国民のための
サイバーセキュリティサイト

総務省

事故・被害事例および対処法

（セキュリティ事故が起きた後にやるべきことは）

家庭での被害事例及び対処法

適切な情報セキュリティ対策を実施していないと、どんな問題が起きる可能性があるのでしょうか？
ここでは、実際に「家庭」で起こった事故・被害をもとにした事例を紹介します。
併せて、被害に遭った際の対処法や、どうすれば防ぐことができたのかについても解説します。

目次

私の名前で誰かがメールを

■ **事故・被害事例**

大学４年生のＡ子さんは、ある会社に就職が内定していました。ところがいつまで待っても、肝心の採用通知が送られてきません。そこで、会社の人事担当者に連絡すると、なんと Ａ 子さんから電子メールで内定を辞退するという連絡があったというのです。驚いた Ａ 子さんは、担当者に再度電子メールを確認してもらいましたが、間違いなくそれは大学で使用しているメールアドレスでした。

慌てて大学に調査を依頼したところ、同じサークルの男子学生が Ａ 子さんになりすまして、人事担当者に電子メールを送っていたことが分かりました。男子学生は、Ａ 子さんのユーザ名とパスワードを盗み出していたそうです。男子学生は、他人のユーザ名を使用して認証サーバにアクセスしたということで、不正アクセス禁止法違反容疑で逮捕されました。

■ **対処法**

同様の被害を受けた場合には、以下の手順での対処を考えることができます。

1. パスワードの変更：メールアカウントのパスワードを変更し、犯人による再度の不正利用を防ぎましょう。
2. 第三者からの支援を受ける：第三者からの支援を受けられないか検討しましょう。例えば、学校ならば教員やシステムの管理者、家庭なら保護者などに相談してみましょう。
3. メール送信先との調整：メール送信先との調整を検討しましょう。
4. 法的アドバイスの検討：もしも問題が解決しない場合や、将来的に法的な問題が発生する可能性がある場合は、法的アドバイスを受けることを検討します。

ネットストーカーに注意

■ **事故・被害事例**

N さん(女性)は、SNS にプロフィールや自分の写真、近況などを投稿し、すべての人に公開していました。N さんは、自分の投稿を見た人たちから寄せられるコメントやメッセージを毎日楽しみにしていました。

ある日、面識のない男性から「僕とつきあってください」というメッセージが届きました。最初は適当に返事をしていましたが、あまりにもしつこくメッセージが送られてきます。たまりかねて、「迷惑ですので、もうメッセージしないでください」という返事をしたところ、事態が急変しました。

次の日から、脅迫的な言葉を並べたメッセージが次々と送られてくるようになり、N さんを誹謗中傷する投稿もされるようになったのです。しばらくすると、「おまえの住んでいる場所は分かっているんだ」というメッセージも送られてきました。そこに書かれているのは確かに N さんの住所でした。気味が悪くなった N さんは、自分の SNS のアカウントを削除し、引越しを検討することになってしまいました。

これは一つの例ですが、このようなネットストーカーの事件は実際に数多く発生しています。今回は、N さんが投稿している内容の公開範囲がすべての人になっていたり、コメントやメッセージを誰からでも受け付ける設定になっていたり、SNS で公開している投稿や写真に住所を特定できる情報が付加されていたことから、ストーカー行為がエスカレートしました。

ネットストーカーによる被害は、電子掲示板や SNS にいやがらせをされたり、大量の電子メールやメッセージを送りつけられたりといったことだけにとどまらない場合があります。実際に自宅にまで押しかけてきたり、後をつけまわしたりといったように、ネット上から実世界のストーカー行為に移行する例もあります。SNS の投稿範囲、コメントやメッセージの受け付け、位置情報の付加などの設定には、十分に注意しましょう。

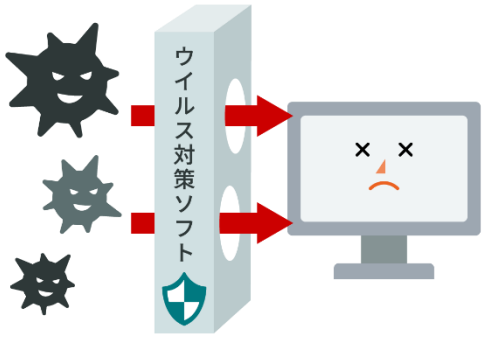
■ **対処法**

このような被害に遭ったときは、まずは証拠を保存しましょう。SNS や電子掲示板に書き込まれた脅迫や誹謗中傷のメッセージは削除される可能性があるため、スクリーンショットなどで保存しておきましょう。

また、住所を特定されたり、実生活でのストーカー行為に発展したりした場合は、速やかに警察に相談しましょう。

マルウェア（ウイルス等）対策はしていたはずなのに・・・

■ **事故・被害事例**



S さんが使用しているコンピュータは、1 年ほど前に購入したものです。当時、コンピュータを使用している友人がウイルスに感染したこともあり、安心して利用できるように、マルウェア対策ソフトが初めからインストールされているコンピュータを選択しました。

