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
CQ2021-71(2021-11)

ICN における個別鍵配送を用いたアクセス制御方式

深川　悠馬†　　上山　憲昭††

† 福岡大学 工学部 電子情報工学科
〒 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: †tl181272@cis.fukuoka-u.ac.jp, ††kamiyama@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．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のコンテンツがある．後者のコンテンツ要求時には，要求したユーザが試聴できるか否かを判断するアクセス制御が必要になる．従来のインターネットでは多くの場合，コンテンツ事業者の権威 DNS (Domain Name System) サーバに配信要求が届く．そのためアクセス制御が容易に可能である．しかし ICN では，コンテンツがルータ上から配信されるためアクセス制御を行うことが困難である．ICN でのアクセス制御法として，コンテンツを暗号化し，周期的に復号のための鍵を変えて全加入ユーザに対し鍵を配布する方式が提案されているが，アクセス権を喪失したユーザも次の鍵更新までは不当にコンテンツの閲覧が可能な問題がある．そこで本稿では，コンテンツの初回 Interest を常に Publisher に到達させることで，Publisher にてアクセス制御を可能とする方式を提案する．また提案方式での初回 Interest によるオーバヘッド遅延時間の解析モデルで遅延時間を導出し数値評価により，Publisher への要求レートが約 250 個/秒より小さい場合には，数 10ms〜数 100ms 程度のオーバヘッド時間のみで処理が可能なことを確認した．また一括鍵配布方式と提案方式のオーバヘッドトラヒック量を簡易な解析モデルで導出し，数値評価により比較した．その結果，提案方式は鍵の交換周期によらず 1 日あたり約 7GB の制御トラヒックが発生している一方，一括鍵配布方式は最低でも約 250 GBytes の不正トラヒックが 1 日あたりに発生することを確認した．そのため提案方式は一括鍵配布方式と比較してオーバヘッドトラヒック量を大きく低減可能である．
キーワード　ICN, 公開鍵暗号, アクセス制御

Access Control with Individual Key Delivery in ICN

Yuma FUKAGAWA† and Noriaki KAMIYAMA††

† Department of Electronic and Information Technology, Fukuoka University
8–19–1, Nanakuma, Jounan, Fukuoka 814–0180
†† College of Information Science and Engineering, Ritsumeikan University
1–1–1, Nojihigashi, Kusatsu, Shiga 525–8577
E-mail: †tl181272@cis.fukuoka-u.ac.jp, ††kamiyama@fc.ritsumei.ac.jp

Abstract　Information-Centric Networking (ICN), which transfers Interest by the name of content without using DNS (Domain Name System) and caches the response content from publishers on routers, is attracting attention as a network that efficiently delivers content such as IoT. There are two types of content: content that anyone can freely obtain and content that only limited users can obtain. When requesting content of the latter type, an access control for determining whether or not the requesting user can access is required. In the current Internet, user requests reach the authoritative DNS server of content providers, so access control is easily realized at the authoritative DNS server. However, in the ICN, it is difficult to control user access because content items are distributed at routers. As an access control method for ICN, a broadcast-based method has been proposed in which the content is encrypted, the key for decryption is changed periodically, and the key is distributed to all subscribing users. However, in this method, users who have lost the access right also have the unchanged key, so there is a problem that the content items can be obtained inadequately by users without access right until the next key is distributed. In this paper, we propose a method that enables access control at publishers by enabling the first Interest packet of content always to reach publishers. We derive the overhead delay of the proposed method by simple analytical model and show that the overhead delay is just several 10 ms to several 100 ms when the requesting rate to a publisher is smaller than 250 per second. Moreover, we show that the proposed method causes approximately 7GB of control traffic per day, while the broadcast-based method causes at least 250 GBytes of unauthorized traffic per day. Therefore, the proposed method can significantly reduce the amount of overhead traffic compared with the broadcast-based method.
Key words　ICN, Public-key cryptography, Access Control

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) の一部のサービスでは，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 [1].

ICN ではユーザ (Consumer) が取得したいデータの条件 (場所，時刻，温度など) を名称として Interest を送信し，ネットワークが要求条件に合致するデータを収集して Consumer に配信する．そのため IoT データなどの効率的な転送が可能となる．従来のインターネットでは CDN (Content Delivery Network) がキャッシュ配信を提供しており，その恩恵を受けるには CDN 事業者との契約が必要になる．ICN ではルータがネットワーク機能としてキャッシュ配信を提供するため，一般ユーザが提供するコンテンツも恩恵を享受することになりキャッシュ配信の民主化が見込まれる．また，要求 Consumer の近くに存在するキャッシュを選択する必要がなく，自動的にユーザの近くのキャッシュから配信が行われるため配信品質や配信効率の向上が期待される．

