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

信学技報
TECHNICAL REPORT OF IEICE.

階層型CDNに対するリアルタイム最適キャッシュ汚染攻撃

劉　　甲奇† 　上山　憲昭††

† 立命館大学 情報理工研究科
〒567–0876 大阪府茨木市岩倉町 2-150
†† 立命館大学 情報理工学部
〒567–0876 大阪府茨木市岩倉町 2-150
E-mail: †is0705vf@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

あらまし　コンテンツ配信ネットワーク（CDN）は，冗長なトラフィックをフィルタリングし，オリジンサーバを保護するために，階層的なキャッシュアーキテクチャに大きく依存している．しかし，このようなトラフィックの局所性への依存は，キャッシュ汚染攻撃（CPA）に対する根本的な脆弱性を生み出す．従来の CPA は静的なフラッディング戦略を採用していたが，敵対的な戦略の出現により，従来の防御を回避可能な，適応的かつ最適化された攻撃の脅威が生じている．本稿では，勾配フリーの強化学習を活用し，多階層 CDN の性能限界を探索する新しい敵対的フレームワークを提案する．完全にブラックボックスな環境で動作する本フレームワークは，攻撃を部分観測マルコフ決定過程（POMDP）としてモデル化し，摂動ベースのポリシィ探索アルゴリズムを使用して攻撃トラフィックの分散を最適化する．3 階層 CDN トポロジにおける広範なシミュレーションにより，システムが以前考えられていたよりもはるかに脆弱であることを示す．我々は，毎秒 120 リクエストという控えめな容量を持つ最適化された攻撃で，オリジンサーバを飽和させ，30% を超えるパケットドロップ率を引き起こすのに十分であることを示す．さらに，我々の微視的分析により，2 つの直感に反する連鎖的な障害メカニズムが明らかになった．それは，エッジの障害が人気のあるトラフィックを上流に押し上げる「中間層ホットスポットのバックプレッシャ（Mid-tier Hotspot Back-pressure）」と，リクエスト量の増加がトラフィックの分散により逆にキャッシュ効用の低下を招く「リクエストレートとヒット率の乖離（Decoupling of Request Rate and Hit Ratio）」である．これらの知見は，最も壊滅的な攻撃とは，単に帯域幅を枯渇させるものではなく，キャッシュロジックの統計的基盤を解体するものであることを強調している．
キーワード　CDN, CPA, 階層型キャッシュシステム

Optimum Cache Pollution Attacks on Real-Time Hierarchical CDN

Jiaqi LIU† and Noriaki KAMIYAMA††

† Graduate School of Information Science and Engineering, Ritsumeikan University
2-150 Iwakuracho, Ibaraki, Osaka 567-8570
†† College of Information Science and Engineering, Ritsumeikan University
2-150 Iwakuracho, Ibaraki, Osaka 567-8570
E-mail: †is0705vf@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

Abstract　Content Delivery Networks (CDNs) rely heavily on hierarchical caching architectures to filter redundant traffic and protect origin servers. However, this dependency on traffic locality creates a fundamental vulnerability to Cache Pollution Attacks (CPA). While traditional CPAs employ static flooding strategies, the emergence of adversarial strategy introduces the threat of adaptive, optimized attacks that can bypass conventional defenses. In this paper, we propose a novel adversarial framework that leverages gradient-free reinforcement learning to explore the performance boundaries of multi-tier CDNs. Operating in a strictly black-box environment, our framework models the attack as a Partially Observable Markov Decision Process (POMDP) and utilizes a perturbation-based policy search algorithm to optimize the dispersion of attack traffic. Extensive simulations on a three-tier CDN topology demonstrate that the system is far more fragile than previously understood. We show that an optimized attack with a modest capacity of 120 requests per second is sufficient to saturate the origin server, inducing a packet drop rate exceeding 30%. Furthermore, our microscopic analysis uncovers two counter-intuitive cascading failure mechanisms: Mid-tier Hotspot Back-pressure, where edge failures force popular traffic upstream, and the Decoupling of Request Rate and Hit Ratio, where increased request volume paradoxically leads to lower cache utility due to traffic dispersion. These findings highlight that the most devastating attacks are those that dismantle the statistical foundations of caching logic rather than merely exhausting bandwidth.
Key words　CDN, CPA, Hierarchical Cache System

1. はじめに

コンテンツ配信ネットワーク（CDN）は現代のインターネットのバックボーンとして機能しており，世界的なデータトラフィックの指数関数的な増加に対処するために，階層的なキャッシュアーキテクチャに大きく依存している [1]．多くの場合，ジップ（Zipf）分布によって特徴付けられるユーザリクエストの時間的局所性を利用することで，CDN は大規模なトラフィック急増からオリジンサーバを効果的に保護している [2]．しかし，この局所性への依存は根本的な脆弱性を露呈している．もしリクエストパターンが悪意を持って変更され，局所性が最小化された場合，キャッシュ効率は崩壊する．この種の脅威はキャッシュ汚染攻撃（CPA）として知られ，帯域幅を枯渇させることによってではなく，キャッシュロジック自体を妨害することによってシステム性能を低下させることを目的としている [3].

