非ボリューム型DDoSは
どこまでネットワークで守れるか？

GMOインターネット株式会社
システム本部 IaaSチーム
木佐木皓平

自己紹介

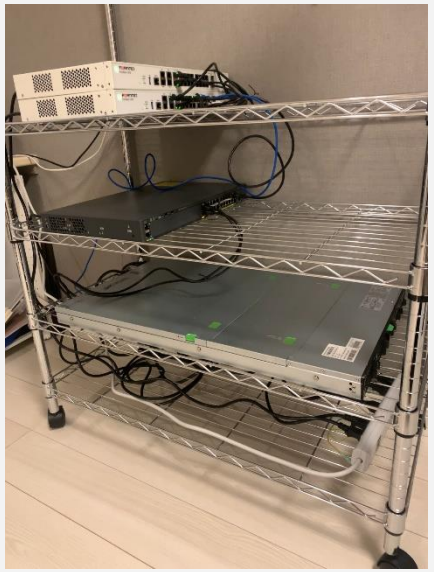
ささき　こうへい
木佐木　皓平

GMOインターネット株式会社
システム本部 IaaSチーム

■略歴
2025年　GMOインターネット 新卒入社

■担当業務
新規・既存商材のネットワーク運用・構築

■趣味
音ゲー、筋トレ



アジェンダ

1. 非ボリューム型DDoSとは
2. GMOの非ボリューム型DDoSへの対策と課題
3. L3/L4で非ボリューム型攻撃を防ぐ仕組みの考案
4. PoCの結果と課題
5. まとめと議論ポイント