ICN の概念を実現するために，TRIAD [3]，コンテンツ中心型ネットワーク (CCN: content-centrICNetworking) [4]，データ指向ネットワークアーキテクチャ (DONA: data-oriented network architecture) [7]，名前付きデータネットワーク (NDN: named data networking) [18] などの様々なネットワークが提案されている [16]．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のコンテンツがある．閲覧者限定のコンテンツには例えば，Hulu や Amazon Prime など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．これら有料コンテンツに対する配信要求時には，要求したユーザが試聴できるか否かを判断するアクセス制御が必要になる．

従来のインターネットでは多くの場合，コンテンツは CDN のキャッシュサーバに存在し，ユーザの配信要求はコンテンツ事業者の権威 DNS サーバに届く．コンテンツ事業者はアクセスが可能なユーザのリストを保有しており，そのためコンテンツ事業者の権威 DNS サーバでのアクセス制御が容易に可能である．しかし ICN 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，コンテンツ事業者の権威 DNS サーバや Publisher のホスト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．そのため ICN では全ての配信要求に対してアクセス制御をすることが困難である．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，プライバシィ上，また処理負荷的に困難である．

ICN アクセス制御方式として，アクセス権を有する全ての Consumer に対して鍵を配布し，その鍵を用いることで閲覧者限定のコンテンツを復号して閲覧することが考えられる．アクセス権を有する Consumer 以外は鍵を持たないため，コンテンツを閲覧することができない．この方式では，該当 Publisher のコンテンツ全体を単位にアクセス制御を行うため，1 つの鍵の配布を行えばコンテンツ全体を閲覧することができる (一括鍵配布方式) [12]．しかしアクセス権を喪失した Consumer も鍵を保有しているため，その鍵を用いて不当に配信を要求し閲覧が可能な問題がある．この問題を解決するためには鍵を定期的に変える必要があるが，そのたびにアクセス権を有する全 Consumer に鍵の再配布と更新が必要になる．そのため処理・トラヒックのオーバヘッドが大きな問題である．そこで本稿では，コンテンツの配信に先立ち Consumer から共通鍵暗号方式で暗号化された Consumer の ID を含む Interest を常に Publisher に到達させることで，Publisher にてアクセス制御を可能とする方式を提案する．また一括鍵配布方式と提案方式とで，オーバヘッド遅延時間，不当配信率と不当配信による損失，オーバヘッドトラック量という観点からシミュレーションを行い定量的に比較する．

以下，2. 節で関連研究を述べ，3. 節で提案方式の概要と特徴，動作について述べる．そして 4. 節で提案方式と一括鍵配布方式の性能を評価するための解析式を導出し，5. 節で性能評価を行い，6. 節で全体をまとめる．

2. 関連研究

これまでに ICN のアクセス制御機構として，コンテンツを暗号化せず，アクセス権限を有する Consumer のみコンテンツの取得を行うことができる Encryption-Independent な方式と，コンテンツを暗号化し，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 な方式が提案されている．

Encryption-Independent な方式では，アクセス権限のないコンテンツ利用者がコンテンツ名を取得することを防ぐために，コンテンツ名に対して暗号化 (ハッシュ) を行うことで名前の難読化を行う [2]．Consumer と Publisher 間であらかじめコンテンツ名を暗号化するための共通鍵を配布しておき，ルータ上でデジタル著名を利用して本人確認を行うことで認証を行う方式である Interest-based 型 [2] などがある．これらの方式はルータでのアクセス制御を行うためルータの負荷が高くなる．

Encryption-based な方式では，アクセス権限のあるコンテンツ利用者 (Consumer) のみ暗号化されたコンテンツを復号することができる．復号に用いる鍵の生成方法としては，コンテンツ所有者 (Content Owner) が一意に鍵を作成する Broadcast-based 型 [11]，プロキシ再暗号化によって Consumer ごとに鍵が設定される方式 [17] [8] [19] などがある．ただし Encryption-based 型の方式は，任意の Consumer がコンテンツを受信することが可能であり，鍵の傍受や解読により，アクセス権をもたない Consumer の不当なコンテンツ閲覧を完全に回避することが困難な前方秘匿性の問題がある．本稿では，Encryption-based な方式でアクセス権を有する Consumer のみがコンテンツを取得可能とすることで，前方秘匿性の問題を解決するアクセス制御方式を提案する．

3. 提案方式

3.1 概要と特徴

提案方式では，CCNx 上でのパケットのフォーマットを考慮し [9]，データパケットのヘッダには未定義のフラグ領域があるため，この中の 1 ビットを用いてキャッシュ可否を示すフラグ (CPF: cache permission flag) を用意し，データパケットを受信したルータは CPF が 1 の場合にのみデータパケットをキャッシュする．Consumer はコンテンツ m の先頭チャンク $I_{m,1}$ の要求に先立ちアクセス承認要求のための Interest パケット $I_{m,0}$

