学 校 現 場 の た め の

サイバーセキュリティ必携

広島県教育委員会

広島県警察本部

平成３０年１０月

は じ め に

近年，ICT（Information and Communication Technology：情報通信技術）は急速に進展し，「いつでも，どこでも，何でも，誰でも」手軽にインターネットが利用できる社会となりました。

学校においても，従来の方法・技術ではできなかった指導や幅広い情報の収集，学習活動の発信・交換などが可能になるなど，ＩＣＴの利点を生かした教育活動を行うことで，子ども達の主体的な学習活動の促進や興味・関心の広がりなどの恩恵を受けています。

一方，子ども達にスマートフォン等が普及したことで，様々な情報が子ども達に直接届いてしまうため，保護者が使用方法を適切に管理しなければ，子ども達は有益な情報以外に，インターネット上で氾濫している違法な情報や有害な情報に接してしまうおそれがあります。

また，SNS（ソーシャル・ネットワーキング・サービス）をはじめとした，コミュニケーションツールは，子ども達に様々な事態が発生しているにも関わらず，発生した事態を保護者や学校が認識できない状態を加速させています。

その結果，子ども達が知らない人と安易に繋がってしまう，あるいは現実世界で言わないこと，やらないこともネット上ではハードルが下がってしまうことで，気がついたときには子ども達が犯罪に巻き込まれたり，犯罪の加害者になっているという深刻な事態も発生しています。

この資料は，インターネットのトラブルなどについて，教職員や保護者に理解していただけるように，インターネット環境をめぐる情勢やスマートフォンの適切な取扱，事案への対応要領等について作成したものです。

皆様には，この資料を参考にして，子ども達がICT社会と適切な関わりを身につけることができるよう，指導にお役立てください。

平成３０年１０月

広島県教育委員会（豊かな心育成課）

広島県警察本部（サイバー犯罪対策課）

もくじ

第1章　総論

サイバー空間に接続？するデジタルネイティブ世代

デジタルネイティブ：生まれた時代に既に十分にインターネットが普及しており，現実の世界とデジタルの世界を垣根無く使いこなせる世代をいう。

サイバー空間　　：本書においてはインターネット空間と同義とする。多様なサービスやコミュニティが形成されており，既に社会生活の場ととらえられている。

　生まれた時からサイバー空間が存在し，スマートフォンを通じて自らが自然にネット接続しているデジタルネイティブとそれ以外の世代では，サイバー空間に接する感覚が全く異なります。SNSの利用によるトラブル等の原因は，この辺りにあるのかもしれません。

サイバー空間は人の思考方法を変える

新しい世界

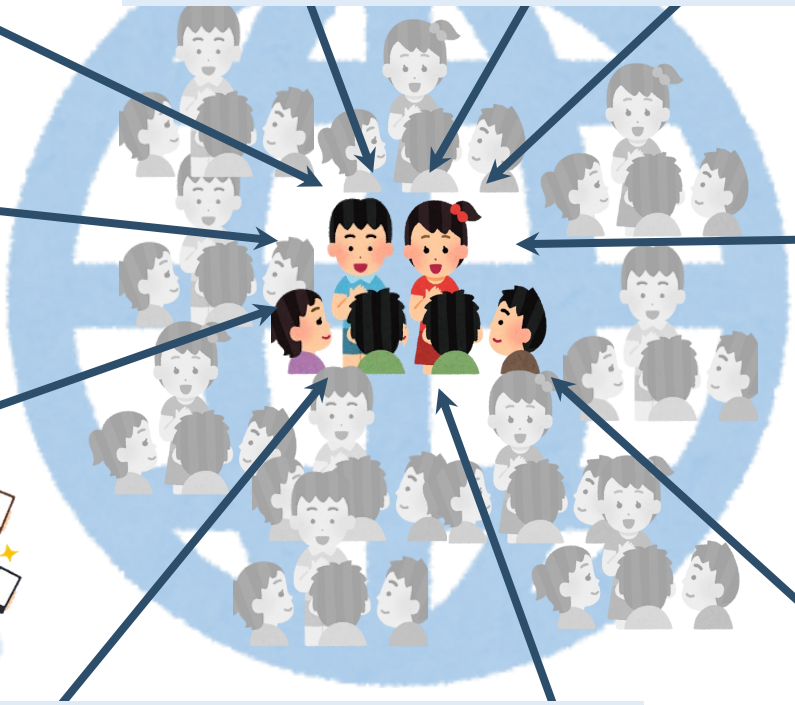
1 「便利な道具」程度の認識では 理解は難しい!

常時だれかと意識が繋がっている世界

- 時間と距離の概念がない世界

あらゆる知識や記憶が共有される世界

- 自分で考えなくても誰かの知識を借りれば事足りる，また覚えなくても検索すれば足りる世界



制約が少なく自由に振舞える世界

- 法律や社会インフラが十分整っていない世界
- 成人，未成年にかかわらず，自己責任が原則

- デジタルネイティブにとって，サイバー空間と現実は一体のもの。これまでとは感覚のズレがトラブルにつながる。

2 大開拓時代

©NISC 内閣サイバーセキュリティセンター National center of Incident readiness and Strategy for Cybersecurity

https://www.kantei.go.jp/jp/froms/nisc_option.html 2018/03/1

インターネットというのは今の40歳代の大人から考えると「便利な道具」であり、現実世界をサポートする存在といったイメージでしょう。それは逆に今のようにネットが無かった「不便な時代」を知っているから比較ができるからでもあります。

しかし生まれたときからインターネットが存在している環境で育った子ども達は、現実世界とインターネットの中の世界を、区別すること無く一体として感じている場合もあります。

たとえばネットへの接続が高速化して、ものを思い出すのとさほど変わらないスピードで、スマホ等の情報端末から目的の情報を引き出させるようになって、「いつでもネットから引き出せる情報」を、「少し思い出すのに時間がかかる記憶」ぐらいのようにあつかい、あまり脳に記憶することにこだわらないようになっている。そんな風に感じる事はありませんか？機器が進化して考えれば答えが分かるようになれば、その「区別」すら感じなくなるかもしれません。また現物の紙や本の形では無い、ネット上のファイルやデータの受け渡しは、もはや「渡す」という概念ですらなく、自分のスマホの中の誰とでも共有できる保存場所（実はクラウドサーバ）があり、「どこからでも呼び出せ、皆がリアルタイムで共有できるもの」といった感じで、もはや現実世界に軸足をおいた人々には感覚的にわからない、次元を超えた情報の管理、というよりは意識の共有とでもいう状態になっている話をときおり聞きます。

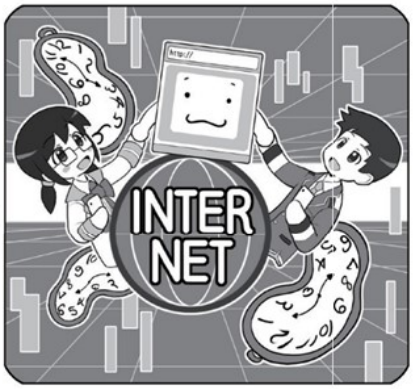
ただ、そういったネットのメリットの部分はものすごいスピードで進化していますが、インターネットの世界はまだ生まれてから年数 が経っていないため、興味を引きやすい通信や情報共有以外、とくに安全を守る社会システムや秩序構築等のインフラは充分に確立されていません。

実は秩序に関してはネットが生まれたごく初期に、現実世界から積極的にネットに移民してきた開拓意識が旺盛な「ネチズン」と呼ばれた人々により、文章化されていない暗黙のモラルとして存在してた事もありました。

ネットは現実世界のオプションではない

インターネットの中の世界を、現実世界のオプションや便利な道具と捉える人もいますが、実際はそれに留まらない存在です。それは人間の思考の方法を変えます。

ネットは距離と時間の概念がない世界

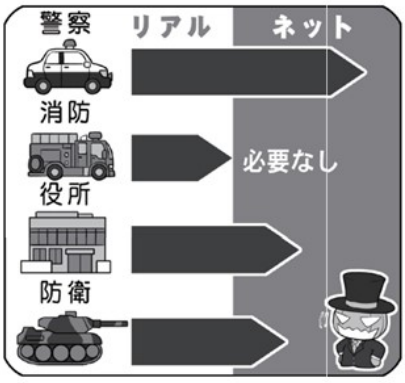


ネットには移動という概念がなく，またそれによって消費されていた時間が必要でなくなる新しい世界です。子ども達はこれを単なる世界の概念とし て自然に捉えています。

新しい世界は昔の開拓時代と同じ

人が先に進出して、社会のシステムや秩序の構築が間に合わない状態では「力こそ正義」となりがちです。ある意味「生きぬく能力がない人には危険な世界」といえます。

現実世界と同じ「社会インフラ」がまだ整っていない



ネットの世界には消防は必要ありませんが、その他のインフラは必要です。サイバー警察、電子政府、サイバー防衛等次第に整いつつあります。しか し国民全体の協力が必要です。

しかしその後、様々な人がネットに移り住んできたことによりネットは多様性を帯び、その人達を含んだ新たな秩序の構築が間に合わない中、現在に至ります。さらにネットの暗部では「強いやつが奪い、奪われるヤツが悪い」という、力こそ正義の、開拓時代風の雰囲気すらあります。

ネットが本当の意味でみんなが安心して使えるようになるには、ネットに必要が無い消防はのぞき、警察や役所、場合によっては防衛等の秩序を作るシステムが対応しなければならず、それにはまだしばらく時間がかかります。

それでも秩序が形作られる片鱗は見えつつあります。

警察組織等は、インターネットの匿名性を悪用して犯罪を行う攻撃者を、地道な努力と解析で追跡し、特定するための技術を磨きつつあります。

私達が現実世界の住人であり、完全にはネットの中だけで生きていくことができない以上、ネットの闇に隠れても、攻撃者が人であれば、現実世界でのその痕跡を完全に消すことはできないのです。

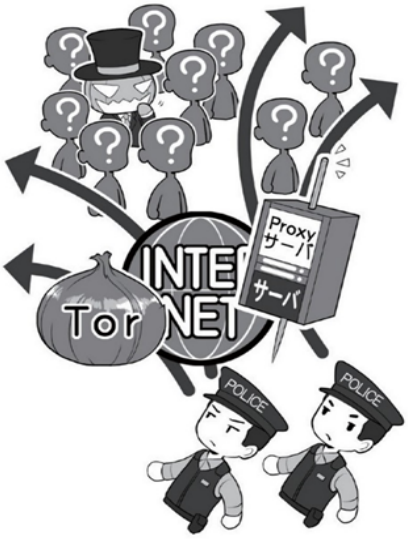
しかしそういった公的な能力の向上とともに大切なのは,ネットを利用する全ての人達が、ネットを守ろうという意識を共有し、協力しあうことです。

現実世界の秩序が、警察だけでなく国民一人ひとりの防犯意識や啓発活動で成り立っているように、会社や学校、友だちの間や、あるいはご両親と子どもさんの間で、どうやったらネットの世界を良くしていけるか、そのためにはなにができるのかを考えることで、初めて「社会全体として情報セキュリティを向上させる」というベクトルを持つことができるのです。ネット上の社会インフラの構築と皆のセキュリティ意識の向上、それは車の両輪であり、いずれかが欠けてしまっても、安全なネットは成り立ちません。

そうしてネットが安全な「社会」になることができたとき、子ども達はもっとネットの世界とともに進化し、より自由な発想で、新しい才能を開花させることができるようになるのでしょう。

そのためにも、ぜひ皆さん一人ひとりが、それぞれの立場でネットの世界のセキュリティを守る知識をもち、これを行う人になってほしいと思います。

匿名の通信は 追跡が困難だが…



ネットでは意図的に正体を隠す環境を作って犯罪が行う者達　がいます。匿名化するネットや　身代わりサーバの利用等です。

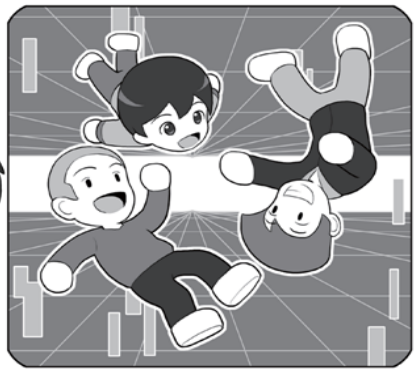
それでも徐々に技術は向上

最近では「バレないと思った」という犯人が捕まったり、ネットの闇に隠れる攻撃者を追跡する能力が向上しつつあります。

取り締まりは大切だがモラル醸成も大事

犯罪を起こしたら、きちんと検挙することは抑止力になります。しかし、皆がセキュリティを守ろうという意識を醸成することも大切です。

デジタルネイティブの子ども達に安全な世界を



デジタルネイティブの子達が 犯罪に巻き込まれず、ネットの世界で才能を開花させられるように、サイバー空間の安全を守らなければなりません。

3 デジタルネイティブと未来

©NISC 内閣サイバーセキュリティセンター National center of Incident readiness and Strategy for Cybersecurity

パーソナルなコンピュータの歴史が始まってからまだ30年しか経っていないこともあり、世の中にはまだ「パソコン」や「ネットワーク」が存在しなかった時代を知る世代の人がたくさんいます。

これらの人々の一部は、世界にパソコンが生まれ、ネットワークが生まれ、やがて大規模なネットワーク化とインターネットの誕生により「距離と移動に必要な時間が消えた世界」が生まれたときに、その世界に未来を見ました。

やがてその先進的な開拓者達は、移民のように生活の軸足を新たな世界に移し「デジタルイミグラント（デジタル移民）」と呼ばれるようになりました。

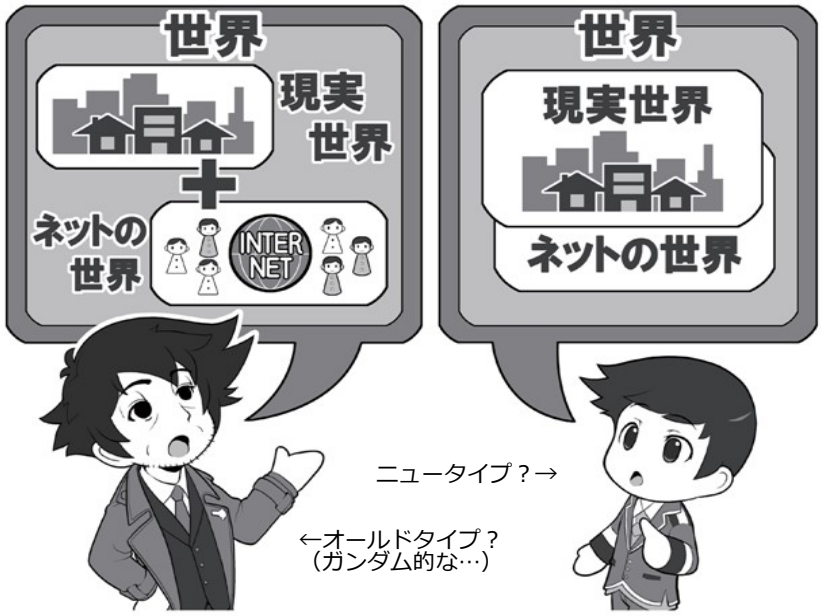
これは現実世界にたとえるならば、旧世界に息苦しさを感じていた人間が、誰も住んでいない新大陸を発見し、夢を描いてそこに移住し、新世界を築き始めたようなものです。

しかしインターネットが一般化したWindows95から20年、初代スマートフォンと呼べる存在であるiPhoneが誕生から10年の時が過ぎると、多くの人々がその世界に移住してきましたし、「距離と移動に必要な時間が消えた世界」にも子ども達が生まれ、ネットを無意識に使いこなす「デジタルネイティブ」と呼ばれる世代が形成されるようになってきました。

そういった世代が社会の中心となると、いままで距離と時間の概念によって形成されていた世界の国の人達との意識の壁が，技術に力とともにあっけなく解決されていくかもしれません。

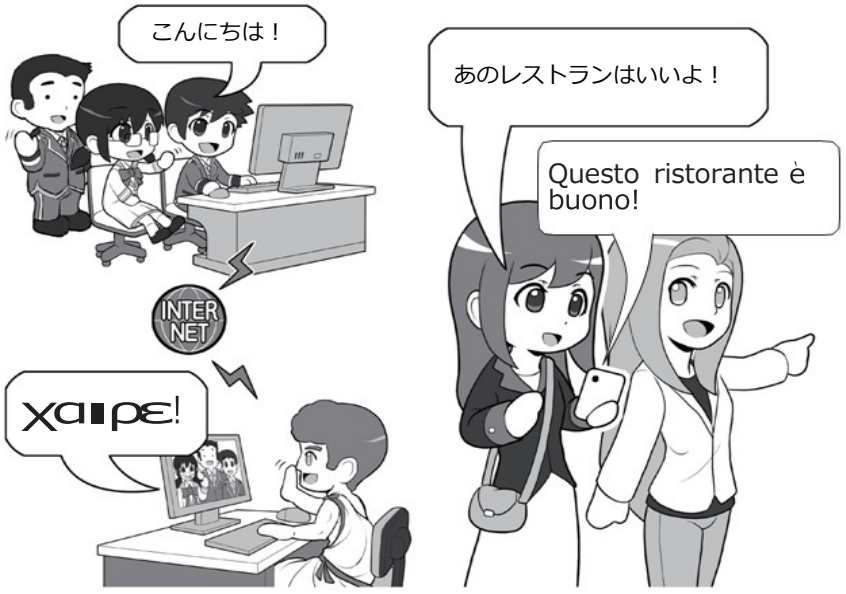
海外で生まれた子ども達が多言語をネイティブのように操り、様々な国の考え方を当然のように理解するように、すべてを楽々と越えていくかもしれません。

デジタルネイティブとデジタルイミグラント



デジタルイミグラントは、手紙に対するメールのように、ネットの世界を現実世界のオプションとして捉えて「便利になった」と考えますが、デジタルネイティブには現実とネットの世界は一体であり、「距離と移動に必要な時間が消費されない」コミュニケーションを、当たり前と捉えています。

技術の進化で文化の壁をあっさりと乗り越えていくかも



自動翻訳つきテレビ電話は、すでに一部の言語で始まっています。スマホの翻訳アプリでは、発音した言葉を翻訳してしゃべってくれます。言葉という壁、それに伴う意識の壁も、あっさりと壊される日がくるかもしれません。

4 バーチャル世界を超えて世界へ

デジタル機器の進化は、さらにネットと私達の融合を進めるかもしれません。

たとえば仮想の3次元空間を目の前に実現するバーチャルリアリティシステムは、驚くべき没入感をもち、まるで自分がその空間に存在しているかのように感じさせてくれます。

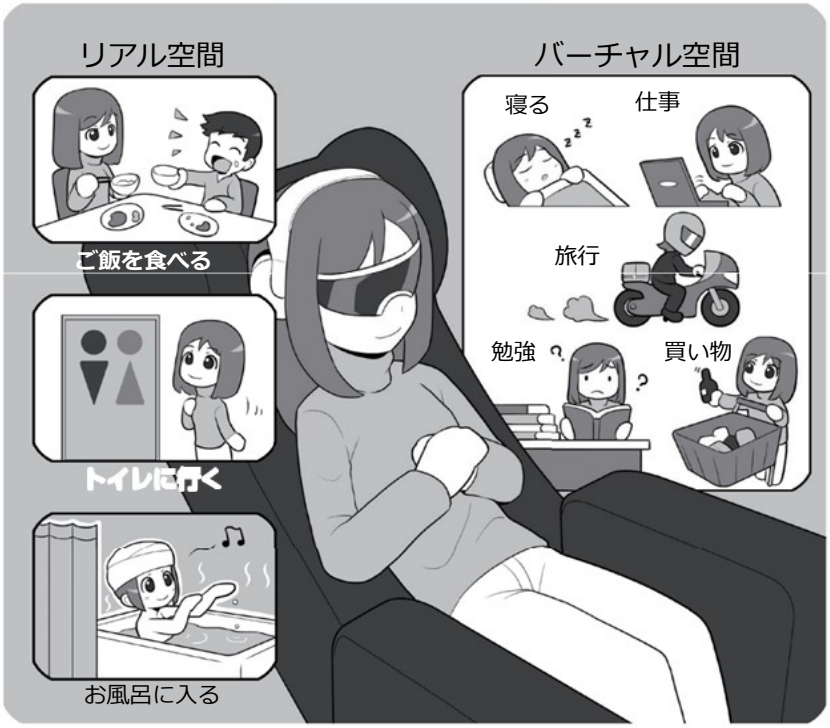
さらに仮想空間を使って生活することを前提に考えると、現実の世界でしかできないことは意外に少なく「ご飯を食べる」「おトイレに行く」「お風呂に入る」といった生理現象と清潔さに関するものだけになるかもしれません。

そんな世界が来るはずがないと思うかもしれませんが、実は私達は毎日「夢」で同じような経験をしています。夢の中の出来事を現実の出来事と混同してしまうことがあるように、「経験」とは必ずしも現実世界だけのものではなく、脳にとっては、どれも等しく同じ経験なのかもしれません。

そしてこういった技術がさらに進化を遂げれば、自分の部屋からネット経由でアクセスして、世界中の何処にでも「アバターのロボット」を操って現れ、実際にそこに訪れるのと同じように、世界の国々を旅してみたり、その国の人とコミュニケーションをしてみたり、あるいは学校で学ぶことができるようになるかもしれません。

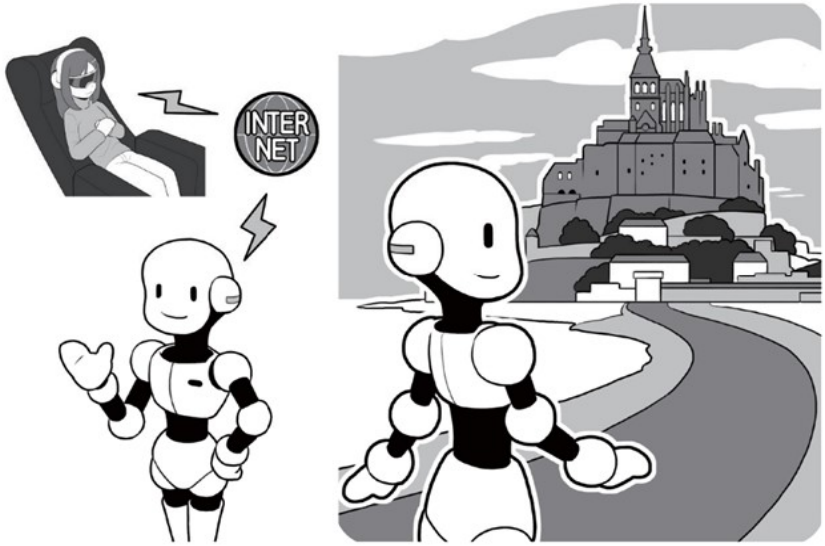
それは体が不自由な人、あるいは病気でベッドから起き上がれない人達にとっても、世界とつながることができるツールにもなるでしょうし、私達が世界の様々な国の人々との相互に理解しあうことにも役に立つでしょう。

リアルである必要は意外と少ない



ゲームに出てくるような素敵な空間で旅行したり、机を広げて仕事や勉強をしたり、お店があれば買い物をしたり等バーチャル空間で実現できることはたくさんあります。私達が夢の世界でやっていることも、現実世界ではないという意味では同じです。一方、ご飯やトイレ、お風呂はバーチャル空間ではできません。残念ながら 100% ネットに漕ぎ出すことはできません。

バーチャル空間だけでなく，ネットの向こうの現実世界に存在することも



何らかの事情でベッドから起き上がることができなくても、ネットを通じて「アバター（自分の代わりのロボット）」を使い、世界のどこかに現れて、様々なところに旅行することができるようになるかもしれません。

5 デジタルネイティブ　どんな傾向がある？

×　サイバー空間と現実世界の区別がつきにくい
全世界へ情報を発信しているという認識が薄い

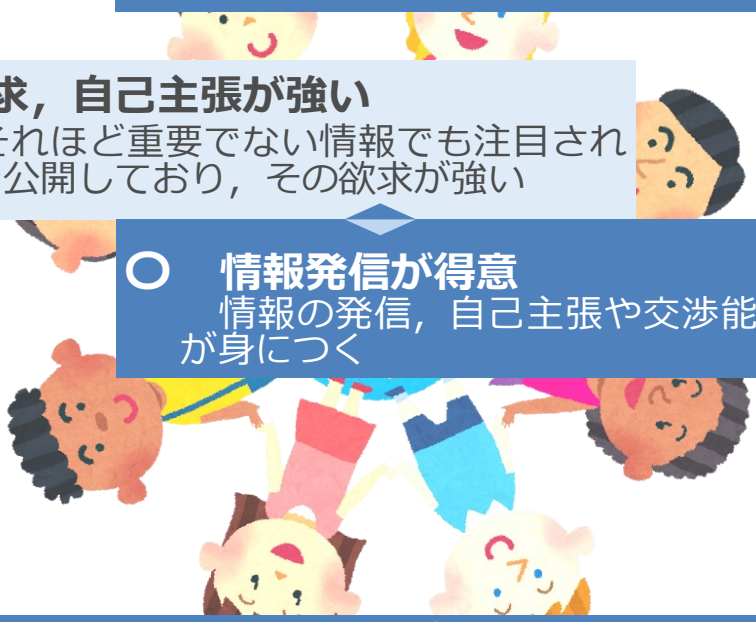
○　日常生活に自然にネットを取り込める
インターネットの恩恵を最大限享受できる

×　サイバー空間の情報をそのまま信じる
情報を軽く扱う また他人の情報の扱いが雑

○　自然に多くの情報に触れられる
知識量が豊富で，経験が不足していても知識で補える

×　注目への欲求，自己主張が強い
つぶやき等それほど重要でない情報でも注目されることを望んで公開しており，その欲求が強い

○　情報発信が得意
情報の発信，自己主張や交渉能力等，重要な能力が身につく



デジタルネイティブは，一般的に×印のような傾向があり，その傾向がトラブルを呼ぶことがあります。

しかし裏を返せば○印のような傾向でもあり，ネット時代では標準的な性格・能力と言えるでしょう。

デジタルネイティブがトラブルに至る原因の多くは，自分を客観視できないことにあります。これはデジタルネイティブだからということではなく，若年者ならだれでも持っている特質です。そして我々と同様，彼ら自身も客観視できるほどデジタルネイティブのことがわかっていないのです。

ネットリテラシー（ネットの読解力，倫理観）を醸成しトラブルに対処するには「トラブル自体の知識」とトラブルに近づかない「自己管理能力」を身に付ける必要があります。知識は教えればいいとして，自己管理するにはそもそも自分のことを理解していることが前提です。そのため指導に当たっては「物心ついてからずっとサイバー空間に触れている世代の君達は，こんな傾向がある。」とはっきり伝えることが必要です。

特別視しているのではありません。これからの子どもは皆デジタルネイティブなのですから。

6 サイバー空間の特徴と危険性

サイバー空間の特徴や一般的な危険性を列挙しました。サイバー空間への理解を深めてもらうため，ハッキングやネット詐欺等学校現場とは直接関係のない情報も取り上げています。

サイバー空間の問題点は非常にわかりづらいものですが，理解の一助になれば幸いです。

サイバー空間の脅威

サイバー空間の出来事は情報端末を通した範囲しか認識できず,危険な空間と言われても何がそうなのかよくわからないと思います。

例えば，「某国の原発がサイバー攻撃で破壊された」「某国はサイバー攻撃で数百億円を得た」「国内のインターネット端末のうち数十万台は検知できないコンピュータ・ウイルス（以下「ウイルス」という。）に感染していて，いつでも操れる」「国内企業のサイバー攻撃の被害総額は一千億円規模」・・・SFの世界の出来事のようですが，いずれも世界中の機関やセキュリティ企業が公表したもので，高い信ぴょう性があります。知らないだけで非常に危険な世界なのです。

また，このような縁遠い話でなくとも，例えば，ネットショップが偽物のサイトだった，ワンクリック詐欺の画面が表示された，フィッシングメールが来た，といったことを多くの人が経験していると思います。現実の店舗でのショッピングは詐欺に頻繁に遭う状況にはなく，サイバー空間がいかに無法地帯であるかを示しています。

