安全・安心で責任あるサイバー市民社会の実現に向けた対策について

平成22年度総合セキュリティ対策会議 報告書

総合セキュリティ対策会議

はじめに

近年めざましい発展を遂げている情報通信ネットワーク、とりわけインターネットは、私たちの生活の利便性を向上させるにとどまらず、社会・経済活動の根幹を支える重大なシステムとして機能するに至っている。その一方で、サイバー犯罪の増加、インターネット上の違法・有害情報の氾濫、コンピュータ・ウィルスの蔓延が社会問題となるとともに、サイバー空間に対する国民の不安感も急速に高まっており、今、正に官民が連携してより効果的な情報セキュリティ対策を検討・実施するべき時期を迎えている。

「総合セキュリティ対策会議」は、情報セキュリティに関する産業界等と政府機関との連携の在り方、特に警察との連携の在り方について意見交換を行うことを目的として、平成13年度以降開催されているものである。当会議においては、情報セキュリティに関する有識者にとどまらず、電気通信事業、コンテンツ事業、コンピュータ製造・販売業、ソフトウェア産業等の各種事業に関する知見を有する方々、さらに、法曹界、教育界、防犯団体の方々という広い分野の有識者により、幅広い意見交換が活発に行われており、平成13年度以降、毎年度、様々な内容の報告書を取りまとめてきた。そして、こうした意見交換の結果は、例えば、平成18年６月のインターネット・ホットラインセンターの運営開始、平成20年５月のファイル共有ソフトを悪用した著作権侵害対策協議会の発足、平成21年６月の児童ポルノ流通防止協議会の発足等の取組に結び付いている。

本年度は、昨今規範意識の低下が見られるサイバー空間において、安全・安心で責任あるサイバー市民社会を実現するため、喫緊に対策が必要と考えられる、不正アクセス対策、違法・有害情報対策及びサイバーボランティア育成の３テーマを取り上げた。各委員には、それぞれが属する企業・組織における知見を背景としつつも、中立的な立場で、各テーマに関して関係者が講じるべき具体的な取組等について議論を行っていただいた。本報告書は、これらの議論の結果を取りまとめたものであり、今後の情報セキュリティの向上及び安全・安心なインターネット社会の発展の一助となれば幸いである。

平成23年４月

総合セキュリティ対策会議委員長

前田雅英

総合セキュリティ対策会議の目的

昨今の官民を挙げた取組により、情報技術の急速な進展や高度情報通信ネットワーク社会が実現されつつあり、市民生活や社会・経済活動のあらゆる分野において、情報技術及び情報通信ネットワークが活用されるようになっている。

特に、インターネット等の活用により生活の利便性が向上するなど、高度情報通信ネットワーク社会の光の部分が拡大する一方、サイバー犯罪が年々増加するなど、その陰の部分とも言うべき、情報セキュリティに対する脅威も増大しつつある。情報通信ネットワークの安全性及び信頼性を確保し、国民がこれを安心して利用することができるようにすることは、高度情報通信ネットワーク社会の形成にとって不可欠な条件であり、情報セキュリティの確保は喫緊の課題となっている。

情報セキュリティについては、①情報セキュリティに対する脅威の舞台であるインターネット等の情報通信ネットワークが社会・経済活動の根幹を担う存在であり、産業界等が発展させてきたものであること、②情報セキュリティに対する脅威に的確に対処するためには、急速に発展している高度な技術の活用が必要であること等から、情報通信ネットワークに関わる広範な層の協力によってこそ確保されるものであると言える。

それゆえ、情報セキュリティに関する警察の活動も、産業界を始めとする多くの関係者・関係機関との連携が不可欠である。情報セキュリティに関する産業界等と警察との連携については、都道府県レベルでは「プロバイダ連絡協議会」等を通じた各種の取組がなされていたものの､国レベルではかかる広範な官民連携の場が設けられていなかったところ、平成 13 年５月に東京で開催されたＧ８ハイテク犯罪対策・官民合同ハイレベル会合（東京会合）においては、産業界等と法執行機関との連携を各国内でも議論することの重要性が改めて確認された。

総合セキュリティ対策会議は、こうした状況を受けて、情報セキュリティに知見を有する各界の有識者による意見交換の場として開催に至ったものであり、当会議における議論が産業界等と警察による情報セキュリティ対策の参考となることを期待するものである。

【これまでの議題】

平成 13 年度	情報セキュリティ対策における連携の推進
平成 14 年度	情報セキュリティに関する脅威の実態把握・分析
平成 15 年度	官民における情報セキュリティ関連情報の共有の在り方
平成 16 年度	インターネットの一般利用者の保護及び知的財産権侵害に関する官民の連携の在り方
平成 17 年度	インターネット上の違法・有害情報への対応における官民の連携の在り方
平成 18 年度	インターネット・ホットラインセンターの運営の在り方及びインターネットカフェ等における匿名性その他の問題と対策
平成 19 年度	Winny 等ファイル共有ソフトを用いた著作権侵害とその対応策
平成 20 年度	インターネット上での児童ポルノの流通に関する問題とその対策
平成 21 年度	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

目　次

委員名簿

開催状況

今後の不正アクセス対策について

不正アクセス行為の禁止等に関する法律（平成 11 年法律第 128 号。以下「法」という。）は、高度情報通信社会の健全な発展に寄与し、「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」と「アクセス制御機能により実現される電気通信に関する秩序の維持」を図るため、不正アクセス行為の禁止、アクセス管理者による防御措置等を定めている。

しかしながら、法が施行されたこの 10 年間で、インターネット接続のブロードバンド化や情報利用端末としての携帯電話の利用拡大等を背景に、インターネットを利用した取引が日常的になるなど、インターネット上の社会経済活動が拡大している状況にある。

このように法をめぐる環境が制定時に比べて大きく変化する中で、法を所管している警察庁、総務省及び経済産業省は、法に定められている措置等によって、所期の目的であるインターネット上の犯罪の防止とアクセス制御機能の向上が図られているか、十分に検証すべき立場にある。

以上を踏まえ、平成 22 年度総合セキュリティ対策会議の下に設置された「不正アクセス対策分科会」では、不正アクセス行為やアクセス管理者の防御措置の現状等に対して、法所定の措置が現時点において立法目的に適った機能を果たしているかどうか運用状況の検証を行い、今後の不正アクセス防止対策の今後の在り方について議論したものである。

第１章　検証を行うに当たって

本項では、法の運用状況の検証を行うに当たり、法が制定された背景・経緯及びその概要を整理して、立法目的を明らかにした後、立法目的を踏まえた検証に当たっての視点を述べることとする。

１　法制定の背景・経緯

(1)　国内情勢の変化

日本国内では、平成５年にインターネットの商用接続サービスが開始されて以降、インターネットが一般の国民生活にまで広く浸透する[1]一方で、インターネット等の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（以下「サイバー犯罪」という。）[2]も増え始め、その検挙件数は、平成５年に警察庁が統計を取り始めてから、わずか５年後の平成 10 年には 10 倍以上に急増した[3]。

---

[1] サービス開始から５年後の平成10年には、インターネット利用者数は1,500万人を超えている（総務省「平成21年 通信利用動向調査」）。

[2] 過去には「ハイテク犯罪」と呼称していたが、国際的動向等を踏まえ、平成 16 年から「サイバー犯罪」と呼称することとしている。

[3] 検挙件数は、平成５年：32 件、平成６年：63 件、平成７年：110 件、平成８年：176 件、平成９年：262 件、平成 10 年：415 件と増加（警察庁 「平成 11 年 警察白書」）。

サイバー犯罪は、従来の犯罪とは異なり、匿名性が高いこと、地理的制約が少ないこと、被害の拡大が早いこと等の特性を有していることや、その被害や影響の程度に鑑みると、早期に未然防止を図る必要性が顕著といえ[4]、特に、サイバー犯罪を助長するとともにネットワークの秩序を乱す不正アクセス行為[5]については、企業や個人ユーザの間で、その規制を求める声が非常に高まっていた。

(2) 国際的な枠組みによる要請

国際情勢に目を向けると、サイバー犯罪は、容易に国境を越えて敢行することが可能なことから、各国が協調して対処することが当時の課題とされており、平成９年６月に開催されたデンヴァー・サミットでは、各国がサイバー犯罪対策に特に力を入れて取り組むことが合意された。これを受けた同年 12 月のＧ８司法・内務閣僚級会合においては、「ハイテク犯罪と闘うための原則と行動計画」が採択され、この結果は、翌年５月に、国際犯罪対策を初めて主要議題として取り上げたバーミンガム・サミットに報告の上、これを迅速に実施することについて各国の意見の一致がみられた。

(3) 法制定に向けた政府の取組

サイバー犯罪対策について国際的な機運も高まっていたこの当時、まだ国内では不正アクセス行為を禁止、処罰する法整備はなされていなかったため、このような国内外の諸情勢を背景に、警察庁では、長官官房長の私的懇談会である情報システム安全対策研究会の下に設けた不正アクセス対策法制分科会における研究を行ったほか、当時の郵政省や通商産業省との協議を進めるなど、不正アクセス対策法制の在り方について検討を行った。その結果、サイバー犯罪の防止と電気通信の安全・信頼性の確保を図るため、不正アクセス行為の禁止等に関する法律案が作成され、平成 11 年８月に国会において全会一致で可決・成立し、翌年２月に施行された。

２ 法の概要

法は、高度情報通信社会の健全な発展に寄与することを究極の目的としつつ、直接の目的として、「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」を掲げている（図１－１）。

「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」が定められてい

[4] 当時の主な検挙事例としては、銀行のオンライン・システムに不正指令を与えて巨額の資金移動を行った事例（電子計算機使用詐欺・愛知）や電子掲示板に虚偽の物品販売広告を掲示して多数の者から代金をだまし取った事例（詐欺・埼玉）等がある。

[5] 他人のＩＤ・パスワードを無断で使用し、電子計算機を使用できる状態にすること、又は電子計算機のソフトウェアの不具合等を悪用して、正当なＩＤ・パスワードなしに電子計算機を使用できる状態にすることをいう。

る理由は、ネットワークを使用したサイバー犯罪の被害や影響が重大かつ広範囲に及ぶことから、発生を未然に防止するための措置を的確に講ずる必要があるということである。また、「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」が定められている理由は、不正アクセス行為が横行すればアクセス制御機能[6]によって実現される電気通信に関する秩序が乱され、ネットワークの利用の不信感につながることにより、ネットワーク相互の接続が抑制されるおそれがあるということである。

(1) 不正アクセス行為の禁止、処罰

アクセス制御機能を有する特定電子計算機[7]に、電気通信回線を通じて、他人のＩＤ・パスワード等を入力して作動させ、その制限されている利用をし得る状態にさせる行為を不正アクセス行為とし、これを禁止、処罰するものとしている。

(2) 不正アクセス行為を助長する行為[8]の禁止、処罰

他人のＩＤ・パスワード等を提供する行為は、不正アクセスを行うための「道具」を提供することであり、これを入手した者が専門的知識・技術を有していなくとも容易に不正アクセス行為を行い得るようにする点で、これを放置すれば不正アクセス行為の禁止の実効性を損なうこととなるほか、このような提供行為には社会的有用性も認められないことから、不正アクセス行為を助長する危険のある他人のＩＤ・パスワード等を無断で第三者に提供する行為を禁止・処罰するものとしている。

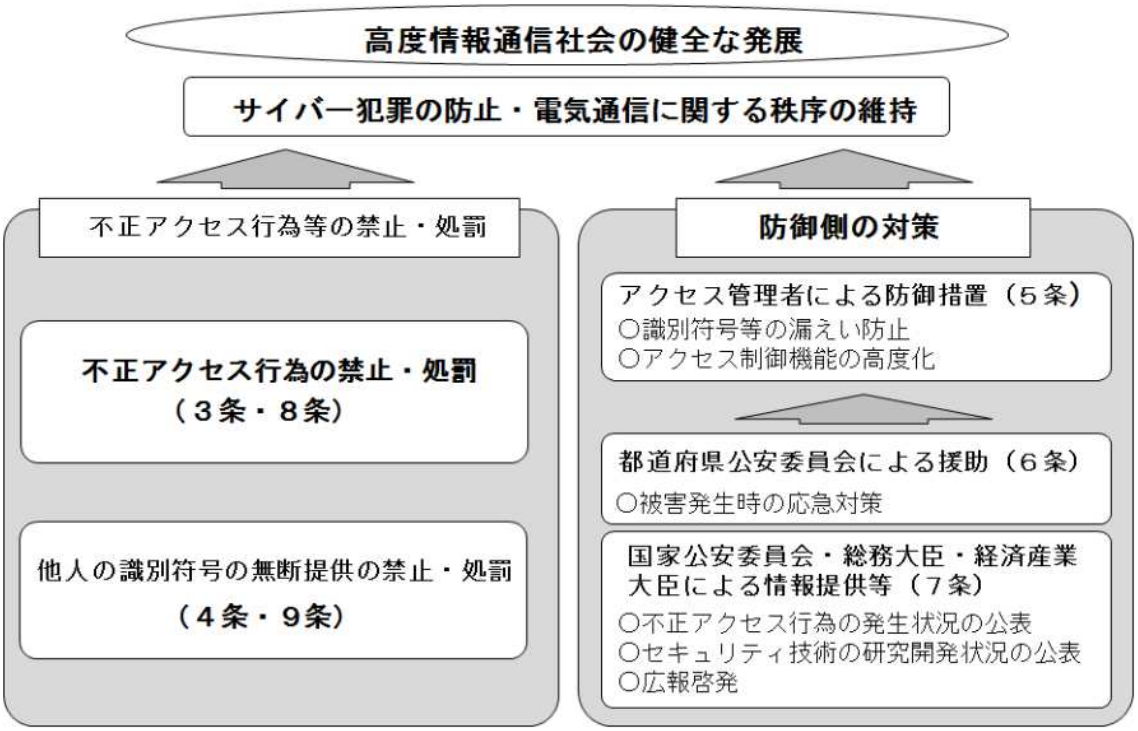
(3) アクセス管理者による防御措置

不正アクセス行為に対する防御措置は、これを講ずるアクセス管理者[9]が不正アクセス行為の被害に遭うことを防ぐだけではなく、当該アクセス管理者が管理する電子計算機にいったん不正アクセス行為をした上、これを踏み台とした他の電子計算機への不正アクセス行為を防止する効果が期待される。不正アクセス行為が行われにくい環境は、それぞれのアクセス管理者が不正アクセス行為に対する防御措置を適切に講じて初めて構築されることから、アクセス管理者は、ＩＤ・パスワード等の適正な管理に努めるとともに特定電子計算機を不正アクセス行為から防御するため必要な措置を講ずるよう努めるものとしている。

---

6 利用者にＩＤ・パスワードを入力させ、電子計算機を使用できるようにするための機能をいう。
7 電気通信回線に接続している電子計算機のことをいう。
8 他人のＩＤ・パスワードを知った者が、第三者にそのＩＤ・パスワードが使用できる電子計算機を明らかにしてＩＤ・パスワードを教示することをいう。
9 ネットワークに接続された電子計算機において、その利用対象や範囲を決定する権限を有する者をいう。

図１－１　不正アクセス行為の禁止等に関する法律（概要）



(4)　都道府県公安委員会による援助等

ア　都道府県公安委員会は、不正アクセス行為の被害に遭ったアクセス管理者に対し、その申出に基づき、再発防止のための援助を行うものとしている。

イ　国家公安委員会、総務大臣及び経済産業大臣は、毎年少なくとも１回、不正アクセス行為の発生状況等を公表するものとするほか、国は、不正アクセス行為からの防御に関する啓発及び知識の普及に努めなければならないこととしている。

３　検証の方法

(1)　検証の手順

運用状況の検証に当たっては、これまでの不正アクセス行為等（不正アクセス行為及び不正アクセス行為の新たな手口をいう。以下同じ。）の傾向を把握するために、不正アクセス事犯の検挙状況やその手口・動機について、法施行後 10 年間の推移を分析することとしたほか、アクセス管理者の防御措置や不正アクセス行為等の実態等を把握するため、開発者と利用者の側面を持つ民間事業者に対するヒアリングを実施することとした。

(2)　検証に当たっての視点

不正アクセス行為等に対しては、法所定の不正アクセス行為の禁止と不正アクセ

ス行為を助長する行為の禁止等の措置が、サイバー犯罪の防止とアクセス制御機能の向上という法の目的を達成する上で十分なものとなっているか検証するものである。特に、不正アクセス行為の新たな手口としてどのようなものがあるか、法所定の措置によって取締りが可能か、取締りを強化するための追加の措置が必要かという視点で検討することとした。

また、アクセス管理者が現在取り組んでいる防御措置については、現状の水準が法の目的を達成する上で十分なものとなっているか検証するものである。特に、アクセス管理者の防御措置の水準はどうなっているか、アクセス管理者の防御措置を向上しようとする意識は十分といえるか、これらの水準や意識を向上させるために必要な対策は何かという視点で検討することとした。

第２章　法施行後の運用状況

１　不正アクセス事犯の情勢

(1)　不正アクセス事犯の相談・認知・検挙状況

不正アクセス事犯の相談・認知・検挙状況の推移は、平成 12 年の法の施行以降、おおむね増加傾向にある（図２－１）。

ア　不正アクセス事犯の相談状況

不正アクセス事犯の相談件数は、これまで不可罰であった不正アクセス行為の処罰化やインターネット利用者の増加に比例するように、法の施行以降、その相談件数は年々増加していった。特に相談件数が平成 17 年、20 年に急増しているのは、フィッシング[10]やオンラインゲームへの不正アクセス事犯に関連するものが増加したからである。

しかしながら、不正アクセス行為の被害実態は統計に表れた数値に全て反映されるものではないことに注意しなければならない。なぜならば、不正アクセス行為の被害者はアクセス管理者であるものの、実際のアクセス者はＩＤ・パスワード等の利用権者であることから、アクセス管理者がその被害を自ら把握することは難しいほか、ＩＤ・パスワード等の利用権者が長時間利用しないことから不正アクセス行為に気付かない、又は金銭的な被害がないことからあえて警察に相談しないなどの理由により、被害が潜在化してしまうことが多く、暗数が相当数あると考えられるからである。

イ　不正アクセス事犯の認知・検挙状況

不正アクセス事犯の認知件数は、警察署等において受理した事件相談についてアクセス管理者に照会するなどの基礎捜査を実施した後に捜査を開始した事件と、検挙した事件の余罪とを計上したものである。一般的な刑法犯の認知件数は被害届の受理件数を意味するが、不正アクセス事犯の場合はＩＤ・パスワード等の利用権者から被害届を受理しないので、このような形で認知件数を表している。

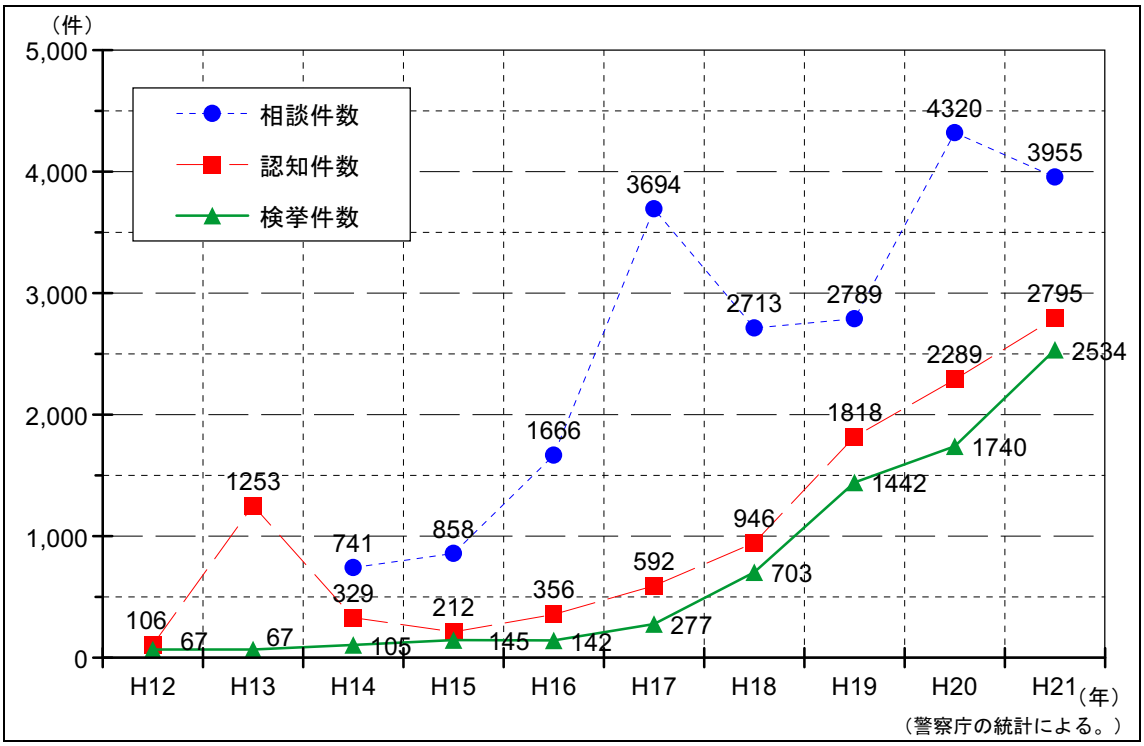
なお、平成 12 年から 13 年にかけて認知件数が急激に増加した理由は、コンピュータ・ウイルス[11]を使った不正アクセス行為が多発したからである。

他方、不正アクセス行為の相談の増加によってこれを端緒とした事件検挙も増加したことに伴い、検挙件数も右肩上がりの傾向を示している。特に、平成 19 年から 21 年の３年間の検挙件数の増加が顕著である理由は、フィッシングにより他人のＩＤ・パスワードを入手して不正アクセス行為に及んだ事件や、ＩＤから推測したパスワードを使用して不正アクセス行為に及んだ事件があり、これらの事件で余罪が 1,000 件を超える検挙があったからである。

10　第３章３(2)参照。

11　コンピュータに感染して利用者の意図に反する動作をするものをいう。

図２－１　不正アクセス事犯の相談・認知・検挙状況の推移



(2)　不正アクセス事犯の特徴（手口・動機）

不正アクセス事犯の手口・動機については、法の施行当初はハッカーと呼ばれる者が、自己の知名度を高めたり、技術の高さを他人に誇示するなど、不正アクセス行為そのものを動機とした、好奇心によるものも散見された。

しかし、おおむね平成 17 年頃からインターネット接続が従量制から常時接続へ移行したほか、接続料金が定額制になるとともに、銀行預金の送金やクレジットカード決裁を始め金融機関等がインターネットを利用したサービスを開始したことに加え、モバイル通信カード、インターネットカフェや私設私書箱等の犯行が匿名化できるツールが使用できるようになり、不正アクセス事犯の目的は、好奇心による不正アクセス行為そのものから不正にお金を得るための比率が急増していった。

発生した事件を分析した結果、現在は、フィッシング等により、他人のＩＤ・パスワード等を大量かつ不正に入手して、ネットショッピングを始めインターネット上の各種サービスを悪用して、財産上の不法な利益を得たり、商品をだまし取る金銭入手を動機とする犯罪が大多数を占めている（図２－２、２－３）。また、民間事業者からのヒアリング結果でも、不正アクセス行為の目的は、10 年前は愉快犯であったり、技術力の誇示等であったものが、事業者によって認識に若干の差異はあるものの、平成 17 年頃から、情報の不正取得やこれを端緒とした金銭目的に移行していることが多くの事業者から指摘されている。

図２－２－１　不正アクセス行為の手口（平成 12 年から 21 年）

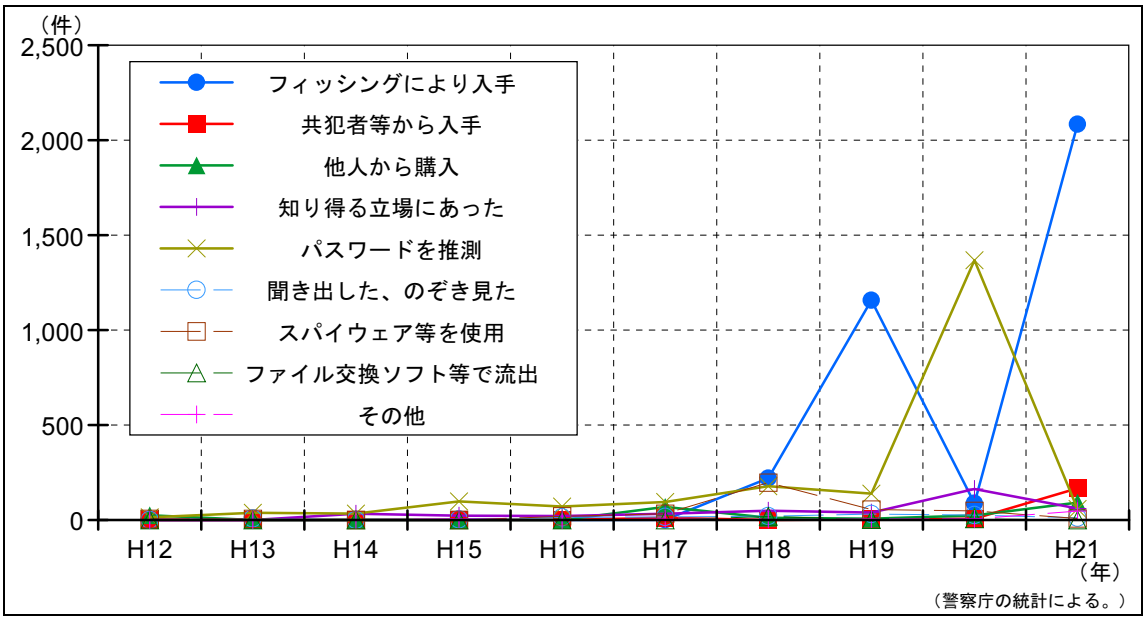


図２－２－２　不正アクセス行為の手口（平成 12 年から 16 年を拡大したもの）

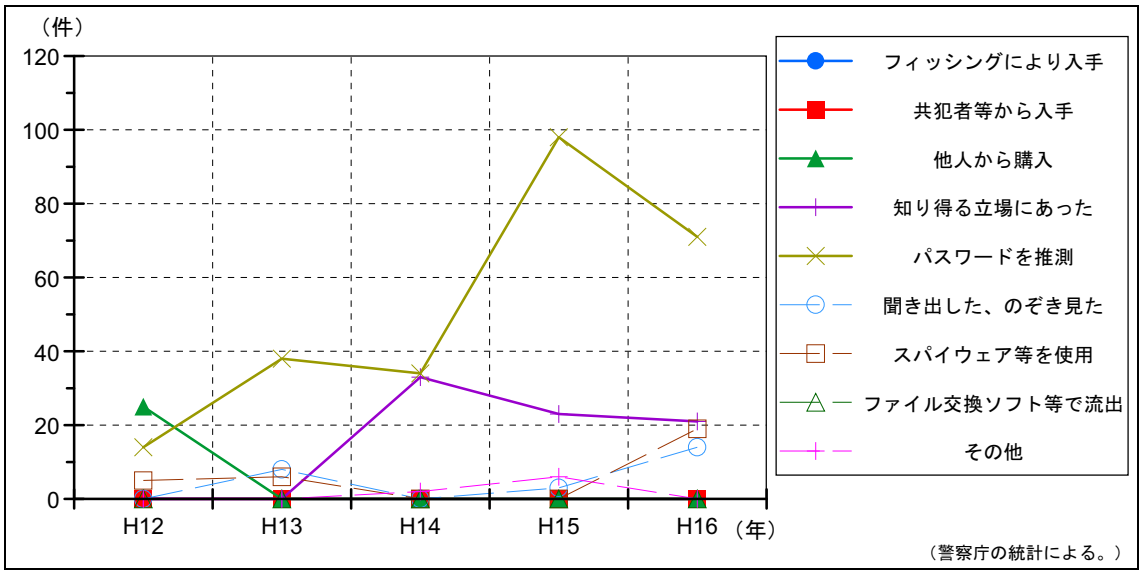


図２－３－１　不正アクセス行為の動機（平成 12 年から 21 年）

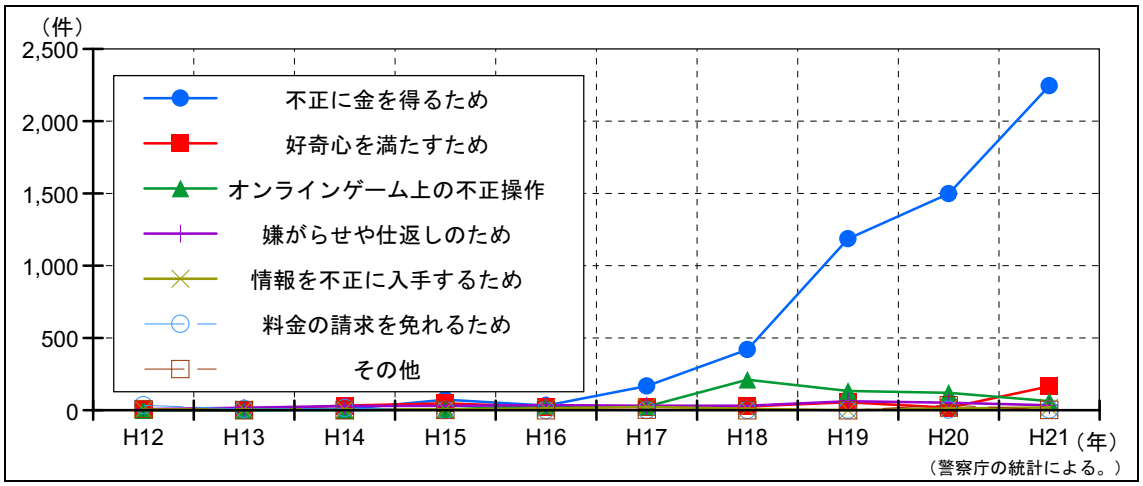
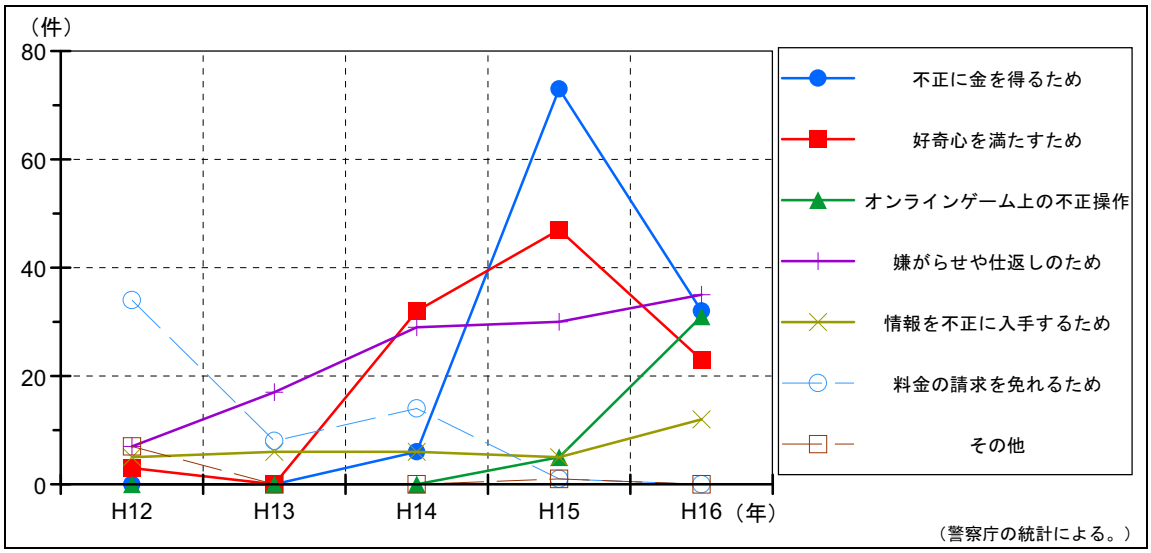


