ノコリス for Business

セキュリティとネットワーク構成

社内でのご検討・稟議にお使いいただけるよう、ネットワーク構成、データの保存先、セキュリティ対策をまとめました。記載内容は2026年11月26日時点のものです。

保存先は東京

在庫・台帳情報と画像は、Google Cloudの東京リージョン（asia-northeast1）に保存します。

通信は暗号化

アプリ・ブラウザとサービスの通信は、すべてTLSで暗号化します。

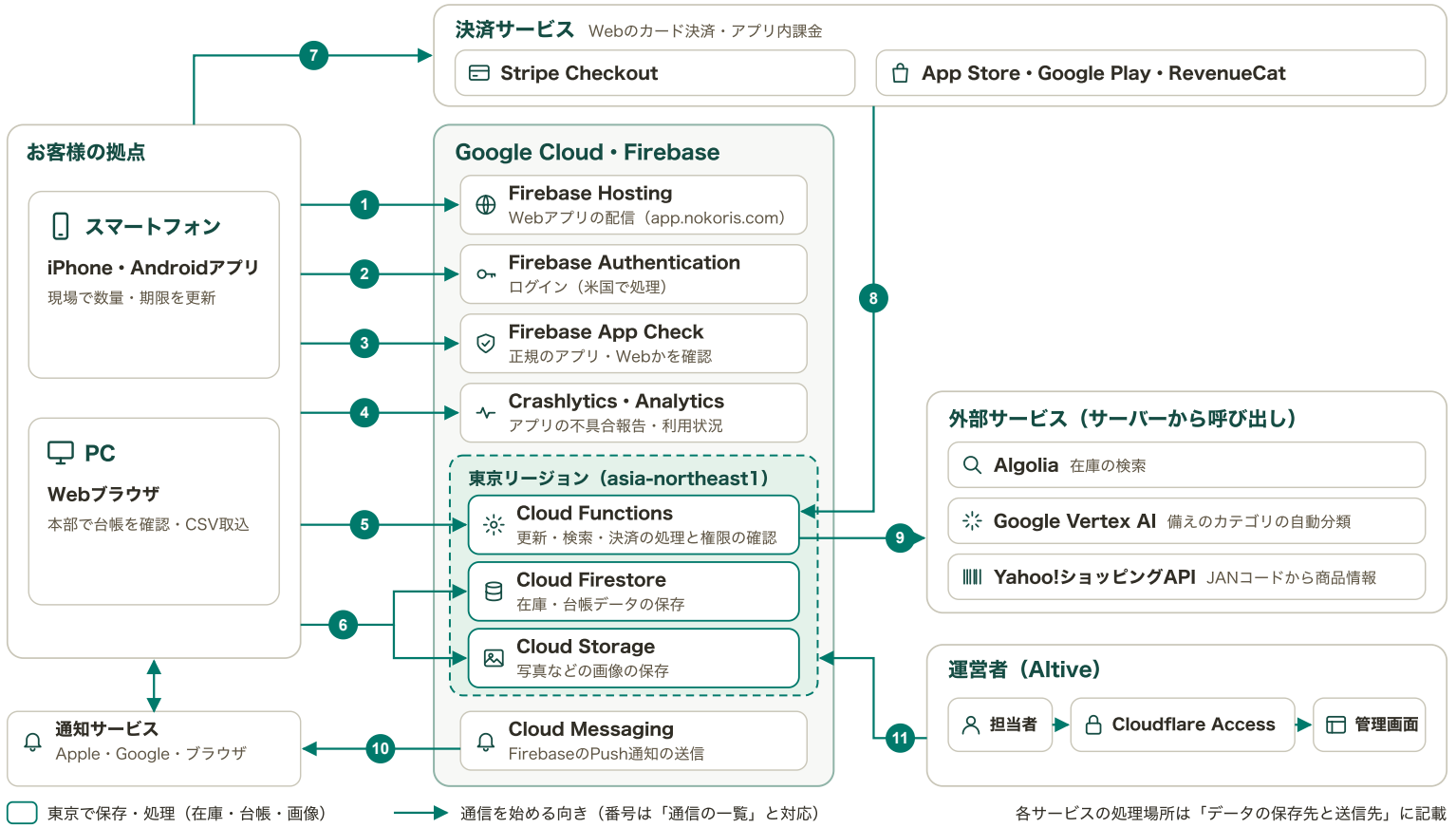
台帳はメンバーだけ

台帳を閲覧できるのは、招待されたメンバーだけです。権限はオーナー・管理者・メンバーの3段階です。

社内への設置は不要

クラウドサービスのため、社内ネットワークへの機器やサーバーの設置は不要です。

ネットワーク構成



通信はすべてインターネット経由で、TLSにより暗号化されます。VPN・専用線や社内への機器の設置は不要です。図を拡大して開く

通信の一覧：お客様の端末から

社内のプロキシやフィルタリングで通信先を制限している場合は、次の接続先を許可してください。いずれもHTTPS（443番ポート）です。

番号	通信	用途・送る情報	接続先
①	**PC → Firebase Hosting**	Webアプリの画面を読み込みます。	app.nokoris.com
②	**端末 → Firebase Authentication**	ログインします。メールアドレスやApple・GoogleのIDを扱い、米国で処理されます。	identitytoolkit.googleapis.com、securetoken.googleapis.com、re-stock.firebaseapp.com、appleid.apple.com、accounts.google.com
③	**端末 → Firebase App Check**	正規のアプリ・Webからの通信であることを確かめます。	firebaseappcheck.googleapis.com、www.google.com、www.gstatic.com
④	**アプリ → Crashlytics・Analytics**	不具合の記録（端末の機種、OS・アプリのバージョン、エラー）と利用状況を送ります。	firebase-settings.crashlytics.com、crashlyticsreports-pa.googleapis.com、app-measurement.com
⑤	**端末 → Cloud Functions（東京）**	在庫・台帳の作成・変更・削除、検索、決済の開始を行います。処理のたびにログインと権限を確かめます。	asia-northeast1-re-stock.cloudfunctions.net、*.run.app
⑥	**端末 → Cloud Firestore・Cloud Storage（東京）**	所属する台帳のデータを読み取り、写真を保存・表示します。商品画像とスタンプも表示します。	firestore.googleapis.com、firebasestorage.googleapis.com、storage.googleapis.com、*.yimg.jp、stickers.altive.co.jp