さらに多くの学校で，SNSを介した生徒間のトラブルが絶えず，新たな少年問題となっています。

まずはサイバー空間の危険性に興味を持ちその危険性に目を向けることが，対策の第一歩です。

ウイルス対策

サイバー空間では，インターネットに接続されているコンピュータ端末を無差別に狙った「サイバー攻撃」で溢れかえっています。実際に攻撃を検知してみると，インターネット端末は，毎日何百回と，侵入を試みる攻撃にさらされることが分かります。皆さんのスマホや自宅のルーター，パソコンは，頻繁にサイバー攻撃されているという事実を認識して下さい。

インターネットの黎明期のサイバー攻撃者は，自分の技術力を誇示する愉快犯が中心でしたが，そのうち技術で金銭を得ようとする者が現れました。そのような攻撃者は当初，企業のサーバを直接狙っていたのですが，次には個人のインターネット端末をウイルスに感染させて数万台単位で操り，企業のサーバの攻撃に使用するようになりました。そして現在では，仮想通貨やネットバンキングを利用する個人のインターネット端末まで攻撃してウイルスを仕掛け，財産を直接狙う者まで現れています。

サイバー攻撃の方法は様々で，ネットワーク越しに侵入を試みるものや，Webサイトで他のファイルに偽装してウイルスに感染させようとするもの，あるいはWebサイトを閲覧しただけで感染するタイプのウイルスまであります。

コンピュータへの侵入やウイルスの感染を完全に防ぐことは不可能です。ですが放置したままインターネットを利用すると，確実にウイルスに感染することになります。このため少なくとも，

■ウイルス対策ソフトの導入

■OS(iOSやWindows等)とインストールしているソフトウェアの最新状態への更新

が必須です。

なにより，サイバーセキュリティに興味を持ってください。「よくわからんから放っとこう」と言っていると，突然預金残高が０になった，ということがあり得る時代です。

情報の信頼性

「ウソをウソと見抜けない人がインターネットを使いこなすのは難しい」と言われます。だれでも気軽に発言できるという性質上，サイバー空間上には錯誤に基づく情報や虚偽の情報が多数存在します。

情報の真偽，信頼性を見抜くのは容易ではありません。子ども達には，ウソの情報を流してはいけないということと，サイバー空間には虚偽の情報が多いため，必ず情報の真否を確認しなければならないということを指導すべきです。

リアルタイム性・広域性

インターネットの最も大きな特徴は，世界の数百億の機器が同じ規格で繋がっているという規模の大きさです。これは言語を超えた世界の統一規格であるということです。

またこのことは，日本のあるところで行われた出来事が，その数秒後には世界に拡散され得るということを意味します。

実行された行為は，場合によってはその瞬間に世界が知るところとなり，また取り消すことができないのです。

インターネットの規模はスマホの画面を見ているユーザーには実感しづらいことでしょうが，このことを踏まえていなければ安全に使うことができません。

匿名性

情報端末を利用した画面越しの交流では匿名性が高いように思えます。匿名の掲示板には，とても見ていられないような言葉が溢れています。

警察は捜査の過程で匿名性を破っていきます。普通にネットサービスを使用する上で完全に痕跡を残さず行えることはないのですが，特に子ども達はそのことに思いが至らないようです。

依存性

サイバー空間には膨大な量の情報で溢れていて，だれでも自由に拾って使うことができます。拾い続けても一杯になることはなく，終わりがありません。

現在，世界で最も活気に溢れているのはインターネット業界です。世界中の企業が顧客を離すまいと，魅力的なサービスを提供し続けています。

子ども達がその魅力に抗うのは難しいでしょうから，時間の制限等，使い方には大人が介入する必要があります。

知識の偏り

サイバー犯罪の加害者の傾向として，特定の情報には非常に詳しいのに常識的な物事を知らない，あるいは思い込みが非常に激しいということがあります。

ネット依存の激しい若年者について言えることですが，ネット上から情報を得ようとするとき，意向に沿わない情報，嫌いな情報を，わざわざ見ようとする人物は少ないということです。そのため，有用であっても気に入らない情報であれば，その情報に触れる機会が非常に少なくなります。

情報に影響を受けやすい子ども達には，意識して偏りがないように色々な情報に触れさせることが必要です。

自己責任

不特定多数の人が利用するサイバー空間は，成人，少年に関係なく利用者間の関係は対等になります。そのため少年であっても言動には責任が伴うこととなります。

他人を中傷したり，遊び半分に他人のゲームアイテムを盗んだりといった行動でトラブルになったり検挙されたりするのは，20代の若者が多いようです。短絡的な動機による事件でも，相手に向けた行為は非常に悪質，ということがよくあります。

SNSの使い方

学校現場では，SNS（ソーシャル・ネットワーキング・サービス）や掲示板サイトでの誹謗中傷に関する事案が大きな問題になっています。その学校だけでなく近隣の学校を巻き込んだもめ事に発展したり,この事が原因で被害者，加害者が家族ごと転居し転校を余儀なくされたりする等，社会問題にまでなっています。

把握が大変難しい上，一度発生してしまうと解決するのは非常に困難です。特効薬はなく，子ども達の自覚を促すしかありません。

ここで問題なのは「相手の表情が見えない」ということです。原因の多くは，相手の感情が分からない状態でやり取りすることで，言葉がエスカレートしてしまったり，誤解を生んでしまったりするといったことにあります。

相手の表情が見えないという特徴を押さえたうえで，相手の気持ちを推し量る，また自分の気持ちを推し量ってもらえるような分かりやすい書き込みをする，メッセージを送る，ということを教える必要があります。もめ事になってしまった場合には,SNSや掲示板サイトの利用を控えて，問題解決のためにも保護者に相談することを指導してください。

写真の公開とネットストーカー

インターネットの利用者の中には，他人の投稿内容を見てその内容を「炎上」させることが趣味のような人もいます。また投稿者の個人情報を特定して，社会生活にダメージを与えようとする者もいます。

このような人が個人の情報を特定する方法は様々あるが，多くはSNSサイトの記載内容から特定するようです。

また最近自分の写真をネットに公開することが流行していますが，写真は情報の宝庫です。顔写真は特に重要な個人情報ですので，インターネットに投稿して世界に晒すのは，十分注意が必要です。

なお，ネットで見つけた個人情報をネタにしつこく付きまといを行う人物のことを，ネットストーカーといいます。

デジタルタトゥーと就活

掲示板やSNS等に書込まれた情報は，知人等によって興味本位で，あるいは悪意をもって他人に晒すために転載されることがあり，このことによるトラブルが頻発しています。

一般的に，書き込んだ本人であればその内容を削除できる掲示板等がほとんどですが，転載等された情報は多くの場合，削除できません。こうして削除できない情報が，サイバー空間には大量に漂っています。

もしその書き込みの内容が「炎上」してしまえば，さらに拡散してしまいます。こういった個人情報は「デジタルタトゥー（電磁的な入れ墨）」と言われ，その個人を表す消えない情報として残ってしまいます。

最近では，企業として採用しようとする人物の経歴を把握するために，SNS等の書込みを調査するケースがあるそうです。悪い情報が残っていれば採用に影響があることも考えられます。人生の大事な時に，思わぬところでつまづかないよう，個人情報を安易に公開しないことが重要です。

セクストーション,リベンジポルノ

「セクストーション」とは，セックス（性的な）＋エクストーション（ゆすり）の造語です。手に入れた性的な写真等を使って相手をゆすることを言います。また別れた腹いせにそのような写真等を公開するような行為を「リベンジポルノ」と言います。写真が児童のものの場合,送らせた側だけでなく送った側も児童ポルノ製造等の犯罪に該当する可能性があります。またセクストーションによって凶悪な事件に発展した実例が多数あります。

交際が終わった後，相手がそれらの写真等を自ら消去することは期待してはいけません。また友人の間で面白半分にそれらを共有され，晒される可能性があります。

スマホの普及で，特に未成年者の間でこのことによるトラブルや検挙事例が激増しています。

パスワードの保護

インターネットサービスが普及し，ネットショッピングやSNSを使用する機会が増えています。その分，住所氏名等の個人情報，クレジット情報や物品の購入等の情報，さらにはメッセージや写真等，膨大な量の個人の情報が各サービスに記録されています。

これらはアカウント（利用権。**【P40　IT用語辞集No,1　「アカウント」】**）を取得して利用しており，パスワードによって守られています。しかしながらそのパスワードが悪意のある者に使われた場合，個人情報が全て知られてしまう，という危険を孕んでいます。

パスワードが知られてしまう状況は様々ですが，

- フィッシングサイトで入力してしまう
- 単純なパスワードで推測されてしまう

といったことが多いと思われます。また一つのパスワードを複数のインターネットサービスで使い回していると，どこか１カ所のサービスでパスワードが流出すると他でも同じように不正アクセスを許してしまう，ということがあります。

以下はパスワードを設定する際の留意事項です。

- ユーザーIDと同じ文字列や生年月日，「Password」や「12345678」といった単純なものや辞書に載っているような単語のパスワードを設定しない
- 長さは最低8文字で，大文字小文字のアルファベット，数字，記号を組み合わせる。
- 同じパスワードを使い回さない
- 何者かにパスワードを知られた恐れがある場合はすぐに変更し，運営会社に連絡する

また，特に子ども達の場合は，パスワードの管理を安易に考えがちで，友人等に教えて不正アクセスされるということがあります。

パスワードが大事なもので，他人に教えてはいけないと指導することが重要です。

フィッシング，詐欺メールの対策

個人情報を騙し取ることが目的の「フィッシング」や，架空の取り引きを装って金銭を騙し取ることが目的の「詐欺メール」の対策は，「相手にしない」「メール中のリンクをクリックしない」ということに尽きます。

「パスワードの変更」や「利用料金を払え」とのメールが来ても，相手には連絡せず，まずブラウザ（インターネット閲覧ソフト）を起動し，そこからそのサービスにアクセスしてログインしてください。もし本当にパスワードの変更や料金請求があるなら，メールと同じ内容がブラウザから確認できるはずです。

第2章　家庭編

スマートフォンの使用開始にあたって

保護者の方から，「いつごろからスマートフォンを持たせればいいか」「いつから持たせるか学校で決めて欲しい」といった相談を受けることがあるようです。

保護者がスマホを持たせると決めた場合に考慮すべきポイントを挙げます。いずれも使い始めてからでは効果が薄いので，スマホを持たせる前から考えておくことが重要です。

子ども達がスマートフォンを使い始めるにあたり指導すべきポイント

1 保護者と子どもの認識の違い

保護者	子ども
子どもとのコミュニケーションツール	子ども同士のコミュニケーションツール
子どもの状況把握，位置の把握	親の監視からの解放
緊急時の連絡手段	好奇心を満たす情報収集ツール

保護者が子どもにスマートフォンを持たせる理由と，子どもの考え方は全く違います。子どもにとっては新しいオモチャ感覚の道具でしかありません。

いつ子どもにスマートフォンを与えるか，保護者は悩ましいところでしょう。おそらく学年が上がるとき，あるいはプレゼントやご褒美に，という理由が多いのではないでしょうか。

保護者の多くはスマートフォンにトラブルがあることを，何となく聞いたことがあると思います。漠然とした不安はあるものの，具体的に何をしたらいいかわからない，といった心境ではないでしょうか。そこで「とりあえず渡しておいて，対策は後で考えよう」とスマートフォンを渡してしまうと，トラブルが生じた後でのリカバリーはなかなか大変です。

これからポイントを二つ上げますが，あらかじめ知っておくべき知識ですので是非活用してください。**ネットトラブルが確実に減るはずです。**

2 フィルタリングソフトの導入

※非常に効果の高い対策です！

スマートフォンを契約する際に，販売店から紹介されます。（格安SIMの場合は要確認）

主な制限機能

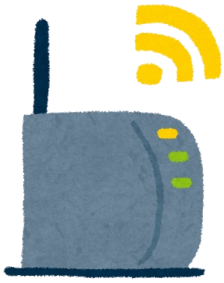
通話先制限

アプリのインストール制限

ゲームアプリ等の使用制限

有害サイト，SNSサイト等へのアクセスの制限

使用時間帯制限



WiFi通信の接続制限

フィルタリングソフトとは

子どもに見せたくないサイトへのアクセスや，使わせたくないスマートフォンの機能を制限するソフトウェア。年齢に合わせ，各機能ごとに使用の可否，使用時間帯等細かく設定できる。各社が推奨する設定があり簡単に設定できる。

保護者がパスワードを管理することで勝手に機能を解除できない仕様。

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

第15条 携帯電話インターネット接続役務提供事業者の青少年有害情報フィルタリングサービスの提供義務

携帯電話インターネット接続役務提供事業者は、役務提供契約の相手方又は役務提供契約に係る携帯電話端末等の使用者が青少年である場合には、青少年有害情報フィルタリングサービスの利用を条件として、携帯電話インターネット接続役務を提供しなければならない。ただし、その青少年の保護者が、青少年有害情報フィルタリングサービスを利用しない旨の申出をした場合は、この限りでない。

広島県青少年健全育成条例

第42条の２　第１項　保護者、家庭を構成する者並びに学校及び職場の関係者その他青少年の育成に携わる関係者は、青少年がインターネットを利用するに当たつては、フィルタリング（インターネットを利用して得られる情報について一定の条件により受信するかどうかを選択することができる仕組みをいう。以下同じ。）の機能を有するソフトウェアの活用その他適切な方法により、インターネットの利用により得られる情報であつてその内容の全部又は一部が第十六条各号のいずれかに該当すると認められる情報（以下「有害情報」という。）を、青少年に閲覧させ、又は視聴させないように努めなければならない。

3 家庭でのルール作り

これはアメリカのある母親が13歳の息子にスマホを与える際に作った「契約書」です。「スマホ18の約束」という呼び名で有名な文章です。スマホの対応に悩む保護者には大変参考になると思います。

私と息子のスマートフォンに関する契約書

1　これは私が買い，料金も払っているスマートフォンです。**あなたに貸しているものです**。

2　パスワードは私が管理します。

3　これは「電話」です。鳴ったら出ること。礼儀正しく話しなさい。お父さんや私からの電話には必ず出ること。

4　学校がある平日はPM7:30，週末はPM9:00になったら私に携帯電話を渡すこと。夜の間は電源を切り，AM7:30に電源を入れます。電話すべきではない時間にメールや携帯電話で話してはいけません。お互いの家族のプライバシーを尊重しましょう。

5　学校に持って行ってはいけません。**メールではなく，直接話しなさい**。人との会話は大切なスキルです。

6　故障，紛失した時の修理や買換え費用は自己負担です。必ず起こるでしょうから自分で準備しておきなさい。

7　だれかを騙すこと，嘘をつくこと，馬鹿にすることに使ってはいけません。たとえ誘われても，**人を傷つけるような会話には参加しないことです**。

8　面と向かって言えないことは，メールでも言わないこと。

9　友達の親の前で言えないことは，メールでも言わないこと。

10　ポルノは禁止。必要ならお父さんや私に聞きなさい。

11　公共の場では電源を切るか，音を消すこと。あなたは礼儀正しい子です。iPhoneがそれを壊さないように。

12　あなたの性的な写真を送ったり，他人からもらったりしないこと。あなたは賢い子ですが，そういう誘惑に駆られる時期が来るでしょう。こうした行為はあなたのこれからの人生を台無しにします。巨大なインターネット空間を消すことはできないし，インターネットに出てしまった悪い評判を消すこともできません。

13　むやみやたらに写真やビデオを撮らないこと。直接肌で体験してください。

14　たまには携帯電話を家において出かけましょう。携帯電話はあなたの体の一部ではありません。携帯電話なしで生活することを覚えてください。流行に流されない，取り残されることを気にしない大きな器の人になってください。

15　新しい音楽だけでなく，いろいろな音楽を聴き，視野を広げてください。

16　時々パズルや知能ゲームで遊んでください。

17　上を向いて歩いてください。周りの世界を良く見てください。窓から外を覗いてください。鳥の鳴き声を聞いてください。知らない人と会話してください。グーグル検索なしで考えてください 。

18　あなたがミスを犯したなら，携帯を取り上げます。そして話し合い，もう一度やり直しましょう。ミスはあなただけの問題ではなく，**私達家族の問題です。**

ネットの世界はまだまだ無法地帯

ルールを作って自己防衛が不可欠。

約束は**書面**で。口約束は効果が薄い。

ユーザーIDと**パスワード**を親子で一緒に設定,またはあとで報告させる。

- 隠し事ができる環境にしない。
- ネットトラブルの際に重要な追跡情報になり得る。

使用する**時間帯**を決める。

- メッセージが届かない時間帯を決める。学校単位等で設定することが望ましい。

プライベートな情報を出さない。

- 住所，名前，写真を出さないことはもちろん，学校名等にも注意する。

トラブルの時はすぐに学校や保護者に**相談**する。

- SNSでのトラブルや詐欺被害等,子どもだけで対処できることは少ない。事態が悪化してからでは遅い。

保護者に対しては，ネットトラブルの対策は**子どもと保護者が共に考えるべき問題**であること，また子どもに対しては，契約や使用方法に関する**決定権は保護者にある**ことを理解させるべき。

「スマホ18の約束」は，ネットリテラシーを醸成する上で基本になる事柄が数多く含まれています。スマートフォンは普段どう使えばよいか，何がトラブルになりそうなのか，また使い方は親子で考えるべきといった重要な理念まで著わされています。

それだけスマートフォンにまつわるトラブルが日常的だという事でしょう。

「SNS外し」という言葉が生まれるほど，実社会以上にインターネットでの付き合いは大変です。子ども達も初めのうちはスマートフォンを楽しいコミュニケーションツールとして使っていますが，使っているうちに大変さに気づくようです。

しっかりしたルールを作ることで，

- ネット依存から脱却
- 仲間外れの状況の改善
- 勉強時間，睡眠時間，自分のための時間の確保

といった効果が見込めます。

子ども達自身も「ネット上の友人関係」を窮屈に感じているということをよく聞きます。子ども達がしがらみに縛られ，大きな問題になる前に，自分を守る方法を示してやることが必要です。

第3章　学校編

インターネット事件簿

　サイバー空間の治安はここ数年で最も大きく悪化したと言われます。それはスマートフォンの急激な普及によって，利用者が突然サイバー空間に放り出された事による混乱によるものです。あたかもモータリゼーションによって交通事故が激増した時代のようです。

　法律や対策は随時見直されていますが，サイバー空間の変化に追い付くには時間が必要です。交通安全教育のように，子どものうちからネットリテラシーを養うための教育を行っていく必要があります。

サイバー空間は公共の場　そこでの行為は現実世界と同様の評価を受ける

1 事案把握時の対応要領，留意点

はじめに

サイバー空間で発生した事案を事件化するにあたっては，個々の事案に関する証拠資料（証言や証拠物）を広く確保することが必須です。

しかしこの種の事案は事案の発覚が遅れがちで，そのため捜査が困難になることがあります。

また，関係者の特定が出来なければ，書き込みや写真の削除等の，重要な目的が達成できなくなる恐れがあります。

したがって，被害届提出の有無にかかわらず，できるだけ早い段階で**警察に連絡・相談**して情報共有と連携を行い，事件化をにらんだ関係者の特定と証拠収集に努める必要があります。

さらに子ども達には，トラブルになった場合にはできるだけ早く保護者や教員等に相談することを教示しておくことが重要です。

発生時の対応

事案の把握当初から検討すべき事項を以下に列挙します。

◆ **緊急性の判断**

脅迫等で身体に危険が及ぶ等の事態が切迫している場合には，迷わず110番通報する。また緊急性がない場合でも，具体的に犯罪が行われることが考えられる場合は，速やかに管轄の警察署等へ相談・連絡する。

◆ **情報の共有**

この種の事案はリアルタイムに把握するのが難しく，発覚したころには状況が拡大し収拾が困難になっていることが多い。そのため，相談等があった場合には静観せずすぐに行動を起こす必要がある。早い段階で学校で問題を共有し組織的に対策することが重要である。

またスマートフォンの確認を要する等保護者の協力が不可欠であることから，関係する保護者とも情報を共有し，共に解決するといった認識を持つ。

◆ **書き込み内容の確認**

掲示板等への書き込みが問題となる事案の場合，その書き込みが何らかの理由で削除されることがあり，事実確認が困難となる恐れがある。そのため実際にそのページを開いて書き込みを確認した上，下記のとおり印字等して記録する。

◆ **資料の収集，保全**

掲示板等に掲載された内容をそのまま印字し，Webサイトの場合にはURL，メッセージサービスの場合には送受信者の情報，メールの場合にはさらにメールヘッダ等並びにサービス上の具体的な場所やその付属情報，参考情報，送受信日時及び印字した日時等を記録する。また書き込んだ者のユーザーIDやプロフィール等の情報を併せて記録し，削除要請，警察での事件化及びその後の紛議等に備える。

◆ **被害関係者との協議**

インターネット上に公開等されたデータを完全に削除することは，現実的に不可能と言われ，このことを認識して対応を考える必要がある。被害者，保護者にはこのことをよく説明し，理解を得ること。

また他にも関係者がいれば早い段階で情報共有し，解決に向けた共通認識を持つ。

◆ **加害少年の指導前の連絡・調整**

指導に入れば関係者が証拠隠滅を行う可能性があるため，事前に警察と連絡・調整をするべきである。

◆ **金銭被害の拡大防止**

詐欺等犯罪の被害に遭い，送金したりクレジット決済をしてしまったとの申し出を受けた場合は，至急金融機関やクレジット会社に連絡を取って送金を停止させるよう指導する。口座からの引き出し等が完了すれば金銭的な被害回復が困難になるため，優先的に行わせる。

◆ **削除要請等**

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（以下「プロバイダ責任制限法」という。）では，削除要請及び情報開示請求の基準等が規定されている。これは損害を受けた者が行うこととされていることから，その手続きを経る場合は損害を受けた当事者が行うこととなる。**【P34 削除要請の考え方と方法】**

※　次のページ以降の各事例ごとに付け加えた罪名や法的考察は一例であって，実際に事案に対応する場合には，具体的な状況を考慮し個別に判断することとなります。

2-1 SNSや掲示板サイトを悪用した誹謗中傷

事例①

◆　SNSや掲示板サイト，チャット等不特定多数が閲覧するサイトへ，特定の人物を誹謗中傷する文章等が書き込まれた。

SNS　【P50 主なSNSサービスの概要と用語】

◆ **SNSとは**

ソーシャルネットワーキングサービスの略。

他人との「繋がり」を促進する機能を提供するオンラインサービス。知人間でのコミュニケーションや，趣味，出身校，友人の友人といった何らかの共通点のあるユーザー同士の繋がりを提示して新たな人間関係を構築する場を提供する。

現在のインターネットにおいて主要なサービスであるものの，匿名性等によってトラブルが発生しやすい。

◆ **主なSNSサービス**

Twitter：その場その場の出来事をリアルタイムに投稿する人向け。投稿内容は，本音，私事を投稿するイメージだと言われる。

Facebook：近況報告等，私生活を誰かにプレゼンしたい人向け。投稿内容は，建前，公式な内容を投稿するイメージだと言われる。

インスタグラム：写真が中心。自分のセンスを認められたい投稿が多い。著名人，有名人等にとってはセルフブランド化の重要な手段と言われる。

LINE（タイムライン）：基本はチャットサービス**【P42 IT用語集No,46「チャット」】**であるものの，「タイムライン」がSNSとして機能している。主に友だちの登録者等，近親者に向けたSNS。

該当し得る罪名

◆ **刑法第230条　名誉棄損**

公然と事実を摘示し、人の名誉を毀損した者は、その事実の有無にかかわらず、３年以下の懲役若しくは禁錮又は50万円以下の罰金に処する。

◆ **刑法第231条　侮辱**

事実を摘示しなくても、公然と人を侮辱した者は、拘留又は科料に処する。

指導のポイント

言葉は刃物より危険な凶器になる

◆ **実情に応じた情報モラル教育**

この種の事案は，発生してから対応するのは極めて困難であるため，普段の教育面での指導が非常に重要である。

社会の変化に応じ，日常的なモラルの指導に加えて情報社会の特性を理解させることにより，インターネットを適切に利用する基本的な考え方，行動を育成する。

◆ **インターネットの向こう側には，現実の「人間」がいることを理解させる**

人間同士のコミュニケーションだから，楽しいこともトラブルも起こり得ることを考えてSNS等を利用する。**【P10 SNSの使い方】**

◆ **一度文章を読み直してから送信することを徹底する**

相手の顔が見えないため表現が過激になりやすい。また送信する情報が文字だけのため，何気ない内容で傷つけてしまうことがある。送信前に立ち止まり，その文章を受けた側がどう感じるかということをよく考えて送る。

◆ **送信したメッセージは取り消すことができない**

送信した情報を削除することは事実上不可能とされる。いたずらであろうと，いったん送信してしまうと自分や相手方の悪評を半永久的に残すことになる。**【P10 デジタルタトゥーと就活】**

◆ **書き込みに囚われ過ぎない**

「ウザイ」等の書き込みは，顔が見えないためその文章を受け取る人物のことをよく考えずに送ったものがほとんど。メッセージ性が低いことから必要以上に気にしないこと。**【P９匿名性】**

2-2 自画撮り被害 ～セクストーション・リベンジポルノ～

事例②

◆　交際している相手に「裸の写真を送れ」と言われ，スマホで写真を撮影して送信した。
これが保護者の知るところとなり，トラブルに発展した。

◆　さらに送った相手から「写真をばらまかれたくなければ言うことを聞け」と脅された。

該当し得る罪名

児童買春、児童ポルノに係る行為等の規制及び処罰並びに児童の保護等に関する法律
（以下「児童ポルノ法」という。）

◆　第７条　児童ポルノ所持、提供等

自己の性的好奇心を満たす目的で、児童ポルノを所持した者（自己の意思に基づいて所持するに至った者であり、かつ、当該者であることが明らかに認められる者に限る。）は、一年以下の懲役又は百万円以下の罰金に処する。自己の性的好奇心を満たす目的で、第二条第三項各号のいずれかに掲げる児童の姿態を視覚により認識することができる方法により描写した情報を記録した電磁的記録を保管した者（自己の意思に基づいて保管するに至った者であり、かつ、当該者であることが明らかに認められる者に限る。）も、同様とする。

２　児童ポルノを提供した者は、三年以下の懲役又は三百万円以下の罰金に処する。電気通信回線を通じて第二条第三項各号のいずれかに掲げる児童の姿態を視覚により認識することができる方法により描写した情報を記録した電磁的記録その他の記録を提供した者も、同様とする。

３　前項に掲げる行為の目的で、児童ポルノを製造し、所持し、運搬し、本邦に輸入し、又は本邦から輸出した者も、同項と同様とする。同項に掲げる行為の目的で、同項の電磁的記録を保管した者も、同様とする。

私事性的画像記録の提供等による被害の防止に関する法律　（いわゆる「リベンジポルノ」関係法令）

◆　第３条　私事性的画像記録提供等

第三者が撮影対象者を特定することができる方法で、電気通信回線を通じて私事性的画像記録を不特定又は多数の者に提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。

２　前項の方法で、私事性的画像記録物を不特定若しくは多数の者に提供し、又は公然と陳列した者も、同項と同様とする。

３　前二項の行為をさせる目的で、電気通信回線を通じて私事性的画像記録を提供し、又は私事性的画像記録物を提供した者は、一年以下の懲役又は三十万円以下の罰金に処する。

４　前三項の罪は、告訴がなければ公訴を提起することができない。

◆　刑法第222条　脅迫

生命、身体、自由、名誉又は財産に対し害を加える旨を告知して人を脅迫した者は、二年以下の懲役又は三十万円以下の罰金に処する。

指導のポイント

裸の写真を送らせるのは，親密になるためではない

◆ **発生してから対応するのは極めて困難　普段からの教育面での指導が重要**

子ども達の間では，交際相手の性的な写真や動画を撮ったり，あるいは撮らせたりということが行われている。

警察庁の統計情報によれば，児童ポルノ事犯の中で，写真等の製造に係るケースのうち自画撮りが占める割合が約４割となっている。

スマートフォンの普及で写真や動画を手軽に撮影できるようになった背景があるため，子ども達は安易にこの種の画像を撮影する等して，製造又は拡散する等の事態を生じさせるケースがあるが，これを未然に防止するためには子ども達に危険性を周知させ，自覚を促す対策が重要となる。

