BIGLOBE クラウドホスティング
ホワイトペーパー
セキュリティ編

2.6 版

(2020 年 8 月 20 日)

ビッグローブ株式会社

BIGLOBE
クラウドホスティング

目次

1 はじめに

1.1 本書の目的

公共機関および一般企業では、システム構築やリプレースにおいて、クラウド環境の導入が増加しています。クラウド環境の採用は大きなメリットが得られる一方で、クラウド環境の特性やサービス仕様に対する認識と理解によっては、導入コストやランニングコストの増大はもとより、セキュリティレベルの低下をももたらすリスクがあります。組織目標を達成するために、どのようにクラウド環境を活用していくのか、それに伴う阻害要因やリスクを明確にし、有効な対策を行なうことが、IT の価値を最大限に引き出していく上で必要です。
本書では、BIGLOBE クラウドホスティング(以下、クラウドホスティングと記載します)をご検討のお客様および関連ベンダー様に対し、クラウドホスティングで提供しているセキュリティ仕様、及び注意・制限事項を開示することを目的としています。
また、別途同様のホワイトペーパーとして「仮想サーバ編」「仮想ディスク編」「ネットワーク編」をご提供しております。
ホワイトペーパーは、BIGLOBE クラウドホスティングの東日本第2リージョンについて記載しています。

1.2 用語の定義

本書で使用する用語を以下に説明いたします。

用語	説明
BIGLOBE クラウドホスティング （以下、クラウドホスティング）	仮想サーバリソースをオンデマンドでご利用いただける IaaS 型パブリッククラウドです。
仮想サーバ	1つの物理コンピュータ上に、擬似的に複数のコンピュータが稼働しているように構築された擬似サーバ。クラウドホスティングでは、お客様の設定完了から最短5分でご提供できます。
物理サーバ	仮想基盤を構成するサーバの実体。
お客様	クラウドホスティングをご利用いただく法人格の企業様。
東日本第1リージョン	既にサービス提供を終了したリージョンです。
東日本第2リージョン	2017 年 7 月にサービス提供を開始したリージョンです。 東日本地域のデータセンタを利用しています。 ※新規のお客様(東)は、第2リージョンになります。
西日本リージョン	既にサービス提供を終了したリージョンです。
コントロールパネル	ご利用担当者様自身でサーバを構築するための管理画面です。 サーバの構築のほか、各種情報の参照や連携サービスのお申し込みができます。
仮想化基盤	お客様ご利用の仮想サーバ(ゲスト OS)を提供するための基盤(インフラ)。特に指定が無い場合は、VMware vSphere。
連携メニュー	BIGLOBE クラウドホスティングと連携して利用可能なオプションサービスです。BIGLOBE 提供とソリューションパートナー企業様提供のメニューがあります。

1.3 クラウドホスティングのセキュリティに対する基本方針

クラウドホスティングは IaaS 型のパブリッククラウドのため、データセンタなどの物理環境、仮想化基盤までのセキュリティ対策が弊社の責任範囲となります。
仮想サーバに対するセキュリティ対策はお客様責任範囲となりますので、お客様にて実施してください。

第 2 章では、クラウドホスティングが信頼のおける企業から提供されるサービスであることをご説明いたします。
第 3 章・第 4 章では、クラウドホスティングの弊社責任範囲におけるセキュリティ対策をご説明いたします。
第 5 章では、クラウドホスティングのお客様責任範囲におけるセキュリティ対策をご説明いたします。ご確認の上、適切なセキュリティ対策を実施してください。

2 企業情報

2.1 公的認証

ビッグローブ株式会社では、下記の資格（マーク）を取得しています。また、経済産業省及び独立行政法人情報処理推進機構（IPA）のセキュリティガイドラインに準拠し、適切にサービスを提供しています。

■P マーク

【認定機関】
一般財団法人日本情報経済社会推進協会（JIPDEC）＜https://privacymark.jp/＞
【概要】
日本工業規格「JIS Q 15001 個人情報保護マネジメントシステム—要求事項」に適合して、個人情報について適切な保護措置を講ずる体制を整備している事業者等を認定する制度

■インターネット接続サービス安心・安全マーク

【認定機関】インターネット接続サービス安全・安心マーク推進協議会
＜https://www.isp-ss.jp/＞
＜協議会構成団体＞一般社団法人テレコムサービス協会／
一般社団法人日本インターネットプロバイダー協会／一般社団法人電気通信事業者協会／
一般社団法人日本ケーブルテレビ連盟
【概要】
一般利用者が事業者を新たに選択する際、ユーザ対策やセキュリティ対策などが、一定基準以上であるという目安を提供するものです。

