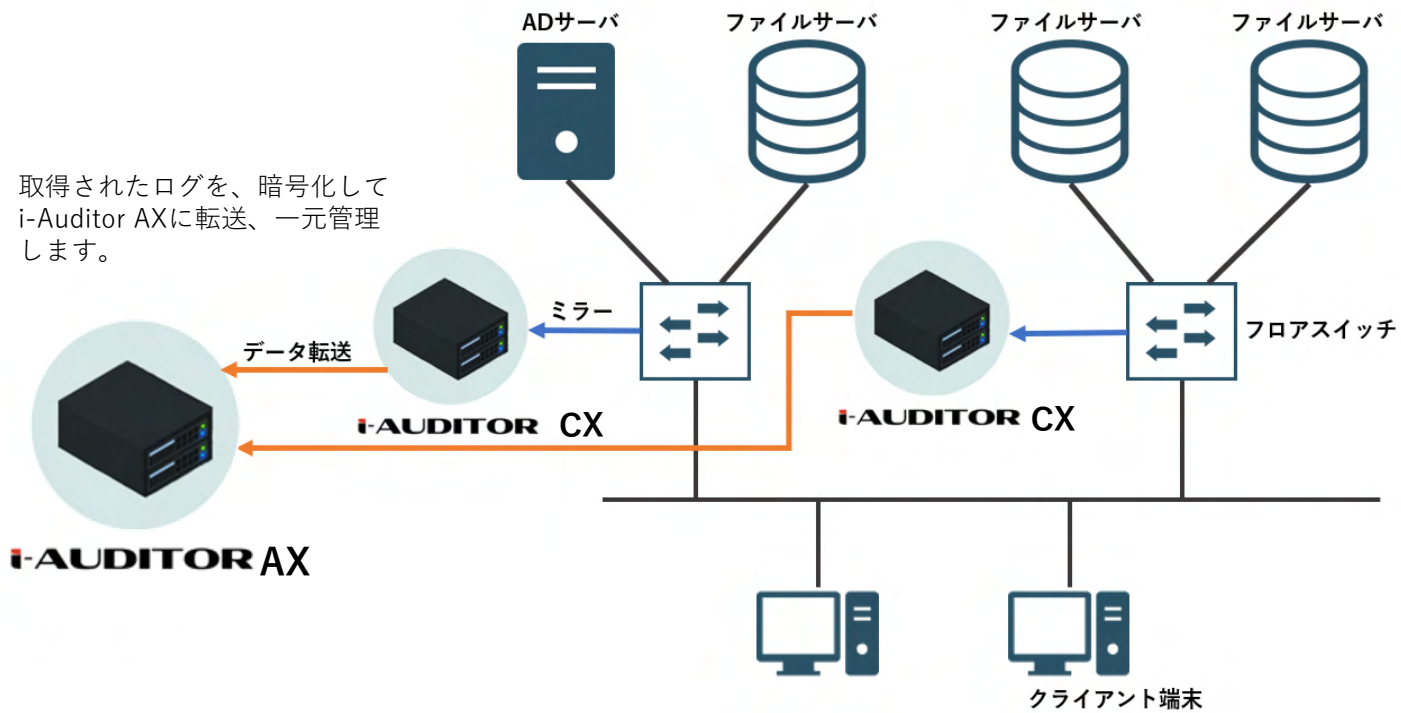


POINT 5 集中管理・冗長化に対応



i-Auditor CX: Capture。パケットを取得し、ログを抽出します。
 i-Auditor AX: Analyzer。抽出されたログを収集し、一元管理します。

ミラーしたトラフィックを分流することで、ポートを追加で使わず冗長化が可能です。

対応環境

i-Auditor ログ出力項目

日時	ユーザ操作が検知された日時
ファイルサイズ	操作が行われたファイルのサイズ
ユーザ名	操作を行ったユーザのアカウント名
クライアントIP	操作を行った端末のIPアドレス
サーバ名	操作が行われたサーバのクライアント名
サーバOS	操作が行われたサーバのOS種別
UNCパス	操作が行われたファイルのパス
操作	ユーザが行った操作の内容
クライアント名	操作を行った端末のクライアント名
クライアントOS	操作を行った端末のOS種別
サーバIP	操作が行われたサーバのIPアドレス

※ i-Auditor のログは、ログサーバに転送できます。

i-Auditor 監視対象環境

対応プロトコル	Kerberos 5(88/tcp), SMB(445/tcp)
対応SMBバージョン	SMB 2.0、2.1、3.0、3.02、3.11*1
対応サーバOS	Windows Server 2012 R2, Windows Server 2008, Linux, VMWare, KVM, Hyper-V

