

CDP-002

ROOM
F

コンサルティングの現場から見えてきた
Azure IaaS インフラ設計の
最新ベストプラクティス

と、
次世代IaaSの
新機能

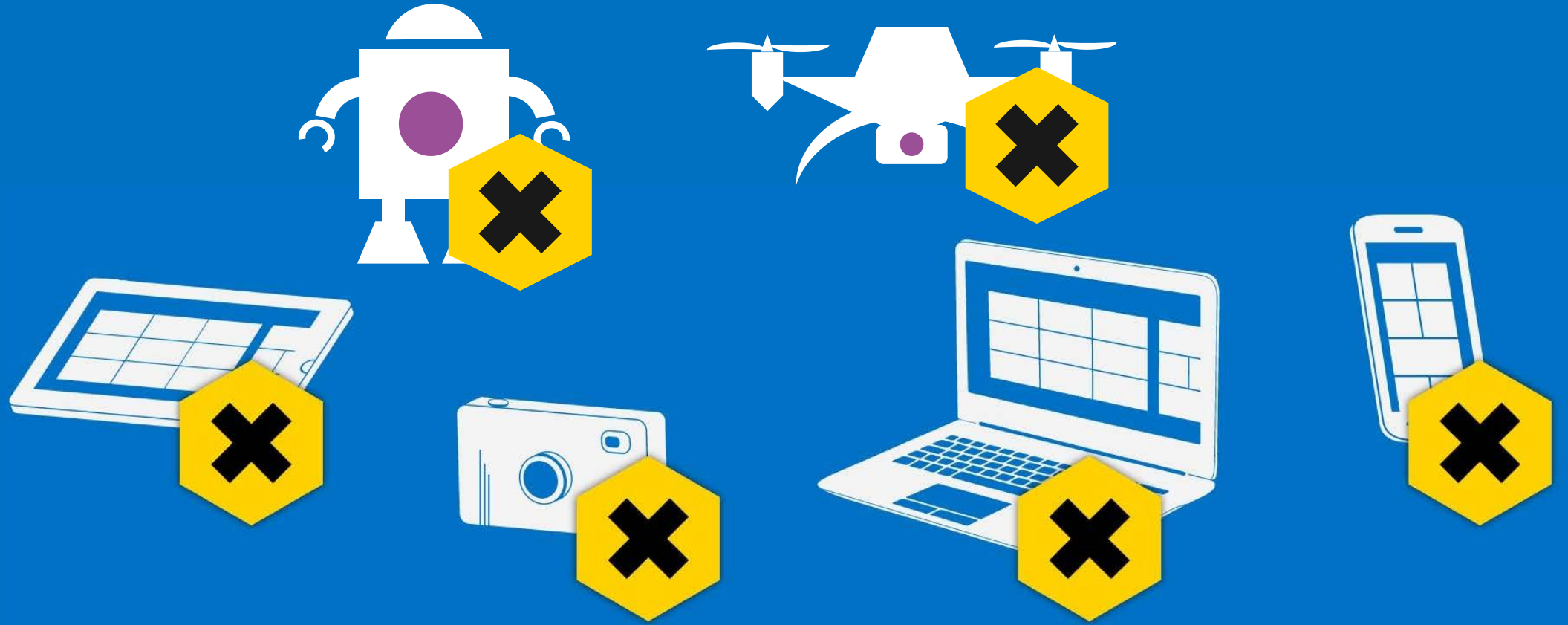
日本マイクロソフト株式会社
コンサルティングサービス統括本部
アーキテクト
大井 雄介

注意事項

- このプレゼンテーション資料は 2015 年 5 月 15 日時点で公開可能な情報をもとに作成されています。
- このプレゼンテーション資料には Windows 10 や Windows Server 2016 など 2015 年 5 月 15 日時点で一般提供（GA）されていない製品やサービス、機能の説明が含まれている場合があります。



セッション中の写真/動画撮影はご遠慮ください



本セッションの目的とゴール

- Azure IaaS設計の「勘所」を理解する。
- 次世代のAzure IaaSの姿にワクワクする！

Azure IaaS 設計の ベストプラクティス

まず「本当にIaaSが必要か」を考える



SaaS/PaaSはマイクロソフトのベストプラクティスのかたまり
まずはSaaS/PaaSでできないか？を考える

クラウド移行を考える時の鉄則

要件

≠

今までの
やり方

**本当の「要件」に立ち返り、
クラウドならではのやり方で実現する**

仮想マシン



- 定番
- **基本と標準**



- 高速CPU
- メモリ大きめ
- ローカルSSD



- 大容量メモリの
モンスター
マシン



- Premium
Storage対応
- その他はDと
同じ

A or D ?

