家庭内で安全快適に在宅勤務を行うための
リファレンスガイド

2020年７月１日

一般社団法人　ICT-ISAC

このページは白紙です。

はじめに

世界各地で急速に広まった新型コロナウイルス感染症から社員と業務を守るため、在宅勤務の手段としてこれまで十分なリモートワーク（またはテレワーク）の仕組みを導入してこなかった企業においてもリモート―ワークが行われるようになってきました。

これまでのリモートワークは、平時に“限られた部署または業務の社員”を対象として企業側が VDI（仮想デスクトップ）環境やパソコン、インターネット回線などを用意することが一般的でした。この場合、社員は会社から用意された環境と決められたルールの下で、ある程度安全・安心にリモートワークを行うことができます。しかしながら今回の新型コロナウイルス感染症の対応では、全社員を対象に在宅勤務を行う上で、社員が自宅のインターネット回線やパソコンなどの利用を認められるケースも多く見られます。こうしたケースでは、自宅のインターネット回線やパソコンなどを業務で安全に利用できるよう社員自らがより注意を払う必要があります。

所属する企業が自宅のリモートワーク環境についてガイドラインで細かく定めている場合は企業のガイドラインに従ってください。本リファレンスガイドでは、社員が自宅でリモートワークのために利用するインターネット回線やパソコンなどの利用にあたり、会社から細かい指示がない場合に社員が個人で注意しなくてはならない点についてセキュリティの観点から気づきを提供することを目的としています。会社の IT 部門の目線ではなく、社員の目線で参考にしていただくことを想定していますが、リモートワーク環境について社員目線で確認しながら、必要に応じて会社の IT 部門との相談材料のひとつとして利用いただくことも想定しています。

本リファレンスガイドは一般社団法人 ICT-ISAC（以下、ICT-ISAC）がリモートワークの安全な導入に向けて国内 ISAC 組織の協力のもと作成しました。本リファレンスガイドの利用は、ISAC 会員企業などの社員を想定していますが、フリーランスなどの個人事業者の方でも十分に参考にいただけるものと考えています。

2020 年 7 月

作成　ICT-ISAC
協力　金融 ISAC
電力 ISAC
交通 ISAC
ソフトウェア ISAC
J-AUTO-ISAC
貿易会 ISAC

リファレンスガイドについて

本書はリファレンスガイドとしてリモートワークのセキュリティに関する総合的な情報を提供します。各企業の規模、業務形態、業務内容、情報の機密度などに合わせて適宜利用する使い方を想定しています。

リファレンスガイドでは、これまでオフィスを中心に実施してきた業務を在宅環境で快適かつ安全に行うため、各企業の社員が自宅でリモートワーク環境を整備するためヒントをまとめました。なお、自宅のインターネット回線を使って家から会社のシステムなどを利用するリモートワークを前提にセキュリティ対策を挙げていますが、所属する企業が自宅のリモートワーク環境についてガイドラインなどで細かく定められている場合には所属する企業のガイドラインを遵守してください。

リファレンスガイドの利用者

- 主に企業に従事する社員（最近リモートワークを始めた、あるいは、これからリモートワークを始める社員）

リファレンスガイドの目指すもの

- 社員が安全にリモートワークを行うために注意すべき事項をできるだけ平易な言葉でわかりやすく伝える
- 快適で安全なリモートワークを行うための気づきを与える

リファレンスガイドの対象範囲と構成

リファレンスガイドの対象範囲は社員が用意するリモートワーク環境（インターネット回線、パソコン、居室など）とし、下記の構成でまとめます。

1. リモートワークを行うための環境
2. リモートワークを行う上で、最低限チェックすべきセキュリティ項目
3. より快適にリモートワークをするためのヒント

1. リモートワークを行うための環境

ここでは、自宅でリモートワークを行うために必要な物理環境について考え方を紹介します。
所属する企業がインターネット回線やパソコンなどのリモートワーク環境を用意する場合には会社の定めるルールやガイドラインに従ってください。
リモートワーク環境を社員が個人の裁量で用意することが認められている場合には、ここで挙げる項目を確認しておくとよいでしょう。

リモートワークを行うためには、自宅にインターネット回線、パソコン、作業場所を用意することが一般的です。

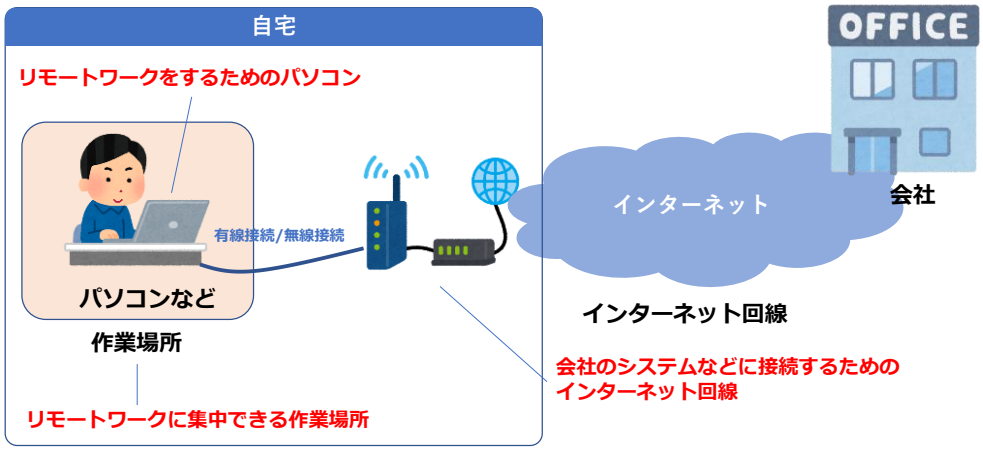

図 1-1 リモートワークを行うための環境

■ インターネット回線

自宅からリモートワークを行うためには、自宅にインターネット回線が必要となります。
自宅で利用可能なインターネット回線には様々なものがありますが、リモートワークを快適に行うためには、高速・広帯域なインターネット回線を用意することが推奨されます。インターネット回線の速度が遅い場合、通信が途切れるなど快適に業務を行えない場合があります。特に家族が同時に通信量の大きい Web 会議やオンライン授業を行う際などに自宅のネットワークが遅いと業務に支障が生じます。

自宅に用意するインターネット回線の例を示します。

- 光回線や CATV インターネット
- モバイル Wi-Fi ルータ
- スマートフォンのテザリング（スマートフォンを経由したインターネット接続）

インターネット回線は、在宅環境に応じて、回線種別、回線速度や接続形態を選択するとよいでしょう。一般的には高速・広帯域の回線の方が快適に使えますが、その分費用もかかりますので、しばらく利用してから必要な速度の回線に変更してもよいかもしれません。

リモートワークに利用するパソコンをインターネット回線に接続する方法としては、有線接続／無線接続があります。一般的には有線接続の方が無線接続よりも安定した通信を行うことができますが、無線接続ではケーブルに接続する必要がないため、無線接続ができる範囲であれば、場所の制約を受けずにリモートワークが可能となります。

