第4章

スマホやパソコン、IoT機器を安全に利用するための設定を知ろう

スマホ・パソコンを中心に、安全を守るための設定について学びましょう。またIoT機器ならではの注意したいリスクについても解説します。どのように情報を守るか、どのように安全にインターネットを利用するか、具体的な設定方法を学び不安なく利用できるようにしましょう。

1 スマホのセキュリティ設定を知ろう

1.1 スマホにはロックをかけ、席に置いて離れたり、人に貸したりするのは×

第1章7(P.42)でも解説しましたが、重要なことなので繰り返します。スマホには必ず画面ロック(以下「ロック▶用語集P.189」という)をかけてください。

ロックにもPINコード▶用語集P.177によるロック、パターンロック▶用語集P.186、指紋や顔など生体情報を用いた認証によるロックなどがあります。過信は禁物ですが、生体認証▶用語集P.183は周りから覗かれPINコードを盗まれる危険性の排除をしつつ、入力の面倒くささを省くので便利な機能です。

そしてセキュリティ向上のためのロック機能を設定しても、そのスマホをロック解除したまま置いてその場所を離れたり、ロックを解除して他人に見せたり貸したりすれば、せっかく施したセキュリティ対策が台無しになります。他人の手に渡れば、情報を盗まれ、乗っ取られる危険性が上がります。

スマホは大事な情報が詰まった貴重品、肌身離さず自分のそばに置き、使わないときはこまめにロックをかけましょう。

また、スマホだけでなくアプリ▶用語集P.179にもロック機能があれば積極的に設定しましょう。

安全性を高めるには、スマホとは別のPINコード、または別のロック機能を選ぶとよいです。

しかし、ロックを設定しているからといって十分ではありません。

ロック中の待ち受け画面に表示される通知内容にも気を配りましょう。

とくに、待ち受け画面でメールの内容を表示できる設定にしていると、メールアドレスによる多要素認証▶用語集P.184を設定している場合、パスワード▶用語集P.186が記載されたメールの内容が待ち受け画面で確認でき盗み見られてしまう可能性があります。

待ち受け画面に表示する通知はよく検討すべきでしょう。

スマホには必ず画面ロックをかけよう

本来は、上記の例のようにスマホを手放してはいけません。しかし、ロックをかけておけば、最低限のセキュリティは保てます。普段からスマホには必ずロックをかけて、肌身離さず持っておきましょう。

待ち受け画面の通知にはなるべく重要な情報は表示させないようにしよう

上記の例のように「こんな場所だし、大丈夫だろう」と油断してはいけません。待ち受け画面の通知は覗き見のリスクが高いので、重要な情報は表示されないようにしたほうがよいです。

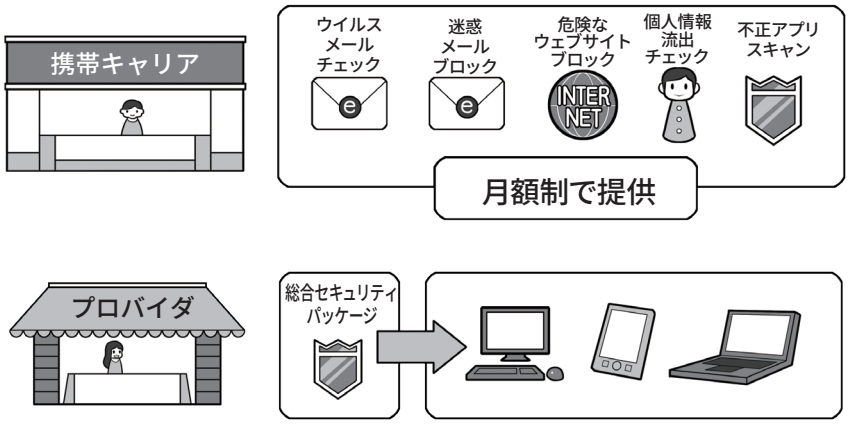
1.2 不安な人は携帯キャリアのセキュリティ対策プランを検討しよう

パソコンがマルウェアの脅威、ワンクリック詐欺やフィッシング詐欺メールなどへ対策する必要があるのと同様に、スマホにもセキュリティ対策は必須です。

まず、アプリ▶用語集P.179はアプリストアなど信頼できるサイトからダウンロードしましょう。その他にも、迷惑メール▶用語集P.189を受信しないようフィルタリングや受信拒否を設定する、不用意にメールやSNS▶用語集P.178などのメッセージ内のリンク▶用語集P.189をクリックしない、といった対策をすれば、ある程度のセキュリティは確保できます。

セキュリティ対策が心配な人は、月額で少額から利用でき、電話窓口や店頭問い合わせができるものも多いので、携帯キャリアやプロバイダ▶用語集P.188が提供しているスマホのセキュリティ対策に対応したプランを利用するのも一案です。

必要性を感じるなら、スマホのセキュリティ対策プランを検討しよう



上記のようなサービスをまとめて複数台に月額制で提供

携帯キャリアからは、セキュリティ関係の機能がパッケージ化されて提供され、インターネットプロバイダも、同様のサービスを提供しています。自分が求める機能があるかを精査して、必要性を感じる場合は導入を検討しましょう。

1.3 情報漏えいを防ぐ

直接スマホを盗まれる以外の情報漏えいには、攻撃者▶用語集P.182による無線LAN▶用語集P.188を使った盗聴があります。

スマホから無線LANのアクセスポイント▶用語集P.179の間の情報通信を盗聴するものです。これを防ぐには通信内容の暗号化▶用語集P.179が重要です。

無線LAN利用時に注意すべき点は以下の通りです。

1. 無線LAN通信が暗号化されていて、かつその暗号化方式▶用語集P.180が安全であるか。
2. きちんと暗号化されていても、その通信で利用する「暗号キー」▶用語集P.180が他人に漏れていたり、共用になっていないか。
3. 無線LAN通信暗号化の確認だけでなく、正しいURL▶用語集P.178であることを確認し、HTTPS通信でエラーなく接続できているかどうか。

などがあります。

無線LAN通信が暗号化されていないまま通信をした場合、通信内容を盗聴され、ID・パスワードを盗用されて使われる、なりすましなどの被害にあう危険性があります。

次に、業務中に万が一スマホを落としてしまった場合に、情報を流出させない方法も考えましょう。

まずはスマホの中身が暗号化されているかチェックします。古い機種では初期状態で暗号化されていないことがあります。本体と記録メディアいずれも暗号化して、落としてしまっても簡単には利用できないようにしましょう。暗号化は本体のロックとセットとなり、必然的にロック機能もオンにする必要があります。

