ivanti

SECURITY CONTROLS

方法は9つ

権限をもつユーザーのセキュリティリスク

ITシステム管理者としてトレーニングを受けていないにも関わらず、自社システムの完全な管理者権限を持つエンドユーザーに警戒してください。管理者ではないのに管理者権限を持つエンドユーザーがいかにセキュリティリスクを高め、管理コストを増やし、コンプライアンスの遵守を困難にしているか、そして各ケースで企業ができる対策をまとめました。

1 マルウェアを侵入させる不正アプリのインストール

管理者がユーザーアカウント制御をオフに設定できないようにし、不正アプリやシステム設定の意図せぬ変更を防止しましょう。

2 アンチウイルスなどクリティカルなサービスの無効化

Microsoft管理コンソール（MMC）により、ユーザーはサービスを管理できるスナップインを読み込むことができます。エンドユーザーが管理者権限を使用してMMCにアクセスできないようにしましょう。

3 GUIベースの制限のオーバーライド

オペレーティングシステムに対するコマンドやスクリプトの実行を制限しましょう。

4 エージェントや保護ソフトウェアのアンインストール

権限を持つユーザーによるサードパーティーソフトウェアのアンインストールを防止しましょう。

5 統合管理の保護ポリシーの回避

Windowsレジストリへの特権アクセスを除外し、ユーザーによる構成設定の変更を阻止しましょう。

6 エンドポイントのファイアウォール設定の無効化または変更

無効化を防止し、ネットワーク全体への悪意のあるソフトウェアの拡散を阻止しましょう。

7 誤った日時を悪用することによるアプリケーションの挙動の変更

監査やトラブルシューティングのためにアプリケーションの完全性を確保し、タイムスタンプを正確に記録するため日時変更を阻止しましょう。

8 保護ソフトウェアの強制終了

セキュリティリスクを軽減するため、プロセス停止制御を追加しましょう。

9 マルウェアを侵入させる可能性のあるアプリケーションの管理者権限での実行

一部のアプリケーションに標準の権限のみで実行させる制限をかけましょう。

Ivanti® Security ControlsのApplication Controlの各種機能を利用すれば、すぐに簡単な制限を設定し、リスクを軽減し、企業のコンプライアンスを遵守し、誤って管理者設定を変更してしまった社員による不必要なITチケットの発行を阻止できます。

ホワイトペーパーのダウンロード

ivanti.co.jp | Contact-Japan@ivanti.com | 03-5226-5960

ivanti