第４章

# スマホ・パソコンのより進んだ使い方やトラブルの対処の仕方を知ろう

ここではパソコン・スマホの扱い方を中心に、安全を守る方法について勉強しましょう。
どのように情報を守るか、どのように安全にネットを利用するか、セキュリティを守るための技術を
障害物競走のように楽しめれば、みなさんのスキルアップになるでしょう。

# 1 スマホのセキュリティ設定

## 1 スマホにはロックをかけよう。席において離れたり、人に貸したりするのは×

スマホの情報を守る第一歩は、待ち受け時にロックすることです。

ロックにはPINコードによるロック、パターンロック、生体認証によるロック、また、最近では特定の機器（普段身につけているスマートウォッチなど）や、GPSに連動して特定の場所（自宅など）で自動的にロックを解除できる機能もあります。

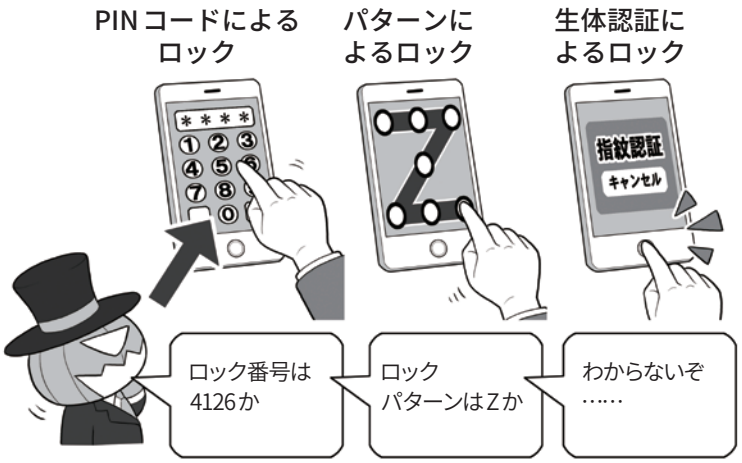
ただ、自分が明示的に指示をしないロック解除は、うっかり端末を無防備にすることもあるので、基本的にはなんらかの動作をして解除する方式にしましょう。周りから覗かれPINコードを盗まれる危険性の排除や、入力の面倒くささを省く点からは、生体認証を利用するのが便利です。

一方、生体認証にも弱点があります。お面や写真から復元した偽の指で指紋認証を破る研究や、「寝ているときに自分の指を勝手に使われ認証突破される」こともあります。生体認証だから安全と過信しないようにしましょう。

そして、各種のロック機能を設定しても、スマホのロックを解除を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、あるいは貸してしまったりすれば、一瞬で情報を盗んだり、乗っ取ったりすることが可能です。

スマホは、持ち歩く情報の金庫だと思って、必ず自分のそばに置き、こまめにロックをかけた状態　にしましょう。

### スマホにはロックをかけよう




### 席において離れたり、人に貸したりしないようにしよう


スマホを席に置いたままでは、本体も情報も盗まれる恐れがあります（特に、ロック解除したままの状態で放置）。

スマホを貸すと、プライバシーを覗かれたり、一瞬で盗み見アプリをインストールされたりすることがあります。注意しましょう。

# 2 情報漏れを防ぐ①

SNS用のアプリなどには、本体のロックとは別にアプリ用のPINコードなど設定できるものもあります。盗難などの際、SNSの内容を見られたくなければ、このアプリPINコードも設定しましょう。守りが二重になります。一部の機種では、指紋認証をアプリのロック解除に利用できるものもあるので、セキュリティを向上させても快適な利用の妨げにはなりません。

一方、攻撃する側から見ると、スマホのロックをなんらかの方法でパスできたとしても、また、別の関門が待ち構えているわけで、手間をかけさせ侵入を諦めさせるセオリーに沿っているわけです。

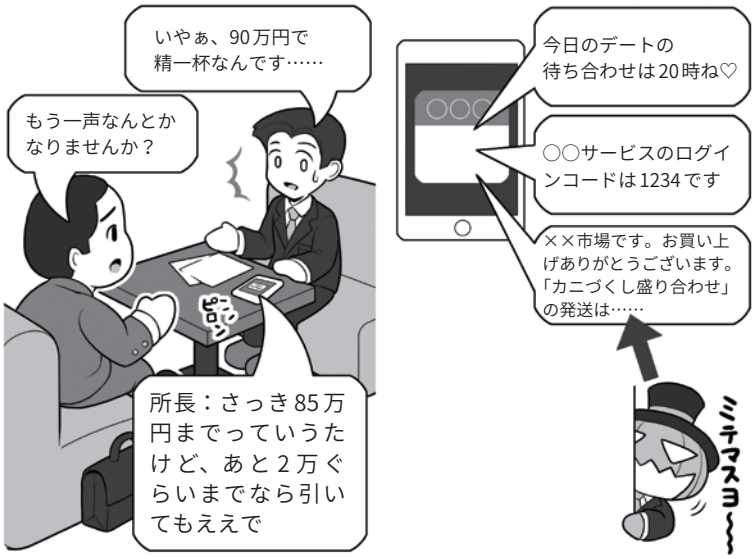
なお、アプリのPINコードを設定する場合は、スマホロック解除のPINコードと異なるものにしましょう。PINコードの使い回しはセキュリティがないのと一緒になってしまいます。PINコードも異なってこそ意味があるのです。

スマホをロックしていても、情報漏れが発生することもあります。

例えば、自分だけで使っているときは便利なメールの通知機能。でもロック画面にメールの内容を表示していると、誰かと会話中や商談中に、うっかり内部の情報を見られてしまったり、あるいは差出人が分かるだけで、状況によっては知られると問題のある情報を提供してしまうことになります。

また、同様にロック画面にメールの内容を表示していると、せっかくセキュリティ向上のために設定した多要素認証の確認メールも見られてしまうことがあり得ます。そうするとIDとパスワード＋ロックのかかったスマホだけでも、「正常に」ウェブサービスのセキュリティをパスできてしまうわけです。

## 待ち受け画面に表示する通知はよく検討する




ロック画面だけでなく、普段使用している画面に通知ウインドウとして表示される場合でも、同じく情報を見られてしまう原因になります。スマホを使って説明しているときに、不適切なメールの内容が表示されることも……。情報の扱いには気をつけましょう。

