

Microsoft Security Forum 2020

B-3

Azure セキュリティのキーポイント - ソリューションとベストプラクティス

日本マイクロソフト株式会社
サイバーセキュリティソリューショングループ
大井 喜智

Microsoft



DIGITAL
TRUST
SECURITY



#digitaltrust

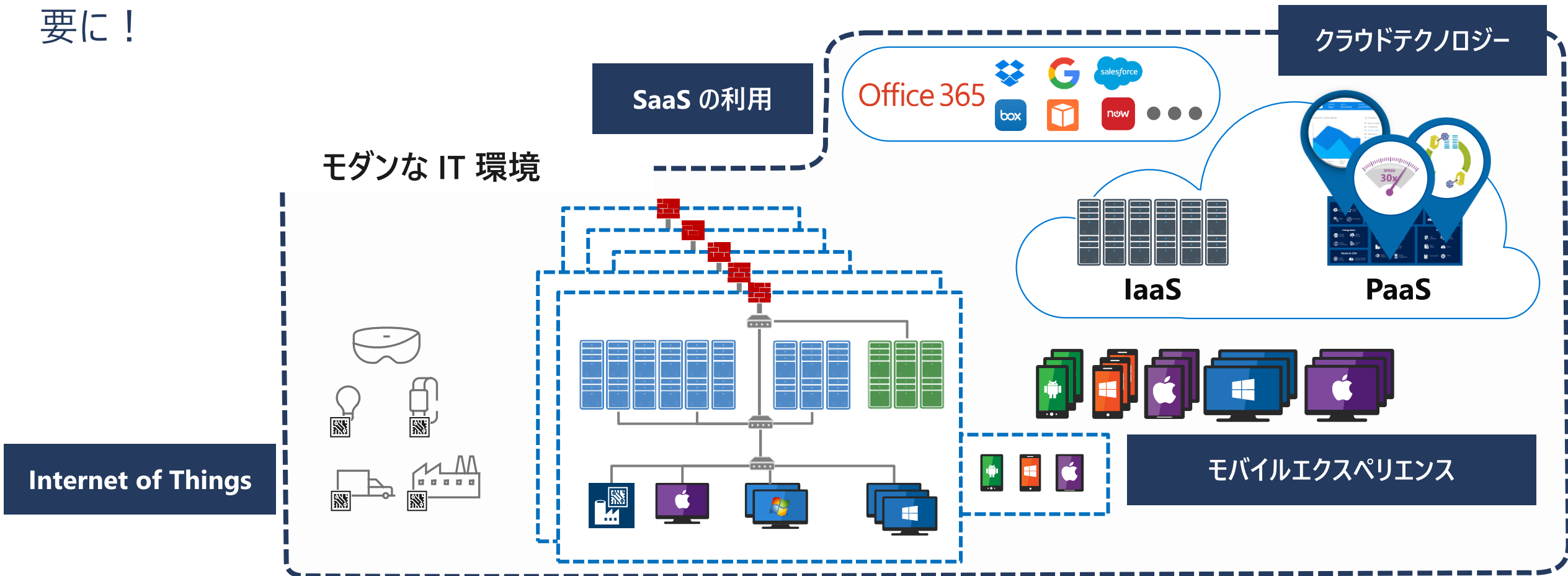


Microsoft

ハイブリッド・マルチクラウド化とセキュリティ

SaaS や モバイルデバイスの利用といった領域に加え、IoT や IaaS・PaaS など新たなテクノロジー領域が利用が進んでいる

Microsoft 365 でカバーする SaaS やモバイル領域に加え、IoT や IaaS・PaaSのセキュリティも重要に！



Microsoft Azure とセキュリティ

Microsoft は Azure によって、IaaS や PaaS, IoT のサービスを提供
加えて、ハイブリッド・マルチクラウドにも対応した**セキュリティソリューション**を提供

IaaS



サーバー

ネットワーク

PaaS



アプリ・API

ストレージ・DB

コンテナー

IoT



ハブ

エッジ



Azure
Active Directory



Azure
Security Center



Azure
Sentinel



Azure
Monitor



Azure
Governance

セキュリティソリューション

Azure のセキュリティで何を考慮すべきか？

本セッションでは、Azure の“クセ”を理解したうえで、組み込まれたソリューションをどう利用すれば Azure / ハイブリッド・マルチクラウド環境のセキュリティを向上できるかをご紹介します

1. GRC ガバナンス・リスク・コンプライアンス
2. クラウドのネットワークセキュリティ
3. リソースにおける脅威からの保護と検知
4. ログの管理とセキュリティ運用

Microsoft Security Forum 2020



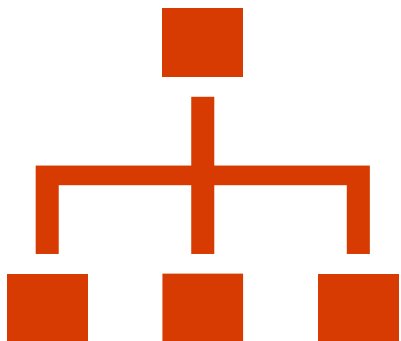
1. GRC ガバナンス・リスク・コンプライアンス

GRC のベース – セグメンテーションと CSPM

パブリッククラウドにおいて、GRC のベースになるのは、リソース管理のセグメンテーションの確立と **CSPM** (Cloud Security Posture Management, クラウドセキュリティ態勢管理)

セグメンテーション

- ロジカルな階層構造をつくる
- それぞれのレイヤーの機能の整理
- 責任やアクセス権を明示的に分離し、横歩きを防ぐ



CSPM

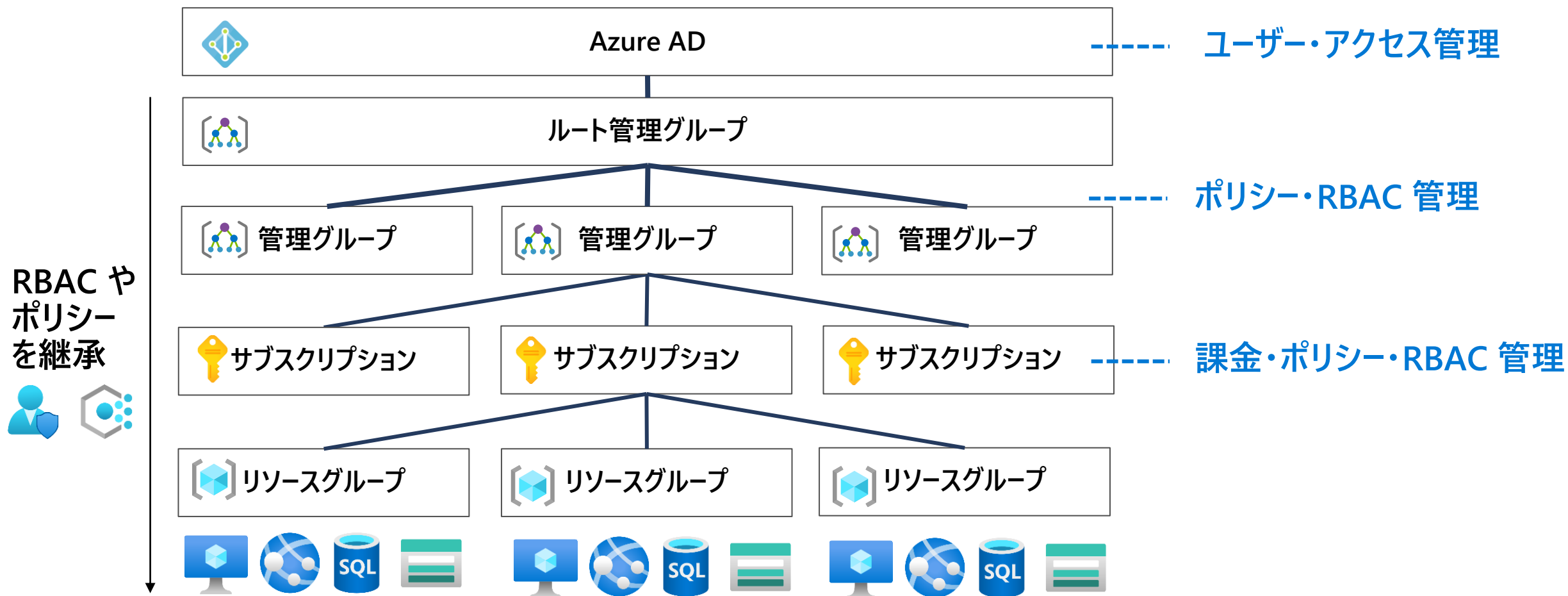
(Cloud Security Posture Management, クラウドセキュリティ態勢管理)

