一般社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
NS2023-222(2024-03)

CDN のキャッシュサーバを騙った DDoS 攻撃の二段階検知法

谷口　和也†　　上山　憲昭†

† 立命館大学 情報理工学部
〒525—8577 滋賀県草津市野路東 1—1—1
E-mail: †tanikazu0912@gmail.com, ††kamiaki@fc.ritsumei.ac.jp

あらまし　近年，ネットワーク上に広く存在する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で，ターゲットサーバを機能不全とする DDoS (Distributed Denial of Service) 攻撃が頻繁に発生している．CDN (Content Delivery Network) の主な目的はコンテンツ配信の高速化であるが，キャッシュサーバ (CS) を複数使うという特性上，DDoS 攻撃の対策にもなる．DDoS 攻撃は，ターゲットサーバに対して膨大な負荷をかける攻撃であるため，サーバが複数であれば負荷が分散され，攻撃が成立しない．しかし攻撃者がオリジンサーバ (OS) の IP アドレスを把握した場合，攻撃者はボットから OS の IP アドレス宛に攻撃パケットを送ることで DDoS が成立するが，OS が CS からの要求パケット以外は棄却するファイアウォールを用いることでそのような攻撃も防ぐことができる．しかしボットが CS の IP アドレスを発アドレスとして偽り，OS へパケットを送信した場合は，ファイアウォールで検知できない．DNS のログを調べれば，CS からの正常な配信要求か，ボットからの DDoS パケットか判別可能である一方で，全ての配信要求に対して DNS のログを調査すると，その処理コストの増大が問題となる．そこで著者らは DDoS 攻撃のパケットが短い時間間隔で多数発生することに着目し，到着時間間隔に対して閾値を設け，閾値以下の間隔で同一 IP アドレスから要求が到着した場合にのみ DNS のログのチェックを実施する，CDN を騙った DDoS 攻撃の二段階検知法と最適閾値設計法を提案した．しかし一般的に配信要求の発生パタンは動的に変化するが，本方式では閾値を固定的に設定するため，動的な環境に対する対処が困難である．そこで本稿では動的な環境への対応が可能な Z スコアを用いた二段階検知法を提案する．性能評価では，DDoS 攻撃の検知精度を評価し，提案方式を用いた場合の OS の負荷の軽減を確認する．また学習時間に対しての検知精度を評価することにより，提案方式を用いた場合に必要な学習時間を評価する．

キーワード　DDoS，CDN，DNS，Z スコア

Two-Level Detection Method of DDoS Attack Mimicking CDN Caches

Kazuya TANIGUCHI† and Noriaki KAMIYAMA†

† College of Information Science and Engineering, Ritsumeikan University
1—1—1, Nojihigashi, Kusatsu, Shiga 525—8577
E-mail: †tanikazu0912@gmail.com, ††kamiaki@fc.ritsumei.ac.jp

Abstract　In recent years, DDoS (Distributed Denial of Service) attacks have been occurring frequently, in which bots, which are widely distributed throughout the network, send large numbers of packets to the target host, causing the target server to malfunction. Since DDoS attacks place an enormous load on the target server, the attack is not feasible if there are multiple servers, since the load is distributed among them. If an attacker knows the IP address of the origin server (OS), the attacker can establish a DDoS by sending attack packets from the bots to the OS IP address. Such an attack can be prevented by using a firewall that allows the OS to reject packets other than those requested by the CS. If a bot sends packets to the OS falsely claiming the CS IP address as its originating address, it cannot be detected by firewalls. By examining DNS logs, it is possible to determine whether the packet is a normal delivery request from the CS or a DDoS packet from a bot. However, if DNS logs are examined for all delivery requests, the processing cost increases. Therefore, the authors focused on the fact that many DDoS attack packets are generated in short time intervals and proposed a two-stage detection method for DDoS attacks that trick CDNs and a method for designing optimal thresholds, in which a threshold is set for arrival time intervals and DNS logs are checked only when requests arrive from the same IP address at intervals below the threshold. However, in general, the occurrence pattern of delivery requests changes dynamically, and this method sets a fixed threshold value, making it difficult to cope with dynamic environments. In this paper, we propose a two-stage detection method using Z-scores that can cope with dynamic environments. In the performance evaluation, we evaluate the detection accuracy of DDoS attacks and prove that the proposed method reduces the load on the OS. We also evaluate the required training time of the proposed method by evaluating the detection accuracy against the training time.

