操作ログから 未来の安心を

WEEDS

Windowsの操作ログ取得技術について

2014年1月20日更新

会社紹介

WEEDS

会社名	ウイーズ・システムズ株式会社
住所	豊島区高田1-36-10 アペックヒルズ目白３F,２F
設立	２００３年１月
代表取締役	田口 孝貴
事業内容	パッケージソフトウェア開発・販売、コンサルティング

- 連続黒字決算(創業以来全期)、自社開発(Made in Japan)
- 完全性・網羅性・正確性を持った操作ログ取得製品開発
- 金融機関を主とした多くの導入実績
- 金融向け監査・検査指針に合わせたバージョンUP無償提供
- 某大手金融機関様、パートナー様の声
  - 「オペレータの理解度によらず、操作ログをレポーティングできて、 ～中略～　オペレータにも負担をかけない、という考えのもとWEEDS製品を導入しました。」
  - 「営業担当者が製品に関して豊富な知識を持っており、問い合わせの対応も敏速で、助かっています。導入においても、インストール作業に大きなトラブルも無く、約30サーバの環境構築もあっという間でした。」
  - 「状況を伝えるだけで調査方法を提示してくれる上に、取得した情報からすぐにパッチを作成してくれるため、導入担当側としては非常に安心できました。」

Windows操作ログ製品との比較

Windows操作ログの取得手法

WEEDS

ログ取得方式	仕組み	メリット/デメリット
イベントログ取得	Windowsが出力する標準ログを取得する方法。	・コピー/移動時の正確な操作ログ取得が不可能
フォルダ監視	WindowsAPI「ReadDirectory　ChangesW」を使用して、フォルダ内の変更（ファイル作成,削除,サイズ時刻変更）を監視する方法。	・ローカルディスク以外はログ取得対象外 ・ファイルコピー、参照はログ取得対象外 ・大量のファイル操作は取り漏れが発生 ・ファイルの移動元・移動先が関連付けられない ・フォルダ削除は内部ファイルの削除が取得不可
ウィンドウタイトル取得	WindowsAPI「SetWindows　HookEx」を使用して、ウインドウの作成、終了、フォーカス移動時に、ウインドウタイトルを取得する方法。	ウインドウタイトルのみなので、ファイルアクセスの取得は別の方式で保管する必要がある
APIフック	WindowsAPI「CreateRemote Thread」を使用してWin32APIをフック。	NativeAPIを直接実行している操作(デバイスをまたがったファイル移動など)は取得不可能
NativeAPIフック	WindowsAPI「CreateRemote Thread」を使用してNativeAPIをフック。	アプリケーションへの影響がより大きい（異常終了など）

各製品が採用するWindows操作ログ取得手法

WEEDS

ログ取得方式	ログイン操作	外部アクセス	採用製品		
			ｴｰｼﾞｪﾝﾄﾚｽ型	多くの製品	WEEDS
イベントログ取得	○	○	○		EVT-Lorder
フォルダ監視	○	○		○	
ウィンドウタイトル取得	○			○	Windows-Trace WinServer-Trace
APIフック	○				Windows-Trace WinServer-Trace
NativeAPIフック	○				Windows-Trace WinServer-Trace

※ WEEDSでは“外部アクセスログ”をSMBﾊﾟｹｯﾄから取得する手法を採用して対応しています。

http://www.weeds-japan.co.jp/

WEEDSで
低コストで意味のあるITガバナンスを
実現して下さい。

人事部長