A1 Standard ★	D1 Standard ★	A2 Standard
1 コア	1 コア	2 コア
1.75 GB	3.5 GB	3.5 GB
 2 データ ディスク	 2 データ ディスク	 4 データ ディスク
 2x500 最大 IOPS	 2x500 最大 IOPS	 4x500 最大 IOPS
 負荷分散	 負荷分散	 負荷分散
 自動スケール	 自動スケール	 自動スケール
4,553.28 JPY/月 (推定)	6,450.48 JPY/月 (推定)	9,106.56 JPY/月 (推定)

* 2015/05/15時点の米国中部での価格です

Basic(基本) or Standard(標準) ?

A2 Basic	
2	コア
3.5	GB



4
データ ディスク



4x300
最大 IOPS

A2 Standard	
2	コア
3.5	GB



4
データ ディスク



4x500
最大 IOPS



負荷分散



自動スケール

6,678.14
JPY/月 (推定)

9,106.56
JPY/月 (推定)

* 2015/05/15時点の米国中部での価格です

ストレージ

課金

- 定義サイズではなく消費サイズベースでの課金 (Standard Storageの場合)
- 必ずクイックフォーマット

キャッシュ

- 既定でOSディスクは読み取り/書き込みキャッシュ
- SYSVOLなどはキャッシュなしのデータディスクに

性能

- 記憶域スペースでディスクを「束ねて」高IOPS
- 束ねたディスクの災害対策はAzure Backupで

復習：Azureストレージの地理的冗長性

ローカル冗長ストレージ(LRS)

- リージョン内で3重化して保存される。

ジオ冗長ストレージ(GRS)

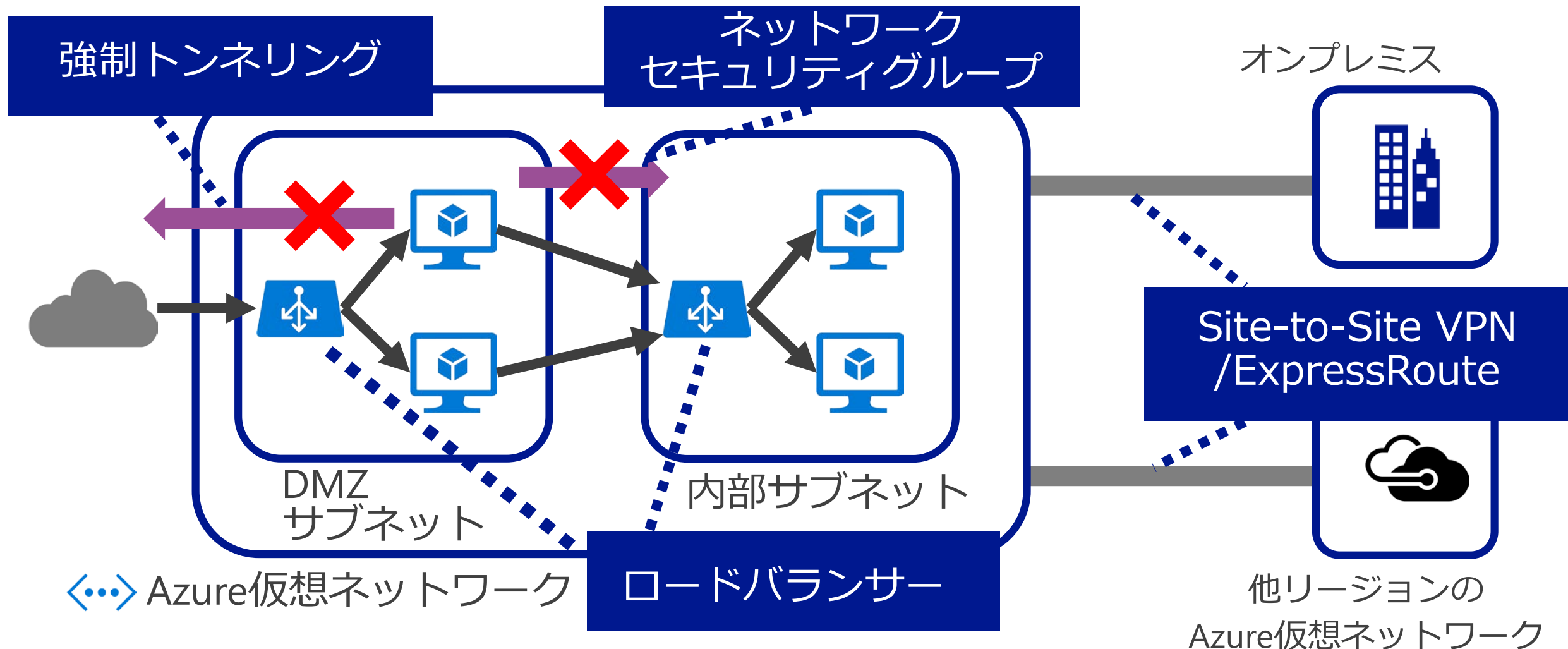
- リージョン内での3重化に加え、別リージョンに非同期で複製される。6重化。
- 複製されたデータは、災害が発生した時点で初めてアクセスできるようになる。

