解説

多様なビジネスの収容基盤としてのネットワークとその課題
――著作権保護や消費税徴収等に関わる技術的・法的課題――

Network Operations as an Infrastructure for Diverse Businesses

浅見　徹　栗原　淳　近藤大嗣　戸出英樹

Abstract

日本国憲法制定時に，「信書」を明確に定義して信書の秘密を規定した郵便事業に対し，電気通信事業は曖昧にしたまま運用され，著作権法と通信の秘密の相克のような様々な社会問題が生じている．このことは，更に将来の新たな課題を生む可能性もはらんでいる．例えば現在隆盛している仮想通貨の取引において，消費税の観点でトランザクションの位置を国税当局が把握する必要があると考えられ，更に大きな社会課題となる可能性がある．本稿では，多様なビジネスを収容するためにネットワークの技術基盤とそれに対応した法制度を整備する必要性を解説し，有望なソリューションとして，5G モバイル網で標準化されたエンドツーエンドのスライス技術の導入によるネットワーク運用法を提案する．

キーワード：通信の秘密，表現の自由，物流，消費税徴収，スライス，サイバーフィジカル空間

1. は　じ　め　に

電気通信は今日まで大きく発展を遂げてきた．電信，電話，テレックスが専用の通信インフラ上でアプリケーション（アプリ）を提供していた段階から，これらを単一の通信インフラ上で提供する統合網構想が 20 世紀後半に提唱され，最終的に ARPANET プロトコルから進化したインターネットプロトコルスイート（TCP/IP）が Web というキラーアプリを持って覇権を握り，インターネットに発展した．以来，Everything over IP が標榜され，ネットワークはパケット転送のみを受け持ち，セキュリティやアクセス制御はアプリに任せる形で発展してきた．しかし，1980 年代の研究者ネットワークと比べ，ビジネスもユーザも様変わりし種々の問題が顕在化している現在，ビジネスやユーザの利用形態に合わせた抜本的な再構築，すなわちネットワークの破壊的イノベーションが喫緊の課題ではないだろうか．

本稿では，2. で，通信，放送と公衆送信権，並びに通信の秘密について，法制度の枠組みを示す．3. では，インターネットにおける著作権保護と，E コマースにおける消費税徴収の困難さを示す．4. では，スライス(用語)技術の導入により通信と商業活動を分離し，技術的・法制度的に新たに設計した物流スライスを作れば，3. の著作権保護での懸念がかなり緩和されたコンテンツブロッキングをディジタルコンテンツ配送サービス向けに実現できることを Information Centric Networking（ICN）[1] を簡略化したモデルで示す．5. はまとめである．

2. 情報共有メディアと法制度

放送は技術的には電気通信から派生しているが，1 対 1 を基本とする電気通信に対し 1 対多（公衆）の情報送信という形態から，本質的に異なったサービスとして運用されてきた．国際電気通信連合憲章は，電話の発明以後 1920 年頃まで有線の音声放送[2] や，株価情報配信（ディジタル放送）[3] があったにもかかわらず，放送業務を無線を前提に定義している[4]．このため，日本の放送法では，第四条二項に“「放送」とは，公衆によつて直接受信されることを目的とする電気通信の送信をいう”

浅見　徹　正員：フェロー　(株)国際電気通信基礎技術研究所
E-mail asami@atr.jp
栗原　淳　正員　(株)国際電気通信基礎技術研究所適応コミュニケーション研究所
E-mail kurihara@ieee.org
近藤大嗣　正員　大阪府立大学大学院工学研究科知能情報工学分野
E-mail daishi.kondo@cs.osakafu-u.ac.jp
戸出英樹　正員：シニア会員　大阪府立大学大学院工学研究科知能情報工学分野
E-mail tode@cs.osakafu-u.ac.jp
Tohru ASAMI, Fellow (Advanced Telecommunications Research Institute International, Kyoto-fu, 619-0288 Japan), Jun KURIHARA, Member (Adaptive Communications Research Laboratories, Advanced Telecommunications Research Institute International, Kyoto-fu, 619-0288 Japan), Daishi KONDO, Member, and Hideki TODE, Senior Member (Graduate School of Engineering, Osaka Prefecture University, Sakai-shi, 599-8531 Japan).
電子情報通信学会誌　Vol.103 No.2 pp.155-161 2020 年 2 月

