第4回大学等におけるクラウドサービス利用シンポジウム

# サイバーセキュリティ対策最前線

## Microsoft Operations Management Suite のご紹介

日本マイクロソフト株式会社
パブリックセクター統括本部
クラウドアーキテクト

中田　寿穂 <Hisaho.Nakata@microsoft.com>

# サイバースペースの現状

企業の90%は
脅威が侵入済み

**90%**

**67%**

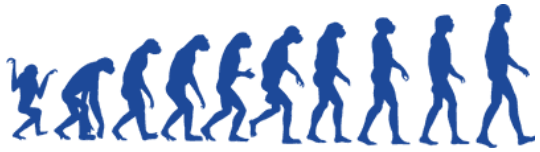
**242日**

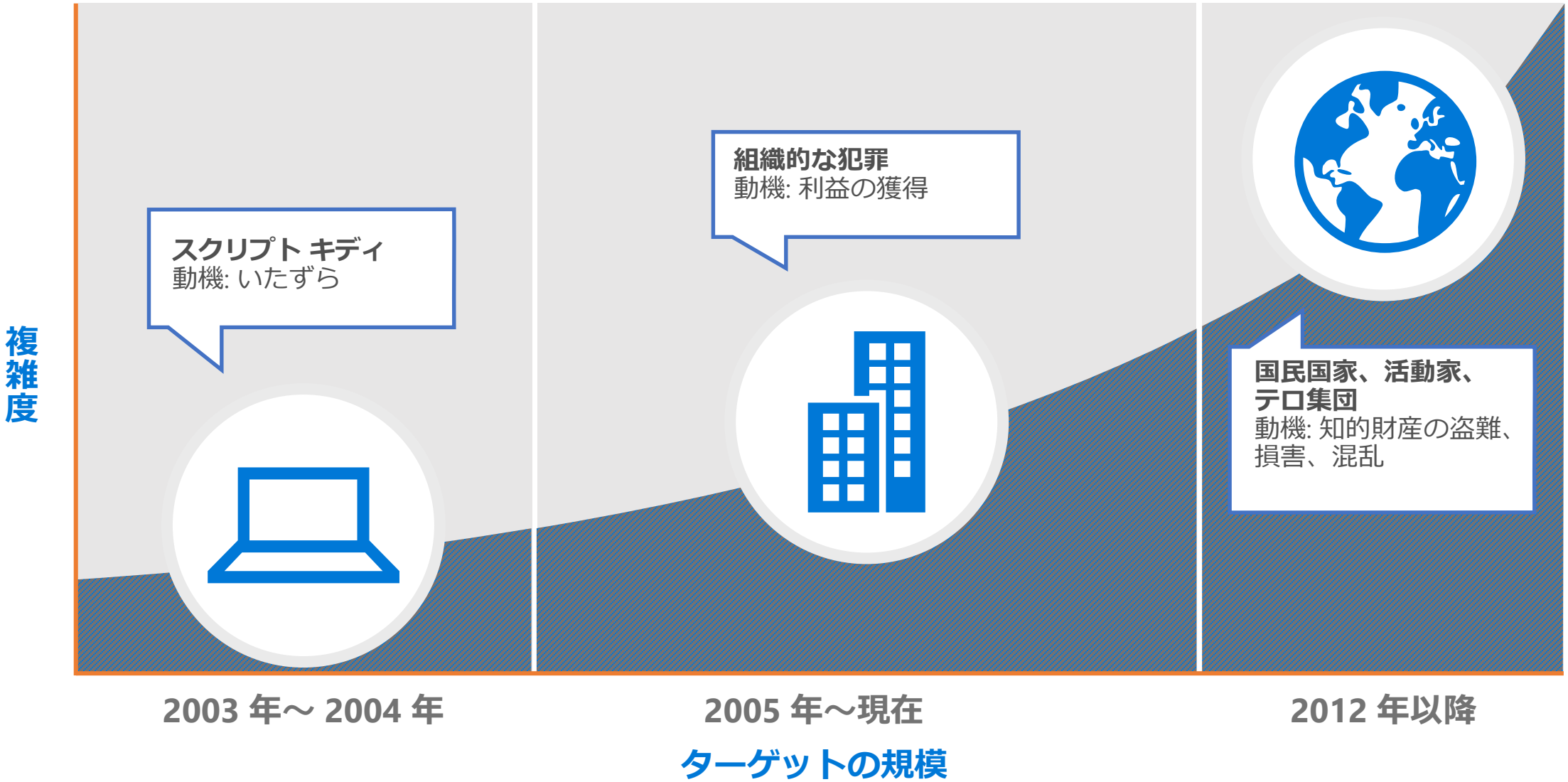
侵入から平均242日、
脅威が検出されていない

ウィルスの
67%は特注品

Copyright@2017 Microsoft. All Right Reverved.

