Ivanti Software株式会社

ランサムウェアの実行を防ぎ アプリケーションの制御と特権管理を実現

IT部門の負担を最小限に留め、エンドユーザーの安全性と利便性を両立

Ivanti Softwareの「Application Control」は、独自のアプローチで開発したアプリケーション実行管理や権限管理機能を提供している。これにより、IT部門の作業負荷を軽減しつつ、使いやすいWindows環境で現場の生産性を落とすことなく、強固なセキュリティも実現できる。

重要な4つの戦略を実行すれば Windowsへの脅威の85%を防げる

近年、ランサムウェアが世界的に流行したり、高度な標的型攻撃で数々の組織から情報が流出したりするなど、マルウェア（不正ソフトウェアの総称）が猛威を振るっている。最新のマルウェアにはセキュリティ技術を回避する高度な手口が盛り込まれ、既存のアンチウイルスだけでは完全に防ぎ切れないのが実態だ。そこで近年では、さまざまな方式のセキュリティを組み合わせた多層防御によりセキュリティを高めることが重要とされている。

オーストラリア通信電子局（Australian Signals Directorate：ASD）も、標的型攻撃に対するリスク低減戦略として35もの項目を挙げている。ただし、その中でも重要な4つの戦略を実行すれば、Windowsへの脅威の85%を防ぐことができるとも示している。

その4つとは、「アプリケーションホワイトリスティング」「アプリケーションパッチ」「OSパッチ」「管理者権限管理」だ。アプリケーションホワイトリスティングとは、実行できるアプリケーションを限定することで不正プログラムの起動を防ぐことを指す。アプリケーションとOSのパッチは、必要なセキュリティパッチを適時適切に適用すること。最後の管理者権限管理は文字通り「管理者権限」を必要な場面でのみ使えるよう管理することだが、Windowsでは管理者権限は「Administrator」とも呼ばれ、システムに手を加える行為を可能にする権限だ。

エンドユーザーの利便性と エンドポイントの安全性を両立

セキュリティに関するASDの4つの重要戦略について、日本企業はあまり本格的に取り組んでこなかった。多くの企業が導入しているアンチウイルスソフトや高機能ファイアウォールなどは、脅威を検知して防ぐことに主眼を置いたもので、それとはまったく異なるアプローチが必要とされている。

この4つの重要戦略に対応するソリューションを提供しているのが、Ivanti Softwareだ。アプリケーションホワイトリスティングと管理者権限管理を実現する「Application Control」、アプリケーションパッチとOSパッチを管理する「Ivanti Patch」といった製品がある。中でもApplication Controlはユニークな機能を持つ。

もともとWindowsの管理者権限とは、非常に多彩な行為を一括で可能にする非常に強力なものだ。Application Controlではその権限の範囲を細分化し、個別に設定することができる。

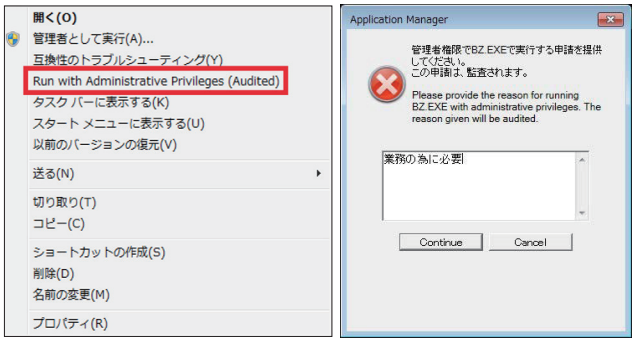
時刻の変更、デフラグなど、リスクが低めでユーザーの利用頻度も多いツールについてはすべてのユーザーに許可するといった設定が可能。逆に、リスクの高いツールや機能、ドライバのインストールなど

については原則禁止とし、必要な場面に限って利用させる設定ができる。そのための手順は複数用意され、同じ企業内でも部署や職務内容などに応じて使い分けることも可能だ。

その手順の1つはポリシー変更リクエスト機能にてヘルプデスク方式でユーザーから申請を受け付け、許可を与えた場合のみ実行できるようにするという方法だ。メール、電話での申請／承認手続が可能となっている。

ほかには、ユーザー自身の判断で利用できる「自己昇格」と呼ばれる手順もある。企業で使用されている独自アプリケーションなどには、今も管理者権限がないと稼働しないものが少なくないが、こうしたアプリケーションを実行させる場面で役に立つ。

これらを使い分けることで、現場の生産性を落とさず、かつIT部門の負担を最小限に留め、従業員の端末（エンドポイント）のセキュリティを高い状態に維持できる。エンドユーザーの利便性とエンドポイントの安全性を両立させることが可能というわけだ。



実行権限を一時的に昇格させる「自己昇格」では、右クリックからの実行で監査ダイアログが現れ、ソフトウェアを起動する申請理由を記入することもできる。これは、ルール違反に対する心理的な抑止力としても有効になる。

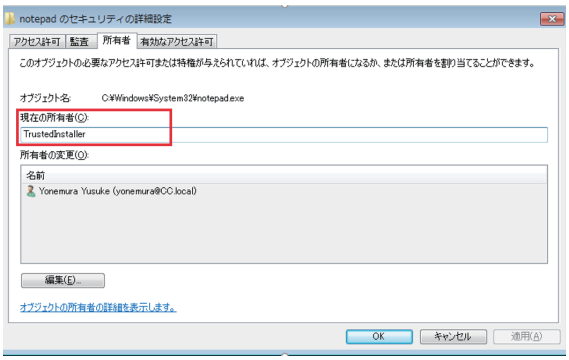
米国特許を取得した技術を使って持ち込みファイルの実行を制御

Application Controlのアプリケーションホワイトリスティング機能も、ユニークな技術が搭載されている。

通常ホワイトリスティングは、実在する実行ファイルの情報を取得しておき、それと合致するファイルのみ実行する。しかし近年のソフトウェアは、セキュリティパッチをはじめとするアップデートが以前より頻繁に行われており、その都度リストを更新しなくてはならないことが課題となる。そのためオフィスワークなどの一般的な用途のPCではホワイトリスティングは実用的でなく、キオスク端末や組み込み用PCなど限定的な用途のPCなどでの利用に留まっている。

一方Application Controlでは、「そのプログラムをPCに持ち込んだのは誰か」という情報（Windowsの「ファイル所有者」情報）をもとに実行ファイルの起動を制限することができる。所有者が「TrustedInstaller」、「Administrators」「System」となっているファイルのみ実行を許可することで、外部から持ち込まれたファイルの実行を制御する。

所有者情報は、ファイルやフォルダのプロパティ情報として管理されている。ユーザーが作成したり持ち込んだりしたファイルの場合は基本的にそのユーザーが所有者となるのに対し、OSや正当なアプリケーションなどの場合は特別な名称が与えられるため、明確に識別することが可能だ。Application Controlではこれを用い、どんなPCでも有効なメンテナンスフリーのホワイトリストを実現している。この技術「Trusted Ownership（信頼された所有者）」は米国特許を取得したもので、非常に特徴的な機能となっている。



所有者情報を利用して実行ファイルの起動を制限することが可能。

Ivanti Software株式会社
〒102-0093東京都千代田区平河町1-1-8 麹町市原ビル5階
お問い合わせ　TEL. 03-5226-5960
https://www.ivanti.co.jp/