Onsites AI

SECURITY WHITEPAPER · EDITION 2.0

セキュリティとデータレジデンシー白書

データが誰の手にあるか、明記する

暗号化、アクセス制御、監査、バックアップと削除の時期、AI のデータ境界、脆弱性の報告。項目ごとに実施方法と責任の所在を明記します。「エンタープライズ級のセキュリティ」のような検証できない形容詞は書きません。



版	発行	対象範囲	文書番号
第2.0版	2026年11月	クラウド・専用クラウド・セルフホスト	ONS-SC-JA-2.0

© 2026 Onsites AI · 本資料は製品の改訂に合わせて更新します。最新版は onsitesai.com/jp/download.html をご参照ください。

目次

CONTENTS

01 **処理の役割とデータ境界** 誰が管理し、誰が処理し、AI は何を見るか 03

02 **暗号化、アクセス制御、監査** 9つの制御項目の具体的な実施方法 04

03 **レジデンシー、バックアップ、ライフサイクル** データの保管場所、保持期間、削除の方法 05

04 **セキュリティ質問票と報告フロー** よくある質問、脆弱性の報告、連絡先 06

要旨

Onsites AI は、お客様のデータをお客様からお預かりした資産として扱います。クラウドとセルフホストのいずれも暗号化、アクセス制御、監査ログを備え、セルフホストを選べばすべてのデータを自社ネットワーク内に留められます。本書は9つの制御項目の実施方法を項目ごとに示し、当社が担う範囲とお客様が担う範囲を明記します。セキュリティ評価で最も困るのは「脆弱性があること」ではなく、「境界が説明できないこと」です。

9項目	TLS 1.3	1 営業日	3形態
標準搭載の制御項目 質問票に1項目ずつ対応	全通信を暗号化 保存データも暗号化	セキュリティ報告の 受領確認までの期限	クラウドと専用、 セルフホストの境界

9つの制御項目一覧

01 通信
TLS 1.3

02 保存
記憶媒体を暗号化

03 鍵
データと分けて保管

04 権限
シート単位で付与、参照のみ可

05 分離
ワークスペース間は不可視

06 共有
外部リンクに期限と回数

07 監査
実行者、日時、内容

08 バックアップ
有償は自動、書き出し可

09 AI 境界
自ワークスペースのみ参照

文書の用途

セキュリティ評価、ベンダー質問票、コンプライアンス審査に使用できます。回答の添付資料としてそのまま提出できます。

対象範囲

クラウド SaaS、商用版・専用クラウド、セルフホストの3形態。相違点は個別に記載しています。

免責

本書は製品に標準搭載された機能を述べるもので、第三者認証と同等ではありません。業界固有の規制対応や適合性評価は別途ご依頼ください。

版とご意見

第2.0版、2026年11月。誤りのご指摘とセキュリティ報告は support@onsitesai.com までお送りください。

01

ROLES & BOUNDARY

誰が管理し、誰が処理し、AI は何を見るか

セキュリティ評価で最初に問われるのは役割です。データは誰のものか、誰が処理し、処理の過程で第三者に渡らないか。データ管理者はお客様、処理者は当社、再処理者は基盤とモデルの2種類です。

1.1 3つの役割

データ管理者

お客様（貴社）

収集する情報、保存期間、開示先を決めるのは貴社です。シート、ロール、権限の設定も、書き出しと削除も貴社が行います。

データ処理者

Onsites AI

貴社の設定に従い、保存、検索、下書きや書類の生成を担います。当社の目的に使うことはせず、横断的な再利用もありません。

再処理者

基盤とモデル

クラウドではクラウド基盤と当社が呼び出すモデル、セルフホストではこの2つを貴社が用意し、当社は保持しません。

1.2 AI 呼び出し1回の4つの境界点

境界内

ワークスペース内

会話、顧客、書類、ファイル。本ワークスペースのメンバーのみが権限内で閲覧します。

検索時

権限フィルタ

実行者のシート権限で範囲を絞り、権限外の記録はコンテキストに載せません。

推論時

モデル呼び出し

必要な最小限のコンテキストのみ送信。セルフホストは社内端点を指定可。

返却後

回答と出典

結果に参照元の記録を表示。学習データへの書き込みなし、横断的な再利用もなし。

図 1-1　4つの境界点。どこか1つでも欠ければ、データをモデルに渡すべきではありません。当社が自ワークスペースのみを参照し、全回答に出典の表示を求めるのはこのためです。

1.3 AI 利用の4つの境界

- **自ワークスペースのみ参照。**Copilot、Harness、Agent Studio、Desk は3形態のいずれでも現在のワークスペースのデータのみを読み取り、横断検索は行いません。
- **回答には出典を付与。**各回答はどの会話、どの顧客項目、どのファイルを参照したかを示し、事後の検証を可能にします。出典を示せない内容は回答に含めません。
- **学習には使用しない。**お客様のデータを共有モデルや公開モデルの学習に使いません。セルフホストではモデルと鍵をすべて貴社が用意し、既定で社内ネットワークから出ません。
- **まとめて無効化できる。**AI 機能はワークスペース単位またはメンバー単位で停止でき、停止後も他の機能は通常どおり動作し、機能制限状態にはなりません。

