IDCF クラウド

セキュリティホワイトペーパー

株式会社 IDC フロンティア

2017 年 1 月 11 日（第 5 版）

もくじ

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、IDCF クラウドの利用を検討されている方、すでに利用いただいている方に向けて、IDCF クラウドのセキュリティへの取り組みを確認いただくとともに、IDCF クラウドをセキュアに利用いただくための留意事項を確認いただくことを目的としております。

セキュリティホワイトペーパーのリリースにあたって

クラウドサービスは、従来のオンプレミスの環境と異なり、オンデマンドセルフサービスやリソースプールなど、さまざまなメリットを享受できる反面、オンプレミスの環境では存在しなかったリスクを考慮する必要があります。

本書においては、当社が IDCF クラウドに対して取り組んでいるセキュリティ対策について説明するとともに、IDCF クラウドをよりセキュアに利用するために活用できるサービスについても紹介します。

なお、本書の情報は、作成時点のものとなります。最新の情報は、当社 Web サイトをご確認ください。
【当社 Web サイト】
http://www.idcf.jp/

IDC フロンティアのセキュリティへの取り組み

IDC フロンティアのセキュリティに対する取り組みを Web サイト上でも紹介しております。

【セキュリティへの取り組み】
http://www.idcf.jp/security/efforts.html

IDC フロンティアでは、「情報セキュリティ基本方針」や「プライバシーポリシー」を定め、当社業務の遂行に関わるすべての関係者に対して、定期的にセキュリティ教育・訓練を実施しております。
また、情報セキュリティマネジメントシステム（ISMS）の国際規格である
ISO/IEC27001:2013（JIS Q 27001:2014）を取得しております。

本書の適用範囲について

IDCF クラウドが本書の適用範囲となります。詳細は次の項をご確認ください。
セルフクラウドやマネージドクラウドおよびその他のサービスについては、該当しない場合があります。

IDCF クラウドの仕様・機能と本書の説明範囲

IDCF クラウドは、標準機能のほかに各種のオプション機能や外部ソリューションを組み合わせて利用することが可能です。その中にはセキュリティに関わる機能や外部ソリューションがあります。

表.本書で取り上げる標準機能、オプション機能および外部ソリューションについて

サービス管理	サーバー/ストレージ	ネットワーク
クラウドコンソール	仮想マシン	仮想ルーター
接続元 IP アドレス制限	ボリューム	ファイアウォール
クラウド API	スナップショット	ロードバランサー
2 段階認証	テンプレート	DDoS 対策
マルチユーザー	ISO イメージ	不正侵入検知/防御
サーバー監視/Mackerel ★	アーカイブデータ	インターネット接続
	HA 機能（フェイルオーバー）	プライベートネットワーク
		GSLB
		ILB
		DNS

サービス運用保守	VPN	組み合わせ可能サービス
ゾーン	リモートアクセス VPN	WAF
標準サポート	拠点間 VPN	オブジェクトストレージ
メンテナンス		ベアメタルサーバー
		コンテンツキャッシュ
		プライベートコネクト
		SSL デジタル証明書
		RDB
		プッシュ配信/Growth Push ★
		メール配信/SendGrid ★

：本書で取り上げている範囲（一部のみ取り上げているものを含む）

★：外部ソリューション

1. IDCF クラウドセキュリティ概要

データセンターのセキュリティ対策について

ロケーションについて

IDCF クラウドのシステムは、当社データセンター施設内に設置しております。当社担当者のみ IDCF クラウドで使用する設備に物理的なアクセスができるようにしております。

データセンターへの入退館について

全てのデータセンターは、24 時間の有人対応による受付を行っております。また、データセンター設備への入室においては、IC カード、生体認証、回転式ゲートなどによって、入退室のログを取得するとともに、共連れを含む不正な侵入を防御しております。

なお、火災などの非常時においては、扉等が自動開錠となるなど、緊急避難を想定した構造となっております。

電力について

電力については、電力会社から複数系統で受電しております。また、UPS および非常用発電機を冗長構成（N+1 以上）で設置しており、非常時においても継続的な電力供給が行えます。あわせて、燃料の備蓄も十分に備え、燃料の優先供給契約などにより継続的な電力供給を行います。

