貴方の企業は大丈夫？クライアント PC をセキュアに保つテレワーク環境の切り札とは
―テレワーク PC の健全性を可視化する方法―

新型コロナウィルス感染症対策に伴う在宅勤務の広がりに伴い、在宅等社外で利用するクライアント PC が増えてきています。社外での利用は情報漏えいや端末のウィルス感染といったリスクが高まるので、社外 PC のセキュリティ状況の見える化が課題というご相談の声を多く耳にします。セキュリティポリシーを企業単位で定めても、実際の運用は社員に委ねざるを得ないシーンも多くあります。

当社では十数年にわたり IT 資産管理ツールをメインとした導入提案からシステム環境構築、保守運用サポートの他、セキュリティ対策商材の販売を行っております。今回このような現場の声をひろい、セキュリティポリシー判定の必要性についてまとめました。

内容

1．テレワーク PC の脅威

テレワーク時は、安全性の低いネットワークを介しているため、職場よりセキュリティレベルが低く、「OS、アプリケーション、ドライバなどに対して最新パッチが適用されていない」、「社内経由ではなく、直接インターネットの閲覧が可能な場合はマルウェアに感染してしまうリスクが高い」、「許可していないソフトウェアの導入」、「社内のセキュリティ設定に準拠されていない」など、従業員がテレワーク中に自社ポリシーに違反することによって、情報漏えいのリスクを発生させる可能性があります。社内よりもテレワークでは見えていない部分が多く存在することで、テレワーク PC の健全性の可視化が重要になり、それを実現するためにセキュリティポリシー判定が重要になります。

2．セキュリティポリシー判定とは

クライアント PC 側がアンチウィルスソフトやその他アプリケーションソフトを最新の状態にアップデートすることで適切に脆弱性を解消していれば、ウィルスの攻撃からのリスクは軽減するはずです。セキュリティ対策を強化している企業であれば、こうした対策をセキュリティポリシーとして明文化していることが多いです。しかし、企業としてのセキュリティポリシーを決め、社員にこれを守るよう教育しても、常に順守していなければ企業はリスクを抱えたままになります。社員の不注意や軽い気持ちが、セキュリティ上大きな問題を発生することになります。クライアント PC がウィルスに感染した後に社内ネットワークに接続し、内部から情報が漏えいしたなどの被害の発生リスクを軽減するためにも、セキュリティポリシー判定は有効な手段になります。

セキュリティポリシー判定は、クライアント PC を立ち上げログインした時点で、以下のような項目の検査が可能となります。

（一例）

・OS、アプリケーション、ドライバなどのセキュリティパッチが適用されているか、
・アンチウィルスソフトなどのパターンファイルは最新のものか
・アンチウィルスソフトのリアルタイムスキャンが無効になっていないか
・指定されたソフトウェアがインストールされているか
・使用禁止ソフトウェアがインストールされていないか
・スクリーンセーバー設定が OFF になっていないか

どのような項目を検査するのかは、企業のセキュリティポリシーによって柔軟に指定できる必要性があります。

3. なぜセキュリティポリシー判定が必要なのか

セキュリティリスクを軽減するには、クライアント PC のアンチウィルスソフトやその他セキュリティソフト、パッチ適用による脆弱性の排除といった複数のセキュリティ対策を確実に行う必要があります。パッチを適用し、アンチウィルスソフトやその他セキュリティソフトを導入し、強化していれば、ウィルス感染のリスクを軽減することが可能です。

にもかかわらず、セキュリティポリシー判定を必要とする理由には、企業内のクライアント PC のすべてが適切にパッチを適用しているかどうかまでを個々のパッチ単位で確認する必要があるため、システム管理者が即座に調べることはできないという課題があります。こうした状況に対して、セキュリティポリシー判定が導入されていれば、クライアント PC に対して最新パッチが適用しているかどうかを一目で確認することができます。従業員もセキュリティポリシー判定の結果を確認することでセキュリティ意識が高まり、「利便性を優先するためにセキュリティ対策を放置している」、「仕事が忙しくて更新する時間がない」といった理由でリスクが潜在化しているクライアント PC のセキュリティポリシー違反を軽減することができます。

