ivanti

Ivanti Application Control
機能&メリット

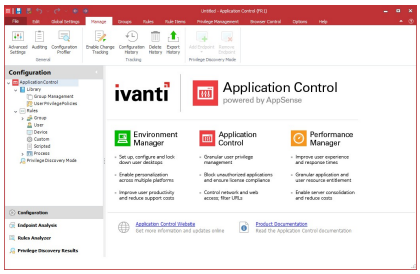
IVANTI ホワイトペーパー

Contents

はじめに

本書は、Ivanti® Application Controlの機能と関連するメリットの概要を提供するものです。

本書に記載されている情報は、Application ControlがIT部門を支援できるエリアについて理解を深める上で役立ちます。



機能＆メリット

信頼された所有者「Trusted Ownership™」 確認機能

ビジネス上のメリット: Ivanti Application Controlは、複雑な構成や継続的な管理を行う必要なく、自動的にエンドポイントを保護します。

ランサムウェア、スパイウェア、悪意のあるモバイルコードだけでなく、実行可能ファイルに寄生したウイルス、トロイの木馬、ワーム、キーロガー、スクリプト攻撃、不正なインターネットコードなどその他のWebベースの脅威を阻止します。

「Trusted Ownership」確認機能は、企業ネットワーク内外でグループ全体のデスクトップ/ノートパソコン保護を提供し、モバイルワーカーに何重にも重なった強力なセキュリティを提供します。

ユーザーが導入する不正なアプリケーションを防止し、ゴールデンイメージの整合性を保つだけでなく、ビジネスアプリケーションにリソースを改めて集中させることで、ユーザーの生産性を向上します。

また、標準ユーザーによる既存のマルウェア対策やウイルス対策ソリューションに関連するアプリケーションへのアクセスを防止することで、そのような既存のソリューションへの投資を守ることができます。さらに、不明なトロイの木馬やワームが瞬時に広まることを防ぎ、既存のソリューションの機能を拡張します。

Ivanti Application Controlは、Microsoft AppLockerなど継続的なホワイトリストの管理が必要な他のアプリケーション管理ソリューションに関連するIT部門の負担を軽減します。

機能/仕組み: 「Trusted Ownership」確認機能は、Application Controlによって使用されるデフォルトの追加設定なしで使える安全性を確保するための方法です。

この機能では、信頼できる情報としてアプリケーションのNTFS所有者検査が使用されます。管理者やMicrosoft SCCMなどのソフトウェア展開システムといった「信頼された所有者」によってアプリケーションが導入、所有される場合、特に指定のない限りすべてのユーザーがそのアプリケーションを実行できます。アプリケーションが標準ユーザーなど信頼されていない所有者によって導入、すなわち所有されると、誰もそのアプリケーションを実行できなくなります。

事前に定義された「信頼された所有者」のリストによって、信頼できるアカウントが瞬時に判断されるため、信頼された所有者であるユーザーが所有するアプリケーションは正常にインストールまたは実行されます。

デフォルトでは、管理者とシステムアカウントのみが信頼された所有者に設定されています。これにより、管理者によって、もしくはオペレーティングシステムの一部としてインストールされたアプリケーションのみが実行されるようになります。

デフォルトの「信頼された所有者」のリストは、編集して、他の信頼できるユーザーやグループを追加することができます。

Windows 権限管理

ビジネス上のメリット: 完全な管理者権限をユーザーに付与することでエンドポイントのセキュリティが脆弱になる可能性があるため、IT部門やシステム管理者は、完全な管理者権限をユーザーに付与しないことを好みます。

また、管理者権限を提供する元々の理由がたいした理由ではない場合、完全な管理者権限をユーザーに付与するとコストがかかるIT関連の問題が生じます。完全な管理者権限をユーザーに付与することで、IT部門はユーザーにエンドポイントへの鍵を効率的に提供できます。これにより、各ユーザーが自分のシステムを100%自分で管理できるようになるため、エンドポイントの管理が極めて困難になります。

これは、セキュリティコストや管理コストの大幅な増加や生産性の低下につながるだけでなく、法的責任に関する問題にもつながる可能性があり、SOX法やHIPAA COSO、FERPAなどのガイドラインを遵守することが非常に難しくなります。

必要なアプリケーション/プロセス/タスクへの昇格権限のみをユーザーに付与することで、企業はTCO（総所有コスト）を削減できます。セキュリティの脆弱性につながる可能性のある過剰な権限を付与することなく、ユーザーに必要なタスクを実行させることができるため、サポートへの問い合わせ電話の件数が減るため、エンドポイントを簡単に管理できるようになります。

