「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

－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の調査　－

株式会社 IT リサーチ・アート

はじめに

本報告書は、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。その前提として、脅威インテリジェンスサービスの概念を整理するとともに、インテリジェンスの取得方法をもまとめています。

特に、「４　米国司法省『オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項』の翻訳」においては、JNSA より提供された翻訳案にかなりの程度、依拠しています。

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３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

1　脅威インテリジェンスの概念

概念

脅威インテリジェンスという用語が注目を浴びている。わが国においても「脅威インテリジェンスの活用によって、従来のセキュリティ対策では見逃されていた高度なサイバー攻撃の検知、特定の業界・業種を標的とした巧妙なサイバー攻撃の防御が可能となります」などと注目を浴びているところである。

具体的な定義について、明確なものは、存在しないが、本報告においては、情報資産に対する脅威に関する情報セキュリティ目的のためのインテリジェンスもしくは、それを構成するデータとする。攻撃者の動機、標的、攻撃行動を理解するためのデータであり、セキュリティインシデントに関する情報交換のためのアプローチが対象とする情報もしくはその分析手法ということができる[1]。また、インテリジェンスとされるので、単なるデータや情報ではなく、それらを特定の目的に役立つように処理されることによって、関連し、行動に利用でき、価値のあるもの、である必要がある[2]。

脅威インテリジェンスは、各国の政策としても注目を引いているが、これは、2017 年の WannaCry と NotPetya の事件が政府の関心をひいたこと、2018 年 5 月には、欧州議会が、ロシア連邦と北朝鮮が国際法に違反していると非難したこと、国際的対応を呼びかけたこと、もし、政府と多国籍企業が情報を共有したら、これらのキャンペーンの戦略、程度、タイムスケールに対する理解が、向上すると考えられること、などがその要因であると考えられている。

分類

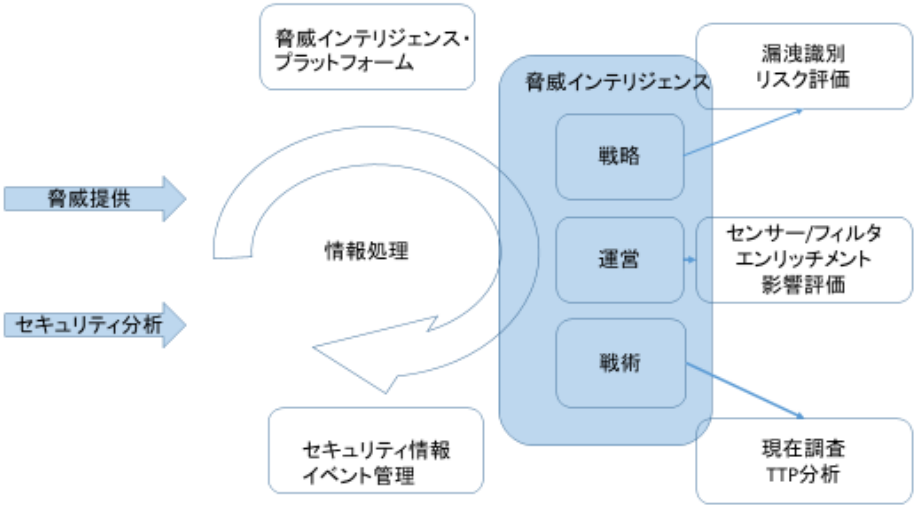
脅威インテリジェンスのプロセスは、以下の図を用いて説明することができる[3]。

---

[1] Friedman & Bouchard「サイバー脅威インテリジェンスの明確なガイド（Definitive Guide to Cyber Threat Intelligence）」は、「サイバー脅威インテリジェンスとは、敵対者やその動機、意図、方法に関する知識であり、企業の重要な資産を保護するために、あらゆるレベルのセキュリティやビジネスに役立つ方法で収集、分析、普及されている」と定義している（http://cyber-edge.com/wp-content/uploads/2016/08/Definitive-Guide-to-CTI.pdf）。その他、は、「脅威インテリジェンスとは、脅威行為者の動機、標的、攻撃行動を理解するために収集、処理、分析されるデータをいう」と定義している（https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/）。

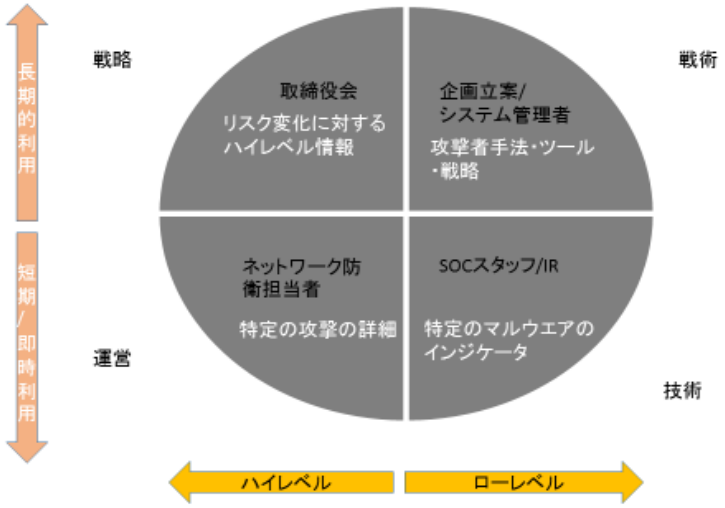
[2] この部分については「脅威インテリジェンス共有：現状及び要求事項（D5.1 Threat Intelligence Sharing: State of the　Art and Requirements」（https://protective-h2020.eu/wp-content/uploads/2017/07/PROTECTIVE-D5.1-E-0517-Threat-Intelligence-Sharing.pdf）による。

[3]「脅威インテリジェンス共有：現状及び要求事項」15 頁。

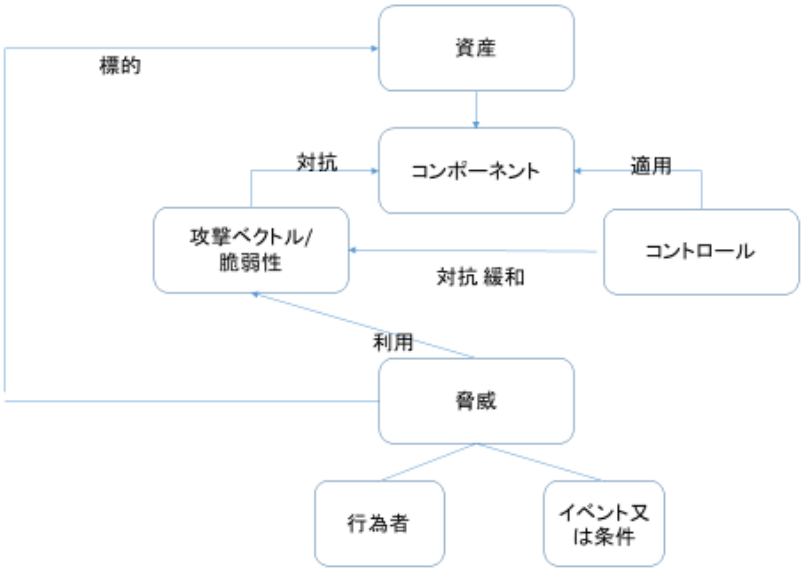


これは、サイバー脅威インテリジェンスが、戦術（脅威指標を用いて積極的に敵を探し出し、敵から防御するなどの技術的な情報。）、運用（敵対者の動機や意図、能力（TTP-Tactics, Techniques, and Procedures-戦術・技術・手順-を含む）に焦点を当てた情報）、戦略（ビジネス上の意思決定やサイバーセキュリティへの直接投資を通知するために使用される脅威に関連するリスクや意味合いについての情報）に分けられること、それらがプラットフォームの上で、イベント管理をもとに、情報の取り扱いのプロセスとしてなされることを物語っている。この戦術、運用、戦略のそれぞれのインテリジェンスの要求者と具体例については、以下の図で示すことができる[4]。

[4] D.Chismon ほか"Threat Intelligence:Collecting, Analysing, Evaluating"（ http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/gheyreboomi/BehtarinRaveshha/CPNI%20-%20Threat%20Intelligence%20-%20Collecting%20Analysing%20Evaluating.pdf）6 頁。



また、資産・脅威・コントロールの関係については、以下の図で示すこともできる[5]。



2　脅威インテリジェンスにおけるインテリジェンスの生成方法等

2.1　脅威インテリジェンスを構成するデータ

脅威インテリジェンスがどのようなデータを処理することによって得られるかという点

[5] Michael Muckin ほか「サイバーセキュリティに対する脅威によるアプローチ」(A Threat-Driven Approach to Cyber Security)(http://ce.sharif.edu/courses/95-96/2/ce746-1/resources/root/Resources/Lockheed%20Martin%20Threat-Driven%20Approach%20whitepaper.pdf)

についていえば、「サイバー脅威インテリジェンスの明確なガイド」は、レベル１（脅威インディケータ)、レベル２(脅威データフィード)、レベル３(戦略的脅威インテリジェンス)にわけて論じている。

レベル１（脅威インディケータ）とは、又は危殆化（compromise）の指標（IOC）は ある種の攻撃や危殆化の可能性を示すエンティティをいう。最も一般的なタイプは、ファイルハッシュ（署名)、攻撃に関連したドメインや IP アドレスの評判データである。技術的には、マルウェアの分析から得られるフィンガープリントが、代表的なものであるが、これは実際のマルウェア以外にもハニーポット、スキャナーから得ることができる。また、攻撃者のドメインや IP アドレスも、このような情報を形作る。実際の脅威インテリジェンスとして、このような情報が実際に提供されてもいる。

レベル２（脅威データフィード）は、脅威指標を分析し相関性のある情報をいう。これらは、セキュリティチームが攻撃に関連するパターンを特定するのに役立つし、また、インシデント対応 (IR) チームが悪意のあるソフトウェアファイルの挙動を理解するのに役立つマルウェア分析も含まれている。

レベル３の戦略的脅威インテリジェンスは、アンダーグラウンドのモニタリング等によって得られる標的企業に対する特定の敵の情報をいう。この情報は、敵の動機・意図・戦略・技術・プロセスに関するものである。この情報は、その取得方法がアンダーグランドのモニタリング等によって得られることから、特に検討すべき事項がある。

2.2　特に問題となる脅威インテリジェンスデータの取得方法

脅威インテリジェンスデータの取得方法として、問題点を引き起こしそうな取得方法について、例示しておく。具体的な手法としては、（１）仮想人格による HUMINT（２）ダークマッケット調査（３）ハニーポット（４）ビーコン（５）シンクホール（６）ハックバックなどがある。

（１）仮想人格による HUMINT

仮想人格による HUMINT（バーチャル HUMINT、脅威カウンター・インテリジェンス収集）とは、ネットワークにおける仮想人格を構築し、その仮想人格と通信する相手に関する情報を収集し、それをもとに、脅威の主体、ツール、技術を分析等することによってインテリジェンスを提供するプロセスである。仮想人格とは、現実には存在しない人格であり、実在の組織等との関連性を有せず、また、それを示唆しない人格であることをいう。実在の人格を偽って名乗る場合については、名誉毀損・業務妨害の問題が発生しうるが、架空の人格になりすますという場合には、そのような問題ではない。かかる仮想人格による情報取得の問題点について、①無権限アクセス／権限超過に関する問題②人格に関する問題③通信の傍受の問題④個人情報の領域外移転などの問題を考察することができる。

（２）ダークウェブ調査

ダークウェブ調査というのは、通常のアクセスではアクセスしえないネットワークにお

いて交換されている情報についての情報収集・分析行為をいう。当該ネットワークにアクセスするためには、通常のウェブブラウザではなく、Tor などのブラウザを利用したりする必要がある。また、特別のアクセス制限のかかっている会議室にアクセスしたりすることもある。そこでは、違法性が高い情報や物品が取引されており、犯罪の温床ともなっているとされる。

（3）ハニーポット

ハニーポットとは、故意に外部からの進入を容易にした囮用のネットワーク機器をいう。マルウェアの感染活動等の検知を目的にネットワーク上に設置する（「総務省の情報セキュリティ政策」資料より）。もし、会社・組織が、国境をこえて、ハニーポットを用いて、マルウェアの情報や通信ログを収集したとした場合に、法的な問題が発生するのかということが議論されうる。

（4）ビーコン

このビーコンの技術であるいわゆるウエブビーコンは、HTML を利用したメールやウェブページの閲覧者を識別する仕組みのことをいう。メールやウエブに埋め込まれた要素の解釈・表示に際してなされるサーバへの通信を分析することによって閲覧者が、IP アドレス、プロバイダホスト名、閲覧時刻、閲覧時間、閲覧した URL、そのページの参照元、検索ワード、（JavaScript を利用した場合）利用しているブラウザの種類、モニタの解像度などの情報を得ることができる。これについて、継続的なキャンペーンを行っている攻撃者にわざと「囮」のデータを取得させてその囮のファイルを開いた場合にビーコンがその攻撃者の情報を送ってくるということが可能である。そのような行為について、どこまでが許容され、どこからが許容されないのか、という問題が生じうる。

（5）シンクホール[6]

シンクホールは、DNS シンクホールといわれ、不正なホストへの解決のリクエストを要求された場合、他の（C&C サーバ以外の）IP アドレスを返すことによりクライアントが不正な C&C サーバなどに接続するのを防止する機能である。ブラックホール DNS（パケット・ブラックホール）などとも呼ばれる。この場合、通信の傍受やネットワークの中立性との関係はどうであるのかという問題が発生しうる。

（6）ハックバック

報復的ハッキング（Retaliatory　Hacking）は、別名、「アクティブ・ディフェンス[7]」「バ

---

[6] https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523

[7] 「Active Cyber Defense (ACD)」というときには、米国国防総省の「脅威及び脆弱性についての発見、探知、分析、対応のための同調された、リアルタイムの作戦」という考え方及びそれにともなう活動をいうのが一般である。この ACD の活動は、そのために、センサー、ソフトウェア及び諜報を利用することによりネットワークスピードで作戦を実行することになる。この作戦のために、サイバー状況に対する意識及びサイバー防衛アクションプラン・実施がなされる。

ック・ハッキング」「ハックバック」「攻撃的対抗措置（offensive countermeasures）」などといわれている。ハックバックというのは、一般によく利用される用語であるということができる一方で、それゆえに法的にはきわめて多義的な意味であるといえる。

3　各国における脅威インテリジェンスサービスの利用と留意点

2.2 でみたような脅威インテリジェンスにおける情報の取得方法が、特に戦略的脅威インテリジェンスにおいては、法的に種々の論点を含みうるものであることから、各国においてこれらの論点をもとに、どのような対応が考えられるのか、ということについてみていくものとする。

3.1　米国一般論

3.1.1　脅威インテリジェンスの利用

サイバー脅威インテリジェンス（cyber threat intelligence; CTI）とは、サイバー脅威に関するデータを収集・加工して有益な情報とした上で、当該情報を加工・分析して意思決定に用いることのできる形態にしたものである[8]。すなわち、サイバー作戦（cyber operation）を実施する敵の能力、機会、意図に関する分析された情報である[9]。

近年、政府機関、私企業におけるサイバー攻撃[10]に対する防御や法執行等において、CTI の重要性は高まっており、CTI を提供するサービスも数多く登場している。

SANS の調査に協力をした世界各国の 240 以上の諸組織（サイバーセキュリティサービスプロバイダ、金融機関、政府機関、技術系が多くを占める）では、CTI を利用又は生成すると回答した組織が全体の 85.0%であり（2021 年）、前年の 7%増となっている[11]。その多くは、組織内と外部のリソースを組み合わせて活用しているが（55.7%、2021 年）、社内のみで CTI を生成・利用している割合は 36.5%（2021 年）と前年の 5%増となっている[12]。

CTI は、最近では、通常の方法ではアクセスできないダークウェブ（「闇サイト」とも呼ばれる）において収集されることが多くなっており、自社でダークウェブをモニタリングする、又はダークウェブをモニタリングするサービスを購入するといった方法によって収集されている[13]。ダークウェブは犯罪の温床となっているところ、かかるダークウェブに潜入し、一定の活動することが各種法令に違反しないかが問題となっている。

---

[8] CREST, “What is Cyber Threat Intelligence and how it is used？“ (https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf) 7 頁参照。
[9] SANS, “2021 SANS Cyber Threat Intelligence (CTI) Survey” (https://www.domaintools.com/resources/survey-reports/sans-2021-cyber-threat-intelligence-survey) 2 頁。
[10] 「サイバー攻撃」という用語は、本稿においては、特段の記載のない限り、コンピュータシステムに対し、ネットワークを通じて、破壊活動、データ窃取、データ改ざんを行う等システムの所有者・管理者の望まないことを行う活動全般をいうものとする。
[11] 前掲 SANS、3-4 頁。
[12] 前掲 SANS、5 頁。
[13] 例えば、https://apmg-international.com/article/using-dark-web-threat-intelligence など。

3.1.2　脅威インテリジェンスの利用における法的留意点

3.1.2.1　インテリジェンスサイクルと法的留意点

CTI も通常のインテリジェンスと同様に、生成から配付に至るまでのインテリジェンスサイクルがある。すなわち、計画/要件（planning/requirements）、収集（collection）、処理（processing）、分析（analysis）、配付（dissemination）である。

