# 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

立命館大学
谷口和也　上山憲昭

# 研究背景(CDNの普及)

- CDN(Content Delivery Network):
  インターネット上でコンテンツを高速かつ効率的に配信するための分散型ネットワーク

- CDNのシェア率: 年々増加傾向
  - CDNの市場規模の成長予測:

  2024年: 199.6億ドル→ 2029年: 424.6億ドルまで成長

- CDN普及の原因
  - オンラインコンテンツの需要の増加
  - モバイルインターネットの普及
  - グローバルなアクセス需要
  - CDNのセキュリティ機能を利用可能

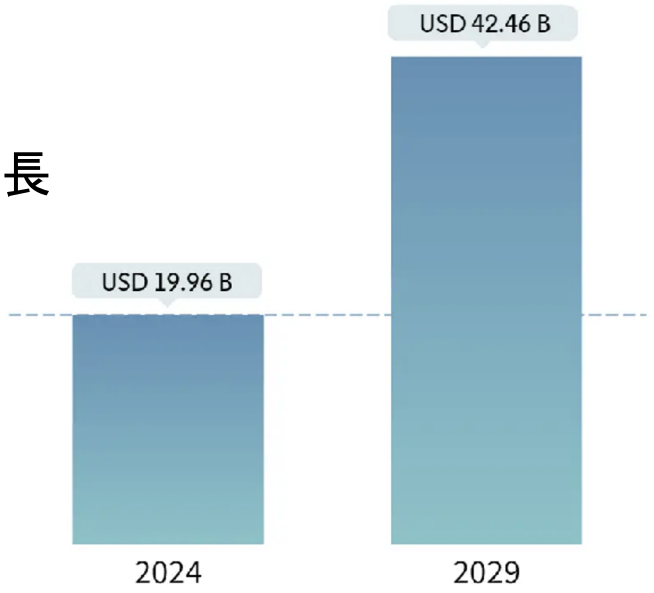



図: コンテンツ配信ネットワークの市場規模と市場規模株式分析 – 成長傾向と成長傾向予測 (2024～2029 年)(Source:mordorintelligence)

# 研究背景(DDoS攻撃の頻繁化)

- DDoS(Distributed Denial of Service)攻撃の頻繁化
  - 攻撃手法の拡散
  - IoTデバイスの脆弱性

  → IPアドレス特定に伴う，OS(Origin Server)への直接攻撃手法の拡大

- CDNを標的とされる事例が存在
  - 2020年6月4日に発生したAkamaiを標的としたDDoS攻撃が発生[1]
    - 攻撃トラフィック量において過去最大級
    - 攻撃トラフィックのピークは1.44 Tbps

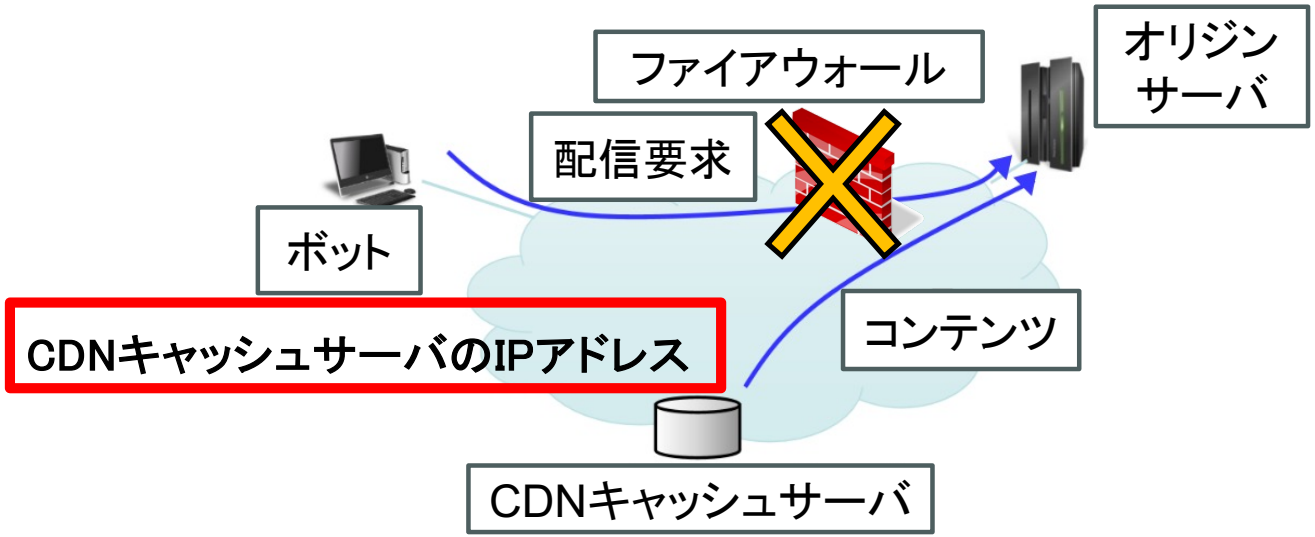
[1] Wagner et al., “United We Stand,” CCS’21, 2021

