文書責任者	取締役 宮村 亜矢子（登記上氏名：稲葉 亜矢子）
正式版原本	security-overview.md
SHA-256	138aedfca5de66b7bec449604d812a83b6d6bc001036cc0a087cacb2a1a22bd7

NIDOME セキュリティ概要

版: 1.0 / 制定日: 2026-08-26 / 適用日: 2026-09-01
状態: 社内承認済み。初期3社限定試行で適用し、一般提供は外部法務レビューの再検討後に別途判断します。

1. 文書の位置付け

本概要は、NIDOMEで設計・実装する主なセキュリティ対策と責任分界を説明します。侵入テスト報告、詳細なネットワーク構成、認証情報、脆弱性その他悪用につながる情報は、必要性と秘密保持を確認した上で限定提供します。

2026年8月7日時点でAWS本番環境は未構築です。 「設計済み」「コード実装済み」と「AWS上で運用確認済み」を区別し、検証環境の受入前に本番環境で実施済みと表明しません。

2. 構成

無料評価環境

最初の有償契約成立前の無料試用は、Amazon Lightsailの単一インスタンス・単一AZへフロントエンド、バックエンド、処理ワーカーおよびPostgreSQLを集約した評価環境で提供する場合があります。この環境は可用性保証とサービスクレジットの対象外であり、利用人数、データ量、機能および投入可能なデータを申込条件で制限します。

- HTTPS、ファイアウォール、管理者MFA、ログイン試行制限、テナント分離および監査を維持します。
- データベースと管理ポートをインターネットへ公開しません。
- PostgreSQLとファイルを日次バックアップし7日保持します。
- Lightsail標準の自動スナップショットは使用せず、インスタンスのスナップショットは最新2世代を保持します。
- 最初の有償契約成立後は別の商用本番環境を構築し、受入後に契約テナントだけを移行します。
- 移行と合意した保持期間の終了後、評価インスタンス、スナップショット、バックアップおよび認証情報を削除します。

商用本番環境

本番環境の目標構成は次のとおりです。

- Amazon CloudFrontを公開入口とし、AWS WAF、TLS証明書、非公開のS3フロントエンドを利用。
- バックエンドと処理ワーカーはAmazon ECS Fargateで複数のAvailability Zoneへ配置。
- 内部ALBはCloudFront VPC originからのみ到達可能。
- Amazon RDS for PostgreSQL 16を非公開の分離サブネット、Multi-AZで運用。
- 在庫画像・帳票・アーカイブは公開を遮断した専用Amazon S3バケットへ保存。
- 認証情報はAWS Secrets Managerへ保存。
- CloudWatch、SNS、Amazon Q Developer in chat applicationsで監視・運用通知。
- 本番環境と検証環境のリソース、シークレット、データベース、ログを分離。

3. テナント分離

1. 明示的な全体共通データを除き、業務テーブルは`tenant_id`を持ちます。
2. APIはトークンの所属情報を検証し、クエリへ`tenant_id`と必要な`store_id`を含めます。
3. 業務上の識別番号はテナントとの複合一意制約を使用します。
4. 役割と店舗担当範囲をバックエンドで検証し、フロントエンドの非表示だけに依存しません。
5. 他テナント・他店舗へのアクセス拒否を自動テストと受入テストで確認します。
6. SaaS運営者によるテナント代理アクセスは、理由、期限、二者承認、読取専用、監査を基本とします。
7. PostgreSQLの行レベルセキュリティ（Row Level Security）は、アプリケーション側の範囲制御を代替せず追加防御として導入可否を評価します。

4. 本人確認・アクセス管理

- パスワードは一方向ハッシュで保存し、平文を保存しません。
- 本番環境では管理者MFAを必須とします。
- TOTPシークレットはアプリケーションシークレットから導出したキーで暗号化します。
- 復旧コードはダイジェストで保存し、1回利用後に失効します。
- パスワード変更、MFA変更、権限変更時に既存セッションを失効させます。
- ログイン、MFA、パスワード再設定へアプリケーションのアクセス頻度制限とWAFの頻度基準ルールを適用します。
- サービスアカウント、移行ユーザー、実行ユーザー、AWS権限を用途別に分離し、最小権限を適用します。

