

オフィス内外で活動するときに 組織の安全性を維持する方法

自宅で仕事する場合でも、オフィスで仕事する場合でも、組織のセキュリティを確保することは最優先事項の1つです。これらの2つの場所は全く異なるように思われるかもしれませんが、オフィスと自宅では共通する注意点があります。ここでは、いくつかの重要なサイバーセキュリティのルールを紹介します。また、オフィスと自宅でこれらのルールを活用する方法を説明します。

安全なデバイスのみを使用する

- デバイスの安全性は、デバイスで実行されているアプリケーションに依存することを忘れないでください。IT部門に確認せずに、アプリケーションやプラグインをインストールしないでください。
- 業務用のデバイスは、業務のためだけに使用してください。個人のコンピューターを業務に使用する場合、ユーザー名とパスワードがそれぞれ異なる別のユーザーアカウントを作成することをお勧めします。
- オフィスのネットワークセキュリティは、通常、IT部門が管理していますが、自宅のネットワークは自分で管理しなければならないことが多くあります。自宅のインターネット接続を安全に維持するために、ルーターに複雑なパスワードを使用してください。組織が仮想プライベートネットワーク（VPN）へのアクセスを提供している場合は、VPNに接続してください。

物理的な作業環境を保護する

- オフィスでは、ピギーバックと共連れ侵入に注意してください。ピギーバックとは、通行許可書やエントリコードを持たないユーザーが、別の誰かに続いて保護区域に入ることを意味します。共連れ侵入とは、侵入口で誰かが通過するのを待って、ドアが開いている間にその人物に続いて保護区域に出入りする行為です。見知らぬ人であれば、疑いをもって、恐れずに身分証明書の提示を求めてください。
- 自宅では、誰にも画面を見られることなく仕事ができる、プライベートで快適な作業空間を確保してください。すべての機密情報は、配偶者や子供、友人など、権限のない人に見られることがないようにしてください。
- 机を離れるときは、必ずパソコンをロックしてください。コンピュータのロックを解除したままにしておくと、誰でもそのコンピュータを使用して機密データにアクセスしたり、ログイン情報を盗んだり、マルウェアをインストールしたりすることができます。

クリックする前に考える

- 不審なメールのリンクをクリックしたり、添付ファイルをダウンロードしたりしないでください。送信者が組織の一員であるように見える場合であっても、メールアドレスが偽装されている恐れがあります。
- メールでアカウントやオンラインサービスへのログインを求められた場合、ブラウザに移動してそのサービスにアクセスします。メールのリンクは決してクリックしないでください。メールのリンクではなく、サイトに直接アクセスすれば、偽装されたサイトではなく、正規のサイトにログインしていることを確認できます。
- 疑わしい場合は、メールの送信者に電話して、リクエスト、リンク、添付ファイルが正当なものかどうかを確認してください。メールに記載されている電話番号は犯罪者につながる恐れがありますので、その番号に通話しないでください。

