AICloud

（AITalk 声の職人クラウド版、AITalk WebAPI、AITalk Web読み職人）

コエステーション

セキュリティホワイトペーパー

第 1.0版

株式会社エーアイ

目次

1. 目的

本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、当社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。

2. 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。
・AICloud（AITalk 声の職人クラウド版、AITalk WebAPI、AITalk Web読み職人）
・コエステーション（法人向け）
※上記サービスをまとめて以下「本サービス」といいます。

＜お問い合わせの窓口：エーアイサポートデスク＞
メール：support@ai-j.jp
営業時間：平日 10:00 ～ 17:00

3. 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。各サービスで利用している用語については、各サービス利用規約でご確認いただけます。

4. 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

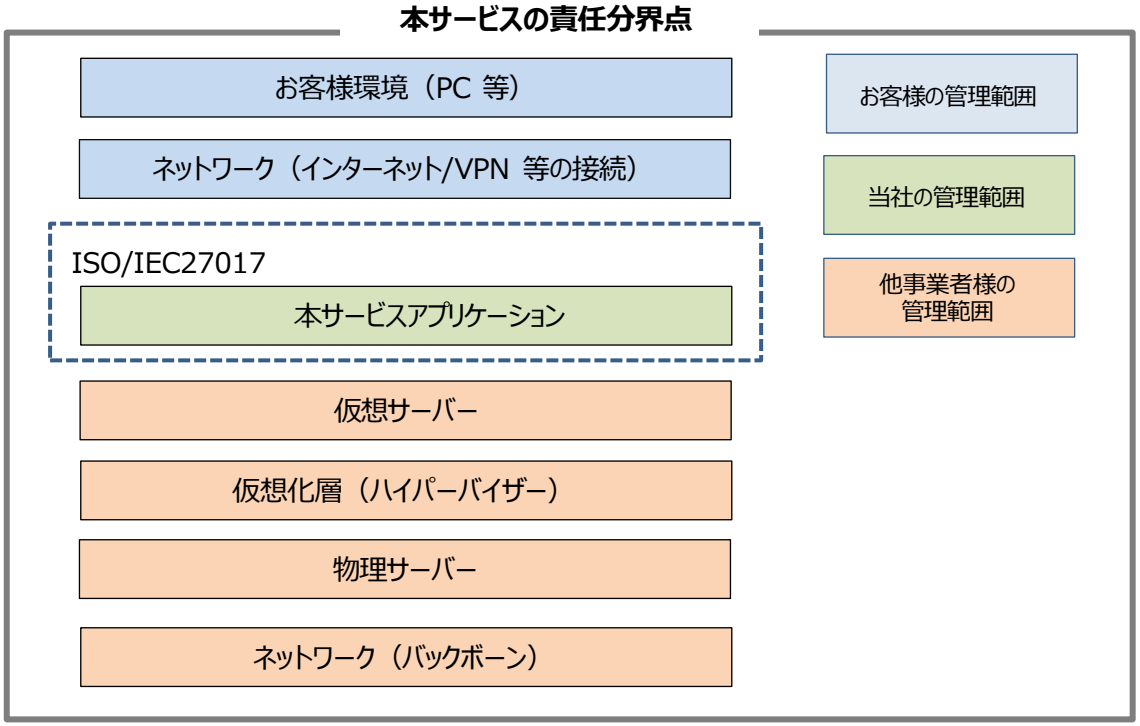
除く）の小項目番号・要求事項原文を示しています。

5.1.1 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。

6.1.1 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

本サービスに保存された情報の所在は日本国内、アメリカ合衆国（バージニア州）となります。詳細は以下の通りです。

・カスタマーデータ：利用者の情報資産(保存データ)
　日本国内
・派生データ：提供機能の設定情報、ログ 等
　アメリカ合衆国(バージニア州)

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本サービス利用規約に定め、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。

7.2.2 情報セキュリティの意識向上、教育および訓練

情報セキュリティ要件の周知徹底と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。

8.1.1 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明確に分離しています。なお、利用者が本サービスに作成・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終了した場合、当社は利用者が本サービスに登録した情報の削除を求める場合はサービス終了時にご連絡ください。

8.2.2 情報のラベル付け

本サービスにおいては、ラベル付け機能は提供しておりません。

9.2.1 利用者登録および登録削除

複数アカウントを登録可能なサービスにおいては、管理者権限を有するログイン ID にて利用者の登録・更新・削除の機能がご利用頂けます。詳細は、オンラインマニュアルにてご確認頂けます。

9.2.2 利用者アクセスの提供(provisioning)

複数アカウントを登録可能なサービスにおいては、本サービスの参照範囲や機能実行範囲を制限し、一部機能のみを利用可能とするアカウントを設定するためのサブユーザ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、複数アカウントを登録可能なサービスにおいてアカウント管理者に付与されます。アカウント管理者は、ログイン ID、パスワード認証により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

