BroadCenter Pracla

ホステッド・プライベートクラウド

ISO/IEC 27017 ホワイトペーパー

株式会社 TOKAI コミュニケーションズ

2022 年 3 月 18 日（1.1 版）

もくじ

内容

はじめに

ホワイトペーパーの目的

このホワイトペーパー（以下、本書）は、ISMS クラウドセキュリティ認証である、「JIP-ISMS517-1.0（ISO/IEC 27017:2015）」で求められている要求事項の中で、特に利用者に向けての情報開示が求められている事項について、BroadCenter Pracla ホステッド・プライベートクラウド（以下、Pracla）におけるセキュリティの取り組みを確認いただくことを目的としています。
また、Pracla を利用して、独自のクラウドサービスを展開されているご利用者様（以下、クラウドサービスカスタマ）において、『ISMS クラウドセキュリティ認証（JIP-ISMS517-1.0）』もしくは、『ISO/IEC 27017 の適合審査』の認証取得を検討されている場合に必要となる情報をご確認いただくことができます。

これらは、ISO/IEC 27017:2015「箇条 4.3 クラウドサービスカスタマとクラウドサービスプロバイダとの関係」に定められている『クラウドサービスプロバイダは，クラウドサービスカスタマがその情報セキュリティ要求事項を満たすために必要な情報及び技術支援を提供することが望ましい。』への対応となります。

なお、Pracla の最新情報については、当社営業までご相談いただくか、サービス Web サイトをご確認ください。
Pracla ｜ BroadCenter

本書の適用範囲について

Pracla が本書の適用範囲となります。

本書で使用する用語について

本書は、JIP-ISMS517-1.0、ISO/IEC 27017:2015 および JIS Q 27017:2016 で記されている用語については、改変せずに使用しております。

ISMS クラウドセキュリティ認証について

ISMS クラウドセキュリティ認証 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に関する国際規格である ISMS（ISO/IEC 27001:2013）認証に加えて、クラウドサービス固有の管理策（ISO/IEC 27017）が適切に導入、実施されていることを証明するものです。

Pracla について

Pracla について

Pracla は、パブリッククラウドに分類される IaaS（Infrastructure as a Service）のサービスです。

責任分界点について

Pracla に関する責任分界点は、以下のようになります。

※仮想マシンの構築・設定など、管理機能の利用については、お客様の責任範囲となります。
※仮想環境管理の「低」は専用物理サーバなど物理層の管理を指し、「高」は仮想マシンや仮想ネットワークなど論理層の管理を指します。

JIP-ISMS517-1.0、ISO/IEC 27017:2015 への対応

1. JIP-ISMS517-1.0 への対応

4.1 クラウドサービスを含む情報セキュリティマネジメントシステムの適用範囲の決定【JIS Q 27001 の 4.3】

認証審査を受けるにあたって、組織は、クラウドサービスを含めた ISMS の適用範囲の決定を行い文書化することが求められています。当社においては、スコープを『Pracla 』と定めています。
なお、Pracla においては、サプライチェーンにほかのクラウドサービスプロバイダは存在していないことから、当社はクラウドサービスプロバイダであり、クラウドサービスカスタマではありません。また、ピアクラウドサービスプロバイダも存在しておりません。

＜認証取得を検討されているクラウドサービスカスタマに向けて＞
Pracla 上でクラウドサービスを提供している事業者様が、ISMS クラウド認証の取得を行う場合は、「クラウドサービスプロバイダ」と「クラウドサービスカスタマ」の両方をスコープとする必要があります。

2. ISO/IEC 27017:2015（JIS Q 27017:2016） への対応

ISO/IEC 27017 は、ISO/IEC 27002 と共通する管理策については、同じ項番が付与されていますので、ISO/IEC 27001 附属書 A の項番とも一致します。

また、既存の ISO/IEC 27001 附属書 A および ISO/IEC 27002 で想定されていないクラウド特有の拡張された管理策については、「附属書 A（規定）クラウドサービス拡張管理策集」として、頭に『CLD』がつく項番が付与されています。また、頭に『CLD』がつく管理策についても、そのあとに続く番号は、ISO/IEC 27001 附属書 A および ISO/IEC 27002 で定められた番号とも整合がとられています。
本書においては、閲覧時の利便性を考慮し、項番の順番に沿って、クラウドサービスプロバイダとしての取り組みについて解説を行います。

5.1.1 情報セキュリティのための方針群

クラウドサービスプロバイダは、クラウドサービスの提供及び利用に取り組むため、情報セキュリティ方針の拡充が求められています。これらについては、当社のセキュリティポリシーの見直しを

行い、クラウドサービスカスタマが安心して利用できるよう取り組みを行っています。

6.1.1 情報セキュリティの役割及び責任

「BroadCenter Pracla ホステッド・プライベートクラウドサービス利用約款 第 27 条（本サービスの目的）」、「BroadCenter Pracla ホステッド・プライベートクラウドサービス利用約款 第 34 条（本サービスの適正な利用）」、「BroadCenter Pracla ホステッド・プライベートクラウド HCI タイプ サービス仕様書」で役割及び責任について明記しており、これらについては、Pracla の利用開始時に利用規約として同意いただく事項となります。

