諸外国におけるサイバー事案の捜査手法等に関する調査研究

報告書

2023 年 3月

公益財団法人 日工組社会安全研究財団

目 次

1. 調査研究概要

1.1 調査の背景と目的

新型コロナウイルス感染症の感染拡大を受けた「新しい生活様式」の定着やこれに伴い加速するデジタル化推進の動きにより、今後、サイバー空間は、全国民が参画し、重要な社会経済活動を営む、重要かつ公共性の高い場への変貌を遂げていくものと考えられる。他方で、令和 2 年のサイバー犯罪の検挙件数が過去最大となったほか、警察庁が把握している国内の企業・団体等におけるランサムウェア被害件数が令和 3 年上半期で 61 件と、前年下半期の 21 件と比べて大幅に増加するなど、サイバー空間をめぐる脅威は、極めて深刻な情勢が続いている。

我が国の警察においては、これまでも取締りと被害防止の両面からサイバー事案への対策に取り組んできたところ、高度化・複雑化するサイバー事案に対処するため、更なる対策強化が必要であり、特に、ランサムウェアを始めとする国境を越えて敢行されるサイバー事案については、外国捜査機関等と連携して対処する必要がある。

警察庁においては、内部部局に関連部署を集約したサイバー警察局を設置するとともに、国の捜査機関として外国捜査機関等と緊密に連携し、国際共同捜査への参画等を通じて重大サイバー事案への対処を担うサイバー特別捜査隊を設置するなど、体制の強化が図られたところである。新たに設置された組織においては、国際連携を強化し、国境を越えて敢行されるサイバー事案に対して対処することが期待される。この点、諸外国のサイバー事案に係る捜査手法や法制度等を理解することは、国際連携を強化するに当たり、有用であると考えられる。

本調査研究事業は、こうした背景を踏まえ、諸外国におけるサイバー事案の先進的な捜査手法や根拠となる法制度等について調査を行い、同結果が我が国のサイバー事案への対処能力向上に活用され、もってサイバー空間の安心・安全の確保に資することを目的とする。

1.2 実施内容

1.2.1 調査対象国

本調査研究では、アメリカ合衆国（以下「アメリカ」という。）、イギリス（イングランド及びウェールズ）、ドイツ及びフランスの 4 か国を対象に、文献調査を行った上で海外現地調査を実施した。

1.2.2 調査項目

本調査研究の目的である、サイバー事案の取締り等における国際連携に必要な体制や、諸外国との国際共同捜査推進を念頭に置いた先進的な捜査手法及び法制度等の情報の整理という目的に照らし、表 1 を調査項目とした。

表 1　調査項目

項目	概要
1. サイバー空間の脅威に対処するための体制	・ サイバー事案の捜査・対策を担う公的機関等の体制・業務分担 ・ サイバーセキュリティに関する総合調整を担う公的機関等の体制 ・ デジタルフォレンジック体制
2. 効率的・効果的な捜査手法及び根拠となる法制度	・ 遠隔地のサーバ等に所在する証拠の収集 ➢ ISP に対する捜索差押え令状等のオンライン送達 ➢ 海外の ISP に対する直接の情報提供要請及び回答データのオンライン受領（その際の暗号化措置の手法） ➢ 国内事業者が保有する海外所在サーバからの情報提供要請 ・ サイバー空間上の通信傍受 ・ サイバー事案に係る仮装身分捜査 ・ 犯罪者が持つオンラインアカウントの乗っ取り ・ 不正に窃取された暗号資産の奪還
3. 先制的な被害防止措置及び根拠となる法制度	・ 攻撃元サーバへのアクセス（保管されたデータの閲覧、複写、改変を含む）及び機能停止措置（テイクダウン） ・ ポリスウェア等の活用 ・ 警察管理に係るサーバ等の運用 ・ 代替サーバ等の運用
4. 民間事業者の義務及び根拠となる法制度	・ 通信履歴（ログ）の保存義務 ・ 暗号化等の解除・破損機器の修復に係る支援義務 ・ システム等へのバックドアの確保義務 ・ サイバー事案発生時の公的機関等への報告義務 ・ 警察等によるテイクダウン作戦への協力義務 ・ 情報開示に関する利用者等への通知義務
5. サイバー捜査における人権確保に関する係争事例	・ サイバー捜査における人権確保に関する係争事例

1.2.3 海外現地調査

文献調査で不明な点を中心に、調査対象各国においてサイバー事案の捜査を担う機関や、サイバー犯罪の捜査手法に知見を有する学識者等に対するヒアリングを行った。

実施方法は、現地における対面での聞き取りまたは書面によるヒアリングとした。

海外現地調査対象国、ヒアリング先機関、選定理由及び実施方法を表 2 に示す。

表 2　海外現地調査ヒアリング先

国	ヒアリング先機関	選定理由	実施方法
アメリカ	連邦検察庁　ニューヨークサザンディストリクト支部、複雑詐欺・サイバー犯罪ユニット	FBI の上部組織で、連邦レベルのサイバー犯罪捜査を統括する。	対面
	コロンビア大学ロースクール Daniel Richman 教授	元連邦検事。米国司法省のコンサルタントを歴任するなど、アメリカのサイバー犯罪捜査に知見を有する。	対面
イギリス	ポーツマス大学犯罪学及び刑事司法学部 Simona Ciobotaru 講師	サイバー犯罪等に知見を有する。	書面
	ポーツマス大学犯罪学及び刑事司法学部 Tom Ellis 主任講師	刑事司法等を専門とする。英国内務省、国連地域間犯罪司法研究所（UNICRI）における勤務経験がある。	書面
	ポーツマス大学犯罪学及び刑事司法学部 Simon Marsden 上級講師	サイバーセキュリティ等に知見を有する。	書面
ドイツ	ハノーファ大学法学部 Susanne Beck 教授	ニーダーザクセン州警察アカデミーで講義を行う等、ドイツのサイバー犯罪捜査における法的議論に知見を有する。	書面
フランス	国家憲兵隊　憲兵隊サイバー指令部、サイバー協力・パートナーシップ担当	サイバー犯罪捜査を担う国家憲兵隊の担当部署。	対面

2. 調査結果

2.1 アメリカ合衆国

2.1.1 サイバー空間の脅威に対処するための体制

(1) サイバー事案の捜査・対策を担う公的機関等の体制・業務分担

サイバー犯罪への対応は、司法省のコンピュータ犯罪・知的財産部門（Computer Crime and Intellectual Property Section (CCIPS)）が総括している[1]。インターネット関連犯罪の第一次的捜査を行うのは連邦機関であり、捜査実務は政府に置かれた産学官連携のタスクフォース「国家サイバー捜査合同タスクフォース（National Cyber Investigative Joint Task Force）」（以下「NCIJTF」という。）の中で、主に連邦捜査局（Federal Bureau of Investigation）（以下「FBI」という。）のサイバー課（Cyber Division）が担う（州法に違反するサイバー犯罪への対応は、州警察が行う場合もある）[2]。

ただし、始めから全国的で大規模、持続的な事案を除き、常に NCIJTF の枠組みで捜査が行われる、あるいは FBI が常に主導するというものではない。後述するとおり、米国の連邦機関では、FBI 以外にも複数の組織がサイバー犯罪捜査を行っている。複数の捜査機関が異なる IP アドレスを追っていたところ実は同じ事件であった場合等、組織間の調整には連邦検察が関わる。令状や召喚状（subpoena）を発行する関係で、どの連邦捜査機関の情報も検察に集まるためとされる。組織間調整においては捜査の進捗状況や組織規模等さまざまな要因が考慮されるが、基本的には NCIJTF による合同対応となる[3]。

また、近年は詐欺等の犯罪は何らかの形でサイバーが絡んでいることが多いため、すべてを連邦機関が担うわけではなく、事案によって判断し、詐欺事件として州警察が対応できるものは州警察が対応することになる[4]（ただしサイバー犯罪への対応能力は州により異なる）。

なお、FBI と州や地域の警察がタスクフォースを組んで捜査を行うこともあるが、FBI は州警察等に協力要請はできるものの、指示する権限はない。この場合、タスクフォースに参加する州警察等の人員は、FBI に出向する形で連邦法を執行する（出向者の人件費及びタスクフォースの運営費は FBI が負担することになる）[5] [6] [7]。

- FBI の主なサイバー犯罪捜査対応部門

FBI のサイバー課は、全米 56 か所の地域事務所それぞれに特別な訓練を受けたサイバー部隊（cyber squads、高度なコンピュータ言語や科学捜査、マルウェア分析の訓練を受けた特

---

[1] 米国司法省ウェブサイト https://www.justice.gov/criminal-ccips（2023 年 2 月 22 日閲覧）

[2] FBI ウェブサイト https://www.fbi.gov/investigate/cyber（2023 年 2 月 22 日閲覧）

[3] 連邦検察庁へのヒアリングに基づく。

[4] コロンビア大教授へのヒアリング結果に基づく。

[5] コロンビア大教授へのヒアリング結果に基づく。

[6] 連邦・州タスクフォースに係る司法省の最終規則 https://www.govinfo.gov/content/pkg/FR-1997-10-08/pdf/97-26660.pdf（2023 年 2 月 22 日閲覧）

[7] FBI が州等の警察と協力する場合の覚書の例 https://documents.law.yale.edu/sites/default/files/mou2.pdf（2023 年 2 月 22 日閲覧）

別捜査官又はコンピュータ科学者）を配置しており、政府関係機関と緊密な連携体制を取っている[8] [9]。

なお、FBI の 2021 年の職員数は 35,742 名（うち特別捜査官 13,275 名、インテリジェンス分析官 3,112 名）である[10]。FBI の主なサイバー犯罪捜査対応部門を以下に示す。

表 3　FBI の主なサイバー犯罪捜査対応部門

部門・機能	主な所掌内容
サイバーアクションチーム Cyber Action Team (CAT)	FBI のサイバー課に 2006 年に設立された、ハッキングや機密情報・顧客情報等の重要データの流出等の重大事案が起きた際の緊急対応を行うチーム。事案発生後 48 時間以内に、世界中どこでも捜査支援を行う専門官を配置可能。 全米 56 カ所の FBI 地域事務所に高度なコンピュータ言語や科学捜査、マルウェア分析の訓練を受けた特別捜査官又はコンピュータ科学者等の職員を配置し、デジタルフォレンジック体制も持つ。
サイバー・アシスタント・リーガル・アタッシェ Cyber assistant legal attachés (ALAT)	2011 年から始まった制度で、アタッシェは全世界の大使館に配置され、日常的に現地の法執行機関と情報共有や捜査協力、全般的な関係構築等の連携を行う。違法なサイバー活動の検挙に当たっては、外国のカウンターパートと物理的に同じ場所で活動することもある。2016 年時点で常駐ポストはロンドン 2、ブカレスト、キャンベラ、ハーグ、タリン、キーウ、オタワの 8 カ所であったが、現在はサイバー脅威のある環境かどうか及び滞在国政府が FBI とサイバー犯罪対応において連携能力があるかどうかによって配置場所が決められている。
インターネット犯罪申告センター Internet Crime Complaint Center (IC3)	インターネット犯罪の被害申告を受ける機関。以前は「インターネット詐欺申告センター（Internet Fraud Complaint Center）」という名称だったが、サイバー犯罪は詐欺に限らず多岐にわたることから 2003 年 10 月に現名称となった。IC3 の「財産回収チーム（Recovery Asset Team）」はこれまでに通報を基にサイバー犯罪に関する多額の犯罪資産を凍結してきた。
サイウォッチ CyWatch	FBI のサイバー指令センター。人員は NCIJTF と FBI が共同で運営。違法、あるいは国の安全保障に関わるサイバー攻撃への国内の法執行機関の対応の調整や、被害事案の追跡、全米各州にある FBI 地域事務所等ほかの連邦サイバーセンターとの連絡・調整を 24 時間・年中無休体制で行っている。

[8] FBI ウェブサイト https://www.fbi.gov/investigate/cyber（2023 年 2 月 22 日閲覧）

[9] FBI 広報「The Cyber Action Team: Rapidly Responding to Major Computer Intrusions」（2015 年 3 月付）https://www.fbi.gov/news/stories/the-cyber-action-team（2023 年 2 月 22 日閲覧）

[10] FBI2022 年予算案 https://www.justice.gov/jmd/page/file/1399031/download（2023 年 2 月 22 日閲覧）

ただし、事案の種別によっては他の連邦機関が行うとされており、ほかにサイバー犯罪の捜査を担う連邦機関は米国シークレットサービス、米国移民・関税執行局、米国郵便監察局、アルコール・タバコ・火器及び爆発物取締局である[11] [12] [13]。

米国でサイバー犯罪捜査を所管する連邦機関と対象となる犯罪種別の一覧を以下に示す。

表 4　米国でサイバー犯罪捜査を所管する連邦機関

連邦機関	犯罪種別
FBI 地域事務所	・ コンピュータへの侵入（ハッキング等） ・ パスワードの不正入手 ・ 児童ポルノ、児童搾取 ・ インターネット詐欺及びスパムメール ・ インターネットによるハラスメント ・ インターネットによる爆発予告 ・ インターネットを介した爆発物・発火物・銃器の不正取引
米国移民・関税執行局	・ コンピュータへの侵入（ハッキング等） ・ パスワードの不正入手 ・ 児童ポルノ、児童搾取 ・ 郵便が関わる児童搾取、インターネット詐欺 ・ インターネット詐欺及びスパムメール
米国シークレットサービス	・ コンピュータへの侵入（ハッキング等） ・ パスワードの不正入手 ・ 児童ポルノ、児童搾取（輸入されている場合のみ） ・ 通貨偽造 ・ インターネット詐欺及びスパムメール
その他の連邦機関	・ 米国郵便監察局：郵便が関わる児童搾取、インターネット詐欺 ・ 連邦取引委員会、証券取引委員会（証券詐欺／投資関連のスパムメールの場合）：インターネット詐欺及びスパムメール ・ アルコール・タバコ・火器及び爆発物取締局：インターネットを介した爆発予告、爆発物・発火物・銃器の不正取引

(2) サイバーセキュリティに関する総合調整を担う公的機関等の体制

全国的で大規模、持続的な事案の対応やサイバー犯罪に関するインテリジェンスの情報共有、研修等は、前述したタスクフォース「NCIJTF」の枠組において行われ、官民が同じ場

[11] 米国司法省ウェブサイト https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime#（2023 年 2 月 22 日閲覧）

[12] National Cybersecurity Alliance ウェブサイト https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/reporting-cybercrime/（2023 年 2 月 22 日閲覧）

[13] 米国シークレットサービスウェブサイト https://www.secretservice.gov/investigation/cyber（2023 年 2 月 22 日閲覧）

所で連携し活動する取組が進められている[14]。NCIJTF は、サイバー犯罪に対する取組を実施するための産学官のハブ機関で、2008 年に設立された。FBI を含む法執行機関や諜報機関、国防総省等、30 以上の関係機関で構成され、各機関の代表者は同じ場所（タスクフォースの所在地）で緊密に連携しつつ活動する。

多機関連携で情報を調整・統合・共有することでサイバー捜査を支援し、各分野の意思決定者にインテリジェンス分析の提供・支援を行うほか、国家に対するサイバー脅威対応における継続的取組を組織の責務とする。

タスクフォースは FBI のサイバー課が主導し、連邦の関係機関や諸外国のパートナー、民間部門と連携体制を組むことによって、ネットワークの防御、違法行為の特定や不正行為への制裁、外国の犯罪者への対抗等を行う。主要なサイバー脅威領域に基づく「ミッションセンター」と呼ばれるグループで構成され、各センターは、関係機関の上級管理職（senior executives）が主導する。このセンターを通じて指令（operations）やインテリジェンスが統合され、サイバー上の攻撃者や犯罪者に対する大きな影響を与えることができるとされている。

テロリストやスパイ等の国防に関する犯罪の捜査に関する取組も共同で行っており、各構成機関の権限活用のほか、国際機関や民間機関と連携し、利用可能なすべてのリソースを投入するとされる。

捜査対応以外の産官学連携体制はこの枠組のほかに NPO 団体が二つあり、一つは「国家サイバーフォレンジックス・トレーニングアライアンス（National Cyber Forensics & Training Alliance）」で、リソースや戦略情報、脅威に関する知見を産官学で構築・共有することを目的としており、事案対応やインテリジェンスの情報共有、研修等も行っている。もう一つは、FBI と連携する非営利の枠組「国家防衛・サイバーアライアンス（National Defense Cyber Alliance）」である。いずれも単一組織ではサイバー犯罪の対応はできないという認識のもと、サイバー犯罪事案やインテリジェンスの情報共有、研修等の取組が進められている。

(3) デジタルフォレンジック体制

FBI や国土安全保障省（Department of Homeland Security）等、サイバー犯罪捜査を担う各連邦機関にデジタルフォレンジック部門があり、組織間で特段の違いはなく、機関間での情報交換や協力はあるが、それぞれ自組織の案件に取り組んでいるとされる[15]。

FBI には、全米 56 か所の地域事務所に配置された、特別な訓練を受けたサイバー部隊（高度なコンピュータ言語や科学捜査、マルウェア分析の訓練を受けた特別捜査官やコンピュータ科学者）が配置されている[16]ほか、国土安全保障省の執行部門（Homeland Security Investigations（HSI））にもサイバー犯罪センター（Cyber Crimes Center（通称：C3））のコンピューターフォレンジックスユニット（Computer Forensics Unit、以下「CFU」という。）

---

[14] FBI ウェブサイト https://www.fbi.gov/investigate/cyber; https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force（いずれも 2023 年 2 月 22 日閲覧）

[15] 連邦検察庁へのヒアリング結果に基づく。

[16] Boston25 News 記事「A look inside the FBI's high-tech lab of digital and computer crimefighting」（2021 年 8 月 30 日付）https://www.boston25news.com/news/local/look-inside-fbis-high-tech-lab-digital-computer-crimefighting/WWWHDCR7GFC4FDF7MMUZZLVPTE/（2023 年 2 月 22 日閲覧）

が設置されている[17]。

CFU は、国土安全保障省の捜査官が捜査過程で調べる対象とするデータの分析を行う。押収した電子記録媒体（ハードドライブやフラッシュドライブ、携帯情報端末、携帯電話、DVD、CD、カセットテープ等）のフォレンジック調査を行うための訓練を受けた捜査員または分析官は、コンピューターフォレンジックス捜査官／分析官（Computer forensics agents/analysts）と呼ばれる。

なお、CFU では児童搾取の捜査支援に絡む以下のプログラムを所掌している。

表 5　CFU における児童搾取の捜査支援関連プログラム

プログラム	概要
人身売買救出員（HERO）児童救出隊プログラム（The Human Exploitation Rescue Operative (HERO) Child Rescue Corp program）	病気、怪我、負傷した軍隊隊員向けのプログラム。1 年間の有給インターンシップで、コンピューターフォレンジックアナリストになるための訓練を 3 か月間受けた後、HSI の現地事務所で 9 か月間児童搾取捜査の支援を行う。プログラム終了後は大多数が HSI の常勤職に就く。
コンピュータ／携帯／車両／ドローン・フォレンジックス（Computer/Mobile/Vehicle/Drone Forensics）	HSI は全米のデジタルフォレンジックを主導しており、400 人以上のデジタルフォレンジック捜査官及び分析官を抱える連邦政府最大のコンピューターフォレンジックプログラムを所管する。捜査官及び分析官は、ほかの連邦、州、地域、外国法執行機関にあらゆるデジタルフォレンジック分野の訓練を提供するほか、現地事務所の初動支援を行う。
3-D プリンティング（3-D Printing）	児童搾取の被害者で身元不明の遺体が発見された場合、身元特定のため 3D プリンティングで作成した頭蓋骨のレプリカを National Center for Missing and Exploited Children（国立行方不明者・搾取被害児童センター）に送り、法医学人類学者が識別を行う。
ハードドライブ修復（Hard Drive Repair）	C3 の専門家は、被疑者が破棄しようとしたデジタルデバイスに含まれる証拠や現場・捜査中に破損したハードウェア等を修理し、起訴で使用されるデジタル証拠を取得するよう訓練されている。
暗号化／暗号化解除（Encryption/Decryption）	担当特別捜査官（SAC）の各事務所にあるコンピューターネットワークにより強化された堅牢な暗号解読プログラムが C3 には配置されている。安全で暗号化された証拠転送のほか、捜査官がコンピュータの処理能力を用いてデジタルデバイスの解読支援を行う。