を送信するが，本パケットに対するデータパケット $D_{m,0}$ の CPF を 0 にセットし，コンテンツのチャンク $D_{m,1}, D_{m,2}, \cdots$ のパケット送信時は CPF を 1 にセットする．その結果，アクセス要求の Interest は常に Publisher に到達するため，Publisher は要求 Consumer のアクセス権の有無を判断し，アクセス権を有する場合にのみコンテンツを配信可能である．

Publisher はコンテンツを DES 等の共通鍵暗号方式で暗号化するが，Publisher は定期的に共通鍵を変更し，アクセス要求に対する応答として最新の共通鍵を要求 Consumer に配信する．そのため共通鍵の再配布を行うことなく，アクセス権を喪失した Consumer の視聴を防ぐことができる．提案方式では先頭チャンクの配信時にのみアクセス制御のオーバヘッドが発生するが，定期的に共通鍵を変えてもアクセス権を保有する全 Consumer に対する鍵の再配布が不要であり，オーバヘッド処理やトラヒック量を抑えることができる．

3.2 提案方式の動作

図 1 に，提案方式の各処理ステップを示す．

（1） 事前にコンテンツ m の Publisher P_m は公開鍵基盤 (PKI: public key infrastructure) の自身の公開鍵 F_m を公開し，共通鍵 E_m を設定して m を構成する全てのチャンクを E_m で暗号化

（2） Consumer c は m の要求に先立ち，自身の ID c を F_m で暗号化した $F_m(c)$ と，PKI の自身の公開鍵 F_c を，アクセス情報 $D_{m,0}$ を要求する Interest $I_{m,0}$ のペイロードに挿入して $I_{m,0}$ を送信

（3） $D_{m,0}$ は経路上のルータのキャッシュに存在しないので，$I_{m,0}$ は P_m に必ず到達

（4） P_m は $I_{m,0}$ から $F_m(c)$ を取り出し，自身の秘密鍵で復号して c を取得

（5） P_m は c が許可された Consumer なら，E_m を F_c で暗号化した $F_c(E_m)$ を $D_{m,0}$ のペイロードに挿入し，$CPF = 0$ にセットして $D_{m,0}$ を送信

（6） $D_{m,0}$ の中継ルータは $CPF = 0$ なので $D_{m,0}$ をキャッシュしないで c に向けて $D_{m,0}$ を転送

（7） $D_{m,0}$ を受信した c は，$D_{m,0}$ から $F_c(E_m)$ を取り出し，自身の秘密鍵で復号して E_m を取得

（8） c は m のチャンクに対する Interest $I_{m,1}, I_{m,2}, \cdots$ を送信し，該当データをキャッシュしているルータもしくは P_m は $CPF = 1$ にセットして，E_m で暗号化された m のチャンク $D_{m,1}$, $D_{m,2}$, …を送信

（9） $D_{m,1}$, $D_{m,2}$, …を受信した c は E_m で受信データを復号

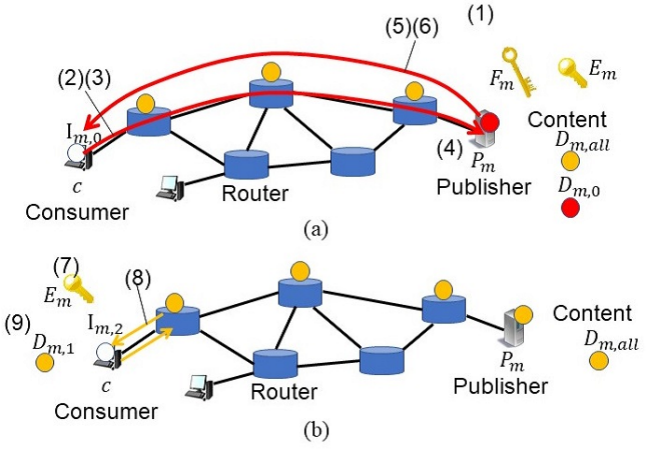

図 1 提案方式の各処理ステップ

提案方式は公開鍵暗号と共通鍵暗号を組み合わせる．Consumer は自身の ID を Publisher に送る際に Publisher の公開鍵で暗号化することで，Consumer の ID を第三者が改ざんすることを防止する．また Publisher はコンテンツの復号に必要な共通鍵を Consumer の公開鍵で暗号化することで，Publisher が送信した共通鍵を第三者が不当に窃取することを防止する．

4. 性能解析

本節では，提案方式と一括鍵配布方式の，オーバヘッド処理時間，オーバヘッドトラヒック量，収益損失を各々，解析により導出する．

オーバヘッドトラヒック量は，鍵の配布に必要な制御トラヒック量と不当な配信による不当配信トラヒック量の和となる．

4.1 提案方式のオーバヘッド処理時間/トラヒック量

提案方式は，アクセス要求 Interest の Publisher への送信と，Publisher でのアクセス判定処理と，共通鍵の Consumer への配信処理時間がオーバヘッドとして必要なため，オーバヘッドの処理時間 T_p は次式で得られる．

$$T_p = \tau + W + S_1 + S_2 \tag{1}$$

ただし τ は Consumer と Publisher との間の RTT, W は Publisher での処理待ち時間，S_1 は $F_m(c)$ の暗号処理時間，S_2 は E_m の暗号化処理時間である．