読み取りアクセス冗長ストレージ(RA-GRS)

- 通常時であっても、別リージョンに非同期で複製されたデータに読み取り専用でアクセスできる。

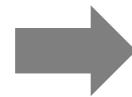
ネットワーク

- 一般的なネットワーク構成はほぼ組める機能が揃っている



バックアップ

ファイル・データの
バックアップ



Azure Backup

仮想マシン単位の
バックアップ



Azure Backup
for IaaS VM
(Preview)

バックアップ
データ
遠隔地保管



Azure Backup
(GRS)

セキュリティ

- やるべきことは、基本的にオンプレミスと変わらない。



複雑なパスワード



アプリケーション
脆弱性チェック



ファイアウォール



暗号化 など...

- インフラ部分はマイクロソフトががっちり守っています！

➤ 詳細はホワイトペーパーを参照

➤ <http://go.microsoft.com/fwlink/?linkid=392408&clcid=0x411>

Microsoft Azure

ホワイトペーパー

Microsoft Azure の
セキュリティ、プライバシー、
コンプライアンス



de:code

注意すべきは「管理ポータル」へのアクセス

- 管理ポータルは、パブリッククラウドにおける最大のセキュリティリスクポイントである

簡単なパスワード

退職者IDの放置



データ持ち出し

システム破壊

など、様々な危険が...

管理者IDのセキュリティ強化



- 推奨は**組織アカウント**で**オンプレAD連携** + **多要素認証**
- 多要素認証だけならMicrosoftアカウントでも組織アカウントでも無償！

Microsoftアカウントの失効に注意！

- Microsoftアカウントは一定期間ログインしないと失効してしまう
- そしてAzureアカウント管理者のIDが失効すると、Azureサブスクリプションも削除される
- <http://blogs.msdn.com/b/windowsazurej/archive/2014/12/25/be-aware-of-msaccount-expiration.aspx>
- 組織アカウント(Azure AD)を利用するか、定期的にログインする運用にすること

MSDN Blogs > Microsoft Azure Japan Team Blog (ブログ) > Azure を管理する Microsoft アカウントの失効にご注意を

Azure を管理する Microsoft アカウントの失効にご注意を



Ayako TANI 24 Dec 2014 11:40 PM 0

Microsoft Azure の「アカウント管理者」として登録されている Microsoft アカウントが失効すると、Azure サブスクリプションが無効化されてしまいます。

通常時、Azure の管理を共同管理者やサービス管理者の ID のみで運用していて、アカウント管理者の ID では管理ポータルやアカウントポータルにアクセスしていないという場合はご注意ください。

Consumerサービスとして提供されている Microsoft アカウントは連続して 2 年以上サインインしていない場合、サーバーから自動的に削除されます。アカウントへの「サインイン」の例としては下記のようなものがあります。

サインイン先の例

- OneDrive (<https://onedrive.live.com/about/ja-jp/>)
- Azure アカウントポータル (<https://account.windowsazure.com>)
- Azure 管理ポータル (<https://manage.windowsazure.com>)

有効期限が切れたMicrosoft アカウントでサインインを試みようとした場合は、「指定した Microsoft アカウントは登録されていません。」というメッセージが表示され、サインインできません。この Microsoft アカウントをアカウント管理者として作成された Azure サブスクリプションは無効化されてしまいます。現在のところ、失効前の通知などはありませんので、Azure のアカウント管理者となっている ID によるサインインを定期的に行っていただくようお願いします。

