



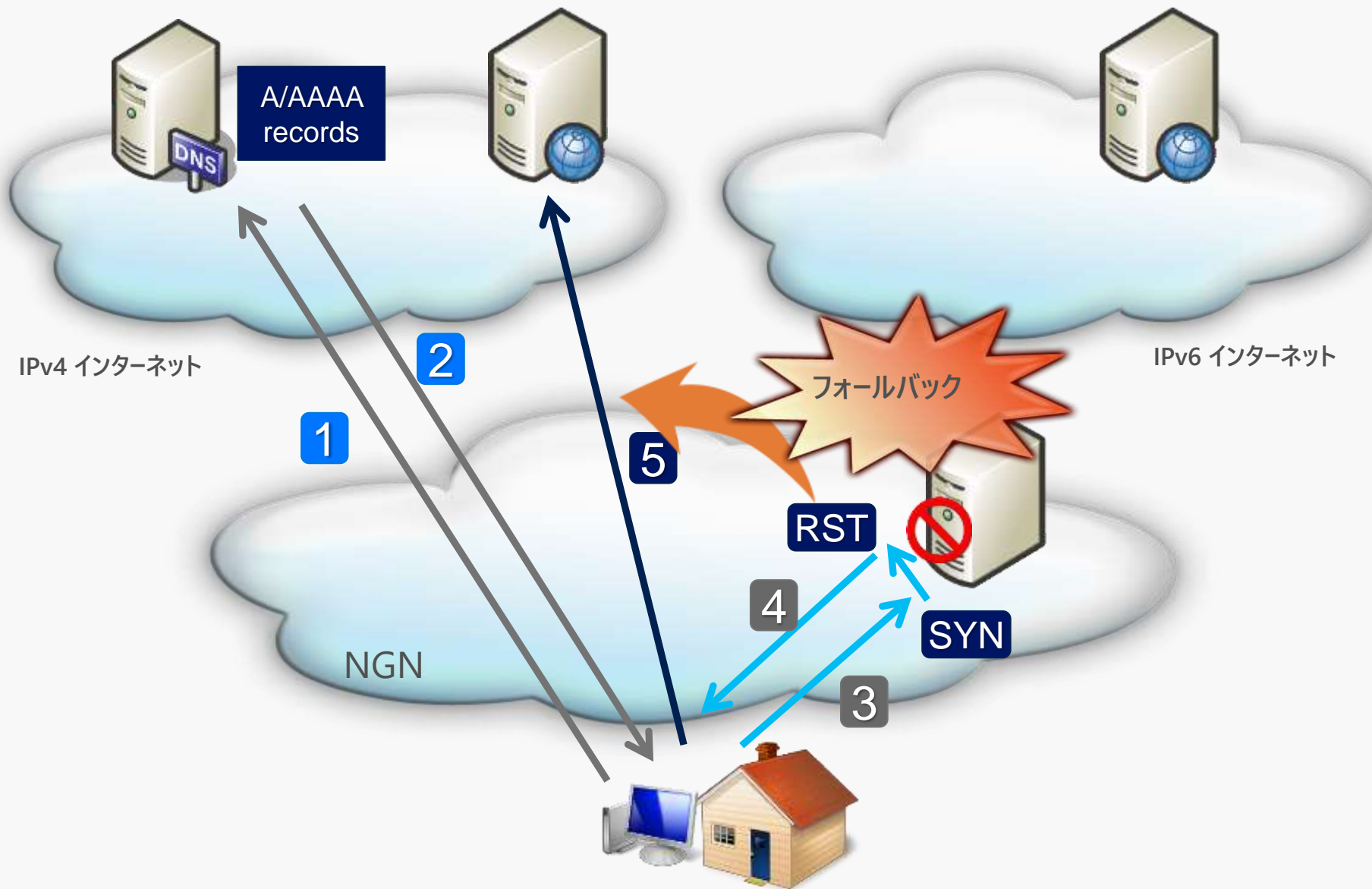
OSベンダー、クラウド事業者から見たIPv6

日本マイクロソフト株式会社
業務執行役 ナショナルテクノロジーオフィサー

田丸 健三郎

これまでの取り組み

TCP RSTへの即応する事への課題



IPv6の必要性について

～議論が尽くされているIPv6への移行の必要性～

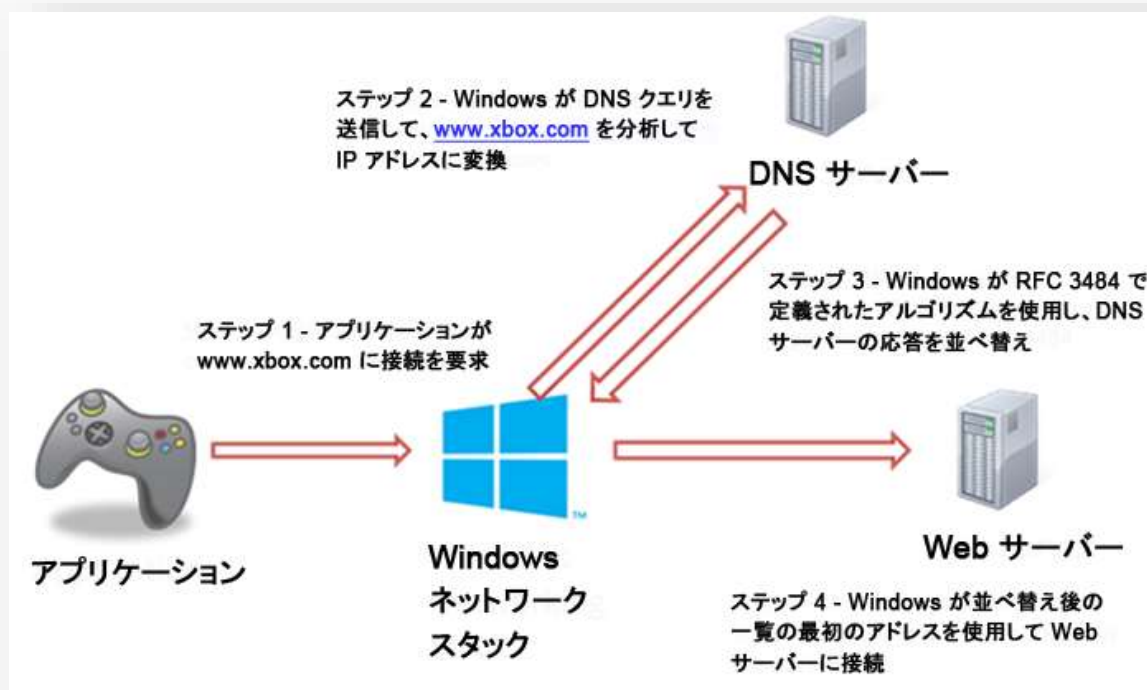
- ユーザーにとって乏しいIPv6使用のメリット
- ユーザーが使用出来るIPv4アドレスの枯渇
 - いつIPv6アドレスしか使用出来ないユーザーが現れる時期

| | IPv4 | IPv4 / IPv6 デュアルスタック | IPv6 Native |
|-------------------------|------|-------------------------|-------------|
| IPv4 | ○ | ○ | × |
| IPv4 / IPv6 デュアルスタック | ○ | ○ | ○ |
| IPv6 Native | × | ○ | ○ |

Windows8以降におけるIPv6アクセス

デュアルスタック ネットワークの接続アルゴリズム

- プロトコルの優先順位、DNSの応答性などにより、使用するプロトコルを選択。
- アクセス先のアドレス選択アルゴリズムへの追加



RFC 3484 (Rule 5 と6の間)

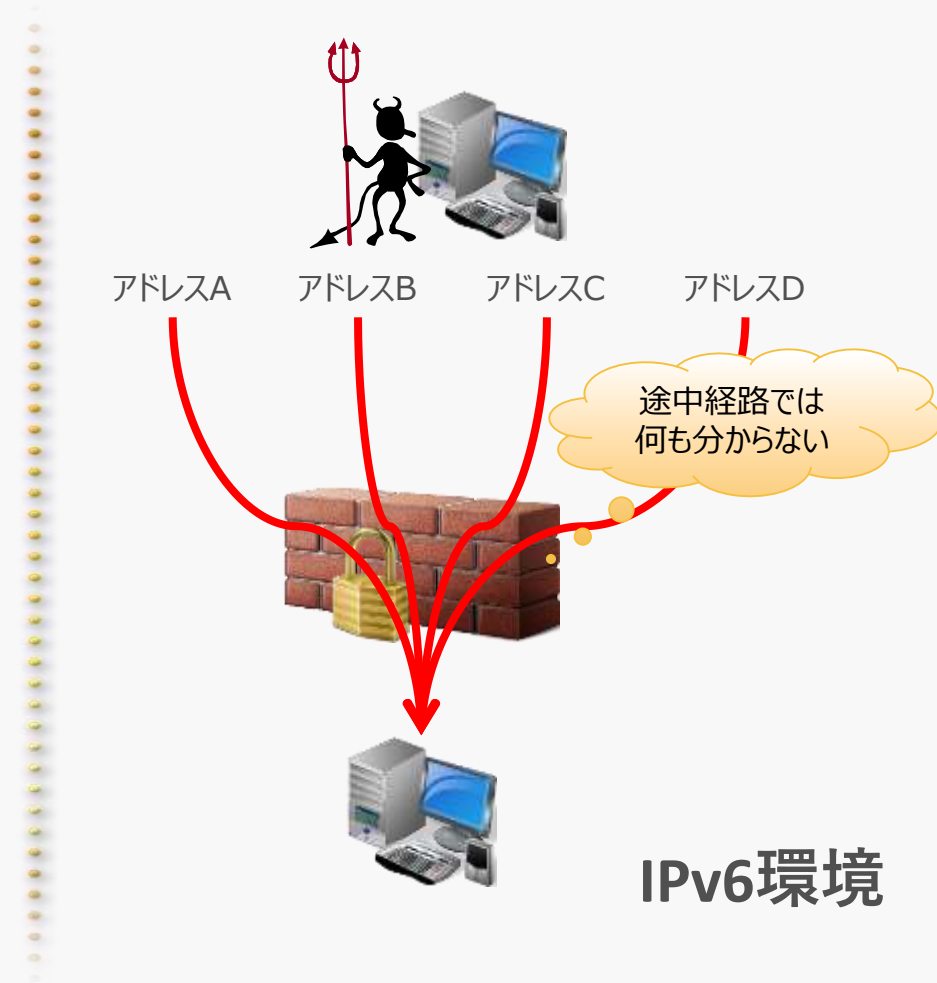
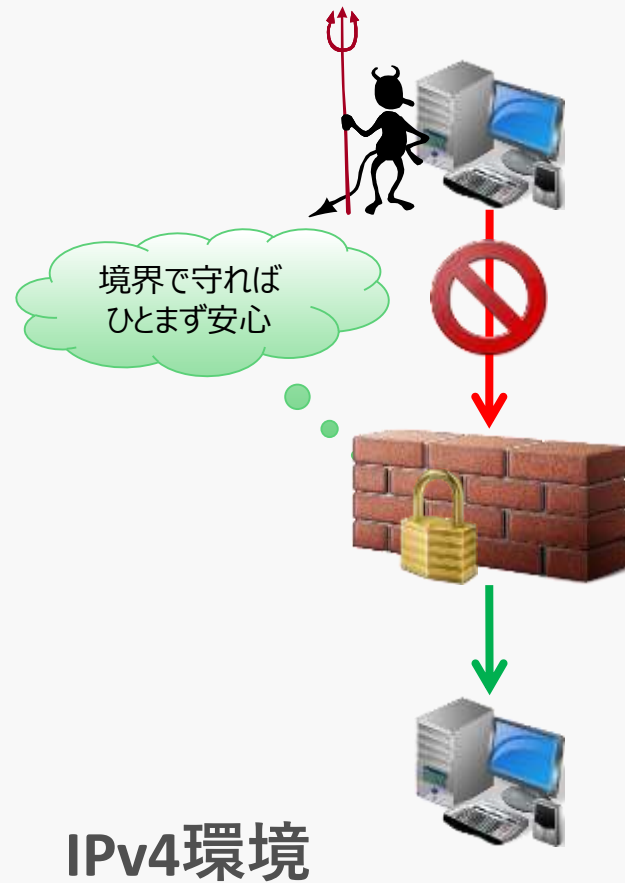
- Windows8以降では、IPv6 のルータビリティ (経路制御可能性) を広告する新規ネットワークへの接続時に、IPv6 接続をテストします。テストには、実際にインターネット上に存在するサーバーに対して、HTTPプロトコルを使用して行います。
- IPv6プロトコルを使用してインターネット上のサーバーにアクセスできず、フォールバックが発生するネットワークでは、IPv4を使用します。
- このアプローチにより、構成に誤りのあるデュアルスタックネットワークに接続されている環境では、標準のWindows APIを使用しているアプリケーションにおいては、IPv6からIPv4へのフォールバックによる遅延の影響を回避出来ます。