非ボリューム型DDoSとは

CISAはDDoSを3つに分類している

ボリューム型攻撃

目的：回線帯域の飽和

手段：数十～数百Gbps級の大規模トラフィックを一気に流し込む

手法：UDP Flood, DNS/NTP Amp攻撃など

プロトコル型攻撃

目的：接続テーブルの枯渇

手段：TCPハンドシェイクやステート管理の隙を突き、未完了接続を大量に作って接続テーブルを埋める

手法：SYN/ACK Floodなど

アプリ層攻撃

目的：サーバープロセスの消耗

手段：HTTPリクエストを大量・低速に送りつけ、サーバのCPUやスレッドを占有する

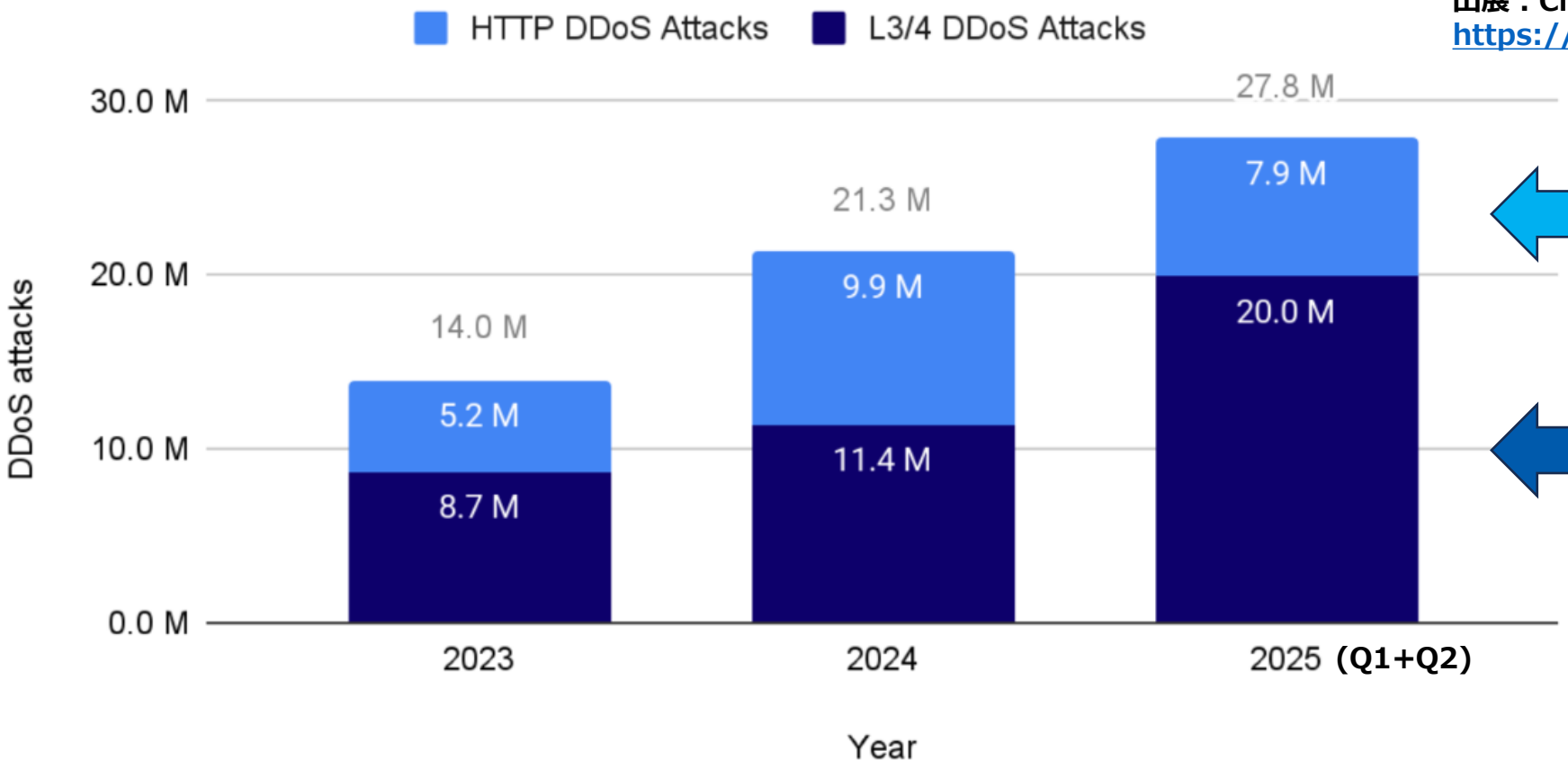
手法：HTTP Flood/Slowlorisなど

非ボリューム型DDoS

大まかな定義：1Gbps未満

近年のDDoSの傾向

出展：Cloudflare Radar
https://radar.cloudflare.com/reports/ddos-2025-q2



アプリ層攻撃

ボリューム型攻撃
プロトコル型攻撃

アプリ層攻撃
(HTTP DDoS Attack)の
増加が著しい

非ボリューム型攻撃への対策も
強化していかなければならない

ネットワーク側の対策状況

ボリューム型攻撃

○

オンプレ/クラウド型ソリューション導入済み

プロトコル型攻撃

△

ソリューション導入済み
一部攻撃はすり抜けて
サーバーまで届いてしまっている

アプリ層攻撃

×

サーバーチームに一任