特定のアプリケーションを実行するためのユーザー権限を昇格します

機能/仕組み: この機能により、IT管理者は特定のユーザーの管理者権限で実行できるアプリケーションを指定できるようになります。完全な管理者権限をユーザーから除去することができますが、引き続きユーザーは必要な場合にのみ昇格権限を使用して必要なタスクを実行できます。

使用事例: Barclays Bankは、エンドポイントで各ユーザーがプリンターのドライバをインストールできるように、これまでユーザーに管理者権限を付与していました。BarclaysはWindows 権限管理を導入することで、ユーザーから完全な管理者権限を除去し、特定のタスクに対して「必要に応じて」権限を昇格できるようになりました。

特定のコントロールパネルのアプレットを実行するためのユーザー権限を昇格します

機能/仕組み: Windows権限管理は、コントロールパネルのアプレットを昇格権限で実行することを可能にします。つまり、これまで完全な管理者権限をユーザーに付与していた場合、代わりにユーザーの権限をタスクに必要なレベルに昇格できるようになるということです。例えば、管理者でなくなったとしてもユーザーは業務に必要なサービスの停止や開始をこれまで通り実行できます。

使用事例: Citi Group USAは、ユーザーがActive Xをインストールでき、開発スタッフがアプリケーションをインストールできるようにするため、かつてユーザーに完全な管理者権限を付与していました。

使用事例: Morgan Stanleyは管理者権限で開発チームにVisual Studioを実行させる必要がありました。

アプリケーションを実行できる権限を制限するため権限を減らします

機能/仕組み: Windowsの権限管理については、2つの見解があります。1つは言うまでもなく権限の昇格です。これはIvantiが取っているアプローチです。もう1つは、現在管理者に付与されている権限を維持するため、特別な権限を減らすことです。ただし、システム管理者は特定のアプリケーションが管理者の認証情報で実行しないことを確認できます。権限を減らす方法は、全社的に管理者権限を除去する場合に適したオプションで、段階的な展開に役立ちます。

使用事例:DSMは、ユーザーがActiveXコントロールをインストールできるようにするため、この機能を導入しました。

望ましくないシステム設定へのアクセスを制限するため権限を減らします

機能/仕組み:管理者が特定のタスクを実行できないようにすることは得策かもしれません。Windowsの権限を管理することで、IT部門はシステム管理者が変更を希望しない設定を管理者ユーザーが変更することを阻止できます。これには、ファイアウォールの設定や、AVソリューションなど特定のサービスの停止を防止することが含まれます。

Application Controlにより、IT部門は管理者権限を持つユーザーを把握し、特定のプロセスに対して権限を下げることができます。つまり、IT部門は環境を管理でき、ユーザーは必要なタスクに対して管理者権限を持てるということです。

使用事例:各自のファイアウォールを設定するため、ユーザーには管理者権限が必要でした。ただしこの設定を可能にするために権限を付与するだけでは、ユーザーに必要以上の権限を付与することになってしまいます。Application ControlによりIT部門は、セキュリティを妥協することなく適切な権限を提供できます。

オンデマンドの変更リクエスト管理

ビジネス上のメリット:モバイルユーザーやオフラインで長時間作業するユーザーには、現時点では承認されていない企業リストにある特定のアプリケーションへのアクセスが必要となることがよくあります。これらのアプリケーションへのアクセスを妨げると、生産性が低下し、好ましくないユーザーエクスペリエンスにつながることがあります。

オフラインまたはモバイルユーザーがメールまたは電話で非標準アプリケーションにアクセスすることを可能にすることで、オフィスベースのIT管理者にサポートを求める必要性を排除し、監査されたアプリケーション管理を実現し、ユーザーの生産性と満足度を向上できます。

機能/仕組み:生産性が妨害されている場合に、エンドユーザーが権限の緊急昇格やアプリケーションへのアクセス権をリクエストすることを可能にします。ユーザーはアプリケーションのダイアログボックスから直接リクエストを送信できます。変更の緊急リクエストの対応は、

操作が簡単なフルフィルメントポータルを使用して、レベル1のヘルプデスクのアナリストに割り当てられます。昇格権限は恒久的または期間限定で付与されます。

Application Network Access Control（ANAC）

ビジネス上のメリット:ルーターやスイッチ、ファイアウォールなど複雑な管理機能を導入することなく、アクセス権のないネットワークリソースに社員や請負業者がアクセスすることを防ぎます。