企業ネットワーク

- 企業ユーザーが固有のルーティング情報を特定のターゲットに提供している場合、Windows8以降は、Windows によって判定された接続とかわりなく、その優先設定に従います。企業ユーザーの環境の場合、Windows では、ルートを構成したネットワーク管理者が、特にそのルートの使用を推奨していると想定します。
- この変更は Web プロキシのあるネットワーク上には適用されません。これらのネットワークでは、プロキシがインターネットへの接続を提供するため、エンドツーエンドのIPv6 の接続テストは有益ではありません。その代わりに、Windows8以降では、可能な限り効率的な方法で、単純にそのプロキシへの接続を開始します。

さて、これまでの
セキュリティに関する議論は？

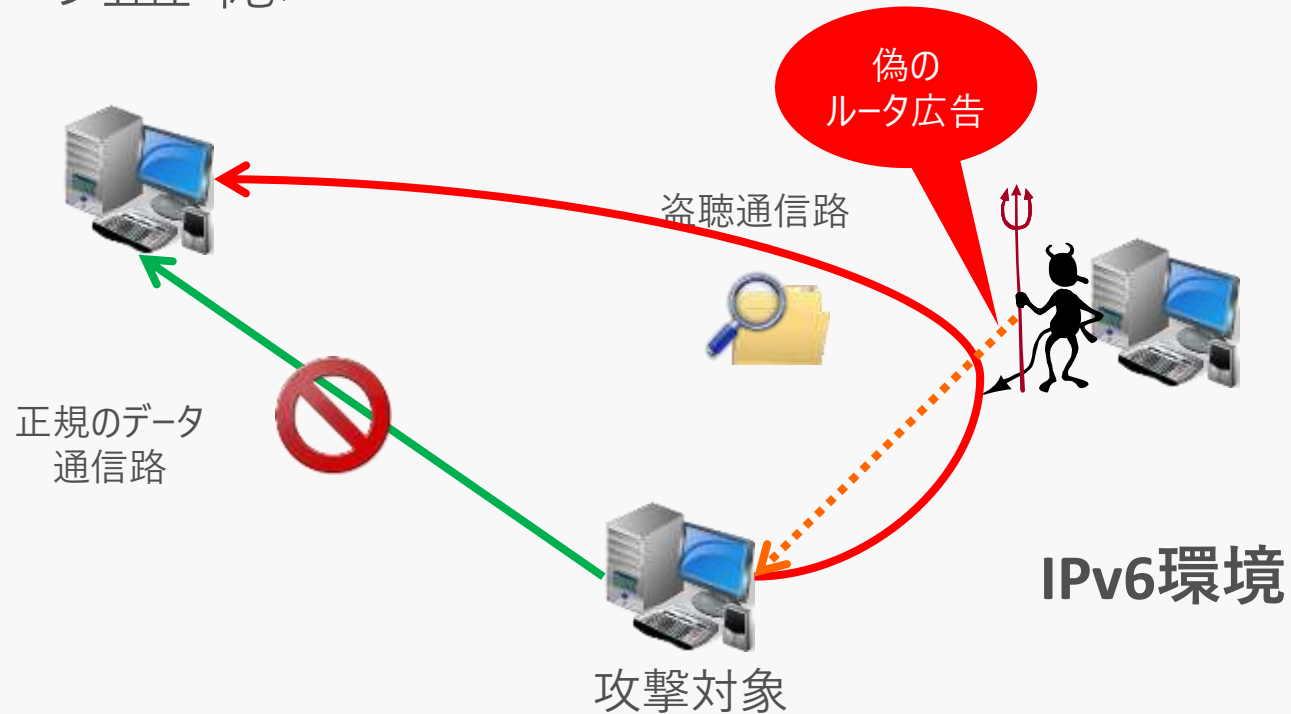
IPv6 環境におけるセキュリティ上の課題 ～ 氷山の一角 ～



セキュリティ上の課題

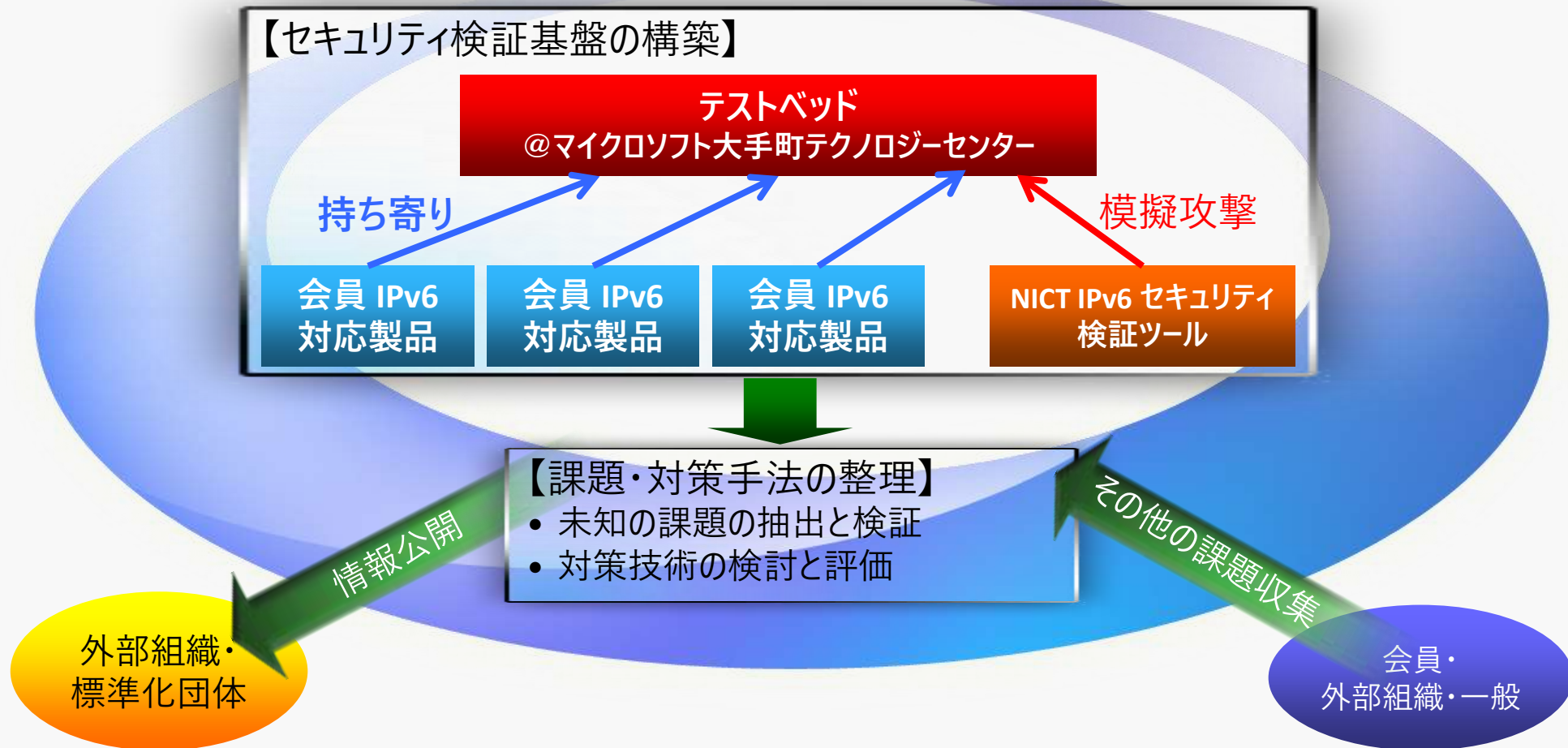
～ 自動設定機能の弊害 ～

- IPv6 のプラグアンドプレイ機能 (自動設定機能) を悪用したデータの盗聴

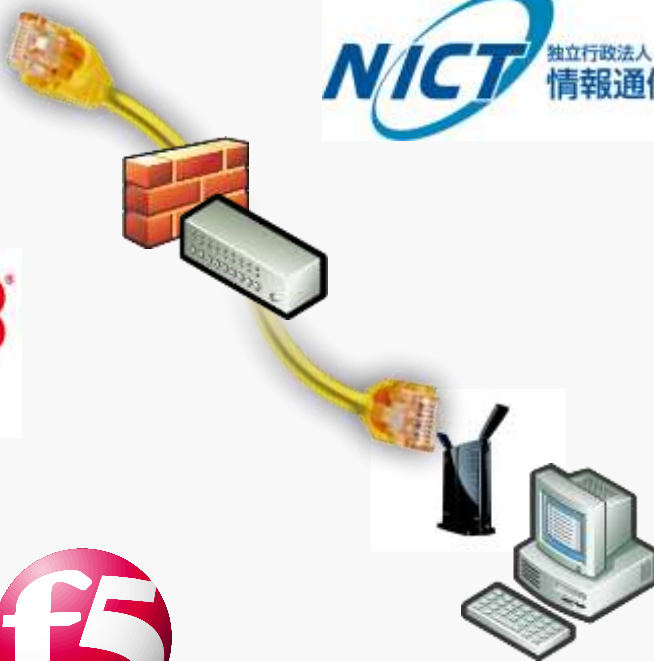


IPv6 技術検証協議会の設立

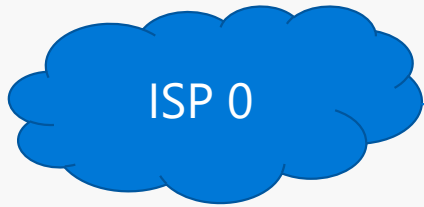
IPv6 技術検証協議会



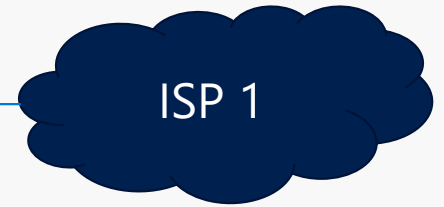
会員企業



検証環境構築



ISP 0

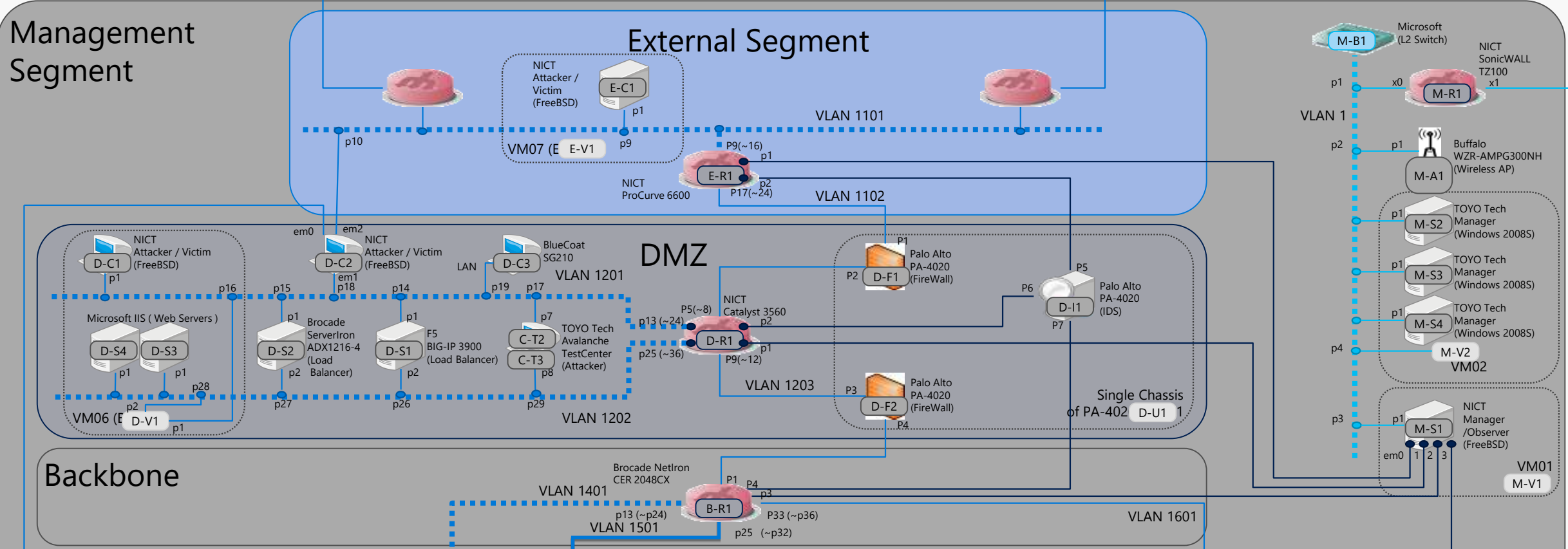


ISP 1



Management Segment

External Segment

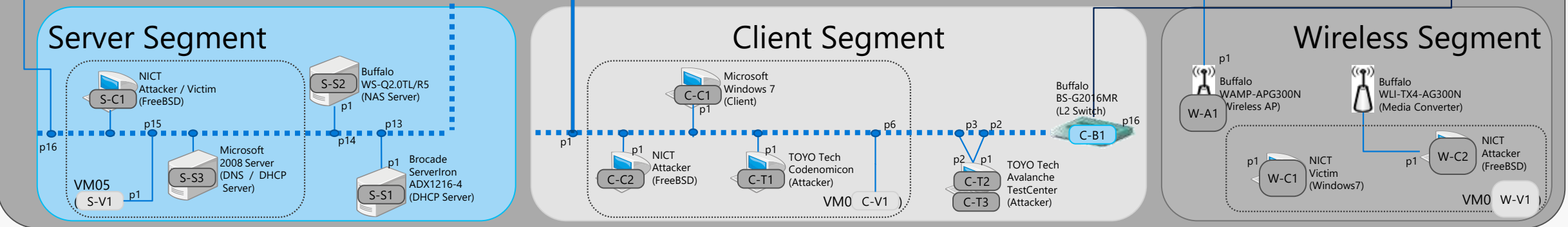


Backbone

Server Segment

Client Segment

Wireless Segment

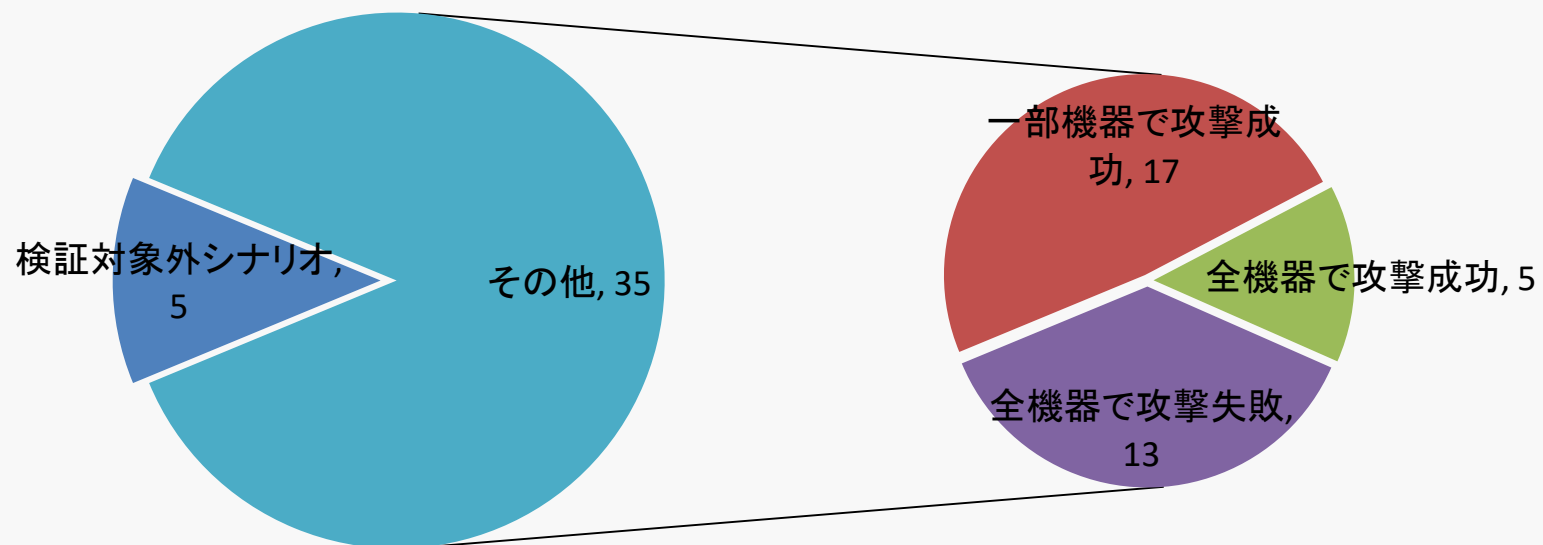


各社提供機材

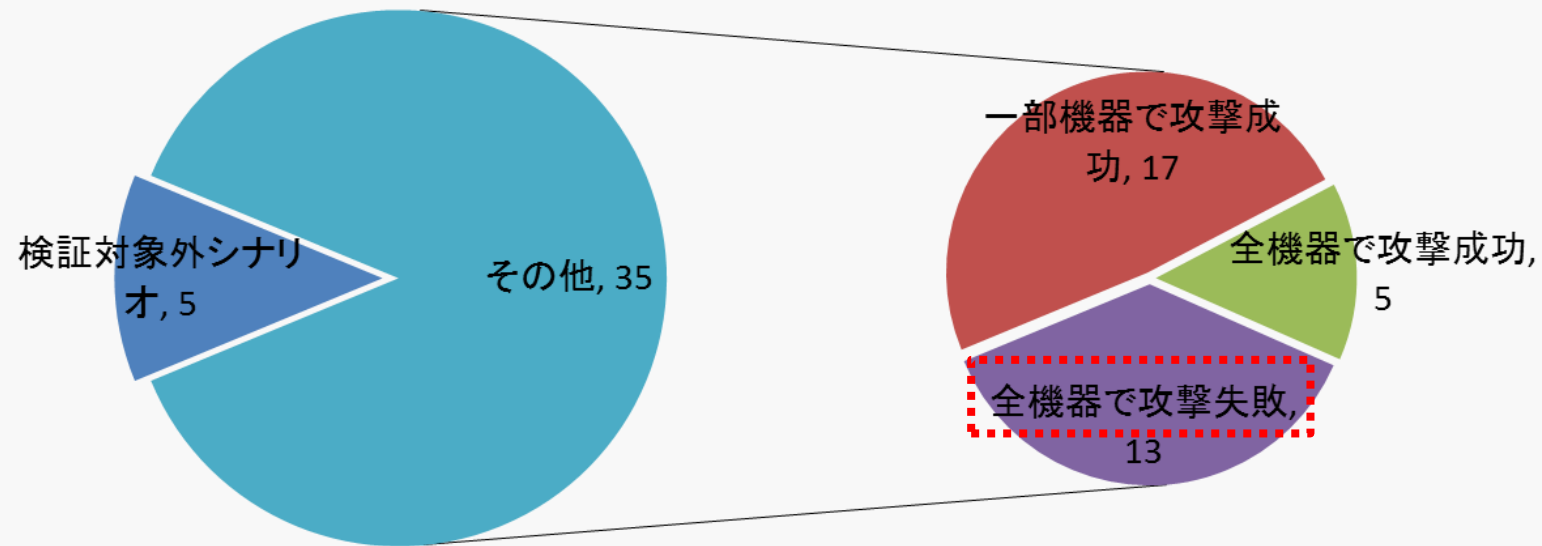
| 提供企業 | 機種名 | 図中番号 |
|-----------|--|------------|
| F5 | BIG-IP 3900 (Load Balance) | D-S1 |
| Palo Alto | PA-4020 (IDS) | D-I1 |
| Palo Alto | PA-4020 (Firewall) | D-F1 |
| Palo Alto | PA-4020 (Firewall) | D-F2 |
| Brocade | ServerIron ADX 1216-4(DHCP Server) | S-S1 |