[14]

「計画/要件」とは当該組織においてどのような CTI を生成するかを定めること、「収集」とは CTI のもととなるデータ・情報を収集すること、「処理・分析」は収集したデータ・情報を一定の文脈のもと照合、編纂し、サイバーセキュリティ上の意思決定に有用な形に処理分析すること、「配付」は必要とする組織・部署に生成された CTI を配付すること、である。

このサイクルにおける各段階のうち、法的に留意すべきは、特に「収集」及び「配付」となる。なぜなら、「収集」においては、外部（特にダークウェブなど）からの情報収集方法や個人情報の収集管理について一定の法令を遵守する必要があり、「配付」においては、特に CTI を外部（CTI サービスプロバイダ）から調達する組織について、その CTI の生成過程の適法性まで考慮すべきかという問題があるからである。さらに、CTI を外部と共有する場合にも一定の法的問題が生じる。

このうち、「収集」に関し、米司法省（DoJ）サイバーセキュリティユニット（CsU）[15]は、2020 年 3 月、「サイバー脅威に関する情報をオンラインで収集し、不正なソースからデータを購入する際の法的な考慮事項」（”Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources”）[16]というガイダンスを発表した。これは、法的拘束力のないものであるが、①ダークマーケットからの CTI の収集及び②違法な情報等（マルウェア、セキュリティの脆弱性、盗まれた自己データ等）の購入が連邦法に違反するかについて考え方の指針を与えるものである[17]。

---

[14] 前掲 SANS、6 頁。

[15] DoJ 犯罪部門コンピュータ犯罪及び知財課内の組織。2014 年 2 月、犯罪者の電子的監視やコンピュータ詐欺・不正利用防止法（CFAA）がサイバーセキュリティに対してどのような影響を与えるかに関する専門家の助言と法的ガイダンスの中核ハブとして設置された（https://www.justice.gov/criminal-ccips/cybersecurity-unit）。

[16] https://www.justice.gov/criminal-ccips/page/file/1252341/download（原文）。翻訳は別紙参照のこと。

[17] 同ガイダンスでは専ら連邦法違反について論じており、州法や外国法が別途適用される可能性があると

以下これを踏まえて米国における CTI 利用における法的留意点について述べる。

3.1.2.2　アクセスにおける問題（不正アクセス、なりすまし）

前述のように CTI は、ダークウェブにおけるダークマーケット[18]において収集される場合があるところ、ダークマーケットに潜入して情報を受動的にモニタリングする行為それ自体が法令違反になる可能性は少ないとされる。

もっとも、ダークマーケットに不正アクセスした場合には、法的問題が生じる。例えば、許可なしにそのようなフォーラムにアクセスしたり、そのフォーラムで発生した通信をひそかに傍受したりする場合は、コンピュータ詐欺・不正利用防止法 （Computer Fraud and Abuse Act ; CFAA）[19]（18 U.S.C.§1030[20]）及び通信傍受法（18 U.S.C.§2511）に触れるおそれがある。また、脆弱性を悪用したり、盗まれた認証情報を使用したりするなど、不正な方法でフォーラムにアクセスすると、CFAA 及びアクセスデバイス不正行為防止法(18 U.S.C.§1029)などの法令に抵触するおそれがある。

また、架空の人物になりすまして、偽のオンライン ID を使用してアクセスすることは連邦刑事法に違反しないが、実在の人物になりすました場合には、州法によってはプライバシー違反の民事的な問題が生じる。また、架空の人物であっても政府職員を装った場合には連邦刑法（18 U.S.C.§912）に抵触するおそれが生じる[21]。

3.1.2.3　ダークマーケットにおけるコミュニケーション

有用な情報を得るためには、ダークマーケットで活動する者らとコミュニケーションをとり、その信頼を得る必要がある場合がある。その際も、提供した情報が犯罪に使用された場合には犯罪の幇助・教唆（aid and abet）となる可能性がある。また、犯罪の共謀に参加し、その犯罪の実行に同意した場合には共謀罪が成立する可能性もある（なお、不正アクセス罪を定める CFAA 第 1030 条は、共謀罪や未遂罪も可罰的としている[22]）。

また、実際に起訴、有罪とならなくとも、犯罪捜査の対象となるおそれもある。

そのため、同ガイダンスでは、犯罪の実行に使用される真実の情報を提供しないよう呼びかけている。その上で、真の目的・意図を疑われ捜査に巻き込まれないためにも、

の断りがある（同 2 頁）。

[18] 同ガイダンスでは、ダークマーケットについて、「ダークマーケットは、TOR（オニオンルーター）ネットワーク上にあり、オンライン通信の発信元を特定しにくくするために設計されたコンピュータの集合体である。TOR ネットワークでは、通信を暗号化し、世界中の一連のリレーを介してルーティングすることで、発信元を追跡しようとする試みを阻止する。TOR 秘匿サービス「ダークウェブ」は、TOR ブラウザを使用しないとアクセスできないサイトである。TOR 秘匿サービスとして動作しているサイトの位置は隠蔽されており追跡が困難であるため、違法行為に関連するサイトのホスティングに適した技術である。」とする（同注 4）。

[19] CFAA は、日本の不正アクセス禁止法に類似する規律を定める法律である（1986 年制定）。

[20] 合衆国法典（U.S.C.）18 巻 1030 条（コンピュータに関連した詐欺その他の関連行為）を意味する。米国の法律は、一部の例外を除きすべて、制定後に合衆国法典の関係個所に組み込まれ編纂される。この際、一つの法律に含まれる条文がすべて同じ個所にまとまって組み込まれるとは限らないため注意が必要である。

[21] 同ガイダンス 3 頁、6 頁。

[22] 18 U.S.C.§1030(b)。本書後記訳注 9 参照。

- 情報収集活動を行う前に法執行機関にその旨知らせて関係を築くこと
- 担当者が従うべき行動規則又はコンプライアンス・プログラムを策定し、法律家の確認を得ておくこと
- 担当者が実際に行った活動と収集した情報の記録をとっておくこと

を強く推奨している。

3.1.2.4 盗まれた情報、マルウェア、セキュリティ脆弱性の購入

より積極的なサイバーセキュリティ活動として、担当者がダークマーケットで売りに出されている盗まれた情報、マルウェア、セキュリティ脆弱性を購入するという場合がある。同ガイダンスでは、売主が誠実とは限らず、代金を受け取って売買目的物を提供しない、盗難データの写しを破棄するとの約束を破る、等々のリスクがあることに言及する。その上で購入する際には、データの所有権、データの性質、売主の身元に鑑み、法令違反となるおそれがあることを指摘する。

なお、これらの注意事項は、CTI を扱うサイバーセキュリティ企業から一般企業が CTI 等を購入する場合（前述のインテリジェンスサイクルの「配付」における法的問題）にも同様にあてはまる。

- データの所有権

自己の盗まれた情報を買い戻すことは法令に違反しない。他人の盗まれた情報を購入することは、その目的によっては、なりすまし罪（identity theft）[23]又は営業秘密窃取になりうる。もっとも、買い取った情報の中に他人の個人情報や営業秘密が含まれる場合もありうる。その場合でも、犯罪の意図や他人の経済的利益に供する目的のない限り犯罪が成立する可能性はないが[24]、他人の情報があることを知りつつ適切な措置をとらない場合にはかかる犯罪の故意や目的が推認され、犯罪捜査や個人による調査（個人情報の場合）の対象となるおそれがある。

したがって、同ガイダンスでは、第三者のデータが含まれていることが判明した段階で、速やかに分離し、それ以上アクセス、確認、使用しないようにした上で、法執行機関又は所有者に知らせ、一連の対応を文書化することを推奨する。

- データの性質

脆弱性やマルウェアを購入することは通常、法令に違反しないが、同ガイダンスでは 2 つの例外を挙げる。

一つは、電子通信をひそかに傍受するように設計されたソフトウェアである。「電子、機械その他の装置の設計が、有線、口頭又は電子通信の秘密裡の傍受の目的に主として有用で

---

[23] 18 U.S.C. § 1028(a)(7)は、Identity Theft and Assumption Deterrence Act により加えられた条文である。「情を知って、法的権限なく、連邦法違反の不法な行為又は州法その他の法律における重罪を実行、教唆、幇助する意図で、他人の身分を証明する手段を譲渡又は使用すること」についてなりすまし（identity theft）犯罪として最大 15 年の有期刑と定める。

[24] 18 U.S.C. §§ 1029(a)(1)-(8), (10); 18 U.S.C. § 1832(a)参照。identification fraud (18 U.S.C. § 1028), credit card fraud (18 U.S.C. § 1029), computer fraud (18 U.S.C. § 1030), mail fraud (18 U.S.C. § 1341), wire fraud (18 U.S.C. § 1343), or financial institution fraud (18 U.S.C. § 1344)

あることを知り、又は知りうる場合に、当該装置」の意図的な所持・販売を禁止する通信傍受法（Wiretap Act）に違反する可能性を指摘する[25]。

もう一つは、後述の売主の身元に関係する問題である。

- 売主の身元

売主がテロ組織と関係していることを知って取引をした場合、外国のテロ組織と指定されたグループに物質的支援を提供すること、又は提供しようとすること、もしくはそのような共謀を行うことを禁じた 18 U.S.C.§ 2339B 違反として刑事責任を問われうる。

販売者が経済制裁又は貿易制裁の対象であることを知って、又は知り得たのに取引をした場合は、国際緊急経済権限法（IEEPA）に基づき刑事責任を追及されうる。

もっとも、ダークマーケットで取引をする場合、売主は身元を隠しているため、上の 2 つの刑事責任が立証される可能性は低いと指摘されている。

もっとも、IEEPA は、刑事責任だけでなく、民事上の責任も定めており、この場合、当事者は、取引の相手方が貿易又は経済制裁の対象となっていることを知らなかったとしても制裁金が課されうる（厳格責任）。このリスクを軽減するため、IEEPA の民事的執行を管轄する米国財務省海外資産管理室（OFAC）は、各企業においてリスクベースのコンプライアンス・プログラムを実施することを奨励している。

3.1.2.5 CTI を外部と共有する場合の法的問題

CTI の共有は、政府・民間間、民間・民間間がありうるが、米国では、連邦政府との CTI の共有は、2015 年サイバーセキュリティ情報共有法（Cybersecurity Information Sharing Act; CISA[26]）に定められている。

連邦政府との共有については、CISA 上、以下における免責措置（FOIA や行政処分等からの免責）が施されているが、その他の私企業間等での共有については、当該免責措置はとられないため注意が必要である[27]。また、当該免責措置の適用は、たとえ連邦政府と共有する場合であっても、国家安全保障省（DHS）の提供するプロセス（自動インディケータ共有（Automated Indicator Sharing (AIS)や指定されたウェブサイト・メール・郵便での共有）で共有した場合に限られる。なお、情報共有分析センター（ISACs）や情報共有分析組織（ISAOs）と共有する場合は、ISACs や ISAOs が DHS のプロセスに従って連邦政府と情報共有するため、当該免責措置が適用される[28]。

---

[25] 18 U.S.C. § 2512(1)(b)

[26] 6 U.S.C. §1501～。

[27] 例えば、正当な理由があれば他社に対する訴訟におけるディスカバリ（証拠開示）手続により自社の CTI が開示されるということがありうる。

[28] 6 U.S.C. §1505(b)(1)。「2015 年サイバーセキュリティ情報共有法において非政府組織が連邦政府とサイバー脅威インディケータ及び防御策を共有するためのガイダンス」（https://www.us-cert.gov/sites/default/files/ais_files/Non-Federal_Entity_Sharing_Guidance_%28Sec%20105%28a%29%29.pdf）15 頁。

情報開示請求に基づく開示請求

米国では、情報自由法（Freedom of Information Act; FOIA）[29]に基づき、例外事由にあたらない限り、請求に応じてすべての政府情報が公開されることとなっている。そのため、政府と共有した情報が FOIA に基づく請求によって開示される懸念がありうる。

これについては、2015 年サイバーセキュリティ情報共有法（Cybersecurity Information Sharing Act; CISA[30]）において、脅威インテリジェンスの共有については FOIA による開示請求から除外される旨明示され、かつ、州法に基づく開示請求からも除外されるとされた[31]。

プライバシー違反の懸念

CISA において連邦政府等と共有できるサイバー脅威情報は、サイバー脅威インディケータ及び防御策（defensive measures）である。「サイバー脅威インディケータ」とは、悪意のある偵察、セキュリティコントロールを破る方法又はセキュリティ脆弱性の悪用、セキュリティ脆弱性、正当なユーザにセキュリティコントロールを破らせたり脆弱性を悪用させたりする方法、悪意のあるサイバーC&C、インシデントによって実際又は潜在的に生じた害、その他のサイバーセキュリティ脅威、その組み合わせをいう[32]。「防御策」とは、既知又は予想されるサイバーセキュリティ脅威又はセキュリティ脆弱性を検知、防止、緩和する情報システム又は情報システム上で保存、処理、送信される情報に適用される対応、装置、手順、シグネチャ、技術、その他の措置をいう。このように、個人情報は、共有すべきサイバー脅威情報には含まれない。

そして、CISA においては、私企業において、脅威データを共有する場合には、データ内容を確認して個人情報を削除することが求められている[33]。

それに反して、セイバーセキュリティ目的に扶養な個人情報が含まれることを知って脅威データを共有し、それが外部に漏れた場合には、私企業は責任を問われる可能性がある。

政府の措置又は民事責任からの免責

CISA においては、CTI の共有につき CISA の手続に従って行われる限り民事上の責任は免除されると明記された[34]。また、共有された CTI に基づいて政府による規制・制裁がされることもない[35]。

もっとも、訴訟のディスカバリ手続で開示される可能性はあり、国外における訴訟については保護を及ぼしていない点に留意する必要がある。

その他

以上の通り、情報共有に伴って、一定の法的保護が施されているものの、データが共有されたのにそれに基づいて行動しなかった場合には、法的責任が伴うことに注意が必要であ

[29] 5 U.S.C. § 552。
[30] 6 U.S.C. §1501～。
[31] 6 U.S.C. §1504(d)(3)
[32] 6 U.S.C. §1501(6)
[33] 6 U.S.C. §1503(d)(2)
[34] 6 U.S.C. §1505(b)(1)
[35] 6 U.S.C. §15054(d)(5)(D)(i)

る[36]。サイバー攻撃等によりデータ流出等が生じ、ユーザ等から民事上の責任を問われた場合、私企業が「合理的（reasonable）」な措置をとったかが判断基準となるところ、脅威インテリジェンスを共有している場合には、それを認識していることを前提として合理性が判断されうる、ということである。

3.2　英国

英国において脅威インテリジェンスサービス[37]の利用についてふれた文献は、非常に多い。例えば、「政府におけるサイバー脅威インテリジェンス：意思決定及び分析のためのガイド」（Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts）[38]は、サイバー脅威インテリジェンスの全方面にわたるガイドラインであり、特に政府におけるサイバー脅威インテリジェンスの利用について解説している。ここでは、ダークウェブでの情報に関しては、インテリジェンスは、オープンソースから得られるものがきわめて多く、ダークウェブの情報を取得することは推奨しないとしている。違法なコンテンツについてアドバイスを求めるときは、NCSC（国家サイバーセキュリティセンター）に相談するか、国家犯罪庁（National Crime Agency (NCA)）に相談するようにとされている。また、政府部門のネットワークについては、Tor ノードに対しての接続をできないようにすることが推奨されている（同書　5.1.3）。また、ヒューミントのソースについての実務規範があり、必要に応じて、それを参照するようにとされている（同 5.1.6）。

また、他のガイダンスとして CREST「サイバー脅威インテリジェンスの概念と利用」（What is Cyber Threat Intelligence and how is it used?）がある[39]。CREST は、情報セキュリティ技術市場を代表し、サポートする国際的な非営利の認定・認証機関である[40]が、この報告書は、サイバー脅威インテリジェンスの実践と調達に関する実践的なアドバイスを提供する入門書である。サイバー脅威インテリジェンスを支える重要な概念と原則を概説し、組織がサイ

---

[36] “Legal Implications of Threat Intelligence Sharing” Sans Cti Summit 2018（https://ciampeathehomedesignings.com/）

[37] 英国においてサイバー脅威インテリジェンスにふれた文献等は、枚挙にいとまがない。公的な団体等から公表されたものとしては、また、イングランド銀行の CBEST　（規制当局の監督ツールキット）についてのガイドである「CBEST　ー脅威インテリジェンスによる評価」（CBEST Threat Intelligence-Led Assessments、https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide）がある。

[38] https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Cyber-Threat-Intelligence-A-Guide-For-Decision-Makers-and-Analysts-v2.0.pdf）　また、この分析は、「不知を探索する　脅威ハンティングのガイド」（“Detecting the Unknown:
A Guide to Threat Hunting”　https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Detecting-the-Unknown-A-Guide-to-Threat-Hunting-v2.0.pdf）「あなたの存在をコントロールする　デジタルリスクとインテリジェンス」（Controlling Your Exposure: A　Guide to Digital Risk and　Intelligence）（https://hodigital.blog.gov.uk/wp-content/uploads/sites/161/2020/03/Controlling-Your-Exposure-A-Guide-to-Digital-Risk-and-Intelligence-v2.0.pdf）、とシリーズをなすものである。

