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
NS2024-253(2025-03)

CDN のキャッシュサーバを騙った DDoS 攻撃の LDNS ログを用いた防御法

谷口　和也†　　上山　憲昭††

† 立命館大学 情報理工学研究科
〒567–8570 大阪府茨木市岩倉町 2–150
†† 立命館大学 情報理工学部
〒567–8570 大阪府茨木市岩倉町 2–150
E-mail: †is0512he@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

あらまし　CDN（Content Delivery Network）は，インターネットにおいてコンテンツを効率的に配信する技術として広く用いられている．その普及に伴い，DDoS（Distributed Denial of Service）攻撃の増加が報告されている．DDoS 攻撃は，OS（Origin Server）の IP アドレスを特定して，OS に膨大なトラフィックを送信することで，OS に過負荷をかける攻撃である．そこで筆者らは，攻撃者が CDN の IP アドレスを偽装して DDoS 攻撃を行うことで，ファイアウォールによる検知を回避する脆弱性に着目し，この脆弱性に対して，Z スコア法を用いた動的閾値設定による二段階検知手法を提案し，高い検知率と低い処理コストを実現した．しかし本手法では，権威 DNS サーバのログ確認を前提としているため，ユーザの名前解決要求が LDNS（Local Domain Name System）サーバで処理される場合，権威 DNS サーバのログだけでは正確な判定が困難である．そこで本稿では，LDNS サーバでのログ確認を行うことで，OS をターゲットとした DDoS 攻撃の，キャッシュヒット時におけるログ欠落リスクの回避を目指した二段階検知方式を提案する．そして有効性の確認のため，ログ確認処理に伴う遅延時間やサーバ負荷を評価する．さらに，従来は単一 OS を標的とした攻撃を前提としていたが，本稿では複数の OS を標的とする攻撃シナリオにおける負荷分散効果についても検証する．

キーワード　DDoS，CDN，LDNS，Z スコア

Defense Method Using LDNS Logs for DDoS Attacks Tricking CDN Cache Servers

Kazuya TANIGUCHI† and Noriaki KAMIYAMA††

† Graduate School of Information Science and Engineering, Ritsumei University
2–150 Iwakuracho, Ibaraki City, Osaka Prefecture, 567–8570
†† College of Information Science and Engineering, Ritsumeikan University
2–150 Iwakuracho, Ibaraki City, Osaka Prefecture, 567–8570
E-mail: †is0512he@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

Abstract　Content Delivery Networks (CDNs) are widely used technologies for efficiently delivering content over the Internet. Along with their widespread adoption, an increase in Distributed Denial of Service (DDoS) attacks has been reported. DDoS attacks target the IP address of an Origin Server (OS) and overwhelm it with massive traffic, causing service disruptions. In this study, we focus on a vulnerability where attackers can evade firewall detection by spoofing the IP address of a CDN to conduct DDoS attacks. To address this issue, we propose a two-stage detection method using dynamic threshold settings based on the Z-score method, achieving both high detection accuracy and low processing overhead. However, this method assumes log verification on authoritative DNS servers. When users' name resolution requests are processed by Local Domain Name System (LDNS) servers, relying solely on authoritative DNS server logs makes accurate detection challenging. Therefore, in this paper, we propose an enhanced two-stage detection method that performs log verification on LDNS servers to mitigate the risk of log omissions during cache hits in DDoS attacks targeting OSs. To validate the effectiveness of the proposed method, we evaluate the delay and server load associated with the log verification process. Additionally, while conventional evaluations assume attacks targeting a single OS, this paper investigates the load distribution effects in attack scenarios targeting multiple OSs.

Key words　DDoS，CDN，DNS，Zscore

1. はじめに

CDN (Content Delivery Network) は地理的に分散したサーバ群で構成され，インターネットのコンテンツをキャッシュし，効率的に配信する技術である．CDN の市場規模は，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ある．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．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，キャッシュサーバ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 を標的としている攻撃は，攻撃トラフィック量において過去最大級のものであり，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].