図２－３－２　不正アクセス行為の動機（平成 12 年から 16 年を拡大したもの）



(3)　まとめ

インターネット接続のブロードバンド化や企業・金融機関の取引等のオンライン化の急速な成長とあいまって、インターネットが国民生活の重要なインフラとして不可欠なものとなったことを背景に、不正アクセス事犯は増加傾向にあるほか、その特徴も変化してきている。不正アクセス事犯の相談件数については、法の施行以降、増加の一途をたどり、これに応じるように、検挙件数についても施行後 10 年で約 38 倍になるなど年々増加している。また、不正アクセス事犯の手口・動機については、好奇心を満たすためのものから、不正に金を得るためのものへと移行している状況にある。

なお、このような状況にあって、無線ＬＡＮやインターネットカフェの利用等による匿名化工作は、被疑者の追跡や特定を困難にするなど捜査上の著しい負担となっており、これを軽減して捜査環境を改善することも必要となっている。

2　アクセス制御機能の高度化等に向けた取組

(1)　国・公的機関における取組

国家公安委員会、総務省及び経済産業省では、法に基づき平成 13 年以降、不正アクセス行為の発生状況のほか、民間企業や大学等において実施されているアクセス制御機能に係る研究開発の状況について公表してきた。また、都道府県公安委員会においては、不正アクセス行為が行われたアクセス管理者による再発防止措置を支援するため、援助措置を行ってきた。

このほか、警察庁では、企業等のネットワーク上での不正アクセス行為等の現状等を把握・分析し、不正アクセス行為に対する防御措置に関する知識を高めることなどを目的として、平成 13 年以降、不正アクセス対策の実態等に関するアンケート調査を実施してきた。

また、（独）情報処理推進機構（ＩＰＡ。当時は情報処理振興事業協会）では、不正アクセス対策基準（平成８年通商産業省告示第 362 号）に基づき、不正アクセス行為の届出の受付が行われてきた。さらに、ジェイピーサートシーシー（JPCERT/CC）[12]では、コンピュータセキュリティインシデント対応や、コンピュータセキュリティ関連情報の発信等の取組がなされてきた。

(2)　民間における取組

法の施行以降、民間事業者では、不正アクセス行為を防止するため、又は不正アクセス行為を容易に認知できるようにするため、次のとおりアクセス制御機能の高度化等に関する様々な取組が行われてきた。

ア　アクセス管理者の取組

アクセス管理者は、法により、不正アクセス行為の発生を防止し、アクセス制御機能に対する信頼を確保することに一定の社会的責務を有する者であるといえる。インターネットを通じて各種サービスを提供している国・地方公共団体や民間企業等はもとより、自宅等でパソコンをインターネットに接続している国民一般も利用の形態によってはアクセス管理者になる可能性がある。

アクセス管理者の代表であるコンテンツ事業者等では、短いパスワードや誕生日等の安易なパスワードを禁止する仕組みをユーザに強制するなどの認証の強化、前回ログイン時刻の表示機能やログイン通知機能[13]の導入等が行われてきた。

その一方で、システムにセキュリティ上の不具合等が発見された場合、この対策を講じるための修正プログラム（パッチ）の提供がシステム開発者からなされ

---

[12]　インターネットを介して発生する侵入やサービス妨害等のコンピュータセキュリティインシデントについて、日本国内サイトに関する報告を受け付け、対応の支援、発生状況の把握、手口の分析、再発防止のための対策の検討や助言等を技術的な立場から行っている。

[13]　ログインが行われた際に、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。

ているが、黎明期には、アクセス管理者が業務の継続性を優先するために、パッチの適用が遅れたり、その適用自体がされなかったことも指摘されている。

イ　セキュリティ関連事業者等の取組

アクセス管理者による防御措置の高度化に関する取組を支援するために、セキュリティ関連事業が始まった。これに伴い、システムを不正アクセス行為等から防護するためのファイア・ウォール製品やコンピュータ・ウイルス対策ソフト等の普及が始まったほか、監視・監査サービス、Web アプリケーションを含むシステムのぜい弱性診断等のサービスも広く提供されるようになった。

(3)　まとめ

法の施行当時は、e-Japan 戦略（平成 13 年１月 22 日高度情報通信ネットワーク社会推進戦略本部決定）を始めとする国を挙げたＩＴ化の取組が始まろうとする時期でもあり、また、学術・研究機関を中心に発展してきたインターネットが生活の基盤として本格的に一般に普及することとなる転換期であったといえる。このような時期に、法は当時既に増加の兆候を見せていたサイバー犯罪の危険性に着目し、取締りと防御の両面からの取組を規定した画期的な法律であったといえる。

一方で、不正アクセス行為を始めとするインターネットの危険性については、一部の専門家では認識されていたものの、不正アクセス行為に対する対処についての考え方が必ずしも明確に定められたものはなく、このことは、法の施行当時におけるセキュリティサービスの利用状況や不正アクセス行為等を検知する対策の実施状況が低かったことからも裏付けられる（図２－４、図２－５）。

図２－４　セキュリティサービスの利用状況

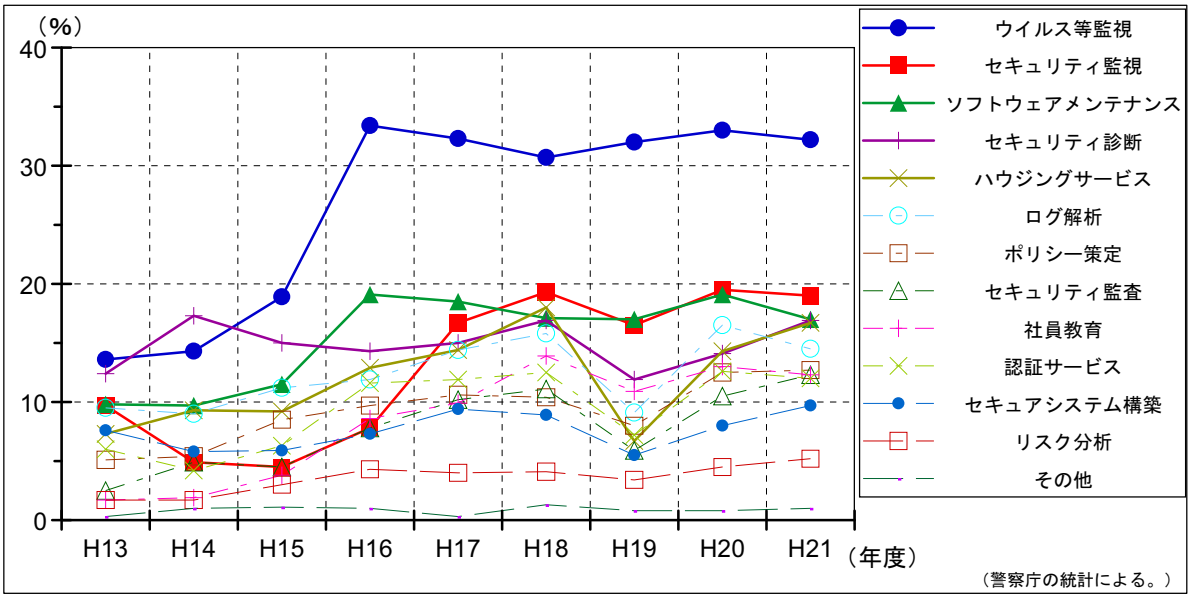
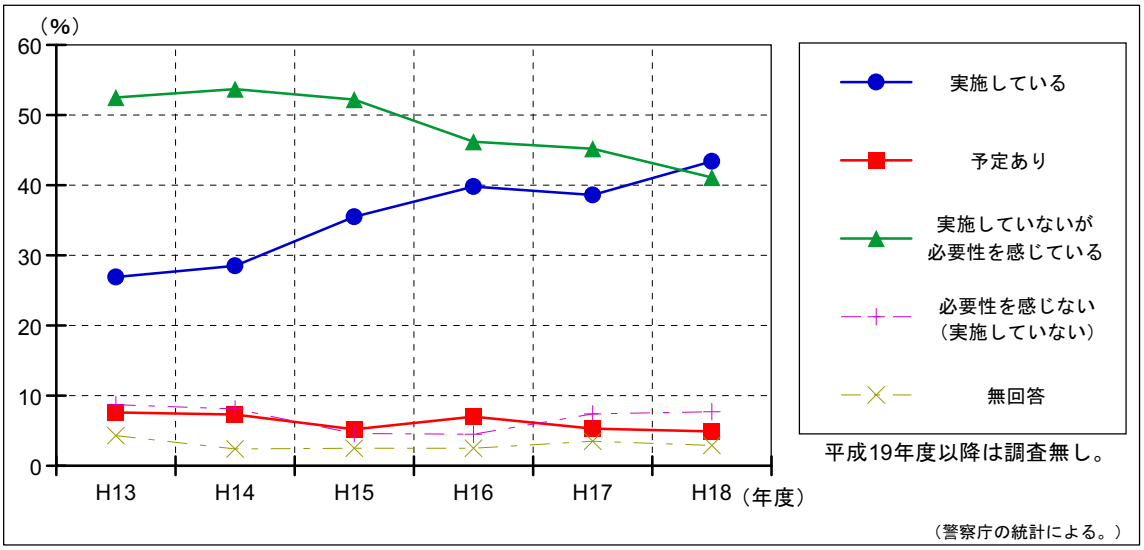


図２－５　不正アクセス行為等を検知する対策の実施状況



第３章　最近の情勢

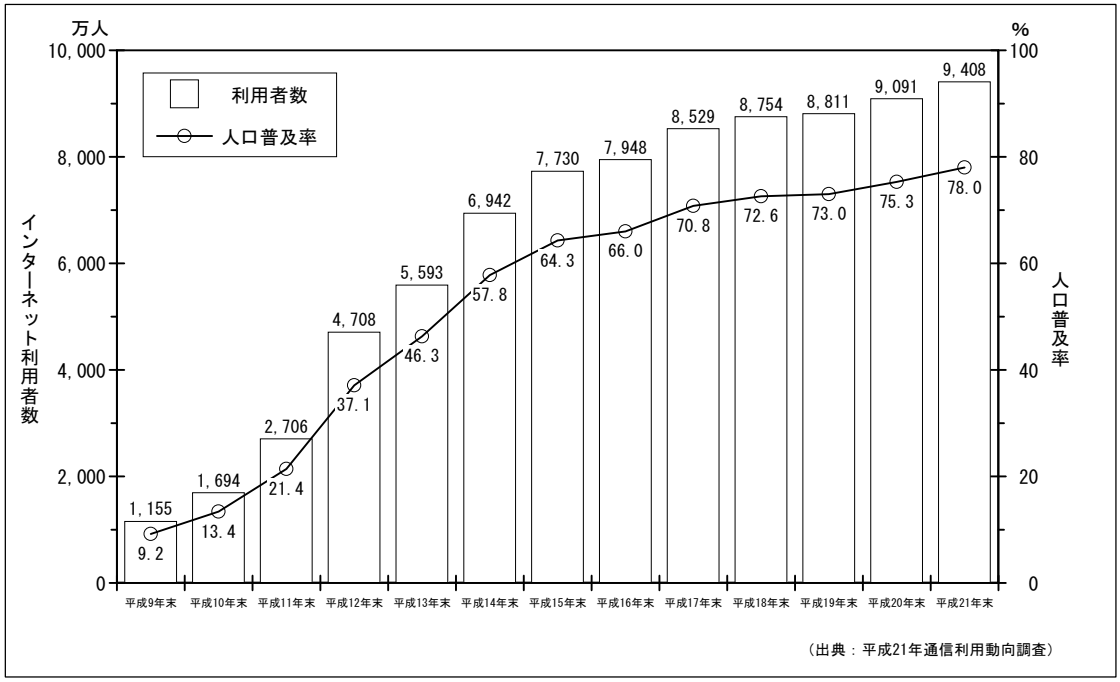
１　インターネットをめぐる最近の情勢

国内のインターネット利用者数は増加を続け、平成 21 年末には 9,400 万人を超えるとともに人口普及率は 78%となっている（図３－１）。「平成 21 年通信利用動向調査」によると、中でも 60 歳以上の世代におけるインターネット利用者数の伸びが顕著であり、若い世代だけではなく高年齢世代でもインターネットの利用が進んでいることがうかがえる。

インターネットの接続方法に目を向けると、電話回線や ISDN 回線といったナローバンド回線の利用が減少する一方、光回線やケーブルテレビ回線といったブロードバンド回線の利用が増加しており、大量の情報を短時間で送受できるブロードバンド化が着実に進展している。

また、携帯電話の世界においてもスマートフォンと呼ばれる高機能な携帯電話が登場しており、自宅や会社からだけでなく屋外からも場所を選ばずインターネットを利用できる環境が整いつつある。従来の携帯電話では、利用できるソフトウェアが携帯電話事業者から提供されるもの等に限られるとともに、インターネットへの接続も携帯電話事業者のサーバを経由して行う必要があったが、スマートフォンでは、一般の利用者が作成したソフトウェアをインターネットから直接ダウンロードして自由に利用できるほか、大きなディスプレイとタッチパネルを具備することで高い操作性を実現しており、携帯型のパソコンに匹敵する性能を有しているといえる。

図３－１　インターネット利用者数及び人口普及率の推移（個人）



このようにインターネットの利用者が増加するとともに、情報通信技術の進歩により大量の情報をどこでも容易に送受できる環境が整いつつある中、インターネット上には送金等を行うインターネット・バンク、商品取引を仲介するインターネット・オークションサイト、利用者同士で交流するコミュニティサイト、音楽を提供するサイト等が数多く存在し、これらを利用した経済活動も活発に行われている。また、政府や地方自治体のウェブサイトでは、住民生活に密着した行政サービスについて様々な情報提供が行われているほか、一部の行政手続はウェブサイトを介して電子的に行えるようになっている。さらに企業においても、テレワーク[14]や電子商取引、広告を掲載する手段として広くインターネットが利用されるなど、インターネットは国民生活に密接に関わると同時にその重要性も高まっている。

インターネットの利用が身近になる一方で、スマートフォンのサイバー犯罪への悪用や、クラウドサービス[15]の利用に起因する情報流出の発生等も懸念されている。スマートフォンについては高機能で拡張性があり、また、場所を選ばずインターネットを利用できることから、サイバー犯罪を行うための道具としても悪用されるおそれがある。また、海外では警察の取締りによる犯罪の抑止効果が十分には期待できない現状において、海外に情報システムを設置するクラウドサービスを利用した場合、情報システムから個人情報を始めとする機微な情報が流出する可能性が高まることも考えられる。

２　アクセス制御機能を取り巻く情勢

インターネットが国民生活に密接に関わるようになった一方で、サイバー犯罪を行いやすい環境も整ってきている中、次のようにアクセス制御機能を取り巻く情勢も変化してきている。

(1)　不正アクセス行為の手口の傾向等

民間事業者からのヒアリングによると、顧客に対するセキュリティサービスの提供やアクセス制御機能の高度化に係る技術開発、また、それらのために必要となる情報収集等によって把握された不正アクセス行為の手口の傾向等については、次の指摘がなされている。

ア　攻撃対象の変化

攻撃対象は、ＯＳ[16]を対象としたものからアプリケーションのぜい弱性を利用したものに推移している。これに加えて、不正プログラム等を巧妙にダウンロードさせ、更なる不正プログラムをダウンロードさせるなど、その攻撃手法の巧妙化とともに、目的を達成するため、攻撃を受けた者がそのことに気付かないよう

---

[14] 勤務先と自宅との間で電子メール等を利用して資料の送受や連絡を行うことによって、在宅勤務を行うことをいう。

[15] クラウドサービスを提供する企業が構築した情報システムに、システムを必要とする企業がインターネットを経由して接続することで、自前でコンピュータやソフトウェア等を調達せずに必要なシステムを利用できるものをいう。

[16] Operating System の略で、コンピュータシステム全体を制御するための基本ソフトウェアをいう。Microsoft Windows 等がこれに当たる。

な動作をするなど、動作の秘匿化も進んでいる。特に最近は、特定の対象からの情報を不正に取得すること等を目的とする標的型攻撃と呼ばれる手法が増加している状況にある。

イ　犯罪の組織化等

対応策が公表されていないぜい弱性を攻撃する、いわゆるゼロデイ攻撃が多くみられるとともに、ウイルス作成等を容易にするためのツールが販売されている状況を踏まえると、これらの攻撃が組織的に行われている状況がうかがえる。

国際的には、攻撃の組織化が進んでいるだけでなく、各組織が専門的に分化している状況（例えば、ツールの作成を行う組織、ボットネット等のインフラ基盤を販売する組織、実際に情報を不正に取得する組織、情報を悪用して金銭を取得する組織等）があるように見受けられる。

このような傾向は、我が国では未だ見受けられていないものの、経済的価値観の相違や言語の壁等の要因がなくなった場合には、我が国においてもこのような犯罪の組織化が懸念される。

(2)　アクセス管理者による防御措置の現状

ア　防御措置の高度化に関する開発状況等

民間事業者では、近年、第２章２(2)で述べた対策が講じられてきたほか、システムの構築を行う立場としては、ＳＱＬ[17]インジェクション攻撃対策のための社内のガイドブックの作成、機械によるソースコードのチェックの実施等による不正アクセス行為等の防止のための取組がなされている。

さらに、ＯＳ等の開発者では、ぜい弱性に関係する情報を収集し、その情報を提供するための体制を構築しているほか、開発段階から防御措置を考慮した設計を行うなどにより、不正アクセス行為等による攻撃を受けにくいＯＳ等の開発に努めている。

また、セキュリティ製品においては、個別攻撃ごとの対応から攻撃手法を分析・評価することにより、より包括的な対応ができるような仕組みが導入されている。

イ　アクセス管理者等の取組

アクセス管理者では、ファイア・ウォール製品やコンピュータ・ウイルス対策ソフトが普及を見せているほか、民間のセキュリティサービス事業者の利用状況も増加傾向にあるなど、その防御措置に係る意識の向上により、その対策が講じられている面も見受けられる（図２－４、図２－５）。

また、近年、同一のＩＤ・パスワードを複数のサイトで使い回すことにより、

[17] Structured Query Language の略で、データベースの構造設計やデータの検索、更新等を行うためのプログラム言語の一種をいう。

セキュリティ対策が不十分なサイトからＩＤ・パスワードが流出する危険性があることから、OpenID[18]の利用に向けた取組も始められている。しかしながら、セキュリティ製品等を導入するだけで対策が万全であるといった過信が見受けられるほか、中小企業では、防御措置が外部委託先に完全に委任される傾向にあることから、防御措置についての主体性が欠如していることについては、ほとんどの事業者から指摘されている。

ウ　課題

ヒアリングを実施した民間事業者からは、中小企業のアクセス管理者における不正アクセス行為等からの防御措置に関する意識は概して低いことが指摘されている。その理由として、自分だけは被害に遭わないという誤った認識や、被害を受けた際にどのような対策を講ずべきか分からないという知識不足等が挙げられている。また、システム構築において、費用不足や納期の逼迫により防御措置の向上が要件から除外されてしまう傾向にあるとされている。

民間事業者からは、これらの意識の低い者が全体のセキュリティの穴となることから、こうした者に対する防御措置向上のための方策が必要であるとの意見が多くなされている。

(3)　国・公的機関による取組

経済産業省では、ソフトウェア等脆弱性取扱基準（平成 16 年経済産業省告示第 235 号）を制定し、ＩＰＡや JPCERT/CC によるぜい弱性情報の共有やコンピュータ・ウイルス、不正アクセス行為等による被害を防止するための枠組みを構築している。

また、総務省及び経済産業省が民間事業者等と連携して、ボットに係る情報を一般のユーザに提供し、ボットに感染したユーザに対策手法を提供してボットの駆除を促進する取組（サイバークリーンセンター）が行われている。

このほか、フィッシングに関しては、フィッシング対策協議会が設立され、フィッシングに関する情報収集・提供、動向分析、技術・制度的対応の検討等の取組がなされている。

(4)　新技術への対応

インターネットに関連する技術革新は著しく、新技術に関連した対策については、今後も継続的に動向を注視していく必要がある。

携帯電話におけるスマートフォンの普及や、インターネット接続が可能なゲーム機やテレビ等の家電の増加に伴い、こうした機器を対象とした攻撃の可能性が指摘

[18] 対応した複数のウェブサイトにおいて、共通のＩＤ・パスワードで利用できる仕組みをいう。ＩＤ・パスワードの情報は発行者のみが管理し、対応したウェブサイトでは、発行者から正規の利用者であることの確認を受けることにより、その利用の認証を行う。

されている。

また、様々な企業がクラウドサービスを提供しているにもかかわらず、これに関する防御措置の基準については確立されたものがないといわれているため、今後、このサービスを利用する側において、このサービスを提供する者による防御措置の状況を見極める仕組みも必要であると考えられる。

(5) 今後対応が必要と考えられる事項

このように、官民による防御措置に係る取組は着実に進んでおり、大企業等では、必要な費用を投じて防御措置を講じることにより高い水準を維持していると評価することができる。しかしながら、中小企業や一般ユーザの多くは、防御措置への関心や知識の不足、必要な費用投入を惜しむこと等により、防御措置が浸透していない状況にある。

コンピュータ・ネットワークが高度に発展し、その重要性が飛躍的に高まった現在、不正アクセス行為の被害は、単にそのシステムだけの問題ではなく、第三者に与える負の影響が極めて大きいといえる。このため、防御措置に関する水準の差により生じる不正アクセス行為等に対する抵抗力の格差は、ネットワーク全体のぜい弱性につながり、ネットワーク上の危険や脅威を増大させる結果となっている。今後は、不正アクセス行為等に対する抵抗力を高めるためにも、防御措置に関する水準を全体的に底上げする必要があると考えられる。

3 法施行後に出現した新たな手口

インターネット環境やアクセス管理者の防御措置を脅かすものとして、法の施行後に出現した不正アクセス行為に関する新たな手口が問題となっている。

(1) ドライブバイダウンロード攻撃[19]

情報通信技術の発展に伴い、コンピュータ・ウイルスやスパイウェア[20]を利用したＩＤ・パスワード等の収集手口も高度化してきている。

コンピュータ・ウイルス等によってＩＤ・パスワード等が流出する事案は以前から発生していたが、これまでは被害者がコンピュータ・ウイルス等を自ら実行しない限り、コンピュータ自体に感染することはなく、怪しいプログラムを実行しないことによって感染を防ぐことが可能であった。

しかしながら、悪意のある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新たな攻撃（ドライブバイダウンロード攻

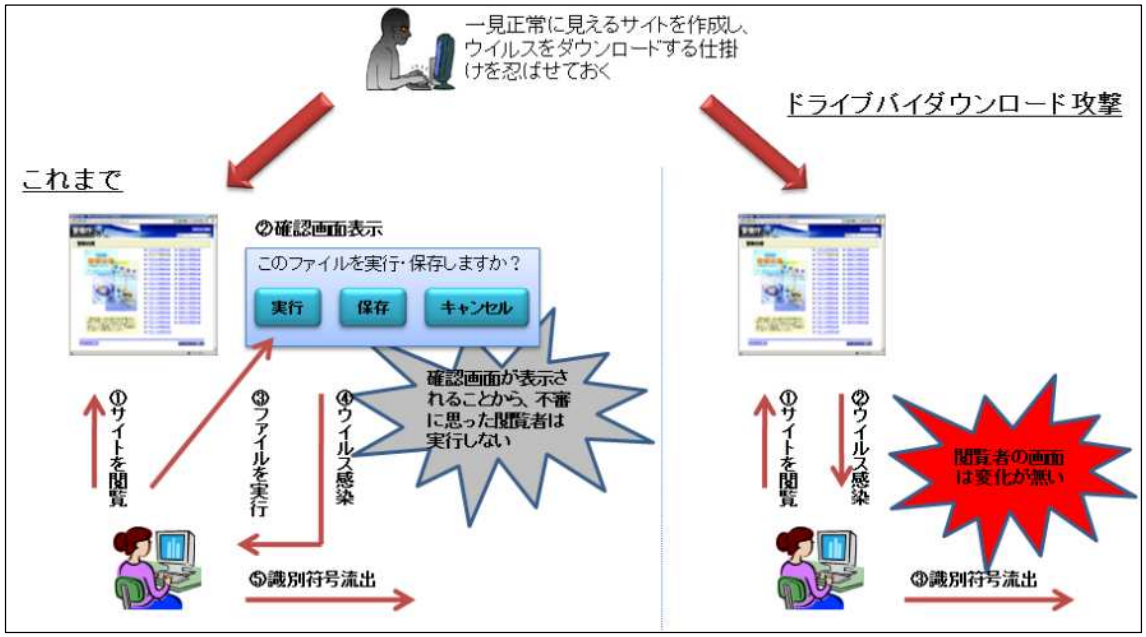
[19] Drive-by download attack：ウェブブラウザを介してユーザに気付かれないように、ウイルスやスパイウェア等をダウンロードさせる行為のことをいう。

[20] コンピュータのハードディスク等に記録された情報やキーボードの捜査情報、表示画面の情報等を外部に流出させるものをいう。

撃。図３－２）の出現により、利用権者が全く気付かないうちにＩＤ・パスワード等が流出してしまうことにつながる可能性が出てきている。特に、平成 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コンピュータ・ウイルスを感染させ、ウェブサイト管理用のＩＤ・パスワード等を入手後、そのウェブサイトを改ざんするというものであった。このため、コンピュータ利用者が全く気付かないままＩＤ・パスワード等が流出し、大手企業等のウェブサイトが改ざんされる被害が多発した。

この攻撃の防止策として、パスワードを他人に読み取られても問題のないワンタイムパスワード（使い捨てパスワード）の導入や、ＩＤ・パスワード等の流出のおそれのない指紋認証や静脈認証等の生体認証が導入され始めている。

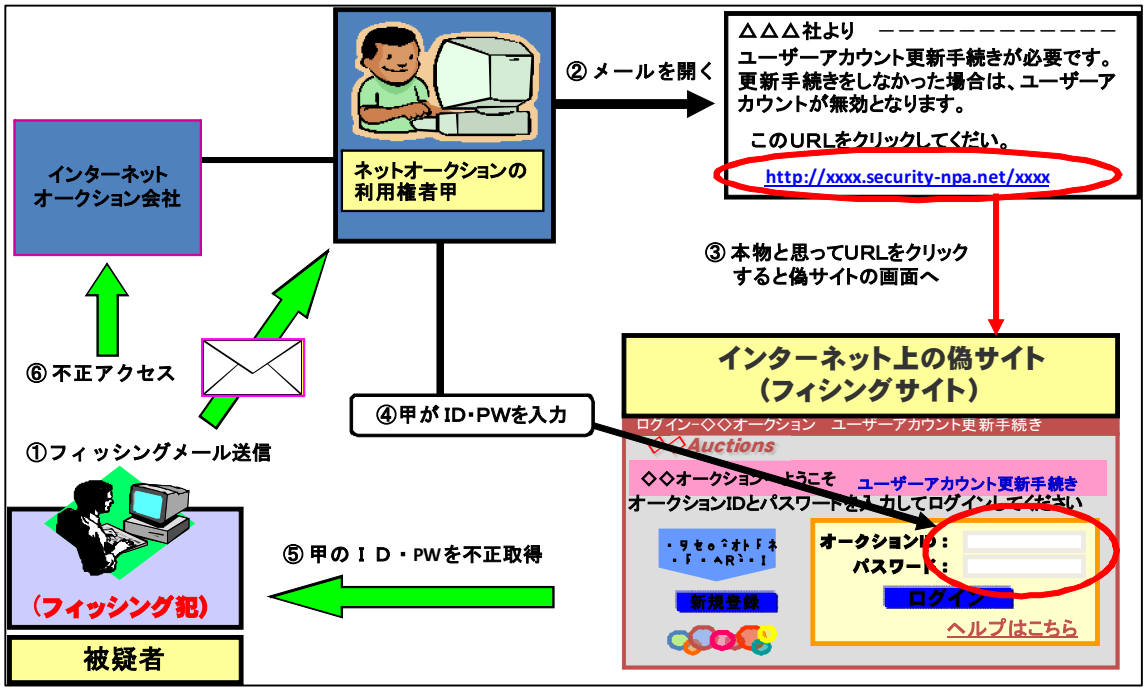
図３－２　ドライブバイダウンロード攻撃の概要



(2)　フィッシング

フィッシングとは、実在する企業を装ってメールを送り、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）をメール受信者が閲覧するよう誘導し、そのサイトでＩＤ・パスワード等を入力させてこれらの情報を不正に入手する手口をいう。

図３－３　フィッシングの概要



これにより、フィッシングサイトを立ち上げて大量にメールを送信することによって、短時間に大量のＩＤ・パスワード等を収集することが可能となる。加えて、フィッシングサイトに入力した者は本物のサイトに入力したと誤信していることから、ＩＤ・パスワード等が悪用されるまでフィッシングの被害に遭ったことに気付かないため、被害を申告した際には既に被害が拡大してしまっている状況にある。

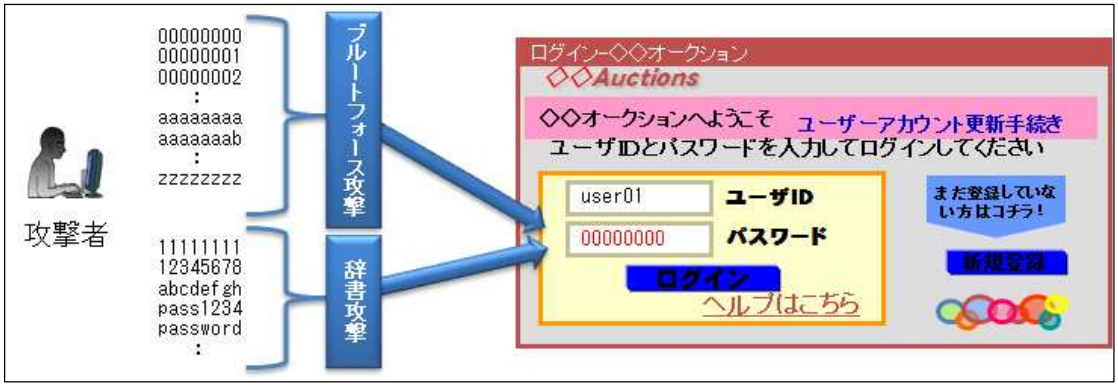
そこで、フィッシングの早期把握と被害防止を図るため、各都道府県警察ではフィッシングに係る情報提供を受け付けるための窓口である「フィッシング１１０番」を設置している。他方、民間事業者では、フィッシングに関する情報収集・提供・注意喚起等の活動を目的とした「フィッシング対策協議会」を設立することによりその対策に取り組んでいる。

しかしながら、フィッシングによるＩＤ・パスワード等の収集は、法の制定当時には想定していなかった手口であり、ＩＤ・パスワード等を収集する行為自体を直接取り締まることができないことから、その立件には苦慮しており、フィッシングサイトの内容によって著作権法違反等を適用して立件している状況である。また、フィッシングも当初はＩＤ・パスワードの収集が中心であったが、最近は、これに加えてクレジットカード情報等を収集するようになるなど、収集したデータから容易に金銭が取得できるようなものを標的とした攻撃に変化している状況にある。

(3)　ブルートフォース攻撃

ブルートフォース攻撃とは、パスワードとして利用可能な文字列の組合せを、自動入力プログラムを使用して最初から一つずつすべて試すことにより不正アクセス行為を行う手口で、総当たり攻撃とも呼ばれる。また、同様の手口として、パスワードに使われそうな単語を集めた辞書を用意し、辞書の文字列を自動入力プログラムを使用して適当に入力する辞書攻撃と呼ばれる攻撃もある。

