



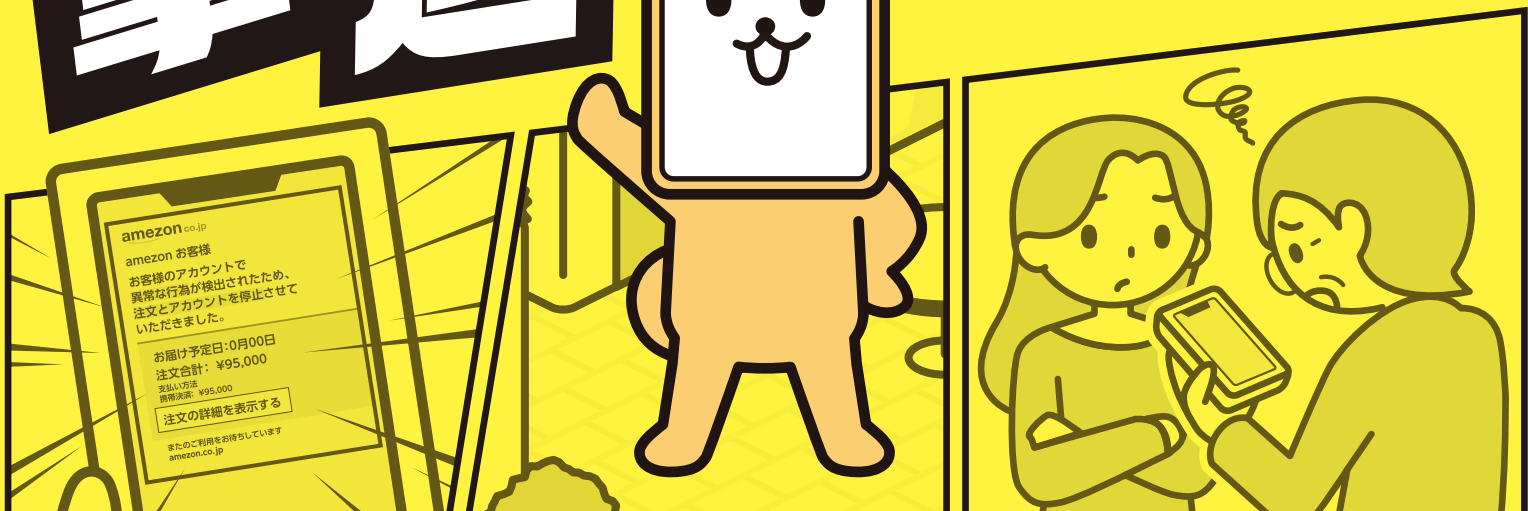
最新!

子どもから大人まで、
ネット・スマホとの上手な付き合い方、教えます

サイバー犯罪 BOOK

撃退

守って安心 ワン!ポイント



公益財団法人全国防犯協会連合会

この冊子は、公益財団法人日工組社会安全研究財団の助成により作成したものです

身近なところに、こんなに危険が!!

サイバー犯罪について 皆で知識をアップデート

このスマホに
おまかせ!



かしこいスマホ型ネットパトロール犬「スマワン」といっしょに学ぼう!

