Vol.2019-DPS-177 No.4
2019/1/31

# ICNにおけるアクセスコントロールに関する一考察

田上 敦士[1,a)]　スクソーブン カリカ[1]

**概要**：ICN（Information Centric Networking）は，新しいネットワークアーキテクチャとして注目を浴びている．ICNは，エンド-エンドのコネクションをベースとしたアーキテクチャから，コンテンツを主体としたアーキテクチャへの考え方の転換を求めている．セキュリティの観点からも，SSL/TLSといったセキュア接続をベースとしたセキュリティではなく，コンテンツ自体の暗号化や電子署名をベースとしたセキュリティが用いられている．特にアクセスコントロールにおいては，これまでのネットワークやサーバへの接続性へのアクセスコントロールではなく，コンテンツへのアクセスコントロールをネットワークレイヤで実現することとなるため，様々な課題が生じるが，現在十分に議論されているとは言い難い．本稿では，ICNにおけるアクセスコントロール技術について，現状と残された課題について概略を示す．さらに，暗号化ベースのコンテンツへのアクセスコントロールと，経路広報を利用したリージョンコントロールについて，我々が提案した技術について紹介し，今後のネットワーク技術の課題について述べる．

# A Study on Access Control in Information Centric Networking

## 1. はじめに

将来インターネットアーキテクチャとして，ICN（Information Centric Networking）が注目されている [1], [2]．その主となる考え方は，端末間の接続から，コンテンツの流通へのネットワークの役割の変化である．これにより，現在のインターネットが抱えているコネクションの保持に起因する課題，すなわち，モビリティやネットワーク内資源（キャッシュや計算機資源）の活用などについて，解決することが期待されている [3]．さらにセキュリティの観点からも，ICNはこれまでのネットワークセキュリティの考え方を変えている [4]．IPネットワークをはじめとするコネクションをベースとしたネットワークアーキテクチャにおいて，セキュア通信とは，通信相手の正当性を保証することと，通信相手との間に傍受されない安全な通信路を生成することを基本としている．しかしながら，コネクションに基づくセキュア通信は，プロキシなどによるネットワークの最適化・効率化において弊害が生じることが指摘されている [5]. ICNにおいては，コンテンツに署名をつけることで発信者を特定し，コンテンツ自体を暗号化することで盗聴を防いでいる [6]．これは，キャッシュされたコンテンツにおいても発信者を特定可能であったり，エッジコンピューティングなどネットワーク側で近傍のノードに要求を転送することを可能としたり，ネットワークの最適化・効率化において優位である．本稿では，そのようなICNのセキュリティの中で，アクセスコントロールに焦点を絞り考察する．

ICNにおけるアクセスコントロールとは，通常複数のユーザに対して配信される静的なコンテンツを参照できるユーザを制限するものである．特定のユーザにのみ配信される動的なコンテンツに対してはキャッシュなどを考慮する必要はなく，SSL/TLSと同等なプロトコルを利用可能である．静的なコンテンツ（以下単にコンテンツと呼ぶ）に対するアクセスコントロール手法としては，暗号化されたコンテンツを復号できるユーザを制御する手法と，コンテンツへの経路を制御し，特定のユーザからのみコンテンツへの経路が見えるようにする手法が考えられる．ユーザが何を要求したかといったユーザ情報の公開範囲をユーザ側で制御するというアクセスコントロールも提案されているが [7]，検閲の回避を目的としており通常プライバシーに分類されるため，本稿のスコープ外とする．

コンテンツを復号できるユーザの制御は，暗号化されたコンテンツを復号できる鍵の配布を制限するものである [6]．暗号化されたコンテンツ自体は，すべてのユーザが

[1] KDDI 総合研究所
KDDI Research, Inc., Fujimino, Saitama 356–8502, Japan
[a)] tagami@kddi-research.jp

同一のものを入手可能であるため，キャッシュの活用や，サーバの負荷という面で優位である．一方で，アクセス権の失効（revocation）処理が難しいという課題もある．また，ICN はネットワーク層の技術であるが，鍵の管理やコンテンツの復号をどのレイヤで行うべきかという議論も十分ではない．

