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

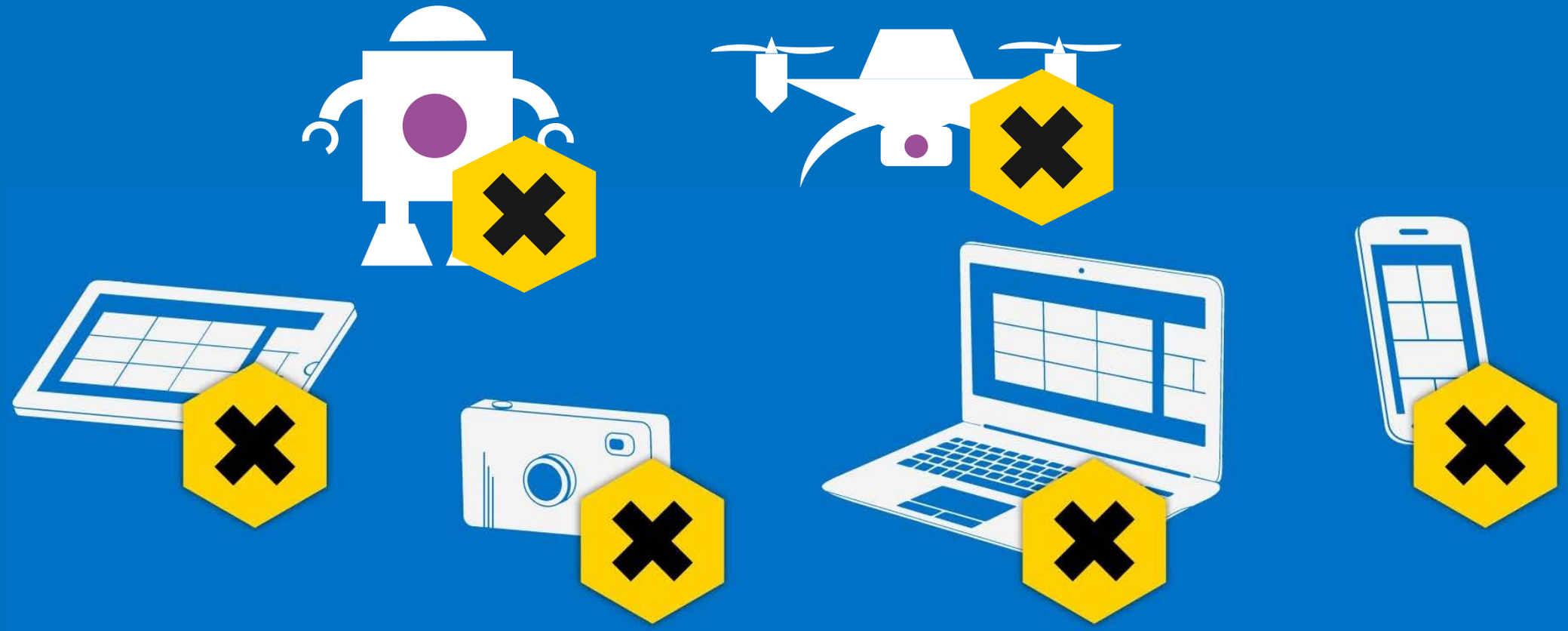
de:code
TechEd + //build/

Microsoft

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

クラウドで
システムを
作りたい！

それ、
SaaS使えば
よくない？

No

それ、
PaaSで
作れない？

No

**どうしても
必要な時は
IaaSで！**

Yes

**SaaSで！
(Office 365 等)**

Yes

**PaaSで！
(Web Apps 等)**

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 ?

＊2015/05/15時点の米国中部での価格です

Basic(基本) or Standard(標準) ?