※1: SMB3.xについては、暗号化機能を無効にしている場合のみ監視可能です。

i-Auditor 提供形態

対応形態	アプライアンス, 仮想イメージ(ISOファイル)
------	--------------------------

情報セキュリティ株式会社

〒650-0012 神戸市中央区北長狭通4丁目9-26 西北神ビル3・8階
 TEL: 078-381-8980 (10:00~17:00 土・日・祝除く)
 FAX: 078-381-8979
 E-mail: inquiry@isec.ne.jp URL: https://isec.ne.jp

※本誌掲載の内容は、予告なく変更になる場合があります。
 (2021年11月作成)



i-AUDITOR

ファイルサーバアクセスログ収集ツール

検索結果一覧

日時	UNCパス	サイズ [KB]	操作	ユーザ名	クライアント名	クライアントIP	クライアントOS	サーバ名	サーバIP	サーバOS
2021/10/01 11:22:11	\\fs01\部門02_マーケティング部\2021年度\製品紹介資料\20200318_製品マニュアル.pdf	140	読み取り	Naoto_Ito	PC-0217	192.168.102.21	Windows 10 Version 2004	fs01	192.168.40.80	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:25:43	\\fs01\部門02_マーケティング部\2021年度\製品紹介資料\20200318_製品マニュアル.pdf	142	書き込み	Naoto_Ito	PC-0217	192.168.102.21	Windows 10 Version 2004	fs01	192.168.40.80	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:26:19	-	-	ログオン	Yusuke_Hasimoto	PC-0148	192.168.101.43	Windows 10 Version 2004	fs01	192.168.40.80	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:28:03	\\fs02\部門03_人事部\会社説明会資料\20210218_2021年度会社紹介資料.ppt	30	読み取り	Takahumi_Tanaka	PC-0320	192.168.103.62	Windows 10 Version 2004	fs02	192.168.40.81	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:34:57	\\fs02\部門03_人事部\会社説明会資料\20210218_2021年度会社紹介資料.ppt	30	書き込み	Takahumi_Tanaka	PC-0320	192.168.103.62	Windows 10 Version 2004	fs02	192.168.40.81	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:42:34	\\fs01\部門01_総務部\2021年度\事業計画\計画書\20210924_事業計画書.xlsx	42	読み取り	Yoshihiro_Sato	PC-0106	192.168.101.19	Windows 10 Version 2004	fs01	192.168.40.80	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:43:51	-	-	ログオフ	Toru_Makino	PC-0436	192.168.104.43	Windows 10 Version 2004	fs02	192.168.40.81	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:45:15	\\fs01\部門01_総務部\2021年度\事業計画\計画書\20210924_事業計画書.xlsx	42	コピー	Yoshihiro_Sato	PC-0106	192.168.101.19	Windows 10 Version 2004	fs01	192.168.40.80	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:45:15	\\fs01\部門01_総務部\2021年度\事業計画\計画書\20210924_事業計画書 - コピー.xlsx	42	ファイル作成	Yoshihiro_Sato	PC-0106	192.168.101.19	Windows 10 Version 2004	fs01	192.168.40.80	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:51:03	-	-	ドメインログオン	guest_user	DESKTOP-007	192.168.45.125	Windows 10 Version 2004	fs02	192.168.40.81	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:52:57	\\fs02\部門04_情報システム部\製品開発\開発計画\20201128_課題管理表.doc	47	読み取り	Aya_Yamamoto	PC-0419	192.168.104.37	Windows 10 Version 2004	fs02	192.168.40.81	Windows 8.1/Windows Server 2012 R2
2021/10/01 11:52:57	\\fs02\部門04_情報システム部\製品開発\開発計画\20201129_スケジュール計	62	読み取り	Aya_Yamamoto	PC-0419	192.168.104.37	Windows 10 Version 2004	fs02	192.168.40.81	Windows 8.1/Windows Server 2012 R2



