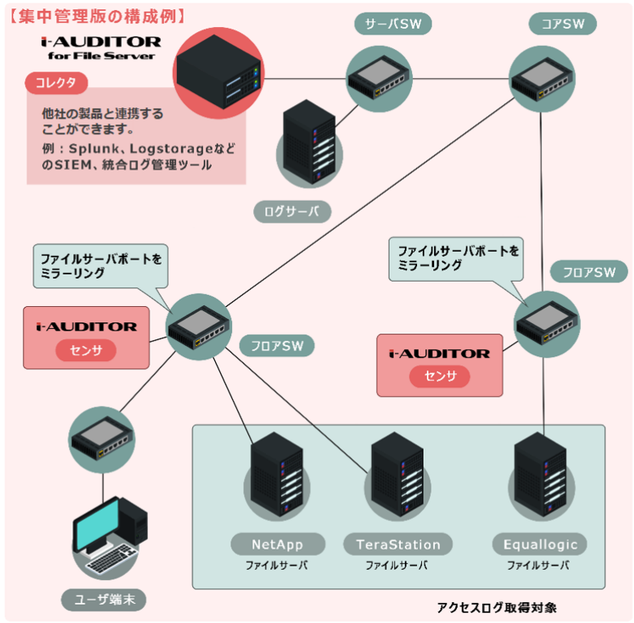
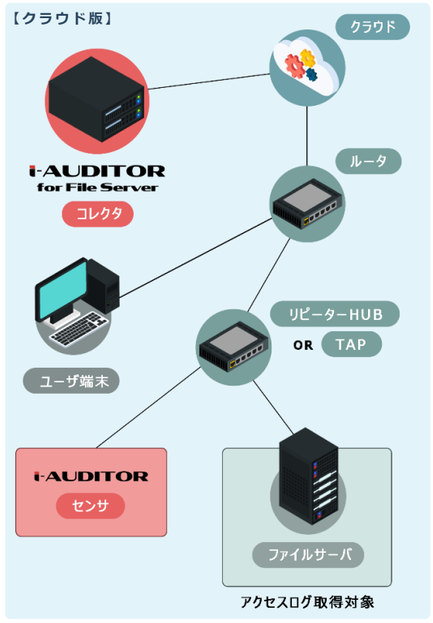
POINT ⑤ 集中管理（オンプレミス）・クラウドに対応



各センサが取得した情報をコレクタに集めることで、ログを一元管理します。



センサでの取得されたログを、暗号技術を用いてクラウド上のコレクタに格納します。

対応環境

■ **i-Auditor for File Server ログ出力項目 (*1)** ※1 i-Auditorのログは、ログサーバに転送できます。

日時	ユーザ操作が検知された日時	ファイル名	アクションが発生したファイル名
クライアントIP	クライアントPCのIPアドレス	サイズ	ファイルサイズ
サーバIP	ファイルサーバのIPアドレス	クライアント名	クライアントPC名
ユーザ名	ユーザアカウント名	サーバ名	ファイルサーバ名
操作	ユーザによる該当操作の表示	クライアントOS	クライアントPCのOS種別
共有名	操作が行われた場所	サーバOS	ファイルサーバのOS種別
プロトコル	プロトコル種別		

■ **i-Auditor for File Server 監視対象環境**

対応プロトコル	SMB/CIFS
対応SMBバージョン	SMB 1.0(*2)、2.0、2.1、3.0、3.02、3.11
対応サーバOS	Windows Server 2012 R2, Windows Server 2008, Linux, VMWare, KVM, Hyper-V

※2 SMB 1.0については、脆弱性があるためファイルサーバ側の設定を無効にしておくことを推奨します。

■ **i-Auditor for File Server 提供形態**

対応形態	アプライアンス

年間ライセンス価格

i-Auditor Platform	無料	ガバメント向け（官公庁や教育機関など）	20%　割引
i-Auditor for File Server	1,250円／人	i-Auditor for DHCP Server	500円／人
i-Auditor for Active Directory	500円／人		

※ ライセンスの最小販売数（最小利用人数）は、200人です。長期契約による最大２０%の割引きがあります。

iSEC information security inc.

