クラウドサービスにおけるセキュリティ対策概要

株式会社 IDC フロンティア

第１版

目次

1 本ドキュメントについて

1.1 総則

本ドキュメントは、株式会社ＩＤＣフロンティア（以下「当社」という。）の提供するクラウドサービスについてのセキュリティに関する取組みを記載しております。
発行日時点での取り組み状況となりますので、最新の状況と異なる部分がある場合もございますので、ご了承ください。
なお、クラウドサービスの仕様は、当社が別途定めるサービス仕様書によるものとします。

1.2 対象サービス

本ドキュメントが対象とする当社の提供するクラウドサービスは、次のとおりです。

・ＩＤＣＦクラウド
・セルフクラウド
・マネージドクラウド
・プライベートクラウド
・オブジェクトストレージ

2 情報セキュリティのための組織

2.1 内部組織

2.1.1 責任の割当て

クラウドサービスに関する情報セキュリティ責任者を選任しています。また当社の情報セキュリティについては、ポータルサイトまたはカスタマーデスクなどを通じて問い合わせが可能です。また個人情報についての問い合わせについても窓口を用意しており、問い合わせ先はプライバシーポリシーに明記しています。

2.1.2 情報処理設備の認可プロセス

クラウドサービスについての資料を提供しています。SLA を含むサービス利用にあたっての合意事項は、約款に明示しています。

2.1.3 秘密保持契約

約款に個人情報の取り扱いを含む秘密保持条項を規定しています。

2.1.4 関係当局との連絡

電気通信事業法に基づいて事業を提供しており監督官庁は総務省です。また個人情報保護に関する監督官庁も総務省となります。サポート窓口をサービス提供開始時に明示しており、また個人情報についての問い合わせ先はプライバシーポリシーに明記しています。

2.2　外部組織

2.2.1　外部組織に関係したリスクの識別

利用上の制限および注意を、サービス仕様書、カスタマーハンドブックに記載しています。障害情報の開示、脆弱性情報などはポータルサイトを通じて開示しています。

3　資産の管理

3.1　資産に対する責任

3.1.1　資産目録

クラウド環境に置かれたデータやプログラムなどの資産については、お客さまに管理いただく事項になります。

3.1.2　資産の管理責任者

クラウド環境に置かれたデータやプログラムなどの資産については、お客さまに管理いただく事項になります。

3.2　情報の分類

3.2.1　分類の指針

クラウドコンピューティング環境にあるクラウド利用者の情報を加工（メタデータ付加など）することはございません。また、クラウドコンピューティング環境は、利用者ごとに論理的に分離されております。

3.2.2　情報のラベル付けおよび取り扱い

提供しているサービスの性質上、情報区分を識別するラベルやマーキングなどを行う機能はありません。仮想マシン上に構築・保存したお客さまの情報管理は、お客さまの責任において実施いただきます。

なお、ポータルサイト上に保存されたお客さまの情報は、権限（管理者および一般ユーザー）に応じて開示範囲が異なる構造としており、情報区分を意識した作りになっています。

4　人的資源のセキュリティ

4.1　雇用の終了または変更

4.1.1　資産の返却

お客さま企業とその利用者の雇用関係が終了した場合の仮想マシンの変更・解約はお客さま企業の責任において変更をお願いします。当社はサービス提供の変更・解約などのお申し出により対応します。

これらは、約款、サービス仕様書で明示しています。

4.1.2　アクセス権の削除

お客さま企業とその利用者の雇用関係が終了した場合、仮想マシンおよびポータルサイトのアクセス権の変更削除はお客さまにて実施いただくことになっております。当社はサービス提供のご解約の申し出によりアカウント削除を行います。
これらは、約款、サービス仕様書で明示しています。