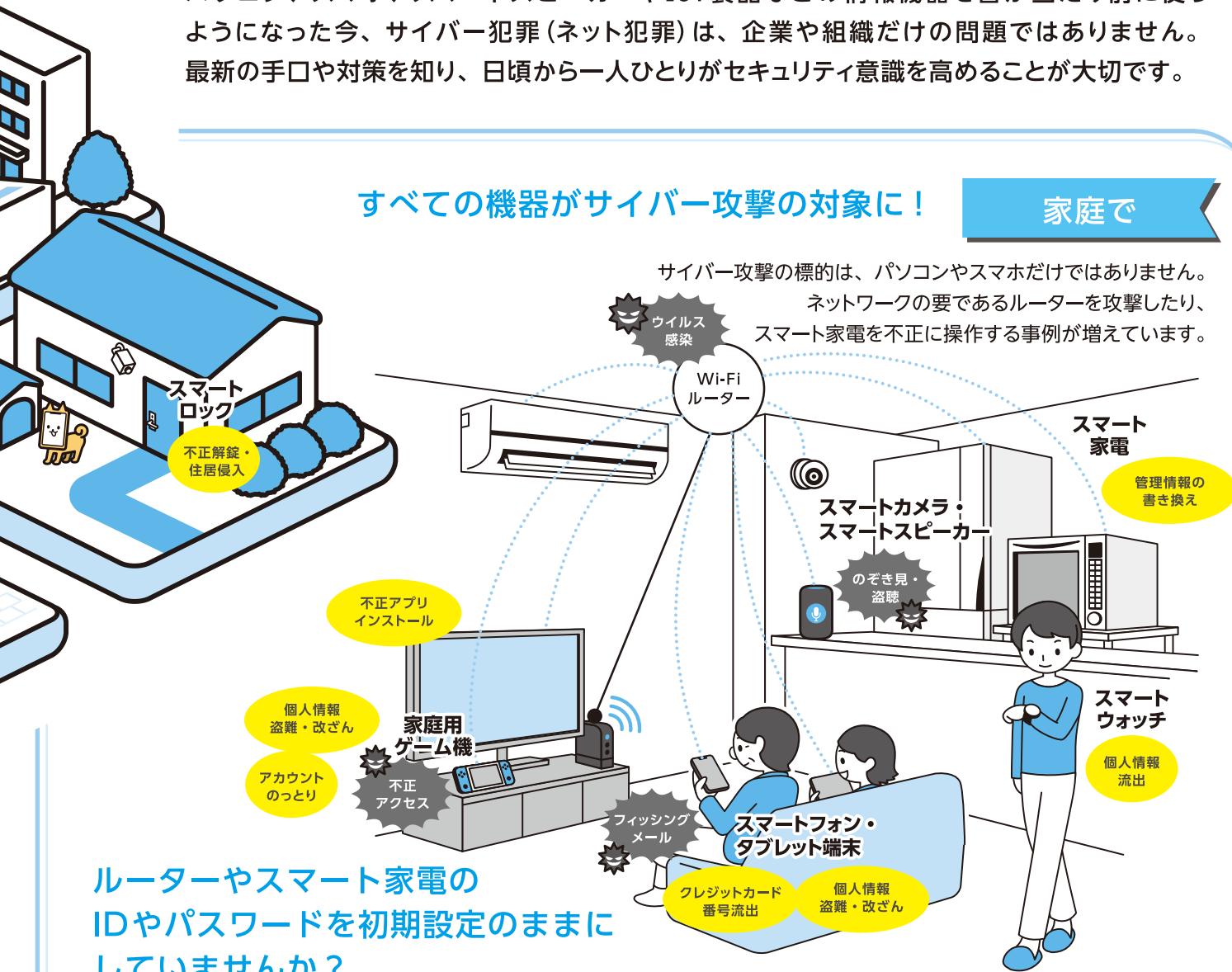
スマワン

パソコン、スマホ、スマートスピーカーやIoT製品などの情報機器を皆が当たり前のように使った今、サイバー犯罪(ネット犯罪)は、企業や組織だけの問題ではありません。最新の手法や対策を知り、日頃から一人ひとりがセキュリティ意識を高めることが大切です。

すべての機器がサイバー攻撃の対象に!

家庭で

サイバー攻撃の標的は、パソコンやスマホだけではなく、ネットワークの要であるルーターを攻撃したり、スマート家電を不正に操作する事例が増えています。



ルーターやスマート家電のIDやパスワードを初期設定のままに
していませんか?