[39] https://www.crest-approved.org/wp-content/uploads/CREST-Cyber-Threat-Intelligence.pdf

[40] https://www.crest-approved.org/index.html　なお、設立時においては、The Council of Registered Ethical Security Testers（Crest）であって、英国で侵入テストのための業界団体及び職業団体という性格を有していた。

バー脅威インテリジェンスを使用して、潜在的なサイバーを予防、検出し、セキュリティインシデントに対応する方法を解説している。また、必要な能力を備えた適格なサプライヤーを選択するためのガイダンスと基準も提示している。同書では、外部の脅威インテリジェンスの利用について、「安心感」があるとして、脅威情報収集のいくつかの側面では、脅威の行為者や潜在的に悪意のある人との相互作用を伴うこと、コンテンツの収集で避けられないリスクの一部を軽減するために、外部の脅威インテリジェンス・サプライヤーを利用することができることが触れられている。これらのプロバイダーは、これらの課題にも精通しており、リスクと潜在的な法的問題を解決することができるとされる。そこでは、関連する規定として 1998 年人権法（第 8 条)、2000 年調査権限規制法（RIPA)、1990 年コンピュータ不正使用法、2018 年データ保護法（DPA)、1996 年刑事手続捜査法（CPIA1996)、2010 年贈収賄法、2002 年犯罪収益法（POCA）などがあげられている[41]。

3.3　ドイツ

不法な情報源からのデータの購入等に対する規制が最近になって刑法に入れられた点に特徴がある。我が国における類似の規制には不正競争防止法 21 条 1 項各号の営業秘密侵害罪や割賦販売法 49 条の 2 等を挙げることができるかもしれないが、同条の罪は情報の価値に基づいた保護であって、ハッキング等、獲得過程の不正性に着目したものではない。それゆえに、事実上、ダークウェブ対策を狙ったものでもない。これに対して、ドイツ刑法 202 条 d のデータ故買罪は、ある程度ダークウェブ対策にも焦点を当てたサイバーセキュリティの維持のための規定だと理解することができる。

2015 年の刑法改正で入ったデータ故買罪は，無権限アクセス罪、データ傍受罪その他の違法な行為により獲得されたデータの移転を包括的に処罰しようとする規定である。

処罰の欠缺があるのでデータ故買を独立して処罰する必要があるとされた。すなわち、まず、本罪が挿入される前にも、既に刑法 202 条 c が、無権限アクセス等の遂行のために使われるパスワードや保護コードの転売等を禁止しているところではあった。もっとも、同規定では、それらに保護の範囲が限定され、無権限アクセス等で取得された場合を除き（この場合は刑法 202 条 a で保護され得る)、キャッシュカードやクレジットカードに関するデータの保護ができなかった（BT-Drs. 18/5088, 25)。データ故買にのみ関与する者は、故買の時点では既に先行する無権限アクセス罪等が終わっているから、故買自体を処罰する規定がない限り、先行犯罪の共犯として処罰できなかった（BT-Drs. 18/5088, 25)。また、データの購入者において当該データを用いて犯罪をするつもりがない限り、当該データを使ったコンピュータ詐欺等を検討することも難しい（BT-Drs. 18/5088, 25)。連邦データ保護法や不正競争防止法上の営業秘密保護の規定では、客体が限定されすぎる（BT-Drs. 18/5088, 25-26)。

---

[41] データ保護法の部分は、GDPR に対応した 2018 年と修正した。なお、調査権限法については、シギントについての 2016 年調査権限法とヒューミントに関する 2000 年調査権限規制法とがあり、現時点においては、双方と関連性があるものと考えられる。

以上の考慮に基づいてデータ故買罪が刑法 202 条 d として入れられた。本罪の保護法益はデータの形式的な秘密（das formelle Datengeheimnis）である（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 3）。データの形式的な処分権といってもよい（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 3, 14）。データの内容は要保護性との関係では重要でない（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 6）。処分権者は、基本的にデータを収集し、保存した者のことであり、データ媒体の所有や占有の帰属自体は決定的ではないし（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 14）、データ保護法上の権利とここでいう処分権の双方が同一人に帰属することはあり得るが、データ保護法上の関係者であるか否かは判断にあたって意味はない（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 15）。

客体は、一般にアクセスができず、かつ他の者が違法な行為により獲得したデータである。一般にアクセスできるデータについては、その利用により上記法益の侵害はない、とされる（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 12）。「一般にアクセスできる」とは、ログイン、許諾、対価の支払いなく、あるいは事前にアカウント登録、許諾、対価の支払いをすることによって、利用可能になっていることをいう（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 12）。公開されている著作物も、有償の場合も含め、「一般にアクセスできる」に該当するゆえに、著作権侵害によって得られた著作物も、本罪の客体の要件を充たさない（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 12）。

違法な行為により獲得したデータというときの違法な行為には幅広い違法行為が含まれる。行為者の責任要件の具備や告訴は不要である（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 13）。無権限アクセス（刑法 202 条 a）やデータ傍受（刑法 202 条 b）だけでなく、処分権者の形式的な処分権に対しても向いている行為によってデータが取得されているのであれば、窃盗、詐欺、コンピュータ詐欺等により獲得される場合も含む（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 13）。一方で、ポルノの頒布のような公共の利益を害するだけの場合、並びに連邦データ保護保護法上、可罰的な行為の場合（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 16）、単なる契約違反、契約上のアクセス制限の違反、及び著作権を侵害してデータを複製する場合には、当該行為は形式的な処分権に向けられたものではないから、ここでいう違法な行為による獲得にはならない（MüKoStGB/Graf, 3. Aufl. 2017, StGB § 202d Rn. 17）。

４　米国司法省「オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項」の翻訳及び解説

4.1　米国司法省「オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項」の翻訳

前掲「サイバー脅威に関する情報をオンラインで収集し、不正なソースからデータを購入する際の法的な考慮事項」を、JNSA から提供された下訳を参考に、別紙の通り正式に翻訳

した。

（別紙訳文）

サイバー脅威に関する情報をオンラインで収集し、不正なソースからデータを購入する際の法的な考慮事項[42]

Version 1.0 (2020 年 2 月)

Ⅰ. はじめに

サイバーセキュリティユニット（CsU）は、特定のサイバーセキュリティ対策の合法性に関する民間団体からの質問に答えるために本文書を作成した[43]。作成には、司法省の他の部門、国家安全保障局やその他の連邦機関も寄与した[44]。本文書は、CsU のミッションに従い、民間団体における効果的なサイバーセキュリティ実践の採用及びその合法的な実施を支援することを目的としている。

本文書は、コンピュータ犯罪が画策され、盗まれたデータが売買されるオンラインフォーラムに関わる情報セキュリティ担当者による、サイバー脅威インテリジェンス収集の取り組みに焦点を当てている。また、民間人が、ダークマーケット（Dark Market）[45]において、マルウェア、セキュリティの脆弱性、又は自己の盗まれたデータ (又は、他者の盗まれたデータであって、当該データ所有者の許可を得ている場合) を購入しようとする場合についても論じる。もっとも、本文書は、児童ポルノ[46]や違法薬物の売買のような、他のタイプの犯罪

---

[42] 本文書は、権利や救済を付与するものではなく、法的効力を有しない。*United States v. Caceres*, 440 U.S. 741, 752-753 (1979)を参照のこと。また、本文書はいかなる規制上の効果も意図するものではない。

[43] 本文書は、民間人の活動に焦点を当てる。政府関係者が本文書で議論されている活動に従事する場合、本文書で扱われていない他の法律上及び政策上の問題が生じる可能性がある。政府関係者は、自己の活動に関し、政府機関又は省庁の顧問に相談する、又は CsU に連絡し、その助言を受けるべきである。

[44] 本文書の作成にあたり、連邦捜査局（Federal Bureau of Investigation; FBI）、合衆国シークレットサービス（United States Secret Service）、外国資産管理室（Office of Foreign Asset Control; OFAC）から貴重な情報提供を受けた。

[45] ダークマーケットは、TOR（オニオンルーター）ネットワーク上にあり、オンライン通信の発信元を特定しにくくするために設計されたコンピュータの集合体である。TOR ネットワークでは、通信を暗号化し、世界中の一連のリレーを介してルーティングすることで、発信元を追跡しようとする試みを阻止する。TOR 秘匿サービス「ダークウェブ」は、TOR ブラウザを使用しないとアクセスできないサイトである。TOR 秘匿サービスとして動作しているサイトの位置は隠蔽されており追跡が困難であるため、違法行為に関連するサイトのホスティングに適した技術である。

[46] インターネットや携帯電話を利用して、意図的に児童ポルノの広告、配布、受信、所持をし、又は児童ポルノに意図的にアクセスすることは違法であるため、児童ポルノの取引やそれに関連する違法行為を扱うフォーラムから情報を収集するための法的分析は、本文書で考察するものと異なる可能性が高い。18 U.S.C. §2251、§2252、及び§2252A を参照。したがって、これらのフォーラムにおいて情報収集やその他の活動を行う場合には、別の法的考察が必要となる。

常に従うべき 2 つのルール

1. 加害者にならないこと

本文書で取り上げている活動の一部は、連邦刑法に関係しており、州法に違反したり民事責任を問われたりする可能性がある。これらの活動に従事することを計画している組織は、その活動の合法性を評価するために弁護士と相談すべきである。場合によっては、この種の計画を検討する際に、FBI 及びシークレットサービスの現地地方局との関係を築くことも有益であろう。連絡先情報は本文書の最後に記載の通りである。

2. 被害者にならないこと

本文書で取り上げているサイバーセキュリティ活動には、高度な犯罪者とのやり取りが含まれる場合があり、慎重なリスク評価なしに実施すべきではない。これらの活動に従事することを計画している組織は、常に警戒を怠らず、適切なセキュリティ保護措置を講じ、被害を受けるリスクを最小限に抑えるサイバーセキュリティ実践を遵守すべきである。

フォーラムにかかるインテリジェンスや証拠の収集を対象とすることを意図したものではない。

本文書において言及するシナリオは、CsU の民間部門への支援及び連携において提言される実践であって、サイバーセキュリティコミュニティにおいて、インテリジェンスを収集し、盗難データを取り返し、マルウェアのサンプルとセキュリティの脆弱性を入手するために一般的に使用されている実践に由来するものである。ここで議論する法的な問題は、情報セキュリティ担当者がこれらの活動に携わる際に生じる可能性がある。本文書は、潜在的な法的問題の特定に役立つことを目的としているが、特に、ほんの少しの事実の違いによって法的分析が大きく変わる可能性があることから、あらゆる状況において担当者が直面する可能性のあるすべての法的問題に全面的に対処することはしておらず、かつ、それは不可能である。したがって、本文書の読者においては、弁護士と相談して、その助言と分析を適切に利用することを強く推奨する[47]。

[47] 本文書は、セキュリティ担当者が所属する組織の法律顧問と話し合うための足掛かりとして役立つ。本文書で強調している考慮事項を、具体的な事実に則して適用することによって、組織は法的利益とリスクの個々の評価に適合するよう計画を調整してから手続を進めることができる。

オンラインフォーラムで合法的に情報を収集するためのヒント

- 受動的な情報収集は原則違法ではない

オンラインフォーラムから受動的に情報を収集するだけでは、コンピュータ犯罪に関連する犯罪行為が行われている場合でも、特に犯罪の意図がない場合には、連邦犯罪を構成する可能性は低い。しかし、許可なしにそのようなフォーラムにアクセスしたり、そのフォーラムで発生した通信をひそかに傍受したりする場合は、コンピュータ不正利用防止法(CFAA)(18 U.S.C.§1030)[訳注 1]及び通信傍受法(18 U.S.C.§2511)[訳注 15]に触れるおそれがある。

- フォーラムに合法的にアクセスする

脆弱性を悪用したり、盗まれた認証情報を使用したりするなど、不正な方法でフォーラムにアクセスすると、CFAA 及びアクセスデバイス不正行為防止法(18 U.S.C.§1029)[訳注 2]などの法令に抵触するおそれがある。

- 同意なしに他人になりすまさない

偽のオンライン ID を使用して、犯罪行為が行われているフォーラムにアクセスしたり参加したりすることは、通常、単独では連邦刑法に違反しない。しかし、架空の人格を作るのではなく、当人の許可なく実在の人物になりすますことは、法的問題を引き起こすおそれがある。

本文書における法的議論は、米国連邦刑法に限定したものである。民事責任、州法、又は米国以外の国の法律には焦点を当てておらず、規制上の制限の可能性についても対象としていない。

II. シナリオの前提条件

以下のシナリオは、サイバーセキュリティ活動の一環としてダークマーケットのフォーラムから情報を収集する民間の情報セキュリティ担当者の活動を前提としている。活動の実施方法と担当者の意図について、法的に重要な前提条件に基づく。

A. *セキュリティ担当者*

本文書は、コンピュータ犯罪に関連するツールやサービスが売買され、盗まれたデータが購入可能なダークマーケットから情報（すなわち、サイバー脅威インテリジェンス、盗難データ、セキュリティの脆弱性、及びマルウェア）を入手する民間の情報セキュリティ担当者に焦点を当てている。これらの活動が米国の管轄内で行われ、米国連邦刑法の適用を受けることを前提としている[48]。また、担当者による情報の取得は、合法的なサイバーセキュリティ目的（例えば、他者がサイバーセキュリティ脅威を特定し、防御することを支援する目的）のために利用及び共有できるようにすることに限られ、犯罪や悪意のある意図又は動機がないことを

[48] オンライン上の活動への連邦刑法の適用は複雑になり得る。一部のサイバー犯罪に関する法律には、管轄範囲が広いものがある。例えば、コンピュータ不正利用防止法（CFAA）は、対象となるコンピュータが米国外にある場合でも、州際間もしくは外国との商取引や通信で使用される、又はそれに影響を及ぼす

前提としている。

この種のオンライン活動に従事する担当者は、セキュリティや個人の安全のためにフォーラムで活動している間、偽名や偽りの ID をよく使用する。後述するように、偽の ID は全く架空のものを捏造すべきであり、許可なしに実在の人物の身元を使用すべきではない。また、捏造したオンライン ID では、政府関係者のような特別な地位にある人物を偽って名乗るべきではない[49]。

B. *フォーラム*

サイバーセキュリティ担当者が、サイバー脅威インテリジェンスを収集するフォーラムは様々である。そのほとんどは、秘匿サービスとして TOR ネットワークを介してアクセス可能なサイト上のダークウェブにある[50]。これらのダークマーケットフォーラムの一部は、招待制のサイトで、情報セキュリティ業界では、違法なサービスを入手し、又は、盗まれた金融データや個人データを購入するために利用されることで知られている。また、運営者を保護すべく TOR が提供する匿名性に依存して、ダークウェブ上でオープンにアクセスできるものもある。これらのフォーラムのディスカッションスレッドには、コーディングやマルウェアに関連する一般的なトピックが含まれている。しかし、セキュリティ担当者が最も関心を持つサイトでは、違法なサービスや、盗まれたクレジットカード番号、パスワード、その他の機密情報の販売を公然と行っている[51]。

C. *フォーラムへのアクセス*

フォーラムにアクセスする方法は、法的に重要である。アクセス手段に関する法的な問題を回避する最善の方法は、フォーラム運営者から提供された正規の認証情報を使用してフォーラムにアクセスすることである。不正な手段でフォーラムにアクセスすることは、連邦刑法に違反するおそれがある。例えば、盗まれた認証情報を使用してフォーラムにアクセスすることは、特に CFAA 違反となる可能性がある[52]。また、フォーラムが運営しているサーバ

コンピュータに対するサイバー攻撃や侵入を対象としている。18 U.S.C.§1030 (e)(2)(B) [訳注 3] 参照。他の刑法上の禁止条項は、より適用範囲が限定されており、多くの場合、域外適用は認められていない。*European Cmty. v. RJR Nabisco, Inc.*, 764 F.3d 129, 141 (2d Cir. 2014)（別の理由で破棄。136 S.Ct. 2090）（*Morrison v. Nat'l Austl. Bank Ltd.*, 561 U.S. 247, 264 (2010)を引用）（第 2 巡回裁判所は 18 U.S. § 1343（通信詐欺法）は、完全に域外の活動には適用されないと判示した）等を参照。オンライン上での行為に対する連邦刑法の適否の問題は、必然的に事実に依存しており、当該法律特有の分析を必要とする。本文書のシナリオの大部分は、連邦管轄権を想定しており、本文書で取り上げた連邦刑法が考慮事実にまで及んでいると想定している。しかし、フォーラムが開催される可能性のある場所など、活動が他国の法律に関係する可能性があるかどうかについては言及していない。

[49] 下記 6 頁及び注 17 を参照。

[50] 上記 1 頁 及び注 4 を参照。

[51] 冒頭で指摘したように、本文書では、児童ポルノを扱うサイトや、児童ポルノに関連するサイトは扱わない。上記 2 頁を参照。

[52] *United States v. Nosal*, 930 F.Supp.2d 1051,1061 (N.D.Ca 2013) (他の従業員のパスワードの不正使用は、18

