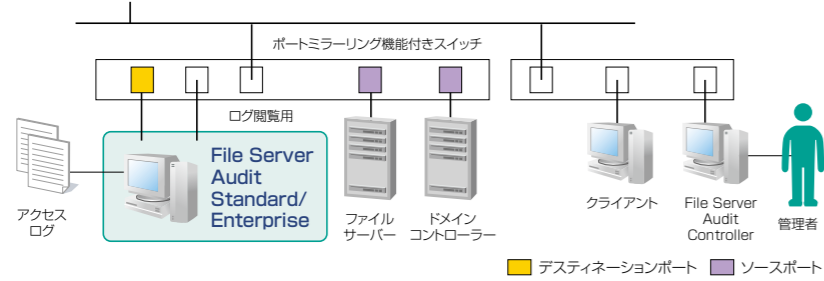


■対応環境

■構成例

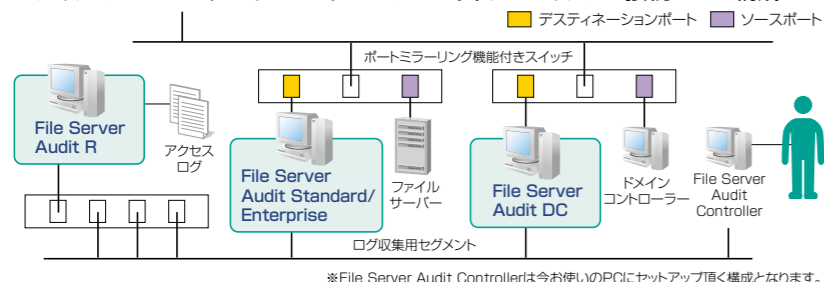
ファイルサーバーとドメインコントローラーが同一のスイッチに接続される構成



File Server Audit V2 Enterprise/Standard	
OS	Windows Server 2003/2008 (各SP1、SP2、R2)
CPU	Intel Core2 Quad以上推奨
メモリ	Enterprise版:4GB以上推奨 Standard版:2GB以上推奨
HDD空き容量	10GB以上 ※別途追加でログを保存するスペースが必要
LANカード	パケットキャプチャ用:1ポート(Intel Server Adapter推奨) ログ閲覧用:1ポート
パケットキャプチャドライバ	WinPcap 4.1.1
ソフトウェア	SQL Server 2008 R2 Express

※1000BaseTネットワークの場合、File Server Audit Standardをインストールした端末のNICの設定を100BaseTに変更することでFile Server Audit Standardは動作しますが、トラフィック量によってはパケットロスが発生する可能性があります。  
 ※同様のSQL Server 2008 R2 Expressでは、データベースのサイズが10GByte(ログ件数に換算して約500万件~2000万件)までに制限されています。File Server Audit Enterpriseをご利用される場合、より多くのログを管理されたい場合はSQL Server 2008 R2 Standard版またはEnterprise版を別途ご購入ください。

ファイルサーバーとドメインコントローラーが異なるスイッチに接続される構成



File Server Audit V2 R	
OS	Windows Server 2003/2008(各SP1、SP2、R2)
CPU	Intel Core2 Quad以上推奨
メモリ	4GB以上推奨
HDD空き容量	10GB以上 ※別途追加でログを保存するスペースが必要
LANカード	ログ受信用:1ポート(Intel Server Adapter推奨) ログ閲覧用:1ポート
ソフトウェア	SQL Server 2008 R2 Express

File Server Audit V2 Enterprise/Standard	
OS	Windows Server 2003/2008(各SP1、SP2、R2)
CPU	Intel Core2 Quad以上推奨
メモリ	2GB以上推奨
HDD空き容量	30MB以上 ※別途ログを保存するスペースが必要
LANカード	パケットキャプチャ用:1ポート(Intel Server Adapter推奨) ログ送信用:1ポート
ソフトウェア	WinPcap 4.1.1