＊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

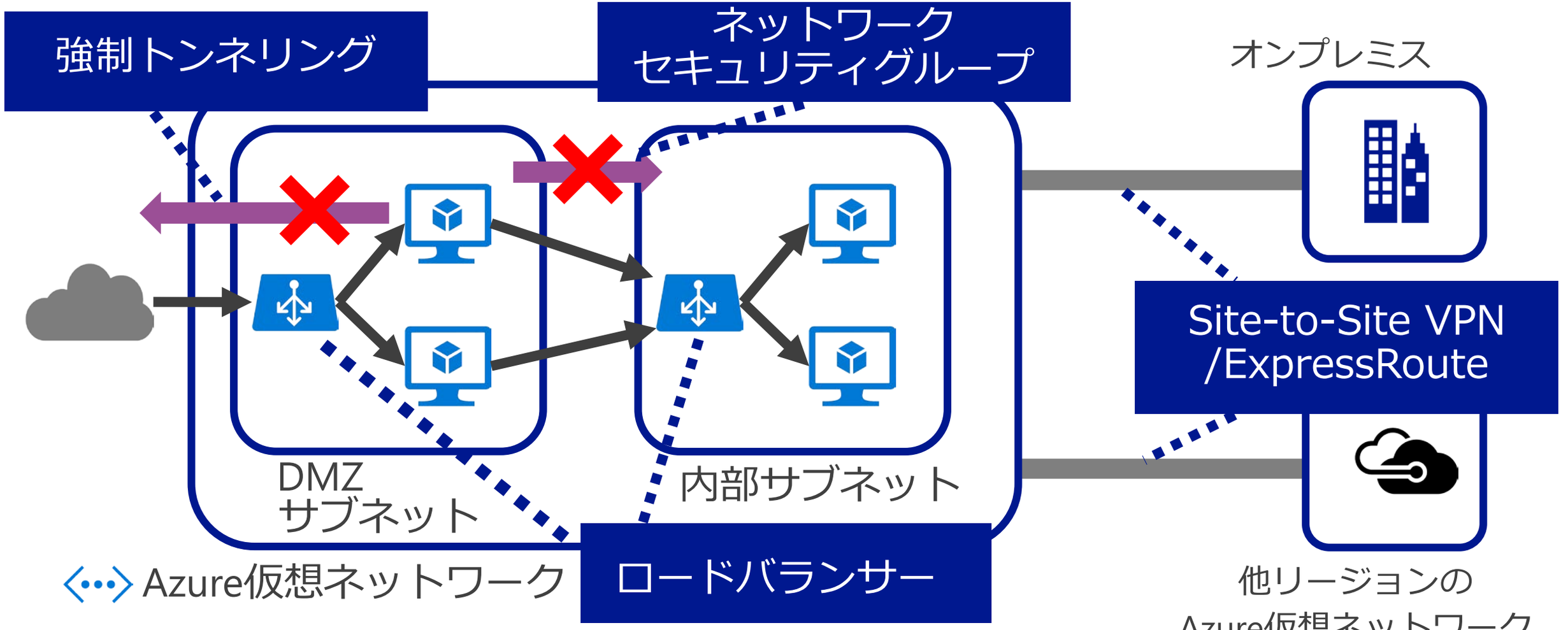
ローカル冗長ストレージ(LRS)
- リージョン内で3重化して保存される。

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。

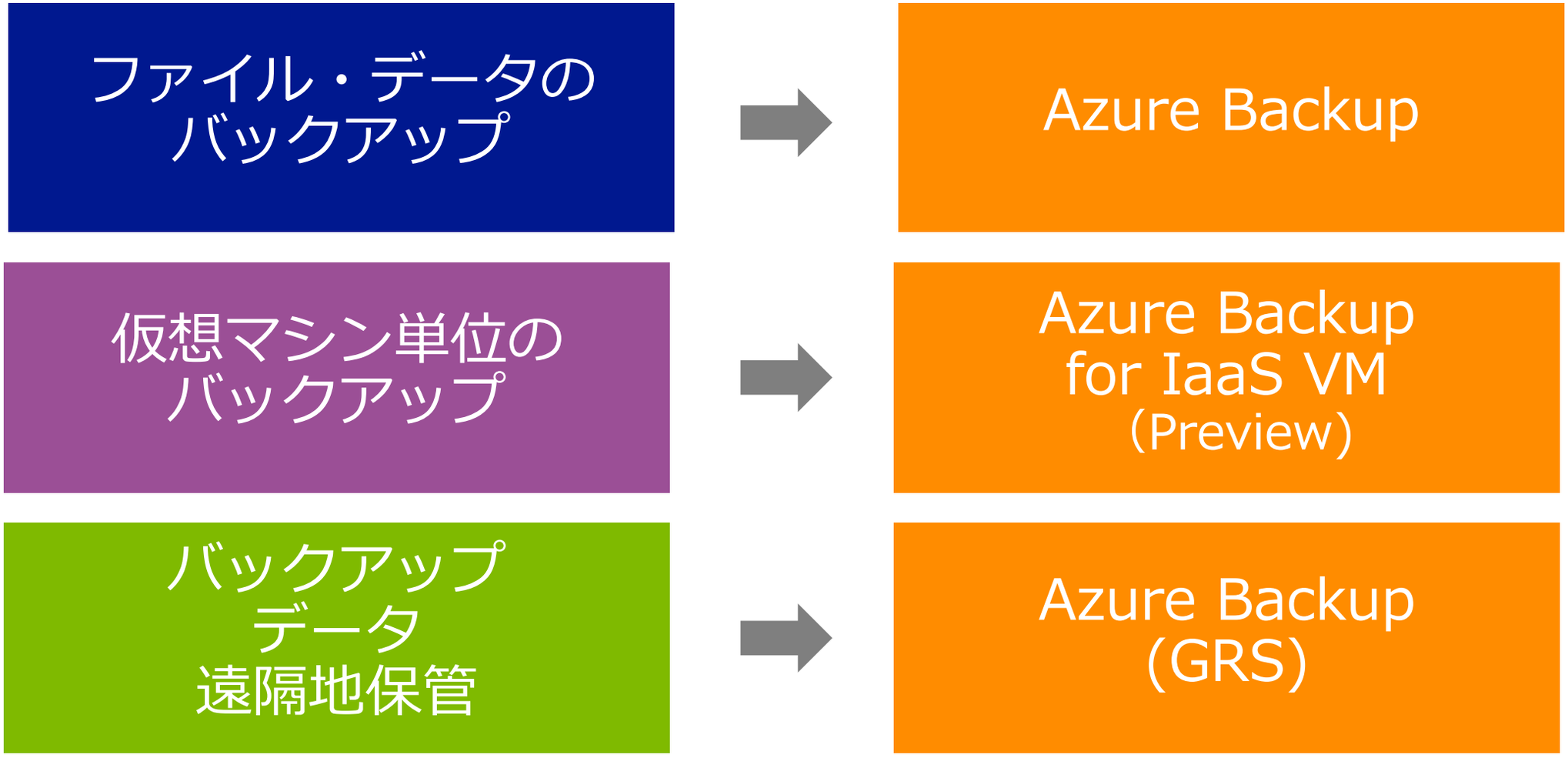
読み取りアクセス冗長ストレージ(RA-GRS)
- 通常時であっても、別リージョンに非同期で複製されたデータに読み取り専用でアクセスできる。

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。

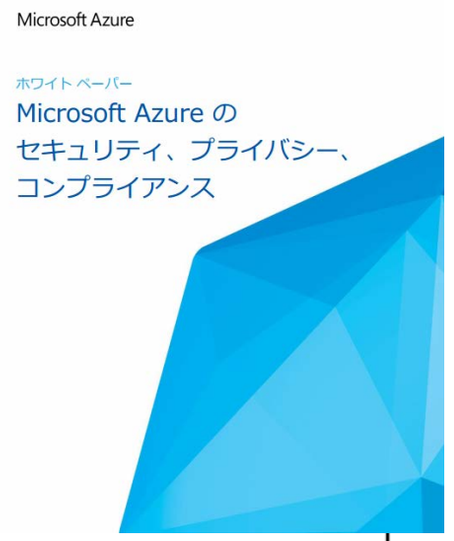

複雑なパスワード


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**<u>がっちり</u>**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