S さんは、そのコンピュータで電子メールやホームページの閲覧、ショッピングなど、インターネットを楽しんでいました。しかし、ある日、友達のＴさんからの電子メールを見てびっくりしました。その電子メールには、「あなたからマルウェア付きの電子メールが送られてきた」と書かれていたのです。

そんなはずはありません。S さんのコンピュータには、購入したときからマルウェア対策ソフトがインストールされているのです。それなのに、マルウェアが侵入したというのでしょうか。

これは、S さんが大切なことを忘れていたのが原因です。マルウェア対策ソフトは、電子メールやホームページのデータに今までに発見されているマルウェアが含まれていないかどうかを検出する仕組みになっています。つまり、まったくの新種のマルウェアは、発見することができない可能性があるのです。

このケースでは、S さんがパソコンを購入した後に、マルウェア対策ソフトのパターンファイル（ウイルス検知用データ）の更新を一度もしていなかったため、新しいマルウェアに感染してしまったというわけです。

■ **対処法**

Wi-Fi 接続を OFF にしたり、LAN ケーブルを抜いたりして、インターネットに接続できない状態にしましょう。

そして、パソコンを購入した家電量販店やパソコンショップ等に持って行って相談しましょう。

フリマアプリの商品が届かない

■ **事故・被害事例**

Ｙ さんは、いつもフリマアプリでお気に入りのブランド品の出物を探しています。今回も、フリマアプリで限定品のバッグを見つけたため、早速フリマアプリを購入しました。その出品者は業者であるらしく、ある理由で手持ちの多くの商品をすぐに売りたいということでした。市価よりもずっと安いとはいえ、かなり高額な商品であったため、最初は少し迷いましたが、既に何人かの会員がその業者から商品を受け取っているのを見て、安心して購入しました。

しかし、何日たっても商品は送られてきません。フリマアプリで出品者に連絡しても返事がありません。仕方なく待っていると、取引完了となり出品者へ支払いが実行されてしまいました。しばらくすると、初期に購入した会員以外には、誰も商品が送られて来ていないということが発覚しました。

時期をずらして大量に出品して、初めの頃の相手にだけ商品をきちんと送ることで、他の購入者を安心させ騙すという手口だったようです。悪質なケースでは、最初の頃は犯人が自ら別の名前で落札していただけで、実は初めから何一つ商品を用意していなかったという例もあります。

■ **対処法**

フリマアプリで購入した商品が発送されたのになかなか届かない場合、取引完了の条件について、フリマアプリの利用規約をよく確認し対処してください。

たとえば、取引メッセージを送り続けている限りは取引完了とならなかったり、逆に取引メッセージが一定期間ないと取引完了となってしまったりする条件が、利用規約に記載されていることがあります。

また、フリマアプリの運営にも商品が届かない旨連絡をしておきましょう。

■ **予防法**

フリマアプリで商品が届かずお金をだまし取られないようにするには、次の対策が考えられま

す。

1. 商品を購入する前に、出品者の評価やコメントを確認します。評価が低い、コメントがない、または悪いコメントが多い場合は、注意が必要です。
2. 商品の写真や説明をよく見ましょう。写真がぼやけていたり、他のサイトからコピーされている可能性があったりする場合は、疑わしいと思ってください。説明が曖昧だったり、重要な情報が抜けていたりする場合も同様です。
3. 商品の値段や送料をチェックしましょう。値段が相場よりも安すぎたり、送料が高すぎたりする場合は、トラブルのリスクが高まります。また、直接取引を持ちかけられた場合も、メルカリの保証制度が適用されなくなるので、断るべきです。

中古パソコンによるデータの漏洩

■ **事故・被害事例**

ある大学生が中古パソコンを購入しました。購入後、市販のデータ復元ソフトを使用してハードディスクのデータを復元してみたところ、ある医療機関が健康保険組合などに医療費を請求するために作成した診療報酬明細書の画像データが残されていました。

この大学生は故意ではありませんでしたが、企業内の機密情報収集を目的として、中古パソコンを購入するという手口も実際に行われているようです。

■ **対処法**

復元された診療報酬明細書の画像データは、個人情報を含む可能性があります。漏えいさせてしまっては大変です。まず、復元した診療報酬明細書の画像データをすぐに削除しましょう。

