プロバイダの捜査対応，ログ保存，被害抑止協力の実務と考え方

Practice and Legal Basis of Internet Service Providers; Cybercrime Investigation, Data Retention and Prevention

丸　橋　　透*

はじめに

筆者の所属するニフティ株式会社（以下「ニフティ」という）は，1987年にパソコン通信サービス NIFTY-Serve を開始して以来，様々なネットワーク関連サービスを展開してきた。ダイヤルアップ接続によるナローバンドサービスの時代を経て，現在ではブロードバンド常時接続他の @nifty ブランドラインアップの総合インターネットサービスプロバイダであり，クラウド事業者である。以下，主要サービスと捜査対応上の特徴を記す。

- 常時接続（固定系 FTTH, ADSL, 無線系 Wi-MAX, MVNO 等）サービスは，インターネットに常時接続する加入者140万人（回線）[1)]を抱えており，必然的に，大都市並みの犯罪捜査対応数がある。
- 電子メールサービス

常時接続加入者は電子メールアカウントを利用できるが，ダイヤルアップ接続時代からの加入者等，他社の常時接続回線を利用していても電子メールアドレスのみ @nifty を利用する加入者もいる。接続契約時には本人

＊　ニフティ株式会社法務部長

1)　ニフティ株式会社平成28年３月期第２四半期報告書。

の住所が確認されている。

- WEB ホスティング，ブログ等の WEB サービス

加入者向けの WEB ホスティングサービス，ブログ等の WEB サービスだけではなく，広告モデルの無料ブログサービスもあり，後者は，本人確認をしていないため，連絡先が不正確な場合が多い。EC やオークションサービスは提供していない。

- クラウドサービス（IaaS, PaaS, SaaS）

企業向けサービスでは，旧来のホスティングサービスに加え，インターネットにオープンなパブリッククラウドサービスを中核にして IaaS（Infrastructure as a Service），PaaS（Platform as a Service），SaaS（Software as a Service）を提供している。パブリッククラウドでは，通常，顧客企業が顔を見せてソーシャルゲーム等の WEB サービスを提供することが多いからか，ニフティ経由の捜査はほとんど無い。

以下，パソコン通信サービス時代から培ってきたニフティの捜査対応，ログ保存，児童ポルノ等の犯罪被害抑止のための協力の実務と考え方を紹介する。

1．ニフティの捜査対応実務の概要

1-1　2014年度の捜査対応実績

ニフティに対する警察・検察からの契約者情報等の差押え[2]や照会[3]の総数は297件で，内訳は，差押139件に対し任意捜査158件であった。その他税関，証券取引等監視委員会からの差押えが11件あった。例年，ほぼ同じボリュームの対応をしている。接続サービスの加入者情報，メールサービスの利用者情報や接続ログ，ウェブホスティングサービスやブログの開設者情報等が差押えや照会の典型的対象である。

2）　差押許可状及び記録命令付差押許可状（刑事訴訟法218条）によるもの。
3）　捜査関係事項照会（刑事訴訟法197条２項）等。

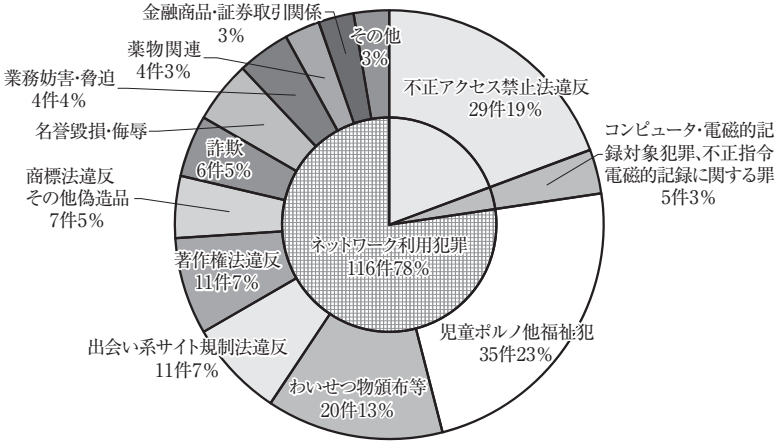
1-2　強制捜査の罪名別割合

2014年度のニフティでの強制捜査（すべて差押え又は記録命令付差押え）[4]対応では，不正アクセスとコンピュータ・データ対象犯罪の合計で２割強，ネットワーク利用犯罪が８割弱であり，例年の傾向と変わらない。ネットワーク利用犯罪の中では，児童ポルノ等違法コンテンツ，福祉犯関係が５割弱と多く，著作権，商標権侵害事案が１割強ある（図表1）。

