セキュリティホワイトペーパー

Orcado セキュリティホワイトペーパー

本書は、Orcado がお客様のデータをどのように守っているかをご説明するものです。ここに書くのは仕組みと方針で、攻撃の手がかりになる細部は書きません。使っている部品（フレームワーク・ライブラリ）の名前と版、第三者の評価の報告書などは、秘密保持契約（NDA）を結んだうえでお渡しします。

第 1.0 版 ／ 2026 年 11 月 7 日 ／ 株式会社Orcado ／ PDF をダウンロード

1　お客様との責任分界点

株式会社Orcadoの責任

当社は、以下のセキュリティ対策を実施します。

Orcado アプリケーションのセキュリティ対策

Orcado に保管されたお客様のデータの保護

Orcado の提供に使うクラウド基盤（ネットワーク・データベース・鍵の管理など）の設定と運用。建物や機器などの物理的な対策は、クラウド事業者が担います

お客様の責任

お客様は、以下のセキュリティ対策を実施する必要があります。

各利用者のパスワード、およびログインに使う Google・Microsoft アカウントの適切な管理（そちらの多要素認証の設定を含む）

Orcado のアカウントの適切な管理（招待、利用の停止、役割の付与など。退職者の停止を含む）

Orcado に接続するサービスの許可と、取り込む範囲の設定

取り込んだ情報と、AI が作った内容の確認と管理（AI の出力を社外に送る前の確認を含む）

2　データ保管場所

お客様からお預かりしたデータは、日本国内（東京）のクラウドに保管されます。

AI による要約・整理だけは、米国の AI 事業者で処理します。詳しくは「20　外部クラウドサービスの利用」をご覧ください。

3　データの削除

Orcado の契約が終了した場合、終了日から 30 日間はデータの書き出しをご依頼いただけます。その後、目安として終了日から 90 日以内に、お客様からお預かりしたデータを復元できない形で削除します。
削除の対象には、取り込んだデータと、AI が作った要約などの生成データを含みます。詳しい範囲は、ご契約の際にお渡しするデータ取扱い別紙に定めます。
削除は、会社ごとの暗号の鍵を破棄して、残った暗号文も読めない状態にする方法（暗号消去）で行います。鍵の破棄で読めなくならないものは、別に消去します。
ご希望があれば、削除を実施したことを当社の様式でお知らせします。
ご契約中でも、当社所定の方法で削除をご依頼いただけます。なお、接続を解除したり取り込む期間を短くしたりしても、それまでに取り込んだデータは自動では消えません。

4　ラベル付け機能

お客様は、チーム・ワークフロー・お客様が作る役割に、任意の名称を付けて識別できます。

5　利用者登録および削除

お客様の管理者は、契約の範囲内で、いつでも利用者を招待し、利用を停止できます。
招待のリンクは 7 日で切れます。
利用を停止した人は、次の操作から Orcado を使えなくなります。

6　アクセス権の管理

お客様は、Orcado が標準で用意する権限に加えて独自の権限を作り、利用者ごとに見られる範囲と操作を分けられます。
役割の変更は、次の操作からすぐに反映されます。
最後のオーナーを外すことはできません。

7　パスワードの配布方法と本人確認

ログインの方法は、メールアドレスとパスワード、Google のアカウント、Microsoft の職場・学校アカウントの 3 つです。招待された人だけがログインできます。
Google・Microsoft のアカウントでログインする場合、パスワードは Orcado には渡りません。お客様がそちらに設定している多要素認証やアクセスの制限がそのまま効きます。
管理者が仮のパスワードを発行した場合、仮のパスワードは 24 時間で切れます。仮のパスワードのままでは使い始められず、最初に本人が変更する必要があります。

パスワードを 5 回間違えると、しばらくログインできなくなります。失敗が続くほど、待つ時間が長くなります（最長 1 時間）。
ログインは最長 24 時間で切れます。ログアウトやパスワードの変更をすると、他の端末のログインも無効になります。
当社の運営スタッフのログインには、確認コード（TOTP）を必須にしています。

