

# DNSインフラの保護 と DNSを利用した セキュリティサービス

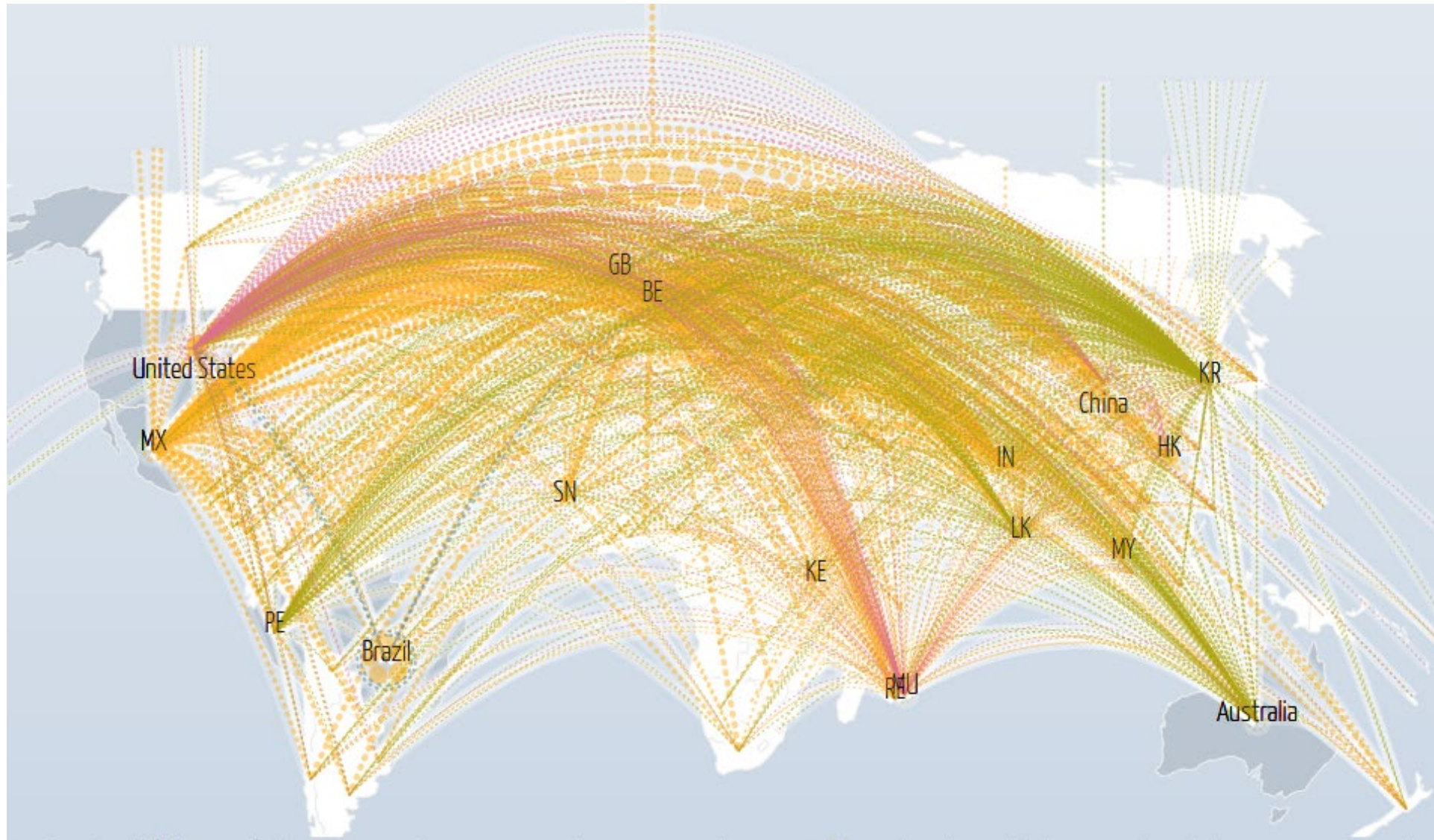
# アジェンダ

---

- DNS への攻撃
- DNS インフラの保護
