講　演

シンポジウム
「サイバー犯罪：捜査とガヴァナンス」

Symposium “Cybercrime: Its Investigation and Governance”

堤　　和　通*

本紹介に続く論稿は，2015年 6 月 3 日（水）に開催した，中央大学学術シンポジウム個別プロジェクト「サイバースペースの法的課題と実務的対応」によるシンポジウム「サイバー犯罪：捜査とガヴァナンス」の基調講演並びにパネリスト報告である。

サイバー犯罪が近年，喫緊の治安課題として急速な関心を集めていることは言うまでもない。サイバー犯罪条約批准に合わせた法改正，リベンジポルノ対策立法，JC3の開設，サイバー防犯ボランティア活動の拡充など，新たな制度設計や運用改善が重ねられ，また，総務省の関連ガイドラインの改定などにみられる，プロヴァイダからの位置情報取得やログの保存に関する検討が進む一方で，TOR 利用犯罪での誤認逮捕，不正送金事案の増大，情報セキュリティの不備による個人情報流出などの，サイバースペースでの安全確保への脅威を物語る事案，状況が報じられている。この問題は日本にとどまらない。参加者の性善説を前提にした規制のない自由な空間という構想で始まったインターネットが，今や，その可能性を十全に発揮し世界を結ぶ網の目となり，Web を利用した情報に出会う場として，また物の管理手法として活用される中で，脆弱性を解消できない機器の利

＊　所員・中央大学総合政策学部教授

用者が防護に必要なコストを十分に掛けないという状況のために，サイバー犯罪やサイバー攻撃の加害者が，被害者それに被害の予防と追跡に当たる捜査機関，法執行機関よりも優位に立つことから，加害行為の促進と被害追跡の益々の難化というサイクルに陥っているという懸念も示されている。

サイバースペースをめぐるこの状況は，サイバー犯罪，サイバー攻撃が日本の現行法と実務を比較法の観点から不断に検討すべき課題であることを示している。加えて，この課題を扱う際には，サイバーの分野ではこれまで多くは議論されてきていないものの，犯罪政策の分野では20年を超える歴史をもつ犯罪のガヴァナンスという視点を明確にすべき時期に来ている。犯罪のガヴァナンスは，犯罪の事後対処の仕組みとして，犯罪の認知と捜査に始まる刑事司法の枠組みを固持するのではなく，むしろ，犯罪の予防という視点も加え，コミュニティを含めた新たなパートナーシップの構築を説き，犯罪減少のための包括的視点に立った，新たな役割分担，責任体制の検討を加えるものとして提唱された見方である。サイバースペースは，現在，インフラとして，それも他に類がないような，多様な効用を生むインフラとして存在している。その安全確保には，従来の刑事司法にはない，包括的な役割分担，責任体制の検討が求められる。このシンポジウムのサブタイトルとして，捜査とガヴァナンスを掲げたのはこのような問題意識による。

シンポジウムでは，Urbas 氏はサイバー犯罪条約とオーストラリアの国内法を中心に捜査法，とくに令状による捜索押収法，オンライン上の覆面捜査，プロヴァイダの義務，責任，ログの保全，保存について報告し，中野目氏は日本の捜索押収法の全体像をふまえながらサイバースペースでの捜査手法と法的規律，それに，プロヴァイダの役割を論じる（中野目氏の報告は本誌次号に掲載予定）。岡部氏は，日本の犯罪情勢，おとり捜査，ポリスウェアを含む捜査手法の現況と課題，民間企業等との連携を論じる。丸橋氏は，ニフティ株式会社における捜査対応実務の詳細を報告するとともに，ログの保全・保存並びに，記録命令付き差し押さえについてそ