ボリューム型攻撃への対策に注力してきた
・サービスの正規トラフィック増加
・Tbps級の大規模なDDoSの出現

非ボリューム型攻撃への
防御は完全ではない

防御策の検討①　L7WAF導入

社内サイトには導入済みだが…
お客様環境への導入は難しい

莫大な管理コスト

L7WAFはホスト単位での防御が基本

↓

膨大な数のお客様ドメインのSSL証明書を
WAFに登録し更新し続ける必要がある

お客様側の改修負担

L7WAFを経由すると接続元IPが変化する

↓

接続元IPでアクセス制限しているお客様は
別途接続元判定の設定を行う必要がある

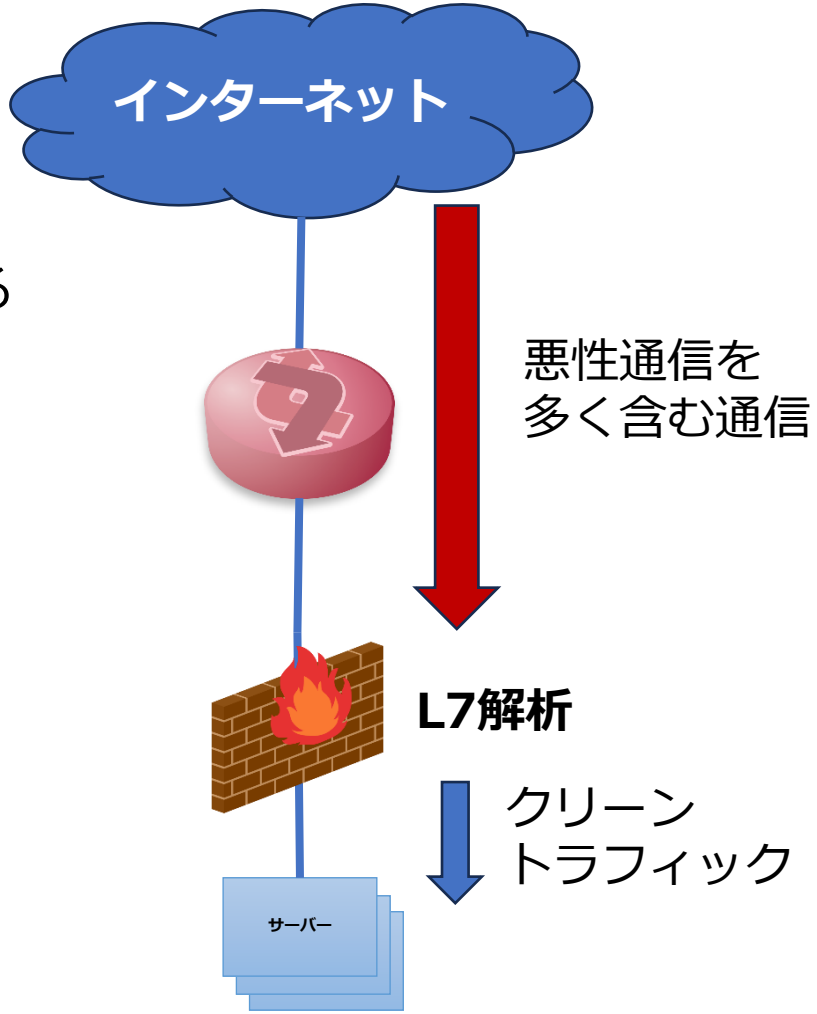
防御策の検討②　インライン型L7DDoS対策装置

L3/L4装置と比べて帯域当たりのコストが数倍

L7解析+判定、TLS終端をリアルタイムで行う必要があるため、
同じ帯域でも L3/L4 装置と比べて帯域あたりのコストが数倍になる

弊社のトラフィック規模(数十Gbps以上)に導入する場合、年間コストが実際の攻撃頻度・影響度と釣り合わない

費用対効果の観点で導入に不安



非ボリューム型攻撃を「ほどほどに」防ぎたい

現状のお客様環境防御：スクリプト+手動ブロック

↓

対応工数がかかる（年に十数回アラート）
新旧のサービスが混在しており、**防御体制が不十分なサービスもある**

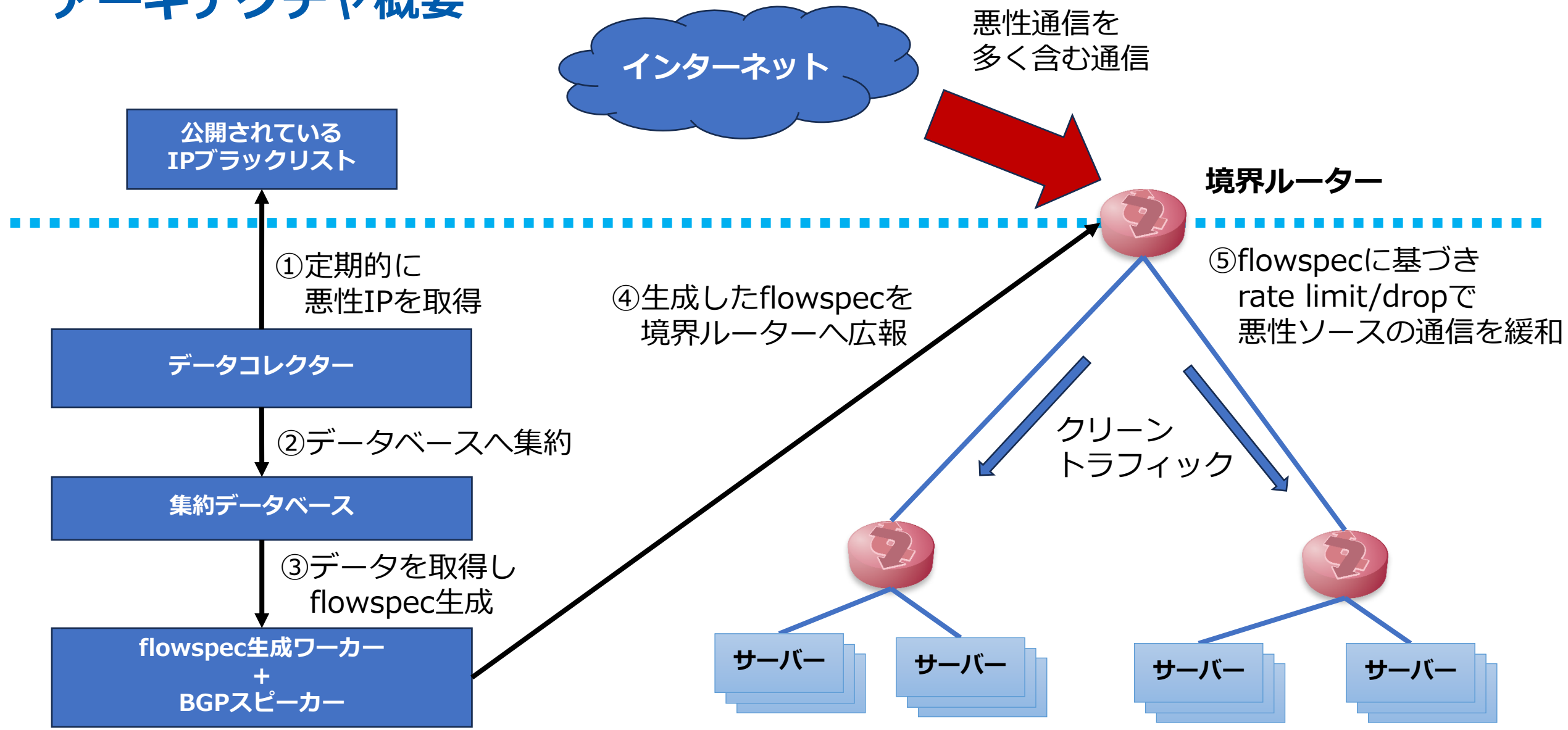
社内で求めていることは、非ボリューム型攻撃を「ほどほどに」防ぐこと（アラート削減）