1.4 3形態による役割の違い

区分	クラウド / 専用クラウド	セルフホスト
基盤	当社が運用。専用は占有	貴社の機器とネットワーク
モデルと鍵	一括呼び出し、鍵は当社	貴社が用意、当社は不保持
データの所在	Onsites 基盤、専用は任意	貴社のデータセンター、オフライン可

同じソフトウェア、同じ機能です。役割分担の違いは「誰が基盤とモデルを用意するか」だけに由来します。

「当社から見えるか」について　クラウドでは障害対応のため運用担当者がマスキング済みのログに触れることがあります。会話本文と添付は日常運用の対象外です。許容できない場合、セルフホストがより徹底しています。

02

CONTROLS

9つの制御項目と実施方法

セキュリティ質問票は通常、制御項目ごとに問われます。以下「暗号化 → アクセス → 記録 → 共有 → AI」の順に実施方法と責任主体を示します。そのまま照合でき、3形態の相違点は個別に記載します。

2.1 暗号化と鍵

区分	実施方法	責任主体
通信	全通信 TLS 1.3。セルフホストは貴社側で終端し、証明書も貴社が管理	クラウドは当社、セルフホストは貴社
保存データ	当社基盤上で保存時に暗号化。セルフホストはディスク暗号化を貴社 OS とストレージ層で実施	クラウドは当社、セルフホストは貴社
鍵の管理	鍵とデータは別々に保管。アクセスはプラットフォームチームのみ	クラウドは当社、セルフホストは貴社が保有
バックアップ媒体	複製ファイルも同じく暗号化。保存先は形態により異なる	第3章を参照

2.2 アクセス制御

- **シート単位で付与。**閲覧範囲はシートとロールで決まり、参照のみにも絞れます。
- **ワークスペースを分離。**相互に不可視でデータも移動せず、AI の検索も制限されます。
- **剥奪は即時反映。**シートを削除すると同時にアクセス権も失効し、追加操作は不要です。
- **共有の制御。**外部リンクは有効期限と開封回数の上限を設定でき、いつでも無効化できます。

2.3 監査と追跡可能性

文書と会話の状態変更には実行者、日時、内容を記録します。誰が見積書を送り、誰が金額を変え、誰が契約を確定したか。ログはデータと共に書き出せ、数か月後も承認の根拠になります。一定期間だけ残る活動ログではありません。Desk の実行も記録し、読取・書込・ポイント消費まで残します。

記録項目	内容	用途
状態変更	書類と会話の状態遷移	承認経路の確認、「この版は誰が送ったか」
権限変更	ロールとシートの付与	退職時の引き継ぎ、監査の証跡
AI の実行	読取、書込、消費ポイント	エージェントが範囲を越えていないか

2.4 制御項目は経路のどこに効くか

入口
ID とシート
ログイン、ロールとシート付与。削除でアクセス権も失効、ワークスペース間は不可視。

通信
TLS 1.3
ブラウザーとアプリ間を常時暗号化。セルフホストは貴社ゲートウェイで TLS を終端。

アプリ
権限フィルタと監査
読み書きのたびに権限で絞り、実行者、日時、内容を記録。AI の検索も同様に制限。

ストレージ
保存データの暗号化と複製
媒体を暗号化し鍵を分離。複製も暗号化され、保持ポリシーに従って失効します。

図 2-1　制御項目の経路ごとの分布。評価では機能一覧で問うより、この4段に分けて順に確認するほうが抜けを見つけやすくなります。

検証のしかた　評価段階では、上記3項目についてマスキング済みの実サンプルを1件ずつ求めることができます。状態変更1件、権限変更1件、AI 実行記録1件です。サンプルを示せることは、質問票に「はい」と記す以上の説得力を持ちます。

03

RESIDENCY

どこに置き、いつまで残し、どう削除するか

レジデンシーの論点は3つに分かれます。データをどこに置くか、複製をいつまで保持するか、契約終了後にどう削除するか。前2つは形態で選べ、3つ目は書き出しの有無で決まります。

3.1 データ1件のライフサイクル



図 3-1　ライフサイクルの4段階。事前に取り決めるべきは最後の段階です。誰が削除を起動し、複製をいつまで保持し、削除済みをどう確認するか。

3.2 3形態のレジデンシーとバックアップ

形態	データの所在	バックアップ	削除
クラウド SaaS	Onsites の基盤	有償は自動バックアップ	要求どおり実行、複製は保持期間で失効
専用クラウド	選択制、開通時に固定	自動、リージョンは同一	同上、リージョンは不変
セルフホスト	貴社のデータセンター	付属スクリプトで実行	貴社が実行、手順は当社提供

