## 価格

i-Auditor シリーズには、オンプレミス版、クラウド版、二つの仕様があります。価格は同一です。
契約は単位は原則として一年間で、翌年契約を更新する場合は、新たにライセンス購入が必要となります。

【基本利用料金】

| | | |
|---|---|---|
| i-Auditor Platformシステム利用料 | | 無料 |
| 年間利用価格（1ユーザあたり） | for File Server | 1,500円 |
| | for Active Directory | 500円 |
| | for DHCP Server | 500円 |

【教育機関・官公庁向け利用料金】

| | | |
|---|---|---|
| i-Auditor Platformシステム利用料 | | 無料 |
| 年間利用価格（1ユーザあたり） | for File Server | 1,200円 |
| | for Active Directory | 400円 |
| | for DHCP Server | 400円 |

【参考価格（基本利用料金）】

| ユーザ数 | for File Server | for Active Directory | for DHCP Server |
|---|---|---|---|
| 500 | 750,000 | 250,000 | 250,000 |
| 1,000 | 1,500,000 | 500,000 | 500,000 |
| 5,000 | 7,500,000 | 2,500,000 | 2,500,000 |
| 10,000以上 | お問い合わせください | | |

※ライセンスの最少販売数（最少利用人数）は、500です。長期契約による最大20%の割引きがあります。
※ライセンスは、ファイルサーバ、アクティブディレクトリ、DHCPサーバそれぞれに通信可能な人数分購入する必要があります。


**情報セキュリティ株式会社**

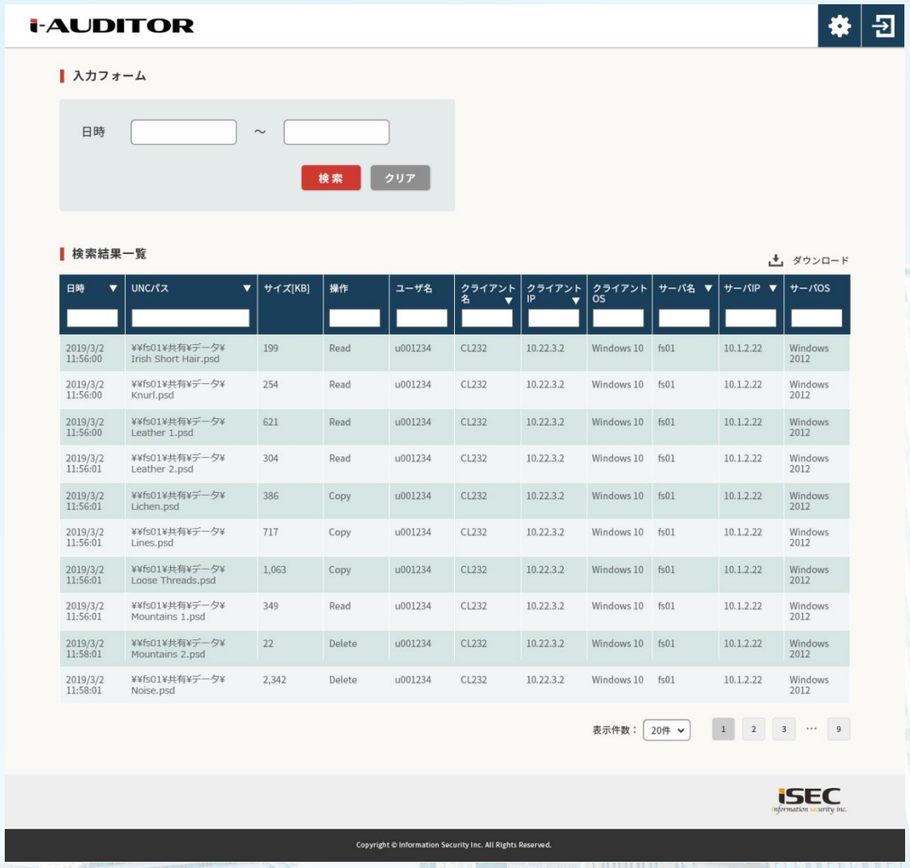
〒650-0012 神戸市中央区北長狭通4丁目9-26　西北神ビル3・8階
TEL：078-381-8980（10:00～17:00　土・日・祝除く）
FAX：078-381-8979
E-mail：inquiry@isec.ne.jp　URL：https://www.isec.ne.jp




i-CYBERTECH 関連製品

サーバログ管理ツール

# i-AUDITOR Platform




## i-Auditor Platformとは

台帳管理とアラート通知の機能を備えたプラットフォームです。
for File Server、for Active Directory、for DHCP Serverという
三つのモジュールを組み合わせることで、容易に端末管理や不正操作の
取り締まりを行うことができます。