5 物理的および環境的セキュリティ

5.1 セキュリティを保つべき領域

5.1.1 セキュリティを保つべき領域での作業

仮想マシンのご利用環境を当社は制限しておりません。お客さまのご利用形態に応じてお決めいただきます。

5.2 装置のセキュリティ

5.2.1 記録媒体を内蔵した装置の処理

記憶媒体を内蔵した装置を処分または再利用する場合は、情報の漏えいなどが発生しないよう適切に処理を行っております。

6 通信および運用管理

6.1 運用の手順および責任

6.1.1 当社運用基準

当社の業務におきましては、ITIL をベースに運用を行っております。

6.1.2 操作手順書

カスタマーハンドブック、クイックスタートガイドを用意し提供しています。また、利用上の不明点を解消いただくための問い合わせ窓口をご用意しています。

6.1.3 変更管理

仮想マシン環境に影響するシステム変更がある場合は、お客さまへ事前に通知をします。お客さまの利用環境に変更が生じる場合は、変更内容も事前にお伝えします。

6.1.4 職務の分割

仮想マシンについては管理者権限のみを提供しており、またシステム環境をご利用開始時にご案内しています。お客さまの契約範囲における権限をどういった職務の方に利用していただくかは、お客さまのポリシーで運用いただくことになります。
ポータルサイトのご利用については、お客さまアカウントの管理者を立てていただき管理いただくこととなります。

6.2　第三者が提供するサービスの管理

6.2.1　第三者が提供するサービス

当社がサービス仕様書で明示している提供範囲に含まれている関係者との間では、当社が設定しているサービスレベルを維持する体制を構築しています。お客さま側環境においてネットワーク環境などを提供している第三者のサービスを利用する場合においては、お客さまにてご確認をお願いいたします。

6.2.2　第三者が提供するサービスの監視およびレビュー

当社がサービス仕様書で明示している提供範囲に含まれている関係者との間では、当社が監査を実施する体制を構築しています。監査結果をお客さまへ明示することはありません。

お客さま側環境においてネットワーク環境などを提供している第三者のサービスを利用する場合については、お客さまにてご確認をお願いいたします。

6.2.3　第三者が提供するサービスの変更に対する管理

当社がサービス仕様書で明示している提供範囲に含まれている関係者との間では、当社が変更を管理する体制を構築しています。お客さまへ影響が及ぶ場合は、事前に通知のうえ変更を実施します。

お客さま側環境においてネットワーク環境などを提供している第三者のサービスを利用する場合については、お客さまにてご確認をお願いいたします。

6.3　システム計画作成および受入れ

6.3.1　容量・能力の管理

お客さまの仮想マシンにおいて容量・能力監視を行える監視機能を提供しています。また仮想マシンのスペックを提示しています。

クラウド基盤のシステム全体においては、当社にてヘルスチェックを実施しています。

6.3.2　システムの受け入れ

システム仕様やサービス仕様の変更がある場合は、事前にお客さまへ提示します。

6.4　悪意のあるコードおよびモバイルコードからの保護

6.4.1　悪意のあるコードに対する管理策

ポートフィルタリング機能を提供しています。

クラウド基盤のシステム全体において何らかのセキュリティ上の課題を発見した場合は、メンテナンスにおいて修正をします。

お客さまがお客さまご自身の仮想マシンへインストールしたアプリケーションについては、お客さまの責任においてセキュリティ上の課題への対

応をお願いします。なお、別途 IPS/IDS および WAF のサービスをご利用いただくことも可能です。

6.5 バックアップ

6.5.1 情報のバックアップ

仮想マシン上のお客さまの情報については、お客さま自らの責任でバックアップして保存するようにしてください。当社は、仮想マシン上のお客さまの情報の保存、バックアップなどの責任を負っておりません。

