IBM Cloud
技術解説書

INDEX

1

はじめに

INDEX

1-1. 本書の目的

本書は、IBM Cloud のインフラ系サービスを利用したシステム開発における実装方式、および理解しておくべきポイントを整理し、効果的、効率的なシステム開発にご参考いただけることを目的としています。

クラウドが、ITの選択肢の一つとして当然ながら検討される、もしくは、クラウド・ファーストで検討されるようになったビジネスにおいて、クラウドを「理解している」ことは提案する側にとっても、提案を受ける側にとっても重要です。
ハイブリッド・クラウドやマルチ・クラウドへと進む昨今、この重要性は増しているでしょう。

クラウドは、その特性上、次々と新しい機能が追加されます。使われている機能は拡張され続け、一方で使われていない機能は縮小され、全体的な効率化が図られています。さらに利用できる機能やサービスが多岐多様にわたるため、検討対象であるクラウドの全体像を把握しつつ、また細部に及ぶ仕様を網羅的に把握することは容易ではありません。

本書は、情報提供および再利用いただくための資料として、IBM Cloud のテクニカル・セールス有志で作成されたものです。
最新情報は、IBM Cloud Docs（https://cloud.ibm.com/docs）をご参照ください。IBM Cloud Docsと本書の内容が異なる場合、IBM Cloud Docsの記載内容が「正」となります。

※ 当資料は、2019年9月改定の「IBM Cloud 柔らか層本」(http://ibm.biz/yawarakasou) を編集したものです。

1-2. 対象読者

● 本書の主な対象読者は以下のとおりです。

IBM Cloud を利用したシステムの企画・設計・構築に携わる立場の方
（システム部門やユーザ部門のプロジェクト参加者）

例：

- クラウド・サービスをビジネス面及び技術面から、**利用者への提案ソリューションとして評価、決定する方**
- **ITアーキテクト及びソフトウェア・アーキテクト**：利用者のビジネス・ニーズのためにクラウドを評価し、その機能をどのように適用するかを評価、決定、提案する方
- **アプリケーション開発者**：クラウドの機能を理解し、担当するアプリケーションにその機能を活用したい方
- **セキュリティ・スペシャリスト**：クラウドを利用する際に、サーバーやデータを保護するための構成や手法を設計する方
- **ストレージ・スペシャリスト**：ストレージを提案、構築、運用、管理するため、ストレージ構成を検討し決定する方
- **ネットワーク・スペシャリスト**：ネットワークを管理、構築、運用、提案することを目的にネットワークの接続方法やパフォーマンス上の考慮点などを理解したい方ネットワークを管理、構築、運用、提案する方

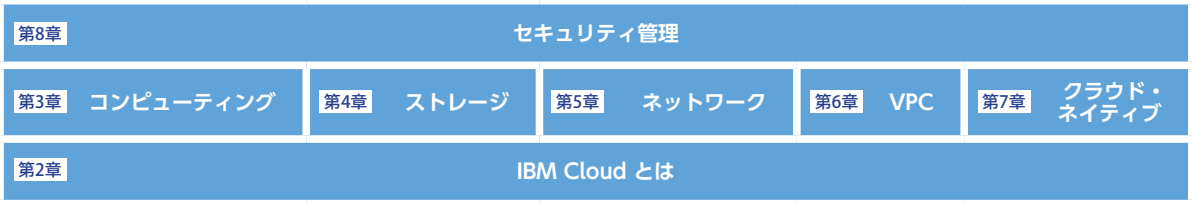
なお、本書では、以下のような見出しで補足情報を記載しています。

作業の効率化やトラブル回避のために知っておくと便利な情報を記載しています。

IBM Cloudを利用すると、類似のサービスと比較して、（強力な）メリットがあるようなお得な情報や推奨構成について記載しています。

1-3. 本書の構成

● 本書では以下の構成となっています。



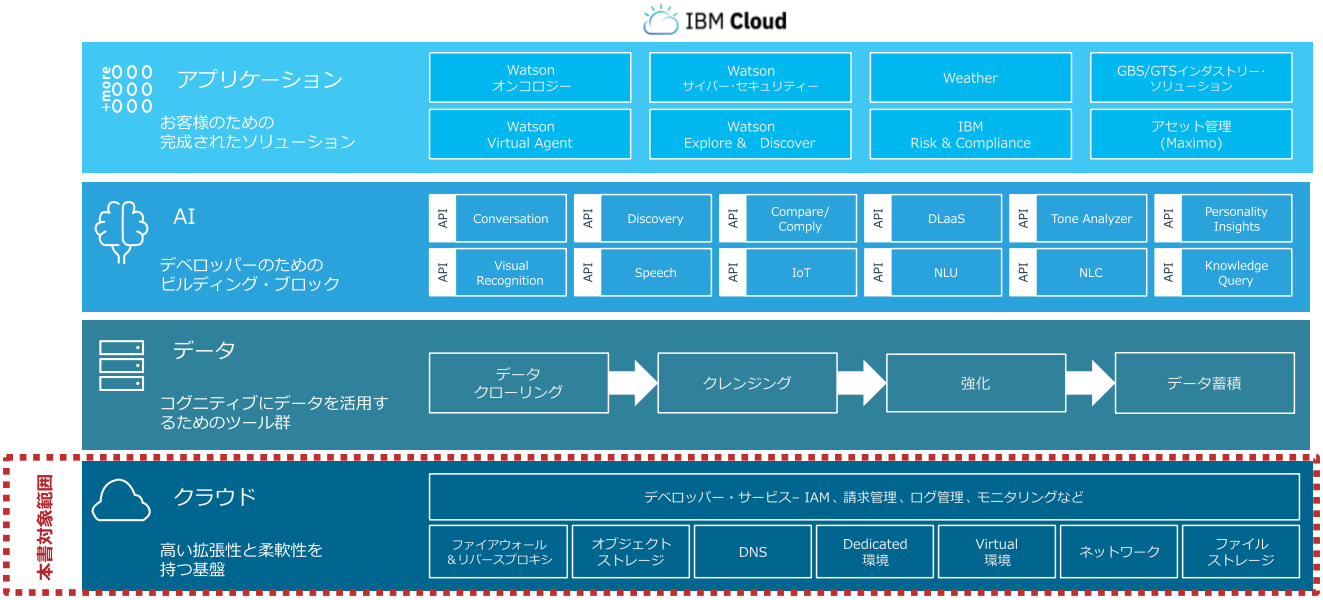
2

IBM Cloud とは

INDEX

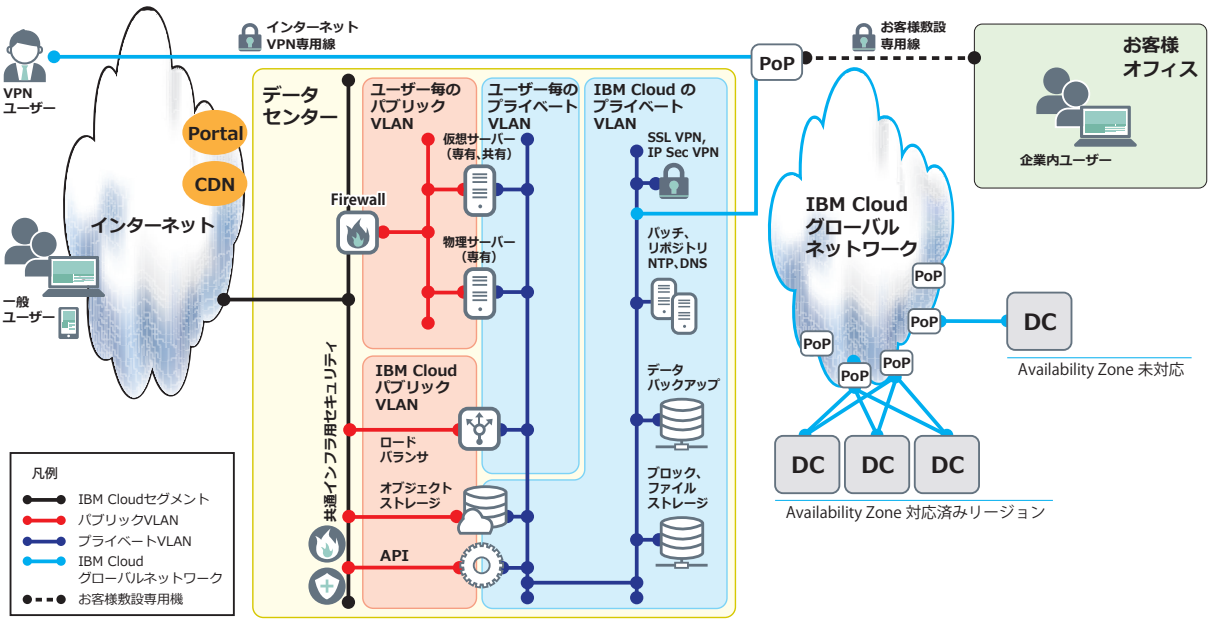
2-1. IBM Cloud とは

IBM Cloud はオープンテクノロジーを基本に構成されたIBMのクラウドサービスです。
「アプリケーション」、「AI」、「データ」を支えるプラットフォームとして、SaaS、PaaS、IaaSなど様々なサービスが利用できます。
本書ではインフラストラクチャーのサービスを中心に記載しています。



2-2. IBM Cloud のインフラとは

IBM Cloud 上で利用できるサービスは、インターネットからアクセスできるパブリックVLAN（赤）と、専用ネットワークとして利用できる、プライベートVLAN（青）上に配置されます。以下はIBM Cloud の概要図です。各コンポーネント内のサービスによっては、配置先が異なるものがあります。



IBM Cloud のインフラは、2013年にIBMに買収されたSoftLayer Technologies Inc.のサービス（2005年創業）が基盤となっています。
IBMによる買収後から現在に至るまで、IBMクラウドのインフラも支えるIaaS として多くの企業様にご利用いただいています。
2016年にPaaSやSaaSのクラウドサービスと統合し、Bluemixに名称が統一されました。そののち、Watsonが加わり、2017年11月にIBM Cloudとしてブランド統合されました。"物理サーバーのラインナップが最も充実している"、"世界中のDC間が接続するグローバルバックボーンを無償で使える"、"VMware、OpenShift、SAPが利用できる"など他のクラウドにはない特徴があります。

物理・仮想サーバーを利用できます

- 物理サーバーも時間単位で利用できる
  最新スペックの物理サーバーを、
  月単位または時間単位で利用できます。
- 専有環境のセキュリティーと性能
  他の利用者の影響や仮想化による
  性能劣化がない専有の物理環境は、
  高いセキュリティー要件や性能要件に
  適しています。

充実の技術サポート

- 日本語による無償の技術サポート
- 24/365の無償で利用できる支援システム
- お客様専用TAM*（プレミアムサポート利用で任命される）

Caseを作成する　チャットする　電話サポート（契約者専用）

*Technical Account Manager

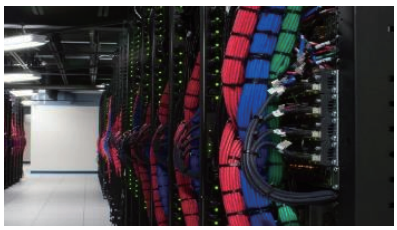
グローバル高速ネットワーク

- 無償で自由に使える国際専用回線
  10Gbps以上のTier1キャリア網で構成された、高品質広帯域の国際専用回線をご利用いただけます。
  利用者ごとに分離されたグローバルプライベートネットワークとしてご利用いただけます。

VMwareやOpenShiftをサービス提供

- ライセンスの持ち込みも可能
- 既存のシステムやノウハウ、スタッフ、ツールをそのまま活用してクラウド利用可

IBM Cloud データセンターは1つのアーキテクチャーに基づいて設計されています。IBM Cloud で利用できるコンピューティング環境には、仮想サーバー、物理サーバー、コンテナ、Cloud Foundry、Serverlessがあります。
前出のパブリックVLANは赤色ケーブル、プライベートVLANは青色ケーブルで構築されています。



IBM Cloud データセンターラック

利用可能な物理サーバーは、
CPU数、内蔵可能なDisk数などによって上図のようなサーバーになります。

物理サーバー

DCを選択 ＋ CPUを選択 ＋ メモリを選択 ＋ OSを選択 ＋ Disk/RAIDを選択 ＋ ネットワークポートを選択 ＋ 各種オプションを選択

仮想サーバー

DCを選択 ＋ CPUとメモリをFlavorから選択 ＋ OSを選択 ＋ Diskを選択 ＋ ネットワークポートを選択 ＋ 各種オプションを選択

2019年8月現在、IBM Cloud のデータセンターは60拠点以上あります。アベイラビリティ・ゾーンは6リージョンあります。各データセンター間は高速・広帯域の専用線で結ばれています。一般的なクラウドでは課金されてしまうデータセンター間の通信料金を支払うことなく、データセンター間を通信できるのが特徴です。
ネットワーク転送の従量課金制に縛られることなく、グローバルにまたがるシステムを比較的安価に構築できることが、多くの利用者から高く評価されています。

● Data Center & Network PoP　◇ Region　● Network PoP　○ Federal Data Center

IBM Cloudのグローバル・データ・センター：https://www.ibm.com/cloud/data-centers/

アベイラビリティ・ゾーン（Availability Zone）とは:

共有する単一障害点を持たない3拠点以上のデータセンター(Zone)構成をアベイラビリティ・ゾーン（AZ）と言います。
クラウドのデータセンターをAZ化することで、障害に強いクラウドになります。
IBM Cloud は、2018年に東京リージョンを含む6つのリージョンをAZ対応しました。
また、2019年6月に大阪PoP（接続拠点）を開設しました。2020年には大阪DC（AZ）も開設予定です。
どのサービスがどのリージョンで利用できるかは、以下のサイトから最新情報を確認できます。

https://mycatalog.mybluemix.net/

【ゾーンの特徴】
・**物理的にそれぞれ隔離された**データセンターに構成される。
・データセンター、サーバールーム、PODなどの**物理的な境界を隠蔽**する。
・独立した電気系統、機器、ネットワーク機器で構成され、他のゾーンとは**共有しない**。
・各ゾーン間で共有された単一障害点は**存在しない**。
・**ゾーン間は1.2Tbpsの広帯域・低遅延**のネットワークで接続されている。

IBM Cloudでは、他社のネットワーク環境に比べて高いスループットが出ていることが第三者の調査で報告されています。安定した回線品質で効率よくデータセンター間のトランザクションが処理できる回線環境であることがわかります。

TCPベースのPing

SCPによる転送

Ping test (milliseconds)						
	US to UK	US to JP	UK to US	UK to JP	JP to US	JP to UK
IBM Cloud	73.9	136.7	73.9	210.9	136.7	210.8
AWS	77.8	154.7	71.9	214.7	147.5	214.3

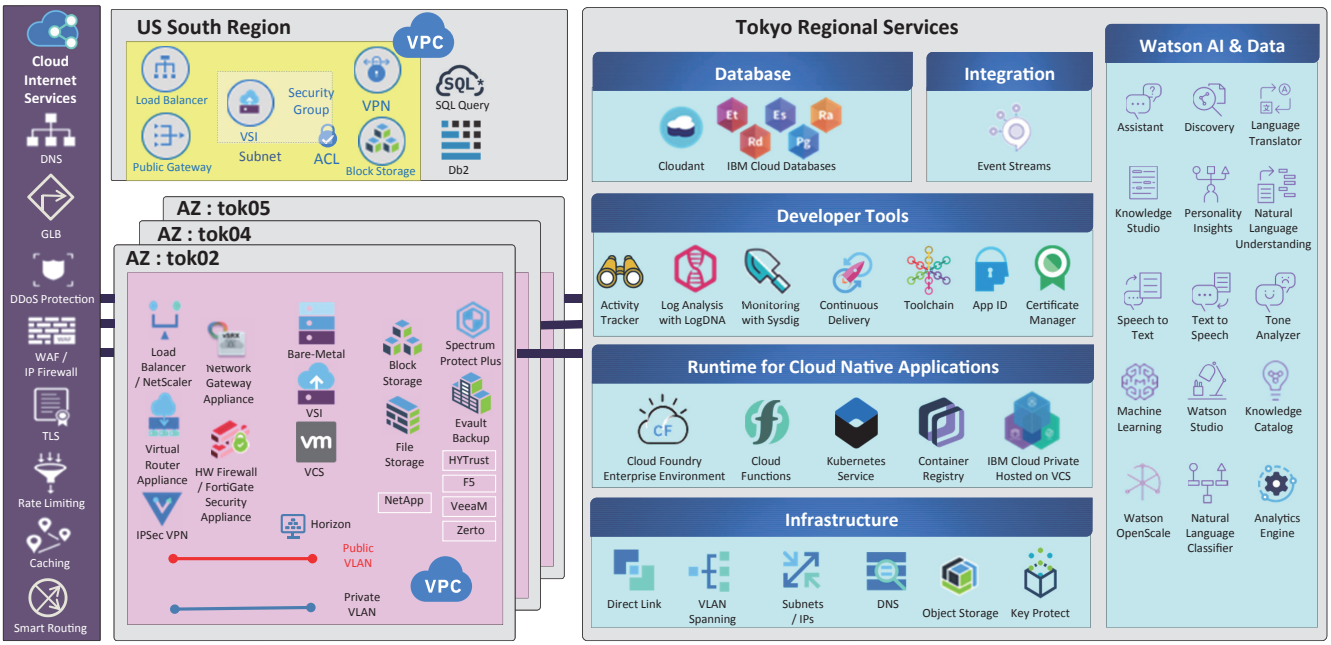
File and directory transfer (seconds)						
25MB file						
	US to UK	US to JP	UK to US	UK to JP	JP to US	JP to UK
IBM Cloud	2.5	4.1	2.5	6.2	4.1	6.1
AWS	5.8	11.4	6.1	16.7	11.3	17.4
500MB file						
	US to UK	US to JP	UK to US	UK to JP	JP to US	JP to UK
IBM Cloud	24.7	46.2	24.5	70.7	46.2	70.9
AWS	104.0	208.6	143.3	286.4	199.5	281.4
100MB directory						
	US to UK	US to JP	UK to US	UK to JP	JP to US	JP to UK
IBM Cloud	99.5	183.6	98.9	280.1	183.2	281.7
AWS	106.2	214.1	112.1	292.8	188.6	293

Faster big data analytics and better responsiveness with IBM Cloud (2017)
https://www.ibm.com/downloads/cas/OMN0KGWJ

SoftLayer時代、「Looking Glass」として下表のような、DC間のpingやTracerouteをとれる無償のツールが公開されていましたが、2018年でサービスが終了しました。
本ページは、IBM CloudのDC間のping値のご参照までに、当時の表をキャプチャして掲載しています。
最新の情報が必要な場合は、それぞれのDCにサーバーを立てて実測していただくとよいでしょう。

	ATL	CHI	DAL	DEN	HOU	LAX	MEX	MIA	MON	NYC	SEA	SJC	TOR	WDC	AMS	FRA	LON	MIL	PAR	CHE	HKG	MEL	SNG	SYD	TOK	SAO
ATL		31	20	34	28	54	44	13	27	18	61	61	33	13	92	98	85	107	109	233	207	200	239	192	160	124
CHI	29		24	25	28	48	48	40	19	22	43	52	11	19	94	104	89	108	96	212	174	201	194	193	126	136
DAL	20	21		15	9	33	25	30	38	41	40	36	31	31	109	122	108	129	112	245	182	178	214	167	133	143
DEN	34	25	15		22	34	39	43	44	46	27	28	36	42	116	125	114	132	118	220	174	183	205	171	126	154
HOU	28	25	9	22		36	30	25	45	45	46	43	37	38	114	125	117	141	121	255	190	188	220	176	141	139
LAX	54	53	32	34	33		48	60	69	69	25	8	65	64	142	158	145	165	141	218	155	149	186	137	109	187
MEX	44	45	25	39	30	53		54	63	66	65	56	56	56	134	145	131	153	137	264	203	198	234	186	151	168
MIA	13	41	30	43	24	60	54		39	32	73	65	46	25	104	111	97	119	120	247	215	210	242	194	176	111
MON	27	19	38	44	45	67	63	39		9	60	64	9	16	81	86	76	95	81	210	217	214	250	201	140	123
NYC	18	21	41	46	49	69	65	32	9		63	73	15	6	73	83	67	93	73	209	195	221	225	212	143	114
SEA	73	43	40	27	46	25	65	70	60	61		18	52	55	136	140	129	147	134	191	131	174	155	162	82	171
SJC	61	45	36	26	43	8	56	70	64	66	18		56	59	137	144	133	159	138	209	142	158	166	146	97	178
TOR	31	0	31	20	37	51	56	44	9	15	52	56		22	88	92	82	103	89	217	209	205	240	192	133	127
WDC	13	17	32	39	38	73	56	26	15	7	55	59	22		80	87	73	100	94	217	215	209	246	197	136	116
AMS	94	94	109	111	114	144	134	105	80	71	134	137	90	80		6	8	21	15	147	204	262	163	254	258	182
FRA	98	103	123	125	125	154	145	111	86	83	140	145	92	87	6		13	10	10	138	193	254	186	281	223	193
LON	85	88	108	114	117	145	131	97	76	67	129	133	82	73	8	13		28	8	126	199	242	159	263	211	183
MIL	111	119	130	137	141	160	154	124	95	93	147	157	102	100	26	10	28		17	147	214	280	184	262	251	205
PAR	108	94	113	118	120	141	137	120	81	73	134	138	88	92	17	10	8	17		151	182	235	151	246	230	186
CHE	233	224	245	226	254	218	264	245	220	201	193	209	219	216	144	146	136	167	140		66	116	33	127	105	311
HKG	224	170	182	174	190	155	202	212	217	193	131	144	208	215	206	195	199	221	182	66		114	34	114	47	328
MEL	200	200	178	183	187	149	198	210	213	220	174	158	205	209	264	270	242	274	235	116	115		84	13	125	321
SNG	265	206	214	201	220	184	234	246	250	246	155	166	240	246	160	186	162	184	151	33	34	85		96	76	359
SYD	192	193	167	171	175	137	186	194	200	210	162	146	192	197	268	279	259	262	246	127	114	12	96		113	309
TOK	160	124	129	126	139	109	151	173	140	143	82	98	133	136	253	223	211	254	228	105	50	125	79	113		276

2-3. IBM Cloud の提供サービス



IBM Cloud では、コンピュータ資源、データベースをはじめ、AI（Watson、DeepLearning）、Blockchain、IoT、DevOps、アナリティクス、Mobile連携、VMwareなど多岐に渡るサービスが提供されています。

https://mycatalog.mybluemix.net/generated/cheatsheet.pdf

Service Type
IBM Service
Third Party Service

Status
New Service (2018)
Service Refresh (2018)
(Plan Add)

AI
Watson Studio
Watson Assistant
Watson Discovery
Compare Comply
Watson Language Translator
Watson Nat. Language Classifier
Watson Personality Insights
Voice Agent with Watson
Garage and Watson Expert Services
Watson Speech to Text
Watson Text to Speech
Watson Nat. Language Understanding
Watson IoT Platform
Watson Machine Learning
AI OpenScale
Watson Knowledge Catalog
Power AI

Security
Activity Tracker
App ID
Network Security
SSL Certificates
Security Advisor
Certificate Manager
Hardware Security Module
Hyper Protect Services
Identity Access Mgmt.
Contrast Security
FusionAuth
Twilio Authy
Twilio Verify

Analytics
Analytics Engine
Apache Spark
Decision Optimization
Db2 Warehouse on Cloud
SQL Query
Master Data Mgmt. (MDM) on Cloud
Information Server on Cloud
Streaming Analytics
Account Score

Web & Mobile
Mobile Foundations
Mobile Analytics
Push Notifications
Accrete.AI Rational Exuberance
Accrete.AI Rumor Hound
Accrete.AI Topic Deltas
Twilio Programmable SMS
Twilio Programmable Video
Twilio Programmable Voice
Phunware Mobile Marketing Automation
Phuneware Location Based Services
Telstra API
Mapbox Maps

DevOps
Continuous Delivery
Continuous Release
Globalization Pipeline
Cloud CLI
Availability Monitoring
Cloud Developer Console for Apple
Cloud Automation Manager
Cloud Event Management
Workload Scheduler
DevOps Insights
Log Analysis
Monitoring
IBM Cloud Monitoring with Sysdig
Log Analysis with LogDNA
Pager Duty
Mendix Platform Services

VMware
Secure Virtualization
Veeam on IBM Cloud
VMware Horizon on IBM Cloud
Skytap on IBM Cloud
VMware vSphere
F5 on IBM Cloud
Fortigate on IBM Cloud
Spectrum Protect Plus on IBM Cloud
Zerto on IBM Cloud
VMware vCenter
VMware Cloud Foundation

Databases
Cloudant
IBM Cloud DBs
Db2 Hosted
Db2 on Cloud
Blockchain
Db2 Warehouse
Informix on Cloud
Lift
Mass Data Migration
Geo Web Services
Influx Cloud

Integration
API Connect
App Connect
Aspera on Cloud
Event Streams (Messaging Hub)
MQ on Cloud
Compose for Rabbit MQ
Direct Link
Secure Gateway
Rocket Mainframe Data
Splice Pre-Cat Insurance Notifications

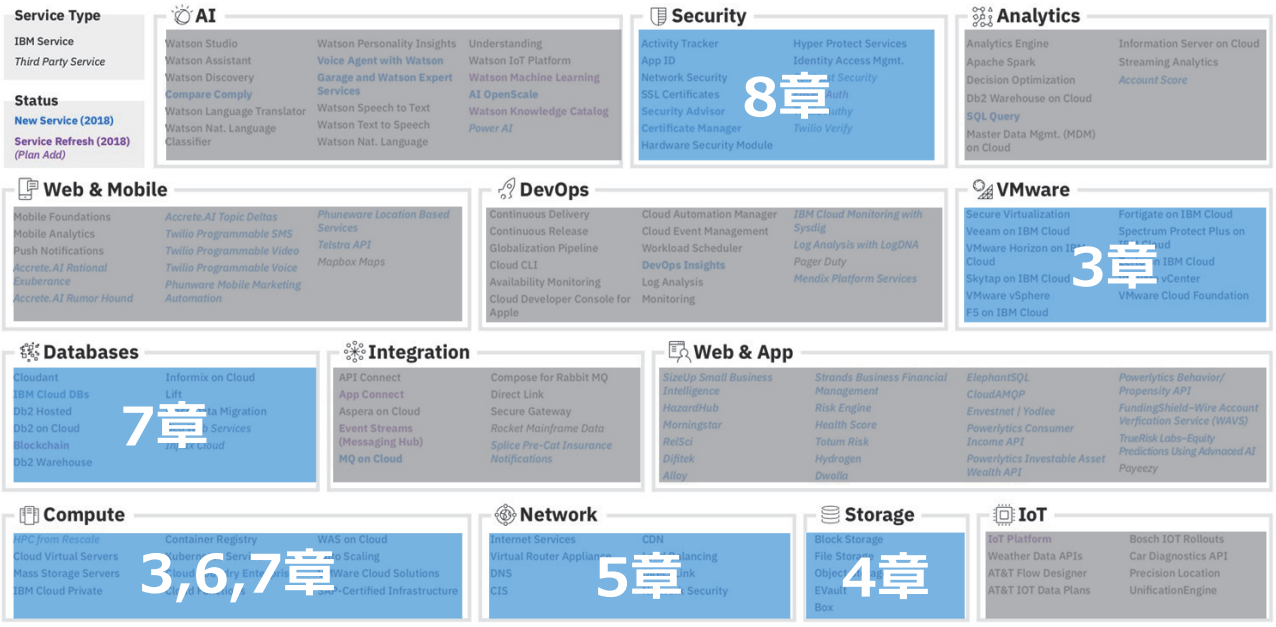
Web & App
SizeUp Small Business Intelligence
HazardHub
Morningstar
RelSci
Diffitek
Alloy
Strands Business Financial Management
Risk Engine
Health Score
Totum Risk
Hydrogen
Dwolla
ElephantSQL
CloudAMQP
Envestnet | Yodlee
Powerlytics Consumer Income API
Powerlytics Investable Asset Wealth API
Powerlytics Behavior/ Propensity API
FundingShield–Wire Account Verfication Service (WAVS)
TrueRisk Labs–Equity Predictions Using Advnaced AI
Payeezy

Compute
HPC from Rescale
Cloud Virtual Servers
Mass Storage Servers
IBM Cloud Private
Container Registry
Kubernetes Service
Cloud Foundry Enterprise
Cloud Functions
WAS on Cloud
Auto Scaling
VMWare Cloud Solutions
SAP-Certified Infrastructure

Network
Internet Services
Virtual Router Appliance
DNS
CIS
CDN
Load Balancing
Direct Link
Network Security

Storage
Block Storage
File Storage
Object Storage
EVault
Box

IoT
IoT Platform
Weather Data APIs
AT&T Flow Designer
AT&T IOT Data Plans
Bosch IOT Rollouts
Car Diagnostics API
Precision Location
UnificationEngine


Service Type
IBM Service
Third Party Service
Status
New Service (2018)
Service Refresh (2018)
(Plan Add)
AI
Watson Studio
Watson Assistant
Watson Discovery
Compare Comply
Watson Language Translator
Watson Nat. Language Classifier
Watson Personality Insights
Voice Agent with Watson
Garage and Watson Expert Services
Watson Speech to Text
Watson Text to Speech
Watson Nat. Language
Understanding
Watson IoT Platform
Watson Machine Learning
AI OpenScale
Watson Knowledge Catalog
Power AI
Security
Activity Tracker
App ID
Network Security
SSL Certificates
Security Advisor
Certificate Manager
Hardware Security Module
Hyper Protect Services
Identity Access Mgmt.
8章
Analytics
Analytics Engine
Apache Spark
Decision Optimization
Db2 Warehouse on Cloud
SQL Query
Master Data Mgmt. (MDM) on Cloud
Information Server on Cloud
Streaming Analytics
Account Score
Web & Mobile
Mobile Foundations
Mobile Analytics
Push Notifications
Accrete.AI Rational Exuberance
Accrete.AI Rumor Hound
Accrete.AI Topic Deltas
Twilio Programmable SMS
Twilio Programmable Video
Twilio Programmable Voice
Phunware Mobile Marketing Automation
Phuneware Location Based Services
Telstra API
Mapbox Maps
DevOps
Continuous Delivery
Continuous Release
Globalization Pipeline
Cloud CLI
Availability Monitoring
Cloud Developer Console for Apple
Cloud Automation Manager
Cloud Event Management
Workload Scheduler
DevOps Insights
Log Analysis
Monitoring
IBM Cloud Monitoring with Sysdig
Log Analysis with LogDNA
Pager Duty
Mendix Platform Services
VMware
Secure Virtualization
Veeam on IBM Cloud
VMware Horizon on IBM Cloud
Skytap on IBM Cloud
VMware vSphere
F5 on IBM Cloud
Fortigate on IBM Cloud
Spectrum Protect Plus on IBM Cloud
vCenter
VMware Cloud Foundation
3章
Databases
Cloudant
IBM Cloud DBs
Db2 Hosted
Db2 on Cloud
Blockchain
Db2 Warehouse
Informix on Cloud
7章
Integration
API Connect
App Connect
Aspera on Cloud
Event Streams (Messaging Hub)
MQ on Cloud
Compose for Rabbit MQ
Direct Link
Secure Gateway
Rocket Mainframe Data
Splice Pre-Cat Insurance Notifications
Web & App
SizeUp Small Business Intelligence
HazardHub
Morningstar
RelSci
Difitek
Alloy
Strands Business Financial Management
Risk Engine
Health Score
Totum Risk
Hydrogen
Dwolla
ElephantSQL
CloudAMQP
Envestnet | Yodlee
Powerlytics Consumer Income API
Powerlytics Investable Asset Wealth API
Powerlytics Behavior/ Propensity API
FundingShield–Wire Account Verfication Service (WAVS)
TrueRisk Labs–Equity Predictions Using Advnaced AI
Payeezy
Compute
HPC from Rescale
Cloud Virtual Servers
Mass Storage Servers
IBM Cloud Private
Container Registry
WAS on Cloud
3,6,7章
Network
Internet Services
Virtual Router Appliance
DNS
CIS
CDN
5章
Storage
Block Storage
File Storage
Object
EVault
Box
4章
IoT
IoT Platform
Weather Data APIs
AT&T Flow Designer
AT&T IOT Data Plans
Bosch IOT Rollouts
Car Diagnostics API
Precision Location
UnificationEngine

3

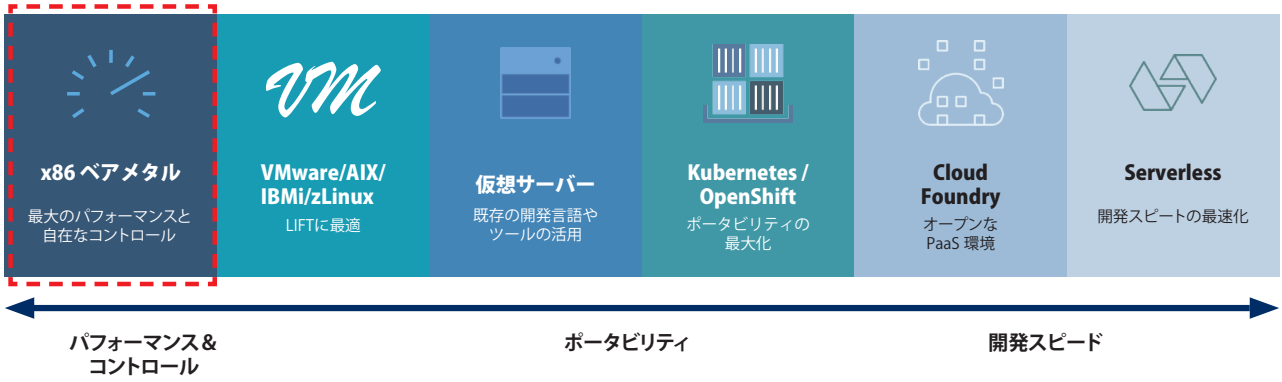
コンピューティング

INDEX

3-1. 物理サーバー

物理サーバー（ベアメタル）概要

IBM Cloud はパブリック・クラウドベンダーでトップクラスのベアメタルラインナップを誇るクラウドです。
データセキュリティの観点から他社と同居できない、パフォーマンスの観点からノイジーネイバーを避けたい、
VMware社やSAP社の認定構成が必要だ、といった様々なニーズにぴったりの構成をお選びいただけます。



IBM Cloud の特徴のひとつである物理サーバーは、CPU、メモリ、OS、内蔵Disk、GPU、ネットワークポートなどを
任意に構成することが可能です。VMwareなどのハイパーバイザー環境を利用することもできます。

https://cloud.ibm.com/docs/bare-metal

種　別	物理サーバー
種別（英語）	Bare Metal Server
共有・専有	専有（シングルテナント）
ハイパーバイザー	なし
CPUコア	1CPU（最小 4 コア）モデルから、8CPU（最大 192 コア）までの Intel CPU および Power Architecture
CPU世代(一部東京DCで利用不可)	Haswell(v3), Broadwell(v4), Skylake(v5), Kaby Lake(v6), Cascade Lake, OpenPOWER
メモリ	8 ～ 8192GB
ネットワークポート	100Mbps, 100Mbps x2, 1Gbps, 1Gbps x2, 10Gbps, 10Gbps x2 (x2 の場合、Redundant/Dual が選択可能)
ローカルDisk	最大 36 ドライブ（1 サーバーあたり） SATA: 1TB ～ 10TB、SAS: 600GB、SSD: 800GB ～ 3.8TB（※時間課金の場合、事前構成されたドライブから選択）
選択できる主要OS	CentOS、CloudLinux、Debian GNU/Linux、FreeBSD、Ubuntu Linux、Microsoft Windows Server、Citrix XenServer、Red Hat Enterprise Linux、VMware ESXi、QuontaStor、Ubuntu Linux on Power8、OS 無し (時間課金の場合は Red Hat Enterprise Linux や Hypervisor 等、一部の OS が利用不可)
課金タイプ	時間 / 月 /1 年 /3 年
デプロイ目安	15 分～最長 4 時間
備考	OS の管理者権限はお客様が持ちます。 部品の障害時には、障害箇所を特定後、2 時間以内に交換します。 時間課金に対応していない OS 等は、時間課金環境での利用はできません。 Intel Optane メモリ（3D XPoint を使った高速キャッシュ）、GPU、冗長化電源、冗長化 NW カードも指定できます。 メモリ、Disk の追加・削除も管理ポータルから操作できます。 月課金タイプの場合、1 サーバーあたり月 20TB(アメリカ、カナダ、ヨーロッパ) もしくは 5TB(それ以外の地域) のアウトバウンド無料枠が付与されます。(初月日割り) 月課金タイプの場合、初月の価格はその月の残りの日数に応じた日割り料金になります。 DB(MS SQL、MySQL、MongoDB、Riak) をオプションで指定できます。

柔軟な課金体系が選択可能な物理サーバー

https://cloud.ibm.com/docs/bare-metal?topic=bare-metal-about-bm

IBM Cloud の物理専有サーバーでは、1時間単位での利用から、1年間/3年間の長期契約まで、様々な利用形態があります。

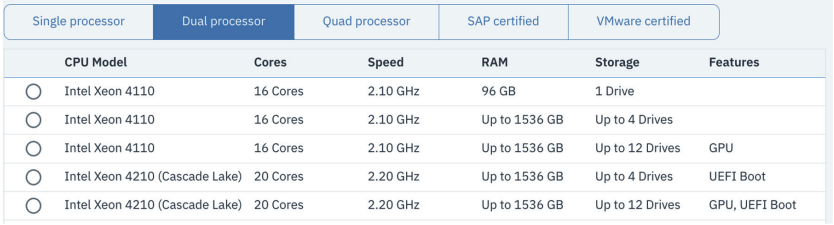
- **時間課金のベアメタルサーバー**
  - あらかじめ構成されているいくつかのプロファイルからサーバーを選択します。
  - デプロイ先のVLANを指定することはできません。
  - Red Hat Enterprise LinuxやHypervisor等、一部のOSを利用することができません。
  - GPUは利用できません。
- **月額課金のベアメタルサーバー**
  - 任意のプロセッサーを選択し、自由に構成を変更することが可能です。
  - 初月の価格はその月の残りの日数に応じた日割り料金になります。
- **リザーブド・ベアメタルサーバー**
  - あらかじめ構成されているいくつかのプロファイルからサーバーを選択します。
  - 1年契約と3年契約のいずれかを選択します。
  - 契約期間中は容量が保証されます。
  - 予約容量に含まれるのは、CPU、RAM、ディスクドライブ、RAIDです。
  - 毎月の支払いを定額にすることができ、時間課金、月額課金のベアメタルサーバーと比較してコストを削減することが可能です。
  - インスタンスの構成変更はできません。
  - 契約期間内での契約のキャンセルはできません。
  - 契約期間が終了すると、通常の月額課金のベアメタルサーバーとして課金が開始されます。

物理サーバーでもGPUの利用が可能

https://www.ibm.com/cloud/bare-metal-servers/gpu

Deep LearningやVDI用の環境として広く利用されているNVIDIA GPUを利用することができます。
IBM Cloud では、これらのGPUを1サーバーあたり最大2カード搭載してご利用いただけます。
サーバーによって利用できるGPUの種類に違いがあります。
※GPUを搭載したサーバーにはIntel Optane SSDを追加することはできません。
※時間課金のベアメタルサーバーでは利用することはできません。

GPU 種別	V100	P100	M60	K80
主用途	GPGPU (Deep Learning や HPC など)	GPGPU または VDI	GPGPU または VDI	GPGPU
GPU 仕様	GPU: 1 x Volta GV100 メモリー : 16 GB HBM2 CUDA コア : 5120 メモリー帯域幅 : 900 GB/s	GPU: 1 x Pascal GP100 メモリー : 16 GB HBM2 CUDA コア : 3584 メモリー帯域幅 : 720 GB/s	GPU: 2 x Maxwell GM204 メモリ : 2 x 8GB GDDR5 CUDA コア : 2 x 2048 メモリ帯域幅 : 2 x 160GB/s	GPU: 2 x Kepler GK210 メモリ : 2 x 12 GB GDDR5 CUDA コア : 2 x 2496 メモリ帯域幅 : 2 x 240GB/s

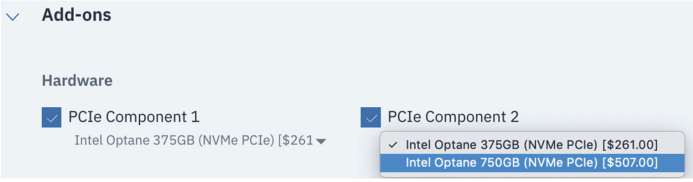


GPUを利用できるサーバーにはポータル上で「GPU」の記載があります。

Intel Optane の利用で高スループットを実現

https://cloud.ibm.com/docs/bare-metal?topic=bare-metal-ordering-ssd

いくつかのベアメタルサーバーではIntel Optane SSDを利用することができます。
Intel Optaneは、3D XPointを使用した記憶装置で、高スループット、低レイテンシー、高いQoSを兼ね備えたSSDです。
利用できるのは、DC P4800Xシリーズの375GBと750GBの2種類です。
詳しい製品の仕様については、下記公式Webサイトをご確認ください。
https://www.intel.co.jp/content/www/jp/ja/products/docs/memory-storage/solid-state-drives/data-center-ssds/optane-ssd-dc-p4800x-p4801x-brief.html



POWER8 の利用

https://www.ibm.com/cloud/bare-metal-servers/power

- IBM Cloud でPOWER8（Habanero）が月課金タイプとして利用できます。
- OSは、Ubuntu です。AIXやIBM iを使うことはできません。
- RHEL、SuSE はOSリロードを使って個別に導入することができます。
- デプロイ時間：最大30分
- 利用可能DC：ダラス
- 選択可能な構成：以下の4パターン

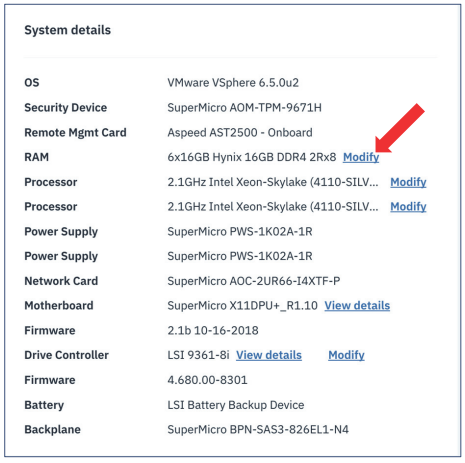
Profile	Cores	Speed	RAM	Storage
POWER8 C812L-S	8	3.86 GHz	64 GB	1 Drive
POWER8 C812L-M	10	3.49 GHz	256 GB	2 Drives
POWER8 C812L-L	10	3.49 GHz	512 GB	2 Drives
POWER8 C812L-SSD	10	3.49 GHz	512 GB	2 Drives

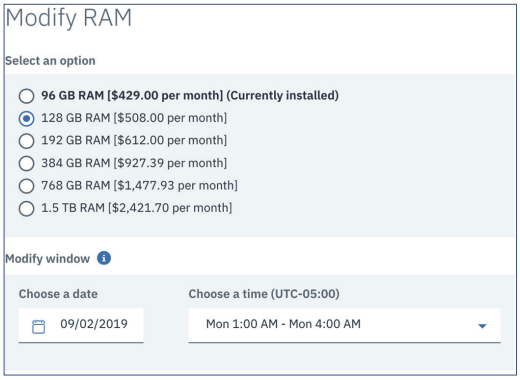
取扱注意 Handle with care

OpenPower環境はSLA（例：部品故障時に2時間以内に交換して再起動、などの）対象外です。

ベアメタルサーバーの構成変更

月額課金のベアメタルサーバーはRAMやプロセッサーなどの構成変更が可能です。
構成変更の際には、再起動の時間を指定します。
スケールアップ・ダウンの両方に対応しますが、CPUについてはソケット形状が同一のものに限り変更可能です。
現地での実作業はクラウド事業者がおこない、システム全体としての復旧はお客様にご確認していただく必要があります。



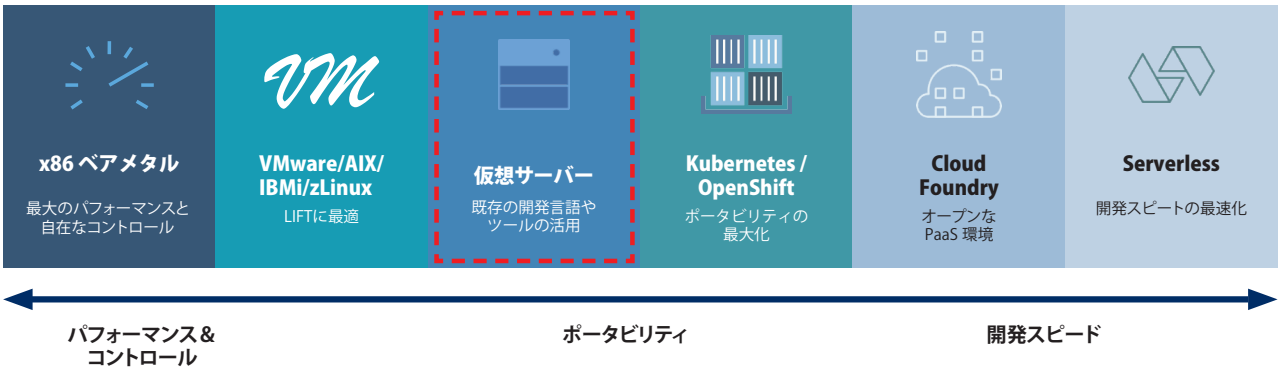


↑メンテナンス時間は、直近1ヶ月の中から3時間とっていただく必要があります。
（ハードウェア変更時はシステムの停止をともないます。）

3-2. 仮想サーバー

仮想サーバー概要

IBM Cloud の仮想サーバーは、XenServer環境で構築された仮想サーバーです。
vCPUやメモリ、内臓Diskなど、必要に応じてさまざまなサイズを指定して利用することができます。



IBM Cloud では**Virtual(仮想)**サーバーも利用できます。物理サーバーだけではなく、これらの異なる特性のリソースをひとつの管理画面で制御できるのが特徴です。(異なるデータセンターのリソースもひとつの画面で制御できます)

https://cloud.ibm.com/docs/vsi

Public Multi-tenant	**Dedicated** Single-tenant	**Transient** Multi-tenant Ephemeral	**Reserved** Multi-tenant Term commitment
• 迅速な立ち上げと拡張が可能なマルチテナントの仮想サーバー • あらかじめ構成された Profile の中から選択 • Suspend Billing や Placement Group を利用可能	• 迅速な立ち上げと拡張が可能なシングルテナントの仮想サーバー • 物理的に専有されたホスト上で稼働 • vCPU、RAM を選択肢の中から自由に構成可能	• 空きリソースを一時的に利用できるマルチテナントの仮想サーバー • 常時稼働が必要なワークロードでは利用不可 • 大幅な割引価格でご利用いただけます	• 1 年間もしくは 3 年間での長期契約が可能なマルチテナントの仮想サーバー • 契約期間中は予約したリソースの起動を保証 • 通常の従量課金方式と比較し、コスト削減が可能

仮想サーバーのリソースは、 下記のオプションの中から自由に選択して構成することができます。
ハイパーバイザーはXenServerを利用しており、お客様は管理の必要がありません。

オプション	Public	Dedicated	Transient	Reserved
課金タイプ	時間/月	時間/月	時間	時間/月
CPU/メモリ	Profileから選択 (GPUにも対応)	Core: 1 - 56 vCPU RAM: 1 -242 GB 任意の組み合わせを選択可能	Profileから選択 (Local, GPUは選択不可)	Profileから選択 (Local, GPUは選択不可)
ハイパーバイザー	XenServer			
ネットワークポート	10Mbps, 100Mbps, 1Gbps			
ストレージ	SAN: 25 GB - 8.1 TB （Windows OSの場合は100 GB - 8.1 TB）。 Local: 100 GB – 900 GB (プロファイルごとに選択できるストレージの容量は異なります。) 一般的にはSANを指定。パフォーマンス優先の場合はLocalを指定。			
選択できる主要OS	CentOS、Debian GNU/Linux、Red Hat Enterprise Linux、Microsoft Windows Server、Ubuntu Linux			
デプロイ目安	5 - 15分			
備考	OSの管理者権限はお客様が持ちます。 時間課金に対応していないOS・アドオン等は、時間課金環境での利用はできません。 CPU、メモリ、Diskの追加・削除も管理ポータルから操作できます。 仮想サーバーは、オートスケール機能に対応しています。 月課金タイプの場合、1サーバーあたり月250GBのアウトバウンド無料枠が付与されます。(初月日割り) 月課金タイプの場合、初月の価格はその月の残りの日数に応じた日割り料金になります。 DB(MS SQL、MySQL、MongoDB、Riak)をオプションで指定できます。			

Public Virtual Server

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-about-public-virtual-servers

マルチテナントの仮想サーバーです。あらゆるビジネス要件を満たすProfileが用意されており、迅速に展開が可能です。
サーバーをプロビジョンした後もコア数やメモリーの変更が可能です。
Public Virtual Serverでは下記の5種類のFamilyからProfileを選択します。

Family	特徴、選択時の注意点
Balanced	• パフォーマンスとスケール性能のバランス型。一般的なトラフィックのWebサーバーや大小様々なデータベースに適しています。 • SANストレージが利用可能です。 • サポートされている全てのOS、データベース、アドオンが利用可能です。
Balanced Local Storage	• ローカスストレージを利用することで、大規模なDBクラスターなど、高IOPS・低遅延が求められるワークロードに適しています。 • HDDとSSDのオプションがあり、**データセンターによって利用できるオプションが異なります**。 • プロファイルによって選択できるストレージの最大容量が変化します。 • サポートされている全てのOS、データベース、アドオンが利用可能です。
Compute	• CPU負荷が高いワークロード、フロント・エンドやバッチ処理を行う用途に適しています。 • SANストレージが利用可能です。 • サポートされている全てのOS、データベース、アドオンが利用可能です。
Memory	• インメモリのアナリティクスなど大きなキャッシュ・メモリが重要となる用途に適しています。 • SANストレージが利用可能です。 • サポートされている全てのOS、データベース、アドオンが利用可能です。
GPU	• NVIDIA Tesla P100/V100 GPUを利用したAIおよびDeep Learningなどのワークロードに適しています。 • AC1, AC2, ACL1, ACL2の4種類のオプションが存在し、**データセンターによって利用できるオプションが異なります**。 • GPUとして、AC1とACL1ではP100、AC2とACL2ではV100が利用可能です。 • ストレージとして、AC1とAC2ではSANストレージ、AC1ACL1とACL2ではローカルストレージ(SSD)が利用可能です。 • **HVM boot modeをサポートしているOSでのみ利用可能**です。 • サーバーをプロビジョンした後でもGPUの数を変更することが可能です。 • 最新の情報はDocsをご確認ください。(https://cloud.ibm.com/docs/vsi?topic=virtual-servers-gpu#gpu)

Dedicated Virtual Server

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-dedicated-virtual-servers

シングルテナントで利用できる仮想サーバーのオファリングです。
Dedicated Virtual Serverには下記の2種類の注文方法があります。
1.「Dedicated Host」を注文し、注文したホスト上のリソースを利用してDedicated Instanceを展開する。
2.「Auto Assign」を選択し、ホストを意識せずDedicated Instanceのみを展開する。

どちらのオプションを選択するかによって、利用できる機能や課金の方式に違いがあります。
利用したいユースケースに合わせて選択すると良いでしょう。

機能	Dedicated Host上に展開	Dedicated Instanceのみ展開(Auto Assign)
シングルテナント	○	○
アフィニティールール	○	
アンチアフィニティールール	○	
リソース管理	○	
課金対象	Dedicated Hostのみ	Dedicated Instanceのみ
仮想サーバーのマイグレーション	○	
容量の保証	○	

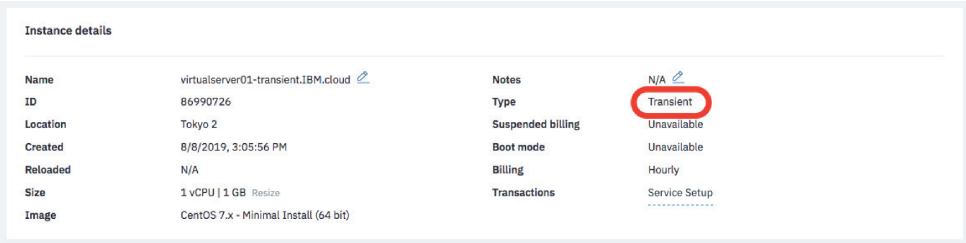
- アフィニティールール: 仮想サーバーを特定のホスト上でのみ稼働できるようにルールを作成することができます。
- アンチアフィニティールール: 複数の仮想サーバーが異なるホストにまたがって配置されるようにルールを作成することができます。
- リソース管理: 各Dedicated Hostのリソース(CPU, RAM, ローカルストレージ)の使用容量を表示します。
- 仮想サーバーのマイグレーション: 管理しているDedicated Host間で仮想サーバーを移行し、任意のホスト上に配置し直すことができます。
- 容量の保証: Dedicated Hostが配置されているPODの容量が上限に達した場合でもすでにオーダーしたホストの容量分はインスタンスを割り当てることができます。

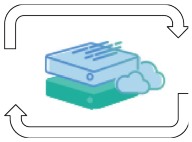
Transient Virtual Server

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-about-vs-transient

以下を念頭におき、非本番環境（例えば開発・テストやバッチなど）に使用することをお勧めします。

- 空きリソースを一時的に活用することで非常に低コストで利用できるマルチテナントの仮想サーバーです。
- **標準のPublic Virtual Serverに対して75 %オフの価格で利用できます。**
  （需給バランスによってリアルタイムに価格が変動するのではなく、固定で75% OFFです。）
- データセンター内で使用されていないリソースに対してデプロイされるため、これらのリソースが他のお客様によって必要になると、通知なく任意のタイミングでキャンセルされる可能性があります。
- 2019年6月現在、**すべてのデータセンターで利用可能**です。
- 「Balanced」「Compute」「Memory」ファミリーが利用できます。「GPU」「Balanced Local Storage」は利用できません。
- CPU、メモリなどの変更機能はありません。リソース変更が必要になる際には再注文となります。





Reserved Virtual Server

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-about-reserved-virtual-servers

1年間もしくは3年間での長期契約の代わりに、大幅値引き価格で利用可能なマルチテナントの仮想サーバーです。

注文方法

契約期間中は一度注文した**Reserved Capacityが保持され、容量が保証されます。**
毎月の支払いを定額にすることができ、通常のPublic Virtual Serverと比べてコストを削減することができます。
「Balanced」「Compute」「Memory」ファミリーが利用できます。「GPU」「Balanced Local Storage」は利用不可。
Reserved Instanceは構成をアップグレード、ダウングレードすることはできません。
Reserved Instanceは、Reserved Capacityの**契約期間が終了すると通常料金で課金が開始されます。**
https://cloud.ibm.com/docs/vsi?topic=virtual-servers-faqs-reserved-capacity-and-instances&locale=en

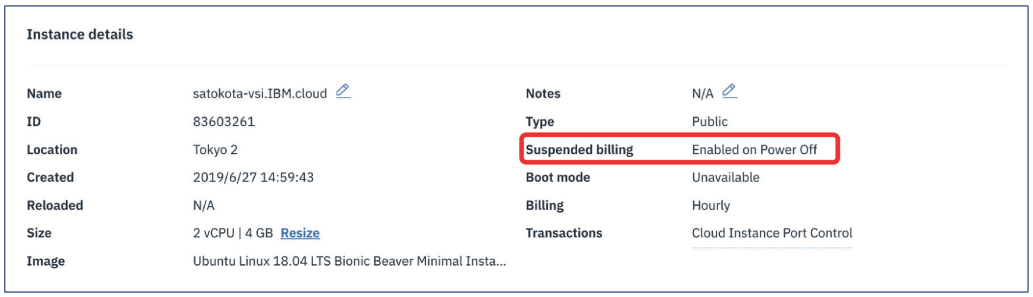
3-3. よく利用される関連サービス

Suspend Billing

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-requirements

この機能がサポートされている仮想サーバーの電源を切るとコンピュートリソースの請求が自動的に停止します。
待機サーバーのコスト削減をすることができ、サーバーが再度必要になったときに再プロビジョンする必要がなくなります。
※請求を停止させるには、IBM Cloudポータル、CLI、APIのどれかを用いて電源をオフにする必要があります。