## アプリごとにPINコードをかけられる場合はかける


本体のロックを解除されても、SNSのアプリに別のPINコードがあれば、流出の危険性は低くなります。それでも、スマホを席に残してはいけません。なお、勝手に人のスマホのロック解除をすることはサイバー攻撃です。

# 3 情報漏れを防ぐ②

直接スマホを盗まれる以外の情報漏れのケースには、攻撃者による無線LAN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が重要です。

暗号化のセクションの繰り返しになりますが、無線LAN利用時のチェックポイントとしては、

1. **無線LAN通信が暗号化されていて、かつその暗号化方式が安全であるか。**
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」が他人に漏れていたり、共用になっていないかどうか。**

などがあります。

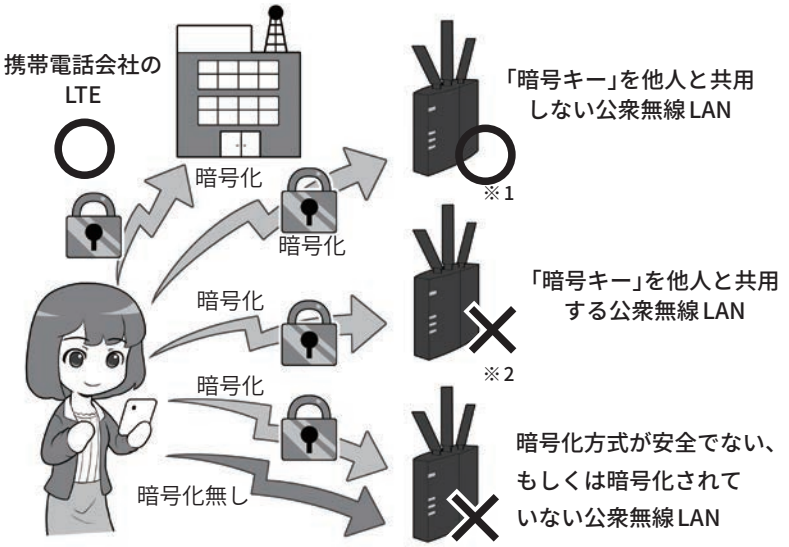
企業によって提供されている公衆無線LANであれば、上記の無線LANの安全性をきちんと理解して提供する能力があるかどうかをチェックしましょう。トラブルを発生させて「謝るだけ」の企業より、情報漏れの芽を摘み「万全の安全性のもとにきちんとサービスを提供する」企業の方が、はるかに優秀で信頼に足るのです。

その点をよく調べた上で、利用する公衆無線LANの企業を選択するのも、重要な情報漏れの防御策です。

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

まずは、スマホのデータが暗号化されているかチェックです。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ONにする必要があります。

## 屋外ではむやみに公衆無線LANを使用しない




そもそも、自分と「契約関係がない」ものは非常時以外は基本的に使わず、また、その中でも運営主体がわからない無線LANアクセスポイントは絶対に使用しないようにしましょう。

※1 携帯電話会社やプロバイダが提供していても、「暗号キー」が共用でないとは限りません。きちんとチェックしましょう。

※2 暗号キーが貼り出してあるような公衆無線LANは、「暗号キー」が他人と共有になり危険です。使わないようにしましょう。

無線LAN暗号化などに関するより詳しい説明は、P64からを参照して下さい。

## 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


本体もメディアも暗号化。最近では、暗号化が標準のものがほとんどですが、必ず確認しましょう。

スマホを落としたときの次の対策としては、リモートロック、位置情報確認やリモートワイプ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」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ほかの端末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、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、子どもの端末などの監視目的では、絶対に使わないようにしましょう。この理由は後ほどご説明します。

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、自分が訪れたお店や、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、そうではない場合は、最後の手段として情報漏れ防止のために「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。

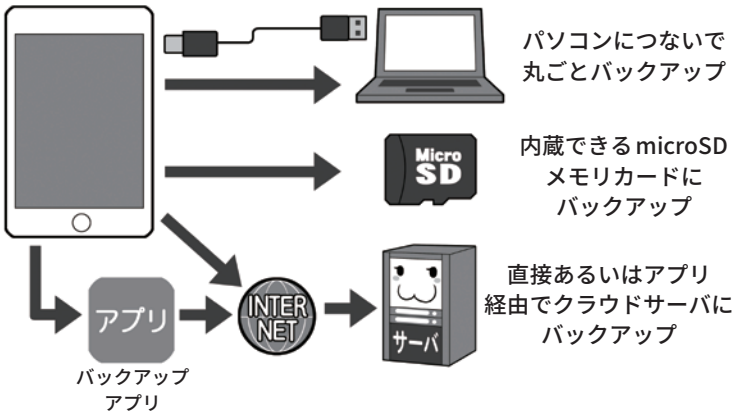
機種によっては、パソコンでバックアップすると、新しいスマホをつないでボタン一発指示するだけで復元できるものもあるので、機種選定時に調べておきましょう。

## 紛失や盗難時のために準備をしておこう

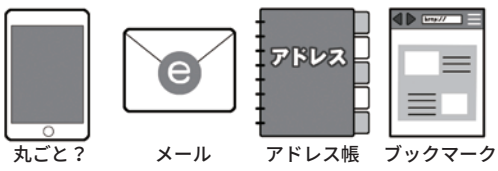

※リモートワイプすると、位置情報が確認できなくなるので、リスクが少ないならばロックだけ行い、遺失物として警察に相談するなどの手段をとりましょう。

## 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。

## 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段を調べておくことが重要になります。

バックアップの項目でも書きましたが、「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」など様々な方式があります。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をしたことがある人に聞いたり、記事を見たりしつつ、どの方法が便利だったり簡単だったか、アドバイスを求めるといいでしょう。

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サーバ（クラウド）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。

