Preferred
Computing
Infrastructure

PFCP セキュリティホワイトペーパー

ISO/IEC 27017に基づくセキュリティ要求事項への取り組み

はじめに

セキュリティホワイトペーパーの目的

この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である「ISO/IEC 27017:2015」の中で、お客様に向けた情報開示が求められている要求事項に対して、当社が提供するPreferred Computing Platform（以下、「本サービス」または「PFCP」）のクラウドセキュリティに関する取り組みをご理解いただくことを目的としています。

サービスの概要

PFCP は深層学習および AI ワークロード向けのクラウドサービスです。本サービスは、オンプレミス環境の強固な計算基盤と外部のパブリッククラウドサービスを組み合わせたハイブリッド構成を採用しており、Kubernetes を用いてワークロードを実行するための計算基盤、ストレージ、ネットワーク、ポータル、認証連携、監視機能などを提供します。

ISMSクラウドセキュリティ認証について

ISO/IEC 27017：2015とは

国際標準化機構（ISO）と国際電気標準会議（IEC）が定める情報セキュリティマネジメントの国際規格にISO/IEC 27000シリーズがあります。ISO/IEC 27017は、このシリーズのうちの１つで、2015年12月に発行されたクラウドサービスにおける情報セキュリティマネジメントのガイドライン規格になります。

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ISO/IEC 27001の取り組みをISO/IEC 27017で強化することにより、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。ISO/IEC27017 にて新たに追加されたクラウドサービス事業者向けの管理策については、本サービスでの取り組みを次項以降に記載しています。

1. 情報セキュリティのための方針群

1.1. 情報セキュリティのための方針群（ISO27017: 5.1.1）

当社は、お客様にクラウドサービスを提供するクラウドサービスプロバイダとして、情報セキュリティに関する方針（情報セキュリティポリシー）を定め、適切に運用・管理しています。

- https://www.pfci.jp/security_policy

2. 情報セキュリティのための組織

2.1. 情報セキュリティの役割及び責任（ISO27017: 6.1.1）

本サービスの利用におけるお客様と当社との役割および責任範囲は、「PFCP利用規約」および「PFCPユーザーガイド」に明記しており、同意をいただく事項となっております。なお、「PFCP利用規約」、「PFCPユーザーガイド」については、当社Webサイトにて公開しています。

2.2. 関係当局との連絡（ISO27017: 6.1.3）

当社の所在地は、当社Webサイトにてご確認いただけます。お客様が保有する情報資産のデータ保管場所は、日本国内（当社が指定する国内のデータセンター、および当社が利用するパブリッククラウドサービスの日本国内リージョン）に限定されます。

2.3. 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（ISO27017: CLD.6.3.1）

本サービスにおけるお客様と当社との責任範囲の概要（責任分界点）は、下記の通りとなります。

- お客様責任範囲: ワークロードの認証認可設定、アクセス制御設定、リソース定義およびその上層となります。
- 当社責任範囲: クラスタ管理ソフトウェアおよびその下層となります。

