ネット社会の危険

インターネットは、現在の私たちのくらしに、もはや欠かせないものとなっています。モバイル端末の普及に伴い、いつでも・どこでも、さまざまな情報を手に入れられるようになりました。しかし、便利になった反面、インターネットを通じて、詐欺被害、個人情報の流出、掲示板での炎上など、さまざまな問題・事件が起こるようになってきました。

スマートフォンが、小学生から高齢者まで幅広い世代に浸透したいま、インターネットにある多くの危険から身を守るため、利用者のICTリテラシーを向上させることが重要となっています。

●ICTリテラシーを学んでトラブルを避けよう

ICTとは、Information（情報）、Communication（通信）、Technology（技術）の略で情報通信技術を意味します。ICTリテラシーは、インターネットの情報を読み解く能力やスマートフォン、クラウドサービスなどのツールを安全・安心に活用してコミュニケーションを行う能力のことです。

インターネットを安全・安心に利用するには、パソコンやスマートフォンの操作ができるだけではなく、ネット社会において危険なトラブルをさけるために必要となる知識やスキルを学ぶことが必要です。

スマートフォンやSNSをもっと楽しむために、ICTリテラシーを身につけましょう。

●ICTリテラシーを学ぶには？

多くの分野において、ICTリテラシー向上のためのさまざまな取組が進められています。

「ICTメディアリテラシーの育成」

総務省では、子どもから高齢者まで安全に安心してインターネットや携帯電話などのICTを利活用できるようホームページで学習コンテンツ等を公開しています。教材は、無料で利用することができます。

https://www.soumu.go.jp/main_sosiki/joho_tsusin/kyouiku_joho-ka/media_literacy.html

「インターネットトラブル事例集」

総務省では、インターネット、スマートフォンを始めとするデジタル機器、SNSなどのコミュニケーションツールについて「賢く活用する知識・知恵」「ルールを守って使える健全な心」「安全に利用するための危機管理意識」を育む一助として、インターネットトラブル事例集を作成し、その予防法と対処法を紹介しています。

https://www.soumu.go.jp/use_the_internet_wisely/trouble/

「インターネットルール＆マナー検定」

（一財）インターネット協会では、インターネットを安全・安心に利用するためのルールやマナーに関する無料のWeb検定試験を行っています。「ビジネス版」、「こどもばん」、「こどもばんふりがな」、「大人版」の四種類があり、サイトから24時間受検することができます。

https://rm.iajapan.org/

情報発信は慎重に行いましょう

●インターネットで発信した情報は消えません

インターネットは、世界中の人々へ個人でも発信できるメディアです。発信した情報は基本的に全世界に公開されることになり、簡単に複製され、短時間で広まると削除することもできなくなります。

そして、発信した内容によっては意図しない想定外の反応が起こることもあります。

●その書き込み、本当に大丈夫？

以前からSNSなどでの発言をきっかけに、個人や企業への批判や誹謗中傷が、不特定多数から集中して寄せられる事象が起こっています。いわゆる“ネット炎上”です。

批判や誹謗中傷の対象とされた方が、無関係の第三者だった場合、問題はさらに深刻になります。

2019年８月に高速道路で発生したあおり運転に関連して男女が逮捕された事件がありました。この際に、暴行の様子を撮影する女の動画が拡散したことをきっかけに、ネット上では、事件とはまったく関係のない女性の名前や写真、会社名が投稿され、多くの事実無根の誹謗中傷を受けることとなりました。

「誤った情報を発信するとその責任を問われます。他人を傷つけるような投稿は自分に跳ね返ってきます」書き込みなどの情報発信をきっかけに、警察に逮捕されたり、相手から損害賠償を請求されたり、学校や職場から処分を受ける事例もあります。情報発信する際は、個人情報を含んでいないか、人を傷つけるような内容が含まれていないか、真偽不明の情報でないか、などを必ず確認するよう心がけましょう。

●個人情報の公開は最小限に

SNSの利用にあたっては、インターネット上に、氏名、メールアドレス、写真といった情報を公開することの危険性についても、きちんと認識しておかなければなりません。不用意に個人情報を書き込んでしまうと、さまざまなトラブルを呼び込むきっかけとなります。