◆ **リスクの自覚**

【P10 デジタルタトゥーと就活】のとおり，送信済みのデータを削除することは事実上不可能とされる。内容によっては，交際相手によって被害者の悪評を半永久的に残すことになり，就活等人生の重要な選択に多大な影響を及ぼすことになりかねない。

また**【P11 セクストーション・リベンジポルノ】**のとおり，交際相手から脅迫や嫌がらせの手段にされる恐れがある。

送信を求める側，それに応じる側に，将来にわたって大きなリスクとなり得るということを指導する必要がある。

◆ **撮影を求める側への指導**

交際中の男女で相手方から性的な画像等を求められた場合に，「断るとふられる」「交際中なのだから他人に見せることはないだろう」と思いがちで，その要求を断りにくい状況になる。そのためこの種の事案を防止するには，撮影を求める側への指導を徹底して行うことが重要である。

交際相手の性的な写真等を撮影したり，また撮影を要求しこれに応じた交際相手が自画撮りすれば，児童ポルノ法の違反が成立する。従って，撮影を求めることは犯罪になり得るということを理解させる必要がある。

また交際中の相手を犯罪に関わらせたり，将来に不安を残させたりするような行為は，相手を大切にしていないということの表れだと認識させるべきである。

◆ **撮影を求められる側への指導**

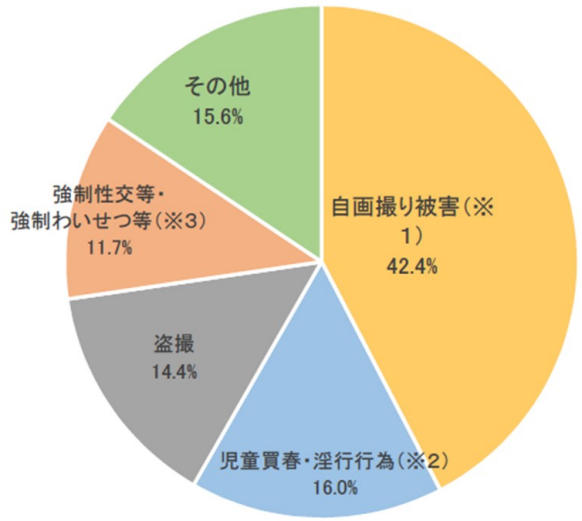
児童ポルノ法の製造罪において，相手方の要求に応じて性的な写真等を自画撮りした場合，その行為は「製造」そのものであって，要求した者と共に製造罪に問われる可能性がある。つまりこのような形態で撮影する行為は犯罪になり得るということを指導するべきである。

裸の画像を要求する目的は，「好きだから」「親密になりたい」ということでは決してなく，性的好奇心を満たすためのもの。このような行為を求めたり強いたりするのは，相手方が被害者のことを大切にしていないということの表れだと認識させるべきである。

コラム　平成29年中の自画撮り被害の実情

警察庁　https://www.npa.go.jp/safetylife/syonen/no_cp/newsrelease/2017_statistcs_data.pdf

【児童ポルノ事件】被害児童の被害態様別の割合

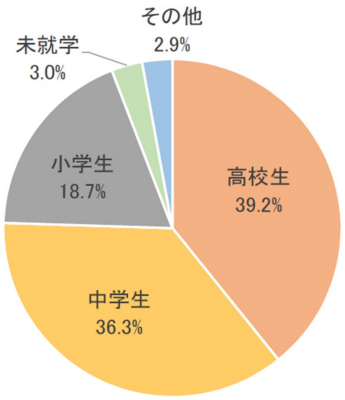


N=1, 216

被害態様	人数
自画撮り被害（※1）	515
児童買春・淫行行為（※2）	194
盗撮	175
強制性交等・強制わいせつ等（※3）	142
その他	190

※1 「自画撮り被害」は、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、メール等で送らされる形態の被害をいう。
※2 「淫行行為」は、「青少年育成条例違反（淫行行為）」をいう。
※3 「強制性交等・強制わいせつ等」には監護者性交等及び監護者わいせつを含む。また、刑法の一部を改正する法律（平成29年法律第72号）による改正前の強姦及び強制わいせつを含む。

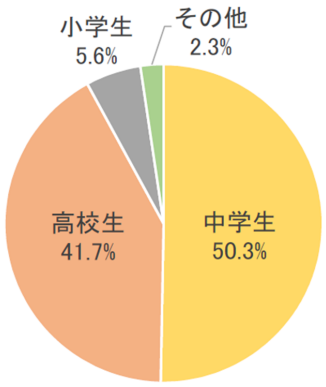
【児童ポルノ事件】被害児童の学職別の推移



N=1, 216

学職	人数
未就学	36
小学生	227
中学生	441
高校生	477
その他	35

【児童ポルノ事件】自画撮り被害に遭った児童の学職別の割合



N=515

学職	人員
小学生	29
中学生	259
高校生	215
その他	12

児童ポルノ事犯の「自画撮り被害」が増加しています。
中学生、高校生等が「自画撮り被害」に遭わないように広報・啓発をお願いします。

- 児童ポルノの製造にかかる事案は，約４割が自画撮りによるもの。
- 自画撮り被害は，SNS等のコミュニティサイトに起因するものが約８割を占める。
- 自画撮りの被害のみに絞ると半数以上を中学生が占める。

2-3 援助交際 及び コンピュータ・ウイルス

事例③

◆　SNSで，援助交際を行う目的で面識のない相手方と知り合い，「裸が見たい」と言われ画像を送信した。
◆　さらに「別のアプリで話そう」とメールを送信されたが，その中のリンクからアプリをインストールしたところウイルスに感染し，電話帳データを盗まれた。「電話帳に記載のある友達にばらまかれたくなければ電子マネーで金を払え」と恐喝され，言われるまま電子マネーの番号を教えたが，裸の写真や電話帳データは消してくれなかった。

該当し得る罪名

◆　**刑法第249条　恐喝**
人を恐喝して財物を交付させた者は、10年以下の懲役に処する。
2　前項の方法により、財産上不法の利益を得、又は他人にこれを得させた者も、同項と同様とする。

◆　**刑法第168条の２　不正指令電磁的記録作成等**（ウイルスの関係法令）
正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。
一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
2　正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。

事例の背景

援助交際の相手を探し出す方法が，出会い系サイトからSNSに移っており，また不特定の相手の求めに応じて性的な画像等を送信したり，実際に相手方と接触する少年等が多数おり，これらの人物が福祉犯罪の被害者となっている。

また出会いを求めている素振りをして，言葉巧みに性的な写真等を送らせ，それをもとに恐喝する者がいる。事例のように，スマートフォンをウイルスに感染させ電話帳を盗み取った後交友関係を把握し，それをもとに脅迫するということを，被害者と接触することなく実行するケースもある。

指導のポイント

◆ **把握時の緊急性の判断**

特にこの種の事案では，援助交際の目的で誘い出され，相手方と接触した結果，恐喝や強姦の被害に遭う等大きな事件に発展することがある。相手方と接触する等事態が切迫している場合には，迷わず110番通報する。また緊急性がない場合でも速やかに管轄の警察署等へ相談・連絡する。

◆ **注意喚起**

盗まれた電話帳のデータを勝手に使用され，なりすまし等により被害が拡大する恐れがある。できるだけ早期に，電話帳に登録された知人等に注意喚起する。

◆ **ウイルスの対策**

普段からの心構えとして

- 不審なファイルを安易に開かない
- ウイルス対策ソフトを導入し，常に更新して最新の状態にする
- OSやソフトウェアも更新し，最新の状態に保つ
- 安全を確認したサイト以外からファイルをダウンロードしない

等がある。

また事例のように既にウイルスに感染している場合は，電話帳を盗むだけでなく他の機能にも影響がある可能性があるため，感染した機器の初期化を検討する。

コラム　サイバー補導

◆ **サイバー補導とは**

児童や生徒が援助交際を求める等のインターネット上に不適切な書き込みをサイバーパトロールによって発見し，客を装った警察官が書き込みを行った少年と接触を図り，不良行為少年の取扱に基づき，直接，注意・指導（継続補導を含む）する少年警察活動の一つである。

◆ **補導された少年の特徴**

- 補導した児童，生徒の6割は非行・補導歴がない。
- 補導した児童，生徒の9割は援助交際等の書き込みにスマートフォンを使用している。
- 保護者の知らないうちに児童，生徒が援助交際等の書き込み等をしている。
- 無料通話アプリのIDを交換する掲示板とともにSNSへの書き込みも見られる。
- 街頭補導と異なり警察官等が児童，生徒と接触できないことがある等対応に手間がかかる。

2-4　アカウントを勝手に使用される「なりすまし」

事例④

- **SNSで，何者かによって自分になりすまされ，第三者を誹謗中傷する内容を勝手に書き込まれた。**
- **自分のWebメールを盗み見られた。**
- **ゲームアイテムが何者かに盗まれた。**

該当し得る罪名

◆　**不正アクセス行為の禁止等に関する法律**

第３条　不正アクセス行為の禁止

何人も、不正アクセス行為をしてはならない。**【P44 IT用語集No,74 「不正アクセス」】**

発生時の対応

◆　**資料の収集，保全**

ログイン履歴が閲覧できるサービスであれば，その情報を全て記録する。またなりすまし後の書き込み等の内容をそのまま印字し，当該サイトのURL，書き込まれた日時，印字した日時を記録する。

◆　**パスワードの変更**

不正アクセスされないために，直ちにパスワードを変更させる。既に犯人によりパスワードを変更されている場合は，サービスの運営会社に連絡させ，アカウントを取り戻す手続きを取らせる。また他のサービスでも同じパスワードを使用していれば，二次被害を防ぐためそのパスワードも変更させる。

◆　**クレジットカード等の無効化**

オンラインゲーム等でクレジットカードを登録していれば，勝手に使われる可能性があるので登録を解除させる。また既にカードを使用されている形跡があれば直ちにクレジット会社に連絡を取るよう指導し，送金を停止させる。

◆　**加害少年への指導**

被害回復を念頭に，アクセス後の行動を聴取する。

場合によっては写真やメールの内容等を加害少年の端末に保存している可能性があるので，よく確認し削除させる。そのためスマートフォン等を持参させ，書き込み等の履歴があるか表示し確認する。※削除に際しては，警察との協議を十分行うこと。

指導のポイント

プライベートは自分で守る

◆　**アカウントは現代生活に密着したプライベート空間**

利用しているサービスには個人情報や行動履歴が大量に保存されている。またクレジット情報が登録してある等，金銭に関する情報と直結していることもある。

現代生活においてWebサービスは不可欠なものとなりつつあり，アカウントは「自宅には鍵を掛ける」ということと同等に，守るべきプライベート空間だということを指導する。

◆　**自分のパスワードの保護**

仲の良い友人であってもパスワードを教えない，また安易に友人等から聞き出そうとしないこと，誕生日や電話番号等，誰でも簡単に推測できるパスワードにしないこと，パスワードは定期的に変更するということを指導する。**【P11 パスワードの保護】**

2-5 フィッシング

事例⑤

◆ **実在する会社から「未納料金があります」「至急ココにアクセスしてください」とのメールが届き，メール内のリンクからアクセスしたサイトに個人名やユーザーID，パスワード，さらにクレジットカードの情報を入力してしまった。**

該当し得る罪名

◆ **不正アクセス行為の禁止等に関する法律**

第７条　識別符号の入力を不正に要求する行為の禁止（フィッシング行為の禁止）

何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。

一　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為

二　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為

被害防止のポイント

多くのサイバー犯罪の入り口

◆ **「フィッシング」とは**

実在の銀行やクレジット会社のサイト，ショッピングサイト等を装った「フィッシングメール」を送り付け，これらの銀行等のWebサイトとそっくりの偽サイトに誘導して，個人情報やパスワード等の重要な情報を入力させて情報を盗み取る行為のこと。またこのようなWebサイトを「フィッシングサイト」という。

フィッシングは**多くのサイバー犯罪の入り口**になっている。

◆ **フィッシングメールへの心構え**

「料金未納」「パスワードを変更してください」等の身に覚えのないメールを受けた場合は，全て無視する。会員登録をしていたり，身に覚えのあるようなメールであれば，その中の**リンクは決してクリックせず**，ブラウザ（インターネット閲覧ソフト）を開いてそこからメールの送信元のWebサイトにログインする。もし本当に請求やパスワード変更が必要であれば，メールと同様の内容が個々のユーザー宛に掲載されているものと思われる。

◆ **フィッシングサイトの対策**

本物のサイトをコピーしたものを使用していることが多く，見た目で偽物と見抜くことはほとんど不可能である。ウイルス対策ソフトの機能によっては，フィッシングサイトにアクセスすると警告画面を表示するものがあるので，活用する。

◆ **送金の停止，パスワードの変更**

フィッシングサイトで送金の処理をしてしまった場合は，至急関係する金融機関等へ相談し，送金の停止やクレジットカードの利用を停止する。

またパスワードを他のWebサイトでも使い回していれば，そのサイトでも不正アクセスされてしまうので，至急そのパスワードを変更する。

2-6 詐欺サイト

事例⑥

◆ **ネットショップで買い物をし，代金を支払ったが，商品が送られてこない。また相手と連絡が取れなくなった。**

関係法令

◆ **刑法第246条　詐欺**

人を欺いて財物を交付させた者は、十年以下の懲役に処する。

2　前項の方法により、財産上不法の利益を得、又は他人にこれを得させた者も、同項と同様とする。

被害防止のポイント

確認の手間を惜しむのは「安物買いの銭失い」

◆ **ネット通販詐欺の不審点を見分けるポイント**

- **電話番号が虚偽又は桁数が少ない**
  確実な確認方法は電話をかけてみること。電話番号の桁数が少ない等虚偽であれば電話が繋がらないため，詐欺サイトの可能性がある。また電話が繋がるようなら相手方と話してみて不審点を解明する。
- **商品が極端に安い**
  新商品なのに極端に安い，新品なのに中古品より安い等，価格に矛盾がある場合や他のショッピングサイトとの整合性がない場合は，詐欺サイトの可能性がある。
- **「会社概要」欄記載の所在地に建物が存在しない，又は公共施設の所在地を窃用している**
  地図サービス等を利用し，会社概要の所在地で検索すると不審点を見つけやすい。その場所に建物が存在しない，公共施設等の所在地が充てられている等およそ店舗と認められない建物の所在地が記載されていれば，詐欺サイトの可能性がある。
- **支払方法が銀行振込しかない**
  詐欺であれば，送金を止められやすい，足がつきやすいとの理由から，クレジット決済を避けようとするケースがある。クレジット決済を選択してカード番号等を送信したのに「受け付けられないので銀行振込で」と変更させられるケースであれば，詐欺と共にフィッシングサイトの可能性がある。情報を送信してしまった場合はすぐにクレジットカードの利用を停止すること。
- **文章の表記に過誤が多い**
  「弊社は輸入品が売っております」「いろいろがあります」等，会社案内等の文章の表現に多くの過誤が認められる場合及び，他国の言語が充てられ，いわゆる「文字化け」が多い場合には，詐欺サイトの疑いがある。
- **振込先口座が外国人名義**
  外国人が違法に取得した銀行口座が詐欺等の犯罪に使用されることがある。
- **インターネット上の「詐欺サイト情報」や「口コミ」を確認する**
  詐欺サイトの情報収集をしている団体や，警告を発している詐欺の被害者の情報がインターネット上に公開されており，詐欺を見分ける上で参考になる。企業名，サイト名，代表者名，メールアドレス及び電話番号等でインターネット検索し，不審か否か判断する。

被害に遭った場合

◆ **詐欺の疑いがある場合に取るべき対応**

- 送金処理が完了していなければ，手続きの停止により送金を止めることができる可能性があるため，まずクレジット会社や金融機関に連絡する。
- クレジット情報等を送信している場合は，クレジット会社でカードを停止する手続きを取る。
- 組み戻し（振込等の取組後に，振込依頼人の都合により，その依頼を撤回する際に取る手続き。）については，金融機関と相談する。
- 取引きに際してやりとりしたメール，売買のページ，注文画面及び代金振込みの控え等の記録を保管しておく。
- 相手に対し，期日を定めて債務履行を求める「内容証明郵便」を配達記録を付けて送達する。内容証明郵便が不受理又は宛先不明で戻ってきた場合等の状況があれば，詐欺を疑う要素となる。

【参考】内容証明郵便とは，いつ，いかなる内容の文書を誰から誰あてに差し出されたかということを，差出人が作成した謄本によって日本郵便株式会社が証明する制度。

◆ **被害の届け出と口座凍結**

捜査機関，弁護士会，金融庁および消費生活センター等公的機関の通報等により，金融機関は口座凍結の手続きを行う。

警察は，その通報等に際し凍結すべき口座の情報及び実際に送金した事実を確認するため，これを示す資料を直接確認する必要がある。

被害の届け出をする場合は，事前に連絡し，これらの資料を持参の上，最寄りの警察署を訪ねること。

2-7 コンピュータ・ウイルス ～不正送金・ランサムウェア～

事例⑦

- **ネットバンキングサービスを使っているが，ある日突然預金が消えた。**
- **学校のパソコンに保管中の大事なファイルが突然開けなくなり，画面上に「戻してほしければ金を払え」と表示された。**

該当し得る罪名

刑法第168条の２　不正指令電磁的記録作成等（ウイルスの関係法令）

正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、三年以下の懲役又は五十万円以下の罰金に処する。

一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録

二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録

２　正当な理由がないのに、前項第一号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。

被害防止のポイント

ウイルス対策ソフトの利用はサイバー空間のたしなみ

- **個人の銀行口座にまで手を出す現代のウイルス**
  現代のウイルスは，個人の口座から預金を盗む目的でパスワードを奪うものにまで悪質化した。つまりウイルスに感染すると全ての財産が盗まれることがあり得る。
- **ウイルス対策ソフトの利用**
  ウイルスは，多くの場合目立った行動を起こさず潜伏し，動き出す時を待っていたり，画面に表れないところで動作している。このようなウイルスはウイルス対策ソフトでなければ検知が難しい。
- **ウイルス対策ソフトの更新**
  インストールしたウイルス対策ソフトは，更新しないままではすぐに役に立たなくなる。サイバー空間では毎日数万の新しいウイルスが生み出されており，過去に例のないウイルスは検知できない。そのため，パソコン等をインターネットにつないでウイルス対策ソフトを更新する必要がある。
- **OSやインストールしているソフトの更新**
  ウイルス対策ソフトと同様に，OS（「Windows」や「iOS」等のオペレーティングシステム）も更新する必要がある。
  OSの脆弱性を狙い，インターネット越しにウイルスを侵入させられるサイバー攻撃がある。新しく発見された脆弱性はOSのメーカーが順次対策しているものの，ユーザーはメーカーの対策後にOSを更新しなければ，脆弱性を残したままとなる。
  またインストールしているソフトに脆弱性がある場合，同じようにサイバー攻撃を受ける可能性があるので，これも更新する必要がある。
- **サイバーセキュリティに関心を持つ**
  何より大事なことは，サイバー空間が危険な場所で，ウイルスに感染すると大変な損害をうけるということを認識すること。サイバーセキュリティに関心を持って，不安があればすぐにネットで調べて対策する。そのようにしてサイバーセキュリティに関する知識を獲得する。
- **参考　ランサムウェア**
  ランサムとは「身代金」という意味。ウイルスに感染するとパソコンのファイルのうち文書ファイル等が暗号化され，画面上に「元に戻して欲しければ金を払え」等と表示される。身代金を払っても暗号化が解除されないケースがある。

2-8 その他の事例

事例⑧ 犯行予告

◆ 掲示板サイトやSNSに「テストを中止しないと学校を爆破します」「卒業式で○○先生を殴ります」との書き込みを見つけた。

該当し得る罪名

- ◆ **刑法 95 条　公務執行妨害**
- ◆ **刑法222条　脅迫**
- ◆ **刑法223条　強要**
- ◆ **刑法233条　偽計業務妨害**
- ◆ **刑法234条　威力業務妨害**

対応時のポイント

◆ **書き込み内容の保存**

特にこのような事案の場合，掲示板サイト等の管理者の判断等により書き込みが削除されることがある。このため書き込みを発見した際に印字等をして記録しておかなければ，書き込んだ者の追跡が不可能となる恐れがある。

事例⑨ 自殺予告

◆ 地域住民から「（インターネット掲示板やSNSで，）『今から自殺します』という書き込みを見つけた。内容からそちらの学校の生徒ではないか。」との連絡を受けた。

対応時のポイント

◆ **投稿者の確認と背景の聴取**

警察では，投稿者の情報を得るため，刑法に言う「緊急避難」を理由に電気通信事業者に協力を求める。緊急避難に該当し電気通信事業者等の協力を得られるかどうかは，「現在の危難」（生命身体等の権利侵害の危険が切迫している状況）の存在等の要件を満たすかどうかによる。書き込んだ背景等の情報があれば切迫性の判断材料になるため，できるだけ多くの情報を警察と共有すべきである。

事例⑩ インターネットを悪用したカンニング

◆　インターネット上の質問サイトに，現に行われている試験の問題が投稿され，答案を求める質問がされた。

該当し得る罪名

刑法第233条　偽計業務妨害

虚偽の風説を流布し、又は偽計を用いて、人の信用を毀損し、又はその業務を妨害した者は、三年以下の懲役又は五十万円以下の罰金に処する。

指導のポイント

◆　**犯罪に該当することの教示**

国家試験でのカンニング行為により，偽計業務妨害で検挙された事例がある。

カンニング行為は受験上のペナルティだけでなく，刑事的な責任を負う可能性があることを教示すべき。

参　考

上記の事例のようにインターネットを悪用したカンニング行為を行った受験生が，偽計業務妨害で逮捕された例がある。

この件では，投稿日時から試験中の犯行であることが明らかであった。

また本人の説明として，カンニングの方法は，

●スマホでない普通の携帯電話で投稿した
●携帯電話を足の間に隠して試験問題を入力した
●試験官が通るときには足を閉じて隠した

と説明していると報道された。

3 削除要請の考え方と方法

関係法令

権利侵害を受けた者からの申し出を要する

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（いわゆるプロバイダ責任制限法）では，「自己の権利を侵害されたとする者」が削除を申し出た場合を規定する。つまり削除の申し出が第三者による場合には，プロバイダ等はこの法律が適用されないため，自らが何らかの責任を負うと判断したときに書き込みを削除しない可能性がある。

※　**海外の企業が運営するサービスには適用されない可能性がある。**

ケース①　書き込んだ者が応じる場合は，その者に削除させる

多くの掲示板等のサイトは，書き込んだ者であれば削除ができる仕様となっている。

ケース②　サイトの専用ページから削除要請する

多くの掲示板等のサイトのトップページや，書き込んだメッセージにある「問題の報告」「削除の要請」等のページから削除要請する。

ケース③　法務省インターネット人権相談受付窓口のページから相談する

法務省人権擁護局にインターネット相談ができる窓口がある。　http://www.jinken.go.jp/

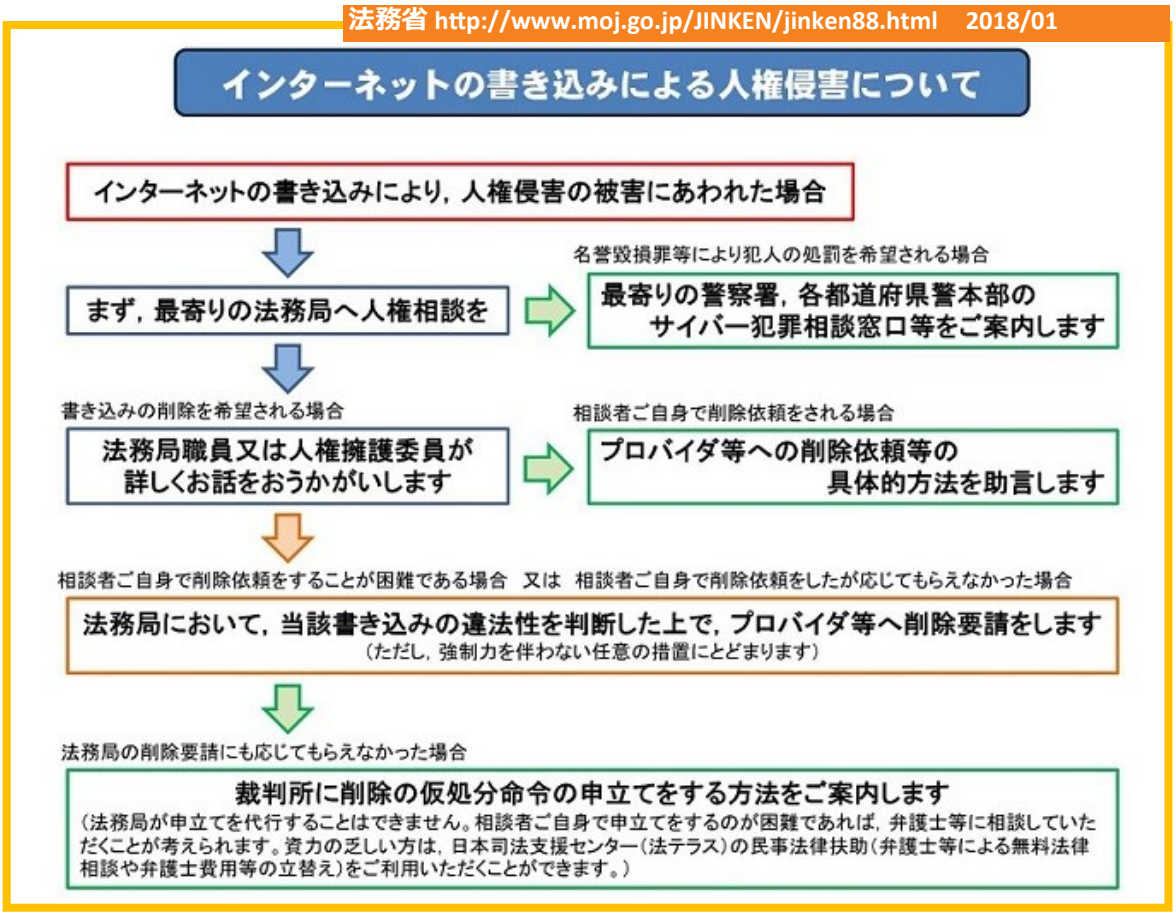
ケース④　法務局の助言を受け，文書を作成してプロバイダ等へ申し出る

法律の要件である

- **書き込みをされた者が**
- **その書き込みの場所や内容**
- **侵害されたとする権利及び権利が侵害されたとする理由**

を記載した書面を作成し，プロバイダ等に申し出る。

法務省 http://www.moj.go.jp/JINKEN/jinken88.html　2018/01



4 学校・警察の適切な連携のあり方

学校・警察との適切な連携の重要性

重要なポイントは，学校と警察が連携する目的を確認し，明確にすることです。

学校と警察の連携の目的は「少年の健全育成」を図ることに尽きます。

問題行動を起こした少年の規範意識を向上させ，立ち直りを促す・助けるといった点が連携の目的となります。

学校側から見ると，問題行動を起こした生徒の「自己指導能力の育成を図る」ことになり，また，警察の立場から見ると「管内の治安を維持するとともに，その向上を図る」ことになります。

