

令和4年2月

サイバー防犯ボランティア
活動のためのマニュアル
(モデル)



平成25年2月 作成
平成29年5月 改訂
令和4年2月 改訂
警察庁生活安全局
情報技術犯罪対策課

目次

はじめに	4
1 活動の目的	5
2 活動を始める前に	6
(1) サイバー防犯ボランティア活動とは	7
(2) 仲間を増やす	8
(3) 活動を長続きさせるために	9
3 活動の基本的心得	12
(1) 安全を第一に	12
(2) インターネットの実態を知る	14
(3) 秘密の保持	17
(4) 最新情報の共有	17
(5) 関係機関・団体等との連携	17
(6) 活動記録の保存	19
(7) 実社会での活動	20
4 具体的な活動方法	20
(1) 教育活動	20
(2) 広報啓発活動	23
(3) サイバー空間の浄化活動	30
5 参考資料	36

<凡例>



ボランティアの現場では

既にサイバー防犯ボランティアの活動を実施している団体や、団体メンバーの皆様から、団体の運営方法や活動方法などについてアンケートを実施し、その集計結果を紹介しています。



事例紹介

既にサイバー防犯ボランティアの活動を実施している団体メンバーの皆様から、日頃の活動の中で感じていることや、工夫している点などについてアンケートを実施し、その内容を紹介します。

はじめに

平穏な市民生活を確保するため、平成15年以降、国を挙げて犯罪抑止対策を推進した結果、刑法犯認知件数が一貫して減少するなど、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いわれています。

インターネットが国民生活や社会経済活動に不可欠な社会基盤として定着し、今や、サイバー空間は国民生活の一部となっていますが、サイバー犯罪の手口は、ますます悪質・巧妙化しているほか、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傾向にあり、インターネット利用に起因する犯罪被害の防止対策が一層重要となっています。

このような状況から、インターネット上においても、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インターネット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ることが重要と考えられます。特に、インターネットは、自分の姿が周りから見えないという匿名性が利用され、人権を侵害する情報の書き込みが行われやすい環境です。これを念頭に、「他人を傷つけるような情報発信は行わない、拡散しない。」という基本的なルールが、インターネット利用者全体に浸透していくことが望ましいと考えています。

そこで、警察庁では、インターネット上においても、自主防犯ボランティアの活動が促進され、その裾野が拡大されることを目的に、「サイバー防犯ボランティア活動マニュアル（モデル）」を作成し、サイバー防犯ボランティアの活動を支援してきたところですが、この度、内容の見直しやアンケート結果を差し替えるなどの改訂をしました。本マニュアル（モデル）が、初めて活動に参加される初心者の方、既に活動をしているが今後どうしたらよいか迷っている方等に対して、安全第一に仲間と楽しみながら、無理をせず活動できるための手引書となり、有意義で効果的なサイバー防犯ボランティア活動の一助となれば幸いと考えています。

1 活動の目的

インターネット上では、その匿名性を利用して、他人の個人情報を勝手に書き込むといった行為や、詐欺、不正アクセスなどの犯罪が敢行されやすく、特にSNS等のコミュニティサイトに起因する児童被害が増加傾向にあり、インターネットの利用に起因するトラブルや犯罪が、いつ私たちの周りで発生してもおかしくありません。

そこで、地域住民に対し、適正なインターネット（携帯電話を含む。）の利用方法についての教育活動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を通じて、サイバー空間の規範意識を改善し、地域住民が安全で安心してインターネットを利用できるようにしましょう。

そして、このようなサイバー防犯ボランティア活動を行うに当たっては、サイバー防犯ボランティア団体結成の契機となった各地域におけるインターネット上の問題や青少年問題等に基づき、それに沿った具体的な活動の目的を定めておくことが大切です。活動の目的を定めないとボランティアメンバーの意識・意欲や活動内容も統一できず、長続きしないことになりかねないため、できる限り目的を定めることをお勧めします。

また、自らの団体の活動の目的を公に発信することで、地域社会や関係機関・団体等との連携がスムーズになり、同じ志を持つボランティアメンバーの参加を促すことにもつながります。

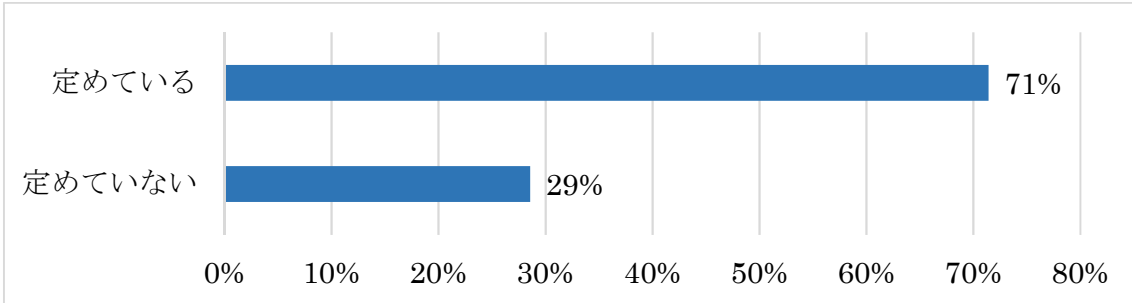
なお、活動の目的を最初から複数挙げて幅広く始めることも一つの方法ですが、最初は目的を絞って設定し、少しずつ目的を拡大していくという方法も考えられます。





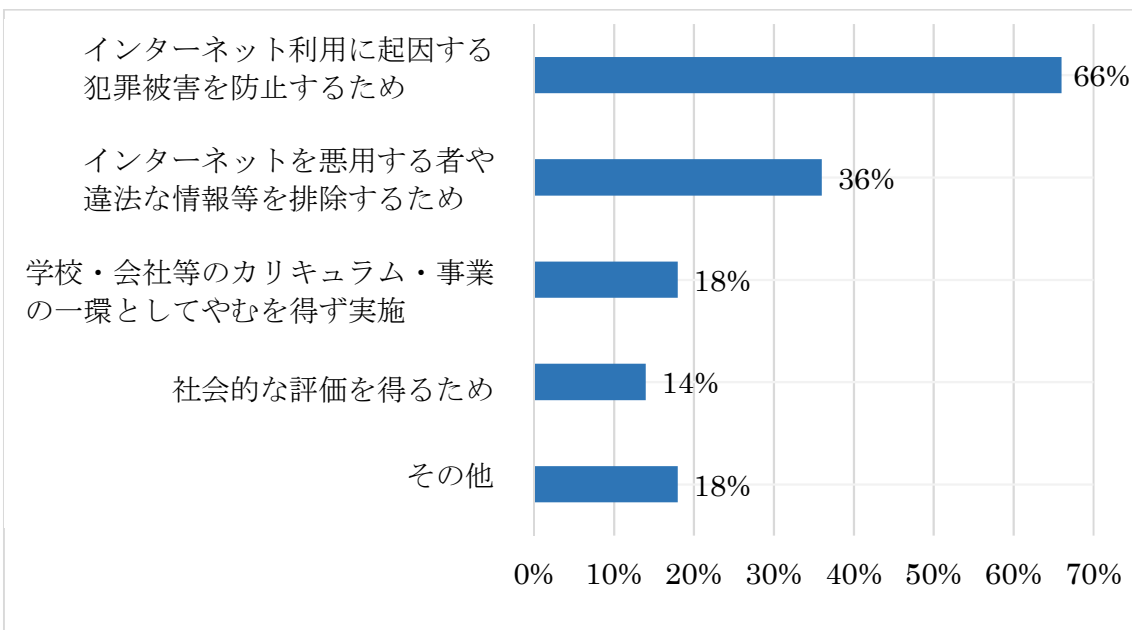
ボランティアの現場では

ボランティアの目的を定めていますか？



ボランティアの現場では

ボランティア活動の目的は？



※「ある」とした回答者における選択率（複数回答）

※その他：社会貢献のためなど

2 活動を始める前に

ボランティア活動は、自主的な活動の目的や計画に基づいて、それぞれが主体となって行うものであり、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もありません。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、ボランティアの活動メンバーみんなでも話し合うことが大切です。