トラブルから身を守るため、投稿する内容は最小限にし、むやみに個人情報を公開しないようにすることが大切です。

SNSは、利用者の使い方にあわせて投稿内容やプロフィール閲覧の公開範囲が制限できますから、トラブルや情報をとられることを避けるため、少なくとも「投稿公開範囲」、「アカウントの検索可能範囲」を次のように設定しておくとよいでしょう。

2024年12月現在

	投稿公開範囲	アカウントの検索可能範囲
LINE	設定＞LINE VOOM＞新しい友だちに自動公開＞OFF 設定＞LINE VOOM＞友だちの公開設定＞友だちごとに公開・非公開を設定	設定＞友だち＞友だち自動追加＞OFF 設定＞友だち＞友だちへの追加を許可＞OFF 設定＞プライバシー管理＞IDによる友だち追加を許可＞OFF
Facebook	メニュー＞設定＞設定とプライバシー＞共有範囲と公開設定＞投稿＞今後の投稿のプライバシー設定＞友達	メニュー＞設定＞設定とプライバシー＞共有範囲と公開設定＞検索と連絡に関する設定＞あなたから提供されたメールアドレスまたは電話番号を使って私を検索できる人＞友達
X（旧Twitter）	設定とサポート＞設定とプライバシー＞プライバシーと安全＞オーディエンスとタグ付け＞ツイートを非公開にする	設定とサポート＞設定とプライバシー＞プライバシーと安全＞見つけやすさと連絡先＞メールアドレスまたは電話番号の照会と通知を許可する＞OFF 見つけやすさと連絡先＞アドレス帳の連絡先を同期＞OFF
Instagram	設定＞設定とアクティビティ＞アカウントのプライバシー＞非公開アカウント＞OK	設定＞設定とアクティビティ＞アカウントセンター＞あなたの情報とアクセス許可＞連絡先をアップロード＞連絡先をリンク＞OFF

※設定方法はOSや機種、アプリのバージョンにより異なります。

また、公開範囲を友だちに限定していてもその友だちが内容を転載してしまうこともあり得ます。ネット上に書きこんだ文章・写真は決して取り消すことはできませんから、普段から不特定多数に読まれたり見られたりしても困らない内容かどうか十分注意をして投稿するようにしましょう。

3 意図しない情報の流出を防ぎましょう

●知らないうちにあなたのいる場所を公開していませんか

いろいろな利用者との日常的な会話から情報収集までできるSNSは便利で楽しいサービスですが、一方で、SNSに掲載されたこれらの情報を狙う犯罪者が増えていることにも注意が必要です。

SNSでは、アプリの位置情報利用をONに設定にしておくと、投稿に位置情報が付けられ、自分の所在地を不特定多数へ知られることにもなりかねません。頻繁に位置情報を公開していると住所や学校などの個人情報が特定されるおそれもありますので注意してください。

スマートフォンのプライバシー設定で位置情報サービスの設定を利用しないこともできますので、一度設定を見直しましょう。

2024年12月現在

	位置情報OFF設定
LINE	スマートフォンの設定でLINEの「位置情報利用」権限をOFFにする
Facebook	スマートフォンの設定でFacebookの「位置情報利用」権限をOFFにする
X（旧Twitter）	「設定」＞「設定とプライバシー」＞「プライバシーと安全」＞「位置情報」＞正確な位置情報をもとにカスタマイズをOFFにする
Instagram	スマートフォンの設定でInstagramの「位置情報利用」権限をOFFにする

※設定方法はOSや機種、アプリのバージョンにより異なります。

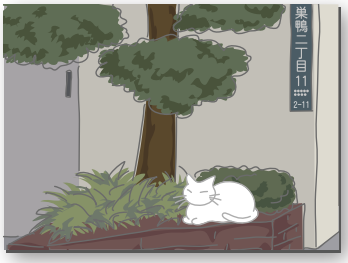
●写真から自宅の場所がわかってしまうこともあります

スマートフォンで撮影した写真に、撮った場所が記録されているって知っていますか？

スマートフォンには、GPS機能がついているので、カメラアプリの設定が位置情報機能ONになっていると、撮影した写真に位置情報が記録されています。

ということは、位置情報機能をONにしたまま、自宅で写真を撮って、その写真をそのままインターネットへ公開してしまうと、自宅の場所が特定できてしまうことになりますね。

