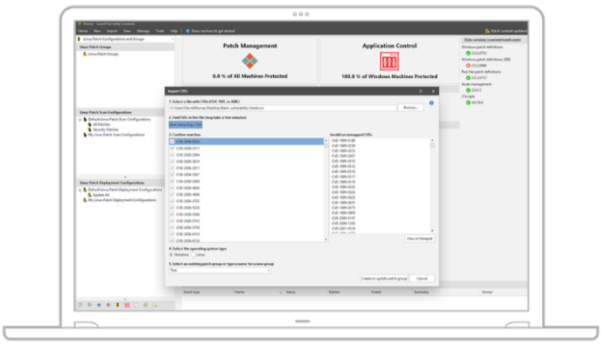
# Ivanti Security Controls

**IT 部門は、無秩序に増加しているデバイスの管理にかなりの時間を費やしており、セキュリティ部門は労働力不足に悩まされています。この現状を踏まえ、Ivanti は企業にとって最大の攻撃区分に的を絞った統合型ソリューションで簡単にセキュリティを確保することを可能にします。Ivanti Security Controls（旧 Ivanti Patch for Windows）には、不正かつ許可されていないソフトウェアから企業を保護し、防御できるようにするためのソフトウェアの検出、異なる OS やサードパーティ製アプリが共存する環境向けのパッチ管理、動的なホワイトリスティング、詳細な権限管理が含まれており、これらは世界のエキスパートが最新のサイバー攻撃に対して最も効果的なバリアを作ると認めているセキュリティツールと IT 部門とセキュリティ部門が企業を守るために連携を強化する上で役立つ追加のパッチツールが集約されています。**

## Windows および Linux 向けのパッチ

Ivanti Security Controls は、物理/仮想 Windows サーバーだけでなくワークステーションも対象とした単一の自動化パッチソリューションです。さらに市場をリードする Windows 向けパッチソリューションに、Red Hat Enterprise Linux 向けのパッチサポートを追加しました。これは 2019 年に予定されている Windows 以外の OS の追加の取り組みの第 1 弾となります。

- **仮想サーバーへのパッチ適用：**オンラインとオフラインのワークステーションとサーバーを検出し、不足しているパッチをスキャンし、展開します。その後、OS やアプリから仮想マシン（VM）まで、あらゆるシステムにパッチを適用します。さらに、VMware との統合により、ESXi ハイパーバイザーにもパッチを適用します。さらにオフラインの仮想イメージも、いつでも実装できる状態に維持できます。（VM を作成し、パッチを適用するという 2 段階のプロセスはできるだけ避けたいはずです。オフラインのテンプレートを常に最新の状態に維持しておけば、VM が最新の状態かどうかを心配せずに VM を展開できます。）



- **エージェントを使用しないパッチ適用：**エージェントレス技術により、チームとシステムの負荷の両方に与える影響を最低限に抑えつつ、お使いのネットワークに接続されているワークステーションやサーバーを評価し、パッチを適用できます。また、エージェントを使用して、お使いのネットワークを管理するために必要なだけ異なるエージェントポリシーを作成し、極めて柔軟なパッチ適用を提供することや、デバイスが常にネットワークに接続されていない環境において、高水準のパッチ精度を実現することもできます。デバイス別に異なるエージェント構成を割り当てましょう。
- **Windows および Linux マシンへのパッチ適用：**様々な環境が混在する状況に対応できるパッチマネジメントソフトウェアが必要です。Windows 以外にもパッチを適用することは必要不可欠です。また単一のインターフェースと自動化ツールを使用して効率的にパッチを適用することで、IT 部門の負担を排除できるだけでなく、防御を強化しつつ人的ミスを軽減できます。
- **アプリケーションへのパッチ適用：**Adobe Acrobat Flash や Reader、Google Chrome、Mozilla Firefox、Oracle Java などサードパーティ製アプリは、アプリとブラウザのアドオンを狙うハッカーの格好の餌食となります。

当社は業界最大のパッチカタログを提供しています。さらに、すべてのパッチが当社のコンテンツチームによる厳しいテストを受けているため、お客様がテストを実施する必要がありません。企業と社員の皆様が主力事業の目標に集中するために時間を有意義に使えるようにするため、当社が時間を節約します。