ボランティア活動に当たっては、活動の方向性を明らかにし、仲間を増やしたり、仲間と楽しみながら無理なく気長に取り組むことをお勧めします。

(1) サイバー防犯ボランティア活動とは

サイバー防犯ボランティア活動とは、サイバー空間における防犯ボランティア活動のことをいい、

- ① 犯罪被害防止のための教育活動
- ② 広報啓発活動
- ③ サイバー空間の浄化活動（サイバーパトロール）

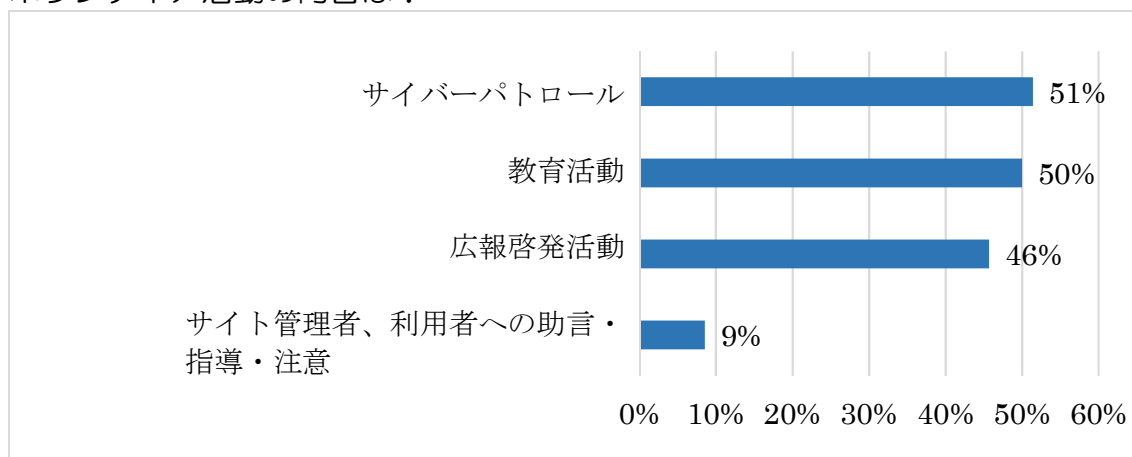
の3つの活動を中心に取り組み、サイバー空間における規範意識の向上に貢献することが期待されます。

なお、本頁以降、サイバー防犯ボランティアを「ボランティア」と表記します。



ボランティアの現場では

ボランティア活動の内容は？

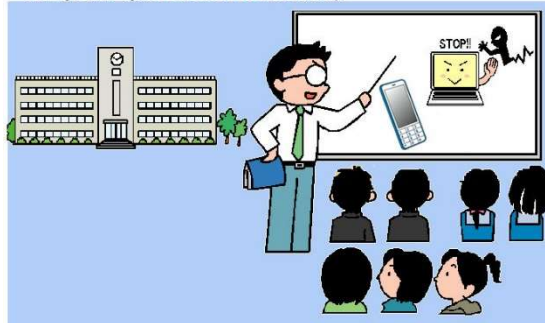


※複数回答あり

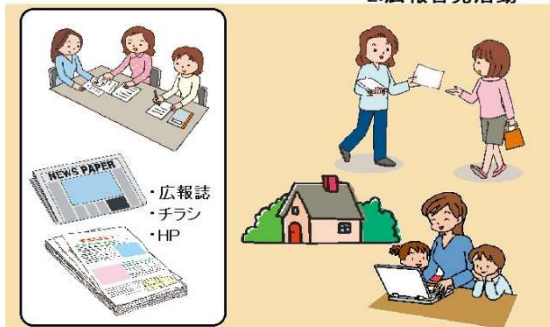
《3つの活動》

サイバー防犯 ボランティアの 3つの活動

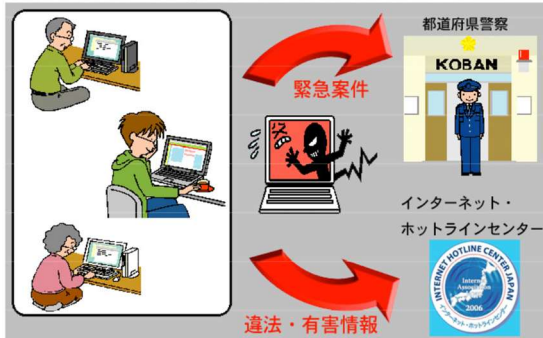
1. 犯罪被害防止のための教育活動



2. 広報啓発活動



3. サイバー空間の浄化活動（サイバーパトロール）



(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「行きすぎた正義感」により、活動が誤った方向へ進む危うさがあります。

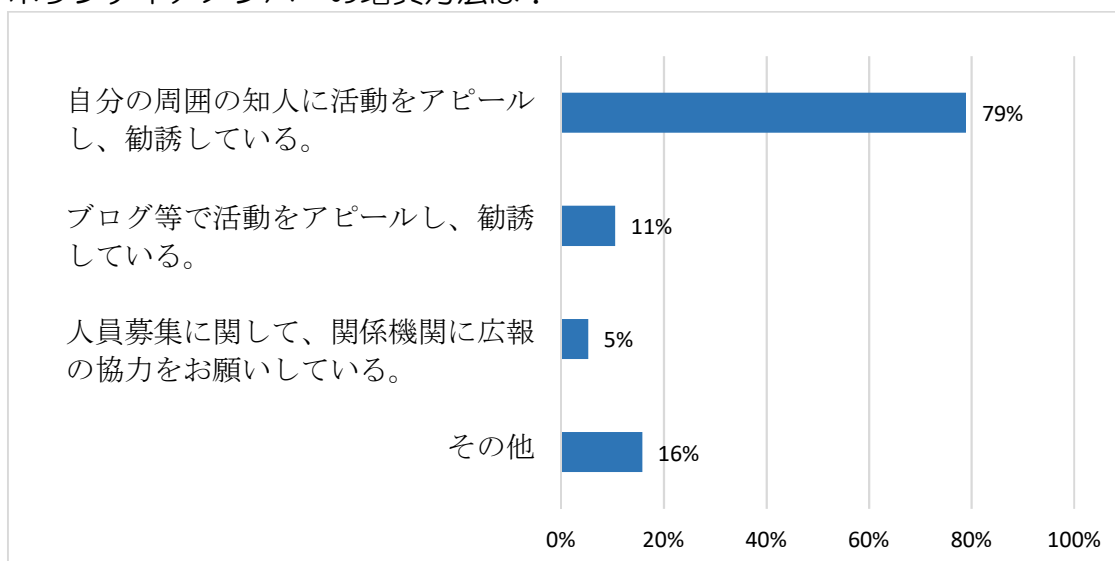
目的に賛同する仲間を増やし、仲間と知識を共有して効果的な活動について話し合い、時には励まし合いながら、楽しんで活動していくことが大切です。





ボランティアの現場では

ボランティアメンバーの増員方法は？



※「ある」とした回答者における選択率(複数回答)

※その他:「情報系学科の学生に対して、ボランティア参加希望者を募る。」、「大学の先輩で勧誘を行う。」、「担当教授の協力を得て、ゼミ生等に声掛けを行うなど。」



事例紹介 (ボランティアメンバーの増員方法)

- ① 同じ学校の後輩に、ボランティアの話をして関心を持ってもらう。
- ② 実際の体験談を交えながら活動の説明を行う。
- ③ 情報系学科の学生に随時参加を呼び掛ける。
- ④ 勧誘パンフレットを配付する。

(3) 活動を長続きさせるために

ボランティア団体に所属しているとはいえ、現状では活動自体を一人で行う機会が多くなる場合があります。一人での活動は、その目的ややりがいを見失い、長続きしないという結果にもなりかねません。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が望ましく、また、活動を活性化することが何より重要です。