6.5.2 バックアップ機能の提供

お客さまがご自身の仮想マシンのバックアップを取得できる機能を提供しています。バックアップからのリストアは、お客さまにてご確認をお願いします。

6.6 ネットワークセキュリティ管理

6.6.1 ネットワークサービスのセキュリティ

基本機能としてファイアウォール機能を提供しています。

6.7 情報の交換

6.7.1 電子的メッセージ通信

仮想マシンへアクセスする際には、SSH サービスまたは SSL を実装したポータルサイトからのアクセス環境をご用意しています。

なお、お客さまの仮想マシンのご利用方法を当社は制限しておりませんので、お客さまの利用方針にしたがって、適切な対策を実施してください。

6.8 監査

6.8.1 監査ログ取得

お客さまの仮想マシン上の監査ログについては、お客さまの運用方針にしたがってお客さま自身で取得いただきます。

6.8.2 システム使用状況の監視

監視サービスを提供しています。

6.8.3 ログ情報の保護

仮想マシンに保存されているデータの管理者はお客さまになりますので、お客さまの運用方針にしたがってご対応いただきますようお願いいたします。

6.8.4 実務管理者および運用担当者の作業ログ

ポータルサイト上での作業は記録しています。

6.8.5 障害のログ取得

クラウド基盤のシステム障害については、ポータル上で通知しております。

仮想マシンの障害については、お客さまに管理いただきます

6.8.6 クロックの同期

NTP プロトコルにより同期をとっています。

7 アクセス制御

7.1 アクセス制御に対する業務上の要求事項

7.1.1 アクセス制御方針

仮想マシンへアクセスする際には、SSH サービスまたは SSL を実装したポータルサイトからのアクセス環境を提供しております

7.2 利用者アクセス管理

7.2.1 利用者登録

お客さま企業の管理者の方が登録・削除できます。

7.2.2 特権管理

お客さまの仮想マシンについては、お客さまの方針に基づいて管理者権限を付与したアカウントを作成可能です。

7.2.3 利用者パスワードの管理　確認

お客さまの仮想マシンでは、お客さまの方針に基づいたパスワード変更が可能です。

ポータルサイト上では、お客さまご自身でパスワードを変更できます。

7.2.4 利用者アクセス権のレビュー

お客さまの仮想マシン上のアクセス権レビュー機能については、お客さまにて構築いただくことになります。

7.3 ネットワークのアクセス制御

7.3.1 外部から接続する利用者の認証

お客さまの仮想マシンへのログオンの初期設定は SSH 鍵認証による提供およびポータルサイト経由での接続となります。利用開始後は、お客さまの方針にしたがって変更いただけます。