Suspend Billing機能を利用するには、下記の条件を全て満たすサーバーをオーダーする必要があります。
① 時間課金のPublic Virtual Server
② SANストレージ
③「Balanced」「Compute」「Memory」ファミリー

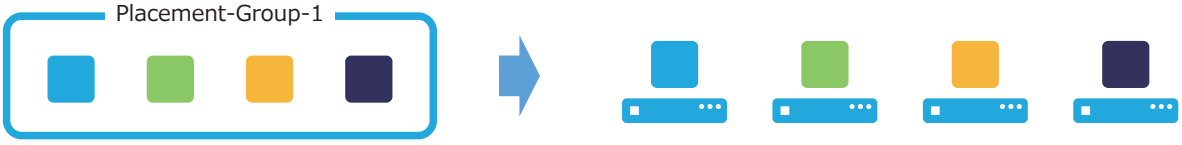


すでにデプロイされているサーバーがSuspend Billingをサポートしているかどうかは、下記の手順で確認することができます。
1.ポータルにログインし、メニューから「Resource List」を選択します。
2.「Devices」のなかから、確認したい仮想サーバーの名前をクリックします。
3.「Instance Details」の「Suspend Billing」欄を確認してください。

Placement Group

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-placement-groups

この機能を利用することで、仮想サーバーが配置されるホストを制御することができます。
サービスの可用性向上のためにHA構成で仮想サーバーを複数台デプロイする場合など、ある仮想サーバーのグループをそれぞれ異なる物理サーバーに配置したい時に利用することが考えられます。
同じグループに登録した仮想サーバー同士が別々のホストに分散して配置されます。
1つのグループには最大5台まで仮想マシンを登録することができます。
グループの数に制限はありません。
この機能は**無料**で利用することができます。
「Public Virtual Server」と「Transient Virtual Server」でのみ利用することができます。

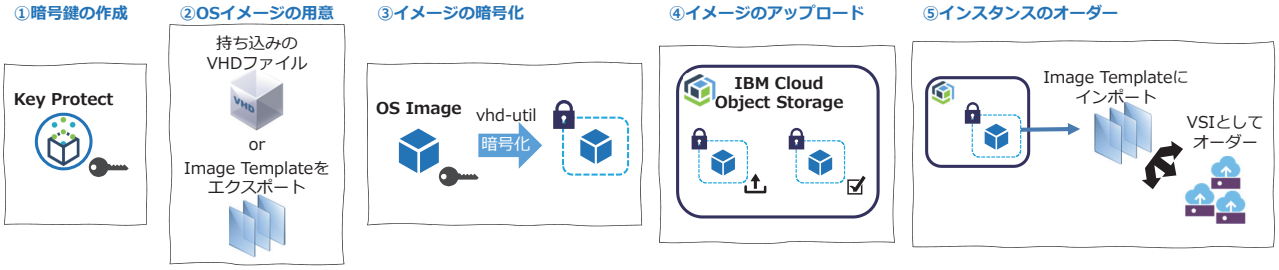


取扱注意
Handle with care

- 既存のインスタンスを作成したPlacement Groupに追加することはできません。
- 仮想サーバーをPlacement Groupに追加することができるのはプロビジョニング時のみです。
- Placement Groupからサーバーの登録を解除するには**サーバー自体をキャンセルする必要があります。**
- Placement Groupを削除するにはそのPlacement Groupに割り当てられたサーバーを全てキャンセルする必要があります。

暗号化されたVSIイメージの利用

IBM Cloudでは、自分が管理する暗号鍵で暗号化したOSイメージを持ち込んで仮想サーバーをデプロイすることが可能です。
OSイメージは持ち込みのVHDファイルを利用するか、Image Templateをエクスポートして利用します。
OSイメージはcloud-initが有効化され、適切に構成されている必要があります。
IBM Cloudでサポートされているでのみこの機能を利用することができます。
鍵管理にはKey ProtectもしくはHyper Protect Crypto Servicesを利用します。
暗号鍵は新しく作成することも、既存のキーを持ち込む(BYOK)ことも可能です。
イメージの暗号化にはvhd-utilツールを利用する必要があります。
IBM Cloud Object StorageからImage Templateにインポートする際にはIAMでサービスIDを作成する必要があります。
持ち込んだOSイメージは、イメージテンプレートとしてインポートし、仮想サーバーとしてデプロイすることができます。



https://cloud.ibm.com/docs/infrastructure/image-templates?topic=image-templates-using-end-to-end-e2e-encryption-to-provision-an-encrypted-instance&locale=en

オート・スケール（Auto Scale）

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-about-auto-scale

サーバーのCPU使用率やネットワーク使用状況に応じ、サーバー台数を動的に増減するオート・スケール機能です。
サーバー増減の条件には、特定の時刻（平日/休日/業務時間内/業務時間外など）を指定する事ができます。

パフォーマンス

- リソース不足を予測して自動的にプロビジョニング
- CPUや帯域幅の監視結果に基づいたスケーリングを設定可能
- Auto Scaleで構築されたリソースは標準のリソースと同じ性能で動作

柔軟性

- 利用者が設定した複数のポリシー・トリガーに対応可能
- ビジネスニーズや要件に基づいて、いつでもAuto Scaleグループの編集が可能

ロール

- グループ・トリガー・ポリシー・クールダウンを含む、Auto Scaleサービス内のすべての機能を利用者がコントロール可能
- 管理ポータルまたはAPIから、Auto Scale グループ・ポリシー・トリガーを管理可能
- チケット・電話・チャットでサポートを利用可能

物理サーバー、仮想サーバーで利用できるその他の機能

IPMIコンソール（物理サーバー）、KVMコンソール（仮想サーバー）

- VPNを通して、ブラウザー経由でデバイスに接続できるようにするJava アプレット
- クラウドにあるサーバーの管理ポート経由で接続できる
- 利用には、Private VLANに接続している端末と、KVM接続ができるユーザー権限が必要

推奨情報 Osusume-desu

コンソールアクセスはいざというとき非常に便利です。
事前に、問題なく接続ができることを確認しておきましょう。

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-faqs-servers-general-#kvm-

保険

- Business Continuance Insurance
  - サーバー単位でオーダー可能な有償オプション。
  - DDoSなどのネットワークを経由した攻撃の被害に遭い、膨大なアウトバウンドが発生した際にアウトバウンド料金の支払いに対応します。（※サーバーやアカウントを乗っ取られた場合は対象外）
- 月課金型のサーバー用のオプションです。

物理サーバー、仮想サーバーで利用できるその他の機能

・プロビジョニングオプション

OSリロード

- 任意のタイミングで、任意のOSイメージを再導入するためのオプションです。
- 無料で利用可能です。
- ロードしたイメージが有償OSの場合、そのOSの利用料金が発生します。
- 公開イメージだけではなく、自分で作成したOSイメージを使ったOSリロードもできます。

https://cloud.ibm.com/docs/infrastructure/software?topic=software-reloading-the-os&locale=ja

プロビジョニング・スクリプト

- 仮想サーバーや物理サーバーのプロビジョニング直後に、自動実行されるスクリプトの指定が可能です。
- 利用には、httpサーバー（スクリプトがダウンロードされるだけ）か、httpsで参照できるサーバー（スクリプトが実行される）上にスクリプトを設置しておく必要があります。

https://cloud.ibm.com/docs/vsi?topic=virtual-servers-provisioning-scripts

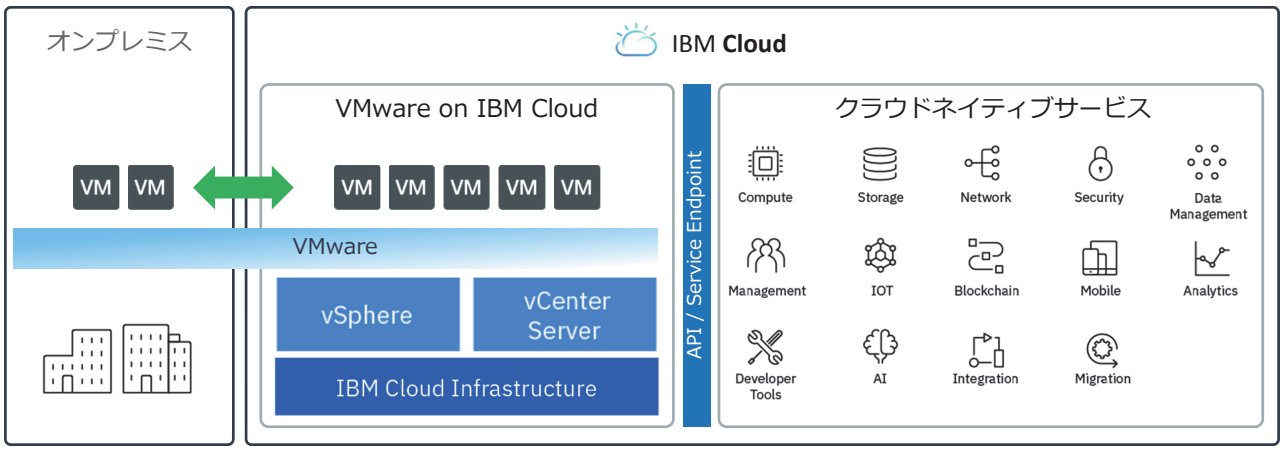
取扱注意
Handle with care

OSリロードは起動ディスク(1st Disk)のすべてのデータが消去されます。
※2nd Disk 以降のデータは、OSリロードによって消去せずに引き継ぐことが可能です。

3-4. VMware on IBM Cloud

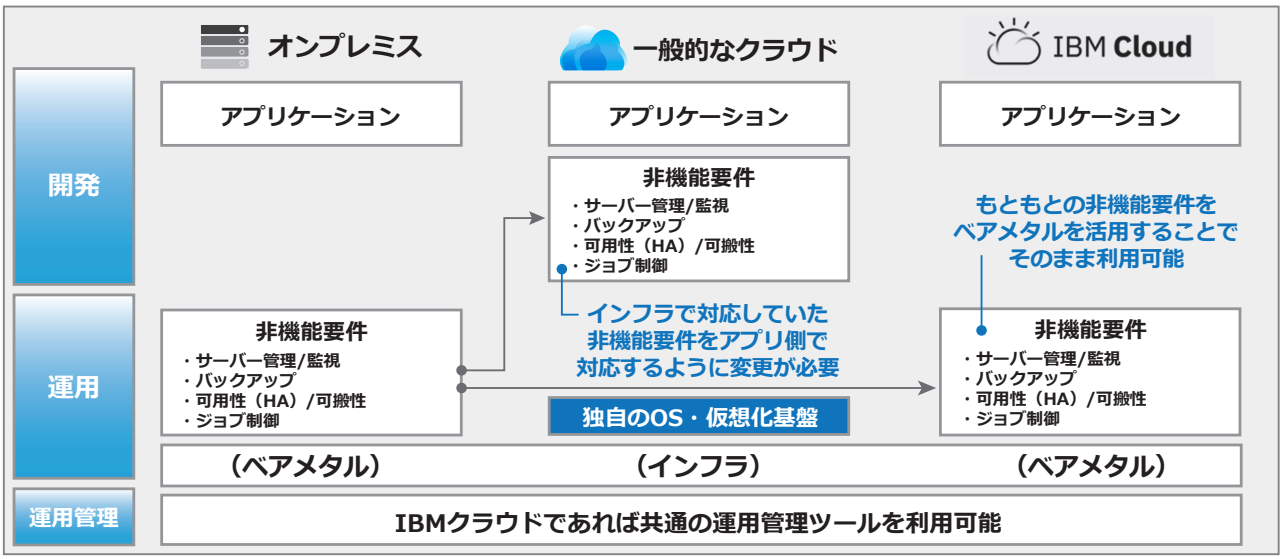
VMware on IBM Cloud とは

IBM Cloud 上で既存VMware ワークロードを活用することができるサービスの総称です。
既存のリソースを活かしつつ、クラウドのメリットを享受することが可能です。
IBM Cloud への高帯域幅、低遅延アクセスを実現し、150 以上のサービスと連携することができます。



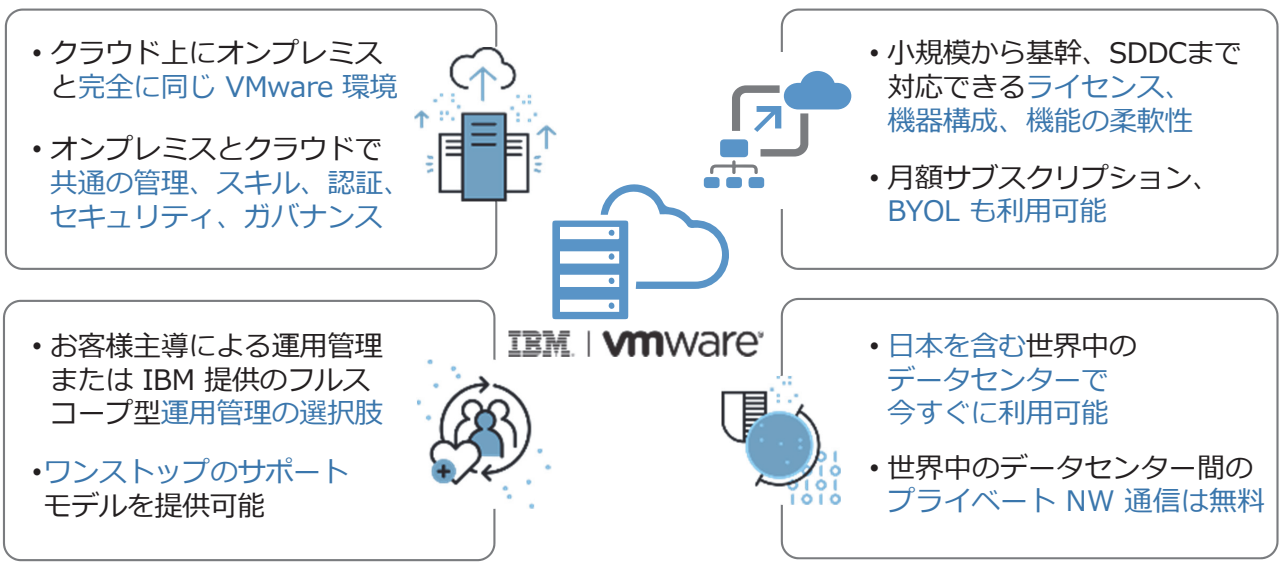
ベアメタルの提供価値：VMware 環境をLiftする

ベアメタルがあるからこそ、オンプレのVMware 環境を変更することなくクラウドへの移行できます。
オンプレで実装されている非機能要件の移行に加え、既存のVMware スキルの活用も可能です。



VMware on IBM Cloud の特長

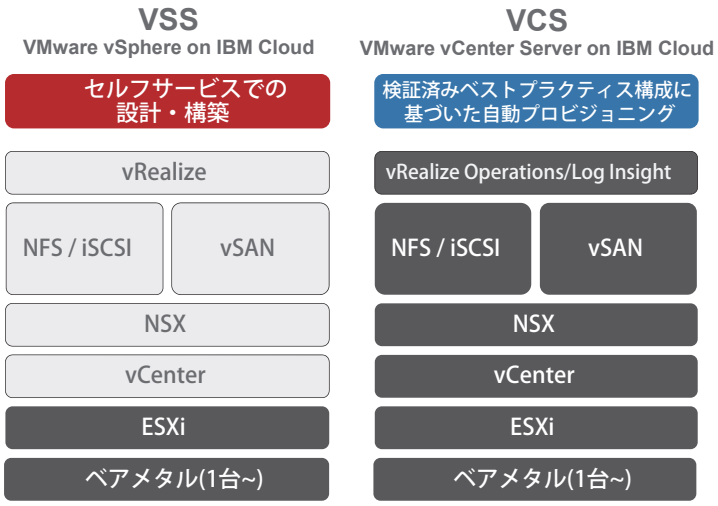
既存のツールや専門知識をそのまま活用し、クラウド上でのVMware利用の価値を最大化



柔軟性の高い構成が選択できます

スペックを柔軟に選択でき、小規模から本番まで要件に応じた適切な構成が選択可能です。
VMware ライセンスは月額サブスクリプション、BYOL で利用可能です。

セルフサービスのオプション
自動プロビジョニング



豊富な VMware 構成オプション

- お客様の要件に応じた適切な構成が選択可能。
- 検証にも利用できる小規模な環境から ミッションクリティカルな大規模環境まで
- SAPも認定済み

IBMによる高度な自動化 (VCS)

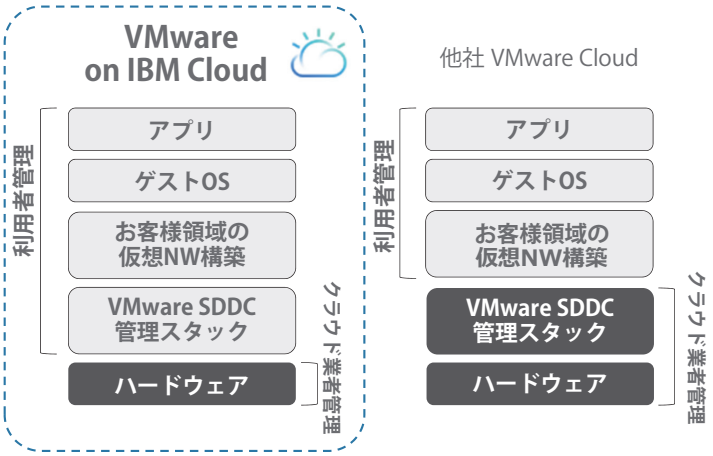
- 高度な自動化（数クリックの注文）により 数日かかっていた構築を数時間に短縮
- ハードウェア等の細かい互換性を気にせず 使えるVMware Certified 構成

VMwareライセンス持ち込みが可能

- ライセンスの持ち込み、 または月額課金でも利用可能

既存の非機能要件を満たすHosted Private Cloud

お客様が管理できるレイヤーが多く、クラウドでありながら最大限の自由度を確保することが可能です。
vCenter Server やNSX Manager などにログインし、自由に構成を変更することが可能なため、
設計・運用・監視・バックアップといったシステム管理を従来の方式で行うことができます。



お客様による基盤の運用管理が可能

- お客様の計画に合わせて メンテナンス時間をコントロールできます。
- 作業調整や障害発生時の対応など 現行運用形態をIBM Cloud上で継続できます。

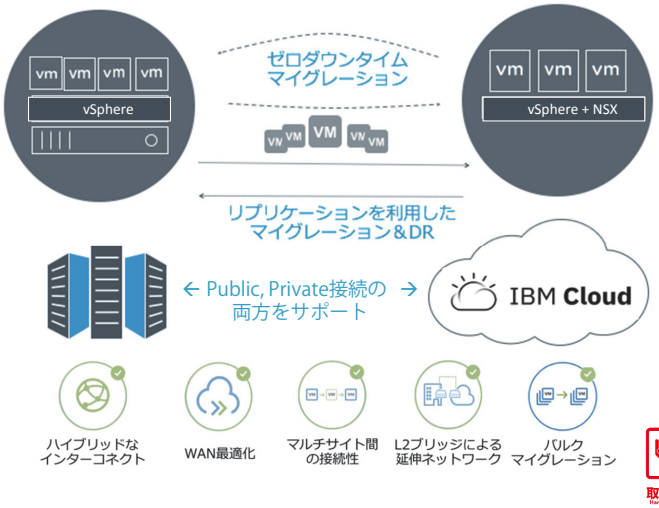
管理者権限による制御

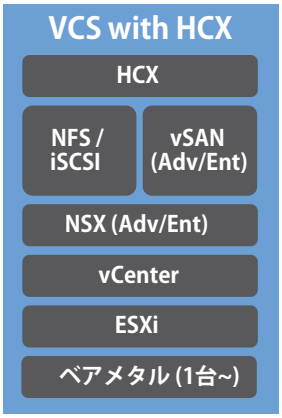
- お客様はHWおよびSW（vCenterを含む） すべての管理者権限を保有します。
- そのため、vSphere HA, DRS, vMotion 等、 全ての機能を今まで通りに制御可能です。
- 現在ご利用中のサードパーティ製品も もちろん継続利用可能です。

クラウド移行を強力に支援する Hybrid Cloud Extension (HCX)

オンプレミスからネットワークを延伸し、ハイブリッド・クラウドに取り組む企業が直面する障壁を取り除きます。

- vSphere 5.0 以降に対応し、VMware バージョンの**アップグレードなし**でVMware-to-VMware の移行が可能です。
- パブリックNWを前提とした複数サイト間の**セキュアなL2延伸ネットワーク**、WAN最適化された接続を提供します。
- 業務に影響を最小限に留める**ゼロダウンタイムのライブマイグレーション**の移行機能を提供します。





VCS with HCX 詳細

- HCX 以外の VMware ライセンスは持込可
- ストレージはvSAN または共有ストレージを選択可能
- NSX の Adv/Ent エディションが必要
- HCX ライセンスは、CPUソケットあたりの月額課金
- 1 HCX ライセンスで 3 サイト同時接続可

取扱注意

HCX の購入には、12か月間のコミットメントが必要なため、月額課金であるものの、12か月分の費用が確定する点にご注意ください。

パートナーソリューションをワンストップで提供

- 自社運用、またはIMI（IBM Integrated Managed Infrastructure）による運用が選択可能です。
- IBM Cloud コンソールからVMware パートナーソリューションをワンストップで提供します。
- 幅広いバージョンや要件に対応し、VMware システムの安定稼働を支援します。

運用

- **お客様主導による運用** - 管理者権限による運用が可能
- **マネージドサービス from IMI** - 遠隔地からの監視、管理サービス
- **マネージドサービス for Veeam, Zerto** - IBM レジリエンシーによるフルマネージドサービス

アドオンソリューション

ビジネス継続性

- **Veeam Backup & Replication** - 高いデータ保全性を誇るバックアップと高速なリカバリを提供
- **Zerto Virtual Replication** - サイト間で仮想マシンを災害対策や移行用途でレプリケーション
- **IBM Spectrum Protect Plus** - サイト間で仮想マシンを災害対策や移行用途でレプリケーション
- **vRealize** - サイト間で仮想マシンを災害対策や移行用途でレプリケーション

ストレージ

- **NetApp ONTAP Select** - 専有かつ高可用性を提供する仮想化されたストレージクラスタ

セキュリティ

- **KMIP** - 暗号鍵のライフサイクル管理
- **F5 BIG-IP VE** - パフォーマンスを最適化し、アプリ継続性とセキュリティ確保
- **HYTRUST Secure Virtualization** - VMwareのワークロードを保護し、コンプライアンス遵守の負荷を軽減
- **FortiGate Appliance** - ネットワーク境界を堅牢なアプライアンスで保護
- **Caveonix RiskForesight** - リスクの検出、予測、対処のためのプラットフォーム

移行

- **VMware HCX (Hybrid Cloud Extension)** - オンプレミスからネットワークを延伸し、変更なくワークロードを移行
- **Single-node Trial** for Migration and App Modernization for Data Protection and Disaster Recovery

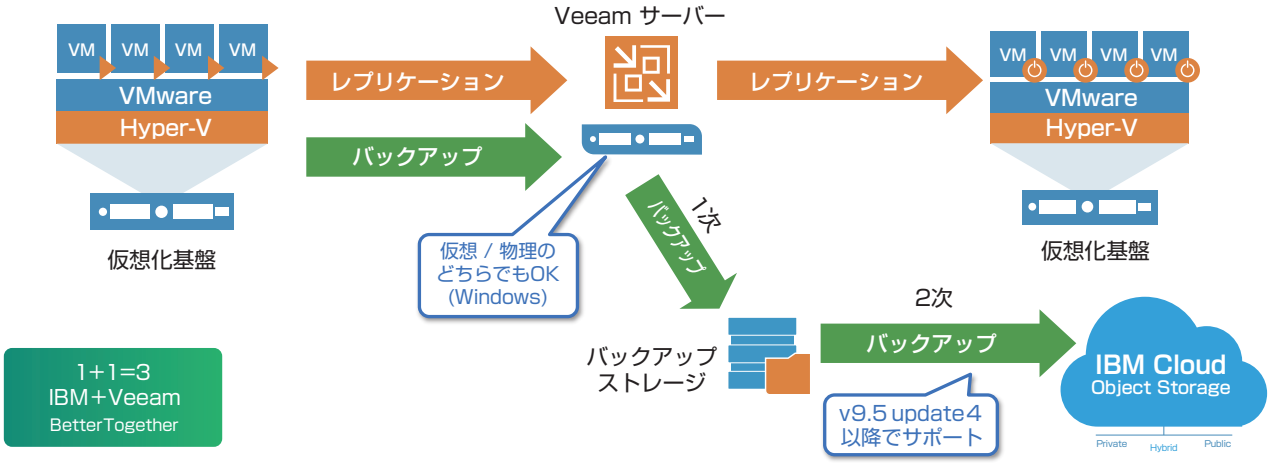
インフラ

- **VMware vSphere**
- **VMware vCenter Server**

Veeam on IBM Cloud

VMware vSphere とMicrosoft Hyper-V 環境のサポートと管理を提供し、クラウド環境での高可用性の実現を支援します。

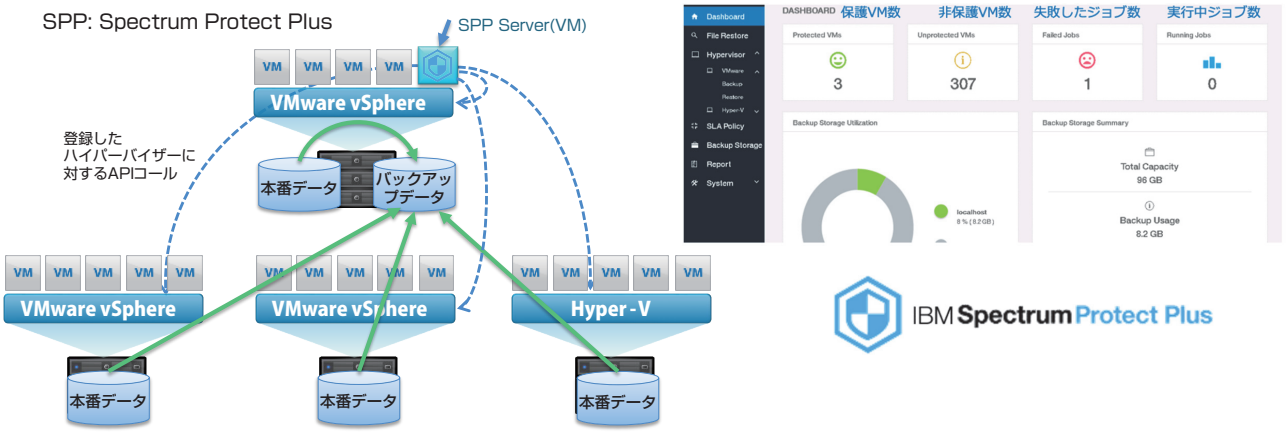
- Veeam on IBM Cloud 1つで、バックアップとレプリケーションの2種類の方法でデータ保護が行えます。
- 仮想化環境に特化したエージェントレスの仕組みにより、システムへの影響を最小限にします。
- ESXi 4.1 以降に対応し、仮想環境の規模に合わせて柔軟な構成が可能です。
- Veeam サーバーに加えて、バックアップ用外部ストレージが接続済みの状態で提供されます。



IBM Spectrum Protect Plus

仮想マシン向けに設計されたデータ保護ソフトSpectrum Protect Plus は簡単に設定・使用開始できます。

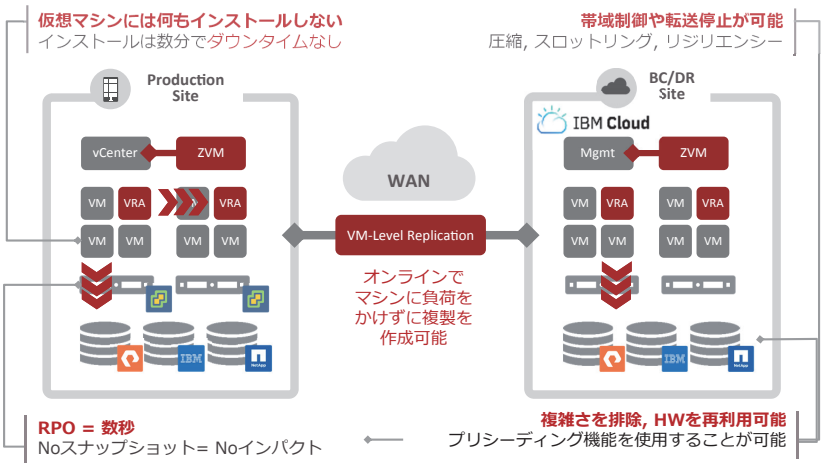
- 仮想アプライアンスで提供され、エージェントレスでVMware, Hyper-V上の仮想マシンをバックアップします。
- 永久増分バックアップ・重複排除・圧縮の機能により、データ量を削減します。
- バックアップ状況やストレージ使用率の確認、仮想マシンやファイルの高速検索をダッシュボードで一括管理します。
- Oracle DB, MS SQL Server をサポートし、データベースからアイテムレベルのリストアが可能です。
- バージョン10.1.3 以降で、IBM Cloud Object Storage へのオフロード機能をサポートします。
  http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_ca/9/897/ENUS219-029/index.html&lang=en&request_locale=en



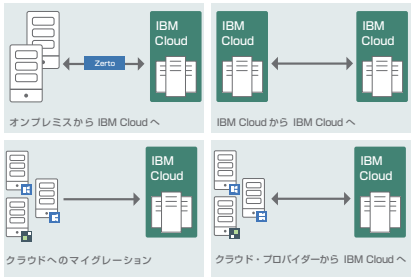
Zerto on IBM Cloud

パブリック、プライベート、ハイブリッドの各クラウドにエンタープライズ・レベルの災害復旧と事業継続性を提供します。

- VMware ESXi 4.0 Update1 以降であれば、異なるバージョン間でレプリケーションが可能です。
- 1時間から30日間の変更情報を持つことで、数秒単位でどの時間帯にも戻すことが可能です。
- クラウドへの災害対策や移行用途にZerto on IBM Cloud を従量課金モデルで提供します。



災害復旧シナリオ



ZVM：Zerto Virtual Manager
Windowsマシンにインストールされるzertoの管理ソフト

VRA：Virtual Replication Appliance
ZVMからデプロイされるLinuxの仮想アプライアンス

取扱注意
Handle with care

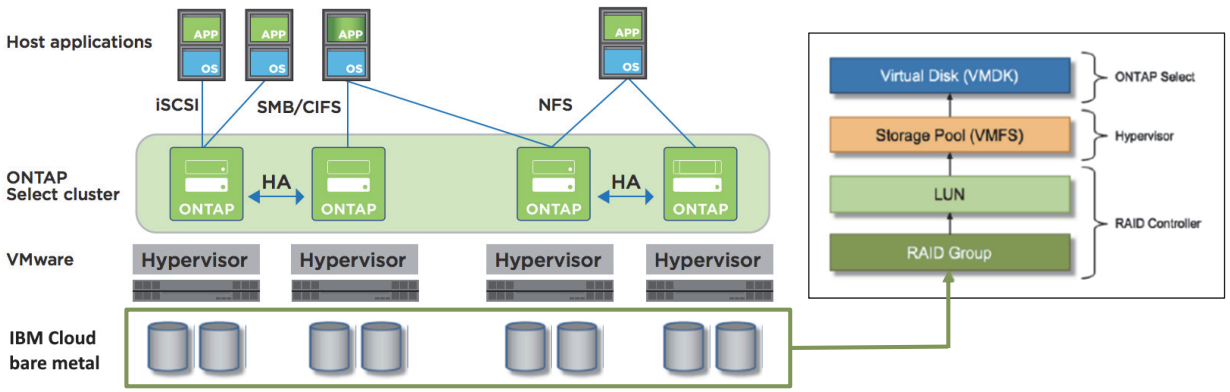
従量課金のため、すべてのサイトの ZVM は zerto.com:443 へのインターネットアクセスが必要、などの通信要件があります。
https://www.zerto.com/myzerto/knowledge-base/zerto-reporting-for-enterprise-environments-call-home/

NetApp ONTAP Select on IBM Cloud

企業向けONTAP ストレージOS を使って、クラウド上でも専有かつ高可用なストレージクラスタを作成することが可能です。

- 重複排除、暗号化、SnapMirror などの機能を使って、ストレージの効率的な運用が継続可能です。
- 利用者は既存環境と同じ運用を、IBM Cloud の世界中のデータセンターで実現可能です。
- 標準化されたハードウェア互換性のあるコンポーネントを使って、高可用性構成を提供します。

システム構成概要



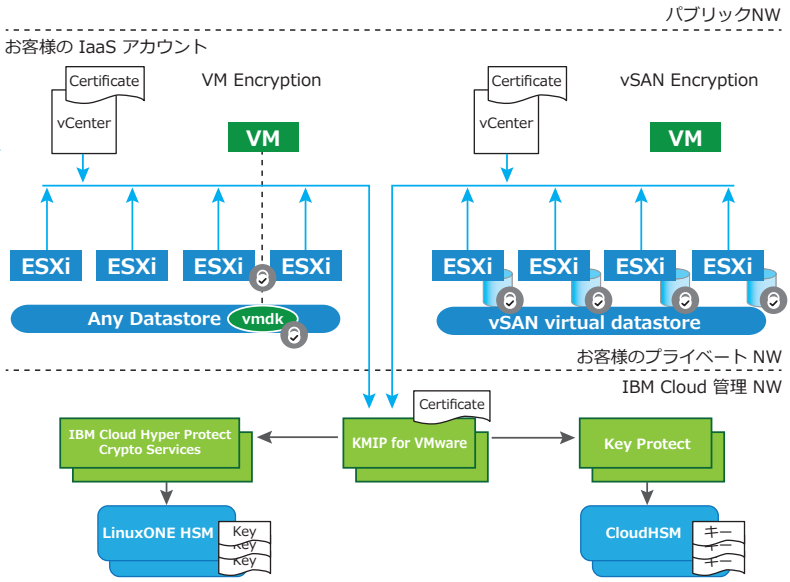
KMIP for VMware on IBM Cloud

https://cloud.ibm.com/docs/services/vmwaresolutions/archiref/kmip?topic=vmware-solutions-kmip-design&locale=en

IBM Key Protect またはIBM Cloud Hyper Protect Crypto Services を使用した鍵管理サービスです。
VMware の暗号化で必要な「サードパーティのキー管理サーバー（Key Management Server (KMS)）」に活用できます。

主な特長：

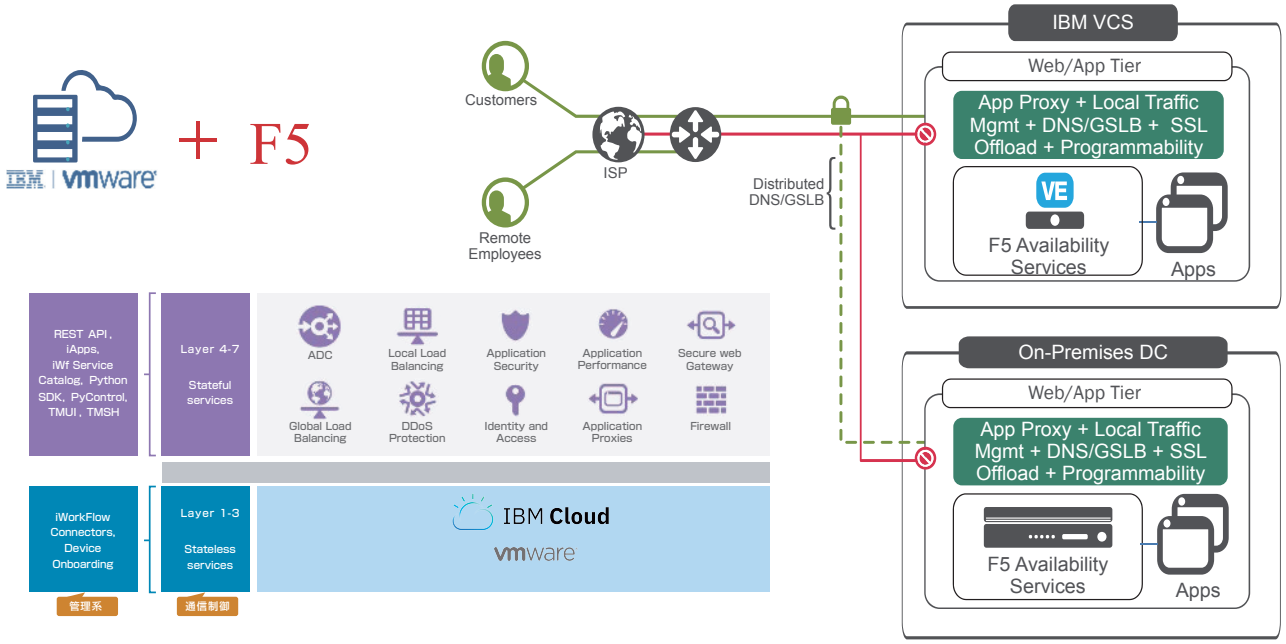
- VMware vSAN Encryption および VMware vSphere VM Encryption に対応
- VMware に認定された鍵管理サービス
  https://www.vmware.com/resources/compatibility/pdf/vi_kms_guide.pdf
- リージョンごとにプライベートエンドポイントが2 つ用意され、高可用性を実現可能
- IBM Cloud プライベートネットワークを使用してセキュアな接続が可能
- セキュリティ要件に応じて2種類の鍵管理バックエンドを選択可能
  - Key Protect
    - マルチテナント
    - FIPS 140-2 Level 2 認定
  - Hyper Protect Crypto Service
    - シングルテナント
    - FIPS 140-2 Level 4 認定



F5 on IBM Cloud

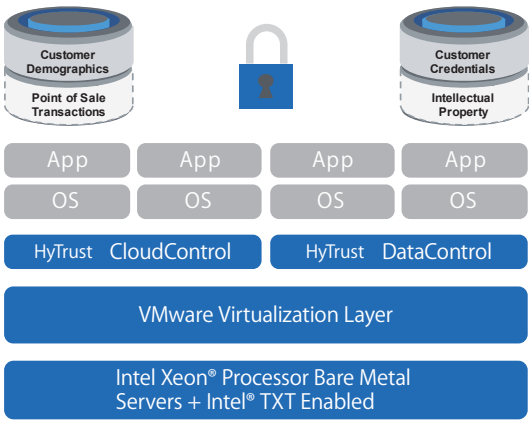
F5 BIG-IP Virtual Edition を使った、クラウド移行・ハイブリッド環境構築を容易に実現可能です。

- F5 BIG-IP のエンタープライズクラスのL4-7 機能を使って、セキュアな基盤を構築可能です。
- 帯域（スループット）と機能群の組み合わせを柔軟に選択でき、必要なときだけクラウドに展開可能です。
- 利用者は既存環境と同じ運用を、IBM Cloud の世界中のデータセンターで実現可能です。



IBM Cloud Secure Virtualization

Intel TXT とHyTrust を使って、GDPRに準拠することで、ハイブリッドクラウドにおける監査リスクを軽減します。
- Intel TXT により、仮想化環境のデータをマイクロチップレベルで保護することが可能です。
- 特定の地理的な境界におけるデータ制御を行うことが可能です。
- 信頼したハードウェア/ソフトウェア構成上でのみ稼働を許可し、継続的な監視・レポーティングが可能です。



セキュリティとコンプライアンスの自動適用

サーバーの完全性
改ざんされていないハードとソフト上でのみ稼働を許可します

承認ユーザーの管理
高度なアクセス制御機能と二次承認ワークフローにより管理リスクを軽減します

場所による復号制御
承認された場所でのみ仮想マシンデータの復号を許可します

場所による稼働ハード制御
承認された場所のハードでのみ仮想マシンの稼働を許可します

Single Node Trial

技術検証専用の1ノード環境を90日間ご提供します。(30日間で削除することもできます。)
いづれも、シングルテナントで、デプロイ後90日経過で自動消去されます。

- Single Node Trial for Migration and App Modernization
  - このトライアルは、20 個までの単純な開発またはテストのワークロードの移行を目的に設計されています。
  - VMware vCenter Server on IBM Cloud with HCX サービスと、Kubernetes ベースのアプリケーション開発プラットフォームによるそれらのワークロードのコンテナー化をお試しいただけます。
- Single Node Trial for Data Protection and Disaster Recovery
  - このトライアルは、VMware vCenter Server on IBM Cloud with HCX、Veeam、Zerto を使用する、25 個までのシンプルな開発やテストのワークロードの移行と複製を目的に設計されています。
  - ご自身のデータ・センターと同レベルの制御や可視性を維持しながら、災害復旧環境に対してクラウドをどう活用できるか、といった技術検証に適しています。

取扱注意
Handle with care

HCX接続に必要なオンプレミス環境の前提条件
- VMware vSphere およびvCenter Server 5.5 以降が必要です。
- vSphere 環境には、IBM Cloud にマイグレーションされる仮想マシン用の分散スイッチが必要です。
- HCX Manager 仮想アプライアンスが、オンプレミス環境のプライベート・ネットワークにデプロイできる状態であり、インターネットにもアクセスできる状態でなければなりません。

VMware on IBM Cloud の他社にない特長 まとめ

IBM | vmware

選択肢と柔軟性のある VMware サービス
ワークロードとビジネス要件に合わせて、サーバーを最適化
VMware クラスタを構成する物理ホストは、アラカルト、VCS と豊富な選択オプションがあり、お客様の拡張計画に合わせてCPU、メモリ、ディスクのスペックを柔軟に構成可能です。

お客様が vSphere 環境の管理者権限を保有
オンプレミスで求められる厳しい非機能要件をそのままリフト
ハードウェアおよびソフトウェア・スタックのアクセス権とコントロールを提供するため、VMware の全機能が利用できるため、計画停止のコントロール、障害発生時の問題判別が可能です。

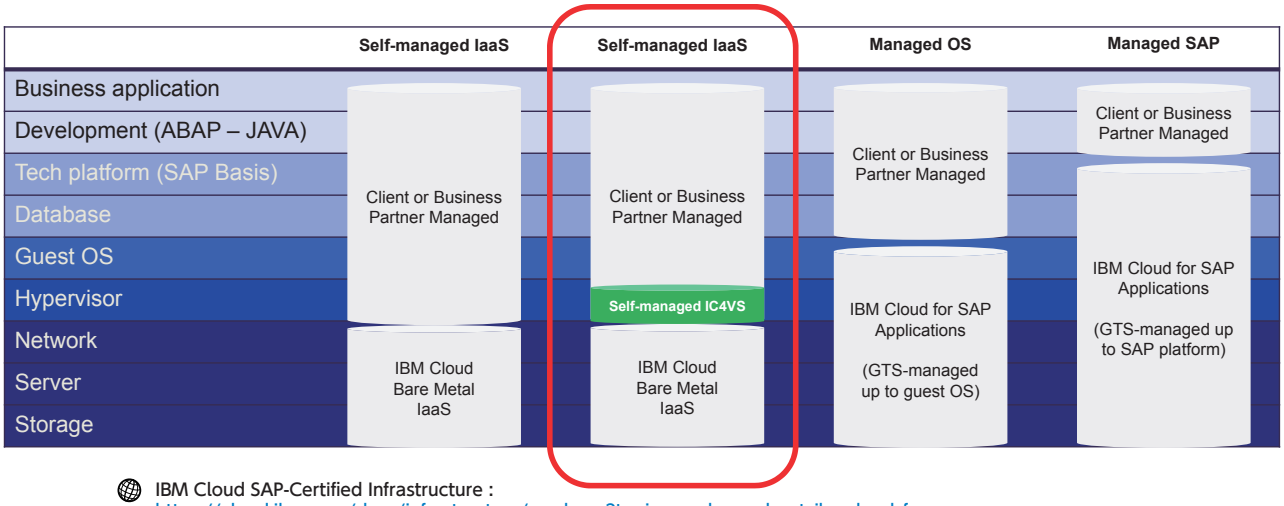
高速グローバル・ネットワークを無料利用
異なるゾーン・リージョン間での VMware データの転送料金コストを抑制
災害対策として海外D Cに仮想マシンのレプリケーションを取る際など無料で高速プライベート回線をご利用いただけます。海外からのアクセスも高速・安定・セキュアな通信が可能です。

エンタープライズにおける1,700社の実績
ハイブリッド・クラウド設計におけるベスト・プラクティスを活用
オンプレミス、クラウドともに多数のVMware 案件の実績があります。単なるテクノロジー・プロバイダーとしてだけでなく、サービス提供者として蓄積したスキル・ノウハウを提供します。

3-5. SAP on IBM Cloud

SAP Certified Baremetal とSAP Certified on VMware

SAP® HANA®およびSAP NetWeaver®の両方がベアメタルでテストされて実行環境としての認定を取得済みです。
大規模から小規模環境まで、様々な既存SAP環境に対応し、時間とコストを抑えてクラウド上に移行することが可能です。
VMware仮想化でベアメタルをより効率的に活用し、オンプレミスVMware環境とのシームレスな連携を実現します。



IBM Cloud SAP-Certified Infrastructure :
https://cloud.ibm.com/docs/infrastructure/sap-hana?topic=sap-hana-about_ibmcloud_for_sap

IBM Cloud には、SAP Certified Baremetal とSAP Certified on VMware の豊富なラインナップと多くの実績があります。

500+ TB of HANA DBs in production

1st SAP HEC partner

150+ SAP HANA Production Customers

HANA	Netweaver	Operating Systems	Other
• 2x 6140 (192GB, 384GB, 768GB) • 4x 8890v4 (1TB, 2TB, 4TB) • 8x 8890v4 (4TB, 8TB)	• 1x 1270v3 (32GB) • 1x 1270v6 (32GB, 64GB) • 2x 6140 (192GB, 384GB, 768GB) • 2x 2690v3 (128GB, 256GB) • 2x 2690v4 (512GB)	• RHEL 7.4 for HANA • RHEL 7.x for NW • SUSE SLES 12 SP2 • VMware 6.0, 6.5 • Microsoft Windows Server 2012, 2016	• Business Objects

3-6. IBM Power Systems Virtual Servers

IBM Power Systems Virtual Servers

https://cloud.ibm.com/docs/infrastructure/power-iaas

AIX/IBM i のPowerVMベースのLPARワークロードをクラウドでご利用いただけます。
他の仮想サーバーと同様にOSの構築まではIBM Cloudが行います。
2019年8月現在ではダラスとワシントンDCで利用することができます。
SLAは通常のIBM CloudのSLAに従います。

システム	E880(POWER8) or S922 (POWER9)
CPU	0.25 - 143 core (S922 は 15 core まで)
プロセッサー	Dedicated、Shared を選択可能
メモリ	2 - 9152 GB (指定したコア数の 64 倍まで)
ストレージ・タイプ	SSD or Standard (HDD)
ストレージ容量	10 GB - 2 TB (10 GB 単位で追加)
ネットワーク	Public(option), Private
IBM Cloud が提供する OS	AIX (7.1, 7.2) IBM i (7.2 , 7.3, 7.4)

ハードウェア仕様

コンピュート
- Power System E880 (9119-MHE)
  - 9 TB memory
  - 8 x 16 Gigabit PCI Express Dual-port FC
  - 10 x 10 Gigabit Ethernet-SR PCI Express Dual-port
- Power System S922 (9009-22A)
  - 384 GB memory
  - 2 x 16 Gigabit PCI Express Dual-port FC
  - 3 x 10 Gigabit Ethernet-SR PCI Express Dual-port

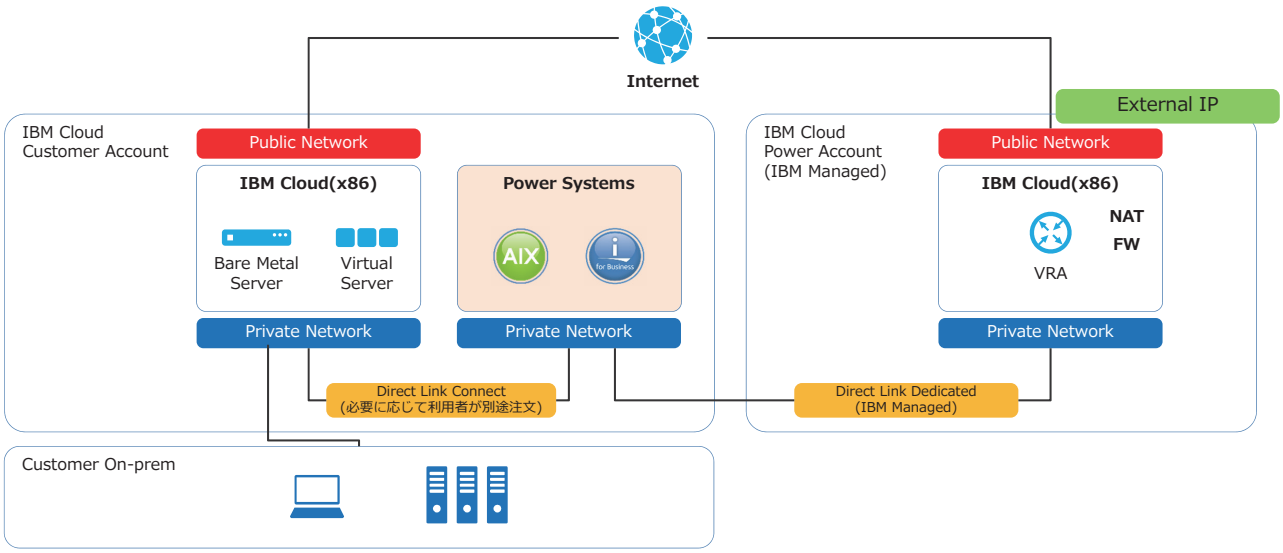
ストレージ
- Storwize V7000F(2076-AF6) Dual Controller
- Storwize V7000 (2076-624) Dual Controller

ネットワーク
- Cisco Nexus9000 93180YC-EX (10G)
- Cisco Nexus9000 C9348GC-FXP (1G)

ネットワーク構成

https://cloud.ibm.com/docs/infrastructurepower-iaas?topic=power-iaas-about-power-virtual-server

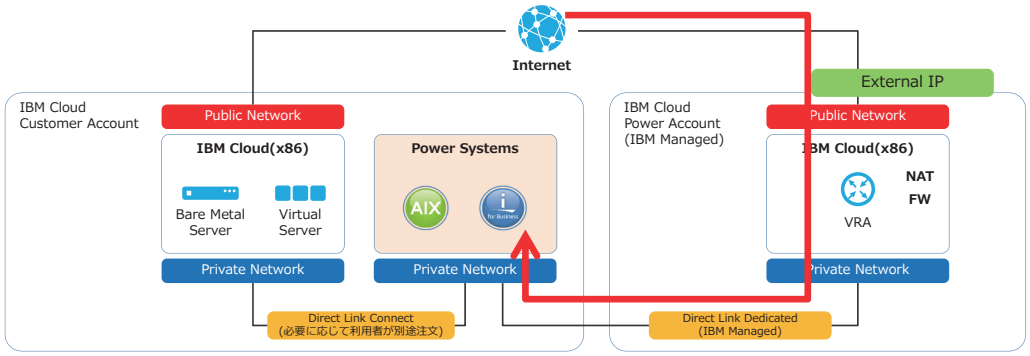
Power Systems Virtual ServersではPublic NetworkとPrivate Networkを利用することができます。
Power Systems Virtual Serversは、IBM Cloud(x86)上のリソースとは独立に管理されています。



Public Network

https://cloud.ibm.com/docs/infrastructure/power-iaas?topic=power-iaas-about-power-virtual-server

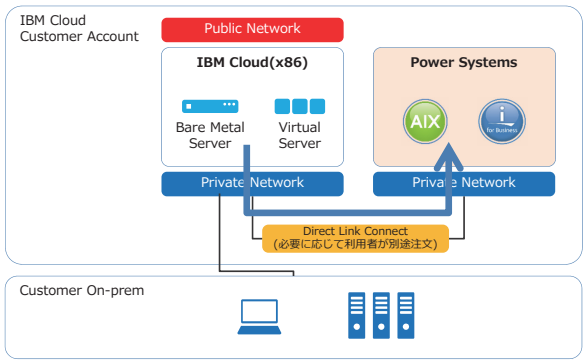
- **インスタンスのオーダー時**に有効化/無効化を選択することができます。
- 外部公開用途ではなく、**管理用途での利用**のみが想定されています。
- 「External IP」という名前のGlobal IPアドレスが払い出され、インターネット側からインスタンスにアクセスする際に利用することができます。「External IP」はOSに直接割り当てられるのではなく、IBM Cloud(x86)上に割り当てられます。「External IP」へのアクセスは、VRAでNATされて、IBM Cloudが管理する専用線経由でPower VMにアクセスされます。
- VRAによりFWが構成されており、SSH、HTTPS、Ping、IBM i 5250 terminal emulation with SSL (port 992)以外の通信はブロックされています。



Private Network

https://cloud.ibm.com/docs/infrastructure/power-iaas?topic=power-iaas-about-power-virtual-server

- **デフォルトで1つのPrivate IPアドレスが割り当てられます。**
- インスタンスにサブネットを割り当てた場合、各サブネットから**1つのIPアドレスが自動で**払い出されます。



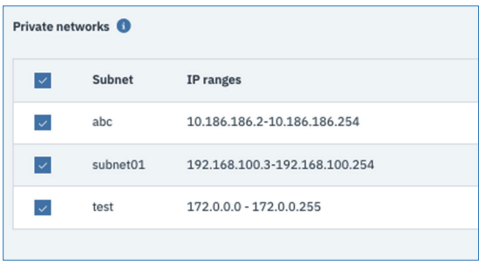
※構成上の注意

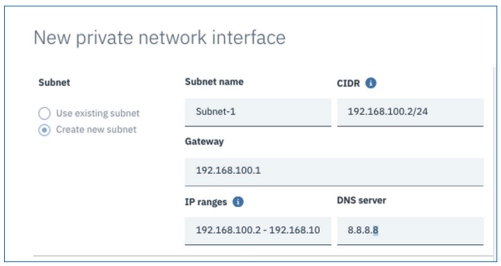
- **Power Systemsは、IBM Cloud(x86)上のリソースとは独立に管理されています。**
- そのため、IBM Cloud(x86)上のリソースと接続する際であっても、**Direct Link Connect(MegaPort)をオーダーする必要があります。**
- オンプレミス環境からPower System Virtual ServersのPrivate Networkに**直接アクセスすることはできません。**
- 接続するには一度IBM Cloud側のネットワークを経由してDirect Link Connect経由でアクセスする必要があります。
- FW、LBなどのサービスはPower Systems Virtual Serversのオファリングとしての提供は有りません。
- パッチサーバーは自分で構築する必要があります。

Private Network Subnetの作成

https://cloud.ibm.com/docs/infrastructure/power-iaas?topic=power-iaas-cps-configuring

Power Systems Virtual Serversでは、Private Networkのサブネットを自由に作成することができます。
インスタンスの作成時に自由に割り当てることが可能です。
IPアドレスの範囲は、CIDR表記で記述する必要があります。





取扱注意
Handle with care

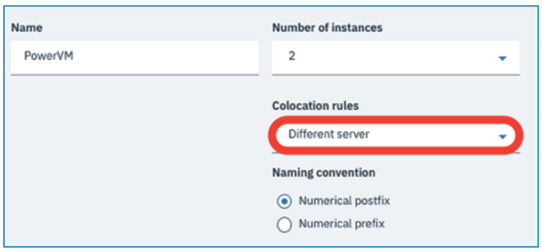
※「Gateway」は、IP rangesの範囲外のIPアドレスを指定する必要があります。
※IP rangesとしてRFC 1918(10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16)の範囲外のIPを指定した場合、そのサブネットを割り当てたインスタンスはPublic Internetには接続できなくなります。

