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
NS2022-221(2023-03)

# NDN におけるプライバシィ保護を考慮したアクセス制御方式

深川　悠馬†　　上山　憲昭††

† 立命館大学 情報理工学研究科
〒 525–8577 滋賀県草津市野路東 1–1–1
†† 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: †gr0579ri@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

**あらまし**　通信開始に先立つ名前解決を行わずにコンテンツの名称で要求パケット (Interest) を転送し，Publisher からの応答コンテンツをキャッシュする ICN (information-centric networking) が，IoT (internet of things) などのコンテンツを効率的に転送するネットワークとして注目されている．ICN のアーキテクチャの一つに NDN (named data networking) が提案されている．NDN では Publisher によるアクセス制御が困難であり，コンテンツ名に対するプライバシー漏洩の課題がある．既存のアクセス制御手法である NAC (name-based access control) ではアクセス制御の課題を解決するが，プライバシー漏洩の課題が残る．また，プライバシー漏洩の問題に対してコンテンツ名を暗号化する対策が考えられるが，頻度攻撃により暗号化コンテンツ名が特定される問題が発生する．そこで本稿では，初回 Interest を常に Publisher に到達させることで Publisher によるアクセス制御を実現し，コンテンツ名暗号化によってプライバシー保護を行い，暗号化コンテンツ名を動的に変化させることで頻度攻撃の影響を減少させるアクセス制御方式を提案する．提案方式では制御トラヒック量の増加，処理時間や遅延時間の増加などが懸念されるため，NAC 方式との比較評価を行う．また，頻度攻撃に対する防御効果も評価することで提案方式の有効性を確認する．
**キーワード**　ICN, NDN, プライバシー保護, アクセス制御, 頻度攻撃, コンテンツ名暗号化

# Access Control Method with Privacy Preservation in NDN

Yuma FUKAGAWA† and Noriaki KAMIYAMA††

† Graduate School of Information Science and Engineering, Ritsumei University
1–1–1, Nojihigashi, Kusatsu, Shiga 525–8577
†† College of Information Science and Engineering, Ritsumeikan University
1–1–1, Nojihigashi, Kusatsu, Shiga 525–8577
E-mail: †gr0579ri@ed.ritsumei.ac.jp, ††kamiaki@fc.ritsumei.ac.jp

**Abstract**　Information-Centric Networking (ICN), which transfers Interest by the name of content without using name resolution and caches the response content from publishers on routers, is attracting attention as a network that efficiently delivers content such as IoT. One of the ICN architectures is Named Data Networking (NDN), which faces the challenge of privacy leakage of content names and access control by Publisher. The existing access control method, Name-Based Access Control (NAC), addresses the access control challenge. However, NAC still leaves the privacy leakage issue. To address this issue, one possible solution is to encrypt the content name. However, frequency attacks can specify the encrypted content name. Proposed method ensures that First Interest always reaches the Publisher to control access by Publisher, encrypts the content name, and dynamically changes encrypted content name to mitigate the impact of frequency attacks. We compare the proposed method with NAC method and evaluate in terms of control traffic, processing time, and delay time. Furthermore, we evaluate the proposed method against frequency attacks to confirm its effectiveness.
**Key words**　ICN, NDN, Privacy preservation, Access control, Frequency attack, Content name encryption

## 1. はじめに

従来のインターネットでは通信開始に先立ち，配信ホスト (Publisher) の名前解決を DNS (domain name system) に依頼し，配信ホストの IP アドレスを取得することでデータの送受信を行っている．しかし普及が進む IoT (internet of things) の一部サービスでは，キーワードや条件などの曖昧な名称でデータを要求するため，DNS による名前解決が困難になることが想定される．そこで通信開始に先立つ名前解決を行わずにコンテンツの名称で要求パケット (Interest) を転送し，Publisher からの応答コンテンツをルータでキャッシュする ICN (information-centric networking) が，IoT などのコンテンツを効率的に転送するネットワークとして注目されている [6].

ICN の概念を実現するためのアーキテクチャの一つに NDN (named data networking) が提案されている [3]．NDN においてコンテンツはユーザ (Consumer) や Publisher から独立して存在するため，アクセス制御とプライバシーに関して課題が存在する．

ネットワークで利用されるコンテンツには，誰もが自由に取得できるコンテンツと特定のユーザだけが取得できる閲覧者限定コンテンツがある．閲覧者限定のコンテンツには例えば，Hulu や Netflix などの月会費の支払いサービスを契約することが求められる有料コンテンツや，特定の会員のみがアクセスできるコンテンツがある．従来のインターネットでは閲覧者限定のコンテンツに対する配信要求時には，要求した Consumer が閲覧可能か否かを判断する Publisher によるアクセス制御を実行している．NDN においても閲覧者限定のコンテンツに対するアクセス制御が必要である．しかし NDN では，コンテンツはルータ上にキャッシュされている．そのため閲覧者限定のコンテンツに対して配信要求を行うと Publisher に配信要求が到達することなく，キャッシュされているルータからコンテンツが配信される可能性がある．NDN では全ての配信要求が Publisher に到達しないため，従来のインターネットのように Publisher でアクセス制御を行うことが困難である．ルータでアクセス制御を行うことで対処可能であるが，コンテンツ事業者ごとのアクセス許可リストを各ルータで管理する必要があり，プライバシー上，また処理負荷的に困難である．そのため，NDN での Publisher によるアクセス制御の実現が課題の一つである．

