情報セキュリティ対策・個人情報保護に関する安全管理に関する方針一覧

ケンオール株式会社 / 2026-11-05

情報セキュリティ対策

1. 可用性

No.	項目	実施内容
1-1	サービスを提供する時間帯はいつですか。設備やネットワーク等の点検／保守のための計画停止時間を含めてお答えください。	24時間365日提供しております。
1-2	定期的な保守停止に関する事前連絡はありますか。事前通知のタイミング／方法を含めてお答えください。	計画停止はあります。実施する場合は、当社ウェブサイトとダッシュボードのお知らせで事前にお知らせします。
1-3	サービスを利用できる確率（（計画サービス時間－停止時間）÷計画サービス時間）は何%ですか。	スタンダードプラン、プレミアムプランの稼働率の目標（SLO）は、95%です。エンタープライズプランのSLAオプションでは、最高98%です。
1-4	災害発生時のシステム復旧／サポート体制はありますか。	各種構成要素の冗長化を行っています。バックアップは論理的もしくは物理的に離れた場所に保管しています。災害やシステム障害が発生した場合の手順を年1回レビューし、事業継続試験を実施しています。目標復旧時間（RTO）は別項に記載しています。

2. 信頼性

No.	項目	実施内容
2-1	障害発生後のサービス提供の再開に関して設定された目標時間は何時間ですか。	障害を検知してから、スタンダードプラン、プレミアムプランは1営業日、エンタープライズプランのSLAオプションでは最短2時間です。
2-2	システム監視基準（監視内容／監視・通知基準）の設定に基づく監視はありますか。	1分間隔でAPIに対し複数箇所から外形的な死活監視を行い、応答がなくなった時点でアラートを発報します。実行時エラーが発生した場合は即座にアラートを発報します。CPU使用率、メモリー使用率、ディスク使用率、単位時間あたりの処理リクエスト数、レスポンスタイムを監視項目とし、閾値を定めています。
2-3	障害インシデントを収集／集計する時間間隔は何分ですか。	1分間隔で、複数箇所から外形的な死活監視を行っています。
2-4	サービス提供状況を報告する方法と時間間隔は何ですか。	サービスの提供状況は、当社ウェブサイトで常時公開しています。障害が発生した場合は、当社ウェブサイトのお知らせでも報告します。定期的な報告は行っていません。

3. 拡張性

No.	項目	実施内容
3-1	カスタマイズ（変更）が可能な事項／範囲／仕様等の条件と、カスタマイズに必要な情報はありますか。	個別のカスタマイズには応じていません。オプションとして、許可ドメインワイルドカード、バッチAPI、データダウンロードを用意しています（いずれも有償）。APIキーごとに、APIバージョンのデフォルトを設定できます。
3-2	既存システムや他のクラウド・コンピューティング・サービス等の外部のシステムとの接続仕様（API、開発言語等）はありますか。	REST APIを公開しています。OpenAPIスキーマ（2023-09-01／2024-01-01／2025-01-01）と、JavaScript・Python向けのSDKを提供しています。
3-3	オンラインの利用者が同時に接続してサービスを利用可能なユーザ数に制約条件はありますか。	APIサービスであるため、ユーザー数という概念は存在しません。同時リクエスト数には、制限を設けています。
3-4	ディスク容量の上限／ページビューの上限はどれくらいですか。	ディスク容量とページビューは、利用者にディスク容量を割り当てるサービスではなく、ページビュー数による上限も設けていないため、該当しません。

4. サポート

No.	項目	実施内容
4-1	障害対応時の問合せ受付業務を実施する時間帯はいつですか。	ダッシュボードのサポートメニューから、問い合わせフォームを利用できます。通常プランはメール対応、有料オプションでは優先対応・チャット対応が含まれます。エンタープライズプランでは、専用のサポート窓口を設け、受付時間帯を定めています。
4-2	一般問合せ時の問合せ受付業務を実施する時間帯はいつですか。	ダッシュボードのサポートメニューから、問い合わせフォームを利用できます。通常プランはメール対応、有料オプションでは優先対応・チャット対応が含まれます。エンタープライズプランでは、専用のサポート窓口を設け、受付時間帯を定めています。

