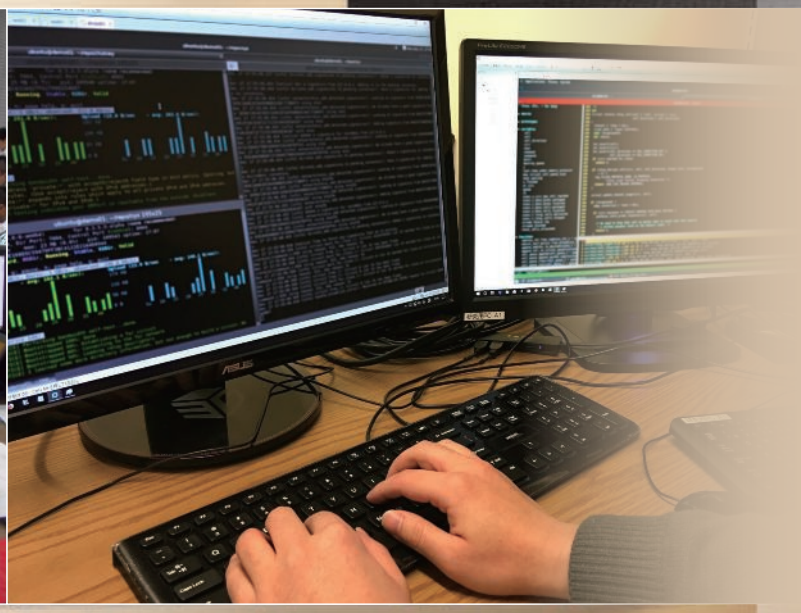
サイバー空間の安全の確保

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、不正アクセス禁止法違反等のサイバー犯罪が多発しているほか、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するなど、サイバー空間における脅威は深刻化している状況にある。

（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、平成30年（2018年）中の検挙件数は9,040件と、前年より26件（0.3%）増加し、過去最多を記録した。

①　不正アクセス禁止法違反

平成30年中の不正アクセス禁止法違反の検挙件数は564件と、前年より84件（13.0%）減少した。また、検挙人員は173人と、前年より82人（32.2%）減少した。

②　不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪(注)

平成30年中の不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪の検挙件数は349件と、前年より６件（1.7%）減少した。

③　その他

平成30年中の児童買春・児童ポルノ禁止法違反の検挙件数は2,057件と、前年より168件（7.6%）減少した。また、著作権法違反の検挙件数は691件と、前年より293件（73.6%）増加した。

図表３－１　サイバー犯罪の検挙件数の推移（平成26～30年）

区分＼年次	26	27	28	29	30
合計（件）	7,905	8,096	8,324	9,014	9,040
不正アクセス禁止法違反	364	373	502	648	564
不正指令電磁的記録に関する罪及びコンピュータ・電磁的記録対象犯罪	192	240	374	355	349
児童買春・児童ポルノ禁止法違反	1,741	1,881	2,002	2,225	2,057
詐欺	1,133	951	828	1,084	972
著作権法違反	824	593	586	398	691
上記以外の罪種	3,651	4,058	4,032	4,304	4,407

注：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

①　サイバーテロの情勢(注)

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。

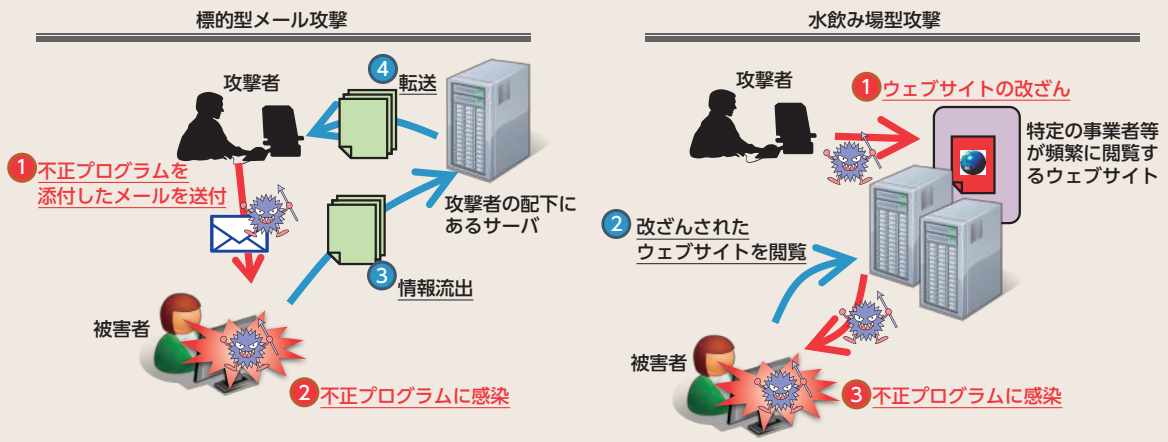
サイバーテロに用いられる手口としては、セキュリティ上のぜい弱性を悪用するなどして攻撃対象のコンピュータに不正に侵入するもの、不正プログラムに感染させることにより管理者や利用者の意図しない動作をコンピュータに命令するものなどがある。