NDN では，コンテンツを要求する際に要求コンテンツ名で Interest を送信する．コンテンツが暗号化されていたとしても，攻撃者がスニッフィングにより，Interest の情報からどのコンテンツを取得しているのかをコンテンツ名の盗聴により特定できる問題がある．ユーザのプライバシーを守るために，要求されたコンテンツ名に対する秘匿性も望まれる．そのため，NDN ではコンテンツ名暗号化によるプライバシー保護の実現も課題となる．

これまでにアクセス制御の課題を解決した手法として，NAC (name-based access control) [9] が提案されている．しかし，NAC ではコンテンツ名を平文で要求するため，コンテンツ名に対するプライバシー漏洩の問題が存在する．コンテンツ名に対するプライバシー漏洩の問題を解決する手法として，コンテンツ名を暗号化するといった対策をとることが考えられる．しかし単にコンテンツ名を暗号化するだけでは，暗号化コンテンツ名を特定する頻度攻撃が可能である [2].

また著者らは以前，ICN での Publisher によるアクセス制御を提案した [8] が，コンテンツ名のプライバシー漏洩の問題は考慮しておらず，また NDN 上での具体的な実装については未検討である．そこで本稿では，常に Publisher に到達させる初回 Interest をコンテンツ要求に先立って送信することで，NDN での Publisher によるアクセス制御を実現し，Publisher による暗号化コンテンツ名の動的な変更により頻度攻撃の影響を減少させる方式を提案する．また，本アクセス制御方式に必要な制御トラヒック量，暗号化，復号化回数や使用する鍵の生成数を既存の NDN アクセス制御方式である NAC と数値比較し，頻度攻撃の影響を独自に作成したネットワークシミュレータを使用して評価することで，その有効性を明らかにする．

以下，4.1 節で NDN について述べ，3. 節で関連研究について述べる．そして 4. 節で提案方式の概要，5. 節で性能評価を行い，6. 節で全体をまとめる．

## 2. NDN のセキュリティの課題

NDN では，従来のネットワークにある送信元 IP アドレスのような Consumer 情報を Interest に載せない．そのため，Interest から要求 Consumer の特定ができないが，以下のようなセキュリティに関する問題が生じる．

### 2.1 リプレイ攻撃

Interest を盗聴した攻撃者が盗聴 Interest を利用し，再度同じ Interest を送信した場合，要求した攻撃者ノードにコンテンツが転送される．この時，攻撃者は不当にコンテンツを取得可能である．このような攻撃をリプレイ攻撃と呼ぶ．アクセス制御を必要とするような閲覧者限定のコンテンツも，攻撃者はリプレイ攻撃により取得可能である．

### 2.2 前方秘匿性

鍵交換には，鍵が漏洩しても過去に暗号化されたコンテンツを復号できないという前方秘匿性を満たすことが求められる．しかし NDN ではコンテンツが Publisher から独立しているためコンテンツ鍵を変えない限り，Consumer がサービス加入時にコンテンツ鍵を取得し，サービス終了後もコンテンツ鍵を保持している場合，サービス終了後もコンテンツを復号可能であるため，前方秘匿性が満たされない．

### 2.3 頻度攻撃

コンテンツを平文の名前で要求することで発生するプライバシー漏洩の問題に対して，コンテンツ名を暗号化するといった対策が考えられる．しかしスニッフィングを行う攻撃者が各暗号化コンテンツ名を収集し，コンテンツの人気順位などのコンテンツを特定可能な情報と比較することで暗号化コンテンツ名からコンテンツ名を特定する頻度攻撃 [2] が可能である．そのため，ただ暗号化するだけでは不十分である．

## 3. 関連研究

### 3.1 Name-based Access Control

NDN のアクセス制御を実現している手法の一つに NAC [9] が存在する．コンテンツを暗号化するコンテンツ鍵やコンテンツ鍵を Consumer 毎に暗号化する KEK/KDK (key-encrypt key/key-decrypt key) を使用して，粒度の細かいアクセス制御を実現している．コンテンツの要求を行い，要求コンテンツを取得する．取得したコンテンツの名前からコンテンツ鍵の名前を推測し，コンテンツ鍵を要求する．取得したコンテンツ鍵の名前からコンテンツ鍵を暗号化している KEK の名前が分かるため，その名前から自身の情報を組み合わせて KDK の名前を推測して要求する．要求名の予測に取得済みのコンテンツ名を利用し平文でコンテンツを要求するため，スニッフィングを行う攻撃者はコンテンツが暗号化されていても，それがどんなコンテンツであるのかが把握可能である．本問題に対処するためにコンテンツ名の暗号化が考えられるが，2.3 節で述べる問題が残る．