の考え方を論じている。最後に，宮下氏は，データ保全や監視プログラムに関するEU，米国などの法状況を報告し，デジタル時代のプライヴァシー権を論じる。

シンポジウムで進行を務めた立場から若干のコメントを許されるとすれば，Urbas氏の基調講演の中で報告があった，プロヴァイダの義務，責任に関するオーストラリア法の立場は参考になるだろう。また，日本の捜査に関連して，サイバースペースでの証拠の発見収集が捜索押収法として構成されているのか否かは検討に値するであろう。また，ガヴァナンスの観点からは，プロヴァイダのきめ細かな実務対応は適切に評価されるべきであろうし，ログの保全，保存については，コストの負担の公正さと効率性という基準からの検討を進めるべきであろう。個人情報の保護については，それに活用すべき民事救済と刑事制裁の在り方，それに，その保護の必要性とサイバースペースを含めた安全確保の要求との衡量が検討課題になるように思われる。

最後に，シンポジウム参加者について一言ずつ紹介しておきたい。Gregor Urbas氏は著書Cyber Criminals On Trial, Cambridge University Press (2004)（Peter Grabosky，Russell G. Smithとの共著）で広く知られているサイバー犯罪の研究者である。同書はサイバー犯罪の被害調査を主とした実態解明と，サイバースペースの刑事規制について実体法並びに捜査と証拠に関する手続法，国際刑事法の現状と課題，刑事制裁と量刑を扱う良書で，2005年にアメリカ犯罪学会から受賞されている。この他にも，サイバー犯罪に関する司法共助や青少年保護に関する論稿などを著している。中野目善則氏は刑事法を専門とし，日本の捜索押収に関する論稿（「緊急捜索・押収の適法性について」中央ロー・ジャーナル9巻1号3頁（2012年）など）のほかアメリカ合衆国の捜索押収法についても最高裁判所の裁判例の紹介評釈を広く行ってきている（渥美東洋編『米国刑事判例の動向Ⅳ』中央大学出版部（2012年）参照）。岡部正勝氏は，現在，慶應義塾大学総合政策学部教授であるが，前・警察庁長官官房参事官（サイバーセキュリティ担当）としての実務経験をふまえ，研究者としての見解を

開陳している。丸橋透氏はニフティ株式会社の法務部で長きにわたり法実務に携わっており，情報ネットワーク法学会で研究会の主査を務めるなど，日本におけるサーバースペースでの事業についてその創成期から現在までを熟知する立場からパネル報告がなされている。宮下紘氏は，近著『プライバシー権の復権：自由と尊厳の衝突』（中央大学出版部，2015年）が示すように，個人情報保護に関する国内法並びに比較法に通じる知見から比較文化の視点を入れた，現在社会でのプライヴァシー論に至るまで考察を巡らせている公法研究者である。基調講演者，パネリストの方々にはこの場を借りて御礼を申し上げたい。

サイバー犯罪の捜査とガヴァナンス

Cybercrime: Its Investigation and Governance

グレゴア・アーバス*
訳 堤　和通**

序

サイバー犯罪がこれまでにない広がりと，インパクト，洗練さ，それに組織性を見せるのに応じて，サイバー犯罪に対する法執行並びにガヴァナンスもまた進展をしている。警察機関は，これまで，犯罪の物証が存在する物理的場所の捜索とその押収に関わる捜査の訓練を受けてきたが，コンピュータ並びにネットワークから情報を収集できるようにその捜査手続きを適応させなければならない。捜査機関の中には，コンピュータ捜査の技量を備えたスペシャリストを配置した「ハイテク」ユニット（高度技術班）を創設しているところがある。また，民間の専門技量と協力に――とりわけ，デジタル・フォレンジック分析の場合に――大きく依拠するところもある。

刑事司法での証拠の保全，組織立て，並びに提示もまた変容してきている。電子媒体を証拠方式として認める立法がなされ，裁判官並びに陪審が複雑な技術情報（technical information）を咀嚼することが求められてき

＊　キャンベラ大学准教授
Gregor URBAS
Associate Professor
＊＊　所員・中央大学総合政策学部教授

ている，というのがその変容の一つの姿である。技術情報の咀嚼には，鑑定証人の証言とリポートの助けが益々必要になってきている。今では，サイバー犯罪のみならず，他の多くの刑事訴追で，スマートフォンのような通信機器，それに，住居やビジネスのコンピュータ，インターネット，「クラウド」のようなデータ保存のプラットフォームから入手した証拠の利用があるのが常である。