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。

サイバーインテリジェンスに用いられる手口としては、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を添付して、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送信し、これを受信したコンピュータを不正プログラムに感染させるなどして、情報の窃取を図る標的型メール攻撃が代表的である。また、このほかにも、対象組織の職員が頻繁に閲覧するウェブサイトを改ざんし、当該サイトを閲覧したコンピュータに不正プログラムを自動的に感染させる水飲み場型攻撃も発生するなど、その手口はますます巧妙化・多様化している。さらに、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。

図表３－２　サイバーインテリジェンスの手口



CASE

平成30年２月、国立研究開発法人産業技術総合研究所に対し、外部から不正アクセスがあったことが確認され、同年７月、当該不正アクセスが同研究所のメールシステムや管理用ネットワーク内のシステムに対するものであり、未公表の研究情報や個人情報等の窃取又は閲覧が行われた可能性があるとの調査結果が発表された。

注：35頁参照

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

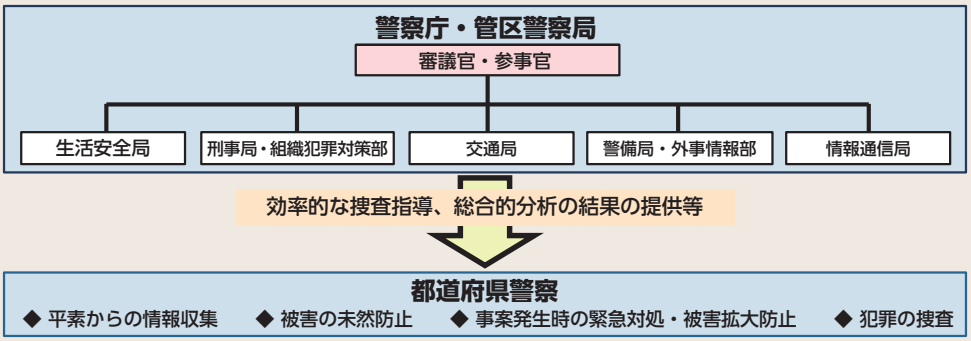
（1）警察におけるサイバー空間の脅威への対処体制

サイバー空間の脅威への対処は警察のいずれの部門にとっても大きな課題となっており、統一的な戦略の下で警察全体の対処能力を強化する必要があることから、警察庁では、サイバーセキュリティの確保に向けた各種取組の総括・調整を行う審議官及び参事官が、

- サイバーセキュリティ戦略の策定
- サイバー空間の脅威への総合的な対処方針の策定
- 捜査員等の人材育成に関する指針の立案
- 民間事業者、外国機関等との連絡の総括
- サイバー空間の情勢の総合的な分析
- 部門横断的な捜査支援・技術支援の調整
- 装備資機材の効果的な整備・活用の調整