会員属性による特色もあるだろうが，ニフティが把握するのはあくまで証拠収集段階の罪名であるため，警察庁が半年毎に発表するサイバー犯罪の検挙件数[5]の割合とは異なる傾向となっている。

業務妨害や脅迫事案には，公共施設の爆破予告等がある。これらの事案は，照会時に緊急性が認められれば任意に加入者情報を開示することがで

図表１　ニフティ株式会社の2014年度強制捜査対応実績



4）　捜査関係事項照会（刑事訴訟法197条２項）では罪名や被疑事実は窺い知れないが，強制捜査の令状には罪名が必須記載事項（同法219条１項）である。

5）　３ヶ月の統計期間のずれはあるものの，『平成26年中のサイバー空間をめぐる脅威の情勢について（警察庁平成27年３月12日）』図６－３サイバー犯罪の罪名別割合を比較参照。

きる類型である。爆破予告の書き込みであっても日時や場所等，具体性に乏しく緊急性が無いと判断したため任意開示しなかった加入者情報が後に差押えられることがままある。

IP 電話や電子メールの通信傍受，その他検証はこれまで実績が無い。

1-3　照会と差押えの切り分け

捜査機関から事前問合せがあるか，捜査関係事項照会書が，郵送又は FAX で直接法務部に送られると，電気通信事業法４条の通信の秘密（以下単に「通信の秘密」）に抵触する照会でなければ対応し，抵触するおそれがある場合（後掲図表２参照）には，記録命令付差押許可状を得るよう依頼する。

通信の秘密に抵触するかどうかの判断は，「電気通信事業における個人情報保護に関するガイドライン」[6]（以下「通信個人情報 GL」）15条（第三者提供の制限）1項１号（法令に基づく場合）とその解説(3)に従っている。

> ○電気通信事業における個人情報保護に関するガイドライン（本文及び解説）
>
> （第三者提供の制限）
>
> 第15条　電気通信事業者は，次の各号のいずれかに該当する場合を除くほか，あらかじめ本人の同意を得ないで，個人情報を第三者に提供しないものとする。
>
> 一　法令に基づく場合
>
> 二　～四　（略）
>
> 解説(1)
>
> 通信履歴は，通信の構成要素であり，電気通信事業法第４条第１項の通信の秘密として保護される。したがって，これを記録することも通信の秘密の侵害に該当し得るが，課金，料金請求，苦情対応，自己の管理するシステムの安全性の確保その他の業務の遂行上必要な場合には正当業務行為として少なくとも違法性が阻却されると考えられる。

6）　平成16年８月31日総務省告示第695号（最終改正　平成27年６月24日総務省告示第216号）。

解説(3)

「法令に基づく場合」とは，例えば，裁判官の発付する令状により強制処分として捜索・押収等がなされる場合や法律上の照会権限を有する者からの照会（刑事訴訟法（昭和23年法律第131号）第197条第２項……がなされた場合である。前者の場合には，令状で特定された範囲内の情報を提供するものである限り，提供を拒むことはできない。これに対し，後者の場合には，原則として照会に応じるべきであるが，電気通信事業者には通信の秘密を保護すべき義務もあることから，通信の秘密に属する事項（通信内容にとどまらず，通信当事者の住所・氏名，発受信場所及び通信年月日等通信の構成要素並びに通信回数等通信の存在の事実の有無を含む。）について提供することは原則として適当ではない。他方，個々の通信とは無関係の加入者の住所・氏名等は，通信の秘密の保護の対象外であるから，基本的に法律上の照会権限を有する者からの照会に応じることは可能である。もっとも，個々の通信と無関係かどうかは，照会の仕方によって変わってくる面があり，照会の過程でその対象が個々の通信に密接に関係することがうかがわれる場合には，通信の秘密として扱うのが適当である。いずれの場合においても，本人等の権利利益を不当に侵害することのないよう提供等に応じるのは，令状や照会書等で特定された部分に限定する等提供の趣旨に即して必要最小限の範囲とすべきであり，一般的網羅的な提供は適当ではない。

