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
CQ2022-23(2022-07)

ICN における Fake 型コンテンツポイズニング攻撃の影響分析

工藤多空飛† 　上山　憲昭††

† 福岡大学 大学院工学研究科
〒 814–0180 福岡市城南区七隈 8–19–1
†† 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: †td212005@fukuoka-u.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

あらまし　コンテンツを効率的に配信するための新しいネットワークアーキテクチャとして情報指向ネットワーク（ICN: information-centric networking）が広く研究されている．しかし，悪意を持ったユーザが正当な名前で偽のコンテンツを大量にネットワークに挿入することでキャッシュの効果を低下させる コンテンツポイズニング攻撃 (CPA: content poisoning attack) の問題が指摘されている．CPA にはその攻撃の性質から四つの型が想定される．CPA に対する対処法を確立するには，CPA がネットワークの性能に与える影響を明らかにする必要があるが，既存研究は限定された CPA 方式を想定しており，その多くが小規模なネットワークトポロジや攻撃者の位置で評価を行っており，汚染コンテンツ数や汚染ノード，攻撃者の位置などが CPA の脅威に与える影響が明らかにされていない．そこで本稿では独自 fake 型の CPA を想定し，大規模なネットワークトポロジで様々な攻撃者の位置で評価を多面的に行うことで，様々な要素が CPA の効果に与える影響を分析し，CPA の脅威を明らかにする．
キーワード　ICN, コンテンツポイズニング攻撃, キャッシュ

Investigating Impact of Fake Type Content Poisoning Attack on ICN

Takuto KUDO† and Noriaki KAMIYAMA††

† Graduate School of Engineering, Fukuoka University
8–19–1, Nanakuma, Jounan, Fukuoka 814–0180
†† College of Information Science and Engineering, Ritsumeikan University
1–1–1, Nojihigashi, Kusatsu 525–08577
E-mail: †td212005@fukuoka-u.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

Abstract　Information-centric networking (ICN) has been widely studied as a new network architecture for efficient content delivery. However, the problem of content poisoning attack (CPA), in which a malicious user inserts a large amount of fake content into the network under a legitimate name, thereby reducing the effectiveness of the cache, has been pointed out. However, existing studies assume a limited number of CPA schemes, and most of them are based on small network topologies and attacker locations, and do not consider the number of contaminated contents, contaminated nodes, and attacker locations. The impact of the number of contaminated contents, contaminated nodes, and attacker locations on the CPA threat has not been clarified. In this paper, we assume a original fake type CPA and analyze the impact of various factors on the effectiveness of CPAs and clarify the threat of CPAs by conducting multifaceted evaluations in a large network topology and at various attacker locations.
Key words　ICN, content availability, original distance

1. はじめに

YouTube などのユーザ生成コンテンツや，映画やドラマなどのコンテンツプロバイダによって生成されたリッチコンテンツを配信することによって生成されるトラフィックは，インターネット上のトラフィックの大部分を占めている．インターネットでは IP アドレスを用いてパケットを転送するため，配信に先立ち配信元となるサーバの IP アドレスをコンテンツの名称から解決するオーバヘッドが発生する．そこでコンテンツをネットワーク (NW) 内のルータでキャッシュし，コンテンツの名称を用いて配信要求 (Interest) を転送し，転送経路上で要求コンテンツを保持しているルータからコンテンツを配信する情報指向ネットワーク （ICN: Information-Centric Networking）が注目され，精力的な研究が進められている [6]．ICN の思想を用いた具体的な NW アーキテクチャとしては，Named Data Networking (NDN) [15] などが提案されている [14]．ICN を用いることで名前解決処理のオーバヘッドを回避し，ユーザに近い位置からコンテンツを配信することで遅延時間や NW 負荷の低減が期待される．

しかし悪意を持ったユーザが正当な名前で偽のコンテンツを大量にネットワークに挿入することでキャッシュの効果を低下させる コンテンツポイズニング攻撃 (CPA: content poisoning attack) の問題が指摘されている [1]．実在するコンテンツの名称で偽りのコンテンツをアップロードすることで，ルータのキャッシュに無意味なコンテンツをキャッシュさせることが可能である．CPA によって正当なコンテンツのキャッシュ配信が減少し，キャッシュの効果が減少するなどの問題がある．CPA は，注入する fake コンテンツなどの攻撃の方法からいくつかの型が想定される．そこで著者らは 4 つの各 CPA タイプを，独自 fake 型，詐称 fake 型，結託 corrupted 型，自然 corrupted 型

と定義した [2]．. CPA に対する対処法を確立するには，CPA がネットワークの性能に与える影響を明らかにする必要があるが，既存研究は限定された CPA 方式を想定しており，その多くが小規模なネットワークトポロジや攻撃者の位置で評価を行っており，汚染コンテンツ数や汚染ノード，攻撃者の位置などが CPA の脅威に与える影響が明らかにされていない [1]．そこで本稿では独自 fake 型の CPA を想定し，大規模なネットワークトポロジで様々な攻撃者の位置で評価を多面的に行うことで，様々な要素が CPA の効果に与える影響を分析し，CPA の脅威を明らかにする．

以下 2 節では CPA の詳細について述べ，3 節では独自 fake 型における fake コンテンツ及びボット (Bot) の配置アルゴリズムについて述べる．そして 4 節では，独自 fake 型における影響分析結果について述べ，最後に 5 節で全体をまとめる．

