特集Ⅱ：安全・安心で責任ある サイバー市民社会の実現を目指して

近年、インターネットは、我々の社会・経済活動にとって極めて重要なインフラとして国民生活を支える一方で、サイバー犯罪が増加し、違法情報・有害情報が氾濫するなど、その負の側面も大きくなっています。そのため、平成18年の警察白書では、「安全・安心なインターネット社会を目指して」と題した特集を組み、サイバー空間における様々な問題と、その解決に向けた取組について取り上げるなどしました。

それから５年が経過しましたが、インターネットの利用者数が9,000万人を超えたほか、インターネットの利便性は飛躍的に向上し、場所を選ばず利用できる環境の整備が進むとともに、電子掲示板やブログ、コミュニティサイト等を利用した活動も活発に行われるようになってきています。

その反面、サイバー犯罪は増加の一途をたどり、サイバー空間に氾濫する違法情報・有害情報の件数やサイバー空間で発生した名誉毀損、誹謗中傷に関する相談件数等も増加しています。依然としてこうした問題が生じ、むしろ悪化しているとも言える状況に陥ったのは、かつて想定していなかった手口の出現やサイバー犯罪を取り巻く捜査環境の厳しさといったことに加えて、匿名性の高さ等から「サイバー空間では何をやってもよい」といった歪んだ認識が生まれ、規範意識が低下していることも原因として考えられます。

すなわち、サイバー空間における社会・経済活動は質量ともに年々増大し、今やサイバー空間は現実空間と同視できる程度の新たな公共空間となっているにもかかわらず、いまだ、現実空間ほどには犯罪の取締りや犯罪抑止の取組が進展していないのです。

こうした状況を打破し、サイバー空間における安全・安心を確保するためには、警察がサイバー犯罪に対する取締りを強力に推進するとともに、全ての人々が、サイバー空間の現状について問題意識を共有し、「安全・安心で責任あるサイバー市民社会」を形成していく必要があります。

そのために、本特集では、「安全・安心で責任あるサイバー市民社会の実現を目指して」と題し、第１節でサイバー犯罪に関する情勢を概観し、第２節でこれに対する警察等の取組について詳述した上で、第３節でサイバー犯罪対策の抜本的強化に向け、今後行う必要のある取組を提示しました。

本特集を通じて、国民の皆様に、サイバー犯罪の脅威やサイバー空間における規範意識の確立の重要性に関する認識を深めていただき、今後の警察の取組に対して御理解と御協力をいただくとともに、皆様一人一人がサイバー市民社会の一員として果たすべき役割について考えていただく契機となれば幸いです。

第1節 サイバー犯罪の現状

1 サイバー犯罪の概況

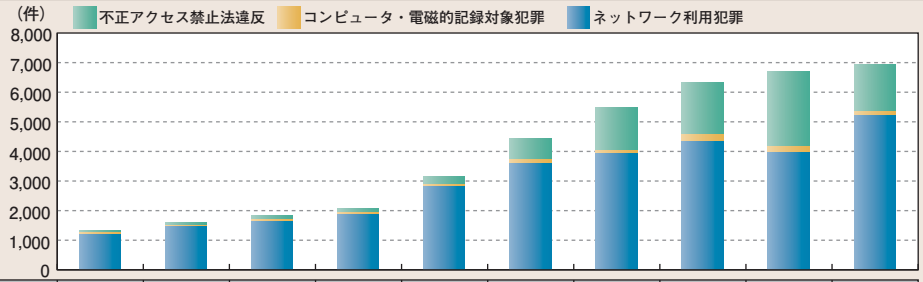
(1)サイバー犯罪の検挙状況

インターネットその他の高度情報通信ネットワークは、国民生活の利便性を向上させ、社会・経済の根幹を支えるインフラとして機能している。その一方で、サイバー犯罪(注1)は年々その深刻さを増している状況にある。

① 検挙状況全般

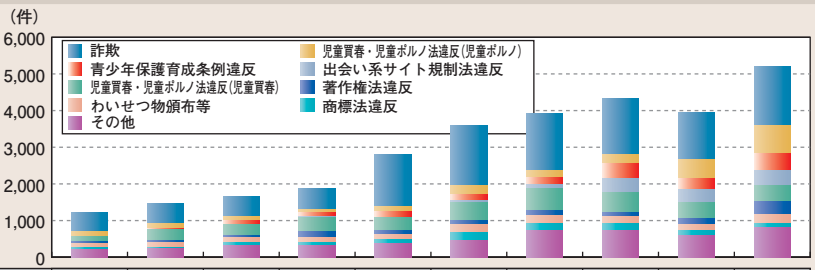
サイバー犯罪の検挙件数は増加の一途をたどっており、平成22年中は6,933件と、前年より243件(3.6%)増加し過去最多となった。また、22年中のネットワーク利用犯罪(注2)の検挙件数についても5,199件と、前年より1,238件(31.3%)増加し、過去最高となった。

図-1 サイバー犯罪の検挙件数の推移(平成13~22年)



区分＼年次	13	14	15	16	17	18	19	20	21	22
合計(件)	1,339	1,606	1,849	2,081	3,161	4,425	5,473	6,321	6,690	6,933
不正アクセス禁止法違反	67	105	145	142	277	703	1,442	1,740	2,534	1,601
コンピュータ・電磁的記録対象犯罪	63	30	55	55	73	129	113	247	195	133
ネットワーク利用犯罪	1,209	1,471	1,649	1,884	2,811	3,593	3,918	4,334	3,961	5,199

図-2 ネットワーク利用犯罪の検挙件数の推移(平成13~22年)



区分＼年次	13	14	15	16	17	18	19	20	21	22
合計(件)	1,209	1,471	1,649	1,884	2,811	3,593	3,918	4,334	3,961	5,199
詐欺	485	514	521	542	1,408	1,597	1,512	1,508	1,280	1,566
児童買春・児童ポルノ法違反(児童ポルノ)	128	140	102	85	136	251	192	254	507	783
青少年保護育成条例違反	10	70	120	136	174	196	230	437	326	481
出会い系サイト規制法違反	−	−	8	31	18	47	122	367	349	412
児童買春・児童ポルノ法違反(児童買春)	117	268	269	370	320	463	551	507	416	410
著作権法違反	86	66	87	174	128	138	165	144	188	368
わいせつ物頒布等	103	109	113	121	125	192	203	177	140	218
商標法違反	31	37	95	82	109	218	191	192	126	119
その他	249	267	334	343	393	491	752	748	629	842

注1：高度情報通信ネットワークを利用した犯罪やコンピュータ又は電磁的記録を対象とした犯罪等の情報技術を利用した犯罪
2：その実行に不可欠な手段として高度情報通信ネットワークを利用する犯罪

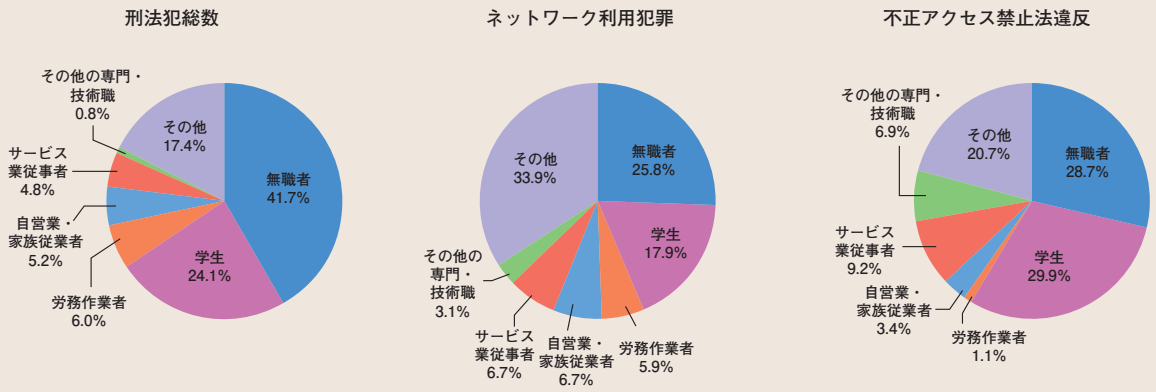
②　被疑者の特徴

警察の犯罪統計を元に、サイバー犯罪に係る被疑者の特徴について分析を行った。その結果、犯行時の職業、被疑者の前科について以下のような特徴が見られた。

ア　犯行時の職業について

犯行時の職業について「その他の専門・技術職」に該当する被疑者の割合は、刑法犯では0.8%であるのに対し、ネットワーク利用犯罪では3.1%、不正アクセス行為の禁止等に関する法律（以下「不正アクセス禁止法」という。）違反では6.9%となっている。このように、刑法犯全体に比べてサイバー犯罪において専門的な知識を持つ者による犯行の割合が多く、ネットワーク利用犯罪に比べて不正アクセス禁止法違反において専門的な知識を持つ者による犯行の割合が高いことがうかがわれる。

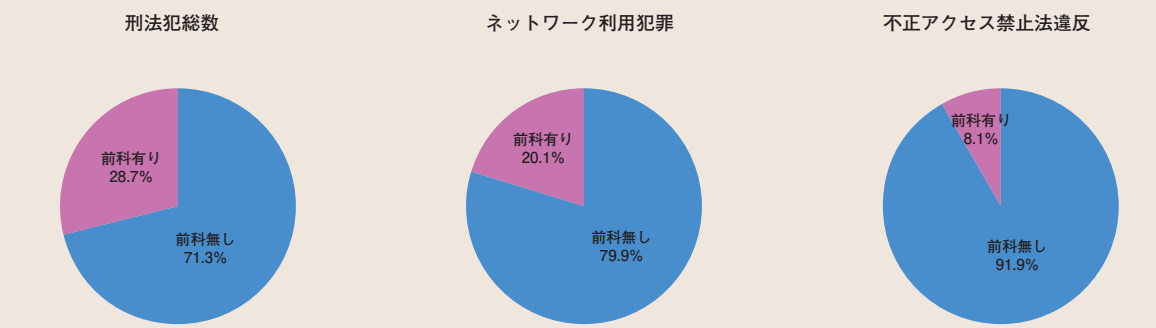
図-3　犯行時における被疑者の職業について（平成21年）



イ　前科について

犯行時に前科を有している被疑者の割合は、刑法犯全体では28.7%であるのに対し、ネットワーク利用犯罪では20.1%、不正アクセス禁止法違反では8.1%と、サイバー犯罪においては前科のない者が犯罪を敢行している割合が高くなっている。

図-4　犯行時における被疑者の前科の有無、同一罪種前科の有無について（平成21年）

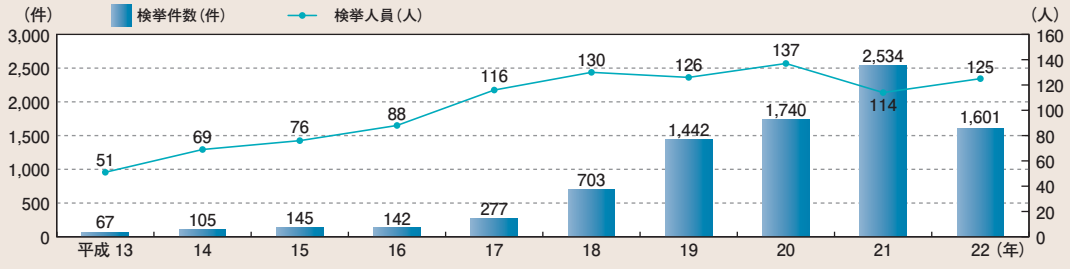


③　不正アクセス禁止法違反

ア　不正アクセス禁止法違反の検挙件数

22年中の不正アクセス禁止法違反の検挙件数は1,601件と前年より933件(36.8%)減少した。しかし、これは21年中に１事件で1,925件検挙という大規模なフィッシングによる不正アクセス事件を検挙したことが要因であり、この10年間をみると、検挙件数は急激に増加している。また、22年中の検挙人員については125人と前年より11人(9.6%)増加しており、不正アクセス禁止法違反についての情勢は依然として深刻な状況にある。

図-5　不正アクセス禁止法違反の検挙件数の推移(平成13～22年)



イ　不正アクセス行為に係る識別符号の入手方法、不正アクセス行為の動機

不正アクセス行為に係る識別符号の入手方法については、フィッシング(注)により他人の識別符号(ID・パスワード等)を大量に入手するものが21年は約８割、22年は約９割と大多数を占めている。しかし、他人の識別符号を知り得る立場にあった者による不正アクセス行為や、推測した識別符号を使用した不正アクセス行為も依然として発生している。

また、不正アクセス行為の動機については、不正アクセス禁止法の施行当初は、不正アクセス行為により好奇心を満たそうとしたものが多かったが、現在は、サイバー空間における各種サービスを悪用して金銭を得たり、商品をだまし取るなど不正に経済的利益を得ることを動機とする不正アクセス行為が大多数を占めている状況にある。

表-1　不正アクセス行為に係る識別符号の入手方法の内訳(平成18～22年)

区分＼年次	18	19	20	21	22
フィッシングにより入手(件)	220	1,157	88	2,084	1,411
識別符号を推測	178	139	1,368	58	70
知り得る立場にあった	49	39	163	61	57
スパイウェア等を使用	197	55	48	8	14
共犯者等から入手	0	3	7	167	12
聞き出した、のぞき見た	20	31	26	12	12
他人から購入	12	7	24	92	4
ファイル交換ソフト等で流出	19	2	6	0	0
その他	3	5	6	47	17

表-2　不正アクセス行為の動機の内訳(平成18～22年)

区分＼年次	18	19	20	21	22
不正に経済的利益を得るため(件)	419	1,186	1,498	2,245	1,455
嫌がらせや仕返しのため	31	62	52	34	66
好奇心を満たすため	26	55	17	165	33
オンラインゲーム上の不正操作	211	133	120	63	19
情報を不正に入手するため	10	0	12	19	18
料金の請求を免れるため	1	2	3	4	4
その他	0	0	35	2	3

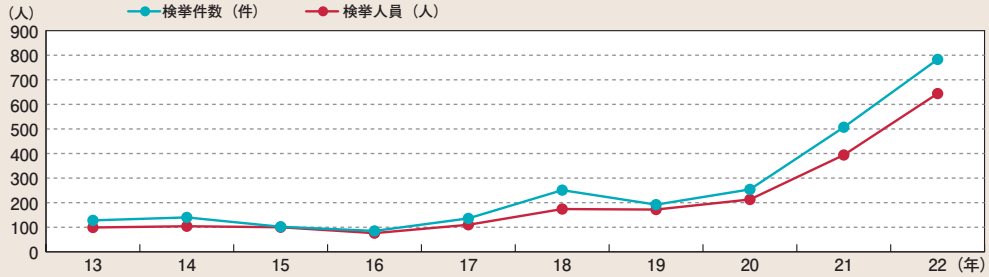
注：フィッシングとは、銀行等の実在する企業を装って電子メールを送り、その企業のウェブサイトに見せかけて作成した偽のウェブサイト(フィッシングサイト)を受信者が閲覧するよう誘導し、そこに当該サイトでクレジットカード番号、識別符号を入力させて金融情報や個人情報を不正に入手する行為をいう。

④　ネットワーク利用犯罪

ア　インターネットを利用した児童ポルノ事犯

22年中のインターネットを利用した児童ポルノ事犯の検挙件数は、783件と前年より276件（54.4％）増加、検挙人員については、644人で前年より250人（63.5％）増加し、過去最多となった。

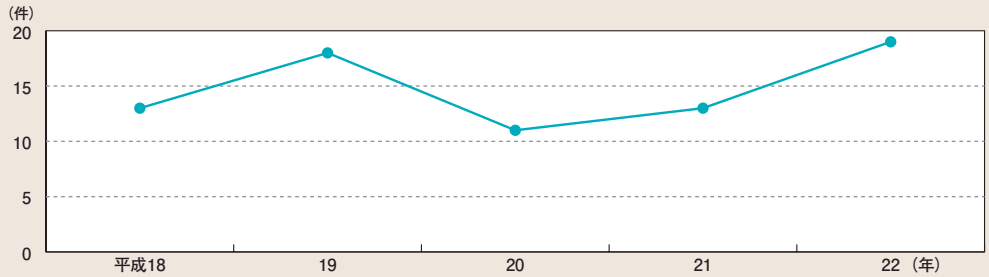
図-6　インターネットを利用した児童ポルノ事犯に係る検挙件数及び検挙人員（平成13～22年）



イ　インターネットを利用した薬物密売事犯

22年中のインターネットを利用した薬物密売事犯(注1)の検挙事件数(注2)は、19事件と、前年より６事件増加しており、違法な薬物密売事犯は後を絶たない状況にある。