| Brocade | ServerIron ADX 1216-4(Load Balance) | D-S2 |
| Brocade | NetIron CER 2048CX(Multi-service Router) | B-R1 |
| Microsoft | Windows 2008 Server (DNS/DHCP Server) | S-S3 |
| Microsoft | Windows 7 (Client) | C-C1 |
| Microsoft | L2 Switch | M-B1 |
| Microsoft | IIS (Web Servers) | D-S3, DS-4 |
| 東陽テクニカ | Codenomicon Defensics | C-T1 |
| 東陽テクニカ | Spirent TestCenter, Avalanche3100 | C-T2, C-T3 |
| 東陽テクニカ | Manager (Windows 2008S) | M-S2 |
| 東陽テクニカ | Manager (Windows 2008S) | M-S3 |
| 東陽テクニカ | Manager (Windows 2008S) | M-S4 |
| Blue Coat | SG210 (Proxy Server) | D-C3 |
| Buffalo | WAMP-APG300N (Wireless AP) | W-A1 |
| Buffalo | WU-TX4-AG300N (Media Converter) | |
| Buffalo | WZR-AMPG300NH (Wireless AP) | M-A1 |
| Buffalo | WS-Q2.0TL/R5 (NAS Server) | S-S2 |
| Buffalo | BS-G2016MR (L2 Switch) | C-B1 |
| NICT | FreeBSD (Attacker / Victim) | E-C1 |
| NICT | FreeBSD (Manager/Observer) | M-S1 |
| NICT | FreeBSD (Attacker) | W-C2 |
| NICT | Windows 7 (Victim) | W-C1 |
| NICT | FreeBSD (Attacker) | C-C2 |
| NICT | FreeBSD (Attacker/Victim) | S-C1 |
| NICT | SonicWALL TZ100 (Router) | M-R1 |
| NICT | Catalyst 3560 (Router) | D-R1 |
| NICT | Procurve 6600 (Router) | E-R1 |
| NICT | FreeBSD (Attacker/Victim) | D-C1 |