- DNS を利用したクリーンパイプの実現
- Allot のソリューション

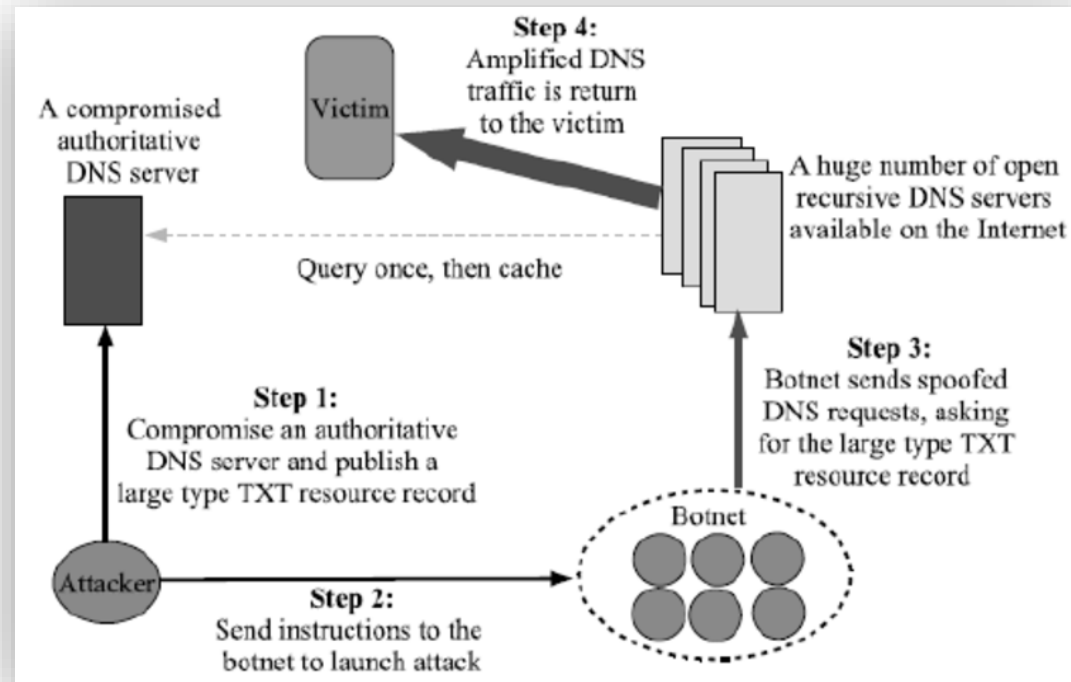
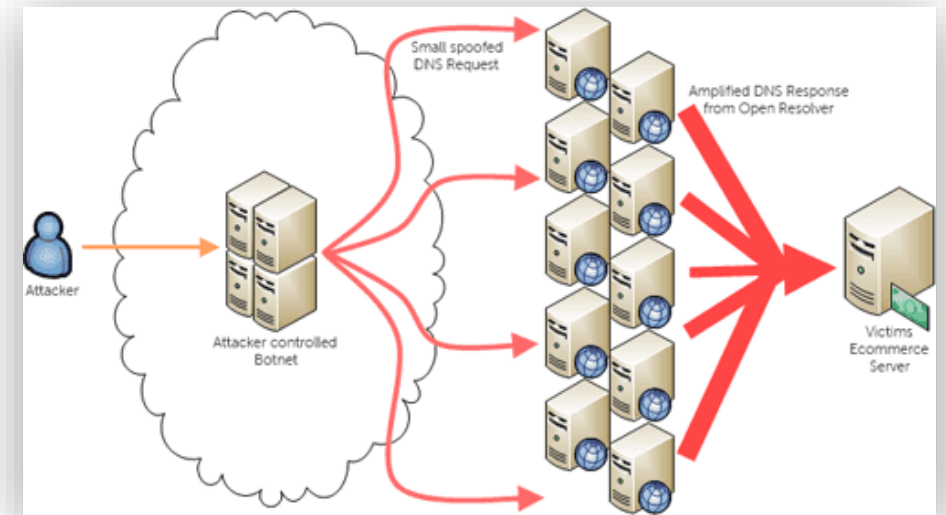


