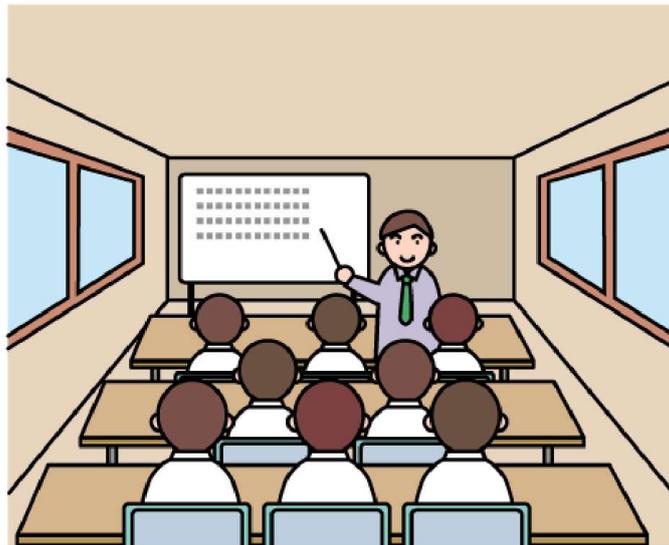


令和4年2月

サイバー防犯ボランティア
育成のための研修カリキュラム
(モデル)



平成25年2月 作成
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	1
1 育成カリキュラム	1
2 参考資料	3
3 サイバー防犯ボランティア団体による実践例	8
4 インターネット基本用語集	10

はじめに

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、その魅力があります。

しかし、サイバー防犯ボランティアの活動を行うに当たっては、インターネットに関する知識や技能を要する場面もあれば、何かしらの判断力を要する場面もあります。

サイバー防犯ボランティア活動を行うに当たっては、少なくとも最低限の育成のための研修カリキュラム（以下「育成カリキュラム」という。）を受講し、インターネット上で問題となっている最新の実態を理解するとともに、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ることが望まれるところです。

そこで、警察庁では、サイバー防犯ボランティアが活動するために必要な知識と技能について、最低限かつ基礎的な内容で構成され、およそ1日から2日の時間をかけて習得することを規定したボランティア育成のカリキュラム（モデル）を作成し、サイバー防犯ボランティアの育成を支援してきたところですが、この度、必要な改訂を行いました。

本育成カリキュラムは、安全に安心してサイバー防犯ボランティア活動ができるようにするための一助として、活動を始める前に受講するものです。また、参考資料も数多く掲載しています。インターネット上のホームページやポータルサイトで掲載されている官公庁や関係団体等の資料です。（資料の活用にあたっては、それぞれのサイト等に示された利用条件等に従ってください。）

さらに、既に活動を行っているボランティア団体が実践している育成カリキュラムの例についても紹介していますので、参考としてください。

1 育成カリキュラム

本育成カリキュラムは、サイバー防犯ボランティアが初めて活動を行う際に必要な知識と技能について、一つのモデルとして項目と時間数を例示するものです。

このモデルを参考に、各ボランティア団体の実情に合わせた必要最低限な育成カリキュラムの内容や実施方法についての検討をお勧めいたします。

全てのカリキュラムを独自で検討、実施することは一般的に負担が大きいことから、例えば、既に活動を行っているボランティア団体の経験者等に、活動の要点の解説や、体験型学習（ロールプレイング）の実施等について、協力を仰ぐような工夫をすることも考えられます。