# 研究課題

- 直接攻撃の可能性
  - 攻撃者が標的サーバのIPアドレスを特定し，特定したIPアドレス宛に直接パケットを送

  → DDoS攻撃が成立
  - CDNキャッシュサーバ以外から到着したパケットはファイアウォールで遮断
- 攻撃者がCDNキャッシュサーバのIPアドレスを発アドレスとして偽る可能性

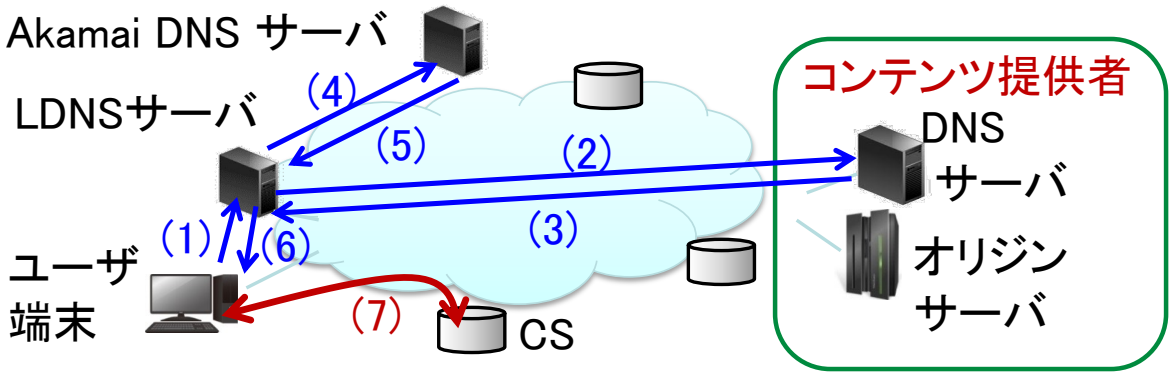
⇒DDoSパケットを送るとファイアウォールで検知不可



# 先行研究(1/2)[2]

- DNSサーバでの名前解決処理でのログの確認により攻撃を検知
  - CSからの正常な問い合わせ時:
    - コンテンツプロバイダのDNSサーバに名前解決のログが残る
  - ボットからのOSのIPアドレスを直接用いた要求:
    - 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

⇒全ての要求に対し，権威DNSのログを確認するとオリジンサーバの負荷が増大




[2] Taniguchi & Kamiyama, “Two-Level Detection Method of DDoS Attack Mimicking CDN Caches,” ICOIN 2025.

