テレワークで留意すべき情報セキュリティ対策とは

このところ、テレワークの導入が急速に進んでいます。インターネットに常時接続するため、セキュリティには十分な注意が必要です。留意すべきポイントを紹介します。

ライター　川本鉄馬

世界中から狙われる脆弱なテレワーク環境

テレワークでの仕事は、ＰＣとインターネットの接続環境が前提となります。

この点では、かつての「モバイルワーク」と同じです。しかしテレワークは、モバイルワークと大きく異なる部分があります。それは利用する人の違いです（**図表１**）。

モバイルワークは、外回りが多い営業職や経営層など、限られた人を対象としていました。そのため、どんな用途に利用するかが明白でした。

たとえば、営業職の場合は客先での打合せの合間に、会社支給のＰＣで見積書や提案書をつくるなど、その使われ方が一定の範囲のなかにありました。

これに対してテレワークは、会社にいる大部分の従業員を対象としています。

そのため、利用環境が幅広く、全体をきちんと管理するのが難しくなります。この状態はセキュリティ面から見ると、かなり危険なことがわかります。

最近テレワークが普及している背景には新型コロナの流行があります。インターネット上では、このような社会的なストレスがある時期に、それに付け込んだフィッシング行為が増える傾向があります（**図表２**）。

実際、このコロナ禍では、ＷＨＯや保健所といった、コロナに関連したキーワードを件名に入れた詐欺メールが増えています。

また、「ｃｏｒｏｎａ」や「ＣＯＶＩＤ」などを含むドメインや証明書の登録が増加中であることが確認されています。

セキュリティの専門家は、この状況を「将来の詐欺や攻撃に向け

図表１　テレワークとは

た準備」と説明します。

急激に普及するテレワーク環境で心配されるのは、このような状況に傾いているインターネットを、仕事のために利用したり、脅威に慣れていない社員が使ったりしなければならないことです。

テレワークは、インターネットなしでは機能しません。安全なテレワーク環境を実現するには、しっかりとしたセキュリティ対策が重要となります。

セキュリティ対策の第一歩はエンドポイントの強化

テレワークで懸念されるセキュリティ被害として代表的なものに情報の漏洩があります。

また、社内のファイルやデータを暗号化して使用不能にし、それを解除するための身代金を要求する被害も報告されています。

これらの被害を引き起こすサイバー攻撃には、一定のパターンがあります（**図表3**）。

たとえば、怪しげなＷｅｂサイトにアクセスしたことでＰＣがウイルス感染することがあります。また、メールに添付されたファイルを開くことでウイルスがＰＣに入り込むこともあります。

このようにＰＣ内に侵入したウイルスは、さらに別のウイルスを呼び込むために外部のサーバにアクセスしたり、ＰＣの制御を外部から行なうために秘密のドアをつくったりします。このように1台のＰＣが汚染されると、そのＰＣを踏み台にして被害が広がることになります。

では、この被害を止めるのに必要なことは何でしょうか。

そのキーワードとなるのが、「エンドポイント」の強化です。

この場合のエンドポイントは、ユーザーが使うＰＣやスマートホン、会社のサーバなどを指します。テレワークの場合は特にＰＣが重要で、ここをしっかりガードすることがセキュリティ対策の第一歩となります。

ＰＣに対しては、ＯＳのバージョンを常に最新に保つことが必須となります。

さらに、未知のウイルスにも対応した〝次世代型〟のアンチウイルスソフトをインストールします。これでＰＣのウイルス感染はある程度回避できます。

問題なのは、最近のウイルスが非常に巧妙化しているということです。一般的なアンチウイルスソフトではなく〝次世代型〟としたのはそのためです。

旧来型のアンチウイルスソフトは、巧妙化する攻撃に十分対処できません。

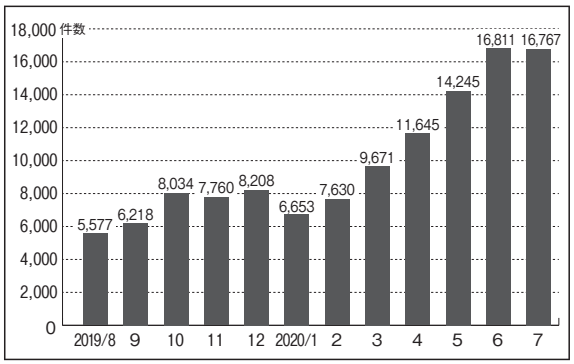
ウイルス側が高度化を続ける以上、防御にも最新のウイルス対策ソフトが必要となります。