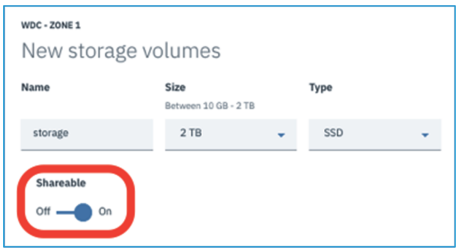
高可用性設計

https://cloud.ibm.com/docs/vsi

Power Systems Virtual Serversではハードウェア障害時には別のホスト上で再始動するRemote Restart機能を採用しています。
また、より高度なHA/DRソリューションとして、下記のソフトウェアを利用することが可能です。

- PowerHA SystemMirror for AIX Standard Edition
  - Power Systemベースの AIX用の高可用性クラスターソリューションです。
  - ソフトウェアを購入後、Entitled System Supportのサイトからダウンロードし、利用するPower Systems Virtual Serversにインストールしてください。
  - この機能を利用するには、インスタンスのオーダー時に**2台以上のインスタンス**を同時にオーダーし、Colocation Rulesを「Different Server」にする必要があります。
  - また、Storageの作成時に「**Shareable**」を**On**にする必要があります。

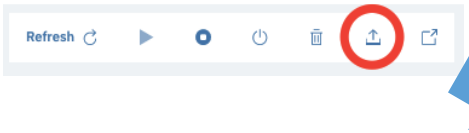




バックアップ

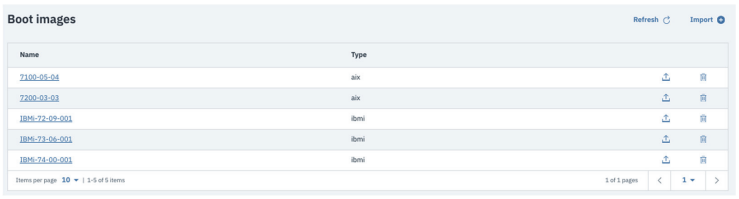
https://cloud.ibm.com/docs/infrastructure/power-iaas?topic=power-iaas-capturing-exporting-vm

Power Systems Virtual ServersではイメージのExport機能を提供しています。
Export機能はIBM Cloud Portal、もしくはCLIから利用することができます。
Exportする際にはストレージのFlash CopyからOVAを作成します。
Export先としてImage Catalog、もしくはIBM Cloud Object Storageを選択することができます。



IBM Cloud Object Storage

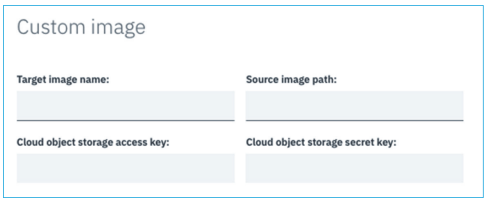
Image Catalog



カスタムイメージの利用

https://cloud.ibm.com/docs/infrastructure/power-iaas?topic=power-iaas-configuring-custom-image

Power Systems Virtual ServersではIBM PowerVCなどで作成した仮想マシンのカスタムイメージを持ち込んで利用することが可能です。
カスタムイメージからインスタンスをデプロイするには、作成したイメージをIBM Cloud Object Storageにアップロードします。



項目	入力内容詳細
Target image name	任意のイメージ名
Source image path	対象のイメージのパス 「エンドポイント名 / バケット名 / ファイル名」を入力
Cloud object storage access key	IBM Cloud Object Storage の Service Credential の access_key_id
Cloud object storage secret key	IBM Cloud Object Storage の Service Credential の secret_access_key

取扱注意
Handle with care

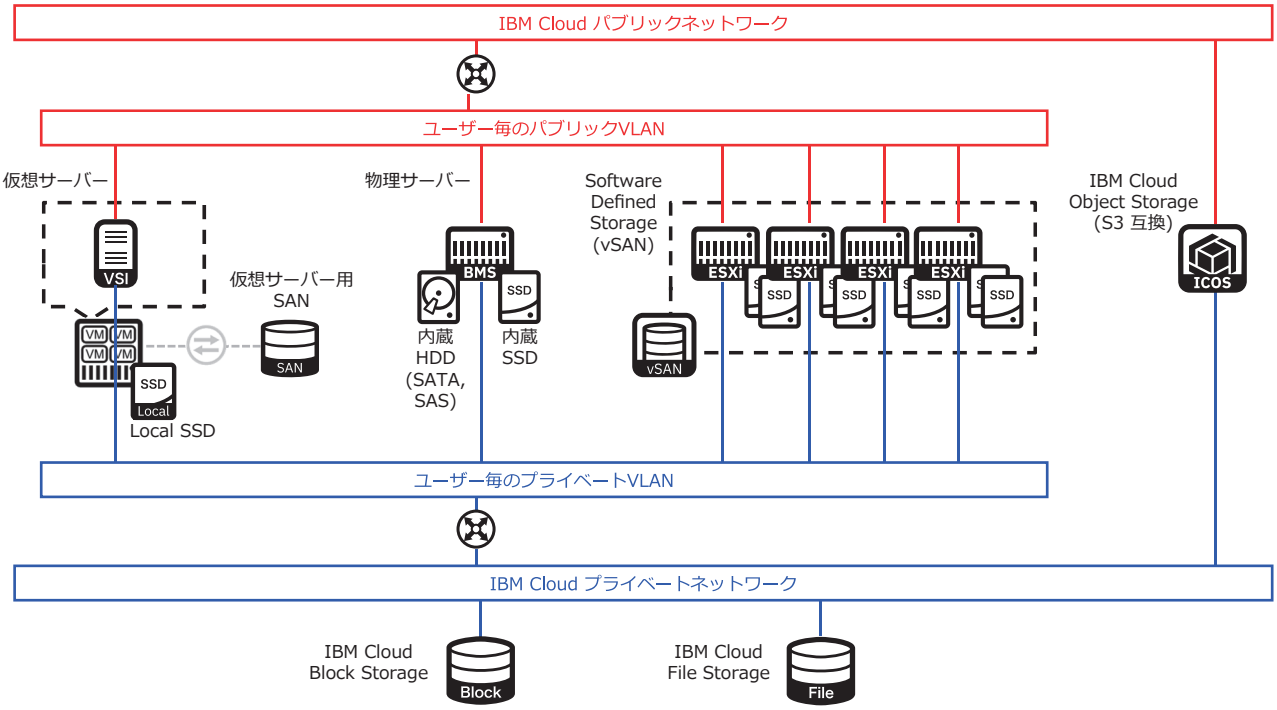
- 持ち込むAIX/IBM iのバージョンやTechnology Levelが、選択したMachine Type(E880 or S922)上でサポートされていることを事前に確認してください。
- IBM Cloud Object StorageのCredential情報を作成する際にHMAC(Hash-based Message Authentication Code)を利用する必要があります。
- OS ライセンスを持ち込むことはできません。

4 ストレージ

INDEX

4-1. ストレージ概要

IBM Cloud では
ローカルストレージの他にも以下のストレージ・サービスを提供します。複数を組み合わせることも可能です。



それぞれ、以下のような特徴があります。

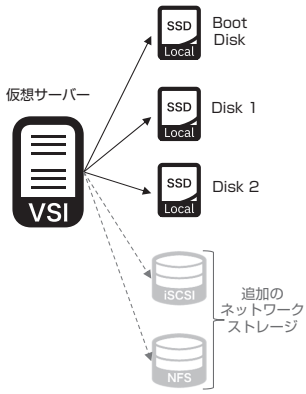
https://www.ibm.com/cloud/storage

名称	Local SSD (仮想サーバー)	SAN (仮想サーバー)	内蔵HDD・SSD (物理サーバー)	VMware vSAN	IBM Cloud Block / File Storage	IBM Cloud Object Storage
主な用途	•OSブート •高速な読み書き	•OSブート •ファイルサーバー	•OSブート •ファイルサーバー •高速な読み書き	•共有データストア •高速な読み書き	•ファイルサーバー •共有データストア •バックアップ	•画像/動画保管 •バックアップ •ログアーカイブ
シングルテナント	×	×	○	○	×	×
物理ディスクに対する耐障害性	×	×	× (任意のRAID)	○ (任意のRAID)	○	○
複数拠点のデータ保管機能	×	×	×	○ (Stretch Cluster)	○ (Replication)	○ (広域分散)
Snapshot 機能	×	×	×	△ (Technical Preview)	○ (論理領域単位)	×
ストレージ暗号化機能	○	○	△ (一部のSED)	○ (vSAN Encryption)	○	○
1 論理領域あたりの性能	50 KIOPS 前後 (100GB)	25 KIOPS 前後 (100GB)	N/A	数百 KIOPS 〜数 MIOPS	〜180 KIOPS	N/A
1 論理領域あたりの容量	25〜500GB	10GB〜2TB	600GB〜432TB	十数〜数百 TB	20GB〜24TB	無制限

4-2. Local SSDストレージ（仮想サーバー）

仮想サーバーの「Balanced local storage」「GPU」プロファイルで、ホストサーバーの内蔵SSD を活用できます。
ただし、ホストサーバーの物理障害時に、仮想サーバーが他のホストサーバーで起動されない点に注意が必要です。

- 「Boot Disk」は、OS が導入されるブート領域。Linux, Windows を問わず、「100 GB」となる。
- 「Disk 1, 2」は、追加のLocal SSD ストレージ領域。追加可能な容量は、仮想サーバーのスペックによって異なる。

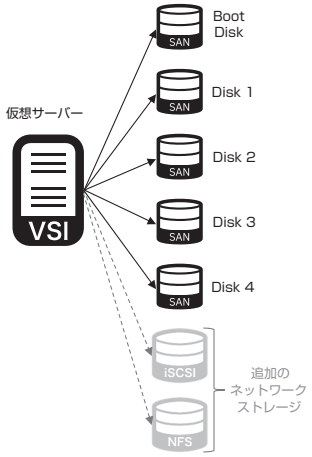


プロファイル	Boot	Disk 1								Disk 2			
Balanced Local	100 GB	25 GB	100 GB	150 GB	200 GB	250 GB	300 GB	400 GB	500 GB	250 GB	300 GB	400 GB	500 GB
BL2.1x2	○	○	○										
BL2.1x4	○	○	○										
BL2.2x4	○		○		○								
BL2.2x8	○		○		○								
BL2.4x8	○			○			○						
BL2.4x16	○			○			○						
BL2.8x16	○					○				○			
BL2.8x32	○					○				○			
BL2.16x32	○						○				○		
BL2.16x64	○						○				○		
BL2.32x64	○							○				○	
BL2.32x128	○							○				○	
BL2.56x242	○								○				○

4-3. SANストレージ（仮想サーバー）

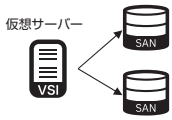
仮想サーバーの「Balanced」「Compute」「Memory」「GPU」プロファイルで、SAN ストレージを活用できます。
ホストサーバーの物理障害時には、仮想サーバーが他のホストサーバーで起動されるため、可用性を維持できます。

- 「Boot Disk」は、OS が導入されるブート領域。Linux は「25 GB」「100 GB」, Windows は「100 GB」から選択。
- 「Disk 1, 2, 3, 4」は、追加のSAN ストレージ領域。追加可能な容量は、Disk あたり25 GB ~ 2 TB。
- 「Disk 1, 2, 3, 4」は、「Portable Storage」として柔軟に着脱が可能。「Portable Storage」の別途注文も可能。



Portable Storage

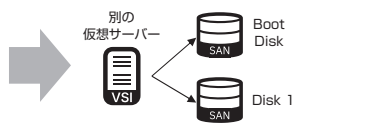
✓ Disk 1 以降を切り離す(Detachする)と「Portable Storage」になる。



✓ 元の仮想サーバーを削除しても「Portable Storage」は残る。

✓ 別の仮想サーバーの追加 Disk として接続(Attach)することができる。

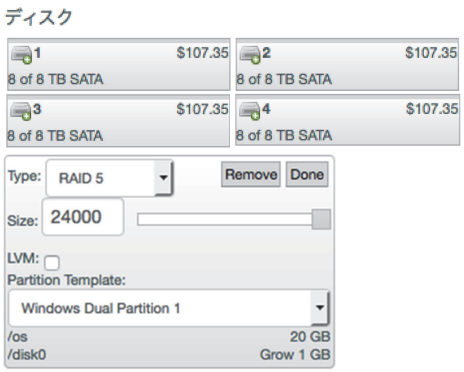
✓ 他のDCの仮想サーバーにも接続可能(Attach によって他のDCに移動する)



4-4. 内蔵HDD・SSD (物理サーバー)

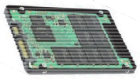
物理サーバーの内蔵ディスクを専有利用することで、安定したパフォーマンスが期待できます。
任意のRAID 構成を組むことで、Disk 障害に対してデータ冗長性を確保することができます。

- ベアメタルの筐体ごとに搭載可能ドライブ数が異なる
- 最小1ドライブ～最大36ドライブ
- RAID構成やパーティションを自由に設定可能
- 一部のDisk で自己暗号化ドライブ(SED) に対応



SATA (serial advanced technology attachment)
- 1 Diskあたり1TB～10TBを構成可能
- 大容量を搭載できるが、他に比べて性能は劣る
- ウェブ、メール、ファイルサーバーなどに最適

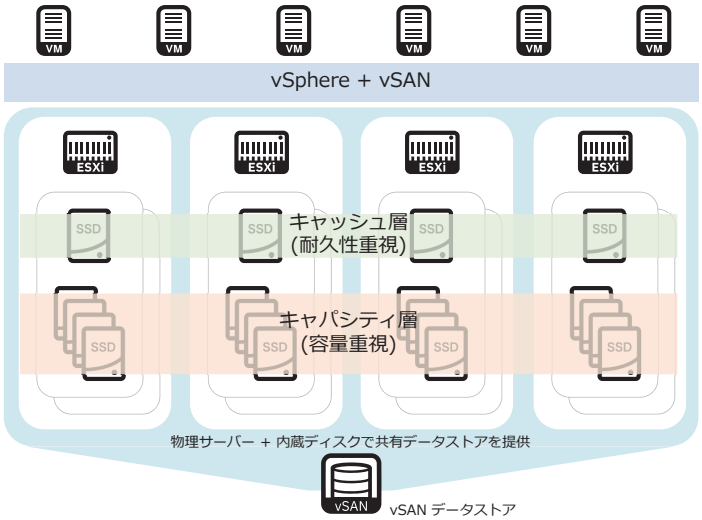
SAS (serial attached SCSI)
- 1Disk あたり600 GB を構成可能
- より信頼性が高く、高速なストレージ
- データベース、重要なシステムなどに最適



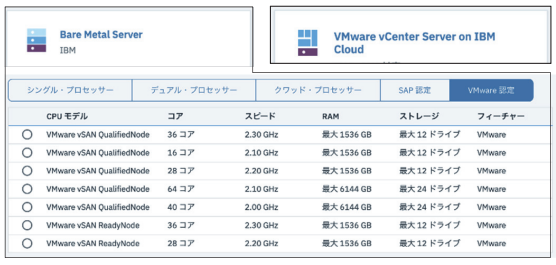
SSD (solid state drive)
- 1Diskあたり800GB～3.8TBを構成可能
- 高速かつ低遅延なストレージ
- データに頻繁にアクセスするアプリなどに最適

4-5 . VMware vSAN (Software Defined Storage)

vSphere ハイパーバイザーに統合されたSDS を活用して、お客様専有のストレージを構成できます。
冗長性と拡張性を備え、物理サーバーやSSD を増設することで簡単にスケールアウトが可能です。
ホスト1 台あたり最大10 万IOPS の、予測可能で非常に優れたパフォーマンスを実現します。



✓ vSAN 認定のコンポーネントを利用するには、
ベアメタルの「VMware 認定」ノードか、
「VMware vCenter Server on IBM Cloud」から
ご注文していただけます。



取扱注意
Handle with care

キャッシュ層、キャパシティ層ともに全てSSD のオールフラッシュのみサポートします。
IBM Cloud のvSAN ライセンスを購入する場合、キャパシティ層の総容量でTier が定められます。

4-6. IBM Cloud Block / File Storage

https://www.ibm.com/jp-ja/cloud/block-storage
https://www.ibm.com/jp-ja/cloud/file-storage

月課金もしくは時間課金で提供されるマルチテナント型のマネージドストレージサービスです。
1 GB あたりにIOPS が割り当てられ、ネットワーク経由で利用できます。管理は、ポータルまたはAPIを介して行います。

・Block Storage : iSCSI 接続
  ・Windows、Linux、VMwareから利用可能
  ・最大64 デバイス/サブネット/IP の接続
  ・マルチパス構成にすることを強く推奨

・File Storage : NFS 接続
  ・Linux、VMwareから利用可能
  ・最大64 デバイス/サブネット/IP の接続
  ・NFS v3の利用を強く推奨

主な機能:

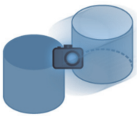
・事前定義されたIOPS Tier「Endurance」と、カスタムIOPS「Performance」のオプションによる柔軟な構成

・保存データの暗号化
  ・IBM が管理する鍵で
  ディスクレベルの暗号化を実施

・1 GB 単位で指定可能なボリュームサイズ
  ・サイズ拡張およびIOPS 変更が可能

・スナップショット
  ・論理領域単位で取得・復元が可能
  ・スナップショットから領域の複製が可能

・レプリケーション
  ・DC間のフェイルオーバー、
  フェイルバックに利用可能



取扱注意 Handle with care

Block Storageにおいて、MPIOが適切に構成されていない場合、計画メンテナンス時に予期せず利用できない可能性があります。
OSごとの設定をご確認ください。
• https://cloud.ibm.com/docs/infrastructure/BlockStorage?topic=BlockStorage-mountingLinux#verifyMPIOLinux
• https://cloud.ibm.com/docs/infrastructure/BlockStorage?topic=BlockStorage-mountingWindows#verifyMPIOWindows

選べる性能タイプ

「Endurance」- 事前定義されたIOPS Tier
  ・GB単位の価格体系で提供される定義済みTier

取扱注意 Handle with care

IOPS は「16KBブロックサイズでread/writeの比率が50:50のランダムなIO」が基準です。
アプリが64KBブロックサイズで書き込む場合、4回の書き込みに相当します。
https://cloud.ibm.com/docs/infrastructure/BlockStorage?topic=BlockStorage-getting-started

・Block Storage
  ・0.25 / 2 / 4 IOPS Tier の場合、最大16 TB, 64000 IOPS
  ・10 IOPS Tier の場合、最大4 TB, 40000 IOPS

・File Storage
  ・0.25 / 2 / 4 IOPS Tier の場合、最大24 TB, 96000 IOPS
  ・10 IOPS Tier の場合、最大18 TB, 180000 IOPS

ラインナップ		概要	代表的な用途
0.25 IOPS/GB	軽めのシステム向け	バックアップ、ファイルサーバー、メールサーバー等	ファイル共有、Exchange、Sharepoint など
2 IOPS/GB	デフォルトはこちら	一般的な IO システム向け。DB や仮想化環境の基盤など	3D VDI、SQL、Oracle、VM OS など
4 IOPS/GB	パフォーマンス重視	高 IO システム向け。パフォーマンス要件のある DB など	SQL、Oracle、SAP、HANA など
10 IOPS/GB	ハイパフォーマンス	ハイパフォーマンスが必要な環境向け	高トランザクション向けの DB、File Server など

「Performance」- カスタムIOPS
  ・カスタムIOPS の割り当てによる柔軟な構成

・Block Storage : 最大16 TB, 76000 IOPS

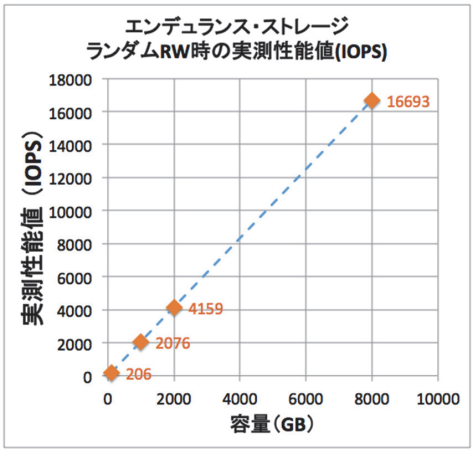
サイズ (GB)	20～	40～	80～	100～	500～	1,000～	2,000～	3,000～	4,000～	8,000～	10,000～	12,001～	14,000～	16,000
最小 IOPS	100	100	100	100	100	100	200	200	300	500	1,000	6,000	8,000	10,000
最大 IOPS	1,000	2,000	4,000	6,000	10,000	20,000	40,000	48,000	48,000	48,000	48,000	56,000	64,000	76,000

・File Storage : 最大24 TB, 96000 IOPS

サイズ (GB)	20～	40～	80～	100～	500～	1,000～	2,000～	3,000～	4,000～	8,000～	10,000～	12,001～	14,000～	16,000～	19,000～24,000
最小 IOPS	100	100	100	100	100	100	200	200	300	500	1,000	6,000	8,000	10,000	10,000
最大 IOPS	1,000	2,000	4,000	6,000	10,000	20,000	40,000	48,000	48,000	48,000	48,000	56,000	64,000	76,000	96,000

「Endurance」タイプでのパフォーマンス実測値

下記は「2 IOPS/GB」のストレージ性能の実測値を、fioコマンドにより測定した実測値から作成しました。
このグラフから、容量(GB) の増加に比例して、性能(IOPS) の実測値が高くなっていることが分かります。
そして、このグラフの傾きが約2 IOPS/GB（「Endurance」タイプのとおり）となっていることが分かります。



【参考】各IOPSにおける性能の目安

性能の目安	性能タイプ－0.25 IOPS/GB			
	容量(GB)	月額料金($)	容量単価($/GB)	性能値(IOPS)
Note PC HDD並み	500	56.5	0.113	125
100～320 IOPS	1000	113	0.113	250
SATA HDD 並み	2000	226	0.113	500
400～1K IOPS	4000	452	0.113	1000
SAN ストレージ並み	8000	904	0.113	2000
2K～8K IOPS	12000	1356	0.113	3000
SSD 並み				
10K IOPS以上				

	性能タイプ－2 IOPS/GB			
	容量(GB)	月額料金($)	容量単価($/GB)	性能値(IOPS)
	80	18.08	0.226	160
	100	22.6	0.226	200
	250	56.5	0.226	500
	500	113	0.226	1000
	1000	226	0.226	2000
	2000	452	0.226	4000
	4000	904	0.226	8000
	8000	1808	0.226	16000
	12000	2712	0.226	24000

性能の目安	性能タイプ－4 IOPS/GB			
	容量(GB)	月額料金($)	容量単価($/GB)	性能値(IOPS)
Note PC HDD並み	40	15.82	0.3955	160
100～320 IOPS	80	31.64	0.3955	320
SATA HDD 並み	100	39.55	0.3955	400
400～1K IOPS	250	98.875	0.3955	1000
SAN ストレージ並み	500	197.75	0.3955	2000
2K～8K IOPS	1000	395.5	0.3955	4000
	2000	791	0.3955	8000
SSD 並み	4000	1582	0.3955	16000
10K IOPS以上	8000	3164	0.3955	32000
	12000	4746	0.3955	48000

	性能タイプ－10 IOPS/GB			
	容量(GB)	月額料金($)	容量単価($/GB)	性能値(IOPS)
	20	13.11	0.6555	200
	40	13.11	0.6555	400
	100	13.11	0.6555	1000
	250	13.11	0.6555	2500
	500	13.11	0.6555	5000
	1000	13.11	0.6555	10000
	2000	13.11	0.6555	20000
	4000	13.11	0.6555	40000

取扱注意

VMware 利用時にデータストアのパフォーマンスを最適化するには、下記リンクの推奨パラメータをご設定ください。
https://cloud.ibm.com/docs/services/vmwaresolutions/vcenter?topic=vmware-solutions-vc_bom#vc_bom-esxi-server-advance-config

サイズ拡張およびIOPS 変更機能

https://qiita.com/testnin2/items/f9816f22ae7777905cae

主な用途:

- まずは小さなLUN容量で始めたい
- 後でLUN容量を大きくしたい
- 繁忙期のみ高速のIOPSに変更したい
- 災害発生後の切替時のみ高速のIOPSに変更したい

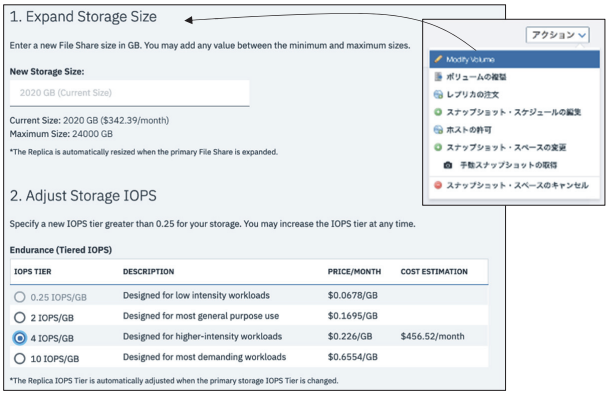
主な特長と制限:

- オンラインで変更されるが即時には反映はされない
- LUN容量拡張は1GB単位から可能
- LUN容量は大きくはできるが、小さくはできない
- Endurance (IOPS Tier) において、
  0.25 IOPS Tier の場合、2/4/10 IOPS Tier に変更できない
  2/4/10 IOPS Tier の場合、0.25 IOPS Tier に変更できない
- Performance (Custom IOPS) において、
  0.3 IOPS/GB 未満の場合、0.3 IOPS/GB 以上に変更できない
  0.3 IOPS/GB 以上の場合、0.3 IOPS/GB 未満に変更できない
- IOPS を低速に変更できるのは、30日に1回まで
- レプリカ構成済みの場合、レプリカ側も変更が自動的に反映される

取扱注意

2017年以前に購入したLUN に対しては
本機能が有効でない場合がありますのでご注意ください。

ストレージ詳細画面の「Modify Volume」から変更可能



コマンドでの実行例

```
# ibmcloud sl file volume-modify <Storage ID> --new-size 100
# ibmcloud sl block volume-modify <Storage ID> --new-tier 4
```

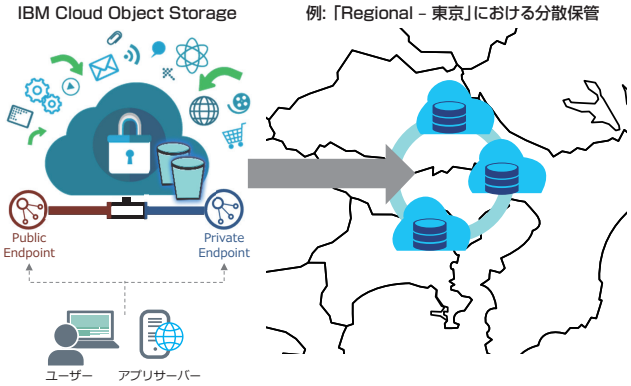
4-7. IBM Cloud Object Storage (ICOS)

文章、写真、PDF、動画、バックアップなど、いかなるフォーマットでも格納できる非定型データ用のストレージです。
静的データの長期保管、メディア・オブジェクトの保管、メディアの配信などに利用されています。

https://www.ibm.com/jp-ja/cloud/object-storage

主な機能:

- 高い回復性と可用性
  - 保存データは3ヵ所以上で自動的に分散保管
  - 99.9999999999999 (15 nine) の耐久性
  - 保存データは自動的に暗号化
- コスト効率の高いストレージ
  - 1GB/月を数円から使える安価な従量課金
  - GB からEB (エクサバイト) 超の拡張性
  - 最大25 GB/月まで無料なライトプラン
- 多様な接続性
  - S3 互換API のため、資格情報およびエンドポイントを既存ツールの連携に利用可能
  - プライベートエンドポイントの提供により、セキュアかつ無制限な帯域幅を利用可能



取扱注意

バケット名は、全てのアカウントを通じてユニークな値を設定する必要があります。
バケット数は最大100ですが、バケットあたりのオブジェクト数は無制限です。1オブジェクトの最大サイズは、10TBです。
https://www.ibm.com/jp-ja/cloud/object-storage/faq

レジリエンシーとロケーション

以下のレジリエンシーとロケーションから、データ保管場所を選択できます。

- Cross Region – 1 つのGeo 内の3 つのリージョンにまたがって保管され、最も可用性と回復性に優れます。
- Regional – 1 つのリージョン内の複数のゾーンにまたがって保管され、最も可用性とパフォーマンスに優れます。
- Single Site – 1 つのデータセンター内の複数のデバイスにまたがって保管され、最も局地性に優れます。

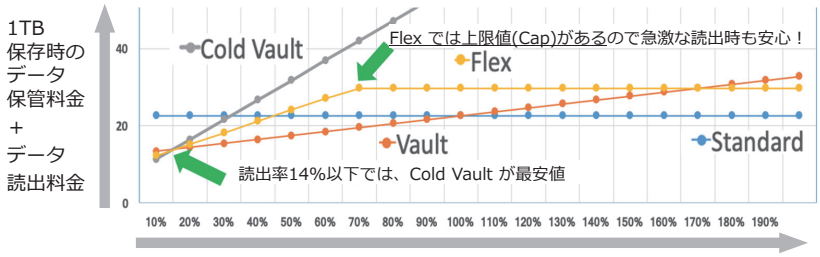
ストレージクラス

お客様のデータ利用パターンに合わせた多様なストレージ・モデルを提供します。

Storage Class	Standard	Vault	Cold Vault	Flex
データ特性	アクセス頻度が高い	よりアクセス頻度が低い	最小限のアクセスでよい	アクセス頻度が動的または予測不可能
主な用途	コラボ、ファイル共有など	バックアップ、災害対策など	アーカイブ、監査ログ保管など	クラウドネイティブ、AI アプリなど
アクセス頻度	月に複数回	月に1回、またはそれ以下	3ヶ月に1回、またはそれ以下	使いたいときに使いたいだけ
最低保管期間	なし	30日	90日	なし
最低オブジェクトサイズ	なし	128 KB	256 KB	なし
データ保管料金	高い ←	普通	→ 安い	普通より安い
データ読出料金	無料	安い →	高い	普通

合算の上限値が設定されています

【参考】ストレージクラスごとの課金イメージ



取扱注意 Handle with care

それぞれの詳細な価格体系は
下記リンクをご参照ください。
https://www.ibm.com/cloud/object-storage/pricing/

SLA

ICOS のSLA は、IBM Cloud共通のSLAとは異なり、
IBM Cloud Object Storage サービス記述書にストレージクラスごとに記載されています。

- SLA は稼働保証ではなく、停止時間に応じた払い戻し(クレジット発行)の基準(ルール)です
  - 翌月(もしく翌々月)の請求分から払戻の分を差し引く形で処理がされます。
  - あくまでも「マイナス請求対応」であり、**単純な払い戻しは行われません**。
    (つまり請求金額がそもそもゼロ円の場合、返金はされません)
  - クレジット発行の手続きは、サービス記述書に記載のある期限内で
    アカウント管理者がチケットで依頼する必要があります。

Object Strage のクラスの可用性レベル			クレジット
Standard/Flex	Vault	Cold	
< 99.95%	< 99.50%	< 99.00%	10%
< 99.90%	<99.00%	< 98.00%	25%

https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7857-04/$file/i126-7857-04_12-2018_ja_JP.pdf

最新情報・詳細条件等については、下記リンクより、ご確認ください。
IBM Cloud サービス記述書 : https://www-03.ibm.com/software/sla/sladb.nsf/sla/bm

第三者による直近の稼働状況については、下記リンクよりご確認いただけます。
IBM Cloud Service Status ｜ CloudHarmony : https://cloudharmony.com/status-of-storage-for-softlayer

ICOSへのアクセス方法

ICOS のアクセス方法として考慮すべきポイントは3つあります。

1. エンドポイント情報(接続先URL情報)
   Regional/Cross Regional/Single DC/EU-Managed によって接続先情報は異なります。以下をご参照ください。
   https://cloud.ibm.com/docs/services/cloud-object-storage?topic=cloud-object-storage-endpoints

2. 認証方式:
   - IAM Token: IBM Cloudが発行するIAM Tokenを利用するアクセス方式。
   - HMAC資格情報: ID/Password方式でのアクセス方式。詳細は次頁参照。

3. アクセス方式
   ICOSへのアクセス方法は以下の２つがサポートされていますが、今後は**仮想ホスト形式でのアクセスが推奨されます**。
   - 仮想ホスト形式(推奨)
     https://<bucket>.<endpoint>/<object>
   - パス形式
     https://<endpoint>/<bucket>/<object>

サービス資格情報を使ったS3 互換ツール連携

S3 CLI, S3cmd, Cloudberry, Cyberduck 等、一般的なS3 プロトコル互換ツールによるアクセスを行うためには、
「HMAC 資格情報を含める」にチェックし、**{"HMAC":true}** が追加されたことを確認してHMAC キーを生成します。
これによって**"access_key_id"** と**"secret_access_key"** が"cos_hmac_keys" として構成され、
これらのキー情報によって各種ツールによるデータアクセスが可能になります。

取扱注意
Handle with care

IAM トークンによる認証とHMACキー認証その他留意事項
IAM資格で署名生成するとREST API コールを行う場合は
追加のヘッダー情報が必要になります。
https://cloud.ibm.com/docs/services/cloud-object-storage/hmac?topic=cloud-object-storage-hmac#using-hmac-credentials

https://cloud.ibm.com/docs/services/cloud-object-storage/iam?topic=cloud-object-storage-service-credentials#service-credentials

各種機能対応表

各種機能の対応表の中から、東京リージョンに関連する内容を表記します。
「Single Site」バケットを含む最新状況は
https://cloud.ibm.com/docs/services/cloud-object-storage/basics/services.html#integrated-service-availability
をご参照ください。

「Cross Region」バケット

ロケーション	Aspera	Key Protect	Hyper Protect Crypto Services	Archive Rule	Expiration Rule	Retention Policy	Access Policy	Activity Tracker With LogDNA	SQL Query	Functions
ap-geo (東京/ソウル/香港)	○	×	×	×	○	×	○	○	○	×
eu-geo (アムステルダム/フランクフルト/ミラノ)	○	×	×	×	○	×	○	○	○	×
us-geo (ダラス/サンノゼ/ワシントン)	○	×	×	×	○	○	○	○	○	×

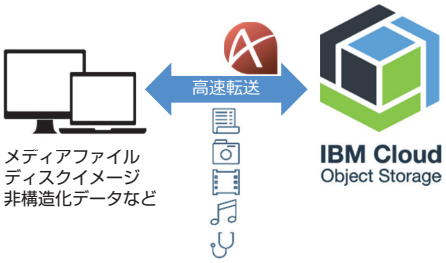
「Regional」バケット

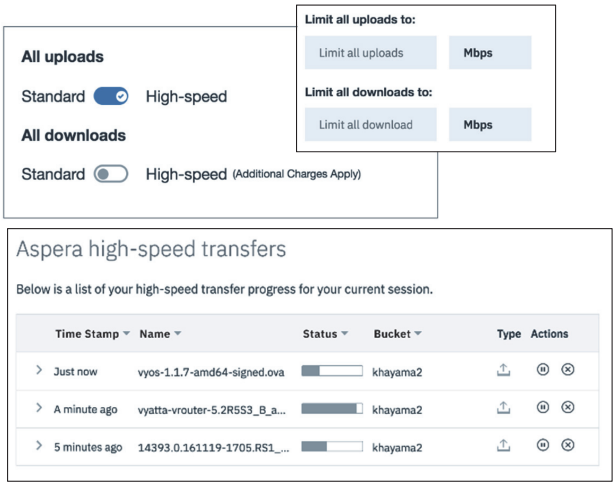
ロケーション	Aspera	Key Protect	Hyper Protect Crypto Services	Archive Rule	Expiration Rule	Retention Policy	Access Policy	Activity Tracker With LogDNA	SQL Query	Functions
au-syd (シドニー)	○	○	○	○	○	○	○	○	○	×
jp-tok (東京)	○	○	×	○	○	○	○	○	○	○
eu-gb (ロンドン)	○	○	×	○	○	○	○	○	○	○
eu-de (フランクフルト)	○	○	○	○	○	○	○	○	○	○
us-south (ダラス)	○	○	○	○	○	○	○	○	○	○
us-east (ワシントン)	○	○	×	○	○	○	○	○	○	○

ICOS にビルトインされたAspera 高速転送オプション

標準のhttps / sftp よりも高速なオンライン転送速度でIBM Cloud にデータを移行できるようになります。
Aspera では、特許取得済みのFASP プロトコルで転送を行うため、距離によるLatency に影響を受けません。
しかも、ICOS へ転送（アップロード）する際のAspera の利用料金は無料です。※取り出し（ダウンロード）時は有料

https://cloud.ibm.com/docs/services/cloud-object-storage/basics?topic=cloud-object-storage-upload#high-speed-transfer
https://www.ibm.com/cloud/object-storage/pricing/#s3api





※ Aspera クライアントもしくはAspera SDK (いずれも無償)をインストールいただくことでご利用いただけます。
※ 転送中のデータは暗号化されます。
※ データ取り出し時は、Aspera利用料に加えて、パブリック・アウトバウンド料金とICOSのREAD料金がかかります。

取扱注意

Aspera サービスへは、Proxy 経由でのアクセスをサポートしません。
リンク先情報に合わせて、社内NW 設定等を変更する必要があります。
https://ats.aspera.io/pub/v1/servers/softlayer

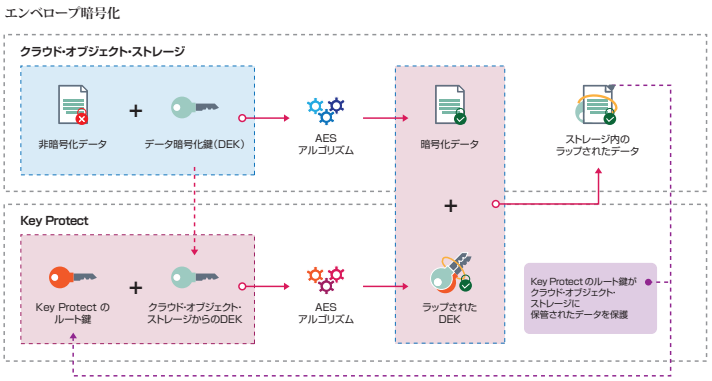
IBM Cloud Object Storage (ICOS) に Aspera を使ってデータを転送する https://www.youtube.com/watch?v=HoBp4a5MTZo

Key Protect / Hyper Protect Crypto Services を統合したBYOK (Bring Your Own Key)

通常ICOS 上のデータはIBM が管理するデータ暗号鍵（DEK）が用いられ、DEK はIBM によって適切に管理されます。
Key Protect / Hyper Protect Crypto Services で発行されるルート鍵でDEK を暗号化することで、
データ暗号化に関するマスター鍵はお客様主体の管理となり、必要なコンプライアンスに準拠した運用が可能です。

✓ Key Protect / Hyper Protect Crypto Services と統合するには、バケット作成時に指定する必要があります。

https://cloud.ibm.com/docs/services/key-protect?topic=key-protect-integrate-cos



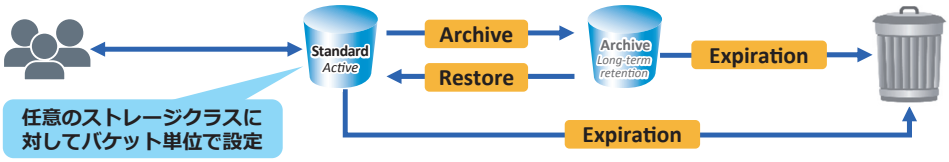
IBM Cloud Object Storage (ICOS) に Key Protect を統合して鍵管理を行う https://www.youtube.com/watch?v=GRHbI1Cv6aY

取扱注意

定期的に鍵をローテーションするには、新しい鍵を発行して新規に統合されたバケットを作成し、オブジェクトをコピーするなどの運用が必要です。
https://cloud.ibm.com/docs/services/cloud-object-storage?topic=cloud-object-storage-encryption

「Archive Rule」「Expiration Rule」によるライフサイクル管理

アクセス頻度が極端に少ないあるいは長期保管が必要なデータは「Archive Rule」で、より低価格な保管を実現できます。
従来のデータ管理でいうと、テープアーカイブに近いイメージでご利用いただけます。
「Expiration Rule」で不要なデータの期限を設定し、削除を事前にスケジュールしておくことで、コストを最適化できます。
「Archive Rule」と「Expiration Rule」と組み合わせることでポリシーベースのライフサイクル管理が可能です。



● Archive Rule
- バケットに保存されてから経過日数に応じて自動で安価なアーカイブに移行する機能
- 0日と設定することで即時アーカイブも可能（最大10年に設定可能）
- 指定した期間中、オブジェクトのコピーがストレージクラスに復元できます。復元時間は必要に応じて延長できます。（最大10年に設定可能）

● Expiration Rule
- バケットに保存されてから経過日数に応じて、または特定の日付を指定してオブジェクトを削除する機能（最大10年に設定可能）
- prefix を使ってフィルタリングをかけることで特定の対象オブジェクトに絞ることができます。
- オブジェクトごとの適用ルール・削除日はヘッダの「x-amz-expiration」で確認できます。

取扱注意
アーカイブの最低保管期間は、90日です。
アーカイブの復元には最大12 時間かかる場合があります。
復元期間中は、ストレージクラス内の復元済みコピーと
アーカイブ済みオブジェクトの両方に対して料金がかかります。

取扱注意
「Expiration Rule」は反映に最大1日かかります。

IBM Cloud Object Storage (ICOS) の Expiration Rule 詳細 https://qiita.com/khayama/items/ea898d2ca2ab97b76fd9

Retention (保存) Policy によるImmutable (不変) データ

追加費用なしで、一定期間データの変更または削除の防止を実現できます。
例えば、訴訟、監査、司法調査には「関連した全ての資料・情報をそのままの状態で安全に保存する」ことが必要です。
また、金融、ヘルスケア、メディアアーカイブ、政府など、特権的な変更または削除を防ぐための規制要件を満たせます。

● Retention (保存) Policy
- バケット単位で、最小/最大/デフォルトの保護期間を設定可能
- オブジェクト単位で適用する保護期間を最小から最大の間で設定可能（必要に応じて延長可能）
- オブジェクト単位で一時的なリーガルホールドフラグを設定可能
- 保護期間切れ、かつ全リーガルホールド削除時に、オブジェクトを削除/上書き可能（それ以外は、削除/上書き不可）
- バケットは、全オブジェクト削除後にのみ削除可能
- Permanent Retention を有効にすることで、永久的な保護が可能（永久に削除不可）

取扱注意
Retention (保存) Policy が有効なバケットでは、Aspera, Key Protect, Mass Data Migration サービスはサポートされません。
ライト（無料）プランのICOS では、Retention (保存) Policy がサポートされません。

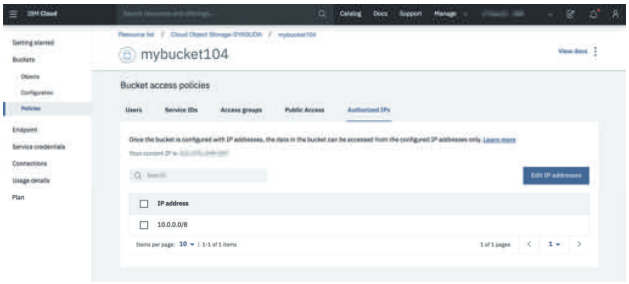
IP Firewall

追加費用なしで、指定したIPアドレスからのみICOSへアクセスを許可することが可能です。

主な特徴

- whitelist 方式（指定したIP subnetからのアクセスのみを許し、それ以外からのアクセスは禁じる）。
- ICOS Firewallの設定がない場合は、全てのsubnetからのアクセスを許可
- IPv4/IPv6に対応
- bucketごとのルール指定
- 無償
- 設定にはIAMのManager権限が必要

Private NW（10.0.0.0/8）からしかアクセスさせないように構成した例



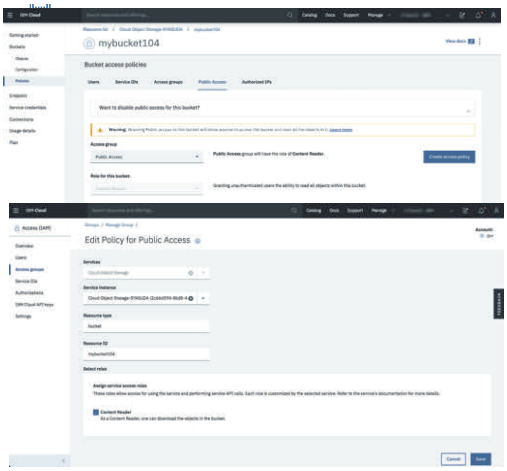
https://cloud.ibm.com/docs/services/cloud-object-storage?topic=cloud-object-storage-setting-a-firewall#setting-a-firewall
https://qiita.com/testnin2/items/0d23bb5b46f32e45eeb3
https://www.youtube.com/watch?v=83mn7fTNGxw

パブリック・アクセス

認証なしでICOSにアクセスが可能になります。

主な特徴

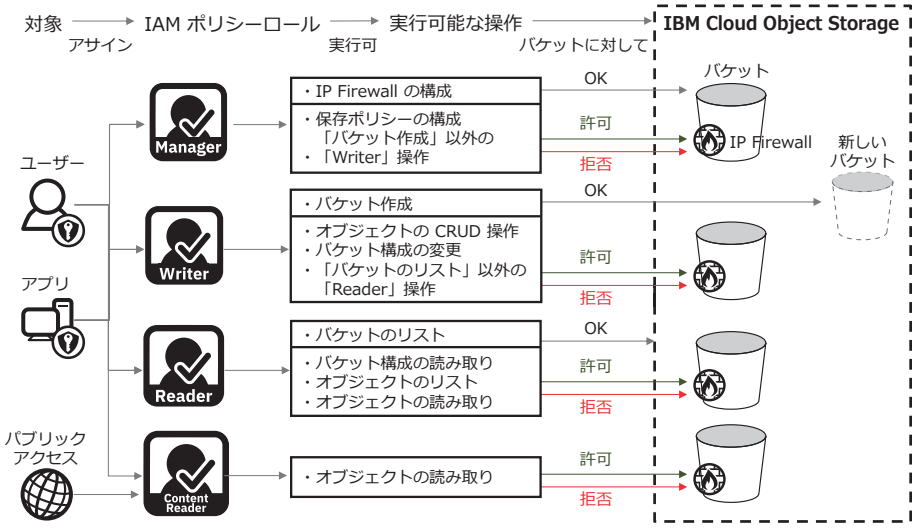
- ICOSにアクセスするにはデフォルトでは必ず認証が必要になるが、この設定をすることで認証なしにアクセスすることが可能。
- IAMの"Content Reader"権限を利用。
- バケット単位、オブジェクト単位で設定が可能。
- 静的Webホスティングなどに利用可能。
- ICOS Firewallと組み合わせると、特定のIPからのアクセスにのみ認証なしでアクセスさせるといった使い方も可能。



https://cloud.ibm.com/docs/services/cloud-object-storage?topic=cloud-object-storage-iam-public-access
https://qiita.com/testnin2/items/6379e5bc5ea165212e15
https://www.youtube.com/watch?v=HP2m3lnRbmg

Access Policyによるきめ細やかな権限設定

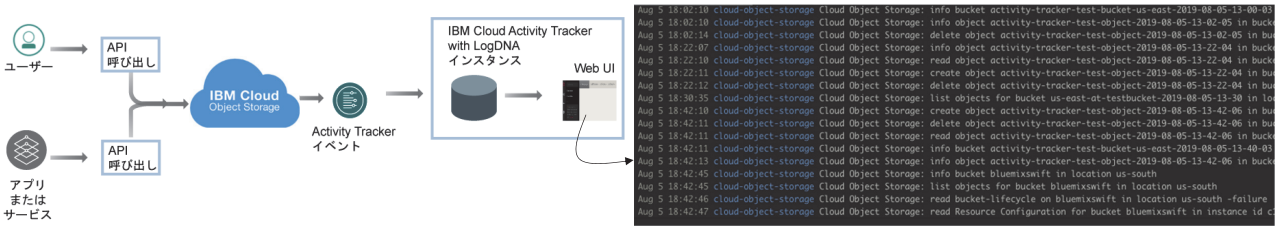
バケットレベルでアクセスポリシーを設定し、権限/ロールを割り当て、ユーザー/アプリの実効可能な操作を制御できます。



IBM Cloud Object Storage (ICOS) のデータをパブリックに公開する https://www.youtube.com/watch?v=HP2m3lnRbmg
IBM Cloud Object Storage (ICOS) に IP Firewall を設定する https://www.youtube.com/watch?v=83mn7fTNGxw

Activity Tracker with LogDNA への監査ログ保管

バケットの作成、オブジェクトのリスト、オブジェクトのアップロードなどの監査ログを保管できます。
データに対して誰が、いつ、何をしたかについての情報収集とトラッキングを行うことができます。



イベントタイプ	対象操作	備考
グローバルイベント	• すべてのバケットをリスト表示 • バケットの作成 • バケットの削除	• フランクフルトにある Activity Tracker with LogDNA に保管 • グローバルイベントを保管するには Activity Tracker with LogDNA を フランクフルトに作成する必要がある
管理イベント	バケットまたはオブジェクトに対する管理操作 • CORS 設定の作成 • Archive Rule、Retention Policy の作成 • バケットのリソース設定 API の操作など	• バケットごとに設定された Activity Tracker with LogDNA に保管 • バケットごとに Activity Tracker with LogDNA を設定するとき、 • UI では、バケットと同一もしくは最寄りのロケーションが自動で割当 • API では、任意のロケーションを割当可能
データイベント	バケットまたはオブジェクトに対するデータ読み書き操作 • オブジェクトのリスト表示 • オブジェクトの読み取り • オブジェクトの作成 • オブジェクトの削除　など	• 管理イベントと同一ロケーションの Activity Tracker with LogDNA に保管 • 以下の対象に設定するオプションが選択可能 　• 読み取りのみ 　• 書き込みのみ 　• 読み取り & 書き込み

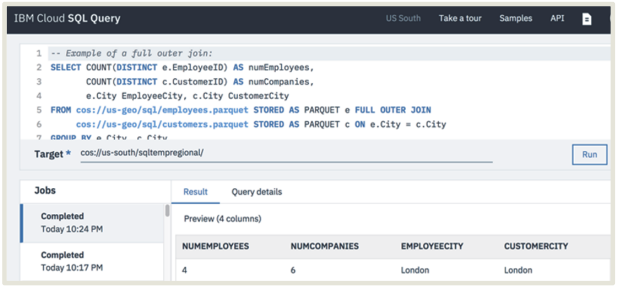
https://www.ibm.com/cloud/blog/announcements/ibm-cloud-activity-tracker-with-logdna-for-ibm-cloud-object-storage

SQL Query によるサーバーレスなデータ分析

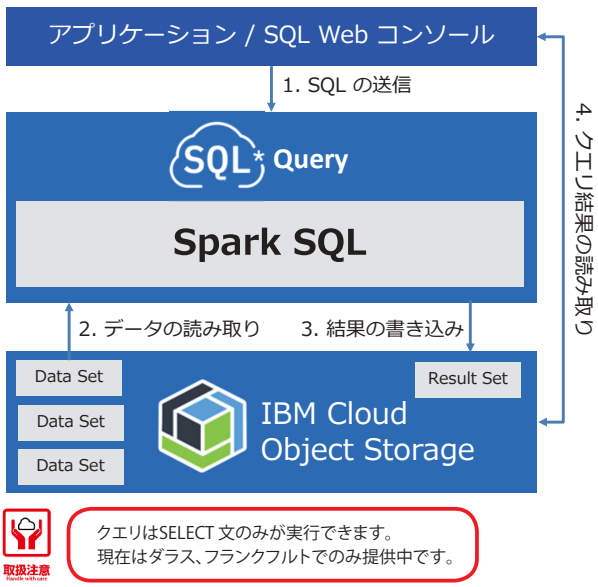
ICOS とSQL Query を使うことで、データ保管から分析までを、サーバーレスで迅速かつ簡単に実現できます。
また、分析済みのデータはWatson Studio を使って、ビジュアライズするといった連携も可能です。

主な特長:

- セットアップ不要なサーバーレス
- データの場所を問わずクエリで問い合わせが可能
- CSV / JSON / Parquet / ORC などの形式に対応
- 1日30GBまでのスキャンが無料なライトプラン
- ICOS オブジェクトに対して一意なSQL URL



ICOS のデータを SQL Query で分析する
https://www.youtube.com/watch?v=bnpq-pyQixo



● 統合パートナーソリューションの幅広いエコシステム

サポートするツール群の中から、よく使われる代表的なツールを列挙します。

https://www.ibm.com/jp-ja/cloud/object-storage/backup-and-recovery
https://www.ibm.com/jp-ja/cloud/object-storage/data-archiving

提供元	製品名	カテゴリ	参考リンク
Actifio	ActifioGO	バックアップ	https://www.actifio.com/solutions/cloud/ibm/
Actifio	SKY	バックアップ	https://www.actifio.com/press-releases/actifio-accelerates-data-revolution-cloud-centric-sky-platform-8-0/
Cloudberry	Cloudberrry Explorer Pro	ファイルシェア	https://cloud.ibm.com/docs/services/cloud-object-storage?topic=cloud-object-storage-cloudberry
CommVault	CommVault Simpana	バックアップ	https://cloud.ibm.com/docs/services/cloud-object-storage?topic=cloud-object-storage-commvault
Ctera	Ctera EFS Platform	ファイルシェア	https://www.ibm.com/downloads/cas/MK3KZA2G
DELL EMC	Data Domain	バックアップ	https://corporate.delltechnologies.com/en-us/newsroom/announcements/2019/02/20190205-01.htm
IBM	Spectrum Protect	バックアップ	https://www-01.ibm.com/support/docview.wss?uid=swg22000915
IBM	Spectrum Protect Plus	バックアップ	https://developer.ibm.com/recipes/tutorials/how-to-configure-ibm-spectrum-protect-plus-to-offload-to-ibm-cloud-object-storage/
IBM	DS8000 Transparent Cloud Tiering	ティアリング	https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.idak100/cloud23.htm
IBM	Aspera	ファイル転送	http://download.asperasoft.com/download/docs/entsrv/3.7.4/cs_admin_linux/webhelp/trap_external/dita/cleversafe_cli.html
IBM	IBM Cloud Tape Connector for z/OS	バックアップ	https://www.ibm.com/jp-ja/marketplace/cloud-tape-connector-for-zos/details
IBM	Spectrum Scale Transparent Cloud Tiering	ティアリング	https://www.ibm.com/developerworks/community/wikis/home?lang=ja#!/wiki/General%20Parallel%20File%20System%20(GPFS)/page/Transparent%20Cloud%20Tiering
Nasuni	Nasuni Cloud File Services	ファイルシェア	https://www.nasuni.com/partner/ibm/
NetApp	AltaVault	バックアップ	https://www.ibm.com/downloads/cas/QMJDMZJV
NetApp	FabricPool	ティアリング	https://docs.netapp.com/ontap-9/index.jsp?topic=%2Fcom.netapp.doc.dot-cm-psmg%2FGUID-622AB62B-5880-483E-94B9-D8A75E2DD59D.html
Oracle	RMAN	バックアップ	https://www.ibm.com/downloads/cas/OOBZVBPN
Panzura	Panzura Freedom NAS	ファイルシェア	https://panzura.com/partners/ibm/
R1soft	Server Backup Manager	バックアップ	http://wiki.r1soft.com/display/ServerBackupManager/Offsite+Backup+and+Archival
Rubrik	Rubrik Cloud Data Management	バックアップ	https://www.rubrik.com/ja/partners/technology-partners/
Veeam	Veeam Backup and Replication	バックアップ	https://www.veeam.com/jp/ibm-storage-solutions.html
Veritas	Netbackup	バックアップ	https://www.ibm.com/downloads/cas/LVQGYAKP