無線接続の方法としてWi-Fiルータを利用する場合には、特に次の点に気を付けましょう。

Wi-Fi ルータのセキュリティ設定が不適切だと、外部の人が勝手に接続し、情報詐取を試みるかもしれません。適切なセキュリティ設定が重要です。

Wi-Fi ルータを利用する際のセキュリティについてのチェック項目は次章「2.リモートワークの際に、最低限チェックすべきセキュリティ項目」で紹介します。

■ パソコン

リモートワークを行うためにパソコンなどを使うことが多いでしょう。快適で安全なリモートワークを行うためには、できれば、高性能で製造年の新しいパソコンを利用しましょう。

特にパソコンの製造年が古い場合には、最新の機器やソフトウェアが利用できない、Web 会議や文書作成などを快適に行うことができない場合があるほか、メーカーのサポートが受けられないなど十分なセキュリティ対策を行えない場合があります。

Windows OS などはメーカーのサポートがあり、最新のセキュリティパッチを適用し、ウイルス対策ソフトを導入してマルウェア感染などに備えましょう。

パソコンのセキュリティについてのチェック項目は次章「2. リモートワークの際に、最低限チェックすべきセキュリティ項目」で紹介します。

■ 作業場所

インターネットが使えて業務に集中できる作業場所を確保することが重要です。

リモートワーク中は家族などからパソコンの画面が見えたり、音声が漏れたりしないよう注意しましょう。特に最近では自宅から会議に参加できる様々な Web 会議システム[1]が使われています。パソコンの画面や音声から業務内容が家族に漏れることを防ぐと同時に、家族のプライバシー情報が Web 会議などを通じて流れることのないよう、できれば専用の居室を確保することが望ましいです。

専用の居室を確保できない場合には次の点を検討しましょう。

- パソコンの画面を家族に覗かれることのないよう、覗き見防止フィルターを使用する。
- 作業場所と家族との間にパーティションを設置する。

[1] 代表的な Web 会議システムには Zoom、Teams、Webex、Skype などがあります。

- 音声が家族に聞かれることのないようヘッドセットなどを使用する。
- Web 会議中に家族が映り込んだり、声が流れたりすることのないよう、予め Web 会議の予定を家族に伝え、家族に注意を促す。

2. リモートワークの際に、最低限チェックすべきセキュリティ項目

ここではリモートワークを行う際に、最低限チェックすべきセキュリティ項目を紹介します。
所属する企業が自宅のリモートワーク環境についてルールやガイドラインを定めている場合には、必ず会社のルールやガイドラインを遵守してください。
社員が個人で用意した環境を使ってリモートワークを行う場合には、最低限、ここで挙げるセキュリティ項目をチェックするとよいでしょう。

■ 自宅のルータの管理画面や機器がインターネットから見えていないこと

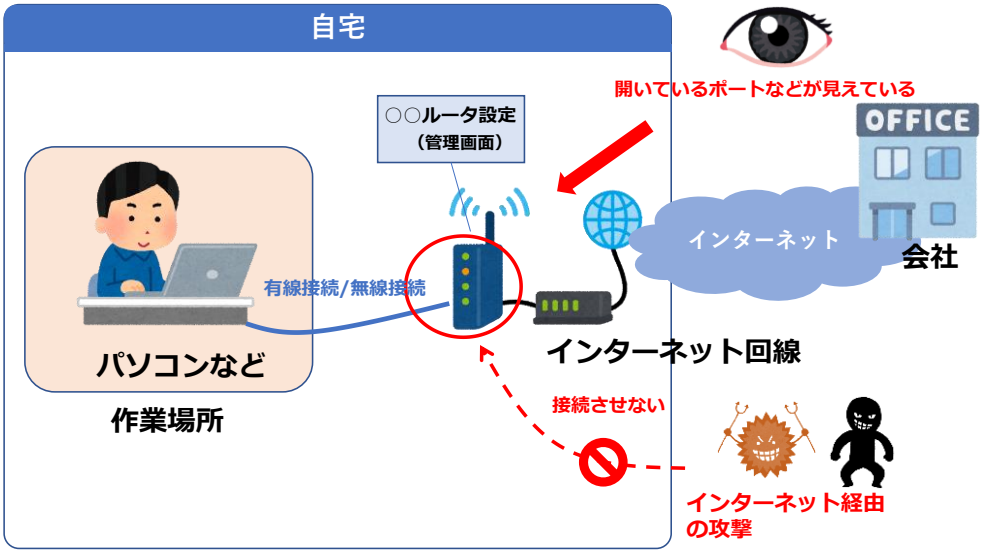

図 2-1　インターネットから機器が見えていないことを確認

インターネットから自宅のネットワーク機器に意図せずにアクセス可能となっている場合があります。この場合、悪意のある人が外部からネットワーク機器へのアクセスを試みたり、機器がマルウェアに感染したりすることがあります。特にルータの管理画面がインターネットから見えていて、外部から設定変更などが可能な場合はとても危険です。まず、インターネットから自宅のネットワーク機器がどのように見えているか確認しておくとよいでしょう。ここでは、自宅の機器がインターネットからどのように見えているかを確認する方法の一例を紹介しますので参考にしてください。

一般的にはインターネットからルータの管理画面へのアクセスは不要[2]です。インターネットから自宅のルータの設定を確認したり変更したりする必要がないのであれば、インターネットからルータへのアクセスをできないようにするとよいでしょう。なお、ルータの設

[2] 意図的にインターネットから管理画面へアクセスできる設定している場合はセキュリティに注意して利用してください。

定変更については、ご利用の機器のマニュアルなどを参照ください。

◆ 自宅の機器がインターネットからどのように見えているかを確認する方法

① グローバル IP アドレスの確認

インターネットに接続されている機器にはグローバル IP アドレスが付与されています。グローバル IP アドレスがインターネットから見える状態であれば、悪意のある人が攻撃のターゲットとするかもしれません。確認くん[3]などを利用してご利用中の機器（ルータなど）の IP アドレスを確認しておきましょう。

確認くん
https://www.ugtop.com/spill.shtml

「あなたのＩＰアドレス(IPv4)」に表示される IP アドレスがインターネットからアクセスできるグローバル IP アドレスです。（通常はルータのインターネット側の IP アドレスが表示されます。）

② Shodan[4]などで自宅のルータのグローバル IP アドレスを検索

グローバル IP アドレスがわかるだけですぐに悪意のある人から攻撃を受けるわけではありません。しかしながら、悪意のある人がよく攻撃に利用するポート[5]が意図せず開いていると攻撃を受ける可能性がありますので、Shodan などのサービスを使って意図しないポートが開いていないことを確認しましょう。

Shodan
https://www.shodan.io/

確認くんなどで調べて自宅の機器（ルータ）のグローバル IP アドレスを Shodan に投入し、自宅の機器がインターネットから見えているかどうかを確認します。

通常は不要なポートが閉じられていれば自宅のルータの IP アドレスを入れても検索結果は表示されないため、何も表示されなければ安心の目安になります。なお、Shodan

[3] 自分が利用している機器のグローバル IP アドレスを調べるサービスです。同様なサービスはほかにもたくさんあります。

[4] インターネットに接続された機器を検索できるサービスです。同様なサービスはほかにもたくさんあります。

[5] ポートはネットワーク上で特定の番号で、一般的には Web サービス(http)は 80 番、telnet は 23 番などのポートを使用します。telnet を使用しないのに 23 番が開いていると悪意のある人が 23 番を狙って攻撃をすることがあるため、不要であれば、ポートは閉じておいた方がよいでしょう。

