2025/11/28

セキュリティ、ほんまに100種類あるんちゃう？
～ MS ってセキュリティも強いんやで～

1st Part

いまさら聞けない Azure セキュリティのキホン！

ANLIMITRIA代表
沓澤 繁臣

話者プロフィール

20年インフラに向き合ってきた、音楽も愛する“裏方クリエイター”

- ITエンジニアとしてサーバー・ネットワーク・仮想基盤など、
  大規模システムの設計～構築～運用まで幅広く担当
- AzureやCitrixなどクラウド系も実務経験多数
- プロジェクトのまとめ役（PL・PM）としての経験もあり、
  技術と部門間調整の両方を担当
- 個人事業主 (ANLIMITRIA) として、
  中小企業や個人事業主のIT伴走サポートや業務効率化(DX含む)
  AIの導入やIT資格の取得サポートなど幅広く対応
- **インフラ×Web×教育×クリエイティブなどの複合案件**にも従事
- 個人ではWebサイト構築や音楽制作も行い、
  裏方としてクリエイターの活動を支える仕事にも力を入れている

苫澤　繁臣
くつざわ しげおみ

7月5日生まれ
40歳

東京都出身
尼崎市在住

ITと音楽が好きです！

このパートの目次

- 1. クラウド時代のセキュリティ
- 2. Azureセキュリティ基礎
- 3. Defender for Cloud 概要

クラウド時代のセキュリティ環境

- 攻撃対象領域 の拡大
- マルチクラウドの常態化
- 境界型防御の限界

クラウド時代のセキュリティ環境

- 攻撃対象領域の拡大
  リモートワークによるシステムの分散化により、守るポイントが急増
  例：SaaS / PaaS / IaaS / API / デバイス / IDなど

- マルチクラウドの常態化
  - 10年前と違い、環境の変化から「守る場所」が爆発的に増えている
    過去：オンプレサーバー数台
    現代：Azure VM・Storage・WebApp・API・Apps・Teams・SaaS まで点在
  - 物理的に社内に置いていたものがクラウドや外部サービスに散らばる
  - ID、デバイス、クラウドサービス、API、ネットワーク…全部が攻撃対象に
  - “攻撃者の視点”からすると、どこか一つ弱い箇所があれば突破される

- 境界型防御の限界
  「攻撃される面」が広がった＝防御が難しくなった

クラウド時代のセキュリティ環境

- 攻撃対象領域 の拡大

  Azure＋AWS＋SaaSなど組み合わせが当たり前
  全体像の把握が難しい＝統合管理が重要

  •今の企業は “Azure だけ使ってる” なんてほぼない
  AWSも使う　GitHub使う　Salesforce使う　Google Workspace併用

- マルチクラウドの常態化

  •リソースが複数のクラウドに散らばると
  全体のセキュリティ状況が把握しづらい

- 境界型防御の限界

  •各クラウドに“設定ミス(Misconfiguration)”が起きやすい
  - •パブリックストレージ公開
  - •認証なしのAPI
  - •弱いパスワード

  •Azure と AWS の設定ルールが違うため
  → セキュリティポリシーを統一しないと穴が生まれる

  •ここをAzureは「**Defender for Cloud**」でマルチクラウド統合管理して補う

クラウド時代のセキュリティ環境

“社内＝安全”という前提が崩壊
在宅・SaaS利用・クラウド接続により境界が消滅
内部からの侵害も増加 → ゼロトラストが必須の時代に

- 昔は「会社のネットワークの中は安全」だった
  → **ファイアウォール**で外からの攻撃を防ぐ発想

- 今は、在宅勤務　SaaSの利用　モバイルデバイス　クラウド接続

つまり・・

ネットワークの“内と外”の境界線が消えた

- さらに・・・

内部からの攻撃（内部犯/乗っ取りによる内部アクセス）が急増

- 境界防御（城の壁方式）は、クラウド時代には根本的に合わない
  ↑Microsoftがゼロトラストを推す理由はここにある！↑

「境界がない世界なので、境界防御が機能しない」
“どこからアクセスしても信用しない” が標準

クラウド時代のセキュリティ環境

- 攻撃対象領域 の拡大

  リモートワークによるシステムの分散化により、守るポイントが急増
  例：SaaS / PaaS / IaaS / API / デバイス / ID など

- マルチクラウドの常態化

  Azure＋AWS＋SaaSなど組み合わせが当たり前
  全体像の把握が難しい＝統合管理が重要

- 境界型防御の限界

  “社内＝安全”という前提が崩壊
  在宅・SaaS利用・クラウド接続により境界が消滅
  内部からの侵害も増加 → ゼロトラストが必須の時代に

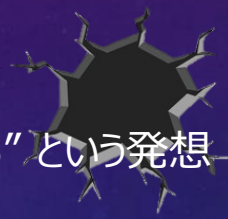
Microsoftのセキュリティ哲学

- Zero Trust (無信頼)