次に、中古パソコンを購入した店舗に連絡し、事情を説明してください。そして、返品できないか交渉しましょう。

クレジットカード番号が盗まれた

■ **事故・被害事例**

いつもインターネットでショッピングを楽しんでいる O さんの元に、ある日、次のような内容の電子メールが届きました。

> ○×カードより
> いつも当社のクレジットカードをご利用頂きまして、誠にありがとうございます。
>
> 最近、他人のクレジットカードを利用して、不正にショッピングを行う悪質な犯罪が増加しています。そのような不正利用への対策として、当社では一定期間ごとに暗証番号の変更をお願いしています。
>
> 以下の URL から弊社のホームページに接続して頂き、お名前、クレジットカード番号、暗証番号をご登録ください。
>
> http://www.××××.com/henkou/
>
> なお、このメールをお受け取り頂いてから 1 ヶ月以内にご登録頂かなければ、お持ちのクレジットカードがご利用できなくなるため、ご注意ください。

この電子メールを受け取った O さんは、早速メールに記載された URL をクリックして、表示されたホームページで、自分の名前、クレジットカード番号、新しい暗証番号を登録しました。

・・・ そして、1 ヶ月後 ・・・

郵送されてきたクレジットカードの請求書を見た O さんは、とてもびっくりしました。そこに記載されていたのは、自分が想像していたものよりもずっと大きな金額だったのです。明細を見ると、まったく買い物をした記憶がないお店で、クレジットカードを使用したことになっていました。

このような、電子メールとホームページを利用した悪質な情報収集の手口をフィッシング詐欺といいます。フィッシング詐欺の多くは、クレジットカード会社や銀行、ショッピングサイトなど、実在する有名な会社の名前を装って、不特定多数の人に電子メールを送信します。そして、電子メールに記載された URL から本物そっくりの偽のホームページに誘導し、重要な個人情報やカード番号などを登録させるのです。

フィッシング詐欺による電子メールの多くは、受信者がついうっかり個人情報を登録してしまうような巧妙な文面になっています。

自分の利用しているクレジットカードの会社や銀行の名前で電子メールが送られてきても、すぐに信用してはいけません。電子メールに記載されている内容をよく読んで、不明な点や怪しい点がある場合には、その会社に問い合わせを行うようにしてください。電子メールに記載されている URL が本当にその会社のものであるかどうかを確認することも大切です。

URL が正しいように見える場合でも、ホームページでクレジットカード番号や暗証番号、パスワードなどを登録したり変更したりするように促す電子メールについては、リンクが詐称されている可能性があるという点にも注意するようにしてください。また、電子メールだけでなく、SMS や SNS でのメッセージでも同様の注意が必要です。

■ **対処法**

クレジットカードの請求に身に覚えのない買い物があった場合、まず、請求書や明細書をよく確認して、本当に自分が行っていない取引かどうかを判断します。時々、店舗名や商品名が異なって表示されることがありますので、よく確認しましょう。

次に、カード会社に連絡して、不正利用の疑いがあることを報告します。カード会社は、取引の詳細や利用履歴を調査して、不正利用かどうかを判断します。不正利用であれば、カード会社はカードを停止したり、新しいカードを発行したりします。

さらに、警察に届け出をします。不正利用は犯罪ですので、警察に被害届を提出することが重要です。警察は、犯人の特定や逮捕に協力してくれます。また、被害届を提出することで、カード会社との補償交渉にも有利になります。

有名サイトからダウンロードしたはずなのに・・・

■　**事故・被害事例**

B さんは、撮りためたデジタルカメラの画像を整理するうちに、気に入った写真の加工をしてみようと思い立ちました。しかし、どんな画像の加工ソフトがあるのか知りませんでした。そこで、検索エンジンを利用して、よく使われていて評判のよい無料ソフトを探すことにしました。

検索エンジンの上位に出てきた口コミサイトで、ある無料ソフトの口コミを見てみると、かなり多数の人がダウンロードしていて、評判を表す☆の数も多く、そのソフトを推奨するコメントばかりでした。またそのソフトは、ある有名ダウンロードサイトから配布されていると説明されていました。そこで B さんは安心して、その無料ソフトを使うことにし、その口コミサイトに掲載されていたリンクから、有名ダウンロードサイトに行き、ソフトをダウンロードしました。

利用してみると、口コミサイトの評判ほどではありませんでしたが、基本的な機能は備わっています。無料ソフトということで納得し、そのまま利用していました。

数ヵ月後、いつものようにこのソフトを利用しようとすると、マルウェア対策ソフトから警告メッセージが出てきました。詳細を調べると、このソフトはマルウェアだったようです。有名ダウンロードサイトから入手したはずなのに、なぜそんなものがインストールされたのでしょうか。

実は B さんは、悪意のある口コミサイトにあったリンクから、有名ダウンロードサイトに似せた偽のホームページに誘導され、画像加工ソフトに見せかけたマルウェアをインストールさせられたのです。口コミサイトに書かれていた評判も、すべて嘘の情報だったのです。しかも新種のマルウェアだったため、インストール時にはマルウェア対策ソフトも検知できませんでした。