### 3.2 関連アクセス制御手法

これまでに NDN のアクセス制御機構として，アクセス権限を有する Consumer に対してのみ復号を行うための暗号鍵を共有する Encryption Based 方式のアクセス制御法が提案されている．Encryption Based 方式では，コンテンツ名に基づく暗号化アルゴリズムを使用してアクセス制御を行う Name-based 型のアクセス制御 [9] [10] と，属性ベース暗号を使用した Attribute-based 型のアクセス制御 [5] [11] が提案されている．

[10] では，Web アプリケーションなどを提供する CP (content provider) が使用する OSN (online social networking) 上で NDN を考慮した SAC (session-based access control) を提案している．Consumer と OSN 間の接続が維持されている間，セッション鍵と呼ばれる鍵を保持する．セッション鍵を使用して Consumer 情報や要求コンテンツ情報を送信することで，セッション鍵を持っていない第三者はその内容を知ることができない手法を実現している．

[5] では，コンテンツとそのコンテンツにアクセス可能な属

性情報を載せたアクセスポリシーを利用してアクセス制御を行う手法を提案している．Consumer はコンテンツのアクセスに必要な属性を持っていない限りそのコンテンツにアクセスできない．[11] は [9] を属性ベース暗号に拡張した手法となる．

## 4. 提 案 方 式

提案方式は，NDN 上での Publisher によるアクセス制御を達成し，頻度攻撃による問題を減少させることが可能なコンテンツ名暗号化を行う手法である．本節では，本稿で提案するアクセス制御方式の概要について述べる．

### 4.1 NDN のパケット仕様の活用

本節では，NDN の Interest パケットや Data パケットの仕様 [4] について述べ，提案方式がどのようにこれらパケットのヘッダ情報を活用するかを述べる．なお NDN の詳細は [3] で述べられている．

提案方式では 4.4.2 節で述べるように，コンテンツ要求時に Consumer の秘密鍵を使用し，要求するコンテンツ名を暗号化して送信する．このとき同一のコンテンツ名に対して，Consumer 毎に異なる固有な暗号化コンテンツ名が生成される．固有な暗号化コンテンツ名により，キャッシュヒットせず常に Publisher に到達するが，同一の Consumer が秘密鍵により生成した暗号化コンテンツ名や各 Consumer が生成する暗号化コンテンツ名が競合しないとは限らない．そのため提案方式では，NDN Packet Format Specification v0.3 [4] における Interest パケット，Data パケットの仕様を以下のように活用する．

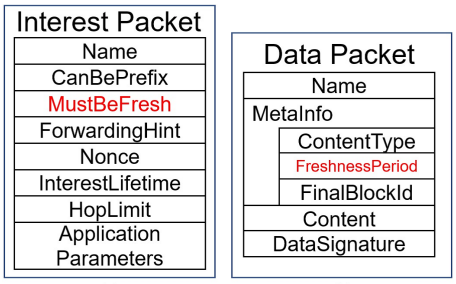


図 1　Packet Format v0.3 in NDN

#### 4.1.1 Interest Packet Format

図 1(a) に NDN の Interest パケットヘッダを示す．提案方式では，Publisher によるアクセス制御を実現するために *MustBeFresh* フラグを使用する．*MustBeFresh* フラグが設定されている Interest に対して，4.1.2 節で述べる *FreshnessPeriod* 要素が新しいデータであることを示すコンテンツのみをキャッシュから選択し，応答パケットとして転送する．キャッシュされているコンテンツが古い場合，キャッシュを無視して Interest を次ノードへと転送する．提案方式では，初回 Interest の要求コンテンツを常に古いコンテンツとして扱い，*MustBeFresh* フラグを設定した初回 Interest を送信することで，既にキャッシュされている要求コンテンツには応答せず，常に Publisher に到達させる．

#### 4.1.2 Data Packet Format

図 1(b) に Data パケットヘッダを示す．提案方式では，初回 Interest の応答パケットがルータ上で応答しないように *MetaInfo* 要素の中の *FreshnessPeriod* 要素を使用する．*FreshnessPeriod* 要素はコンテンツがルータに到着してから *fresh* なデータとして扱う期間を指定可能である．この要素を 0 に設定するか，設定期間を過ぎると *non-fresh* なデータとして扱われる．この時，4.1.1 節で述べた *MustBeFresh* フラグがセットされた Interest に対する応答パケットとして返せなくなる．提案方式では初回 Interest の応答パケットの *FreshnessPeriod* を常に 0 に設定することで，初回 Interest を常に Publisher に到達させる．

### 4.2 コンテンツ名

提案方式で使用するコンテンツ名は以下の 3 つに分類される．

#### 4.2.1 Content Name

*youtube/watch/content1* といった URL に含まれる *content1* のようなコンテンツ名を *ContentName* と呼び，全ての Consumer はこのコンテンツ名を知っている．提案方式では，コンテンツの名前には *ContentName* が使用されない．しかし，Consumer が要求したいコンテンツ名を指定するのに *ContentName* を使用する．