  Microsoft のセキュリティは、Zero Trust がベース
  つまり『最初から誰も信用しない』『いつかは破られる前提で設計する』という思想
  すべてのアクセスを都度チェックする

- Assume Breach（侵入前提）

  “絶対に破られない城を作る” のではなくて、
  “どこかは破られるから、その前提で被害を最小化する” という発想



- 信頼せず、常に検証する

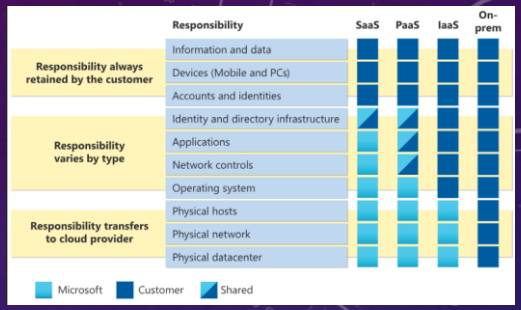
  Zero Trust のキーワードは “Never trust, always verify”
  社内からのアクセスでも、VPNで入ってきても、一度通した端末でも、
  『一回通したから次もOK』にしない、**毎回検証する** というのが基本

- 最小権限で守る

  もうひとつ重要なのが 最小権限(Least Privilege)
  “なんとなく管理者権限” ではなくて、必要な人に必要なときだけ必要な範囲だけ権限を渡す
  Azureでは RBAC や PIM などで実現する

Shared Responsibility Model

- クラウドでは、Microsoft と利用者の責任が分担される
- サービスモデルによって守る範囲が変わる(IaaS / PaaS / SaaS)
- “設定ミス(Misconfiguration)”は利用者側の責任



1. そもそもなぜ責任分担が必要か？
クラウドに移行しても“自動で全部守ってくれる”わけではありません。
クラウドは“環境を提供する責任”と、“使い方を適切に管理する責任”に分かれます。

2. IaaS → PaaS → SaaS の話
IaaS の場合、インフラまでは Microsoft が守るけどOS以上は利用者が責任を持つ必要があります。
PaaSになると OS管理が不要で、さらに責任範囲が減ります。
SaaSでもデータやアクセス権限は利用者の責任です。

3. 設定ミスがなぜ問題か？
一番多い攻撃の入り口はストレージ公開、弱いパスワード、認証未設定のAPIなどの
“設定ミス(Misconfiguration)”で、ここを自動で教えてくれるのが Defender for Cloud です。

モデル	Microsoftの責任	利用者の責任
IaaS	ハード／ネットワーク／仮想化	OS・パッチ・アプリ・データ・アクセス制御
PaaS	OS／ランタイム／基盤管理	アプリ構成・データ・ID管理
SaaS	すべての運用管理	データ・ユーザー設定・アクセス制御

https://learn.microsoft.com/ja-jp/azure/security/fundamentals/shared-responsibility

Azureセキュリティの全体像

Azure セキュリティは、4つのレイヤーで構成される

1. Identity (Entra ID:認証・認可の基盤)

- **“誰がアクセスしているか”**を保証する階層
  “この人は本当に本人か怪しくないか？” を確認
- MFA / 条件付きアクセス / RBAC / PIM
- ゼロトラストの中心になるレイヤー
- **まずは“人”を守るレイヤー**

2. Network (ネットワークの保護)

- NSG（Network Security Group）
- Azure Firewall
- Private Link / Service Endpoint
- DDoS Protection
- **“入口”と“通り道”を守るレイヤー**
  “どこから入ってきてどこに行けるのか”のコントロール

3. Resource (Defender for Cloud:リソース保護)

- VM / Storage / SQL / Container など
- 脆弱性管理（CSPM）
- 脅威検知（Defenderプラン）
- 推奨事項による改善
- **“中身（リソースそのもの）”を守るレイヤー**

4. Monitoring (Sentinel:監視・分析)

- ログ収集（Log Analytics）
- SIEM / SOAR
- 自動化対応
- Copilot for Security への接続
- **“気づく・分析する・対応する”レイヤー**
  “何が起きたのか”“どこから攻撃されたのか” を可視化する