従来の CPA は通常，ランダムフラッディングや偽の局所性注入といった静的で事前に定義されたパターンを採用していたが，サイバー脅威の状況はより高い知能と適応性へと進化している．強化学習（RL）の出現により，攻撃者はシステム防御に応じて戦略を動的に最適化することが可能になった．これは重要な研究課題を提起する．システムの混雑を最大化するように自律的に学習できる適応的な攻撃者に直面したとき，多階層 CDN の性能限界はどこにあるのか？そしてさらに重要なことに，そのような最適化された攻撃下でシステムを障害に追い込む微視的なメカニズムとは何か？

これらの問いに答えるために，我々は勾配フリーのポリシィ探索アルゴリズムを利用して階層型 CDN の回復力を調査する，新しい敵対的フレームワークを提案する．ターゲットのホワイトボックス知識を仮定する先行研究とは異なり，我々のエージェントは完全にブラックボックスな環境で動作し，観測されたサービス品質（QoS）フィードバックのみに基づいて攻撃戦略を最適化する．我々は攻撃を部分観測マルコフ決定過程としてモデル化し，摂動ベースの最適化手法を用いて，オリジンサーバの遅延とパケットドロップ率を最大化するトラフィック分布を学習する．

3 階層 CDN アーキテクチャにおける広範なシミュレーションにより，システムが以前理解されていたよりもはるかに脆弱であることを明らかにする．我々は，総リンク容量の一部に過ぎない毎秒 120 リクエストという控えめな容量の最適化された攻撃で，オリジンサーバを飽和させ，30% を超えるパケットドロップ率を引き起こすのに十分であることを実証する．攻撃の潜在能力を示すだけでなく，本稿は障害メカニズムの深いフォレンジック分析を提供する．我々は 2 つの直感に反する現象を発見した．エッジの障害が人気のあるトラフィックを上流に押し上げる「中間層ホットスポットのバックプレッシャー」と，トラフィック量の増加が分散によって逆にキャッシュヒット率の低下を招く「リクエストレートとヒット率の乖離」である．これらの知見は，最も壊滅的な攻撃とは，ボリュームでネットワークを氾濫させるものではなく，リクエスト分布の分散（dispersion）を最大化し，キャッシュの統計的基盤を体系的に解体するものであることを示唆している．

2. 関 連 研 究

コンテンツ配信ネットワークのセキュリティは広範な研究の対象となってきたが，主にボリューム型の分散型サービス拒否（DDoS）攻撃とその緩和に焦点が当てられてきた．しかし，キャッシュ汚染攻撃という特定の領域は，より洗練された脅威ベクトルを表している．CPA に関する初期の研究は局所性破壊攻撃に焦点を当てており，攻撃者は人気のないコンテンツリクエストのストリームを生成して有効なキャッシュエントリを追い出す [4]．理論モデルは，そのような攻撃がキャッシュヒット率を大幅に低下させる可能性があることを示しているが，これらの研究は多くの場合，キャッシュの置換ポリシィや動的な負荷変化に適応しない静的な攻撃戦略を仮定している．

より最近の研究では，ネットワークセキュリティにおける敵対的 AI の応用が探求されている．いくつかの研究では，深層強化学習（DRL）を適用して敵対的トラフィックフローを生成しており [5] [6]，主に侵入検知システムの回避やボットネットの調整の最適化の文脈で行われている．しかし，既存の RL ベースの攻撃フレームワークのほとんどは，ターゲット環境の微分可能なモデルを必要とする勾配ベースの手法に依存しており，現実世界のブラックボックスなシナリオではめったに利用できない [7]．本稿は，勾配フリーの 0 次最適化アプローチを採用することで他と一線を画しており，CDN のトポロジや状態に関する内部知識なしに，エージェントが効果的な戦略を学習することを可能にする．

さらに，CPA の影響分析に関して，先行文献は主に全体的なヒット率の低下などの巨視的な指標に焦点を当ててきた [8]．多階層構造内での連鎖的な影響を調査した研究はほとんどない．本稿は，エッジおよび中間層ノード全体でのトラフィックダイナミクスの微視的な分析を提供し，バックプレッシャーの現象とトラフィック分散によって引き起こされるキャッシュスラッシングのメカニズムを明確に特徴付けることで，このギャップを埋める．この粒度の高い視点は，次世代の分布認識型防御メカニズムを設計するための新しい洞察を提供する．

3. 脅威モデルと問題定式化

本節節では，攻撃者の能力と，攻撃者と階層型 CDN アーキテクチャ間の相互作用メカニズムを形式的に定義する．我々は適応的な攻撃戦略を部分観測マルコフ決定過程（POMDP）として枠組み化する．

3.1 攻撃シナリオ

我々は，攻撃者が $\mathcal{N} = \{1, 2, \ldots, N\}$ と表記される N 個の侵害されたエッジノードからなるボットネットを制御する分散型の敵対的設定を検討する．ターゲット CDN は，$\mathcal{M} = \{1, 2, \ldots, M\}$ のコンテンツアイテムセットをホストする．

