「現代のサイバーセキュリティの法的課題についての国際的な研究」に関する調査報告書

－　情報セキュリティサービス提供者と法執行機関・監督官庁などとの協力－

株式会社 IT リサーチ・アート

はじめに

本報告書は、情報セキュリティサービス提供者と法執行機関・監督官庁などとの協力脅威インテリジェンスサービスの利用における注意すべき法令上の問題について調査をなした報告書です。

具体的な協力状況については、マイケル・ステイン氏(AMETOS 社)、John Kirch 氏(Uppsala Security 社）にインタビュー等に協力いただきました。

なお、本報告は、経済産業省委託調査「令和２年度サイバー・フィジカル・セキュリティ対策促進事業（サプライチェーン・セキュリティ対策に関する調査)」(委託先　株式会社三菱総合研究所）において作成した「現代のサイバーセキュリティの法的課題についての国際的な研究に関する調査報告書」(株式会社 IT リサーチ・アート）を元に作成しました。

令和３年８月５日

株式会社ＩＴリサーチ・アート
代表取締役弁護士　高橋郁夫

（調査分担）
西貝吉晃　（千葉大学　准教授）
有本真由（弁護士）

内容

情報セキュリティサービス提供者と法執行機関・監督官庁などとの協力.....4
1　意義.....4
2　法執行機関・監督官庁などとの協力.....4
3　世界における協力状況と法.....5
3.1　米国.....5
NCFTA（国家サイバーフォレッジックス・トレーニング・アライアンス）.....5
金融セクタ ISAC（FS-ISAC）.....6
ボットネットテイクダウン等における協力（マイクロソフト）.....6
民間会社に対する調査権限の委託.....7

3.2　欧州.....7
欧州サイバー犯罪センター（European Cybercrime Center）.....7
3.3　イギリス.....7
シンクホール手法等における協力.....7
捜査権限法における捜査技術の拡充と技術者によるコントロール.....8
3.4　ドイツ.....8
ボットネットのテイクダウン.....8
研究者のボットネットの報告義務.....9
3.5　韓国.....9
マイケル・ステイン氏インタビュー録.....10

情報セキュリティサービス提供者と法執行機関・監督官庁などとの協力

1　意義

法執行機関・官公庁が果たすべき役割を民間のサイバーセキュリティ会社・脅威インテリジェンス会社が協力することがよく行われているということがいわれる[1]。これは、サイバー犯罪の調査に関していえば、法執行機関は、人的スタッフにも予算にも限りがあるからである。また、特に攻撃者側の手法や状況等についての知識は、サイバー犯罪の状況を明らかにして、将来の攻撃を抑止する効果もあるとされる。また、サイバーセキュリティ会社・脅威インテリジェンス会社にとっても、その専門的な知識を社会の秩序の維持に役立たせることができれば、それは、その企業の社会的な責任を果たすという見地からも望ましいものということができる。

このような問題意識から、本章においては、世界で実際に行われているサイバーセキュリティ会社・脅威インテリジェンス会社のサイバー犯罪対応等に対する協力を明らかにしようと努めるものである。

具体的な協力の態様としては、民間において自らがサイバーセキュリティ会社等に依頼して、その依頼の結果を法執行機関等に提供する場合と、法執行機関が自らの業務を行うのに際して、サイバーセキュリティ会社等に協力を求める場合とがある。これらの場合について、世界における具体的な状況を明らかにするものである。なお、当該調査については、現時点において、我が国でも一般的なものとして認識されていると考えられるデジタルフォレンジックス・機器の調査・通信傍受への協力の例は除くものとする。「犯罪捜査のプレゼンスに民間企業の知見を取り入れる必要」に限って調査するということになる。また、児童ポルノ等の発見、通報等を民間によっていわばアウトソースするという点についても、本調査の対象とはしない。

