W3 DataPlatform

個人データ取扱特約（DPA）

Data Processing Addendum

第 1.2 版

W3 DataPlatform 個人データ取扱特約（DPA）

効力発生日：[要入力：効力発生日]

本個人データ取扱特約（以下「本 DPA」といいます。）は、株式会社ダイアログ（以下「当社」といいます。）と顧客との間の W3 DataPlatform サービス利用規約、注文書その他本サービスの利用に関する契約（以下総称して「原契約」といいます。）の一部を構成します。本 DPA で定義しない用語は原契約の定義に従います。

第 1 条（目的、適用範囲および優先順位）

1. 本 DPA は、当社が本サービスの提供に関連して、顧客の委託または指示に基づき顧客個人データを取り扱う場合に適用します。当社が契約管理、請求、営業連絡、セキュリティ管理その他自己の目的で取得する担当者情報、利用状況情報その他の個人情報には、当社の個人情報保護方針、当社ウェブサイトに掲載する「個人情報の取り扱いについて」および適用データ保護法令が適用され、本 DPA は適用されません。

2. 顧客個人データの取扱いに関して本 DPA と原契約が抵触する場合、本 DPA が優先します。ただし、注文書が本 DPA の特定条項を明示して変更する場合は、注文書が優先します。安全管理措置については別紙 3（データセキュリティ措置）が、可用性およびサービスクレジットについては SLA が適用されます。

3. 本 DPA は、顧客が第三者から個人データの取扱いの委託を受け、当該個人データを本サービスで取り扱う場合にも適用します。この場合、当社は再委託先として顧客個人データを取り扱い、顧客は当該第三者から本 DPA に必要な指示および権限を受け、当社への連絡および指示を一元的に行います。

第 2 条（定義）

1. 本 DPA における用語の意味は、次の表のとおりとします。

用語	定義
適用データ保護法令	個人情報の保護に関する法律（以下「個人情報保護法」といいます。）、同法施行令、同法施行規則および個人情報保護委員会が定めるガイドラインその他顧客個人データの取扱いに適用される日本の法令等。
顧客個人データ	顧客データに含まれる個人情報または個人データで、当社が顧客の委託または指示を受けて取り扱うもの。
委託元	個人情報保護法上の個人情報取扱事業者として、顧客個人データの取扱いを委託する者。顧客が第三者から個人データの取扱いの委託を受けている場合の当該第三者を含む。
本人	顧客個人データによって識別され、または識別可能な自然人。
再委託先	当社が、本サービスの提供のため顧客個人データの全部または一部を取り扱わせる第三者または当社関係会社。
漏えい等	当社の管理下にある顧客個人データの漏えい、滅失、毀損、改変、権限のない開示またはアクセスにつながる、発生したまたは発生したおそれのある事象。原因がバグ、設定誤り、内部行為または外部攻撃のいずれかを問わない。
取扱い	取得、記録、整理、保存、変更、検索、参照、利用、送信、開示、結合、制限、削除その他個人データに対して行われる操作。

2. 顧客個人データへの影響が認められない遮断済みのスキャン、ログイン試行、DDoS 試行その他の不成功の活動は、漏えい等に含みません。ただし、当社は必要な調査および防御措置を行います。

第 3 条（当事者の役割および法令遵守）

1. 顧客は、顧客個人データの取扱いを当社に委託する者（顧客が第三者から委託を受けている場合は、当該委託を受けた者）として、当社は、顧客から委託または再委託を受けた者として、それぞれ個人情報保護法その他の適用データ保護法令を遵守します。

2. 顧客は、顧客個人データの取得、当社への提供、本サービスによる取扱いおよび当社への指示について、必要な利用目的の特定・通知または公表、本人の同意の取得その他個人情報保護法上必要な手続を履践し、必要な権利および権限を確保します。顧客は、当社への指示が適用データ保護法令に適合することについて責任を負います。

3. 当社は、指示が適用データ保護法令に違反すると合理的に判断した場合、法令上許される範囲で顧客へ通知し、必要な範囲で当該指示の実行を停止できます。当社は、顧客個人データの内容を常時監視し、法令上の区分または正確性を判定する義務を負いません。

