サイバー空間の安全の確保

第１節　サイバー空間の脅威

第２節　サイバー空間の脅威への対処

第3章
CHAPTER 3

第1節 サイバー空間の脅威

インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着し、今や、サイバー空間は国民の日常生活の一部となっている。こうした中、サイバー空間における脅威は深刻な情勢が続いている。

令和元年（2019年）中の警察によるサイバー犯罪の検挙件数は、過去最多となった。インターネットバンキングに係る不正送金事犯は、平成28年（2016年）以降、金融機関のセキュリティ対策の強化等により発生件数・被害額ともに減少傾向が続いていたが、令和元年９月から被害が急増し、発生件数・被害額のいずれも前年と比べて大幅に増加した。このほか、コード決済(注1)不正利用事案等の国民に身近なサイバー犯罪が発生した。

また、サイバー攻撃も後を絶たない。国外においては、豪州連邦議会等に対するサイバー攻撃、アンチドーピング関連機関に対するサイバー攻撃等が発生した。国内においても、国際的ハッカー集団によるものとみられる地方自治体、民間企業等のウェブサイトの閲覧障害が発生したほか、大手電機会社が、不正アクセスを受け、情報が流出した可能性がある旨を公表した。警察庁が国内で検知したサイバー空間における探索行為等とみられるアクセスの件数も増加傾向にある。

（1）サイバー犯罪の検挙状況

最近５年間のサイバー犯罪の検挙状況は、図表３－１のとおりである。

サイバー犯罪の検挙件数は増加傾向にあり、令和元年中の検挙件数は9,519件と、前年より479件（5.3%）増加し、過去最多を記録した。

①　不正アクセス禁止法(注2)違反

令和元年中の不正アクセス禁止法違反の検挙件数は816件と、前年より252件（44.7%）増加した。また、検挙人員は234人と、前年より61人（35.3%）増加した。

②　コンピュータ・電磁的記録対象犯罪(注3)

令和元年中のコンピュータ・電磁的記録対象犯罪の検挙件数は436件と、前年より87件（24.9%）増加した。

③　その他

令和元年中の児童買春・児童ポルノ禁止法違反の検挙件数は2,281件と、前年より224件（10.9%）増加した。また、著作権法違反の検挙件数は451件と、前年より240件（34.7%）減少した。

図表３－１　サイバー犯罪の検挙件数の推移（平成27年～令和元年）

区分＼年次	平成27	28	29	30	令和元
合計（件）	8,096	8,324	9,014	9,040	9,519
不正アクセス禁止法違反	373	502	648	564	816
コンピュータ・電磁的記録対象犯罪	240	374	355	349	436
児童買春・児童ポルノ禁止法違反	1,881	2,002	2,225	2,057	2,281
詐欺	951	828	1,084	972	977
著作権法違反	593	586	398	691	451
上記以外の罪種	4,058	4,032	4,304	4,407	4,558

注１：バーコード又はQRコード®（株式会社デンソーウェブの登録商標）を用いたキャッシュレス決済
２：不正アクセス行為の禁止等に関する法律
３：刑法に規定されているコンピュータ又は電磁的記録を対象とした犯罪

（２）サイバー攻撃の情勢

重要インフラの基幹システムを機能不全に陥れ、社会の機能を麻痺させるサイバーテロ(注)や情報通信技術を用いて政府機関や先端技術を有する企業から機密情報を窃取するサイバーインテリジェンス（サイバーエスピオナージ）といったサイバー攻撃が世界的規模で発生している。

①　サイバーテロの情勢

情報通信技術が浸透した現代社会において、重要インフラの基幹システムに対する電子的攻撃はインフラ機能の維持やサービスの供給を困難とし、国民の生活や社会経済活動に重大な被害をもたらすおそれがある。我が国では、社会的混乱が生じるようなサイバーテロは発生していないものの、標的型メール攻撃等によるサイバー攻撃事案は発生しているほか、海外では、不正プログラムによって金融機関のシステムや原子力関連施設の制御システムの機能不全を引き起こす事案が発生している。

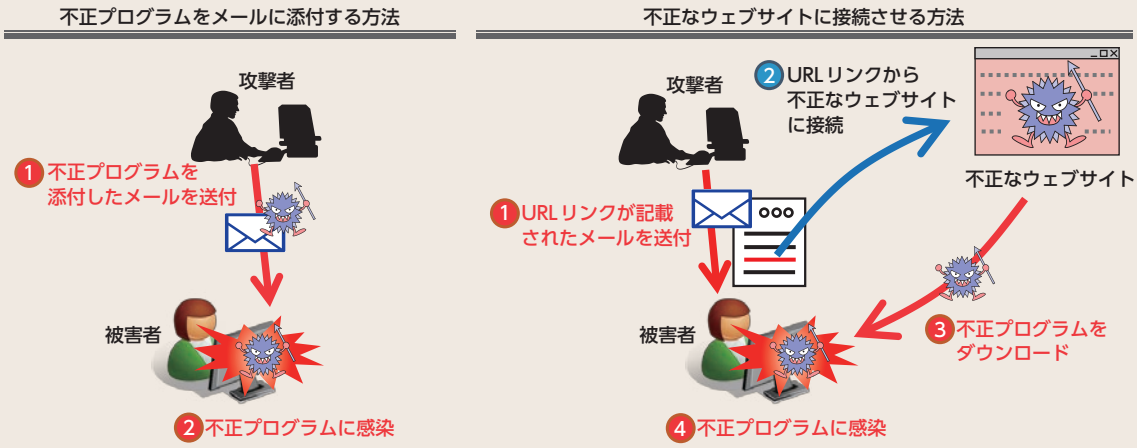
②　サイバーインテリジェンスの情勢

近年、情報を電子データの形で保有することが一般的となっている中、軍事技術への転用も可能な先端技術や、外交交渉における国家戦略等の機密情報の窃取を目的として行われるサイバーインテリジェンスの脅威が、世界各国で問題となっている。また、我が国に対するテロの脅威が継続していることを踏まえると、物理的なテロの準備行為として、重要インフラ事業者等のシステムに侵入し警備体制に関する情報を窃取するなどのサイバーインテリジェンスが行われるおそれがある。