4-8. データ移行

● データ転送ソリューション選択の目安

データ転送方法を選択する場合の2つの主要な決定要因は、
転送されるデータ容量とその転送がどのくらいのスピードで行われる必要があるかです。

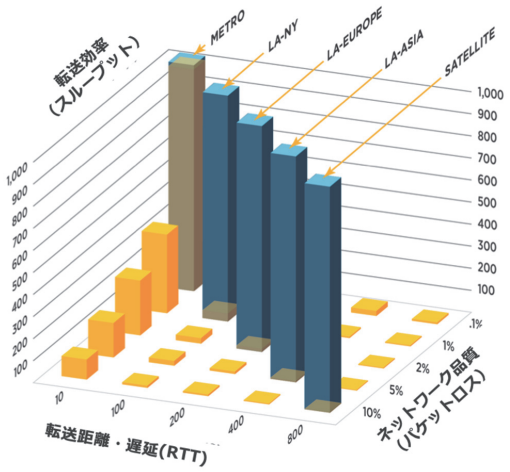
	10Mbps	50Mbps	100Mbps	500Mbps	1Gbps	10Gbps
100GB	24 hr	4.7 hr	2.4 hr	0.5 hr	0.25 hr	0.03 hr
1TB	240 hr	48 hr	24 hr	5 hr	2.4 hr	0.25 hr
5TB	1,224 hr	240 hr	122.4 hr	24 hr	12 hr	1.2 hr
10TB	2,472 hr	480 hr	240 hr	50.4 hr	24 hr	2.4 hr
50TB	12,336 hr	2,424 hr	1,224 hr	240 hr	120 hr	12 hr
100TB	24,672 hr	4,848 hr	2,472 hr	504 hr	240 hr	24 hr
1PB	246,720 hr	48,480 hr	24,720 hr	5,040 hr	2,400 hr	240 hr

Aspera 対象
Data Transfer Service 対象
Mass Data Migration 対象

Network transfer times in a Coast-to-Coast scenario (90msec delay, 1% packet loss)

IBM Aspera (IBM Software)

特許技術FASP によりFTP やHTTPに比べて数十～百倍の高速化を実現します。
ICOS にビルトインされて提供する機能に加えて、別途ソフトウェアとしてもご購入いただけます。



(1) 基本コンポーネント：クライアント製品	
Aspera Point-to-Point	サーバー製品不要の二拠点間高速ファイル転送ツール（1:1 型）
Aspera Desktop Client	FASP による高速ファイル転送を実施する転送クライアント
Aspera Connect web plugin	無料で提供される Web ブラウザー・プラグイン
(2) 基本コンポーネント：サーバー製品	
Aspera Enterprise Server	汎用ファイル転送サーバー（1:N 型）
(3) サーバー製品に Web インターフェイスを提供	
Aspera Connect for Web Access	汎用ファイル転送サーバーに Web インターフェイスを追加
(4) 個人間でのファイル交換、メールの操作性で社内外と大容量ファイルを転送	
Aspera Faspex Application	個人間や業務プロジェクトベースでのファイル交換
(5) グローバルにまたがる複数ノード間で統合的なファイル共有を実現	
Aspera Shares Application	Web インターフェイスを用いた高速ファイル共有
(6) ファイル同期・レプリケーション	
Aspera Sync Application	Enterprise Server や Point-to-Point に同期やレプリカ機能を追加
(7) アプリケーションとの連携や、独自の埋め込みクライアント機能を開発可能	
Aspera SDK	クロスプラットフォームに対応するライブラリー・API を提供
(8) インターネットを介したセキュアーなネットワーク構成に対応可能	
Aspera fasp Proxy	FASP 対応プロキシー・サーバー
(9) Aspera ネットワーク全体のファイル転送管理・監視・制御をブラウザから集中管理	
Aspera Console	Aspera ファイル転送業務全体を集中管理、モニタリング、制御

IBM Data Transfer Service (DTS)

少量のデータ(10 TB 以下) をIBM Cloud に迅速かつ効率的に転送し、使用可能な帯域幅が限られているお客様に最適です。

プロセス:

・USB 対応デバイス/ CD / DVD などをIBM Cloud DC に発送して、ネットワークに直接接続して、高速データ転送を遠隔制御できます。（お客様自身によるハンドデリバリーにも対応可能です。）

特長:

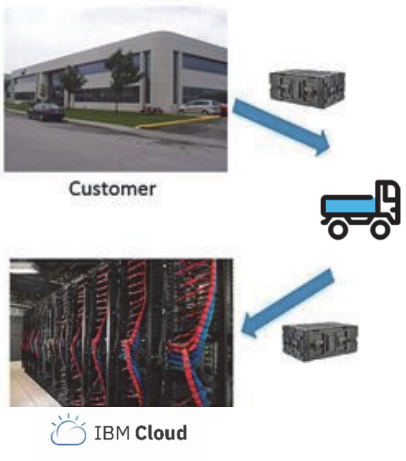
・受領したお客様デバイスは、IBM Cloud 内のDTS ラックに格納され、iSCSI ターゲットとしてマウントされます。

価格:

・サービス料金：無料
・送料：国別に異なる（日本では、ヤマト運輸などの配送料に従う）
・使用方法: 2 週間無料。以降1 週間ごとに延長料金として25 ドル

提供エリア:

・世界中のすべてのIBM Cloud データセンターで利用可能です。

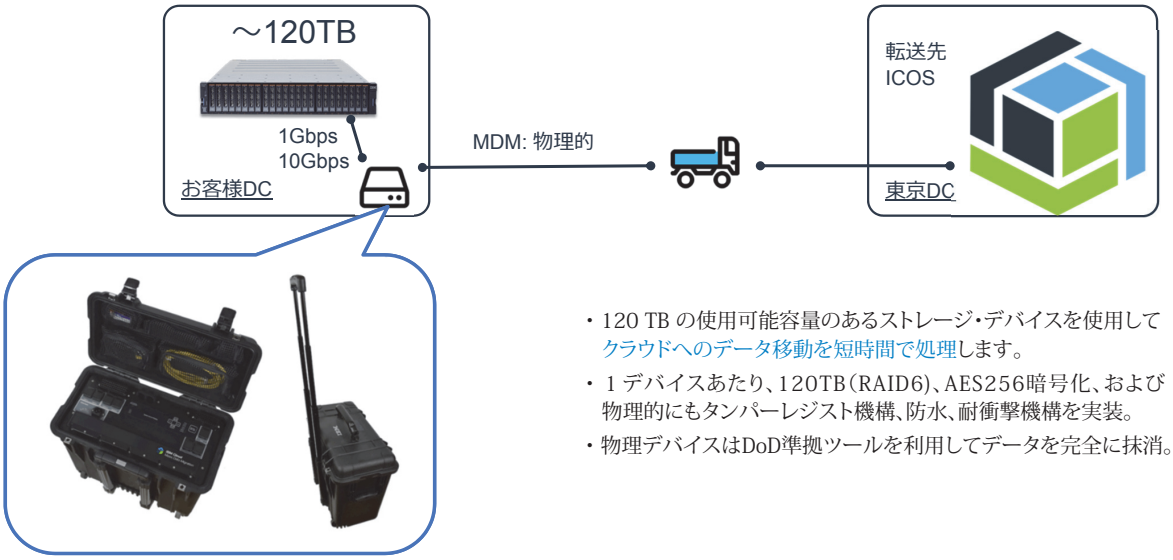


取扱注意

アカウント管理者のみがDTS を申請可能です。重要なデータを輸送される場合は、セキュリティ配送サービスなどをご利用ください。
データ転送速度の理論上限値は、USB 3.0 の4.8 Gbps ですが、実効速度は利用するファイル転送プロトコルによって異なります。

Mass Data Migration (MDM) を利用したデータの物理輸送

テラバイト～ペタバイト級のデータをIBM Cloud Object Storage に安全に移動することができます。
大量データ移行における、高いネットワークコスト、長い転送時間、セキュリティ上の問題などの課題を克服できます。



- 120 TB の使用可能容量のあるストレージ・デバイスを使用してクラウドへのデータ移動を短時間で処理します。
- 1 デバイスあたり、120TB（RAID6）、AES256暗号化、および物理的にもタンパーレジスト機構、防水、耐衝撃機構を実装。
- 物理デバイスはDoD準拠ツールを利用してデータを完全に抹消。

https://cloud.ibm.com/docs/infrastructure/mass-data-migration?topic=mass-data-migration-getting-started-tutorial#ibm-cloud-

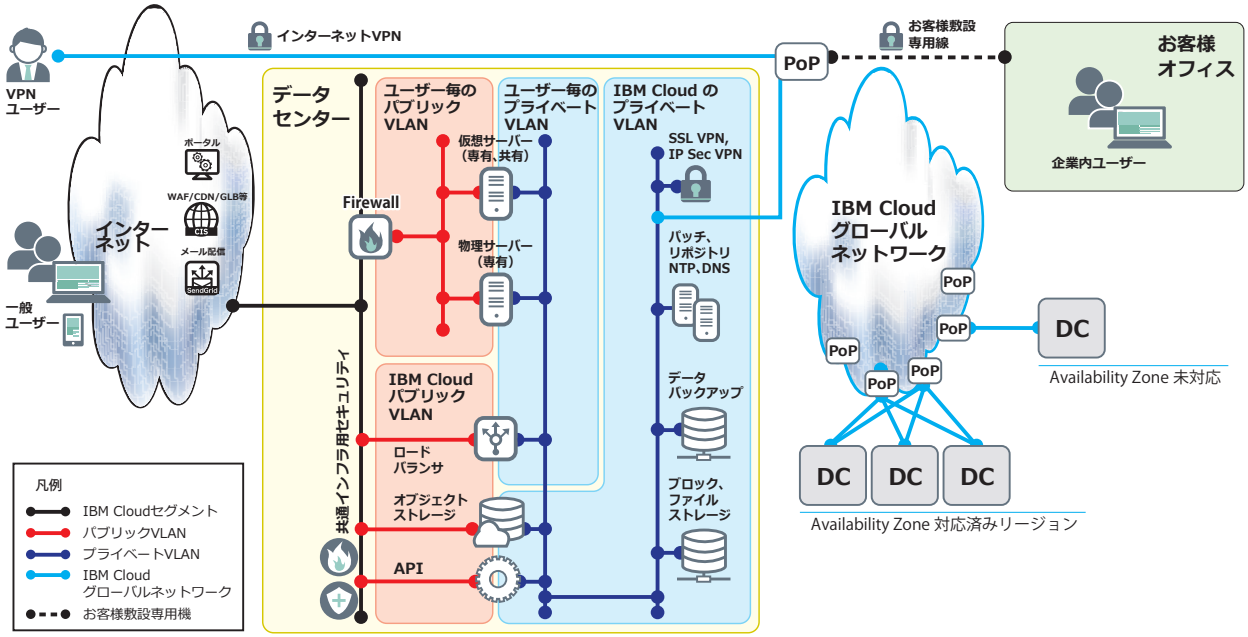
5

ネットワーク

INDEX

5-1. ネットワーク概要

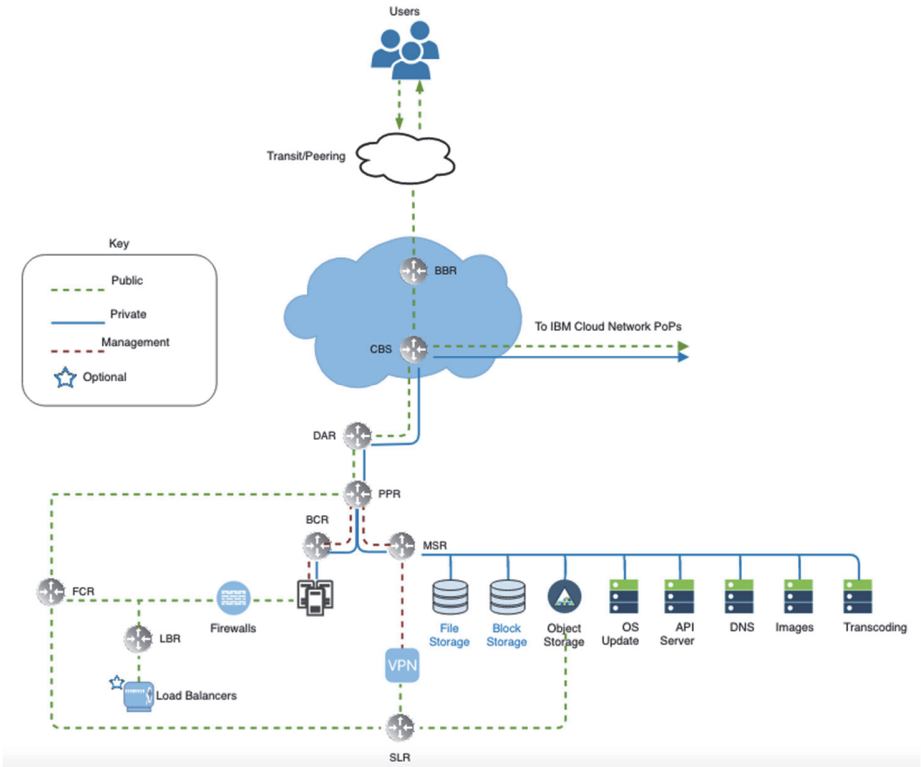
本章では、IBM Cloudにおけるネットワーク関連のサービスについて記載しています。



IBM Cloudネットワークを物理的な観点で表した図です。

https://cloud.ibm.com/docs/services/vmwaresolutions/services?topic=vmware-solutions-design_physicalinfrastructure&locale=en

Reference :
BBR = BackBone Router
CBS = Core Backbone Switch
DAR = Datacenter Aggregation Router
PPR = Pod-to-Pod Router
FCR = Frontend Customer Router
LBR = Load Balancer Router
BCR = Backend Customer Router
MSR = Master Services Router
SLR = SoftLayer Router



取扱注意

IBM Cloud 提供の各種サービスを利用するためには、Private NW側への通信として10.0.0.0/8、161.26.0.0/16、166.8.0.0/14 への通信が行える必要があります。FirewallでPrivate側の通信を制御する際は、各サーバーから上記の経路への通信は許可するようにしておきましょう。

サーバーのポートスピード

・仮想サーバー

- Port Speed: 10Mbps, 100Mbps, 1Gbps
- 仮想サーバーが稼働する物理ハードウェアのネットワークは冗長化されています。
- 専有仮想サーバー(Dedicated Host)の場合、1Gbpsを選択してもそれ以上の性能を出せる場合があります。

https://www.ibm.com/cloud/blog/achieving-10-gbps-network-throughput-on-dedicated-host-instances

・物理サーバー

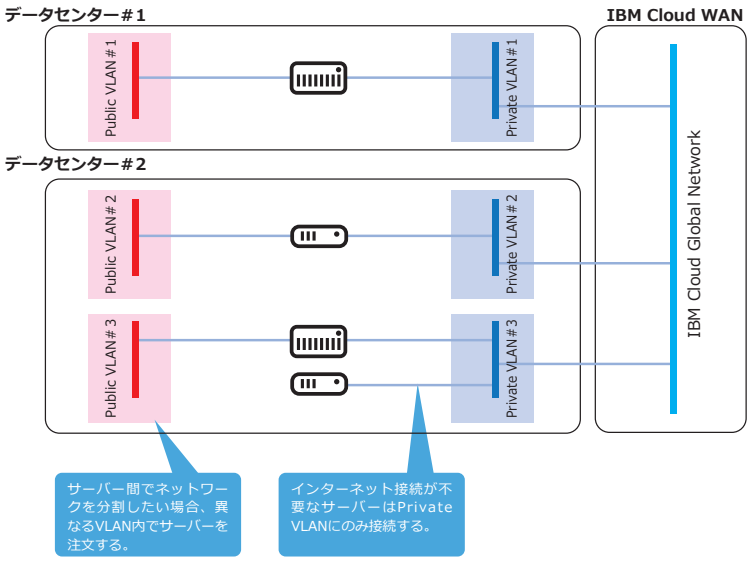
- Port Speed: 100Mbps, 100Mbps x2, 1Gbps, 1Gbps x2, 10Gbps, 10Gbps x2
- x2 の場合、オプションで、ネットワークポートの冗長(Redundant)、独立(Dual)を選択できます。

サーバーのネットワークスループットや使用量

・仮想サーバー

- カスタマーポータルからグラフを使って確認が可能です。パケットロスなどのネットワークエラーに関しては、個別に構築したVRA(Virtual Router Appliance) などの機能を通して確認することが可能です。

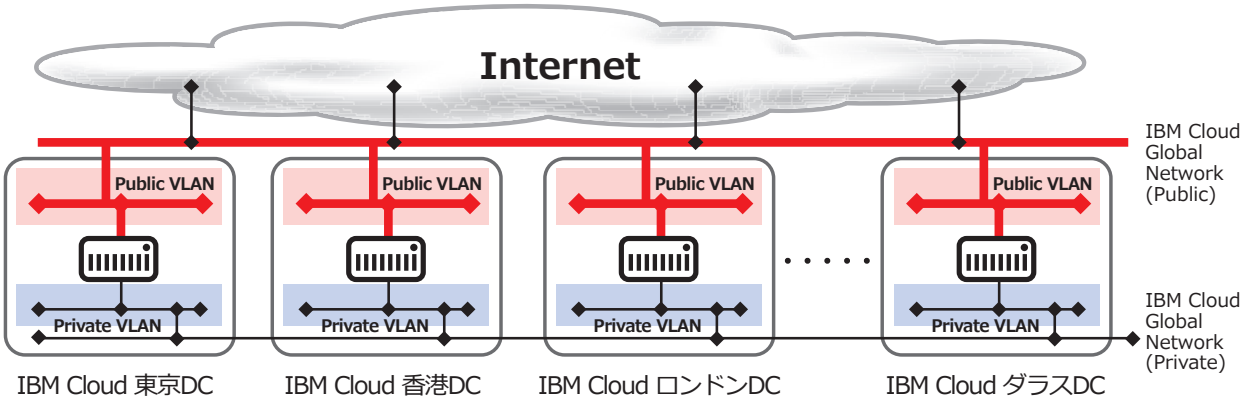
IBM Cloudでは、VLAN (Virtual LAN)を使用してネットワークを論理的に分割しています。
IBM Cloudのサーバーは、デフォルトでPublic VLANとPrivate VLANの両方に所属します。
必要に応じてPrivate VLANにのみ接続する構成とし、セキュリティリスクの低減をはかることもできます。



- VLANとは、ブロードキャストドメインの分割を行う技術です。
- 例えば、あるサーバーが同一ネットワーク内の別のサーバーと通信するためにはMACアドレスを知る必要がありますが、そのためにはブロードキャスト通信を利用します。VLANが分かれているサーバーには、ブロードキャスト通信は届きません。
- VLANが分割されていることにより、無駄なトラフィックが減り、必要のないサーバーとの間にブロードキャストが転送されないため、セキュリティーも向上します。

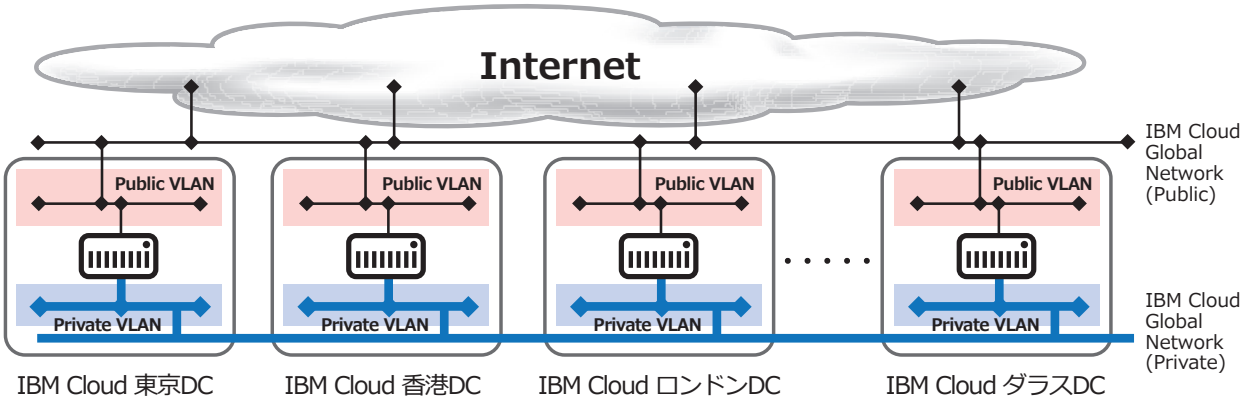
Public VLAN

・サーバに対してインターネット側の接続を提供します。
・サーバーをパブリック側ネットワークポートを付けてオーダーすると、インターネットからアクセス可能なパブリックIPアドレスが付与されます。
・オーダーには対応する権限（パブリック側ネットワークポート付きでサーバーをオーダーできる権限）が必要です。
・1つのデータセンターにおいて複数の通信キャリアと回線契約しています。
・社内システムからのみ使う場合、パブリック側ネットワークポートを付与しない構成も可能です。
・インターネットからのアクセスを受け付けるので、セキュリティには十分配慮し、ファイアウォールやロードバランサでアクセス制御を行うことを考慮してください。
・同一DC内間の通信の場合、異なるアカウント間のサーバーであっても、DC内での折り返しで通信します。
・異なるDC間の通信の場合、異なるアカウント間のサーバーであっても、インターネットに出ることなく通信します（同一AS内通信）。



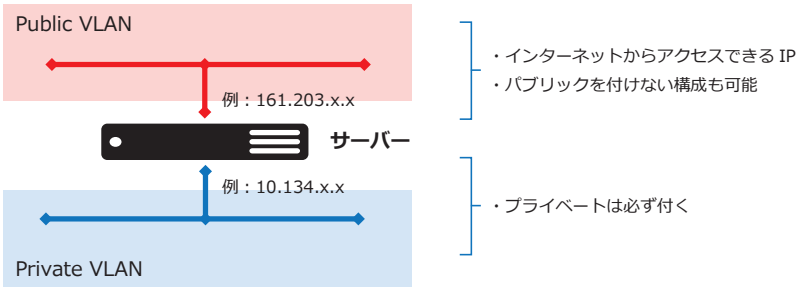
Private VLAN

・IBM Cloud全体で1つの大きなプライベートネットワークが存在しており、ユーザにはその一部が割り当てられます。
・異なるアカウントのプライベートVLAN同士は通信できないよう、分離されています。
・同一アカウントの場合、世界中のデータセンターのどこでサーバを購入してもプライベート経由で通信可能です。
（後述のVLANスパニングオプションを有効にする必要があります）
・プライベートネットワークを介したデータセンター間の通信は無料です。
・お客様はインターネットVPNや専用線を介して、プライベート・ネットワークにアクセス可能です。
・IBM Cloudが提供するEndurance Storage等のストレージ・DNS・NTP・パッチサーバー等は、IBM Cloud管理のプライベートネットワーク上に存在します。



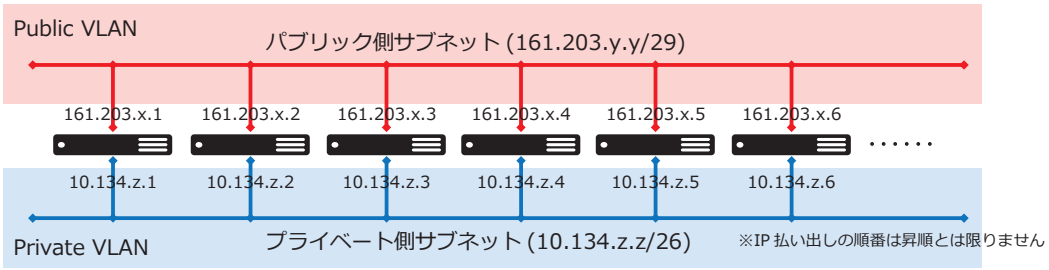
IPアドレス

・IBM Cloudでサーバーをオーダーすると、サーバーはネットワークに接続された状態で提供され、IPアドレスを持ちます。



IPアドレスとサブネット

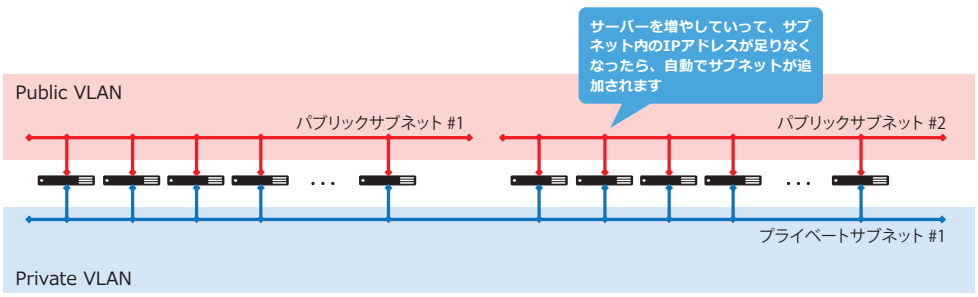
・IPアドレスは、ユーザーごとに割り当てられたサブネットの中から払い出されます。



・サーバの購入台数にかかわらず(たとえ1台しか持っていなくても)、サブネット単位でユーザーに割り当てられます。
・例えば、161.203.x.x/29（8アドレス）、10.134.x.x/26（64アドレス）等の形式で払いだされます。
・サブネットの中の未使用のIPアドレスはそのユーザーの将来のサーバー用に予約された状態です

サブネットとVLAN

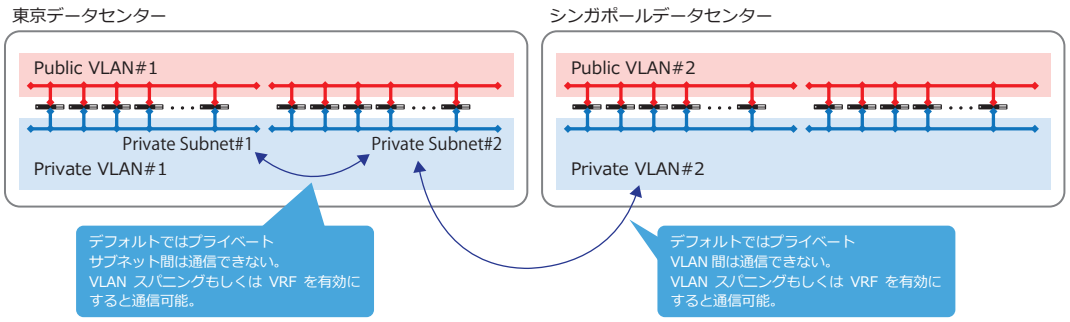
・サブネットは、VLANに属します（１つのVLAN内に複数のサブネットが存在する事もあります）
・VLANも、ユーザーごとに割り当てられるネットワークリソースです。
・VLANを追加したい場合、管理ポータルからオーダーを行います。
（PoD内のVLANに余剰が無く、指定したPoDにVLANを追加できない場合もあります）



https://cloud.ibm.com/docs/infrastructure/vlans?topic=vlans-getting-started-with-vlans&locale=ja

VLANスパニング/VRF

・同じユーザー（同じアカウントID配下のユーザー）でも、異なるプライベートVLANやプライベートサブネット間は、
　デフォルトでは通信できません。
・「VLANスパニング」もしくは「VRF」を有効にすることでVLAN間が通信可能になります。
・異なるアカウントID同士のプライベートVLANを接続することはできません。



取扱注意
Handle with care

VLANスパニングとVRF方式は、一見その効果は同じように見えますが、その実装方法と今後の機能拡張について違いがあります。VLANスパニング方式は内部的にはNetwork ACLによって実装されており、実装上のスケーラビリティーがないため、IBM Cloudのサービスが新規に実装される際には利用されなくなっています。既に、Direct Link、Cloud Service Endpoints、VPC、VMware Solutionsなどを利用する際にはVRFを有効にすることが前提になっています。これらの機能はVLANスパニング環境下ではサポートされません。VRFを有効にする際には短時間ですがNW通信が遮断されるため、これらのサービスを利用する予定がある場合は、アカウント作成後に余裕をもってVRFを有効にすることを推奨します。Caseを起票することでVRFを有効化できますが、ibmcloudコマンドからVRFを有効にするCaseを起票することも可能です。
https://qiita.com/testnin2/items/b3f3a112cb21ad8c07e9

IPアドレスの種類

IBM Cloudで利用できるIPアドレスは、パブリックIPとプライベートIPに分かれています。
オプションで、利用するIPアドレスの種類を選択することができます。
IPv4、IPv6を利用することができます。

【IPアドレスとVLAN】

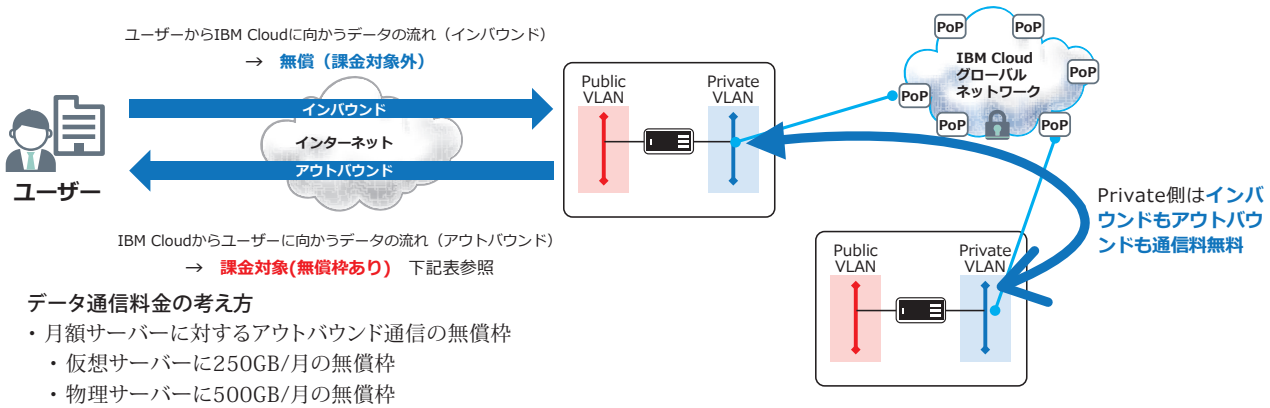
・IBM Cloudのサーバーは、デフォルトでPublic VLANとPrivate VLANの両方に所属する。
　・Public VLANに所属しない構成も可能。Private VLANには必ず所属する。
・VLANに所属するデバイスには、以下のIPアドレスが1つ割り当てられる。
　・Public IP　：インターネットを経由してアクセスできるGlobal IPアドレス
　・Private IP　：10.xのPrivate IPアドレス
・VLANは追加することができる。(チケットによる申請と承認が必要)
・1つのVLANに複数のセグメント（サブネット）を追加することができる。
・1つのセグメントには、Public側は最大32個(/27)、Private側は最大64個(/26)のIPアドレスを持たせることができる。

【4種類のIPアドレス】

・Primary：　サーバー注文時に付与されるIPアドレス
・Static　：　特定のIPアドレスに紐付けて、そこにルーティングさせるためのIPアドレス
・Portable：　VLAN内で任意に使い回す事が可能なIPアドレス
・Global　：　異なるDC間でも紐付けの変更が可能なIPアドレス

● 課金

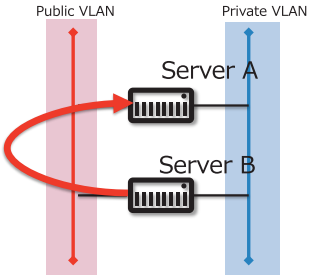
各サーバー毎に、Publicネットワークポートに対するアウトバウンド通信に課金が発生。



データ通信料金の考え方

- 月額サーバーに対するアウトバウンド通信の無償枠
  - 仮想サーバーに250GB/月の無償枠
  - 物理サーバーに500GB/月の無償枠
- Virtual Router Applianceに20TB/月の無償枠
- 無償枠を超過した分はアウトバウンド通信は従量課金
- 事前購入（Pre-purchase）では割安に通信枠を事前購入可能
- 月額タイプサーバーが持つ無料枠は、オプションにより他サーバーと共有可能（Bandwidth Pooling）
- Private Networkによる通信は、どれだけ使っても無料(他DCとのデータ通信も無料)

- アンチデザイン
  - **Publicネットワークポート**に対するアウトバウンド通信に課金が発生するため、Public VLAN経由でノード間通信をすることで、同じデータセンター内でも無料枠を超えると課金されてしまう。
- 望ましい方式
  - 可能な限りPrivate Port経由で通信する。
  - IBM CloudはPrivate NW通信は無料。



取扱注意
Handle with care

Server Aにとっては、inbound(中に入ってくる通信）なので課金なし。
Server Bにとっては、outbound(外に出て行く通信）なので**課金対象**。

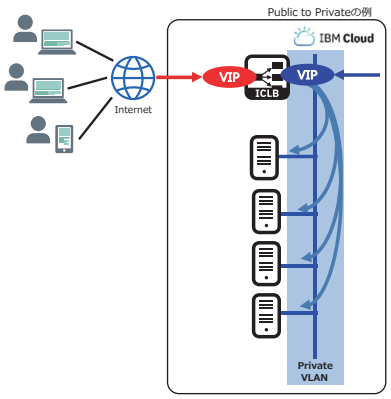
5-2. ロードバランサー

IBM Cloudから提供される負荷分散機器（ロードバランサー）は、以下になります。
ロードバランシングだけでなく、WAF（Web Application Firewall）や、データセンター間の負荷分散機能を備えたロードバランサー等が選択可能です。

	LVS, Nginx などのOSS	IBM Cloud Load Balancer (従量型)	Citrix NetScaler VPX / MPX	NSX Edge on VMware on IBM Cloud	F5 on VMware on IBM Cloud	IBM Cloud Internet Services
概要	利用者が持ち込むロードバランサ	IBM Cloudのマネージドロードバランサー	ベンダー製品によるロードバランサー。仮想専有(VPX)または専用物理アプライアンス(MPX)あり。	VMwareソリューション(VCS)付属のNSXで追加コスト無しで利用可能	ベンダー製品によるロードバランサー。VMwareソリューション(VCS)のオプションとして選択。	Cloudflareによるマネージドロードバランサー
マルチテナント・シングルテナント	サーバー構成に依存	マルチテナント	シングルテナント	シングルテナント	シングルテナント	マルチテナント
GSLB機能の有無	なし	なし	Platinum Editionのみ	なし	Better/Best Optionのみ	あり
共有・専有	専有	共有	専有	専有	専有	共有
VIP	Public/Private アドレス	Public/Private ドメイン名	Public/Private アドレス	Public/Private アドレス	Public/Private アドレス	Public ドメイン名
割り振り先	Public/Privateネットワーク (L4/L7)	Public/Privateネットワーク (L4, L7)	Public/Privateネットワーク (L4/L7)	Public/Privateネットワーク (L4/L7)	Public/Privateネットワーク (L4/L7)	Publicネットワーク(L4)
HA構成	可能	標準提供	可能	可能	標準提供	標準提供
SSLオフロード	OSSの機能に依存	可能	可能	可能	可能	可能
能力	サーバー性能に依存	400~500Mbps 最大同時接続15000程度 (参考値)	10Mbps ～1000Mbps（VPS） 1Gbps～10Gbps（MPX）	アプライアンスのサイジングに依存 (Compact/Large/Quad Large/X-Large)	25Mbps～5Gbps	–
その他特徴	-	従量課金	Platinum EditionでWAF、GSLBの機能が利用可能	Firewall機能やLoad Balancing機能はNSX Baseライセンスから利用可能。 https://cloud.ibm.com/docs/services/vmwaresolutions?topic=vmware-solutions-solution-appendix	Good/Better/Bestの3エディションから選択 Best EditionでWAF対応	GlobalLB、DDoS防御、WAF、コンテンツキャッシュ、DNSなど標準装備

IBM Cloud Load Balancer

IBM Cloud Load Balancerは、基本料金（時間課金）＋負荷分散したデータ量に応じた従量課金で利用できる
マネージドのロードバランサーです。



推奨情報 Osusume-desu

Public to Publicタイプを使えば、EOMになった Local Load Balancer配下のサーバー構成を変える事なくLBを置き換えられます。それ以外のケースでは、サーバーのパブリックアウトバウンド課金やセキュリティの観点から、Privateに振り分けるタイプのLBを選びましょう。

- 共有型
- Load BalancerのVIPと割り振り先のサーバーが所属するネットワークは3パターン。
  - Public to Private、Private to Private、Public to Public
- L4（HTTP、HTTPS、TCP）、L7
- プライベートネットワーク側への割り振りをサポートするため、割り振り先のサーバーがパブリックネットワークに足を出しておく必要がない。
- LB Methods:
  - ラウンドロビン(RR), Weighted RR, Least Connections
- 課金方式
  - 基本料金（時間課金）＋負荷分散したデータ量に応じた従量課金＋パブリックOutbound通信費用
  - パブリックOutbound通信費用は、1ヶ月あたり5GBまで無料（Private VIP の場合、非課金）
- SSLオフロード機能
- セッションパーシスタンス機能
- VIPはPublicまたはPrivateネットワーク上のFQDN
- パブリックVIPは、以下のどちらかを指定可能。
  - IBM Cloudが割り当てるプール
  - 利用者アカウントに割り当て済みのPublicサブネット(明示的にサブネットは指定不可)
- プライベートVIPは利用者アカウントに割り当て済みのPrivateサブネット
- VIPポートあたりの最大接続制限機能あり。
  - 1-15,000同時接続から選択可能。
  - ～500Mbps（参考値）
- 高可用性は標準提供
- 負荷に応じてロードバランサー自体が水平スケーリング（最小2台、最大16台）
- VLAN Spanning=ON またはVRF=ONの時にMZR対応（Load Balancerのインスタンス自体が複数ゾーンに分散配置）
- 管理ポータル・APIで操作・管理可能
  - APIにより、Portable IPや他リージョンのIPアドレスも割り振り先に指定可能（IBM Cloudが払い出していないBYOIPには割り振り不可）

NetScaler VPX/MPX

専有ロードバランサーとして、Citrix社のNetScaler VPXまたはMPXが利用できます。
上位のプラチナ・エディションでは、アプリケーションレベルでのファイアーウォールや、グローバルロードバランシング機能が利用できます。

NetScaler VPX

- 仮想アプライアンスとして仮想専有サーバー上で構成
- GUIでの操作が可能
- IBM Cloudのパブリック、プライベートネットワーク双方の環境に配置が可能
- レイヤー7までをサポート
- Global load balancing機能（Platinum Edition）
- 高可用性（オプション）
- 10 Mbps、200 Mbps、1 Gbps
- 1、2、4、8、16 パブリックIPアドレス

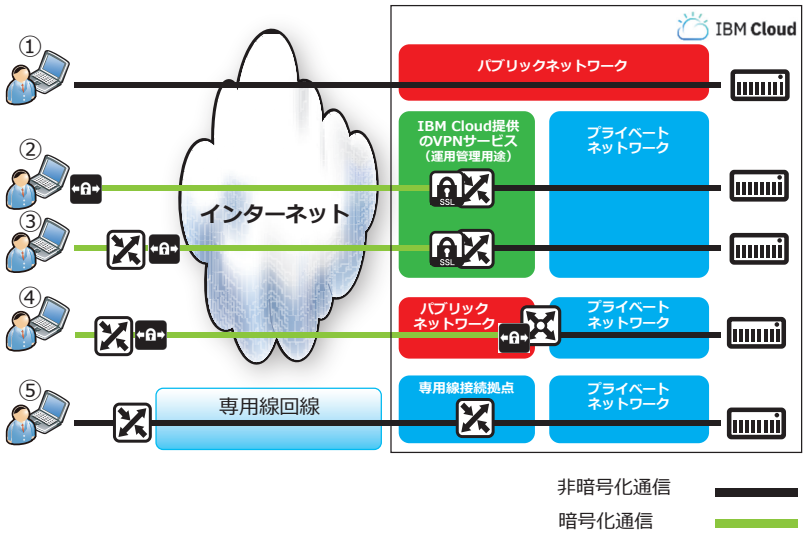
NetScaler VPX

- 機能はVPXと同じだが、MPXは専用物理アプライアンス上で構成
- 秒間10万接続以上を制御したいユーザー向け

Citrix NetScaler	
Standard Edition	**Platinum Edition**
• TCP buffering • TCP multiplexing • SSL offload and acceleration • Client and server TCP optimizations • L4 DoS defenses • Layer 7 content filtering • HTTP rewrite • URL rewrite • Citrix Access Gateway • Layer 4 load balancing • Layer 7 content switching • AppExpert rate controls • IPv6	• TCP buffering • TCP multiplexing • SSL offload and acceleration • Cache redirection • Client and server TCP optimizations • Citrix AppCompress for HTTP • Citrix AppCache • L4 DoS defenses • Layer 7 content filtering • HTTP rewrite • URL rewrite • Citrix Access Gateway • Layer 7 DoS defenses • NetScaler Application Firewall • Layer 4 load balancing • Layer 7 content switching • AppExpert rate controls • IPv6 • Global server load balancing • Surge protection • Priority queuing

5-3. 外部接続

IBM Cloudとの接続には、次の方法があります。
①インターネット接続。デフォルトでは暗号化されていないため、暗号化が必要な場合はSSHやHTTPSなどを利用。
②IBM Cloud提供のSSL VPN接続サービス。運用管理用途で提供されているため低速。
③IBM Cloud提供のIPsec VPN接続サービス。運用管理用途で提供されているため低速
④クラウド側に自前で専有のVPN環境を構築して接続。
⑤専用線接続（Direct Link）：閉塞網を利用してクラウドに接続



取扱注意
Handle with care

・オンプレミスとの接続は、接続方式によってはNATされます。アプリケーションによって、NAT越えをサポートしないものがあります。
・NAT超えをサポートしないアプリケーションとして、代表的なものではActive Directory（AD）があります。オンプレミスとIBMCloud上のADを連携する場合、GREやIPsec VPNなどでトンネルを張ったり、VMware NSXなどのSDN製品を活用してNATの影響を回避する方法が考えられます。

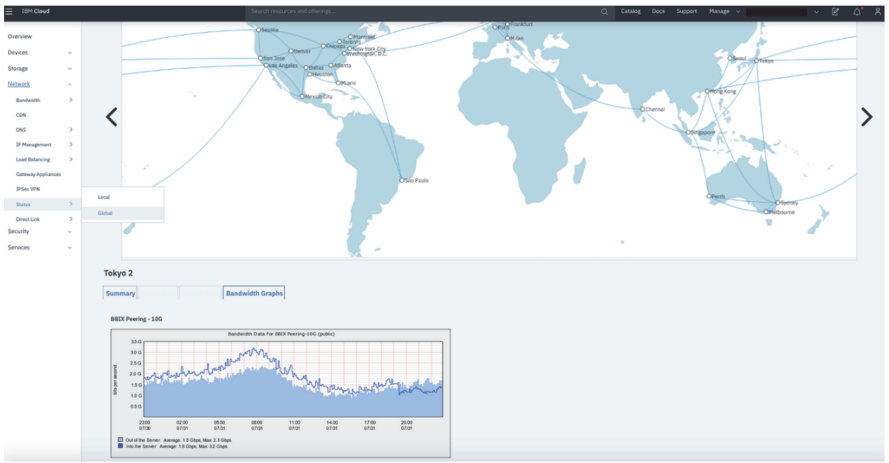
インターネット接続

https://www.ibm.com/cloud-computing/bluemix/ja/our-network

・IBM Cloudのデータセンターには、複数のインターネットキャリアが10Gbps x Nのインターネット回線を引き込んでいます。
東京データセンタには下記キャリアの回線が引き込まれています。
　・NTT/Pacnet/PCCW/Telstraは、Tier1キャリアと呼ばれ、世界中に数多く存在するインターネット接続キャリアの中でも、その規模において最上位に分類されるキャリアです。
　・これらのキャリア回線を通し、IBM Cloud上のサーバーは、広帯域のインターネット接続を行うことができます。
・IBM Cloudでは、各キャリアごとの回線の利用状況を管理ポータルから確認できます。

Public Network Status

BBIX Peering - 10G	Up
Equinix Peering - 20G	Up
JPNAP Peering - 10G	Up
NTT1 - 20G	Up
PCCW1 - 10G	Up
Pacnet1 - 10G	Up
Telstra1 - 10G	Up
Telstra2 - 10G	Up



インターネットVPN接続

接続方式名称	提供形態	VPN 種類	IBM Cloud 側で必要な準備	特徴
SSL VPN 接続サービス	・IBM Cloud が運用 ・無償	・リモート接続型 VPN ✓ SSL VPN	・VPN を利用するユーザーに対して、サービスの有効化	・クラウド内サーバーの保守・管理用を想定したサービスのため低速（数 MB/s 程度）（ファイル転送には向いていない） ・Outbound 課金が発生しない ・利用者の PC 端末から個別に接続
IPsec VPN 接続サービス	・IBM Cloud が運用 ・有償	・拠点間 VPN ✓ IPsec VPN	・IPsec VPN サービスの購入と設定	・クラウド内サーバーの保守・管理用を想定したサービスのため低速（ファイル転送には向いていない） ・Outbound 課金が発生しない ・お客様拠点の VPN ルータから接続 ・NAT 変換が必ず発生する
個別の VPN 環境の構築	・利用者が構築・運用	・拠点間 VPN ✓ IPsec VPN ✓ Open VPN ・リモート接続 VPN ✓ SSL VPN ✓ OpenVPN ✓ L2TP/IPsec ✓ NCP Exclusive Remote Access	・利用者が IBM Cloud 上に注文したサーバー上に VPN 環境を構築 ・IBM Cloud では以下のソフトウェアを提供しています。 ✓ Virtual Router Appliance(VRA) ✓ Juniper vSRX ✓ Fortigate ✓ NetScaler VPX ✓ VMware NSX ✓ F5 on VMware	・利用者が構築・運用を行う必要がある。 ・Outbound 課金が発生する ・vSRX では NCP Exclusive Remote Access を使ってリモート接続 VPN 可能。 同時接続２人までのライセンスが提供。

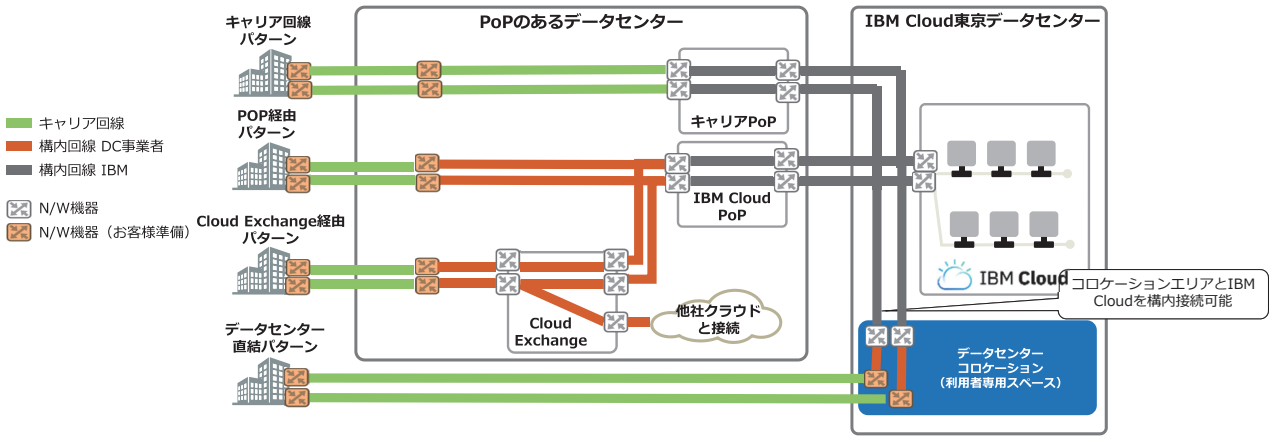
取扱注意 Handle with care

・SSL VPN接続サービスは、VRF ONのアカウントではVPN接続先と同じリージョンのサーバーのみアクセスできます。
・IPsec VPN接続サービスはVRF ONのアカウントでは利用できません。
https://cloud.ibm.com/docs/direct-link?topic=direct-link-overview-of-virtual-routing-and-forwarding-vrf-on-ibm-cloud&locale=en#benefits-of-moving-to-vrf

専用線接続

IBM Cloudより提供される専用線接続サービス（Direct Link）には以下の方法があります。

- PoPにおける専有のクロスコネクト経由で接続する方法（国内ではTOK01/TOK03/OSK01にPoPがあります）
- Exchange業者経由で接続する方法（他社クラウドにも接続可能。国内ではEquinix社のCloud Exchange、アット東京社のATBeXが利用可能）
- 東京データセンターに直結する方法（隣接している利用者専用スペースとIBM Cloudを構内配線で接続可能）
- キャリア回線を直接引き込む方法（NTTコミュニケーションズ、ソフトバンク、TOKAIコミュニケーションズ、Colt、PCCWなど、対応キャリアの回線を直接IBM Cloudに接続可能）

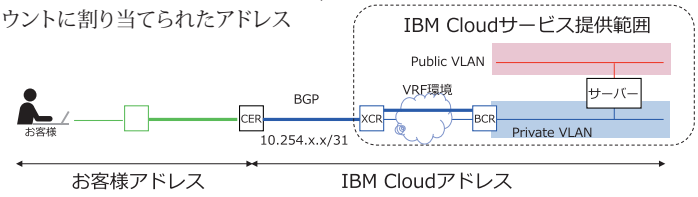


取扱注意 Handle with care

専用線接続を利用する際にはVRF(Virtual Routing and Forwarding)構成にすることが前提になります。
VRFへの移行によってVLAN間通信が暗黙的に許可されるようになることにご注意ください。

Direct Link技術詳細

- Direct Linkの接続用のお客様側ルーターをCER (Customer's Endpoint Router)、IBM Cloud側のルーターをXCR (Cross Connect Router)と呼びます。
- IBM Cloudからは、CERとXCR間のsubnet (10.254.x.x/31) が払い出されます。ルーターによって/31のsubnetが設定できない場合は、/30でリクエストしてください。
- XCR/BCR間にVRF環境が構成され、お客様ネットワークまでのルーティングが可能になります。
- CERとXCRの間にBGPセッションを構成します。
- CERからXCRへはお客様ネットワークへのルーティング情報を、XCRからCERへはIBM Cloudネットワークへのルーティング情報を、それぞれ広告します。
- CERからXCRへは、IBM Cloud側で予約する以下のアドレスへのルーティングを広告することはできません。
  - 10.0.0.0/14、10.200.0.0/14、10.198.0.0/15、169.254.0.0/16、224.0.0.0/4
  - Direct Link用のアドレス(10.254.0.0/16の中から/31または/30)
  - Private VLAN用にお客様アカウントに割り当てられたアドレス



XCR-CER間のBGPについてのFAQ

1. 使えるASの範囲は?
   IBM Cloud側のAS番号は13884です。これはpublic側、private側共通となります。また、広告する各ルートにAS PATH属性にIBM Cloud内部のprivate ASNの一部(65200～65235、65400～65435)を指定します。
   お客様側AS番号は、public AS番号(1～64495)もしくはprivate AS番号(64999)または4byte ASN (4201000000～4201064511)を指定してください。

2. IBM Cloud側から広告されるルートのsubnetの単位は?
   接続先アカウントに属するPrivae VLAN上のsubnetの単位で広告されます。10.132.a.0/26と10.132.b.128/26など、複数のsubnetを持っている場合、subnetの数だけルートが広告されます。

3. 利用できるattributeは?
   Well-known mandatoryとWell-known discretionaryがサポートされます。

4. 利用できるcapabilityは?
   以下のものが確認できています。利用不可のcapabilityを送ると単に無視します。
   Multi protocol Extensions Capability(address family IPv4 unicastのみ)
   Route-Refresh Capability
   4 Octets-AS Capability

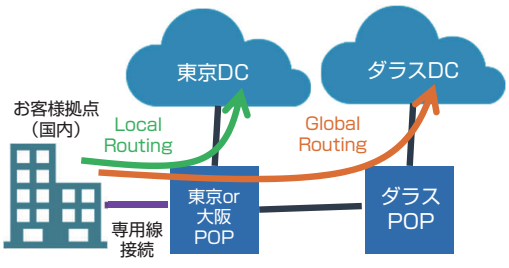
5. keepalive/holdタイマーの設定値は?
   デフォルトでkeepalive 30sec / hold time 90secという設定です。

Direct Link接続にかかる料金は、以下の合計となります。

1. Direct Link月額ポート費用
   - こちらのドキュメントをご参照ください。
     https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-pricing-for-ibm-cloud-direct-link&locale=en
2. (オプション)Global Routing オプション費用
   - お客様拠点からDirect Link経由で異なるRegionのDCに通信する際に必要です。
     https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-pricing-for-ibm-cloud-direct-link&locale=en#pricing-for-global-routing-add-on
   - 2019年7月から、それまで無償枠を超えた分は従量課金の対象だった他リージョンのDCからのアウトバウンド通信が無償となりました。
   - OSK01はTOK02/04/05と同一のLocal Marketとして扱われ、OSK01に接続し、Local Routingのみ(Global Routing オプション無し)でTOK02/04/05のサーバーにアクセス可能です。
3. 接続タイプによって別途プロバイダーに支払う料金
   (回線費用やルータのハウジング費用、クロスコネクト費用など)

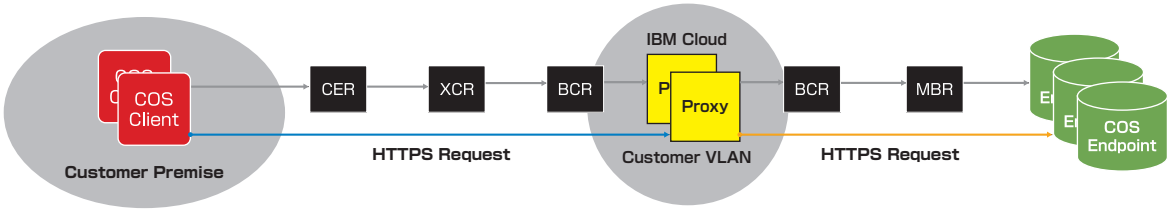
推奨情報 Osusume-desu

専用線接続すると、国内のお客様の拠点から、IBM Cloud 東京リージョン間における、データのアウトバウンド料金が発生しません。
また、国内のお客様拠点から、海外のIBM Cloudデータセンター間では、Global Routing Option(定額)で、どのデータセンターからの通信料金も発生しなくなります。
インバウンド通信はどの場合においても、課金されません。



Direct Link 経由でのIBM Cloudサービスネットワーク上のサービスへのアクセスについて

・Direct Linkはお客様のオンプレミス環境からIBM Cloudのお客様VLAN上のサーバーへの通信を目的としたソリューションであり、オンプレミスから、直接、IBM Cloudのサービスネットワーク上のサービスにアクセスする事はできません。
・オンプレミスからIBM Cloudのサービスネットワーク上のサービス（下記の例ではIBM Cloud Object Storage）にアクセスする場合は、IBM Cloud上に払い出したお客様サーバーにてProxyやNATの設定を行ってアクセスする必要があります（全てのサービスがこの方法でのアクセスを想定して作られている訳では無い点にご留意ください）。



https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-using-ibm-cloud-direct-link-to-connect-to-ibm-cloud-object-storage

2019年8月時点で、日本国内のDCやPOPに対しオーダー可能なDirect Linkタイプと場所は下記の通りです。
（最新の状況はページ下部のリンク先からご確認ください）

IBM Cloud 施設名 / Direct Link タイプ	TOK01 (POP)	TOK02 (DC)	TOK03 (POP)	TOK04 (DC)	TOK05 (DC)	OSK01 (POP)
Direct Link Exchange	○ Equinix	○ AT Tokyo	○ Equinix	-	-	-
Direct Link Dedicated	○ Equinix TY2	○ AT Tokyo CC2	○ Equinix TY4	○ Softbank	○ NTT	○ Equinix OS1
Direct Link Connect	○ COLT, Console Connect by PCCW	-	○ TOKAI	○ Softbank	○ NTT	-

https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-how-to-order-ibm-cloud-direct-link-exchange&locale=en
https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-how-to-order-ibm-cloud-direct-link-dedicated&locale=en
https://cloud.ibm.com/docs/infrastructure/direct-link?topic=direct-link-how-to-order-ibm-cloud-direct-link-connect&locale=en