**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

### サポート切れのWindows OS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 を及ぼさず、ファイルサーバアクセスログを取得することができます。

### 組織全体のアクセスログを一元管理したい

同時に 複数のファイルサーバへのアクセスを監視することができます。また、出先 拠点（支店、支社等 ）へのアクセスログを取得することが可能です。

### 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>**

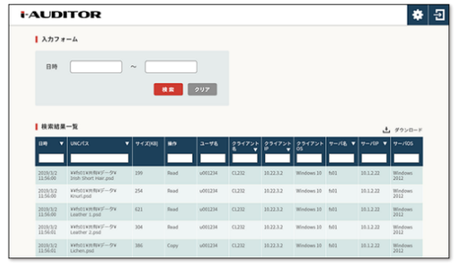
| 機能 | 一般的なログ収集ツール | i-Auditor for File Server |
|---|---|---|
| ログの集約 | 一つの操作が複数のログに記録されるため、ユーザの挙動を把握するのが困難 | PC利用者が実際に行った操作が集約され、ログとして記録される<br>→ **操作したユーザとその内容が一目で確認できる**<br>→ **ログの件数が大幅に削減されることで、見落としを防ぎ、調査時間も短縮できる** |
| ファイルサーバ上での操作の判別 | ファイルサーバ上でファイル・フォルダーがコピーされた際、操作履歴上では「読み取り」表示される | 「コピー」や「読み取り」などの操作を判別できる<br>→ **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<br>→ **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。
※本機能は、for Active Directoryとの連携により有効となります。




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

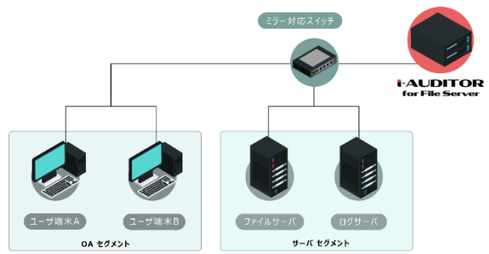
■ **モニタリング機能**
機密性の高いファイルサーバへのアクセス状況を、リアルタイムに確認できます。