スマホを落としてしまったときの対策のためには、リモートロック▶用語集P.189、位置情報確認やリモートワイプ▶用語集P.189機能を使える状態にしましょう。

iOSではiCloudの「iPhoneを探す」、Androidでは「スマートフォンを探す▶用語集P.183」として、それ

ぞれ該当の機能があり、パソコンや同じアカウントを紐付けた他のスマホやタブレットから操作ができるようになっています。

無料なので必ず試してマスターしておきましょう。

リモートロックとは遠隔操作でスマホをロックして使えなくする機能です。

スマホの所在がわからなくなったら不正利用されないよう、なによりもまずスマホをロックしましょう。

次に「位置情報」を確認しましょう。

事前にこの機能を使ってスマホの位置確認ができるかどうかを試し、確実に使えるように設定しておきましょう。

ただし、こども、職員や会員の監視目的では絶対に使わないようにしましょう。それはプライバシーの侵害になります。

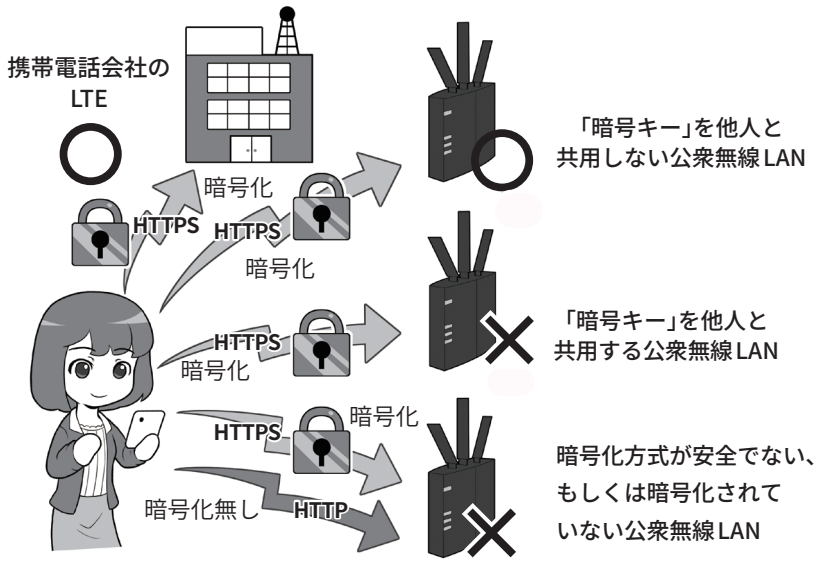
この機能は、建物の中などでは明確な場所が特定できない場合もありますが、現在のスマホのおおよそのありかが地図上に表示されます。

見つかった場所が、自分が訪れた場所や、遺失物として届けられた警察などなら、連絡をして取り戻す段取りをします。

一方、取り戻せそうになく、とくに仕事上の問題がある場合は、最後の手段として情報漏えい防止のために「リモートワイプ」機能でスマホの中身を全部消すことも考えましょう。

ただし、リモートワイプをすると、位置情報を取ることができなくなり

屋外ではむやみに公衆無線LANを使用しない



盗難されたときのために中を見られないように暗号化しよう

紛失・盗難時のために準備をしておこう

リモートワイプすると位置情報が確認できなくなるので、リスクが少ないならばロックだけ行い、遺失物として警察に相談するなどの手段をとりましょう。

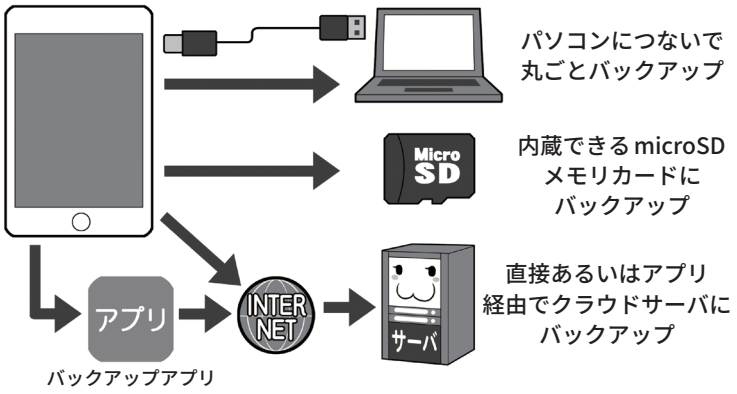
ますので、情報を守るための捨て身の手段になります。

そして、仮にスマホが戻ってこなくても、本体を買い直したらすぐに復旧できるように、スマホの中身は定期的にバックアップ▶用語集P.186しておきましょう。

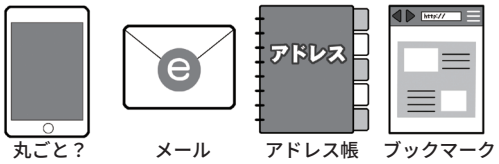
機種によってはパソコンでバックアップすると、新しいスマホをつないでボタン一発指示するだけで復元できるものもあるので、機種選定時に調べておきましょう。

バックアップは定期的に取ろう

バックアップの方法はいろいろ



なにがバックアップできるか確かめる



なにがバックアップできるのか確かめて、機種やバックアップ方法を選択します。

1.4 スムーズな機種変更と、予期せぬデータ流出の防ぎ方

スムーズな機種変更を行うためには、その前に機種変更手順を調べておくことが重要になります。

機種変更にはバックアップが重要ですが、「丸ごとバックアップ」、「データごとにバックアップ」、「アプリを使用してバックアップ」などさまざまな方式があります。

このあたりは自分で調べるとともに、実際に機種変更やデータの移行▶用語集P.185をしたことがある人に聞いたり、記事を見たりして、どの方法が便利かアドバイスを求めるなど、検討するとよいでしょう。

最近ではデータがスマホ自体の中（ローカル）にあるだけでなく、インターネットのどこか、利用者から見て姿が見えない雲のような存在のクラウドサーバ▶用語集P.181に保存されている場合もあり、機種によっては移行のためのバックアップ作業という概念そのものがないこともあります。

一方で、本体のデータ移行手段とは別に、機種変更に際して、特定の機能の移行処理をしておかなければならないものもあります。

ここ2、3年で普及したスマホの決済サービス（Apple Pay、Google Pay、おサイフケータイなど）の中には、登録しているクレジットカードや交通系ICカードなどの情報を、一旦サーバ側にバックアップしてから、かわりにパスワードを受け取り、スマホから機能を削除して、その後新しい機種でログイン用語集P.189し、そのパスワードを使い機能を復元▶用語集P.187する処理が必要になるものもあります。

一部のSNSでは、旧機種と新機種からの同時アクセスができてしまうようにならないように、移行処理の前に、一度旧機種からアクセス権を削除する手続きをしたのち、新しい機種でアクセスするための利用開始の手続きをする方式のものもあり、手間がかかります。

いずれの場合も機種変更の移行処理にあたって、移さなければならない機能やアプリを書き出し、それぞれの移行手順がどうなっているか調

べ、各サービスを提供する企業の公式ページなど確認してください。

次は機種変更をした後の情報漏えいを防ぐ処理です。

機種変更した前のスマホには、個人情報である住所録、撮りためた写真、今までやりとりしたメールなど、あなたや会社の情報が全部詰まったままになっています。

いずれの場合も機種変更の移行処理にあたって、移さなければならない機能やアプリを書き出し、それぞれの移行手順がどうなっているか調べ、各サービスを提供する企業の公式ページなど確認してください。

売却、譲渡や廃棄する場合、必ずデータを消去しなければなりません。

さもないと、知られたくないメールや写真が流出したり、住所録にある取引先に詐欺メールが送られてくるかもしれません。

また、修理に出す場合でも、モラルの低い修理会社が情報を流出させた例があるので、必ずデータをすべてバックアップをした上で、本体のデータは消去してから修理に出したほうが安全でしょう。

最初にデータをバックアップした上で、各種サービスはアプリもウェブ▶用語集 P.180 版もすべてログアウト▶用語集 P.189 します。

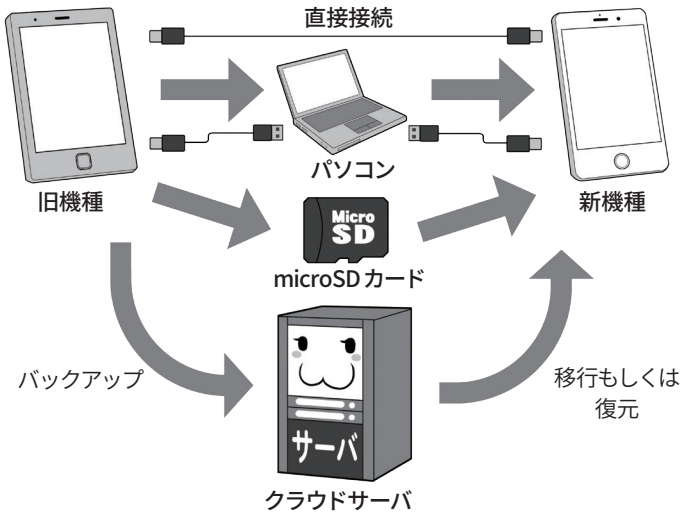
続いてそれぞれのスマホにある「初期化」▶用語集 P.182 や「データ消去機能」▶用語集 P.185 を使って内部のデータを消去します。なおスマホでマイナンバーカード機能が使えるようにしている場合は、端末の初期化だけでは機能は削除されません。手順を確認の上、スマホ用電子証明書の失効手続などを実施する必要があります。

