「JIS Q 27017:2016(ISO/IEC27017：2015) 情報技術－セキュリティ技術－
JIS Q 27002に基づくクラウドサービスのための情報セキュリティ管理策の実践の実施の規範」の主な管理策の対応状況

2021/2/3発行

クラウドコンピューティングに関する情報セキュリティ方針

当社は、クラウドコンピューティング環境におけるユーザ様の情報資産を情報セキュリティ上の脅威から保護するための措置を講じ、ユーザ様が安心してご利用いただけるセキュアなサービスを提供します。

管理策	チェック内容	結果
6.1.1 情報セキュリティの役割及び責任	クラウドサービスカスタマ、クラウドサービスプロバイダ及び供給者との間の、情報セキュリティロバイダ及び供給者との間の、情報セキュリティ情報セキュリティの役割及び責任	仮想レイヤーや施設におけるコンポーネントは、当社が基盤として利用するクラウドサービス事業者によって管理されます。当社は、基盤上に構築したアプリケーションに対して責任を負います。アプリケーション上のデータについては、ユーザ様の責任において保護していただく必要があります。 【データ　　】　利用者の管理範囲 【アプリケーション】　当社の管理範囲 【ミドルウェア　】　当社の管理下でPaaS事業者が管理を行う範囲 【ＯＳ　　】　同上 【ハードウェア　】　同上 【ファシリティ　】　同上
6.1.3　関係当局との連絡	組織の地理的所在地、カスタマデータを保存する可能性のある国	当社の所在地、並びに当社がお客様のデータを保存する国は日本国となります。
CLD6.3.1　ｸﾗｳﾄﾞｻｰﾋﾞｽｶｽﾀﾏとｸﾗｳﾄﾞｻｰﾋﾞｽﾌﾟﾛﾊﾞｲﾀﾞとの関係	当社が提供する情報セキュリティ機能、役割及び責任 クラウドサービスカスタマが実施及び管理することが必要となる情報セキュリティの役割及び責任	当社が提供する情報セキュリティ機能 ・上記の「セキュリティチェックシート」及び本チェックシートの通りです。 当社の責任 ・「AI議事録革命ログミーツサービス」のセキュリティ対策 ・「AI議事録革命ログミーツサービス」に保管されたユーザ様情報の保護 ユーザ様の責任 ・利用者アカウントの管理（登録、削除、権限設定、管理者設定、アクセス権の設定など） ・パスワード等の利用者の秘密認証情報の管理 ・利用者間での対象物の録音の許可
CLD.8.1.5　ｸﾗｳﾄﾞｻｰﾋﾞｽｶｽﾀﾏの資産の除去	クラウドサービス利用の終了時における、クラウドサービスカスタマの全ての資産の返却及び除去について	上記の「セキュリティチェックシート　40データ消去の要件」の通りです。
8.2.2　情報のラベル付け	クラウドサービスカスタマが情報及び関連資産を分類し、ラベル付けする為のサービス機能	タグ、ブックパーク、メモの挿入による機能を提供し、のデータ分類をサポートします。 使用方法の詳細は「ユーザマニュアル」をご参照ください。
9.2.1　利用者登録及び登録削除	クラウドサービスカスタマに対し、利用者登録・登録削除の機能及びそれを利用するための仕様の提供	登録用のページからアカウントの登録が出来ます。アカウントの削除については、当社のお問合せ窓口への依頼になります。 詳細は「ユーザマニュアル」をご参照ください。 また、アカウント登録・削除、権限の割り当てを行える「お客さまは管理者画面」を準備中です。
9.2.2　利用者アクセスの提供	クラウドサービスカスタマに対し、クラウドサービスユーザのアクセス権管理の為の機能及びそれを利用するための仕様の提供	同上
9.2.3　特権的アクセス権の管理	クラウドサービスカスタマのクラウドサービス実務管理者に対して、リスクに応じた充分に強い認証技術を提供する。	現状は、管理者も含め全利用者全員がID/パスワードによる認証になります。 今後は、選択による２段階認証、IPアドレス制限の導入を予定しています。
9.2.4　利用者の秘密認証情報の管理	パスワード等の秘密認証情報を割当てる手順及び利用者認証手順を含むクラウドサービスカスタマの秘密認証情報の管理手順	パスワードは命名ルールの従い、利用者による変更ができます。
10.1.1　暗号による管理策の利用方針	情報を保護するための暗号の利用環境	・ユーザデータ：上記の「セキュリティチェックシート　27データの暗号化　および　42データ保護のため暗号化要件」の通りです。 ・通信：上記の「セキュリティチェックシート　51通信の暗号化」の通りです。 ・パスワード：ハッシュ化（SHA-256）しています。
12.1.2　変更管理	クラウドサービスに悪影響を与える可能性のあるクラウドサービスの変更についての情報提供	ユーザ様に影響を与える「AI議事録革命ログミーツサービス」の変更は、メールにて通知されます。 また、サービスのWeb画面上への掲載機能を準備中です。
CLD.12.1.5　実務管理者の運用のセキュリティ	重要操作の手順提供	管理者マニュアル（準備中）を提供します！
12.3.1　情報のバックアップ	バックアップ機能の仕様	上記の「セキュリティチェックシート　37バックアップの方法、38バックアップデータを取得するタイミング、バックアップデータの保存期間」の通りです。
12.4.1　イベントログ取得	ログ取得機能の提供	上記の「セキュリティチェックシート　40データ消去の要件」の通りです。　（現状はテキストのみ） ユーザ様が必要となる場合は、当社の問合せ窓口までご相談ください。 今後は、管理者画面からのダウンロード機能の提供を予定しています。また、音声も対象となります。