は定期的に IP アドレスやポートの情報を収集していますが、検索結果に表示されるのは Shodan が調査した時点の情報です。ご利用中のインターネット回線によっては、ご利用中の IP アドレスが時々変更になる場合があり、その場合は、Shodan で正しく確認できない場合があります。

Shodan の検索結果で、Ports の欄に 23 などの数字があれば、その数字のポートがオープンとなっていてインターネットからそのポートへのアクセスが可能であることを示します。まずはオープンとなっているポートがあり、インターネットからアクセス可能かどうかは把握しておきましょう。そのポートをオープンとしておくべきかどうかは一概にはいえませんが、一般的にはポート 23 はマルウェア（コンピュータウイルス）の感染などに使われることが多く、注意が必要です。

■ 自宅のルータの管理画面のパスワードを適切に設定しておく

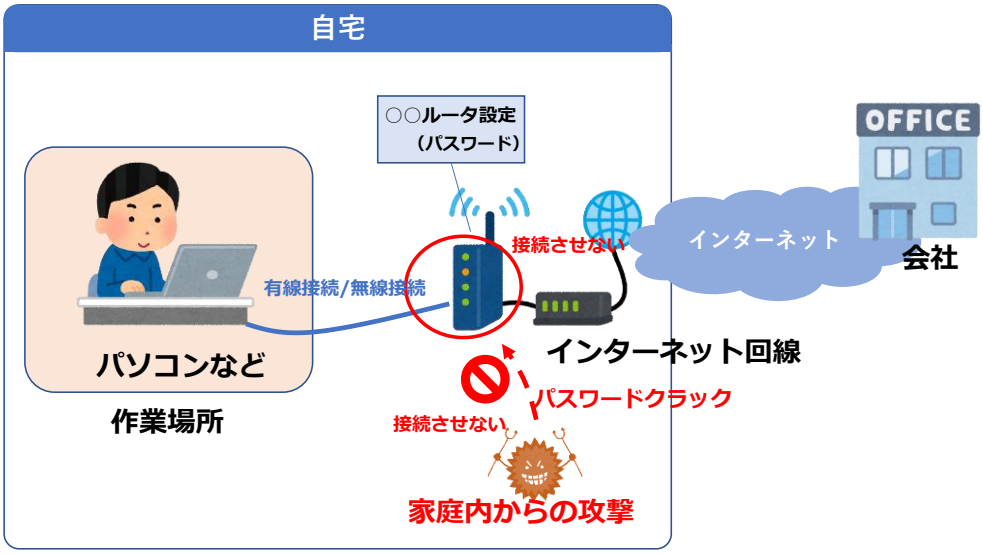

図 2-2　自宅のルータの管理画面のパスワード設定

インターネットから自宅のルータなどへのアクセスが出来なければ[6]、インターネットから直接の攻撃は防げると考えられます。しかしながら、自宅の LAN にある機器からルータにアクセスできれば、家庭内の機器がマルウェアに感染するなどにより、家庭内からの不正アクセスも想定されます。

自宅の LAN からルータの管理画面が操作できる場合には、管理画面のパスワードはデフォルト設定（初期設定）を使わず、適切に設定しておきましょう。（ルータのマニュアルがインターネットで公開されている場合、攻撃者はデフォルトのパスワードを容易に取得することができるので、家庭内に入り込んだマルウェアなどにパスワードクラックを試行さ

6 不要なポートが閉じられていて Shodan などで自宅の機器が表示されない状態。

せることができます。）

パスワードは、一般的には大小英字、数字および記号を混在させて最低でも 8 文字以上で推測されにくいものがよいとされています。なおパスワードの設定方法については、ルータのマニュアルなどを参照ください。

■ 自宅の Wi-Fi ネットワークのセキュリティを適切に設定する

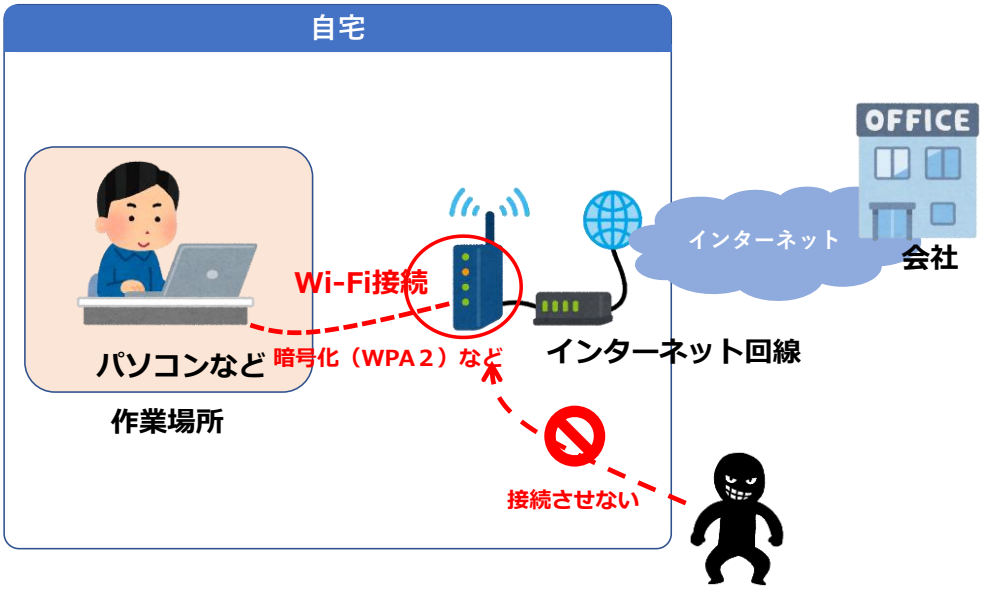

図 2-3　自宅の Wi-Fi ネットワークのセキュリティ設定

リモートワークで使用するパソコンなどを有線接続ではなく、無線接続している場合には、Wi-Fi ネットワークのセキュリティを適切に設定する必要があります。

Wi-Fi ネットワークのセキュリティが不適切である場合、他人が容易に自宅の Wi-Fi ネットワークに接続できてしまいます。自宅の Wi-Fi ネットワークに意図せず他人がアクセスし、Wi-Fi ネットワークを勝手に利用されたり、情報を詐取されたりすることがないよう、自宅の Wi-Fi ネットワークのセキュリティを適切に設定しましょう。

- セキュリティ方式は適切な暗号方式（WPA2 など）に設定されていることを確認する（古い Wi-Fi ルータでは WEP という暗号方式を使用するものがあるかもしれませんが、脆弱性が指摘されていますので使用は厳禁です。）
- 推測されにくいパスワードを設定する。（パスワードは、一般的には大小英字、数字および記号を混在させて最低でも 8 文字以上で推測されにくいものがよいとされています。）