Key words　DDoS，CDN，DNS，Z score

1. はじめに

CDN (content delivery network) は, 地理的に分散したキャッシュサーバ (CS) で構成され，HTML ページ，画像，動画などのインターネット・コンテンツをキャッシュし，効率的に配信する．CDN は非常に普及しており，ウェブトラフィックの大部分を配信している．CDN の市場価値は，2024 年の 199 億 6,000 万ドルから 2029 年には 424 億 6,000 万ドルに達すると予想されている [1]．CDN はまた，CDN サービスやエンドユーザーエクスペリエンスに影響を与えるサービス拒否などのセキュリティ攻撃の対象となる [2]．CDN の運用に対する攻撃は，CDN の機能を損ない，否定的な報道を引き起こす可能性が存在する．したがって，CDN をセキュリティ攻撃から保護することは非常に重要である．また CDN はコンテンツの盗難や損失から保護するだけでなく、セキュリティ攻撃を軽減することでコンテンツの可用性を確保する必要がある [3].

一方で近年, ネットワーク上に広く存在する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で, ターゲットサーバを機能不全とする DDoS (Distributed Denial of Service) 攻撃が頻繁に発生している．CDN の主な目的はコンテンツ配信の高速化であるが， CS を複数使うという特性上，DDoS 攻撃への対策として期待される．DDoS 攻撃はターゲットサーバに対して膨大な負荷をかける攻撃であるため，サーバが複数であれば負荷が分散され，攻撃が成立しない [4]．しかし攻撃者が CDN を用いたネットワークを標的として攻撃を行った時の攻撃が成立する可能性が存在する．実際に 2020 年 6 月 4 日に発生した CDN の Akamai を標的とした攻撃は，攻撃者が脆弱な DNS サーバを利用して正当なトラフィックを大量に送信する DNS 増幅攻撃であり，攻撃トラフィック量において過去最大級のもので攻撃トラフィックのピークは 1.44 Tbps と報告されていている [5].

また攻撃者は Origin Server (OS) の IP アドレスを宛先として，直接 OS(Origin Server) に対して攻撃パケットを送ることで，OS をターゲットとした DDoS 攻撃が可能である．しかし CDN ではユーザの配信要求に対し，選択された CS に要求コンテンツが存在しない場合のみ OS に要求が届く．そのためボットが標的 OS に直接パケットを送信した場合，OS は CS 以外からの配信要求をファイアウォールで棄却することで DDoS 攻撃を防ぐことができる [2] [6]．しかしボットが CS の IP アドレスを発アドレスとして偽り OS へパケットを送信した場合は，ファイアウォールで検知できない．

CS からの正常な問い合わせ時には，コンテンツ提供者の DNS サーバに名前解決のログが残るが，ボットからの直接要求は DNS の名前解決を用いないため名前解決のログが残らない．そのため DNS のログを調べれば，CS からの正常な配信要求か，ボットからの DDoS パケットか判別可能である．しかし全ての配信要求に対して DNS のログを調査すると，その処理コストの増大が問題となる．そこで本稿では，DDoS 攻撃のパケットが短い間隔で多数発生することに着目し，到着時間間隔に対して閾値を設け，閾値以下の間隔で同一 IP アドレスから要求が到着した場合にのみ DNS のログをチェックする二段階検知法を提案する．攻撃者はフィルタリングを回避するため動的にパケットレートを変動させる可能性がある．そこで提案方式では，動的に検知閾値を変更可能な Z スコア法 [7] を用いる．また DDoS 攻撃の検知精度，提案方式の OS 負荷低減効果に着目し，提案方式の有効性を計算機シミュレーションにより明らかにする．

以下，2. 節で CDN のキャッシュサーバを騙った DDoS 攻撃法と DNS ログによる検知法について述べ，3. 節で関連研究について述べる．そして 4. 節で提案方式の詳細を述べ，5. 節で性能評価結果を示し，6. 節で全体をまとめる．

2. CDN のキャッシュサーバを騙った DDoS 攻撃法と DNS ログによる検知法

DDoS 攻撃の主なものには以下の攻撃パタンがある．ボリューム攻撃では，大量のトラフィックが一斉にターゲットホストに対して送信され，ターゲットホストが過負荷に陥る．アプリケーション層攻撃では，特定のアプリケーションやサービスに対して厳密に計画された攻撃が行われ，サーバのリソースが枯渇する．リフレクション攻撃では，攻撃者がボットからターゲットホストの IP アドレスを発アドレスとして偽った大量のクエリパケットを DNS サーバ等の公開サーバに対して送り，大量の公開サーバからターゲットホストに向けて大量の応答パケットを送信させる．これに IP スプーフィングが結びつくことがあり，攻撃者は自身の IP アドレスを偽装して攻撃を匿名化し，追跡を困難にする．これらの攻撃への対策としては，継続的な監視，トラフィックのフィルタリング，セキュリティ対策の実施が不可欠である．

2.1 CDN キャッシュサーバを騙った DDoS 攻撃

攻撃者が CDN の CS の IP アドレスを悪用して行う DDoS 攻撃が存在する．本稿で着目する CDN の CS の IP アドレスのスプーフィング攻撃は，CDN を用いたネットワークに対して重大なセキュリティリスクをもたらす．まず，この攻撃はファイアウォールで検知しにくい．スプーフィングによって正規のトラフィックと見なされ，ファイアウォールは通常トラフィックの送信元 IP アドレスを CS として信頼していることから攻撃の検知が難しい．そのため図 1 に示すように，DDoS の攻撃パケットが CDN の CS を経由せずに直接 OS に到達し，正規のトラフィックと混在し，OS へのアクセスが不正に行われる可能性がある．