図３－４　ブルートフォース攻撃の概要



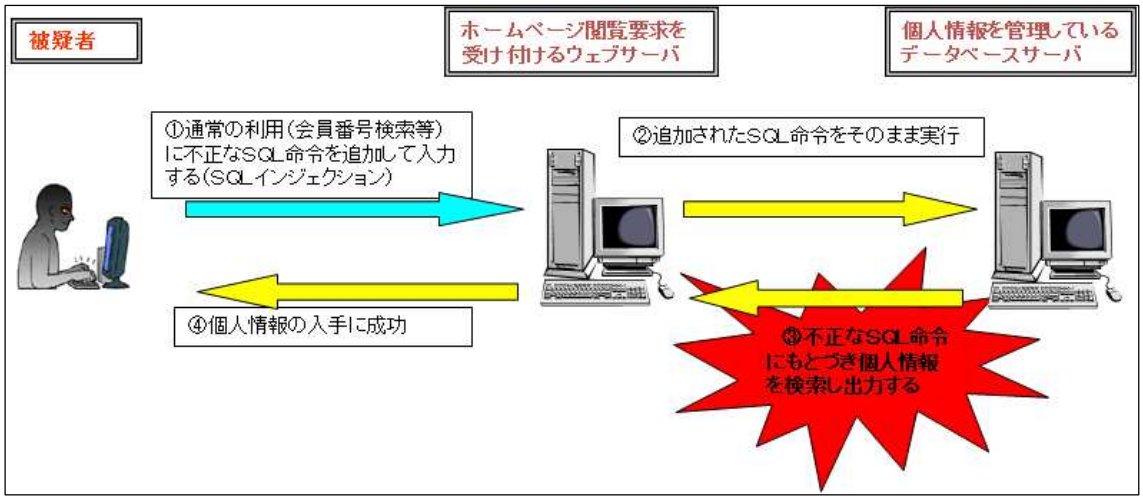
この攻撃には、短時間に同一のユーザＩＤに対して同一の発信元から複数回のログインが試行された場合に、ブルートフォース攻撃の可能性が高いと見なして、数回連続してログインに失敗した時点で該当ユーザＩＤをロックするなどのシステムによる対策が取られている。

しかしながら、最近では、ボットネットを利用して複数の発信元からログインを仕掛け、システムで検知されないようにする高度化されたブルートフォース攻撃が出現している状況にある。

(4)　ＳＱＬインジェクション攻撃

ＳＱＬインジェクション攻撃とは、データベースからデータの検索や更新等を行うためのプログラム言語であるＳＱＬ命令を不正に追加することにより、データベースから情報を収集する手口をいい、これにより、大量のＩＤ・パスワードやクレジットカード情報が流出する事案が発生している。

図３－５　ＳＱＬインジェクション攻撃の概要



この攻撃を受けるとデータベースに存在する全ての情報が収集される可能性があり、注意が必要である。実際には１回の攻撃で十万件以上のクレジットカード情報が流出した事案も把握されており、一度の攻撃で大きな被害が発生する非常に危険な攻撃手法であるといえる。

この攻撃は、通常手当たり次第に接続確認による攻撃を行って、攻撃可能なサーバを探し出した後、情報取得のための攻撃を行う場合が多いことから、接続確認による攻撃の段階を敏感に察知し、情報取得のための攻撃がされ、実際に情報が盗まれる前の段階で防御措置を講じることが重要である。他方で、最近は一見してこの攻撃と判明しないようにＳＱＬ命令の難読化が施される手口も出現していることから、注意が必要である。

第４章　不正アクセス防止対策の今後の在り方

１　基本的考え方

法の施行以降、不正アクセス事犯は増加しており、特にここ数年の増加傾向は顕著である。また、不正アクセス行為に関する新たな手口も発生しているほか、その手口も巧妙化が進んでいる状況にある。一方で、現在の法においては、不正アクセス行為が成功しない限りこれを処罰することができない。しかしながら、企業等により保有されている個人情報等の量が増加しつつある中、不正アクセス行為を受けることは、これら個人情報等の流出に直結すると言っても過言ではなく、その被害は甚大なものとなる。

したがって、このような状況に対応するには、警察による取締り強化とアクセス管理者による防御措置の強化という両輪の対策が必要不可欠である。

２　新たな手口への対応等

法制定当時に比して多くのサービスが提供され、様々な情報がインターネットを通じてやりとりされるようになるなど、現在は国民生活や社会経済活動のインターネットへの依存度は高まっている。不正アクセス行為が及ぼす影響が増大するなど、アクセス制御機能により実現されるインターネットに対する信頼性を確保する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ついて、電気通信に関する他の犯罪との均衡も勘案しつつ、法の罰則の法定刑の引上げについて検討する必要がある。

また、不正アクセス行為に関する新たな手口やコンピュータ・ネットワークをめぐる情勢の変化により、不正アクセス行為が既に敢行された後に検挙しても、検挙までの間に情報の流出や金銭的損害等の被害が拡大してしまう。しかしながら、現行の法では、実際に不正アクセス行為が成功しない限り検挙できないという限界がある。そのため、新たな手口に関してその危険性を捉え、法の目的である「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」の観点から、不正アクセス行為に至る前の段階で防止することが必要である。

(1)　フィッシング

現在、多くのシステムにおいては、アクセス制御機能により利用権者を識別し、認証するための識別符号として、ＩＤ・パスワードが採用されている。ＩＤ・パスワードは、法において他に識別符号として規定されている生体情報や署名と異なり、何らかの理由により利用権者以外の者にも知られ得るものである。ＩＤ・パスワードが他人に知られた場合、原理的にはこれを利用した不正アクセス行為を防ぐ手段はないと言ってよい。

そのため、法においては、他人のＩＤ・パスワードを第三者に無断で提供する行為が不正アクセス行為を容易にすることの危険性に着目して、これを禁止しているところである。

フィッシングは、正規の Web サイト等であるとユーザに誤認させ、いわばＩＤ・パスワードをだまし取る行為である。フィッシングの目的がだまし取ったＩＤ・パスワードにより他人になりすまして不正に金銭を取得することであること、更に、このＩＤ・パスワードを悪用した不正アクセス行為は、前述のとおり防ぐことが困難であること等から、不正アクセス行為を誘発する危険な行為であると言える。

少なくとも当面の間は、ＩＤ・パスワードによる認証は主流であると考えられるため、フィッシングによるＩＤ・パスワードの不正取得を防止する方策について検討する必要がある。

(2)　ＳＱＬインジェクション攻撃

ＳＱＬインジェクション攻撃については、成功した場合には、現行法違反（第３条第２項第２号）に該当し得るものである。しかしながら、ＳＱＬインジェクション攻撃の成功は、そのデータベース内の情報がすべて流出し得ることを意味し、その危険性とこれによる被害は極めて大きいと言える。

また、ＳＱＬインジェクション攻撃は、システムのぜい弱性を診断する目的でアクセス管理者自ら、又は事業者等に委託して実施する場合を除き、およそ正当な目的で実施されることは想定しがたい。

そのため、ＳＱＬインジェクション攻撃について、対応する方策について検討する必要がある。

３　アクセス管理者による防御措置の向上等

(1)　アクセス管理者による防御措置の向上方策

法の制定時点においても、いわゆる踏み台とされて他のコンピュータに対する不正アクセス行為がなされる危険性については認識されており、こうした行為を予防するため、アクセス管理者による防御措置が責務として規定されているところである。

現在においても、この危険性は何ら変わっていないことに加え、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により、企業においては、個人情報等を保有することが多くなり、不正アクセス行為に引き続き、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などの状況にある。特に不正アクセス行為の目的が金銭目的に移行し、その手口が潜行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、不正アクセス行為から派生する金銭的な被害を防止する上でも、根本的な対策であると言うこと

ができる。法においても、アクセス管理者の努力義務として、識別符号の適正な管理、アクセス制御機能の有効性の検証・高度化、その他不正アクセス行為から防御するために必要な措置を講ずることが定められている。

これを受けて、第２章及び第３章で述べられたとおり、民間においては、不正アクセスを防止するため、アクセス制御機能の高度化に関する取組が行われてきたところである。しかしながら、中小企業や一般のユーザにおけるセキュリティ対策は万全とは言えない状況にある。これには、一般のアクセス管理者に不正アクセス行為の実態に関する情報が提供されていないことが一因であると考えられる。

電気通信の秩序の維持に関しては、有線通信及び無線通信においては、それぞれ有線電気通信法及び電波法に基づき法令により規格化されており、これによって電気通信の秩序の維持が図られているところであるが、アクセス制御機能に関しては、民間主導でなされてきたインターネットの発展の経緯から、法令で規格を定めることになじまない性質のものである。一方で、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。そのため、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。

(2)　ログの保存の在り方に係る継続的な検討

不正アクセス行為は、典型的なサイバー犯罪であり、基本的にログ以外に痕跡がほとんど残らないことから、不正アクセス行為を発見、防止するためには、ログを保存し、定期的にチェックすることが不可欠である。そのため、不正アクセス禁止法の制定時には、警察庁が公表した「不正アクセス対策法制の基本的考え方」において、不正アクセス行為の発見・防止上の必要性と負担とのバランスを考慮した必要最小限度として、罰則、担保措置を課さないこととした上で、３項目（日時、ＩＤ、ＩＰアドレス）を３か月保存することを義務づけることについて、提案され、パブリックコメントに付されたところである。

ログの保存義務については、ログの保存義務を課さないこととすることなどを盛り込んだ「電気通信システムに対する不正アクセス対策法制の在り方」を発表した郵政省（当時）との調整を経て、最終的には法に盛り込まれなかったものの、国際動向を踏まえ引き続き検討することとされたところである。第５条においてアクセス管理者の責務として規定された、不正アクセス行為からの防御措置の内容として、「アクセス制御機能の有効性を検証」することが規定されており、コンピュータの動作記録であるログを一定期間保存して定期的に当該アクセス制御機能が有効であるか否かを判断する以外に一般的に有効な方法・手段がない以上は、ログの保存とアクセス制御機能の有効性の検証とは不可分一体のものということができ

る。

民間事業者へのヒアリングや都道府県警察へのアンケートの結果によると、大手通信事業者等においては、課金や苦情対応等のために、一定期間ログを保存している実態も見受けられ、こうした状況や諸外国におけるログの保存義務に係る動向等を踏まえつつ、ログの保存の在り方については、引き続き検討していく必要があると考えられる。

4　官民の意見集約を通じた不正アクセス対策の検討・充実

本分科会としては、不正アクセス対策の今後の在り方について以上のような結論を提示するところであるが、不正アクセス行為の実態については、情報通信技術に係る最新の動向を踏まえる必要があるため、不正アクセス防止施策の実施を検討する際には、官民が一体となって意見集約を行い、実施しようとする施策の内容を更に掘り下げ、充実させることが重要である。

すなわち、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、不正アクセス行為に係る実態の把握が不可欠なのであり、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し、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。また、不正アクセス行為に係る実態の把握を踏まえ、官民それぞれの立場において有する知見を元に現状分析を行い、問題点を抽出するとともに、関係者においてこの問題点を共有し、講ずべき対策についての共通認識を持つことが重要である。こうした共通認識に基づいて、不正アクセス防止対策の官民の役割分担や連携施策の実施が検討され、実施されていくことが適切である。

警察庁においては、今後、総務省、経済産業省、関係民間事業者と共に不正アクセス行為の防止のための官民意見集約委員会を立ち上げることとしているところであり、本分科会としては、同委員会において、本報告書を踏まえ、新たな手口への対応方策やアクセス管理者による防御措置の具体的向上方策についての議論が深められ、そこで結論が得られた施策が速やかに実施されていくことを期待する。

今後のインターネット上の違法・有害情報対策について

平成 22 年度総合セキュリティ対策会議の下に設置された「違法・有害情報対策分科会」では、「今後のインターネット上の違法・有害情報対策について」を課題として議論を行った。インターネット上の違法・有害情報の現状や問題点、とりわけ、現時点でインターネット上の違法・有害情報対策の中心となっているインターネット・ホットラインセンター[1]（以下「ＩＨＣ」という。）によるホットライン業務の現状や問題点について議論を重ねる中で、違法・有害情報に対処するためには、インターネット上にサービスを提供している事業者（サイト管理者、サーバー管理者及びプロバイダを指す。以下「サイト管理者等」という。）[2]のみならず、警察やＩＨＣも含めて、社会の連帯責任として、それぞれの立場で、また、それぞれが連携・協力して取り組まなければならない課題であるとの認識に至った。

本分科会では、ＩＨＣで取り扱う違法・有害情報（図１－１）がインターネット上の様々な情報の中でも、特に違法性や危険性が高いものであることから、その取扱いを主な対象として議論を行ったものであり、本報告書では、これらの議論の結果を踏まえ、違法・有害情報の現状とこれらに対する関係者の取組について述べた後、その問題点を明らかにした上で、ＩＨＣへの通報を活性化させるための方策、違法・有害情報に対処するためのサイト管理者対策について提言することとする。

図１－１　ＩＨＣが取り扱う違法・有害情報の類型

違法情報

① **わいせつ物公然陳列**（刑法第175条）
② **児童ポルノ公然陳列**（児童ポルノ法第７条第４項）
③ **売春周旋目的の誘引**（売春防止法第６条２項第３号）
④ **出会い系サイト規制法違反の禁止誘引行為**（同法第６条）
⑤ **薬物犯罪等の実行又は規制薬物**（覚せい剤、麻薬、向精神薬、大麻、あへん及びけしがら）**の濫用を、公然、あおり、又は唆す行為**（麻薬特例法第９条）
⑥ **規制薬物の広告**（覚せい剤取締法第２０条の２、麻薬及び向精神薬取締法第２９条の２及び第５０条の１８、大麻取締法第４条第１項第４号）
⑦ **預貯金通帳等の譲渡等の誘引**（犯罪収益移転防止法第２６条第４項）
⑧ **携帯電話等の無断有償譲渡等の誘引**（携帯電話不正利用防止法第２３条）

有害情報

① **情報自体から、違法行為**（けん銃等の譲渡等、爆発物の製造、児童ポルノの提供、公文書偽造、殺人、脅迫等）**を直接的かつ明示的に請負・仲介・誘引等する情報**
② **列挙する違法情報について、違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度認められる情報**
③ **人を自殺に誘引・勧誘する情報**（集団自殺の呼びかけ等）

[1] 平成 18 年６月以降、インターネット上の違法・有害情報に関する通報を受理し、警察への通報、サイト管理者等への削除依頼を行うホットライン業務を警察庁から民間に委託して運用している。詳しくは第２章第１の４参照。
[2] 違法・有害情報の書き込みに対して、削除する権限を有するものを想定している。

第１章　違法・有害情報の現状

近年におけるインターネットの国民生活への浸透はめざましく、国内のインターネット利用者（以下「利用者」という。）の数は増加を続け、平成 21 年末には利用者数が 9,400 万人を超えるとともに人口普及率（利用率）は 78%となっている。この背景には、光回線やケーブルテレビ回線といった大量の情報を短時間で送受信できるブロードバンド回線の整備によるブロードバンド化の着実な進展とともに、携帯電話やスマートフォン等のモバイルインターネット環境の急速な普及がある。

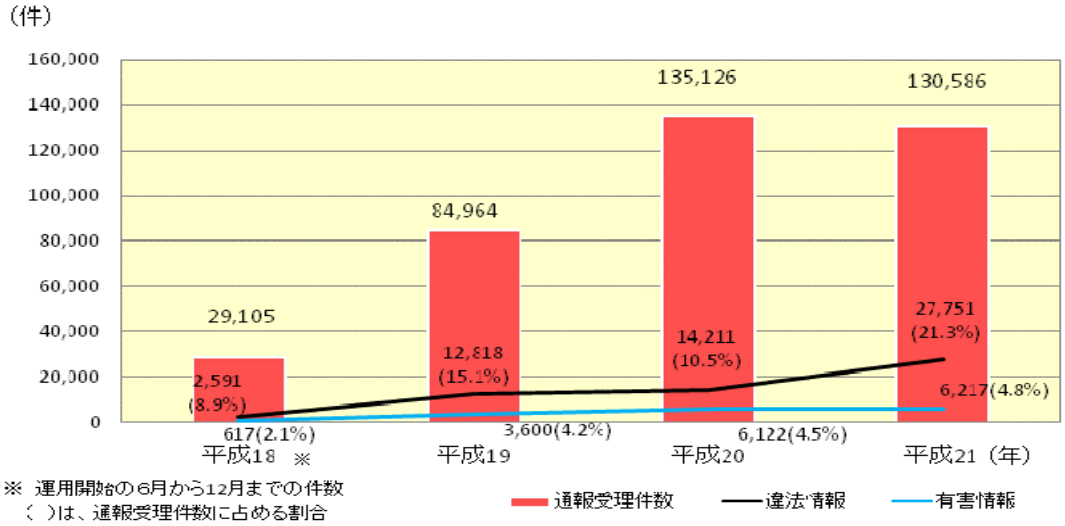
この大量の情報を容易に送受信できる環境整備の進展は利用者による有益な情報の迅速な取得を可能にするとともに、ブログを始め電子掲示板等による情報交換やコミュニケーションを容易にしているが、他方で、これらの性質や匿名性等を悪用してインターネットは犯罪の手段として利用され、様々な犯罪が誘引される危険性がある違法・有害情報が書き込まれており、その結果、あらゆる対象や場面に悪影響を与えて、問題となっている（図１－２）。例えば、違法情報では、電子掲示板に児童ポルノが掲載された場合には、被写体になった児童に大きな心の傷を残し、閲覧した児童等の健全な育成を害するほか、児童を性的搾取の対象とする風潮を助長している。また、規制薬物の広告の場合には、薬物の入手を極めて容易にし、乱用者を助長することにつながっている。その一方で、有害情報では、殺害・報復依頼の場合には、殺人を始めとする凶悪な犯罪を助長しているほか、自殺を募集する書き込みの場合には、人命保護の観点から問題があり、生命の尊厳を著しく害するものである。

インターネット上ではこのような違法・有害情報の書き込みとサイト管理者による削除等が同時並行でなされており、一定時点の違法・有害情報の流通の状況を数的に把握することは困難ではあるが、違法・有害情報の通報を公的に受け付ける機関であるＩＨＣへの通報件数を一つの指標として見てみると、ＩＨＣへの通報件数は、運用開始以降増加傾向にあり、平成 21 年には 130,586 件になっている（図１－３）。また、通報された情報を分析した結果、違法・有害情報に該当すると判断された件数については増加の一途をたどっており、平成 21 年における該当件数は 33,968 件となっているとともに、通報件数に占める違法情報の割合も増加傾向にあり、平成 21 年には 21.3%を占めている[3]。

[3] 通報件数が増加傾向になるのはインターネット上の違法・有害情報の増加が考えられ、特に平成 20 年に通報件数が増加したのはＩＨＣの活動が頻繁にマスコミに取り上げられたことが大きいと考えられている。また、平成 21 年に違法情報の通報件数に占める割合が増加した理由としては、警察庁が民間委託したサイバーパトロールによる通報が増加したこと等が挙げられる。

図１－２　違法・有害情報の書き込み例

図１－３　ＩＨＣに対する通報受理件数、違法・有害情報の通報件数の推移



第２章　違法・有害情報対策における関係者の取組

１　解決に向けた基本的な考え方

インターネット上に問題となっている違法・有害情報は、これらの情報が掲載されること自体が違法で犯罪を構成したり、様々な犯罪が誘引される危険性があって、極めて悪質なものであり、インターネット上の安全・安心を損なうとともに、利用者等の財産や生命も脅かすことになることから、これらに対しては、社会全体で対処していく取組が重要である。

そのためには、利用者や事業者、警察、ＩＨＣ等のインターネットに関係するあらゆる者が、違法・有害情報に対処するために、社会の連帯責任として、それぞれの立場で、また、それぞれが連携・協力して取り組むべきである。もとより、警察による違法情報の強力な取締りは重要であるが、インターネット上で検索エンジンの運営、サーバーのレンタル事業、各種情報の発信等、様々なサービスを提供して利益を得ている事業者は、インターネット上でサービスを提供するとともに、様々な技術や管理権を有していることから、違法・有害情報に対処する上で重要な役割を担っている。

違法・有害情報対策として関係者は、これまで次のように取組を行ってきた。

２　事業者の取組

一般的なサイト管理者等は、通信関連の業界４団体[4]が作成した「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」及び「違法・有害情報への対応等に関する契約約款モデル条項」に沿って、各罪種における違法情報の具体的な態様に基づき、該当する情報を発見した場合、発信者に対しその発信をやめるように要求した上で、要求に応じない場合には、その情報を削除するなどしている。また、警察やＩＨＣからの違法情報の削除依頼に基づき、その情報が違法であるとサイト管理者等自身が判断した場合には、可能な限り速やかに削除措置を行っている。

このほか、事業者によっては、自社が提供するサービス内で、違法・有害情報や不適切な利用がないかを定期的にパトロールしたり、違法・有害情報に関するデータベースを広く一般の企業等に提供したりして、違法・有害情報の選別に役立てるなど、自主的に独自の違法・有害情報対策を講じている。

(1)　情報発信の場を提供する事業者

レンタル掲示板サービスやブログサービス、ＳＮＳ等、インターネット上における利用者の情報発信を可能とするサービスを提供する事業者は、利用者が安心してサービスの提供を受けられるよう、サービス内に違法・有害情報や不適切な書込み・情報が掲載されていないか事業者自らが選別するシステムの構築や目視による監視を始め、利用者への啓発活動、通報受付体制の整備、規約違反者に対する利用停

[4]　（社）電気通信事業者協会、（社）テレコムサービス協会、（社）日本インターネットプロバイダ協会及び（社）日本ケーブルテレビ連盟をいう。

止措置等を行っている。

例えば、株式会社ライブドアでは、違法・有害情報の書き込みを分析して書き込みを行えなくする機能を有するシステム（「スパムちゃんぷるー」）を開発し、大規模ブログ事業者から個人のサイト管理者に対して無償で提供しているほか、2004年秋以降、24時間365時間体制で自社コミュニティサイト内の目視による監視を、在宅障害者雇用やテレワークの推進と絡めて行っている。

(2) フィルタリングソフト提供事業者

インターネット上の情報を分類し、パソコンや携帯電話によって有害なサイトへの接続を制限するフィルタリングソフトを提供している事業者は、インターネットへ接続できるゲーム機や各種家電製品へ対応するフィルタリングサービスの迅速な開発に努めているとともに、フィルタリングソフトとして活用するために分類したカテゴリ別の情報のデータベースを一般に提供して、利用者にとって有害な情報を選別・削除をできるようにして、利用者の違法・有害情報対策の促進に努めている。

例えば、パソコンを中心にフィルタリングソフトのサービスを提供しているデジタルアーツ株式会社では、据置き型又は携帯型のゲーム機やインターネットに対応したテレビを対象としたフィルタリングサービスを提供しているほか、行政機関主催の展示会や講演会等を通じて、インターネットの安全な利用方法やインターネット接続可能な機器へのフィルタリングの提供状況等を周知して、利用者に対する啓発活動を行っている。

また、法人・家庭向けフィルタリングソフトメーカーや携帯電話事業者等にフィルタリング要素技術を提供しているネットスター株式会社では、交流サイト等の運営事業者に対して、フィルタリングで使用される「アダルト」や「詐欺」等の不適切なサイトのＵＲＬアドレスを網羅的に掲載したリストデータを提供したり、利用規約に反する表現を自動判別する自然言語処理技術を提供するなどして、運営事業者の監視・削除業務の精度向上やコスト削減に寄与する取組を行っている。

(3) 検索エンジンサービス提供事業者

インターネット上の検索エンジンサービスを提供している事業者は、インターネット上の情報を短時間に大量に判別・処理できる検索機能を活用し、インターネット上の違法・有害情報等についてワード検索するとともに、これにより抽出した情報を関係機関に提供するなどして、業務を通じて違法・有害情報対策を推進している。

例えば、マイクロソフト・コーポレーションの研究部門であるマイクロソフト・リサーチは、米国ダートマス大学と連携して、ハッシュ法[5]を活用し、インターネッ

[5] 複雑なデータを高速に検索するための手法をいう。

ト上に存在する画像に識別用のシグネチャを生成し、同一のシグネチャを有する画像を検出・照合する「Photo ＤＮＡ」技術を共同開発し、自社の検索エンジンやオンラインサービスに組み込むとともに、ＮＣＭＥＣ（National Center for Missing & Exploited Children）[6]に提供することによって、インターネット上の児童ポルノ画像の流出阻止を効率的に行っている。

また、グーグル社では、利用者から違法なコンテンツやサービスの不正使用の報告を受け付けているほか、直接苦情を受け付けるヘルプセンターを設置している。また、業務を通じて把握した児童ポルノの掲載に関する情報については、即時にコンテンツを削除してＮＣＭＥＣに報告するとともに、違法なサイト等については、指定団体が保有する児童ポルノを含む可能性のあるサイトのデータベースを用いて、自社の検索エンジンの検索結果から取り除いている。

３　政府の取組

政府においては、国民が安心してインターネットを活用できるよう、関係省庁が一丸となって、民間の事業者による自主的・自律的な取組と連携しながら、インターネット上の違法・有害情報対策に取り組んでいる。

「インターネット上の違法・有害情報等に関する関係省庁連絡会議（ＩＴ安心会議）」では、平成 17 年６月、インターネット上の青少年有害情報[7]を排除するフィルタリングソフトの普及促進や技術開発、プロバイダ等による自殺サイトや違法・有害情報への自主的な規制等に対する支援、違法・有害情報対策に関するモラル教育の充実、国民への相談窓口の充実等を含む「インターネット上における違法・有害情報対策について」を取りまとめるとともに、これらの対策を充実させるため、平成 19 年 10 月「インターネット上の違法・有害情報に関する集中対策」を決定し、関係省庁でこれらの施策を推進している。

また、「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」（平成 20 年法律第 79 号。以下「青少年インターネット環境整備法」という。）に基づき、「青少年が安全に安心してインターネットを利用できるようにするための施策に関する基本的な計画」が策定され、関係省庁において、青少年のインターネットの適切な利用に関する教育及び啓発の推進、青少年有害情報を排除するフィルタリングの性能の向上及び普及、青少年のインターネットの適切な利用に関する活動を行う民間団体等の支援等の施策を推進している。

特に、児童ポルノについては、児童に対する著しい人権侵害であることから、平成 22 年７月、犯罪対策閣僚会議において「児童ポルノ排除総合対策」が策定されたほか、民間においても児童ポルノのブロッキング等の流通防止対策に係る取組が進んでいる。

---

[6] 児童誘拐・性的搾取を防止し、失踪児童の発見や児童誘拐・性的搾取の被害児童、家庭及び専門家への支援を行っている民間の非営利組織（1984 年設立）。

[7] インターネットを利用して公衆の閲覧（試聴も含む。）に供されている情報であって青少年の健全な成長を著しく阻害するものをいう。青少年インターネット環境整備法第２条第３項参照。

４　ＩＨＣと警察が連携した取組

(1)　ＩＨＣの運用開始に至るまでの経緯

平成 17 年当時、インターネット上には、すでに児童ポルノ、薬物取引等に関する情報や、直ちに違法とは評価されないものの、いわゆる自殺サイトや殺人等の違法行為の請負等に関する情報が氾濫している状況にあり、また、これらの情報に関連した事件[8]が社会的に大きく取り上げられるなど、これらの情報に対する社会の関心が非常に高まっていた。

警察では、ウェブサイトや電子掲示板等を閲覧してサイバーパトロールを行い、これらの情報を把握するとともに、これを端緒として発信者の取締りやサイト管理者等に対する削除依頼を実施するなどの対策を講じてきたが、インターネット上に流通する情報は違法情報だけでも膨大に上るほか、匿名性が高いこと、被害対象が広範囲にわたること、証拠の隠滅が図りやすいこと等の特性から、警察による取締りだけでは限界があった。

このような情勢の下、総合セキュリティ対策会議においては、平成 17 年度のテーマとして、「インターネット上の違法・有害情報への対応における官民の連携の在り方について」を取り上げ、官民連携の一つの方策として、すでに諸外国でも運用され、一定の成果を上げていたインターネット上の「ホットライン」[9]活動の運営の在り方等について、関係事業者や学識経験者等を交えた専門的な検討を行った。

この結果、インターネット上の違法・有害情報対策について、表現の自由等の基本的人権と公共の福祉とのバランスを考慮した上で効果的に推進するためには、利用者等が発見した違法・有害情報を「ホットライン」に通報する仕組みを整備することが重要とされ、インターネット上の「ホットライン」を導入する必要性が提言された。その後、平成 18 年６月には、警察庁の委託を受けた民間団体により、インターネット上の違法・有害情報に関する通報を受け付けるＩＨＣの運用が始まり、現在に至っている。

(2)　ＩＨＣで取り扱う違法・有害情報の選定手続

ＩＨＣで取り扱う違法・有害情報は、インターネット上における流通が社会問題化し、かつ、ＩＨＣにおいて適切かつ円滑に判断することができる情報を対象としており、その情報の範囲・判断基準・手続等については、ＩＨＣにおける対応の正当性を確保・維持するため、関係者の意見を踏まえて策定されたホットライン運用ガイドラインを根拠としている。このガイドラインは、インターネット上を流通する情報をめぐる状況の変化等を踏まえ、関係事業者や学識経験者等から構成されるホットライン運用ガイドライン検討協議会において見直しが図られ、パブリックコ

---

[8] 山口県光市で発生した高校生による爆弾製造・爆破事件（６月）、大阪府において発生したいわゆる自殺サイトを利用した連続殺人事件（８月）等。

[9] インターネット利用者からインターネット上の違法・有害情報についての通報を受け付け、その情報について一定の基準に基づいて判断を行い、警察への通報やサイト管理者等に削除依頼等を行う仕組みをいう。

メントを経た後に運用されている。

このような手続きを経て、違法情報については、インターネット上の流通が法令に違反する情報で、上記の条件を満たした８類型の情報が対象とされ、また、有害情報については、インターネット上における情報の流通を契機として現実の社会において違法行為が発生した事例等を踏まえ、表現の自由と公共の福祉とのバランスに配慮し、違法行為を引き起こすおそれがある３類型の情報が対象とされている（図１－１）。

(3)　ＩＨＣの取組

ＩＨＣは、インターネット上における違法・有害情報に該当する情報に関する通報を受理し、その該当性を判断した後、違法情報については、取締りにあたる警察へ通報するとともに、サイト管理者等へ当該情報の削除依頼を行っている一方で、有害情報については、サイト管理者等に対し、契約約款等に基づく削除等の対応を依頼している（図２－１）。このように、ＩＨＣの仕組みは、削除依頼という事実行為を行うにとどまり、実際に削除するかどうかの最終的な判断はサイト管理者等の自主的な判断に委ねることで、表現の自由等の基本的人権と公共の福祉との均衡を図っている。

これ以外にも、外国のサーバー上に蔵置されている違法情報について、諸外国におけるホットライン相互間の連絡組織であるＩＮＨＯＰＥ[10]を通じて情報提供を行っているほか、フィルタリングソフト提供事業者等の関係機関・団体への情報提供も行っている。

図２－１　ＩＨＣの取組

[10]　International Association of Internet Hotlines。1999 年に設立された団体で、2010 年５月の時点で 38 団体（33 の国・地域）が加盟。日本では、財団法人インターネット協会が 2007 年３月に加盟。