空調設備について

空調設備は、非常用発電設備から電力を供給することにより、停電時にも継続的に温度・湿度の管理を行えるようにしております。また、N+1 構成にするなど機器のメンテナンスや故障を想定した設計となっております。

また、外気空調方式の採用により空調設備に係る消費電力抑制と効率化を図っております。

地震対策について

データセンター建物においては、N≧50 となる地層まで杭を打ち込んでおります。また、重要度係数を 1.25 として設計された耐震建物となります。

火災対策について

データセンター内においては、空気中の微粒子を検知することができる超高感度煙検知システムを設置し、火災の初期段階で検知できるようにしております。また、消火システムには、不活性ガス消火システムを採用しており、サーバーをはじめとした機器類に損傷を与えずに消火を行えます。

落雷対策について

雷による被害は「直撃雷」と「誘導雷」の二種類が想定され、それぞれに対して次の通り対策を行っております。

- 直撃雷対策：避雷導線設置（一部突針）
- 誘導雷対策：サージアレスタの設置

水害対策について

データセンターの立地については、水害の想定がない地域を選定しております。また、建物内において水を使用する設備に対しては、防水処理・防水堤の設置および漏水センサーを設置するなど必要な対策を行っております。

監視カメラ（CCTV）について

建物周辺および建物内の各所に監視カメラを設置し、集中監視を行っております。合わせて映像の録画を行うとともに、一定期間保存することによって過去にさかのぼっての調査も行えるようにしております。

エリア／リージョン／ゾーンについて

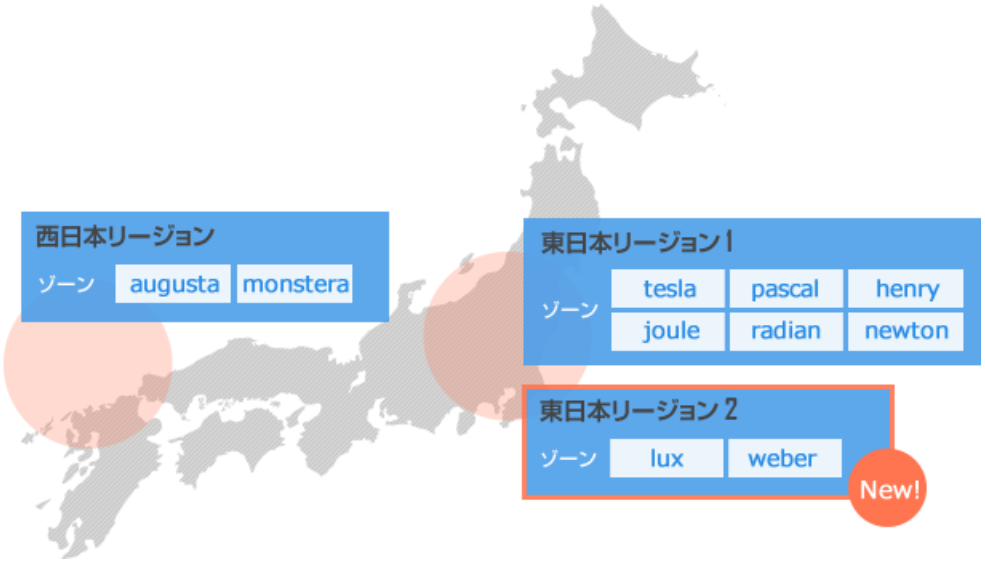
サービスの提供は東日本リージョン・西日本リージョンの 2 リージョンとなります。