- 構成ミスを防ぐ
- マイクロソフトや CIS ベースのベストプラクティスを把握
- 自社ポリシーの適用状況を確認



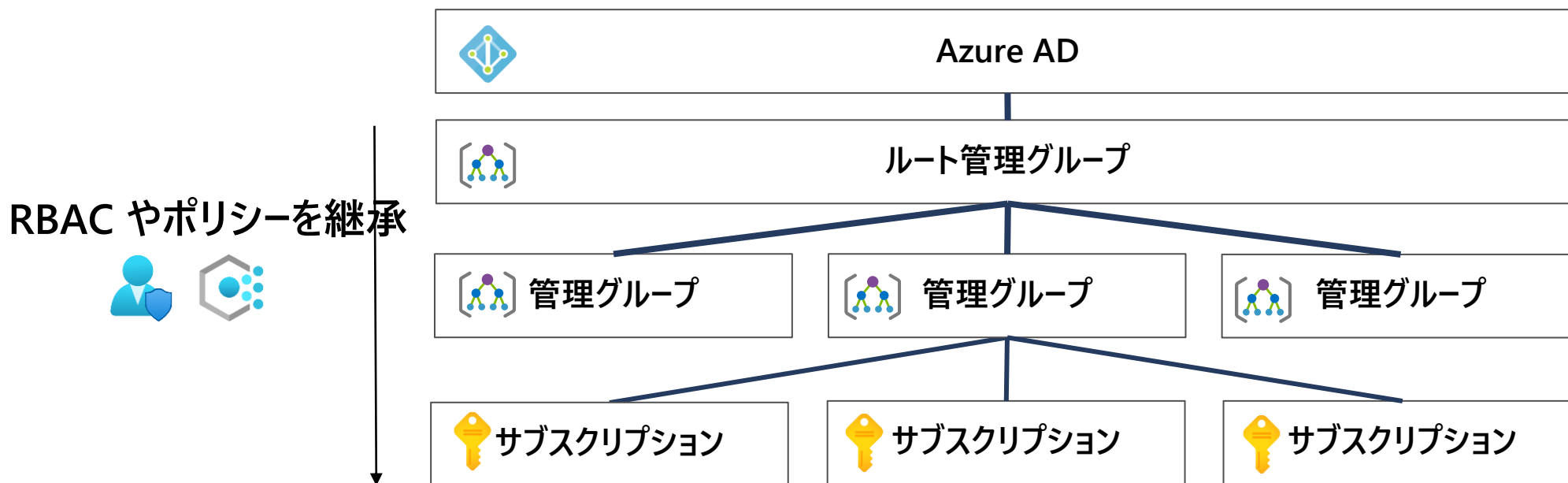
Azure のセグメンテーション

Azure において、**Azure AD** は絶対的な境界で、ユーザー・アクセスの管理を担う
その配下に、**管理グループ・サブスクリプション**という Azure 自体の管理セグメントを持つ



Azure のセグメンテーションの推奨事項

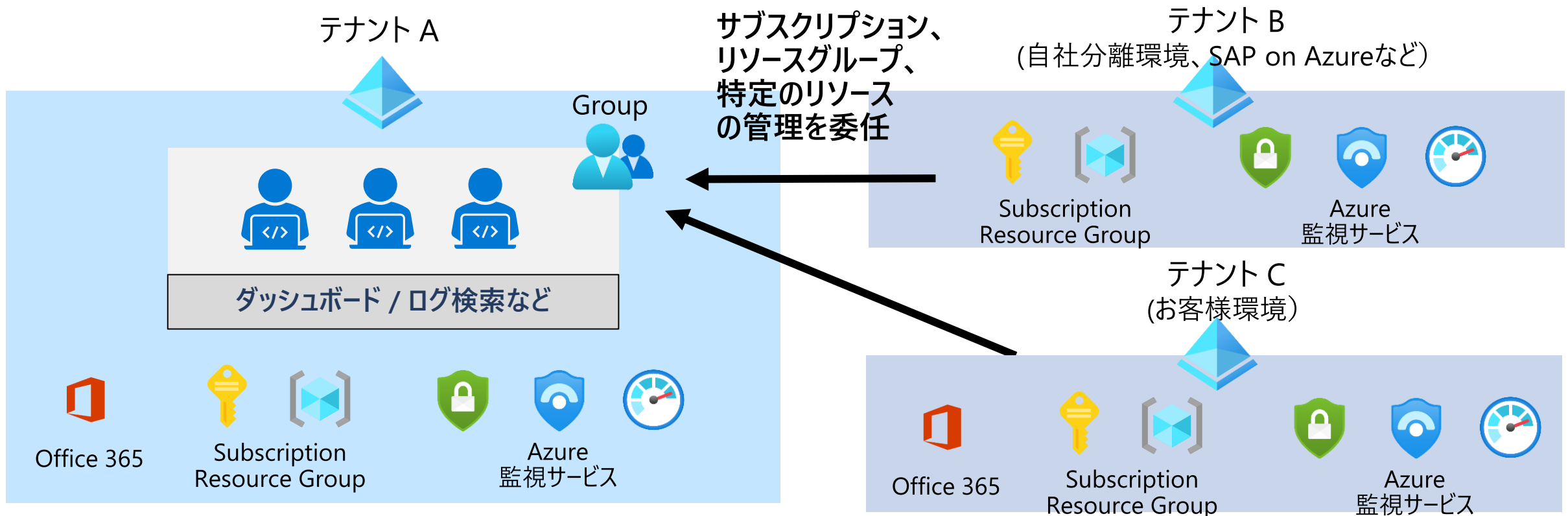
- Azure AD に関しては、なるべくシングルテナントで ID を統合管理する
- **管理グループ**を使い、サブスクリプションが分かれる環境でも、統合的なポリシーは管理グループに適用する
 - ただし、管理グループは深い層構造を持たせず、**3層以内**に収める
- サブスクリプションは課金とRBACの大きな区切り目となるので、システムごとや 開発環境用・本番環境用など、**ロジカルな理由付け**を持って分ける



マルチテナント管理 – Azure Lighthouse

一企業内に複数テナントがある場合や、セキュリティ運用を他社に委任する場合など、絶対的な境界である **Azure AD** をまたぐ必要が出てくる

→ **Azure Lighthouse** がテナントをまたいだリソースの集中管理を提供

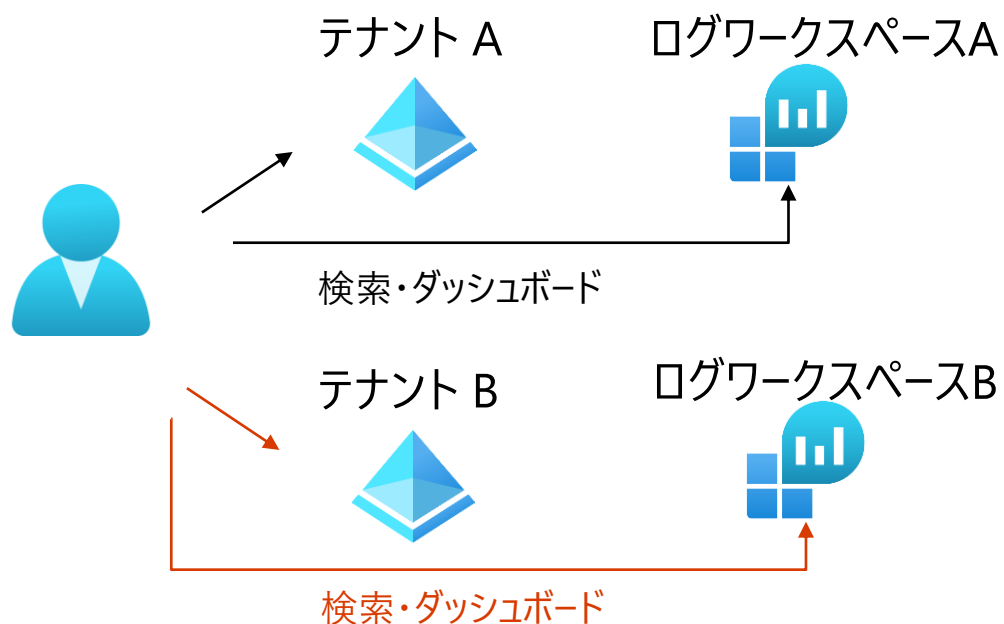


Azure AD B2B vs Azure Lighthouse

マルチテナント管理において、Azure Lighthouse は Azure AD B2B では提供できない統合管理を提供

Azure AD B2B

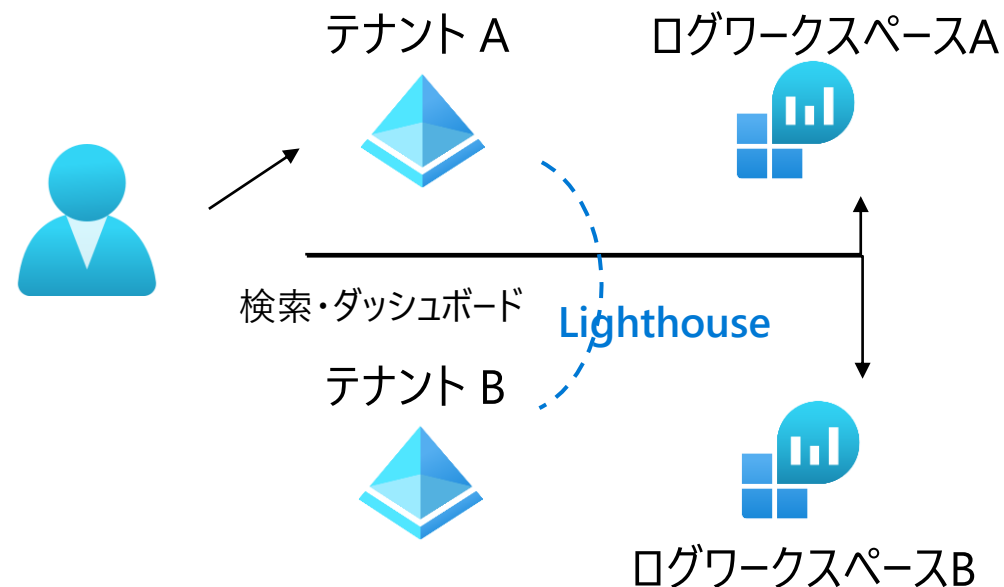
各テナントへのサインインが必要で、複数テナントをまたぐ検索やダッシュボード化ができない