本稿で着目している攻撃方式は CDN の IP アドレスを悪用して，直接 OS (Origin Server) を狙うものである．CDN ではユーザの配信要求に対し，選択されたキャッシュサーバ (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，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 に対処できる [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．しかし CDN の CS からの正規リクエスト時には DNS サーバに名前解決ログが残るのに対し，ボットネットを用いた不正リクエストでは DNS の名前解決が行われず，ログが残らない．このため DNS ログを解析することで，正規リクエストと攻撃トラフィックを識別可能である．

しかし全てのリクエストに対して DNS ログを確認すると，システムの処理コストが大幅に増大するという課題がある．そこで筆者らは，正常なトラフィックと攻撃トラフィックの発生パターンに着目し，Z スコアアルゴリズムを用いた動的閾値設定による二段階検知手法を提案した [7]．この手法は，短時間に高頻度で発生する攻撃パケットを異常値として検出し，異常値と判断された場合のみ DNS ログの確認を行うことで，処理コストを低減する．また攻撃者がフィルタリングを回避するためにパケットレートを動的に変動させるためこの手法は有効であることを示した．しかし要求ユーザは通常，最初に LDNS (Local Domain Name System) サーバに名前解決処理を依頼し，LDNS サーバに回答内容がキャッシュされていた場合，要求が OS に届かず，OS の DNS にログが残らない．

そこで本稿では，新たに LDNS サーバにおけるログ確認を用いた，DDoS 攻撃の 2 段階検知方式を提案する．権威 DNS ではなく LDNS でのログ確認を行うことで，キャッシュヒット時のログ欠落リスクを回避する．またログ確認処理に伴う遅延時間およびシステム負荷について，計算機シミュレーションにより評価を行う．さらに先行研究では，単一の OS を前提としたシミュレーションを行っていたため，本稿では複数の OS に対し同量の攻撃トラフィックを仕掛けた場合の負荷分散シミュレーションを行い，提案方式に対して単一攻撃の方が有効であることを明らかにする．以下，2. 節で研究課題である DDoS 攻撃方式と LDNS でのログ確認の意義について述べ，3. 節で筆者らの先行研究について述べる．そして 4. 節で提案方式の概要，5. 節で性能評価を行い，6. 節で全体をまとめる．

2. OS をターゲットとした DDoS 攻撃

DDoS 攻撃は，多岐にわたる手法を駆使し，その主要なパターンには次のものが含まれる．ボリューム攻撃では，大量のトラフィックが一斉にネットワークやサーバに送り込まれ，これによりサービスが過負荷に陥る．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，攻撃者が他のコンピュータやサーバを乗っ取り，そのリソースを悪用して攻撃対象に向けてトラフィックを送信する．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 OS への直接的な攻撃の可能性

OS によって直接提供されるサービスの IP アドレスは，オリジンアドレスを公開する可能性がある．通常，OS は CDN を使用せずに，メール，FTP，SSH などのサービスを直接提供する．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].

2.2 CS の IP アドレス特定手法

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 [9].

2.3 CDN キャッシュサーバを騙った DDoS 攻撃

図 1 に示すように，攻撃者が CDN を用いたネットワークにおいて CDN の IP アドレスを悪用して行う DDoS 攻撃が存在する．本稿で着目している CDN キャッシュサーバの 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傾向がある．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 アドレスを信頼していることにより攻撃の検知が困難となる．そのため悪意のあるトラフィックが 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の区別ができず，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 CDN キャッシュサーバの信頼できる 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，対象のサーバ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，サーバは過負荷に陥り，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 の可用性や性能の低下が生じる可能性がある．このように CDN の 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，深刻な危険性を有している．

