Ivanti を活用したテレワーク環境のセキュリティ対策

近年、在宅勤務の普及に伴い、社外でクライアント PC を利用する場面が増えています。社外での利用の際は、情報漏洩や端末のウイルス感染といったリスクが高まることもあり、テレワーク環境のセキュリティ対策をより強化する必要があります。本資料では Ivanti を活用したテレワーク環境のセキュリティ対策を紹介いたします。

内容

テレワークとは？

テレワークとは、情報通信技術を活用し、場所を選ばず仕事ができる柔軟な働き方のことを指します。テレワークは、働く場所によって以下の 3 つに分けられます。

在宅ワーク	勤務先から離れて、自宅を就業場所とする働き方
モバイルワーク	移動中の交通機関や顧客先、カフェ、ホテルなどを就業場所とする働き方
施設利用型ワーク	勤務先から離れたところに設置した部門共用オフィスで就業する施設利用型の働き方

テレワークは、社外のさまざまな場所で業務や会議が可能になるため、通勤や移動にかかるコストや時間を軽減することができ、業務の効率化、柔軟な働き方が可能となります。

テレワーク導入の課題

多様化する働き方にテレワークは効果的だといわれていますが、テレワーク時は、職場よりセキュリティレベルが低い環境で、職場より安全性の低いネットワークを介して PC を使用するため、テレワーク PC のセキュリティ対策に頭を抱える企業も増えています。主な情報漏えいのリスクとして、以下の点が挙げられます。

●OS、アプリ、ドライバーなどのセキュリティパッチ未適用リスク

・セキュリティパッチを PC に適用せずに脆弱性を放置していると、マルウェア感染などの攻撃に悪用され、機密情報の漏えいやデータ損失に繋がる

●社外からのインターネット閲覧によるマルウェア感染リスク

・悪意を持った第三者による不正サイトへの誘導などにより、マルウェア感染から業務停止や情報漏えいなど様々な被害が発生する

●許可していないソフトウェアの導入リスク

・許可していないソフトウェアのインストールによるマルウェア感染から業務停止や情報漏えいなど様々な被害が発生する

・コンプライアンス違反によりソフトウェア会社から多額の損害賠償を求められる

●PC や記録媒体の紛失リスク

・業務用 PC や USB メモリといった機器・記録媒体の社外持ち出し時に、物理的な紛失や盗難による情報漏えいが発生する

リスク回避のためには、運用ポリシーの明確化や従業員の教育も重要ですが、同時にセキュリティ対策ツールの導入も検討が必要です。

対策

Ivanti とは？

Ivanti では、企業内のデスクトップ、サーバ、モバイル、デバイスのシステム、セキュリティ、プロセスを統合的に管理するソリューションを提供しています。Windows をはじめ Mac、UNIX、Linux、スマートフォン等のプラットフォームに対応し、かつそれらをシングルコンソールで一元管理することが可能です。

セキュリティパッチの適用「パッチ管理」

セキュリティパッチとは、OS やアプリやドライバーに脆弱性や問題点などが発見された際に、それらの脆弱性や問題点を修正するためのプログラムです。セキュリティパッチを PC に適用せずに脆弱性を放置していると、マルウェア感染などの攻撃に悪用され、機密情報の漏えいやデータ損失に繋がるリスクが生じるため、セキュリティパッチの適用が重要となります。セキュリティパッチを適用することで、不正アクセスやマルウェア感染のリスクを低減することができます。

情報セキュリティ部門の担当者は、社外のテレワーク PC に対して、脆弱性がないか、セキュリティパッチがリリースされていないかを定期的に確認し、未適用のセキュリティパッチがある場合には、速やかにセキュリティパッチの適用を実施する必要があります。これらの作業を Ivanti のパッチ管理機能を活用して自動化することで、情報セキュリティ部門の担当者の負荷を軽減することができます。

Ivanti の「パッチ管理」の特長は以下の通りです。

・サブスクリプションサービスで 100 ベンダー以上のパッチを Ivanti が収集

・診断用定義ファイルとともに顧客のサーバへ自動配布

・中継サーバ無しでもソフト配信と同じ仕組みでネットワーク負荷を抑えてすばやく配信

・パッチ本体も判定プログラムもサブスクリプションサービスで自動提供

・適用するパッチさえ決めれば、OS もバージョンも Ivanti が判定し自動適用

・インターネット越しでもパッチ管理の使用が可能（VPN 不要）

許可していないソフトウェア導入禁止「ソフトウェア配布ポータル」

許可していないソフトウェアのインストールを行うことは、マルウェア感染から業務停止や情報漏えいなど様々な被害が発生するリスクがあるほか、ライセンス違反によってソフトウェア会社から多額の損害賠償を求められるリスクにもつながります。