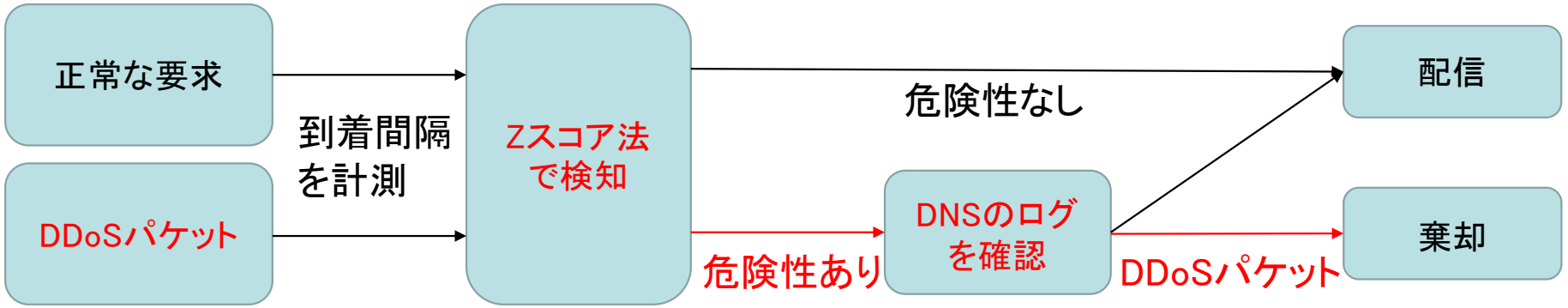
# 先行研究(2/2)

- 二段階検知法
  - 要求発生パターンの違いに着目
    - 正常な配信要求: キャッシュミス時に発生
    - DDoS攻撃: 短い時間間隔で膨大な数が連続して発生

  → 一段階目として，到着間隔に閾値を設定し，危険性を判断

- 異常値検知アルゴリズムであるZスコア法を活用
  - リアルタイムでの閾値設定を可能に

  → 攻撃者のフィルタリング回避のための動的なパケットレート変動に対応



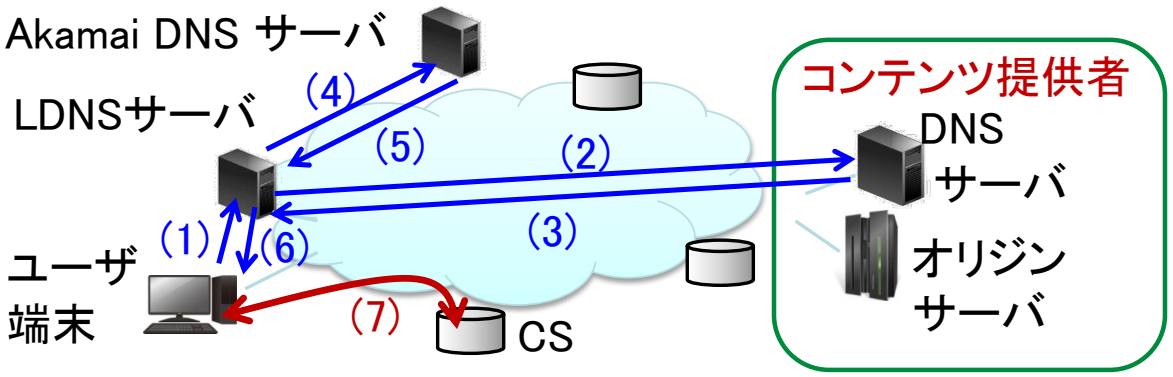
# 先行研究の課題

- 先行研究では，権威DNSサーバでログ確認を実施

- LDNS(Local Domain Name System)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，適切な検知が困難

