Crepo パッケージデザイン AI

クラウドセキュリティ

ホワイトペーパー

第 1.0 版

株式会社プラグ

目次

I. 目的

セキュリティホワイトペーパー（以下本書）は、ISMS（情報セキュリティマネジメントシステム）のクラウドセキュリティ認証である「ISO/IEC 27017：2015」で求められている要求事項の中で、株式会社プラグ(以下、当組織という)がお客様に対し提供しているセキュリティの取組みについて明確にし、ご確認いただくことを目的としています。

- ISO/IEC 27017 について

  ISO/IEC 27017 は、クラウドサービスの提供及び利用に適用できる情報セキュリティ管理策のための指針を示した国際規格です。

  クラウドサービスに関する情報セキュリティ管理策の実践の規範として、ISO/IEC 27017 で、情報セキュリティ全般に関するマネジメントシステム規格 ISO/IEC 27001 の取り組みを強化します。これにより、クラウドサービスにも対応した情報セキュリティ管理体制を構築し、その実践を支援します。

II. 適用範囲について

当社の ISO/IEC 27017 の適用範囲は、以下のサービス内容に対するものです。

Crepo（クレポ）　パッケージデザイン AI

https://hp.package-ai.jp/

お問い合わせの窓口

お問い合わせサポート

- 電話：03-5577-7850
- メール：plugai@plug-inc.jp
- 営業時間：平日 9:00 ～ 18:00

用語について

本書では ISO/IEC 27017:2015 (JIS Q 27017:2016)で記されている用語については、そのまま使用しています。本サービスで利用している用語については、利用規約にてご確認いただけます。

III.ISO/IEC 27017:2015 (JIS Q 27017:2016) への対応

以下に ISO/IEC 27017:2015 (JIS Q27017:2016)が求める要求事項に対する管理策を記載します。番号・タイトルは、ISO/IEC 27017 が求める「情報セキュリティ管理策の実践の規範」 5～18（17 を除く）の小項目番号・要求事項原文を示しています。

5　情報セキュリティ方針のための方針群

5.1　情報セキュリティのための経営陣の方向性

5.1.1 情報セキュリティのための方針群

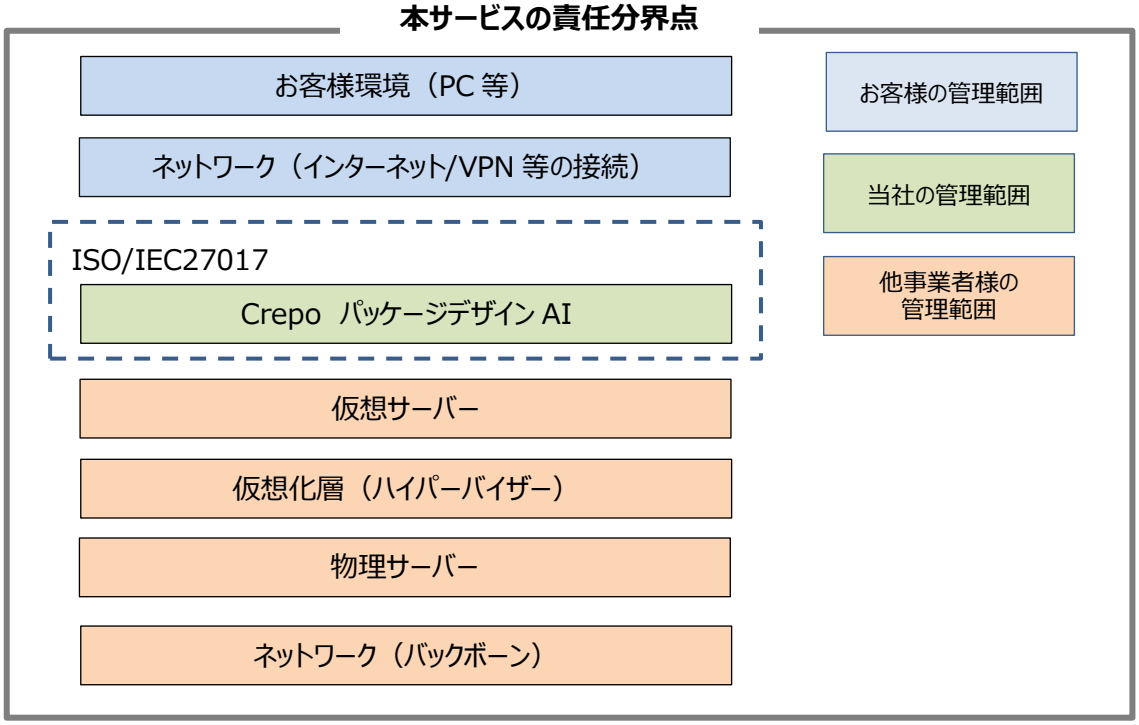
クラウドサービスプロバイダ(CSP)は、 クラウドサービスの提供および利用に取り組むため、情報セキュリティ方針を拡充することが求められています。本サービスでは、当社の情報セキュリティ方針並びにクラウドサービス情報セキュリティ方針に従いサービスを運用しています。