1-4　捜査対応説明文書

ニフティの捜査対応方針は，全国都道府県警察にニフティの捜査への対応を説明する文書に記載し，警察庁を通じて配布・更新している。以下主な内容を挙げる。

- 通信の秘密の該当性による捜査関係事項照会での対応の可否（図表２参照）

  例）オークション詐欺の出品者連絡先としてのメールアドレス（IP 電話番号）から加入者情報を照会するのは可。特定のメールの送信元情報から加入者情報を照会するのは差押えで対応

図表２　照会・差押えの区分

		判明している事項					
		住所・氏名・生年月日等	@nifty ID	メールアドレス	IP アドレス＋日時	ココログ ホームページ	IP 電話番号
照会対象情報	会員情報	照会書	照会書	場合による	差押	差押	場合による
	接続ログ	差押	差押	差押	差押	—	—
	メール送受信ログ	差押	差押	差押	差押	—	—
	IP 電話発信ログ	—	—	—	—	—	差押
	会員契約の有無	照会書	照会書	照会書	—	—	照会書

出所：都道府県警向け捜査対応説明書より

- 捜査関係事項照会書の文例
- 記録命令付差押えの手順と「べきもの」記載例
  ※　ニフティはサイバー刑事法[7]施行日（平成24年６月22日）から記録命令付差押えで対応。
- 通信履歴の保存方針と期間
- 通信履歴（メール送受信記録）の保全要請（後掲図表３参照）

2．ログ保全

2-1　ログ保全の制度化

1990年代後半から犯罪捜査のためにコンピュータデータそのものや，通信履歴が消去されないようにする（保全）法的制度の必要性が議論されていた。代表的なフォーラムとしては G8（G7+ ロシア）ハイテク犯罪サブグループと欧州評議会である。

7）　情報処理の高度化等に対処するための刑法等の一部を改正する法律　平成23年６月24日法律第74号。

欧州評議会[8]では，サイバー犯罪条約[9]16条「保存されたコンピュータデータの迅速な保全」[10]において捜査機関によるトラフィックデータ（通信履歴）を含むコンピュータデータの迅速な保全（expedited preservation）を導入（16条１項）し，保全期間は90日（更新可能）を限度（同２項）とし，守秘義務を課す（同３項）立法を義務付けた。

サイバー犯罪条約批准にあたり，わが国では刑事訴訟法を改正し，捜査機関が，差押え又は記録命令付差押えをするため必要があるときISPが業務上記録している通信履歴の電磁的記録を特定し，30日を超えない期間保全要請でき（刑事訴訟法197条３項），計60日まで延長可であり（同４項），守秘義務を課せる（同５項）とした。なお，通信個人情報GL23条の解説⑸が平成27年６月24日に改正され，本保全要請に従う場合は，例外的に通信履歴の保存を継続することができる旨確認された。

○電気通信事業における個人情報保護に関するガイドライン（本文及び解説）

（通信履歴）以下網掛け部分は平成27年改正での追加部分

第23条　電気通信事業者は，通信履歴（利用者が電気通信を利用した日時，当該通信の相手方その他の利用者の通信に係る情報であって通信内容以外のものをいう。以下同じ。）については，課金，料金請求，苦情対応，不正利用の防止その他の業務の遂行上必要な場合に限り，記録することができる。

（中略）

解説⑸

いったん記録した通信履歴は，第10条の規定に従い，記録目的に必要な範囲で保存期間を設定することを原則とし，保存期間が経過したときは速やかに通信履歴を消去（個人情報の本人が識別できなくすることを含む。）する必要がある。また，保存期間を設定していない場合には，記録目的を達成後，速やかに消去する必要がある。

8）Council of Europe

9）Convention on Cyber Crime

10）Article 16－Expedited preservation of stored computer data

（中略）
ただし，刑事訴訟法第197条第３項及び第４項に基づく通信履歴の電磁的記録の保全要請等法令の規定による場合その他特別の理由がある場合には例外的に保存し続けることができると考えられる。自己又は第三者の権利を保護するため緊急行為として保存する必要がある場合は，その他特別な理由がある場合として保存が許されると考えられる。

2-2　実務と考え方

ニフティでの保全実務は図表３のとおりである。

ニフティでは，常時接続では通信履歴の保全要請事例は無い。加入者の特定が捜査上必要なことが明白であれば，１日でも記録命令付差押許可状が取得できるからであろう。サイバー犯罪条約で想定した捜査共助目的の保全要請[11]も実績が無い。