6.1.3 関係当局との連絡

地理的所在地は「BroadCenter Pracla ホステッド・プライベートクラウドサービス利用約款 第 30 条（提供場所）」で定めています。また、現時点においてクラウドサービスカスタマデータを保存する可能性のある国は、日本国となります。

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分担

サービスに関する提供範囲は「BroadCenter Pracla ホステッド・プライベートクラウド HCI タイプ サービス仕様書」のサービス提供範囲および各種説明を参照ください。

7.2.2 情報セキュリティの意識向上、教育及び訓練

当社では情報セキュリティ方針(https://www.tokai-com.co.jp/security_policy/)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を適切に取り扱うために、本サービスの担当者に対し、定期的な教育・訓練を実施しております。

8.1.1 資産目録

ご契約者様の情報資産(ご契約者様にて保存されるデータ)と当社がサービスを運営するための情報は、明確に分離しております。
なお、ご契約者様の情報資産につきましては、ご契約者様の管理範囲となります。

CLD.8.1.5 クラウドサービスカスタマの資産の除去

仮想マシンの管理については、クラウドサービスカスタマで実施いただく必要があり、仮想マシンの削除においてもクラウドサービスカスタマが実施いただくことになります。また、クラウドサービスカスタマが仮想マシンの削除を行わずに解約となった場合は、専用物理サーバの初期化を実施させていただきます。

8.2.2 情報のラベル付け

仮想マシン上に保存されたデータに対してラベル付けを行う機能は提供しておりません。

9.2.1 利用者登録及び登録削除

Pracla の利用者についてはクラウドサービスカスタマの管理となっていますので、契約時に作成した Pracla 環境の管理者権限 ID（root、Administrator 等）で、クラウドサービスカスタマの定める規定に従い運用いただくことができます。

9.2.2 利用者アクセスの提供(provisioning)

仮想マシンにアクセスするために SSL-VPN ユーザ ID 及び Pracla 環境の管理者権限 ID（root、Administrator 等）を提供します。仮想マシンへのアクセス権については、クラウドサービスカスタマの定めた規定により運用いただくこととなります。

9.2.3 特権的アクセス権の管理

Pracla Web ポータルは Pracla のご契約者様のみがアクセスできるよう、SSL-VPN 接続が前提となっています。

9.2.4 利用者の秘密認証情報の管理

SSL-VPN 接続ユーザ ID の管理はサービス申込書で受け付けています。パスワードの変更や再発行については、パスワード設定用画面でクラウドサービスカスタマが行い、登録いただいたメールアドレスにパスワードが届きます。

9.4.1 情報へのアクセス制限

Pracla Web ポータルへのアクセスについては、SSL-VPN ユーザ ID を保持しているクラウドサービスカスタマが利用することができます。また、Pracla 環境の管理者権限 ID（root、Administrator 等）はクラウドサービスカスタマが保有していますので、クラウドサービスカスタマの定めた規定に従い運用いただくことができます。

9.4.4 特権的なユーティリティプログラムの使用

Pracla の利用を支援する使用者の特権的なユーティリティプログラムは、「Pracla Web ポータル上での機能」です。利用においては認証が必要となっており、セキュリティ手順を回避することのできるユーティリティプログラムは提供しておりません。

CLD.9.5.1 仮想コンピューティング環境における分離

クラウドサービスカスタマの利用する仮想マシンやネットワークは、VLAN によって論理的に分離されています。

CLD.9.5.2 仮想マシンの要塞化

Pracla はご契約者様専用の物理サーバを提供し、外部とのネットワークは FW で制御しています。内部ネットワークの設定は、クラウドサービスカスタマ自身で設定いただく必要があります。あわせて、Pracla 環境の管理者権限 ID（root、Administrator 等）は、クラウドサービスカスタマが保有していますので、クラウドサービスカスタマ自身で必要なサービスの選定やログの取得など実施いただくことができます。

10.1.1 暗号による管理策の利用方針

仮想マシンについては、標準で暗号化の処理を提供しておりません。Pracla 環境の管理者権限 ID（root、Administrator 等）は、クラウドサービスカスタマが保有していますので、クラウドサービスカスタマの定めるポリシーに基づき運用いただくことができます。

11.2.7 装置のセキュリティを保った処分又は再利用

使用している記憶媒体については、複数のディスクにより冗長化された領域に、仮想のストレージ領域を保持しているため、ストレージを構成する ディスク を一つだけ取得しても、中の情報が取り

出せない状態になっています。なお、故障等により交換した記憶媒体の処理については、当社と機器ベンダーとの契約に基づき適切に処理を行っています。

12.1.2 変更管理

クラウドサービスカスタマに何らかの影響が発生する可能性のある変更及びメンテナンスについては、事前に通知を行っています。通知方法については、「BroadCenter Pracla ホステッド・プライベートクラウドサービス利用約款 第 47 条（契約者への通知等）」で定めています。