# DDoS 攻撃 – 常態化

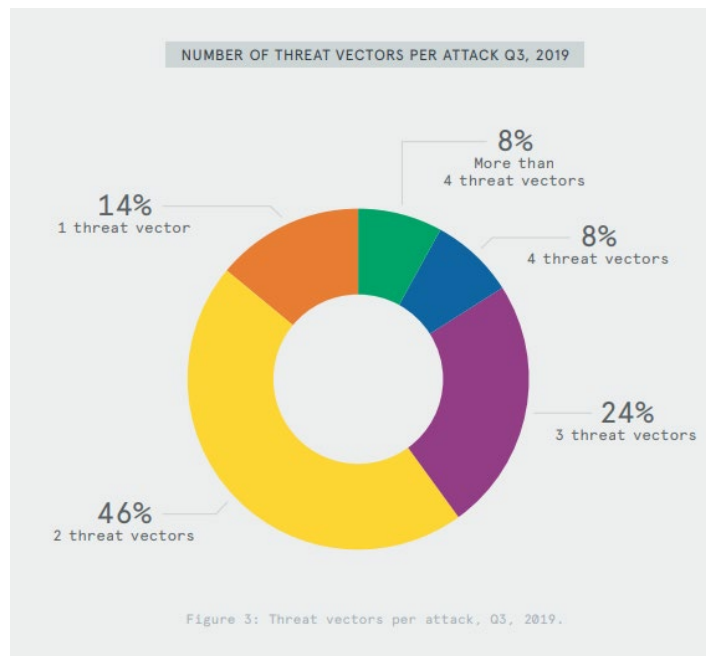
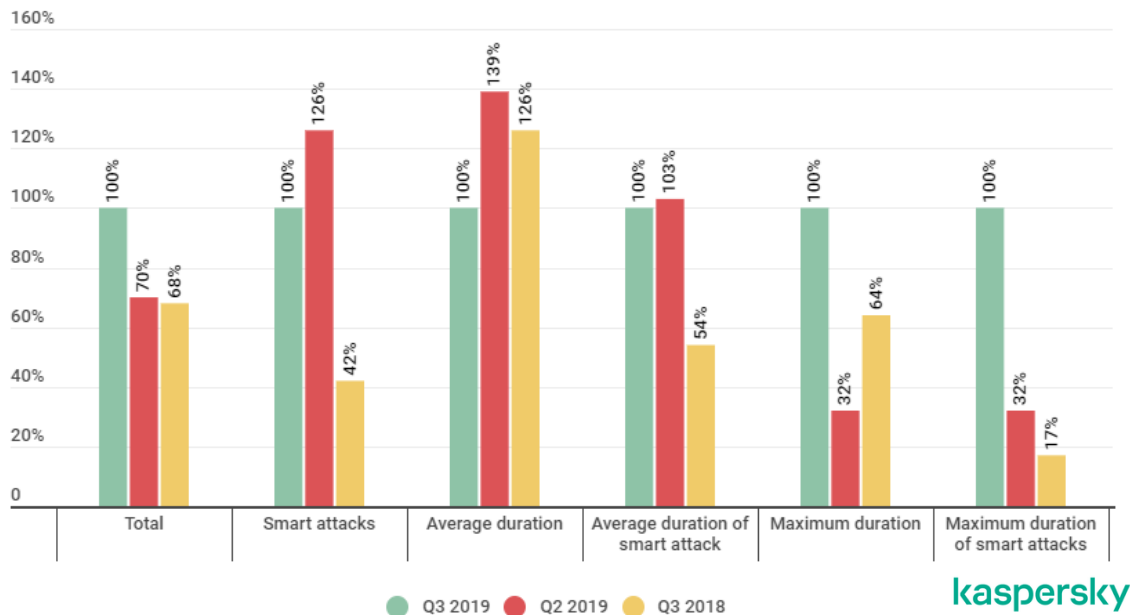


# DNSインフラへの攻撃

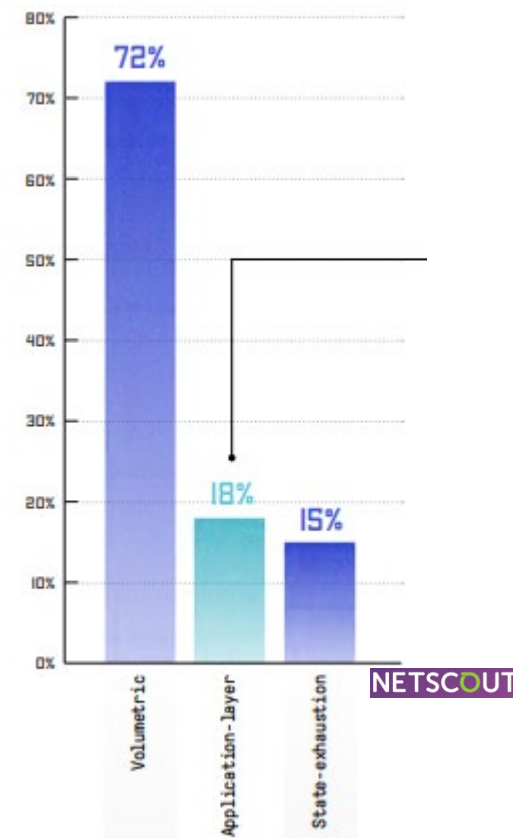
- DNSはどの事業者においても最もクリティカルなインフラの一つですが近年DNSサービスを狙った攻撃が増加しています
- DNSサービスに影響を与えるような攻撃には以下のように多くのタイプが存在します
  - ドメイン名ハイジャック
  - DNS フラッド攻撃
  - DoS リフレクション攻撃 (DRDoS)
  - DNS キャッシュポイズニング
  - DNS トンネリング
  - DNS ハイジャック
  - ランダムサブドメイン攻撃
  - UDP フラッド
  - TCP SYN