検索エンジンで出てくる情報が、すべて無害とは限りません。このように悪意のあるホームページへと誘導されることもあります。インターネット上でソフトなどをダウンロードする場合は、できる限り信頼できる正規のホームページからダウンロードするようにしましょう。

■　**対処法**

＜家庭の利用者＞

Wi-Fi 接続を OFF にしたり、LAN ケーブルを抜いたりして、インターネットに接続できない状態にしましょう。

そして、パソコンを購入した家電量販店やパソコンショップ等に持って行って相談しましょう。

＜職場でシステムを“利用”する人＞

一般的に企業や組織ではパソコンにマルウェアが感染した可能性がある場合の対応方法が定められているはずなので、まずはそのルールに従いましょう。一般的には Wi-Fi 接続を OFF にしたり、LAN ケーブルを抜いたりして、インターネットに接続できない状態にします。その上で、システムを管理している担当者に報告し、指示を仰ぎましょう。

＜職場でシステムを“管理”する人＞

■ **被害範囲の調査**

被害の内容を正確に特定するために調査を実施しましょう。

その際には必要に応じてマルウェア感染パソコンに対してフォレンジクス分析などの高度な調査分析を（外部の専門業者に依頼するなどして）実施することも検討しましょう。

また、社内システム全体に被害が広まっている可能性も考慮して、外部の専門業者に調査分析を依頼することも検討しましょう。

■ **マルウェアの駆除**

従業員にパソコンを返却する場合は完全にクリーンナップ（初期化）した上で OS の再インストールを実施してください。

■ **関係各所への報告**

被害が社外にも及んでいる場合には被害を受けた関係各所への報告、必要に応じてプレスリリースや記者会見といった対応を検討しましょう。

Wi-Fi ルーターの認証情報が盗まれた・・・

■ **事故・被害事例**

Wi-Fi ルーターは、一般にインターネット回線と自宅内ネットワークの境界に設置するもので、現在、多くの製品が発売されています。しかし、中には脆弱性（ぜいじゃくせい）のあるものがあり、アクセスを許可されていない第三者がルーターの内部にアクセスし、その Wi-Fi ルーターを外部への攻撃の踏み台に悪用する事例が発生しています。