5-4. よく利用される関連サービス

Content Delivery Network

Content Delivery Network（CDN）は、グローバルに展開された複数のサーバ上にコンテンツを複製し、最も地理的に近いエンドユーザーにインターネット経由で迅速にコンテンツを配信することを可能にするシステムです。
最初にコンテンツへのアクセスが発生した際に、オリジナルのサーバーからデータを取得してキャッシュし、その後のアクセスはキャッシュを使用します。

CDN が効果的な業種例
- Social networking
- Entertainment
- Gaming
- Software development
- E-Commerce
- Financial services

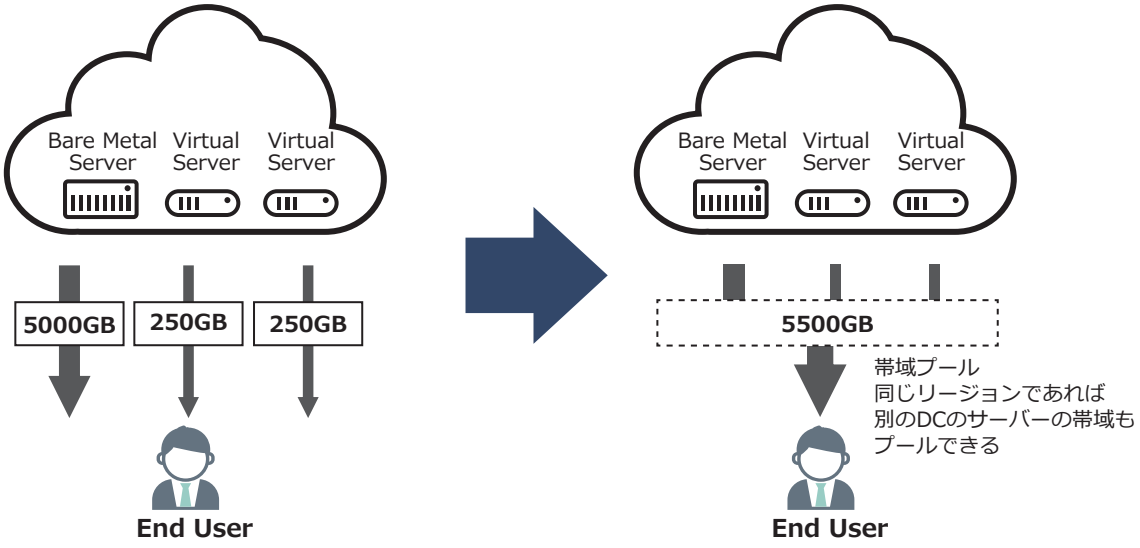
IBM Cloudで利用できるCDNサービス：
IBM Cloud Internet Services Akamai

https://cloud.ibm.com/docs/infrastructure/cis?topic=cis-getting-started#getting-started-withibm-cloud-internet-services-cis-

https://cloud.ibm.com/docs/infrastructure/CDN?topic=CDN-getting-started#cdn-

Bandwidth Pooling

IBM Cloudでは、それぞれのサーバーにある無償（およびオプションで購入した有償の）アウトバウンド枠を共有して分け合うことができます。
この仕組みを使うと、下図の例のように無料枠を足しあって分け合うこともできます。



IBM Cloudアウトバウンド無料通信枠（標準）
- Bare Metal Server: 5000 GB / month（東京DC）
- Virtual Server: 250 GB / month

IBM Cloud 帯域プール利用料金
- 初期費用: $25 / Server（設定時に発生）
- 月額費用: $25 / Server（翌月から発生）

インターネットドメインの登録、預かり

IBM Cloud環境では以下の4つのオプションをDNSサービスとして選択可能です。

1. ドメインをIBM Cloud経由で取得し、IBM CloudのDNSサーバーに登録
2. 取得済みのドメインを、IBM CloudのDNSサーバーに登録
3. 取得済みのドメインを、IBM Cloudに作成したDNSサーバーに登録
4. 取得済みのドメインを、外部ベンダーのDNSサーバーに登録

・IBM Cloud Domain Service

- ドメイン取得サービス
- .com/.net/.org/.info/.biz/.usの取得が可能
- 1-10年単位で購入可能（１年ごと更新も可能）

・IBM Cloud DNS

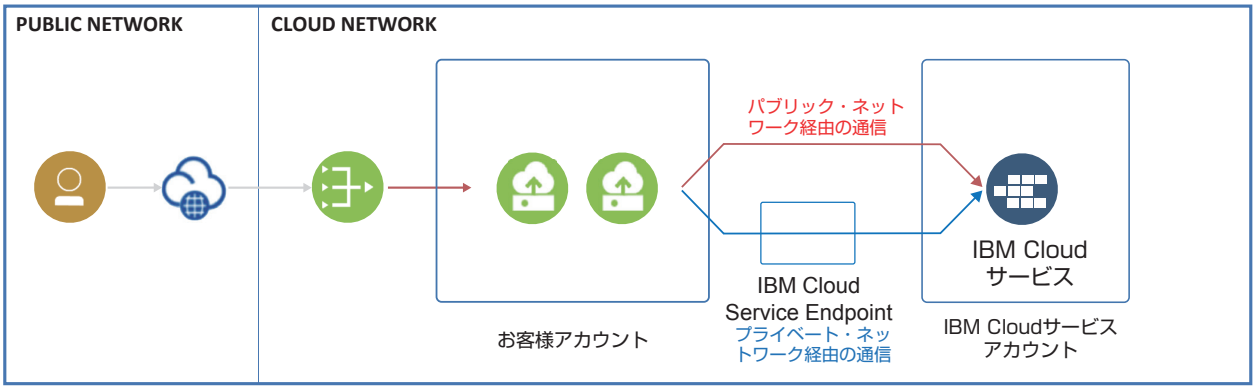
- ポータルを通じて、IBM Cloud環境のDNSサーバーを権威DNSとして使用することが可能。
- Primary DNS/Secondary DNS/Reverse DNSのmanaged serviceを提供
- Resource Type: A, AAAA, CNAME, MX, TXT, SRV, SPF
- TTL: 900(15分), 3600(1時間), 86400(1日), 604800(1週間)

取扱注意
Handle with care

IBM Cloud DNSサービスに登録する情報は、特定の利用者からのアクセスに制限することはできません。よって、プライベートIPアドレスの名前解決にも利用できますが、その登録したレコード情報はインターネット上に公開されることにご注意下さい。

IBM Cloud Service Endpoints

- これまで、サービスによってはパブリックネットワークを経由してエンドポイントへアクセスする必要がありましたが、IBM Cloud Service Endpoints に対応したIBM Cloud上のサービスについては、IBMのプライベートネットワークのみを用いてアクセスできるようになります。
- IBM Cloud上のサービスに対するアクセスについて、インターネットからのアクセスを制限することができます。
- IBM Cloud上のサービスへのアクセスは従来のIBM Cloudパブリック・ネットワーク経由、Service Endpointsを介したIBM Cloudプライベート・ネットワーク経由のいずれかもしくは両方をサービス・インスタンス毎に選択可能となります。
- IBM Cloud上のサービスへのアクセスにおいて、データ転送費用が発生していた項目は、Service Endpointsを利用することで費用が不要となります。



https://cloud.ibm.com/docs/resources?topic=resources-service-endpoints

・Service Endpointsを使用するには、アカウントでVRF (Virtual Routing and Forwarding) を有効にする必要があります。その後、Service Endpointsの使用を有効にすることができます。両方のオプションを有効にした後、カタログからService Endpointsをサポートするサービスを作成できます。

https://cloud.ibm.com/docs/resources?topic=resources-private-network-endpoints&locale=ja

・Service Endpointsをサポートするサービスの情報は下記に記載されています。最新情報は、表示を英語にしてご確認ください。

https://cloud.ibm.com/docs/resources?topic=resources-private-network-endpoints&locale=ja#services-support-service-endpoints

Service Endpointsをサポートするサービス（2019年8月8日時点）

サービス	資料
Databases for Elasticsearch	Databases for Elasticsearch service endpoints integration
Databases for etcd	Databases for etcd service endpoints integration
Databases for MongoDB	Databases for MongoDB service endpoints integration
Databases for PostgreSQL	Databases for PostgreSQL service endpoints integration
Databases for Redis	Databases for Redis service endpoints integration
Db2 on Cloud	Connectivity options
Db2® Warehouse on Cloud	Connecting to a private endpoint
Event Streams	Adding a private endpoint
IBM Cloudant	Available for all dedicated hardware plans deployed after 1 January 2019
IBM Cloud Container Registry	IBM Cloud Container Registry documentation
IBM® Streaming Analytics for IBM Cloud	Managing service endpoints for Streaming Analytics
Key Protect	Connecting to Key Protect on the IBM Cloud private network
KMIP for VMware on IBM Cloud	KMIP for VMware on IBM Cloud documentation
Kubernetes Service	Public and private service endpoints for Kubernetes Service
Object Storage	Object Storage utilizes Key Protect's service endpoint for its BYOK integration
Messages for RabbitMQ	Messages for RabbitMQ service endpoints integration

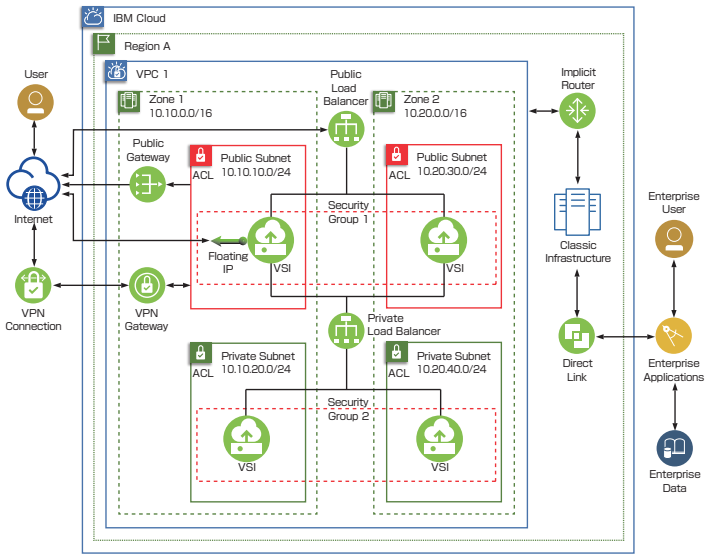
6

VPC

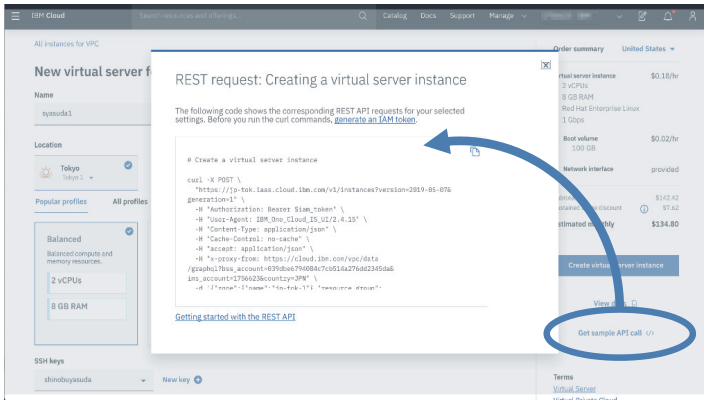
INDEX

6-1. VPC(Virtual Private Cloud)とは

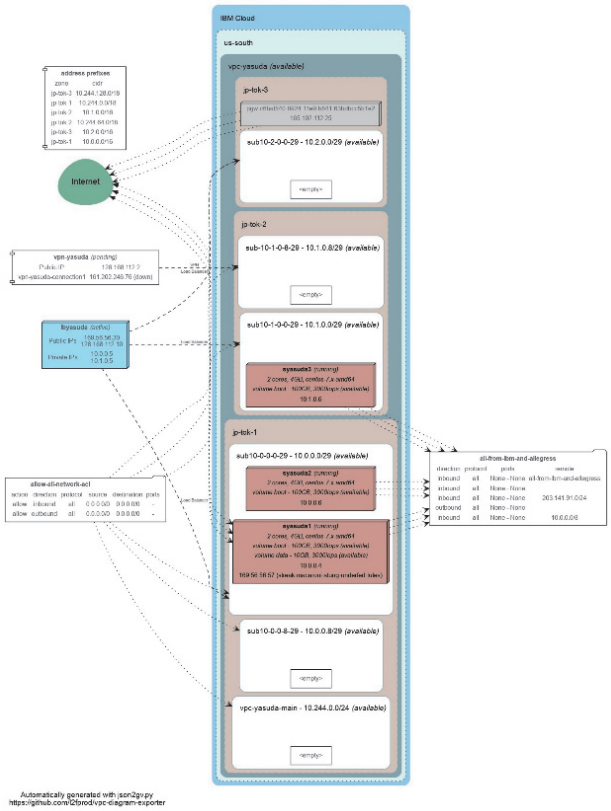
本章では、IBM CloudにおけるVPC(Virtual Private Cloud)について解説します。
VPCを使うと、利用者が指定したVSIにコンピューティングリソースをデプロイできます。
VPCは2019年9月時点で5つのリージョン（東京、ダラス、フランクフルト、ロンドン、シドニー）で利用できます。



ポータルからREST APIの生成が簡単に可能なため
Infrastructure as a codeの実践が容易になっています。



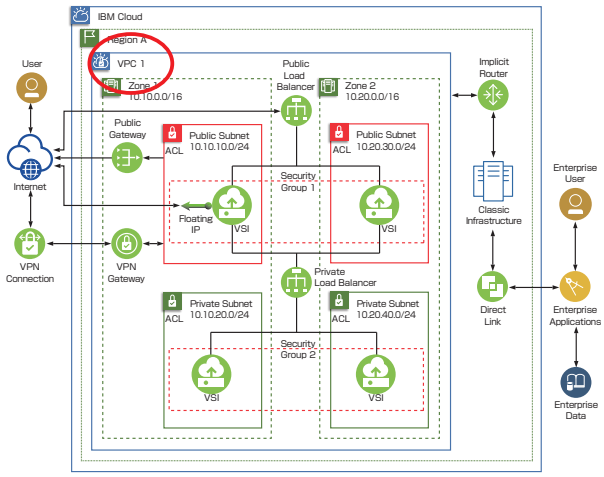
VPC視覚化ツール（VPC-diagram-exporter）も
利用できます。
https://github.com/l2fprod/vpc-diagram-exporter



6-2. VPCの構成要素

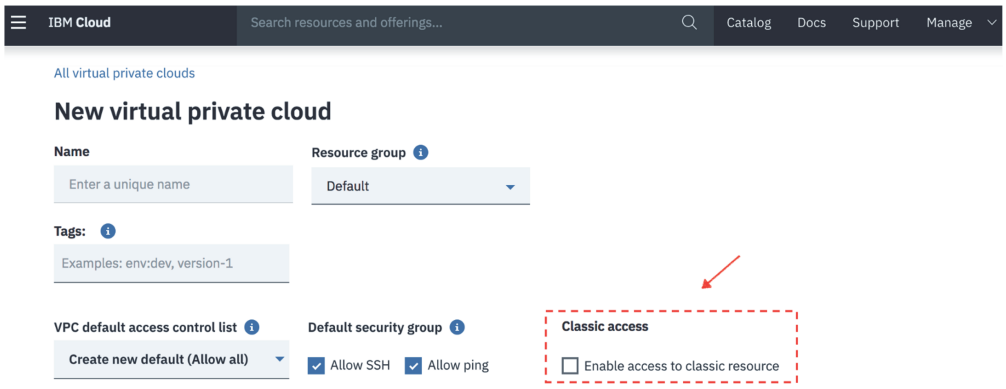
VPC

・VPCはRegionごとに作成し、複数のZoneにまたがって構成します。
・IBM CloudのVPCには、二種類のVPCが存在します。



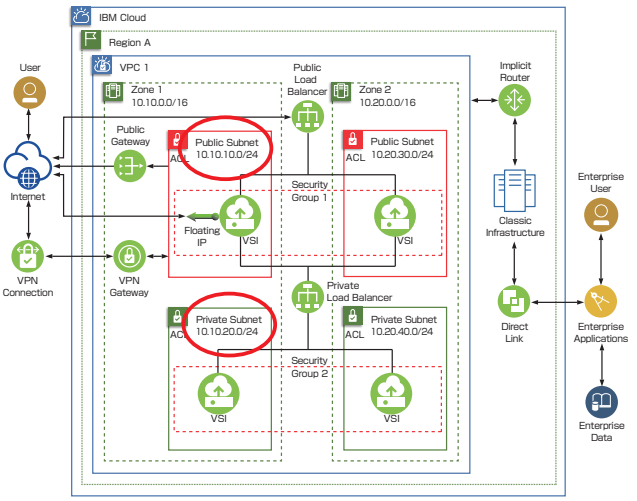
	Classic Access VPC	（標準の）VPC
作成可能数	Region ごとに 1 つのみ	Region ごとに、Classic Access VPC と (Standard VPC) を合わせて 5 つまで
Classic Infrastructure（物理サーバーなど）との Private NW 通信	可能（通信費用は無料）	不可
専用線接続	可能 (Classic Infrastructur 経由)	不可
Zone 間 Private NW 通信	可能（通信費用は無料）	可能（通信費用は無料）
VPC 間 Private NW 通信	Classic Access VP 同士であれば可能（通信費用は無料） ※ Classic Access VPC は Region ごとに 1 つしか作成できないので、Classic Access VPC 間通信は Region 間通信になる	不可
他アカウントの VPC との Private NW 通信	不可	不可

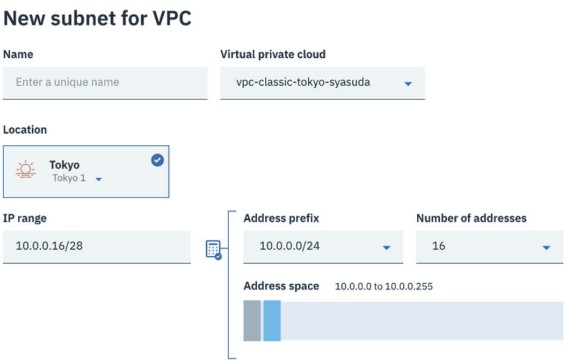
Classic Access VPCの有効化方法



address prefixとsubnet

・VPCでは、まずaddress prefixと呼ばれるIP rangeをZoneごとに定義します。
・subnetはaddress prefixから切り出して定義します。
・address prefixがZoneごとに構成されるため、subnetはZoneをまたいで構成することはできません。





取扱注意
Handle with care

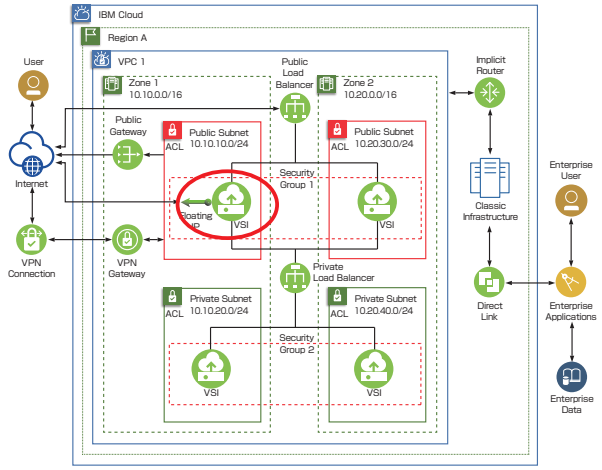
現時点で、以下の制約があります。
- address prefixはzoneごと5個まで
- subnetはVPCごとに15個まで
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-quotas

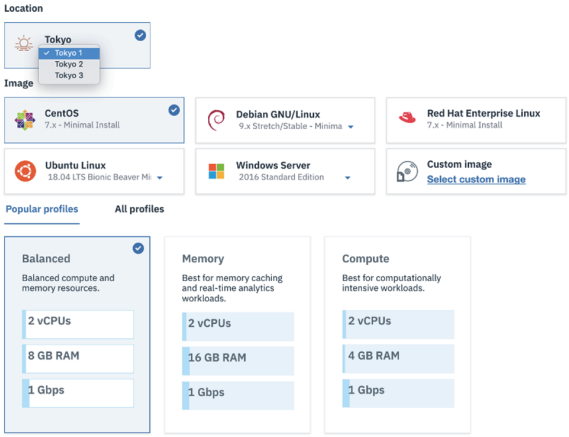
取扱注意
Handle with care

・VPCを作成する際には、defaultのaddress prefixが自動的に作成されます。本資料作成時点では、このdefault address prefixとしてユーザーが任意のaddress rangeを指定することはできませんし、別のaddress prefixに変更することもできません。
  • https://cloud.ibm.com/docs/vpc-on-classic-network?topic=vpc-on-classic-network-working-with-ip-address-ranges-address-prefixes-regions-and-subnets# default-vpc-address-prefixes
  • https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-setting-up-access-to-your-classic-infrastructure-from-vpc# classic-access-default-address-prefixes
・Subnetを作成する場合には、defaultのaddress prefixに加えて、作成したいsubnetを包括するaddress prefixを最初に作成してください。
・Subnetの中の全てのIPアドレスが利用できる訳ではありません
  • 以下がVPCで予約されているアドレスです。https://cloud.ibm.com/docs/vpc-on-classic-network?topic=vpc-on-classic-network-about-networking-for-vpc#reserved-ip-addresses
  • https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-setting-up-access-to-your-classic-infrastructure-from-vpc# classic-access-default-address-prefixes
  （例）10.10.10.0/24の場合
    • 10.10.10.0: Network Address
    • 10.10.10.1: Gateway Address
    • 10.10.10.2: reserved by IBM
    • 10.10.10.3: reserved by IBM for future use
    • 10.10.10.255: Network broadcast address
・subnetの指定はできますが、IP addressの指定はできません。システムがsubnetの中から自動的に割り当てます。
・subnetの指定はできますが、任意のsubnetをいきなり作成することはできません。
  • 例えば、10.0.0.16/29をいきなり作ることはできず、"10.0.0.0/29と10.0.0.8/29の作成後"もしくは"10.0.0.0/28"を作って前方のrangeを埋めてからでないと作れません

VSI（仮想サーバー）

・VPCのVSIは、Balanced/Compute/Memoryの3つのProfileから選択可能です。
・利用時間に応じた自動割引が行われます。suspend billingにも対応しています。





取扱注意

現時点で、以下の制約があります。
・システムバックアップの代替手段がない（都度作り直しが必要）
・プロビジョニング後に、プロファイルの変更やvNICの追加ができない
（CPUやメモリサイズを変更したい場合は作り直しが必要）
・仮想共有サーバーのみの提供。仮想専有サーバーや物理サーバーは利用できない。

VSIのストレージ

・Boot領域として100GB/Max 3000 IOPSのストレージが割り当てられます。
・データ領域として以下の数のVolumeを追加することができます。
  ・4 core未満：4まで
  ・4 core以上: 12まで
・データ領域用Volume（1 Volumeあたりの構成）
  ・Tier構成：
    ・3 IOPS/GB, 5 IOPS/GB, 10 IOPS/GB
    ・10GB~2TB
  ・Custom構成
    ・100 IOPS ~ 20,000 IOPS
    ・10GB~2TB
・暗号化オプション
  ・Provider Managed(IBMが鍵を管理)
  ・Key Protect(ユーザー鍵の持ち込みが可能): FIPS 140-2 *Level 2*準拠
  ・Hyper Protect Crypto Services(Dallasのみ利用可): FIPS 140-2 *Level 4*準拠

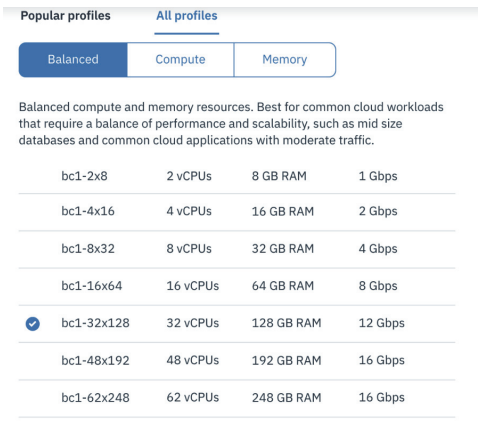
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-quotas#secondary-volume-quotas
https://cloud.ibm.com/docs/vpc-on-classic-block-storage?topic=vpc-on-classic-block-storage-block-storage-profiles

取扱注意

Classic InfrastructreのEndurance Storageとは異なり、複数のVSIからアクセス可能な共有ストレージはVPCには現時点で提供されていません。

VSIのvNIC

・5つまでvNICを付与可能です。
・プロファイルによっては、16Gbpsモデルまで選択可能です。
  ・1vNICあたりの性能は、付与されているvNICの数で分割され、その値でキャップされます。
    ・例：16Gbps / 4vNIC = 4Gbps per vNICが最大値
  ・5Gbps以上のプロファイルを選択した場合は、NW性能を十分に引き出すためにjumbo frameの構成をしてください。

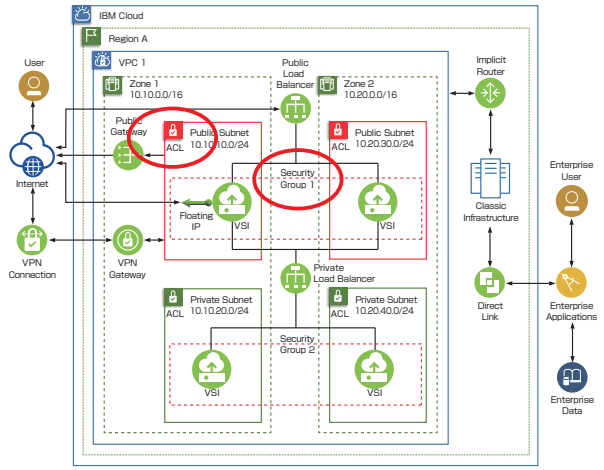


取扱注意

ネットワークの速度は、性能保証ではなく、上限値です。
（参考）https://cloud.ibm.com/docs/vpc-on-classic-vsi?topic=vpc-on-classic-vsi-profiles&origin_team=T15GKHBT4#network-perf-notes-for-profiles

Security Group/Network ACL

・Security GroupとNetwork ACLはVPCでのパケットフィルタリング機能を提供します。
・両者の違いは以下になります。

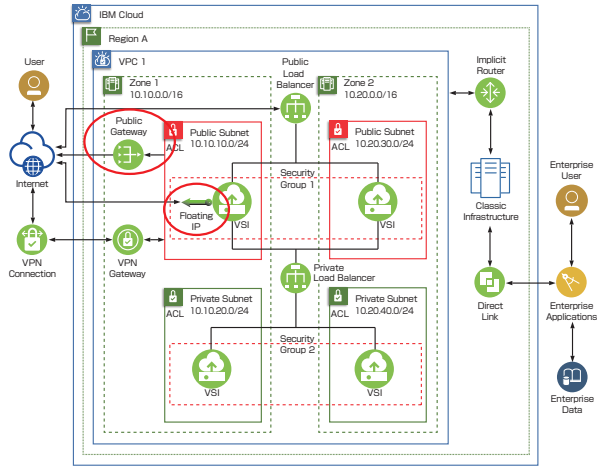


	Security Group	Network ACL
制御レベル	VSI	subnet
State 管理	Stateful firewall（インバウンド接続が許可されると、その応答も許可される）	Stateless firewall（インバウンド接続とアウトバウンド接続の両方を明示的に許可する必要がある）
サポートされているルール	許可ルール	許可ルールと拒否ルール
ルールの適用方法	全てのルールが評価される	ルールは順番に処理される。
VPC 間の Private NW 通信	1つの VSI に複数のセキュリティーグループを適用することができる	複数の subnet に同一の Network ACL を適用することができる。

https://cloud.ibm.com/docs/vpc-on-classic-network?topic=vpc-on-classic-network-compare-security-groups-and-access-control-lists

Floating IP/Public Gateway

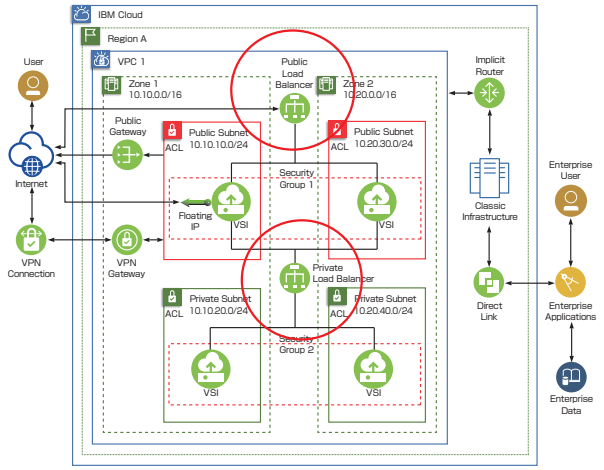
・VSIがインターネットと通信する手段としては、Floating IPを使う方法とPublic Gatewayを使う方法があります。



	Floating IP	Public Gateway
制御レベル	VSI の vNIC ※ただし、仮に複数の vNIC を持っていたとしても1つの VSI には1つまでしか Floating IP を関連づけることはできない。	subnet
利用可能な通信	インターネットからの Inbound/Outbound 両方の通信が可能	インターネットへの outbound 通信のみ可能（インターネットからの Inbound は許可しない）
Global IP アドレスの予約（付け替え可能かどうか）	可能。 ただし、同一 Zone 内の subnet に対してのみ付け換え可能。	可能。 ただし、同一 Zone 内の subnet に対してのみ付け換え可能。

Load Balancer

・Managed ServiceのLoad Balancer。
・異なるAZ上にある複数のsubnetを選択することで、Zoneまたぎで配置することが可能。

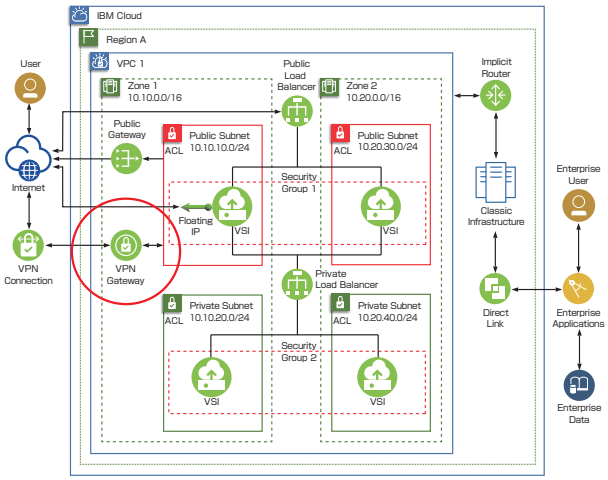


・defaultではLoad BalancerのFQDNに対して2つのインスタンスがデプロイされる(IPアドレスが2つ割り振られる)。
・負荷に応じて自動的にインスタンス数が増減する(IPアドレスの数が変化する。)
・フロントエンド側リスナーは以下をサポート
  ・プロトコル:
    ・HTTP
    ・HTTPS(SSL Offload機能あり)
    ・TCP
・バックエンド側プールは以下をサポート
  ・プロトコル:
    ・HTTP
    ・TCP
  ・割振り方法
    ・Round Robin
    ・Weighted Round Robin
    ・Least Connections
  ・Session Stickiness
    ・Source IPベース

https://cloud.ibm.com/docs/vpc-on-classic-network?topic=vpc-on-classic-network---using-load-balancers-in-ibm-cloud-vpc

VPN Gateway

・Managed ServiceのSite-To-Site VPNサービス。
・最大で650Mbpsのスループットをサポートします。



取扱注意
Handle with care

- IKEv1 and IKEv2
- Authentication algorithms: md5, sha1, sha256
- Encryption algorithms: 3des, aes128, aes256
- Diffie-Hellman (DH) groups: 2, 5, 14
- IKE negotiation mode: main
- IPSec transform protocol: ESP
- IPSec encapsulation mode: tunnel
- Perfect Forward Secrecy (PFS)
- Dead Peer Detection
- Routing: Policy-based
- Authentication Mode: Pre-shared key
- HA Support in Active/Standby mode only

・VPN GatewayはZoneを指定して構成します。Zone内でActive/Standbyで構成されていますが、Zoneまたぎで冗長化はされていません。
・VPN ゲートウェイは、VPCで定義されたsubnet以外（例：Classic Infrastructureなど）からは利用できません。（※VPN ConnectionのLocal subnetにVPCで定義されたsubnet以外は指定できない）
・VPN ゲートウェイは、デフォルトでは同一Zone内のVSIからのみ利用可能です。別Zoneに存在するVPN Gatewayを使ってVPN通信はできません。この問題を回避するためには、後述のVPC Routesを利用してください。

https://cloud.ibm.com/docs/vpc-on-classic-network?topic=vpc-on-classic-network---using-vpn-with-your-vpc

VPN新機能

・IaaS endpoints(DNSやNTPなど)やCloud Service endpoints（ICOSやPaaSサービスなど）にも、VPN経由でアクセスが可能になった。

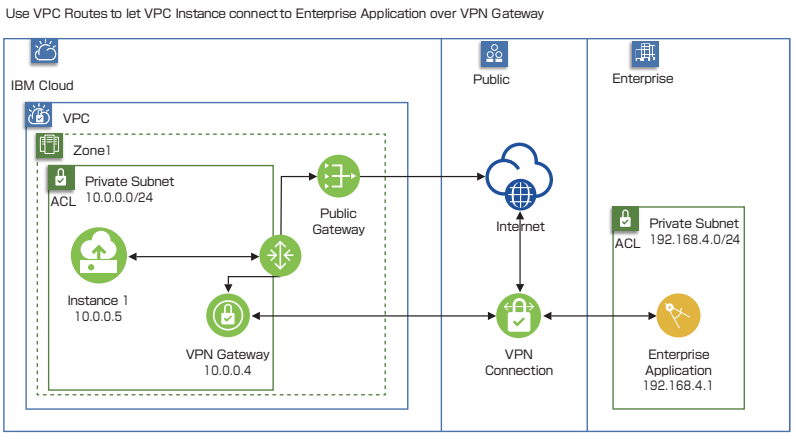
設定方法

・VPN Connectionの設定時のlocal subnetとして以下を指定。
  ・161.26.0.0/16: IaaS endpoints
  ・166.8.0.0/14: Cloud Service endpoints
・詳細は以下をご参照ください。
https://cloud.ibm.com/docs/vpc-on-classic-network?topic=vpc-on-classic-network---using-vpn-with-your-vpc#build-se-connectivity-using-vpn

VPC Routes

・デフォルトの経路情報に加えて、追加のstatic routeを構成することが可能です。(API/CLIのみ)
・経路情報として、宛先CIDR, next hope, Zoneを指定します。

ユースケース1:
・問題:
  ・Public Gatewayを関連づけているsubnet上のVSIにおいて、デフォルトの経路はPublic Gateway経由であるため、たとえVPN Gatewayを構成してもインターネットにアクセスしてしまう。
・解決策:
  ・VPC Routesを構成することで、特定の宛先（この例では192.168.4.0/24)に関してはVPN Gatewayを利用する。



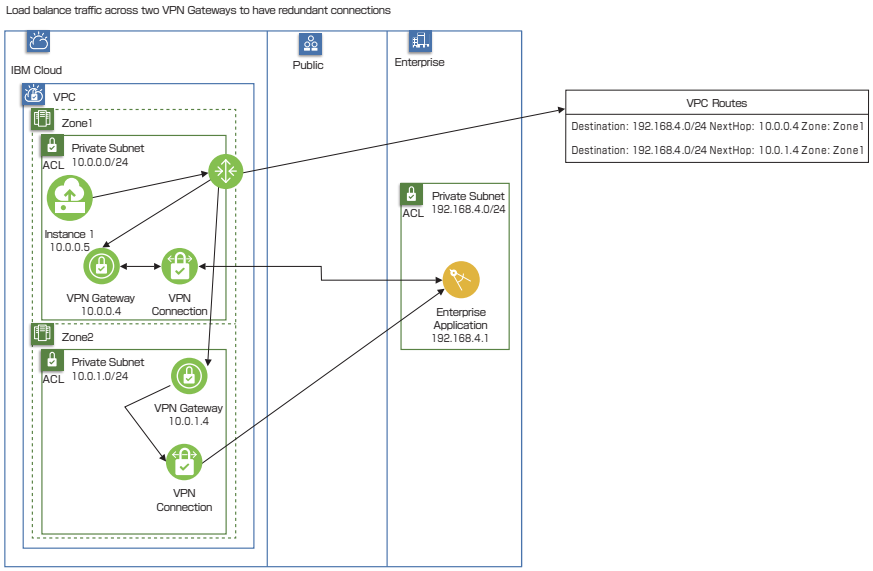
VPC Routes
Destination: 192.168.4.0/24 NextHop: 10.0.0.4 Zone: Zone1

https://cloud.ibm.com/docs/vpc-on-classic-network?topic=vpc-on-classic-network-setting-up-advanced-routing-in-vpc
https://cloud.ibm.com/apidocs/vpc-on-classic#create-a-route-on-your-vpc
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-infrastructure-cli-plugin-vpc-reference#vpc-route-create

ユースケース2:

・問題:
  ・デフォルト経路のままでは、同一Zone内のVPN Gatewayしか利用できない。

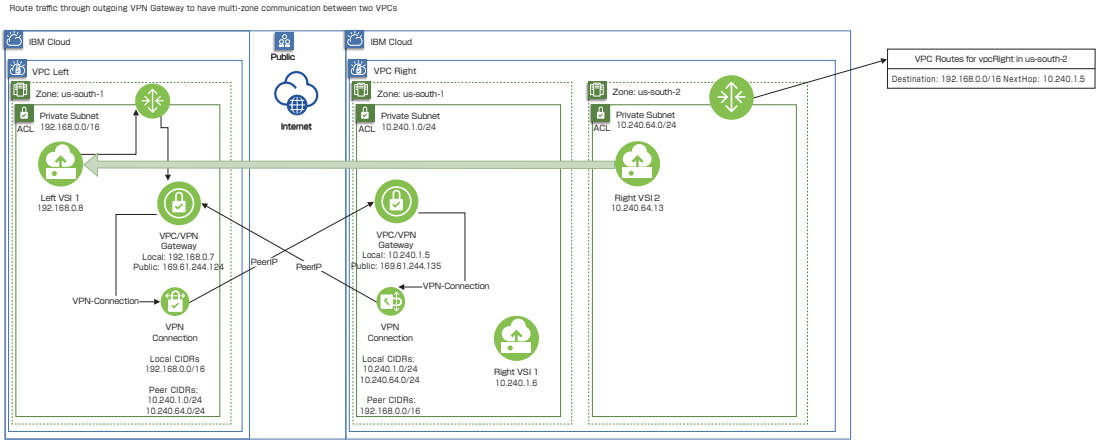
・解決策:
  ・ZoneごとにVPN Gatewayを作成し、VPC Routesを設定することで、複数のZone内のVPN GatewayをRound Robinで利用することが可能にする。



ユースケース3:

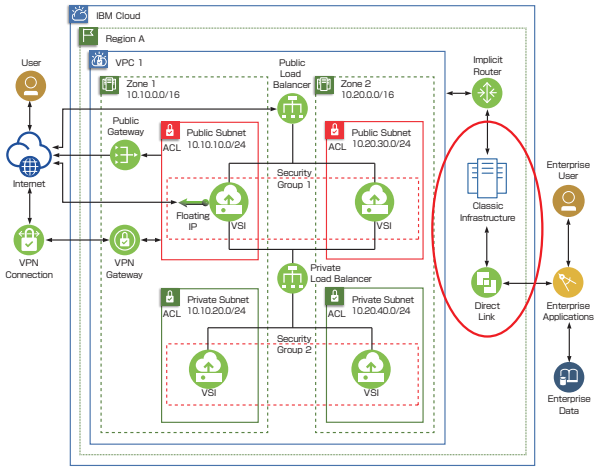
・問題:
  ・デフォルト経路のままでは、別ZoneにあるVPN Gatewayを使ってVPN通信することはできない

・解決策:
  ・別ZoneのVPN Gatewayを使ってVPN通信を行う



Direct Link

・Classic Access VPCのみでサポートされています。
・現在はClassic Infrastructure経由でのみ接続がサポートされてます。そのため、Direct LinkはClassic Infrastructureから注文します。



・Classic Infrastructureに対して、過去一度も何れのリソースを作成していないアカウントに限って、Classic Infrastructureで存在していた制約に縛られずに、VPC上のaddress prefixがXCR経由でBGP広告されます
・subnetを定義していないaddress prefixは広告されません

取扱注意
Handle with care

Classic InfrastructureにVSIやBaremealを一度でも構成した場合は、Classic Infrastructure固有の制約(10.0.0.0/14などがBGPで広告されない、等)が発生します。
オンプレミスのネットワークとのIP重複問題を避けるためには、Classic Infrastructureには何も作成しないでください。
一度でもClassic Infrastructureのリソースを作成してしまった場合は、その後に削除しても、Classic Infrastructureの制約は残り続けます。
この場合は、アカウント再作成が必要になります。

6-3. その他

課金情報

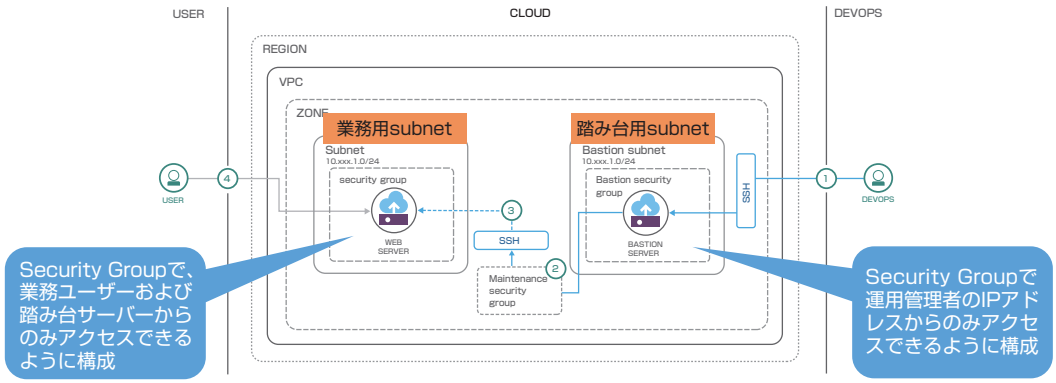
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-pricing-for-vpc
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-pricing-for-virtual-servers-for-vpc
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-block-storage-pricing

その他制約事項

https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-known-limitations
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-quotas
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-faqs

よくある質問

・Q: VPC上のVSIに、Classic InfrastructureのSSL-VPNを使ってアクセスすることはできますか?
・A: できません。
代替策1）Direct Linkを構成する(Classic Access VPCの場合）
代替策2) VPCのVPNサービスを使う
代替策3) Classic IaaSのVSIにSSL-VPNでログインし、そこを踏み台としてVPC上のVSIにアクセスする
代替策4) 以下のような踏み台subnetと踏み台サーバーを構成する



https://cloud.ibm.com/docs/vpc-on-classic?topic=solution-tutorials-vpc-secure-management-bastion-server

・Q: DNSやNTPサーバーのIPアドレス情報を教えてください。
・A: 以下を参照してください。
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-service-endpoints-available-for-ibm-cloud-vpc

・Q: VPC上のVSIからICOSにPrivate NW経由で通信費無料でアクセスすることはできますか?
・A: 可能です。Endpoint情報はこちらを利用してください。なお、(Classic Access VPCではない標準のVPCからでも、他RegionのICOSにはPrivate NW経由で通信費無料でアクセス可能です。
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-connecting-to-ibm-cloud-object-storage-from-a-vpc

・Q: VPC上のVSIからCloud Service Endpoint経由でPaaSサービスを利用可能ですか?
・A: 利用するPaaSサービスによって異なります。確認が必要なサービスに関してはIBM営業経由でご相談ください。

・Q: 新機能情報はどこで入手できますか?
・A: 以下のRelease notesをご参照ください。
https://cloud.ibm.com/docs/vpc-on-classic?topic=vpc-on-classic-release-notes

7

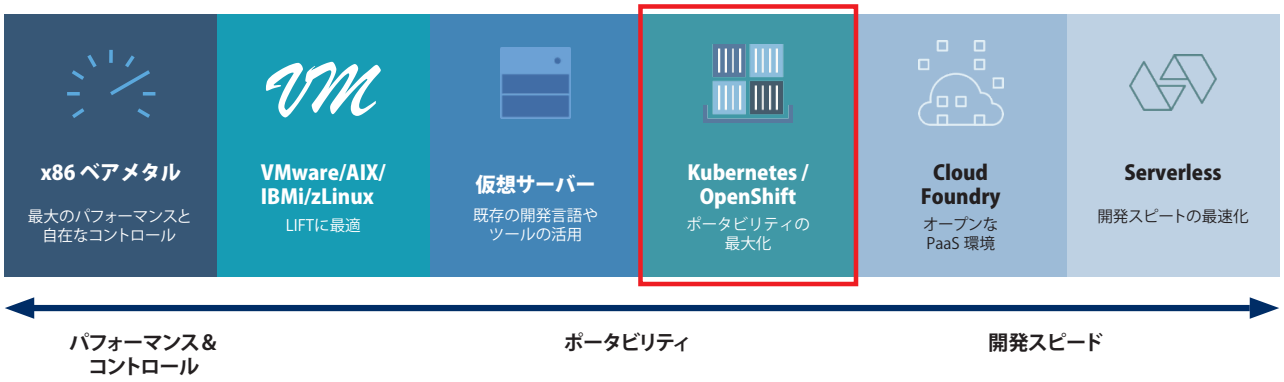
クラウド・ネイティブ

INDEX

7-1. IBM Cloud Kubernetes Service

IBM Cloud Kubernetes Service 概要

IBM Cloud上で最も簡単にコンテナ環境をご利用いただけるプラットフォームです。
IBM Cloud Kubernetes Serviceでは、Kubernetes Cluster または、RedHat OpenShift Clusterをマネージド・サービスとして
ご利用いただけます。



IBM Cloud Kubernetes Service(IKS) で利用可能な Cluster

フルマネージドでご利用いただけるKubernetesサービスをご提供しています。
利用可能なClusterはKubernetes Cluster とRed Hat OpenShift Cluster の２つから選択してご利用いただけます。

IBM Cloud Kubernetes Service
Kubernetes Cluster フルマネージドサービス

Kubernetes Cluster
ネイティブKubernetesをベースとしたクラスター

- フルマネージドサービス
  IBM管理のMasterノードをHA構成で運用
- 最新の３バージョンから選択可能
  1.15, 1.14, 1.13
- ノードOSにUbuntuを利用
- Container Registry / Continuous Delivery等
  サービスを組み合わせた運用
- Helmを利用したアプリのデプロイ・運用

Red Hat OpenShift Cluster(OCP)
Red Hatと連携してご提供するOpenShiftクラスター

- フルマネージドサービス
  IBM管理のMasterノードをHA構成で運用
- Kubernetesバージョン 1.11(OCP 3.11の場合)
- ノードOSにRed Hat Enterprise Linuxを利用
- 統合された CI/CD
- 統合された OpenShift カタログ

IBM Cloud Kubernetes Service(IKS) としての特徴

https://cloud.ibm.com/kubernetes/catalog/cluster

フルマネージドでご利用いただけるKubernetesサービスとして、
IKSでは直感的なユーザー・エクスペリエンスと容易なクラスタ管理ご提供しています

簡略化されたクラスタ管理

- 高可用性(HA)の
  マネージドMaster
- Nodeの自動リカバリー
- IBM Cloud IAMによる
  アクセス管理

独自のクラスター設計

- 仮想サーバー(共有/専有)、
  ベアメタルから選択
- マルチゾーンクラスター
  による高可用性構成

セキュリティの担保

- 脆弱性アドバイザー
  によるコンテナーイメージと
  実行中のコンテナーの検査
- HSMによる鍵管理

IBM Cloud & Watsonの活用

- Watson, IoT, Analyticsなど
  IBM Cloudサービスと連携
- Secretは自動で暗号化

ネイティブKubernetes体験

- Kubernetesの公式認証
  プロバイダー
- Kubernetes APIとツール
  を100%利用可能

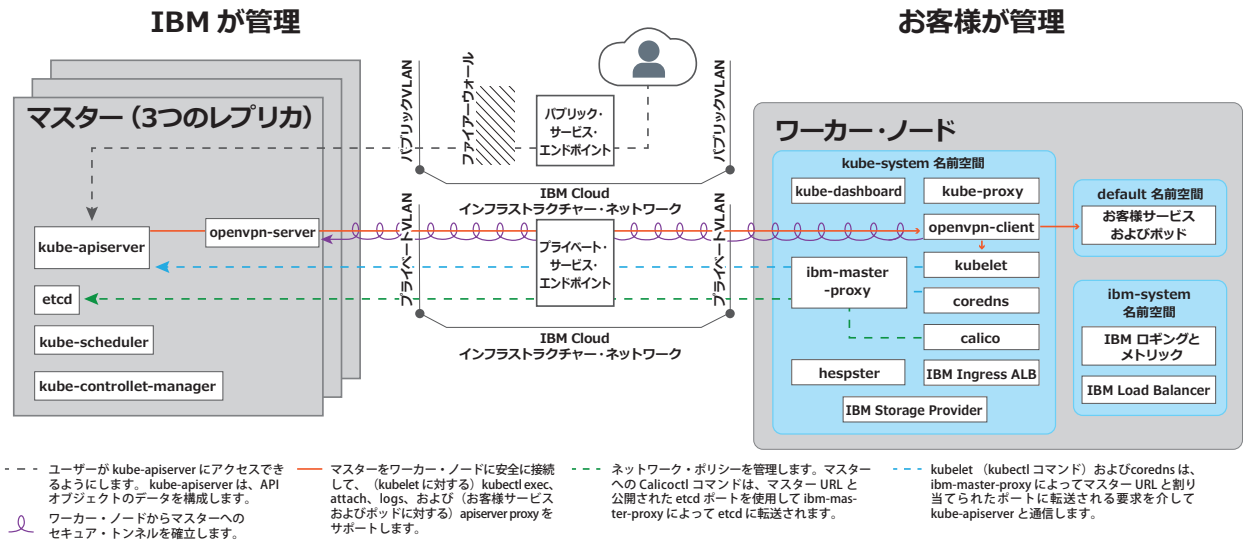
統合された運用ツール

- ロギング、監視サービスが
  ビルトイン
- Prometheusやfluentdなど
  アドオンツールのサポート

IBM Cloud Kubernetes Service(IKS) テクノロジー

https://cloud.ibm.com/docs/containers?topic=containers-ibm-cloud-kubernetes-service-

IKSはマネージド・サービスとしてご提供しており、マスターノードをIBMが管理、ワーカーノードをお客様が管理します



複数ゾーンを組み合わせたMulti Zone Cluster構成

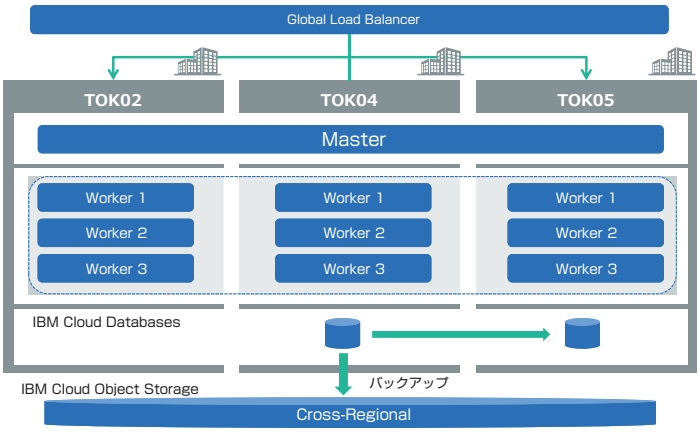
https://cloud.ibm.com/docs/containers?topic=containers-storage_planning#persistent_storage_overview

MZCを利用することで国内で高可用性構成を実現できます

グローバルロードバランサー
・GLBはIKSの機能としてご提供

マスター
・マスターノードも３ゾーンで構成

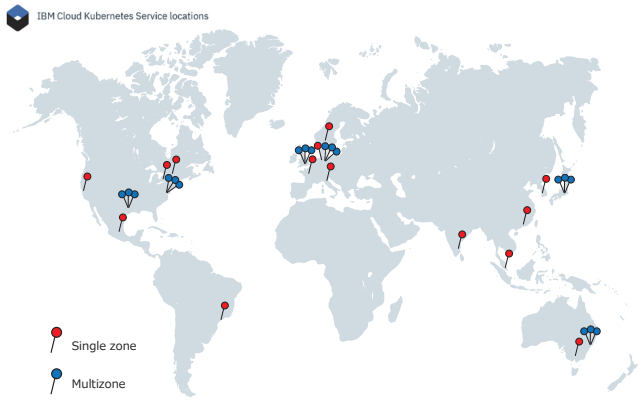
ストレージ
・マルチゾーン対応のサービスを組み合わせて利用
　・IBM Cloud Database
　・IBM Cloud Object Storage
・Portworx を使用したソフトウェア定義ストレージ(SDS)



利用可能な地域

https://cloud.ibm.com/docs/containers?topic=containers-regions-and-zones#regions-and-locations

全世界の多数のデータセンターでご利用いただけます。
東京では複数ゾーンを組み合わせた高可用性の構成である
Multi Zone Clusterもご利用いただくことが可能です。



複数ゾーンの大都市ロケーション
１６の国、２０の地域で提供

地理	国	大都市	データ・センター	非推奨の地域
アジア太平洋	オーストラリア	シドニー	syd01、syd04、syd05	南アジア太平洋地域 (ap-south、au-syd)
アジア太平洋	**日本**	**東京**	**tok02、tok04、tok05**	**北アジア太平洋地域 (ap-north、jp-tok)**
ヨーロッパ	ドイツ	フランクフルト	fra02、fra04、fra05	中欧 (eu-central、eu-de)
ヨーロッパ	英国	ロンドン	lon04、lon05*、lon06	英国南部 (uk-south、eu-gb)
北アメリカ	米国	ダラス	dal10、dal12、dal13	米国南部 (us-south)
北アメリカ	米国	ワシントン D.C.	wdc04、wdc06、wdc07	米国東部 (us-east)

料金体系

IKSの料金体系は割り当てられたワーカーノード料金、IPアドレスの割り振り料、
そして複数ゾーン構成の場合は複数ゾーンのロード・バランサー料金がかかります。

推奨情報 Osusume-desu

IBM Cloudでは、マスターノードの利用料金はかかりません。
AZに分散配置することで、高可用なコンテナ環境をご利用いただけます。

ワーカーノード
- 選択したマシンタイプと合計稼働台数に対して課金
- 仮想-共有, 仮想専有のマシンタイプでは**時間課金**
- ベア・メタルのマシンタイプでは**月課金**

※OpenShift Clusterの場合はRed Hat Enterprise Linuxのライセンス料金が含まれます。

複数ゾーンのロード・バランサー
- マルチゾーンクラスタを利用する場合に必要なロードバランサー料金
- **時間課金**

IPアドレスの割り振り
- IKSクラスタに必要な一連のIPアドレス料金
- **月課金**

OpenShiftのライセンス料金
- OpenShift Clusterを利用する場合のライセンス料金
- **4vCPU/月課金**

その他
- パブリック・アウトバウンド料
- IBM Cloud Container Registry料

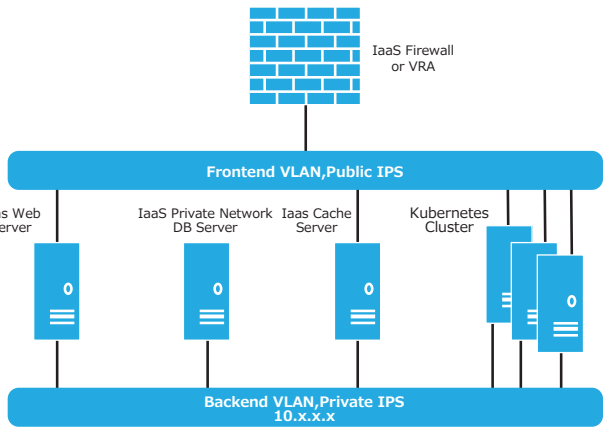
ネットワーク

https://cloud.ibm.com/docs/containers?topic=containers-firewall#firewall

IKSのワーカーノードはクラシック・インフラストラクチャ環境のサーバーとして構築されます。

ワーカーノードはユーザーのクラシック・インフラ・ストラクチャー上に配置
- IaaSサーバーとPrivateでの通信が可能
- 割り当てるPublic VLAN, Private VLANを選択
- Public VLANを割り当てないプライベートクラスタを作成可能