学校と警察が連携し，管内で発生する少年事案の件数を減らし，少年の立ち直りを促して再非行を防止できれば，管内における犯罪の発生率を大きく減少させることができます。

また，校内で事案が発生した際に，早い段階で学校が警察と連携することで，児童生徒や保護者が安心感を得ることができ，さらなる問題行動等の抑止につながります。

事案発生後の早期連携

問題行動に対しては，事案が発生した後の初期的な対応と毅然とした指導が大切です。

学校から警察に対する連携に際しては，被害申告を「する」「しない」だけの申し出に止まらず，早い段階からの相談や情報提供が重要となります。

早い段階での対応の機会を逃すことにより，事態が重大化・複雑化して，解決への道のりが一層困難になってしまいます。

学校において正確に事案内容を把握しようとするあまり，それに時間をかけ過ぎてスピード感が失われないよう，迅速な対応に留意することが重要です。

把握した問題行動等の警察連携

問題行動等が発生した後，警察連携をしないことで，事態が深刻化する具体例として，生徒間暴力の発生を受け，

◆当初，被害者と加害者との話し合いで解決することになり，学校は警察へ通報しなかった。しかしながら，その後，双方の関係がこじれたことから，被害者の保護者から警察に被害届が出された。このことを受け，警察が捜査をするも，相当な期間が経過していたことから証拠等がなくなっており，真相究明ができなくなっていた。

等のケースがあります。

このような事例を教訓として，事案を学校が把握した場合には，原則として，学校から警察へ連携することについて，児童生徒や保護者に周知しておくことが大切です。

なお，警察連携することが，即ち被害申告することではなく，学校から警察に対し「相談しておくこと」が重要となります。

緊急時の連携

学校で対教師暴力や生徒間暴力等の違法行為が発生した際には，関係する児童生徒からの聞き取り，負傷者がある場合の救護措置，保護者への連絡，市町教育委員会への報告，対処方針の決定等を学校が行うことになりますが，通報を受けた警察においても，これらの対応と並行しながら，事件化を含めたさまざまな対応を進める必要があり，事案発生後，躊躇することなく学校から警察へ連携を図る必要があります。

また，いじめに関する事案が発生した場合にも，学校と警察が連携の上，適切な対応を図ることが重要であるほか，児童虐待の容疑事案を認知した際にも，時機を逸することなく，警察への通報，こども家庭センターへの通告や市町担当課等の関係機関との緊密な連携が重要となります。

平素からの連携

警察連携にあたっては，学校で問題行動等が発生した場合のみならず，平素から学校・市町教育委員会から所轄警察署へ定期的な情報交換を行う等，相互の交流を深めつつ人間関係を構築することが重要となります。

5 少年事件の手続きと流れ

警　察

警察は犯罪が発生した場合，第一次的に捜査を行い，犯人の特定，証拠の収集及び取調べ等により犯罪の事実を明らかにします。**逮捕**によって取調べる場合もあります。

- 14歳以上の少年で，法定刑が懲役・禁錮等の比較的重い犯罪を犯した場合は，検察庁に事件を送致します。
- 14歳以上の少年で，法定刑が罰金以下の犯罪を犯した場合は，直接家庭裁判所に事件を送致します。
- 14歳未満の少年は罰せられませんが，少年の行為や環境等に応じ児童相談所に送致・通告します。

逮捕の場合は **【48時間】** 以内

検　察　庁

検察庁では送致された事件について，検察官が自ら取調べ等の捜査をしたり，警察を指揮して補充捜査を行わせたりします。

- 検察官は，逮捕された犯人について，引続き身柄の拘束が必要と判断した場合，裁判官に勾留を請求します。
- 在宅事件，逮捕した事件にかかわらず，警察から送致を受けた事件の処分は，検察官が決定します。
  警察,検察官の捜査を遂げたのち,少年による事件の場合は，処分についての意見を付して家庭裁判所に送致します。

児童相談所

- 少年の性格等から保護処分が相当と認められる場合は，事件を家庭裁判所に送致します。

逮捕の場合は **【24時間】** 以内

地方裁判所等

- 裁判官は勾留請求があった場合，犯人を勾留質問して勾留の適否を判断します。

留置施設（各警察施設）

「勾留」

最長 **【20日間】** で事件の取調べが行われます。

少年鑑別所

少年鑑別所は，審判を開くために少年を収容し，処分を決めるための調査，健全育成のための観護を行います。

「勾留に代わる観護措置」

最長 **【10日間】** で鑑別と事件の取調べが行われます。

「観護措置」

おおむね **【４週間】** の鑑別が行われます。

家庭裁判所

家庭裁判所は，家庭に関する事件の審判や調停，少年審判等の権限を持ちます。

- 取調べ等の捜査を経た少年は，**【24時間】** 以内に処遇が決定され，観護措置となれば審判の要否と鑑別のため，少年鑑別所に収容されます。

- 審判不開始
- 審　判
  - 不処分
  - 保護処分
    - 児童自立支援施設等送致
    - 児童相談所送致
    - 少年院送致
    - 保護観察
    - 検察庁（逆送）

6 処遇決定に係る手続き，法的根拠

観護措置，調査

観護措置とは，主に家庭裁判所に送致された少年の審判を円滑に進めたり，少年の処分を適切に決めるための検査を行ったりすること等が必要な場合に，少年を少年鑑別所に送致し，一定期間そこに収容することをいいます。 収容後，家庭裁判所調査官の面接を受けることになります。この面接では，事件の内容，家庭，友人や学校，仕事のこと，これまでの生活歴等を聴かれます。

◆ 少年法８条（事件の調査）

家庭裁判所は、審判に付すべき少年があると思料するときは、事件について調査しなければならない。検察官、司法警察員、警察官、都道府県知事又は児童相談所長から家庭裁判所の審判に付すべき少年事件の送致を受けたときも、同様とする。

2 家庭裁判所は、家庭裁判所調査官に命じて、少年、保護者又は参考人の取調その他の必要な調査を行わせることができる。

◆ 少年法９条（調査の方針）

前条の調査は、なるべく、少年、保護者又は関係人の行状、経歴、素質、環境等について、医学、心理学、教育学、社会学その他の専門的智識特に少年鑑別所の鑑別の結果を活用して、これを行うように努めなければならない。

◆ 少年審判規則11条（調査の方針・法９条関係）

審判に付すべき少年については、家庭及び保護者の関係、境遇、経歴、教育の程度及び状況、不良化の経過、性行、事件の関係、心身の状況等審判及び処遇上必要な事項の調査を行うものとする。

2 家族及び関係人の経歴、教育の程度、性行及び遺伝関係等についても、できる限り、調査を行うものとする。

3 少年を少年鑑別所に送致するときは、少年鑑別所に対し、なるべく、鑑別上及び観護処遇上の注意その他参考となる事項を示さなければならない。

◆ 少年法17条（観護の措置）

家庭裁判所は、審判を行うため必要があるときは、決定をもって、次に掲げる観護の措置をとることができる。

一　家庭裁判所調査官の観護に付すること。

二　少年鑑別所に送致すること。

審判不開始

審判を開始せずに調査のみ行って手続を終えることです。
少年保護事件において，家庭裁判所が少年に関する調査を行った結果，審判に付することができないかまたは審判に付するのが相当でないと認めるときになされます。

少年法19条（審判を開始しない旨の決定）

家庭裁判所は、調査の結果、審判に付することができず、又は審判に付するのが相当でないと認めるときは、審判を開始しない旨の決定をしなければならない。
（例）・少年に非行がない。
・事案が軽微である。

少年審判

少年審判とは，罪を犯した少年等に過ちを自覚させ， 更生させることを目的として，本当に非行を犯したかどうかを確認した上，非行の内容や個々の少年の抱える問題性 に応じた適切な処分を選択するための手続です。

区　分	内　容	
不処分 ◆ **少年法23条２項**	少年に保護処分を付することができない場合，又は付する必要がない場合 （例）・非行の原因，動機が単純偶発的 ・保護者に監護能力があり，再犯のおそれがない。	
保護処分 ◆ **少年法24条**	保護観察	・保護観察対象者の改善更生を図ることを目的として，指導監督及び補導援護を行うことにより実施するもの。保護観察官，保護司が行う。 ・保護観察中，保護観察対象者が，保護観察の継続によって改善更生を図ることができないと認める場合，家庭裁判所は,児童自立支援施設等送致又は少年院送致の決定をすることができる。
	児童自立支援施設・児童養護施設 送致	・児童自立支援施設　◆ **児童福祉法44条** 不良行為をなし，又はなすおそれのある児童及び家庭環境その他の環境上の理由により生活指導等を要する児童を入所させ，又は保護者のもとから通わせて，個々の児童の状況に応じて必要な指導を行い，その自立を支援することを目的とする施設 ・児童養護施設　◆ **児童福祉法41条** 保護者のいない児童，虐待されている児童その他環境上，養護を要する児童（乳児を除く。）を入所させて，これを養護し，あわせてその自立を図ることを目的とする施設
	少年院送致	少年を少年院に強制的に収容する保護処分で，少年の自由を拘束する点で最も強力な処分である。 ・第１種：心身に著しい障害がない概ね12歳以上23歳未満の者 ・第２種：心身に著しい障害がない犯罪的傾向が進んだ概ね16歳以上23歳未満の者 ・第３種：心身に著しい障害がある概ね12歳以上26歳未満の者 ・第４種：少年院において刑の執行を受ける者

第4章　資料編

データベース

1 IT用語集

総務省　http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/glossary/01.html　2017/12/1

1	あ	重要	アカウント	利用権。コンピュータやソフトウェア，ネットワーク等を使用するための権利や資格のこと。 また，それらのシステムにログインするために必要なIDとパスワードの組み合わせをアカウントと呼ぶこともあります。
2	あ	重要	アクセスポイント	通常は，無線LANアクセスポイントを指します。アクセスポイントは，ノートパソコンやスマートフォン等の無線LAN接続機能を備えた端末を，相互に接続したり，有線LAN等他のネットワークに接続するための機器です。「親機」，「基地局」，「ステーション」等とも呼ばれます。
3	あ		アクセスログ	利用者がソフトウェアやネットワーク機器等に接続した履歴（記録）のこと。 例えば，Webサーバのアクセスログであれば，接続元のIPアドレスや接続日時，閲覧されたファイル名等を確認することができます。
4	あ		アップロード	自分のコンピュータから，ネットワーク上のWebサーバやFTPサーバ等にファイルを保存すること。
5	あ		アドミニストレータ	コンピュータやネットワーク，データベースの管理者，または管理する権限のこと。 管理者とは，あらゆる権限を与えられる利用者を表します。そのため，アドミニストレータ権限を第三者に使用されてしまうと，コンピュータシステムを破壊されたり，格納されているデータを盗まれたり改ざんされたりする可能性があります。
6	あ		アプリケーション	コンピュータのOS上で動作するソフトウェアのこと。 ファイル管理やネットワーク管理，ハードウェア管理，ユーザ管理といった基本的な機能を持つOS（基本ソフト）に対して，ワープロソフトや表計算ソフトといったソフトウェアのことをアプリケーション（応用ソフト）と呼びます。 また，スマートフォンの場合は，ゲームをはじめ，辞書機能や動画再生，文書作成等，さまざまな目的に応じたアプリケーションがあります。「アプリ」と略されて使われる場合もあります。
7	あ	重要	暗号化	大事な情報を他人には知られないようにするため，データを見てもその内容がわからないように，定められた処理手順でデータを変えてしまうこと。暗号化されたデータは，復号という処理によって元のデータに戻すことができます。
8	あ		暗号鍵	データを暗号化するときに使われる鍵のこと。
9	あ		アンチウイルスソフト	ウイルス対策ソフトのこと。
10	い		インターネットサービスプロバイダ	インターネットに接続できるサービスを提供する事業者のこと。 通常，電子メールを送ったり，ホームページを閲覧したりするには，インターネットサービスプロバイダと契約する必要があります。
11	う	重要	ウイルス	他のコンピュータに勝手に入り込んで，意図的に何らかの被害を及ぼすように作られたプログラムのこと。ディスクに保存されているファイルを破壊したり，個人情報等を盗むこともあります。また感染経路として，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や，他人から借りたCDメディアや，USBメモリ，電子メールの添付ファイル，ホームページの閲覧等媒介して感染します。ウイルスにはウイルス対策ソフトでは検出・駆除できないものもあり，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ウイルス自身が自分を複製する仕組みを持っていた場合には，他のコンピュータにウイルスを感染させてしまう危険性もあります。
12	う	重要	ウイルス対策サービス	ウイルスからコンピュータを防御するためのサービスのこと。 多くの場合，インターネットサービスプロバイダ等が提供しています。このサービスを利用することで，ウイルス対策ソフトと同様に，ウイルスのチェックや駆除を行うことができます。
13	う		ウェブアプリケーションファイアウォール	Webアプリケーションに対して行われる外部との通信を監視し，脆弱性（ぜいじゃくせい）への攻撃や情報の窃取等を防御するファイアウォールのこと。 Web Application Firewall（ウエブ・アプリケーション・ファイアウォール）を略して，WAF（ワフ）とも呼ばれています。 一般的なファイアウォールはネットワークレベルで監視していることに対して，WAFはアプリケーションレベルでの監視を行います。Webアプリケーションの脆弱性によって引き起こされるSQLインジェクション等を防ぐことができます。
14	お		オートコンプリート	キーボードの入力を補助する機能のひとつ。過去の入力履歴を参照して次の入力内容を予想し，あらかじめ表示すること。Web ブラウザのアドレス入力等に搭載されています。 また，この機能はパスワードの入力等にも使えますが，情報セキュリティの観点からは第三者でも冒頭の数文字が合うだけでパスワードを入力できてしまいかねません。そのため，オートコンプリートのもととなる入力履歴を消したり，オートコンプリート機能自身を使わないように設定できます。

15	お		オンライン ストレージ	インターネット上にデータを格納するサービスのこと。 Web ブラウザやFTPクライアントソフトを利用してデータをやり取りする方式のほかに，専用のソフトウェアを利用するサービスもあります。
16	か	重要	可用性	認可された利用者が，必要なときに情報にアクセスできることを確実にすること。 国際標準化機構（ISO）が定める標準に定義されるもので，Availability（アベイラビリィティ）の訳語です。
17	か	重要	完全性	情報および処理方法の正確さおよび完全である状態を安全防護すること。 国際標準化機構（ISO）が定める標準に定義されるもので，Integrity（インテグリティ）の訳語です。
18	き		キーロガー	キーボードからの入力を記録するソフトウェア。 最近は，ウイルス等を使ってコンピュータに常駐させることで，ユーザIDやパスワード，クレジットカード番号等を不正に入手するために利用されることが増えています。
19	き	重要	機密性	情報にアクセスすることが認可されたものだけがアクセスできることを確実にすること。 国際標準化機構（ISO）が定める標準に定義されるもので，Confidentiality（コンフィデンシャリティ）の訳語です。
20	き		キャッシュ	データを一時的にメモリやディスク上の領域に格納して，次回のWebサイトへのアクセスの際にサーバにアクセスすることなく表示できる複製されたデータのこと。 サーバへのアクセスを軽減するとともに，表示の高速化が可能となります。
21	き		共通鍵	共通鍵暗号方式で使われる暗号鍵のこと。 暗号化と復号とで同じ共通の鍵を使用するため，こう呼ばれています。
22	き		共通鍵暗号方式	暗号化と復号で同じ鍵を使用する暗号方式のこと。 同じ鍵を持つ人の間で，途中で覗き見されることなくデータを送受信できます。 処理速度が速い半面，相手先ごとに固有の鍵を作成し，管理しなければならないという特性があります。 大きなサイズのデータの暗号化や，限られた特定の相手とのやり取りに使われます。
23	く		クライアント	ネットワーク上で情報やサービスを利用するコンピュータのこと。 通常は，一般利用者が使用するコンピュータがクライアントになります。 なお，クライアントが要求した情報やサービスを提供するコンピュータは，サーバと呼ばれています。
24	く	重要	クラウド コンピューティング	インターネット上のネットワーク，サーバ，ストレージ，アプリケーション，サービス等を共有化して，サービス提供事業者が，利用者に容易に利用可能とするモデルのことです。クラウドコンピューティングには主に仮想化技術が利用されています。
25	く	重要	クラッカー	悪意を持って，システムに不正侵入したり，データの改ざんや破壊等を行ったりする人のこと。
26	く	重要	クラッキング	悪意を持って，システムに不正侵入したり，データの改ざんや破壊等を行う行為。
27	く		グローバル IPアドレス	インターネットにおいて，全世界で固有の番号を持つIPアドレスのこと。 企業や組織内のネットワークでは，利用者が自由に使うことが許可されているプライベートIPアドレスという番号を使用して，コンピュータを管理します。しかし，プライベートIPアドレスでは，インターネット上で数多くのコンピュータが重複することになるため，インターネットに接続する場合には，すべてのコンピュータがグローバルIPアドレスを使用しなければなりません。 現在のアドレス体系では，全世界のコンピュータにグローバルIPアドレスを割り当てるには，アドレスの数が不足しているため，ルータがプライベートIPアドレスとグローバルIPアドレスの変換作業を行います。個人利用者の場合には，プロバイダから一時的にグローバルIPアドレスを割り当ててもらいます。
28	こ	重要	公開鍵	公開鍵暗号方式による暗号化を利用する場合に，相手に渡す鍵のこと。パブリック鍵とも呼ばれます。多くの場合，不特定多数に公開します。
29	こ		公衆無線LAN	駅や街中等，公共の場所で利用できるように設定された無線LANの施設やサービスのこと。
30	こ		コンテンツ	「内容」や「中身」を表す言葉。 インターネットでは，ホームページ上の情報をコンテンツと呼んでいます。また，小説や映画，テレビ番組，音楽等を電子化したデータについてもコンテンツと呼びます。
31	さ		サーバ	ネットワーク上で情報やサービスを提供するコンピュータのこと。 逆に，サーバに対して，情報やサービスを要求するコンピュータをクライアントと言います。 例えば，インターネットでは，Webサーバやメールサーバ，DNSサーバ等が使用されています。
32	し		肖像権	人格権の一部で，自分の写真や絵の使用に関する権利のこと。 たとえば，自分の写真や絵を承諾なしに公開されることを拒否することができます。
33	し	重要	情報セキュリティ ポリシー	情報の機密性や完全性，可用性を維持していくために規定する組織の方針や行動指針をまとめたもの。
34	し		ショルダハッキング	キーボードで入力しているところを後ろから盗み見て，パスワード等の重要な情報を不正に入手する方法。 ショルダハッキングは，ソーシャルエンジニアリングの手法のひとつで，肩越し（ショルダは“肩”の意味）に覗くことから，このように命名されています。

35	し		信頼済みサイト	Webブラウザのセキュリティゾーンのひとつで，あらかじめ信頼できることがわかっているWebサイト用のゾーンのこと。 一般的に信頼済みサイトでは，通常のインターネットサイトに比べて，セキュリティレベルを下げることでプログラム等の実行を可能にします。
36	す		スクリプト	1行ずつ実行される簡易なプログラム言語。 たとえば，JavaScriptやVBScriptといったスクリプト言語を使用することで，ホームページにさまざまな動きを付け加えたり，利用者の操作に合わせた処理を実行できるようになります。
37	す	重要	スパイウェア	利用者の使用するコンピュータから，インターネットに対して個人情報やコンピュータの情報等を送信するソフトウェアのこと。 一般的には，そのようなソフトウェアがインストールされていることや動作していることに利用者が気づいていない状態で，自動的に情報を送信するソフトウェアをスパイウェアと呼びます。
38	す	重要	スパムメール	迷惑メールのこと。
39	せ		生体認証	ひとりひとりが異なる人間の身体的特徴を利用する認証技術全般のこと。 指紋や声紋，虹彩（眼球の模様）を登録しておくことで，本人以外の人間がコンピュータやシステムを利用したり，施錠された空間に入ったりすることができないようにするために利用されます。
40	せ	重要	セキュリティホール	OSやソフトウェアにおいて，情報セキュリティ上の欠陥となる不具合のこと。脆弱性（ぜいじゃくせい）とも呼ばれます。
41	そ	重要	ソーシャル エンジニアリング	人間の心理的な隙等を突いて，コンピュータに侵入するための情報を盗み出すこと。 ソーシャルには“社会的な”という意味があります。ソーシャルエンジニアリングの方法には，さまざまなものがあるため，万全な対策が取りにくいという点に注意しなければなりません。
42	そ		ソーシャルゲーム	メンバーが交流しながら対戦したり，協力しあったりしながら，遊べるゲームのこと。ソーシャルネットワーキングサービスの1つとして提供されることもあります。
43	そ		ソーシャルネット ワーキングサービス	SNSのこと。
44	た		ダウンロード	ネットワーク上のFTPサーバやWebサーバからファイルを取り出して，自分のコンピュータに保存すること。
45	ち		チェーンメール	同じ内容のメールの転送を促す文章が書かれた電子メールのこと。 連鎖メールとも呼ばれています。チェーンメールを送信してしまうと，インターネットで送信される電子メールの数がねずみ算的に増加してしまうため，ネットワークの負担を大きくしてしまう可能性があります。
46	ち		チャット	インターネットで，複数の人と同時に文字やイラストを用いて会話できる仕組みのこと。 チャット（chat）とは“おしゃべり”の意味で，インターネット上のチャットサーバに接続して利用します。
47	ち		著作権	知的財産権のひとつで，著作物に対する著作者の権利のこと。 たとえば，自分の作った画像や撮った写真等を勝手に公開されることを拒否できます。
48	て		データセンター	インターネットに接続するための回線を装備して，顧客のサーバを預かる施設のこと。 場所とインフラを提供するだけでなく，サーバの保守や運用を請け負うこともあります。
49	て		電子掲示板	ネットワークを利用して，複数の人がコンピュータで同じWebページに読み書きを行うことができる仕組みのこと。 業務連絡や友達同士での情報のやり取りに利用されます。省略して，掲示板と呼ばれたり，BBSと呼ばれたりすることもあります。
50	て		電子商取引	インターネットを使用して，商品の売買やサービスの提供等，商業活動を行う仕組みのこと。EC（Electronic Commerce－エレクトロニック・コマース），eコマースとも呼ばれます。 主に，企業と企業で行うBtoB（Business-to-Business）の仕組みと，企業と消費者で行うBtoC（Business-to-Consumer）の仕組みがあります。たとえば，ショッピングサイトやオンライントレードも，電子商取引のひとつです。 電子商取引においては，顧客の情報や購入履歴をデータとして保有することになるため，不正アクセスやデータ漏洩の問題等，もっとも情報セキュリティの強化が要求されているシステムと言えます。
51	て		電子署名	電子署名は，一般に暗号技術の一つである公開鍵暗号方式を利用して作成されます。電子署名は，メッセージの作成者が自分の鍵ペアのうちの秘密鍵（プライベート鍵とも呼ばれる）を使って作成します。メッセージを受信した人は，作成者の鍵ペアのうちの公開鍵（パブリック鍵）を使用して，受信したメッセージを検証します。つまり，作成者本人しか持ち得ない秘密鍵を使ってメッセージが作成されたことを検証することで，作成元の確認ができることになります。電子署名を利用することにより，なりすましやメッセージの改ざんが行われていないことの検証と，否認防止が可能になります。
52	て		電子メール	インターネットを用いて，コンピュータや携帯電話でやり取りする電子版の手紙のこと。 文章を送信するだけでなく，ファイルを添付することができます。なお，HTML形式の電子メールを利用すると，文字の色やサイズを指定したり，文中に画像を挿入すること等が可能になります。
53	と	重要	ドメイン	インターネット上で接続しているネットワークに設定される名前のこと。 本来ドメインは，IPアドレスという数字の範囲によって管理されていますが，IPアドレスは人間にとって判別が困難であるため，“soumu.go.jp.”のようにドメイン名で記述できるようになっています。
54	と		トラフィック	ネットワークを流れるデータの流れのこと。 本来は「往来」や「交通」という意味を持ちます。 通常，ネットワークの混雑具合を説明する際に，「トラフィックが増加する」，「トラフィックが大きい」等の言い方をします。ネットワークのトラフィックが増加すると，ホームページがなかなか表示されなかったり，電子メールの受信に時間がかかったりするようになります。 なお，通信の分野では，通常トラヒックと言います。

55	と		トロイの木馬	コンピュータの内部に潜伏して，システムを破壊したり，外部からの不正侵入を助けたり，そのコンピュータの情報を外部に発信したりするプログラム。 トロイの木馬は感染能力を持つプログラムではないため，本来はウイルスに含まれるものではありませんが，現在では利用者には分からないように悪意のある行為を働くことがあるため，広義の意味で，ウイルスのひとつとして扱われることがあります。
56	に		認証サーバ	利用者が本人であることを確認するためのサーバのこと。 OSやデータベース等にも認証の機能が付属していますが，認証サーバは認証の機能のみを独立して提供するサーバです。 認証サーバと，OSやデータベース等を連携させることによって，シングルサインオンの横断的な認証基盤を導入することができます。
57	は	重要	パーソナルファイアウォール	個人で利用するためのファイアウォール製品。 ソフトウェアとして提供されることが多く，インターネットに接続するコンピュータにインストールして利用します。
58	は		ハイパーリンク	リンクのこと。
59	は	重要	パケット	ネットワークを通して送信されるデータを分割する際に使われる単位のこと。 たとえば，ファイルを他のコンピュータに送信する際には，ファイルのデータをいくつかのパケットに分割して，各パケットにヘッダ情報を付加します。 ヘッダには，IPアドレス等の相手のコンピュータを識別する情報，受信した相手がパケットに分割されたデータを組み立て直すためのそれぞれのパケットの順番情報と，データのエラー補正のための情報等が含まれています。 送信データをパケットに分割することにより，データの送信途中にエラーが発生してデータの再送信が必要になっても，データ全体を再送信するのではなく，パケット単位で再送信を行うだけで済むため，データの転送効率を向上させることができます。 現在の携帯電話では，インターネットの接続料金をこのパケットの単位で課金されることが多いようです。
60	は	重要	パスワード	本人であることを確認するために，ユーザ名とともに入力する文字列。 銀行のキャッシュカードの暗証番号も，一種のパスワードです。
61	は	重要	ハッカー	コンピュータ技術に長けた人のこと。または，コンピュータ技術を利用して，ハッキングを行う人のこと。 本来は，悪い意味の言葉ではありませんでしたが，現在では，悪意を持って，コンピュータの不正利用や攻撃を行うクラッカーと同じ意味でも使われることが増えています。
62	は	重要	ハッキング	高度なコンピュータ技術を利用して，システムを解析したり，プログラムを修正したりする行為のこと。本来は悪い意味を持つ言葉ではありませんでしたが，現在は不正にコンピュータを利用する行為全般のことをハッキングと呼ぶことが増えています。そのような悪意のある行為は，本来はクラッキングと呼ばれます。
63	は		バックアップ	データを磁気テープ等の別の記憶媒体に保存して，大事なデータの複製を作っておくこと。 バックアップを取っておくことで，データが壊れてしまったときに，バックアップ時の状態に復元することができます。
64	は	重要	バックドア	外部からコンピュータに侵入しやすいように，“裏口”を開ける行為，または裏口を開けるプログラムのこと。 このプログラムが実行されてしまうと，インターネットからコンピュータを操作されてしまう可能性があります。 なお，一部のウイルスでは，感染時にバックドアを埋め込むことがあります。
65	ひ	重要	秘密鍵	公開鍵暗号方式による暗号化や電子署名を利用する場合に，他人に見せることなく所有する鍵のこと。プライベート鍵やシークレット鍵とも呼ばれます。
66	ひ	重要	標的型攻撃	特定の組織を狙って，機密情報や知的財産，アカウント情報（ID，パスワード）等を窃取しようとする攻撃です。この攻撃では，標的の組織がよくやり取りをする形式のメールを送りつけ，そこについている添付ファイルやリンクをクリックさせ実行させ，そこからマルウェア配布サイトに誘導する等の手口がよく使われています。
67	ふ		ファームウェア	ハードウェアの基本的な制御のために，コンピュータ等機器に組み込まれたソフトウェアのこと。コンピュータ等の機器に固定的に搭載され，あまり変更が加えられないことから，ハードウェアとソフトウェアの中間的な存在としてファームウェアと呼ばれています。コンピュータや周辺機器，家電製品等に搭載されており，内蔵された記憶装置やメモリ等に記憶されます。パソコンのBIOSもファームウェアの一種です。機能の追加や不具合修正のため，後から変更できるようになっているものが多くなっています。
68	ふ	重要	ファイアウォール	外部のネットワークと内部のネットワークを結ぶ箇所に導入することで，外部からの不正な侵入を防ぐことができるシステムのこと。またはシステムが導入された機器。 ファイアウォールには“防火壁”の意味があります。火災のときに被害を最小限に食い止めるための防火壁から，このように命名されています。 また，ウイルス対策ソフトに機能が統合された，個人向けのパーソナルファイアウォールソフトもあります。
69	ふ	重要	ファイル共有ソフト	複数の利用者によるネットワークでのファイルのやり取りを可能にしたソフトウェア。ファイルの交換は，P2P（ピア・トゥー・ピア）で実行されます。 同じような機能を持つソフトウェアには，ファイル交換ソフトがあります。 厳密な分類としては，WinMXやNapsterのようにクライアントを特定するシステムをファイル交換ソフトと呼び，Winny のようにクライアントを特定しないシステムをファイル共有ソフトと呼びます。 インターネットで利用できるファイル共有ソフトを使用すると，ファイル自体を保管するサーバを用意することなく，必要なファイルを個々のコンピュータ間でやり取りすることができるようになります。 利用者にとっては便利なソフトウェアですが，このようなファイル共有ソフトを利用して，インターネットで音楽，映画，ゲームソフト等，違法なデータがやり取りされ著作権等法令に抵触することもあり，大きな社会問題のひとつになっています。
70	ふ		ファイルサーバ	ファイルを保存して，ファイル共有の機能を提供するコンピュータのこと。 企業や組織では，共有する文書ファイルを保管するために利用しています。