#### 4.2.2 Actual Content Name

*ContentName* を Publisher が独自に暗号化したコンテンツ名を *ActualContentName* と呼ぶ．4.2.1 節で述べたように，コンテンツの名前に *ContentName* は使用しないが，Publisher はすべてのキャッシュされるコンテンツの名前に *ActualContentName* を使用する．Consumer は *ActualContentName* を知らないため，Publisher に対して *ContentName* で要求を行うことで，サービスに加入している正常な Consumer であれば，その応答として *ActualContentName* を取得する．

また，*ActualContentName* は Publisher が管理しているため，定期的に変更することで使用される *ActualContentName* が動的に変化し，同一暗号化コンテンツ名が永続的に使用されないため頻度攻撃の影響を減少させることが可能である．

#### 4.2.3 Encrypted Content Name

コンテンツやコンテンツ鍵を *ContentName* や *ActualContentName* で要求を行う場合，スニッフィングを行う攻撃者にとって，どちらもコンテンツ名を特定する情報として有益である．そこで提案方式では Consumer と Publisher 間でパケットを送信する際，コンテンツ名を Consumer の秘密鍵や公開鍵を使用して暗号化する．これにより攻撃者はスニッフィングを行っても暗号化されているため，*ContentName* や *ActualContentName* が知られることはない．この時のコンテンツ名をそれぞれ *EncryptedContentName*, *EncryptedActualContentName* と呼ぶ．

また，各 Consumer の秘密鍵で暗号化を行うため，Consumer 毎に異なるコンテンツ名で要求を行う．そのため攻撃者は特定の一人の要求を監視しない限り頻度攻撃のような推測は難しくなる．また，2. 節で述べたように NDN の特性上，Interest から要求 Consumer の特定ができないため，特定の Consumer の監視が難しい．

### 4.3 Consumer ID

2. 節で述べたように，NDN では Interest に Consumer の情報を載せないため，アクセス制御行うための *ConsumerID* が必要である．*ConsumerID* はサービス加入時に Publisher から Consumer に対して交付される Consumer 判別ための ID である．*ConsumerID* 配布においても RSA 暗号等を使用して配布することで，*ConsumerID* の第三者への漏洩を防ぐことを想定する．

提案方式では，*ConsumerID* を Publisher の公開鍵で暗号化して初回 Interest を送信することを想定しているが，頻度攻撃を *ConsumerID* に対して行うと *ConsumerID* を復号できなくとも Interest の要求者を識別できる問題がある．そのため，Diffie-Hellman 鍵交換プロトコル [7] のような一時的な公開鍵を使用することで，要求毎に異なる暗号化を行うことが望ましい．

### 4.4 提案方式の動作

Consumer は Publisher のサービス加入時に，Publisher から Publisher 名と *ConsumerID* を取得する．さらに Consumer は Publisher の公開鍵を取得し，Publisher も Consumer の公開鍵を取得しているものとする．

#### 4.4.1 コンテンツ公開

Publisher はあらかじめコンテンツを公開しなければならない．公開するコンテンツの名前に *ContentName* を使用する場合，Consumer は平文のコンテンツ名で要求しなければならないため，図 2 に示すように Publisher は暗号化コンテンツ名である *ActualContentName* を使用してコンテンツを公開する．また，*ActualContentName* は Publisher から認証を受けたのちに取得しない限り Consumer は知ることができない．また，コンテンツ鍵を使用してコンテンツの暗号化も行う．

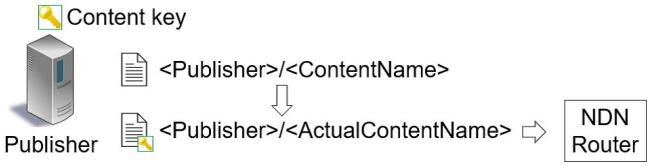


図 2　コンテンツ公開時の処理フロー

#### 4.4.2 初回 Interest

Consumer はコンテンツ要求に先立ってコンテンツ鍵に対して Publisher に初回 Interest を送信する．同時に初回 Interest を用いてアクセス制御を行う．図 3 に示すように，初回 Interest のコンテンツ名には Consumer の認証情報である *ConsumerID*，要求したいコンテンツの *ContentName* を挿入する．*ConsumerID* は Publisher の公開鍵で暗号化し，*ContentName* も Consumer の秘密鍵で暗号化して *EncryptedContentName* として要求する．また，*FOR* は同一コンテンツ名の競合を防ぐための予約語として定義する．この初回 Interest のパケットヘッダには *MustBeFresh* フラグを使用し，*non-fresh* のコンテンツが応答しないように設定する．そのため，常に初回 Interest は Publisher へと到達する．

