「AI+予約・業務管理 ASP サービス」
セキュリティホワイトペーパー

2023/2/3（Ver4.0）

ICT ラボラトリーズ株式会社

はじめに

White Paper の目的

AI+予約・業務管理 ASP サービスは、映像・音声アプリケーションにより KIOSK 端末上においてカスタマーサポートを実現する当社のクラウドサービスです。

本ドキュメントは、AI+予約・業務管理 ASP サービスの提供において基盤として利用するクラウドサービスにおけるセキュリティに関する方針、並びにプロセスの概要をご理解いただくとともに、ISMS クラウドセキュリティ認証である ISO/IEC 27017 の要求に従う公表を行うことを目的とします。

White Paper の対象

AI+予約・業務管理 ASP サービスの導入を検討中の方
AI+予約・業務管理 ASP サービスを利用中の方

クラウドコンピューティングのための情報セキュリティ方針

当社では、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の方針を定め、ユーザ様に満足いただける機能的でセキュアなサービスの提供を目指しています。

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。

第 3 者認証

ISO/IEC27001

当社は、全社を認証範囲として 2023 年 3 月に国際規格である ISO/IEC27001（ISO/IEC 27001）ISMS 認証を取得する予定です。

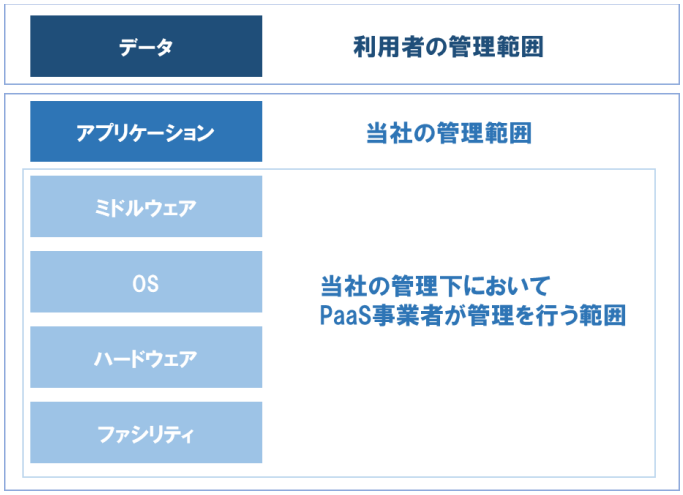
ISO/IEC27017

当社は、AI+予約・業務管理 ASP サービス「RESV」を認証範囲として 2023 年 3 月に国際規格である ISO/IEC27017（ISO/IEC 27017）ISMS クラウドセキュリティ認証を取得する予定です。

情報セキュリティのための組織(A.6)

責任分界点(A.6.1.1)

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、当社のサプライヤーに対するセキュリティポリシーに従い、調達時のセキュリティ審査、及びパフォーマンスのモニタリングによりクラウドサービス事業者を管理します。
また、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。



当社の責任
・AI+予約・業務管理 ASP サービスのセキュリティ対策
・AI+予約・業務管理 ASP 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
・お客様運運用環境情報の提出（法人名、IP アドレス、施設情報、管轄情報、端末情報）
・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

本サービスは、上記図の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本ホワイトペーパーを合意文書とし、サービスを提供します。
尚、本ホワイトペーパーは、お客様へ事前周知後、改訂する場合が有ります。

地理的所在地(A.6.1.3)

当社の所在地、並びに当社がお客さのデータを保存する国は日本国となります。当社が基盤として利用するクラウドサービスにおいて、日本国以外のリージョンにユーザ様のデータを保存する必要性が生じた場合、ユーザ様に事前に通知したうえで行います。

資産の管理 (A.8)

情報のラベル付け（A.8.2.2）

AI+予約・業務管理 ASP サービスは、基本情報として宿泊施設情報、端末情報、顧客管理者などについて当社へ事前に提出いただき、登録完了後お客様にて顧客従業員・顧客管理者を個別に名称を付与することが可能です。使用方法の詳細は「Customer Mgr マニュアル」をご参照ください。