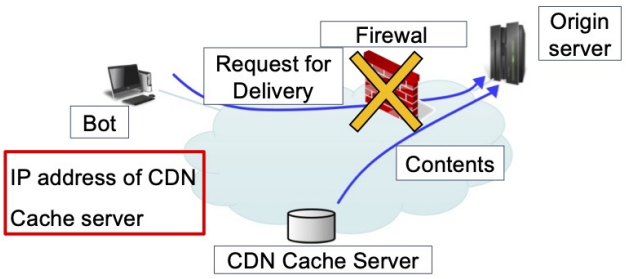

図 1　Attack against origin servers from bots mimicking IP address of cache servers

2.4　DNS の名前解決手法と検知法の課題

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，ユーザの配信要求時にコンテンツ事業者 (CP: content provider) の DNS サーバとの名前解決手順に加え，CDN 事業者の DNS サーバとの間で図 2 に示す手順が生じる．以下に CDN の名前解決の手順について述べる．

（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 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

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．

そのため筆者らの先行研究 [7] では，Z スコア法でボットからの要求の疑いの高い要求のみを検出し，検出した要求に対してのみ権威 DNS サーバでログ確認を行うことで，見逃しなくボットからの DDoS 攻撃パケットを検知する方式を提案した．しかし LDNS サーバでキャッシュヒットした場合，権威 DNS サーバを経由しないためログが残らず，適切な検知が難しい．LDNS サーバでログ確認を行えば攻撃の確実な判断が可能だが，都度確認することで遅延が発生する．そこで本稿では，LDNS での確認処理の遅延時間を M/M/1 待ち行列から算出し，処理コストを評価する．

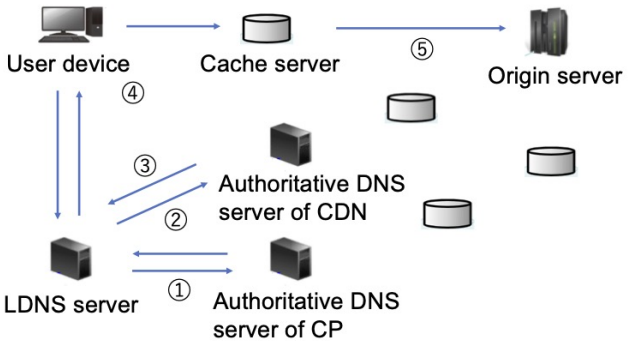

図 2　Name resolution procedure using DNS

3.　二段階検知による OS を対象とした DDoS 攻撃の検知

[7] で筆者らは，CDN の CS の IP アドレスを偽った DDoS 攻撃の検知達成を目的に，DNS の名前解決のログでの検知方式に加え，OS の負荷軽減を目的とした Z スコア法を用いた動的な閾値設定による 2 段階検知法を提案した．本節では，本方式の概要を述べる．

3.1　Z スコア法

第一段階の検知方式として，DDoS 攻撃のパケットの疑いのある配信要求パケットを OS への到着レートから検知するが，到着レートの閾値の設定法に Z スコア法を用いている．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．

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

$$E_i = \begin{cases} E_c, S_i = 0 \\ \alpha \times E_c + (1-\alpha) \times E_{i-1}, otherwise \end{cases} \tag{2}$$

$$\mu_i = mean(E_{i-L+1}, E_{i-L+2}, \cdots, E_i) \tag{3}$$

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

ラグ L は考慮する過去のデータの個数，閾値 η は信号を検知する際の感度．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を用いて更新する．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ーンの違いを検知することが可能になる．

3.2 2 段階検知による DDoS パケットの検知

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どうかを Z スコアを用いて検査し，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．

3.3 処 理 負 荷

検知方式として，Z スコア法を用いてパケットレートにより到着した要求の危険性を検査している．それにより，DDoS パケットが到着してから棄却するまでの処理負荷がどのくらい軽減されているかが本方式の性能評価の重大点である．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．

