

第6章

第178回国際研修

「サイバー犯罪－電子証拠が問題となるあらゆる形態の犯罪」

本章の掲載資料は、UNAFEI's Resource Material Series No. 114に掲載されている論文のうち以下の論文を翻訳したものである。

- Cybercrime and Digital Evidence: The Nigeria Police Force in Perspective
by Mr. Olusoji Abraham Obideyi (Nigeria)

サイバー犯罪と電子証拠：ナイジェリア警察の展望

オルソジ・アブラハム・オビデイ*

1 はじめに

サイバー犯罪とは、サイバー空間に接続するコンピュータ、デジタル機器及びネットワークシステムに対する様々な形態の攻撃を指す。一方、サイバー空間は、安全保障を含む、保健、運輸、金融、エネルギー、農業、食品加工等の重要なインフラ部門の効果的な運営と稼働に不可欠なデジタルネットワークの相互作用的な領域である。サイバー犯罪は、刑事司法制度が存在しているにもかかわらず、ナイジェリアにおいて、また世界中で著しく大きな課題となっている。社会におけるサイバー犯罪の逮捕及び訴追を成功させるためには、電子証拠を発見し、保全し、収集し、分析し、活用するための専門的アプローチが極めて重要である。

サイバー犯罪は、法律に違反する行為であり、情報通信技術（ICT）を不正使用して犯罪を助長したり、ネットワーク、システム、データ、ウェブサイト及び／又はテクノロジーを攻撃したりする。欧州刑事警察機構（Europol）はサイバー犯罪をサイバー依存犯罪（cyber-dependent crimes）とサイバー利用犯罪（cyber-enabled crimes）に区別している。これらのサイバー犯罪カテゴリーの主な違いは、犯行におけるICTの役割である。ICT機器が犯行の標的である場合、サイバー犯罪は、コンピュータデータ又はシステムの機密性、完全性、及び／又は可用性に悪影響を及ぼす¹。

ナイジェリアにある国際刑事警察機構（INTERPOL）などのナイジェリア国内の警察組織はナイジェリア国内のサイバー犯罪の動向データを定期的に作成している。これらの犯罪測定ツールや被害調査は、収集・分析されるサイバー犯罪データの種類や、当該データの収集・分析に使用される方法によって異なるものとなる。

世界中のセキュリティ、ビジネスリスク及び／又は脅威の分析に重点を置いているサイバーセキュリティ企業やその他の民間組織は、過去のサイバーセキュリティ事件とその種類、頻度、影響に基づいて、サイバー犯罪及び／又はサイバーセキュリティの傾向に関するレポートを発行している。モノのインターネット（IoT）、ドローン、ロボット、自動運転車などの新しいテクノロジーの登場に伴い、サイバー犯罪の新しい傾向が出現することは間違いない。

* ナイジェリア警察庁警察監査事務局監査官

¹ <https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html>

(1) ナイジェリアにおけるサイバー犯罪のカテゴリー

世界的にサイバー犯罪には多様な分類が存在しており、例えば、Maitanmi et al (2013) は、サイバー犯罪を以下の三つの主要なカテゴリーに分類している。標的サイバー犯罪（コンピュータが標的とされる）、ツールサイバー犯罪（コンピュータがサイバー犯罪のツールとされる）、及びコンピュータ付随犯罪（コンピュータの犯罪における役割が小さい）である²。しかし、最も一般的なサイバー犯罪の分類は、もちろん、本稿でも採用されているものであるが、以下の通りである。

- i. 人々（個人）に対するサイバー犯罪：これらは、個人、人格及び財産を標的とした活動であり、電子メールによる嫌がらせ、サイバーストーカー行為、わいせつ物の頒布、名誉毀損、コンピュータシステムに対する不正な制御又はアクセス、公然わいせつ、電子メールのなりすまし、詐欺、コンピュータ破壊行為、ウイルスの送信、ネットへの侵入、知的財産の犯罪、他人のID等をハッキングしてインターネットを使用する行為（internet time theft）を含む。
- ii. 資産に対するサイバー犯罪：これらは、ルータ、通信マスト及び基地局（又はBTS）、データベースシステム、企業のデジタル設備などのコンピュータ/デジタルインフラストラクチャーを標的とした活動である。これらの犯罪には、DDOS攻撃、ハッキング、ウイルス送信、サイバースクワッティング及びタイポスクワッティング、コンピュータ破壊、著作権侵害、知的財産権侵害などが含まれる。
- iii. 政府（政府、企業、会社、企業団体）に対するサイバー犯罪³：これには、ハッキング、機密情報へのアクセス、サイバー戦争、政府や企業に対するサイバーテロ、海賊版ソフトウェアの運用・使用、スパイ行為などが含まれる。