5. データ管理

No.	項目	実施内容
5-1	データを保護するにあたり、暗号化要件はありますか。	内規で定める重要情報を保存する際に、暗号化しています。暗号化方式は、AES-256または同等以上の強度を持つものです。資格情報など、機微かつ復号の必要がないものは、暗号学的ハッシュ化などの措置を施して保管しています。通信はTLS 1.3および1.2で暗号化しています。バックアップデータは暗号化しています。
5-2	データの整合性を検証する手法が実装され、検証報告の確認作業が行われていますか。	顧客から預託されたデータの検証を行っています。
5-3	入力データ形式の制限機能はありますか。	入力データの形式を検証しています。形式が不正なリクエストには、エラーを返します。

6. セキュリティ

No.	項目	実施内容
6-1	JIPDECやJQA等で認定している情報処理管理に関する公的認証（ISMS、プライバシーマーク等）を取得していますか。	ISMS認証を取得しています。登録番号 IS 793749（ISO/IEC 27001:2022+Amd 1:2024 ／ JIS Q 27001:2025）。
6-2	不正な侵入、操作、データ取得等への対策について、第三者の客観的な評価を得ていますか。	第三者機関による定期的な脆弱性診断を実施しています。
6-3	提供者側でのデータ取扱環境が適切に確保されていますか。	従業者の端末にはディスク暗号化とマルウェア対策を、システム運用には運用者の限定と多要素認証を、稼働システムには不正アクセスの監視・遮断と第三者機関による定期的な脆弱性診断を、データには暗号化と最小権限によるアクセス制限を実施しています。
6-4	システムとやりとりされる通信の暗号化強度はどれくらいですか。	TLS 1.3 および TLS 1.2 に対応しています。
6-5	異なる利用企業間の情報隔離、障害等の影響の局所化はできていますか。	利用企業間の情報隔離は、実施しています。専用テナントのオプションも用意しています。
6-6	利用者のデータにアクセスできる利用者が限定されていますか。また、利用者組織にて規定しているアクセス制限と同様な制約が実現できていますか。	当社側では、1名以上の情報セキュリティ管理者を指名し、最小権限の原則に基づき、必要最小限の従業者のみがアクセスできるようにしています。全てのシステムで多要素認証を強制しています。アカウントは1アカウント1ユーザーを想定しており、利用者組織内のアクセス制限（ID登録・削除、権限割当など）を再現する仕組みは、提供していません。 補足：項目の「利用者のデータにアクセスできる利用者」は、提供者側の従業者を指すものと読んで、回答しています。
6-7	ウイルススキャンの頻度はどれくらいですか。	従業者の端末にマルウェア検知・除去システムを導入し、常時スキャンを有効化しています。OSは常に最新バージョンを利用しています。
6-8	バックアップメディア等では、常に暗号化した状態で保管していますか。廃棄の際にはデータの完全な抹消を実施し、また検証していますか。USBポートを無効化しデータの吸い出しの制限等の対策を講じていますか。	バックアップデータは、クラウド上に保管しており、暗号化しています。保存期間は、データの種別に応じて定め、期間を過ぎたものは削除しています。 補足：項目は、物理的なバックアップメディアを想定した記述です。バックアップはクラウド上に保管しているため、「バックアップデータの暗号化と廃棄(削除)」として、回答しています。
6-9	データ保存地の各種法制度の下におけるデータ取扱い及び利用に関する制約条件を把握していますか。	データの保存地について、所在国とその国の法制度を把握したうえで、必要な措置を講じています。