サイバー防犯ボランティア育成カリキュラム（モデル）

項目	小項目	内 容	目 標	時間
概況	インターネットの実態	<ul style="list-style-type: none"> ○インターネットの実態、利便性 ○インターネットの危険性 ○サイバー犯罪相談、検挙状況 ○具体的な相談事例、検挙事例 	インターネットの実態、利便性及びその背後に潜む危険性を理解させるとともに、サイバー防犯ボランティア活動の必要性や活動上の基本的な心構えを理解させる。	0.5
	ボランティア活動の要点	<ul style="list-style-type: none"> ○ボランティア活動の在り方 ○ボランティア活動の具体的目的 ○基本的な心構え 		0.5
基礎知識	インターネットの基礎知識	<ul style="list-style-type: none"> ○インターネットの基礎用語 ○インターネットの仕組 ○各種コンテンツの仕組、利用方法 	インターネットの仕組や広く一般に利用される各種コンテンツの仕組、利用方法を理解させるとともに、関係法令や官民連携した違法・有害情報対策を理解させ、ボランティア活動上必要とされる基礎知識を習得させる。	1.0
	違法情報	<ul style="list-style-type: none"> ○IHCの違法情報（13類型） ○その他の違法情報 ○違法情報の具体例 		0.5
	有害情報	<ul style="list-style-type: none"> ○IHCの有害情報（自殺誘引等情報） ○その他の有害情報 ○有害情報の具体例 		0.5
	関係法令	<ul style="list-style-type: none"> ○サイバーセキュリティ基本法 ○プロバイダ責任制限法 ○電子消費者契約法 ○青少年インターネット環境整備法 ○出会い系サイト規制法 など 		0.5
	違法・有害情報対策	<ul style="list-style-type: none"> ○政府における推進体制・取組、官民連携 ○民間事業者の主な取組 		0.5
活動要領	教育活動	<ul style="list-style-type: none"> ○講習素材の収集 ○講習の内容及び方法の選定 ○活動上の留意事項 	サイバー防犯ボランティアに期待される各種活動につき、活動重点、活動要領及び活動上の留意事項等を理解させるとともに、安全かつ安心して活動を継続させるために必要な知識と技能を習得させる。 (実際に予定する活動のみを選択し、カリキュラムとして設定するものとする。)	1.0
	広報啓発活動	<ul style="list-style-type: none"> ○参考資料の収集 ○啓発資料の作成要領 ○活動上の留意事項 		1.0
	インターネット空間の浄化活動（サイバーパトロール）	<ul style="list-style-type: none"> ○情報収集のポイント ○違法情報等の発見時の措置 ○活動上の留意事項 		1.0
	体験型学習	<ul style="list-style-type: none"> ○実際の活動の見学 ○ロールプレイング方式の演習 		2.0
その他	関係機関・団体等	<ul style="list-style-type: none"> ○関係機関・団体等の紹介 ○連携を要する関係機関・団体等 ○情報共有を要する関係機関・団体等 	ボランティア活動を実施していく上で、関係機関・団体等との連携の必要性を理解させる。 ボランティアを組織化し、安全に活動するための知識や心得を習得させる。	0.5
	その他	<ul style="list-style-type: none"> ○ボランティアの育成、組織化 ○安全に活動するための基本的心得 ○ネット社会の常識など 		0.5
育成カリキュラム時間総計				10.0

(注) 上の表中「IHC」とは、インターネット・ホットラインセンターのこと。

2 参考資料

(令和4年1月現在)

(1) 概況

インターネットの実態、利便性及びその背後に潜む危険性並びにサイバー防犯ボランティア活動の必要性や活動上の基本的な心構えを理解させるための資料です。

ア インターネットの実態、利便性、危険性

	参考サイト名等	参考となる内容	アドレス
1	首相官邸 (IT総合戦略本部)	○高度情報通信ネットワーク社会の形成に関する施策の企画・立案等を行うための各種会議状況、提言等を紹介	https://www.kantei.go.jp/jp/singi/it2/index.html
2	官民ボード (ここからセキュリティ!)	○不正アクセス防止対策に関する官民意見集約委員会 (官民ボード) が構築した情報セキュリティサイトで、警察庁等の統計情報などを含むセキュリティ関連コンテンツを多数紹介	https://www.ipa.go.jp/security/kokokara/
3	IPA (独立行政法人情報処理推進機構)	○ウイルス・不正アクセスの届出、対策のしおり、年毎の10大脅威、注意喚起など	https://www.ipa.go.jp/security/
4	(財) インターネット協会 (インターネット統計情報)	○インターネット人口の調査 ○インターネット白書、情報通信白書等を紹介	https://www.iajapan.org/internetdata/

イ サイバー犯罪相談、検挙状況、具体的な相談事例、検挙事例

	参考サイト名等	参考となる内容	アドレス
5	内閣府 (児童虐待、いじめ、ひきこもり、不登校等についての相談窓口)	○児童虐待、いじめ、ひきこもり不登校等の相談・通報窓口の紹介	https://www8.cao.go.jp/youth/soudan/
6	警察庁 (サイバー犯罪対策)	○統計資料 ○サイバー空間の脅威情勢など	https://www.npa.go.jp/cyber/statics/index.html
7	警察庁 (なくそう、子供の性被害)	○児童ポルノ関係の検挙状況、被害状況 ○参考リンク集 (関係法令等) の紹介など	https://www.npa.go.jp/policy_area/nokuso_cp/statistics/
8	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/