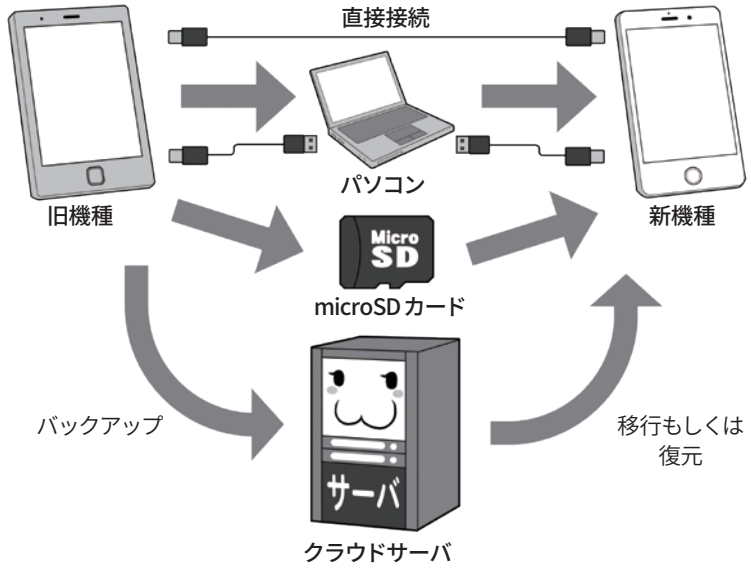
また、本体のデータ移行処理とは別に、機種変更に際して、特定の機能の移行処理をしておかなければならないものもあります。

例えば、いわゆる「おサイフケータイ」に関する機能では、一旦情報をサーバ側に預け、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して貰ったパスワードを使い機能を復元する処理が必要になるものもあります。

一部のSNSでは、旧機種がアクセス可能なまま新機種がアクセス可能になって、複数台から同時アクセスできないように、移行処理の前に一度手続きを踏んで、旧機種からSNSにアクセス権を削除してから、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ものもあります。

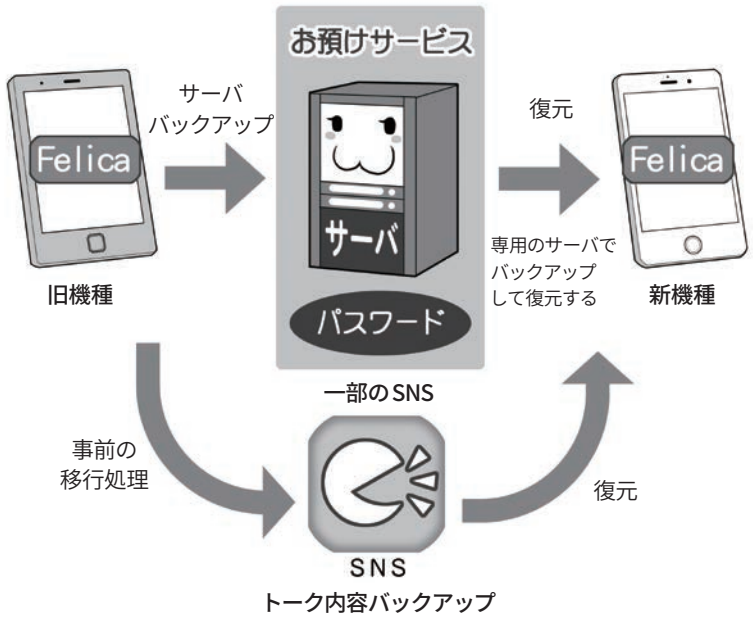
いずれの場合も、機種変更の移行処理にあたって、移さなければならない機能を紙などに書き出し、それが網羅されているかどうかをチェックしてください。さもないと、電子マネーが旧機種とともに消えてしまって取り戻すのが困難になることもあります。

### 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。

### おサイフケータイや、SNSデータなどの移行



次は、機種変更をした後の情報流出を防ぐ処理です。

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、あなたの情報が全部詰まったままになっています。売却、譲渡や廃棄する場合、データを必ず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、住所録にある友人宛にフィッシング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、芸能人のスマホから写真を抜き出して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。

手順としては、各種サービスはアプリもウェブもすべてログアウト。続いて、それぞれのスマホにある「初期化」や「データ消去機能」を使って内部のデータを消去します。

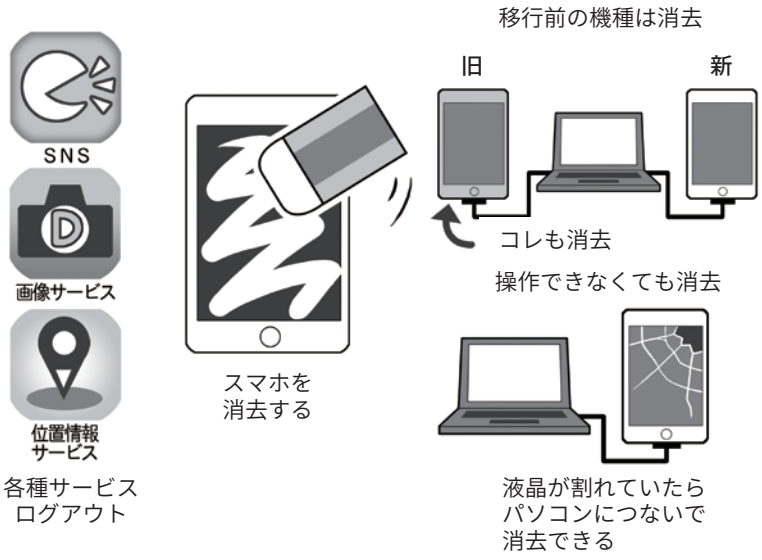
一部のスマホでは、紛失時に探せるように設定した「位置情報を確認するためのサービス」を事前にログアウトしておかないと修理などに出せないものもあるので、消去の前に確認してください。

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。

余談ですが、業務用などで情報漏えいのリスクを少しでも排除したいなら、中古品を使ったりしないようにしましょう。中古販売店が良心的でも、プロの組織が仕込むようなマルウェアやバックドアには対処できない可能性があります。それを排除するには信頼できる国で生産された、正規ルートの新品を購入して使いましょう。

## 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 で移行処理が必要なものは行っておきます。その後、移行処理をして、移行後きちんと復元できたら、前の機種を売却・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、パソコンにつなげば消去することはできます。

## 業務用のスマホは物理的に破壊する。心配ならば新品で情報流出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、販売したもの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

## 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、まず復旧のときに必要になるリカバリメディアを作成しましょう。

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外付けDVDドライブやUSBメモリで作成します。

また、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」が必要になる場合があります。本体の裏側などにシールで貼られているか、付属しているリカバリメディアに貼り付けられているので、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。