# サイバー攻撃の進化






Copyright@2017 Microsoft. All Right Revered.

# 正しい
# セキュリティ対策
# の考え方

Copyright@2017 Microsoft. All Right Revered.

# 正しく怖がる

Copyright@2017 Microsoft. All Right Revered.

# セキュリティ対策の考え方

以　　前

サイバー攻撃を受けないようにする対策

現　　在

攻撃者の費用対効果を

下げる対策

Copyright@2017 Microsoft. All Right Reverved.

# セキュリティ対策の考え方

1. **防御力向上**　やられないようにする
2. **検知分析**　やられていることをすぐに検知する
3. **被害軽減**　やられても被害を小さくする
4. **事後対応**　やられた後でも、情報を保護する

Copyright@2017 Microsoft. All Right Reverved.

# マイクロソフトが推奨する
# セキュリティ対策

Microsoft

Copyright@2017 Microsoft. All Right Reverved.

# 結局何を守ればよいのか？

攻撃の着弾点となる

**パソコン**

の保護

被害拡大の要因となる

**ID**

の保護

第三者が読めないように

**データ**

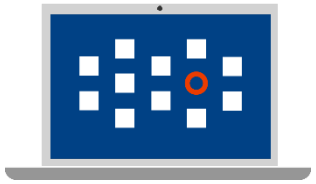
を保護

**この３点が非常に重要**

Copyright@2017 Microsoft. All Right Reverved.

# Enterprise Mobility Suite

ID および
アクセス管理



行動分析による
サイバー攻撃の
分析、検出

モバイル デバイスと
アプリの管理

情報の
保護と追跡

| Azure Active Directory | Advanced Threat Analytics | Intune | Azure Rights Management |
|---|---|---|---|

Enterprise Mobility Suite

Copyright@2017 Microsoft. All Right Reverved.

# 結局何を守ればよいのか？

攻撃の着弾点となる

**Windows 10/Defender**

の保護

被害拡大の要因となる

**Azure Active Directory**

の保護

第三者が読めないように

**Azure RMS**

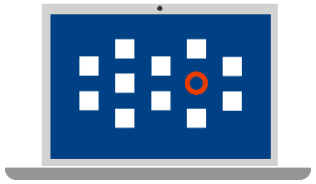
を保護

**この３点が非常に重要**

Copyright@2017 Microsoft. All Right Reverved.

# Enterprise Mobility Suite

ID および
アクセス管理



行動分析による
サイバー攻撃の
分析、検出

モバイル デバイスと
アプリの管理

情報の
保護と追跡

| Azure Active Directory | Advanced Threat Analytics | Intune | Azure Rights Management |
|---|---|---|---|

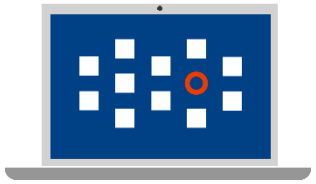
Enterprise Mobility Suite

**やられていることにすぐに気づく**

Copyright@2017 Microsoft. All Right Reverved.

# Microsoft Cloud App Security

ID および
アクセス管理



行動分析による
サイバー攻撃の
分析、検出

モバイル デバイスと
アプリの管理

情報の
保護と追跡

クラウドアプリ
のセキュリティ

Azure Active Directory

Advanced Threat Analytics

Intune

Azure Rights Management

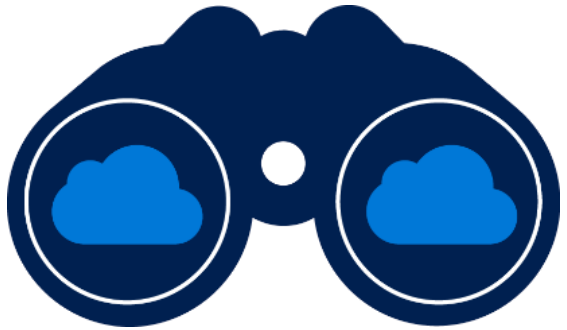
Cloud App Security

Enterprise Mobility Suite

**クラウドは安全… でも危険なのはユーザーの使い方 →**

Copyright@2017 Microsoft. All Right Reverved.