9	(財) インターネット協会 (インターネットホットライン連絡協議会)	○相談窓口の紹介、各種対策など ○名誉棄損/誹謗中傷トラブルの種類と対策、相談事例等を紹介	https://www.iajapan.org/hotline/consult/index.html
10	違法・有害情報相談センター	○ネット利用者用の FAQ ○サービス提供者用・運営者用の FAQ	https://ihaho.jp/faq/index.html
11	インターネット・ホットラインセンター (参考サイト)	○各種参考サイトのリンク集 ○架空請求、迷惑メール、人権侵害、知的財産権侵害等の通報相談窓口、参考サイトの紹介	https://www.internethotline.jp/pages/link/index
12	国民生活センター	○相談事例 ○身近な消費者トラブル Q&A ○土曜、日曜に利用できる相談窓口の紹介など	http://www.kokusen.go.jp/

ウ ボランティア活動の要点

	参考サイト名等	参考となる内容	アドレス
13	警察庁 (自主防犯ボランティア活動支援サイト)	○自主防犯ボランティア活動の状況、活動事例等 ○全国都道府県による防犯活動支援情報の URL ○活動事例の紹介、Q&A など	https://www.npa.go.jp/safetylife/seianki55/
14	警察庁サイバー犯罪対策 (平成 22 年度総合セキュリティ対策会議)	○「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」の報告書内「第 3 章 サイバー防犯ボランティア育成」	https://www.npa.go.jp/cyber/csmeeting/h22/pdf/pdf22.pdf
15	(社福) 全国社会福祉協議会 (地域福祉・ボランティア情報ネットワーク)	○ボランティア活動とは ○多様なボランティア・市民活動の例 ○ボランティア・市民活動で知っておきたい 5 つのポイント ○私のボランティア体験	https://www.zcwvc.net/volunteer/beginner.html

(2) 基礎知識

インターネットの仕組みや広く一般に利用される各種コンテンツの仕組み、利用方法を理解させるとともに、関係法令や官民連携した違法・有害情報対策を理解させ、ボランティア活動上必要とされる基礎知識を習得させるための資料です。

ア インターネットの基礎用語、インターネットの仕組み、各種コンテンツの仕組み、利用方法

	参考サイト名等	参考となる内容	アドレス
16	警察庁 (@police)	○インターネット情勢 ○デジタル・フォレンジック ○不正プログラムなど	https://www.npa.go.jp/cyberpolice/

17	総務省(国民のための情報セキュリティサイト)	<ul style="list-style-type: none"> ○安心してインターネットを使うための基礎的な情報 ○基礎知識(インターネットを使ったサービス) ○一般利用者の対策 ○企業・組織の対策 	https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/
18	(財)インターネット協会(インターネットルール&マナー検定)	<ul style="list-style-type: none"> ○インターネットを利用するためのルールやマナーの評価測定(無料) 	https://rm.iajapan.org/

イ インターネット・ホットラインセンター(IHC)が取り扱う違法情報

	参考サイト名等	参考となる内容	アドレス
19	インターネット・ホットラインセンター(違法情報)	<ul style="list-style-type: none"> ○一般から通報を受けた違法情報の警察への通報、プロバイダ等への削除依頼を実施(違法情報13種類の解説) 	https://www.internethotline.jp/pages/guideline/ihou