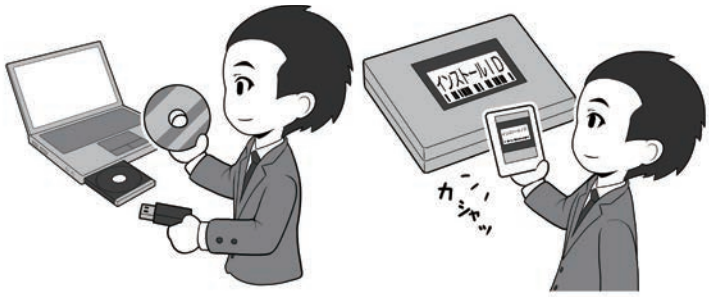
次に、セキュリティの設定をします。初期設定時にIDと「ログインパスワード」の設定を必ず行いましょう。また、マニュアルにしたがって起動用「BIOSパスワード」や「ファームウェアパスワード」といった、電源を入れた段階で入力することを求められるパスワードを設定しましょう。

これを設定しておくと、盗難されてもそもそも電源を入れることができなくなり、盗難時の情報流出をより防ぐことができます。

生体認証を使用する場合は、パスワードのセオリーにしたがって「ログインパスワード」を設定した上で、生体認証の登録を行い、セキュリティを高めつつログインの手間を省きましょう。

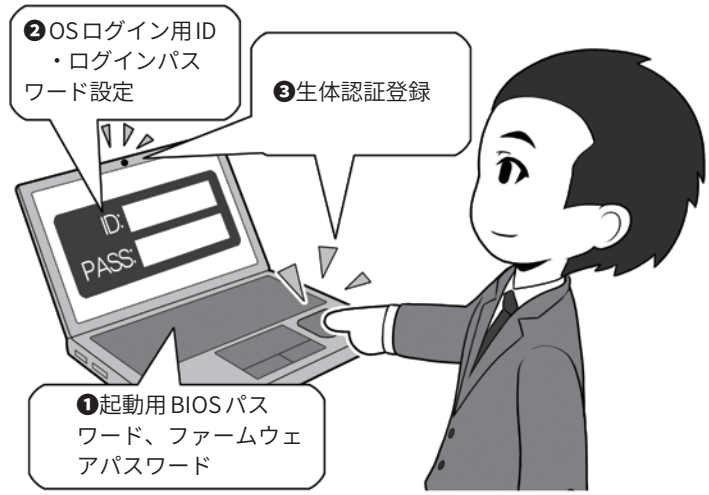
生体認証機能が無い場合はパスワードをしっかり設定しましょう。

### パソコンを買ったらまずリカバリメディアを作る




DVD-R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、セオリー通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きます。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。

# 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、攻撃者に嫌がらせ、ではなく、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、くくりつけて移動できないようにしてあります。

こういった場合、攻撃者は情報だけでも入手すべく、パソコンの内部記憶装置(ハードディスクやSSD)だけを盗む場合もあります。

そうやって盗んでも情報が漏れないようにするため、内蔵記憶装置には暗号化処理を行いましょう。

この場合の「暗号キー」は「ログインパスワード」と共用になっているものもあるので、その場合はより複雑な「暗号キー」のセオリーに従い、15桁以上に設定します。

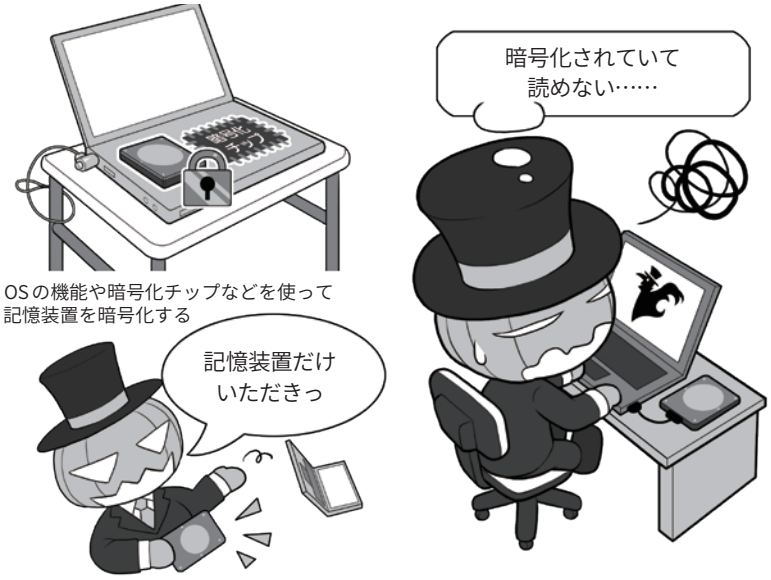
きちんとした複雑さと長さの「暗号キー」で暗号化された記憶装置は、盗んで別のパソコンにつないで暗号化を解除しようとしても、解読が非常に困難であり、情報流出を防ぐ力になります。

また、スマホにあるロック機能やリモートワイプも、業務用でかつLTEなどの通信回線を内蔵している一部パソコンでは可能です。

特に、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初期化することもでき、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。

なお、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無しでも盗まれた機器の現在地を探索することができるので、置き忘れのままや届け出られて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。

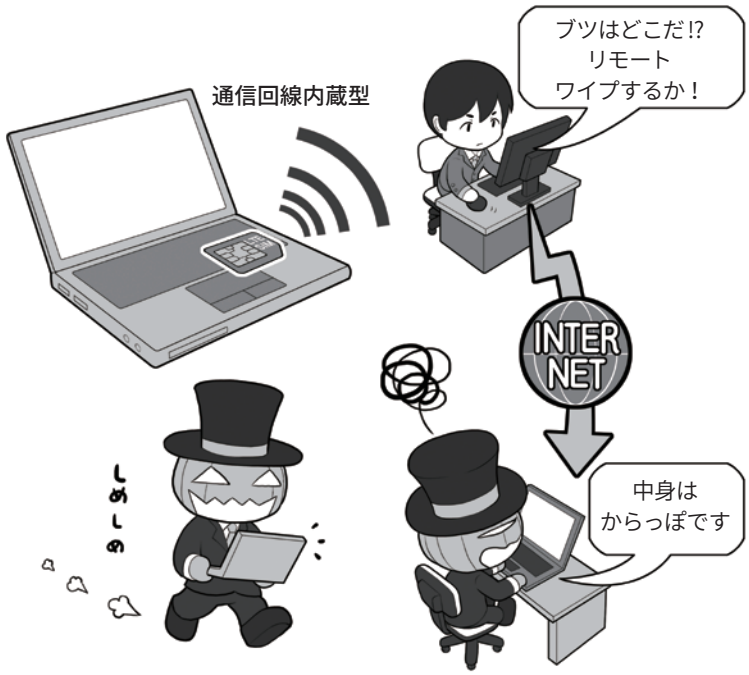
## 盗難にそなえての記憶装置の暗号化




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

暗号化のための専用のTPM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、記録装置を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