「エリア」、「リージョン」と「ゾーン」の関係性は、次のとおりです。

エリア　　：データセンターのある物理的に離れた地域

リージョン：複数のゾーンを管理する集合

ゾーン　　：仮想マシンを構成するサーバー、ストレージ機器等の物理的な設備の集合



有事に備え、複数のエリア・リージョンをご利用いただくことを推奨しております。

データセンターの設備概要

IDCF クラウドで使用している当社のデータセンター設備などは次のようになっております。

地域	東日本	西日本
エリア名	東日本エリア	西日本エリア
リージョン名	東日本リージョン　東日本リージョン 2	
ゾーン	tesla, henry, pascal, joule, lux、weber radian, newton	augusta, monstera
所在地	福島県白河市	福岡県北九州市
給電方式	本線/予備線方式	
停電対策	無停電電源装置(UPS):15 分(定格負荷)N＋1構成 非常用発電機(GTG):48 時間(定格負荷、備蓄燃料のみ)N＋1構成 ※継続した燃料の供給可能 UPS から電力を供給、非常時においては、約 1 分で GTG に自動で切り替わり継続した電力供給が行えます。	
雷対策	直撃雷対策:避雷導線設置(一部突針)(JIS A 4201-2003 規格　保護レベル 1) 誘導雷対策:サージアレスタ	
地震対策	重要度係数:1.25 構造:S 造(耐震) 杭:N≧50 となる地層に杭入れ 最寄りの断層:関谷断層 断層からの距離:約 23km	重要度係数:1.25 構造:SRC 造(耐震) 杭:N≧50 となる地層に杭入れ 最寄りの断層:頓田断層 断層からの距離:約 7km
津波・洪水対策	海抜:377m 海からの距離:約 69km 内陸に立地しており、津波の影響はありません。また近隣に河川もなく被害想定がありません。	海抜:5.39m 海からの距離:約 500m 洞海湾から比較的近い場所にありますが、過去に津波被害の報告はありません。また、近年推測されている東南海沖地震の被害想定においても津波被害の発生のない場所と推定されております。 また、備えとして水防設備(各ピット内に湧水ポンプを設置)を設置しております。
その他の環境	最寄りの原子力発電所:福島第 2 原発 原子力発電所からの距離:約 73km	最寄りの原子力発電所:玄海原発 原子力発電所からの距離:約 97km
漏水対策	必要箇所に漏水センサーを設置	
火災対策	超高感度煙検知システム設置 窒素ガス消火設備による消火 適所に ABC 消火器および CO2 消火器を配備	

空調対策	N＋1構成
	外気空調使用可能
	自動制御システム（BAS）による監視および制御
防犯対策	有人警備
	敷地周辺および建物内部に CCTV を設置
	データセンターエリアは無窓
入退室管理	有人受付（24 時間対応）
	本人確認による IC カード貸与
	生体認証
	共連れ防止設備
ラック管理	ラック毎に施錠
	鍵の貸し出し管理を実施
	スラブにアンカーを打ち固定
準拠法	日本法

仮想化基盤のセキュリティ対策および脆弱性対応について

IDCF クラウドでは仮想化基盤において脆弱性を含めた脅威が確認された場合は、当社基準に基づき対応いたします。影響が長期にわたる場合や、対応のためポータルサイト等の停止を伴う場合は、事前に告知を行い対応するとともに、内容によっては、ポータルサイト、コーポレートサイト等で対応状況の公開を行います。

IDCF クラウドは、お客さまごと独立したネットワーク（VLAN）とし、仮想ルーターや仮想マシン、ボリュームを組み合わせてクラウドを利用できます。 作成した仮想マシンのデータは、定期的なスナップショットの取得や、テンプレート化して保存をすることで、仮想マシンの複製も容易に行えます。

クラウドコンソールのセキュリティ対策について

クラウドコンソールは、当社において定期的に第三者による脆弱性診断を実施するとともに、追加機能等により、変更が加わる場合においても、リリース前に第三者による脆弱性診断を行っております。また、WAF や IPS、DDoS 対策システム等を設置し、不正な通信の遮断を行っております。
また、脆弱性を含めた脅威が確認された場合は、当社基準に基づき対応致します。影響が長期にわたる場合や、対応のためポータルサイト等の停止を伴う場合は、事前に告知を行い対応するとともに、内容によっては、ポータルサイト、コーポレートサイト等で対応状況の公開を行います。

クラウドコンソールへのログインについては、Google 社の提供する Google Authenticator を利用した二段階認証を利用することが可能です。利用については、クラウドコンソールから個別に設定を行えます。なお、管理者によって管理するユーザーに対し強制的に二段階認証を適用させることができます。二段階認証を設定いただくことによって、「ユーザーが知っていること」に加え、「ユーザーが持っているもの」に基づく認証を行うことができます。