ーやシステムから情報にアクセスして収集するために、意図した（つまり正規な）手段ではなく、エクスプロイトやその他の手法を使用することは、CFAA や、場合によっては電子的監視を規制する他の連邦刑法に違反する可能性がある[53]。同様に、フォーラムのポリシーに反してフォーラムにアクセスすることは、CFAA に基づく合法的なアクセスに関する法的問題を引き起こす可能性がある[54]。

犯罪者が運営するフォーラムでは、アクセスしようとする者が犯罪の故意を真に有しているという証拠を要求する場合がある。例えば、フォーラム運営者から、マルウェア又は盗まれた個人情報の購入又は提供を要求される場合がある。以下に説明するように、そのような要求に従うことは、担当者を法的な危険にさらす可能性がある[55]。

フォーラムにアクセス後、情報を収集する方法についても、法的な問題を引き起こす可能性がある。以下でさらに議論されているように、オンライン情報を記録するためのスクリーンキャプチャ及び他の一般的に使用される方法であって、サイトのセキュリティ機能を迂回

U.S.C.§1030 (a) (4) に基づく起訴における犯情の一つとなった。)参照; *Global Policy Partners, LLC v.Yessin*, 686F.Supp.2d631 (ED.Va2009)（許可なく妻のパスワードを使用して夫が妻の電子メールアカウントにアクセスしたことは、第 1030 条違反であるとした）。また、フォーラム管理者がフォーラムへのアクセスを許可するために満たすべき特定の要件を課す場合、CFAA が問題となるおそれがある。

[53] 例えば、通信者の同意を得ずに、ホストサーバに密かにインストールした「sniffer」又は同様のプログラムを使用して電子通信が傍受された場合、通信傍受法（18 U.S.C. §2511 以下）が適用される可能性がある[訳注 15]。このような行為は、他の法律や、同一サーバー上のスペースを共有するウェブサイトを有する罪のない人々のプライバシーを侵害する可能性もある。

[54] アクセスポリシーに反してオンラインサイトにアクセスした場合、合法性について疑義が生じる場合がある。*hiQ Labs, Inc. v. LinkedIn Corp*., 938 F.3d 985 (9th Cir. 2019)（アクセス許可を回避していない場合、公開されているアクセス可能な Web サイトについて Web スクレイピングをすることは CFAA 違反ではない）と、*Konop v. Hawaiian Airline,Inc*., 302 F.3d 868, 876 (9th Cir. 2002)（ウェブサイトへのアクセス制限が合法的なアクセスに影響を与える可能性について傍論で議論）とを比較のこと[訳注 4]。

[55] 下記 7-9 頁を参照。

ベストプラクティスⅠ

- 「行動規則」の作成

組織が本文書に記載する活動を実施する場合、または実施を計画している場合、犯罪者や犯罪組織とやりとりをする当該組織の職員又は請負業者に許容される行動の概要を示すプロトコルを記載した「行動規則」または「コンプライアンス・プログラム」を作成すべきである。事前に法的、セキュリティ、運用上の考慮事項を慎重に検討して作成されたプロトコルに従うことで、組織、その従業員、及びそのデータを危険にさらす可能性のある軽率な決定を防止できる。規則を文書化することは、組織が刑事上、民事上、または規制上の措置に直面した場合にも役立ちうる。

- 調査に備える

本文書で取り上げた状況では、連邦捜査官は犯罪者と情報収集に従事している罪のない者とを容易に区別できないかもしれない。その結果、合法的なサイバーセキュリティに従事する者が犯罪捜査の対象となる可能性がある。したがって、FBI の現地地方局またはサイバー・タスク・フォース、及び合衆国シークレットサービス電子犯罪タスク・フォース[訳注 5]の現地地方局と継続的な関係を構築することが有益な場合がある。信頼できる関係を予め築いておけば、情報収集活動に関する誤解を避けることができる。

- 優れたサイバーセキュリティの実践

本文書で議論している場面では、サイバー犯罪者と情報交換が行われる。そうした状況において「疑り深過ぎる」ということはない。常に優れたサイバーセキュリティを実践し、サイバー犯罪者と通信する際には、社内ネットワークに接続されていない、適切にセキュリティ保護されたシステムを使用すべきである。

しない、又は不正な方法で情報にアクセスしない方法を用いて情報を収集することにより、法律違反のおそれを回避することができる。

Ⅲ. サイバー脅威インテリジェンスの収集

サイバー脅威インテリジェンスを使用してサイバーインシデントの準備や対応を行うことで、悪意のあるサイバーインシデントの影響を緩和し、場合によっては完全に防止することも可能である。タイムリーで正確な脅威インテリジェンスによって、既知のサイバーセキュリティの脅威と脆弱性から組織とその顧客を保護することができる。CsU が積極的な防衛に関する産業界へのアウトリーチ活動の中で学んだように、多くのサイバーセキュリティ組織は、サイバー脅威インテリジェンスを収集することがサイバーセキュリティ活動の中で最も有益なものの一つであると考えて

いる[56]。

サイバー脅威インテリジェンスを発信する民間組織は、複数の情報源から情報を収集しており、中には、違法行為が計画され、違法行為に利用されたマルウェアや盗まれたデータが販売されているオンラインフォーラムその他の通信経路から情報を収集している場合もある。これらのソースから収集された情報は、過去・現在・将来のサイバー攻撃又は侵入、マルウェアのサンプル、現在使用されている又は開発中の犯罪者の戦術・ツール・手順、攻撃や侵入に関与している個人のエイリアスやIDに関するサイバー脅威インテリジェンス及びネットワーク防御情報の豊富なソースとなりうる。しかし、合法的な目的のために情報を収集する民間組織がこれらのオンラインフォーラムに参加する場合、脅威に関する情報を収集することと犯罪活動に従事することとの境界線を見分けるのは難しいこともある。以下に示す様々なシナリオは、組織が情報収集活動を行う計画を立てる際に、連邦刑法違反の可能性を減らすのを支援することを目的としている。

A.　シナリオ1：サイバー脅威インテリジェンスを収集するためのフォーラムでの「潜伏」

担当者がフォーラムにオープンに投稿されたやり取りを読んで情報収集をし、フォーラムのコミュニケーションに応答をせず、又はフォーラム上もしくはフォーラムを介して他の人と連絡しない場合は、実質的に連邦刑法上の責任を負うリスクはない。そこにいるだけであったり、架空の人物になりすましたり、フォーラムに参加してコミュニケーションをとるために偽名を使ったりすることは、その行為が詐欺やその他の罪を犯す手段ではなく、かつ、許可された方法でアクセスをする限り、連邦刑法に違反しない[57]。とはいえ、許可なく実在の人物になりすますことは、法的に問題があるとされる可能性がある。なりすましをされた実在の人物と、なりすましの下で行われた行為に応じて、セキュリティ担当者は刑事及び民事訴訟に直面する可能性がある[58]。

B.　シナリオ2：犯罪者フォーラムに問い合わせの投稿をする

さらに積極的に情報を収集するために、フォーラムに違法行為に関する情報を求める問い合わせを掲載すれば、犯罪捜査の対象になる危険性が高まる。一般的な質問をするだけであればわずかな法的リスクしかもたらさないが、投稿内容が犯罪の実行を誘発するように見える場合、そのリスクは著しく増大する。コンピュータ犯罪の実行を誘発又は喚起した場合、

---

[56] CSIS/DOJ Active Cyber Defense Experts Roundtable（2015年3月10日）を参照。https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/05/18/CSIS%20Roundtable%205-18-15.pdf

[57] 上記II.C.を参照。

[58] 例えば、連邦政府の役員や従業員になりすます行為は、連邦刑法に違反する。18 U.S.C.§912参照[訳注6]。オンライン上でのなりすましについて民事訴訟上の請求原因となる旨定める州もある。例えば、WA ST 4.24 .790（2012年6月7日）（ワシントン州法 「電子的なりすまし―プライバシー侵害訴訟」）等を参照。

刑事責任を問われる可能性がある[59]。

ベスト・プラクティス II

• 情報収集活動中に発見した進行中又は計画中のコンピュータ犯罪に関する情報は、FBI の現地地方局又はサイバー・タスク・フォース、及び合衆国シークレットサービスの現地地方局又は電子犯罪タスク・フォース（ECTFS）の窓口―既に関係が構築されていることが望ましい―を通じて、法執行機関に速やかに報告すべきである。

• 一部の犯罪フォーラムでは、犯罪行為に加担するか、以前に犯罪を犯したことの証拠を提出することによって、真に犯罪者であることの立証を求められる場合がある。犯罪を助長するような有効かつ有用な情報は一切提供してはならない。そのような行為は、民事上又は刑事上の責任を負うことになりうる。

• 実行計画に法務部門を関与させるべきである。法的問題を発見し、回避するための助言を得ることができる。

担当者がフォーラムで入手した情報を使用して連邦犯罪を実行するつもりがなければ、フォーラムで質問をしたり助言を求めたりしても犯罪にはならない可能性が高い。しかし、法執行機関は犯罪行為が行われているフォーラムを調査するのであって、犯罪行為について質問したり助言を求めたりすることは、犯罪が発生している可能性があることを示している。したがって、犯罪行為に関する議論が含まれていると思われるフォーラム上での質問や他者との交流によって、担当者は、フォーラム又はその構成員を対象とした刑事捜査に巻き込まれる可能性がある。

このように担当者は捜査の対象になりうる。しかし、担当者や組織はそのリスクを軽減するための手段を講じることができる。

例えば、サイバー脅威の情報収集を実施するための運用計画を文書化し、オンラインでの活動や、情報がどのように収集され使用されたかの記録を残すことができる。犯罪捜査の場合、そのような記録は、その行為が正当なサイバーセキュリティ活動であったことを立証するのに役立ち、違法行為に関与した悪質な従業員の行為ではなく、企業の正当なサイバーセキュリティ活動を推進するために行為が実行されたと法執行機関が判断するのに役立ちうる。

---

[59] 誘発（solicitation）罪は、他者に特定の犯罪行為を実行させようとするものである[訳注 7]。カリフォルニア州刑法典§ 653 (f) (West 2016)等参照。コンピュータ犯罪を構成しうる行為の誘発に適用されうる連邦法はほとんどない。18 U.S.C. §2512 (1) (c) （違法電子傍受装置の広告）等参照[訳注 14]。しかし、多くの州には誘発に関する規定があり、当該行為がその州の管轄内で行われた場合に適用される可能性がある。さらに、誘発は、連邦犯罪やその共謀を幇助し教唆することにつながりうる。18 U.S.C.§2 (a)、§371 等参照[訳注 8]。

組織はまた、フォーラム（他の場所も含む）での従業員や請負業者の活動を指導するために、法律顧問の確認を経たポリシー及びプロトコルを確立させておく必要がある[60]。「行動規則」又は「コンプライアンス・プログラム」を確認確立しておくことにより、従業員が偶発的又は非意図的に組織やその従業員を法的に危険にさらしたり、セキュリティを侵害したりするリスクを回避できる。また、こうした情報収集活動を行う前に、現地の FBI 地方局又はサイバー・タスク・フォース、及び現地の合衆国シークレットサービス地方局又は電子犯罪タスク・フォースと継続的な関係を構築して、法執行機関に情報を提供することも有益である。法執行機関と早期に関与することは、担当者の活動が、法執行機関による進行中又は予期される調査を意図せず妨害しないようにすることにも役立つ。本文書の最後に各連絡先を記載している。

C. シナリオ 3：フォーラムでの他者との情報交換

フォーラムにおいてアクティブなメンバーになって情報を交換し、フォーラムの他のメンバーと直接コミュニケーションを取った場合、気を付けておかないと、すぐに違法行為に巻き込まれる可能性がある。潜伏中の担当者にとっては、担当者を信頼したフォーラム上の情報源から情報を引き出す方が簡単かもしれない。しかし、犯罪者の仲間として信頼を築き、善意を確立するためには、犯罪に利用できる有益な情報、サービス、ツールを提供する必要がありうる。そのような活動に従事することは、連邦刑法に違反する結果となる可能性が高い。

犯罪が起きたかどうかは、通常、個人の行為と意思による。担当者は、フォーラム上で他者の犯罪目的を助長するような行為は一切避けなければならない。たとえ犯罪を実行する意図を有していなくても、犯罪行為に関与している他者を助けることは、幇助や教唆の連邦犯罪となる可能性がある[61]。犯罪を助長し、犯罪の実行を容易にする意図で行われた積極的な行為を行った場合には、（それ自体は合法的な行為であっても）連邦犯罪の幇助及び教唆について責任を問われることがある[62]。関係する状況を十分に理解した上で犯罪的な思惑に積極的に参加することは、たとえその犯罪的思惑のあらゆる側面に同意しない場合でも、幇助・教唆責任を立証するのに十分である[63]。

---

[60] このようなポリシーや手続は、行動規則やコンプライアンス・プログラムと呼ばれることがあり、オンラインフォーラムへのアクセス方法、オンライン上の人物の設定、潜在的な犯罪行為への関与等のトピックについて方向性を提供しうる。

[61] 幇助・教唆に関する連邦法では、「（犯罪）実行を幇助、教唆、助言、命令、誘導し、もしくは（犯罪を）実行させ」又は「本人もしくは他人によって直接実行された場合、連邦犯罪となる行為を故意に惹起した」者は幇助・教唆で有罪となり、正犯として罰せられる。18 U.S.C.§2 参照[訳注 8]。

[62] *Rosemond v. United States*, 572 U.S. 65, 71 (2014)。

[63] 前掲 *Rosemond* 78 頁。

例えば、担当者がフォーラムのメンバーに対しマルウェアに関する技術的な支援を提供し、その助言がメンバーによるネットワーク侵害に有益であると知っていた場合であって、フォーラムメンバーがその計画を実行した場合、たとえ担当者がその*特定の*犯罪の実行を支援する意図がなかったとしても、幇助・教唆にかかる連邦刑法に違反する可能性がある。さらに、たとえ犯罪の実行を支援する意図がなく、最終的に犯罪の実行について起訴されなかったとしても、そのような支援行為は、損失が大きく不必要で執拗な捜査をもたらす可能性がある。

担当者はまた、共謀に関する連邦法に違反することも避けなければならない[64]。共謀に関する法令は、ある個人が一人以上の他者と連邦犯罪を実行することに合意した場合に適用される。法律の中には、その犯罪を助長するような外形的行為を誰かが行うことを構成要件としているものもある[65]。したがって、担当者がフォーラム上で情報を提供すること自体が連邦犯罪ではないとしても、犯罪が実際に起こるかどうかにかかわらず、担当者が犯罪が起こることに同意した場合には、犯罪の共謀に関与したことになりうる[66]。共謀に関する一般法は、共謀に関与した一部の構成員が共謀を超え犯罪を目的とした行為を実行したことを要求しているが、その行為自体が犯罪である必要はなく、またその行為が刑事責任を問われた者によって実行される必要もない[67]。CFAA は、共謀を超えた外形的行為を要求せず、CFAA 違反を行うことの合意で足りるとする独自の共謀罪規定を有している[68][訳注 9]。とはいえ、担当者に犯罪を実行する意図がなく、実際に犯罪目的の達成を他者と合意していない場合には、担当者は、連邦法に基づく犯罪としての共謀には参加していないことになる[69]。

要するに、セキュリティ担当者は、他の者が犯罪を実行するのを助けたり、犯罪が起り得ることに同意したりするような行動をとらないように注意すべきである。この種の情報収集活動に従事する者は、犯罪行為を容易にするために存在するオンラインサイトで、犯罪を計画している可能性のある個人とやりとりをして、活動していることに留意すべきである。担当者は、そのような犯罪を進展させる可能性のある真の、正確な、又は有用な情報を提供することを避けるべきである。

---

64 18 U.S.C.§371[訳注 8]。共謀に関する連邦法は、「連邦犯罪を犯し、又は合衆国その他の省庁を欺罔するために、何らかの方法、目的により、2 人以上の者が共謀し、そのうち 1 人以上の者が共謀の目的を達成するための何らかの行為をした.」ことを犯罪と定める。同条。

65 *Braverman v. United States*, 317 U.S. 49, 53 (1942).

