重要ファイル転送プラットフォーム「Kozutumi」

クラウドセキュリティホワイトペーパー

－第 1 版－

文書番号:ISMS230101-024-01

2023/01/01

株式会社ハートビーツ

目　　次

1. はじめに

1.1. 本ホワイトペーパーについて

本ホワイトペーパー（以下、本書）は、ISMS クラウドセキュリティ認証規格であるJIS Q 27017：2016（ISO/IEC 27017：2015）で求められている要求事項の中で、特に利用者様（以下、ユーザー。下記参照）に向けて情報開示が求められている事項について、株式会社ハートビーツ（以下、当社）が提供するクラウドサービス（以下、本サービス）における当社の情報セキュリティへの取り組みを確認して頂くことを目的としています。

また、本書の本文中に登場する人格などについては、下記のように表記いたします。

- ユーザー：別紙利用規約に基づいて本サービスの利用者として登録がなされた個人、団体または法人
- 組織：ユーザーが所属するグループの総称
- 管理者：組織を管理している、管理者権限のあるユーザー
- 一般ユーザー：管理者以外のユーザー

1.2. 本書の適用範囲について

当社が提供する、重要ファイル転送プラットフォーム「Kozutumi」が、本書の適用範囲です。

1.3. JIS Q 27017：2016（ISO/IEC 27017：2015）について

JIS Q 27017：2016（ISO/IEC 27017：2015）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為の指針を示した国際的な第三者認証規格です。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、JIS Q 27017：2016（ISO/IEC 27017：2015）認証の維持・向上により、安全かつ安定したクラウドサービスの提供を実現して参ります。

1.4. 本書で使用する管理策の表記について

本書は、JIS Q 27017：2016（ISO/IEC 27017：2015）で記されている管理策については、改変せずに使用しております。

2. 本サービスの管理策への取り組み

当社が提供する本サービスにおけるJIS Q 27017:2016(ISO/IEC 27017:2015)の定める管理策への取り組みは以下の通りです。

2.1. A.5.1.1 情報セキュリティのための方針群

本サービスは、当社が定めた「情報セキュリティ基本方針」に従い、情報セキュリティに関して最も重要な事項として取り扱い、ユーザーの情報資産（ユーザーが保存されるデータ）を情報セキュリティ上の脅威から保護する為の施策を講じ、機能的でセキュアなサービスの提供・運営を目指しています。
また、当社がサービス提供の為に利用するクラウドサービスに関しては、当社のセキュリティ要求事項を満たしている事を検証し、安全なクラウドコンピューティング環境を実現しています。

2.2. A.6.1.1 情報セキュリティの役割及び責任

本サービスは、管理範囲における情報セキュリティの役割及び責任について図 1 に示すように定め、サービスの提供・運営を行います。

図 1. 本サービスの責任分界点

2.3.　A.6.1.3 関係当局との連絡

当社の所在地など会社概要に関しては、当社ウェブサイトにてご確認下さい。「https://heartbeats.jp/」
また、本サービスにて保存されるデータの所在地は、日本国内のデータセンターです。

2.4.　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及び責任の共有及び分担

本サービスは、サービスの提供関係における役割と責任について利用規約に定めサービスの提供・運営を行います。
また、本サービスの責任分界点に関しては、上記「2.2. A.6.1.1 情報セキュリティの役割及び責任」をご参照ください。

2.5.　A.7.2.2 情報セキュリティの意識向上、教育及び訓練

本サービスに携わる当社サービス運営担当者に対し、教育・訓練の計画を策定し実施しております。
また、実施結果に基づき理解度を評価し、必要に応じて再教育・再訓練を行い、情報セキュリティに関する更なる理解向上に努めております。

2.6.　A.8.1.1 資産目録

本サービスでは、ユーザーの情報資産（ユーザーが保存されるデータ）と当社がサービスを運営する為の情報を、明確に分離しています。
なお、ユーザーの情報資産に関しては、ユーザーの管理範囲となります。

2.7.　CLD.8.1.5 クラウドサービスカスタマの資産の除去

ユーザーの情報資産（ユーザーが保存されるデータ）は、ご利用が終了後、速やかに廃棄いたします。
ただし、ユーザーの情報資産を含まない、ログなどの当社が本サービス運営に必要であると判断した情報は対象外といたします。