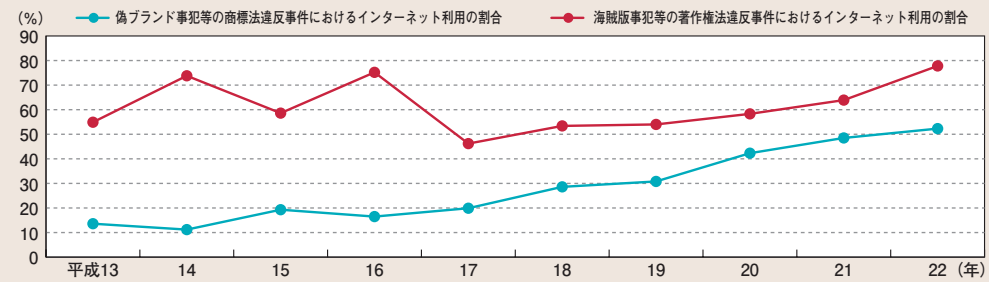
図-7　インターネットを利用した薬物密売事犯の検挙事件数の推移（平成18～22年）



ウ　インターネットを利用した知的財産権侵害事犯

22年中の知的財産権侵害事犯において、偽ブランド事犯等の商標法違反の検挙事件数のうちインターネットを利用したものの割合は52.3％であり17年以降上昇している。また、海賊版事犯等の著作権法違反の検挙事件数のうちインターネットを利用したものの割合は77.8％であり、18年以降上昇している。

図-8　インターネットを利用した知的財産権侵害事犯の割合の推移（平成13～22年）

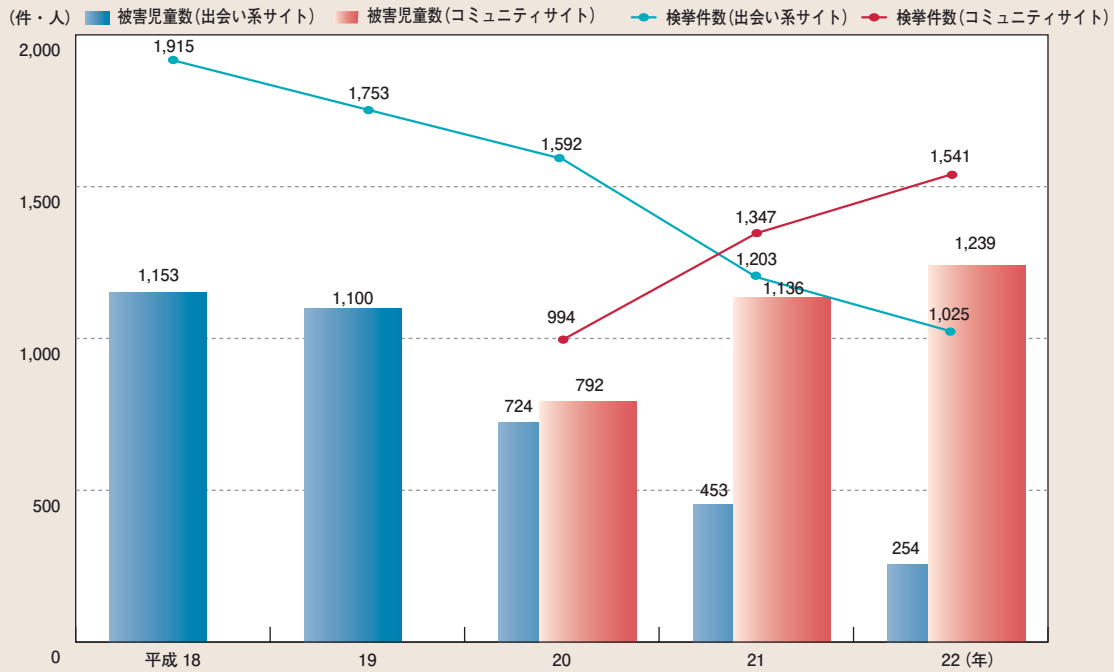


注１：広告違反、あおり・唆しを含む。
　２：同一の被疑者で関連の余罪がある場合でも、一つの事件として計上した統計

エ　コミュニティサイト等の利用に起因する事犯

22年中の出会い系サイト(注1)の利用に起因する事件の検挙件数は1,025件と、前年より178件(14.8%)減少し、19年から４年連続して減少する一方、コミュニティサイト(注2)の利用に起因して児童(18歳未満の者をいう。以下同じ。)が被害に遭った一定の事件(注3)として警察庁に報告のあった検挙件数は1,541件であり、前年より194件(14.4%)増加した。

図-9　出会い系サイト及びコミュニティサイトの利用に起因する検挙件数及び児童被害の推移(平成18～22年)



また、22年中に出会い系サイトの利用に起因する犯罪の被害に遭った児童は254人と、前年より199人(43.9%)減少する一方、コミュニティサイトの利用に起因する犯罪の被害に遭った児童は1,239人と、前年より103人(9.1%)増加した。

被害児童数について罪種別でみると、出会い系サイトの利用に起因する犯罪の被害に遭った児童については、児童買春の被害児童が151人(59.4%)と最も多く、コミュニティサイトの利用に起因する犯罪の被害に遭った児童については、いわゆる青少年保護育成条例違反(みだらな性行為等違反等)の被害児童が772人(62.3%)と最も多くなっている。

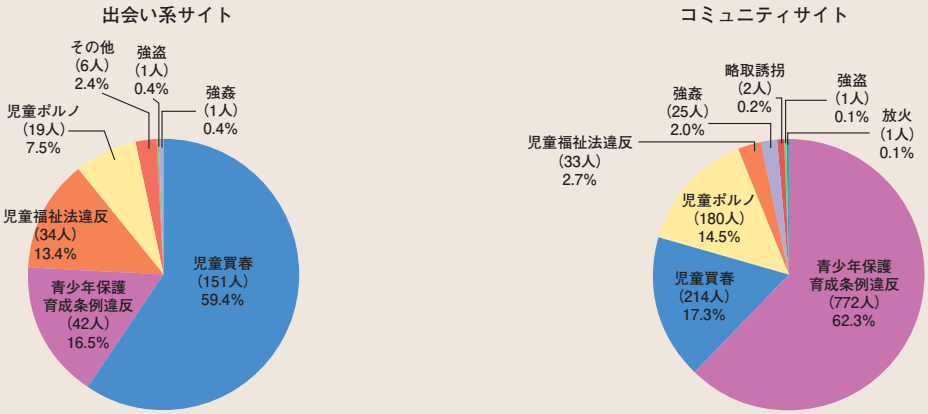
注１：面識のない異性との交際(以下「異性交際」という。)を希望する者(以下「異性交際希望者」という。)の求めに応じ、その異性交際に関する情報をインターネットを利用して公衆が閲覧することができる状態に置いてこれに伝達し、かつ、当該情報の伝達を受けた異性交際希望者が電子メールその他の電気通信を利用して当該情報に係る異性交際希望者と相互に連絡することができるようにする役務を提供するウェブサイト

２：SNS、プロフィールサイト等、ウェブサイト内で多人数とコミュニケーションがとれるウェブサイトのうち、出会い系サイトを除いたものの総称をいう。

３：児童買春、児童ポルノに係る行為等の処罰及び児童の保護等に関する法律(以下「児童買春・児童ポルノ法」という。)違反、児童福祉法違反、青少年保護育成条例違反及び重要犯罪(殺人、強盗、放火、強姦、略取誘拐・人身売買及び強制わいせつ)に係る事件

年齢別でみると、14歳以下の被害児童数については、出会い系サイトの利用に起因する犯罪の被害に遭った児童は50人（19.7％）であるのに対し、コミュニティサイトの利用に起因する犯罪の被害に遭った児童は362人（29.3％）となっており、コミュニティサイトの利用に起因する被害児童の低年齢化が顕著である。

図−10　出会い系サイト及びコミュニティサイトの利用に起因する事件(注)の被害に遭った児童の罪種別被害状況（平成22年）



図−11　出会い系サイト及びコミュニティサイトの利用に起因する事件の被害に遭った児童の年齢別被害状況（平成22年）

注：出会い系サイトの利用に起因する事件として警察庁に報告のあったもの及びコミュニティサイトの利用に起因して児童が被害に遭った一定の事件として警察庁に報告のあったもの

(2)違法情報・有害情報や相談受理の状況

① インターネット上の違法情報・有害情報

インターネット・ホットラインセンター(35頁参照)に通報される情報のうち、違法情報・有害情報(注)に該当するとされた件数は増加の一途をたどっており、平成22年中は4万4,683件と、前年より1万715件増加している。また、22年中の違法情報の内訳は、わいせつ物公然陳列に関する情報が56.7%とその多数を占めている状況にある。

図-12 違法情報・有害情報該当件数の推移(平成18~22年)

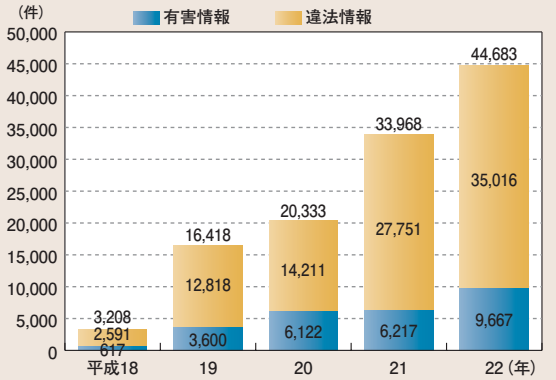
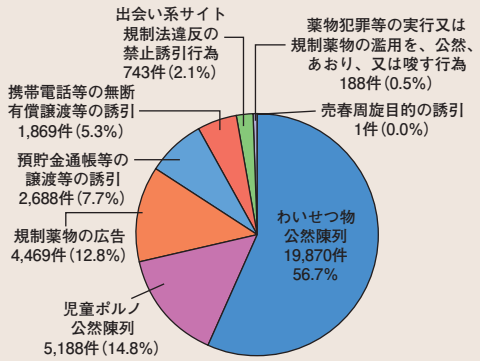


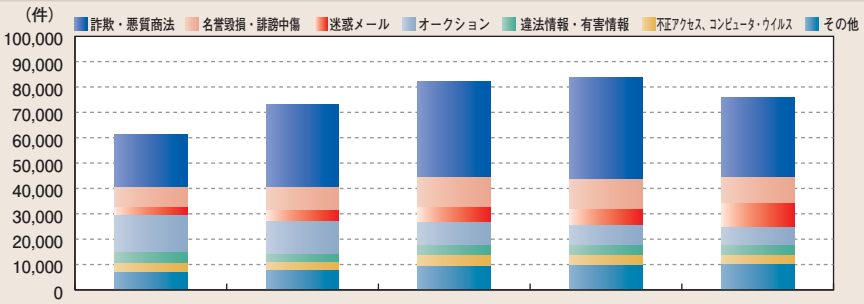
図-13 違法情報の内訳(平成22年)



② サイバー犯罪等に関する相談受理状況

22年中の都道府県警察におけるサイバー犯罪等に関する相談の受理件数は7万5,810件と前年より7,929件(9.5%)減少したが、依然として高い水準にある。

図-14 サイバー犯罪等に関する相談受理件数の推移(平成18~22年)



区分＼年次	18	19	20	21	22
合計(件)	61,467	73,193	81,994	83,739	75,810
詐欺・悪質商法	21,020	32,824	37,794	40,315	31,333
名誉毀損・誹謗中傷	8,037	8,871	11,516	11,557	10,212
迷惑メール	2,930	4,645	6,038	6,538	9,836
オークション	14,905	12,707	8,990	7,859	6,905
違法情報・有害情報	4,335	3,497	4,039	3,785	3,847
不正アクセス、コンピュータ・ウイルス	3,323	3,005	4,522	4,183	3,668
その他	6,917	7,644	9,095	9,502	10,009

注:違法情報とは、児童ポルノ画像、わいせつ画像、覚せい剤等規制薬物の販売に関する情報等、インターネット上に掲載すること自体が違法となる情報をいう。有害情報とは、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観点から放置することのできない情報をいう。

(３)サイバー空間をめぐる捜査環境

(１)及び(２)でみたとおり、サイバー犯罪はますます深刻さを増しており、警察では様々な事案に対応している。しかしながら、サイバー空間は、①匿名性が高く、痕跡が残りにくい、②地理的・時間的制約を受けることが少なく、短期間のうちに不特定多数の者に影響を及ぼしやすいといった特性を有していることから、サイバー犯罪の被害拡大の防止、被害の未然防止を図ることが困難である場合もあり、サイバー空間をめぐる捜査環境は厳しい状況にある。

①　匿名性が高く、痕跡が残りにくい

サイバー空間では、相手方の顔や声を認識することはできず、筆跡、指紋等の物理的な痕跡も残らない上、相手方が本人かどうかの確認は、専ら識別符号によって行われる。このような特性に着目し、正規の利用者の識別符号を盗用するなどの不正アクセス行為により、正規の利用者になりすましてサイバー犯罪を実行する以下のような事例が発生している。

事例１ Case

インターネットカフェのアルバイト店員の男(25)は、平成20年１月、客用のコンピュータに仕掛けておいたキーロガー(注)により、客が入力したインターネットバンキングに係る識別符号を不正に入手し、インターネットバンキングに対する不正アクセス行為を行い、客の口座から自らが管理する電子マネーカードに不正にチャージするなどし、財産上不法の利益を得た。同年３月、不正アクセス禁止法違反(不正アクセス行為)、電子計算機使用詐欺罪等で検挙した(千葉)。

サイバー犯罪の捜査では、犯罪に使用されたコンピュータを特定するとともに、そのコンピュータを誰が使用したのかを明らかにすることが必要である。しかしながら、本人確認を行っていないインターネットカフェやセキュリティ対策が不十分である無線 LAN を利用するなどして敢行されたサイバー犯罪については、被疑者の特定は非常に困難である。

事例２ Case

会社員の男(33)らは、21年４月から22年１月までの間、他人名義で契約したデータ通信カードを使用してフィッシングサイトを構築し、本人確認を行わないインターネットカフェから当該フィシングサイトへのアクセスを誘導する電子メールを送信して、当該サイトにアクセスした者にクレジットカード番号やインターネット上のクレジットカード決済時に必要となる本人認証用の識別符号を不正に入力させ、インターネットショッピングサイトにこれを入力して不正アクセスを行い商品をだまし取った。22年１月、５人を詐欺罪で逮捕するとともに、そのうち３人を同年７月、不正アクセス禁止法違反(不正アクセス行為)で検挙した(静岡、熊本)。

事例３ Case

デザイナーの男(29)らは、ウェブサイトでモデル募集と称して男子児童を集め、わいせつな姿態をとらせた上、その様子を撮影して児童ポルノを製造し、これを販売した。男らは、他人の無線 LAN を無断で使用してウェブサイトに児童ポルノをアップロードしていた。22年２月から同年10月にかけて、デザイナーの男に児童ポルノ画像を提供した会社員の男(47)ら２人を含め、合計６人を児童買春・児童ポルノ法違反(児童ポルノ提供等)等で逮捕した(埼玉、警視庁、兵庫)。

注：コンピュータのキーボードでどの文字が入力されたかを記録するプログラムをいう。

② 地理的・時間的制約を受けることが少なく、短時間のうちに不特定多数の者に影響を及ぼしやすい

サイバー空間では地理的・時間的な制約を受けることが少ないため、不特定多数の者に対して瞬時に情報を発信することができるなど、短時間のうちに不特定多数の者に影響を及ぼしやすいものであり、こういった特性は、サイバー空間の利用者にとって、大きな便益がもたらされるものである。

その一方で、一たびサイバー空間で犯罪が敢行された場合、その被害は全国に拡大し、捜査を困難にするといった側面を持つものである。具体的には、インターネット・オークション詐欺の被害者が全国的に所在していたりウェブサーバが外国に所在していたりすることなどにより、サイバー犯罪の捜査においては、犯罪の実行地、証拠の所在地、被害発生地等の間に地理的関連性が希薄な場合があり、被害の全貌を把握することが困難となっている。さらに、それらが判明した場合でも、外国を含む広大な地域において捜査を展開していかなければならないことが多く、捜査が困難となっている。

事例4 Case

会社役員の男(20)らは、21年11月、アダルトゲームの実行ファイルに偽装したコンピュータ・ウイルスをファイル共有ソフト上に公開した。当該ウイルスは、これをインストールしたコンピュータのデスクトップ画面やインストール時に入力する個人情報を遠隔地のウェブサーバに自動送信するものであり、当該コンピュータの設定情報やインストール時に入力された個人情報をウェブサイトに掲載した上、あたかもゲームソフトについて著作権を有するかのように装って被害者らを欺き、著作権侵害の和解金名下に２万3,400円をだまし取った。22年５月、２人を詐欺罪で逮捕した(警視庁)。

事例5 Case

無職の男(32)は、22年５月、米国所在の事業者が運営している簡易投稿サイトに、「きょうで死にます　ゆるさない　確実にころします」などと交際していた女性の殺害予告を書き込んだ。日本所在の当該事業者の関連事業者を通して通信記録を入手して被疑者を特定し、同月、脅迫罪で逮捕した(警視庁)。