次世代Azure IaaSの新機能

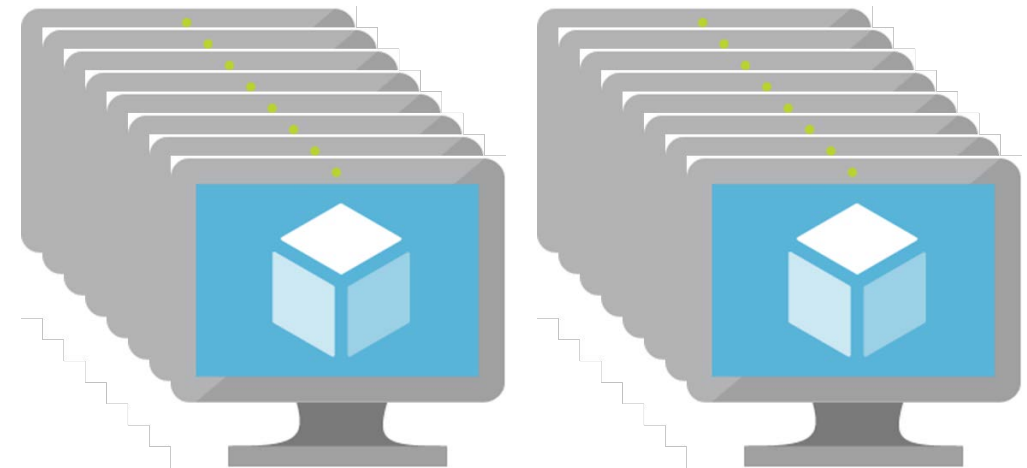
以降の内容は現時点でプレビューの機能です。

米国東部、米国西部、ヨーロッパ西部、東アジアおよび東南アジアで利用可能です。

Azure IaaS v2

- 大量の仮想マシンをパラレルに展開可能
- アベイラビリティセット内に3つの障害ドメイン
 - これまでは2つ
- ネットワーク関連リソースモデルの改善
- カスタムスクリプトVM拡張にカスタムURLを指定可能
- Azure Key Vaultとの統合

そのベースとなっているのが...



基盤となる管理APIのモデルが変わります

Azure
Service Management
(ASM)

XMLベース



Azure
Resource Manager
(ARM)