■ISMS（情報セキュリティマネジメントシステム）適合性評価制度　ISO／IEC27001 認定

【認定機関】一般財団法人日本情報経済社会推進協会（JIPDEC）
＜http://www.isms.jipdec.or.jp/＞
【概要】
組織が自社で保護すべき情報資産を洗い出し、各情報資産に対して機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）をバランスよく維持し、改善していくことを可能にする仕組みを構築することを目的とした規格です。

登録活動範囲：
BIGLOBEデータセンタにおけるデータセンタ構築・運用業務

ISO 27001 証明書の対応状況は、下記のサイトで検索することが可能です。
・一般財団法人日本情報経済社会推進協会 「ISMS 認証取得組織検索」
http://www.isms.jipdec.or.jp/lst/ind/index.html
・一般財団法人日本品質保証機構（JQA）「登録事業者検索」
http://www.jqa.jp/cgi-bin/06manage/14_touroku/search_j.cgi

■エコリーフマーク

【認定機関】一般社団法人　産業環境管理協会
＜http://www.ecoleaf-jemai.jp/＞
【概要】
エコリーフ環境ラベルは LCA（ライフサイクルアセスメント）手法を用いて 製品の全ライフサイクルステージにわたる環境情報を定量的に開示する 日本生まれの環境ラベルです

2.2 BIGLOBE クラウドホスティングのサービス開始日、実績

サービス開始日 ： 2011 年 1 月 27 日
実績 ： 3000 社（2020 年 3 月末現在）
利用者 ： 法人格の企業様
SLA（※） ： 月間サーバ稼働率 99.99%
（※）対象範囲はサーバ（追加 CPU、メモリ含む）及びストレージ（追加ディスク含む）です。
ロードバランサなどのオプション、連携メニューは対象範囲外です。

2.3 情報セキュリティへの組織的な取り組みについて

クラウドホスティングは、弊社情報セキュリティポリシーに則り、継続的にセキュリティ教育を受けた適切な人・組織により運用されています。
技術的なセキュリティ対策を講じ、お客様の情報資産に対する不正な侵入、漏えい、改ざん、紛失、盗難、破壊、利用妨害などが発生しないようにするだけではなく、運用に携わる人員には、最低限のアクセス権限しか与えず、かつアクセスログを取るなどのセキュリティ対策を講じ、問題が発生しないように努めています。
また、万が一セキュリティ上の問題が発生しても、その原因を迅速に究明し、その被害を最小限に留めるとともに再発防止を実施します。

弊社は、情報セキュリティに関係する法令、国が定める指針、その他の社会的規範を遵守します。各法令に従った開示請求があった場合は、開示請求の範囲内で情報を開示することがあります。関係する法令は、「BIGLOBE クラウドホスティングサービス契約約款」をご確認ください。

3 物理的・環境的セキュリティ

3.1 データセンタについて

クラウドホスティングでは、信頼性の高いファシリティを持つデータセンタでサービスを運用しています。
運用においては、BIGLOBE セキュリティポリシーを習得したセキュリティ対策チームが 24 時間／365 日のサービス体制で常駐しており、プライバシーマークの認定取得事業者として個人情報の取扱い管理を徹底しています。
なお、データセンタは、日本国内に存在しますが、セキュリティ確保の観点から、所在地およびファシリティに関する詳細は公開しておりません。

（参考）日本データセンタ協会（JDCC）が制定した「データセンタファシリティスタンダード」ガイドラインの項目を基準に弊社データセンタのファシリティ情報をまとめています。

【基準項目　一覧表】 最低限必要と考えられる項目

項目	東日本第2リージョン
建物（B）	
建物用途（建物としてDC専用であるか否か）	DC専用　DC 関連複数テナント
地震リスクに対する安全性　建築基準法による評価の場合	1981 年 6 月改正の建築基準法に準拠、かつ官庁施設の総合耐震計画基準 I 類に準拠
セキュリティ(S)	
セキュリティ管理レベル	敷地、建屋、サーバ室、ラック
電気設備(E)	
受電回線の冗長性	あり
電源経路の冗長性（受電設備～UPS 入力）	あり
電源経路の冗長性（UPS～サーバ室 PDU）	あり
自家発電設備の冗長性	あり
UPS設備の冗長性	あり
空調設備(H)	
熱源機器・空調機器の冗長性	あり
熱源機器・空調機用　電源経路の冗長性	あり
通信設備（T）	
引き込み経路　キャリアの冗長性	あり
建物内ネットワーク経路の冗長性	あり
設備運用(M)	
常駐管理体制	24 時間×365 日の常駐管理
運用マネジメントの仕組みと運用（運用要員の育成プログラムなど含む）	ISO27001 の認証又は FISC 運用基準に準拠