また提案方式の 1 日の制御トラヒック量 V_p は，アクセス要求 Interest パケット $I_{m,0}$ のサイズ $L_{I,m,0}$ と Publisher から帰ってくる応答パケット $D_{m,0}$ のサイズ $L_{D,m,0}$ と平均ホップ長 h, 総ユーザ数 n，各加入ユーザの 1 日あたりのコンテンツ要求数 λ_r を用いて次式で得られる．

$$V_p = 2h\lambda_r n(L_{I,m,0} + L_{D,m,0}) \tag{2}$$

また提案方式はアクセス権を有さないユーザへの不当配信を完全に防ぐことができるため，収益損失がゼロとなり、不当配信トラヒック量もゼロとなるため，オーバヘッドトラヒック量は V_p となる．

4.2 一括鍵配布方式の制御トラヒック量と収益損失量

一括鍵配布方式ではコンテンツ配信ごとには鍵配布を行わないことから，オーバヘッド処理時間はゼロとなる．1 日あたりの制御トラヒック量は，全てのルータにコンテンツがキャッシュされる場合 (Min) と，どのルータにもコンテンツがキャッシュされない場合 (Max) の各々の場合に対し導出する．鍵要求におけるパケットのサイズ L_I，鍵配布におけるパケットのサイズ L_D，総ユーザ数 n，平均ホップ長 h，ルータ数 n_r，鍵の交換周期 T_m から，Min における 1 日あたりの制御トラヒック量 $V_{b,c,min}$ は，鍵を全てのルータ上にキャッシュする際にかかるトラヒック量 $L_D n_r h$ と 1 ホップで鍵を要求し受け取るのにかかるトラヒック量 $(L_I + L_D)n$ を用いて，

$$V_{b,c,min} = \frac{L_D n_r h + (L_I + L_D)n}{T_m} \tag{3}$$

で得られ, Max における 1 日あたりの制御トラヒック量 $V_{b,c,max}$ は，鍵を Publisher まで要求するのにかかるトラヒック量 $L_I nh$ と Consumer まで Publisher から鍵を配布する際にかかるトラヒック量 $L_D n(h+1)$ を用いて次式で得られる．

$$V_{b,c,max} = \frac{L_I nh + L_D n(h+1)}{T_m} \tag{4}$$

日々，既存ユーザの何人かが退会し，新たに別のユーザが入

会するが，総ユーザ数 n は定常状態にあると仮定すると，1 日に入会するユーザ数 n_{in} と 1 日に退会するユーザ数 n_{out} は同じ値になるため，各加入ユーザが 1 日に退会する確率 p は，

$$p = \frac{n_{in}}{n} = \frac{n_{out}}{n} \tag{5}$$

と仮定できる．1 日に退会するユーザ数 n_{out} は二項分布 $Bin(n,p)$ に従うが，二項分布は n が十分に大きいとき，期待値 $E[x] = np$，分散 $V[x] = np(1-p)$ の標準正規分布に近似できる．そのため 1 日の退会ユーザ数が x である確率 $f(x)$ は，

$$f(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{1}{2}(\frac{x-E[x]}{\sqrt{V[x]}})^2} \tag{6}$$

で近似できる．

サブタイムスロット (STS) をもつタイムスロット (TS) を考える．鍵の交換周期 T_m を TS とみなし，さらに各日を STS とみなすと，各 TS は T_m 個の STS から構成される．つまり 1TS は STS を T_m 個もつ鍵の交換周期 1 回分を表すことになる．x の範囲として，約 99.7%のサンプルが含まれる範囲である 1 から $np+3\sqrt{np(1-p)}$ を考慮すると，各 STS 内で退会者数が x 人である確率 $U(x)$ は次式で得られる．

$$U(x) = \frac{f(x)}{\sum_{k=1}^{np+3\sqrt{np(1-p)}} f(k)} \tag{7}$$

退会したユーザのうち不当配信を行う割合を y，不当配信を行うユーザが退会後に各 STS 内で不当配信を行う平均回数を r とすると，TS の先頭から k 番目の STS で退会したユーザが，その TS の残り STS 内で行う総不当配信回数 G_k は，