⑦	**端末 → 決済サービス**	Webのカード情報はStripeの画面で入力し、当社のサーバーを通りません。アプリはApp Store・Google Playで購入します。	checkout.stripe.com、billing.stripe.com、api.revenuecat.com

通信の一覧：サーバー・運営者から

⑧・⑨・⑪はお客様のネットワークを通りません。⑩は、スマートフォンでPush通知を受け取るための通信です。

番号	通信	用途・送る情報	接続先
⑧	**決済サービス → Cloud Functions**	決済・購入状態の変化を知らせます。署名や共有の秘密値を確かめて受け取ります。	サーバー間の通信
⑨	**Cloud Functions → 外部サービス**	検索（品名・保管場所・メモ・JANコード・期限など）、カテゴリの自動分類（商品名・JANコード）、商品情報の取得（JANコードのみ）に使います。	サーバー間の通信
⑩	**Cloud Messaging → 通知サービス ⇄ 端末**	Push通知を届けます。端末はAppleまたはGoogleの通知サービスへの接続を保ちます。	iPhone：TCP 5223番（Wi-Fiでは443番に切り替わる場合あり）、Android：TCP 5228〜5230番、Web：ブラウザの通知サービス
⑪	**運営者 → 管理画面 → 基盤**	当社の担当者がサポートや請求の操作を行います。Cloudflare AccessとGoogleアカウントの二段階で認証し、権限を付与した担当者だけが利用します。	お客様のネットワークは通りません

データの保存先と送信先

データ	保存・処理するサービス	場所
在庫・台帳・点検・買い物リスト・タイムライン	Cloud Firestore	東京（asia-northeast1）
写真などの画像	Cloud Storage	東京（asia-northeast1）
ログイン情報（メールアドレス、Apple・GoogleのID、パスワード）	Firebase Authentication（パスワードは復元できない形で管理し、当社は保存しません）	米国
カード情報	Stripe（当社は完全なカード番号を保存しません）	Stripeの基盤（国外を含む）
アプリ内課金の購入状態	App Store・Google Play・RevenueCat	各社の基盤（国外を含む）
検索用の在庫情報（品名・保管場所・メモ・JANコード・期限など）	Algolia	Algoliaの基盤（国外を含む）
カテゴリ分類に使う商品名・JANコード	Google Vertex AI	Googleの基盤（国外を含む）
商品情報の取得に使うJANコード	Yahoo!ショッピングAPI	LINEヤフーの基盤
アプリの不具合報告・利用状況	Firebase Crashlytics・Google Analytics for Firebase	Googleの基盤（国外を含む）