【推奨項目 一覧表】信頼性確保のために採用が望まれる項目

立地条件その他リスク(R)	
地盤の安定性	ハザードマップ被害想定区域外
施設周辺の環境(地震後火災による延焼危険度の高い住宅密集地，爆発物を持つ危険施設がある地域、復旧活動のためのアクセスルートが確保し難い地域などに位置していないか)	位置していない、もしくは位置しているが、対応準備がある
建物(B)	
設備(機器、配管等)の耐震安全性 震度 6強以上	IT 機器、重要機器、一般機器 耐震対応あり(※1)
地震発生後の早期復旧体制・準備地震時に被害や施設の機能停止が発生した場合に早期に復旧できるための体制・準備(緊急対応マニュアル、防災マニュアル、BCP 等)があるか	早期復旧体制・準備がある
建物の耐火性能	耐火建築物
サーバ室及びデータ保管室(C)	
耐火性能、区画	建築基準法による耐火建造物
サーバ室の前室	建築基準法による耐火建造物
サーバ室の超高感度火災検知システム	あり
ガス系消火システム	あり
サーバ室の漏水検知システム	あり
セキュリティ(S)	
アクセス管理 敷地	人又は IC カード
アクセス管理 建物	人又は IC カード・生体認証
セキュリティ監視 敷地	人又はカメラ、センサー
セキュリティ監視 建物	人又はカメラ(画像の記録またはモニタリングのみ)
電気設備(E)	
電気室、UPS 室の区画	独立した専用区画室
サーバ室照明電源の冗長性	商用+自家発電設備
UPSの停電補償時間	10 分
オイル確保量(オイル供給会社の優先供給契約を含む)	72 時間
中央監視設備の冗長性	なし(FTサーバを採用し、信頼性を上げた構成としている)

通信設備(T)	
建物内通信機器（ルータ／スイッチ）の冗長性	あり
通信関連機器電源の冗長性	あり
通信ケーブルと電源ケーブルとの離隔	あり
設備運用(M)	
全体エネルギーマネジメントの実施（電力・温湿度・他の常時監視を含む）	実施している

（※1）IT 機器：サーバラック、フリーアクセスフロア等
重要機器：サーバ等の機能維持に関連する設備
一般機器：IT 機器・重要機器以外の設備

3.2 入館ポリシー

お客様による弊社データセンタへの入館はできません。

4 仮想化基盤のセキュリティ対策

仮想化基盤（お客様が利用する仮想サーバを収容しているインフラ）のセキュリティ対策を説明しています。

4.1 耐障害性

クラウドホスティングの仮想化基盤で利用している主要な物理サーバ、ネットワーク回線、ストレージ等は冗長構成にて運用しており、サービス停止のリスクを軽減しています。
また、仮想化基盤にはヴイエムウェア社の vSphere を採用し、物理サーバに障害が起きた際、お客様の仮想サーバを正常稼働する別の物理サーバ上に再配置（フェイルオーバー）します（HA 機能）。

ただし、基盤の冗長構成は、お客様がご利用中の仮想サーバの無停止を保証するものではありません。
仮想化基盤の障害やメンテナンス時には、ネットワーク I/O やストレージ I/O の瞬断が発生する場合があります。
また、VMware の HA 機能（vSphere HA）によるフェイルオーバーが発生した場合は、仮想サーバの強制再起動が発生します。お客様がご利用中の仮想サーバについては「5.1 障害対策」をご確認ください。

4.2 アクセス制御／アカウント管理

仮想化基盤へのアクセスはサービス運用者しか行えないように制御されています。また、弊社の運用者であっても社外からインターネット経由で仮想化基盤の操作ができないようになっています。
サービス運用者のアカウントは、共通 ID を利用せず、必要最低限のアクセス権限を付与した形で個別に払い出されています。そのアクセス権限は、適切な承認を得られないと付与できないようにシステム的に管理されています。
また、弊社が所有しているいかなるアカウント権限を利用しても、お客様が利用されている仮想サーバ上のデータへのアクセスはできないようにシステムを設計・構築しています。

4.3 データ保全

仮想化基盤システムのストレージ装置では、1 日 1 回スナップショットを取得しています。仮想化基盤障害が発生した場合は、スナップショットデータを利用して、前回取得した状態までリストアすることが可能です。

このスナップショットデータは、仮想化基盤の障害復旧を目的としているため、お客様事由による障害復旧にはご利用いただけません。
ご利用中の仮想サーバのバックアップについては、「ホワイトペーパー 仮想ディスク編」をご確認の上、お客様にてご対応ください。
※上記の “スナップショット” とは、ストレージ基盤のスナップショット機能のことであり、クラウドホスティングのコントロールパネルで提供しているスナップショット機能とは異なります。