2.8.　A.8.2.2 情報のラベル付け

本サービスでは、サービスコードにてユーザーごとの識別及びユーザーの情報資産（ユーザーが保存されるデータ）を分類しています。

2.9.　A.9.2.1 利用者登録及び登録削除

本サービスでは、管理者が一般ユーザーのアカウントの登録・削除を行うためのユーザーインターフェース（管理画面）と機能を提供しております。

2.10. A.9.2.2 利用者アクセスの提供（プロビジョニング）

本サービスは、管理者が管理画面より一般ユーザーに対するアクセス権の設定を行うことが出来ます。
なお、ユーザー側で作成されたサービスへのアクセス権に関しては、ユーザーの定めた規定により運用して頂くこととなります。

2.11. A.9.2.3 特権的アクセス権の管理

本サービスでは、システムに対する特権的なアクセス権については当社が保有し、管理者には一般ユーザーの管理に必要な権限のみを付与しております。

2.12. A.9.2.4 利用者の秘密認証情報の管理

本サービスは、ユーザーが利用できる認証機能について利用マニュアルなどに定め提供いたします。

2.13. A.9.4.1 情報へのアクセス制限

本サービスは、管理者による一般ユーザーのアクセス権の設定を行うことができます。

2.14. A.9.4.4 特権的なユーティリティプログラムの使用

本サービスでは、特権的ユーティリティプログラム及び特権的ユーティリティプログラムを利用する当社サービス運営担当者を制限し、定期的なレビューを実施しております。
また、ユーザーに対して、特権的ユーティリティプログラムは提供しておりません。

2.15. CLD.9.5.1 仮想コンピューティング環境における分離

本サービスでは、ユーザーが別のユーザーのデータを閲覧する事が出来ない様、また当社サービス運営担当者がユーザーのデータを必要な場合を除き閲覧する事が出来ない様に適切に分離しております。

2.16. CLD.9.5.2 仮想マシンの要塞化

本サービスでは、サービス提供に必要なポート、プロトコルのみを提供しております。また、ファイル送信時のウイルス検査と定義ファイルの自動更新機能を実装しております。

2.17. A.10.1.1 暗号による管理策の利用方針

本サービスの暗号による管理策は、以下の通りです。

- 通信経路：TLS による暗号化通信
- 保存領域：FIPS140-2 準拠の暗号ストレージ

2.18. A.11.2.7 装置のセキュリティを保った処分又は再利用

本サービスでは、装置の処分及び再利用に関しては、ピアクラウドサービスプロバイダ（当社がサービス提供の為に利用するクラウドサービス提供事業者）の責任範囲であり、適切なプロセスで対応することに関する取り決めがあることを確認しております。

2.19. A.12.1.2 変更管理

本サービスは、サービス内容を変更する場合、影響のあるユーザーに対し変更内容をヘルプセンターサイト「https://support.kozutumi.com/」にてご連絡いたします。またメンテナンスを実施する際、ユーザーに影響がある場合においても同様にご連絡いたします。