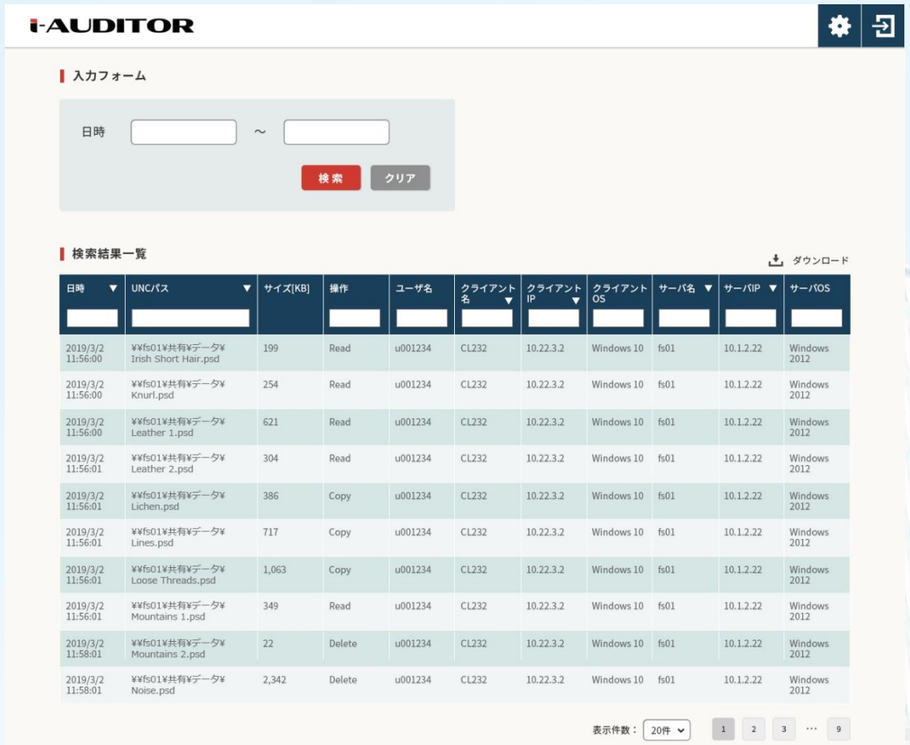
情報セキュリティ株式会社

〒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

i-CYBERTECH 関連製品

i-AUDITOR for File Server

ファイルサーバアクセスログ収集ツール



エージェントレスでスムースに導入
不正操作の監視やサイバー攻撃の検知に

iSEC information security inc. 情報セキュリティ株式会社

i-AUDITOR for File Server

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

Windows XP, 7搭載の端末を排除したい

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

スピーディにサーバアクセス状況を確認したい

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。

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。

接続端末をリアルタイムで把握したい

リアルタイム、あるいは指定した期間で、IPアドレス・コンピュータ名・OS情報・ユーザ名を取得することができます。また、特定の場所にアクセスした場合に、管理者にアラート通知することができます。

これまでのログ収集ツールになかった機能を搭載

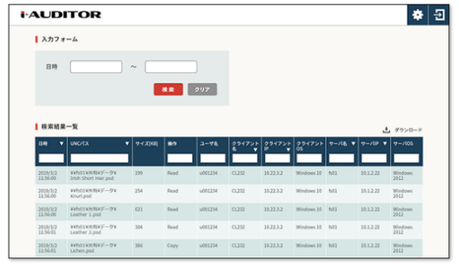
ログの集約機能、操作の判別機能を強化し、従来製品にない快適な使い勝手を実現しました。見やすく・使いやすい仕様で、ログ解析にかかる時間を大幅に短縮できます。

<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 for File Server
ログの集約	一つの操作が複数のログに記録されるため、ユーザの挙動を把握するのが困難	PC利用者が実際に行った操作が集約され、ログとして記録される → **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**
ファイルサーバ上での操作の判別	ファイルサーバ上でファイル・フォルダーがコピーされた際、操作履歴上では「読み取り」表示される	「コピー」や「読み取り」などの操作を判別できる → **操作履歴が正しく出力される**
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ント名の不一致が判明する**

POINT ❶ 優れた操作性

- **インシデント調査時間を大幅削減**
  ユーザ操作に無関係なログは表示されません。
  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。
- **Windows OS情報やユーザ名の検出**
  Windows OS情報やユーザ名を検出し、フィルタ設定することで、脆弱性が存在するOSや、特定ユーザのふるまいを検出したりすることができます。また、OS情報はビルド番号のレベルで検出することが可能です。



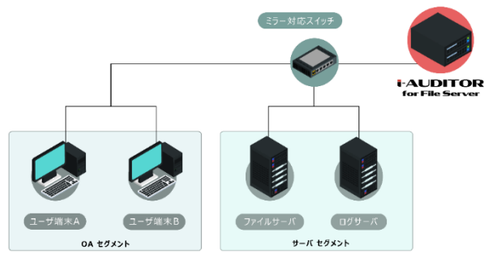
複数の条件を組み合わせ、必要な情報のみを抽出することができます。

POINT ❷ 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 ❸ 導入のスムースさ

- **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、エンドユーザに負担をかけません。



※i-Auditor for File Serverのログは、ログサーバに転送することができます。

POINT ❹ 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やCIFS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 for File Server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。