## 適切なホワイトリスティングと権限管理の実現

Ivanti Security Controls は、より動的なホワイトリスティングオプションも提供しています。このオプションは、リストの代わりに信頼モデルを使用し、高水準のセキュリティを実現しつつ、増強、実行後の所有コスト、パフォーマンスへの影響を軽減します。さらにこのオプションは、ユーザーが必要な業務を遂行できる状態を維持しつつ、IT 部門がユーザーから管理者権限を取り戻し、必要な場合に権限を追加するプロセスを簡易化することを可能にします。

- **ホワイトリスティングを簡易化：**Ivanti は、IT 部門に膨大なリストを手動で管理する負担をかけず、ユーザーを制限することなく、アプリケーション、サービス、コンポーネントへの許可されたアクセスを提供できます。例えば Trusted Ownership™は、ホワイトリスティングのプロセスを簡易化するため NTFS のファイルの所有権を許可します。信頼できるファイルの所有権を定義するため少数の信頼できるアカウントを使用することにより、信頼できる所有者がインストールと更新/アップグレードを実行するアカウントとなるため、ホワイトリストを簡単に実装できるだけでなく、自社の管理システムのアプリケーションを継続的に追加、更新できるようになります。
- **成功の鍵は管理者権限の適切な管理：**悪用された場合、既存のユーザーと同等の権限が攻撃者に付与されてしまう脆弱性がたくさんあります。攻撃者は盗んだ認証情報とユーザーの管理者権限を使用して、情報およびシステムへの完全なアクセス権限を手に入れ、さらに広範なネットワークに攻撃の手を広げる可能性があります。また、サーバーに完全な管理者権限を付与すると、サービスの開始/停止やソフトウェアのインストール/アンインストールが誤って実行されるなど他のリスクが生じます。

  今もなおユーザーの権限を完全にロックダウンするポリシーを施行できる企業は存在しますが、ユーザーのシステムで管理者権限をユーザーに付与することが避けられない一部の機能をユーザーが必要としているのが現実です。Microsoft は、ユーザー権限と完全な管理者権限の 2 つのレベルのコントロールしか提供していません。この 2 つの権限の間には、いくつかのバリエーションが存在しますが、ユーザーと管理者の両方を満足させるエクスペリエンスを提供するには十分ではありません。

Ivanti は Just Enough Administration（JEA）と Just-in-Time Administration（JIT）を実装しています。JEA と JIT は、ユーザーから管理者権限を取り戻しつつ、必要な場合に権限を昇格するプロセスや別の権限を追加するプロセスを簡易化し、ユーザーが必要な業務を遂行することを可能にします。選択権はお客様にあります。完全な管理者権限を一般ユーザーから取り戻し、アクセス権から、アプリケーションのインストール、プリンターのインストール、PowerShell の使用、その他ユーザーが必要な操作を実行する権限まで必要な場合に権限の昇格を提供しつつ、ユーザーに付与すべきではない権限は付与しないようにすることか、もしくは、完全な管理者権限を管理者のみに付与し、一般ユーザーがアクセスすべきでないコンテンツへのアクセス権を剥奪するか、それとも例えば PowerShell を使用する権限を剥奪するか、特定の機能へのアクセス権のみを提供するか…すべてはお客様次第です。管理者権限を特定のコンソールやアプリケーション、サービスやコマンドに制限し、管理者に起因するマルウェアのリスク、基幹サービスの中断、ミッションクリティカルなサービスのパフォーマンスへの影響を軽減しましょう。

## 時間と労力を節約する追加ツール

Ivanti Security Controls には、セキュリティ部門と IT 運用部門にとって、企業のセキュリティを確保する業務をさらに容易にする以下の機能も装備されています。

- **Ivanti の製品との統合＆自動化** Patch REST API：Security Controls と他の製品との統合、共有プロセスの自動化、リモートアクセスとコンソールのコントロールの提供を実現します。
- **CVE とパッチのリスト作成でセキュリティ部門と IT 運用部門間のギャップをなくす機能：**Ivanti Security Controls は、企業が使用しているベンダーを問わず、あらゆるベンダーからの脆弱性評価を取得し、CVE（Common Vulnerabilities and Exposures：共通脆弱性識別子）に関連するすべてのパッチを特定し、実環境で速やかに修正を承認できる更新プログラムのパッチリストを作成します。これは現在手動で行われているプロセスに代わるソリューションとなり、大幅な時間の節約につながります。

**お問い合せはこちら**

**www.ivanti.co.jp**

**03-5226-5960**

**Contact-Japan@ivanti.com**