# DDoS 攻撃のトレンド



## TYPES OF DDoS ATTACKS (CSPs)



DNSサーバの半数以上が攻撃を受けている

攻撃の複雑化

平均的な攻撃の約40%が短時間による攻撃の一方で半数は過去最大の攻撃を経験

サービス・プロバイダへの攻撃は量的な攻撃が圧倒的多数を占める

# アジェンダ

---

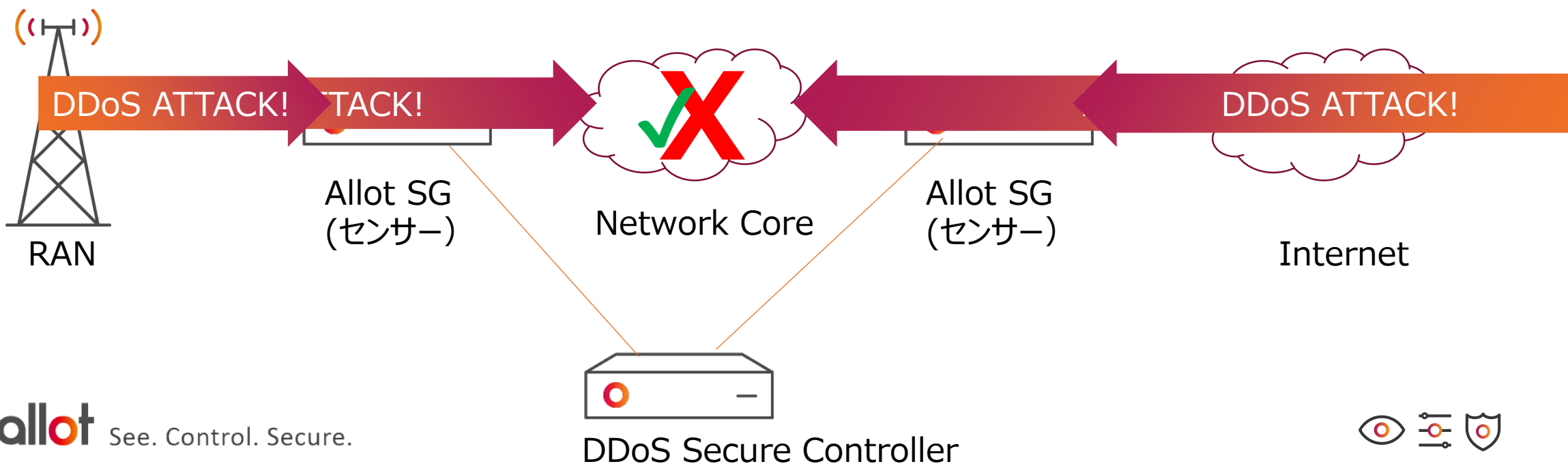
- DNS への攻撃
- DNS インフラの保護
- DNS を利用したクリーンパイプの実現
- Allot のソリューション



# AllotによるDDoS対策 (DDoS Secure)

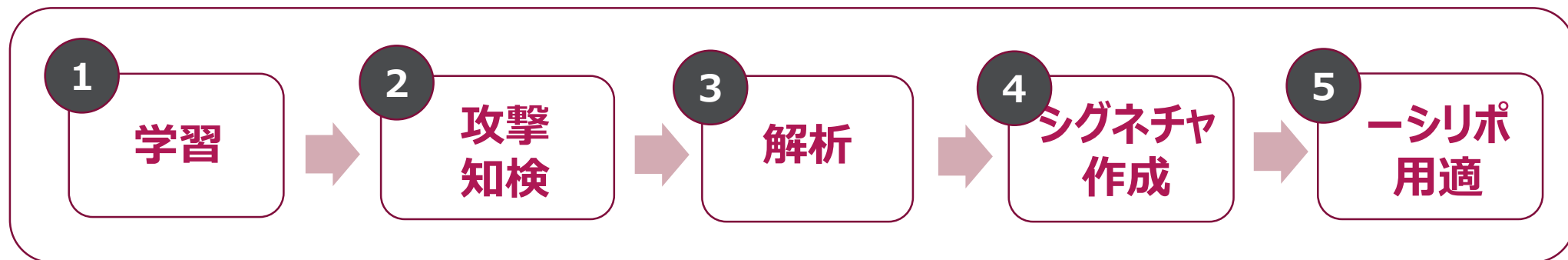
## 主な特徴

- インターネットからの攻撃だけでなく、Bot化した場合の内部から外部への攻撃にも対応
- 5Gにも対応
- フルIPv6 対応
- 短時間攻撃、スロー攻撃にも対応
- DPIエンジンを搭載しているため、攻撃を受けている間もQoS処理により重要なトラフィックをブロックせずに攻撃トラフィックだけをブロックすることが可能