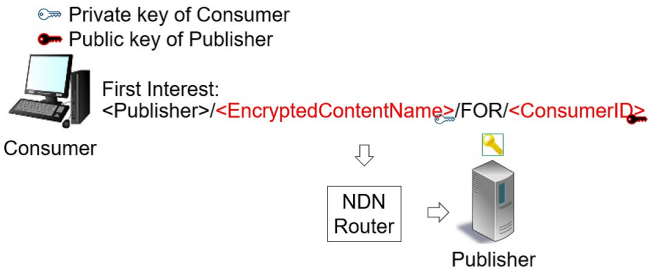


図 3　初回 Interest 送信時の処理フロー

#### 4.4.3 アクセス制御

コンテンツ鍵要求である初回 Interest を受信した Publisher は，アクセス制御を行うために図 4 に示すように，*ConsumerID* を Publisher の秘密鍵で復号する．この時 *ConsumerID* が正常な Consumer でなければ初回 Interest を棄却する．正常な Consumer であれば，Publisher は Consumer の公開鍵を特定できるため，*EncryptedContentName* を Consumer の公開鍵を用いて復号し *ContentName* を取得する．Consumer がこのコンテンツにアクセスが許可されている場合，Publisher は *ContentName* から *ActualContentName* を生成する．要求されたコンテンツ鍵を Consumer の公開鍵で暗号化し，*ActualContentName* も Consumer の公開鍵で暗号化を行い，*EncryptedActualContentName* としてコンテンツ名に挿入し初回 Interest の応答パケットとして返送する．また，この応答パケットのパケットヘッダにある *FreshnessPeriod* は 0 に設定することで，常に *non-fresh* のデータとして扱い，初回 Interest に応答させない．

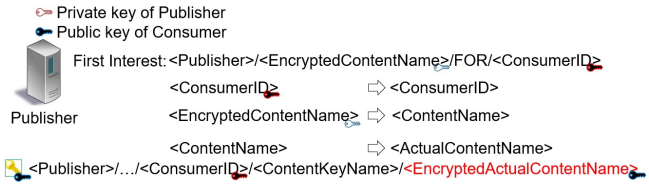


図 4　アクセス制御時の処理フロー

#### 4.4.4 コンテンツ要求

コンテンツ鍵を取得した Consumer は，図 5 に示すように，Consumer の秘密鍵を使用してコンテンツ鍵と *EncryptedActualContentName* を復号し，*ActualContentName* を取得する．そのため，Consumer は *ActualContentName* を用いてコンテンツを要求し，取得したコンテンツをコンテンツ鍵で復号する．

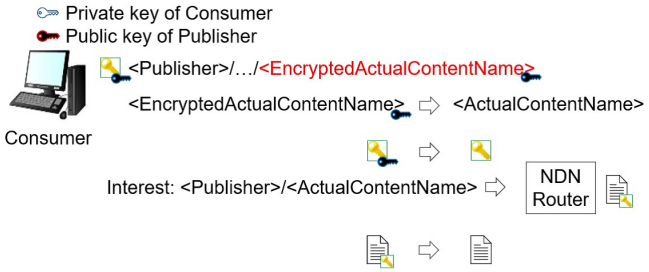


図 5　コンテンツ要求時の処理フロー

### 4.5 アクセス制御における考察

#### 4.5.1 アクセス失効

提案方式では初回 Interest を常に Publisher に到達させることでアクセス制御を行う．そのため，アクセス権を失った Consumer からの要求は *ConsumerID* で判断可能である．アクセス権を失った Consumer に対して現在利用可能なコンテンツ鍵の配布が行われないため，アクセス失効が可能となる．また，*ConsumerID* を不当に利用した第三者からの要求で認証が成功しコンテンツ鍵の配布が行われたとしても，コンテンツ鍵は *ConsumerID* 本人の公開鍵で暗号化されているため，第三者の Consumer が秘密鍵を所持していない限りコンテンツは復号不可能である．

#### 4.5.2 緊急のアクセス失効

コンテンツ鍵を所持したままの Consumer が途中退会を行った結果，Publisher によってコンテンツ鍵の変更が行われるまでの間，不当にコンテンツを閲覧可能である．そのため，途中退会を行った Consumer に対してもアクセス権の失効を必要とする．Hulu や Netflix では，鍵の入手などをアプリケーション層でブラックボックス化しており，鍵を入手しても使用後に削除することで，Consumer が鍵を永続的に保持することを防いでいる．提案方式においてもこのような技術を使用することを推奨する．これにより Consumer は鍵の保持ができないため，途中退会を行っても即座にアクセス権を失効可能である．

### 4.6 セキュリティ

#### 4.6.1 リプレイ攻撃

攻撃者が初回 Interest を傍受しリプレイ攻撃に使用した場合，コンテンツ鍵を不正に取得可能である．また，コンテンツ要求においても同様である．しかし，コンテンツはコンテンツ鍵で暗号化されており，コンテンツ鍵は Consumer の公開鍵で暗号化されている．そのため，攻撃者は Consumer の秘密鍵を所持していない限りコンテンツ鍵の復号ができず，同時にコン

テンツの復号もできない．また，提案方式では各コンテンツに対して別々のコンテンツ鍵で暗号化を行っているため，一つの鍵を不当に取得したとしても鍵の復号に時間を要し，Publisher は定期的にコンテンツ鍵の変更を行うことが可能なため，リプレイ攻撃の影響を減少させることが可能である．