コンテンツへの経路の制御は，名前をベースにフィルタリングを行うことで，コンテンツへの到達性を制限するものである [8], [9]．これまで，本手法は，主にプライベートネットワークからの情報漏洩を防ぐ目的で検討されており，アクセスコントロールとしての観点からは議論されていない．しかしながら，リージョンコントロールなどネットワークドメインをベースとしたアクセスコントロールも必要である．

本論文では，前述した 2 種類のアクセスコントロールについて，現状の課題を示し，それぞれの解決方法について考案する．以後，2 節において，ICN の概要ならびにそのアクセスコントロールに関する既存研究について，3 節において，現状のアクセスコントロールの課題について述べる．4 節において，前節で述べた課題についての解決手法について述べ，5 節において，今後の課題についてまとめる．

## 2. 関連研究

### 2.1 ICN

ICN（Information Centric Networking）とは，コンテンツを主体としたネットワークアーキテクチャの総称である [3]．本稿では，現在一般的な ICN アーキテクチャである CCN（Content Centric Networking）[10]/NDN（Named Data Networking）[11] を前提とする．CCN/NDN において，すべてのコンテンツは，`ndn:/ipsj.or.jp/sig/dps/177/paper20.pdf` のような，階層的な名前を持つ．コンテンツを求めるユーザ（Consumer）は，コンテンツの名前に対して要求パケット（Interest パケット）を送信する．ICN ルータは，FIB（Forwarding Information Base）に従い，Interest パケットを，コンテンツが存在するサーバ（Producer）まで転送する．FIB には，名前のプレフィックス毎に次ホップが記載されており，最長部分一致によって次ホップが決定される．Interest パケットを受信した Producer は，要求された名前を持つコンテンツを Data パケットに格納して送信する．

CCN/NDN においてネットワークを流れるすべてのデータ片はユニークな名前が付けられている．これにより，ICN ルータはどのコンテンツが要求されたのか，また，どのコンテンツを現在配送しているのかを把握できる．IP ベースのネットワークアーキテクチャでは，ネットワーク内のキャッシュを実現する場合，アプリケーションレベルでの解析が必要であったが，ICN では名前を用いて容易に実現可能となる．

以後簡単化のために，CCN/NDN を単に ICN と呼ぶ．また，通常 CCN/NDN において，ユーザとサーバを Consumer，Producer と呼ぶが，本稿では明瞭さを重視してユーザ/サーバで統一する．

### 2.2 暗号化ベースのアクセスコントロール

現在 ICN で採用されているアクセスコントロールの手法は，暗号化に基づいたアクセスコントロールである．本アクセスコントロールの考え方は，暗号化されたコンテンツの復号鍵を持つユーザがアクセス権を持つことである．Misra ら [12] は，BCE（BroadCast Encryption）を，Ion ら [13] は ABE（Attribute-based Encryption）を用いたアクセスコントロール手法を提案している．BCE/ABE の特徴としては，1 つの暗号鍵に対して複数の復号鍵が存在するということである．つまり，それぞれ異なる復号鍵を保持する複数のユーザに対して，1 つの暗号化コンテンツを送信することができる．この特徴により，キャッシュの有効利用が可能となる．一方で，一度アクセス権を与えたユーザの権利を剥奪する場合，コンテンツを再暗号化する必要がある．

Kurihara ら [6] は Manifest と呼ぶメタファイルを起点としたフレームワークを提案している．サイズの大きいコンテンツの場合，コンテンツ自体は共通鍵で暗号化し，その共通鍵（もしくは暗号化された共通鍵の復号鍵）を BCE や ABE, RSA 等の方法で暗号化する．公開鍵暗号は，共通鍵暗号と比較して計算量が大きくなるため，コンテンツ自体を共通鍵で暗号化する本手法は，計算機負荷の面で有利である．しかしながら，共通鍵が流出した場合，前述の手法と同様にコンテンツの再暗号化は必要となる．