トラブルを避けるためにも、カメラアプリの位置情報機能はOFFにしておきましょう。



●位置情報機能をOFFにしても場所がわかってしまう？

写真に写り込む情報から、その場所がわかってしまうこともあります。電信柱などに書いてある住所が写真に写っているかもしれませんし、お子さんの入学式の写真だったらその学校がわかってしまうかもしれません。

SNSの中には、投稿するときに付近のお店などのスポット情報を「位置情報」として追加することもできるものもありますが、自宅や学校などで撮影した写真にその「位置情報」をつけてしまうと、おおよその場所がわかってしまいます。自宅周辺などからの投稿では「位置情報」を追加するのはやめましょう。

カメラの位置情報利用をOFFにしても、決して安心はできません。写真をインターネットへ公開する際は、事前によく確認するようにしましょう。

コラム

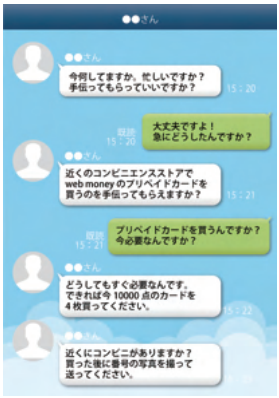
SNSアカウントが乗っ取られる被害が増えています！

スマートフォンの普及でSNSの利用者が増えてくると、SNSでも悪質サイトへ誘導する迷惑メッセージや詐欺被害なども発生するようになりました。知らないうちにアカウント（ID・パスワード）を乗っ取られて不正利用されるという被害もあとを絶ちません。

●アカウント管理がとても重要です

アカウントを乗っ取られるとクラウド上に保存してあるプライベートな情報が盗まれたり、詐欺サイトへ誘導しようと、つながっている友人知人にあなたのアカウントで不正なメッセージが送信されたりします。

特に、SNSアカウントとアプリの連携には注意が必要です。アプリ側がこの機能を利用できるようになると本来アカウント利用者しか行えない操作をアプリ側が外部から行えるようになってしまいます。不正なアプリだった場合、不正ログインされてアカウント情報を盗みとられてしまうわけです。



●アカウント乗っ取りでこんな被害も

IDとパスワードを不正な手段で入手した乗っ取り犯が、勝手にログインしたうえで、そのアカウントの友人・知人へ「緊急で必要だからプリペイドカードを購入して番号を知らせて」とメッセージを送り、金券番号をだましとるという事件もありました。

全く知らない他人なら、怪しんだり警戒したりしますが、友人・知人の名前で送られてきたメッセージだったために疑うことはなく協力してしまい、多数の被害が発生してしまいました。少し不審な内容でも信じて協力してしまったようです。

●パソコンなどからはログインできないようにもできます

LINEはパソコンやタブレットからも利用することが可能です。もし、乗っ取り犯がパソコンやタブレットから不正にログインしたとしても、スマートフォンでは、いつもどおりLINEアプリが利用できるため、通知が届いても乗っ取られたことに気づかない可能性があります。

スマートフォンでの利用しかしない場合は、パソコンなどからログインできないよう設定しておくと安全です。

「設定」→「アカウント」→「ログイン許可」をタップし、チェックを外す

乗っ取られないための対策

アカウントを乗っ取られないために、以下の点に注意し、対策をしておきましょう。

1．複数サービスでIDやパスワードの使い回しをしない
乗っ取り犯は、入手したIDやパスワードで他のサービスにも不正ログインを試みます。同じID・パスワードにしておくと複数のSNSが乗っ取られる可能性があり危険です。

2．SNSサービス間のアカウント連携を避ける
最近のSNSの多くは連携機能を利用して同時投稿などができますが、上記と同じように、１つのアカウントが乗っ取られた場合、連携機能を利用して他サービスにもアクセスされることになってしまいます。

3．２段階認証を利用する
２段階認証は、ログイン時にSMSで届く認証コードの入力を必要とする機能です。多くのSNSサービスでは、アカウント乗っ取り対策として、いつもと異なるスマートフォンやパソコンなどの環境からログインした場合、登録しておいた携帯番号へSMSで認証コードが送られ、そのコードを入力しないとログインできない設定とすることができます。もし、IDやパスワードが流出してしまっても、これにより不正ログインを防ぐことができます。