5　警察の取組

(1)　全国協働捜査方式による取締りの強化

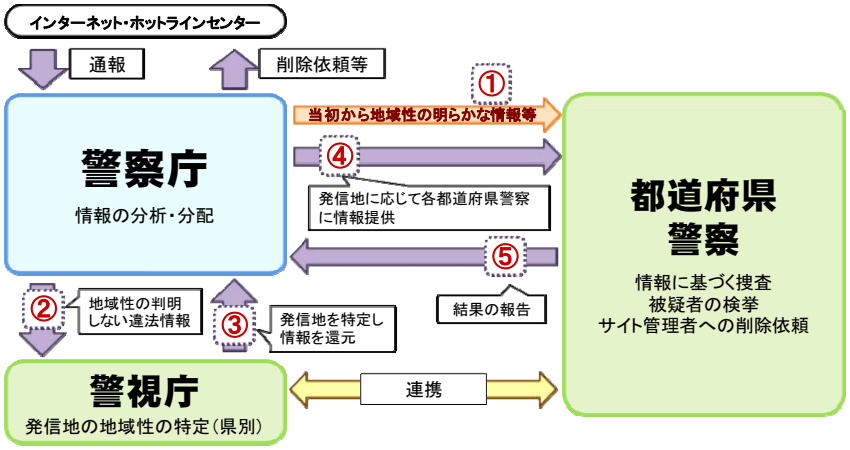
警察では、サイバーパトロールやＩＨＣから提供された情報によって、発信者の検挙等とともに、違法・有害情報の削除依頼を行うなどして違法・有害情報対策を講じてきた。このような取組は、ＩＨＣによる削除依頼によってインターネット上の多数の違法・有害情報が削除されていることと相まって、一定の成果を上げてきた。その一方で、ＩＨＣに通報された違法・有害情報の件数は増加の一途をたどっており、警察とＩＨＣによる削除依頼を通じたインターネット上の違法・有害情報の除去には限界があることから、インターネット上に流通する違法情報の総量抑止を図る必要性が高くなった。これを踏まえ、警察では、より悪質な違法情報の取締りを強化することとし、平成 22 年 10 月から新たな捜査態勢である全国協働捜査方式を試行している（図２－２）。

その特徴は、警視庁において初期捜査を集中的に行うというものである。これまでＩＨＣから警察庁に通報された違法情報は、都道府県警察に全てを通知した後、各都道府県警察がプロバイダへ照会するなど所要の捜査を行うことによって発信者を特定し、取締りを行っていた。しかしながら、違法情報が各都道府県警察に通知される段階では書き込み等の発信地が不明であることから、取締りを担当すべき都道府県警察が不明確となっており、取締りが必ずしも十分に推進されてこなかった。

この点を改善するため、全国協働捜査方式ではＩＨＣから警察庁に通報された違法情報について、警視庁に設置する情報追跡班において、違法情報が掲載されているサイト管理者等への照会によって発信者が使用した端末が存在する都道府県を割り出した後、その結果を違法情報と合わせて発信地を管轄する都道府県警察に通知し、通知を受けた都道府県警察がプロバイダに対する契約者情報の差押え、契約者に関する捜査を行い、発信者の検挙を行うものである。

この全国協働捜査方式によって取締りを強化し、多量のわいせつ図画等を掲載し、不特定多数の者に閲覧させるなど、悪質な違法情報の発信者に対しては断固とした姿勢で臨み検挙するとともに、違法情報の削除依頼に故意に応じない悪質なサイト管理者に対しては刑事責任を追及することとしている。

図２－２　全国協働捜査方式



第３章　違法・有害情報対策における問題の所在

違法・有害情報対策については、第２章で述べたように、関係者がそれぞれの立場で取り組んでいるところであるが、利用者等からの違法・有害情報を受け付け、その情報について一定の基準に基づいて判断を行い、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であるホットライン業務を国から委託され、その運営資金を財政的に手当されているＩＨＣの活動については、事業者がその社会的責任の一環として自主的に行う対策とは異なり、国家予算による違法・有害情報の削除依頼に関する唯一の公的機関として位置付けることができることから、関係者による議論を通じて活動を向上・充実させる必要がある。しかしながら、現状においては、ＩＨＣへの通報制度が必ずしも活用されていないこと、ＩＨＣがサイト管理者に削除依頼を伝達できていないこと、削除依頼に応じないサイト管理者がいること等の問題点も認められるところであり、現時点においては、そのような問題点を解決する方策について早急に検討し、当初の制度検討の中でホットライン業務として期待された機能を果たすよう取り組むことが現実的かつ喫緊の課題となっている。

第１　ＩＨＣへの通報に係る問題点

１　ＩＨＣへの通報制度が必ずしも活用されていないこと

現実社会では、違法行為等を受けたり、発見した場合等に警察に通報するため１１０番が設けられており、これを受け付けた警察では、警察官を派遣し、事件の捜査・検挙を行うほか、紛争を処理するなど適切に対応している。１１０番は、警察に対する通報の窓口として広く認知されていることから、現実社会における違法行為等については１１０番通報がなされ、警察における違法行為等への対応の基点として活用されているといえる。

インターネット上の違法・有害情報に係る１１０番通報制度に相当する役割を担っているものがＩＨＣへの通報制度であり、これによって違法・有害情報が削除され、その状況を改善するきっかけになることから、違法・有害情報対策としても非常に有効であると考えられる。この通報制度を活用することによって、違法・有害情報には積極的に対処すべきではあるものの、現状は、インターネット上の違法・有害情報の一部しか通報されておらず、ＩＨＣへの通報制度が必ずしも活用されていない状況にある。

その要因としては、ＩＨＣの活動や取組が利用者等に十分に認知されていない[11]ことが考えられる。企業等においても、ウェブページにおいて違法・有害情報を発見した際の通報先としてＩＨＣへのリンクを張り、利用者等をＩＨＣのウェブページに誘導するように協力しているものもあるが、その数も多いとは言えず、利用者等が認知するのに十分とはいえない状況にある。

また、児童ポルノについては、児童に対する著しい人権侵害であり、その排除気運

[11] 警察庁が都道府県警察を通じて行ったアンケート調査（運転免許試験場等で優良運転者講習受講者を対象とし、平成23年１月に実施）では、4,294名のうち、ＩＨＣを知っている者は単に名称のみを知っている者を含めても1,310名（約30.5%）でその認知度が非常に低いことがうかがわれる。

も高まっていることから、ＩＨＣに児童ポルノの掲載に関する情報を集約して流通防止対策を的確に進める必要があるが、現状では、児童ポルノの掲載に関する通報も利用者等の善意によるところが大きく、特に、業務上児童ポルノの掲載に関する情報を取り扱う機会が多い事業者からの情報の提供が必ずしも十分とはいえない状況にある。

このように、違法・有害情報対策を推進するためには、ＩＨＣへの通報制度を活用すべきであるところ、利用者等に対するＩＨＣの活動等の周知の不徹底、企業等におけるＩＨＣの活動の意義に対する理解の不足等により、必ずしも活用されていないという問題がある。

2　利用者等における情報の違法性・有害性の判断の困難性

平成 17 年度総合セキュリティ対策会議では、ホットライン実施主体には、様々な情報について通報が寄せられることが予想されることから、人権侵害、知的財産権侵害に係る通報等については関係機関・団体に対して情報提供することとされるとともに、ホットライン実施主体において、頻繁に寄せられる質問に対応するために、ウェブページ上でＦＡＱを作成するなどして適切な相談機関等を教示することができる仕組みを作ることとされた。

これらを受け、ＩＨＣのウェブページでは、ＦＡＱを設けるとともに、通報フォームにおいてＩＨＣが受理する違法・有害情報の詳細についての記載を設けている。また、ＩＨＣが受理する違法・有害情報以外の違法・有害情報の通報先等へのリンクを掲載している。しかしながら、これらの記載は、法令の条文をほぼそのまま引用したような文章も多く、利用者等にとって通報しようとする情報が違法・有害情報に該当するか否かを判断しにくい状況にあると考えられる。

さらに、通報するに当たっては、情報が違法・有害情報のいずれの類型に該当するかを利用者等が自身で判断しなければならず、いずれの類型にも該当しないと誤った判断をした情報については、ＩＨＣに通報されないことになる。

このように、利用者等は、違法・有害情報の通報に際し、違法・有害情報の該当性の判断が困難で、必ずしも的確にできていないために、本来通報されるべき情報が通報されていない場合もあると考えられる。

3　通報対象となる情報の該当性が困難な場合のＩＨＣ内の判断手続の未整備

通報を受け付けたＩＨＣでは、個別の通報について、ホットライン運用ガイドラインに基づき適切に違法・有害性の判断を行っている。これまでの業務を通じて、判断基準については一定の蓄積がなされてきているものの、最近では様々な違法・有害情報があり、これまでの蓄積では必ずしも判断しにくいものもある。例えば、児童ポルノについては様々なものがあり、被写体となっている人物が児童であるか否か、また、児童であった場合において当該画像が法で規定される児童ポルノに該当するか否かなど、違法性・有害性の判断に迷う情報も少なくない。今後、児童ポルノに関しては、ブロッキングといった、より踏み込んだ流通防止対策が実施される情勢に鑑みると、

児童ポルノに関する違法性の判断については、厳格な判断が求められる。

一方で、ホットライン運用ガイドラインでは、「違法情報該当性の判断が難しい場合には、法律家等の専門家に相談した上で判断する」とされているが、その明確な手続きは定められておらず、難しい判断であるほど個々のＩＨＣ職員の知見に頼ってしまう場合もある。

このように、ＩＨＣにおける違法・有害情報の該当性の判断について、組織的な判断を行うための手続や運用の在り方について必ずしも明確になっていない問題がある。

第２　違法・有害情報に対処するためのサイト管理者に係る問題点

１　サイト管理者における連絡受付体制の未整備

サイト管理者は、情報の流通の場を提供するとともに、その管理権に基づいて、サイト内の違法・有害情報のみを個別に削除するなどの対応が可能であることから、その事業の特性に応じて、サイト管理者の自主的対応として、サイト内に違法・有害情報があった場合には削除するなどの適切な対応を講じることが社会的にも期待されている。また、サイト管理者は、サイト内で違法・有害情報が掲載されている全ての場合を発見することは必ずしも容易ではないことから、利用者等やＩＨＣから連絡を受け付けるための体制（以下「連絡受付体制」という。）を整備することで、サイト内の違法・有害情報を察知し、削除することを促進させる必要がある。

現に、青少年インターネット環境整備法第 21 条では、特定サーバー管理者[12]に対しては、管理する特定サーバーを利用して青少年有害情報の発信が行われたことを知ったときや自ら当該情報の発信を行おうとするときは、当該情報について閲覧防止措置をとるよう努めなければならないとされており、また、第 22 条では、管理する特定サーバーを利用して発信した当該情報について、国民からの連絡受付体制を整備するよう努めなければならないとされているところである。

大手サイト管理者においてはおおむね連絡受付体制が整備されており、措置も講じられているが、一部のサイト管理者においては、その管理するサイトに自らの連絡先等[13]を記載していない場合が散見され、平成 22 年上半期にＩＨＣになされた通報について、違法情報が掲載されていた 2,296 サイトのうち 57％に当たる 1,319 サイト、有害情報が掲載されていた 97 サイトのうち 54％に当たる 52 サイトには、連絡が取れない状況であった（図３－１、２）。

このように、違法・有害情報が掲載されたサイトにおいて、連絡受付体制が整備されていない場合に、ＩＨＣがサイト管理者に削除依頼を伝達できていないという問題がある。

---

[12] インターネットを利用した公衆による情報の閲覧の用に供されるサーバー（特定サーバー）を用いて、他人の求めに応じ情報をインターネットを利用して公衆による閲覧ができる状態に置き、これに閲覧をさせる役務を提供する者をいう。青少年インターネット環境整備法第２条第 11 項参照。

[13] メールアドレスや問合せフォーム等をいう。

図　サイトに連絡先等が記載されている割合

図３－１　違法情報

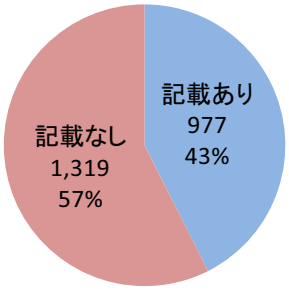
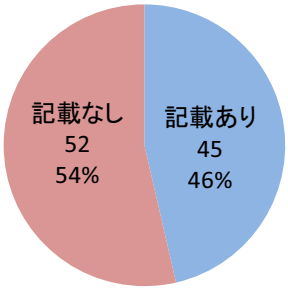


図３－２　有害情報



２　削除依頼に応じないサイト管理者の存在

平成 21 年にＩＨＣが削除等の依頼を行った違法情報 16,496 件のうち 14,518 件、有害情報 1,971 件のうち 1,546 件が削除されており、違法情報の削除率は 88.0%（前年：85.0%）、有害情報の削除率は 78.4%（前年：75.8%）であった。違法情報について 1,978 件（12.0%）が削除依頼を行ったにもかかわらず削除されておらず、インターネット上に放置されていることが分かる（図３－３、４）。

図３－３　違法情報の削除推移

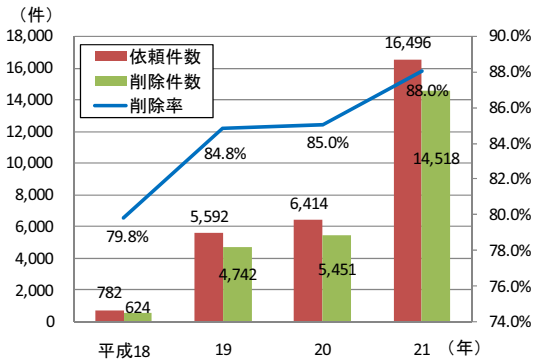
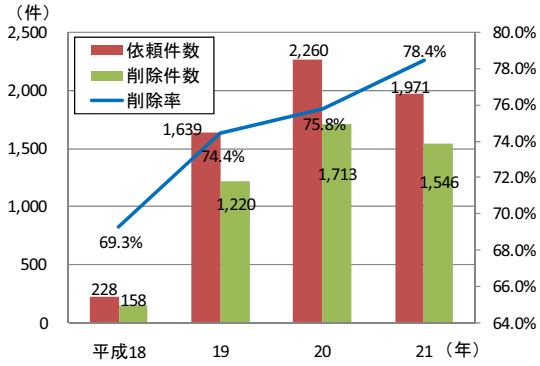


図３－４　有害情報の削除推移



サイト管理者で見ると、平成 21 年にＩＨＣが行った違法情報の削除依頼について応じなかったサイト管理者が 75 者存在しており、最も削除依頼に応じなかったサイト管理者の 1,227 件を始め、上位 10 者で未削除の件数が全体の 87.0%を占めている状況にある（図３－５）。このような、削除依頼に応じないサイト管理者の存在が、削除依頼の実効性を阻害している問題がある。

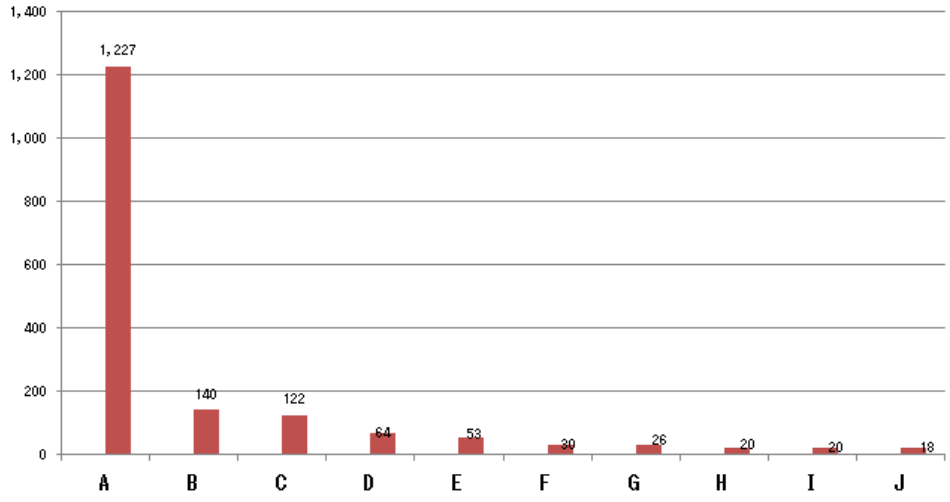
このようなサイト管理者に対しては、上位管理者であるプロバイダ等[14]が問題となっているサイト内の違法情報を削除するなどの対応が考えられるが、現状では、プ

[14] サイト管理者にインターネット上のサービスを提供し、かつサイト管理者のメールアドレスや電話番号を始め連絡先に関する情報を保持し、ＩＨＣからの削除依頼を伝達できる立場にある者（例えば、ホスティングプロバイダ）を想定している。

ロバイダ等が、サイト管理者の意思に反して削除を行うために必要となる法規又は契約上の根拠（例えば、プロバイダ等とサイト管理者間の契約等）が整備されていないために、プロバイダ等がその自主的な判断により削除することが適切であると認めた場合についてまで、対応ができないという問題がある。

なお、国内法では対処できない海外サーバーに蔵置される違法情報が存在するが、これらについては、ＩＮＨＯＰＥを通じた対応を頼らざるを得ない状況である。

図３－５　未削除の違法情報が多い上位のサイト管理者とその未削除数



第４章　ホットライン業務の機能向上のための対応策について（提言）

インターネット上の違法・有害情報対策では、第３章で明らかになった問題点を踏まえ、ＩＨＣが行っているホットライン業務の実効性を担保する観点から、その対応策を講じることが重要である。

具体的には、①インターネット上の違法・有害情報がより多くＩＨＣに通報されるにはどうすればよいか、②インターネット上の情報の違法・有害の該当性について、利用者等及びＩＨＣが判断しやすくするにはどうすればよいか、③連絡受付体制が整備されていないサイト管理者に対して、ＩＨＣの削除依頼の実効性を担保するにはどうすればよいか、④削除依頼に応じないサイト管理者に対して有効な措置は何かという点について、本章では、その対応策を提言することとする。

第１　ＩＨＣへの通報を活性化させるための方策

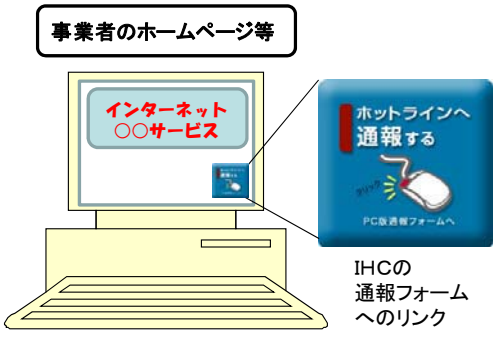
１　ＩＨＣの認知度を向上させるための取組等

ＩＨＣへの通報制度が、利用者等に十分認知されていないために必ずしも活用されていないことから、ＩＨＣの存在や活動内容について、多くの利用者等に認知されるようにするとともに、インターネットを利用している企業等に対しては、ＩＨＣの意義や活動内容を理解してもらった上で、その活動に協力してもらうことにより、ＩＨＣに対する通報制度を一層機能させることが重要である。

また、児童ポルノについては、官民が一体となった排除気運が高まっていることから、業務上児童ポルノの掲載に関する情報を取り扱う機会が多い事業者等からＩＨＣへ積極的に情報提供してもらうことにより、より効果的に排除することが考えられる。

そこで、利用者等に対しては、ＩＨＣの活動についてそのホームページで具体的に広報したり、警察による事件検挙の広報の際に盛り込むなどして、ＩＨＣの認知度を向上させるための取組を行うことが望ましい。また、企業等に対しては、そのホームページの目立つ位置に、ＩＨＣのホームページへリンクする通報ボタンを設置してもらうとともに、ＩＨＣの活動を分かりやすく紹介して利用者等が通報しやすいよう工夫するなどしてもらうことによって、ＩＨＣの認知度を向上させ、その活動に協力してもらうための取組を行うことが望ましい（図４－１）。

図４－１　ＩＨＣの通報フォーム例



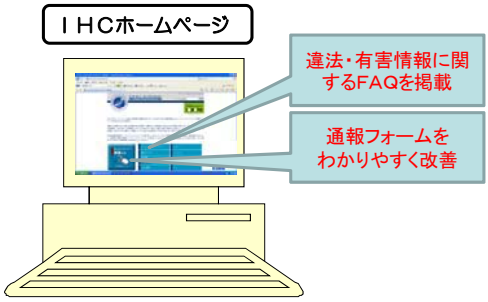
また、事業者等が、業務上の影響や保秘等を考慮した上で、児童ポルノの掲載に関する情報を積極的に提供できるよう協力してもらうために、ＩＨＣはこれらの情報提供を受け付ける体制を整備することが望ましい。

２　利用者等が通報対象となる情報の該当性を判断しやすくする工夫

ＩＨＣがその機能を十分に発揮するためには、利用者等が該当する情報を発見した場合には、その情報がＩＨＣの通報対象となる違法・有害情報に該当するかどうかを的確に判断した上で、通報してもらうことが必要である。

そこで、「分かりやすさ」と「使いやすさ」をキーワードに、ＩＨＣへの通報フォームに記載されている違法・有害情報の判断に関する説明について平易な表現にしたり、通報フォームに設けられている入力の手間をより簡易にするとともに、ＩＨＣのホームページに記載されている違法・有害情報の該当性に関するＦＡＱについても、ＩＨＣがこれまで判断して積み重ねた知見を活かした具体例を交えながら、より分かりやすいものに改善したりするほか、質問に対し違法・有害情報の事例集を適宜示しながらそのポイントを説明するなどして、ＩＨＣの取組として、利用者等が通報対象となる情報が違法・有害情報に該当するかどうかを判断しやすくする工夫を加えることが望ましい（図４－２）。

図４－２　ＩＨＣのホームページの工夫例



３　通報対象となる情報の該当性判断が困難な場合のＩＨＣ内の判断手続の制度化

ＩＨＣが通報対象となる情報の該当性を的確に判断するためには、その判断が困難な場合に、組織内でその問題を顕在化させ、情報を共有化した上で、的確に判断し、解決策を蓄積することが必要である。

そこで、ＩＨＣには、児童に該当するかどうか判断が難しい児童ポルノを始め、当該情報の該当性の判断が困難な場合に、的確に判断するために、法律の専門家等にどのような形で協力してもらうかについて、手続面や運用面も含めて見直してもらった上で、組織内で判断する手続を制度化することが望ましい。

第２　違法・有害情報に対処するためのサイト管理者対策

１　ＩＨＣの削除依頼をサイト管理者に確実に伝達するための方法の確保等

ＩＨＣの削除依頼の実効性を担保するためには、違法・有害情報が掲載されているが、連絡受付体制を整備していないサイト管理者に対して、ＩＨＣの削除依頼を確実に伝達するための方法を確保する必要がある。しかしながら、このような方法が確保

されていない場合には、インターネット上の表現の自由やプライバシーに十分配慮しつつ、サイト管理者に連絡受付体制を整備するよう努めてもらうとともに、プロバイダ等の協力を得て、連絡受付体制を整備していないサイト管理者に対して、ＩＨＣの削除依頼を確実に伝達するための方法を確保するよう促すことが望ましい。

プロバイダ等が行う取組としては、プロバイダ等とＩＨＣが協力して、サイト管理者に対してＩＨＣの削除依頼を確実に伝達するための方法を確保するため、例えば、通信関連の業界４団体において、プロバイダ等とサイト管理者との間の契約に関する標準約款を作成し、その中で、サイト管理者は連絡受付体制を整備し、プロバイダ等においては、ＩＨＣの削除依頼をサイト管理者に伝達する旨を定めることなどが考えられる。その際には、個人情報の保護や通信の秘密が侵害される可能性について慎重に検討する必要がある。また、これと並行して、当該標準約款がプロバイダ等とサイト管理者の間における契約実務に幅広く用いられることとなるよう、標準約款を契約に用いることのインセンティブを付与することについて検討することも必要と考えられる。

２　違法情報を排除するための取締りの強化と効果的な対策の検討

インターネット上の違法情報が放置されている要因の一つは、悪質なサイト管理者が違法情報の削除に応じないことにあり、掲載自体が法令違反となる違法情報をインターネット上に放置することは、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といえる。合理的な理由もなく、このような違法情報の削除依頼に応じない悪質なサイト管理者は、犯罪を誘発している場所を作り出し、容認している蓋然性が高く、犯罪と認められる場合には、警察において積極的に検挙する必要がある。

その一方で、今後は、違法情報を効果的に排除する観点から、ＩＨＣの削除依頼の実効性をより担保するために、このようなサイト管理者に対する効果的な対策や措置を考える必要がある。また、このようなサイト管理者に対しては、プロバイダ等が契約に基づいて対応することが違法情報の流通を早期に防止する観点から有効であることから、両者の契約の在り方についても、上記の標準約款の作成を通じて検討する必要がある。

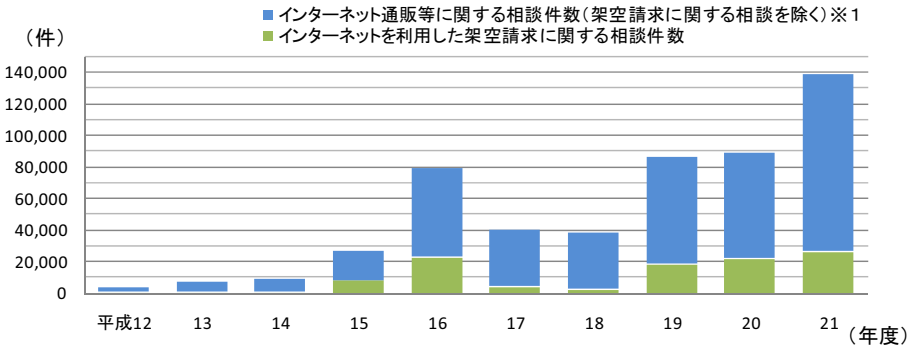
試論　インターネット上の個人をめぐるトラブルについて

第１　インターネット上の個人をめぐるトラブルの現状

インターネット上には、違法・有害情報が問題となっている一方で、この他にも個人をめぐるトラブル（以下単に「トラブル」という。）が年々増加しており、今後は、問題として大きく発展することが予想される。このようなトラブルの例としては、インターネット通販をめぐるトラブルや電子メールを利用した架空請求、不当請求事案等があるが、これらの相談件数が独立行政法人国民生活センター（以下「国民生活センター」という。）に数多く寄せられている状況にあるほか、インターネット上の名誉毀損、誹謗中傷に関する相談も増加傾向にある（図１－１、２）。

このようなトラブルは、次々と重なったり、そのまま放置すれば個人の財産や知的財産の侵害になるなど、犯罪につながる場合も少なくない。本分科会では、その重要性にかんがみ、インターネット上の個人をめぐるトラブルに対する関係者の取組等について、議論を試みたものである。

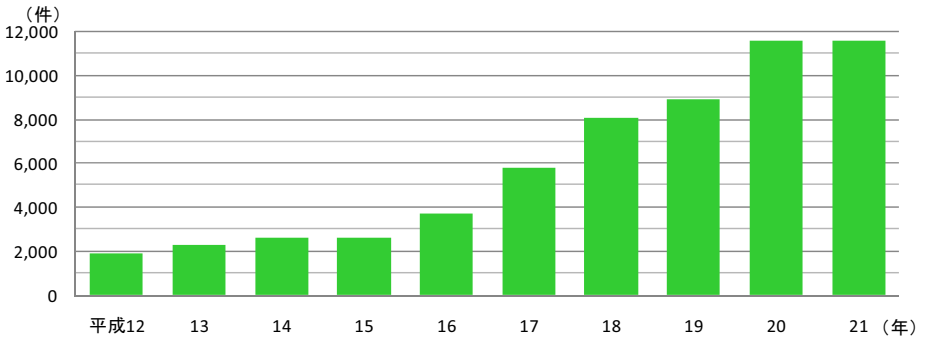
図１―１　インターネット通販等に関する相談件数



	平成12	13	14	15	16	17	18	19	20	21
インターネット通販等に関する相談件数（架空請求に関する相談を除く）※1	3,125	6,647	8,404	18,220	56,240	35,422	35,875	67,795	66,495	111,868
インターネットを利用した架空請求に関する相談件数	521	582	745	8,256	22,825	4,292	2,711	18,442	22,094	26,343

・「独立行政法人国民生活センター」調べ
・平成22年８月19日までのPIO-NET登録分
※1 平成12年度から平成20年度：「電子商取引」、「インターネット」に関する相談
　　平成21年度から平成22年度：「インターネット通販」、「インターネットオークション」に関する相談

図１－２　インターネット上の名誉毀損、誹謗中傷に関する相談



	平成12	13	14	15	16	17	18	19	20	21
インターネット上の名誉毀損、誹謗中傷に関する相談	1,884	2,267	2,566	2,619	3,685	5,782	8,037	8,871	11,516	11,557

※　都道府県警察の相談窓口に寄せられた相談

第２　インターネット上の個人をめぐるトラブルに対する関係者の取組

１　解決に向けた基本的な考え方

このようなトラブルは、違法・有害情報とは異なり、主に個人間や相談者と事業者間の問題で、個人の権利や財産が侵害されて、民事上の問題となることが少なくないが、問題解決がこじれると刑事事件に発展する可能性もある。このことから、個人の自由な意思に委ねてその解決方法を選択・決定できる「私的自治の原則」に基づいて、話し合い等を通じて円滑に解決される方法が望ましい。なぜならば、このトラブルによって権利等を侵害された個人は、早期にトラブルとなった書き込みが削除されるなどして名誉が回復されたり、行為者を特定し謝罪を求め再発を防止することなどを主眼に置いていて、必ずしも警察や裁判所等の介入による方法を望まない場合が多いからである。

２　事業者の取組

事業者の多くは、その運営するサイト上に、一般的な利用者からの問合せ等を受け付けるフォームやメールアドレス等が設けられており、ここで、利用者のトラブルが生じた場合に受け付けて対応している。

３　国民生活センターの取組

国民生活センターでは、消費者と事業者との消費生活に関するトラブルに対応している。同センターに寄せられるインターネット関連の相談としては、いわゆる架空請求メールや出会い系サイトで高額な利用料を請求されたというもの、アダルトサイトやパチンコ必勝サイト等における高額な情報提供料の請求に関するもの、インターネット通販における商品の破損・未配達等に関するもの等がある。

これらの相談に対しては、同センターでは、相談内容に応じた助言等を行っている。他方、ブログやサイトに自分の写真や名前が無断で貼られているといった相談や、インターネット・オークションによる個人間売買でのトラブル等については、いわゆるプロバイダ責任制限法に基づく掲示板管理者等への削除依頼の方法や弁護士を通じて救済を求める方法を教示するにとどまっている。

４　社団法人テレコムサービス協会の取組

社団法人テレコムサービス協会では、電気通信事業者、特定サーバー管理者、学校関係者等からのインターネットにおける違法・有害情報や安全・安心に関する相談に対応するために、「違法・有害情報相談センター」（http://www.ihaho.jp/）の窓口を設置し、相談員が解決に向けた助言を行っている。

５　ＩＨＣや警察の取組

ＩＨＣでは、このようなトラブルについては必要に応じて関係機関・団体への情報提供を行っており、中でも、名誉毀損・誹謗中傷に関する情報等の関係機関・団体において処理することが適当な場合は、法務省人権擁護局等の専門的な対応を行ってい

る関係機関・団体に提供するなどしている。

また、警察では、警察庁のホームページ上の「インターネット安全・安心相談」（http://www.npa.go.jp/cybersafety/）を始め、都道府県警察の各種相談窓口等によって、トラブルのアドバイスをしたり、適切な関係機関・団体を紹介するなどしている。

第３　インターネット上の個人をめぐるトラブル対応における問題の所在

国民生活センターや都道府県警察に寄せられたトラブルに関する相談は近年増加傾向にあるが、このようなトラブルについては、相談者が適切な相談先の知識がないなどのために、比較的知名度の高い警察、国民生活センター等に対して相談がなされるものと考えられる。しかしながら、相談者は書き込みの削除等を望む場合も多く、相談先として適切ではない場合もあり、このことが相談者にとって二重の手間となっている。

このように、相談者がトラブルを適切に解決するための関係機関・団体の周知が不十分であり、相談者にとって適切な関係機関・団体が分からないという状況が起きている。

第４　トラブルの解決に向けた適切な関係機関・団体に相談できる環境の整備等

このようなトラブルについては、近年増加傾向にあるにもかかわらず、相談者が必ずしも適切な関係機関・団体を見つけることができず、そのことが相談者の負担となっていることから、相談者が適切な関係機関・団体に相談できる環境を整備する必要がある。その前提として、このようなトラブルに関する実態や問題点、対応可能な相談窓口の有無等を整理する必要がある。