6 情報セキュリティのための組織

6.1 内部組織

6.1.1 情報セキュリティの役割および責任

情報セキュリティの役割および責任について利用規約に定め、サービスを提供しています。本サービスにおける責任分界点は下図のとおりです。



6.1.3 関係当局との連絡

当社所在地は、東京都千代田区神田神保町 1-3-5 冨山房ビル 3F となります。また、クラウドサービス上に保存されるデータの所在は日本国内（東京）になります。

CLD.6.3　クラウドサービスカスタマとクラウドサービスプロバイダとの関係

CLD.6.3.1 クラウドコンピューティング環境における役割および責任の共有および分担

情報セキュリティの役割および責任について利用規約に定め、サービスを提供しています。本サービスの責任分界点に関しては「6.1.1 情報セキュリティの役割および責任」をご参照下さい。

7 人的資源のセキュリティ

7.2 雇用期間中

7.2.2 情報セキュリティの意識向上、教育および訓練

本サービスのセキュリティ要件及びクラウドサービスの運営ルール徹底を目的として、サービスに従事する要員を対象とした教育・訓練および意識向上の策を実施しています。

8 資産の管理

8.1 資産に対する責任

8.1.1 資産目録

利用者の情報資産(保存データ)とサービス提供者が運営するための情報資産は情報資産台帳上で明確に識別の上分離しています。

なお、本サービスに利用者が作成・保存する情報資産は、利用者の管理範囲となります。

CLD.8.1.5 クラウドサービス利用者の資産の除去

利用者が本サービスの利用を停止または終了したい場合、利用者は当社へ連絡する必要があります。その連絡を受け、当社は速やかに、利用者が本サービスに登録した情報や、登録した情報等を含む書面及びその複製物に対し、削除します。

8.2 情報の分類

8.2.2 情報のラベル付け

本サービスをご利用いただくにあたり、お客様はプロダクトコードをラベル付け機能として利用し、対象案件を識別することができます。

9 アクセス制御

9.2 利用者アクセスの管理

9.2.1 利用者登録および削除

利用者登録は自身でシステム上および管理者権限を有するアカウントにて、利用者削除は管理者権限を有するアカウントにて、ご利用頂けます。詳細は、弊社営業・サポート担当者までお問い合わせください。

9.2.2 利用者アクセスの提供(provisioning)

本サービスでは、権限に応じて参照範囲や機能実行範囲を定めるための権限管理機能を提供しています。

9.2.3 特権的アクセス権の管理

特権的アクセス権は管理者アカウントが該当いたします。当該権限の利用においては、メールアドレス、パスワード、ワンタイムパスワード（SMS）により認証し、セキュリティを確保しています。アカウントは自己の責任で適切に管理をお願いします。

9.2.4 利用者の秘密認証情報の管理

新規登録後の初回利用時は、ご自身で決めたパスワードにてログインできます。管理者権限にて追加したユーザーの場合は、担当よりご案内いたします。パスワードはログイン後、お客様のパスワードポリシーに従って設定・変更いただくことが可能です。