#### 4.6.2 前方秘匿性

一度サービスに加入した Consumer が Publisher の所有する全ての鍵を正当に入手したのちに，Publisher によってコンテンツ鍵が変更されるよりも前に退会する場合を考える．このとき Consumer は正当に入手したコンテンツ鍵を用いて不当にコンテンツを復号可能である．そのため，前方秘匿性を満たすには 4.5.2 節のような対策を施すことで影響を減らすことが可能である．アプリケーション層で対処しない場合は，コンテンツ鍵の交換周期を短くすることで影響を減少させることが可能だが，コンテンツ鍵変更と同時にコンテンツを再暗号化する必要がある．そのため，キャッシュ済みのコンテンツが使用できなくなるため，キャッシュ効率が低下する．

#### 4.6.3 頻度攻撃

Publisher が $ActualContentName$ を動的に変更可能なため，暗号化コンテンツ名の特定に必要な要求サンプルが集まりづらくなる．そのため，頻度攻撃はコンテンツ名の変更回数を増加させると影響を減少させることが可能である．しかし，提案方式ではコンテンツ名変更と同時にコンテンツを再暗号化する必要があるため，4.6.2 節と同様の問題が発生する．

## 5. 性能評価

提案方式では NAC [9] で問題であったプライバシーの問題を解決するが，一方で制御トラヒック量の増加，暗号化，復号化の処理の増加が懸念される．そこで本節では，NAC との配信要求あたりの制御トラヒック量，暗号化，復号化の回数，使用する鍵の生成数の数値評価を行う．制御トラヒック量はコンテンツ鍵のやり取りに発生するトラヒック量とする．また，頻度攻撃の影響を独自に作成したネットワークシミュレータを使用して評価する．

### 5.1 制御トラヒック量

表 1 評価に用いたパラメタ

| Parameter | Value | Description |
|---|---|---|
| $T_{C_k}$ | 1 (h) | time of key exchange |
| $T_k$ | 24 (h) | time of KEK/KDK exchange |
| $N_c$ | 10000 | number of contents |
| $N_k$ | 1 - 10000 | number of content keys |
| $N_{R_c}$ | 1 - 100 (/h) | number of consumer requests |
| $V_I$ | 100 (Byte) | traffic of Interest |
| $V_{C_k}$ | 100 (Byte) | traffic of content key |
| $V_k$ | 100 (Byte) | traffic of KEK/KDK |

表 1 に評価に用いたパラメタを示す．提案方式では，要求の度に初回 Interest としてコンテンツ鍵要求が発生するため，制御トラヒック量 $V_p$ は次式で得られる．

$$V_p = V_I + V_{C_k} \tag{1}$$

NAC では，全てのコンテンツを一つのコンテンツ鍵で暗号化する場合，制御トラヒック量 $V_{NAC1}$ は次式で得られる．

$$V_{NAC1} = \frac{V_I + V_{C_k}}{N_{R_c}} + \frac{V_I + V_k}{24N_{R_c}} \tag{2}$$

提案方式は常にコンテンツ鍵を要求するため，コンテンツ鍵の増加によるトラヒック量の増減は発生しない．しかし NAC では，$N_c$ 個のコンテンツを $N_k$ 個のコンテンツ鍵で分割して暗号化する場合，コンテンツ鍵 $i$ を要求する確率 $P_{c_i}$ を用いて，制御トラヒック量 $V_{NAC2}$ は次式で得られる．

$$V_{NAC2} = \frac{\sum_{i=1}^{N_K}(1-(1-P_{c_i})^{N_{R_c}})(V_I + V_{C_k})}{N_{R_c}} + \frac{V_I + V_k}{24N_{R_c}} \tag{3}$$

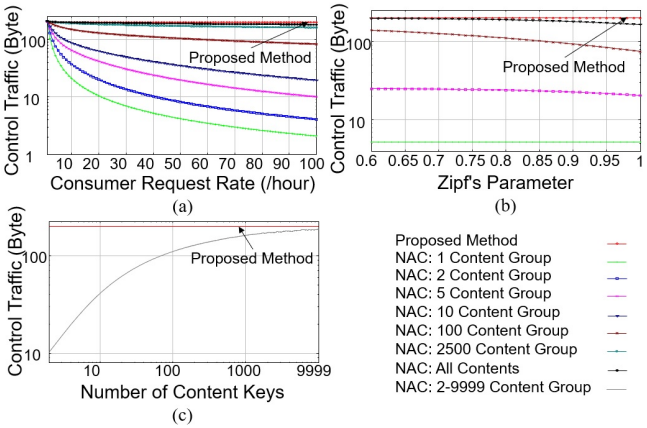


図 6 制御トラヒック量

各コンテンツの要求分布として Zipf 分布を想定する．図 6 に 1 回のコンテンツ配信において発生する制御トラヒック量の評価結果を示す．提案方式ではどのパラメタにおいても，初回 Interest は常に発生するため約 200Byte の制御トラヒックが常に発生する．図 6(a), (b), (c) から NAC は 1 時間に Consumer が要求する回数が増加し，Zipf 分布のパラメタの偏りが大きく，コンテンツ鍵の数が減少するほど制御トラヒック量が減少する．そのため提案方式は NAC よりも制御トラヒック量が増加することが確認できる．しかし制御トラヒック量はコンテンツのデータ量と比較すればごく僅かな量であり，1 回の配信要求において発生するトラヒックの大部分はコンテンツデータであり問題はないと考えられる．

