2020 年 6 月 16 日

サービス＆セキュリティ株式会社 e-Gate センター

新型コロナウイルス感染症緊急事態解除宣言後のセキュリティリスク

1. 概要

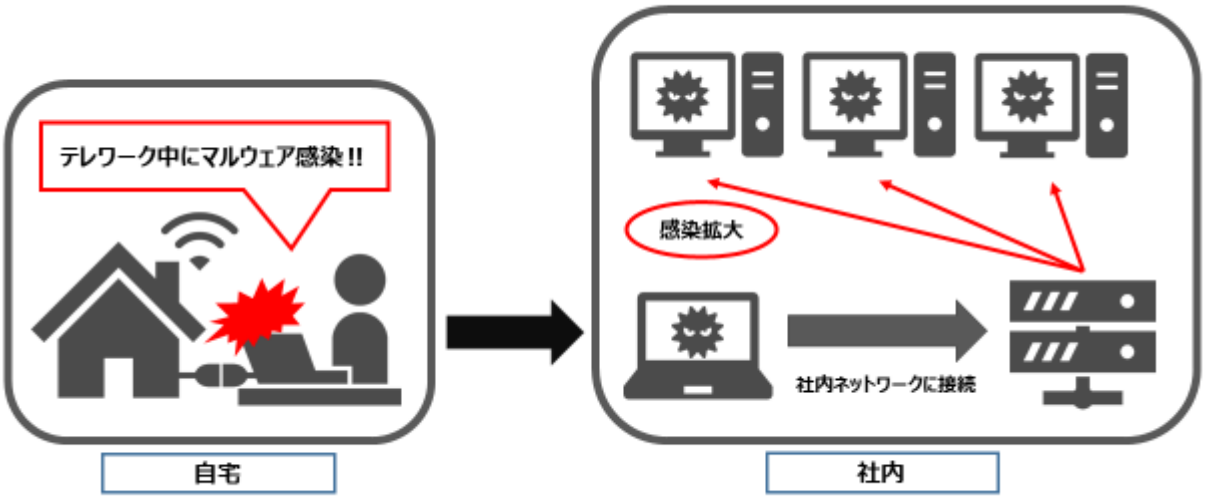
政府より新型コロナウイルス感染症の緊急事態宣言が解除され、テレワーク(在宅勤務)での業務形態から通常のオフィス勤務への業務形態に戻す企業が増えて参りました。しかし、テレワークで使用していた端末等を企業・組織内のネットワークに戻す際や、オフィス勤務に戻り、停止されていたシステムを稼働させる際にセキュリティリスクが存在することをご存知でしょうか。そこで本稿では、コロナ禍で急激に変化した”新常態”の働き方でオフィス勤務に戻る際のセキュリティリスクと対策について紹介いたします。

2. オフィス勤務に戻る際のリスク

テレワークからオフィス勤務に戻る際には、潜在的なセキュリティリスクが存在します。大きく２つのケースに分けてご紹介いたします。

2.1. 自宅からオフィスへ戻る際のリスク

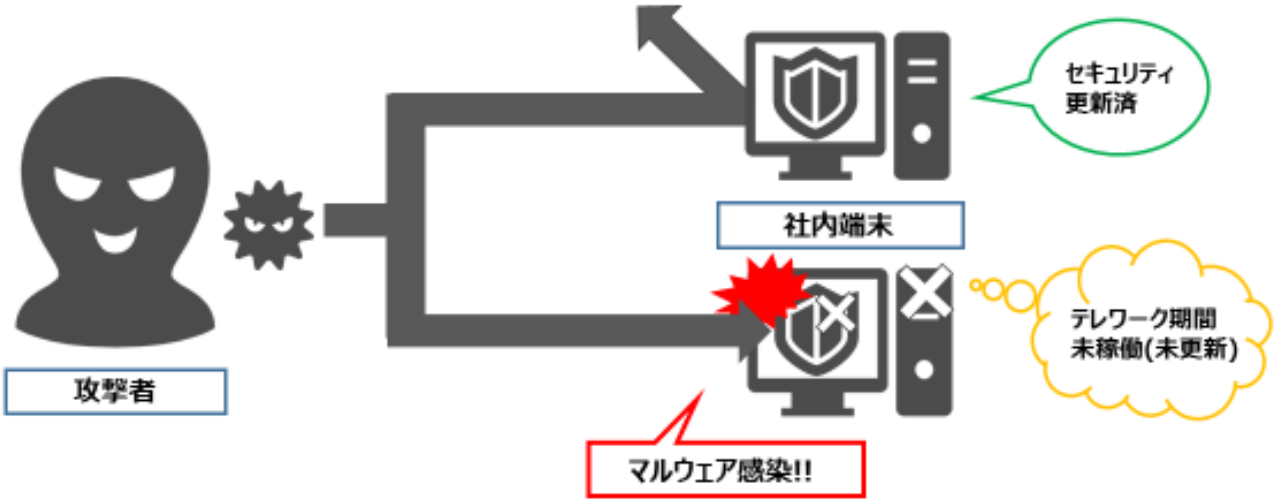
テレワークにて使用してきた端末等の多くは厳格なセキュリティ対策が取られているオフィスと比較するとセキュリティレベルが低い自宅のネットワーク環境に接続されていると思われます。万が一、テレワークの間にマルウェアに感染してしまって、気付かぬままオフィス勤務に戻って端末を企業内ネットワークに接続してしまうと、企業内ネットワーク全体にマルウェアを拡散してしまい、感染拡大、”クラスタ”が発生してしまうリスクが存在します。