ネットワークセキュリティ
- インターネットからクラスターを保護するにはFirewallやCalicoを使用
- Firewall：VRA, Fortigate
- Calico：IKS内部のネットワーク制御で標準利用しているため別途構築は不要
- Security Group



IBM Cloud Kubernetes Service を使用する際の責任

https://cloud.ibm.com/docs/containers?topic=containers-responsibilities_iks

タイプ別の責任	責任	内容
 クラウド・インフラストラクチャー	IBM	• ワーカーノードのプロビジョニング、追加と削除 • クラスター管理コンポーネントをセットアップおよびプロビジョニング
	お客様	• コンピュートおよびストレージ容量の調整 • ワークロードのニーズを満たすようにネットワーク構成
 管理対象クラスター	IBM	• クラスタの構築、運用、監視及びクラスタ管理用のAPI、CLI、コンソールの提供（MZR提供地域でのマルチマスター構成、etcd のバックアップおよびリカバリー） • クラシックインフラストラクチャーと統合するためのプラグイン提供など • マスター及びワーカーノードに対してOS、バージョン、およびセキュリティーのバージョン更新を適用できるように提供
	お客様	• マスターノード、ワーカーノードのバージョン更新の適用（パッチバージョンの場合、マスターノードには自動適用されます）
 セキュリティーが充実した環境	IBM	• PCI DSS など、さまざまな業界のコンプライアンス規格に対応した制御を維持 • マスターとワーカー・ノードの間の通信を TLS で暗号化 • ワーカーノードのストレージ暗号化、SSHの無効化 • Kubernetes 役割ベース・アクセス制御
	お客様	• ワークロードのニーズを満たすように追加のセキュリティー設定 https://cloud.ibm.com/docs/containers?topic=containers-security#security
 アプリのオーケストレーション	IBM	• Istio や Knative など、多くの管理対象アドオンを提供 • IBM Cloud上の様々なサービスとの統合（Container Registry、LogDNA、Sysdigなど） • サービス公開するためのロード・バランサーおよび Ingress ルートをサポート
	お客様	• 提供されたツールおよび機能を使用して、構成とデプロイ、許可のセットアップ、他のサービスとの統合、 外部からの処理、正常性のモニター、データの保存、バックアップ、およびリストアを行い、それ以外の場合は可用性が高く、回復力の高いワークロードを管理

Kubernetesのバージョン管理

https://cloud.ibm.com/docs/containers?topic=containers-cs_versions

サポートバージョン

複数のバージョンのKubernetes を同時にサポートします。
最新バージョン(n) がリリースされると、2 つ前のバージョン(n-2) までサポートされます。
最新バージョンから2 つより前のバージョン(n-3) は、まず非推奨になり、その後サポートされなくなります。

バージョン	サポート状況	IBM Cloud Kubernetes Service リリース日付	IBM Cloud Kubernetes Service サポート終了日
1.14.2 (n)	サポートあり	2019 年 5 月 7 日	2020 年 3 月†
1.13.6 (n-1)	サポートあり	2019 年 2 月 5 日	2019 年 12 月†
1.12.9 (n-2)	サポートあり（デフォルト）	2018 年 11 月 7 日	2019 年 9 月†
1.11 (n-3)	非推奨	2018 年 8 月 14 日	2019 年 6 月 27 日†
1.10 (n-4)	サポートなし	2018 年 5 月 1 日	2019 年 5 月 16 日
1.9 (n-5)	サポートなし	2018 年 2 月 8 日	2018 年 12 月 27 日

Kubernetesのバージョン管理

https://cloud.ibm.com/docs/containers?topic=containers-update

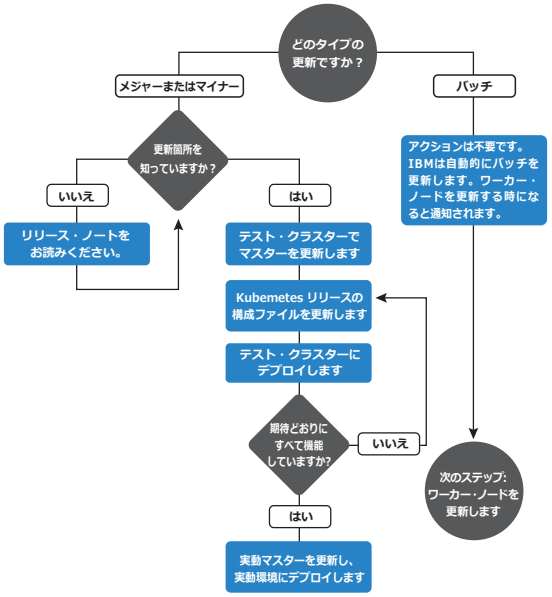
稼働中のIKSクラスタへのバージョンアップでは、
はじめにマスターノードを更新し、その後ワーカーノードを更新してください。

適用するバージョンの種類によって、お客様に実施いただく範囲が異なります。

メジャーバージョン（例：1.x.x）、マイナーバージョン（例：x.9.x）
お客様にてCLIまたはWebコンソールより更新を行います。
1. お客様にてマスターノードを更新
2. お客様にてワーカーノードごとに個別で更新

※ Kubernetes マスターを更新できるのは2 つ先のマイナー・バージョンまでです。例えば1.11から1.14に更新する場合は一度1.12に更新する必要があります。
※ ワーカー・ノードは、マスターよりも大きいKubernetes メジャー・バージョンまたはマイナー・バージョンを実行できません。

パッチバージョン（例：x.x.4_1510）
IBMとお客様にて更新を行います。
1. IBMにてマスターノードにパッチを自動適用
2. お客さまにてワーカーノードにCLIまたはWebコンソールより
   ワーカーノードごとに個別で更新



IBM ソフトウェアの利用方法

https://www-01.ibm.com/support/docview.wss?uid=ibm10733271

IBMの多くのソフトウェアはコンテナとして提供しております。
コンテナとして導入する場合、以下３つのご提供形態があり、用途に合わせて別途ライセンス契約を行います。

	Ad hoc containers IBM提供のソフトウェアバイナリをもとに独自のコンテナイメージを作成して利用	IBM Provided containers IBM提供のコンテナを利用イメージ	IBM Cloud Paks IBM提供のソリューションを利用
IBM ソフトウェアサポート	製品機能のみ	サポートあり	サポートあり
フルスタック・サポート by IBM (Base OS, software, deployment on cloud platform)	X	X	フルスタック・サポート
脆弱性スキャン (コンテナイメージの脆弱性を管理します)	独自に実施	IBMによる実施	IBMによる実施
Kubernetesベースでの構築 (Helm Chart)	なし	なし	IBM提供
マネージメントとオペレーション	独自に管理	独自に管理	ビルドイン
ライセンスメータリングの連携	独自に実施	独自に実施	○
ライフサイクル管理	独自に管理	独自に管理	テスト済みのアップグレードとロールバック

IBM ソフトウェアのサポート範囲

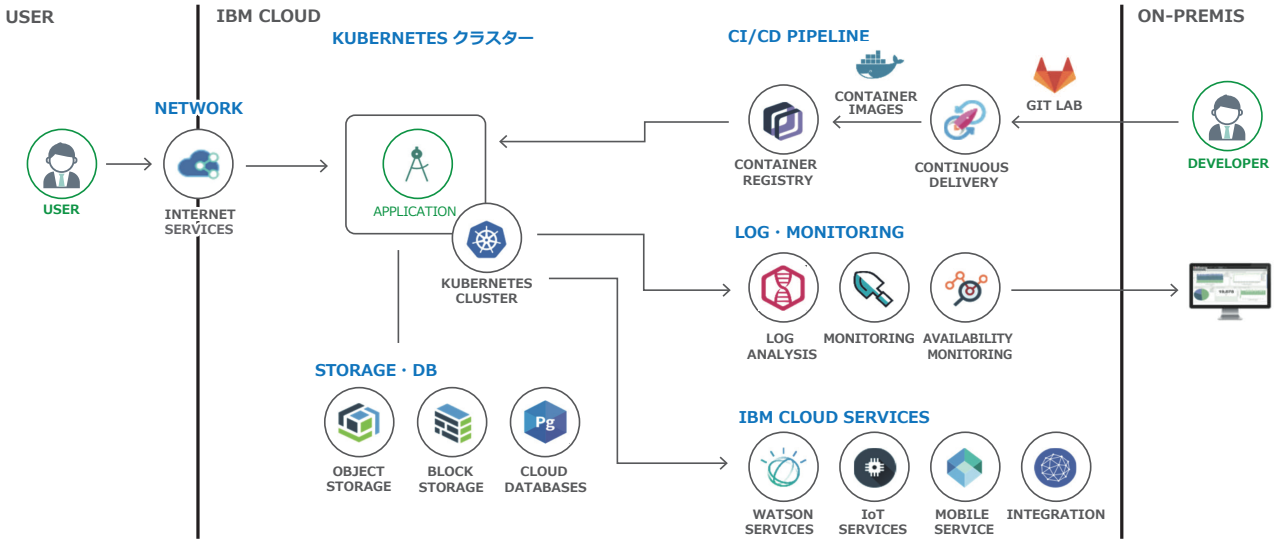
https://www-01.ibm.com/support/docview.wss?uid=ibm10733271

IBM ソフトウェアをコンテナ利用する場合、デリバリーモデルやコンテナイメージの作成者によって
サポート範囲が異なります。

	Ad hoc containers IBM提供のソフトウェアバイナリをもとに独自のコンテナイメージを作成して利用	IBM Provided containers IBM提供のコンテナを利用イメージ	IBM Cloud Paks IBM提供のソリューションを利用
デプロイメント/オーケストレーション (Helm Chart)	-	-	☑ サポートあり
IBM ソフトウェア (製品のコア機能)	☑ サポートあり	☑ サポートあり	☑ サポートあり
ベースOS コンテナ・イメージ	-	☑ サポートあり	☑ サポートあり
プラットフォーム・サービス (ログ、モニタリングなど)	-	-	☑ サポートあり
クラウド プラットフォーム (Kubernetes)	-	-	☑ サポートあり
オペレーティング・システム & ハイパーバイザー	-	-	☑ Supported by IBM for Linux on Power and Z Supported by RH when running certified content

IKSを活用したアプリ開発における関連サービス

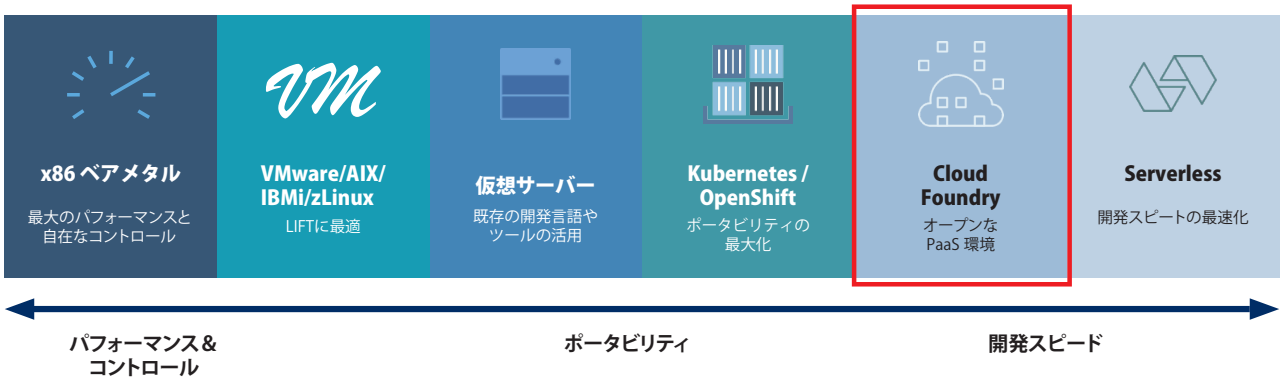
IBM Cloud上の様々なサービスを活用することで運用コストを小さく保ちながらアプリを拡張できます。



7-2. Cloud Foundry Application Runtime

IBM Cloud 上で最も簡単にクラウド・ネイティブ・アプリケーションを稼働させられるプラットフォーム

Cloud Foundryはオープンな PaaS(Platform as a service)環境です。Cloud Foundryを利用することで開発者が開発に注力でき、作成されたアプリケーションが迅速かつ簡単にビルド、テスト、デプロイでき、スケールも簡単に実施できます。IBM Cloudではマルチテナント環境のCloud Foundry Publicとシングルテナント環境のCloud Foundry Enterprise Environmentの2つのサービスが利用できます。

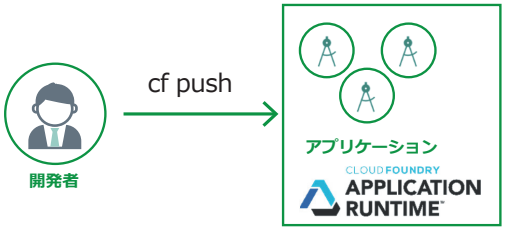


Cloud Foundryとは

オープンソースのPaaS(Platform-as-a-Service)のアプリケーション稼働基盤のソフトウェア

- 開発者が開発業務に注力できるようコード中心で設計されているプラットフォーム
- 任意の開発言語やフレームワークで記述されたアプリケーションを様々な環境で利用可能
- アプリケーション本体の周辺で稼働するAPIをサービスブローカーを通じて柔軟かつ簡単に統合可能

Pushコマンドを用いて簡単にアプリのデプロイが可能




```
> cf push APP_NAME
```

http://cli.cloudfoundry.org/en-US/cf/push.html

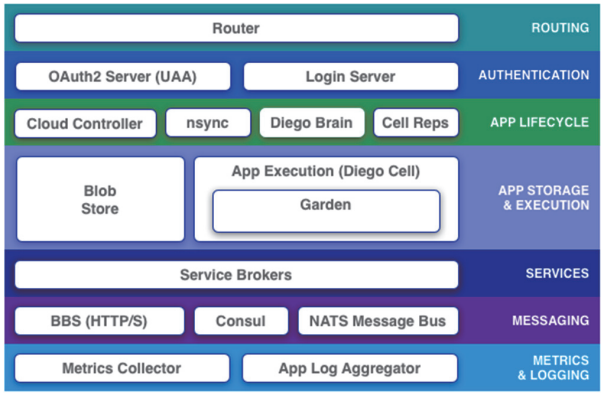
Cloud Foundry Communityの歴史

2011/4	VMware社がオープンなPaaSプラットフォームCloud Foundryを提供。
2013/3	VMWare社がCloud FoundryをPivotal社に移管。
2014/2	Pivotal社がCloud Foundry Foundationの設立と移管を発表。
2014/12	Cloud Foundry Foundationが非営利法人化。
2017/10	Cloud Foundry Container Runtimeが正式な商用プロジェクト化。

Cloud Foundryを構成する主要なコンポーネント

Cloud Foundryはアプリケーションを稼働させる基盤として多様なコンポーネントを有し、開発者が開発業務に注力できるような仕組みを提供します。

- Router
  - 外部システムからのトラフィックの適切な内部トラフィックに変換
  - 動的なルーティング・テーブルを管理し、外部からアプリケーション・インスタンスへのアクセスを稼働するIPアドレス・ポートを識別しルーティング
- Cloud Controller
  - Cloud Foundry全体を管理し、APIインターフェースを提供
- Diego Cell
  - Diego Cellは仮想マシンとして稼働
  - アプリケーション・インスタンスに相当するGardenコンテナがDiego Cell内で稼働。複数のGardenコンテナがDiego Cell内部で稼働。
  - アプリケーションのビルドから実行までのライフサイクルを管理
- Garden
  - Gardenコンテナのインスタンスは Linuxコンテナ
  - 分離された各環境を管理するためのAPIを提供
- Diego Brain
  - 複数のアプリケーションを稼働させるための管理し、個々のアプリケーション・インスタンスの配置や、実行状況の監視や状況に応じた管理を実行。



https://docs.cloudfoundry.org/concepts/images/cf_architecture_block.png

IBM Cloud Foundry

IBMがご提供するCloud Foundryオファリングはハイブリッド・マルチクラウドでの稼働をサポートしています。全てのオファリングを通じて開発者には同じエクスペリエンスを提供し、稼働環境によらない同様な開発を実施できます。

Cloud Foundry Public	Cloud Foundry Enterprise	Cloud Foundry Private
IBM Cloud上で稼働し、PaaS基盤部分をフルマネージド・サービスで提供するマルチ・テナントの Cloud Foundry環境 コミュニティが提供するランタイムと IBMが提供するランタイムを利用可能 全世界の 5マルチゾーン・リージョンで利用可能	IBM Cloud上で稼働できるシングル・テナントの Cloud Foundry環境。セルフサービスでのプロビジョン、利用に応じた規模の拡大が可能。 また、全管理者権限を利用可能 コミュニティと IBMそれぞれが提供するランタイムを利用可能 全世界の 6マルチゾーン・リージョン(東京を含む)を含む多くのリージョンで利用可能	お客様データセンターや他社クラウド上で稼働できる Cloud Foundry環境のソフトウェア製品。 Cloud Foundry Enterprise環境と同等の環境をお客様のデータセンター上のインフラストラクチャーなどで稼働可能

IBM Cloud Foundry – 利用可能なビルドパック

https://cloud.ibm.com/docs/runtimes-common?topic=runtimes-common-available_buildpacks

ビルドパックは複数言語での稼働をサポートする仕組み

ビルドパックはCloud Foundryアプリケーションを稼働させるために用意されている開発言語に応じたソフトウェアのパッケージ群です。
開発言語を選択する際にはビルドパックが提供されている言語から選択します。
IBM CloudではIBM提供のビルドパックおよびコミュニティのビルドパックを提供しております。

IBM Cloudで提供中のビルドパック

IBM提供のビルドパック

- Liberty for Java
- ASP.NET Core
- SDK for Node.js
- Runtime for Swift

コミュニティ提供のビルドパック

PHP　Python　Ruby　GO　Tomcat

IBM提供のビルドパックにかかるサポート・ポリシー

- Liberty for Java, SDK for Node.js, ASP.NET Core
  → 最新のバージョンおよび1つ前のバージョンをサポート
- Runtime for Swift
  → 最新のSwiftバージョンに適合するビルドパックをサポート

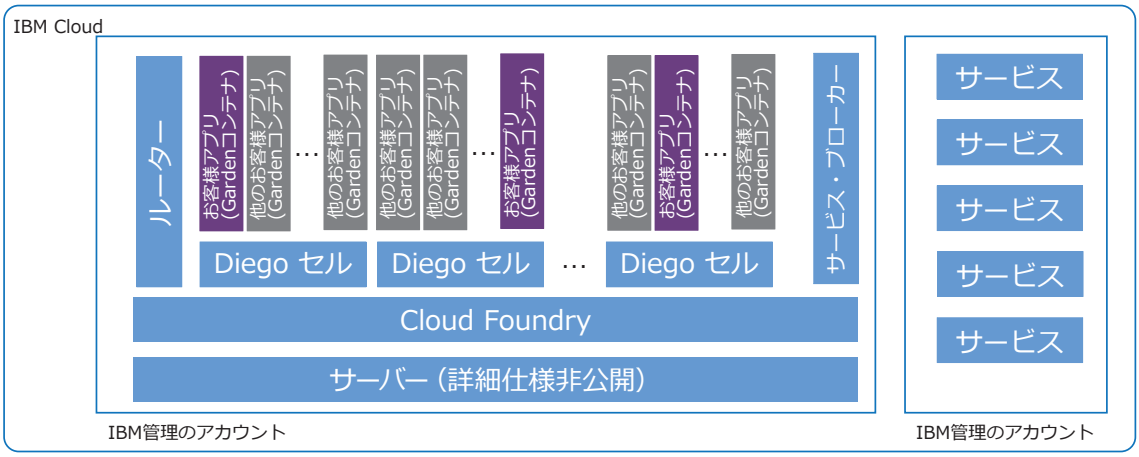
以下のコマンドで利用可能なビルドパックの一覧を取得できます。

```
> cf buildpacks
```

Cloud Foundry Public

Cloud Foundry PublicはマルチテナントのPaaS環境。

Cloud Foundry PublicはIBMがフルマネージドで提供する環境です。
• IBM管理のアカウント内部で稼働し、お客様はお客様アプリケーションの管理を行う責務を持ちます。



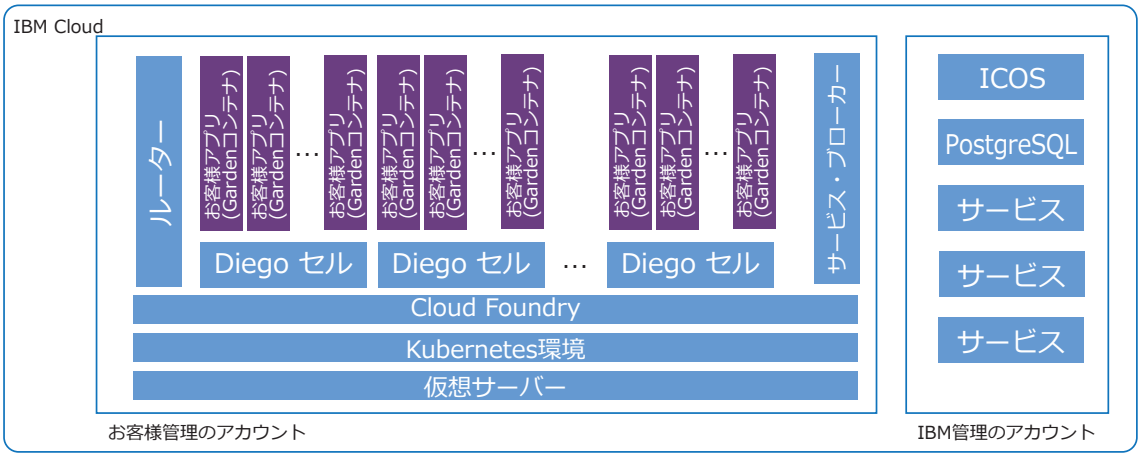
・メンテナンス等を考慮し、アプリケーション・インスタンスは必ず複数インスタンスで稼働させるようにします。複数インスタンスで稼働 させた時には、可能な場合IBM Cloudリージョンの複数ゾーンに分散配置されます。
・アプリケーションにアクセスする際のIPアドレスは可変なので、IPアドレスによるアクセス制限等は単独では実施できません。Cloud Internet Servicesサービスとカスタムドメイン機能を用いることで実施可能です。
・プライベートIPアドレスを用いたアクセスは不可です。

Cloud Foundry Enterprise Environment(CFEE)

Cloud Foundry Enterprise Environmentはシングルテナントの PaaS環境。

Cloud Foundry EnterpriseはIBMがマネージドで提供するCloud Foundry環境です。

- お客様管理のアカウント内部で稼働し、お客様はお客様アプリケーションの管理を行う責務を持ちます。
- お客様管理のアカウントに紐づくネットワーク等のインフラストラクチャー部分はお客様も管理の責務を負います。

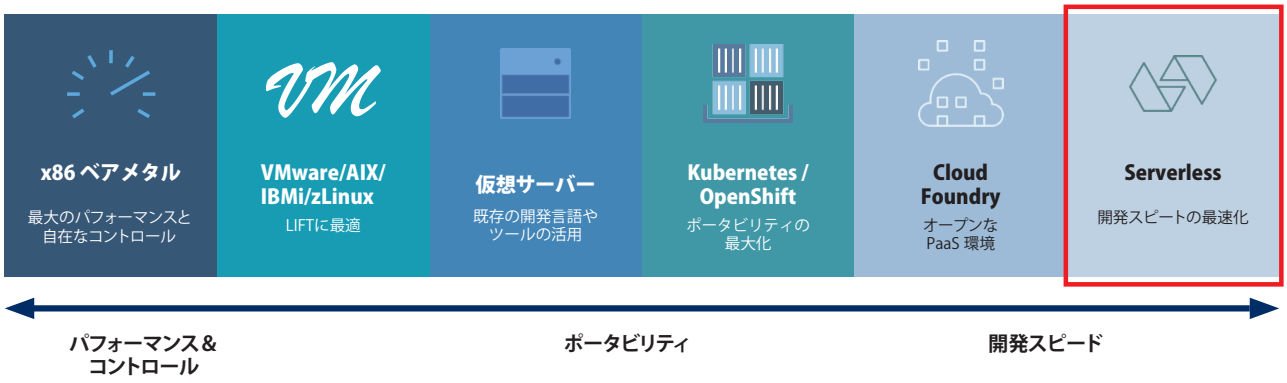


- Cloud Foundry Enterprise環境はKubernetesサービス(IKS) 上で稼働します。
- メンテナンス等を考慮し、アプリケーション・インスタンスは必ず複数インスタンスで稼働させるようにします。複数インスタンスで稼働させた時には、可能な場合IBM Cloudリージョンの複数ゾーンに分散配置されます。
- Kubernetes環境の制約でセキュリティ・グループ機能をご利用いただくことはできません。
- プライベートIPアドレスを用いたアクセスも可能です。

7-3. IBM Cloud Functions

IBM Cloud Functions概要

IBM Cloud FunctionsはIBM Cloudが提供する、イベント駆動型のFaaS (Function as a Service)実行環境です。
Apache OpenWhisk をベースに、マネージド・サービスとして提供されています。



主な特長：

サーバーの管理・運用が不要（サーバーレス）

- 実行したい関数（アクション）と、実行する条件（トリガー、ルール）を指定

効率的なコストモデル

- 関数が実際に実行した時間（0.1秒単位）での課金
- 待機中のインフラコストは不要

柔軟なスケール

- リクエストの数に応じて無限にスケール
- キャパシティプランニングを簡素化

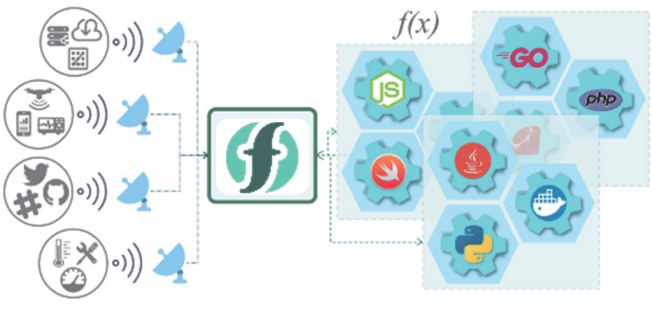
Dockerベース

- アクションはDockerコンテナとして実行される
- デフォルトで対応していない言語も、Dockerコンテナを利用することで対応可能

https://cloud.ibm.com/functions/

2019年8月現在、以下のリージョンでご利用いただけます。

- ダラス
- ワシントンDC
- ロンドン
- フランクフルト
- 東京

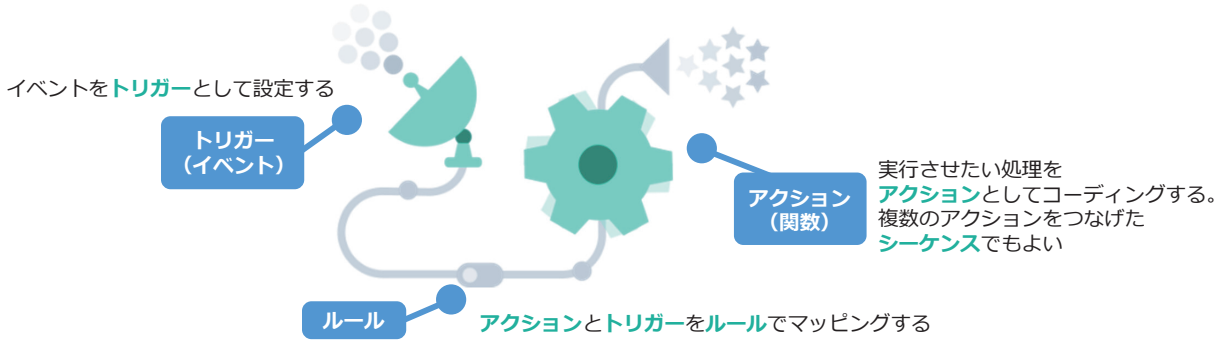


※FaaSと、IaaSやPaaSとの違いについてはDocsの比較表を参照してください
https://cloud.ibm.com/docs/openwhisk?topic=cloud-functions-faas

IBM Cloud Functionsで出てくる用語

https://cloud.ibm.com/functions/learn/concepts

用語	説明
アクション	何らかのトリガーが起動した際に実行されるコード・スニペット。 ソースコードまたは Docker イメージとして登録する。 アクションを直接 REST API 経由で呼び出すことも可能。
トリガー	特定のイベント（例：DB の更新や HTTP リクエスト）に対するチャネル。 具体的なイベントが発生すると、対応するトリガーが起動する。
ルール	トリガーとアクションの関連付け。 トリガーが起動すると、ルールに従って紐付けられたアクションが呼び出される。
シーケンス	複数のアクションが直列に接続されたもの。 先頭から順にアクションが実行され、先に実行されたアクションの出力が次のアクションの入力となる アクションと同様に REST API 経由やルールでと紐付けて呼び出せる。

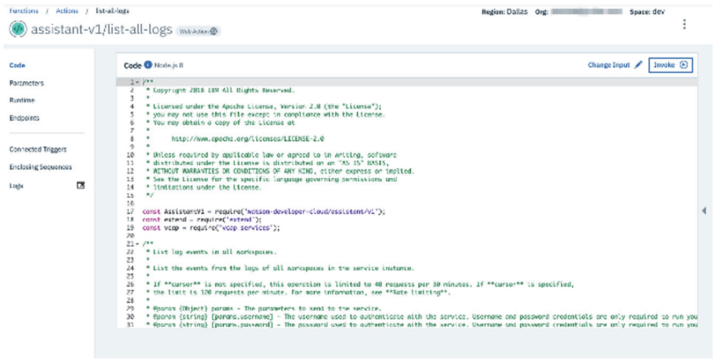


IBM Cloud Functionsの開発インタフェース

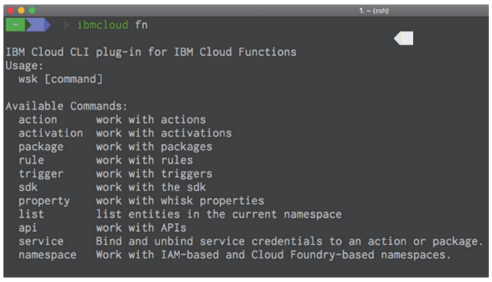
https://cloud.ibm.com/functions/learn/cli

IBM Cloud Functionsでアプリ開発を行うためのインタフェースとして、ブラウザー上のWebIDEとCLIの2種類があります。
アプリに複数のファイルや依存関係がある場合はZIP形式にパッケージ化し、CLI経由でアップロードします。

Webブラウザー（WebIDE）



CLI（ibmcloud fnコマンド）



※一部のランタイムにはデフォルトで利用可能なパッケージがインストールされており、WebIDE上から呼び出し可能です。
https://cloud.ibm.com/docs/openwhisk?topic=cloud-functions-runtimes

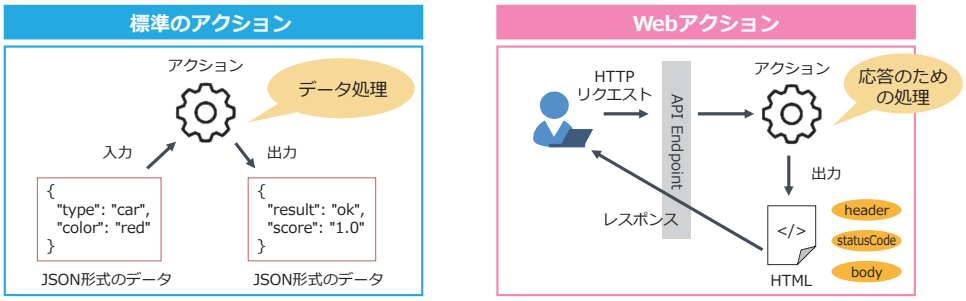
IBM Cloud Functionsでのアクションの開発

https://cloud.ibm.com/docs/openwhisk?topic=cloud-functions-runtimes

・IBM Cloud Functionsでは以下の言語/ランタイムを使って開発できます。
ランタイムによって、GUIでも開発できるものとCLIでしか開発できないものがあります。

- Node.js
- Python
- Swift
- PHP
- Go
- Ruby
- Java（CLI のみ）
- .NET Core（CLI のみ）
- Docker（CLI のみ）

・アクションはインプット/アウトプットともにJSON形式である必要があります。
・「Webアクション」にするとアクションを実行するための資格情報が不要なURLが発行されます。
また、レスポンスにヘッダーやボディーを含めることができるようになります。



IBM Cloud Functionsと組み合わせられるサービス

パッケージの利用

IBM Cloud Functionsには一部のサービスに対してパッケージが用意されています。
パッケージには、サービスを操作するためのアクションや、トリガーとして設定できるイベントが定義されています。

Alarm / Cloudant / Event Streams / Push Notification / Weather / Object Storage / Github / Slack

Watson Assistant / Discovery / NLC / NLU / Personality Insights / Speech to Text / Text to Speech / Tone Analyzer

Language Translator / Visual Recognition / Utility / Websocket

トリガー

・IBM Cloud Functionsのトリガーとして以下のイベントを設定可能です。

Alarm (Periodic)
指定の時刻・実行間隔を過ぎたら

Cloudant NoSQL Database
データベースに対し、ドキュメントが作成・更新・削除されたら

Event Streams
指定のトピックにメッセージがPublishされたら

Push Notification
デバイスのアクティビティー(登録、登録解除、購読、購読解除）が発生したら

GitHub
指定のリポジトリーに対しpushなどのイベントが発生したら

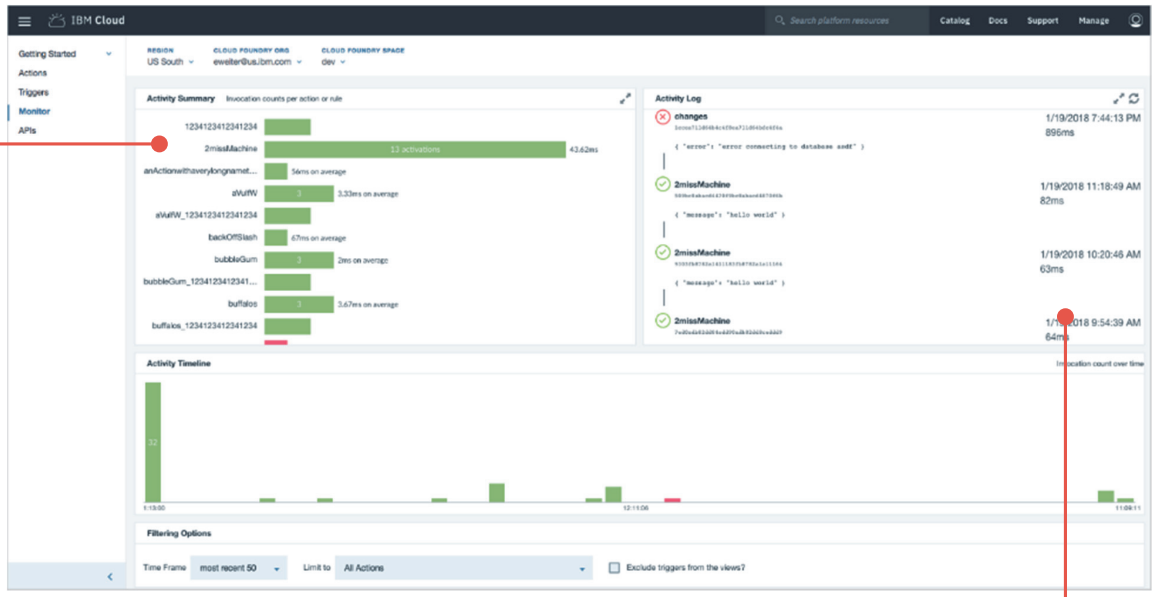
Object Storage
指定のバケットに変更（アップロード、編集、削除）が発生したら

カスタム・トリガー
特定のRESTエンドポイントにPOSTされたら

実行結果の確認

「モニター」画面で、アクション／ルールの呼び出しカウント数や所要時間、出力結果の確認ができます。

アクション／ルールごとの呼び出しカウント数と平均所要時間（請求対象）を表示



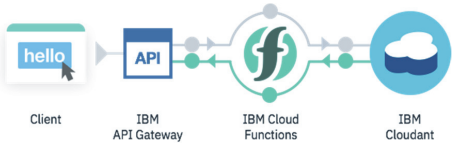
実行したアクションの出力・実行時刻・課金対象となる所要時間を一覧表示

APIゲートウェイ

作成したアクションをAPIゲートウェイ経由で外部に公開できます。

機能：

- **認証・認可**
  - APIキー、APIシークレット(オプション)での認証/認可
  - OAuthでの認可(App ID, Google, GitHub, Facebook)
- **レート制限**
- **CORS対応**
- **利用状況のモニタリング**
  - APIコール、エラー、レスポンスタイム
- **API Explorerによるテスト**
- **Swagger/OpenAPI 定義書のアップロードも可能**



https://cloud.ibm.com/docs/services/api-management?topic=api-management-manage_openwhisk_apis

取扱注意

APIゲートウェイ機能は東京リージョンでは利用できません。

● 制限事項

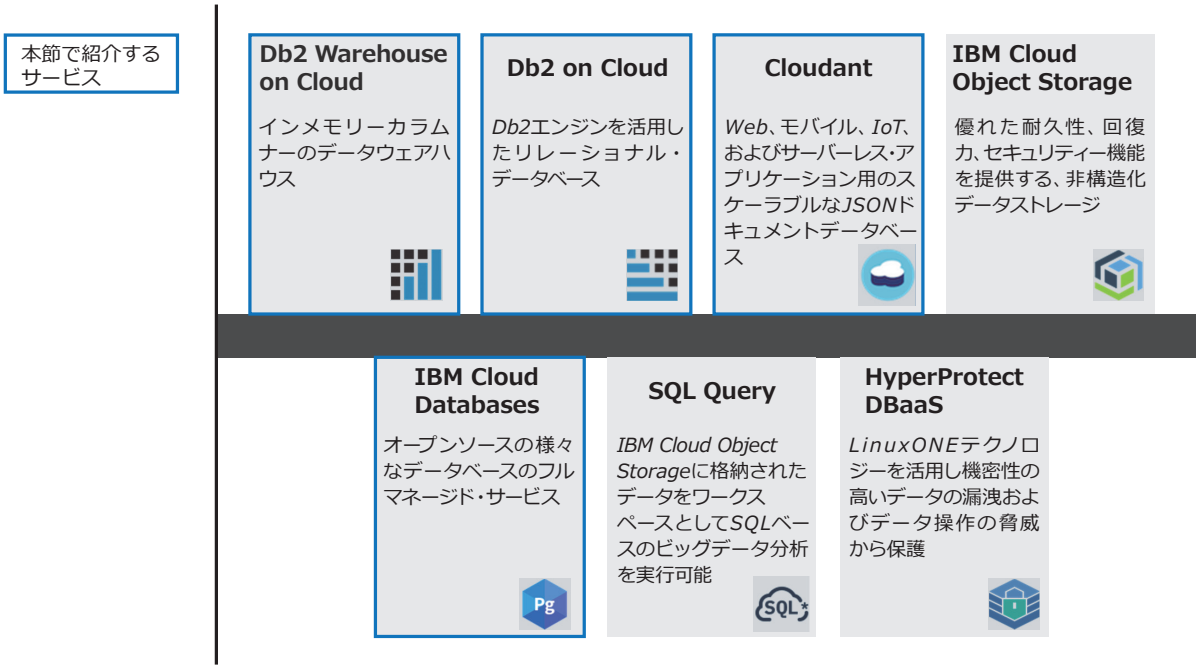
https://cloud.ibm.com/docs/openwhisk?topic=cloud-functions-limits

IBM Cloud Functionsには以下のシステム制限があります。

リソース	デフォルト	制限
アクションのタイムアウト	60000 msec	100 – 600000 msec
アクションのメモリ割り当て	256 MB	128 - 2048MB
アクション・コードのサイズ	48 MB	1 – 48 MB
アクションに付加できるパラメーターのサイズ	5 MB	0 – 5 MB
同時に起動できるアクションの数	1000	1 - 1000
1 分間に呼び出せるアクションの数	5000	1 - 5000
アクションのログサイズ	10 MB	0 – 10 MB
Docker アクションのオープン・ファイル数 (--ulimit nofile=1024:1024)	1024	0 - 1024
Docker アクションで使えるのプロセス数 (--pids-limit 1024)	1024	0 - 1024
アクションの呼び出し結果の出力サイズ	5 MB	0 – 5 MB
1 つのシーケンスを構成するアクションの数	50	0 - 50

7-4. 主なデータストア・サービス

● IBM Cloud で利用可能な主なデータストア・サービス



マネージド・データベースの作業分界点

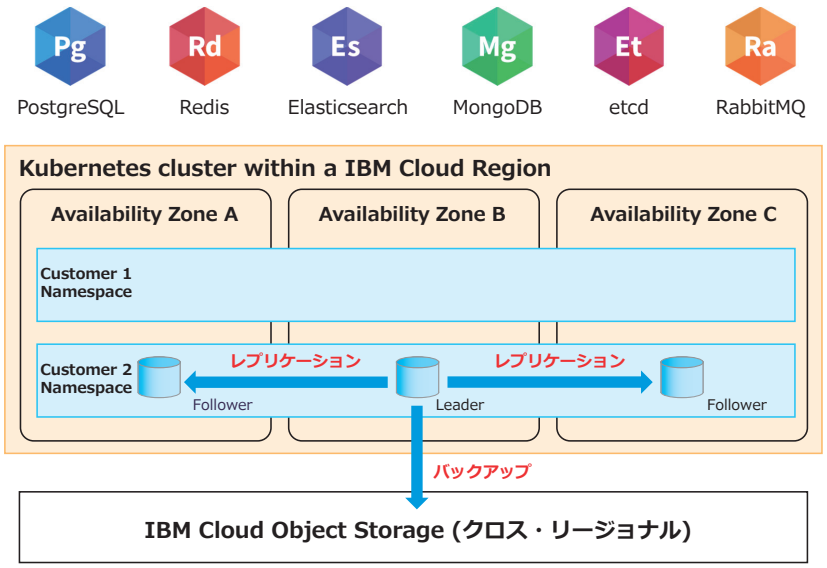
作業項目	作業主体
環境構築 (ハードウエア , OS, ネットワーク)	IBM
24時間のモニタリング	IBM
バックアップ	IBM
新機能の適用 (kernel updates, Webコンソールの新機能など)	IBM
OSやデータベースのパッチ適用	IBM
データモデル作成やユーザー管理	利用者
BIツールや ETLツールからの接続	利用者
データのロード	利用者
アプリケーション開発	利用者
セキュリティ管理	利用者
セキュリティが企業のガイドラインを遵守しているかの確認	利用者

IBM Cloud Databases (ICD)

IBM Cloud Databasesは、オープンソースのデータベースのフルマネージド・サービス(DBaaS)です。

特徴:

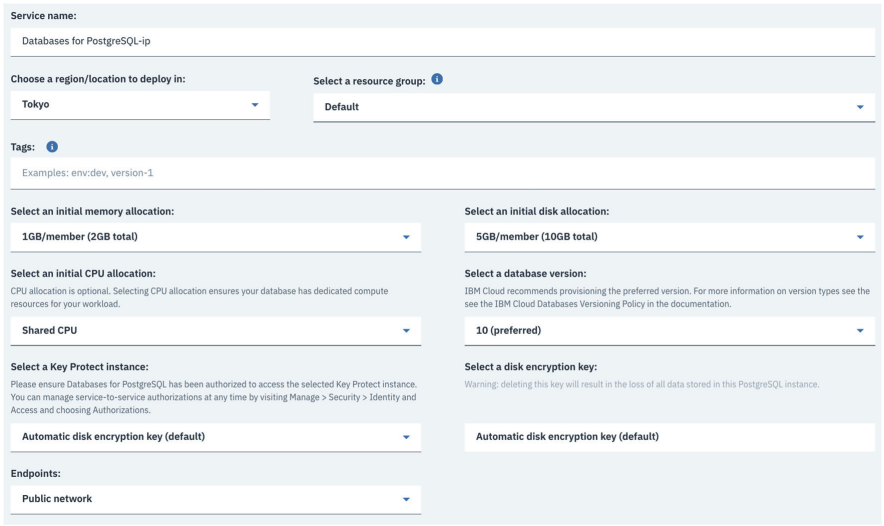
- IBMが管理するIKS上でサービス提供
- Uptime SLA 99.95%の高可用性構成
- デフォルトでMZRに分散配置(データベースの種類ごとに2メンバーまたは3メンバーで構成)
- シンプルな接続のための1つのエンドポイント
- クロス・リージョナルのCloud Object Storageに自動バックアップ
- メンバー間は非同期レプリケーション
- 障害時は自動でフェイルオーバー(30秒以内に切り替え)
- ストレージには10 IOPS/GBのEndurance Storageを利用



IBM Cloud Databases（ICD）で選択可能なオプション

以下の項目を選択可能

- デプロイするリージョン
- メモリとディスクサイズ
  - データベースごとに最小割り当て量が決まっている
- CPU コア
  - 共有または専有を選択
  - 専有の場合はメンバーに何コア割り当てるか選択
- バージョン
- ディスクの暗号鍵
  - Key Protectサービスと組み合わせて利用
- エンドポイント
  - パブリック/プライベートを選択
  - プライベートを選択する場合はCSEを有効化する必要がある



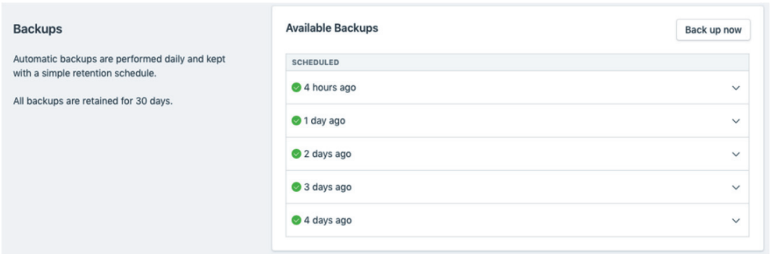
IBM Cloud Databases（ICD）バックアップとリストア

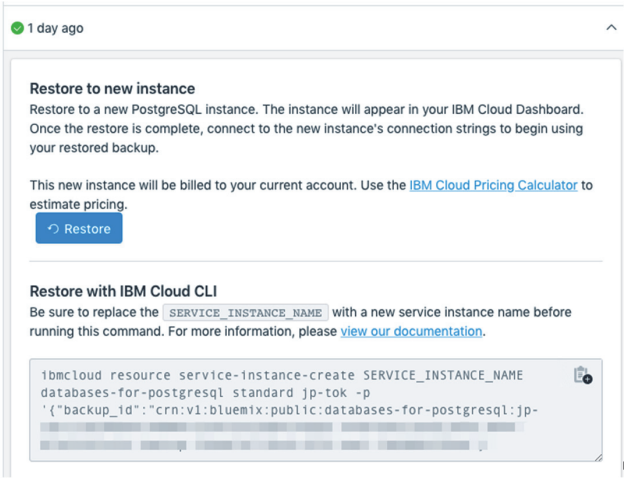
バックアップ

- 日次で自動バックアップ
- 任意のタイミングで取得も可能
（ダッシュボード、API、CLI）
- データはクロスリージョナルのICOSに保管
- 保存期間は30日
- バックアップ時にデータは圧縮
- DBインスタンス全体のサイズと同サイズまでストレージ料金が無料
- バックアップは削除不可

リストア

- ダッシュボードまたはCLI経由でリストア
- リストアすると新規インスタンスが作成される
- 直近7日のPITR（Point-in-Timeリカバリ）にも対応
（PostgreSQLのみ）
- クロスリージョンのリストアも可能





IBM Cloud Databases（ICD）スケールとアクセス制御

コンソールやAPI、CLIからリソースのスケールが可能

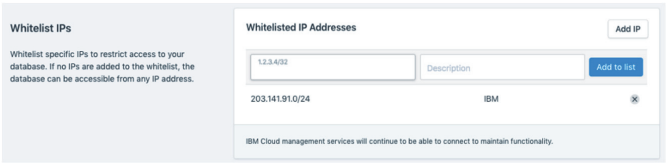
メモリ
- スケールアップ/ダウンが可能

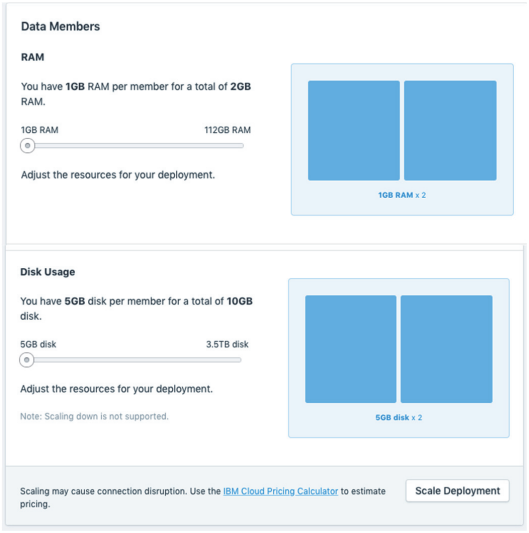
ストレージ
- スケールアップのみ
- ディスク容量を少なくしたい場合は
  新規インスタンスを作成して対応

CPU
- 専有CPUプランを選択している場合のみ、
  スケールアップが可能

アクセス制御

IP ホワイトリストによるアクセス制御が可能





取扱注意

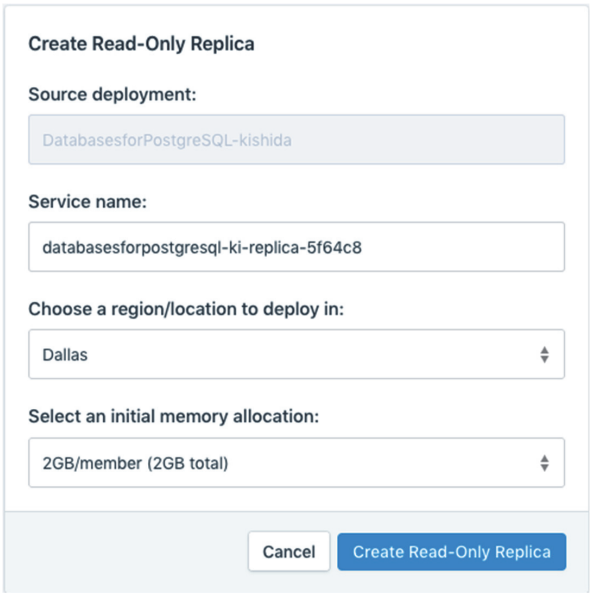
オートスケールは未対応です

IBM Cloud Databases（ICD）リードレプリカ

読み取り専用のレプリカDBを作成可能（PostgreSQLのみ）

特徴：
- ソースDBの負荷軽減
- DR用途としても利用できる
- 同一/別リージョンどちらでも可能
- リーダーと非同期レプリケーション
- リーダーと同じ資格情報で操作可能

制約
- メジャーバージョンはリーダーと同一にする必要がある
- リードレプリカに対するバックアップは取得されない
- IPホワイトリストとの共存はできない
- 東京で作成した場合、EUリージョン（eu-de）には配置
  できない
- リードレプリカは5つまで
- リーダーと同期してスケールしない
- リードレプリカのディスク容量は作成時に自動で計算



IBM Cloud Databases（ICD）バージョニングポリシー

メジャーバージョンへの対応ポリシー
- メジャーバージョンは少なくとも３年間サポート

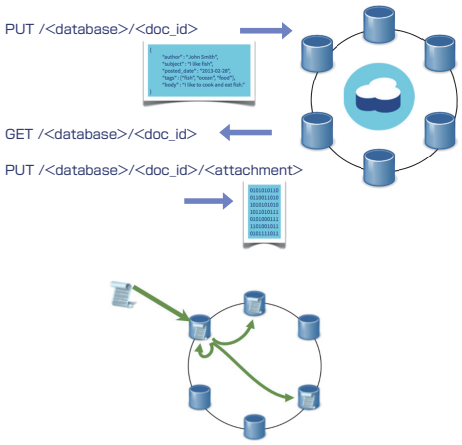
Deprecatedになったときのポリシー
- 利用バージョンがDeprecatedになると利用者に対して通知される。
  通知後30日が経過すると、非推奨バージョンの新規デプロイができなくなる。
- その後、6ヶ月間の移行期間が与えられ、ユーザーはその間の好きなタイミングで移行できる。
  期間内であれば非推奨バージョンへの切り戻しも可能だが、移行期間を過ぎるとバックアップ
  がとられ既存インスタンスにはアクセスできなくなる。
  バックアップは新しいバージョンにのみリストア可能。

Cloudant NoSQL DB 概要

Cloudant NoSQL DBは、マネージド・サービスとして提供するドキュメント型のNoSQL DBです。

特徴:

- ドキュメント指向型DB
  - データはJSON形式で記述される
  - 柔軟にスキーマの変更が可能
- Apache CouchDB ベース
- HTTP APIおよびWebインターフェースを通して利用
- すべてのデータはクラスター内の3つの別々の物理サーバーに三重化されて保管
- マスター マスタ型でノード障害時もサービスを継続可能
- 集計・分析処理はMapReduce技術を使い、高速な並列処理が可能
- データはバージョン管理(MVCC)されており、更新の順番を保証



APIの種類とスループットキャパシティー

https://cloud.ibm.com/docs/services/Cloudant?topic=cloudant-pricing

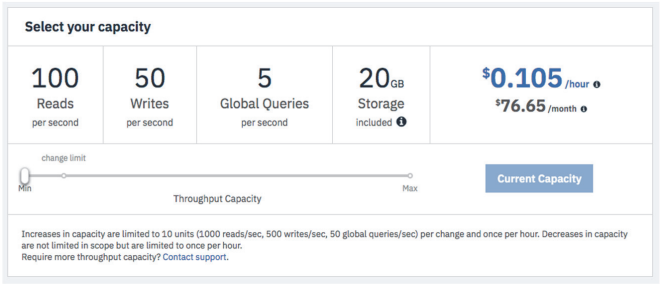
Cloudantは呼び出すAPIの種類ごとにそれぞれキャパシティーが設定されます。キャパシティーはダッシュボードから柔軟に変更できますが、個別に設定できるわけではなく、3つのAPIが連動した組み合わせでしか設定できないので注意が必要です。

APIの種類(3種類)

- Read(旧称:Lookup)
  - _idベースで特定のドキュメントを読み込む操作
  - 以下に対するpartition query
    - Primary Index (_all_docs)
    - MapReduce View (_view)
    - Search Index (_search)
    - Cloudant Query (_find)
- Write
  - 個別のドキュメント書き込み(作成・変更・削除)
- Global Query
  - partition queryではない以下の操作
    - Primary Index (_all_docs)
    - MapReduce View (_view)
    - Search Index (_search)
    - Cloudant Query (_find)
    - Geospatial Index (_geo)

スループットキャパシティー

- 「100 reads/sec、50 writes/sec、5 global queries/sec」の組み合わせの単位で増減可能(Standard プランのみ)
- キャパシティーを超過しようとすると、HTTP 429 が返ってくる



Cloudantで利用可能なAPI

Cloudant では、複数の種類のクエリー機能が用意されています。

CRUD – Document	Primary Index	Secondary Index (view)	Search Index	Geospatial Index	Cloudant Query
					
•ドキュメントのCRUD操作	•ドキュメントの主キーに基づくクエリー •デフォルトで作成される	•MapReduceに基づくクエリー •集計・Gorupなど •ユーザーカスタマイズ可能	•Luceneを用いたデータベース内ドキュメント検索機能 •ランク付き検索、フレーズ、ワイルドカード、ファジー検索、範囲検索など。	•地理情報データ用のクエリー •境界ポリゴン、長方形、円/楕円を使用した照会 •最近接分析や予測経路分析を実行可能 •座標参照系 (CRS) をサポート	•データの条件に応じた宣言的なクエリー •MongoDBに似た使いやすいクエリ