2. コンテンツポイズニング攻撃

ICN ではコンテンツの正当性を，パケットのヘッダに付与された公開鍵暗号を用いたディジタル署名により判断できる．しかし経路上のルータでは大量のパケットが到着するため，処理負荷が大きく，ディジタル署名による検査が困難である．そのため CPA の検知法としては，コンテンツの要求者 (Subscriber) が受信コンテンツの正当性を検査し，不当コンテンツをルータに通知する方式が提案されている [5]．CPA は，コンテンツと紐づいた公開鍵から生成されたディジタル署名と一致する偽のコンテンツをキャッシュ (CS: content store) に注入する Fake 型と，ディジタル署名と一致しない無意味なコンテンツを CS に注入する Corrupted 型の二つに大別されるが [2]，ディジタル署名により検知可能な CPA は Corrupted 型に限定される．さらにそれぞれにおいて，攻撃者と結託したユーザの有無によって CPA の攻撃方法は四つのタイプを想定することができる．以下にそれぞれについて示す．

独自 *fake* 型: 攻撃者が独自に作成した fake コンテンツを攻撃者の指示に従って Bot から要求することで CS に注入

詐称 *fake* 型: 実在するコンテンツの fake コンテンツを正常な Client からの要求時に配信することで CS に注入

結託 *corrupted* 型: 実在するコンテンツを騙ったディジタル署名と一致しない fake コンテンツを攻撃者の指示に従って Bot から要求することで CS に注入

自然 *corrupted* 型: 実在するコンテンツを騙ったディジタル署名と一致しない fake コンテンツを正常ユーザからの Interest 到着直後に配信することで CS に注入

詐称 fake 型では，攻撃者のコンテンツに Client からの Interest が転送されるよう FIB が設定される．実在する高人気コンテンツの fake コンテンツであるためアクセス数が非常に多く，攻撃の影響が非常に大きいことが予想される．正当な Publisher の公開鍵を管理している CA の職員と結託するなど，公開鍵を攻撃者の公開鍵に書き換えることで本タイプの攻撃が可能である [2]．正当な Publisher の公開鍵を乗っ取って書き換える結果，攻撃者のコンテンツの方が正当化される．

Corrupted 型においては，fake コンテンツはコンテンツに紐づいた公開鍵から生成されたディジタル署名と一致しないため，コンテンツ要求者が署名検証を行うことで容易に検知可能である．そこで本稿では，実現が容易でかつ検知が困難な独自 fake 型に着目し，ICN のキャッシュ方式や NW トポロジ，攻撃者の位置が CPA の効果に与える影響について分析し，CPA の脅威を明らかにする．

3. 配置アルゴリズム

独自 fake 型 CPA においては，fake コンテンツ及び Bot の配置を行う必要がある．独自 fake 型においては，攻撃者が独自に作成した fake コンテンツに Interest を転送するのは攻撃者と結託したユーザ (Bot) のみであり，Interest の転送機会も少ない．そのため独自 fake 型 CPA においては，fake コンテンツ及び Bot の配置が CPA の効果に大きく影響する．しかしこれまでに，fake コンテンツ及び Bot の配置法に関した研究は見られない．そこで本節では，fake コンテンツおよび Bot の配置方式を検討する．fake コンテンツと Bot のうち，先に割り当てるものを先行配置，次に割り当てるものを後続配置と呼ぶ．

3.1 先行配置方式

NW において重要なノードの CS に fake コンテンツが注入されることで，CPA の効果が大きくなることが想定される．そこで NW 内の重要なノードの概念として中心性を考える．具体的には，任意のノードペア間の最短パスの経由数についての指標を表す媒介中心性 (BC: Betweenness Centrality) 及び各ノードが持つリンクの数についての指標を表す次数中心性 (DC: Degree Centrality) に着目し，本稿では fake コンテンツ及び Bot を先に配置する配置方式として，以下の二つを考える．

BC: BC が最大のノードに配置

DC: DC が最大のノードに配置

以後，各配置方式を用いて fake content を配置する場合には BCf および DCf と表記し，Bot を配置する場合には BCb および DCb と表記する．

3.2 後続配置方式

CPA の効果をより大きなものとするために，先に割当てたノードからより遠いノードに fake コンテンツまたは Bot を配置することで，より多くのノードを fake コンテンツが経由することが可能である．そこで本稿では，以下の配置アルゴリズムを提案する [3] [4]．C を配置数とし，$\boldsymbol{N}$ を全ノード集合，$\boldsymbol{U}$ を配置ノード集合，$x(l)$ をリンク l を経由する fake content パス数と定義する．$f(l)$ をリンク重みとし，PC (path count) を考え，$f(l) = 1/x(l)$ に設定する．そして $z(n)$ を $f(l)$ の総和とし，$z(n)$ が最大のノードから順番に配置する．以後，PC を用いて fake content を配置する場合には PCf，Bot を配置する場合には PCb と表記する．

4. 性 能 評 価

4.1 評 価 条 件

4.1.1 ネットワークトポロジ

CAIDA の Web ページで公開されている米国の商用 ISP のうち，At Home Network，Allegiance Telecom の 2 つのバックボーンネットワークトポロジを評価に用いた [10]．図 1，2 に，これら 2 つの NW のトポロジを示す．ネットワーク内の N 個すべての PoP ノードに ICN ルータが設置されているとする．ノード n の人口比，すなわちノード n の人口を全 N 個のノードの人口の総和で除したものを r_n とする．人口比で重みづけたノード間の平均ホップ距離を D とする．