リージョンは開通時に固定され、後から変わりません。移す場合は新規インスタンスへの移行として扱います。

3.3 書き出し、プラン変更、保持

- **書き出しは権利であり、機能のスイッチではありません。**会話、連絡先、文書をすべて標準形式で書き出せます。形式の囲い込みも、書き出しの課金もありません。
- **プラン変更でデータは消えません。**停止や変更の後も保存済みデータは保持され、再開できます。
- **無償版にサーバー側の複製はありません。**定期の書き出しが唯一の複製です。見落とされやすい点です。
- **削除は確認できる形で。**実行記録と複製の失効時期を提供し、「削除したのに残る」争いを避けます。

3.4 保持ポリシーの決め方

データの種類	推奨保持	理由
会話と顧客	業務と同じ周期	サポートも再購入の判断も過去の会話に依存。早すぎる整理は文脈を失わせます。
見積・契約・請求	税務・会計の要件	通常は会話より長く、番号と金額の検証に旧版も要ります。
監査ログ	書類本体より長く	承認や紛争対応には「誰がいつ何を変えたか」が必要です。
バックアップの複製	主データより短く	復旧のためだけのもの。期限が来たら失効させ、削除の争いを避けます。

以上は一般的な推奨です。実際の保持期間は、貴社が属する業界の規制要件に従ってください。

契約に明記したい3つの期間　① 書き出し可能な日数（終了後いつまで取り出せるか）、② 複製の保持期間、③ 削除完了後の書面確認までの期限。この3つの数字を明確にするほうが、質問票に丸を付けるより有用です。

04

QUESTIONNAIRE

セキュリティ質問票の早見と脆弱性の報告

以下はベンダー質問票で頻出する項目です。回答はそのまま引用できます。細かい点はお気軽にお問い合わせください。貴社の様式に沿って1項目ずつ記入し、汎用の宣伝資料をお返しすることはありません。

4.1 よくある質問

質問	回答
学習へのデータ利用	いいえ。AI は自ワークスペースのデータのみ参照し、共有・公開モデルの学習には使いません。
保存リージョンの指定	商用版 · 専用クラウドは選択制、開通時に固定。クラウドは標準、セルフホストは任意です。
当社による会話内容の閲覧	クラウドでは障害対応でマスキング済みログに触れることがあります。本文と添付は対象外です。
監査ログの有無と書き出し	あります。状態変更、権限変更、AI 実行の実行者・日時・内容を記録し、データと共に書き出せます。
外部リンクの制限と無効化	できます。有効期限と開封回数の上限を設定でき、いつでも無効化できます。
契約終了後のデータの扱い	標準形式で書き出せます。削除は所定の手順で実行し、実行記録と複製の失効時期を提供します。
AI 利用量の上限設定	できます。既定はソフトリミット（上限が近づくと通知、停止はしない）で、ハードリミットも選べます。
オフラインでの更新	できます。新版はオフラインパッケージで提供し、取り込み後に案内に従って更新します。

4.2 脆弱性の報告

STEP 01

報告

support@onsitesai.com へ。該当製品の開発チームに直接届きます。

STEP 02

受領確認

1営業日以内に受領をお知らせし、初期的な判断と担当者をお伝えします。

STEP 03

修正

影響度で優先順位を付け、修正を計画。期間中も進捗を共有し、公開まで待ちません。

STEP 04

振り返り

修正公開後に結論を共有。貴社側の対応が必要なら手順をお示しします。

図 4-1　報告の流れ。当社は報奨金制度を設けていませんが、匿名を希望される場合を除き、報告者への謝意を表明します。

4.3 追加の資料が必要な場合

評価に特定様式の質問票記入、ペネトレーションテスト報告、セルフホスト環境の構成確認書が必要な場合は、様式と締め切りをお知らせください。セルフホストのお客様は、社内のセキュリティ審査に備えて構成確認書もご依頼いただけます。

4.4 関連文書

文書	文書番号	用途
製品ガイド	ONS-PM-JA-2.0	製品の構成、機能範囲、形態、価格体系（21ページ）。
セルフホスト導入ガイド	ONS-SH-JA-2.0	適する場面、構成、リソース、費用（6ページ）。
セキュリティとデータレジデンシー白書	**ONS-SC-JA-2.0**	本資料。質問票とコンプライアンス審査に用います（6ページ）。

3つの文書はいずれも onsitesai.com/jp/download.html から無償でダウンロードできます。フォームの記入は不要です。

連絡先　セキュリティとコンプライアンス：support@onsitesai.com（報告も同じアドレス、1営業日以内に受領確認）
製品とドキュメント：onsitesai.com/jp/download.html　·　セルフホスト評価：onsitesai.com/jp/self-host.html