③　サイバー攻撃の手口

サイバー攻撃に用いられる手口としては、セキュリティ上のぜい弱性を悪用するなどして攻撃対象のコンピュータに不正に侵入するもの、不正プログラムに感染させることにより管理者や利用者の意図しない動作をコンピュータに命令するものなどがある。また、不正プログラムに感染させる手口としては、業務に関連した正当なものであるかのように装った電子メールを介して、市販のウイルス対策ソフトでは検知できない不正プログラムに感染させるなどする標的型メール攻撃が代表的である。

図表３－２　不正プログラムに感染させる手口



CASE

令和元年６月、米国航空宇宙局（NASA）は、ジェット推進研究所（JPL）のネットワークが約10か月にわたって外部から侵入され、火星探査計画に関するデータを含む、約500メガバイトのデータが窃取されたとの報告書を発表した。

注：重要インフラ（「重要インフラの情報セキュリティ対策に係る第４次行動計画」（平成29年４月サイバーセキュリティ戦略本部決定、令和２年１月改定）において、情報通信、金融、航空、空港、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む。）、医療、水道、物流、化学、クレジット及び石油の14分野が指定されている。）の基幹システム（国民生活又は社会経済活動に不可欠な役務の安定的な供給、公共の安全の確保等に重要な役割を果たすシステム）に対する電子的攻撃又は重要インフラの基幹システムにおける重大な障害で電子的攻撃による可能性が高いもの

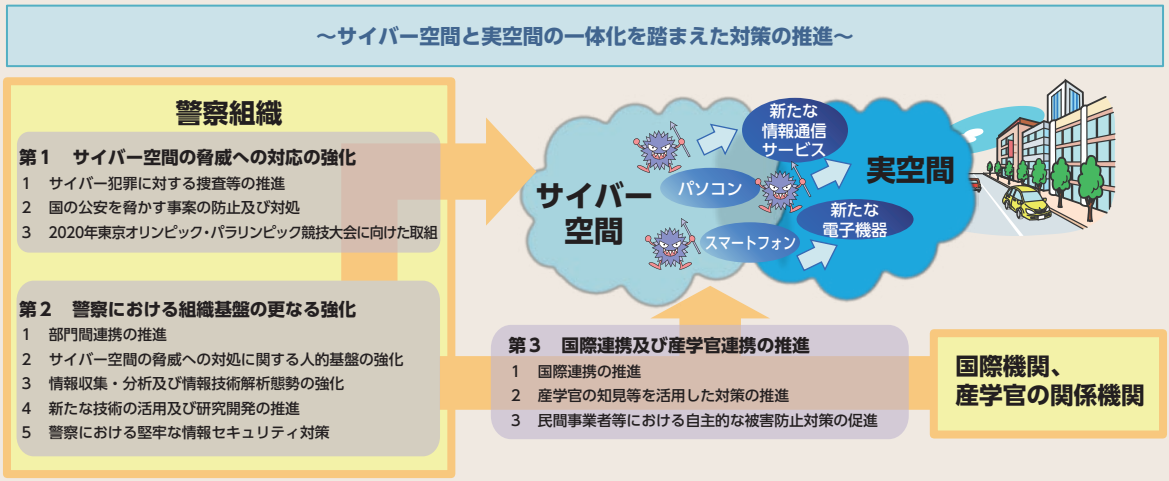
第2節 サイバー空間の脅威への対処

1 総合的なサイバーセキュリティ対策の強化

（1）警察におけるサイバーセキュリティ戦略

社会情勢等の変化に的確に対応しつつ、サイバー空間の脅威に先制的かつ能動的に対処するため、警察では、「警察におけるサイバーセキュリティ戦略」（平成27年（2015年）９月策定、平成30年９月改定）に基づき、警察における組織基盤の更なる強化を図るなど、警察組織の総合力を発揮した効果的な対策を推進している。

図表３－３　改定後の警察におけるサイバーセキュリティ戦略の概要



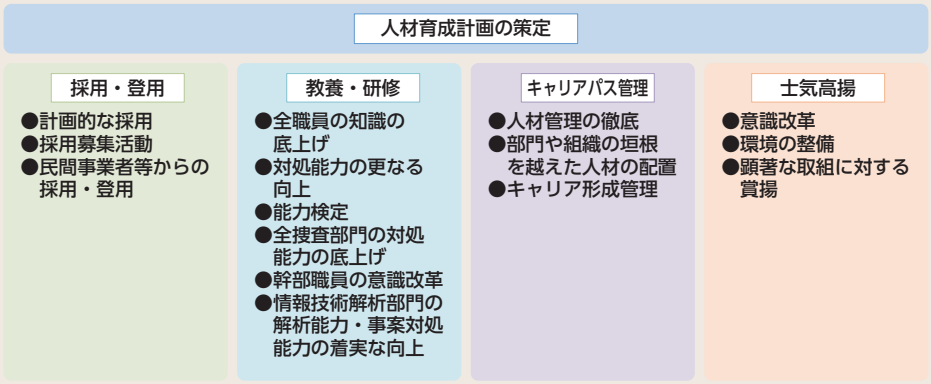
（2）サイバー空間の脅威への対処に係る組織基盤の強化

①　サイバー空間の脅威への対処に係る人材の確保・育成

警察では、サイバー空間の脅威への対処に係る人的基盤を強化するため、「サイバー空間の脅威への対処に係る人材育成方針」（平成27年12月策定、平成31年４月改定）に基づき、職員の採用・登用、教育・研修、キャリアパスの管理等を部門横断的かつ体系的に実施している。

また、サイバー空間の脅威への対処に関する知識及び技能のレベルごとに警察職員の育成数の目標等を定め、計画的な人材育成を推進することにより、警察全体のサイバー空間の脅威への対処能力の向上を図ることとしている。

図表３－４　サイバー空間の脅威への対処に係る人材育成



memo

サイバーセキュリティコンテストの開催

警察庁では、各都道府県警察の捜査員等を対象に、サイバー空間の脅威への対処に関する知識・技能を競うサイバーセキュリティコンテストを開催している。同コンテストでは、実際の事案を想定したシナリオを使用し、捜査員等の知識・技能の向上を図っているほか、全国の優秀な人材の発掘に取り組んでいる。

サイバーセキュリティコンテストの状況

②　サイバー犯罪捜査等に関する教養

警察大学校に設置されているサイバーセキュリティ対策研究・研修センター(注)には、解析研究室と並んで捜査研修室が置かれており、同研修室では、各都道府県警察においてサイバー犯罪対策やサイバー攻撃対策に従事する幹部職員及び捜査員をはじめ、全部門の警察職員を対象に、より高度な技術的知見等を修得させるための研修を実施している。

