# 

**安全な在宅勤務のための最も重要な5つの手順**

在宅勤務に慣れていないという方もいることでしょう。もしかしたら、新しい環境に適応するのと同じくらい大変な経験かもしれません。可能な限り安全な状態で自宅から業務を行ってもらうということも私たちの目標の一つです。以下に安全に働くための5つの手順を記します。これらの手順は、安全に働くために役立つだけではありません。自宅のサイバーセキュリティを強固にすることで、自分と、ご家族の安全性も格段に高まるという利点もあるのです。



**あなた自身について**: まず何より、テクノロジーのみではセキュリティは完全とは言えません。あなた自身が最大のセキュリティなのです。攻撃者たちは、あなたのコンピューターやその他の機器を狙うのではなく、あなた自身をターゲットにすることが、目的のものを手に入れる最も簡単な方法だと知っています。あなたのパスワードや業務用データにアクセスしたり、コンピューターを操りたいのであれば、彼らはあなたを騙して目的のものを渡すように仕向けます。多くの場合、緊急性を装って騙そうとしてきます。例えば、Microsoftの技術サポートになりすまして電話をかけ、あなたのコンピューターが感染していると主張するといったケースがあります。あるいはメールで、荷物の配送ができなかったとお知らせを送り、有害なリンクを踏ませようとすることもあります。最も一般的なソーシャルエンジニアリング攻撃の徴候には次のようなものがあります。

* **恐怖を感じさせる、脅す、危機感を煽る、重要な期限があると迫り、大げさな切迫感を演出する。サイバー攻撃者は説得力のあるメッセージを作成することに長けています。銀行や政府、国際機関など、信頼できる組織からのメッセージに見えるものを送ってくるのです。**
* セキュリティーポリシーを回避、無視させようと圧力をかけてくる。またはうますぎる話（ご注意を。抽選に当たってなんていません！）
* 友人や同僚から送られてきたかのようなメールが届くが、署名、言葉遣い、文体がその人らしくない。

結局のところ、こういった攻撃を防ぐのは、ソフトではなく人なのです。



**ホームネットワーク**: ほぼすべてのホームネットワークはワイヤレス（Wi-Fi）ネットワークに繋がっています。すべての機器はWi-Fiを通してインターネットに繋がるのです。ほとんどの家のワイヤレスネットワークはインターネットルーターや、専用の無線アクセスポイントによって管理されています。どちらも同じ働きをします。無線信号を発信し、これに自宅の機器が接続するのです。だからこそワイヤレスネットワークを保護することこそが、自宅のセキュリティの鍵なのです。以下の手順でセキュリティを確保しましょう。

* ワイヤレスネットワークを管理する機器のデフォルトの管理者パスワードを変更する。管理者アカウントを使えば、ワイヤレスネットワークの設定を行えます。
* 信頼できる人以外には、絶対にワイヤレスネットワークに接続させないようにしましょう。セキュリティを強固にすれば、これを実現できます。これにより、ワイヤレスネットワークに接続するのにパスワードが必要になり、接続後のオンライン活動は暗号化されます。
* ワイヤレスネットワークへの接続に使うパスワードは、必ず安全性が高く、管理者パスワードとは異なるものにしてください。パスワードは機器によって記録されますので、各機器で一度入力すれば大丈夫です。

どのようにやるのかわかりませんか？インターネットサービスプロバイダに問い合わ  
せる、彼らのwebサイトを確認する、お使いの無線アクセスポイントの説明書を確認  
する、あるいは販売会社のwebサイトを確認しましょう。



**パスワードについて:** パスワードを作成するようにサイトから要請された場合、安全性の高いパスワードを作成しましょう。文字数が多いほど、安全なパスワードになります。簡単に安全性の高いパスワードを作る方法の一つに、パスフレーズがあります。パスフレーズとは、いくつかの言葉からなるパスワードです。例えば、「hachi-hachimitsu-bahbon」などです。個別のパスフレーズを使用するとは、それぞれの機器やオンラインアカウントごとに異なるパスフレーズを使うことを指します。これなら、たとえパスフレーズの1つが流出しても、他のアカウントや機器の安全は保たれます。全てのパスフレーズを覚えていられない？

パスワードマネージャーを使いましょう。これはお使いのパスフレーズのすべてを暗号化し、安全に管理できる（そして他にも数多くの素晴らしい機能を持つ）特別なプログラムです。最後に、可能な限り二段階認証と呼ばれる（二要素認証または多要素認証とも呼ばれます）認証方法を有効にしましょう。二段階認証でもパスワードを使用しますが、二段階認証ではもう一段階の手順が追加されます。お使いのスマートフォンにコードが送られる、あるいはアプリがコードを作成するなどといった手順です。二段階認証は恐らく、オンラインアカウントの保護に際して最も重要なものです。ですが、これは想像するよりもずっと簡単です。

****

**アップデート:** それぞれのコンピューターやモバイルデバイス、プログラムやアプリでは、必ず最新バージョンのソフトウェアを使用してください。サイバー攻撃者は、機器が使用しているソフトウェアに新たな脆弱性が見つからないか、常に探しています。脆弱性を発見した攻撃者たちは、特別なプログラムを使用してそこにつけ込み、あなたのデバイスに侵入します。一方で、それらの機器用にソフトウェアを作成した会社は、その脆弱性の修正に勤しみ、アップデートを公開しています。お使いのコンピューターや機器にこれらのアップデートをすぐにインストールすることで、各段にハッキングされにくくなるのです。コンピューターや機器を最新の状態に保つために、可能な限り自動アップデートを有効にしておきましょう。最新の状態に保つということに関しては、ネットワークに接続されるほぼすべてのテクノロジーについて当てはまります。すなわち、業務用の機器に限らず、インターネットに接続されているTV、ベビーモニター、防犯カメラ、ホームルーター、ゲーム機、自動車でも必要なのです。



**子ども/訪問客**: オフィスにいる場合は、あなたの仕事用ノートパソコンや、その他の機器がお子さんや訪問客、その他のご家族に使用される心配はほとんどありません。あなたの仕事用機器を使ってはいけないということを、ご家族やご友人に必ず理解してもらいましょう。というのも、誤って情報を消去したり改変したり、さらに悪い場合は機器をウイルスに感染させてしまうことがあるからです。