第 4 条（処理指示および目的制限）

1. 原契約、本 DPA、注文書、別紙 1、認定ユーザーが本サービス上で行う設定および操作は、顧客から当社に対する顧客個人データの取扱いの指示（以下「処理指示」といいます。）を構成します。当社は、本サービスの提供、運用、保守、障害対応、セキュリティ確保、サポートおよび法令遵守に必要な範囲でのみ顧客個人データを取り扱います。追加指示は、当社が書面で承諾した場合に限り適用されます。

2. 当社は、顧客個人データを広告、販売、第三者の利益のための利用、または AI モデル（当社または第三者が提供するものを問いません。）の学習に使用しません。当社は、法令により取扱いを義務付けられる場合、法令上禁止されない限り、当該法的要件を事前に顧客へ通知します。

3. 顧客は、目的達成に必要な最小限の個人データのみを本サービスへ投入し、保持期間、アクセス権限、出力先および AI 機能への入力を適切に設定します。要配慮個人情報、マイナンバー、カード会員データ、認証用秘密情報その他利用規約上の制限データは、当社の事前の書面による承諾および追加条件がない限り投入できません。

4. 前項までの定めにかかわらず、当社は、顧客データから、顧客および本人を識別できず、かつ元のデータを復元できない形式に加工した統計情報を作成し、本サービスの改善ならびに業界動向の分析およびベンチマーク情報の作成のために利用できます。当該統計情報の作成に顧客個人データを用いる場合は、適用データ保護法令上許容される範囲に限ります。

第 5 条（秘密保持および取扱担当者）

1. 当社は、顧客個人データへアクセスする役員、従業員、専門家および再委託先を、本サービスの提供等に必要な者に限定し、職務上必要な範囲の権限のみを付与します。

2. 当社は、当該者に契約上または法令上の秘密保持義務を負わせ、顧客個人データの取扱いに関する適切な教育および監督を行います。秘密保持義務は、アクセス終了後および原契約終了後も、顧客個人データ性が存続する限り適用されます。

第 6 条（安全管理措置およびプライバシー・バイ・デザイン）

1. 当社は、取扱いの性質、範囲、状況および目的、顧客個人データの性質ならびに本人の権利利益に対するリスクを考慮し、合理的かつ適切な組織的、人的、物理的および技術的安全管理措置を維持します。契約上の最低措置は別紙 3（データセキュリティ措置）に定めます。

2. 当社は、アクセス制御、テナント分離、通信および保存時の暗号化、秘密情報管理、ログ・監視、バックアップ、脆弱性対応、インシデント対応ならびに終了時の削除を、リスクに応じて実施します。当社は、全ての事故を完全に防止することを保証するものではありませんが、事故原因が外部攻撃であることだけを理由に本 DPA 上の義務を免れません。

3. 顧客は、本人の請求への対応、保持期間、データ最小化およびアクセス権限の設定に利用できる本サービスの機能を、顧客の責任で適切に使用します。顧客の設定、端末、ネットワーク、データソース、出力先および顧客が選定する外部 AI クライアントには、顧客の安全管理責任が適用されます。

第 7 条（漏えい等の通知および対応）

1. 検知、封じ込めおよび調査

当社は、漏えい等を認識した場合、速やかに影響を評価し、必要に応じてアクセス遮断、認証情報の無効化、対象処理の停止、証拠保全その他の封じ込め措置を行い、原因、期間、対象、影響および再発防止策を合理的に調査します。

2. 顧客への通知

(1) 当社は、顧客個人データに関する漏えい等が発生した、または発生したおそれがあると合理的に判断した場合、調査完了を待たず、速やかに顧客の指定連絡先へ第一報を行います。当社は、顧客が適用法令上の報告期限に対応できるよう合理的に配慮します。固定時間内の通知を合意する場合は、注文書に明示します。

(2) 前号の通知には、その時点で合理的に判明している範囲で、事象の性質、発生または判明日時、対象となる個人データおよび本人の区分・概数、想定される影響、当社が講じたまたは予定する措置、顧客に推奨する措置ならびに照会先を含めます。未確定事項は暫定情報として示し、重要な追加情報が判明した場合は合理的な範囲で更新します。

3. 法定報告・本人通知への協力

(1) 顧客は、個人情報保護法第 26 条に基づく個人情報保護委員会への報告および本人への通知の要否、内容および方法を決定します。当社は、取扱いの性質および当社が利用できる情報を考慮し、顧客が法令上必要な対応を行うため合理的に協力します。当社は、個人情報保護法第 26 条第 1 項ただし書に基づき、本条第 2 項第 1 号の通知を顧客に行うことにより、当社の個人情報保護委員会への報告義務を履行するものとします。ただし、法令上当社が自ら報告すべき場合はこの限りではなく、この場合、当社は事前に顧客と報告内容を協議します。