  → LDNSサーバでログ確認を行うことでキャッシュヒット時におけるログ欠落リスクを回避
  - 都度の確認処理により遅延が発生

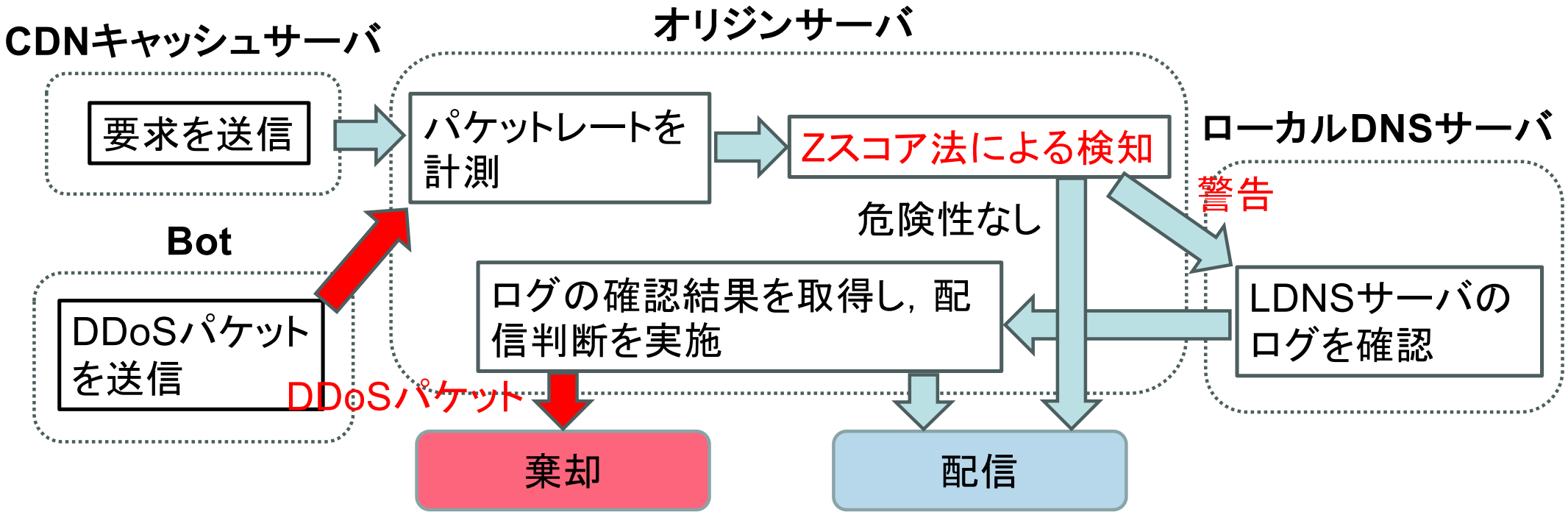
→ LDNSでの確認処理の遅延時間をM/M/1待ち行列から算出し，処理コストを評価



# 提案方式(検知フロー)

- 検知方式としてZスコア法を用いた二段階検知法を使用
- 変更点として，LDNSサーバでのログ確認を実施

→ キャッシュヒット時におけるログ欠落リスクを回避



# 提案方式(処理負荷)

- 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
  → 検知に要する処理遅延が増大
- 遅延時間$T$: 伝搬遅延とメモリアクセス処理での遅延の和
  - 伝搬遅延$T_d$: 1kmあたり5$\mu$秒
    - $d$: 物理的距離（東京都と福岡県を想定した場合: 約1,000km）

$$T = 5 \times 10^{-6} d + T_m \qquad (1)$$

- メモリアクセスでの遅延時間$T_m$をM/M/1待ち行列から算出し，処理コストを評価
  - LDNSサーバのログのメモリ検索処理に要する時間

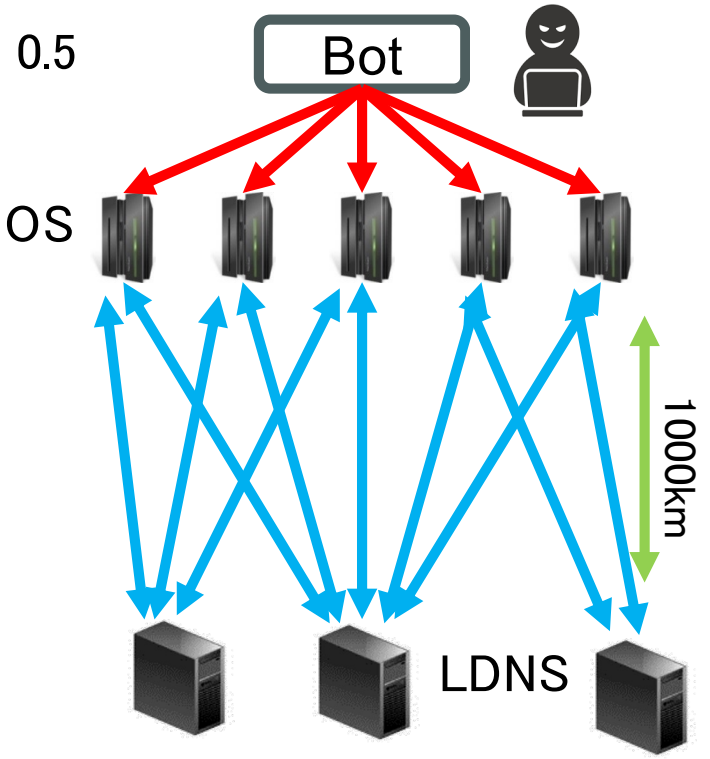
$$T_m = \left( \frac{2}{n \cdot T_r} - \frac{\mathrm{c}}{T_s} \right)^{-1} \qquad (2)$$