[17] アメリカ合衆国移民・関税執行局ウェブサイト https://www.ice.gov/features/cyber#content1（2023 年 2 月 22 日閲覧）

2.1.2 効率的・効果的な捜査手法及び根拠となる法制度

(1) 遠隔地のサーバ等に所在する証拠の収集

1) ISP に対する捜索差押え令状等のオンライン送達

捜査機関が ISP 等から電子データを取得・押収する場合、捜索差押え令状等の電子的処理・送達が可能で、全米で広く行われている[18]。

捜査機関が通信事業者から電子データを取得・押収する際の手段の選択は各事業者によるとされる[19]。具体的には、通信事業者が用意した安全なポータルサイトに押収の対象となる電子データに関するリンクを貼り付け、捜査機関は同サイトにアクセスしリンク先に保存された電子データをダウンロードして押収する方法や、通信事業者が捜査機関に対し対象となる電子データを電子メールで直接送信する方法等がある。

なお、捜索と押収に関する規定[20]は、具体物、情報、電子媒体いずれも適用可能であり、遠隔アクセスについても適用される。

2) 海外の ISP に対する直接の情報提供要請及び回答データのオンライン受領（その際の暗号化措置の手法）

米国政府が外国政府と「Clarifying Lawful Overseas Use of Data Act（通称：CLOUD Act）」（以下「米クラウド法」という。）に基づく行政協定を締結することで、米国政府は当該外国に所在するプロバイダーに直接、通信内容の開示要求ができる[21]。

なお、データの開示を求められたプロバイダーは、①当該データの主体が米国に居住していない米国人以外の者で、かつ②開示に応じることで行政協定を締結した相手国の法律に違反する重大なリスクを伴うと合理的に信じる場合は、米国裁判所に対して当該開示命令の修正又は取消を要求することが可能とされる[22]。

3) 国内事業者が保有する海外所在サーバからの情報提供要請

通信保管法（Stored Communication Act 18 U.S. Code）第 2701～2713 条では、米国内所在のサーバにあるデータのみ要請可能とされている[23]。そのため、米クラウド法に基づく行政協定を当該外国と締結しない限り、直接要請はできない。

なお、国外に所在する暗号資産交換事業者に対してアカウント情報等の情報提供要請を

---

[18] 連邦検察庁へのヒアリング結果に基づく; 連邦刑事規則（Federal Rule of Criminal Procedure）第 4.1 条 https://www.uscourts.gov/sites/default/files/federal_rules_of_criminal_procedure_-_december_2020_0.pdf（2023 年 2 月 22 日閲覧）

[19] 連邦刑事規則第 49 条(a)(3), (b)(2)

[20] 連邦刑事規則第 41 条

[21] 米クラウド法第 104 条; 米国司法省白書 p.3、https://www.justice.gov/opa/press-release/file/1153446/download（2022 年 9 月 26 日閲覧）

[22] 米クラウド法第 103 条(b)

[23] 通信保管法第 121 章第 2701～2713 条

行う場合は、刑事共助条約（Mutual Legal Assistance Treaty（MLAT））が必要となる[24]。

情報提供要請に関する捜査手続の概要は以下のとおりである。

表 6 米国における情報提供要請に関する捜査手続の概要

捜査手続	概要
電子証拠の開示要求	・ 管轄裁判所が発した令状を得た場合、電子通信システムに保管されている 180 日以内の有線又は電子通信の内容について、電子通信サービスや遠隔情報処理サービスのプロバイダーに対し、開示（提供）を要求できる[25]。 ・ 遠隔情報処理サービスのプロバイダーに対し、電子通信の内容の開示を要求できる[26]。 ・ 電子通信サービス又は遠隔情報処理サービスのプロバイダーに対し、当該サービスの契約者又は利用者に関する記録やその他の情報（通信内容を含まない）の開示を要求できる[27]。
越境捜査における電子証拠の保全・開示要求	・ 適格外国政府の団体に、当該国の国民又は居住者である契約者又は利用者の記録や情報の開示を要求できる[28]。 ・ プロバイダーに対し、データが保存されているサーバの所在地が米国内外であるかを問わず、保有している通信、顧客に関する情報の保存、バックアップ、開示を要求できる[29]。

(2) サイバー空間上の通信傍受

合衆国法典（United States Code）第 18 編第 119 章「有線及び電子通信の傍受並びに口頭通信の傍受」第 2511 条[30]において、通信傍受という手段自体は法的に可能と規定されている。実施主体は連邦の捜査機関である（法令上は「捜査機関」とされているが、サイバー犯罪の捜査は連邦機関が行うと規定されているため）[31] [32] [33]。

---

[24] 連邦検察庁へのヒアリング結果に基づく。

[25] 通信保管法第 2703 条(a)

[26] 通信保管法第 2703 条(b)

[27] 通信保管法第 2703 条(c)

[28] 通信保管法 18 編第 2713 条(c)(h); 同第 119 章第 2523 条; 米クラウド法第 103 条(a)(1)

[29] 米クラウド法第 104 条

[30] 合衆国法典第 18 編第 119 章第 2511 条 https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter119&edition=prelim（2023 年 2 月 22 日閲覧）

[31] 米国司法省ウェブサイト https://www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime#（2023 年 2 月 22 日閲覧）

[32] National Cybersecurity Alliance ウェブサイト https://staysafeonline.org/stay-safe-online/identity-theft-fraud-cybercrime/reporting-cybercrime/（2023 年 2 月 22 日閲覧）

[33] 米国シークレットサービスウェブサイト https://www.secretservice.gov/investigation/cyber（2023 年 2 月 22 日閲覧）

ただし、通信傍受については、都度、実施の適切性や比例原則（proportionality）[34]等を勘案し、令状で具体的に指定されることで実施可能となる（正当な令状に基づく手法が適用されることで、取得された情報が証拠能力を持つ）[35]。

2021 年実績（サイバー犯罪に係る傍受の件数は非公開。有線・口頭・電子通信の傍受に関する連邦全体の合計件数は以下のとおりである[36]。

表 7　米国における有線・口頭・電子通信の傍受総件数（2021 年）

項目	件数
承認数	2,245 件（うち連邦機関 1,102 件）
傍受実施数	1,750 件（うち連邦機関 691 件） ・ 電子通信（電子書類、Fax、コンピュータ等）19 件（うち連邦機関 18 件） ・ 有線電話 778 件 ・ 口頭 8 件 ・ 以上の手段の組み合わせ 674 件（うち連邦機関 224 件）

(3) そのほかの捜査手法

身分秘匿捜査は、サイバー空間においても実施可能[37] [38]であるが、法的根拠はなく、判例法によるものとされる[39]。

過去の事例としては、米国シークレットサービスのオンライン詐欺となりすまし（identity theft、個人情報盗）事案を対象にしたプロジェクト「Operation Rolling Stone」において、2006 年 3 月に米国シークレットサービスの仮想身分捜査官が複数の被疑者を逮捕したものがある[40] [41]。また、2009 年にも、FBI がおとり捜査で児童ポルノ組織を摘発したプロジェクト「Operation Koala」について広報している[42]。

---

[34] 目的達成のために取られる手段と、権利・利益の制約との間に均衡を求める原則を指す。

[35] 連邦検察庁へのヒアリング結果に基づく。

[36] 連邦裁判所 2020 年通信傍受報告書（2020 年 12 月 31 日）https://www.uscourts.gov/statistics-reports/wiretap-report-2021; 傍受総数 https://www.uscourts.gov/statistics/table/wire-4/wiretap/2021/12/31; 傍受種別 https://www.uscourts.gov/statistics/table/wire-6/wiretap/2021/12/31（いずれも 2023 年 2 月 22 日閲覧）

[37] 米国司法省 Cybersecurity Unit 広報「Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources」（2020 年 2 月付）P7 https://www.justice.gov/criminal-ccips/page/file/1252341/download（2023 年 2 月 22 日閲覧）

[38] 連邦検察庁「Prosecuting Computer Crimes」p. 135 https://www.justice.gov/criminal/file/442156/download（2023 年 2 月 22 日閲覧）

[39] 連邦検察庁へのヒアリング結果に基づく。

[40] 米国司法省広報（2006 年 3 月 28 日付）https://www.justice.gov/archive/criminal/cybercrime/press-releases/2006/operationRollingStoneArrest.pdf（2023 年 2 月 22 日閲覧）

[41] 米国シークレットサービス広報（2006 年 3 月 28 日付）https://www.secretservice.gov/press/releases/2006/03/united-states-secret-services-operation-rolling-stone-nets-multiple-arrests（2023 年 2 月 22 日閲覧）

[42] FBI 広報（2009 年 9 月 2 日付）https://archives.fbi.gov/archives/news/stories/2009/february/jointhammer_020909（2023 年 2 月 22 日閲覧）

犯罪者のオンラインアカウントの（捜査機関による）乗っ取りについては、犯罪者にも人権があるとして、当該対象者が把握していない状況で乗っ取ることはできない。ただし、司法取引に応じた犯罪当事者のアカウントを、同意の上で捜査機関が用いることはあり得るとされる[43]。

不正に窃取された暗号資産の奪還に関しては、資金の追跡及び窃取先の特定後、家宅捜索で押収した紙のメモや PC 等からフォレンジック調査を経て犯罪者のウォレットの鍵（パスワード）を取得することができれば、差押えることが可能とされる。差押え令状に基づき、裁判所が発行したウォレットに窃取された資産が移される[44]。

コラム　不正に窃取された暗号資産の奪還

FBI が 2021 年 6 月、ランサムウェアの恐喝者「DarkSide（ダークサイド）」に支払われた 230 万ドルの暗号通貨（63.7 ビットコイン）を押収した事例がある[45]。押収した資産は、コロニアルパイプラインを標的にしたグループ「ダークサイド」の個人に対する身代金の支払いの収益とみられる。

コロニアルパイプラインは、同 5 月にコンピューターネットワークが DarkSide という名前の組織によってアクセスされ、ランサムウェア攻撃の被害を受けた結果、インフラの一部運用停止となる事態となり、約 75 ビットコインの身代金要求を受け支払ったことを FBI に報告したことで事件が発覚した。

宣誓供述書によると、FBI は、特定のビットコインアドレスからのみアクセスできる資産にアクセスするために必要なパスワードに相当する「private key」と呼ばれるものを持っており、ビットコインの公的台帳を基にビットコインの複数回の送金を追跡し、被害者の身代金の支払いとみられる約 63.7 ビットコインが特定のアドレスに送金されたことを特定したという。

資産の押収に取り組んだ部門では、ランサムウェア及びデジタル恐喝攻撃の増加に対抗するために組織されたタスクフォースを通じて取組を調整したとされる。

2.1.3 先制的な被害防止措置及び根拠となる法制度

先制的な被害防止のための捜査手法については、法律や規則で規定されているものではなく、検察において個々に適切性を判断した上で許可・指定の上、裁判所が発行する令状に記載されることで実行可能となる[46] [47]。

---

[43] 連邦検察庁へのヒアリング結果に基づく。

[44] 連邦検察庁へのヒアリング結果に基づく；被害者の財産の回復については、合衆国法典第 18 編第 3663a 条、3664 条等で規定

[45] 米国司法省広報（2021 年 6 月 7 日付）https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside（2023 年 2 月 22 日閲覧）

[46] 連邦検察庁へのヒアリング結果に基づく。

[47] 連邦検察庁「The Attorney General's Guidelines for Domestic FBI Operations」（2008 年 9 月 29 日署名）第 V 章 C. OTHERWISE ILLEGAL ACTIVITY 3、p.33 https://www.justice.gov/archive/opa/docs/guidelines.pdf（2023 年 2 月 22 日閲覧）

具体的な事例としては、攻撃元サーバへのアクセス（保管されたデータの閲覧、複写、改変を含む。）及び機能停止措置（テイクダウン）として、FBI が外国の法執行機関と合同で、海外に設置された Emotet のサーバへ合法的に接続し、IP アドレスを特定の上、米国内にあるサーバ上の Emotet 自体を法執行機関が作成したソフトウェアに置き換えたという Emotet のテイクダウン事例[48] [49]がある。

また、FBI には、対象とする被疑者の PC に「感染」させ、PC のシステムプロファイル情報やログイン名／アカウント情報等を取得し、FBI のサーバに送信するポリスウェアとされるツールがあるとされる[50]。

警察管理に係るサーバや代替サーバ等の運用では、警察管理によるハニーポッドとしてのシステム運用として「おとり掲示板」といったものの運営は可能である。ただし、そこに個人情報が書き込まれる場合は法的対処が必要となる。ほかに、FBI がオーストラリア連邦警察と協力しておとり捜査用に開発した偽装暗号化通信ネットワーク「ANOM」を用いて行われた共同捜査の事例[51]がある。

ANOM は、2019 年から秘密裏に運用されてきたものである。ANOM を用いた共同捜査の事例として、ANOM を構成する 12,000 以上の暗号化デバイスと約 2,700 万通のメッセージから得られた情報をもとに、EUROPOL が主体となって「OTF Greenlight/Trojan Shield」と呼ばれる作戦を 16 か国において実施した事例がある。700 件以上の家宅捜査を行い、800 人以上を逮捕したほか、8 トン以上のコカインの押収等の成果を上げたとされる。

なお、脆弱な状態のサーバについては、捜査機関から保有する企業への警告はするが、犯罪に使用される前に直接機能停止することはない。

2.1.4 民間事業者の義務及び根拠となる法制度

(1) 通信履歴（ログ）の保存義務

通信保管法において、政府機関は通信事業者に 180 日以内の有線又は電子通信の内容の提出要請ができると規定しており、事業者に保存が義務付けられている[52]。180 日以上保管されている通信内容は、以下の場合、契約者又は利用者に事前通知の上、捜査機関はプロバイダーに開示要求できる。なお、適用される罰則は、事業者の業種や事業を行っている場所

---

[48] EUTOPOL 広報（2021 年 1 月 27 日付）https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action（2023 年 2 月 22 日閲覧）

[49] 米国司法省広報（2021 年 1 月 28 日付）https://www.justice.gov/opa/pr/emotet-botnet-disrupted-international-cyber-operation（2023 年 2 月 22 日閲覧）

[50] Electronic Frontier Foudation ウェブサイト広報「New FBI Documents Provide Details on Government's Surveillance Spyware」（2011 年 4 月 29 日付）https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government（2023 年 2 月 22 日閲覧）

[51] FBI 広報（2021 年 6 月 8 日付）https://www.fbi.gov/news/stories/fbi-global-partners-announce-results-of-operation-trojan-shield-060821; EUROPOL 広報（同日付）https://www.europol.europa.eu/media-press/newsroom/news/800-criminals-arrested-in-biggest-ever-law-enforcement-operation-against-encrypted-communication（いずれも 2023 年 2 月 22 日閲覧）

[52] 通信保管法第 2703 条(a)(b) https://www.govinfo.gov/content/pkg/USCODE-2010-title18/html/USCODE-2010-title18-partI-chap121.htm（2023 年 2 月 22 日閲覧）

によって異なる。

① 政府機関が令状を取得した場合
② 法令・大陪審・裁判の召喚状によって許可された行政召喚状を使用した場合
③ 裁判所命令を取得した場合

また、電子通信サービスや遠隔情報処理サービスのプロバイダーは、政府機関の要求に基づく裁判所命令等に応じるため、所有記録や証拠の保存に必要なあらゆる措置を講じる義務がある。記録の保存期間は 90 日（再度要求があれば 90 日延長可能）[53]。

政府機関は、電子通信サービスや遠隔情報処理サービスのプロバイダーに対し、以下を要求できる。

① 管轄裁判所の令状を得た場合、電子通信システムに保管されている 180 日以内の有線・電子通信の内容
② 管轄裁判所が発した令状を得た場合、裁判所命令を取得した場合、契約者又は利用者の同意を得た場合等は、契約者又は利用者に関する記録やその他の情報（通信内容を含まない）

また、事業者は一定の条件下で、任意で通信内容及び加入者情報を開示することも可能である[54]。

(2) 捜査への協力義務

通信保管法第 2703 条(f)において、事業者は証拠保全のためのあらゆる措置を講じる義務が規定されているほか、合衆国法典第 18 編第 119 章第 2522 条において、法執行機関への支援義務も規定されている[55]。

ただし、情報提供や証拠保全以上のテイクダウンへの協力について、民間事業者に全般的な協力義務は課されていない。捜査機関は事業者に対して協力の依頼をすることは可能だが、強制することはできない。システム等へのバックドアの保全についても、依頼自体は可能であるが、証拠として（バックドアを含めた）コピーを取得するに留まる場合が多いとされる。なお、機器の製造元等への復号化等指示を特別に行うためには、裁判所命令が必要となる[56]。

捜査機関からの情報開示要請に応じた場合、利用者等への通知は不要と規定されている[57]。

サイバー犯罪やサイバー空間の脅威に関する情報は、セキュリティ関連事業者を始めとする民間企業が察知することになる。FBI と被害者を結びつけるのが民間企業となることか

---

[53] 通信保管法第 2703 条(f)

[54] 通信保管法第 2703 条(a)(b)(c)、第 2702 条

[55] 合衆国法典第 18 編第 119 章第 2522 条
https://uscode.house.gov/view.xhtml?path=/prelim@title18/part1/chapter119&edition=prelim（2023 年 2 月 22 日閲覧）

[56] 連邦検察庁及びコロンビア大教授へのヒアリング結果に基づく。

[57] 通信保管法第 2703 条(b)(c)

ら、サイバー捜査においては捜査機関と民間事業者との密接なコネクションが鍵となると考えられる[58]。

(3) サイバー事案発生時の公的機関等への報告義務

バイデン大統領は 2022 年 3 月、重要インフラのためのサイバー事案通報法（Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)）に署名し、即時発効した[59] [60]。これにより、公的機関や民間事業者、個人等で重要なインフラを所有または運用する者に、以下のケースにおけるサイバーセキュリティ・インフラセキュリティ庁（Cybersecurity & Infrastructure Security Agency（略称：CISA）、国土安全保障省に属する政府機関）への通報義務が課された[61] [62]。

- 対象となるサイバー攻撃を受けたと合理的に信じた時点から 72 時間以内
- ランサムウェア攻撃を受け身代金を支払った場合の 24 時間以内

なお、「サイバー事案」とは、情報システム上の情報または情報システムそのものを、差し迫った危険がなくとも現実的に危険にさらすような事案のことを指すとされる[63]。

2.1.5 サイバー捜査における人権確保に関する係争事例

マイクロソフト社が、データセンターに保存した顧客の電子メールを、FBI から令状に基づき顧客の電子メールを開示するよう 2013 年に命じられたことに対し、国外に保有する顧客情報を押収することはできないとして令状の取り消しを求め争った係争事例（注：米クラウド法制定前）[64]がある。ニューヨーク州南部連邦地方裁判所は 2014 年 7 月、マイクロソフト社の主張を退けたが、同社が控訴したところ、第 2 巡回区連邦控訴裁判所は同社の主張を認めた。これに対し、アイルランド政府は同社を支持するアミカスクリエ意見書（訴訟の当事者でない第三者が提出する意見陳述書）を提出し、他国のプライバシーを守るべきとの主張をした[65]。

なお、裁判はその後米クラウド法制定により、裁判の必要性がなくなったとして終結して

---

[58] コロンビア大教授へのヒアリング結果に基づく。

[59] 米国議会ウェブサイト https://www.congress.gov/bill/117th-congress/house-bill/5440; https://www.congress.gov/117/bills/hr5440/BILLS-117hr5440ih.pdf（2023 年 2 月 22 日閲覧）

[60] 重要インフラのためのサイバー事案通報法 https://www.congress.gov/bill/117th-congress/senate-bill/2875/text（2023 年 2 月 22 日閲覧）

