Cloud Farm

ISO/IEC 27017 セキュリティホワイトペーパー

Innovation Farm 株式会社

2024 年 4 月 1 日（第 2.0 版）

はじめに

ホワイトペーパーの目的

「Cloud Farm ISO/IEC 27017 セキュリティホワイトペーパー」（以下、本書）は、クラウドセキュリティの国際規格 JIS Q 27017:2016(ISO/IEC27017:2015)で求める要求事項に対して Innovation　Farm 株式会社（以下、当社）クラウドサービスプロバイダが実施する管理策をご理解いただくことを目的としております。

本書の適用範囲について

当社の提供する「Cloud Farm」が、本書の適用範囲となります。

ISO27017 の概要

ISO27017 は、クラウドサービスに関する情報セキュリティ管理策のガイドライン規格です。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である ISO27001 の取り組みを ISO27017 で強化することで、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することができます。

JIS Q 27017:2016(ISO/IEC27017:2015)への対応

JIS Q 27017:2016(ISO/IEC27017:2015)が求める要求事項に対する管理策を記載します。
番号、及びタイトルは ISO27017 が求める「情報セキュリティ管理策の実践の規範“箇条 5～18（17 条を除く）の小項番番号・要求事項原文を示し、後に続く内容は、当社サービスの要求事項に対する解釈および管理策となります。

5.1.1 情報セキュリティのための方針群

当社は Cloud Farm 及び関連するサービスの提供に必要なセキュリティ水準を維持向上させるため、情報セキュリティ基本方針に加えクラウド情報セキュリティ基本方針を定めるものとします。情報セキュリティ基本方針につきましては弊社ホームページ（https://www.inn-farm.co.jp/ifinc.html）をご覧ください。クラウドサービス情報セキュリティ基本方針は下記のとおりです。

1. クラウドサービスの設計及び実装について
   お客様からの情報セキュリティ要求事項を勘案し、当社で確立した基本方針を定めクラウドサービスの設計及び実装を行います。
2. クラウドサービス内部関係者のリスクについて
   リスクアセスメントで特定されたリスクに対し、適切に管理策を作成し実施いたします。

3. クラウドコンピューティング環境の隔離
   仮想化技術を採用し、お客様毎に論理的または物理的に独立した領域を提供いたします。
4. 当社従業員によりお客様データへのアクセス
   当社は、サービス提供上の問題解決のため、または当社が定める約款に則り、お客様の領域にアクセスすることがあります。また、当社の約款に定める場合を除き、お客様の事前の許可無くお客様の資産へのアクセスは行いません。
5. 管理画面へのアクセス制御
   お客様が利用する管理画面に対し、適切な認証方式を提供いたします。
6. お客様への通知について
   クラウドサービスに関する仕様変更等の通知は、当社ホームページへの掲載を通じ情報提供いたします。
7. アカウント管理
   当社の約款に定める場合を除き、アカウント管理はお客様の責任において管理していただきます。
8. 情報共有
   インシデントに関する通知および、フォレンジック支援のための情報共有をいたします。

6.1.1 情報セキュリティの役割及び責任

当社とお客様との責任範囲につきましては、以下のとおりとなります。

6.1.3　関係当局との連絡

当社の所在地は、ホームページにて（https://www.inn-farm.co.jp/）ご確認ください。お客様のデータは、日本国内で保存されております。

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及び責任の共有及び分担

役割および責任につきましては以下のとおりとなります。

7.2.2　情報セキュリティの意識向上、教育及び訓練

弊社では情報セキュリティ方針を定め、方針に従いサービスを運営しています。また、クラウドサービスカスタマデータ及びクラウドサービス派生データを取り扱う社員に対する定期的な教育を実施しています。

8.1.1　資産目録

カスタマデータとクラウドサービス派生データは、明確に分離しています。

CLD.8.1.5　クラウドサービスカスタマの資産の除去

お客様のデータは、契約完了 60 日後に削除いたします。

8.2.2　情報のラベル付け

お客様のクラウド環境は、お客様専用の仮想環境内で分類を行うことが可能です。

9.2.1　利用登録及び登録削除

お申込書にてお申込みいただきました担当者の登録、変更、削除機能を提供しています。
登録、変更、削除に必要な手順、情報は個別メールに記載しています。

9.2.2　利用者アクセスの提供(provisioning)

お客様専用の管理画面は、お申込み受理後に発行された申込 ID 及び登録者自身が設定したパスワードでアクセスができます。

9.2.3　特権的アクセス権の管理

お客様専用の管理画面は、登録者のみが知りえる申込 ID 及び登録者自身が設定したパスワードでアクセスができます。

9.2.4　利用者の秘密認証情報の管理

お客様専用の管理画面を利用される際のパスワード登録、変更、再発行方法につきましては、個別メールに記載しています。

9.4.1　情報へのアクセス制御

クラウド環境へのアクセス情報は、特権管理者宛に発行する開通通知に記載しています。
特権管理者でユーザーの追加などを行うことが可能です。

9.4.4　特権的なユーティリティプログラムの使用

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。

CLD.9.5.1　仮想コンピューティング環境における分離

お客様の仮想環境は論理的に分離し、制御しています。

CLD.9.5.2　仮想マシンの要塞化

仮想マシンの要塞化のために、VLAN/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。

10.1.1　暗号による管理策の利用方針

本サービス利用におけるデータをやり取りする通信は、 SSL/TLS 通信を行うオプションを提供しています。

11.2.7　装置のセキュリティを保った処分又は再利用

設備を再利用、廃棄する際には適切なプロセスで、資源の削除や設備の破壊を実施しています。

12.1.2 変更管理

本サービスの利用者様に影響のある変更およびメンテナンスを実施する場合には、事前にメールもしくは WEB にて通知を行います。

12.1.3　容量・能力の管理

当社にて日々のプロセスの中で稼働監視を行っています。
また、本サービスの管理者向けに利用状況を確認する機能を提供しています。契約容量の90%を超過した際、管理者のメールアドレスに通知メールが送信される基本設定となっています。