(2) 通知または協力は、当社の責任、過失または賠償義務の承認を意味しません。標準的な第一報、更新および当社保有情報の提供には追加料金を課しません。顧客固有の大規模な調査・資料作成等については、当社の本 DPA 違反に起因する場合を除き、事前協議の上で合理的な費用を請求できます。

第 8 条（本人からの請求等）

1. 本人から、顧客個人データに関する開示、訂正、追加若しくは削除、利用停止若しくは消去、第三者提供の停止、第三者提供記録の開示その他個人情報保護法に基づく請求（以下「開示等の請求」といいます。）を当社が直接受け、当該顧客を特定できる場合、当社は、法令上禁止されない限り、当該請求を速やかに顧客へ転送し、本人へ実質的な回答を行いません。ただし、本人を顧客の窓口へ案内することができます。

2. 顧客は、本サービスの標準機能を用いて本人からの請求に対応します。顧客が当該機能により合理的に対応できない場合、当社は、取扱いの性質を考慮し、当社が利用できる情報および技術的に可能な範囲で合理的に協力します。追加開発その他標準外の対応は、当社の本 DPA 違反に起因する場合を除き、別途費用の対象とできます。

第 9 条（委託先の監督への協力および記録）

1. 顧客が、個人情報保護法第 25 条に基づく委託先の監督、個人情報保護委員会からの報告徴収その他の求めへの対応その他適用データ保護法令上必要な確認を行う場合、当社は、顧客が本サービスまたは公開資料から取得できない情報について、取扱いの性質および当社が利用できる情報を考慮し、合理的に協力します。

2. 当社は、本 DPA に基づく義務の履行状況を確認できるよう、合理的に必要な記録を作成し、保存します。顧客は、顧客個人データについて、利用目的、本人の区分、データ項目、保存期間およびアクセス権限を管理し、個人情報保護法に定める第三者提供に係る記録を作成し、保存します。

第 10 条（再委託）

1. 顧客は、当社が本サービスの提供に必要な再委託先を利用することを一般的に承認します。本 DPA の効力発生日現在の再委託先は、別紙 2 または当社が指定する再委託先一覧に記載します。

2. 当社は、顧客個人データを取り扱う再委託先との書面契約において、その役務に応じ、本 DPA と実質的に同等以上のデータ保護および秘密保持義務を課します。当社は、再委託先の行為について、当社自身が行った場合に原契約および本 DPA 上負う範囲で責任を負います。

3. 当社は、新たな再委託先が顧客個人データの取扱いを開始する 30 日前までに、再委託先一覧を更新し、第 17 条（連絡先）第 2 項に基づき顧客が指定した連絡先へ通知します。緊急のセキュリティ対応またはサービス継続のため事前通知が合理的に困難な場合、当社は可能な限り早く通知します。

4. 顧客は、通知受領後 10 日以内に、データ保護上の合理的な理由を明示して異議を述べることができます。当事者は代替措置を誠実に協議し、合理的な代替策がなく当該再委託先なしに該当機能を提供できない場合、顧客は当該機能に関する注文を終了し、未利用期間の前払料金の按分返金を受けることができます。再委託先の変更に関する顧客の救済は、本項に定めるものに限ります。

第 11 条（公的機関等からの開示要求）

1. 当社が、顧客個人データの開示、保存またはその他の取扱いを求める法的拘束力のある公的機関、捜査機関または裁判所からの要求を受けた場合、合理的に可能なときは、要求主体に顧客から直接取得するよう求めます。

2. 当社が開示を法的に義務付けられる場合、当社は、法令上禁止されない限り、顧客が保護命令その他の救済を求められるよう速やかに通知し、要求の適法性および範囲を合理的に確認し、必要最小限の顧客個人データのみを開示します。法令上通知が禁止される場合、当社は合理的に可能な範囲で禁止の解除を求めます。

第 12 条（処理場所および越境移転）

1. 当社は、注文書または別紙 1 に記載された標準 AWS リージョンで顧客個人データを保存します。顧客によるアクセス元、顧客が指定するデータソース・出力先、および顧客が選定する外部 AI クライアントに起因する移転は、顧客が管理します。