【図 1】例：テレワーク中にマルウェア感染が発生したケース

2.2. 長期間停止されたオフィスで業務を開始する際のリスク

テレワークで利用する端末以外にもオフィス内には端末があり、長期間未稼働の場合があります。このような端末はセキュリティの更新が行われていない可能性が高いです。同様に一時的に停止、またはアップデートが行われていないサーバやシステムもあるかと思われます。さらにはテレワークの影響を受けた対応として一時的にシステム上の設定変更（例：通信の経路変更や許可制限等）が行われたまま放置されたシステムがあるかもしれません。このようなセキュリティや、システムの更新やシステムの設定変更が正しく戻されていないまま使用してしまうと最新のマルウェア等に感染してしまうリスクが存在します。



【図 2】例：セキュリティソフト未更新の感染ケース

3. 対策

前項のようなセキュリティリスクはもとのオフィス勤務に戻る前に以下の確認を行うことで、マルウェアの感染防止や被害の最小化が可能です。

3.1. テレワーク利用者

●自宅ネットワーク環境のセキュリティ対策を確認

最近の攻撃傾向として家庭用ルータが狙われるケースが多発しています。最新のソフトウェアが適用されているか、製品が初期設定のまま使用されていないかを確認してください。また、自宅ネットワーク内にある IoT 機器、個人用の端末も同様です。基本的なセキュリティ対策ができているか確認することで、自宅ネットワーク環境のセキュリティレベルを上げることができます。

●テレワーク用に持ち出した端末にマルウェア等が感染していないか確認

テレワークで利用した端末を社内ネットワークに接続する前にアンチウィルスソフトを用いて“フルスキャン”を行います。マルウェアに感染した端末からオフィス内の端末に感染が拡大することを防止できます。

3.2.オフィスの情報セキュリティ管理者

●オフィス内機器のセキュリティ対策が最新に更新されているか確認

サイバー攻撃の手法やマルウェア等は常に進化を続けている為、オフィス内の端末やサーバ等は常に最新のセキュリティ対策の状態である必要があります。オフィスでの業務を再開する前にシステムの最新アップデートや各種ソフトウェアの更新が行われているか確認してください。

●ソフトウェアを無許可でインストールされていないか確認

テレワーク勤務者が勝手な判断で本来インストールの許可が必要なソフトウェアを無許可でインストールしている可能性があります。安全性が確認できないソフトウェアにはセキュリティリスクが存在します。オフィス勤務に戻る前に、セキュリティ管理者がそのようなソフトウェアがないかを確認してください。

3.3 新常態に向けて

新型コロナウイルス対策の影響により、働き方が大きく変化してきています。これからも継続的にテレワークを行う企業は多く、継続した運用を行う場合には前述の確認だけではなく、恒久的な対策が必要となります。今後どのような対策が必要になるのかご紹介いたします。

●テレワーク時のネットワーク環境固定化

オフィスから Wi-Fi ルータ等の通信機器を支給することで、テレワーク時のネットワーク環境を固定化できます。その結果、セキュリティレベルが一定で信頼されたネットワーク環境でのテレワークが行えるようになります。

●セキュリティスキャンの自動化

テレワーク端末に予め決められた時間帯でのセキュリティスキャン実施設定を行うことで、自動で定期的なマルウェアの感染確認が行われるようになります。また、長期間稼働していない場合でも次回稼働時にセキュリティスキャンが行われるよう設定を行っておくことで、より安全な状態を保つことが可能です。