データ並びにデータを個人に結びつける情報をはじめとして，現代の通信インフラとサーヴィスはその多くが民間企業その他の，政府とは異なる部門の手中にある。そのため，サイバー犯罪との戦いに一定の役割を果たすよう，民間部門をどのように説得し，あるいは義務づけるのか，という点に益々焦点が当てられてきている。これは，具体的な事案での法執行への協力をめぐるものがあるが，より一般的には，将来の捜査に役立つ可能性があるデータの収集と保全に関するポリシーを通した役割に関わる。この点には，他方で，コストや消費者のプライヴァシーをはじめとする，ビジネス組織に関連する事情，それに，市民，ビジネスと政府間の関係が関わっている。

1．サイバー犯罪の訴追に必要な証拠

コンピュータ・ハッキング，マルウェア使用，ウェッブ・サイト破損，コンピュータ・システムと通信の毀損など，広くサイバー犯罪と称される種類の犯罪では，捜査並びに訴追段階で必然的に電子的証拠が扱われる。そのような証拠の発見，分析と収集に必要な技量と専門能力は警察部門に通常見出されるものでは間に合わない。そのため，コンピュータ関連の捜査のための特別ユニットが創設されてきている。オーストラリア連邦警察のハイテク犯罪センターはその一つである。今では，ハイテク犯罪オペレーション（High Tech Crime Operations，HTCO）[1)]として知られている。

1） http://www.afp.gov.au/jobs/current-vacancies/high-tech-crime-operations

「HTCO 手持ちの手法により，オーストラリア連邦警察は重大で複雑なテクノロジー犯罪の実行を中断させ，捜査・訴追する高い能力を備えている。テクノロジー犯罪には，分散型 DOS 攻撃のようなコンピュータへの重要な侵入，主要なコンピュータ・システムの損壊，個人，ビジネス，金融データの組織的で大規模な取得，マルウェアの作成，支配または頒布，それに，銀行並びに金融部門に直接影響を与える犯罪がある。
HTCO は，子どもに対するオンライン上の，並びに旅行・観光での性的搾取を捜査する責任を負う。HTCO は，他の法域，とりわけ，社会経済的な発展を遂げる地域の法域が旅行・観光での子ども対象の性的搾取と戦う支援をしている。そこでは，HTCO は，地方の法執行機関，並びに NGO などの他の関連機関と協働している。HTCO は，子供の性的搾取を進める意図でインターネットを利用する犯行者を捜査しターゲットにしている。」

同様の特別ユニットが，日本をはじめ他の国々に設置されてきている。そこでは，銀行やコンピュータ会社などの民間部門とインターポールなどの国際団体の支援を得ている[2)]。

サイバー犯罪の捜査に多く必要になる種類の証拠には，コンピュータ・ログ，使用者とパスワードの詳細，蔵置並びにトラフィック・データ，閲覧したウェッブ・サイト，ネットワーク上の他のコンピュータとのリンクが含まれる。他方で，こうした種類の証拠がより伝統的な捜査にも重要であることが多いことには留意しておかなければならない。例えば，「2007 年，Melanie McGuire は夫の William の殺害で有罪と認定された。訴追側によれば，McGuire 夫人は抱水クロラール（催眠剤）を夫に飲ませ，3，

2） Online news report, “Japan police to launch national cyber crime force” (28 March 2013): http://phys.org/news/2013-03-japan-police-national-cyber-crime.html; “INTERPOL National Cybercrime Training Seminar, 4–6 February 2014, Tokyo, Japan,” reported online at: http://www.interpol.int/News-and-media/Events/2014/INTERPOL-National-Cybercrime-Training-Seminar2/INTERPOL-National-Cybercrime-Training-Seminar.