さらにスプーフィング攻撃は OS に直接ボリューム攻撃を行う手段としても利用される．攻撃者が CS の信頼できる IP アドレスを偽装すると，信頼されたソースからのトラフィックとして受け入れられ，攻撃対象の OS に向けて大量のリクエストが送信される可能性がある．これにより OS は過負荷に陥り，正規のトラフィックへの対応が困難になる．ファイアウォールはこの攻撃を通常検知できず，OS への直接の影響は大きく，可用性やパフォーマンスの低下が生じる可能性がある．このように CDN CS の IP アドレスのスプーフィング攻撃は，セキュリティインフラの弱点を悪用し，ファイアウォールでの検知が難しくなることから，深刻な危険性を持っている．

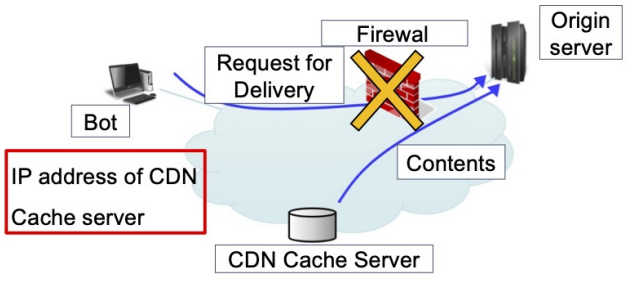

図 1　発アドレスのスプーフィングを用いた OS に対する DDoS 攻撃

2.2 DNS の名前解決方法

前節で述べたような攻撃に対して DNS の名前解決に残ったログを用いて検知することは効果的である．CDN を用いている場合，図 2 に示すように，ユーザの配信要求時にはコンテンツ事業者 (CP) の権威 DNS サーバとの名前解決手順に加え，CDN 事業者の DNS サーバとの間で名前解決の手順が生じる．以下に CDN の名前解決の手順を示す．

（1） LDNS (Local DNS) サーバの要求に対し CP の権威 DNS サーバは CNAME を LDNS サーバへ回答

（2） LDNS サーバは CNAME の名前解決を CDN 事業者の権威 DNS サーバへ要求

（3） CDN 事業者の権威 DNS サーバは CS を選択しその IP アドレスを LDNS サーバへ回答

（4） LDNS サーバはユーザに選択された CS の IP アドレスを回答し，ユーザは指定された CS へアクセス

（5） CS にキャッシュされていない場合は，CS は OS からコンテンツを取得してキャッシュ後，ユーザに配信

そのため CS からの正常な問い合わせ時には，CP の DNS サーバに名前解決のログが残るが，ボットからの OS の IP アドレスを直接用いた要求は DNS の名前解決を用いないため名前解決の履歴が残らない．そのため DNS のログを調査することより，CS からの正常な配信要求か，ボットからの DDoS パケットかの区別が可能である．しかし OS には大量の配信要求が到着することから，すべての配信要求に対して DNS のログを調べると OS の処理負荷の増大が懸念される．

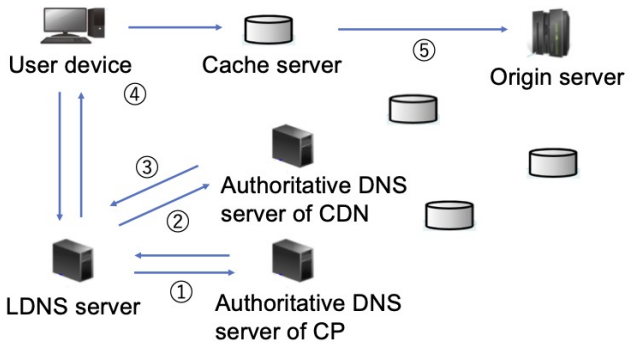

図 2 DNS の名前解決方法

2.3 名前解決における検知法の課題

前節で述べたように，DNS ログの確認は CDN の CS の IP アドレスのスプーフィング攻撃を検知する重要な手段である．しかし OS に到着した大量の全ての配信要求に対し，DNS のログの確認処理を実施すると OS の負荷が増大する．過剰なログ確認処理を行うことで，OS のパフォーマンスが低下し，正当なトラフィックへの応答が遅延し，結果，OS に対する DDoS 攻撃の目的が達成される．そのため DNS のログ確認を，必要のある要求に対してのみに限定する必要がある．そこで本稿では，DDoS 攻撃と正常なコンテンツ配信要求の要求発生パタンの違いに着目し，直前の同一コンテンツに対する要求との到着間隔から，DDoS 攻撃パケットの可能性の高い要求パケットを検知し，そのようなパケットに対してのみ DNS のログ検査を行う方式を提案する．