攻撃者の目的は，トラフィック分布をインテリジェントに調整することで，オリジンサーバでのサービス品質（QoS）の低下を最大化することである．具体的には，攻撃者は平均リクエスト待機時間とパケットドロップ率を増加させることを目指す．しかし，攻撃者はリソースの制約下で動作する．総トラフィック生成能力は，攻撃容量（C_{max}）と呼ばれる最大帯域幅予算によって制限される．攻撃者は，被害を最大化するために，この容量を N 個のノードと M 個のコンテンツアイテム全体に動的に配分しなければならない．

3.2 POMDP 定式化

攻撃者と CDN 環境との相互作用は，タプル $\langle \mathcal{S}, \mathcal{A}, \mathcal{P}, \mathcal{R} \rangle$ で定義される離散時間 POMDP としてモデル化される．

3.2.1 状態空間 ($\mathcal{S}$)

攻撃者はネットワークエッジで動作するため，CDN の内部状態は直接観測できない．エージェントは外部からのフィードバックに依存する必要がある．タイムステップ t において，観測された状態 S_t は，前の時間枠 $[t-1, t)$ の間に観測されたターゲットオリジンサーバの QoS フィードバックから構築される．状態ベクトルは次のように定義される．

$$S_t = \{W_{t-1}, D_{t-1}\} \tag{1}$$

ここで，W_{t-1} は平均リクエスト待機時間を表し，D_{t-1} はリクエストドロップ率を示す．これら 2 つの指標は，ターゲットシステムの混雑レベルの代理指標（プロキシ）として機能する．

3.2.2 行動空間 ($\mathcal{A}$)

行動はトラフィック分布ポリシィを定義する．時間 t において，行動 $\mathbf{A}_t$ は $N \times M$ 行列として表され，各要素 $a_{i,j}$ はノード i がコンテンツ j をターゲットとして生成するトラフィックレートに対応する．

攻撃をステルス性を保ち，物理的な帯域幅制約を遵守させるために，我々は潜在的パラメタ化手法を採用する．$\boldsymbol{\theta}_t \in \mathbb{R}^{N \times M}$ を潜在ポリシィパラメタ行列とし，これは最適化アルゴリズムにおける解ベクトルに対応する．実際の行動行列 $\mathbf{A}_t$ は，$\boldsymbol{\theta}_t$ にソフトマックス関数を適用し，攻撃容量でスケーリングすることによって導出される：

$$\mathbf{A}_t = C_{max} \cdot \mathrm{Softmax}(\boldsymbol{\theta}_t) \tag{2}$$

ここで，ソフトマックス関数はすべての $N \times M$ ペアの平坦化されたベクトルに対して適用され，以下を保証する．

$$\sum_{i=1}^{N}\sum_{j=1}^{M} a_{i,j}^{(t)} = C_{max} \tag{3}$$

この定式化により，総攻撃トラフィックが一定かつ C_{max} によって制限されることが保証される一方で，トラフィックの分布は学習されたポリシィに基づいて動的にシフトする．

3.2.3 報酬関数 ($\mathcal{R}$)

報酬関数は，強化学習エージェントを最も損害を与える戦略へと導くために重要である．我々は報酬 R_t を，オリジンサーバの性能低下の複合指標として定義する．遅延の増加とパケットドロップの誘発を同時に動機付けるために，我々は以下の非線形報酬関数を提案する．

$$R_t = W_t \times (1 + D_t) \tag{4}$$

この設計には，2 段階のインセンティブメカニズムが組み込まれている．

（1） **遅延フェーズ:** システムが軽負荷の場合（$D_t \approx 0$），報酬は主に W_t によって駆動される．エージェントは，キャッシュミスを引き起こし，処理時間を増加させるリクエストパターンを見つけるように促される．

（2） **飽和フェーズ:** 攻撃がシステムを限界点まで押し上げることに成功すると（$D_t > 0$），係数 $(1 + D_t)$ が乗数として作用する．これにより報酬が大幅に増幅され，エージェントがシステムを崩壊および高パケット損失の状態に維持するための強力な勾配を提供する．

4. 提案フレームワーク

本節節では，提案するフレームワークについて詳述する．まず，攻撃者がブラックボックス環境で効果的な戦略を学習できるようにする勾配フリー最適化アルゴリズムを紹介する．次に，階層型 CDN のダイナミクスをシミュレートするために使用される確率的トラフィック生成モデルについて説明する．

4.1 勾配フリーポリシィ探索アルゴリズム

報酬関数の明示的な勾配 $\nabla_\theta R(\theta)$ にアクセスできない CDN のブラックボックスな性質を考慮し，我々は 0 次最適化アプローチを採用する．具体的には，摂動ベースの確率的山登り法（Stochastic Hill Climbing）を利用して，高次元の行動空間を探索する．

