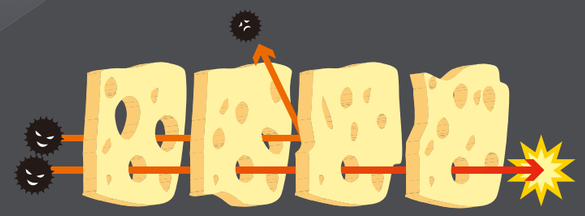
ivanti

Ivanti Application Control

ホワイトリスティングで実現する
標的型 / サイバー攻撃対策

多様化するサイバー攻撃 - 多層防御の重要性

近年、さまざまなタイプのサイバー攻撃が発生していますが、視点の異なる防御策を何重にも組み合わせることで、セキュリティリスクが発生する危険性を低減させることができます。



多層防御
＝ スイスチーズモデル

対策例 1 アプリケーション ホワイトリスティング

対策例 2 OS・アプリ セキュリティパッチ管理

対策例 3 管理者権限管理

各国政府の推奨対策

各国の情報機関においてセキュリティ対策モデルが研究されており、
下記のような研究結果が公表されています。

Australian Signals Directorate (ASD)

オーストラリア通信電子局(ASD)が掲げる サイバー攻撃への有効な対策

“企業は4つの主要な戦略(Top 4)を実行することによって、**85%の標的型攻撃**を緩和することができます。”

▶ASDが掲げるサイバー攻撃への有効な対策 TOP4

①利用するアプリケーションのホワイトリスト化
②アプリケーションに対するパッチ適用、パッチマネジメント
③OSに対するパッチ適用、パッチマネジメント
④OSや利用するアプリケーションの管理者権限の制限

(出展)https://acsc.gov.au/infosec/top-mitigations/mitigations-2017-table.htm

総務省

総務省「サイバー攻撃(標的型攻撃) 対策防御モデルの解説」(2017年)

下記3対策で**85%のサイバー攻撃**が防御可能

① アプリケーションの利用制限(ホワイトリスト化)
② アプリケーションを最新の状態に保持(セキュリティパッチ適用)
③ 管理者権限の最小化

(出典)http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000125.html

セキュリティパッチ管理だけでなく、『Ivanti Application Control』を組み合わせて

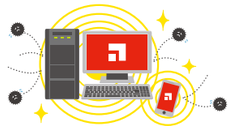
『ホワイトリスティング』『管理者権限制御』

も併せて対策すべき!!

『Ivanti Application Control』4つのメリット

1
ランサムウェアやその他の悪質な実行可能ファイルからユーザーを保護します。

2
Ivanti独自のセキュリティ技術を使用して、最も単純で最も費用対効果の高いセキュリティを実現します。

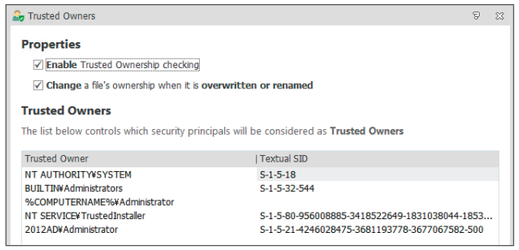


3
ユーザーが導入した指定外アプリケーションをブロックすることで、端末を望ましい状態に維持します。

4
IT部門は、日常的に必要な特権をユーザーに付与しつつ、PCから管理者権限を無くすことができます。

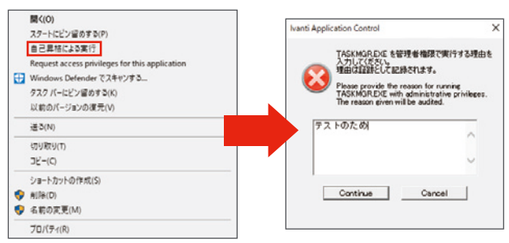
『Ivanti Application Control』の主な機能のご紹介

信頼された所有者による制御



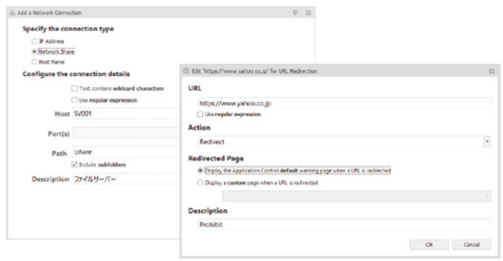
“ファイルの所有者”をチェックすることで、外部から入手した不正なファイルの実行を抑止。

