

EVENTLOG方式との比較

	項目	説明	File Server Audit(パケットキャプチャ方式)	EVENTLOG方式
基本項目	ログ解析方式		パケット解析	EVENTLOG解析
	取得方式		パケットキャプチャ	サーバ上で動作するプログラム(エージェント等)
導入関連	インストール、設定変更項目		スイッチの設定変更 + 専用PCへのインストール・設定	ファイルサーバへのインストール・設定変更 + 専用PCへのインストール・設定
	ファイルサーバへの負荷		なし	あり (取得するログ範囲に依存)
	ファイルサーバへのアクセス権	ファイルサーバへの管理権限などが必要か	一切不要	アドミニストレータ権限が必要。設定・登録が必要な場合もある。
	テスト導入の可否		フル機能評価版を提供	評価版を提供
	テスト導入時のリスク		なし	影響がある可能性あり (サーバへのインストール、設定が必要)
	不具合時の影響	万が一、ログ収集システム等に不具合があった場合の影響	ログが取得できない	ファイルサーバへの悪影響の可能性 ファイルサーバ上のメンテナンス要
	アンインストール・廃止時	利用を中止せざるを得なくなった場合	専用PCの停止または撤去	サーバ上のアンインストール + 専用PCの停止・撤去
運用関連	全ファイルへのアクセス監視	実用上の監視対象。内部統制、情報漏えい対策上、全ファイル監視が必須。	全ファイルへのアクセスを監視	サーバに負荷にならない範囲で重要ファイルのみ限定して監視
	ファイルサーバのアップグレード時	ファイルサーバを多機種(NAS等)に置き換えたり、変更する場合	基本的にそのまま利用可	再設計・購入・インストール
	クラスタリングサーバの監視		そのまま監視可能(IP単位)	クラスタ内の個別サーバごとに監視
	ログの保護 / ログへのアクセス権限	ログファイルやログ収集システムへの権限者。内部統制上、権限分離が望ましい。	ファイルサーバ管理者と完全に分離可能。	ファイルサーバ管理者が権限者。
	ステルス化	ネットワーク経由での攻撃対策	可能	不可
	Windowsサービスパックでの影響		なし	都度評価
	アラート機能	特定条件における管理者へのアラート通知	あり	?
ログ内容	コピー判別		あり	なし
	ログとユーザ操作の対応	ユーザの操作と一対一に対応したログ表示できる	一対一	一対複数
	コマンドラインアクセス		監視対象	Windows Server 2003のみ監視対象