともに、契約目的以外に使用してはならない。また、契約期間終了後も同様とする。

・サービス提供者は、別記１「個人情報取扱特記事項」及び別記２「情報セキュリティ関連業務特記事項」を遵守すること。個人情報の保護については十分に注意し、流出・損失を生じさせないこと。

６　その他

（１）契約締結後速やかに県と協議を行い、業務内容について十分な理解を図るとともに、サービス提供契約期間においても定期的に協議を行うこと。

（２）県が本サービスの次年度以降の利用の継続を希望する場合は、予算の範囲内で、所定の手続により改めて次年度利用に係る契約を締結するものとする。

（３）本業務において取得した登録者等に関するデータは、本契約が終了し、かつ次年度以降の契約が締結されない場合に限り、サービス提供者において完全に消去すること。

（４）クラウドサービス提供者は、本事業の実施に当たっては、本仕様書及び企画提案書に従い実施するものとし、実施内容の詳細について事前に県と協議すること。なお、本仕様書と企画提案書で相違する内容があるときは県とクラウドサービス提供者が協議し、協議が整わないときは本仕様書が優先する。

（５）クラウドサービス提供者は、やむをえない事情により、本仕様書の変更を必要とする場合は、県と協議のうえ、仕様書変更の承認を得ること。本仕様書に定めのない事項及び本仕様書に疑義が生じた場合には、県及びクラウドサービス提供者双方で協議の上、決定するものとする。

別記１

個人情報取扱特記事項

（基本的事項）

第１　乙は、個人情報（個人に関する情報であって、特定の個人が識別され、又は識別され得るものをいう。以下同じ。）の保護の重要性を認識し、この契約による業務を実施するに当たっては、個人の権利利益を侵害することのないよう、個人情報を適正に取り扱わなければならない。

（秘密の保持）

第２　乙は、この契約による業務に関して知ることのできた個人情報を他に漏らしてはならない。この契約が終了し、又は解除された後においても、同様とする。

（収集の制限）

第３　乙は、この契約による業務を行うために個人情報を収集するときは、その業務の目的を達成するために必要な範囲内で、適法かつ公正な手段により行わなければならない。

（適正管理）

第４　乙は、この契約による業務に関して知ることのできた個人情報の漏えい、滅失及びき損の防止その他の個人情報の適切な管理のために必要な措置を講じなければならない。

（利用及び提供の制限）

第５　乙は、甲の指示がある場合を除き、この契約の業務に関して知ることのできた個人情報を契約の目的以外の目的に利用し、又は甲の承諾なしに第三者に提供してはならない。

（複写又は複製の禁止）

第６　乙は、この契約による業務を処理するために甲から引き渡された個人情報が記録された資料等を甲の承諾なしに複写し、又は複製してはならない。

（再委託の禁止）

第７　乙は、この契約による業務を行うための個人情報の処理は、自ら行うものとし、甲が承諾した場合を除き、第三者にその処理を委託してはならない。

（資料等の返還等）

第８　乙は、この契約による業務を処理するために甲から引き渡され、又は乙自らが収集し、若しくは作成した個人情報が記録された資料等は、業務完了後直ちに甲に返還し、又は引き渡すものとする。ただし、甲が別に指示したときは、その指示に従うものとする。

（従事者の監督）

第９　乙は、この契約による業務に従事している者に対して、在職中及び退職後において、その業務に関して知ることのできた個人情報を他に漏らしてはならないこと、又は契約の目的以外の目的に使用してはならないことなど、個人情報の保護に関して必要かつ適切な監督を行わなければならない。

（実地調査）

第 10　甲は、必要があると認めるときは、乙がこの契約による業務の執行に当たり取り扱っている個人情報の状況について随時実地に調査することができる。

（指示等）

第 11　甲は、乙がこの契約による業務に関して取り扱う個人情報の適切な管理を確保するため、乙に対して必要な指示を行い、又は必要な事項の報告若しくは資料の提出を求めることができる。

（事故報告）

第 12　乙は、この契約に違反する事態が生じ、又は生ずるおそれのあることを知ったときは、速やかに甲に報告し、甲の指示に従うものとする。

注　「甲」は新潟県を、「乙」は受託事業者を指す。

別記２

情報セキュリティ関連業務特記事項

（基本的事項）

第１　乙は、情報セキュリティ対策の重要性を認識し、この契約による業務を実施するに当たっては、受託事業者が守るべき内容を十分理解するとともにこれらを遵守しなければならない。

（情報資産の取扱い）

第２　乙は、情報資産（複製されたものを含む。以下同じ。）を他へ持ち出す場合には、甲の許可を受けなければならない。

第３　乙は、重要な情報を記録した媒体を廃棄する場合、情報を復元できないよう消去を行った上、甲の許可を受けなければならない。

（機器等の取扱い）

第４　乙は、使用する機器、記録媒体等を第三者に使用されること又は情報を閲覧されることのないようにしなければならない。

（従事者への啓発）

第５　乙は、この契約による業務に従事している者に対し、情報セキュリティ対策について啓発しなければならない。

（異常時の報告）

第６　乙は、情報資産に対する侵害又は侵害の恐れのある場合には、直ちに甲に報告しなければならない。

第７　乙は、ネットワーク又は情報システムの誤作動等の異常を発見した場合には、直ちに甲に報告しなければならない。

（再委託の禁止）

第８　乙は、この契約による業務を行うための情報資産の処理は、自ら行うものとし、甲が承諾した場合を除き、第三者にその処理を委託してはならない。

（ソフトウェアの無許可導入・更新・削除の禁止）

第９　情報システムで使用する端末等におけるソフトウェアの導入、更新又は削除は、甲の許可がなければ行ってはならない。

（機器構成の無許可変更の禁止）

第 10　情報システムを構成する機器の増設又は交換は、甲の指示がある場合を除いて行ってはならない。

（ネットワークへの無許可接続の禁止）

第 11　乙は、ネットワークへの機器の接続又はネットワークに接続している端末等の他ネットワークへの接続は、甲の指示がある場合を除いて行ってはならない。

（コンピュータウィルス対策）

第 12　乙は、次の事項を遵守しなければならない。

(1) 外部からファイルを取り入れる場合及び外部へファイルを提出する場合は、ウイルスチェックを行うこと。

(2) 甲が提供するウイルス情報を常に確認すること。

（法令遵守）

第 13　乙は、業務の遂行において使用する情報資産について、次の法令等を遵守し、これに従わなければならない。

(1) 不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号）

(2) 著作権法(昭和 45 年法律第 48 号)

(3) 新潟県個人情報保護条例(平成 17 年新潟県条例第 2 号)

（実地調査）

第 14　甲は、必要があると認めるときは、乙がこの契約による業務の執行に当たり実施している情報セキュリティ対策の実施状況について随時実地に調査することができる。

注　「甲」は新潟県を、「乙」は受託事業者を指す。