■ 見知らぬ Wi-Fi アクセスポイントに接続しない

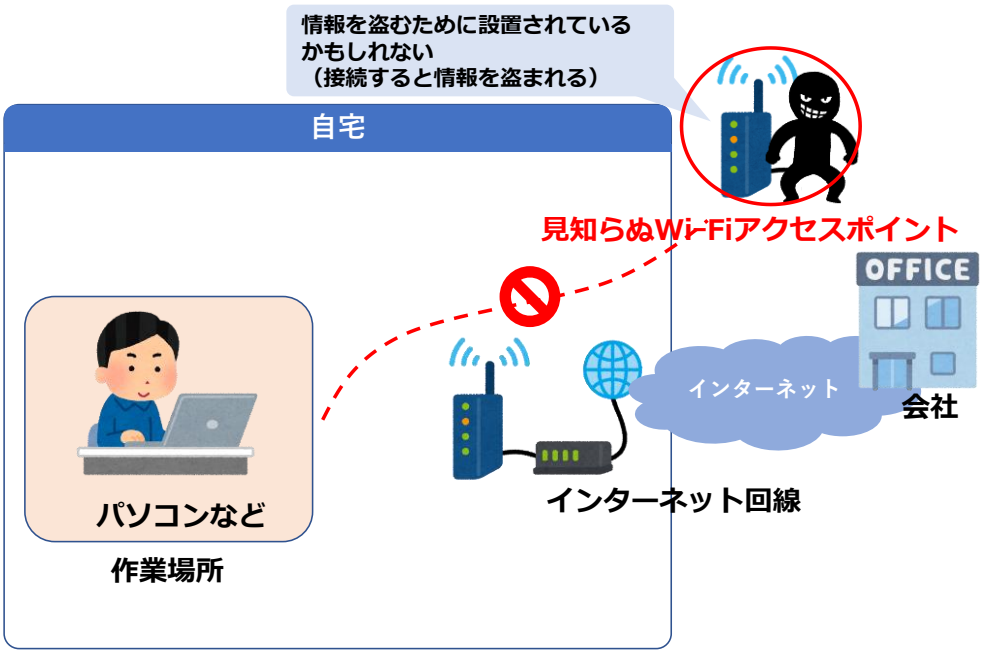

図 2-4　見知らぬ Wi-Fi アクセスポイント

自宅、外出先に関わらず、見知らぬ Wi-Fi アクセスポイントに接続しないようにしましょう。誰が管理しているのかわからない見知らぬ Wi-Fi アクセスポイントは、情報を詐取するために設置された悪意のあるものかもしれません。悪意のある Wi-Fi アクセスポイントに接続した場合、情報を詐取されたり、マルウェアに感染させられたりするといった被害[7]に遭う場合があります。仮に、悪意のある Wi-Fi アクセスポイントではないとしても、パスワードなしに簡単にアクセスできるような Wi-Fi アクセスポイントは適切にセキュリティ設定がされていないはずですので、見知らぬ Wi-Fi アクセスポイントへの接続は避けるべきです。

なお、誰もが知っているような企業などが提供する Wi-Fi アクセスポイントを装った悪意のある Wi-Fi アクセスポイント（偽 Wi-Fi）もあるかもしれません。普段使っている Wi-Fi アクセスポイントを装っていた場合、パソコンの Wi-Fi 接続の設定を「自動」としていると、偽 Wi-Fi に接続してしまい、情報を搾取されてしまうことがあります。Wi-Fi 接続の設定は「手動」にしておいた方がよいでしょう。

[7] 写真や動画、ID、パスワード、クレジットカード番号などの個人情報の流出やマルウェア感染、不正なサイトへのアクセス、遠隔操作など様々な被害が想定されます。

■ 利用するパソコンの OS、ドライバ、セキュリティソフト、その他のソフトウェアを最新化する

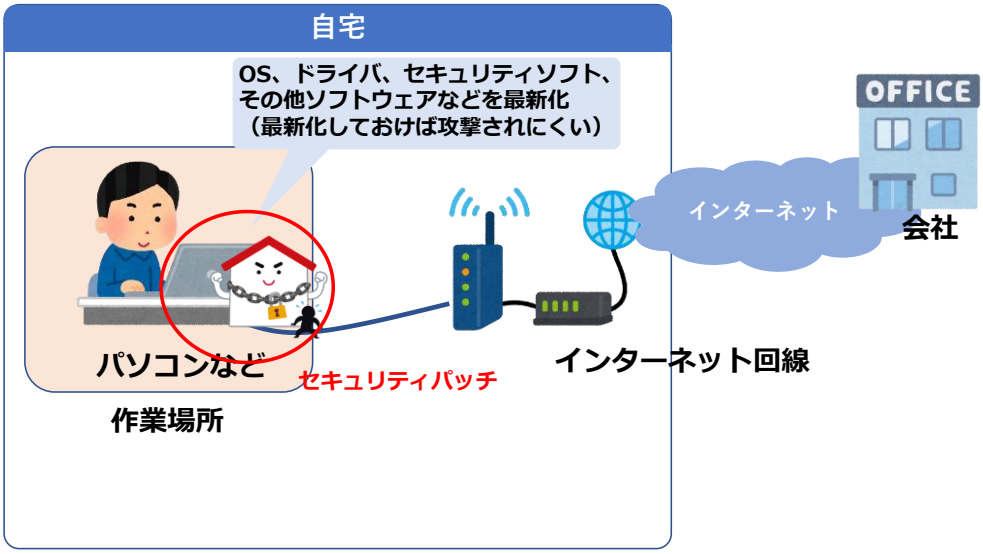

図 2-5 ソフトウェアの最新化

多くのソフトウェアはリリース後に脆弱性が見つかることが多々あります。

脆弱性のあるソフトウェアを放置して使い続けていると、ソフトウェアの脆弱性が悪用され、マルウェアに感染したり、情報を詐取されたりすることがあります。こうした被害を防ぐため、常に最新のセキュリティパッチ（製品に脆弱性が見つかった場合の修正プログラム）を適用したソフトウェアを利用しましょう。Windows OS を利用していると定期的の Windows Update を要求されますが、脆弱性が見つかった場合の修正プログラムを含みますので必ず実施しましょう。

なお Windows 7 など、サポートが終了している古い OS の使用は厳禁です。新たな脆弱性に対してセキュリティパッチが提供されないため、脆弱性が残り続け、攻撃に利用されます。