71	ふ	重要	フィッシング	実在の金融機関（銀行やクレジットカード会社），ショッピングサイト等を装った電子メールを送付し，これらのホームページとそっくりの偽のサイトに誘導して，住所，氏名，銀行口座番号，クレジットカード番号等の重要な情報を入力させて詐取する行為のことを言います。
72	ふ		フィルタリング	一般的な意味では「ろ過」することですが，コンピュータやWeb等インターネットの世界では「情報ろ過」を指します。情報ろ過としては，未成年者に対する成人サイトや有害情報サイト等からの保護等が代表的な例です。その他に，コンピュータウイルスや不正アクセスからの保護を主な目的とするファイアウォールも，フィルタリングの一種と言えます。こうしたそれぞれの目的によって，Webサイトの内容に応じて閲覧の制御を行うコンテンツフィルタリングや，ネットワークを行き交うパケットをポリシーに応じて制御するパケットフィルタリング等の手法があります。
73	ふ	重要	復号	暗号化されたデータを元に戻して，人やコンピュータが識別できる情報にすること。
74	ふ	重要	不正アクセス	正規利用権者を識別，認証する電子計算機に，電気通信回線を通じて他人のユーザーID・パスワード等を入力してログインする行為。またこの電子計算機の認証を回避する，いわゆるハッキング行為も含まれる。正規利用権者の承諾を受けてするものは除く。
75	ふ		不正侵入	利用する権限を与えられていないネットワークやコンピュータに侵入して，不正にネットワークやコンピュータを操作する行為のこと。
76	ふ	重要	踏み台	不正侵入の中継地点として利用されるコンピュータのこと。 他人のコンピュータに侵入するときに，直接自分のコンピュータから接続すると，接続元のIPアドレスによって，犯人が特定されてしまう可能性があります。そこで，いくつかのコンピュータを経由してから，目的のコンピュータに接続することで，犯人が自分のコンピュータを探しにくくします。このように，現実的な被害はないけれども，不正侵入の中継地点としてのみ利用されるコンピュータのことを踏み台と言います。
77	ふ		プライバシーの侵害	他人のプライバシーに関する権利を損なうこと。
78	ふ		プライバシーポリシー	ホームページ等で個人情報の扱い方や考え方を明記したもの。 たとえば，ショッピングサイトで買い物するときには，住所や氏名等の個人情報の入力が必要です。そのため，ショッピングサイトでは多くの個人情報が収集されます。これらの個人情報については，ホームページの管理者がプライバシーポリシーを定めて，正しい方法で管理する責任があります。
79	ふ		ブラウザクラッシャ	ホームページの訪問者に対して，連続的に新しいウィンドウを開いたり，電子メールのメッセージウィンドウを開いたりすることで，訪問者のコンピュータに異常な動作をさせるWeb ページのこと。 省略して，ブラクラとも呼ばれています。
80	ふ		フリーウェア	無償で使用できるソフトウェアのこと。フリーソフト，フリーソフトウェアと呼ばれることもあります。主に，インターネットで公開されており，ダウンロードして利用できるようになっています。ただし，利用制限等のあるフリーウェアも存在するので，商用利用の場合等には確認が必要です。
81	ふ		フリーメール	インターネットを通じて無料で提供される電子メールサービスのこと。登録すれば誰でも無料でメールアドレスが割り当てられ，電子メールの送受信が行えるようになります。Web ブラウザを使って受信メールの閲覧やメッセージの作成・送信を行う「Webメール」型のシステムが一般的です。
82	ふ		ブロードバンド	ネットワークにおける広帯域幅を表す言葉。 大容量のデータを高速に流すことができるADSLや光回線等のネットワークやそこで提供されるサービスを指すこともあります。
83	ふ		プロキシサーバ	企業・組織等の内部のネットワークとインターネットの間にあって，直接インターネットに接続できない内部ネットワークのコンピュータに代わって，「代理」としてインターネットとの接続を行うコンピュータ，またはそのための機能を有するソフトウェアのことを言います。
84	ふ		ブログ	インターネット上で公開されている日記形式のホームページのこと。 もともとは，「Web log」（ホームページの履歴の意味）から派生した言葉であると言われています。
85	ふ		プロトコル	ネットワークを介してコンピュータ同士がデータをやり取りするために定められた，データ形式や送受信の手順等の国際標準規則のこと。通信プロトコルとも呼ばれます。 文化や言語が異なる国と国との外交様式の決めごとというのが元々の意味です。コンピュータや通信機器も，メーカーや機種ごとに通信形式が異なると相互に通信が行えないため，ITU-T等の国際機関で標準が決められています。標準に準拠した形で開発されるため，コンピュータや通信機器は，メーカーが異なっても相互に通信を行うことができるのです。
86	へ		ヘッダ	データの先頭にあるデータ自体の内容を表す情報。または，印刷した用紙の上部に固定で印字するタイトル等の文字。 たとえば，電子メールには，本文の前にヘッダの情報があります。電子メールのヘッダには，送信者，送信先，送信日時等の情報が書き込まれています。なりすましやスパムメールの被害にあった場合に，電子メールの送信者を突き止めるための情報として利用できます。
87	へ		傍受	交信者以外の人間が無線の通信内容を入手する行為。 故意または偶然のどちらであっても傍受となります。
88	ほ		ポート	インターネットで情報のやり取りを行うために，使用される番号のこと。ポート番号またはサービス番号とも呼ばれています。 IPアドレスとともに指定される補助用のアドレスで，通常，プロトコルに応じてポートが割り当てられています。 たとえば，FTPはTCPの21番ポート（制御用）と20番ポート（データ用），HTTPはTCPの80番ポート，HTTPSはTCPの443番ポートを使用します。
89	ほ		ホスト名	ネットワーク上の1台1台のコンピュータを識別するための名前のこと。

90	ほ	重要	ボット	コンピュータを外部から遠隔操作するためのコンピュータウイルスの一種。 ボットに感染してしまうと，インターネットを通じて，悪意のあるハッカーにコンピュータを遠隔操作されてしまうことがあります。外部から遠隔操作するという動作から，このようなウイルスのことをロボット（Robot）をもじってボット（BOT）と呼んでいます。
91	ほ		ボットネット	多数のコンピュータウイルスの一種であるボットに感染したコンピュータによって構成される特殊なネットワークのこと。 ボットネットに接続されたコンピュータは，インターネット上から攻撃者が指示を出すことで，迷惑メールの配信や他のコンピュータへの攻撃，情報の窃取等を行うようになります。
92	ま		マクロウイルス	Office アプリケーションで動作する，マクロ機能を使って作成されたコンピュータウイルスの一種。
93	ま	重要	マルウェア	マルウェアとは，「Malicious Software」（悪意のあるソフトウェア）を略したもので，さまざまな脆弱性や情報を利用して攻撃をするソフトウェア（コード）の総称です。コンピュータウイルスと同じ意味で使われますが，厳密にはさらに広義な用語として使われています。ウイルスのほか，ワーム，スパイウェア，アドウェア，フィッシング，ファーミング，スパム，ボット，キーロガー（キーストロークロガー），トロイの木馬，論理爆弾，等さまざまな種類のマルウェアが存在しています。
94	む	重要	無線LAN	ケーブル線の代わりに電波を使ったLANのこと。ADSLや光回線等の敷設が困難な地域への接続手段として伝送距離が2～10kmで，最大伝送速度は最大74.81Mbps，2.5GHz帯や3.5GHz帯，5.8GHz帯を使用するWiMAXという規格もあります。最近では携帯電話等の通信帯域がひっ迫しないようにするオフロード対策のひとつとしても注目されています。
95	め	重要	迷惑メール	利用者が送信を要求していないのにも関わらず，勝手に送りつけてくる商品広告等の電子メールのこと。スパムメールとも呼ばれています。 電子メールを受信する通信料を利用者側が負担しなければならないということもあり，大きな社会問題になっています。
96	め	重要	迷惑メールフィルタ	迷惑メールを取り除く機能のこと。 統合セキュリティ対策ソフトや一部の電子メールソフトに装備されています。受信した電子メールの内容を分析して，迷惑メールと判断された場合に，件名に「SPAM」や「MEIWAKU」等の文字列を追加するという仕組みを提供しています。
97	め		メーラー	電子メールソフトのこと。
98	め		メールサーバ	電子メールを送受信するためのサービスを提供するソフトウェア。または，そのソフトウェアが動作しているサーバ。 主なメールサーバには，電子メールの受信を行うためのPOP3サーバや電子メールの送信や転送を行うためのSMTPサーバがあります。
99	め		メモリ	コンピュータが使用する記憶領域のこと。 コンピュータは，このメモリにプログラムやデータ等を記憶することで処理を実行するようになっています。
100	ゆ		ユーザアカウント	コンピュータやネットワークで，利用者を識別するための情報。 ユーザアカウントには，ユーザ名，パスワード，環境設定，使用権限等が含まれます。
101	ゆ	重要	ユーザ権限	コンピュータやネットワーク上のサービスにおいて，個々の利用者がどのような機能を利用できるかといった使用権限の設定内容のこと。 ユーザ権限を詳細に設定すると，組織やネットワーク内の情報資産を限られたユーザにアクセスを許すように制限できるため，情報セキュリティを強化することができます。
102	ゆ	重要	ユーザ認証	利用者が本人であるかどうかを確認する仕組み。 一般的には，ユーザ名とパスワードでユーザ認証を行いますが，なりすましを困難にするために，最近ではICカードや指紋，声紋，網膜等を利用する技術も登場しています。
103	ゆ		ユーザ名	コンピュータやネットワークに接続する利用者を区別するために，それぞれの利用者に割り当てられた名前。ユーザIDとも呼ばれています。
104	り		リンク	ハイパーリンクの略。Webページの文章内に埋め込まれた，他の関連文章の URL を示すもの。 一般的な Web ブラウザでは，リンクが設定されている文字列には下線と色が付いて表示されます。Web ブラウザでリンクをクリックすることにより，設定された URL のWebページが表示されます。
105	る		ルータ	セグメントと呼ばれるネットワークの単位にネットワークを分割する装置のこと。もしくは，別のセグメントのネットワークへ通信する際の経路情報の管理を行う装置のこと。 ルータは，ネットワークをセグメントに分割することで，セグメント外に不要な通信を流さない役割を担います。また,個々のコンピュータ自身で通信する相手の経路情報を管理させないため,ルータを使うことで,効率的な通信が実現されます。
106	ろ	重要	ログ	コンピュータが保有するユーザの接続時刻や処理内容等を記録したファイル。 通常は，ログを参照することで，コンピュータが正常に動作しているかどうかを管理することができます。 たとえば，Webサーバの場合には，管理しているWebサイトに訪問してきたユーザの情報が格納されます。
107	ろ		ログアウト（ログオフ）	コンピュータやネットワークの利用を終了すること。
108	ろ		ログイン（ログオン）	コンピュータやネットワークの利用を開始するために，利用者が認証を行って，コンピュータを使用可能な状態にすること。 一般的には，ユーザ名とパスワードを用いて，ユーザ認証を行います。
109	わ		ワーム	他のファイルに寄生して増殖するのではなく，自分自身がファイルやメモリを使って自己増殖を行うタイプのウイルスのこと。
110	わ	重要	ワンクリック詐欺	電子メールとWebサイトを利用した詐欺行為のこと。携帯電話やパソコンに送りつけた電子メールによってWebサイトに誘い込み，Webサイトを訪問した人に対して，脅迫めいた手口で料金の振り込みを迫るという詐欺行為です。
111	A		ADSL	Asymmetric Digital Subscriber Line（アシンメトリック・デジタル・サブスクライバ・ライン：非対称デジタル加入者線）の略。 ブロードバンドの回線のひとつ。 現在，光回線とともに，高速な通信回線として普及しています。 通常の音声では使用しない周波数帯を利用することで，通常のアナログの電話回線で高速なデータ転送を可能にしています。

111	A		ADSL	Asymmetric Digital Subscriber Line（アシンメトリック・デジタル・サブスクライバ・ライン：非対称デジタル加入者線）の略。 ブロードバンドの回線のひとつ。 現在，光回線とともに，高速な通信回線として普及しています。 通常の音声では使用しない周波数帯を利用することで，通常のアナログの電話回線で高速なデータ転送を可能にしています。
112	A		AES	米国標準技術局が選定した強固な暗号化アルゴリズム。Advanced Encryption Standard（アドバンスト・エンクリプション・スタンダード）の略。米国標準技術局により，「今後30年以上，暗号として利用可能な強度が見込める暗号化技術」として全世界に対して公募が行われ，集まった提案の中から審査を経て2000年10月に選定されました。
113	A		ASP	Application Service Provider（アプリケーション・サービス・プロバイダ）の略。 インターネット上でアプリケーションを提供するサービスの提供者（事業者）のことを言い，提供されるソフトウェアやサービスのことをASPサービスと言います。
114	B		BCC	Blind Carbon Copy（ブラインド・カーボン・コピー）の略。電子メールの送信先指定方法のひとつ。 ブラインドには“隠れた”，カーボンコピーには“複写したもの”という意味があります。通常の宛先であるTOに指定したユーザ以外に，同じ内容の電子メールを送信する場合に使用します。 CC（カーボン・コピー）と違い，電子メールのほかの受信者には，同じ内容の電子メールがBCCに指定したユーザにも送信されているということは通知されません。 そのため，他の受信者には，そのユーザに電子メールを送っているということを隠しておきたい場合に利用できます。
115	B		Bluetooth	パソコンや，スマートフォン，携帯電話等で，数メートル程度の離れた機器の接続に使われる短距離無線通信技術のひとつ。IEEE 802.15.1として標準化されています。ケーブルを使わずに接続し，音声やデータをやり取りすることができます。
116	C		CC	Carbon Copy（カーボン・コピー）の略。電子メールの送信先指定方法のひとつ。 カーボンコピーには，“複写したもの”という意味があります。通常の宛先であるTOに指定したユーザ以外にも同じ内容の電子メールを送信する場合に使用します。 電子メールの受信者は，同じ内容の電子メールがCCに指定されたメールアドレスに送信されていることがわかります。
117	C	重要	Cookie（クッキー）	ホームページを閲覧した際に，Webサーバが利用者のコンピュータに保存する管理用のファイルのこと。利用者の登録情報や今までのショッピングカートの内容等を利用者のコンピュータに保存しておくことで，次回その利用者が同じWebサイトを訪問した場合に，それらのデータを利用できるようにする仕組みです。 たとえば，Cookieを利用すると，ログイン情報を保管することもできるため，次回利用するときにログイン処理を省略できるようになるといった利点があります。
118	D	重要	DDoS攻撃（ディー・ドス・こうげき）	Distributed Denial of Service attack（ディストリビューテッド・デナイアル・オブ・サービス・アタック）。分散サービス拒否攻撃のこと。 Webサーバやメールサーバ等に対して，複数のコンピュータから大量のサービス要求のパケットを送りつけることで，相手のサーバやネットワークに過大な負荷をかけ，使用不能にします。 同様の攻撃方法であるDoS攻撃は1台のコンピュータから実行するものですが，DDoS攻撃の場合は，例えば第三者のコンピュータをボットに感染させておく等して，攻撃者の指示によって複数のコンピュータ(ボット)が一斉に攻撃します。
119	D		DHCP	Dynamic Host Configuration Protocol（ダイナミック・ホスト・コンフィグレーション・プロトコル）の略。 LANに接続するコンピュータやデバイス等に対して，IPアドレスを始めとして，ホスト名や経路情報，DNSサーバの情報等，通信に必要な設定情報を自動的に割り当てるプロトコルのこと。
120	D	重要	DNS	Domain Name System（ドメイン・ネーム・システム）の略。“soumu.go.jp.”等のドメイン名をIPアドレスに変換する仕組みのこと。 インターネットに接続されたコンピュータは，数字で構成されるIPアドレスで通信を行いますが，ドメイン名はIPアドレスとは異なり，“soumu.go.jp.”のような文字列で記述できるため，人間にとって扱いやすいことから，ドメイン名とIPアドレスとの対応付けを行うDNSという仕組みが作られました。
121	D	重要	DoS攻撃（ドス・こうげき）	Denial of Service（デナイアル・オブ・サービス）攻撃の略。サービス拒否攻撃のこと。攻撃者は，Webサーバやメールサーバ等に対して大量のサービス要求のパケットを送りつけ，過大な負荷をかけて相手のサーバやネットワークを使用不能にします。
122	E		EXE（エグゼ）	Windows で実行可能なファイルに付けられる拡張子。“実行”を意味するExecute（エクゼキュート）の先頭3文字からつけられています。
123	F		FTP	File Transfer Protocol（ファイル・トランスファー・プロトコル）の略。他のコンピュータとファイルを送受信するためのプロトコルのこと。 トランスファーには“転送する”，プロトコルには“規約”という意味があります。 FTPは，インターネットで主に大きなサイズのファイルの送受信を行うときに，標準的に利用されています。
124	G		GPS	Global Positioning System（グローバル・ポジショニング・システム）の略。人工衛星を利用して自分が地球上にいる位置を正確に測定できるシステムです。日本語では「全地球測位システム」と呼ばれています。
125	H		HTML	Hyper Text Markup Language（ハイパー・テキスト・マークアップ・ランゲージ）の略。ホームページを作成するための言語。 HTMLには，文字だけでなく画像や音声を埋め込むことができます。HTML形式のファイルは，Web ブラウザで閲覧することができます。また，HTML形式のファイルに埋め込まれたリンクをクリックすることで，参照先等のWebページに移動できます。

126	H		HTMLメール	HTMLで記述された電子メール。 通常の電子メールとは異なり，文字だけでなく，文字の大きさや色，レイアウトを工夫した電子メールを作成することができます。また，通常のホームページと同様に，さまざまな動作を実行するスクリプトを埋め込むこともできます。
127	H		HTTP	Hyper Text Transfer Protocol（ハイパー・テキスト・トランスファー・プロトコル）の略。Web ブラウザが，Webサーバに対してHTML形式のファイルを受け取るためのプロトコル。 トランスファーには“転送する”という意味があります。
128	I		ICT	Information and Communication Technology（インフォメーション・アンド・コミュニケーション・テクノロジー）の略。情報通信技術のこと。従来から使われていたIT（Information Technology:インフォメーション・テクノロジー）に替わって，通信ネットワークによって情報が流通することの重要性を意識して使用される言葉です。
129	I		ID	identification（アイデンティフィケーション）の略。個人を識別・把握する情報の総称のこと。ユーザ名，ユーザIDとも呼ばれます。
130	I		IPS	Intrusion Prevention System（イントリュージョン・プリベンション・システム）の略。侵入防止システムのこと。
131	I	重要	IPアドレス	コンピュータをネットワークで接続するために，それぞれのコンピュータに割り振られた一意の数字の組み合わせのこと。 IPアドレスは，127.0.0.1のように0～255までの数字を4つ組み合わせたもので，単にアドレスと略されることがあります。 現在主に使用されているこれらの4つの数字の組み合わせによるアドレス体系は，IPv4（アイ・ピー・ブイフォー）と呼ばれています。また，今後情報家電等で大量にIPアドレスが消費される時代に備えて，次期規格として，IPv6（アイ・ピー・ブイシックス）と呼ばれるアドレス体系への移行が検討されています。なお，IPv6では，アドレス空間の増加だけでなく，情報セキュリティ機能の追加等の改良も加えられています。
132	I		ISO	International Organization for Standardization（インターナショナル・オーガニゼーション・フォー・スタンダーディゼーション）のこと。 電気および電子技術分野を除く全産業分野（鉱工業，農業，医薬品等）における国際標準の策定を行う国際標準化機関です。 略称が英文名称の頭文字語「IOS」ではなく「ISO」になっているのは，ギリシャ語で「平等」を意味する「isos」という言葉が起源のためです。
133	I		ISP	インターネットサービスプロバイダのこと。
134	I		IT	Information Technology（インフォメーション・テクノロジー：情報技術）の略。コンピュータやネットワークに関わるすべての技術を総称する言葉として使用されています。
135	J		Java（ジャバ）	サン・マイクロシステムズ社が1995年に発表したプログラミング言語。 Javaは，どのコンピュータ上でも動作することを目的に開発された言語です。Javaで開発されたプログラムは，Java仮想マシン（Java Virtual Machine）と呼ばれる仮想環境上で動作するため，OSに関係なく同じプログラムを実行することができます。 現在は，パソコンだけでなく，携帯電話のアプリケーション等でも利用されています。
136	J		JavaScript（ジャバスクリプト）	ネットスケープ社とサン・マイクロシステムズ社が共同で開発したホームページに埋め込むことができるスクリプト言語。 JavaScriptは，静的な文字と画像しか表示できなかったWebページに，動きを付け加えたり，利用者の操作に合わせた処理を実行できるようにしたりすることを目的として開発された言語です。 Javaが言語のベースになっているため，Javaという名前が付いていますが，実際にはまったく別の言語です。現在は，事実上のWebページ用の標準的なスクリプト言語となっています。
137	L		LAN	Local Area Network（ローカル・エリア・ネットワーク）の略。同じ建物内等の比較的近い距離でコンピュータを接続するネットワークのこと。LAN を導入すると，同じ LAN に接続しているコンピュータとのファイル共有や，プリンタの共有等を行うことができます。
138	M		Mac OS	アップル社のパーソナルコンピュータMacintoshに搭載されているOS。
139	M		MDM	Mobile Device Management（モバイル・デバイス・マネジメント）の略。 主に企業や組織等で，スマートフォンやタブレット端末等の携帯端末を安全に管理する仕組みのこと。スマートフォンやタブレット端末は，企業や組織の外に持ち出され，さまざまな環境や場所で利用されることから，紛失・盗難時の対策等，端末内の情報を安全に管理するためのさまざまな機能があります。
140	O		OS	Operating System（オペレーティング・システム）の略。コンピュータを動作させるための基本的な機能を提供するシステム全般のこと。 たとえば，メモリやディスク等のハードウェアの制御，キーボードやマウスといったユーザインタフェースの処理，画面への表示とウィンドウの制御等，コンピュータが動作するための数多くの基本処理を行っています。さらに，コンピュータシステムを管理するための数多くのツールが用意されています。代表的なOSには Windows，Mac OS 等があります。
141	P	重要	P2P（ピー・ツー・ピー）	Peer To Peer（ピア・ツー・ピア）の略。コンピュータの世界では，toがtwoと同じ発音であることから，“to”を“2”に置き換えた命名を行うことがあります。 P2Pとは，不特定多数のコンピュータを直接接続して情報をやり取りするタイプのシステム提供方式のことです。インターネットの世界では，これまでサーバとコンピュータが連携した情報提供方法 が採用されていましたが，最近では，P2Pを利用したシステムも増えてきました。たとえば，音楽配信サービスのNapster，データ配信サービスの Winny 等がP2Pのシステムです。 サーバとコンピュータが連携した情報提供を行うシステムでは，サーバという情報を管理するコンピュータが決められていましたが，P2Pの仕組みではすべてのコンピュータがそれぞれ情報を配信するサーバの役割を果たします。
142	P		POP3（ポップ・スリー）	Post Office Protocol - Version 3（ポスト・オフィス・プロトコル・バージョン・スリー）の略。 メールサーバに保存されている電子メールを電子メールソフトが取りに行く際に利用されるプロトコルです。

143	S		SMTP	Simple Mail Transfer Protocol（シンプル・メール・トランスファー・プロトコル）の略。電子メールの送信と転送を行うためのプロトコル。 Windows が搭載されているコンピュータと Mac OS が搭載されているコンピュータや，携帯電話とパソコンといった異なった機種の間でも電子メールのやり取りができるのは，このプロトコルに準拠しているためです。
144	S		SNS	Social Networking Service（ソーシャル・ネットワーキング・サービス）の略。登録した利用者だけが参加できるインターネットのWebサイトのこと。
145	S	重要	SQL インジェクション	SQLとは，データベースを操作するためのプログラミング言語のこと。インターネットのWebサイト等の入力画面に対して，直接SQL命令文の文字列を入力することで，データベースに不正アクセスを行い，情報の入手や，データベースの破壊，Webページの改ざん等を行うこと。これはWebアプリケーションにおけるエスケープ処理が適切に行われていない脆弱性を狙った攻撃で， 最近では，SQLインジェクションによる情報漏洩事件や，Webページの改ざんにより正規のWebサイトにウイルスを埋め込まれる事件が増加しています。
146	S		SSH	Secure Shell（セキュア・シェル）の略。ネットワークを介して別のコンピュータにログインしたり，遠隔地のコンピュータから命令を実行したり，他のコンピュータへファイルを移動したりするためのプログラムのこと。 SSHを利用するとネットワーク上を流れるデータは暗号化されるため，インターネット経由でも安全に操作を行うことができます。
147	S	重要	SSID	Service Set Identifier（サービス・セット・アイデンティファイア）の略。無線LANで特定のコンピュータや通信機器で構成されるネットワークを指定して，接続するためのユニークな識別コードのこと。ESS ID（イー・エス・エス・アイ・ディ）とも呼ばれています。 無線LANで送信するパケットのヘッダに含まれ，受信側は，SSIDが一致しない場合は，そのパケットを無視するため通信ができません。
148	S	重要	SSL	Secure Socket Layer（セキュア・ソケット・レイヤ）の略。 インターネットにおいてデータを暗号化したり，なりすましを防いだりするためのプロトコルのこと。ショッピングサイトやインターネットバンキング等，個人情報や機密情報をやり取りする際に広く使われています。 利用者は，認証機関により発行されたサーバ証明書によって，サーバの真正性を確認します。現在は，SSL3.0をもとに改良が加えられたTLS1.2が標準的なプロトコルとして利用されています。
149	T		TCP	Transmission Control Protocol（トランスミッション・コントロール・プロトコル）の略。インターネットで使用されているプロトコルのひとつ。 TCPは，相手と接続を確立してから通信を行うため，UDPに比べて信頼性が高いプロトコルです。TCPは，HTTPやFTP，SMTP，POP3といった，インターネットにおける主要なサービスで使用されるプロトコルの基盤となっています。
150	T		TO	電子メールの送信先指定方法のひとつ。 TOには，電子メールの通常の送信先のメールアドレスを記述します。電子メールの宛先は，TO以外に，CCやBCCに指定することができます。
151	U		UDP	User Datagram Protocol（ユーザ・データグラム・プロトコル）の略。インターネットで使用されているプロトコルのひとつ。 インターネットを利用するアプリケーション等の通信では，TCPとUDPのいずれかのプロトコルが使用されています。UDPは，TCPに比べてシンプルなプロトコルであるため，高速ですが信頼性が低いという特徴があります。そのため，確実なデータ転送が要求されるWebや電子メールでは，TCPが使用されています。
152	U		UPS	Uninterruptible Power Supply（アンインタラプティブル・パワー・サプライ）の略。無停電電源装置のこと。
153	U		URI	Uniform Resource Identifier（ユニフォーム・リソース・アイデンティファイヤ）の略。インターネット上で情報が格納されている場所を示すための住所のような役割を果たす文字列のこと。 HTML4 の仕様より URL を拡張した URI が定義されたことから，徐々に URI という表現を見かけるようになっています。
154	U	重要	URL	Uniform Resource Locator（ユニフォーム・リソース・ロケータ）の略。インターネット上で情報が格納されている場所を示すための住所のような役割を果たす文字列のこと。 URL は，Web ブラウザ等でホームページを閲覧するときの指定に利用されます。プロトコル名，ホスト名，パス名で構成されます。 たとえば，“http://www.soumu.go.jp/index.html” のように記述します。
155	U		USB	Universal Serial Bus（ユニバーサル・シリアル・バス）の略。コンピュータにさまざまな周辺機器を接続することができる外部ポートの規格。 USBには，コンピュータの電源を切らずに，機器を抜き差しできるという特徴があります。 USBのポートには，CD-ROMドライブ，ハードディスク，光磁気ディスク等のドライブ類から，マウス，キーボード等のインターフェースまで，数多くの周辺機器を接続することができます。 当初使用されていたUSB1.1という規格では，転送速度が最大12Mbpsと比較的低速なものであったため，ハードディスク等の高速なドライブの接続にはあまり適しませんでしたが，現在は転送速度を最大5Gbpsまで可能にしたUSB3.0 という規格が登場したため，さらに数多くの対応機器が登場してきています。
156	U		USB 媒介ウイルス	USB メモリ等をコンピュータに差し込んだだけで感染するウイルスのこと。 USB媒介ウイルスは，感染したコンピュータに差し込まれた他の USB メモリに感染する形で広がっていきます。なお，USB メモリだけでなく，記憶領域を持つ外付けハードディスクやデジタルオーディオプレーヤー等でも感染します。
157	U	重要	USB メモリ	コンピュータのUSB端子に接続して利用できる小さなメモリデバイスのこと。 USB端子に接続するだけで，外部ドライブとして簡単に読み書きができる。消しゴム程度のサイズであるため，手軽に利用できるという利点はありますが，その分だけ盗難や紛失の危険性が高く，情報セキュリティ上のリスクが高いという欠点があります。また，最近はUSBメモリをターゲットにした USB 媒介ウイルスが発生しています。USB 媒介ウイルスは，コンピュータにUSBメモリを差し込んだだけでウイルスに感染してしまうものです。