3. 関 連 研 究

3.1 OS への直接的な攻撃の可能性

メール，FTP，SSH などのの，CDN を用いないサービスの OS の IP アドレスは公開される．したがって攻撃者はこれらのサービスの DNS レコード (メール サービスを参照する MX レコードなど) から発信元アドレスを収集可能である．コンテンツ所有者は，SSH(例: ssh.owner.com) などの一部のサービスに非表示のサブドメインも使用する．辞書攻撃を使用すると，攻撃者は隠れたサブドメインを推測してクエリを実行し，発信元 IP アドレスを収集可能である [2]．またこれら以外にも攻撃者が OS の IP アドレスを取得したり推定するための様々な方法の存在が指摘されている [8]．

3.2 CDN と CBSP による DDoS の防御

CDN と CBSP (Cloud-based Security Providers) は，ウェブサーバへのリクエストを傍受し，キャッシュされたコンテンツを提供するか，動的な応答のためにリクエストをウェブサーバに転送する共通の機能を持っている．CDN はリクエストを検査してインテリジェントなキャッシング技術を使用し，クラウドベースのセキュリティを提供するために適している．トラフィックが既に CDN を介してリダイレクトされているため，スクラビングセンタや WAF をインフラ内で連鎖させることが容易である．地理的に分散された CDN は，Anycast を使用して分散攻撃の対処と大量の悪意のあるトラフィックの吸収に理想的である．CDN と CBSP の機能が重複することから，CDN プロバイダと CBSP は統合され，その境界が曖昧になりつつある．従って，CDN とセキュリティ拡張を持つ CBSP の両方に適用される．

4. 提 案 方 式

提案方式は CDN の CS の IP アドレスのスプーフィング攻撃の検知を目的とした DNS の名前解決のログ検査負荷を低減するため，要求の到着間隔に対して閾値を設けた二段階検知方式と，さらに動的な環境に変化に対応するための Z スコア法を用いた動的な閾値設定法から構成される．以下に各々の技術の詳細を述べる．

4.1 二段階検知法

CS からの正常な問い合わせ時には，コンテンツ提供者の DNS サーバに名前解決のログが残るのに対し，ボットからの IP アドレスを直接用いた要求は DNS の名前解決を用いないため名前解決のログが残らない．そのため DNS のログを調べれば，CS からの正常な配信要求か，ボットからの DDoS パケットか判別が可能である．しかし，OS には大量の配信要求が到着することからすべての配信要求に対して DNS のログを調べると OS の処理負荷の増大が懸念される．そのため問い合わせ間隔に閾値 T を設定し，コンテンツごとに要求の到着間隔を計測し，T に対しての要求の到着間隔の長さにより DNS サーバの問い合わせの有無を確認する必要のある要求を絞り込む．具体的な判別の方法としては，T より長い間隔の要求は CS からの正常な要求と見做し,T より短い間隔の要求はボットからの DDoS 攻撃の可能性を考え問い合わせの有無を DNS ログに対して確認する．これは，正常な配信要求がキャッシュミス時に発生するのに対し，DDoS パケットは短い時間間隔で連続して発生するという要求発生パタンの違いに由来する．さらに問い

合わせが有れば CS からの正常な要求と見做し，問い合わせがなければ DDoS 攻撃と見做しアクセスを棄却する．本方式により DNS のログの検索負荷を減らし，DDoS 攻撃を効率よく検知することができる．

DDoS 攻撃の二段階検知法では，閾値 T を大きく設定しすぎると DNS サーバでの問い合わせの有無を確認する回数が増え OS の負荷が増大する．一方，閾値 T を小さく設定しすぎると DDoS 攻撃を検知できない可能性があり，DDoS 攻撃に対しての防御性能が低下するという問題がある．本問題を解決するため，閾値 T を最適なものに設定する必要がある．閾値 T は DNS の検査レートの許容上限を満たす範囲で最大化することが必要になる．このように閾値を設定することで，DNS サーバの処理能力上限を考慮しながら DDoS 攻撃を最大限，検知することができる．DNS サーバの処理能力上限とは，コンテンツ毎の DNS 検査レートを全てのコンテンツに対して考慮したものになる．ここでは DNS の総検査レートとする．最適な閾値 T を求めるには，DNS の総検査レートが必要になる．検査コンテンツ数を M，閾値 T に対してのコンテンツ m の DNS の検査レートを $r_m(T)$ とすると，T に対する DNS の総検査レート R_n は

$$R_n(T) = \sum_{m=1}^{M} r_m(T) \tag{1}$$

で求まる．この DNS の総検査レートを用いて，DNS の検査レートの上限値を U_n とするとき，$R_n(T) = U_n$ となる T の最大値を T に設定する．こうすることで最適な閾値 T が求まる．

