

NETSCOUT.

DDoS対策ソリューション

NETSCOUT Systems

なぜ今DDoS対策なのか？

DDoS攻撃は事業者の通信に悪影響（サービス停止等）を及ぼします

- ✓ 通信不可 : DDoS攻撃はネットワークを劣化させ、サービスが全く提供出来ない状況が発生させる
- ✓ 身代金 : ランサム DDoS 攻撃では、企業機密情報(の破壊・流出)に対して身代金を要求する
- ✓ イメージ低下 : 攻撃された事実は、ニュースやSNSで世界に拡散され、企業イメージを低下させる

DDoS攻撃は年々増加し、巧妙化し、進化しております

- ✓ DDoSの進化 : 難しくなる検知（DDoS攻撃手法の組合せ、短期攻撃、非ボリューム攻撃）
- ✓ 自分が加害者 : 自社網に感染したデバイスから他社攻撃（アウトバウンド攻撃）
- ✓ 身代金要求 : 脅迫型DDoS攻撃の台頭（エクステーション型攻撃）

対策の不備は甚大なる影響を及ぼす

- ✓ 2023年5月 : 国内自動車向けサービス提供企業が、215万件の顧客データ流出の可能性
- ✓ 2022年6月 : グーグルに毎秒4600万件の要求が発生させ、グーグルのインフラを停止させた
- ✓ 2020年2月 : AWSに最大 2.3 TB/秒（過去最大）の攻撃を送付



DDoSグローバルトレンド

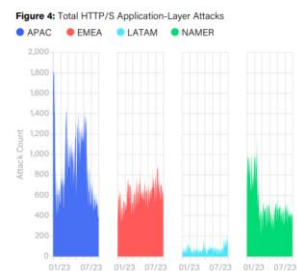
2023年上半期

- 増加傾向のDDoS攻撃
 - 790万件のDDoS攻撃総数（前年比 31%増）
 - ウクライナやサミット、オリンピックなどのイベントで上昇
- 非ボリューム型攻撃増加
 - 絨毯爆撃、DNS水責め攻撃の増加
 - 難解な検知：プロトコル併用、小規模大量、短期型
- 内部デバイスの感染による脅威の深刻化
 - 多額の身代金要求

<https://horizon.netscout.com>



HTTP/S Application-Layer Attacks



DNS Amplification Attacks

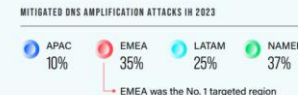
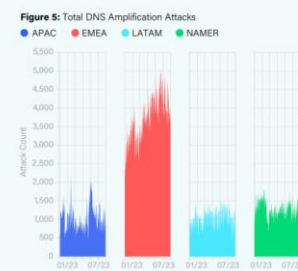
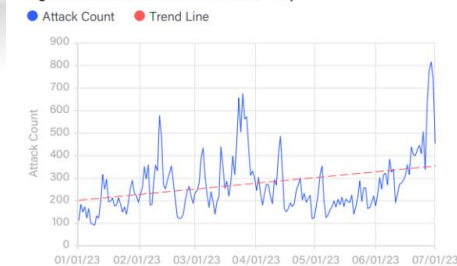