$$G_k = \sum_{x=1}^{np+3\sqrt{np(1-p)}} xU(x)yr(T_m - k) \tag{8}$$

となるので，各 TS における総不当配信回数 B_b は次式で得られる．

$$B_b = \sum_{k=1}^{T_m} G_k \tag{9}$$

各 STS 内での各加入ユーザの平均配信要求数は λ_r なので，不当配信率 R_b は次式で得られる．

$$R_b = \frac{B_b}{n\lambda_r + B_b} \tag{10}$$

不当配信による不当配信トラヒック量は，各コンテンツの取得のために送信される総 Interest パケットサイズ $L_{I,all}$ と，コンテンツの総パケットサイズ $L_{D,all}$ を用いて，Min の場合，コンテンツをすべてのルータ上にキャッシュする際にかかるトラヒック量 $L_{D,all}n_r h$ と，1 ホップで不当配信要求を行い受け取るのにかかるトラヒック量 $B_b(L_{I,all} + L_{D,all})$ を用いて，

$$V_{b,u,min} = \frac{L_{D,all}n_r h + B_b(L_{I,all} + L_{D,all})}{T_m} \tag{11}$$

Max の場合，Consumer が不当配信要求でコンテンツを Publisher まで要求して，Publisher からコンテンツが配信する際にかかるトラヒック量 $B_b h(L_{I,all} + L_{D,all})$ を用いて，

$$V_{b,u,max} = \frac{B_b h(L_{I,all} + L_{D,all})}{T_m} \tag{12}$$

で得られる．また，1 人の不当配信ユーザから被る 1 日あたりの収益損失を ψ とすると，1STS あたりの不当配信による収益損失量 Q_b は次式で得られる．

$$Q_b = \frac{B_b \psi}{T_m} \tag{13}$$

また一括鍵配布方式は制御トラヒック量 $V_{b,c,min}$，$V_{b,c,max}$ に加え，不当配信による不当配信トラヒック量 $V_{b,u,min}$，$V_{b,u,max}$ が発生しているため，オーバヘッドトラヒック量は Min の場合 $V_{b,c,min} + V_{b,u,min}$，$Max$ の場合 $V_{b,c,max} + V_{b,u,max}$ となる．

5. 性能評価

5.1 評価条件

提案方式のオーバヘッド処理時間に関して，S_1 を 1.5 (ms)，S_2 を 2.5 (ms) とする [15]．アクセス要求 Interest のパケット $I_{m,0}$ のサイズ $L_{I,m,0}$ を 520 (byte)，一括鍵配布方式の鍵要求におけるパケットのサイズ L_I を 8byte，アクセス要求に対する応答パケット $D_{m,0}$ のサイズ $L_{D,m,0}$，一括鍵配布方式の鍵配布によるコンテンツのパケットサイズ L_d を 264 (byte) とする [5] [9]．

総ユーザ数 n を 6,000,000 とし，各 STS 内で各加入ユーザが配信を行う平均回数 λ_r を 0.1 とする [13]．また，総ユーザ数 n は定常状態にあるので，1 ユーザの平均サービス利用期間を 2 年間とすると 1 日に入会するユーザ数 n_{in} は 8,200 となる．また [6] によると 1 つのネットワークのルータ数は数個から 200 個程度であり，その約 9 割はルータ数が 50 個以下であり，残りの 1 割は 51 以上 200 個以下である．そこでルータ数 n_r を 200 とし，ネットワークの平均ホップ長 h を $\sqrt{200}/2$ と仮定する．

1 人の不当配信ユーザから被る 1 日あたりの収益損失 ψ を Amazon を参考に 500/30 (円) とし，総 Interest パケットサイズ $L_{I,all}$ を 636.16 (kBytes) [9]，100 分の動画，6Mb/s のビットレートを想定しコンテンツの総パケットサイズ $L_{D,all}$ を 4.97(GBytes) とする．

5.2 提案方式のオーバヘッド遅延時間

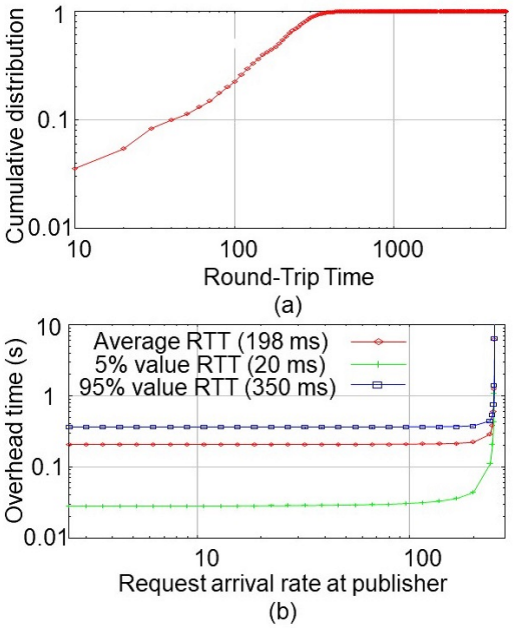

図 2　(a)RTT の累積分布，(b) 要求レートに対する提案方式のオーバヘッド処理時間

図 2(a) に，Amazon EC2 の 8 つのデータセンタから Public DNS server のリスト [14] に掲載されている公開 DNS サーバ