さらに、接続元となる IP アドレスの制限を行うことで、アカウントを不正に利用されるリスクを低減させることができます。

仮想化基盤のパフォーマンスについて

IDCF クラウド全体の稼働状況やレスポンスタイムなどのパフォーマンスをクラウドコンソールから確認することが可能です。閲覧できる情報は次の通りです。

- Computing Service
  HTTP リクエストの平均応答時間
- Computing API
  REST API の平均応答時間
- IDCF Cloud Web Interface
  クラウドコンソールの平均応答時間
- Object Storage
  オブジェクトストレージサービスのオブジェクトの Get にかかる平均応答時間

アカウント管理（マルチユーザー）について

IDCF クラウドでは、サインアップを行ったアカウントを管理者アカウントとして、マルチユーザーの設定することが可能です。また、ユーザー機能は 4 タイプに分かれていますので、職責に応じた権限管理を行うことができます。

タイプ	想定利用者	操作権限	作成可能数
マスターユーザー	契約アカウント	全て	1 ユーザー
パワーユーザー	サーバー管理者	ユーザー作成機能を除く全て	合計 100 ユーザー
ユーザー	運用担当者	クラウドコンソール・API の利用	
ビリングユーザー	請求/支払担当者	利用明細の閲覧	

IDCF クラウドにおける当社の管理範囲について

IDCF クラウドは IaaS 型のサービスです。当社の管理範囲はインフラまでとなります。なお、テンプレートで提供しております OS イメージは、使用開始後はお客さまに管理いただくものとなります。

IDCF クラウドにおける情報セキュリティインシデントへの対応について

当社からお客さまに報告する情報セキュリティインシデントについて

以下に該当するインシデントについては、当社よりご連絡させていただく場合があります。

(1)　次項に記載する禁止事項に抵触している場合

(2)　DDoS 等の外部からの不正により、他のお客さまに影響が波及するおそれのある場合

(3)　当社の管理するシステムで発生した障害等によって、何らかの影響が発生している場合

(4)　その他、当社が報告すべきと判断した場合

情報セキュリティインシデントの検出および開示ポリシーについて

当社の管理するシステムについては、24 時間体制で監視を行い、インシデントの検知が行える体制を整えております。当社で検知したインシデントで、お客さまへのサービス提供に影響が発生する場合、予め登録いただいている通知先等に対し、通知を行います。

なお、当社が検知したインシデントで、お客さまへのサービス提供に影響が発生しない場合については、この限りではありません。

情報セキュリティインシデントの通知を行う目標時間

当社で検知した情報セキュリティインシデントは、検知した時点から 15 分以内での通知を目標としております。

情報セキュリティインシデント対応のための対応窓口

標準サポートの窓口において対応をおこないます。お客さま側で情報セキュリティインシデントの検知をされた場合においても、標準サポートの窓口までご連絡ください。

禁止事項

お客様は本サービスを利用して以下の各号の行為を行ってはならず、又、お客様等にも以下の行為を行わせないよう指揮監督するものとします。（ホスティングサービスに関する契約約款から抜粋）