2.20. A.12.1.3 容量・能力の管理
本サービスでは、安定的にサービスを提供する為、日々の稼働監視を実施しています。
また、監視・分析の結果、必要と判断された場合、適切なタイミングにてシステムメンテナンスを実施いたします。

2.21. CLD.12.1.5 実務管理者の運用のセキュリティ
本サービスでは、サービスの利用に必要な操作手順をマニュアルなどのドキュメントとして提供しています。

2.22. A.12.3.1 情報のバックアップ
本サービスでは、システムのバックアップを適切に取得・保持しております。
なお、ユーザーからのバックアップデータの復元などに関するご要望には対応しておりません。

2.23. A.12.4.1 イベントログ取得
本サービスでは、サービスの維持・管理に必要な範囲にて、適切なログを取得しています。
また、管理者へ一般ユーザーのサービス利用に関わるログの確認機能を提供しています。

2.24. A.12.4.3 実務管理者及び運用担当者の作業ログ
本サービスでは、サービス提供に関わる作業及び結果を記録し、定期的なレビューを実施しています。

2.25. A.12.4.4 クロックの同期
本サービスでは、サービス提供に必要なシステムのクロック同期を、NTP 技術を用いて実施しています。

2.26. CLD.12.4.5 クラウドサービスの監視
本サービスでは、サービス提供に必要なシステム及びログの監視を行っています。
また、管理者が一般ユーザーの利用状況を確認する機能を提供しています。

2.27. A.12.6.1 技術的脆弱性の管理
本サービスでは、脆弱性情報を収集し、収集した情報を元にサービスへの影響を評価し、当社の責任範囲において影響がある場合には速やかに対応いたします。

2.28. A.13.1.3 ネットワークの分離
本サービスでは、ユーザーが別のユーザーのデータを閲覧する事が出来ない様、また当社サービス運営担当者がユーザーのデータを必要な場合を除き閲覧する事が出来ない様に適切に分離しております。

2.29. CLD.13.1.4 仮想及び物理ネットワークのセキュリティ管理の整合
本サービスでは、物理ネットワークと仮想ネットワークの間で整合が取れなくなる様な変更作業が行えない様に、ネットワークセキュリティを管理しています。

2.30. A.14.1.1 情報セキュリティ要求事項の分析及び仕様化

本サービスで使用している主なセキュリティ機能は、以下の通りです。

・通信経路：TLS による暗号化通信
・保存領域：FIPS140-2　準拠の暗号ストレージ
・ウイルス：ファイル送信時のウイルス検査と定義ファイル自動更新

2.31. A.14.2.1 セキュリティに配慮した開発のための方針

本サービスは、当社で定めた「情報セキュリティ基本方針」に従ったセキュリティに配慮した開発を行っています。また、開発を外部に委託する際も、これに準じた契約のもと開発が行われます。
具体的には以下の活動をしながらセキュリティレベルを保つ努力をしています。

・テスト駆動開発（Test Driven Development）
・継続的インテグレーション（Continuous Integration）
・継続的デリバリー（Continuous Delivery）
・インフラのコード管理（Infrastructure as Code）
・外部セキュリティ専門家による脆弱性診断
・定期的なペアプログラミング

2.32. A.15.1.2 供給者との合意におけるセキュリティの取扱い

本サービスでは、サービスの提供環境における役割及び責任について利用規約に定め、サービスを提供いたします。本サービスの責任分界点に関しては、上記「2.2. A.6.1.1 情報セキュリティの役割及び責任」をご参照ください。
また、セキュリティ対策に関しても「図 1.本サービスの責任分界点」に記載する当社の責任範囲において、必要なセキュリティ対策を実施しています。

2.33. A.15.1.3 ICT サプライチェーン

本サービスでは、ピアクラウドサービスプロバイダ（当社がサービス提供の為に利用するクラウドサービス提供事業者）に対して当社の情報セキュリティ方針を示し、それを達成するためのリスクマネジメント活動の実施を要求するよう定めています。

2.34. A.16.1.1 責任及び手順

本サービスでは、当社が確認したセキュリティインシデントがユーザーに重大な影響を及ぼす場合、速やかにヘルプセンターサイトにて通知いたします。
また、ユーザーからのセキュリティインシデントに関するご報告・お問い合わせは、当社ヘルプセンターにてお受けいたします。

2.35. A.16.1.2 情報セキュリティ事象の報告
本サービスでは、ユーザーの責任の範囲で発生したインシデントに関しては、ヘルプセンターサイト内お問い合わせフォームにてご報告を頂き、当社のインシデント対応フローに従って対応いたします。
また、当社原因のインシデントに関しての報告は、ヘルプセンターサイトにて掲載し、ユーザーがインシデントを追跡できるようにしております。

2.36. A.16.1.7 証拠の収集
本サービスの利用に関して、法令または裁判所等の命令に基づき開示が義務付けられた情報は、ユーザーの同意なく当該機関に開示する事があります。

2.37. A.18.1.1 適用法令及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国の法令です。

2.38. A.18.1.2 知的財産権
本サービスをご利用いただく上での知的財産権に関わるご相談は、ヘルプセンターまでお問い合わせ下さい。

2.39. A.18.1.3 記録の保護
本サービスは、ユーザーのサービス利用に関連する情報に関しては、重要な記録であると区分をするとともに、適切な保護を実施いたします。

2.40. A.18.1.5 暗号化機能に対する規制
本サービスにおいて、輸出規制の対象となる暗号化の利用はありません。

2.41. A.18.2.1 情報セキュリティの独立したレビュー
当社は、JIS Q 27017:2016(ISO/IEC 27017:2015)について認定審査機関による審査を受審し、認証取得の状況を当社ウェブサイトにて公開しています。

3. 改訂履歴

・第 1 版：2023 年 1 月 1 日　初版発行