に対して traceroute を行い測定した RTT の累積分布を示す．測定 RTT の平均値 198 (ミリ秒)，5%値 20 (ミリ秒)，95%値 350 (ミリ秒) を，RTT τ のサンプルとして評価に用いる．また Publisher には λ(個/秒) のポアソン分布に従い配信要求が到着し，Publisher のサービス時間は平均が $1/\mu = S_1 + S_2 = 4.0$ (ミリ秒) の指数分布に従うとすると，Publisher での処理時間 W は $W = 1/(\mu - \lambda)$ で与えられる．

図 2(b) に RTT の 3 つの値に対し，式 (1) から得られる提案方式のオーバヘッド処理時間 T_p を λ に対してプロットする．提案方式は Publisher への要求レートが約 250 個/秒より小さい場合には数 10ms〜数 100ms 程度のオーバヘッド時間でアクセス制御が可能であるが，要求レートがそれより増加すると急激にオーバヘッド時間が大きくなり鍵の配布が困難になる．これは S_1 と S_2 の値に大きく影響されるが，これら値が小さくなれば，さらに高い要求レートでも配布が可能となる．

5.3 一括鍵配布方式の不当配信数と収益減少度

図 3 に，鍵の配布周期 T_m に対し，式 (10) から得られる一括鍵配布方式の不当配信率 R_b をプロットする．ただし退会したユーザのうち不当配信を行う割合 y を (a)0.0001，(b)0.001，(c)0.1 に各々設定し，退会後に各不当配信ユーザが各 STS 内で不当配信を行う平均回数 r を 0.3，0.5，1.0，3.0 に設定した各々の場合で評価する．不当配信を行う退会ユーザの割合 y が大きなほど，また 1 日あたりの不当配信回数 r が大きなほど，さらに鍵の配布周期 T_m が大きなほど，不当配信が全配信に占める割合 R_b は増加する．例えば，不当配信を行うユーザが 0.1%程度，T_m が 10 日程度，r が 3 程度の場合，不当配信率は 0.01 程度になることが確認できる．

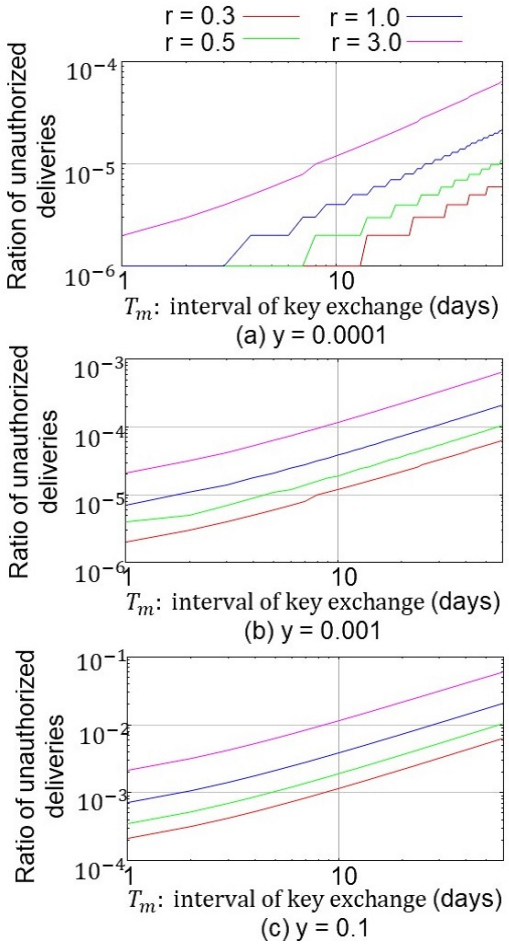

図 3　鍵の交換周期に対する一括鍵配布方式の不当配信率

次に図 4(a) に鍵の交換周期 T_m に対し，一括鍵配布方式の 1STS あたりの収益減少量 Q_b をプロットする．ただし y を 0.01 とした．鍵の交換周期 T_m の増加に伴い，不当配信が可能な期間が増大する．また r の増加に伴い不当配信率が増加する．そのため T_m や r の増加に伴い Q_b も増加する．また，図 4(b) に，退会したユーザのうち不当配信を行う割合 y に対し，Q_b をプロットする．ただし r を 0.5 とした．T_m や y の増加に伴い Q_b が増加することが確認できる．