JSONベース

複数リソースから構成される複雑なシステムを、
JSON形式のテンプレートファイルで表現し、展開できる

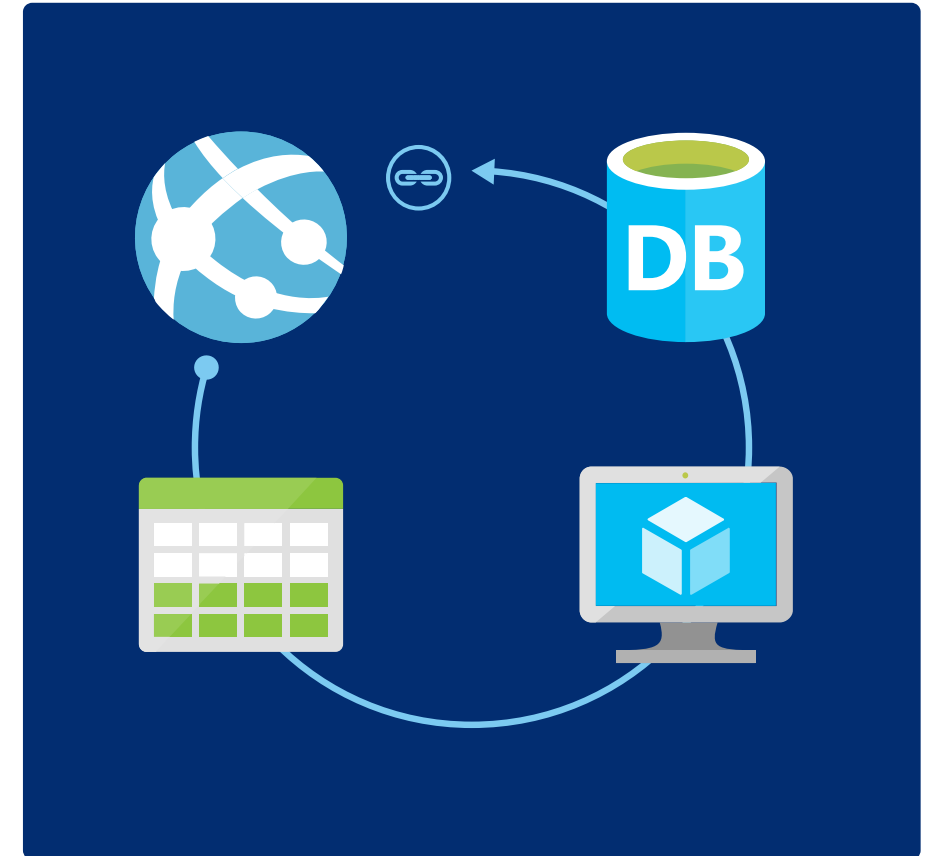
Azure Resource Managerで変わること

概念	Azure Service Management (XML)	Azure Resource Manager (JSON)
クラウドサービス	VMのコンテナ	考慮不要
可用性セット	各VMのラベルとして設定	新規リソースタイプ
NIC	各VMの一要素	新規リソースタイプ、 VMとは独立したライフサイクル
ロードバランサー	クラウドサービスの一機能	新規リソースタイプ
DNS名	クラウドサービスに自動的にアサインされるDNS名 <name>.cloudapp.net	パブリックIPリソースに指定可能なオプションリソース <name>.<region>.cloudapp.azure.com

その他いろいろあります

リソースグループ

- 複数のリソースを束ねる論理的な器
- 関連する各種リソースを種類をまたいで一覧・一括管理できる
- 全てのリソースは必ず 1 つのリソースグループに紐づけられる



頑張ってコツコツとJSONファイルを作りました！

```
    "vmSize": [
      {
        "type": "string",
        "defaultValue": "Standard_A0",
        "allowedValues": [
          "Standard_A0",
          "Standard_A1",
          "Standard_A2",
          "Standard_A3",
          "Standard_A4"
        ]
      },
      {
        "type": "string",
        "description": "This is the allowed list of vm sizes"
      }
    ],
    "variables": {
      "availabilitySetName": "[concat('availabilitySet-', variables('storageAccountName'))]",
      "storageAccountType": "Standard_LRS",
      "subnetName": "backendSubnet",
      "vnetID": "[resourceId('Microsoft.Network/virtualNetworks', parameters('virtualNetworkName'))]",
      "subnetRef": "[concat(variables('vnetID'), '/subnets/', variables('subnetName'))]",
      "numberOfInstances": 2,
      "lbID": "[resourceId('Microsoft.Network/loadBalancers', parameters('loadBalancerName'))]"
    },
    "resources": [
      {
        "apiVersion": "2015-05-01-preview",
        "type": "Microsoft.Storage/storageAccounts",
        "name": "[parameters('newStorageAccountName')]",
        "location": "[resourceGroup().location]",
        "tags": {
          "displayName": "StorageAccount"
        }
      }
    ]
  }
}
```

**なんてことは言わないので
安心して下さい！**

テンプレートはゼロから作らなくてもOK

- Azure クイック スタート テンプレート
- <http://azure.microsoft.com/ja-jp/documentation/templates/>
- ここからAzureポータル経由で直接編集 & デプロイできる

Microsoft Azure

セールス 1-800-867-1389 | アカウント | ポータル | 検索

機能 料金 ドキュメント ダウンロード Marketplace ブログ コミュニティ サポート

無料評価版 >

Azure クイック スタート テンプレート

Azure リソース マネージャーを通じてコミュニティ提供のテンプレートで Azure リソースをデプロイし、生産性を高めます。デプロイ、学習、フォークして、自分も貢献しましょう。

Azure リソース マネージャーとは

Azure リソース マネージャーでは、宣言テンプレートを使用して、アプリケーションをプロビジョニングできます。1 つのテンプレートで、複数のサービスとその依存関係をデプロイできます。アプリケーション ライフサイクルの各ステージで、同じテンプレートを使用して、アプリケーションを繰り返しデプロイします。