４回夫を撃ち，遺体をバラバラにしてチェサピーク湾に遺棄した。遺体発見後，警察は捜査を開始した。……警察のコンピュータ・フォレンジック分析者は夫妻住居のコンピュータを調査し，殺害の前に，何者か――おそらくは Melanie McGuire ――がそのコンピュータを使用して『殺し方』，『銃の違法入手方法』，『検知不能毒物』などのトピックを調べていたことをつきとめた。」[3)]

このように，コンピュータの使用は，犯罪の前と犯罪の間の犯行者の計画と意図に関する有用な証拠になる。また，コンピュータの使用は，共謀の事案で個人間の繋がりを立証する上で重要な役割を果たすことができる。サイバー犯罪の事案では，コンピュータのデータは，DOS 攻撃の命令，ネットワークへのマルウェアの放出，年少者との不品行な会話などの犯罪事実の証拠になる場合がある。例えば，子どもの搾取の事案では，ポルノ画像や他の違法なコンテンツの証拠が，被疑者のコンピュータや，性的な目的で子どもを誘引しているチャットのログから得られるのは今では普通のことである[4)]。このような証拠は有罪判決の獲得に大変重要であり，これにより，証人の証言や被疑者の証人だけに基づく訴追をせずに済むのである。

2．令状によるまたは無令状の証拠の収集方法

電子的証拠の収集には捜索令状の執行などの伝統的な方法が用いられることがある。被疑者の住居またはオフィスを，コンピュータ並びにコンピ

3） SW Brenner, Cybercrime: Criminal Threats From Cyberspace, Greenwood Publishing, 2010, chapter 3: Three Categories of Cybercrime; for an Australian case, see “Killer brought undone by chilling step-by-step murder plan jailed for 26 years,” The Age, 30 April 2014: http://www.theage.com.au/victoria/killer-brought-undone-by-chilling-step-by-step-murder-plan-jailed-for-26-years-20140430-zr1yo.html.

4） 本稿第５章で論じるオーストラリアの事案参照。

ュータ蔵置データを含めて捜索する必要がある場合がそうである。ヨーロッパ評議会のサーバー犯罪条約は，捜索押収をはじめとする，コンピュータ蔵置データの収集方法に関する広範な規定を定める[5]。例えば，19条は「権限のある機関が」「(a)コンピュータ・システムまたはその一部並びにその蔵置データ，及び」「(b)自国領土でコンピュータ・データを蔵置できる媒体」「を捜索しまたは他の方法でアクセス」でき，さらには，「(a)コンピュータ・システム若しくはその一部またはコンピュータ・データの蔵置媒体を差押えまたは他の方法で支配下に置き」，「(b)コンピュータ・データのコピーを作成並びに保全し」，「(c)関連するコンピュータ蔵置データの完全性を守り」，「(d)アクセスしたコンピュータ・システムにあるコンピュータ・データへのアクセスを遮断し，またはデータを削除」することを許されるのに必要な「立法並びにその他の措置を」締約国が講じることを義務づけている[6]。それに応じて，多くの国が国内法を改正し，令状による捜索権限を広げて，捜索場所で発見したコンピュータの作動，コンピュータ・ファイルのコピーの作成に必要な，警察官持参装置の作動と技術支援，他の場所での詳細な分析のための，コンピュータ並びに蔵置装置の移動まで含むように改めてきている。オーストラリアでは，2001年オーストラリア連邦・サイバー犯罪法の下で，そのような捜索権限の規定が定められた。同法は，併せて，パスワード，アクセス制御，暗号化／暗号解読などの知識がある者にその情報提供を義務づける裁判所命令の規定をおいている[7]。興味深いことに，警察が令状によるコンピュータの捜索を許され

5） オーストラリア，カナダ，日本，南アフリカ，アメリカ合衆国のほか，ヨーロッパの40を超える国が署名している。日本は署名を早くにしているが，批准をしたのは，オーストラリア同様，2012年である。条約は，日本では2012年11月１日から，オーストラリアでは2013年３月１日からそれぞれ発効している。

6） サイバー犯罪条約は，このほかに，蔵置データの迅速保全（preservation）（16条），トラフィック・データの迅速保全と一部開示（17条），提出命令（18条），トラフィック・データの同時収集（real-time collection）（20条），コンテント・データの傍受（21条）がある。

