リモートワークとセキュリティポリシー

リモートワークで再確認が必要なセキュリティポイント

- VPN での接続先の IP 制限
- 共有ファイルのアクセス権限
- 使用デバイス（モバイル端末、USB、プリンター）の制限
- 使用可能場所の制限
- リモートワーク対象 PC 資産の状況把握
- 使用可能アプリの対象確認
- アンチウィルス・パターンファイルアップデート
- OS や使用アプリのアップデート
- 保管場所、画面ロックのポリシー
- パスワード記憶機能や、クッキーの使用制限
- リモートワークの通信ログ取得
- 出社、移動時の PC の取り扱い

感染症拡大を阻止するため、政府主導で企業や団体組織に対してテレワークである在宅勤務が推奨されています。
今回の緊急事態宣言を機に、大急ぎで社員を可能な限り在宅勤務にさせる企業が増えてきましたが、自宅からのリモートワークとなるとセキュリティリスクが増すため、今一度セキュリティポリシーを再確認する必要があります。
在宅の場合、多くはインターネット経由で会社にリモートアクセスするわけですが、セキュリティを考慮すれば VPN 等で暗号化して専用線のように使用できるようにしないと、データが漏えいするリスクが極端に高まります。
当然のことながら、VPN 経由でしか会社のネットワークに侵入できないようにするわけですが、その際、実際にテレワークする人だけに使用限定して、申請および承認された人が使用する PC の IP のみの設定になっていることが大切です。そして、ファイルサーバ上の共有ファイルは、本来権限がない人がアクセスできないようになっているか再確認が必要です。
社内で閲覧が可能だったファイルは、リモートであれば情報漏えいの危険が増します。
リモートアクセスする方法によっては、会社支給の PC が間に合わず、個人所有の PC を許可する場合も想定されます。
VPN 接続するネットワーク元は、個人の Wi-Fi であったりすると、そのネットワーク上に個人所有のプリンターやリムーバルディスクの接続も考えられ管理が必要です。そして、在宅はストレスが溜まるからといって、コワーキングスペースなどに出かけて仕事をするような人がいては、第三者に見られるリスクもあるため使用場所も制限すべきです。
その使用 PC については、PC 資産管理状況が把握できることが必要です。Web 会議用アプリなど、新規に導入が必要な場合もあるでしょうから、どのアプリは会社として導入してよいのかを徹底していないと、他の人の目がないからと、不必要で危険なアプリをダウンロードしてしまう可能性もあります。
また、会社のネット環境にくらべ、速度が遅くなるケースが多いので忘れがちですが、脆弱性を無くすためにも、アンチウィルスソフトのパターンファイルや、OS などは、常に最新にアップデートしなければなりません。家には家族を含め第三者がいる場合もあるため、PC を使用されないよう保管場所には気を付けて、画面ロックのパスワード設定やクッキーの使用制限は必須です。安心して運用するためにも、リモートワークのログ取得は重要であり、出社時の PC の持ち運びについても、事故が無いよう気をつけなければいけません。
テレワークが広がりをみせる今だからこそ、セキュリティポリシーは最良のものに更新されるべきです。