2015年2月

Windows Server® 2003/2003 R2 固定利用支援サービスのご紹介

東芝ソリューション株式会社

注）本資料は、保守が切れたOSやサーバを、そのまま継続使用することを推奨するものではありません。

1 Windows Server® 2003のサポート終了は2015年7月15日

迫るサポート終了！高まるリスク

・セキュリティリスクの増大
サポート終了後は、セキュリティ更新プログラムが提供されません。ウィルス感染による情報漏洩やシステムダウンのリスクが更に増大します。

・最新ＯＳへの移行が不安
OSのアップデートを行うとアプリケーションの互換性が心配、検証作業や、最悪の場合は改修が必要になってくるケースもあります。

・古いハードウェアの継続使用もリスク
最新のHWはWindows Server 2003/2003R2のドライバーは供給されていせん。しかし、老朽サーバーを使い続けると故障の可能性が増大、修理部品の調達も困難になります。性能、消費電力などの点でも不利です。

今すぐにはOS入替えできない、せめて時間稼ぎができないものなのか？

Windows Server 2003をそのまま利用する場合のリスク低減策として以下があります。

・P2V移行で仮想化環境へ移行（老朽化対策）
完全なローカル環境ならば、現状のWindows Server 2003の物理環境をそのままWindows Server 201２R2のゲスト環境で動作させることができます。まずは、HWの老朽対策から！

・ホワイトリストによるアプリケーション実行制御（セキュリティ対策）
ホワイトリストに登録されたアプリケーションのみ実行可能な環境を作ることができます。サポートが切れたような古いOSでも対応可能です。

2 固定利用支援サービスのメリット･デメリット

基本的には最新OSへ移行をお勧めしますが、既存のWindows Server® 2003環境を継続利用のケース

提供内容	メリット	デメリット	こんな時に選択
P2V移行＋ホワイトリスト型アプリケーション実行制御	・アプリ変更不要 ・最新HWを利用可能 定義ファイルの更新が不要なので、インターネット接続不要。 ・ブラックリスト型に比べて性能劣化が少ない。	・マクロ型ウイルス対策は不可。 ・プログラムの相性問題により動作が保証できないケースがある。	サーバー老朽化対策しつつ、既存環境をそのまま利用したい時。
P2V移行サービス	・アプリ変更不要 ・移行コストと期間が最少限 ・最新HWを利用可能	・セキュリティ脅威	サーバー老朽化対策。 最新HWでWindows Server 2003のドライバーなどがない場合に有効。短期間の経過措置クローズドシステムのみ
ホワイトリスト型アプリケーション実行制御（McAfee Application Control）	・既存環境にインストールするだけ。 ・定義ファイルの更新が不要なので、インターネット接続不要。 ・ブラックリスト型に比べて性能劣化が少ない。	・マクロ型ウイルス対策は不可。 ・プログラムの相性問題により動作が保証できないケースがある。 ・老朽化対策なし	・既存環境をそのまま利用したい時。 （後からアプリケーションの追加・変更を行うことも可能ですが、設計・設定変更作業が別途必要となります）。

3 McAfee Application Control の特徴

McAfee Application Control の特徴

McAfee Application Control の特徴
・予め実行を許可するアプリケーション（exe、dll、batなど）のみをホワイトリストに登録して実行制御するため、未知ウイルスの実行を防止することが可能となります。
・レガシーOSに対応し、WindowsNT/2000の固定利用対策として国内で数千以上の導入実績があります（現行OSに対しても、他社の同等製品と比較し圧倒的な実績有）。
・ウイルス定義ファイル（ブラックリスト）がないので誤検知の心配がありません。
・実行されたアプリケーションがホワイトリストに登録されているかどうかをチェックするだけなので、使用リソースは最小限で、既存環境への性能劣化を抑えることができます。

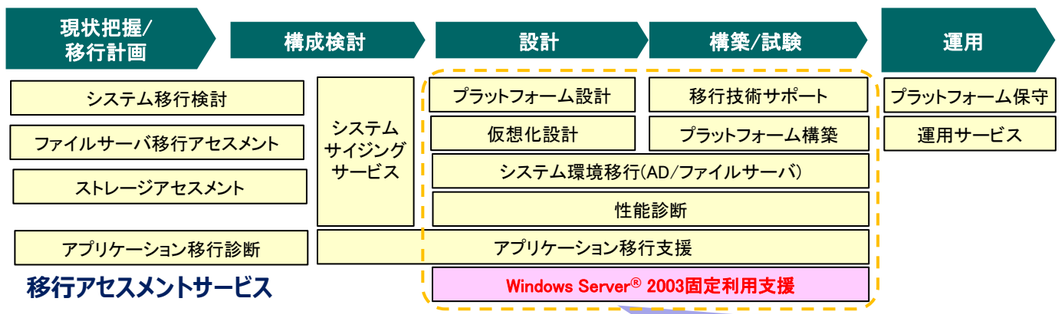
McAfee Application Control の機能
・Updater ⇒ 特定のアプリケーションにファイルの更新・変更を許可
・Trusted User ⇒ ユーザベースで実行を許可
・Trusted Directory ⇒ フォルダベースで実行を許可
・Trusted Certificates ⇒ 証明書ベースで実行を許可
・除外機能 ⇒ 実行制御対象から除外