- $n$: LDNSサーバのエントリ数
- $c$: LDNSサーバログの確認回数
- $T_r$: 一回のメモリ検索時間
- $T_s$: 攻撃継続時間

# 性能評価

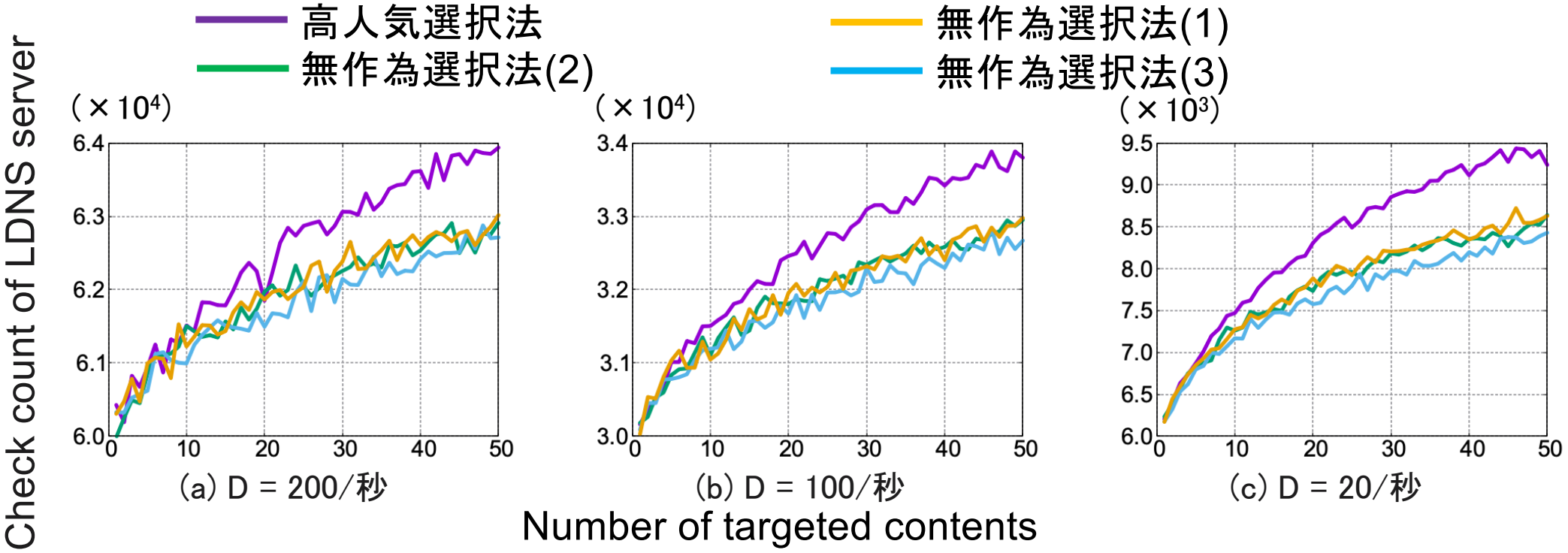
- シミュレーション条件
  - Zスコアのパラメタ: ラグ(L): 10, 閾値($\eta$): 4.0, 影響($\alpha$): 0.5
  - コンテンツ要求のシミュレータの設定

| 項目 | 設定した値 |
|---|---|
| シミュレーション時間 | 100秒 |
| OSの数 | 100個 |
| キャッシュ容量 | 10個 |
| 正常な配信要求の平均発生回数 | 200回 |
| 攻撃を受ける期間 | 50秒経過後30秒間 |
| DDoSパケットの平均発生回数$D$ | 20, 100, 200回 |