Azure Lighthouse

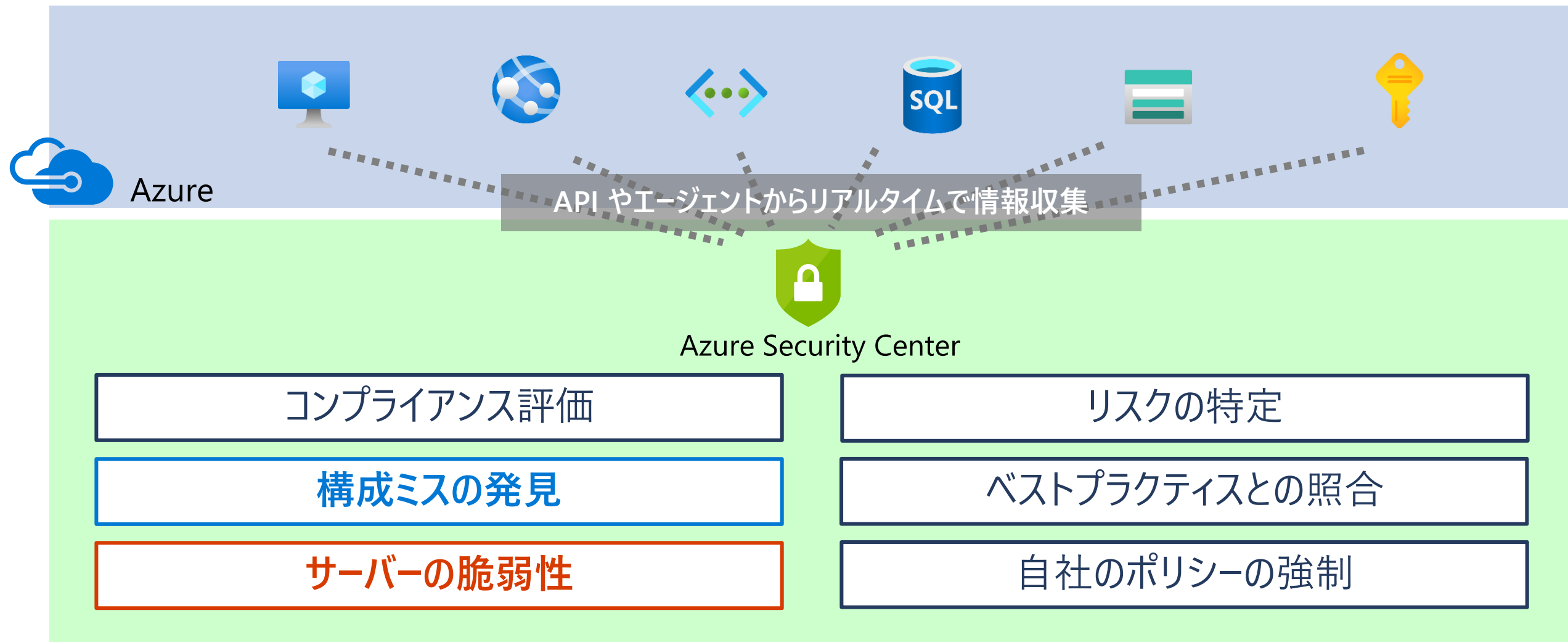
ひとつのテナントへのサインインのみで、複数テナントのリソースの管理ができる

複数テナントをまたぐ検索やダッシュボード化も可能



CSPM - セキュリティ正常性の可視化

Azure では Azure Security Center が 1st Party CSPM として GRC の評価を提供



セキュリティ正常性の可視化

特に Azure Security Center では、Azure 上での構成ミスと、サーバーの脆弱性を可視化
サーバーの脆弱性に関しては、Azure Security Center Standard で Qualys のエージェントによる脆弱性評価と Microsoft Defender ATP による脆弱性評価を提供

Azure 上での構成ミス

- Azure 仮想マシンの構成
- NSG, Storage Firewall などのネットワーク設定
- Subscription 管理者の設定

サーバー上の脆弱性

- **Qualys のエージェント**を利用した、Windows Server と Linux Server の脆弱性評価（Azure VMのみ対応）
- **Microsoft Defender ATP の TVM** を利用した Windows Server の脆弱性評価
- パッチの適用状況や Windows OS の設定の確認

Microsoft Security Forum 2020



Demo: Azure Security Center

CSPM (Cloud Security Posture Management)

セグメンテーション × CSPM – Azure GRC への道！

GRC の担当者がすべてのリソースの GRC をチェックできるように構成することが重要！

NG

サブスクリプションがばらばらでセキュリティ管理者が確認できない

Group A



Subscription A



Group B



Subscription B



Group C



Subscription C



Good

セキュリティ管理者が、一元的に監視・管理

Security Team



Subscription A



Subscription B



Subscription C



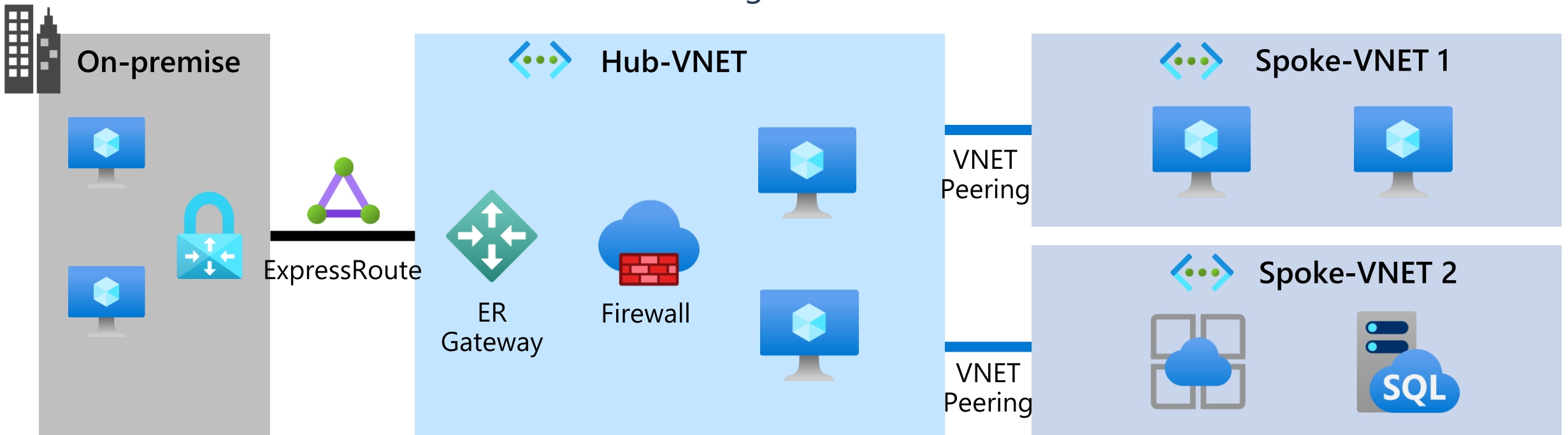
2. クラウドのネットワークセキュリティ

Azure ネットワークのベストプラクティス – Hub & Spoke

ネットワークもセグメンテーションが重要

全体で共有する Hub VNET と各システムのある Spoke VNET の構成がおすすめ！

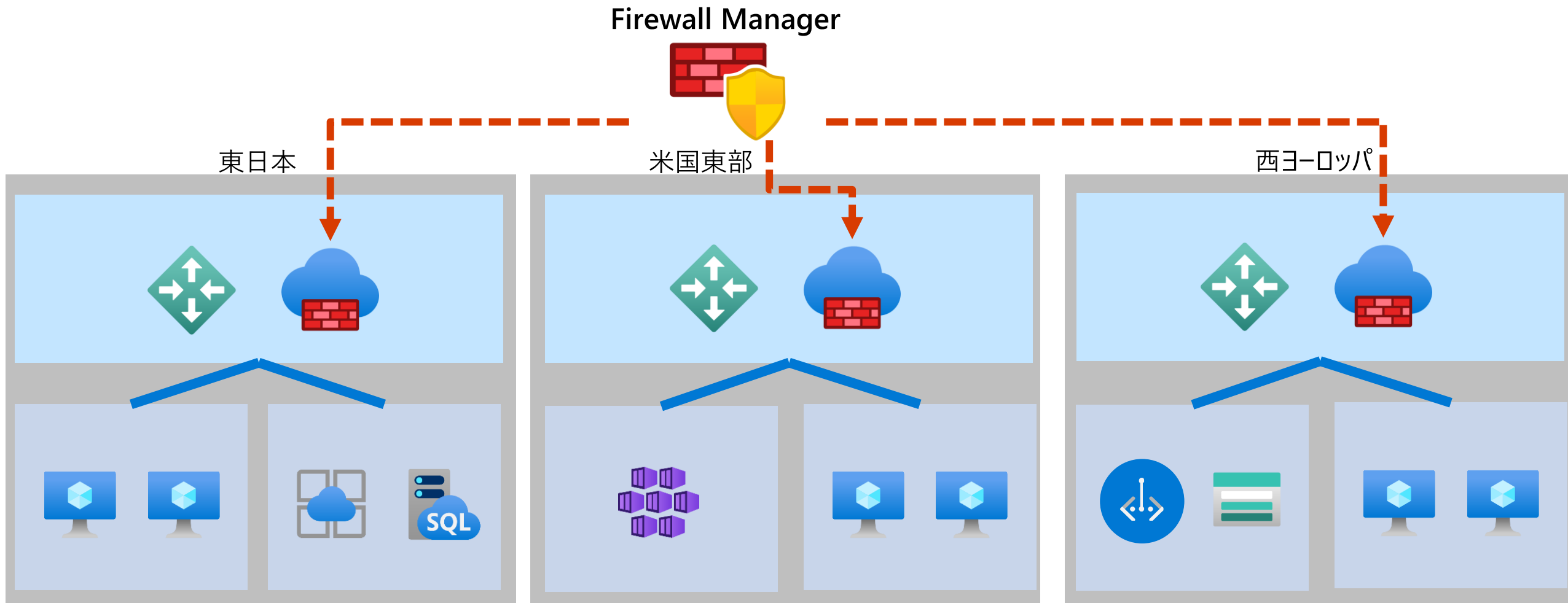
- Hub VNET
 - ExpressRoute と接続するゲートウェイやファイアウォール、AD/DNS など
- Spoke VNET
 - 各システムを設置、Hub VNET と VNET Peering を使って接続