### 2.3 経路ベースのアクセスコントロール

アクセスコントロールのもう 1 つの考え方は，コンテンツに対しての要求（Interest パケット）の到達性を制御するというものである．Ghali ら [14] は，コンテンツの名前が暗号化されている IBAC（Interest-Based Access Control）を提案している． 本手法は，コンテンツの名前をハッシュベースもしくは暗号化ベースの名前にすることで，許可されていないユーザが名前を予測することを困難にする．一方で，ユーザ毎に個別の名前を生成するため，ネットワーク内キャッシュの活用によりコンテンツの配信効率を上げるという ICN の設計とは矛盾する．

ネットワーク内の ICN ルータでにおいて名前によるフィルタリングを行うことによるアクセスコントロールも提案されている．Goergen ら [8] は，Data パケットをフィルタリングするためのファイアウォールを ICN 上で設計した．Kondo ら [9] は，プライベートネットワークのエッジにおいて異常な名前を用いた情報漏えいのリスクについて

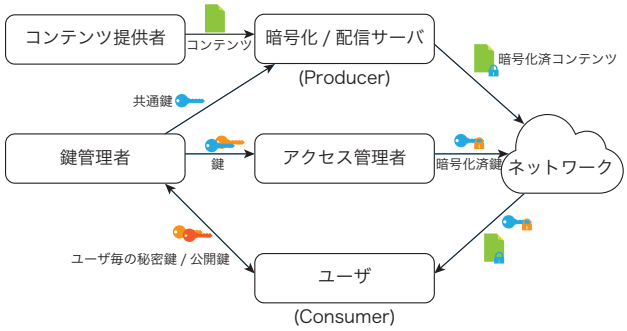


**図 1** ICN のコンテンツへのアクセスコントロールの一例 (Kurihara ら [6] の図をベースに作成)

**Fig. 1** An example of access control framework on ICN. (adapted from Kurihara [6])

分析した．これらは，ゲートウェイノード上で送受信される Data パケットをフィルタリングし，特定のネットワークとの間で悪意のあるデータが送受信されるのを防ぐことを目的としている．

## 3. 課題

### 3.1 アクセスコントロール

図 1 に，ICN における暗号化ベースのアクセスコントロールの一例を示す．暗号化/配信サーバは，鍵管理者から渡された共通鍵を用いてコンテンツを暗号化する．アクセス管理者はアクセスポリシーに従って，共通鍵を暗号化し配布する．ユーザは暗号化されたコンテンツと共有鍵を取得し，自らの秘密鍵を用いて復号する．これにより，ネットワークに流れる全てのコンテンツ（鍵も含む）が暗号化され，アクセスポリシーに反するユーザがコンテンツを見ることはできない．

本フレームワークには以下の 2 つの課題が存在する．

- 共通鍵が流出した場合，もしくは，とあるユーザのアクセス権が失効する場合，コンテンツを再び新しい共通鍵で暗号化する必要がある．
- ユーザに対して，どの単位でアクセス権を与えるかどうかの議論が不十分である．

前者の課題に関しては，コンテンツが共通鍵で暗号化されている以上，回避できない課題である．SSL/TLS などのように鍵を定期的に変更する手法も提案されているが [15]，キャッシュ上にある永続的なコンテンツに対しては意味がない．

後者の課題に関しては，ICN がネットワークレイヤの技術であることに起因する．ネットワークレイヤにおけるアクセスコントロールとは，とあるネットワークもしくはサーバにアクセス可能であるかどうかの制御である．一方で，ICN においてアクセスする対象はコンテンツである．これは既存のシステムにおいてはアプリケーションレイヤで考慮すべき制御である．例えば，iOS や Android OS のような最近のモバイル OS は，*App Sandbox* [16] や *Application Sandbox* [17] と呼ばれる機能をファイルストレージシステムに有している．この機能は，アプリケーション毎にファイル格納コンテナを提供し，他のアプリケーションからのコンテンツへのアクセスを制限することを実現する．これらより，ICN においてもアプリケーション単位でのアクセス制御を実現すべきである．しかしながら，これらの議論は十分になされていない．