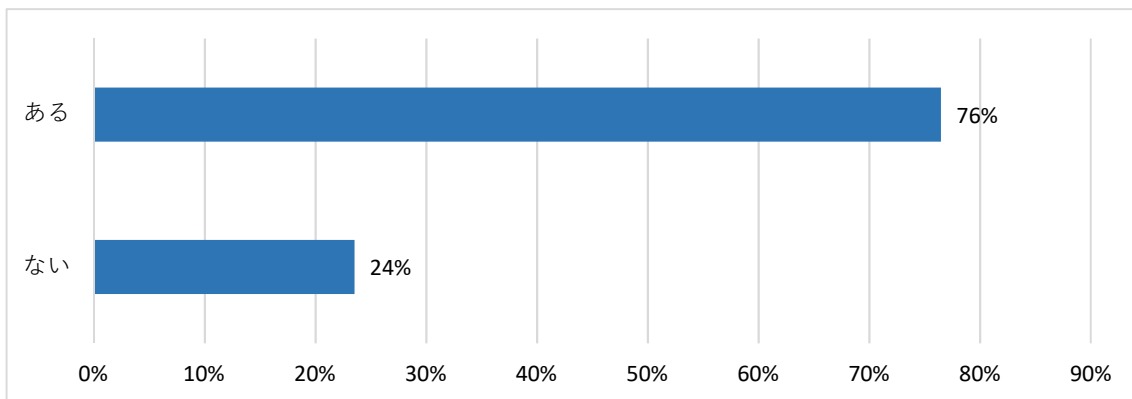
ボランティアメンバー同士で話し合いを心掛けてチームワークを求める一方で、自分の意見に偏りがないように心掛けたり、プライベートの時間とボランティア活動の時間のメリハリをつけたり、ボランティア活動に没頭しすぎないようにするなど、「無理をしない」ことが重要になります。

そして、仲間と楽しみながら、無理なく気長に取り組んでいると、地域の方々から感謝されたり、テレビ放送、ニュース記事、関係機関のホームページ、機関誌等に活動状況が報道、掲載されたりすることで達成感が得られ、更なる活動意欲がわいてくることもあります。



ボランティアの現場では

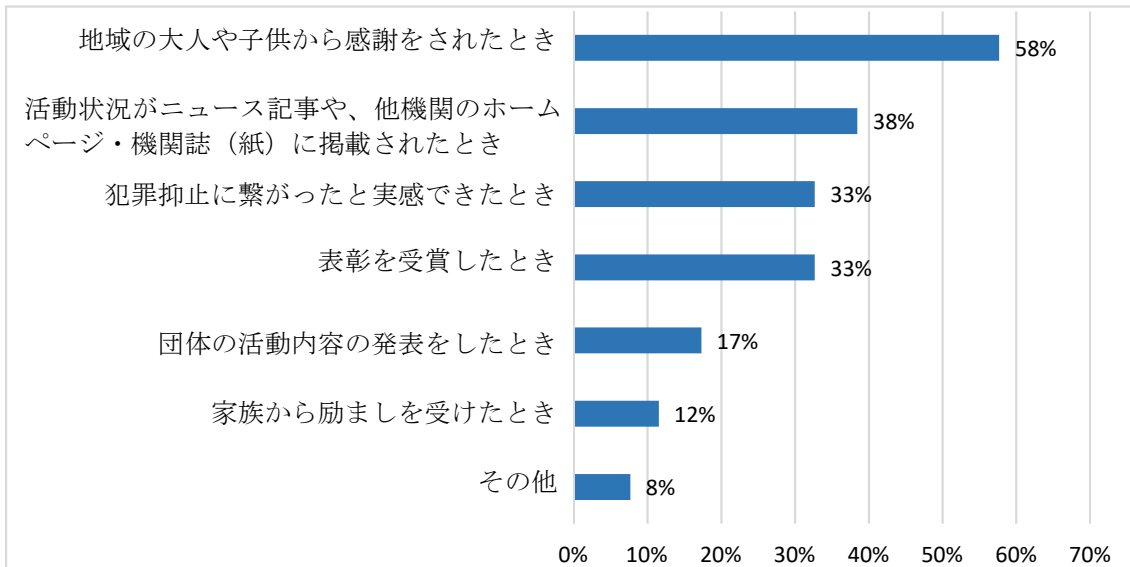
ボランティア活動で達成感を得られたことはあるか？





ボランティアの現場では

達成感の内容は？



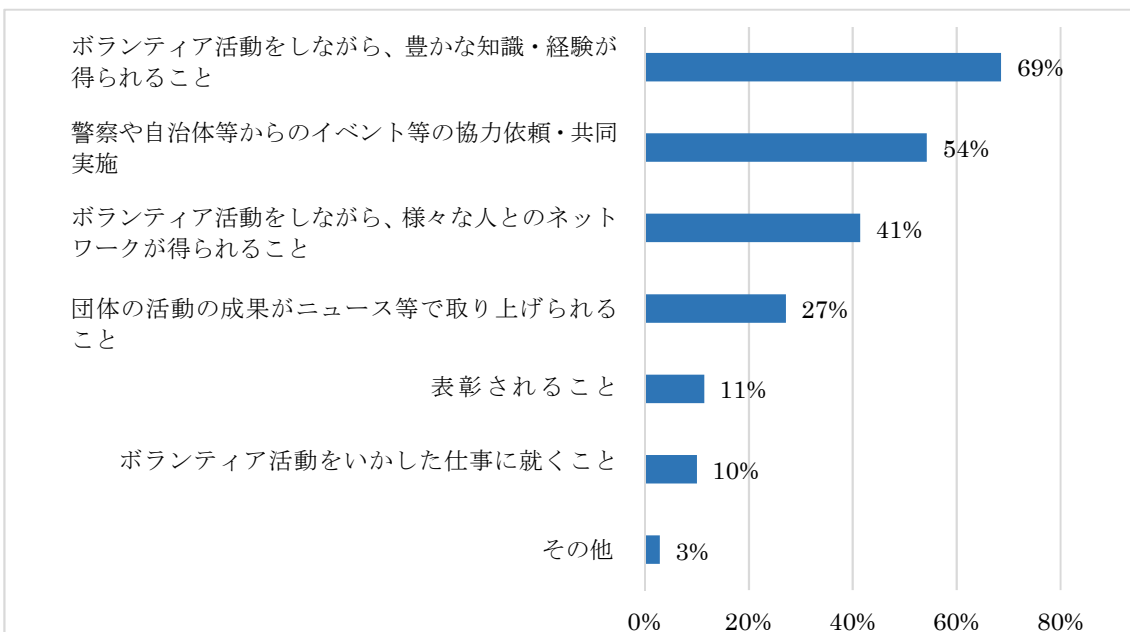
※「ある」とした回答者における選択率(複数回答)

※「その他」:「広報動画の作成に携わることができたとき」、「伝えたいことが伝わったと感じるとき」など



ボランティアの現場では

達成感を得るために何が必要ですか？



※複数回答あり



事例紹介(活動を長続きさせるための方法)

- ① 機会があるごとに、少しでもいいから活動を実施する。(活動の継続)
- ② 警察や学校の担当者とのコミュニケーションを取り、積極的にイベント等に参加する。
- ③ ボランティアの定例会で、報告・検討を実施し、メンバー間の課題共有に努める。



事例紹介(メンバー1人1人がやりがいを持つために工夫していること)

- ① 目標を設定する。
- ② 活動結果を公表する。
- ③ 活動の種別ごとに班分けし、各班のリーダーを中心にメンバー1人1人が協力しながら活動する。

3 活動の基本的心得

(1) 安全を第一に

ボランティア活動に取り組むに当たっては、コンピュータ・ウイルスへの感染やインターネット上での誹謗中傷等の被害に遭わないよう、ウイ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・技能を身に付けて、安全を確保できる範囲内で活動しましょう。

また、インターネットを見続けることにより、通常では知り得ない情報や信憑性のない情報によって混乱を招く事態も想定されます。インターネットの実態を知り、冷静な判断を心掛けましょう。