9.4 システム及び業務用ソフトウェアのアクセス制御

9.4.1 情報へのアクセス制限

本サービスのご利用にあたっては、ユーザー設定メニューの権限設定機能により情報へのアクセス制限を行うことができます。

9.4.4 特権的なユーティリティプログラムの使用

利用者に対し、セキュリティ手順を回避し各種サービス機能の利用を可能とする API 等のユーティリティプログラムの提供は行っておりません。

また、当組織にて運用保守のために保持する特権的ユーティリティプログラムについては、利用者を厳しく限定し、ログによるレビューを実施しております。

CLD.9.5 共有する仮想環境におけるクラウドサービスカスタマデータのアクセス制御

CLD.9.5.1 仮想コンピューティング環境における分離

本サービスはマルチテナント環境で動作し、データベースをスキーマ分割することにより資源の分離を実施しています。

CLD.9.5.2 仮想マシンの要塞化

構築するすべての仮想化環境は、当社の開発・構築ルールに従ってセキュリティ要件を決定し、ポート・プロトコルへの制限を実施し、不正アクセスを遮断して適切にログを保存しています。

10 暗号

10.1 暗号による管理策

10.1.1 暗号による管理策の利用方針

本サービスでは以下の暗号化を実施しております。

ストレージ：Amazon S3 managed keys(SSE-S3)

データベース：AWS Key Management Service(KMS)

通信：SSL/TLS（TLS1.3 / SHA-256 With RSA）

なお、お客様のデータについてはお客様にて選定した暗号化ツールを利用可能です。

11 物理的及び環境的セキュリティ

11.2 装置

11.2.7 装置のセキュリティを保った処分又は再利用

機器の老朽化、故障等により交換した機器媒体の処理については、当社では

直接装置の処分を行うことはありません。AWS の施設、建物、および物理上のセキュリティに基づきます。
https://aws.amazon.com/jp/blogs/news/data_disposal/

12 運用のセキュリティ

12.1 運用の手順及び責任

12.1.2 変更管理

提供するサービスの更新や定期メンテナンスを実施する場合、原則 1 週間前までにログイン後の画面にて通知させていただきます。

12.1.3 容量・能力の管理

安定的なサービス提供を行うため、各サーバーのリソースを監視し、必要に応じてキャパシティの増強を行っています。

CLD.12.1.5 実務管理者の運用のセキュリティ

本サービス操作方法は、弊社営業・サポート担当より、お客様にご案内しており、改訂された場合には都度お知らせいたします。

12.3 バックアップ

12.3.1 情報のバックアップ

本サービスではバックアップ機能は提供しておらず、お客様の責任でデータエクスポートを行う等で実施いただきます。

なお、当社内部ではバックアップ・リカバリ設計に基づくバックアップを実施しております。

12.4 ログ取得及び監視

12.4.1 イベントログ取得

本サービスではお客様にアクセスログの取得機能を提供しております。マイページ画面にてご確認ください。

当社側でアクセスログの追跡はできかねますので、お客様ご自身で管理をお願い致します。

12.4.4 クロックの同期

本サービスでは AWS が指定する NTP サーバーを参照することで時刻を同

期しています。同期の仕様については、以下を参照。
https://aws.amazon.com/jp/blogs/news/keeping-time-with-amazon-time-sync-service/

CLD.12.4.5 クラウドサービスの監視

本サービスでは、開発・構築時に監視要件を決定し、実装しております。お客様においてはアクセスログの取得によりアクセス監視を実施することができます。

12.6 技術的脆弱性管理

12.6.1 技術的脆弱性の管理

当社は、担当部署および監視サービス委託会社にて脆弱性情報を収集し、評価し、対応しております。お客様への影響がある場合には、ログイン後の画面にてお知らせいたします。

13 通信のセキュリティ

13.1 ネットワークセキュリティ管理

13.1.3 ネットワークの分離

本サービスでは、開発・構築時に NW セキュリティ要件を決定し、用途別にネットワークを分離しております。

14 システムの取得、開発及び保守

14.1 情報システムのセキュリティ要求事項

14.1.1 情報セキュリティ要求事項の分析および仕様化

当社で定めている「AWS 利用ガイドライン」の基準に従い、サービスの設計・開発・構築時にセキュリティ要件を決定し、実装しております。
主にお客様が検討される情報セキュリティの機能の仕様として、当ホワイトペーパーは以下の項目を記載しています。