しかし絶えずパケットレートが変化するネットワーク環境においては，一段階目の判断基準として単一の固定閾値では対応できない．そこで次節では動的な環境に対して閾値を動的に調整することで外れ値検知が可能な，Z スコアアルゴリズムによる動的閾値設定法を用いる方法を述べる．

4.2 Z スコア法

提案方式では，閾値の設定法に Z スコアアルゴリズムを用いる．Z スコア法はデータの外れ値を検知するアルゴリズムである．過去の直近のデータから移動平均と標準偏差を更新し，大きく平均から外れた値を検知し，アラームを発生する．Z スコア法のアルゴリズムを下記に記す．

$$S_i = \begin{cases} 1 & E_c - \mu_{i-1} > \eta\delta_{i-1} \\ -1 & E_c - \mu_{i-1} < \eta\delta_{i-1} \\ 0 & otherwise \end{cases} \tag{2}$$

$$E_i = \begin{cases} E_c, S_i = 0 \\ \alpha \times E_c + (1-\alpha) \times E_{i-1}, otherwise \end{cases} \tag{3}$$

$$\mu_i = mean(E_{i-L+1}, E_{i-L+2}, \cdots, E_i) \tag{4}$$

$$\delta_i = std(E_{i-L+1}, E_{i-L+2}, \cdots, E_i) \tag{5}$$

S_i が 1 もしくは-1 のときタイムスロット i においてアラームを生成する．ただし E_c は現在の測定値，E_i はタイムスロット i での測定値，ラグ L は考慮する過去のデータの個数であり，閾値 η は信号を検知する際の感度である．影響 α は検出時の信号補正における信号の影響の強さである．過去 L 期間の想定値から計算された平均と標準偏差を用いて外れ値を検知し，外れ値として検知された測定値を直前の測定値との重みづけ和に更新する．Z スコア法を用いることで過去のデータを反映した外れ値検知を実現でき，正常なコンテンツ配信要求と DDoS 攻撃の要求発生パタンの違いを検知することが可能になる．

4.3 Z スコア法導入による処理負荷の低減程度

本稿では，Z スコア法を用いて到着した配信要求の中から DDoS 攻撃パケットの可能性が高いものを検出する．そのため DDoS パケットが到着してから棄却するまでの処理負荷が軽減される程度が本方式の重要な有効性評価項目である．提案方式を用いた場合と用いない場合の処理負荷の比較には，Z スコア法での外れ値かどうかの計算処理と大量の DNS クエリを含むログの中から該当の要求を検索する処理負荷を比較することに概ね等しい．この二者の処理負荷をオーダ表記により比較することにより提案方式の処理負荷軽減の妥当性を示す．

Z スコアにおいて，(3)〜(5) の平均値と標準偏差の更新はタイムスロットごとに行えばよいのに対し，(2) は要求パケットの到着ごとに行う必要があるため (2) の計算量が支配的となるが，(2) は単純な比較のみであり， Z スコアアルゴリズムの時間計算量は $\mathcal{O}(1)$ となる．また，DNS ログの検索方式は様々なものが考えられるが，単純な線形探索を想定するとエントリ数 n に対して，DNS ログの検索処理の最悪時間計算量は $\mathcal{O}(n)$ となる．そのため Z スコアを用いることで処理負荷が低減できることが確認できる．

4.4 検 知 方 式

コンテンツの要求が OS に到着した際に，そのコンテンツに対しての直前の要求との到着間隔を記録する．Z スコア法は測定値と平均値との差異が大きな場合に検知するが，通常のコンテンツ要求と比較して，DDoS 攻撃では短い時間間隔で要求が到着する傾向があり，到着間隔を Z スコアの測定値に用いると DDoS が検知できない．そこで到着間隔の逆数を Z スコア法の入力 E_c に用いる．

そして到着した要求が外れ値か否かを Z スコアにより検査し，アラームが発生した場合は，攻撃の可能性があると判断して DNS のログを確認し，最終的な攻撃判断を行う．攻撃の継続中は，要求の到着間隔が正常な要求だけの時とは異なり，攻撃データを用いて過去 L の平均や標準偏差を更新すると，Z スコアの検知に用いる平均や標準偏差が歪む．そこで攻撃検知後は，Z スコア法での平均値や標準偏差の更新を行わない．そして DNS ログ検査の結果，連続して P 回，正常な要求と判断された場合に，攻撃が終了したと判断し，平均値と標準偏差の更新を再開する．このような方法を用いることで，攻撃が発生する前の正常な要求だけのデータを用いた外れ値の検査が可能となる．