例えば、サイバー犯罪・サイバー攻撃対策に関する専門的な知識を有する捜査員を対象に、実際の事案を想定した演習等を通じて、犯罪捜査の観点からより高度な技術的知見を修得させることにより、各都道府県警察においてサイバー犯罪等の捜査の中核として活躍する人材を育成するための研修を実施しているほか、サイバー犯罪対策やサイバー攻撃対策に従事する幹部職員を対象に、サイバー空間の脅威に先制的かつ能動的に対処するため、適切な捜査方針を樹立する上で必要となる知識等を修得させるための研修を実施している。


捜査研修室における研修の様子

注：サイバーセキュリティ対策研究・研修センターにおける研究及び研修の内容については、28頁（トピックスⅡ　科学捜査を支える取組）参照

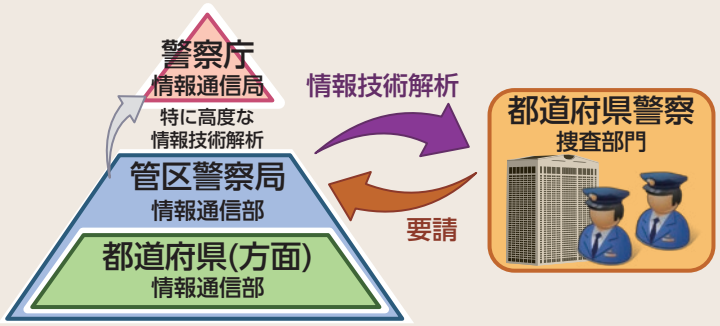
2 技術支援と解析能力の向上

（1）犯罪の取締りへの技術支援

情報化社会の進展は、匿名性が高く、追跡が困難なサイバー空間を利用した様々な犯罪の敢行を容易にさせており、こうした犯罪の取締りにおいては、高度な技術的知見が必要となっている。

このため、警察では、警察庁及び地方機関に情報技術解析課を設置し、都道府県警察に対して、捜索差押え現場でコンピュータ等を適切に差し押さえるための技術的な指導や、押収したスマートフォン等から証拠となる情報を取り出すための解析を実施する技術支援を行っている。

図表３－５　犯罪の取締りへの技術支援



また、警察庁に設置された高度情報技術解析センターでは、高度で専門的な知識及び技術を有する職員を配置するとともに、高性能な解析用資機材を整備し、破損した電磁的記録媒体からの情報の抽出・可視化、コンピュータ・ウイルス等の不正プログラムの解析等を行っている。

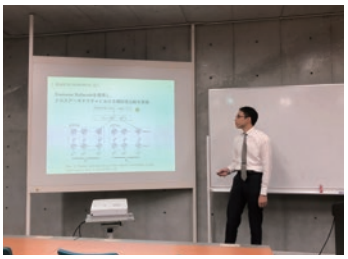
（2）解析能力向上のための取組

近年、コンピュータ・ウイルス等の不正プログラムを悪用したサイバー犯罪・サイバー攻撃が多発する中、その手口の巧妙化・多様化により、不正プログラム解析には極めて高い技術力が求められている。また、IoT機器をはじめとする新たな電子機器やそれに関連するサービスの社会への定着、スマートフォン等のアプリの多様化・複雑化、自動運転システムの実現に向けた技術開発等が進む中、警察捜査を支えるためには、最新の技術に対応した解析能力の向上を図っていく必要がある。

そのため、警察では、解析手法の開発や資機材の整備、高度な解析技術を持つ職員の育成のほか、犯罪に悪用され得る最先端の情報通信技術の調査・研究(注)を推進している。

memo 国内外研究機関への職員派遣

警察では、電子機器の解析やサイバー犯罪・サイバー攻撃への対策に資する最先端の研究を行っている国内外の研究機関に職員を派遣し、不正プログラムの解析手法や、今後悪用され得るネットワークを利用したサービス等に関する調査を実施し、解析能力の向上に努めている。


調査内容の発表状況

注：サイバーセキュリティ対策研究・研修センターにおける研究の内容については、28頁（トピックスⅡ　科学技術を支える取組）参照

3 サイバー犯罪への対策

（1）不正アクセス対策

① 発生状況等

令和元年（2019年）における不正アクセス行為の認知件数(注)は2,960件であり、これを不正アクセス行為後の行為別にみると、「インターネットバンキングでの不正送金等」が1,808件（61.1％）と最多であった。

また、検挙した不正アクセス禁止法違反に係る不正アクセス行為の手口は、「利用権者のパスワードの設定・管理の甘さにつけ込んだもの」が310件（39.4％）と最多であった。

図表３－６ 不正アクセス行為後の行為別認知件数（平成30年及び令和元年）

区分＼年次	平成30	令和元
合計（件）	1,486	2,960
インターネットバンキングでの不正送金等	330	1,808
インターネットショッピングでの不正購入	149	376
メールの盗み見等の情報の不正入手	385	329
オンラインゲーム・SNSの不正操作	199	60
インターネット・オークションの不正操作	29	47
知人になりすましての情報発信	24	30
暗号資産交換業者等での不正送信	169	22
ウェブサイトの改ざん・消去	13	19
その他	188	269

図表３－７ 検挙した不正アクセス禁止法違反に係る不正アクセス行為の犯行手口の内訳（平成30年及び令和元年）

区分＼年次	平成30	令和元
合計（件）	520	787
識別符号窃用型(注)	502	785
利用権者のパスワードの設定・管理の甘さにつけ込んだもの	278	310
他人から入手したもの	13	182
識別符号を知り得る立場にあった元従業員や知人等によるもの	131	161
言葉巧みに利用権者から聞き出した又はのぞき見たもの	17	20
スパイウェア等のプログラムを使用して識別符号を入手したもの	0	5
インターネット上に流出・公開されていた識別符号を入手したもの	7	3
フィッシングサイトにより入手したもの	3	1
その他	53	103
セキュリティ・ホール攻撃型	18	2

注：アクセス制御されているサーバに、ネットワークを通じて、他人の識別符号を入力して不正に利用する行為

CASE

カザフスタン国籍の男（27）は、平成30年９月、ポイントサービス運営会社のサーバに不正アクセスし、他人のポイントを自らが作成したアカウントに移動させた上、店舗にて不正使用し、飲食物をだまし取ったほか、平成31年１月、複数の他人のID・パスワードを不正に保管した。同年５月までに、同男を不正アクセス禁止法違反（不正アクセス行為・識別符号保管）、詐欺罪等で逮捕した（千葉）。