66 *Ocasio v. United States*, 136S. Ct. 1423, 1432 (2016) 参照。(「共謀者らが、その背後にある犯罪が、それを実行する能力のある共謀者の一員によって行われることに合意したことを証明すれば十分である。言い換えれば、各共謀者は、*共謀者の誰か*が実体的犯罪の各構成要件を満たすことを具体的に意図していたことが必要である。」)。

67 前掲 *Braverman*, 317 U.S.、53 頁参照（「共謀罪は、外形的行為の証拠がない限り、起訴できないところ、共謀者のうちの一人の行為で足り、それ自体が犯罪である必要はない。」）。

68 18 U.S.C. § 1030(b)参照。

69 *United States v. Mahkimetas*, 991 F.2d 379, 383 (7th Cir.1993)（連邦法上の共謀罪には、合意された犯罪行為を実行しようとする個人間の合意を必要とする）。

担当者が連邦法上の犯罪の捜査の対象となった場合、捜査官は、ある程度客観的及び状況的証拠を用いて、意図を認定しようとするであろう。従って、上述のように、担当者及びその雇用主は、フォーラムにおける担当者の行動及び担当者の活動の正当なビジネス目的の記録を保管し、正当な動機及び違法行為の拡大を回避する措置をとったことを立証できるようにしておくべきである。

IV. サイバーセキュリティのための盗難データや脆弱性の購入

一部のサイバーセキュリティ企業は、顧客へのサービスとして特定の種類の情報を求めてダークマーケットを監視している。売りに出されている顧客記録やその他の種類の機密顧客データを探索する場合もある。ダークマーケットでの当該情報の販売は、事前に検知されていないデータ侵害の兆候を示す可能性があるからである。また、顧客のネットワークや製品をターゲットとしたマルウェアやセキュリティの脆弱性を探索することもある。これは、顧客のデータや資産が悪用の対象となる可能性を示す。こうした種類の情報がオンラインで販売されていることが判明した場合、サイバーセキュリティ企業は、ダークマーケットから当該情報を削除をするために、当該情報の購入を試み、販売者との取引を仲介する場合がある。

ダークウェブ上で盗品やセキュリティの脆弱性を販売する匿名の当事者と交渉することは、多くの望ましくない結果を生む大きなリスクとなる。例えば、購入者が支払いをしたにもかかわらず、販売者が約束したデータを提供しなかったり、契約に違反してデータのコピーを他者に販売したり、盗まれたデータすべてのコピーを所有又は管理していないためデータのさらなる拡散を防ぐことが不可能であったり、収益を他の犯罪に充てたり、さらには、購入者のシステムを侵害することを意図したトロイの木馬を組み込んだデータや脆弱性が生成されたりする可能性がある。これらのリスクは、被害組織が、ダークマーケットの商人と取り決めをして金員を詐取された後、当該インシデントを当局に報告するのをためらうだろうと、違法な商品を販売する商人が予期していることによって、さらに増大する。

また、ダークマーケットの商人に金員を詐取された組織は、販売者が匿名であったり、米国裁判所の管轄外の国に所在していたり、追跡不能・取消不能の支払方法を使用して支払われたりことが多いため、法的手段がほとんどない可能性が高い。これらすべての理由から、組織はこのような方法で盗まれたデータやセキュリティの脆弱性を入手しようとする際は注意する必要がある。

それでも、組織によっては、リスクを上回る成果が得られると予測し、これらのリスクを引き受けることをいとわない場合もある。例えば、これまで検出されていなかったデータ侵害

の性質と範囲を評価し、さらなる喪失を回避するためにネットワークにパッチを適用できるよう盗難データのコピーの取得を求める場合がある。また、サイバーセキュリティ企業は、盗まれた情報を利用して、他の企業が自社ネットワークをより適切に保護するために利用できるインテリジェンス報告書を作成しうる。

有効性と実用性に関する疑問はさておき、個人の盗まれたデータ（サイバーセキュリティ企業の場合は、盗まれたデータの購入を承認したデータ所有者のデータ）を購入すること場合、考慮すべき法的な問題が生じる。まず、連邦検察官は、これまで、盗まれた自己のデータを購入し、又はセキュリティ脆弱性を購入することを試みただけでは通常起訴していない。しかし、これらの活動を行う者は、以下に述べる法的リスクを考慮すべきである。

A. シナリオ1：盗難データの購入

このセクションのシナリオでは、盗まれたデータの購入に関する、法的分析に影響を与える可能性のある様々な側面に焦点を当てる。

- 購入者がデータの正当な所有者であるかどうか：:盗まれたデータはデータ所有者、又はデータ所有者が認めた代理人によって購入されるのか。
- 販売されているデータの種類：盗まれたデータは、連邦法において譲渡又は所有が禁止されている種類の情報か（盗まれたクレジットカード情報や営業秘密など）。
- 販売者の身元：連邦法でデータ所有者が取引を行うことを禁じられている販売者か。

以下の各シナリオでは、前述の情報収集シナリオで説明した仮定ーすなわち、セキュリティ担当者に関する仮定、アクセスされるフォーラムの性質に関する仮定、及びそのようなフォーラムにアクセスする手段に関する仮定―と同様の仮定を用いる[70]。しかし、ここでの議論は、担当者がサイバーセキュリティ企業の顧客のものと思われるデータが売りに出されていることを発見した場合に焦点を当てている。これらの仮定では、担当者は、ダークウェブサイトの指示に従って販売者に連絡し、顧客の承認を得てデータの購入を申し込む。この仮定では、支払いが行われ、販売者が合意どおりにデータを提供することも前提としている[71]。

1. データの所有権

前述したように、自己の盗難データを購入しても、通常は連邦政府による起訴のリスクはほとんどない。しかし、購入者が盗難データを見直しているうちに、ダークマーケットの販売者によって生成されたデータの一部に他社に属するデータが含まれることを発見する。そ

[70] 上記 2-4 頁参照。
[71] この法的分析では、取引が成功したと仮定している。（しかし）上記の理由により、オンライン上で盗品を購入する試みが期待した結果をもたらすという保証はない。

して、購入者の盗難データには、他のデータ侵害の被害者から盗まれた可能性のあるデータが混在していることが判明する。

もし購入者が、購入した盗難データが他人のものであることを知らず、知りうる理由もなかった場合、それを購入したことで刑事訴追を受ける可能性はほとんどない。以下に述べる例外はあるものの、盗まれたデータを所有又は取り扱ったことに対する刑事責任は、一般に、そのデータを不法な方法で使用する意図を必要とするが、本文書では、担当者にはそれがないものと仮定している。例えば、アクセス機器詐欺法は詐欺の故意を必要とし、営業秘密の窃取に関する規定は情報を所有者以外の誰かの経済的利益に供する意図を必要とする[72]。

しかし、他者の盗難情報を許可又は権限なく購入することは、購入者の意図について疑義を生じさせ、購入者の動機を判断するための調査を招くおそれがある。このリスクに対処するために、購入データに所有する権利がない情報が含まれていることを認識した場合、購入者はそれを速やかに分離し、それ以上アクセス、確認、使用しないようにする必要がある。その後、購入者は、直ちに法執行機関に連絡してデータを提供するか、分かる範囲で実際のデータ所有者にそのデータを所有していることを知らせるべきである。これらの措置は、刑事訴追に値する犯罪の意図が一切ないことを示すのに役立つ。所持するに至った盗難データの所有者に連絡する場合は、脅迫と誤解されるような方法で連絡してはならない[73]。

2. データの性質

また、盗まれたデータの種類によって、そのデータの購入を禁止している刑事法令があるかどうかも決まる。前述のように、ダークマーケットで販売される傾向のある盗難データ (パスワード、アカウント番号、その他の個人識別情報など) に関連する連邦の刑事法令の多くは、別の犯罪を助長する意図（例えば、詐欺のために当該情報を使用する意図など）がある場合に限り適用される[74]。このため、犯罪の動機を持たない盗難データの購入者は、これらの法令に基づいて起訴される可能性は低い。

知らずに他人の盗難情報を購入しても、通常、刑事責任を問われる可能性は低いが、故意に他人の盗難データを本人の承認なしに購入すれば、法的なリスクが発生する可能性がある。特に営業秘密が含まれている場合は、購入者の動機に疑義が生じ、法執行機関や正当なデータ所有者による調査の対象となる可能性が高くなる[75]。

---

[72] 18 U.S.C. §§ 1029(a)(1)-(8), (10); 18 U.S.C. § 1832(a)参照[訳注 2、訳注 10]。

[73] サイバーセキュリティ担当者が所持するに至った盗難データの所有者は、担当者が盗難データの返還に条件を課そうとする場合、それを脅迫と解釈しうる。担当者は、盗まれたデータの返還について、担当者のサービスの購入や、価値のあるその他の要求の充足を条件とすることを回避すべきである。

[74] 18 U.S.C. §§ 1029(a)(1)-(8), (10)参照[訳注 2、訳注 10]。

[75] 「『営業秘密』とは、すべての形式及び種類の財務情報、ビジネス情報、科学情報、技術情報、経済情報、工学情報であって、パターン、計画、編集、プログラムデバイス、製法、設計、プロトタイプ、方

意図せず営業秘密を購入することは、営業秘密窃盗法（以下、「同法」）に違反しないが、盗まれたことを知りながら、又は許可なしに取得した営業秘密[76]を受領、購入、又は所持することは、同法の他の要件を満たす場合、同法違反となりうる。同法は、営業秘密の所有者を害することを意図し、又はそれを知って、営業秘密の正当な所有者以外の者の利益になるよう営業秘密について譲渡その他の処分をすることを禁じている[77]。したがって、当該情報の使用は、いかなる場合であれ、当局又は営業秘密所有者による調査の対象となりうる。同法は民事上の請求を定めており、刑事訴追が否定された場合でも、営業秘密の所有者は、民事訴訟を起こすことが可能である。

上記で推奨されるように、他者に帰属する盗難データを意図せず購入したことで捜査及び起訴されるリスクを軽減する最善の方法は、販売者において購入者に帰属しないデータを提供しないようにすることの他、法執行機関及び/又は正当なデータ所有者に速やかに連絡して、購入者とは関係のない当該データを引き渡すことである。そうすることで、購入者の意図しないデータの所有が犯罪行為と誤解されるリスクを最小限に抑え、民事責任を軽減しうる。

3. 売主の性質

特定の個人や団体と金融取引をすることは、法律に違反する可能性がある。例えば、18 U.S.C.§ 2339B[訳注 11]は、外国のテロ組織と指定されたグループに重要な支援を提供すること、又は提供しようとすること、もしくはそのような共謀を行うことを禁じている[78]。第 2339B 条に違反したというためには、被疑者が取引先組織とテロとの関係を知っている必要がある。ただし、被疑者が当該組織のテロ活動を支援する具体的な意図を有していることまでは必要ない[79]。したがって、担当者において販売者がそのような外国のテロ集団の一員であることを知りながら盗難データを購入した場合、当該担当者は第 2339B 条違反となるお

法、技術、プロセス、手順、プログラム、又はコードを含み、有形であるか無形であるかを問わず、また物理的、電子的、グラフィック、写真、又は書面によって保存、編集、又は記録されているかどうかを問わないものであって、
(A) その所有者が当該情報を秘密にするための合理的な措置を講じており、かつ、
(B) 当該情報が、当該情報の開示又は利用により経済的価値を得ることができる他の者に一般的に知られておらず、かつ、他の者が適切な手段により容易に確認することができないことによって、実際的又は潜在的な独立した経済的価値をもたらすものをいう。」18 U.S.C. § 1839 (3)

[76] 18 U.S.C. § 1832(a)(3) [訳注 10]。

[77] 1832 条(a)(2) は、営業秘密をその所有者以外の者の経済的利益に供する目的で、かつ、その営業秘密の所有者を害することを意図し、又は知って、不正な複写、複製、スケッチ、描画、アップロード、改変、破棄、コピー、転送、送信、郵送、通信又は譲渡することを禁止する。

[78] 第 2339B 条に基づく責任は、ある団体が移民国籍法第 219 条に基づいてテロ組織に指定されたこと、その団体が移民国籍法第 212 条 (a)(3)(B) に定義されるテロ活動を行った若しくは行っていること、又はその団体が外国関係許可法第 140 条 (d)(2) に定義されるテロリズムを行った若しくは行っていることについて、別のある者が悪意である（認識している）ときに適用される。

[79] *Holder v. Humanitarian Law Proj*., 561 US 1, 17 (2010)

それがある。

国際緊急経済権限法（IEEPA）[80][訳注 12]の下では、同様の禁止措置により、購入者は米国政府によって指定された特定の個人又は団体から盗難データを購入することが禁じられている。ここ数年、米国政府は、サイバー関連の不正行為を含む国家安全保障上の理由から、イラン、北朝鮮、ロシアの個人及び団体を制裁する大統領命令を出している[81]。これらの大統領命令及び規則は、特に、指定された対象者との貿易又は経済取引を禁止する。とりわけ IEEPA は、これらの大統領命令や規制、及びそれらが定める経済取引や貿易取引の禁止に故意に違反することを犯罪としている。

司法省の国家安全保障部は、IEEPA の犯罪違反を訴追しているところ、IEEPA の故意の基準は、上記シナリオの事実に基づき IEEPA の下で担当者を刑事訴追する上で重大な障害となる。ダークマーケットで盗難データを販売する者の身元は、匿名のオンライン上の人格で隠されている可能性が高いため、盗難データの販売者の素性が購入者に知られ、又は知られうる可能性は低い。購入者が販売者の身元を知らない、つまり販売者が経済制裁又は貿易制裁の対象であることを知らない場合、故意の証拠を必要とする刑事訴追は不可能であろう。米国家安全保障部の対諜報・輸出管理課の連絡先は(202) 233-0986 である。

しかし、IEEPA の下では民事責任も課される可能性がある。米国財務省海外資産管理室（OFAC）は、米国の経済・貿易制裁制度の民事的な執行について責任を負う。OFAC は、米国の外交政策上及び国家安全保障上の目標に基づいて経済・貿易制裁を実施、執行する。IEEPA の民事的な執行は、「厳格責任」に基づいて課されることがある。すなわち、当事者は、貿易又は経済制裁の対象となった個人又は団体と取引を行っていたことを知らなかった場合であっても、民事責任を負う可能性がある。OFAC の IEEPA 制裁の下で不正な取引を行った場合、民事上の制裁金が課される場合がある。制裁金の法定最高額はインフレ率に応じて毎年調整される[82]。

企業は、経済制裁や貿易制裁の対象となっている個人や団体と取引していないことを保証するためにあらゆる努力をすべきである。OFAC は、経済制裁や貿易制裁の対象となっている個人、地域、国と取引をするリスクを軽減するために、リスクベースのコンプライアンス・プログラムを実施することを企業に奨励している。OFAC は、一般市民を支援するために、

---

[80] 50 U.S.C. § 1705

[81] 大統領命令 No. 13694「重大な悪意のあるサイバー活動に従事する特定の者の資産の凍結」（Blocking the Property of Certain Persons Engaged in Significant Malicious Cyber-Enabled Activities）, 80 Fed. Reg. 18077（2015 年 4 月 1 日）参照[訳注 13]。

[82] 法定最高額は、2015 年連邦民事制裁金インフレ調整法改正法によって定められている。Public Law（公法）114-74 第 701 条参照。

リスクベースの制裁遵守プログラムの 5 つの必須要素の枠組みを組織に提供することを目的とした文書 「A Framework for OFAC Compliance Commitments」（OFAC コンプライアンス取組みのための枠組み） をウェブサイトで公開している。

合理的なコンプライアンス・プログラム（又は「行動規則」）（取引相手である外国企業が経済・貿易制裁の対象となっているかどうかをチェックする措置を含む）を整備することは、IEEPA 上の刑事責任を回避する賢明な方法であり、民事責任の可能性を軽減することもできる。また、OFAC は、「Sanctions List Search[83]」（制裁リスト検索） や 「Resource Center web pages for Sanctions Programs and Country Information」（制裁プログラム及び制裁国の情報に関するウェブページのリソースセンター） など、米国の制裁の対象となっている特別指定国民・凍結者（Specially Designated Nationals and Blocked Persons; SDN）を特定するためのツールも提供している[84]。これらの情報を参照することは、IEEPA その他の制裁関連法令に基づく民事又は刑事上の責任を負うリスク軽減する上で有益であろう。また、OFAC の任意自己開示プログラムや、明白な違反に対する適切な対応を決定する際に OFAC が一般的に考慮する要素など、OFAC による米国経済制裁の執行に関する詳細な情報については、経済制裁執行ガイドライン（31C.F.R.第 501 部付録 A）を確認することが推奨される。[85]

OFAC への問い合わせは、OFAC ホットラインフリーダイヤル 1(800)540-6322、普通電話(202) 622-2490、又は電子メール ofac_feedback@treasury.gov.で受け付けている。さらに、特定のライセンス申請は、OFAC のウェブサイト www.treasury.gov/ofac からオンラインで提出することができる。保留中のライセンス申請に関する問い合わせは、(202) 622-2480 で受け付けている。

シナリオ 2：脆弱性の購入

ダークマーケットでサイバー脅威インテリジェンスを収集している最中に、セキュリティ脆弱性が販売されていることを発見した場合、特に脆弱性が担当者の顧客を対象としている場合、それらの脆弱性を関連ベンダーに開示し、又は脆弱性の悪用を防ぐためのパッチを開発するために、担当者がそれらの購入を決断する場合がある。また、マルウェアの新しい亜種を分析し、又はイルススキャン製品で使用するためのシグネチャを開発するために、ダークマーケットで販売されているマルウェアの新しい亜種を探す担当者もいる。

セキュリティ脆弱性とマルウェアはコンピュータ犯罪のために頻繁に使用され、犯罪行為

---

[83] https://sanctionssearch.ofac.treas.gov/
[84] https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx、https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx.
[85] https://www.ecfr.gov/cgi-bin/textidx?SID=093f4d5ea37955ea6a767ad337f4f75d&mc=true&tpl=/ecfrbrowse/Title31/31cfr501_main_02.tpl