検証結果のまとめ

検証結果概要

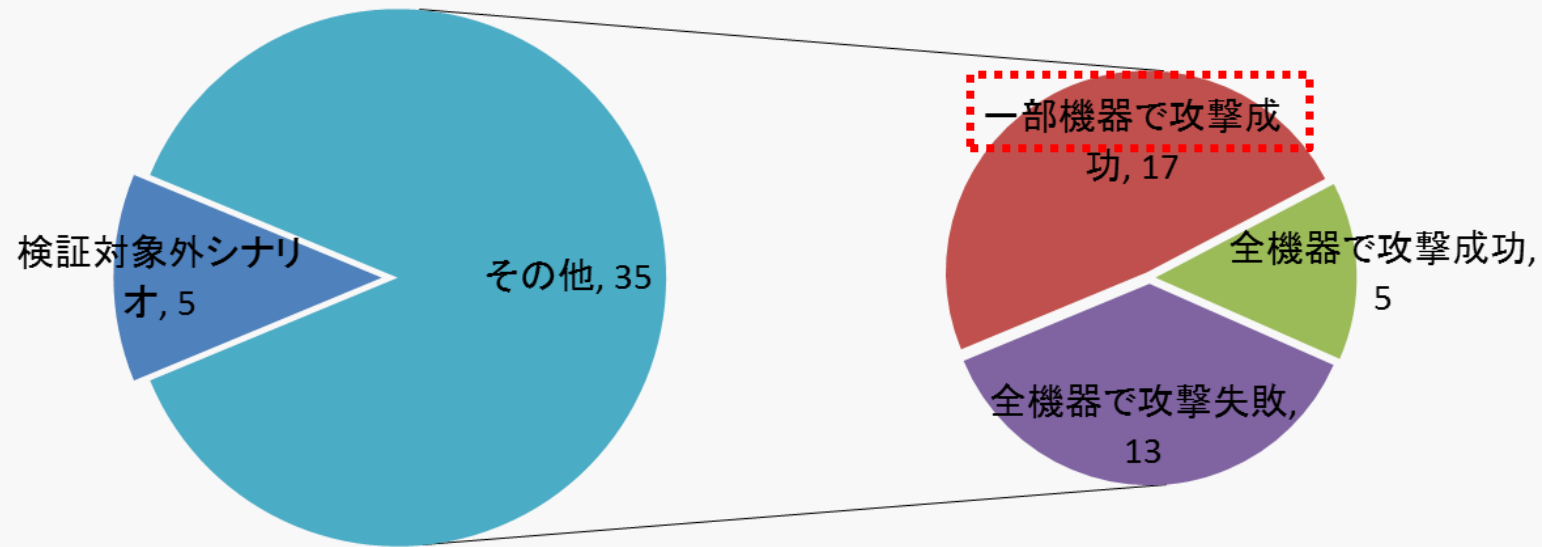


全ての機器で攻撃が不成立となったシナリオ



- シナリオ 30、32、33、34、35、39、40
 - 30 大量のセッションを作成してNAT64 (NAT66) の状態テーブルを枯渇させる
 - 32 大量のセッションを作成してファイアウォールのテーブルを枯渇させる
 - 33 MACアドレスの異なる大量の packets を送信してスイッチのFDBを枯渇させる
 - 34 マルチキャストDNSを使用して虚偽の情報を送信する
 - 35 虚偽のDNSサーバの情報をRAで広告する
 - 39 虚偽のDHCPv6サーバで広告した虚偽のDNSサーバから大量のAAAAレコードを送信してアプリケーショントラフィックを妨害する
 - 40 ファジングにより対象機器のIPv6スタックの脆弱性を検出する
- RFC によってすでに無効とされている、または実装や運用によって回避可能なシナリオであったため

一部の機器で攻撃が成立したシナリオ



- 検証対象シナリオのうち1つ以上のシステムで攻撃が成立し、かつそれ以外のシステムで攻撃が不成立となったもの
- シナリオ 31、36、37、38
 - 31 大量のprefixを広告して端末のプレフィックステーブルを枯渇させる
 - 36 Anycast DNSを使用して虚偽の情報を送信する
 - 37 RAで大量のmore specific routeを広告して端末のルーティングテーブルを枯渇させる
 - 38 ソースアドレスを詐称してlifetimeを0にしたRAを広告し、端末に付与するプレフィックスを無効化する

検証結果一覧

| シナリオ | | | | | | | | | | |
|------|---|------|---|---|---|---|---|---|---|---|
| 1 | X | | | X | X | X | | | X | X |
| 2 | X | | | O | X | X | | | O | O |
| 3 | X | | | X | X | O | | O | X | X |
| 4 | O | | O | O | | | | | | O |
| 5 | | | | | | | | | | X |
| 6 | | X | | | | | | | | X |
| 7 | X | | | X | | | | | | X |
| 8 | X | | | X | X | X | | | X | O |
| 9 | X | | | X | X | X | | | X | O |
| 10 | | | | | O | O | | | | O |
| 11 | | | | | O | O | | | | O |
| 12 | | | O | | | | | | | X |
| 13 | X | | X | X | O | X | | | X | O |
| 14 | | | | | O | O | | | X | O |
| 15 | | O | | | | | | | | O |
| 16 | O | | X | X | X | X | | | | O |
| 17 | O | | O | O | | | | | O | O |
| 18 | | | | | | | | | | O |
| 19 | | | | | O | O | | | | O |
| 20 | | | | | | | | O | | O |
| 21 | | | | | | | | O | | O |
| 22 | | | | | | | | | | O |
| 23 | | | | | | | | | | O |
| 24 | | O | | | | | | | | O |
| 25 | | | | | X | X | X | O | | O |
| 26 | X | | X | X | X | X | | | | O |
| 27 | | | X | | | | | | | X |
| 28 | | | | | | | | | | X |
| 29 | | (+1) | | | | | | | | |
| 30 | X | | | X | | | | | | O |
| 31 | | | | | O | O | O | O | | X |
| 32 | X | X | | X | | | | | | O |
| 33 | | | X | | | | | | | |
| 34 | | | | | X | X | X | X | | |
| 35 | | | | | X | X | X | X | | O |
| 36 | | | | | O | O | O | O | | X |
| 37 | | | | | O | O | O | O | | X |
| 38 | | | | | O | O | X | X | | O |
| 39 | | | | | X | X | X | X | | O |
| 40 | | | | | X | X | X | X | | |