■ **対処法**

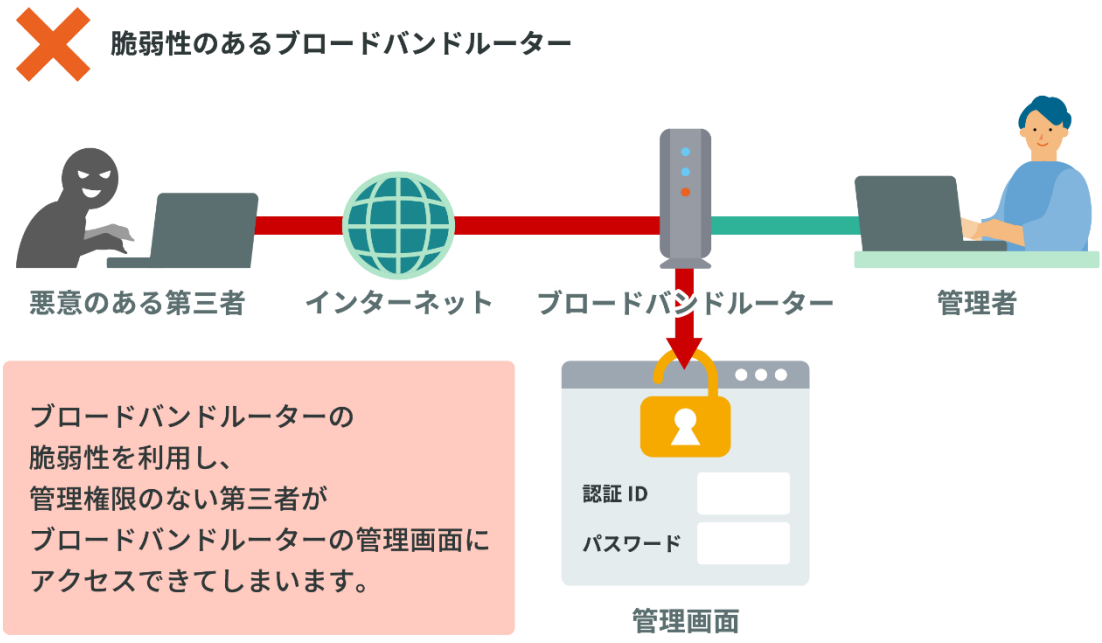
Wi-Fi ルーターの認証情報が盗まれた場合、下記の対処を行いましょう。

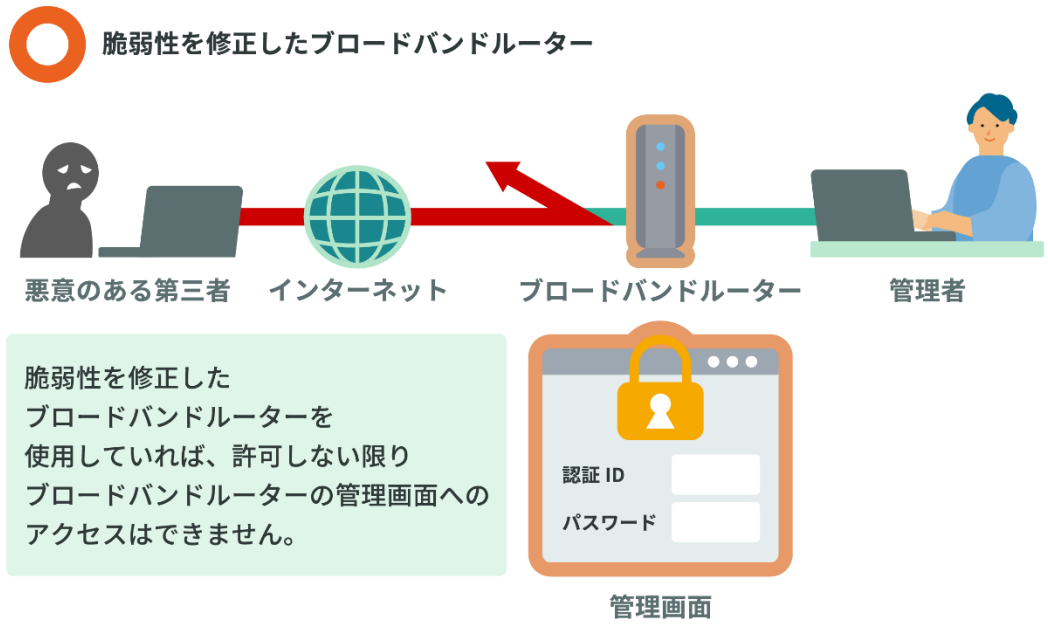
1. ルーターの管理画面にアクセスして、管理者パスワードを変更しましょう。
2. 接続されているデバイスを確認して、不審なものがないかチェックしてください。もし不審なデバイスがあれば、ブロックするか、Wi-Fi のパスワードを変更しましょう。
3. VPN 機能や DDNS 機能などリモートからルーターにアクセスできる機能が意図せず有効になっていないか確認し、意図しない機能が有効になっていた場合には無効化しましょう。
4. ルーターのファームウェアを最新版に更新して、セキュリティの脆弱性を修正してください。

※その他の対処法として、Wi-Fi ルーターを初期化（工場出荷時の状態に）してからファームウェアを更新して再設定する方法もあります。初期化の際の注意事項や再設定のやり方について、Wi-Fi ルーターの取り扱い説明書を確認してください。

■ **予防法**

総務省｜無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について（soumu.go.jp）





スマホが壊れて写真や動画を失った

■ **事故・被害事例**

S さんは、普段からよくスマホを使っていました。特に友人や家族と写真や動画を撮って楽しんでいました。

ある日、スマホが水没してしまい、S さんはパニックになりました。スマホに保存していた思い出の写真や動画を失ってしまうからです。どうすればいいのか分からず、困ってしまいました。

■ **対処法**

水没したスマホの電源をすぐに切りましょう。すでに電源が切れている場合は、電源を入れないでください。

次に、タオルや柔らかい布で、スマホの表面から水分をできるだけ拭き取ります。スマホ内部を乾燥させるために、風通しの良い日陰の場所にスマホを 1 日程度置いておきましょう。

十分に乾かした後は、データ復旧の専門業者に相談しましょう。必ず復旧できるわけではないため、このような事態に事前に備えておくことが重要です。

■ **予防法**

このような事故は、誰にでも起こり得ます。スマホは便利ですが、壊れたり紛失したりするリスクもあります。そこで、大切なデータを守るためには、バックアップをすることが必要です。バックアップとは、データを別の場所にコピーしておくことです。例えば、パソコンや外付けハードディスク、クラウドサービスなどにデータを保存しておくことができます。バックアップをすることで、万が一の場合でもデータを復元することができます。

バックアップの方法はいくつかありますが、ここでは簡単なものを紹介します。まず、スマホに搭載されているバックアップ機能を利用する方法です。iPhone なら iCloud、Android なら Google アカウントにログインして、設定からバックアップを有効にするだけです。これで、スマホのデータが自動的にクラウドに保存されます。次に、パソコンや外付けハードディスクに接続してバックアップする方法です。USB ケーブルや Wi-Fi などでスマホとパソコンや外付けハードディスクをつなげて、ファイルをコピーします。これで、スマホのデータが手元に保存されます。