[61] CISA ウェブサイト https://www.cisa.gov/circia; 「Sharing Cyber Event Information Fact Sheet」（2022 年 4 月公表）https://www.cisa.gov/sites/default/files/publications/CIRCIA_07.21.2022_Factsheet_FINAL_508%20c.pdf（いずれも 2023 年 2 月 22 日閲覧）

[62] 重要インフラのためのサイバー事案通報法第 2232 条

[63] 重要インフラのためのサイバー事案通報法第 2240 条(6)

[64] 第 2 巡回区連邦控訴裁判所 2016 年 7 月 14 日判決（United States v. Microsoft Corp., 829 F.3d 197 (2nd Cir. 2018)） https://www.justice.gov/archives/opa/blog-entry/file/937006/download（2023 年 2 月 22 日閲覧）

[65] マイクロソフト社広報「Government of Ireland, European MEP file amicus briefs in New York privacy case」（2014 年 12 月 23 日付）https://blogs.microsoft.com/on-the-issues/2014/12/23/government-ireland-european-mep-file-amicus-briefs-new-york-privacy-case/（2023 年 2 月 22 日閲覧）

いる[66]。

係争事例以外では、2018 年に米クラウド法が成立したことに対し、米国自由人権協会（American Civil Liberties Union、ACLU）は、LGBTQ[67]の権利や宗教的自由、男女平等のために闘っているグローバルな活動家の情報を米国企業が政府に開示するようなことになれば、それらの活動家に害が及ぶ可能性があるとして反対の意を表明している[68]。

[66] United States v. Microsoft Corp., 138 S. Ct. 1186 (2018)

[67] 性的少数者（セクシュアルマイノリティ）を表す言葉。レズビアン（Lesbian、同性を恋愛や性愛の対象とする女性）、ゲイ（Gay、同性を恋愛や性愛の対象とする男性）、バイセクシュアル（Bisexual、同性も異性も恋愛や性愛の対象とする人）の 3 つの性的指向と、トランスジェンダー（Transgender、（出生時の戸籍上の性とは異なる性自認を有する人）という性自認、及びクエスチョニングまたはクィア（Questioning / Queer、性的指向・性自認が定まらない人）を指す。
参考文献：内閣府「第 5 次男女共同参画基本計画 用語解説」（令和 2 年 12 月 25 日閣議決定）https://www.gender.go.jp/about_danjo/basic_plans/5th/pdf/yougo.pdf; 特定非営利活動法人 東京レインボープライドウェブサイト https://tokyorainbowpride.org/learn/lgbtq/（いずれも 2023 年 2 月 24 日閲覧）

[68] ACLU 記事「The Cloud Act Is a Dangerous Piece of Legislation」（2018 年 3 月 13 日付）https://www.aclu.org/blog/privacy-technology/internet-privacy/cloud-act-dangerous-piece-legislation（2023 年 2 月 22 日閲覧）

2.2 イギリス[69]

2.2.1 サイバー空間の脅威に対処するための体制

(1) サイバー事案の捜査・対策を担う公的機関等の体制・業務分担

国家犯罪対策庁（National Crime Agency (NCA)）が重大なサイバー犯罪の捜査を所管している[70]。NCA に設置された国家サイバー犯罪ユニット（National Cyber Crime Unit (NCCU)）が、サイバー犯罪捜査を統括する。NCA 全体の職員数は約 5,900 名（2022 年時点）[71]である。2023 年 2 月現在の NCA 組織図（幹部）[72]を図 1 に示す。

また、地方警察、及び地方警察により設立された組織犯罪ユニット（Regional Organised Crime Units (ROCUs)）が、所管地域のサイバー犯罪捜査を行っている[73]。

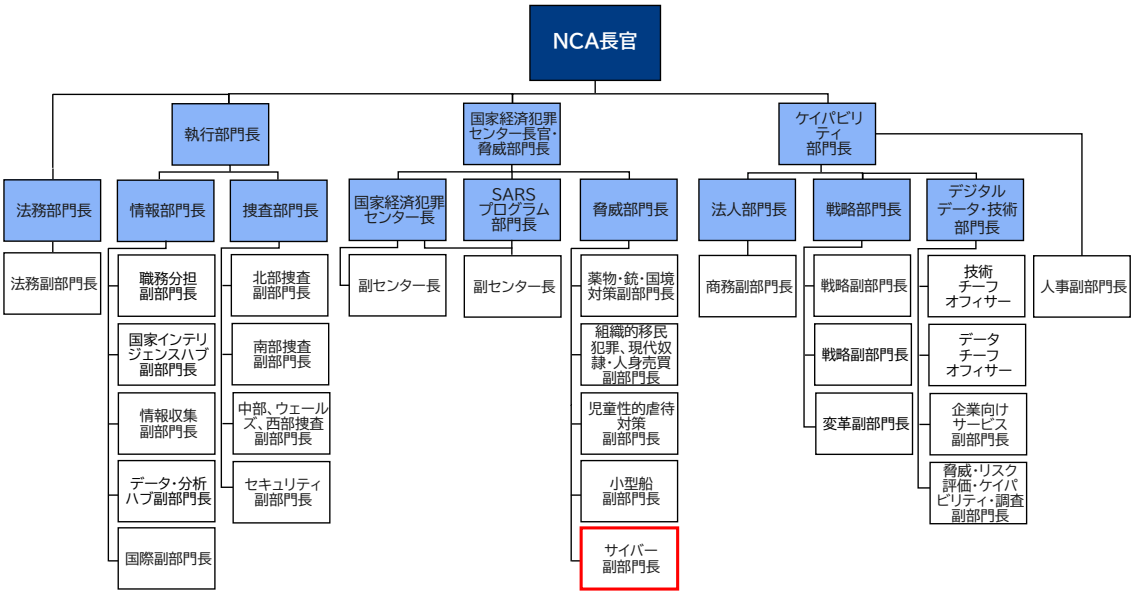

図 1　NCA 組織図（幹部）

（出所）NCA ウェブサイトよりエム・アール・アイ　リサーチアソシエイツ株式会社作成

---

[69] イギリス（グレートブリテン及び北アイルランド連合王国）は、イングランド、ウェールズ、スコットランド、北アイルランドの 4 地域から構成される。イングランド及びウェールズ、スコットランド、北アイルランドで法体系等が異なる。本資料ではイングランド及びウェールズを主な対象としている。

[70] 国家犯罪対策庁ウェブサイト https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/investigating-and-disrupting-the-highest-risk-serious-and-organised-criminals（2023 年 2 月 22 日閲覧）

[71] 国家犯罪対策庁「Annual Report and Accounts 2021- 2022」（2022 年発行）https://www.nationalcrimeagency.gov.uk/who-we-are/publications/606-national-crime-agency-annual-report-2021-2022/file（2023 年 2 月 22 日閲覧）

[72] 国家犯罪対策庁ウェブサイト https://www.nationalcrimeagency.gov.uk/who-we-are/our-leadership（2023 年 2 月 22 日閲覧）

[73] 国家犯罪対策庁ウェブサイト https://www.nationalcrimeagency.gov.uk/what-we-do/how-we-work/investigating-and-disrupting-the-highest-risk-serious-and-organised-criminals; HMICFRS ウェブサイト https://www.justiceinspectorates.gov.uk/hmicfrs/publication-html/regional-organised-crime-units-effectiveness/（いずれも 2023 年 2 月 22 日閲覧）

(2) サイバーセキュリティに関する総合調整を担う公的機関等の体制

政府通信本部（Government Communications Headquarters (GCHQ)）の傘下に設置されている国家サイバーセキュリティーセンター（National Cyber Security Centre (NCSC)）が、サイバーセキュリティに関する総合調整を実施している。NCSC は、以前 GCHQ の情報セキュリティ部門であった国家情報保証技術局（The UK government's National Technical Authority for Information Assurance（通称：CESG））や、サイバーアセスメントセンター（Centre for Cyber Assessment）、コンピュータ緊急対応チーム（CERT-UK）、国家インフラ保護センター（Centre for Protection of National Infrastructure）の専門家を集めて組成されている[74]。

(3) デジタルフォレンジック体制

NCA 内にデジタルフォレンジックを専門とする職員が在籍している。また NCA は、押収機器のフォレンジックのために外部事業者と協定を締結している。

ただし、NCA では初期評価や電子機器の分析のための技術的装置に限りがある。NCA や外部事業者における対応の遅れがあった場合に、NCA 職員は地方警察によるデジタルフォレンジックの結果を用いることがある[75]。

地方警察で行われているデジタルフォレンジックの支援に関しては、フォレンジック機能ネットワーク（Forensic Capability Network (FCN)）が行っている[76]。FCN は、全国警察本部長評議会（National Police Chiefs' Council (NPCC)）フォレンジックポートフォリオの傘下にあり、内務省から資金提供を受けている[77]。

2.2.2 効率的・効果的な捜査手法及び根拠となる法制度

(1) 遠隔地のサーバ等に所在する証拠の収集

1) ISP に対する捜索差押え令状等のオンライン送達

2020 年刑事手続規則（The Criminal Procedure Rules 2020）[78]に基づき、令状等のオンライン送達が可能である。

なお、刑事訴訟規則委員会（Criminal Procedure Rules Committee）及び司法省（Ministry of Justice）が令状等の申請フォームを設けており、1984 年警察・刑事証拠法（Police and Criminal Evidence Act 1984）等の一部の法律の、一部の条文に関して捜査令状の電子申請が可能である[79]。

---

[74] NCSC ウェブサイト https://www.ncsc.gov.uk/information/about-the-ncsc（2023 年 2 月 22 日閲覧）

[75] HMICFRS ウェブサイト https://www.justiceinspectorates.gov.uk/hmicfrs/publication-html/inspection-of-national-crime-agencys-crime-reduction-function/（2023 年 2 月 22 日閲覧）

[76] FCN ウェブサイト https://www.fcn.police.uk/who-we-are（2023 年 2 月 22 日閲覧）

[77] FCN ウェブサイト https://www.fcn.police.uk/about-us/our-governance、https://www.fcn.police.uk/who-we-are（いずれも 2023 年 2 月 22 日閲覧）

[78] 2020 年刑事手続規則 https://www.legislation.gov.uk/uksi/2020/759/contents/made（2023 年 2 月 22 日閲覧）

[79] 英国政府ウェブサイト https://www.gov.uk/guidance/criminal-procedure-rules-forms（2023 年 2 月 22 日閲覧）

2) 海外の ISP に対する直接の情報提供要請及び回答データのオンライン受領（その際の暗号化措置の手法）

2019 年犯罪（国外データ提出命令）法（Crime (Overseas Production Orders) Act 2019）に基づき、指定された国際協力協定のもと一定の条件が満たされている場合に、情報提供要請が可能である[80]。それ以外の場合は、直接 ISP に要請するのではなく、刑事共助条約（MLAT）に基づき相手国の当局に要請する[81]。

なお、上記の「指定された国際協力協定」に該当する、米クラウド法に基づく米英行政協定[82]は、2022 年 10 月 3 日に発効した[83]。

3) 国内事業者が保有する海外所在サーバからの情報提供要請

2016 年調査権限法（Investigatory Powers Act 2016）上は、原則として国内所在のサーバに関する要請が想定されている。

(2) サイバー空間上の通信傍受

1994 年情報保安法（Intelligence Services Act 1994）[84]において、英国秘密情報部（Secret Intelligence Service (SIS)）及び GCHQ による活動について規定されている。同法第 3 条では、重大犯罪の予防・確知等の目的のもと、電子機器等の監視や妨害、電子機器等からの情報収集等を行うことが、GCHQ の役割として規定されている。

また、2016 年調査権限法[85]では、Part 2（第 15～60 条）の「通信の合法的傍受」において、令状に基づく傍受・捜査、合法的傍受に関するその他の方法等について規定されている。第 15 条には、傍受・捜査のために発行される令状として、表 8 に記載するとおり 3 種類の令状があることが示されている。

---

[80] 2019 年犯罪（国外データ提出命令）法 https://www.legislation.gov.uk/ukpga/2019/5/contents/2019-02-12（2023 年 2 月 22 日閲覧）

[81] 内務省ウェブサイト https://www.gov.uk/guidance/mutual-legal-assistance-mla-requests（2023 年 2 月 22 日閲覧）

[82] 英国政府広報「UK and US sign landmark data access agreement」（2019 年 10 月付）https://www.gov.uk/government/news/uk-and-us-sign-landmark-data-access-agreement（2023 年 2 月 22 日閲覧）

[83] 米国司法省広報「Landmark U.S.-UK Data Access Agreement Enters into Force」（2022 年 10 月付）https://www.justice.gov/opa/pr/landmark-us-uk-data-access-agreement-enters-force（2023 年 2 月 22 日閲覧）

[84] 1994 年情報保安法 https://www.legislation.gov.uk/ukpga/1994/13/contents（2023 年 2 月 22 日閲覧）

[85] 2016 年調査権限法 https://www.legislation.gov.uk/ukpga/2016/25/contents（2023 年 2 月 22 日閲覧）

表 8　傍受・捜査のために発行される令状の種類

令状の種類	主な内容
標的型傍受令状（Targeted interception warrants）	郵便または電子システムにおいて通信傍受を行うこと等を認める令状
標的型捜査令状（Targeted examination warrants）	第 152 条(4)（英国諸島における個人の通信の特定禁止）に違反する形で、関連する通信コンテンツに対して、選択的に傍受することを認める令状
共助令状（Mutual assistance warrants）	以下の条件のうち一つ以上に該当する場合に発行される令状 ・ 刑事共助条約に基づく通信傍受に関する援助要請 ・ 共助に関する条約等に基づく、英国内外の当局に対する傍受に係る援助の提供 ・ 取得された通信情報の開示

2016 年調査権限法の行為規範（Code of Practice）[86]には、同法に基づく通信傍受を行う場合の手続き等に関するガイダンスが示されている。

上記の令状に基づく通信傍受は、合法的な傍受として認められており、上掲の行為規範に則って当該手法により入手した情報の証拠能力は認められる。

なお、第 19 条によると令状は、緊急の場合を除き、司法委員の承認を得た上で内務大臣が発行する。

(3) そのほかの捜査手法

2000 年調査権限規制法（Regulation of Investigatory Powers Act 2000）[87]の Part II 等に基づき、仮装身分捜査を行うことが可能である。なお、2000 年調査権限規制法に基づく仮装身分捜査は、オンライン上であるかどうかを問わず、特定の関係性を通じて情報や諜報の提供を行うことを主な目的としたものである[88]。

2013 年調査権限規則（内密の人的情報源：関連情報源）（The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013）[89]も、仮装身分捜査の根拠となる規則である。また、2021 年内密人的情報源（犯罪行為）法（Covert Human Intelligence Sources (Criminal Conduct) Act 2021）[90]によると、国家安全保障や、犯罪の防止・確知、無秩序な状態の防止等の目的のもと、一定の条件を満たした場合に、許可を受けた上

[86] 2016 年調査権限法（通信傍受　行為規範）
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1123773/revised_Interception_of_Communications_Code_of_Practice_Dec_2022.pdf（2023 年 2 月 22 日閲覧）

[87] 2000 年調査権限規制法 https://www.legislation.gov.uk/ukpga/2000/23/contents/enacted（2023 年 2 月 22 日閲覧）

[88] ポーツマス大講師らへのヒアリング結果に基づく。

[89] 2013 年調査権限規則（内密の人的情報源：関連情報源）
https://www.legislation.gov.uk/uksi/2013/2788/contents/made（2023 年 2 月 22 日閲覧）

[90] 2021 年内密人的情報源（犯罪行為）法 https://www.legislation.gov.uk/ukpga/2021/4/contents/enacted（2023 年 2 月 22 日閲覧）

で仮装身分捜査を行うことが可能である。

上記いずれの法令も、サイバー事案を含めた犯罪等に関する仮装身分捜査に関して一般的に規定するものである。

ハッキングについては、欧州議会の報告書[91]によると、2016 年調査権限法等において通信・機器データやその他情報の取得という目的のみにおいて認められており、法執行機関によるその他のハッキング行為に関して、1997 年警察法（Police Act 1997）[92] Part III（財産に関する行為に係る権限）に基づき実施可能との記載がある。ただし、機器干渉に係る法的枠組みにおいては、令状に基づき講じることができる技術的な手段を指定する規定はなく、英国の法執行機関が利用可能なツールに関してもほとんど情報が公開されていないとされる。

また、暗号資産の差押えは、法律及び判例に基づき行われる[93]。財産の押収は 2002 年犯罪収益法（Proceeds of Crime Act 2002）[94]等に基づき可能である。なお、2023 年 2 月現在、経済犯罪及び企業透明性法案（Economic Crime and Corporate Transparency Bill）[95]が提出されており、同法案には暗号資産の押収等に関する規定も含まれている。

これらの捜査手法で得られた情報に証拠能力が認められるかに関しては、1984 年警察・刑事証拠法に基づき、令状や証拠の内容等を踏まえて判断される[96]。

コラム　暗号資産の押収事案

マネーロンダリングに関連する暗号通貨の押収事案は英国内で複数確認されており、2021 年にロンドン警視庁はマネーロンダリングに関する捜査の一環で、暗号通貨の押収を複数回行っているとされる[97]。

報道によると、2021 年 6 月には、同庁の経済犯罪部隊（Economic Crime Command）の捜査員がマネーロンダリングの疑いで 39 歳の女を逮捕し、国際的なマネーロンダリングに関する約 1 億 8,000 万ポンド相当の暗号通貨をロンドンで押収した。これはイギリスにおける暗号通貨の押収額として当時過去最高であり、世界的にも最大規模の押収額の一つとされる。

記事においてロンドン警視庁の副長官は、デジタルプラットフォームが発展していくとともに、暗号通貨を使って資金洗浄をする組織犯罪者が増えていると指摘している[98]。

---

91 欧州議会報告書「Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices」（2017 年 3 月発行）
https://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf（2023 年 2 月 22 日閲覧）

92 1997 年警察法 https://www.legislation.gov.uk/ukpga/1997/50/contents（2023 年 2 月 22 日閲覧）

93 ポーツマス大講師らへのヒアリング結果に基づく。

94 2002 年犯罪収益法 https://www.legislation.gov.uk/ukpga/2002/29/contents（2023 年 2 月 22 日閲覧）

95 経済犯罪及び企業透明性法案 https://bills.parliament.uk/publications/49554/documents/2831（2023 年 2 月 22 日閲覧）

96 ポーツマス大講師らへのヒアリング結果に基づく。

97 ロイター通信記事「British police seize record $408 million haul of cryptocurrency」（2021 年 7 月 13 日付）
https://www.reuters.com/world/uk/british-police-seize-250-million-cryptocurrency-2021-07-13/（2023 年 2 月 22 日閲覧）

98 BBC 放送記事「Met Police seize record £180m of cryptocurrency in London」（2021 年 7 月 13 日付）
https://www.bbc.com/news/uk-england-london-57816644（2023 年 2 月 22 日閲覧）

2.2.3 先制的な被害防止措置及び根拠となる法制度

国家サイバー部隊（National Cyber Force (NCF)）は、GCHQ、国防省、SIS、国防科学技術研究所の職員を集めて組成され、法執行機関とも協力しながら攻撃的なサイバー作戦を行っている。NCF の活動の根拠法令は 1994 年情報保安法、2000 年調査権限規制法、2016 年調査権限法等であり[99] [100]、被害防止措置のための攻撃的な措置は、これらの法令等に基づき行われる。

なお、英国では通常個々のサイバー作戦の詳細を明らかにしないが、「国家サイバーセキュリティ戦略 2022（National Cyber Strategy 2022）」[101]によると、NCF の活動には以下が含まれている。

- 犯罪グループによるオンラインプラットフォームやサービスの利用を妨害することで、犯罪グループが利益をあげないようにする
- 敵対者がサイバー攻撃のために用いるインフラを破壊することで、英国等をサイバー攻撃から守る　等