5. 暗号化とシークレット

1. ブラウザからCloudFront、アプリケーションからRDSへの通信にTLSを使用します。
2. RDS、S3、バックアップ、SNSトピックは保存時暗号化を有効にします。
3. DBパスワード、JWTキー、MFAキー、OAuth認証情報、APIキーはSecrets Manager等で管理し、ソースコードやGitHub変数の平文へ保存しません。
4. Slack Botトークンはテナント別のシークレットとし、DBにはシークレット参照とワークスペース情報だけを保存します。
5. Google Calendarの更新トークンは暗号化して保存します。
6. キーのローテーションで既存データを復号不能にしないよう、対象ごとに更新手順と再認証手順を定めます。

6. データ・ファイル保護

- S3のパブリックアクセス遮断設定（Block Public Access）を維持し、S3のウェブサイト用エンドポイントを使用しません。
- 在庫画像は認証付きAPIでテナント・店舗の範囲を検証して返します。
- アップロードのファイル形式、容量、件数、CSV/XML構造を検証します。
- データ出力には有効期限、ダウンロード監査、チェックサムを使用します。
- 外部サービス提供者からのレスポンスは、トークン、シークレット等を除外して保存します。
- ログへパスワード、JWT、クッキー、シークレット、CSV本文等を出力しません。
- 消去証明原本、請求書、画像等の保持・削除はデータの保存周期に従います。

7. アプリケーションセキュリティ

1. 認証・認可、テナント範囲、入力検証、CSRF・クッキー、冪等性をバックエンドで実装します。

2. 金額確定、帳票発行、入出金、証明書、物理削除等の重要操作は状態遷移、ロック、一意制約、監査で多重実行を防止します。
3. 依存パッケージの版を固定し、バックエンドは`pip-audit`、フロントエンドは`npm audit`をCIの必須確認とします。
4. DependabotでPython、npm、Docker基盤イメージ、GitHub Actionsを定期確認します。
5. コードレビュー、移行テスト、E2E、アクセシビリティ、負荷、越境アクセステストを変更リスクに応じて実施します。
6. 本番環境へのデプロイはGitHub ActionsのOIDC、環境保護、固定したイメージダイジェストを使用する設計です。

8. ログ・監視

- 重要操作を追記型の`audit_logs`へ記録します。
- `X-Request-ID`と`audit_logs.request_id`でアプリケーションログと業務監査を追跡します。
- ALBの5xx・正常性・応答時間、ECSタスク・CPU・メモリ、処理ワーカーの死活、RDSのCPU・ストレージ・メモリ・接続・応答時間、エラーログを監視します。
- CloudFront経由の`/ready`を5分間隔で外形監視する設計です。
- アラームと復旧を運用Slackチャンネルへ通知し、個人情報・業務明細・認証情報を含めません。
- ログイン試行制限、WAF遮断、通知失敗、メールの不達・苦情を監視します。

9. バックアップ・事業継続

1. 無料評価環境はPostgreSQLとファイルの日次バックアップを7日、インスタンスのスナップショットを最新2世代保持します。無料評価にはRPO・RTOを保証しません。
2. 本番環境のRDSはMulti-AZ、自動バックアップ、Point-in-Time Recovery、削除保護を有効にする設計です。
3. 本番環境の初期バックアップ保持期間は7日です。
4. データの復元は専用インスタンスで検証し、件数・整合性・テナント分離を確認してから切替えます。
5. 検証環境で定期的にバックアップ・復元訓練を行い、RPO・RTOの実測値をSLAへ反映します。
6. フロントエンド生成物、コンテナイメージ、データベース、S3オブジェクトの復旧・切戻し手順を分離します。
7. AWS受入前の設計目標はRPO 24時間、RTO 8時間とし、少なくとも6か月ごとおよび重大な構成変更後に復旧訓練を行うこと。実測・受入前は契約保証としないこと。