●ソフトウェアの制限化

テレワーク端末に対して管理者権限にてソフトウェアの制限をかけることにより、ソフトウェアのインストール自体を行えないように設定します。業務に必要なソフトウェアがある場合は事前にインストールしておくか、管理者に確認を行ってからインストールできるように制限することができます。

●セキュリティシステムの全体点検ルール化

テレワークや長期休暇でオフィスから長期間離れ、戻った時に必ずセキュリティの点検を行うようルール化します。セキュリティ対策が更新されているか、システム変更の戻し忘れが無いかをオフィス全体で点検実施することにより、より効果的なセキュリティ対策となります。

※ テレワークにおける対策については以下 URL でも紹介しております。ご参照ください。
『テレワーク(在宅勤務)におけるセキュリティリスクと対策について』
https://www.ssk-kan.co.jp/topics/?p=10829

4. 今後のテレワーク・セキュリティ

新型コロナウイルス感染症緊急事態宣言の解除後も第二波の可能性や新常態での働き方に多様化がすすみ、テレワークを実施する企業はこれからも増加していくと思われます。進化していく働き方と共に、新たなリスクも同時に増加していきます。

今後のテレワークが当たり前となる新常態を標準としたセキュリティ対策には、端末にセキュリティソフトを利用するだけでなく、ファイアウォールや IPS といったネットワークセキュリティ機器の導入をご検討ください。ネットワークセキュリティ機器を導入することにより、マルウェアや悪質な攻撃のふるまい等を検知して、攻撃者からの通信を遮断することが可能です。また、ネットワークセキュリティ機器が出力するログやネットワーク接続のアクセスログを監視・分析することで、怪しい送信者からの通信がないか、業務に不要な通信がないか等を確認することもできます。普段からセキュリティ対策の運用をオフィス全体で行う事が肝要です。

しかし、社内のシステム部門の体制だけでこれらの運用を行うには多くのコストがかかってしまい、対応が困難な場合があります。そのような場合は、外部の SOC（セキュリティオペレーションセンター）にネットワーク機器の運用をアウトソーシングするという手段があります。

6 章にて弊社 SOC の”e-Gate センター”についてご紹介しております。ぜひご覧ください。

5. 参考情報

・日本ネットワークセキュリティ協会(JNSA)

緊急事態宣言解除後のセキュリティ・チェックリスト

https://www.jnsa.org/telework_support/telework_security/index.html

・Think with Google

「テレワークを続けたい」のはどんな人？：3000 人に聞いた今・これからの働き方

https://www.thinkwithgoogle.com/intl/ja-jp/articles/interview/covid-19-8/

・トレンドマイクロ

テレワークから職場に戻るときにセキュリティの観点から注意すべきこと

https://www.is702.jp/news/3686/

・パーソル総合研究所

第三回・新型コロナウイルス対策によるテレワークへの影響に関する緊急調査

https://rc.persol-group.co.jp/news/202006110001.html

6. e-Gate のサービスについて

e-Gate のセキュリティ機器運用監視サービスでは、24 時間 365 日、リアルタイムでセキュリティログの有人監視を行っております。サイバー攻撃への対策としてセキュリティ機器を導入する場合、それらの機器の運用監視を行い、通信が攻撃かどうかの分析、判断をして、セキュリティインシデント発生時に適切に対処できるようにすることが重要です。“e-Gate“のセキュリティ監視サービスをご活用頂きますと、迅速なセキュリティインシデント対応が可能となります。

また、e-Gate の脆弱性診断サービスでは、お客様のシステムにて潜在する脆弱性を診断し、検出されたリスクへの対策をご提案させていただいております。

監視サービスや脆弱性診断サービスをご活用いただきますと、セキュリティインシデントの発生を予防、また発生時にも迅速な対処が可能なため、対策コストや被害を抑えることができます。

■総合セキュリティサービス 「e-Gate」

SSK（サービス＆セキュリティ株式会社）が 40 年以上に渡って築き上げてきた IT 運用のノウハウと、最新のメソッド、次世代 SOC“e-Gate センター“この 2 つを融合させることによりお客様の情報セキュリティ全体をトータルにサポートするのが SSK の“e-Gate”です。e-Gate センターを核として人材・運用監視・対策支援という 3 つのサービスを軸に全方位のセキュリティサービスを展開しています。

【参考 URL】

https://www.ssk-kan.co.jp/e-gate/

«お問合せ先»
サービス＆セキュリティ株式会社
〒150-0011
東京都渋谷区東 3 丁目 14 番 15 号 MO ビル 2F
TEL 03-3499-2077
FAX 03-5464-9977
sales@ssk-kan.co.jp