また、英国の法執行機関等による先制的な措置の適用事例として、前述の欧州議会の報告書には、携帯電話の通信への侵入を目的として、GCHQ がハッキングのためのマルウェアを送信したことが確認されているとの記載がある。また NCSC は、テイクダウンの一環として、フィッシングサイトやマルウェア等の削除を実施している[102]。他国と協力して違法な VPN 等のテイクダウンを実施した事例も、複数確認されている。

警察管理に係るサーバのハニーポッド等としての運用や、代替サーバ等の運用に関しては、利用を禁止するような特定の法律はない[103]。

---

[99] 英国政府広報「Permanent location of National Cyber Force campus announced」（2021 年 10 月付）https://www.gov.uk/government/news/permanent-location-of-national-cyber-force-campus-announced（2023 年 2 月 22 日閲覧）

[100] 国家サイバー部隊「NATIONAL CYBER FORCE EXPLAINER」https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1041113/Force_Explainer_20211213_FINAL__1_.pdf（2023 年 2 月 22 日閲覧）

[101] 「国家サイバーセキュリティ戦略 2022」https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022

[102] 国家サイバーセキュリティーセンターウェブサイト https://www.ncsc.gov.uk/information/takedown-service（2023 年 2 月 22 日閲覧）

[103] ポーツマス大講師らへのヒアリング結果に基づく。

コラム　VPN のテイクダウン、EncroChat への侵入

2021 年 6 月にオランダ国家警察主導で行われた DoubleVPN のテイクダウンでは、NCA が英国側のノード（接続ポイント）をオフラインにし、また同 VPN 経由でネットワークへの非合法的なアクセスを受けた多数の英国企業を特定した。同事案について NCA 担当者は、「犯罪に利用されるこの種のサービスに対する、法執行機関による初めての直接的な行動である」と説明した[104]。

ほかにも、NCA と ROCUs、地方警察が 2020 年に、他国との連携のもとで EncroChat に侵入して、ユーザのやり取りを監視し摘発するという「Venetic 作戦」を行った。NCA によると、この作戦は英国における同様の作戦の中でも最大かつ最も重要なものである[105]。

2.2.4 民間事業者の義務及び根拠となる法制度

(1) 通信履歴（ログ）の保存義務

2016 年調査権限法 Part 4 等に基づき、一定の条件のもと、通信事業者に対して通信データを最大 12 か月保全するよう求めることが可能である。

(2) 捜査への協力義務

暗号化等の解除は、2000 年調査権限規制法 Part III に基づき要請可能であり、要請に応じない場合は罰則がある。

(3) サイバー事案発生時の公的機関等への報告義務

2018 年 NIS 規則（The Network and Information Systems Regulations 2018）[106]において、エネルギー・医療・デジタルインフラ等の基幹サービスを提供する事業者に対し、サービスに影響をもたらす事案に限定する形で報告義務を課している。なお、同規則改正の検討が現在進められており、マネージドサービスプロバイダ（Managed Service Providers）[107]を対象機関に含めることや、報告義務の強化等が改正案に盛り込まれている[108]。

(4) 情報開示に関する利用者等への通知義務

2018 年データ保護法（Data Protection Act 2018）Part 3（第 29～81 条）「法執行機関の処

---

104 国家犯罪対策庁ウェブサイト https://www.nationalcrimeagency.gov.uk/news/doublevpn-takedown-nca-takes-uk-server-of-criminal-network-offline（2023 年 2 月 22 日閲覧）

105 国家犯罪対策庁ウェブサイト https://www.nationalcrimeagency.gov.uk/news/operation-venetic（2023 年 2 月 22 日閲覧）

106 2018 年 NIS 規則 https://www.legislation.gov.uk/uksi/2018/506（2023 年 2 月 22 日閲覧）

107 コンピュータ、ネットワーク等の運用・保守・監視等を行う事業者のこと。

108 英国政府広報（2022 年 1 月 19 日付）https://www.gov.uk/government/news/new-laws-proposed-to-strengthen-the-uks-resilience-from-cyber-attack（2023 年 2 月 22 日閲覧）

理」において、法執行機関による個人データの処理の原則や利用者の権利、管理者や処理者の義務等について規定されている[109]。同法第 35 条では、利用者が処理に合意している場合、もしくは当局の任務遂行のために必要な場合には、法執行のための個人データの処理が合法的行為であると規定されている。また第 44 条では、公的または法的な捜査・手続きの妨害や、犯罪の予防・確知・捜査の妨害等を回避するためであれば、利用者の基本的な権利や正当な利益を考慮した上で、利用者への通知を全体的もしくは部分的に制限できることが規定されている。

2.2.5 サイバー捜査における人権確保に関する係争事例

人権 NGO（非政府組織）のヒューマン・ライツ・ウォッチは 2019 年に、米国と英国が締結した米クラウド法に基づく行政協定について、法執行機関による通信データへのアクセスの障壁を下げるものであり、2 か国の市民のプライバシーが十分に守られなくなるとして、同協定の発効に反対する声明を発出していた[110]。

[109] 2018 年データ保護法 https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted（2023 年 2 月 22 日閲覧）

[110] ヒューマン・ライツ・ウォッチ広報「Groups Urge Congress to Oppose US-UK Cloud Act Agreement」（2019 年 10 月 29 日付）
https://www.hrw.org/sites/default/files/supporting_resources/usuk_cloud_act_letter_20191028.pdf（2023 年 2 月 22 日閲覧）

2.3 ドイツ

2.3.1 サイバー空間の脅威に対処するための体制

(1) サイバー事案の捜査・対策を担う公的機関等の体制・業務分担

1) 連邦刑事庁

ドイツは連邦制を採る。日本の憲法に相当する連邦基本法において、連邦の所管あるいは連邦と州の共同所管が定められていない限り、国家権力の行使及び国家任務の遂行は、州の責任である[111]。この原則に基づき、通常の犯罪捜査は、各州警察が行う。

ただし、連邦基本法では、別途連邦法により連邦刑事庁（Bundeskriminalamt (BKA)）を設置し[112]、1 つの州で所管できない州の境を超えるリスクのある事案や、州当局から要請があった場合の国際テロ防止に係る対応、その他刑事警察業務に係る連邦・州協力、国家犯罪、公安、安全保障事案等を行う連邦当局としての権限・役割等を定めるよう規定している[113]。これに基づき制定されたのが、BKA の設置法に相当する連邦刑事庁法である。

同法第 4 条では、麻薬、マネーロンダリングほか国際組織犯罪、国家犯罪、管轄地不定の犯罪、安全保障、社会基盤に対する犯罪、国外諜報に係る犯罪等を BKA 所管事案として指定するとともに、上記に該当しない場合でも、州当局から BKA に捜査依頼があった場合や、連邦内務省が BKA による対応が適当と判断した場合、連邦検事総長の要求・指示があった場合は、州警察ではなく BKA が刑事捜査を行うとしている。連邦機関である BKA が捜査を実施する際には、関係する州の当局にその旨を遅滞なく通知する。また BKA が各地で捜査を行う際には、BKA が各州警察機関に対し、協力の指示を出すことができる[114]。

BKA ウェブサイトでは、BKA が対応する刑事犯罪の一つとして、サイバー犯罪が挙げられている。サイバー犯罪においても、対応地域が限られる場合には州警察が対応するが、BKA は全国警察組織の調整、国際協力のハブ、また連邦関連施設や重要インフラ等が関係する場合、また BKA に捜査依頼があった場合等で捜査活動を担う。

こうした活動を担う部署として、BKA 内には、サイバー犯罪局（Abteilung “Cybercrime”（CC））が設置されている。BKA では従来、重大・組織犯罪局がサイバー犯罪捜査を所管していたが、近年のサイバー犯罪の増加・高度化を背景に、2020 年 4 月に新たに独立した 1 局として CC 局が設置された[115] [116]。

2023 年 1 月現在の BKA の組織図及びサイバー犯罪捜査の主担当部署である CC 局の構成

---

111 連邦基本法第 30 条 https://www.gesetze-im-internet.de/gg（2023 年 2 月 22 日閲覧）

112 連邦基本法第 87 条

113 連邦基本法第 73 条

114 連邦刑事庁法第 4 条 https://www.gesetze-im-internet.de/bkag_2018/（2023 年 2 月 22 日閲覧）

115 BKA CC 局ウェブサイト https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html（2023 年 2 月 22 日閲覧）

116 BKA 広報「連邦刑事庁、サイバー犯罪との闘いを強化」（2020 年 4 月 1 日付）https://www.bka.de/SharedDocs/Pressemitteilungen/DE/Presse_2020/pm200401_AbteilungCC.pdf?__blob=publicationFile&v=4（2023 年 2 月 22 日閲覧）

を図 2 に示す[117]。

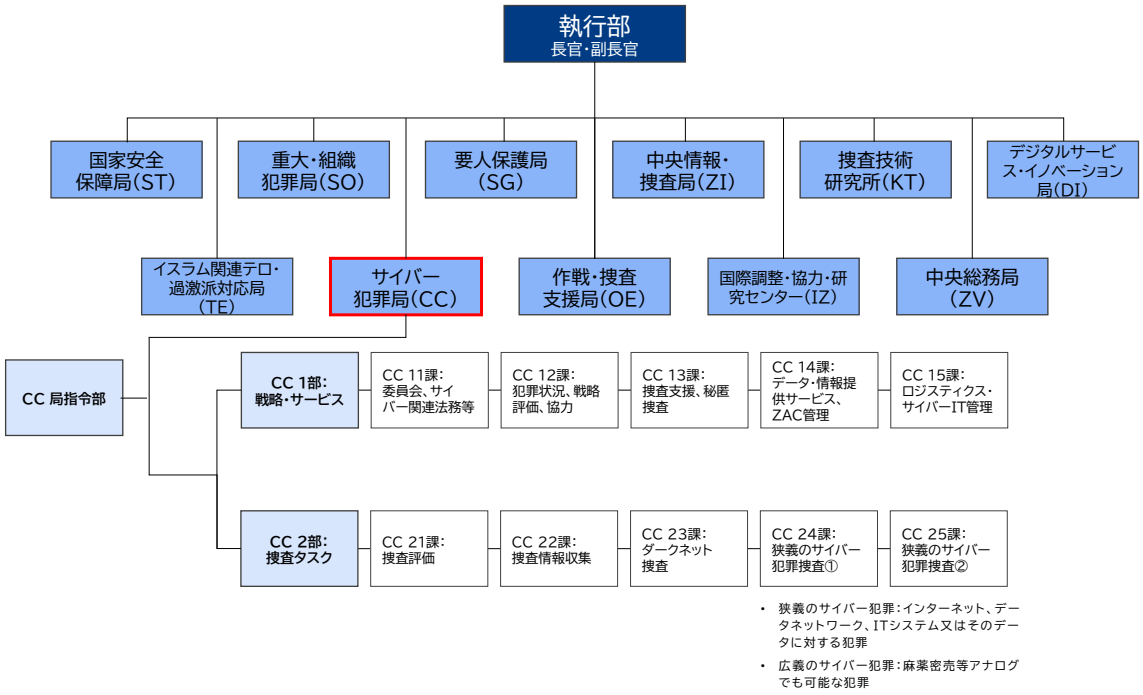

図 2　連邦刑事庁（BKA）及びサイバー犯罪局の組織構成

（出所）BKA ウェブサイトよりエム・アール・アイ　リサーチアソシエイツ株式会社作成

CC 局は、特に「狭義のサイバー犯罪」（インターネットその他データネットワーク、IT システム、及びそれらに含まれるデータ等を対象とする犯罪）を対象に捜査活動を行う。CC 局の活動内容と目的は次のように説明されている [115]。

- サイバー空間で活動する犯罪者に対する捜査を実施し、ドイツの主要なサイバー攻撃に関わる犯罪ネットワーク及び体制を解体する
- 連邦及び州警察が実施する高度に複雑なサイバー技術を用いた捜査の基礎となるような、関連情報の取得・処理及び分析能力を確保する
- ドイツ連邦施設や重要インフラに対するサイバー攻撃を追跡する
- BKA 内上層部に対し、狭義のサイバー犯罪に関する刑事政策上の課題について助言する
- 助言活動を通じて、サイバー犯罪関連の法規定のさらなる発展に積極的に寄与する

図 2 に示すとおり、CC 局は戦略、政策法制度関連、調査支援等を主とする CC1 と、サイバー犯罪捜査の実行部隊である CC2 に分かれている。

なお、CC 局の所属人員数は不明である。2022 年現在、BKA には全体で 8,139 名の職員が

[117] BKA 組織図（2023 年 1 月付）
https://www.bka.de/SharedDocs/Downloads/DE/DasBKA/Organisation_Aufbau/organigramm_neu.pdf?__blob=publicationFile&v=58（2023 年 2 月 22 日閲覧）

在籍し、うち 4,190 名が刑事であるが、部局別の人員配分は公表されていない[118]。

このほか、BKA では CC 局以外に、作戦・捜査支援局、犯罪技術研究所等も、デジタルフォレンジックの側面から捜査活動に関与するが、これら組織の部署構成については、(3)で後述する。

2) 州警察におけるサイバー犯罪捜査部局（ベルリン州）

上述のとおり、ドイツにおける犯罪捜査は原則として州警察の所管である。州や国をまたぐ広域犯罪、組織犯罪、高度なオペレーションを要する事案等では、上掲の BKA が捜査を担うため、大規模なサイバー犯罪では BKA 主導となることが主である。ただしサイバー犯罪であっても、州内の犯罪への対応は州警察が行う他、州警察は BKA が実施する広域捜査において、BKA の指示の下、各地域での捜査に協力する。

ドイツには 16 の州があるが、このうちベルリン州（首都ベルリン市）刑事庁（Landeskriminalamt Berlin (LKA-Berlin)、以下州刑事庁とする）における組織構成、及びサイバー犯罪捜査における役割は以下のとおりである。

州刑事庁は、州内の刑事政策を担うとともに、州内各警察署と協力して、刑事犯罪捜査を担うほか、BKA のベルリン州コンタクトポイントとして対応を行う[119]。2021 年 8 月時点のベルリン州刑事庁の組織構成及びサイバー犯罪捜査の主担当部署である LKA7（捜査支援、分析、サイバー犯罪）局の構成を図 3 に示す[120]。

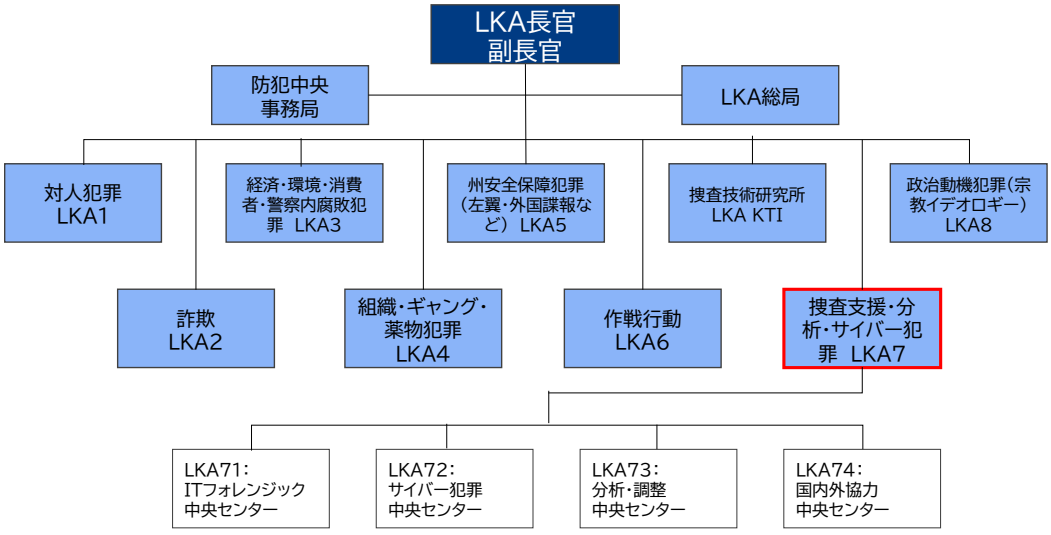

図 3　ベルリン州刑事庁（LKA-Berlin）及びサイバー犯罪対応部局の組織構成

（出所）LKA ウェブサイトよりエム・アール・アイ　リサーチアソシエイツ株式会社作成

---

[118] BKA ウェブサイト https://www.bka.de/DE/DasBKA/FaktenZahlen/faktenzahlen_node.htm（2023 年 2 月 22 日閲覧）

[119] ベルリン州刑事庁ウェブサイト https://www.berlin.de/polizei/dienststellen/landeskriminalamt/（2023 年 2 月 22 日閲覧）

[120] ベルリン州警察組織図（2021 年 8 月付）
https://www.berlin.de/polizei/_assets/dienststellen/organigramm_polizei_berlin_2021-08-27.pdf（2023 年 2 月 22 日閲覧）

図 3 のとおり、LKA7 局では LKA71 でデジタルフォレンジック、LKA72 でサイバー犯罪捜査を担当している。LKA7 局全体では、約 200 人の職員が在籍している[121]。

デジタルフォレンジックを担当する LKA71 については、(3)で後述のとおり、39 名の職員が所属していることが示されているが[122]、サイバー犯罪捜査の中央部署である LKA72 の人員数は不明である。

(2) サイバーセキュリティに関する総合調整を担う公的機関等の体制

ドイツではサイバー犯罪、サイバーインテリジェンス、サイバー防衛の関係機関の連絡調整組織として、2011 年の閣議決定に基づき、「国家サイバー防衛センター（Nationales Cyber-Abwehrzentrum (NCAZ)）」が設置された。事務局は、連邦内務省傘下の連邦情報技術安全庁である[123]。NCAZ は、サイバーセキュリティの省庁・機関間連絡・調整プラットフォームである。参加組織はそれぞれ NCAZ に連絡官を出しており、日次ブリーフィング、作業部会等を通じてドイツ国内のサイバーに係る犯罪、防衛、諜報等事案の情報共有・対策のハブとして活動している。

NCAZ は複数官署から担当者が集まるプラットフォームであり、連絡担当官の人数等詳細は文献調査では把握できていない。

NCAZ の参加組織及び各官署が国家サイバーセキュリティにおいて担う役割を以下に示す[124] [125]。

表 9　NCAZ の中核メンバー

組織名	役割
連邦刑事庁（BKA）	連邦内務省傘下。サイバー犯罪（CC）局を中心にサイバー犯罪捜査を実施。また、連邦各州の法執行機関に設置されたサイバー犯罪関連情報の通報連絡窓口「サイバー犯罪コンタクトポイント（Zentrale Ansprechstellen Cybercrime (ZAC)）」の連邦中央窓口として、情報の共有集約を管理。また、連邦・州の警察情報集約システムである「警察中央情報システム（Elektronische Informationssystem der Polizei (INPOL)）」を運用管理。事案によっては軍・情報機関ともファイルを共有する。

121 ベルリン州刑事庁ウェブサイト https://www.berlin.de/polizei/dienststellen/landeskriminalamt/lka-7/（2023 年 2 月 22 日閲覧）

122 ベルリン警察ウェブサイト https://www.berlin.de/polizei/verschiedenes/vorgestellt/artikel.1102109.php（2023 年 2 月 22 日閲覧）

123 連邦議会文書 Drs 17/5694（2011 年 5 月 2 日付）https://dserver.bundestag.de/btd/17/056/1705694.pdf（2023 年 2 月 22 日閲覧）

124 BKA ウェブサイト https://www.bka.de/DE/UnsereAufgaben/Kooperationen/NCAZ/ncaz_node.html（2023 年 2 月 22 日閲覧）

125 スイス連邦工科大学 Center for Security Studies (CSS) 報告書「National Cybersecurity Strategies in Comparison – Challenges for Switzerland」（2019 年 3 月 18 日発行） https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/363696/Cyber-Reports-2019-08-NationalCybersecurityStrategiesinComparison.pdf?sequence=1&isAllowed=y（2023 年 2 月 22 日閲覧）