機能/仕組み:ANACは、禁止されているネットワークリソースへのリクエストをインターセプトし、阻止して、ルール処理の結果に基づいてIP、ホスト名、URL、UNC、ポートによるアウトバウンドのネットワーク接続を制御します。

プロセスルール

ビジネス上のメリット: Application Network Access Control（ANAC）にプロセスルールを適用するということは、アウトバウンドのネットワークアクセスが特定のプロセス自体によって決定されるということです。すなわち、各アプリケーションに専用の制限を設けることができるということです。プロセスルールを適用することで、IT部門はアプリケーション（親）によって実行できるプロセス（子）を決定できます。

アプリケーションごとにネットワークアクセスを制御します

機能/仕組み:既存のルールセットにプロセスルールを導入することで、管理者はアプリケーションがアクセスできるネットワークリソースを決定できます。つまり、各アプリケーションに専用の制限を設けることができます。

アプリケーションが実行できることとできないことを制御します

機能/仕組み:アプリケーションやスクリプトが別のアプリケーションやスクリプトを呼び出すことは可能です。この機能により、管理者はアプリケーションが実行できることを指定できます。

例えば、ユーザーによる実行が禁止されているアプリケーションが別の昇格アプリケーションによって呼び出された場合、IT部門は特定のプロセスによって呼び出された場合にアプリケーションの実行を許可する、もしくは実行させないようにApplication Controlを設定できます。

アプリケーションの終了

ビジネス上のメリット: 一部のMS OfficeアプリケーションをRDSHやCitrix XenAppなど複数のユーザーがいる環境からユーザーが切断し、同じセッションにライセンスが付与されていないエンドポイントから再接続した場合、MS Officeのアプリケーションは実行したままとなり、企業はMicrosoftのライセンスルールを遵守できなくなります。ところがそのようなシナリオにおいて、Application Controlを使用すると、IT部門はアプリケーションがシャットダウンされてから一定時間が経過するとユーザーに警告が通知される、もしくはアプリケーションがすぐに終了され同じセッションから再実行されることが防止されることを保証できます。

機能/仕組み: Application Controlは常に不正なアプリケーションの実行を阻止することができます。ただし、現在実行中のアプリケーションの中で、構成や環境を変更した場合にアクセスが禁止されるのはどのアプリケーションでしょうか？ライセンス付与の観点から考えると、これは大きな影響を及ぼします。MSのプロジェクトやMS Visioを使ったセッションを実行したままユーザーが切断し、帰宅しライセンスが付与されていない別のエンドポイントデバイスを使用して、同じ開いたままのセッションに再接続した場合、これらのアプリケーションは実行したままとなり、企業はライセンス違反となってしまいます。アプリケーションの終了機能は、ライセンスが付与されていないエンドポイントで開くことが禁止されているアプリケーションをシャットダウンし、アプリケーションを閉じる前にユーザーが作業を保存すること、もしくは、警告なくアプリを終了することを可能にします。

アプリケーショングループ

ビジネス上のメリット: この機能は、簡単かつ速やかな構成を可能にします。

機能/仕組み: 通常Application Controlに必要な構成はほとんどありませんが、デフォルトのTrusted Ownershipモデルを変更する場合、ホワイトリストとブラックリストのシナリオの施行が必要となる場合があります。また、一般的なWindows環境にあるアプリケーションの数により、これらのリストは膨大になり、維持管理が難しくなる場合があります。アプリケーショングループ機能は、すべてのルール項目をひとつにまとめ、はるかに整理された構成を可能にします。

デジタル署名

ビジネス上のメリット: デジタル署名、すなわちデジタルハッシュチェックにより、IT部門はシステムにインストールされているアプリケーションやファイルが変更されていないことを把握することができ、システムの整合性を維持し、保守コストを削減できます。

デジタル署名は個々のファイルを非常に簡単に特定する方法であるため、究極のセキュリティとなります。デジタル版の指紋のようなものだとお考えください。ファイルに些細な変更が加えられた場合、デジタル署名も変更されます。デジタル署名グループを作成すると、大規模かつより複雑な構成の管理を簡易化できます。

