＜これだけは知っておきたい＞　テレワークにおける情報セキュリティ リスクとその対策

SOMPOリスクマネジメント株式会社

テレワークにおける情報セキュリティリスク

■ 情報セキュリティに関わるインシデントの脅威は、「外部からの脅威」と「内部からの脅威」に分類できます。テレワーク環境でも会社ルールに則った情報の取り扱いを心がけてください。

外部からの脅威 （サイバー攻撃等による脅威）	内部からの脅威 （社員の故意・過失等による脅威）
標的型攻撃（マルウェア等）	不正な持ち出し
不特定多数を狙った攻撃（フィッシング詐欺等）	不正な操作（システム誤操作・メール誤送信）
不正アクセス	ポリシー違反
改ざん	改ざん
DDoS攻撃	システム制御不備
盗聴・盗難	盗難・紛失
その他（停電・通信障害等）	その他（物理的破損・破壊等）

テレワークにおいて注意すべきサイバー攻撃

■ テレワークの導入により、企業のITシステムや重要情報がマルウェア感染や不正アクセスなど、外部からの脅威に晒されやすくなります。普段、社内で業務をしているとき以上にセキュリティ意識を高めていただくことが大切です。

なりすましメールによる攻撃

テレワークではメールの利用が大きく増加します。攻撃者は、標的型攻撃メールやビジネスメール詐欺、フィッシング詐欺など、巧妙に偽装したメールによる攻撃を仕掛けてきます。

自宅ネットワークの脆弱性を狙った攻撃

私用パソコンや自宅ネットワークのセキュリティが十分でない場合、その脆弱性を突いた攻撃による情報漏えいやマルウェア感染等への注意が必要となります。

認証システムを狙った攻撃

テレワークの環境は万全ではないため、IDやパスワード等が窃取されるリスクが高まります。認証システムを狙った攻撃や、社員になりすました不正アクセス等への対策が必要となります。

サイバー攻撃への対策

■ 基本的なセキュリティ対策がしっかりと実施されてることが重要です。まず第一にここを確認しましょう。次に企業の実情に応じた対策を実施しましょう。

【自宅でのテレワークの場合】 ～個人所有のパソコンを利用する際の主な注意点～

① ウイルス対策ソフトの導入。
② OS、ブラウザ、ウイルス対策ソフト等のアップデート。
③ サポート終了OSに対するサポート中OSへのバージョンアップ。
④ 複数人（家族等）共用パソコンでは仕事の情報をPC内に保存しない。
⑤ 容易に推測できないパスワードの利用。

【自宅以外でのテレワークの場合】 ～不特定多数の中で仕事をする際の主な注意点～

① 不特定多数が利用するパソコンの業務使用は避けること。
② フリーWi-Fiの使用は極力避けること。
③ 情報の盗み見リスク、パソコン紛失・盗難への対処。
・ショルダーハッキング（後ろから盗み見）されない場所に座る。
・パソコンに「のぞき見防止フィルター」を付ける。
・離席する際は、パソコンは一旦カバンにしまうか携行する、もしくはパソコンを閉じ、その上にノートや本などを置いておくなど、ちょっとしたことも大切です。

■ 情報事故発生時の対処を確認しておきましょう。事故発生時の報告経路は確実に整備しておきましょう。また、個人所有のパソコンを利用中にウイルス感染した場合はどうするか、などテレワークで想定される環境・状況を考慮した対応を優先することも大切です。

■ 当社では、比較的導入・運用負荷が低く、新型コロナウイルスの影響下においてもご利用いただきやすい様々なセキュリティサービスをご提供しています。

IRONSCALES　：SaaS型アンチフィッシング
DEEP INSTINCT　：ディープラーニングを用いた次世代型マルウェア対策
SOMPO SHERIFF　：パソコンの監視・分析・駆除までをオールインワンで提供

内部からの脅威への対策

■ テレワークでは、従業員に起因するパソコンの紛失や盗難、許可されていないパソコンからの社内サーバーへのアクセス、許可されていないサービスの利用などによる情報漏えいなど、「内部からの脅威」によるインシデントにも注意が必要です。

■ テレワーク導入前の段階では、情報セキュリティポリシーや就業規則といった各種社内規定の整備およびその内容をテレワーク勤務者へ認知・浸透させることが重要となります。導入後の対策としては、監査目的で収集しているパソコンのログデータ等を平時から分析・活用し、「リスクの即時検知・対応」と「就業状況を可視化」していくことによって、リスクを低減していくことが可能となります。

■ 当社では、企業内のログデータや管理情報を解析し、重大なインシデントの発生を未然に防ぐサービスをご提供し、企業のリスク検知業務の効率化をサポートしています。

Internal Risk Intelligence　：内部脅威検知サービス

【お問い合わせ先】SOMPOリスクマネジメント/サイバーセキュリティ事業本部　E-Mail：cyber@sompo-rc.co.jp