この4つのレイヤーは、全部が必要で、全部つながって動いています。

Azureセキュリティの全体像

基盤で絶対に必要

レイヤー	家に例えると	チェックするもの	具体的には
Identity	住民の本人確認 (鍵)	ユーザー本人か？ 権限は適切か？ 怪しいログインか？	・パスワード、MFA、FIDO、条件付きアクセス ・ロール(RBAC)で権限を決める ・特権を使う場合はPIMで一時的に管理者権限付与 ・サインイン異常の検知
Network	門・塀・通路	入ってくる経路と通る道を コントロール	・NSG：このVMはこのIPからのみアクセスOK ・Azure Firewall：外部への通信制限 ・Private Link：インターネット経由せずに安全につなぐ ・DDoS保護 ・VNetを分離してトラフィック制御
Resource	家の中のモノ	そのリソース自体に 問題がない？ 攻撃されていない？ 設定が危険じゃない？	・VMの脆弱性スキャン ・Storageの不審アクセス検知 ・SQLインジェクション警告 ・コンテナイメージの脆弱性 ・セキュリティスコア ・推奨設定（Security Benchmark）
Monitoring	防犯カメラ・警備会社	何が起きた？ どこから攻撃された？	・Sentinelでログを分析（SIEM） ・攻撃の流れを可視化 ・自動対応（SOAR） ・Copilotでアラート説明 ・SOC運用につなげる

分析・運用レイヤー

Defender for Cloudとは

- マルチクラウド統合セキュリティ管理

  Azure・AWS・GCP を一元的に可視化

- 脆弱性管理・保護・検知を一元化

  CSPM と Defender プランで包括的に防御

・設定ミス（Misconfiguration）を自動検出

・主要リソースの脆弱性を継続的にスキャン

・攻撃の兆候をリアルタイムに検知

・セキュリティスコアで状況を数値化

Azureセキュリティの全体像

基盤で絶対に必要

レイヤー	家に例えると	チェックするもの	具体的には
Identity	住民の本人確認 (鍵)	ユーザー本人か？ 権限は適切か？ 怪しいログインか？	・パスワード、MFA、FIDO、条件付きアクセス ・ロール(RBAC)で権限を決める ・特権を使う場合はPIMで一時的に管理者権限付与 ・サインイン異常の検知
Network	門・塀・通路	入ってくる経路と通る道を コントロール	・NSG：このVMはこのIPからのみアクセスOK ・Azure Firewall：外部への通信制限 ・Private Link：インターネット経由せずに安全につなぐ ・DDoS保護 ・VNetを分離してトラフィック制御
Resource	家の中のモノ	そのリソース自体に 問題がない？ 攻撃されていない？ 設定が危険じゃない？	・VMの脆弱性スキャン ・Storageの不審アクセス検知 ・SQLインジェクション警告 ・コンテナイメージの脆弱性 ・セキュリティスコア ・推奨設定（Security Benchmark）
Monitoring	防犯カメラ・警備会社	何が起きた？ どこから攻撃された？	・Sentinelでログを分析（SIEM） ・攻撃の流れを可視化 ・自動対応（SOAR） ・Copilotでアラート説明 ・SOC運用につなげる