組織名	役割
連邦情報技術安全庁	連邦内務省傘下。国家 IT のセキュリティ・防護、事故対応に加え、国家サイバーセキュリティ戦略の立案を担当。NCAZ の事務局。
連邦市民保護・災害救援庁	連邦内務省傘下。重要インフラのサイバー攻撃等からの防御（官民協力含む）を担う。
連邦国防省	サイバー・情報空間指令部が、サイバー国防の観点から、重要インフラへのサイバー含む攻撃からの防衛支援、サイバー防衛・攻撃能力の育成、電子戦タスクの実行、プロパガンダ・偽情報の調査、軍事情報収集とリスク分析を実施。
連邦憲法擁護庁	連邦内務省傘下。主に国内の反憲活動に対するサイバー含む諜報・防諜に従事（ネオナチ・イスラム過激派等）。
連邦情報局	連邦首相府傘下。主に対外国のサイバー含む諜報・防諜に従事。
連邦警察	連邦内務省傘下。国境警備、重要施設警備、テロ・武力攻撃への対処等国家事案対応における警備警察業務の所掌に関わる範囲で、サイバー事案に協力する。

上掲の中核メンバーに加え、バイエルン州、ヘッセン州のサイバー防衛センター、バンベルク、ケルンのサイバー対策検察、連邦金融監督庁もパートナーとして参加している。

(3) デジタルフォレンジック体制

（1）で上述のとおり、サイバー犯罪の捜査においては、連邦刑事庁（BKA）が広域犯罪を中心に捜査の中心的な役割を担うほか、各州警察でも対応を行っており、それぞれの組織にデジタルフォレンジックを担当する組織が存在する。

1) 連邦刑事庁

BKA には、犯罪捜査全般の技術分野の調査や、作戦行動を支援する部署として作戦・捜査支援局（Abteilung “Operative Einsatz”、OE 局）が設置されている。OE1 部のもと、国内 3 か所（ヴィースバーデン（BKA 本部）、ベルリン（首都）、メッケンハイム（旧首都ボン近郊））でデジタルフォレンジックを行っている。なお OE 局ではフォレンジック以外に IT・通信傍受（OE2 部）、身分秘匿捜査（OE4 部）等も担う。BKA の OE 局の組織構成図を図 4 に示す。

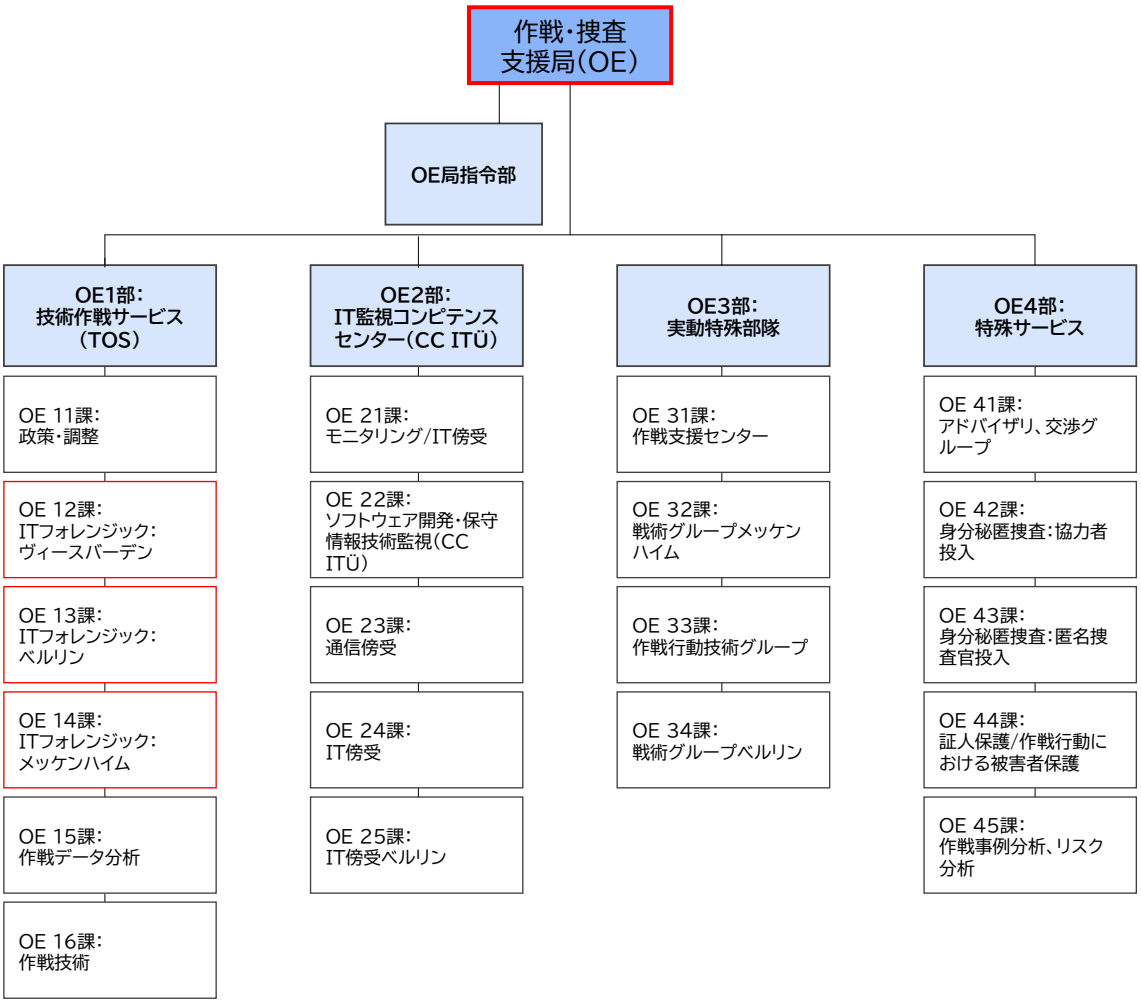

図 4　BKA におけるフォレンジック担当組織（OE 局組織図）

（出所）BKA ウェブサイトよりエム・アール・アイ　リサーチアソシエイツ株式会社作成

OE 局のデジタルフォレンジックでは、新旧技術による電子証拠（最新のサーバやコンピュータ、モバイル機器だけでなく、旧式の携帯情報端末（Personal Digital Assistant (PDA)）や磁気ディスク、テープ、電子書籍端末等も含む）のフォレンジックにも対応する。媒体が物理的に破損している場合もあるが、それらも一定程度調査が可能であるとしている。押収した媒体はイメージを作成、OE 局で調査が行われる。OE 局では、クラウド上のデータに関するフォレンジックに係る捜査支援や証拠保全を目的とした手法、ツールの開発も行っている。

BKA 内部においてデジタルフォレンジックは実施可能であるが、捜査部隊等に迅速に捜査情報を提供するには、膨大かつ外国語も含むデータの解析を効率的・効果的に行う必要がある。そのため、BKA は、高い技能を持つ IT 専門家への外注を行っているとしている。

BKA は国内外の安全保障当局や主要な科学機関と協力して、デジタルフォレンジックに係る研究開発を進めているとしている[126]。

[126] BKA ウェブサイト https://www.bka.de/DE/UnsereAufgaben/Ermittlungsunterstuetzung/Technologien/IT-Forensik/it_forensik.html（2023 年 2 月 22 日閲覧）

2) 州警察におけるサイバー犯罪捜査部局（ベルリン州）

（1）に示したとおり、ベルリン州刑事庁では、LKA7 局（捜査支援・分析・サイバー犯罪局）内の LKA71（IT フォレンジック中央センター）で、デジタルフォレンジックを担っている。LKA7 局ウェブサイトによると、LKA71 は、押収された IT システムとデータキャリアの調査を扱い、さまざまな分析技術・ツールを用いて証拠を特定、保全、準備し刑事訴訟のためのドキュメンテーションを行う。調査対象となるシステムには、携帯電話、コンピュータ、記憶媒体に加えて、ナビゲーションシステム、ビデオシステム、ネットワークルータ等の技術装置も含まれる[127]。

LKA71 は 39 名の職員と、4 つの部門で構成される。LKA71 として直接的な犯罪捜査（犯人の捜索）は行わないが、フォレンジックチームとして他の部門に対し、必要な支援を提供するとされている[128]。LKA7 局を中心とした組織構成は図 3 に前掲したとおりである。

2.3.2 効率的・効果的な捜査手法及び根拠となる法制度

(1) 遠隔地のサーバ等に所在する証拠の収集

1) ISP に対する捜索差押え令状等のオンライン送達

ドイツにおける刑事手続きは、刑事訴訟法（Strafprozeßordnung (StPO)）に定められている。刑事訴追、司法文書の電子文書化や電子送達については、StPO32b 条（刑事訴追機関及び裁判所の電子文書作成と送達、政令の制定権限）で規定しており、司法文書一般を電子ファイルで作成・送達することが法律上は可能である。同条等において、文書の種類や罪種により電子文書化の対象から除外し、作成や送達を紙媒体等の従来手段に限定するような規定はない[129]。よって、法制度上は令状発行手続きも電子化が可能である。しかし 2021 年時点における既往調査によると、ドイツでは令状以外の記録文書等については電子化が進んでいるものの、令状は実態として紙媒体で発付・執行されており、試験的なものも含めて、運用に至っていないと報告されている[130]。同条は令状の電子化を義務付けるものではなく、電子化の有無は検察当局の裁量による[131]。

---

127 ベルリン州刑事庁ウェブサイト https://www.berlin.de/polizei/dienststellen/landeskriminalamt/lka-7/（2023 年 2 月 22 日閲覧）

128 ベルリン警察ウェブサイト https://www.berlin.de/polizei/verschiedenes/vorgestellt/artikel.1102109.php（2023 年 2 月 22 日閲覧）

129 刑事訴訟法第 32b 条

130 刑事手続における情報通信技術の活用に関する検討会 第 9 回会議（令和 3 年 12 月 23 日）資料 33「諸外国における情報通信技術の活用に関する法制・運用の概要【暫定版・更新版】」 https://www.moj.go.jp/content/001360915.pdf（2023 年 2 月 22 日閲覧）

131 ハノーファ大教授へのヒアリング結果に基づく。

2) 海外の ISP に対する直接の情報提供要請及び回答データのオンライン受領（その際の暗号化措置の手法）

刑事訴訟の証拠として有効な情報として国外 ISP から情報を取得するには、国際刑事共助の枠組みに基づく手続きが必要である。対象が EU 域内の他国であっても同様で、当該国に対し欧州捜査命令指令（2014/41/EU）に基づく欧州捜査命令（European Investigation Order (EIO)）を発行し、当地の法執行機関から情報を送付してもらう必要がある。EIO は、EU 加盟国の法執行機関が別の加盟国の法執行機関に対し刑事訴訟の証拠の収集、証拠としての使用を目的とした捜査措置を依頼するもので、互恵を原則として、受領側の加盟国はこの要求に応じる必要がある[132]。国際刑事共助及び EIO について定めるドイツの国内法は、刑事問題における国際相互援助に関する法律[133]である。

StPO はドイツ国内を適用範囲としている。同法では 100a 条で電気通信監視、100b 条で対象者のシステム・端末内のデータ検索・取得（ドイツでは「オンライン捜索」と呼称）を捜査手法として位置づけているが[134]、これらの条項において、米クラウド法に見られるような、法執行機関に対し、自国外のデータ保全・開示に係る要請権限を明示的に賦与する規定はない。

またドイツの電気通信法（Telekommunikationsgesetz）170 条等では、ISP における StPO100a、100b 条等に基づく法執行機関による監視措置への協力、情報提供義務を定めているが[135]、同法についても適用対象として国外事業者は想定していない。

欧州及びドイツは 2022 年現在、米クラウド法に基づく行政協定を締結しておらず、米国 ISP に対しても、ドイツ法執行機関から直接、訴訟の証拠として有効な形での情報提供を要求することはできない。

コラム　国外からの取得情報の証拠能力を巡る訴訟

ドイツにおける国外からの取得情報の証拠能力に関しては、2022 年 3 月の連邦裁判所判決（5StR 457/21）[136]で取り扱われた事案が参考となる。本件では、フランスから送達された EncroChat（暗号化携帯）データのドイツでの刑事訴訟における証拠能力について争われた。

当該事案では、ドイツで麻薬密売の罪で起訴された被告が原告となり、2020 年にフランス当局が同国の司法傍受制度に基づいて取得したのち、ドイツの法執行機関に送信した EncroChat のデータについて、ドイツにおける刑事訴訟の証拠としては無効と訴えた。これに対しドイツの連邦裁判所は、当該データの証拠能力を認める判断を下し、反訴した原告の訴えを退けた。

---

132 欧州司法機構（EUROJUST）ウェブサイト https://www.eurojust.europa.eu/judicial-cooperation/instruments/european-investigation-order（2023 年 2 月 22 日閲覧）

133 刑事問題における国際相互援助に関する法律 https://www.gesetze-im-internet.de/irg/index.html（2023 年 2 月 22 日閲覧）

134 刑事訴訟法第 100a 条、100b 条

135 電気通信法第 170 条 https://www.gesetze-im-internet.de/tkg_2021/（2023 年 2 月 22 日閲覧）

136 連邦裁判所 2022 年 3 月 2 日判決（Beschluss des 5. Strafsenats vom 2.3.2022 - 5 StR 457/21 -）https://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=127966&pos=0&anz=1（2023 年 2 月 22 日閲覧）

このとき当該原告の EncroChat のデータがフランスからドイツ当局にもたらされた流れは以下のとおりである。

- フランス検察が麻薬取引に関連して、同国内サーバを介して EncroChat の暗号通信が行われている事を把握。2020 年 4 月から、フランス検察が裁判所の許可を得て、同サービスのフランス国内サーバ及び携帯電話の司法傍受実施
- その後ユーロポール経由で、多くのドイツ内ユーザが重犯罪に関わっているとの情報が BKA に提供された
- これを受け、ドイツで容疑者不明の犯罪捜査が開始され、2020 年 6 月にドイツ側からフランス当局に対し、EncroChat のデータ（ドイツに関係するデータに限定）を転送し、ドイツにおける刑事手続に使用することを認めるよう求める EIO が発出された。フランスの裁判所は 6 月 13 日にこの要求を認め、データが送られた

こうした手続きを経てフランスからドイツに送られたデータについて、同判決では刑事共助条約（MLAT）等の枠組みで国外において取得されたデータの証拠能力を認めている。また本事案は、麻薬犯罪という重罪に関わるものであり、他の手段での立証が困難なものであったことから、比例原則に照らしても手段の選択は正当であるとしている。

3) 国内事業者が保有する海外所在サーバからの情報提供要請

StPO に基づく情報取得は、ドイツ国内所在のサーバを想定しており国外所在サーバに対する直接の情報提供を想定していない。

(2) サイバー空間上の通信傍受

1) 通信傍受の根拠法令と制限

StPO 第 100a 条（電気通信監視）において、犯罪捜査手段として法執行機関が行うサイバー空間上の通信傍受及び対象罪種等が定められている。同法の規定の範疇で実施される通信監視・情報取得であれば、刑事訴訟における証拠能力を有する。監視行為、情報取得が StPO の許容する範囲を超える、あるいは同法が規定する制限に抵触すると判断される場合、当該情報は証拠能力を認められないことがある。

同条（1）では、「犯人又は共犯者として、（2）に規定する重大犯罪を実施または実施しようとしたが未遂、あるいは実施準備を行ったことを疑わせる特定の事実が存在すること」、「当該事案が事案としても重大であること」、「当該手段に拠らなければ事件の事実の捜査や被疑者の所在確認が実質的に困難、不可能であること」を条件に、対象者に知らせずに電気通信を監視（傍受）するとともに、記録することができるとしている。

また、この（1）では第 2 文において、通信監視に際し、暗号化される前の通信を取得することを目的として、対象者の使用する情報通信手段に技術的手段を用いて侵入することや、監視中の通信が暗号化されている場合に、対象者の使用する情報技術システムに保存された通信の内容やステータスを傍受・取得することも認めている。表現は抽象的であるが、これは法執行機関仕様のトロイの木馬型ソフトウェア、いわゆるポリスウェア等の技術手

段の使用容認を法的に位置づけるために、2017 年法改正で追加された規定である。

2) 犯罪者の通信機器傍受及びシステムへの技術的介入

StPO 第 100e 条（100a 条～100c 条に基づく措置の手続）により、100a 条に基づく通信監視（傍受）には、検察の要請に基づく裁判所の命令（令状）が必要である。差し迫った危険が存在する場合には、検察命令での実施も可能だが、3 営業日内に裁判所承認を得ない場合、無効となる[137]。無効となった場合、この間に取得された情報は証拠としての取り扱いができない。

上記の令状の対象者、すなわち通信監視・収集が認められる対象者は、第 100a 条（3）において、被疑者に加え、被疑者に送信されたあるいは被疑者から発信された通信を受信もしくは伝達する者、被告人がその接続・情報技術システムを使用していると推定される者に限定するとされている。すなわち、被疑者に加え、被疑者の通信対象者や、被疑者の使用する通信等手段の提供者も通信監視の対象となりうる。

対象罪種は、第 100a 条（2）において、刑法、租税法、アンチドーピング法、亡命法、在留管理法、爆発物前駆体法、外国貿易法、麻薬取締法、麻薬原料物質取締法、新型向精神物質法、国際刑事法典、武器法から指定されている。刑法犯罪としては、国家、組織犯罪、重犯罪、コンピュータ含む詐欺その他、22 の対象類型が挙げられている。

通信監視・収集が認められるのは、第 100a 条（5）1.において、リアルタイムでの通信や令状発行時点以降の通信内容、通信状況に限定されており、令状発行前の過去に遡った通信は対象に含まれていない。また、情報技術システムに加える変更（同条（1）第 2 文による技術的手段（トロイの木馬型ソフトウェア等）による侵入等）は、データ収集に不可欠な変更に限るほか、こうした変更は可能な限り、措置終了後に自動的に消去できるものとすること、投入される技術的手段及びこれによって取得、コピーされたデータは、最新技術に基づいて不正使用、削除、変更、アクセス等から保護されるようにすることが義務付けられている[138]。

3) 実施の状況

StPO100a 条に基づく通信監視や、100b 条に基づくオンライン捜索の実施状況については、連邦司法庁のウェブサイトにおいて、毎年、2 年前の統計情報が公表される。それぞれのドイツ連邦全体における実施状況は、下掲の表のとおりである。

表 10　ドイツにおける StPO100a 条に基づく通信監視状況（2020 年）

内容	件数
通信監視令状が発行された事件数	5,222 件
通信監視令状発行数	初回：14,601 件、延長：3,130 件
第 100a 条（1）第 2 文、第 3 文に基づく、対象者使用システムへの侵入件数	裁判所令状：25 件 うち実施：14 件

137 刑事訴訟法第 100e 条

138 刑事訴訟法第 100a 条

上掲のとおり、StPO100a 条に基づく通信監視が年間 1 万件以上実施されている中で、ポリスウェア等を用いた対象者システムへの侵入を伴う通信傍受は、実施が 14 件と大きく限定される[139]。

法執行機関による犯罪捜査を目的とした通信監視・情報取得に関して、StPO 第 100a 条（4）では、通信のサービスプロバイダに対し、法執行機関が措置を講じることを可能にし、遅滞なく必要な情報を提供しなければならないとしている。こうした措置については電気通信法、さらなる技術的・組織的要件は電気通信監視令に規定されている。

手法については 2019 年の連邦議会答弁により、BKA がサイレント SMS、WLAN キャッチャ、IMSI キャッチャといった手法を用いたことが確認されている[140]。

(3) そのほかの捜査手法

- サイバー事案に係る仮装身分捜査

ドイツでは、StPO 第 161 条や第 110a 条等により、仮装身分による捜査が可能である。ニーダーザクセン州警察アカデミーウェブサイトから入手できる、ハノーファ大学 Susanne Beck 教授による資料「ソーシャルネットワークにおける覆面捜査」[141]では、先行研究となる Dieter Kochheim 氏[142]の報告「インターネットにおける覆面捜査」[143]を参照しつつ、仮装身分（Legende）を用いる捜査手法とその法的根拠を、以下のように示している。