4.4 パッチ適用

仮想化基盤へのパッチ適用は、十分な情報収集及び動作検証を実施した上で必要に応じて実施しています。
セキュリティパッチは、仮想化基盤で利用している OS、ミドルウェア、アプリケーションに対して行われます。
お客様ご利用中の仮想サーバには適用されません。お客様ご利用中の仮想サーバについては、「5.7 パッチ適用」をご確認ください。

リリース管理
クラウドホスティングでは、以下の3つの過程を経て新機能をリリースしています。

(1) 評価環境での検証
検証は、評価環境で実施しています。
評価環境で異なる複数人員が同じ項目に対して条件を変えながら繰り返し検証することで、不具合を迅速に検出するように努めています。
また、操作検証だけではなく、本番環境適用中に不具合が発生する可能性も考慮し、切戻し作業を想定したリリース作業検証も行っています。

(2) 脆弱性チェック
リリースされるプログラムは、コードチェックなどのセキュリティ（脆弱性）診断を必ず実施し、本番環境適用後に問題が発生しないような予防対策を行っています。

(3) 本番環境への適用
検証結果をまとめた移行作業手順を元に本番環境への適用を行います。リリース作業は、複数人員によるクロスチェックを徹底しています。検証と異なる事象が発生した場合は、作業担当者だけの判断で作業内容を変更することはなく、適切な承認プロセスを経て作業を進めていきます。

4.5 ネットワークセキュリティ対策

仮想化基盤のネットワークについては、外部からの攻撃に対して、セキュリティを確保するため、弊社が培ってきたノウハウを基にネットワークセキュリティ対策を実施しています。

この対策は、仮想化基盤で利用しているネットワークに対してのみ行われ、ご利用中のお客様の仮想サーバへは実施されません。お客様の仮想サーバは直接インターネットへ接続している状態ですので、適切なセキュリティ対策を実施してください。なお、弊社対策の設定内容詳細についてはお客様に開示いたしません。

対象	管理者	対策
仮想サーバ	お客様	お客様にて実施していただく必要があります。 ※仮想サーバ作成後の初期状態では「5.2 章　アクセス制御」に記載されている最低限のセキュリティ対策を実施しております。
仮想化基盤	弊社	・通信フィルタリングによる不要なポートの閉塞 ・不要なネットワーク間の接続禁止 ・重要性・脆弱性に応じた適切なアクセス制限 ・外部からの攻撃対策　　等

また、仮想サーバが送受信するネットワーク上のデータをキャプチャし、弊社から内容を確認することはありません。

4.5.1 外部からの攻撃対策

仮想化基盤の上位ネットワークにて振る舞い検出型の DoS/DDoS 防御対策を実施しています。攻撃として検出されたトラフィックのみを遮断し、それ以外のトラフィックはサーバへ配送します。外部からの攻撃対策は自動化しており、即時対応を可能にすることで、仮想化基盤への影響を最大限軽減しています。

お客様の仮想サーバが攻撃元となっていることが判明した場合、他のお客様への波及を防ぐために、弊社にて仮想サーバのネットワークを遮断いたします。

4.6 監視

仮想化基盤に対する監視においてアラートが発生した場合は、24 時間 365 日体制で待機している弊社オペレータが迅速に適切な対処を実施します。

例）

基盤を構成する物理サーバに対する監視

・IP アドレスに関する死活監視
・サービス応答監視
・リソース監視
・イベント監視
・ログ監視　　等

これらの監視内容の詳細は開示いたしません。また、仮想化基盤のシステムログ等はお客様に提供いたしません。

監視は仮想化基盤に対してのみ行われ、お客様ご利用中の仮想サーバに対しては行われませんので、仮想サーバに対する監視は、お客様にてご対応ください。

4.7 障害対応

お客様からの障害申告を受け、クラウドホスティングの仮想化基盤の不具合または障害と確認された場合、平日／休日／夜間問わず、迅速に障害復旧体制を整え、早期復旧に努めます。

ただし、弊社営業時間外(平日夜間 17:00-9:00 および休日)にお問い合わせいただいた際の対応範囲は、「サーバに接続できない」または「コントロールパネルのログイン画面に接続できない」場合で弊社が再現可能な不具合・障害に限ります。それ以外の場合には、翌営業日以降の対応となります。

翌営業日対応の例）

・利用料金、費用に関するもの
・サーバへのリモート接続（SSH/RDP）は可能だが、コンソール接続ができない

また、ご利用中の仮想サーバのお客様責任範囲（OS、ミドルウェア、アプリケーション）の設定等に起因する障害には対応できません。

障害情報は、運用／障害情報サイトに、随時掲載いたします。

障害情報の初報を掲載した際に、お客様の通知先メールアドレスへ障害通知メールを送信します。通知先メールアドレス、障害通知メールの送信設定はコントロールパネルから変更可能です。