提案方式を用いた場合，Z スコアの計算処理により DDoS パケットを検知することができる．Z スコアは上節の 2 の式は主の計算式であり，単純な式であるため，平均値と標準偏差を事前に計算することで瞬時に結果を出力可能で，Z スコアアルゴリズムの時間計算量は入力数に依存しないことがわかる．したがって，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であるが，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．これらを比較した時，提案方式を使用した方が処理負荷が小さい．

4. 提 案 方 式

[7] で筆者らが提案した方式では，Z スコア法で検知された後の第二段階の検知として，CP の権威 DNS サーバでログ確認を行う．しかし，LDNS サーバでキャッシュヒットした場合，権威 DNS サーバを経由しないため権威 DNS サーバでログが残らず，DDoS パケットの検知が難しい．一方で LDNS サーバでログ確認を行えば攻撃の確実な判断が可能である．そこで本稿では LDNS サーバでログ確認を第二段階の検知法として行うことを提案する．

4.1 提案方式の処理フロー

OS は，ユーザからの配信要求を受信するたびに要求数をカウントし，Z スコア法を用いて異常なレートの要求を検出する．異常と判定された要求に対しては，要求元の LDNS サーバのログを参照し，過去に正規の名前解決が実施されたかを確認する．その後，ログ照合結果を OS へ送信し，OS が棄却判断を行う．OS は LDNS サーバのログに記録があった場合は正当な要求と判断してコンテンツを配信し，LDNS サーバのログに記録がなかった場合は攻撃パケットと判断し，要求を棄却する．本方式により，LDNS ログの参照回数を抑制しつつ，誤判定による正当な要求の棄却を回避しつつ，OS の負荷軽減と適応的な DDoS 攻撃対策の両立を実現する．

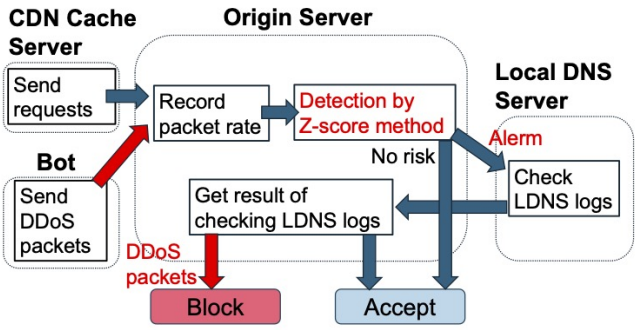

図 3 Flow of proposed method checking log of LDNS servers

4.2 提案方式の処理負荷量

提案方式では CP で Z スコア法により DDoS パケットが検知された際，LDNS サーバのログを確認するため，検知に要する処理遅延が増大することが予想される．そこで確認処理で生じる遅延時間を M/M/1 待ち行列から算出し，処理コストを評価する．遅延時間は権威 DNS サーバと LDNS サーバとの間の伝搬遅延時間と，LDNS サーバのログのメモリ検索処理に要する時間の和となる．メモリ検索遅延 T_m は，LDNS サーバのエントリ数 n，1 回のメモリ検索時間 T_r，LDNS 確認回数 c，攻撃継続時間 T_s を用いて，次式で得られる．

$$T_m = \left(\frac{2}{n \cdot T_r} - \frac{\mathrm{c}}{T_s} \right)^{-1} \tag{5}$$

伝搬遅延 T_d は 1km あたり 5μ 秒の遅延で，権威 DNS サーバと LDNS サーバとの距離を d km とすると，全体の遅延時間 T は次式で得られる．

$$T = 5 \times 10^{-6} d + T_m \tag{6}$$

5. 性 能 評 価

5.1 LDNS サーバのログ検査回数

LDNS サーバのログ確認処理に要する遅延時間，LDNS サーバの処理負荷，および CDN の CS を偽装した DDoS 攻撃が複数の OS を標的とした場合の各 OS の処理負荷について，計算機シミュレーションを用いて評価する．キャッシュの置換方式には LRU 方式を採用し，コンテンツ数は $N = 100$，CS 容量は $C = 10$ とする．異常検知には Z スコア法 [8] を用いる．この手法では，短時間に高頻度で発生する攻撃パケットと正常パケットの要求発生パタンの違いを利用して異常値を検出する．検出された異常値のみ DNS ログ確認を実施することで，処理コストの低減を図る [7]．Z スコア法のパラメタは，$L = 10$，$\eta = 4.0$，$\alpha = 0.5$ に設定する．