本サービスの利用申し込み後、通知されたログイン ID とパスワードを対象者へ通知してください。
パスワード変更方法は、オンラインマニュアルをご参照下さい。

9.4.1 情報へのアクセス制限

複数アカウントを登録可能なサービスにおいては、利用者管理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。

CLD.9.5.1 仮想コンピューティング環境における分離

マルチテナント環境で動作します。テナント毎の ID によるアクセス資源の分離を実施し、別テナントへのアクセス制御を実施しています。

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。

10.1.1 暗号による管理策の利用方針

本サービスのデータ(アプリケーション及びデータベースのストレージ)は暗号化を行っており、鍵の管理は AWS Key Management Service を利用しています。お客様パスワードはハッシュ化して保管しています。
本サービスにおいてお客様データをやり取りする通信は SSL/TLS（TLS1.2/TLS1.3 対応） 通信を用いて暗号化しています。

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/

12.1.2 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し、お客様の運用に影響があると判断した場合、メール又はお客様への直接連絡、HP 若しくは本サービスログイン後のお知らせのいずれかの

方法で事前に通知いたします。

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

本サービスの操作方法は、本サービスログイン後のオンラインマニュアルページにて各種マニュアルを提供しています。

12.3.1 情報のバックアップ

システムおよびお客様情報資産のバックアップは 7日間、差分バックアップにて保持しています。バックアップデータは暗号化を行い保管しています。（10.1.1 暗号による管理策の利用方針に記載の通りです。）

12.4.1 イベントログ取得

本サービスの維持管理に必要となる適切なログを取得し、最低14日以上保管しています。
また、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、アクセスログから調査を実施しますので、本サービスサポートデスクまでお問い合わせください。

12.4.4 クロックの同期

本サービスでは NTP サーバーを参照することで時刻を同期（日本標準時）しています。

CLD.12.4.5 クラウドサービスの監視

WAF や IDS 等を用いることで、不正に利用されていないことを常に監視しています。また、
CPU・メモリ・ディスクの使用率等のシステムに関するリソース状況も監視しています。

12.6.1 技術的脆弱性の管理

定期的に脆弱性情報の収集を実施し、当社の責任の範囲で対応が必要となった場合には、定期または緊急メンテナンスにて対応を実施します。
メンテナンス情報については、12.1.2 変更管理と同様の方法で通知いたします。

13.1.3 ネットワークの分離

インターネット回線を利用して本サービスへ接続し、契約 ID とログインID により論理的にセキュ

リティを確保しています。

14.1.1 情報セキュリティ要求事項の分析および仕様化

当社では、情報セキュリティ方針の下で、お客様が要求される情報セキュリティを維持、提供しています。
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、本書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）
- バックアップ機能（12.3.1 情報のバックアップ）
- ログ取得機能（12.4.1 イベントログ取得）

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、開発時点からセキュリティに関するリスク対応、脆弱性対応を行い、必要に応じて、第三者による脆弱性診断、及びネットワーク診断を行っています。

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、本サービス利用規約に定め、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/

16.1.1 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、サービスレベルに基づき通知いたします。サービスレベルについて詳細は本書別紙をご確認ください。
セキュリティインシデントに関する問合せは、本サービスサポートデスク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

情報セキュリティ事象発生時は、12.1.2 変更管理 と同様の方法で通知いたします。また個別のお問い合わせは、本サービスサポートデスク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、利用者の同意なく、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。

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関連法規管理要領に従い、法的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、本サービスサポートデスク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 SSL/TLS （TLS 1.2/TLS 1.3 対応）による通信の暗号化を使用しています。なお、輸出規制の対象となる暗号化の利用はありません。

18.2.1 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。

5. 変更履歴

版	改訂日	改訂内容
1.0	2024/10/21	初版作成

（別紙）サービスレベルについて

【サービス提供時間帯】
原則 24 時間 365 日（うるう年は 366 日）。ただし、機器の保守ならびにソフトウェアのバージョンアップ作業のため、計画停止を行なうことがあります。

【サービス停止時間帯】
計画停止。止むを得ず停止する場合は、7 日前までにメールにて指定された連絡先に通知します。

【障害監視間隔】
原則として 5 分ごとに、サーバ、ネットワーク機器、ストレージに対して生死監視を実施します。

【障害通知時間】
平日 10 時から 17 時（土・日・祝日および弊社指定の休日を除く）に生じた場合、原則として 1 時間以内に指定された連絡先に通知します。それ以外の場合、翌営業日に通知します。

【情報セキュリティインシデント通知時間】
原則として翌営業日のサポート時間内（平日 10 時から 17 時）に通知します。

以上