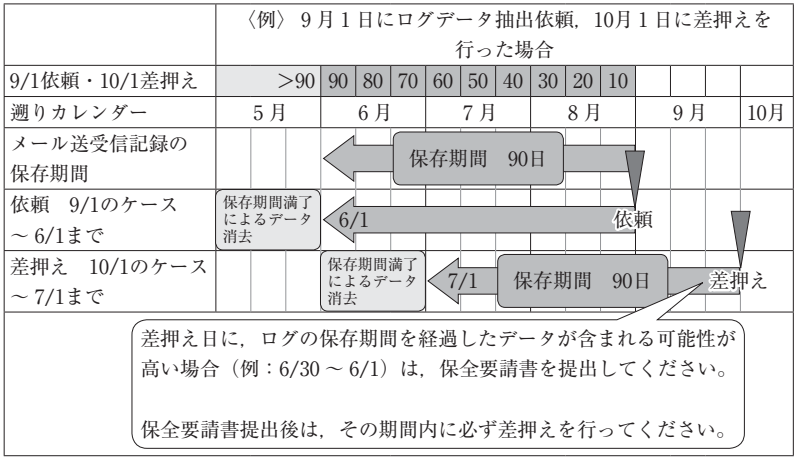
なぜかつい最近まで本制度は役に立たない，または使いにくいとされていたようであり，2013年度以前はニフティにも実例が無かった。2014年度にメール送受信ログの保存期間満了ぎりぎりに差押えが可能かどうか大阪府警から問合せがあったときに，保全要請書を提出するよう勧めたところ，保全要請がなされたのが初めてである。2014年度の実績は計４件，すべてメール送受信ログだった。

メールの送受信ログは，ISP の加入者たる被疑者の数日～数週間にわたるネット上の通信活動事実の立証をしたい場合に差押えられるものであろう。日々活動の痕跡が消えていくのを止めるニーズがある類型と思われる。一方，被疑者の１回の通信について特定を急ぐ事情があれば，最初から（記録命令付）差押えをすればよく，１日で裁判所の差押許可が得られるのに，保全要請をする時間は無駄である。

なお，ログ保全制度を活用すれば事後追跡性を確保できるのに，活用していないためにログが失われた事案も相当あるものと推察される。そのよ

11）　Article 29 – Expedited preservation of stored computer data

図表３　保全要請の説明



出所：都道府県警向け捜査対応説明書より

うな事例については，後述のログ保存の義務化賛成論の根拠とならない。

3．ログ保存

3-1　G8 ハイテク犯罪サブグループ官民対話（2000 ～ 2001）

G8 ハイテク犯罪サブグループでは，2000年から2001年にかけてパリ―ベルリン―東京においてハイテク犯罪における官民対話を続け，東京ラウンドでは，データ保全，脅威分析・予防，電子商取引の保護・ユーザー認証，ハイテク捜査訓練と並んでデータ保存について議論がされた。コスト・リソース，ビジネスモデルによる事情の違い，法律上・技術上・コスト・プライバシーの課題を考慮した実務について議論された[12)]が，結論は出ず，物別れに終わっていた。私も参加者の一人として CNN のインタビ

12）G8ハイテク犯罪対策・官民合同ハイレベル会合プレス・リリース http://www.mofa.go.jp/mofaj/gaiko/hitech/01tokyo/press.html

ューを受け，「単に犯罪をコントロールすることに役立つからといって人権やプライバシーをないがしろにして不注意な立法をすべきでない」旨，答えていた[13]。

3-2　サイバーセキュリティ戦略

ログ保存は，常に捜査機関から制度化の要望はあったが，サイバー犯罪の事後追跡可能性の手段としてあらためて脚光を浴びたのは「サイバーセキュリティ戦略」（情報セキュリティ政策会議平成25年６月10日，以下「旧戦略」という）[14]である。そこでは通信履歴等に関するログ保存のあり方の検討，特に①通信の秘密との関係，②セキュリティ上有効な通信履歴の種類，③保存する通信事業者等における負担，③海外でのログの保存期間，④一般利用者としての国民の多様な意見等を勘案することとされている。サイバーセキュリティ基本法[15]12条にもとづく新サイバーセキュリティ戦略[16]では，「サイバー犯罪に対する事後追跡可能性を確保するためには，サイバー関連事業者の協力が不可欠であることから，その事業活動に関し，適切な取組がなされるよう必要な対応を行う。特に，通信履歴の保存の在り方については，通信個人情報 GL の解説の改正を踏まえ，関係事業者における適切な取組を推進する。」とされている。