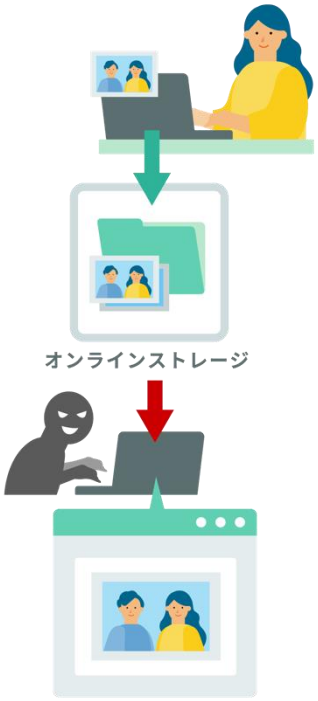
以上のように、バックアップは簡単にできるものですが、非常に重要です。スマホの紛失や故障に備えて、定期的にバックアップをする習慣をつけましょう。

友達だけに共有したつもりの写真が全世界に公開されてしまった

■ **事故・被害事例**

S さんは先月、友達と一緒に海外旅行に行きました。そのときに撮った写真を、友達だけに見せるためにファイル共有サービス（オンラインストレージ）にアップロードしました。

しかし、S さんはうっかり写真の共有設定を間違えて、誰でもアクセスできるようにしてしまいました。その結果、S さんの写真がインターネット上で拡散されてしまいました。中には、S さんが水着姿でポーズをとっている写真や、友達と飲酒している写真もありました。



これらの写真は、S さんのプライバシーを侵害するだけでなく、S さんの仕事や人間関係にも悪影響を及ぼす可能性があります。S さんはすぐに写真の共有設定を変更しましたが、すでに遅すぎました。

S さんはこの事態に対して、どう対処すべきかわかりません。S さんは自分の不注意で大きなトラブルを引き起こしてしまいました。

■ **対処法**

紹介した例では手遅れですが、誤った共有設定を変更することが大切です。

拡散されてしまった写真を削除することはできません。せめて写真に写っている友達への謝罪を行いましょう。

■ **予防法**

ファイル共有サービスにアップロードする前に、公開範囲をしっかりと確認し、適切な範囲に設定しましょう。

突然データが見られなくなった

■ **事故・被害事例**

ある日Xさんは、いつも利用している社内システムへ接続できないことに気づきました。システムの担当者に調査を依頼したところ、右図のような警告がでていると報告を受けました。調査した結果、システムがサイバー攻撃を受け、ランサムウェアに感染したことによりシステムが使用できない状態になっていることがわかりました。

原因は、社外から社内へ接続する際に使用するVPN機器の脆弱性を悪用されたことによるものでした。その結果、社内の ID を窃取され、社内システムにランサムウェアを展開されたのです。

ランサムウェアはマルウェアの一種であり、システムの不正ロックや、データの不正な暗号化により、使用できない状態にします。またランサム（身代金）と呼ばれているように、身代金が要求され、支払わない限りシステム復旧ができないことが多いですし、支払ったとしてもシステムが復旧できると限りません。
ランサムウェアに感染した際に、データが窃取されていることもあり、当該データの公開を人質に身代金要求されることもあります。
今回挙げた事例は VPN の脆弱性を突かれたケースですが、その他にも悪意のあるメールの添付ファイルを開いて感染するケースや、不正なコードを埋め込まれたWebサイトを閲覧することによって感染するケースもあります。

■ **対処法**

ランサムウェアに感染した場合、感染原と接続されているネットワークストレージ等が暗号化されないよう、速やかに感染した端末・システムをネットワークから遮断してください。警察への被害報告も忘れずに実施しましょう。

その後は下記のサイトなどを参考に調査や復旧、再発防止対策を行いましょう。

ランサムウェア被害防止対策｜警察庁 Web サイト（npa.go.jp）
ストップ！ ランサムウェア - NISC

■ **予防法**

ランサムウェアの被害を防ぐためには、以下の対策が必要です。

- ソフトウェアの最新化
- マルウェア（ウイルス等）対策
- 悪意のあるウェブサイトへの対策
- データ保護・バックアップ

Word ファイルを開いただけで・・・

■ **事故・被害事例**

Y さんは、ある日、取引先の会社からメールが届きました。メールには、「契約書の最終確認をお願いします」と書かれており、Word ファイルが添付されていました。Y さんは、何も疑わずに Word ファイルを開きました。すると、画面に「マクロを有効にしてください」というメッセージが表示されました。Y さんは、メッセージに従ってマクロを有効にしました。しかし、それが間違いだったことに気づくのは、後のことでした。

マクロを有効にしたことで、Word ファイルに隠されていた Emotet というマルウェアが実行されました。Emotet は、Y さんのパソコンからメールアドレスやパスワードなどの個人情報を盗み取りました。さらに、Emotet は、Y さんのパソコンを乗っ取って、Y さんの知り合いや取引先にも同じようなメールを送りました。その結果、Y さんの周囲では多くの人が Emotet に感染してしまいました。