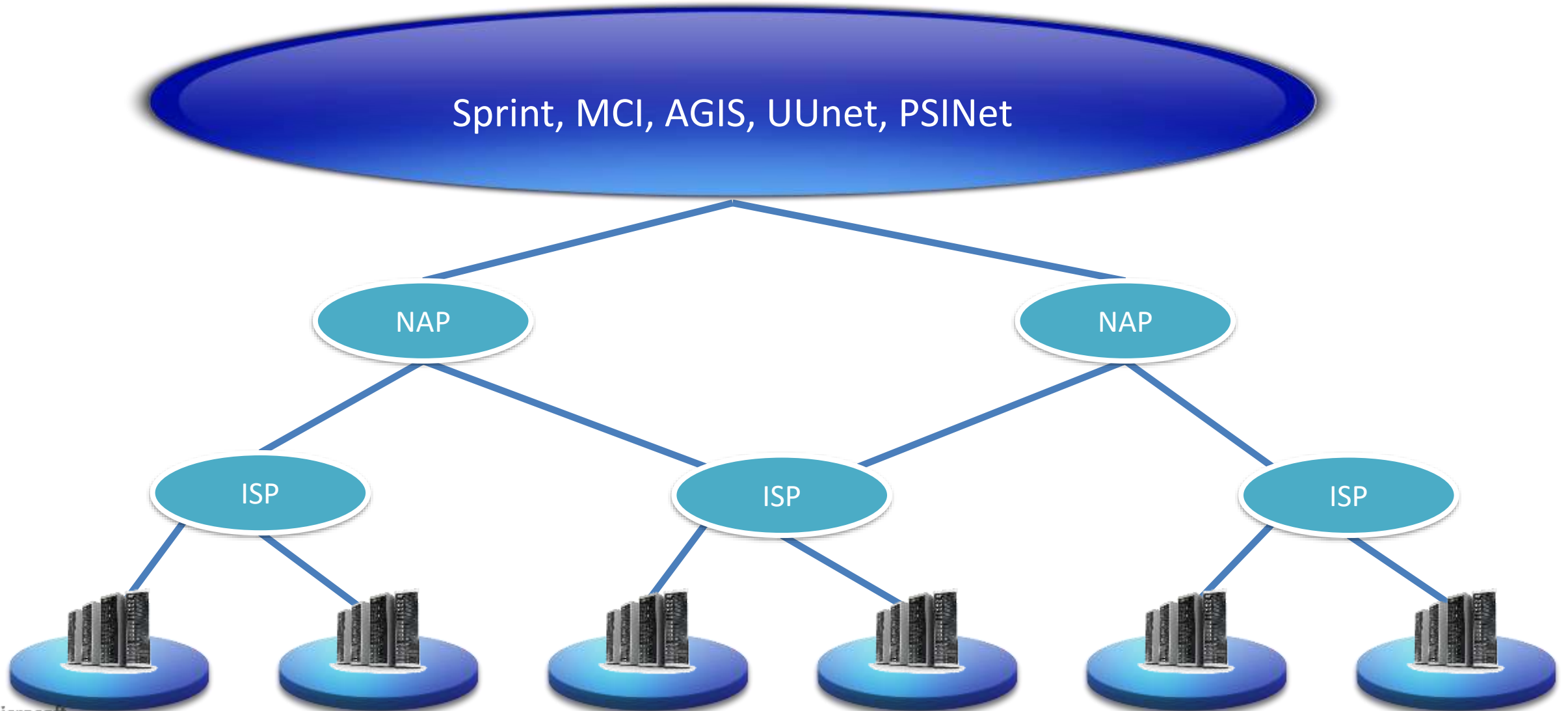
○：攻撃成立
 ×：攻撃不成立

Cloud

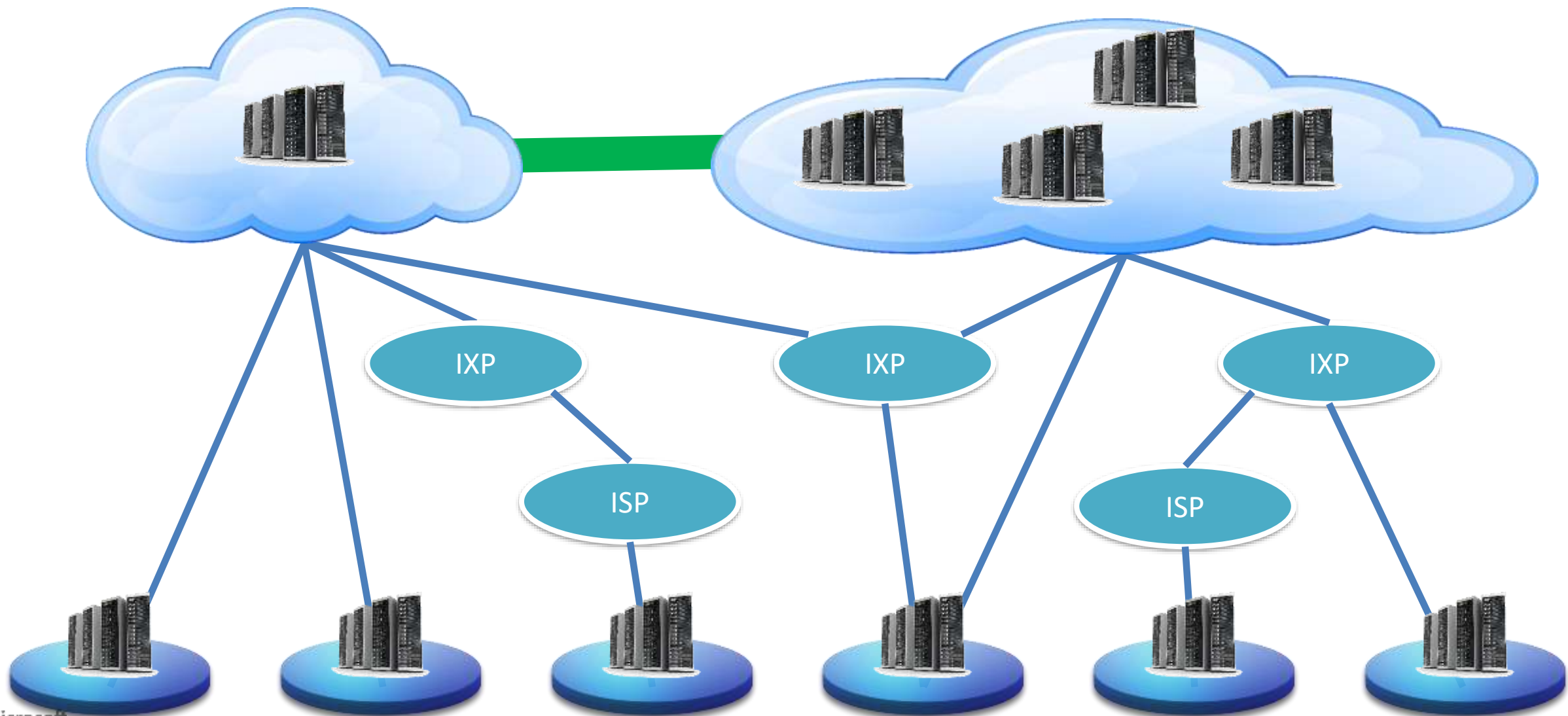




変わるインターネットアーキテクチャ



爆発するデータ、変わる流れ



世界最大のインフラストラクチャー

32 の地域でサービス中、38 の地域まで拡大予定

<https://azure.microsoft.com/en-us/regions/>

Azure is generally available in 32 regions around the world, and has announced plans for 6 additional regions. Geographic expansion is a priority for Azure because it enables our customers to achieve higher performance and it support their requirements and preferences regarding data location.

Explore products per region ▶






- 100カ所以上のデータセンター
- AWS の 2 倍、Google 6 倍の地域サポート
- 米国 国防総省 (US DoD) も採用

- 稼働中
- アナウンス済み / 構築中

マイクロソフトのネットワークは、世界第2位の規模 (上にいるのは、米国政府のネットワークのみ)

1.4

million miles of
fiber in our DCs

-  Datacenter
-  CDN Locations
-  Edge Node
-  Internet Exchange
-  Terrestrial Network
-  Subsea Network



マイクロソフトの製品とサービス



Windows Live



skype



XBOX 360 Gets TV



Microsoft SQL Server 2012



KINECT for XBOX 360 Star Wars Launch



NOKIA Lumia 900



Microsoft System Center 2012



Microsoft SkyDrive



BARNES & NOBLE Microsoft



Microsoft Dynamics CRM



bing facebook



KINECT for Windows



Windows Azure IaaS/Apps



Windows Intune



Windows Server



Microsoft Office 365 For Education



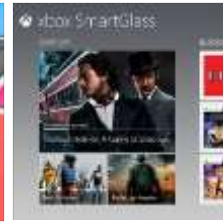
Windows



Windows Explorer



Surface



XBOX SmartGlass



Microsoft Dynamics NAV



Microsoft Dynamics GP



Microsoft Dynamics AX



Windows Phone



Visual Studio



Microsoft .NET Framework



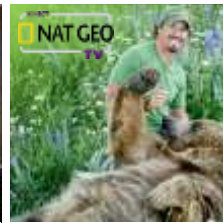
KINECT for XBOX 360 Nike + Kinect Training



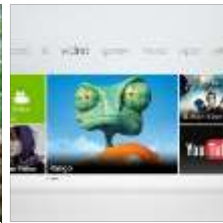
HALO 4



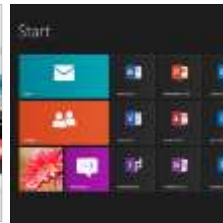
KINECT Playful Learning Sesame Street TV



KINECT Playful Learning Nat Geo TV



XBOX LIVE Marketplace



Office



Yammer

The Azure Platform

Platform Services

Security & Management

- Portal
- Azure Active Directory
- Azure AD B2C
- Multi-Factor Authentication
- Automation
- Scheduler
- Key Vault
- Store/Marketplace
- VM Image Gallery & VM Depot

Services Compute

- Cloud Services
- Service Fabric
- Batch
- RemoteApp

Web and Mobile

- Web Apps
- API Apps
- Mobile Apps
- Logic Apps
- API Management
- Notification Hubs

Data

- SQL Database
- Data Warehouse
- DocumentDB
- Redis Cache
- Azure Search
- Storage Tables

Hybrid Operations

- Azure AD Health Monitoring
- AD Privileged Identity Management
- Domain Services
- Backup
- Operational Analytics
- Import/Export
- Azure Site Recovery
- StorSimple

Integration

- Storage Queues
- BizTalk Services
- Hybrid Connections
- Service Bus

Developer Services

- Visual Studio
- Azure SDK
- VS Online
- App Insights

Analytics & IoT

- HDInsight
- Machine Learning
- Stream Analytics
- Data Lake
- Data Factory
- Event Hubs
- Data Catalog
- IoT Hub
- Mobile Engagement

Media & CDN

- Media Services
- Content Delivery Network (CDN)

Infrastructure Services

OS/Server Compute

- Virtual Machines
- Container Service

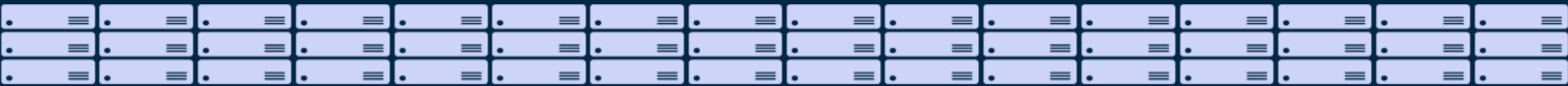
Storage

- BLOB Storage
- Azure Files
- Premium Storage

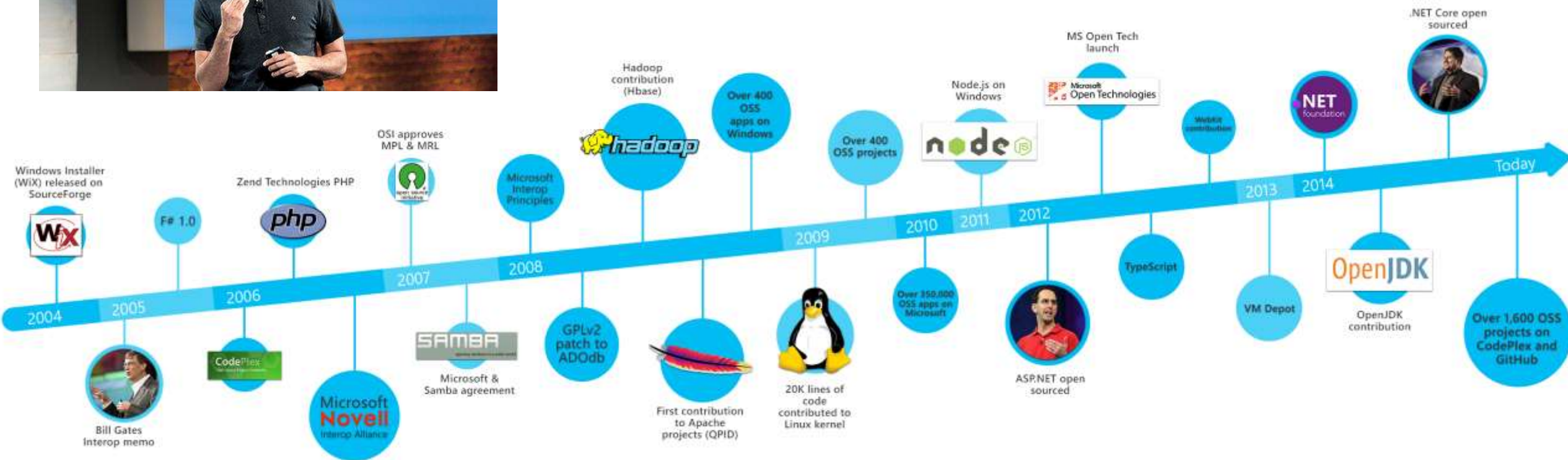
Networking

- Virtual Network
- Load Balancer
- DNS
- Express Route
- Traffic Manager
- VPN Gateway
- App Gateway

Datacenter Infrastructure (34 Regions, 26 Generally Available)



10年を超えるオープンソースへの取り組み



Microsoft Azure はオープンプラットフォーム



■ 幅広いLinux ディストリビューションを動作保証

- Red Hat Enterprise / CentOS / SUSE / Ubuntu など各Linuxディストリビューションをサポート
- Oracle、MySQL、Redis、MongoDB を実行可能
- 動作保証済みLinuxディストリビューション

<https://azure.microsoft.com/ja-jp/documentation/articles/virtual-machines-linux-endorsed-distros/>