Azure Firewall と Firewall Manager (New)

Azure Firewall は FQDN でのフィルタリングが可能なマネージドな Firewall as a Service

Azure Firewall Manager は複数の Firewall のポリシーを管理



Microsoft Security Forum 2020

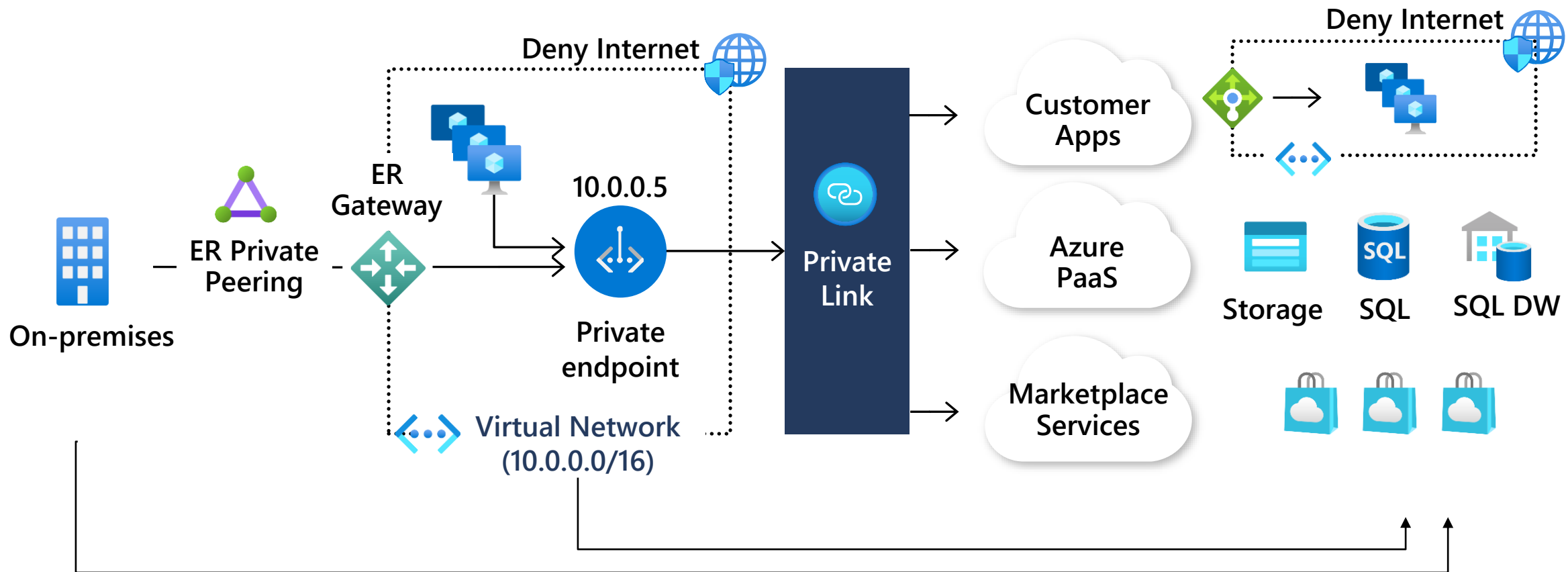


Demo: Azure Firewall

Azure Firewall Manager

Azure Private Link – サービスへのプライベート接続

Azure の PaaS や 他 VNET にある Load Balancer 配下のアプリケーションへのプライベート IP アドレスでのアクセスを提供



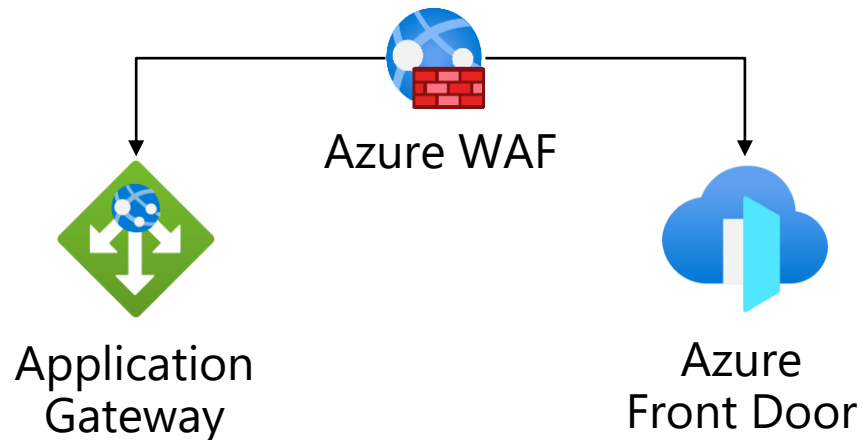
VNETやオンプレミスから、プライベートIPでリソースにアクセス！

外向けアプリケーション向けソリューション – WAF & DDoS

公開アプリケーションに対して、Azure では Azure WAF と DDoS Protection Standard を提供

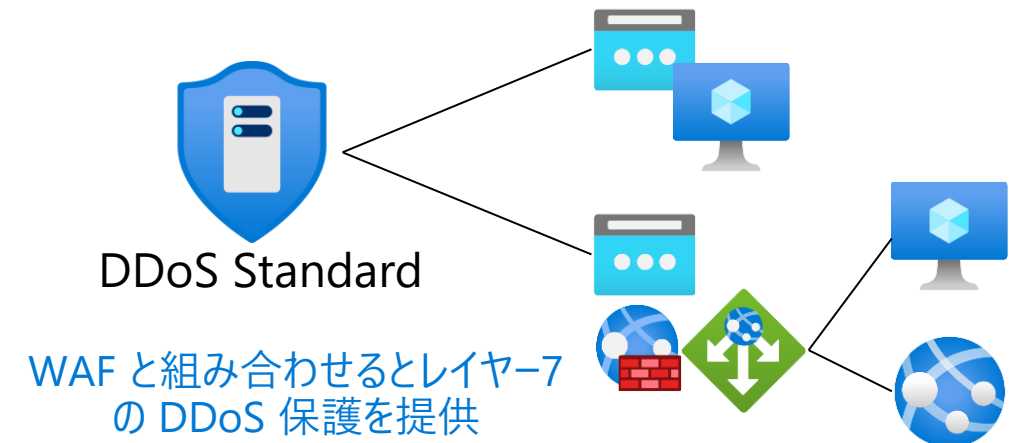
Azure WAF

- VNET 上に置かれる L7 ロードバランサーである Application Gateway か グローバルに分散するアクセスポイントである Azure Front Door に WAF を設置
- OWASP のルールセットを適用



DDoS Protection Standard

- 自分が利用するパブリック IP へのトラフィックにチューニングした動的な閾値を用いた DDoS 保護を提供
- マイクロソフトのネットワークを用いるため遅延が少なく、また Office 365 や XBOX での知見を活用

