法的リスクマネジメント講座 第84回

テレワーク時代の法的リスクとは②
サイバーリスク、安全配慮義務違反、リモート・ハラスメント

長谷川俊明法律事務所
弁護士
長谷川 俊明

はじめに

2021年1月5日、政府の新型コロナウイルス対策分科会は、首都圏の感染状況が最も深刻なレベルに達しているとし、緊急事態宣言が出た場合に実施すべき具体策として、飲食店のさらなる営業時間短縮や不要不急の外出自粛、イベント開催要件の強化、テレワークの徹底などを求めました。

人同士の接触を極力減らすべきとの考えから、「テレワークの徹底」を以前にも増して、具体的対策として重視しているのがわかります。

テレワークとリスク管理

テレワークには、業務の生産性を上げるメリットの反面、やり方次第ではかえって生産性を下げるデメリットが指摘されています。

また、テレワークは社屋内が勤務場所ではなく、各社員の自宅などリモートに分散して勤務を行う体制です。そこで、大震災などで社屋や工場が被害を受け、当分の間、勤務ができなくなっても、テレワークの各拠点で対象の事業を継続できます。

リスクの分散は、リスク管理上の鉄則です。危機対応に向けたBCP(事業継続計画) の内容にテレワークを入れるのは、事業拠点の分散に役立つからです。

反面、テレワークによる勤務場所の拡散は、勤務を行うのに必要な秘密情報の大量“ネット流出”リスクを増大させます。コンピュータ・ネットワークは、接続拠点を多くし横にも縦にも広げれば広げるほど、サイバー攻撃などへの脆弱性を増します。

法的リスクとしては、前号でも紹介したコンプライアンスリスクに加え、サイバー攻撃による個人データの流出リスクなども考えられます。

リスク管理で最も重要なのは、リスクの洗い出しです。今回、テレワークにおけるリスクの洗い出し・想定は、普段から何に注意し、具体的にどう行えばよいかを考えてみましょう。

サイバーセキュリティの重要性

2020年8月下旬、国内の主要企業38社が不正アクセスを受け、テレワークに欠かせないリモート接続の暗証番号が流出したと報道がされました。

漏洩したのは、VPN(仮想施設網) と呼ばれる接続サービスの利用情報で、VPNは通信データを暗号化し、会社の外から仕事用のシステムに接続することで、専用線の敷設よりも低いコストで済むため、テレワーク・在宅勤務によく使われます。

ここで懸念されたリスクは、流出した情報が悪意ある第三者の手に渡れば、VPNを介して会社の基幹システムへ侵入されかねないことです。VPNサービスを提供するアメリカの専門企業は、自ら、2019年4月に「脆弱性」についての情報を公表し、修正プログラムも公開していましたが、必要な対策を取らない企業が多く、そこをハッカーに突かれ、情報を取られてしまいました。

大地震で工場が倒壊したメーカーも、製造拠点を他に分散して保有していれば、縮小しながらでも事業を継続でき、事業拠点の分散は、テレワークによっても実現できます。テレワークの活用による事業中断リスクの分散は、企業のシステムと従業員が使う端末をネットワークでつなぐことで可能になります。反面、拠点数が増し脆弱性を増すネットワークの安全をどう守るかが課題になります。

一般に、コンピュータ・ネットワークが「くもの巣(web)状」に広がり、つなぐ端末など拠点の数が多くなればなるほど、ネットワークの“脆弱性”が増します。(図1)テレワークの場合、従業員が使う端末は、いわゆるセキュリティレベルが極端に低いことがあり狙われやすいのです。

テレワークによるセキュリティレベル向上の目的は、ネットワークを破られ会社の秘密情報を盗み出されることなどの防止です。そのためには、会社のシステムへセキュリティレベルの低いIT 端末を接続しない、させないことが重要です。もし社内ネットワークへの接続を許すとしたら、原則として私用端末は使わせず、セキュリティ対策をしっかり施したIT 端末の貸与などによるべきです。

さらに会社システムに接続しているのが、アクセスする権限を有する「本人」なのかどうかを認証する方法の高度化が、今は課題としては大きくなっています。

詳しくは、総務省発行「中小企業担当者向けテレワークセキュリティの手引き(チェックリスト)」[※1]をご活用ください。

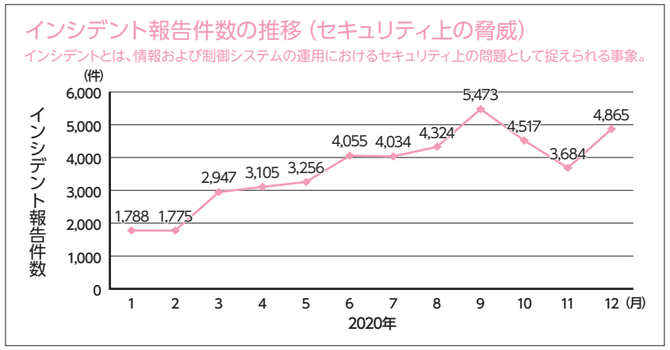
なお、もしセキュリティ対策を怠ったため、サイバー攻撃で社内システムから大切な顧客や取引先の情報を盗まれたとします。会社は、顧客や取引先から流出した秘密情報を乱用されるなどして生じた損害につき、賠償請求を受けかねません。

