イーベ！
セキュリティについて

令和６年３月１日版

イーベ！運営部

セキュリティについて

1. 信頼性・安全性の高いデータセンター「AWS」を使っています

イーベ！はサービスを提供するデータセンターとして Amazon Web Services（以降、AWS）を利用しています。AWS は、全世界で利用されているオンラインショップである Amazon がもつデータセンターの設計・構築・運用のノウハウが詰まったサービスで、非常に高い信頼性と安全性を有しています。

AWS が取得している認証の詳細はこちらから

- AWS クラウドセキュリティ（https://aws.amazon.com/jp/security/#certifications）
- AWS コンプライアンス（https://aws.amazon.com/jp/compliance/）

2. 細心の注意をはらってデータを管理しています

AWS 上に構築している環境には弊社環境からのみアクセスできるように、ファイアーウォールで制限サーバーにアクセス出来るものを限定しています。 サーバーに保管されているデータには、調査が必要な場合など、お客様から依頼があった場合のみアクセスします。 その他、個人情報の取り扱いについてはプライバシーポリシーに従った運用を行っています。

3. 情報セキュリティ体制

イーベ！を運営する株式会社フラッグシステムは、ISMS（情報セキュリティマネジメントシステム）認証基準の国際規格「ISO/IEC 27001:2022」を取得しています。

4. 個人情報保護

個人情報を取り扱う際には、データを暗号化。不正アクセスや情報漏えいのリスクが低減し、利用者のプライバシー保護に努めています。

5. 外部の脆弱性診断

GMO サイバーセキュリティ by イエラエ株式会社の脆弱性診断を実施。専門家による診断結果やアドバイスを元に、最新のサイバー攻撃の手法に合わせセキュリティを強化。

6. バックアップ体制

イーベ！のすべてのデータは 1 日 1 回以上のバックアップを行い、過去 7 日間分を保存しています。障害発生や人的な操作ミス等によりデータの消失が生じた場合にも、任意の時点のデータを復元できます。

7. SSL 暗号通信採用

第三者が通信内容を確認できることがないように、イーベ！ではすべての通信を SSL によって暗号化しています。 SSL とは、インターネット上でやり取りされる情報（個人名、住所、電話番号、クレジットカード番号等）を暗号化し、安全に送受信できるようにするための通信プロトコルです。 これにより通信内容の漏えい、データの改ざん、なりすまし等を防ぎます。

8. サーバーの監視・障害対応

万が一のトラブルに備え、24 時間 365 日体制でサーバーの監視を無停止で行い、異常を検知した場合はシステム運用担当のスタッフへ即座に通知がされます。通知を受け取ったスタッフは、状況に応じて対応します。 また、平常時より障害状況に応じた対応マニュアルの整備を行い、迅速な復旧が出来る体制を整えています。

9. 障害・メンテナンス情報

計画的なメンテナンス実施は、原則 2 週間以前に、イーベ！内（ログイン後の管理画面等）や登録者宛のメールでお知らせいたします。 障害発生時は「障害・メンテナンス情報（https://news.event-form.jp/news-list/）」から確認いただけます。

10. クレジットカード情報の管理

イーベ！フォームを介したクレジットカード決済は、決済代行サービス Stripe（ストライプジャパン株式会社）と PG マルチペイメントサービス（GMO ペイメントゲートウェイ株式会社）を採用しています。 決済時に入力するクレジットカード情報などはそれぞれのサービスに保存されるため、イーベ！は一切保持しません。

- Stripe のセキュリティについて（https://stripe.com/docs/security）
- PG マルチペイメントサービスのセキュリティについて（https://www.gmo-pg.com/service/mulpay/security/）

11.登録情報の安全

イーベ！を介して登録があった個人情報への広告、流用はありません。

12.1 通ずつメール送信。丁寧な配信

メール送信では、CC・BCC と違い 1 通ずつ配信しているため、メールから他の受信者のアドレスが漏洩することはありません。

13.不正メール対策に「DMARC（ディーマーク）」を採用

イーベ！では、不正メール対策に DMARC（Domain-based Message Authentication,

Reporting, and Conformance）を採用しています。 DMARC とは、電子メールにおける「ドメイン認証」の一つで、メールを送受信する際、フィッシング攻撃や改ざん、なりすましなどの不正を防止するために開発されたセキュリティに関する技術です。 送信元の IP アドレスの信頼性を判断する「SPF」と、メールの改ざんの有無を検証する「DKIM」の両者の認証結果を活用しています。

14.管理者ログイン IP の設定

ログイン可能な IP アドレスを設定をすることで不正ログインを防ぎます。リモートワーク中などの安全な情報管理対策となります。

15.2 段階認証、Google Authenticator 採用

ログイン時のメール通知、2 段階認証としてメール認証、もしくは Google 認証システム・Google Authenticator を採用しています。

16.セキュリティチェックシートの提供

イーベ！では経済産業省による「クラウドサービスレベルのチェックリスト」、及び 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を提供しています。また、OWASP Top 10（2021 年版）のリスクに対する対応策も公開しています。導入をご検討の際にご活用ください。

- セキュリティチェックシートについて（https://news.event-form.jp/security_ck_sheet/）

お客様独自のチェックリストへの回答をご希望の場合は、有料にて対応させていただいております。 まずは お問い合わせ（https://www.event-form.jp/inquiry）ください。