業務用の一部パソコンでは、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。

# 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

マルウェアに感染しにくいようにするには、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、少なくとも3個以上の複製、2種類以上の記録メディア、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＋バックアップ用外部記憶装置＋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、何世代分かのバックアップを可能にいましょう。また、昨今顕著な、パソコンの中のファイルを勝手に暗号化し、解除するには身代金を要求する「ランサムウェア」に対抗するために「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ることを防げます。

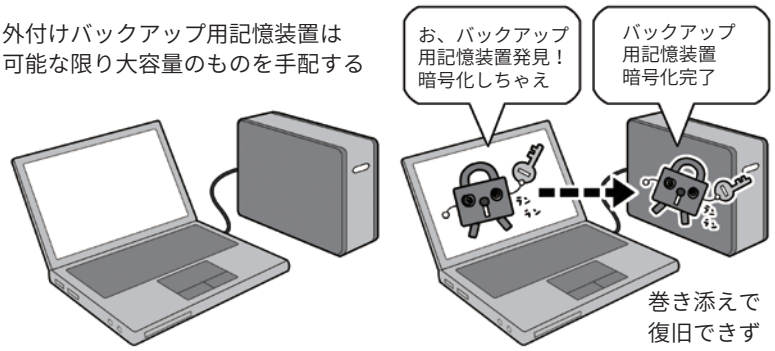
また、特に重要なデータは、信頼できるクラウドサーバ上にセキュリティを固めた上でバックアップして、地震だけでなく仮に自宅が風水害などに遭っても、復旧できるようにしておきましょう。

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。

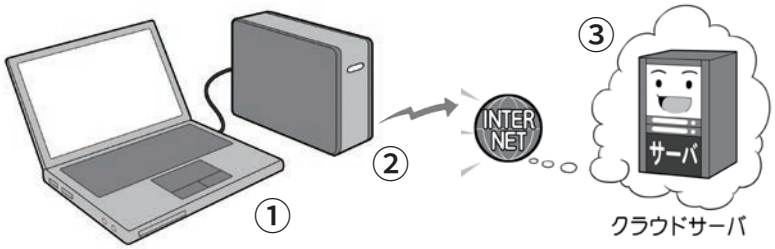
## バックアップの体制を整える

外付けバックアップ用記憶装置は
可能な限り大容量のものを手配する



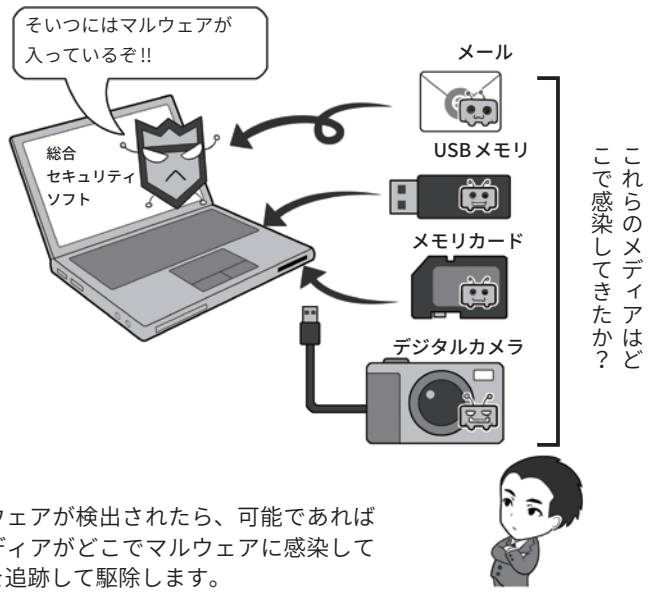

環境を整えたらバックアップを開始します。ソフトの導入や、環境を変更したらバックアップします。システムのアップデート後もバックアップします。ただし、バックアップ用記憶装置を常に接続しておくとランサムウェア感染で巻き添えになって、復旧に使うためのデータも失われてしまいます。

## バックアップは3媒体、2種類、1個は遠い場所




本体＋バックアップ用外部記憶装置＋クラウドサーバで条件を満たします。クラウドサーバは多要素認証で、攻撃者に乗っ取られないようにしましょう。

## 様々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。

# 4 売却や廃棄するときはデータを消去する

スマホの廃棄と同様に、パソコンの廃棄でも、個人情報、メールや写真などの情報流出を防ぐため、記憶装置に含まれるデータを絶対に読み出せない形で確実に消去しなければなりません。

ハードディスク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。無い場合は消去用のソフトウェアを利用。裸のディスクで保管していた場合などは本体に接続して消去するか、消去用の専用機器などを利用しましょう。

データの最低限の消去は、ディスク全域に無意味な情報を複数回書き込むことで、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。例えば、かつて米国国防総省や軍などでは、この方式で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。

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、この方法では消えず、注意が必要です。生産メーカーの専用ソフトや破壊装置を使う必要があります。

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、本体から取り出し物理的に、もしくは磁気的破壊する必要があります。

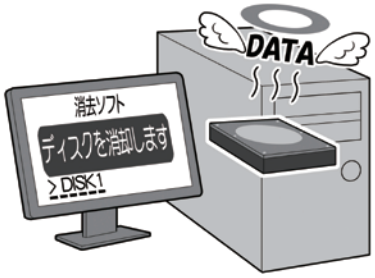
有料ではありますが、家電量販店などに破壊サービスがあります。これらは自分が見えるところで破壊してくれるので確認しましょう。

企業などで多量に廃棄する場合は、きちんと安全が確保された環境で、ディスクを読み出し不可能な状態に破壊するか、破壊用の専用機器やハードディスクや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。機密性を確保し情報漏洩を防止する投資です。

