マイクロソフトの脅威インテリジェンスフィード

https://info.microsoft.com/rs/157-GQE-382/images/JA-JP-CNTNT-WhitePaper-Microsoft-Security-GEP-MECH.pdf

検出機能の向上:
明瞭なシグナルの重要性

大企業はより短い時間で攻撃を検出するために、矛盾するジレンマに取り組んでいます。つまり、処理するセキュリティ関連のデータが多すぎる一方で、ノイズからシグナルを選別して事象をすばやく理解するための情報は不十分、ということです。

ここでの課題は、単にボリュームが膨大であるというだけでなく、それらを選別する必要があるということです。多くの攻撃の兆候は、それ自体は無害に見えるか、業界、距離、時間フレームごとに分けられます。データセット全体に対する明確な洞察がないなら、早期に検出できるかどうかは運しだいになります。最も大きな企業であっても次のような限界に直面しています。

- 本当の脅威インテリジェンスには、大半の組織が独自で入手できるデータよりもさらに多くのデータが必要です。
- 大量のデータ プールの中からパターンを見つけて、よりスマートに処理するには、巨大な処理能力に加えて機械学習のような高度な技術が必要です。
- 最終的に、新しいインテリジェンスを適用してセキュリティ対策およびテクノロジを継続的に改善していくには、データが示す内容を理解し、アクションを実行できる専門家が必要です。

これこそ、Microsoft が流れを変えるために力を入れている分野です。プラットフォームおよびサービス企業として、Microsoft の脅威データおよびアクティビティ データは、テクノロジ チェーン、あらゆるバーティカル業界、世界中のすべてのポイントから寄せられたものです。

Microsoft のセキュリティ製品とクラウド テクノロジは、問題が発生したときに、連携して悪意のある脅威データを報告するように設計されています。これは "フライト データ レコーダー" として機能し、攻撃の診断、高度な脅威技術のリバース エンジニアリング、プラットフォーム全体でのインテリジェンスの適用を可能にします。