安全なパスワードの三原則

1 できるだけ長く

最低でも
10桁以上

2 複雑なものを

英数字、記号、
大文字小文字を
ランダムに

3 使い回さない

例えば…
PASSWORD
kasHikoi@suMa1



企業で

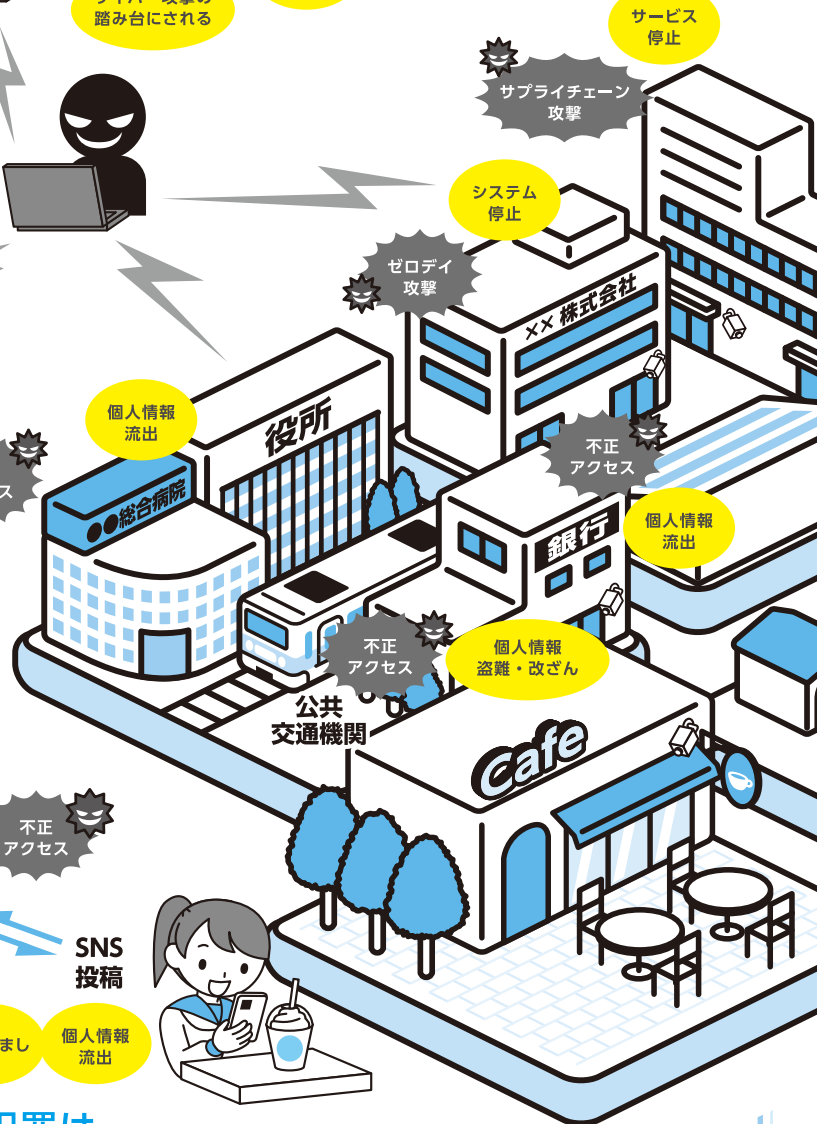
今や大企業はもちろん、中小企業がサイバー攻撃の足がかりになるケースが多発しています。