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

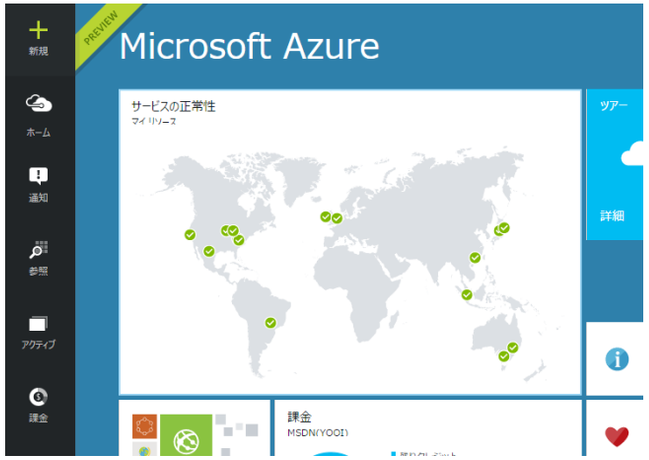
退職者IDの放置

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



Azureポータル

Microsoft
アカウント

組織アカウント
(Azure AD)

オンプレミス
AD/AD FS

多要素認証
(Multi-Factor Authentication)

- 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にお願いします。

次世代Azure IaaSの新機能

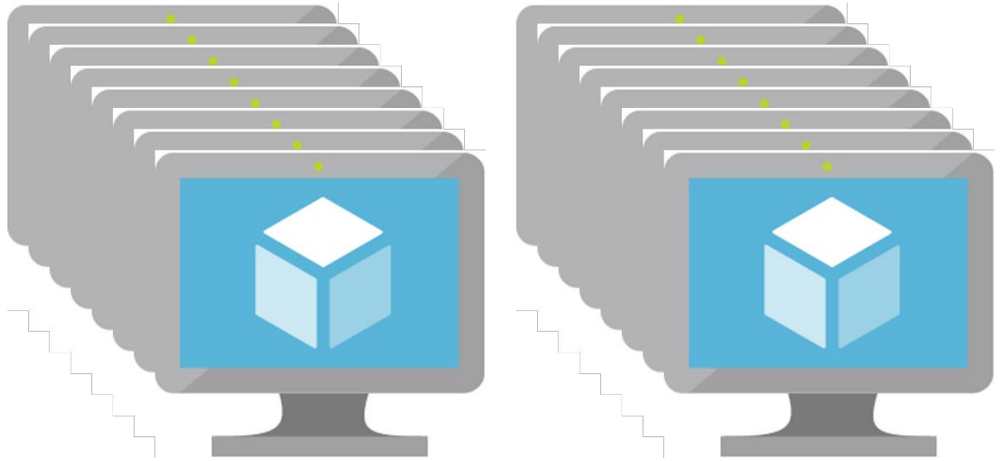
以降の内容は現時点でプレビューの機能です。