5 仮想サーバのセキュリティ対策

仮想サーバ（お客様がご利用されるサーバ）のセキュリティ対策を記載しています。

5.1 障害対策

「第 4.1 章　耐障害性」で記載した通り、仮想化基盤のメンテナンス時等にお客様が利用している仮想サーバのネットワーク I/O 等に瞬断が発生することがあります。また、物理サーバ障害で vSphere HA が実行された場合、仮想サーバは強制再起動されます。
強制再起動は VMware の製品仕様であり、クラウドホスティングのサービス仕様であるため回避することはできません。また、物理装置の故障を完全に回避することもできません。

このため、ご利用中の仮想サーバに対しては、お客様にて監視を行い、瞬断および再起動が起こった場合は必要に応じて適切な対処を行っていただくようにお願いいたします。
万一の障害に備え、仮想サーバやアプリケーションサービスの冗長構成を組むことやバックアップを取得することを推奨いたします。
ロードバランサを利用した仮想サーバの冗長構成については、「ホワイトペーパー　ネットワーク編」、バックアップについては「ホワイトペーパー　仮想ディスク編」をご確認ください。

なお、フェイルオーバーによる強制再起動が発生した場合は、運用／障害情報サイトに掲載いたします。お客様への個別連絡はいたしません。

5.2 アクセス制御

仮想サーバのアクセス制御はお客様にて実施していただく必要があります。
クラウドホスティングで作成した直後の仮想サーバには、OS のアクセス制御機能（iptables・firewalld・TCPWrapper／Windows ファイアウォール）を利用して最低限のセキュリティ対策を行っています。
不要なポートを閉塞することで外部からの攻撃対象となるリスクを軽減することができます。仮想サーバ作成直後に設定されているアクセス制御については、「ホワイトペーパー　仮想サーバ編」をご確認ください。

また、仮想サーバ上のデータは、契約者であるお客様およびお客様よりアクセス許可を受けた第三者（SIer 等）しかアクセスできません。

5.3 アカウント管理

(1) OS アカウント

仮想サーバのアカウント管理はお客様責任範囲となります。弊社では、特権アカウント（※1）も含め、OS アカウントについての問い合わせや調査依頼にはお応えできません。

仮想サーバの特権アカウントの初期パスワードは、サーバ作成時に自動的に割り当てています（※2）。セキュリティ対策上、SSH 接続またはリモートデスクトップ接続にて特権アカウントで初回ログイン後、特権アカウントのパスワードを必ず変更してください。
合わせて、セキュリティ確保の観点より、以下の対策を推奨いたします。
・仮想サーバで作業をする際は特権アカウントを使用せず、新規アカウントを作成して利用する
・特権アカウントも含め、アカウントのパスワードは定期的に変更する
・Windows Server 2008 の場合、「Administrator」を無効化する

（※1）Linux 系 OS ： root
Windows Server 2008 ： Administrator
Windows Server 2012 / 2016 / 2019 ： サーバ作成時に任意の名前で管理者アカウントを作成

（※2）Linux 系 OS ： root の初期パスワードはお知らせしておりません。
Windows Server 2008 ： 特権アカウントの初期パスワードは、サーバ作成時のメールにてお知らせしています。
Windows Server 2012 / 2016 / 2019 ： 初期状態で「Administrator」は無効化されています。

(2) コントロールパネルのユーザ ID

コントロールパネル（クラウドホスティング上でサーバ作成・変更・削除などの操作をするための管理ポータル）へログインする際に利用するユーザ ID とパスワードは、弊社より払い出された後、お客様にて管理していただく必要があります。
ログインの際、パスワードを 3 回間違えて入力すると画像認証の入力が必要となります。

また、ユーザ ID を追加登録する際にはコントロールパネルの操作権限を指定することが可能です。
操作権限は以下の 3 種類です。
・アドミニストレータ :コントロールパネルの全ての操作が可能
・オペレータ :利用料が変動しない操作のみ可能
・モニタリングユーザ :コントロールパネルでの参照のみ可能
これにより、担当者の業務内容に応じた権限の設定が可能になるため、複数担当者がいる場合でも、より安全にクラウドホスティングを運用することができます。

5.4 データ管理

クラウドホスティングでは、お客様データの暗号化に関するオプションはご用意しておりません。
仮想サーバで利用しているデータの暗号化が必要な場合は、お客様にて実施していただく必要があります。

また、仮想サーバ削除時のデータ廃棄ポリシーは、「ホワイトペーパー 仮想ディスク編」をご確認ください。

5.5 バックアップ

クラウドホスティングでは、仮想サーバのデータ保全のために BIGLOBE クラウドバックアップというメニューを用意しております。BIGLOBE クラウドバックアップは、仮想化基盤以外の場所へデータを保存することができるため、