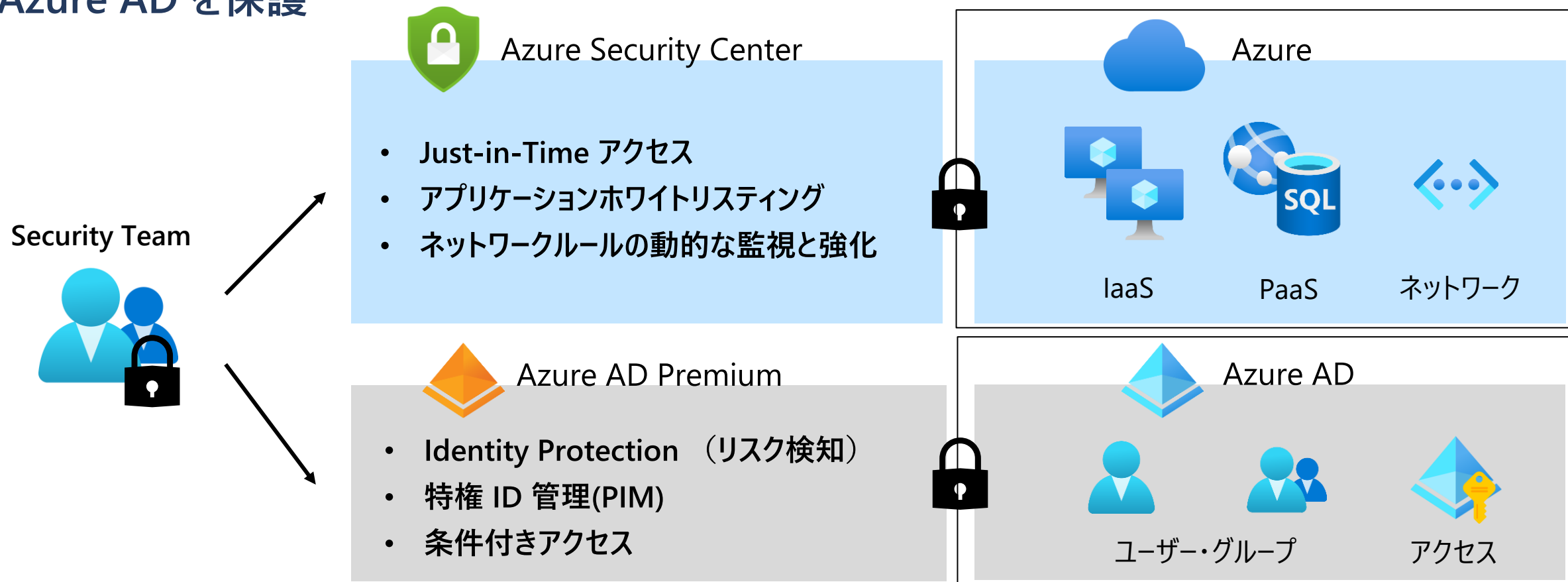


3. リソースの脅威からの保護と検知

リソースの脅威からの保護

Azure における脅威からの保護では、IaaS と PaaS の保護と Azure AD におけるユーザー・アクセスの保護を検討することが必要

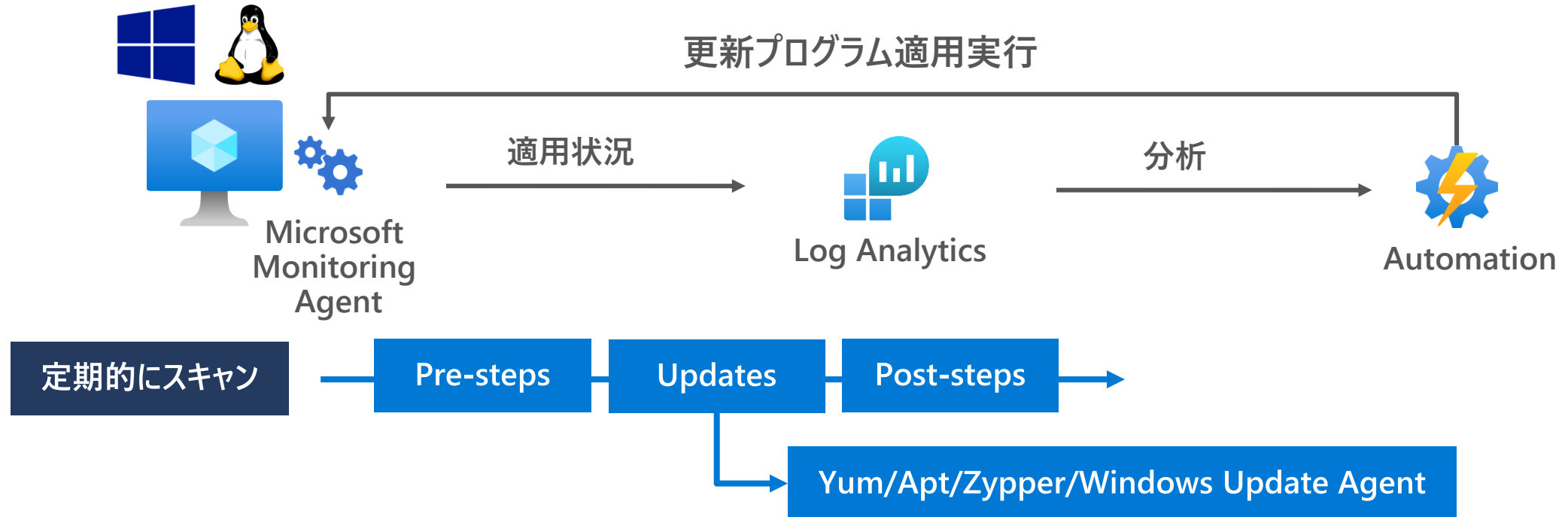
Azure では、Azure Security Center で IaaS と PaaS を保護し、Azure AD Premium の機能で Azure AD を保護



リソースの脅威からの保護 - サーバーのパッチ管理

Azure Automation Update Management を使い、すべての場所の Windows / Linux Server のパッチの適用状況を監視し、適用をスケジュール実行

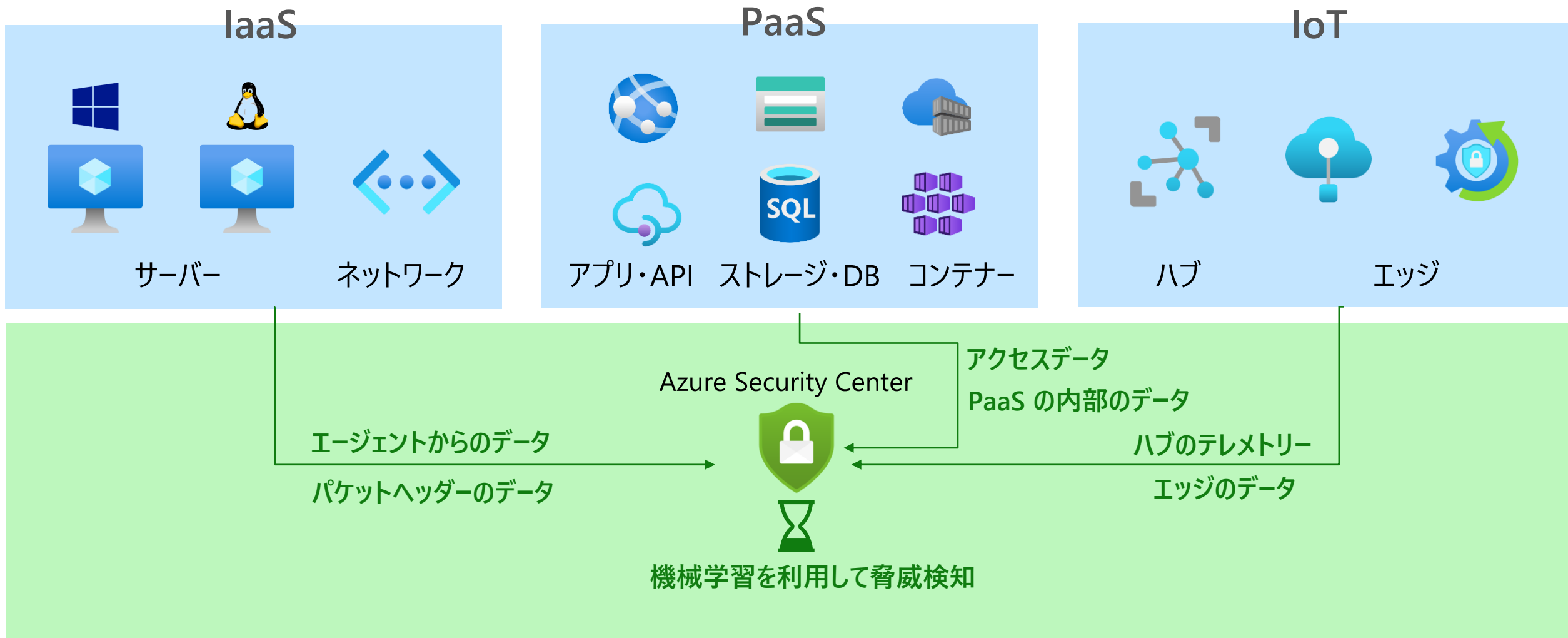
マイクロソフト自体も、SCCM から Update Management にサーバーのパッチ管理を移行^[1]



[1] How Microsoft is transforming its own patch management with Azure
<https://www.microsoft.com/itshowcase/blog/how-microsoft-is-transforming-its-own-patch-management-with-azure/>

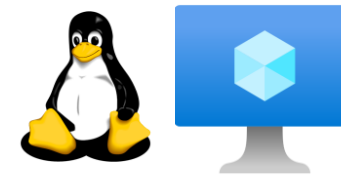
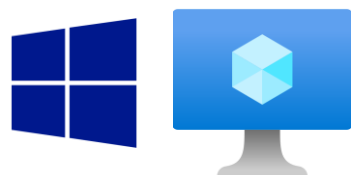
リソース上の脅威の検知

Azure において脅威検知は **Azure Security Center** が担うが、対象によって方式が大きく異なる



Azure Security Center / MDATP のサーバー・IaaS の脅威検知

サーバーに関しては、Azure Security Center と MDATP を組み合わせて脅威を検知
Windows Server では、Azure Security Center があれば MDATP も合わせて利用可能



高度な
ふるまい検知



EDR



イベントログやダンプ
ファイルベースの検知



EDR
(Coming Soon)



Auditd ベース
の検知

アンチウイルス

Windows Defender
マイクロソフトアンチマルウェア (Azure)



アンチマルウェア (Preview)