詳細情報 ▶

検索

並べ替え: 追加日 ▼

テンプレート	GITHUB 作成者	説明	公開
List Azure Storage Account keys-Windows Custom...	singhkay	This template creates a Windows VM and ru...	2015/05...
Deploy a CoreOS cluster hosting Fleet	nmackenzie	CoreOS cluster hosting Fleet	2015/05...
OS Patching extension on a Ubuntu VM	thomas1206	This template creates a Ubuntu VM and inst...	2015/05...
Create one HPC cluster with custom compute node...	justintian	This template creates one allinone HPC clus...	2015/05...
IIS Server using DSC extension on a Windows VM	singhkay	This template creates a VM with IIS server...	2015/05...
High IOPS 32 Data Disk storage pool Standard D1...	jvallery	Create a Standard D14 VM from 32 Data Di...	2015/05...
Create an new HA SharePoint Farm	simonandruiz	This template creates a Highly Available Sh...	2015/05...

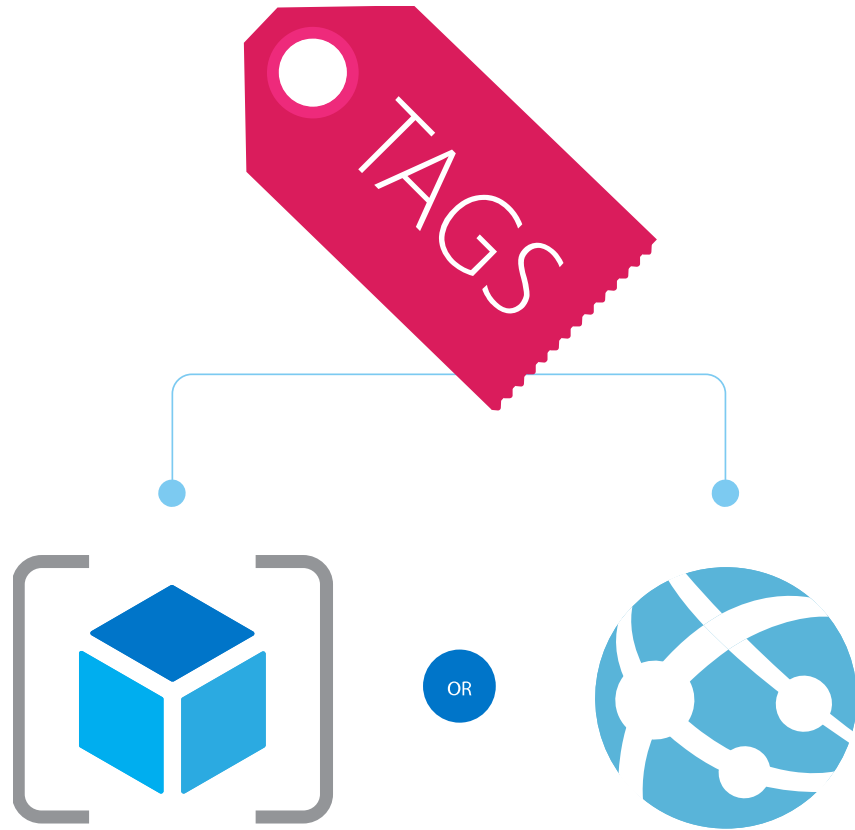
Visual Studioからも

Visual StudioのAzure Resource Group管理画面のスクリーンショット。JSON アウトラインで、resources (6) が展開されており、StorageAccount、AvailabilitySet、VirtualNetwork、NetworkInterface、LoadBalancer、VirtualMachines がリストアップされている。中央のJSONエディタには、LoadBalancedVirtualMachine.json が開かれ、https://schema.management.azure.com/schemas/2015-01-01/deploymentTemplate.json# のURLが示されている。右側のパネルには、パラメーターの編集ダイアログボックスが表示されている。このダイアログボックスには、次のパラメーター値がこの配置に使用されます:

パラメーター名	値
virtualNetworkName	vnet01
networkInterfaceName	nic01
loadBalancerName	lb01
adminUsername	masadmin
adminPassword	●●●●●●●●
imagePublisher	MicrosoftWindowsServer
vmNamePrefix	BackendVM
imageOffer	WindowsServer
imageSKU	2012-R2-Datacenter
vmStorageAccountContainerName	vhds
vmName	vm01
newStorageAccountName	sa01
vmSize	Standard_A1