といった取組を推進している。

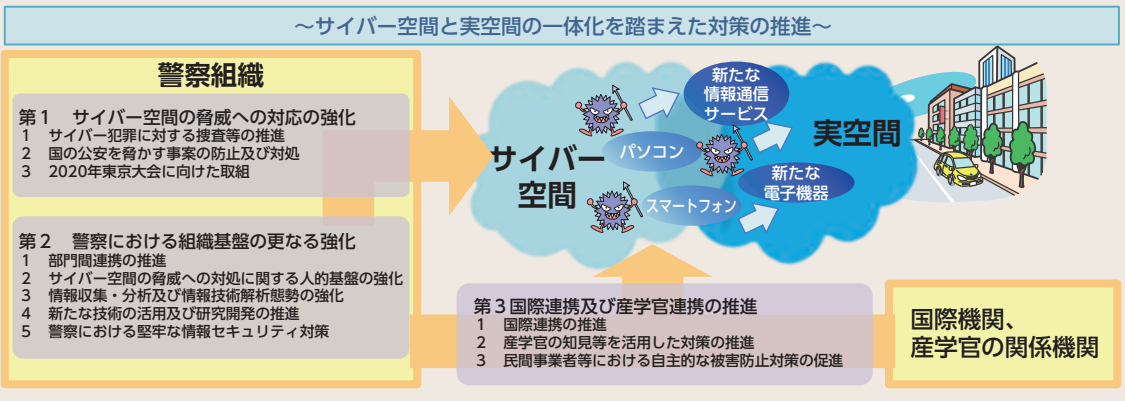
図表３－３ 警察におけるサイバー空間の脅威への対処体制



（2）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、2020年東京オリンピック・パラリンピック競技大会（以下この節において「2020年東京大会」という。）及びその後の社会情勢の変化を見据え、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３－４ 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



（３）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３－５　サイバー空間の脅威への対処に係る人材育成

さらに、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

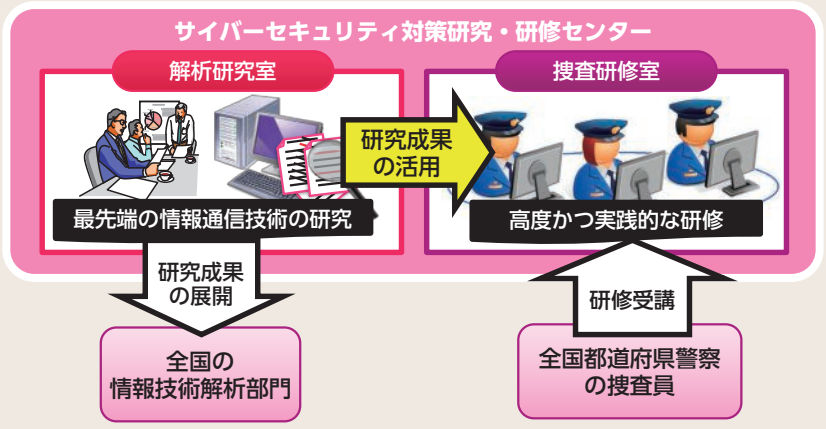
②　サイバーセキュリティ対策研究・研修センターにおける研修

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・研修センターには、解析研究室(注)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、より高度な技術的知見を修得させ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、ロールプレイング方式の演習等を通じて、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。

また、解析研究室においては、サイバー犯罪等に悪用され得る最先端の情報通信技術に関する研究、各種電子機器等の解析手法の確立に向けた研究等が行われており、その研究成果は、捜査研修室における研修にも活用されている。

図表３－６　サイバーセキュリティ対策研究・研修センター



注：152頁参照

2 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

平成30年における不正アクセス行為の認知件数(注1)は1,486件であり、これを不正アクセス行為後の行為別にみると、「メールの盗み見等の情報の不正入手」が385件（25.9%）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おけ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278件（53.5%）と最多であった。

図表３－７ 不正アクセス行為後の行為別認知件数（平成29年及び30年）

区分＼年次	29	30
合計（件）	1,202	1,486
メールの盗み見等の情報の不正入手	146	385
インターネットバンキングでの不正送金等	442	330
オンラインゲーム・SNSの不正操作	83	199
仮想通貨交換業者等での不正送信	149	169
インターネットショッピングでの不正購入	133	149
インターネット・オークションの不正操作	28	29
知人になりすましての情報発信	110	24
ウェブサイトの改ざん・消去	14	13
その他	97	188

図表３－８ 検挙した不正アクセス禁止法違反における不正アクセス行為の犯行手口の内訳（平成29年及び30年）

区分＼年次	29	30
合計（件）	599	520
識別符号窃用型 (注)	545	502
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	230	278
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	113	131
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	42	17
他人から入手したもの	74	13
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	0	7
フィッシングサイトにより入手したもの	2	3
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	37	0
その他	47	53
セキュリティ・ホール攻撃型	54	18

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

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2)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3)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。

CASE

無職の男（22）は、平成29年2月、掲示板サイトから不正に入手したID・パスワードを使用して、国内のインターネットオークションサイトへ不正アクセスし、オークションの商品売買を装って現金をだまし取った。平成30年3月、同男を不正アクセス禁止法違反（不正アクセス行為）、詐欺罪等で検挙した（和歌山）。

注1：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：平成23年に、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設置した委員会

3：https://www.ipa.go.jp/security/kokokara/

memo 仮想通貨の不正送信事犯

平成30年中における仮想通貨の不正送信事犯は、認知件数が169件、被害額は約677億3,820万円相当となっている。特に、平成30年１月には約580億円相当、同年９月には約70億円相当の仮想通貨が、国内の仮想通貨交換業者等からそれぞれ不正に送信されたとみられる事案が発生した。