Azure
ネットワーク

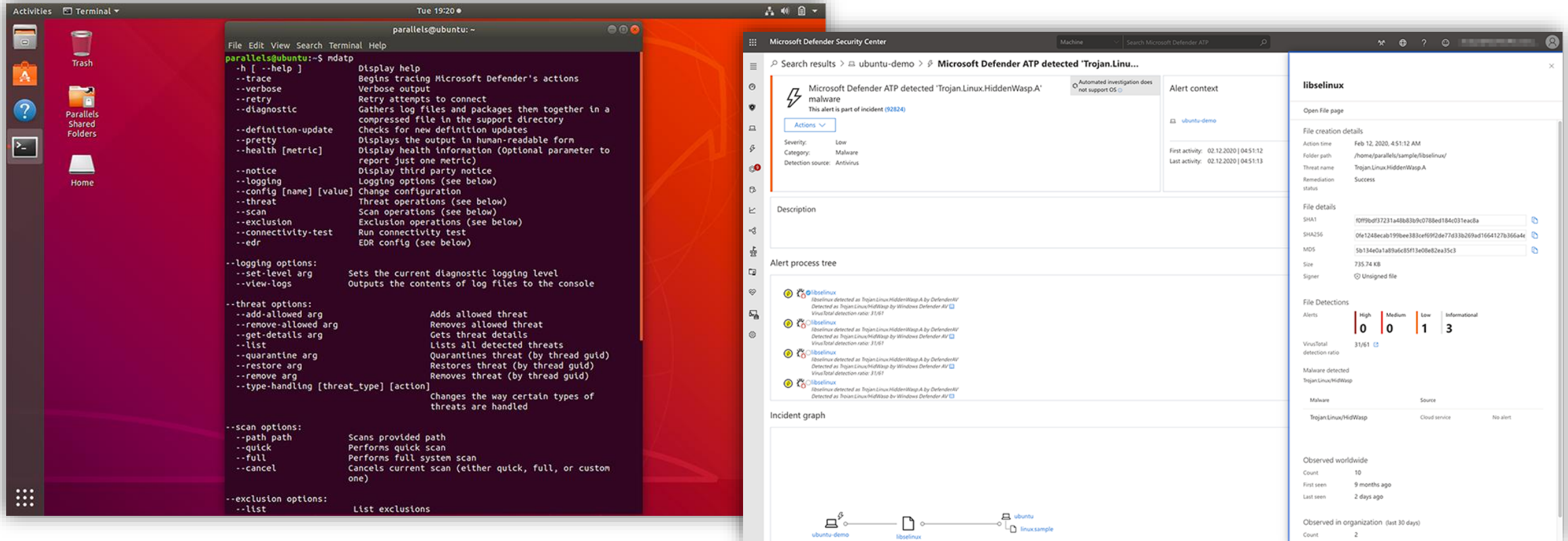


Azure のコアルーターの持つパケットヘッダーの情報から、不正な通信を検知

[New] Microsoft Defender ATP for Linux

RSA Conference 2020 にて、Microsoft Defender ATP が Linux サーバーに対象を広げることを発表

アンチウイルスがプレビュー提供開始、今後 EDR 機能を提供予定



Microsoft Defender ATP for Linux

<https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/microsoft-defender-atp-linux>

Microsoft Security Forum 2020

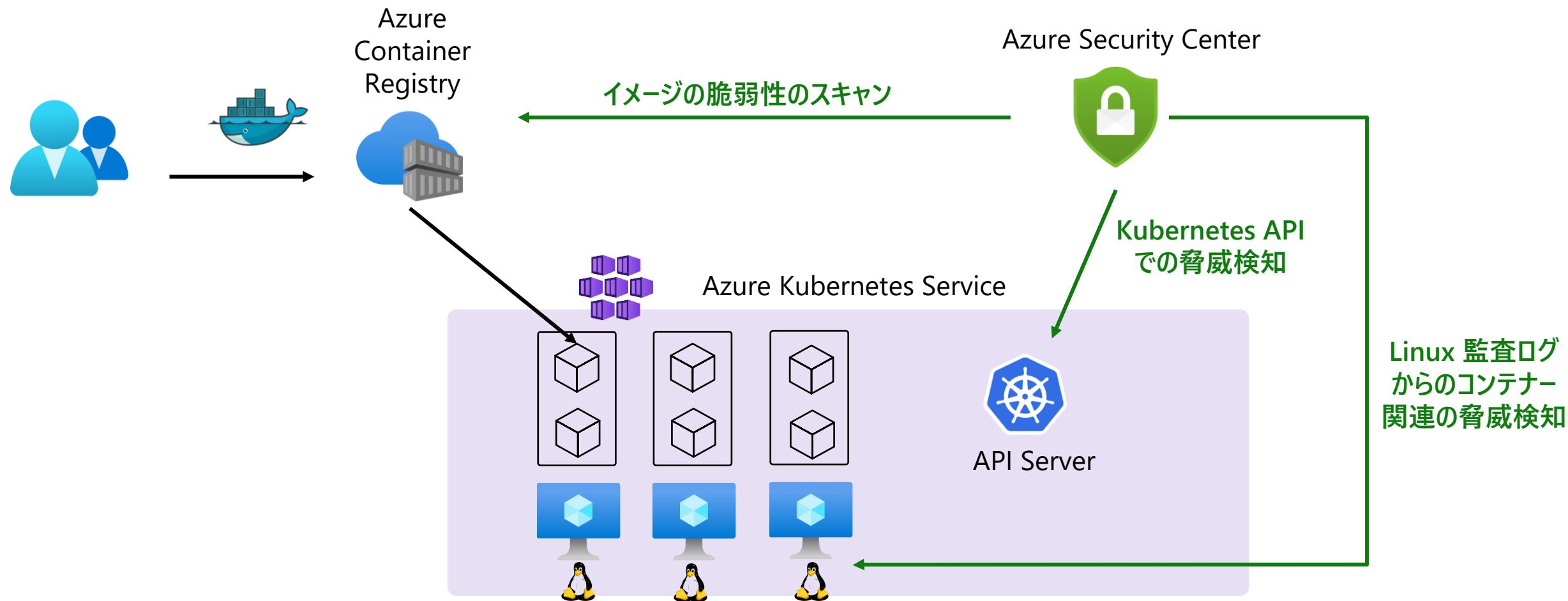


Demo: Microsoft Defender ATP

Windows Server and Linux Server

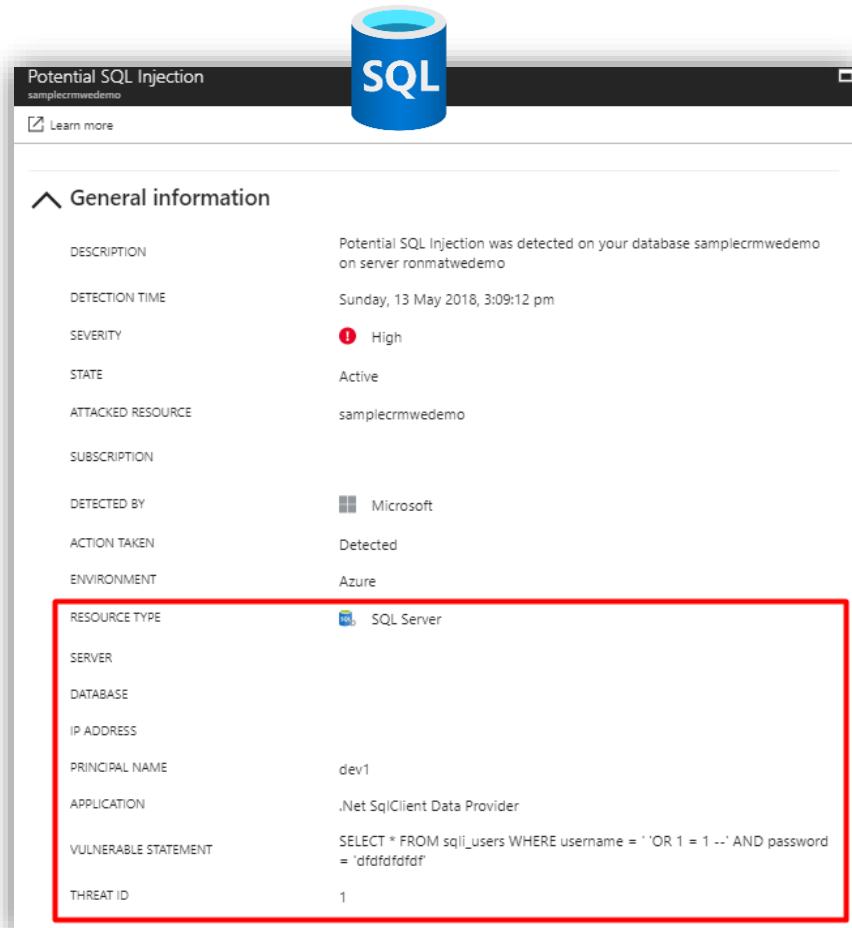
Azure Security Center のコンテナでの脅威検知

Kubernetes (AKS), Linux Host, レジストリ上のイメージ (Azure Container Registry) のそれぞれのレイヤーで脅威を検知



Azure Security Center の PaaS での脅威検知

Storage や データベースへの不審なアクセスやふるまい、データベースへのSQL インジェクションや Storage へのマルウェアのアップロードなどを検知



The screenshot shows an alert titled "Potential SQL Injection" with a severity of "High". The alert details include the detection time (Sunday, 13 May 2018, 3:09:12 pm), the state (Active), the attacked resource (samplecrmwedemo), the subscription (samplecrmwedemo), the detected by (Microsoft), the action taken (Detected), and the environment (Azure). A red box highlights the "RESOURCE TYPE" section, which includes the server (SQL Server), database (dev1), IP address, principal name (dev1), application (.Net SqlClient Data Provider), vulnerable statement (SELECT * FROM sql_users WHERE username = 'OR 1 = 1 --' AND password = 'dfdfdfdf'), and threat ID (1).