クラウドホスティングの重大障害からのデータ復旧にも利用することができます。BCP／DR 対策にご利用ください。
また、以下の連携メニューもご用意しておりますので、必要に応じてご検討ください。
・リモートバックアップサービス ライト（株式会社 TOKAI コミュニケーションズ提供）
・大容量バックアップ専用サーバ構築サービス（株式会社レオンテクノロジー提供）

その他、追加ディスクを利用してデータ保存を行う、お客様にてバックアップツールをご導入いただくなどの対策をとることも可能です。

仮想サーバのバックアップについては「ホワイトペーパー 仮想ディスク編」に記載しておりますので、ご確認いただいた上で、お客様の環境に合わせたバックアップ対策を実施してください。

※BIGLOBE クラウドバックアップの詳細については、以下 URL をご参照ください。
https://business.biglobe.ne.jp/hosting/app/appliDetail.do?APP_ID=0000001448&NEXT_DISPLAY_ID=M100121&APP_IMG_FLG=0&APPLICATION_ID=00000000000000000000000000000000001181

5.6 マルウェア対策

仮想サーバのマルウェア対策はお客様にて実施していただく必要があります。

5.7 パッチ適用

仮想サーバの OS、ミドルウェア、アプリケーションのパッチ適用はお客様にて実施していただく必要があります。
仮想サーバ作成直後の自動更新設定（yum コマンド／WindowsUpdate）は、有効となっています。環境に合わせて設定変更等行ってください。
仮想サーバの初期設定詳細は、「ホワイトペーパー　仮想サーバ編」をご確認ください。

5.8 ネットワークセキュリティ対策

グローバル IP アドレスが付与された仮想サーバの作成直後は、「5.2　アクセス制御」の設定をされた状態で直接インターネットへ接続されている状態です。外部からの攻撃に対しては、お客様にて必要に応じて適切なセキュリティ対策を実施してください。
一般的な対策としては以下の通りです。

(1) ファイアウォール
クラウドホスティングでは、仮想ファイアウォールをオプションとしてご用意しています。ファイアウォールの詳細は、「ホワイトペーパー　ネットワーク編」をご確認ください。

(2) 不正侵入防御（IPS）／不正侵入検知（IDS）
クラウドホスティングでは、不正侵入検知のために以下の連携メニューをご用意しております。
・最新サーバーセキュリティ IPS（不正侵入防御システム） for BIGLOBE クラウドホスティング
（株式会社サイバーセキュリティクラウド 提供）

その他、お客様にて仮想サーバ上へ不正侵入防御（IPS）／不正侵入検知（IDS）のソフトウェアをインストールして実現することも可能です。

(3) Web アプリケーションファイアウォール（WAF）
クラウドホスティングでは、ホスト型 Web アプリケーションファイアウォール（WAF）「InfoCage SiteShell」をオプションとしてご用意しています。
また、連携メニューとして、「クラウド型 WAF / cloudbric ＆ シマンテック クラウド型 WAF」をご用意しています。クラウド型 WAF（cloudbric ＆ シマンテック クラウド型 WAF）は、お客様のサービスシステムに対し、設備投資なしで WAF（Web Application Firewall）の機能を提供するサービスです。
サイバー攻撃のリスクを軽減しつつ、頻発するパッチ適用やシステムリニューアルを計画的に行えるようにし、TCO の改善に寄与します。

(4) Web 改ざん検知
クラウドホスティングでは、連携メニューとして、「クラウド型Web改ざん検知 / gred」をご用意しています。二重三重の対策を整えていても、Web を改ざんされる恐れは残念ながらゼロにはなりません。
不測の事態に備え、自社のサイトが改ざん・マルウェア汚染してしまっていないかを自動で監視し、迅速な被害の検知と拡大防止・ブランド毀損予防を支援します。

5.9 ログ確認／監視

クラウドホスティングでは、コントロールパネルの操作ログ、仮想ファイアウォールのアクセスログを確認できる機能を標準で提供しています。仮想サーバのサーバログについては、お客様にて OS へログインした後確認をしていただく必要があります。

・コントロールパネルの操作ログ
コントロールパネルから当月および当月を含まない過去3カ月の間に行った操作ログを確認することができます（例：11/30 に表示した場合は 8/1 以降のデータを確認可能）。

・仮想ファイアウォールのログ
ファイアウォールのドロップログを確認することができます。ログで確認できる内容は以下の通りです。

日付、アクション、通信方向、プロトコル※、送信元 IP アドレス/送信元ポート番号->宛先 IP アドレス/宛先ポート番号 TCP のフラグ
※TCP、UDP 以外のプロトコルの場合、プロトコルの後にプロトコル番号が入ります。

コントロールパネル上では最新 100 件を表示しています。ログをダウンロードすることで上限値（※）まで確認できます。
（※）上限値は標準で 1 万件です。有償オプションを利用すると 30 万件まで拡張することができます。
また、ログは DROP のみで Allow は確認できません。保管期限は最長で 1 年となります。