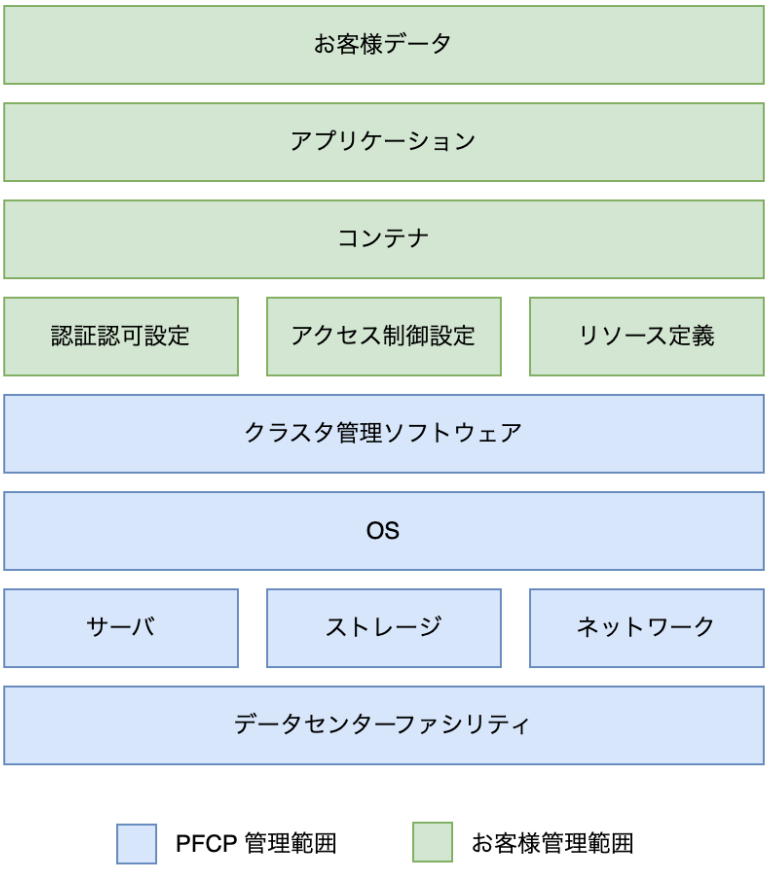

図1: 責任分界点

3. 人的資源のセキュリティ

3.1. 情報セキュリティの意識向上、教育及び訓練（ISO27017: 7.2.2）

当社の従業員がお客様の情報資産を適切に取り扱うため、定期的もしくは必要に応じて随時、情報セキュリティ教育および訓練を実施しています。

4. 資産の管理

4.1. 資産目録（ISO27017: 8.1.1）

お客様の情報資産と、当社がサービスを運営するために必要となるシステム情報資産は、論理的に明確に分離して管理しています。

4.2. クラウドサービスカスタマの資産の除去（ISO27017: CLD.8.1.5）

お客様が本サービスの利用を終了（解約）された場合、利用規約に基づき、該当テナントに関連する稼働サーバ上のデータおよびリソースを、所定のフローに従って速やかに削除いたします。

なお、システム登録情報のバックアップ（第8.3項に記載）は、解約後、最大90日間の保存期間の経過をもって完全に消去され、以降は一切の復元ができなくなります。

したがいまして、本サービスの利用終了の際は、必要に応じてお客様自身にてデータの退避等を実施してください。

4.3. 情報のラベル付け（ISO27017: 8.2.2）

本サービスは、情報資産を分類するためのラベル付け機能を提供します。利用者は、本サービスが提供する機能およびクラスタ管理ソフトウェア Kubernetes のラベル機能を用いて、データやリソースを任意に整理・分類できます。

5. アクセス制御

5.1. 利用者登録及び登録削除（ISO27017: 9.2.1）

本サービスでは、お客様が選任された組織管理者が、所属組織のユーザを任意のタイミングで招待、登録、削除できる機能を提供しています。

5.2. 利用者アクセスの提供（ISO27017: 9.2.2）

本サービスでは、利用者の職務や役割に応じて、組織管理者と一般ユーザのロール（役割）を割り当て、許可された範囲内でワークロードを実行できるアクセス管理機能を提供しています。

5.3. 特権的アクセス権の管理（ISO27017: 9.2.3）

本サービスへのログインおよび認証管理には、外部認証基盤との連携（OIDC等）によるグループ単位の管理、またはポータル上での直接管理に対応しており、管理者権限などの特権的なアクセスに対しても適切な制御を実施しています。