8　暗号化の状況

データベースに保存されるお客様のデータは、クラウド事業者の仕組みにより、バックアップを含めてディスク上で暗号化されます（AES 256 ビット）。この暗号化は常に有効で、無効にできません。
外部サービスの接続の鍵など特に大事な情報は、会社ごとに分けた鍵で、アプリの側でもう一重に暗号化します（AES-256-GCM）。その鍵自体も専用の鍵管理サービスで暗号化しており、鍵の元はそのサービスの外に出ません。鍵管理サービスの鍵は 90 日ごとに自動で更新します。
お客様の端末と Orcado の間の通信は、TLS で暗号化されます。対応している TLS は TLSv1.2 以降で、安全な暗号の方式だけを使っています。外部の診断サービスで最上位の評価（A+）を確認しています。
暗号化しない通信に戻らないよう、ブラウザにも指示しています（HSTS）。
アプリとデータベースの間は、暗号化した接続だけを許しています。
パスワードは元に戻せない形（bcrypt）で保管します。当社の社員もパスワードを知ることはできません。

9　変更管理

業務のやり方に影響する機能の変更は、事前にご案内します。
保守点検でサービスを止めるときは、事前にお知らせします。
利用規約を変更するときは、効力が生じる日の 30 日前までに、ウェブサイトへの掲示と登録メールアドレスへの通知でお知らせします。データの取扱いの条件をお客様に不利に変えるときは、60 日前までにお知らせします。
当社からのご連絡は、ご登録のメールアドレスへの送信、または管理画面への掲示で行います。

10　手順書の提供

お客様が使う手順書（利用の手引き）は、ご契約時に所定の方法でご提供します。

11　バックアップの状況

データベースに保管される、お客様の各種情報は、毎日自動でバックアップを取得しています。バックアップは 7 日分保管されます。
さらに、直近 7 日間は任意の時点の状態に戻せます。
失われるデータは最大 5 分、復旧は 60 分以内を目標にしています（社内の目標です）。復旧の手順は実際に試して確かめています。
データベースと暗号の鍵には、誤って消せないように保護をかけています。

12　ログのクロックに関する情報

Orcado を動かすサーバーの時刻は、クラウド事業者の時刻サーバーと同期しています。
当社が保管するログの時刻は、協定世界時（UTC）で記録しています。画面に表示する時刻は日本時間です。

13　脆弱性管理に関する情報

当社は、システムで使っている部品（ライブラリなど）の弱点の情報を集めています。
弱点が公表されたときは、影響があるかを確かめ、必要なものは版を上げます。
外から攻撃を試す検査ツールで、本番の画面を検査しています。直近の検査（2026 年 10 月）では、危険度「高・中・低」の指摘は 0 件でした。
個別の弱点について影響があるかは、お問い合わせいただければお答えします。使っている部品の一覧や版は、攻撃の手がかりになるため公開していません。NDA を結んだうえでお渡しします。

14　開発におけるセキュリティ情報

変更のたびに、型の検査と自動テスト（会社ごとのデータの分離のテストを含む）を通らないと、本番に出せない仕組みにしています。
本番への反映は、責任者の承認を経て行います。
他のサイトに埋め込ませない、読み込める先を限る、などのブラウザ向けの安全の指示を出しています。
秘密の情報（鍵やパスワード）はプログラムに書かず、専用の秘密の管理サービスに置いています。使えるのは本番のアプリだけです。

15　インシデント発生時の対応

サービスの状態は外から定期的に確かめています。エラーの急増やデータベースの負荷、秘密の情報への想定外のアクセスなど、異常があれば担当者に自動で通知されます。

当社が情報の漏えい、またはそのおそれを知ったときは、速やかにお客様に通知します。調査中であることを理由に通知を遅らせず、分かったことを順に追加でご報告します。
セキュリティの事故に関するお問い合わせは、本書の末尾の窓口にご連絡ください。