事例6 Case

無登録貸金業者(30)らは、19年３月頃から20年２月頃にかけて、インターネット上に登録業者を仮装して広告を掲載するなどの方法により融資を勧誘し、全国47都道府県にわたって約2,600人に総額約１億2,000万円を貸し付け、法定金利の約56倍から約102倍の利息を他人名義の口座に振り込ませ受領するなどした。20年５月までに、貸金業法違反(無登録)、出資の受入れ、預り金及び金利等の取締りに関する法律(以下「出資法」という。)違反(超高金利等)、組織的な犯罪の処罰及び犯罪収益の規制等に関する法律(以下「組織的犯罪処罰法」という。)違反(犯罪収益等隠匿)等で10人を逮捕した(富山)。

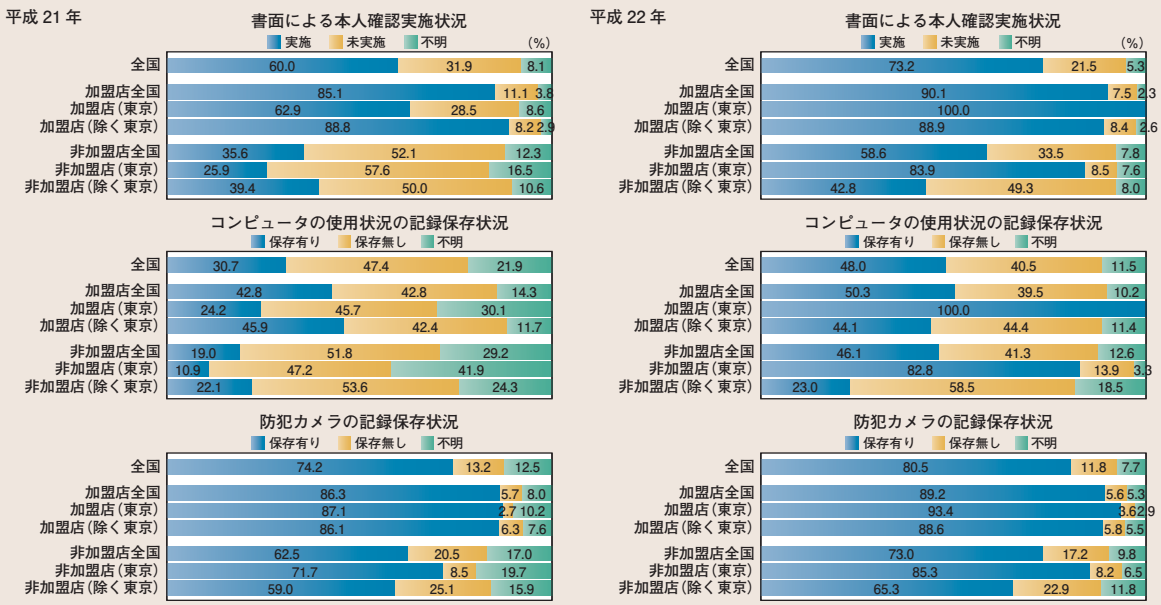
(4)インターネットカフェの現状

匿名性の高さ及び痕跡の残りにくさを利用したサイバー犯罪の事例の一つとしてインターネットカフェを利用したものを取り上げたが、インターネットカフェにおいては、事業者が利用者の本人確認を行い、その使用状況を記録していなければ、犯行に利用されたコンピュータを特定することができたとしても、これを利用していた者を特定することは困難である。

警察庁では、平成20年からインターネットカフェの実態について調査を行っているところ、22年の調査結果を21年の調査結果と比較すると、全国のインターネットカフェにおける本人確認の実施率は大きく向上した。この要因の一つとして、東京都においてインターネット端末利用営業の規制に関する条例が制定されたことがあると思われる。

しかしながら、東京都以外の道府県においては、日本複合カフェ協会(注)に加盟していない店舗における書面による本人確認の実施率は半数にとどまっており、さらにこうした店舗ではコンピュータの使用状況の記録保存や防犯カメラの記録保存もあまり行われていない状況が見受けられる。

図-15　インターネットカフェについての調査結果(平成21、22年)



注１：平成21年調査時におけるインターネットカフェ店舗数は2,648店、22年調査時におけるインターネットカフェ店舗数は2,669店
２：加盟店とは日本複合カフェ協会に加盟している店舗、非加盟店とは当該協会に加盟していない店舗をいう。
なお、非加盟店には、調査時において協会への加盟の有無が不明であった店舗を含む。

コラム　①「インターネット端末利用営業の規制に関する条例」(東京都)

東京都では、インターネットカフェ等におけるサイバー犯罪の防止及びその他各種犯罪の発生を防止することを目的として、事業者が店舗を設けてインターネットカフェ等を営もうとする際には東京都公安委員会への営業に関する届出義務を課すとともに、インターネットカフェ等の営業者に対し、運転免許証等の本人確認書類による利用者の本人確認を義務付けること等の規制を行うインターネット端末利用営業の規制に関する条例を制定し、22年７月１日に施行された。

注：平成13年７月に設立されたインターネットカフェ及び漫画喫茶等の業界における唯一の事業者団体であり、業界の健全発展等を図るため、運営ガイドラインを策定し、これに従った店舗運営を加盟店舗に推奨している。

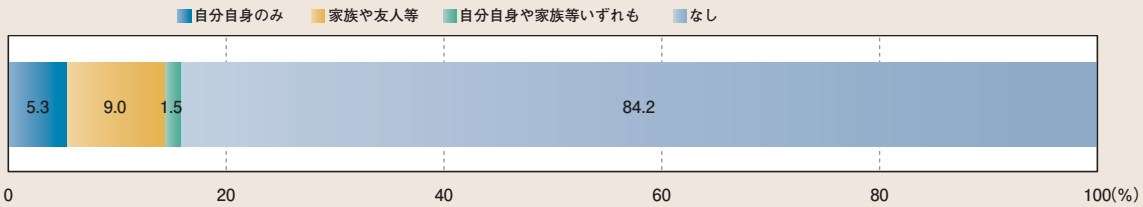
2 サイバー空間に対する国民・事業者の意識

(1)サイバー空間に対する国民の意識

警察庁では、平成23年１月、都道府県警察を通じて、インターネット利用に関する意識調査(注)を行った。

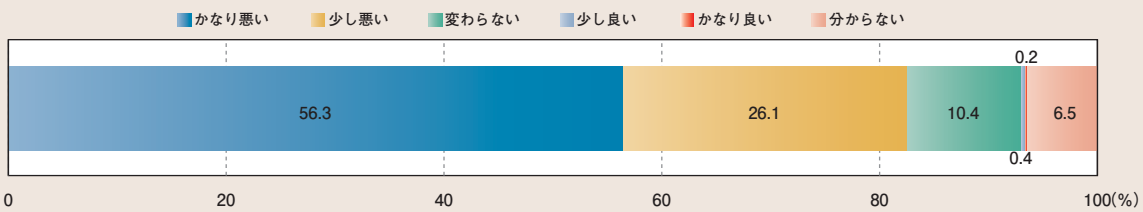
インターネットを利用した犯罪やトラブルに巻き込まれた経験があるか質問したところ、15.8%の者が「自分自身のみ巻き込まれた経験が有る」、「家族や友人等が巻き込まれた経験が有る」、「自分自身や家族等が巻き込まれた経験が有る」と回答している。

図-16 サイバー犯罪やトラブルに巻き込まれた経験の有無



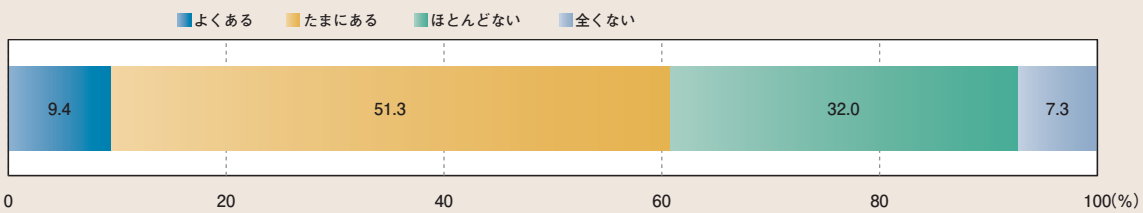
インターネット上のモラルやマナーは、現実社会でのモラルやマナーと比較してどう思うかについて質問したところ、82.4%の者が「かなり悪い」又は「少し悪い」と回答しており、国民においても、サイバー空間におけるインターネット利用者の規範意識の低下について認識していることがうかがわれる。

図-17 サイバー空間におけるモラルやマナーの現実社会との比較



また、日頃、インターネットを利用した犯罪の被害に遭いそうで不安に感じることはあるかについて質問したところ、60.7%の者が「よくある」又は「たまにある」と回答しており、国民がサイバー空間における安全性が十分に確保されていないと考えていることがうかがわれる。

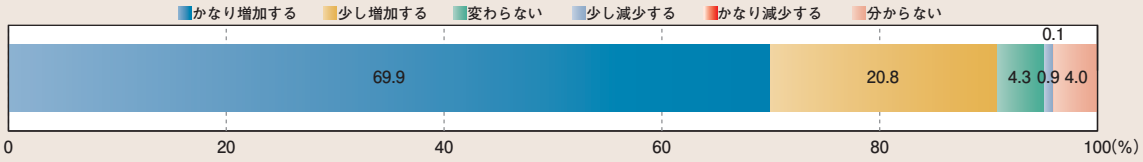
図-18 サイバー犯罪の被害に遭う不安



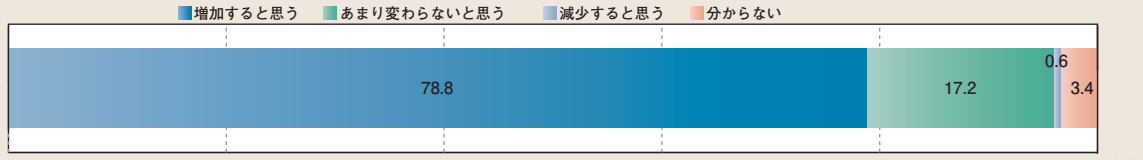
注：全国の運転免許試験場等において、運転免許証の更新に訪れた方5,120人を対象に、警察庁において作成した質問票を配付し回答を求める形式で実施（有効回答数4,294人のうち、インターネットを利用しないと回答した853人を除く3,441人について分析）

今後、インターネットを利用した犯罪が増加すると思うかについて質問したところ、90.7％の者が、「かなり増加する・少し増加する」と回答している。18年３月に実施した意識調査(注)では、同様の問いに対し78.8％の者が「増加すると思う」と回答しており、今回の調査結果は、当時の調査結果を上回っており、国民が、サイバー犯罪の情勢の更なる悪化を認識していることがうかがわれる。

図−19　サイバー犯罪の今後の情勢（平成23年）

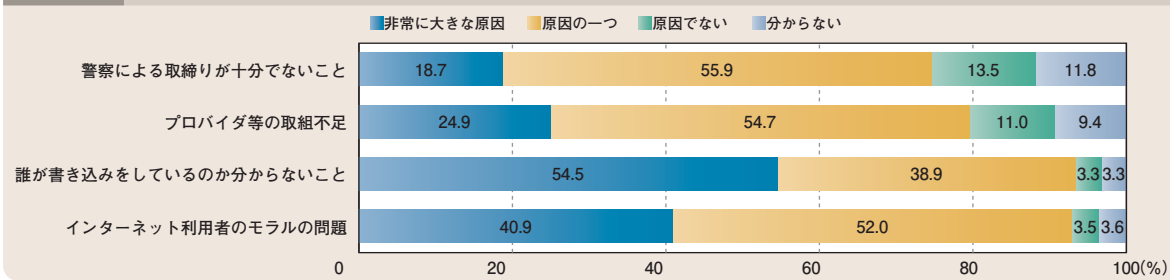


図−20　サイバー犯罪の今後の情勢（平成18年）



一方、インターネット上に違法情報・有害情報が氾濫している原因について質問したところ、「非常に大きな原因となっているもの」として、54.5％の者が「誰が書き込みしているのか分からないこと」と、40.9％の者が「インターネット利用者のモラルやマナーの問題」と回答しており、国民が、規範意識の低さの要因として匿名性の高さを認識していることがうかがわれる。

図−21　サイバー空間に違法情報・有害情報が氾濫している原因



このように、多くの国民が、インターネットを利用した犯罪の増加を懸念しているところ、その要因としては、インターネット利用者のモラルの欠如やサイバー空間における匿名性にあると考えているとうかがわれる。

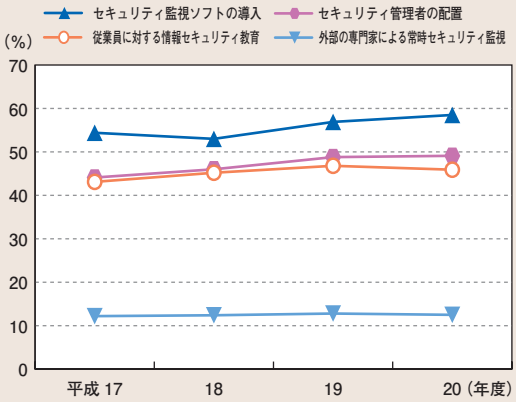
注：全国のインターネット利用者1,000名を対象に、調査を委託した民間事業者のウェブサイト上に警察庁において作成した質問票を掲示して回答を求める形式で実施

(2)サイバー空間に対する事業者の意識

警察庁では、サイバー空間に対する事業者の意識について、警察庁において民間事業者に対して実施した情報セキュリティに関する意識調査(注1)、ヒアリング(注2)及び経済産業省が実施した情報処理実態調査(注3)を基に分析した。

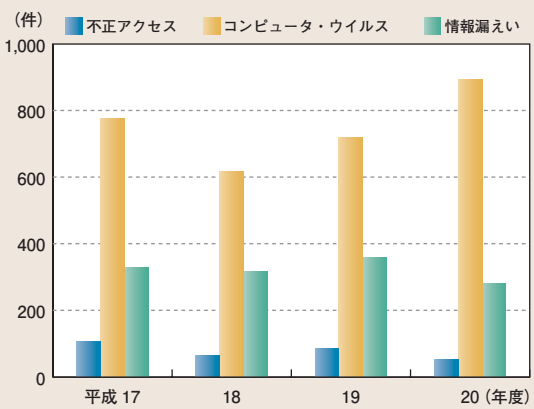
経済産業省の情報処理実態調査によると、企業における情報セキュリティに関する諸対策は、セキュリティ監視ソフトの導入、情報セキュリティ管理者の配置、従業員に対する情報セキュリティ教育が、それぞれ約半数の企業において行われており、わずかながらではあるが、対策を講じる企業の割合は増加傾向にある。その一方で、情報漏えいを始めとする事故は依然として多く、特にコンピュータ・ウイルスによる被害は近年再び増加している。

図-22 企業における情報セキュリティに関する対策状況(平成17~20年度)



注:経済産業省が実施した情報処理実態調査による。

図-23 情報セキュリティに関する事故発生状況(平成17~20年度)



注:経済産業省が実施した情報処理実態調査による。

警察庁が実施したヒアリングでは、経営者層の情報セキュリティ対策への理解が不十分であったり、対策をどこまで実施すればその効果が得られるか不明確であることから、なかなか対策が進まない傾向があるといった意見や、資金的に余裕のない事業者においては情報セキュリティ対策にまで手が回っていないのではないかといった意見があった。

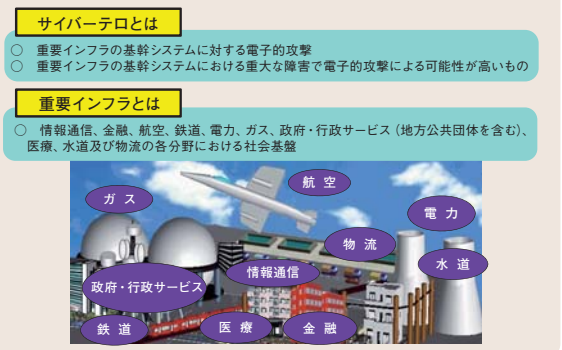
その一方で、警察庁が実施した意識調査では、情報漏えい事案の防止について、77.3%がコンピュータの廃棄に当たってデータを確実に消去している、78.1%がアクセス権を設定していると回答するなど対策が進展している企業もみられた。これは、当該事案が発生すると企業のイメージダウンにつながるため、経営者層の関心が高いことが一つの要因であると考えられ、経営者層の理解や費用負担の軽減が進んだ際には、情報セキュリティ対策を行う企業がさらに増加するものと予測される。

注1:全国の企業、教育機関、医療機関、行政機関から、特定の業種、地域に偏りのないよう無作為に抽出した3,000件に対し、警察庁において作成した質問票を送付し回答を求める方法で実施(送付した3,000件のうち、回答のあった841件について分析)。当該意識調査は平成12年から毎年実施している。
2:平成22年10月から12月にかけて、セキュリティ関連事業者、コンテンツ事業者、電気通信事業者等の20社及び1団体を対象に実施
3:IT産業の競争力強化に加え、ITの戦略的活用による経済・産業・社会の再生に向けた政策を適切に進めていく上で、情報処理の実態や影響等を正確に把握・分析するために昭和44年から実施している調査