- シミュレーションモデル
  - 攻撃者は各OSを標的とし，あるコンテンツを騙ってDDoS攻撃を実施
  - 標的となるコンテンツは特定のLDNSサーバで名前解決を実施
  - 攻撃者は標的コンテンツに一定量のDDoSパケットを分散して送信

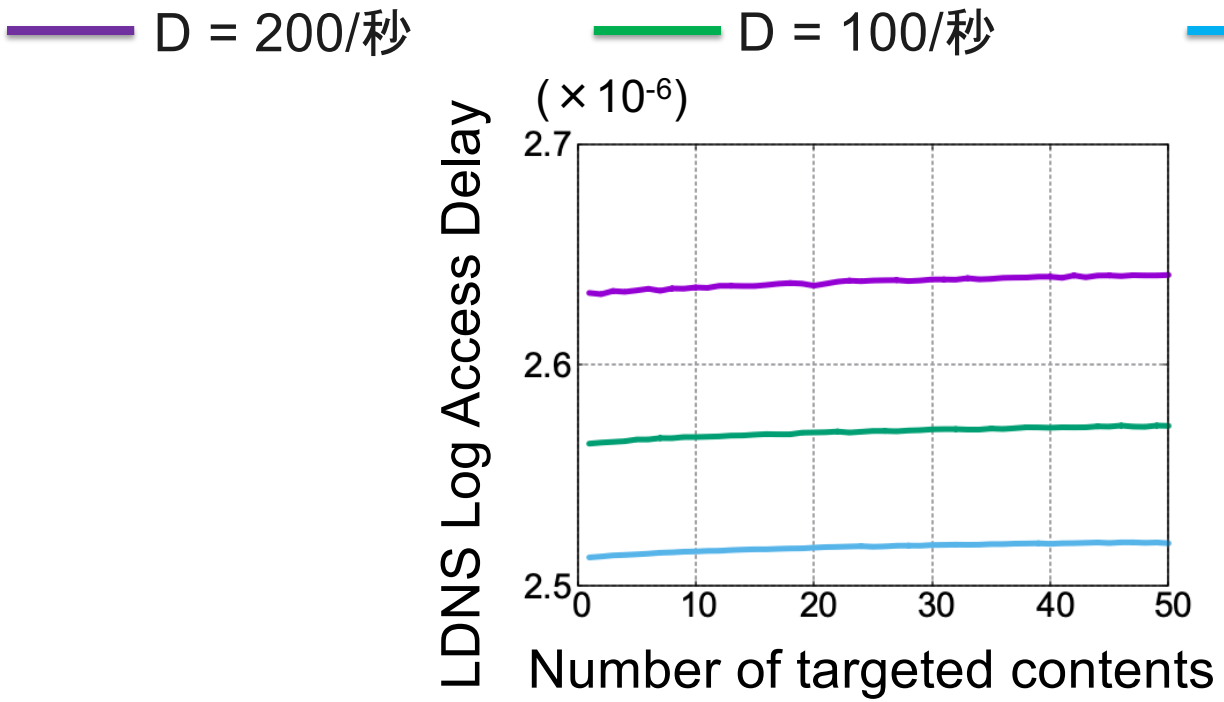
# 性能評価(LDNSサーバのログ検査回数)