2 つの NW は米国に存在するが，そのトポロジ形状によって，これらを 2 つのタイプに分類する．まず Allegiance Telecom を，多数のノードを接続した少数のハブノードが存在する hub and spoke (H&S) 型に分類する．H&S 型においては，ハブノードを経由することで少数のホップ数で他の目的ノードにパケットは到達することができるため D は小さい．そして At Home Network を，ハブノードが存在しないラダー型に分類する．ラダー型においては，パケットは目的ノードに到達する前に多数の中継ノードを経由する必要があり，D が大きい．

4.1.2 コンテンツ要求

コンテンツ数 M を 10,000 に設定する．Web ページやユーザ生成ビデオなどの様々な種類のデジタルコンテンツの要求数分布は Zipf 分布に従うことが報告されている [11] [12]．例えば Web ページの要求数分布はパラメタ θ が 0.64〜0.83 の，YouTube 動画は約 0.8 の Zipf 分布に従う [12]．そこでコンテンツ m の要求比率 Q_m をパラメタ θ の Zipf 分布で与え，特に明記しない限り $\theta = 0.8$ に設定する [13]．また，fake コンテンツ数 F は 32 もしくは 1024 に設定し，Bot の要求比率 ρ は全要求比率に対して 0.1%から 10%を想定する．以降，特に明記しない限り Bot の要求比率 ρ は 0.1 に設定する．

4.1.3 キャッシュ方式

経由ルータでのコンテンツのキャッシュ判断を行うキャッシュ方式に関し，以下の 3 つの方式を想定する．

AC (AllCache): 発ルータ s から目的ルータ u に至るコンテンツ配信経路 (default path) 上のすべてのルータでキャッシュ [7]

EC (edge cache): default path 上の最終ホップノードでのみキャッシュ [9]

LCD (leave copy down): コンテンツ配信ノードから default path 上の次ホップのルータでのみキャッシュ [8]

4.2 配置結果

fake コンテンツと Bot の両方をランダムに配置した場合 (Random) と，NW 内のホップ長が最大となるノード組に両者を各々配置した場合 (Hop) を，3. 節の配置方式に追加して評価する．ただし各方式の略語は，先行配置，後続配置の順に表記する．例えば先行配置は fake コンテンツを BC を用いて行い，後続配置は Bot を対象に行った場合は，BCf・PCb と表記する．また，fake コンテンツ及び Bot の配置数は各々，1 個ずつとする．Random 及び Hop について，それぞれ 10 組の配置パターンの評価データの平均値を結果として用いる．図 1，2 に，DCf・PCb，DCb・PCf，BCf・PCb，BCb・PCf の 4 つの各配置方式において，NW トポロジごとに，fake コンテンツ (青色) と Bot(赤色) の配置ノードと，fake コンテンツが最も多く注入されたノード (緑色) を示す．ただし fake コンテンツの最大注入ノードは，キャッシュ方式や fake コンテンツ数 F によって異なったため，「キャッシュ配置法 (F)」という形で表記している．fake コンテンツ数が少ない場合は Bot 付近のノード，fake コンテンツ数が多くなるにつれ fake コンテンツのオリジナルが存在するノード付近に，より多くの fake コンテンツが注入される傾向がある．これは F が少ない場合は Bot からの多数の要求が少数の fake コンテンツに集中するため，Bot 近くのノードでキャッシュヒットする可能性が高く，fake コンテンツの提供位置まで Interest が到達しないためである．

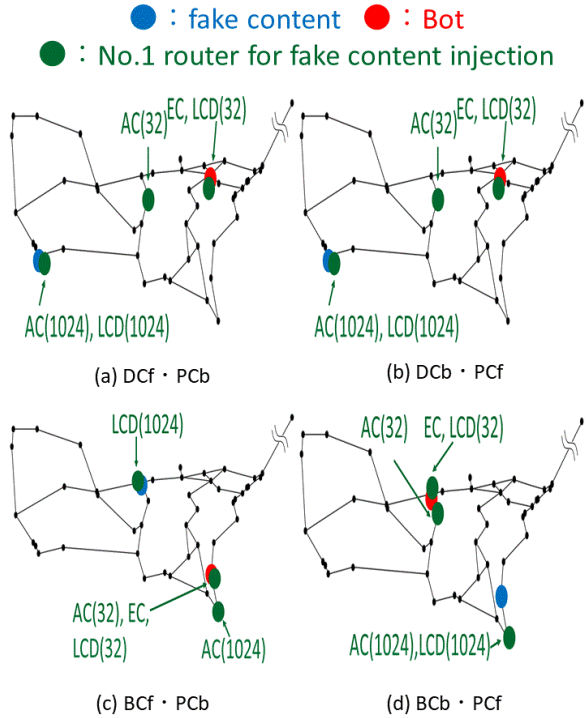

図 1　Placement results in At Home Network

4.3 fake コンテンツ注入数

図 3，4 に fake コンテンツ数 32，1024 個における fake コンテンツ注入数の平均値 (ANFC: average number of fake contents) を示す．EC (edge cache) を用いた場合，fake コンテンツの注入は Bot 配置ノードに限定されるため CPA の効果は小さい．一方，AC (AllCache) を用いた場合，経路上の多数のルータにコンテンツがキャッシュされるため，CPA の効果が大きい．Ladder 型 NW では，F が大きく，多数の fake コンテンツを分散して要求した方が，より多くのノードで多数の fake コンテンツの注入が可能となるが，H&S 型 NW では少数のハブノードを経路が経由することが多く，ハブノードではキャッシュの入れ替えが激しく，fake コンテンツをキャッシュに残すためには少数の fake コンテンツに絞って多数の要求を出す必要がある．そのため F が小さい方が，より多数のノードに多くの fake コンテンツを注入可能である．また DCb・PCf 及び BCb・PCf に従って，先に Bot を，続いて fake コンテンツを配置することで CPA の効果は大きくなる．このように Bot の配置方式がより重要である．また Bot を主要なノードに配置することで，キャッシュの入れ替わりが激しく起こる．そのため Interest がオリジナルまで転送される機会が増え，NW 全体に fake コンテンツを広げることが可能である．一方，fake コンテンツを先に配置した場合，Bot は主要ではないノードに配置されるため，キャッシュの入れ替わりが余り起きず，Bot が存在するノード付近でしか，fake コンテンツを注入できない．