一方，提案方式は不当配信率がゼロとなるため，一括鍵配布方式とは違い不当配信による収益減少が生じない．

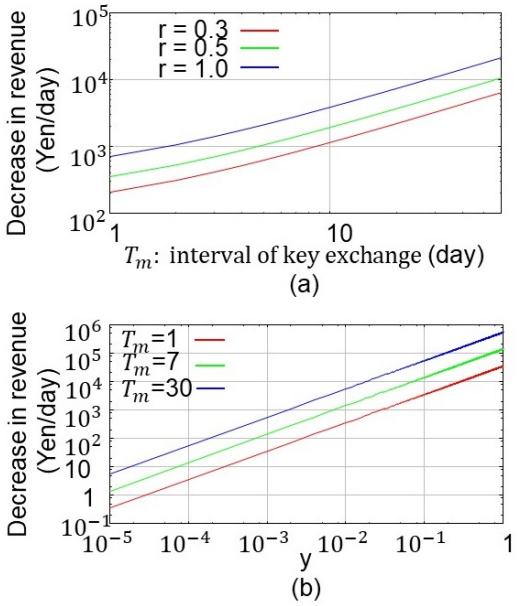

図 4　(a) 鍵の交換周期に対する収益減少量，(b) 不当配信ユーザ割合に対する収益減少量

5.4 両方式のオーバヘッドトラヒック量

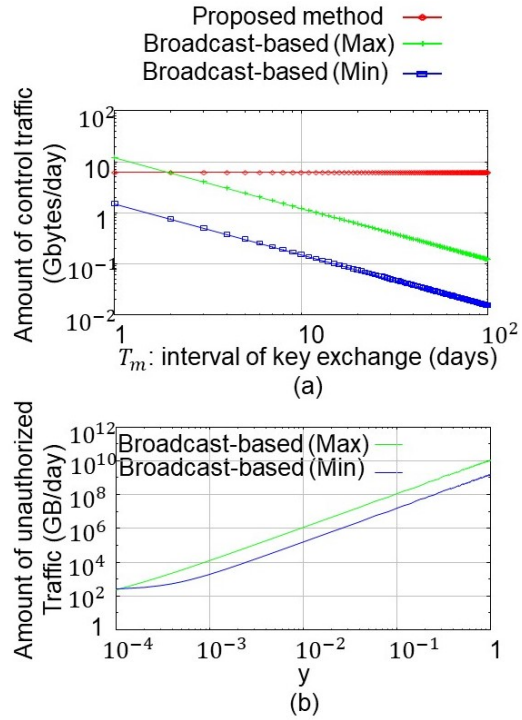

図 5　(a) 鍵の交換周期に対するオーバヘッドトラヒック量，(b) 不当配信ユーザ比率に対する一括鍵配布方式の不当配信トラヒック量

式 (2) から算出できる提案方式の制御トラヒック量 V_p と，

式 (3) と式 (4) から得られる一括鍵配布方式の Min と Max における制御トラヒック量 $V_{b,c,min}$，$V_{b,c,max}$ を各々，T_m に対して図 5(a) にプロットする．一括鍵配布方式では，鍵の交換周期が来るたびにトラヒックが発生するが 1 日あたりに換算した値をプロットしている．一括鍵配布方式は鍵の交換周期の増加に伴い 1 日あたりの制御トラヒック量が減少するが，提案方式は T_m とは無関係に一定の制御トラヒックが 1 日あたりに発生する．提案方式は 1 日あたり $7GB$ 近くの制御トラヒックが発生し，一括鍵配布方式と比べると T_m の広い領域で制御トラヒック量が多い．しかし，一括鍵配布方式は不当配信により，本来発生しなかったコンテンツ配布による不正トラヒックが発生する．

そこで図 5(b) に，式 (11)(12) から得られる一括鍵配布方式の不当配信トラヒック量 $V_{b,u,min}$，$V_{b,u,max}$ を y に対してプロットする．ただし r を 0.5，T_m を 30 とした．退会したユーザのうち不当配信を行う割合 y が増加するほど不当配信トラヒック量 $V_{b,u,min}$，$V_{b,u,max}$ は増加し，最大で 10^9〜10^{10} (GBytes) の，最低でも約 250 (GBytes) の不正トラヒックが 1 日あたりに発生している．一括鍵配信方式の不当配信トラヒック量は，提案方式の制御トラヒック量よりも遥かに大きく，制御トラヒック量と不当配信トラヒック量を考慮したオーバヘッドトラヒック量を考えると，提案方式は一括鍵配布方式と比較してオーバヘッドトラヒック量を大きく低減できることが確認できる．

6. ま と め

IoT データやコンテンツを効率的に転送できるネットワークとして ICN が注目されているが，ICN ではルータでコンテンツがキャッシュされるため，コンテンツ提供者 (Publisher) でのアクセス制御が困難である．そのため特定のユーザのみ取得可能なコンテンツに対するアクセス制御が課題である．そこで本稿では，データの配信に先立ちアクセス制御のための要求パケットに対する応答パケットを経路上のルータでキャッシュさせないことで，コンテンツの要求時に常に Publisher に要求が届くようにする方式を提案した．そして提案方式のオーバヘッド処理時間とオーバヘッドトラヒック量，そして既存のアクセス制御方式として Broadcast 型の一括鍵配布方式のオーバヘッドトラヒック量と不当配信による収益減少量を解析的に導出した．そして数値評価により，以下のことを確認した．