病院などの社会インフラが攻撃対象に！私たちの生活がおびやかされるように…

公的機関で

政府機関や地方公共団体、企業・団体等の本物のウェブサイトそっくりの「偽サイト」が多数、確認されています。



カフェ等で

外出先で無線LANを利用する時も要注意！データのやりとりには通信経路を暗号化するVPNなどのサービスを利用しましょう。



サイバー犯罪は、
私たちの隙を狙って行われます！

目次

P4-P9 これだけは知っておきたい！サイバー犯罪の最新事情

■ フィッシング詐欺を中心に、
ネット詐欺の手口を徹底解剖

- ① フィッシング詐欺（スミッシング詐欺）
- ② ネットショッピング詐欺
- ③ ワンクリック詐欺（架空請求詐欺）
- ④ マッチングアプリ詐欺（投資詐欺）



P10-P11 サイバー犯罪から身を守る10か条

P12-P15 ネット&SNSトラブルから子どもたちを守る

- クイズで学ぼう！SNSとの上手なつきあいかた
- トラブルを防ぐワン！ポイント
- 親子でつくろう！スマホのお約束

【保護者の方へ】ペアレンタルコントロールでSNS環境を整えましょう

裏表紙 困ったときの相談先

これだけは知っておきたい！サイバー犯罪の最新事情 フィッシング詐欺を中心に、 ネット詐欺の手口を徹底解剖

ついアクセスしてしまいそうになる有名な企業のサービスを装ったメールで攻撃してくるフィッシング詐欺。年々、巧妙化や悪質化が進んでおり、注意が必要です。



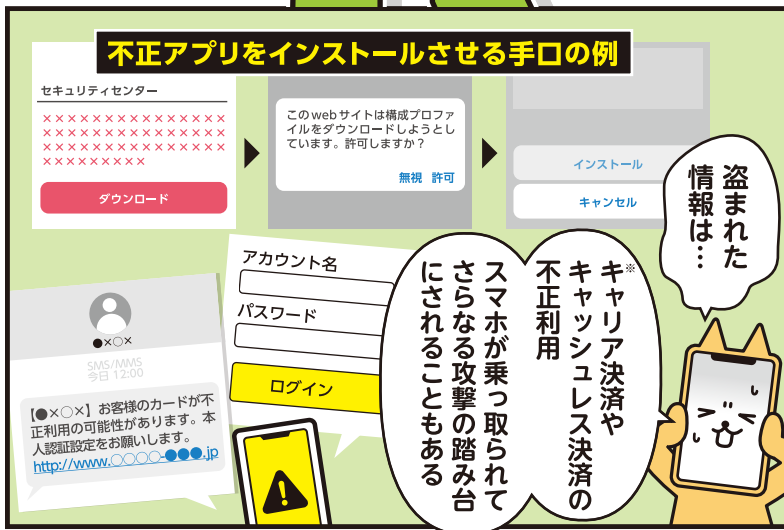
携帯電話やスマホのSMSを 悪用した攻撃が増えています

信頼性の高い
公的機関や有名企業
になりすます！

ポイント！



スミッシング詐欺は、ショートメッセージサービス(SMS)を悪用して行われるフィッシング詐欺の一種です。郵便局や銀行、宅配業者などを装ってメッセージを送り、受信者を偽のウェブサイトに誘導し、個人情報や盗み取ったり、不正アプリをインストールさせたりします。



*キャリア決済…商品やサービスの代金を、携帯電話料金と合算して支払う決済方法

傾向

最近の事例では、本物の文面やサイトの内容をコピーしたものが多く、見分けることが難しくなっています。また、2段階認証の認証コードが盗まれる事例も発生するなど、手口の巧妙化も進んでいます。SMSやメールにあるリンクへのアクセスは慎重に行うようにしましょう。

【緊急】〇〇銀行

お客様の口座に不正なアクセスがありました。以下のURLよりパスワードを変更してください。

<http://xxx.xxx.jp>



対策

- SMSに記載されたURLには原則としてアクセスしない
- 通信事業者、宅配事業者の公式サイトを確認する
- よくアクセスする会社は、あらかじめURLをブックマークに登録しておく
- アプリのインストールは、正規のアプリ配信サイト等、信頼できるサイトから行う
- 日頃から決済サービスの利用明細を見て、身に覚えのない支払いが含まれていないか確認する
- 怪しいメールを受信した、フィッシングサイトを発見した、情報を入力してしまった場合には、警察へ通報を！ **フィッシング110番**
- 最新情報の収集は、**フィッシング対策協議会** ウェブサイトをチェック！

間違ってもアクセスした時は画面をすぐ閉じて！



フィッシング
110番



フィッシング
対策協議会

実在する有名サイトにそっくり！ なりすまし通販サイトに注意

偽サイトからの購入で、
個人情報の流出や
商品未着の危険が！



スマートフォン等を活用したネットショッピングが定着する一方で、「頼んだ商品が届かず、事業者に連絡がとれない」などの通販サイトの被害が増加。また、正規サイトの入力フォームなどを不正に改ざんしてクレジットカード情報を盗み取る「ウェブスキミング」の手口も報告されています。

「ウェブスキミング」って何？
被害に遭っても気づきにくい特徴があるよ。流れを見ていこう！

1 決済画面に不正なコードが埋め込まれる

2 見た目は実際のECサイトで動作しているフォームと同じ

3 不正なプログラムが作動して、個人情報送信されてしまう！

4 商品が届く物とは違う物に気づけないのね…

5 悪質なサーバーへの通信をブロックするウイルス対策ソフトの導入

定期的な確認する

私たちができる対策はあるの？

残念だけど偽サイトを完璧に見分けるのは難しいんだ

私がよく使うECサイトね

いつもどおり買い物をしよう

注文を確定

氏名・住所・電話番号クレジットカード番号など

購入完了

ECサイト側は不正に気づかない

商品が届く物とは違う物に気づけないのね…

悪質なサーバーへの通信をブロックするウイルス対策ソフトの導入

定期的な確認する

被害に遭った場合は、クレジットカード会社や警察等へ相談を！

傾向

SNS上の広告に誘導されて大手百貨店を偽る通販サイトで注文してしまった、ウェブを検索して割引額が大きいブランド品を注文したら偽物だったなどの事例が増えています。家電や家具・生活雑貨店などの公式サイトを偽る通販サイト、大手通販サイトの悪質な出品者などにも注意が必要です。