そのＰＣは安全なのか

テレワークでは、会社から支給されたＰＣのほか、社員が個人所有するＰＣが使われることもあります。この場合、その管理状況が問われます。

会社が支給するＰＣでは、ＯＳやアンチウイルスソフトなど、セ

図表２　フィッシング報告件数



出典：フィッシング対策協議会「2020/07 フィッシング報告状況」

図表３　情報セキュリティの10大脅威

個人	順位	組織
スマホ決済の不正利用	1位	標的型攻撃による機密情報の窃取
フィッシングによる個人情報の詐取	2位	内部不正による情報漏えい
クレジットカード情報の不正利用	3位	ビジネスメール詐欺による金銭被害
インターネットバンキングの不正利用	4位	サプライチェーンの弱点を悪用した攻撃
メールやSMS等を使った脅迫・詐欺の手口による金銭要求	5位	ランサムウェアによる被害
不正アプリによるスマートフォン利用者への被害	6位	予期せぬIT基盤の障害に伴う業務停止
ネット上の誹謗・中傷・デマ	7位	不注意による情報漏えい（規則は遵守）
インターネット上のサービスへの不正ログイン	8位	インターネット上のサービスからの個人情報の窃取
偽警告によるインターネット詐欺	9位	IoT機器の不正利用
インターネット上のサービスからの個人情報の窃取	10位	サービス妨害攻撃によるサービスの停止

出典：情報処理推進機構「情報セキュリティ10大脅威 2020」

キュリティ関連の状態がある程度把握できます。

しかし、個人所有のPCはその限りではありません。

さらに、1台のPCを家族が共用している場合も問題です。たとえユーザーを切り替えて使用していたとしても、そのPCで誰がどんなWebサイトにアクセスし、どんなメールを受信したかは不明です。

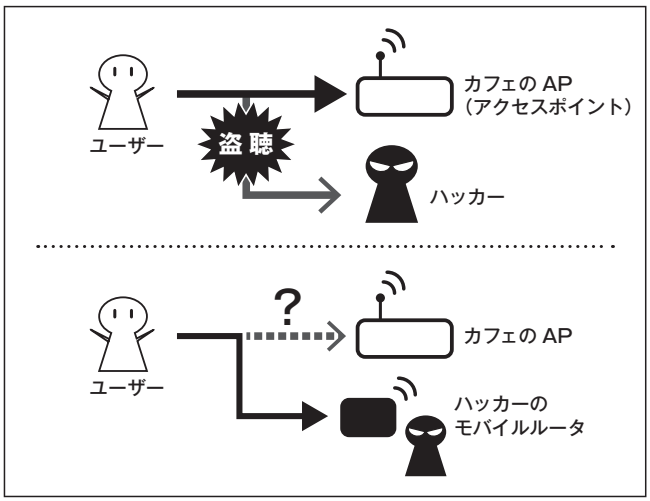
このような場合、ハードウェア全体のセキュリティは確保できません。もし可能であれば、このような家族の共用PCはテレワークで使うべきではありません。

また、自分だけしか使わないPCの場合でも、テレワークを開始する前に最新のアンチウイルスソフトで全体をスキャンし、ウイルスの感染がないことを確認すべきでしょう。

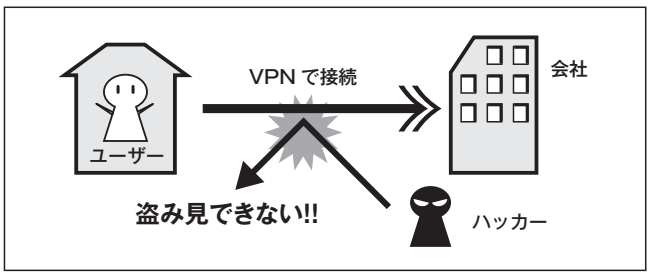
最近ではBYOD（Bring Your Own Deviceの略）といって、個人所有のPCを会社で使うことを推奨する企業もあります。

しかしそれは、社内という安全な環境で使うことが前提になります。テレワークのような環境では、PCの安全性を高めるための仕組みや行動ポリシーをつくる必要もありそうです。

図表4　カフェのWi-Fiの危険性



図表5　VPNでデータを暗号化



通信の安全性を高めるVPN

安全なエンドポイントの実現と同様、テレワークでは通信回線の安全性を高めることも必要です。

オフィス内での業務は、社内ネットワークという閉じられた範囲で行なわれます。

しかし、テレワークでは誰が使っているか管理できないインターネットを使います。このため、インターネット上でデータが盗み見られたり盗まれたりしないための施策が必要になります。

特に、カフェなどに設置されたWi-Fiは要注意です。多くの場合、カフェのWi-Fiは暗号化されていません。

また、店内にいるハッカーが情報を抜き取るためにモバイルルータを持ち込んでいる可能性もあります。カフェのものだと思って接続したアクセスポイントが実はハッカーのものなら、そこでやり取りされる情報はハッカーに筒抜けになります（**図表4**）。これは、自宅から会社にアクセスする場合も同様にハッカーに盗み見られる可能性があります。

インターネットを利用した通信で安全性を高めるには、たとえばVPNの利用が手軽です。VPNは、エンドポイント間の通信をカプセル化します。これによって、第三者による情報の盗み見や改ざんなどを防止します（**図表5**）。