■ **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。



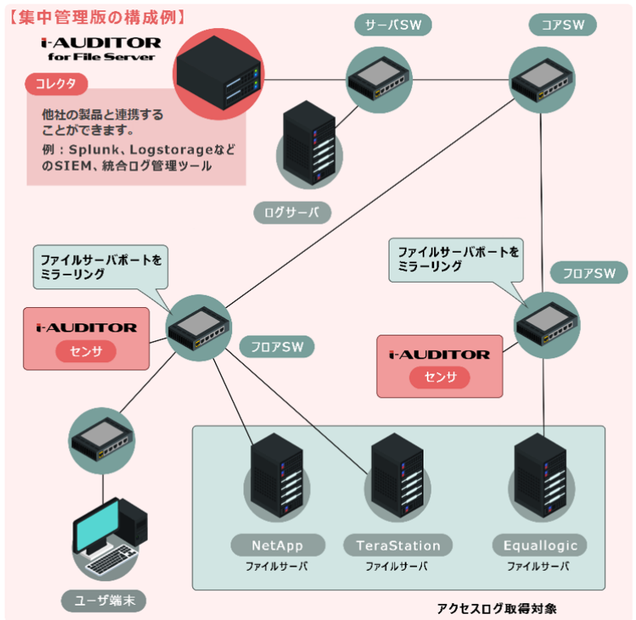

※i-Auditor for File Serverのログは、ログサーバに転送することができます。

## POINT ❹ 監視対象の広さ

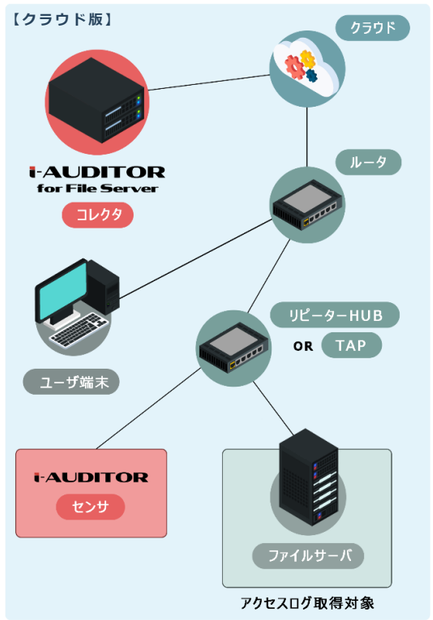

■ **あらゆるサーバ種別に対応**
ファイル共有プロトコルである、SMBやCIFSによる通信を監視対象としているため、OSの種別を問わず、対応可能です。

■ **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。

## POINT ❺ 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。

## i-Auditor for File Server 対応環境

### ■ i-Auditor for File Server ログ出力項目 (*1)

| | | | |
|---|---|---|---|
| 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 |

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

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

| | |
|---|---|
| 対応プロトコル | SMB(139/tcp) / CIFS(445/tcp) |
| 対応SMBバージョン | SMB 1.0(*2)、2.0、2.1 |
| 対応サーバOS | Windows 2019, Windows Server 2012 R2, Windows Server 2008, Linux |

*2 SMB 1.0については重大な脆弱性が存在するため、ファイルサーバ側にて無効にすることを推奨

### ■ i-Auditor for File Server 提供形態

| | |
|---|---|
| 種別 | アプライアンス |

## 姉妹製品（モジュール）紹介

# for Active Directory

エージェントレスなファイルサーバユーザの資産管理補助ツールです。ドメインにアクセスした端末のログイン情報をパケットから取得して表示します。姉妹製品の「i-Auditor for File Server」と組み合わせることで、ファイルサーバーへの操作の完全なログを取得できるようになります。

# for DHCP Server

DHCPサーバが行っているIPアドレス管理を記録できます。どのホストがサーバに対して要求を行ったのか、そして、その要求がどう処理されたのかを追跡することができます。 他のi-Auditorシリーズ同様、完全なエージェントレス仕様です。

## for Active Direcotry / for DHCP Server 対応環境

### ■ i-Auditor for Active Directory ログ出力項目

| | | | |
|---|---|---|---|
| IPアドレス | クライアントのIPアドレス | ドメイン名 | 使用ユーザが参加しているドメイン |
| クライアント名 | クライアントPCのホスト名 | ユーザ名 | ログイン時に使用したユーザ名 |
| クライアントOS | クライアントのOS | 最終更新日 | ログイン時にパケットを取得した時間 |

### ■ i-Auditor for Active Directory 監視対象環境

| | |
|---|---|
| 対応プロトコル | SMB(139/tcp) / CIFS(445/tcp) |
| 対応SMBバージョン | SMB 1.0(*)、2.0、2.1 |
| 対応サーバOS | Windows 2019, Windows Server 2012 R2, Windows Server 2008, Linux |

*SMB 1.0については重大な脆弱性が存在するため、ファイルサーバ側にて無効にすることを推奨

### ■ i-Auditor for File Server 提供形態

| | |
|---|---|
| 種別 | アプライアンス |

### ■ i-Auditor for DHCP Server ログ出力項目

| | | | |
|---|---|---|---|
| クライアントIP | クライアント端末のIP | リクエストIP | クライアントがサーバに要求したIP |
| クライアントMACアドレス | クライアント端末のMACアドレス | 操作 | クライアントがサーバにどのような要求を行ったか、またそれに対する返答 |
| クライアント名 | クライアント端末のホスト名 | サーバIP | サーバ端末のIP |

### ■ i-Auditor for DHCP Server 監視対象環境

| | |
|---|---|
| 対応プロトコル | DHCP |

### ■ i-Auditor for DHCP Server 提供形態

| | |
|---|---|
| 種別 | アプライアンス |