こうした状況を踏まえ、警察庁、金融庁及び消費者庁は、「仮想通貨交換業者等に関する３省庁局長級連絡会議」を開催し、これらの事案に対する対応、利用者保護に向けた取組、他の仮想通貨交換業者、みなし仮想通貨交換業者及び無登録業者への対応等について、意見交換を実施し、更なる連携強化を図っている。

CASE

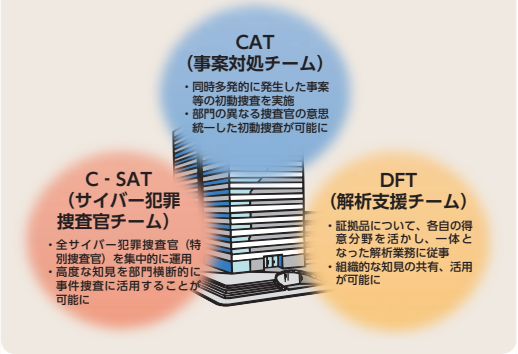
平成30年８月から同年９月にかけて、仮想通貨関連サービスに使用するサーバに虚偽の情報を与え、同サービスの運営会社が管理する仮想通貨合計約1,500万円相当を移転させ、財産上不法の利益を得たなどとして、平成31年３月、少年（18）を電子計算機使用詐欺罪等で検挙した。(警視庁)。

memo 都道府県警察における部門横断的なサイバー犯罪捜査を推進するための取組

警視庁では、高度化・深刻化するサイバー犯罪等に組織の総力を挙げて対処するため、平成30年４月、サイバー関連部署を集約した。

これにより、初動捜査を任務とする事案対処チーム(CAT(注1))、専門的知識を有する捜査員で構成されたサイバー犯罪捜査官（特別捜査官）チーム（C－SAT(注2)）、解析業務を担当する解析支援チーム（DFT(注3)）の３チームがそれぞれ部門横断的に編成され、相互に緊密な連携を図りながら、サイバー犯罪等に効果的に対処することが可能となっている。

図表３－９　各チームの概要



（２）コンピュータ・ウイルス対策

警察では、コンピュータ・ウイルスに関する罪の取締りを推進するとともに、民間事業者と連携したコンピュータ・ウイルス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コンピュータ・ウイルスに関する情報をウイルス対策ソフト事業者等に提供し、当該コンピュータ・ウイルスによる被害の拡大防止を図るための枠組み(注4)を構築している。

CASE

地方公務員の男（49）は、平成28年２月、人の電子計算機における実行の用に供する目的で、スマートフォンの位置情報等を特定のサーバに送信するアプリケーションを作成し、男の元交際相手の女性が使用するスマートフォンに無断でインストールして実行可能な状態にした。平成30年４月、同男を不正指令電磁的記録作成罪等で逮捕した（徳島）。

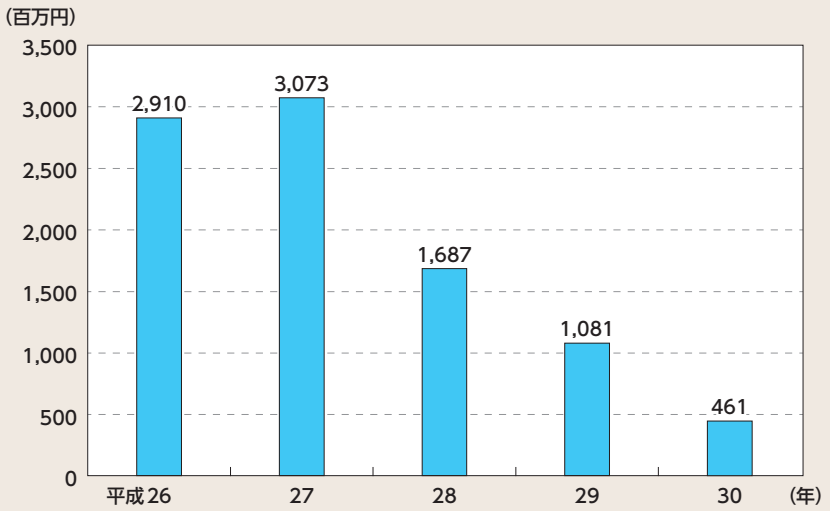
注１：Cyber Action Teamの略
２：Cyber Special Agent Teamの略
３：Digital Forensics Teamの略
４：154頁参照