3 サイバーテロに関する情勢

高度情報通信ネットワークが発達した現代社会では、重要インフラの基幹システムに対してサイバー攻撃が実行された場合、国民生活や社会経済活動に甚大な支障が生じるおそれがある。サイバー攻撃は、コンピュータとネットワークへのアクセスが確保できれば、時と場所を選ばず実行が可能であるという特徴がある。こうした中、以下のような事例が発生しており、サイバーテロの脅威はますます現実のものとなっている。

図−24 サイバーテロと重要インフラ



事例 1 Case

平成22年９月、中国のハッカー集団である「中国紅客（こうきゃく）連盟（れんめい）」と称する者が、尖閣諸島の中国領有権を主張する民間団体のウェブサイト上で、我が国の政府機関等に対してサイバー攻撃を行うよう呼び掛け、警察庁のウェブサイトに対してこれに関連したとみられるアクセスが集中し、閲覧困難な状態となった。

事例 2 Case

22年９月、イラン国営通信等は、同国の原子力発電所等のコンピュータ約３万台が、電力、ガス等の産業用システムを標的とする「スタックスネット」と呼ばれるコンピュータ・ウイルスに感染した旨報じた。我が国では、産業用システムにおける被害は確認されていないが、複数のコンピュータが感染したとみられる。

事例 3 Case

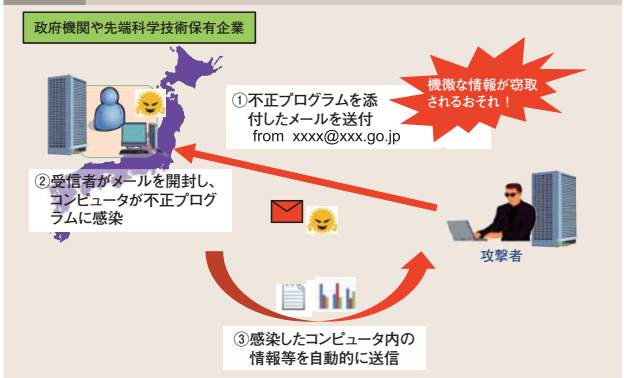
21年から22年にかけ、鉄道事業者等のウェブサイトが改ざんされ、ウェブサイト利用者のコンピュータがガンブラー・ウイルスに感染する事案が発生した。

コラム ❷サイバーインテリジェンスの脅威

政府機関や民間企業において、情報を電子データとして保存することが一般的となっているところ、近年、これらの機関等に対する標的型メール攻撃が発生しており、サイバー空間における諜報活動であるサイバーインテリジェンスの脅威も現実のものとなっている。

サイバーインテリジェンスにより機密情報が窃取されると、我が国の治安、外交や安全保障に重大な影響が生じるおそれがある。また、重要インフラの基幹システムの設計やぜい弱性に関する情報が窃取された場合、それらを悪用して、サイバーテロが実行されるおそれもある。警察では、こうした活動の実態解明に努めるとともに、違法行為に対しては厳正な取締りを行うこととしている。

図−25 不正プログラム添付メールを利用したサイバーインテリジェンス



第2節 サイバー犯罪に対する取組

1 サイバー犯罪対策に係る体制整備等

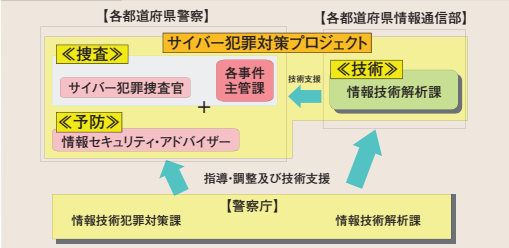
(1)対策全般

警察では、サイバー犯罪に適切に対応するため、体制整備による取締りの徹底や広報啓発活動や相談対応等によるサイバー犯罪の未然防止を推進している。

① 体制整備

地理的・時間的制約を受けることなく、短時間のうちに不特定多数の者に影響を及ぼしやすい特性を有するサイバー空間については、関係都道府県警察が捜査の重複を避けつつ、連携して対処する必要がある。

図-26 サイバー犯罪対策のための体制



注1：サイバー犯罪捜査官とは、民間企業等において専門的知識、能力を取得し、サイバー犯罪の捜査に要求される捜査技能の取得に必要な資質を有する警察職員をいう。
2：情報セキュリティ・アドバイザーとは、国民からのサイバー犯罪等に関する相談への対応、地方公共団体、学校、民間企業等に対する情報セキュリティに関する広報啓発及びサイバー犯罪対策に関する産業界との連携等サイバー犯罪の予防に資する施策の推進に従事する者をいう。

このため、警察では、平成16年、警察庁に情報技術犯罪対策課を設置するとともに、都道府県警察及び都道府県情報通信部にサイバー犯罪対策に関する知識及び技能を有する捜査員等により構成されるサイバー犯罪対策プロジェクトを設置した。この体制において、警察庁では、都道府県警察が行うサイバー犯罪捜査に関する指導・調整を行っているほか、捜査員の能力向上のための研修、産業界や外国関係機関等との連携を推進している。

また、23年度予算において地方警察官350人を増員するとともに、「全国協働捜査方式」(36頁参照)を導入するなど、サイバー犯罪の取締り体制を強化している。

さらに、技術面に関して、警察では、解析用資機材の増強・整備を行っているほか、関係機関と連携し技術情報の収集・分析を推進するとともに、民間企業でシステム・エンジニアとして勤務していた者等をサイバー犯罪捜査官として採用するなどにより、最新の技術や機器等を利用して敢行されるサイバー犯罪に対応している。

② 広報啓発活動及び相談対応

情報セキュリティ対策DVD

警察では、情報セキュリティに関する国民の知識やサイバー空間における規範意識の向上を図るため、警察やプロバイダ連絡協議会(注1)等が主催する研修会、学校関係者等からの依頼による講演会、情報通信技術関連イベント等の機会を利用して情報セキュリティ・アドバイザー等が講演等を行うほか、警察庁ウェブサイト(http://www.npa.go.jp/cyber/)、広報啓発用パンフレット、情報セキュリティ対策DVD(注2)等により、サイバー犯罪の手口やインターネット上の違法情報・有害情報の現状、対策等について周知を図っている。

また、サイバー犯罪に関する相談に的確に対応するため、都道府県警察では、サイバー犯罪相談窓口を設け、情報セキュリティ・アドバイザー等の専門職員によりサイバー犯罪に関する相談に対応している。

注1：都道府県警察ではプロバイダ、関係機関、消費者団体等で構成され、サイバー犯罪の情勢や手口、サイバー犯罪被害防止等に関する情報交換を行っているほか、講習会等の実施、一般向け広報資料の作成等を行っている。
2：ケーブルテレビでの放映、特定非営利活動法人 POLICE チャンネルのウェブサイト(http://www.police-ch.jp/)への掲載、警察署や図書館での貸出し等も行われている。

(２)違法情報・有害情報対策

①　インターネット・ホットラインセンターにおける取組

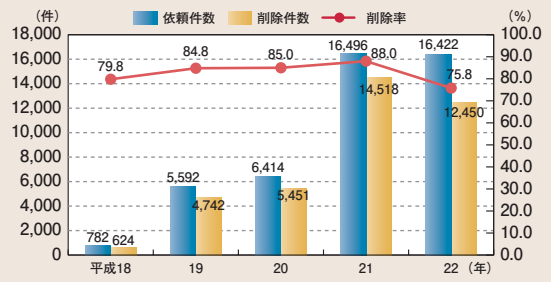
図−27　インターネット・ホットラインセンターの概況

警察庁では、一般のインターネット利用者からの違法情報・有害情報に関する通報を受理し、違法情報の警察への通報や国内のウェブサーバに蔵置された違法情報・有害情報に係るサイト管理者等への削除依頼を行うインターネット・ホットラインセンターの運用を平成18年６月から開始した。運用開始以降、同センターの取組が、被疑者の検挙や国内の違法情報・有害情報の削除に結び付くなど、その取組は一定の成果を上げている。同センターは、外国のウェブサーバに蔵置された違法情報についても、19年３月に各国のホットライン(注１)相互間の連絡組織として設置されたINHOPE(注２)へ加盟し、INHOPE加盟団体に対して削除に向けた措置を依頼するなど、INHOPE加盟団体との連携による取組を推進している。

また、社会における情勢の変化を受け、20年には硫化水素ガスの製造を誘引する情報が、21年には痴漢行為を誘引等する情報が、同センターにおいて受理する違法情報・有害情報の定義に追加された。

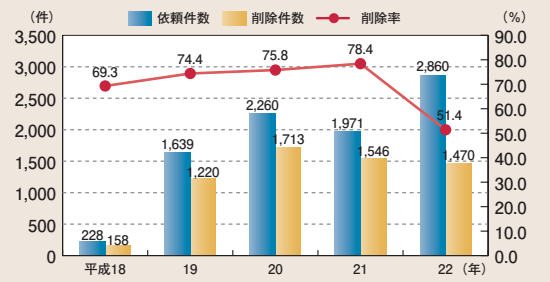
22年中においては、同センターがサイト管理者等に対して削除依頼を行った違法情報１万6,422件のうち１万2,450件、有害情報2,860件のうち1,470件が削除されており、違法情報の削除率は75.8％、有害情報の削除率は51.4％であった。違法情報については、3,972件(24.2％)が削除依頼を行ったにもかかわらず削除されておらず、これを放置することは、犯罪を放置するばかりか、新たな犯罪も引き起こしかねない危険なものである。このため、合理的な理由もなく違法情報の削除依頼に応じない悪質なサイト管理者の中には、犯罪を誘発している状況を作り出し、それを容認している者も少なくないことから、警察において積極的に捜査・検挙していく必要がある。また、有害情報については、これを端緒とした捜査活動を今後進めていく必要がある。

図−28　削除された違法情報の件数の推移(平成18〜22年)



注：平成18年は、運用開始の６月〜12月の件数

図−29　削除された有害情報の件数の推移(平成18〜22年)



注：平成18年は、運用を開始した６月以降の件数

注１：インターネット利用者からインターネット上の違法情報・有害情報等に関する通報を受理し、一定の基準により、それらの情報に係る違法情報・有害情報の該当性判断を行い、警察への通報やサイト管理者等への削除依頼等を行う仕組み
２：International Association of Internet Hotlines(旧名称は、Internet Hotline Providers in Europe Association)。平成11年に設立され、23年３月現在、39団体(34の国・地域)からなる国際組織

②　全国協働捜査方式の試行

インターネット・ホットラインセンターに通報される違法情報は、同センターによって警察に通報され、最終的には事件検挙に結び付いてはいるものの、発信地に関する情報が含まれていないことが多く、その通報だけでは直ちに発信元が判明しない場合が多いため、捜査を主体的に担当すべき都道府県警察が不明確となり、その結果捜査の競合等が発生し、効率的な捜査を行うことが困難となっていた。

このような問題に対処し、効率的な捜査を進めるため、22年10月から23年６月までの間、同センターから警察庁に対して通報された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「全国協働捜査方式」の試行を行った。

試行期間中における検挙状況は、23年５月10日現在、302件（前年同期比185件増加）であり、その内訳は、わいせつ情報による検挙が257件（前年同期比157件増加）、薬物関連情報による検挙が32件（前年同期比19件増加）、振り込め詐欺等関連情報による検挙が13件（前年同期比９件増加）と増加している。

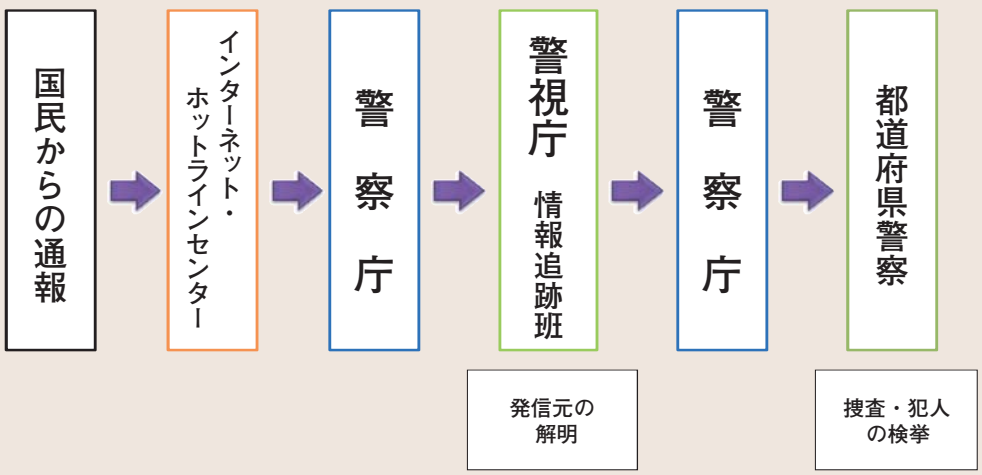
このように、検挙件数の増加が顕著にみられ、全国協働捜査方式での捜査が効果的であることが明らかになったことから、増員した350人の地方警察官などにより23年７月から本格実施を開始した。

コラム　❸「全国協働捜査方式」の具体的な流れについて

「全国協働捜査方式」は、匿名性と広域性を特徴とするサイバー犯罪に対処するために導入された全く新しい形態の捜査方式である。

インターネット・ホットラインセンターから警察庁に対して通報された違法情報のうち、発信元がどの都道府県にあるか推認できないものを警察庁から警視庁生活安全部サイバー犯罪対策課に設置されている情報追跡班に送付し、この情報追跡班で違法情報の発信元を割り出す捜査を行い、これによって発信元が判明した違法情報について、警察庁の調整により、発信元を管轄する都道府県警察がその後の捜査を行うものである。

図−30　全国協働捜査方式の流れ



２　不正アクセス禁止法違反への対策

不正アクセス禁止法違反の検挙件数は年々、増加傾向にあることから、警察では、各種教育訓練を通じた捜査力の強化を図るとともに、事業者に対しセキュリティ機能の強化について働き掛けを行うなどの被害の未然防止に取り組んでいる。

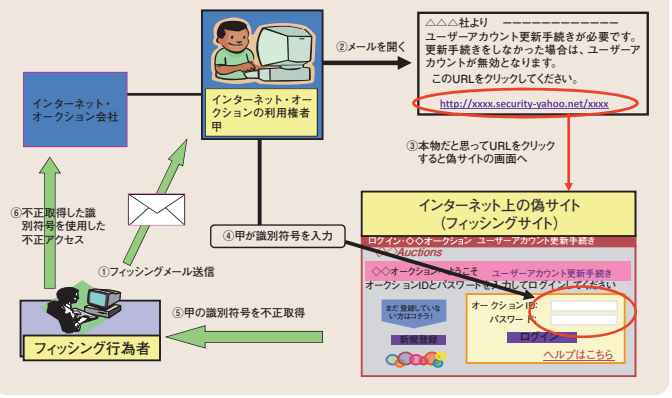
（１）取締りの強化

警察においては、不正アクセス禁止法違反に的確に対応するため、不正アクセス行為に係る識別符号の入手方法及び不正アクセス行為の手口についての把握や、警察官の能力向上により、取締りを強化している。

①　フィッシングに係る事案等の取締り

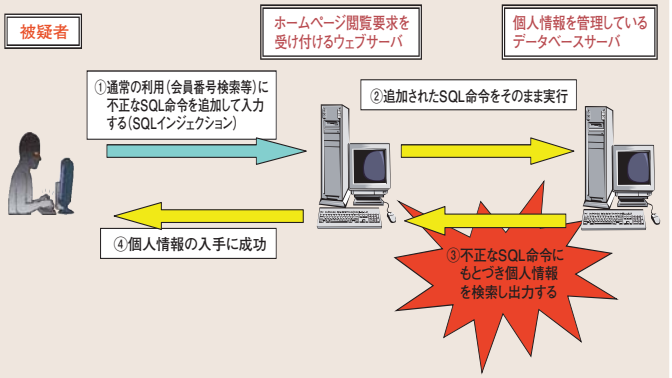
第１節でみたとおり、不正アクセス行為に用いる識別符号を取得する手口の大部分をフィッシングが占めている。警察では、平成16年に設置した「フィッシング110番」等を活用した情報収集により、フィッシングにより識別符号を入手して敢行した不正アクセス禁止法違反を早期に把握し、検挙することで被害の拡大防止に努めている。

図-31　フィッシングの概要



また、セキュリティ・ホール攻撃(注１)の一つであるSQLインジェクション攻撃(注２)による識別符号やクレジットカード情報等の大量流出も大きな問題となっている。警察では、このような手口による不正アクセス禁止法違反の取締りに努めているほか、不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況を毎年公表し、その中でセキュリティ・ホールの検知技術の研究開発状況を紹介することなどにより、不正アクセス行為に対する防御措置の重要性に関する国民の理解を深め、不正アクセス禁止法違反が行われにくい環境が構築されるよう努めている。