File Server Audit V2 DC	
OS	Windows Server 2003/2008(各SP1、SP2、R2)
CPU	Intel Core2 Duo 以上推奨
メモリ	1GB以上推奨(Server2008の場合は2GB以上)
HDD空き容量	30MB以上 ※別途ログを保存するスペースが必要
LANカード	パケットキャプチャ用:1ポート(Intel Server Adapter推奨) ログ送信用:1ポート
ソフトウェア	WinPcap 4.1.1

■監視対象環境

監視対象ファイルサーバー	
OS	Windows NT以降、Windows 2003/2008 Storage Server、Samba、NetApp、EMC、他各種NAS
CPU	特に制限なし
メモリ	特に制限なし
HDD空き容量	特に制限なし

監視対象クライアントPC	
OS	Windows 2000 SP4/XP SP3/Vista/7 他
CPU	特に制限なし
メモリ	特に制限なし
HDD空き容量	特に制限なし

対応ファイルフォーマット  
 Office 2000/XP/2003/2007、PDF、text  
 その他Windows ExplorerやDOSプロンプト等で操作可能なファイル形式  
 ※アプリケーション、OS等の組み合わせによっては、1操作に対して複数回のログが出力される可能性があります。ログの収集自体には問題ございません。

対応ネットワーク  
 10/100/1000BaseT(File Server Audit Enterprise)  
 10/100BaseT(File Server Audit Standard)

※File Server Audit V2 Enterprise/Standardは下記ソフトウェアを使用しています。パケットキャプチャドライバ Win Pcap、セキュリティファイアウォール、SQL Server 2008 R2 Standardが必須です。  
 ※SQL Server 2008 R2 Express、Microsoft .NET Framework はインストーラーに含まれます。

■出力ログ

ログ出力項目	
No	解析したログの番号を表示 番号はシステムが自動的に付与
日時	ログが出力された日時を表示
グループ名	管理者が登録したグループ名を表示
登録ユーザー名	管理者が登録したユーザー名を表示
アカウント名	自動検出したアカウント名を表示
クライアントマシン名	クライアントPCのマシン名を表示
クライアントIP	クライアントPCのIPアドレスを表示
クライアントOS	クライアントPCのOSを表示
サーバー名	ファイルサーバーのマシン名を表示
サーバーIP	ファイルサーバーのIPアドレスを表示
サーバーOS	ファイルサーバーのOSを表示
アクション	該当ログのアクションを表示
フォルダー名	アクションが発生したフォルダー名を表示
ファイル名	アクションが発生したファイル名を表示
ファイルサイズ	ファイルサイズを表示

アクション内容  
 ■選択 ■読み込み ■書き込み ■コピー ■作成  
 ■削除 ■名前変更 ■印刷 ■フォルダー作成 ■フォルダー削除  
 ■ログオン ■ログオフ ■ログオン失敗 ■ドメインログオン  
 ■ドメインログオン失敗 ■アクセス拒否

※"選択"は取得できない場合があります。  
 ※"選択"と"読み込み"は判別できない場合があります。  
 ※"印刷"はSMB/ネットワークがファイルサーバーに流れる場合のみ出力されます。  
 ※"コピー"はクライアントファイルサーバー間のOSおよびアプリケーションの組み合わせによっては、出力されない場合があります。  
 ※サーバーOS、クライアントOSはネットワーク環境によっては取得できない場合があります。  
 ※アカウント名、マシン名を取得するには、ドメインコントローラーも監視対象とする必要があります。  
 ※ファイルサイズは、アクションが"コピー"と"読み込み"の場合のみ出力されます。  
 ※ファイルサイズが取得できない場合は、ファイルサイズには0が出力されます。

■価格

●File Server Audit Standard 396,000円~

- ・10/100BaseT対応
- ・監視対象サーバー1台の価格となります。
- ・価格はクライアントPCの台数には依存しません。

※記載の価格はライセンス費のみです。年間サポート費、初期設定費等は含まれません。 ※年間サポート費は初年度必須です。 ※記載の価格には消費税は含まれておりません。  
 ※製品の仕様・機能は予告なく変更する場合がありますので、ご了承下さい。記載されている会社名・商品名などの固有名称・ロゴは、各社の商標または登録商標です。