---

[139] 連邦司法庁（BfJ）「司法統計・電気通信監視 2020 年（刑事訴訟法第 100a 条に基づく措置）」（2022 年 8 月発行）
https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_TKUE_2020.pdf?__blob=publicationFile&v=6（2023 年 2 月 22 日閲覧）

[140] 連邦議会文書 Drs 19/17055（2020 年 2 月 6 日付）https://dserver.bundestag.de/btd/19/170/1917055.pdf（2023 年 2 月 22 日閲覧）

[141] ニーダーザクセン州警察学校資料（Susannne Beck 著）「ソーシャルネットワークにおける覆面捜査」
https://www.pa.polizei-nds.de/download/72621（2023 年 2 月 22 日閲覧）

[142] 元上級検察官。サイバー犯罪と刑法に関する複数の著作がある。

[143] Dieter Kochheim「インターネットにおける覆面捜査」（2012 年発行）
http://www.cyberfahnder.de/doc/Kochheim-Internet-Ermittlungen.pdf（2023 年 2 月 22 日閲覧）

表 11　仮装身分捜査の種類と法的根拠

捜査員による仮装身分を用いた活動	法的根拠
a. 単純な身分偽装（刑事であることの秘匿等）によるフェイクアカウント作成等	StPO 第 161 条（1）
b. 仮装身分によるソーシャルネットワーク等でのコミュニケーション、議論参加	同上
c. 偽のビジネスの持ちかけ、あるいは少ない接触での被疑者識別を目的とした、被疑者との短期的にコミュニケーション ※ この場合の捜査官は秘匿捜査官（NOEP）と呼ばれ、d のように偽の経歴を与えられる潜入捜査官と異なり、個々の事案で一時的に身分を偽って活動を行う	同上（容認できない挑発に抵触しないという制限あり）
d. 刑事訴訟法（StPO）110a 条の覆面（潜入）捜査における、より高度な仮装身分（ライフストーリー）の作成・付与	StPO 第 110b 条（1）
e. 重大犯罪に係るコンテンツを含むフォーラム等での長期的な議論参加	StPO 第 110a 条、 第 110b 条（1）
f. 被疑者とのより長期的なオンラインでの接触	StPO 第 110a 条、 第 110b 条（2） 第 163f 条（2）

上記表 11 のとおり、より軽微でアドホックな仮装身分捜査（a.～c.）では StPO 第 161 条が法的根拠とされる一方で、より高度・長期的な仮装身分捜査（d.～）では、第 110a 条、110b 条（110a 条に係る手続きを定める条文）が法的根拠として挙げられている。第 110a 条、110b 条では特に偽の経歴を以て長期的に活動する特殊な捜査について規定している。第 161 条は身分秘匿を問わず捜査官による通常の捜査活動について定める条文である。

以下に StPO 第 110a 条（1）、161 条（1）の条文を示す。

StPO 第 110a 条 潜入捜査官（Verdeckter Ermittler）

（1）以下に該当する重大な犯罪が行われていることを示す十分な事実がある場合、犯罪捜査を目的として潜入捜査官を派遣することができる。

1.不正な麻薬、武器取引、貨幣等の偽造関連

2.国家防護 関連

3.職業的、継続的な犯罪

4.ギャングその他組織的犯罪

また、特定の事実に基づいて犯罪が繰り返される恐れがある場合に、潜入捜査官の投入が可能である。潜入捜査官は、その投入が無ければ有益な捜査が不可能あるいは著しく困難になる場合に限って認められる。潜入捜査官は特に、犯罪の特殊性により潜入捜査が必要で、他の手段が有益で無い場合に投入可能である。第 100d 条（1）及び（2）を準用する[144]。

[144] 刑事訴訟法第 100d 条は私生活の中核領域にかかる情報の取得を規制する規定。

StPO 第 161 条 検察の捜査権限

（1）検察は、第 160 条（1）から（3）に規定する目的[145]上、他の法令規定による特段の制限が無い限り、すべての当局に情報を要求し、かつあらゆる種類の捜査を自ら実施あるいは警察当局及び警察官にその捜査を実施させる権利を有する。当局及び警察官は、検察の要請又は命令に従う義務を負い、この場合、すべての当局に情報を求める権利を有する。

StPO 第 161 条に基づくアドホックな仮装身分捜査（フェイク ID 使用等）については、法執行機関による通常の捜査活動の一環として実施されている。

一方、第 110a 条等に基づく長期にわたる覆面・潜入捜査については、サイバー犯罪捜査[146]への適用件数は限られている。連邦レベルでは、2011 年の連邦議会答弁において、BKA がソーシャルネットワーク等の仮想空間上で、第 110a 条に基づく仮装身分を付与された長期的な潜入捜査を「過去 24 か月間に 6 件」実施したと述べられている[147]。州レベルでは、バイエルン州の 2017 年議会答弁において、サイバー犯罪捜査に従事する捜査官として、第 110a 条に基づく覆面捜査官の投入はないとの回答が確認されている[148]など、覆面捜査官の投入事例はより少ない。

コラム　インターネット上の身分秘匿捜査の合法性

ドイツでは 2008 年 2 月 27 日の連邦憲法裁判所判決（BverG, Urteil vom 27.02.2008 – 1 BvR 370/07,595/07）において、インターネット上での身分秘匿捜査に係る活動について、合法・合憲であるとの司法判断が示されている。ドイツでは、具体的な事件、被害が存在しなくても、市民を含めて特定の法律の違憲性について憲法裁判所に審査を求めることが可能である（抽象的違憲立法審査）。この裁判では、2 名の市民がインターネット、IT システムへの身分秘匿、フェイク ID によるアクセスについて、人権侵害の可能性があるとして違憲の疑義を呈し、憲法裁判を提起した。連邦憲法裁判所は、国家権力側が仮装身分で対象者とコミュニケーションを取ることが、対象者の情報自己決定権といった基本的権利を侵害するとはいえず、違憲性はないと判断している[149]。

ただし仮装身分捜査において捜査官が被疑者に接触する際等に、捜査官からの持ちかけが、刑事犯罪を誘発する「容認できない挑発」と判断される場合、被疑者の人権を侵害すると見なされ、裁判の証拠として認められないケースがある。

欧州人権裁判所は、「容認できない挑発」に抵触しない行為と認められるための判断基

---

145 刑事訴訟法第 160 条では、検察による事実関係解明義務を規定している。

146 ここでのサイバー犯罪捜査は、もっぱらインターネット上等で行われる狭義のサイバー犯罪を指す。

147 連邦議会文書 Drs 17/6587（2011 年 7 月 14 日付）https://dserver.bundestag.de/btd/17/065/1706587.pdf（2023 年 2 月 22 日閲覧）

148 バイエルン州議会答弁 17/16300（2017 年 6 月 2 日付）https://www.bayern.landtag.de/www/ElanTextAblage_WP17/Drucksachen/Schriftliche%20Anfragen/17_0016300.pdf（2023 年 2 月 22 日閲覧）

149 連邦憲法裁判所 2008 年 2 月 27 日判決（BverG, Urteil vom 27.02.2008 - 1 BvR 370/07,595/07）、Rn310 https://www.bundesverfassungsgericht.de/entscheidungen/rs20080227_1bvr037007.html（2023 年 2 月 22 日閲覧）

準として、次の 3 点を挙げている。

(a) 容疑者が犯罪を実行しようとしている状況にあること

(b) 捜査官が本質的に受動的に行動していること

(c) 対象者に犯罪行為実行を強要していないこと

上記の基準はあるが、その上で個々のケースで法執行機関の行動を「容認できない挑発」とみなすかの判断は、結局のところ司法による解釈・判断による。

ドイツでは連邦裁判所が、「当初は疑わしくなく、犯罪を実施する意向でなかった人物が、公務員または公務員の指示を受けた人物によって国が仕組んだ手段で刑事犯罪を実施するよう誘導され、これが刑事犯罪につながる場合」、警察の挑発に相当し、連邦基本法第 2 条（1）（すべて人は、他人の権利を侵害せず、かつ、憲法上の秩序又は道徳律に違反しないことを条件として、自己の人格を自由に発達させる権利を有する。）に違反するとの判断を示している[150] [151] [152]。

仮装身分捜査が上掲のような原則に抵触すると判断された場合、これを通じて得られた証拠は、刑事訴訟における証拠としては認められない。

- 不正に窃取された暗号資産の奪還

StPO 第 100a 条、100b 条では法執行機関による通信傍受やサーバ、システムへの侵入を認めている。これによりアカウントの特定やウォレットの確保等が可能になる。

事例としては、連邦刑事庁（BKA）が 2021 年 5 月に、還付金詐欺グループを検挙、暗号資産を押収している[153]。2022 年にもドイツにある世界最大の違法ダークネット市場「Hydra Market」のサーバインフラストラクチャを押収して閉鎖、2,300 万ユーロ相当のビットコイン（543 ビットコイン）を確保、ビットコインミキサー（仲介ウォレット）も確保したことを公表している[154]。

上記のとおり、サーバインフラストラクチャの差押え、ウォレット確保に伴い、これに付随して確保可能な暗号資産が確保された形となる。

---

[150] 連邦裁判所 2021 年 12 月 16 日判決（BGH, Urt. v. 16.12.2021 – 1 StR 197/21）http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=125759（2023 年 2 月 22 日閲覧）

[151] 連邦裁判所 2018 年 9 月 13 日判決（BGH, 1 StR 320/17 vom 13. September 2018）http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=88441&pos=0&anz=1（2023 年 2 月 22 日閲覧）

[152] Prof. Dr. Thomas Weigend ,Kripoz 4/2022, 「国家捜査官による許容できない挑発-その前提と影響」（2022 年 3 月） https://kripoz.de/2022/03/31/unzulaessige-tatprovokation-durch-staatliche-ermittler-voraussetzungen-und-folgen/（2023 年 2 月 22 日閲覧）

[153] BKA 広報「「ジャーマン・リファンドクルー」に対する捜査 - ギャング・商用コンピュータ詐欺の容疑者 7 人の捜索」（2021 年 5 月 19 日付）https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2021/Presse2021/210519_pmRefund.html（2023 年 2 月 22 日閲覧）

[154] BKA 広報「違法ダークネットマーケットプレイス「ヒュドラマーケット」閉鎖」（2022 年 4 月 5 日付）https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html（2023 年 2 月 22 日閲覧）

2.3.3 先制的な被害防止措置及び根拠となる法制度

- 犯罪者の通信機器傍受及びシステムへの技術的介入

ドイツでは、StPO において、いわゆるポリスウェアの使用を明示的に認めている。StPO100b 条では、データ主体の同意なく、データ主体が使用する情報技術システム（サーバや端末等）に技術的手段で法執行機関が介入し、システム内にあるデータを収集する「オンライン捜索」について規定している。条件は、同条（2）に指定する重大な犯罪の疑いがあること、ケースとして深刻であること、当該手段を用いなければ捜査や容疑者の所在特定が困難であることである。同条（2）のうち、刑法に基づく対象罪種としては、15 類型が挙げられている[155]。多くが第 100a 条（通信監視）の対象罪種と重複するが、より対象が限定される。

第 100b 条のオンライン捜索においても、第 100a 条に基づく通信監視の（5）を準用し、情報技術システムに加える変更（トロイの木馬型ソフトウェア（＝ポリスウェア）による侵入等）は、データ収集に不可欠な変更に限るほか、こうした変更は可能な限り、措置終了後に自動的に消去できるものとすること、投入される技術的手段及びこれによって取得、コピーされたデータは、最新技術に基づいて不正使用、削除、変更、アクセス等から保護されるようにすることが義務付けられている。ポリスウェアを用いて取得収集されたデータを警察の運用する代替サーバに転送する活動等も、同条の範疇で理解される。

こうした手段は、暗号化された通信に対する法執行機関の監視介入を目的としており、2017 年の StPO 改正において、法執行機関が採りうる手段として明示的に盛り込まれた。

2017 年改正時の連邦議会文書では、当該改正について、被疑者のコンピュータや携帯電話を被疑者に気づかれることなくスパイすることができるプログラム、「いわゆる国家トロイの木馬（Staatstorojaner）」（＝ポリスウェア）の使用を許容するものと説明している。

より具体的には、この改正により、従前は通信監視の一種として司法解釈の範疇で、限定的な範囲内で実施されていた 2 つの手法が、StPO に基づき可能な捜査手法として明示的に盛り込まれた。

その第 1 が、「ソース TKÜ[156]」という捜査手法である。通常の TKÜ では、電話やその他通信手段の通信経路の切り替えによって通信を傍受するが、通信が暗号化された場合、制約が生じうる。ソース TKÜ は、暗号化される前のデータにインターセプトするものであり、この問題を回避することができると説明されている。

加えて第 2 の手法として、「オンライン捜索」が挙げられる。これは疑わしいデータを特定、取得するため、対象者の使用する電子機器に遠隔で侵入し、そのシステム全体を検索することを可能にするものであり、その適用にはより厳格な条件が課される。

連邦議会文書では、これら第 1、第 2 の手段は共に、スパイプログラム、いわゆるトロイの木馬を密かに対象デバイスにインストールする必要があり、国家権力により実施されることから、国家トロイの木馬（Staatstorojaner）と呼称されると説明されている。

また、議会公聴会の議論の中で、BKA の当時の副長官はこれらソフトウェアについて、市販のものをそのまま投入するのではなく、捜査用に裁判所命令で認められる範囲に合わ

155 刑事訴訟法第 100b 条

156 ドイツでは通信監視、すなわち傍受を Telekommunikationsüberwachung（TKÜ）と呼ぶ。

せて専用に設定（カスタマイズ）されたものが用いられると述べている[157]。

なお、ドイツ政府報告書によると、Emotet のテイクダウンにおいて、BKA が Emotet の修正バイナリを配布して通信パラメータを修正し、これらのシステムを犯人のコントロールサーバでなく、BKA が運用する一連の sinkhole サーバに接続するよう仕向けたとあり、BKA による代替サーバの運用事例が確認される[158]。誘導は BKA による修正バイナリ配布の結果であり、StPO 第 100b 条でカバーされる。

なお、国家トロイの木馬の投入を前提としたソース TKÜ やオンライン捜査が StPO 第 100a 条、100b 条において、捜査に利用可能な手段として法律に明示されたのは、2017 年法改正以降であるが、それ以前から、これらの手段は実態として、一部で運用されていた。連邦裁判所は 2008 年に、当時の StPO 規定の下では、国家トロイの木馬の使用について、ソース TKÜ を目的とした使用は一部認められる一方で、被疑者等端末の全体検索を行うオンライン捜索目的での使用は認められないこと、また国家トロイの木馬の使用が裁判所令状に基づき限られた条件下のみで可能であるとの判断を示していた[159]。現在は、上述の 2017 年の StPO 改正により、オンライン捜索を目的とした国家トロイの木馬の使用は法的に正当である。

StPO 第 100b 条に基づくオンライン捜索の実施状況については、連邦司法庁のウェブサイトにおいて、毎年、2 年前の統計情報が公表される。ドイツ連邦全体における実施状況は、下掲の表のとおりである。

表 12　ドイツにおける StPO 第 100b 条に基づくオンライン捜索状況（2020 年）

内容	件数
オンライン捜索令状が発行された事件数	10 件
オンライン捜索令状発行数	初回：12 件、延長：11 件
第 100b 条（1）に基づく、対象者使用システムへの介入件数	実施：8 件

対象者システムに侵入、検索してデータ収集を行う第 100b 条のオンライン捜索は、第 100a 条に基づく一般的な通信監視と比較して大きく件数が限定されている（2.3.2(2)参照）[160]。

---

157 連邦議会ドキュメントアーカイブ 2017 年「刑法改革に係る公聴会における国家トロイの木馬に関する賛否」https://www.bundestag.de/dokumente/textarchiv/2017/kw22-pa-recht-strafrecht-508168（2023 年 2 月 22 日閲覧）

158 連邦情報技術安全庁「ドイツにおける 2021 年 IT セキュリティ状況」（2021 年）https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2021.pdf?__blob=publicationFile&v=5（2023 年 2 月 22 日閲覧）

159 Deutche Welle 放送「国家トロイの木馬：国家のハッキングツール」（2016 年 2 月 22 日付）https://www.dw.com/de/der-bundestrojaner-das-hacking-tool-des-staates/a-19065654（2023 年 2 月 22 日閲覧）

160 連邦司法庁（BfJ）「司法統計 電気通信監視 2020 年（刑事訴訟法 100b 条に基づく措置）」（2022 年 3 月発行）https://www.bundesjustizamt.de/SharedDocs/Downloads/DE/Justizstatistiken/Uebersicht_Online_Durchsuchung_2020.pdf?__blob=publicationFile（2023 年 2 月 22 日閲覧）

コラム　ドイツにおける「国家トロイの木馬（Staatstorojaner）」等利用事例

オンライン捜索の実施事例については、国際捜査として行われた EnchroChat の捜査において、ユーロポールから BKA に転送されたドイツの犯罪者の情報（デバイス番号、メールアドレス、チャットメッセージ等）をもとに、StPO 第 100b 条に基づくオンライン捜索を適用したことが確認されている。この事件で逮捕されたドイツの麻薬密売人は、国際捜査における転送データに基づくオンライン捜索による証拠の有効性を巡って、ハンブルク地方裁に訴えを起こした。しかし同裁は、情報の転送は、EU の法執行機関間の情報交換に関する枠組み決定等に基づき正当に行われており、また StPO 第 100b 条に基づくオンライン捜索による証拠取得に関しても、麻薬、組織犯罪といった同手法の適用対象罪種に合致していることなどから、訴えを退けた[161]。

実際に投入された国家トロイの木馬に関しては、2019 年に、インターネット上のサイバー関連情報サイトの運営者が BKA に対し、国家トロイの木馬の提供企業との契約変更（更新）に関して情報公開請求をかけており、ヴィースバーデン行政裁判所が 2022 年 5 月 6 日に、情報開示命令を発出している。公開された文書に拠れば、BKA は 2013 年に初めて Elaman/Gamma 社の FinFisher ソフトウェアを調達している[162]。同ソフトウェアはさまざまな OS のコンピュータ、モバイル端末に、偽のアップデート等を介して侵入し、BKA にデータを転送するものとされている。

2.3.4 民間事業者の義務及び根拠となる法制度

(1) 通信履歴（ログ）の保存義務

ドイツでは電気通信法第 176 条（通信記録の保存義務）により、ISP や携帯電話等含む通信事業者に対し、過去 10 週間分の通信記録をドイツ国内で保存することを義務付けている。なお、同条では事業者に対し、これらの記録を上記期間終了後、1 週間以内に削除することも義務付けており、意図的に削除しない場合は罰金対象となる。

保存される通信記録は、インターネット通信の場合、エンドユーザに割り振られた IP アドレス、インターネット接続時の一意の識別子、及び割り当てられたユーザ ID、割り当てられた IP アドレスによるインターネット使用開始日時と終了日時とされている。また、法執行機関含む、情報要求権限を持つ当局からの要請があった場合に速やかに情報を提供できるようにしておくことも義務付けられている[163]。

---

161 ハンブルク上級裁判所 2021 年 1 月 29 日判決（Hamburg - 1 Ws 2/21 1 Ws 2/21 - 7 OBL 3/21）https://www.landesrecht-hamburg.de/bsha/document/JURE210003021（2023 年 2 月 22 日閲覧）

162 情報公開請求ポータルウェブサイト「ヴィースバーデン行政裁 2022 年 5 月 6 日決定 6 K 924/21.WI 06.05.2022」 https://fragdenstaat.de/anfrage/anderungen-zum-vertrag-mit-elamangamma-uber-staatstrojaner/#nachricht-721632（2023 年 2 月 22 日閲覧）

163 電気通信法 176 条

(2) 捜査への協力義務

StPO 第 100j 条では、オンラインストレージや携帯端末等のデータの復号化に必要なパスワード等の提供を事業者に義務付けている[164]。対象罪種は、第 100b 条に指定される各種重大犯罪である。パスワードの提供については、電気通信電子メディアデータ保護法 23 条にも規定されている[165]。

