共創ナビ **ivan** セキュリティポリシー

制定日：2025年3月6日
改訂日：2025年10月17日

株式会社HackCamp

---

1. はじめに

共創ナビivan（以下ivan）は、ユーザーの機密情報を最優先に保護し、安全に活用できる環境を提供することを基本方針としています。
本ポリシーは、データ管理・アクセス制御・情報セキュリティ対策の方針を明確にし、ユーザーが安心して利用できるようにすることを目的としています。

また、ivanはGoogle Cloud Platform（GCP）上で運用されており、GCPの強固なセキュリティ基準に準拠したクラウド環境を活用することで、安全性を確保しています。
GCPは、ISO 27001、SOC 2、SOC 3、GDPR、CCPAなどの国際的なセキュリティ・コンプライアンス認証を取得しており、ivanはこの環境を利用することで業界標準のセキュリティ対策を実施しています。

---

2. GCPのセキュリティ基準への準拠

ivanは、GCPが提供するセキュリティ基盤をフル活用することで、強固なデータ保護環境を実現しています。

2.1 GCPの取得認証と準拠基準

- ISO/IEC 27001（情報セキュリティマネジメントシステム）
- ISO/IEC 27017（クラウドサービスのセキュリティ管理）
- ISO/IEC 27018（クラウドでの個人情報保護）
- SOC 2 & SOC 3（内部統制とリスク管理の証明）
- GDPR（EU一般データ保護規則）準拠
- CCPA（カリフォルニア州消費者プライバシー法）準拠

---

3. データ管理ポリシー

3.1 ユーザーデータの取り込み

- ivanでは外部データの読み込みが可能です。対応するファイルフォーマットはテキスト形式です。拡張子が.txtまたは.mdのファイルを取り込むことができます。
- PDFは変換ツールなどでテキスト形式に変換することで読み込み可能です。
- 画像ファイルは読み込むことができません。
- ivanの特許検索機能で文脈内学習に使用できる特許件数は100件～300件程度です。

3.2 ユーザーデータの取り扱い

- ivanは、ユーザーが登録したデータ並びに生成AIが出力した結果をすべて暗号化するため、管理者であってもアクセスできない設計になっています。
- ivanに入力した顧客データの保管および削除の管理責任はユーザー側にあります。
- セッション内で登録されたデータ（アセット、戦略などの企業情報）は、そのセッション内でのみ利用され、他のセッションには引き継がれません。
- セッションを跨いだデータ共有はシステム内では不可能な設計にしています。セッション間でデータ共有を行いたい場合は、エクスポート／インポート機能を用いることで可能です。

3.3 AIモデルと学習について

- ivanが利用するLLMと最大コンテキスト長は以下の通りです。
  ・OpenAI GPT-4.1 / GPT-4.1 mini：100万トークン
  ・OpenAI GPT-5 /　GPT-5 mini　：40万トークン
- 利用者が入力したデータはOpenAI社のAPIを通じて処理されますが、学習には使用されません。（参照：https://openai.com/enterprise-privacy/）
- ivanは、ユーザーの入力データやAIが生成したデータを学習に利用することはありません。

3.4 データ削除ポリシー

- 契約終了後、ivanに保存されているユーザーデータは原則として30日以内に完全削除されます。
- 削除は暗号化データを含む全バックアップ領域を対象に実施され、復元不可能な形式で処理されます。
- ユーザーがエクスポートしたデータについては、ユーザー自身の責任において管理・削除を行うものとします。

4. アカウントポリシー

4.1 アカウントの種類

- ivanには管理者，利用者，招待者の3種類のアカウントが存在します。
- 管理者IDはHackCampが管理するため非公開です。利用者IDのみの提供となります。招待者は招待リンク経由でアクセスできるため，IDの発行はありません。

アカウント種別	利用できる機能	アクセス方法
管理者 （HackCamp）	アカウント・アプリ管理、開発・カスタマイズ	多要素認証(MFA)によるログイン必須
利用者	データ入力、AIアシスタント、出力閲覧・編集、印刷・出力、招待リンク作成	MFAによるログイン ID共用禁止
招待者	指定セッションのみアクセス可。 データ入力・結果閲覧のみ	期限付き（5日間）招待リンク

---

5. セキュリティ対策

- すべての通信はTLS/SSLで暗号化され、データストレージはAES-256暗号化を採用しています。
- パスワードは大文字・小文字・数字・記号を含む8文字以上が必須で、リトライ回数は制限されます。
- ログイン時にはスマートフォンの認証アプリで発行されるコードを入力する多要素認証（MFA）を採用しています。
- WebアプリケーションにはWAF（Web Application Firewall）を導入し、SQLインジェクションやXSS攻撃などへの対策を実施しています。

---

6. 稼働／障害監視およびログ管理

6.1 稼働・障害監視

- WAF導入によりアプリケーションレベル攻撃対策を実施。

- サービスの稼働は以下のページで確認できます：
  https://app.ivan-x.jp/ja/networkcheck
  https://status.cloud.google.com/?hl=ja
  https://health.aws.amazon.com/health/status

6.2 ログ管理・保管期間

- アクセスログ：ユーザーのログイン・ログアウト履歴を一定期間保管します。
- 操作ログ：主要な操作履歴を一定期間保管します。
- 上記のログはセキュリティ監査および障害調査の目的に限り利用されます。

---

7. 第三者委託・再委託の管理

- ivanの開発・運用は、株式会社HackCampおよび株式会社ミーティングテクノロジーが共同で実施しています。

- 業務の再委託は原則として禁止されており、やむを得ず第三者への再委託を行う場合にはHackCampの事前承認を必要とします。

- 再委託先には同等以上のセキュリティ基準を要求し、監査可能な契約を締結します。

---

8. セキュリティインシデント対応

- セキュリティインシデント発生時には影響範囲を速やかに調査し、必要に応じてユーザーに通知します。

- 重大なインシデント発生時には、事前に定められた対応計画に基づき報告および復旧対応を行います。

---

9. 個人情報の取り扱い

- ivanでは基本的に個人情報を取り扱いません。
- システムとして利用者に個人情報を入力させる設計にはなっていません。

---

10. 責任分解

管理対象	責任者	説明
顧客データ（ユーザー入力データ）	顧客（利用企業・利用者）	顧客責任で管理され、ivan運営側はアクセス不可
ivanコンテンツ　開発	株式会社HackCamp （取締役副社長：矢吹博和）	アプリ設計・プロンプト設計・UX開発
システム開発・　運用管理	株式会社ミーティングテクノロジー（代表取締役社長：伊勢川暁）	システム開発・クラウド運用・セキュリティ管理
インフラ	Google Cloud Japan / AWS Japan	データは日本国内を中心に保存、一部米国領域を使用

---

11. お問い合わせ

株式会社HackCamp
所在地：東京都千代田区霞が関1丁目4番1号 SENQ霞ヶ関
取締役副社長：矢吹博和
連絡先：info@hackcamp.jp
https://hackcamp.jp/