ソフトウェアを最新化する方法については、ソフトウェアごとに異なりますので、メーカーのホームページなどを参照してください。

また、ソフトウェアに自動でアップデートする機能があれば利用しましょう。

■　パソコンの共有設定を確認しておく

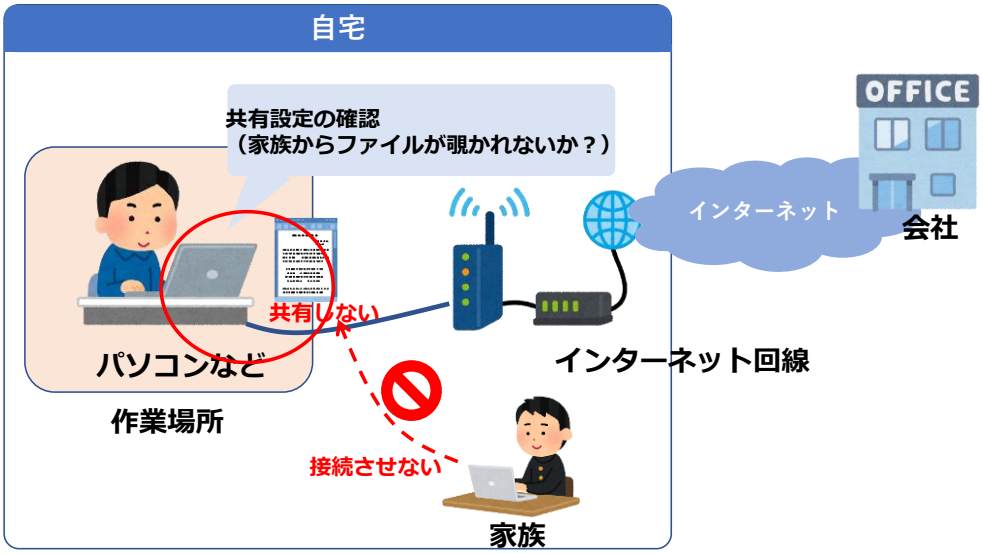

図 2-6　共有設定の確認

リモートワークで利用するパソコンに不要な共有設定がされていないか確認しましょう。

一般的には業務に関係するファイルなどを家族に共有する必要はありません。共有設定が適切にされていない場合、家族などにファイルを覗かれるだけでなく、マルウェアなどにより情報が詐取されることがあります。業務に関係するファイルが流出してインターネットに公開されたり、悪意のある人に利用されたりすると大きな問題となります。

なお、共有設定の確認方法については、メーカーのマニュアルなどを参照ください。

■ 自宅の LAN に接続されている機器を確認しておく

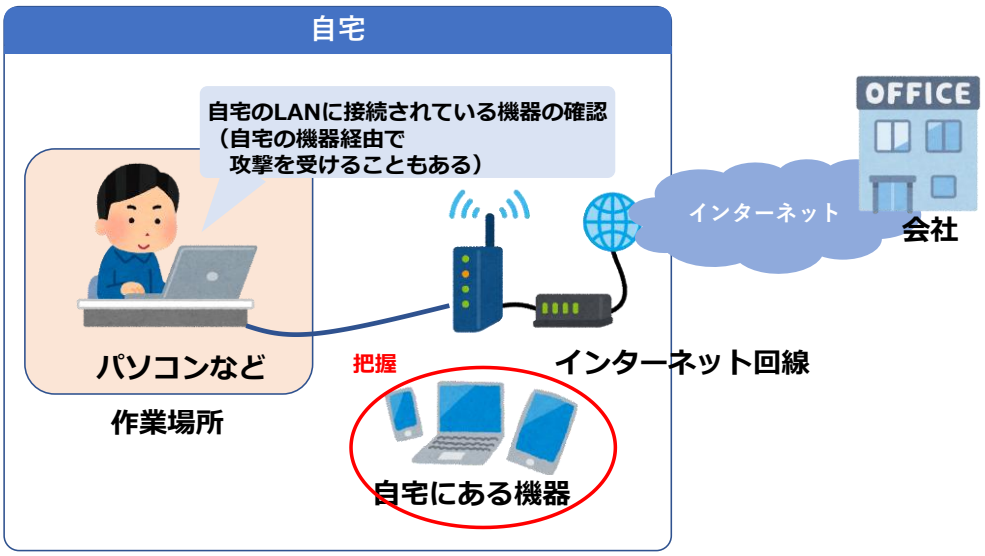

図 2-7　自宅にある機器

自宅の LAN にはパソコンだけでなく、プリンターやカメラ、テレビ、スマートスピーカーなどの様々な機器が接続されているかもしれません。自宅の LAN に接続されている機器がマルウェア感染の踏み台などになる場合があるため、まず自宅の LAN にどのような機器が接続されているのかを確認しておきましょう。自宅の LAN に不審な機器が接続されている場合は、機器を特定して不審な機器であるかどうかを確認しましょう。自宅の LAN に接続されている機器は、家族が知らない間に機器を接続するなどで状況が変化することがあるため、定期的に自宅の LAN の接続機器を確認しましょう。

なお、自宅の LAN に家族が管理している機器が接続されている場合には、家族に各機器のセキュリティ対策を依頼しましょう。

◆　簡単に自宅の LAN に接続されている機器を確認する方法

自宅の LAN に接続されている機器を確認するツールはここで紹介する以外にも様々なものがあります。

トレンドマイクロ「オンラインスキャン　for Home Network」
https://www.trendmicro.com/ja_jp/forHome/products/hw_onlinescan.html

自宅の LAN に不審な機器が接続されている場合には、機器を特定の上、必要に応じて自宅の LAN から切り離すなどの対応を検討しましょう。

■　すべての機器のファームウェアを更新する

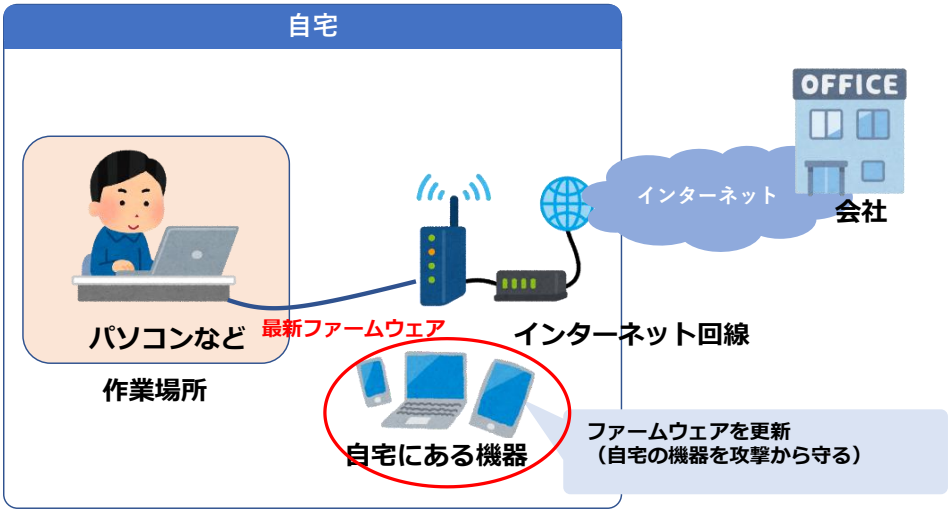

図 2-8　ファームウェアの更新

自宅にある機器を確認したら、すべての機器のファームウェアバージョン[8]を確認し、最新のバージョンに更新しましょう。

ファームウェアバージョンの確認方法については、機器のマニュアルなどを参照してください。ファームウェアバージョンが最新であるかどうかは、メーカーのホームページのサポートページなどで調べることができます。

最新のファームウェアが公開されていれば、機器のマニュアルなどに従いファームウェアを更新しましょう。ファームウェアが最新ではない場合、機器に脆弱性があるかも知れません。

機器にファームウェアの自動更新機能があれば、設定しておきましょう。

[8] ファームウェアは機器に組み込まれ、機器を動かすためのソフトウェアです。機能の追加やセキュリティパッチの適用によりバージョンが上がるため、利用している機器のファームウェアのバージョンを確認することが重要です。