# Microsoft Cloud App Security でできること



## 検出 / 調査

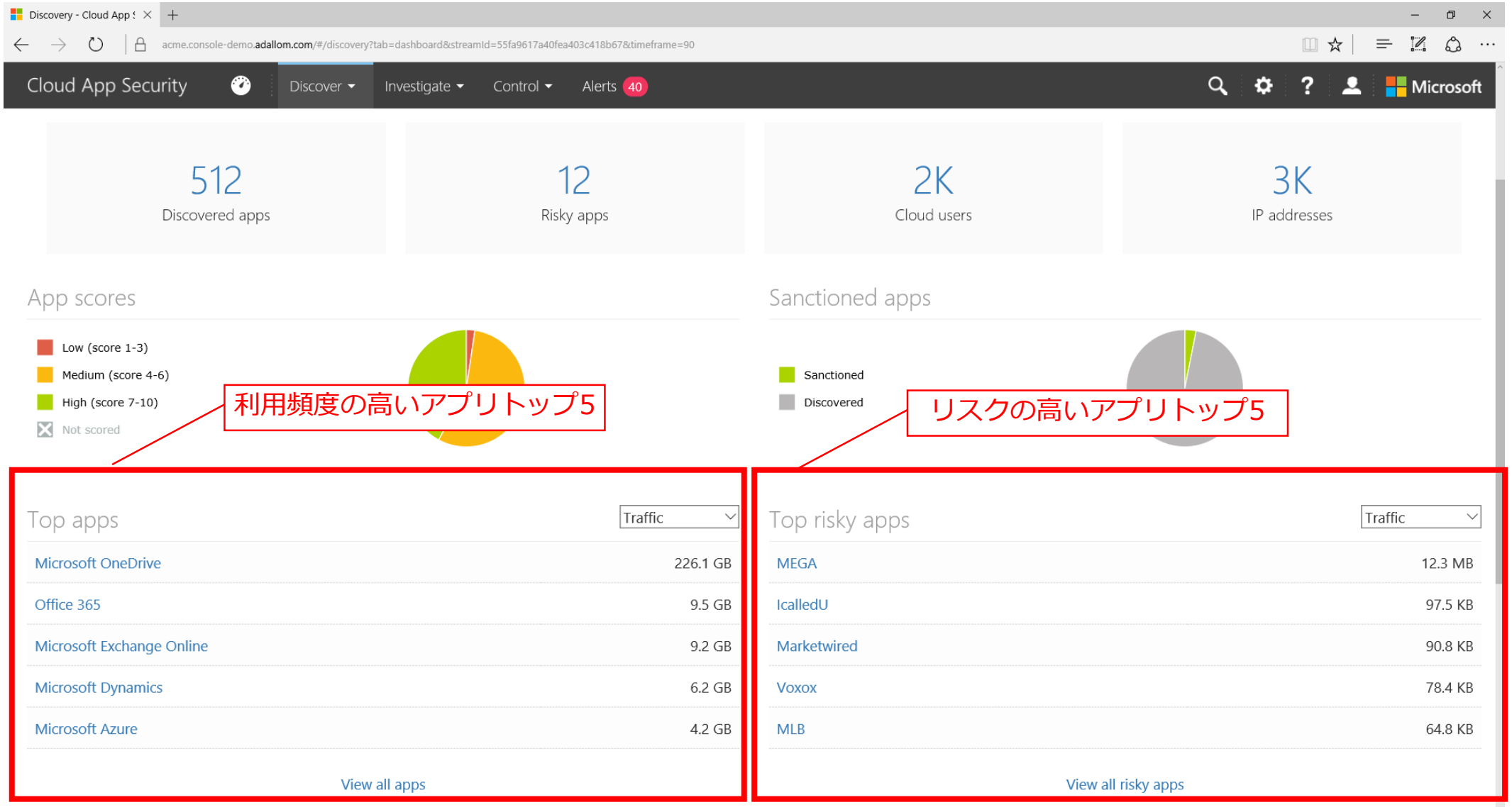
- シャドウ IT の検出 (未承認アプリの検出)
- リスクの高い行動、データ、異常な動作、脅威を把握
- 特定のユーザーや行動を簡単にドリルダウン