乗っ取られてしまったときは

乗っ取り犯により不正ログインされたことに気づいたときは、すぐにパスワードを変更しましょう。もし、既にパスワードが変更されてログインできないときは、運営会社に連絡して対処してください。

参考Webサイト

LINE
ヘルプセンター

Facebook
ヘルプセンター

X(旧Twitter)
ヘルプセンター

Apple
サポート

緊急時の情報発信

●緊急時にはデマが広がります

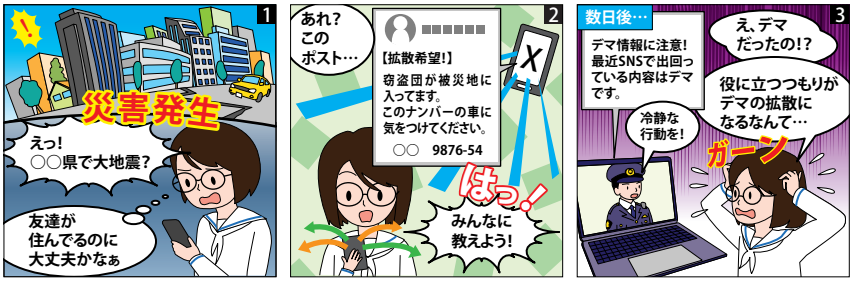
災害発生時や緊急時には、安否確認、緊急情報、最新の災害情報、救急救命情報の収集や支援要請の情報発信などスマートフォンなどのモバイル端末を使ったコミュニケーション手段が大きな役割を果たしています。反面、メールやX（旧Twitter）、LINEなどのSNS上では、実際に起こっていない事故や事実と異なる情報、必ずしも正確ではない情報、面白半分で載せたウソの情報などが発信されデマとして広がります。過去の震災、大型台風による災害時も、多種多様のデマ情報が発生しました。

●デマが広がる理由

緊急時においては、人々は、不安な状況が続く中、少しでも役に立つ情報を得ようとします。そして、「役に立ちそうな情報」を見つけると、「みんなに伝えるべき情報」と考え、情報の信頼度にかかわらず、友人や知人へ伝えようとします。

友人や知人から得た情報は、一般的にその価値を高く見てしまうようで、チェーンメールとなったり、SNS上で拡散していきます。

SNSでは書き込み後、ボタンひとつで全世界に情報を発信することができます。災害時のこうした拡散しやすい状況と便利なツールが重なり、災害後にデマが広がりやすくなっていきます。



●デマがもたらす悪影響

1．内容によっては混乱を引き起こしたり、被災者の不安を拡大させる

災害時や緊急時だからこそ、正確な情報が必要です。真偽を確かめないまま情報を送ることは、たとえ善意の気持ちからであってもやめましょう。

2．誤った情報や不確かな情報は混乱や活動に支障をきたすおそれがある

刻一刻と状況が変わる中で、最初は正しかった情報だったとしても時間の経過により誤った情報になることも考えられます。不確かな情報は、現場に無用な負担を強いることになりかねず、現場が混乱し活動に支障をきたしかねません。

3．限られた通信環境を圧迫し、必要な情報が行き届かないことにもなりかねない

デマ情報の拡散で、通信ネットワークの負荷が上昇し通信環境への深刻な影響を引き起こすことにもなりかねません。

●災害時や緊急時だからこそ、情報発信は正確に

真偽の分からない情報が拡散すると、本当に必要な情報を阻害する原因にもなりかねません。

もし、根拠の疑わしい情報・未確認の情報のメールやSNS上の情報を見たときは、もしかしたらデマかもしれないと疑い、まずは情報の真偽を確かめるようにしましょう。

情報を誰かに伝えるときは、真偽を確かめてから責任を持って発信するように心がけましょう。

- ✓情報の発信源は誰かを確かめる。
- ✓いつの時点の情報かを確かめる。
  →刻一刻と変わる現場では常に最新の情報が必要です。
- ✓複数の報道機関、媒体でも確認する。
  →ネットの情報だけではなく、ラジオなど複数の情報源で確認しましょう。