一部のスマホでは、紛失時に探せるように設定した「位置情報を確認するためのサービス」を事前にログアウトしておかないと修理などに出せないものもあるので、消去の前にログアウトを確認してください。

落としてしまって液晶が割れ操作ができない場合、消去作業をすることもできないと思いがちですが、パソコンに接続することで消去することが可能ですので、あきらめず必ず行いましょう。

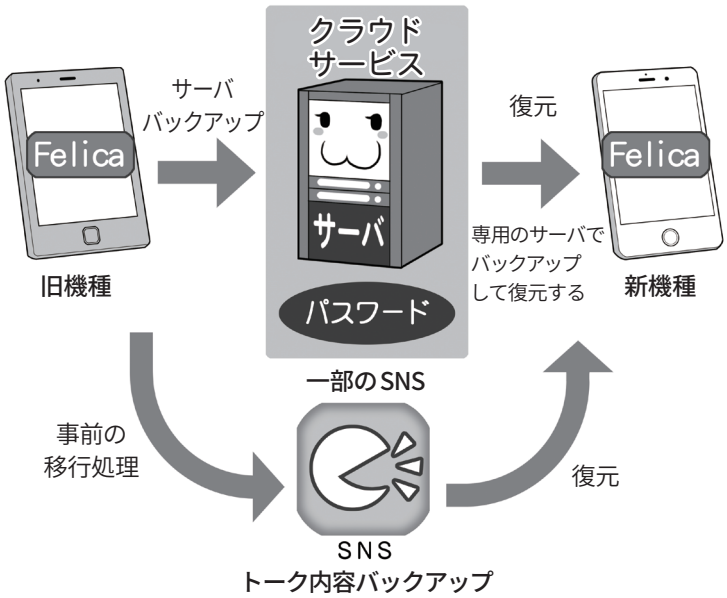
業務用に使用しているスマホなどで、万が一にでもデータが復元される可能性を排除したい場合は、各携帯電話会社や家電量販店などで、スマホを物理的に破壊してくれるサー

データの移行は事前に手段を調べる



移行処理は事前に目的の機種でどういった移行手段が使えるのか調べておきます。

スマホの決済サービスやSNSデータなどの移行



ビスを利用して、データを読み出せないようにしてしまいましょう。

なお情報機器については、OSなどのサポート切れのものは原則として使わないようにするべきですが、特にスマホの場合には個人情報▶用語集 P.182などが集積しているので、よほどの理由がない場合以外は、サポート切れのものを使うのは避けましょう。

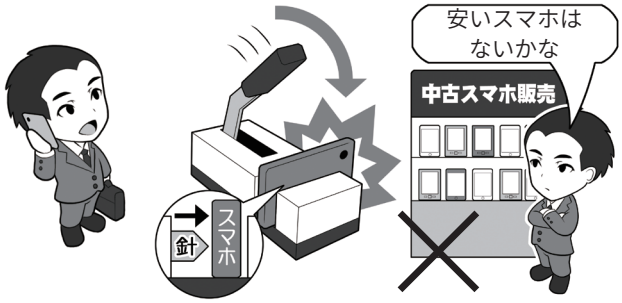
転売、譲渡、廃棄のときは必ずデータを消去する

消去する前には、利用しているサービスはすべてログアウトして、サーバなどに情報を預けなければならないもの（おサイフケータイなど）は預けましょう。

SNSで移行前手続が必要なものは行い、その後移行処理をして、移行後きちんと復元できたら、旧機種を売却・譲渡や廃棄する場合は、必ずデータを消去しましょう。

液晶が割れて操作できなくても、パソコンに繋げば消去することは可能です。一部機種ではマウスを接続して操作することも可能です。

業務用のスマホは物理的に破壊する。心配ならば新品を購入し、スパイウェア混入の可能性を排除する



仕事に使うスマホを廃棄する場合は、物理的に破壊する機械がある場所に持ち込んで破壊しましょう。大手携帯電話会社での回収も信頼できます。

一方、中古で購入したスマホに攻撃者がスパイウェアを仕込んでいて、企業の情報が流出しても、販売した会社にその責任を取る能力はないでしょう。ましてやオークションでの購入などではなおさらです。前所有者の残債で購入後使用不能になるケースもあります。業務用に使用するならIT機器は新品を利用しましょう。

2 パソコンのセキュリティ設定を知ろう

2.1 パソコンを買ったら初期設定などを確実に

パソコンを購入したら、まず復旧のときに行うリカバリ▶用語集P.189の方法を確認し、必要があればリカバリメディア▶用語集P.189を作成しておきましょう。

リカバリメディアがDVDなどで付属している場合は必要ありませんが、最近の機種ではコストダウンの影響で添付されないものや、そもそもDVDドライブなどを搭載していないものも多いので、マニュアルなどにしたがってDVD-RディスクやUSB▶用語集P.178メモリで作成します。

なお、Windowsではリカバリメディアなどを使ったときに「プロダクトキー▶用語集P.188」の入力が必要になる場合があります。

プロダクトキーは本体の裏側や付属しているリカバリメディアにシールが貼り付けられているので、紛失に備えスマホなどで写真に撮っておくか、メモに書き写して保管しておきます。

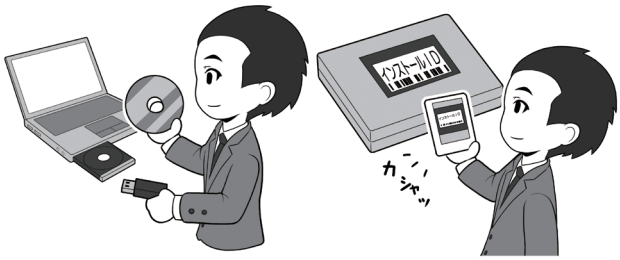
次に、セキュリティ設定をします。

初期設定時にIDと「ログインパスワード*1▶用語集P.189」の設定を必ず行いましょう。

また、マニュアルにしたがって起動用「BIOSパスワード▶用語集P.176」や「ファームウェアパスワード▶用語集P.187」という、電源を入れた段階で入力が求められるパスワードも設定しましょう。

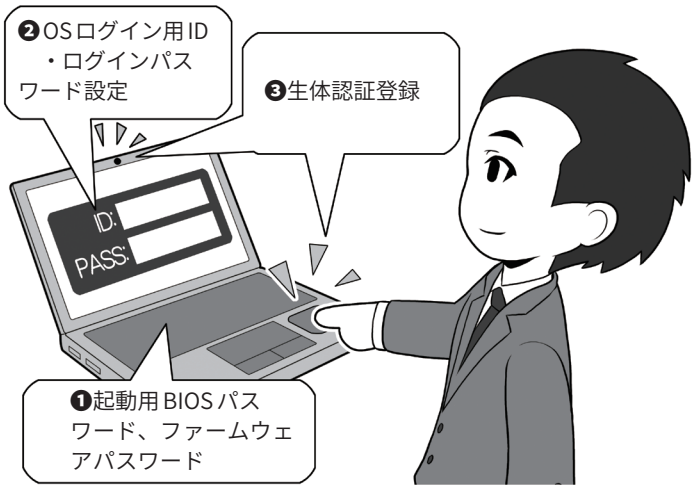
これを設定しておくと、盗難されてもOS▶用語集P.177の起動ができなくなり、盗難時の情報流出をより強固に防ぐことができます。

