

kickflow セキュリティホワイトペーパー

1. はじめに

株式会社kickflow(以下、「当社」といいます。)が提供するクラウドワークフローシステム「kickflow」(以下、「本サービス」といいます。)における、情報セキュリティ対策の実施状況、およびセキュリティ機能について説明します。

当社は、お客様に安心してサービスをご利用いただくため、情報セキュリティマネジメントシステム(ISMS)を構築し、適切な運用を行っています。

2. 利用者との責任分界点

本サービスの利用におけるセキュリティ対策は、当社(クラウドサービスプロバイダ:CSP)とお客様(クラウドサービスカスタマ:CSC)がそれぞれの責任範囲において実施する必要があります。

本サービスはSaaS(Software as a Service)として提供されており、OS、ミドルウェア、アプリケーション、ネットワーク、物理基盤までを当社の責任範囲とします。

【責任分界イメージ】

レイヤー	責任主体	内容
データ / コンテンツ	お客様	入力データの管理、権限設定、アカウント管理
アプリケーション	当社	アプリケーションの脆弱性対策、機能開発
ミドルウェア / OS	当社	パッチ適用、設定管理
仮想化 / 物理基盤	当社	クラウドインフラ(Google Cloud/AWS等)の管理・選定

当社の責任

- 本サービスを提供するアプリケーション、ミドルウェア、OS、およびインフラストラクチャ(物理サーバ、ネットワーク等)のセキュリティ対策
- お預かりしたデータの適切な保管、バックアップ、および論理的な分離
- 当社運用担当者による特権アクセスの厳格な管理と監査

お客様の責任

- アカウント(ユーザーID)およびパスワード等の秘密情報の適切な管理

- ユーザーに対する権限設定(ロール管理)、組織管理、およびアカウントの棚卸し
- 本サービスに入力・保管されるデータ、および生成されたデータの利用に関する管理
- 登録する個人情報の取扱いに関する法令遵守(利用目的の通知・公表等)
- 登録する個人情報の本人(ユーザー)に対する当社が示す個人情報保護方針ならびにプライバシーポリシーの説明

3. データ保管場所と越境移転

お客様が本サービスに登録したデータは、以下の堅牢なクラウド基盤上に保管されます。当社は、各保管先において適切なセキュリティ対策が講じられていることを確認しています。

- データベース(**Google Cloud**): 日本(東京)リージョン
- ファイルストレージ(**AWS S3**): 日本(東京)リージョン
- 認証情報(**Auth0**): 米国(US)リージョン他(グローバル分散)

これらのデータセンターは、世界最高水準のセキュリティ基準(ISO 27001, SOC2等)を満たしており、物理的・論理的に厳重に管理されています。

お客様データの保護及び第三者提供について

- お客様から預かったデータを適切に保護することは、当社の責任です。ログデータを含むお客様データは、不正なアクセスや改ざんを防ぐため、開発チーム(委託先を含む)の一部の人間しかアクセスできない、限られたアクセス権のもとで保管されます。
- 但し、裁判所からの証拠提出命令など、法的に認められた形でお客様のデータの提供を要請された場合、お客様の許可なく、必要最小限の範囲で、お客様情報を外部に提供する可能性があります。

4. データの分離と削除

データの分離(マルチテナント管理)

本サービスはマルチテナント方式を採用しておりますが、テナントIDによる厳格な論理分離を行っています。アプリケーションレベルおよびデータベースレベルでアクセス制御が実装されており、他のお客様(テナント)のデータにアクセスすることはできません。

解約時のデータ削除

- お客様が本サービスを解約された場合、テナント(組織)は契約終了後30日以内に削除されます。
- ただし、システム運用上保存している各種ログ等については、一定期間(セキュリティ上の必要性に基づき)保持した後に削除されます。

バックアップデータの削除

- バックアップデータについては、最大7日間の保管期間経過後に完全に削除され、復元することはできません。

5. アカウント・組織管理機能

お客様の組織ポリシーに合わせ、柔軟な管理機能を提供しています。

- 利用者登録・削除:

- 管理画面より、いつでもユーザーの招待(登録)および論理削除(ステータス変更)が可能です。
- API・CSVによる一括登録にも対応しています。
- カスタムロール作成:
 - ユーザーに対し、任意の管理権限(閲覧のみ、設定変更可など)を組み合わせた「管理者ロール」を自由に作成・付与することが可能です。

6. アクセス権の管理

意図しない情報の閲覧や操作を防ぐため、詳細なアクセス制御機能を提供しています。

- 機能単位の制御: 管理者権限を持つユーザーのみが、システム設定やユーザー管理機能にアクセス可能です。
- チケット単位の制御: 閲覧権限のないユーザーは、他部署や関係のない申請チケットを閲覧できないよう制御されています。
- IPアドレス制限: 接続元のIPアドレスを制限することで、社外や許可されていないネットワークからのアクセスを遮断できます(※エンタープライズプラン等で提供)。
- リモートアクセス: 運用中の本番環境へのアクセスは、お客様で業務上必要な最小限の権限に限定し、リモートアクセスで招待します。管理センターで閲覧以外の操作内容はすべて監査ログとして記録されます。