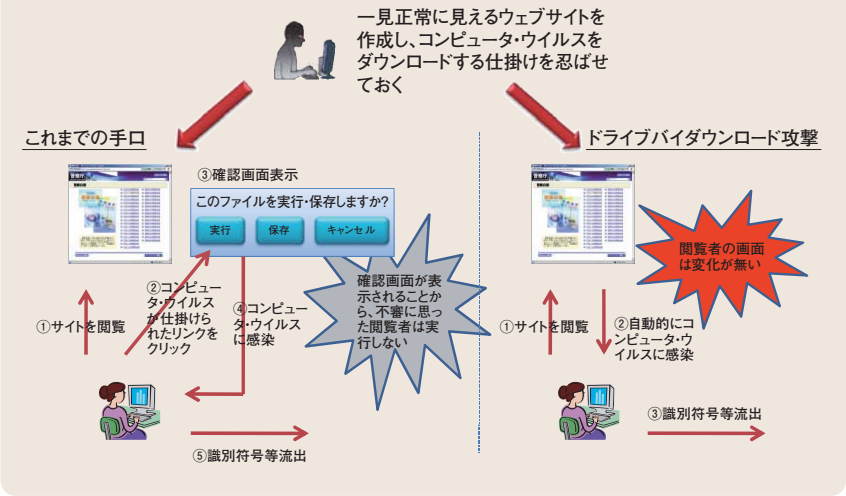
図-32　SQLインジェクション攻撃の概要



注１：セキュリティ・ホール攻撃とは、アクセス制御されているウェブサーバに、セキュリティのぜい弱性を突いて情報（他人の識別符号を入力する場合を除く。）や指令を入力して不正に利用する行為をいう。
２：SQLインジェクション攻撃とはSQL（Structured　Query　Language）というプログラム言語を用いて、企業等が管理するデータベースを外部から不正に操作する行為をいう。

②　ドライブバイダウンロード攻撃に対する対策

図-33　ドライブバイダウンロード攻撃の概要



ウェブサイトを閲覧しただけで、画面の変化もないままコンピュータ・ウイルス等に感染してしまうドライブバイダウンロード攻撃という手口が最近新たに出現しており、その攻撃を受けたコンピュータの利用者が全く気付かないうちに識別符号が流出してしまう可能性が生じている。21年末に猛威を振るったガンブラー・ウイルスは、この攻撃を利用することによりコンピュータにこのウイルスを感染させ、ウェブサイト管理用の識別符号を入手後、そのウェブサイトを改ざんするというものであった。これを受け、警察庁では、一般のインターネット利用者や企業等に対して適切なセキュリティ対策を講じるよう注意喚起をするとともに、ホームページの改ざんを認知した場合は都道府県警察のサイバー犯罪相談窓口に対する早期の通報と改ざんされたホームページのデータ、ログ等証拠の保全を呼び掛けている。

③　捜査能力の強化

不正アクセス禁止法違反に対する捜査能力を一層充実させるため、警察では、サイバー犯罪捜査に必要な知識・技術の向上に努めるとともに、教育訓練の実施等により、各捜査員が自らの捜査能力向上に必要な知識・技能を選択して修得できるようにするなど、人材育成の多様化・高度化の実現に向けた取組を行っている。

(2)事業者に対するセキュリティ機能強化に向けた働き掛け

第１節でみたとおり、不正アクセス行為の動機として「不正に金を得るため」が平成18年以降急増しているとともに、今もなお「オンラインゲーム上の不正操作」といった動機も見受けられ、インターネット・オークションやオンラインゲームの利用者等が金銭的な被害を被っていることから、警察庁から事業者等に対してセキュリティ機能強化に対する働き掛けを行っている。この働き掛けを踏まえ、ワンタイムパスワード(注１)等が一部の事業者で導入された。

また、不正アクセス行為に対する自発的な未然防止対策として、短い文字列や誕生日等の推測されやすい数字のみの文字列を識別符号とすることができないといった認証の強化、前回ログイン時刻の表示機能やログイン通知機能(注２)の導入等も事業者において行われている。

注１：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。
２：ログインが行われた時に、その旨をあらかじめ指定されたメールアドレスに通知する機能をいう。

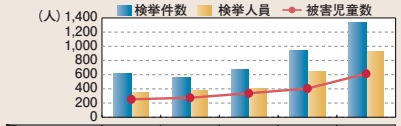
3 ネットワーク利用犯罪への対策

(1)インターネットを利用した児童ポルノ対策

① 児童ポルノの現状

近年、高画質画像の高速かつ大量な流通や、ファイル共有ソフトの利用拡大などにより、児童ポルノ情勢が深刻化している。平成22年中の児童ポルノ事犯の検挙件数は1,342件、検挙人員は926人、被害児童数は614人と、それぞれ前年より407件(43.5%)、276人(42.5%)、209人(51.6%)増加し、いずれも過去最多となった。このうち、ファイル共有ソフトを利用した児童ポルノ画像の交換、掲示板への児童ポルノ画像の掲載、販売サイトを利用した児童ポルノDVDの販売等のインターネットを利用した事件の検挙件数は783件で、全体の検挙件数の58.3%を占めている。

図-34 児童ポルノ事犯の検挙状況等の推移(平成18～22年)



区分＼年次	18	19	20	21	22
検挙件数(件)	616	567	676	935	1,342
うちインターネット利用	251	192	254	507	783
検挙人員(人)	350	377	412	650	926
うちインターネット利用	174	172	213	394	644
被害児童数(人)	253	275	338	405	614

② インターネットを利用した児童ポルノ事犯の取締り

警察では、21年６月に警察庁が策定した「児童ポルノの根絶に向けた重点プログラム」に基づき、インターネットを利用した児童ポルノ事犯の取締りを強化しており、インターネット・ホットラインセンターからの通報を活用するほか、ウェブサイトや電子掲示板等の閲覧による違法情報・有害情報の有無の調査を行うサイバーパトロールその他あらゆる活動を通じた児童ポルノ事犯の情報収集に努めている。

また、都道府県警察では、児童ポルノ画像に係る被疑者、被害児童等の居住地が広範囲に及ぶ場合があるなどのインターネット利用事犯の特殊性を踏まえ、関係都道府県警察が合同捜査・共同捜査を積極的に実施している。警察庁においても、全国会議の開催等により情報共有を図るなどして、都道府県警察の捜査力の向上等に努めるほか、ファイル共有ソフトを利用した児童ポルノ公然陳列事犯等の一斉取締りを調整するなど、効果的な取締りの推進による児童ポルノの根絶を図っている。

事例1 Case

公務員の男(51)らは、ファイル共有ソフトを利用して、児童ポルノ等を閲覧可能な状態に設定することにより不特定多数の利用者に対して公然と陳列した。22年９月、警察庁の調整により21都道府県警察で全国50か所の被疑者の自宅等の捜索を一斉に実施し、18人を児童買春・児童ポルノ法違反(児童ポルノ公然陳列)等で逮捕した。

③ 児童ポルノ画像の流通防止対策

児童ポルノ画像が一度インターネット上に流出すれば、その回収は事実上不可能となり、被害児童の精神的苦痛が将来にわたって続く。このため、警察では、インターネット上での児童ポルノ画像発見時には、速やかにサイト管理者等に削除を依頼するとともに、インターネット関係事業者に児童ポルノ画像の掲載・流通防止に係る自主的な取組の要請やプロバイダによる実効性のあるブロッキングの実施に向けた積極的な協力を行うなど、インターネット上の児童ポルノ画像の流通防止に取り組んでいる。

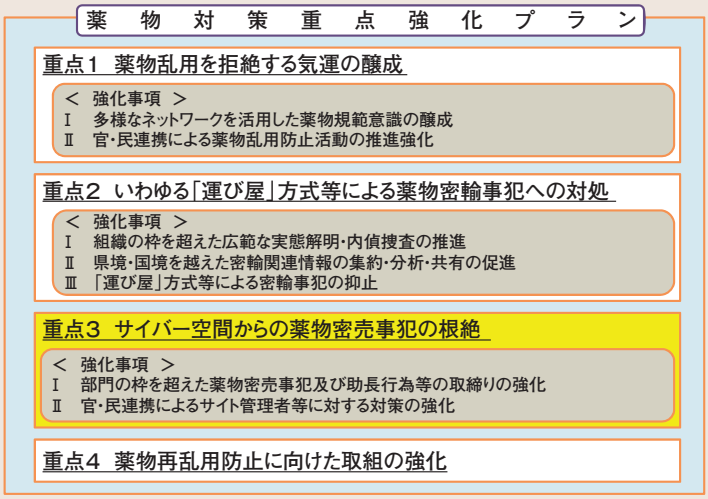
事例2 Case

22年４月、児童ポルノ画像を含む複数のウェブサイトの紹介、これらウェブサイトへの誘導を行う14のランキングサイトをサイバーパトロールにより把握し、警察において削除依頼を実施したところ、全て削除された(警視庁)。

(2)インターネットを利用した薬物密売事犯対策

現在、政府全体で「第三次薬物乱用防止五か年戦略」や当該戦略を加速化するために策定された「薬物乱用防止戦略加速化プラン」等に取り組んでいるところであるが、警察庁においてもこれら政府全体の取組や最近の薬物犯罪情勢の変化等に的確に対処するため、平成22年11月、関係部門間の連携により重点的に強化すべき施策を「薬物対策重点強化プラン」として策定した。その重点の一つに「サイバー空間からの薬物密売事犯の根絶」を挙げ、インターネットを利用した薬物密売事犯対策を推進している。

図-35　薬物対策重点強化プランの概要



その取締りに当たっては、サイバーパトロールやインターネット・ホットラインセンターからの通報等により薬物密売情報の収集を強化し、譲受け捜査(注)等の効果的な捜査手法を活用した密売人の検挙を推進している。また、薬物密売関連情報を掲載しているウェブサイトのサイト管理者等に対しても薬物の密売や広告、これらのほう助に関する罪を適用するなど、インターネット上で薬物密売・乱用を助長する行為の取締りに努めている。

さらに、薬物関連の違法情報・有害情報については、インターネット・ホットラインセンター等を通じて削除要請を徹底しており、特に、インターネットを利用した薬物密売事犯を検挙した場合は、サイト管理者等に対して警告及び再発防止指導等を行っている。

事例1 Case

無職の男(35)らは、電子掲示板に「◆信頼と実績100%納得！◆各種揃えています◆S＝0.15g￥10,000－◆直接取引又は郵送にて取引」等と書き込みをして覚醒剤の密売を行っていたことから、22年４月、６名を覚せい剤取締法違反(共同所持等)で逮捕した。また、この掲示板の管理者の男(36)は、同掲示板に覚醒剤の密売に関する書き込みが行われていることを知りながら、これらの書き込みの削除や掲示板の閉鎖をしていなかったことから、覚醒剤密売を手助けしたとして、同年９月、覚せい剤取締法違反(営利目的譲渡ほう助)で逮捕した(兵庫)。

事例2 Case

自営業の男(30)らは、インターネットの会員制コミュニティサイトを悪用して、大麻密売に関する書き込みをし、インターネットにより客から注文を受け付けて全国的に乾燥大麻を密売していた。22年５月、２人を大麻取締法違反(営利目的共同所持)で逮捕するとともに、乾燥大麻約26.4キログラムを押収した(大阪)。

注：譲受け捜査とは、薬物に関する犯罪捜査に当たり、警察官等が薬物の密売人等に接触し、薬物を譲り受けるなどする捜査手法をいう。

(3)インターネットを利用した生活経済事犯対策

① インターネットを利用した知的財産権侵害事犯

サイバー空間では、映像や音楽等のファイルを複製したものが著作権者の許諾を受けずに動画投稿サイトやファイル共有ネットワークで不特定多数の者に対して公開され、インターネット・オークションサイト等で偽ブランド品や海賊版DVDの違法販売が横行している。特にファイル共有ネットワークはそのネットワークの管理者が存在せず、発信元を容易に特定できないことから、著作権侵害ファイルについての警察による取締りやプロバイダによる警告が困難である。このため、著作権侵害に係るファイルのネットワーク上における流通が容易な状況にあり、知的財産権保護の観点から重大な問題となっている。警察では、この問題に対して、取締りを推進するとともに、事業者等との連携を図っている。

ア 取締りの徹底

警察では、インターネット・オークションにおける偽ブランド品や海賊版DVDの違法販売事犯の買受け捜査、多数の音楽ファイルが違法に投稿されている電子掲示板管理者に対するほう助に関する罪の適用、権利者からの取締り要望、警察庁が運用するP2P(Peer to Peer)観測システムによるファイル共有ネットワークの観測やサイバーパトロールを端緒とした被疑者の検挙を行うことにより、取締りに努めている。

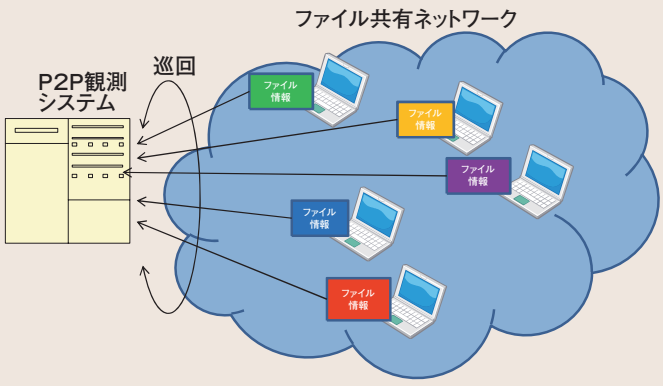
事例1 Case

無職の女(26)は、正規のプログラムを改変したものを内蔵し商標を付した改造ゲーム機を作成し、これをインターネット・オークションを利用して販売していたことから、平成22年５月、商標法違反(商標権の直接侵害)で逮捕した。また、無職の男(35)が、ゲームソフトデータを、ファイル共有ソフトを使用して不特定多数の者がダウンロードし得る状態にしたことから、同年６月、著作権法違反(公衆送信権侵害)で逮捕した(いずれも愛知)。

コラム ❹P2P観測システムについて

P2Pと呼ばれる通信技術を利用したファイル共有ネットワークは、参加者の匿名性が高く、多数の違法ファイルが流通している実態がある。警察庁では、ファイル共有ソフトによるファイル流通状況等の実態を把握するため、P2P観測システムを導入し、22年から運用している。同システムは、ファイル共有ネットワークを巡回してファイル情報を収集し、分析・検索を行うシステムである。

図-36 P2P観測システムの概要



イ　事業者等との連携

19年度総合セキュリティ対策会議(注)における提言を受け、20年５月、著作権団体等及びプロバイダにより構成され、警察庁等関係省庁がオブザーバとして参加する「ファイル共有ソフトを悪用した著作権侵害対策協議会」が設立された。同協議会では、22年２月、権利者からの要請を受けたプロバイダが権利侵害者に対して行う侵害行為の中止通知手続の透明性を確保すること等を目的としたガイドラインを策定し、22年３月からこのガイドラインをもとに「Winny ユーザへの啓発メール等送付スキーム」の運用を開始し、ファイル共有ソフトによる著作権の権利侵害が犯罪であることの周知を図っている。

②　生活経済事犯に係るインターネット上の違法な情報への対策

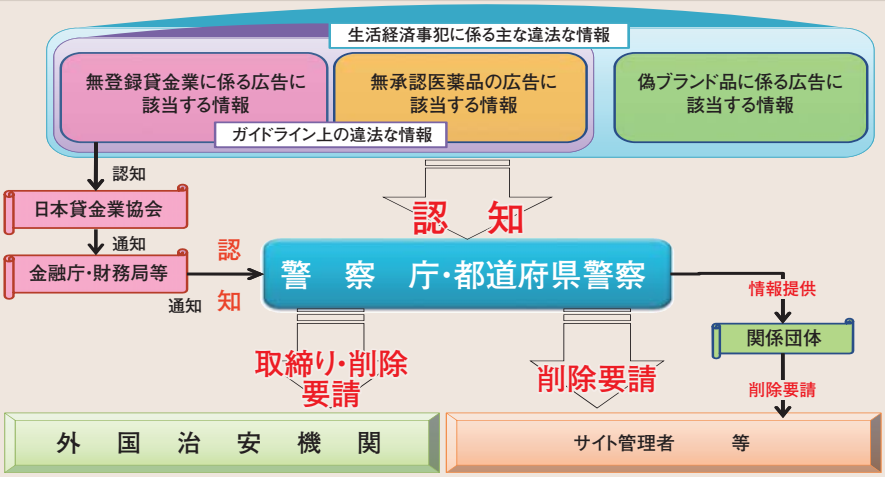
貸金業者としての登録を受けていないのに契約の締結を勧誘するなどの無登録貸金業（ヤミ金融）に係る広告、医薬品として承認を得ていない製品の購入を勧誘するなどの無承認医薬品に係る広告等、生活経済事犯に係るインターネット上の違法な情報の削除を求める社会的要請が高まっている。22年９月には、プロバイダ等関係団体において、違法性判断基準や警察からの削除依頼への対応手続等について整理した「インターネット上の違法な情報への対応に関するガイドライン」が改訂され、削除すべき違法な情報として、無登録貸金業に係る広告に該当する情報及び無承認医薬品の広告に該当する情報が明記された。