159	W		Webアプリケーション	Web ブラウザを利用して，Webサーバに接続することで，動作するアプリケーションソフトのこと。Webサーバは，Web ブラウザからの要求やデータ送信に応じて，動的にコンテンツを配信したり，データを格納したりします。
160	W		Webサーバ	HTMLファイルや画像ファイル等を格納して，利用者の要求によって，Webページを送信するソフトウェア。または，そのソフトウェアが動作しているコンピュータのこと。 本来のWebサーバは，コンテンツを送信する機能だけしか持っていませんでしたが，最近のWebサーバではプログラムを利用することで，利用者の要求に合わせた情報を送信することができるようになっています。
161	W		Webサイト	ホームページのサービスを提供しているシステムやサーバのこと。
162	W		Web ブラウザ	ホームページを閲覧するためのソフトウェア。代表的なソフトとして，Internet ExplorerやGoogle Chrome，Firefox，Safari等があります。
163	W		Webページ	HTMLで記述されたファイルのこと。 ホームページでは，多くの Web ページが公開されています。利用者は Web ブラウザを使用して，これらの Web ページを閲覧することができます。
164	W		Webメール	ホームページを閲覧するWeb ブラウザで利用可能な電子メールシステムのこと。 メールの閲覧や，新規メッセージの作成・送信等を Web ブラウザで行いますが，通常の電子メールと違ってメールの内容をサービス提供事業者側のサーバで管理するため，利用者はインターネットを使って，どこからでもメールをチェックしたり過去のメールを参照したりできる利点があります。
165	W		WEP	Wired Equivalent Privacy（ワイアード・エクイヴァレント・プライバシー）の略。無線LANの規格であるIEEE802.11で採用されている暗号化方式。 無線LANは無線区間内での傍受が簡単であるため，暗号化によって送信されるデータの解読を困難にする必要があります。 しかし，WEPは現在では容易に解読可能とされていますので，なるべく使用しない方が良いでしょう。
166	W	重要	Wi-Fi（ワイ・ファイ）	無線通信の国際標準通信規格で，IEEE 802.11シリーズ（IEEE802.11a / IEEE802.11b / IEE-E802.11g / IEEE802.11n / IEEE802.11ac 等)を利用した無線通信のこと。業界団体のWi-Fi Allianceが発行しており，相互接続性等に関する試験をパスした装置には，このロゴの表示が許可されています。
167	W		WiMAX	無線を使ったブロードバンドモバイル通信規格の1つで，ADSL並みの速度と料金でデータ通信ができる技術として注目されています。WiMAXは，従来は10～66GHzの周波数帯を使用していましたが，IEEE802.16aという規格では2～11GHzを利用するよう改められています。また，見通しのきかない範囲にある端末とも通信できるよう改良されています。通信速度や最大距離は変わらず，1台のアンテナで半径約50km（30マイル）をカバーし，最大で70Mbpsの通信が可能になっています。
169	W		Windows Update	Windows に搭載されているOSやソフトウェアの更新補助機能。インターネットに接続している環境であれば，Windows Update を実行することで，現在のコンピュータの環境やインストールされているソフトウェアに応じて，更新が必要なプログラムをダウンロードし，インストールしてくれます。
171	W		WPA	無線LANの暗号化方式「Wi-Fi Protected Access」（ワイファイ・プロテクテッド・アクセス）のひとつで，従来のWEP方式によるSSIDとWEPキーに加えて，ユーザ認証機能を備え，暗号鍵を一定時間ごとに自動的に更新する「TKIP」（Temporal Key Integrity Protocol）と呼ばれる暗号化プロトコルを使用しています。 WPAには，家庭等小規模なネットワークを想定したWPA-PSKと，企業等の大規模なネットワークで利用されるWPA-EAPがあります。
172	W	重要	WPA2	無線LANの暗号化方式「Wi-Fi Protected Access」（WPA）の新バージョン。暗号化には，WPAより強度の高い「AES」を採用しており，128～256ビットの可変長鍵を利用した強力な暗号化が可能です。WPA2には，家庭等小規模なネットワークを想定したWPA2-PSKと，企業等の大規模なネットワークで利用されるWPA2-EAPがあります。

2 主なSNSサービスの概要と用語

◆ この資料は，対象となる各SNSサービス及びその運営者が発行したものではありません。

公式サイトの情報に加え，公開日が平成29年１月から平成30年１月までのインターネット上の記事を基に，使い方やトラブル事例から必要と思われる機能の情報を掲載しています。

なお，各機能は変更されることがありますので，必要に応じ各サービスの公式サイト等を確認してください。

Twitter

サービスの概要	「ツイート」（つぶやきと訳される）と呼ばれる280文字（日本語は140文字）以内のメッセージや画像，動画等を投稿するサービス。友人や有名人を「フォロー」して生活の一部を垣間見たり，相互に情報交換するという使い方がされる。リアルタイムの情報収集を目的とした利用も多い。短文で手軽にツイートできることが魅力。
匿名性	あり。匿名登録が基本のため，攻撃的な投稿がある。
タイムライン	ツイートの表示領域。複数のツイートが時系列に並ぶ。
ホーム	自分専用のタイムライン。友達にも公開されている。
公開範囲	「公開」「非公開」の設定ができる。「非公開」の場合は自分のフォロワーだけが閲覧可能となる。
いいね！	友達等の投稿に好意や励まし等を簡単に表す機能。Favoriteから「ふぁぼる」と表現される。
フォロー	指定したユーザーのツイートを継続的に自分の画面に表示させる仕組み。
フォローリクエスト	ツイートを非公開にしているユーザーをフォローするには，フォローリクエストを送って承認を得る必要がある。
リツイート	既に投稿されているツイートを再びツイートすること。他のユーザーへの紹介や拡散目的で使用される。自分のフォロワーのタイムラインに表示させることができる。「拡散希望」に応じる場合リツイートする。
タグ・ハッシュタグ	＃記号と，半角英数字で構成される文字列のことをハッシュタグと呼ぶ。ツイートに「＃○○」と入れて投稿すると，その記号つきの発言の検索が容易になる。
タグ付け	ツイートに画像を添付する際，ユーザーと画像を紐づけする機能。例えば「このユーザーがこの写真の人物」と記録したいときに使用する。
リプライ	「@ユーザー名」から始まるツイートで，そのユーザーに宛てたツイートであることを示す。このツイートは自分と相手の共通フォロワーに表示される。

ツイッター	
知り合いかも・おすすめユーザー	アップロードした連絡先の情報や，住んでいる地域の登録情報，フォローしているユーザー等，ユーザー間で共通している情報からフォローを勧める機能。
グループ	ダイレクトメッセージを複数人で行うための登録
ダイレクトメッセージ	フォローし合ってる人の間で直接メッセージが送信し合える機能。非公開。グループに登録して複数間で送受信する機能もある。
リスト	特定のユーザーを選んで，そのユーザーだけで構成されるタイムラインを作ることができる機能 。リストの内容は，非公開にしない限りプロフィール画面に表示される。
ブロック	ツイート等を表示させない機能。フォローが相互に強制解除，相手のツイートが表示されない，相手のフォロー，リストやお気に入りへの追加，プロフィールの閲覧等ができない，といったことが行われる。
アクティビティ	ツイートアクティビティ。いいねやリツイートされた件数が表示され，自分のツイートの影響力を把握するのに使われる。

facebook

サービスの概要	実名登録が基本で，共通の友達や職歴・学歴，連絡先等の情報から自動的に互いを紹介する機能があり，古い知人や共通の趣味を持つ人との交流が促進される。実名登録であること等から，比較的トラブルが少ないと言われる。
匿名性	なし。上記のとおり実名登録が基本で，それを良しとするユーザーが使用するためトラブルが起きにくい。ただし偽名で登録する方法は存在する。
タイムライン	自分のプロフィールやこれまでの自分の投稿文や写真，いいね！した投稿等が表示される自分の履歴のような機能。他のユーザーから閲覧されたり，自分のタイムラインに投稿されることがある。ツイッター等のタイムラインとは機能が異なる。
ニュースフィード	Twitterやインスタグラムのタイムラインに相当する。友達やフォローしているアカウントの更新情報が一覧表示される。
公開範囲	投稿やプロフィール項目ごとに,公開するか,友達まで知らせるかといった公開範囲を細かく指定できる。大きく分けて，自分だけ・友達まで・友達の友達まで・一般公開の４種類。
いいね！	友達等の投稿に好意や励まし等を簡単に表す機能。他のユーザーを「いいね」した場合，ニュースフィードに追加される。
友達	相手に友達申請を送り，相手が承認することで「友達」という関係になる。友達にしか公開していない投稿を見ることができるようになる。
コメント	投稿に対して文章で返答する機能。自分の投稿にコメントできるユーザーを，「誰でも」「友達」「友達の友達」のいずれかに制限することができる。
フォロー	自分のニュースフィードに表示させる機能。芸能人等投稿をチェックしたいユーザーに対して行うことで，ニュースフィードに表示されるようになる。
フォロワー	あるユーザーをフォローしているユーザーのこと。
シェア	友達等の投稿に自分のコメントを付けたうえで投稿すること。他の友達にも教えたいときに使用する。
タグ・ハッシュタグ	「#」＋文字列のことをハッシュタグと呼ぶ。ツイートに「#○○」と入れて投稿すると，その記号つきの発言の検索が容易になる。

フェイスブック	
タグ付け	投稿したことの通知機能。投稿とユーザーを「タグ付け」することで，投稿をそのユーザーに通知する。
メンション	特定のユーザーやグループに向けたメッセージであることを示す機能。「@」＋ユーザー名又はグループ名，先頭が大文字のユーザー名を付けて投稿すると，そのユーザーやグループに通知される。
知り合いかも・おすすめユーザー	共通の友達や職歴・学歴，所属しているネットワーク，連絡先等の情報等，ユーザー間で共通する情報を基にフォローを勧める機能。「友達の友達」等直接の関係が薄くても紹介され得る。
グループ	家族や友達等少人数のグループでのコミュニケーション機能。公開（閲覧自由）・非公開（グループメンバー以外にはグループ名，参加メンバーのみ公開）・秘密（グループメンバー以外には一切非公開）の三つの状態を選択できる。
メッセージ	一般的な電子メールに似た機能。指定したユーザー以外には非公開。
Facebookページ	主に企業やサービスの名前で表示，掲載するページ。企業の宣伝等で使用されることが多い。実名登録の必要がない。
リスト	特定のユーザーを選んで，そのユーザーだけで構成されるタイムラインを作ることができる機能 。リストの内容は，非公開にしない限りプロフィール画面に表示される。
ブロック	相手がFacebook上に存在しなくなる機能。友達リスト等からも削除される。またURLを直接入力してもアクセスできなくなる。ただし過去のメッセージ等,一部残るものがある。
アクティビティ	アクティビティログ。ユーザーの行動記録。

インスタグラム

サービスの概要	スマートフォンで撮影した画像や動画の投稿に特化したサービス。写真に簡単なコメントを付けて投稿する。
匿名性	あり。ただしアカウント登録にFacebook・電話番号・メールアドレスのいずれかが必要。Facebookと連携して使用するユーザーが多いことや，自画撮りを投稿する目的のユーザーが多いことから，完全に匿名で使用するユーザーは比較的少ないと言われる。また潜在的にセンスの良い写真を投稿したい，良く見られたいとの欲求があるため，批判を受けるような投稿が少なく，「炎上」が起きにくいと言われる。
タイムライン	フォローしている相手の投稿が，おすすめ順（関心の高い順）に表示される機能。
公開範囲	基本的に全てのユーザーに公開状態にある。非公開にするにはその設定を行う必要があり，フォローリクエストに承認した場合にそのフォロワーにのみ公開される。
いいね！	友達等の投稿に好意や励まし等を簡単に表す機能。いいねするとお気に入りに登録される。また相手が自分の投稿にいいねをすると，「アクティビティ」の機能により誰がしてくれたのかを表示できる。

インスタグラム	
コメント	投稿に対して返答する機能。自分の投稿にコメントできるユーザーを，「誰でも」「フォロー中の人とフォロワー」「フォロー中の人」「フォロワー」のいずれかに制限することができる。
フォロー	特定のユーザーの投稿がタイムラインに表示されるようになる仕組み。投稿を非公開にしているユーザーをフォローするにはフォローリクエストを送る必要がある。
フォロワー	あるユーザーをフォローしているユーザーのこと。 お互いフォローし合っている場合は，相互フォローという。
フォロー リクエスト	投稿を非公開にしているユーザーをフォローするために承認を求める送信。
アンフォロー	フォローをやめること。
タグ・ ハッシュタグ	「#」＋文字列のことをハッシュタグと呼ぶ。ツイートに「#○○」と入れて投稿すると，その記号つきの発言の検索が容易になる。
タグ付け	写真とユーザーを紐づけする機能。例えば「このユーザーがこの写真の人物」と記録したいときに使用する。
メンション	特定のユーザーに向けたメッセージであることを示す機能。「@ユーザー名」を付けて投稿すると，そのユーザーのアクティビティフィードに通知される。
知り合いかも・ おすすめユーザー	影響力のあるユーザーや，自分と趣味や興味が共通するユーザーのフォローを勧める機能。自分がフォローしているユーザーがフォローしているユーザーは趣味が似ている，として勧めていると思われる。
ダイレクト メッセージ	ユーザー間で直接メッセージの送受信ができる機能。グループに登録することで複数での送受信ができる。フォローしていない相手への送信ができ，またユーザーを指定して受信を拒否する機能もある。送信側には既読マークがつく。
ブロック	自分の投稿を相手に見られなくする機能。フォローが相互に強制解除，ユーザーが検索できない，投稿が全て非表示，といったことが行われる。
ピク（pic）	写真のこと。
ポスト（post）	投稿のこと。
アクティビティ	アクティビティ。自分や他のユーザーの行動記録（いいね！やフォロー等）。フォローしているユーザーの行動記録や，自分の投稿等に関する他のユーザーの反応等を表示する。
リポスト （repost）	再投稿。公式にはない機能で，他のアプリを利用する。
位置情報	投稿に，その場所の情報を追加する機能。
ストーリー	インスタグラムの新機能であるストーリーズを利用した投稿を指す。ストーリーズは投稿後24時間経過すると自動で削除される投稿形式であり，通常投稿とは異なるタイムラインへの投稿が可能。
スナップチャット	友達に共有したい写真や10秒以内の動画を撮影してその場で送ること。選択した友達のアカウントにのみ送ることができる。
バトン	ユーザー間で特定のテーマを出題し，テーマに沿った投稿を行うこと。投稿内容に「#バトン」というタグと出題したい相手を明記してやり取りされる。
インスタ ジェニック	写真写りのよい状態を指す「フォトジェニック」が転じた言葉で，「インスタグラムに生える物品や風景」を指す。
インスタグラマー	特に多くのユーザーにフォローされている影響力を持ったユーザーを指す。
Hl4l	#Like for like＝いいなと思ったら「いいね！」してねの略。

LINE

サービスの概要	メッセージを文字で送信する「トーク」や，音声での「通話」を無料で利用できるコミュニケーションツール。ゲームや音楽等関連サービスもある。トーク等ができるのは，LINE上で「友達」として登録したユーザー間のみ。本来メッセージの送受信サービスであるが，「タイムライン」にSNSの機能がある。
匿名性	あり。だたしユーザーIDが携帯電話の番号かFacebookのアカウントと紐づけされる。またタイムラインへの表示は基本的に友達かグループのメンバーであるため，匿名性は低い。
タイムライン	SNSとして使用される機能で投稿が時系列で表示される。 基本的に友達かグループのメンバーによる限定的なSNS機能。友達の投稿に対して，テキスト，画像，「スタンプ」を投稿することができる。
ホーム	自分専用のタイムライン。友達にも公開されている。
公開範囲	基本的に自分が登録している友達の範囲かグループに限定されるが，「全体に公開」に設定することで全てのLINEユーザーに公開される。
いいね！	友達等の投稿に好意や励まし等を簡単に表す機能。他のユーザーを「いいね」した際に「友達のタイムラインにシェア」にチェックしていれば，友達のタイムラインに「〇〇がこの投稿を気に入っています」と表示される。
友達	LINEのアプリを通して連絡がとり合える登録ユーザー。自分のLINEの「友達」に追加すると，メッセージのやりとりを行ったり，相手を「グループ」に招待することができる。友達の追加は，自分の携帯電話の電話帳から登録するか，「LINE　ID」を利用した登録の方法がある。タイムラインではフォローに相当する。LINEを利用している相手が，自分を友達に追加した場合は「知り合いかも？」の欄にその相手が表示されることで，登録メンバーが広がる。
コメント	タイムラインの投稿に対するメッセージ。投稿者にコメントしたことが通知される。
シェア	タイムラインに流れてきた投稿を，自分の友達やグループで共有すること。再投稿する方法と，「いいね」スタンプを押すことで共有される方法がある。また自分の投稿が「全体に公開」の設定になっている場合で，いいねを押したユーザーが「友達のタイムラインにシェア」にチェックしていれば，そのユーザーの友達のタイムラインに「〇〇がこの投稿を気に入っています」と表示されることになり，自分の投稿が思わぬ範囲に拡散してしまうおそれがある。
タグ・ ハッシュタグ	「#」＋文字列のことをハッシュタグと呼ぶ。ツイートに「#○○」と入れて投稿すると，その記号つきの発言の検索が容易になる。
タグ付け	写真とユーザーを紐づけする機能。例えば「このユーザーがこの写真の人物」と記録したいときに使用する。
メンション	特定のユーザーに向けたメッセージであることを示す機能。「@ユーザー名」を付けて投稿すると，そのユーザーに「〇〇がコメントしました」と通知される。
知り合いかも・ おすすめユーザー	連絡先の情報や，自分のことを登録しているユーザー，グループには登録しているが友達には登録していないユーザー等を紹介する機能。
グループ	主にグループでのトークを目的に，ユーザーを登録する機能。グループのメンバー全員で管理しており，メンバーであれば，グループ名の変更やグループへの招待，他のメンバーの強制退会等を自由にできる。
ブロック	トークやタイムラインを非表示にする機能。ホームへの訪問やタイムラインへの投稿の表示が出来なくなる。過去のコメントやいいねの表示は消えない。

3　資料

写

平成27年2月24日

各県立学校長様

豊かな心育成課長

「携帯電話の問題から子どもを守ろう運動」に係る
保護者向け啓発資料の送付について（通知）

携帯電話等に係る啓発活動推進会議では，携帯電話等を学校に持ち込まないことや情報モラル教育の徹底を図るとともに，保護者が子供の携帯電話等に責任を持ち，「わが家の『ケータイルール』」を作成することを提案するなど，この運動の推進に取り組んできたところです。

この度，携帯電話等の使用時間と睡眠時間や学力との関係性が指摘されている現状を踏まえ，同会議において，家庭での学習時間を確保するため「携帯電話・スマートフォンによる通信を午後９時以降はしない」という「わが家の『ケータイルール』」を各家庭において作成する取組を全県一斉展開することが提案されました。

ついては，別紙の保護者向け啓発資料を作成しましたので，入学予定者説明会やＰＴＡ総会等の機会に，この啓発資料を活用するなど，携帯電話等に係る指導の一層の充実を図ってください。

担当　生徒指導係
電話　（082）513-5043（ﾀﾞｲﾔﾙｲﾝ）
（担当者　植野）

㊞

平成27年2月24日

各市町教育委員会教育長 様

広島県教育委員会教育長
（豊かな心育成課）

「携帯電話の問題から子どもを守ろう運動」に係る
保護者向け啓発資料の送付について（通知）

携帯電話等に係る啓発活動推進会議では，携帯電話等を学校に持ち込まないことや情報モラル教育の徹底を図るとともに，保護者が子供の携帯電話等に責任を持ち，「わが家の『ケータイルール』」を作成することを提案するなど，この運動の推進に取り組んできたところです。

この度，携帯電話等の使用時間と睡眠時間や学力との関係性が指摘されている現状を踏まえ，同会議において，家庭での学習時間を確保するため「携帯電話・スマートフォンによる通信を午後９時以降はしない」という「わが家の『ケータイルール』」を各家庭において作成する取組を全県一斉展開することが提案されました。

ついては，別紙の保護者向け啓発資料を作成しましたので，所管の各学校が入学予定者説明会やＰＴＡ総会等の機会に，この啓発資料を活用するなど，携帯電話等に係る指導の一層の充実を図ってください。

担当　生徒指導係
電話　（082）513-5043（ﾀﾞｲﾔﾙｲﾝ）
（担当者　末本）

携帯電話等に係る啓発活動推進会議

STOP 9

保護者のみなさまへ

携帯電話の問題から子どもを守ろう運動

わが家の「ケータイルール」

全県一斉展開

ケータイ・スマホを置いて，有意義な時を過ごそう！

携帯電話・スマートフォンによる通信を

午後9時以降はしない

- 携帯電話等でインターネットを利用している青少年のうち，約4割が1日2時間以上利用しています。
- メールや通話，SNSなどに熱中し，深夜まで使用することで，学習時間や睡眠時間が減少しています。
- 使用時間が長いことで，学力に顕著な影響が出ています。

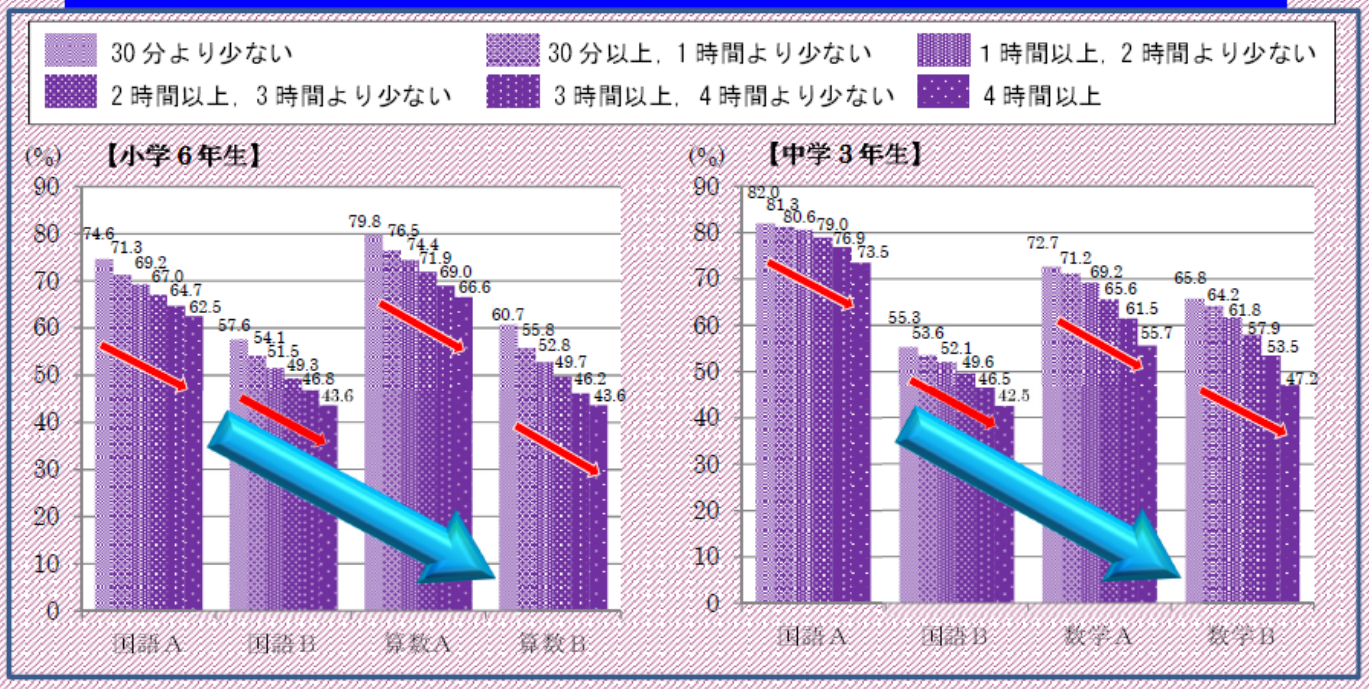
【携帯電話等に係る啓発活動推進会議】
（構成メンバー）広島県都市教育長会会長，広島県町教育長会会長，広島県連合小学校長会会長，広島県公立中学校長会会長，広島県公立高等学校長協会会長，広島県ＰＴＡ連合会会長，広島県高等学校ＰＴＡ連合会会長，広島市ＰＴＡ協議会会長
（事　務　局）広島県教育委員会，広島市教育委員会

携帯電話・スマートフォンの使用時間と学力との関係性について

■ 携帯電話やスマートフォンで通話やメール，インターネットをする時間が長い児童生徒の方が，全ての教科で

平均正答率が低くなっています。

携帯電話・スマートフォンの１日あたりの使用時間別の各教科の平均正答率



「平成26年度 全国学力・学習状況調査 調査結果のポイント」（文部科学省 国立教育政策研究所，平成26年８月）より作成

携帯電話の問題から子どもを守ろう運動

1. 学校には，携帯電話の持ち込みをやめましょう
2. 家庭では，保護者が子供の携帯電話に責任を持ちましょう
3. 家庭では，わが家の「ケータイルール」を作りましょう
4. 学校では，発達段階に応じた情報モラル教育を徹底しましょう