CASE

中国国籍の男（29）は、令和元年７月、不正に入手したID・パスワードを使用して、国内のコード決済サービス運営会社のサーバに不正アクセスし、コンビニエンスストアにおいて、電子タバコカートリッジをだまし取った。同年11月までに、同男を不正アクセス禁止法違反（不正アクセス行為）及び詐欺罪で逮捕した（熊本）。

注：不正アクセス被害の届出を受理した場合のほか、余罪として新たな不正アクセス行為の事実を認知した場合、報道を踏まえて事業者等に不正アクセス行為の事実を確認した場合その他関係資料により不正アクセス行為の事実を確認することができた場合において、被疑者が行った犯罪構成要件に該当する行為の数をいう。

② 不正アクセス防止対策に関する官民連携

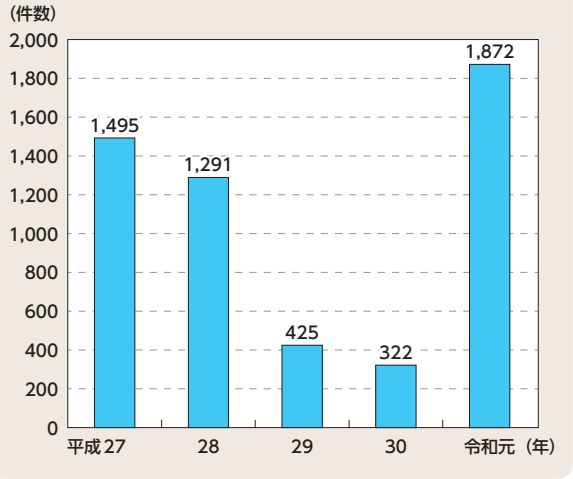
不正アクセス防止対策に関する官民意見集約委員会(注1)における「不正アクセス防止対策に関する行動計画」に基づき、情報セキュリティに関する情報を掲載した情報セキュリティ・ポータルサイト「ここからセキュリティ！」(注2)を公開するなど、不正アクセスを防止するための官民連携した取組を実施している。

（2）インターネットバンキングに係る不正送金事犯への対策

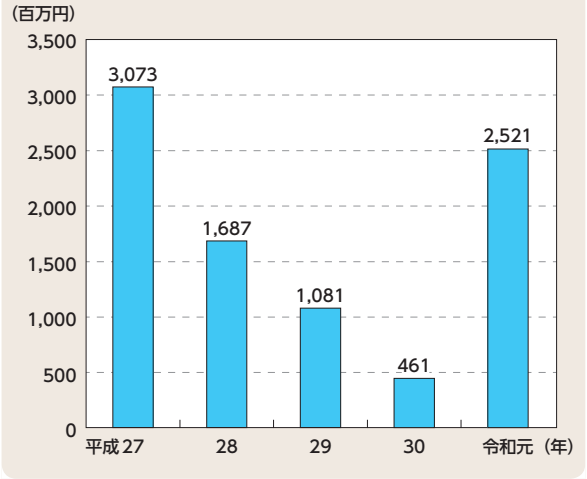
① 発生状況

令和元年における不正送金事犯の発生件数は1,872件、被害額は約25億2,100万円と、発生件数は過去最多であった平成26年に次ぐ件数であり、被害額も前年から大幅に増加したが、その被害の多くは、金融機関を装ったフィッシングサイトへ誘導するショートメッセージや電子メールを用いた手口によるものと考えられる。また、銀行口座を不正送金先とする従来の手口のほか、電子マネーを購入する手口等が確認された。

図表３－８ インターネットバンキングに係る不正送金事犯の発生件数の推移（平成27～令和元年）



図表３－９ インターネットバンキングに係る不正送金事犯の被害額の推移（平成27～令和元年）



② 不正送金事犯に対処するための取組

ア 不正送金事犯に関与した者の検挙状況

警察では、令和元年中、不正送金事犯に関連して、他人に利用させる意図を隠して口座を開設した者、口座を譲渡した者、不正に送金された資金を引き出した者等合計46人を検挙した。

イ 金融機関と連携した抑止対策

警察では、金融機関等に対し、モニタリング(注3)の強化、ワンタイムパスワード(注4)及び二経路認証(注5)の利用、本人確認の徹底等の被害防止対策の強化を要請している。

ウ インターネットバンキングに係る不正送金被害の急増に関する注意喚起

警察庁では、インターネットバンキングの不正送金被害の急増を受けて、令和元年10月、一般財団法人日本サイバー犯罪対策センター（JC3(注6)）と連携し、それぞれのウェブサイトにおいて、被害防止の注意喚起を実施した。

また、全国銀行協会と手口や被害状況等に関する情報共有を行うとともに、同年12月、同協会と連携し、それぞれのウェブサイトにおいて、被害防止の注意喚起を実施した。

注1：平成23年から、警察庁、総務省及び経済産業省が主体となって、社会全体としての不正アクセス防止対策の推進に当たって必要となる施策に関して、現状の課題や改善方策について官民の意見を集約するため、民間事業者等と共に開催している委員会
2：https://www.ipa.go.jp/security/kokokara/
3：金融機関等が、顧客があらかじめ登録した口座以外への送金等について、不正なものであるかどうかを確認すること
4：インターネットバンキング等における認証用パスワードであって、認証のたびにそれを構成する文字列が変わるもの。これを導入することにより、識別符号を盗まれても次回の利用時に使用できないことになる。
5：インターネットバンキング等において、コンピュータ（第一経路）で振り込み等の取引データを作成した後、スマートフォン等（第二経路）で承認を行うことで取引を成立させる認証方式
6：117頁参照

（3）不正プログラム対策

警察では、不正指令電磁的記録に関する罪の取締りを実施するとともに、民間事業者と連携した不正プログラムによる被害拡大防止のための対策を講じている。

警察庁では、犯罪捜査の過程で警察が把握した新たな不正プログラムに関する情報をウイルス対策ソフト事業者等に提供し、当該不正プログラムによる被害の拡大防止を図るための枠組み(注1)を構築している。

CASE

無職の男（54）らは、平成29年３月、アダルト動画を再生しようとした男性のパソコンで、有料動画配信サービスの利用契約が完了した旨及び料金の支払を求める旨のウインドウが繰り返し表示されるプログラムを実行させ、契約が成立し、利用料金を支払う義務があるものと誤信した男性から７万円をだまし取った。令和元年５月までに、同男らを不正指令電磁的記録供用罪、詐欺罪等で逮捕した（茨城、宮城、愛知、静岡、石川、愛媛、鹿児島）。