安全に活動するための知識や心得について、次の参考情報をご覧ください。



《情報セキュリティ初心者のための三原則》

- 1 ソフトウェアの更新（最新の修正プログラムの適用）
- 2 ウイルス対策ソフト（ウイルス対策サービス）の導入
- 3 IDとパスワードの適切な管理

《スマートフォン情報セキュリティ3か条》

- 1 OS（基本ソフト）を更新
- 2 ウイルス対策ソフトの利用を確認
- 3 アプリケーションの入手に注意

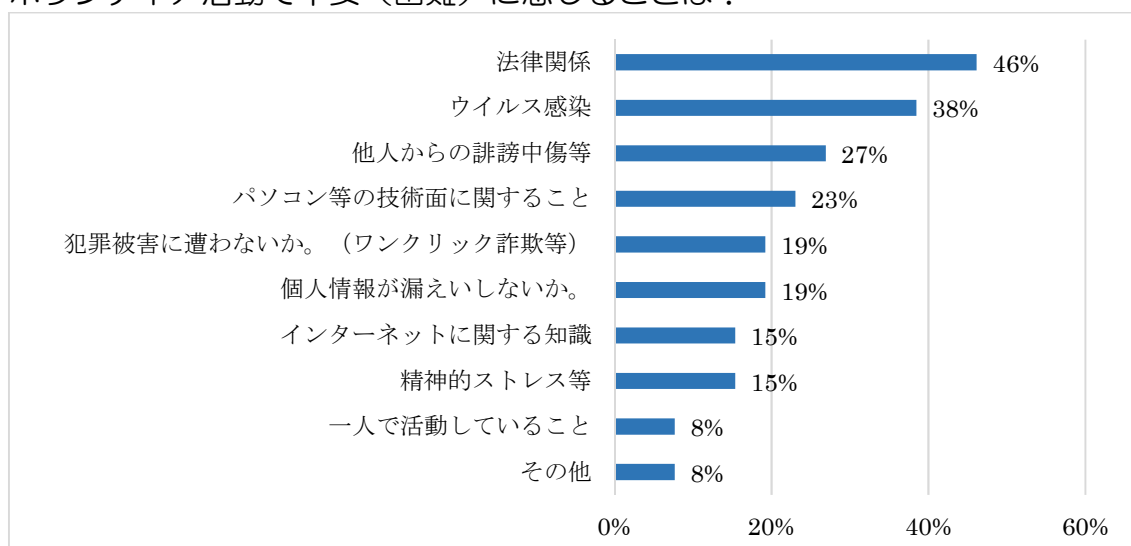
（出典：総務省 国民のための情報セキュリティサイト）

アンケート結果（下記参照）でも、ウイルス感染等に不安を感じている方が多いことが分かります。不安や危険を感じたら、決して無理をせずに、経験のあるリーダーや専門家に相談するなど、自分自身のできる範囲で活動が続けることが大切です。



ボランティアの現場では

ボランティア活動で不安（困難）に感じることは？



※「ある」とした回答者における選択率（複数回答）

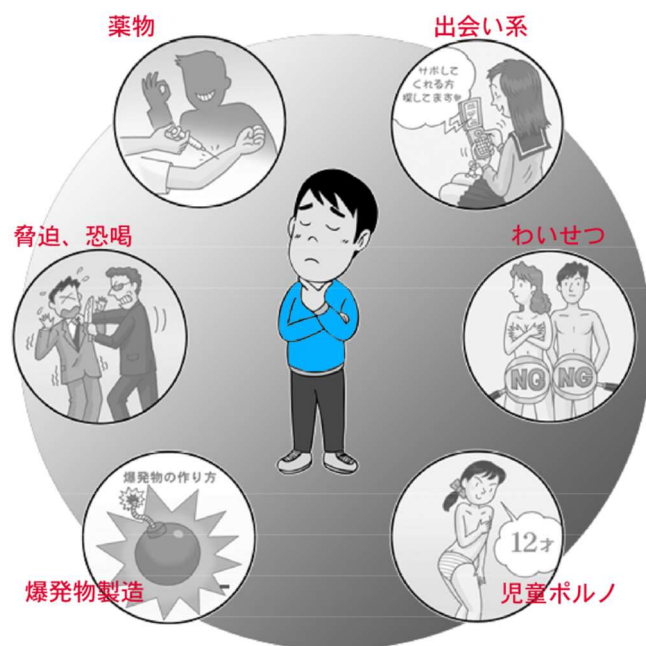
※その他：「自分が子育て中のため、子供に負担を掛けていないか。」「防犯教室で子供たちの心にしっかりと伝わっているか。」など

(2) インターネットの実態を知る

活動中、犯罪被害やトラブルに遭わないために、今、インターネット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。

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、児童ポルノ画像及び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のほか、違法情報には当たらないものの、殺害や報復の請負等の犯罪行為を助長するものや、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ます。

また、このような違法・有害情報とまではいえないものの、青少年にとっては有害となる情報もあふれており、大人の感覚と違いのある青少年の特性や利用実態等も把握した上で活動を進める必要があります。

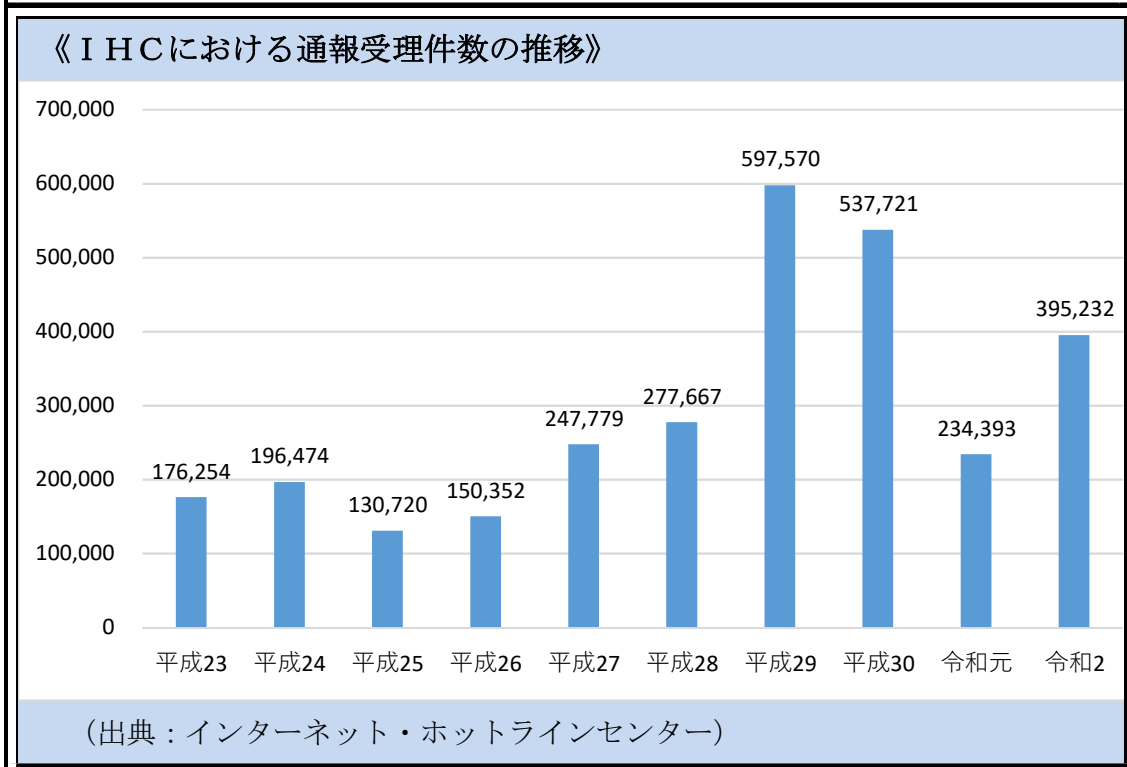
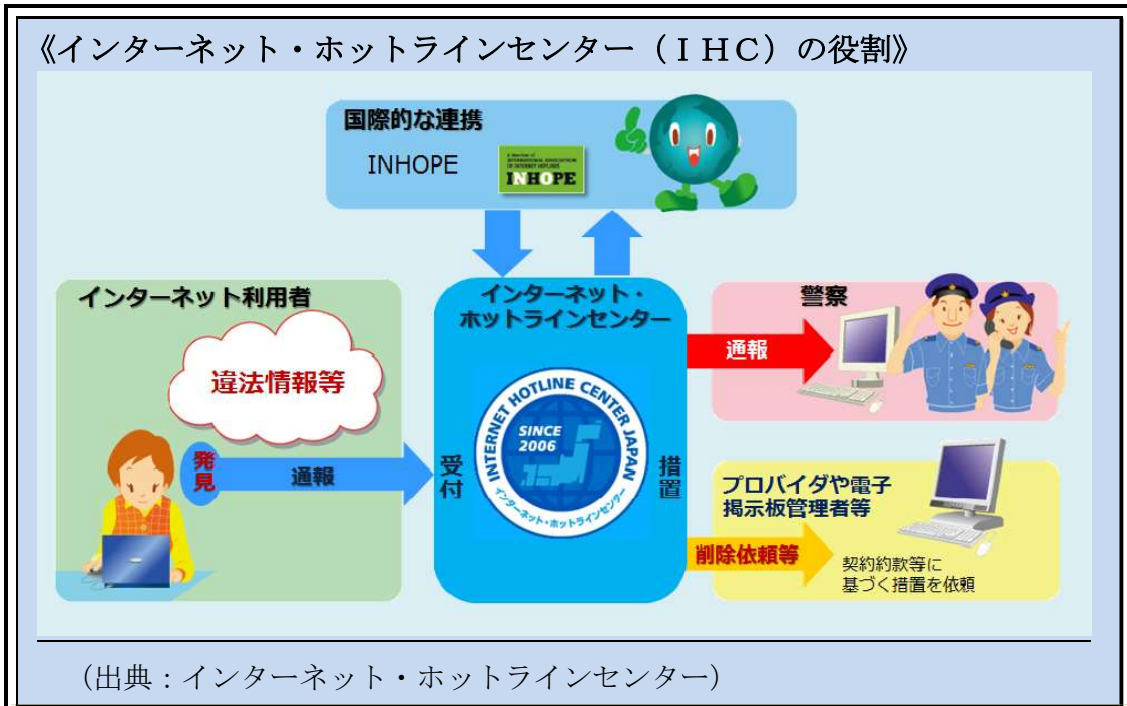