10. インシデント対応

1. 検知、優先度判定、封じ込め、根絶、復旧、監視、事後検証の手順を定めます。
2. 公開情報と内部調査情報をバックエンドで分離し、公開履歴は追記型で管理します。
3. セキュリティインシデントはプライバシー・法務・運用責任者へ上申・連携し、法令と契約に従って顧客、本人、当局へ連絡します。
4. 復旧後に原因、影響、検知、対応、再発防止を確認します。
5. 詳細は障害連絡方針と内部運用手順に従います。

11. 提供事業者・委託先管理

- 提供事業者のプライバシー、DPA、セキュリティ、データ保管場所、再々委託先、削除条件を利用開始前に確認します。
- OAuthの許可範囲を機能上必要な範囲に限定します。
- テナントが有効化した任意機能の提供者だけへデータを送信します。
- 提供者の障害、認証情報の失効、API変更時に機能を安全に停止し、中核業務データを失わない設計とします。
- AI分析は固定済みの指標スナップショットを送信し、APIリクエストで`store=false`を指定します。

12. セキュリティ責任分界

当社

- アプリケーション、クラウド構成、テナント分離、バックアップ、監視、脆弱性対応。
- 当社管理の認証情報、運用権限、委託先の選定・監督。
- インシデントの調査と契約上・法令上必要な連絡。

契約者

- ユーザー、役割、店舗権限、退職者アカウント、端末、ネットワークの管理。
- MFA復旧コード、ダウンロード後のファイル、印刷物、外部サービスのアカウント管理。
- 入力データの適法性、正確性、必要な本人通知・同意、法定保存。
- 不審操作、誤権限、漏えいのおそれの速やかな連絡。

共同

- 任意連携の許可範囲と送信データの確認。
- インシデント時の事実確認、本人・取引先対応。
- データ出力、契約終了、法的保全の計画。

13. 未完了の本番受入

本概要を顧客向けに承認する前に、少なくとも次を完了します。

- [ ] AWS検証環境へのデプロイと本番同等構成との差分確認
- [ ] Lightsail無料評価環境のバックアップ・復元、2世代スナップショット、テナント移行および削除訓練
- [ ] WAF、MFA、Secrets Manager、OIDCデプロイの受入
- [ ] バックアップ・PITR・復元の整合性とRPO/RTO測定
- [ ] アラーム・Slack・稼働状況ページ・インシデント訓練
- [ ] テナントデータのアーカイブ出力と二者承認による物理削除訓練
- [ ] 脆弱性検査、侵入テストの範囲と実施
- [ ] 提供事業者のDPA・国外処理・再々委託先レビュー
- [ ] セキュリティ責任者と連絡先の確定

AWS検証環境・本番環境の受入前における設計目標は、本番環境全体の重大障害についてRPO 24時間、RTO 8時間とします。少なくとも6か月ごと、およびバックアップ、データベースまたはストレージ構成の重大変更後に復旧訓練を行います。実測と受入が完了するまで、これらは契約上の保証ではありません。個別データ、外部サービス提供者、契約者環境および不可抗力に同一値を保証するものでもありません。

14. 問い合わせ

- セキュリティ窓口: security@nidome.jp（Microsoft 365共有メールボックス。2026-08-25に開通・外部往復、アクセス制御および不在時引継ぎを確認済み。担当者通知は公開前に最終確認）
- 脆弱性報告窓口: security@nidome.jp（報告手順、秘密保持、公表調整および禁止事項を公開し、将来/.well-known/security.txtからも案内）
- プライバシー窓口: privacy@nidome.jp（2026-08-25に開通・外部往復確認済み）
- セキュリティインシデント受付窓口: incident@nidome.jp（2026-08-25に開通・外部往復確認済みで24時間受信。標準サービスの有人対応および初動目標はSLA・サポート条件に従い、担当者通知および引継ぎは公開前に最終確認）

以上