### 3.2 リージョンコントロール

著作権もしくは国/地域の法律のために，一部のコンテンツは，地理的な特定地域にサービスを限定する必要がある [18]．現在のインターネットでは，このような配信地域の制御（リージョンコントロール）は，GPS（Global Positioning System）や WPS（Wi-Fi Positioning System）を用いて実現されている [19]．ネットワーク上の情報を利用する手法としては，IP アドレスを用いて制御する方法も存在する [20]．しかしながら，これらの技術は，ユーザからの情報を利用するため，制御を回避可能である課題 [21] や，位置情報を取り扱うプライバシーの課題 [22] が存在する．

リージョンコントロールはアクセスコントロールの一種である．このため，暗号化ベースのアクセスコントロール技術においても実現可能である．例えば ABE を用いて各ユーザに位置情報を属性を持つ鍵を配布することで実現可能である．しかしながら，一般的に国/地域間の回線は帯域に限りがあるため，リージョンコントロールはコンテンツ配信範囲の制限で実現することが好ましい．ICN の名前をベースにした経路制御により，ネットワークレイヤでのリージョンコントロールの実現できるポテンシャルはあるが，それに関して十分に議論されていない．

## 4. 提案手法

### 4.1 再暗号化に基づくアクセスコントロール

我々は，アクセスコントロールの課題を解決するために，Proxy Re-encryption を用いたアクセスコントロール技術を提案した [23], [24]．Proxy Re-encryption [25] とは，暗号化されたデータ列を，復号することなしに，別の鍵で暗号化されたデータに変換する技術である．この時用いる変換器を再暗号化鍵（re-encryption key）と呼ぶ．応用例としてはクラウドストレージサービスがあり，暗号化されたクラウド上のコンテンツを，クラウドで復号することなしに，特定のユーザに向けて配信することを実現する [26]．提案手法のアイデアは，ユーザのデバイス上で再暗号化を行い，アプリケーション毎のアクセスコントロールを実現することである．

図 2 に，Proxy Re-encryption に基づくアクセスコントロールにおける，ユーザ端末のコンポーネント図を示す．

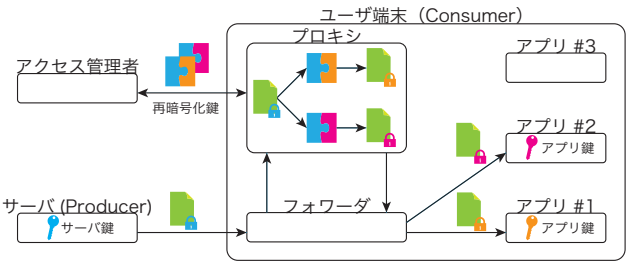


**図 2** 再暗号化（Proxy Re-Encryption）に基づく ICN アクセスコントロール

**Fig. 2** An ICN access control framework based on in-device proxy re-encryption.

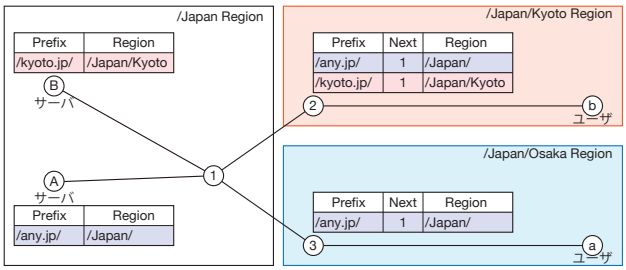


**図 3** 経路広報に基づくリージョンコントロールの基本的アイデア

**Fig. 3** Basic idea of the region control based on the route advertisement.

ICN 実装の特徴として，フォワーダ（forwarder）と呼ばれる ICN ルータと同等の転送モジュールがユーザ端末に組み込まれていることがある．ICN パケットを送受信するアプリケーションは *face* と呼ばれる仮想インタフェースを生成し，フォワーダに接続する．フォワーダは受信した ICN パケットを，FIB や PIT（Pending Interest Table）など ICN のフォワーディングテーブルに従い転送する．すなわち，各アプリケーションが論理的に 1 つのネットワークノードとしてフォワーダに接続されている形となる．この実装形態により，再暗号化処理を行うプロキシを端末内にアプリケーションと独立した形で組み込む．