（3）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

平成30年における不正送金事犯の被害額は約４億6,100万円と、前年の半分以下に減少したが、その要因としては、金融機関のセキュリティ対策が強化されたことによって、地方銀行・信用金庫等を中心とした法人口座の被害が大幅に減少したことなどが考えられる。また、不正送金先の口座名義人の国籍についてはベトナムの割合が高いことが特徴として挙げられる。

図表３－10　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26～30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、平成30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48人を検挙した。

イ　金融機関等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1)の強化、ワンタイムパスワード(注2)及び二経路認証(注3)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。

（4）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、民間事業者や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4)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１：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
２：インターネットバンキング等における認証用の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となる。
３：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
４：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

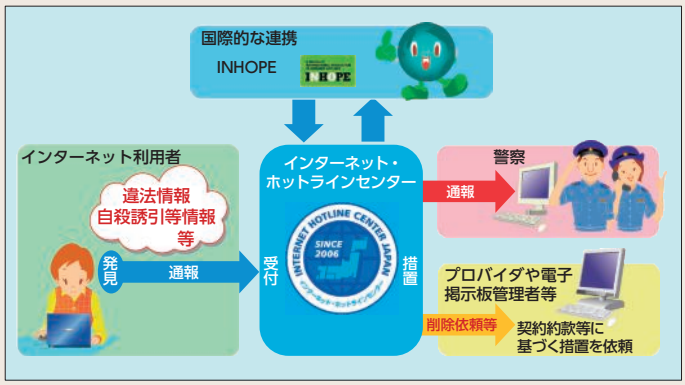
（５）インターネット上の違法情報・有害情報対策

インターネット上には、児童ポルノや覚醒剤等規制薬物の販売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等

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、警察への通報や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。平成30年中、IHCでは1,668件の違法情報の削除依頼を行っており、そのうち1,482件（88.8％）が削除された。また、神奈川県座間市における殺人事件(注1)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に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。平成30年中、IHCでは2,466件の自殺誘引等情報の削除依頼を行っており、そのうち1,814件（73.6％）が削除された。

図表３－11　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2)の加盟団体に対して、削除に向けた措置を依頼している。

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、IHCからの通報に対して全国協働捜査方式(注3)を活用し、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。

（６）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や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３－12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３－12　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26～30年）

区分＼年次	26	27	28	29	30
サイバー防犯ボランティア団体数（団体）	199	224	202	221	244
サイバー防犯ボランティア団体構成員数（人）	7,474	9,406	8,598	8,294	9,022

注：数値は、各年末現在

注１：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
２：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
３：IHCから警察庁に通報された違法情報について効率的な捜査を進めるため、違法情報の発信元を割り出すための初期捜査を警視庁が一元的に行い、捜査すべき都道府県警察を警察庁が調整する捜査方式。平成23年７月から本格実施している。

3 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。

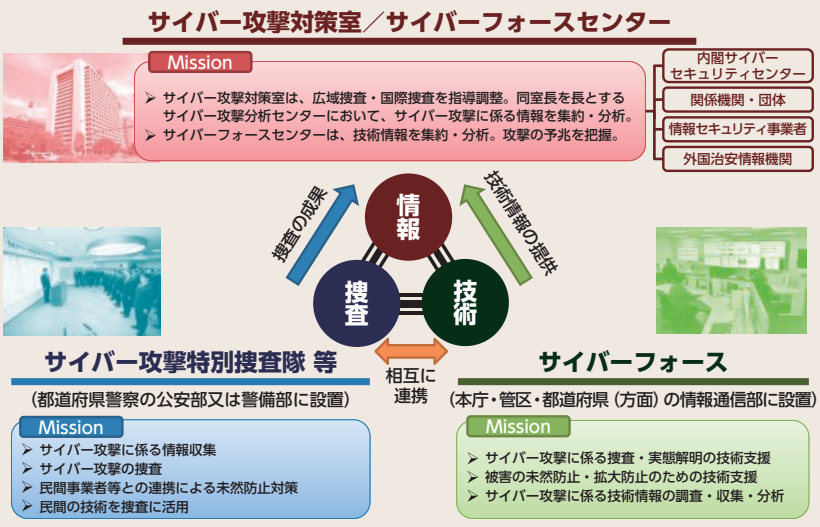
（1）サイバー攻撃対策の推進体制

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にサイバーフォース(注)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３－13　サイバー攻撃対策の推進体制