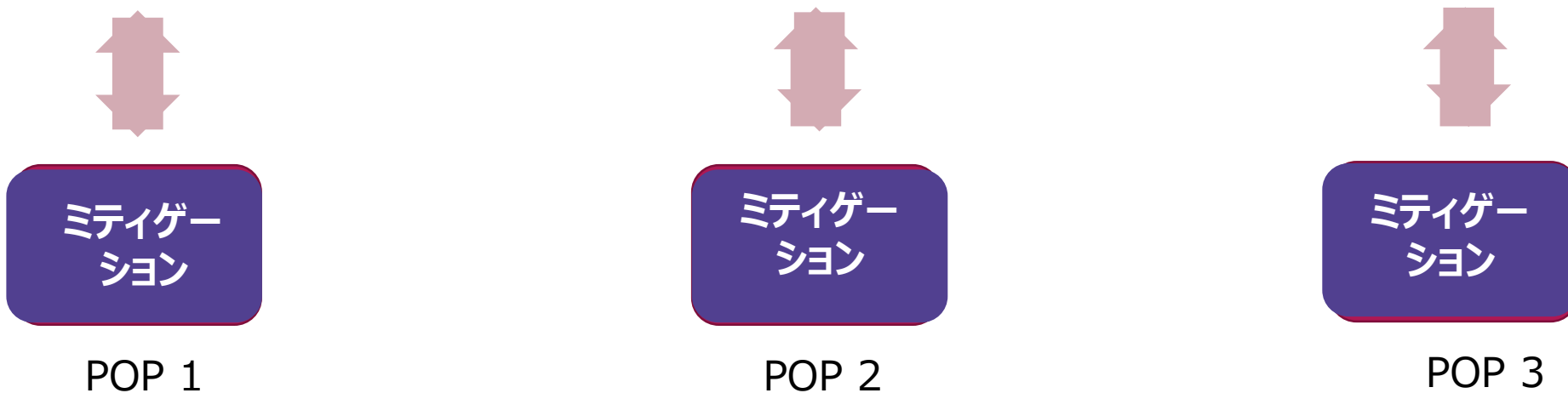


# DDoS SecureによるDDoS攻撃のミティゲーション

AllotのDDoS Secureによる攻撃を検知してからのミティゲーションまでのフロー



パケット収集

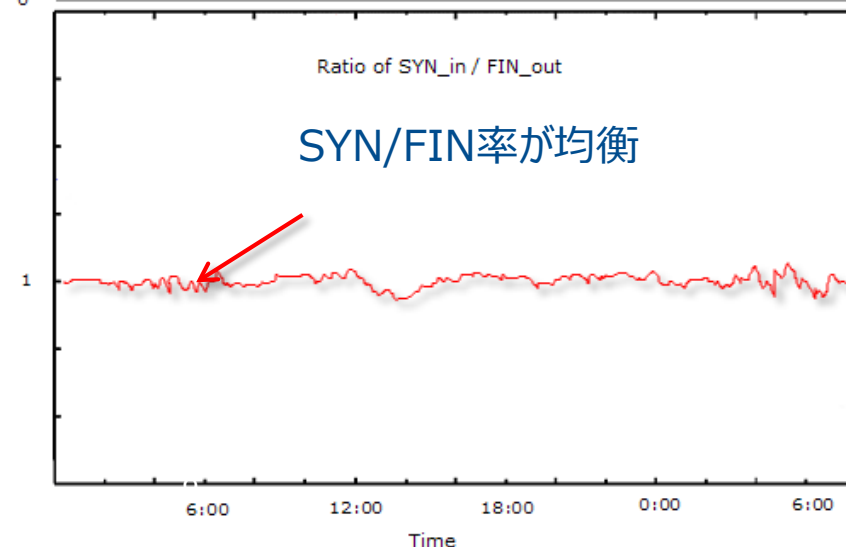
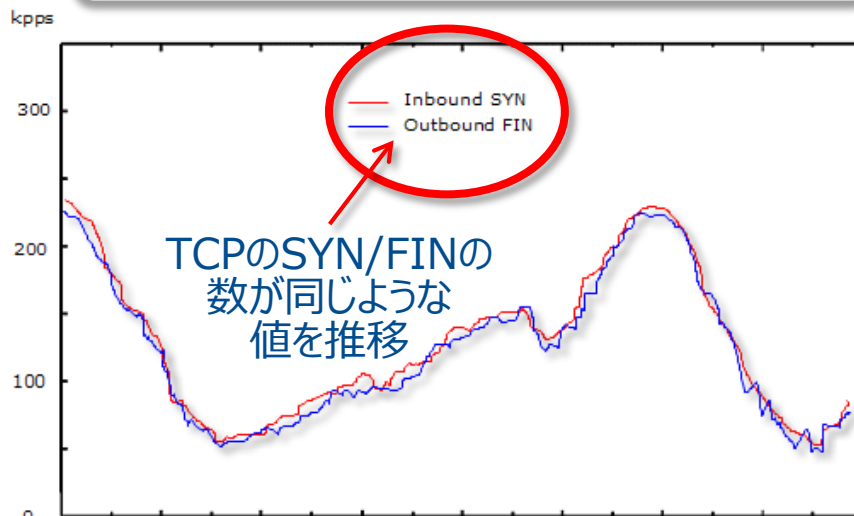