サービス利用停止後のデータの扱い(CLD.8.1)

AI+予約・業務管理 ASP サービスで利用者様が作成・保存した利用者様のデータの除去に関して以下の方針に従い完全に消去いたします。

・30 日経過後、サービスがアクセスしている DB から消去（法人と連なるデータ（法人・施設・管轄・ユーザ））。
・7 日経過後、全ての DB バックアップからも消去。
※利用者様のデータを含まないサービス共通のアクセスログデータは、31 日経過後自動削除されます。

アクセス制御 (A.9)

利用者アクセスの管理(A.9.2.1)(A.9.2.2)

AI+予約・業務管理 ASP サービスは、ユーザ様がストレスなく、安全に利用者アクセスの管理を行うためのユーザインターフェイスと機能を提供します。お客さまは管理者画面から簡単な操作により「顧客管理者」「顧客従業員」のアカウント登録・削除を行い、またユーザに対する権限の割り当てを行うことが出来ます。使用方法の詳細は「Customer Mgr マニュアル」をご参照ください。
弊社にて、「顧客管理者」「顧客従業員」の登録は可能ですが、管理はユーザ様にて行ってください。

認証情報の管理(A.9.2.3)(A.9.2.4)

初期のアカウント登録手順は「Customer Mgr マニュアル」をご参照ください。

暗号 (A.10)

暗号化(A.10.1.1)

ユーザ様のパスワードは、そのままのコードで保存せず、不可逆のハッシュ化をしています。
AI+予約・業務管理 ASP サービスとユーザ様との間での通信は TLS1.2/1.3 で暗号化し、情

報の盗聴等のリスクに対処しています。(https://www.ssllabs.com/ssltest/index.html にて「A 評価」)

運用のセキュリティ (A.12)

変更(A.12.1.2)

ユーザ様に影響を与える AI+予約・業務管理 ASP サービスの変更は、ご指定いただいた連絡先へ事前通知します。

バックアップ(A12.3.1)

システム及びユーザ様データのバックアップは、日次で 7 世代分のデータを保持します。
ただし、ユーザ様からのバックアップデータの復元等に関するご要望には対応してせん。

ログ(A.12.4.1)(A.12.4.4)

AI+予約・業務管理 ASP サービスの維持管理に必要となる適切なログを取得しています。
サービスの利用履歴については、customermanager(顧客管理者用)以上の権限で参照することができます。確認方法の詳細は「Customer Mgr マニュアル」をご参照ください。

AI+予約・業務管理 ASP サービスは、基盤として利用する Amazon Web Services（AWS）が提供する時刻同期サービスを利用し時刻同期を行っています。
ログは、日本標準時（UTC＋９）で提供されます。

技術的脆弱性の管理(A.12.6.1)

アプリケーションを構築する上で使用するソフトウェアに脆弱性が検知された場合、ご指定いただいた連絡先へ通知をし、速やかに影響調査を行い、必要な対策を講じます。対策の状況についてもご指定いただいた連絡先へ通知をします。

管理者用手順(CLD12.1.5)

AI+予約・業務管理 ASP サービスを含むお客様の情報資産保護のため、外部から悪意ある侵入がされないよう、ネットーワークルータ等のファイアーウォールを適切に設定してください。
また、侵入を手助けや情報資産を外部に送信するツールのインストールや実行がされないよう、対策を講じてください。
それ以外の遠隔サポートの設定等に関しましては「Customer Mgr マニュアル」にてご確認いただけます。

クラウドサービスの監視(CLD12.4.5)

当社は、AI+予約・業務管理 ASP サービスの稼働状況並びに障害発生状況について監視を

行っています。
監視結果を customer manager(顧客管理者用) 以上の権限で参照することができます。参照方法の詳細は「Customer Mgr マニュアル」をご参照ください。

通信のセキュリティ (A.13)

ネットワーク(A.13.1.3)