5. 性 能 評 価

提案方式の有効性を計算機シミュレーションにて評価する．キャッシュ置換方式は LRU 方式とし, コンテンツ数を $N = 100$, キャッシュ容量 $C = 10$ とする．以降，コンテンツの人気度が x 番目に高いコンテンツを RANKx と表記する．また正常ユーザからは平均 1 秒の指数分布に従う間隔で要求を発生させ，コンテンツの要求頻度の分布をパラメタ 0.8 の Zipf 分布で与えた．Z スコアのパラメタは，$L = 10$，$\eta = 4.0$，$\alpha = 0.5$ に設定した．シミュレーションを 10,000 秒間実行し，シミュレーション開始より 5,000 秒後からの 3,000 秒の間，DDoS 攻撃を発生させ，DDoS 発生期間中は設定した平均発生間隔 D(秒) の Zipf 分布に従う間隔で DDoS の要求パケットを特定のコンテンツに対して発生させた．また，攻撃検知後の攻撃終了判断に

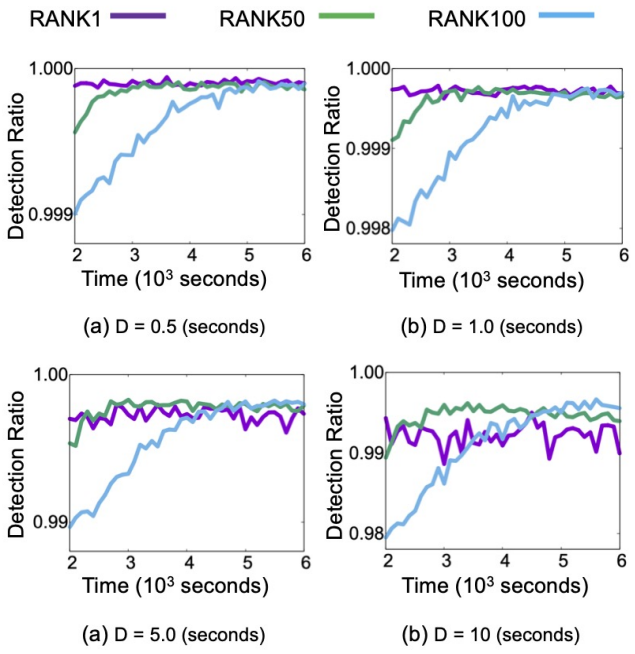

図 3　3 つの各コンテンツに対する DDoS パケット検知率の時間推移

用いる P は $P = 5$ に設定した．学習時間の適切性，人気度の異なるコンテンツに対する評価，DDoS パケットの到着数に対する評価を行い，提案方式の有効性を確認する．

5.1　検知率の時間変化

本節では，提案方式の Z スコアによる DDoS パケットの検知率の時間変化を評価する．ただし検知率を，OS に到着した DDoS パケットの中で検知できた割合で定義する．Z スコア法で検知された場合，DNS 検査で確実に DDoS パケットが検知できるので，検知率は Z スコアで検知できた割合に相当する．評価では，人気度に関わらず影響度を調査するため，RANK1，RANK50，RANK100 に対して攻撃を行った場合を想定した場合の，経過時間に対する検知精度を図 3 に示す． DDoS パケットの平均発生間隔を 0.5，1，5，10 秒の 4 パタンに設定した．検知率の時間変化を評価することは，提案方式における学習時間の適切性を評価することに相当する．DDoS パケットの発生時間に対する検知率の変化を観察することで，検知率がほぼ一定で変化しなくなる点を学習が完了したとみなしている．これは，正常発生パターンを適切に学習したことを示唆している．

低人気コンテンツに対する DDoS 攻撃の方が，シミュレーションを開始してからの Z スコアの学習に要する時間が大きなことが予想されるが，評価した中では最も低人気コンテンツである RANK100 においても 5,000 秒ほど時間が経過すると検知率が横ばいになり，ほぼ一定になっている．これらより，攻撃の検知が可能になるまでに 5,000 秒は要するが，その時間以降はほぼ正確に攻撃を検知することができる．高人気コンテンツにおいて，提案方式のアルゴリズム上，DDoS パケットの発生間隔が長くなるほど検知が困難になると予想されるが，$D = 10$ 秒の平均発生間隔で DDoS パケットを発生させた場合でも RANK1 の検知率は 99% 程度を維持している．

