法人 GAI セキュリティホワイトペーパー

株式会社ギブリー

2024/06/17 初版

内容

1. 目的

当ホワイトペーパーは、株式会社ギブリー（以下「当社」）が提供するクラウドサービスである法人 GAI（以下「本サービス」）に関する情報セキュリティへの取り組みを記載したものです。
記載内容については、クラウドサービスに関する情報セキュリティの国際規格である ISO/IEC 27015:2022 において、クラウドサービス事業者が、クラウドサービス利用者に対して、開示もしくは公開を求めている事項に基づき、構成されています。
なお、各項目の末尾に記載されているカッコは、ISO/IEC 27017:2015 の該当する項番を表しています。

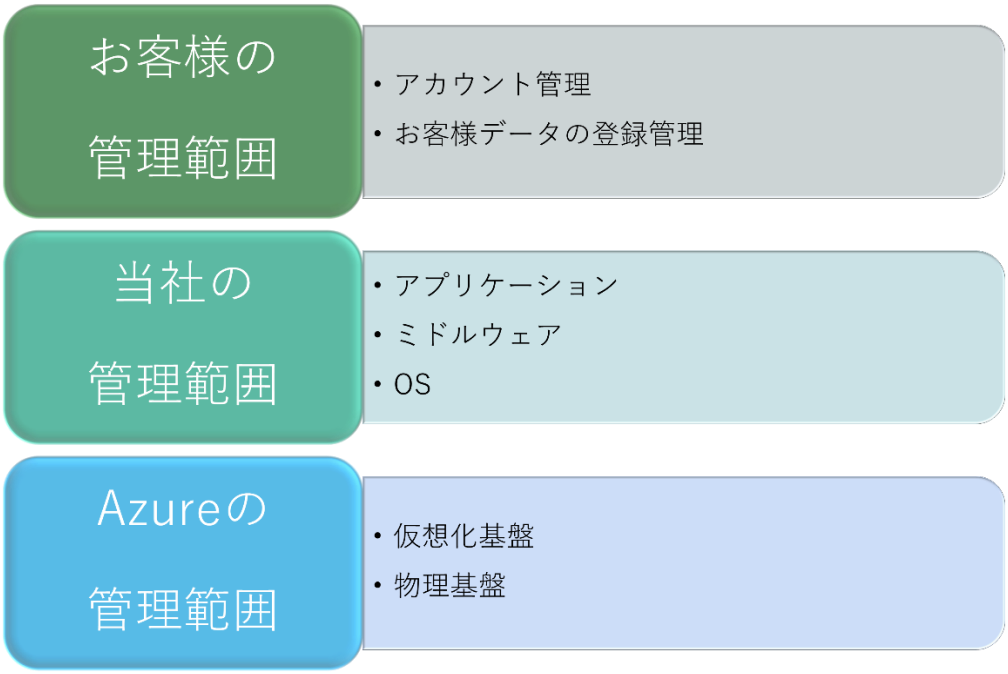
2. 情報セキュリティの取り組み

2-1 情報セキュリティのための方針群

当社は、当社の定めた情報セキュリティ方針（https://givery.co.jp/information-security/）、並びにクラウドサービス情報セキュリティポリシーを以下とし、サービス運営を行います。

2-2 情報セキュリティの役割及び責任（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）

法人 GAI では、利用規約にて契約やサービス内容を定義し、サービス提供を実施しております。法人 GAI は、Microsoft Azure（以下、Azure）を基盤にシステムを構築しており、 情報セキュリティ上の役割及び責任については、下記の責任共有モデルに基づくものとします。
また、サービスの利用契約が終了した場合、本サービス内に保管されているデータは、速やかに物理的に削除します。



責任共有モデル

2-3 関係当局との連絡

本サービスを運営する株式会社ギブリーは日本の法人であり、本店所在地は東京です。本サービスの主たるデータは、日本国内のデータセンターに保管しています。

2-4 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、サービスを提供します。

2-5 情報セキュリティの意識向上、教育及び訓練

本サービスでは、サービス運営担当者に対し、当社が定めたセキュリティ教育に加え、クラウドサービス情報セキュリティポリシーに定めた管理事項の運営に必要な教育を実施しています。

2-6 資産目録

本サービスでは、お客様の情報資産（お客様が保存されるデータ）と、当社が本サービスを運営するための情報を、明確に分離しています。なお、お客様の情報資産（お客様が保存されるデータ）に関しては、お客様の管理範囲です。

2-7 クラウドサービスカスタマの資産の除去

サービスの利用契約が終了した場合、サービス内に保管されているデータは、速やかに物理的に削除します。

2-8 情報のラベル付け

本サービスでは、以下の機能を提供し、ユーザ様のデータ分類をサポートします。
・スレッドによって情報をラベル付けして管理
使用方法の詳細はサポートサイトをご参照ください。