16　お客様のデータの保護及び第三者提供について

Orcado は複数の会社が同じ仕組みを使うクラウドサービスです。他の会社のデータが見えることがないよう、データベースそのものが会社ごとに絞り込む仕組みにしています。「どの会社の操作か」の指定がない読み書きは、何も返しません。
アプリに不具合があっても、データベースの段階で他の会社のデータは返りません。この仕組みは、開発のたびに自動のテストで確かめています。
当社の運営スタッフ用の管理画面からも、お客様のメールや議事録の中身は読めません。障害の調査などで中身を見る必要があるときは、お客様の了解を得てから行います。
誰がいつ何をしたかを、書き換えできない形で記録しています。当社の運営スタッフの操作も記録します。パスワードや接続の鍵などは、ログに出さないようにしています。
お客様の外部サービスへの接続は、各サービスの標準の許可の仕組み（OAuth）で行い、お客様のパスワードを当社が預かることはありません。必要な分だけ許可をもらい、許可の画面から戻るときには毎回ちがう予測できない値を照合して、接続の横取りを防いでいます。
お客様のデータは、ご契約の目的以外に使わず、第三者に提供しません。ただし、法令に基づく開示を求められた場合は、必要な範囲で応じることがあります。

17　AI の利用とデータの扱い

お客様のデータを、当社や第三者の AI モデルの学習に使うことはありません。ここでいう学習には、追加学習・ファインチューニングなど、AI モデル自体を変えることすべてを含みます（データ取扱い別紙第 2 条）。
AI に送るのは、その処理に必要な分だけです。
AI の委託先は、送ったデータを学習に使わない契約条件で利用しています。

18　適用法令

お客様と株式会社Orcadoとの間の契約は、日本法に基づいて解釈されるものとします。

19　独立したレビュー

Google が定める、Google のデータを扱うアプリ向けのセキュリティ評価（CASA：Cloud Application Security Assessment）を、Google が認定した評価機関で受けています。評価では、認証・権限・暗号・ログなど 48 の要件を確かめます。
外から攻撃を試す検査ツールで、本番の画面を検査しています（「13　脆弱性管理に関する情報」）。

20　外部クラウドサービスの利用

Orcado の基盤には、大手クラウド事業者のサービスを使っています。特に記載がない限り、日本（東京）のリージョンを使います。
データベースはインターネットに直接つながっていません。当社のアプリだけが、クラウドの内部の通信で接続します。
外からの通信は、すべて 1 つの入口（ロードバランサー）を通ります。アプリに直接入る経路は塞いでいます。同じ接続元から短い時間に大量の要求が来たら遮断し、ログイン画面は特に厳しく制限しています。
一部の機能では、お客様のデータの処理に、以下の国外の事業者を使います。
AI による要約・整理：米国の AI 事業者で処理します。保管は国内です。送ったデータは学習に使われません（「17　AI の利用とデータの扱い」）。
会議の記録：記録の対象とした会議に限り、国外の事業者を使います。記録の取得と保管は日本（東京）のリージョンで行います。
委託先の名称は、秘密保持のもとで個別にお伝えします（データ取扱い別紙 第 3 条）。委託先を追加・変更するときは、事前にお知らせします。

21　物理的な機器の廃棄及び再利用時のセキュリティ

当社は自社でサーバーを持たず、Orcado の基盤にはクラウド事業者のサービスを使っています。
サーバーやディスクなどの機器は、クラウド事業者が管理しています。不要になった機器は、クラウド事業者が安全な方法で廃棄します。

よくあるご質問

Q. ニュースで見た「○○（プログラム言語や部品の名前）の弱点」の影響はありますか。何の技術で作っていますか。
A. 弱点が公表されたときは、当社で影響を確かめ、必要な対応をします。個別の弱点についてはお問い合わせいただければお答えします。使っている部品の一覧や版は、NDA を結んだうえでお渡しします。
Q. セキュリティチェックシートに答えてもらえますか。
A. はい。御社の様式でお送りください。委託先の名称などを含む回答は、秘密情報としてお渡しします。

改訂履歴

版	改訂日	改訂内容
0.1	2026-10-29	初版（ドラフト）
1.0	2026-11-07	公開版

この資料に関するお問い合わせ

株式会社Orcado　問い合わせ窓口：sales@orcado.ai