機能/仕組み: デジタル署名は、高度なセキュリティを実現するため、ブラックリストやホワイトリストと照らし合わせてファイルの暗号学的ハッシュ関数（デジタル指紋だとお考えください）を確認し、SHA-1、SHA-2、またはAdler32デジタル署名をアプリケーションやファイルに割り当て、アプリケーションの整合性を保証します。改竄されたアプリケーションやなりすましアプリケーションの実行が防止されます。ただしデジタル署名は、サービスパックやパッチによって毎回ファイルが更新される度に、もしくはオペレーティングシステムにパッチが適用された場合に新しい署名を取得する必要があるため管理にかかる経費が高額になります。デジタル署名はファイルシステムとは無関係で、ローカル、ネットワークおよびリムーバルメディアで使用できます。

パッシブモニタリング

ビジネス上のメリット: 完全実装前にユーザーの行動を正確に追跡する際や、ソフトウェアライセンスを管理するためにアプリケーションの使用状況を理解する際に非常に役立つツールを提供します。

機能/仕組み: ユーザーによるアプリケーションの実行を妨げることなく、不正な実行の試行をモニタリングします。パッシブモニタリングは、ユーザー、デバイス、グループベースでオン/オフに設定できます。

アプリケーション制限＆時間制限

ビジネス上のメリット: アプリケーション制限は、企業のライセンスポリシーを施行するために使用され、権限が付与されたユーザーのみが一定の時間内のみビジネスアプリケーションを実行できることを保証します。

機能/仕組み: ユーザー、デバイス、アプリケーションごとに実行できるインスタンスの数を制限します。時間制限を適用することにより、アプリケーションへのアクセスについてさらに上のレベルの制御を実現することができます。これにより、ユーザーは指定の時間内に一定の時間のみプログラムを実行できます。

圧縮（zip）ファイル＆Windows インストーラーパッケージ

ビジネス上のメリット: 実行できるパッケージに適用されるルールを指定することによりWindowsインストーラーパッケージへのアクセスを制限します。これにより、隠れたトロイの木馬やワーム、そのほかの不正な実行可能ファイルを防止します。

機能/仕組み: 内蔵のZip Extractorを使用して自己解凍形式の圧縮ファイル（zip）を安全に開きます。

ホワイトリスト＆ブラックリストの設定

ビジネス上のメリット: 極めて安全な環境を実現する堅牢かつロックダウンされた環境を確保するため、Ivantiの追加設定なしで使える「Trusted Ownership」確認機能に代わるアプリケーション管理方法を提供します。

機能/仕組み: 既知の脅威や問題からアプリケーションを保護するため

ブラックリストを設定するか、既知および信頼できるアプリケーションのみをシステムで実行できるようにするためホワイトリストを作成します。

「ホワイトリスト」は、許可されている一連のアプリケーションを定義し、他の不明な実行可能ファイルをすべて防ぎます。デジタル署名のハッシュと組み合わせることで、非常に安全なアプリケーション管理方法となりますが、管理にかかる経費が高額になります。

「ブラックリスト」は、実行が許可されていない一連のアプリケーションを定義します。ブラックリストは実行を妨げる必要があるアプリケーションを指定する必要があり、不明なアプリケーションを対象としないため、安全性は低くなります。

VBScripts＆バッチファイルの管理

ビジネス上のメリット: 管理者によって許可されているスクリプトのみをユーザーが呼び出せるようにすることで、悪意のあるコードやウイルスによる攻撃を防止します。

機能/仕組み: 実行が許可されているかを確認するためWindows Script HostファイルやDOSバッチスクリプトなどのスクリプトがルールと照らし合わせて確認されます。スクリプトのコンテンツが変更されていないことを保証するためデジタル署名確認を適用するとセキュリティをさらに強化できます。

Rules Analyzerコンソール

ビジネス上のメリット: IT部門がセキュリティの脆弱性やユーザー環境の過剰なロックダウンを速やかかつ簡単に特定、解決することを可能にします。

機能/仕組み: Rules Analyzerにより、管理者は展開した構成に起因するあらゆる問題を解決できます。ログファイルは、アプリケーションの実行が許可された/許可されなかった理由に関する詳細への容易なアクセスを提供します。

信頼できるベンダー

ビジネス上のメリット: 特定の信頼できるソフトウェアベンダーからのアプリケーションの実行を許可するシンプルなメカニズムを提供します。

機能/仕組み: 特定のベンダーに関連付けられているデジタル署名を確認し、ファイルが該当するベンダーから提供されていることと、変更されていないことを保証します。

デバイスごとのライセンス施行

ビジネス上のメリット: Ivanti Application Controlは、強制的なデバイスベースのソフトウェアライセンス管理でMicrosoftより評価されています。Ivantiのお客様は、3年間でユーザー1人あたり2,000ドル以上を節約しており、わずか数ヶ月でROI（投資対効果）を達成しています。