警察では、関係機関・団体と連携を図りつつ、生活経済事犯に係るインターネット上の違法な情報を掲載しているウェブサイトについて、サイト管理者等に対して削除を要請している。また、偽ブランド品の広告に該当する情報については、関係団体に対してその情報を提供している。さらに、中国等の外国のウェブサイトに当該違法な広告を掲載しているものが多いことから、外国治安機関に情報提供を行い、違法な情報の取締りや削除を要請している。

事例２ Case

婦人服雑貨店経営者（48）らは、22年５月、同人らが経営する婦人服雑貨店において、偽ブランド品65点を販売する目的で所持していた。同年５月、２人を商標法違反（譲渡目的所持）で逮捕した。また、同人は、偽ブランド品を中国のウェブサイトを利用して購入していたことから、同年６月から９月にかけて、ICPO を通じて中国警察に情報提供するとともに、当該偽ブランド品の流通販売業者の取締り及び当該ウェブサイトの削除を要請した（兵庫）。

図−37　生活経済事犯に係るインターネット上の違法な情報への対策



注：有識者、関連事業者、PTA の代表者で構成し、情報セキュリティに関する産業界と政府の連携の在り方について検討している。

4 サイバー犯罪捜査への支援

(１)技術支援

① 技術支援のための体制

情報通信技術の発展に伴い、サイバー犯罪に悪用される技術が高度化し、その取締りには、高い技術的知見が必要とされるようになったことから、警察庁では、サイバー犯罪対策に関し都道府県警察を技術的に指導する組織として、情報通信局、管区警察局情報通信部及び都道府県(方面)情報通信部に情報技術解析課を設置している。

② 技術支援の取組

サイバー犯罪の捜査に当たっては、犯行に使用されたコンピュータの特定が必要となる。情報技術解析課では、サイバー犯罪捜査への技術支援として、犯人が使用したとみられるコンピュータや犯人が不正にアクセスしたコンピュータ等から、当該犯行に係る情報を抽出する作業を行っているほか、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指導等を行っている。

また、コンピュータ・ウイルス等の不正プログラムを用いたサイバー犯罪に対しては、当該プログラムの動作解析を行い、手口の解明に資する情報を収集するほか、コンピュータ・ウイルスに感染したコンピュータの動向を把握するためのインターネット上の情勢の観測等を行っている。


解析の様子

さらに、警察庁では、ファイル共有ソフトによるファイルの流通状況等の実態把握を目的とした、Ｐ２Ｐ観測システム(41頁参照)を平成22年から運用している。同システムは、ファイル共有ソフトを用いた著作権法違反事件、児童買春・児童ポルノ法違反事件等の捜査において有用な情報を提供するなどしている。

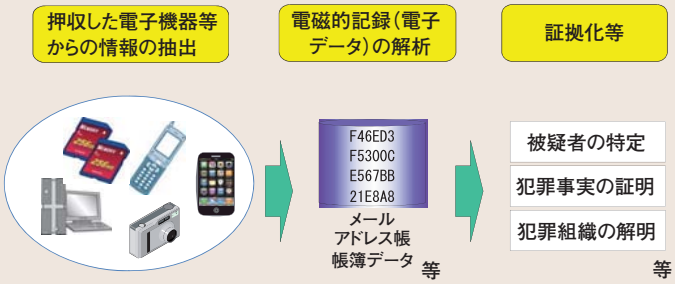
事例 Case

出会い系サイト運営会社取締役(36)らが、20年９月頃から21年３月頃にかけて、SNS サイトに不正アクセスして女性会員になりすまし、SNS サイトの男性会員にメールを送信して自らが運営する出会い系サイトへ誘導して会員登録させた上、実際には異性会員との電子メール交換ができないにもかかわらず、同サイト内において同社従業員らがなりすました架空の女性会員とのメール交換を継続させることにより、男性会員のポイントを消費させ、男性会員から出会い系サイト利用料をだまし取った詐欺事件に関し、21年２月から22年３月にかけて東北管区警察局宮城県情報通信部は、捜査員へのネットワークサービスに関する技術指導、約120台のコンピュータ等の解析、警察専用捜査支援ツールの作成等、事件解決に向けた技術支援を行った。

コラム ❺デジタルフォレンジック(注1)に係る取組

携帯電話、コンピュータ等の電子機器が一般に普及し、多くの犯罪に利用されるようになってきているとともに、客観的証拠の収集の徹底が強く求められていることから、犯罪に利用された各種電子機器に保存されている電磁的記録を適正に解析することが必要不可欠となっている。警察では、消去、改ざん等が容易な電磁的記録について、適正な手続による解析・証拠化等を行うための取組を強化している。

図-38　デジタルフォレンジックの概要



電子機器等に保存されている犯罪捜査に必要な情報を証拠化するためには、電子機器等から当該情報を抽出した上で、文字や画像等の人が認識できる形に変換するという電磁的記録の解析が必要不可欠であるところ、犯罪に利用された電子機器等は、証拠隠滅を企図した被疑者によって破損させられている場合があるほか、電磁的記録が暗号化されていることもあるなど、その解析には高度な技術が求められる。

また、電子機器等の製造技術の進歩は著しく、次々と新たな機器が登場することから、常に最新の技術や情報を収集・活用していくことが重要となる。

警察では、電磁的記録の解析に必要な技術情報を得るため、電子機器等の製造業者を始めとする企業との技術協力を推進するとともに、国内捜査関係機関が参加するデジタルフォレンジック連絡会及びアジア大洋州地域の治安機関が参加するアジア大洋州地域サイバー犯罪捜査技術会議を開催しているほか、21年5月には、欧州においてデジタルフォレンジックの中心的役割を担っているNFI(注2)との間で技術協力の推進を目的とした意図表明文書に署名するなど、関係機関との連携を推進している。

さらに、警察庁には、警察庁技術センター(注3)が開設されており、警察におけるデジタルフォレンジックの技術的中核として機能している。同センターには、高度かつ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、高性能の解析用資機材を整備し、都道府県(方面)情報通信部等で対応が困難な破損・水没した携帯電話やハードディスク等に記録された情報、暗号により隠蔽された情報等の抽出・解析等を行っているほか、新たな解析手法の検討等を行っている。

注1：犯罪の立証のための電磁的記録の解析技術及びその手続
2：Netherlands Forensic Institute(オランダ司法省法科学研究所)
3：平成11年4月、サイバー犯罪対策に関し都道府県警察を技術的に指導する組織として警察庁情報通信局に技術対策課(現情報技術解析課)が設置された際、その技術的な中核組織として同課に設置されたもので、特に高度かつ専門的な知識及び技能を有する職員が配置され、高性能の解析用資機材を備えている。

(２)国際連携

①　国際的なサイバー犯罪捜査協力の推進

ア　国際捜査共助

国境を越えて行われるサイバー犯罪に関し、国内における捜査で犯人を特定できないときは、外国捜査機関の協力を求める必要がある。

警察庁では、国際刑事警察機構(ICPO-Interpol)(注１)、刑事共助条約(協定)(注２)、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に対処している。

第12回アジア・南太平洋ＩＴ犯罪作業部会

イ　国際会議・協議

警察庁では、Ｇ８ローマ／リヨン・グループに置かれたハイテク犯罪サブグループ、ICPO アジア・南太平洋 IT 犯罪作業部会等の国際会議、外国捜査機関との協議を通じ、国際的なサイバー犯罪対策プロジェクトの実施、外国捜査機関職員との情報交換、協力関係の確立等に積極的に取り組んでいる。

また、平成23年５月、フランスで開催されたＧ８ドーヴィル・サミットでは、サイバー空間の安全確保等について首脳レベルでの初めての合意がなされ、各国政府や国際機関等が、Ｇ８ローマ／リヨン・グループと連携して情報通信技術のテロや犯罪目的利用の防止等に取り組んでいく必要があることなどが首脳宣言に盛り込まれた。これを踏まえ、警察庁では引き続き国際連携を推進していくこととしている。

②　国際的なサイバー犯罪捜査技術協力の推進

犯罪のグローバル化に伴い、外国製の電子機器等が犯罪に悪用される事例が増加している。これらの電子機器等に保存されている情報の抽出・解析を行うためには、外国における最新の技術動向の把握、外国治安機関との情報共有等を推進し、解析能力を向上させる必要がある。このため、警察庁では、各国治安機関等との情報技術解析に係る情報共有を始めとする国際連携を推進している。

ア　アジア大洋州地域サイバー犯罪捜査技術会議

警察庁では、アジア大洋州地域の治安機関が情報技術の解析に係る知識・経験等を共有し、円滑な情報交換を促進するとともに、各国・地域のサイバー犯罪等の対策に資する解析能力の向上を図ることを目的として、アジア大洋州地域サイバー犯罪捜査技術会議を12年度から毎年度開催している。


第11回アジア大洋州地域サイバー犯罪捜査技術会議

イ　サイバー犯罪技術情報ネットワークシステム

警察庁では、13年３月から、サイバー犯罪対策等に係る技術情報の共有を目的として、アジア大洋州地域の治安機関を結ぶサイバー犯罪技術情報ネットワークシステム(CTINS(注４))を整備・運用しており、22年12月現在、14の国・地域が参加している。

注１：International Criminal Police Organization−Interpol
２：208頁参照
３：平成９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」に基づき設置されたもので、現在58の国・地域に設置されている。
４：Cybercrime Technology Information Network System の略。電子掲示板やデータ共有等の機能を備え、暗号化されたネットワークにより、各国の担当官が安全に情報をやり取りできる手段を提供している。

5　事業者等による自主的かつ主体的な取組の促進

サイバー犯罪は、匿名性や広域性といったサイバー空間の特性に起因して捜査の困難性が極めて高いことや、この犯罪に的確に対処するためには高度な技術の活用が必要であることなどから、警察における取締りに加えて、事業者等においても自主的かつ主体的な取組を行うなど官民連携した対策を行う必要がある。

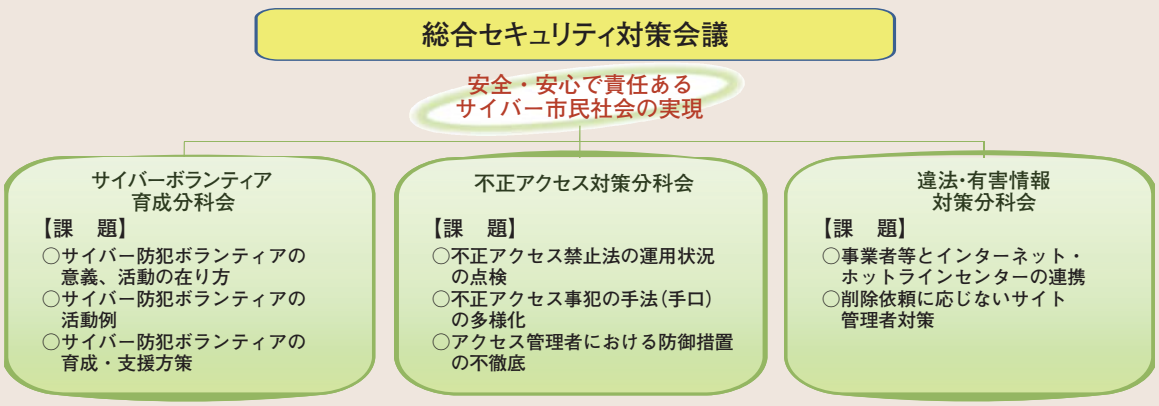
(1)総合セキュリティ対策会議


平成22年度総合セキュリティ対策会議

警察庁では、情報通信ネットワークの安全性・信頼性を確保することを目的として総合セキュリティ対策会議を開催し、情報セキュリティに関する産業界と政府の連携の在り方等について検討を行っている。同会議における提言を受け、これまでに、インターネット・ホットラインセンター(35頁参照)の運営が開始されたほか平成21年６月、児童ポルノの流通防止対策に関係する事業者、児童ポルノの流通防止に取り組む民間団体、学識経験者等からなる児童ポルノ流通防止協議会が発足した。また、21年度の会議では、インターネット・オークションにおける盗品の流通防止対策について検討が行われ、インターネット・オークションに商品が出品される際には、製造番号等必要な情報を出品物が掲載されたウェブサイトに表示させた上で、製造番号等から当該出品物が盗品であると判明した場合に適切に排除できるようにすることが必要である旨の提言がなされた。

22年度の会議では、安全・安心で責任あるサイバー市民社会の実現をテーマに、①不正アクセス対策、②違法情報・有害情報対策、③サイバー防犯ボランティアの育成について検討を行った。この結果、不正アクセス対策に関しては、フィッシングやSQLインジェクション攻撃の防止方策や民間事業者による自主的なアクセス制御機能高度化の促進を支援する枠組みづくりについて、違法情報・有害情報対策に関しては、インターネット・ホットラインセンターへの通報の活性化や違法情報の削除依頼に応じない悪質なサイト管理者の積極的な検挙について、サイバー防犯ボランティアの育成に関しては、活動ガイドラインの策定による組織化の促進等について提言がなされた。

図-39　平成22年度総合セキュリティ対策会議の概要



(2)コミュニティサイトへの対策

コミュニティサイトの利用に起因して児童が被害に遭った事件に係る検挙件数は増加している。

警察庁において行った平成22年中のコミュニティサイトの利用に起因する児童被害の詳細調査の分析(注1)では、被疑者の犯行動機としては児童との接触目的が90.9%(児童との性交目的70.1%、児童と遊ぶ目的13.8%)であった。また、被疑者が年齢等のプロフィールを詐称したものが44.0%、被疑者がミニメール(注2)からコミュニティサイト以外におけるメールのやり取りへ移行したものは94.0%であったほか、被害児童のうち、フィルタリング(注3)に加入していない児童の割合が96.6%であった。以上のことから、被疑者が、コミュニティサイトにおける児童被害に係る防止対策が不十分な点を利用して犯罪を敢行している状況や、被害児童におけるフィルタリング加入の不十分な状況が明らかになった。

そこで、23年２月、「犯罪から子供を守るための対策に関する関係省庁連絡会議」において「コミュニティサイトの利用に起因する犯罪から子どもを守るための緊急対策」を取りまとめ、警察庁及び関係省庁では、青少年が安全に安心してインターネットを利用できる環境の整備等に関する法律(以下「青少年インターネット環境整備法」という。)に基づくフィルタリングの普及、民間事業者による実効性のあるゾーニング(注4)の自主的導入の支援及び民間事業者による自主的なミニメール内容確認の支援に係る取組を推進している。

図-40 被疑者の犯行動機

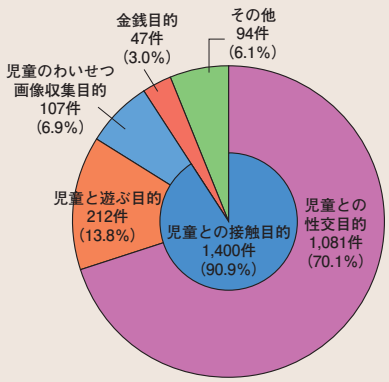


図-41 被疑者のプロフィール詐称状況

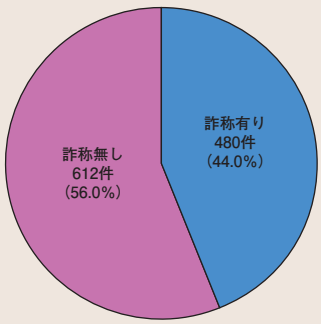


図-42 被疑者のミニメールから直接メールへの移行状況

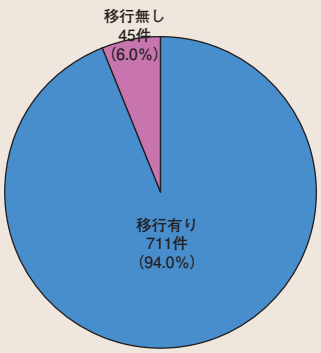
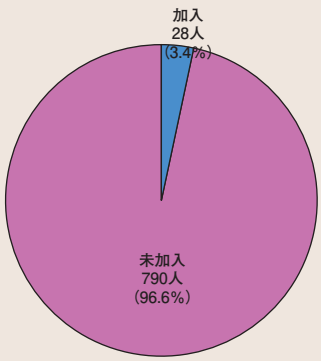


図-43 被害児童のフィルタリング加入状況



注１：平成22年中に検挙したコミュニティサイトの利用に起因して児童が被害に遭った事件1,541件(被疑者1,230人、被害児童1,239人)について、捜査の過程で判明した事実を基に、調査項目ごとに集計し、調査項目に係る事実が判明した検挙事件のみの件数を集計している。
２：コミュニティサイト内において、会員同士でメッセージの送受信ができる機能。
３：インターネット上のウェブサイト等を一定の基準に基づき選別し、青少年に有害な情報を閲覧できなくするプログラムやサービス
４：利用者の年齢等属性に応じて利用可能なサービスを区別して設定すること。