ナイジェリアは複数の多様な民族で構成されており、それ自体により、独自の困難な社会問題を抱えている。ビジネス界や市民社会からの何度かの緊急の要請を受けて、議員らは「2015年サイバー犯罪法（Cybercrime Act 2015）」を制定した。同法では、とりわけコンピュータや電子機器の使用及び不正使用に関連する法規が定められている。しかし、現在までのところ、同法が事案終結に役立った画期的な事例は確認されていない。これは、法執行機関やその他の利害関係者が裁判所で犯罪者を納得のいく形で起訴するために必要な専門知識の欠如と無関係ではないかもしれない。コンピュータ犯罪の判決を下すために、裁判手続は過去の判決に頼らざるを得ないことが何度もあった。これは2011年のナイジェリア証拠法の改正前の慣行であり、現在では

² https://www.researchgate.net/publication/327111080_Impact_of_Cyber_Crimes_on_Nigerian_Economy

³ 編集注：原文ではiiiとして項目立てられてはいないが、読みやすさの観点から分類のひとつに含めた。

改正法が電子証拠の許容性を規定している。Ajayi (2016) が指摘しているように、サイバー犯罪の脅威を阻止するための世界的な取組に対するあらゆる障害の中で、サイバー犯罪者の身元の謎めいた特性は今なお残っている⁴。

サイバー犯罪に関する法律がある場合であっても、当該現行法の規定が、サイバー犯罪者の違法行為を抑止するほど厳格ではないことに留意することは有益である⁵。また、かなりの数の法執行機関の職員が実際にはテクノロジーに関心を持っていない。中には、ウェブを閲覧する気さえない人もいる。残念ながら、サイバー犯罪者は、法律を遵守する技術専門家のスキルを超えていない場合であっても、同等の高度なレベルは持っている。

ナイジェリアのサイバー犯罪事件は、法執行機関によって行われた捜索や押収の間に収集された証拠書類を使用して、主にナイジェリア警察サイバー犯罪部門と経済金融犯罪委員会 (EFCC) によって起訴されていることは、確固たる事実である。ナイジェリアにおけるサイバー犯罪の証拠収集方法では、裁判所に提出されたときに、訴訟手続上証拠として許容されるため、犯罪に関わる被疑者が証拠と明確かつ肯定的に結び付いていることを明らかにするべく、収集手続から保全までの電子証拠の取得過程において、全ての選択肢を適切に調査する必要がある。

2 サイバー犯罪とグローバル化のナイジェリアへの影響

サイバー犯罪は多くの点で諸国の国民経済に深刻な結果と損失をもたらした。それゆえ、世界中の政府がこの怪物を根絶するために真剣に戦っている。アメリカ、アジア、ヨーロッパ、アフリカを含む世界の多くの大陸の政府、個人、組織によって真剣かつ連携した取組がなされてきたが、ナイジェリアでの戦いは、サイバー犯罪の根本原因が解明されず、対処されていないため、連携されていないように見える。このため、政府による一連の努力にもかかわらず、犯罪は依然として急増しているようである。

(1) サイバー犯罪のナイジェリア経済への影響

- i. 資本逃避と外国からの投資の損失：ナイジェリアで蔓延しているサイバー犯罪のために、ナイジェリアへの信頼の欠如の結果、ナイジェリアに来るはずだった資本が他のアフリカ諸国に流れている。
- ii. 国のイメージと評判の悪さ：これはナイジェリア国とナイジェリア人に対する信頼の喪失をもたらす。外国人はハンセン病患者に対するようにナイジェリア人との取引を避けているため、外国からの直接投資の不足につながっている。また、多くの正当なナイジェリアのオンライン起業家は、他の国の国民とビジネスをする機会を拒否されている。