CLD.12.1.5　実務管理者の運用のセキュリティ

サービスの操作手順は、個別にご案内いたします。

12.3.1　情報のバックアップ

お客様ご利用のサービス内容により、バックアップ環境を提供しています。

12.4.1　イベントログ取得

当社の責任範囲において、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ています。必要あればお問い合わせください。

12.4.4　クロックの同期

システムは NTP による時刻同期を行っており、日本時間(JST)で管理しています。
本サービスで記録される時刻は、すべて時刻同期に基づいて記録しています。

CLD.12.4.5　クラウドサービスの監視

ネットワークおよびCPU・メモリ等の使用率増加を検知する監視は、弊社が実施しています。 監視結果が必要となる場合、弊社サポート窓口までご連絡ください。

12.6.1　技術的ぜい弱性の管理

本サービスに影響がある技術的ぜい弱性に関する情報は、お客様管理者宛にメールで一斉通知します。

13.1.3　ネットワークの分離

他のお客様とは、物理的もしくは論理的に分離しています。

CLD.13.1.4　仮想及び物理ネットワークのセキュリティ管理の整合

当社で管理しています。

14.1.1　情報セキュリティ要求事項の分析及び仕様化

本サービスの主なセキュリティ機能は以下となります。

・ウィルスチェック機能
・ログ管理機能
・監視機能

14.2.1　セキュリティに配慮した開発のための方針

変更管理に関するプロセスを定めてサービス開発・運営を実施しています。 変更管理プロセスでは、リスクアセスメントを実施した後、サービスのリリースをしています。

15.1.2　供給者との合意におけるセキュリティの取扱い

本サービスはクラウドサービスとなり、責任分界点は、“6.1.1　情報セキュリティの役割及び責任”を参照ください。 また情報セキュリティ対策も“6.1.1　情報セキュリティの役割及び責任”の範囲において必要なセキュリティ対策を実施しています。

15.1.3　ICT サプライチェーン

当サービスは、当社利用のデータセンターに当社で環境を構築しています。当社からの委託先については。契約約款の定めにしたがい管理を行っています。また、現時点においてピアクラウドサービスプロバイダは存在しません。今後利用する場合には、同等の情報セキュリティ水準を要求するよう定めています。合わせて、サプライチェーンでクラウドサ

ービスを提供する場合は、供給者に対して情報セキュリティ目的を示し、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。

16.1.1　責任及び手順

本サービスは、当社がセキュリティインシデントを確認しお客様に重大な影響を及ぼす場合に、当社が確認した後に 4 時間以内を目標にお客様管理者様へメールにて御連絡いたします。情報セキュリティインシデントに関するお問い合わせは、個別にご案内していますサポートセンターでお受けいたします。

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故が発生した場合には、メールもしくは WEB 等にて速やかに報告します。 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います。

16.1.7　証拠の収集

法令または裁判所の命令に基づき開示が義務付けられた際、お客様への通知または同意を経ることなく開示することついて、利用規約に合意いただく必要があります。

18.1.1　適用法令及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。

18.1.2　知的財産権

知的財産権に関わるお問い合わせは、当社サポート窓口へお問い合わせください。

18.1.3　記録の保護

当社の責任範囲において、保存期間を定めログを取得しています。必要な場合は、弊社サポート窓口へお問い合わせください。

18.1.5　暗号化機能に対する規制

SSH もしくは SSL/TLS の暗号化を使用しています。

18.2.1　情報セキュリティの独立したレビュー

当社では組織的な取組として ISMS を取得しています。

改訂履歴

版数	日付	変更内容
第 1 版	2023 年 4 月 17 日	初版発行
第 1.1 版	2023 年 4 月 26 日	関係当局との連絡 クラウドサービスカスタマの資産の除去 クラウドサービスの監視 仮想及び物理ネットワークのセキュリティ管理の整合 責任及び手順 記録の保護 クラウドサービス情報セキュリティ基本方針 上記の記載を追加
第 2 版	2024 年 4 月 1 日	フォーマットの変更、及び下記項目の記述追加 ホワイトペーパーの目的 本書の適用範囲について ISO27017 の概要 JIS Q 27017:2016(ISO/IEC27017:2015)への対応 5.1.1 情報セキュリティのための方針群 7.2.2　情報セキュリティの意識向上、教育及び訓練 8.1.1　資産目録 9.2.1　利用登録及び登録削除 9.2.2　利用者アクセスの提供(provisioning) 9.2.3　特権的アクセス権の管理 9.2.4　利用者の秘密認証情報の管理 9.4.4　特権的なユーティリティプログラムの使用 CLD.9.5.2　仮想マシンの要塞化 10.1.1　暗号による管理策の利用方針 11.2.7　装置のセキュリティを保った処分又は再利用 12.1.2 変更管理 12.1.3　容量・能力の管理 12.3.1　情報のバックアップ 12.4.1　イベントログ取得 12.4.4　クロックの同期 12.6.1　技術的ぜい弱性の管理 14.1.1　情報セキュリティ要求事項の分析及び仕様化 14.2.1　セキュリティに配慮した開発のための方針 15.1.2　供給者との合意におけるセキュリティの取扱い 15.1.3　ICT サプライチェーン 16.1.2　情報セキュリティ事象の報告

		16.1.7　証拠の収集 18.1.1　適用法令及び契約上の要求事項の特定 18.1.2　知的財産権