表1　郵便事業における信書の例[9]

信書	信書でないもの
書状	書籍の類
請求書の類	カタログ
会議招集通知の類	小切手の類（手形，株券等）
許可書の類	プリペイドカードの類，乗車券の類，クレジットカードの類，会員カードの類
ダイレクトメール（文書自体に受取人が記載，特定の受取人に差し出す趣旨が明らか）	ダイレクトメール（もっぱら街頭における配布や新聞折り込みを前提）
証明書の類（印鑑証明書，納税証明書，戸籍謄本，住民票の写し，健康保険証，登記簿謄本，車検証，履歴書，給与支払明細書，産業廃棄物管理票，保険証券，振込証明書，輸出証明書，健康診断結果通知書・消防設備点検表・調査報告書・検査成績票・商品の品質証明書その他の点検・調査・検査などの結果を通知する文書）	説明書の類（市販の食品・医薬品・家庭用または事業用の機器・ソフトウェアなどの取扱説明書・解説書・仕様書，定款，約款，目論見書），求人票，配送伝票，名刺，パスポート，振込用紙，出勤簿，ナンバープレート

と広義に定義し矛盾の回避に努めた形跡がある[5]．一方，著作権法では第二条で（無線）放送と有線放送に分け，自動公衆送信を追加した上で，公衆送信権，「公衆によつて直接受信されることを目的として行う無線通信又は有線電気通信の送信」の権利，を著作権者に認めている[6]．Web サーバを介した著作物の配布は自動公衆送信に該当し，Request に対し該当コンテンツを送信する Web サーバの動作を考慮し，更に著作権法第九十二条二項で送信可能化権を著作権者に認めている．ここで，放送法，著作権法共に電気通信を前提に規定されているが，条文中には通信の秘密に関する条項はない．このため，通信の秘密の束縛から解放されたように条文が解釈される可能性がある．

日本国憲法は第二十一条二項[7]で通信の秘密の保護を定めている．これを受けて郵便法第七条と第八条[8]，電気通信事業法第三条と第四条で，それぞれ検閲の禁止と秘密の確保がほぼ同文で規定されている．歴史的に古い郵便事業では，電気通信事業よりも体系立った運用がされてきたため，以下では郵便法をベースに議論する．第八条には，日本郵便株式会社の「取扱中に係る」信書の秘密の保護と，郵便物に関して知り得た他人の秘密の保護が規定されている．保護の対象には，通信の内容だけでなく，封筒に記載された差出人や受取人の住所や氏名，送受信時刻等の構成要素を含む信書に関する一切の事項が含まれる．この構成要素部分は，第八条二項に知り得た他人の秘密として別に言及されている．ここで，信書とは郵便法第四条二項[8]によれば，「特定の受取人に対し，差出人の意思を表示し，又は事実を通知する文書」であり，表現の自由を守るための通信の秘密のコア概念として運用されて今日に至っている．残念ながら，電気通信事業法にはこのような通信モデルに対する言及も，守るべき通信内容に関する言及もない．

信書の秘密とプライバシー保護は異なる．表1は日本郵便株式会社の定める信書の例である[9]．売り込みなどで使われるダイレクトメールでも，文書自体に受取人が記載され特定の受取人に差し出す趣旨が明らかであれば信書となるが，パスポートやクレジットカードのような個人情報としては最上位に位置付けるべきものでも信書としては取り扱わず，信書の内容を DVD にして送ると信書とならない．また，通販で，小切手を郵便で送って書籍等を購入する手続きは，郵便法では信書の送受とはみなされず，罰則の軽い第八条二項の「知りえた他人の秘密」で拘束される．以下では，郵便法における信書のモデルを「通信」とし，一般の通信と区別して議論する．