ア 違法情報等の通報受理と対応状況

警察庁が民間事業者に委託して運営しているインターネット・ホットラインセンター（IHC）では、一般のインターネット利用者等から違法情報等に関する通報を受理し、警察への通報やサイト管理者等への削除依頼を行っています。IHCが受理した年間の通報件数は平成27年以降、23万件を超えており、平成29年と平成30年は、50万件を超えています。近年、IHCが受理する違法情報等で多いものは、わいせつや児童ポルノ画像、

規制薬物の広告、自殺誘引等情報などであり、インターネット上にはこうした違法情報等が氾濫しています。

このような違法情報等の通報状況の実態を知ることも活動の参考となります。



イ 警察への相談及び検挙状況

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、相談者に対する助言・指導等を行っています。

平成28年から令和2年の5年間においては、年間のサイバー犯罪等に関する相談件数が、11万件を超えています。

警察庁では、「サイバー空間をめぐる脅威の情勢」について広報しており、その中で、サイバー犯罪等に関する相談件数やサイバー犯罪の検挙状況についても記載しています。

このような警察への相談の実態等を知ることも活動の参考となります。

ウ 青少年を取り巻くインターネット環境

インターネット上では、青少年が閲覧するには、望ましくないと考えられる情報が氾濫し、青少年の興味を引く多様なサービスが次々と登場し、一部ではそれらが悪用されて犯罪被害につながる場合もあるなど重大な問題が起きています。児童買春や児童ポルノを始めとするSNSに起因する事件の被害児童も増加傾向にあり、だまされたり、脅かされたりして児童が自分の裸体を撮影させられた上、メール等で送られるなどの児童ポルノ被害も問題となっています。また、過去には殺人・死体遺棄事件等、SNSを悪用した痛ましい事件も発生しています。

エ 高齢者を取り巻くインターネット環境

政府の調査によれば、高齢者のインターネット利用者の割合は、以前に比べれば、増加し、特に60歳から69歳の年齢層で8割を超えています。また、同年齢層で約6割がスマートフォンを、約5割がパソコンを使用しています。高齢者が、インターネットを使用した詐欺の被害者や不正アクセスなどのサイバー犯罪の被害者となる事件が発生しています。

(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。その取扱いには、十分注意しましょう。

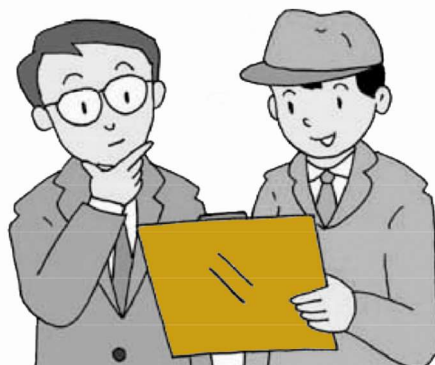
活動を実施する中で他人の個人情報やプライバシー情報を把握してしまうケースもあり、それらを保存した機器等の取扱いも含めて、機密情報保持に関するボランティア団体ごとの取扱基準を作成し、それに沿った活動を実施することが望まれます。

特に、サイバーパトロールを行うと、通常では知り得ない情報（他人のプライバシー情報等）に接する機会がありますので、情報の取扱いを慎重にし、秘密の保持に十分に留意する必要があります。



(4) 最新情報の共有

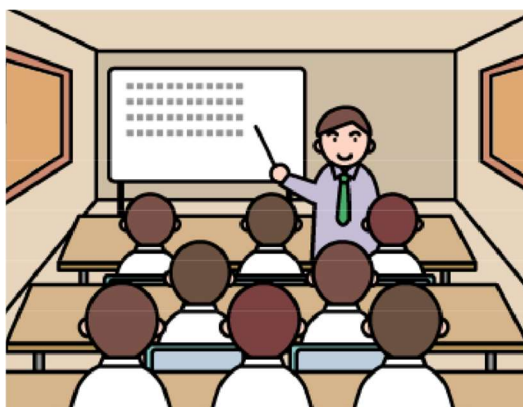
警察や関係機関、自治体から提供される最新の情報は、積極的に活用して、ボランティアメンバー内で共有するとともに、意見交換や研修会等の場で、トラブル事例や効果的な活動例等の情報を交換しましょう。情報を共有することで、活動の活性化にもつながります。



(5) 関係機関・団体等との連携

警察や自治体をはじめ、他の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。

また、他のボランティア団体との交流を深めれば、それぞれの地域独自の特徴や経験談、苦労話を聞くこともできます。苦労を分かち合うことにより、自分たちだけではないんだと勇気がわいてきます。