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。

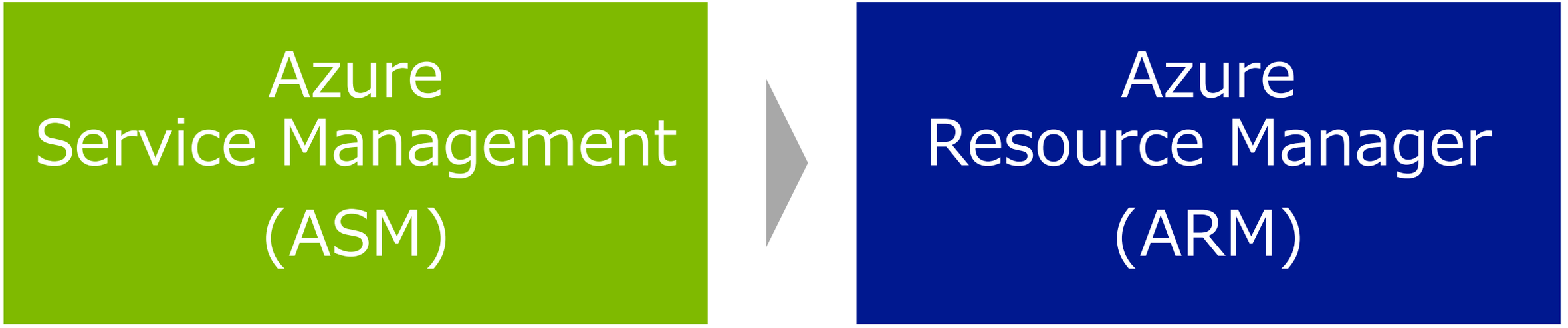
Azure IaaS v2

- 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



XMLベース

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

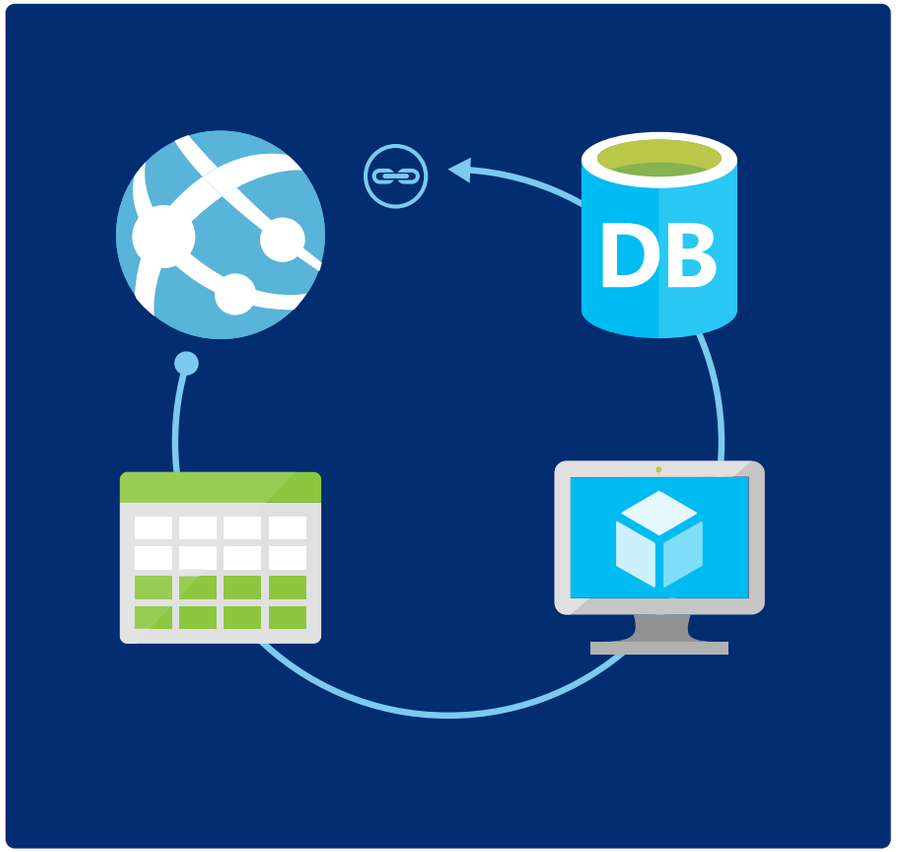
Azure Resource Managerで変わること

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ょう！

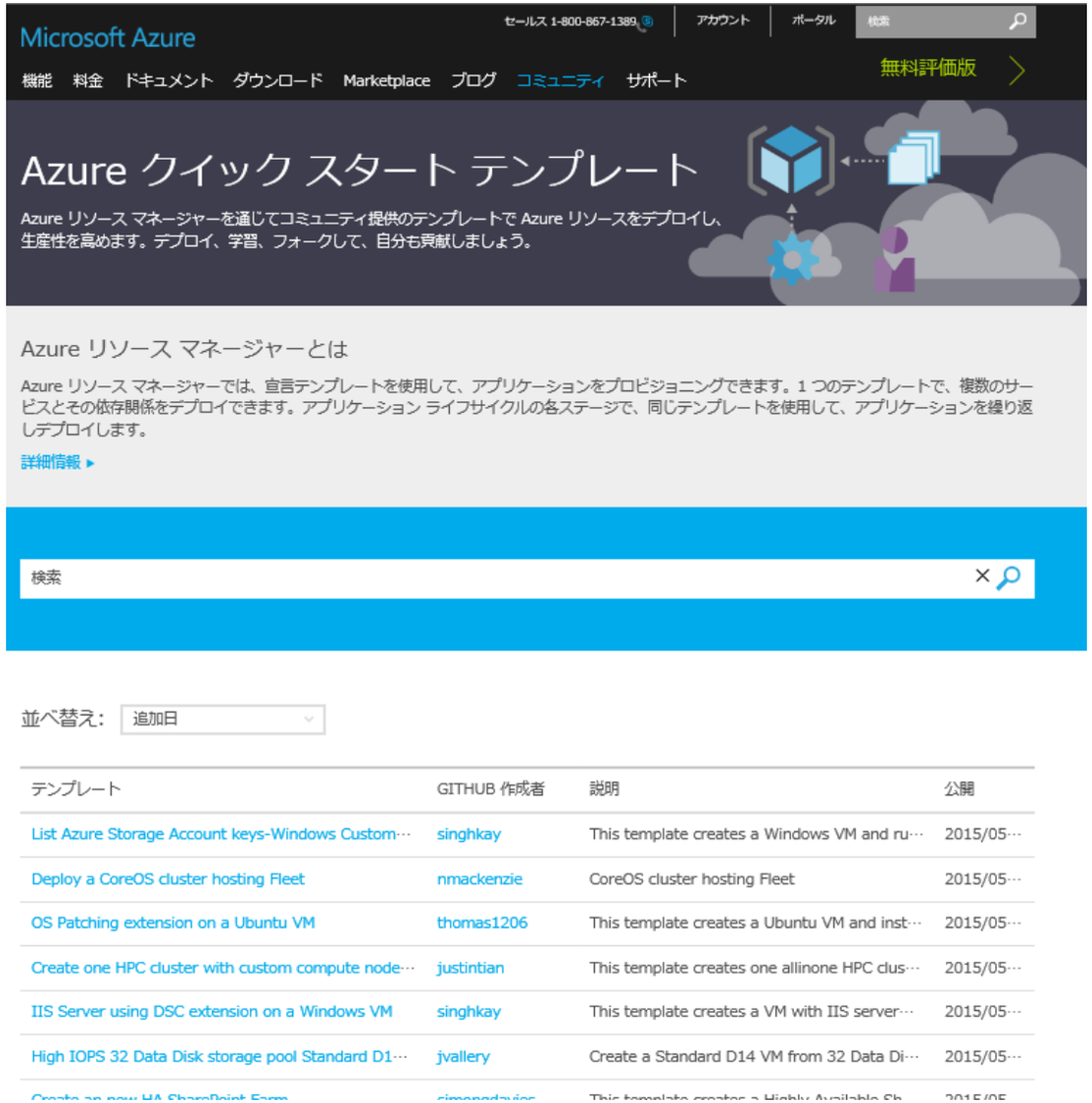
```
    "vmSize": {
        "type": "string",