3. インターネットプロトコルで解けない課題

通信の難題は，著作権保護や消費税の徴収を「通信」の秘密と合法的に両立させることが難しいことである．

3.1 著作権保護と「通信」の秘密の両立

2018 年内閣府のインターネット上の海賊版対策に関する検討会議において海賊版サイトへのアクセスをブロッキングすべきか否かについて長い議論があった．しかし，結局結論を出せずに終わっている[10]．主に，DNS（Domain Name System）ブロッキングと IP ブロッキングが議論されたが，本稿では IP ブロッキングを特に取り上げて表2に要約する．

比較的効果があるとされている IP ブロッキングでも，大部分の Web アプリが昨今 HTTP から HTTPS（Hy-

用　語　解　説

スライス　用途に応じたサービスを提供するために，ネットワークを仮想化した上で，分割されたネットワークリソースをスライスと呼ぶ．

ライドシェア　他人同士が一台の乗り物を「相乗り」することを指し，サービスに登録したドライバが自家用車を使って同乗希望者を運ぶビジネスとして展開している．

表2　ブロッキングと違法性への懸念[10),11)]

Article 19 の指摘	概要
(1) Over-blocking or false positives	Web サーバの実装によっては，違法 Web サイトと正当なサイトの IP アドレスが同一の可能性があるため，正当サイトもブロッキングされてしまう．
(2) Under-blocking or false negatives	違法 Web サイトの IP アドレスは可変にもできるため，違法 Web サイトを 100% ブロッキングできるわけではない．
(3) Failure to address the root causes	ブロッキング／フィルタリングは問題の根本的な解決にはならず，インターネット上の重大犯罪への法執行や訴追に代わるものではない．
(4) Possibility of circumvention	ブロッキング／フィルタリングは，ブロッキングリストに追加されたことが分かれば，技術のあるユーザならば簡単に回避できる．
(5) Failure to consider the changing nature of websites	Web ページではなく，Web サイトのブロックは，Web サイトのコンテンツが時間とともに大きく変化する可能性があることを無視している．
(6) Violation of human rights	ブロッキング／フィルタリングのためにユーザ間の通信内容を詳細に分析すると，プライバシーと表現の自由という権利を深刻に侵害してしまう．
(7) Interference with the Internet infrastructure	ブロッキング／フィルタリングは，インターネットのインフラや設計における重要な構成要素を阻害し，インターネットの中継速度を下げ，ネットワーク機器への投資増を招いてしまう．
内閣府検討会議の指摘	**概要**
(i) 受信者一般の接続先を網羅的・一般的に検知	海賊版サイトの閲覧とは関わらない受信者一般の接続先を網羅的・一般的に検知すること．
(ii) 知る権利一般に対する重大な制約	ブロッキングの仕組み自体がインターネット上の知る権利一般に対する重大な制約たり得ること．
(iii)「通信」の秘密に関する懸念	「通信」の秘密に関する多くの懸念があること．

表3　インターネットの海賊版サイトの技術基盤[10)]

サービス種別	サービス
Naming Service	自らが購入したドメインの使用権を海賊版サイト等に売りつける「完全な匿名性」をうたったドメイン登録サービスが出現．
Hosting Service	データ関連の法律の執行が不十分な国にサーバを設置し，著作権者等からの削除依頼に応じないことを売りにする「オフショアホスティング」，「防弾ホスティング」が出現．
Transfer Service	分散形サーバシステムを採用し，侵害コンテンツの公衆送信の差止請求を出したいサーバの特定が難しい CDN 事業者の出現．

pertext Transfer Protocol Secure）に移行したため，中継ルータが使うことのできる情報は少なく，5 タプル（発信元アドレス，着信先アドレス，発信元ポート，着信先ポート，プロトコル番号）しかない．このため，ブロッキングの粒度はページごとではなくサイト（サーバ）単位となり，この検討会議では，表 2 の（i）～（iii）の観点でブロッキング慎重論が出た．同様な議論は世界各国にあり，例えばイギリスの人権団体 Article 19 は，IP ブロッキングの法制化に関し，表 2 の（1）～（7）の違法性の懸念を表明している[11)]．