## データ制御 / 脅威からの保護

- アクセス、行動、データ共有に関するポリシーを作成
- データ漏えいを防止 (DLP)
- リスクを最小限に抑え、脅威の回避とポリシーの適用を自動化

Copyright@2017 Microsoft. All Right Reverved.

# Microsoft Cloud App Security でできること

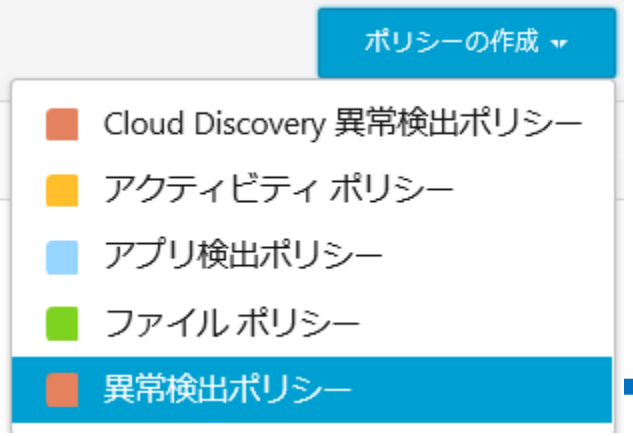



Copyright@2017 Microsoft. All Right Reserved.

# Microsoft Cloud App Security でできること

## クラウドアプリの異常な使われ方があった際に検出

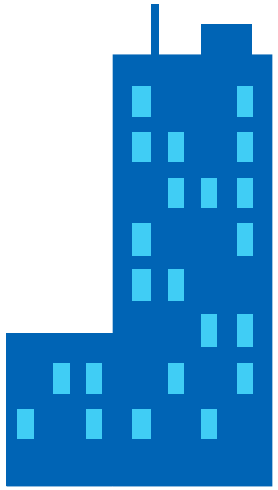
- ✓ これまで使用していないアプリで、突然 500 GB のデータをアップロードした
- ✓ 通常よりもはるかに多いトランザクションがあった　…など



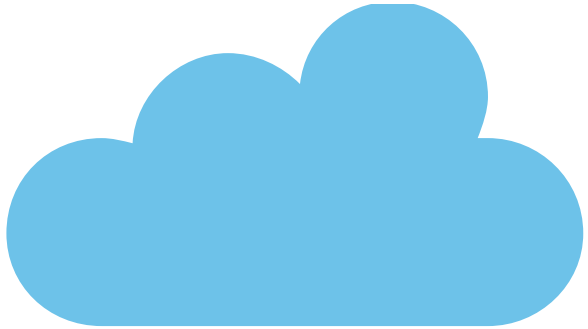
Copyright@2017 Microsoft. All Right Reverved.

# Operations Management Suite (OMS)

マルチ OS、マルチクラウドな **ハイブリッドクラウド時代** だからこそ、
**一元管理ができる運用管理** サービスを



**オンプレミス DC**
Windows Server, Linux,
VMware, OpenStack



**クラウド環境**
Public and Hosted
Azure, AWS

| インサイト＆分析 | 自動化＆コントロール | セキュリティ ＆ コンプライアンス | 保護＆可用性 |
|---|---|---|---|
| ハイブリッド クラウド 全体の可視化と分析 | 複雑で反復的な操作の 自動化と制御 | セキュリティと 監査情報の可視化 | データ保護と ディザスタリカバリー対策 |