- 全ての攻撃レートにおいて，高人気選択法の方がLDNSサーバに対し負荷が高い

→ 提案方式を考慮した攻撃者は高人気選択法で負荷を増加させると推測

# 性能評価(LDNSサーバのログ検査に要する遅延時間)

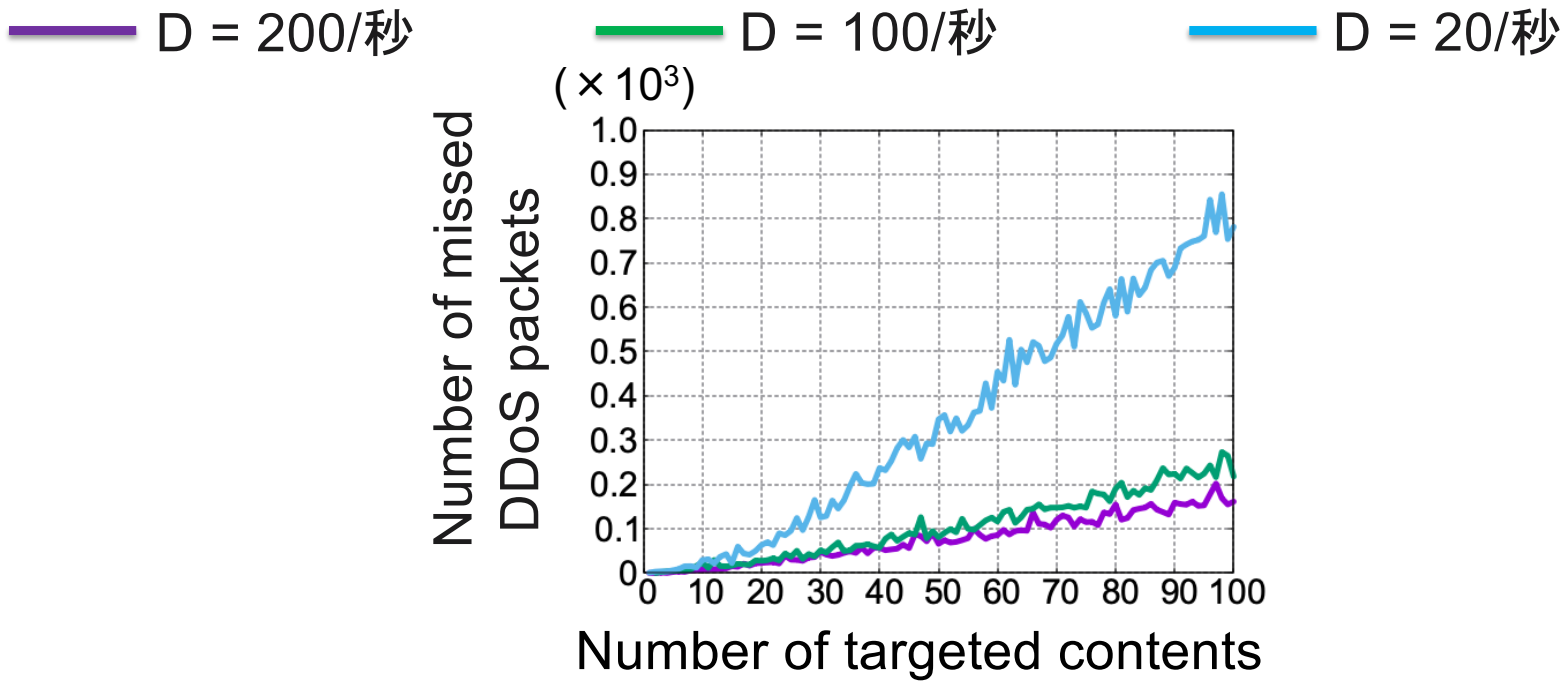



$n$(LDNSサーバのエントリ数)=100
$T_r$(一回のメモリ検索時間)=50ns

- メモリ検索遅延は数マイクロ秒で極めて小さい
  - Ex)東京都と福岡県間の伝搬遅延(約1,000km): 5ms
- 伝搬遅延と比較すると，無視可能な程度

→ 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

# 性能評価(DDoSパケットの見逃し数)




- 標的コンテンツ拡大に伴い，見逃されるDDoSパケット数が増加し，OSの負荷増加
  - 正常パケット数と比較し，OSへの総攻撃成功数は少ない
- 攻撃レートDの減少に伴い，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

# まとめ

- 先行研究で提案されたZスコア法を用いたDDoS攻撃方式への課題に着目
- LDNSサーバでのログ確認を行う方式を提案
- ログ確認に伴う遅延時間は，極めて小さく無視できる程度
- キャッシュヒット時におけるログ欠落リスクを回避しながら，OSの負荷を大幅に軽減可能

- 今後の方針
  - 危険性のあるCDNキャッシュサーバの特定
  - クラスタリングにより，送信元IPアドレスの種類が少なく，異常に高いレートで送信を行うIPアドレスを危険性が高いと判断

  → 提案方式の適用範囲を限定可能で，処理負荷を低減可能