Figure 17: DNS Water-Torture Attacks Per Day

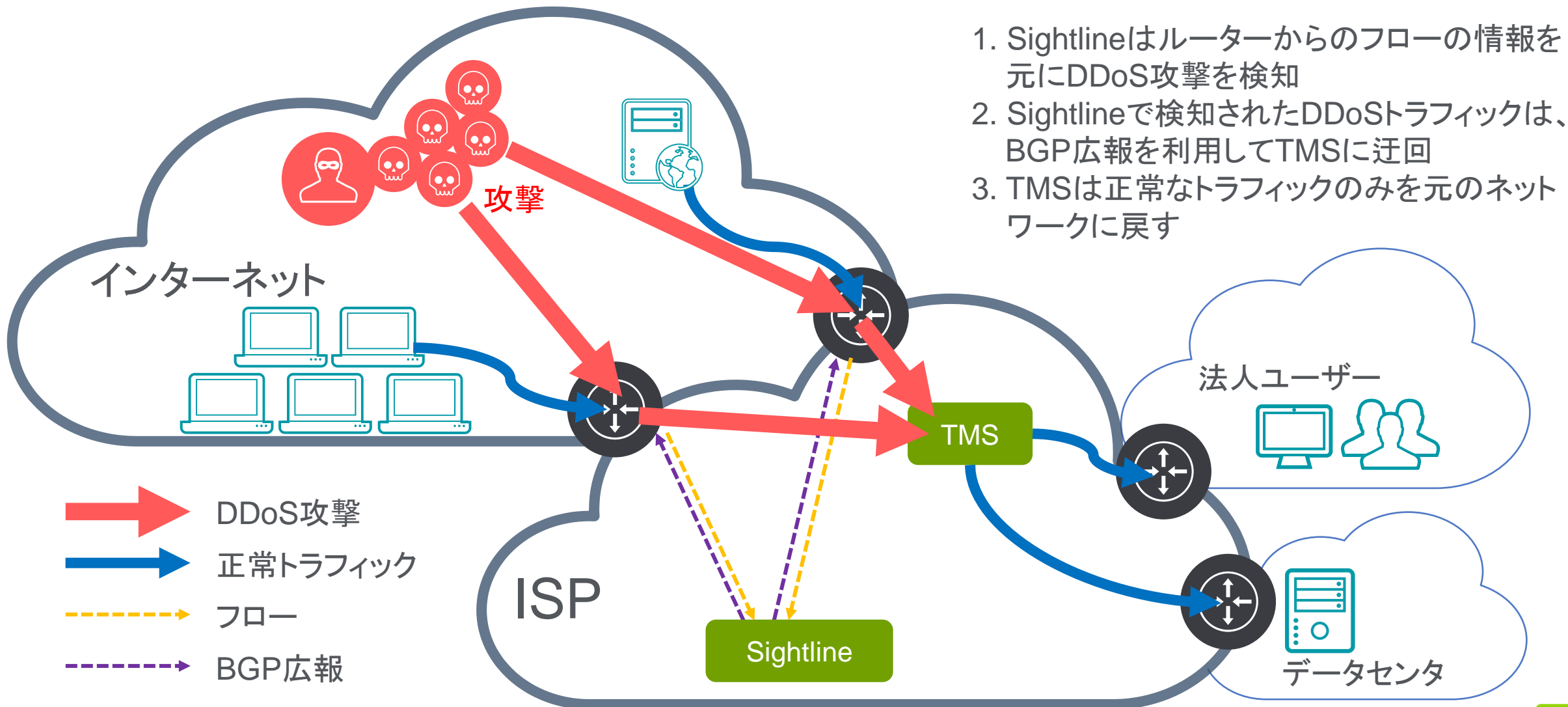


NETSCOUT DDoS対策ソリューション

- 従来の(ボリウム型)DDoS攻撃から強かにネットワークを守るソリューション
- Netflowでは検知の難しい、非ボリウム型攻撃の検知・緩和
- 内部デバイスの感染を可視化して、自社トラフィックや機密情報を保護