Emotet は、非常に巧妙なマルウェアです。メールの差出人や内容を偽装して、信頼できる相手から送られたように見せかけます。また、添付ファイルやリンクを開くように誘導します。しかし、それらはすべて罠であり、開くと感染する危険があります。Emotet に感染すると、個人情報の流出やパソコンの故障などの重大な被害に遭う可能性があります。

■ **対処法**

Emotet 感染の疑いがある場合、まずは Emotet 感染の有無をチェックしましょう。チェックするために、JPCERT/CC が無償提供する EmoCheck というツールを利用することができます。「マルウェア Emotet への対応 FAQ」をご確認いただき、EmoCheck を入手してください。

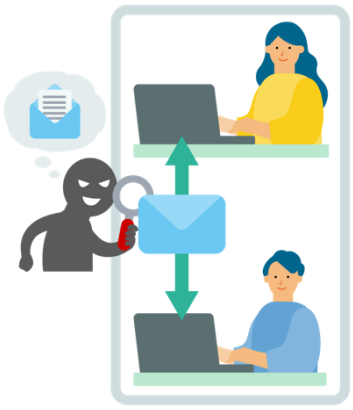
感染が確認された場合、感染拡大を防ぐために、感染した端末を自宅や会社などネットワークから遮断しましょう。さらに、その端末がつながっていたネットワークの他の端末にも感染が広がっている可能性があるため、そのネットワークをインターネットなど他のネットワークから遮断しましょう。

その後は、下記の Web サイトなどを参考に調査や復旧を行ってください。

Emotet(エモテット)感染を疑ったら　警視庁（tokyo.lg.jp）
マルウエア Emotet への対応 FAQ - JPCERT/CC Eyes

メールが他人に読まれている？

■　**事故・被害事例**



「E さん、温泉はどうだった？」

　雑談の中で、なにげなくもらした同僚の F 君のひとことに、E さんは驚きました。週末の旅行は急に決まったため、会社内ではまだ誰にも話していません。この前も誰にも話していないことを F 君が知っているので、不思議に思ったことがありました。あのときは、誰か他の人から聞いたのかな、と思っていたのですが。

　以前もなぜか読んでいないはずの電子メールが既読になっていました。もしかして、F 君に電子メールを盗み読まれているのでは・・・。

　このように、他人に電子メールを読まれてしまうという事件は非常に多く発生しています。ほとんどの場合、電子メールはユーザ ID とパスワードだけで読むことができるため、何らかの方法でパスワードを入手してしまえば、他人の電子メールを読むことはそれほど難しいことではありません。多くの事件は、身近な人間によるものですが、好きな芸能人の電子メールのパスワードを推測して読み出した、という事件も発生しています。

　事件の中には、コンピュータの設定を手伝ってもらう際にパスワードを教えて、その後も変更していなかったり、簡単に推測できるパスワードを使用し続けていたりなどのように、利用者の不注意が原因の場合もあります。

■　**対処法**

パスワード変更

速やかにパスワードを安全なパスワードに変更しましょう。

調査の依頼

職場で働いている方は、システム管理者に調査を依頼し、自身のメールアカウントに不正アクセスされていないか確認しましょう。

■　**予防法**

予測されにくいパスワードを設定する

暗号化して送ったはずが・・・

■　**事故・被害事例**

Xさんは、重要書類をメールに添付して送付しました。重要書類はパスワード付きzipファイルにしたので、後から別のメールでzipファイルの解凍パスワードを送付しました。
しばらく経ってから、そのときに送った重要書類がSNSで拡散されていることに気づきました。確認したところ、添付ファイル付きメールとパスワード送付メールの双方の宛先に、間違ったメールアドレスが入っていました。

パスワード付きzipファイルを送付後に、別メールでパスワードを送付する手法は、誤送信対策として今日でも多く見られるのではないでしょうか。
一見安全に見える送付方法ですが、別送するパスワードメールも添付ファイル付きメールと同じ間違った宛先に送ってしまうケースが多く見受けられるため、本質的に有効とはいえません。

■　**対処法**

SNS等へ不正に公開されてしまった場合には、当該サービス運営者へ削除の依頼を行いましょう。
間違った宛先にファイルを送ってしまった場合には、受信者へ当該ファイルの削除を依頼しましょう。

■　**予防法**

クラウドストレージサービスを利用

メール添付ではなく、クラウドストレージサービスを利用してやりとりすることも検討しましょう。ファイルのリンクを誤送信しても、権限がなければ閲覧できないような機能を持つサービスもあります。

メール以外でのパスワード伝達手段を用いる

メールでパスワードを送付しなければ今回のような事例も防ぐことができます。事前にパスワードルールを決めておくことや、電話等のメール以外でのパスワード伝達手段を用いることを検討しましょう。