        "defaultValue": "Standard_A0",
        "allowedValues": [
            "Standard_A0",
            "Standard_A1",
            "Standard_A2",
            "Standard_A3",
            "Standard_A4"
        ],
        "metadata": {
            "description": "This is the allowed list for VM sizes"
        }
    }
},
"variables": {
    "availabilitySetName": "AvSet",
    "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

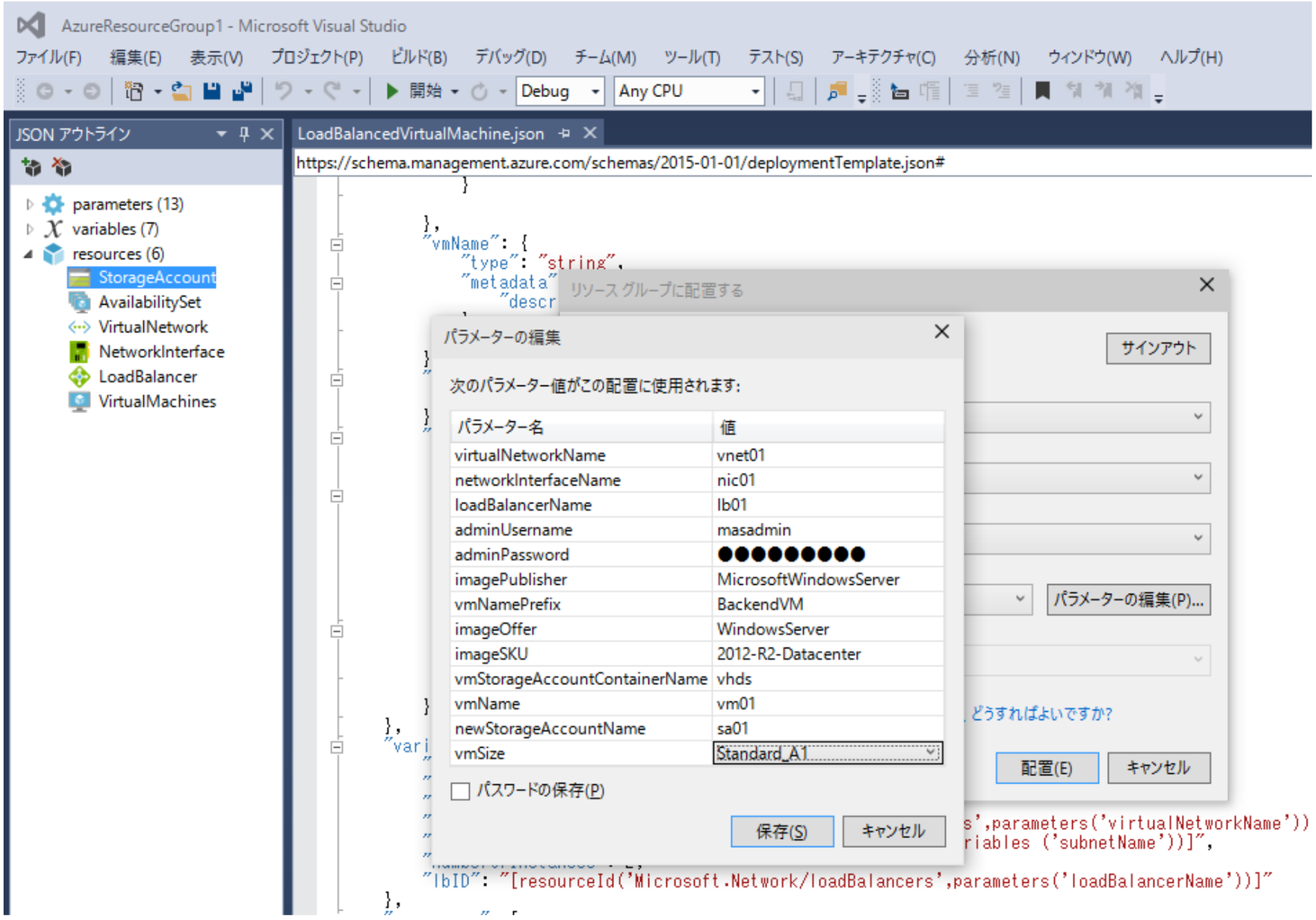