ここで，インターネットの海賊版サイトで運営管理者の特定や侵害コンテンツの削除要請が困難であるのは，表 3 に示すサービスに依拠する[10)]．

3.2　消費税徴収と「通信」の秘密の両立

さて，我が国の 2018 年度一般会計歳入総額 97.7 兆円のうち，消費税収入は 17.6 兆円であり，全体の 18.0% を占める[12)]．ただし，同年度の名目 Gross Domestic Product（GDP）が 548.9 兆円[13)]だったことからかなりの徴収漏れがあると考えられ，今後のディジタル化の進展に伴い徴収漏れが更に増える可能性もある．例えば，昨今話題のライドシェア(用語)は節税手段ともみなすことができる．2015 年の全国のタクシー事業の営業収入は約 1.7 兆円[14)]であり，おおむね 1,360 億円の消費税が徴収されたと考えられる．ライドシェアはドライバと乗客と仲介者から構成され，ドライバは乗客の支払いの一部を仲介者に取次料として支払う．ドライバを仲介業者が社会保険料等も負担しなければならないパートタイム労働者（w2 worker）とみなすか契約請負業者（contractor 1099）とみなすかで争われた米国の裁判[15)]は，消費税制の面からも再考されるべきである．契約請負業者とみなせば，ドライバと乗客との間の取引になり，年間売上げが 1,000 万円未満のドライバには消費税代納の義務はない[16)]．このため，ほとんどのドライバは消費税を代納する必要はない．サービスや商品の売り手と消費者を結び付ける仲介サービスの興隆を考えると，小規模事業者への安易な優遇税制は見直される必要がある．

売り手のモラルに頼る消費税徴収は既に破綻してい

表 4　サービス別プライバシー公開の程度

	送受信者 ID	メッセージ本体
「通信」	送受信者以外には非公開	送受信者以外には非公開
放送	放送局は公開．受信者 ID は放送局以外には非公開	放送局と多数の契約受信者間でコンテンツを共有．それ以外は非公開．
E コマース	サーバは公開．クライアントはサーバ以外には非公開．	サーバとクライアント間以外には原則非公開．ただし，トランザクションの存在と購入者の位置，購入物，購入価格は政府に公開
広告型	サーバは公開．クライアントはサーバと複数の契約事業者以外には非公開．	サーバ，クライアント，複数の契約事業者間でクライアント ID（クッキー等）とアクセスページを共有．それ以外には非公開．

る．例えば，国外のインターネット通販業者からの電子書籍・音楽・広告の配信は，「電気通信利用役務の提供」と呼ばれ，その役務の提供が国内の事業者・消費者に対して行われる場合は，国内取引として消費税が課される[17]．これは経済協力開発機構（OECD）の内外判定基準[18]によって運用されるが，そのためには，海外のインターネット通販業者は「登録国外事業者」にならなければならない．この制度は，導入から 4 年後の 2019 年 4 月 1 日現在でも登録国外事業者が 91 社[19]しかなく，韓国や中国からの登録がないことから，機能しているとは言い難い．コスト増（内税を国税庁に支払うには日本向け消費税計算プログラムを実装する必要がある）と収入減（消費税分減収）が見込まれ，海外のインターネット通販業者にインセンティブはない．国外事業者に対する日本国内法の法的拘束力が小さいことを考えると，消費税収入を確保し事業者間の公平な競争を実現するには，売り手の代納に依存しない消費税徴収方法を発明する必要がある．

そのためには，日本国内にいる消費者を起点にした消費税徴収方法を設計しなければならないが，売り手と買い手が HTTPS あるいは Transport Layer Security（TLS）上のプロトコルで交渉する現状では，売買の特定が困難なため，モラルの高い消費者以外の納税は期待できない．売り手が国税に協力的な場合ですら，消費者は Virtual Private Network（VPN）などソース IP アドレスを偽装するサービスによって消費税徴収のない国若しくは州に位置を詐称して消費税を回避できるからである．