㊞

平成２６年３月３日

各県立学校長様

豊かな心育成課長

「携帯電話の問題から子どもを守ろう運動」に係る
保護者向け啓発資料の送付について（通知）

この度，「携帯電話の問題から子どもを守ろう運動」に係る保護者向け啓発資料（ＰＤＦファイル）を作成しましたので送付します。

ついては，学校においては，携帯電話等の問題から子供を守るため，児童生徒が携帯電話等を学校に持ち込まない指導や発達段階に応じた情報モラル教育を徹底してください。

また，保護者に対しては，啓発資料等を活用し，入学予定者説明会やＰＴＡ総会等，機会をとらえて繰り返し，子供の携帯電話等に保護者が責任を持つことや，携帯電話等を持たせる際には「わが家の『ケータイルール』」を親子で話し合って作ることを伝えるなど，学校と家庭が協力してこの運動が実効性のあるものになるよう，指導の一層の充実を図ってください。

担当　生徒指導係
電話　（082）513-5043（ﾀﾞｲﾔﾙｲﾝ）
（担当者　平野）

写

平成２６年３月３日

各市町教育委員会教育長 様

広島県教育委員会教育長
（豊かな心育成課）

「携帯電話の問題から子どもを守ろう運動」に係る
保護者向け啓発資料の送付について（通知）

この度，「携帯電話の問題から子どもを守ろう運動」に係る保護者向け啓発資料（ＰＤＦファイル）を作成しましたので送付します。

ついては，学校においては，携帯電話等の問題から子供を守るため，児童生徒が携帯電話等を学校に持ち込まない指導や発達段階に応じた情報モラル教育の充実を図るとともに，保護者に対しては，啓発資料等を活用し，入学予定者説明会やＰＴＡ総会等，機会をとらえて繰り返し，子供の携帯電話等に保護者が責任を持つことや，携帯電話等を持たせる際には「わが家の『ケータイルール』」を親子で話し合って作ることを伝えるなど，学校と家庭が協力してこの運動が実効性のあるものになるよう，所管する学校を指導してください。

担当　生徒指導係
電話　（082）513-5043（ﾀﾞｲﾔﾙｲﾝ）
（担当者　平野）

広島県教育委員会

学校には，携帯電話は必要ありません

携帯電話に係る様々な問題から
お子さんを守るために

保護者のみなさまへ

ケータイ・スマホは，本当に必要？

「携帯電話等に係る啓発活動推進会議」からの **4** つの提案

【携帯電話の問題から子どもを守ろう連動】

1. 学校には，携帯電話の持ち込みをやめましょう
2. 家庭では，保護者が子供の携帯電話に責任を持ちましょう
3. 家庭では，わが家の「ケータイルール」を作りましょう
4. 学校では，発達段階に応じた情報モラル教育を徹底しましょう

家庭では

携帯電話等は，どんな時に必要なのか，何のために使うのかなど，子供と十分話し合いましょう。

子供に携帯電話等を持たせる場合には，

■ **保護者が子供の携帯電話に責任を持ちましょう**

- ○ 契約時に，フィルタリング機能をはずさないようにしましょう
- ○ 家庭における「ケータイルール」を作成しましょう
- ○ 使用状況（メールや通信記録等）を定期的に確認しましょう
- ○ 学校や家庭におけるルールが守れない時は，使用を禁止しましょう
- ○ 子供が困った時は，子供の話をしっかり聞きましょう

■ **わが家の「ケータイルール」を作りましょう**

1 どんな時に使うのか 時間が心配

- □ 食事中は電源を切る
- □ 風呂に持ち込まない
- □ 夜＿＿時を過ぎたら使わない
- □ 利用は１日＿＿分まで
- □ 家ではリビングで使う
- □ 充電器はリビングに置く

2 何のために使うのか やりとりが心配

- □ 自分の個人情報は書かない
- □ 悪口を書き込まない
- □ 迷惑メールに返信しない
- □ チェーンメールを転送しない
- □ 知らない人からメールが来たら保護者に報告する

3 使うための約束 料金が心配

- □ 料金が＿＿円を超えた場合は小遣いで払う
- □ 料金が＿＿円を超えた翌月は使用しない
- □ ゲーム，音楽，アプリ等を勝手にダウンロードしない
- □ 勝手に会員登録をしない

【参考　ちょっと待って！ケータイ&スマホ　文部科学省】

広島県教育委員会

使い方を間違えると大変なことに！！

1 他人を誹謗中傷する情報の掲載

掲示板やチャットなどで，他人を誹謗中傷する内容が書き込まれるネットいじめなどの問題が発生しています。

2 下着や裸の写真の掲載

未成年者が，自ら肌を露出した写真などを撮影し，ネットに掲載する事案が増えています。「お金をもらえる」などの理由で，自分の下着姿や裸の写真，動画の送信やネット上の掲載などは絶対にしてはいけません。淫行の被害など，重大な危険に巻き込まれることがあります。

3 ネット上で知り合った異性とのトラブル

出会い系サイトだけでなく，一般のコミュニティサイトや無料通信アプリのIDを交換するサイトを経由して知り合った異性により，トラブルに巻き込まれ，犯罪にまで発展してしまうケースもあります。

4 著作権侵害

他人が作った作品（絵画，写真，音楽，小説など）を無断で掲載することは，著作権の侵害になります。また，平成24年10月，著作権法の一部が改正され，販売または有料配信されている音楽や映像の「違法ダウンロード」は，刑罰の対象となりました。

5 他人のプライバシー情報の掲載

無断で他人の氏名や住所，写真，アドレスなどをインターネットに公開することは，プライバシーの侵害に当たります。

【参考　(公財) 人権教育啓発推進センター】

気軽に相談してください

「ネットいじめ」にあってしまったら・・・

- 全国統一ダイヤル
  『２４時間いじめ相談ダイヤル』　電話０５７０－０－７８３１０
- 広島県立教育センター
  『いじめダイヤル２４』　電話０８２－４２０－１３１３

ネットトラブルで困ったら・・・

- 広島県警察サイバー犯罪対策課　代表電話０８２－２２８－０１１０
  http://www.pref.hiroshima.lg.jp/site/police3/
- 警察庁インターネット安全・安心相談
  http://www.npa.go.jp/cybersafety/

「情報モラル」について勉強したいと思ったら・・・

- ｅ－ネットキャラバン
  http://www.e-netcaravan.jp
- インターネットを利用する方のためのルール＆マナー集
  http://www.iajapan.org/rule/

【携帯電話等に係る啓発活動推進会議】
（構成メンバー）広島県都市教育長会会長，広島県町教育長会会長，広島県連合小学校長会会長，広島県公立中学校長会会長，広島県公立高等学校長協会会長，広島県ＰＴＡ連合会会長，広島県高等学校ＰＴＡ連合会会長，広島市ＰＴＡ協議会会長
（事　務　局）広島県教育委員会，広島市教育委員会

写

平 成 25年 8 月 13日

各 県 立 学 校 長 様

豊 か な 心 育 成 課 長

「携帯電話の問題から子どもを守ろう運動」の徹底について（通知）

児童生徒の携帯電話等の取扱い等については，「学校における携帯電話の取扱い等について（通知）」（平成21年２月９日付）や「『携帯電話の問題から子どもを守ろう運動』について（通知）」（平成21年３月４日付）により，各学校において，校内における携帯電話等の取扱いに係る指導方針を明確に定め，児童生徒に徹底し，携帯電話等を校内に持ち込まないよう，指導の充実を図っていただいているところです。

近年，携帯電話やスマートフォン等の「無料通話・メッセージアプリ」（ＬＩＮＥ等）の急速な普及により，青少年の犯罪被害が増加するとともに，これを悪用した青少年による問題行動や犯罪が発生しております。携帯電話やスマートフォン等の利用をめぐっては，こうした詐欺等の犯罪や出会い系サイト又はコミュニティサイトによる被害などに巻き込まれる問題だけでなく，掲示板やブログ等へ誹謗・中傷を書き込む，いわゆる「ネットいじめ」の問題や，食事や入浴，就寝時にも使用する極度の携帯電話やスマートフォン等への依存の問題，インターネットやメール送受信のための時間や金銭の浪費の問題など，児童生徒の人間関係づくりや生活スタイルの面にも大きな影響を与えます。これらの問題は，携帯電話やスマートフォン等を所持しているどの児童生徒にも起こりうるものであることから，情報モラル教育や規範意識を醸成する取組が一層必要となっています。

ついては，各学校において，平成20年度に教育長会，校長会及びＰＴＡ団体の代表で構成される「携帯電話等に係る啓発活動推進会議」が，携帯電話等に係る様々なトラブルから児童生徒を守るために行った４つの提案，①「学校には，携帯電話の持ち込みをやめましょう」，②「家庭では，保護者が子どもの携帯電話に責任を持ちましょう」，③「家庭では，わが家の『ケータイルール』を作りましょう」，④「学校では，発達段階に応じた情報モラル教育を徹底しましょう」を再度確認していただき，ＰＴＡと合同の研修会を開催するなど，保護者と協力しながら，「携帯電話の問題から子どもを守ろう運動」の更なる徹底を図ってください。

なお，参考として，資料「『携帯電話の問題から子どもを守ろう運動』の充実のために」及び過去の通知文を添付するとともに，県教育委員会等が作成した資料を示しますので，指導の際に活用してください。

担当　生徒指導係
電話　（082）513－5043（ﾀﾞｲﾔﾙｲﾝ）
（ 担当者　平野 ）

写

平 成 25年 8 月 13日

各市町教育委員会教育長様

広島県教育委員会教育長
（豊かな心育成課）

「携帯電話の問題から子どもを守ろう運動」の徹底について（通知）

児童生徒の携帯電話等の取扱い等については，「学校における携帯電話の取扱い等について（通知）」（平成21年２月９日付）や「『携帯電話の問題から子どもを守ろう運動』について（通知）」（平成21年３月４日付）により，各学校において，校内における携帯電話等の取扱いに係る指導方針を明確に定め，児童生徒に徹底し，携帯電話等を校内に持ち込まないよう，指導の充実を図っていただいているところです。

近年，携帯電話やスマートフォン等の「無料通話・メッセージアプリ」（ＬＩＮＥ等）の急速な普及により，青少年の犯罪被害が増加するとともに，これを悪用した青少年による問題行動や犯罪が発生しております。携帯電話やスマートフォン等の利用をめぐっては，こうした詐欺等の犯罪や出会い系サイト又はコミュニティサイトによる被害などに巻き込まれる問題だけでなく，掲示板やブログ等へ誹謗・中傷を書き込む，いわゆる「ネットいじめ」の問題や，食事や入浴，就寝時にも使用する極度の携帯電話やスマートフォン等への依存の問題，インターネットやメール送受信のための時間や金銭の浪費の問題など，児童生徒の人間関係づくりや生活スタイルの面にも大きな影響を与えます。これらの問題は，携帯電話やスマートフォン等を所持しているどの児童生徒にも起こりうるものであることから，情報モラル教育や規範意識を醸成する取組が一層必要となっています。

ついては，各市町教育委員会において，所管する学校に対し，平成20年度に教育長会，校長会及びＰＴＡ団体の代表で構成される「携帯電話等に係る啓発活動推進会議」が，携帯電話等に係る様々なトラブルから児童生徒を守るために行った４つの提案，①「学校には，携帯電話の持ち込みをやめましょう」，②「家庭では，保護者が子どもの携帯電話に責任を持ちましょう」，③「家庭では，わが家の『ケータイルール』を作りましょう」，④「学校では，発達段階に応じた情報モラル教育を徹底しましょう」を再度確認し，学校がＰＴＡと合同の研修会を開催するなど，保護者と協力しながら，「携帯電話の問題から子どもを守ろう運動」の更なる徹底を図るよう，指導してください。

なお，参考として，資料「『携帯電話の問題から子どもを守ろう運動』の充実のために」及び過去の通知文を添付するとともに，県教育委員会等が作成した資料を示しますので，指導の際に活用してください。

担当　生徒指導係
電話　（082）513－5043（ﾀﾞｲﾔﾙｲﾝ）
（担当者　平野）

資　料

広島県教育委員会

「携帯電話の問題から子どもを守ろう運動」の充実のために

1　「携帯電話の問題から子どもを守ろう運動」について

平成 20 年度に，教育長会，校長会及びＰＴＡ団体の代表で構成される「携帯電話等に係る啓発活動推進会議」が，携帯電話の問題から子どもを守る（「携帯電話をめぐるトラブルから守る」，「携帯電話への依存から守る」，「時間・金銭の浪費から守る」）ために４つの提案を行い，「携帯電話の問題から子どもを守ろう運動」が展開されているところです。

「携帯電話等に係る啓発活動推進会議」からの **「４つの提案」**

- ○　学校には，携帯電話の持ち込みをやめましょう。
- ○　学校では，発達段階に応じた情報モラル教育を徹底しましょう。
- ○　家庭では，保護者が子どもの携帯電話に責任を持ちましょう。
- ○　家庭では，わが家の「ケータイルール」を作りましょう。

2　携帯電話等の問題に係る最近の事例について

近年の携帯電話やスマートフォン等の急速な普及と機能の高度化により，児童生徒が携帯電話等のトラブルに巻き込まれる機会が急激に増加しています。

（１）「携帯電話等をめぐるトラブルから守る」

□　誘い出しにより性的被害にあった事例

コミュニティサイトで女子生徒Ａと知り合った男が，年齢や職業などを偽り，「本気で好きだ。」「付き合いたい。」などと言って近付き，裸の写真をメールで送らせた。その後，生徒Ａは「言うことを聞かなければ，裸の写真をネットに流す。」と言って脅され，ホテルでわいせつな行為をされた。

□　書き込みによる誹謗中傷を行った事例

生徒Ｂは，友人とケンカをして腹を立て，携帯電話で，ネット上の学校裏サイトの掲示板にその友人の氏名や住所，電話番号を書き込んだ上で，悪口を書き込んだ。その後，無料通話メッセージアプリを使って，数名の友人にその悪口を広めるよう頼んだ。

（２）「携帯電話等への依存から守る」

□　オンラインゲームをやめることができなくなった事例

オンラインゲームにはまってしまった児童Ｃは，深夜でも親に隠れてこっそりゲームをするようになった。オンラインゲームに参加しないと学校で仲間はずれにされることも心配でますますやめられなくなり，睡眠不足が続いた結果，学校でも授業に集中できなくなった。

□　携帯メール依存により情緒不安定になった事例

生徒Ｄは，いつも携帯を手元においてメール等をしており，外出しても電波の届かないところには行きたがらないなど，メールなどをすることを何よりも最優先していた。次第に，誰かとメールしていないと孤独感を感じ，友だちからのメールが来なかったり，返信が少しでも遅れたりすると不安になるなど，情緒不安定になった。最近は，友人とメール以外で直接話すことにも抵抗を感じるようになった。

（３）「時間・金銭の浪費から守る」

□　携帯メールに時間を浪費し生活習慣が乱れた事例

生徒Ｅは，友だちから携帯メールが１日に 100 通くらい届いている。その返事を５分以内に返さないといけないという「５分間ルール」があるため，歩きながらや食事中，さらには入浴中や寝るときにも返信しなければならず，１日のほとんどの時間を携帯メールにしばられている。

□　オンラインゲームで金銭を浪費した事例

児童Ｆは，テレビで「無料オンラインゲーム」とコマーシャルしていたソーシャルゲームに参加した。そのゲームの中でアイテムを購入すると，後日，ゲーム配信会社から数万円を請求された。

【参考】広島県警察本部生活安全部サイバー犯罪対策課提供資料，総務省「インターネットトラブル事例集」

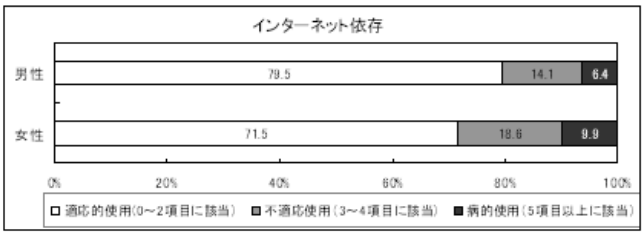
【参考】「インターネット依存」について

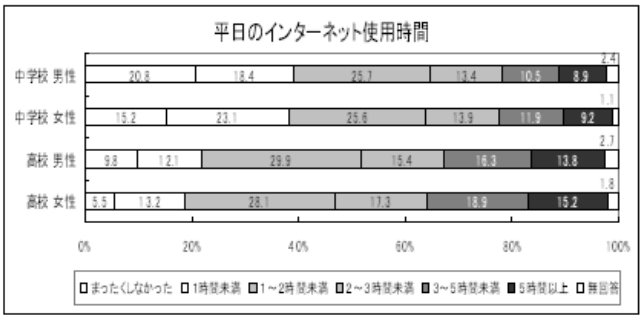
厚生労働省研究班による「平成 24 年度未成年の喫煙・飲酒状況に関する実態調査」では，「インターネット依存」について，次の８つの質問項目のうち５項目以上に該当する場合を「病的使用」としています。中・高校生における「病的使用」の割合は，男性で 6.4%，女性で 9.9%を占め，全国で 51 万８千人に上ると推計しています。

また，平日のインターネット使用時間が５時間以上であると回答した生徒の割合は，高校生男子で 13.8%，高校生女子で 15.2%を占めています。

【インターネット依存に係る質問項目】

① インターネットに夢中になっていると感じているか。
② 満足を得るために，ネットを使う時間を長くしていかなければならないと感じるか。
③ 使用時間を減らしたり，やめようとしたりしたが，うまくいかなかったことが度々あったか。
④ ネットの使用をやめようとした時，落ち込みやイライラなどを感じるか。
⑤ 意図したよりも，長時間オンラインの状態でいるか。
⑥ ネットのため，大切な人間関係，学校，部活のことを危うくしたことがあったか。
⑦ 熱中しすぎていることを隠すため，家族や先生にうそをついたことがあるか。
⑧ 嫌な気持ちや不安，落ち込みから逃げるためにネットを使うか。





３　「携帯電話の問題から子どもを守ろう運動」の充実に向けて

こうした状況を踏まえ，各公立小・中・高・特別支援学校においては，引き続き，携帯電話を校内に持ち込まない指導，及び発達段階に応じた情報モラル教育を徹底するとともに，様々な機会をとらえて保護者と連携し，この運動に対する理解と協力が得られるよう積極的な働きかけを行うことによって，４つの提案が実効性のあるものになるよう，再度取組の充実を図る必要があります。

学　校

学校には，携帯電話の持ち込みをやめましょう

○ 携帯電話を学校へ持ち込まないことへの指導を徹底します。
○ 携帯電話に係る様々な問題点やトラブル事例等を児童生徒に周知します。

学校では，発達段階に応じた情報モラル教育を徹底しましょう

○ 各教科の授業等で，プライバシーの保護，著作権の尊重，サイバー犯罪への対応等について指導します。

保護者

家庭では，保護者が子どもの携帯電話に責任を持ちましょう

○ 携帯電話が本当に必要かどうかをしっかりと検討するとともに，子どもに携帯電話を持たせる場合には，必ずフィルタリング機能を付加するなど，保護者が責任を持ちましょう。

家庭では，わが家の「ケータイルール」を作りましょう

○ 子どもに携帯電話を持たせる場合には，家庭における使い方をお子さんと十分話し合い，家族でルールを作りましょう。

写

平成２３年１０月２６日

各県立学校長様

指導第三課長

「携帯電話の問題から子どもを守ろう運動」に係る
保護者向け啓発資料について（通知）

この度，「携帯電話の問題から子どもを守ろう運動」に係る保護者向け啓発資料（ＰＤＦファイル）を作成しましたので送付します。

ついては，携帯電話の問題から子どもを守るため，児童生徒が携帯電話を学校に持ち込まない指導や発達段階に応じた情報モラル教育を徹底してください。

また，保護者に対しては，啓発資料等を活用し，子どもの携帯電話に保護者が責任を持つことや携帯電話を持つ際には，「わが家の『ケータイルール』」を親子で話し合って作るなど，学校と家庭が協力してこの運動が実効性のあるものになるよう指導の充実を図ってください。

なお，平成２１年３月２７日付け「『携帯電話の問題から子どもを守ろう運動』に係る啓発資料について（通知）」も指導の参考にしてください。

担当　生徒指導係
電話　082-513-5043
（担当者　齋藤）

写

平成２３年１０月２６日

各市町教育委員会教育長様

広島県教育委員会教育長
（指導第三課）

「携帯電話の問題から子どもを守ろう運動」に係る
保護者向け啓発資料について（通知）

この度，「携帯電話の問題から子どもを守ろう運動」に係る保護者向け啓発資料（ＰＤＦファイル）を作成しましたので送付します。

ついては，啓発資料等を活用し，携帯電話の問題から子どもを守るため，児童生徒が携帯電話を学校に持ち込まない指導や発達段階に応じた情報モラル教育の充実が図られるよう，所管する学校を指導してください。

また，保護者に対しては，啓発資料等を活用し，子どもの携帯電話に保護者が責任を持つことや携帯電話を持つ際には，「わが家の『ケータイルール』」を親子で話し合って作るなど，学校と家庭が協力してこの運動が実効性のあるものになるよう指導の充実を図ってください。

なお，平成２１年３月２７日付け「『携帯電話の問題から子どもを守ろう運動』に係る啓発資料について（通知）」も指導の参考にしてください。

担当　生徒指導係
電話　082-513-5043
（担当者　小田）

広島県教育委員会

子どもたちはこんな危険にさらされています！！

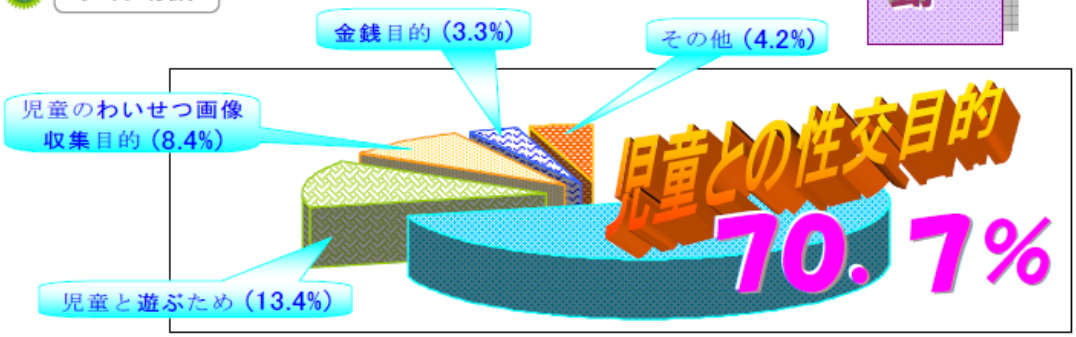
保護者のみなさまへ

携帯電話の問題から子どもを守ろう運動

近年，出会い系サイトに起因する児童（※）被害の事犯が減少する一方，コミュニティサイト（出会い系サイトを除く。）に起因する事犯が大幅に増加しています。
（※ 児童とは，18 歳に満たない者をいう。）

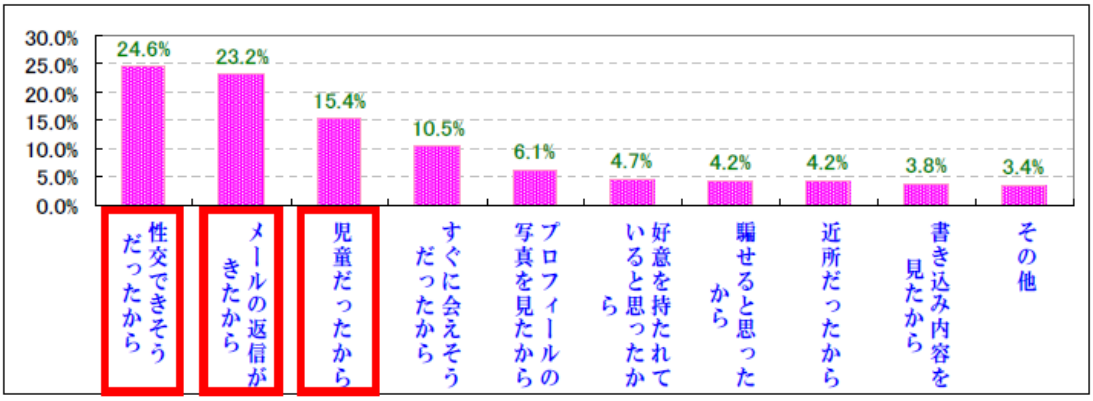
1 福祉事犯等で検挙された者の状況

犯行動機

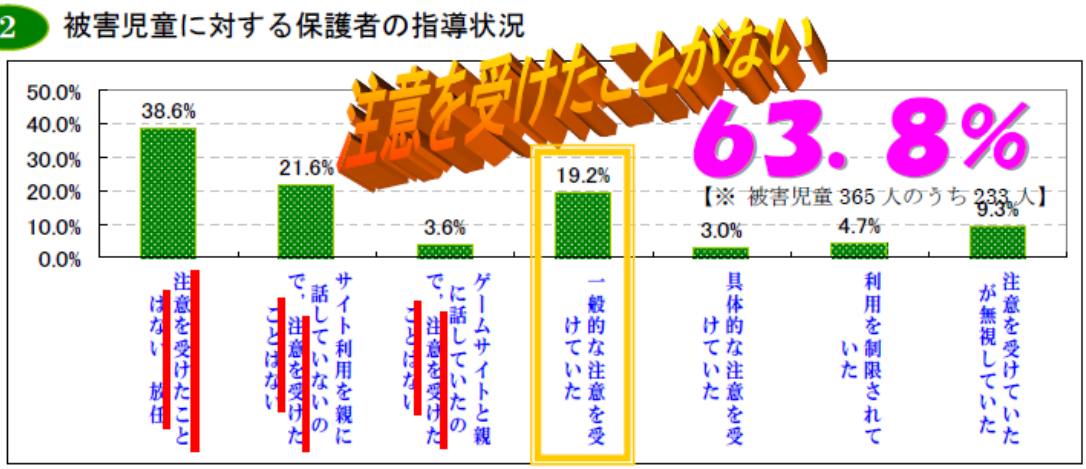


【※ 検挙した福祉事犯等 811 件のうち 573 件】

被害児童を選んだ理由



2 被害児童に対する保護者の指導状況



【参考資料】警察庁広報資料平成 23 年５月 19 日
コミュニティサイトに起因する児童被害の事犯に係る調査分析について（平成 22 年下半期）

ケータイは，本当に必要？

学校には，携帯電話は必要ありません

携帯電話に係る様々な問題からお子さんを守るために

- ○ *携帯電話をめぐるトラブルから守る*
- ○ *携帯電話への依存から守る*
- ○ *時間・金銭の浪費から守る*

「携帯電話等に係る啓発活動推進会議」からの **4** つの提案

学　校

学校には，携帯電話の持ち込みをやめましょう

○ 携帯電話を学校へ持ち込まないことへの指導を徹底します。
○ 携帯電話に係る様々な問題点やトラブル事例等を児童生徒に周知します。

学校では，発達段階に応じた情報モラル教育を徹底しましょう

○ 各教科の授業等で，プライバシーの保護，著作権の尊重，サイバー犯罪への対応等について指導します。

保護者

家庭では，保護者が子どもの携帯電話に責任を持ちましょう

○ 携帯電話が本当に必要かどうかをしっかりと検討するとともに，子どもに携帯電話を持たせる場合には，必ずフィルタリング機能を付加するなど，保護者が責任を持ちましょう。

家庭では，わが家の「ケータイルール」を作りましょう

○ 子どもに携帯電話を持たせる場合には，家庭における使い方をお子さんと十分話し合い，家族でルールを作りましょう。

広島県教育委員会

写

文書分類記号	H1216
保存年限	

平成２１年３月４日

各県立学校長様

指導第三課長

「携帯電話の問題から子どもを守ろう運動」について（通知）

児童生徒の携帯電話の取扱い等については，「学校における携帯電話の取扱い等について（通知）」（平成２１年２月９日付）により，指導方針の検証・見直しを行うとともに，情報モラル教育を徹底するなど，更なる取組みの充実を図るようお願いしてきたところです。