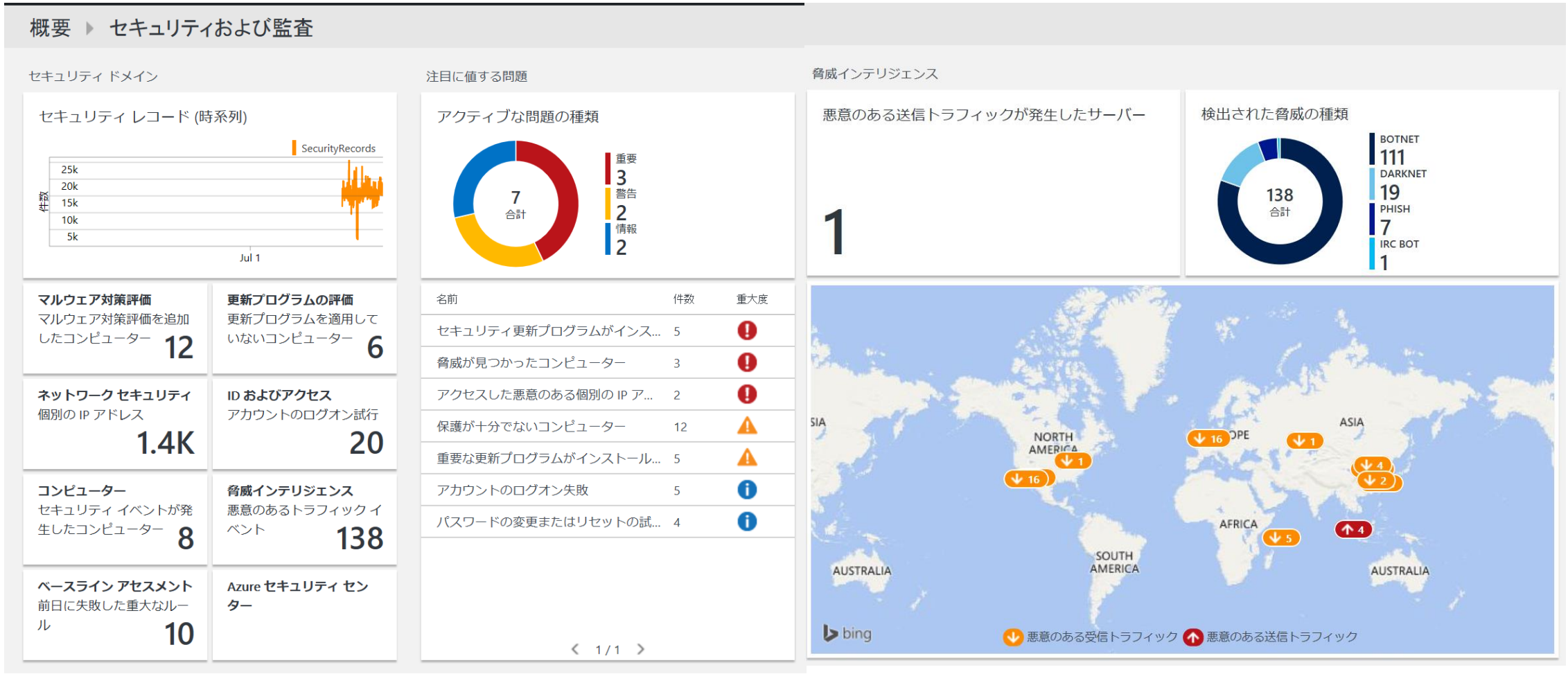
Copyright@2017 Microsoft. All Right Revered.

# Azure Log Analytics

- Log収集対象(Windows Server/Windows Client/Linux)のOSに展開したAgent経由で、各種logデータをAzure上のLog Analytics にアップロード（容量無制限）
- アップロードされた各種logデータから自由な検索構文で高速検索、自由に定義した検索を最小間隔で5分に1度実行、結果を元にアラート処理(メール送信、Webhook、Azure Automationによるジョブ実行)が可能。
- Microsoftが様々な分析ロジックと各分析結果の表示画面を多数用意。Logをアップロードするだけで様々な分析結果の把握が可能。Zabbix/NagiosやOffice 365とのlog連携も可能。

Copyright@2017 Microsoft. All Right Reverved.