また、警察庁では、その利用に起因する被害児童数が多いコミュニティサイトの事業者に対し、ユーザー数等その規模に応じ、ミニメールの内容確認を含む十分な体制の構築、年齢認証等のなりすましを防止するためにフィルタリングの有無に関する情報を活用することによるゾーニングの効果的運用やサイト管理者と携帯電話事業者が連携して年齢確認を行う体制の構築・運用を要請するとともに、フィルタリングの普及促進について、都道府県警察により、事業者に対する指導・要請、保護者に対する啓発活動、関係機関と連携した広報啓発活動等を推進している。

コラム ⑥児童が使用する携帯電話に係るフィルタリングの100%普及を目指した取組の推進について

児童が携帯電話を通じてインターネットに接続し青少年有害情報を閲覧することを防止するためには、携帯電話に係るフィルタリングの利用が有効であるが、保護者や関係事業者の責務等を定めてフィルタリングの利用促進を図った「青少年インターネット環境整備法」が21年４月に施行されたにもかかわらず、児童の携帯電話に係るフィルタリングの利用率は、23年２月に内閣府が公表した調査結果によれば、小学生で77.6%、中学生で67.1%、高校生で49.3%にとどまっている(注1)。一方、22年上半期にコミュニティサイトの利用に起因する犯罪の被害に遭った児童の９割以上は、フィルタリングに加入していない携帯電話からコミュニティサイトに接続しているという実態が明らかになっている(注2)。このため、警察では、コミュニティサイトの利用に起因する児童の犯罪被害を防止するため、関係省庁等と連携しながら、フィルタリングの100%普及を目指した取組を推進している。

特に、携帯電話の販売・契約現場は、利用者にフィルタリングの利用を促す「最後の砦（とりで）」と考えられることから、携帯電話関係事業者（販売代理店、家電量販事業者等を含む。）等に対し、販売・契約現場において、児童の保護者等に対するフィルタリングの必要性の説明や、より安全なフィルタリングサービスの推奨等を徹底してもらいたい旨の要請を強化している。

また、携帯電話の利用に起因する児童の犯罪被害の実態やインターネットの危険性、フィルタリングの利用を含めた保護者の責務等についての認識・理解の浸透を図るため、学校の入学説明会等の機会を捉えて保護者の意識啓発に努めているほか、教育委員会等の関係機関・団体と連携し、フィルタリングの普及に向けたキャンペーンや広報啓発活動を推進している。

事業者に対する要請（宮崎日日新聞）

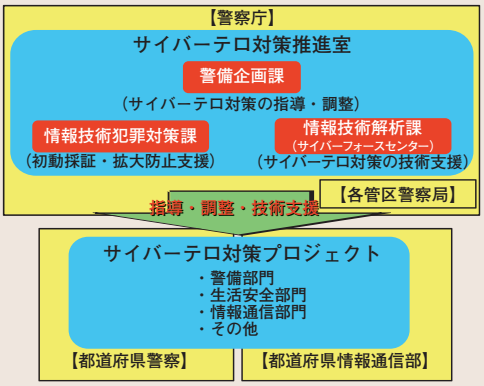
注１：平成22年度青少年のインターネット利用環境実態調査結果（平成23年２月、内閣府）
２：非出会い系サイトに起因する児童被害の事犯に係る調査分析（平成22年10月、警察庁）

6 サイバーテロ対策

(1)サイバーテロ対策のための体制

① 平素からの措置と事案発生時の対応

図−44 サイバーテロ対策のための体制



警察庁では、警備局、生活安全局及び情報通信局の職員により構成される部門横断的なサイバーテロ対策推進室を設置し、都道府県警察に対してサイバーテロ対策に関する指導・調整のほか、都道府県警察の職員に対する教育訓練を行うなど、総合的なサイバーテロ対策を推進している。

また、都道府県警察及び都道府県情報通信部では、サイバーテロ対策プロジェクトを設置し、重要インフラ事業者等への個別訪問や共同訓練を行うなど官民連携した諸対策を推進している。

さらに、サイバーテロ又はそのおそれがある事案を認知した場合には、都道府県警察のサイバーテロ対策要員が、情報通信部門の技術支援を受けつつ、被害状況の把握、被害拡大の防止、証拠保全等の緊急対処活動等を行うこととしている。

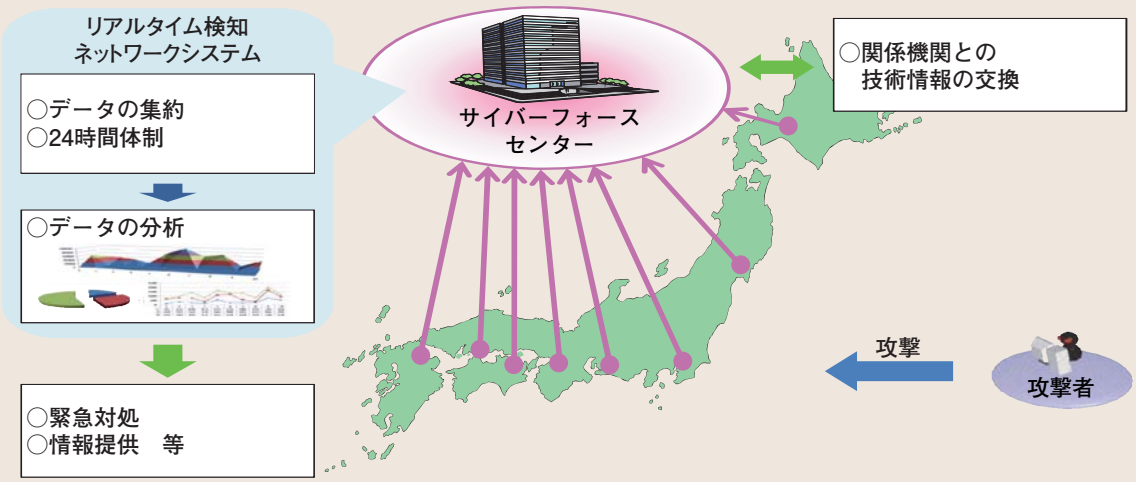
② サイバーテロ対策の技術的基盤

ア サイバーフォース

サイバーテロ対策の技術的基盤として、各管区警察局等に、サイバーフォースと呼ばれる技術部隊が設置されている。サイバーフォースは、全国の警察職員から選抜された高度かつ専門的な知識及び技術を有する者で構成されており、都道府県警察に対する技術支援を実施している。

また、警察庁には、全国のサイバーフォースの司令塔として、サイバーフォースセンターが設置されている。同センターは、24時間体制でサイバーテロの予兆把握に努めるとともに、集約された情報を分析し、その分析結果を重要インフラ事業者等へ提供するなどしている。さらに、同センターは、警察におけるサイバーテロ対策の技術的中核として、全国のサイバーフォースに対する指導等を実施するとともに、サイバーテロ発生時には緊急対処の技術支援の拠点として機能する。

図−45 サイバーフォースセンターの機能



イ　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からの情報を集約・分析することで、DoS(注)攻撃の発生やコンピュータ・ウイルス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。平成21年３月には、同システムの更新・高度化を行い、サイバーテロに係る情報の集約・分析能力を強化した。

リアルタイム検知ネットワークシステム

③　人材育成

サイバーテロ対策を行うに当たっては、サイバー攻撃の手法や情報セキュリティに関する知識及び技術が必要であることから、対策に従事する職員を対象として、警察大学校等で教育訓練を実施している。

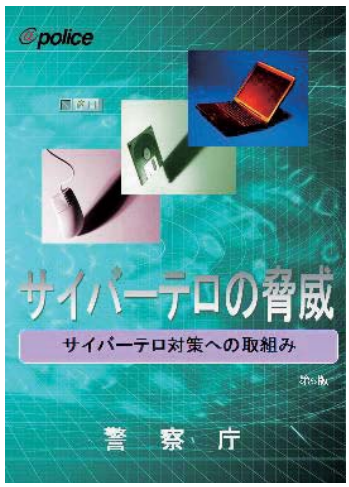
(２)サイバーテロ対策のための取組

サイバーテロの未然防止及び発生時における的確な対処のため、警察では、重要インフラ事業者等との連携強化を始め、様々な取組を推進している。

①　官民連携したサイバーテロ対策の推進

ア　個別訪問による情報提供

警察では、重要インフラ事業者等に対し個別に、サイバーテロの脅威や情報セキュリティに関する情報の提供を行うとともに、事案発生時における警察への速報を要請するなどしている。平成21年から22年にかけては、APEC 首脳会議等を標的としたサイバーテロの未然防止に万全を期すため、APEC 関連事業者等に対しても個別に、基幹システムの安全確保について必要な助言を行うなどした。



サイバーテロ対策パンフレット

イ　共同訓練

警察では、重要インフラ事業者等とサイバーテロの発生を想定した共同訓練を実施し、緊急対処能力の向上に努めている。APEC 首脳会議等が開催された22年中には、APEC 関連事業者等と共に、会議場がサイバー攻撃を受けたとの想定で、初動措置や原因究明等を行う共同訓練を実施した。

共同訓練の様子

注：Denial of Service 攻撃の略。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

ウ　サイバーテロ対策協議会

22年12月末現在、34の都道府県において警察及び重要インフラ事業者等で構成されるサイバーテロ対策協議会を設置し、サイバーテロに関する警察からの情報提供、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。

サイバーテロ対策協議会

エ　サイバーテロ対策セミナー

警察では、重要インフラ事業者等の基幹システムの運用に携わる情報セキュリティ担当者を対象としたサイバーテロ対策セミナーを実施している。このセミナーでは、サイバー攻撃の実演のほか、攻撃に対する防御手法の解説等の情報提供に努めている。

②　国際連携の強化

サイバーテロは容易に国境を越えて行われ、一国だけでは解決できない問題であることから、警察では、外国関係機関・団体と連携し、平素からサイバーテロ対策に資する情報交換を行うとともに、事案発生時に適切な対処を行うために合同訓練を行うなどしている。

事例 1 Case

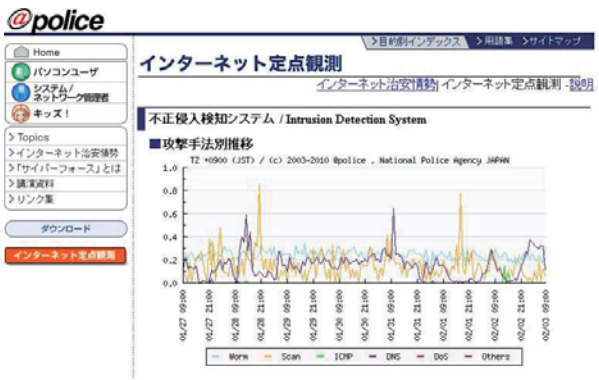
22年９月、警察庁は、米国国土安全保障省が主催する国際的なサイバー攻撃対処演習である「サイバーストームⅢ」に参加し、同省を始めとする外国関係機関等と連携して大規模なサイバー攻撃へ対処するための訓練を行った。

事例 2 Case

22年10月、警察庁は、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)の技術会合に出席し、事案が発生した際の適切な対処活動に資する情報の収集を行った。

③　インターネット利用者への情報提供

警察庁では、警察庁セキュリティポータルサイト「@police」(http://www.npa.go.jp/cyberpolice/)を開設し、各種プログラムのぜい弱性や不正プログラムに関する注意喚起情報等を公開しているほか、リアルタイム検知ネットワークシステムの観測データを一定時間ごとに集計・分析して表示する「インターネット定点観測」、インターネット上の情勢を分析したレポート等、情報セキュリティの向上に資する情報を提供している。



警察庁セキュリティポータルサイト「@police」

注：Forum of Incident Response and Security Teams の略

第3節 サイバー犯罪対策の抜本的強化に向けて

サイバー犯罪を取り巻く環境は変化を続け、新たな課題を警察に対して突き付けている。警察においては、こうした変化に迅速・的確に対応し、サイバー空間の安全・安心を確保するため、サイバー犯罪の取締り、犯罪の痕跡を確実にたどるための環境整備や官民の連携によるサイバー空間の秩序維持を強力に推進していく必要がある。

1 不正アクセス対策の強化

不正アクセス禁止法は、電気通信回線を通じて行われる電子計算機に係る犯罪の防止及びアクセス制御機能により実現される電気通信に関する秩序の維持を目的として、不正アクセス行為等の禁止・処罰及びアクセス管理者による防御措置を規定しており、不正アクセス禁止法違反について、警察における取締りとアクセス管理者における予防の両面からの対策を求めている。

第１節でみたとおり、不正アクセス禁止法違反をめぐる情勢は深刻な状況にあり、警察とアクセス管理者それぞれにおいて実施すべき対策についての更なる強化に向けた検討を行う必要がある。

(１)不正アクセス防止のための官民意見集約委員会(官民ボード)の設置

社会全体として不正アクセス行為からの防御を進めるためには、官民それぞれの立場において不正アクセス行為に係る情報を収集するとともに、それらを共有することにより、不正アクセス行為に係る実態をより詳細かつ正確に把握することが必要である。そこで、警察庁、総務省及び経済産業省が主体となって、官民連携した情報共有の場として不正アクセス防止のための官民意見集約委員会(官民ボード)を平成23年６月に設置した。

官民ボードでは、事業者等が活動を行う上で知り得たぜい弱性情報及び関係団体が被害拡大を防止する上で必要となる対策等を共有し、不正アクセス行為等の脅威から国内の企業等を守ることを主眼に活動を行うこととしている。併せて、サイバー空間において対策を講ずる必要のある事象について事業者側の意見を集約し、関係省庁において当該対策の検討を実施する予定である。

(２)取締り強化に向けた検討

不正アクセス禁止法の制定当時に比して、サイバー空間において多くのサービスが提供され、様々な情報がやりとりされるなど、国民生活や社会経済活動におけるサイバー空間への依存度が高まっている。このため、不正アクセス行為が及ぼす影響が増大しており、アクセス制御機能の社会的信頼を確保する不正アクセス禁止法の位置付けも変化してきている。こうした情勢を踏まえ、不正アクセス行為に対する制裁の在り方について検討する必要がある。

また、敢行されると膨大な量の個人情報の流出を発生させるSQLインジェクション攻撃のような新たな不正アクセス行為の手口が出現したり、現行の不正アクセス禁止法では対処できないフィッシングといった新たな識別符号の入手方法が出現したりしている。

これら新たな手口等の危険性を捉え、不正アクセス禁止法の目的の一つである「電気回線を通じて行われる電子計算機に係る犯罪の防止」の観点から、これら新たな手口等に的確に対処する

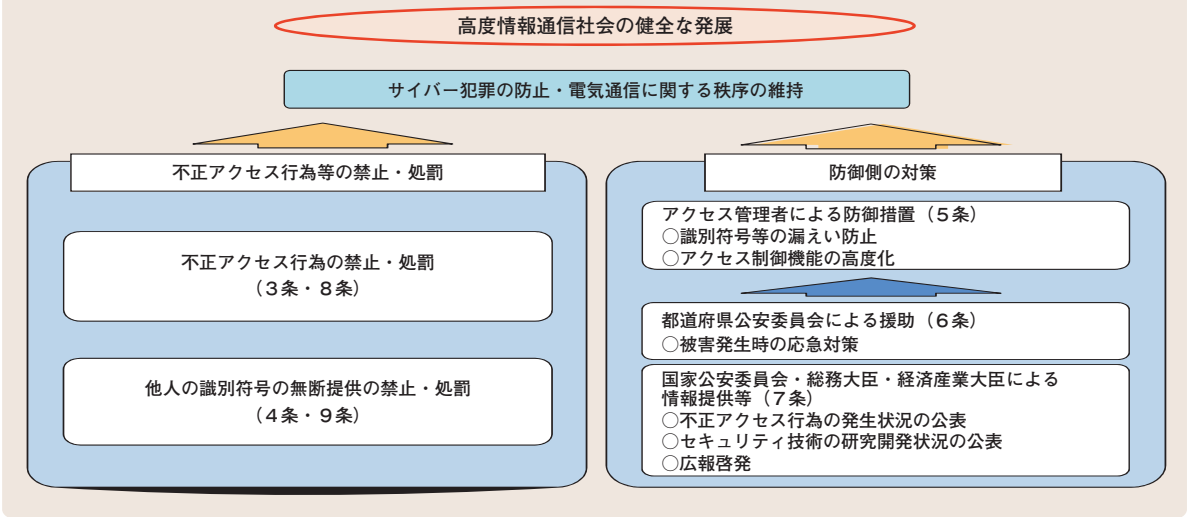
ための諸対策について検討を行う必要がある。

(3)アクセス管理者による防御措置の向上

経済活動がインターネットに依存する傾向が高まったことで、企業においては、個人情報等を保有することが多くなり、その結果、不正アクセス行為によって保有している個人情報等が流出し、顧客に多大な影響を与える事案などが発生している。特に不正アクセス行為の目的が金銭目的に移行し、その手口が巧妙化していることに鑑みれば、不正アクセス行為を防止するためにアクセス管理者が防御措置を講じることは、根本的な対策であると言うことができる。