ウ 関係法令

	参考サイト名等	参考となる内容	アドレス
20	内閣府(インターネット利用環境整備)	<ul style="list-style-type: none"> ○青少年のインターネット利用環境実態調査を紹介、青少年インターネット環境整備法の説明等 	https://www8.cao.go.jp/youth/kankyouu/index.html
21	NISC(内閣サイバーセキュリティセンター)	<ul style="list-style-type: none"> ○サイバーセキュリティ基本法 ○サイバーセキュリティ戦略 	https://www.nisc.go.jp/index.html
22	警察庁(なくそう、子供の性被害)	<ul style="list-style-type: none"> ○出会い系サイト規制法の解説など 	https://www.npa.go.jp/policy_area/no_cp/deai/
23	文部科学省(学校ネットパトロールに関する取組事例・資料集(教育委員会等向け)資料編第1章(第5節))	<ul style="list-style-type: none"> ○青少年インターネット環境整備法、出会い系サイト規制法、プロバイダ責任制限法、不正アクセス禁止法などの解説 	https://www.mext.go.jp/b_menu/shingi/chousa/shotou/081_1/houkoku/1325771.htm (学校ネットパトロールに関する取組事例・資料集一覧内の資料編第1章(第3節)～(第5節)のPDFを選択)
24	経済産業省(電子消費者契約法の逐条解説)	<ul style="list-style-type: none"> ○電子消費者契約及び電子承諾通知に関する民法の特例に関する法律についての逐条解説 	https://www.meti.go.jp/policy/it_policy/ec/e11225bj.pdf
25	プロバイダ責任制限法関連情報webサイト	<ul style="list-style-type: none"> ○プロバイダ責任制限法の解説、送信防止手続きなど 	http://www.isplaw.jp/

エ 違法・有害情報対策

	参考サイト名等	参考となる内容	アドレス
26	警察庁(サイバー犯罪対策)	○警察庁、各都道府県警における取組・施策等を紹介 ○各都道府県警へのリンク ○官民ボードなど	https://www.npa.go.jp/cyber/index.html
27	官民ボード(ここからセキュリティ!)	○不正アクセス防止対策に関する官民意見集約委員会(官民ボード)が構築した情報セキュリティサイトで、警察庁等の統計情報などを含むセキュリティ関連コンテンツを多数紹介 (1)ア2を再掲)	https://www.ipa.go.jp/security/kokokara/

(3) 活動要領

サイバー防犯ボランティアに期待される各種活動につき、活動重点、活動要領及び活動上の留意事項等を理解させるとともに、安全かつ安心して活動を継続させるために必要な知識と技能を習得させるための資料です。

ア 教育活動

講習素材の収集、講習の内容及び方法の選定、活動上の留意事項

	参考サイト名等	参考となる内容	アドレス
28	文部科学省(情報モラル教育の充実)	○情報モラル教育の児童生徒向け啓発資料、教員向けの指導手引き、保護者向けの動画教材スライドなど	https://www.mext.go.jp/a_menu/shotou/zyouhou/detail/1369617.htm
29	文部科学省(「ネット上のいじめ」に関する対応マニュアル)	○ネット上のいじめについて、特徴、事例、対応要領を紹介	https://www.mext.go.jp/b_menu/houdou/20/11/08111701/001.pdf
30	(財) インターネット協会「フィルタリングを知っていますか」	○フィルタリングを知ってもらうためのページ。日本のフィルタリングソフト等を紹介	https://www.iajapan.org/filtering/
31	(一社) インターネットユーザー協会	○青少年に対するネットリテラシー教育のための読本「ネットと上手く付き合うためにVer1.1」を公開	https://miau.jp/ja/l10
32	(社) 電気通信事業者協会	○携帯電話契約者数の公開、青少年の携帯電話利用・スマートフォン利用についてなど	https://www.tca.or.jp/
33	安心ネットづくり促進協議会	○青少年のスマホ利用のリスクと対策 ○青少年の安心安全なインターネット利用など	https://www.good-net.jp/

34	e-ネットキャラバン (資料ダウンロード、 参考資料リンク集)	○小中学生向けの基本的な講話 内容のテキスト紹介 ○保護者・教職員向けのテキスト 紹介	https://www.fmmc.or.jp/e-netcaravan/news/download.html
----	---------------------------------------	--	---

(注) 前記「(2)基礎知識」に挙げた資料も講習素材として活用しましょう。

イ インターネット空間の浄化活動 (サイバーパトロール)

情報収集のポイント、違法情報等の発見時の措置、活動上の留意事項

	参考サイト名等	参考となる内容	アドレス
35	文部科学省(学校ネットパトロールに関する取組事例)	○学校ネットパトロールに関して、実際の取組事例等を紹介	https://www.mext.go.jp/b_menu/shingi/chousa/shotou/081_1/houkoku/1325771.htm
36	埼玉県教育委員会(ネット上の見守り活動の手引)	○ネットパトロールの実際 ○ネットパトロールの検索方法 ○発見時の措置 ○インターネット上の隠語など	https://www.pref.saitama.lg.jp/documents/26963/467571.pdf