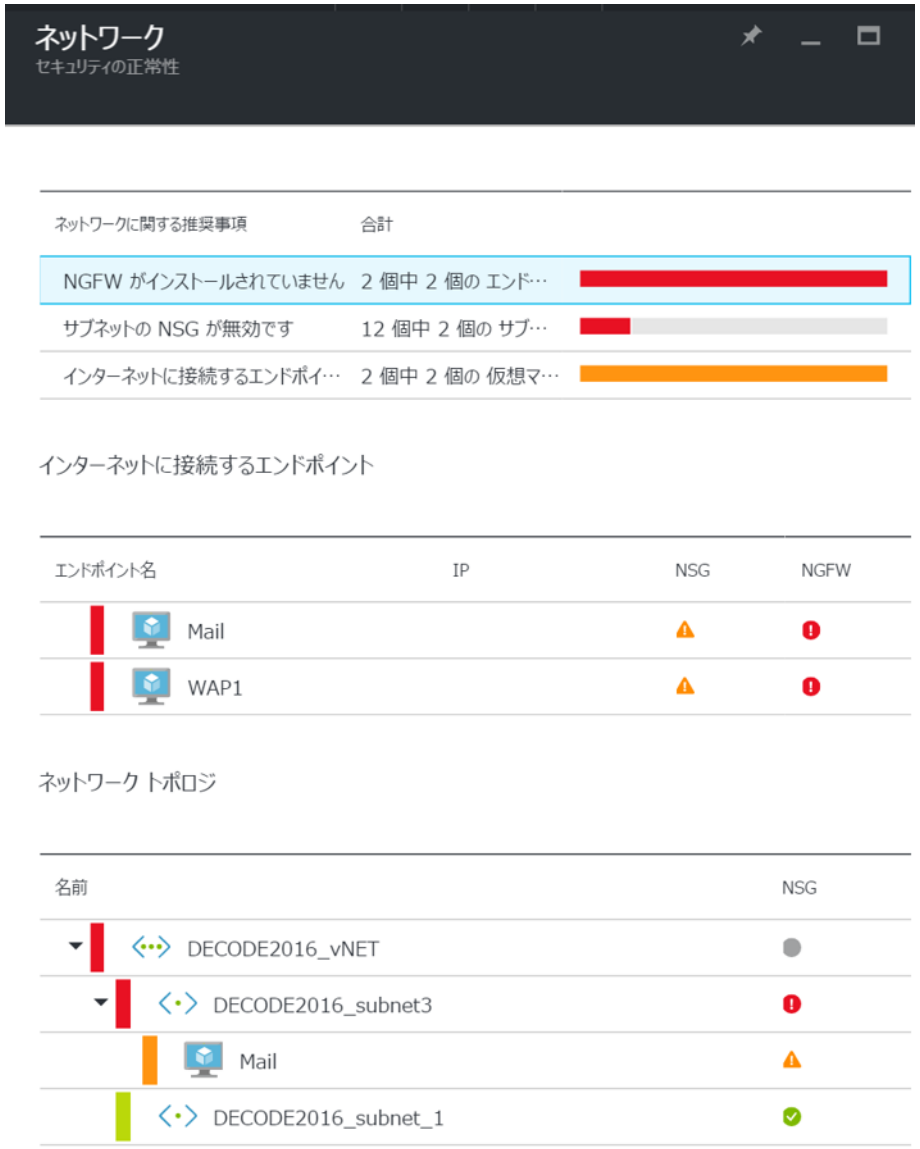
# Security and Audit 機能




収集Logデータから、Darknet,Botとの通信、login(成功、失敗)情報、通信IP情報、パスワードが変更された等、セキュリティ関連情報の一元把握を実現

Copyright@2017 Microsoft. All Right Reverved.

# Azure Security Center




サブススクリプションレベルで構成変更に自動追従
IaaS VM の新規作成/削除、各NWの変更等にも自動追従
セキュリティ管理者は全環境の最新ステータスを常に監査可能

Copyright@2017 Microsoft. All Right Reverved.

# まとめ

**正しくおそれる**ことが、セキュリティ対策費用の過剰投資を防ぐ第一歩です。

「やられることを防ぐ」だけではなく

**① やられたことを検知する**

**② やられても被害を少なくする**

**③ やられた後でも情報を保護する**

ためのシステムを構築しましょう。

Copyright@2017 Microsoft. All Right Revered.