アルゴリズムの核となるのは，反復的な「摂動観測（Perturb-and-Observe）」プロセスである．攻撃者は，トラフィック分布の正規化されていないロジットを表す潜在ポリシィベクトル $\theta \in \mathbb{R}^{N \times M}$ を保持する．各タイムステップ t において，エージェントは現在のポリシィにガウス摂動ノイズ $\epsilon_t \sim \mathcal{N}(0, \sigma^2\mathbf{I})$ を加えることで局所的なポリシィランドスケープを探索し，候補ポリシィ $\tilde{\theta}_t = \theta_{t-1} + \epsilon_t$ を生成する．

この潜在的な候補を物理的に実現可能な攻撃トラフィック行列 $\mathbf{A}_t$ に変換するために，総攻撃容量 C_{max} でスケーリングされたソフトマックス正規化を適用する．これにより，生成されたトラフィックが帯域幅の制約を厳密に遵守しながら，異なるコンテンツアイテム間で動的に焦点を移動することが保証される．

$$\mathbf{A}_t = C_{max} \cdot \frac{\exp(\tilde{\theta}_t)}{\sum_{i,j} \exp(\tilde{\theta}_t)_{i,j}} \tag{5}$$

$\mathbf{A}_t$ を実行すると，エージェントはシステムフィードバック S_t を観測し，報酬 $R_t = W_t(1 + D_t)$ を計算する．ポリシィの更新は貪欲選択メカニズムに従う．候補ポリシィは，過去最高報酬（R_{best}）よりも高い報酬をもたらす場合にのみ採用され，この論理分岐は形式的に次のように表される．

$$\theta_t = \begin{cases} \theta_{t-1} + \eta \cdot \epsilon_t & \text{if } R_t > R_{best} \\ \theta_{t-1} & \text{otherwise} \end{cases} \tag{6}$$

ここで，η は学習率である．このメカニズムは，微分可能な環境モデルを必要とせずに勾配方向を効果的に推定し，攻撃者が最大の混雑を引き起こすトラフィックパターンに適応的に収束することを可能にする．本手順をアルゴリズム 1 にまとめる．

Algorithm 1 確率的山登り法による適応型攻撃戦略

Require: 攻撃容量 C_{max}, 学習率 η, 摂動スケール σ
Ensure: 最適化された攻撃分布 $\mathbf{A}$

ポリシィ初期化 $\theta \leftarrow \mathbf{0}$, 最高報酬 $R_{best} \leftarrow -\infty$
loop
  摂動: ノイズ $\epsilon \sim \mathcal{N}(0, \sigma^2\mathbf{I})$ をサンプリング
  行動生成: $\tilde{\theta} \leftarrow \theta + \epsilon$
  $\mathbf{A} \leftarrow C_{max} \cdot \mathrm{Softmax}(\tilde{\theta})$
  実行: CDN に $\mathbf{A}$ を適用し，フィードバック W_t, D_t を観測
  評価: $R_t \leftarrow W_t \times (1 + D_t)$
  更新:
  if $R_t > R_{best}$ **then**
    $\theta \leftarrow \theta + \eta \cdot \epsilon$
    $R_{best} \leftarrow R_t$
  end if
end loop

4.2 確率的トラフィックモデリング

現実的なトラフィックモデリングは，階層型キャッシングの堅牢性を評価するために不可欠である．我々は，異なる確率過程を使用して，正当なユーザ行動と敵対的トラフィックの間の相互作用をシミュレートする．

正当なトラフィック（Benign Traffic）: 正当なユーザリクエストは，Web トラフィックに典型的な強い時間的局所性を反映するようにモデル化される．ジップ分布を仮定し，k 番目に人気のあるコンテンツのリクエスト確率を $P(k) \propto k^{-\alpha}$ で与え．実験では歪度パラメタを $\alpha = 1.2$ に設定する．この高い値は，効率的なキャッシング（「80/20 の法則」）が行われているシナリオをシミュレートしており，破壊が困難な堅牢なベースライン防御を作成する [9]．リクエストの到着時間はレート λ_{benign} のポアソン過程に従い，到着間隔が指数分布になるようにする．

攻撃トラフィック（Attack Traffic）: 単純な周期性やボリュームの異常に基づく検出メカニズムを回避するために，各ノードによって生成される攻撃トラフィックもポアソン過程に従う．ただし，正当なトラフィックとは異なり，各攻撃フローのレートパラメタは，前節で導出された行動行列 $\mathbf{A}_t$ の要素 $a_{i,j}$ によって動的に制御される．固定レートのバーストを送信するのではなく，これらのポアソンストリームのレートを変調することで，攻撃者は敵対的リクエストを背景ノイズに紛れ込ませ，単にネットワークを氾濫させるのではなく，総トラフィックの統計的特性（例：全体的なジップパラメタの低下）をターゲットにする．

5. 数値評価の環境

本節では，攻撃フレームワークを評価するために構築されたシミュレーション環境について詳述する．実験設計は，階層的でリソース制約のある CDN アーキテクチャに焦点を当てており，特に敵対的ストレス下での多階層キャッシング調整の脆弱性を露呈するように調整する．