(4) その他

ボランティア活動を実施していく上で、関係機関・団体等との連携の必要性を理解させるとともに、ボランティアを組織化し、安全に活動するための知識や心得を習得するための資料です。

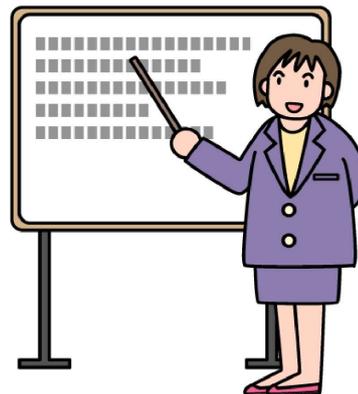
	参考サイト名等	参考となる内容	アドレス
37	警察庁(自主防犯ボランティア活動支援サイト)	○自主防犯ボランティア活動の状況、活動事例等 ○全国都道府県による防犯活動支援情報のURL ○活動事例の紹介、Q&A など (1)ウ13を再掲)	https://www.npa.go.jp/safetylife/seianki55/
38	警察庁(サイバー防犯ボランティア活動マニュアル)	○既存団体からのアンケートなどを基にして、サイバー防犯ボランティアの基礎を集約したマニュアル	https://www.npa.go.jp/cyber/policy/index.html
39	総務省(国民のための情報セキュリティサイト)	○情報セキュリティ初心者のための三原則を紹介	https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/intro/beginner/index.html
40	IPA(独立行政法人情報処理推進機構)	○ウイルス・不正アクセスの届出、対策のしおり、年毎の10大脅威、注意喚起など (1)ア3を再掲)	https://www.ipa.go.jp/security/
41	IPA(独立行政法人情報処理推進機構)	○スマートフォンを安全に使用するための六箇条を紹介	https://www.ipa.go.jp/security/txt/2011/08outline.html

42	(財) インターネット協会 (インターネットルール&マナー検定)	○インターネットを利用するためのルールやマナーの評価測定 (無料) (2)ア 18 を再掲)	https://rm.iajapan.org/
----	----------------------------------	---	---

(注) 上記のほか、既存のサイバー防犯ボランティア団体がホームページを立ち上げて活動状況を公開している場合があります。

3 サイバー防犯ボランティア団体による実践例

既に活動を行っているサイバー防犯ボランティア団体が、新しいボランティアに対して、ボランティア活動を始める前に実践している育成カリキュラムの例をご紹介します。



(1) KC3 (熊本県の大学生サイバー防犯ボランティア) の例

内容		回数
1	新しいボランティアメンバーに対する KC3 の活動内容紹介	1 回
2	ウェブサイトのサイバーパトロール方法の説明	1 回
3	講話の実施方法の説明	1 回
4	サイバー防犯ボランティア活動についての留意点の説明	1 回
5	既ボランティアメンバーによる、新しいボランティアメンバーが実施する講話のサポート(見取り稽古)	1 回

(2) 神奈川少年補導員連絡協議会の例

内容		時間
◆養成講座 1 日目		
1	子供たちの周りのインターネット機器	0.5 時間
2	インターネットのメディア特性	0.5 時間
3	子供のインターネット利用の問題点	0.5 時間
4	子供の遊び場としての危険性	0.5 時間
5	ペアレンタルコントロールとは何か	0.5 時間
6	フィルタリングの方法と問題点	0.5 時間
7	子供の利用しているサイトの実例 (演習)	1 時間

◆養成講座 2 日目		
1	1 日目の復習	0.5 時間
2	既存 NPO の活動事例	0.5 時間
3	確認テスト	1 時間
4	ネット利用に必要な「3 つの力」	0.5 時間
5	啓発活動における留意点	1 時間
6	修了証交付式	0.5 時間