5.2　人気度の異なるコンテンツに対する評価

提案方式では CS からの要求到着率が低い低人気コンテンツの方が，DDoS パケットとの要求発生率の違いが顕著になり，

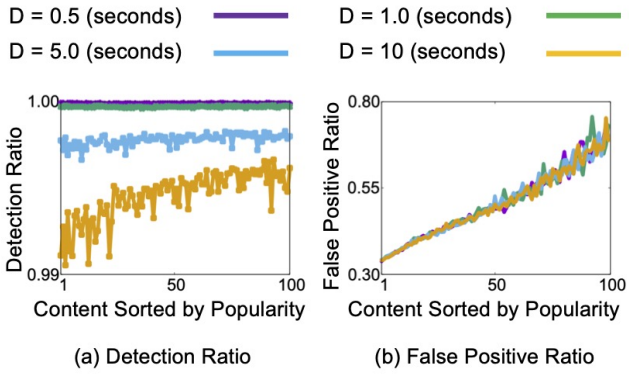

図 4　各コンテンツが攻撃対象時の検知精度

DDoS の検知が容易になると予想できる．一方，高人気コンテンツにおいては，DDoS パケットの発生間隔の設定値によっては検知が困難になる場合が考えられる．また，そのような場合に検知が困難になるだけでなく，正常な配信要求を危険性が高いと見做してしまう場合も存在する．しかし，このような場合は，DNS の名前解決のログを確認した際に，問い合わせの有無により判断が可能であるため正常パケットを誤って棄却してしまう危険性はなく，CS からの正常要求に対する誤検知は完全に回避できる．しかし誤検知が増加すると，DNS のログ検知回数が増加し，OS の処理負荷は増加する．そのため誤検知は依然として小さい方がよい．そこで本節では DDoS パケットの検知率と正常パケットの誤検知率を，各コンテンツが DDoS の標的となった場合について評価する．

前節と同様に，DDoS パケットの発生間隔を平均 0.5，1，5，10 秒の 4 つに設定する．図 4 に，各コンテンツを対象に DDoS 攻撃を行ったときの検知率を左図に，正常な要求 (CS からの要求) を誤って Z スコア法で検知した確率 (False positive ratio) を各々，非攻撃コンテンツの人気の高い順にプロットする．

提案方式は到着間隔に着目しているため，高人気コンテンツの方が検知困難と推測されるが，図 4 (a) より，人気度に関わらず 0.99 以上の高い検知率が得られる．$D = 10$ 秒程度の頻度の攻撃であれば，どのコンテンツに対しても同等の検知精度で検知が可能である．しかし一方で，誤検知は 0.3〜0.8 と大きな値となっている．提案方式では，Z スコアで誤検知をした場合も，さらに二段階目の検査として DNS のログを確認し，最終的にフィルタ対象となる攻撃パケットを特定するため，CS からの正常な要求パケットを棄却することは防げる．しかし誤検知による OS の処理負荷増加が生じる点は課題である．

5.3　DDoS パケットの到着レートに対する評価

本節では，DDoS パケットの到着レート (到着間隔の逆数) を変化させた時の提案方式の検知能力を評価する．危険性の高い低人気コンテンツに対しての検知能力を調査するため，RANK1，RANK2，RANK3，RANK5，RANK10，RANK20 に対して攻撃が行われた場合を想定して評価する．提案方式の性能を検知能力の様々な点から評価するため，DDoS パケットの検知率，正常パケットの誤検知率に加え，OS の処理負荷，DDoS の攻撃強度，攻撃率を評価する．OS の処理負荷とは，単位時間当たりの DNS ログを確認した回数である．Z スコアで検知された回数と一致し，この値が多いほど OS の処理負荷が大きなことを意味する．DDoS の攻撃強度とは，単位時間当たりに OS からコンテンツを配信した回数であり，正常コンテン