5.1 トポロジとネットワークアーキテクチャ

単一のオリジンサーバ，3 台の中間層サーバ（Mid-tier），および 15 台のエッジサーバで構成される 3 階層コンテンツ配信トポロジをモデル化する．現実世界のネットワークに固有の構造的不均質性を反映するために，階層間の接続は非対称に分散されている．3 台の中間層サーバ（A，B，C とラベル付け）は，エッジノードの異なるクラスタにサービスを提供する．中間サーバ A は 3 台，中間サーバ B は 5 台，中間サーバ C は 7 台のエッジサーバに接続する．この構成は不均等な負荷分散の可能性を生み出し，中間サーバ C は本質的により高い総トラフィック圧力に直面するため，このようなトポロジ上のボトルネックを特定して悪用する攻撃者の能力を評価する．

5.2 サーバ仕様とトラフィックダイナミクス

システムは，高負荷の本番環境をシミュレートするために，厳格な処理制約の下で構成されている．階層内のすべてのサーバ（エッジ，中間，オリジン）は，毎秒 200 リクエストのサービスレート（μ）で標準化されている．しかし，それらのストレージの役割は大きく異なる．15 台のエッジサーバはそれぞれ，10 アイテムの制限された容量を持つ一時的なキャッシュとして動作する．同様に，3 台の中間層サーバは，30 アイテムの容量を持つ中間キャッシング層として機能する．両方の層は，CDN で広く使用されている LRU（Least Recently Used）置換ポリシィを用いる [10]．対照的に，オリジンサーバはコンテンツ全体のユニバース（$M = 100$）の恒久的なリポジトリとして機能する．利用可能なすべてのコンテンツアイテムを保存するため，キャッシュ置換メカニズムやストレージ制限の対象にはならない．その主な制約は，ストレージ容量ではなく処理帯域幅である．

混雑を管理するために，すべてのサーバは最大容量 $L_{max} = 1000$ リクエストの先入れ先出し（FIFO）キューを維持する．システムは「ドロップテール」ポリシィの下で動作し，キューが満杯のときに到着したリクエストは即座に破棄され，パケットドロップ率指標（D_t）に寄与する．コンテンツ集合は，均一なサイズの $M = 100$ 個のユニークなアイテムで構成される．正当なユーザトラフィックは，各エッジサーバで毎秒 60 リクエストの到着率（λ_{edge}）を持つポアソン過程に従って生成される．これらのコンテンツの人気度は，歪度パラメータ $\alpha = 1.2$ のジップ分布に従う．この高い歪度は，少数の人気コンテンツがリクエストの大部分を占めることを意味し，通常の状態ではキャッシングが非常に効果的なシナリオを作成する．

5.3 システム負荷分析

この設定の重要な側面は，エッジとオリジンの間の意図的なリソースの不一致である．15 台のエッジサーバによって生成される総リクエストレートは，合計で毎秒 900 リクエスト（15×60）になる．オリジンサーバのサービス能力が毎秒 200 リクエストに制限されていることを考慮し，システムが効果的なキャッシングなしでは持続不可能になるように設計する．多階層アーキテクチャは，オリジンの飽和を防ぐために，着信トラフィックの少なくとも 78% を正常にフィルタリングしなければならない．この脆弱性により，システムはキャッシュ汚染攻撃の理想的なテストベッドとなる．キャッシュヒット率のわずかな低下でさえ，連鎖的な混雑とサービス拒否を引き起こす可能性があるためである．

強化学習エージェントは，$\Delta t = 10$ 秒の離散時間スロットでこの環境と相互作用し，パフォーマンス指標がポリシィ更新のために集計される前に，キューのダイナミクスが安定するのに十分な時間を確保する．主なシミュレーションパラメタを表 1 にまとめる．

表 1: シミュレーションパラメタの設定値

パラメータ	値
総コンテンツアイテム数 (M)	100
ジップ歪度パラメータ (α)	1.2
タイムスロット期間 (Δt)	10 秒
キュー容量制限 (L_{max})	1000 リクエスト
エッジ層 *(15 ノード)*	
到着率 (λ_{edge})	60 req/s
サービスレート (μ_{edge})	200 req/s
キャッシュ容量	10 アイテム (10%)
中間層 *(3 ノード)*	
トポロジ分布 (A, B, C)	3, 5, 7 接続
サービスレート (μ_{mid})	200 req/s
キャッシュ容量	30 アイテム (30%)
オリジン層 *(1 ノード)*	
サービスレート (μ_{origin})	200 req/s
ストレージ容量	全コンテンツ (制限なし)

6. 数 値 評 価

本節では，最適化された攻撃戦略下でのシステムの挙動を分析することにより，攻撃フレームワークの性能を評価する．特に攻撃容量が 120 req/s のシナリオに焦点を当て，巨視的なサービス品質指標と微視的なキャッシュ状態を対照群（攻撃なし）と比較する．