を支援するために販売された場合、それは連邦犯罪であるが、脆弱性やマルウェアの単なる*購入*は、その行為単体で犯罪の故意のない限り一般的に違法ではない。しかし、言及すべき二つの例外がある。第一に、電子通信をひそかに傍受するように設計されたソフトウェアの所持又は販売は、「電子、機械その他の装置の設計が、有線、口頭又は電子通信の秘密裡の傍受の目的に主として有用であることを知り、又は知りうる場合に、当該装置」の意図的な所持を禁止する通信傍受法に違反する可能性がある[86]。電子通信を傍受するように設計された特定のマルウェアは、この定義に該当する可能性があり、したがってその所持は違法となる[87]。第 2512 条に該当する可能性のあるマルウェアを購入した場合の法的リスクを最小限に抑える最善の方法は、取引が発生する前に法執行機関と調整することである。

第 2 の例外は、販売者が指定された外国のテロ組織であるか、IEEPA の下で経済制裁又は貿易制裁の対象となっている個人又は団体であるために購入が禁止されている場合である。これらの問題は、盗難データを購入する際に生じるものと同じである。これについては IEEPA 等の当局の下での法的責任とそれに対処する最善の方法を説明している上記の議論を参照のこと。

V. 結論

本文書は、民間部門のサイバーセキュリティ担当者が、犯罪フォーラムに関与するサイバーセキュリティ活動を行う際に連邦刑事法に違反することを回避するために取るべき手段と考慮すべき問題を特定することにより、担当者を支援することを目的としている。このような活動が適切に実施されれば、組織のサイバーセキュリティに対する準備体制が改善され、サイバーセキュリティの脅威に効果的かつ合法的に対応するのに有用である。

---

[86] 18 U.S.C. § 2512(1)(b) [訳注 14]。

[87] *Luis v. Zang*, 833 F.3d 619, 635 (6th Cir. 2016)（オンライン通信をひそかに傍受するために使用されたソフトウェアの製造者と、そのソフトウェアを妻の通信を傍受するために使用した夫に対する第 2512 条に基づく民事上の請求を認容）[訳注 15]。通信傍受法の適用の詳細については、コンピュータ犯罪に関する CCIPS のこれまでの出版物、例えば、U.S. Department of Justice Office of Legal Education（米司法省法教育局）「Prosecuting Computer Crimes（コンピュータ犯罪の起訴）」59-72(2009)を参照。

法執行機関への連絡方法

- FBI の現地地方局または合衆国シークレットサービスの現地地方局との関係があらかじめ確立されている場合は、インテリジェンス収集と盗難データの取戻しを実行する計画を通常の連絡先に通知し、差し迫った犯罪、進行中の犯罪、または過去の犯罪に関する情報がある場合はそれを報告する。
- 以下の URL にて最寄りの FBI または合衆国シークレットサービスの現地地方局を検索できる。
  https://www.fbi.gov/contact-us/field-offices
  https://www.secretservice.gov/contact/
- 詳細情報及びリソースについては、以下のウェブサイトを参照のこと。
  https://www.justice.gov/criminal-ccips

4.2　米国司法省「オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項」の解説

同ガイドラインの翻訳に訳注をつけた部分につき米国法の見地から解説を付加する。

訳注 1

ダークマーケットに不正アクセスした場合、CFAA（18 U.S.C.§1030「コンピュータに関連した不正及び関連する行為」）違反となりうると指摘されている。具体的に 18 U.S.C.§1030(a)の概要[88]を見ると以下の通りである。

(a) 以下のいずれかの行為をした者は罰せられる。

(1) 無権限で又は授与されたアクセス権限を超過して，コンピュータにアクセスし、政府によって保護された情報を取得し、故意に他者に送信等した者。

(2) 権限なく、又は、権限を超えてコンピュータに故意にアクセスし、それによって、以下の情報を取得した者。

(A) 金融機関もしくは 15 巻 1602(n)条に定めるカード発行者の金融記録に含まれる情報、又は、公正信用報告法（15 U.S.C.§1681 以下）に定める消費者報告機関における消費者に関するファイルに含まれる情報、

(B) 合衆国のいずれかの省庁からの情報、

(C) いずれかの保護されたコンピュータ（専ら金融機関や合衆国政府が用いるコンピュータ又は州際もしくは外国との取引もしくは通信に用いられるコンピュータ）からの情報

(3) 故意に、権限なく、合衆国政府のコンピュータであって、一般公衆がアクセスできないものにアクセスし、合衆国政府の使用に影響を及ぼした者

(4) 情を知って、詐欺の意図で、保護されたコンピュータにアクセスし、その行為が詐欺を助長するものであり、何らかの価値のあるものを取得した者

(5) (A) 情を知って（knowingly）、プログラム、情報、コード又はコマンドを送信し、この行為によって、意図的に、権限なく、保護されたコンピュータに対し損害を与えた者

(B) 意図的に(intentionally)、権限なく、保護されたコンピュータにアクセスし、この行為によって、無謀に（recklessly）損害を惹起した者

(C) 意図的に(intentionally)、権限なく、保護されたコンピュータにアクセスし、この行為によって、損害及び損失を惹起した者

(6) 情を知って、詐欺の意図で、コンピュータを無権限でアクセスできるパスワード又

[88] 逐語訳ではないため注意されたい。原文は、https://www.law.cornell.edu/uscode/text/18/1030 参照。

はそれに類似の情報を譲渡その他の処分をした者であって、

(A) 当該譲渡等が州際取引又は外国取引に影響を及ぼした場合

(B) 当該コンピュータが合衆国政府によって用いられるものである場合

(7) 金員その他の価値ある物を人から奪う意図で、以下を含む通信を、州をまたいで又は外国との間で送信した者

(A) 保護されたコンピュータに損害を生じさせるとの脅迫

(B) 保護されたコンピュータから権限なく、又は権限を超えて情報を取得するとの脅迫

(C) 保護されたコンピュータの損害に関連して金員その他の価値ある物の要求

正当なサイバーセキュリティ目的でダークマーケットに不正アクセスした場合、該当しうるのは、18 U.S.C.§1030(a)(2)(C)、(a)(4)である。CFAA は、従前よりかなり拡張的に適用されてきているという背景があるため[89]、十分に注意する必要がある。

訳注 2

アクセスデバイスとは、「金員、物品、サービスその他価値ある物を取得するために、又は、資金移動を開始するために（専ら書面に端を発する移動を除く）、それ単体で、又は他のアクセスデバイスと合わせて用いることのできる、カード、プレート、コード、アカウント番号、携帯端末のシリアルナンバー（ESN）、携帯端末の識別番号、個人識別番頭、その他の電気通信サービス・施設・装置の識別子、その他のアカウントにアクセスのための手段」を意味する（18 U.S.C.§1029(e)(1)）。例えば、アカウントにアクセスするためのパスワードもアクセスデバイスに該当する。

18 U.S.C.§1029（「アクセスデバイスに関連した不正及び関連する行為）は、アクセスデバイスの所持等を犯罪と定める。すべての類型について、「*情を知って（knowingly）、かつ、詐欺の意図をもって*」という主観的要件が要求されており、サイバーセキュリティ目的を有していることにより自動的にこの主観的要件がないということにはならないが、犯罪の動機を持たずにダークマーケットにアクセスし、盗難データ等を購入する場合には、これに基づき起訴される可能性は低い。

訳文は以下の通りである[90]。

(a) 以下に該当する者は、当該行為が州際取引又は外国商取引に影響する場合には、本条(c)

---

[89] 「権限なく（無権限）」という構成要件について、使用約款違反の場合も含まれるとされており、使用約款違反が民事上の責任のみならず、刑事上の責任につながることについて強い批判があるものの法改正には至っていない。*United States v. Swartz,* 357 F.2d 322（被告人は、ハーバードの学生で論文アーカイブである JSTOR のアカウントを所持していたところ、MIT のコンピュータを使用して JSTOR にアクセスし、そこから 400 万以上の記事を自己のパソコンに自動ダウンロードしようとし、その過程で JSTOR のコンピュータの機能を損ない、MIT のサーバーをダウンさせ、MIT の他のコンピュータからのアクセスを不可能にしたことにより、通信詐欺（wire fraud）、コンピュータ詐欺、不正アクセスによる情報取得、不正アクセスによるコンピュータ損害等により逮捕、起訴され、公判中に被疑者が自殺した。）参照。

[90] なお、1029 条(b)は、同条(a)の行為の未遂、共犯についての定めである。

に定める法定刑によって罰せられる。

(1) 情を知って（knowingly）、かつ、詐欺の意図をもって、一つ以上の偽アクセスデバイス（counterfeit access devices）を製造、使用、不正に売買をした者

(2) 情を知って（knowingly）、かつ、詐欺の意図をもって、1 年間において一つ以上の偽アクセスデバイスを不正に売買し、又は使用し、かつ、その行為によって、当該期間中に累計 1000 ドル以上の価値を得た者

(3) 情を知って（knowingly）、かつ、詐欺の意図をもって、15 個以上の偽アクセスデバイス又は無権限アクセスデバイス（unauthorized access devices）を所持する者

(4) 情を知って（knowingly）、かつ、詐欺の意図をもって、デバイス製造装置（device-making equipment）を製造、管理、所持、不正に売買した者

(5) 情を知って（knowingly）、かつ、詐欺の意図をもって、一つ以上のアクセスデバイス（access devices）を一人以上の者に発行し、1 年の間に 1000 ドル以上の価値を取得する取引を成立させた者

(6) アクセスデバイスの発行者の権限なく、情を知って（knowingly）、かつ、詐欺の意図をもって、以下を人に求めた者

(A) アクセスデバイスの提供、又は、

(B) アクセスデバイスに関する情報若しくはアクセスデバイスを取得するためのアプリケーションの販売

(7) 情を知って（knowingly）、かつ、詐欺の意図をもって、通信サービスの無権限使用を取得するために改ざん又は変更された通信装置を使用、製造、不正に売買、所持、管理する者

(8) 情を知って（knowingly）、かつ、詐欺の意図をもって、スキャニングレシーバー[91]を使用、製造、取引、管理、保有、所持する者

(9) （略）

(10) クレジットカードの加盟店又はその代理人の権限なく、情を知って（knowingly）、かつ、詐欺の意図をもって、他人に、アクセスデバイスによって生成された 1 つ以上の証拠又は記録を、支払のために、加盟店又はその代理人に対し、提示させた者

訳注 3

18 U.S.C.§1030 (e)(2)(B)は、CFAA の域外適用の根拠規定である。訳文は以下の通りである

(e)(2) 「保護されたコンピュータ」とは、以下のいずれかのコンピュータを意味する。

(A) （略）

[91] 「スキャニングレシーバー」とは、119 章に違反して音声通信（wire communication）もしくは電気通信（electronic communication）を傍受するために、又は、携帯端末のシリアルナンバー（ESN）、携帯端末の識別番号、電気通信サービス・装置・ツールのその他の識別子を傍受するために使用されるデバイス又は装置を意味する。

(B)　州際間又は外国との取引又は通信に使用されるものであって、米国の州際間又は外国との取引又は通信に影響を及ぼす方法で使用される米国外に所在するコンピュータも含む。

訳注 4

*hiQ Labs, Inc. v. LinkedIn Corp.*事件は、ボットを使用して LinkedIn の公開プロフィール情報を web スクレイピングしていたデータ分析会社 hiQ Labs, Inc.に対して、LinkedIn が停止通告書（cease-and-desist letter）を送付したことについて、hiQ Labs, Inc.が、LinkedIn による停止通告を解除する旨の仮処分（preliminary injunction）及び CFAA 違反等がないことの確認判決を求める訴訟を起こしたものである。地裁において hiQ Labs, Inc.の求める仮処分が認められたところ、連邦高裁においてもこれを支持する判決を下した。

仮処分に対する控訴の判断の基準は、原判決が裁量の範囲を逸脱したか、という控訴人にとってはハードルの高いものであって、仮処分の要件は、(1)本案で勝訴の可能性があること、(2)仮処分がなければ回復不能な損害（irreparable harm）が生じるおそれがあること、(3)利益較量（balance of equities）上仮処分をすべきこと、(4)仮処分が公共の利益に資すること、であり[92]、本件では、LinkedIn に使用を中止されると原告の事業が停止してしまうという強力な事情があったため（(2)の要件）、公開情報についての web スクレイピングが CFAA 違反にあたらないかについて直接判断したものではない。もっとも、停止通告書を受領した後のスクレイピングは CFAA 上の「無権限（without authorization）」にあたり CFAA 違反にあたりうるとの LinkedIn の主張に対し、詳細な検討を加えている。その中で、最近の高裁判決では企業の利用規約違反を「無権限」とする契約ベースの解釈が否定されていると指摘した上で、CFAA は、(1)アクセスが一般に公開されアクセスに許可が必要のない情報、(2)アクセスに許可が必要であり許可が与えられた情報、(3)アクセスに許可が必要であり許可が与えられていない情報を想定しており、本件の情報は(1)にあたるとし[93]、一般に公開されたデータへのアクセスは CFAA 上の無権限アクセスにあたらないと結論づけたことは注目に値する。

現在、仮処分の判断につき最高裁に係属中である[94]。

これに対し、*Konop v. Hawaiian Airline,Inc.*事件は、被告会社の労働組合の運営に反対する被告会社の従業員であった原告が、被告会社等を批判するサイトをクローズトの環境で立ち上げ、会社幹部に見せない等と定めた利用規約に同意した他の従業員に限りアカウントとパスワードを付与していたところ、一部の従業員がその付与されたアカウントとパスワードを幹部に渡し、被告会社が原告のサイトを数十回にわたり閲覧していたことにつき、原告が通信傍受法や保存通信法（Stored Communications Act; SCA）違反を主張して提訴したと

---

92 Munaf v. Geren, 553 U.S. 674, 128 S.Ct. 2207, 2218-19 (2008)

93 *hiQ Labs, Inc. v. LinkedIn Corp*., 938 F.3d 985 (9th Cir. 2019)、29-30 頁。
https://law.justia.com/cases/federal/appellate-courts/ca9/17-16783/17-16783-2019-09-09.html

94 https://www.natlawreview.com/article/hiq-files-opposition-brief-supreme-court-linkedin-cfaa-data-scraping-dispute

いう事件である。なお、通信傍受法違反で認められる民事上の損害額は SCA 違反の場合よりも大きいためにいずれの法律違反が認められるかが問題となった。この点、高裁は、同サイトは、「電子通信（electronic communication）」にあたるが、傍受（interception）は送信中のデータを見ることであって保存中のデータを閲覧することは含まれないとして通信傍受法違反は認めなかった。しかし、SCA では、「電子通信サービスが提供される施設に故意に権限なく（without authorization）アクセス」した場合を法令違反としているところ[95]、「無権限」の定義には触れずに原被告とも無権限であることを認めているとして被告の SCA 違反の主張を認めた。ここでは、他人のユーザアカウントとパスワードを使用して当該他人の承諾を得て制限サイトに入ることが「無権限」とされていることになる。

SCA も CFAA も「無権限」アクセスを違法としているところ、「無権限」の定義を定めていない[96]。そのため、本書注 77 にも述べたように、運営者の設定する利用規約違反も「無権限」とされて刑事責任が問われうる状況があり、それに対して批判があり改正の試みがなされているものの実現していない。2010 年に改訂（第 2 版）されたサイバー犯罪起訴に関する司法省発行のマニュアル「Prosecuting Computer Crimes（コンピュータ犯罪の起訴）」[97]では、18 U.S.C.§1030 において無権限アクセスと同様に犯罪とされる「権限超過（exceeding authorized access）」アクセスの要件である「権限超過」の立証として、利用規約（terms of use）違反を示せばよいとされている[98]。もっとも、同マニュアルにおいても、故意による利用規約違反のみで 1030(a)(2)(C)に基づく犯罪が成立するとすれば警察に過大な権限を付与し、インターネットを使用する市民に対する不意打ちとなる、と判示した United States v. Drew 事件（地裁判決）[99]について言及している[100]。最近は、利用規約違反は無権限としない旨の判例が出てきている[101]。

訳注 5

サイバー・タスク・フォース（CTF）は、FBI の 56 の地方局に存在する。情報共有、インシデント対応、共同法執行、インテリジェンス活動を通じて国内のサイバー脅威の捜査に携わることをミッションとする。全国サイバー捜査ジョイント・タスク・フォース（National Cyber Investigative Joint Task Force; NCIJTF）が連邦レベルでの捜査を担当するのに対し、CTF は州・地方レベルでの捜査を主に担当するが、NCIJTF とも常に連携を図っている[102]。

合衆国シークレットサービス電子犯罪タスク・フォース（ECTF）は、2001 年米国愛国者

---

[95] 18 U.S.C. § 2701(a)(1)

[96] *Konop v. Hawaiian Airline,Inc*., 302 F.3d 868, 876 (9th Cir. 2002)、注 8。https://caselaw.findlaw.com/us-9th-circuit/1167429.html#footnote_8

[97] 同ガイドライン注 46 記載の出版物である。

[98] 同マニュアル 8-9 頁。https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf

[99] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009)