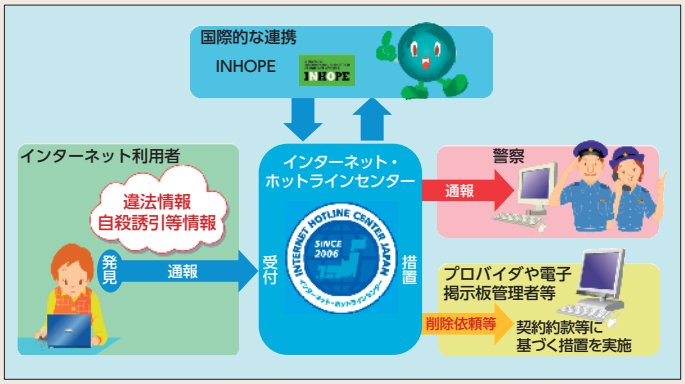
（4）インターネット上の違法情報・有害情報対策

インターネット上には、児童ポルノ、規制薬物の広告に関する情報等の違法情報や、違法情報には該当しないが、犯罪や事件を誘発するなど公共の安全と秩序の維持の観点から放置することができない有害情報が多数存在している。

①　インターネット・ホットラインセンターにおける取組

警察庁では、一般のインターネット利用者等から、違法情報等に関する通報を受理し、警察への通報、サイト管理者への削除依頼等を行うインターネット・ホットラインセンター（IHC）を運用している。令和元年中、IHCでは1,617件の違法情報の削除依頼を行っており、そのうち1,482件（91.7%）が削除された。また、神奈川県座間市における殺人事件(注2)を受け、IHCでは、平成30年１月から、他人を自殺に誘引・勧誘する情報等（以下「自殺誘引等情報」という。）を受理したときは、警察庁を介さずにサイト管理者へ削除依頼等を直接行うとともに、緊急の対応を要する場合には当該情報を都道府県警察に通報することとしている。令和元年中、IHCでは2,560件の自殺誘引等情報の削除依頼を行っており、そのうち1,758件（68.7%）が削除された。

図表３－10　インターネット・ホットラインセンターにおける取組



IHCに通報された違法情報等の中には、外国のサーバにそのデータが蔵置されているものがある。このうち児童ポルノについては、各国のホットライン相互間の連絡組織であるINHOPE(注3)の加盟団体に対して、削除に向けた措置を依頼している。

注１：116頁参照
２：平成29年10月、神奈川県座間市において、SNS上に自殺願望を投稿するなどした者が、言葉巧みに誘い出された上、殺害されたもの
３：現在の名称はInternational Association of Internet Hotlinesであるが、旧名称のInternet Hotline Providers in Europe Associationの略称を現在も使用している。平成11年（1999年）に設立され、平成31年１月末現在、IHCを含む52団体（47の国・地域）から構成される国際組織

② 効果的な違法情報等の取締り

警察では、サイバーパトロール等により違法情報・有害情報の把握に努めるとともに、効率的な違法情報の取締り及び有害情報を端緒とした取締りを推進している。

また、合理的な理由もなく違法情報の削除依頼に応じないサイト管理者については、検挙を含む積極的な措置を講じている。

（5）サイバー防犯ボランティアに対する支援

サイバーパトロールにより発見した違法情報・有害情報をIHC、サイト管理者等に通報する取組やインターネット利用者に対する講演活動等を行うサイバー防犯ボランティアの団体数及び団体構成員数は、図表３－11のとおりであり、警察では、研修会を開催するなどして、こうした活動を行う団体の拡大と取組の活性化を図っている。

図表３－11　サイバー防犯ボランティア団体数及び団体構成員数の推移（平成27～令和元年）

区分＼年次	平成27	28	29	30	令和元
サイバー防犯ボランティア団体数（団体）	224	202	221	244	274
サイバー防犯ボランティア団体構成員数（人）	9,406	8,598	8,294	9,022	9,625

注：数値は、各年末現在

memo　サイバー防犯ボランティアの活動に対する内閣総理大臣表彰

文教大学サイバー防犯ボランティア（神奈川県茅ヶ崎市）では、研究・開発したシステムを活用して多くの違法情報・有害情報を効率的に発見し、IHC等に通報を行い、サイバー空間における犯罪防止に大きく貢献したほか、他の大学生防犯ボランティアと積極的に意見交換を実施し、サイバーパトロール実施要領を伝える研修会を開催するなど、活動の裾野拡大を推進した功績により、令和元年安全安心なまちづくり関係功労者内閣総理大臣表彰を受賞した。

文教大学サイバー防犯ボランティアによる小学校でのサイバー防犯教室の様子

（6）民間事業者、外国捜査機関等と連携した被害防止対策

サイバー犯罪における手口が悪質・巧妙化する中、被害防止対策の重要性が高まっていることから、警察では、民間事業者、外国捜査機関等と連携し、都道府県警察が相談等で把握した海外の偽サイト等(注)に関する情報をウイルス対策ソフト事業者等に提供するなど、積極的な被害防止対策を推進している。

注：海外のサーバに開設された、実在する企業のウェブサイトを装ったウェブサイトや、インターネットショッピングを利用した詐欺や偽ブランド品の販売を目的とするウェブサイト等

4 サイバー攻撃への対策

警察庁及び各都道府県警察では、サイバー攻撃対策を担当する組織を設置しているほか、各部門が連携し、サイバー攻撃の実態解明や被害の未然防止等を推進している。また、各国治安情報機関との捜査や情報収集に関する協力を強化したり、民間事業者等との協力関係を確立して被害の未然防止を図ったりするなど、サイバー攻撃をめぐる新たな情勢に対処するための対策に取り組んでいる。

