

サーバアクセスログ

Alog SMASH

Watch Your Data,
Not Your Employees

監視すべきは社員ではなく
重要データそのもの



いまや『守るべき重要情報』を持たない企業を見つけるほうが困難な時代です。
漏れてはいけない重要情報の保護は、セキュリティの最優先課題です。



機密情報



財務情報



個人情報



人事情報



開発情報



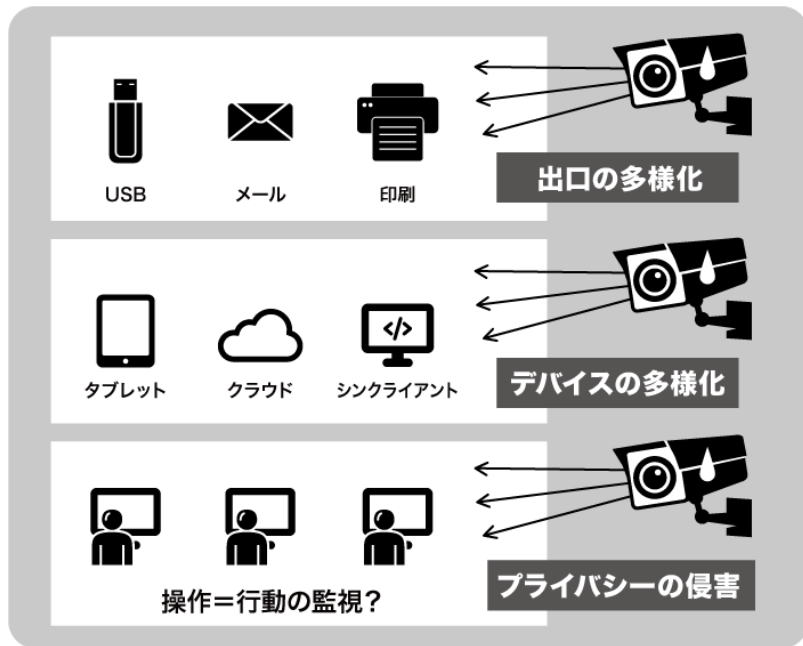
重要情報が漏れいすると、多くのケースで金銭被害よりも責任問題のほうが重大だと捉えられます。

重要情報の無防備なままの放置は、**経営者とシステム部門の責任者**に非難や追及が集中する結果を招きます。

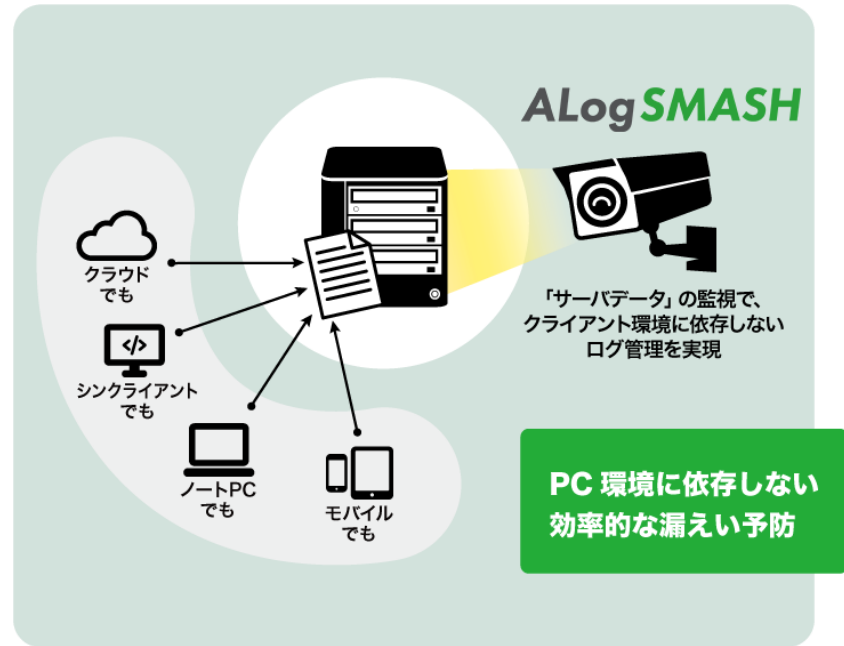


社員のミスを含めた情報の流出を防ぐために、USBメモリの利用やメール送信を監視・制限することはもちろん有効です。
しかしこれらの対策は膨大なコストと手間がかかる上に、社員の士気を下げる結果にもなり得ます。
大事なデータが保管されているサーバを重点的に監視するALog SMASHなら、PCの監視・制御に比べ圧倒的に効率的です。

PCの監視/制御



サーバのデータ監視



これからの セキュリティ対策

誰がそのデータにアクセスしたか？を記録しておけば、有事の証拠になり、不正の予防にもなります。

社員の端末を見張るのではなく、サーバ上の大切なデータを監視する。これが最低限かつ最適なセキュリティ対策です。

日時	ユーザー	サーバ	対象	操作
2023/1/12 15:04:50	amiya¥sasaki	fs001	D:¥fsvol1¥企画部¥FY13事業計画.doc	WRITE
2023/1/12 20:04:03	amiya¥Yamada	fs001	D:¥fsvol1¥経理部¥給与明細_田中.xls	READ
2023/1/12 22:34:23	amiya¥Nakai	fs001	D:¥fsvol1¥営業部¥製品別購入者一覧.xls	DELETE