(1) 本サービスの内容や本サービスにより利用しうる情報を改ざん又は消去する行為
(2) 商用、非商用その他用途の如何を問わず、本サービス利用契約に違反して、第三者に本サービスを利用させる行為
(3) 当社若しくは第三者の財産（知的財産権を除く）、プライバシー又は肖像権を侵害する行為、又は侵害する虞のある行為
(4) 当社若しくは第三者の特許権、著作権、商標権その他知的財産権を侵害する行為、又は侵害する虞のある行為
(5) 当社若しくは他社を差別若しくは誹謗中傷・侮辱し、他社への不当な差別を助長し、又はその名誉若しくは信用を毀損する行為
(6) 詐欺、児童売買春、預貯金口座及び携帯電話の違法な売買等の犯罪に結びつく、又は結びつく虞の高い行為
(7) わいせつ、児童ポルノ又は児童虐待に相当する画像、映像、音声若しくは文書等を送信若しくは表示する行為、若しくはこれらを収録した媒体を販売する行為、又はその送信、表示、販売を想起させる広告を表示又は送信する行為
(8) 薬物犯罪、規制薬物等の濫用に結びつく、若しくは結びつく虞の高い行為、又は未承認医薬品等の広告を行う行為
(9) 無限連鎖講（ネズミ講）を開設し、又はこれを勧誘する行為
(10) 第三者になりすまして本サービスを利用する行為
(11) ウイルス等の有害なコンピュータプログラム等を送信又は掲載する行為
(12) 無断で第三者に広告、宣伝若しくは勧誘のメールを送信する行為、又は社会通念上第三者が嫌悪感を抱く、若しくはその虞のあるメール（嫌がらせメール）を送信する行為
(13) 第三者の設備等又は本サービス用設備等の利用若しくは運営に支障を与える行為、又は与える虞のある行為
(14) 違法な賭博・ギャンブルを行わせ、又は違法な賭博・ギャンブルへの参加を勧誘する行為
(15) 違法行為（けん銃等の譲渡、爆発物の不正な製造、児童ポルノの提供、公文書偽造、殺人、脅迫等）を請負し、仲介し、又は誘引（他人に依頼することを含みます。）する行為
(16) 人の殺害現場の画像等の残虐な情報、動物を殺傷・虐待する画像等の情報、その他社会通念上他者に著しく嫌悪感を抱かせる情報を不特定多数の者に対して送信する行為
(17) 人を自殺に誘引若しくは勧誘する行為、又は第三者に危害の及ぶ虞の高い自殺の手段等を紹介するなどの行為
(18) その行為が前各号のいずれかに該当することを知りつつ、その行為を助長する態様・目的でリンクをはる行為

(19) 犯罪や違法行為に結びつく、又はその虞の高い情報や、他者を不当に誹謗中傷・侮辱したり、プライバシーを侵害したりする情報を、不特定の者をして掲載等させることを助長する行為
(20) 法令若しくは公序良俗に違反し、又は当社若しくは第三者に迷惑若しくは不利益を及ぼす行為
(21) 上記各号の外、本サービスの提供の目的を逸脱するものと当社が判断する行為

その他、詳細については、当社約款を参照ください。
【ホスティングサービスに関する契約約款】
http://www.idcf.jp/pdf/common/hostingservices.pdf

上記のような禁止行為が確認され、当社から通知等を行ったにもかかわらず、改善が認められない場合は、当社側で速やかに仮想マシンの停止、または削除などを実施する場合があります。なお、お客さまの故意ではなく過失（たとえば、第三者による不正利用）による場合であっても、同様の対応となります。

2. 提供している OS について

提供している OS に共通する事項

仮想マシンの作成・設定について

仮想マシンの作成や仮想ルーターの設定などは、クラウドコンソールから作業を行うことができます。作成手順については、「めちゃ楽ガイド」を参照ください。

【めちゃ楽ガイド】

http://www.idcf.jp/pdf/cloud/IDCFCloud_installation_guide.pdf

プライベート IP アドレスについて

利用者が仮想マシンを作成するとプライベート IP アドレスが1つ割り当てられます。プライベート IP アドレスは、自動で付与されますが、明示的に指定いただくことも可能です。このプライベート IP アドレスについては、ネットワーク情報として管理されており、追加することも可能です。

パブリック IP アドレス（グローバル IP アドレス）について

インターネットと直接つなぐための IP アドレスです。IDCF クラウドでは契約時点で 1 つ用意されております。インターネットと通信を行うためには、別途ネットワーク設定が必要となります。

仮想マシンはネットワーク設定を行うことでパブリック IP アドレスを使用して、インターネットとの接続を行うことができるようになります。ネットワーク設定によっては、インターネット側から仮想マシンへの通信を許可することになりますので、外部（インターネット）からの脅威に晒されます。ネットワーク設定を行う前に必ず仮想マシン側の設定を見直すなど、第三者による脅威にご注意ください。