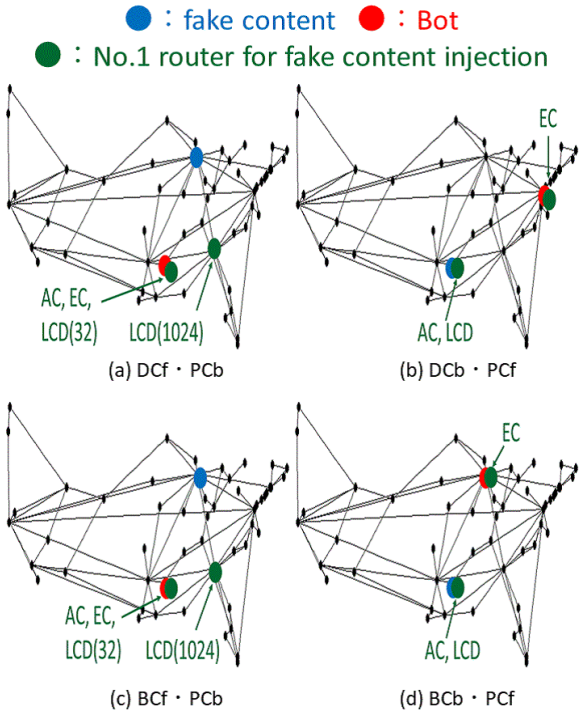

図 2　Placement results in Allegiance Telecom

また，図 5，6 に fake コンテンツ数に対する，平均注入 fake コンテンツ数が 1 位 (rank 1) と 3 位 (rank 3) の各ノードでの ANFC を示す．ただし EC においては rank 3 ノードの ANFC は 0 であったため，グラフを省略している．多くの場合，fake コンテンツ数 F の増加に伴い ANFC は増加するが，多数の fake コンテンツを分散的に Bot から要求することで，Bot からの Interest が fake コンテンツ配置ノードまで到達し，多数のノードに fake コンテンツを注入可能なことが要因と思われる．しかし LCD を用いた場合の rank 3 ノードの ANFC は，F が大きな領域で，F の増加に伴い ANFC が減少する．LCD は Publisher ノードから段階的にキャッシュ位置が Subscriber ノードに近づいていくため，Subscriber の近くのノードで fake コンテンツが注入され，そこから fake コンテンツを取得することで fake コンテンツが拡散しない問題を回避できる．一方で，F が大きいと各 fake コンテンツへの要求数が減少することが要因と思われる．

図 7 から図 10 に，Bot の要求比率 ρ に対し，各 NW トポロジ，各キャッシュ方式，各配置方式において，fake コンテンツ数 32，1024 とした場合の，rank1，3 ノードにおける ANFC を示す．ρ の増加に伴い ANFC は増加するが，図 7(e) の BCf・PCb 方式において，ANFC が減少後，増加する現象がみられる．これは rank1 ノードが fake コンテンツ要求比率の小さい場合と大きい場合とで，異なるためである．図 11 の左側に，ρ が小さい領域で rank1 となったノード 8 と，ρ が大きい領域で rank1 となったノード 33 の，ABFC を ρ に対してプロットする．ノード 8 では ρ が 1%付近から ANFC が減少していき，一方，ノード 33 では増加していることがわかる．BCf・PCb 方式では fake コンテンツを主要ノードに先に割り当てているた

め，rank2 以降のノードではあまり fake コンテンツが注入されず，このような現象がみられる．一方，図 7(f) においては，DCf・PCb 及び BCf・PCb の ANFC が ρ の増加に伴い急激に増加している．rank1 ノードが主要ノードから非主要ノードに置き換わっており，非主要ノードのため，fake コンテンツがキャッシュに残りやすいことが要因である．また，図 8，10 の結果から，Bot の配置が重要であることがわかり，その結果は H&S 型において顕著である．

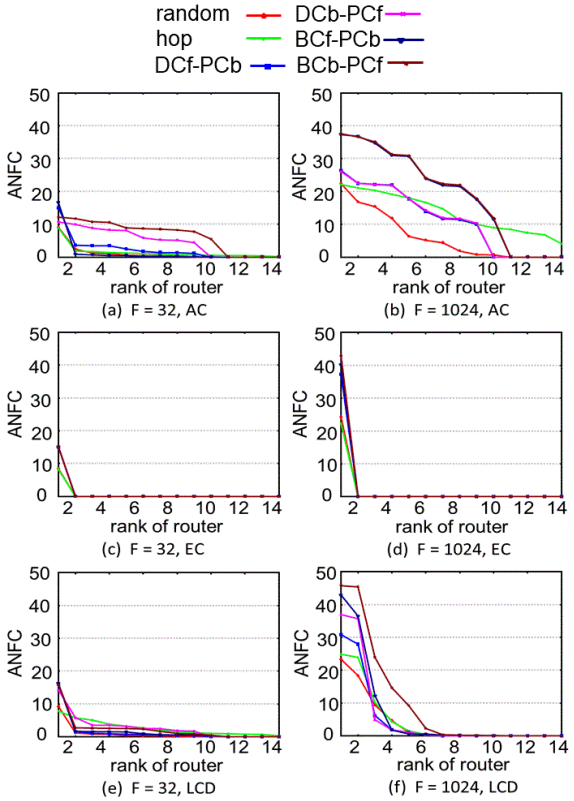

図 3　Average number of fake contents injected at each node in descending order in At Home Network