インターネットには，物流的側面のある E コマースのほかに，「通信」，放送，あるいは Google の検索サービスや facebook に代表される広告型のサービスが存在し，表 4 に示すような異なったレベルのプライバシー基準で運用されている．物流ビジネスで消費税を徴収するには〈消費者の位置，購入価格，購入日時，（商品名）〉を国税庁が把握できなければならない．また，国境を越えた個人情報の流通に関して，EU 一般データ保護規則（GDPR；General Data Protection Regulation）にのっとった国家の保証も求められている．このように，国境を考慮したサービス運用を迫られることは，これからますます多くなる可能性があり，その種の保証や監視をするには，現在のネットワークアーキテクチャでは「通信」の秘密に抵触する可能性が高い．

4. スライスによる「通信」と流通の分離

電気通信網に関して，当初の対象とした「通信」以外に種々のサービスが追加され統合網となった結果，関連する様々な国内法の間で相互矛盾が生じていることを 3. で指摘した．「通信」の秘密では，「取扱いに関わる通信の秘密」の規定が重く，「知得，窃用，漏えい」の行為が全て禁止されている．これらの課題を抜本的に解決するには，「通信」を他のサービスから切り離し，更に法規制の異なるサービスごとに専用網を構築することが第一歩であろう．5G モバイル網では，端末までスライスを延ばせるようになったため，サービス別に仮想網を安価に構築することができ，関連法にのっとった専用のプロトコルを開発して運用することも夢ではない．図 1 にその概念図を示す．

完備な消費税徴収プロトコルの設計は今後に委ねるとして，以下では，E コマース・サービスのサブセットでもあるディジタルコンテンツ配送サービスに専用のスライスを割り当てれば，購入者のプライバシーを守りつつ違法コンテンツへのアクセスをブロッキングする専用のプロトコルを設計できる可能性があることを示す．そのため，既提案のプロトコルの中から，ICN を取り上げ，3. の懸念をどこまで払拭できるかを示す．

Named Data Networking（NDN）[20]を極端に単純化した図 2 のパケット構造を用いて，情報共有プロトコルとしての ICN と HTTP/HTTPS とを比較評価する．ICN では，コンテンツ入手者から出すコンテンツ要求にはコンテンツの名前のみ，それに対するコンテンツ所有者若しくはキャッシュからの応答（データパケット）にはコンテンツの名前，コンテンツのデータとコンテンツ所有者の署名があるだけとする．ICN ルータの動作