管理策	チェック内容	結果
12.4.4　クロックの同期	システムで使用しているクロック及びその同期方法	基盤として利用するクラウドサービス事業者の時刻同期サービスを利用しています。 ログは、日本標準時（UTC＋９）で提供します。
CLD.12.4.5　クラウドサービスの監視	クラウドサービスの操作の監視をできるようにするサービス監視機能の提供	12.4.1　の通りです
12.6.1　技術的ぜい弱性管理	クラウドサービスカスタマに対し、提供するクラウドサービスに影響し得る技術的ぜい弱性に関する情報提供	当社では、脆弱性情報を常時収集しております。ユーザ様に影響がある脆弱性については、メールにて通知されます。また、サービスのWeb画面上への掲載機能を準備中です。
13.1.3　ネットワークの分離	マルチテナント環境においてはテナント間の分	データベースで、データリソースを別けて、各アカウント事に分離しています
14.1.1　情報セキュリティ要求事項の分析及び仕様化	クラウドサービスカスタマにカスタマが利用する情報セキュリティ機能に関する情報	上記の「セキュリティチェックシート」及び本チェックシートの通りです。
14.2.1　セキュリティに配慮した開発のための方針	使用しているセキュリティに配慮した開発の手順及び実践に関する情報	IPAの安全なWebサイトの作り方に準じて開発を行っています。
16.1.1　責任及び手順	クラウドサービスカスタマとプロバイダとの間の、情報セキュリティインシデント管理に関する割当て及び手順	**<報告する範囲>**□ データの消失、長時間のシステム停止等のユーザ様に大きな影響を及ぼす可能性のある 情報セキュリティインシデント **<対応の開示レベル>** 当社に起因する情報セキュリティインシデントでユーザ様に影響が あるものは、すべて同等のレベルで対処します。 **<通知を行う目標時間>** 検知から72時間以内を目標に通知します。 **<通知手順>** サービスのWeb画面、ご登録頂いたメールアドレス宛 （必用に応じて電話等の手段を使用する場合もあります。） **<問合せ窓口>** メールアドレス（contact@zi-ku.com）　当社のお客様担当窓口 **<適用可能な対処>** 当社に起因する情報セキュリティインシデントでユーザ様に 影響があるものは、 あらゆる手段を講じて対処します。
18.1.1　適用法令及び契約上の要求事項の特定	クラウドサービスカスタマに対し、自身の提供するクラウドサービスに適用される法域についての情報	準拠法は、日本法になります。別途、「利用規約」をご参照ください。
18.1.5　暗号化機能に対する規制	クラウドサービスに適用する暗号による管理策	暗号化の規制対象になる地域へのサービス提供はありません。
18.2.1　情報セキュリティの独立したレビュー	クラウドサービスプロバイダは、自身が主張(宣言)した情報セキュリティ管理策の実施を立証する証拠	定期的（最低でも年に一回）に情報セキュリティに関する内部監査を実施しています。 以下の認証／認定を１取得し、定期的に第三者による審査を受けています。 ・JISQ27001　ISMS認証（MSA-IS-435） ・プライバシーマーク（17003922）