個人情報保護に関する安全管理

A. 基本方針

No.	項目	実施内容
A-1	個人データの適正な取扱いの確保について、組織として取り組むための基本方針を策定しているか。	「個人情報保護に関する基本方針」を定め、公表しています。
A-2	基本方針に事業者の名称を定めているか。	基本方針に、名称、住所および代表者の氏名を記載しています。
A-3	基本方針に関係法令・ガイドライン等の遵守を定めているか。	基本方針に、個人情報の保護に関する法律その他の関係法令、個人情報保護委員会および総務省の定めるガイドラインの遵守を定めています。電気通信事業法の定める通信の秘密の保護についても、あわせて定めています。
A-4	基本方針に安全管理措置に関する事項を定めているか。	基本方針に安全管理措置に関する事項を定め、講じている措置の内容を同じページに記載しています。
A-5	基本方針に質問及び苦情処理の窓口を定めているか。	基本方針に、開示等の請求および苦情の窓口を記載しています。

B. 規律

No.	項目	実施内容
B-1	取得・利用・保存・提供・削除／廃棄の各段階ごとに、取扱方法・責任者・担当者及びその任務を定めた取扱規程を策定しているか。	個人データの取得から削除・廃棄までの取扱いの方法、責任者の役割および取扱いの状況の点検について、社内の規程を定めています。

C. 組織的

No.	項目	実施内容
C-1	個人データの取扱いに関する責任者を設置し、責任を明確化しているか。	個人情報管理責任者を選任し、氏名を公表しています。
C-2	個人データを取り扱う従業者及びその役割を明確化しているか。	トップマネジメント、情報セキュリティ管理者、内部監査員および従業者の役割を規程に定めています。
C-3	法や取扱規律に違反している事実又は兆候を把握した場合の、責任者への報告連絡体制があるか。	情報セキュリティ事象を発見した従業者は、情報セキュリティ管理者にすみやかに報告します。報告の対象には、情報区分ごとに定めた取り扱いにそぐわない扱いを行った場合を含みます。
C-4	漏えい等事案の発生又は兆候を把握した場合の、責任者への報告連絡体制があるか。	情報セキュリティ事象を発見した従業者は、情報セキュリティ管理者にすみやかに報告します。報告の対象には、媒体の紛失、メールの誤送信、外部からの情報漏えいに関する連絡を含みます。
C-5	複数の部署で取り扱う場合、各部署の役割分担及び責任を明確化しているか。	情報資産管理台帳の部署名欄と責任者欄で、情報資産ごとに定めています。

No.	項目	実施内容
C-6	個人情報データベース等の利用・出力状況を記録しているか。	操作者の操作にかかる記録を監査ログとして取得しています。ログはアクセス制御により改ざんを防止し、時刻を同期し、定期的に点検・分析します。
C-7	書類・媒体等の持ち運び状況を記録しているか。	外部記憶媒体は申請制とし、外部記憶媒体貸出管理表に記入します。機器・媒体を輸送する場合は、配達の記録が残るサービスを利用します。
C-8	作業を委託する場合、委託先が確実に削除・廃棄したことを証明書等により確認しているか。	外部業者へ廃棄を委託する場合、廃棄証明書およびデータ消去の証明書を取得すると定めています。
C-9	担当者の情報システムの利用状況(ログイン実績、アクセスログ等)を記録しているか。	社内システムおよびクラウドサービスについて、認証ログと監査ログを取得しています。ログはアクセス制御により改ざんを防止し、時刻を同期し、定期的に点検・分析します。
C-10	個人情報データベース等の種類・名称を明確化しているか。	情報資産管理台帳に情報資産名を記載し、情報分類、媒体、保管場所および保管期間とあわせて管理しています。
C-11	個人データの項目を明確化しているか。	取得する項目をプライバシーポリシーに記載しています。従業者に関するものは情報資産管理台帳に記載しています。
C-12	責任者・取扱部署を明確化しているか。	情報資産管理台帳の責任者欄と部署名欄で、情報資産ごとに定めています。個人情報管理責任者は基本方針に記載しています。
C-13	利用目的を明確化しているか。	利用目的をプライバシーポリシーに記載しています。
C-14	アクセス権を有する者を明確化しているか。	情報資産管理台帳の閲覧可能者欄に記載しています。年1回、不要なアカウントおよびアクセス権が残っていないことを確認します。
C-15	漏えい等事案発生時に事実関係の調査及び原因の究明を行う体制があるか。	二次被害の防止、原因の特定および被害範囲の特定に取り組みます。
C-16	個人情報保護委員会等への報告を行う体制があるか。	情報セキュリティ管理者が関係する省庁等へ連絡します。電気通信事業者としての報告先は、権限の委任を受けた総務大臣です。
C-17	再発防止策の検討及び決定を行う体制があるか。	対応結果と再発防止策をまとめ、責任者に報告します。