パソコンを買ったらまずリカバリメディアを作る



DVD-Rディスクや USBメモリでリカバリメディアを作り、本体裏などにあるプロダクトキーを撮影し保存します。メディアが添付されていれば作る必要はありません。

起動用のパスワードや生体認証登録をしよう



「ログインパスワード」はセオリーどおり複雑なものを設定し、その上で生体認証を使いログインの手間を省くようにします。盗難や不正利用防止のためBIOSパスワードなども設定しましょう。BIOSパスワードなどは「ログインパスワード」相当に設定します。

これらのパスワードは、「ログインパスワード」のセオリー通り複雑で安全性の高いものを設定してください。

生体認証を使用すると、パスワードの桁数が多くても毎回入力する必要がなくなるので、ログイン操作が楽になるメリットがあります。

*1 パスワードにはいろいろな種類があるので、詳しくは第5章1(P.99)を参照

2.2 暗号化機能などでセキュリティレベルを高める

パソコンを盗まれたときに、情報が流出しないように、攻撃者からの攻撃が難しくなるようにセキュリティレベルを上げましょう。

会社のパソコンは泥棒などが盗んで帰れないように、ワイヤーロックという盗難防止用のワイヤーで、机などに固定して、持ち運べないようにしましょう。

こういった状態だと、盗みに入った泥棒はパソコンの中の情報だけでも入手すべく、パソコンを壊して中の記憶装置▶用語集 P.181 であるハードディスクやSSD▶用語集 P.178 だけを盗む可能性もあります。

そのように盗まれても情報が漏れないようにするため、記憶装置は暗号化処理▶用語集 P.180 を行っておきましょう。

なお、暗号化機能付き外付け記憶装置の場合、使用開始時に入力するのは暗号化の鍵になる「暗号キー」になっているので、「暗号キー*2」は「ログインパスワード」より複雑にし、数字＋英大文字＋英小文字で推認できない程度の桁数 に設定します。

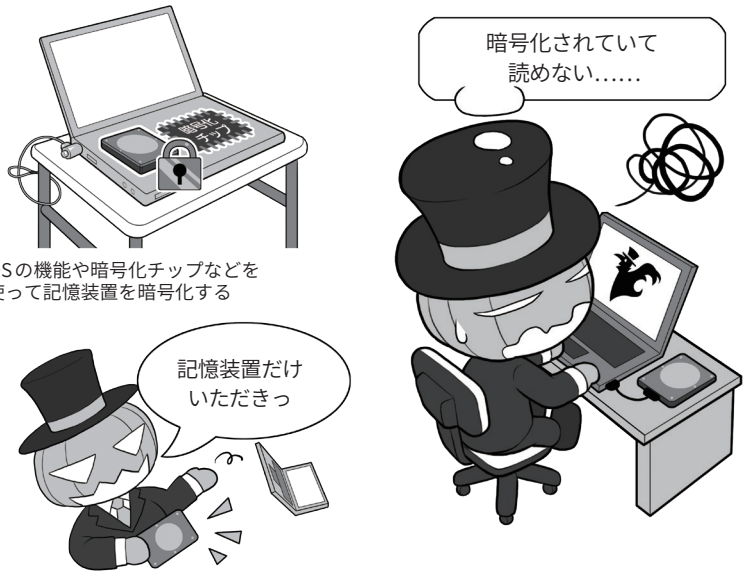
きちんとした複雑さと長さの「暗号キー」で暗号化された記憶装置は、仮に盗んで別のパソコンに繋いでも、解読が非常に困難であり、情報流出を防ぐ力になります。

また、スマホにあるリモート（遠隔）ロックやリモートワイプは、業務用かつLTE▶用語集 P.177 などの通信回線を内蔵している一部のパソコンでも可能です。

とくにこういった用途を前提に開発をされている機種は、相手から電源が入っているように見えない状態で記憶装置の中身を消すこともでき、重要情報を持ち出す必要がある場合は有効な防御手段となります。

スマホほどの精度ではありませんが、こういったパソコンではGPS▶用語集 P.176 無しでも盗まれた機器の現在地を探索することもできるので、置き忘れのままや届け出られている場合は取りに行き、盗まれている場合は情報を添えて警察に相談しましょう。

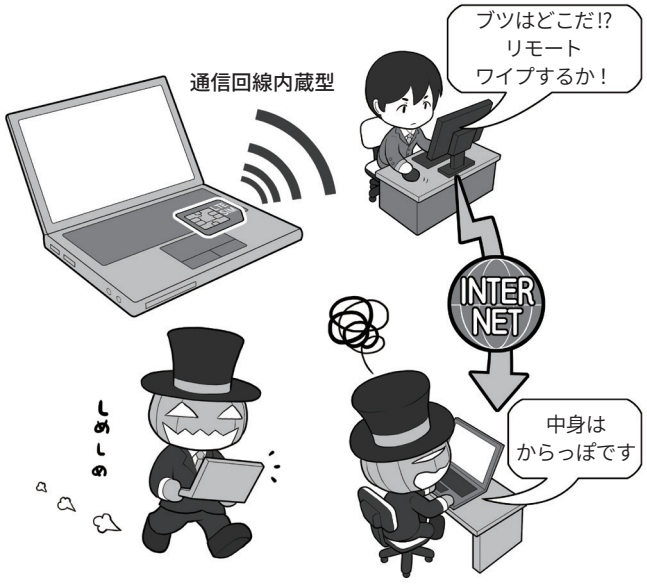
盗難にそなえて記憶装置の暗号化



OSの機能や暗号化チップなどを使って記憶装置を暗号化する

TPMチップ（≒暗号化チップ）で暗号化されている記憶装置は、「暗号キー」が元の本体の TPM チップ内に残されているので、盗み出しての暗号化解除がさらに困難になります。

パソコンでもリモートワイプはある



業務用の一部機種では、起動をさとられないステルス状態で、リモートワイプ（遠隔操作でパソコンの中身を消去）などが可能です。盗んだ相手が気づく前に処置することができます。もちろん、そもそも盗まれないようにするのが第一ですが。

*2 暗号キーに関しても、詳しくは第５章１(P.99)のパスワードに関する項目を参照

2.3 マルウェア感染に備え、3-2-1のバックアップ体制を整える

マルウェア▶用語集P.188の感染に負けない環境を整えるには、システムやソフトウェアを最新の状態に保つこと、セキュリティソフト▶用語集P.183を導入し同様に最新の状態に保つことが重要です。

しかし、それでも感染してしまったとき、素早く復旧させるためには、定期的なデータのバックアップが重要です。

バックアップは「3-2-1ルール」といって、本体含め3個以上の複製、2種類以上の記録メディアで、1個は遠い場所に保管することを推奨します。

具体的には、パソコン＋バックアップ用記憶装置＋クラウドサーバといった形です。

メインのバックアップ用記憶装置は外付けで、最低でも内蔵記憶装置の3〜4倍の容量にして、何世代分かのバックアップを可能にすることが理想です。

昨今顕著になってきたランサムウェア▶用語集P.189に備えるために「定期的にバックアップをしつつ、普段は本体に接続しておかない」という、やや煩雑な対応が必要です。

こうすることでバックアップ用記憶装置もろとも暗号化されてしまうことを防げます。

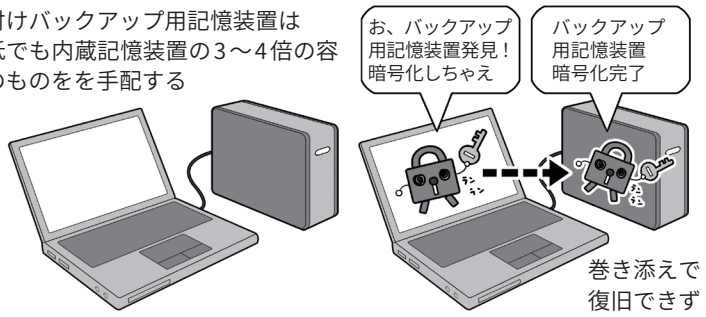
また、とくに重要なデータは、信頼できるクラウドサーバ上にセキュリティを固めた上でバックアップして、地震、火災、水害などの災害に遭っても重要なデータが巻き添えにならないようにしておきましょう。