注：61頁（トピックスⅤ　警察捜査を支える情報技術解析）参照

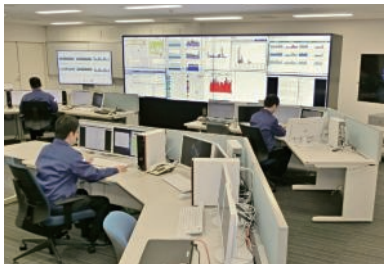
（２）サイバー攻撃の予兆・実態の把握

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１)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。

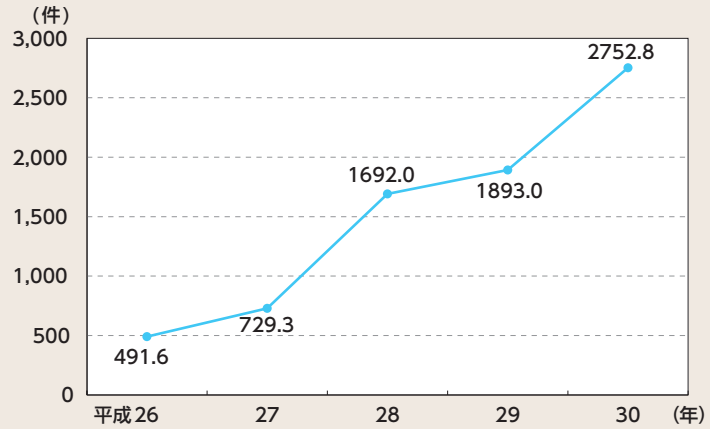


サイバーフォースセンターにおける
リアルタイム検知ネットワークシステムの運用状況

memo　平成30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、平成30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30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３－14　１つのセンサーに対する１日当たりの不審なアクセスの件数の推移（平成26～30年）



特に、平成30年９月以降、ウェブサーバ等に対するアクセスの増加を断続的に観測した。

この観測結果は、何者かがウェブサイトの閲覧等に必要となる通信の仕組みを悪用し、DoS攻撃の一種であるSYN/ACK(注２)リフレクター攻撃を狙ったものと考えられる。

このSYN/ACKリフレクター攻撃では、セキュリティ対策が不十分であった場合、攻撃対象のコンピュータだけではなく、当該攻撃の踏み台となったウェブサーバ等の機器についてもサービス不能の状態に陥る可能性があることから、警察庁では、ウェブサーバ等の管理者に対し、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：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
２：ウェブサイト等を閲覧する際には、利用者からSYNパケット（接続要求）をウェブサーバに送信し、これに対しSYN/ACKパケット（接続許可）が利用者に送信された後、利用者からACKパケット（接続開始）を送信することで接続が確立され、データの送受信が行われる。

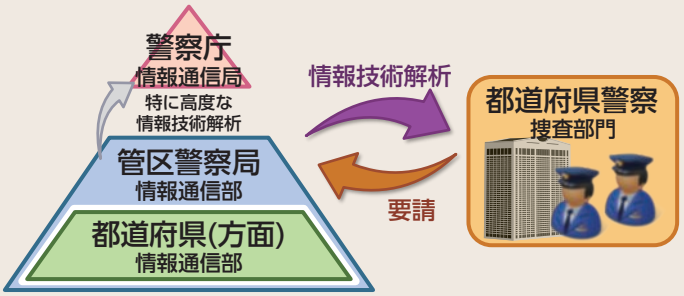
4 技術支援と解析能力の向上

（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(注1)。

図表３－15　犯罪の取締りへの技術支援



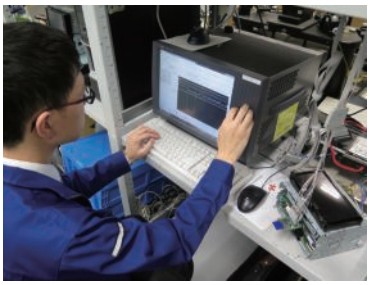
また、警察庁に設置された高度情報技術解析センター(注2)では、高度で専門的な知識及び技術を有する職員を配置するとともに、高性能な解析用資機材を整備し、破損した電磁的記録媒体からの情報の抽出・可視化、コンピュータ・ウイルス等の不正プログラムの解析等を行っている。