2. AI コード生成機能では、ユーザーの指示文、編集中のコードおよび入力データの列名・型等のスキーマ情報が米国リージョンで処理されます。本サービスは業務データの行データを AI コード生成へ自動送信しませんが、ユーザーが指示文またはコードに個人データを記載した場合、その情報は送信されます。外部 AI クライアントからの MCP 接続では、顧客が実行を指示したクエリ結果（行データを含みます。）が、別紙 1 に記載する経路および処理場所を経由して顧客の指定する外部 AI クライアントへ返却されます。具体的な処理場所および再委託先は別紙 1 および別紙 2 に記載します。

3. 当社は、顧客個人データを日本国外で取り扱う場合（再委託先が日本国外で取り扱う場合を含みます。）、取り扱う国の個人情報の保護に関する制度を把握した上で、安全管理措置を講じます。日本国外での取扱いが生じる機能及び国は、別紙 1 に記載します。

4. 当社が日本国外にある事業者を再委託先とする場合、当社は、当該再委託先との契約により、日本の個人情報保護法が求める水準の保護措置を講じさせ、その実施状況及び所在国の制度の変化を定期的に確認します。

5. 当社は、顧客の求めに応じ、顧客が本人への説明及び安全管理措置の公表に用いるため、次の情報を提供します。

(1) 顧客個人データを取り扱う国の名称

(2) 当該国の個人情報の保護に関する制度の概要

(3) 当社及び再委託先が講じている措置の内容

6. 顧客は、日本国外の法令（EU 一般データ保護規則を含みます。）の適用を受ける個人データを本サービスで取り扱おうとする場合、事前に当社に通知するものとし、当社および顧客は、その取扱いの可否および必要となる追加の条件について別途協議します。当該条件について書面による合意がない限り、当社は、日本国外の法令に基づく義務を負いません。

第 13 条（データ返却、削除および保存例外）

1. 顧客は、契約期間中、本サービスの標準機能を用いて顧客個人データを取得または削除できます。顧客は、契約終了日までに必要な顧客個人データを取得するものとし、契約終了日をもって顧客のアクセスは停止します。契約終了後 30 日間、当社は顧客個人データを通常の稼働領域に保管し、顧客から書面による要請があった場合は、利用規約第 27 条（契約終了時のデータ取扱い）第 3 項に従い提供します。パイプライン定義、設定情報、実行ロジックおよび内部表現の出力は、注文書またはドキュメントで明示されない限り返却対象に含みません。

2. 前項の期間終了後、当社は顧客個人データを通常の稼働領域から速やかに削除し、バックアップまたは災害復旧用複製に残存する顧客個人データを契約終了後 60 日以内に削除または上書きします。当該期間中、バックアップ内の顧客個人データを復旧およびセキュリティ目的以外に使用しません。

3. 法令、裁判所・公的機関の命令、監査または紛争対応のため保存が必要な場合、当社は必要な範囲および期間に限り当該データを隔離して保存し、当該目的以外に使用しません。当社は、削除処理を実行するたびに、対象テナントの識別子、削除した範囲（データベース上のレコードおよびオブジェクトストレージ上のオブジェクトの別を含みます。）、削除件数、実行日時および実行結果を削除実行ログとして記録します。削除証明書は、顧客から合理的な要請があった場合、当該削除実行ログに基づき提供します。

第 14 条（情報提供および監査）

1. 当社は、顧客が委託先監督または本 DPA への適合性を合理的に確認できるよう、秘密保持義務の下で、当社が保有し提供可能なセキュリティ概要、セキュリティ技術仕様書、質問票回答、第三者認証・監査報告書その他の資料を提供します。当社が取得していない認証または報告書の作成を約束するものではありません。

2. 前項の資料だけでは適用データ保護法令上必要な確認を合理的に満たせない場合、顧客は原則として年 1 回、30 日前までに書面で追加監査を要請できます。当事者は、対象サービスに直接関係する範囲、時期、期間、方法、秘密保持、他の顧客および当社のセキュリティへの影響防止について事前に合意します。

3. 監査は、可能な限り遠隔資料確認または独立第三者の報告書で行い、立入監査は法令上必要で代替手段がない場合に限ります。監査費用は、当社の重大な本 DPA 違反が確認された場合を除き、顧客が負担します。顧客または監査人は、当社の事前の書面承諾なく、ソースコード、他の顧客の情報、脆弱性診断またはペネトレーションテストを要求・実施できません。

