F1-Cloud

セキュリティホワイトペーパー

2024/08/27 第 2 版

目的

当ホワイトペーパーは、株式会社フリーダム（以下「当社」）が提供するクラウドサービスである F1-Cloud（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 27017:2015 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。

情報セキュリティの取り組み

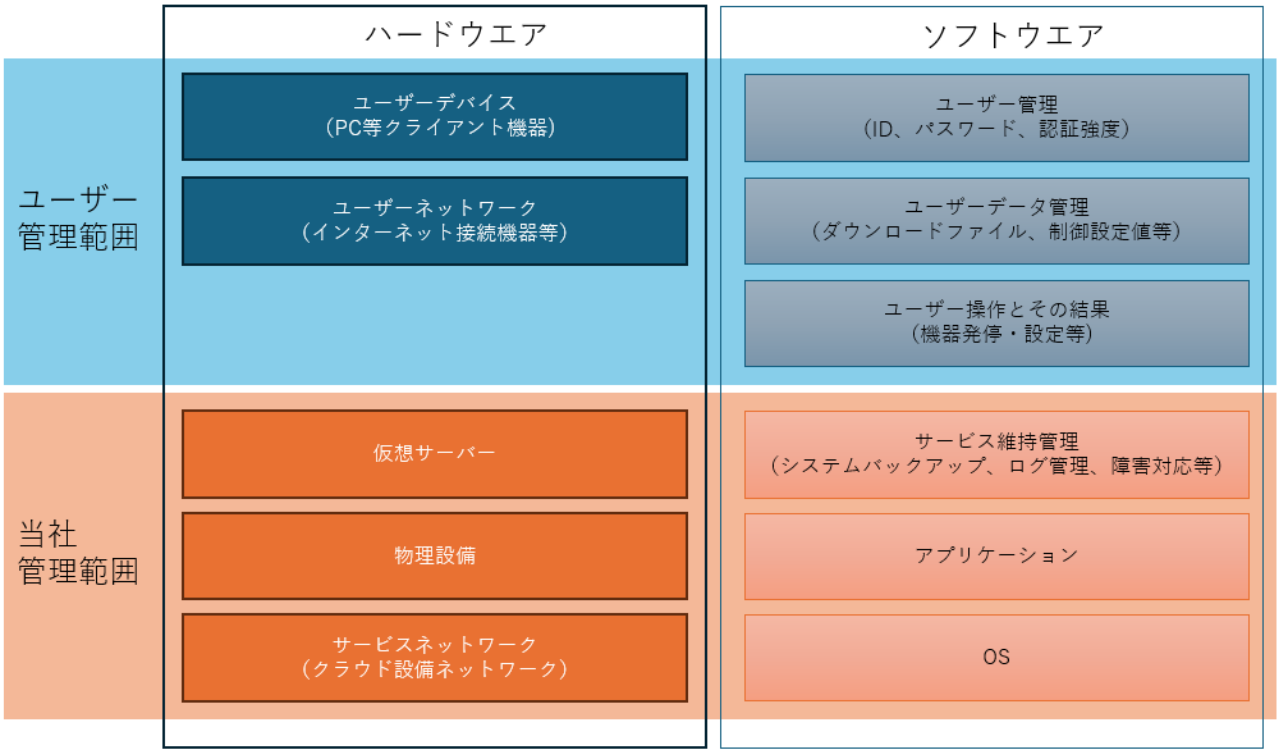
情報セキュリティのための方針群(A.5.1.1)

本サービスは、当社の定めた情報セキュリティ基本方針（https://www.frdm.co.jp/company/infomation-security に従い、サービス運営を行います。

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）(A.6.1.1)

以下に本サービスの管理範囲の概要図を示します。

本サービスは、情報セキュリティの役割及び責任について、当社の管理範囲を責任範囲とします。



関係当局との連絡(A.6.1.3)

サービス内のデータは、ユーザーからの特段の指定が無い限り、日本国内のデータセンターに保管しています。

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(CLD.6.3.1)

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。また、本サービスの責任分界点に関しては、上記「情報セキュリティの役割及び責任」をご参照ください。

情報セキュリティの意識向上、教育及び訓練(A.7.2.2)

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方針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。

資産目録(A.8.1.1)

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。

クラウドサービスカスタマの資産の除去(CLD.8.1.5)

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、利用約款に従い、速やかに削除します。

情報のラベル付け(A.8.2.2)