↓

L3/L4ベースで、自分たちで防御システムを実装できないか？

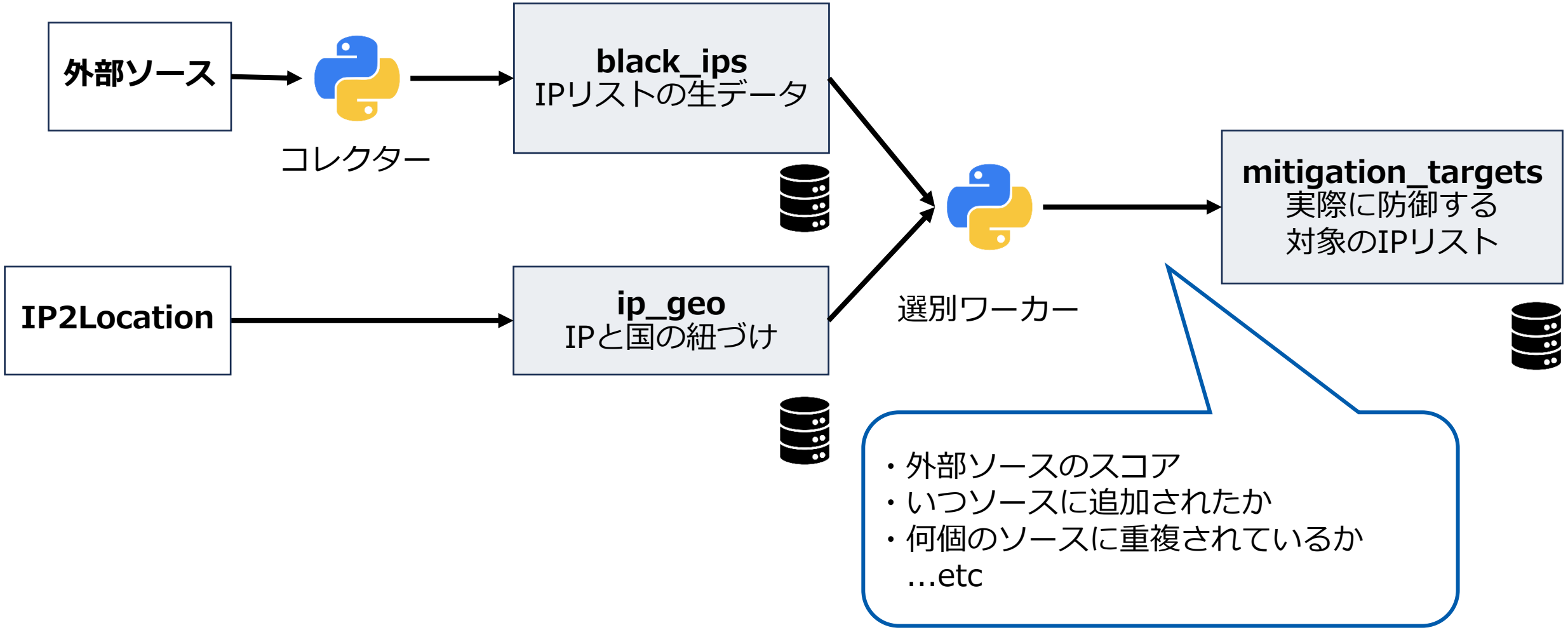
アプローチ：動的ブロックリスト方式（IPリスト連携）
悪性の疑いがあるIPを一定条件で帯域制限・ブロック／解除