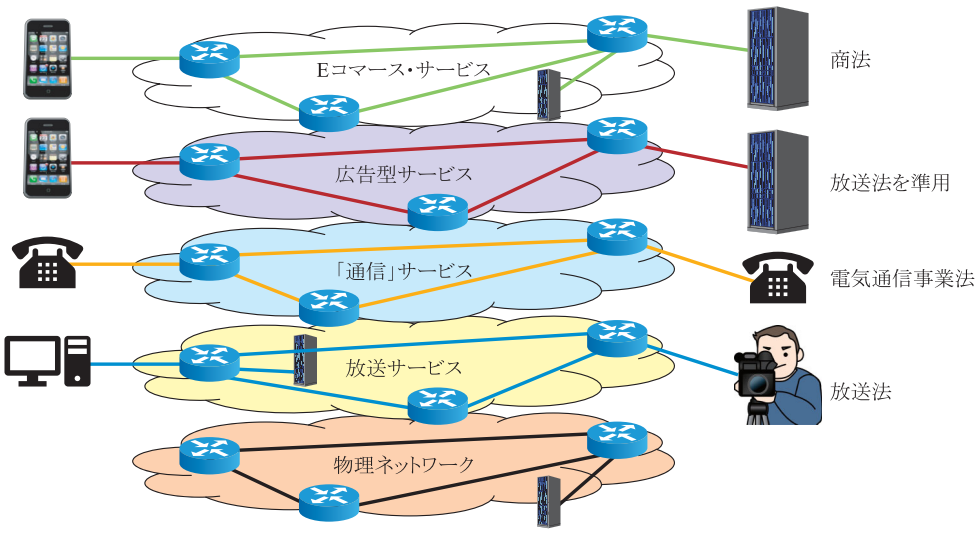

図1　法規制に応じたスライス設定によるサービスの独立運用法

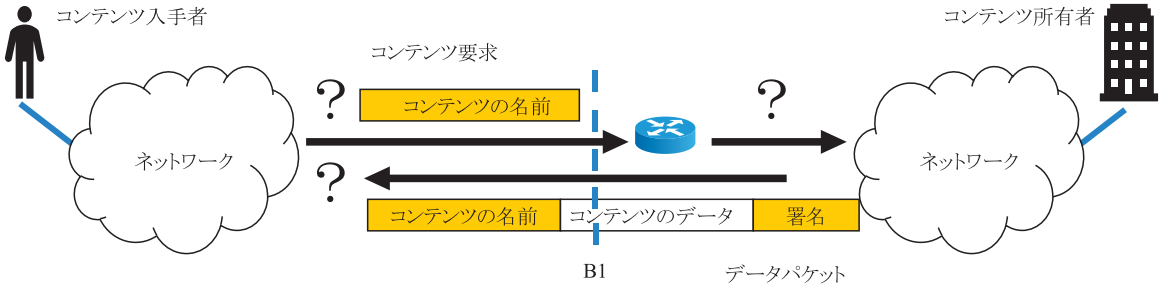

図2　任意のコアルータを通過する単純化したICNパケット[(1)]　B1を通過するパケットの送信者若しくは受信者が不明であるとき，それぞれ「？」で示している．

も単純化し，コンテンツ要求が図2に示すICNルータに入力されたとき，コンテンツの名前の示すコンテンツがキャッシュにあれば，それをデータパケットとして当該入力ポートに返し，なければ当該入力ポート番号とコンテンツの名前をコンテンツ要求済みテーブルに記憶し経路表の示す出力ポートにコンテンツ要求を送り出すものとする[(1)]．また，送信経路を逆にたどって到来した対応するデータパケットが当該出力ポートから受信したら，それをキャッシュに書き込むとともに，コンテンツ要求済みテーブルに記憶されていた入力ポートに送り出すものとする．以下では，コンテンツとコンテンツの名前の1対1の対応を特徴の1と呼ぶ．

コンテンツ要求には宛先（コンテンツ所有者／キャッシュ），送信元（コンテンツ入手者），ペイロードがない．このため，コンテンツアクセスのブロッキングを実施する場合，コンテンツ要求を図2に示す任意のコアルータの入力端B1でブロックするのが送信者のプライバシー情報の利用が少なく有望である．更に，ネットワーク内で公知のコンテンツの名前が受信者（コンテンツ所有者）を明示しないように運用していれば，受信者のプライバシーも参照しないブロッキングを実現できる．これを特徴の2と呼ぶ．

ICNでは，特徴の1により表2の懸念の（1），（2），（5）を解決でき，かつコンテンツ入手者の知る権利やコンテンツ所有者の表現の自由への侵害も違法コンテンツ[(注1)]のみに限定できる．また，コンテンツへのアクセス制御時のプライバシーに関しては，特徴の2から懸念の（6）が解決できる．（7）に関しては，コンテンツの名前によるパケット転送はICNのデフォルトの機能であり，新たな処理機能を追加せずに実装可能である．ただし，ブロッキングリストが大きいと，経路表のメモリサイズや処理オーバヘッドが過大になるおそれはある．（4）の解決は難しい．違法コンテンツがブロッキングされていると分かれば，違法コンテンツ所有者は別のコンテンツの名前を広報してフィルタリングを回避できるか

（注1）　ブラックリストで明示した違法コンテンツだけがアクセスできない．

らである．しかし，インターネットの大多数のカジュアルユーザにはブロッキングリストは有効である．(3) は根本的には裁判等で解決すべきものであり，ICN でも解決できない．ブロッキングは，あくまで，犯罪者を捕まえるまでの対症療法と考えるべきものだろう．

日本の内閣府でのインターネット上の海賊版対策に関する検討会議における懸念事項 (i)〜(iii) に関しては以下のように考えられる．(i) に関しては，特徴の 2 から該当しない．また，コンテンツが大きく，分割ダウンロードされる場合，分割されたコンテンツ（チャンク）のキャッシュが下流すなわちコンテンツ入手者側のルータにできて残存している可能性があり，全てのコンテンツ要求を B1 で観測できるわけでもない．B1 ではコンテンツのダウンロードの一部に対応するコンテンツ要求を観測できるだけである．したがって，「網羅性」は違法コンテンツそのものに対してさえ成立しない．ブロッキングの実現には，当該コンテンツの違法性を主張する国の全 ICN コアルータに同じブロッキング手法を実装する必要がある．