●File Server Audit Enterprise 2,500,000円~

- ・10/100/1000BaseT対応
- ・監視対象サーバー1台、クライアントPC100台の価格となります。
- ・監視対象ファイルサーバーの台数、クライアントPCの台数によって価格が異なります。



東京：〒163-0777 東京都新宿区西新宿2-7-1 小田急第一生命ビル  
 TEL. 03-3342-0992 FAX. 03-3342-0956

大阪：〒541-0043 大阪市北区堂島1-6-20 堂島アバンザ  
 TEL. 06-6442-1314 FAX. 06-6442-1316

名古屋：〒450-6213 名古屋市中村区名駅4-7-1 ミッドランドスクエア13F  
 TEL. 052-563-0232 FAX. 052-563-0233

E-mail: fsa@nsd.co.jp

http://www.nsd.co.jp/service/fsa/

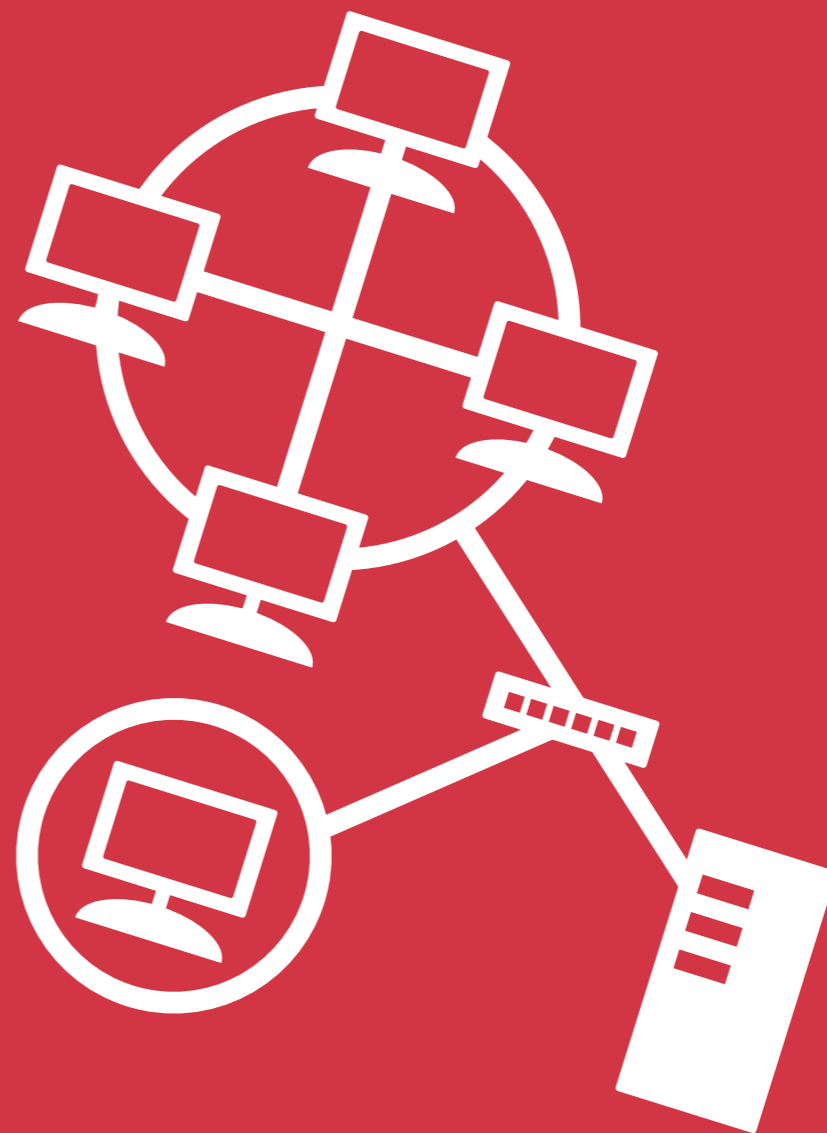
0906-03000(2)

本当に使える!