機能/仕組み: Microsoft Licensingは、クライアントアクセス（CAL）モデルに基づいているため、ライセンス付与はユーザーと関係がありません。Remote Desktop Server Host（RDSH）に接続できるすべてのデバイスにMicrosoft CALが必要となります。Ivanti Application Controlにより、IT部門はユーザーではなく、接続中のデバイスに基づいてソフトウェアのアクセスを定義できます。

自己権限付与

ビジネス上のメリット: 一部の環境では、頻繁に社内のソフトウェアを更新、テストする開発者や、新しいまたは不明なアプリケーションにアクセスする必要がある推薦権限を持つユーザーなど、ユーザーが新しい実行可能ファイルをコンピューターに追加する必要があります。自己権限付与機能は、推薦権限を持つユーザーがシステムに導入したアプリケーションを実行することを可能にします。推薦権限を持つユーザーは、IT部門のサポートに頼らずオフィス外で安全なエンドポイントにアプリケーションを追加できます。これにより、隠れたマルウェアや実行可能ファイルに対する高水準の保護を提供しつつ、開発チームや推薦権限を持つユーザー、管理者にソフトウェアをインストールしテストする柔軟性を提供できます。

機能/仕組み: 自己権限付与が許可されたユーザーには、信頼されていない実行可能ファイルを実行中のセッション中に毎回1回、または常に実行することを許可するオプションが提供されます。総合的な監査により、アプリケーション名や実行日時、デバイスといった情報の詳細を取得できます。さらに、調査のためにアプリケーションのコピーを取得し、中央システムに保存できます。

信頼できるアプリケーション

ビジネス上のメリット: 実行またはインストールする必要のあるカスタマイズされたオンザフライのコンテンツに依存するビジネスアプリケーションが求められている通りに機能し続けることを保証します。

機能/仕組み: 子の実行可能ファイルやDLLなどのコンテンツは、特定の親アプリケーションによって呼び出された場合のみ許可されます。これは、動作中にアプリケーションがユーザープロファイル外のエリアに実行可能ファイルを書き込む場合に役立ちます。

アーカイブ

ビジネス上のメリット: IT部門が、ネットワーク上の不正な実行可能ファイルを特定し、不正なアプリケーションの名前を変更して既存のセキュリティ制御を回避しようとしているユーザーを検出することを可能にします。

機能/仕組み: ユーザーが実行しようとした禁止ファイルを自動コピーし、分析のために、セキュアなリポジトリに保存します。

エンドポイント分析

ビジネス上のメリット: 大規模な企業デスクトップでアプリケーションのコンテンツの管理と制御を簡易化します。

機能/仕組み: エンドポイント分析は、企業環境内のエンドポイントにインストールされているアプリケーションを確認するために使用されます。リモートマシンにはApplication Controlエージェントがインストールされている必要があります。この機能は、Windowsインストーラー技術（MSI/MSP）を使用してインストールされたアプリケーションを検出します。Dependency Walkerにより、子コンポーネントがすべてモニタリングされレポートが作成されていることが保証されます。このレポートから、構成内のルールや署名グループにアプリケーションを簡単に追加できます。

アプリケーション使用状況のスキャン

ビジネス上のメリット: 使用中のアプリケーションや使用されていないアプリケーションを特定することで、ライセンスが付与されていないソフトウェアを特定または制限し、ライセンスが付与されているソフトウェアを削除することができるため、デバイス上のアプリケーションの数を軽減し、これらのアプリケーションのライセンスコストを削減します。**機能/仕組み:** 対象デバイスをスキャンし、ユーザーベースで各アプリケーションが実行された回数を特定します。

Ivanti構成テンプレート

ビジネス上のメリット: Ivantiの構成テンプレートをインポートして、事前に策定された企業ポリシーのベストプラクティスを最大限に活用しましょう。

機能/仕組み: Ivanti Application Controlは、無限に構成ファイルをインポートでき、インポートした構成を組み合わせて使用します。

選択できる構成テンプレートに
https://community.ivanti.com/community/appsenseで利用できる「共通の禁止項目（common prohibited items）」や「エンドポイント分析（end-point analysis）」などが含まれます。テンプレートライブラリは、頻繁に管理、更新されます。

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