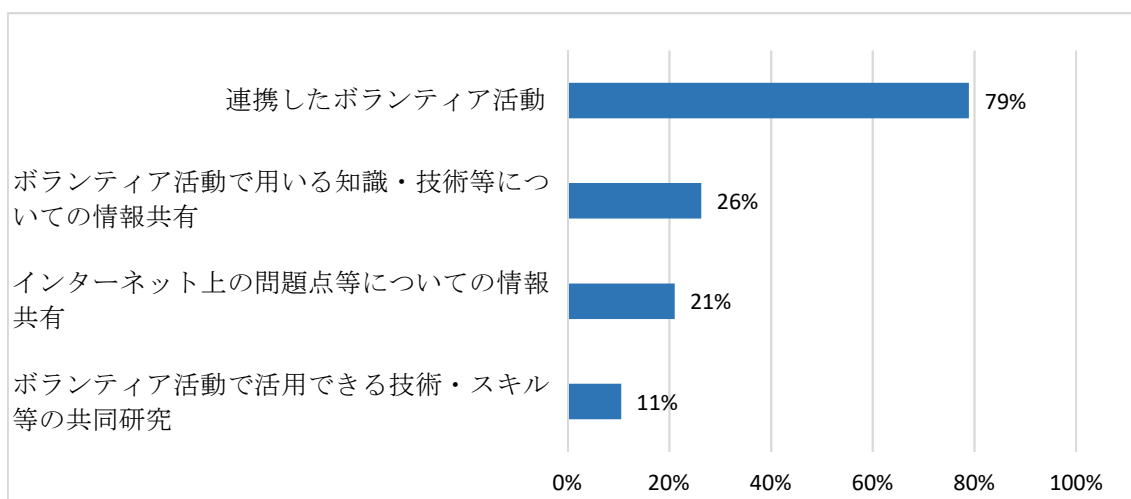


さらに、地元の警察等の公的機関が主催する講習会や、生涯学習教育を行って

いる団体が主催する講習会に参加して、インターネットの知識を高めることもできるでしょう。

ボランティアの現場では

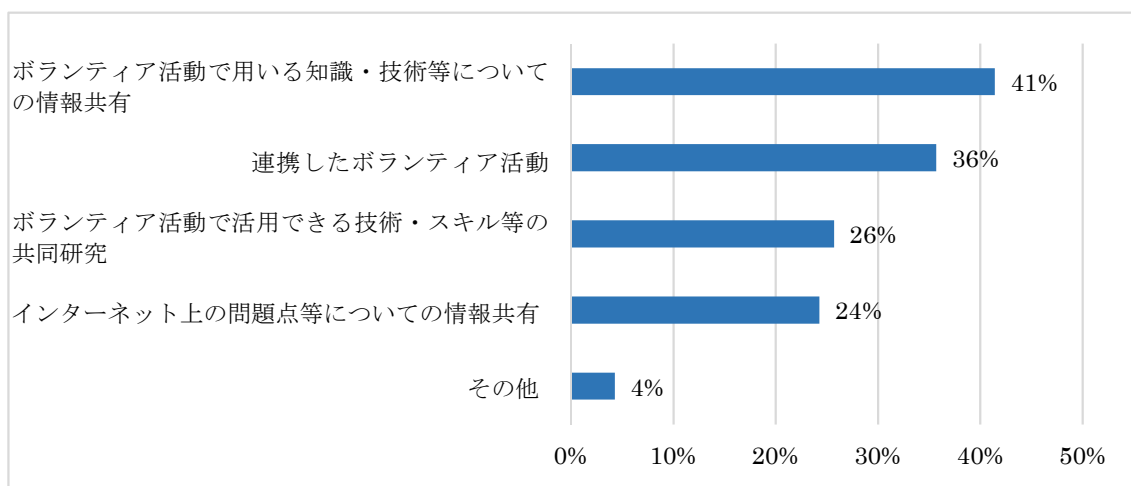
他のボランティア団体とどのような交流を行っていますか？



※「交流がある」とした回答者における選択率（複数回答）

ボランティアの現場では

他のボランティア団体とどのような交流を行いたいですか？



※複数回答

※その他：SNS上で発生する問題について話し合う。



事例紹介(関係機関・団体との連携)

- ① 他の団体と一緒にサイバーパトロールを実施している。
- ② サイバーパトロールシステムを開発し、他のサイバー防犯ボランティア団体に向けて提供している。
- ③ 教育委員会等と連携し、セミナー等を実施している。

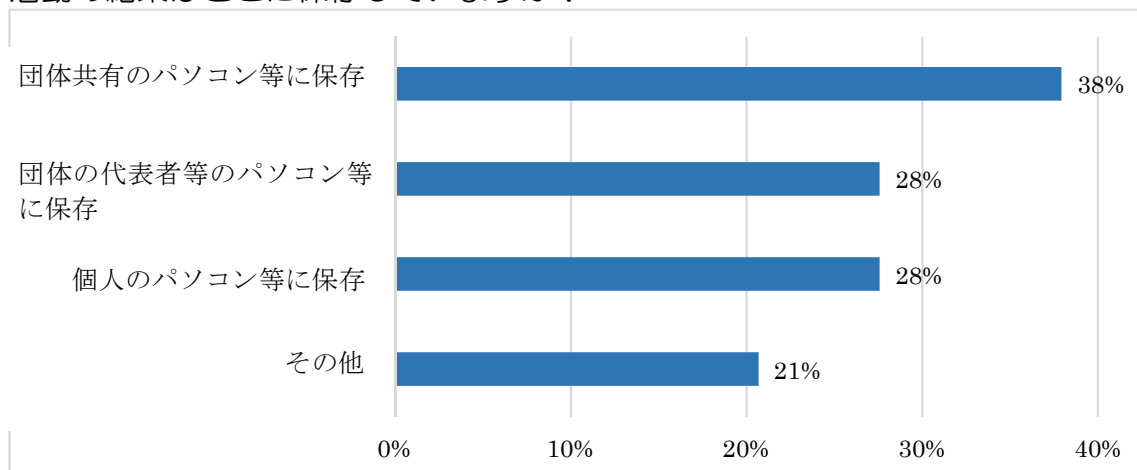
(6) 活動記録の保存

活動の結果については、記録して保存しておきましょう。記録があれば活動を報告する時や過去の活動を振り返る時などに役立ちます。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・効率的なものに改善することにつながります。



ボランティアの現場では

活動の結果はどこに保存していますか？



※「保存している」とした回答者における選択率（複数回答）

※その他：団体のサーバに保存等

(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をしたり、話し合いをするなど実社会での活動が求められる場合には、その必要性や効果を慎重に判断しましょう。

不確かな知識で曖昧な対応をすると、トラブルに巻き込まれることもありますので、事案によっては自分達だけで対応しようとせず、専門機関へ相談するように努めるとよいでしょう。

4 具体的な活動方法

(1) 教育活動

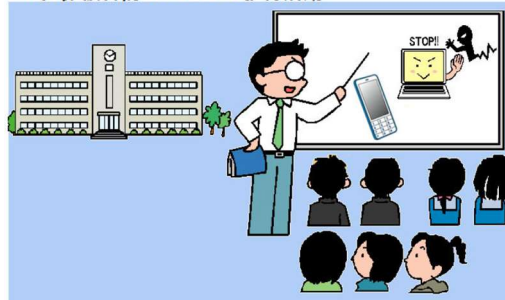
インターネットや携帯電話を利用する青少年及びその保護者、地域住民等を対象に、警察や教育機関、自治体等と連携して、インターネットの実態や危険性、被害防止のための講習を行いましょう。

講習を実施する際には、受講者の年齢、職業、インターネット経験等を踏まえた

講習内容や事前にどのような内容の講習を希望するかを相手方に確認して実施することが重要です。また、後述する「サイバー空間の浄化活動」で把握したインターネット空間の実状を踏まえた講習、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取り入れることで、より大きな効果が得られます。

なお、SNSが悪用された場合の児童被害を防ぐために、まず保護者に対してその危険性等を認識していただくことや、インターネット上での誹謗中傷等により他人の人権を侵害することがないように、インターネットの特性を踏まえた上でルールやモラルを守って利用することが大事であることを教えることも重要です。

1.犯罪被害防止のための教育活動



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当たって収集するものと変わるところはありません。ただし、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

- ①インターネットの各種サービスの仕組み
- ②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
- ③犯罪被害やトラブルを未然に防止するための対策
- ④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。

イ 講習の内容及び方法

講習は、対象者のインターネットに関する知識や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、

- ワークショップ形式で行う
- クイズ形式で行う
- スマートフォン、タブレット等を活用して行う（可能な場合）

など、参加・体験・実践型の教育を行うことが効果的です。

なお、諸般の事情により直接出向いて教育活動ができない場合には、インターネットによるリモート形式で教育活動を行うことも重要です。

参考：児童に対する講習風景



参考：保護者に対する講習風景



参考：リモート防犯教室風景



参考：ワークショップ形式の活動



参考：警察が主催したボランティアのための研修会





事例紹介(講習会資料等を作成する際に工夫していること)

- ① テーマを選ぶ際は、最近増加傾向にあるインターネット上の問題などを取り上げるようにしている。
- ② デザインについては、チラシの配付対象や配置場所を考慮した文字の配置、大きさ、色を考える。シンプルかつインパクトの強い言葉を使う。
- ③ チラシを閲覧した人が自発的に考えることができる内容にする。
- ④ 一般的な統計資料のみではなく、なるべく独自で収集した内容を盛り込む。



事例紹介(講演を行う際に工夫していること)