ファイルサーバーの情報漏洩対策なら、「エージェントレス」「コピー」「クライアント情報」が決め手!

ファイルサーバー専用アクセス監視ツール

Access Log Analyze & Management System  
**File Server Audit**



使える!

1 情報漏洩対策に必須!

ファイルコピーやアカウントの不一致がわかる!

使える!

2 真のエージェントレス!

パケットキャプチャ型でサーバーにもクライアントにも影響ゼロ!

使える!

3 各種NASにもオールマイティ対応

Windowsはもちろん、NASが混在する環境でもOK!



本当に使える!

ファイルサーバー専用アクセス監視ツール

# Access Log Analyze & Management System File Server Audit

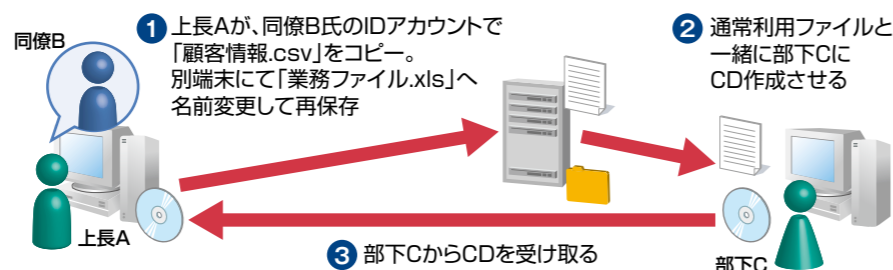
使える!

## 1 ファイルコピーやアカウントの不一致がわかる!

■御社のログは有事の際に活用できますか?

「とりあえずログを取得」すれば良かったのはもう過去の話です。アカウントの不正利用はないのか、データのコピーはしていないのか? ファイルサーバー上のデータが漏洩してしまった時、アクセスログに「コピー」や「クライアントIP」が記録されていないから...御社では有効な対応が取れますか?

例えば、このような方法で情報漏洩した場合...



File Server Auditなら、不正アクションがログからわかる!

クライアントIPアドレス	クライアントコンピューター名	ユーザーアカウント	アクション	ファイル名	ファイルサイズ
192.168.1.20	上長A	同僚B	コピー	顧客情報.csv	*300M/バイト
192.168.1.20	上長A	同僚B	作成	業務ファイル.xls	
192.168.1.25	部下C	部下C	読み込み	ファイルA	500K/バイト
192.168.1.25	部下C	部下C	読み込み	ファイルB	200K/バイト
192.168.1.25	部下C	部下C	読み込み	業務ファイル.xls	*300M/バイト
192.168.1.25	部下C	部下C	読み込み	ファイルC	125K/バイト

クライアントコンピューター名とユーザーアカウントの不一致!

大容量の顧客情報.csvをファイルサーバー外へコピー

ファイル名、サイズが同じ

大容量ファイルの読み込み

監査イベント利用型では...

クライアントIPアドレス	クライアントコンピューター名	ユーザーアカウント	アクション	ファイル名	ファイルサイズ
192.168.1.20	同僚B	同僚B	Read	顧客情報.csv	
192.168.1.20	同僚B	同僚B	Write	業務ファイル.xls	
192.168.1.25	部下C	部下C	Read	ファイルA	
192.168.1.25	部下C	部下C	Read	ファイルB	
192.168.1.25	部下C	部下C	Read	業務ファイル.xls	
192.168.1.25	部下C	部下C	Read	ファイルC	

ログを見ても一連の日常業務にしか見えない

わからない!

使える!