安心してください！

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

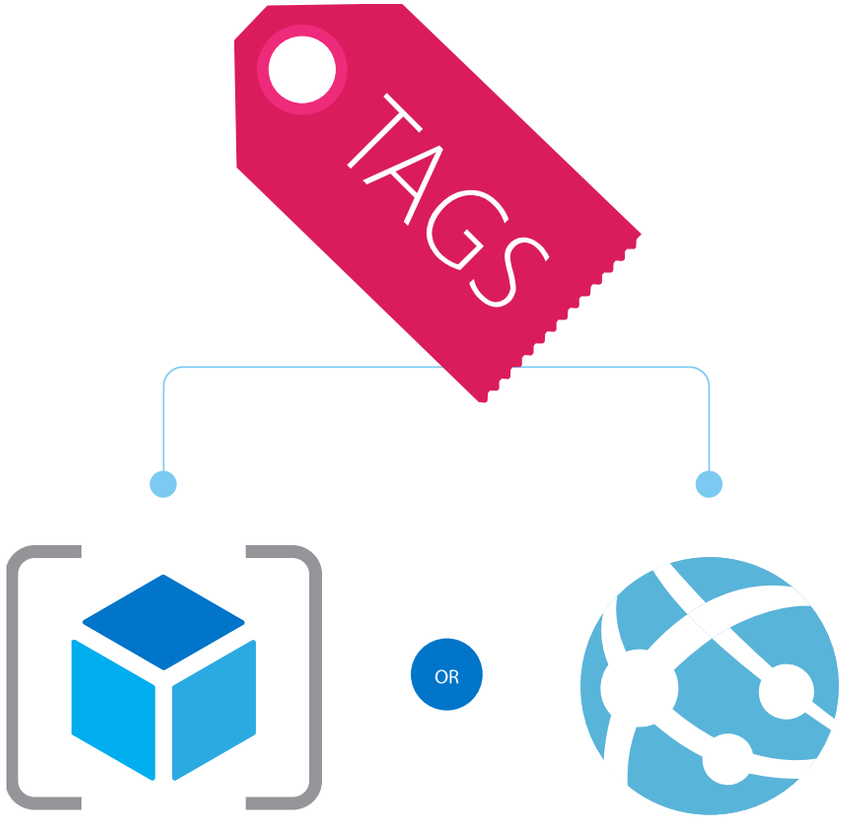


Visual Studioからも



de:code

リソースへのタグ付け

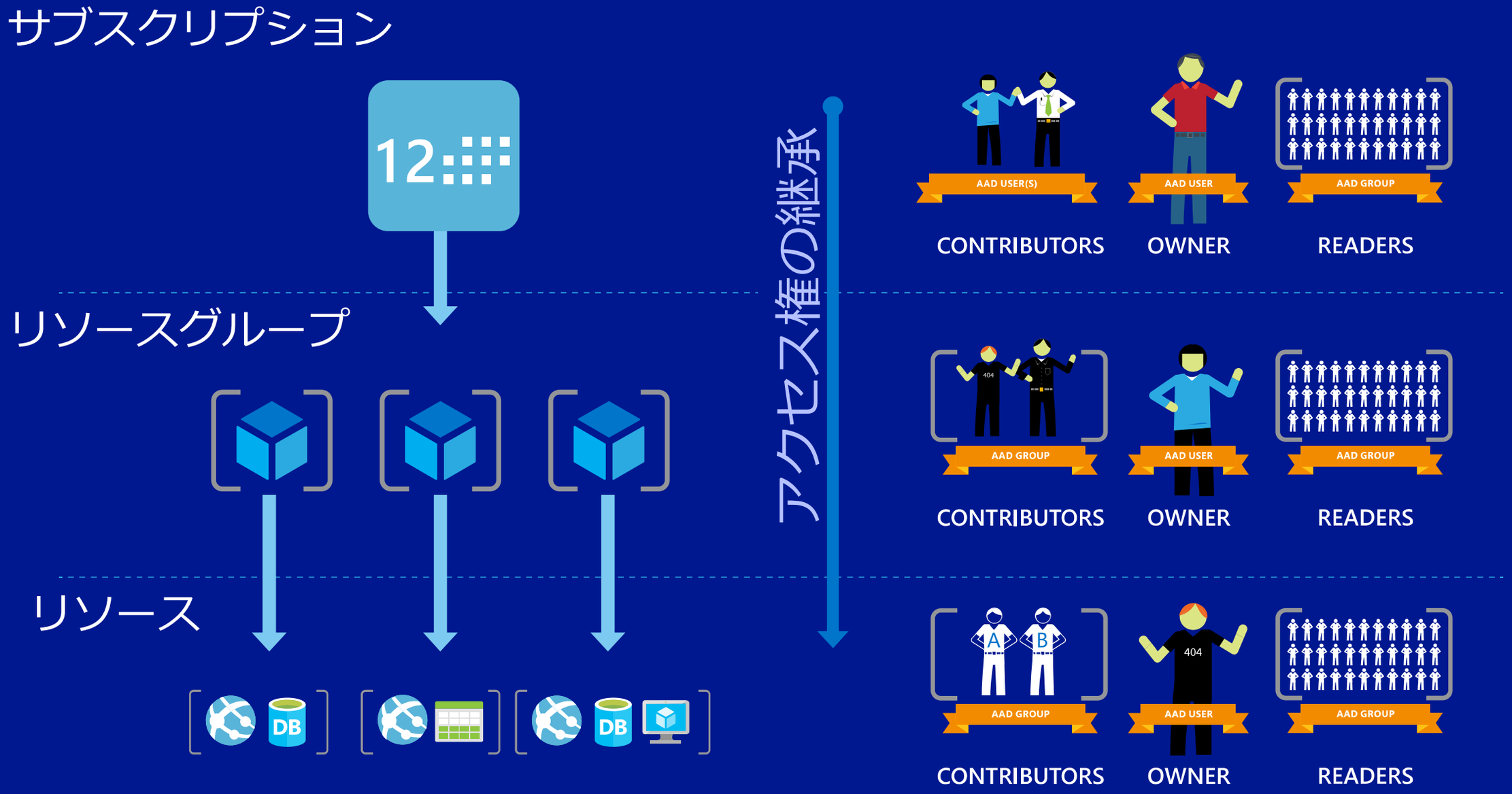


- 各リソースに名前(Key)と値(Value)のペアを設定できる。
  - 例えば“部署”=“経理部”など
- 1リソースあたり最大15のタグをつけられる
  - “作成者”とか“本番/開発/テスト”とか“ちょっとしたメモ”とか

RBAC (Role-Based Access Control)

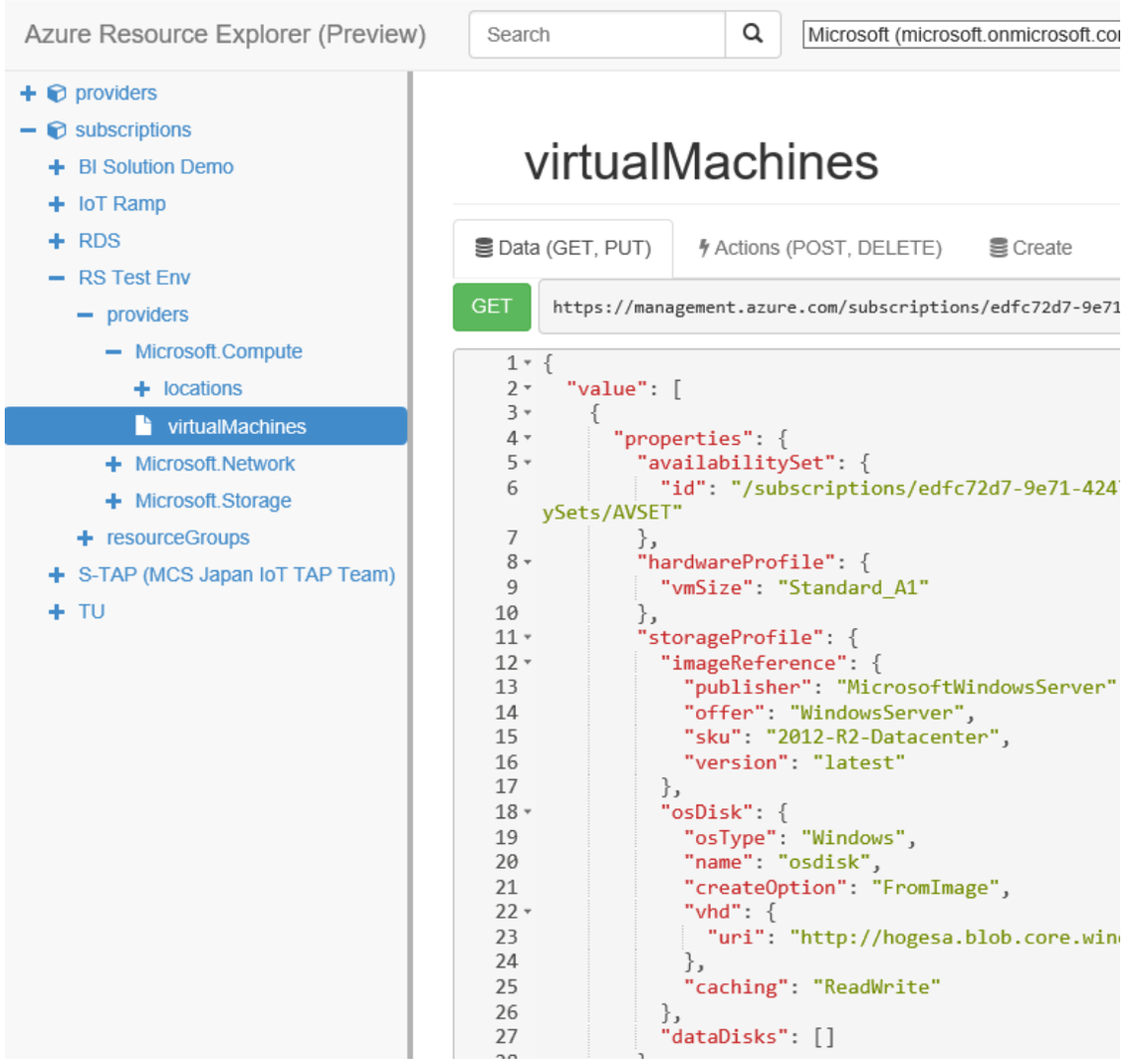
- より細かい単位で、より細かい権限設定ができる。
- たとえば、