アーキテクチャ概要



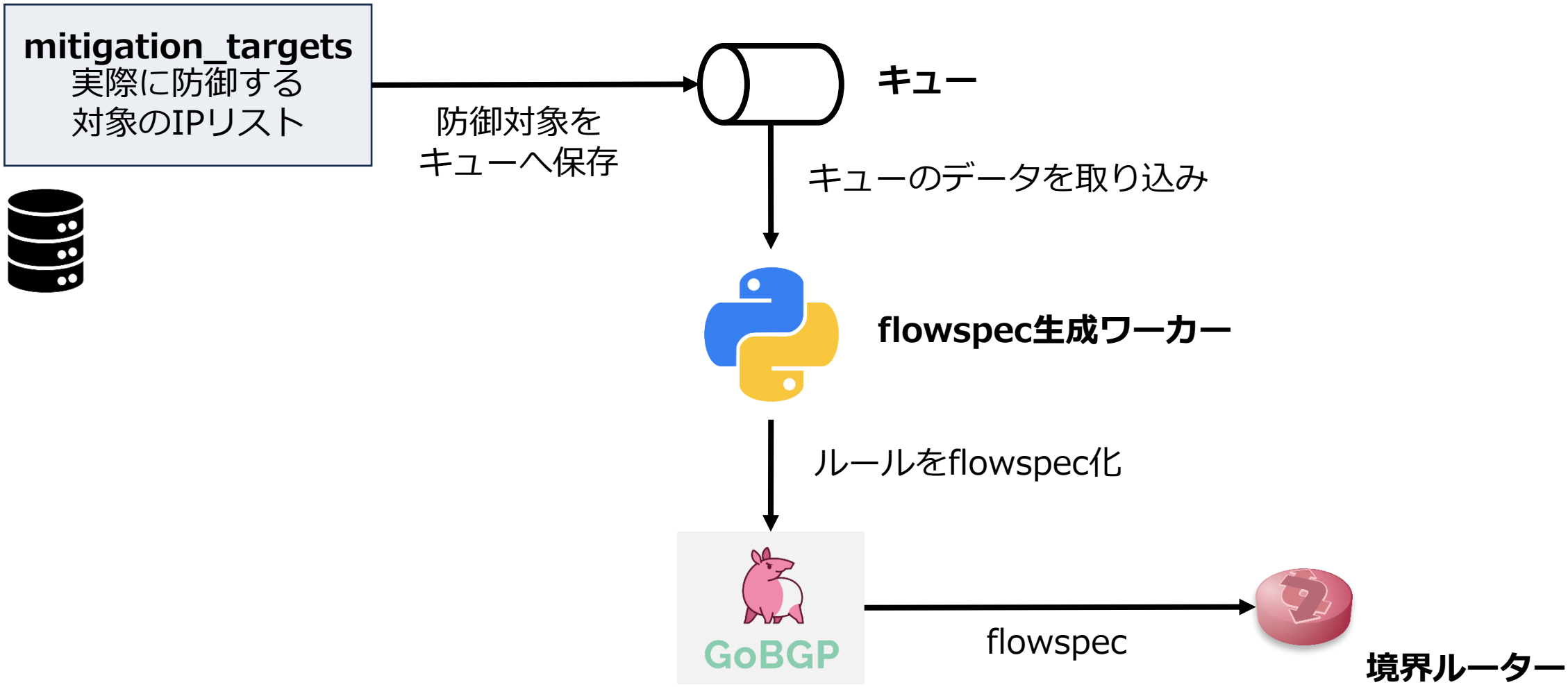
アーキテクチャ詳細①

悪性IPリストをデータベースへ集約

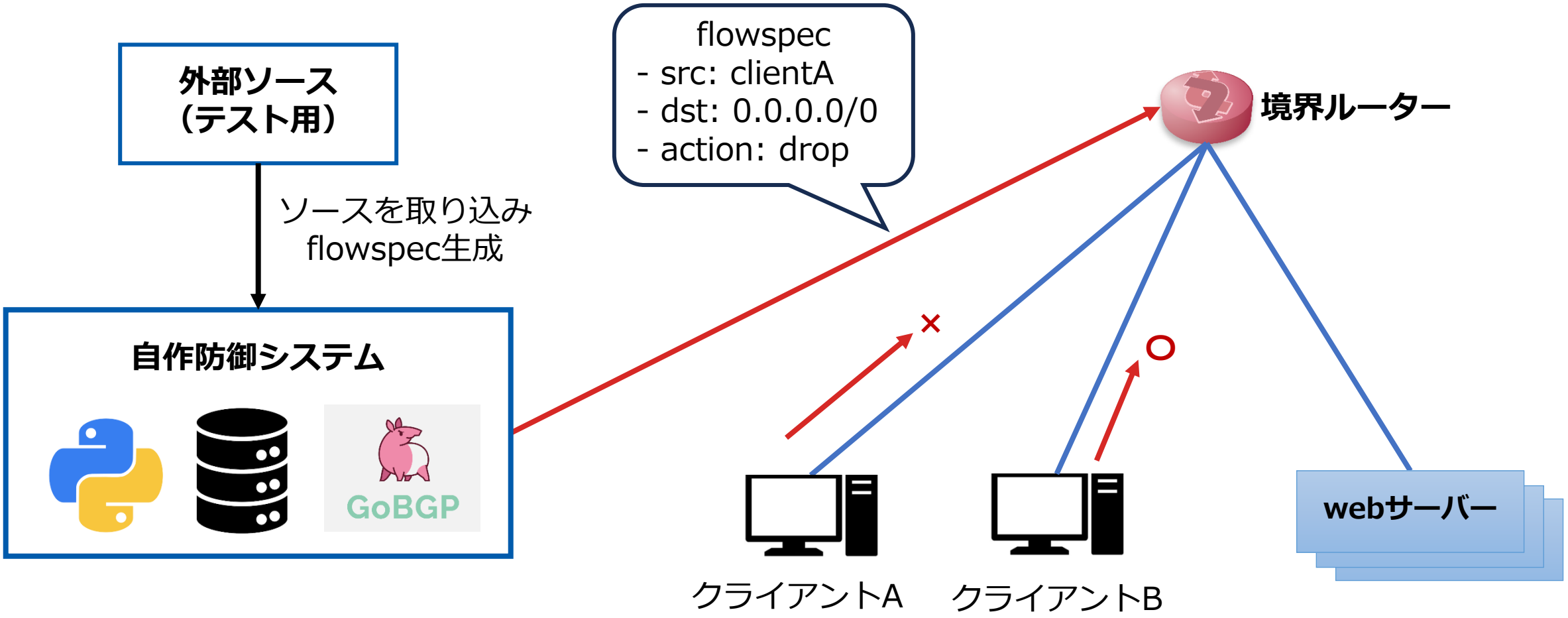


アーキテクチャ詳細②

データベースの情報を境界ルーターへ反映



検証環境で実際に通信が遮断できることを確認



課題

IPリストの
カバー率

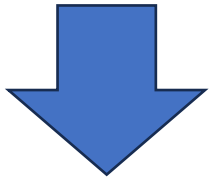
社内に来ていた攻撃の
50%しかカバー
できていなかった

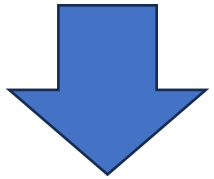
境界ルーターの
キャパシティ

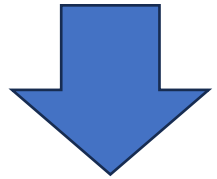