2011年2月　総合セキュリティ対策会議資料

Google　子供の安全への取り組み

Google は、全ての利用者様に安全にインターネットを楽しんでいただけるよう、有害なコンテンツから子どもたちを守ることに全力を注いでいます。
Google では、以下のような3つの観点から対策を行っています:

ツール

子どもがインターネットで閲覧可能なページを設定するための権限を保護者に与えるツール

連携

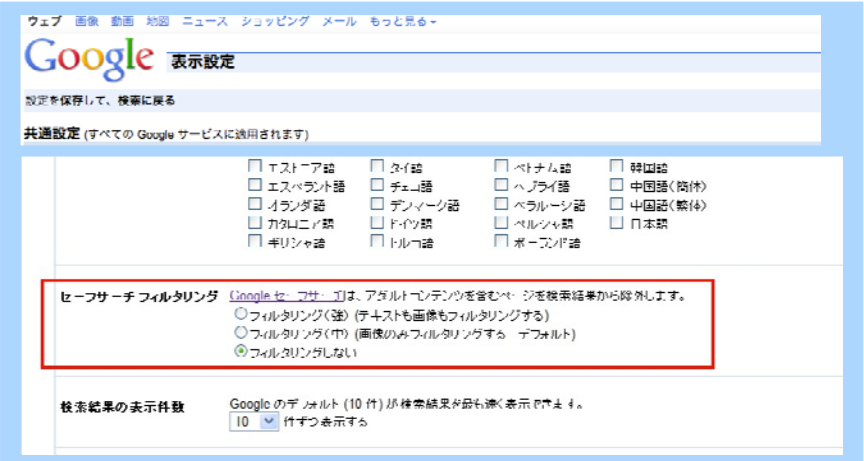
インターネットを利用する子どもたちを保護するための法執行機関や児童保護団体との連携

教育

子どもたちにインターネットの安全な使い方を教えるための教育

ツール　セーフサーチ

- Google の検索結果から、アダルト・コンテンツを除外する機能です。
- Google 独自の高度な技術により、アダルト・コンテンツの含まれる画像やテキストをブロックします。
- Google 検索ウィンドウの画面右上にある「検索設定」をクリックすると、検索設定をカスタマイズすることができます。



ツール　セーフサーチをロック

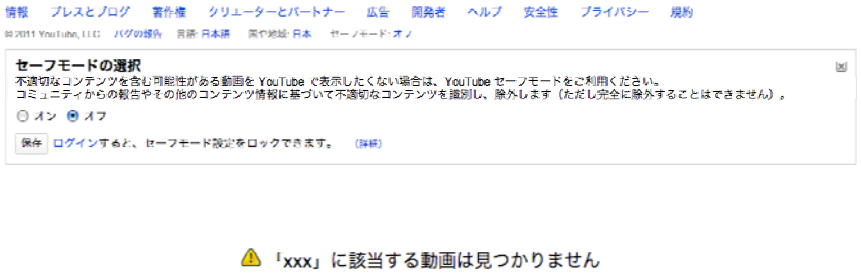
Google

- セーフサーチのレベルを設定後、変更にはパスワードが必要です。
- 保護者の方は、部屋の反対側にいても、画面右上のボールを見ればセーフサーチがオンになっているかどうか一目で分かります。

ツール　YouTube セーフモード

Google

- セーフモードは、ユーザーが目にしたくない動画や家族に見せたくないコンテンツをページに表示させないために作られた機能です。
- セーフモードを設定すると、ユーザーが不快に感じる可能性のある動画や、成人向け動画がフィルタリングされます。
- 保護者は、任意の動画のページ下部にあるリンクをクリックすればセーフモードを設定することが可能です。



ツール　不正コンテンツの報告ツール

違法コンテンツや Google サービスの不正使用を報告するための、業界トップクラスのツールを提供しています。以下はその一例です：

- [フラグ] ボタン
  ユーザーは YouTube の動画を見ながら簡単に不適切な動画を報告することが可能。動画を報告する理由を、10 以上の項目から選択することができ、補足情報も追加することができる。

  - 他サービスにも、不正使用を報告する機能を実装。（例：Picasaウェブアルバム）
- ユーザーが直接苦情を報告できるオンラインヘルプセンターを設置。

連携　法執行機関との協力体制

子どもたちをインターネット上の不適切なコンテンツから守るため、法執行機関に全面的に協力しています：

- 常時体制で法執行機関の対応にあたる専任の法律チームを設置
- 年間数千件にも上る、法執行機関からの支援要請に対応
- 子どもに対する犯罪捜査に関する自治体や連邦政府からの法律に基づく要請について、年間数百件の対応
- 児童ポルノは速やかに削除。このようなコンテンツを扱ったアカウントは即刻削除する
- インターネット審査監視機構（イギリスの Internet Watch Foundation (IWF)、ドイツのFreiwillige Selbstkontrolle Multimedia-Diensteanbieter (FSM)）を支持し、定期的にデータベースに登録された児童ポルノを含む疑いのあるウェブサイトのリストを用いて Google 検索結果から違法サイトの URL を取り除く
- 4月からは日本の児童ポルノ掲載アドレスリスト管理団体との協力も開始予定

連携　ユーザーから連携機関への通報の支援

未成年者に有害なコンテンツをユーザーが適切な機関に報告することができるようにしています。

教育　「Google安心利用のために」ページ
http://www.google.co.jp/familysafety/

Google のサイトには、安全なインターネット利用への取り組みや、ツールや資料についての説明が記載されたページが設けられています。
各サービスの使用方法でも、安全利用のためのアドバイスを記載しています。

教育　YouTube を利用した啓発活動

Child Exploitation and Online Protection (CEOP) Centre や Beatbullying などの児童保護団体と連携し、子どもたちがさらされている危険への認識を高めるための YouTube チャンネルを展開しています。

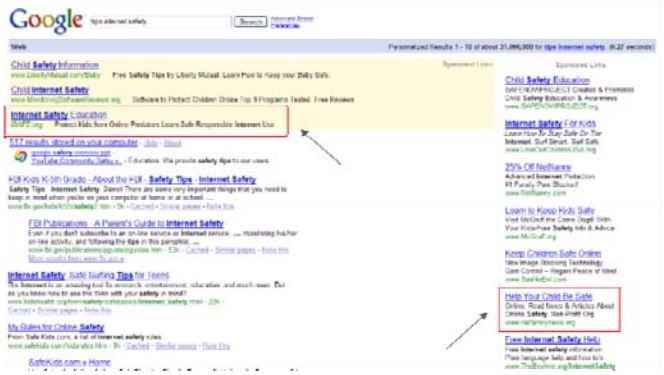
教育　児童保護団体への無償広告の提供

特定非営利活動法人を対象とした Google Grants プログラムにおいて、10団体以上の児童保護団体の検索広告を無償で掲載しています。

「Tips Internet Safety（インターネット・安全・アドバイス）」などの言葉でキーワード検索をすると、児童保護団体のHPへのリンクが広告欄のトップに出てきます。

無償広告を提供している団体
↓

NCMEC、CEOP、ConnectSafely.org、Common Sense Media、the Family Online Safety Institute、i-Safe、iKeepSafe、Net Family News、Childnet、National Society for the Prevention of Cruelty to Children (NSPCC)、Spun Out



DigitalArts

平成22年度総合セキュリティ対策会議　違法・有害情報対策分科会

違法・有害情報対策に関する取組について

～ゲーム機やインターネット対応TV向けフィルタリング～

平成23年2月23日

デジタルアーツ株式会社

本日のご説明

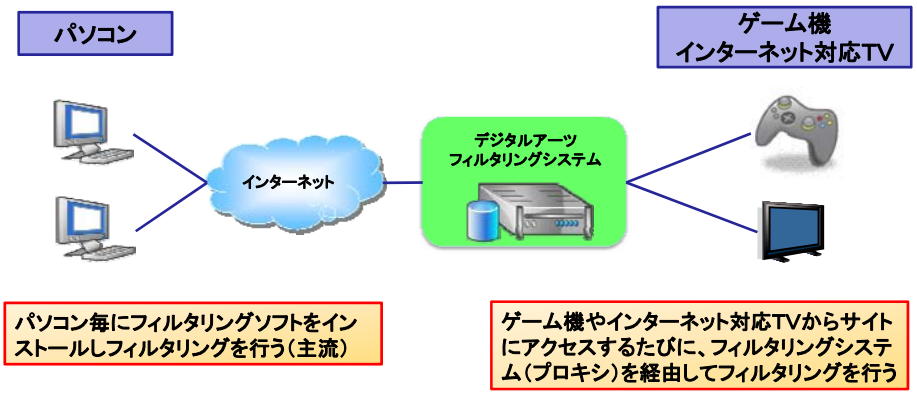
i-フィルター

- ゲーム機やインターネット対応TV向けフィルタリングサービスの仕組み
- ゲーム機向けフィルタリングサービス
  ・フィルタリングサービスの提供状況や加入方法
- インターネット対応TV向けフィルタリングサービス
  ・フィルタリングサービスの提供状況や加入方法
- フィルタリングの普及・啓発活動

フィルタリングサービス の仕組み（概略）

i-フィルター

- ゲーム機やインターネット対応TV向けのフィルタリングサービス
  デジタルアーツ運営のフィルタリングシステムを経由して実施



パソコン毎にフィルタリングソフトをインストールしフィルタリングを行う（主流）

ゲーム機やインターネット対応TVからサイトにアクセスするたびに、フィルタリングシステム（プロキシ）を経由してフィルタリングを行う

ゲーム機向けフィルタリングサービス

i-フィルター

- ゲーム機向けフィルタリングサービス提供先
  子どもの利用するゲーム機にも、安全かつ安心できるインターネットの閲覧環境を提供したいとの各社の考えもあり、2006年よりフィルタリング専用サービスを提供

メーカー名	対応機種	フィルタリングサービス（名称および提供開始月）
任天堂株式会社	Wii（据え置き型）	「i-フィルター for Wii」2007年4月
	ニンテンドーDS（携帯型）	「i-フィルター forニンテンドーDSブラウザ」2006年7月
	ニンテンドーDSi（携帯型）	「i-フィルター forニンテンドーDSiブラウザ」2008年11月
	ニンテンドーDSi LL（携帯型）	「i-フィルター forニンテンドーDSiブラウザ」2009年11月
株式会社ソニー・コンピュータエンタテインメント	PS3（据え置き型）	「i-フィルター for PS3」2007年5月
	PSP（携帯型）	「i-フィルター for PSP」2006年11月
	PSP go（携帯型）	「i-フィルター for PSP」2009年11月

ゲーム機向けフィルタリングサービス

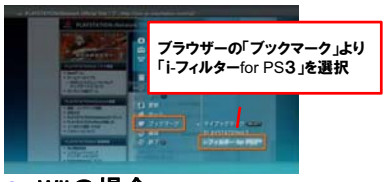
i-フィルター

➢ **サービス案内**

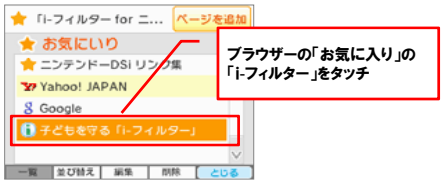
「ブックマーク」や「お気に入り」に予めアイコンを配置し、保護者がスムースにフィルタリングをご利用いただけるよう配慮

● **PSPの場合**

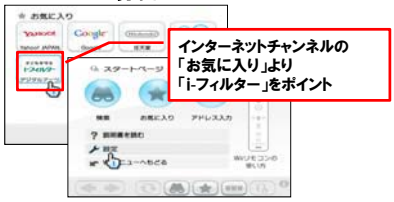
● **PS3の場合**



● **ニンテンドーDSiの場合**



● **Wiiの場合**



➢ **申し込み方法の説明動画** （ http://www.daj.jp/cs/sp/movie/ ）

機器の設定が苦手な方向けに、簡単に手順を解説した動画をご準備

インターネット対応TV向けフィルタリングサービス

i-フィルター

➢ **インターネット対応TV向けフィルタリングサービス提供先**

「青少年インターネット環境整備法」やインターネット対応テレビの普及が見込まれるなか、リビングで観るインターネットでも、ご家族にとって安全かつ安心できる閲覧環境を提供したいとの各社の考えもありフィルタリング専用サービスを提供

メーカー名	対応機種	フィルタリングサービス（名称および提供開始月）
株式会社 日立製作所	ハイビジョンテレビ「Wooo シリーズ」	「i-フィルター for TV」2009年4月
ソニー株式会社	液晶テレビ<ブラビア>	「i-フィルター for TV2」2010年2月
シャープ株式会社	液晶テレビ AQUOS（アクオス）	「i-フィルター for TV2」2010年3月
三菱電機株式会社	液晶テレビ「REAL」	「i-フィルター for TV2」2010年10月

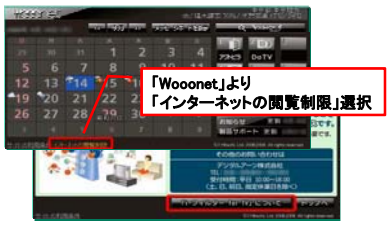
インターネット対応TV向けフィルタリングサービス

i-フィルター

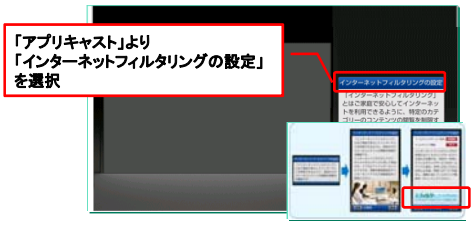
➢ **サービス案内**

インターネット接続画面上などに予めメニューを配置し、保護者がスムースにフィルタリングをご利用いただけるよう配慮

- **日立「Wooo シリーズ」の場合**

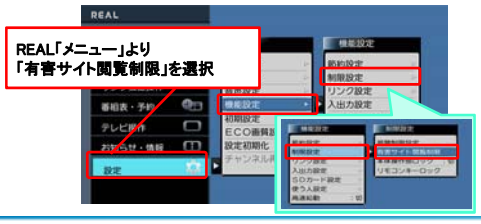


- **ソニー <ブラビア>の場合**



- **シャープ AQUOS（アクオス）の場合**

- **三菱電機 「REAL」の場合**



フィルタリングの普及・啓発活動

i-フィルター

➢ **普及・啓発活動**

行政、NPO、PTAなど各種団体と協力し、37回（2010年）のセミナーや講演会などの啓発活動を実施

➢ **学識経験者と保護者による研究会**

「保護者のためのフィルタリング研究会（座長　下田博次氏）」の運営に参画し、家庭向けフィルタリングサービスの現状と課題について、調査・検討を行い、保護者向けの情報提供と、フィルタリングサービス提供者向けの行動指針等のとりまとめに協力

➢ **普及に向けたフィルタリングソフトの機能向上（パソコン向け）**

子ども専用パソコンだと自由に触れないといった保護者の意見を踏まえ、外部パソコンから遠隔でフィルタリング機能の設定や解除、インターネット利用状況の確認などの保護者の見守り活動を支援する機能を追加した「i-フィルター6.0」を提供（2010年11月）

警察庁　総合セキュリティ対策会議　違法・有害情報対策分科会　資料

違法有害情報対策への取組み

2011年2月23日

ネットスター株式会社

1

事業概要

- フィルタリング・迷惑メール対策等のメーカーや通信事業者等に要素技術を提供（OEM）
  - URLリスト、ソフトウェアモジュール等
  - セキュリティソフトやゲートウェイアプライアンスメーカー、ISP、モバイル通信キャリア等向け
- フィルタリングサービスの提供（自社ブランド）
  - 法人向け・家庭向け
  - パソコン向け・スマートフォン向け

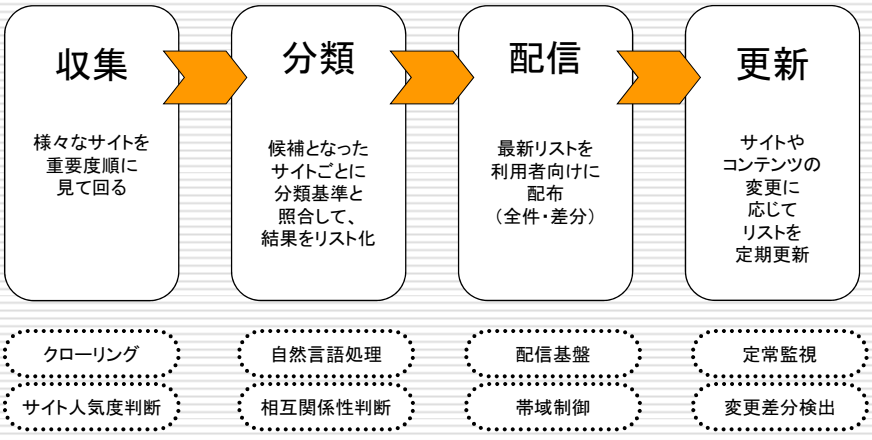
2

URLリストデータ提供先の拡がり

- URLリストデータ
  - アダルト・出会い系・詐欺などの不適切サイトを中心に、URL（サイトアドレス）を網羅的に分類・リスト化
- 従来の主な提供先
  - フィルタリング製品・サービス、迷惑メール対策サービス提供事業者
- 提供先・用途の拡がりの例
  - 交流サイト運営事業者等による、ソーシャルスパム対策業務向けにデータを提供、対策精度の向上や監視等のコスト削減に寄与
  - アフィリエイト広告事業者による、不適切サイトへの広告出稿検知技術サービス向けにデータを提供、広告主による対策を支援

3

リスト作成のための要素技術例



4

要素技術の提供先や用途の例

- 自然言語処理技術
  - リストデータ作成工程の一部として、サイト・ページ内コンテンツの自動分類技術を開発・運用中、その要素技術として、自然言語処理（解析）へ独自の取り組み
- 提供先・用途の例
  - 交流サイト運営事業者等による、自社サイトへの不適切書き込み監視・削除業務は、検出精度やコスト負担が課題
  - 自然言語処理（解析）技術の活用で、多数の利用者の投稿・書き込みの中から、利用規約等に反する、違法または有害な表現等を含むものだけを自動判別することが可能になり、精度向上やコスト削減に寄与

5

利用者啓発への取組み

- フィルタリングの理解・活用の促進
  - 保護者団体や公共機関との連携
    - セミナ講師、教材開発
  - 利用者に伝えるべき知識体系の整理にも尽力
    - 子どもたちのインターネット利用について考える研究会
      - 2008年4月から活動中
      - これまでに「双方向利用型サイトの利用リスク評価モデル」、「段階的利用モデル」を提言
    - 保護者のためのフィルタリング研究会
      - 2010年4月～2011年1月
      - 提供事業者・利用者向けに改善提言・活用ガイドライン提供

※いずれもヤフー株式会社との共同運営

6

違法・有害情報対策に向けた取組み
PhotoDNA技術のご紹介

日本マイクロソフト株式会社
法務・政策企画本部　担当部長
浅井　英里子

MICROSOFT DIGITAL CRIMES UNIT

背景

- 通報に基づく削除要請では、違法・有害情報対策に限界がある
- 一度削除された画像が、再度アップロードされる例が後を絶たない
- 各国における児童ポルノ法制強化（単純所持の罰則化等）により、企業・組織・団体が保有するシステムにおける法令順守が課題となる
- 米国では、ISP等のオンライン・サービス事業者が児童ポルノ画像を検知した場合、NCMEC（National Center for Missing & Exploited Children）へ通報することが法律で義務付けられており、すでに精度の高い画像データベースが存在する

PhotoDNA

- マイクロソフト・コーポレーションの研究部門であるマイクロソフト・リサーチと、米国ダートマス大学が連携して、ハッシュ法 を活用し、インターネット上に存在する画像に識別用のシグネチャを生成し、同一のシグネチャを有する画像を検出・照合する「Photo ＤＮＡ」技術を共同開発
- PotoDNA技術を自社の検索エンジンやオンラインサービスに組み込むとともに、ＮＣＭＥＣに提供することによって、インターネット上の児童ポルノ画像の流出阻止を効率的に行っている。
- 加えて、企業・組織・団体のシステムに児童ポルノ画像が存在しないかどうか検出も可能

紹介ビデオ（英語）：www.microsoftphotodna.com

違法・有害情報に関する取り組み

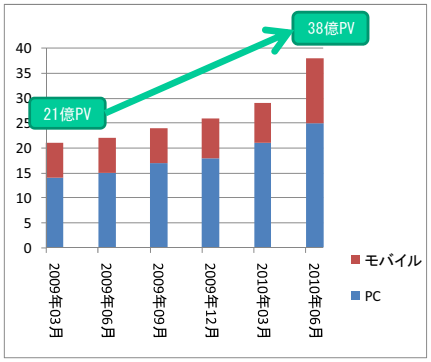
株式会社ライブドア

livedoor

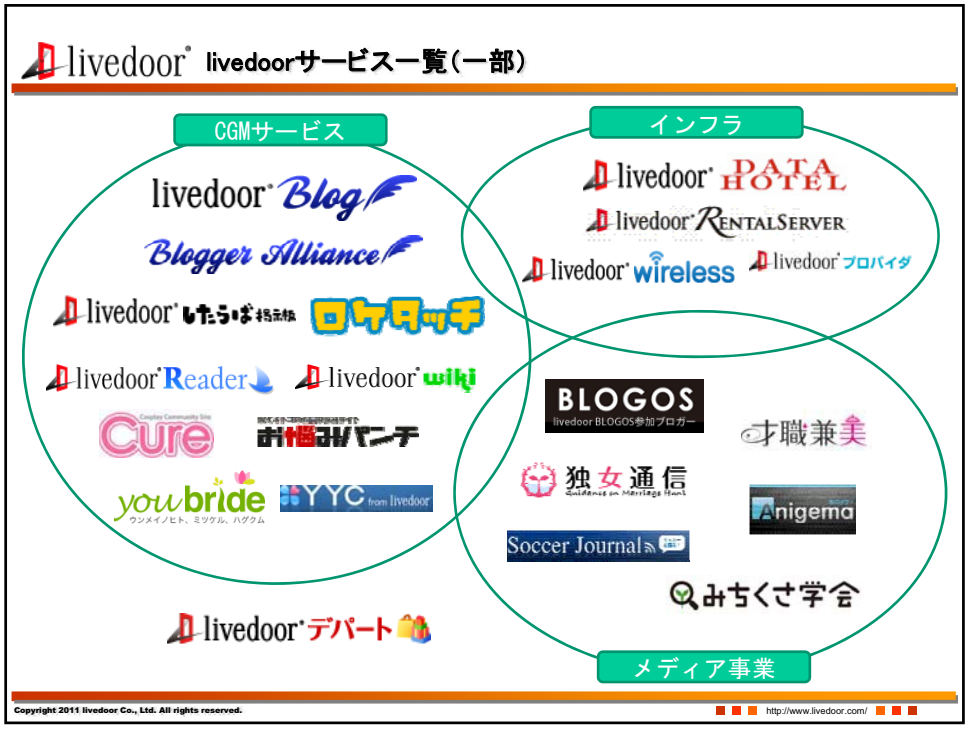
livedoor ポータルサイトlivedoorのご紹介

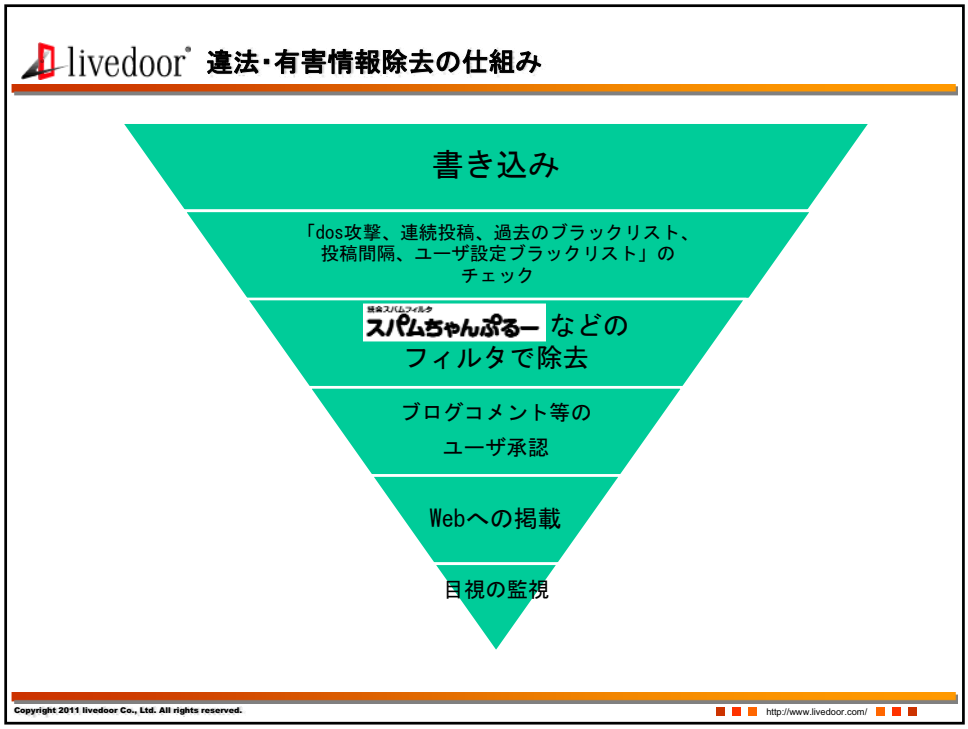
■ポータルサイトlivedoor
・ユーザーID数:900万人(2010年10月現在)
・月間総ページビュー数(PV数):約38.5億PV(2010年10月/自社調べ)
・月間総訪問閲覧者数(UU数):約3,100万人(2010年10月現在/コムスコア調べ)
・男女比:男性65% 女性35% (2010年/Netratings調べ)

■会社概要
・従業員数360名(アルバイト含む)
・売上高:約55億円
(第4期 2010年9月決算)
・2010年5月より[illegible]グループに



http://www.livedoor.com/


livedoor livedoorサービス一覧（一部）
CGMサービス
livedoor Blog
Blogger Alliance
livedoor したらば掲示板
ロケタッチ
livedoor Reader
livedoor wiki
Cure
お悩みポンチ
youbride
YYC from livedoor
livedoor デパート
インフラ
livedoor DATA HOTEL
livedoor RENTALSERVER
livedoor wireless
livedoor プロバイダ
メディア事業
BLOGOS
livedoor BLOGOS参加ブロガー
才職兼美
独女通信
Anigema
Soccer Journal
みちくさ学会
Copyright 2011 livedoor Co., Ltd. All rights reserved.
http://www.livedoor.com/


livedoor 違法・有害情報除去の仕組み
書き込み
「dos攻撃、連続投稿、過去のブラックリスト、
投稿間隔、ユーザ設定ブラックリスト」の
チェック
スパムちゃんぷるー などの
フィルタで除去
ブログコメント等の
ユーザ承認
Webへの掲載
目視の監視
Copyright 2011 livedoor Co., Ltd. All rights reserved.
http://www.livedoor.com/

livedoor 設定による拒否

■運営に支障を来すアクセスの拒否
・dos攻撃などを行うアクセスを拒否
・自動化プログラムによる大量の書き込みを拒否
　⇒その多くが、違法有害情報に関するもの
など

■利用者別の設定
・自分の管理スペースに書き込みができる内容や、書き込みできる人などについて、管理が可能
・禁止ワード設定
・不適切な利用者の書き込みを拒否
・ブログでは、承認制による事前チェックも可能
など

ブログコメント設定（利用者の画面）

ブログ禁止ワード設定（利用者の画面）

livedoor フィルタでの除去

■「スパムちゃんぷるー」について
・「スパムちゃんぷるー」は弊社独自開発フィルタ
・ブログや掲示板等のサービスで使用
・数十種類のプラグインを用意
・プラグインの組み合わせでサービスごとに最適化
・機能の一部をサービス運営者へ無料開放

一部機能の提供を説明するページ

■プラグインについて
・単純に過去の掲載内容から学習したプラグイン
・ログを集計して除去リストに入れるプラグイン
・過去の判定結果をもとに再学習するプラグイン
など

livedoor フィルタでの除去

■判定
・一つ一つのプラグインが判定（採点）
・判定結果を総合判断
・合議制で一定以上の点数になるとアウト

※合議制・・・採点結果を独自の計算式に入れ、
いわば合議制のような仕組みになっています

■違法・有害情報対策
・携帯電話、銀行口座等の売買を未然に防ぐ
・出会い系サイトへの誘導なども阻止
など

管理画面の一例
※上記はYAPC::Asia 2008で発表したもので、
現在のバージョンと異なります。

livedoor 違法・有害情報の監視体制

■目視による監視
・フィルタをすり抜けたものを目視監視
・異常動作があったものをくまなくチェック
・フィルタへデータを登録し最適化

■監視体制
・2004年10月から実施
・24時間365日体制で監視
・東京と地方複数拠点で相互チェック
・地方では在宅障害者雇用と絡めて行っている

■在宅障害者雇用について
・在宅障害者で5名の正社員を雇用
・短時間しか労働できない障害者も登用
・2006年にテレワーク推進賞の奨励賞を受賞

在宅での仕事の様子

毎月実施している研修会の様子

livedoor 監視業務

■監視業務方法（サービスにより異なるため、あくまで一例）
・自動検出分のチェック
　アラートで上がった内容の監視
・通報内容のチェック
　閲覧者から通報していただいた内容の監視
・新規投稿内容のチェック
　投稿された内容の監視

管理画面一例

■見つけた場合の対処方法
・軽度の場合、掲載者に自主削除要請
・消えない場合や、軽度以外のケースでは当方で削除し警告
・再掲時は削除＋厳重警告、止まらない場合アカウントの削除や退会措置
・メールアドレスなどの情報を元に、再利用をお断りするケースあり

livedoor 利用者への注意喚起

■利用者への注意喚起
・自ら掲載しないように注意喚起
・各種法令の解説ページへ誘導
・掲示板やブログの管理者においては、コメントなど
　他者の書き込みを管理する責任が生じることの説明

サービス利用者への注意喚起ページ

掲示板管理者向けの注意喚起ページ

サイバー防犯ボランティアの育成について

「自分たちの町は自分たちで守る」という趣旨の下、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社会における自主防犯ボランティアの青パト[1]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と言われている。一方、サイバー空間においても、警察と連携したサイバーパトロールや青少年の不適切なインターネット利用者に対する補導等を通じて、様々な個人・団体が、安全で安心して利用できるインターネット社会の実現を目指して活動している。しかし、刑法犯認知件数が７年連続して減少している現実社会と比較して、サイバー空間では、サイバー犯罪の検挙件数は年々増加し、さらに都道府県警察の相談窓口へ寄せられるサイバー犯罪等に関する相談も増加しており、サイバー空間における早急な治安改善対策が求められている。

平成 22 年度総合セキュリティ対策会議の下に置かれた「サイバーボランティア育成分科会」では、「サイバーボランティアの支援・育成について」を課題として議論を行い、サイバー空間の規範意識の低下への対策として、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、結成を促進し、官民連携により育成する気運を醸成することの必要性を認識するに至った。

本報告書では、本分科会における審議結果を踏まえ、サイバー空間の現状と実際にサイバー空間で防犯ボランティア活動に従事している団体を紹介し、サイバー防犯ボランティアの活動要領、サイバー防犯ボランティアの育成の在り方、サイバー防犯ボランティアの組織化について提言することとする。

第１章　サイバー空間における防犯ボランティア活動

情報技術の高度化・普及、高度情報通信ネットワークの発展に伴い、インターネットは国民生活の中へ急激に浸透している。これにより、国民生活の利便性が高まる一方で、匿名性の高いサイバー空間では何をやっても許されるという誤った風潮が蔓延している。刑法犯認知件数が年々減少する中、サイバー犯罪の検挙・相談件数は増加の一途をたどり、また、多数の違法・有害情報が書き込まれ、削除依頼に応じることなく放置されたままのインターネット掲示板の存在も社会問題化している。サイバー犯罪対策や違法・有害情報対策として、官民一体となった取組を推進しているところであるが、「自分たちの利用するインターネットの安全は自分たちで守る」と利用者自身が防犯意識を高め、インターネット上の安全を守る活動を他の利用者に示すことにより、一般利用者の規範意識を高める取組が求められる。本章では、サイバー空間における規範意識の現状とそれを改善する担い手として期待できるサイバー防犯ボランティアの役割について述べることとする。