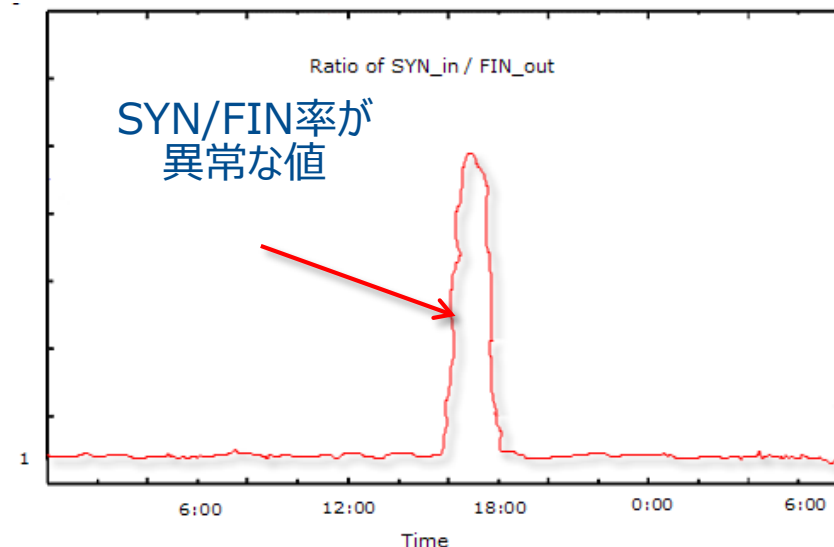
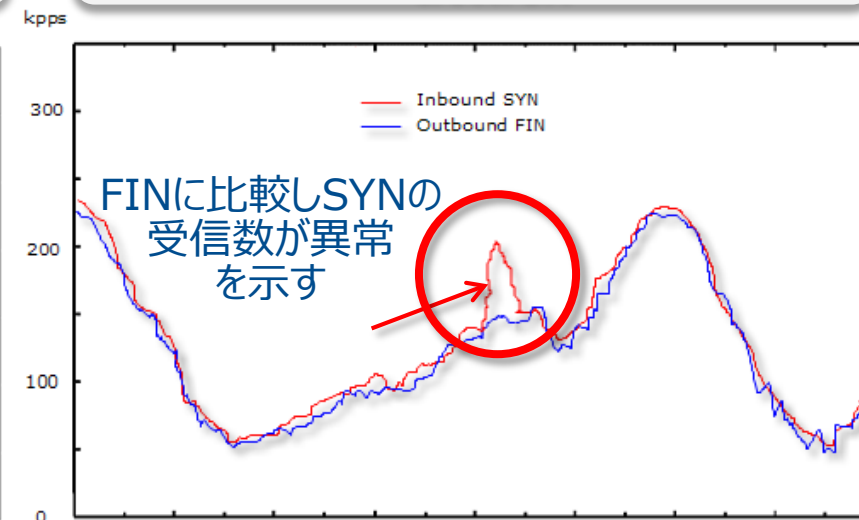
# 攻撃トラフィック検知の仕組み（一部抜粋）

- 機械学習AIによる攻撃検知及びミティゲーションが可能
- 通常トラフィックの自動学習
- 学習した通常トラフィックと機械学習AIによる直前トラフィックの予測と比較し逸脱したトラフィックの検知

通常の振る舞い



TCP信号率の異常 = DDoS attack



# アジェンダ

---

- DNS への攻撃
- DNS インフラの保護
- DNS を利用したクリーンパイプの実現
- Allot のフルセキュリティソリューション



## 全てのプラットフォームを 統一された顧客中心のエクスペリエンスで提供



### HomeSecure/ BusinessSecure

CPEベースのセキュリティ

- スマートホーム、オフィスでのIoTを含むすべてのデバイスを保護
- ホームルータの保護
- ホーム/オフィスネットワークの完全な可視化

### IoTSecure

ネットワークベースのIoTセキュリティ

- マルウェア、ボットネット及びDDoS攻撃からの保護
- ふるまい保証

### EndpointSecure

APPベース(デバイスにインストール)のセキュリティ

- オフネット時の保護
- サードパーティクライアントとの統合ソリューション

### NetworkSecure

モバイルコンシューマ及びSMB向けプレミアムデータパスネットワークベースのセキュリティ

- 脅威プロテクション及びペアレンタルコントロール
- スムーズな導入が可能
- 50%に及ぶの普及率
- 大規模アクティベーション可能
- カスタマーエンゲージメント

### DNS Secure

コンシューマ及びSMB向けのネットワークベースのセキュリティ

- 脅威プロテクション及びペアレンタルコントロール
- スムーズな導入が可能
- 50%に及ぶの普及率
- 大規模アクティベーション可能

# CSPにおける DNS Secure の価値

---

- AllotのNetworkSecure は多くのCSP様において非常に高い加入率 (30-50%) を獲得し、多額の収益をもたらし、結果ARPUが3~5%の向上が見られています。
- 加えてブランド力の向上、NPS値が30%を超え、解約率の低下にも貢献し、他CSPとは安全性という面で差別化に成功しています。
- 加入者には安心を提供し、インターネット使用の増加に繋がっています。
- AllotのDNS Secureは実績のあるNetworkSecureと同じ機能をDNSサーバを利用して実現します！