■ すべての機器に対して適切なパスワードを設定する

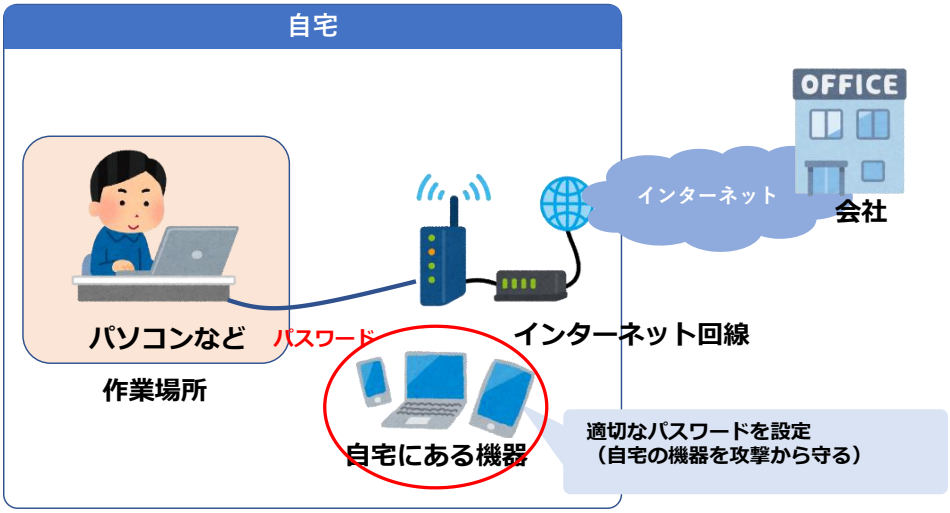

図 2-9　自宅にある機器のパスワード設定

自宅にある LAN 上のすべての機器のファームウェアを最新化した後は、自宅にある LAN 上の機器に適切なパスワードを設定し、マルウェア感染などのサイバー攻撃の踏み台として利用されることを防ぎましょう。（パスワードは、一般的には大小英字、数字および記号を混在させて最低でも 8 文字以上で推測されにくいものがよいとされています。）

また、これらの機器を利用する人を限定し、不要なアクセスは不許可とするなどアクセス権限の見直しを行いましょう。

■ 利用しようとするツールが業務上使用を許可されているか確認する

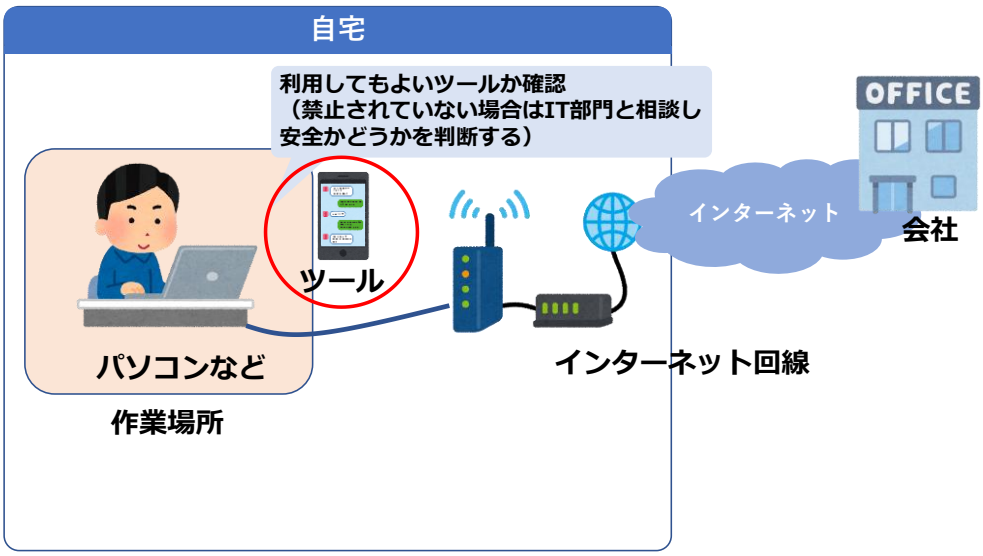

図 2-10　ツール利用の確認

リモートワークでは、コミュニケーションや業務の効率化のため、様々なツールを活用することが想定されます。これまで利用したことのない SNS や Web 会議システム、ファイル共有システムなどのツールの利用を取引先などから指定されることもあるでしょう。

原則、所属する企業が許可したツールを利用し、禁止されているツールは利用してはいけません。利用しようとするツールが業務上使用を許可されているかどうかを確認しましょう。

他社との会議を円滑に進めるために利用したいが、所属する企業が明確に禁止していない場合、IT 部門と相談の上、次のような観点で利用を検討するとよいかもしれません。

- セキュリティの問題などがニュースなどで指摘されていないツールであること
- 多くの人が業務に利用している実績のあるツールであること
- 一般的に信頼できると考えられる企業が提供しているツールであること
- データなどがクラウドに送信される場合にはその扱いを理解した上で利用すること

■ パソコンに接続されたマイクやカメラの状態を意識する

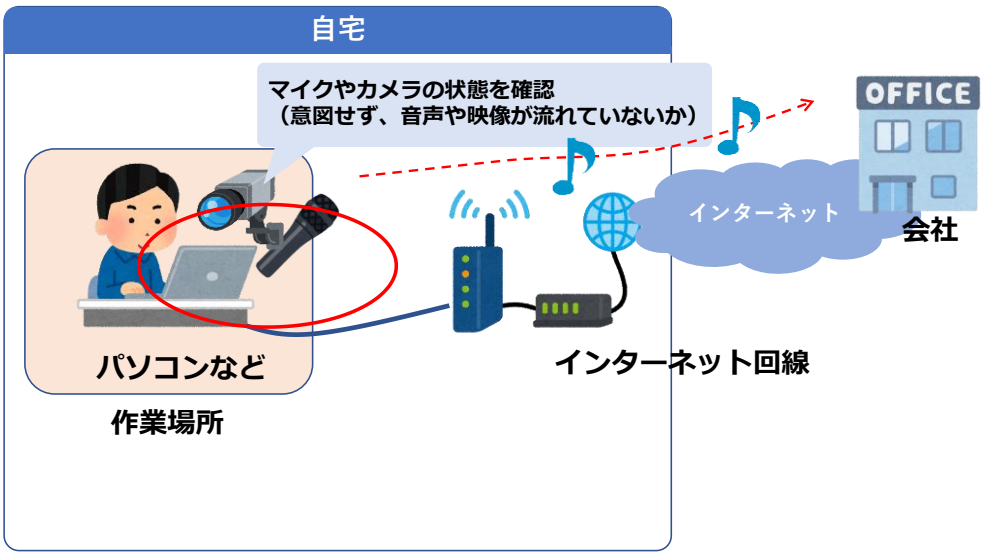

図 2-11　マイクやカメラの状態確認

リモートワークでは、Web 会議を利用する際にマイクやカメラを利用する場合が多くなります。業務内容が家族に漏れることに注するのと合わせて、プライバシーの観点から、不必要に家族の会話など周囲の声がマイクに入り込む、周囲の状況がカメラに映りこむことがないように注意しましょう。