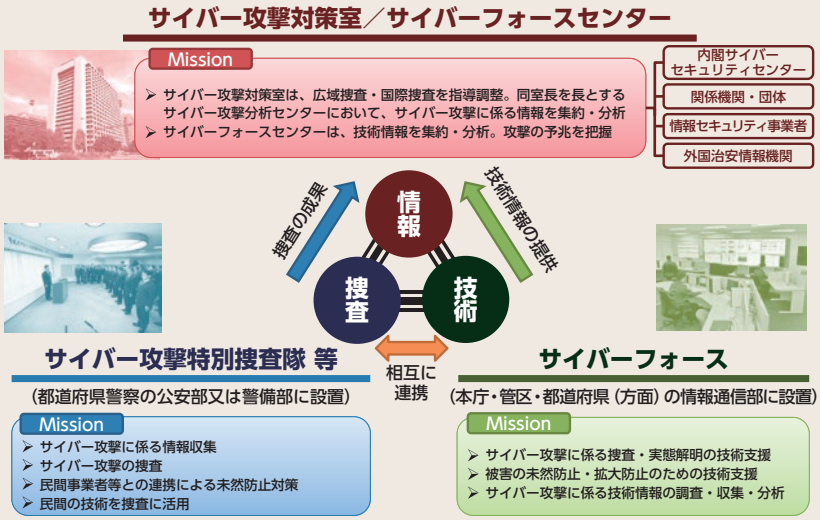
（1）サイバー攻撃対策の推進体制

警察庁では、サイバー攻撃対策室が、都道府県警察が行う捜査に対する指導・調整、官民連携や各国治安情報機関との情報交換に当たるとともに、サイバー攻撃対策室長を長とするサイバー攻撃分析センターにおいて、サイバー攻撃に係る情報の集約・分析を実施している。

また、政府機関、重要インフラ事業者、先端技術を有する事業者等が多く所在する14都道府県警察には、サイバー攻撃特別捜査隊を設置している。サイバー攻撃特別捜査隊は、サイバー攻撃に係る捜査に関する専門的な知識、技能及び経験をいかし、設置された都道府県におけるサイバー攻撃対策のみならず、他の都道府県警察に対して技能・技術・体制面の支援を行うことにより、サイバー攻撃事案に対する警察全体の捜査能力の向上を図っている。このほか、情報収集活動の推進や民間事業者等との協力関係の確立においても、中核的な役割を果たしている。

さらに、警察庁及び地方機関の情報通信部門(注)にサイバーフォースを設置しており、都道府県警察のサイバー攻撃対策部門に対する技術支援を実施している。また、警察庁のサイバーフォースセンターは、全国のサイバーフォースの司令塔の役割を担っており、サイバー攻撃発生時においては被害状況の把握、被害拡大の防止、証拠保全等の技術支援を行う拠点として機能するほか、24時間体制でのサイバー攻撃の予兆・実態把握、標的型メールに添付された不正プログラム等の分析、全国のサイバーフォースに対する指示等を行っている。

図表3－12 サイバー攻撃対策の推進体制



注：管区警察局情報通信部（四国警察支局情報通信部を含む。以下同じ。）、東京都警察情報通信部、北海道警察情報通信部、府県情報通信部（四国警察支局の管轄区域内の県情報通信部を含む。以下同じ。）及び方面情報通信部

（2）サイバー攻撃の予兆・実態の把握

①　実態解明の推進

警察では、違法行為に対する捜査を推進するとともに、サイバー攻撃を受けたコンピュータやサイバー攻撃に使用された不正プログラムを解析し、その結果や犯罪捜査の過程で得た情報等を総合的に分析するなどして、攻撃者及び手口に関する実態解明を進めている。また、各国治安情報機関との情報交換を行うとともに、ICPO(注1)を通じるなどして、外国捜査機関との間で国際捜査協力を積極的に推進している。

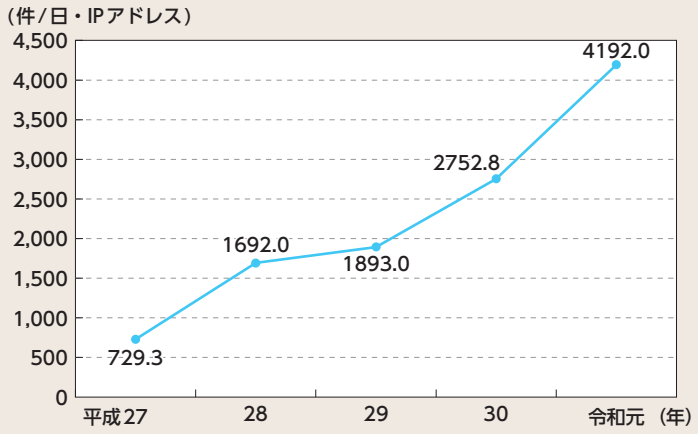
②　リアルタイム検知ネットワークシステム

サイバーフォースセンターでは、インターネットとの接続点に設置したセンサーにおいて検知したアクセス情報等を集約・分析することで、DoS(注2)攻撃の発生や不正プログラムに感染したコンピュータの動向等の把握を可能とするリアルタイム検知ネットワークシステムを24時間体制で運用している。このシステムにより分析した結果をインターネット観測結果として重要インフラ事業者等への情報提供に活用するほか、警察庁ウェブサイト「@police」で広く一般に公開している。

memo　令和元年中のインターネット観測結果

サイバーフォースセンターでは、令和元年中に、インターネットとの接続点に設置したセンサーにおいて、一つのセンサー当たり約20秒に１回の割合という高い頻度で世界中から不審なアクセスが行われていることを観測した。

図表３－13　１つのセンサーに対する１日当たりの不審なアクセス件数の推移（平成27～令和元年）



令和元年５月中旬にマイクロソフト社から、同社が提供するOSの遠隔操作に使用されるリモートデスクトップサービス(注3)について、攻撃に成功すると外部から管理者権限で任意の操作が実行可能となるぜい弱性に関する緊急の修正プログラムが公開された。警察では、この情報を受けてリアルタイム検知ネットワークシステムにおいて観測したアクセス情報を分析した結果、同年３月下旬から同年５月下旬にかけて、同サービスを標的とした広範囲の宛先ポート(注4)に対するアクセスが急増していることを確認したことから、同サービスの利用者に対し、適切なセキュリティ対策を講じるよう注意喚起を行った。

注１：International Criminal Police Organization（国際刑事警察機構）の略
２：Denial of Serviceの略。特定のコンピュータに対し、大量のアクセスを繰り返し行い、コンピュータのサービス提供を不可能にするサイバー攻撃
３：職場等に設置されたコンピュータのデスクトップ環境を、別の場所に設置されたコンピュータ等から閲覧・操作等できるサービス
４：TCP・UDP/IP通信において、利用するサービスを識別するためのインターフェースであり、０から65535までの番号が割り当てられている。