また、攻撃者は流出情報をいわば人質に取り、多額の“身代金”を要求してくることがあります。要求に応えて身代金を支払うと、その分、会社に与えた損害賠償を求める株主代表訴訟を会社の役員個人宛に起こすことがあり、十分に注意が必要です。

テレワークにおける安全配慮義務

企業(雇用主) は、労働基準法に従い、新型コロナウイルス感染症についても、従業員が安心して安全に働けるように職場の環境を整えなくてはなりません。

図1



出典:一般社団法人JPCERTコーディネーションセンター(2021年1月21日)

ただ、職場は安全でなくてはならないのですが、在宅勤務を認めるとしても、社員の自宅の環境が社員ごとに異なることで、会社のオフィスより安全とは限りません。実際に、テレワークで上司や同僚とのコミュニケーションがうまく取れず、自宅にほとんどこもりっきりの状態で、メンタルヘルスを害する社員が増加しています。

今後は、従来とは異なる感覚で、日頃から心身の労働安全衛生を確保するためコミュニケーションの円滑化に努めたり、具体的に手指や室内の消毒液などの購入費支援として手当の支給もあり得るかと思われます。

さらに、社員のテレワーク勤務中における病気やけがは、場合によって「労災」の対象になることもありますので、会社としては緊急時の「連絡網」整備などに万全の体制を築くべきです。

テレワークにおけるリモート・ハラスメント

在宅勤務者に対しては、上司からの連絡がつい素っ気ない乱暴な内容になりがちです。場合によっては、ハラスメントの一形態であるリモート・ハラスメント(リモハラ) と認定されたり、最悪の場合に訴訟となる恐れがあります。

メール等での指示の出し方について、相手の立場を無視するようなコミュニケーション不足に陥らないよう、詳しい運用マニュアルを用意し、それに沿って節度あるテレワークを行うのが良いでしょう。

また、自宅からのWeb会議 (多数の方が参加する場合もあり)では、自宅内の映像・生活音、本人の服装などが垣間見える場合もあり、公私が混在しがちです。会議参加者の不用意な言動によって、訴訟ともなり得るプライバシーの侵害やセクハラ・パワハラとならないよう、節度あるコミュニケーションを心掛ける必要があります。

以下、筆者が簡易的なリスクチェック表を作成しましたので、社内のリスク実態の洗い出しにご活用ください。

リモート・ハラスメントに関してのチェック表

1	テレワークによる在宅勤務者とのコミュニケーションは、メールやチャットによることも多く、つい乱暴でハラスメント的な差別内容になっていないか。	
2	メールで仕事上の指示を出す際は、一方的で説明不足の内容にならないようにし、必要に応じ電話によるフォローなどをしているか。	
3	Web会議においては、在宅勤務者の自宅や居室の様子、服装、髪型などについて、ことさらに不必要なコメントをしたりしていないか。	
4	Web会議での司会者は、発言者が、例えば上司からの発言だけに片寄らないように、公平性に配慮をしているか。	
5	Web 会議中に、子供の泣き声、電話の呼び出し音など、自宅では完全に遮断できない“生活音”につき、必要以上に苦情を言ったりしていないか。	

安全配慮義務に関してのチェック表

1	テレワークを実施することが、従業員が安全・安心に働ける職場づくり (労働基準法の順守) の一環であることを、会社として認識・理解しているか。	
2	テレワークで在宅勤務を認める場合、作業環境の「安全性」について、必要なアドバイスを行っているか。	
3	テレワーク勤務者のストレスチェックは実施しているか。	
4	会社は、テレワーク勤務者の労働安全衛生 (ストレスの軽減、長時間労働の防止など) を確保し改善するために、必要な措置を講じているか。	
5	テレワーク勤務者が、体調不良や情報機器の故障などの緊急事態発生時における連絡方法や連絡先は、予め明らかになっているか。	

※1 中小企業担当者向けテレワークセキュリティの手引き(チェックリスト) https://www.soumu.go.jp/main_content/000706649.pdf 参照