Potential SQL Injection
samplecrmwedemo

Learn more

General information

DESCRIPTION	Potential SQL Injection was detected on your database samplecrmwedemo on server ronmatwedemo
DETECTION TIME	Sunday, 13 May 2018, 3:09:12 pm
SEVERITY	High
STATE	Active
ATTACKED RESOURCE	samplecrmwedemo
SUBSCRIPTION	samplecrmwedemo
DETECTED BY	Microsoft
ACTION TAKEN	Detected
ENVIRONMENT	Azure

RESOURCE TYPE

SERVER

DATABASE

IP ADDRESS

PRINCIPAL NAME

APPLICATION

VULNERABLE STATEMENT

THREAT ID

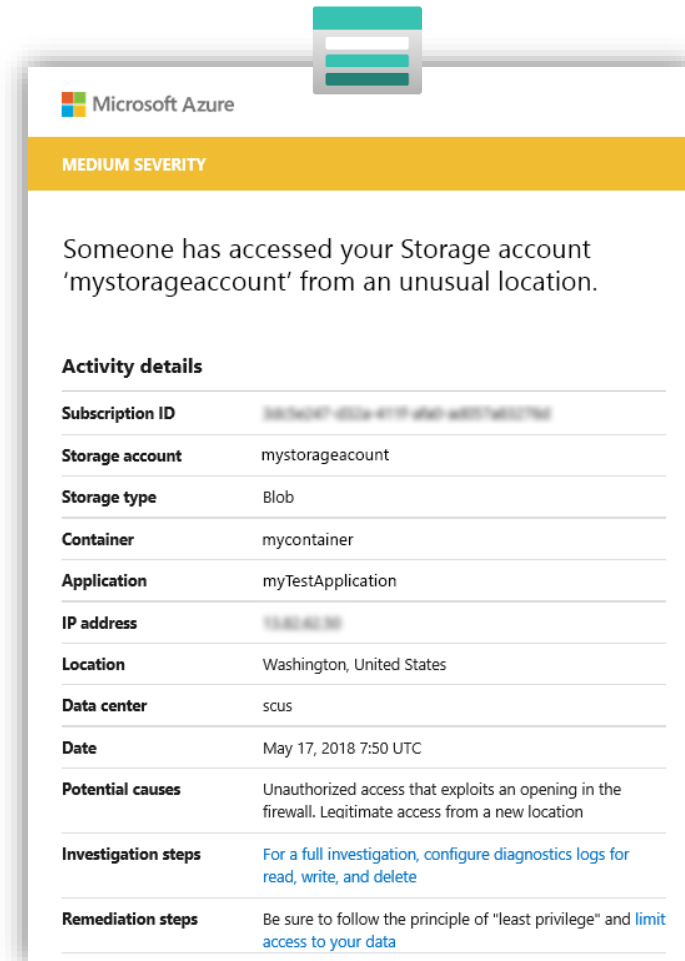
SQL Server

dev1

.Net SqlClient Data Provider

SELECT * FROM sql_users WHERE username = 'OR 1 = 1 --' AND password = 'dfdfdfdf'

1



The screenshot shows an alert titled "Someone has accessed your Storage account 'mystorageaccount' from an unusual location." with a severity of "MEDIUM SEVERITY". The alert details include the subscription ID (samplecrmwedemo), storage account (mystorageaccount), storage type (Blob), container (mycontainer), application (myTestApplication), IP address (192.168.1.1), location (Washington, United States), data center (scus), date (May 17, 2018 7:50 UTC), potential causes (Unauthorized access that exploits an opening in the firewall. Legitimate access from a new location), investigation steps (For a full investigation, configure diagnostics logs for read, write, and delete), and remediation steps (Be sure to follow the principle of "least privilege" and limit access to your data).

Microsoft Azure

MEDIUM SEVERITY

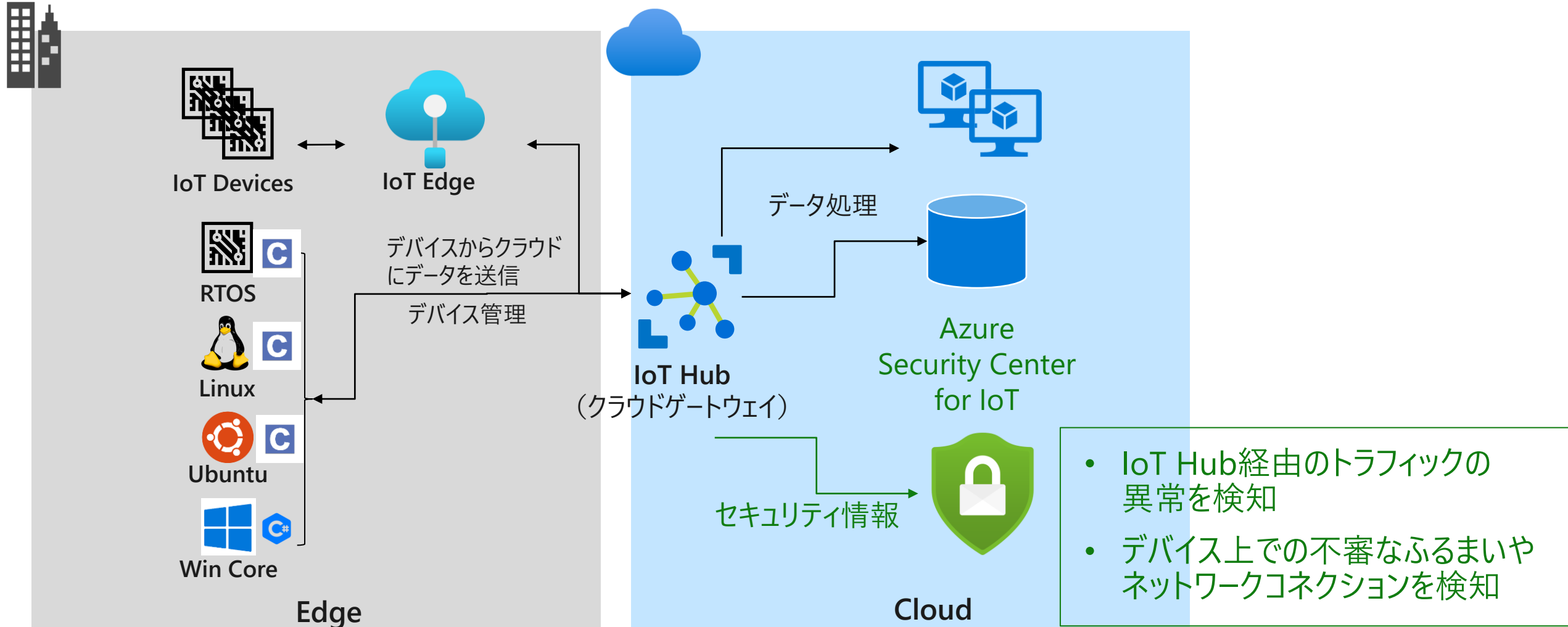
Someone has accessed your Storage account 'mystorageaccount' from an unusual location.

Activity details

Subscription ID	samplecrmwedemo
Storage account	mystorageaccount
Storage type	Blob
Container	mycontainer
Application	myTestApplication
IP address	192.168.1.1
Location	Washington, United States
Data center	scus
Date	May 17, 2018 7:50 UTC
Potential causes	Unauthorized access that exploits an opening in the firewall. Legitimate access from a new location
Investigation steps	For a full investigation, configure diagnostics logs for read, write, and delete
Remediation steps	Be sure to follow the principle of "least privilege" and limit access to your data