5 国際連携の推進

（１）国際捜査共助

国境を越えて行われるサイバー犯罪・サイバー攻撃について、国内における捜査で犯人を特定できない場合は、外国捜査機関の協力を求める必要がある。

警察庁では、サイバー犯罪に関する条約(注１)、刑事共助条約（協定）(注２)、ICPO、サイバー犯罪に関する24時間コンタクトポイント(注３)等の国際捜査共助の枠組みを活用し、国境を越えて行われるサイバー犯罪・サイバー攻撃に対処している。

（２）外国捜査機関等との連携の推進

警察庁では、多国間における情報交換や協力関係の確立等に積極的に取り組んでおり、令和元年中は、G7ローマ／リヨン・グループ(注４)に置かれたハイテク犯罪サブグループ、ICPO及びEUROPOL(注５)が共催するサイバー犯罪会議等の国際会議に参加した。また、FBI(注６)による米国内外の捜査機関等の職員を対象としたサイバー犯罪対策等に関する研修や、ICPO等が主催するワークショップに我が国の警察職員を派遣するなど、サイバー空間の脅威に関する情報の共有や、国際捜査共助に関する連携強化等を推進している。

ハイテク犯罪サブグループ

さらに、情報技術解析に関する知識・経験等の共有を図るため、ICPO加盟国の法執行機関に加えて、国外の民間企業や学術機関が参加するICPOデジタルフォレンジック専門家会合に平成28年から参加しているほか、情報セキュリティ事案に対処する組織の国際的な枠組みであるFIRST(注７)に平成17年から加盟しており、組織間の情報共有を通じ、適切な事案対処に資する技術情報の収集を行っている。

（３）国際協力の推進

警察庁では、サイバー空間の脅威への諸外国の対処能力の向上を図るとともに、外国捜査機関等との協力関係を強化することを目的として、外務省や独立行政法人国際協力機構（JICA）と連携して外国捜査機関等に関する支援を行っている。平成26年度からは、外国捜査機関等のサイバー犯罪対策等に従事する職員を招へいし、サイバー空間の脅威への対処に関する知識・技術を習得させることなどを目的とした研修を実施しているほか、平成29年度からは、ベトナム公安省の職員を受け入れて、サイバーセキュリティ対策等に関する知識・技術の習得を目的とした研修を行っている。

注１：サイバー犯罪から社会を保護することを目的として、コンピュータ・システムに対する違法なアクセス等一定の行為の犯罪化、コンピュータ・データの迅速な保全等に係る刑事手続の整備、犯罪人引渡し等に関する国際協力等につき規定している。平成24年に我が国について発効した。
２：205頁参照
３：平成９年（1997年）12月のG8司法内務閣僚会合で策定された「ハイテク犯罪と闘うための原則と行動計画」等に基づき設置されたもので、平成31年２月現在、86の国・地域に設置されている。
４：昭和53年（1978年）にボン・サミットを契機に発足したG8テロ専門家会合（G8ローマ・グループ）と平成７年（1995年）にハリファクス・サミットで設置されたG8国際組織犯罪対策上級専門家会合（G8リヨン・グループ）が、平成13年（2001年）の米国における同時多発テロ事件以降合同で開催されているもので、国際組織犯罪対策やテロ対策等について検討している。なお、平成26年（2014年）３月より、G7として実施している。
５：European Union Agency for Law Enforcement Cooperationの略。欧州連合（EU）の法執行機関であるが、捜査権限はなく、加盟国間の情報交換の促進や収集した情報の分析等が主な任務である。
６：Federal Bureau of Investigation（米国司法省連邦捜査局）の略
７：Forum of Incident Response and Security Teamsの略

6 官民連携の推進

（1）サイバーテロ対策協議会

警察では、各都道府県警察とサイバー攻撃の標的となるおそれのある重要インフラ事業者等とで構成するサイバーテロ対策協議会を全ての都道府県に設置し、サイバー攻撃の脅威や情報セキュリティに関する情報提供、民間の有識者による講演、参加事業者間の意見交換や情報共有を行っているほか、サイバー攻撃の発生を想定した共同対処訓練等を行っている。

CASE

埼玉県警察では、令和元年11月、「埼玉県サイバーテロ対策協議会第10回総会」を開催した。同協議会では、警察の取組報告、民間の有識者によるサイバー攻撃の情勢及び対策に関する講演、事案発生時を想定した演習等を行った。演習では、ウェブサーバに保存されている各種ログファイルの解析等を通して、事案発生時における各種対応について確認した。

サイバーテロ対策協議会

（2）サイバーインテリジェンス情報共有ネットワーク

警察では、情報窃取の標的となるおそれの高い先端技術を有する事業者等との間で、情報窃取を企図したとみられるサイバー攻撃に関する情報共有を行うサイバーインテリジェンス情報共有ネットワークを構築しており、このネットワークを通じて事業者等から提供された情報を集約するとともに、これらの事業者等から提供された情報及びその他の情報を総合的に分析し、事業者等に対し、分析結果に基づく注意喚起を行っている。

（3）不正プログラム対策協議会

警察では、警察庁とウイルス対策ソフト提供事業者等とで構成する不正プログラム対策協議会において、不正プログラム対策に関する情報共有を行っている。特に、警察からは、市販のウイルス対策ソフトで検知できない新たな不正プログラムに関する情報や未知のぜい弱性に関する情報を提供し、情報セキュリティ対策の向上を図っている。

（4）不正通信防止協議会

警察では、警察庁とセキュリティ監視サービス又はセキュリティ事案に対処するサービスを提供する事業者とで構成するサイバーインテリジェンス対策のための不正通信防止協議会において、標的型メール攻撃等に利用される不正プログラムの接続先等の情報を共有することにより、我が国の事業者等が不正な接続先へ通信を行うことを防止している。

（5）共同対処協定の締結

サイバー犯罪の潜在化の防止、捜査活動の効率化及び再発防止を図るため、警察では、民間事業者等との共同対処協定の締結を推進している。事業者と信頼関係を構築し、サイバー犯罪の警察への通報の促進等を図るため、令和元年末までに、金融機関や暗号資産交換業者等、全国で577事業者・団体と本協定を締結している。

（6）高度な研究開発等を行う大学に対するサイバー攻撃への対策の推進

近年、高度な研究開発を行う大学に対するサイバー攻撃が発生していることから、警察では、当該サイバー攻撃に関する情報収集・分析を強化するとともに、大学と連携し、サイバー攻撃をめぐる最新の情勢や被害防止対策等に関する情報共有、サイバー攻撃の発生を想定した共同対処訓練を実施することなどにより、高度な研究開発を行う大学に対するサイバー攻撃への対処能力の強化を図っている。