### 5.2 暗号/復号化評価

評価条件としてコンテンツ鍵の交換周期を 1 時間, KEK/KDK の交換周期を 24 時間，鍵を生成する Publisher の数を $N_{P_k}$，Publisher のコンテンツに 1 日の間アクセスが許可されている Consumer の数を $N_{C_{24}}$ とする．提案方式は，暗号化や復号化にかかる処理時間，遅延時間などが，コンテンツ鍵要求が多いため NAC よりも多く発生する．このような値に比例する 1 要求あたりの暗号化，復号化の回数を評価する．NAC はコンテンツ鍵生成の分散機構を持つため，NAC の暗号化，復号化回数 $N_{NAC_k}$ は以下になる．

$$N_{NAC_k} = 2 + 2N_{P_k} \tag{4}$$

提案方式は鍵生成を分散させる機構がなく，コンテンツ名暗号化も行うため常に 10 回発生する．そのため，$N_{P_k}$ が増加しない限り，提案方式が多くなる．また，NAC は新規コンテンツ鍵を要求するときのみ $N_{NAC_k}$ 回発生するのに対し，提案方式はすべての要求に対して 10 回発生するため，処理時間や遅延時間も比例して NAC よりも増加する．

次に暗号化，復号化に使用する鍵の生成数を 1 日当たりで評価する．NAC では 24 回のコンテンツ鍵生成に加え，KDK が 1 時間毎に $N_{C_{24}}$ 人分生成されるため，NAC の 1 日当たりのコンテンツ鍵生成数 $N_{NAC_g}$ は以下になる．

$$N_{NAC_g} = 24 + N_{C_{24}} \tag{5}$$

提案方式は，1 時間毎に $N_{C_{24}}$ 人にコンテンツ鍵を生成するため，提案方式の 1 日当たりのコンテンツ鍵生成数 $N_{p_g}$ は以下

になる．

$$N_{p_g} = 24N_{C_{24}} \tag{6}$$

どちらの方式もオーダ表記で考えると，$O(N_{C_{24}})$ となり Consumer の数の増加とともに鍵生成数が増え，Publisher の負担が増加する．そのため，コンテンツ鍵の生成数による差異は見られない．

### 5.3 頻度攻撃に対する評価

本節では，ネットワークシミュレータを用いて提案方式における頻度攻撃の影響を評価する．頻度攻撃は人気コンテンツほど特定されやすいため，コンテンツ数 10,000 の内，上位 100 個の人気コンテンツを対象に攻撃者の $ActualContentName$ から $ContentName$ を特定した正答率を評価する．

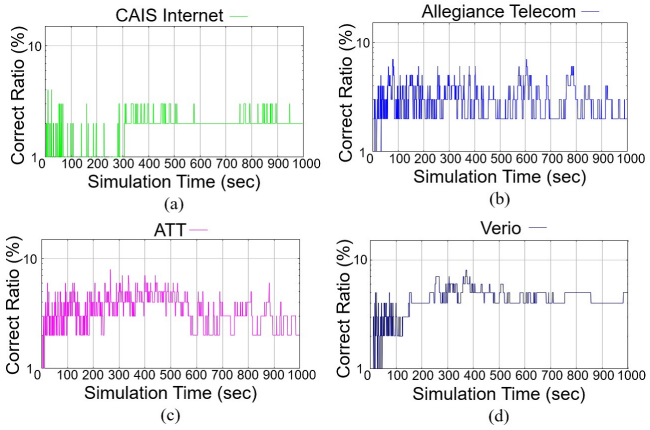


図 7　各トポロジにおける攻撃者の正答率の時間変化

図 7 にシミュレータ時間経過における鍵交換を行わない場合の各トポロジにおける攻撃者の正答率を示す．正答率とは対象コンテンツ 100 個における攻撃者の特定数である．どのトポロジにおいても攻撃者の傾向として，時間経過とともに正答率が一定の値に安定する．また，より上位の人気コンテンツほど要求情報を多く収集が可能であり，特定が安定しないコンテンツは要求数のばらつきがある．そのため，特定に必要な要求数が十分に収集可能なより上位のコンテンツが安定して特定される．