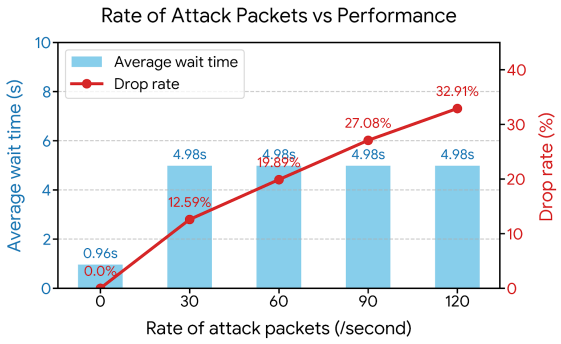


図 1: 平均待機時間とドロップ率に対する攻撃強度の影響: 120 req/s で，ドロップ率は 32.91% に達し，待機時間はキューの制限（$\approx 5s$）で飽和．

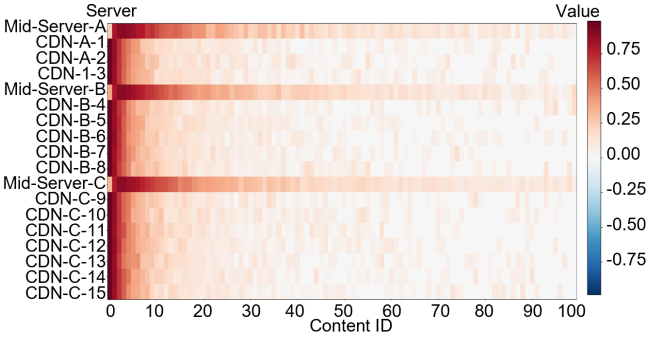
6.1 全体的な影響分析

図 1 に，攻撃者のシステム全体への攻撃強度 (1 秒あたりの攻撃パケット数) に対して，平均待機時間と要求のドロップ率をプロットする．攻撃が発生しない場合，システムは平均待機時間約 0.96 秒，パケットドロップゼロで健全に動作しており，LRU

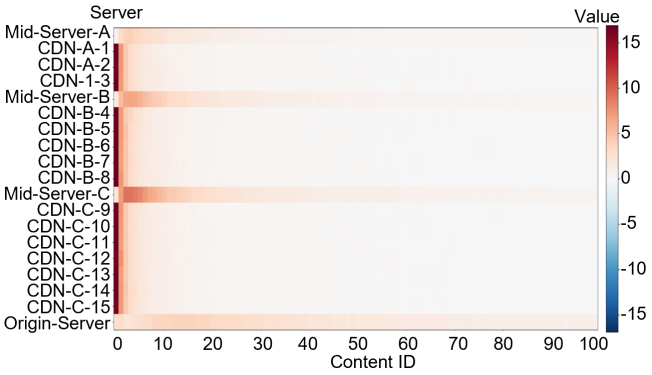
キャッシング戦略が通常のジップ分布下で 900 req/s の総エッジトラフィックを効果的にフィルタリングしていることを確認できる．しかし，攻撃容量が増加するにつれて劇的な低下が観察される．攻撃強度が 120 req/s において，平均待機時間は即座に 4.98 秒に飽和し，理論上のキュー制限（1000 req/200 req/s = 5s）に近づく．同時に，ドロップ率は線形に上昇し，32.91% に達する．この飽和は，攻撃が正当なトラフィックをハイジャックすることに成功し，オリジンサーバに到着する総量が攻撃者自身の注入レートをはるかに超える原因となっていることを示しており，単なる帯域幅の消費ではなく，キャッシュ障害の増幅効果によって損害が引き起こされていることを示している．

6.2 キャッシュダイナミクスの分析

CDN の飽和現象を促進するメカニズムを理解するために，攻撃が発生していない状態と攻撃状態を比較し，攻撃強度とキャッシュヒット率の分布を分析する．



(a) キャッシュヒット率

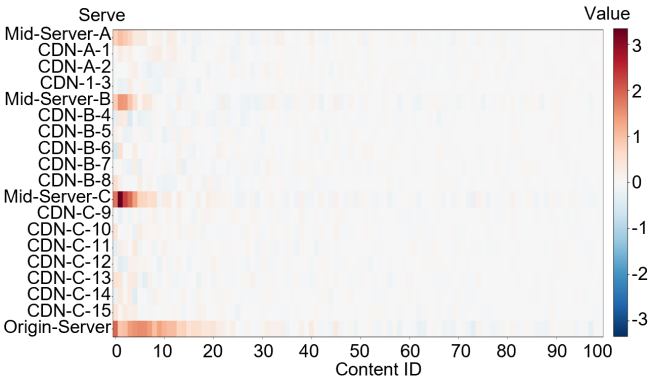


(b) リクエスト入力レート

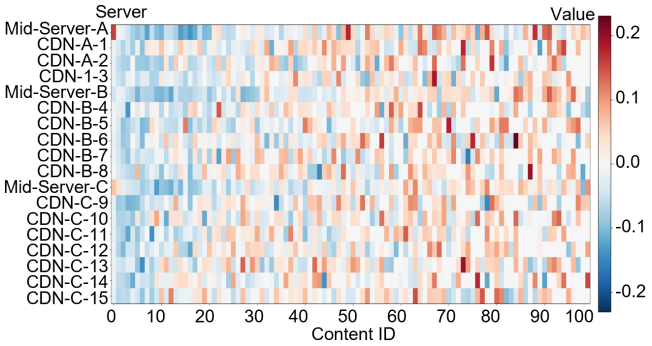
図 2: 正常時のシステム状態: 人気コンテンツはエッジで効率的にキャッシュされ，バックエンドを保護