7. 認証およびパスワード管理

- 認証方式の制御: テナントごとに利用可能な認証方式(ID/PW、SSO等)を制御・強制することが可能です。
- 多要素認証(MFA): 各ユーザー設定において、パスワードに加え認証コードを用いた2要素認証を設定することで、なりすましによる不正ログインを防止できます。
- 不正ログイン対策: 認証基盤としてAuth0を採用しており、パスワードリスト攻撃などの不正なアクセス試行を自動的に検知・ブロックする仕組みを備えています。

8. 暗号化とネットワークセキュリティ

- 通信の暗号化: お客様の端末と本サービス間の通信は、SSL/TLS(TLS 1.2以上)により全て暗号化され、盗聴や改ざんを防止しています。
- 保存データの暗号化: データベース等のストレージに保存される機微な情報は、暗号化された状態で保管されます(アプリケーションレベルまたはDBレベル)。
- ネットワーク防御: インフラストラクチャレベルでのファイアウォール、WAF(Web Application Firewall)、およびDDoS対策機能により、外部からの不正な攻撃を防御しています。

9. 変更管理

本サービスの機能追加や仕様変更を行う際は、お客様への影響を考慮し、以下の通り対応します。

- 通知: 新機能のリリースやメンテナンス情報は、サービス内の「お知らせ」やヘルプセンター、またはメールにて通知します。

- 破壊的な変更への対応: APIの仕様変更など、お客様の運用に重大な影響を与える変更(破壊的な変更)が生じる場合は、原則として事前に通知を行い、十分な周知期間を設けます。

10. バックアップの状況

- バックアップ頻度: データベースは常時トランザクションログを取得しており(ポイントインタイムリカバリ)、システム障害時に直前の状態まで復旧可能な体制をとっています。
- 保管期間: バックアップデータは最大7日間保管されます。
- 保管場所: データの種類に応じ、Google Cloud(日本)またはAWS(日本)の堅牢なストレージに保管されます。

11. ログの管理と時刻同期

- 監査ログ: 管理者の操作履歴(ユーザー追加、権限変更等)を記録しており、権限を持つ管理者が閲覧可能です。
- 操作ログ: チケットに対する申請・承認等の操作履歴を記録しています。
- ログの保護と保持期間: 取得したログは適切なアクセス権限のもとで保管され、監査および不正検知の目的で一定期間(種類により異なります)保持されます。
- 時刻同期: システム時刻は信頼できる時刻配信サービス(Google 内部の時刻源)と同期しています。

12. 脆弱性管理

- 脆弱性診断: 第三者機関によるプラットフォーム診断またはWebアプリケーション診断を、最低年に1回以上実施しています。
- パッチ適用:
 - インフラ/OS/ミドルウェア: マネージドサービスを採用し、クラウド事業者によりセキュリティパッチが速やかに適用されることを確認・管理しています。
 - アプリケーション: 使用しているフレームワークやライブラリにセキュリティパッチが公開された場合、または重大な脆弱性が発見された場合は、検証環境での確認を経て速やかに適用します。

13. 開発におけるセキュリティ

- セキュアコーディング: IPA「安全なウェブサイトの作り方」等の業界標準ガイドラインに基づき、SQLインジェクションやXSS(クロスサイトスクリプティング)等の脆弱性を作り込まないよう開発を行っています。
- コードレビュー: 開発されたプログラムは、リリース前に必ずコードレビューおよびテストを実施し、品質と安全性を確認しています。

14. インシデント発生時の対応と監査・セキュリティチェックシート

- 通知体制: データの消失や長時間のシステム停止など、お客様に重大な影響を与えるセキュリティインシデントが発生した場合、発生から可能な限り速やかにメールまたはサービス上の掲示等により第一報を通知します。
- 連絡窓口: セキュリティ上の懸念や脆弱性を発見された場合は、[サポート窓口](#)までご連絡ください。

- 監査対応: お客様からのセキュリティチェックシートや監査への対応については、合理的な範囲で誠実に対応いたします。
- セキュリティチェックシートについて: kickflowでは、経済産業省が公開している「クラウドサービスレベルのチェックリスト」とIPA(独立行政法人情報処理推進機構)による「安全なウェブサイトの作り方改訂第7版」に準拠したセキュリティチェックシートに記入したものを公開しております。まずはこちらを参考にお客様ご自身でご記入をお願いします。ダウンロードは[こちら](#)のヘルプページからご確認ください。

15. 外部クラウドサービスの利用(サプライチェーン)