1　青色回転灯を装備した防犯パトロール用自動車。

第１　サイバー空間における規範意識

人は、その経験を通じて、法令・モラル等の社会規範を守ろうとする意識が育まれる。この意識が社会の治安を維持する上で重要な役割を果たしている。しかし、サイバー空間においては、その匿名性の高さや「インターネットでは何を行ってもよい」という誤った認識の広まりなどから、利用者の中に法令・モラル等の社会規範を守ろうとする意識が十分に働いているとは言えない状況にある。

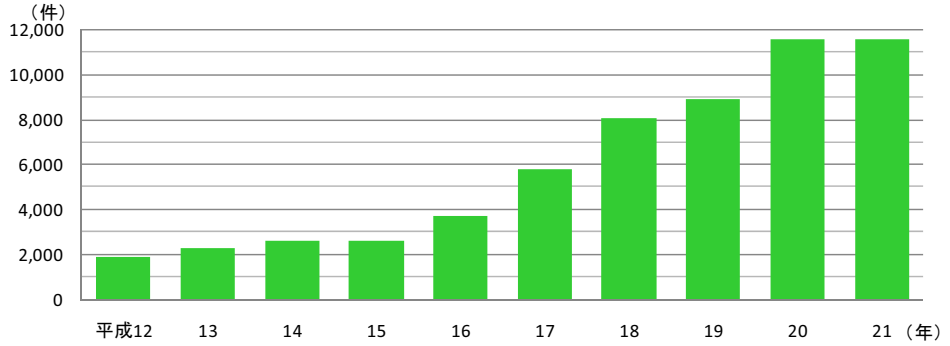
１　規範意識とは

規範とは、「判断・評価または行為などの拠るべき基準」（広辞苑から）を言い、規範意識は、「法令・モラル等の社会規範を守ろうとする意識」と言うことができる。規範意識は、人の内心にあって人の行動を正しい方向へと導いていくものであり、規範意識が人の内心に形成される過程では、諸々の要因がそれに影響を与えるものと考えられる。そのような諸々の要因には、その人の置かれた環境や今まで受けた教育、関係する法律や警察による取締りといったものが考えられる。

２　規範意識の現状

現実世界の公共空間で見られる迷惑行為、例えば、公共の場所で他人に対して大声で暴言を吐くといった行為を例に挙げると、そのような行為を注意できる人が減ってきていると言われるものの、多くの周りの人の目に見られているという事実が、そのような行為を行うことを思いとどまらせている、すなわち、現実世界では「多くの周りの人の目」が人の規範意識の保持に影響を与えているという見方もできる。しかし、サイバー空間においては、自分の姿が周りから見えていないという匿名性を悪用して前掲[2]のとおり違法・有害情報が氾濫しているほか、違法・有害情報には至らないものの、インターネット掲示板に他人の個人情報やプライバシーを公開したり、他人に対する無責任な中傷といった書き込みなどが安易に敢行されやすい。

図１―１　インターネット上の名誉毀損・誹謗中傷に関する相談件数



	平成12	13	14	15	16	17	18	19	20	21
インターネット上の名誉毀損、誹謗中傷に関する相談	1,884	2,267	2,566	2,619	3,685	5,782	8,037	8,871	11,516	11,557

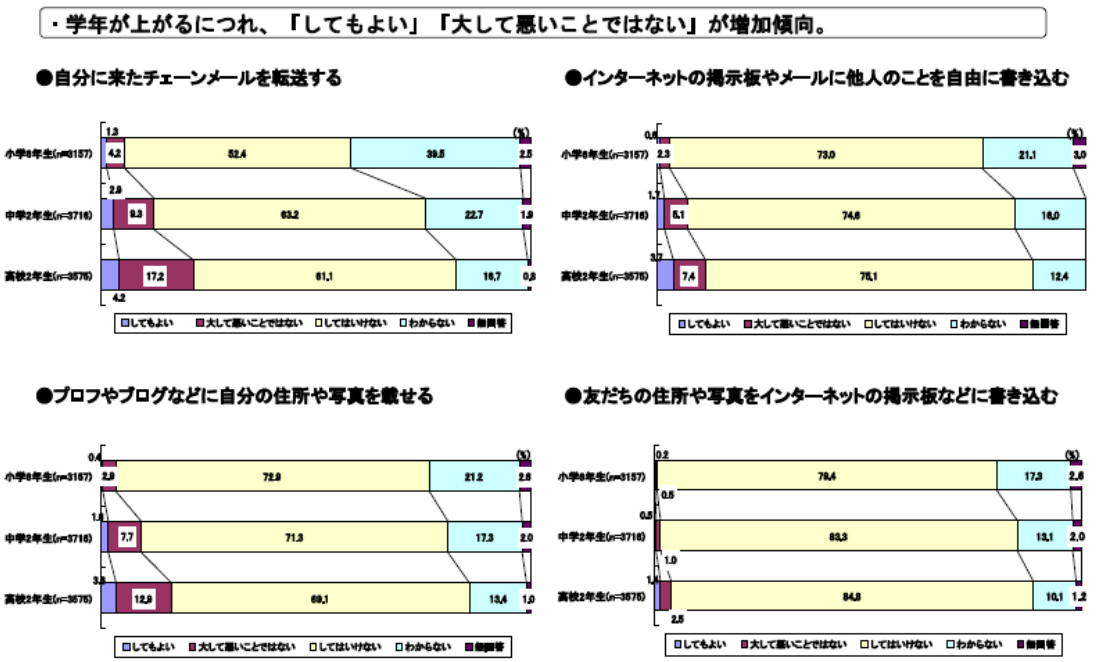
※　都道府県警察の相談窓口に寄せられた相談

2　「今後のインターネット上の違法・有害情報対策について」第１章参照。

各都道府県警察においては、多様化するインターネットに関する相談を受理し、必要に応じて相談者に対し、助言・指導を行っているところであるが、この相談窓口に寄せられたインターネットに関する相談の中で名誉毀損・誹謗中傷に関する相談件数は年々増加しており、平成 21 年には 11,557 件を受理している（図１－１）。

平成 20 年 11 月から 12 月にかけて、文部科学省が、全国 5,000 の小学校、中学校、高等学校を対象に、子どもたちの携帯電話の利用実態や意識等について、児童生徒とその保護者を対象として調査を実施したところ、インターネットの利用態様に関する意識では、自分に来たチェーンメールを転送する、インターネットの掲示板やメールに他人のことを自由に書き込む、プロフやブログに自分の住所や写真を載せる、友達の住所や写真をインターネットの掲示板に書き込むといった行為について、いずれも学年が上がるにつれて、「してもよい」、「大して悪いことではない」と回答した者が増加しており、子どものインターネット利用に関する規範意識が、年齢が増すとともに低下している状況がうかがわれた（図１－２）。

図１－２　インターネットの利用態様に関する意識[3]



３　規範意識の低下を示す事例

インターネット上に掲載されている情報の中には、わいせつ画像、児童ポルノ画像、規制薬物の広告のように、掲載すること自体が違法に当たる違法情報や、違法情報に

3　「子どもの携帯電話等の利用に関する調査」の結果について（平成 21 年５月 15 日文部科学省公表）

は当たらないものの、殺害や報復の請負のように犯罪行為を助長したり、人を自殺に誘引するなどの公序良俗に反する有害情報が多数含まれているが、このような違法・有害情報には至らないものの、他人の個人情報やプライバシーを無断で公開するといった情報や他人を中傷する情報も含まれている。

サイバー空間における規範意識の低下を示す実際にあった事例として、公の場であるインターネット上の違法情報対策や児童の被害防止対策の重要性を述べた者に対して、誹謗中傷する書き込みがなされた事例、動画投稿サイトに人気漫画を無断で公開した者に対して、著作権法違反に当たるとして違法行為を止めるようにインターネット掲示板で注意したところ、逆に注意した者に対して、「君は何様のつもりだ」とか「早く死んで下さい」等と非難する書き込みが続いた事例（図１－３－１）、「死んでほしい人」というタイトルのインターネット掲示板に、実在する学校名、個人の名前が書き込まれ、さらに真偽の判断が困難な無責任な書き込みが追加された事例（図１－３－２）、プロフと呼ばれる自己紹介サイトに、未成年が名前、住所とともに自らの裸の写真を掲載した事例等が見られる。

図１－３－１　規範意識の低下を示す事例１

著作権法違反を注意した者に対し、逆に注意した者を批判する書き込みが続いた事例

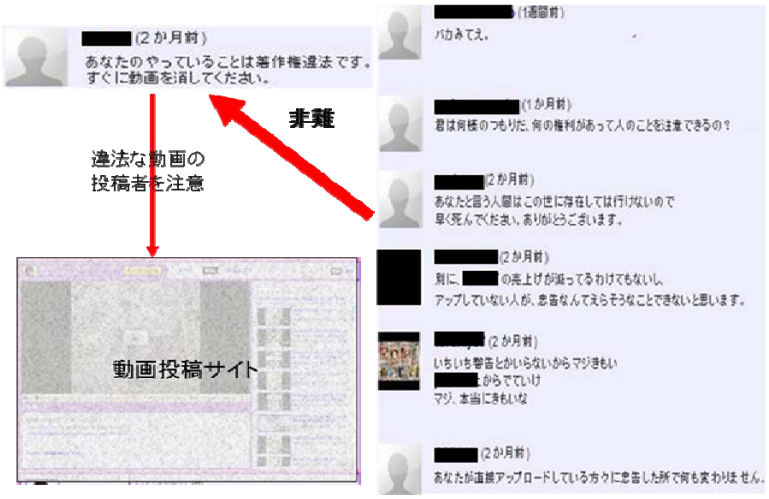
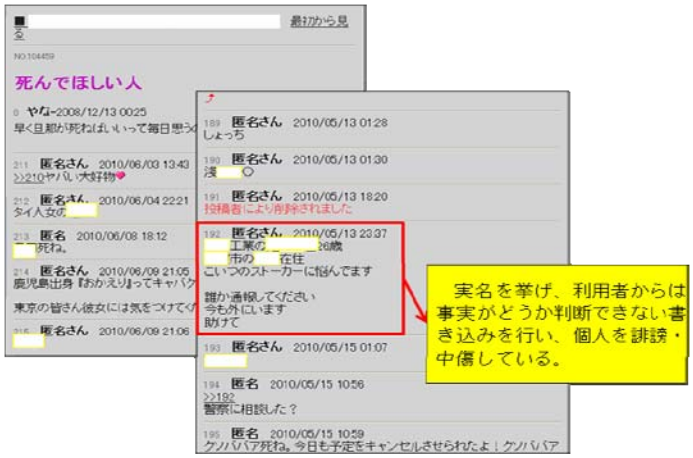


図１－３－２　規範意識の低下を示す事例２

「死んでほしい人」という掲示板に実名が書き込まれた事例



4　規範意識の改善に向けて

現実社会においては、平成 14 年当時、刑法犯認知件数が約 285 万件に達し、街頭犯罪・侵入犯罪や来日外国人犯罪も増加するなど、国民の犯罪被害に対する不安はより身近に感じられるようになっていた。他方で、治安悪化の一因に規範意識の低下や住民相互の人間関係の希薄化があり、これらをいかにして改善するかが治安回復の鍵であると認識されていた。このような状況の下、防犯ボランティア団体の結成により、自らの手で身近な犯罪を抑止しようとする動きが国民の間に広がりはじめ、平成 15 年には約 18 万人だった防犯ボランティアの人数は、平成 21 年には約 263 万人へと急増していった。

平成 21 年の刑法犯認知件数は約 170 万件と平成 15 年以降 7 年連続で減少したところであるが、この成果には、警察による街頭犯罪・侵入犯罪に対する強力な取締りに加えて、街頭パトロールや広報啓発活動を地道に推進し、地域住民の規範意識の改善に取り組んできた防犯ボランティアが果たした役割も大きいと考えられる。

現在のサイバー空間の現状は、違法・有害情報の氾濫やインターネット利用者の規範意識が低下している状況等、平成 14 年当時の現実社会の犯罪情勢と類似する点も多い。よって、低下したサイバー空間の規範意識を改善するためには、前掲[4]のとおり警察による違法情報の強力な取締りや関係機関、事業者等による違法・有害情報の排除に向けた取組と並行して、サイバー空間における防犯活動を行うサイバー防犯ボランティアの活動が期待されるところである。

以上のサイバー空間の現状を踏まえ、サイバー防犯ボランティアが果たす役割やその効果等につき検討する。

第２　サイバー空間における防犯ボランティアの活動例

現在、サイバー空間では、様々な個人・団体が防犯ボランティア活動に取り組んでいる。その活動例として、サイバーパトロールによるサイバー空間の浄化活動、専用システムを利用した悪質なインターネット利用者への指導、注意活動、インターネット利用者やその保護者への教育活動、自治体と連携した防犯ボランティアの育成事業、広報啓発活動等について紹介する。

1　サイバーパトロールモニター

パソコンや携帯電話を使用して、サイバー空間に存在する違法・有害情報を発見する活動をサイバーパトロールと呼んでおり、全国 18 の県警察では、民間のインターネットに関する知識に長けている者を「サイバーパトロールモニター」として委嘱し、違法・有害情報を発見した場合には、警察への通報等を依頼している。これらの県警

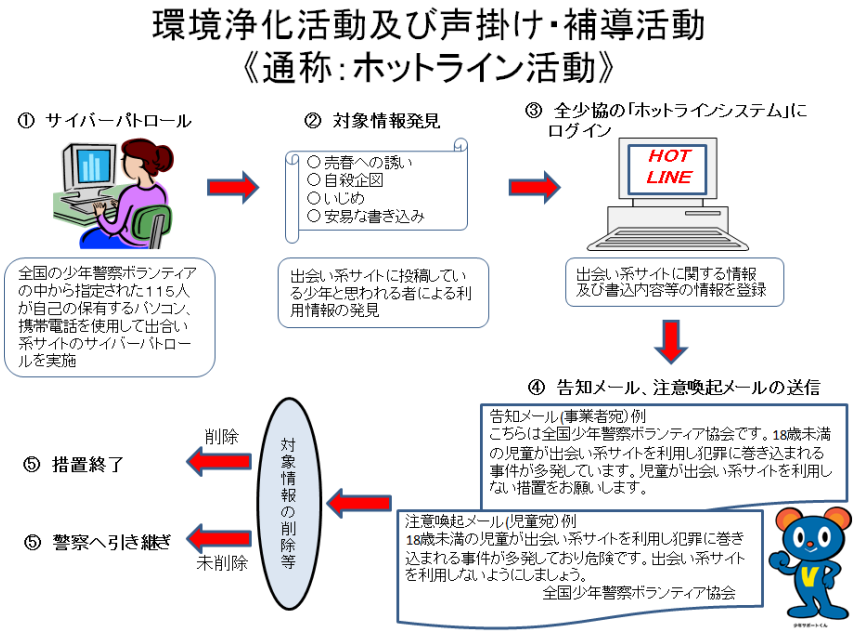
4　「今後のインターネット上の違法・有害情報対策について」第 2 章参照。

察では、平成 21 年中、19 団体 357 人に委嘱しており、これらサイバーパトロールモニターがサイバーパトロールを通じて、1,561 件の違法・有害情報を警察へ通報している。サイバーパトロールモニターから通報された情報は、それぞれの県警察で、児童ポルノ公然陳列や出会い系サイト規制法[5]に規定する禁止誘引行為（児童を性交等の相手方となるように誘引する行為等）等の事件の検挙に結びついたほか、サイト管理者への削除依頼による違法・有害情報の流通防止や、サイバー空間に関する実態把握のために活用され、サイバー犯罪の取締りやサイバー空間の浄化に寄与している。

2　全国少年警察ボランティア協会

全国少年警察ボランティア協会（以下「全少協」という。）では、青少年の健全育成に寄与するため、少年補導員等の少年警察ボランティアによるインターネット上の環境浄化活動、声掛け・補導活動、少年相談等を組織的に推進している。具体的には、インターネット上に「ホットラインシステム」と呼ばれるプラットフォームを構築し、このシステムを活用することにより少年警察ボランティア個人のプライバシーや安全性を保護しつつ、インターネット上に氾濫する少年に有害な情報を提供するサイトの管理者に対して、少年の健全育成を阻害しないよう必要な措置を求める告知メールを送信する環境浄化活動や、不適切な書き込みを行っている青少年に対して、出会い系サイト利用の危険性や個人情報を掲載する行為の危険性を注意喚起するメールを送信するインターネット上での声掛け・補導活動を推進している（図１－４）。平成 21 年中、サイト管理者に対して 124 件の告知メールを、青少年に対して 3,367 件の注意喚起メールを送信している。また、全少協では、ホームページ上に会員専用掲示板を設けて、全国の会員同士の情報の共有と連帯意識の向上を図っている。

図１－４　全少協のホットライン活動の流れ



[5] インターネット異性紹介事業を利用して児童を誘引する行為の規制等に関する法律（平成 15 年法律第 83 号）

3　日本ガーディアン・エンジェルス

日本ガーディアン・エンジェルスでは、現実社会における街頭でのパトロール活動、イベントサポート活動等の地域安全や子どもの健全育成を図る活動以外に、インターネットの安全利用やインターネットが関係する事件、トラブルの防止に関する広報啓発活動に特化した活動をする「サイバー・ガーディアン・エンジェルス」を組織し、民間事業者と連携したインターネット安全教室や独自のインターネットの安全に関する講演活動など啓発に重点を指向した取組を推進している。具体的には、電気通信事業者との共催により、小・中学生を対象に、実際にパソコンを操作しながら、インターネット上の事件やトラブルから身を守る方法を学ぶ体験型の「インターネット安全教室」を開催しているほか、インターネットの安全利用に関するハンドブックや携帯用小冊子を作成・配付するなどの広報啓発活動を行っている（図１－５）。

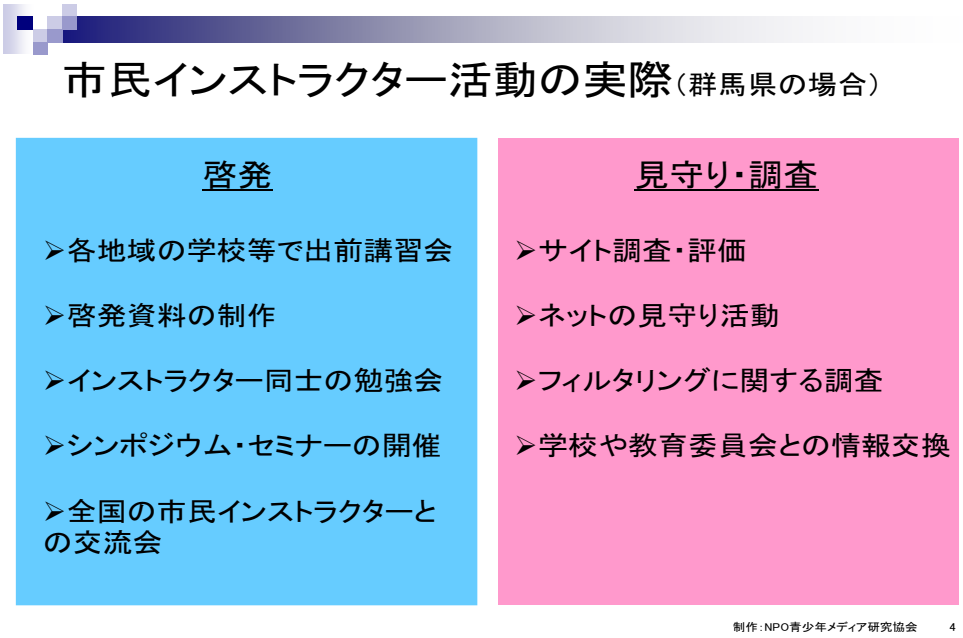
図１－５　サイバー・ガーディアン・エンジェルスによる講演活動

4　青少年メディア研究協会

青少年メディア研究協会では、インターネット時代の子育て、教育の責任者である保護者と教師の能力向上を目的として「市民インストラクター養成講座」を開設している。「市民インストラクター養成講座」では、自治体からの要請により、子どものインターネット利用に関する危険性やペアレンタル・コントロール（子どものメディア利用の管理・指導）の原理を理解するための講座のほか、インターネット上の各種コンテンツを評価できる能力を獲得するための実技指導を通じて、携帯電話やゲーム機などインターネット端末機の特性を理解し、子どものメディア利用を見守り、指導

できる保護者や、保護者と連携して学校教育に当たることができる教師を「市民インストラクター」として養成している。市民インストラクターは、養成講座やその後の勉強会の場を通じて習得した知識を用いて、各地域の学校における出前式の講習会やシンポジウム・セミナー等の開催による啓発活動のほか、インターネット上での子どもの見守りや、ウェブサイトの閲覧・監視活動であるサイトモニタリングによる各種インターネットコンテンツの調査・評価といった見守り・調査活動を推進している（図１－６）。

図１－６　市民インストラクター活動



また、青少年メディア研究協会は、携帯電話を利用することのリスクから子どもを守る活動を続けている保護者や学校関係者、自治体、民間事業者と連携して、全国各地で「子どもの携帯電話利用を考える全国市民会議」を開催し、それぞれの活動内容の発表や情報交換等を通じて、子どもを取り巻くインターネット利用環境の把握と課題の共有を図っている。

5　サイバーモンキーズ

「学生の街・京都」の特性を活かし、京都府内の大学に在籍する学生により防犯ボランティア「ロックモンキーズ」が創設され、自主的な防犯活動を行っている。

「ロックモンキーズ」では、平成 22 年度からサイバー空間にも活動の場を広げ、サイバー空間における防犯活動を行う際には、「サイバーモンキーズ」と称して、サイバー空間における浄化活動や各種広報・啓発活動を行っている。具体的には、インターネット上に流通する違法・有害情報の警察への通報や、各種イベントの開催時や街頭キャンペーンの機会を捉えて、インターネットの安全利用や被害防止を呼びかける啓発チラシの配布やポスターの掲載といった広報・啓発活動に取り組んでいる。

以上、サイバー空間で防犯ボランティア活動に取り組んでいる団体の活動について紹介したが、これら団体の活動は、サイバー空間の浄化活動やインターネット利用者に対する安全・安心な利用促進を目的とするものであり、これらの活動はサイバー空間の規範意識の改善につながるものと期待されている。

第３　サイバー防犯ボランティアに期待される役割

第２で見たサイバー空間における防犯ボランティアの活動例を踏まえると、サイバー空間における防犯ボランティアには、次のような４種の活動を中心として、サイバー空間における規範意識の改善に貢献することが期待できる。

１　サイバー空間の浄化活動

パソコンや携帯電話を利用してサイバーパトロールを実施し、インターネット掲示板やサイトに掲載された違法・有害情報を発見した場合は、インターネット上の違法・有害情報を受け付け、警察への通報やサイト管理者等への削除依頼を行っている「インターネット・ホットラインセンター」（http://www.internethotline.jp/）へ通報する。犯行予告や自殺予告等の人命保護の観点から早急に対応する必要がある情報については、関係都道府県警察へ通報する。違法・有害情報は、キーワードや隠語による検索エンジンでの検索、常習的に違法・有害情報が掲載される掲示板の検索、発見した違法・有害情報掲載サイトに貼られたリンクの確認といった方法により発見することが考えられる。

２　犯罪被害防止のための教育活動

これからインターネットを利用し始める小学生、中学生を対象に、インターネットを利用する上でのモラル、インターネットの危険性について教育するとともに、その保護者に、家庭でのインターネット利用に関するルール作りを提唱する。また、高校生や一般利用者に対しては、サイバー犯罪の実態、サイバー犯罪の被害に遭わないための対策等についての教育活動を行う。その具体的な方法として、インターネットの危険性について、実際にパソコンや携帯電話を用いて体験させる研修会や勉強会の開催、青少年のインターネット利用犯罪の被害実態の紹介といった、利便性の陰に隠れたインターネットの姿を、特に保護者に理解させることが効果的である。

３　広報啓発活動

サイバー犯罪の被害防止やインターネットの安全利用を呼び掛けるため、自治体、関係事業者と連携し、インターネット利用者のみならず、広く一般国民に対し、街頭でのキャンペーンやイベントを通じて、最新のサイバー犯罪の実態等について広報し、サイバー犯罪被害防止のための広報啓発活動を行う。その具体的な方法として、政府で定める情報セキュリティ月間（２月）に合わせたキャンペーン、セミナー、シンポ

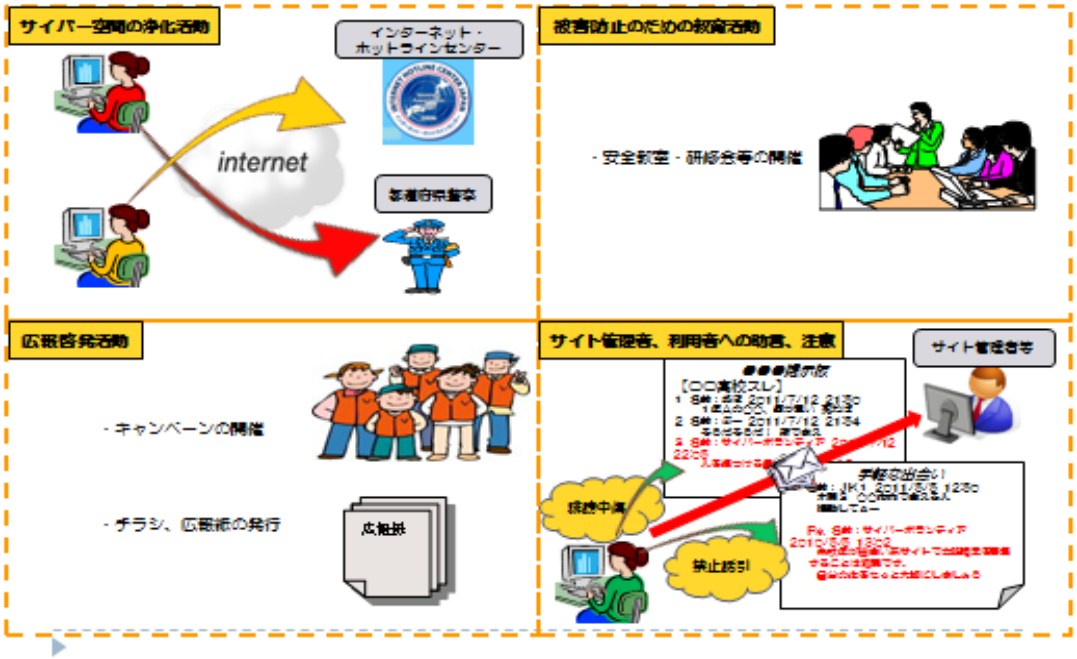
ジウム等を開催して行う、広報・啓発チラシの配布、防犯や情報セキュリティの専門家による講演、パネルディスカッションを通じた広報・啓発活動が考えられる。

4　サイト管理者、利用者への助言、注意

サイバーパトロール等を通じて、違法・有害情報には至らないものの、インターネット上に他人の人権やプライバシーを侵害する書き込みや公序良俗に反する情報、少年の健全育成を害する情報を発見した場合、そのサイトの管理者や書き込んだ者に対して、サイトの運営方法の改善やインターネットの安全・安心な利用法について助言、指導を行う。助言、指導を行うに当たっては、専用のシステムやフリーメールアドレスを利用するなどして、防犯ボランティアのプライバシーや安全性を確保することが必要である。その具体的な方法として、助言、指導の対象となる情報をあらかじめ定めておくとともに、助言、注意の具体的内容についても定型化しておくと効率的である。また、助言、指導に対する反論、抗議に対する対処方針、方法についても事前に検討しておく必要がある。

助言、指導に応じることなく、違法・有害行為を誘発したり、容認しているサイトについては、警察と連携した対応も検討する必要がある。

図１－７　サイバー防犯ボランティアに期待される役割



第２章　サイバー防犯ボランティアの活動

現実社会の自主防犯ボランティアは、多くの仲間と一緒に活動する中で、適切・模範的な活動が自然と身に付いていくと考えられる。一方、サイバー防犯ボランティアは、相手の見えないサイバー空間において、また、インターネット端末の前で一人で取り組むことが多いことから、その活動に当たっては、より活動しやすいよう具体的な要領を示す必要がある。本章では、サイバー防犯ボランティアが活動するに当たって留意すべき事項について述べることとする。

第１　人材の募集

サイバー防犯ボランティアの募集に当たっては、サイバー防犯ボランティアの活動上有する特性を理解しつつ、募集の門戸を広げ、より多くの適した人材を確保する必要がある。

１　基本的な考え方

サイバー防犯ボランティアの活動に際しては、防犯ボランティア自らの安全を確保しつつ、サイバーパトロールやサイト管理者・利用者への助言・注意を行う場面や、教育活動における講習会の場での質疑への対応の場面等において、インターネットに関する知識や技能を求められることが少なくない。よって、人材を確保する上では、これらの知識等を有する者を募集する必要があるが、これらが募集の門戸を狭める要因ともなり得るところである。他方で、サイバー防犯ボランティアの活動には広報啓発活動のように、必ずしも高度な知識を要しない活動もあるため、活動をより平易なところから始め、これらの知識を習得していく過程で徐々に活動の範囲を広げていくことも考えられる。

２　幅広い人材の募集

サイバー防犯ボランティアの人材募集に関しては、インターネットに関する知識や技能を要することが、募集の門戸を狭める特性がある反面、インターネットの特性による利点も存在する。すなわち、現実社会における防犯ボランティアの活動に見られるパトロール活動等の多くは時間的、場所的制約を受けることとなるが、サイバー空間の浄化活動やサイト管理者・利用者への助言・注意といった活動は、時間的、場所的な制約を受けることなく、好きな時に好きな場所で行うことができる。普段から防犯ボランティア活動に参加したいという意思を持ちながらも、時間的、場所的制約から防犯ボランティア活動に取り組めないといった者に対して、サイバー防犯ボランティアの活動への門戸を広げ、防犯ボランティア活動を始めるきっかけとして捉えることもできる。

３　防犯ボランティア活動の地域性

「インターネットは全世界共通」という考え方から、サイバー防犯ボランティアの

活動に地域性は必要ないという意見もあり、市町村や都道府県の枠を超えて防犯ボランティア団体として組織化し活動していくことも可能である。その反面、活動の趣旨・目的や内容によっては、防犯ボランティア個々人相互が比較的近い地域に居住している方が、より効果的かつ効率的に活動を推進できることも多く、特定の地域に密着したサイバー防犯ボランティアの活動も期待されるところである。

第２　活動要領

サイバー防犯ボランティアが適正に活動するためには、具体的なガイドラインに基づき活動すること、活動を適正に管理すること、積極的に関係機関と連携すること等が求められる。

１　活動ガイドライン

サイバー防犯ボランティアの活動に際しては、活動の目的や方法、活動時の留意事項等をまとめた活動ガイドラインに基づき活動することが重要である。多くの防犯ボランティアは強い正義感を持つことから、過去にはその強い正義感のゆえに、防犯活動という本来の目的を逸脱し、本来警察等の捜査機関がすべき犯人の検挙、取締りに目的を指向したがために活動の限界を実感し、防犯ボランティア活動が持続しなかったという事例も存在する。また、特にサイバーパトロールといったサイバー空間の浄化活動やサイト管理者、利用者への指導、注意活動は、防犯ボランティア個々人が単独で行い得る活動であり、防犯ボランティア相互の目に触れることが少ないことから、防犯ボランティア側がインターネット上における誹謗中傷被害やワンクリック詐欺等の架空請求・不当請求といった犯罪被害に遭うケースも想定されるところである。これらの被害から防犯ボランティア個々人を保護するとともに、サイバー防犯ボランティアの活動の適正性を保つ観点から、各サイバー防犯ボランティアが活動ガイドラインを定め、同活動ガイドラインに沿った活動を推進することが求められる。