12.1.3 容量・能力の管理

サービスの適正なスペックをシステム監視し、定期的なキャパシティー管理において増強などを行っています。

CLD.12.1.5 実務管理者の運用のセキュリティ

契約時に通知する「利用開始のご案内」および「Web ポータルマニュアル」を提供しています。
また、「ポータルご利用ガイド」は SSL-VPN 接続後にポータルからダウンロードすることができます。

12.3.1 情報のバックアップ

バックアップは同一筐体は取得することが可能です。
詳細は「BroadCenter Pracla ホステッド・プライベートクラウド HCI タイプ サービス仕様書」を参照ください。

12.4.1 イベントログ取得

Pracla Web ポータルへのログインのログは、Pracla Web ポータルから閲覧できます。また、仮想マシンについては、クラウドサービスカスタマに管理者権限 ID（root、Administrator 等）が付与されていますので、クラウドサービスカスタマのポリシーに従い取得いただくことができます。

12.4.4 クロックの同期

当社が契約時に提供している専用物理サーバおよびハイパーバイザーは、当社が管理する NTP サーバを参照するよう設定しています。

CLD.12.4.5 クラウドサービスの監視

ネットワークの利用量等を Pracla Web ポータルから参照いただくことができます。また、仮想マシンについては、CPU やメモリ等の異常を検知できるよう、標準で監視機能を提供しています。

12.6.1 技術的ぜい弱性の管理

当社の管理する Pracla Web ポータル等については、リリース前および、定期的なぜい弱性診断の確認を行っています。

また、サービス提供機器やソフトウェアのぜい弱性が発見され利用に影響が発生する場合には、情報の収集を行い、対策を行うとともに、必要に応じてポータルサイト等で対応の呼びかけなどを実施しています。

13.1.3 ネットワークの分離

VLAN により、契約アカウントごとにネットワークの分離をしています。

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

セキュリティ要件として当社の内部資料で文書化しています。また、構成変更が発生する場合においては、変更管理プロセスにより、設計及び検証を実施して変更内容の確認を実施しています。

14.1.1 情報セキュリティ要求事項の分析及び仕様化

Pracla においては、「Web ポータルマニュアル」を提供しています。

14.2.1 セキュリティに配慮した開発のための方針

ご契約者様の Pracla 環境へ接続するための SSL-VPN 接続画面については、リリース前および、定期的なぜい弱性診断の確認を行うことを方針として定めています。

15.1.2 供給者との合意におけるセキュリティの取扱い

当社とクラウドサービスカスタマの責任分界点は、契約約款およびサービス仕様書で示しています。Pracla の申込時に契約約款に同意いただきますと、Pracla の利用ができるようになります。
なお、責任分界点についての解説は、前出の「責任分界点について」の項を参照ください。

15.1.3 ICT サプライチェーン

Pracla は、当社のデータセンターに当社で環境を構築しています。当社からの委託先及び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求めます。

16.1.1 責任及び手順

当社で確認したインシデントについては、当社内の通知規定に基づき、通知を行います。なお、通知は、「クラウドサービスに関する契約約款」で定めた方法で行います。

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象の問い合わせや報告は、クラウドサービスカスタマの担当アカウントが受け付け、当社内でインシデント管理を行っています。
また、サービスで発生した情報セキュリティ事象は該当ご契約者様に通知を行います。

16.1.7 証拠の収集

Pracla 環境の管理者権限 ID（root、Administrator 等）は、クラウドサービスカスタマが保有しているため、ディジタル証拠となり得る情報については、ご契約者様に管理いただく必要があります。
なお、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、「BroadCenter Pracla ホステッド・プライベートクラウドサービス利用約款」で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

「BroadCenter Pracla ホステッド・プライベートクラウドサービス利用約款 第 51 条（準拠法）」で準拠法を日本法と定めています。

18.1.2 知的財産権

クラウドサービスカスタマからの問い合わせは、クラウドサービスカスタマの担当アカウントが受け付け、当社内でインシデント管理を行っています。

18.1.3 記録の保護

「BroadCenter Pracla ホステッド・プライベートクラウドサービス利用約款　第 20 条（情報の取り扱い）、第 44 条（個人情報保護）、第 46 条（契約者のデータの権利）」で定めています。

18.1.5 暗号化機能に対する規制

仮想マシン上で利用できる暗号化機能は、提供しておりません。クラウドサービスカスタマの定める規定に基づき運用いただくことができます。

サービスポータルへの Web アクセスにおいては、TLS による通信の暗号化を行っています。

その他、リモートアクセス機能（VPN）など提供しております。詳細は仕様書をご確認ください。

18.2.1 情報セキュリティの独立したレビュー

以下の各事項を実施しています。

- ISO/IEC 27001 について第三者による審査を受け、それぞれの認証を取得していることで、情報セキュリティに対する取り組みの証憑としています。
- Pracla の利用を検討している事業者およびクラウドサービスカスタマの定めるチェックシート等について回答を行っています。
- 使用しているデータセンターについては、データセンター見学の受け入れを行っており、建物設備や運用について見学いただくことができます。
- 本書により情報の開示を行っています。

改訂履歴

版数	日付	主な変更内容
初版	2021/12/1	初版発行
1.1 版	2022/3/18	7.2.2,8.1.1,CLD12.4.5 を更新