7） 1914年連邦犯罪法セクション3LA。2001年サイバー犯罪法で追加された。

ている場合には，その捜索は，そのコンピュータを使用したデータ――捜索場所に保持されていないデータを含む――へのアクセスまで広がる。そうすると，捜索権限は，コンピュータ・ネットワークを通した，遠隔地捜索，それも，おそらくは国境を越えた遠隔地捜索に及ぶように思われる[8)]。

国境を越えた捜索の可能性は，国際間でセンシティヴな問題であり，中には，領土主権の侵害としてそのような捜索に異議を唱える国が見られる。ヨーロッパ評議会は，「公けに利用できる（publicly available）」データに関する場合と，「データを開示する合法な権限がある者が合法かつ任意に同意している」場合に，サイバー犯罪条約上，国境を超えた捜索が許されることを明確にしようとしている。このうち前者は，国内法上は捜索令状が要件とならないのが通常のデータである。後者は，サーヴィス・プロヴァイダー並びに，データへのアクセス制御ができる他の第三者を含むであろう[9)]。

中には，アメリカ合衆国のように，令状による，また無令状での，コンピュータの捜索を律する高度に詳細な規律を用意している国がある。米国で無令状捜索が許されるのは，所有者の同意，緊急状況，合法な逮捕に伴う場合，データがプレイン・ヴューである場合，ボーダー・サーチの場合などである[10)]。令状要件と令状捜索押収の範囲は大きく変わってきてお

8） 1914年連邦犯罪法セクション3L。2001年サイバー犯罪法で追加。さらに，G Urbas and P Grabosky, “Cybercrime and Jurisdiction in Australia” in Cybercrime and Jurisdiction: A Global Survey (eds B-J Koops and SW Brenner), TCM Asser Press, The Hague (2006) 参照。

9） ヨーロッパ評議会，サイバー犯罪条約委員会（T-CY），ガイダンス・ノート＃３：国境を越えるデータへのアクセス（32条），2014年12月２，３日，フランス，ストラスブルグ採択：http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY%282013%297REV_GN3_transborder_V12adopted.pdf.

10） 司法省，コンピュータ犯罪知的財産部（Computer Crime and Intellectual Property Section, CCIPs），“Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation”: http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009pdf.

り，現代の立法は，令状による捜索押収を規律するだけでなく，電子工学的監視，通信傍受，蔵置された会話やトラフィック・データの取得まで規律している[11]。そこでは，第三者が犯罪捜査を助ける役割の重要性が問われる。

3．ISP 並びに他のプロヴァイダーの捜査での役割

大量のコンピュータ・データは最早，PC に主に蔵置されてはおらず，ネットワーク上の「トラフィック・データ」として，あるいは，「蔵置データ」としてプロヴァイダーの記録に存在するので，そのような第三者が犯罪捜査の協力で果たす役割を明らかにしておく必要がある。中には，善良な企業市民として協力を惜しまないつもりでいても，プライヴァシーに関する顧客との同意事項から制約を受ける者がおり，また，法律上の義務づけがある場合でなければ捜査支援を拒絶する者がいる。

最近のカナダの事案が問題の複雑さをよく表している。それは，インターネット・サービス・プロヴァイダー（ISP）が警察の求めに応じて顧客情報を任意で提供した事案である。その情報で，IP アドレスからプロヴァイダー契約で登録している顧客の住所が判明し，警察はその情報に基づいて顧客住居を捜索し，被告人は子どもポルノ犯罪で起訴されている。カナダ最高裁判所は，ISP に対する警察の情報提供の要請はカナダ権利章典が保障する，憲法上のプライヴァシー権――これは，子どもポルノの閲覧といった，オンライン上の違法な活動にまで及ぶ――を侵害するものであり，したがって，令状を入手するか，若しくは，提供を義務づける他の命令の発出を待って請求をすべきであったと結論づけている。ただ，カナダ

11） とりわけ，蔵置会話法（Stored Communications Act）とワイアタップ法について，司法省，コンピュータ犯罪知的財産部（Computer Crime and Intellectual Property Section, CCIPs），“Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigation”（前註），並びに，オーストラリアの「通信の傍受とアクセスに関する1979年連邦法」参照。