2　法執行機関・監督官庁などとの協力

具体的なサイバー犯罪対応のための法執行機関と民間企業の協力という観点から、脅威アナリストは、捜査官のために刑事事件を立証するためのサポートと十分に開発されたリードを消化しやすくするためには、まず範囲と被害を明確にすること、攻撃者との結びつきと問題となる法域を明らかにすること、業務と連絡の一元化をすること、人的なネットワーキングの重要性を認識すること、法執行機関の人員も事件に関するフィードバックや最新情報を提供することで、情報のループを閉じること、が推奨されている。これは、民間の脅威アナリストとの法執行機関との連携が、実際に頻繁におこなわれていること、そして、き

[1] Levi Gundert, ”5 steps for a successful public-private cyber crime fighting partnership”（https://gcn.com/articles/2019/02/28/cyber-crime-fighting-partnership.aspx）

わめて重要であることを物語っている[2]。

また、国連においても、その関心から、「誰が、サイバー犯罪の捜査を指揮するのか？」という報告がなされている[3]。そこでは、もっぱら、サイバー犯罪に対する証拠の収集という観点から、種々の捜査主体があげられている。刑事司法機関、国家安全保障機関、民間企業、官民連携とタスクフォースに分けてそれぞれ検討されている。民間企業に関していえば、特に重要インフラを運営している企業においては、それ自体が、サイバー犯罪の探知、防止、緩和、捜査に関して重要な役割をはたす。重要インフラは、民間企業によって保有、運営されているために、サイバー犯罪者の標的となりうるので、サイバー犯罪／犯罪者をプロアクティブに特定し、サイバー犯罪を防止し、緩和し、対応することができるようにセキュリティ措置を展開することが良いとされている。また、官民パートナーシップについても注目がなされており、米国における NCFTA、日本における JC3、欧州における 2 Centre が紹介されている。

特に、脅威インテリジェンスを法執行機関が利用することについては、サイバー捜査における官民協力のための新しいモデルが、執行活動を可能にするための民間部門の重要性がよりよく理解されている特定の法域で出現しており、成功しているものがいくつかあるとして[4]、全米サイバーフォレンジック・トレーニング・アライアンス（NCFTA、以下、NCFTA という）、ユーロポールの EC3 諮問グループ、金融セクタ ISAC（FS-ISAC）、マイクロソフトのデジタル犯罪対策本部などが紹介されている。これらについては、以下において、具体的に検討する。

3　世界における協力状況と法

3.1　米国

NCFTA（国家サイバーフォレッジックス・トレーニング・アライアンス）

NCFTA は、2002 年に民間、政府、学会からなるサイバー犯罪を特定、緩和、根絶するために相互協力を可能にする中立的で、信頼しうる環境を構築する目的のために、創立された。2015 年から 2019 年までの間に、2517 件を法執行機関に連絡し、1096 人が逮捕されていると報告されている。NCFTA は、ブランド・消費者保護（BCP）、サイバー金融（CyFin）、マルウェア及びサイバー脅威（MCT）の三つのプログラムを有している。ブランド・消費者保護（BCP）は、偽造品対策・偽医薬品・小売業の保護の分野に注力している。サイバー金融

---

[2] 上記 Gundert 論文。

[3] UNODC　”Who conducts cybercrime investigations?”（https://www.unodc.org/e4j/en/cybercrime/module-5/key-issues/who-conducts-cybercrime-investigations.html）

[4] Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime（https://www.thirdway.org/report/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime）

（CyFin）は、金融業に対するサイバー脅威対応に注力している。マルウェア及びサイバー脅威（MCT）は、ダークウェブの傾向に対応するものである。マルウェアのサンプルを分析し、攻撃のインディケータの情報共有の起点となっている。

金融セクタ ISAC（FS-ISAC）[5]

FS-ISAC は、インテリジェンス・プラットフォーム、回復力のあるリソース、信頼できるピアツーピアの専門家ネットワークを活用して、金融機関、ひいてはその顧客にサイバー脅威の予測、緩和、対応のサービスを提供する金融サービスに特化した唯一のグローバルなサイバーインテリジェンス共有コミュニティである。もともとは、1998 年の米国大統領指令に対応して発足したもので、米国の重要インフラを保護するために、官民が物理的・サイバーセキュリティの脅威と脆弱性に関する情報を共有することを義務づけている。その後、2013 年以降、よりグローバルなアプローチをとるようになっている。