- 提案方式のデメリットとして，アクセス承認要求のために Consumer と Publisher との間で 1 往復の制御パケットの交換が必要となるが，その処理遅延時間は Publisher への要求レートが約 250 個/秒より小さい場合には，数 10ms〜数 100ms 程度に抑えられる．
- 一括鍵配布方式では，不当配信を防ぐために定期的に鍵を変え，鍵の再配布と更新を行なう必要がある．そのため鍵の更新までには退会ユーザが不当にコンテンツを取得できる期間が発生し，Publisher は収益が減少する．例えば一月の 1 人あたりの利益が 500 円の場合，不当配信ユーザ割合が 0.01 程度の時 1 日あたり 7500 円程度である．これは月会費が低いため大きく影響を及ぼさない．しかし月会費が高くなると更なる収益減少が発生する可能性がある．一方，提案方式は不当配信を完全に防ぐことができ，Publisher の収益の減少を回避できる．
- 提案方式の制御トラヒック量をオーバヘッドトラヒックとみなすと，提案方式では約 7GBytes のオーバヘッドトラヒック量が毎日発生する．一方，一括鍵配布方式の不当配信による不当なトラヒック量や鍵の一括配布による制御トラヒック量をオーバヘッドトラヒックとみなすと，一括鍵配布方式では不当トラヒックが最低でも約 250 (GBytes) 発生し，提案方式よりもオーバヘッドトラヒック量が大きい．今後は実際のネットワークトポロジを作成しシミュレーション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] 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.
[2] C. Ghali, M. Schlosberg, G. Tsudik, and C. Wood, Interest-based access control for content centric networks (extended version), in Proc. 2nd Int. Conf. Inform.-Centric Netw., 2015, pp.147-156.
[3] M. Gritter and D. R. Cheriton, An architecture for content routing support in the Internet, USENIX USITS 2001.
[4] V. Jacobson, et al., Networking Named Content, ACM CoNEXT 2009.
[5] J. Jonsson, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version2.1, IRTF RFC 3447, Feb. 2002.
[6] S. Knight, H. X. Nguyen, N. Falkner, R. Bowden, and M. Roughan, The Internet Topology Zoo, IEEE Journal on Selected Areas in Communications, Vol. 29, No. 9, Oct. 2011.
[7] T. Koponen, M. Chawla, B. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, A data-oriented (and beyond) network architecture, ACM SIGCOMM 2007.
[8] M. Mangili, F. Martignon, and S. Paraboschi, A cache-aware mechanism to enforce confidentiality, trackability and access policy evolution in content-centric networks, Elsevier Computer Networks, Vol. 76, pp. 126–145, 2015.
[9] M. Masko, I. Solis, and C. Wood, Content-Centric Networking (CCNx) Messages in TLV Format, IRTF RFC 8609, July 2019.
[10] S. Misra, R. Tourani, and N. E. Majd, Secure content delivery in information-centric networks: Design, implementation, and analyses, ACM ICN 2013.
[11] S. Misra, R. Tourani, F. Natividad, T. Mick, N. E. Majd, and H. Huang, Accconf: An access control framework for leveraging in-network cached data in the icn-enabled wireless edge, IEEE Trans. on Dependable and Secure Computing, Vol. 16, No. 1, pp. 5–17, 2017.
[12] S. Misra, et al., AccConF: An access control framework for leveraging in-network cached data in the ICN-enabled wireless edge, IEEE Trans. Dependable and Secure Computing, 16 (1), Jan./Feb. 2019.
[13] 日経クロストレンド, 2020/1/31, https://xtrend.nikkei.com/atcl/contents/watch/00013/00841/
[14] Public DNS Server List, https://public-dns.info
[15] K. Xue, et al., A Secure, Efficient, and Accountable Edge-Based Access Control Framework for Information Centric Networks, IEEE/ACM Transactions on Networking, Vol. 27, No. 3, pp. 1220-1233, June 2019.
[16] G. Xylomenos, et al., A Survey of Information-CentrICNetworking Research, IEEE Communications Survey and Tutorials, Vol. 16, No. 2, pp.1024-1049, 2014.
[17] C. Wood and E. Uzun, Flexible end-to-end content security in CCN, IEEE CCNC 2014.
[18] L. Zhang, et al., Named Data Networking (NDN) Project, Technical Report NDN-0001, Oct. 2010.
[19] Q. Zheng, G.Wang, R. Ravindran, and A. Azgin, Achieving secure and scalable data access control in information-centric networking, IEEE ICC 2015.