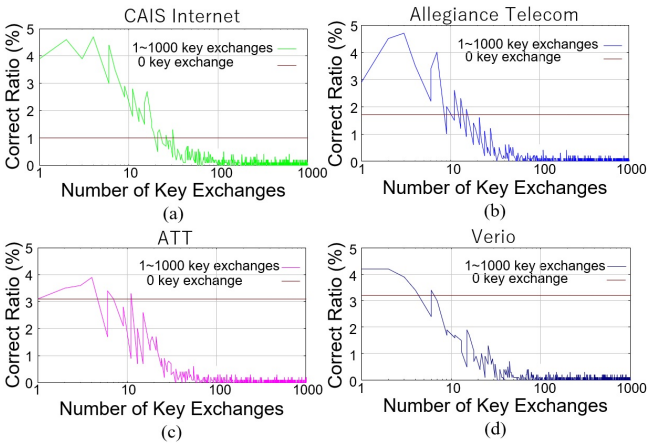


図 8　鍵交換頻度に対する攻撃者の正答率

提案方式は，コンテンツ鍵変更と同時に $ActualContentName$ を変更することにより頻度攻撃による影響を減少させることができるため，鍵交換を行った場合の攻撃者の正答率を図 8 に示す．横軸はシミュレーション時間内に行った鍵の交換回数である．また，攻撃者の正答率は，図 7 から時間経過によって安定することがわかっているため，各鍵交換回数におけるシミュレーション終了時の攻撃者の正答率を示す．どのトポロジにおいても攻撃者の傾向として，鍵交換回数が増加するとともに攻撃者の正答率が低下する．しかし，適切な鍵交換回数を設定する必要があり，鍵交換回数が増加するとキャッシュが活かされないためネットワーク全体のトラヒック量が増加する可能性がある．

また，今回は Publisher のコンテンツ名変更が単純なアルゴリズムで設定されているため，鍵交換無しの場合よりも攻撃者の正答率が高くなる傾向がある．そのため，Publisher の変更アルゴリズムを複雑にする必要がある．

## 6. ま と め

NDN ではルータでコンテンツがキャッシュされるため，Publisher によるアクセス制御が困難である．そのため，閲覧者限定のコンテンツに対するアクセス制御が課題である．また，コンテンツ名が平文で要求されるため，コンテンツ名を盗聴することによるプライバシー漏洩の問題がある．対策としてコンテンツ名暗号化が考えられるが，頻度攻撃が可能なため単純な暗号化だけでは不十分であることも課題である．既存方式である NAC ではアクセス制御の課題を解決するが，プライバシー漏洩の問題が残る．そこで本稿では，初回 Interest を常に Publisher に到達させることで Publisher によるアクセス制御を実現し，暗号化コンテンツ名を動的に変化させることで頻度攻撃の影響を減少させる方式を提案した．

提案方式は制御トラヒック量や処理時間，遅延時間などが NAC 方式に比べて増加する．しかし，制御トラヒック量においては 1 回の配信要求に発生するトラヒックの大部分はコンテンツデータであるため，コンテンツデータと比較すると制御トラヒック量はごく僅かであるため問題ないと考えられる．また NAC ではプライバシー漏洩の問題が残るが，提案方式ではコンテンツ名を暗号化することによりプライバシーを保護し，頻度攻撃による影響を，暗号化コンテンツ名を変更することにより，影響を減少させることが可能である．今後は頻度攻撃の影響評価において，Publisher の暗号化コンテンツ名の変更アルゴリズムを複雑化した場合における攻撃者の正答率傾向の評価を行う予定である．

**謝辞**　本研究成果は，JSPS 科研費 18K11283 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] B. Nour, H. Khelifi, R. Hussain, S. Mastorakis, H. Moungla, Access Control Mechanisms in Named Data Networks: A Comprehensive Survey, ACM CS, Apr. 2022.
[2] C. Ghali, G. Tsudik, CA. Wood, When encryption is not enough: Privacy attacks in content-centric networking, ACM ICN, 2017, p1-10.
[3] L. Zhang, et al., Named Data Networking (NDN) Project, Technical Report NDN-0001, Oct. 2010.
[4] NDN Packet Format Specification v0.3, 2023/1/30, https://docs.named-data.net/NDN-packet-spec/0.3/.
[5] R. S. da Silva, S. D. Zorzo, An Access Control Mechanism to Ensure Privacy in Named Data Networking using Attribute-based Encryption with Immediate Revocation of Privileges, IEEE CCNC 2015, Jan. 2015.
[6] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT), IEEE Internet of Things Journal, Vol. 6, No. 2, pp. 2128-2158, Apr. 2019.
[7] W. Diffie, M. E. Hellman, New directions in cryptography, IEEE Trans. Inform. Theory., Nov. 1976.
[8] Y. Fukagawa, N. Kamiyama, Access Control with Individual Key Delivery in ICN, IEEE LANMAN 2022, July. 2022.
[9] Y. Yu, A. Afanasyev, L. Zhang, Name-Based Access Control, Technical Report NDN-0034, Jan. 2016.
[10] Y. Wang, M. Xu, Z. Feng, Q. Li and Q. Li, Session-based Access Control in Information-Centric Networks: Design and Analyses, IEEE IPCCC 2014, Dec. 2014.
[11] Z. Zhang, Y. Yu, A. Afanasyev, J. Burke, L. Zhang, NAC: Name-based Access Control in Named Data Networking, ACM ICN 2017.