2026 年 10 月 28 日

セキュリティ対策のご説明

はじめに

昨今、ランサムウェアによる業務停止や、不正ログイン、クラウドの設定不備、委託先を経由した情報流出など、企業を狙うセキュリティ事案が相次いでいます。お客様からお預かりする文書データを守るため、当社ではこうした脅威を前提に対策を組み合わせ、継続的に強化しています。

2026 年 10 月からは全社的なセキュリティ対応として、インフラ・アプリケーション・運用・社内環境の 4 つの領域を横断的に見直し、発見した課題に順次対応しています。本書では、主な脅威ごとに当社が実施している対策をご説明します。

1. 第三者認証と管理体制

当社は、情報セキュリティマネジメントシステムの国際規格である ISO/IEC 27001:2022（JIS Q 27001:2025）の認証を取得しています（認証番号 IR0210）。年 1 回の維持審査を通じて、管理・運用の状況を第三者機関に確認いただいています。また、当サービスは公益社団法人日本文書情報マネジメント協会（JIIMA）の電子帳簿ソフト法的要件認証を取得しています。

サービスで利用する生成 AI は文書解析などの推論用途に限定しており、お客様データが AI モデルの学習に利用されない条件のサービスのみを利用しています。

2. 不正ログイン・なりすましへの対策

当サービスでは二段階認証に対応しています。お客様ごとに接続元の IP アドレスを制限することもでき、この制限は画面操作と API の両方に適用されます。

ログイン、パスワード再設定、二段階認証の各操作には試行回数の制限を設け、連続して失敗したアカウントはロックしています。一定時間操作がない場合や、パスワード・権限が変更された場合には、ログイン状態やアクセストークンを失効させます。パスワード再設定やログイン状態の保持に関する設定も見直しを行いました。

当社の運用者が使う管理画面については、二段階認証と接続元 IP アドレスの制限を必須とし、総当たり攻撃への対策も実施しています。ログインや権限変更、二段階認証の設定といった重要な操作は監査ログに記録しており、お客様の管理者が CSV 形式で出力できます。

3. 外部からの攻撃・マルウェアへの対策

サービスの入口には Web アプリケーションファイアウォール（WAF）を導入し、海外からのアクセスや、既知の悪性 IP アドレス・攻撃パターンを含む通信を遮断しています。送信元の IP アドレスを偽装するヘッダを含むリクエストも、システムの入口で遮断しています。

お客様がアップロードしたファイルはマルウェアスキャンを行い、不正なファイルの取り込みを防止しています。あわせて、圧縮ファイルの展開後のサイズや画像の画素数に上限を設け、過大なファイルによるサービス妨害を防いでいます。Webhook 送信や URL からの取り込みなど外部と通信する機能では、送信先を検証し、内部ネットワークへの不正なアクセスに悪用されないようにしています。

4. 情報流出につながる設定不備・権限の悪用への対策

当サービスのサービス基盤には AWS の東京リージョンを利用しており、お客様データは国内に保管しています。お客様環境ごとに独立したクラウドアカウントで運用しているため、他のお客様の環境とは分離されています。本番環境と開発・検証環境も分離しており、当サービスの環境を統括する管理アカウントも他の事業から切り離して運用しています。

サービスへの通信は HTTPS で暗号化しており、保存する文書ファイルも暗号化しています。すべてのクラウドアカウントで文書の保存先への公開アクセスを遮断し、データベースは外部から直接接続できない内部ネットワークに配置しています。データベースのパスワードや暗号鍵などの機密設定値は、専用の秘密情報管理サービス（AWS Secrets Manager）で管理しています。

アプリケーション内では、管理者・一般利用者などのロールごとに操作権限を制御し、お客様の環境をまたいでデータにアクセスできないようにしています。このデータ分離が保たれていることは、自動テストで継続的に検証しています。AI の推論基盤についても、お客様間で処理が分離されていることを確認しています。

5. ランサムウェア・データ破壊への備え

データベースは自動でバックアップを取得して 14 日間保持しており、文書ファイルは変更前の版を保持しています。加えて、文書とバックアップを一定期間は改ざんや削除ができない形式（WORM）で保護し、ランサムウェアなどによってデータが破壊された場合にも復元できるよう備えています。バックアップから実際に復元できることは、定期的な訓練で確認しています。

6. 監視とインシデント対応

クラウド環境全体の管理操作を記録し、ログの改ざんを検知できる形式で保管しています。全お客様環境のネットワーク通信の記録も取得しており、問題が起きた際に事後の調査ができるようにしています。

サーバーの負荷やエラー率、応答時間、処理の滞留などは常時監視しており、普段と異なる挙動を自動で検知して担当者へ即時に通知します。アプリケーションに異常があった場合は自動で再起動し、更新に失敗した場合は自動で前の状態に戻します。

セキュリティインシデントの対応手順は文書として整備しています。障害が発生した場合は影響範囲を確認してお客様へご連絡し、復旧と必要なデータの復元を進めます。セキュリティ上の問題が疑われる場合は、影響の拡大防止とデータの保全を優先して対応します。

7. ソフトウェアの脆弱性への対策

開発の過程では、ソースコードの静的解析（SAST）、利用しているライブラリの既知の脆弱性の検査、ソースコードへのパスワードや API キーなどの混入の検査を、変更のたびに自動で実行しています。ライブラリの脆弱性は毎日も検査しており、アプリケーションのコンテナイメージも登録時に脆弱性スキャンを行っています。

さらに、外部からの擬似攻撃による脆弱性診断（DAST）と、セキュリティに特化した AI モデルによるソースコードのレビューを定期的に自動で実行し、見つかった脆弱性の候補を修正しています。2026 年 10 月には、認証・権限・外部連携を中心にシステム全体のセキュリティ監査を実施し、発見した課題を順次修正しています。

8. 社内・委託先経由のリスクへの対策

社内の PC にはセキュリティソフトを導入してセキュリティ設定を整備し、マルウェアに感染していないことを確認しています。

クラウド環境へのログインはシングルサインオンに一本化し、管理者権限は役割ごとに分割して日常的には使わない運用に改めました。最上位の管理者アカウントには多要素認証を必須としています。長期間有効なアクセスキーは棚卸しを行って不要なものを廃止し、開発者が使う認証情報も必要な範囲に限定しています。クラウドの権限や当社運用者のアカウントは定期的に棚卸ししています。

従業員の退職・異動の際は、文書化した手順とチェックリストに沿ってアクセス権を削除しています。業務で利用している外部のツールも棚卸しして管理しており、検証環境で本番データを扱っていないかどうかも点検しています。従業員には、ISMS に基づく情報セキュリティ教育を実施しています。

9. 今後の取り組み

より高度なセキュリティ分析に向けて、Anthropic 社の「Claude Mythos」を利用するセキュリティプログラムへの参加を申請しています。承認と利用条件の確認を前提に、脆弱性分析への活用を予定しています。

情報漏洩のリスクを完全になくすことはできませんが、当社は不正アクセスの予防と、問題の早期発見・対応の両面から、引き続きセキュリティの向上に取り組んでまいります。詳細は担当窓口までお問い合わせください。