ランサムウェアをはじめ、こういったマルウェアの感染はネット経由だけだと思われがちですが、それだけとは限りません。

例えば、仕事相手の会社の人から「資料をコピーしてくれ」と渡されたUSBメモリにマルウェアが仕込まれていたり、パーティでプレゼントされたデジタルカメラに仕込まれていたりというケースも実際に存在します。注意しましょう。

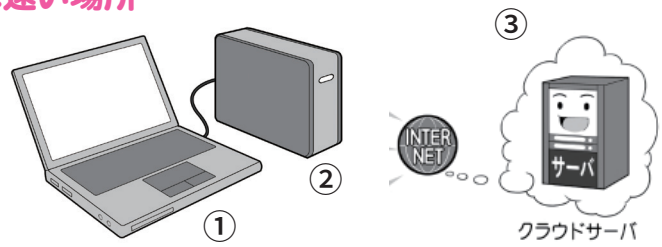
バックアップの体制を整え、普段は接続しない

外付けバックアップ用記憶装置は最低でも内蔵記憶装置の3〜4倍の容量のものをを手配する



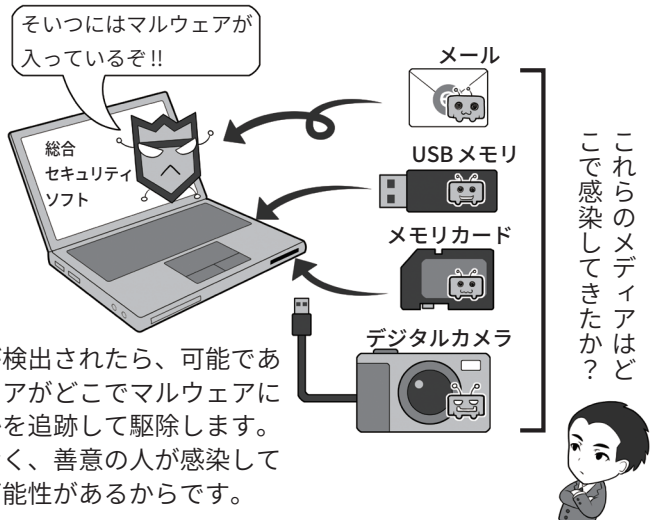
環境を整えたらシステムのバックアップを開始します。ソフトウェアの導入や環境の変更があればバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェアに感染して巻き添えで暗号化され、復旧に使うためのデータも失われてしまうので注意が必要です。

バックアップは3個以上、2種類以上の記録メディア、1個は遠い場所



このルールは、①本体＋②バックアップ用記憶装置＋③クラウドサーバで条件を満たせます。クラウドサーバは多要素認証、USBセキュリティキーなどを使って攻撃者に乗っ取られないようにしましょう。暗号化が可能なら暗号化して、共有設定をしっかり確認しましょう。

さまざまなマルウェア感染源に注意する



マルウェアが検出されたら、可能であればそのメディアがどこでマルウェアに感染してきたかを追跡して駆除します。攻撃者だけでなく、善意の人が感染してしまっている可能性があるからです。

2.4 売却や廃棄するときはデータを消去する

パソコンの廃棄にあたっては、機密情報などの情報漏えいを防ぐために、内蔵記憶装置のデータを復元できない形で消去しなければなりません。

とくに個人情報などを扱う場合は、個人情報保護の観点から、廃棄時は確実に情報を消去する努力義務が求められています。

内蔵記憶装置が正常に読み書きできる状態で、パソコン本体にディスク消去機能があるなら、それを使い消去しましょう。

無い場合は、消去用のソフトウェアを利用します。記憶装置単体で保管していた場合などは本体に接続して消去するか、専用の機器などで消去します。

データの最低限の消去は、記憶装置全域に無意味な情報を書き込むことで、記録されていた情報の残留の可能性を消す方法が考えられます。

かつて米国国防総省や軍などでは、3〜4回以上の繰り返し上書きによる消去を推奨していましたが、2014年に米国の政府機関NIST（National Institute of Standards and Technology 米国国立標準技術研究所）が発表した「NIST Special Publication 800-88 Revision 1 Guidelines for Media Sanitization」によると、上書き回数は1回でも十分で、専門機関であっても上書きされたハードディスクの復旧は困難、という見解が示されています。

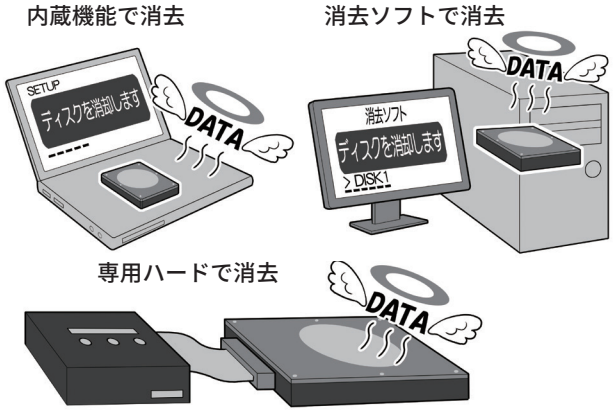
ハードディスクの場合、これに従わないと、消えたように見えたデータを復旧できる可能性が残るのです。

なお、SSDはデータの管理方式がハードディスクとは異なるので、生産メーカーの「Secure Erase」用ソフト▶用語集 P.184を探してこれらを利用するなどの方法があります。

故障して正常に読み出せない、あるいは機密性を求められるものの場合は、物理的もしくは磁気的に破壊する方法もあります。また家電量販店などに有料の破壊サービスがあります。

企業などで多量に廃棄する場合、安全が確保された環境でハードディスクを読み出し不可能に破壊するか、ハードディスクやSSDでも粉砕できるシュレッダーの導入も検討しましょう。

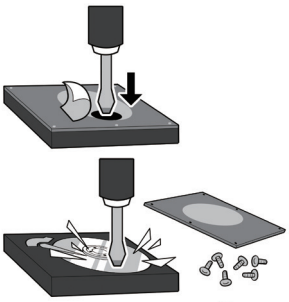
記憶装置の中のデータは必ず消去する



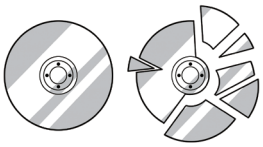
ハードディスクは、いずれの場合も最低1回以上の繰り返し消去（データ上書き）処理をするモードを選択します。SSDはメーカー製の消去用ソフトなどを使います。

動作不能、機密性確保には破壊する

①ハードディスクは破壊用の穴を使うか、分解してディスクを取り出し壊す

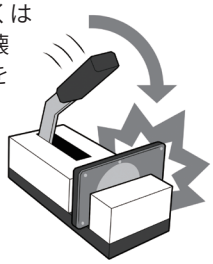


中のディスクを割るか、穴を開ける



②目の前で破壊してくれる店に持ち込む（有料）

物理的もしくは磁気的に破壊できる機器を購入する（企業など向け）



ガラス製のディスクならば割れればOKです。金属製ならばドリルを利用して穴を開け読み出し不能にします。壊れて動かなくても、記録ディスクだけを他に移植して読み出すという手段があるので確実に破壊しましょう。SSDは中のメモリチップを物理的に破壊するのが理想です。