[100] 同マニュアル注 3。

[101] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067 (9th Cir. 2016)（ウェブサイトの利用規約違反のみでは―他に何もない限り―CFAA 上の責任は成立しない。）、United States v. Nosal, 676 F.3d 854, 858 (9th Cir. 2012)（「CFAA について会社のコンピュータ使用制限違反や忠実義務違反まだ CFAA の適用を広く及ぼす解釈をする他の高裁の判断は説得的ではない。」）

[102] https://www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view

法において設置が義務付けられた組織で、教育機関、民間、地方・州・連邦法執行機関が協力して「重要インフラ及び金融決済システムに対する潜在的なテロ攻撃を含む様々な形態の電子犯罪を防止、検知、調査する」ための組織である[103]。

訳注 6

18 U.S.C.§912 は、連邦政府の役員や従業員になりすます行為を禁じる。訳文は以下の通りである。

> *連邦政府その他の省庁、その職員の権限を有する職員又は従業員であると偽り、もしくはなりすますこと、又はそのように偽り、なりすまして、何らかの金員、書類、文書その他の価値のある物を要求もしくは取得した場合、本章に従って罰金又は/及び 3 年以下の有期刑が科される。*

訳注 7

誘発（solicitation）罪は、通常、(1)他人に犯罪を実行させる目的で、 (2)他人に犯罪を実行するよう奨励し、又は他人に贈賄、要求、命令すること、を構成要件とする。日本法における教唆・幇助（aid and abet）では、他人（正犯）が犯罪の実行行為に出る必要があるが、誘発罪では正犯の実行行為は必要なく、単独で成立する。また、誘発を受けた者が犯罪行為を行う意思がない、又はできない場合でも成立する。さらに、共謀（conspiracy）罪では通常、犯罪の合意に沿った犯罪に向けた何らかの明白な行為（overt act）が必要であるが、誘発罪ではそれも不要である。

訳注 8

18 U.S.C.§2 は、正犯の定義を定める。訳文は以下の通りである。

> *(a) 連邦犯罪を犯した者、その実行を幇助、教唆、助言、命令、誘導し、もしくは実行させた者は、正犯として処罰される。*
>
> *(b) 本人もしくは他人によって直接実行された場合、連邦犯罪となる行為を故意に惹起した者は、正犯として処罰される。*

18 U.S.C.§371 は、共謀に関する規定であり、訳文は以下の通りである。

> *連邦犯罪を犯し、又は合衆国その他の省庁を欺罔するために、何らかの方法、目的により、2 人以上の者が共謀し、そのうち 1 人以上の者が共謀の目的を達成するための何らかの行為をした場合、本章に従って罰金又は/及び 5 年以下の有期刑が科される。（略）*

訳注 9

18 U.S.C. § 1030(b)は、18 U.S.C.§1030「コンピュータに関連した不正及び関連する行為」における共謀罪及び未遂罪の規定である。一般的な共謀罪には、共謀（合意）の他、1 人以上の者が共謀の目的を達成するための何らかの外形的行為をすることが必要であるが（18

---

103 https://obamawhitehouse.archives.gov/files/documents/cyber/United%20States%20Secret%20Service%20-%20Electronic%20Crimes%20Task%20Forces.pdf

U.S.C.§2)、§ 1030 の共謀ではそうした行為は必要なく共謀だけで足りるとされている。

したがって、この場合、構成要件は、共謀の事実と共謀の故意のみとなる。担当者がフォーラムにおいて他人とコミュニケーションを図り外観上共謀があるように見える場合には、共謀の故意がないことを示すことが、無用な捜査に巻き込まれないために非常に重要となる。したがって、同ガイダンスが指摘するように、セキュリティ目的で行動している担当者は、共謀の故意がないことを示すため、事前に FBI 等に連絡をし、行動規則を遵守し、活動履歴を記録するなどすることが重要となる。

18 U.S.C. § 1030(b)の訳文は以下の通りである。

(b) 本条(a)（18 U.S.C.§1030(a)）の犯罪を実行を共謀し、又はそれを実行しようとする者は、本条(c)項の通り罰せられる。

訳注 10

18 U.S.C. § 1832 は、営業秘密の窃取に関する規定であり、訳文は以下の通りである。

(a) *州際間取引又は外国取引で使用されている、もしくは使用されようとしている製品又はサービスに関連する営業秘密を、その所有者以外の者の経済的利益に供する目的（intent）で、又は、その営業秘密を害することを目的として、もしくはそれを知りながら、以下のことを知りつつ（knowingly）行った場合には、本条(b)に定める場合を除き、本章に従って罰金又は/及び10 年以下の有期刑が科される。*

(1) 当該情報を窃取し、権限なく私用に供し、横領し、持ち去り、もしくは隠し、又は詐欺、術策、欺罔により取得した場合

(2) 当該情報を、権限なく、複写、複製、スケッチ、描画、撮影、ダウンロード、アップロード、変更、破棄、コピー、転送、送信、郵送、通信又は譲渡した場合

(3) 窃取され、権限なく横領、取得、変更されたことを知りつつ、当該情報を受領、購入、所持した場合

(4) (1)から(3)に定める罪の未遂

(5) (1)から(3)に定める罪を犯すために、2 人以上の者が共謀し、そのうち 1 人以上の者が共謀の目的を達成するための何らかの行為をした場合。

このように、営業秘密の窃取の罪が成立するには、所有者以外の者の経済的利益に供する目的又は営業秘密を害する目的もしくは害することについての悪意（害することを知っていること）が必要である。したがって、セキュリティ目的で脆弱性等を購入する場合には、これらの主観的要件がないことを後日示すことができるように行動していくことが重要となる。

訳注 11

18 U.S.C.§ 2339B は、情を知って（knowingly）、外国のテロ組織に重要な支援又は資源

（material support or resources）[104]を提供すること、又は提供しようとすること、もしくはそのような共謀を行うことを禁じている。「情を知って（knowingly）」とあるため、犯罪が成立するためには、外国のテロ組織に支援を提供していること、すなわち取引の相手方が外国のテロ組織に関係していることを知っている必要はあるが、テロ活動を支援する具体的な意図を有している必要はない[105]。

よって、セキュリティ担当者やその帰属するセキュリティ企業が、取引の相手方についてテロ組織と関係していることを知らなければ、この犯罪は成立しないが、主観的な要件について無用な捜査に巻き込まれないためにも、そして、後述の民事的責任を追及されないためにも、コンプライアンス・プログラム等を厳格に遵守する必要がある。

なお、本罪には域外規定があり（同条(d)）、行為者が合衆国民である場合や、行為後に合衆国に滞在している場合、州際間取引や外国取引に影響する場合には適用されるとあるため、広範囲で適用されることに注意が必要である。

訳注 12

国際緊急経済権限法（International Emergency Economic Powers Act; IEEPA）は、1977 年に施行された法律である。対敵貿易法（Trading with Enemy Act）が大統領に戦時に限り対外的な経済制裁の権限を認めるのに対し、IEEPA は、戦時のみならず平時においても、米国外において、米国の国家安全保障、外交政策、経済に対し、異例かつ重大な脅威がある場合に[106]、大統領が国家緊急事態宣言を発付して、指定国・国民が関与する取引又は指定国等が利害関係を有する財産の使用、譲渡、輸出入等[107]を調査、規制、禁じる制裁を行うことを認めるものである[108]。2020 年 12 月時点で同法に基づき有効な国家緊急事態宣言は 40 あり[109]、2020 年 11 月に発令されたトランプ政権下における中国に対する証券投資の経済制裁も同法に基づくものである[110]。

IEEPA 違反、その未遂、共謀、教唆・幇助に対しては、民事上の制裁金及び刑事上の法定刑が定められている。なお、IEEPA に基づく刑事訴追は司法省の国家安全保障部（National Security Division）が、民事上の責任追及は米国財務省海外資産管理室（OFAC）が担ってい

---

104 「重要な支援又は資源（material support or resources）」とは、有形無形の資産又はサービスを意味し、通貨、通貨代替物、有価証券、金融サービス、宿泊施設、訓練、専門家の助言・支援、隠れ家、虚偽の文書・身分証明書、通信装置、施設、武器、致死物質、爆発物、人員（1 人以上の個人で行為者本人を含む）、輸送を含むが、医療品又は宗教的物質は含まない、とされる（18 U.S.C.§ 2339A(b)(1)）。

105 *Holder v. Humanitarian Law Proj*., 561 US 1, 17 (2010)

106 また、IEEPA に含まれる規定（50 U.S.C. § § 1701-1707）ではないが、米国国民によって開発された技術や専有情報をサイバー空間における経済スパイ又は産業スパイ活動を、情を知りながら要求、関与、支援、推進、又はそれにより不当に多大な利益を得た外国人について、大統領は、IEEPA に基づいて、その取引を禁じ、資産を凍結することができる、との規定もある（50 U.S.C. § § 1708(b)(1)(2)）。当該外国人は、特別指定国民・凍結者（Specially Designated Nationals and Blocked Persons; SDN）に登録される。

107 資産凍結も含まれるが、資産没収は戦時の場合に限られる（50 U.S.C. § § 1702(c)）。

108 50 U.S.C. § § 1701, 1702

109 梅川健「アメリカ大統領権限と緊急事態法制：国際緊急経済権限法と経済制裁を中心に」1-2 頁。（https://www.cistec.or.jp/publication/journal_mokuji/2101-04_tokusyuu01.pdf）

110 同経済制裁は、「共産党軍需企業に融資する証券投資の脅威への対応策（Addressing the Threat from Securities Investments that Finance Communist Chinese Military Companies）」という大統領命令に基づく。

る。根拠条文は、具体的には以下の通りである。

50 U.S.C. § § 1705

(a)　（略）

(b)　民事上の制裁金

本条(a)に定める違法行為（注：IEEPA 違反、その未遂、共謀）を行った者は、以下のいずれか大きい額を超えない金額の民事上の制裁金が課される。

(1) 250,000 ドル、又は

(2) 制裁金が課される違反の基礎となる取引額の 2 倍の額。

(c)　刑事上の法定刑

本条(a)に定める違法行為（注：IEEPA 違反、その未遂、共謀）を、故意に行い、故意に行おうとし、又はその実行について故意に共謀し、もしくは幇助・教唆した者が有罪判決を受けた場合、1,000,000 ドル以下の罰金、又は、自然人の場合は同額の罰金もしくは/及び 20 年以下の有期刑が科される。

この条文から明らかなように、刑事責任を追及する場合には、行為者に故意が必要であるから（すなわち過失犯規定はない）、セキュリティ担当者がセキュリティ目的で経済制裁対象と知らずに取引した場合に起訴されることはまずない。もっとも、捜査に巻き込まれる可能性はあるため、故意がないことを示すことができるようにしておくべきである。

これに対し、民事上の責任を追及する場合には、条文上明らかなように、故意は要求されておらず、同ガイダンスでも指摘されているように[111]、「厳格責任」に基づいて、すなわち、取引相手が指定国であると知らなかったことに過失がある場合はもとより過失がなくても、民事上の制裁金が課される場合がある。

したがって、ダークマーケットにおいて情報等を購入するセキュリティ企業等は、現在存在する制裁の対象国と制裁内容を常時把握しておく必要がある。その方法として、OFAC は、「A Framework for OFAC Compliance Commitments（OFAC コンプライアンス取組みのための枠組み）」[112]という文書において、各組織において、制裁コンプライス・プログラム（sanctions compliance program; SCP）を策定しておくことを求めており、SCP に組み込むべき要素、そこでの考慮要素について説明している。民事上の制裁金を課すかどうかの判断にあたっては、適切な SCP が存在するか、それが適切に運営されているかが斟酌され、適切な場合には制裁金が課されない又は軽減される、としている[113]。

具体的に SCP に組み込むべき要素としては、(1)経営陣の関与、(2)リスク評価、(3)内部統制、(4)テスト及び監査、(5)研修、の 5 つである。各要素で組み込むべき事項は以下の通りである。

---

111 同ガイダンス 13 頁。

112 https://www.american-club.com/files/files/cir_33_19_p2.pdf。なお、同ガイダンスにあるリンク先は、制裁プログラムの情報に関する OFAC のサイトであり、同文書そのものへのリンクではないため、注意されたい。

113 前掲枠組み 1 頁。

(1) 経営陣の関与：

(i) 経営陣が SCP を確認・承認していること。

(ii) SCP を実際に運用する部署に対し、経営陣が、必要な権限を付与しており、当該部署から経営陣に対し、直接報告できる体制を整備していること。

(iii) SCP を実際に運用する部署が人材、専門知識、情報技術等について十分なリソースを得られるように、経営陣において取り計らい続けていること。

(iv) 経営陣が、組織全体において「コンプライスの文化」を醸成すること。

(v) 経営陣において、明白な法令違反の重大性について理解し、将来的に明白な違反が起きないように必要な措置をとること。

(2) リスク評価

(i) 組織において、潜在的なリスクに応じた必要十分な頻度及び方法において OFAC リスク評価を実施すること（なお、OFAC の経済制裁執行ガイドライン[114]に、リスク評価に使用することのできる OFAC リスクマトリクスが添付されている。）。

(ii) 組織において、特定したリスクについて特定、分析、対応する方法論を開発していること。

(3) 内部統制

(i) 組織において、SCP の概要を示すポリシー、手順を書面で準備していること。

(ii) 組織において、OFAC リスク評価の結果に対応する内部統制制度を整備していること。

(iii) 内部監査、外部監査を通じて上記ポリシー及び手順を組織内において実行すること。

(iv) 必要十分な記録管理ポリシー及び手順を整備すること。

(v) 内部統制システムの脆弱性を把握した場合、直ちに実効的な対策をとること。

(vi) SCP のポリシー及び手順について社内に周知徹底すること。

(vii) SCP のポリシー及び手順を日常業務に実装するための人員を配置すること。

(4) テスト及び監査

(i) 経営陣が、テスト及び監査機能に責任を持ち、テスト及び監査の実施は経営陣から独立して行われ、その実施部隊に十分な権限、リソースが付与さ

[114] 31 C.F.R. Part 501 別紙 A。なお、C.F.R.は、連邦規則集（Code of Federal Regulations）のことであり、各種行政手続を定める。そのうち、タイトル 31（31 編）では、「金融：財務省」を扱う。

れていること。

(ii) 当該組織における SCP のレベルと緻密さに応じてテスト及び監査が実施され、テスト及び監査が包括的かつ客観的であるようにすること。

(iii) テスト及び監査の結果がよくなかった場合、直ちに実効的な対策をとること。

(5) 研修

(i) OFAC 研修プログラムにおいて十分な情報及び説明を従業員に対して提供すること。

(ii) 組織が提供する製品及びサービスに適した OFAC 研修プログラムを提供するよう取り組むこと。

(iii) 組織の OFAC リスク評価及びリスク内容に応じて、適切な頻度で OFAC 研修プログラムを実施すること。

(iv) テスト及び監査の結果がよくなかった場合、直ちに従業員に対し必要な研修等を提供すること。

(v) 関連する従業員すべてが簡単にアクセスできる研修資料・リソースを用意すること。

現在存在する制裁の対象国と制裁内容は、OFAC のウェブサイトで確認することが可能である[115]。直近では、2021 年 2 月 26 日、3 月 2 日、3 月 3 日、3 月 5 日に内容が更新された制裁があり、遵守するには相当の頻度で確認しておく必要がある。

訳注 13

大統領命令 No. 13694「重大な悪意のあるサイバー活動に従事する特定の者の資産の凍結」（Blocking the Property of Certain Persons Engaged in Significant Malicious Cyber-Enabled Activities）は、オバマ大統領が発付したものであり、合衆国の国家安全保障、外交政策、健全な経済、金融の安定に重大な脅威をもたらし、又は当該脅威に相当程度寄与する悪意のあるサイバー活動について責任のある者、又はそれに関与した者（個人又は団体）に対して取引の停止や資金の凍結を命じるという内容のものである[116]。これに基づき、同年、本書注 94 に詳述した 50 U.S.C. § § 1708 が、2015 年国防権限法（National Defense Authorization Act）として制定された。なお、この大統領命令は、選挙の過程に介入し、侵害する目的で情報を改ざん、改変、濫用する個人又は団体に対して制裁を加えるべく、大統領命令 No. 13757「サイバー活動に関する国家緊急事態に対応するための追加方策（Taking Additional Steps to Address the National Emergency With Respect to Cyber-Enabled Activities）」[117]によって、改定さ

---

[115] https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information。同ガイドライン注 43 に記載のウェブサイト。

[116] https://www.federalregister.gov/documents/2015/04/02/2015-07788/blocking-the-property-of-certain-persons-engaging-in-significant-malicious-cyber-enabled-activities

[117] https://www.federalregister.gov/documents/2021/01/25/2021-01714/taking-additional-steps-to-address-the-national-emergency-with-respect-to-significant-malicious

れている。

訳注 14

通信傍受法 18 U.S.C. § 2512 (1)は、一定の例外を除き、故意に、主として傍受に有用な設計であることにつき悪意又は善意有過失で、当該設計を有する電子装置、機械装置、その他の装置を、(a) 州際間取引又は外国取引において郵送、送付、運搬した者、(b) 製造、組立て、所持、販売した者、(c) 新聞や電子媒体等に広告を出した者は、本章に従って罰金又は/及び 5 年以下の有期刑が科される、と定める。