- ① 学校等の子供向けの講話は学生が中心となって馴染みのある内容を提供できるように心懸けている。
- ② 自作のポスターやキーホルダーなどのグッズを作成して、配布している。
- ③ 講演資料をより良くするため、講演時に学校を訪問し、現状把握活動を行っている。
- ④ 実施前には必ず資料に目を通すとともに、聞き取りやすい声のトーンや間の取り方等のイメージトレーニングを行っている。

(2) 広報啓発活動

自治体、関係機関・他のボランティア団体、民間事業者等と連携し、インターネット利用者のみならず、広く一般市民に対して、街頭での防犯キャンペーンやイベントなどを行ったり、また、最新のサイバー犯罪の実態等について広報するなどして、サイバー犯罪被害防止とインターネット利用時の規範意識の向上のための広報啓発活動を積極的に行いましょう。

広報啓発活動の具体的な方法として、

- ①政府の情報セキュリティ月間（毎年2月～3月）に合わせたキャンペーン、セミナー、シンポジウム等の開催、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習、パネルディスカッションを通じた広報啓発活動
- ②青少年の携帯電話等の購入が多く見込まれる進級・進学時期における学校・PTAと連携した集中的かつ効果的な広報啓発活動
- ③各地域における公民館活動時等を利用した広報啓発活動等が考えられます。

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、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るだけでなく、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。また、独自にボランティア団体のホームページを作成し、その活動状況や広報啓発資料を掲載することも有効な手段であると考えられます。

なお、広報啓発資料を作成する際は、著作権を侵害しないように注意する必要があります。ホームページ等に掲載されている写真や絵図等は、誰かが著作権を有している場合があります。

(7) 素材の収集

素材は

- ①警察やセキュリティ関連団体・企業が発信する防犯・セキュリティ情報
- ②各公的機関等が作成している違法・有害情報対策のホームページ等のポータルサイト情報
- ③活動に際して知り得た防犯・トラブル事例
- ④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。

(1) 資料の作成

読む人に応じた内容（年齢、インターネットの経験、青少年・保護者・教職員等の属性の別、公開・限定公開等の方針の別などに応じたもの）の資料を作成しましょう。また、作成する資料は、簡潔・明瞭な文書構成を基本として、文字ばかりではなく、写真や絵図等を使用してできるだけ分かりやすくすることが大切です。しかし、必要以上に綺麗に仕上げるために多大な時間を要したり、高額な費用や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

独自に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布しましょう。また、各公的機関が作成し、無料配布している広報資料も効果的に利用するとともに、配布に際しては、ボランティア活動への参加も呼び掛けてみましょう。

イ 防犯キャンペーン・イベント等の開催

防犯キャンペーン・イベント等の開催は、より多くの人への周知が図られるばかりでなく、その活動が広報、紹介されることで、活動の認知度も上がり、さらに大きな効果が得られます。

(7) 計画について

開催の趣旨・目的を明らかにし、それに適した方法（キャンペーン・イベント等）、場所（駅・レジャー施設・イベント会場等）を選択し、計画を立てましょう。

既に複数のボランティア団体で行われている一例としては、

- ①防犯・セキュリティ関連担当者の基調講演
- ②インターネット機器等を用いた体験型学習
- ③広報啓発資料の配布

等が挙げられます。

また、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掛け、支援・後援を得ることも大切です。

(イ) 実施について

対象とする参加者は、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青少年ばかりでなく、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掛けましょう。

参考：サイバー防犯ボランティアによる広報啓発活動



学生防犯ボランティアが主体となって実施した広報啓発活動において、サイバー防犯ボランティアの学生らによるサイバー検定を実施しました。パソコンを使用した〇×クイズ形式で、インターネット動画の視聴上の注意点、オンラインゲームの危険性等について、来場した子供達に学んでもらいました。

参考：広報啓発資料

(福岡県警察作成)

サイバー犯罪に 気をつけて

サイバー
妖怪出現中!



ねらっちゃうぞ
セキュリティの
あまい人

あなたのセキュリティあまい度チェック!

- ✓ 届いたメールやショートメッセージに添付されたファイルや記載されたリンクは身に覚えがなくても(無条件に)開いてしまう
- ✓ 同じパスワードをあちこちで使い回している
- ✓ セキュリティ対策ソフトを使っていない
- ✓ パソコンやスマートフォンは買った時のまま、アップデートはしていない
- ✓ インターネット上の記事や投稿などの情報をすべて信じている
- ✓ 自分の名前や写真、行動などをSNSでバンバン公開している

チェックがある人、ねらっちゃうぞ!

福岡県警察本部サイバー犯罪対策課

参考: 広報啓発資料

(サイバー防犯ボランティアと富山県警が連携して作成)

富山県警察本部 サイバー犯罪対策課

SNSの危険性!!

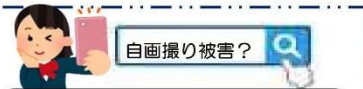
富山県警察
学生安全ボランティア



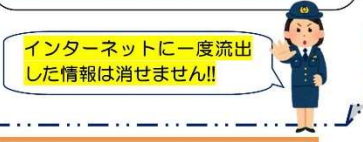
～被害者にも加害者にもならないために～

サイバー関連の被害や犯罪

ネットを使った被害や犯罪はたくさんあります。



相手から言われるままに、下着姿の写真を送ったところ、「言うことを聞かないとネット上に写真を公開するぞ」などと脅された、ということも。
SNSで知り合った人はもちろん、友人や恋人であっても**第三者に見られたら恥ずかしい写真は撮らない、送らない!!**



被害に遭わないために

1 個人情報のをせない
個人情報や住所、顔が分かる写真などを安易にアップしてはいけません。
・ 誰かに悪用されることも!
・ 写真に写っている背景だけで自宅を特定されることもあるので注意しましょう。
・ 投稿の閲覧権限を友達限定の公開にするなど適切な設定を。

2 SNSで知り合った人と会わない
「会おう」「写真が欲しい」「電話番号や住所を教えて」と言われても応じてはいけません。
・ SNS上の情報では、プロフィールの年齢や性別が本当なのか分かりません。

3 人を傷つける投稿をしない
相手を思いやる気持ちが大切です。
・ 軽い気持ちの投稿が相手を傷つけることも。
・ 顔が見えないからこそ、言葉を慎重に選びましょう。

加害者にならないために

WARNING
ダメ、犯罪!!

- 相手を傷つける書き込み → 名誉毀損
- 他人のID、パスワードを勝手に使う → 不正アクセス禁止法違反
- 雑誌などの記事や写真を無断転載 → 著作権法違反
- 悪ふざけ写真の投稿 → 業務妨害

重要 困ったことがあったら
一人で悩まず周りの人や警察に相談しよう!!

※不正アクセス禁止法…不正アクセス行為の禁止等に関する法律

参考: 広報資料

(長野県飯田OIDE長姫高等学校作成)

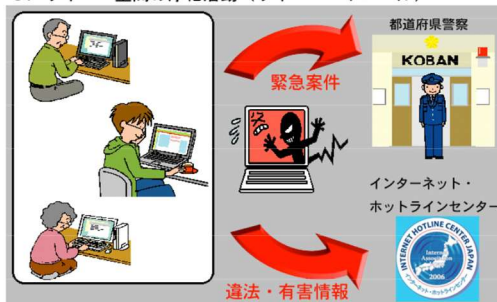


(3) サイバー空間の浄化活動（サイバーパトロール）

サイバーパトロールとは、インターネット上の違法情報等を発見する活動のことをいいます。サイバーパトロールを通じて発見した違法情報等については、インターネット・ホットラインセンターやサイト管理者等に通報しましょう。

なお、犯罪予告や自殺予告に関する書き込み等の緊急案件は、110番か最寄りの警察署に通報を行うようにしてください。

3. サイバー空間の浄化活動（サイバーパトロール）



ア サイバーパトロールの進め方

サイバーパトロールの進め方は、実施主体（個人又は団体）、実施時間、閲覧対象等により様々な方法が考えられます。ここでは、いくつかのサイバーパトロールの進め方の例を紹介します。

