セキュリティホワイトペーパー

改訂履歴

Ver.	改訂日	改訂内容	作成	承認
1	2026/8/7	初版発行	志村一憲	李東潤

目次

1.はじめに

1.1 ホワイトペーパー の目的
本ホワイトペーパー（以下、本書）は NAZOLの利用を検討されている方、既に利用いただいている方に向けて、NAZOLのセキュリティへの取り組みを確認頂くと共に、NAZOLをセキュアに利用頂くための留意事項を確認頂くことを目的としております。

1.2 本書の適用範囲について
Nazol株式会社提供する「NAZOL」サービスが本書の適用範囲となります。
Googleクラウドサービスは本書の提供範囲外となります。

2.第三者認証機関によるセキュリティ認証について

2.1 情報セキュリティマネジメントシステム（**ISO/IEC27001**）
NAZOLはNazol株式会社が提供するサービスです。また、本サービスのシステム運用を担当するSYコンサルティング株式会社は、情報セキュリティマネジメントシステム（ISMS: Information Security Management System）の国際規格である ISO/IEC 27001 の認証を取得しております。
国際規格 ISO/IEC 27001 および日本産業規格 JIS Q 27001「情報セキュリティマネジメントシステム－要求事項」を基準とし、NAZOLが保有する情報資産を機密性、完全性、可用性の観点から維持・改善するため、セキュリティルールを確立し、継続的な運用、監視、見直しを行っています。

3.情報セキュリティ基本方針

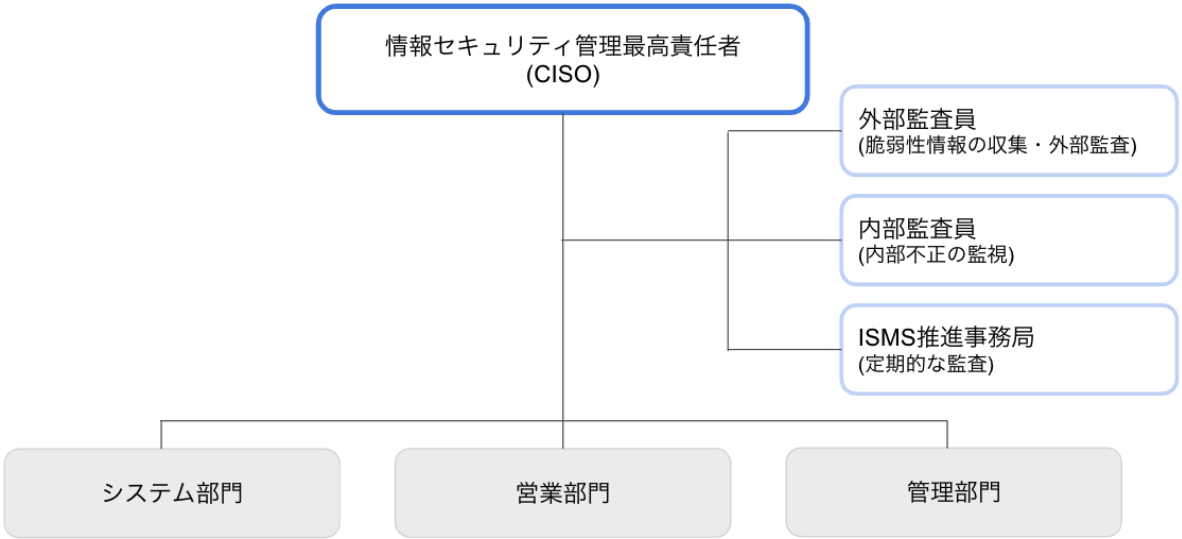
3.1 情報セキュリティの方針群
情報セキュリティの基本方針につきまして、当社WEBサイト（https://nazol.jp/security）にて掲載しておりますのでご確認ください。

3.2 情報セキュリティの役割及び責任
クラウドサービスに関する契約にて役割、及び責任について明記しており、NAZOL利用開始時の利用規約として同意頂く事項となります。

3.3 責任分解点
NAZOLは、会議の発言、AIチャットの回答、Web記事、PDF、メールなど、あらゆるテキスト情報を「なぞる」だけで付箋化し、ワークスペース上で整理・構造化するための思考整理ワークスペースです。複数人でのリアルタイム共同編集にも対応しています。
本サービスは Google Cloud Platform 上に構築されており、基盤インフラの可用性等は Google 社のサービスポリシーに準拠します。
NAZOLのアプリケーション機能についてはNazol株式会社のサービスポリシーに準拠します。

3.4 関係当局との連絡
お客様データは Google Cloud Platform（Cloud Firestore / Cloud Storage）に保存されます。アプリケーション基盤は asia-northeast1（東京）リージョンで稼働しており、データストアについても国内リージョンでの運用を前提としています。