しかし、事業者に暗号化解除や機器修復を義務付ける規定はない。

また StPO 及び電気通信法では、通信傍受等について、法執行機関の技術的手段の受け入れを義務付けているが、「バックドア等の保全」に関する規定はない。なお、前述のとおり、捜査機関の行動は、犯罪行為の誘発につながらないことが求められる。

ISP 等の捜査協力については、電気通信法第 170 条等において、通信傍受準備の義務付、令状に係る事業者責任者の届出（連邦ネットワーク庁への）ほか、協力義務が定められている。

罪種については StPO における通信監視（傍受）規定（StPO 第 100a 条、100b 条等）が対応する。

(3) サイバー事案発生時の公的機関等への報告義務

また、サイバー事案発生時の公的機関等への報告義務については、電気通信法 168 条において、ネットワークの運用又はサービスの提供に重大な影響を及ぼすセキュリティインシデントの通知義務が定められている。通知先の当局は連邦ネットワーク庁及び連邦情報安全局である。電気通信法上の措置であり、通知のクライテリアは同条に定める影響範囲等により判断される。

(4) 情報開示に関する利用者等への通知義務

情報開示に関する利用者等への通知義務について、StPO 第 100a 条～100f 条、100h 条、100i 条、及び 110a 条に基づく仮装身分捜査（覆面捜査）等においては、対象者の同意なく事業者等からの情報取得、対象者システム、携帯電話への侵入、傍受等が行われる。第 100j 条に基づく通信事業者等への接続・登録情報取得についても、対象者の同意は伴わない。ただし、第 100j 条の単純な登録者情報等一部を除いて、第 101 条等に基づき、これらの措置の実施については、捜査の目的や人命、財産、自由を脅かさない限りにおいて、対象者に速やかに通知することが原則として定められている。しかし、当該措置の影響が軽微で対象者の利害に関わらないと見なされる場合や、対象者による通知のメリットがデメリットを上回る場合（データ主体や第三者保護、捜査の観点等）等は省略や延期（延期期間は 12 か月。司法承認で更なる延期も可能）が可能である。

同意なき情報取得、介入の条件（罪種等）については、それぞれの捜査活動を規制する各条に規定されている。

---

[164] 刑事訴訟法第 100j 条

[165] 電気通信電子メディアデータ保護法 23 条 https://www.gesetze-im-internet.de/ttdsg/__23.html（2023 年 2 月 22 日閲覧）

2.3.5 サイバー捜査における人権確保に関する係争事例

StPO100b 条において捜査手法として認められているオンライン捜索だが、各州の警察における捜査では各州法令の規定に基づき運用が行われている。

「公安・秩序に関するヘッセン州法第 25a 条」及び「警察によるデータ処理に関するハンブルク州法第 49 条」は、いずれも各州警察が自動化されたアプリケーションを用いて、いわゆるビッグデータの評価を行うことを可能にしている。

ドイツでは 2022 年に、両州の上掲条項における人権保護が不十分であり、こうしたデータ評価の実施により人権侵害が発生する恐れがあるとして、違憲立法を訴える訴訟が提起され[166]、2023 年 2 月現在係争中である。

連邦憲法裁判所で審理が行われている本件であるが、本件に係る 2022 年 12 月 20 日の口頭審問に関する同裁判所のプレスリリース、また本件について報じる公共放送の報道によると、こうしたアプリケーションの使用により、捜査を担当する州警察当局は、州内の別の警察の持つデータも含めて、州内で発生した過去の事件に関連して収集・保存したデータを自動で横断検索、利用する。ドイツ国内 16 州の州警察のうち、2022 年末時点でこうしたソフトウェアを実際に運用しているのはヘッセン州とノルトライン・ヴェストファーレン州のみである。ヘッセン州で使用されているソフトウェアは「ヘッセンデータ」と呼ばれ、州警察の約 2,000 人の捜査官が使用している。なお同ソフトウェアは、米国 Palantir 社の製品を、ヘッセン州警察用にカスタマイズしたものである。ハンブルク州については、現時点で同様のソフトウェア運用は行われていないが、法的には可能である。

原告の弁護士らは、「公安・秩序に関するヘッセン州法第 25a 条」及び「警察によるデータ処理に関するハンブルク州法第 49 条」は、暗殺やテロの疑いといった重大犯罪以外でも、ソフトウェアを用いたデータ分析が可能な規定となっている点を懸念点として挙げている。また、この訴訟では、警察による人工知能（AI）、自己学習アルゴリズムの利用についても議論されている。原告の一人である弁護士は、AI 等による自動評価が広範に行われる場合、法廷弁護士として多くの容疑者と連絡をとる機会が多い自らが、自動的に監視の対象となる恐れがあるとし、権利侵害のリスクを訴えている。この裁判においてヘッセン州警察当局は、自主的な組織内規範として、ヘッセンデータの適用を、テロ、児童ポルノ、深刻な組織犯罪に限定していると主張した。また、ヘッセン州はこの裁判の審理において、米国 Palantir 社製品は AI 機能に対応しているが、ヘッセン州警察向けにカスタマイズされた「ヘッセンデータ」では AI 機能を外しており、実装していないと述べている。このように自主的な制限・規制はあるものの、法的・技術的には AI によるアルゴリズムの利用は可能な状態である。これに対し憲法裁判所判事は、ヘッセン州によるこうしたソフトウェアの運用、自己規制に理解を示しつつも、自己規制ではなく明確な制限、利用可能範囲を法令において明文化することが望ましいとの見解を示している。

裁判の判決はまだ出ていないが、ドイツ国内ではバイエルン州も同様のソフトウェア導入を検討している。ヘッセン州は米国 Palantir 社と、枠組み契約を締結しており、他の州で同じシステムを導入する場合、これに則って調達を進めることができる。よって、現在進められているヘッセン州（とハンブルク州）の州法を巡る憲法裁判は、今後の各州における同

[166] ドイツでは、具体の事件がなくとも、誰でも人権侵害の恐れがあると考えられる法令規定について、憲法裁判所の審査を求める事ができる（抽象的違憲立法審査）。

様のシステム導入における範囲と条件、その法律上の明文化について規範的な司法判断を示すものとなることが期待される[167] [168]。

[167] 連邦憲法裁判所広報「ヘッセン州及びハンブルク州における自動データ評価に関する口頭審問」（2022 年 11 月 11 日付）
https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/DE/2022/bvg22-090.html（2023 年 2 月 22 日閲覧）

[168] ARD 放送 Tagesschau 番組ウェブサイト放送記事「警察はどのような時にビッグデータを利用できるのか？」（2022 年 12 月 20 日付）https://www.tagesschau.de/inland/innenpolitik/polizei-ermittlungen-datenbanken-101.html（2023 年 2 月 22 日閲覧）

2.4 フランス

2.4.1 サイバー空間の脅威に対処するための体制

(1) サイバー事案の捜査・対策を担う公的機関等の体制・業務分担

フランスでは、刑事訴訟法典に基づき、国家憲兵隊と国家警察の 2 組織が司法警察権を持つ。国家警察が主に 2 万人以上の都市部を所管するのに対し、国家憲兵隊はその他地方部を所管することが多い。国家憲兵隊は司法警察機能に加え施設防衛その他、軍としての性質も帯びるため、内務省と軍事省の共管となっている。国家警察は内務省の所管である。

＜国家憲兵隊＞

国家憲兵隊では、従来、中央刑事情報局の下の「デジタル犯罪対策センター（Centre de lutte contre les criminalités numériques（通称：C3N）」（将校 12 名、下士官 44 名の計 56 名：2020 年）が、サイバー犯罪捜査の実施や全国の国家憲兵隊におけるサイバー犯罪捜査の統括、調整、支援に中心的な役割を果たしてきた。また、国家憲兵隊フォレンジック研究所（Institut de recherche criminelle de la gendarmerie nationale (IRCGN)）内にもデジタルフォレンジックを担う工学・デジタルフォレンジック部門等があり、複数部門でサイバー犯罪に関連する業務を行ってきた。近年のサイバー犯罪事案の増加、重要性の増大を反映し、国家憲兵隊では、2021 年に新たに国家憲兵隊総局（Direction générale de la Gendarmerie Nationale：DGGN）直轄の指令部として、「憲兵隊サイバー指令部（Commandement de la gendarmerie dans le cyberespace（通称：ComcyberGend）」を設置した。同指令部は、サイバー問題に係る国家憲兵隊のワンストップ窓口として機能し、C3N 及び C3N 傘下の各種のサイバー警察機能、IRCGN 内のサイバー技術機能等、以前からある複数のサイバー関連の各署の統括・指示調整を担う[169]。

同指令部の組織図を図 5 に示す[170]。

[169] 国家憲兵隊情報広報「COMCyberGEND：サイバー脅威に対し憲兵隊が能力強化」（2021 年 8 月 4 日付）https://www.gendinfo.fr/actualites/2021/comcybergend-la-gendarmerie-monte-en-puissance-face-a-la-menace-cyber（2023 年 2 月 22 日閲覧）

[170] 国家憲兵隊提供資料（ヒアリング資料）「THE GENDARMERIE FACING CYBER THREATS PRESENTATION OF THE COMCYBERGEND」に基づく。

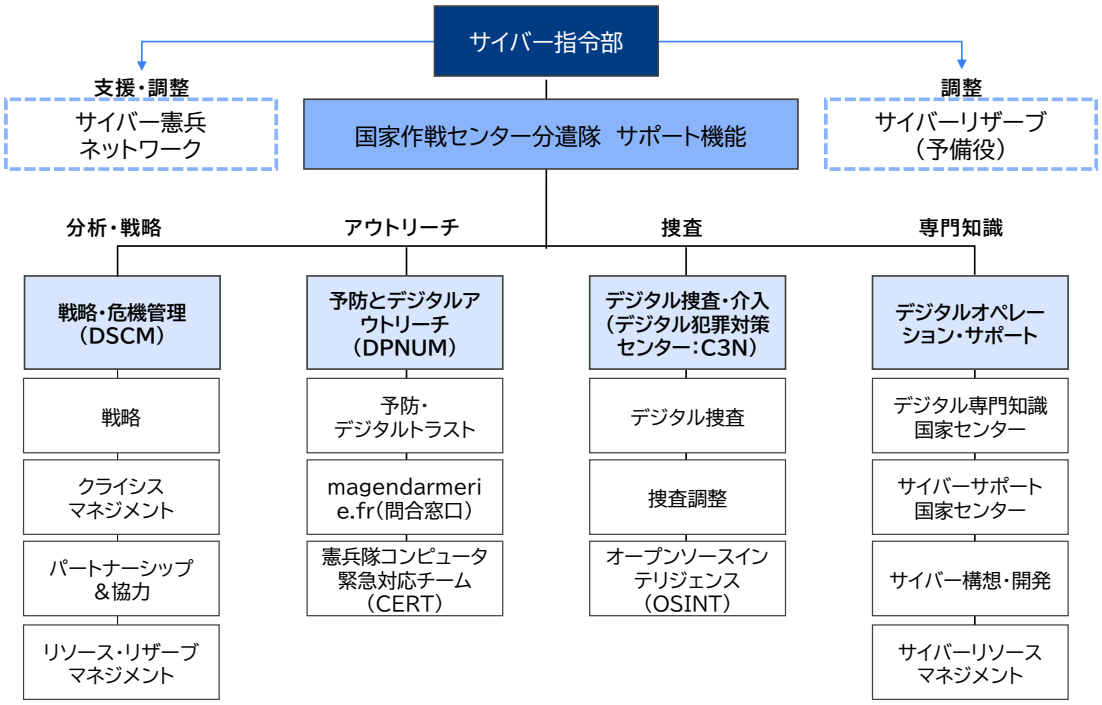

図 5　ComcyberGend 組織図

（出所）国家憲兵隊資料に基づきエム・アール・アイ　リサーチアソシエイツ株式会社作成

各部署の概要は以下のとおりである[171]。

表 13　ComcyberGend の部署概要

部署名	任務概要
戦略・危機管理	サイバー憲兵のネットワーク調整、憲兵隊のサイバーポリシー策定、機関間協力・国際協力、サイバーリスクや重要インシデントマネジメント
予防とデジタルアウトリーチ	デジタル空間における窓口機能として、サイバー脅威に対する予防・保護活動を実施。国民、経済界、自治体等にサイバーセキュリティカルチャーを普及させる。ComcyberGend のデジタルアウトリーチ部門であり、デジタル旅団を擁する。この旅団には magendarmerie.fr から 24 時間 365 日アクセス可能。同旅団が問合せ者の質問に答え、適切なサービスにつなぐ。また、サイバー脅威の分析・グループ化を行うセンターの機能も有し、脅威の予測を目的とした監視と分析を実施。デジタル脅威への「反応」だけでなく、「先読み」も担う。
デジタル捜査・介入（デジタル犯罪対策センター：C3N）	デジタル空間における司法調査及び行動監視を実施。サイバー犯罪捜査を担当する上級捜査官で構成される。暗号資産、ウェブ上の違法取引、オンライン小児性愛者犯罪、自動データ処理

[171] 国家憲兵隊へのヒアリング結果に基づく。

部署名	任務概要
	システムに対する攻撃等の分野を取り扱う。
デジタルオペレーション・サポート	デジタル証拠の処理、捜査官の支援、IT ツールの開発等を行う。ComcyberGend の技術部門として、優秀なデジタル専門家を擁する。スマートフォン、サーバ、ハードディスク、車載マルチメディアシステム、正規または悪意のあるソフトウェアのリバースエンジニアリング等、あらゆる種類のデジタルシールを活用して、確実に証拠を収集・処理する。同部門の一部が、「サイバーキャンパス」（後述）に移転済み。

国家憲兵隊全体では、フランス全土に 8,500 人のサイバー憲兵ネットワークを構築し、各地のデジタルセキュリティを確保。このうち 1,600 人はデジタル捜査や暗号資産監視等を行う資格を有する[172]。

＜国家警察＞

国家警察においては、司法警察中央局の下のサイバー犯罪対策準局（Sous-direction de lutte contre la cybercriminalité (SDLC)）がサイバー犯罪捜査を主管する。以下の図のとおり、SDLC 内には、情報・通信技術関連犯罪対策中央事務局（Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC)）が置かれ、国家警察の警察官の他、国家憲兵隊の憲兵、行政官、エンジニア等合わせて 2021 年時点で、約 150 名が活動している[173] [174]。

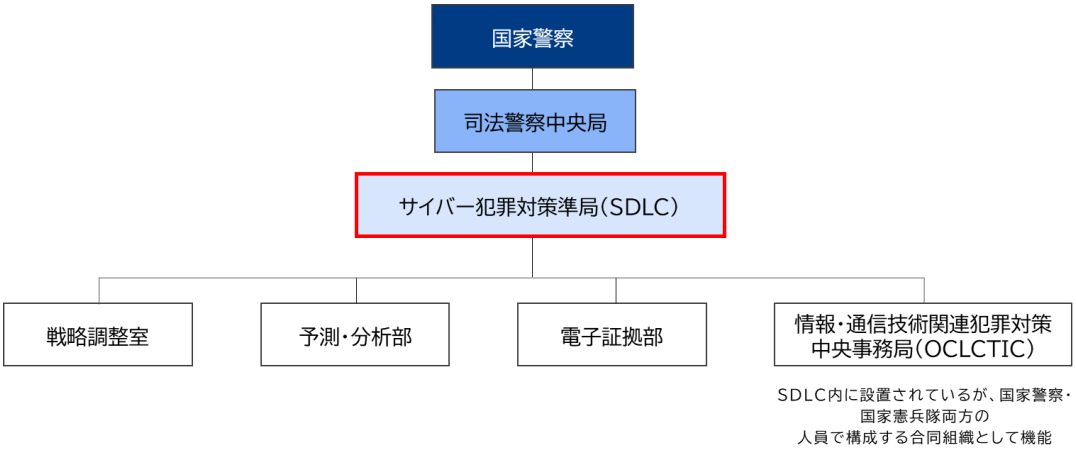

図 6　国家警察 SDLC 組織図

（出所）国家警察ウェブサイトよりエム・アール・アイ　リサーチアソシエイツ株式会社作成

[172] 国家憲兵隊へのヒアリング結果に基づく。

[173] 国家警察 SLDC ウェブサイト https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite（2023 年 2 月 22 日閲覧）

[174] 国家警察 SDLC 資料（2022 年 4 月発行）https://www.police-nationale.interieur.gouv.fr/content/download/131878/1047654/file/Triptyque_SDLC.pdf（2023 年 2 月 22 日閲覧）

＜広域犯罪における担当分担＞

前述のとおり、フランスには国家憲兵隊、国家警察と 2 つの刑事警察があるが、広域での犯罪（国家憲兵隊の管轄区域と国家警察の管轄区域の両方にまたがる犯罪）の場合に、どちらが担当あるいはリードするかは、さまざまな要素を勘案して、検察が決定する。捜査においては国家警察と国家憲兵隊は協力して情報収集等を行う。

(2) サイバーセキュリティに関する総合調整を担う公的機関等の体制

フランスでは、首相直属の国家情報システム安全保障庁が、国家のサイバー・情報セキュリティを統括する。

その他関係する各官署と役割の概要は、以下のとおりである[175]。

表 14 フランス国家サイバーセキュリティの関係官署

組織名	役割
国家情報システム安全保障庁	首相府直属。国家情報セキュリティの中央機関として政府のサイバー犯罪・防衛・諜報関連情報の集約調整、法整備民間への助言、セキュリティの重要インフラ改善、教育、啓蒙等を担当。
国家警察	内務省傘下。情報・通信技術関連犯罪対策中央事務局（OCLCTIC）がサイバー犯罪の国家コンタクトポイントの役割を担う。OCLCTIC には、国家憲兵隊のスタッフも常駐。ハッキング、不法コンテンツ、オンライン詐欺等捜査を実行。サイバー捜査技術の開発、教育等も担う。
軍事省	サイバー指令部が軍部内のサイバー防衛関連情報、活動を統括・調整。軍部としての防衛的・攻撃的サイバー活動を実施。対外治安総局が対外サイバー諜報を担当、国防情報総局がサイバースペース監視、対抗的スパイ活動、情報、対人、対物、対インフラ防護担当。軍事偵察局も関与。
国内治安総局	内務省傘下で防諜を担う。重要インフラ、政府インフラへのサイバー攻撃対応。

(3) デジタルフォレンジック体制

2.4.1(1)で言及したとおり、国家憲兵隊では国家憲兵隊フォレンジック研究所（IRCGN）内に、デジタルフォレンジックを担う工学・デジタルフォレンジック部門（Division Criminalistique Ingénierie et Numérique (DCIN)）が設置され、治安判事等の要請のもと、パスワード保護、暗号化されたデータへのアクセスを含むフォレンジック業務を実施している。

[175] スイス連邦工科大学 Center for Security Studies (CSS) 報告書「National Cybersecurity Strategies in Comparison – Challenges for Switzerland」（2019 年 3 月 18 日発行） https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/363696/Cyber-Reports-2019-08-NationalCybersecurityStrategiesinComparison.pdf?sequence=1&isAllowed=y（2023 年 2 月 22 日閲覧）

特にデジタルフォレンジックに関しては、DCIN 内のコンピュータサイエンスエレクトロニクス部門（Département Informatique-Electronique（通称：INL））が中心的役割を果たしている。同部門は 1992 年に設置され、「データ抽出」「情報処理」「ネットワークと電気通信」「運用支援」の 4 部署で構成される[176] [177]。

こうした DCIN 等におけるデジタルフォレンジック含め、上掲の ComcyberGend のデジタルオペレーション・サポートが、国家憲兵隊におけるデジタルフォレンジック機能の統括調整を担う。

もう一つの司法警察組織である国家警察においては、（1）で言及したサイバー犯罪対策準局（SDLC）のもとに電子証拠部が設置されており、デジタルフォレンジックを担当する。同部では、デジタル調査グループが、モバイル機器含むハードウェアのフォレンジックを担うほか、暗号資産フロー捜査を専門とする特別技術グループ等がある[178]。