訳注 15

Luis v. Zang 事件[118]は、オンライン通信をひそかに傍受するために使用されたソフトウェアの製造者と、そのソフトウェアを妻の通信を傍受するために使用した夫に対する、妻の通信相手による 18 U.S.C. § 2511（傍受禁止）違反及びプライバシー違反に基づく損害賠償請求において、夫に対する請求は認容したものの製造者に対する請求は棄却した第一審について、製造者に対する請求についても認容すべきであるとして破棄差戻しをした事件である。

前提として、通信傍受法（Wiretap Act）では、一定の例外を除き、音声通信（wire communication）、口頭又は電気通信（electronic communication）による通信を故意に傍受し、傍受することを試み、人に傍受させ、傍受を試みさせることを禁じており[119]、傍受された被害者が通信を傍受、開示、故意に使用した者に対して仮処分、衡平法上の処分、損害賠償（合理的な弁護士費用も含む）を求める民事上の請求権を認める[120][121]。

本判決では、①18 U.S.C. § 2511 の「傍受」が送信中の通信内容を取得することを意味する、すなわち保存された通信を事後的に取得することは「傍受」にあたらないという判例法理（同時性の要件）を改めて確認したこと、②傍受に使用されたソフトウェアによって、送信中の通信内容が製造者のサーバを経由して使用者に送信される仕組みとなっていたことをもって、製造者が「傍受」したと認めたこと、③18 U.S.C. § 2520 は、傍受された被害者について通信を傍受、開示、故意に使用した者に対する民事上の損害賠償請求権を認める旨定めており、一見 18 U.S.C. § 2511（傍受禁止）違反の場合に限り適用される（よって傍受装置の製造等を禁じる§ 2512 違反には適用されない）ように読め、単に傍受装置を所持しただけでは「通信を傍受、開示、故意に使用」したとはいえないが、本件のように、傍受装置を宣伝、販売し、自らのサーバを使用して装置のユーザによる傍受に関与している場合には、「通信を傍受、開示、故意に使用」したと言え、被害者による 18 U.S.C. § 2512 違反に基づく損害賠償請求は成立すると判断したこと、が注目に値する。

---

[118] *Luis v. Zang*, 833 F.3d 619, 635 (6th Cir. 2016)
[119] 18 U.S.C. § 2511(1)(a)。
[120] 18 U.S.C. § 2520(a)(b)。
[121] したがって、セキュリティ担当者が購入した盗聴マルウェアを使用した場合には、刑事上の責任のみならず、被害者から損害賠償請求されるおそれもある。

５　日本におけるサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項についての論点の検討

5.1　日本における論点の法的位置づけ

前掲「オンラインサイバー脅威インテリジェンスを収集し、不法な情報源からデータを購入する際の法的考慮事項」で種々の論点が提起されている。

検討すべき論点としては、「被害者にならないこと」「加害者にならないこと」「オンラインフォーラムでの合法的な情報収集」「盗難データや脆弱性の購入」「コンプライアンスのためのベストプラクティス」がある。

これらの論点のうち、「被害者にならないこと」は、通常のサイバーセキュリティの保護措置の重要性、サイバーセキュリティ実践そしてそれらのための脅威インテリジェンスの重要性を意味しており、ここでは、詳述はしない。

「加害者にならないこと」「オンラインフォーラムでの合法的な情報収集」「盗難データや脆弱性の購入」において論じられている事項は、個々の行為の適法性の問題となる。一方、「コンプライアンスのためのベストプラクティス」については、脅威インテリジェンスの提供の問題／推奨事項の問題については、また、別個の問題としてみていくことができよう。

5.2　適法性の検討

「加害者にならないこと」は、司法省ガイドラインにおいて「本文書で取り上げている活動の一部は、連邦刑法に関係しており、州法に違反したり民事責任を問われたりする可能性がある。これらの活動に従事することを計画している組織は、その活動の合法性を評価するために弁護士と相談すべきである。」（常に従うべき２つのルール）とされている。そこで、具体的には、「オンラインフォーラムでの合法的な情報収集」「盗難データや脆弱性の購入」についての検討がなされている。以下、これらの二つの局面について日本法の観点から、検討する。

また、同ガイドラインにおいてもふれられているように資金洗浄／テロリストの支援を規制する法律等との論点についても検討する必要がある。この論点は、本調査第１章でも検討した事項である。

オンラインフォーラムでの合法的な情報収集

ここでの問題は、フォーラムへのアクセスの問題（認証情報の利用、不正アクセスの問題、ポリシーに反するアクセス）、フォーラムでの活動の問題（潜伏、投稿、情報交換）がある。

フォーラムへのアクセスへの問題をみる場合に前提として、不正アクセス禁止法をみていくことにする。不正アクセス禁止法は、「電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を図」ろうとする法律である。同法は、「不正アクセス行為」を定義しており（同法２条４項１ないし３号）、他人の識別符号を悪用する行為及びコンピュータプログラムの不備をつく行為

をそれぞれ処罰している。また、ここで問題となる「アクセス制御機能」というのは、「当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（略）であることを確認して、当該特定利用の制限の全部又は一部を解除する」と定義されている（同法２条３項)。

これらの解釈については、①入力先が、「アクセス制御機能を有する特定電子計算機」であること②「電気通信回線を通じて」行う者であること③入力されるものが、「当該アクセス制御機能にかかる他人の識別符号」であること④「入力」した結果として、「特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をしうる状態にさせる」こと、などが要件として求められている。

これらの解釈を前提に、上記の問題について検討する。

ここで、認証情報の利用というのは、アクセスのための資格や招待を必要とする公衆がアクセスしうるといえないインターネット上のエリアにアクセスして情報を取得する行為、もしくは、ディープウェブ／ダークウェブといわれるエリアにアクセスして情報を取得する行為の問題である。具体的には、招待を受ける、料金を支払う、入会「テスト」をクリアする、専門用語を使えることを示す、オンラインセキュリティに関する情報を交換することによりアクセスしうる領域にアクセスして情報を得る行為ということになる。我が国の不正アクセス禁止法においては、「他人の識別符号を入力して当該特定電子計算機を作動させ」るか、「アクセス制御機能による特定利用の制限を免れることができる情報又は指令を入力」することによってアクセスすることを処罰している。アクセスのための資格や招待を必要とするとしても、そのための資格や招待を受けることにより特定のアクセスのための権限を得ることは、「他人の識別符号を入力」することでないのは、もちろんのこと、「アクセス制御機能による特定利用の制限を免れることができる情報又は指令を入力」とはいえない。したがって、日本法上においては、これらの行為は、処罰の対象とはならないと解される。

不正アクセスの問題というのは、脆弱性を悪用したり、盗まれた認証情報を使用したりする場合の問題である（司法省２　（２）イ（イ）参照)。これについては、米国と同様であり、これらの行為は、上記不正アクセス禁止法にいう不正アクセス行為として処罰の対象となる。

また、他人名義といっても架空の名義でみずから取得した識別符号の入力は、構成要件に該当しない。上記のように「他人」の識別符号であることが求められていることから、「他人名義も架空の名義で取得した識別符号の入力についてみると（略)、アクセス管理者との関係においては、当該識別符号を取得したものが利用権者であるから、そのものが当該識別符号を入力しても不正アクセス行為とはならない」とされている。また、入力の「結果として」、アクセスしうる状態になることが求められているので、そもそもアクセスしうる状態である場合には、成立の余地はない。SNS で友人に限って公開とされる情報について、虚偽の事実を申告して、友人になって、それらの特別の情報にアクセスする場合でも同様である。SNS で公開している本人に対して虚偽の事実を申告することは、それらの情報について特

定利用の制限を免れる情報を入力したということはできない。

フォーラムでの活動の問題（潜伏、投稿、情報交換）については、どうか。米国においては、提供した情報が犯罪に使用された場合には、犯罪の幇助・教唆（aid and abet)、共謀罪が成立する可能性もあるとされているところである。この理については、我が国においても、全く同様である。従って、このような活動には、従事するべきではないということがいえる。米国においては、特定の条件のもとで、誤解を避けるように試みた上で、活動の可能性は否定されていないが、我が国においては、柔軟な対応が実務的に期待できるとも思われないし、また、犯罪捜査の開始自体のもつインパクトが非常に強いこともあるので、そのような行為については、現に慎むべきであるということがいえる。

「盗難データや脆弱性の購入」

インテリジェンスの成果は、それ自体としては、脅威を引き起こす可能性のある人物、脅威の態様、その対象、脆弱性の情報などである。それらは、一般には、情報自体として取引が禁止される、いわば、「禁制品」というものではない。しかしながら、それらの情報が、違法な手段によって取得されているときにかかる成果が法的にどのように評価されるのか、というのが問題となる。

この点を考えるのにあたっては、資金洗浄／テロリストの支援を規制する法律等や反社会的勢力の排除ポリシーとの関係についてについて考える必要がある。

資金洗浄／テロリストの支援を規制する法律等

我が国における資金洗浄／テロリストの支援を規制する法律として、犯罪による収益の移転防止に関する法律（平成十九年法律第二十二号）（以下、犯罪収益移転防止法という)、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律（平成十一年法律第百三十六号）（以下、組織的犯罪処罰法という）などがあげられる。また、外国為替及び外国貿易法（外為法)」についても検討する必要がある。

犯罪収益移転防止法

犯罪収益移転防止法は、犯罪による収益が組織的な犯罪を助長するために使用されるとともに、これが移転して事業活動に用いられることにより健全な経済活動に重大な悪影響を与えるものであること、及び犯罪による収益の移転が没収、追徴その他の手続によりこれをはく奪し、又は犯罪による被害の回復に充てることを困難にするものであることから、犯罪による収益の移転を防止することが極めて重要であることに鑑み、特定事業者による顧客等の本人特定事項等の確認、取引記録等の保存、疑わしい取引の届出等の措置を講ずる旨を定めた法律である。犯罪収益移転防止法上の特定事業者については、本人確認義務（犯罪収益移転防止法４条)、取引記録等の作成義務（同法６条）や疑わしい取引の届出義務（同法８条）等を負う。仮想通貨（制定法上は、暗号資産）の交換業者は、同法上の特定事業者であるとされています（同法２条２項３1 号)。もっとも、ここで、疑わしい取引というのは、収受した財産が犯罪による収益である疑いがある、又は顧客等が当該取引に関し組織的犯罪処罰法第十条の罪若しくは麻薬特例法第六条の罪に当たる行為を行っている疑いがあ

ると認められる場合をいう（同法 8 条)。被害者もしくは、そのために活動をするものが、突如として法貨を仮想通貨に交換し、多額の金額を攻撃者に対して支払う行為は、それ自体は、上記要件に該当するとは考えられない。しかしながら、金融庁は、「疑わしい取引の参考事例」として、仮想通貨交換業者については、通常は取引がないにもかかわらず、突如多額の仮想通貨の売買又は他の仮想通貨との交換が行われる口座に係る取引（同第 4　取引の携帯に着目した事例（1))、資金洗浄・テロ資金供与対策に非協力的な国・地域又は不正薬物の仕出国・地域に拠点を置く顧客に係る取引（第 5　外国との取引に着目した事例）などを具体例としてあげている。従って、それらの事例と認識される可能性があり、関係者は、弁護士等のアドバイスを求める必要があるといえる。

組織的犯罪処罰法等

組織的犯罪処罰法は、組織的に行われた殺人等の行為に対する処罰を強化し、犯罪による収益の隠匿及び収受（略）を目的とする行為を処罰するとともに、犯罪による収益に係る没収及び追徴の特例等について定めている。まず、そこでは、3 条において、同法が対象とする犯罪が、「組織的な殺人等」として明らかにされている。一般的なサイバー犯罪は、この犯罪の定義に含まれていない。しかし、組織としてランサムウェアを利用して身代金を取得している場合には、同条 1 項 14 号の恐喝の罪をおこなっているものと考える[122]。そのような場合には、同法 10 条は、取得若しくは処分につき事実を仮装し、又は犯罪収益等を隠匿する行為を処罰している。また、同法 11 条は、情を知った犯罪収益等の収受を処罰している。もっとも、ランサムウェアの被害者が、送金等を行ったという場合には、その収受を幇助したということに該当するというのは、困難であろうと考える。

外為法

外国為替、外国貿易その他の対外取引は自由に行われることを基本とするが、種々の要請から、対外取引に対し必要最小限の管理又は調整を行うことか必要とされることになる。これにより、対外取引の正常な発展並びに我が国又は国際社会の平和及び安全の維持を期すことが可能になる。このような目的から制定されているのが、外国為替及び外国貿易法である。

同法によると、我が国の平和及び安全の維持のため特に必要があるときは、閣議において、対応措置を講ずべきことを決定することができる。この対応措置としては、支払いに対する許可の指定（同 16 条)、(21 条)、などがある。また、同 19 条は、支払手段等の輸出入として、　財務大臣は、支払手段（第六条第一項第七号ハに掲げる支払手段が入力されている証票等を含む。）又は証券を輸出し、又は輸入しようとする者に対して、許可を受ける義務を課することができるとしている。外為法は、1997 年の改正時において、同法 6 条 7 号により、仮想通貨による送金の許可の義務をさだめることができるようになっていた（同法 16

122 なお、恐喝行為の実行行為者が、海外であることがどのように影響するかという論点があるが、被害が我が国で起きている限り、組織犯罪処罰法の 12 条で引用される刑法 4 条の２の問題ではなく、国内犯として扱われるものと考える。

条 1 項)。もっとも、現時点においては、特定のサイバーテロリスト集団が指定されているとう事実はないので、当該規定の適用については、考えられないことになる。

反社会的勢力の排除ポリシーとの関係について

反社会勢力とは、暴力、威力と詐欺的手法を駆使して経済的利益を追求する集団又は個人をいう（指針 1 頁　脚注)。具体的には、平成 19 年 6 月 19 日の、犯罪対策閣僚会議の「企業が反社会的勢力による被害を防止するための指針」の申し合わせをもとに、これの遵守によって実際に行われている。

この指針は、1　反社会的勢力による被害を防止するための基本原則、2　基本原則に基づく対応 ((1) 反社会的勢力による被害を防止するための基本的な考え方、(2) 平素からの対応、(3) 有事の対応（不当要求への対応))、3　内部統制システムと反社会的勢力による被害防止との関係、から成り立っている。組織としては、脅威インテリジェンス情報のための情報購入やランサムウェアへの支払いを考えると、この申し合わせとの関係を検討する必要がでてくる。ここで特に検討されるべきは、(3) 有事の対応（不当要求への対応）の問題であって、上記指針においては「反社会的勢力への資金提供は、反社会的勢力に資金を提供したという弱みにつけこまれた不当要求につながり、被害の更なる拡大を招くとともに、暴力団の犯罪行為等を助長し、暴力団の存続や勢力拡大を下支えするものであるため、絶対に行わない」とされているところである。しかしながら、上記脅威インテリジェンス情報のための情報購入やランサムウェアへの支払いについては、それ相応の合理性もあり、この衝突について、どのように考えるべきかという論点が生じる。

この論点については、我が国では、正面から議論されていない。報告者としては、本報告を契機として、議論が正面からなされることが望ましいものと考える。

5.3　違法な手法によって取得した情報をもとに脅威インテリジェンスサービスを提供／利用することの法的問題と推奨事項

脅威インテリジェンスサービスの利用について

脅威インテリジェンスサービスを利用するにあたって、提供されるインテリジェンスを構築するためのデータが違法な手法によって取得される可能性がある場合について、どのように考えるのか、という問題がある。

この点については、我が国においても、また、諸外国においても明確な回答は得られていないということができよう。まず、インテリジェンスとそれを生成するために利用されるデータとは別個であるという前提がある、もっとも、そのような違法な手法によってデータを取得することを促進するかのような価格その他でのサービスの購入は、インテリジェンス利用者自身のコンプライアンス体制の問題も生じるものと考えられる。

このように考えると、脅威インテリジェンスサービスの利用については、そのインテリジェンスのソースたるデータの取得方法についても留意を払いながら、その取得及び利用に関する種々の情報を総合的に判断して、利用者の組織のコンプライアンス体制のもとで、その利用の是非等を判断すべきということになる。また、その際に、疑念が生じる場合におい

ては、法律専門家の意見書等を取得することが推奨されることになろう。

脅威インテリジェンスサービスの提供について

我が国において、脅威インテリジェンスサービスを提供する者についても、同様の観点からコンプライアンスを考えなければならないのは、いうまでもない。

自ら違法な行為に基づいて脅威インテリジェンスのためのソースとなるデータを取得することは現に慎まなければならない、ということが前提となる。インテリジェンスサービスの提供者といっても、例えば、海外の会社などからインテリジェンスの成果の提供を受け、その成果を自らのものとして販売する場合には、自ら、社会的責任を果たす、公正で透明性のあるサービスを果たすという理念から、違法行為がないことを確認し、それを積極的に確からしくする必要があることになる。サプライチェーンのコンプライアンスという観点から考えた場合において、このような義務が求められるものと考えられる。このような観点からは、そもそも、そのようなリスクをも踏まえたコンプライアンス体制を構築し、そのポリシーを徹底するとともに、契約、周知徹底、書面確認、現地監査の各手法等をリスクに応じて採用し、コンプライアンスの観点から、対応しなければならないこととなる。