3.5 情報セキュリティの意識向上、教育及び訓練
当社は、体制図に基づき情報セキュリティに関する教育・訓練を全ての従業者（役員、一般社員、パートタイマー、派遣労働者等を含む）に継続的に実施します。



4.利用者情報の管理

4.1 利用者登録及び登録削除
NAZOLでは、メールアドレスによる登録（Google Identity Platformを利用）、Googleアカウント、LINEアカウントの3種類の方法でユーザー登録・ログインが可能です。

ワークスペースへの参加は、オーナーによる招待、または共有リンクの発行によって行われます。ユーザーの自己登録自体は上記いずれかの認証方式で可能ですが、特定のワークスペースへのアクセスは招待または共有リンク経由に限定されます。

4.2 利用者アクセスの提供**(Provisioning)**
ワークスペースへのアクセス権は、ワークスペースのオーナーが管理します。オーナーは招待したメンバーに対して「閲覧のみ」「編集可」の権限を設定できるほか、共有リンクを発行してアクセス範囲を制御することも可能です。
- 共有リンクのアクセス範囲:「招待者のみ」「リンクを知っている人は誰でも」の2種類
- 共有リンクにはパスワードを設定することも可能です

4.3 特権的アクセス権の管理
NAZOLへのログイン認証には、Google Identity Platformによるメールアドレス・パスワード認証のいずれかを利用します。セッションはcookieベースで管理し、本番環境ではsecure属性・httpOnly属性を付与しています。
なお、現時点で二段階認証（多要素認証）機能は提供しておりません。

4.4 利用者の秘密認証情報の管理
NAZOLのパスワードはGoogle Identity Platform側で管理されており、NAZOL側のデータベースに平文はもとよりハッシュ化した状態でも保持しません。パスワードの設定・再設定は、登録メールアドレス宛に送付する確認トークンによる本人確認を経て行われます。

4.5 情報へのアクセス制限
NAZOLが利用するデータベース（Cloud Firestore）はセキュリティルールにより、クライアントからの直接アクセスを一切拒否する設定としています。データへのアクセスは、認証を経たAPIおよびリアルタイム同期基盤経由に限定されます。
ワークスペースへのアクセス制御は「4.1 利用者登録及び登録削除」「4.2 利用者アクセスの提供」記載の通り、オーナーの設定に従って運用されます。

4.6 特権的なユーティリティプログラムの使用
現時点で、お客様向けの外部連携用「API」は提供しておりません。

4.7 お客様の資産の除去
ワークスペースを削除した場合、一定期間（30日間）はゴミ箱として保持されたのち、削除処理の対象となります。アカウントの削除やご契約終了時のデータの取り扱いについては、別途お問い合わせください。

4.8 イベントログ取得
NAZOLでは、アプリケーションの稼働状況やセキュリティ上必要な情報についてサーバー側でログを記録・保持しています。

5.ITインフラ環境のセキュリティ

5.1 クラウドサービスの監視とセキュリティ実装
NAZOLでは、HTTPS通信の強制、および HTTPセキュリティヘッダー（HSTS、X-Frame-Options、X-Content-Type-Options、Referrer-Policy等）の付与を実装しています。
また、認証系エンドポイントに対する総当たり攻撃対策として、Firestoreベースのレート制限を実装しているほか、リアルタイム共同編集を行う通信経路についても、接続単位でのレート制限（トークンバケット方式）を設けています。
Content Security Policy（CSP）については現在整備を進めています。

5.2 技術的脆弱性の管理
本サービスでは、リリース前のセキュリティレビューを実施しており、検出した課題には適宜パッチ適用等の対策を実施しています。また、脆弱性情報の収集を行い、対策を適宜実施しています。

5.3 ネットワークの分離
NAZOLはユーザーアクセスを受けるアプリケーション本体（Cloud Functions／リアルタイム同期基盤）とデータストア（Cloud Firestore、Cloud Storage）が分離された構成になっています。アプリケーションのIngressは内部及びロードバランサー経由のみに限定されており、外部からデータベース・ストレージへ直接アクセスすることはできません。
画像・添付ファイル等の実ファイルはCloud Storageの非公開バケットに保存され、有効期限付きの署名付きURLを経たリクエストのみが取得できます。データベースへのアクセス権限はアプリケーション経由でのみ許可されており、NAZOLが保有するお客様情報にアクセスできる従業員は必要最低限の運用管理担当者のみに制限しています。

6.データの取り扱い

6.1 システム保持情報
NAZOLでは以下の情報を取得・保持します。
- お客様のログイン認証情報（Google Identity Platform、Google OAuth、LINEログインにて管理。パスワードは NAZOL側のデータベースに平文・ハッシュ含め保持しません）
- ワークスペース上で作成されたコンテンツ（付箋、描画、画像、投票、文字起こし、要約、取込みファイル等）
- 共有設定情報（共有先ユーザー、共有リンクのアクセス範囲、共有リンクのパスワード（暗号化して保存）等）
- ワークスペースの基本情報（タイトル、ステータス等）