# DNS Secureの機能

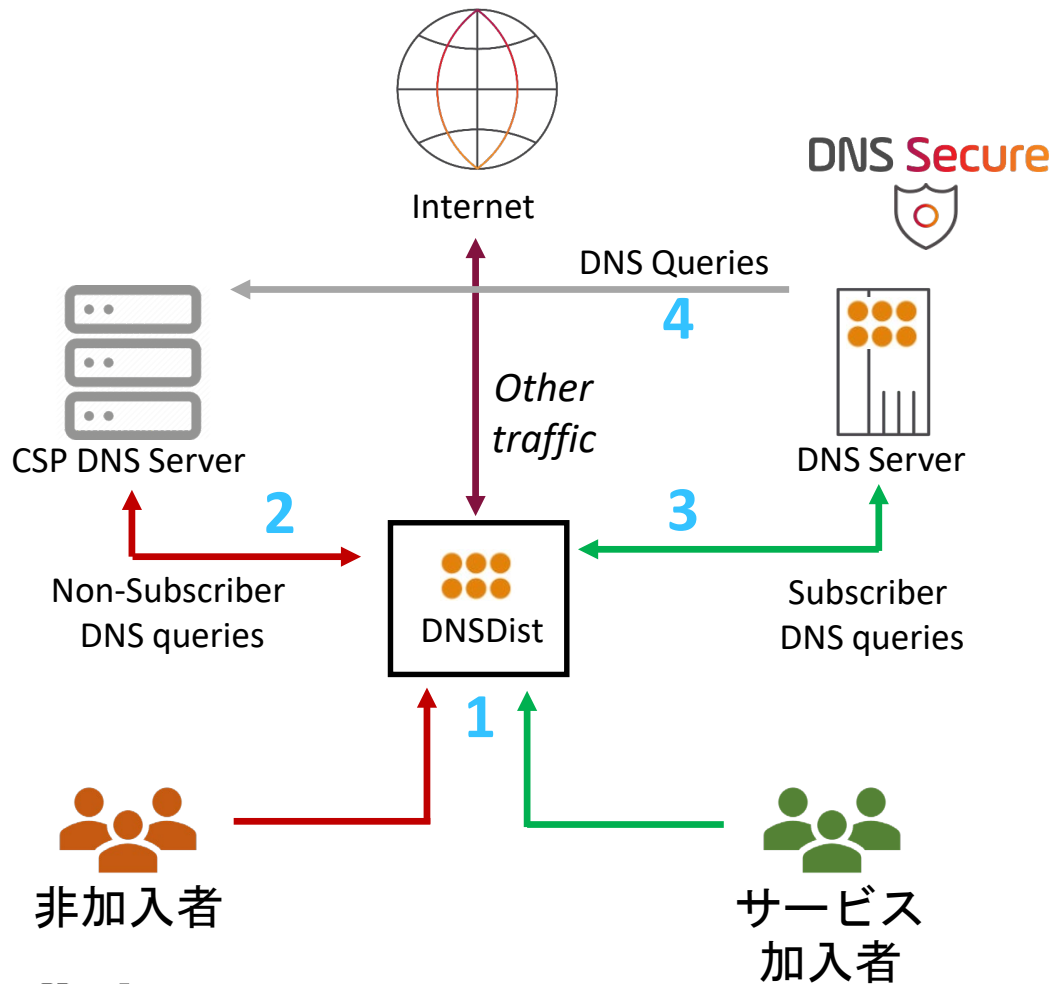
---

- **脅威からの保護** – マルウェア対策、フィッシング対策、ボットネット、およびアドウェアから保護します。既に2300万ユーザを超えるAllot Network Secureで実証済みのThreat Databaseを使用します。
- **ペアレンタルコントロール** – カテゴリに分けられたURLフィルタリングを提供
- **導入が容易** – シームレス、ゼロタッチ、クライアントアプリケーションが不要など導入における障壁がないため、ユーザには容易に利用開始していただくことが可能です。
- **拡張性及び高いパフォーマンス**
- **マルチテナント** – ユーザ自身で、スレットタイプやURLカテゴリを設定することが可能、また個人へのレポートが充実しているため守られてる感を実感することが可能です。