第 15 条（変更、期間および存続）

1. 本 DPA は効力発生日に発効し、当社が顧客個人データを取り扱う間、適用されます。当社は、法令、サービスまたはセキュリティ上の必要に応じて本 DPA（別紙を含みます。）を変更できますが、契約期間中、顧客データのプライバシーまたはセキュリティの保護水準を実質的に低下させる変更を行いません。同等以上の措置への置換えは、保護水準の低下に当たりません。変更の通知および適用時期は、利用規約第 34 条（本規約等の変更）に従います。

2. 秘密保持、漏えい等への対応、法令上必要な協力、削除、監査資料の秘密性、責任制限その他性質上存続すべき条項は、原契約終了後も必要な範囲で存続します。

第 16 条（責任、損害賠償および保険）

1. 漏えい等または本 DPA 違反が発生したことだけで、当社の損害賠償義務が当然に生じるものではありません。当該義務は、当社の契約違反または帰責事由、因果関係、現実に生じた直接かつ通常の損害および適用法令に基づき判断されます。

2. 本 DPA に起因または関連する各当事者およびその関係会社の責任は、全ての請求を合算し、利用規約第 32 条（損害賠償）の損害範囲、責任上限および例外に従います。二重の回収は認められません。

3. 当社が加入するサイバー保険または IT 賠償責任保険は、当社の損失を補填するためのものであり、顧客が保険会社へ直接請求できること、保険金が必ず支払われること、または本条の責任上限を拡張することを意味しません。

第 17 条（連絡先）

1. 顧客個人データに関する問合せ及び漏えい等の連絡は、当社所定の窓口に対して行うものとします。当社は、窓口を管理画面又は当社ウェブサイトで案内します。漏えい等の連絡は、SLA に定めるサポート受付時間外においても受け付けます。

2. 顧客は、本 DPA に基づく当社からの通知（漏えい等の通知及び再委託先の変更の通知を含みます。）を受領する連絡先を、注文書又は管理画面で指定し、変更があった場合は速やかに更新します。

3. 再委託先一覧及びその変更は、当社ウェブサイトに掲載します。

4. 本契約の解除その他本契約に関する重要な通知は、利用規約第 38 条（通知）に従います。

別紙 1（データ処理の詳細）

本別紙は、顧客個人データの取扱い内容を特定するものです。注文書に異なる内容を明示した場合、当該注文書の記載が優先します。

項目	内容
処理の対象	顧客が W3 DataPlatform へ送信し、保存し、または本サービスを通じて処理する顧客個人データ。
目的	本サービスの提供、ETL／データ処理、保存、出力、運用、保守、サポート、障害対応およびセキュリティ確保。広告、販売または AI モデルの学習には使用しない。
処理の性質	取得、記録、整理、保存、変換、検索、参照、送信、出力、バックアップ、復旧、制限および削除。認定ユーザーが設定・実行した処理を含む。
頻度・期間	認定ユーザーの操作および設定に応じ継続的または随時。原契約期間および第 13 条（データ返却、削除および保存例外）の返却・削除期間。
本人の区分	[要選択・追記：顧客の従業員／役職員、取引先担当者、顧客・利用者、仕入先、業務委託先、その他]
個人データの項目	[要選択・追記：氏名、所属、連絡先、顧客 ID、IP アドレス、端末・アクセス・操作ログ、業務データに含まれる個人情報、その他]
特に保護を要するデータ	原則として対象外。要配慮個人情報、マイナンバー、カード会員データ、認証用秘密情報、医療・遺伝・生体情報、児童に関する情報等は、事前の書面承諾および追加条件がある場合のみ。
標準ホスティング場所	AWS アジアパシフィック（東京）リージョン／日本
AI コード生成	Amazon Bedrock の米国リージョンで、指示文、編集中コード、列名・型等のスキーマ情報を処理。行データは自動送信しないが、ユーザー入力に含まれる情報は送信される。
MCP	外部 AI クライアントからの MCP 接続は、Amazon Bedrock AgentCore（［要確認：リージョン］）を経由し、顧客が実行を指示したクエリ結果（行データを含みます。）が当該リージョンを経由して顧客の指定する外部 AI クライアントへ返却される。読み取り専用、所属テナント・グループの範囲に限定。
顧客の役割	[要選択：委託元／第三者から委託を受けた者]
当社の役割	委託先（顧客が第三者から委託を受けている場合は再委託先）。