⁴ <https://academicjournals.org/journal/JIIS/article-full-text-pdf/930ADF960210>

⁵ 同上

- iii. 電子商取引コミュニティ又はプラットフォームについて、一定の国からの拒絶：これは、ナイジェリアの真に正当なビジネスマンにとって、最も目に見えて大きな課題の一つである。PayPal、eBay、MoneyGramsのようないくつかの電子商取引プラットフォームや電子決済プロバイダーは、ナイジェリアや、サイバー犯罪者にとって安全な避難所であることで悪名高い国に対して、決済ゲートウェイの使用を禁止している。
 - iv. 特にナイジェリア国内でのサイバー犯罪者の活動による銀行、個人、政府機関の収入の損失。これはシステムへの信頼を破壊し、オンライン取引に関係する人々に不必要な恐怖をもたらす。
- (2) サイバー犯罪捜査の課題

深刻なサイバー犯罪の報告が増加しているため、それに応じて有罪判決の割合が増加することを予想するかもしれない。しかし、多くの捜査と起訴が軌道に乗らなかったため、これは事実ではない。この結果の主な原因は、管轄権を越える障壁、ごまかし、刑事司法制度の主要な利害関係者がテクノロジーを用いた犯罪の基本的な側面を把握できないことにあると考えられる⁶。

サイバー犯罪は、長年ナイジェリア政府の議題になっている。特に詐欺関連のサイバー犯罪の調査は、ナイジェリア警察サイバー犯罪部門、経済金融犯罪委員会（EFCC）によって行われてきている。ナイジェリア連邦政府は、「2015年サイバー犯罪（禁止、防止等）法」（The Cybercrimes (Prohibition, Prevention, Etc) Act, 2015）として知られる国家サイバーセキュリティ政策と戦略を採用した。

サイバー犯罪者の訴追に使われている法律と2015年のサイバー犯罪法の執行手続との間のギャップは、提出された証拠に瑕疵があり、事件の訴追の成功のためにその証拠価値が決定的ではないと判明した場合、弁護人によってしばしば悪用される。サイバー犯罪者が逮捕されると、彼らは非常に高い弁護士費用を請求する有名な私立弁護士に自由にアクセスする。弁護士費用はサイバー犯罪者にとって問題ではない。サイバー犯罪を専門とする最高の弁護士に高い顧問料を楽に支払う余裕があるからである。

同様に、訴訟手続における電子証拠の提示ももう一つの重要な問題である。弁護士や裁判官の技術的知識が限られている可能性があるため、電子証拠の提示は、明確で理解しやすい方法で行われなければならない。ほとんどの法律専門家は技術についての理解が限られており、法廷で認められる証拠を提出する技術専門家の能力に自信を持ってない傾向があることが指摘されている。裁判官は、そのような証拠の価値を公正に評価するために、電子証拠が導き出される基礎となる技術とアプリケーションにつ

⁶ Brown, C.S.D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology* 9(1), doi: 10.5281/zenodo.22387 (サイバー犯罪の捜査と訴追：鑑識への依存と司法への障壁)

いてある程度の理解を持つべきである⁷。

言及すべき、もう一つの重要な課題として、ベストプラクティス、デジタル鑑識ツールのテスト、及び専門家の証言に関する問題が挙げられる。多くのデジタル鑑識技術が捜査員や調査員によって使用されている。ただし、現時点ではベストプラクティスガイドが用意されていない。

サイバー空間を規制する法令は、各国のサイバー犯罪者を追跡する上で必要な司法管轄上の困難さや追加的な資源の必要性のために、ほとんど訴追に至らない傾向がある。ナイジェリア国内の現在のサイバー犯罪に関する法律は、先進国の基準を満たすように見直される必要がある。ナイジェリアは、かつては鑑識能力の弱さが大きな課題となっていたが、現在は、西アフリカ全体で初めてと言われる、国営の高性能DNA鑑識研究センターを保有している。それは、ラゴス国家DNA法科学センター (Lagos State DNA Forensic Centre=LSDFC) として知られており、英国政府が設立したEFCCのデジタル科学捜査研究所 (Digital Forensic Lab) に加えて設立されたものである。