  - Aさんはサブスクリプション**X**の設定を参照できる
  - Bさんは仮想ネットワーク**Y**の設定を変更できる
  - Cさんは仮想マシン**Z**の権限設定を変更できる

アクセス権は上位から継承される



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



Infrastructure as Code の時代

物理
サーバー

仮想
サーバー

サーバーは
JSONで
「論理的に」
表現される時代に！

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

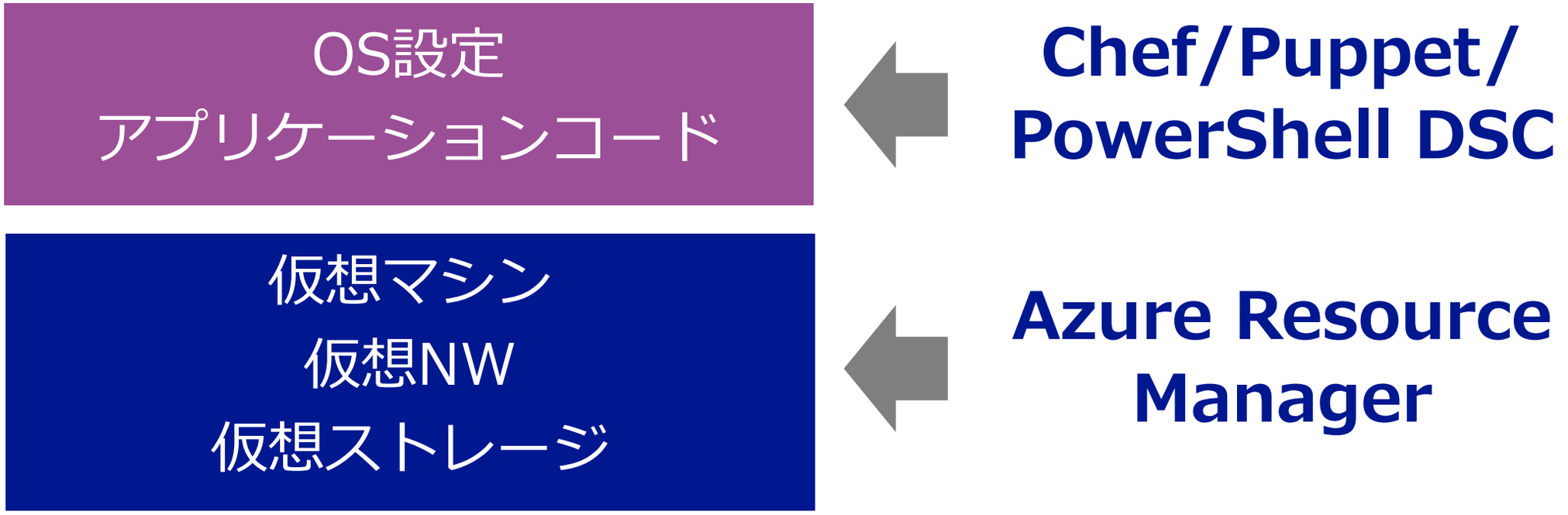
ARMテンプレートの特性

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+)



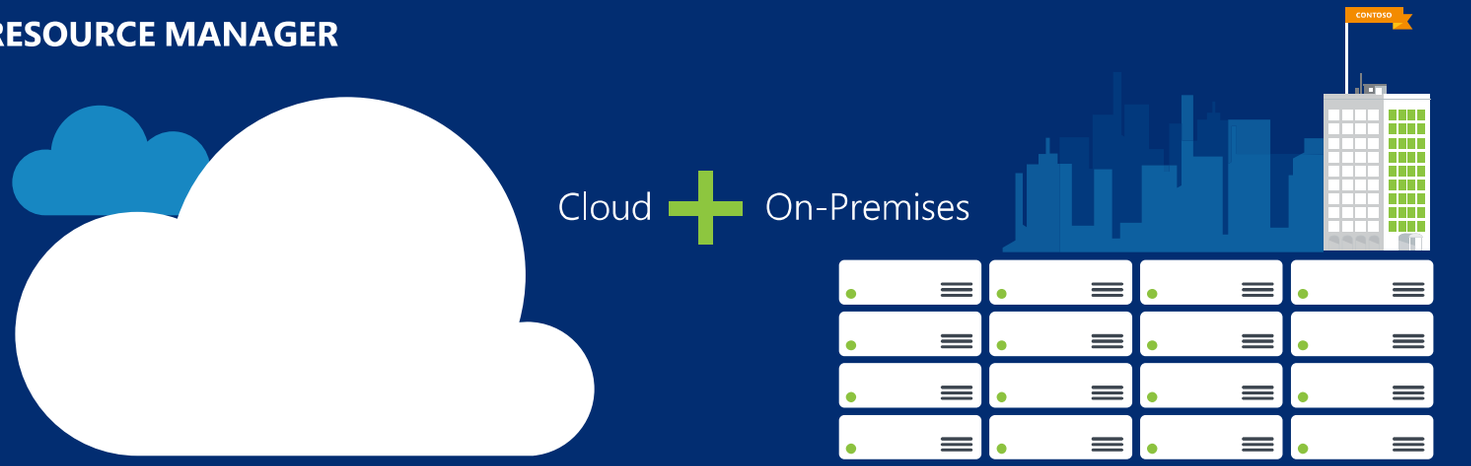