コラム.1 ダブルラインでトラブルに備える

インターネットを閲覧していると、突然サーバが無反応になることがあります。そのときどうやって原因を解明するのがよいのでしょう？

使用しているパソコンやスマホが原因なのか、無線 LAN か、それともウェブサーバ▶用語集 P.180 自身がダウンしているのか。

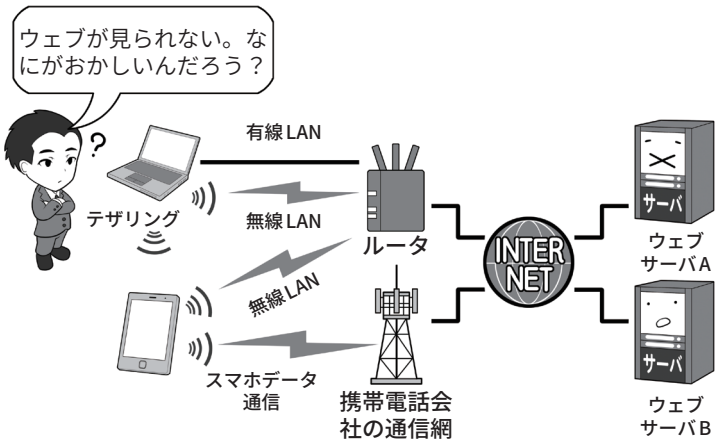
ネットを仕事に使っているなら、通信ができなくなるのは死活問題。速やかにトラブルを特定し、別経路でのアクセスを確保するテクニックを身につけましょう。

それには主要な機器の二重化（ダブルライン化）が有効です。パソコンで見られないならスマホで確認。無線 LAN がダメならば有線で。ルータ▶用語集 P.189 がおかしいなら携帯電話回線 LTE で。A というサーバがダメならば B へアクセスして、トラブルが発生した部位の機器を避けるなどの処置をしましょう。

また、所有する特定の機器がマルウェアに感染したり、セキュリティホール▶用語集 P.184 が明らかになったアプリなどを避けてサービスを利用したりする場合も、同様の考え方になります。

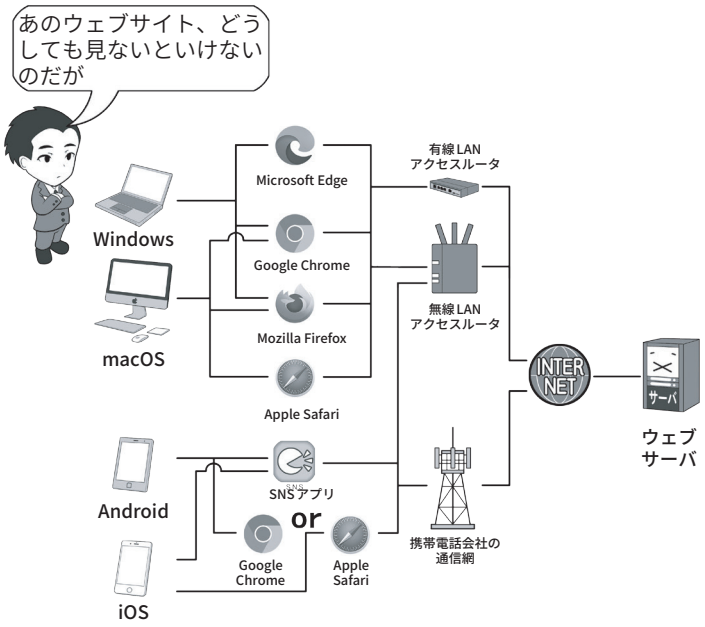
特定の機種へのサイバー攻撃▶用語集 P.182 が流行っているなら別機種で、ウェブブラウザ▶用語集 P.180 にセキュリティホールがあるなら別のウェブブラウザで、問題があるものを積極的に避けて利用するわけです。複数台の機材を持つ場合は、機材のタイプを分散することも備えとしては有効でしょう。

通信状態がおかしいときに問題点を絞り込む手段



自分から見ると、インターネットのウェブサーバを見る機器、ルータまでの通信方法、インターネットまでの通信方法、そして目的のサーバまで切り替えることで、どの部分にトラブルがあるかを絞り込めます。なお、すべてを切り替えてもネットが表示されない場合は、しばらく時間をおいて確かめましょう。いずれかの場所で通信が集中し混雑して通信ができなくなっている可能性があります。

パソコンがマルウェアに感染したり、ブラウザがセキュリティホールで使えないときの回避手段



Windows にトラブルが発生したら macOS で、特定のウェブブラウザにトラブルが発生したら別のウェブブラウザで、スマホのアプリにトラブルが発生したらウェブブラウザ版サービスを利用するなどの回避手段を設けるのも、1 つの防衛策です。

ここでは簡略化して描いているため、上のイラストを含めインターネットの部分で二重化が収束してしまっているように見えますが、そもそもインターネットは通信経路上にあるサーバが攻撃で破壊されても、迂回して通信が確保されるようになっているので、通信が断絶するトラブルがあった場合、自然と迂回路が形成され通信が確保されるはずなのです。

3 IoT機器のセキュリティ設定を知ろう

3.1 常にインターネットに接続するIoT機器は注意が必要

IoT（Internet of Things）▶用語集 P.177 機器とは、従来ネット接続しなかった電気機器が、インターネットに接続可能になったものを指します。

例えば、従来の監視カメラはネットに接続する機能を持っていませんでしたが、IoTの監視カメラは撮影した映像をネット経由でスマホなどに送信して危険を通知するなどの機能を備えており、より便利に使うことができます。

注意したいのはインターネットにつながるということは、インターネット上にいる、世界中の攻撃者から攻撃対象になりうるということです。

例えばIoTの監視カメラであれば、攻撃者がセキュリティホールを突いて乗っ取り盗撮カメラとしても使うことができるわけです。

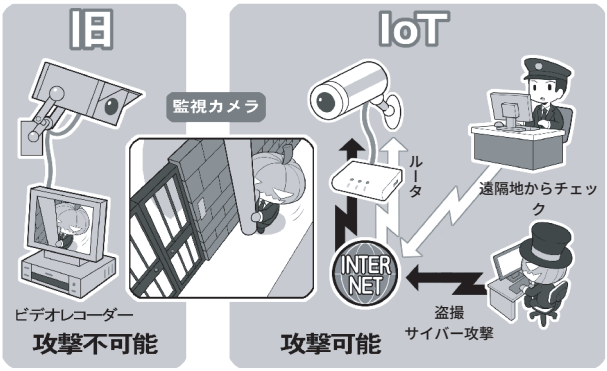
諸外国においては、クラッカー▶用語集 P.181 がIoT機器を乗っ取りボットネット▶用語集 P.188 として悪用し、大規模なサイバー攻撃（DDoS攻撃▶用語集 P.176）を仕掛けたことで、インターネットサービスが停止し、社会経済に深刻な被害が生じた例があります。

被害を避けるためには、IoT機器のファームウェア▶用語集 P.186 を最新にしてセキュリティの不備をなくす必要があります。

総務省はIoT機器のセキュリティ向上を目指し、「NOTICE」というサポートセンターを設置し、ウェブや電話による対応窓口を通じて、IoT機器利用者へ適切なセキュリティ対策を案内しています。

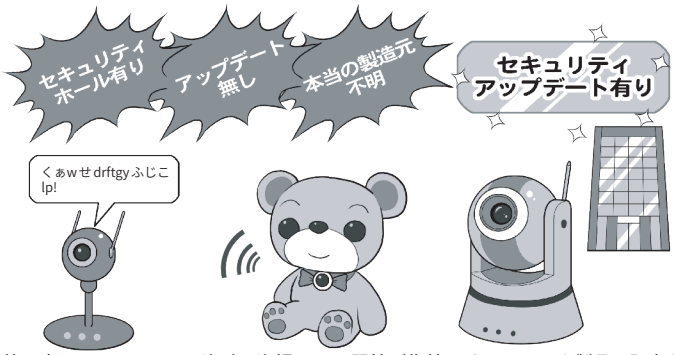
IoT機器の挙動がおかしいと感じたときは電源を入れ直す、ファームウェアアップデートを怠らずなるべく自動更新の設定にしておく、とスマホやパソコンと同様の対策を講じることが重要です。