特定のポートについては特殊な条件下（リフレクター攻撃の踏み台にされる等）でログが大量に出力されるため、現在 DROP はしますがログに出力されません。（ファイアウォールのルールに定義（許可）した場合、他のルールと同様に通信は可能となります。）
（※）現在ログに出力されないポート番号：389/udp

ログはファイアウォールを購入しているサーバ全てについて一括表示されます。

ログ上限値を超過したログ、保管期限を超過したログは自動削除されるため、必要に応じてログダウンロードを実施してください。

同一の宛先 IP アドレスに対して、1 秒あたり 30 件以上のログがある場合、参照可能なログは 1 件となります。

同一の送信元 IP アドレスに対して、1 秒あたり 30 件以上のログがある場合、参照可能なログは 1 件となります。

・仮想サーバのログ
仮想サーバ上の OS システムログ、アクセスログ、アプリケーションログ等は、お客様にて OS にログイン後、OS 既定の場所をご確認ください。

クラウドホスティングでは、連携メニュー「サーバ運用支援サービス」にてログ監視のオプションをご用意しています。イベントログ（Windows）やアプリケーションログファイル監視などについて有償対応が可能です。
詳細は「サーバ運用支援サービス」をご確認ください。

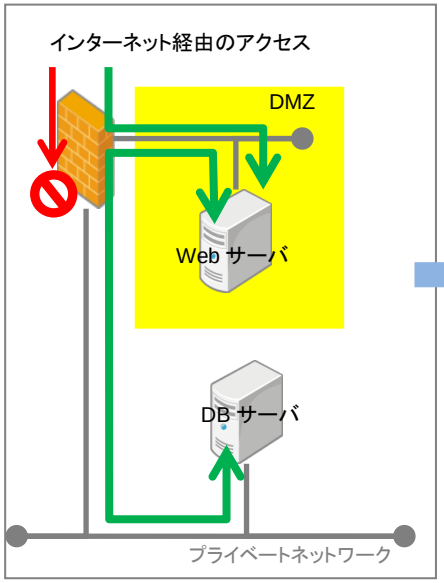
5.10非武装地帯（DMZ）

クラウドホスティングでは、非武装地帯（DMZ）に関するオプションをご用意しておりません。
OS のアクセス制御機能（iptables・firewalld・TCP Wrapper／Windows ファイアウォール）や仮想ファイアウォールを利用して、アクセス可能なサーバの IP アドレスを設定することにより擬似的な DMZ を作成する事ができます。
その際、インターネットからのアクセスがないサーバは、グローバル IP アドレスを割り当てないことで、高いセキュリティレベルを保つことも可能です。

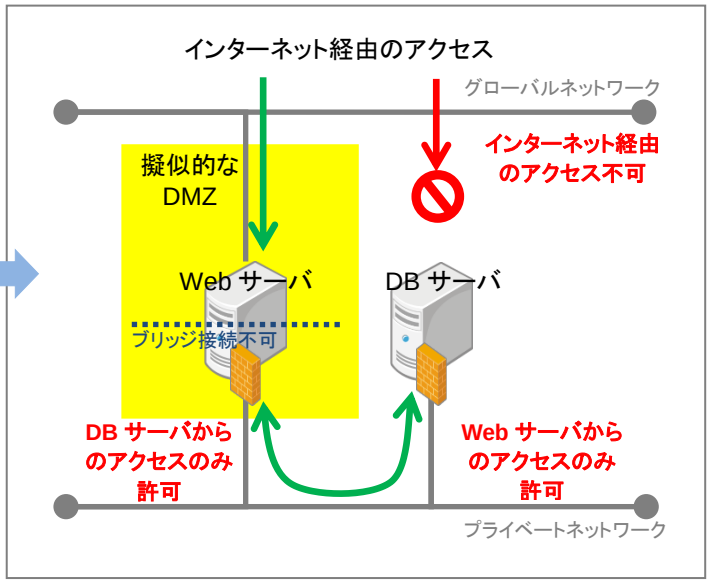
以下、DMZ 構成を擬似的な DMZ に置き換えた場合の構成（例）です。

・Web サーバの設定
　グローバルネットワーク側　：インターネットからのアクセスはすべて許可する
　プライベートネットワーク側　：ファイアウォールで DB サーバ間のアクセスのみ許可する
・DB サーバの設定
　グローバルネットワーク側　：グローバル IP アドレスを持たないサーバとして構築する
　プライベートネットワーク側　：ファイアウォールで Web サーバ間のアクセスのみ許可する