各アプリは，それぞれアプリ固有の共通鍵（以後，アプリ鍵と呼ぶ）を持つ．各アプリケーションは，アクセス管理者に依頼し，アプリ鍵への再暗号化鍵（re-encryption key）を端末内のプロキシに設置する．プロキシは再暗号化鍵を用いて，サーバ（もしくはキャッシュ）から受信した暗号化されたコンテンツを，それぞれのアプリ鍵で暗号化されたコンテンツへ変換する．本アクセスコントロールには以下の利点がある．

**共通鍵が流出しない** サーバが暗号化に用いた共通鍵（サーバ鍵と呼ぶ）を復号に用いるノードは存在しないため，共通鍵が流出することはない．

**アクセス権の失効が容易** もし，あるアプリのアクセス権が失効した場合，プロキシから再暗号化鍵を削除するだけで，アプリに対するアクセス権を削除することができる．アプリ鍵で復号可能なコンテンツがキャッシュに残ることもない．

**アプリ毎のアクセス制御が可能** コンテンツは，アプリ内以外ではプロキシも含めてコンテンツが暗号化されており，アプリ毎に保持するアプリ鍵を用いて復号されるため，他のアプリ（例えば図 2 におけるアプリ#3）では復号できない．

**キャッシュを活用可能** ネットワークを流れるコンテンツは，サーバ鍵で暗号化されたコンテンツのみであるため，ネットワーク内のキャッシュを活用可能である．

欠点としては，暗号化によるオーバーヘッドが考えられる．しかしながら，再符号化によるオーバーヘッドは ms オーダーであり [24]，利点と比較すると無視できると考える．

### 4.2 経路広報に基づくリージョンコントロール

名前を用いてコンテンツの配信範囲を制限する手法は，インターネットプロトコルにおいて一般的な手法である．例えば，NNTP（Network News Transfer Protocol） [27] は，`fj.os.linux` のような階層的なニュースグループを持ち，各サーバは指定したニュースグループを購読する．例えば，通常 `japan.` で始まるニュースグループは，日本国内のサーバからのみ購読され，日本国外には配信されない．同様にチャットプロトコルである IRC（Internet Relay Chat） [28] においてはチャンネルマスクと呼ばれる機能があり，例えば `#example:*.jp` という名前のチャンネルは，`.jp` で終わるサーバにのみ配信される．これらの考え方に基づいて ICN におけるリージョンコントロールを提案する．

基本的なアイデアは，各ルータならびに各サーバが広報する経路に階層的なリージョン情報を付与し，経路の広報範囲を制限するものである．図 3 に本アイデアを図示する．図中においてサーバ B が広報したプレフィックス `/kyoto.jp/` はリージョン `/Japan/Kyoto` に配信を制限しているため，`/Japan/Osaka` リージョンには広報されず，ユーザ a から送出した要求パケットはサーバまで到達できない．一方で，サーバ A が広報したプレフィックス `/any.jp/` はリージョン `/Japan/` すべての広報されるため，ユーザ a, b どちらからもアクセス可能となる．

本手法は，ネットワーク側の情報のみを利用し，ユーザ端末の位置情報などの個人情報を送受信する必要がないため，プライバシーやリージョン回避の面で優位である．また，実際のプロトコルは，経路制御プロトコルに依存する．しかしながら ICN の経路制御手法に関しては多くが提案されている状況 [29], [30] であり，標準化されていない．このため，一般的な経路制御であるリンクステートプロトコルと名前解決プロトコルに関して議論する．