(ii) の知る権利一般の侵害についてはそのとおりである．ただし，違法コンテンツに限定されているため，公共の福祉の観点から，このような違法コンテンツに対しては，表現の自由が制約されてもよいと判断される可能性が高い．

(iii) に関しても以下の観点から大きな問題とは言えないのではなかろうか．第 1 に，データパケットと同様，コンテンツ要求は基本的に特徴の 1 を持つネットワークへの公衆送信に近く，「通信」の秘密で問題となる信書の秘密には抵触していないとも考えられる．この部分は，電気通信事業法の規定と運用に曖昧なところがあるため，郵便法レベルに引き上げることにより解決することを目指すべきであろう．

表 5 に ICN と HTTP/HTTPS（実際は IP ブロッキング）のブロッキングに関し，その違法性の懸念の程度を示した．ここで，◎，○，△，×で，「無条件で解決可能」，「解決可能」，「条件付きで解決可能」，「解決不可能」を示した．

表 5　ブロッキングと違法性への懸念

指摘課題	ICN	HTTP/HTTPS
(1) Over-blocking	◎	×
(2) Under-blocking	○*	×
(3) Failure to address the root causes	×	×
(4) Possibility of circumvention	×	×
(5) Failure to consider the changing nature of websites	◎	×
(6) Violation of human rights	○**	×
(7) Interference with the Internet infrastructure	△	×
(i) 受信者一般の接続先を網羅的・一般的に検知	○	×
(ii) 知る権利一般に対する重大な制約	○**	×
(iii) 通信の秘密に関する懸念	△***	×

* ブラックリスト次第，** 違法コンテンツアクセスのみ表現の自由と知る権利を阻害，*** 通信の定義次第

5. ま　と　め

2018 年は，いわゆる違法漫画サイトの問題から，著作権法と通信の秘密の相克が大きな問題となった．また，国家の歳入の要となる消費税徴収に関しても，重大なリスクがある．本稿では，スライス技術により狭義の「通信」と物流等他のサービスを分離し，その上で，各サービスに合った適切なプロトコルと法制度を開発して運用することによる令和の時代のネットワークのあり方を提案した．トラヒックのモニタリングが可能なスライスの運用が許されれば，プライバシー露出を最小に抑えた的確な消費税徴収プロトコルを設計する道も開ける．コンテンツのブロッキングに関しては HTTP/HTTPS プロトコルの場合，違憲性が高いと懸念されているが，ICN のコンテンツの名前ベースのブロッキングでは大幅に払拭され，多くの人の許容レベル範囲内になる可能性を示し，そのようなサービスに即したプロトコル開発の可能性，またそれを許すスライスの運用法を提案した．筆者らは法律に関しては素人であるため，その解釈に関しては，誤びゅうや極論がある可能性はある．個人情報保護，表現の自由に加えて知的財産権や徴税方法をハーモナイズした新たなネットワークアーキテクチャを創造するには，どのような技術と法運用が必要になるのか，本稿が議論の端緒になれば幸いである．

文　献

(1) B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," IEEE Commun. Mag., vol. 50, no. 7, pp. 26-36, July 2012.

(2) J. Wright, "The electrophone," The electrical engineer, p. 344, Sept. 1897.

