HRBrain

セキュリティホワイトペーパー

1.0 版

株式会社 HRBrain

1　利用者との責任分界点

株式会社 HRBrain の責任

株式会社 HRBrain（以下、「当社」）は、以下のセキュリティ対策を実施します。

- HRBrain サービス（以下、「HRBrain」）における各アプリケーションのセキュリティ対策
- HRBrain における各アプリケーションに保管されたお客様データの保護
- HRBrain における各アプリケーションの提供に利用するミドルウェア、OS、その他インフラのセキュリティ対策。但し、当社以外の第三者が開発・提供するサービスについては、当該サービスの提供事業者が定義する責任範囲に従い、当該サービスによりお客様に生じた損害について当社は責任を負わないものとします。

お客様（以下、「利用者」）の責任

利用者は、以下のセキュリティ対策を実施する必要があります。

- 各ユーザーに付与されたパスワードの適切な管理
- HRBrain アカウントの適切な管理（登録、削除、組織管理者権限の付与など）
- HRBrain の利用にあたり生成、保存等されたデータの管理、利用に関する責任
- HRBrain の利用にあたり生成されたデータの利用に関する責任
- HRBrain に保存等する個人情報の取扱いに関する適切な管理（本人に対する利用目的の通知・公表その他の個人情報保護法上必要な対応）

なお、HRBrain とは以下各種サービスを包括しております。

- HRBrain タレントマネジメント
- HRBrain 組織診断サーベイ
- HRBrain 人事評価
- HRBrain 労務管理
- HRBrain AI チャットボット
- HRBrain 360 度評価

2　データ保管場所

- HRBrain 利用にあたり保存等または生成されたデータ（以下、「本データ」）は、GCP 東京リージョンに保管されます。

3　データの削除

- 本データは、利用者により削除の操作が行われた場合、データベース上から削除されます。また、利用者により削除の操作が行われたデータはデータベース上から完全に削除され、復元を行うことはできません。
- HRBrain 利用契約が終了した場合、契約終了日の翌日から3ヶ月以内に、本データは完全に削除されます。本データの返還、復元はできません。ただし、ユーザーが HRBrain を利用する際の通信ログや操作ログ、バックアップ（バックアップは、1 日 1 世代とし、7 世代分に限り保管され、その後削除されます。）、当社が利用規約に従い作成した統計データ、チャットサポート等への問合せ記録は、削除されず、適切なアクセス権のもと保管いたします。
- HRBrain の利用に関する契約が終了した後に保管し続ける各データの利用目的は以下のとおりです。
  - ○　HRBrain に関するお問い合わせ対応のため
  - ○　HRBrain のセキュリティ保護、効果測定及び品質向上のため
  - ○　HRBrain の提供、改善、開発のため
  - ○　上記の利用目的に付随する利用目的のため

4　ラベル付け機能

- お客様は、ユーザーに対して、任意の名称を付けたロール（役割）を付与することが可能です。

【ヘルプページ】
○　ロール設定について

5　利用者登録および削除

- お客様は、契約の範囲内において、いつでも自由にユーザーの登録・削除を行うことが可能です。

【ヘルプページ】
○　メンバー登録の方法
○　メンバー削除の方法

6　アクセス権の管理

- お客様は、登録したユーザーの権限を、自由に切り替えることが出来ます。組織管理者権限を付与することで、各種機能の管理画面にアクセスすることが可能です。

【ヘルプページ】
○　ロールの設定方法

7　ログイン方法

- 新規登録したユーザーがログインする方法は以下 2 通りあります。お客様は、以下の 2 通りの方法から、好きな方法を選んで、ユーザーへログイン案内を送ることが可能です。

【ヘルプページ】
○　メールアドレスの登録があるメンバーへのログイン案内方法
○　メールアドレスの登録がないメンバーへのログイン案内方法

- ユーザーは、初回ログイン時に任意のパスワードに変更することが可能です。

【ヘルプページ】
○　メンバーがログインする方法

- ユーザーはパスワードを忘れた場合、自らパスワードの再設定を行うことが可能です。

【ヘルプページ】
○　ログイン/ログイン後のパスワード変更方法

8　暗号化の状況

- データベースに保管される、本データ（ユーザーの氏名、メールアドレス、各機能で利用するデータなど）は、暗号化されずに、適切なアクセス権のもとで保管されます。ただし、データベース自体には暗号化を施しています。

- パスワードは、不可逆暗号化(ハッシュ化)された状態で、データベースに保管されます。
- 利用者の端末と、システムとの間のインターネット通信は、SSL 通信(SHA256)によって暗号化されます。
- 暗号技術を採用する際には、CRYPTREC 電子政府推奨暗号リストを参照し、安全な技術を選定しています。また、暗号輸出入(外為法等)による規制に抵触することが無いように配慮しています。

9 変更管理

- サービスのバージョンアップ情報を始めとした、各種の変更に関する情報は、ヘルプページ上のリリースノートより閲覧することが可能です。
- サービスの計画的な停止を伴うメンテナンスが実施される場合、停止日の 1 週間以内に、HRBrain サポート担当から、連絡先として当社にご提供いただいたメールアドレスに対し、メールでご連絡いたします。
- また、サービスのバージョンアップが実施された場合も同じく、連絡先として当社にご提供いただいたメールアドレスに対し、メールにてご連絡いたします。

10 手順書の提供

- 利用者向けのマニュアル・活用方法ならびによくある質問は、ヘルプページより閲覧することが可能です。

11 バックアップの状況

- 日次でシステム全体のバックアップを取得しています。このバックアップは、1 日 1 世代とし、7 世代分保管され、その後削除されます。
- バックアップデータの復元等に関する要望は、承っておりません。