IoT機器に進化するとセキュリティ上のリスクも生む



従来の監視カメラはSDカードや有線接続などで内部記憶するタイプが主流で限られた場所でしか確認できませんでしたが、IoT機器化することで、遠隔地からチェックできたり、問題が発生すればスマホで通知や映像を受け取ることもできるようになりました。しかし、代わりにサイバー攻撃を受ける可能性も生まれたのです。

セキュリティ上、注意が必要な製品も少なくない



悪意ある第三者によって不正な操作が可能なホームカメラ

盗聴・盗撮のぜい弱性が指摘された、カメラ付きぬいぐるみ

ネットワーク製品の販売実績が豊富なセキュリティリテラシーの高い企業の製品

IoT機器の中には、セキュリティホールがあっても対処されない、アップデートが提供されるウェブサイトも不明など注意が必要な製品も流通しています。ネットワークに接続する製品は、セキュリティのリテラシーが高い企業製で、なるべく自動更新機能付きのものを購入しましょう。

NOTICE IoT機器のセキュリティ対策周知啓発

https://notice.go.jp/

●NOTICEサポートセンター
0120-769-318（無料・固定電話のみ）
03-4346-3318（有料）
受付時間 10:00～18:00（年末年始12/29～1/3を除く）

●お問い合せフォーム
https://notice.go.jp/inquiry

3.2 購入後は初期パスワード変更などの設定を

ウェブブラウザで機器の設定画面にアクセスするための、管理者用パスワード▶用語集 P.181は出荷時の状態から必ず変更しましょう。

機種によってはそのモデルすべてで同じパスワードが設定されていたりするものもあり、格好の攻撃対象となります。

また、ネットワークの設定も適切に行う必要があります。

IoT機器を意図せずインターネットに公開する可能性のある機能は基本的にオフにして、必要な機能を精査して使うようにすべきです。

これは社内などのネットワークと外部のインターネットの境目にあるルータでも同様に設定します。

IoT機器は記憶容量が少なく、パソコンなどのように総合セキュリティソフトをインストール▶用語集 P.180できません。

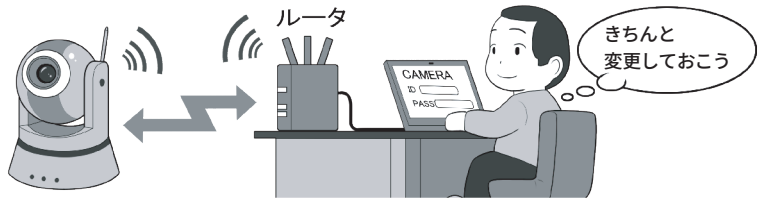
そのためにルータ自体がIoT機器に対応した、包括的なセキュリティ機能を持つ「IoT対応セキュリティ機能内蔵ルータ」にしましょう。

その中にはパスワードの変更不要な安全な設計のルータもあります。

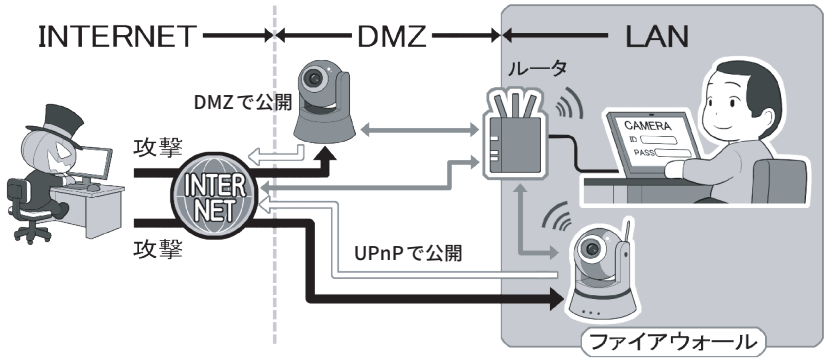
外部からの攻撃だけでなく、IoT機器が勝手に外部に情報を送信しないように、監視できる体制を整えましょう。ただ、IoT機器に関する一番のセキュリティ対策は、ネットワークに接続する明確な理由のないときは、そもそも接続しないことです。

ワイヤレスイヤホンなどにより普及しているBluetooth機器についても同様です。常に最新版にアップデートし、使用しないときはオフにしましょう。

初期の管理者パスワードは変更する

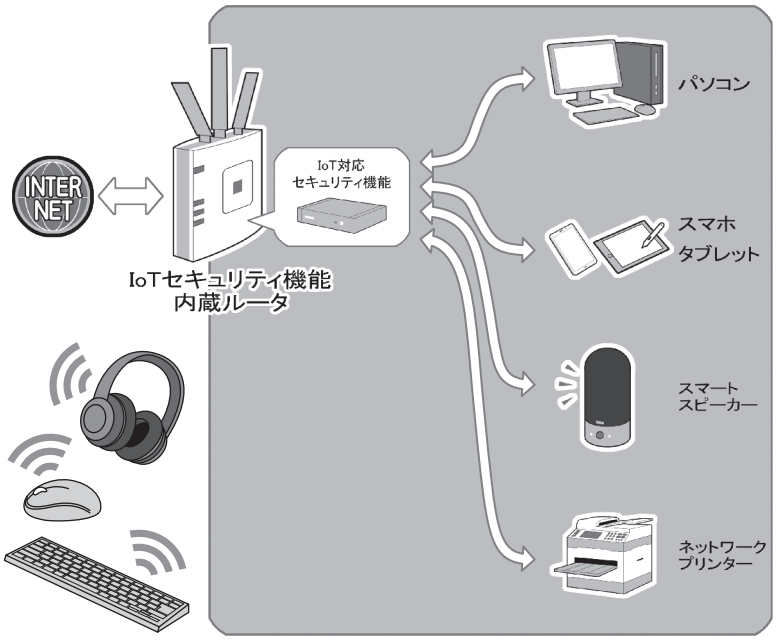


IoT機器を導入したら不正アクセス防止のため、まず初期の管理者用パスワード（初期パスワード）は変更しましょう。大抵の場合、ウェブブラウザ経由でIoT機器にアクセスして変更するようになっています。



そのほかにも、インターネットに対してLAN内部の機器を公開してしまう可能性のある、UPnP機能はオフにして、インターネット側（DMZ）にIoT機器を設置することもやめましょう。いずれも攻撃者からIoT機器へのアクセスが容易になるからです。

小さい会社などならIoT対応セキュリティ機能内蔵ルータも



IoT機器、Bluetooth機器はパソコンやスマホと異なって、記憶容量が小さいためセキュリティソフトなどを導入することがほぼできません。したがってサイバー攻撃に弱く、また、モニターなどがないため機器の状態をチェックしづらく、乗っ取られてもこれを察知することが難しいのです。そういった状態を察知するために、最近ではIoT機器に対する監視機能を持った装置を、インターネットの玄関口になるルータに接続したり、あるいはルータ自身の中にそういった機能を内包するものがあるので、これらの導入を検討しましょう。こういった装置はIoT機器などLAN内の機器を監視し、不自然な点があれば連携したスマホのアプリなどで確認できます。