上記の画像・添付ファイル等の実ファイルは、いずれも Google Cloud Storage 上の非公開バケットに保存され、必要な権限を持つ主体（署名付きURLによる検証を経たリクエスト）のみが取得できます。

6.2 契約・管理者情報
有償プランをご契約いただく際、以下の情報をご登録いただきます。
- 会社名（法人でご契約の場合）
- 連絡先担当者：氏名、連絡先メールアドレス
- ご契約プラン

6.3 連携情報
NAZOLがメール送信等の外部連携に利用する認証情報は、暗号化された状態で安全に管理し、必要時にシステムから自動で読み出す運用としています。
お客様アカウントのパスワードは Google Identity Platform 側で管理されるため、NAZOL側のデータベースに平文で保持されることはありません。

7.セキュリティに配慮した開発のための方針

7.1 セキュリティに配慮した開発のための方針
本サービスでは、変更管理に関するプロセスを定めてサービス開発・運営を実施しております。
変更管理プロセスでは、リスクアセスメントを実施した後、サービスのリリースをしております。

7.1.1 メンテナンス
NAZOLのモノリス部分はサーバーレス構成（Cloud Functions）を採用しており、サーバーOSへの日常的なパッチ適用によるメンテナンスは発生しません。リアルタイム共同編集基盤についても、マネージドサービスの自動アップデートを基本としています。
アプリケーションの構成要素に脆弱性が発見された場合は、適宜パッチの適用等メンテナンスを行います。

7.1.2 告知方法
登録されている管理者情報のメールアドレスにてメンテナンス告知、またはポータルサイトの通知機能によるお知らせを表示いたします。

7.2 ICTサプライチェーン (委託開発先)
当社からの委託先については、原則として日本国内の企業に限定し、契約約款の定めに従い管理を行なっています。委託会社では弊社同等のセキュリティ水準を要求するよう定め、合わせて情報セキュリティ目的を示し、それを達成するためのリスクマネジメント活動の実施を要求するよう定めています。

8.セキュリティインシデント対応

8.1 責任及び手順
情報セキュリティインシデントの対応については情報セキュリティ基本方針にて対策を記載しておりますのでご確認ください。
https://nazol.jp/security

8.2 情報セキュリティ事象の報告
以下に該当するインシデントについては、当社よりご連絡させて頂く場合があります。
- 禁止事項に抵触している場合
（NAZOL利用規約 https://nazol.jp/terms 第6条(禁止事項)）
- 外部からの不正なアクセスにより、他のお客様に影響が波及する恐れのある場合
- 当社の管理するシステムで発生した障害等によって、何かしらの影響が発生している場合
- その他、当社が報告すべきと判断した場合

8.3 情報セキュリティインシデントの検出及び開示ポリシー
当社の管理するシステムについては、平日9時～18時体制で監視を行い、インシデントの検知が行える体制を整えております。
それ以外の時間についてはベストエフォートでの対応となります。
当社で検知した情報セキュリティインシデントは、検知した時点から180分以内での通知を目標としております。
当社で確認したインシデントについては、当社内の通知規定に基づき、登録されている管理者情報のメールアドレスにて通知を行います。

お客様からの問い合わせや報告、お客様が発見した情報セキュリティ事象の報告は、以下のメールアドレスからご連絡いただければと思います。

お問い合わせメールアドレス：back-office@nazol.co.jp

9.法令対応について

9.1 証拠の収集
捜査機関または監督官庁より指導、摘発、注意もしくは紹介を受けた場合は、お客様への通知及び同意を経ることなく、該当期間に情報を開示する場合があります。

9.2 適用法令及び契約上の要求事項の特定
準拠法は日本法と定めています。

9.3 記録の保護
9.3.1 機密保持
秘密情報の取り扱いについては、NAZOL利用規約（https://nazol.jp/terms）に定めています。

9.3.2 個人情報
個人情報の取扱いについては、NAZOLプライバシーポリシー（https://nazol.jp/privacy）に定めています。

9.3.3 プライバシーポリシー(個人情報保護方針)
プライバシーポリシーにつきまして、当社WEBサイトにて掲載しておりますのでご確認ください。
https://nazol.jp/privacy

9.4 暗号化機能に対する規制
クラウドポータルサイトへのWebアクセスにおいては、TLSによる通信の暗号化を行なっています。

9.4 情報セキュリティの独立したレビュー
以下の各事項を実施しています。
①システム運用を担う SYコンサルティング株式会社において、ISO/IEC 27001 の第三者機関による審査を受け、認証を取得しています。これを NAZOLにおける情報セキュリティへの取り組みの証憑としています。
②お客様に安心してご利用いただくため、本セキュリティホワイトペーパー（本書）を通じて適切な情報開示を行っています。