図 2 に，横軸にコンテンツの人気順位を，縦軸に各キャッシュサーバ別に，各コンテンツの CPA が生じていない正常時の，各キャッシュサーバにおける (a) キャッシュヒット率と (b) 要求到着レートを，値の大小に応じて色を変えて表示することで，これら指標の値の大小を可視化する．システムはエッジサーバで人気コンテンツに対して高いヒット率を示す．その結果，トラフィックの大部分はエッジで吸収され，中間サーバとオリジンサーバには最小限の入力負荷しかかからない．これは，高局所性トラフィックの処理における多階層 LRU アーキテクチャの有効性を実証している．

しかし CPA 発生時は，この状況は劇的に変化する．図 3 に，CPA 発生時の，これら指標の変化（$Value_{attack} - Value_{control}$）を同様に可視化する。中間層，特に 7 つのエッジノードとオリジンサーバに接続する中間サーバ C において，リクエスト量の大規模な急増が観察される．中間サーバ C 上のコンテンツ ID 0-5 に対応する濃い赤色の帯は，人気コンテンツのリクエストが上流に漏洩していることを示している．同時に，ヒット率の差分マップは，中間層でこれらの人気アイテムのヒット率が大幅に低下していることを示している．この入力の増加とヒット率の低下の組み合わせは，キャッシュロジックの根本的な混乱を示している．



(a) 入力レートの変化



(b) ヒット率の変化

図 3: 攻撃下（120 req/s）のシステム状態: 青は減少，赤は増加を表し，中間サーバ C での大規模なトラフィック急増とヒット率低下が発生

6.3 メカニズム分析: 直感に反する現象

ヒートマップの観察に基づき，CPA を特徴付ける 2 つの直感に反する現象を特定し説明する．

6.3.1 人気コンテンツの漏洩

直感的には，キャッシュ汚染攻撃は主に「コールド（不人気）」なコンテンツでネットワークを氾濫させると予想される．しかし，前節結果は，最適攻撃を行った際，CDN 階層の中間層において人気コンテンツのリクエストレートが大幅に増加した．この現象はエッジ障害の直接的な副作用であり，攻撃トラフィックはまずエッジサーバで人気コンテンツを追い出し，ローカルヒット率を急落させる．その結果，これらの人気アイテムに対する正当なリクエストはミスとなり，上位のキャッシュサーバに転送される．このプロセスは事実上，ホットスポットをエッジから中間層へ「押し上げ」，上位層が処理するように設計されていない人気トラフィックのバックプレッシャーを生み出す．

6.3.2 リクエストレートとヒット率の乖離

さらに逆説的な観察は，リクエストレートとヒット率の乖離である．中間層での人気コンテンツのリクエストが急増しているにもかかわらず，これらのアイテムのキャッシュヒット率は

大幅に低下しており，高頻度が通常高いヒット率をもたらすという標準的な局所性の原則と矛盾している．この異常は，総トラフィックの分散によって引き起こされる．攻撃者は，低ジップパラメタに相当する，高度に分散されたトラフィックパターンを生成する．これが正当なトラフィックと混在すると，アクティブコンテンツの「ワーキングセット」が劇的に拡大する．LRU ポリシィの下では，人気アイテムが頻繁に到着しても，連続するリクエスト間の間隔が大量のユニークな攻撃リクエストで満たされてしまう．これはキャッシュスラッシングを引き起こし，人気アイテムが挿入直後に追い出されるため，トラフィックがオリジンサーバまで貫通することを余儀なくされる．

7. 議論と示唆

前節で示された結果は，提案フレームワークが階層型 CDN の性能を低下させることに成功することを示している．数値的な指標を超えて，これらの知見はキャッシュ汚染攻撃の本質と現在の防御パラダイムの限界についての深い洞察を提供する．

7.1 攻撃者の視点: ボリュームよりも分散

本稿から得られる重要な教訓は，最適な攻撃ベクトルへのシフトである．伝統的に，サービス拒否攻撃はボリュームの問題と見なされており，ターゲットが処理できる以上のビット/秒で圧倒することを目的としていた．しかし，我々の強化学習エージェントはより巧妙な戦略を発見した．それはリクエスト分布の分散を最大化することである．総入力の実効ジップ曲線を平坦化するような散乱したトラフィックを生成することで，攻撃者はキャッシングアルゴリズムが直面する予測不可能性を最大化する．LRU ポリシィの下では，この高度に分散した状態は最悪のシナリオを表し，安定したワーキングセットを確立することなく，キャッシュにアイテムを継続的に追い出すことを強制する．これは，CDN のようなステートフルなシステムにとって，分散攻撃がボリューム攻撃よりも大幅に費用対効果が高いことを示している．エージェントは，リクエストのパターンをよりランダムで均一にすることで混乱させる方が，単に頻度を増やすよりもはるかに大きな損害を与えることを学習した．