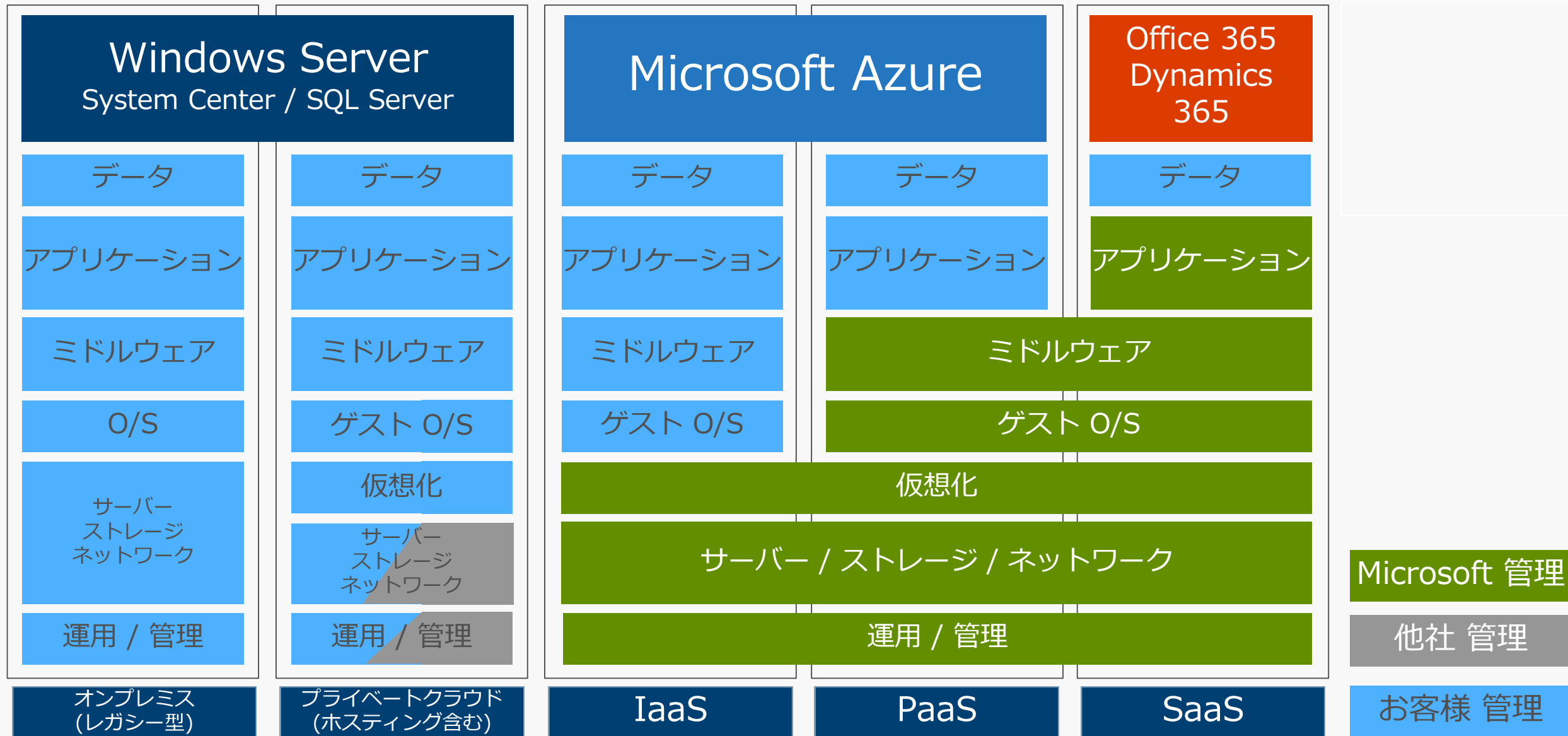
Microsoft Azure = オープンクラウド

オープンかつ柔軟なクラウドで幅広い選択肢をご提供してきました



マイクロソフトのクラウドソリューションマップ

←— パブリック クラウド —→



Cognitive Services : 人工知能サービス API 群

画像認識、音声認識、テキスト認識など、ディープラーニング手法による大きなコンピューティングパワーを必要とする処理などを Azure の API Service として提供。

参照 : <https://www.microsoft.com/cognitive-services/>



Computer Vision API

- 画像から有益な情報を自動抽出



Face API

- 写真から人の顔を自動的に検知・特定、分析・整理



Emotion API

- 人の感情を自動認識



Video API

- 動画の分析と編集



Bing Speech API

- 音声とテキストの相互変換と意図の自動認識



Speaker Recognition API

- 話をしている人物の自動特定



Custom Recognition API

- モデルのカスタマイズにより、音声認識の障害 (話し方/ノイズ/語彙) を排除



Bing Spell Check API

- スペルミスの検知と訂正



Language Understanding Intelligent Service

- 自然言語をアプリが理解可能なコマンドに変換



Linguistic Analysis API

- テキストに対する言語分析



Text Analytics API

- 感情/キーワード/話題/言語の自動認識



Web Language Model API

- Web 学習モデルによるワード分割や言語出現等を求める



Academic Knowledge API

- 論文/学術誌/著者等の学術データに基づいたオートコンプリートやヒストグラム計算



Entity Linking Intelligent Service

- 複数単語から成る固有名詞の自動認識



Bing Auto Suggest API

- Bing オートコンプリート



Bing Image Search API

- Bing 画像検索



Bing News Search API

- Bing ニュース検索



Bing Video Search API

- Bing 動画検索



Bing Web Search API

- Bing Web 検索



Knowledge Exploration Service

- 構造化データに基づいたオートコンプリートやヒストグラム計算



Recommendation API

- レコメンデーション

Cognitive Services : Emotion API

画像や動画を分析し、人の感情を自動的に認識。怒り・軽蔑・嫌悪・怖れ・幸福・中立・悲しみ・驚きの8つの要素を確率で回答

Microsoft Project Oxford

Cognitive Services - Emotion API

Subscription Key Management

Select a scenario:

- Detect emotion using a stream
- Detect emotion using a URL
- Detect emotion in a Video

Detect emotion by an bitmap stream

Please click [Load Image] to specify the images to detect.

The top 3 emotions will be shown in the list box. For more details on other emotions, please see the status.

Detection Done

| | | | |
|--|--|--|--|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

```

[13:47:43.824764]: FaceRectangle = left: 368, top: 77, width: 112, height: 112
[13:47:43.824764]: Anger : 0.2360841
[13:47:43.840372]: Contempt : 0.0408594
[13:47:43.856068]: Disgust : 0.708052
[13:47:43.871619]: Fear : 1.17069E-06
[13:47:43.887244]: Happiness: 0.0001521924
[13:47:43.902943]: Neutral : 0.00929694
[13:47:43.909504]: Sadness : 0.00554609
[13:47:43.909504]: Surprise : 8.098536E-06
    
```

Microsoft will receive the images you upload and may use them to improve Face API and related services. By submitting an image, you confirm you have consent from everyone in it.

感情を自動認識

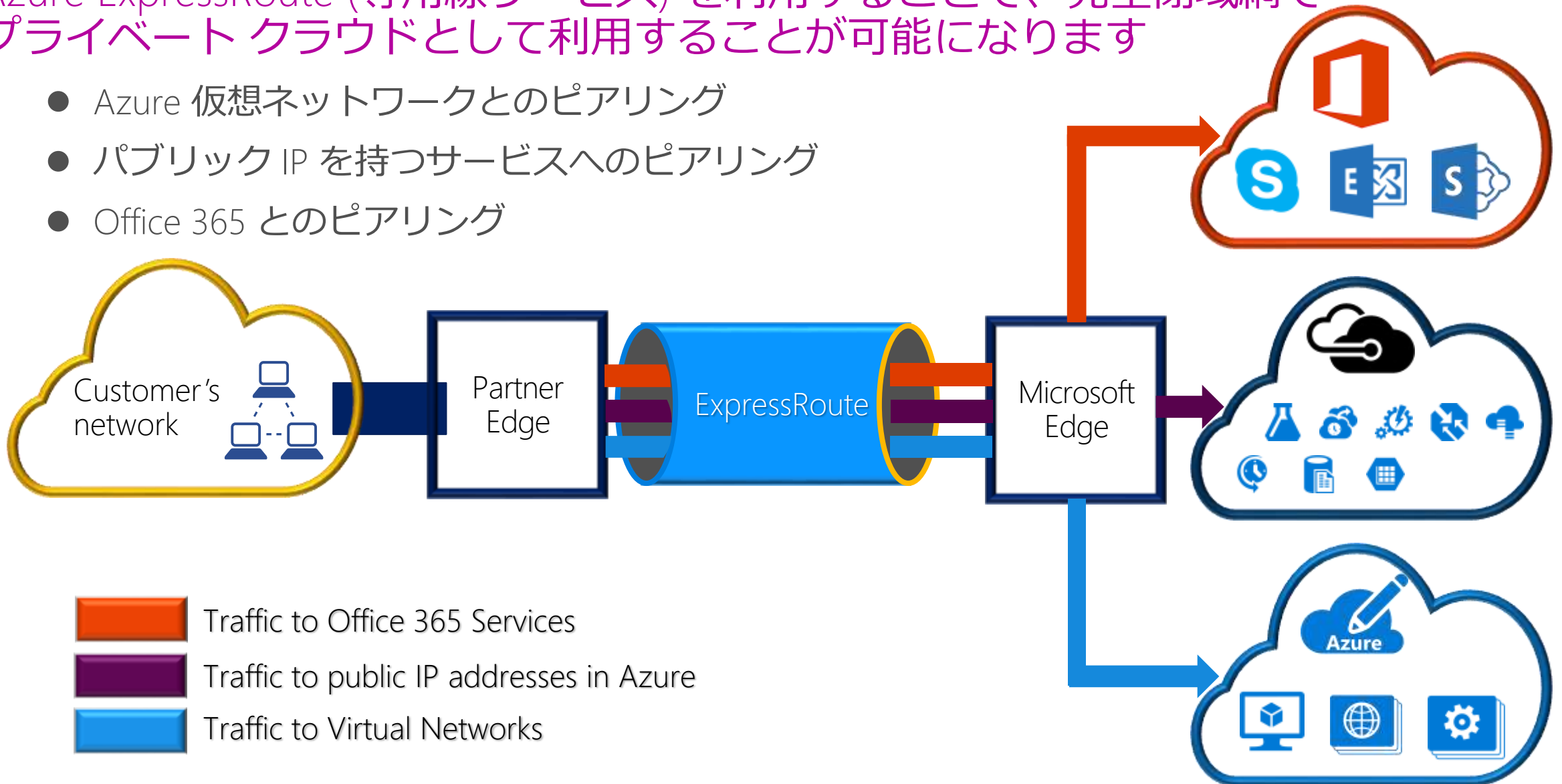
Pricing options

| Plan | Description | Price |
|----------|--|---|
| Free | 30,000 image transactions per month 300 video uploads (limit 1 per min), 3,000 query status (limit 5 per min) | Free |
| Basic | 10 image transactions per second (face must be pre-specified) 300 video uploads (limit 1 per min), 3,000 query status (limit 5 per min) | \$0.10 per 1000 transactions Free for video |
| Standard | 10 image transactions per second 3000 video uploads (limit 2 per min), 30,000 query status (limit 10 per min) | \$0.25 per 1000 transactions Free for video |

専用線によるプライベートクラウド化

Azure ExpressRoute (専用線サービス) を利用することで、完全閉域網でプライベートクラウドとして利用することが可能になります

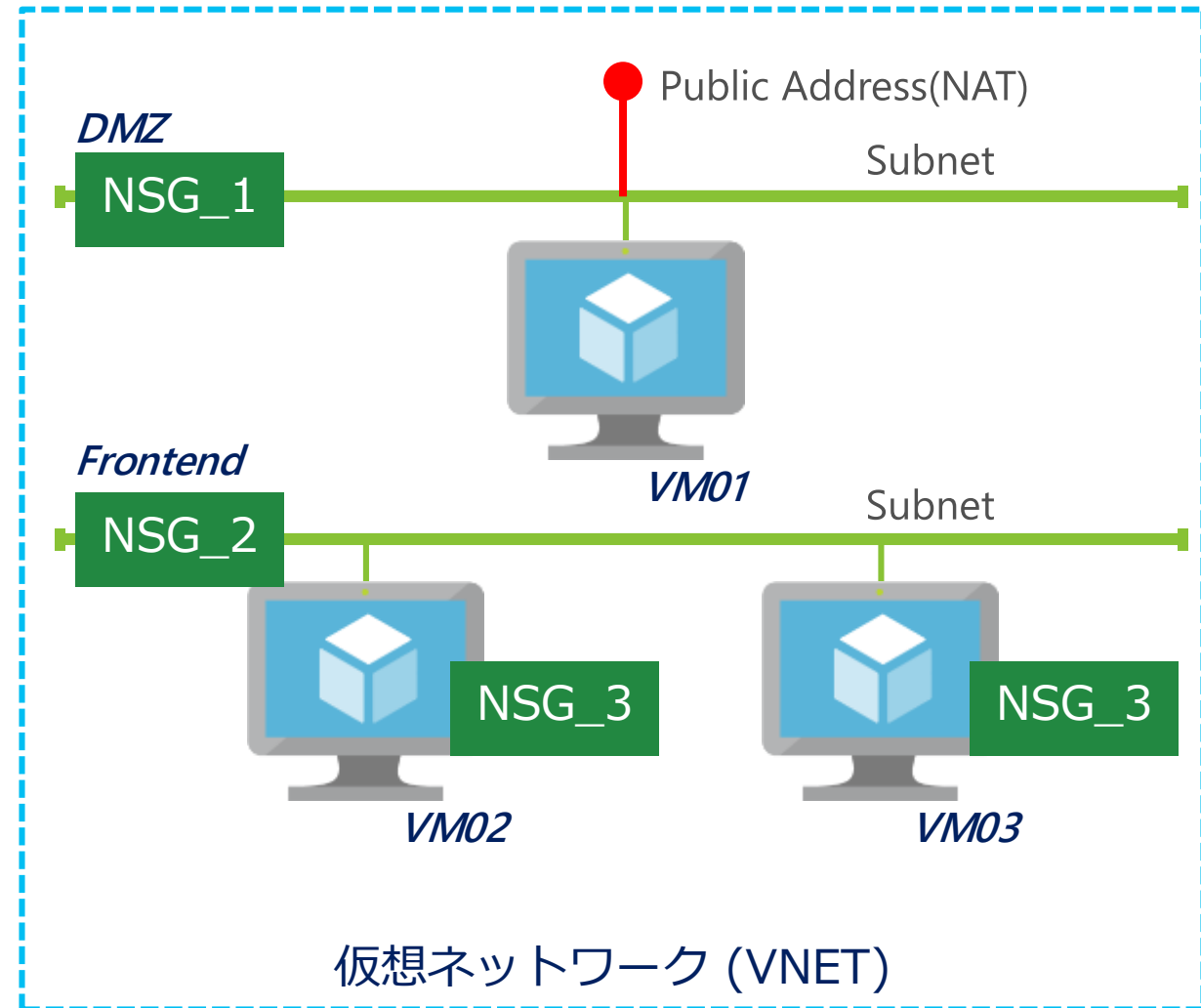
- Azure 仮想ネットワークとのピアリング
- パブリック IP を持つサービスへのピアリング
- Office 365 とのピアリング