対策

- 購入を希望する通販サイトのURLと、実際に表示されているURLが一致しているかを確認
- 商品の価格が相場よりも大幅に安い場合は、特に注意を
- 「特定商取引法に基づく表記」のページを見て、信頼できる事業者かどうかを確認
 - 事業者の名称・所在地・電話番号・代表者名、利用者の口コミなどもチェックを
 - デタラメな住所が記載されていることもあるため、住所や電話番号が実在するかも確認
- 代金支払い方法が前払い・銀行振込みのみで、振込先が個人名の口座の場合は要注意
- おかしいと思ったら、速やかに各地の消費生活センター、警察等に相談しましょう

大手通販サイトを装っているケースもあるよ！



有料サイトに登録したと思わせ 不安や焦りにつけこんで高額請求！

サイト閲覧中に
突然警告が!?
基本的には詐欺なので
無視でOK



アダルトサイト等の無料動画を見ようと画面をクリックしたところ、会員登録を装い、料金を請求される手口が一般的ですが、迷惑メールのリンク、アニメやゲーム・占いなどのコンテンツから誘導されることもあり、子どもから高齢者まで、年齢・性別を問わず被害に遭う危険性があります。

「ワンクリック詐欺」の魔の手が忍び寄る...

絶対電話しなうで!

電話しなきゃだめかな...

アダルトコンテンツ契約
契約料 **30万円**
登録完了

プロバイダ情報: 00000000
IPアドレス: 000.000.000.000

誤操作の方はこちら
☎00-000-0000

うわっ
むひひ...

R-18

ウェブ閲覧中にいきなり警告が出る「サポーター詐欺」も多発!

不審なアクティビティが原因
すぐにご連絡ください。

今から5分以内に電話してください
サポート:000-000-000

至急! 「すぐに」など不安をあおる!

実際の企業を装って信用させようとする!

アクセスするとサポート料の名目で料金をだまし取られます

コンピュータでギフトカードを買おうとするワン

Microsoft Window
サポートに連絡:000-000-000

電話やメールで問い合わせを促す!

警告画面の連絡先には絶対に連絡しないこと!

いろいろなパターンがあるけどまずは警告が偽物だと疑おう

電話しちゃダメ!

一旦個人情報が相手に知られてしまうと、何度も請求されたり、他の業者にも情報を共有されてしまったりします

傾向

サイトを閲覧中、勝手にウィンドウが開くポップアップの機能により、「スマホが感染しました」などの偽の警告画面や不正な請求画面が表示されたり、画面に端末情報やIPアドレスなどを表示させ、スマホから個人情報を抜き取ったかのように装うこともあります。「法的手段を取る」などの文言で脅してきても無視すればOKです。



対策

- 怪しいサイトにアクセスしない、ポップアップの広告やURLを不用意にクリックしないこと
- 契約は当事者双方が合意していなければ成立しないため、不当な請求に対する支払い義務はありません。なお、解約や退会を希望する際のアドレスや電話番号が記載されていても、決して連絡しないこと
- 請求画面が表示されても、慌てずに画面を閉じましょう
画面を閉じることができない時は、閲覧履歴とキャッシュを削除すれば画面を消すことが可能です
詳しい方法は **IPA (情報処理推進機構) 安心相談窓口** だよりを参照してください



IPA
安心相談窓口だより



怪しいサイトに
アクセスしない!
クリックしない!