#### 4.2.1 リンクステートプロトコル

NLSR（Named-data Link State Routing）[29] は，ICN 向けのリンクステートプロトコルであり，NDN のプロジェクトの 1 部として開発されている [31]. NLSR は、特定ドメイン内のすべてのルータが同じリンクステート情報を持つように，ChronoSync [32] を用いて LSA（Link State Advertisement）を同期させる．LSA にはルータの隣接情報を交換する Adjacency LSA だけでなく，Prefix LSA と呼ぶコンテンツへの接続情報を交換する LSA も定義している．

これらの LSA にリージョン情報を示すエントリを追加することで，前述のリージョンコントロールを実現可能である．各 ICN ルータはリージョン情報を元に不要なルータ/コンテンツを持つ LSA を除いた状態で経路を計算し FIB テーブルを生成する．これにより，リージョン外の経路が FIB に掲載されることは無い．また，LSA は，ドメイン毎に同期されるため，不要な LSA を最初から同期させない事により，余分な制御メッセージを削減することも可能である．

#### 4.2.2 名前解決プロトコル

ICN の経路数に関しては様々な仮定があるが，主なものは URI の TLD（Top Level Domain）がそのまま流れるというものと，BGP のフルルートと同等のものに集約されるというものである．現在インターネットの TLD 数は 2018 年の Q3 において 3.4 億あると予測されており [33]，BGP のフルルートが 80 万程度 [34] であるとすると 400 倍近くになる．これらのギャップを埋める，または，グローバルレベルでのスケーラビリティを保証するために，NRS（Name Resolution Service）が提案されている．Kim ら [30] は，経路がない名前に対して NRS サーバに問い合わせる手法を提案している．Ascigil ら [35] は，各ルータの FIB を Routing Service（NRS に相当）のキャッシュと考え，スケーラビリティを担保する手法を提案している．これらの手法は LISP（Locator/ID Separation Protocol）[36] と同様に，ドメイン内で広報する経路数を減らすことを可能とする．

NRS の各エントリにリージョン情報を付与し，リージョン外からの要求パケットへの応答をブロックすることで提案するリージョンコントロールを実現可能である．要求パケットがどのリージョンから送出されたかの判断は，エッジルータが，どのリージョンから受信した要求パケットかどうかを判断することで実現可能である．例えば図 3 において，ルータ 1 で NRS のリゾルバが動作している場合，ルータ 3 から受信した `/kyoto.jp/` に対する Interest パケットは NRS が応答しない（経路がないと返信する）ことにより，`/Japan/Osaka` リージョンからの要求をブロックすることができる．

#### 4.2.3 ネットワークトポロジと地理的トポロジとの関係

本提案では，階層的なリージョン情報を想定している．本階層はネットワークトポロジと一致している必要がある．例えば，図 3 において，`/Japan/Kyoto` リージョンが `/Japan/Osaka` リージョンの下にある場合，`/Japan/Osaka` リージョンでブロックされている経路が，`/Japan/Kyoto` リージョンに到達できない．このため，物理的もしくは論理的にネットワークトポロジと地理的トポロジは一致する必要がある．

ICN において論理的なネットワークを構築する手段としては，Link Object [37] の活用が考えられる．これは，プレフィックスと Forwarding Hint のマッピングを示しており，Interest パケットを任意のルータに転送することを可能とする．

## 5. おわりに

本稿では，ICN のアクセスコントロールに関して，アプリケーション単位でのアクセスコントロールと，リージョンコントロールについて，現状の課題と解決方法について述べた．ICN は，コンテンツを中心に据えた新しいネットワークアーキテクチャであり，最終的にコンテンツを管理・利用するアプリケーションや OS などとの連携が重要となる．アクセスコントロールに関しては，キャッシュなどネットワーク内の機能を有効活用するために，複数ノード間でのコンテンツの共有を考慮してアクセスコントロールを設計する必要がある．また，リージョンコントロールのように従来アプリケーションレイヤで行ってきた機能をネットワーク側で実現することで，プライバシや制御回避の問題を解決できる可能性もある．さらに，よりネットワークと OS が融合し，ローカルストレージをすべて ICN のキャッシュとして扱うことで，統一的なアクセスコントロールを実現することも考えられる．