いつ

誰が

どのファイルに

何をした

サーバアクセスログ

ALog SMASH

ALog SMASH（以下SMASH）は、サーバにある重要データに「いつ、誰が、何をしたか」を記録するサーバアクセスログ製品です。対象のサーバに直接インストールするので、**ログサーバが不要**です。また、**データベース構築**や**PCへのエージェントインストールも不要**です。SMASHは、サーバアクセスログ-シェアNo.1 ALog ConVerterを小規模向けに新設計した製品です。

SMASHが できること



大事な事業計画ファイルが 勝手に書き換えられている!

日時	ユーザー	対象	操作
2023/12/18 22:04:03	amiya¥Nancy	D:¥fsvol1¥マーケティング部¥SMASH資料.ppt	READ
2023/12/18 22:11:25	amiya¥Kamei	D:¥fsvol1¥経営企画部¥事業計画(機密).doc	WRITE

SMASH なら、誰が書き換えたか分かります。



顧客名簿ファイルが いつの間にか無くなった!

日時	ユーザー	対象	操作
2023/6/28 11:24:03	amiya¥Nakata	D:¥fsvol1¥経理部¥給与計算¥給与明細_田中.xls	DELETE
2023/7/19 22:34:12	amiya¥Ishida	D:¥fsvol1¥顧客管理部¥顧客名簿.xls	DELETE

SMASH なら、誰が削除したか分かります。

SMASHの 特長

簡単インストール

インストールはわずか数十秒！
システムに不慣れな方でもすぐ
にインストールできます。

専用サーバ不要

ファイルサーバに直接インス
トールするので、専用の管理
サーバが不要です。

超コンパクト

収集したログは数千分の一に圧
縮保管。“超”コンパクトだから
大容量ディスクも不要です。

インストール&初期設定は、簡単なウィザードであっという間に完了。
IT管理者が不在のオフィスでもすぐにログ管理を始められます。

The image displays three sequential screenshots of the 'Initial Setup Wizard' (初期セットアップウィザード) for a log management application.

- ① 見張りたいフォルダをセットする (Set the folder you want to monitor):** The first screenshot shows the 'Folder Selection' (フォルダの指定設定) screen. A file explorer view on the left lists various system folders. 'testfolder01' is highlighted with a green callout bubble.
- ② 保存期間を決める (Decide the retention period):** The second screenshot shows the 'Database Setting' (データベース設定) screen. It allows configuring retention periods for 'Access Log' (アクセスログ), 'Report Data' (レポートデータ), and 'System Log' (システムログ). For each, the 'Keep for next' (次の期間保持する) option is selected with a 3-month (3ヶ月) retention period. A green callout bubble points to these settings.
- ③ レポートをセットする (Set the report):** The third screenshot shows the 'Report Setting' (レポートの設定) screen. It includes options for report status (有効/無効), report name, and output format. A green callout bubble points to the 'Report Name' field.

専

用サーバ不要

ファイルサーバに直接インストールするので、専用の管理サーバやデータベースを用意する必要がなくリーズナブル。



超

コンパクト

独自のログ変換ロジックでログを見やすく翻訳変換し、変換したログは数千分の一に圧縮。
超コンパクトだから大容量ディスク不要で長期保管を実現します。

見やすく

複雑な
ログを

5-21-2910433525-404745982-3962478095-
Y/Toshio/2008SP2/0x50b70/Security/File/E:YDATA
客情報¥取引先重要顧客リスト.xls
534/%4416 /0x1/0x4//
5-21-2910433525-404745982-3962478095-
Y/Toshio/2008SP2/0x50b70/Security/File/E:YDATA
客情報¥取引先重要顧客リスト.xls
534/%4416 /0x1/0x4//
5-1-5-21-2910433525-404745982-3962478095-
500/Toshio/2008SP2/0x50b70/Security/File/E:YDATA
¥顧客情報¥取引先重要顧客リスト.xls

見やすく
変換

時刻	ユーザー	サーバ	対象	操作
2023/1/18 15:04:50	amiya.co.jp¥kawasaki	fs-vol1	D:¥エンジン開発部¥次世代 EV開発¥EV特許技術.xls	READ
2023/1/18 15:05:22	amiya.co.jp¥kawasaki	fs-vol1	D:¥機密¥個人情報¥個人ブ ロフィール.doc	WRITE
2023/1/18 15:05:34	amiya.co.jp¥kawasaki	fs-vol1	D:¥機密¥個人情報¥個人ブ ロフィール.doc	DELETE