本サービスは、安定したサービス提供のために以下の外部クラウドサービスを利用しています。

当社はこれらの委託先に対し、契約等を通じて適切なセキュリティ水準(ISO 27001, SOC2等の取得、秘密保持条項等)を求めています。

クラウドサービス名	利用用途	運営会社	保管または共有する国
Google Cloud	アプリケーション基盤・DB	Google LLC	日本
Amazon Web Services (AWS)	ファイルストレージ・ログ基盤・バックアップ	Amazon Web Services, Inc.	日本
Auth0	認証基盤・ID管理	Okta, Inc.	米国他
SendGrid	メール配信	Twilio Inc.	米国
Datadog	システム監視・ログ監視	Datadog, Inc.	日本
BigQuery / GCS	ログ保管	Google LLC	日本
Sentry	エラー検知	Functional Software, Inc.	米国

Elastic Cloud	検索エンジン基盤	Elasticsearch B.V.	日本
Firebase	プッシュ通知基盤・通知機能	Google LLC	日本
Scalebase	請求書発行	Scalebase株式会社	日本
OpenAI	生成AI機能	OpenAI, L.P.	米国
CloudConvert	帳票PDF出力	Lunaweb GmbH	米国・ドイツ

16. 知的財産権の保護

当社は、第三者の知的財産権を尊重し、本サービスの利用において知的財産権の侵害が行われないよう、利用規約に基づき適切な対応を行います。

- 権利侵害に関する通報窓口：
 - 本サービス上に保管されたデータが、第三者の知的財産権（著作権、商標権等）を侵害している懸念がある場合は、当社サポート窓口までご連絡ください。
- 対応プロセス：
 - 知的財産権侵害の申立てを受けた場合、情報流通プラットフォーム対処法および当社利用規約に基づき、対応を検討・実施します。

17. 生成AIの利用について

本サービスでは、サービス機能の一部において生成AI（大規模言語モデル等）を利用しています。AI機能の提供にあたり、以下のセキュリティおよびプライバシー対策を講じています。

お預かりデータの学習利用の禁止

お客様が本サービスに登録したデータ（以下、「預託データ」といいます。）は、AIモデルの学習（トレーニング、ファインチューニング等）には一切使用しません。預託データは、お客様がご利用になる機能の処理のためにのみAIモデルへ入力されます。

AIへの入力データの取扱い

AI機能の処理に際してモデルへ入力されたデータは、処理完了後、AIサービス提供元の基盤上に原則として保存されません。ただし、AIサービス提供元のポリシーに基づき、不正利用の検知・防止およびサービスの安全性確保など、最小限の目的に限り一時的に保持される場合があります。当社は、AIサービス提供元との契約等を通じ、当該データの取扱いが適切であることを確認しています。

AIモデルのアップデート

サービスの品質向上および最新技術への対応のため、本サービスで利用するAIモデルは随時アップデートされる場合があります。モデルの変更にあたっては、出力品質や安全性の検証を行った上で適用します。

AI利用におけるお客様の責任

AI機能による出力結果は、統計的な推論に基づくものであり、その正確性・完全性を保証するものではありません。出力結果の採用・利用に関する判断は、お客様の責任において行っていただきますようお願いいたします。

18. 認証取得状況

当社は、情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS適合性評価制度における、ISMS認証を取得しています。

クラウドセキュリティの国際規格「ISO/IEC 27017」の認証を取得予定です。

- **ISO/IEC 27001 (ISMS)**
 - [認証登録詳細ページ](#)
- **ISO/IEC 27017 (ISMS-CLS)**
 - (※取得完了後に登録証情報を記載)

お問い合わせ

本ドキュメントに関するご質問は、当社サポート窓口までお問い合わせください。

- 株式会社kickflow サポート窓口
 - <https://support.kickflow.com/hc/ja/requests/new>
- 営業時間: 平日10:00～18:00
 - 年末年始、祝日は除きます。
 - 休み明けや繁忙期など、状況によっては回答までにお時間をいただく場合がございます。
 - 上記時間外でもお問い合わせいただけますが、回答は翌営業日以降となります。

改訂履歴

版	改訂日	改訂内容
1.0	2026/02/18	初版発行
1.1	2026/03/30	17. 生成AIの利用についての追加
1.2	2026/04/24	リモートアクセスに関する文言を変更
1.3	2026/08/07	3. データ保管場所と越境移転 お客様データの保護及び第三者提供についての追加 18. 認証取得状況 「情報マネジメントシステム認定センター(ISMS-AC)が運営する、ISMS適合性評価制度における、ISMS認証を取得しています。」の追加
1.4	2026/09/30	15. 外部クラウドサービスの利用(サプライチェーン)に「CloudConvert(帳票PDF出力)」を追加
1.5	2026/10/13	インフラ移行に伴う3・10・11・15・18章の更新