アクセス制御機能に関しては、インターネットの発展が民間主導でなされてきたという経緯から、法令で規格を定めることになじまない性質のものであり、民間事業者等は、アクセス制御機能の高度化を図り、不正アクセス行為からの防御水準を向上させることについての責務を有するものと考えられるため、アクセス制御機能に関しては、民間事業者による自主的な高度化の取組を基本として、これを促進、支援するための枠組みを検討する必要がある。

図-46　不正アクセス禁止法の概要



2　不正指令電磁的記録作成罪の新設等による取締りの強化

近年におけるサイバー犯罪その他の情報処理の高度化に伴う犯罪等の実情に鑑み、人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録（不正指令電磁的記録）の作成を処罰する不正指令電磁的記録作成罪の新設を始めとする「情報処理の高度化等に対処するための刑法等の一部を改正する法律」が平成23年６月に公布され、当該罪については同年７月に施行された。

警察庁では、都道府県警察に対して改正趣旨を通知するとともに、不正指令電磁的記録作成罪の効果的取締り等に係る指導を行うなどして、本罪に係る適切な取締りを推進していく。

3　サイバー犯罪捜査の環境整備

サイバー犯罪を抑止するためには、サイバー犯罪が認知された場合に速やかに捜査され、その被疑者が迅速に検挙されることが必要である。このようなサイバー犯罪捜査の環境を整備する

ためには、サイバー犯罪における事後追跡可能性、すなわち、被疑者が被害者のコンピュータに接続した際の接続ログ、インターネットに接続した際の認証ログ、契約者情報等の被疑者を特定するために必要なデータが確保される状態にあるかという視点が必要であり、現在、この確保を行う上での支障となっている犯罪インフラ(注1)等について対策を行う必要がある。

(1)海外の捜査機関との連携強化と海外の企業との協力関係の構築

世界規模のSNS(ソーシャル・ネットワーキング・サービス)やインターネット・ショッピング等の利用者の増加、クラウド・コンピューティング(注2)の普及等今後ますますサイバー犯罪の捜査環境が悪化することが予想される。このような情勢に的確に対処するためには、外国捜査機関とより緊密な協力体制を確立し、事案によっては、二国間又は多国間で並行して捜査を行うことが必要である。

また、サイバー犯罪を捜査するために必要となる通信ログや契約者情報等が海外事業者等で管理されており、日本に照会の窓口が設置されていない場合、当該情報の入手を外交ルート等を通じて当該国の法執行機関に対して要請しているところであるが、要請した情報を入手するために長期間を要することもある。このため、捜査に必要な情報を迅速に入手できるよう、警察庁から海外の企業に対して日本での照会窓口の設置を働き掛けるなど海外の企業との連携を強化する必要がある。

(2)インターネットカフェにおける利用者の匿名性排除に向けた対策

インターネットカフェについては、インターネットカフェにおいて敢行される犯罪の抑止対策として、利用者の匿名性排除が必要不可欠である。警察庁では、平成19年から、日本複合カフェ協会に対し、利用者の本人確認や使用する端末の記録、防犯カメラの設置等、匿名性を排除するための諸対策を申し入れるとともに、各都道府県警察におけるインターネットカフェ連絡協議会設置の推進等の諸対策を行ってきた。

警察庁においては、インターネットカフェに係る条例を制定しようとする道府県に対する支援の実施や、東京都における条例の制定後の犯罪の発生状況の推移を踏まえ、引き続き諸対策を推進することとしている。


インターネットカフェ店内


インターネットカフェ個室

(3)無線LAN、データ通信カードの悪用防止に係る対策

無線LANについては、他人の無線LANを無断で介した他人名義によるインターネットの接

注1：127頁参照
2：データサービス等がネットワーク上にあるサーバ群(クラウド(雲))にあり、ユーザのコンピュータでデータを加工・保存することなく、「どこからでも、必要な時に、必要な機能だけ」を利用することができる新しいコンピュータネットワークの利用形態。

続が問題となっている。警察庁ではこの問題に対処するため、暗号化を初期設定とした無線LAN機器の販売についての事業者等への協力要請や、利用者に対しセキュリティ設定に関する広報啓発を行っていく必要がある。

また、データ通信カードについても、本人確認を受けることなく購入できるデータ通信カードの利用者の匿名性が問題となっているため、事業者等に対し、販売時における本人確認の実施を要請し、事業者等の自主的な取組を促進していく必要がある。

今後は、警察庁において事業者等と共に、無線LANやデータ通信カードの匿名性対策の在り方を検討していくこととしている。

事例 Case

電気店の店長の男(42)らは、電波法が定めた上限の数十倍の電波を出力できる無線LANアダプターを「無銭LAN」と称して販売することにより、購入者がこれを利用して他人の無線LANを介してインターネットに接続できるようにした。平成22年９月、電波法違反(無線局の無免許開設)、同ほう助で合計11人を検挙した(大阪)。

(４)通信記録(ログ)の保存に向けて

サイバー犯罪の捜査では、使用されたコンピュータを特定するとともに、そのコンピュータを誰が使用したのかを特定する必要があり、そのためには通信記録が不可欠であるところ、この通信記録が保存されていないために犯人の特定に至らない事件がしばしば見受けられる。昨今の高度化・多様化が進むサイバー犯罪に係る対策において、通信記録の重要性はますます高まっている。

また、通信記録は、犯罪捜査のみならず民事上の紛争における相手方の発見や証拠の確保、セキュリティサービス事業者等によるネットワーク障害の原因究明等においても必要不可欠なものとなっている。通信事業者等による通信記録の保存は、電磁的記録媒体の容量が少なく、容量当たりの価格も高価だった時代に比べ、技術の進歩等により容量が増大し、価格も安価になった今日では、必ずしも大きな負担ではなくなってきていると考えられる。

こうしたことから、通信記録の保存の必要性について、捜査の円滑化以外の観点からも、国民全体に議論を広げ、国民の理解を深めていく必要がある。

事例 Case

平成21年４月、オンラインゲームの利用者から「オンラインゲームに不正アクセスされ、ゲーム上の仮想通貨等を盗まれた」との相談を受けたことから、不正アクセスに係るIPアドレスを特定し家宅捜索を実施したところ、同所にはオンラインゲームへのアクセスを中継するウェブサーバが設置されていた。しかし同ウェブサーバはいずれかの場所からのオンラインゲームに対する接続を中継しているだけであったことから、真の不正アクセスの発信元を特定すべく、同ウェブサーバの解析を行ったが、ログが保存されていなかったことから、不正アクセスの発信元の特定には至らなかった。

同ウェブサーバを設置していた者については、無届で電気通信事業を行っていたことから、22年２月、電気通信事業法違反(届出義務違反)で逮捕した(山口)。

4 官民の連携によるサイバー空間の秩序維持

(１)サイバー防犯ボランティア活動の促進

「自分たちの町は自分たちで守る」という理念の下、安全で安心して暮らせる地域社会の実現を目指して結成された、現実空間における自主防犯ボランティアの青色パトロールを始めとす

るパトロール活動等は、街頭犯罪等の抑止や規範意識の向上に一定の成果を上げてきた。第１節でみたサイバー空間における現状に鑑みると、サイバー空間においても、一般のインターネット利用者の規範意識を向上させ、サイバー空間の安全・安心を確保するため、犯罪被害防止についての国民に対する広報啓発、悪質な利用者への指導・注意といった活動を行う、インターネット利用者によるサイバー防犯ボランティア活動を促進する必要がある。

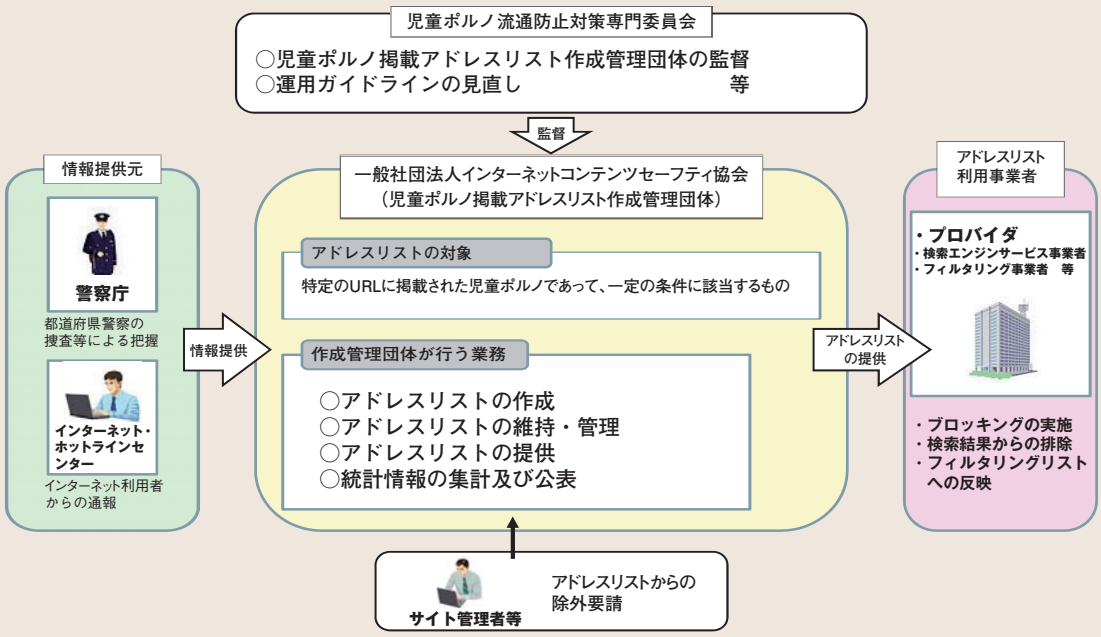
現在、このような活動に取り組んでいる団体として、公益社団法人全国少年警察ボランティア協会、日本ガーディアン・エンジェルス等がある。このような団体の先進的取組を参考にしながら、警察では、今後、サイバー防犯ボランティア活動ガイドラインの作成等によりサイバー防犯ボランティア活動を行いやすい基盤を整備するとともに、サイバー防犯ボランティアの活動の重要性を国民に訴え、その結成を促進し、官民連携によりサイバー防犯ボランティアを育成していくこととしている。

（２）児童ポルノのブロッキングに係る支援

児童ポルノ流通防止協議会（46頁参照）における、ブロッキングの実施に向けた法的・技術的課題の整理、アドレスリスト利用事業者に対してアドレスリストを提供する、児童ポルノ掲載アドレスリスト作成管理団体（以下「作成管理団体」という。）の設置に向けた検討や、平成22年７月に政府の犯罪対策閣僚会議において決定された、22年度中を目途に関係事業者がブロッキングを自主的に実施できるよう環境整備の推進を内容とする「児童ポルノ排除総合対策」を受け、同年12月、作成管理団体を選定・監督する児童ポルノ流通防止対策専門委員会が発足した。

警察庁では、作成管理団体について試験的運用を実施し、ブロッキングの円滑な実施に向けた検証を行い、作成管理団体の基本的な業務に係る運用の流れや技術を構築した。これを受けて、23年３月に、プロバイダ等が中心となって発足した一般社団法人インターネットコンテンツセーフティ協会が作成管理団体として選定され、同年４月から運用を開始しているところである。今後は、情報提供元となる警察庁等を含め作成管理団体とプロバイダ等のアドレスリスト利用事業者が一体となって児童ポルノ排除に向けた取組を一層推進していく必要がある。

図−47　「児童ポルノ掲載アドレスリスト作成管理団体」の運用イメージ



(3)コミュニティサイトにおける児童の犯罪被害防止対策

平成23年２月、「コミュニティサイトの利用に起因する犯罪から子どもを守るための緊急対策」が取りまとめられ、コミュニティサイトの利用に起因する児童被害の更なる増加を防ぐ取組がなされているところである（47頁参照）。今後とも、コミュニティサイトの利用に起因する犯罪の取締りの徹底を基本としつつ、関係省庁と連携して、携帯電話事業者の保有する利用者年齢情報を活用した実効性のあるゾーニングの自主的導入の支援等、同対策に基づく取組を緊急に推進していく。

また、警察庁では、23年２月、サイトの審査監視機関（一般社団法人モバイルコンテンツ審査・運用監視機構（EMA）(注)）に対しての情報提供を合意締結するなど、児童の犯罪被害の抑止に向けた官民連携した取組を推進している。

5 終わりに

インターネットは、世界中にある様々な情報の収集のみならず、インターネットショッピング等による経済取引やコミュニティサイトによる交流活動等を行うために気軽に利用されるなど、今や国民生活に必要不可欠なものとなっている。加えて、インターネット関連企業等において、インターネット利用者のニーズに応えるために新たな技術やサービスが生み出され続けており、サイバー空間における利便性は向上し、サイバー空間を利用する上での便益はますます大きくなっている。

その一方で、サイバー空間における犯罪の敢行は、捜査をより困難にしたり、被害をより拡大させるおそれがあり、現に、第１節で示した事例のように、インターネット接続をより簡易にするための機器や施設が犯罪の匿名性を高めてしまったり、情報発信や交流を容易にするサービスが被害の標的となり得る対象を増やすといった状況が見受けられる。

また、国民からのアンケート結果にもみられるように、現実社会と比較して自由度の高いサイバー空間においては、一般のインターネット利用者においても規範意識が必ずしも高いとはいえない状況にある。

警察では、巧妙化し続けるサイバー犯罪に対して、様々な対策を講じてきたところではあるが、サイバー犯罪の情勢はいまだ厳しく、引き続き、警察組織を効果的に活用した捜査体制の構築や新たな手口についての対応を検討していくこととしている。

それらに加え、今後は、インターネット利用者全体に向けた対策をさらに推進し、インターネットを利用する全ての人々が、サイバー空間において高い規範意識を持ち、責任ある行動をとるよう、産業界、関係機関・団体はもとより、インターネットを利用する組織や個人と警察とが連携を強化し、社会を挙げて対策を進めることにより、安全・安心で責任あるサイバー市民社会の実現を目指していく必要がある。

注：平成20年４月に設立された携帯等のフィルタリングで一律にアクセスが制限されてしまうコミュニティサイトなどについて、青少年を違法情報・有害情報から保護する観点から、青少年にとって有害でないサイトを認定・監視するための有識者からなる第三者機関。

警察活動の最前線


埼玉県警察
ポッポくん

サイバー犯罪と対峙するために

前　埼玉県警察本部生活安全部生活安全企画課（現　草加警察署地域課）
三上山（みかみやま）　知子（ともこ）　巡査部長

「皆さん全員が、サイバー犯罪の被疑者にも被害者にもなる危険があります。」

サイバー犯罪対策係として事件捜査や被害防止の広報啓発活動等に携わる中で、インターネット利用者の危機意識の低さを強く感じている私は、サイバー犯罪防止を訴える講演等において、必ずこうした言葉を伝えるようにしています。

インターネットの普及で世の中が便利になった一方、利用者の危機意識と規範意識の希薄さを受けて、私たちの身近なものとなっているサイバー空間には違法・有害な情報が氾濫して、今や社会問題となっています。私は統計も担当しているので、数字からもサイバー空間の状況の悪化を感じます。

先日も、不正アクセスで検挙した中学生から「他人のIDを勝手に使ってもバレないし、ゲームにアクセスしただけなら犯罪にならないと思った。」と聞きました。その中学生は、現実と非現実を区別できず、パソコン上の行為なら許されるだろうというゲーム感覚で犯罪を犯していたのですが、目の前にあるものはただの機械でも、その向こうには心を踏みにじられている人がいる事を忘れないで欲しいものです。

今は、サイバー犯罪に対峙（じ）するため経験を積み、基礎と実戦の業務知識をしっかり身に付けたい！その思いが募っています。

サイバーテロとの闘い

前　関東管区警察局新潟県情報通信部情報技術解析課（現　栃木県情報通信部情報技術解析課）
菊池（きくち）　祐司（ゆうじ）　技官

重要インフラの基幹システムがサイバー攻撃を受けるといった事案が発生した場合、限られた時間内で情報を正確に分析し、攻撃の遮断、被害拡大の防止やシステムの復旧を図る必要があります。

そのためには日頃からの備えが重要であり、警察では、こうした事案に備え、警備部門、生活安全部門、情報通信部門が連携して緊急対処訓練を実施していますが、訓練には「サイバー攻撃手法や防御方法の技術的知見」を反映させるという情報通信部門の役割が非常に重要になっています。また、訓練には警察だけでなく重要インフラ事業者等も参加していることから、それら事業者等に対しても的確な指導・助言をする必要があります。この訓練の成功に向け、私は寸暇を惜しんで最近のサイバー攻撃対策の技術を勉強し、得られた知識を訓練シナリオに反映させて、より充実した訓練の実施に努めています。

このように、今後とも日々進化する情報通信技術を熱心に勉強し、サイバーテロ対策に活かして、国民生活の安全に寄与していきたいと思います。