２　活動の管理

現実社会における防犯ボランティアの活動においては、合同パトロール活動等のように防犯ボランティアが相互に意見交換を行って、補導や注意活動を行うなど、相互に連携して活動する場面がほとんどである。しかしながら、サイバー防犯ボランティアの活動は、サイト管理者や利用者への指導・注意活動のように、活動の内容が高度化するにつれて、防犯ボランティア個々人による単独の判断が求められる場面に遭遇することが予想される。その際、誤った判断、行き過ぎた行為を防ぐために、日頃から研修の機会を提供するとともに、活動を適正に管理することが必要である。

適正な活動を行うためには、活動を管理する立場のリーダーを配置したり、インターネット上に専用のサイトを設けて活動計画等を報告させ、代表者がそれを把握するといった方法が考えられる。

3　関係機関との連携

サイバー防犯ボランティアが、より効果的かつ効率的に活動を実施するためには、サイバー空間の実態や被害防止に資する情報等のインターネット関連情報を幅広く収集して、実態に即した活動を推進することが望ましい。また、市民から防犯ボランティア活動への理解と協力を得ることも重要な要素となる。適時的確な情報を収集し、市民の理解と協力を得るための一つの方法として、警察や教育機関、自治体、インターネット関連事業者との連携を密にすることがある。例えば、犯罪の被害実態を知るためには警察、児童のインターネット利用実態を知るためには教育機関、情報セキュリティに関する情報を知るためにはインターネット関連事業者から情報提供を受けることが考えられる。また、これらの行政機関や企業等の後援、支援を受けることで、防犯ボランティア活動に対する市民の信頼を得やすくなり、さらに、活動に要する資金や資機材の面でも支援を得ることも可能である。そのほか、サイバー防犯ボランティア活動において、情報提供や支援を受けるばかりではなく、インターネット利用者の立場から、インターネット関連事業者、携帯電話事業者、サイト管理者の提供する各種インターネットサービスを随時点検し、その改善点を調査・評価し、その結果を各事業者や関係機関に対して情報提供することで、その活動への理解が得られ、サイバー防犯ボランティア及び関係機関相互の良好な関係を醸成し得るものと考えられる。

第3　活動の維持、継続

サイバー防犯ボランティアにとって、その活動を維持、継続させることは、大きな課題である。その課題を克服するため、何のために活動をやるのか明らかにすること、活動の成果が目に見える形で表れる場を提供すること、あらゆる機会に広報を行うこと、個々の防犯ボランティアの安全を確保することなどを通じて、活動に「やり甲斐」を見いだすことが必要である。

1　活動の動機付け

活動に当たっては、明確な動機付け、「この活動は何のためにやるのか」を明確に示す必要がある。明確な動機付けなく活動を開始した場合には、防犯ボランティア個々人の意思疎通が図れず、活動の方向性が不安定となるため、活動が低迷、衰退する要因となり得る。また、動機付けも、「サイバー空間の被害防止」といった漠然としたものよりも、活動する地域や対象が抱える問題点を的確に捉えたより具体性のあるものとすることが望ましい。例えば、地域の子ども達の間でインターネット上でのいじめやコミュニティサイト利用に関する問題が発生しているのであれば、「潜在化している、いわゆる学校裏サイトにおける子どものいじめ防止」とか「携帯電話のコミュニティサイトにおける子どもの犯罪被害防止」といったより具体的な内容が望まれる。

2　効果的な活動の場の提供

サイバー防犯ボランティアの活動に当たっては、活動の動機付けに対する活動の成果がより顕著に現れる場を得ることが重要である。防犯ボランティア活動においては、活動を行う側とそれを享受する側との意思が一致することで、より高い効果が得られることは言うまでもないが、防犯ボランティア個々人が活動に対する達成感や充実感を得る上でも、活動の成果がより顕著に現れる場を得ることは必要となる。例えば、児童の安全・安心なインターネット利用を促進するための啓発活動を行うには、真に啓発の必要な児童の保護者がより多く集まる機会（入学式、入学説明会等）を得ることが効果的である。また、入学式や入学説明会等の場は、小中学校等の教育機関やそのＰＴＡに働きかけることで得られやすくなるものと考えられる。

また、防犯ボランティアが活動することを楽しく思い、自ら向上心を持って活動に当たる雰囲気が求められるところ、効果的な活動の場を得ることで、防犯ボランティア個々人は活動に対する達成感や充実感を得ることができ、ひいては防犯ボランティア活動を楽しみ、また更なる高みへの向上心を持って、活動を維持、継続できるものと考えられる。

3　活動成果を示す

現実社会における防犯ボランティアの活動では、地域社会におけるパトロール活動等の各場面において地域住民と接する機会も多く、これらの機会を通じて、地域住民から感謝の声を掛けられる場面も少なくない。しかし、サイバーパトロールを始めとするサイバー空間の活動は、自宅のインターネット端末を操作して活動するなど表に出ないことが多いことから、防犯ボランティア活動を通じて地域住民と接する機会も少ないため、活動の成果を地域社会から得、又は示す機会に乏しいと考えられる。したがって、サイバー防犯ボランティアが活動の成果を地域住民やインターネット利用者に目に見える形で示すためには、現実社会の防犯ボランティアの活動と比較して、より積極的に活動成果を示していく必要がある。例えば、講習会や街頭キャンペーンの開催、自治体や自治会の広報紙、回覧板への活動成果の掲載のほか、ウェブサイトの構築による情報発信等のあらゆる機会や媒体を活用して効果的に広報し、世間一般にサイバー防犯ボランティアの活動を周知することが望ましい。これらにより、サイバー防犯ボランティアの活動成果を示すことで、地域住民から防犯ボランティア活動への理解を得られ、防犯ボランティアの活動に対する、「ありがとう」、「お陰様で犯罪に遭わなくてすみました」という感謝の言葉が防犯ボランティアに伝えられることとなり、防犯ボランティア個々人にとっては何物にも代え難い「やり甲斐」に通じるものになると期待できる。

また、著しい功労のあった防犯ボランティアに対しては、関係機関・団体による表彰も検討されるべきであり、世間一般や関係機関・団体からのサイバー防犯ボランティアに対する理解や期待が、防犯ボランティア活動を維持、継続させるための糧となるものと考えられる。

4　活動に対する安全の確保

防犯ボランティアが活動を進める上で、その安全を確保することは重要である。現実社会における防犯ボランティア活動においては、活動の目的を同じくする者が合同パトロール等といった形で活動し、防犯ボランティア個々人相互が互いの安全を確保し合いながら活動することが可能である。しかし、インターネット上での活動に際しては、個人で活動する機会も多く、インターネット上での誹謗中傷や架空・不当請求等の被害やトラブルに巻き込まれることが懸念される。インターネット上での活動で安全を確保するための方法については、防犯ボランティアが活動上被害を防止するための教育・研修を受けることのできる十分な機会を提供し、自らの個人情報を明らかにしないことやトラブルへの対処法等を周知して、防犯ボランティア個々人の能力を高めることが、まず挙げられる。この際には、防犯ボランティア自らが被害に遭うことのみならず、防犯ボランティア自身がインターネット上に不用意な書込み等を行い、防犯ボランティア自身がトラブルの元にならないようにすることも周知しなければならない。

また、サイト管理者、利用者への助言、注意の活動を行う場合等の防犯ボランティアが個別にやり取りを行う活動には、特に重大な被害やトラブルに巻き込まれることが予想されるため、全少協で活用されている「ホットラインシステム」のような防犯ボランティアの個人情報を明らかにせずに電子メールの送信等を行うことができるプラットフォームの構築等が強く推奨される。

第３章　サイバー防犯ボランティアの育成

一般にボランティアの活動は、誰でも気軽に始められるところに、その魅力がある。

サイバー防犯ボランティアも活動するに当たっては、インターネットに関する知識や技能を求められる場面もあるが、特別な知識や技能を要しない、より平易なところから活動を始め、徐々に知識を習得していく過程で活動の範囲を広げていく方法も考えられる（第２章第１の１参照）。特に、サイバー防犯ボランティアに求められる活動のうち、サイバー空間の浄化活動、悪質な利用者に対する指導・注意といった活動に関しては、防犯ボランティアが日々研鑽しながら経験を積み重ねることで、活動に習熟し、必要な知識・技能を徐々に身につけていくことも考えられる。

一方、サイバー空間での防犯ボランティアの活動に対しては、サイバー空間の特徴である匿名性を背景に姿が見えない相手からの反発や攻撃を受けることもあり、それにより防犯ボランティアの士気の低下も招きかねない。

サイバー防犯ボランティアが活動するに当たって、インターネットの危険性を十分に理解し、インターネット上で問題となっている最新の実態やインターネットに関係する法律に対する十分な知識を備えた上で行うことが理想的である。本章では、サイバー防犯ボランティアを育成するための必要な技量と、その向上方策について述べることとする。

１　技量の向上方策

技量の向上のためには、警察、自治体やインターネット関連事業者との連携、協力が不可欠である。一緒に防犯ボランティア活動を行う者の中に、特に知識、経験を有する者が存在するのであれば、その者を中心として意見交換や研修会を継続的に開催することにより、防犯ボランティア全体の技量向上を図ることも可能であろう。しかし、このような人物が存在すること自体が希であろう現状を考えると、関係団体が連携、協力して、技量向上のための研修会や活動成果の報告、意見交換の場を設定することが望まれる。このような場において、警察からは、最新のサイバー犯罪情勢についての情報提供が定期的に行われることが必要であり、インターネット関連事業者からは、最新のインターネット技術の紹介を始め、技術的、物理的な支援が期待される。

これら関係機関・団体の支援と平行して、防犯ボランティア自身も、定期的かつ継続的な勉強会や意見交換会を開催し、防犯ボランティア個々人が習得した知識や技能を相互に持ち寄り、不足する部分を補完し合いながら、お互いの技量を向上させていくことも重要である。

また、技量を向上させる方法として、大学や自治体が市民講座としてサイバー防犯ボランティア養成講座を提供することも期待される。

２　学びの場の提供

サイバー防犯ボランティアとして活動を開始するには、ある程度の知識を習得する

ことが必要であり、気軽に学び、知識を習得できるような仕組みが望まれる。そのためには、警察や自治体が、関係事業者の協力を得ながら、連絡会議や情報交換の場を防犯ボランティアへ積極的に提供していくことが効果的である。

防犯ボランティアが防犯ボランティアとしての活動を持続させる動機付けとして、「自分たちの町は自分たちで守る」といった目的を達成するために活動するということは、論をまたないところであるが、これらの目的に加えて、防犯ボランティアによっては、自ら学び、自らの能力や知識を高めることに「やり甲斐」を感じ、防犯ボランティア活動を継続する者もいるということも考えられる。これらの者も含め、防犯ボランティア自身が自ら学び、楽しみながら技量を向上させ、防犯ボランティア活動を維持、継続させていく上でも、防犯ボランティアに対して学びの場を提供していくことが、警察や自治体、関係事業者に求められる。

また、学びの場の提供と平行して、活動のためのガイドラインやＱ＆Ａを作成して防犯ボランティアに配付したり、具体的な活動方法について、ロールプレーイング式で体験させることで自信を持った実際の活動が期待できる。

3　知識の充実

サイバー防犯ボランティアに期待される教育、広報啓発、サイバー空間の浄化、悪質利用者への助言、注意といった活動を行うに当たっては、様々な知識を身に付けておくことが理想的である。

それは、インターネットの仕組みや最新のインターネット端末の取扱いに関する技術的な知識であったり、青少年をインターネット上における有害情報から保護するためのフィルタリングの普及やサイト管理者等の義務について規定している、いわゆる青少年インターネット環境整備法[6]に関する知識であったりする。また、インターネット上で敢行される犯罪の多く、例えば、インターネットサイトや掲示板で見られる、携帯電話、預貯金通帳、規制薬物の売買やわいせつ物の公然陳列といった行為は、現実社会においても法律に触れる行為であり、このように現実社会でも違法な行為が、インターネットを経由して行われる場合にも共通して適用される法律に関する知識を備えておくことも必要である。さらに、インターネット上で発生する民事紛争トラブルについては、インターネットにおけるプロバイダ等の損害賠償責務の範囲や発信者情報の開示について規定している、いわゆるプロバイダ責任制限法[7]に関する知識も求められる。

このようにサイバー防犯ボランティアには、多岐にわたる知識の充実が求められるが、サイバー防犯ボランティアとして活動を始めようとする者が、当初からこのような知識を身に付けておくことは困難であり、徐々に身に付けることを目指して、まずは経験を積むために実践することが大事である。

しかしながら、徐々に知識を身に付けていく過程で、より高度な知識が求められる

6　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（平成 20 年法律第 79 号）
7　特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律（平成 13 年法律第 137 号）

場面に遭遇することも予想されることから、そのような場面で助言を受けることができるような十分な知識を持つ者を、顧問やアドバイザーとして防犯ボランティア活動に参加してもらい、いざという時に助言を得ることができるようにしておくことが望ましい。

4　事業者からの支援の活用

サイバー防犯ボランティアの活動には、現実社会の防犯ボランティア活動と異なる点として、サイバー空間の実態の把握や浄化活動において、パソコンや携帯電話等といったインターネット接続機器や通信費等が必要不可欠であるため、活動資金につき負担を強いられることが予想される。

インターネット関連事業者の中には、インターネット社会の安全で健全な発展のために取り組もうとする団体の育成のため助成金制度を設けている事業者もあることから、これら事業者の施策を積極的に活用し、財政面での支援を受けることも活動を推進することに繋がる。

第４章　サイバー防犯ボランティアの組織化

第２章及び第３章では、サイバー防犯ボランティアの活動及び育成について述べてきたところであるが、サイバー防犯ボランティアの活動は、より多くの人の理解と支援を得て進めることで、その成果を発揮することにつながると考えられる。本章では、サイバー防犯ボランティアの活動を組織化するに当たって留意すべき事項について述べることとする。

１　知名度を高める

サイバー防犯ボランティアが活動するに当たって、その活動内容を積極的に広報し、より多くの人の理解を得ることで、効果的な活動を推進することができる。また、防犯ボランティアを募集する際も、その活動が周知されていれば、より多くの優秀な人材の参加も期待できる。そのためには、活動の知名度を高めることが必要であり、個人で活動を進めるより、組織として幅広く活動を進める方が有効である。

知名度を高める方法として、警察や自治体、教育機関、関係事業者から後援や支援を受けるほか、活動を紹介する広報・啓発用チラシの配布、ホームページ上で活動実態を広報する方法等が考えられる。関係機関や事業者等から後援、支援を受けることにより、防犯ボランティア団体の活動に対するインターネット利用者からの信頼を得られやすくなるほか、これら関係機関等を通じて広く防犯ボランティア活動の周知が図られることも期待できる。

２　ガイドラインの策定

防犯ボランティアが活動を個人で行うことには、その個人の主観的な意見、倫理観が影響し、時として活動が行き過ぎてしまう可能性も否定できない。

防犯ボランティアの活動の具体的な方法について、それぞれの防犯ボランティアが、あるべき姿を議論して、より多くの意見を集約し、それを反映したガイドラインを策定し、それに基づき活動することで、防犯ボランティアの強い正義感ゆえの行き過ぎた活動が自己抑制され、自信を持った、適正な活動が期待できる。

ガイドラインの策定に当たっては、防犯ボランティア団体の「この活動は何のためにやるのか」という動機付けを明記した「活動の目的」や、活動上の被害防止の観点や活動の逸脱防止等を明記した「活動に当たっての留意事項」、活動の種別や方法を明記した「具体的な活動要領」を記載しておくことが望ましい。

３　「やり甲斐」の醸成

防犯ボランティアが活動を通じて、その活動に「やり甲斐」を見いだすことの必要性は前述のとおりであるが、防犯ボランティア同士が、活動を通じて、その活動を相互に評価し、励まし合うことで、「やり甲斐」に繋がり、それぞれの防犯ボランティアの向上心も生まれる。「やり甲斐」を醸成する方法として、防犯ボランティアが一同に会する機会を設けて、お互いの活動内容の適否や防犯ボランティア活動により得

られた成果、経験した問題点等を議題として意見交換を行うことや、個々の防犯ボランティアの電子メール交換による情報交換や電子掲示板を用いた情報共有という方法も考えられる。

4　研修会の開催

それぞれの防犯ボランティアが、活動により得られた成果や経験した問題点等について、定期的に研修会等の場を通じて意見を交わし、お互いが切磋琢磨することは、防犯ボランティアの技量の向上とともに、防犯ボランティアの活動の活性化に資する。サイバー防犯ボランティアの活動は、一人で活動できるものも多く、防犯ボランティア相互の顔を合わせることなく組織化することも可能であるが、このような場合でも定期的に研修会や勉強会で防犯ボランティア相互が実際に顔を突き合わせ、互いの言葉で意見を交換し合うことで、防犯ボランティア相互の信頼感や団体の連帯感を醸成することも期待できる。

また、活動は全国規模で拡大することも予想されることから、研修会等は、都道府県単位だけでなく、全国規模で開催し意見交換することがより効果的である。

5　インターネット上の情報の活用

サイバー防犯ボランティアが活動するに当たり、インターネット上で提供されている大量の情報の中から信頼できる情報を適切に選択し、それを積極的に活用することができれば、防犯ボランティア個々人の知識や技能の拡充を図ることができるほか、防犯ボランティアの組織的な運営・管理に資することも可能である。すなわち、インターネット上では、警察庁を始め、関係省庁、民間のインターネット関連事業者が、サイバー空間における防犯ボランティア活動に参考となる情報を掲載するサイトやインターネット上のトラブル、相談に対応するサイトを運営している（図４－１）。

サイバー防犯ボランティアは、これらのサイトに掲載された最新のサイバー空間の犯罪情勢や課題等を把握しておくとともに、活動する中で直面することが予想されるトラブルや相談への対処要領をあらかじめ身に付けておくことで、落ち着いて対応することが可能となる。

また、これらサイトに掲載された情報の中から、サイバー防犯ボランティア活動を組織として運営する上で参考となる情報を集めて、防犯ボランティア団体の会則等の中で活用することも期待できる。

図４－１　参考サイト一覧

○ 民間事業者サイト

サイト名（制作）	内容	アドレス
違法・有害情報相談センター （（社）テレコムサービス協会）	インターネット環境における違法・有害情報および安心・安全に関わる相談、疑問に相談員が助言する。	http//www.ihaho.jp/
インターネットルール＆マナー検定 （（財）インターネット協会）	インターネットを利用するためのルールやマナーの知識を身につけているか評価測定できる。	http//rm.iajapan.org/
家族のケータイルール （（社）電気通信事業者協会）	携帯電話を利用するにあたって、家族内でルールを決めること、保護者の見守り等、保護者に知っておいてもらいたい内容をまとめている。	http//www.tca.or.jp/mobile/child.html

○ 省庁関係サイト

サイト名（制作）	内容	アドレス
インターネット上の違法・有害情報対策 （内閣官房）	インターネット上の違法・有害対策に関する政府等の取組みや青少年を有害環境から守るための情報を紹介している。	http//www.it-anshin.go.jp/
国民のための情報セキュリティサイト （総務省）	安心してインターネットを使うための情報を紹介している。	http//www.soumu.go.jp/main_sosiki/joho_tsusin/security/index.htm
やってみよう情報モラル教育 （文部科学省）	情報モラル教育のねらいはどこにあり、どのような指導をしたらよいか、知っておくべき基本的な知識が解説されている	http//kayoo.info/moral-guidebook-2007/
CHECK PC！ （経済産業省）	インターネットに関する犯罪の被害を未然に防ぎ、安心してインターネットを利用するための意識及び知識の向上を図るための情報を紹介している。	http//www.checkup.go.jp/top.html
ひとりで悩まずにご相談ください （法務省）	「人権上問題はないか」「法律上問題はないか」等に関わる相談、質問に人権擁護委員や法務局職員が助言する。	http//www.moj.go.jp/JINKEN/index_soudan.html

○ 警察関係サイト

サイト名（制作）	内容	アドレス
サイバー犯罪対策 （警察庁）	サイバー犯罪の情勢、警察におけるサイバー犯罪対策、最新のサイバー犯罪の予防策を紹介している。	http//www.npa.go.jp/cyber/
インターネット安全・安心相談 （警察庁）	インターネット上の様々なトラブルの解決策を紹介している。	http//www.npa.go.jp/cybersafety/
@ police （警察庁）	サイバー犯罪、サイバーテロの未然防止及び被害の拡大防止のためのネットワークセキュリティに関する情報を紹介している。	http//www.npa.go.jp/cyberpolice/
都道府県警察本部のサイバー犯罪相談窓口等一覧	サイバー犯罪の被害に遭ったり、遭いそうになったときの相談を受け付ける全国都道府県警察の相談窓口電話、URLを紹介している。	http//www.npa.go.jp/cyber/soudan.htm

サイバー防犯ボランティア
活動ガイドラインのイメージ

目　次

はじめに **（組織結成の背景、必要性等について、起草者等が記述）**

平穏な市民生活を確保するため、平成15年以降、国をあげて犯罪抑止対策を推進した結果、刑法犯認知件数は７年連続減少するなど、数値の面から見れば、治安情勢は確実に改善しつつあります。また、「自分たちの安全は自分たちで守る」という趣旨で結成された自主防犯ボランティアによる青パト*1を始めとするパトロール活動等は、街頭犯罪の抑止や体感治安の向上に一定の成果を上げたと言われています。

一方、インターネット利用者は、9,000万人を超え、インターネットがますます国民の日常の生活に欠かせないものとなっていますが、それに伴い、サイバー犯罪も年々増加し、平成21年のサイバー犯罪の検挙件数は、平成17年の約２倍に増加しています。

このような状況から、サイバー空間においても、自主的な防犯ボランティア活動を推進して、「自分たちの利用するサイバー空間の安全は自分たちで守る」という意識を醸成し、安全で安心して利用できるサイバー空間を作りましょう。

平成○○年○○月○○日

○　○　○　○

*1　青色回転灯を装備した防犯パトロール用自動車。

１　活動の目的　（組織結成の契機、具体的目的について記述）

インターネット上では、自分の姿が周りから見えないという匿名性を利用して、他人を誹謗中傷したり、他人の個人情報を書き込むといった行為が敢行されやすく、インターネット上の規範意識は低いと言われています。また、携帯電話のコミュニティサイトでは、青少年が被害にかかる犯罪が急増しています。インターネットは全国どこでも同様に利活用できることから、この種の犯罪が、いつ私たちの周りで発生してもおかしくありません。

地域の人々に対し、適正なインターネット（携帯電話を含む）利用法についての教育や広報啓発活動を行うとともに、インターネットサイトや掲示板における違法・有害情報の浄化活動、不適切なインターネット利用者に対する助言、注意を通じて、サイバー空間の規範意識を改善し、地域の人々が安全で安心して利用できるインターネットにしましょう。

２　活動を始める前に　（活動を始めるにあたって基本的事項について記述）

(1)　ボランティア活動とは

ボランティア活動は、自主的な活動計画に基づいて、それぞれが主体となって行うもので、法律に基づき行うものではありません。また、活動に対し、何らかの特権を与えられるものではありません。活動の目的を達成するために、どのような活動が必要で効果的なのか、ボランティアみんなで話し合うことが大切です。

(2)　仲間を増やす

サイバー防犯ボランティア活動は、インターネット環境さえあれば一人でも活動できるというメリットがある反面、一人での活動は個人の主観に左右されることから、時として「行き過ぎた正義感」により、活動が誤った方向へ進む危うさがあります。目的に賛同する仲間を増やし、仲間と知識や効果的な活動について話し合い、時には励まし合いながら、楽しんで活動していくことが大切です。

(3) 活動を長続きさせるために

一人での活動は、その目的、やりがいを見失い、長続きしないという結果にもなりかねません。また、ボランティア活動を維持、継続するためには、熱意を持って活動することは当然ですが、活動を活性化することが何より重要です。そのためには、仲間と楽しみながら、無理なく、気長に取組むことが大切です。

3　活動の基本的心得　（活動についての基本的心得について記述）

(1)　安全を第一に

サイバー防犯ボランティア活動に取り組むにあたっては、コンピュータ・ウィルスへの感染やネット上での誹謗中傷等の被害に遭わないよう、ウィルス対策ソフトを最新のものに更新することや安易に個人情報を公開しないことなどに注意することが必要です。安全に活動できるための知識を身につけて、安全を確保できる範囲内で活動しましょう。

(2)　サイバー空間の実態を知る

活動中、犯罪被害やトラブルに遭わないために、今、サイバー空間で発生している犯罪や問題となっているトラブル等の実態をよく理解しておくとともに、活動の目的を達成するために予想される課題や問題点について知っておきましょう。

(3)　秘密の保持

インターネット上には、個人のプライバシーに関わる情報も多数掲載されています。活動を通じて知った個人情報を他人に漏らしたりしてはいけません。その取り扱いには、十分注意しましょう。

(4)　最新情報の共有

警察や関係機関、自治体から提供される最新の情報は、積極的に活用して、防犯ボランティア間で共有するとともに、意見交換や研修会等の場で、トラブル事例や効果的な活動例等の情報を交換しましょう。情報を共有することで、活動の活性化にも繋がります。

(5)　関係機関、団体との連携

警察や自治体をはじめ、インターネット上の違法・有害情報の通報を受け付けるインターネット・ホットラインセンター、他の防犯ボランティア団体と良好な関係を保ち、連携して活動に取り組みましょう。

(6)　活動記録の保存

活動の結果については、記録して保存しておきましょう。定期的に活動結果を振り返り分析することで、その後の活動をより効果的なものに改善するのにつながります。また、活動に起因するトラブル等の対処のためにも役立ちます。

(7) 実社会での活動

活動を通じて扱うインターネット上の問題や相談を解決するために、実際に当事者と面接したり、話し合いをするなど実社会での活動が求められる場合もあります。

実社会での活動にあたっては、その必要性、効果を慎重に判断しましょう。事案によっては、専門機関へ紹介した方が良い場合もあります。

4 具体的な活動要領 （具体的な活動内容について記述）

(1) 教育活動

インターネットや携帯電話を利用する児童やその保護者、地域住民等を対象に、警察や教育機関、自治体等と連携して、インターネットの実態や危険性、被害防止のための講習を行いましょう。被害の実例やインターネット機器を用いた体験型の講習を行うことで、より大きな効果が得られます。

ア 講習素材の収集

講習素材の収集は、広報啓発資料の作成にあたって収集するものと変わるところはありません。但し、講習を聞く方は、インターネットの各種サービスやインターネットの危険性を踏まえて、犯罪被害やトラブルを如何に防止し、もし被害に遭った場合に、どう対処すべきかという点に興味を持っているので

- ○ インターネットの各種サービスの仕組み
- ○ インターネットに関する犯罪被害や危険性の具体的事例
- ○ 犯罪被害やトラブルを未然に防止するための対策
- ○ 被害に遭った場合の具体的措置

等に関する情報について収集しましょう。(巻末の関係機関のホームページ参照)

イ 講習の内容及び方法

講習は、対象のインターネットに関する知識、興味に応じた内容にすることが大切です。また、一方的な講義式の講習ではなく、インターネット機器を利用して、実際にインターネット上の各種サービスを見ながら、参加・体験・実践型の教育を行うことが効果的です。

(2) 広報啓発活動

ア 広報啓発のための資料の作成

広報紙や活動ニュースといった広報啓発資料を作成し、配布することは、正しいインターネット利用等について周知し、サイバー犯罪の未然防止を図れるだけではなく、防犯ボランティアの活動成果をアピールし、さらに、活動への参加を呼びかける効果もあります。

(ｱ) 素材の収集

素材は

- ○ 警察やセキュリティ関連団体・企業が発信する防犯情報
- ○ 活動に際して知り得た防犯・トラブル事例
- ○ ボランティア団体の活動計画やその結果

等、読む人が関心を寄せるような素材を収集しましょう。

(ｲ) 資料の作成

読む人に応じた内容の資料を作成しましょう。また、分かり易いものを作ることは大切ですが、綺麗に仕上げるために多大な時間を要したり、高額な費用、過度に負担のかかるものを作る必要はありません。無理せず継続して発行できるものを作成しましょう。

(ｳ) 資料の配布

作成した広報啓発資料は、読む人に応じて、教育機関、自治会等の協力をもらって配付しましょう。また、配布に際しては、防犯ボランティア活動への参加も呼びかけてみましょう。

イ 防犯キャンペーンの開催

防犯キャンペーンの開催は、より多くの人への周知が図られるばかりでなく、その活動を広報、紹介されることで、活動が広く周知され、さらに大きな効果を得られます。

(ｱ) 計画について

開催の趣旨・目的を明らかにし、それに沿って、キャンペーンや集会等の様

々な方法から、また、駅、レジャー施設、イベント会場等の様々な場所から適した方法・場所を選択し計画を立てましょう。

内容については、

○　防犯やセキュリティ関連担当者の基調講演

○　インターネット機器等を用いた体験型学習

○　広報啓発資料の個別配布

等が考えられます。

計画段階から最寄りの警察署や自治体、教育機関、セキュリティ関連企業、開催場所を管理する事業所等へ協力を呼びかけ、支援・後援を得ることも大切です。

(ｲ)　実施について

開催にあたっては、参加対象は、開催の趣旨・目的により異なりますが、インターネット等を利用している人ばかりでなく、小・中学生の保護者や教職員、地域住民など、なるべく多くの人に参加を呼びかけましょう。

(3)　サイバー空間の浄化活動

サイバーパトロールとは、サイバー空間に存在する違法・有害情報を発見する活動のことを言います。サイバーパトロールを通じて発見した違法・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へ通報することで、情報が削除されます。

ア　サイバーパトロールの進め方

インターネット上の膨大な情報をいかに効率良く発見し、必要な情報に辿り着くかは、違法・有害サイトの特徴を知ることが重要です。

(ｱ)　発見するためのヒント

情報を発見するためには

○　検索サイトの活用方法

インターネット上の膨大な情報の中から、特定の情報を探し出す場合に利用するのが、検索サイトです。探したい情報に関するキーワードを入力して検索すると、そのキーワードが含まれたサイトを抽出で

きます。（違法・有害サイトは、直接的な表現を避け、隠語や伏せ字が使われることが多い。）

○　実施時間帯

インターネット・オークションや電子掲示板では、多くの人の目に触れないように、深夜や早朝の時間帯を狙ったり、休日に特定して禁制品の売買等、違法行為が行われることがあります。

○　発見した違法・有害サイトからの検索

違法・有害サイトを発見した場合、そのサイトに貼られたリンクを辿ると、同様の違法・有害サイトにアクセスすることがあります。

(ｲ)　発見時の措置

違法・有害情報を発見した際は

○　インターネット・ホットラインセンター

URL　http://www.internethotline.jp/

へ通報して下さい。ただし、インターネット・ホットラインセンターが取り扱う違法・有害情報の種類は決められていますので注意して下さい。

「インターネット・ホットラインセンター」で取り扱う違法情報、有害情報について

違法情報

① **わいせつ物公然陳列**（刑法第175条）
② **児童ポルノ公然陳列**（児童ポルノ法第７条第４項）
③ **売春周旋目的の誘引**（売春防止法第６条２項第３号）
④ **出会い系サイト規制法違反の禁止誘引行為**（同法第６条）
⑤ **薬物犯罪等の実行又は規制薬物**（覚せい剤、麻薬、向精神薬、大麻、あへん及びけしがら）**の濫用を、公然、あおり、又は唆す行為**（麻薬特例法第９条）
⑥ **規制薬物の広告**（覚せい剤取締法第２０条の２、麻薬及び向精神薬取締法第２９条の２及び第５０条の１８、大麻取締法第４条第１項第４号）
⑦ **預貯金通帳等の譲渡等の誘引**（犯罪収益移転防止法第２６条第４項）
⑧ **携帯電話等の無断有償譲渡等の誘引**（携帯電話不正利用防止法第２３条）