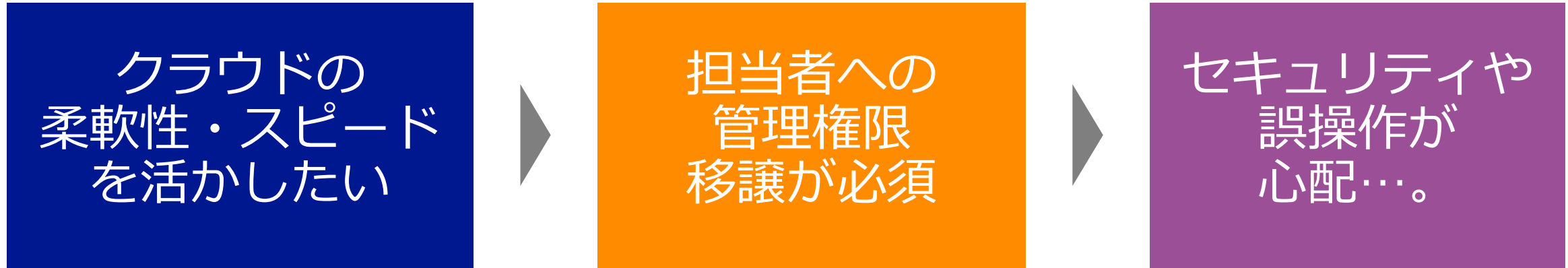
下部には「パスワードの保存(P)」のチェックボックスと「保存(S)」「キャンセル」ボタンがある。右側のパネルには「サインアウト」ボタンと「パラメーターの編集(P)...」ボタンがあり、「配置(E)」と「キャンセル」ボタンも表示されている。

リソースへのタグ付け



- 各リソースに名前(Key)と値(Value)のペアを設定できる。
 - 例えば“部署”=“経理部”など
- 1リソースあたり最大15のタグをつけられる
 - “作成者”とか“本番/開発/テスト”とか“ちょっとしたメモ”とか

RBAC (Role-Based Access Control)



- より細かい単位で、より細かい権限設定ができる。
- たとえば、
 - AさんはサブスクリプションXの設定を参照できる
 - Bさんは仮想ネットワークをYの設定を変更できる
 - Cさんは仮想マシンZの権限設定を変更できる

アクセス権は上位から継承される

サブスクリプション



リソースグループ



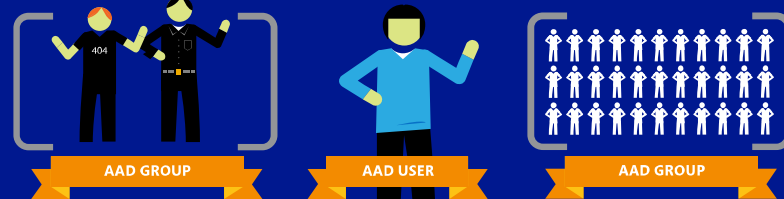
リソース



アクセス権の継承



CONTRIBUTORS OWNER READERS



CONTRIBUTORS OWNER READERS



CONTRIBUTORS OWNER READERS

Azure Resource Explorer

- Azure Resource Manager APIに直接アクセスするためのツール
 - <https://resources.azure.com/>
- ARMのイメージや機能を理解するのに役立つ
 - その気になれば直接APIを叩いて自分のサブスクリプションを操作することも可能

The screenshot displays the Azure Resource Explorer (Preview) interface. On the left, a sidebar shows a tree view of providers and subscriptions. The 'virtualMachines' resource is selected under the 'Microsoft.Compute' provider. The main panel shows the 'virtualMachines' resource with a search bar and a 'Data (GET, PUT)' button. Below the button, a green 'GET' button is visible. The right side of the panel displays the JSON response for the 'virtualMachines' resource, which includes details about the virtual machine's properties, hardware profile, storage profile, and operating system disk.

```
1 {
2   "value": [
3     {
4       "properties": {
5         "availabilitySet": {
6           "id": "/subscriptions/edfc72d7-9e71-424
7             ySets/AVSET"
8         },
9         "hardwareProfile": {
10          "vmSize": "Standard_A1"
11        },
12        "storageProfile": {
13          "imageReference": {
14            "publisher": "MicrosoftWindowsServer"
15            "offer": "WindowsServer",
16            "sku": "2012-R2-Datacenter",
17            "version": "latest"
18          },
19          "osDisk": {
20            "osType": "Windows",
21            "name": "osdisk",
22            "createOption": "FromImage",
23            "vhd": {
24              "uri": "http://hogesa.blob.core.win
25            },
26            "caching": "ReadWrite"
27          },
28          "dataDisks": []
29        }
30      }
31    ]
32  }
```