4. 出社する際に見落としてはいけないリスクと対策

従業員がテレワーク時に使用しているクライアント PC を職場に持ち込む際には、職場での使用を再開する前にクライアント PC の健全性を担保する必要があります。直近のテレワークの際にセキュリティポリシー判定を実施し、セキュリティポリシー違反が無いか以下の項目などを確認します。

・OS、アプリケーション、ドライバに最新のパッチが適用されていること

・クライアント PC 内にマルウェアが存在せず、侵害された兆候がないこと

・セキュリティポリシー判定にて違反している項目がないこと

問題が見つかった場合は、是正した後にクライアント PC を社内 LAN に接続することを許可するなどの対策が必要になります。

5．シンプルな機能で導入しやすい

検疫システムは、ネットワークの構成やセキュリティポリシーの考え方、導入後の運用方法などを考慮しながら製品を選択する必要があるため、非常に導入に時間がかかり、コストもかかります。それに比べ、セキュリティポリシー判定は、ネットワークの構成を変更することなく、クライアント PC にエージェントを導入するだけで比較的安価に実現が可能です。また検疫システムだと「検査」、「隔離」、「治癒」の 3 つのステップがあり、導入後の運用方法などを決めるのに時間がかかりますが、セキュリティポリシー判定は、「検査」のみシンプルな機能になるため、導入がしやすく、従業員へのセキュリティポリシー違反の抑止、および、是正を促すことが可能です。

6．マネージドサービスの利用

セキュリティポリシー判定を導入したいと思っても、インフラ準備、サーバ死活監視、サーババージョンアップなど管理者の業務負荷やコストの理由から導入を見合わせているような場合、マネージドサービスを利用することを推奨します。マネージドサービスを利用する場合、利用する企業は、追加機器やソフトウェアの購入といった新規の設備投資が必要なく、クライアント PC の数量に応じた月々のサービス利用料だけで済みます。また日々の運用に関しても、サーバへのパッチ適用やウィルス定義ファイル更新などもサービス提供者が行うので運用にかかる管理者の負担を軽減することが可能です。

終わりに

当社では、クラウド型 IT 資産管理の「Smart 資産管理サービス」を手掛けております。このサービスを利用することで社外、社内にあるクライアント PC はもちろん、その他デバイスも含めた一元管理が可能です。また、セキュリティポリシー判定の機能があることで企業環境をセキュアに保ち PC の健全性を担保できます。

その他当社では、「運用代行」「その他セキュリティ対策」「ローコード開発基盤」「無拘束の複合現実ヘッドセット」「RPA」といったサービスも展開しており、ご相談も随時お受けしております。課題に困っているご担当者の方は、どうぞお気軽にお声掛けください。

【「Smart 資産管理サービス」Web サイト】https://www.tdi.co.jp/solution/smart
【お問い合わせ】https://www.tdi.co.jp/inquiry/

tdi 情報技術開発株式会社　営業本部　iDC&セキュリティ推進部
東京:〒163-6013 東京都新宿区西新宿六丁目 8 番 1 号 住友不動産新宿オークタワー
TEL.03-6853-1781(直通) FAX.03-3372-1899
中部:〒450-0002 愛知県名古屋市中村区名駅二丁目 41 番 5 号 CK20 名駅前ビル 4 階
TEL.052-571-6871(代表) FAX.052-571-3856
関西:〒530-0005 大阪府大阪市北区中之島二丁目 2 番 7 号 中之島セントラルタワー20 階
TEL.06-6201-7739(代表) FAX.06-6201-7740
九州:〒812-0013 福岡県福岡市博多区博多駅東二丁目 10 番 1 号 福岡ビル S 館 7 階
TEL.092-451-8218(代表) FAX.092-474-7379