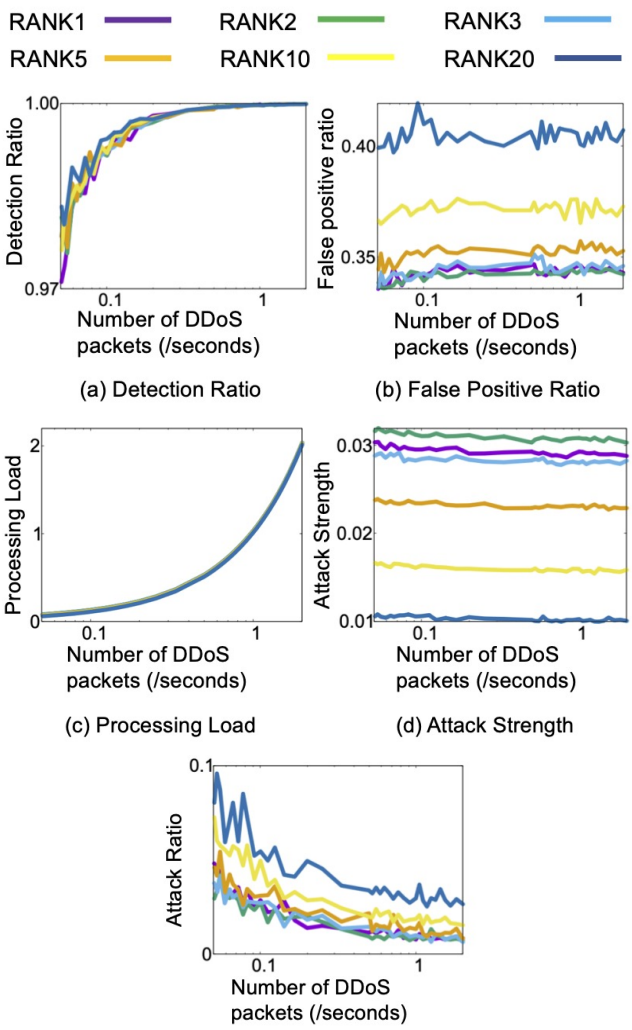

図 5　DDoS パケットの到着レートが様々な評価尺度に与える影響

ツ配信と，見逃した DDoS パケットに対するコンテンツ配信が含まれる．また攻撃率は，攻撃強度における DDoS パケットの割合を示している．

図 5 に，6 つの各コンテンツに対して DDoS 攻撃を発生させたときの，DDoS パケットの OS への到着レートに対し，(a) 検知率，(b) 誤検知率，(c)OS の処理負荷，(d)DDoS 攻撃強度，(e) 攻撃率を各々プロットする．検知率は DDoS パケットの到着レートが高い方が検知が容易であると予想されるが，(a) ではそのような推測を反映した結果が得られている．検知レートの増加に伴い検知率は増加し，ほぼ 100 %となる．誤検知率は DDoS の発生レートに依存しない結果であり，攻撃対象コンテンツの人気度によりで値が異なる．これは，ランダムで発生する要求の中には一定数の短い間隔の要求が含まれるからである．しかし前節で述べた通り，正常なコンテンツ配信要求を誤って棄却することはない．処理負荷は DDoS パケットの到着レートの増加に伴い増加しているが，正常パケットの誤検知数は一定数でほぼ変化がないため，単位時間当たりに発生した攻撃数を反映した結果になっている．発生レートを考慮すると，DDoS パケットの検知精度が高いことがわかる．(d) より DDoS パケットを棄却することで，正常なコンテンツ配信要求のキャッシュミスの発生間隔を反映した結果になっている．すなわち高人気コンテンツほど配信回数は増加している．しかし RANK1 と RANK2 を比較すると，RANK1 の方が要求数は多いがキャッシュヒット率が高いため，キャッシュミスの平均発生間隔においては逆転する結果となっている．(e) の結果より，配信要求中に DDoS パケットが含まれる割合は低いことが確認できる．DDoS パケットの検知の見逃しは少なく，ボリューム攻撃の危険性を大幅に低下させている．

6. ま と め

CDN キャッシュサーバの IP アドレスを攻撃者に特定された場合に，その IP アドレスを騙った DDoS パケットによるオリジンサーバの直接攻撃が想定される．このような攻撃はファイアウォールでの検知が困難である．しかし DNS の名前解決のログを確認することにより，正常なコンテンツ配信との判別が可能である．DNS のログは膨大な DNS クエリと応答データを保持しているため検索に要する処理負荷が課題となる．本稿では，正常パケットと DDoS パケットの発生パタンの違いから発生する到着間隔の差異に着目し，Z スコア法を用いて動的に DNS ログを確認する必要のある要求を絞る検知方式を提案した．提案方式は 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である．数値評価結果より，提案方式の DDoS パケットの検知精度は高いことを確認した．，今後は送信元 IP アドレスの種類に着目することで，危険性のある CDN キャッシュサーバを絞りこむ方式を実現することを考えており，それにより，多大な CDN キャッシュサーバ全てに提案方式を適応する必要がなく，検知を行うコストを低減できると予想される．

謝辞　本研究成果は JSPS 科研費 21H03436 と 21H03437 の助成を受けたものである．ここに記して謝意を表す．

文　献

[1] Mordor Intelligence, Content Delivery Network Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029), https://www.mordorintelligence.com/industry-reports/content-delivery-market
[2] M. Ghaznavi, E. Jalalpour, A. Salahuddin, R. Boutaba, D. Migault, and S. Preda, Content Delivery Network Security: A Survey, IEEE Communications Survey & Tutorials, Vol. 23, No. 4, Fourth Quarter 2021
[3] R. Guo, W. Li, B. Liu, S. Hao, J. Zhang, H. Duan, K. Shen, J. Chen, and Y. Liu, CDN Judo: Breaking the CDN DoS Protection with Itself, Network and Distributed Systems Security (NDSS) Symposium 2020
[4] GMO.INTERNET GROUP, https://www.gmo.jp/security/cybersecurity/vulnerability-assessment/blog/ddos-attack/
[5] D. Wagner, D. Kopp, M. Wichtlhuber, C. Dietzel, O. Hohlfeld, G. Smaragdakis, A. Feldmann, United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale, ACM CCS 2021
[6] Protecting Websites from Attack with Secure Delivery Networks, Comp. Mag, 2015
[7] C. Hou, H. Han, Z. Liu, and M. Su, A Wind Direction Forecasting Method Based on Z Score Normalization and Long Short Term Memory, ICGEA 2019
[8] T. Vissers, et al., Maneuvering Around Clouds: Bypassing Cloud-based Security Providers, ACM CCS 2015