> ○電気通信事業における個人情報保護に関するガイドライン（本文及び解説）
> （通信履歴）以下網掛け部分は平成27年改正での追加部分
> 第23条　電気通信事業者は，通信履歴……については，……記録することができる。
> （中略）
> 解説(5)

13）　http://edition.cnn.com/2001/TECH/internet/05/31/g8.cyber.crime.idg/
14）　http://www.nisc.go.jp/active/kihon/pdf/cyber-security-senryaku-set.pdf
15）　平成26年11月12日施行。
16）　平成27年９月４日閣議決定。

いったん記録した通信履歴は，……保存期間が経過したときは速やかに通信履歴を消去する……必要がある。また，保存期間を設定していない場合には，記録目的を達成後，速やかに消去する必要がある。

この保存期間については，提供するサービスの種類，課金方法等により各電気通信事業者ごとに，また通信履歴の種類ごとに異なり得るが，業務の遂行上の必要性や保存を行った場合の影響等も勘案し，その趣旨を没却しないように限定的に設定すべきであると考えられる。

例えば，通信履歴のうち，インターネット接続サービスにおける接続認証ログ（利用者を認証し，インターネット接続に必要となるIPアドレスを割り当てた記録）の保存については，利用者からの契約，利用状況等に関する問合せへの対応やセキュリティー対策への利用など業務上の必要性が高いと考えられる一方，利用者の表現行為やプライバシーへの関わりは比較的小さいと考えられることから，事業者がこれらの業務の遂行に必要とする場合，一般に6か月程度の保存は認められ，適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など，より長期の保存をする業務上の必要性がある場合には，1年程度保存することも許容されると考えられる。

3-3　通信個人情報GLの本文及び解説の改正

旧戦略を受け，総務省では「ICTサービス安心・安全研究会」に「個人情報・利用者情報等の取扱いに関するWG」を設置し，ISPに接続認証ログの保存を義務付けるのではなく，通信個人情報GL23条（通信履歴）1項の解説⑸に通信の秘密の観点からログ保存を許容できる期間の考え方を例示する改正をした。

3-3-1　通信の秘密と正当業務行為（刑法35条）

もともと，通信個人情報GL23条では，通信履歴は，課金，料金請求，利用者の苦情対応，不正利用の防止その他の業務の遂行上必要な場合記録することができ（1項）第三者提供については禁止し，利用者の同意がある場合及び刑法35条にて違法性阻却される場合を確認的に例外として明記

している（2項）。

通信履歴の保存期間については，記録目的に必要な範囲で保存期間を設定し，期間経過後は消去する必要があるが，各事業者毎に業務上の必要性や保存を行った場合の影響等も勘案し限定的に設定すべきである（解説(5)）。

3-3-2　接続認証ログの例示

正当業務行為の範囲であるかどうかの物差しとして，*接続認証ログ*が例示された。保存許容期間は，

(i)　一般に6ヶ月程度：利用者からの契約，利用状況等に関する問合せへの対応やセキュリティー対策への利用など業務上の必要性が高いと考えられる一方，利用者の表現行為やプライバシーへの関わりは比較的小さいこと

(ii)　1年間：適正なネットワークの運営確保の観点から年間を通じての状況把握が必要な場合など，より長期の保存をする業務上の必要性がある場合

とされた。

3-4　実務と考え方

@ niftyの常時接続サービスでは接続認証ログを1年間保存しており，その旨警察向け捜査対応説明書に明記している。捜査当局から接続認証ログが消去されてしまったことの苦情を受けたことは無い。捜査対応説明書が奏効し，過去1年超のログを頼りとする証拠収集をはじめから諦めた場合もあると思うが，そもそもそれほどニーズが無いとも考えられる。

4．強制捜査――差押えから記録命令付差押えへ

4-1　サイバー犯罪条約の提出命令（18条）と記録命令付差押え（刑事訴訟法99条の2）

サイバー犯罪条約では，物理的な差押えに加え，コンピュータデータの

保有者に当該データ（18条１項(a)項）そしてISPに加入者情報（同(b)項）の提出を命ずる立法を義務付けた。サイバー犯罪条約を受け，サイバー刑事法では記録命令付差押え（データを保管する者その他利用権限を有する者に命じてメディアに記録させまたは印刷させた上で，メディアまたは紙を差押えること）を導入した。