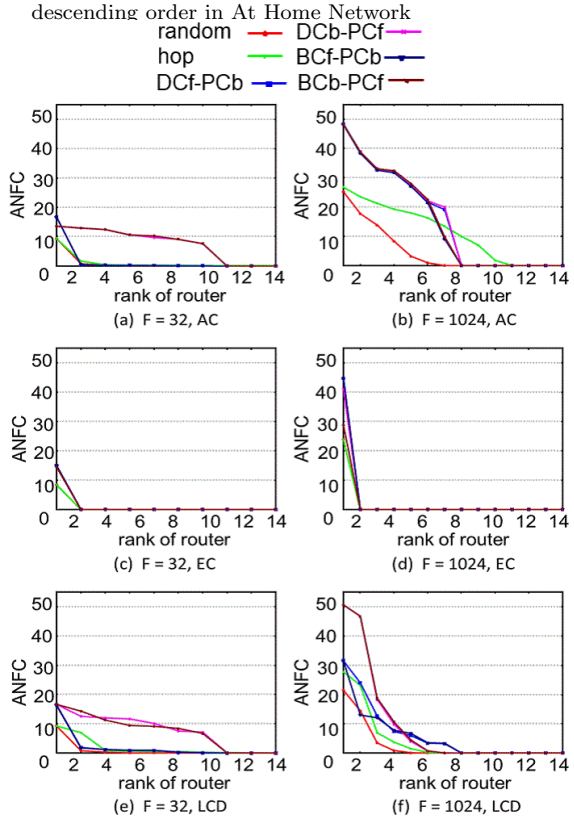

図 4　Average number of fake contents injected at each node in descending order in Allegiance Telecom