分析・運用レイヤー

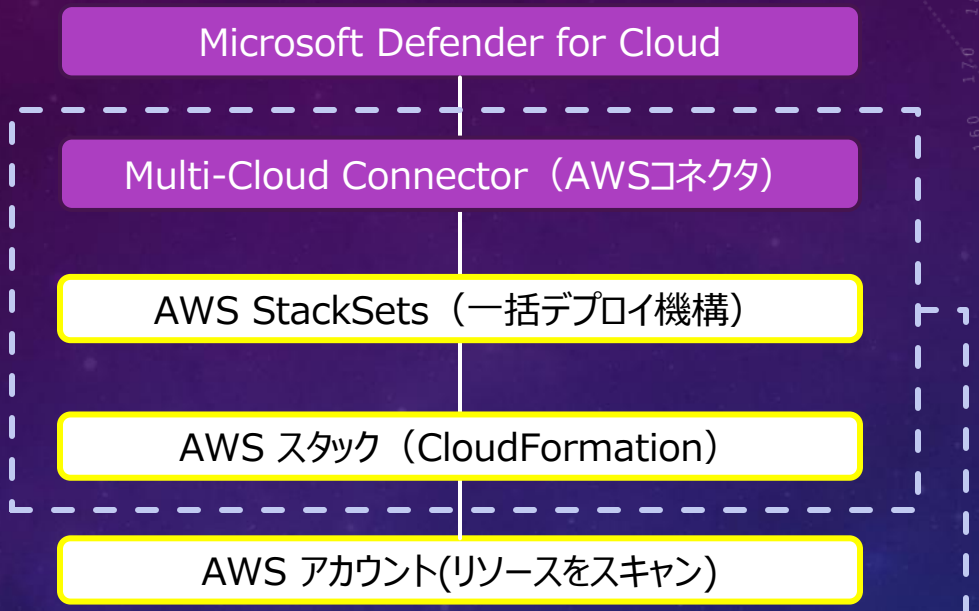
Azureセキュリティの全体像

基盤で絶対に必要

レイヤー	家に例えると	チェックするもの	具体的には
Identity	住民の本人確認 (鍵)	ユーザー本人か？ 権限は適切か？ 怪しいログインか？	Entra ID
Network	門・塀・通路	入ってくる経路と通る道を コントロール	NSG Firewall
Resource	家の中のモノ	そのリソース自体に 問題がない？ 攻撃されていない？ 設定が危険じゃない？	Defender for Cloud
Monitoring	防犯カメラ・警備会社	何が起きた？ どこから攻撃された？	Microsoft Sentinel Log Analytics

分析・運用レイヤー

Microsoft Defender for Cloud と AWS接続



Defender for Cloud が AWS とつながる仕組みは、
コネクタ → StackSets → CloudFormation
という順番で構成されます。

Azure から AWS に直接アクセスするのではなく、AWS 側に必要なロールや設定を CloudFormation で自動作成し、そのロールを通じて EC2 や S3 の状態を安全に読み取っています。

この仕組みによって、Azure から AWS のセキュリティ状況が統合的に可視化できるようになります。

運用シナリオ

ここからは Defender for Cloud を実際の運用でどう使うか をイメージします

- 脆弱性の自動検出：設定ミス・古いバージョン・危険な構成を自動で可視化

  Defender は VM や Storage、SQL など、それぞれのサービスにある設定ミスや、
  古くなったバージョン、危険な構成を自動でスキャンしてくれます。
  “どこを直せばいいか” が一覧で出てくるので、改善の優先順位が一気に分かります。

- 不審なアクセスの検知：異常な認証、攻撃の兆候、怪しいIPをリアルタイム通知

  例えば、普段来ない国から急にログインがあったり、権限のないリソースにアクセスしようとしたり、
  そういう“おかしい動き”をリアルタイムで拾ってくれます。
  Azure だけでなく、AWS 側の不審な動きも一元的に見えるのがポイントです。

- SQL攻撃の分析：パターンを特定し、影響範囲と改善策まで提示

  SQL インジェクションのような攻撃が来た場合、
  その内容や攻撃元、どのクエリが使われたか、どこまで影響した可能性があるか、
  というところまで解析してくれます。
  さらに “何をどう直せば次回防げるか” という改善ガイドも出てきます。

こういった仕組みによって、Defender for Cloud は
脆弱性の管理 → 攻撃の検知 → 改善
まで を全部1つのサービスで回せるようになっています

Sentinel連携

Microsoft Defender for Cloud

アラートを送信

Microsoft Sentinel

相関分析・インシデント化

Copilot for Security

要約・KQL生成・対応支援

このパートのまとめ

- 可視化（Security Posture）
- 検知（Defender for Cloud）
- 分析（Microsoft Sentinel）

セキュリティ運用の“最初の3ステップ”が完成

- Azure のセキュリティ運用は、**可視化** → **検知** → **分析** の3ステップが基本になります。
- Security Posture で現状を可視化して、
  Defender for Cloud が攻撃の兆候を検知して、
  Sentinel がそれらを相関分析してインシデントとしてまとめてくれる。
- ここまで来ると、クラウド全体のセキュリティ運用が一気に回り始めます。
- そして次のステップが、**Sentinel と Copilot を使った“高度なSOC運用”** です。
  攻撃の内容を自動で要約したり、調査クエリを生成したり、今まで手作業だった部分が大きく効率化されます。

資料ご利用にあたって

本資料は、本イベント参加者向けに作成されたものです。資料の著作権は ANLIMITRIA に帰属します。

■ 再配布について

本資料の **無断転載・複製・再配布** は原則禁止しています。
ただし、以下の目的に限り **日本マイクロソフト株式会社** に対して再配布を許可します。

- **日本マイクロソフト社内での共有**
- **本イベント参加者への「特典資料」としての配布**

上記以外の第三者への配布・公開は認められていません。

■ 許可される利用範囲

- 個人学習のための閲覧
- 社内での参照
- Azure / セキュリティ理解向上のための利用

■ 禁止事項

- SNS / ブログ / 外部サイト等への掲載
- スライド画像の投稿
- 本資料内容の改変・再編集版の外部配布

■ 免責事項

本資料はイベント時点の情報に基づき作成しています。

Azure / Microsoft Defender / Sentinel などの仕様は
随時更新されるため、挙動・機能を保証するものではありません。

本資料の利用に伴ういかなる損害についても、
ANLIMITRIA は責任を負いません。

■ お問い合わせ

ANLIMITRIA
代表：沓澤 繁臣
Web: https://anlimitria.com/