○ SNSなどのコミュニティサイトにおけるパトロール

令和2年中のコミュニティサイトにおける被害児童数は1,819人で、平成20年以降増加傾向にあります。事業者に対しては自主的な児童被害防止対策を講じるよう働き掛けを行っているところですが、未だ公然と援助交際を誘引するような書き込みが後を絶たず、児童被害における出会いの温床となっています。

児童ポルノ、児童買春、青少年保護育成条例違反等の児童被害に関心のある方は、SNSなどのコミュニティサイトにおいて被害児童数が増加傾向にあるという現況を踏まえ、ご自身に身近なSNSで、検索機能を用いた重点的なサイバーパトロールを実施することが有効な方法の一例として挙げられるでしょう。その際には、隠語や伏せ字に注意を払うことが重要です。

どのような情報に重点を置いてよいか判断できないという方は、警察が主催する各種キャンペーンやサイバー防犯ボランティア研修会等に参加し、サイバー空間の犯罪情勢について理解を深めるとよいでしょう。

また、コミュニティサイトでは、人を自殺に誘引・勧誘する情報等が書き込まれる場合があります。こうした情報についてサイバーパトロー

ルを行うことも重要です。

○ 電子掲示板におけるパトロール

インターネット上には、不特定多数の者が自分の身元を隠したまま
で自由に書き込んだり、閲覧できる「電子掲示板（ＢＢＳ）」が多数存
在し、無修正ビデオの販売や児童買春の勧誘に関する情報等が書き込
まれている場合があります。

○ インターネット・オークションサイトにおけるパトロール

インターネット・オークションサイトなどにはわいせつ物や違法薬
物等の禁制品が出品されている場合があります。

検索機能等を活用し、こまめに語句検索を行うなどのパトロールが
有効です。

○ 技能を活かしたパトロール

高度な情報通信技術を有する方は、その能力を活かしたサイバーパ
トロールをすることが可能です。例えば、ＩＴ関係企業の社員や大学生
で構成されるボランティアの方の中には、インターネット上の隠語等に
対応する独自の検索システムを開発し、ＳＮＳ上の違法情報等を効率的
に発見できるサイバーパトロールを実施されている方もおられます。

イ 発見時の措置

○ インターネット・ホットラインセンターへの通報

違法情報等を発見した際は、インターネット・ホットラインセンター
等へ通報しましょう。

インターネット・ホットラインセンターでは、一般のインターネット
利用者等から違法情報等に関する通報を受理し、警察への通報やサイト
管理者等への削除依頼を行っています。

インターネット・ホットラインセンターへの通報は、インターネット
上の通報フォームから匿名で行うことが可能であるほか、後日処理結果
を確認することも可能です。通報フォームには、違法情報等の種別につ
いて参考となる内容が掲載されていますので、サイバーパトロールで発
見した情報と照らし合わせながら通報を行いましょう。

IHCに通報される違法情報

- ① わいせつ電磁的記録記録媒体陳列（刑法第175条第1項）
- ② 児童ポルノ公然陳列（児童ポルノ法第7条第6項）
- ③ 売春目的等の誘引（売春防止法第5条第3号及び第6条第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（覚醒剤、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（覚醒剤取締法第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 指定薬物の広告（医薬品医療機器等法第76条の5）
- ⑧ 指定薬物等である疑いがある物品の広告（医薬品医療機器等法第76条の6の2第1項及び同
3項）平成27年4月1日追加
- ⑨ 危険ドラッグに係る未承認医薬品の広告（医薬品医療機器等法第68条）
- ⑩ 預貯金通帳等の譲渡等の勧誘・誘引（犯罪収益移転防止法第28条第4項）
- ⑪ 携帯電話等の無断有償譲渡等の勧誘・誘引（携帯電話不正利用防止法第23条）
- ⑫ 識別符号の入力を不正に要求する行為（不正アクセス禁止法第7条第1号）
- ⑬ 不正アクセス行為を助長する行為（不正アクセス禁止法第5条）

IHCに通報される有害情報

- ① 情報自体から、違法行為（けん銃等の譲渡等、爆発物等の製造、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・勧誘する情報等

○ サイト管理者等への通報

前記のIHCに通報される情報に該当しない情報であっても、援助交際誘引等、不適切な出会いに関する書き込みなどについては、サイトの規約で禁止されているものもあります。このようなものを発見した際は、サイトの規約等を確認した上で、サイト内の通報フォームからサイト管理者等に対して積極的に通報し、書き込みなどの削除等を求めましょう。

ウ 基本的留意事項

サイバーパトロールの実施に当たっては、様々な危険性が潜んでいますので、次の点に留意しましょう。

- ①安全が確かめられる範囲内でパトロールを実施しましょう。

- ②精神的な負担が大きくなるように注意しましょう。
- ③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をしましょう。
- ④ウイルス対策ソフトを導入し、アップデートを確実に行いましょう。
- ⑤データ及びシステムのバックアップを行いましょう。
- ⑥他人のID、パスワードは使用してはいけません。（不正アクセス禁止法違反に当たるおそれがあります。）
- ⑦フィッシングメール・フィッシングサイトに注意しましょう。
- ⑧掲示板等に氏名や電話番号等の個人情報を入力しないようにしましょう。
- ⑨インターネットに接続するパソコン等には、IDやパスワード、クレジットカード番号等の重要な個人情報を保存しないようにしましょう。
- ⑩知り得た不正な攻撃方法等（クラッキング等）を試してはいけません。（業務妨害等の罪に当たるおそれがあります。）



参考：サイバーパトロール活動の状況
～大学生ボランティアによる活動～



参考：関係団体と連携したボランティアの取組
～JC3(※)と連携したサイバーパトロール活動の状況～



※ 一般財団法人日本サイバー犯罪対策センター（JC3）

JC3は、我が国における新たな産学官連携の枠組みとして、平成26年から業務を開始したものであり、産学官の情報や知見を集約・分析し、その結果等を還元することで、脅威の大本を特定し、これを軽減及び無効化することにより、以後の事案発生の防止を図っています。



事例紹介(サイバーパトロールで苦労していること)

- ① 違法・有害情報がなかなか発見できない。
- ② どのサイトをどのようにパトロールすればよいかわからない。
- ③ 長時間のパトロール疲れ

5 参考資料

※各サイトの利用条件に従うこと。

○民間事業者等サイト

サイト名 (制作)	内容	URL
違法・有害情報相談センター	インターネット環境における違法・有害情報及び安心・安全に関わる相談、疑問に相談員が助言する。	https://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。	https://rm.iajapan.org/

○省庁関係サイト

サイト名 (制作)	内容	URL
青少年有害環境対策 (内閣府)	青少年が安全に安心してインターネットを利用するために必要な情報や保護者・事業者の方に取り組んでもらいたいこと、青少年の安全・安心なインターネット利用環境整備に関する法制度や施策等の推進について紹介している。	https://www8.cao.go.jp/youth/kankyoku/index.html
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。	https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
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。	https://www.moj.go.jp/JINKEN/index_soudan.html

○警察関係サイト

サイト名 (制作)	内容	URL
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。	https://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くれる。	https://www.npa.go.jp/cyber/safety/
@ p o l i c e (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。	https://www.npa.go.jp/cyber/police/
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。	https://www.npa.go.jp/cyber/soudan.htm

○違法情報等通報サイト

サイト名 (制作)	内容	URL
IHC (インターネット・ホットラインセンター)	一般のインターネット利用者等から違法情報等に関する通報を受理し、警察への通報やサイト管理者等への削除依頼を行う。	https://www.internethotline.jp/

○講習・広報啓発素材収集のための参考サイト

サイト名 (制作)	内容	URL
サイバー犯罪対策 統計 (警察庁)	サイバー犯罪に関する統計情報を発表している。	https://www.npa.go.jp/cyber/statistics/index.html
サイバー犯罪 広報・施策 (警察庁)	サイバー犯罪対策に関する取組、注意喚起情報、広報啓発資料等を掲載している。	https://www.npa.go.jp/cyber/policy/index.html
JC3 (一般財団法人日本サイバー犯罪対策センター)	○脅威具体例 ○注意喚起情報	https://www.jc3.or.jp/