OS テンプレートのネットワーク設定について

初期構築時においては、パブリック IP アドレスが付与されておりませんので、仮想マシンは外部からの脅威にさらされるようなことはありません。

LINUX 系 OS のセキュリティ

当社提供のテンプレートについて

当社の提供するテンプレートは、提供時点でリリースされているパッチの適用までとなっております。初期にインストールされているパッケージは、当社の基準に基づき最小構成となるようにしておりますので、お客さま側でアップデートおよび必要となるパッケージのインストールが必要となります。なお、セキュア OS 機能（SELinux）は無効化されておりますので、必要に応じて設定を行ってください。

当社提供のテンプレートのライセンス費用について

Red Hat については、テンプレートは無償で使用できますが、別途サブスクリプション費用が必要となります。

その他、CentOS、Debian、Ubuntu などのイメージを提供（無償）しております。

サーバーへの接続

初期構築時に SSH 公開鍵を登録することが可能です。公開鍵、秘密鍵は、仮想マシン構築時に作成することができます。また、ご利用者様が用意されているキーペアの使用も可能です。

WINDOWS 系 OS のセキュリティ

当社提供のテンプレートについて

当社の提供するテンプレートは、パッチは適用されていないため、お客さま側で Windows Update を行っていただく必要があります。

当社提供のテンプレートのライセンス費用について

Windows Server については、別途ライセンス費用が必要となります。

サーバーへの接続

初期構築時においては、クラウドコンソールからの接続のみとなります。

3. ネットワークについて

仮想ルーター

アクティブ/スタンバイ構成の仮想ルーターにより、インターネットとの接続が冗長化されたお客さま専用ネットワークをご利用いただけます。仮想ルーターを経由したインターネットとの通信はパブリック IP アドレスの NAT 接続を利用します。

サービス仕様

仮想コア		メモリ容量	帯域	HA機能	ご利用料金
2	2.4GHz相当	2GB	2Gbps	あり	無料

項目		詳細
HA機能		アクティブ/スタンバイ構成
外部との接続	内部→外部	ソースNAT または スタティックNAT
	外部→内部	ポートフォワーディング または スタティックNAT ※上記以外にロードバランシングが可能です。詳細は「ロードバランサー」をご覧ください。

ファイアウォール

仮想マシン群とインターネットの間に設置されている冗長化されたファイアウォールを、無料でご利用いただけます。

外部ネットワークからの不正アクセスからシステムを守るため、送信元 IP アドレスにより必要な通信のみを許可し、不要な通信を遮断することができます。

サービス仕様

		詳細
HA機能		アクティブ/スタンバイ構成
デフォルトポリシー	Inbound	All Deny
	Outbound	All Accept

ロードバランサー

外部ネットワークからのアクセスを配下の仮想マシンに負荷分散させることができます。ロードバランサーが Cookie を挿入しセッションを維持する「lbCookie」の設定を行うことも可能です。

また、データベースなどの内部ロードバランシングとしても利用できます。

サービス仕様

		詳細
HA機能		あり（アクティブ/スタンバイ構成）
分散方式		■ラウンドロビン ※分散対象の仮想サーバーに順番にアクセスを振り分けます。 ■リーストコネクション ※最も少ないセッションの仮想サーバーにアクセスを振り分けます。 ■ソースIPハッシング ※送信元IPアドレス毎に同じ仮想サーバーにアクセスを振り分けます。
ヘルスチェック	方式	TCP
	間隔	2秒
	しきい値	失敗3回

リモートアクセス VPN

自宅や外出先からマルチデバイスでセキュアに仮想ルーターにリモート接続できる、リモートアクセス VPN をご利用いただけます。

VPN ユーザーはクラウドコンソールで管理でき、自由に作成・削除可能です。

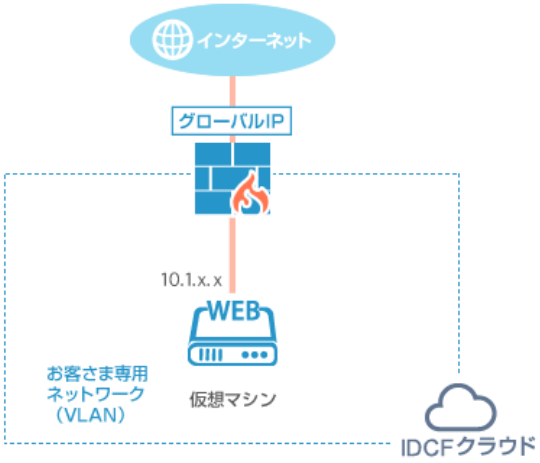
サービス仕様

	詳細
プロトコル	L2TP over IPsec *1
認証方式	Pre-shared key *2
同時接続	可能 ※ただし、ソースIPアドレスが同一の場合は接続できません