(3) ロックモンキーズ（京都府の大学生ボランティア団体）の例

内容		時間
1	団体活動紹介 ○DVD 上映 ○既存メンバー紹介	1 時間
2	「犯罪機会論」講義・防犯ボランティア活動の留意点 ○安全・安心なまちづくりの基本的な考え方 ○自主防犯活動の進め方 ○犯罪に強い三つの要素（領域性・監視性・抵抗性） ○犯罪が起りやすい場所・起りにくい場所の具体的説明	1 時間
3	特別講座 ○サイバー犯罪対策について ○サイバー防犯ボランティアの活動について	2 時間
4	フィールドワーク ○午前中の講義内容を踏まえ、実際に町並みを見て歩き、犯罪が起りやすい場所・起りにくい場所を学生達に考えさせる	2 時間
5	地域安全ニュースの作成 ○地域安全ニュースを作成させ、学生や地域住民への情報伝達を学ばせる	2 時間

(注) ロックモンキーズは、サイバー防犯ボランティアのほか、地域の見回り活動を実施する自主防犯ボランティア活動も行っています。

4 インターネット基本用語集

○アカウント

コンピュータ用語でのアカウントは、ユーザーがネットワークやコンピュータなどにログインするための権利のこと。例えば、SNS にログインするため、電子メールを送受信するためのアカウントなどがある。アカウント(ID)には、パスワードが関連付けられており、利用者はアカウントと併せてパスワードを入力することにより、ログインする権利を認められたネットワークやコンピュータにログインすることができる。

○アバター

プロフィールや SNS の中で、自分の分身となるキャラクターのこと。髪型、洋服、アクセサリなどのアイテムを選ぶことで、オリジナルのアバターを作成し楽しむことができる。

匿名でプロフィールや SNS を行う場合に顔写真の代わりにアバターを表示することが多い。

○アプリ

アプリケーションソフトウェアの略。パソコンに年賀状作成アプリや、スマートフォンに地図アプリなどをインストールし、機能を拡張・カスタマイズして使うことができる。インターネットから不正なアプリをダウンロードすると、機器がウイルスに感染するなどのリスクがある。

○インターネットリテラシー

インターネットを正しく使いこなす基本的な能力を指す言葉。青少年が身に付けるべきリテラシーには、違法コンテンツ・有害コンテンツに適切に対処できる能力、ネット上で適切にコミュニケーションができる能力、プライバシー保護や適切なセキュリティ対策ができる能力などがあげられる。

○学校裏サイト

学校の生徒または卒業生が、学校による公式サイトとは別に立ち上げた非公式のサイト。生徒同士の交流や行事・テストなどの情報交換などに使われるのが主な目的だが、誹謗(ひぼう)・中傷の書き込みや個人情報の流布、裏サイト内でのいじめなどが問題となっている。現在では携帯電話でのアクセスが主流。サイト名に正確な学校名を表記していないものも多く、サイトの発見が難しい。

○ガラケー

ガラケーとは、ガラパゴスケータイの略で従来型携帯電話のこと。世界標準とは異なる独自の進化をした日本の携帯電話のことをガラパゴス諸島に例えている。また、ガラケーとは別に、従来型携帯電話のことをフィーチャーフォンと呼ぶ場合もある。

○個体識別番号

一台一台の携帯電話に割り振られる重複しない識別番号のこと。携帯電話でインターネットに接続する際は相手のサーバーに個体識別番号が送信される。

○コンピュータウイルス

他人のコンピュータに入り込んで悪さをするプログラム。画面表示をでたらめにしたり、パソコンのハードディスクに保存されているファイルを破壊したりする。

ウイルスはインターネットからダウンロードしたファイルなどを通じて感染する。大抵はユーザーの知らないうちに感染する場合が多い。またウイルスに感染したことに気づかずにコンピュータを使用し続けると、ネットワークを介して他のコンピュータにウイルスを移す危険性もある。

○スマートフォン

インターネットとの親和性が高く、パソコンの機能をベースとして作られた多機能携帯電話のこと。「スマフォ」、「スマホ」と略されることもある。

一般的なスマートフォンの持つ代表的な機能としては、タッチパネルによる操作、無線LAN(Wi-Fi)によるネット接続、ダウンロードによるアプリケーションの追加などがあげられる。

○チェーンメール

チェーンメールとは、転送を呼びかけ、次々と鎖のように連鎖していくメールのこと。チェーンメールは転送されることを目的としているため、受信者の恐怖心をあおるホラーな内容や幸せになれるおまじないなど、善悪様々な種類の内容で転送させようとする。