TSOL のアドバンテージ
・東芝ソリューショングループ内で1万台の導入実績があります。
・自社実践を元にしているので、多くのノウハウや経験を蓄積した技術者によるサポートを受けることが可能です。

4 移行サービスのご紹介

サービス概要：
Windows Server® 2003/2003 R2で動作しているITシステムを、そのまま最新HWへ移行し、継続利用を可能にする有償サービスを提供します。HW老朽化対策をしたり、Windows Server® 2003/2003 R2を利用しながらセキュリティ性を付与したり利用シーンに応じたご提案をします。

アセスメントサービスの位置づけ：
弊社では、移行の各フェーズで各種サービスをご提供しております。移行アセスメントを実施後、システム環境移行の提案を実施します。



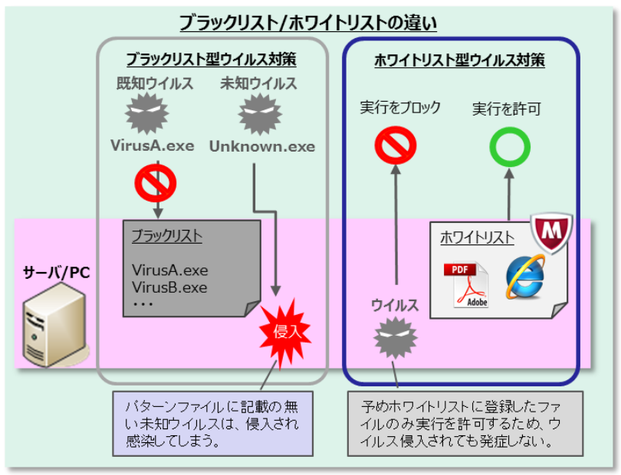
メニュー	サービス内容
P2V移行＋ホワイトリスト型アプリケーション実行制御	■現在の物理サーバーをゲストOSで動作させて、老朽化対策をしつつ、セキュリティ性を向上することができます。 下記のサービスを組みあわせたサービスです。
P2V移行サービス	■物理サーバ上の2003環境を、2012 Hyper-V仮想環境にゲストOSとして移行します。 最新ドライバーはホストのWindows Server 2012R2が対応しますので、最新HWでWindows Server 2003が動作できます。
ホワイトリスト型アプリケーション実行制御	■ **McAfee Application Control** ・当社からインストール手順書をお送りいたします。ソフトウェア自体はMcAfeeからお客様に送付されるGrant Letterに記載されているキーをご利用になり、McAfeeのホームページから直接ダウンロードしていただくことになります。 ・インストールとその後の動作確認はお客様に行っていただきます（既存環境の動作確認はお客様しか行えないため）。 ・インストール等でご不明な点がある場合は、メールベースでQ&A対応させていただきます。 ※ 既存環境に存在するアプリケーションとの干渉により、動作の保障ができない場合があります。ただし、製品の持ついくつかの機能により、干渉を回避することが可能な場合もあります（現時点ではTrendmicro社のアンチウイルス製品とは同居できないことがわかっております）。

※ ブラックリスト型ウイルス対策製品も別途ご紹介・ご対応可能です。
ただし、2015/12/31でWindows2003環境のサポートが終了となりますので、2015年末までに新HW・新OSへ移行の目途が立つ場合に限定した延命措置となります。

5 導入の流れ と 動作概要

Ｐ２Ｖ移行の構成例

Ｐ２Ｖの移行の概要:
Ｐ２Ｖ変換支援サーバーを貸出して、移転元サーバーから移転先のゲスト環境へ環境の移動を行い移行支援を行います。移行後、IPアドレスの重複対応や、サーバー名の変更など、後処理も実施します。



■ 購入前の確認

予めバックアップを取得した上で、当社からお送りする手順書に沿って評価版での事前動作確認を行ってください。評価版は指定期日がくると機能が提供されなくなりますのでご注意ください。

■ 導入の流れ

①既存のアンチウイルス製品でフルスキャンを実施し、ウイルスを駆除する。
②既存のアンチウイルス製品をアンインストールする。
③McAfee Application Control のインストール＆ホワイトリスト作成（コマンド1つでディスク内をスキャンしてホワイトリストは自動作成されます）。
④アプリケーションの動作確認を行い、必要に応じてMcAfee Application Control の機能を適用してチューニングを行う。
⑤運用開始。 ［①と②は可能なら実施していただきます］

■ ホワイトリスト型製品の挙動

インストール後にコマンド実行することで、バイナリファイル(exe,dll,sys等)やスクリプトファイル(bat,vbs等)が初期ホワイトリストとして登録され、リストにないファイルの実行はブロックされます。
ホワイトリストはハッシュ値で管理しており、同一ファイル名であってもハッシュ値が違えば異なるファイルとして認識します。また、リストにあるファイルの作為的な改ざんを防止する機能もあります。

本サービスに関するお問い合わせ： IAサーバ MAGNIAシリーズお問い合わせ窓口
http://www.toshiba-sol.co.jp/pro/magnia/contact/index.htm （MAGNIAシリーズ以外をご使用のお客様もこちらをご利用下さい）