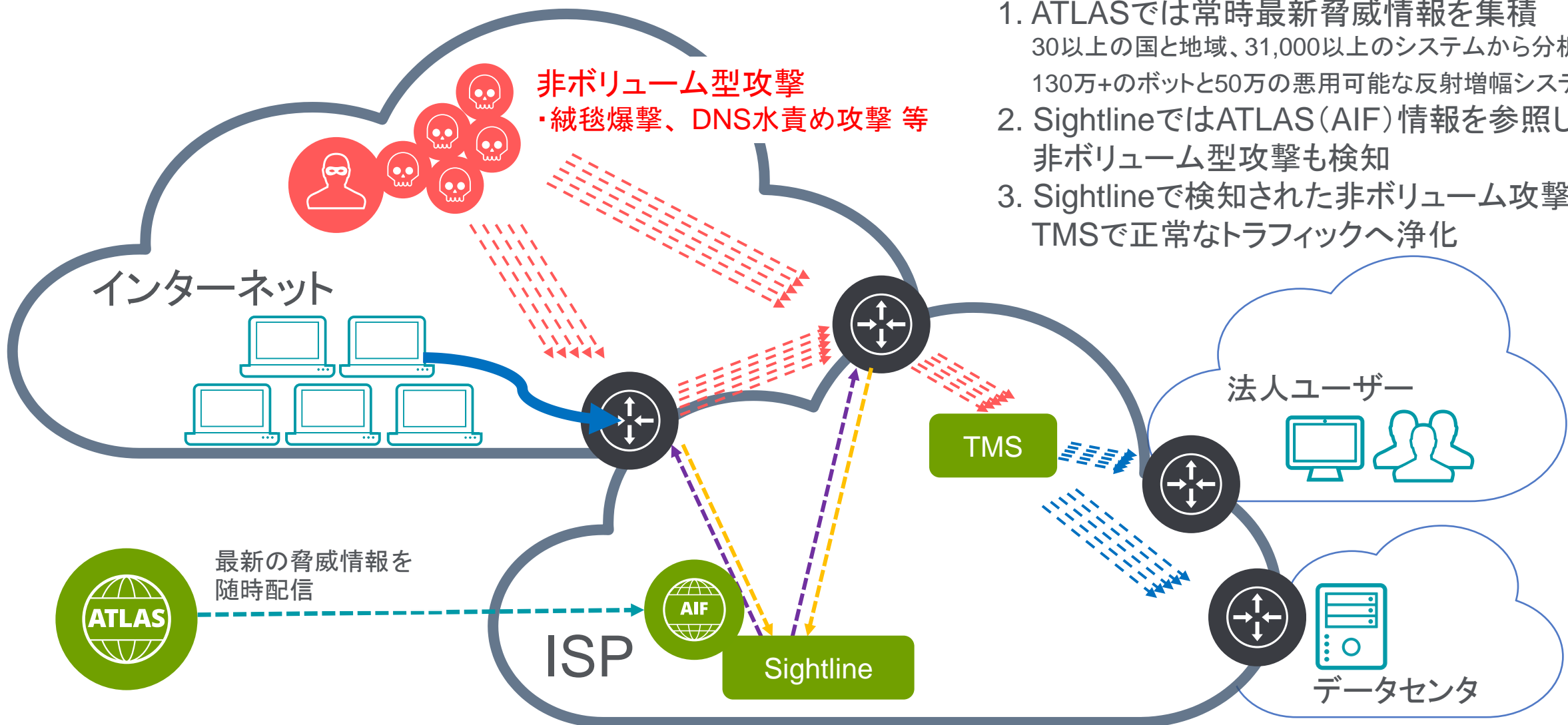
DDoS攻撃から強かにネットワークを守る Sightline/TMSによる本格的なDDoS対策