AI・外部連携に関する補足

1. 顧客が MCP その他の機能を通じて外部 AI クライアントへクエリ結果を送信する場合、当該外部 AI クライアントは顧客が選定・管理するシステムであり、当社が契約する再委託先でない限り別紙 2 には含みません。
2. 顧客は、AI 機能へ入力する情報から不要な個人データを除外し、必要に応じて仮名化またはマスキングします。
3. 案件固有の処理国、データ分類、保持期間または追加の法令要件がある場合は、注文書で明示します。

別紙 2（再委託先）

次の一覧は、本 DPA の効力発生日時点の主要な再委託先です。

再委託先	目的・対象機能	主な処理場所	備考
アマゾン ウェブ サービス ジャパン合同会社	クラウド基盤、ホスティング、保存、認証、ログ、バックアップ、通知等	日本（東京リージョン）	契約上のデータ保護条件に従う。
アマゾン ウェブ サービス ジャパン合同会社（Amazon Bedrock）	AI コード生成の推論処理	米国	指示文、編集中コード、スキーマ情報。行データは自動送信しない。入力を基盤モデル学習に使用しない条件で利用。
アマゾン ウェブ サービス ジャパン合同会社（Amazon Bedrock AgentCore）	外部 AI クライアントからの MCP 接続の受付、認証および中継	［要確認：リージョン］	MCP クエリ結果（行データを含む）。トークンを検証し、テナント・グループの範囲に限定。
[要入力：その他の事業者]	[目的・対象機能]	[国・地域]	[対象データ]

変更通知と異議手続

4. 再委託先一覧および変更内容：当社ウェブサイトに掲載します（第 17 条（連絡先）第 3 項）。
5. 通知期間：処理開始の 30 日前まで（緊急時を除く）
6. 異議申立期間：通知受領後 10 日以内
7. 異議申立先：当社所定の窓口（第 17 条（連絡先）第 1 項）

別紙 3（データセキュリティ措置）

本別紙は、当社が顧客データ（顧客個人データを含みます。以下本別紙において同じ。）を保護するために維持する最低限の安全管理措置、当事者間の責任分界、セキュリティインシデントへの対応および確認資料の取扱いを定めます。利用規約第 17 条（安全管理措置及びセキュリティ事故）第 1 項により、本別紙は顧客個人データ以外の顧客データにも適用されます。無償トライアルには、無償トライアル利用規約第 9 条（個人情報の取扱い）に定める範囲で準用されます。

1. 基本方針

(1) 当社は、取り扱う顧客データの性質およびリスクを考慮し、多層防御および最小権限の考え方に基づき、組織的、人的、物理的および技術的な安全管理措置を講じます。

(2) セキュリティ概要、セキュリティ技術仕様書その他の説明資料は、本別紙に定める措置の実装内容を説明するものであり、契約上の義務を追加するものではありません。

(3) 当社は、全てのセキュリティ事故を完全に防止することを保証するものではありません。ただし、事故原因が外部攻撃であることのみを理由として、本 DPA 上の義務を免れるものではありません。

2. 組織的・人的措置

(1) 当社は、顧客データへアクセスできる者を、本サービスの提供、運用、保守、障害対応およびセキュリティ確保に必要な者に限定し、職務に必要な範囲の権限のみを付与します。

(2) 当社は、当該者に秘密保持義務を課し、顧客データの取扱いに関する教育および監督を行います。

3. 認証およびアクセス制御

(1) 当社は、OAuth 2.0／OIDC に準拠した認証基盤、招待制のアカウント登録および役割に基づくアクセス制御（RBAC）を提供します。

(2) 当社は、テナントおよびグループの単位で顧客データへのアクセスを分離し、アプリケーション側の認可とクラウド基盤側の権限境界の二重の制御を維持します。

(3) ストレージへのアクセスには、対象領域に限定された短時間で失効する一時認証情報を用います。

4. 暗号化および秘密情報の管理

(1) 当社は、通信経路を TLS で保護し、オブジェクトストレージおよびデータベースに保存する顧客データを保存時に暗号化します。

(2) 当社は、プラットフォームの秘密情報を専用の秘密情報管理サービスで管理し、顧客が入力した接続用認証情報を分離された暗号化領域に保存し、画面および API 上で表示しません。