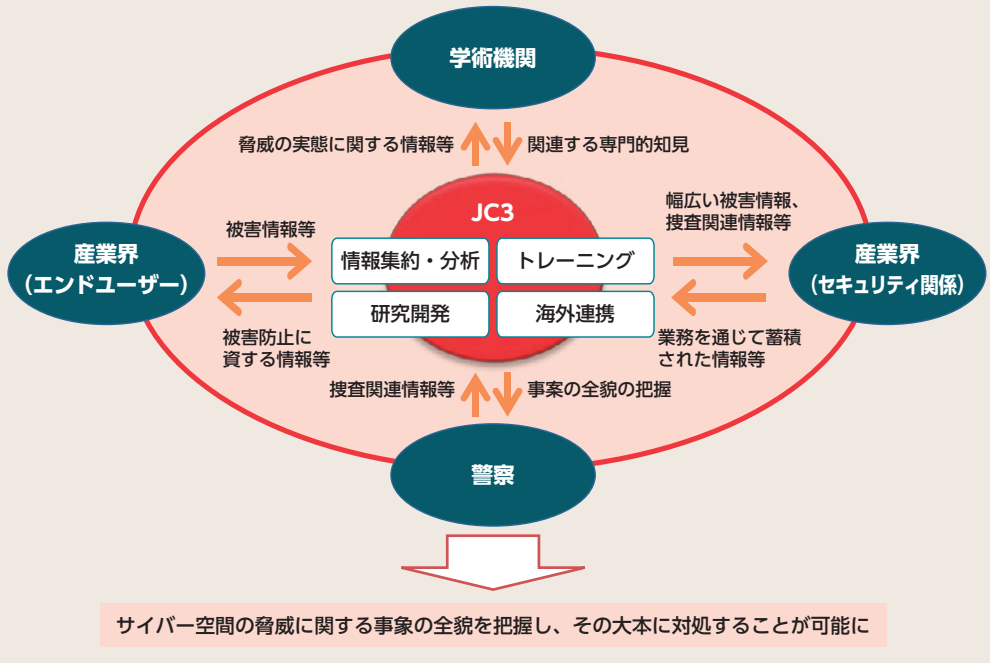
（7）事業者等における自主的な被害防止対策の推進

事業者やインターネット利用者等がサイバー犯罪・サイバー攻撃の被害に遭わないよう、警察では、商工会議所、学術機関、地方公共団体等と連携し、事業者等に対して自主的な被害防止対策を促すための広報啓発活動等を実施している。

（8）日本サイバー犯罪対策センターとの連携

我が国における新たな産学官連携の枠組みとして平成26年から業務が開始された一般財団法人日本サイバー犯罪対策センター（JC3(注)）においては、産学官の情報や知見を集約・分析し、その結果等を還元することで、脅威の大本を特定し、これを軽減及び無効化することにより、以後の事案発生の防止を図ることとしている。警察では、捜査関連情報等をJC3において共有し、産学におけるサイバーセキュリティに関する取組に貢献するとともに、JC3において共有された情報を警察活動に迅速・的確に活用している。

図表３－14　日本サイバー犯罪対策センター（JC3）の概要



注：Japan Cybercrime Control Centerの略

警察活動の最前線

サイバー攻撃対策の重要性

北海道警察情報通信部情報技術解析課支援分析係
朝野（あさの）　奈輝（だいき）

私は、サイバー空間の脅威への対処について考えてもらうため、重要インフラ事業者等に対するサイバーセキュリティに関するセミナーや、サイバー攻撃共同対処訓練等を実施しています。

その一つに、「社内CSIRTを発足しているが、サイバーセキュリティインシデントが発生した際の行動や対応について理解を深めるため、セミナーを開催してほしい」という相談を受けて実施したものがありました。

CSIRTとは、サイバー攻撃を受けた場合や情報通信システム等の不具合が発生した場合に、原因の究明や被害拡大防止のため対応する組織の総称であり、サイバーセキュリティインシデントが発生した場合に迅速かつ的確な対応が求められます。セミナーでは、CSIRTの社内における位置付けや、パソコンが不正プログラムに感染した際の原因究明の手掛かりとして重要な揮発性情報の保全方法等、CSIRTに必要な知識を様々な側面から伝えることができました。

サイバー攻撃の手口は日々巧妙化し、その脅威は私たちの近くに潜んでいるかもしれません。サイバー空間の脅威から組織や個人の情報を守るためには、一人一人の技術力や情報リテラシーを向上させることが重要です。これからもセミナーを通じて、サイバー空間の脅威から身を守る術を伝えていきたいです。

指揮官の何げない一言に着想を得た情報技術解析

広島県警察本部生活安全部サイバー犯罪対策課サイバー犯罪捜査第三係（現　広島県福山北警察署生活安全課長）
伊藤（いとう）　直也（なおや）

私は平成17年に情報技術解析の任に就き、以来捜査経験をいかした解析のあり方を模索してきました。

ある殺人事件の解析に従事した時のことです。捜査は難航を極め、逮捕状請求の決め手がないまま、捜査会議ではギブアップが喉元まで出ていました。

その時、捜査の指揮を執っていた参事官がある映像を指して「これは何で真っ黒なんだ。カメラに袋でも被せたのか？」と何げなく一言。

それは犯行現場を撮影したはずの、被疑者方の防犯カメラの復元映像でした。

「袋を被せるくらいなら電源を切るでしょう」正直私はそう思いました。しかし何かが引っ掛かる。なぜ黒い？

膨大なデータと格闘し、捜査員総出で何百回と再現を繰り返した結果、その映像が撮影される条件は「夜間、照明を消した屋内に設置のカメラで」「カメラの前にあったカーテンを開いた時」以外にないことが分かったのです。

実際に殺人が起こった時にその場所で、照明を消し息を潜めて被害者を待ち構えていたなど、襲撃を狙った人物以外にあり得ません。

こうして逮捕状の発付を受けることができたのです。

解析とはともすればデータを出力する作業だと考えがちです。しかし捜査は被疑者の行動を疎明することであり、この解析も被疑者の行動を「データで解釈」した結果でした。

捜査は機械でなく人が判断するものと再認識したエピソードです。

今後も捜査の柱のひとつとして、サイバー的手法で貢献したいと考えています。