4 それでも攻撃を受けてしまったときの兆候と対処を知ろう

対策を講じサイバー攻撃の大部分を防げても、残念ながら攻撃を受けてしまう可能性をゼロにはできません。攻撃を受けてしまったときの兆候と対処行動を説明しましょう。

まず、システムを最新の状態にしたのち総合セキュリティソフトを入れたとしても安心してはいけません。

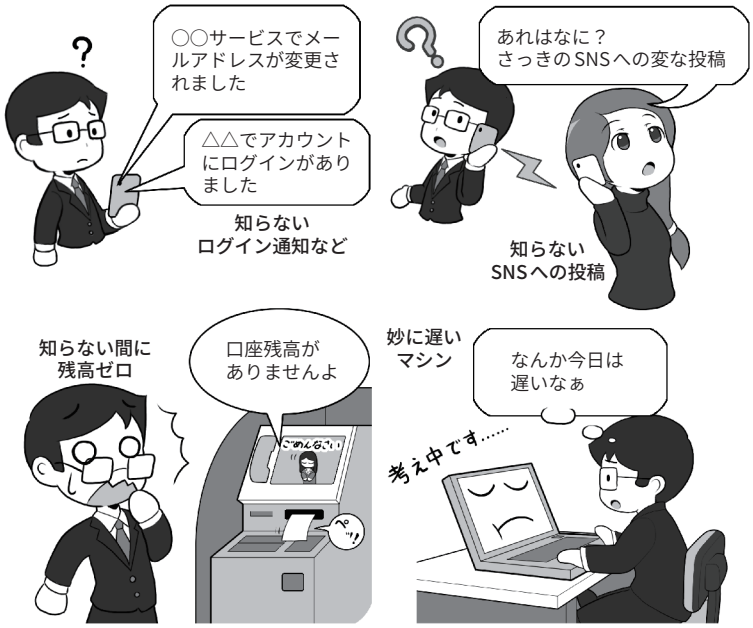
セキュリティホールの発見に対してアップデートなどの提供が間に合わない状態で、攻撃をしかけられたら、防ぐことが難しいからです。(ゼロデイ攻撃▶用語集 P.184)

備えるだけでなく、攻撃を受けたときの兆候を敏感に察知する能力を身につける意味はここにあります。

攻撃の兆候として、例えば知らないログイン通知やログイン履歴、SNSでの自分が知らない投稿やアプリ連携▶用語集 P.179などが挙げられます。また知らない銀行口座の引出しや、クレジットカードの請求などがあります。そしてパソコンやスマホなどの情報機器が乗っ取られている場合などは、動作が普段より遅かったり重かったりすることがあります。

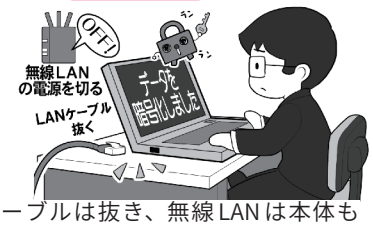
もしこれらの兆候から、実害が判明したら、とりあえずは有線でも無線でもネットにつながる回線から切断した上で、本体の電源はそのままにして、証拠保全を図りましょう。

セキュリティソフトが検知しなくても、兆候に敏感になれ



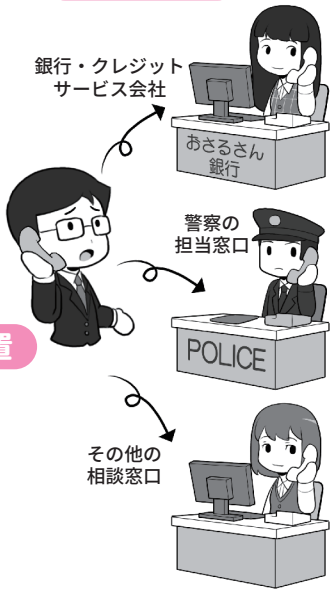
実被害が出ているときは証拠を保全して通報

証拠保全



LANケーブルは抜き、無線LANは本体もアクセスポイントもオフにします。被害拡大防止になります。なお証拠保全のため、パソコンの電源は切ってはいけません。

各所に連絡



原因究明までの緊急避難措置

感染したマシンでメールでの連絡や仕事のやりとりは×。感染経路やマルウェアの種類などが判明するまで、同一LAN内、同種の機器の利用も避け、別の種類の機器、別の種類の回線を使います。会社や家のパソコンなどが感染したら、スマホなどの通信回線を使用するなどの暫定的な回避策を行いましょう。

通信を切断するのはマルウェアの拡散▶用語集P.180防止と外部の攻撃者との通信を絶つためで、本体の電源を切らない理由はパソコンなどのメモリ上の証拠を消してしまわないためです。

その後、必要に応じて各種金銭取引関係のサービスを一旦止めてもらう連絡をし、相談窓口などに連絡して対処方法を相談しましょう。また、警察の担当部署に通報・相談しましょう。

侵入経路の解明やマルウェアの駆除が終わるまでは、感染が疑われる機器は使わないようにしましょう。

マルウェアが発見されただけで実害が出ていない場合、セキュリティソフトなどで駆除できるときは駆除します。

駆除できないときは機器を初期化してバックアップから復元や再設定し、再びネットに接続して使用し始める前に、感染や乗っ取りの原因と思われるものをクリアにしましょう。またシステムやセキュリティソフトは再度最新の状態か確認しましょう。

その他、疑わしき原因となるものは削除しましょう。例えば不審なメールの削除、セキュリティホールになりかねないサポート期間切れの機器やソフト、アプリはアンインストール▶用語集P.179、知らない又は不要なアプリやサービス連携▶用語集P.182も解除しましょう。

なお、ウェブサービスのアカウントが乗っ取られてパスワードが変更されてしまった場合は、自分で再設定することはできないので、サービス側に連絡してアカウントを取り戻す処理をしてもらいましょう。とこ

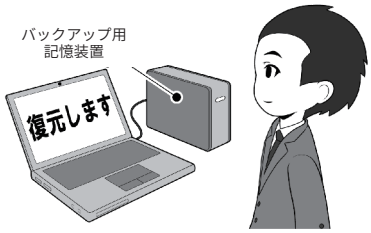
実被害が出ていない場合

マルウェアの駆除

セキュリティソフトなどを最新にしてフルスキャンをかけて駆除します。

バックアップから復元

セキュリティソフトで対処できない場合は、本体を初期化してバックアップから復元します。



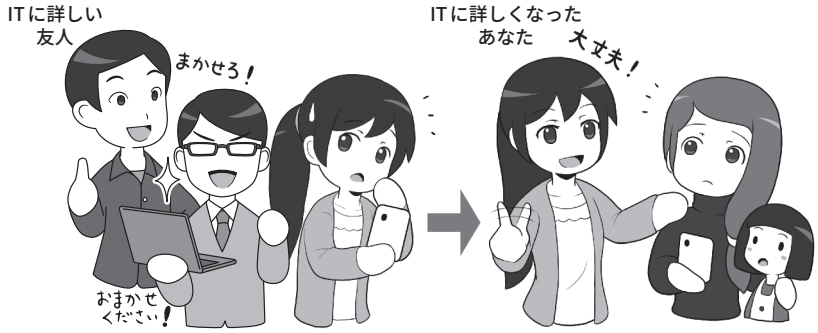
システムをチェックする

古いソフト、サポート終了しているソフトおよびアプリは削除します。

サービスやアプリ連携の見直し

SNSのサービス連携機能は見直します。

信頼できる相談窓口やITに詳しい友人を頼ろう



困ったときには、信頼できる相談窓口やITに詳しい知人に意見をもらうとともに、自らも勉強しましょう。

そして将来同様のケースがおきたら、あなたが困っている人に「ITに詳しい友だち」として手を差しのべて、力になってあげてください。

ろで、攻撃が明白でない状況で疑心暗鬼になりそうなとき、知り合いの専門家などがいると心強いです。また適宜、各種の相談窓口へ相談するのも一案です（付録02（P.165-P.166）参照）。そのうえで、必要な関係機関への届け出を行いましょう。

そのときあなたが誰かに助けられたら、次は誰かを助ける番になってください。

1人また1人と、こういったセキュリティに詳しい人が増え、みんなでサイバー攻撃に立ち向かう姿勢が広まることは、きっとネットの安全を守る力になります。