Ivanti Device Control

リムーバルデバイスやリムーバルメディアの予期せぬ使用や悪意ある使用に起因するデータ漏洩は警戒レベルに達しています。Ivanti® Device Control は、リムーバルデバイスの使用状況とデータの暗号化に関するセキュリティポリシーを施行します。このソリューションは、 ホワイトリスト/「デフォルト拒否」のアプローチを使用して、デバイスとデータの管理を一元化します。さらに、物理的な手段を経路とするマルウェアの侵入を防止するための保護層を追加します。

損失や盗難からデータを保護

リモートで業務を行う社員の増加に伴い、ネットワーク外からのアクセスが求められています。一方、不測であるか悪意があるかを問わず、データ損失によってもたらされる可能性がある影響は、深刻な懸念事項であることも事実です。現在最も一般的なデータ漏洩の経路はリムーバルメディアやデバイスです。リムーバルメディアやデバイスは、ファイルコピーの制限がなく、データは暗号化されず、追跡記録もなく、中央管理もされません。Ivanti Device Control は、データ漏洩の可能性や漏洩による影響を制限しつつ、リムーバルメディアやデバイスといった生産性を向上するツールの安全な使用を可能にします。

主な特徴

ホワイトリスト/「デフォルト拒否」

許可されているリムーバルデバイスとメディアの権限を個々のユーザーやユーザーグループに割り当てます。デフォルトでは、明確に許可されていないデバイスやメディア、ユーザーによるアクセスは拒否される設定になっています。

リムーバルストレージ向けの暗号化ポリシーの施行

リムーバルデバイス（USB フラッシュドライブなど）およびリムーバルメディア（DVD、CD など）の暗号化を一元管理します。さらに、デバイスやメディアにコピーする際に暗号化ポリシーを施行します。

データコピー制限

ユーザー単位で 1 日にリムーバルデバイスやメディアにコピーできるデータ量を制限します。また、特定の時間帯や曜日に使用を制限します。

ファイルタイプの絞り込み

ユーザー単位でリムーバルデバイスやメディアに移動できるファイルタイプを制御します。マルウェアの増殖を制限する上で役立ちます。

一元化された管理/管理者の役割

ネットワーク上の許可されたリムーバルデバイスやリムーバルメディアへのユーザー、ユーザーグループ、コンピューター、コンピューターグループのアクセスを集中定義、管理します。デフォルトでは、明確に許可されていないデバイスやメディア、ユーザーによるアクセスは拒否される設定になっています。

一元化された管理/管理者の役割

ネットワーク上の許可されたリムーバルデバイスやリムーバルメディアへのユーザー、ユーザーグループ、コンピューター、コンピューターグループのアクセスを集中定義、管理します。デフォルトでは、明確に許可されていないデバイスやメディア、ユーザーによるアクセスは拒否される設定になっています。

一次アクセス権/予定アクセス権

ユーザーにリムーバルデバイスやリムーバルメディアへの一時アクセス権や予定アクセス権を付与します。これは「将来」の制限された期間のアクセス権を付与するために使用されます。

状況に応じた許可

接続状況に関わらずアクセス/使用状況のポリシーを施行状態に維持します。また、エンドポイントをネットワークに接続した状態にするか接続を切断するかをカスタマイズできます。

役割ベースのアクセス管理

Windows Active Directory または Novell eDirectory の ID（いずれも完全にサポートされています）に基づいて個々のユーザーやユーザーグループに許可を割り当てます。

改竄防止エージェント

ネットワーク上のすべてのエンドポイントにエージェントをインストールします。エージェントは、不正なアンインストールから保護されます。管理者権限が付与されたユーザーによるアンインストールであっても保護されます。この保護を無効にできるのは、デバイスコントロールの管理者のみとなります。

柔軟で拡張可能なアーキテクチャ

パフォーマンス向けに最適化された中央データベースが装備された拡張可能なクライアント–サーバーアーキテクチャを使用して、全社規模のコントロールと施行を実現します。仮想化されたサーバー構成をサポートします。

Ivanti Device Control の機能/仕組み

1.エンドポイントに現在接続されている、もしくはこれまでに接続したことのあるリムーバルデバイスすべてを**検出します**。

2.クラス、グループ、モデル、固有の ID ごとに全ての「プラグアンドプレイ」デバイスに**評価**し、ホワイトリストのアプローチを通してポリシーを定義します。

3.ファイルのコピー制限、ファイルタイプの絞り込み、リムーバルデバイスに移動されたデータに対する暗号化ポリシーの施行を**実行します**。

4.継続的なポリシー施行を保証するためすべてのポリシーの変更、管理者の操作、ファイルの移動/転送を**モニタリング**します。

5.企業や規制の方針遵守を文書化するため、デバイスとデータの使用状況について**レポートを作成**します。

「Ivanti Device Control を導入するメリットのひとつは、ホワイトリスト機能です。この機能は、許可されていない限り、プラグインの方法を問わず、すべてのデバイスを使用できない状態にします。企業のデータの盗難や、「マルウェア」侵入につながる可能性のあるフラッシュメモリ USB デバイスは、深刻なリスクとなり得ます。マルウェアは、コンピューターを使用できない状態にし、同じネットワーク上の他の PC に瞬時に感染します。Device Control は、非常に機能が充実した使いやすい製品です。だからこそ、Barclays はこのソリューションを選びました」

Barclays

ADIR デスクトップビルドチームマネージャーポール・ダグラス

Ivanti Device Control のメリット

- 損失や盗難からデータを保護
- 生産性を向上するツールの安全な使用を実現
- セキュリティポリシーの施行を強化
- アクセスを制限し正確なコントロールを実現
- 物理的な手段を経路とするマルウェアの侵入を防止 / 一元化された管理構造と分散された管理構造のマッピング
- プリンターや物理的なメディアへのファイルの転送/移動をすべてモニタリング

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