最高裁判所は，被告人に対する有罪判決を破棄するのは「司法への不信を招く（bring the administration of justice into disrepute）」[12]として，有罪判決を維持している。

オーストラリアでは，「キャリアー（carrier）」といわれる，通信サーヴィスのプロヴァイダーが，通信ネットワークとその設備が，連邦法または州法若しくはテリトリー法に違反する違法行為の実行に，または，違法行為の実行に関連して使用されないように「最善を尽くす（do the carrier's best）」義務を定める[13]。この規定については現在，議会調査が行われている。議会調査で示された証拠によると，

「1997年連邦通信法313条により，州政府を含むオーストラリア政府機関はオーストラリア法を執行する際に通信事業から支援を受けることができる。連邦政府は，313条を根拠に，不正利得を取得する金融不正をはたらくサイトなどオーストラリア法に違反するオンライン・サーヴィスの継続を止めてきている。313条は，オーストラリア連邦警察が，インターポールの子ども虐待ワースト・リストを用いて，苛烈な子ども虐待並びに搾取による画像などを載せたウェッブ・サイトをブロックするときの根拠にもなっている。ユーザーがこうしたサイトにアクセスを試みた場合には，ユーザーにはアクセス・ブロックを告げるページが提示され，ブロックの理由が明らかにされ，インターポールのワースト・リストに関するものを含めた，不服・異議申立ての手続きの詳細が案内される[14]。これに加えて，

12） R v. Spencer［2014］2SCR212 (Supreme Court of Canada), per Cromwell J at［81］: http://www.scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do.

13） 1997年連邦通信法（Telecommunications Act 1997 (Cth)）313条。

14） オーストラリア議会，コミュニケーション基盤に関する下院常設委員会（House of Representatives Standing Committee on Infrastructure and Communications），「1997年連邦通信法313条3項に関する政府機関の法運用調査：違法なオンライン・サーヴィスの中断（Inquiry into the use of subsection of 313 (3) of the Telecommunications Act 1997 by government agencies to disrupt the operation of illegal online services）」。この調査では公聴会が開かれ意見の具申を受ける。最終報告書は2015年7月1日に完成が予定されている。

サーヴィス・プロヴァイダーは，そのサーヴィスを介して流通するデータが子どもポルノまたは子ども虐待の画像等であると疑う合理的な根拠がある場合には，そのデータの詳細をオーストラリア連邦警察に知らせる義務を負っている[15)]。

4．データ保存要請

通信サーヴィスのプロヴァイダー等の第三者が，関連情報を開示して法執行期間の捜査に協力する義務は，プロヴァイダーがそのような情報を十分な期間にわたって，かつ，捜査官が利用できる形態で保全（preserve）していなければ実効性を欠く。各国の立法府が，現在，重要な証拠となる可能性があるデータ（sources）を確保するためのデータ保存（retention）の要件を定める立法に取り組んでいる。この立法作業は，他方で，通信サーヴィスを利用する全市民，並びに，犯罪捜査で被疑事実に関する疑いを受けていない者のプライヴァシーはもちろん，保全の費用と費用の負担をはじめとする，捜査の必要性とは別の論点を提示している。「オンライン上のプライヴァシー」は常に論争の的であるが，他方で，データ保存に関するある程度の枠組みは現れ始めている。

オーストラリアでは，広範囲にわたる一般公衆からの意見聴取の末，通信のメタデータについて２年間の保存義務を課す立法がなされている。法執行機関が蔵置会話にアクセスする場合，並びに，電子会話を傍受する場合には依然として令状が要件になっている。サーヴィス・プロヴァイダーが蔵置するメタデータへのアクセスは，ジャーナリストの情報源を開示する場合を除いて，令状は要件ではない[16)]。12ヶ月の保存を義務づけるヨ

15） 1995年連邦刑事法474条25項。ISP 並びにコンテンツ掲載サイト（internet content hosts）の義務を定める。違反行為は罰金（金銭制裁）に処せられる。