（2）情報技術解析に関する調査・研究

近年、最先端の情報通信技術を用いたサイバー犯罪・サイバー攻撃への対応が求められているところ、警察では、警察大学校サイバーセキュリティ対策研究・研修センターの解析研究室において、犯罪の取締りのための情報技術の解析に関する調査・研究を行っている。また、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・研究を実施している。それらの成果は、全国の情報技術解析部門で活用されている。

memo　解析研究室における調査・研究

解析研究室では、犯罪捜査及び情報技術解析の対処能力向上に寄与することを目的として、各種の調査・研究を行っている。例えば、携帯電話、スマートフォン、ナビゲーション機器等の各種電子機器の解析手法の確立に向けた調査・研究に加え、不正プログラムの発見、抽出及び動作の解明のための解析手法並びに仮想通貨の取引を追跡するための手法の確立に関する調査・研究等、サイバー犯罪等の捜査に活用し得る技術の調査・研究を行っているほか、サイバー犯罪等に悪用され得る最先端の情報通信技術に関する調査・研究を進めている。



ナビゲーション機器の解析に関する研究の状況

注１：デジタル・フォレンジックについては、60頁（トピックスⅤ　警察捜査を支える情報技術解析）参照
　２：高度情報技術解析センターの解析事例については、60頁（トピックスⅤ　警察捜査を支える情報技術解析）参照

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、平成30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及びユーロポールが共催するサイバー犯罪会議、日中韓香サイバー犯罪対策課長級会議等の国際会議に参加した。また、FBI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、国内外の民間企業や学術機関が参加する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５)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対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。

２：237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）にハリファックス・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：Forum of Incident Response and Security Teamsの略

6 官民連携の推進

サイバー空間の脅威に対処するためには、民間事業者との連携が重要であり、警察では、人事交流や新種の不正プログラムの情報共有枠組みの構築等の各種取組(注)を行っている。

（1）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。

（2）不正プログラム対策協議会

警察では、ウイルス対策ソフト提供事業者等との間で、不正プログラム対策協議会を設置しており、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。

（3）不正通信防止協議会

警察では、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の間で、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を設置しており、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。

（4）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、平成30年末までに、金融機関や仮想通貨交換業者等、全国で585事業者・団体と本協定を締結している。

（5）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。

（6）事業者等における自主的な被害防止対策の推進

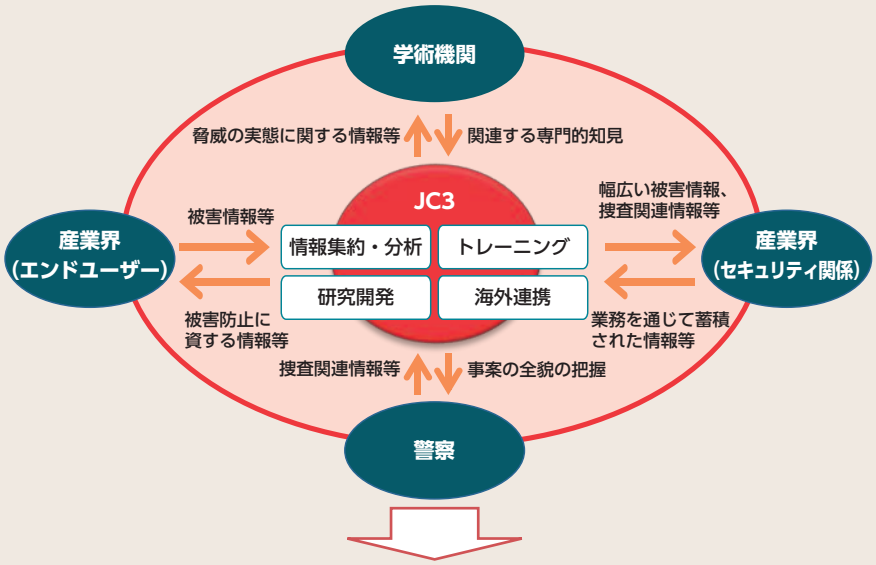
事業者やインターネット利用者等がサイバー犯罪・サイバー攻撃の被害に遭わないよう、警察では、商工会議所、学術機関、地方公共団体等と連携し、事業者等に対して自主的な被害防止対策を促すための広報啓発活動等を実施している。

注：サイバーテロ対策協議会については、42頁参照

（７）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1]）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・的確に活用することにより、安全で安心なサイバー空間の構築に努めている。