# DNS Secureの設置タイプ

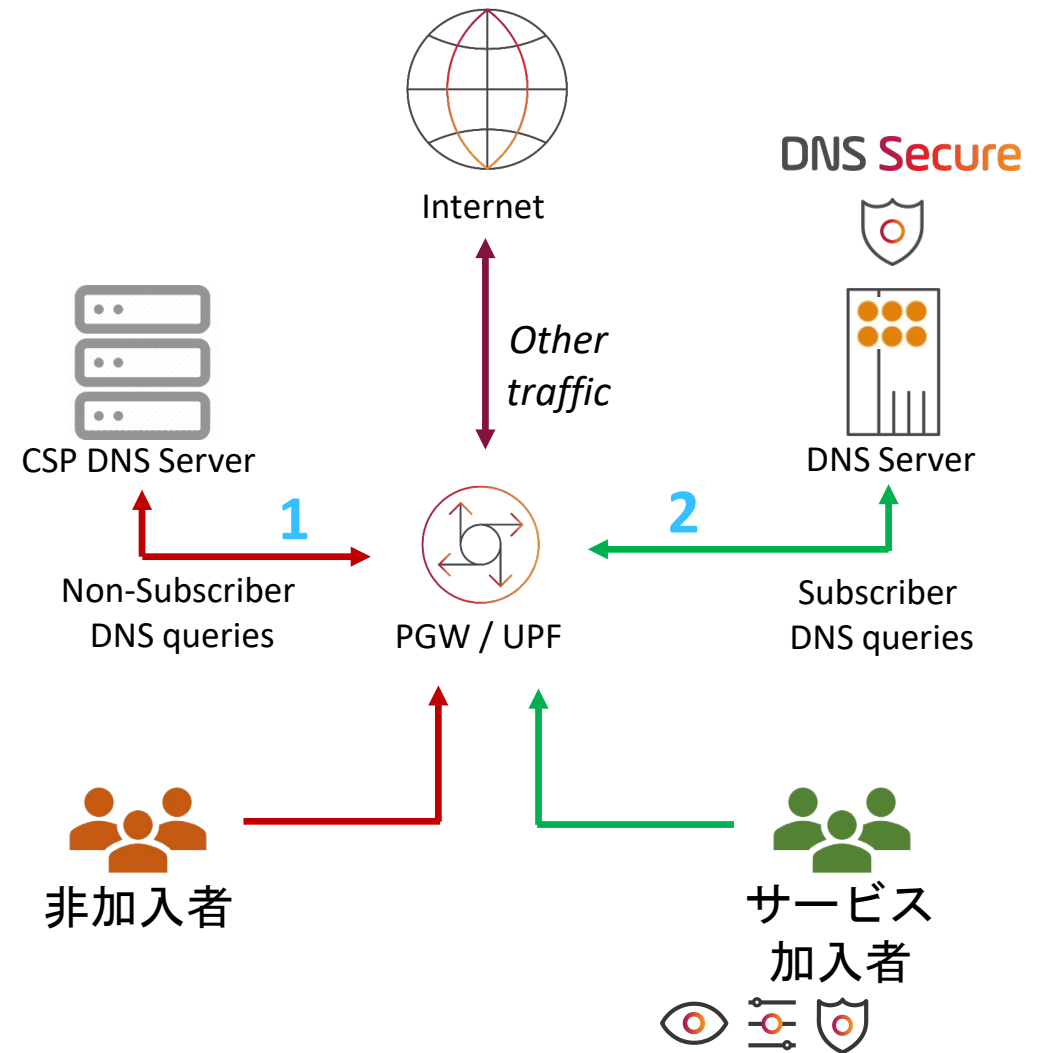
## Option 1: ステアリング

DNS Distによるサービス加入者・非加入者の判別



## Option 2: DNS設定

DNS設定によるサービス加入者・非加入者の判別



# アジェンダ

---

- DNS への攻撃
- DNS インフラの保護
- DNS を利用したクリーンパイプの実現
- Allot のフルセキュリティソリューション



## 全てのプラットフォームを 統一された顧客中心のエクスペリエンスで提供



### HomeSecure/ BusinessSecure

CPEベースのセキュリティ

- スマートホーム、オフィスでのIoTを含むすべてのデバイスを保護
- ホームルータの保護
- ホーム/オフィスネットワークの完全な可視化

### IoTSecure

ネットワークベースのIoTセキュリティ

- マルウェア、ボットネット及びDDoS攻撃からの保護
- ふるまい保証

### EndpointSecure

APPベース(デバイスにインストール)のセキュリティ

- オフネット時の保護
- サードパーティクライアントとの統合ソリューション

### NetworkSecure

モバイルコンシューマ及びSMB向けプレミアムデータパスネットワークベースのセキュリティ

- 脅威プロテクション及びペアレンタルコントロール
- スムーズな導入が可能
- 50%に及ぶの普及率
- 大規模アクティベーション可能
- カスタマーエンゲージメント

### DNS Secure

コンシューマ及びSMB向けのネットワークベースのセキュリティ

- 脅威プロテクション及びペアレンタルコントロール
- スムーズな導入が可能
- 50%に及ぶの普及率
- 大規模アクティベーション可能



Thank  
You!