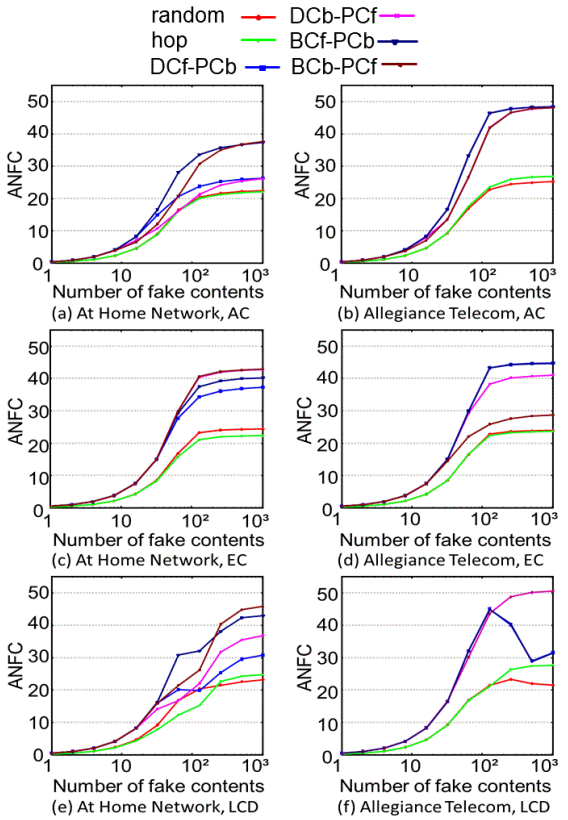

図 5　Average number of fake contents injected at rank 1 router

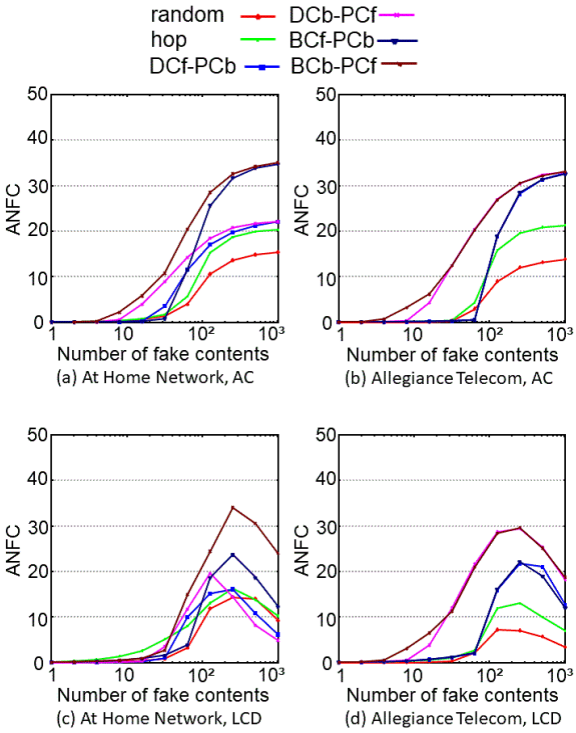

図 6　Average number of fake contents injected at rank 3 router

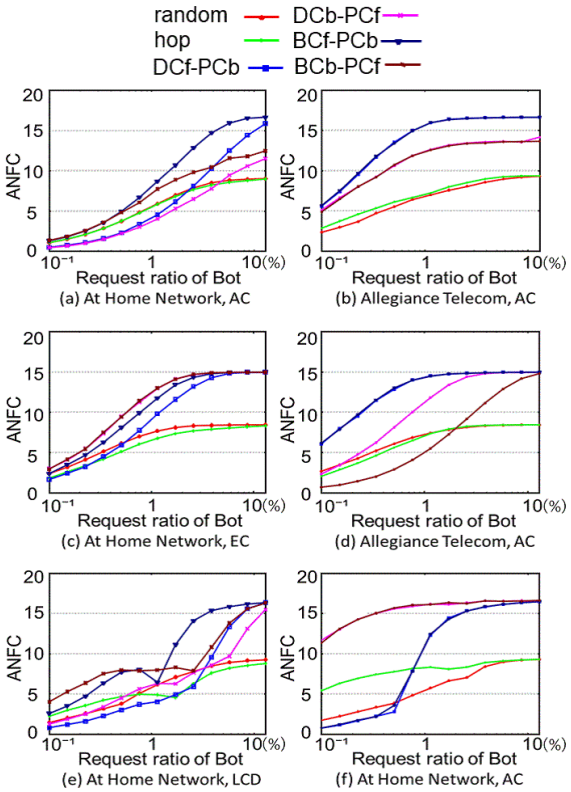

図 7 Average number of fake contents injected at rank 1 routers against request ratio with 32 fake contents

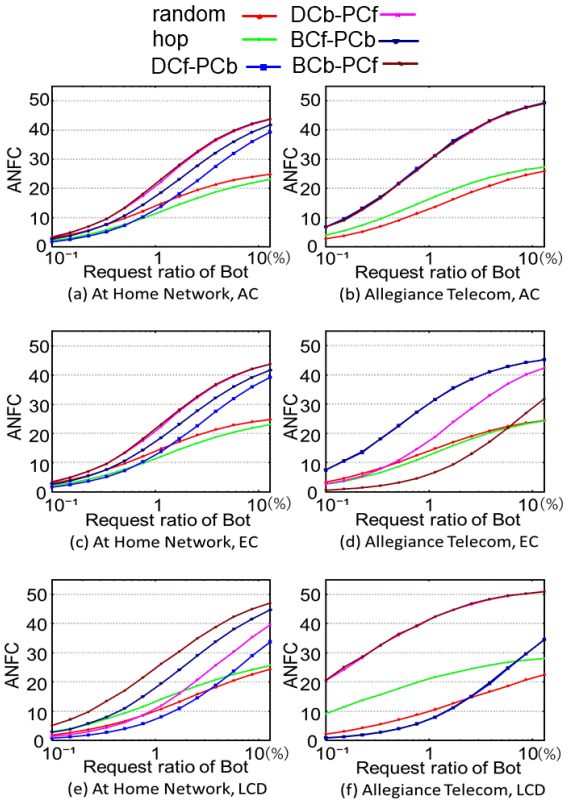

図 9 Average number of fake contents injected at rank 1 routers against request ratio with 1024 fake contents

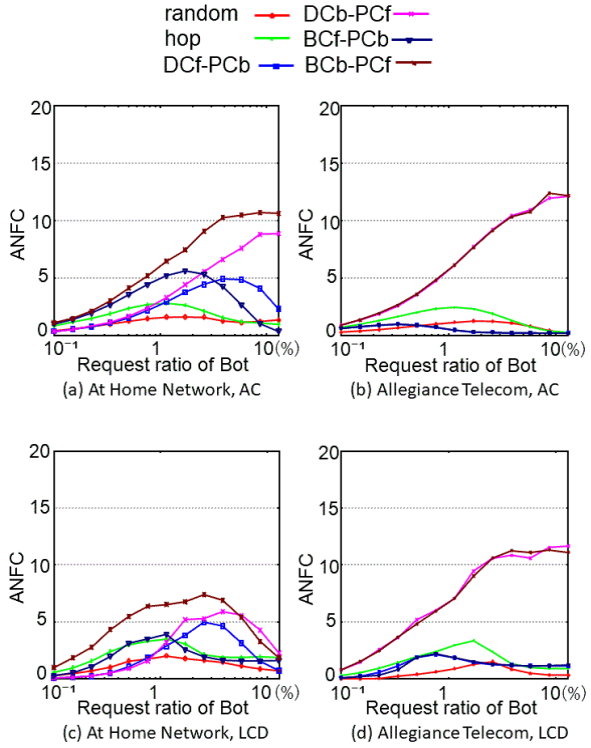

図 8 Average number of fake contents injected at rank 3 routers against request ratio with 32 fake contents