その活動は、インテリジェンス、レジリエンス、トラストの三つの分野に分かれている。インテリジェンスの分野においては、種々の分析やピアツーピアの情報共有がなされている。レジリエンスの分野においては、演習、ベストプラクティス、教育・トレーニングプログラム、危機対応などがある。トラストの分野においては、イベント・コミュニティ活動・セミナーなどがある。

ボットネットテイクダウン等における協力（マイクロソフト）

マイクロソフトのデジタル犯罪対策部門（(Digital Crimes Unit、DCU）は、お客様を保護し、マイクロソフトの信頼を促進するために、技術の革新的な応用、フォレンジック、市民活動の革新的な応用をなし弁護士、調査員、データ科学者からなる国際的なチームであり、サイバー犯罪との戦いをリードしている[6]。マルウェアによってなされるサイバー犯罪や国家支援活動を特定し、調査し、撲滅する活動を行っている。2010 年から、22 のマルウェア活動を撲滅している。具体的な事件としては、Thallium(2019)、phosphorus(2019)、Gamure（Andromeda）（2018)、Citadel（2013)、Game over Zeus（2012)、Rustock（2011）などがある[7]。

また、国家支援活動に対する対抗策としては、Strontium（2016）に対する活動がある。これは、マイクロソフト社が、裁判所命令を取得し、マイクロソフト類似のドメインへの通信をシンクホールに誘導することが可能になった。また、Strontium によって新しく登録されるドメインに対抗するためにスペシャルマスターを指名してもらい，それらの攻撃を防止

[5] https://www.fsisac.com/
[6] https://3er1viui9wo30pkxh1v2nh4w-wpengine.netdna-ssl.com/wp-content/uploads/prod/sites/358/2018/12/DCUOverview.pdf
[7] 具体的な事件については、佐々木勇人「民事手続きを活用した攻撃インフラのテイクダウンに向けて」参照
(https://www.janog.gr.jp/meeting/janog45/application/files/1815/7962/2373/janog45-domain-sasaki-01.pdf)。

した。

国際 BEC（電子メール詐欺）に対して、戦略執行チーム（GSET）が、対抗している。また、技術サポート詐欺に対してデータ分析・機械学習をも活用して対抗している。

民間会社に対する調査権限の委託[8]

実際の捜査に関して、FBI と民間の調査会社が契約に基づいて、調査を支援することがある。実際に、そのような支援に従事しているアメトス社[9]へのインタビューによると、協力をする際には、必ず着手前に事前に基本合意書を交わす。事案によっては特別の覚書を交わすこともある。FBI の場合は FBI から提示してきた合意書にサインをするか、しないかの二択のみで、契約書の条項について交渉の余地はない。イスラエル政府に協力する場合は、信頼関係が構築されているため、支払事項、実施事項のみの簡易な合意書を交わしているという。

また、そのようなセキュリティサービス提供会社は、クライアントからの依頼に基づいて証拠を収集し、法執行機関に対して法の適用を求める支援をもしている。この場合、クライアントのシステムに脆弱性が発見されたり、インシデントが発生したりした場合、クライアントが同意しない限りは当局に報告できない。政府に報告するかはインシデントの種類にも依存し、犯人が（元）従業員であれば内部的に処理するし、テロ関連であれば当局に報告することも検討するが、いずれにしても最終的にはクライアントの判断によるという。

3.2 欧州

欧州サイバー犯罪センター（European Cybercrime Center）

欧州警察機構（Europol）は EU におけるサイバー犯罪への法執行の対応を強化し、欧州市民、企業、政府をオンライン犯罪から守ることを目的として 2013 年に欧州サイバー犯罪センター（EC3）を設立した。EC3 は、数十件の注目を集める作戦や数百件の現場での作戦支援活動に携わり、何百人もの逮捕者を出し、何十万ものファイルを分析してきている。