第三者のチェックを必須とする

添付メールを社外へ送付する際には、第三者のチェックを受けた上で送付するようにしましょう。

SNS の儲け話に注意

■ **事故・被害事例**

SNS で簡単に儲けられる方法を教えるという情報商材が宣伝されていました。T さんはその情報商材に興味を持ち、購入することにしました。

しかし、その情報商材は詐欺でした。内容は、SNS でフォロワーを増やすためのテクニックや、アフィリエイトの仕組みなど、インターネット上で無料で見つけられるようなものばかりでした。しかも、その情報商材を購入した後には、さらに高額な情報商材を買わないと儲けられないというメールが送られてきました。

T さんは騙されたことに気づき、返金を求めましたが、返答がありませんでした。結局、T さんは数万円の損失を被りました。このような情報商材には注意しなければなりません。SNS で簡単に儲けられるというのは、ほとんどの場合、嘘です。

■ **対処法**

消費生活センターに相談してみましょう。消費生活センターは、消費者の権利を守るために設置された公的機関です。消費生活センターに相談することで、被害の状況や対応策をアドバイスしてもらえます。また、消費生活センターは、販売者に対して交渉を行うこともあります。

警察に被害届を提出することも考えてみましょう。情報商材の販売者が詐欺の場合は、刑事事件として扱われます。警察に被害届を提出することで、販売者の捜査や逮捕を促すことができます。また、警察は、被害者の支援や相談も行っています。

弁護士に依頼することも取り得る対処法の一つです。消費生活センターや警察の対応が不十分だと感じる場合や、返金や損害賠償を求める場合は、弁護士に依頼することもできます。弁護士は、法的な知識や経験を持っていますので、被害者の立場から最善の解決策を提案してくれます。ただし、弁護士に依頼する場合は、弁護士費用や訴訟費用などの経済的な負担も考える必要があります。

以上のように、SNS で簡単に儲けられる方法を教えるという情報商材に騙された場合でも、諦めずに対処することが大切です。消費者として自分の権利を主張しましょう。

■ **予防法**

情報商材の販売者やサイトの信頼性を調べることが大切です。販売者の名前や連絡先、サイトの運営者や所在地、利用規約やプライバシーポリシーなどが明記されているかどうかを確認しましょう。また、口コミや評判、消費生活センターなどの情報も参考にしましょう。

情報商材の内容や効果にも疑問を持つようにしましょう。簡単に儲けられる方法など存在しないことを理解しましょう。情報商材の内容や効果が具体的に説明されていない場合や、過大な宣伝や保証がされている場合も要注意です。

情報商材の購入は慎重に行いましょう。情報商材の購入は契約になりますので、慎重に判断しましょう。特に、返品や返金ができない場合や、高額な料金が発生する場合は注意が必要です。また、個人情報やクレジットカード情報などを入力する前に、セキュリティ対策がされているかどうかを確認しましょう。

暗号化されたカフェの Wi-Fi

■ **事故・被害事例**

F さんはカフェで過ごすことが好きです。カフェの中には、Wi-Fi の SSID とパスワードが書かれた掲示物があります。その Wi-Fi は暗号化されているということで、安心して使っていました。

ある日、カフェでノート PC を Wi-Fi につなぎ、ブログを更新していました。ブログに新規の記事を公開し、しばらくカフェでゆっくりしていました。すると、ブログにコメントが入ったと、メール通知がありました。コメントを見てみると、F さんや家族のことが書き込まれていました。まるで、F さんのノート PC に保存されている最近撮影した写真をのぞかれているようなコメントでした。

F さんは家族と共有するために、写真を共有フォルダに保管しています。もしかしたらカフェの Wi-Fi に接続している他の端末の共有フォルダが表示されるかもしれないと思い、確認してみました。すると、いくつかの共有フォルダが表示されました。どうやら、そのカフェの Wi-Fi では共有フォルダへのアクセスを防ぐ対策がされておらず、F さんのノート PC の共有フォルダに保管されていた写真が、その Wi-Fi に接続していた第三者からのぞかれてしまったようです。

■ **対処法**

接続している Wi-Fi のネットワークプロファイルをパブリックに設定すれば、使っているパソコンにネットワーク上のその他のデバイスからアクセスできなくなります。もしくは、ノート PC の共有フォルダの共有を解除するか、パスワードを設定することで、第三者からのアクセスを遮断します。

次に、ブログのコメントを削除します。コメントに個人情報が含まれている場合は、他への拡散も心配されるため、警察に相談することも検討します。

最後に、念のため、ノート PC のセキュリティソフトを更新し、ウイルスやマルウェアの感染をチェックします。必要に応じて、ノート PC の初期化やデータのバックアップを行います。

■ **予防法**

総務省｜無線 LAN（Wi-Fi）の安全な利用（セキュリティ確保）について（soumu.go.jp）