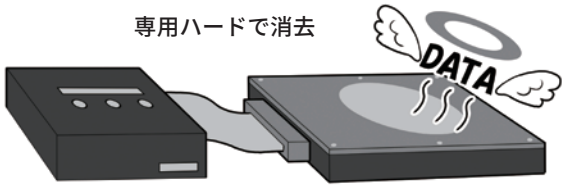
## 記憶装置の中のデータは必ず消去する

内蔵機能で消去


消去ソフトで消去



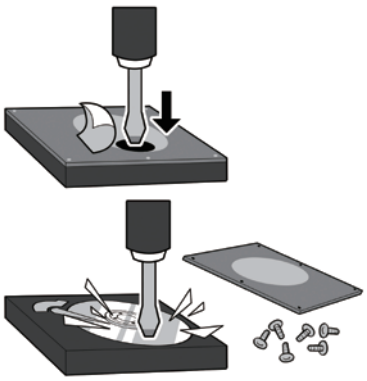

専用ハードで消去



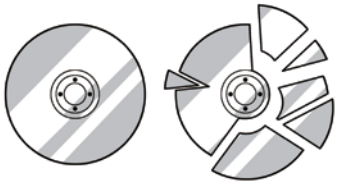

最低3回以上の繰り返し消去(データ上書き)処理をするモードを選択します。

## 動作不能、あるいは機密性確保には破壊する

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

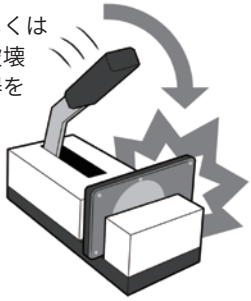


中のディスクを割るか、穴を開ける



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ほか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。

## 5 盗難や紛失のとき、スマホとパソコン、どっちが安全？

盗難や紛失という視点から見たときに、スマホとノートパソコンとデスクトップパソコン、どれがより安全なのでしょう。

置かれている環境にもよりますが、「盗まれた後」までを、その要素に入れて考えてみます。

図のとおり、人目に付きやすいスマホは、当たり前ですが盗みやすい。その代わり盗難時の不正なロック解除は困難。また、基本的に通信機能があり、落とした後の位置情報の確認や盗まれたときのリモートロックやリモートワイプ機能といったセキュリティ機能が標準で備わってます。

ノートパソコンは、ログインパスワードの試行に制限が無い場合もあり。一方、PIN コードや指紋認証型もあり。盗難された場合に場所を特定し取り戻すには LTE などの「通信機能内蔵」が現実的な最低条件となり、現状ではほとんどの機種で利用できないので、盗難や紛失した後の探知が困難です。

デスクトップパソコンは、基本的に屋内にあるので、空き巣に入られるのでもなければ盗まれたり人目についたりすることが少なく、また、大きいので目立たないように持ち運びは困難。したがって盗まれる機会が少ないので、盗難後の探知機能は必要ないといえばありません。代わりに、設置場所の戸締まりや監視カメラの設置で安全性を高められるので、その分は補えるでしょう。

結果として、「実質的に盗難紛失時のリカバリ手段のないノートパソコン」が、盗難紛失に最もリスキーといえるかもしれません。

そうなった場合のために、せめてデータを読み出すことができない起動用パスワードや記憶装置暗号化の手段を講じておきましょう。

### 要素から安全性のポイントを検証する

| | 盗まれにくい | 人の目につきにくい | ロック解除が困難 | LTE などの内蔵通信機能 | GPS を使った位置情報 | リモートロック リモートワイプ |
|---|---|---|---|---|---|---|
| スマホ（タブレット）  | × | × | ○<br>生体認証<br>PIN コード<br>多数失敗でロック | ○ | ○ | ○ |
| ノートパソコン  | △ | △ | △<br>失敗しても<br>ロック無しも<br>○<br>生体認証<br>PIN コード | △※1 | △※2 | △※3 |
| デスクトップパソコン  | ○ | ○ | △<br>失敗しても<br>ロック無しも | × | × | × |

※1　LTE などの無線 WAN 通信機能を内蔵しているものが対象
※2　LTE など内蔵機のみ。ノートパソコンの場合は GPS が内蔵されていなくても、通信基地局を使ったおよその位置確認が可能な場合もある
※3　LTE など内蔵機のみ。リモートロック、リモートワイプを本体が起動していないように見せつつ行うことは、専用に設計された機種のみ可能

# コラム：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対処するのがいいのでしょう？

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自身がダウンしているのか。それを特定し、別経路でのアクセスを確保するのです。

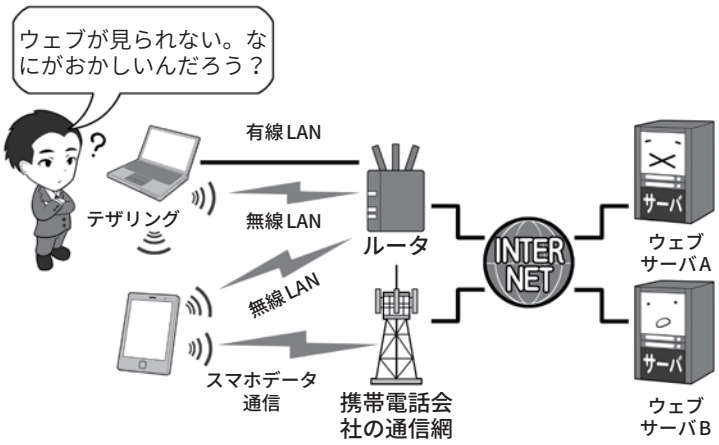
それには主要な機器の二重化(ダブルライン化)が有効です。パソコンで見られないならスマホで確認。無線LANがダメならば有線で。ルータがおかしいならLTEで。Aというサーバがダメならば Bへアクセスして、トラブルが発生した部位の機器を避けるなどの処置をしましょう。

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が流行っているなら別機種で、ウェブブラウザにセキュリティホールがあるなら別のブラウザで。問題があるものを避けて利用するわけです。