ネットワークセキュリティグループ (NSG)

仮想ネットワーク上のトラフィックを制御することでより、セキュアなクラウド環境を提供

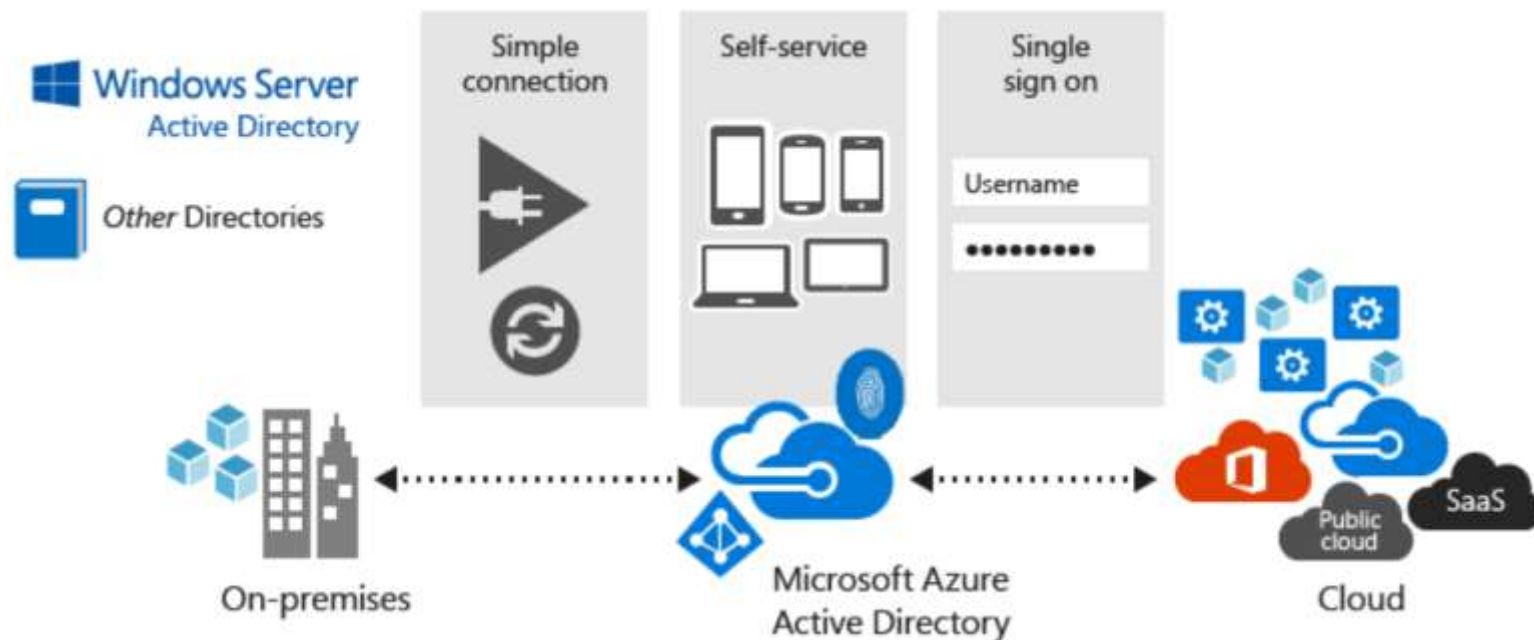
- 送信元 or 宛先 IP アドレス、ポートの制御（範囲も可）
- プロトコルを指定して送受信両方向の通信を許可禁止するルールを作成
- NSG は仮想マシン単位、あるいはサブネット全体に対して設定可能
- エンドポイント ACL では不可能だった送信方向のトラフィックに対する制御も可能に
 - Azure VM のインターネットアクセスを禁止することも可能
 - Azure 上で DMZ 的な構成がとれる



Azure Active Directory による ID 管理

Azure Active Directory (Azure AD) は、マルチテナントに対応したクラウドベースのディレクトリと ID の管理サービスによって、優れた使い勝手とコンプライアンスを実現します

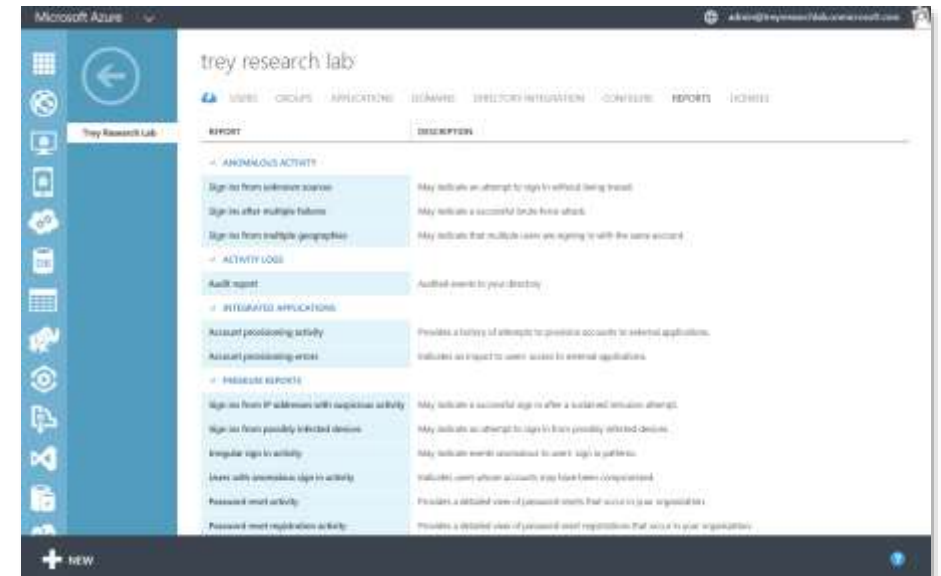
- Office365、Salesforce.com、DropBox、Concur など、さまざまなクラウド型 SaaS アプリケーションへのシングルサインオン (SSO) の実現
- Multi-Factor Authentication、デバイスの登録、セルフサービスのパスワード管理、セルフサービスのグループ管理、特権を持つアカウントの管理、ロールベースのアクセス制御、アプリケーション使用状況の監視、機能豊富な監査とセキュリティの監視、アラートなど、一連の ID 管理機能の提供
- Azure AD を既存の Windows Server Active Directory と統合が可能



Azure AD Report

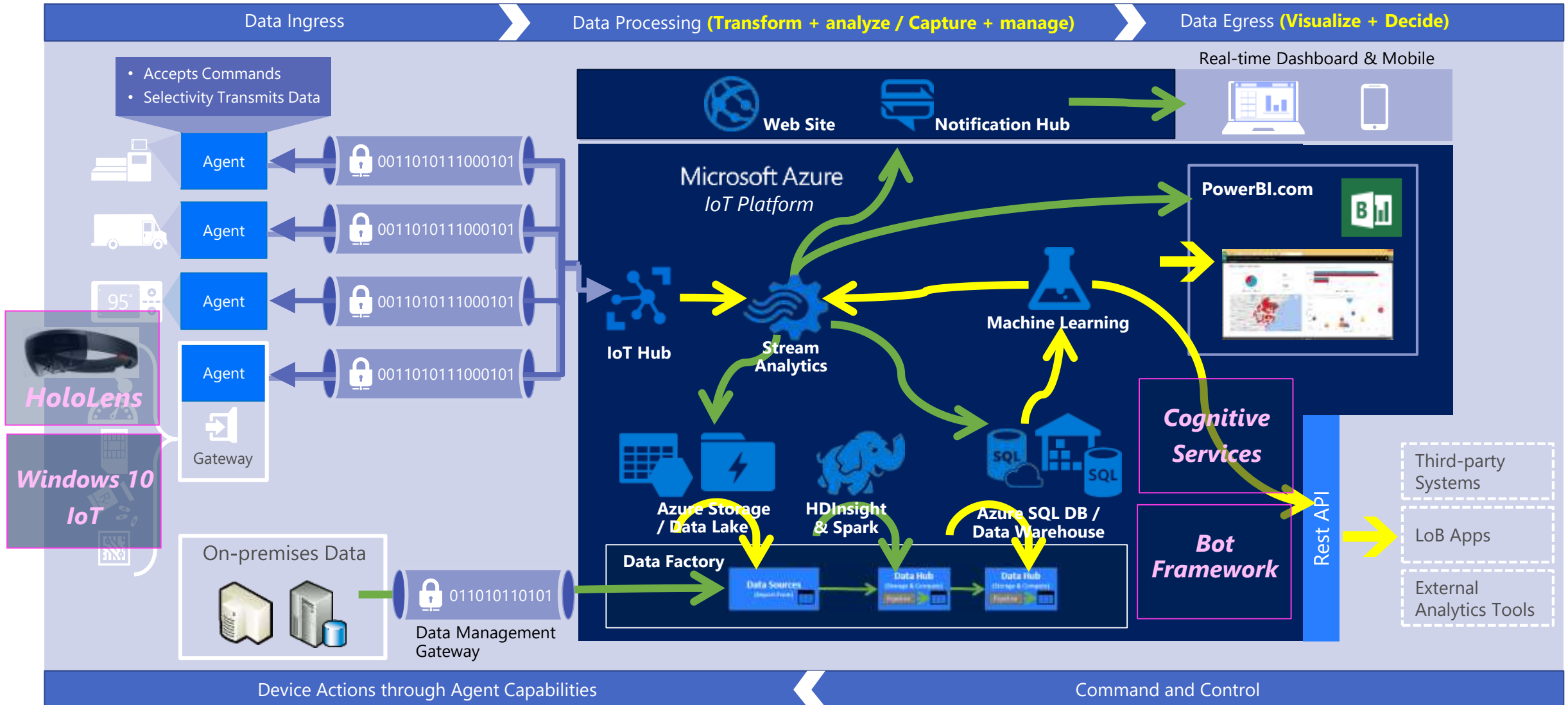
Azure AD Report により、以下のレポートを行うことが可能です

- ライセンス
 - ✓ 許可されていない使用
- 異常なアクティビティ
 - ✓ 不明なソースからのサインイン
 - ✓ 複数のエラー発生後のサインイン
 - ✓ 複数の地域からのサインイン
 - ✓ 資格情報が脅かされているユーザー
 - ✓ 資格情報が漏洩されたユーザー
- アクティビティログ
 - ✓ 監査レポート
- 統合アプリケーション
 - ✓ アカウントプロビジョニングのアクティビティ
 - ✓ アカウントプロビジョニングエラー
- 外部アクセス
 - ✓ 招待の概要
- PREMIUMレポート
 - ✓ 疑わしいアクティビティを示すIPアドレスからのサインイン
 - ✓ 感染の疑いのあるデバイスからのサインイン
 - ✓ 不規則なサインインアクティビティ
 - ✓ 異常なサインインアクティビティのユーザー
 - ✓ パスワードリセット アクティビティ
 - ✓ パスワードリセット登録アクティビティ レポート
 - ✓ セルフサービスグループアクティビティ
 - ✓ Office365グループ名の変更
 - ✓ アプリケーションの使用状況