本サービスでは、以下の機能を提供し、ユーザーのデータ分類をサポートします。

- ユーザーが取り出すダウンロードファイルが、対象データの日付とタイトルを使ったファイル名になります
- ユーザーアカウントに対する権限を権限ロールの割当で管理できます

利用者登録及び登録削除(A.9.2.1)

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・削除を行うための機能を提供しております。登録や削除の手順は、マニュアルに記載しております。

利用者アクセスの提供(A.9.2.2)

本サービスの 初期アカウントの発行は、ユーザーの契約担当者様へ管理者権限を持つ ID 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。

特権的アクセス権の管理(A.9.2.3)

本サービスでは、多要素認証をはじめとした、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。

利用者の秘密認証情報の管理(A.9.2.4)

本サービスは、ユーザーが利用できる認証機能についてマニュアルに記載しております。

情報へのアクセス制限(A.9.4.1)

本サービスは、管理者には一般ユーザーがアクセスできる情報を管理できる権限を付与しております。

特権的なユーティリティプログラムの使用(A.9.4.4)

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。

仮想コンピューティング環境における分離(CLD.9.5.1)

本サービスでは、仮想コンピューティング環境を契約ユーザーまたは契約システムごとに分離しています。

仮想マシンの要塞化(CLD.9.5.2)

ユーザー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。

暗号による管理策の利用方針(A.10.1.1)

本サービスの通信経路では、TLS による暗号化を使用しています。

装置のセキュリティを保った処分又は再利用(A.11.2.7)

装置の処分又は再利用については、本サービス提供の為に利用する IaaS のピアクラウドサービス事業者の責任範囲であり、その事業者が NIST 800-88 で説明されている方法でメディアの処分が行われていることを確認しています。なお、IoT GW 等現地機器についてはユーザー資産であり、その処分についてもユーザーの責任範囲となります。

変更管理(A.12.1.2)

変更はユーザーの窓口担当者への事前連絡と日程調整をおこなってから実施します。

容量・能力の管理(A.12.1.3)

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。

実務管理者の運用のセキュリティ(CLD.12.1.5)

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。

情報のバックアップ(A.12.3.1)

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。

イベントログ取得(A.12.4.1)

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、ユーザー操作ログの確認機能を提供しています。

実務管理者及び運用担当者の作業ログ(A.12.4.3)

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。

クロックの同期(A.12.4.4)

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。

クラウドサービスの監視(CLD.12.4.5)

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、ユーザーがシステム状態を確認する機能を提供しています。

技術的ぜい弱性の管理(A.12.6.1)

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。

ネットワークの分離(A.13.1.3)

本サービスでは、ネットワークを契約ユーザーまたは契約システムごとに分離しています。

仮想及び物理ネットワークのセキュリティ管理の整合(CLD.13.1.4)

本サービスでは、仮想化技術やネットワークセキュリティ技術を利用し、サーバやネットワーク、ストレージをクラウドサービスカスタマごとに論理的に分離しています。

情報セキュリティ要求事項の分析及び仕様化(A.14.1.1)

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 暗号化

認証：多要素認証、証明書認証

ウイルス対策：日次のスキャン

セキュリティに配慮した開発のための方針(A.14.2.1)

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。

供給者との合意におけるセキュリティの取扱い(A.15.1.2)

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、上記「情報セキュリティの役割及び責任」をご確認ください。なお、当社管理範囲においては、必要に応じて限定されたアクセス管理をおこなっています。

ICT サプライチェーン(A.15.1.3)

本サービスでは、セキュリティ面の水準を満たしたピアクラウドサービスプロバイダを選定しています。

責任及び手順(A.16.1.1)

当社で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、確認後、営業日当日以内を目標に、ユーザーの窓口担当者にメールまたは電話にて通知します。なお、情報セキュリティインシデントに関する問い合わせは、契約ユーザーごとの担当者がお受けいたします。

情報セキュリティ事象の報告(A.16.1.2)

情報セキュリティ事故が発生した場合には、ユーザーの窓口担当者に速やかに報告いたします。また、ユーザーからの事象報告は、契約ユーザーごとの担当者がお受けいたします。

証拠の収集(A.16.1.7)

本サービスのご利用に関して、ユーザー管理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。当社管理範囲でのログなどの証拠が必要な場合は、ユーザー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、ユーザー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があります。

適用法令及び契約上の要求事項の特定(A.18.1.1)

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。

知的財産権(A.18.1.2)

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事項は、利用約款に定めています。

記録の保護(A.18.1.3)

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。

暗号化機能に対する規制(A.18.1.5)

本サービスは 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。

情報セキュリティの独立したレビュー(A.18.2.1)

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。

以上