また複数の Web 会議システムを利用していると、意図せず前の Web 会議にマイクやカメラが接続されたまま、情報漏洩につながることなどがあります。終了した Web 会議にマイクやカメラが接続されたままになっていないことを確認しましょう。

なお、スマートスピーカーにも注意が必要です。スマートスピーカーには音声に反応して家電などを制御できるものもありますが、Web 会議システムを通じた誰かの音声に反応[9]してしまうかもしれません。スマートスピーカーのマイクはオフにしておくのがよいでしょう。

9 例えば、離席中に誰かが Web 会議システムの音声を通じてスマートスピーカーに向かってテレビを ON にするなどの命令ができるかもしれません。

■　業務で利用するパソコンは家族とは共有しない

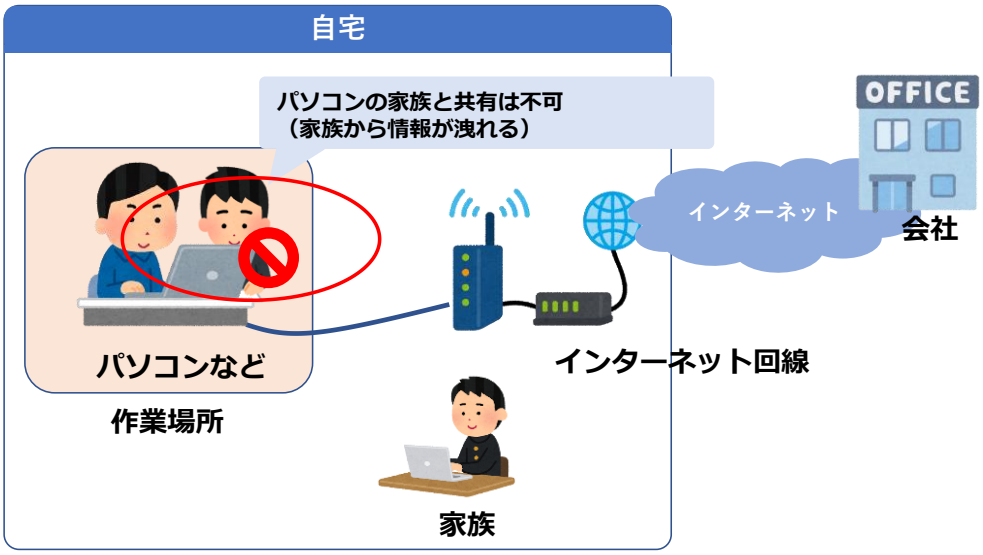

図 2-12　パソコンの共有は不可

業務で利用するパソコンを家族と共有することは避けましょう。家族に悪意がなくても不適切な設定で情報が漏洩する、マルウェアに感染するなど、家族が誤ってパソコンを壊したり、大事なデータを消してしまうなど、家族を巻き込んだトラブルに発展することも想定されます。

■ 利用機器のサポート体制を確認する

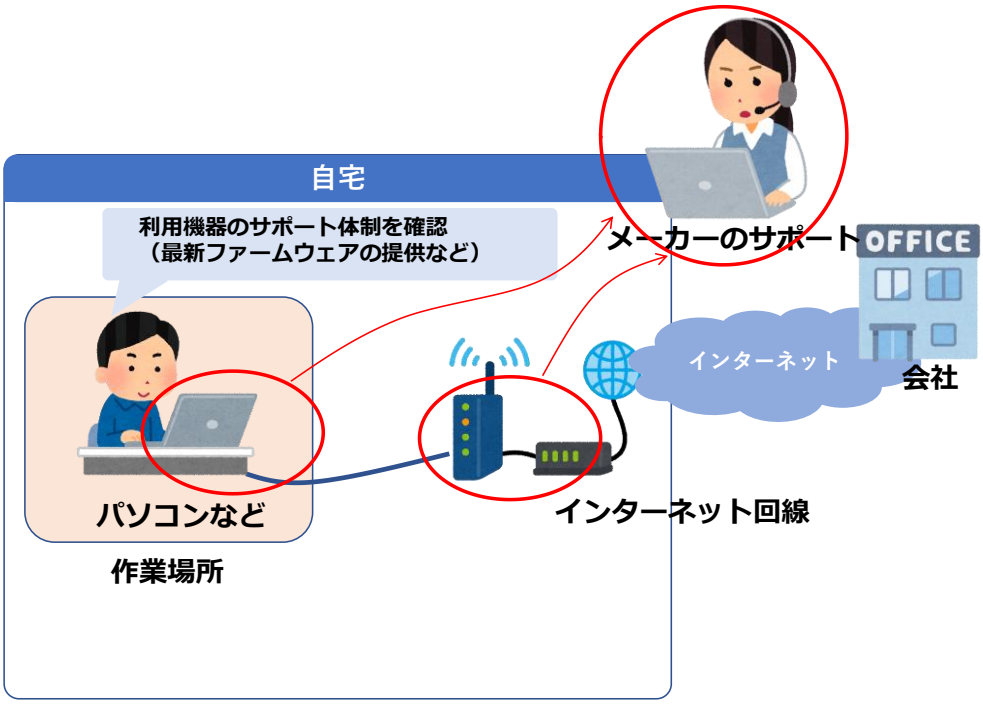

図 2-13　利用機器のサポート体制確認

機器を購入後に脆弱性が見つかることは多々あります。脆弱性を放置しておくとマルウェアに感染したり、不正なアクセスを受けたりしますので、速やかに脆弱性を修正することが重要です。そのためには、迅速にセキュリティパッチやファームウェアを提供するなどサポートがしっかりしているように見えるメーカーの機器を利用しましょう。

ひとつの目安としては、メーカーのホームページにサポートページがある、過去にセキュリティパッチやファームウェアを提供している実績があるなども参考になります。

■ 業務内容が漏れないよう家族の目や耳も意識する

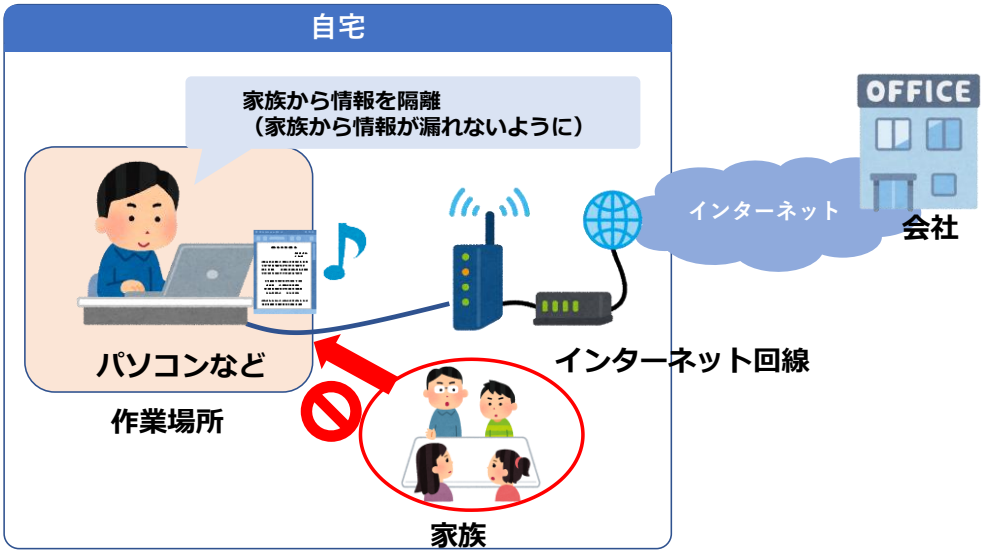

図 2-14　家族に見られない環境

業務内容を家族などにみられることのないよう、作業場所は個室を確保できることが理想です。作業場所として個室を確保できない場合など、業務の内容が意図せず家族に漏洩し、トラブルとならないよう、家族の目や耳も意識しましょう。