本稿では，それぞれの解決手法についてアイデアのみを述べた．今後はそれぞれの手法について詳細設計ならびに評価を行うとともに、これらの議論の中から新たなセキュリティフレームワークが出現することを期待する．

**謝辞** 本研究成果の一部は，NICT 委託研究（No.181）ならびに欧州連合 HORIZON2020（No.723014）により得られたものです。

### 参考文献

[1] Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H. and Braynard, R. L.: Networking Named Content, *International Conference on Emerging Networking Experiments and Technologies*, CoNEXT, ACM, pp. 1–12 (2009).

[2] Zhang, L., Afanasyev, A., Burke, J., Jacobson, V., Claffy, K. C., Crowley, P., Papadopoulos, C., Wang, L. and Zhang, B.: Named Data Networking, *ACM SIGCOMM Computer Communication Review*, Vol. 44,

No. 3, pp. 66–73 (2014).
[3] Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D. and Ohlman, B.: A Survey of Information-centric Networking, *IEEE Communications Magazine*, Vol. 50, No. 7, pp. 26–36 (2012).
[4] Tourani, R., Misra, S., Mick, T. and Panwar, G.: Security, Privacy, and Access Control in Information-Centric Networking: A Survey, *IEEE Communications Surveys Tutorials*, Vol. 20, No. 1, pp. 566–600 (2018).
[5] : Proxy User Stories, HTTP/2 Specification Wiki (online), available from ⟨`https://github.com/http2/http2-spec/wiki/Proxy-User-Stories`⟩ (accessed 2018-12-28).
[6] Kurihara, J., Uzun, E. and Wood, C. A.: An Encryption-based Access Control Framework for Content-centric Networking, *IFIP Networking Conference*, IFIP Networking, pp. 1–9 (2015).
[7] Kurihara, J., Yokota, K. and Tagami, A.: A Consumer-Driven Access Control Approach to Censorship Circumvention in Content-Centric Networking, *ACM Conference on Information-Centric Networking*, ACM-ICN, pp. 186–194 (2016).
[8] Goergen, D., Cholez, T., Francois, J. and Engel, T.: A Semantic Firewall for Content-Centric Networking, *Proc. of IFIP/IEEE International Symposium on Integrated Network Management*, IM, pp. 478–484 (2013).
[9] Kondo, D., Silverston, T., Tode, H., Asami, T. and Perrin, O.: Name Anomaly Detection for ICN, *Proc. of IEEE International Symposium on Local and Metropolitan Area Networks*, LANMAN, Rome, Italy, IEEE (2017).
[10] fd.io: CICN, FD.IO Project (online), available from ⟨`https://wiki.fd.io/view/Cicn`⟩ (accessed 2018-12-28).
[11] : Named Data Networking (NDN), NDN Project (online), available from ⟨`https://named-data.net/`⟩ (accessed 2018-12-28).
[12] Misra, S., Tourani, R. and Majd, N. E.: Secure Content Delivery in Information-centric Networks: Design, Implementation, and Analyses, *ACM SIGCOMM Workshop on Information-centric Networking*, ACM, pp. 73–78 (2013).
[13] Ion, M., Zhang, J. and Schooler, E. M.: Toward Content-Centric Privacy in ICN: Attribute-based Encryption and Routing, Vol. 43, pp. 513–514 (2013).
[14] Ghali, C., Schlosberg, M. A., Tsudik, G. and Wood, C. A.: Interest-Based Access Control for Content Centric Networks, *ACM Conference on Information-Centric Networking*, ACM ICN, pp. 147–156 (2015).
[15] Yu, Y., Afanasyev, A. and Zhang, L.: Name-Based Access Control, Technical report, NDN-0034 (2015).
[16] Apple Inc.: File System Programming Guide, Apple Developer Guides (2016).
[17] : Security, Android Open Source Project (online), available from ⟨`https://source.android.com/security/index.html`⟩ (accessed 2018-12-28).
