# CDNのキャッシュサーバを騙った DDoS攻撃の防御法

## 1. はじめに

■ DDoS攻撃が頻繁に発生

ボットから大量のパケットをターゲットホストに送信することによりで機能不全にする攻撃

■ 攻撃者が標的サーバのIPアドレスを特定した場合

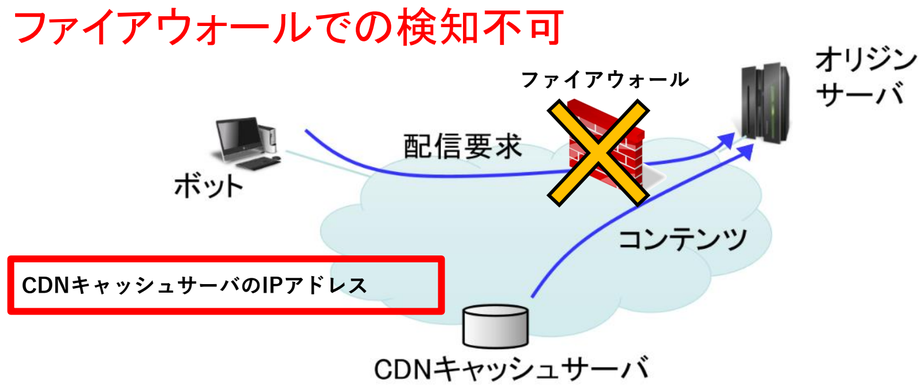
DNS (Domain Name System)を用いずに，特定したIPアドレス宛に直接パケットを送信

→ CDNキャッシュサーバ以外からのパケットファイアウォールで遮断

■ CDNのキャッシュサーバを騙ったDDoS攻撃

ボットがキャッシュサーバ(CS)のIPアドレスを発アドレスとして偽り，標的オリジンサーバへパケットを送信

→ ファイアウォールでの検知不可




■ 要求発生間隔の違いを利用した動的な検知方式

→ Zスコア法を用いた検知方法を提案

## 2. 先行研究について

■ 先行研究: DDoS攻撃の二段階検知法

DNSの名前解決ログにより，攻撃を検知

■ DNSの名前解決ログによるパケットの判別法

- 問い合わせあり: 配信処理を実施
- 問い合わせなし: DDoS攻撃と判断し，アクセスを棄却

→ 全要求に対しDNSのログを確認するとOSの負荷増大

→ 固定閾値で危険性のある要求を判別

■ 先行研究の特徴

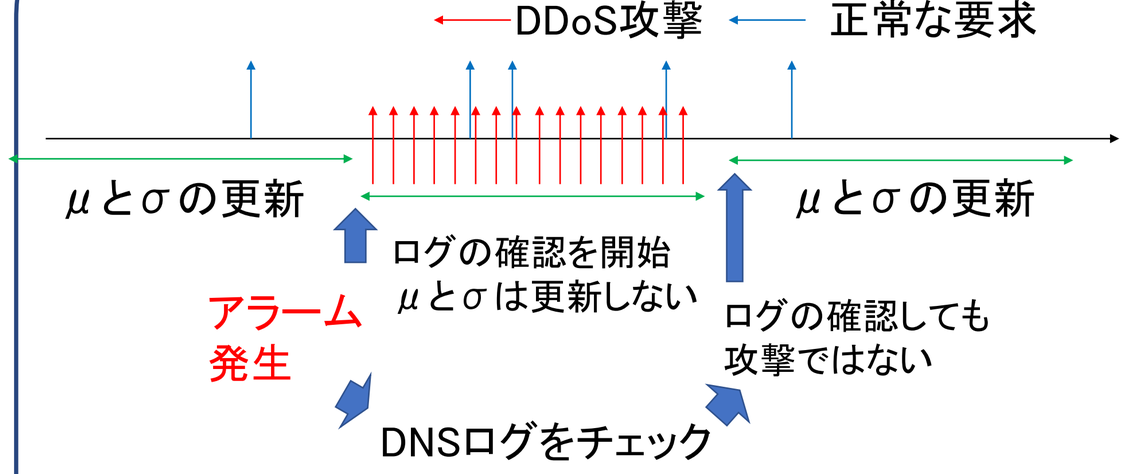
- 固定閾値を用いる検知法
- 要求発生パターンの違いを利用

■ 問題点

固定閾値を用いているため，見逃し誤検知が多い

## 3. 提案方式

■ アルゴリズム




■ 提案方式のメリット

■ 到着間隔の逆数をデータとしてZスコア法に使用

→ 到着間隔の違いによりDDoSパケットを判別

■ 攻撃発生中の誤ったデータを平均に反映しない

→ 正常な要求のみとは異なった到着間隔のパターン

■ Zスコア法のメカニズム

- 過去のデータより平均μと標準偏差δを算出
- 平均から外れ値を検知
- 外れ値を平均に基づいて編集しデータとして記録

## 4. 性能評価

■ オーダ表記での処理負荷軽減度の評価

■ DNSログの検索処理: O(n)

■ Zスコアアルゴリズムの時間計算量: O(1)

→ Zスコア法とDNSのログ検索の計算量の違いにより処理コストの低減が可能

■ シュミレーションで有効性を評価

■ 攻撃パケットの検知率で評価

- 検知率は90%以上
- 誤検知はログの確認により完全に回避