16） 通信傍受並びにアクセスに係る2015年連邦データ保全改正法は2015年３月26日に議会を通過し同年４月13日に国王同意を得た。全面的な施行期日は2015年10月13日である。同法は通信傍受並びにアクセスに係る1979年連邦法を改正

ーロッパのデータ保存指令（Date Retention）は，EU 司法裁判所が無効を宣言しているが，EU 各国はそれぞれで保存要件を定めて対応している[17]。アメリカ合衆国には限定的な保存要件を整え，保全後90日までは無令状でのアクセス権限を定め，90日を越える場合に裁判所の令状によるアクセスを認める[18]。

5．オンライン上の覆面捜査

サイバー犯罪捜査で検討すべき，もう一つの興味深い側面は「覆面（covert）」捜査手法の活用である。一般的には，これは過去数十年に及んで，違法な麻薬の輸入などの重大な組織犯罪に対抗するために警察が採用してきており，そのような覆面捜査についての国際法上並びに国内法上の基礎は十分整っている[19]。近時では，同様の覆面捜査を用いてオンライン上の子ども搾取のネットワークに進入し，「子どもを誘引」している者の身元を突き止めている。この手法では，警察官が身元を秘して子供であるよう

し，データ保全に関する新しい章，５－１－Ａを加えている。重要なのは，情報並びに文書の保持（keep）義務を定める第１節で，187条Ａが，サーヴィス・プロヴァイダーの義務を，187条 AA が保持すべき情報を，187条 B が第１節の適用が及ばないプロヴァイダーを，187条 BA が情報保秘の確保を，187条 C が保持期間を，それぞれ定める。新たな第４節 C「ジャーナリスト情報取得令状」は，1979年連邦法第４章１に規定を設けて，ジャーナリストの情報源が明らかになるようなメタデータに法執行機関がアクセスする場合には令状によるべきことを定める（rather than an authorization）（180条 G）。

17） ヨーロッパ評議会移民並びに内務部，警察協力，「データ保全」（http://ec.europa.edu/dgs/home-affairs/what-we-do/policies/police-cooperation/data-retenton/index_en.htm），並びに英国の2014年データ保全並びに捜査権限法（Data Retention and Investigatory Powers (DRIP) Act 2014, http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf）。

18） 合衆国法典18編2703条（顧客の会話または記録の開示義務）。

19） 麻薬及び向精神薬の不正取引の防止に関する国際連合条約（1988年12月20日署名）第１条はコントロールド・デリヴァリーを定義づける。

に装い，チャットで訪問者と会話をする。訪問者の中に，性的な目的で子どもとコンタクトを取ろうとしている者がいる。オーストラリアの次の事例がその手法をよく表している。

「本件公訴事実は，2007年８月21日から2008年１月21日まで展開した捜査（operation）で浮かび上がった。その間，被告人は職場，インターネットカフェ，並びに図書館のコンピュータから，インターネットを介してイーメイルとチャットで会話をしていた。会話の相手は，オークランドを拠点とするニュージーランド警察の Stephen Waugh 刑事であった。Waugh 刑事は，身元を偽り，”miss Tafsey 14, Roxanne Taylor” であると自らを称した。本日は，事実の主張並びに提出があった証拠が実際の会話の通りであるという前提に立って判断を下す。その後のやり取りで，被告人は自分のことをある程度詳しく明かしている。Waugh 刑事は自分が14歳の少女であることを告げてそれに応えた。被告人は次第に，より性的な連想をさせる誘発の度を深めていった。2007年10月25日から12月14日までの会話で，被告人は，二人きりになって Roxanne とどのような性的行為を行おうかと考えていたと話しているところを録音されている。被告人は裸の写真を自分宛てに送るように Roxanne に要求した。」[20)]

この事例で，被告人は，Roxanne との長期にわたるチャットのログなどの証拠について，警察の不適法または違法な方法で得られたものとして排除申立てをしている。しかし，裁判所は，公序と，オンライン上の覆面捜査を許した議会の意図を根拠に，次のように判示して排除申立てを斥けている。

「このような捜査で立ち向かうべき害悪は社会公共に甚大な影響を及ぼす。インターネットが普及したために，子どもを腐敗させ性的に搾取しようとする者は，これまでにない，大規模な数の潜在的被害者に近づく術を得ている。実際の被害者からの告訴または本件のような捜査がなされないかぎり，そのような略奪者を発見するのはまず困難であろう。マタイによ

20） R v. Stubbs［2009］ACTSC 63 (26 May 2009), per Higgins CJ at［8］－［11］.