3.3 イギリス

シンクホール手法等における協力

英国において、法執行機関等と民間企業が、協力して積極的な調査手法を活用して、サイバーセキュリティ活動を行うことは、実際によく行われている。その場合に、そのような活動と法執行機関等との関係は、具体的な活動との関係で定まる。一般的な情報提供に関して

---

[8] AMETOS 社及びインタビュー内容については、Michael 氏インタビュー録を参照。

[9] AMETOS 社は、イスラエルのセキュリティ会社であるが、イスラエル政府の他に、米国の政府機関（FBI、FCC）やインターポール、南アフリカ、IATA（国際航空運送協会）などの依頼を受けて調査等に協力している。

は、法執行機関・会社・大学などは、情報についての要求者として、リサーチャーとは、情報提供契約を締結して、その情報の取得についての合法性を担保させようとする。具体的な手法として、シンクホールを用いて調査をなすという手法については、英国においては、セキュリティ会社の通常の調査手法であって一般的である。攻撃者、ターゲットのセクタ、被害者になっている者の情報を得ることができることから非常に豊富なインテリジェンスが得られる手法であると考えられている。トラフィック情報については、大変な機密情報を含んでいるということではないし、より、マルウェアが、何をもとめたのか、次のコマンドは何か、という情報になる。トラフィックは、100 パーセント被害にあった企業の情報ということになる。セキュリティ会社は、実際に、シンクホールを運用しているし、それは、会社からも法執行機関からも感謝されている。このような運用に際して、法執行機関との協力もなされている。一方、英国において、それ以外の手法、一般の民間のセキュリティ会社が、ボットネットの中立化に自ら協力するなどの手法をとることは、特にないとのことであった。

捜査権限法における捜査技術の拡充と技術者によるコントロール

英国における通信に関するデータの合法的アクセスの法的な規制に関する主な制定法は、シギント（通信、電磁波、信号等に対する傍受等を利用した諜報）活動について定める 2016 年調査権限法 （Investigatory Powers Act 2016）(IPA2016 という） である。同法は、合法的（特定）通信傍受、通信データの取得許可、（特定）機器干渉（Equipment Interference)、一括令状（1 章：一括傍受令状、2 章：一括取得令状、3 章：一括機器干渉令状)、一括・パーソナル・データセット令状などの調査権限を定めている。これらの権限について、適切に行われるように技術助言委員会（Technical Advisory Board）(245 条)、技術助言パネル (246 条) が設けられている。

3.4 ドイツ[10]

ドイツにおいては、ISP とボットネットの切断、研究者のボットネットの報告義務において、民間と法執行機関との協力が議論されている。

ボットネットのテイクダウン

ボットネットが検知された場合、警察（連邦レベルのケースになりやすいとはいえ、主な管轄は州警察（the regional Länder Police）にある）は、公衆の安全への危険がある場合、又は生命若しくは身体的な完全性への脅威がある場合には、C&C サーバをテイクダウンする

[10] 基本的に以下の記述は、Liis Vihul, Christian Czosseck, Dr. Katharina Ziolkowski, Lauri Aasmann, Ivo A. Ivanov, Dr. Sebastian Brüggemann, M.A., “Legal Implications of Countering Botnets”, Joint report from the NATO Cooperative Cyber Defence Centre of Excellence and the European Network and Information Security Agency (ENISA)（https://ccdcoe.org/library/publications/legal-implications-of-countering-botnets/）におうところがほとんどである。

ために、適切な法執行命令（捜索令状(Nordrhein-Westfalen (NRW)州警察法（以下「州警察法」という）41 条、42 条[11]))やサーバの没収命令（州警察法 43 条、44 条）に基づいて行動できる。さらに、C&C サーバのテイクダウンは、問題となっているそのボットネットによる攻撃が公衆の安全の危殆化又は公序の侵害を構成するものである場合には、州警察法 1 条の一般条項により正当化され得る。このような場合、当該警察は、C&C サーバをホストしているボットマスター、ISP、同様に感染しているそれぞれのコンピュータの個別の所有者に対して、問題ある行動を止めるように要請することができる。ただし、後者はあまり意味がなく、それゆえほとんど行われていない。