5. ネットワークおよび基盤

(1) 当社は、仮想ネットワークを公開領域と非公開領域に分離し、データベースをインターネットから直接到達できない領域に配置します。

(2) 当社は、WAF、セキュリティグループその他の手段により、必要な通信のみを許可します。

(3) 当社は、開発・検証・本番の各環境を分離して運用します。

6. 開発および脆弱性対応

(1) 当社は、入力検証、パラメータ化クエリその他の安全な開発手法を採用し、コンテナイメージの脆弱性スキャンを実施します。

(2) 当社は、本サービスに影響する重大な脆弱性を認識した場合、リスクに応じて合理的な期間内に是正または緩和措置を講じます。

7. ログおよび監視

(1) 当社は、アクセスログおよび実行ログを集約して保管します。保持期間は、標準で 30 日（一部の運用ログは 14 日）とします。

(2) 当社は、アプリケーションログに顧客データのレコード内容を出力しない方針で運用します。

8. バックアップ

(1) 当社は、本番データベースについて冗長化、削除保護および自動バックアップ（30 日保持）を、オブジェクトストレージについてバージョニング（旧版 30 日保持）を維持します。

(2) バックアップは当社の復旧およびセキュリティ確保のために維持するものであり、顧客は利用規約に従い、元データおよび必要なバックアップを自ら保持します。RTO および RPO は、注文書で合意した場合を除き保証しません。

9. AI 機能および外部連携

(1) AI コード生成機能へ送信される情報は、ユーザーの指示文、編集中のコードおよび入力データの列名・型に限られ、行データは自動送信しません。当社は、顧客データを AI モデル（当社または第三者が提供するものを問いません。）の学習に使用しません。

(2) 外部 AI クライアントからの MCP 接続は、所属テナント・グループの範囲に限定した読み取り専用とし、実行できる処理、返却行数および実行時間に制限を設けます。

(3) 顧客が選定する外部 AI クライアントへ返却されたデータの取扱いは、顧客の責任とします。

10. 責任分界

当社、クラウド基盤事業者および顧客の責任分担は、次の表のとおりとします。

項目	クラウド基盤	当社	顧客
データセンター・物理セキュリティ	●		
クラウド基盤（ハードウェア・ネットワーク）	●		
マネージドサービスの運用（OS パッチ等）	●	○	
本サービスの実装・脆弱性対応		●	
テナント分離・アクセス制御の仕組み		●	

項目	クラウド基盤	当社	顧客
ユーザーアカウントの発行・権限設定・棚卸し		○	●
接続先システムの認証情報の発行・管理		○（保管）	●（発行・更新）
取り込むデータの内容・適法性			●
AI／MCP クライアントの選定と利用範囲の管理		○（制御機能の提供）	●（利用判断）

●：主たる責任　○：分担・支援

11. セキュリティインシデントへの対応

(1) 当社は、監視、ログまたは顧客その他からの連絡によりセキュリティインシデントを検知した場合、アクセス遮断、認証情報の無効化その他の初動措置を講じ、原因、期間、対象および影響を合理的に調査します。

(2) 当社は、原因がバグ、設定誤り、内部行為または外部攻撃のいずれであるかを問わず、顧客データへの影響またはそのおそれを確認した場合、速やかに顧客へ通知します。顧客個人データに関する通知および協力は、本 DPA 第 7 条（漏えい等の通知および対応）に従います。

(3) 当社は、安全を確認した上で復旧し、是正措置および再発防止策を講じます。

12. 顧客データの削除および削除証明

契約終了時の顧客データの返却、削除、削除実行ログの記録および顧客の要請に応じた削除証明書の交付は、本 DPA 第 13 条（データ返却、削除および保存例外）および利用規約第 27 条（契約終了時のデータ取扱い）に従います。

13. 再委託先の管理

当社は、顧客データを取り扱う再委託先に対し、本別紙と実質的に同等以上の安全管理措置を契約により求めます。再委託先の一覧および変更手続は、本 DPA 第 10 条（再委託）に従います。

14. 確認資料および検査

(1) 確認資料の提供および監査は、本 DPA 第 14 条（情報提供および監査）に従います。

(2) 顧客は、当社の事前の書面による承諾なく、脆弱性診断、ペネトレーションテストまたは負荷試験を実施できません。

15. 標準提供外の措置

多要素認証（MFA）、外部機関による脆弱性診断および閉域接続（VPN、AWS PrivateLink 等）は、現時点で標準提供していないため、本別紙の義務に含みません。将来の計画項目は、実装され本別紙に明示されるまで本別紙の義務に含みません。

以上