4-2　従来の差押えと記録命令付差押えのISP実務の違い

従来の差押えでは，ニフティなどのISPは，サーバー（通常は遠隔地のデータセンターにあるサーバー）が物理的に差押えられることを回避するために，自ら進んで加入者情報その他の情報をメディアに複写したり紙に印刷したりして準備しておき，当該モノを「差押えるべきもの」として記載するよう捜査当局に要請していた。

しかし，差押え前の状態（令状が強制力を持つ以前に加入者を特定する等，通信の秘密やプライバシーを侵害する作業をしていること）が通信の秘密やプライバシーの侵害である，と解釈されるリスクは，――提出を拒絶すればサーバーが差押えられサービス停止を余儀なくされることを回避する目的があるための行為であるから正当防衛ないし緊急避難が成立し得るとしても――現に存在していた。

したがって，令状の強制力が加入者の特定等の作業時点から発生する記録命令付差し押さえのほうがISPにとっては好ましい（同様の指摘がサイバー犯罪条約のEM171[17]にある）。

17）“171. A “production order” provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.”

5．児童ポルノブロッキング

5-1　児童ポルノブロッキングの実施体制

ブロッキングとは，ブラックリストに掲載されたサイトや個々の画像等の要素をドメイン，URL等の単位により接続を遮断するものである。フィルタリングの一種であるが利用者個別の例外的接続要求（オプトアウト）を許さないものを指す。児童ポルノのブロッキングについては，民間のリスト作成管理団体である一般社団法人インターネットコンテンツセーフティ協会（“ICSA”）[18]がブラックリストを作成管理している。

2009年頃からの官民の議論を経て，ICSAは，児童ポルノ排除総合対策（2010年7月）の枠組みにより設立され，2011年4月から運用を開始した。ICSAはインターネットホットラインセンター[19]から提供された児童ポルノの情報から，ブロック対象となる画像かどうかの判定をした上でアドレスリストを確定しニフティ等ISPや検索事業者等の事業者へ提供している。

5-2　通信の秘密の緊急避難による違法性阻却

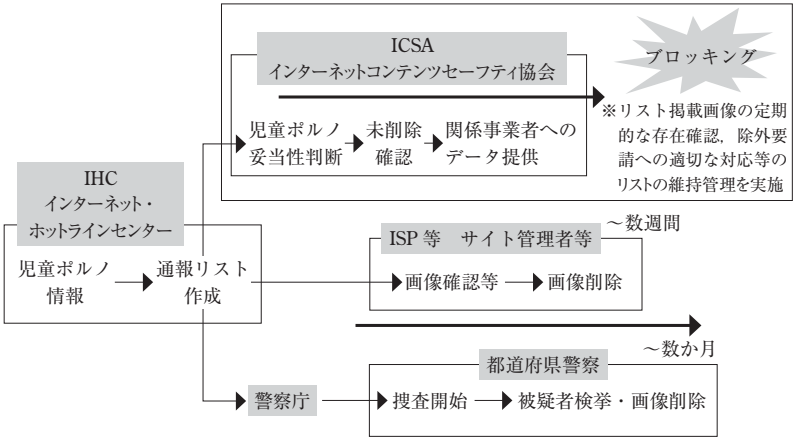
ISPによる児童ポルノブロッキングは加入者のすべての通信の宛先をブラックリストと照合して行われるので当然に通信の秘密に抵触する。ISPとICSAがブロッキングを実施できるのは，緊急避難として整理されているからである。安心ネットづくり促進協議会児童ポルノ対策作業部会最終報告書（2010年6月8日）[20]によると緊急避難の3要件については以下の

18）　http://www.netsafety.or.jp/

19）　https://www.internethotline.jp/

20）　http://www.good-net.jp/investigation/working-group/anti-child-porn/2010/169-1751.html 通信の秘密，表現の自由等の法的問題については法的問題検討サブワーキング報告書 http://www.good-net.jp/investigation/uploads/2013/10/30/20100618_4.pdf 参照。

図表４　ブロッキング実施イメージ図



出所：http://www.netsafety.or.jp/blocking/index.html より

とおり解されている。

- 「現在の危難の存在」

児童ポルノがウェブ上に流通し得る状態に置かれた段階で，当該児童の人格権等に対する侵害が生じ，誰でもアクセスし得る状態が継続している限り，危難が常時存在する。

- 「補充性」

児童ポルノの削除，流通させたものの検挙により危難を防止することが容易でも実効的でもない場合，典型的には海外にサーバーがある場合かつ管理者に国内での接点が無い場合に認められる。