(3) S.S. Pratt, The work of Wall Street, D. Appleton and Company, New York, 1903, https://babel.hathitrust.org/cgi/pt? id=uc2.ark:/13960/t3513xw8b;view=1up;seq=5（2018 年 10 月 4 日参照）

(4) 国際電気通信連合憲章，http://www.soumu.go.jp/main_content/000171443.pdf（2019 年 4 月 28 日参照）

(5) 放送法，http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail? lawId=325AC0000000132（2019 年 4 月 28 日参照）

(6) 文化審議会著作権分科会，"IP マルチキャスト放送の著作権法上の取扱い等について，" http://www.mext.go.jp/b_menu/shingi/bunka/toushin/06083002/004.htm（2019 年 4 月 28 日参照）

(7) 日本国憲法，http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail?lawId=321CONSTITUTION&openerCode=1（2019 年 4 月 28 日参照）

(8) 郵便法，http://elaws.e-gov.go.jp/search/elawsSearch/elaws_search/lsg0500/detail? lawId=322AC0000000165（2019 年 4 月 28 日参照）

（9） https://www.post.japanpost.jp/question/57.html（2019年4月28日参照）
(10) インターネット上の海賊版対策に関する検討会議，“「インターネット上の海賊版対策に関する検討会議」中間まとめ(案)～インターネット上の海賊版サイトに対する総合対策～，” https://www.kantei.go.jp/jp/singi/titeki2/tyousakai/kensho_hyoka_kikaku/2018/kaizoku/dai7/siryou5.pdf（2018年10月4日参照）
(11) Article19, “Freedom of expression unfiltered : How blocking and filtering affect free speech,” https://www.article19.org/resources/freedom-of-expression-unfiltered-how-blocking-and-filtering-affect-free-speech/（2019年4月28日参照）
(12) https://www.mof.go.jp/budget/fiscal_condition/related_data/201811_00.pdf（2019年4月28日参照）
(13) https://www.esri.cao.go.jp/jp/sna/menu.html（2019年4月28日参照）
(14) http://www.taxi-japan.or.jp/pdf/toukei_chousa/eigyousyuunyuu_suii.pdf（2019年4月28日参照）
(15) https://www.spengleraganslaw.com/blog/ubercase/（2019年4月28日参照）
(16) http://www.nta.go.jp/taxes/shiraberu/taxanswer/shohi/6501.htm（2019年4月28日参照）
(17) https://www.nta.go.jp/publication/pamph/shohi/cross/01.htm（2019年4月28日参照）
(18) https://www.oecd.org/ctp/international-vat-gst-guidelines-9789264271401-en.htm（2019年4月28日参照）
(19) https://www.nta.go.jp/publication/pamph/shohi/cross/touroku.pdf（2019年4月28日参照）
(20) L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, “Named data networking,” ACM SIGCOMM CCR, vol. 44, no. 3, pp. 66-73, July 2014.

（2019年8月9日受付　2019年9月4日最終受付）

浅見　徹（正員：フェロー）
昭49京大・工・電子卒．昭51同大学院修士課程了．同年国際電信電話（現KDDI）入社．以来，UNIX通信，ネットワーク障害診断等の研究に従事．平13(株)KDDI研究所代表取締役所長．平18東大大学院情報理工学系研究科教授．平27から(株)ATR代表取締役社長．博士（情報理工学）．平9年度前島賞，平30年度志田林三郎賞各受賞．

栗原　淳（正員）
平16東工大・工・情報卒．平18同大学院修士課程了，同年KDDI株式会社入社．平24東工大大学院博士課程了．現在，(株)ゼタント主任研究員，及び(株)ATR連携研究員．符号理論，情報セキュリティ，システム・ネットワークアーキテクチャの研究等に従事．博士（工学）．

近藤　大嗣（正員）
平25阪大・工・電情卒．平27東大大学院学際情報学府修士課程了．平30ロレーヌ大大学院（LORIA（CNRS UMR 7503), Inria Nancy-Grand Est）博士課程了．Ph.D.（computer science）．平31から阪府大大学院工学研究科助教授．

戸出　英樹（正員：シニア会員）
昭63阪大・工・通信卒．平2同大学院修士課程了．平3同大学院博士課程退学後，阪大・工・通信・助手．平10同情報システム・講師．平11同助教授．平14同大学院情報科学研究科情報ネットワーク学専攻助教授．平19同准教授．平20阪府大大学院工学研究科電気・情報系専攻知能情報工学分野教授．現在に至る．将来のインターネットや全光／無線ネットワークを対象としたトラヒック制御や網設計技術，並びに，コンテンツ検索・取得・配信技術に関する研究に従事．IEEE会員，博士（工学）．