2-9 利用者登録及び登録削除

本サービスは、管理者と一般の登録及び削除機能を提供しております。
登録や削除の手順は、サポートサイトに記載しております。

2-10 利用者アクセスの提供

本サービスの 初期アカウントの発行は申込書へ記載されたメールアドレスを ID として、管理者を発行します。本サービスは、利用者ごとの権限設定によるアクセス制御機能について、利用者登録、変更の機能を提供しております。

2-11 特権的アクセス権の管理

本サービスでは、SSO をはじめとした、お客様のセキュリティに配慮した認証技術を提供しています。

2-12 利用者の秘密認証情報の管理

本サービスは、管理者 ID、一般 IID の登録やパスワード変更、再発行方法につきましては、サポートサイトに記載しております。

2-13 情報へのアクセス制限

本サービスは、管理権限と一般権限によって、機能制限を行うことができます。

2-14 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、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ユーティリティプログラムの提供は行っておりません。

2-15 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、アプリケーションの機能によって、各お客様の情報が論理的に分離されており、セキュリティ影響がないよう設計されています。

2-16 仮想マシンの要塞化

お客様が利用するサービスの提供に用いる仮想環境は、IP/プロトコル/ポートへのアクセス制限などを実施しています。

2-17 暗号による管理策の利用方針

本サービスのご利用において保存されるデータは、「AES-256」で暗号化され保管されます。 お客様の利用するサイトでは SSL/TLS による通信の暗号化を使用しています。

2-18 装置のセキュリティを保った処分又は再利用

本サービスは、サービスの提供に関連する機材の故障などにより交換した記憶媒体の再利用、廃棄に際し、適切なプロセスでデータの削除や設備の破壊を行います。

2-19 変更管理

本サービスは、サービスの仕様変更について利用規約に定め、サービスを提供します。

2-20 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ため、日々の稼働監視を実施しています。 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します。

2-21 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、サポートサイトとして提供しています。

2-22 情報のバックアップ

本サービスでは、サービスの提供に用いる仮想マシンのバックアップを、日次で 7 世代を取得/保持しています。

2-23 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となる適切なログを取得しています。また、管理権限を有している利用者へエンド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 実務管理者及び運用担当者の作業ログ

本サービスでは、サービスの提供に関わる作業及び結果を記録し、レビューを実施しています。

2-25 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 などの技術を用いて実施しています。

2-26 クラウドサービスの監視

本サービスでは、サービスの提供に必要なシステムおよびログの監視を行っています。 また、エンドユーザーの利用できるサービスを確認する機能を提供しています。

2-27 技術的ぜい弱性の管理

本サービスでは、ぜい弱性情報を収集し、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、速やかに対応します。

2-28 ネットワークの分離

本サービスでは、サービス運営で必要となるネットワークに関して、自社とサービス間のネットワークを分離しています。

2-29 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、Azure の機能を利用して、下記の点に従って設計しています。
・機密情報および社外秘情報が通過するネットワークの通信経路は暗号化する。
・インターネットを利用するシステムを構築または利用する場合、インターネットにおける通信は暗号化する。

2-30 情報セキュリティ要求事項の分析及び仕様化

本サービスでは、監視機能を提供しています。詳しくはお客様ごとのサービス仕様書において定義します。

2-31 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、当社にて定めた規約に則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。

2-32 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、サービスを提供します。 本サービスの責任分界点については、「情報セキュリティの役割及び責任」をご確認ください。

2-33 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 責任及び手順

本サービスは、当社が確認したセキュリティインシデントがお客様に重大な影響を及ぼす場合、確認より 24 時間以内を目標にお客様管理者様へメールにて通知を行います。 情報セキュリティインシデントに関する問合せは、お問い合わせ窓口でお受けいたします。

2-35 情報セキュリティ事象の報告

情報セキュリティ事故が発生した場合には、メールなどにて速やかに報告いたします。また、お客様からの事象報告はお問い合わせ窓口にて受け付けております。

2-36 証拠の収集

本サービスのご利用に関して、お客様責任範囲における情報セキュリティインシデントに関するログなどの証拠の収集はお客様にてご実施いただく範囲となります。
弊社責任範囲でのログなどの証拠が必要な場合は、お客様の要望に応じて個別に対応しております。都度、ご相談ください。
また、法令に基づき権限を有する公的機関から適法な手続により、開示または提供の要請があった場合は、クラウドサービスカスタマへの通知および同意を経ることなく、当該機関に情報を開示することについて合意いただく必要があります。

2-37 適用法令及び契約上の要求事項の特定

本サービスのご利用に関して、適用される準拠法は日本国の法令です。

2-38 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、当社までお問い合わせください。

2-39 記録の保護

本サービスは、クラウドサービスカスタマの契約情報の保護や廃棄については、重要な記録の区分をするとともに、管理基準を定め、適切に管理しております。

2-40 暗号化機能に対する規制

本サービスは SSL/TLS の暗号化を使用しております。なお、輸出規制の対象となる暗号化の利用はありません。

2-41 情報セキュリティの独立したレビュー

当社は、ISO/IEC 27001 と ISO/IEC 27017 について第三者による審査を受け、認証の取得状況を当社ウェブサイトで公開しています。