管理しているネットワーク内に C&C サーバがある場合、ISP は、同サーバを切断し、ドイツ民法 314 条に基づいて契約を終了させることさえできる。実際には、C&C サーバをテイクダウンする ISP の権利は、規約に書くことが出来るし、今日では既に、インターネットサービスの多くはそうなっている。

研究者のボットネットの報告義務

なお、研究者の行為規範に関して、ボットネットを見つけた際にそれを報告する義務があるかどうかが問題となる。ドイツ刑法 138 条は犯罪の報告義務違反罪を規定している。もっとも、これは、ボットネットについての知識を有しているだけの者には適用されない。しかし、ドイツ刑法 138 条にあげられている犯罪がボットネットの利用によって行われていることを知っている場合には、報告義務違反罪に該当しうる[12]。

3.5 韓国

韓国において、仮想通貨（暗号資産）のブロックチェーン上の取引を追跡し、分析するサービスが提供されており、その報告をもとに法執行機関に被害届出をなすことがおこなわれている。インタビューに対応いただいた Uppsala Security 社によると現在までに同社により 129 件の報告書が提出されており、暗号資産をめぐる犯罪の捜査に貢献している[13]。うち、2 件については、容疑者が逮捕されている。

---

[11] https://recht.nrw.de/lmi/owa/br_text_anzeigen?v_id=3120071121100036031 https://www.gesetze-im-internet.de/bgsg_1994/BJNR297900994.html (2021 年 3 月 5 日最終確認)

[12] ドイツ法上、ボットネットの構築や運用それ自体が犯罪に当たるかどうかが立法論的に議論されていることに注意されたい(BT-Drs. 19/1716)。ボットネットをいわば法的に攻撃するアプローチだといえよう。そこでは、現状、ボットネットの構築から運用のそれぞれのプロセスにおいて、一つずつ行為を検討してみると、既存のサイバー犯罪対策規定(ドイツ刑法 202 条 a,b,c、303 条 a,b)のみを利用するのでは処罰の欠缺があるとし、新たにドイツ刑法 202 条 e が提案されていた。もっとも、ボットネットを包括的に処罰し得る本罪は、軽微な事案をも同時に補足してしまうとして批判が強く(詳しくは西貝吉晃「ドイツにおける新たな無権限アクセス罪の立法論」情報法制研究 6 号 36 頁以下参照)、未だ立法にも至っていない点に注意が必要である。

[13] John Kirch 氏（Uppsala Security）からの教示による。

マイケル・ステイン氏インタビュー録

日時：2021 年 3 月 17 日午後 5 時から午後 5 時 45 分（日本時間）
場所：zoom インタビュー
参加者：　AMETOS 社：ミハエル・ステイン（Michael）氏、原倫太郎氏
　　日本側：高橋郁夫弁護士、有本真由弁護士（東京）

１．　Michael 氏の地位

AMETOS 社[14]アジアパシフィックの長

２．　Michael 氏の回答内容

- サイバー犯罪捜査において政府と ISP が協力することについて（情報共有の重要性）
  - 情報共有が非常に重要である。
  - イスラエルにおいては、関係者が一堂に会する形での情報共有がなされるようになってきている。その方法だと情報共有から決断までが速やかに行われるため有益である。
  - 例えば、児童の保護（誘拐など）の関係では、警察関係者、教育大臣、社会福祉従事者、心理学者などが参加する会議がある。
  - その他に、シークレットサービス、警察、軍の幹部が一堂に会する会議もあり、関係論点について各省庁が把握し、即座に決定を下すようになっている。
  - サイバーセキュリティ分野では首相をトップとする Israel National Cyber Directorate (INCD)[15]がある。警察、軍、民間企業（インフラ企業、サイバーセキュリティサービス事業者）などが会する。脅威情報がある場合には特定の企業に警告を出すことができる。それによって企業は迅速に対応できる。そこでは、オンラインでの即時の情報共有が可能となっている。
  - 例えば、イランがイスラエルの水道に毒を盛ろうとするという未遂事件があった。