[18] Burnett, J.: Geographically Restricted Streaming Content and Evasion of Geolocation: The Applicability of the Copyright Anticircumvention Rules, *Michigan Telecommunications and Technology Law Review*, Vol. 19, No. 2, p. 423 (2013).
[19] Zandbergen, P. A.: Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi and Cellular Positioning, *Transactions in GIS*, Vol. 13, No. s1, pp. 5–25 (2009).
[20] : IP Geolocation and Online Fraud Prevention, MaxMind (online), available from ⟨`https://www.maxmind.com/`⟩ (accessed 2018-12-28).
[21] Muir, J. A. and Oorschot, P. C. V.: Internet Geolocation: Evasion and Counterevasion, *ACM Computing Surveys*, Vol. 42, No. 1, pp. 4:1–4:23 (2009).
[22] Trimble, M.: The Future of Cybertravel: Legal Implications of the Evasion of Geolocation, *Fordham Intellectual Property, Media and Entertainment Law Journal*, Vol. 22, No. 3, p. 567 (2012).
[23] Suksomboon, K., Tagami, A., Basu, A. and Kurihara, J.: IPRES: In-device Proxy Re-encryption Service for Secure ICN, *ACM Conference on Information-Centric Networking*, ICN, pp. 176–177 (2017).
[24] Suksomboon, K., Tagami, A., Basu, A. and Kurihara, J.: In-Device Proxy Re-encryption Service for Information-Centric Networking Access Control, *IEEE Conference on Local Computer Networks*, LCN, pp. 1–4 (2018).
[25] Syalim, A., Nishide, T. and Sakurai, K.: Realizing proxy re-encryption in the symmetric world, *International Conference on Informatics Engineering and Information Science*, Springer, pp. 259–274 (2011).
[26] Fotiou, N. and Polyzos, G. C.: Securing content sharing over ICN, *ACM Conference on Information-Centric Networking*, ICN, pp. 176–185 (2016).
[27] Feather, C.: Network News Transfer Protocol (NNTP), RFC 3977, RFC Editor (2006).
[28] Kalt, C.: Internet Relay Chat: Channel Management, RFC 2811, RFC Editor (2000).
[29] Lehman, V., Hoque, A., Yu, Y., Wang, L., Zhang, B. and Zhang, L.: A Secure Link State Routing Protocol for NDN, Technical Report NDN-0037, NDN Technical Report (2016).
[30] Kim, S., Duan, Z. and Sanchez, F.: Scalable Name-based Inter-domain Routing for Information-centric networks, *IEEE International Performance Computing and Communications Conference*, IPCCC, pp. 1–8 (2015).
[31] : NLSR – Named Data Link State Routing Protocol, NDN Project (online), available from ⟨`http://named-data.net/doc/NLSR/current/`⟩ (accessed 2018-12-28).
[32] Zhu, Z. and Afanasyev, A.: Let's chronosync: Decentralized Dataset State Synchronization in Named Data Networking, *IEEE International Conference on Network Protocols*, ICNP, pp. 1–10 (2013).
[33] Verison, Inc.: The Domain Name Industry Brief, Technical Report Vol. 15, Issue 4 (2018).
[34] : CIDR Report, APNIC (online), available from ⟨`https://www.cidr-report.org/`⟩ (accessed 2018-12-28).
[35] Ascigil, O., Rene, S., Psaras, I. and Pavlou, G.: On-Demand Routing for Scalable Name-Based Forwarding, *ACM Conference on Information-Centric Networking*, ICN, pp. 1–10 (2018).
[36] Farinacci, D., Fuller, V., Meyer, D. and Lewis, D.: The Locator/ID Separation Protocol (LISP), RFC 6830, RFC Editor (2013).
[37] Afanasyev, A., Yi, C., Wang, L., Zhang, B. and Zhang, L.: SNAMP: Secure namespace mapping to scale NDN forwarding, *IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 281–286 (2015).