なお、フランスでは 2022 年 2 月に、政府が「サイバーキャンパス」を創設した[179]。国家憲兵隊の ComcyberGend のデジタルオペレーション・サポート部門の一部も、同キャンパス内に移転している[180]。同キャンパスには 13 階建てのビルに、サイバー犯罪フォレンジックに係る政府機関、研究機関、民間企業等、サイバー犯罪対応リソースが順次集約される見込みである。

2.4.2 効率的・効果的な捜査手法及び根拠となる法制度

(1) 遠隔地のサーバ等に所在する証拠の収集

1) ISP に対する捜索差押え令状等のオンライン送達

刑事訴訟法典 801-1 条（訴訟関係書類のデジタル形式での作成等）に基づき、デジタル形式による令状作成、発付が可能である。デジタル形式のままでの映像画面での提示、交付も可能であり、実際に運用されている[181]。罪種の特定等の制限は無い。

---

[176] 国家憲兵隊ウェブサイト https://www.gendarmerie.interieur.gouv.fr/pjgn/ircgn/division-criminalistique-ingenierie-et-numerique-dcin（2023 年 2 月 22 日閲覧）

[177] 国家憲兵隊ウェブサイト https://www.gendarmerie.interieur.gouv.fr/pjgn/ircgn/division-criminalistique-ingenierie-et-numerique-dcin/departement-informatique-electronique-inl（2023 年 2 月 22 日閲覧）

[178] 国家警察 SLDC ウェブサイト https://www.police-nationale.interieur.gouv.fr/Organisation/Direction-Centrale-de-la-Police-Judiciaire/Lutte-contre-la-criminalite-organisee/Sous-direction-de-lutte-contre-la-cybercriminalite（2023 年 2 月 22 日閲覧）

[179] 国家憲兵隊情報ウェブサイト https://www.gendarmerie.interieur.gouv.fr/gendinfo/actualites/2022/inauguration-du-campus-cyber-a-la-defense（2023 年 2 月 22 日閲覧）

[180] 国家憲兵隊へのヒアリング結果に基づく。

[181]刑事手続における情報通信技術の活用に関する検討会 第 9 回会議（令和 3 年 12 月 23 日）資料 33「諸外国における情報通信技術の活用に関する法制・運用の概要【暫定版・更新版】」https://www.moj.go.jp/content/001360915.pdf（2023 年 2 月 22 日閲覧）

2) 海外の ISP に対する直接の情報提供要請及び回答データのオンライン受領（その際の暗号化措置の手法）

刑事訴訟の証拠として有効な情報として国外 ISP から情報を取得するには、刑事共助条約（MLAT）の枠組みに基づく手続きが必要である。対象が EU 域内の他国の場合は、当該国に対し欧州捜査命令指令（2014/41/EU）に基づく欧州捜査命令（European Investigation Order (EIO)）を発行し、当地の法執行機関から情報を送付してもらう必要がある。EIO は、EU 加盟国の法執行機関が別の加盟国の法執行機関に対し刑事訴訟の証拠の収集、証拠としての使用を目的とした捜査措置を依頼するもので、互恵を原則として受領側の加盟国はこの要求に応じる必要がある[182]。国際刑事共助については刑事訴訟法典第 694～694-13 条、EIO については、刑事訴訟法典第 694-14～695-9-57 条に規定されている。

欧州及びフランスは 2022 年時点で、米クラウド法に基づく行政協定を締結しておらず、米国 ISP に対しても、フランス法執行機関から直接、訴訟の証拠として有効な形での情報提供を要求することはできない。

3) 国内事業者が保有する海外所在サーバからの情報提供要請

国家憲兵隊に対するヒアリングによると、フランス法人が持つフランス関連のデータであれば、要求が可能である[183]。

(2) サイバー空間上の通信傍受

フランスでは刑事訴訟法典第 100 条～100-8 条に基づき、懲役刑対象となる犯罪に関連して、電気通信に対する司法傍受が可能である。組織犯罪等指定犯罪の予備捜査上必要な場合、検察の要請に基づく勾留決定判事命令により、検察官あるいは検察官の指示を受けた司法警察が同判事の監督下で実施される（1 回 1 か月以内。延長は 1 回 1 か月のみ可能）。また予審手続では予審判事命令の下で同判事の監督下で実施される（1 回 4 か月以内。延長可能）（刑事訴訟法典第 100～100-8 条、706-95～706-95-3 条）。

古い情報であるが、2017 年 11 月段階で、継続中の司法傍受が約 8,500 件、傍受した通話が約 60 万件/週、傍受した SMS が約 90 万件/週、データ入手照会が約 200 万件/年と相当量の司法傍受が実施されている[184]。国家憲兵隊に対するヒアリングにおいても、具体の件数への言及はなかったが、「相当に広範な司法傍受が可能」とのことであった。

フランスでは、司法傍受のワンストップ窓口として設置された「国家司法傍受プラットフォーム」（刑事訴訟法典第 230-45 条）を通じて、情報の要請送信、取得、取得した情報の管理が行われている。刑事訴訟法典第 100-3 条では、法執行機関が電子通信事業者（の責任者）に対し、傍受に必要な装置の設置を要求できるとしている。

国外に関しては、刑事訴訟法典第 100-8 条において、EU 域内で使用される通信アドレス

---

182 欧州司法機構（EUROJUST）ウェブサイト https://www.eurojust.europa.eu/judicial-cooperation/instruments/european-investigation-order（2023 年 2 月 22 日閲覧）

183 国家憲兵隊へのヒアリング結果に基づく。

184 司法省広報「国家司法傍受プラットフォーム」（2017 年 11 月 3 日付）http://www.presse.justice.gouv.fr/communiques-de-presse-10095/archives-des-communiques-de-2017-12858/la-plateforme-nationale-des-interceptions-judiciaires-en-chiffres-30997.html（2023 年 2 月 22 日閲覧）

であって、かつ EIO を伴わないものである場合、法執行機関は傍受対象者がいる加盟国の当局に傍受の実施を通知することが定められている。相手 EU 加盟国がフランス側からの通知を受領後 96 時間以内に、その傍受が当該国の国内法で認められないものであることを通知してきた場合、取得した傍受データは無効となるとされている。

(3) そのほかの捜査手法

- サイバー事案に係る仮装身分捜査

フランスにおいては、刑事訴訟法典第 230-46 条に基づき、フェイク ID 含む仮装身分を用いた、サイバー空間上での捜査、証拠収集が可能である。2020 年公開のフランス上院報告書によると、2019 年 3 月 23 日の法改正により、偽名等を用いた捜査に関する刑事訴訟法典上の規定が第 230-46 条に整理集約された。

オンライン上での偽名による捜査活動の適用範囲は、当初は性犯罪や人身犯罪等に限定されていたが、順次対象が拡大され、現行の刑事訴訟法典第 230-46 条では、電子通信媒体を通じて実施された、懲役刑の対象となりうるあらゆる犯罪が適用対象に含まれている。仮装身分での捜査権限を与えられた捜査員は、特に以下のことを実施可能である。

- ✓ 仮装身分での電子取引参加
- ✓ 犯罪容疑者に関する証拠やデータの抽出、取得、保持
- ✓ 明示的な要求に応じて、違法なコンテンツを抽出、送受信、保持（一部犯罪に限る）

制限事項に関して、不正なものを含むコンテンツや製品、材料、サービス等の取得に際しては、判事の許可が必要となるなど、規制が強化される。また、偽名による捜査行為は、他人に犯罪を扇動するものであってはならず、扇動と判断された場合、そうした行為（取得した証拠）は無効となる[185] [186]。

なお、上記のとおり犯罪を扇動する捜査行為は認められず、犯人の意図に拠らない犯罪行為は訴追できない。こうしたことから、犯罪者のものであることが判明しているオンラインアカウント（メールアカウントや SNS アカウント等）を窃取（乗っ取り）し、当該人物になりすます捜査手法について、国家憲兵隊に対するヒアリングでは現実的ではないとの回答を得た。

- 不正に窃取された暗号資産の奪還

暗号資産回収については、刑法典第 131-21 条、刑事訴訟法典第 706-153 条に基づき犯罪収益、犯罪資産の差押えで対応する。上掲条文に基づき、動産・不動産に加え無形資産も差押えの対象となる。暗号資産の奪還の手法は、暗号通貨がどのように盗まれたかにより異なるが、技術的には、暗号資産の差押え、奪還といった対応は、暗号資産を保持するプラットフォームの差押え、または対象者が自分の秘密鍵を捜査官に伝える場合に実行可能となる。ただし、実際には犯罪者が秘密鍵を捜査官に容易に教えないケースも多く、家宅捜索で端末

[185] 仏上院（元老院）報告書「サイバー犯罪上院報告書 情報番号 613 号（2019-2020）2020 年 7 月 9 日」（2020 年 7 月発行）https://www.senat.fr/rap/r19-613/r19-613_mono.html（2023 年 2 月 22 日閲覧）

[186] 刑事訴訟法典第 230-46 条 https://www.legifrance.gouv.fr/codes/id/LEGITEXT000006071154/（2023 年 2 月 22 日閲覧）

やメモその他の解析・分析から探すこともある。

暗号資産含め、フランスにおける法執行に係る差押え・押収資産の管理、処分（没収、被害者への返還等）は、押収資産管理庁に集約されている。暗号資産の場合、同庁で専用のウォレットを保有している。以前は同庁で単一のウォレットを保持していたが、現在は捜査事案ごとに個別のウォレットで管理している[187]。

コラム　不正に窃取された暗号資産の押収

ダークネット上での暗号資産、仮想通貨アカウントの追跡については、国家憲兵隊ウェブサイトにおいて事例が紹介されている。ダークネットでの取引に利用されるビットコインはクリアウェブでも使用される完全公開型の仮想通貨で、本来誰でもアクセスできるものである。しかし、「ミキサー」と呼ばれる仲介ウォレットが存在し、これがナビゲーションを匿名化するノードと同じ原理で、買い手と売り手の間のやり取りの痕跡を隠すことを可能にする。これにより、支払元や取引量を特定することが困難になる。捜査ではビットコインウォレットを特定することにより、犯罪資産として仮想通貨の差押えを行うことが可能となると説明されている。フランスでは 2016 年初め、西部地域で行われていた大麻密売に関する捜査（サイバー捜査ではない従来型捜査）の過程で、地元の捜査官が捜索中にコンピューターサーバとビットコインの情報を発見、サイバー捜査を担う C3N が、ウォレットを特定し、ビットコインを押収したと報告されている[188]。

上掲事例では犯罪に使用されたコンピュータ、及び犯罪の収入としてのビットコインの押収を実施している。

2.4.3 先制的な被害防止措置及び根拠となる法制度

- 攻撃元サーバへのアクセス（保管されたデータの閲覧、複写、改変を含む。）及び機能停止措置（テイクダウン）

刑事訴訟法典第 57-1 条では、捜査の過程で、操作が行われる敷地内にあるコンピュータシステムを用いて、当該捜査に関するデータにアクセスすることに加え、このコンピュータからアクセス可能な別のコンピュータシステムにアクセスすることを認めている。警察、国家憲兵隊の敷地内にあるコンピュータシステムから、他のコンピュータシステムに保存されるデータにアクセスすることも可能である。アクセスが認められるデータは、進行中の捜査事案に関係するデータに限られる。取得したデータの記憶媒体へのコピー、記憶媒体の差押えも可能である。

また、コンピュータデータ等の差押えについて定める刑事訴訟法典 97 条は、データの差押えの過程でコピーが作成された場合であって、当該コンピュータデータに違法あるいは人や財産の安全を脅かす危険がある場合、令状に基づき、司法の手元にない物理媒体（コピー元のコンピュータ等を指すと考えられる）から永久に消去されることがあるとしている。

187 国家憲兵隊へのヒアリング結果に基づく。

188 国家憲兵隊情報ウェブサイト https://www.gendinfo.fr/dossiers/la-menace-cyber/Faire-la-lumiere-sur-le-Darkweb（2023 年 2 月 22 日閲覧）

● その他サイバー犯罪捜査における技術的装置の活用

刑事訴訟法典第 706-102-1 条では、対象者の同意なく、あらゆる場所のコンピュータシステムの保存データや、ユーザ画面表示、ユーザの入力内容、周辺機器からの送受信にアクセスし、保存、転送できる技術的装置を設定できると規定している。

上掲条項に基づき、捜査を目的としたトロイの木馬型ソフトウェア等いわゆるポリスウェアによる被疑者端末の情報監視・取得、また取得した情報を警察が準備したサーバに転送・迂回させる行為等を、捜査手法として投入することが可能となり得る。具体の捜査手法の適用は、捜索時の令状で具体的に指定される。一方、警察がおとりとしてのサーバ運用を行うことは、捜査機関による犯罪の扇動に相当する可能性がある[189]。

コラム　国家憲兵隊によるポリスウェア及び代替サーバの使用

ドイツの報道ではドイツ、フランス、オランダ等により 2020 年 7 月まで行われた EnchroChat の国際捜査において、フランス国家憲兵隊による EnchroChat サーバのハッキングが行われた。フランス側は同サービスのハッキングに利用した技術について「機密」と宣言したが、ドイツの裁判所の文書から、フランスがオランダの支援を受け、フランス北部の EnchroChat サーバに、アップデートを装ってマルウェアをインストールしたことが確認できる。このソフトウェアはいわゆるトロイの木馬で、データはフランス国家憲兵隊のサーバに転送され、そこからさらにユーロポールのサーバに転送された[190]。

2020 年公表の上院報告書においても、法執行機関による代替サーバ運用の実施事例が報告されている。最終目的はマルウェア感染端末の情報収集ではなく、感染端末からのマルウェアの「クリーンアップ」である。

2019 年、国家憲兵隊の C3N が、コンピュータセキュリティ会社 Avast と協力して、マルウェア Retadup に係る巨大なボットネットの活動を食い止める大規模な作戦を実行した。Retadup は、主に米国とラテンアメリカに拠点を置くマルウェアで、感染したコンピュータはボットネット（何十万台ものハッキングされたコンピュータのネットワーク）を形成し、所有者の知らないうちに暗号通貨を生成するものであった。この目的のため、感染したコンピュータは「コマンドアンドコントロール」サーバに接続する。Avast 社は、感染したコンピュータがパリ地方に拠点を置くサーバに接続されていることを把握、C3N に通知し、パリ検察庁が捜査を開始した。

Avast と C3N は、ハッカーが使用するプロトコルに欠陥を発見、C3N はこの欠陥を、リモート経由でコンピュータの感染を駆除するために利用した。

具体的には、感染したコンピュータが接続するサーバを国家憲兵隊の用意したサーバに置き換え、このサーバから、マルウェアを無効にする効果のある空のコマンドを実行する指示を発出した[191]。この空のコマンドについて国家憲兵隊ウェブサイトでは、新たなデータコードを追加するものではないと報告されている。

---

189 国家憲兵隊へのヒアリング結果に基づく。

190 Deutschlandfunk Kultur 放送記事「捜査のための革新か、危険な大衆監視か」（2022 年 2 月 14 日付）https://www.deutschlandfunkkultur.de/encro-chat-hack-ueberwachung-daten-100.html（2023 年 2 月 22 日閲覧）

191 仏上院（元老院）報告書「サイバー犯罪上院報告書 情報番号 613 号（2019-2020）2020 年 7 月 9 日」（2020 年 7 月発行）https://www.senat.fr/rap/r19-613/r19-613_mono.html（2023 年 2 月 22 日閲覧）

2.4.4 民間事業者の義務及び根拠となる法制度

(1) 通信履歴（ログ）の保存義務

通信履歴（トラフィックデータ）については、2022 年 3 月の法改正で刑事訴訟法典第 60-1-2 条が新設され規定がより明確化された。同条に基づき、法執行機関は懲役 3 年相当の犯罪に関する場合、あるいはサイバーを用いた懲役 1 年以上の犯罪に関連して、他に犯罪者を特定する手段が無い場合に、令状に基づき法執行機関が事業者に要求可能である。

電気通信法典第 L34-1 条に基づき、事業者は接続または端末機器の使用の日から 1 年間、接続元を特定するための技術データまたは使用端末機器に関するデータの保管を義務付けられる。保全要請は「国家司法傍受プラットフォーム」を介して事業者に送信され、提供された情報も同プラットフォームで保管管理される。

(2) 捜査への協力義務

刑事訴訟法典第 230-1 条以下に基づき、暗号化・パスワード保護されたデータの復号化は、裁判所判事命令のもとで専門家等を指定して行う。国防秘密関連のデータや傍受データは、国の機関で対応するとされている。

なお、国家憲兵隊情報サイトによると、国家憲兵隊フォレンジック研究所（IRCGN）内の工学・デジタルフォレンジック部門（DCIN）内のコンピュータサイエンスエレクトロニクス部門（INL）では、国家憲兵隊全体で使用する復号化プラットフォーム「Gendpass」を設置運用しており、Android 携帯のロック解除、スマートフォンの復号化、trueCrypt 等暗号化コンテナの開封、暗号化アプリケーションの分析等を実施している[192]。

国家憲兵隊へのヒアリングによると、復号化や修復等において高度専門的なニーズがある場合、外部委託は可能であるが、復号化や修復を事業者に義務付けるものではない。

また、ISP 等において、犯罪に用いられたバックドアを保全する義務もない[193]。

サイバー犯罪捜査では司法傍受等の技術的手段が用いられるが、これに関して刑事訴訟法典第 60-1 条、60-2 条、100-3 条では、通信事業者に対し、業務捜査に関連する情報（GDPR 規則 9 条に定める特別なカテゴリの個人情報除く）の提供、法執行機関によるテレマティクス[194]、コンピュータ手段による介入の受入、通信傍受に伴う機器等の受入を義務として定めている。対象罪種や令状等制限事項については情報取得、通信傍受における制限による。

(3) サイバー事案発生時の公的機関等への報告義務

郵便・電子通信法典 33-14 条では通信事業者に対し、情報システムのセキュリティに影響を与える可能性のある事象が検出された場合、遅滞なく国家情報システム安全保障庁に通知することとしている。

---

192 国家憲兵隊情報ウェブサイト https://www.gendinfo.fr/dossiers/la-menace-cyber/Cybercriminalite-techniciens-et-enqueteurs-au-service-du-terrain（2023 年 2 月 22 日閲覧）

193 国家憲兵隊へのヒアリング結果に基づく。

194 電気通信（テレコミュニケーション）と情報処理（インフォマティクス）を組み合わせた用語。

(4) 情報開示に関する利用者等への通知義務

データ処理、ファイル及び自由に関する 1978 年 1 月 6 日の法律第 78-17 号第 107 条において、刑事犯罪防止、捜査、訴追等に関わるデータ処理に関して、その人の基本的権利及び正当な利益を考慮に入れつつ、民主的社会において必要かつ均衡のとれた措置を構成する限りにおいて、権利を一部制限することを認めている。この範囲において、データ主体への通知なくデータ処理を行うことが可能である[195]。

2.4.5 サイバー捜査における人権確保に関する係争事例

訴えを起こそうとする事例は多くあるが、フランスでは犯罪捜査に関係する範疇で、広範な司法傍受を認めており、基本的には犯罪とは無関係とはいえないケースが多く、却下されている[196]。

[195] データ処理、ファイルおよび自由に関する 1978 年 1 月 6 日の法律第 78-17 号第 107 条 https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000886460/（2023 年 2 月 22 日閲覧）

[196] 国家憲兵隊へのヒアリング結果に基づく。

諸外国におけるサイバー事案の捜査手法等に関する調査研究　報告書

令和 5 年（2023 年）3 月 15 日発行

発　行　者　公益財団法人日工組社会安全研究財団
101−0047 東京都千代田区内神田一丁目 7 番 8 号 大手町佐野ビル 6 階
TEL (03)3219-5177　http://www.syaanken.or.jp/

調査・制作　エム・アール・アイ リサーチアソシエイツ株式会社
技術・安全事業部
100-0014 東京都千代田区永田町二丁目 10 番 3 号 東急キャピトルタワー
TEL (03) 6858-3529

ISBN 978-4-904181-36-2 Printed in Japan