境界ルーターの
flowspecルール上限数

判定ルールの
最適化

チューニングの精度と工数
リアルタイム防御の限界







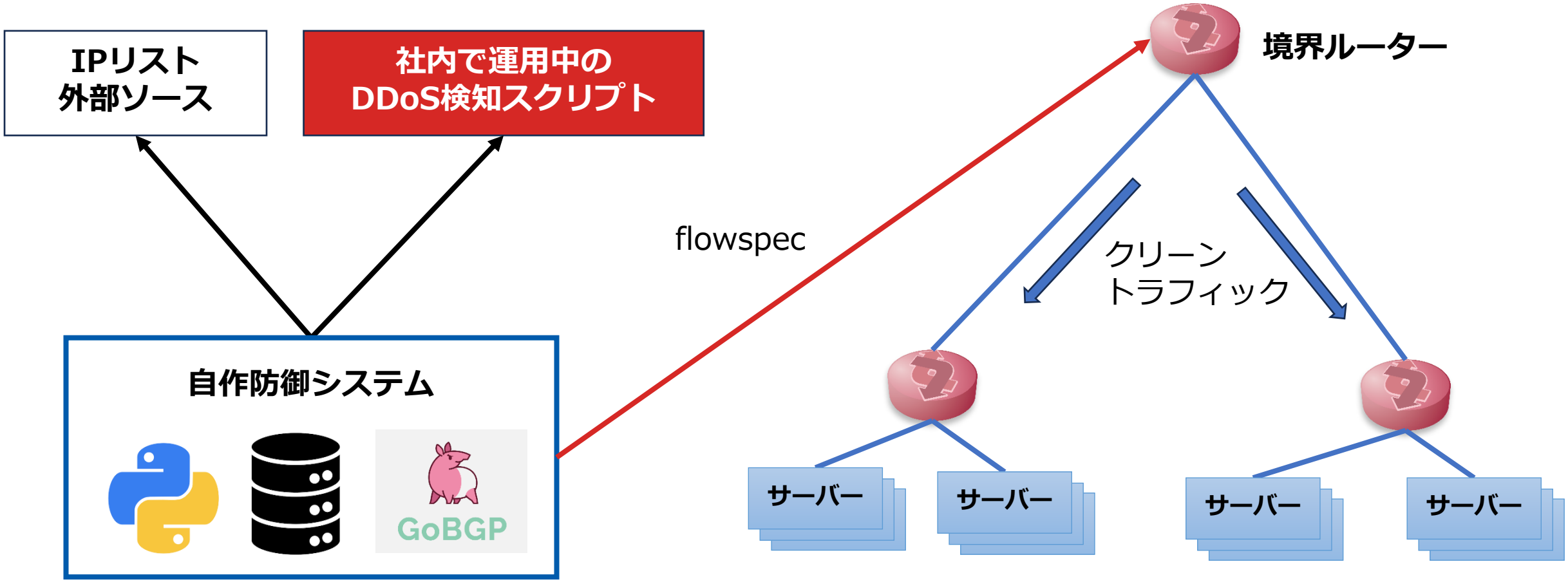
IPリストの
質・量を高める

必要なルールのみを
投入する仕組み

AIによる自動化

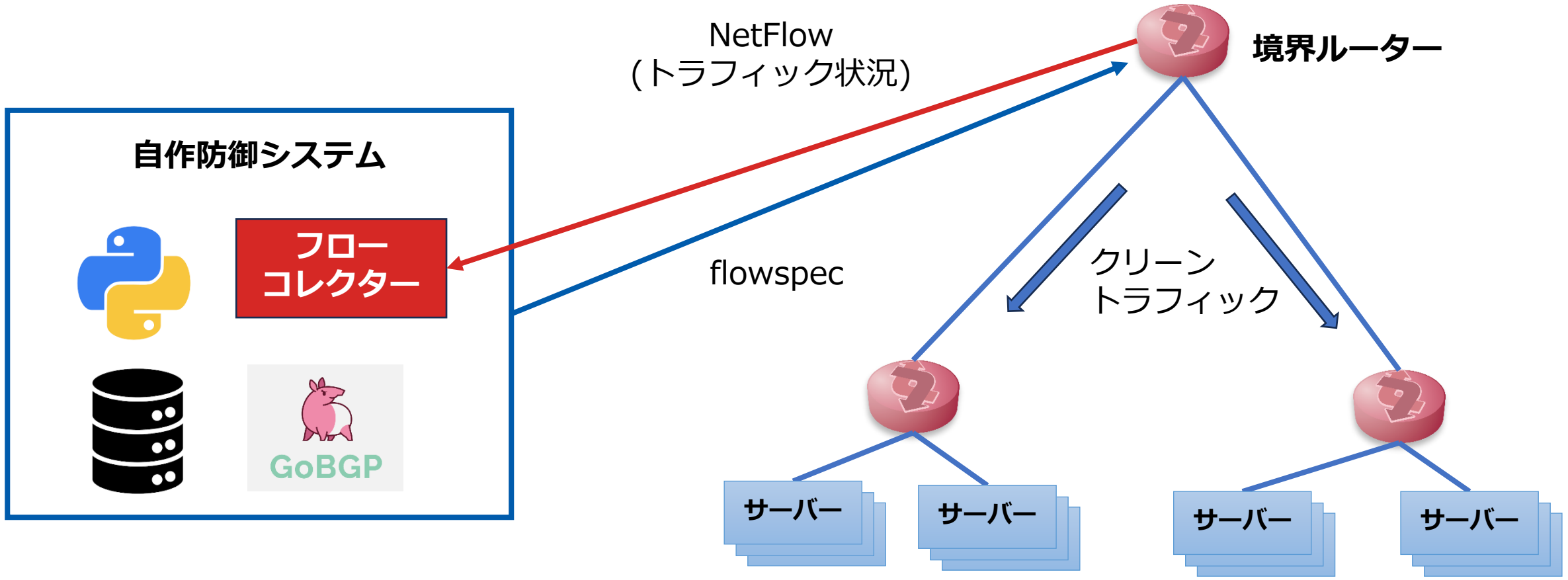
課題①IPリストのカバー率

量→新しいIPリストを選定、追加
質→社内商材への過去の攻撃の送信元IPもIPブラックリストとして利用



課題②flowspecのキャパシティ

境界ルーターのFlow情報をもとに、今来ている悪性通信のみを防御



課題③選別ルールの最適化