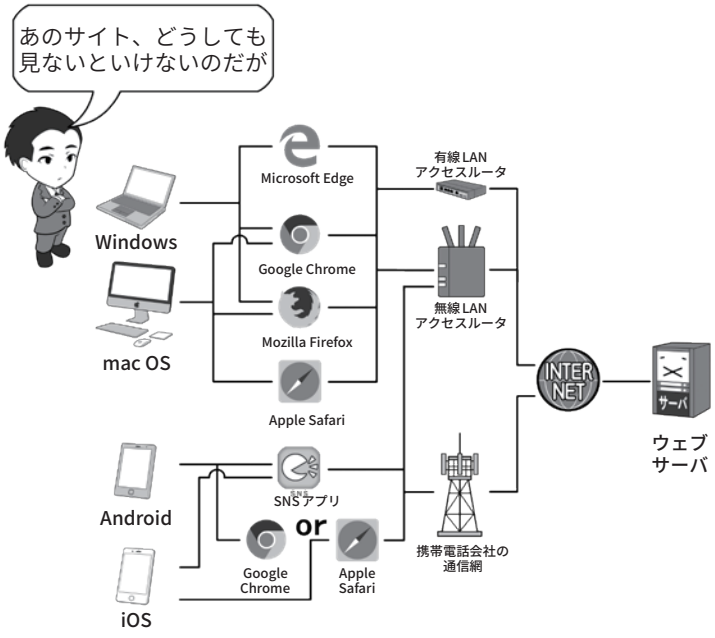
複数台の機材を持つ場合は、機材のタイプを分散することも備えとしては有効でしょう。生物界でも特定の品種に偏った生物は、一つの病気(ウイルスなど)で一気に絶滅に追い込まれる可能性があります。

## 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mac OS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経由で利用するなどの回避手段を設けるのも、一つの防御手段です。

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です。

雑草のような多様な環境を　作って、力強く備えましょう。

# 3 それでも攻撃を受けてしまったときの対処

## 1 兆候に気をつけて、被害が出たら対処

ここまでお伝えしてきた内容を的確に実行してもらえれば、定型化されているサイバー攻撃のかなりの部分は防げるでしょう。

しかし、それで安心してはいけません。人間の心の隙を突く攻撃をしかけられたり、セキュリティホールの発見に対してパッチなどの提供が間に合わない状態で、ゼロデイ攻撃をしかけられたら、防ぐことが難しいからです。

ですから、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、これに対処するスキルを磨きましょう。

攻撃の兆候の中からいくつかの例をあげてみます。

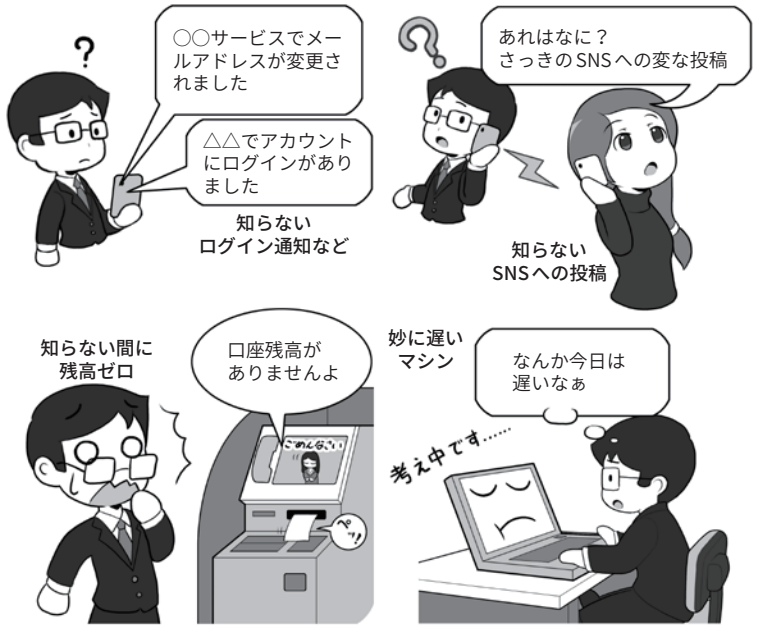
アカウントの乗っ取りは、知らないログイン通知やログインの履歴、ログインしている機器の一覧に知らないものがあったり、あるいはSNSで自分が知らない投稿やアプリ連携などがあります。

銀行口座関連も、ログイン通知があればそれを受け察知し、通帳や取引履歴を見てチェック。クレジットカードはたとえ少額の送金であっても検証しましょう。

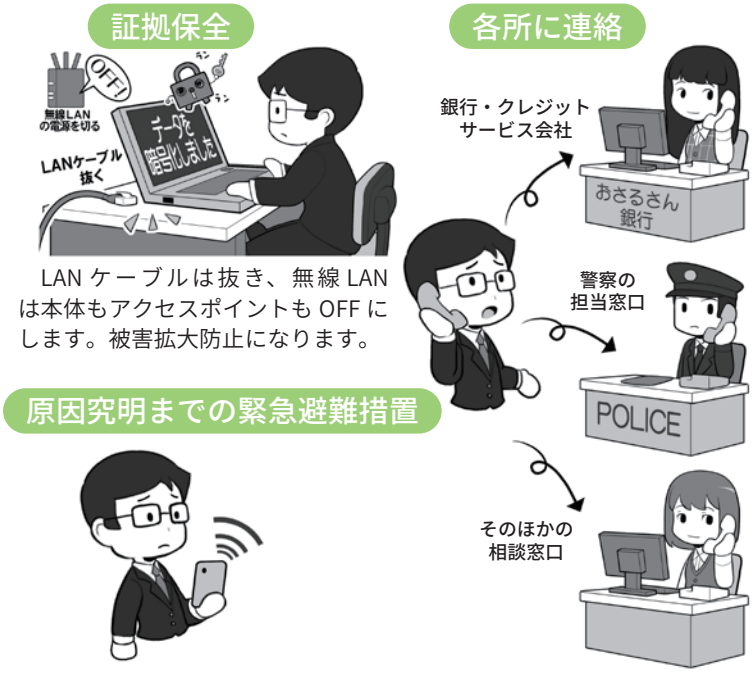
そして、マシンが乗っ取られている場合などは、動作が普段より遅かったり重かったりすることがあります。

もしマルウェアの感染の疑いや、アカウント乗っ取り、情報の流出や不正送金など、実害が判明した

### 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




LANケーブルは抜き、無線LANは本体もアクセスポイントもOFFにします。被害拡大防止になります。

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。家のパソコンが感染したら、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。