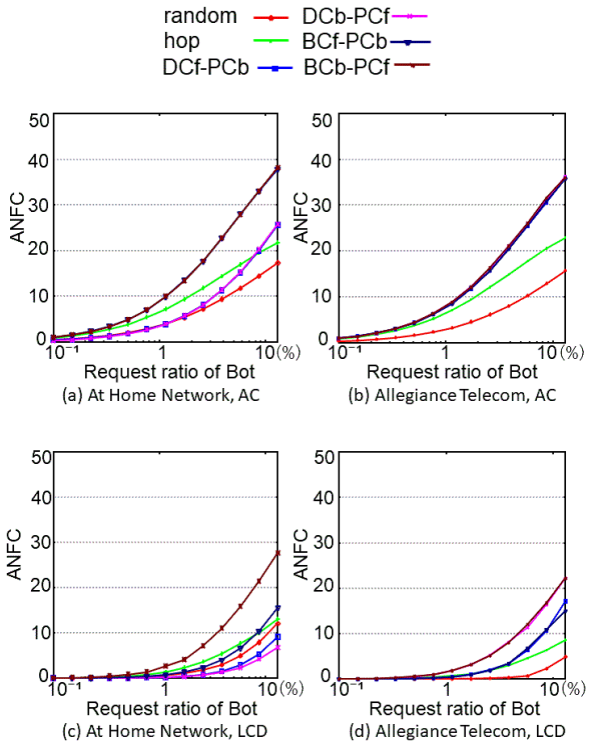

図 10 Average number of fake contents injected at rank 3 routers against request ratio with 1024 fake contents

4.4 キャッシュヒット率

表 1 から表 4 に各 NW トポロジ，各配置方式，各キャッシュ方式において，ANFC が 1 位から 3 位のノードにおけるローカルキャッシュヒット率の変化率を示す．ただしローカルキャッシュヒット率を，対象となるノードに到着した正常コンテンツに対する Interest 数のうち，そのノードに要求コンテンツが

キャッシュされていた割合と定義する．表 1，3 より，Bot を DC または BC 方式で先に割当て，fake コンテンツを PC 方式で配置することで fake コンテンツ数が少ない場合でも rank1 だけではなく，rank2，rank3 ノードにおけるローカルキャッシュヒット率を大きく低減させることが確認できる．一方，fake コンテンツ数が多い場合，Bot の配置が重要ではなく，主要なノードに fake コンテンツや Bot を割当てていることが重要となる．これは fake コンテンツへの Interest が分散され，Interest がオリジナルまで転送される機会が増加するためである．表 4 では，Hop 配置方式においても，rank1 ノードでのローカルキャッシュヒット率が大きく低減している．これは NW トポロジ内の最も主要ではないノードに fake コンテンツが注入されており，キャッシュの入れ替わりが頻繁に起こらないことが要因だと考えられる．従って，ローカルキャッシュヒット率への影響は大きいが，NW 全体の影響としては小さく，これは先行配置方式が DC，BC の場合も同様である．

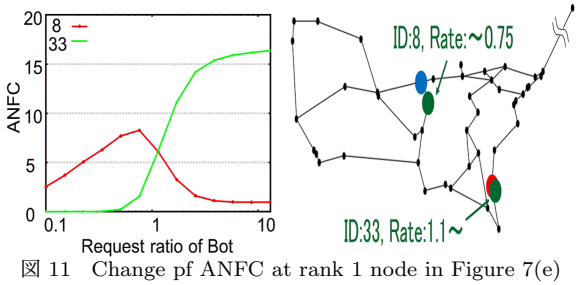

図 11　Change pf ANFC at rank 1 node in Figure 7(e)

表 1　Local cache hit ratio (At Home Network, F=32)

	rank1			rank2		rank3	
	AC	EC	LCD	AC	LCD	AC	LCD
Random	-7.7	-3.6	-4.7	-1.3	0.9	3.4	0.5
Hop	-2.5	-11.2	-1.5	2.7	-2.1	-7.1	-3.0
DCf-PCb	-37.7	-27.0	-22.3	1.0	-2.3	-9.0	-2.6
DCb-PCf	-20.5	-11.5	-15.0	-27.2	-5.3	-18.3	-3.7
BCf-PCb	-27.7	-24.5	-18.8	16.0	3.3	6.5	2.8
BCb-PCf	-39.7	-29.2	-16.8	-18.9	-3.4	-5.1	-2.2

表 2　Local cache hit ratio (At Home Network, F=1024)

	rank1			rank2		rank3	
	AC	EC	LCD	AC	LCD	AC	LCD
Random	-14.6	-8.2	-0.8	-7.1	-10.5	-1.4	4.4
Hop	-19.9	-14.6	-4.5	-13.8	-6.2	-21.0	-1.8
DCf-PCb	-53.8	-70.4	-33.8	-32.9	-34.1	-53.5	28.9
DCb-PCf	-52.9	-87.7	-53.1	-37.7	-48.7	-45.5	9.1
BCf-PCb	-65.5	-75.6	-59.4	-62.2	-39.7	-55.8	-0.2
BCb-PCf	-68.3	-91.6	-67.8	-60.3	-69.5	-62.2	-11.4

表 3　Local cache hit ratio (Allegiance Telecom, F=32)

	rank1			rank2		rank3	
	AC	EC	LCD	AC	LCD	AC	LCD
Random	-7.1	-5.9	-4.5	-0.1	-0.8	-0.1	-0.2
Hop	-12.2	-9.8	-7.2	-2.1	-2.4	-1.7	-0.9
DCf-PCb	-13.8	-1.4	-4.7	-2.0	-0.9	-4.1	-1.7
DCb-PCf	-25.6	-32.5	-25.7	-29.1	-23.9	-20.0	-37.4
BCf-PCb	-17.9	-14.5	-0.2	-5.5	-0.9	-0.5	-0.1
BCb-PCf	-8.5	-27.2	-16.5	-22.9	-17.6	-18.5	-18.5