7.2 防御への洞察: レート制限を超えて

提案手法の成功は，従来の防御メカニズムの不十分さを浮き彫りにしている．従来の防御は，ヘビーヒッターや異常に高いレートを持つフローを特定することによって動作するレート制限に依存することが多い．我々の攻撃は，平坦な分布を使用して多数のノードとコンテンツアイテムにトラフィックを分散させるため，単一のフローが典型的なレート制限の閾値をトリガーすることはない．その結果，攻撃はステルス性を保ちながらバックエンドに最大の損害を与える．

ボリュームに依存するのではなく，我々のメカニズム分析は検出のための新しい青写真を示唆している．人気コンテンツのリクエストレートが上昇しているにもかかわらずヒット率が低下するという直感に反する現象は，この攻撃の明確な署名（シグネチャ）として機能する．我々は，将来の防御システムがレートベースから分布認識型の検出に移行すべきであると提案する．防御側は，着信トラフィックのリアルタイムの平坦度またはジップパラメタを監視すべきである．コンテンツ人気度の突然の説明のつかない分散，またはコンテンツ人気度とキャッシュヒット確率の間の乖離は，進行中のキャッシュ汚染攻撃の高信頼度の指標として機能するはずである．

8. 結　　論

本稿では，勾配フリーの強化学習を活用して階層型 CDN の脆弱性境界を探索する適応型攻撃フレームワークを紹介した．我々は攻撃を部分観測マルコフ決定過程としてモデル化し，摂動ベースのポリシィ探索アルゴリズムを利用して，ブラックボックス環境での攻撃戦略を最適化した．広範な計算機シミュレーション評価により，多階層アーキテクチャは標準的なトラフィックに対しては堅牢であるものの，最適化された分布攻撃の下では脆弱性を示すことが明らかになった．我々は，120 req/s という控えめな攻撃容量で，攻撃者がオリジンサーバを飽和させ，30% を超えるパケットドロップ率を引き起こすことができることを実証した．さらに微視的分析により，2 つの重要な連鎖的障害メカニズム，「中間層ホットスポットのバックプレッシャー」と「リクエストレートとヒット率の乖離」が明らかになった．これらの現象は，攻撃がキャッシュ効率に必要な時間的局所性を体系的に解体することによって成功することを確認している．

本稿は，CDN セキュリティ設計に対する警鐘となるものである．攻撃者が静的なフラッディングから知的で適応的な最適化へと進化するにつれ，多階層キャッシングの静的な冗長性はもはや保証された盾ではないことを示している．今後の研究では，本稿で特定された分布の異常に応じてキャッシングポリシィを動的に調整できる適応型防御メカニズムの開発に焦点を当てる予定である．

謝　　辞

本稿は JSPS 科研費（25K03113, 23K28078）の助成を受けたものである．

文　　献

[1] A. K. Pathan, R. Buyya, et al., “A taxonomy and survey of content delivery networks,” Grid computing and distributed systems laboratory, University of Melbourne, Technical Report, vol. 4, no. 2007, p. 70, 2007.

[2] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, “Web caching and Zipf-like distributions: Evidence and implications,” Proc. IEEE INFOCOM’99, vol. 1, pp. 126–134, 1999.

[3] M. Xie, I. Widjaja, and H. Wang, “Enhancing cache robustness for content-centric networking,” *Proc. 2012 IEEE INFOCOM*, pp. 2426–2434, 2012.

[4] H. Park, I. Widjaja, and H. Lee, “Detection of cache pollution attacks using randomness checks,” Proc. 2012 IEEE International Conference on Communications (ICC), pp. 1096–1100, 2012.

[5] A. Hidouri, H. Touati, M. Hadded, N. Hajlaoui, P. Muhlethaler, and S. Bouzefrane, “Q-ICAN: A Q-learning based cache pollution attack mitigation approach for named data networking,” *Computer Networks*, vol. 235, p. 109998, 2023.

[6] N. U. Saqib and S. Isnain, “A Survey on Mitigation of Cache Pollution Attacks in NDN,” Acta Technica Jaurinensis, vol. 18, no. 2, pp. 93–101, 2025.

[7] P.-Y. Chen, H. Zhang, Y. Sharma, J. Yi, and C.-J. Hsieh, “Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models,” Proc. 10th ACM workshop on artificial intelligence and security, pp. 15–26, 2017.

[8] L. Yao, J. Li, J. Deng, and G. Wu, “Detection of cache pollution attack based on federated learning in ultra-dense network,” omputers & Security, vol. 124, p. 102965, 2023.

[9] M. Cha, H. Kwak, P. Rodriguez, Y.-Y. Ahn, and S. Moon, “I tube, you tube, everybody tubes: analyzing the world’s largest user generated content video system,” Proc. 7th ACM SIGCOMM conference on Internet measurement, pp. 1–14, 2007.

[10] S. Podlipnig and L. Böszörmenyi, “A survey of web cache replacement strategies,” ACM Computing Surveys (CSUR), vol. 35, no. 4, pp. 374–398, 2003.