「暗号資産で送金」「必ず儲かる」に注意！ 投資を勧められたら、詐欺を疑おう

高年齢者だけでなく、
若年層にも被害が
及んでいます

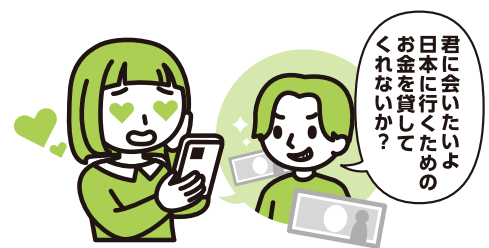


マッチングアプリやSNSで出会った異性の相手から投資話を持ちかけられ、大金をだましとられる「投資詐欺」「国際ロマンス詐欺」の被害が後を絶ちません。詐欺師は、用意周到に相手からの信頼を勝ち取るように工作を行ったあとで、暗号資産(仮想通貨)の口座開設や取り引きを勧めてきます。



傾向

投資詐欺では、投資の初期段階に利益が出ているように見せかけることで信頼を得ようとする手口が多く使われます。また、投資詐欺を行っているのは日本人だけでなく、外国人が投資家を装って近づいてくるケースもあります。外国籍の軍人・医師・国連職員・資産家等を装う異性から交際や結婚を申し込まれ、投資資金や渡航経費の送金を求めたりする「国際ロマンス詐欺」の被害も後を絶たない状況です。



対策

- マatchingアプリやSNSで出会った相手から送金や投資を勧められた際は、まずは詐欺を疑い、きっぱりと断ること
- 勧誘者や事業者と連絡がとれなくなると、被害を回復することは困難です。不安に思った場合や、トラブルに遭った場合は、すぐに最寄りの消費生活センター等へ相談しましょう
- マatchingアプリは会員の質や安全性など吟味した上で使いましょう
出会った相手に情報商材を売りつけられた、暴力Barに連れて行かれた、暴行・殺害される等、様々なトラブルも起こっています
また相手に会うときは、昼間の時間帯・人が多くいる場所を選ぶ、密室で2人きりにならないなど、警戒をおこらないことが大切です



甘い言葉には十分注意！常に警戒しておこう！

身を守る



以下の意識を高めることが大切です。



5 家庭のWi-Fiルーターのセキュリティを強化しよう
購入時の初期パスワードは必ず変更し、機器を動かすプログラムの更新（ファームウェアアップデート）にも気を配りましょう。



4 スマホのOSやアプリは常にアップデートしておこう
スマホの本体やアプリを最新の状態に保つとともに、アプリは必ず公式ストアや信頼できる提供元から導入するようにしましょう。



3 ウイルス対策ソフトを導入して、常に最新の状態に更新しよう
ウイルスやフィッシングなどの脅威を検知し、ブロックするためには、常にソフトを最新の状態に保っておく必要があります。



2 重要なアカウントは多要素認証を導入しよう
ID・パスワードの他に、生体認証やワンタイムパスワードなどを必要とする「多要素認証」が提供されているサービスでは、必ず設定しましょう。



1 パスワードを使い回さず、長くて複雑なものに設定し、適切に管理
パスワードを使い回していると、一つ流出することにより複数のアカウントで不正アクセスの被害を受ける可能性が出てきてしまいます。

サイバー犯罪から

日々、巧妙さを増すサイバー攻撃から身を守るためには、セキュリティ今すぐ、家族皆で気をつけたいポイントをご紹介します。



添付ファイルはすぐに開かない。送信者の身元を確認し、なりすましにも気をつける
急いで添付ファイルやリンクを開くことを要求するメールやSMSには必ず警戒を。



必要なウェブサイトはブックマークしておき、メールやSMS内のリンク先はクリックしない
よく利用するサイトはブックマーク（お気に入り）に登録しておき、公式のアプリやブックマークからのみアクセスするようにしましょう。



個人情報 はむやみに発信しない

悪意がある第三者にとつて、個人を特定する手がかりになる情報は載せないこと。一度公開した個人情報はネットから消し去ることができません。



情報の真偽はきちんと確認し、相手を傷つけるような発信はしない

ネットでの誹謗中傷、名誉毀損は、刑事上・民事上の責任を問われる可能性があります。



脅威はいつもすぐそばにあると心得てサイバーセキュリティ情報に敏感になろう

利用しているセキュリティソフトのメーカーや、フィッシング対策協議会、警察庁などのSNSアカウントをフォローすると、最新の情報を入手しやすくなります。

Q1

SNSいじめ

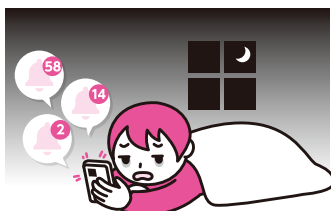
SNSいじめについて、
間違っているのはどちらでしょう？

- A SNSいじめの被害にあったので、
相手をブロックした。
- B クラスメイトに向けて「キモい。死ぬ」と
悪口を書きこんだけど、匿名だから大丈夫。

Q2

メッセージアプリトラブル

既読スルーは良くないことだから、
メッセージアプリのメッセージには
速攻で返信しなければならない。

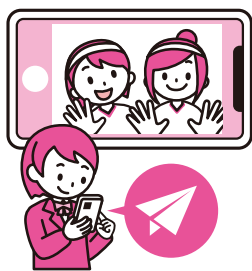


()