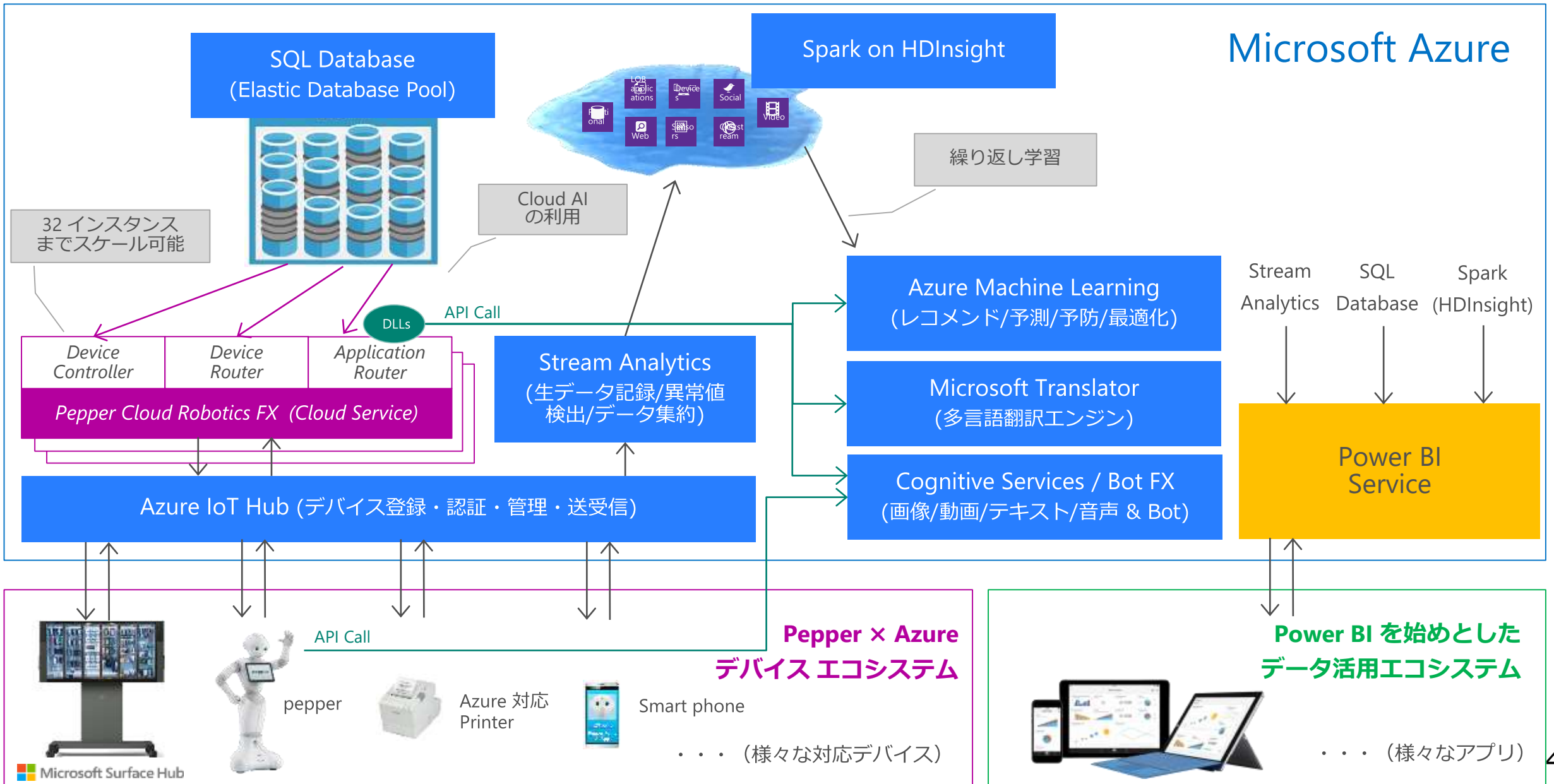
Azure IoT Platform >> Cloud AI Platform

→ : データ消費
 → : データ生成



Cloud Robotics Azure Platform

■ : Azure PaaS
 ■ : Robotics SDK



Power BI のアーキテクチャ

オンプレミス環境

分析用
インメモリDB

SQL Server AS

PowerPivot
Microsoft Excel

PowerPivot

Power BI Desktop

Microsoft Azure

On-premises
Data Gateway

PowerBI
Service

Upload (Report Design)

Upload (PowerPivot)

PowerPivot
ダイレクトクエリ

データは Power BI Service の PowerPivot に
キャッシュ、もしくは、ダイレクトにクエリ

DocumentDB

Stream Analytics

SQL DB / DW

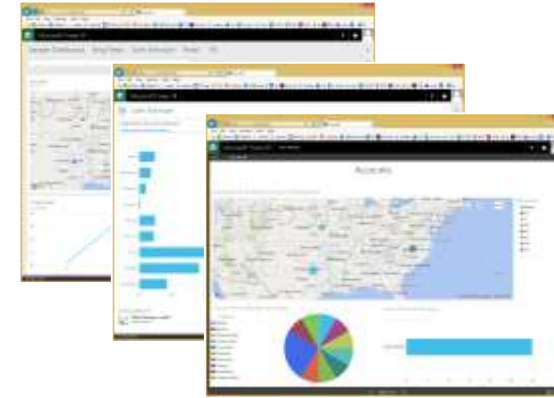
Spark
on HDInsight

非 Azure 上のソフトウェアシステム
(例. SaaS 型アプリケーション,
IoT シナリオ, データストリーム)

Azure 上のソフトウェアシステム
(例. 顧客のアプリケーション,
1st パーティ サービス)

ブラウザ

- リアルタイム ダッシュボード
- 自然言語クエリ
- Advanced Analytics & Machine Learning フロントエンド
- ビジュアル探索



モバイルアプリ

- iOS, Android, Windows
- リアルタイム ダッシュボード
- 閾値アラート
- ビジュアル探索



Cortana for business (Windows 10)

- Cortana - Power BI 連携

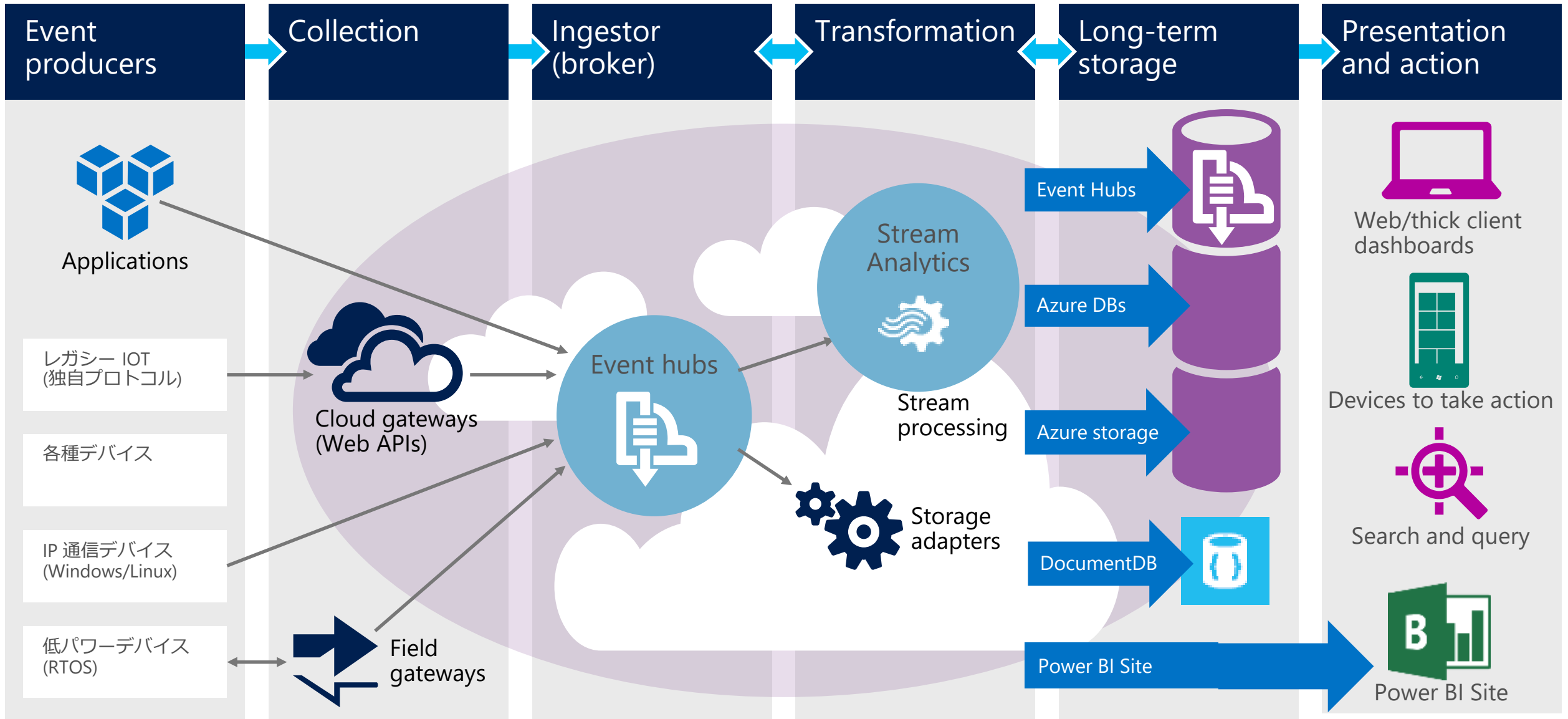


Embedded </> insights

- Power BI の埋め込み



End-to-End のアーキテクチャ



Azure の機能を拡張する サードパーティ オフアリングの幅広いエコシステム

Microsoft Azure



Azureマーケットプレイス*



* 製品/サービスの一覧は網羅的なリストではありません。

IPv6 サポートレベル

- 多岐に渡る通信を行うコンポーネント、サービス
- 向上し続けるIPv6サービスレベル
- 継続的にリリースされる新機能、新サービス

| Service name | Full IPv6 support | Limited IPv6 Support | Full IPv4 support | Additional information |
|-----------------------|-------------------|----------------------|-------------------|--|
| Azure | | | ● | Does Azure support IPv6? |
| Bing | | | ● | World IPv6 Launch |
| Dynamics CRM Online | | | ● | |
| Microsoft.com | ● | | ● | |
| Office 365 2013 | ● | | ● | IPv6 support in Office 365 services Office 365 IPv6 Test Plan for Chiayi Educational Network Center |
| Office 365 2010 | | | ● | |
| OneDrive | | | ● | |
| Outlook.com | | | ● | |
| Skype | | ● Mobile Only | | |
| SQL Azure | | | ● | |
| System Center Advisor | | | ● | |
| Microsoft Intune | | | ● | |
| Windows Update | ● | | ● | Connecting with IPv6 in Windows 8 |



Microsoft