この度，「携帯電話等に係る啓発活動推進会議」において，携帯電話に係る様々なトラブルから児童生徒を守るため，各教育委員会，各学校及び各ＰＴＡ団体が，児童生徒が携帯電話を学校に持ち込まないこと等について４つの提案を行い，「携帯電話の問題から子どもを守ろう運動」を展開することとしました。

ついては，各学校において実効性のある取組みができるよう，別紙「携帯電話を学校に持ち込まないことへの指導に関するガイドライン」を参考に，校内における携帯電話の取扱いに係る指導方針を明確に定め，児童生徒に徹底し，携帯電話を校内に持ち込まないよう指導の充実を図ってください。

また，この提案が保護者代表を含む推進会議の提案であることを踏まえ，添付の啓発資料を活用し，携帯電話の取扱いに係る指導方針を繰り返し保護者に説明し，理解と協力を得るよう働きかけを行ってください。

なお，啓発資料（配付用）は，後日，送付します。

担当　生徒指導係
電話　082-513-5043
（担当者　西永）

写

平成２１年３月４日

各市町教育委員会教育長様

広島県教育委員会教育長
（指導第三課）

「携帯電話の問題から子どもを守ろう運動」について（通知）

児童生徒の携帯電話の取扱い等については，「学校における携帯電話の取扱い等について（通知）」（平成２１年２月９日付）により，指導方針の検証・見直しを行うとともに，情報モラル教育を徹底するなど，更なる取組みの充実を図るようお願いしてきたところです。

この度，「携帯電話等に係る啓発活動推進会議」において，携帯電話に係る様々なトラブルから児童生徒を守るため，各教育委員会，各学校及び各ＰＴＡ団体が，児童生徒が携帯電話を学校に持ち込まないこと等について４つの提案を行い，「携帯電話の問題から子どもを守ろう運動」を展開することとしました。

ついては，各学校において実効性のある取組みができるよう，別紙「携帯電話を学校に持ち込まないことへの指導に関するガイドライン」を参考に，校内における携帯電話の取扱いに係る指導方針を明確に定め，児童生徒に徹底し，携帯電話を校内に持ち込まないよう指導の充実を図ってください。

また，この提案が保護者代表を含む推進会議の提案であることを踏まえ，添付の啓発資料を活用し，携帯電話の取扱いに係る指導方針を繰り返し保護者に説明し，理解と協力を得るよう働きかけを行ってください。

なお，啓発資料（配付用）は，後日，送付します。

担当　生徒指導係
電話　082-513-5043
（担当者　西永）

㊞

平成２１年３月４日

広島県ＰＴＡ連合会会長様

広島県教育委員会教育長
（指導第三課）

「携帯電話の問題から子どもを守ろう運動」について（依頼）

このことについて，別紙（写）のとおり各市町教育委員会へ通知しておりますので，御協力をお願いします。

「携帯電話の問題から子どもを守ろう運動」が保護者の理解と協力により実効性のあるものになりますよう，定例総会等で啓発資料を活用するなど，各小中学校ＰＴＡへ周知していただきますよう，お願いします。

担当 生徒指導係
電話 082-513-5043
（担当者　西永）

写

平成２１年３月４日

広島県高等学校ＰＴＡ連合会会長様

広島県教育委員会教育長
（指導第三課）

「携帯電話の問題から子どもを守ろう運動」について（依頼）

このことについて，別紙（写）のとおり各市町教育委員会へ通知しておりますので，御協力をお願いします。

「携帯電話の問題から子どもを守ろう運動」が保護者の理解と協力により実効性のあるものになりますよう，定例総会等で啓発資料を活用するなど，各高等学校（特別支援学校を含む）ＰＴＡへ周知していただきますよう，お願いします。

担当 生徒指導係
電話 082-513-5043
（担当者　西永）

㊞

平成２１年３月４日

広島市ＰＴＡ協議会会長様

広島県教育委員会教育長
（指導第三課）

「携帯電話の問題から子どもを守ろう運動」について（依頼）

このことについて，別紙（写）のとおり各市町教育委員会へ通知しておりますので，御協力をお願いします。

「携帯電話の問題から子どもを守ろう運動」が保護者の理解と協力により実効性のあるものになりますよう，定例総会等で啓発資料を活用するなど，各小中高等学校（特別支援学校を含む）ＰＴＡへ周知していただきますよう，お願いします。

担当 生徒指導係
電話 082-513-5043
（担当者　西永）

別紙

平成２１年３月４日

携帯電話を学校へ持ち込まないことへの指導に関するガイドライン

広 島 県 教 育 委 員 会

１　趣旨

このガイドラインは，このたび，教育長会，校長会及びＰＴＡ団体の代表で構成される『携帯電話等に係る啓発活動推進会議（※）』（以下，「推進会議」という。）から「学校には，携帯電話の持込みをやめましょう」など４つの提案があったことから，この呼びかけに応え，各学校及び各家庭において実効性のある取組みができるよう，学校での指導の在り方や留意点について目安を示したものである。

（※広島県都市教育長会会長，広島県町教育長会会長，広島県連合小学校長会会長，広島県公立中学校長会会長，広島県公立高等学校長協会会長，広島県ＰＴＡ連合会会長，広島県高等学校ＰＴＡ連合会会長，広島市ＰＴＡ協議会会長）

２　児童生徒の指導について

各学校は，このガイドラインを踏まえ，児童生徒に対して携帯を校内へ持ち込まないように徹底するとともに，校内における携帯電話の取扱いに係る指導方針を明確に定めること。

３　保護者の理解と協力について

携帯電話を校内へ持ち込まないことなどについて，各学校は，この４つの提案が保護者の代表を含む推進会議によるものであることを踏まえ，携帯電話の取扱いに係る指導方針を繰り返し保護者に説明し，理解と協力を得るよう働きかけること。

４　指導の在り方について

学校における教育活動において，携帯電話が必要でないことは明らかであり，携帯電話を持ち込まないよう校則に定めること。

一方，各学校は，児童生徒の登下校中の安全確保，通学範囲が広い学校や帰宅連絡に係る保護者の要望及び職業上携帯電話を必要とする高校生に係る就業先からの直接登校などの場合には，次の２点を踏まえ，発達段階に応じた指導を行うように配慮すること。

（１）　保護者の申し出によりやむを得ず携帯電話を学校へ持ち込もうとする場合には，携帯電話の会社名，商品コード（商品名称），製造番号，電話番号等を確認するとともに，携帯電話を持ち込む理由を明確にし，児童生徒及び保護者の連名による文書で許可申請させ，校長が許可すること。

（２）　持込みを許可した携帯電話についても，校内では，学校が預かる又は電源を切った状態にし，けっして身につけさせないなど，校内で使用できないよう指導すること。

５　指導上の留意点について

（１）　携帯電話を校内へ持ち込まないことについて，単なる呼びかけにならないよう指導を徹底すること。

（２）　携帯電話を持ち込ませることを安易に許可することで，携帯電話を学校へ持ち込まない取組みを徹底する妨げとならないよう細心の注意を払うこと。

（３）　学校の指導方針に違反した児童生徒については，予め示した方法による特別な指導を行うなど毅然とした態度で指導すること。

（４）　携帯電話の持込みを学校が許可する際に学校が把握した個人情報は，取扱いに細心の注意を払って確実に管理するとともに，目的外使用をしないこと。

（５）　携帯電話を学校が預かる場合，盗難，破損，紛失及び取り違え並びに，プライバシー情報の侵害や漏洩事故が起きないよう配慮し，適切に管理すること。

（６）　課業中に保護者から緊急の連絡が必要な場合には，学校を通じた連絡が可能であることを周知・徹底するなど，携帯電話を利用しない連絡方法について具体的に示し保護者の理解を得ること。また，緊急の場合には，児童生徒が校内から保護者へ連絡できるよう配慮すること。

（７）　保護者が登下校中やむを得ず携帯電話を持たせようとする場合は，必要な機能に限定した機種の選定又は携帯電話の機能の制限などを働きかけること。

（８）　「携帯電話を使用しない週間」など一定期間携帯電話に頼らず生活する取組みを各家庭に働きかけるなど，児童生徒及び保護者の携帯電話の問題に関する意識を喚起すること。

（９）　児童生徒の発達段階に応じた，情報モラル教育，情報リテラシーの指導計画を立て，指導を徹底すること。

保護者のみなさまへ

携帯電話等に係る啓発活動推進会議

携帯電話の問題から子どもを守ろう運動

ケータイは，本当に必要？

携帯電話をめぐるトラブルに子どもたちが巻き込まれています

3人に2人 以上の中高生が，
携帯電話によるトラブルを経験しています。
（携帯電話を所有している中学2年生の67%，高校2年生の68%）

学校には，携帯電話は必要ありません

携帯電話に係る様々なトラブルからお子さんを守るために

「携帯電話等に係る啓発活動推進会議」からの **4つの提案**

1 学校には，携帯電話の持ち込みをやめましょう

108分 が，高校生が１日に
携帯電話等でインターネットを使う平均時間です。
（中学生は７５分です。）

- 携帯電話の利用時間が増えると，学習時間等が確保できなくなります。

2 家庭では，保護者が子どもの携帯電話に責任を持ちましょう

65% の高校２年生の保護者が，
メールやインターネットをすることを放任しています。
（中学２年生の保護者は３１%です。）

- お子さんは，保護者の想像以上の危険にさらされています。

3 家庭では，わが家の「ケータイルール」を作りましょう

84% の高校２年生が，フィルタリング機能を使っていません。
（中学２年生は５４%です。）

- フィルタリング機能がないと，有害な情報にもアクセスできてしまいます。

4 学校では，発達段階に応じた情報モラル教育を徹底しましょう

74% の中学生が，インターネットを使うとき「ネチケット（礼儀やマナー）を守る」ことに気をつけていません。
（高校生は７１%です。）

- 学校では，情報化社会における正しい判断や望ましい態度を育てていきます。

携帯電話は，どんな時に必要なのか，何のために使うのかなど，お子さんと十分話し合い，家庭のルールを作ってみましょう。

※ 文部科学省調べ「子どもの携帯電話等の利用に関する調査」，内閣府調べ「第5回情報化社会と青少年に関する意識調査」による

家庭における携帯電話の使用ルールを作りましょう！

子どもに携帯電話を持たせる場合には，トラブルに巻き込まれないように，家族でルールを決めましょう。

～ わが家の「ケータイルール」10か条 ～

（例）

1　誹謗・中傷，いじめに使わない。
2　家庭では，保護者のいるところで使う。
3　保護者は，メール及び通信記録をチェックできる。
4　フィルタリング機能をはずさない。
5　インターネットに接続するときは，保護者の許可を得る。
6　メールの返信「５分ルール」でしばらない，しばられない。
7　食事中や学習中は，電源を切る。
8　学校のルールを守る。
9　困ったことがあれば保護者に相談する。
10　ルールが守れない時は，使用を禁止する。

気軽に相談してください

「ネットいじめ」にあってしまったら・・・

◎全国統一ダイヤル
『２４時間いじめ相談ダイヤル』　電話　０５７０－０－７８３１０（なやみ言おう）

◎広島県立教育センター
『いじめダイヤル２４』　電話　０８２－４２０－１３１３

ネットトラブルで困ったら・・・

『広島県警察サイバー犯罪対策室』　代表電話０８２－２２８－０１１０
http://www.police.pref.hiroshima.lg.jp/041/hightech/index.html
『警察庁インターネット安全・安心相談』
http://www.cybersafety.go.jp/

「情報モラル」について勉強したいと思ったら・・・

『e－ネットキャラバン』
http://www.fmmc.or.jp/e-netcaravan/
『インターネットを利用するためのルールとマナー集』
http://www.iajapan.org/rule/rule4child/v2/

「フィルタリングの設定」について知りたいと思ったら・・・

『有害サイトアクセス制限サービス』
http://www.soumu.go.jp/joho_tsusin/d_syohi/filtering.html

【携帯電話等に係る啓発活動推進会議】

（構成メンバー）広島県都市教育長会会長，広島県町教育長会会長，広島県連合小学校長会会長，広島県公立中学校長会会長，広島県公立高等学校長協会会長，広島県ＰＴＡ連合会会長，広島県高等学校ＰＴＡ連合会会長，広島市ＰＴＡ協議会会長
（事　務　局）広島県教育委員会，広島市教育委員会

児童生徒のみなさんへ

携帯電話等に係る啓発活動推進会議

携帯電話の問題から子どもを守ろう運動

ケータイは，本当に必要？

学校には，携帯電話は必要ありません

学校，家庭のルールを守りましょう

Q 携帯電話って，本当に必要なの？

● 携帯電話は，学校生活や勉強にはいりません。

- 携帯電話は，どんな時に必要なのか，何のために使うのかなど，自分にとって本当に必要かどうか，しっかり考えましょう。

Q 携帯電話に，振り回されていませんか？

● 携帯電話は，あなたの大切な時間をうばってしまいます。

- 「メールは５分以内に返さなければならない。」という『５分ルール』（こんなルールはありません）にしばられて，食事中や寝るときも携帯電話をはなせない人がいます。
- あなたにとって，携帯電話でメールのやりとりや書き込みをすることよりも，もっと大切なことがあるはずです。
- 携帯サイトには危険がいっぱいです。好奇心でアクセスすると大変なことになります。

Q 携帯電話で，友情が深まるの？

● 携帯電話では，本当の気持ちは伝わりません。

- メールや掲示板への書き込みによるコミュニケーションでは，本当の友情を深めることはできません。
- 携帯電話では，本当の気持ちが伝わらないため，相手が傷ついていることが分からないことがあります。
- ブログやプロフで安易に自分のことを紹介すると，悪い人に使われて，危ない目にあうことがあります。

携帯電話は，どんな時に必要なのか，何のために使うのかなど，
保護者と十分話し合い，家庭のルールを作ってみましょう。

家庭における携帯電話の使用ルールを作りましょう！

子どもに携帯電話を持たせる場合には，トラブルに巻き込まれないように，家族でルールを決めて，下に書いてみましょう。

～ わが家の「ケータイルール」＿つの約束 ～

携帯電話に係る様々なトラブルからお子さんを守るために

「携帯電話等に係る啓発活動推進会議」からの 4つの提案

1 学校には，携帯電話の持ち込みをやめましょう
2 家庭では，保護者が子どもの携帯電話に責任を持ちましょう
3 家庭では，わが家の「ケータイルール」を作りましょう
4 学校では，発達段階に応じた情報モラル教育を徹底しましょう

ひとりで，悩まないで・・・

「ネットいじめ」にあってしまったら・・・

◎全国統一ダイヤル
『２４時間いじめ相談ダイヤル』　電話　０５７０－０－７８３１０（なやみ言おう）

◎広島県立教育センター
『いじめダイヤル２４』　電話　０８２－４２０－１３１３

ネットトラブルで困ったら・・・

『広島県警察サイバー犯罪対策室』　代表電話　０８２－２２８－０１１０
http://www.police.pref.hiroshima.lg.jp/041/hightech/index.html
『警察庁インターネット安全・安心相談』
http://www.cybersafety.go.jp/

「情報モラル」について勉強したいと思ったら・・・

『e－ネットキャラバン』
http://www.fmmc.or.jp/e-netcaravan/
『インターネットを利用するためのルールとマナー集』
http://www.iajapan.org/rule/rule4child/v2/

「フィルタリングの設定」について知りたいと思ったら・・・

『有害サイトアクセス制限サービス』
http://www.soumu.go.jp/joho_tsusin/d_syohi/filtering.html

【携帯電話等に係る啓発活動推進会議】
（構成メンバー）広島県都市教育長会会長，広島県町教育長会会長，広島県連合小学校長会会長，広島県公立中学校長会会長，広島県公立高等学校長協会会長，広島県ＰＴＡ連合会会長，広島県高等学校ＰＴＡ連合会会長，広島市ＰＴＡ協議会会長
（事　務　局）広島県教育委員会，広島市教育委員会

4 関係機関，相談窓口及び参考サイト

【参考サイト等】			
1	広島県教育委員会	広島市中区基町９－42 http://www.pref.hiroshima.lg.jp/site/kyouiku/	082-513-4911
2	広島県警察本部	広島市中区基町９－42 http://www.pref.hiroshima.lg.jp/site/police/index.html	082-228-0110
3	広島県警察本部生活安全部 サイバー犯罪対策課	広島市中区基町１－４ http://www.pref.hiroshima.lg.jp/site/police3/	082-228-0110 （広島県警察本部） 082-212-3110 （サイバー110番）
4	広島県警察本部生活安全部 少年対策課	広島市中区基町１－４ http://www.pref.hiroshima.lg.jp/site/police7/	082-228-0110
【広島県内の警察署】			
5	安芸高田警察署	安芸高田市吉田町吉田1204-2 http://www.pref.hiroshima.lg.jp/site/police-akitakata/	0826-47-0110
6	安佐北警察署	広島市安佐北区可部四丁目14-13 http://www.pref.hiroshima.lg.jp/site/police-asakita/	082-812-0110
7	安佐南警察署	広島市安佐南区西原九丁目3-20 http://www.pref.hiroshima.lg.jp/site/police-asaminami/	082-874-0110
8	江田島警察署	江田島市江田島町中央四丁目13-1 http://www.pref.hiroshima.lg.jp/site/police-etajima/	0823-42-0110
9	大竹警察署	大竹市本町一丁目8-10 http://www.pref.hiroshima.lg.jp/site/police-otake/	0827-53-0110
10	尾道警察署	尾道市新浜一丁目7-34 http://www.pref.hiroshima.lg.jp/site/police-onomichi/	0848-22-0110
11	海田警察署	安芸郡海田町つくも町1-45 http://www.pref.hiroshima.lg.jp/site/police-kaita/	082-820-0110
12	呉警察署	呉市西中央二丁目2-4 http://www.pref.hiroshima.lg.jp/site/police-kure/	0823-29-0110
13	佐伯警察署	広島市佐伯区倉重一丁目26-1 http://www.pref.hiroshima.lg.jp/site/police-saeki/	082-922-0110
14	庄原警察署	庄原市中本町一丁目3-8 http://www.pref.hiroshima.lg.jp/site/police-shobara/	0824-72-0110
15	世羅警察署	世羅郡世羅町大字西上原427-1 http://www.pref.hiroshima.lg.jp/site/police-sera/	0847-22-0110

16	竹原警察署	竹原市中央一丁目1-13 http://www.pref.hiroshima.lg.jp/site/police-takehara/	0846-22-0110
17	廿日市警察署	廿日市市本町1-10 http://www.pref.hiroshima.lg.jp/site/police-hatsukaichi/	0829-31-0110
18	東広島警察署	東広島市西条昭和町4-11 http://www.pref.hiroshima.lg.jp/site/police-higashihiroshima/	082-422-0110
19	広警察署	呉市広大新開一丁目5-6 http://www.pref.hiroshima.lg.jp/site/police-kure/	0823-75-0110
20	広島中央警察署	広島市中区基町9-48 http://www.pref.hiroshima.lg.jp/site/police-hiroshimachuo/	082-224-0110
21	広島西警察署	広島市西区商工センター四丁目1-3 http://www.pref.hiroshima.lg.jp/site/police-hiroshimanishi/	082-279-0110
22	広島東警察署	広島市東区二葉の里三丁目４-22 http://www.pref.hiroshima.lg.jp/site/police-hiroshimahigashi/	082-506-0110
23	広島南警察署	広島市南区宇品東四丁目1-34 http://www.pref.hiroshima.lg.jp/site/police-hiroshimaminami/	082-255-0110
24	福山北警察署	福山市神辺町大字新道上三丁目14 http://www.pref.hiroshima.lg.jp/site/police-fukuyamakita/	084-962-0110
25	福山西警察署	福山市神村町3106-1 http://www.pref.hiroshima.lg.jp/site/police-fukuyamanishi/	084-933-0110
26	福山東警察署	福山市三吉町南二丁目5-31 http://www.pref.hiroshima.lg.jp/site/police-fukuyamahigashi/	084-927-0110
27	府中警察署	府中市鵜飼町542-3 http://www.pref.hiroshima.lg.jp/site/police-fuchu/	0847-46-0110
28	三原警察署	三原市皆実三丁目2-6 http://www.pref.hiroshima.lg.jp/site/police-mihara/	0848-67-0110
29	三次警察署	三次市十日市中二丁目6-6 http://www.pref.hiroshima.lg.jp/site/police-miyoshi/	0824-64-0110
30	山県警察署	山県郡安芸太田町大字加計3760-1 http://www.pref.hiroshima.lg.jp/site/police-yamagata/	0826-22-0110
【少年留置，保護等関係施設】			
31	広島県警察本部警務部 留置管理課	http://www.pref.hiroshima.lg.jp/site/police6/001-kunrei-ryukan.html	082-228-0110
32	広島少年鑑別所	広島市中区吉島西三丁目15-8 http://www.moj.go.jp/kyousei1/kyousei03_00039.html	082-244-3388

33	広島保護観察所	広島市中区上八丁堀2-31 http://www.moj.go.jp/hogo1/soumu/hogo_k_hiroshima_hiroshima.html	082-221-4495
34	広島少年院	東広島市八本松町原11174-31 http://www.moj.go.jp/kyousei1/kyousei03_00097.html	082-429-0821
35	貴船原少女苑	東広島市八本松町原6088 http://www.moj.go.jp/kyousei1/kyousei03_00103.html	082-429-3001
【児童自立支援施設】			
36	広島県立広島学園	東広島市八本松町原10844 https://www.pref.hiroshima.lg.jp/site/hiroshimagakuen/	082-429-0351
【児童養護施設（12施設）】			
37	似島学園	広島市南区似島町長谷1487 http://www.ninoshima-gakuen.jp/	082-259-2456
38	広島新生学園	東広島市西条町田口391-2 http://h-shinsei.or.jp/	082-425-1378
39	広島修道院	広島市東区尾長西二丁目8-1 http://shudoin.or.jp/	082-261-1356
40	光の園摂理の家	廿日市市地御前1895 http://hikarinosono.jp/	0829-39-1121
41	仁風園	呉市仁方西神町35-11 http://kure-dousai.jp/index.php/%E6%96%BD%E8%A8%AD%E7%B4%B9%E4%BB%8B/%E5%85%90%E7%AB%A5%E9%A4%8A%E8%AD%B7%E6%96%BD%E8%A8%AD%E3%80%80%E4%BB%81%E9%A2%A8%E5%9C%92/	0823-21-5395
42	八幡学園	広島市佐伯区八幡一丁目5-20 https://yahata.jungenkai.or.jp/	082-928-0602
43	子供の家三美園	尾道市美ノ郷町三成372 http://www.dohen.or.jp/intro/child/sanbien01/	0848-48-0045
44	救世軍愛光園	広島県呉市狩留賀町3-5	0823-27-5361
45	救世軍豊浜学寮	呉市豊浜町豊島3082-5	0823-68-2029
46	こぶしケ丘学園	福山市加茂町下加茂899 http://kobushinomura.com/kobushi/	084-972-5811
47	津田子供の家	廿日市市津田596- 1 http://www.sakurafukushikai.or.jp/tsuta-index.html	0829-72-0364
48	福山ルンビニ園	福山市加茂町字北山176-12 https://runbini.jimdo.com/	084-972-8004
【国の機関等及び参考サイト】			
49	文部科学省	http://www.mext.go.jp/	
50	文部科学省 （教材，手引書）	http://jouhouka.mext.go.jp/school/information_moral_manual/	
51	総務省　情報通信政策に関するポータルサイト	http://www.soumu.go.jp/main_sosiki/joho_tsusin/joho_tsusin.html	
52	総務省　国民のための情報セキュリティサイト	http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/basic/service/index.html	

53	総務省　国民のための情報セキュリティサイト キッズ	http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/kids/	
54	法務省　人権擁護局	http://www.moj.go.jp/JINKEN/index.html	
55	警察庁情報技術犯罪対策課（サイバー犯罪対策）	http://www.npa.go.jp/cyber/index.html	
56	NISC　内閣サイバーセキュリティセンター	https://www.nisc.go.jp/	
57	IHC　インターネット・ホットラインセンター（違法・有害情報の通報）	http://www.internethotline.jp/	
58	IPA　独立行政法人情報処理推進機構（子ども向けサイバーセキュリティ読本を公開）	https://www.ipa.go.jp/security/keihatsu/security-himitsu/	
59	一般財団法人インターネット協会（子ども向けルール，マナー検定を公開）	https://www.iajapan.org/	
60	JNSA　特定非営利活動法人日本ネットワークセキュリティ協会（子ども向け教材等を公開）	http://www.jnsa.org/net-anzen/html/	
61	フィッシング対策協議会（ﾌｨｯｼﾝｸﾞﾒｰﾙの通報）	https://www.antiphishing.jp/	
※この他，教材等が各種サイトで公開されています。「インターネット　教材」等で検索してください。			
【インターネット相談窓口】			
62	法務省（子どもの人権110番）	http://www.moj.go.jp/JINKEN/jinken112.html	
63	広島法務局（人権相談窓口）	http://houmukyoku.moj.go.jp/hiroshima/category_00009.html	
64	日本いのちの電話連盟	https://www.inochinodenwa.org/	
65	チャイルドライン支援センター（相談窓口）	http://www.childline.or.jp/index.html	
66	警察庁（インターネット安全・安心相談）	https://www.npa.go.jp/cybersafety/	
67	広島県警相談窓口	http://www.pref.hiroshima.lg.jp/site/police/soudan.html	
【削除要請・発信者情報開示請求関係】			
68	違法・有害情報相談センター（総務省支援事業）	http://www.ihaho.jp/	
69	法務省（「インターネットを悪用した人権侵害をなくしましょう」）	http://www.moj.go.jp/JINKEN/jinken88.html	
70	プロバイダ責任制限法ガイドライン等検討協議会	http://www.isplaw.jp/	

◆　本書の使用にあたり

本文書に記載されている会社名，システム名，製品名等は各社の商標または登録商標です。なお，本書では文中にて，TM，®は明記しておりません。

本書は，サイバーセキュリティの普及・啓発に利用する限りにおいては，紙媒体及び電子媒体での配布や印刷の制限はありません。

著作権は広島県教育委員会及び広島県警察が保留しますので，利用に当たっては可能な限りクレジット表記を行ってください。

教材などのために部分的な配布を行う場合は，意図を変更しない範囲において，部分的な利用又は一部を変更しての利用を可能とします。

ただし，他からの引用部分やイラストは第三者が著作権等を有している場合がありますので，権利を侵害しないように注意してください。引用部分やイラストを単独で利用する場合は，利用者の責任において各権利者にご確認ください。

◆　本書中の引用部分及び著作権

第１章 ２～４ ： 内閣サイバーセキュリティセンター　ネットワークビギナーのための情報セキュリティハンドブック （https://www.kantei.go.jp/jp/froms/nisc_option.html ）

第３章 ２－２ 「コラム 自画撮り被害の実情」 ： 警察庁少年課　広報資料（https://www.npa.go.jp/safetylife/syonen/no_cp/newsrelease/selfy.pdf）

第３章 ３ 「削除要請の考え方と方法」中の図 ： 法務省「インターネットを悪用した人権侵害をなくしましょう」（http://www.moj.go.jp/JINKEN/jinken88.html ）

第４章 １ 「IT用語集」 ： 総務省「用語辞典」（http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/glossary/01.html）

第４章 ３ 「資料」：広島県教育委員会

上記以外のイラスト： かわいいフリー素材 いらすとや（http://www.irasutoya.com/）

◆　謝辞

本書中のイラストの使用をご承諾頂いた，かわいいフリー素材 いらすとや の みふねたかし様に感謝の意を表します。

◆　免責事項

広島県教育委員会及び広島県警察は，利用者が本書を用いて行う一切の行為について何ら責任を負うものではありません。

本書の内容は，予告なく変更，削除等が行われることがあります。

制作・著作　広島県教育委員会（豊かな心育成課）・広島県警察（生活安全部サイバー犯罪対策課）
Copyright © 2018 Hiroshima Prefectural Board of Education and
Hiroshima Cybercrimes Control Division.