＜一般的な DMZ 構成＞



＜クラウドホスティングによる擬似的な DMZ 構成＞



5.11セキュリティ（脆弱性）診断

クラウドホスティングでご利用中の仮想サーバに対するセキュリティ（脆弱性）診断は、他のお客様に影響を与える可能性があるため、基本的にはお断りしています。
ただし、お客様の業務上どうしても必要な場合は、遵守事項に同意していただくことを条件に実施できる場合もございます。

【遵守事項】
- ・擬似 DoS 的なアタックテストをしないこと
- ・同時に複数サーバを診断しないこと
- ・ご利用中のサーバだけを対象とすること
- ・基盤に影響が見られた場合は、弊社の判断でお客様への確認なく当該サーバを停止（診断の中断・終了）する可能性があること
- ・負荷試験および破壊検査を行わないこと
- ・土日祝日・弊社指定の休日を除く 9:00～16:00 に実施し、診断開始、終了時にご連絡頂くこと

脆弱性診断をご検討の場合は、必ず BIGLOBE 法人コンタクトセンターまでご相談ください。
ご申告がない場合、診断か攻撃かを区別できないため、強制切断を行う場合があります。

クラウドホスティングでは、連携メニューとして「クラウド型ぜい弱性診断 / SCT SECURE クラウドスキャン」をご用意しています。SCT SECURE クラウドスキャンは、リリースされたサービスシステムにおいて新たな脆弱性が生まれていないかを自動で定期的に診断するサービスです。
お客様自身による臨時点検やバグ情報トレースの手間を大幅に軽減できます。

6 その他関連情報

BIGLOBE クラウドホスティング　ユーザマニュアル
https://biz.biglobe.ne.jp/hosting/customer.html

クラウドホスティングのサービス詳細および利用方法をまとめたドキュメントです。
上記サイト以外にも、ご契約後のコントロールパネルからもご確認いただけます。

BIGLOBE クラウドホスティング　API リファレンスガイド
http://help.cloudhosting.biglobe.ne.jp/cloudhosting/api/

クラウドホスティングの API 情報をまとめたドキュメントです。
API をご利用いただくには、別途お申し込みが必要になります（無料）。

BIGLOBE クラウドホスティング　ホワイトペーパー
https://biz.biglobe.ne.jp/hosting/customer.html

クラウドホスティングの詳細情報です。
「仮想サーバ」、「仮想ディスク」、「ネットワーク（予定）」、「セキュリティ（本書）」を提供しています。

BIGLOBE クラウドホスティング　よくあるご質問
https://biz.biglobe.ne.jp/hosting/faq/index.html

クラウドホスティングの検討・ご利用にあたって、お客様のお問い合わせが多い項目について記載しています。
疑問点がございましたら、まずこちらをご確認下さい。

BIGLOBE クラウドホスティング　サービス仕様
https://biz.biglobe.ne.jp/hosting/feature.html

クラウドホスティングのサービス仕様および品質保証について記載しています。
サービス導入をご検討の方は最新の情報をご確認頂き、ご検討ください。

BIGLOBE クラウドホスティング　料金シミュレータ
https://sim.business.biglobe.ne.jp/hosting/cloud/

クラウドホスティングの料金を月額プランでシミュレーションします。

BIGLOBE クラウドホスティング　運用／障害情報掲載サイト
http://help.cloudhosting.biglobe.ne.jp/cloudhosting/info/

クラウドホスティングに障害が発生した場合に障害情報を掲載します。

その他お問い合わせ先（サービスご契約済のお客様）
https://biz.biglobe.ne.jp/hosting/login/index.html

コントロールパネルのお問い合わせフォームをご利用ください。

その他お問い合わせ先（サービスご利用検討中のお客様）
https://biz.biglobe.ne.jp/hosting/index.html

お問い合わせフォームからお問い合わせください。

ご注意

本書の内容の一部または全部を無断転載することは禁じられています。
本書の内容に関しては将来予告なしに変更することがあります。
本書の内容については万全を期して作成いたしましたが、万一ご不審な点や誤り、記載もれなどお気づきのことがありましたら、BIGLOBE 法人コンタクトセンターへご連絡ください。

商標について

- ✓ VMware vSphere は VMware, Inc.の米国および各国での商標または登録商標です。
- ✓ Linux は、Linus Torvalds 氏の米国およびその他の国における商標または登録商標です。
- ✓ Red Hat は、米国およびその他の国における Red Hat.Inc.の商標または登録商標です。
- ✓ Microsoft、Windows は米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
- ✓ Oracle は米国 Oracle Corporation の登録商標です。
- ✓ InfoCage、SiteShell は日本電気株式会社の登録商標です。
- ✓ その他、本マニュアルに掲載された各社名、各製品名、各ロゴは、各社の登録商標または商標です。

BIGLOBE クラウドホスティング
ホワイトペーパー
セキュリティ編

2.6 版　2020 年 8 月

ビッグローブ株式会社