VPNの利用に際しては、会社のネットワークとインターネット回線の接続点にVPNルータを設置します。またPC側ではVPN通信を実現する設定を行ないます。ビジネスで一般的に使われているWindows10には、標準でVPN通信を可能にする機能が用意されています。

VPNの弱点は、多くのユーザーが通信を行なうとレスポンスが低下するということです。

すでにVPNを導入している企業でも、すべての社員が同時に接続して快適に作業できるVPN環境を用意しているところはないはずです。

社内のサーバにあるファイルや情報を参照するには、VPNを利用しますが、それ以外ではインターネット接続を切断したり、VPN以外で安全なテレワークを実現

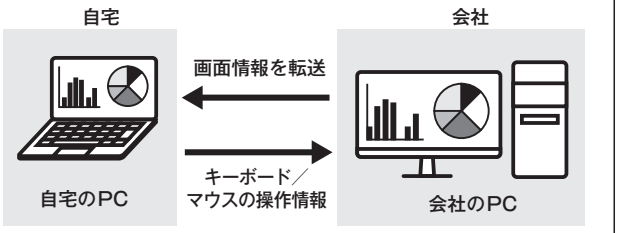
する仕組みを使うことが多いようです。

保存しなければ情報漏洩の心配はいらない

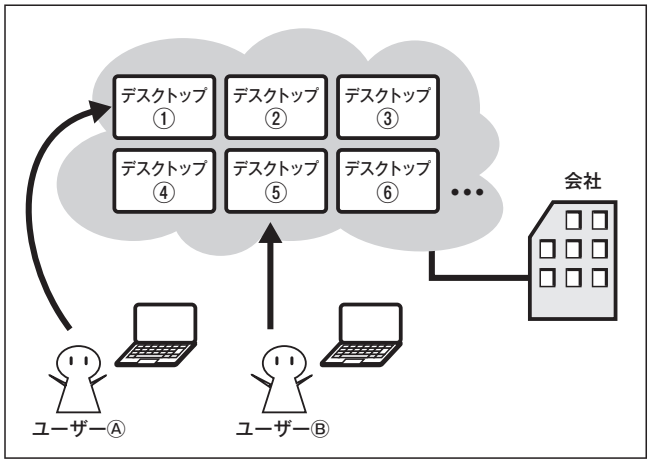
テレワーク環境での仕事では、重要な情報が外部に漏洩する懸念が消えません。

しかし、これにはすでに有効なソリューションが用意されています。いくつかの方法がありますが、いずれも〝PC上にデータを保存しない〟というアプローチを取っているのが特徴です。

図表6　会社のPCに自宅PCからリモートアクセス



図表7　仮想デスクトップ



PCにデータを保存しなければ、PCがウイルスに感染しようがPCそのものを紛失しようが情報は漏洩しません。

もちろん、USBメモリなどへデータをコピーするのもダメです。情報はあくまで社内や厳格に管理されたクラウド上に置き、PCはそれを参照・編集するだけに徹することでPCからの情報漏洩は回避できます。

PC上にデータを置かずにテレワークを行なう方法として手軽なのは、会社にあるPCに対し自宅のPCからリモート接続して仕事を行なう方法です。

データは会社のPC上、あるいは会社が管理するサーバから移動させません。データの編集を行なうのは会社のPCで、その操作を自宅から遠隔で行なうのがリモート接続を利用した仕事のやり方です（**図表6**）。

この方法では、データ本体がインターネット上を流れません。インターネット上を流れるのは、会社のPCを操作している画面情報とキーボードやマウスの操作情報だけです。

この方法は、Windowsに標準の機能だけで実現できるのも利点です。社内にあるPCへの接続時に2段階認証などを利用すれば、かなり有効なセキュリティ対策になります。

このほか、クラウド上に仮想的なWindowsの環境を構築する方法もあります。マイクロソフトには、同社のクラウドサービス上で稼働する仮想デスクトップ環境であるWVD（Windows Virtual Desktop）があります。

また、ほかの会社からも同様のソリューションが提供されています（**図表7**）。

これらの仮想環境でも、社員が操作するPC上にはデータを置きません。また、Windowsのデスクトップ環境そのものがクラウド上にありますから、OSやアプリに対するセキュリティも確保されることになります。

安全なテレワークを実現するソリューションが加速中

コロナ禍の影響もあり急速に普及が進むテレワークですが、それによって得られるメリットは少なくありません。

たとえば、テレワークの導入で出社する社員が減り、オフィスのスペースを見直す企業が出始めています。また、社員側でも通勤の必要がなくなり、時間的な余裕や柔軟な働き方が実現しつつあります。このようななか、セキュリティを担保しつつ快適なテレワークを実現するソリューションも各社から発表されています。

現時点ではスタートしたばかりのテレワークですが、この効率的な働き方はコロナが収束した後も継続されると思われます。そんな将来に向け、そろそろソリューションの選択や行動規範を定める必要があるのかも知れません。▲

かわもと　てつま　広告業界を経てフリーランスのライターへ。現在、クラウド、基幹系システム、建築関係を中心に取材・執筆活動中。