Infrastructure as Code の時代



インフラ管理の効率とスピードの向上

インフラ設計の共有・再利用

ARMテンプレートの特性

宣言型

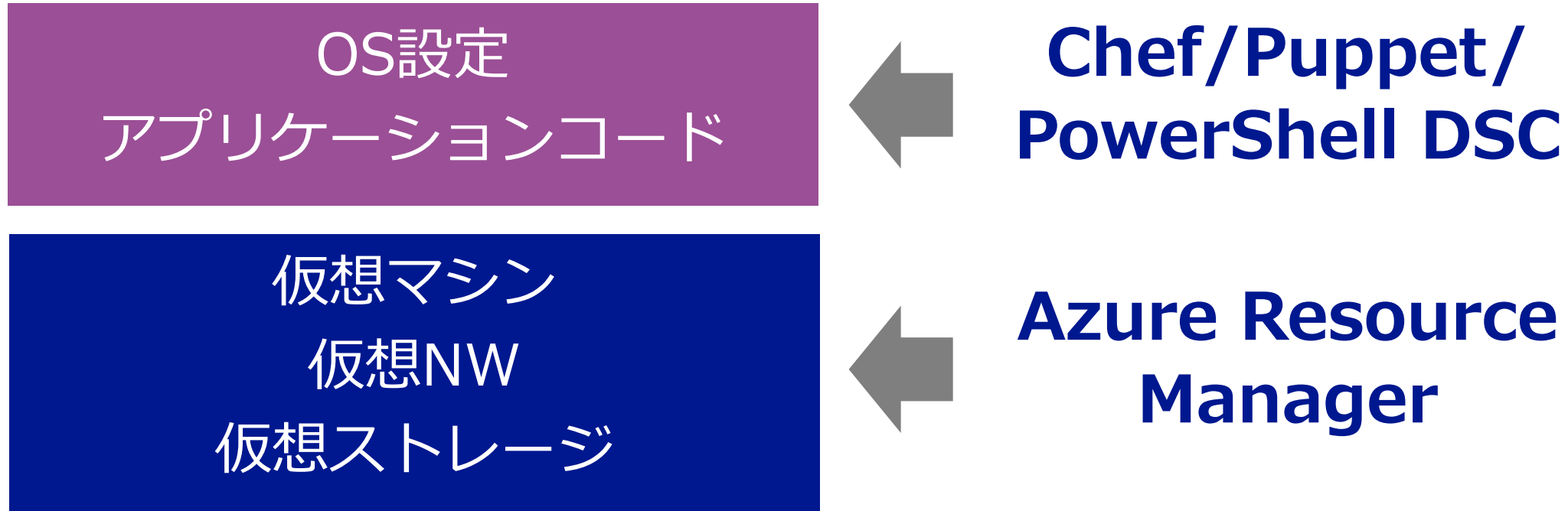
処理手順ではなく結果状態を記述する。

べき
等性

何度繰り返しても同じ結果になる。

Chef/Puppet/PowerShell DSCも同じ特性

Managed IaaS (IaaS+)



宣言的かつべき等なツールで、
インフラとVM内部の両方を構成

ARMテンプレートはクラウドとオンプレミス両方で

Tools



Microsoft Azure

+



Command Line

+



Visual Studio

SERVICE MANAGEMENT API

RESOURCE MANAGER



Cloud + On-Premises



ADFS

AAD

RESOURCE PROVIDER CONTRACT

Provider
Rest Points



...

Azure Stackでも
同じテンプレート
が使える！

さいごに

- **今後もAzure IaaSの進化は止まりません**
- **Azure IaaSの新機能を常にチェックし、
もっともっと便利にご活用ください！**

【 Session ID 】

de:code
TechEd + //build/

CDP-002

アンケートにご協力ください。

- アンケートに 上記の Session ID のブレイクアウトセッションにチェックを入れて下さい。
- アンケートはお帰りの際に、受付でご提出ください。
マイクロソフトスペシャルグッズと引換えさせていただきます。

Room F

de:code
TechEd + //build/

Ask the Speaker のご案内

- 本セッションの詳細は、EXPO 会場内『Ask the Speaker』コーナー
Room F カウンタにてご説明させていただきます。是非、お立ち寄りください。