図表３－16　日本サイバー犯罪対策センター（JC3）の概要



memo　重要インフラ事業者との連携

警察では、重要インフラに対するサイバー攻撃に備え、事業者等とも連携した各種取組を実施している。

例えば、福岡県警察では、平成30年10月、G20財務大臣・中央銀行総裁会議等の開催を見据えたサイバー攻撃対策の一環として、九州管区警察局と連携し、空港会社との共同対処訓練を実施した。同訓練の実施に当たっては、同社の基幹システムがサイバーテロを受けたとの想定で、ブラインド方式[注2]を採用したほか、同社と共同で作成した想定シナリオを使用し、実際にサイバーテロが発生した場合と同様の対処を行うなど、実践的な内容とすることで、事案対処能力の向上を図った。

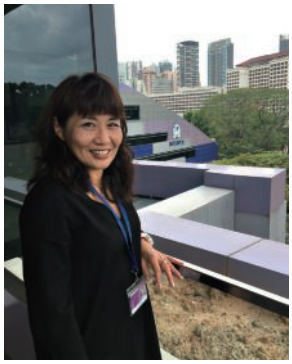

サイバーテロの発生を想定した共同対処訓練

注１：Japan Cybercrime Control Centerの略
　２：訓練参加者に対し、事前に想定シナリオの内容を知らせずに実施する訓練

警察活動の最前線

サイバー犯罪対策～IGCIに出向して～

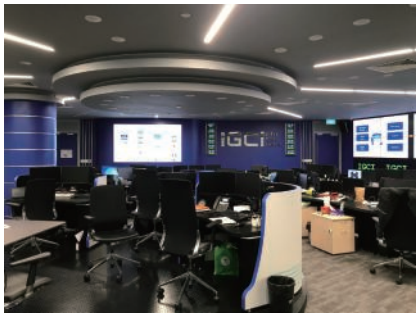
埼玉県警察本部刑事部刑事総務課通訳運用係
椎名（しいな）　美雪（みゆき）　警部



IGCI（INTERPOL Global Complex for Innovation）とは、ICPO（国際刑事警察機構）が2015年にシンガポールに開局したサイバー犯罪の国際協力を目的とした総局で、サイバー犯罪対策、サイバーセキュリティ及びICPO職員や加盟国警察官の能力開発・訓練を担当する部局から構成されます。私は、2016年１月より２年半にわたり、警察庁生活安全局情報技術犯罪対策課からIGCIに派遣されました。

IGCIでは、サイバー犯罪局（Cybercrime Directorate）におけるデジタル捜査支援課（Digital Investigative Support）において、サイバー犯罪対策の国際協力における官民連携業務に従事しました。IGCIの同僚らは世界各国の法執行機関から派遣されており、上司もブラジル国家警察から派遣された警察官であるなど国際的な職場でありました。外国での勤務スタイルは日本とは異なる面も多くあり、そこにこれまでの自身の働き方を合わせていく中で成果を出すことは容易ではありませんでした。

具体的な業務の中で最も印象に残っているのは、民間企業等との協定の締結です。サイバー犯罪の多様化、巧妙化は著しく、サイバー犯罪捜査における国際協力においても官民連携を進める必要があり、加盟国を対象としたサイバー犯罪対処のトレーニングや加盟国の捜査に資する情報提供などに民間企業等との協定締結は必須でした。協定締結に当たっては、「ICPOとして何が必要なのか」を考える一方で「民間企業は何を提供できるのか」等をコストの観点からも分析し、その必要性を事務総局に訴える必要がありました。さらに、ICPOの存在意義のひとつである「加盟国の捜査支援」の観点からは、加盟国の捜査機関と情報共有を行う意義は大きく、サイバー犯罪局にあるサイバーフュージョンセンター（Cyber Fusion Center）と連携のうえ、民間企業から提供されるサイバー空間の脅威に関する情報を捜査に使える形に分析し、加盟国に提供するため、関係する民間企業との間でのデータ共有協定の締結を推進しました。



また、世界各国の金融機関が集中するシンガポールにおいては、金融機関が狙われる事案も多く、サイバー犯罪への対処は国家施策でもあることから、新たな事象に迅速に対応するシンガポールの姿勢はスマート国家と呼ぶにふさわしく、非常に学ぶべき点が多いと感じました。例えば、センサーやカメラが各所に設置されていたほか、各種手続のデジタル化、キャッシュレス化がとても進んでいました。

今後、技術革新が進む中で新たなサービスが次々に生まれ、我々の生活が豊かになる一方、従来は考えもしなかった事故や事件が立て続けに起こることになるかもしれません。2020年東京オリンピック・パラリンピック競技大会が目前に迫り、警察の国際化の必要性は言うまでもありませんが、引き続き、自身の国際対応力の強化に努め、警察の国際化に向けた取組に貢献していきたいと思います。