## 2 真のエージェントレス!「負荷ゼロ」だから使える!

■エンドユーザーに負担をかけない

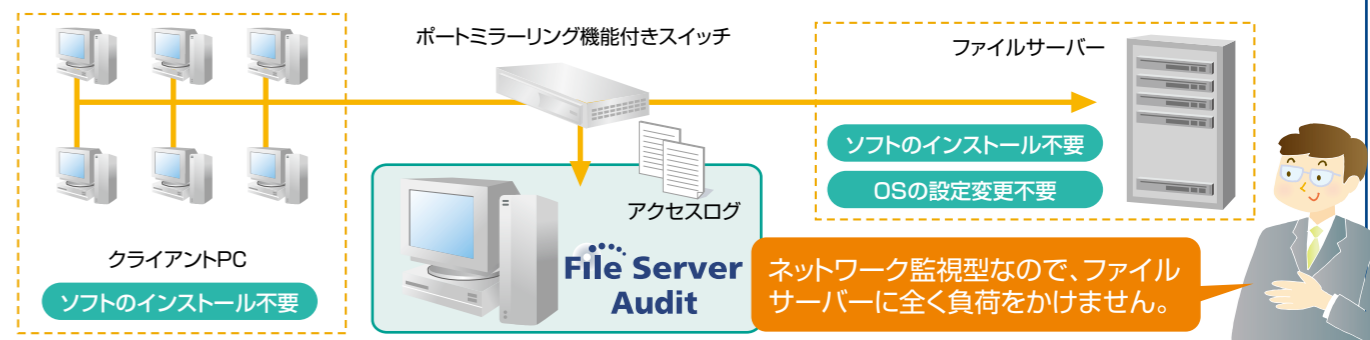
「クライアントエージェント型」の場合、クライアントPCにソフトをインストールする必要があり、他のソフトの動作が不安定になるなどの問題も考えられます。File Server Auditの場合、ソフトのインストールが不要であるため、こういったエンドユーザーに対する負担は発生しません。

■ファイルサーバーへの影響ゼロ

「イベントログ収集型」のツールでは、ファイルサーバー自体で監査ログを収集し、それを解析した結果をアクセスログとして記録します。この監査ログはファイルサーバーの機能を利用して収集するため、導入時にファイルサーバーの設定を変更する必要があります。また、アクセスの多い環境では、ファイルサーバー自体に負荷がかかり、ファイルサーバーのレスポンスが悪くなる可能性があります。File Server Auditは、ネットワークパケットを監視する方式ですので、ログを収集する際にファイルサーバーのリソースを一切使用しません。そのため、ファイルサーバーに余分な負荷をかけることもありません。

■短時間で導入が完了し、運用コストも抑制できる

導入は、専用PCとポートミラーリング機能付きスイッチを設置するだけ。導入時間を大幅に抑えることができます。



使える!

## 3 Windowsサーバーはもちろん、各種NASにも使える!

■各種NASに対応

SMB/CIFSのプロトコルで接続していればファイルサーバー側のOSは問いません。複数のOSが混在する環境や、異なるメーカーのNASにリプレースしても、ログを取得することが可能です。



### 使いやすい過去ログ検索機能

過去ログをさまざまな条件指定で抽出可能。検索結果表示までをマウスのみで行うことが可能です。

土日の深夜11:00~03:00のログだけを抽出するなど、きめ細かな条件を指定できます。また、検索条件をファイルに保存し、再利用することができますので、毎回検索条件を指定しなおす必要がありません。

検索結果は操作の内容毎に色分けして表示できますので、注意すべき操作を直感的に識別できます。



### リアルタイムアラート通知機能

指定した条件に一致するアクセスをメールで通知。不正な持込PCの検出にも有効です。

あらかじめ指定した条件に一致するアクセスがあった場合、管理者にメールでアラートを通知する機能を装備しています。通知条件は、ユーザー名、ファイル名、ディレクトリ名、アクションなどを指定できます。

非登録PCのアクセスにアラートを設定しておけば、不正アクセス対策としても有効になります。



### レポートングオプション

急激なアクセス増加やコピーアクションの急増などを視覚的に把握。平常時の傾向を把握し、日々の状況をチェックすることが、異常値の発見を助けます。

アクセス総数やアクセスランキングを、アクション別、ユーザー別、ファイル別に分かりやすくダッシュボードに表示します。アクセスランキングで気になる項目があれば、明細データにドリルスルーできます。