3 推奨事項

この主題に関する前述の様々な概念を検討した上で、ナイジェリアにおいて、既に悪化しているサイバー犯罪の状況を改善するためのいくつかの提案を以下に示すこととする。

- a) **協力、啓発活動**：適切な法的枠組の存在のみでは、サイバー犯罪のような犯罪と戦うには十分ではない。法的枠組の実務に基づく効果的な実行もまた重要である。これは、とりわけ捜査機関とデジタル鑑識研究所の協力によって達成することができる（例えば、電子証拠の保全及び収集の手順に関する情報の共有、分析結果を迅速に入手するための協力等）。
- b) **コンピュータ技術カリキュラム**：ほとんどの警察関係者は必要な技術的知識を持っていないが、インターネット犯罪者はコンピュータ技術の専門家である。これらの犯罪に対処するためには、最も信頼できる戦略の一つとして人材の教育・育成が必要である。さらに、大学、高等教育機関、学術機関は、裁判官、検察官、弁護士の将来世代がこの極めて重要な分野において研修を受けられるように考案された特別コースを開設すべきである。
- c) **関係者向けの能力開発プログラム**：サイバー攻撃に対する法執行当局の運用能力と対応の改善が必要である。そのためには、サイバー犯罪の捜査・訴追の分野の専門家を増やす必要がある。これは、専門的な研修を頻繁に実施し、関係職員を

⁷ Kessler, G. C. (2011). Judges' awareness, understanding, and application of digital evidence. *Journal of Digital Forensics, Security and Law*, 6(1). <http://commons.erau.edu/db-security-studies/25>から取得（電子証拠に対する裁判官の認識、理解、及び適用）

海外に派遣して専門的な研修を受けさせることで可能となる。サイバー犯罪の分野におけるエキスパートの専門化、この分野における国内法令及び国際法令に関する知識の向上、及びこれらの法令を最も適切かつ効果的なやり方で実施するための方法及び手段は、これらの研修を通じて達成することができる。

- d) **鑑識専門家資格**：鑑識専門家報告書の審査官は、鑑識専門家の能力を精査して、無資格の鑑識専門家が、欠陥のある、又は信頼できない報告書を作成するという不幸なシナリオを避けるべきである。デジタル鑑識専門家の能力を評価するための統一された基準は存在しないが、審査官は、現在の事例を考慮して、認証、教育、実務経験の最適な組み合わせを検討すべきである。
- e) **個人、公的及び民間部門の組織が報告する経路を確立すること**：当該報告は、法執行機関による捜査の引き金となり、サイバー犯罪の範囲、脅威、動向をよりよく理解するための情報を提供し、組織的犯罪のパターンを検出するためのデータ照合を可能にすることができる。

4 結論

サイバー犯罪捜査は、司法関係者だけでなく法執行機関の職員の知識不足やスキル不足によって妨げられているという幅広いコンセンサスがある。本稿は、ナイジェリアにおけるサイバー犯罪の傾向に焦点を当て、サイバー犯罪とグローバリゼーションが国の経済に及ぼす影響、サイバー犯罪とその他の関連犯罪への刑事司法対応において当事者が直面する課題を列挙している。最後に、ナイジェリアの立法者、捜査官、検察官の間に存在する溝を埋める方法について議論し、サイバー犯罪の脅威という危機に対処するための提言を行った。

確かに、刑事裁判や民事裁判で電子証拠の量と重要性が増大するにつれ、裁判官は提供された証拠の価値を公平かつ正当に評価する必要がある。そうするためには、電子証拠を導き出すための基礎となる技術とアプリケーションについての一般的な理解が裁判官には必要である。利害関係者のニーズに協調的、補完的かつ持続可能な方法で応じるためには、主要な利害関係者（すなわち、立法者や法執行機関の職員）の間で意識が醸成されなければならない。