5.4. 利用者の秘密認証情報の管理（ISO27017: 9.2.4）

お客様（組織管理者および利用者）の責任において、本サービス利用者のアカウント情報、およびパスワードやAPIトークン等の認証情報を適切に管理していただきます。

5.5. 仮想コンピューティング環境における分離（ISO27017: CLD.9.5.1）

お客様のワークロードは、実績のあるコンテナ型の分離技術を用いて実行され、他のお客様の環境から安全に隔離されています。

5.6. 仮想マシンの要塞化（ISO27017: CLD.9.5.2）

お客様が利用する環境においては、利用ソフトウェア・サービス・開放ポートの最小化、アクセスの監視、アクセス時の認証の要求、コンテナログの取得、およびアクティビティ監視を実施し、セキュリティレベルを高めています。

6. 暗号

6.1. 暗号による管理策の利用方針（ISO27017: 10.1.1）

本サービスでは、以下のとおり暗号化によるセキュリティ対策を実施しています。

- 通信の暗号化: インターネットから本サービスへの通信（TLS）、およびオンプレミス環境とパブリッククラウド環境の間の通信は、専用線またはVPN等の暗号化された安全な通信経路を介して行われます。
- データの暗号化: ユーザ登録情報のうち機密に該当する情報、および基盤側の永続ストレージ内のデータは、業界標準の暗号化アルゴリズム（AES-256等）を用いて暗号化されています。

7. 物理的及び環境的セキュリティ

7.1. 装置のセキュリティを保った処分又は再利用（ISO27017: 11.2.7）

本サービスで利用するオンプレミス環境の物理装置を廃棄または再利用する場合は、事前にデータの完全消去手順の実施を行い、OSの再インストールや指定業者による廃棄を適切に実施します。また、当社が利用するクラウドベンダーのシステム環境におけるストレージデバイス等の装置の処分に関しては、各クラウドベンダーの廃棄プロセスに基づいて適切に実施されていることを確認しています。

8. 運用のセキュリティ

8.1. 変更管理（ISO27017: 12.1.2）

サービスに関する変更、メンテナンス、障害、脆弱性対応などの情報は「PFCPお知らせサイト」にて通知します。定期メンテナンスの方針は「メンテナンスポリシ」において開示しています。

- https://pfcomputing.com/news/
- https://docs.pfcomputing.com/maintenance-policy.html

8.2. 実務管理者の運用のセキュリティ（ISO27017: CLD.12.1.5）

本サービスでは、お客様が安全かつ適切にシステムを運用できるよう、包括的な各種手順書やガイドラインを「PFCPユーザガイド」として提供しています。

8.3. 情報のバックアップ（ISO27017: 12.3.1）

お客様の情報資産については、冗長化やバックアップの取得により、適切に保管しています。

- 永続ストレージ: レプリケーション等によるデータの冗長化を行い、またお客様ご自身が必要に応じてスナップショット機能（同一システム上に作成）を利用したバックアップが取得可能
- システム情報: ユーザが登録したシステム情報は、日次で全件バックアップを取得し、90日間安全に保持する

8.4. イベントログの取得（ISO27017: 12.4.1）

本サービス利用者の最終ログイン日時等の各種ログを取得しており、お客様のお求めに応じて、イベントログ等を提供することができます。

8.5. クロックの同期（ISO27017: 12.4.4）

本サービスで記録される時刻は、全て時刻同期に基づいて記録されます。時刻同期はクラウドベンダーもしくはOSベンダーから提供される NTP サービスを利用しています。

8.6. クラウドサービスの監視（ISO27017: CLD.12.4.5）

本サービスでは、サーバおよびネットワークの状態を常時監視しています。計算機全体の状態確認を定期的に行うとともに、異常検知時のアラート発報システムを構築しています。お客様向けの監視機能の詳細な情報は「PFCPユーザガイド」のモニタリングに関するドキュメントで提供しています。

8.7. 技術的ぜい弱性の管理（ISO27017: 12.6.1）

JPCERTや主要OSSの脆弱性情報を常時購読し、当社規定の深刻度評価に基づき影響を個別判断します。利用者への影響が大きい脆弱性については対応内容を「PFCPお知らせサイト」で報告します。