4. IDCF クラウドの構成・その他の機能などについて

基本構成

IDCF クラウドの最小構成は以下のようになります。



- 仮想マシンにはプライベート IP アドレスが設定されます。
- パブリック IP アドレスが 1 つ割り当てられます。
- 外部からの通信は、仮想ルーターでプライベート IP アドレスに変換されて仮想マシンに転送されます。
- アカウント作成後、ゾーンごとに 1 台目の仮想マシン作成時に 2 台の仮想ルーターも作成されます。
- 当社の提供しているテンプレートを使用した場合、当社の NTP サーバーと時刻同期する設定となっています。
- 当社の NTP サーバーは、ご契約の環境からのみ接続することができます。ご契約者様の社内環境の時刻調整を当社の NTP サーバーから直接行うことはできません。仮想マシンを NTP サーバーとして使用するなどで、時刻調整を行っていただくことは可能です。

仮想マシン上に保管されるデータのセキュリティ対策について

OS などの管理について

仮想マシン上で稼働しているシステムについては、当社テンプレートとして提供した OS を含め、アカウント管理やパッチマネジメントなどについては、お客さま側で管理・運用いただく必要があります。

データの管理について

仮想マシン上に保存されたデータについては、お客さま側で管理・運用いただく必要があります。

データの暗号化などが必要な場合は、専用ツール等を導入いただくか、あらかじめ暗号化したデータを保存するなどの対応を行っていただく必要があります。

データのラベル付けについて

IaaS のサービスとなるため、仮想マシン上に保存されたデータについてラベル付けを行う機能は提供しておりません。

データの消去について

仮想マシン上に保存しているデータや、クラウドコンソールより仮想マシンを削除した場合、仮想マシンが使用していた領域も消去されます。この際にストレージ内のメタデータも削除されるため、一度削除を実施されると、仮想マシンの復元ができないようになっております。仮想マシンの削除を実施される際にはご注意ください。

なお、データの削除証明書に類する文書については発行しておりません。

故障したハードディスクの取扱について

故障もしくは故障予兆の発生したハードディスクについては、適宜入れ替えを行うとともに、交換したハードディスクは弊社規定に基づきデータの再利用がされないよう処理をおこなっております。

スナップショットについて

お客さまの運用をサポートするため、スナップショット機能を用意しておりますので、必要に応じてご活用ください。

暗号化について

IaaS のサービスとなり、ストレージに対する暗号化サービスは現時点で提供しておりません。仮想マシン上に保管するデータを暗号化する場合、お客さまにおいて、仮想マシン上に暗号化システムを構築いただくなど、別途対応が必要となります。

なお、通信については、TLS などのプロトコルをご利用いただけます。

脆弱性診断実施時の注意事項

お客さまにおいて脆弱性診断を実施される場合、想定以上のネットワーク負荷やシステム負荷がかかることがあります。その際に当社では、脆弱性診断によるものであるのか、不正なアクセスなどによるものなのか区別できません。

そのため、お客さま側においてウェブシステムの脆弱性診断（アプリケーション診断・ネットワーク診断）を実施される場合は、事前に当社までご連絡ください。

セキュリティサービス（オプション）について

IDCF クラウドでは、オプションサービスとしてセキュリティサービスを提供しております。お客さまのご利用の用途に合わせて採用いただくことで、セキュリティを高めることができます。

DDoS 対策サービス

当社バックボーンでの自動防御に加え、より高度なサイバー攻撃に対して有効な対策を提供するサービスです。お客さまネットワークに対するトラフィックを常時引込により監視し、DDoS 攻撃を検知した場合、自動的に不正トラフィックのフィルタリングを実施します。