外部サービスへは、各機能に必要な項目だけを送信します。詳しくはプライバシーポリシーをご確認ください。

認証とアクセス制御

対策	内容
ログイン	Apple、Google、メールアドレスとパスワードでログインします。パスワードはFirebase Authenticationが復元できない形で管理し、当社のサーバーやデータベースには保存しません。当社がパスワードそのものを知ることはできません。Apple・Googleでのログインでは、パスワードはノコリスに送られません。
台帳の閲覧	台帳を閲覧できるのは、その台帳のメンバーだけです。データベースのルールで、メンバー以外の読み取りを拒否します。
台帳の更新	在庫や台帳の作成・変更・削除は、サーバーの処理だけが行います。端末からデータベースへ直接は書き込めません。処理のたびに、ログインと台帳の権限を確認します。
権限	オーナー・管理者・メンバーの3段階です。権限の変更はオーナーだけ、メンバーの除外はオーナーと管理者だけが行えます。
担当交代・退職	対応版のWeb・iOS・Androidでは、除外したアカウントは台帳を閲覧できず、招待コードでも再参加できません。取得・出力済みのデータは遠隔消去できないため、社内端末の返却や保存データの削除も併せてご確認ください。
正規アプリの確認	App Check（iOSはApp Attest、AndroidはPlay Integrity、WebはreCAPTCHA Enterprise）で、サーバーの処理を呼び出す端末を確認します。
アカウントの削除	削除の直前に再ログインを求め、本人以外による削除を防ぎます。

通信・決済・運営の管理

対策	内容
通信の暗号化	アプリ・ブラウザとサービスの通信は、HTTPS（TLS）で暗号化します。
保存時の暗号化	Google Cloudの標準機能により、保存するデータは暗号化されます。
Webアプリの保護	Content Security Policyで読み込めるスクリプトと接続先を制限し、他サイトへの埋め込みを禁止します。
決済	カード情報はStripe Checkoutで入力し、当社のサーバーを通りません。申込時のカード決済では3Dセキュアによる本人認証を求めます。決済の通知は署名を検証して受け取ります。
秘密鍵の管理	決済や外部サービスの秘密鍵は、Google CloudのSecret Managerで管理します。
運営の管理画面	Cloudflare AccessとGoogleアカウントによる二段階の認証を通過し、当社が権限を付与した担当者だけが利用できます。法人の請求に関する操作は監査ログに記録します。
脆弱性への対応	Web・サーバーで使う外部ライブラリを毎週自動で確認し、重大な既知の脆弱性がある場合は検査を失敗させて対応します。

基盤の第三者認証と稼働率

ノコリスは、Googleが提供するFirebase・Google Cloudの上で動いています。基盤の第三者認証と稼働率の目標は、Googleが公開している次のとおりです。

項目	内容
データの保存・処理	Firestore、Cloud Functions、Cloud Storage、Firebase Authenticationは、ISO/IEC 27001・27017・27018とSOC 1・2・3の評価を受けています。
配信・通知・監視	Firebase Hosting、Firebase Cloud Messaging、Crashlytics、App Checkは、ISO/IEC 27001とSOC 1・2・3の評価を受けています。
稼働率の目標	Googleは、Firestoreの単一リージョン（東京など）で月間稼働率99.99%以上、Cloud Run functionsで99.95%以上をSLAとして定めています。

いずれもGoogleの基盤についての認証・SLAで、当社（Altive株式会社）が取得・提供するものではありません。出典：Firebaseのプライバシーとセキュリティ、Firestore SLA、Cloud Run functions SLA。

データの保持と削除

場面	扱い
解約後	利用期限の終了後は無料プランの範囲へ移ります。解約だけで既存データを一括削除しません。
アカウントの削除	本人がアプリ・Webから削除できます。所有する台帳は、ほかのメンバーがいれば管理者を優先して引き継ぎ、いなければ台帳ごと削除します。
長期間利用がない場合	730日間利用がなく有料契約もない場合は、画像を削除することがあります。削除の90日前までにお知らせします。画像以外のデータは、利用がないことを理由に削除しません。
操作の履歴	台帳の更新はタイムラインに記録します。無料プランで閲覧できるのは直近90日分ですが、期間の経過を理由に削除はしません。
障害・誤操作への備え	データベースは、過去7日以内の任意の時点（1分単位）の状態を保持し、障害や誤操作の際に復元できます。データベースそのものの誤削除を防ぐ保護も有効にしています。
データの取り出し	在庫の台帳はCSVで出力できます。社内の報告や監査にお使いいただけます。

付録：現在提供していないもの

現在は次の機能を提供していません。

- 利用者アカウントの多要素認証、SAML等によるシングルサインオン。
- 接続元IPアドレスによるアクセス制限。
- お客様に対する稼働率の保証（SLA）。
- 7日より前の時点へのデータの復元。

これらの機能は、ご要望に応じて実装・提供を前向きに検討します。 導入にあたって必要な機能や希望の時期を、お気軽にお知らせください。貴社のセキュリティチェックシートへの回答や、記載のない項目についてもご相談を承ります。

メールで相談する · 導入相談フォーム · プライバシーポリシー · 利用規約

運営：Altive株式会社（東京都板橋区）。2020年からノコリスを開発・運営しています。