AI+予約・業務管理 ASP サービスは、ネットワークの仮想化技術を利用して、他のユーザ様とのネットワークの分離を適切に行っています。
また、ユーザ様に提供するクラウドコンピューティング環境(商用)と、当社の開発用環境(開発・テスト)を別セグメントとして分離しています。
提供するサービスの役割は端末同士をつなげるための管理と制御を行うのみで、会話や PC の表示内容の通信は、お客様のローカルネットワーク内で行われます。

システムの取得、開発及び保守 (A.14)

情報セキュリティ機能(A.14.1.1)

主にユーザ様が検討される情報セキュリティ機能として、本ホワイトペーパーは以下を記述しています。

機能（ISO/IEC27017 の管理策）	本ホワイトペーパーの記述
A.9.2.1 利用者登録及び登録削除	利用者アクセスの管理
A.9.2.2 利用者アクセスの提供	利用者アクセスの管理
A.9.2.3 特権的アクセス権の管理	認証情報の管理
A.9.2.4 利用者の秘密認証情報の管理	認証情報の管理
A.9.4.1 情報へのアクセス制限	利用者アクセスの管理
A.10.1.1 暗号による管理策の利用方針	暗号化
A.12.3.1 情報のバックアップ	バックアップ
A.12.4.1 イベントログ取得	ログ
CLD.12.4.5 クラウドサービスの監視	クラウドサービスの監視

開発プロセス(A.14.2.1)

当社のクラウドサービスの開発は、商用とは異なる独立した開発・検証環境で行われ、機能性とユーザビリティの確保はもちろんのこと、情報セキュリティについても配慮することを方針として行われます。開発は非機能要件としてのセキュリティ要件を定義し、厳格な承認プロセスを得たうえで実施されます。セキュリティ機能に関するソースコードはレビューされ、テストプロセスを経たうえでビルドされます。
また、リリース前のみならず、リリース後も定期的な脆弱性診断を行っています。

サプライチェーン

当社のクラウドサービスの提供に関連するサプライヤー、及びサプライチェーンは以下の手段により管理することを方針としています。

・情報セキュリティ水準を当社と同等又はそれ以上に保つことを事前の審査により確実にする
・契約により秘密保持の確保を担保する
・サプライヤーがサプライチェーンを形成しサービス提供している場合、サプライヤーのサプライチェーンメンバーに対するセキュリティ管理の能力について審査する

情報セキュリティインシデントの管理 (A.16)

インシデント対応プロセス(A.16.1.1)

当社では、ISO/IEC27001 に準拠した標準化された情報セキュリティインシデント対応プロセスを整備しています。情報セキュリティインシデントに関する報告、エスカレーションに関する全ての手順が文書化され、情報セキュリティ委員会により一元的に管理されています、報告されたインシデントはインパクトや緊急性に応じてハンドリングされています。

インシデント対応

AI+予約・業務管理 ASP サービスに関連した情報セキュリティインシデントを検出した場合、以下の内容で速やかに通知します。

ギリシャ語のアルファベット

項目	内容
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	ご登録頂いたメールアドレス宛、管理者画面 （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	問合せ窓口
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。

また、ユーザ様において情報セキュリティインシデントを検出された場合、またはその疑いをもたれた場合は、当社問合せ窓口からご連絡ください。

順守 (A.18)

適用法令及び契約上の要求事項(A.18.1.1)

本サービスの利用に関して、適用される「準拠法」は日本法とします。

暗号化機能に対する規制(A.18.1.5)

AI+予約・業務管理 ASP サービスにおいて暗号化の規制対象になる地域にはサービスを提供していません。

情報セキュリティのパフォーマンス評価(A.18.2.1)

ISO/IEC27001 と ISO/IEC27017 について第三者による審査を受け、認証の取得状況を弊社ウェブサイトで公開しています。
上記認証取得に伴い、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。定期的な内部監査以外に、組織、施設、技術、プロセス等の重大な変化にあわせて、独立した内部監査を行っています。
監査結果に関しては、弊社サポートセンターまでご連絡下さい。

AI+予約・業務管理 ASP サービスに関するお問い合わせ

■ICT ラボラトリーズサポートセンター
TEL：050-3188-9763
Mail：nbs-support@ictl.jp