Azure Security Center for IoT の脅威検知

Azure IoT の一部としてセキュリティ機能を提供し、IoT 環境での脅威を検知



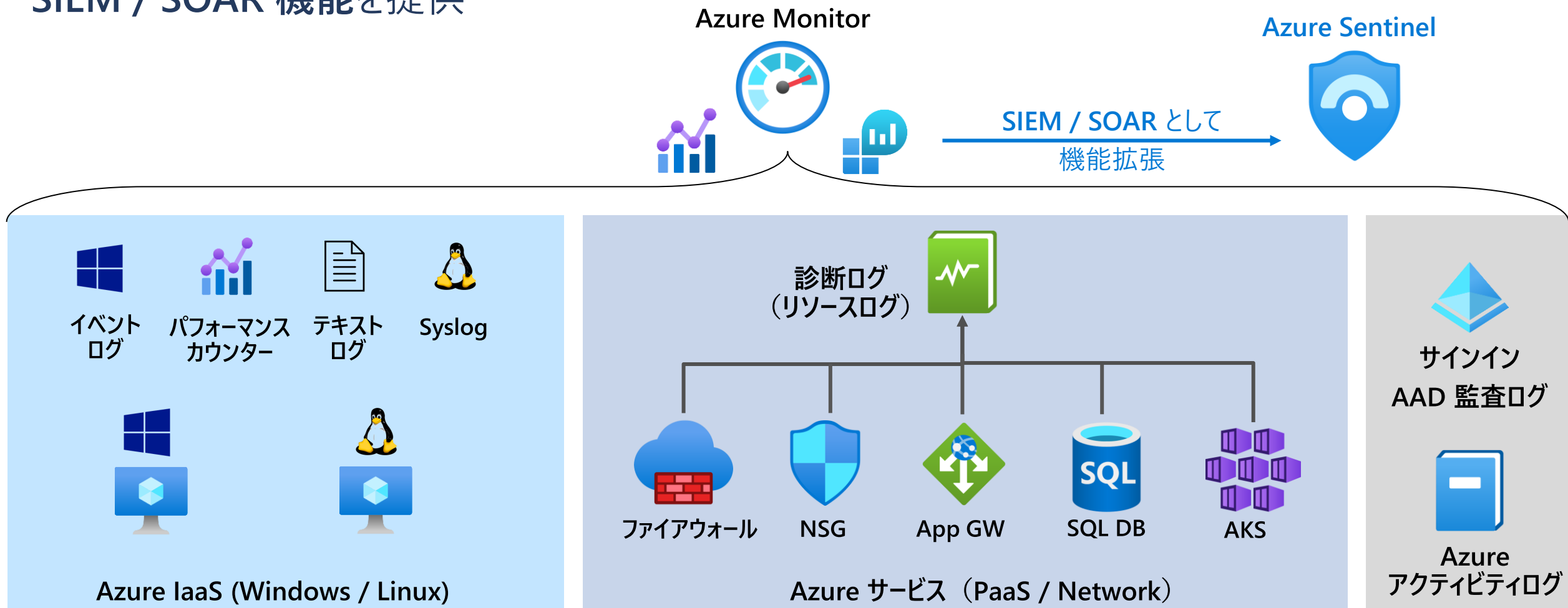
Demo: Azure Security Center for IoT

Azure IoT Hub and Sentinel Connector

4. ログの管理とセキュリティ運用

Azure におけるログ集約と分析

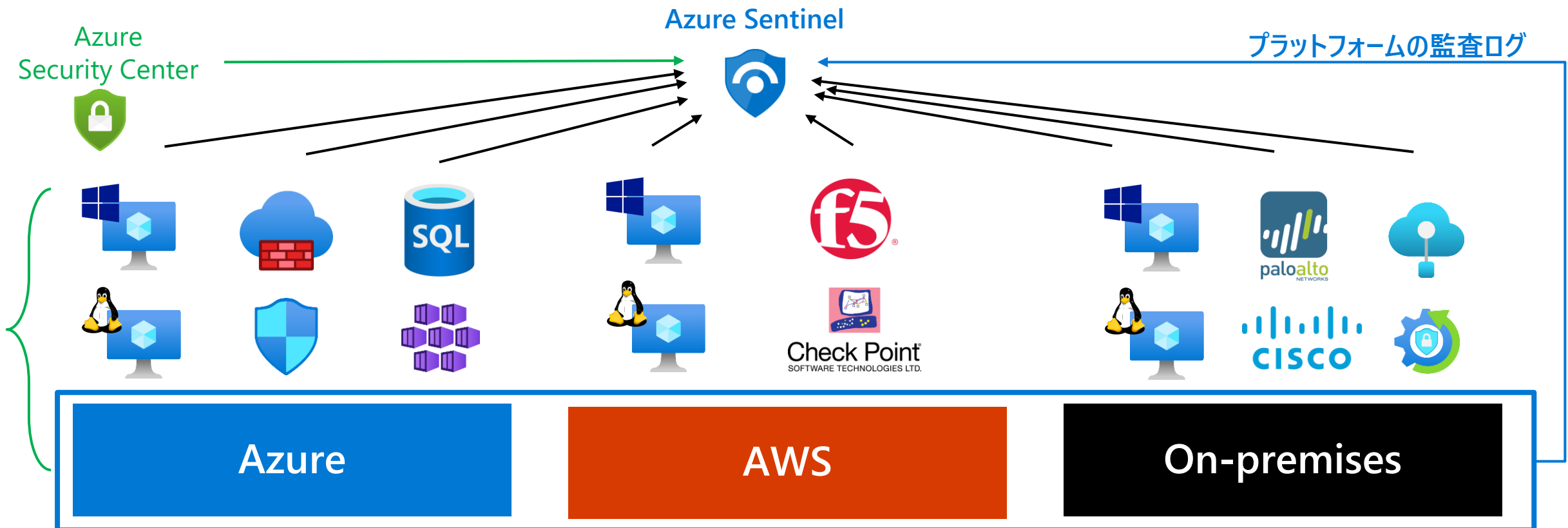
Azure Monitor が統合的なログ管理や監視ツールを提供し、Sentinel はそのアドオンとして、**SIEM / SOAR 機能**を提供



Azure Sentinel によるハイブリッド・マルチクラウドログ集約

Azure Sentinel はハイブリッド・マルチクラウド環境からのセキュリティログ集約基盤としても最適

- AWS CloudTrail からのログ収集が期間限定で無償に！^[1]
- Azure Security Center for IoT コネクターを利用し、IoT デバイスからの情報を Sentinel に収集

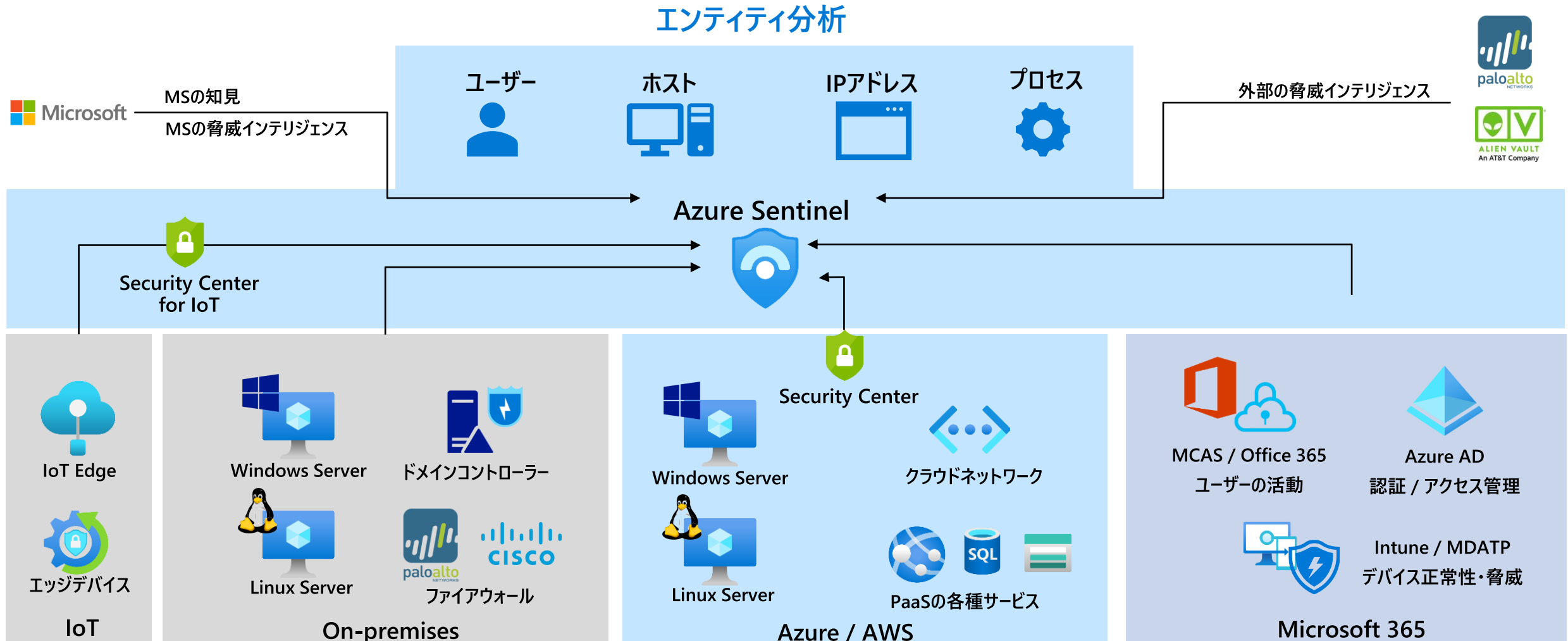


[1] Free import of AWS CloudTrail logs through June 2020 and other exciting Azure Sentinel updates

<https://www.microsoft.com/security/blog/2020/02/20/free-import-of-aws-cloudtrail-logs-through-june-2020-and-other-exciting-azure-sentinel-updates/>

Azure Sentinel の価値 – Entity Analytics (Preview)

Azure Sentinelは、オンプレミス、IaaS / PaaS、SaaS、IoT にわたって、様々なエンティティの情報を取得



Microsoft Security Forum 2020



Demo: Azure Sentinel

Entity Analytics (Preview)

本セッションのサマリ

本セッションでは、Azure の“クセ”を理解したうえで、組み込まれたソリューションをどう利用すればセキュリティを向上できるかご紹介しました

1. GRC ガバナンス・リスク・コンプライアンス
 - セグメンテーションと CSPM (Cloud Security Posture Management)
2. クラウドのネットワークセキュリティ
 - Hub-Spoke 構成と、適切なソリューションの選定
3. リソースにおける脅威からの保護と検知
 - Azure Security Center / MDATP による各レイヤーでの脅威検知
4. ログの管理とセキュリティ運用
 - Azure Monitor / Sentinel での統合管理とエンティティ分析



#digitaltrust

© 2020 Microsoft Corporation. All rights reserved.

本情報の内容 (添付文書、リンク先などを含む) は、Microsoft Security Forum 2020 開催日 (2020年3月12日) 時点のものであり、予告なく変更される場合があります。
本コンテンツの著作権、および本コンテンツ中に出てくる商標権、団体名、ロゴ、製品、サービスなどはそれぞれ、各権利保有者に帰属します。