9. 通信のセキュリティ

9.1. ネットワークの分離（ISO27017: 13.1.3）

利用者が使用するネットワークは、物理ネットワークから論理的に切り離された仮想ネットワークとして提供され、他テナントや外部環境と適切に分離されています。

10. システムの取得、開発及び保守

10.1. 情報セキュリティに配慮した開発のための方針（ISO27017: 14.2.1）

開発時には、自動テストや整形ツールの利用に加え、プロセスに沿ったコードレビューを実施し、コードの潜在的なバグやパフォーマンスの問題、安全でないコーディングパターンの検出に努めています。

また、特にお客様の情報資産を取り扱う新機能をリリースする場合には、社内のセキュリティチームによるレビューを実施しています。さらに、第三者によるウェブアプリケーションのぜい弱性診断やプラットフォーム診断を実施することで、重ねて安全性を確認しています。

11. 供給者関係

11.1. 供給者との合意におけるセキュリティの取扱い（ISO27017：15.1.2）

本サービスは、SaaS型のクラウドサービスであり、責任分界点の詳細は「2.3. クラウド環境における役割及び責任の共有」をご参照ください。また、情報セキュリティ対策については当社の責任の範囲において必要な対策を実施しています。

11.1. ICT サプライチェーン（ISO27017: 15.1.3）

当社は、システムの一部にクラウドサービスベンダーが提供するクラウド環境を利用して本サービスを構築しています。

これら外部供給者の選定にあたっては、ISO/IEC 27001をはじめとする国際的なセキュリティ認証の取得状況や、当社のセキュリティ基準を満たしていることを事前に評価しています。また、選定後も年1回の定期的な見直しを実施することで、サプライチェーン全体における適切なリスク管理を徹底しています。

12. 情報セキュリティインシデント管理

12.1. 責任及び手順（ISO27017: 16.1.1）

当社の責任範囲において重大な情報セキュリティ事象（お客様情報の漏えい等）を検知した場合には、当社が定めるインシデント対応手順に基づき、速やか、かつ適切に対応いたします。

12.2. 情報セキュリティ事象の報告（ISO27017: 16.1.2）

当社の責任範囲において情報セキュリティ事象が発生した場合には「PFCPお知らせサイト」にてお客様に報告します。また、お客様が本サービスに関する情報セキュリティ事象を発見された場合には、PFCP ポータル画面のお問い合わせ窓口からご連絡いただけます。

12.3. 証拠の収集（ISO27017: 16.1.7）

当社の責任範囲において情報セキュリティ事象が発生した結果、法的処置が取られる可能性があると判断した場合には、記録、証拠の保全を行い、お客様の情報資産を第三者に開示することがあります。

13. 順守

13.1. 適用法令及び契約上の要求事項の特定（ISO27017: 18.1.1）

本サービスの利用における適用法令は「PFCP利用規約 第49条」において、準拠法を日本法と定めています。また、本サービスを提供する国・地域の法域に該当する法規制を特定し、順守しています。

13.2. 知的財産権（ISO27017: 18.1.2）

本サービスの利用における準拠法、管轄裁判所、およびお客様データの権利（知的財産権）の取り扱いについては、「PFCP利用規約」において明確に定めています。

13.3. 記録の保護（ISO27017: 18.1.3）

情報セキュリティに関係する重要な記録は、法令、規制、契約及び事業上の要求事項に従い、消失、破壊、改竄がないよう、適切に管理しています。

13.4. 暗号化機能に対する規制（ISO27017: 18.1.5）

暗号化機能は、外国為替及び外国貿易法等の関連する法令及び規制を順守しています。

13.5. 情報セキュリティの独立したレビュー（ISO27017: 18.2.1）

本サービスは、ISO/IEC 27001 および ISO/IEC 27017 の認証取得に向けた情報セキュリティマネジメントシステム（ISMS）を構築・維持しており、第三者機関による独立したレビュー（審査）を受けることで、その客観的な安全性を担保しています。