表 4　Local cache hit ratio (Allegiance Telecom, F=1024)

	rank1			rank2		rank3	
	AC	EC	LCD	AC	LCD	AC	LCD
Random	-7.8	-11.4	-7.7	-4.9	-2.1	-9.6	-3.0
Hop	-85.1	-37.9	-9.1	-11.3	-2.2	-67.4	-1.4
DCf-PCb	-90.6	-84.7	-45.2	-65.9	-34.4	-51.3	-1.0
DCb-PCf	-90.2	-89.0	-97.5	-68.2	-71.2	-47.6	-3.4
BCf-PCb	-90.4	-86.7	-43.5	-67.3	-15.8	-47.8	-8.6
BCb-PCf	-91.7	-55.6	-97.6	-68.4	-71.5	-49.6	-1.6

5. ま と め

ICN における CPA に対する対処法を確立するには，様々な要素が CPA の効果に与える影響を分析し，CPA の脅威を明らかにすることが望ましい．そこで本稿では独自 fake 型の CPA を想定し，大規模なネットワークトポロジで様々な攻撃者の位置で評価を多面的に行うことで，様々な要素が独自 fake 型 CPA の効果に与える影響を分析し，CPA の脅威を明らかにした．本稿で得られた知見を以下に示す．

- fake コンテンツ数が少ない場合は Bot からの多数の要求が少数の fake コンテンツに集中するため，Bot 近くのノードでキャッシュヒットする可能性が高く，fake コンテンツの提供位置まで Interest が到達しない．そのため fake コンテンツ数が少ない場合は Bot 付近のノード，fake コンテンツ数が多くなるにつれ fake コンテンツのオリジナルが存在するノード付近に，より多くの fake コンテンツが注入される．
- EC (edge cache) を用いた場合，fake コンテンツの注入は Bot 配置ノードに限定されるため CPA の効果は小さい．一方，AC (AllCache) を用いた場合，経路上の多数のルータにコンテンツがキャッシュされるため，CPA の効果が大きい．
- 独自 fake 型においては Bot の配置が重要であり，Bot を高 BC や高次数といった NW の主要ノードに配置することで，CPA の影響は大きくなる．特に H&S 型 NW において，その重要度は高い．
- fake コンテンツ数が少ないまたは Bot の要求比率が小さい場合，Bot 付近のノードにのみ fake コンテンツが注入される傾向がある．そのため独自 fake 型 CPA の脅威は小さい．一方，fake コンテンツ数が多い，または Bot の要求比率が大きい場合，オリジナル付近のノードにまで fake コンテンツが注入される結果，独自 fake 型 CPA の脅威は増大する．

今後は fake コンテンツ及び Bot の配置数を増加させた場合の影響について分析する予定である．

謝辞　本研究成果は，JSPS 科研費 18K11283 および 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] T. Nguyen, et al., ” Content Poisoning in Named Data Networking: Comprehensive Characterization of real Deployment.” IFIP/IEEE IM 2017.
[2] 工藤多空飛, 上山憲昭, ” コンテンツポイズニング攻撃の影響 分析”, 2021 信学総大, B-6-24, 2021 年 3 月.
[3] 工藤多空飛, 上山憲昭, ” 攻撃者の位置がコンテンツポイズニング攻撃の脅威に与える影響の分析”, 2021 信学ソ大, B-11-18, 2021 年 9 月.
[4] 工藤多空飛, 上山憲昭, ” ネットワークトポロジがコンテンツポイズニング攻撃に与える影響の分析”, 2022 信学総大, B-14-12, 2022 年 3 月.
[5] W. Cui, et al., “Feedback-Based Content Poisoning Mitigation in Named Data Networking, IEEE ISCC 2018
[6] J. Choi, J. Han, E. Cho, T. Kwon, and Y. Choi, “A Survey on Content-Oriented Networking for Efficient Content Delivery,” IEEE Commun. Mag., vol.49, 3, pp.121-127, Mar. 2011.
[7] K. Cho, et al., “WAVE: Popularity-based and Collaborative In-network Caching for Content-Oriented Networks,” IEEE NOMEN 2012.
[8] N. Laoutaris, H. Che, and I. Stavrakakis, “The LCD interconnection of LRU caches and its analysis,” Elsevier Performance Evaluation, Vol. 63, Issue 7, pp. 609-634, July 2006.
[9] V. Sourlas, L. Tassiulas, I. Psaras, and G. Pavlou, “Information Resilience through User-Assisted Caching in Disruptive Content-Centric Networks,” IFIP Networking 2015.
[10] CAIDA web page, http://www.caida.org/data
[11] L. Breslau, P. Cao, L. Fan, G. Phillips, and S. Shenker, ” Web Caching and Zipf-like Distributions: Evidence and Implications,” IEEE INFOCOM 1999.
[12] M. Cha, H. Kwak, P. Rodriguez, Y. Ahn, and S. Moon, ” Analyzing the Video Popularity Characteristics of Large-Scale User Generated Content Systems,” IEEE/ACM ToN, Vol.17, NO.5, pp.1357-1370, Oct. 2009.
[13] H. Yu, D. Zheng, B. Y. Zhao, and W. Zheng, “Understanding User Behavior in Large-Scale Video-on-Demand Systems,” ACM EuroSys 2006.
[14] G. Xylomenos, et al., “A Survey of Information-Centric Networking Research,” IEEE Communications Survey and Tutorials, Vol. 16, No. 2, pp.1024-1049, 2014.
[15] L. Zhang, et al., “Named Data Networking (NDN) Project,” Technical Report NDN-0001, Oct. 2010.