1. Sightlineはルーターからのフローの情報を元にDDoS攻撃を検知
2. Sightlineで検知されたDDoSトラフィックは、BGP広報を利用してTMSに迂回
3. TMSは正常なトラフィックのみを元のネットワークに戻す



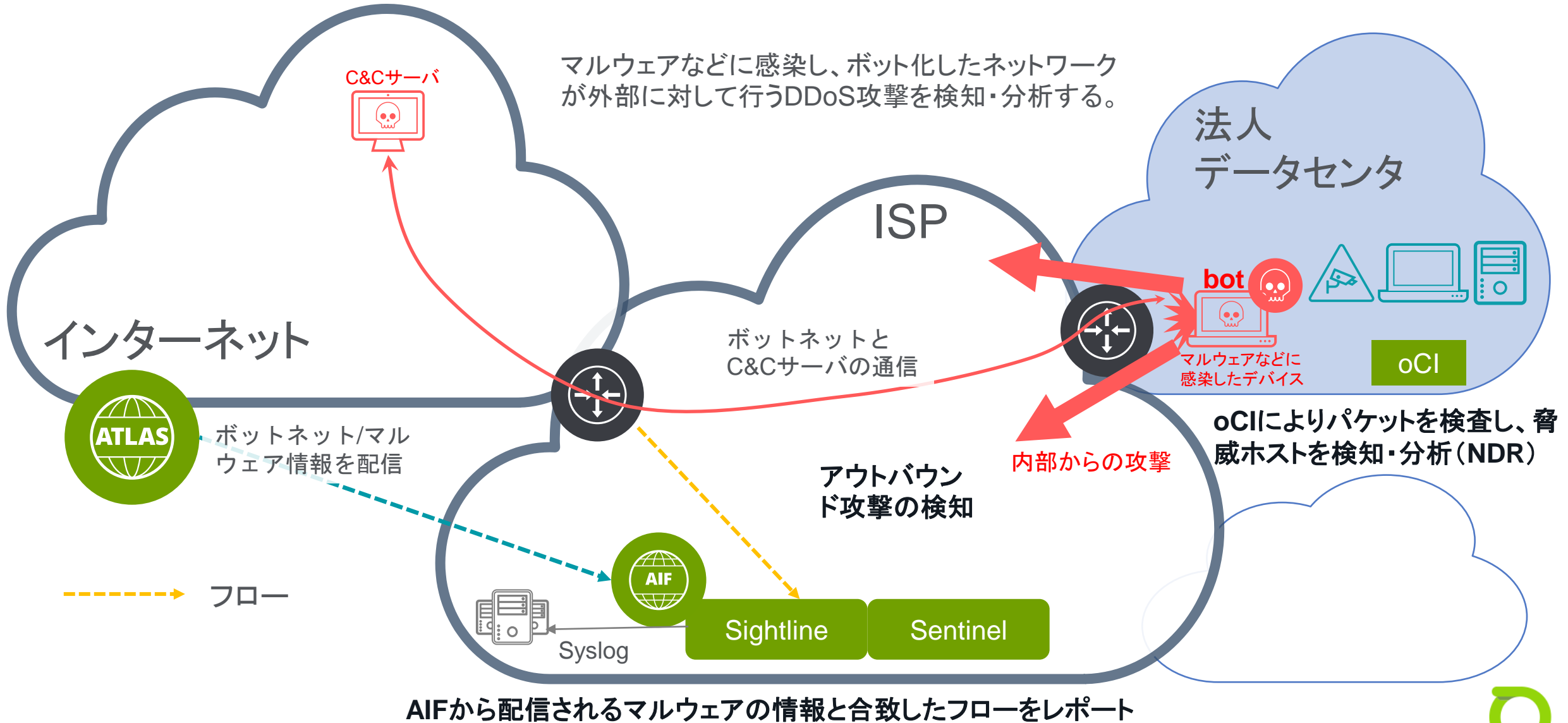
Netflowでは検知の難しい、非ボリューム型攻撃の検知・緩和 AIF (ATLAS Intelligent Feed)



1. ATLASでは常時最新脅威情報を集積
30以上の国と地域、31,000以上のシステムから分析
130万+のボットと50万の悪用可能な反射増幅システム
2. SightlineではATLAS (AIF) 情報を参照し
非ボリューム型攻撃も検知
3. Sightlineで検知された非ボリューム攻撃は
TMSで正常なトラフィックへ浄化



内部デバイスの感染を可視化して、自社トラフィックや機密情報を保護 oCI (Omnis Cyber Investigator)



Sightline/TMSによるDDoS防御のアドバンテージ

- NETSCOUTだけでDDoSの可視化/脅威検知から防御までソリューションを提供
- 全世界のISP/MSSP様や多くのグローバル企業様で採用
- DDoS攻撃で想定される帯域のみを考慮したソリューションの設計により高い費用対効果を実現
- マルチテナントのサポートにより、エンドユーザーごとに異なる設定やレポート画面を作成可能



NETSCOUT®

Guardians of the Connected World

本資料の内容のご興味のある方は、ぜひこちらまでご連絡ください。

メールアドレス : japan-sp@netscout.com