○デジタルネイティブ

生まれた時からインターネットやパソコン、携帯電話が空気や水のように、あたりまえにある生活環境の中で育ってきた世代のことを指す。

○ネット依存

日常生活に干渉を及ぼす程度の、インターネットや携帯電話への過剰に依存した状態を指す。インターネットやメールに熱中するあまり、それを離れると孤独感や絶望感にさいなまれ、睡眠障害や生活リズムの崩れなどの症状に陥る状態。

○フィッシング

フィッシング(Phishing)とは、金融機関(銀行やクレジットカード会社)などを装った電子メールを送り、住所、氏名、銀行口座番号、クレジットカード番号などの個人情報を騙し取る行為。電子メールのリンクから偽サイト(フィッシングサイト)に誘導し、そこで個人情報を入力させる手口が一般的に使われている。

○フィルタリング

利用者の意思によって、インターネット上の青少年にとって有害なウェブ情報へのアクセスを自動的に遮断することができる技術的手段で、有害サイトブロック、ウェブフィルタリングなどとも呼ばれる。

○不正アクセス

あるコンピュータやサービスに、本来のアクセス権を持たない人が、ソフトウェアの不

具合などを悪用してアクセス権を取得し、不正にコンピュータを利用する、あるいは試みること。不正アクセス事例として、オンラインゲーム上などで、他人のユーザーIDとパスワードでなりすましてログインし、他人のキャラクターのアバターやアイテムを自分のキャラクターに移し替えたために、不正アクセス禁止法違反で検挙・補導されたケースがある。

○プロフィール

プロフィールサイトの略。インターネット上で自分のプロフィール（自己紹介）を作成して公開するサービス。入力フォームに名前やニックネーム、趣味などを入力することで簡単に自己紹介ページを作成することができる。オンライン上に自己紹介サイトを設置するという特性から、不特定多数に自分自身の情報を発信してコミュニケーションの輪を広げていくという使い方もでき、ゲストブック（通称ゲスブ）で訪問者からコメントを受け付けることもできる。

○ブログ

ブログとはウェブログ（weblog）を省略した言葉で、日付入りの記事ページを中心としたウェブサイトのこと。ブログでは、文章を入力するだけで簡単にページを作ることができるツールやサービスが充実しているため多くの人がブログを作成、公開している。

○ペアレンタルコントロール

DVD やインターネット、携帯電話などの電子メディアにおいて、性的表現や暴力的表現など青少年に悪影響を及ぼす可能性のあるサービスやコンテンツに対して、保護者が視聴・利用制限をかけること。また、そのための装置やソフトウェアの機能のこと。パスワードによる視聴制限やフィルタリングサービスなどが代表的なものとしてあげられる。

○迷惑メール

受け取る人の意思に関わらず、勝手に送りつけられてくるメールのことを総称して「迷惑メール」と呼ぶ。迷惑メールの種類には、「フィッシングメール」、「広告宣伝メール」、「架空請求メール」などがある。

○ワンクリック詐欺

迷惑メールに記載されたリンク先やアダルトサイト上の画像などをクリックすると、突然入会登録などの表示が現れ、法外な利用料金が請求される。画面には、振り込まなければ勤務先や自宅に直接請求しに行くなどの脅し文句もあわせて表示される場合もある。

○IP アドレス

インターネットに接続されたパソコンや機器の1台1台に割り振られた識別番号。世界中のインターネット上でこの番号に重複があってはならない。例えば「8.8.8.8」のように表記されている。

○SNS

ソーシャルネットワーキングサービスの略。友人・知人間のコミュニケーションを円滑にする手段や場を提供したり、趣味や嗜好、居住地域、出身校、あるいは「友人の友人」

といったつながりを通じて新たな人間関係を構築する場を提供する会員制のコミュニティ型ウェブサービスのこと。代表的なサービスに、LINE（ライン）、Twitter（ツイッター）、Facebook（フェイスブック）、Instagram（インスタグラム）などがあげられる。

○Wi-Fi 接続

パソコン、スマートフォン、ゲーム機などを、携帯電話会社の電波を使わずにアクセスポイントを経由し、インターネットへ無線 LAN 接続することを指す。Wi-Fi とは本来は無線 LAN 接続の仕様を指す用語だが、Wi-Fi 接続と無線 LAN 接続を同義に使うことが多い。最近では顧客サービスの一環として駅のホームやファーストフード店などで無料の Wi-Fi 接続用アクセスポイントが設置されている。