計算機シミュレーションでは，正常ユーザが全体で平均 200/秒のレートでコンテンツの配信をランダムな時間間隔で要求し，計算機シミュレーションの実行時間を 100 秒とする．このうち 30 秒間，攻撃者は DDoS 攻撃を実施し，攻撃パケットを平均 $D = 20$，100，200 のレートでランダムな時間間隔で発生させる．ただし攻撃者は Y 個の各 OS で配信される標的コンテンツに対してランダムに攻撃パケットを送信する．また攻撃者の標的コンテンツの選択法として，高人気コンテンツを選択する場合と，無作為にランダムに標的コンテンツを選択するランダム選択の二つの攻撃方式を評価する．ただしランダム選択においては，シミュレーション開始時に 100 個のコンテンツから無作為に標的を選択した 3 パタンの標的集合に対して固定的に攻撃を行った．

図 4 は，$D = 200$，100，20 の各々に設定した際の，LDNS ログの総確認回数を DDoS 攻撃のターゲットコンテンツ数 Y に対して示す．攻撃発生レート D によらず，Y の増加に伴い，LDNS ログの総確認回数が増加し，LDNS サーバの負荷が増加する．また 2 つの標的選択法のうち，高人気コンテンツを選択した方が，LDNS サーバのログ検査回数が増加する．

5.2 LDNS サーバのログ検査に要する遅延時間

図 5 に，式（5）で算出した LDNS サーバのログのメモリアクセス処理で生じる遅延時間を示す．標的選択法として高人気コンテンツ選択の方が LDNS 負荷が大きいため，高人気選択を想定する．評価では，単位時間あたりの平均攻撃発生回数 D を $D = 200$，100，20 に設定した．LDNS の性能に関して，LDNS サーバのエントリ数 n は $n = 100$，1 回のメモリ検索時間 T_r は DRAM の検索性能を考慮し，$T_r = 50ns$ に設定した．権威 DNS サーバと LDNS サーバとの距離 d を，例えば東京都と福岡県間の距離とした場合，約 1,000km となり 5ms の遅延となる．評価結果として，攻撃発生間隔にかかわらず 1km あたり 5μ 秒の伝搬遅延と比較して，メモリ検索遅延は数 μ 秒で無視できるほど小さいことが確認された．そのため LDNS サーバのログ確認を行った場合，権威 DNS サーバと LDNS サーバとの間のネットワーク遅延が，遅延時間の支配要因となる．

5.3 DDoS パケットの見逃し数

図 6 に，標的コンテンツ数 Y に対して，DDoS パケットの総見逃し数を示す．総攻撃パケット数を一定とし，単位時間あたりの平均攻撃発生回数 D を 200，100，20 に設定した場合の結果を比較した．標的コンテンツ数 Y の増加に伴い，標的コンテンツあたりの攻撃パケット数が減少し，正常時との到着レートの差異が低減するため，Z スコア法で検知されず見逃される DDoS パケット数が増加する．今後の課題として，攻撃者にとって最適な標的コンテンツ数およびその選択戦略について，さらなる評価を進める予定である．