ポータルサイトは、ID/Password による認証を行っています。

7.3.2 遠隔診断用および環境設定用ポートの保護

SSL などの暗号化通信を用いたコンソール接続を提供しています。

7.3.3 ネットワークの接続制御

制限なく利用できます。

7.4 オペレーティングシステムのアクセス制御

7.4.1 セキュリティに配慮したログオン手順

お客さまの仮想マシンへのログオンの初期設定は、SSH 鍵認証による媒体です。利用開始後は、お客さまの方針にしたがって変更いただけます。

7.4.2 利用者の識別および認証

仮想マシン上の利用者の識別は、お客さまの利用方針にしたがって、適切な保護策をとっていただくこととなります。

当社は、仮想マシンをご利用いただくご契約者の管理者に対して、一意な利用者 ID を付与しています。当社ポータルサイトにおいては、利用者 ID

とパスワードによって利用者の同一性を検証しております。

7.4.3　パスワード管理システム

ポータルサイトのアカウントについては、対話式のパスワード変更サイトを用意しております。

お客さまの利用方針にしたがって、適切な保護策をとっていただくことになります。

7.4.4　システムユーティリティの使用

仮想マシンで使用されるアプリケーションはお客さまの管理となります。

お客さまの利用方針にしたがって、適切な保護策をとっていただくことになります。

7.4.5　セッションのタイムアウト

お客さまの仮想マシンの利用方法を当社は制限しておりません。またお客さまの仮想マシン上で当社が何かしらの機能を提供することはありません。

お客さまの利用方針にしたがって、適切な保護策をとっていただくことになります。

7.4.6　接続時間の制限

お客さまの仮想マシンの利用方法を当社は制限しておりません。またお客さまの仮想マシン上で当社が何かしらの機能を提供することはありません。

お客さまの利用方針にしたがって、適切な保護策をとっていただくことになります。

7.5　業務用ソフトウェアおよび情報のアクセス制御

7.5.1　情報へのアクセス制限

お客さまの仮想マシンの利用方法を当社は制限しておりません。またお客さまの仮想マシン上で当社が何かしらの機能を提供することはありません。

お客さまの利用方針にしたがって、適切な保護策をとっていただくことになります。

なお、サービスを提供しているクラウド基盤のシステム側からお客さま仮想マシンへのアクセスは仕様上行えないようになっています。

7.5.2　取り扱いに慎重を要するシステムの隔離

お客さまのご要望に応じて独立したサーバーの提供も可能です。

7.6　モバイルコンピューティングおよびテレワーキング

7.6.1　モバイルのコンピューティングおよび通信

当社では利用環境の制限をしておりません。お客さまの運用方針にしたがってご対応いただく事項となります。

7.6.2　テレワーキング

当社では利用環境の制限をしておりません。お客さまの運用方針にしたがってご対応いただく事項となります。

8 情報システムの取得、開発および保守

8.1 情報システムのセキュリティ要求事項

8.1.1 セキュリティ要求事項の分析および仕様化

約款・会員規約・仕様書および本書において開示しております。

8.2 暗号による管理策

8.2.1 暗号による管理策の利用方針

8.2.2 ポータルサイトは SSL による暗号化を行っています。

ご利用いただくお客さまの仮想マシン上の対策については、お客さまにおいて実施いただくことをお願いしています。

8.3 開発およびサポートプロセスにおけるセキュリティ

8.3.1 変更管理手順

事前にお客さまへ通知をしたうえでシステムの変更作業を実施します。

8.3.2 オペレーティングシステム変更後の業務用ソフトウェアの技術的レビュー

仮想環境でご利用できる OS を提示しております。変更が生じる場合は事前に通知を行います。

8.3.3 情報の漏えい

情報漏えい対策に関する当社社内ルールを策定し、実施しております。
ご利用いただくお客さまの仮想マシン上の対策については、お客さまにおいて実施いただく事項となります。

8.4 技術的脆弱性の管理

8.4.1 技術的脆弱性の管理

ご利用いただくお客さまの仮想マシンのリスクについては、お客さまにて情報収集と対策を実施いただくことになります。
クラウド基盤のシステムについては、当社で情報収集を実施し、必要に応じて対応しています。

9 情報セキュリティインシデントの管理

9.1 情報セキュリティの事象および弱点の報告

9.1.1 情報セキュリティ事象の報告

クラウドサービス全般の問い合わせ窓口を用意しています。

9.2 情報セキュリティインシデントの管理およびその改善

9.2.1 情報セキュリティインシデントからの学習

当社内のナレッジとしてまとめていますが、お客さまへ開示はいたしませ

ん。ただし、影響範囲に応じて予防措置を講じるように依頼をさせていただくことがあります。

9.2.2　証拠の収集

記録し適切に保管しています。

ご利用いただく仮想マシン上の情報については、お客さまにおいて適切に記録・保管いただくこととなります。

10 事業継続管理

10.1 事業継続における情報セキュリティの側面

10.1.1 事業継続およびリスクアセスメント

サービスの継続性を担保するためのリスク評価を行っています。

11 遵守

11.1 法的要求事項の遵守

11.1.1 適用法令の識別

約款で明示しています。

11.1.2 組織の記録の保護

法令や規制にしたがって記録の保護を行っています。ただし、仮想マシン上の記録についてはお客さまで保護いただきます。

11.1.3 暗号化機能に対する規制

法令にしたがってご利用いただくように約款で明示しています。

11.2 セキュリティ方針および標準の順守、並びに技術的順守

11.2.1 技術的順守点検

定期的に内部監査を実施しておりますが、結果については、開示しておりません。なお、仮想マシンにおける技術的点検はお客さまに実施いただく事項となります。

11.3 情報システムの監査に対する考慮事項

11.3.1 情報システムの監査に対する管理策

お客さまから事前申告をいただくことで、お客さまの監査へ協力させていただきます。提供可能な情報はお客さまのご契約範囲内となります。

11.4 各種ガイドラインなどへの適合状況

11.4.1 認証規格

ISO27001:2005(JIS Q 27001:2006)

を取得しております。

11.4.2 各種ガイドラインなどに関する管理策

次のガイドラインなどにおきましては、定期的にセルフチェックを行い適合状況の確認を行っております。

■経済産業省
・医療情報を受託管理する情報処理事業者における安全管理ガイドライン

■総務省
・ASP・SaaS 事業者が医療情報を取り扱う際の安全管理に関するガイドライン
・ASP・SaaS における情報セキュリティ対策ガイドライン

■厚生労働省
・医療情報システムの安全管理に関するガイドライン

■金融情報システムセンター
・FISC

■日本データセンター協会
・データセンターファシリティスタンダード

詳細については、当社営業担当までご相談ください。
※一部のガイドラインなどにおいては、当社管理範囲のチェックとなります。

附則

１．本ドキュメント（第 1 版）は、2014 年 10 月 1 日に発行します。