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を切断して本体の電源はそのままにして、証拠保全を図りましょう。通信を切断するのは拡散防止のため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、必要に応じて各種サービスに取引を一旦止めてもらう連絡をし、必要に応じて相談窓口などに連絡して対処方法を相談しましょう。実害があれば警察の担当部署に被害届を出しましょう。

問題の解明やマルウェアの駆除が終わるまでは、連絡や仕事のやりとりは、感染したと思われる機器とは別種の機器を用いて行いましょう。同種の機種は同じLANに接続していたことで、感染し攻撃を受けている可能性が否定できないからです。

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場合は駆除します。駆除できない場合は機器を初期化してバックアップから復元し、再びネットに接続して使用し始める前に、まずは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。

システムやセキュリティソフトは最新の状態にし、不審なメールや添付ファイルなどが原因だったならばメールを削除、セキュリティホールになるサポート期限切れの古い機器は買い換え、ソフトやアプリはアンインストールし、アプリやサービス連携の棚卸(たなおろし)をして、知らないものを解除しましょう。

なお、どこかのウェブサービスからパスワードなどが流出した結果、アカウントを乗っ取られてパスワードまで変えられた場合は、自分で再設定はできないので、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。

そして、こういったとき、なんだかんだで一番頼りになるのが、ITに詳しい友だちだったりします。あなたが困っているときにその友だちが復旧を手伝ってくれたとしたら、いつかはあなたが「ITに詳しい友だち」になって、誰かを助ける番になってください。

一人、また一人と、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。

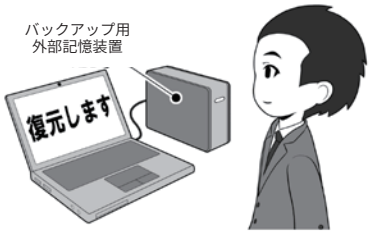
## 実被害が出ていない場合

### 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。



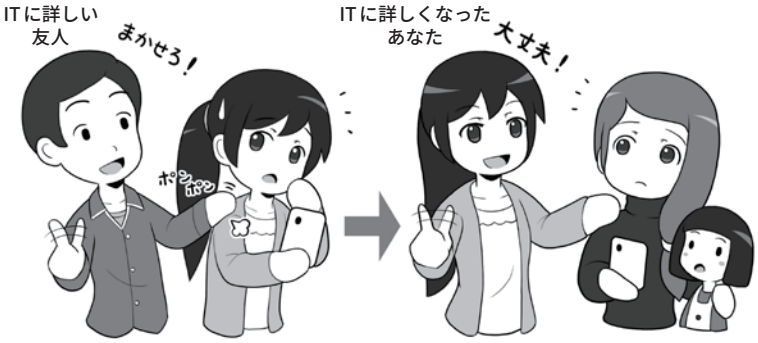

### システムチェックする


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棚卸(たなおろし)


SNSのサービス連携機能は見直しをします。

## そんなとき頼りになるのは……




ITに詳しい友人に対処を手伝ってもらうとともに、一緒に勉強しましょう。その相手が動いてくれる時間には、労力分のお礼をすること忘れずに。

そして、将来同様なケースがおきたら、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。

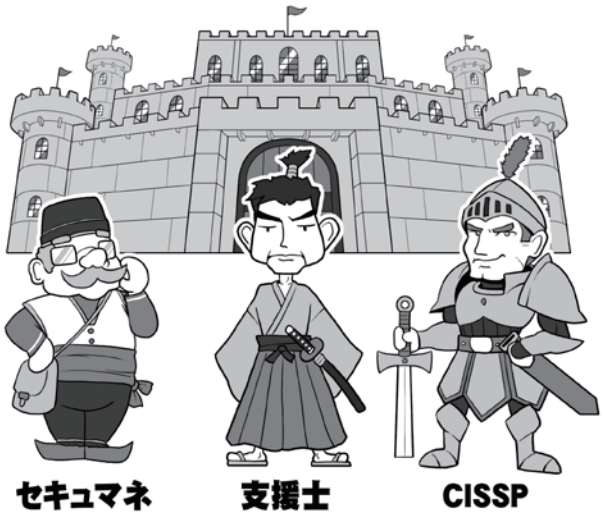
# コラム：セキュリティの資格取得を目指そう

セキュリティについて深く知りたい、もっと詳しく学びたいと考えているのであれば、オススメしたいのが資格の取得を目指した勉強です。すでにセキュリティ関連の資格は数多く存在していて、自分自身のレベルや目的に合わせて選択できる環境が整っているほか、資格取得のための勉強を進めることで、体系立てて知識を獲得できるメリットがあります。

そうしたセキュリティ関連の資格として、比較的取り組みやすいものの1つに「情報セキュリティマネジメント試験」があります。これは、脅威から継続的に組織を守るための基本的なスキルを認定する試験であり、業務で個人情報を取り扱ったり、情報管理を担当したりするすべての人を対象としています。情報セキュリティについて、基礎知識からバランスよく学習したいと考えているのであれば、まずはここからチャレンジするのも1つの方法です。

さらに、高度な試験としては、「情報処理安全確保支援士」やグローバルで普及している「CISSP」(Certified Information Systems Security Professional)などがあります。情報処理安全確保支援士はサイバーセキュリティに関する実践的な知識や技能を有する専門人材の育成や確保を目的とした国家資格制度であり、情報セキュリティに関する高度な知識と技能を持つことを証明することができます。一方、CISSP は(ISC)$^2$(International Information Systems Security Certification Consortium)が認定を行う、国際的な情報セキュリティのプロフェッショナル認証資格です。これらの資格取得に向けた勉強を積み重ねれば、自身のスキルアップにもつながるでしょう。

## 数多くあるセキュリティ資格




現在、セキュリティに関する資格試験は数多くあり、自分のレベルや目的に合わせて取得することが可能です。情報セキュリティに特化した試験にチャレンジする前に、IT に関する全般的な知識が問われる「IT パスポート試験」を受けてみてもよいでしょう。そして、支援士の「士」は騎士や武士の「士」。現代の騎士や武士としてセキュリティを守りましょう。

## セキュリティを網羅的に学ぶことができる


資格取得を目指して勉強する大きなメリットは、その領域に関する知識を段階的かつ網羅的に学べることにあります。また、自分の知識レベルを判断する上でも、こうした試験は大いに役立ちます。