D. 人的

No.	項目	実施内容
D-1	個人データの取扱いに関する留意事項について、従業者に定期的な研修等を行っているか。	従業者に対し、個人データの取扱いに関する教育を定期的に実施しています。

E. 物理的

No.	項目	実施内容
E-1	管理区域について、入退室管理及び持ち込む機器等の制限を行っているか。	個人データを取り扱う区域について、入退室を管理しています。
E-2	取扱区域について、のぞき込み防止措置等により、権限を有しない者による閲覧を防止しているか。	オフィスを一般エリアとセキュリティエリアに分け、クリアデスクを定めています。
E-3	機器・電子媒体・書類等を、施錠できるキャビネット・書庫等に保管しているか。	個人情報を含む紙は、施錠できるキャビネットで保管します。
E-4	持ち運ぶ個人データを暗号化・パスワード保護した上で電子媒体に保存しているか。	持ち運ぶ個人データは、暗号化またはパスワード保護を行います。
E-5	施錠できる搬送容器を利用しているか。	該当しません。配達の記録が残る輸送サービスを利用します。
E-6	書類を廃棄する場合、復元不可能な手段を採用しているか。	不要となった紙媒体は、社内のシュレッダーで破棄します。
E-7	情報システムにおいて個人データを削除する場合、容易に復元できない手段を採用しているか。	PCおよび記憶媒体は、媒体種別ごとに消去方式を定め、消去後に読み取りができないことを確認します。
E-8	機器・電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用しているか。	情報セキュリティ管理者がデータの消去または破壊の措置を行い、外部業者に委託します。

F. 技術的

No.	項目	実施内容
F-1	個人情報データベース等を取り扱うことのできる情報システムを限定しているか。	各アクセス権は最小権限の原則に基づいて設定し、あわせて個人データを取り扱う情報システムをシステム・サービス管理表で管理しています。
F-2	情報システムによってアクセスすることのできる個人情報データベース等を限定しているか。	情報システムからアクセスできる範囲をアクセス権により限定し、各サービスの管理画面で管理して定期的に確認します。
F-3	ユーザーIDに付与するアクセス権により、使用できる従業者を限定しているか。	アカウントは申請制で必要な権限のみを付与し、年1回、不要な権限が残っていないことを確認します。
F-4	情報システムを使用する従業者を、ユーザーID・パスワード等により識別・認証しているか。	すべてのPCおよびサーバにログイン認証を設定しています。共有アカウントは原則禁止です。
F-5	情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断しているか。	インターネットからのアクセス経路に、遮断する仕組みを導入しています。
F-6	自動更新機能等の活用により、ソフトウェア等を最新状態としているか。	常に最新バージョンを利用するよう定め、緊急性の高いパッチはシステム管理者から指示します。
F-7	ログ等の定期的な分析により、不正アクセス等を検知しているか。	ログはアクセス制御により改ざんを防止し、時刻を同期し、点検・分析します。

No.	項目	実施内容
F-8	個人データを含む通信の経路又は内容を暗号化しているか。	インターネットを経由する通信を暗号化しています。
F-9	移送する個人データについて、パスワード等による保護を行っているか。	個人情報を含むファイルをメールで送る場合は、クラウドストレージに置いて共有リンクを送付します。機器・媒体を輸送する場合は、パスワードまたは暗号化による保護を行います。

G. 外的環境

No.	項目	実施内容
G-1	外国において個人データを取り扱う場合、当該外国の個人情報の保護に関する制度等を把握した上で、必要かつ適切な措置を講じているか。	個人データの取扱いを委託する外部サービスについて、所在国および当該国の個人情報の保護に関する制度を把握したうえで、必要な措置を講じています。所在国および事業者は「外国にある委託先への個人データの提供について」で公表しています。