Q3

肖像権、プライバシーの侵害

楽しかった体育祭、
皆が参加した行事だから
SNSにアップしても大丈夫？



()

Q4

個人情報の保護

家族旅行の写真をリアルタイムで
SNSに投稿。匿名だし、位置情報も
オフにしているから大丈夫？



()

SNSとの上手なつきあいかた クイズで学ぼう！

ネット&SNSトラブルから子どもたちを守る



小学校でも一人につき一台パソコンやタブレットが配布されるようになった今、子どものうちからしっかりと、インターネットのリスクについて知っておくことが必要です。安全に利用する方法を、親子で一緒に考えてみましょう。

Q7

違法サイトのアップロード、ダウンロード

好きなアイドルの
ライブ動画が
無料でアップされている！
ダウンロードしても大丈夫？

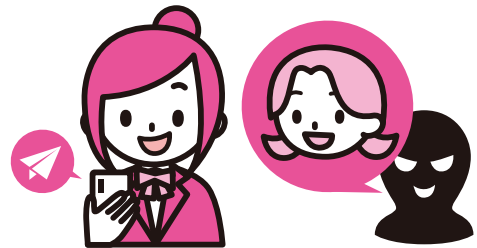
()

Q5

自撮り被害

SNSで知り合った人から、
顔写真を送ってほしいと
言われた。
相手は同性みたいだし、
顔写真だけなら送ってもいい？

()



Q8

誹謗・中傷、拡散

有名人の気に入らない
コメントへの書きこみを見て、
自分もリツイート。
匿名だし、悪いのは
有名人なんだから、問題ない？

()



Q6

オンラインゲームを めぐるトラブル

オンラインゲームで
知らない人とボイスチャット。
個人情報と話さなければ、
とくに問題はない？

()

こたえ

Q1 B Q2 × Q3 × Q4 × Q5 × Q6 × Q7 × Q8 ×

←くわしくは次のページを見てね!

24時間子供 SOSダイヤル (通話料無料) ☎ 0120-0-78310

いじめで困ったり、友だちのことで不安や悩みがあったりしたら、
一人で悩まず、いつでもすぐ電話で相談してください。

裏表紙の困ったときの相談先も見てください

トラブルを防ぐワン!ポイント



トラブルを早期に発見して対応するために、
お子さまといっしょにポイントをチェックしてみてください。

5 自画撮り被害

同世代のフリをして近づき、脅したりして裸の写真を送るように迫る「自画撮り被害」が増えています。また、たとえ送ったのが顔写真であっても、それを拡散するなど脅迫されたり、個人情報が悪用されることもあります。

ポイント

自画撮りを要求されたら、「危ない」と思いましょ

1 SNSいじめ

悪口を書きこむ以外にも、「LINEのグループから外された」「写真を変に加工して拡散された」などのいじめは後を絶ちません。自分がされたらイヤなこと、困ることはたとえ匿名でもしてはいけません。

ポイント

いじめの被害にあったときは、画面をスクリーンショットで保存するなど、いじめの証拠を残すこと

6 オンラインゲームをめぐるトラブル

オンラインゲームをきっかけとした小学生の誘拐事件が発生するなど、知らない人とのボイスチャットにはリスクがあります。うっかり個人情報をもらってしまうこともあるため、機能を制限するなど、細心の注意が必要です。

ポイント

知らない人だけでなく、友だちにも自分のIDやパスワードを教えない!