Cloudantにおけるデータの構造

Cloudantでは、「_id」と「_rev」キーを持つJSON形式のデータをドキュメントとして扱います。

・_id (必須、作成時にのみ指定が可能)
  ・データベース内でユニーク(一意的)である必要がある
  ・明示的に指定しなければ、Cloudantにより自動的に文字列が割り当てられる

・_rev (必須、ユーザーによる値の書き換えは不可)
  ・MD5ハッシュ値
  ・_revの先頭の値はドキュメントの更新回数を表す
  ・ドキュメントの更新をする場合には、最新の_rev値を指定する必要がある

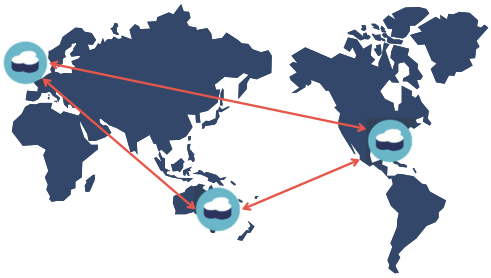
```
{
  "_id": "nodered-imaz-003/flow",
  "_rev": "1-1d8d5704d6f1b223bc57104e0a2ae2c1",
  "user": "IBM"
  "message": "hello!"
}
```

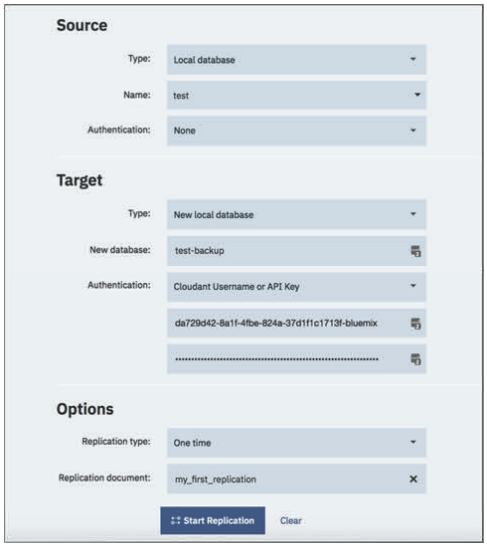
JSON形式であれば、_idと_rev以外は任意に設定できる

Cloudant - レプリケーション

Cloudant では、データベース間のデータ同期を容易に設定できます。
これにより離れた地域でもデータを同期でき、地域的冗長化を実現できます。

・SourceとTragetを指定してレプリケーションを設定
・レプリケーションは単発あるいは継続的(continuous)を選択
・SourceとTargetを入れ替えて相互にデータ同期を行う
「双方向レプリケーション」も可能





IBM Cloud で利用できるDb2系サービス

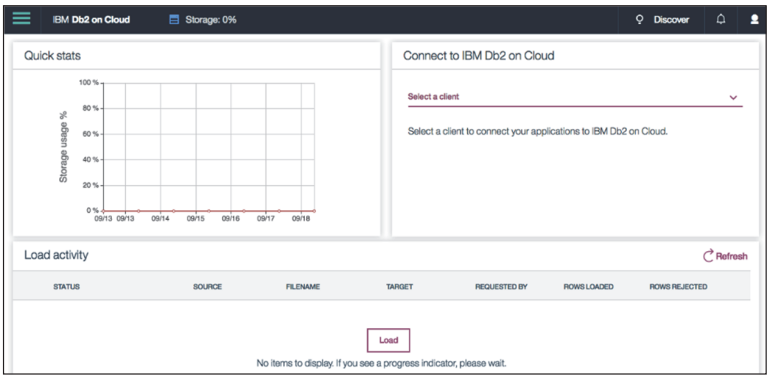
製品・サービス名		Db2	Db2 Hosted	Db2 on Cloud (*)	Db2 Warehouse on Cloud
主な用途	OLTP	○	○	○	※OLTPに強い行表も作成可能
	OLAP/DWH	○	○	※DWHに強い列表も作成可能	○
提供形態		ソフトウェア（含むDockerコンテナ）	クラウドサービス	クラウドサービス	クラウドサービス
課金		ソフトウェア・ライセンス＋保守	従量課金	従量課金	従量課金
インフラ		•お客様準備のHW •クラウド（IBM, AWS,MS等あらゆるクラウド）	IBM Cloud AWS	IBM Cloud	IBM Cloud AWS
運用	HW	お客様	IBM	IBM	IBM
	OS	お客様	IBM	IBM	IBM
	DB	お客様	お客様	IBM	IBM
	アプリ	お客様	お客様	お客様	お客様

(*) IBM Cloud 上ではDb2というサービス名で提供中ですが、SW版との区別をするために本資料ではDb2 on Cloudと表記します。

Db2 on Cloud

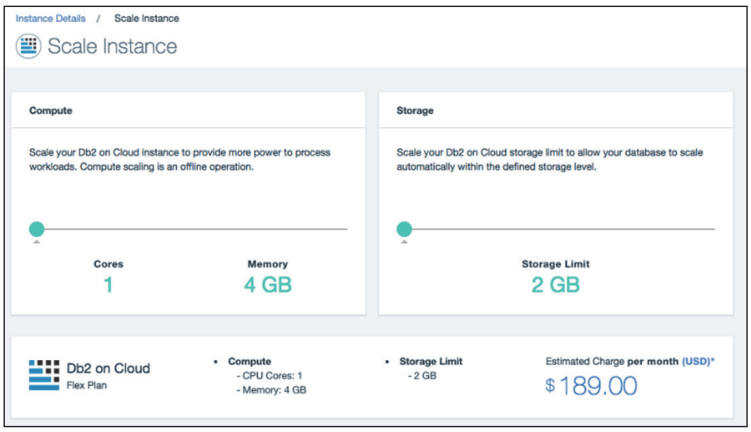
概要:

- フルマネージドのDb2 as a Service
  - IBMがデータベースを24x7x365 管理
- Db2 Enterprise Advanced Edition の機能を利用可能
- スモールスタートが可能なプランを提供
  - Flex プラン(推奨)
    - メモリ、ストレージ、CPU コアを個別に拡張可能
  - Precise Performance プラン
    - 固定のリソースとベア・メタル・サーバーを提供
- 高い可用性と信頼性
  - コンテナベースの環境を提供し復旧時間を短縮。
    クラウドストレージが高い可用性を提供
  - バックアップを自動的に取得
  - HA、DRも構成可能
  - 99.99のuptime SLA を提供（HA構成選択時）
- 他データベースとの互換性
  - Oracle 互換機能を提供
  - ANSI SQL 準拠
  - Microsoft SQL Server, Oracle, MySQL, PostgreSQLに対してのアクセスインターフェースを提供
- Cloud Service EndpointによるPrivate接続が可能

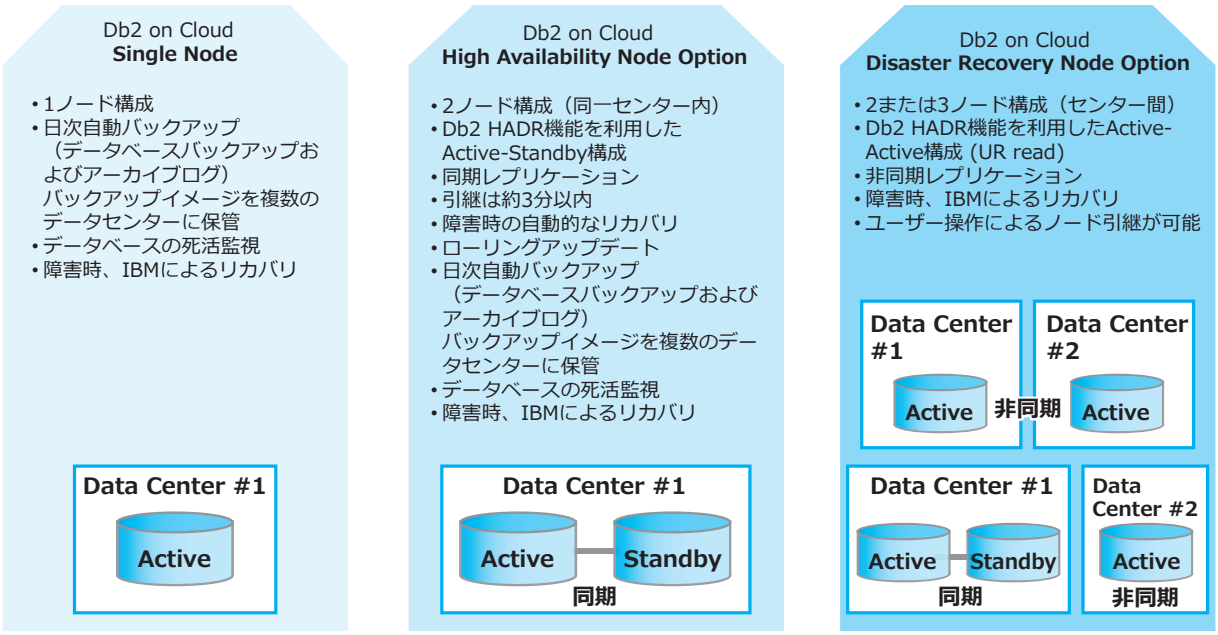


Db2 on Cloud 機能詳細

- Flexプランは1core/4GB メモリー、2GBストレージの小規模環境からスタート
  - リソースはスライドバーで簡単に変更可能
  - ゼロ・ダウンタイムのスケールも可能(要HA構成)
- 自動および任意のバックアップ
  - バックアップは自動的に日次取得
  - 14世代のイメージを保存
- バックアップの冗長化
  - バックアップイメージはICOSに保管され自動的に複数のデータセンターにコピー
- 冗長化構成による安定したサービスを提供
  - ログミラーリングによる冗長化構成（HADR機能によるローカルHAを提供）
  - 障害時にもトランザクションをロスせずスタンバイノードへの引継を完了
- 災害構成により他の地域に引継可能なデータベースノードを構成
  - ローカルの冗長化に加え、万が一の災害時やメンテナンス時のサービス継続のために他地域にもデータベースを構成可能



Db2 on Cloud の高可用性オプション



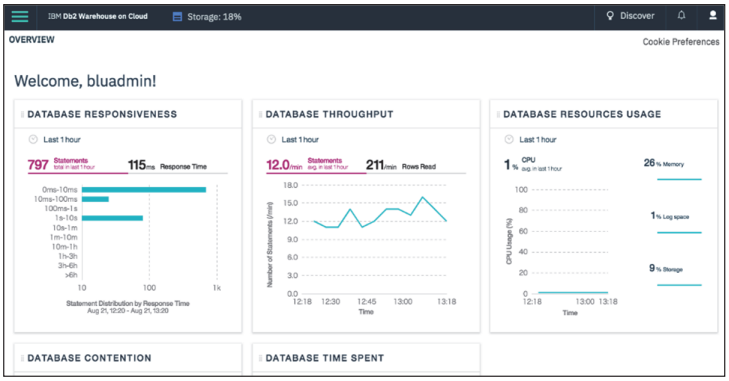
Db2 on Cloud のセキュリティ

- 通信の暗号化
  - セキュアな通信プロトコルとしてSSL/TLSをサポート
- データの暗号化
  - データベース全体を暗号化
  - 暗号化キーは定期的に変更される
  - バックアップデータの暗号化
- アクセス制御
  - ユーザーID/パスワードによる認証
  - ユーザー、グループ、ユーザーの役割に応じてデータの行および列のレベルで細かなアクセス制御を設定可能
- Firewallによるポートスキャンやネットワーク浸入からの保護
- IBM データベース監査製品（Guardium）によるセンシティブ・データへのアクセスモニタリング
- セキュリティ強化のために以下をご提供可能
  - プライベートネットワーク接続
  - Source IP Filtering
    - ホワイトリストの設定、特定のIPアドレスからの接続のみを許可

Db2 Warehouse on Cloud 概要

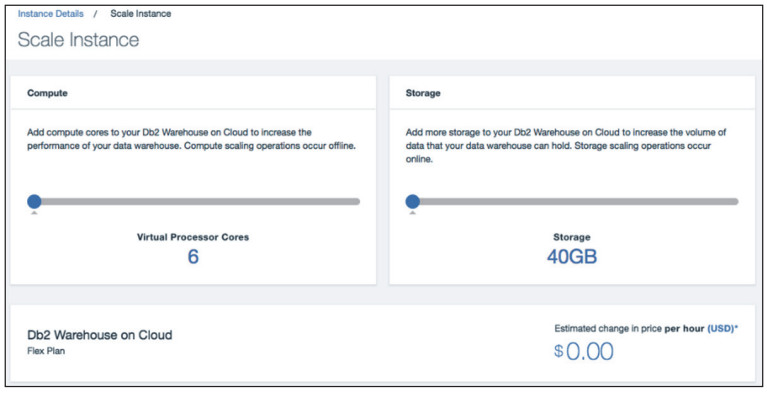
概要:

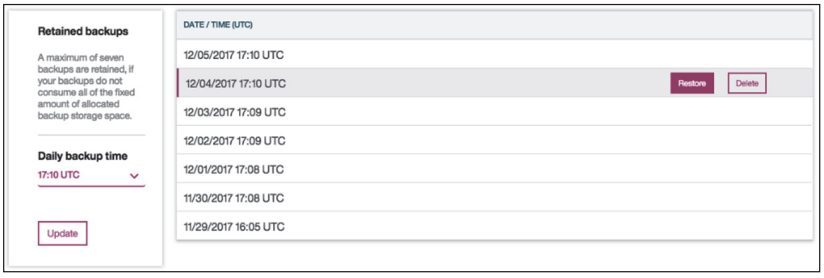
- ハイパフォーマンス
  - 列指向(カラム型)・インメモリーデータウエアハウス
    - 分析・集計などに最適な列指向型でデータを運用
  - ダイナミック・インメモリー
    - 必要なデータセットをメモリーに随時展開し高速処理
  - 圧縮処理
    - データは自動的に圧縮し格納。クエリーは圧縮されたままの状態で処理され、リソースの節約とハイパフォーマンスを両立
  - データスキッピング
    - 要求されるデータの格納場所を把握しピンポイントでデータを取得
    - 最小限のディスクI/Oで最大のパフォーマンス
- ユーザーのニーズに応じたプランの提供
  - 柔軟なリソース拡張が出来るプランやベアメタル環境のプランなど幅広いオプション
- 高い可用性と信頼性
  - コンテナベースの環境を提供し復旧時間を短縮クラウドストレージが高い可用性を提供
  - バックアップを自動的に取得
- 他のデータベースとの互換性
  - Netezzaとの高い互換性を確保
  - Oracle 互換機能を提供



Db2 Warehouse on Cloud 機能詳細

- CPU/メモリおよびストレージを必要に応じて動的に拡張可能
  - リソースはスライドバーで簡単に変更
  - メモリーはCPUコアに合わせてスケール
- 自動および任意のバックアップ
  - バックアップは自動的に日次取得。
  - 7世代のイメージを保存(Flexプラン)
  - ユーザー任意のタイミングでのバックアップも可能
  - 取得したバックアップイメージを用いた復旧も任意のタイミングで即時復旧が可能(1時間以内に復旧)
- バックアップの冗長化
  - バックアップイメージはICOSに保管され自動的に複数のデータセンターにコピー
- 冗長化構成による安定したサービスを提供
  - ノード:
    - ノードはKubernetesサービスで構成障害のあるノードは切り離され、正常なノードを即時復旧
  - ストレージ:
    - SSDベースのRAID6構成で信頼性とパフォーマンスを提供
  - ネットワーク:
    - ネットワークスイッチの二重化で信頼性を確保





Db2 Warehouse on Cloud のセキュリティ

- 通信の暗号化
  - セキュアな通信プロトコルとしてSSL/TLSをサポート
- データの暗号化
  - データベース全体を暗号化
  - 暗号化キーは定期的に変更される
  - バックアップデータの暗号化
- アクセス制御
  - ユーザーID/パスワードによる認証
  - ユーザー、グループ、ユーザーの役割に応じてデータの行および列のレベルで細かなアクセス制御を設定可能
- Firewallによるポートスキャンやネットワーク浸入からの保護
- IBM データベース監査製品（Guardium）によるセンシティブ・データへのアクセスモニタリング
- セキュリティ強化のために以下を提供可能
  - プライベートネットワーク接続
  - Source IP Filtering
    - ホワイトリストの設定、特定のIPアドレスからの接続のみを許可

8

セキュリティ管理

INDEX

8-1. セキュリティの管理概要

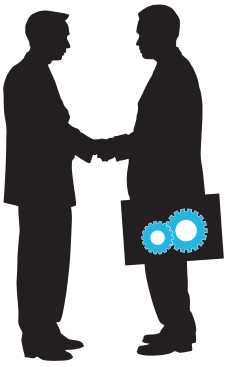
本章では、IBM Cloudにおける脆弱性のテストや防御の方法、脆弱性管理のベストプラクティスについて記載しています。
一般的にクラウドでの脆弱性対策には、暗黙的に実装されるものと、取捨選択の後、利用者が構築もしくは設定する必要があるものがあります。

セキュリティー実装のステップ

1. クラウド業者と利用者間の責任範囲の境界を理解する。
- セキュリティーはIBM Cloud と利用者の共同作業です。
- IBM Cloud が脅威の全てから保護することを保障している訳ではありません。
- 各種の第三者認定は、IBM Cloud の責任部分を保証しています。

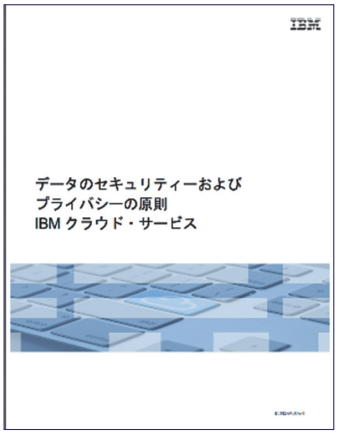
2. クラウド業者の責任内容と取り組みを理解する。
- IBM Cloud(IaaS) の責任範囲は利用者が操作できないデータセンター設備、共用機器等です。
- 運用は人手を介さないよう極力自動化されています。

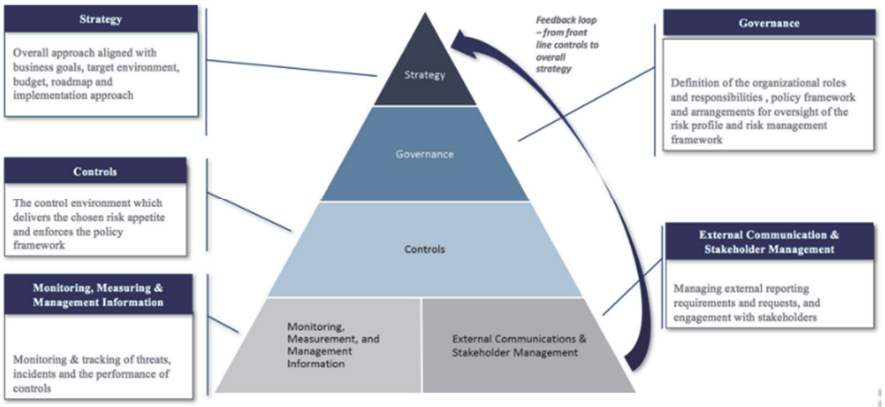
3. 利用者が対応すべき部分に対して、クラウド業者提供の製品・サービスや3rd Party提供の製品サービスを組み合わせて 実装・運用する。
- 必要に応じて適切な製品を持ち込み、対策を行ってください。
- 多層防御での保護が推奨されます。
- IBM Cloud(IaaS) の場合、OS、アプリケーションやデータは、利用者の責任で保護する必要があります。
- 自社運用要員へのセキュリティー教育、セキュリティーポリシーの策定、CSIRTなども利用者側で実施します。


利用者　IBM Cloud

IBM Cloudにおけるセキュリティーの考え方を理解するためのドキュメント

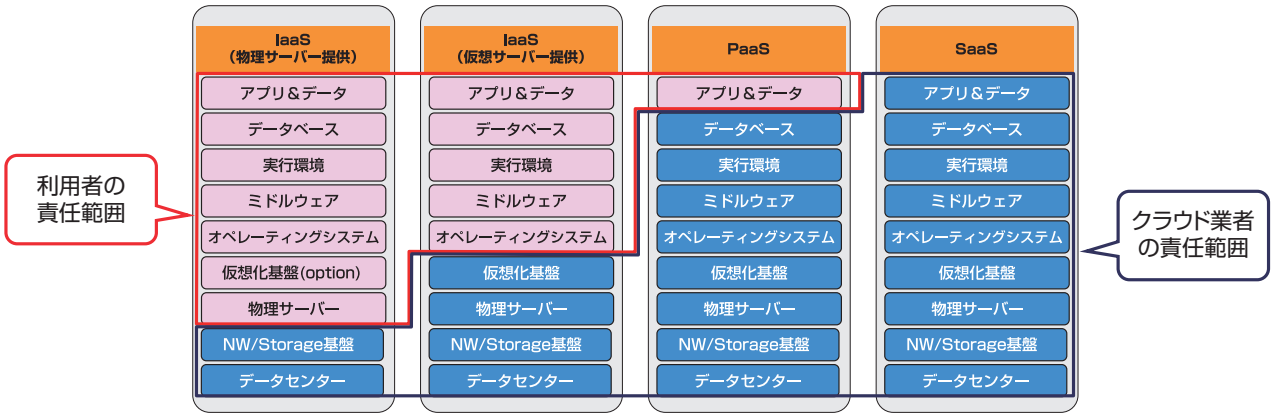
・データのセキュリティーおよびプライバシーの原則- IBMクラウド・サービス
https://goo.gl/xEFfkS
・サービス記述書
https://www-03.ibm.com/software/sla/sladb.nsf/sla/bm-6605-18
・Securing Architecture
https://www.ibm.com/cloud/garage/architectures/securityArchitecture





8-2. 責任分界点

・IaaS/PaaS/SaaSの責任分界点は一般的には下図のようになります。
・これは、責任の境界も同時に表してます。
・権利と義務は表裏一体です。「**xxxはクラウド利用者が自由に変更できる（権利）**」ということは、
同時に「**xxxの構成責任はクラウド利用者側にある（義務）**」ということを指します。



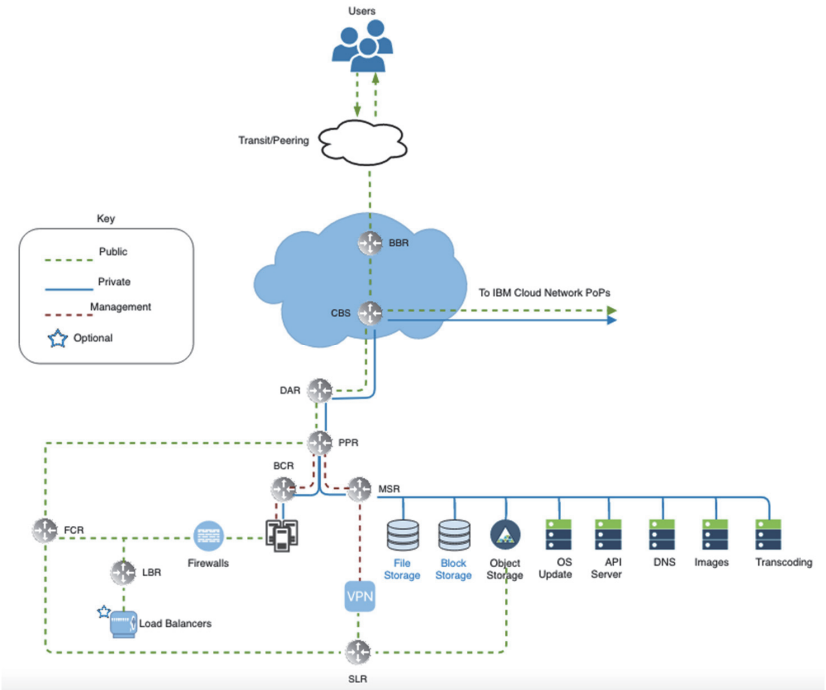
・IBM Cloud IaaSにおけるより細部な責任分界点は下図のようになります。
・基本的な考え方としては、以下の通りです。
　・利用者が操作できる領域は利用者の責任
　・利用者が操作できない領域はクラウド業者の責任

責任項目 ＼ オファリング項目		物理サーバー（専有）	仮想サーバー（専有・共有）
運用・管理	アプリケーションやデータ	利用者	利用者
	OS	利用者	利用者
	ハイパーバイザー	（もしハイパーバイザーを導入する場合は利用者）	クラウド業者
	ハードウェア	利用者: IPMI監視やHW交換要求 BIOS更新要求 クラウド業者: 定期ランプチェック HW交換やBIOS更新の実行	クラウド業者
プロビジョニング	OSの導入	利用者: 要求 クラウド業者: 実行	利用者: 要求 クラウド業者： 実行
	サーバーの準備	利用者: 要求 クラウド業者： 実行	利用者: 要求 クラウド業者： 実行
データセンター管理		クラウド業者	クラウド業者

IBM Cloudネットワークを物理的な観点で表した図です。

https://cloud.ibm.com/docs/services/vmwaresolutions/services?topic=vmware-solutions-design_physicalinfrastructure&locale=en

Reference :
BBR = BackBone Router
CBS = Core Backbone Switch
DAR = Datacenter Aggregation Router
PPR = Pod-to-Pod Router
FCR = Frontend Customer Router
LBR = Load Balancer Router
BCR = Backend Customer Router
MSR = Master Services Router
SLR = SoftLayer Router

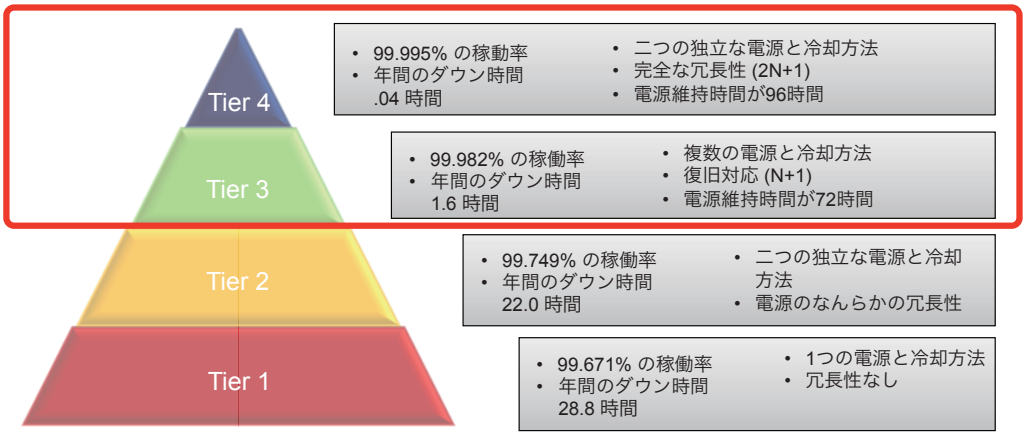


IBM Cloudの責任範囲:
ルーターやスイッチは、IBM Cloudによって構成・管理されており、構成設定・ロギング・パッチがクラウド業者の責任で行われています。

利用者の責任範囲:
利用者のサーバーはVLANに割り当てられています。利用者はVRA(Virtual Router Appliance)等の仮想ゲートウェイやファイアーウォールを配置することでサーバー間の通信を制御したり、サーバー上にセキュリティーソフトを導入することで保護可能です。

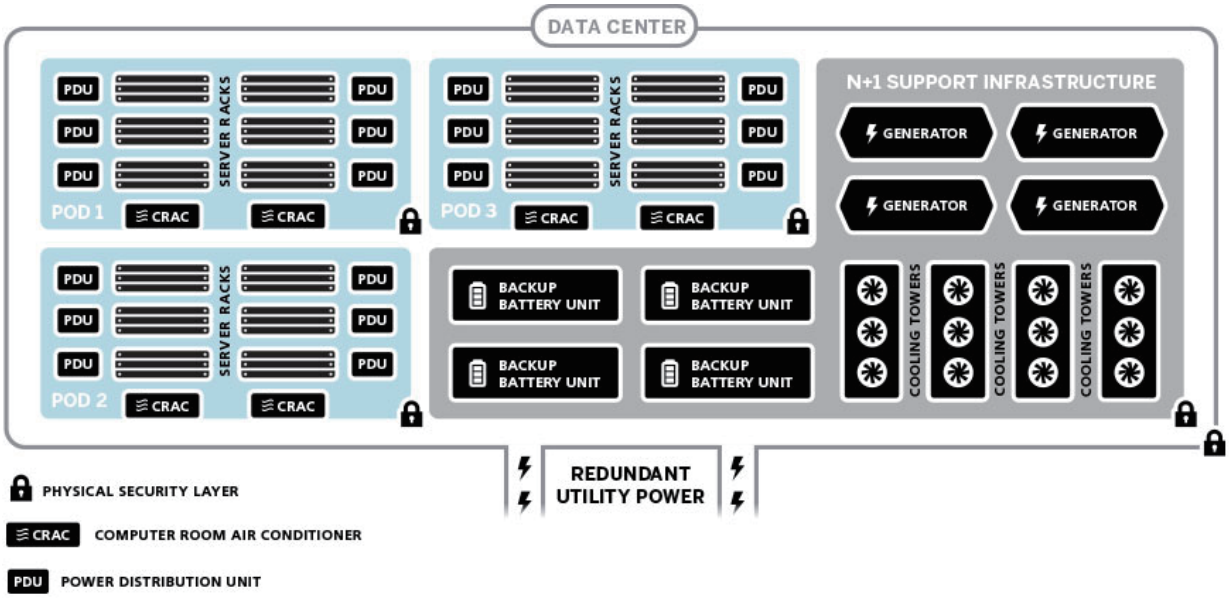
8-3. データセンターセキュリティー

・IBM Cloud DCのセキュリティ管理は、NIST 800-53 frameworkを基準としたUS政府標準に従います。
・Tier3以上のデータセンターを選択し、データセンター内のUPS装置や冷却装置などに冗長性を持たせています。
・SOC2 Type2を初めとした第三者外部認定を取得・拡充に努め、その監査結果や認定情報を公開することで透明性の拡充に努めています。
・エンジニアや技術者は、IBMのセキュリティーガイドラインに従い、BCGにも毎年署名する。およびIBM社員業界標準ポリシーと行動に対して教育が実施され、毎年監査されています。
・災害対策とビジネス継続性のために、IBM Cloudを支える管理システム(IMS)は地理的に分散された冗長性を持ちます。



全てのデータセンターで、"最低限"下記の仕組みを提供する施設を採用しています。

- n+1 UPS Battery Backup Units
- n+1 Backup Power Generators
- n+1 Cooling Infrastructure
- Pre-Action Dry Pipe Fire Suppression
- Multi-Level Access Control

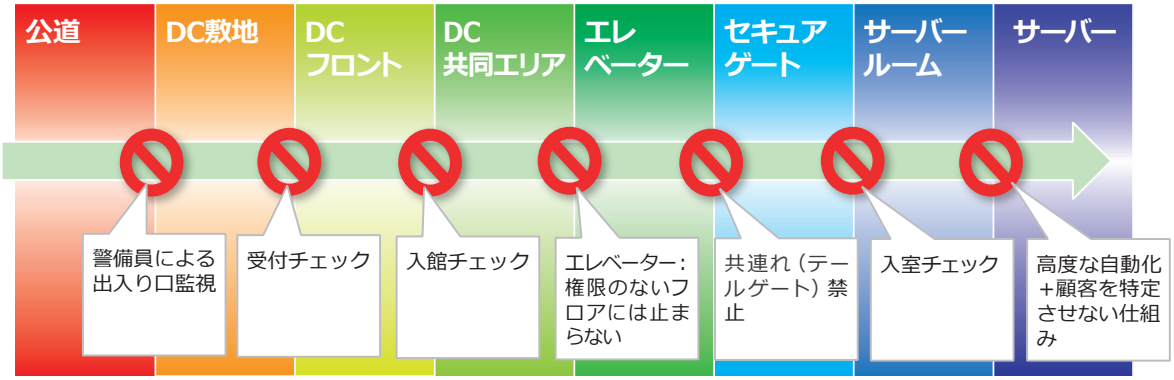


データセンターの入退室管理

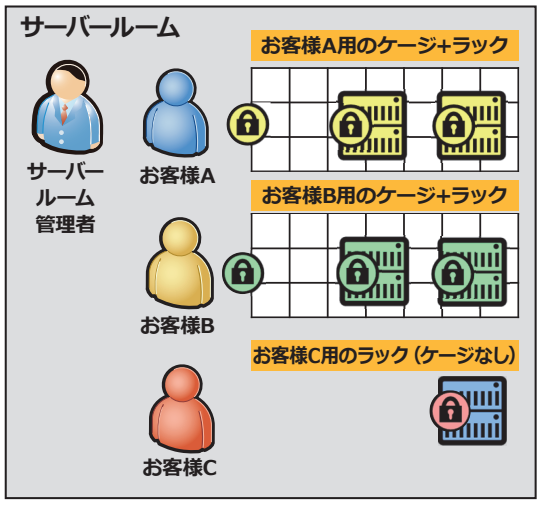
- アクセスコントロールがあり、24時間監視された施設を利用している。
- 生体認証セキュリティが、データセンター全体で利用されている。
- 監視カメラ（CCTV）による監視がされており、ログは少なくとも90日間保存される。

サーバールームの特徴

- 公開エリアに面した出入り口は1つも存在しない。
- 出入り口のドアには、施設を特定できるような表示は出ていない。
- 24時間/365日、スタッフが常駐している。
- デジタルセキュリティビデオによる監視がされている。
- IBM Cloudの従業員とエスコートされた契約者と訪問者に厳格に制限されている。
- 下図は東京データセンターでの例です。

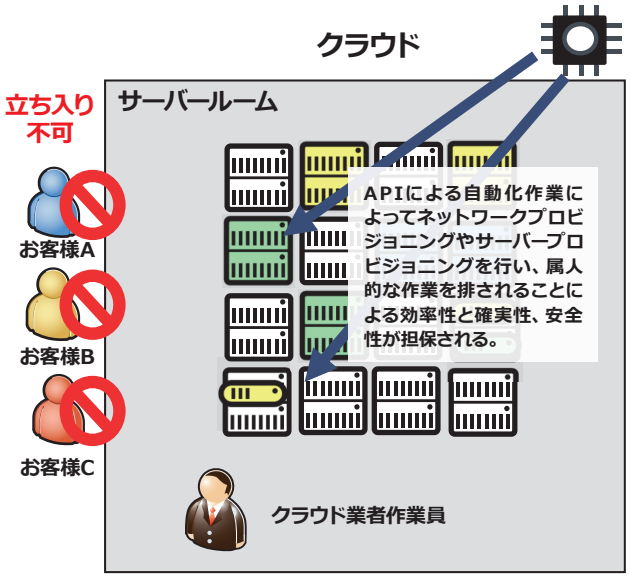


オンプレミス or ホスティング



- 他のお客様もサーバールームに立ち入り可能。サーバー直前まで、他の利用者も物理的に立ち入れてしまうため、ケージやラックの施錠等による保護が必須。
- 外部認証も限定的（一般的には自社内の監査部門による評価）。自社内での甘い評価になるリスクがあり、監査期間もまばら。（3ヶ月に一度、年に１度、等）
- 作業ミスを防止する手段が手順書作成や技術員の教育といった属人的な対応に限定される。（自動化されていない）

クラウド



- 独立した第三者の監査業者のみ立ち入りを許可。お客様ごとの入室は許可しない。
- 第三者による監査業者が継続的に監査を実施（SOC2などの外部監査業者による認証取得）。
- NWプロビジョニングもサーバープロビジョニングもすべて自動化されており、データセンター内の作業員も個々の利用者のサーバーの用途を特定できない。サーバーには、機器を特定するバーコードのみが割り振られており、利用者を特定付ける情報は付与されていない。
- 生体認証を初めとしたアクセス制御、ビデオ監視だけでなく、必ず誰かが常駐。

よくある疑問	答え
IBM Cloud 内の要員に対するセキュリティ教育はどうなっているのか？	・IBM Cloud IaaS の運用をしているのは IBM 社員です。 ・IBM が定める Business Conduct Guideline に従い、IBM のセキュリティ研修も毎年受講していることは、第三者の監査機関からも報告されています（SOC2）。
IBM 社員は誰でも DC に入れるのか？	・DC に入れるメンバーは、（典型的には）各 DC ごとに 17 人～ 23 人の Server Build Tech(SBT) のみです。
DC 内のメンバーに自分達のサーバーを特定付けされてしまうのではないか？	・IBM Cloud はクラウドであり、ホスティングではありません。サーバーには、サーバー名やお客様を特定付けるような情報は付いていません。故障対応などサーバーの物理的な管理のために、バーコードが付与されています。
USB メモリや CD-ROM ドライブを使ったコピーがされてしまうのではないか？	・IBM Cloud の運用ポリシーとして、左記の機材を使ったメンテナンスを実施していません。
クラッシュカートを使って直接サーバーにアクセスして操作されてしまうのではないか？	・IBM Cloud の運用ポリシーとして、左記の機材を使った修正や問題解析を実施していません。
スイッチ上の空きポートにケーブルを挿されることで、持ち込み機器が接続できてしまうことはないのか？	・VLAN はアカウントごとに割り振られ、サーバーがプロビジョニングされた際に初めて構成されます。逆に言うと、プロビジョニングが実施されるまではスイッチ上の VLAN は構成されていませんので、適当な空きポートにケーブルを挿しても接続されません。
キャンセル後のサーバーの HDD を引き抜いてデータがコピーされてしまうのではないか？	・専有サーバーのキャンセルが実施されると、ドライブ消去ソフトウェア（Defense (DoD) 5220.22-m standards）によって、自動的にデータは消去されます。削除に失敗したディスクは物理的に破壊されます。これにより、全ての過去データは新規にプロビジョニングされた専有サーバーのローカルディスクから削除されていることが保証されます。 ・別途有償で、お客様ご自身でディスクを買い取ることができます。ディスクを破壊する場合は、輸送・受領後にお客様ご自身でご対応いただけます。

クラウドのデータセンターに入って
自社のセキュリティポリシーを満たしているかチェックしたい

高度なセキュリティーレベルを担保するため、
サーバールームへの立ち入りは**例外なく禁止**されています。

- 日本のデータセンターの見学はIBM営業経由のリクエストで可能。
- 情報や確認が必要な監査項目は、外部監査レポート（SOC2）から確認可能。
- データセンターの所在地もすべて明示的に公開。

契約上の問題が起きた時はどの国の法律が適用されますか？

日本国法人のお客様が日本アイ・ビー・エム株式会社との間で契約を取り交わした場合は、ご契約いただいたお客様の事業所が存在する国の法律に従うことになっているため、

- 日本国法が適用されます。
- IBM Cloudに関する両者の係争は日本の裁判所にて訴訟が提起されます。

IBM Cloudがもつコンプライアンス認定一覧

共通認定
- CSA STAR
- ISO 9001
- ISO 22301
- ISO 27001
- ISO 27017
- ISO 27018
- ISO 31000
- SOC1
- SOC2
- SOC3

US政府関連
- CJIS
- DoD DISA
- FedRAMP
- FIPS 140-2
- FFIEC
- FISMA
- ITAR

業界別
- FFIEC
- FISC(日本)
- HIPPA
- HITRUST
- ITAR
- PCI

地域別
- IRAP(オーストラリア)
- MTCS(シンガポール)
- マイナンバー法(日本)
- C5(ドイツ)
- European Banking Authority(EU)
- ENISA IAF (EU)
- ENS (スペイン)
- EU Model Clauses
- EU-US Privacy Shield
- GDPR (EU)
- G-Cloud (UK)
- Health Data Hosting (フランス)
- IT-Grundschutz (ドイツ)
- FERPA (US)
- BaFin (US)

https://www.ibm.com/cloud/compliance
https://www.ibm.com/cloud/compliance/global
https://www.ibm.com/cloud/compliance/government
https://www.ibm.com/cloud/compliance/industry
https://www.ibm.com/cloud/compliance/regional

FISC安全対策基準への対応

お客様がクラウドサービスを活用するに当たり、リスク評価の参考にしていただくために、IBM Cloud IaaSに関して『金融機関等コンピュータシステムの安全対策基準解説書』(FISC安対基準)をベンチマークし安全評価した資料を公開。
第三者による支援として新日本監査法人による助言を受けている。

http://www.ibm.com/cloud-computing/jp/ja/softlayer_fisc.html

医療業界向け3省4ガイドライン

医療機関向けIBM Cloud IaaSクラウドサービス対応
セキュリティリファレンス

https://www.mri.co.jp/service/201602_021630.html

政府統一基準やガイドラインに対するセルフチェック

IBMでは、以下の政府統一基準についてセルフチェックを完了しています。
必要な方は、IBMの営業担当者にお問い合わせください。

http://www.nisc.go.jp/active/general/pdf/kijyun28.pdf
http://www.nisc.go.jp/active/general/pdf/guide28.pdf

学認クラウド導入支援サービス参加済

学認クラウドとは、大学・研究機関がクラウドを導入・利用するための支援サービスです。
IBMでは定期的に更新されるチェックリストに対応しています。

https://cloud.gakunin.jp/

JAMA(日本自動車工業会)CAEクラウド活用ハンドブックに対するセルフチェック

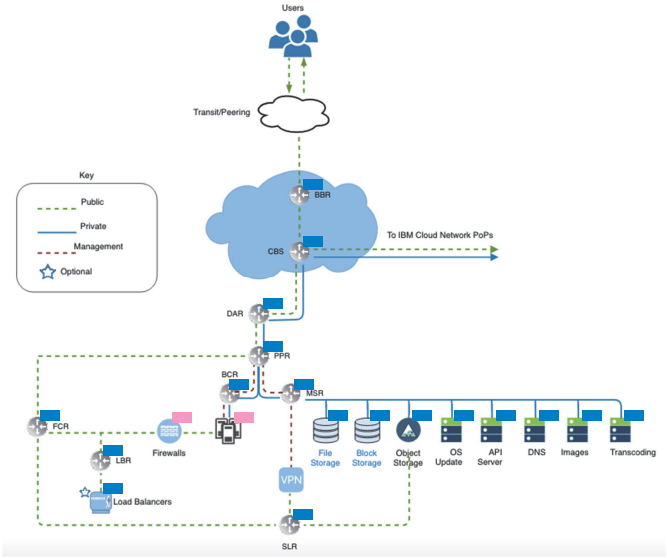
CAE用途でクラウドを利用する際にどのような手順と視点で確認(チェック)する必要があるのかの手引きを記載したハンドブックに対するセルフチェックを完了しています。必要な方は、IBMの営業担当者にお問い合わせください。

http://www.jama.or.jp/cgi-bin/it/download_06.cgi (テンプレートはこちらからダウンロードできます)

8-4. ネットワークセキュリティー

IBM CloudのNW機器やカスタマーポータルへの対応

- VLANによるネットワーク分離
  - IBM Cloud自身が管理するサービスネットワーク用のVLANと利用者のVLANは明確に分離されています。利用者には、他の利用者とは共有しない専有のVLANが割り当てられ、このVLAN上にサーバーが配置されます。
- 脆弱性スキャン
  - Internetに面しているネットワーク機器は、IBMのDigital Threat Risk Assessment(DTRA)チームによって、定期的に脆弱性スキャンを実施しています。このスキャンによって発見された脆弱性に対しては、重要度に応じて変更管理プロセスにしたがって修正されます。
- Firewallルールの再評価
  - Network Engineeringチームは、定期的にファイアーウォールルールの再評価を行っています。そのためのベースラインは、リスク管理に責任を負うVice Presidentの承認に基づいて定められています。
- Penetration Test(侵入テスト)
  - ネットワークの脆弱点を探査し、侵入できるかどうかを調査するテストを実施しています。
- Secure Data Transmission
  - IBM Cloudのカスタマーポータルや APIアクセスは、TLS1.2を利用して利用者端末との間で暗号化を行っています。そのために必要となるSSL証明書を維持・管理しています。



IBM Cloudの責任範囲:

利用者の責任範囲:

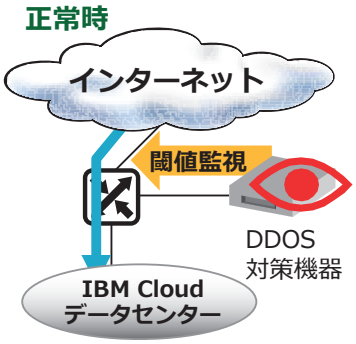
IBM Cloudが標準で備えているDDoS対策の仕組み

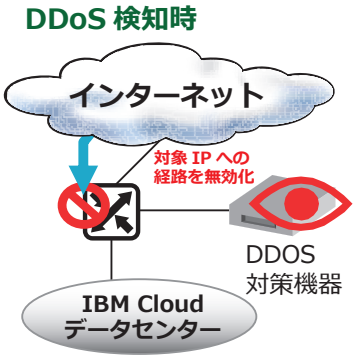
- IBM CloudのDDoS対策は、あるサーバーが攻撃を受けることによってIBM Cloud全体のネットワーク・リソースが逼迫し、直接攻撃を受けていない他のお客様までサービス影響を受けてしまうことを避けることが目的です。

- IBM Cloud自身を保護するためのサービスであるため、利用者ごとのカスタマイズは行なっていません。

- Network Operations Center(NOC)とSecurity Operation Center(SOC)のチームが、IBM Cloudの環境を24/365監視し、問題の特定およびインシデント対応の責任を負います。

- DDoS攻撃を検知した際には、
攻撃対象へのトラフィックをDDoS対策機器へ転送し、問題が解決されたとみなされるまで、そのIPアドレスへの経路を無効化(null route)します。

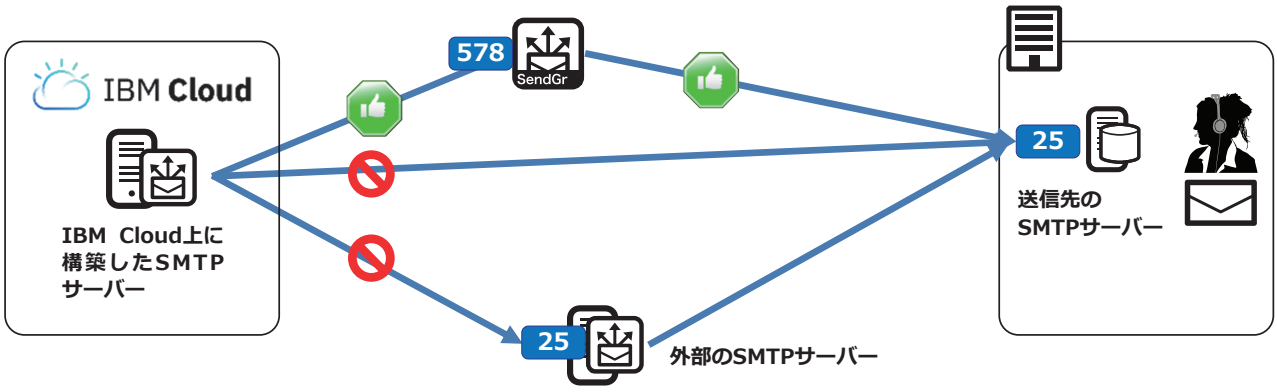




IBM CloudにおけるOP25B(Outbound Port 25 Blocking)対策

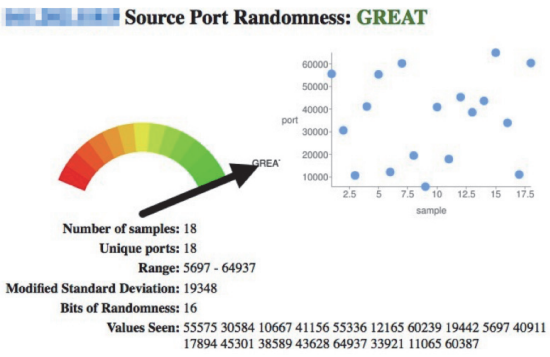
・IBM Cloudは原則Outboundをフィルタリングしません。
・例外としてOP25B(Outbound Port 25 Blocking)対策を行っており、25番ポートへのPublic VLAN経由のOutbound通信はブロックしています。
・IBM Cloudからメールを送信する際には、submission portとして25番以外を利用しているSendGridなどのサービスを利用する必要があります。

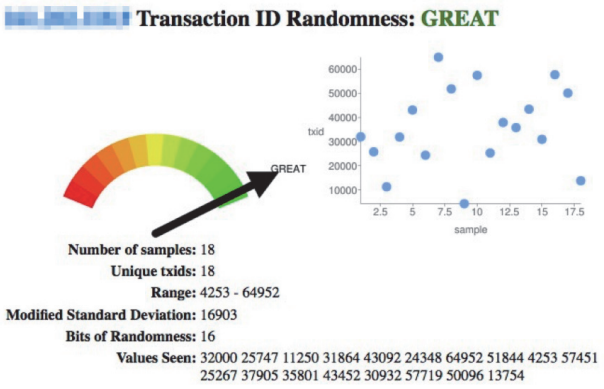
https://cloud.ibm.com/docs/infrastructure/email-delivery?topic=email-delivery-email-delivery-faw



IBM CloudにおけるCache DNSのキャッシュポイズン対策

・Source Port番号のランダム性およびTransaction IDのランダム性の両方において、良好な結果が確認されています。

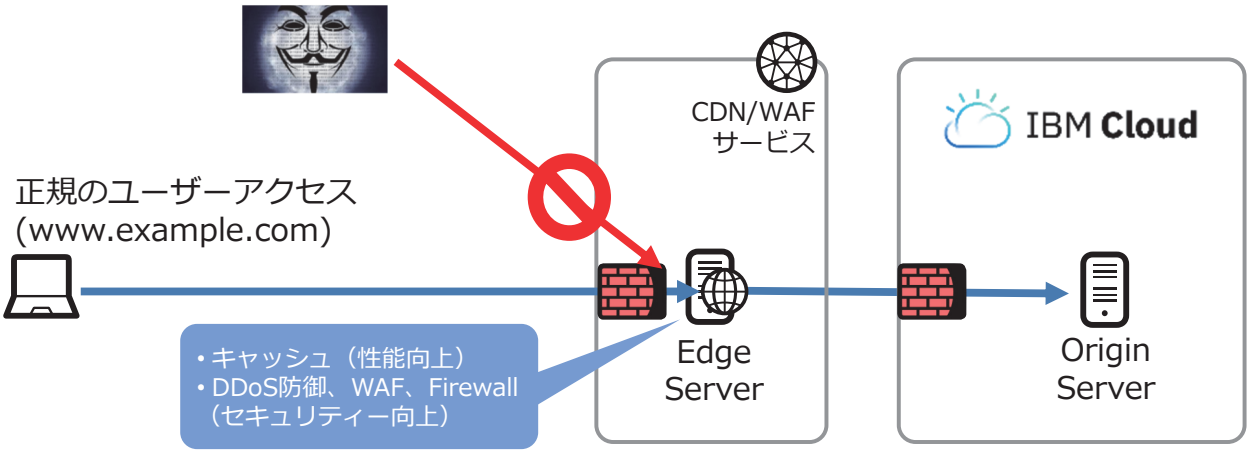




利用者によるネットワークセキュリティー実装方式
IBM Cloud外部に存在するCDN/WAFサービス(IBM Cloud Internet Services(CIS)、Akamaiなど)の利用

・IBM Cloudデータセンターに入ってくる前段階で攻撃をシャットアウトすることで、IBM Cloudデータセンター内のファイアーウォール機器やサーバーが直接攻撃を受けない。

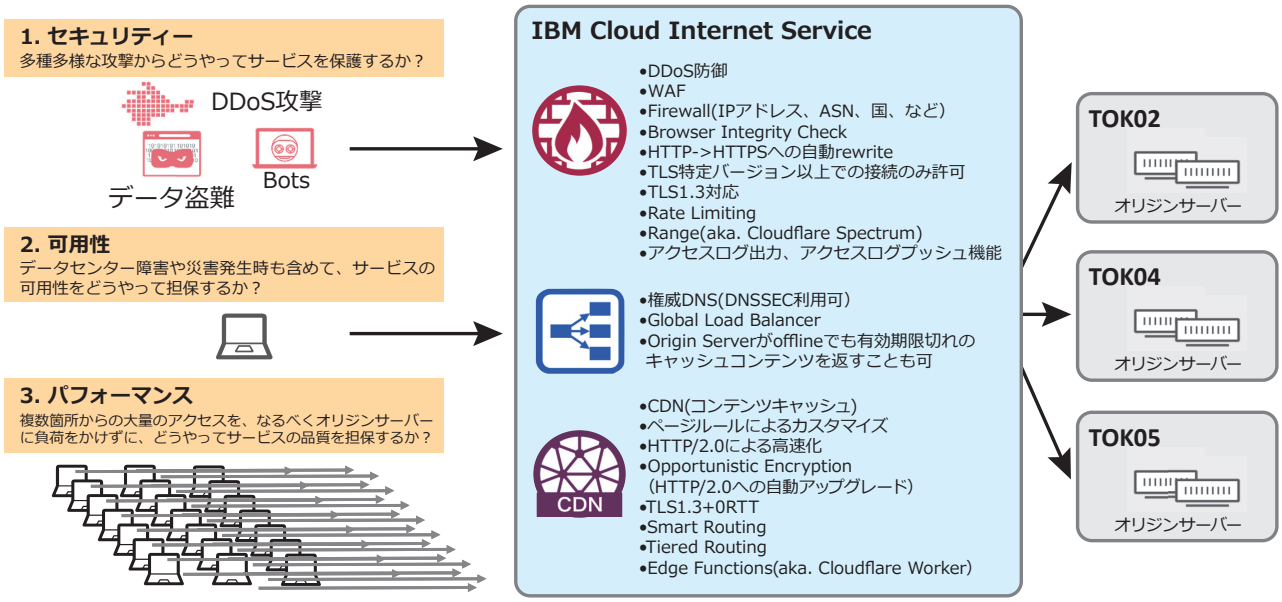
www.example.comの名前解決先アドレスが外部のCDN/WAFサービスになるため、IBM Cloud上のサーバーは直接被害を受けない。



IBM Cloud Internet Services(CIS)とは

CIS(IBM Cloud Internet Service) についての FAQ
https://qiita.com/testnin2/items/bfa08112616ebdfb5244

・アプリケーションの「セキュリティー」「可用性」「パフォーマンス」を向上させる機能をオールインワンで利用できるサービスです。



IBM Cloud Internet Services(CIS)のPlan比較

CIS(IBM Cloud Internet Service) についての FAQ
https://qiita.com/testnin2/items/bfa08112616ebdfb5244

	Standard Plan	Enterprise Usage/Package Plan	GLB Plan	Security Plan
料金	固定	従量課金	固定	固定
DNS	可能	可能	可能	可能
Cache	可能	可能	不可	可能
GLB	可能	可能	可能	不可
WAF	可能	可能	不可	可能
DDoS保護	可能	可能	可能	可能
Firewall	可能	可能	不可	可能
ログの export	不可	可能	可能	可能
Edge Functions	1つのみ	可能	不可	不可
Range	不可	可能	不可	可能

可能と書いてあるものでも、Planによって上限や機能は異なります。詳細は以下を参照ください。
https://cloud.ibm.com/docs/infrastructure/cis?topic=cis-cis-plan-comparison#plan-comparison
https://cloud.ibm.com/catalog/services/internet-services