数十億の「データポイント」

Microsoftのサービス	Microsoftのデータ
Web スキャン	Windows Defender

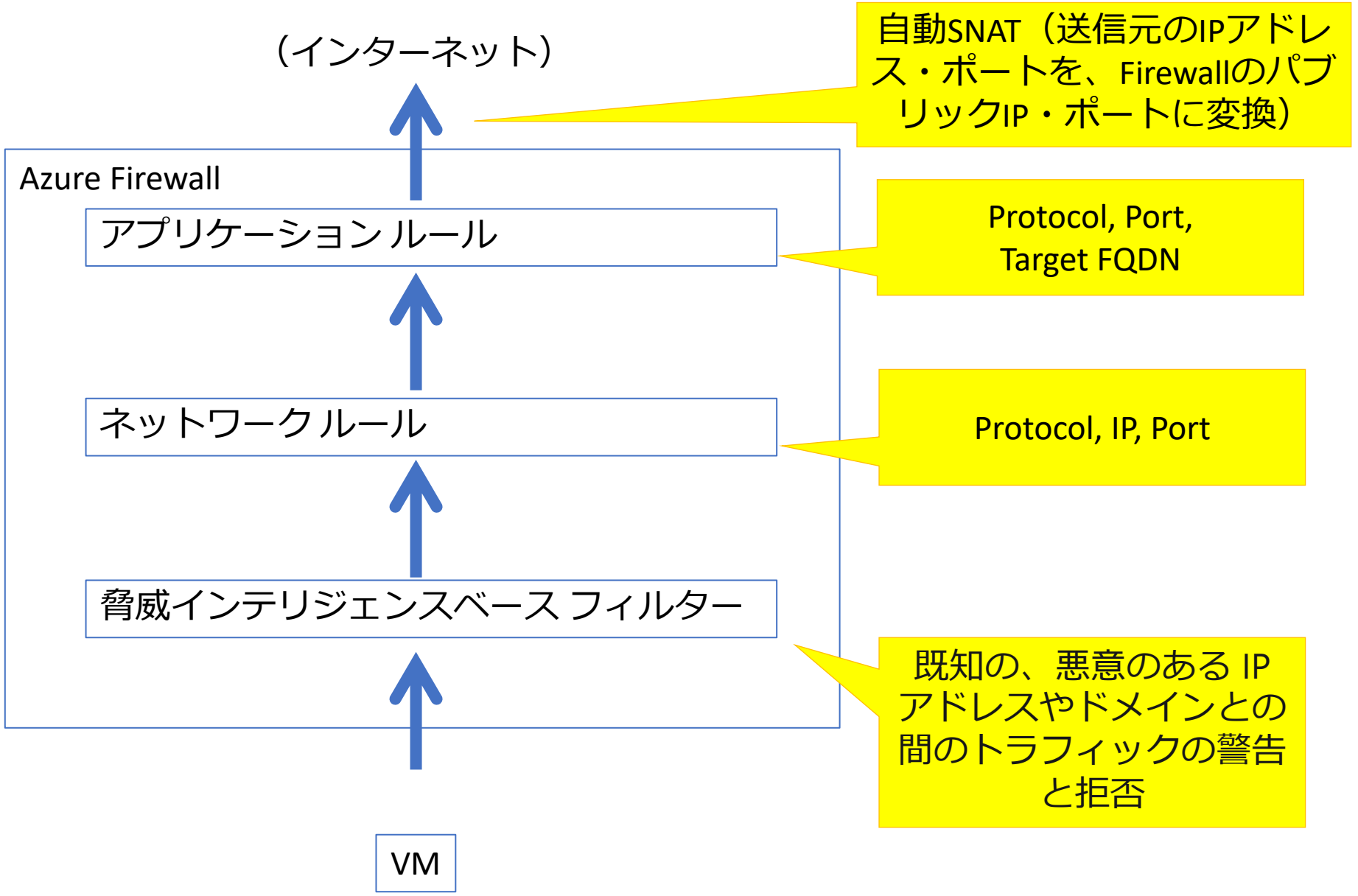
↓ 分析

脅威インテリジェンスフィード

↓ 情報提供

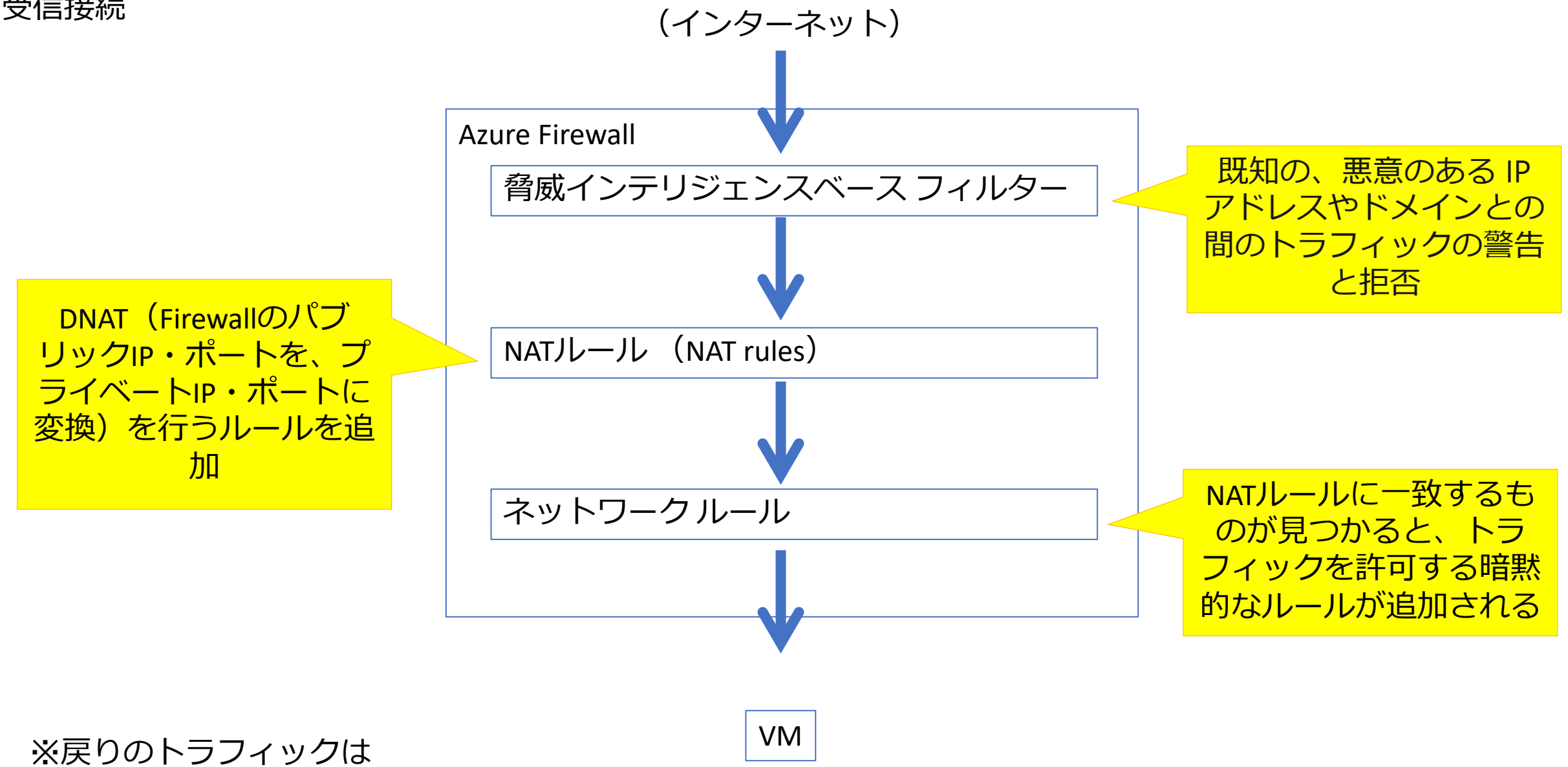
Azure Firewall などのサービス

送信接続



※戻りのトラフィックは
ステートフルで許可される

受信接続



※戻りのトラフィックは
ステートフルで許可される