宣言的かつべき等なツールで、
インフラとVM内部の両方を構成

ARMテンプレートはクラウドとオンプレミス両方で

Tools

SERVICE MANAGEMENT API

RESOURCE MANAGER



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 】

CDP-002

de:code
TechEd + //build/

アンケートにご協力ください。

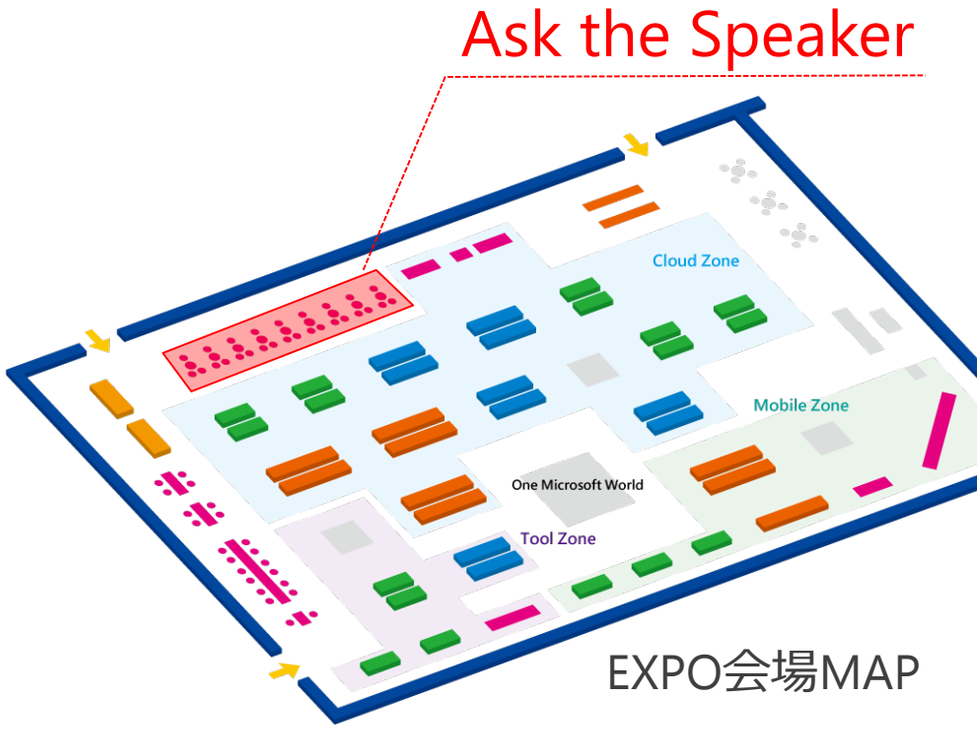
- アンケートに 上記の Session ID のブレイクアウトセッションにチェックを入れて下さい。
- アンケートはお帰りの際に、受付でご提出ください。
  マイクロソフトスペシャルグッズと引換えさせていただきます。

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。



EXPO会場MAP