6. ま と め

本稿では，[7] で筆者らが提案した Z スコア法を用いた動的閾値設定による OS を標的とした DDoS 攻撃の検知方式の課題に着目し，LDNS サーバでのログ確認を行う方式を提案し，その有効性を評価した．権威 DNS サーバとは異なり，LDNS サーバでのログ確認は，伝搬遅延やメモリアクセス処理による遅延遅延が発生するため，これらの遅延について評価を行った．その結果，攻撃発生間隔にかかわらず，1km あたり約 5μ 秒の伝搬遅延に対して，メモリ検索遅延は数 μ 秒程度と極めて小さく，無視できるレベルであることが確認された．したがって，LDNS サーバでログ確認を行う場合，遅延の主要因は LDNS サーバまでのネットワーク遅延である．また，標的 OS 数の変

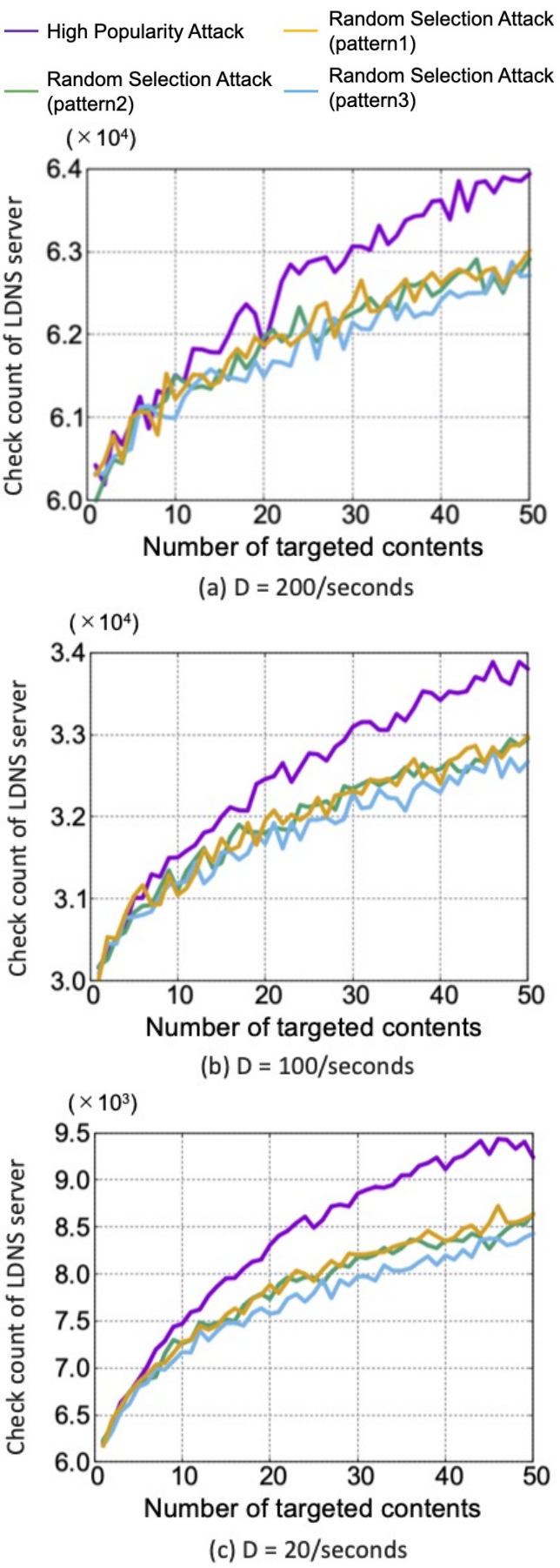

図 4　Total number of checks of LDNS server

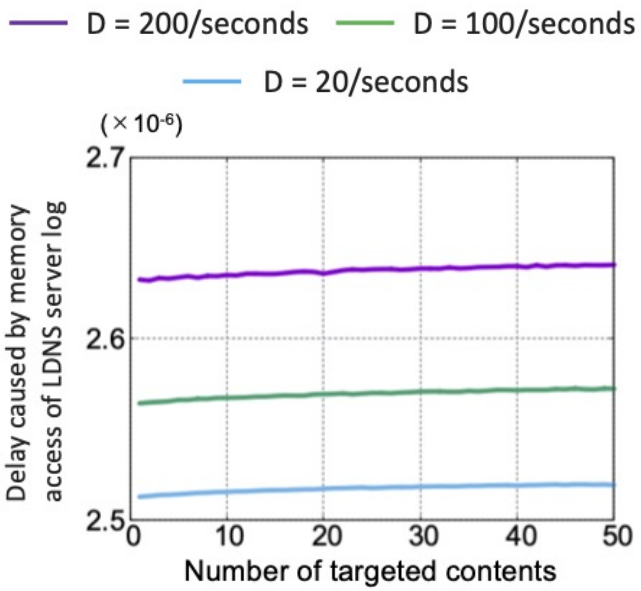

図 5　Delay caused by memory access of LDNS server log

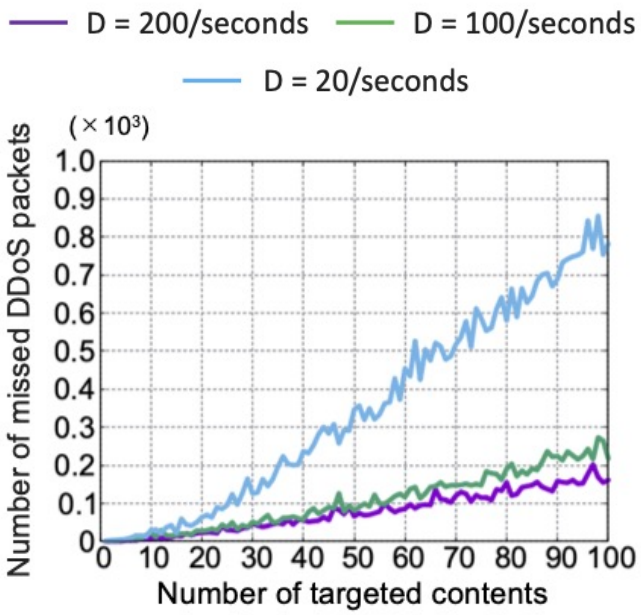

図 6　Number of undetected DDoS packets against number of target contents

化に伴う各 OS への負荷を評価した．総攻撃パケット数が一定であることから，標的 OS 数が増加すると攻撃トラフィックが分散され，各 OS への負荷が低減することが確認された．この結果から，攻撃者は本提案方式に対して高い攻撃効率を維持するため，単一 OS を標的とする攻撃を選択する可能性が高いと推測される．今後の課題として，現在は盗聴された CDN キャッシュサーバの IP アドレスが単一である場合を前提に研究を進めているが，盗聴範囲が拡大した場合の攻撃手法についても考慮する必要がある．具体的には，複数の CDN キャッシュサーバが盗聴された際のトラフィックパタン分析を通じて危険性の評価を行い，提案方式の適用範囲の最適化を検討する．このアプローチにより，全体の要求数に対するログ確認回数を大幅に削減し，OS および LDNS サーバへの負荷軽減にさらに貢献できると考えている．

謝辞

本研究成果は JSPS 科研費 23K21664, 23K21665, 23K28078 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 Surveys & Tutorials, Vol. 23, No. 4, Fourth Quater 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/cyb-ersecurity/vulnerability-assessment/blog/ddos-attack/

[5] D. Wagner, D. Kopp, M. Wichtlhuber, C. Dietzel, O. Hohlfeld, G. Smaragdakis, and A. Feldmann, United We Stand: Collaborative Detection and Mitigation of Amplification DDoS Attacks at Scale, ACM CCS 2021

[6] D. Gillman, et al., Protecting Websites from Attack with Secure Delivery Networks, Comp. Mag, 2015

[7] T Taniguchi and N. Kamiyama, Two-Level Detection Method of DDoS Attack Mimicking CDN Caches, ICOIN 2025

[8] 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

[9] T. Vissers, et al., Maneuvering Around Clouds: Bypassing Cloud-based Security Providers, ACM CCS 2015