[14] AMETOS グループは、セキュリティ及び戦略サービスを提供する高度なプロフェッショナル集団であり、イスラエルを本拠とする。銀行等に部外者が侵入できるかという物理的なペネトレーションテストを実施して当該組織の脆弱性を見出すといった特徴的なサービスを提供する AMETOS REDTEAM という部署を有する。サイバー分野を担当するのが AMETOS IT & CYBERSECURITY であり、ペネトレーションテスト、サイバーインテリジェンス、ダークウェブ分析、マルウェア分析、モバイルセキュリティ等を提供している。https://ametosgroup.com/

[15] イスラエル国家サイバー理事会（INCD）は、首相官邸直轄の組織であり、同じく官邸直轄であった国家サイバーセキュリティ局（National Cyber Security Authority; NCSA）とイスラエル国家サイバー事務局（Israeli National Cyber Bureau）が統合してできた組織である。イスラエルの国家サイバー空間を防護し、イスラエルのサイバー能力を高めることを使命とし、その一環として重要インフラや民間企業にインシデントハンドリングの支援及びガイダンスを提供している。https://www.gov.il/en/departments/about/newabout

National Cyber Security Authority が事前に把握し、事態を防いだ[16]。

- 民間企業との協力のメリット
  - 民間企業は金銭で動き、競争原理が働くため、最良のサービスを提供する。最良の人材、最良のデバイスを有している。政府が ISP と提携すれば民間のリソースを利用でき、より良い結果を獲得できる。

- 政府機関との協力
  - 米国（FBI、FCC）やインターポール、南アフリカ、IATA（国際航空運送協会）などに協力している。
  - 誘拐や金銭詐欺（デジタル通貨を含む）など。
  - 具体的な内容はなかなかオンラインでは話せないが、イスラエル政府を介したウクライナ警察からの依頼でボットネットのテイクダウンとその実行者の逮捕に協力したことがある。
  - 政府機関と協力する場合には事前に基本合意書を交わす。事案によっては特別の覚書を交わすこともある。FBI の場合は FBI から提示してきた合意書にサインをするか、しないかの二択のみで交渉の余地はない。イスラエル政府に協力する場合は支払事項、実施事項以外は合意書を交わしていない。弊社はイスラエルの会社なので信頼関係が既に構築されているということだろう。イスラエル政府との場合は合意書を作成するのはイスラエル政府と弊社とどちらの場合もある。

- クライアントの脆弱性・インシデントの当局への報告
  - クライアントとのやりとりやインシデントはすべて書面化又は録画している。
  - クライアントが同意しない限りは当局に報告できない。クライアントはインシデントが公にならない限りは報告したがらない。
  - インシデントの種類にもよる。犯人が（元）従業員であれば内部的に処理するし、テロ関連であれば当局に報告することも勘案する。いずれにしてもクライアントの判断による。
  - 当局に報告した後は当局に委ねる。当局が要請すればフォレンジックなどを支援する。フォレンジックは主に犯人を特定するためだが、時には政府は犯人特定を望ま

[16] 2020 年 5 月ころに起こった事件。政府関係者は公式には認めていないが英 Financial Times に匿名でのリークがあり判明。イランが、居住区に水を供給するイスラエルの水道施設にサイバー攻撃をしかけ、塩素レベルを上げようとしたというもの。その他の化学物質も混合させる意図があったとも言われる。実現した場合、数 100 人が病気になる可能性があり、逆に、施設の安全装置が機能すれば、酷暑の中で配管が閉鎖され数日にわたり水が供給できない状況に陥っていた可能性もある。攻撃は当初想定されたより高度で間一髪のところで食い止められたとされるが、なぜ攻撃が成功しなかったかの原因は不明とされている。同年 7 月にもイランがイスラエルの農業供水施設にサイバー攻撃をしかけたというニュースもある。
https://www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

ない場合もある（犯人が特定されると報復を検討しなければならないため)。

以上