実行権限の自己昇格



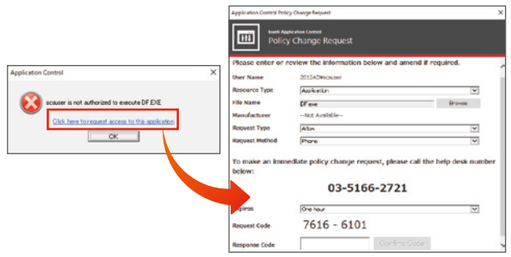
IT管理者の手を煩わせることなく、自己昇格により実行許可。ロギング機能により証跡も自動取得。

アクセス制御



特定のサーバーや共有フォルダ、Webサイトへのアクセスを制御。不正な通信をブロック。

権限の一時承認

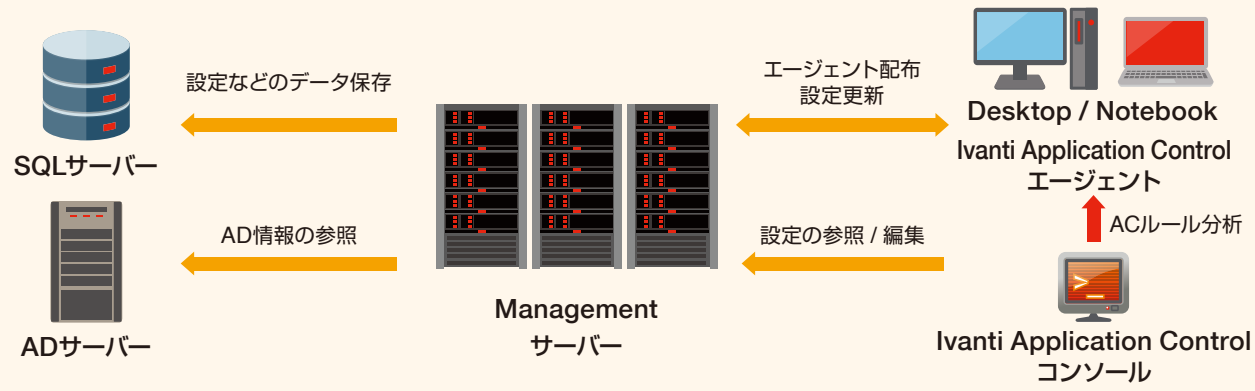


ワンタイムコードの発行により、一時的な利用許可をヘルプデスクで付与することが可能。

Ivanti Application Control 機能一覧

機能	機能概要
アプリケーション実行制御	ユーザー名やコンピュータ、グループなどの条件に基づいて、対象アプリケーションの実行を許可もしくは禁止
特権管理	ユーザー名やコンピュータ、グループなどの条件に基づいて、アプリケーションの実行権限を制御
ネットワーク接続制御	ユーザー名やコンピュータ、グループなどの条件に基づいて、対象IPアドレスやコンピュータへの接続を許可もしくは禁止
ブラウザ制御	ユーザー名やコンピュータ、グループなどの条件に基づいて、対象URLへの接続を許可、リダイレクト、Webインストールの許可を制御
アプリケーション強制終了	アプリケーションを終了するためのトリガー、動作、および警告メッセージを制御
エンドポイント分析	コンピュータにインストールされているアプリケーションの一覧および使用状況を収集
ルール分析	ACによって許可・拒否されたアプリケーションの一覧を収集し、許可・拒否された理由を確認
特権検出	管理者権限で実行されたアプリケーションの一覧を収集
自己昇格	エンドユーザー自身で実行権限を昇格、ヘルプデスクによる一時的な実行許可が可能
監査	コンピュータで発生したACに関するイベントをイベントログやファイルに出力
アーカイブ	拒否された実行可能ファイルを保護されたローカルフォルダにコピー

システム構成



【Managementサーバー要件】
CPU:2コア以上、メモリ:4GB 以上、HDD:100GB 以降
OS : Windows Server 2012 R2 以降
DB:SQL Server 2012 SP3 以降
■必須コンポーネント
・Internet Information Services (IIS)
・Background Intel igent Transfer Service (BITS)
・Microsoft .NET Framework 4.6.1
・Microsoft Visual C++ Redistributable package

【エージェント対応OS】
・Windows 7 SP1
・Windows 8.1
・Windows 10
・Windows Server 2008 R2 SP2
・Windows Server 2012
・Windows Server 2012 R2
・Windows Server 2016

製品およびご購入に関するお問い合わせ先

Ivanti製品詳細は今すぐチェック!

Ivanti