る福音書によれば，若者を堕落させる者をキリストが次のように非難したという。

『わたしを信じるこの小さい者たちのひとりをつまずかせる者がいるとしたら，大きなひきうすを首にかけられて海の深くに沈められるほうがその者にとって益である。（18章６節）（マルコ伝９章42節，ルカ伝17章２節をみよ）』

わたしには，これが，本件のような違法行為と違法行為者に対するコミュニティの態度を映し出しているように思われる。このような態度は，覆面捜査によって，本当の少年を危険にさらさずに違法行為を発見することを支持するであろう。」[21]

多くの国で法執行機関による覆面捜査の利用を規律する法が定められているが，オンライン上での適用に関する具体的な規定を置くのは数少ない。サイバー犯罪捜査のガヴァナンスの一環として，警察と裁判所の双方に指針を示すことができるように議会で十分な検討がなされるのが望ましい。

結　　論

人間の行動は益々オンライン上にその場を映してきている。犯罪もその点で同様である。法執行の術と整えるべきガヴァナンスは，益々オンライ

21）R v. Stubbs［2009］ACTSC 63 (26 May 2009), per Higgins CJ at［69］－［70］. 別の事例，R v. Priest［2011］ACTSC 18 (11 February 2011) でも同様の結論に至っている。さらに，T Krone, “Queensland police stings in online chat rooms,” Trends and Issues in Crime and Criminal Justice no. 301 (July 2005), Australian Institute of Criminology; G Urbas, “Protecting Children From Online Predators: The Use of Covert Investigation Techniques by Law Enforcement” (2010) 26 (4) Journal of Contemporary Criminal Justice 410参照。

ンを想定したものが求められている。サイバー犯罪並びにそれよりも伝統的な犯罪で，電磁的証拠は今や，日常的に取得，分析され，法廷に提出されている。現在の規制権限とメカニズムは大きな変更をせずにオンライン上に移すことができる場合があるが，権限並びにメカニズムの明確化とより良い指針が必要な場合が多い。例えば，捜索押収法は，捜索場所や他の場所でコンピュータとデータについてフォレンジック分析を加えることを認めるように改正されているが，蔵置会話並びにトラフィック・データについては，そのアクセスのための別の令状が新たに用意されている。このような変化とともに，データ保全の要件並びに，通信サーヴィス・プロヴァイダーが負う法執行への他の協力義務がよりはっきりとしたものになってきている。これにより，そのような協力が任意のもので法の規律を受けないというのではなく，予見可能性がある一群のルールにしたがって，裁判所の審査権限が及ぶところで求められることがはっきりしている。これは刑事法システムと産業部門双方にとって有用である。

クラウド・サーヴィスのプロヴァイダーからの情報入手などのような問題に対処するにはさらなる発展が必要である。ここでは，データが分散して蔵置され，法域を超える場合がある。これは，国境を越えた捜索と，データに対する合法なアクセス並びに制御権原者の発見という課題を突き付けている。個人情報を保有する民間部門が中に入ったグッド・ガヴァナンスが決定的に重要である。法執行機関による，オンライン上の覆面捜査の利用と，それで入手した証拠の許容性は，また別の興味深いテーマである。その点で，「インターネット上では，だれもあなたが警官であることを知らない」ということを忘れないほうが賢明である。そのことは，捜査官と被疑者にも当てはまる。

法とテクノロジーの相互作用は常に変転している。しかし，サイバー犯罪条約のような国際社会での同意が広がり，国内法が詳細なものになっていけば，我われの前途はより明るく，すべての者にとってより安全なものになるだろう。