- アクセス制限機能（9.4.1 情報へのアクセス制限、CLD.9.5.2 仮想マシンの要塞化）
- 通信暗号化機能（10.1.1 暗号による管理策の利用方針）
- ログ取得機能（12.4.1 イベントログ取得）

14.2 開発及びサポートプロセスにおけるセキュリティ

14.2.1 セキュリティに配慮した開発のための方針

当社では、セキュリティに配慮した開発方針として「セキュリティ・バイ・デザイン」の原則に則り、当社の「AWS 利用ガイドライン」の基準に従って開発時点からセキュリティに関するリスク対応、脆弱性対応を行っています。

15 供給者関係

15.1 供給者関係における情報セキュリティ

15.1.2 供給者との合意におけるセキュリティの取扱い

本サービスにおける役割及び責任については、利用規約に定め、サービスを提供します。本サービスの責任分界点に関しては「6.1.1 情報セキュリティの役割および責任」をご参照下さい。

15.1.3 ICT サプライチェーン

当社が利用するクラウドサービスプロバイダの情報セキュリティ水準を把握し、本サービスの情報セキュリティとの整合性が取れていることを確認しています。

本サービスは、AWS をクラウドサービスプロバイダとして運用しています。AWS のコンプライアンス状況については下記をご参照下さい
https://aws.amazon.com/jp/compliance/

16 情報セキュリティインシデント管理

16.1 情報セキュリティインシデントの管理及びその改善

16.1.1 責任および手順

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、インシデントの発生を確認してから 翌営業日以内を目標に、全体的なインシデントの場合には、本サービスログイン後のお知らせ、またはメールで通知いたします。特定のお客様に生じたインシデントの場合には、メールおよびお電話にて通知いたします。
セキュリティインシデントに関する問合せは、本サービスお問い合わせサポートより受け付けています。

16.1.2 情報セキュリティ事象の報告

本サービスログイン後のお知らせ、またはメールで通知いたします。

また個別のお問い合わせは、本サービスお問い合わせサポートより受付けています。

16.1.7 証拠の収集

裁判所からの開示請求など、法律に基づいた正当な開示請求が行われた場合、お客様の同意なく、利用者のデータを当該機関に開示することがあります。詳細は、本サービス利用規約をご確認ください。なお、お客様に重要なインシデントが発生し、実態調査を目的としたログ情報等が必要な場合には本サービスお問い合わせサポートまでお問い合わせください。

18 順守

18.1 法的及び契約上の要求事項の順守目的

18.1.1 適用法令および契約上の要求事項の特定

本サービスの利用に関して適用される「準拠法」は「日本法」となります。本サービス運用に関連する各種法令に関しては法規制管理台帳を作成し、準拠するように努めています。

18.1.2 知的財産権

本サービスをご利用いただく上で知的財産権に関わるお問い合わせは、本サービスお問い合わせサポートまでお問い合わせ下さい。

18.1.3 記録の保護

利用者の本サービスご利用に関して蓄積された記録に対しては不正アクセス・改ざんなどを防ぐためアクセス制限を実施しています。

18.1.5 暗号化機能に対する規制

本サービスでは 各種暗号化機能を利用しています。 （10.1.1 参照）なお、輸出規制の対象となる暗号化の利用はありません。

18.2 情報セキュリティのレビュー

18.2.1 情報セキュリティの独立したレビュー

当社では、社内内部監査、マネジメントレビュー、年度リスクアセスメントの実施に加え、ISO/IEC 27001、ISO/IEC27017 に基づく第三者による認証審

査を受け、情報セキュリティに対する取り組みを行うことで、安全なセキュリティレベルを確保します。（初回認証審査は 2026 年 3 月を予定）

IV. 変更履歴

版	日付	改訂内容
第 1.0 版	2025/12/2	初版作成

以上