- 離席する際はパソコンの画面をロックする。
  ショートカットキー 「Win 」+「 L」
- 覗き見防止フィルターを導入し、画面を覗かれないようにする。
- ヘッドセットを利用し、Web 会議などの会話が漏れないようにする。
- 背後に家族がいない場所で業務を行う。

3. より快適にリモートワークをするためのヒント

ここでは、リモートワークをより快適にするためのヒント、急なトラブルに遭遇した際の解決するためのヒントなどを紹介します。

■ Windows OS のアップデートの時期を意識する

Windows OS の定期的なアップデートで意図しないタイミングでパソコンが再起動されることがあります。業務の中断を避けるため、Windows OS のアップデートは自分が都合の良いタイミングで早めに実施することが望ましいです。

■ ネットワークの負荷を軽減する

急激なリモートワーク需要に企業側の設備容量が十分に足りていない場合など、社員のアクセスが集中すると業務に支障が生じる場合があります。設備増強は企業が判断して実施すべきものですが、ここでは社員ができる対策の例を示します。

- 業務開始のオフピーク化（朝定時開始時刻前後のアクセス集中を避けるなど）
- Web 会議時の工夫
  - VDI（仮想デスクトップ）環境を避け、モバイルデバイス、音声回線などを利用
  - マイクは話す時だけ ON
  - ビデオ通話は OFF

■ 不具合に備えて代替手段を用意しておく

インターネットが利用できない、パソコンの調子が悪いなどでリモートワーク環境をすぐに復旧ができない場合に備えて代替手段を用意しておくとよいでしょう。

◆ インターネットが利用できない場合

モバイルルータの利用やスマートフォンのテザリングなど、普段リモートワークで利用しているインターネット回線と別の回線が利用できるとよいでしょう。特にテザリングはスマートフォンを利用中であれば、新たにインターネット回線を用意しなくてもスマートフォン経由でパソコンをインターネットに接続する手軽な方法ですが、利用できるかどうかはスマートフォンで利用しているサービスに拠りますので、利用している携帯電話会社に確認してください。

◆ パソコンの調子が悪い場合

Web 会議などはスマートフォンでも利用が可能です。セキュリティポリシー上、別のパソコンやスマートフォンの利用が可能な場合には代替手段として利用できます。Web 会議の時間が迫っている場合などはパソコンの復旧を試みるよりも代替手段に切り替える方がよ

いでしょう。急なトラブルに素早く切り替えられるよう、スマートフォンなどには Web 会議アプリなどをインストールしておくとよいでしょう。

■ ネットワークを最適化する

家族が同時に Web 会議やオンライン授業などを行う場合にネットワークが遅いと Web 会議やオンライン授業などに支障をきたします。Web 会議がうまくつながらない、時々途切れるなどが生じた場合には、ネットワークの混雑や速度の確認をしましょう。

① ネットワークの速度を計測する

インターネットの速度を計測するツールは多くあります。頻繁に利用しすぎるとかえってネットワークに負荷を生じますが、在宅勤務で利用するパソコンがインターネットにどのくらいの速度で接続されているかは把握しておくとよいでしょう。

インターネット速度測定
https://www.speedtest.net/

具体的にどのくらいの回線速度が理想であるかは一概にはいえませんが、ストレスなく動画などを利用する際には数 Mbps 以上の速度が必要だといわれています。家族が同時に Web 会議や動画配信サービスなどを利用している場合にはより高速な回線が必要となるかもしれません。

なお、インターネット速度測定はインターネットに負荷を与えるため、頻繁に実施することは避けましょう。

② ネットワークを最適化する

インターネットが遅いと感じる場合には次の点を検討しましょう。

- Wi-Fi で接続している場合には、Wi-Fi の電波状況、方式などを確認して適切に設定することでインターネットへの接続速度が改善することがあります。Wi-Fi ルータとパソコンとの間に物理的な遮蔽物があったり、電子レンジなどの電波を発する家電などがあったりすると影響を受ける場合があるため、Wi-Fi-ルータとパソコンの位置を変えることで電波状況が改善する場合もあります。
- 一般的には、インターネットへの接続を無線接続から有線接続へ変更することでインターネットへの接続速度は改善します。
- Web 会議で不必要な動画や画面共有などはオフにする。
- 家庭内 LAN 内の通信量を減らす。特に家族が動画サービスなどを視聴している場合、視聴時間をずらしてもらうことができれば、インターネットへの接続速度が改善する

かもしれません。

- より高速なインターネット接続サービスへ変更する。なおどのようなインターネット接続サービスがあるかについては、インターネットサービスプロバイダに確認してください。

■ Web 会議の音声が通らない場合に他の Web 会議システムを確認する

Web 会議の音声が通らないトラブルは頻繁に発生します。

Web 会議の音声が通らない原因はたくさんあるため、ここでは対策の例を示します。

- Web 会議システムの音声設定を確認する
- マイクの設定を確認する
- Web 会議システムやパソコン自体の再起動などを試みる

直前に利用していた別の Web 会議システムにマイクが使用されている場合に音声が通らないことがあるため、終了した Web 会議システムは停止すると、Web 会議で音声が通る場合があります。

■ Web 会議のビデオとプライバシーを考える

Web 会議のビデオをオンにして顔を出すことでコミュニケーションが取りやすくなるほか、Web 参加者会議への参加者の確認がしやすいなどの理由で Web 会議ではビデオをオンにする運用をしているケースがあります。しかしながらプライバシーの観点から自分の顔や部屋を見せたくないという意見もあります。どのような Web 会議が適切であるかは一概にはいえませんが、参加者が納得して業務を進めやすい方法を採用するとよいでしょう。部屋を見せたくない場合には Web 会議の際にバーチャル背景を使用するなどの方法もあります。また、参加者の確認のためにビデオをオンにしているのであれば、他の手段で参加者の確認ができればビデオの強要はしないなども検討するとよいでしょう。

おわりに

新型コロナウイルスへの対応のため、リモートワークを余儀なくされた側面も否めませんが、これをきっかけに多くの企業でリモートワークが定着し、働き方が大きく変わると言われています。リモートワークは生産性を向上させる働き方改革のツールとして期待されていますが、業務の環境がオフィスから自宅にシフトすることから、自宅においてもきちんとしたセキュリティ対策を行うことが重要となります。

本リファレンスガイドが自宅のセキュリティ対策向上の一助となり、リモートワークの普及を下支え出来れば幸いです。