2 メッセージアプリトラブル

「既読」がついた状態で相手を待たせてはならないと思いがちですが、気持ちが正しく伝わるように、メッセージを送る前に「見直す」ことを習慣にしましょう。

ポイント

顔が見えないからこそ、思いやりの気持ちを大切に

7 違法サイトのアップロード、ダウンロード

市販されている音楽や映像、ネットで有料で配信されている動画などを、有償コンテンツと知っていながら違法サイトから無償でダウンロードすることは違法です。また、テレビや動画の画面を撮ってSNSに投稿するのもNGです。

ポイント

映像、音楽、マンガ、小説などの「著作物」は、正規のサイトからダウンロードしましょう

3 肖像権、プライバシーの侵害

友だちやクラスメイトの許可なく投稿してしまうと、肖像権やプライバシーの侵害にあたります。映っている全員の許可を得ることが事前に必要です。また、いっしょに映っている知らない人にも配慮が必要です。

ポイント

本人にことわりなく氏名や写真、出来事を公開しない!

8 誹謗・中傷、拡散

たとえ有名人やタレントでも、相手の人格を否定または攻撃する投稿が許されるわけではありません。また、「再投稿」などで拡散した場合も同じです。

ポイント

「誹謗・中傷」への対策として、「侮辱罪」が厳罰化されました。だれもが加害者や被害者になる可能性があり、大変な問題であることを覚えておきましょう

4 個人情報の保護

写真を撮影した日付や位置情報をオフにするのは◎ですが、リアルタイムで投稿するのはちょっと待って! たとえ友だち限定で情報を公開しているとしても、「今、留守です」と皆に言いふらしていることになり、危険です。

ポイント

実名や住所はもちろん、その日の予定や出来事は書きこまない!



親子でつくろう! スマホのお約束

ルールを決めたらチェック しよう!

1	<input type="checkbox"/>	スマホは学校の宿題や明日の準備が終わってから使います
2	<input type="checkbox"/>	1日 時間以内。 時から 時まで使います
3	<input type="checkbox"/>	通話、SNS、メールは決められた人とだけします
4	<input type="checkbox"/>	SNSやメールのやりとりは、よく考えて、注意して行います
5	<input type="checkbox"/>	自分や友だちの個人情報を書きこみません
6	<input type="checkbox"/>	友だちや有名人の悪口を書きこみません
7	<input type="checkbox"/>	見られて困る写真や動画を撮らせません、送りません
8	<input type="checkbox"/>	ゲームやアプリでお金がかかる時は親に相談します
9	<input type="checkbox"/>	SNSで困ったことがあったら、すぐに親に相談します
10	<input type="checkbox"/>	フィルタリングを使います
11	<input type="checkbox"/>	「歩きスマホ」や「ながらスマホ」は絶対にしません
12	<input type="checkbox"/>	画面ロックのパスワードは一緒に決めたものを利用します
13	<input type="checkbox"/>	

↑ 13はご家庭オリジナルのルールを決めてご記入ください。

保護者の方へ 「ペアレンタルコントロール」でSNS環境を整えましょう

ペアレンタルコントロールとは、子どもが安全にスマホやパソコンを活用するために、利用状況を保護者が適切に管理・制限することで、18歳以下にスマホを持たせるときは、フィルタリング(有害サイトアクセス制限サービス)の導入が義務づけられています。スマホ本体の機能や通信会社のサービス、フィルタリングアプリなどを上手に利用して、子どもたちを危険から守りましょう。

フィルタリングでできること

- 有害なサイト等へのアクセスやアプリの利用の制限
- 長時間の利用、課金を防ぐ
- 居場所確認機能、子どものスマホ利用状況のレポート

大切なのは、親子でしっかりと話し合っ、安全な利用を実現することです。また、子どもから相談を受けたときに適切な対応がとれるよう、親も知識のアップデートをおこたらないようにしたいですね。

困ったときの相談先

ネットトラブルに関する被害相談

消費者ホットライン

い や や
(局番なし) **188**

18歳までの子ども専用 電話・チャット相談

チャイルドライン®

■ 電話番号 0120-99-7777

(毎日 16:00~21:00)

※12/29~1/3はお休みとなります。



フィッシングに関する相談・情報提供

フィッシング 110 番



SNSトラブル相談窓口

法務省インターネット
人権相談受付窓口



警察への相談

警察相談電話

#9110



全国防犯協会連合会

発行

公益財団法人 全国防犯協会連合会

<http://www.bohan.or.jp/>



監修

警察庁サイバー警察局