不正侵入検知／防御サービス（IDS/IPS）

不正侵入検知/防御サービスは、お客さまのネットワークを最新の状態に保ち、不正アクセスや攻撃などの兆候や深刻な脅威を検知・防御するサービスです。

お客さまネットワークに対するトラフィックを常時監視し、不正侵入攻撃を検知した場合、自動的にお客さまへの通知もしくは、自動的に防御を実施します。
クラウド型は現在のネットワーク構成を変更せずに導入が可能です。

ウェブアプリケーションファイアウォール（WAF）

外部からの攻撃を検知し、該当の接続を遮断します。Web アプリケーションの脆弱性を総合的に保護します。従来のファイアウォールがネットワークレベルで管理していたことに対してウェブアプリケーションファイアウォールはアプリケーションのレベルで管理を行います。

サポートについて

無料の標準サポートと、オプションのプレミアムサポートの 2 つのサポートメニューをご用意しております。

標準サポート

クラウドコンソール上の問い合わせチケット経由で、いつでも無料でオンラインサポートをご利用いただけます。
はじめてクラウドをご利用になられる場合やテクニカルなご質問にも、専門スタッフが手厚くサポートしますので、安心してご利用いただけます。

プレミアムサポート

お電話でのサポートをご利用になりたいお客さま向けに、「プレミアムサポート」もご用意しております。技術知識豊富な専門スタッフがお電話口にて直接ご対応します。チケット対応のタイムラグを気にされる方や、ビジネスユースに人気のオプションです。

※お申し込みいただいたお客さまに PIN コードを発行し、本人確認を行わせていただきます。

<table>
<tr><th colspan="2">サポート内容</th><th>サポート内容</th><th>受付時間</th><th>対応時間</th></tr>
<tr><td rowspan="2">標準サポート
標準</td><td>サービスの問い合わせ *1</td><td rowspan="2">チケット問い合わせ
*4</td><td>24時間365日</td><td>平日9:00-17:00</td></tr>
<tr><td>障害連絡受付 *2</td><td>24時間365日</td><td>24時間365日 *3</td></tr>
<tr><td rowspan="2">プレミアムサポート</td><td>サービスの問い合わせ *1</td><td rowspan="2">電話問い合わせ</td><td colspan="2" rowspan="2">平日9:00-17:00</td></tr>
<tr><td>障害連絡受付 *2</td></tr>
</table>

*1 サービス問い合わせに関しましては、土日・祝日、当社所定の休業日を除きます。
*2 当社が障害を検知した場合は、指定された連絡先にメール、電話、クラウドコンソールのいずれかで通知を行います。
*3 当社がお客さまに影響を及ぼさない事象と判断した場合を除きます。
*4 チケット問い合わせはクラウドコンソール上から行えます。

その他

デジタル証拠等について

仮想マシン等お客さまの管理が必要となる箇所のデジタル証拠については、お客さま側で取得を含めた情報の管理をお願いいたします。弊社管理部分のデジタル証拠が必要になる場合については、別途ご相談ください。

その他の基準等への対応状況について

J-Tier や FISC など他の基準については、弊社内でセルフチェックを行っております。セルフチェックの結果について必要な場合は、営業までご相談ください。また、お客さまフォーマットによるチェックシートへの記載等につきましても対応を行っております。（お客さまフォーマットによる依頼の場合回答までに時間がかかる場合があります）

5. クラウド API

IDCF クラウドは仮想化基盤として CloudStack を採用し、世界で広く利用されているオープンソースの CloudStack API を無料で公開しております。

仮想マシンの作成/削除、スナップショットの取得やボリュームの追加、オートスケール（自動拡張・縮退)など、外部プログラムから API を使って、直接クラウドリソースをコントロールすることができます。

API の利用により、手軽に開発ができるようになり開発工程の大幅短縮が可能です。さらに、システム運用の自動化によって、コスト削減・運用負荷軽減などのさまざまなメリットがあります。

6. 改訂履歴

版数	日付	主な変更内容
初版	2015/9/30	初版発行
第 2 版	2015/11/30	西日本リージョン追加
第 3 版	2016/8/22	クラウドセキュリティに関連する情報の追加
第 4 版	2016/10/14	クラウドセキュリティに関連する情報の追加
第 5 版	2017/1/11	東日本リージョン 2 追加