エージェントレスでスムーズに導入
不正操作の監視やサイバー攻撃の検知に



i-AUDITOR

ファイルサーバアクセスログ収集ツール

このようなニーズにお応えします

不審な操作に関連するログを取得したい

豊富な検索オプションにより、特定の操作に関連するログを絞り込んで表示できます。また、ログをCSV出力し、さらなる分析を行うことも可能です。

スピーディなサーバのアクセス監査を行いたい

ミラーポートに設置するだけで導入が完了するため、既存のネットワークへの影響を考慮する必要がありません。設置後すぐにアクセスログの取得を開始できます。

Windows 7/XP搭載の端末を排除したい

ネットワーク上の、脆弱性がある古いWindows OSバージョンの端末を簡単に検出できます。

全ての拠点のファイルサーバを一元管理したい

同時に複数のサーバを監視することができます。出先拠点（支店、支社等）までを含めた、複雑かつ大規模なネットワークにも、柔軟に対応します。

これまでのログ収集ツールになかった機能を搭載

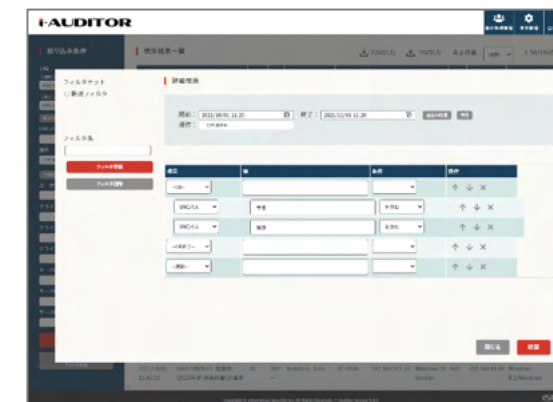
ログの集約機能、操作の判別機能を強化し、従来製品にない快適な使い勝手を実現しました。見やすく・使いやすい仕様で、ログ解析にかかる時間を大幅に短縮できます。

<一般的なログ収集ツールとの比較>

機能	一般的なログ収集ツール	i-Auditor
操作内容の判別	ユーザの行った操作が「読み取り」「書き込み」のような少数のログの組み合わせで表示される	作成、削除、コピーなどの細分化されたログが表示される → 操作したユーザとその内容が一目で確認できる → ログの件数が大幅に削減されることで、見落としを防ぎ、調査時間も短縮できる
操作対象の判別	操作内容のみが表示され、種別はファイル名から判断	操作対象がファイルかフォルダか判別して表示される → ファイル種別に応じた対応ができる
ユーザの操作に関連する情報の記録	ユーザ名のみ	ユーザ名に加え、クライアント名とサーバ名の情報も記録される → アカウント名とクライアント名の不一致が判明する

POINT ① 優れた操作性

- **インシデント調査時間を大幅削減**
実際に通信が行われたログのみが表示されます。ログの識別作業が不要となり、インシデント発生時、ログの解析や監査にかかる時間を大きく削減できます。
- **直観的なインターフェース**
専門的な知識がなくても理解しやすい仕様となっており、経験の浅い担当者でも、迅速に対処できます。
- **OS情報やユーザ名の検出**
OS情報やユーザ名を検出し、フィルタ設定することで、脆弱性があるOSを抽出したり、特定ユーザのふるまいを確認したりすることができます。



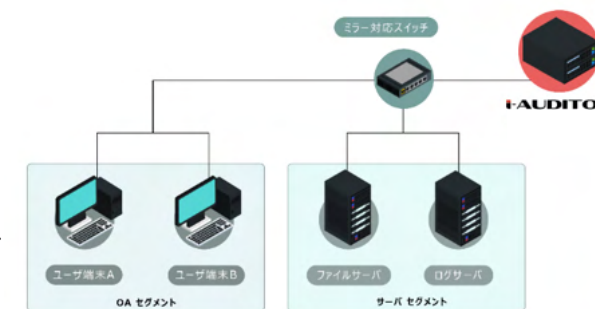
詳細な検索条件を設定し、ログを過不足なく抽出することができます。

POINT ② リアルタイムでのモニタリング機能とアラート機能

- **モニタリング機能**
機密性の高いファイルサーバへのアクセス状況を、リアルタイムに確認できます。
- **アラート機能**
事前に「不正アクセス」について定義し、アラート通知設定を行うと、不正アクセス発生時、リアルタイムで管理者へ通知メールが届きます。他の条件での通知も選択できます。

POINT ③ 導入のスムーズさ

- **スピーディーな導入を実現**
導入は、ミラー設定されたスイッチに接続するだけで完了します。
- **サーバやPCの設定変更は不要**
サーバの通信パケットを監視対象としているため、サーバ上での設定は不要です。また、クライアントPCへのソフトウェアインストールも必要なく、エージェントレスでの運用が可能です。



※i-Auditorのログは、ログサーバに転送することができます。

POINT ④ 監視対象の広さ



- **あらゆるサーバ種別に対応**
ファイル共有プロトコルである、SMBによる通信を監視対象としているため、OSの種別を問わず対応可能です。
- **複数のサーバを一台で監視**
スイッチ配下すべてのファイルサーバを監視対象とするため、一台のi-Auditorで、複数のサーバに対するアクセスをモニタリングできます。