有害情報

① **情報自体から、違法行為**（けん銃等の譲渡等、爆発物の製造、児童ポルノの提供、公文書偽造、殺人、脅迫等）**を直接的かつ明示的に請負・仲介・誘引等する情報**
② **列挙する違法情報について、違法情報該当性が明らかであると判断することは困難であるが、その疑いが相当程度認められる情報**
③ **人を自殺に誘引・勧誘する情報**（集団自殺の呼びかけ等）

イ　基本的留意事項

・使用しているOSやアプリケーションは、パッチプログラムの適用や最新バージョンに更新する。

・ウィルス対策ソフトを導入し、アップデートを確実に行う。
・他人のＩＤ、パスワードは使用しない。（不正アクセス禁止法違反になる。）
・掲示板等に氏名や電話番号等の個人情報を入力しない。
・データ及びシステムのバックアップを行う。

(4)　悪質な利用者への指導・注意

サイバーパトロールを通じて、インターネット上に不適切な書込み等を発見した場合、書込者に対して電子メール等で、指導・注意を行いましょう。インターネット上で指導、注意を行うことにより、インターネット利用者の規範意識（モラル）の改善を促し、違法行為の未然防止を図る効果が得られます。

ア　指導・注意の対象

サイバーパトロールにより発見したインターネット・ホットラインセンターへ通報すべき違法・有害情報には当たらないものの、他人の人権を侵害する行為、公序良俗に反する行為や未成年者が閲覧できるサイト等における少年の健全育成を阻害する情報を対象にします。サイバー空間の浄化活動と異なり、その行為・情報自体が違法・有害ではないものも対象となり得るため、対象の選定にあたっては、あらかじめ具体的に定めておくことが必要です。

【指導・対象の例】
○　18歳未満の児童による出会い系サイト利用
○　他人の氏名や住所、連絡先等の無断掲載

イ　指導・注意の方法

インターネットを利用した指導・注意は、顔の見えない相手とのやりとりであるため、電子メール等の文章により行うことになりますが、文章の内容により、相手方から感謝されることもあれば、相手方とトラブルになることも予想されます。

無用のトラブルを避けるため、あらかじめ指導・注意の対象に応じた定型文を作成しておくことも大切です。

【注意文例】

○　出会い系サイトへの書込みに対して

　18歳未満の青少年が出会い系サイトを利用することは禁止されています。また、出会い系サイトの利用をきっかけに凶悪犯罪に巻き込まれた事案も発生しています。絶対に使用しないようにしましょう。

○　他人の氏名等の書込みに対して

　個人情報を掲載すると悪用されるおそれがあります。他人の氏名等の個人情報を無断で書き込むことはやめましょう。

ウ　指導・注意の実施

指導・注意の方法として、相手方の電子メールアドレス宛てに電子メールを送信する方法や、電子掲示板であれば、その電子掲示板へ書き込む方法があります。

指導・注意メールの送信等にあたっては、相手方の連絡先をしっかり確認し、誤送信がないように注意しましょう。

送信した後の返信メールの確認や書込みの削除状況を確認し、指導・注意メールの効果を確認してみましょう。

エ　留意事項

(ｱ)　防犯ボランティアとしての活動

指導・注意は、特別な権限が与えられたものではないことを自覚し、関係者の名誉や人権を侵害しないように注意しましょう。

(ｲ)　安全の確保

指導・注意メール等を相手方に送信する際には、不用意に自分の氏名や住所等を掲載してはいけません。悪意のある相手方であった場合には、迷惑メールやウィルスメールの多量送信、電子掲示板等での誹謗中傷被害に遭うことも予想されます。専用のシステムを構築するか、送信に使用する電子メールアドレスは、フリーメールを利用するなど、被害に遭わないようにしましょう。

ワンクリック詐欺（不正請求）への対応要領

・ワンクリック詐欺（不正請求）とは

メールやホームページにおいて、リンクやボタンをクリックする前に利用料金・利用規約等において明確な説明もなく、又は事実と異なる説明によりクリックを促し、リンク先において即座に「契約完了」や「料金請求」といった内容を表示させるなどして金銭を振り込ませようとします。

・被害に遭わないために

ワンクリック詐欺（不正請求）のほとんどは、法令上も契約の正当性を欠くものが多く、契約の無効が主張でき、支払いを拒否できます。

不審なメール等のリンクは、クリックしないようにしましょう。

最近は、アダルトページのみならず、懸賞や占い、動画など、人の興味をひくような様々な手法でリンクやボタンをクリックさせようと、手口が巧妙になっています。見知らぬサイトで安易にリンクやボタンをクリックすることがないように気をつけましょう。

・被害に遭ったときは

クリックする前のホームページ等に利用規約等が掲載されているか確認してください。これがなかったり、わかりにくくなっている場合は契約の無効を主張できます。

支払う義務があるとわかるまでは、相手との連絡は控えてください。

不当な請求であることがわかったら無視してください。

不明な点があったら、消費生活センター、警察などに相談してください。

(ｳ) トラブルの防止

指導・注意を行った場合、相手方の反応が気になるところですが、相手方からの反論等に対しては冷静に対応し、トラブルに発展しないよう注意し、返信には一切対応しないなどのルールを決めておくことが大切です。

５　ＦＡＱ　（活動に関して予想される疑問点等について記述）

(1)　活動にあたっての必需品は

あくまでボランティアによる活動ですので、自分のできる範囲で、無理なく活動することが大切ですが、効果的に活動するためには、インターネットの現状や危険性等を的確に把握する必要がありますので、インターネット環境（携帯電話も含む。）は必要です。

(2)　効果的に活動するには

活動にあたっては、活動内容がより多くの人に周知され、理解を得ることで、より多くの協力や人材が得られ、効果的に活動を推進することができます。そのためには、ボランティア団体の名称や活動の知名度を高めることが重要です。積極的な広報啓発活動やその成果を示す教育活動等の機会を増やすとともに、警察や教育機関、関連企業との連携を深めましょう。

(3)　活動を長続きさせるためには

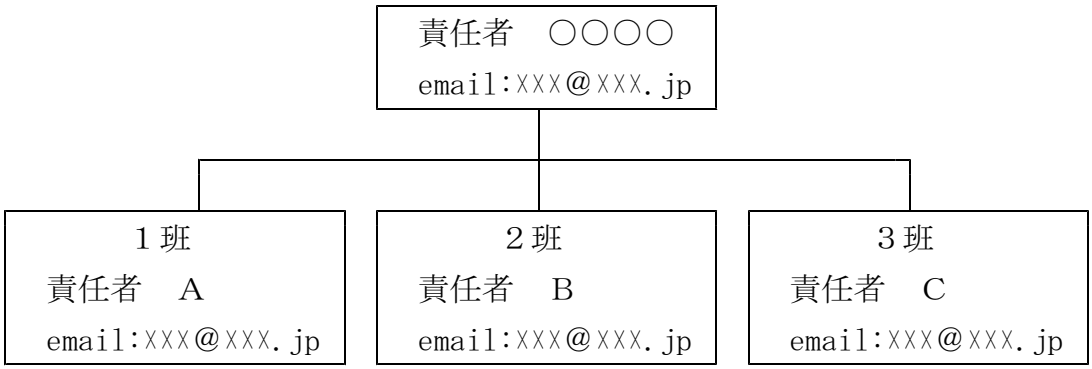
ボランティア活動を維持、継続させるためには、ボランティア個々人が活動を通じて「やりがい」を見い出すことが大切です。そのためには、活動の目的を明確に持つことや、活動の成果を目に見える形で感じることが重要です。その方法として、意見交換をする場や研修会等に参加し、ボランティアが互いに学びながら、また、励まし合いながら、その成果を確認することが大切です。

(4)　犯罪を予告する書込みや自殺を予告する書込みを発見した場合

犯行予告や自殺予告に関する書込み等は、人命救助の観点から緊急に対処する必要がありますので、最寄りの警察署か１１０番へ通報を行うようにして下さい。

６　組織の構成

(1)　組織の責任者の氏名、連絡先、組織系統図



(2)　活動の拠点、住所、連絡先

事務局　○○県○○市○○町○○番地

電話　００－０００００－００００

平成 22 年度総合セキュリティ対策会議委員名簿

前田　雅英 （委員長）	首都大学東京　法科大学院教授
荒木　浩一	（社）電気通信事業者協会　業務部長
尾崎　克行	デジタルアーツ（株）　経営企画室　室長代理
小田　啓二	特定非営利活動法人日本ガーディアン・エンジェルス　理事長
上林　靖史	（株）ディー・エヌ・エー執行役員　経営企画本部　本部長
久保田　裕	（社）コンピュータソフトウェア著作権協会（ＡＣＣＳ） 専務理事　兼　事務局長
桑子　博行	（社）テレコムサービス協会　サービス倫理委員会　委員長
国分　明男	（財）インターネット協会　副理事長
下道　高志	日本オラクル（株）システム事業統括　ソリューション統括本部 プリンシパルセールスコンサルタント
関　　聡司	楽天（株）　執行役員　広報渉外室　室長
谷川　哲司	日本電気（株）経営システム本部セキュリティ技術センター シニアマネージャー
冨沢　高明	日本マイクロソフト（株）法務・政策企画統括本部　政策企画本部 技術政策部長　工学博士
苗村　憲司	情報セキュリティ大学院大学　客員教授
西村　達之	セコムトラストシステムズ（株）代表取締役副社長
藤井宏一郎	グーグル（株）公共政策部長
藤原　静雄	中央大学　法科大学院教授

別所　直哉　　ヤフー（株）　最高コンプライアンス責任者（ＣＣＯ）・
　　法務本部長　兼　政策企画室長

松浦眞紀子　　神奈川県少年補導員連絡協議会　会長

丸橋　　透　　ニフティ（株）　コーポレート部門副部門長兼法務部長

宮下　正彦　　弁護士

安田　　浩　　東京電機大学　教授

山田　浩史　　（社）日本ＰＴＡ全国協議会　副会長

計２２名（敬称略・５０音順）

（オブザーバ）
内閣官房
内閣府
総務省
法務省
外務省
文部科学省
経済産業省
消費者庁

事務局：警察庁生活安全局情報技術犯罪対策課

不正アクセス対策分科会委員名簿

前田　雅英 （委員長）	首都大学東京　法科大学院教授
下道　高志	日本オラクル（株）　システム事業統括　ソリューション統括本部 プリンシパルセールスコンサルタント
杉尾　秀哉	（株）ＴＢＳテレビ　報道局　解説・専門記者室長
田嶋　　龍	（株）ジェーシービー　セキュリティー推進部長
中野目善則	中央大学　法科大学院教授
西村　達之	セコムトラストシステムズ（株）　代表取締役副社長
早貸　淳子	フィッシング対策協議会　事務局長
別所　直哉	ヤフー（株）　最高コンプライアンス責任者（ＣＣＯ）・ 法務本部長　兼　政策企画室長
前島　幸仁	一般社団法人情報通信ネットワーク産業協会 ユビキタスフォーラム企画部長
松浦　幹太	東京大学生産技術研究所　准教授
宮下　正彦	弁護士
安冨　　潔	慶應義塾大学　大学院法務研究科教授
若松　　修	日本複合カフェ協会　顧問

計 13 名（敬称略・５０音順）

（オブザーバ）
内閣官房
総務省
外務省
経済産業省
特許庁

事務局：警察庁生活安全局情報技術犯罪対策課

違法・有害情報対策分科会委員名簿

国分　明男 （委員長）	（財）インターネット協会　副理事長
浅井英里子	日本マイクロソフト（株）　法務・政策企画本部　政策渉外担当部長
尾崎　克行	デジタルアーツ（株）　経営企画室室長代理
桑子　博行	（社）テレコムサービス協会　サービス倫理委員会　委員長
小向　太郎	（株）情報通信総合研究所　主席研究員
齋藤　雅弘	弁護士
新谷　珠恵	（社）東京都小学校ＰＴＡ協議会　会長
高橋　大洋	ネットスター（株）コーポレートコミュニケーション部　部長
高橋　　誠	ＮＨＮＪａｐａｎ（株）　取締役付　政策担当 （兼　（株）ライブドア　法務部政策担当）
藤井宏一郎	グーグル（株）　公共政策部長
吉川　誠司	ＷＥＢ１１０代表

計 11 名（敬称略・50 音順）

(オブザーバ)
内閣府
消費者庁
総務省
法務省
外務省
文部科学省
経済産業省

事務局：警察庁生活安全局情報技術犯罪対策課

サイバーボランティア育成分科会委員名簿

苗村　憲司　　情報セキュリティ大学院大学客員教授
（委員長）

石附　　弘　　日本市民安全学会　会長（（財）国際交通安全学会　専務理事）

大久保貴世　　（財）インターネット協会　主幹研究員

小田　啓二　　特定非営利活動法人日本ガーディアン・エンジェルス　理事長

下田　博次　　特定非営利活動法人青少年メディア研究協会　理事長

藤川　大祐　　千葉大学教育学部教授

松浦眞紀子　　神奈川県少年補導員連絡協議会　会長

計７名（敬称略・50 音順）

（オブザーバ）
総務省
外務省
文部科学省
経済産業省

事務局：警察庁生活安全局情報技術犯罪対策課

平成 22 年度総合セキュリティ対策会議の開催状況

第１回会議　　平成22年 10月４日（月）

第２回会議　　平成22年 12月21日（火）

第３回会議　　持ち回り開催

不正アクセス対策分科会の開催状況

第１回会議　　平成22年 10月19日（火）

第２回会議　　平成22年 12月15日（水）

第３回会議　　平成23年 ２月25日（金）

違法・有害情報対策分科会の開催状況

第１回会議　　平成22年 10月20日（水）

第２回会議　　平成22年 12月６日（月）

第３回会議　　平成23年 ２月23日（水）

サイバーボランティア育成分科会の開催状況

第１回会議　　平成22年 10月７日（木）

第２回会議　　平成22年 11月29日（月）

第３回会議　　平成23年 ２月16日（水）

インターネット上の児童ポルノ流通防止に向けた取り組み

平成２３年４月

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

児童ポルノ流通防止をめぐるこれまでの主な動き

児童ポルノ流通防止協議会の設置（平成２１年6月）

・「児童ポルノ掲載アドレスリスト作成管理団体運用ガイドライン」の策定
・専門委員会の設置

警察庁・総合セキュリティ対策会議における議論

安心ネットづくり促進協議会の発足（平成２１年２月）

調査企画委員会
児童ポルノ対策作業部会
－アドレスリスト作成・管理の在り方ＳＷＧ　（法的問題の検討）
－ＩＳＰ技術者ＳＷＧ　（技術的検討）
－アドレスリスト作成・管理団体の在り方ＳＷＧ（団体の在り方の検討）

総務省
インターネット上の違法有害情報への対応に関する検討会おける議論

アドレスリストの作成・管理は民間主導の団体が必要

2

児童ポルノ排除対策推進協議会

深刻化する児童ポルノ情勢
- ●平成２１年中の事件送致件数、被害者児童数いずれも過去最多
- ●インターネット上に画像が蔓延
- ●国際的気運の高まり

児童ポルノ排除対策推進協議会　平成２２年１１月２２日に発足

「児童ポルノ排除対策推進協議会」規約

（名称）
第１条 この会議は、児童ポルノ排除対策推進協議会（以下「推進協議会」という。）と称する。
（目的）
第２条 推進協議会は、児童ポルノ排除総合対策（平成22 年７月27 日犯罪対策閣僚会議決定）を踏まえ、官民一体となって、児童ポルノ排除に向けた総合的な活動を推進することを目的とする。
（活動）
第３条 推進協議会は、次の活動を行う。
(1) 児童ポルノ排除のための活動方針を定めること。
(2) 児童ポルノ排除対策に関し、情報を交換して相互に連携、協力を図ること。
(3) 児童ポルノ排除のため広報、啓発、普及等の自主的な活動を推進すること。
(4) その他目的を達成するために必要な活動に関すること。
以下略

児童ポルノ排除対策推進協議会構成団体等

（民間団体等）安心ネットづくり促進協議会、財団法人日本ユニセフ協会、児童ポルノ流通防止協議会、社団法人テレコムサービス協会、社団法人電気通信事業者協会、社団法人日本インターネットプロバイダー協会、社団法人ケーブルテレビ連盟、全国市長会、全国知事会、全国都道府県教育協議会、日本教職員組合など　３５団体
（行政機関）　内閣府、総務省、警察庁、法務省、文部科学省など　１０機関

児童ポルノ排除対策推進協議会役員等

会長	内閣府副大臣	末松 義規	政府
副会長	社団法人日本ＰＴＡ全国協議会 会長 社団法人テレコムサービス協会 会長 財団法人日本ユニセフ協会 会長 内閣府政策統括官（共生社会政策担当）	相川 敬 中尾 睦雄 赤松 良子 村木 厚子	教育 事業者 ＮＰＯ等団体 政府
事務局長	内閣府大臣官房審議官	太田　裕之	政府

3

児童ポルノ排除総合対策の概要（平成２２年７月　犯罪対策閣僚会議にて決定）

１．児童ポルノの排除に向けた国民運動の推進
- ○　国民運動の効果的な推進
- ○　ホームページによる広報・啓発活動　等

２．被害防止対策の推進
（１）　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
- ○　青少年保護に向けたメディアリテラシーの向上及び新たな取組に対する支援
- ○　フィルタリングの普及促進等のための施策　等

（２）　情報モラル等の普及の促進
- ○　学校及び家庭における情報モラル教育の充実　等

３．インターネット上の児童ポルノ画像等の流通・閲覧防止対策の推進
- ○　事業団体によるガイドライン等の策定の支援
  - ・　「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」及び「違法・有害情報への対応等に関する契約約款モデル条項」の不断の見直しを支援する。
- ○　違法・有害情報相談センターの運営の支援
  - ・　インターネット上の違法・有害情報に関して、プロバイダ等から個々の事案への対応についての相談業務等を行う違法/有害情報相談センターの運営を支援
- ○　**児童ポルノ掲載アドレスリスト作成管理団体との連携等を通じた児童ポルノ流通防止対策の推進**
  - ・　ISP、検索エンジンサービス事業者及びフィルタリング事業者に対して児童ポルノが掲載されているウェブサイトに係るアドレスリストの作成、維持・管理、提供等の中立性の確保に配慮しつつ民間のイニシアティブにて行うための児童ポルノ掲載アドレスリスト作成管理団体の設置に向けた作業を進め、同団体との官民連携した児童ポルノ流通防止対策を推進
- ○　**ブロッキングの導入に向けた諸対策の推進**
  - ・　インターネット利用者の通信の秘密や表現の自由に不当な影響を及ぼさない運用に配慮しつつ、平成２２年度中を目途にISP等の関連事業者が自主的に実施することが可能となるよう、対策を講ずる。
    - ✔　アドレスリストの迅速な作成・提供等実効性のあるブロッキングの自主的導入に向けた環境整備
    - ✔　ISPによる実効性のあるブロッキングの自主的導入の促進
    - ✔　一般ユーザに対する広報・啓発

４．被害児童の早期発見及び支援活動の推進
５．児童ポルノ事犯の取締りの強化
６．諸外国における児童ポルノ対策の調査等

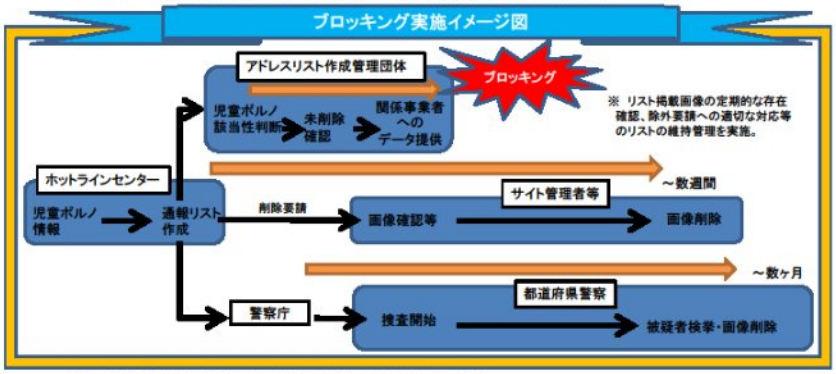
4

ブロッキングについて

ブロッキングについて（児童ポルノ排除対策WT了承事項）

関係省庁においては、インターネット上の児童ポルノについて、以下のような実効性のあるブロッキングを関係事業者が自主的に実施できるよう、環境整備を進める。

- ブロッキングの対象となりうるものは、蔵置されているサーバーの国内外を問わず、児童ポルノ禁止法第2条第3項に規定する「児童ポルノ」。
  - ※ 同法に該当するか否かの判断については、警察及びインターネット・ホットライン・センター（IHC）が適切に行い、これを受け、当該児童ポルノがブロッキングの対象となるリストに掲載されるか否かをアドレスリスト作成管理団体が運用ガイドラインに基づき慎重に行う。（下記イメージ図）
- 児童ポルノ画像について、警察の捜査、IHCからのサイト管理者等への削除要請が行われた場合であっても、画像の掲載が続いている限り、画像発見後、速やかにリスト掲載の判断及びリスト掲載後のブロッキングを実施（下記イメージ図）
  - ※ インターネット利用者の通信の秘密や表現の自由に不当な影響を及ぼさない運用に配慮



上記のような児童ポルノのブロッキングは、現行法の下で実施可能である。

出典：首相官邸「犯罪対策閣僚会議」＜http://www.kantei.go.jp/jp/singi/hanzai/＞より引用

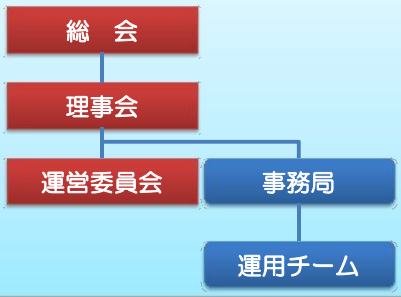
5

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の概要

計画中の主な事業（定款より）

（事業）
第4条
1．当法人は、前条の目的を達成するため、次の事業を行う。
（1）児童ポルノ画像が掲載されたサイトに係るアドレスリストの作成・管理及び提供に関する事業
（2）前号に関連した各種調査・研究及びレポートの作成
2．当法人は、前項の事業のほか、前条の目的を達成するため必要があるときは、次の事業を行う。
（1）インターネットコンテンツセーフティに関連した民間事業者等の支援事業
（2）インターネットコンテンツセーフティに関連した各種調査・研究レポートの作成
（3）前2号に掲げる事業に附帯又は関連する事業

協会の組織・設立時構成メンバー



設立時構成メンバー一覧（五十音順）

株式会社インターネットイニシアティブ
ＥｄｉｔＮｅｔ株式会社
ＮＥＣビッグローブ株式会社
ＮＴＴコミュニケーションズ株式会社
株式会社ＮＴＴぷらら
NTTレゾナント株式会社
グーグル株式会社
ＫＤＤＩ株式会社
ソネットエンタテインメント株式会社
ソフトバンクテレコム株式会社
ソフトバンクBB株式会社
デジタルアーツ株式会社
社団法人テレコムサービス協会
社団法人電気通信事業者協会
ニフティ株式会社
社団法人日本インターネットプロバイダー協会
社団法人日本ケーブルテレビ連盟
日本マイクロソフト株式会社
ネイバージャパン株式会社
ネットスター株式会社
ヤフー株式会社

6

想定している児童ポルノアドレスリスト作成のイメージ

IHC

インターネットホットラインセンターからの情報提供

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

○警察及びインターネット・ホットラインセンターからの情報受理

○受理情報のインポート

○画像単位のレコード作成
（パトロール業務の実施を含む）

○存在確認と削除確定確認

○存在する場合、児童ポルノの判定
（アドバイザー（医師、弁護士）による判定）

○アドレスリストの確定

○アドレスリストの事業者への提供

ISP等

ISP、検索事業者、フィルタリング事業者による児童ポルノのブロッキングの実施
（当初ブロッキング方法としては、DNSブロッキングを想定）

7

DNSブロッキングにおけるリスト対象ドメイン判定基準

1.（サイト開設の目的）

当該ドメインに含まれるサイトの相当部分の開設目的の全部又は一部が、児童ポルノの画像等をそれと知りながらインターネット上で流通させることにあると認められること。

2.（児童ポルノ画像の数量）

当該ドメインに含まれるサイトの中に、
（ア）児童の権利等を著しく侵害するものであることが明白な画像等が存在するか、
（イ）児童の権利等を著しく侵害する画像等が相当数存在するか、
（ウ）児童の権利等を著しく侵害する画像等が相当の割合で存在するか、
のいずれかであること。

3.（発信者の同一性）

（ア） 当該ドメイン内に複数のサイトがある場合には、各サイトの管理者が同一であること。
（イ）（ア）にいう管理者以外の第三者が、当該ドメイン内に設置された電子掲示板等において情報を発信している場合には、
（i）当該情報に2の対象となる児童ポルノの画像等が含まれており、かつ、サイト管理者を当該画像等の実質的な発信者であるとみなしうるような特段の事情が存在すること。
（ii）また、当該情報に児童ポルノ以外の情報が含まれる場合には、当該情報の発信者の多くが、児童ポルノの流通が当該サイトの開設目的であることを認識・認容しながら、当該情報を発信したものと認められること。

4.（他の実効的な代替手段の不存在）

当該ドメインをDNSブロッキングの対象とすることが、1ないし3及びその他の諸般の事情を総合的に考慮した上で、やむを得ないと認められること。

8

ICSA報道発表関係

○ 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の設立総会を開催
平成23年3月3日
URL　　http://www.netsafety.or.jp/news/press/press-000.html

○ 児童ポルノ画像が掲載されたサイトに係るアドレスリストの提供をスタート
平成23年4月1日
URL　　http://www.netsafety.or.jp/news/press/press-002.html

○ 児童ポルノ画像が掲載されたサイトのブロッキングなどの流通防止の取り組みを開始
平成23年4月21日
URL　　http://www.netsafety.or.jp/news/press/press-003.html

(参考)

平成 22 年 11 月 10 日
児童ポルノ流通防止協議会

「児童ポルノ流通防止対策専門委員会」の設置及び運営に関する要綱

1　本要綱の目的

本要綱は、児童ポルノ掲載アドレスリスト作成管理団体の監督等を行う専門委員会の設置及び運営に関し、必要な事項を定めることを目的とする。

2　専門委員会の設置及び名称

(1)　児童ポルノ掲載アドレスリスト作成管理団体運用ガイドライン（平成 22 年３月 25 日児童ポルノ流通防止協議会決定。以下「ガイドライン」という。）第２の２(2)に基づき、児童ポルノ掲載アドレスリスト作成管理団体（以下「リスト作成管理団体」という。）の監督等を行うため、専門委員会を設置する。

(2)　前項の専門委員会の名称は、児童ポルノ流通防止対策専門委員会（以下「専門委員会」という。）とする。

3　専門委員会の構成

(1)　専門委員会は、20 名以上 25 名以内の委員をもって構成する。

(2)　専門委員会の委員は、学識経験者、法律専門家、民間団体・業界団体の代表者等の児童ポルノの流通防止に関する知見を有する者の中から選任されるものとする。

(3)　委員は、次のいずれかに該当するものが選出されてはならない。

ア　リスト作成管理団体の職員

イ　リスト作成管理団体の職員の親族その他特別な関係にある者

ウ　児童ポルノ該当性判定アドバイザー

4　委員の任免

(1)　専門委員会は、３(1)の定員の範囲内において、３(2)の要件を満たし、委員２名以上の推薦を得た者を新任の委員として選任することができる。

(2)　委員は、いつでも辞任することができる。

(3)　専門委員会は、委員にふさわしくない著しい非行があった場合には、当該委員を罷免することができる。

5　委員長

(1)　専門委員会に委員長を置く。

(2)　委員長は、専門委員会を招集し、議事を進行する。

(3)　委員長は、委員の互選により選出する。

(4)　委員長の任期は１年として、再任することができる。

6　専門委員会の任務

専門委員会は、ガイドラインに基づき、次に掲げる事項について審議し、議決するものとする。

(1)　児童ポルノ流通防止対策に関して知見を有する公益法人・民間団体等の中から適切なものをリスト作成管理団体として選定すること。

(2)　リスト作成管理団体の運営状況等について報告を受け、リスト作成管理団体の行う業務の公正かつ円滑な遂行を図るために必要な事項について審議し、その結果をリスト作成管理団体に通知すること。

(3)　ガイドラインの内容、運用等について検討を行うとともに、ガイドラインの改訂その他の必要な措置を講じること。

(4)　リスト作成管理団体の行う業務のうち、次に掲げる重要な事項について承認すること。

ア　児童ポルノ該当性の判定基準に関すること。

イ　アドレスリストからの除外要請の対応要領に関すること。

ウ　リスト作成管理団体とアドレスリスト利用事業者との契約に関すること。

エ　リスト作成管理団体の予算及び決算の承認に関すること。

オ　その他リスト作成管理団体の行う業務のうち特に重要であると専門委員会が認めるもの。

(5)　迅速かつ重層的な流通防止対策が必要な児童ポルノについて、アドレスリストへの掲載を承認すること。

(6)　国内の ISP、検索エンジン事業者、フィルタリング事業者以外の者で、リスト作成管理団体がアドレスリストの提供を行うものを承認すること。

(7)　リスト作成管理団体の監督を行うために必要と認められること。

(8)　本要綱の改定及び本要綱を施行するために必要な細則を制定すること。

7　専門委員会の運営

(1)　専門委員会は、年１回以上定期的に開催するものとする。開催にあたっては、原則として１週間以上前に通知する。

(2)　委員長は、必要と認める場合又は５名以上の委員から議題を指定して開催の要請があった場合には、臨時に専門委員会を開催するものとする。

(3) 専門委員会は、委員の過半数の出席をもって成立する。

(4) 委員長は、専門委員会が必要と認めるときは、インターネット上の児童ポルノの流通防止対策に知見を有する者を参考人として専門委員会に出席を求め、意見を聴取することができる。

(5) 委員長は、専門委員会の陪席を求める者があった場合において、議事の進行又は児童の権利保護の観点から支障がないと認めるときは、専門委員会の陪席を許可するものとする。

(6) 専門委員会は、関係省庁の申し出に基づき、オブザーバとしての参加を認める。

(7) 専門委員会の議事は、出席委員の過半数により決する。可否同数の場合には、委員長の決するところによる。

(8) 前項の規定にかかわらず、次に掲げる事項については、出席委員の４分の３以上の賛成をもって決するものとする。

ア　４に基づく委員の選任及び罷免

イ　６(1)に基づくリスト作成管理団体の選定

ウ　６(3)に基づくガイドラインの改訂

エ　６(4)に基づく同項各号に掲げる重要な事項の承認

オ　６(8)の本要綱の改訂及び細則の制定の承認

(9) 専門委員会においては、十分な審議を尽くすものとする。

(10) 専門委員会は、ガイドラインの改訂に当たっては、パブリックコメントを実施するなど、広くインターネット利用者をはじめ国民の意見を聴くものとする。

8　分科会の設置

(1)　専門委員会は、６に掲げる特定の事項を処理するため、必要に応じて「分科会」を置くことができる。

(2)　分科会の任務及び委員は専門委員会が定める。

(3)　前２項の決定については、出席委員の４分の３以上の賛成をもってする。

９　開催と議事録の公開

専門委員会は、原則、公開として開催する。また、議事録を作成し、原則、公開するものとする。ただし、非公開の場合は議題および理由を公開するものとする。

１０　その他

(1)　専門委員会の事務局は、リスト作成管理団体において行う。

(2)　専門委員会は、ガイドラインの改訂その他必要な措置を講じる場合には、アドレスリストの対象とする範囲を児童ポルノ以外の情報に拡大してはならない。

(3)　専門委員会は、児童ポルノ流通防止対策のために検討すべきことについて議論することができる。

１１　経過措置

(1)　当初の専門委員会の委員は、児童ポルノ流通防止協議会の構成員とする。

(2)　児童ポルノ流通防止協議会は、専門委員会設置後は解散するものとする。

(3)　専門委員会の事務局は、リスト作成管理団体が選定されるまでの間は、本協議会の事務局において行うものとする。