- 「法益の権衡」

ブロッキングによる通信の秘密の侵害による害は，児童の受ける重大かつ深刻な人格的利益に比肩するが，特に画像の内容が著しく児童の人格権等を侵害するものであれば，満たされる。

5-3　オーバーブロッキングと表現の自由

ISP = ICSA という民間の枠組みでブロッキングを行う場合には，憲法

上の検閲の禁止が直接適用されないし，表現の自由を国が制約したことにもならない[21]が，自らは児童ポルノを流通させていないオーバーブロッキングの被害者は表現の自由を侵害されたことになり ISP 又は ICSA が民法の不法行為責任を負う可能性がある。したがって，オーバーブロッキングのリスクができるだけ少ない方式を採用し，リスト作成時にも回避策をとること，被ブロック者への通知画面やリスト除外措置等のセーフガードが要求される。

5-4　児童買春・児童ポルノ禁止法改正による努力義務

改正児童買春・児童ポルノ禁止法16条の３（2014年７月15日施行）は，ISP に対し，捜査協力，情報の削除と並び，児童ポルノの所持，提供等の行為の防止に資するための措置を講ずる努力義務を課した。当該措置にブロッキングが含まれているとされている。

5-5　実務と考え方

ニフティは ICSA に加盟し，児童ポルノのブロッキングリスト配布を受けブロッキングを実施するとともに理事会，運営委員会[22]等で積極的に活動している。リストの作成自体は ICSA に任せるしかないが，受領したリストの適用を誤るとオーバーブロッキングが生じかねないので，慎重なオペレーションを続けている。

21）　トルコ政府が，トルコ共和国建国の父アタチュルクを冒瀆するメッセージを記載したサイトを含むドメインをブロックするよう裁判所に申立て，ブロッキング命令が実行されたが，オーバーブロッキングとなり欧州人権条約違反であるとされた欧州人権裁判所事例 Ahmet Yildirim v Turkey ECtHR (Second Section) no. 3111/10, (18 December 2012) page 505 ECHR 2012−VI 参照。

22）　http://www.netsafety.or.jp/about/002.html

6．ボットネット対策への協力

以下，いずれも銀行のオンラインバンキング口座の ID，パスワードを窃取するためのマルウェア（Banking Trojan）に感染し，ボットネットのゾンビクライアントとして稼動している端末に対して駆除を呼びかける活動である。警察庁または欧米の司法当局から得た感染端末情報が，Telecom-ISAC の Active Project 経由で ISP に通知され，ニフティ他の ISP は感染端末を稼動させている加入者に駆除を要請した。

- Citadel（2013年 8 月）

初めて大規模な Banking Trojan 駆除活動に日本の ISP が参加した事例である。

- Game over Zeus ボットネットのテイクダウン作戦（2014年 7 月）

米国司法省・FBI の大規模なボットネットテイクダウン作戦の一環であった。

- VAWTRAK（2015年 4 月）

日本を中心に感染活動をしているとされる。

このような加入者への駆除要請活動と通信の秘密との関係は，総務省「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」[23]にて緊急避難として整理[24]されている。

同研究会では，さらに感染端末と C&C サーバーのドメインネームとの通信を DNS によりフィルタリングすることの可否を検討し，加入者から一定の同意を得れば可能[25]であるとした。

23） http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/index.html

24） 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会第一次とりまとめ http://www.soumu.go.jp/main_content/000283608.pdf 22–24 頁。

25） 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会

おわりに

ニフティをはじめとするISPの任意・強制捜査対応と，ログの保全と保存，児童ポルノブロッキングやボットネットに関する協力施策の例に見られる犯罪被害の拡大を抑止・防止する協力の実務と考え方は慎重な議論を経ながらも着実に整理され進んできた。

新たな施策に踏み込む（，又は旧来の施策を拡大する）場合には，通信の秘密やプライバシー，表現の自由への影響等を分析しつつ慎重な議論が望まれるが，事後追跡性の確保や被害拡大の抑止・防止の必要性に係わるファクトをベースとした議論であれば，今後とも，ISPは誠意を持って参加していくであろう。

（2015年10月29日脱稿）

第二次とりまとめ http://www.soumu.go.jp/main_content/000376396.pdf 12–14頁。児童ポルノのブロッキングでは緊急避難構成であることと対比されたし。