許可していないソフトウェアの導入を禁止する前に、まずは Windows の管理者権限を付与しないことが適切な対応です。従業員に対して完全な管理者権限を付与すれば、セキュリティのリスクが高まり、コンプライアンス遵守が困難となってしまいます。

しかし、管理者権限を付与しない場合、許可しているソフトウェアのインストールも従業員が任意にできなくなるため、IT 部門の担当者が個別に対応することになります。そうなると IT 部門の運用負荷は非常に高くなり、運用が回らなくなってしまう可能性があります。

Ivanti の「ソフトウェア配布ポータル」を使うことで、管理者権限を与えなくても、社内で許可されたソフトウェアであれば、従業員がセルフインストールを行うことができるようになります。これにより、許可していないアプリケーションのインストールを抑止し、マルウェア感染による被害の発生や、ライセンス違反による損害賠償のリスクを軽減することが可能です。

Ivanti の「ソフトウェア配布ポータル」の特長は以下の通りです。

・ユーザ側に Windows の管理者権限は不要

・必要なときにユーザのタイミングで許可したソフトウェアのインストールが可能

・インストーラー、バッチファイル、リンク（URL/実行ファイル）に対応

PC や記録媒体の紛失対策「インベントリ管理と外部デバイス制御」

在宅勤務の普及に伴い、業務用 PC や USB メモリなどの記憶媒体を社外で利用する場面が増えています。機器を社外に持ち出すことで、紛失の危険性、また紛失時にメディア内の情報が

漏えいする危険性も高くなってしまうため、PC の暗号化、リムーバブルドライブの暗号化などの対策が必要となります。

Ivanti の「インベントリ管理」と「外部デバイス制御」を利用することで、BitLocker で暗号化していない PC の見える化と該当従業員へのアラート発信、リムーバブルドライブの自動暗号化が可能となります。これにより、機器・記録媒体の社外持ち出し時の物理的な紛失や、盗難による情報漏えいのリスクの軽減が期待できます。

Ivanti の「インベントリ管理」「外部デバイス制御」の特長は以下の通りです。

・インターネット越しでもインベントリ収集の使用が可能（VPN 不要）

・LAN/WAN 外の PC をインターネット越しに社内 LAN 上の PC と同ポリシーで管理

・BitLocker のボリューム暗号化ステータス、回復キーID、回復キー収集

・リムーバブルドライブの暗号化

・シャドーコピー　※USB メモリへの書き出しを記録

クラウドサービスの利用

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による管理者の業務負荷やコストの増加が理由で、テレワーク環境のセキュリティ対策導入を見合わせている、といった場合には、クラウドサービスの利用をお勧めします。クラウドサービスを利用すれば、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は必要なく、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セキュリティ対策が可能となります。また、日々の運用においても、サーバへのパッチ適用やウイルス定義ファイルの更新などをサービス提供者が行ってくれるため、運用にかかる管理者の負担を軽減することができます。

終わりに

当社は、2006 年より Ivanti（当時名称：LANDesk）を手掛け、提案、導入構築、アフターフォローを行っている Ivanti ゴールドパートナーです。海外にも事業展開する大手企業様に対し、多数の導入実績があります。

また、広範なセキュリティ対策製品により、ネットワークインフラからエンドポイントまで、お客様のニーズに応じた包括的なソリューションを提供しています。

IT 資産管理、セキュリティにお悩みの際は、お気軽にご相談ください。

【統合 IT 資産・セキュリティ管理ツール：Ivanti】https://www.tdi.co.jp/ivanti/

【セキュリティソリューション】https://www.tdi.co.jp/category/security

【当社・取り扱い製品へのご意見・ご質問・お問い合せ】https://www.tdi.co.jp/inquiry/

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: 〒163-1332 東京都新宿区西新宿六丁目 5 番 1 号 新宿アイランドタワー32 階
TEL.03-5325-4826 (直通) FAX.03-5325-4812

中部:〒451-6027 愛知県名古屋市西区牛島町 6 番 1 号 名古屋ルーセントタワー27 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