IBM Cloud Internet Services(CIS)の適用例

教育機関

DDoSや その他の攻撃に備える

DDoS防御と WAFの対応が 必要だった

フルマネージドの DDoS防御とWAFを ご評価いただいた

ポータルサイト

サイトやアプリの パフォーマンスを向上

より 高コスト・パフォーマンスな CDNを検討

フルマネージドの DDoS防御とWAFを ご評価いただいた

イベントサイト

ピーク・トラックへの 対応

アクセスが集中する イベントサイトで、 安定したパフォーマンスを確保

そのための、 CDN、DDoS防御と、 グローバル・ロード・バランサー 機能が必要だった

会員向けページ

高可用性(HA)の 実現

個人情報を取り扱うために、 ログインページのIPアドレスを隠し、 PCI DSS対応済みである 必要があった

グローバル・ロード・ バランサー機能が 必要

利用者によるネットワークセキュリティー実装方式
L4ファイアーウォール

取扱注意

利用者が意図的に設定しない限りは、インターネットからの接続を無制限に許可する構成になっています。ファイアーウォール等のセキュリティ対策を十分に行いましょう。

	Security Groups	Shared Hardware Firewall	Dedicated Hardware Firewall	FortiGate Security Appliance	Virtual Router Appliance	FortiGate Security Appliance 10 Gbps	Juniper vSRX Virtual Gateway/Firewall
Stateful Packet Inspection	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Customer managed appliance	No	No	Yes	Yes	Yes	Yes	Yes
VLAN Protection	No	No	Yes	Yes	Yes	Yes	Yes
Ingress Rules	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Egress Rules	Yes	No	No	Yes	Yes	Yes	Yes
NAT Support	No	No	No	Yes	Yes	Yes	Yes
Multi-VLAN Support	No	No	No	No	Yes	Yes	Yes
DMZ and Multi-Tiered Network Support	No	No	No	No	Yes	Yes	Yes
Public and Private Network Support	Yes	No	No	No	Yes	Yes	Yes
SSL VPN Termination	No	No	No	Yes	Yes	Yes	Yes
IPsec VPN Termination	No	No	No	Yes	Yes	Yes	Yes
Open VPN Termination	No	No	No	No	Yes	No	No
HA Option	N/A	No	No	Yes	Yes	Yes	Yes
Manage from API & Portal	Yes	Yes	Yes	Appliance GUI	Appliance GUI	Appliance GUI	GUI + API
10Gbps Support	N/A	No	No	No	Yes	Yes	Yes
NGFW Add-ons (IPS, AV, WAF)	No	No	No	Yes	No	Yes	Yes (2019)
Cost	$0 / 月	$99.00 / 月～	$999.00 / 月～	$999.00 / 月～	$219.00 / 月～	$4,999.00 / 月～	$299 / 月～

Security Group

仮想サーバーに適用できる無償のファイアーウォール
※Security Groupはデフォルトでは適用されません。

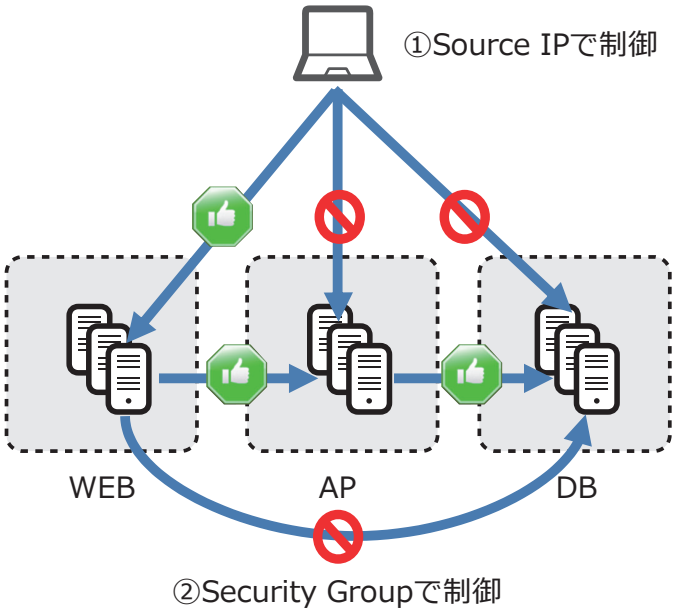
以下の手順に従ってRuleを作成し、仮想サーバーに適用

1. Directionの選択
- Inbound
- Outbound

2. IP Typeの選択
- IPv4
- IPv6

3. Protocolの選択
- TCP → Port範囲を追加で選択
- UDP → Port範囲を追加で選択
- ICMP → Type/Codeを追加で選択
- ALL
- ALL TCP
- ALL UDP
- ALL ICMP

4. Source Typeの選択
- CIDR Block → アドレスレンジを指定
- Security Group → 対象のSecurity Groupを指定

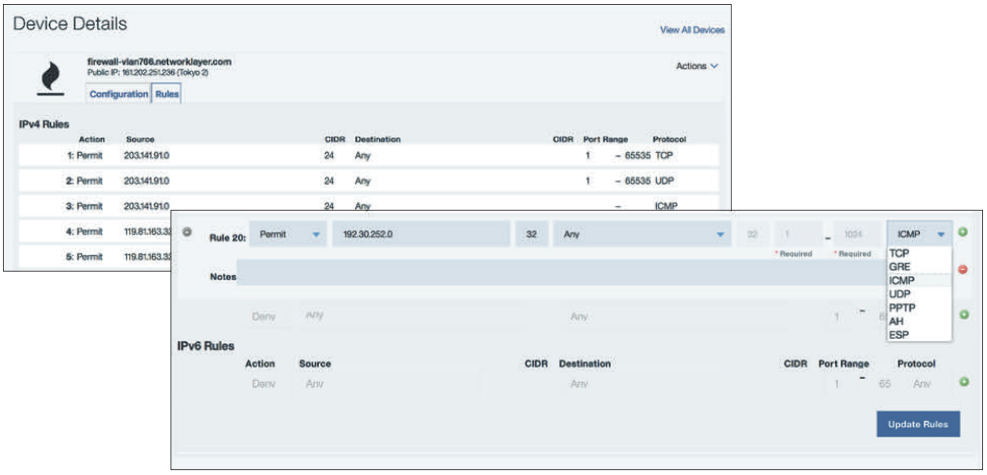


取扱注意

- Security Groupを割り当てると、明示的にルールとして許可しない限り、割当先に関するイン/アウトの通信は拒否されます。
- ステートフルな挙動をとります。つまり、許可されたルールに関する戻りのパケットは暗黙的に許可されます。

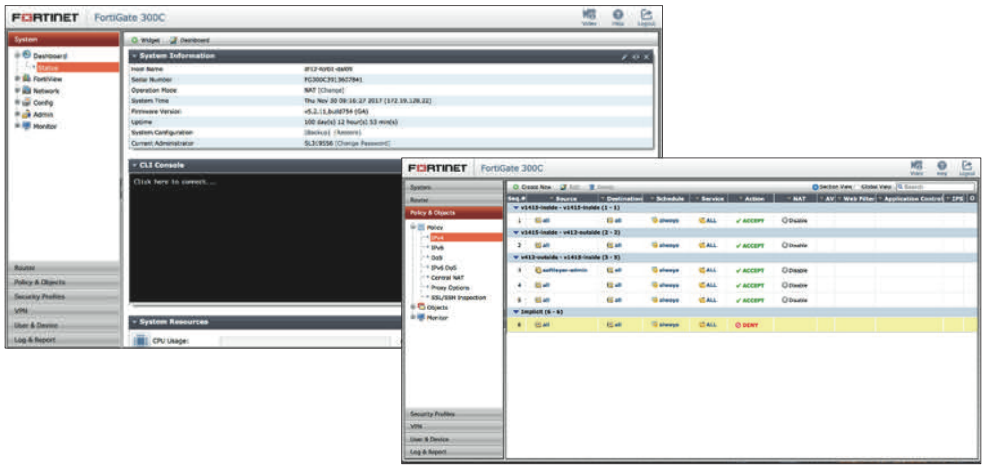
Hardware Firewall

IBM CloudのCustomer Portalから容易に構成可能



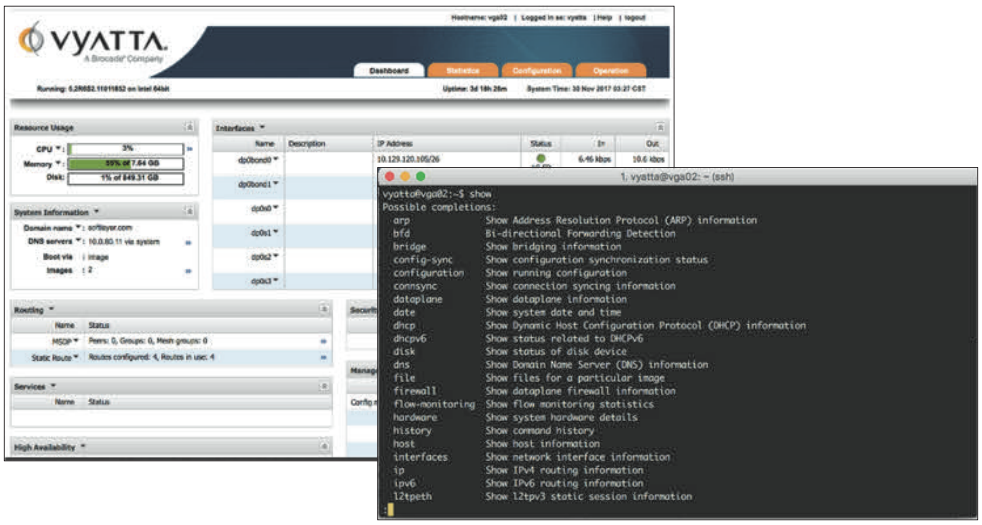
Fortigate Security Appliance

Fortigate Applianceを直接操作することで、よりきめ細やかなセキュリティー運用が可能。



Virtual Router Appliance

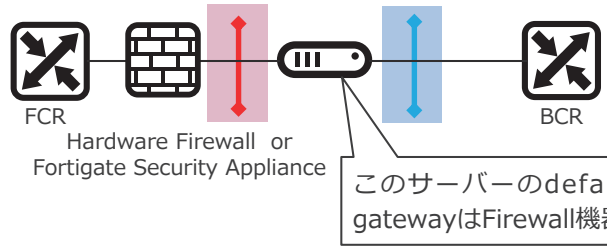
Brocade vRouter 5600ベースの仮想ルーターにより、Firewallだけでなく VPNやトンネル技術も利用可能



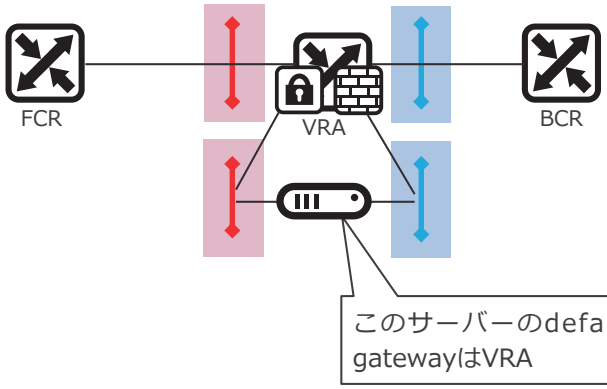
ファイアーウォール構成上の注意点

取扱注意

Public VLANは、VRA/Hardware Firewall/Fortigateのどれか１つでのみ保護可能。
１つのPublic VLANに対してこれらのFWを兼用できないので、以下のどちらかの構成しか選択できない。(既に紐付け済みのVLANに対してFWの注文ができない)



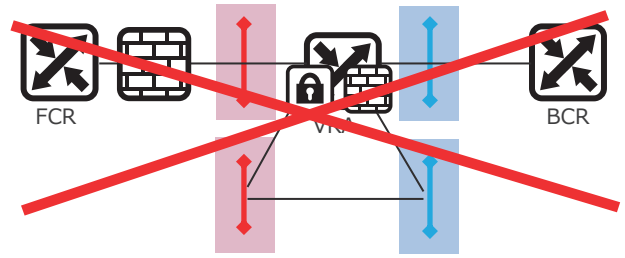
ユーザーVLANに入ってくる前で**Hardware Firewall や Forti-gate**が保護



VRAに保護対象のユーザーVLANを紐付け（トランク）して、**VRAが保護**

取扱注意

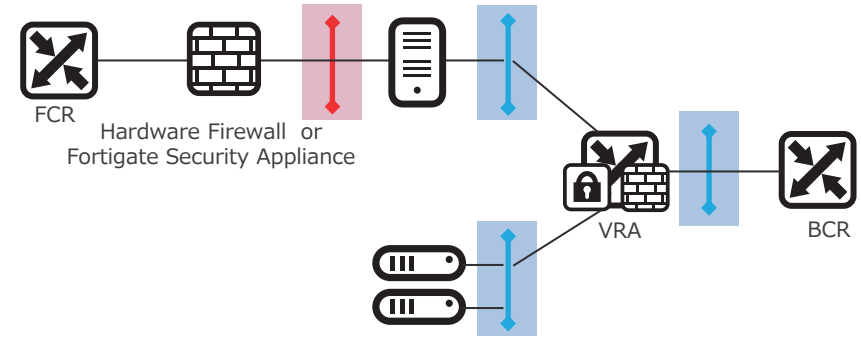
VRAをHardware FirewallやFortigate で保護することはできません。



VRAのVLANに対してFirewall機器を注文しようとすると、"The selected VLAN is a transit VLAN and therefore ineligible for a dedicated firewall."というエラーメッセージが出る。

取扱注意

Public VLANはHardware Firewall/Fortigateで保護し、Private VLANをVRAで保護することが可能。



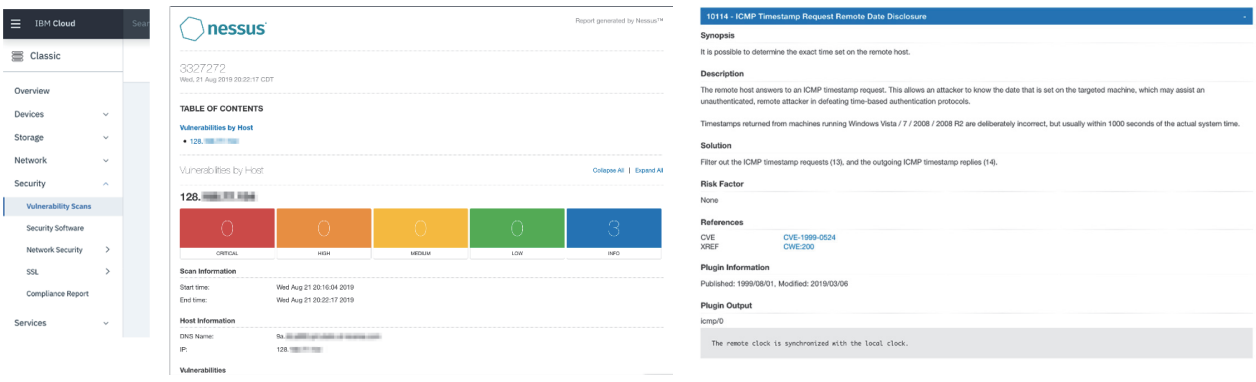
利用者によるネットワークセキュリティー実装方式
Reverse Proxy, SSL Offload, WAF(L7 Firewall)

	NetScaler VPX/MPX Standard Edition	NetScaler VPX/MPX Enterprise Edition	NetScaler VPX/MPX Platinum Edition	F5 on VMware (Good)	F5 on VMware (Better)	F5 on VMware (Best)	CIS
Customer managed appliance	Yes（仮想専有）	IBM Cloud では提供なし（物理サーバー上に別途ライセンス持ち込みをすることは可能）	Yes（仮想専有）	Yes（利用者の VCS 上に構築）	Yes（利用者の VCS 上に構築）	Yes（利用者の VCS 上に構築）	No (Managed Service)
複数VLANにまたがる配置	No		No	Yes (Trunk 構成可)	Yes (Trunk 構成可)	Yes (Trunk 構成可)	N/A
VXLAN サポート	No		No	No	Yes	Yes	No
DoS 防御機能	Yes		Yes	No	Yes	Yes	Yes
DDoS 防御機能	No		No	No	No	No	Yes
WAF 機能	No		Yes	No	No	Yes	Yes
SSL Offload	Yes		Yes	Yes	Yes	Yes	No
CDN 機能	No		No	No	No	No	Yes
Global Load Balancer	No		Yes	No	Yes	Yes	Yes
帯域	10Mbps 200Mbps 1Gbps		10Mbps 200Mbps 1Gbps	25Mbps 200Mbps 1Gbps 3Gbps 5Gbps	25Mbps 200Mbps 1Gbps 3Gbps 5Gbps	25Mbps 200Mbps 1Gbps 3Gbps 5Gbps	制限なし

* VCS=VMware vCenter Server on IBM Cloud

利用者によるネットワークセキュリティー実装方式
脆弱性レポート

- 「Nessus vulnerability Assessment & Report」という脆弱性診断システムを無償で利用できます。管理ポータルからの操作で、サーバー毎の脆弱性レポートを約10分で取得できます。実行回数や実行頻度の制限はありません。
- Linux系とWindows系のOSに対応しています。
- 検査はパブリックNWを通して、Public Primary IPに対して実施されます。Pubic Static IP/Portable IPやプライベートNWには対応していません。



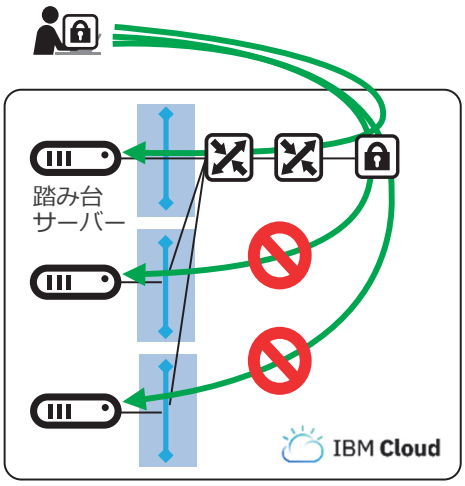
【すぐに使える】	【無償】	【実績】
管理ポータルの操作により実施可能で環境構築が不要。	無償で回数制限なく最新のスキャナーを使用可能。	脆弱性スキャナーに広く使われている「Nessus」を使用

利用者によるネットワークセキュリティー実装方式 SSL VPNサービス

※PPTP VPN サービスは、2019年6月12日をもって、サポートを停止しました。
（引き続き、利用可能な状態ではありますが、SSL VPN への移行を推奨します。）

- **特徴**
  - 利用者が別途VPNサーバーを構築・運用する必要がない。
  - Public NWを使っていないので、Outbound Bandwidthに対しても課金されない。
  - Public NWを使わずにアクセスできるので、セキュアな通信が可能。
  - SSL VPNは、手動で特定のVLAN上のサブネットのみにアクセス許可を与えることが可能。そのため、VPN経由でも直接一般サーバーにアクセスすることを防止し、踏み台サーバー経由でアクセスすることを強制する仕組みが可能。

接続先のサブネットが指定できるので、
例えば、踏み台サーバーだけにSSL VPN
できる、といった使い方もできる。



SSL VPNサービスの考慮点

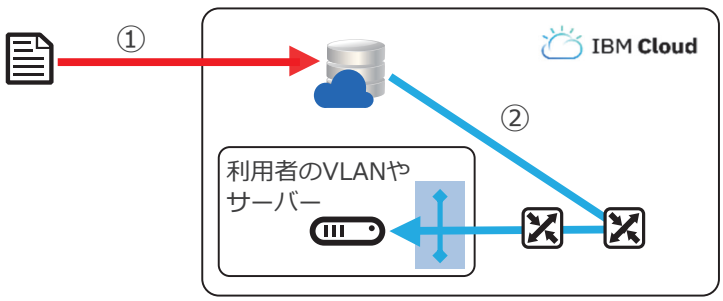
※PPTP VPN サービスは、2019年6月12日をもって、サポートを停止しました。
（引き続き、利用可能な状態ではありますが、SSL VPN への移行を推奨します。）

取扱注意 Handle with care

- 管理用途（SSH接続やRDP接続）のため、低速です。また12時間に1度切断されます。
- サービスとして冗長化されておらず、接続できない際には他のデータセンターを選択していただかなければいけない場合もあります。
- 常時接続、大容量ファイル転送などには以下の代替案を検討してください。

- **代替策1:**
  Object Storageにインターネット経由でファイルをSFTPやpython-swiftなどでuploadし、Object Storageからはprivate NW経由でダウンロードする。（サーバー側に割り当てられたPublic NWは使用しない）

sftp を使った SoftLayer Object Storage への簡易アクセス方法
Qiita：https://qiita.com/testnin2/items/64f934f61bcaf7ac2572

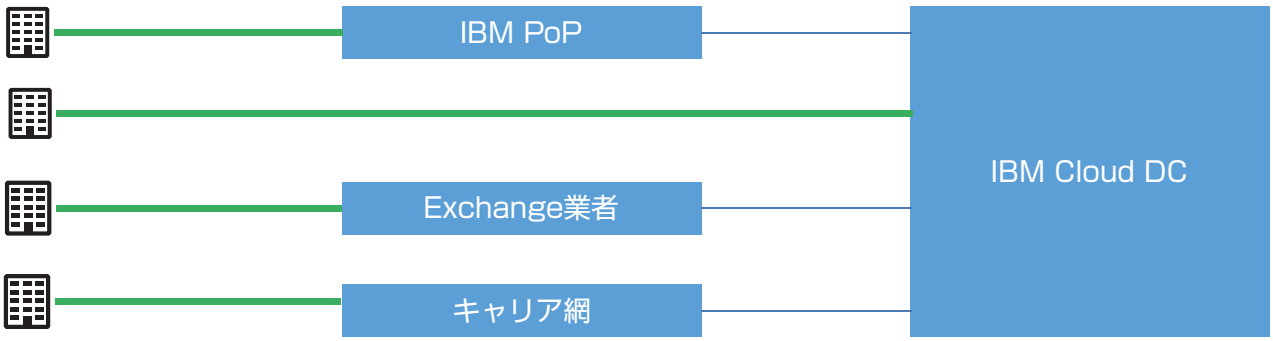


- **代替策2:**
  VRAなどを使い、Public NW経由でVPNを構築する。
  （この場合はPublic NW経由の通信になるので、Outbound Bandwidthが発生する。）

- **代替策3:**
  専用線を敷設する。

利用者によるネットワークセキュリティー実装方式
専用線サービス

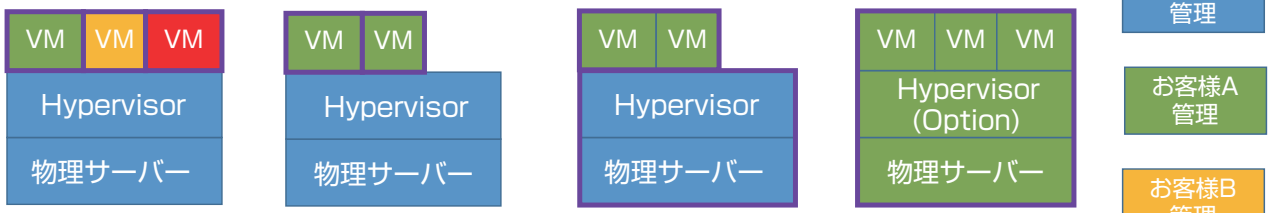
- **専用線接続方式には、以下の3種類が存在します。**
  - Direct Link Dedicated
    - PoP経由で接続する方法（東京ではEquinix DCに存在するPoPが利用可能）
    - データセンターに直結する方法（隣接している利用者専用スペースとIBM Cloudを構内配線で接続可能）
  - Direct Link Exchange
    - Exchange業者経由で接続する方法（他社クラウドに接続可能。東京ではEquinix社のCloud Exchangeが利用可能）
  - Direct Link Connect
    - キャリア網経由でIBM Cloudに接続する方法



8-5. サーバーセキュリティー

サーバーの選択

IBM Cloudは、稼働させるワークロードに応じて複数の選択肢があります。
セキュリティーの観点において、どの形態を利用するかは重要な選択になります。



Public Virtual Server

- マルチテナント
- 同一ホストに他アカウントの仮想サーバーが稼働する可能性がある。
- ハイパーバイザーはIBM Cloud管理。

Dedicated Virtual Server

- シングルテナント
- どのホストにプロビジョニングされるかが不明（複数のホストにプロビジョニングされる可能性もあるし、そのホストのスペックも公開されない）。
- ハイパーバイザーはIBM Cloud管理。

Dedicated Host

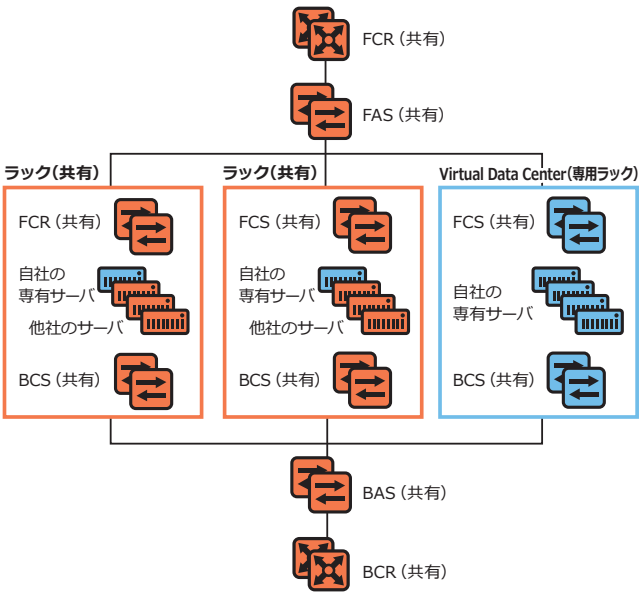
- シングルテナント
- 事前に56 Cores, 242GB RAM,1.2 TB SSD のホストを購入し、その上でその購入したホストを指定して仮想サーバーを追加購入する。
- ハイパーバイザーはIBM Cloud管理。

Bare Metal Server

- シングルテナント
- 物理サーバーまで含めて利用者が管理できる。

Virtual Data Center(専用ラック)

・一般的に、IBM Cloud上のNW機器は共有されているが、ネットワークはVLANで利用者ごとに分離されているため、サーバー間通信は安全に保たれている。
・Virtual Data Center(VDC)とは、お客様ごとに専有ラックを利用できるサービスです。さらなる分離性を強化できます。
・以下の特徴を持ちます。
  ・物理的な配置場所やラックまで含めて利用者専有になる。
  ・ラック内のサーバーは自社サーバーのみを配置できる。
  ・ラックごとにサーバを収容するスイッチ（FCS（Frontend Customer Switch）やBCS（Backend Customer Switch））も利用者専有になる。
  ・自社サーバー間通信がラック内折り返しになり、ラック間通信が発生しないので、高速になる。
  ・あくまでIBM Cloudの物理サーバーやVRAを配置するものであり、以下のサーバーは配置できない。
    ・仮想サーバー
    ・時間課金の物理サーバー（事前構成済みなので）
    ・持ち込み機器



サーバー削除時のドライブワイプ

・これまでご利用いただけた「データ破壊証明書発行サービス（有償）」は、「Disk買取サービス」に変更されました。
・お客様がDiskを買い取るので、お客様はそのDiskを使用していたデータセンターからお客様ご指定の場所に郵送することが可能です。
・Diskを破壊する必要がある場合は、Disk受領後、お客様ご自身でご対応いただくことになります。
・なお、国外輸送となる場合、輸出となります。必要な書類の準備等、お客様の責任で実施いただく必要があります。

対象ロケーション：すべてのデータセンター

必要な書類:

• サーバーから取り出すHDDのリスト（対象のサーバー/HDDすべて）
• お客様がDriveを購入するためのIBM Cloud VPによる承認（IBM Cloudのサイトマネージャーが取得）
• 購入のための契約（HDDの販売が承認されるとSoftLayer社法務による対応とお客様の署名が必要になります）
  ＊お客様はIBM Japanではなく、SoftLayer社と契約することになります。契約書は英語となります。
• 以下の出荷伝票
  • 前払い済みの出荷ラベル(prepaid shipping label)
  • コマーシャル・インボイス（国際輸送の場合）
  • 輸出ライセンス(国際輸送で要求された場合）

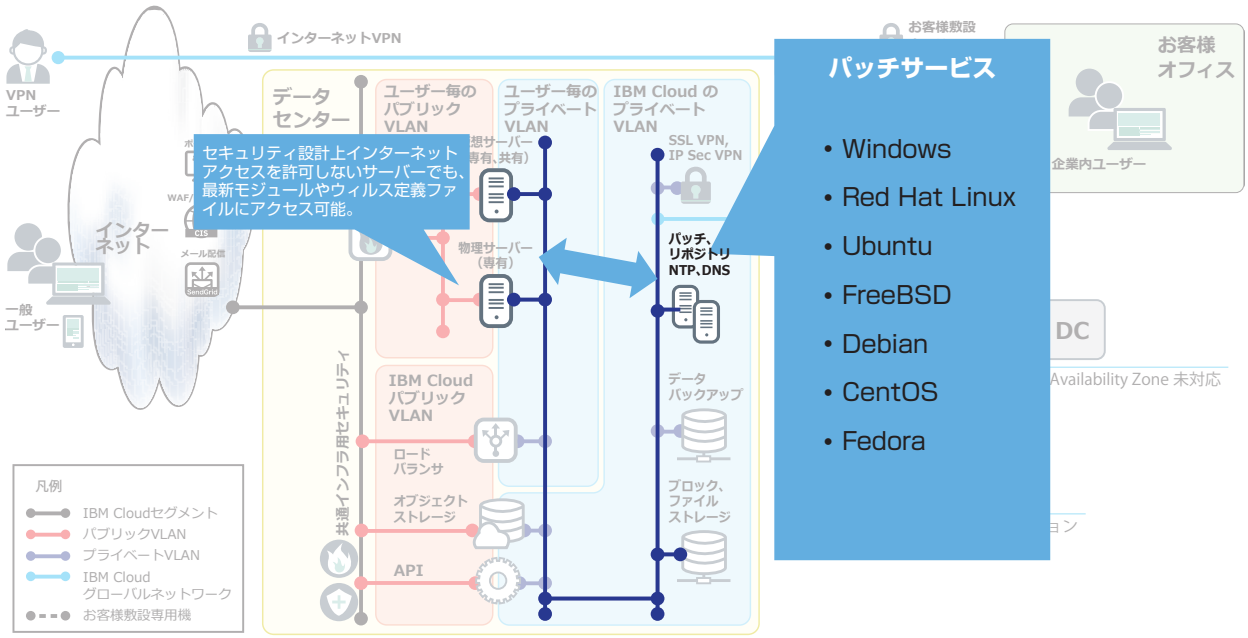
お客様に負担いただく料金:

HDDの費用(full face current day market value 現在の市場価格)
アドミ料金$150
SoftLayer社は国内輸送に限り、HDDの郵送手配を行うことが可能。
SoftLayer社が輸送を手配する場合の輸送費は常に$75。

届いた Disk の中央に穴を空けて破壊するのも自由

パッチ配布（脆弱性からの防御）

IBM Cloudでは、各OS用にアップデートサーバーが設置され、最新のモジュールやウィルス定義ファイルを参照できます。
プライベートネットワーク上にあるため、インターネットに接続していないサーバーでも追加費用なく利用できます。



OS のハードニング

一般的には、以下の対応を行うことが望ましいとされています。

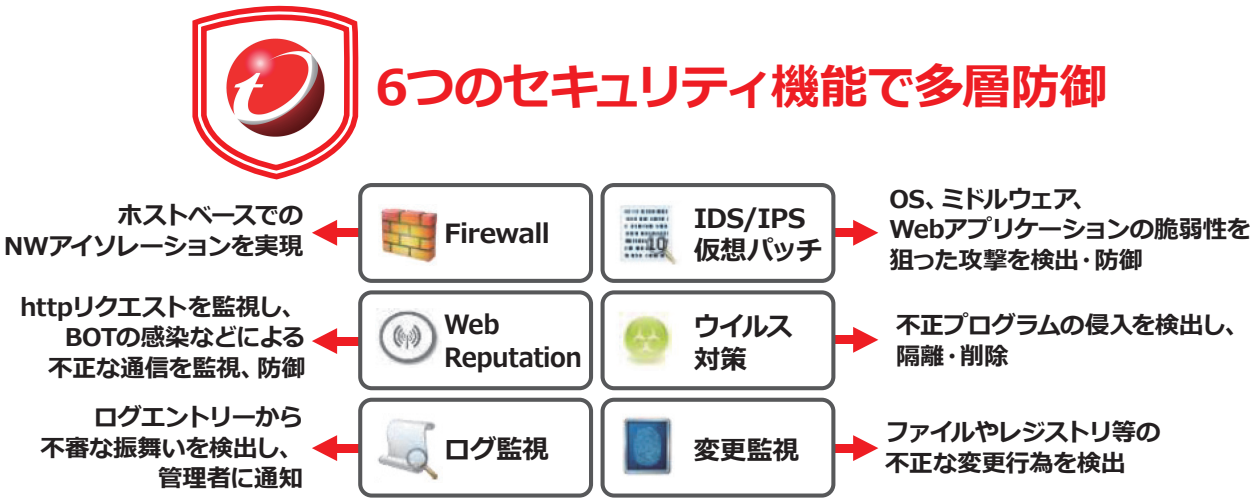
- 不要なサービスを起動しない。
- デフォルトのポートを変更する。
- 外部公開しないポートは閉じる。
- パスワードを定期的に変更する。
- OSレベルでもFirewallを実装する。
- アンチウィルスソフトやアンチスパイウェア対策ソフトウェアを導入する。
- IDS機能をもつ対策ソフトウェアを導入する。
- ログ監視や変更監視を行う。

IBM Cloud IaaSでは以下のソフトウェアが利用できます。別途セキュリティーソフトウェアを持ち込むことも可能です。

種別	名称	特徴・仕様
アンチウィルス スパイウエア	・McAfee Windows VirusScan Anti-Virus Windows	・Windowsのみで使用可能 ・IBM Cloudプライベートネットワークにパターンファイル配布サーバーを設置 ・Linux版のアンチウィルスソフトウェアは利用者の持ち込みになります。その際の候補は、Linux版のMcAfeeやFreeのアンチウィルス製品（ClamAVやAVG）やTrendmicro等
IDS	・McAfee Host Intrusion Protection w/Reporting	・ネットワーク侵入検知機能を提供（Windows のみの機能）
ファイアーウォール	・Microsoft Windows Firewall ・APF Software Firewall for Linux	・サーバー毎のファイアウォール機能を提供 ・個別の設定は各サーバーで実施が必要

(参考) Trend Micro Deep Security

Trend Micro Deep Securityはサーバが抱えているセキュリティ課題を仮想・クラウド・物理環境にまたがって、トータルに解決する統合型サーバセキュリティソリューションであり、IBM Cloudでも豊富な実績を持つソリューションです。
OS上にインストールするエージェント型と、VMWare上にVirtual Applianceとして導入することでゲストサーバーにエージェント導入を不要とするエージェントレス型が存在します。IBM Cloudでは物理サーバーを利用できるため、どちらのタイプも利用できます。



8-6. データセキュリティー

わたしのデータが
勝手にIBMに使われて他社向けに提供されたりしますか？

IBM Cloudではお客様のデータはお客様のものです。
クラウドサービス契約書(CSA)に以下の記載があります。

「コンテンツ」は、お客様またはお客様の承認を受けたユーザーが、提供するまたはアクセスを承認するすべてのデータ、ソフトウェアおよび情報、ならびに「クラウド・サービス」に入力するすべてのデータ、ソフトウェアおよび情報で構成されます。「クラウド・サービス」の使用は、当該「コンテンツ」に対するお客様の既存の所有権または使用許諾権に影響を及ぼしません。IBMおよびその従契約者ならびにサブプロセッサーは、個別契約書に別途記載がない限り、「クラウド・サービス」を提供し管理する目的のためにのみ、「コンテンツ」にアクセスし使用することができるものとします。

Cloud act法によって、
IBMがユーザーに許可なく米国政府にデータを提供しませんか？

CLOUD actは、広義で捉えると米国政府が他国にあるデータに対して、
安全保障上の手段として、アクセスが可能になるというものです。

IBMはUS政府の大量データ収集プログラムには関与していません。また、IBMには2014年に定めたポリシー（Data Responsibility @IBM: https://www.ibm.com/blogs/policy/dataresponsibility-at-ibm/）を遵守します。二国間協定またはMLAT（相互法的支援条約）などの国際的に認められた法的手段がない限り、IBMは司法行為またはその他の手段により政府の法域外に保存されたデータの要求に対して、異議を申し立てる適切な措置を講じます。

https://www.ibm.com/blogs/policy/cloud-act/

データ暗号化の方法

・クラウドストレージでの暗号化は標準で実装されています。
・より強固なセキュリティが求められるデータを扱う場合は利用者側で鍵の管理が行える方法を検討する必要があります。

暗号化の種類	利用する機能・サービス	該当する IBM Cloudサービス	役割分担			
			暗号化/復号	鍵の保管	鍵の生成/管理	KMI機器の運用
アプリケーションでのデータ暗号化	利用者が独自のツール(Guardiumなど)を導入して利用	N/A	利用者	利用者	利用者	利用者
	鍵管理の専用環境を利用	・IBM Cloud HSM	利用者	利用者	利用者	利用者
	鍵管理の共用サービスを利用	・IBM Key Protect	利用者	IBM	利用者	IBM
バックアップツールでのデータ暗号化	利用者が独自のツールを導入してバックアップデータを暗号化	・R1Soft(Idera) ・Veeam	利用者	利用者	利用者	利用者
	IBM Cloud提供のバックアップツールを利用してバックアップデータを暗号化	・Evault	IBM	IBM	IBM	IBM
クラウドストレージでのデータ暗号化	クラウドストレージの暗号化機能を利用(全データが標準で暗号化)	・Endurance Storage ・Performance Storage ・Object Storage (ICOS)	IBM	IBM	IBM	IBM

※KMI：Key Management Infrastructure

IBM Cloud HSM (hardware security module)

IBM Cloud ハードウェア・セキュリティ・モジュール(HSM)は、暗号鍵を管理することを主目的とし、それらの鍵を使用して暗号操作を提供する暗号プロセッサです。HSMの主な機能には、キーの生成と保管、暗号化された形の機密データの高速対称および非対称暗号化とバックアップが含まれています。
HSM 7.0でFIPS 140-2 Level 3に対応するようになりました。

- ✓ Redundant Power Supplies
- ✓ Multi-level access control
- ✓ Intrusion-resistant, tamper-evident hardware
- ✓ Support up to 100 clients
- ✓ Multiple Roles for Administration
- ✓ Strong Separation of Duties
- ✓ Partitioning and strong cryptographic separation
- ✓ Host Trust Links
  - ✓ Secure binding of client to HSM in Virtual Cloud Environment
- ✓ Keys stored in hardware
- ✓ Secure transport mode for high-assurance delivery
- ✓ Multi-level access control
- ✓ Multi-part splits for all access control keys
- ✓ Suite B algorithm support
- ✓ Secure decommission
- ✓ Secure Audit Logging
- ✓ Strongest cryptographic algorithms
- ✓ Only the customer can access encryption keys

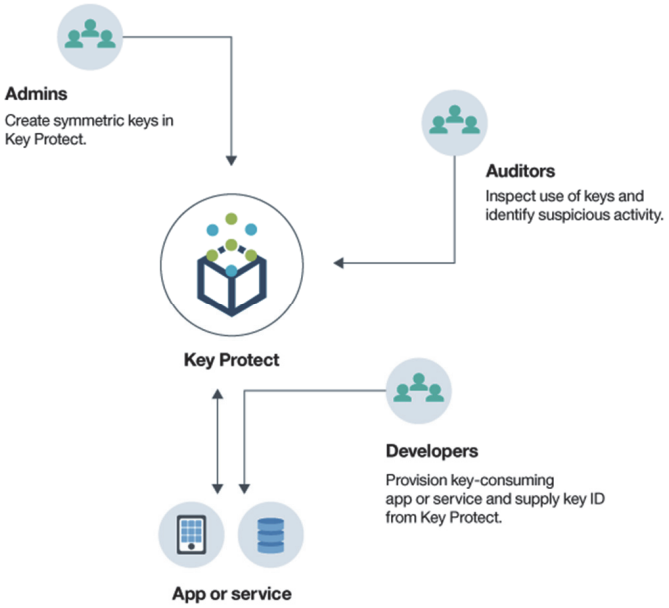
Gemalto

https://www.ibm.com/cloud/hardware-security-module
https://cloud.ibm.com/docs/infrastructure/hardware-security-modules?topic=hardware-security-modules-getting-started

IBM Key Protect

暗号鍵の生成、保管、取得、および管理のための、アプリケーションから独立したクラウド・ベースの鍵管理の仕組み。

- ✓ FIPS-140-2 Level3 認定のハードウェア・セキュリティ・モジュール(HSM) でプロビジョンした暗号鍵を保護
- ✓ 保管した暗号鍵は、管理者あるいは開発者の権限を持つユーザーのみAPIで閲覧可能
- ✓ VMware vCenter Server(VCS)のvSANの暗号化鍵の管理のために、KeyProtectを利用可能(KMIP for VMware)



管理者(Admin)：
　暗号化のための鍵を管理
監査人(Auditor)：
　鍵の使用を検査し、疑わしい活動を特定
開発者(Developer)：
　アプリケーションやサービスで暗号鍵を使用したコードを開発

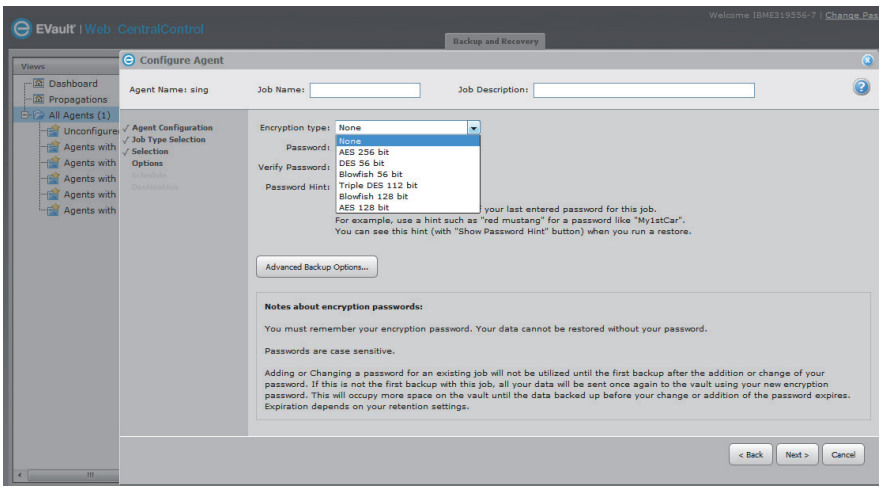
https://cloud.ibm.com/docs/services/key-protect?topic=key-protect-getting-started-tutorial#getting-started-tutorial

Idera/R1Softの暗号化機能

- AES 256 bit

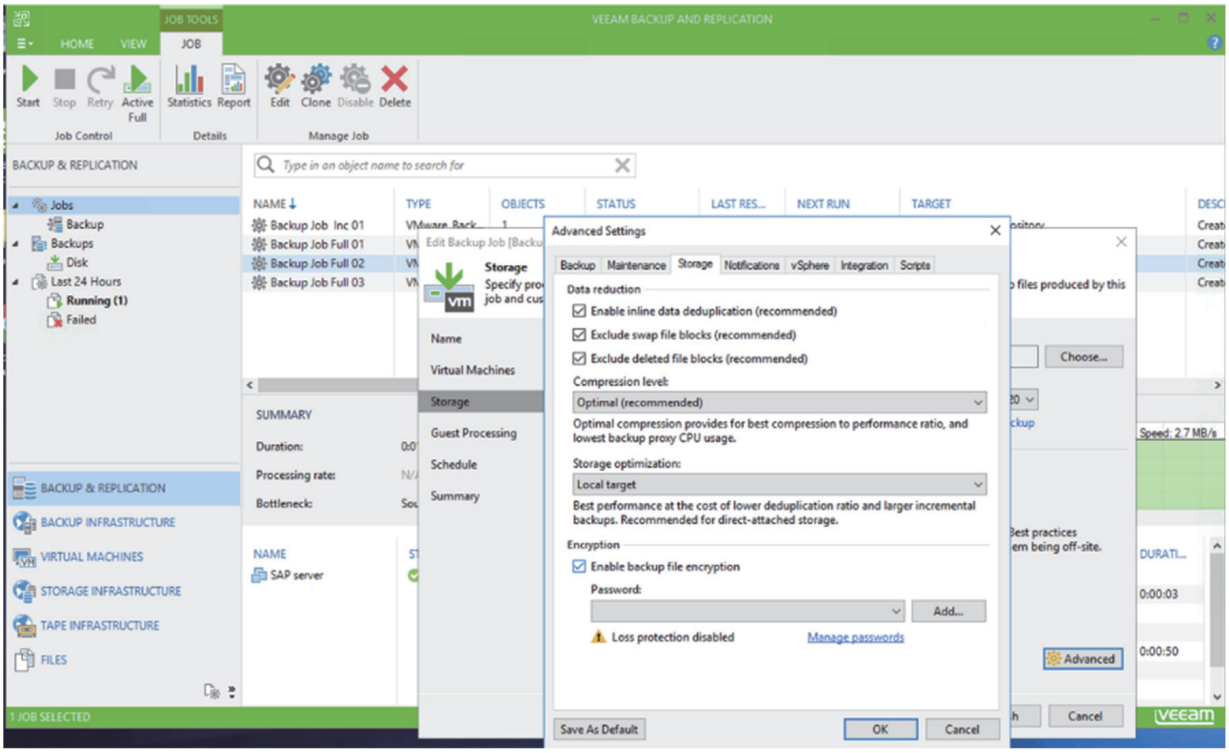
Evaultの暗号化機能

- AES 256 bit
- DES 56 bit
- Blowfish 56 bit
- Triple DES 112 bit
- Blowfish 128 bit
- AES 128 bit



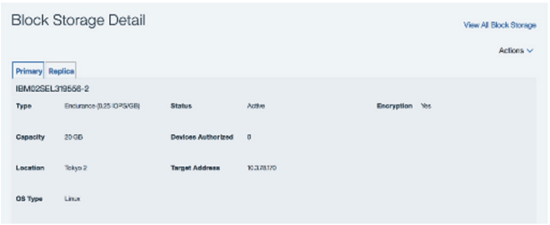
Veeamの暗号化機能

- AES 256 bit



ブロックストレージ及びファイルストレージでの暗号化

- 追加コストや性能への影響なく、IBM Cloud管理のもとで暗号化機能が提供されています。それらのストレージのスナップショットやレプリケーションも全て暗号化されます。
- 業界標準のAES-256暗号化
- キーは、業界標準のKey Management Improbability Protocol（KMIP）を使用して社内で管理
- ストレージは、連邦情報セキュリティマネジメント法（FISMA）認定の連邦情報処理標準（FIPS 140-2）、医療保険の携行性と責任に関する法律（HIPAA）、PCI、バーゼルII、カリフォルニア州セキュリティ違反情報法（SB 1386）およびEUデータ保護指令95/46/ECに準拠



オブジェクトストレージ(ICOS)での暗号化

- 情報分散アルゴリズムとオール・オア・ナッシング変換の2つのアルゴリズムの組み合わせで、データのセキュリティ性を確保している。また、データの移動時も暗号化される。
- 全ての書き込み情報に対してオール・オア・ナッシング変換で暗号化
  - RC8-128 encryption with MD5-128 Hash for data integrity
  - AES-128 encryption with MD5-128 Hash for data integrity
  - AES-256 encryption with SHA-256 Hash for data integrity
- ストレージはHTTPS経由でアクセス
- 分散ストレージデバイス内はTLSを使用した相互認証のもと通信

8-7. 監査

IBM Cloud Activity Tracker with LogDNA

IBM Cloud上でのCustomer portalもしくはAPIでの操作を記録してくれる仕組みです。
global eventsというアカウント全体にまたがったイベント（例：ユーザー作成など）と、location-based events（例: Tokyoリージョンで提供されているサービスの構成変更など）というリージョンごとに管理されるイベントが管理されます。

対応サービス一覧
https://cloud.ibm.com/docs/services/Activity-Tracker-with-LogDNA?topic=logdnaat-cloud_services

対応リージョン一覧
https://cloud.ibm.com/docs/services/Activity-Tracker-with-LogDNA?topic=logdnaat-regions

FAQ:
https://qiita.com/testnin2/items/f2ddd6f502be6cb8599e

取扱注意 Handle with care

1. 名前が似ていて紛らわしいですが、「IBM Cloud Activity Tracker」はすでに販売を中止しています。
   今後は「IBM Cloud Activity Tracker with LogDNA」を利用してください。
2. global eventsを参照するためにはFrankFurtリージョンにインスタンスを作成する必要があります
   （ただし、CIS（Cloud Internet Services）に関してはDallasで管理されるといった例外も存在します）。

https://cloud.ibm.com/docs/services/Activity-Tracker-with-LogDNA?topic=logdnaat-getting-started#getting-started
https://qiita.com/testnin2/items/f2ddd6f502be6cb8599e

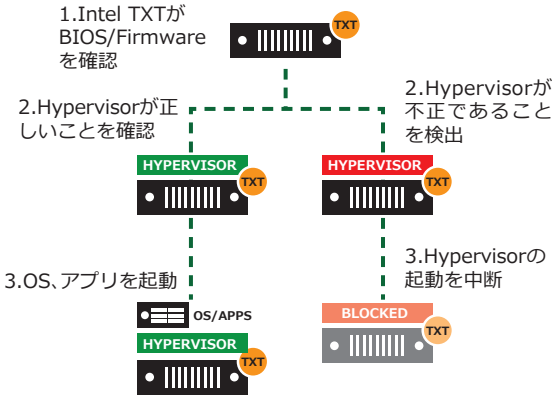
8-8. その他

Intel TXT によるサーバーセキュリティの強化

Intel Trusted eXecution Technology（Intel TXT）はクラウドに更なるセキュリティを実装するためのオプションです。
あらかじめ認証された環境以外での仮想マシン（ゲストOS）の起動を禁止するものです。

物理サーバーに追加することができます。
対象となっているCPUラインナップは最新情報を参照してください。

https://cloud.ibm.com/docs/bare-metal?topic=bare-metal-bm-hardware-monitroing-security-controls



推奨情報 Recommendation

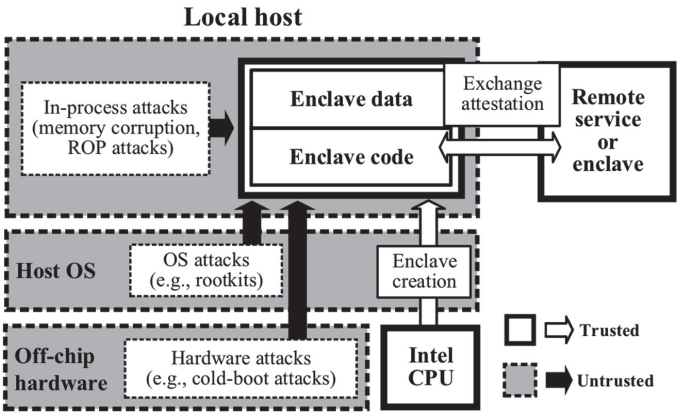
Intel TXTが指定できるクラウドは多くありません。

Intel SGX

Intel SGXは、メモリ上に「Enclave」と呼ばれる厳重に保護された領域を生成することで、センシティブデータを保護しながらプログラムを実行する為のCPUの拡張機能です。
IBM Cloudでは物理サーバーのオプションとして購入可能です。

・対応環境

Section	Option to select
Server	Single processor, Intel Xeon E3-1270 v6 with Storage up to four drives
Image	Windows Server 2016 Standard Edition (64 bit) Windows Server 2016 Standard Edition (64 bit) Windows Server 2016 Datacenter Edition (64 bit) CentOS 7.x (64 bit) Ubuntu Linux 16.04 LTS Xenial Xerus (64 bit) - CentOS 7.x (64 bit) Red Hat Enterprise Linux 7.x (64 bit) (per-processor licensing)
Image Add-ons	Software Guard Extensions

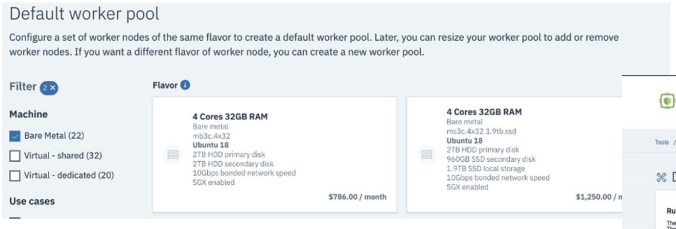


https://www.ibm.com/blogs/solutions/jp-ja/data-use-protection-ibm-cloud-using-intel-sgx/
https://qiita.com/Cliffford/items/2f155f40a1c3eec288cf
https://cloud.ibm.com/docs/bare-metal?topic=bare-metal-bm-server-provision-sgx

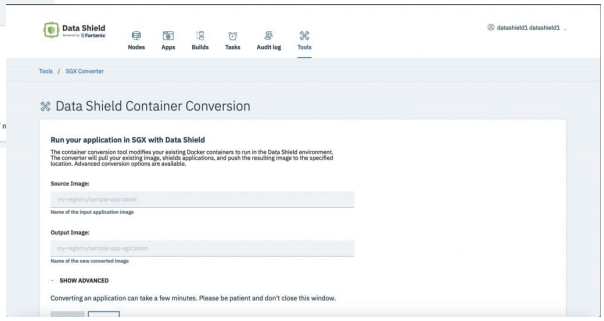
IBM Cloud Security Shield

IBM Cloud Kubernetes Service環境上のコンテナをIntel SGXで保護することで、センシティブデータを保護しながらプログラムを実行する為のサービスです。
IBM Cloud Kubernetes ServiceのWorker Nodeは物理サーバーである必要があります。

・対応環境



**Data Shieldを使って既存のコンテナを
Intel SGX対応に変換**



https://cloud.ibm.com/docs/services/data-shield?topic=data-shield-getting-started
https://www.ibm.com/cloud/blog/announcements/announcing-ibm-cloud-data-shield-beta-at-think-2019

本書をご利用いただくにあたってのご注意事項

本資料は、日本IBMのクラウド・エンジニア有志によって準備され、それぞれ独自の見解を反映したものです。
これらは情報提供の目的のみで提供されており、いかなる読者に対しても法律的またはその他の指導や助言を意図したものではなく、またそのような結果を生むものでもありません。本資料に含まれている情報については、完全性と正確性を期するよう努力しましたが、「現状のまま」提供され、明示または暗示にかかわらずいかなる保証も伴わないものとします。本資料またはその他の資料の使用によって、あるいはその他の関連によって、いかなる損害が生じた場合も、IBMは責任を負わないものとします。本資料に含まれている内容は、IBMまたはそのサプライヤーやライセンス交付者からいかなる保証または表明を引きだすことを意図したものでも、IBMソフトウェアの使用を規定する適用ライセンス契約の条項を変更することを意図したものでもなく、またそのような結果を生むものでもありません。

本資料でIBM製品、プログラム、またはサービスに言及していても、IBMが営業活動を行っているすべての国でそれらが使用可能であることを暗示するものではありません。本資料で言及している製品リリース日付や製品機能は、市場機会またはその他の要因に基づいてIBM独自の決定権をもっていつでも変更できるものとし、いかなる方法においても将来の製品または機能が使用可能になると確約することを意図したものではありません。本資料に含まれている内容は、読者が開始する活動によって特定の販売、売上高の向上、またはその他の結果が生じると述べる、または暗示することを意図したものでも、またそのような結果を生むものでもありません。パフォーマンスは、管理された環境において標準的なIBMベンチマークを使用した測定と予測に基づいています。ユーザーが経験する実際のスループットやパフォーマンスは、ユーザーのジョブ・ストリームにおけるマルチプログラミングの量、入出力構成、ストレージ構成、および処理されるワークロードなどの考慮事項を含む、数多くの要因に応じて変化します。したがって、個々のユーザーがここで述べられているものと同様の結果を得られると確約するものではありません。

記述されているすべてのお客様事例は、それらのお客様がどのようにIBM製品を使用したか、またそれらのお客様が達成した結果の実例として示されたものです。実際の環境コストおよびパフォーマンス特性は、お客様ごとに異なる場合があります。

[当資料に関するお問い合わせ]
IBMアクセスセンター
Tel：0120-550-210　受付時間 9:00～17:00（土、日、祝日を除く）

〒103-8510 東京都中央区日本橋箱崎町19-21
当資料は、2019年9月改定の「IBM Cloud 柔らか層本」(http://ibm.biz/yawarakasou)
を編集したものです。製品、サービスなどの詳細については、弊社もしくはビジネス・パートナーの営業担当員にご相談ください。