12 ログのクロックに関する情報

- HRBrain における各アプリケーション内で提供されるログは、タイムゾーン JST(UTC+9)で提供されます。
- ログの時間は、GCP が提供する Google Public NTP を利用し、日本標準時と同期しています。

13 脆弱性管理に関する情報

- HRBrain 開発チームは、システムで利用している OS、ミドルウェア等に関する脆弱性情報を収集しています。
- HRBrain を構成するミドルウェア、OS、ライブラリ等については、適時にアップデートを行っており、既知の脆弱性に対応しています。
- 脆弱性対応を行う際は、テスト環境での検証を経た後、速やかに適用されます。
- 年に 1 回以上、第三者検証企業に脆弱性診断を依頼し、その結果を分析し、必要に応じた対応を実施しています。

14 開発におけるセキュリティ情報

- HRBrain の開発には、主に Go 及び TypeScript を使用しております。また、社内で定めたコーディング規約に従って開発しています。

- クラウドサービス基盤として使用されているハードウェアデバイスはすべて Google 社が管理しています。装置の処分及び再利用に関する詳細はこちらからご確認ください。

15 インシデント発生時の対応

- 利用者に大きな影響を与えるセキュリティインシデント(データの消失、長時間のシステム停止等)が発生した場合は、インシデント発生から 72 時間以内を目標に、当社に連絡先としてご提供いただいたメールアドレス又は電話番号に連絡いたします。
- 個人情報に関わるインシデントが発生した場合、当社に連絡先としてご提供いただいたメールアドレス、電話番号その他の連絡先に連絡いたします。
- 大規模なインシデント発生時には、発生原因及び対応策を連絡し、又は公表します。
- 情報セキュリティインシデント(システム障害、情報漏洩など)に関するお問い合わせは、専任のカスタマーサクセス担当、又は専用のお問い合わせ窓口より受け付けております。お問い合わせ窓口につきましては、HRBrain を契約した企業のご担当者様にお伝えをさせていただきます。なお、知的財産権侵害に関するお問い合わせは、corporate@hrbrain.co.jp にて受け付けております。

16 お客様データの保護及び第三者提供について

- 本データを適切に保護することは、当社の責任です。ログデータを含む利用者のデータは、不正なアクセスや改ざんを防ぐため、HRBrain の開発、提供に関わる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本データを含むお客様の情報の提供を要請された場合、当社は、お客様の許可なく、必要最小限の範囲で、本データを含むお客様の情報を当該外部機関に提供する可能性があります。詳細は「HRBrain 利用規約 第 22 条第 4 項」をご確認ください。

17 適用法令

- 利用者と当社との間の契約は、日本法に基づいて解釈されるものとします。

18 認証

- 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[1]を取得しています。
- 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 クラウドセキュリティ認証[2]を取得準備中です。※2024 年 3 月頃取得完了予定

【ISMS クラウドセキュリティ認証登録範囲】
HRBrain の提供に係るクラウドサービスプロバイダとしての開発、保守、運用、及び Google Cloud Platform のクラウドサービスカスタマとしての利用に係る ISMS クラウドセキュリティマネジメントシステム

[1] https://isms.jp/lst/ind/
[2] https://isms.jp/isms-cls/lst/ind/

19　外部クラウドサービスの利用

- HRBrain では、次に示す機能を運用するために、外部のクラウドサービスを利用しています。

クラウドサービス	機能	運営会社	情報
Google Cloud Platform	インフラ構築,運用	[Google Asia Pacific Pte. Ltd.]	利用者が保存等したユーザーの個人名、所属、メールアドレス、画像、PDF ファイル、評価データ等のデータ、生成されたデータ
SendGrid	メール配信	Twilio Inc.	ユーザーのメールアドレス、メール配信内容
Zendesk	ヘルプページ	Zendesk, Inc.	閲覧履歴、行動履歴、ユーザーID その他識別情報、IP アドレス
Freshchat	チャットサポート	Freshworks, Inc.	問い合わせをしたユーザーの氏名、所属先、問い合わせ内容
Thinkific	e-learning	Thinkific Labs Inc.	ユーザー氏名、メールアドレス、受講履歴
WOVEN.io	HRBrain の多言語化	Woven Technologies 株式会社	HRBrain のウェブサイトの文字データ、画像 URL、言語情報等
Sentry	フロントエンドのエラーの検知、可視化	Functional Software, Inc.	閲覧履歴、IP アドレス、ユーザーID その他識別情報、HRBrain におけるエラー状況
Datadog	サーバ、アプリケーションのエラー検知、可視化	Datadog, Inc.	閲覧履歴、IP アドレス、ユーザーID その他識別情報、HRBrain におけるエラー状況
テックタッチ	ユーザーへの通知、チュートリアル表示、利用状況の確認	テックタッチ株式会社	閲覧履歴、ユーザーID その他識別情報
Google Analytics	プロダクト及びヘルプページのアクセス解析]	Google 合同会社	[ユーザーの IP アドレス、ユーザー識別子、ログデータ]
ChatGPT(API)	生成 AI	OpenAI L.L.C.	ユーザーが該当機能に入力したデータ
eviDaemon	電子署名	セイコーソリューションズ株式会社	[電子署名を施す文書のハッシュ値等の情報]s

改訂履歴

版	改訂日	改訂内容
1.0	2023/12/01	初版発行

この資料に関するお問い合わせ

株式会社 HRBrain
HRBrain サポート担当
Email：support@hrbrain.co.jp