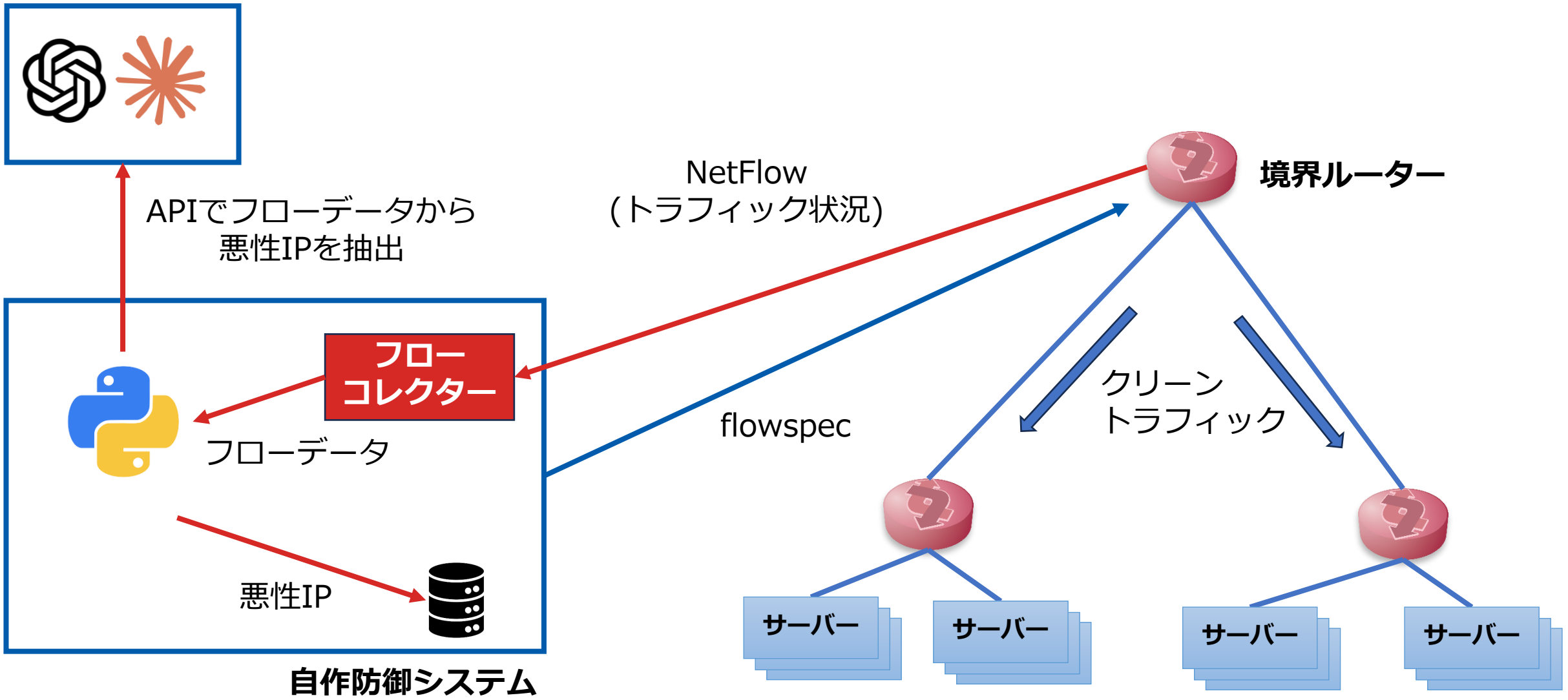
AIを用いて柔軟に防御対象IPを選別

現状の判定方法：静的な情報
（外部ソースのスコア、何個のソースに重複されているか、etc…）

・都度ルールの最適化が必要で工数がかかる
・リアルタイムで生まれた攻撃は防御できない

実トラフィックの動的特徴量＋AI解析でリアルタイムかつ柔軟な防御
・PPS変動、パケット種類、フロー継続時間を踏まえた防御
・ロジック化が難しい「怪しい通信」への柔軟な対応

課題③選別ルールの最適化



まとめと展望

【まとめ】
・**非ボリューム型DDoSが増加している**（特にアプリ層攻撃）
・L7防御は有効だが、**コスト・運用面のハードル**が高い
　→「影響緩和・アラート削減」にスコープを限定し、**L3/L4で対策**を考えた
・**IPブラックリスト × BGP Flowspec** により、
　非ボリューム型攻撃の50%程度は上位NWで吸収できることを確認
・一方、**①IPカバー率**、**②flowspecエントリ数**、**③判定ルールの精緻化**
　の観点で改善課題がある

【展望】
　課題①～③への対策実装→本番環境への導入

議論ポイント

To: ALL
・非ボリューム型DDoSの対策をどうしている？
・アプリ層攻撃はNWで対策している？

To：ホスティング事業者
・お客様環境へのアプリ層攻撃への対策機器(L7WAFなど)は導入している？
コストに見合っていると感じる？
・L7防御導入に伴うお客様への影響や負担についてどう考えている？

すべての人にインターネット

GMO