小さく

大容量
のログを

元のログ
1GB



変換後

1MB



更に
圧縮して

25KB



超
コンパクト

最大1/40,000に
ファイル容量を軽減

SMASHは ココが すごい！

例

社員の「としお」が、エクセルのファイルを『開いて』『書き込んだ』
ログの出力は『**READ**』と『**WRITE**』だけ出るはず。

A製品は…

ファイル	操作
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	WRITE
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	WRITE
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	WRITE
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	WRITE
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ

生ログを
セル区切りしただけ…

そのままではどんな操作をしたのかはわかりません。

B製品は…

ファイル	操作
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ/WRITE
E:\DATA\顧客情報\取引先重要顧客リスト.xls	RENAME
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ/WRITE
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ

なんとなく整理は
しているようです…

頑張ったのは認めるけど
実際の操作と違います…

SMASHなら

ファイル	操作
E:\DATA\顧客情報\取引先重要顧客リスト.xls	READ
E:\DATA\顧客情報\取引先重要顧客リスト.xls	WRITE

しっかり
操作通りのログ
を出力

実際の操作に合わせるように
調査して分析変換

サーバアクセスログ

ALog **SMASH**

機能紹介

- 検索

AlogSMASH

管理者

検索

56 件中 1 - 56 件

☐ 折り返して全体を表示する

PDF出力 CSV出力

	時刻	ユーザー	対象	操作	
1 +	2021/07/27 20:12:50	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	READ	ClientIP:10.249 ^
2 +	2021/07/27 20:10:21	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10258_△△△△¥Acces...	WRITE	AppName:C:¥W
3 +	2021/07/27 20:10:21	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10258_△△△△¥Acces...	WRITE	AppName:C:¥W
4 +	2021/07/27 20:10:06	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10258_△△△△	WRITE	AppName:C:¥W
5 +	2021/07/27 20:10:06	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥新しいフォルダー	RENAME	AppName:C:¥W
6 +	2021/07/27 20:09:41	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥新しいフォルダー	WRITE	AppName:C:¥W
7 +	2021/07/27 20:08:32	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
8 +	2021/07/27 20:08:32	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
9 +	2021/07/27 20:08:32	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
10 +	2021/07/27 20:08:32	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
11 +	2021/07/27 20:08:32	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
12 +	2021/07/27 20:08:32	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
13 +	2021/07/27 20:08:32	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
14 +	2021/07/27 20:08:31	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
15 +	2021/07/27 20:08:31	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
16 +	2021/07/27 20:08:31	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
17 +	2021/07/27 20:08:31	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W
18 +	2021/07/27 20:08:31	2019-FSSK01¥Ad...	C:\share¥04_開発部¥サポート¥01_顧客データ_重要¥#10256_●●株式会社¥S...	WRITE	AppName:C:¥W

シンプルなビューアを使って、見たいログを簡単に抽出できます。

「退職予定者の1ヶ月間のファイル操作を知りたい」

「重要ファイルを最後に更新した人を知りたい」

といった絞り込みも簡単です。

機能紹介

- レポート / アラート

ALogSMASH ホーム 検索 レポート/アラート 管理

フィルター 確認済みにする 操作

新規作成

お気に入り	レポート名	概要説明	未確認アラート	最終更新日時	状態	有効な機能	メール	編集
☒	★ ファイルの読み込み		-	2019/10/16 13...	✓	監視	重	編集
☐	★ 土日のアクセス		-	-	✓	監視	重	編集
☐	★ 夜間のアクセス		-	-	✓	監視	重	編集

編集

状態 ☒ 有効 ☐ 無効

機能 ☒ レポート ☒ アラート

レポート名 ファイルの読み込み

概要説明

出力件数 ☒ 制限しない

「制限しない」がONの場合、大量のアクセスログがヒットした際にパフォーマンスが悪化する可能性があります。フィルター条件が厳しく、ヒットするアクセスログが限られているレポートでの利用を推奨します。

フィルター追加 ユーザー

条件1

ユーザー [対象とする] AND OR ⊕
複数指定する場合、改行区切りで入力します。

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

対象 [対象とする] AND OR ⊕
C:\共通

[除外する] AND OR
複数指定する場合、改行区切りで入力します。

操作 1 selected 操作一覧

OK キャンセル

不審な操作をピックアップ

不審な操作を検知すると文字色が赤く変わるので一目瞭然です。

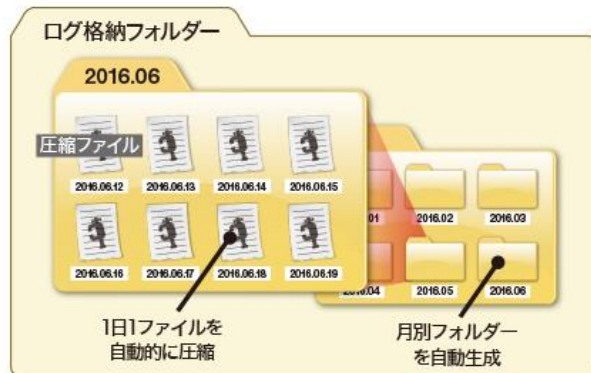
監視設定

時間や曜日を細かく指定できるので、「土日のアクセス」や「深夜のアクセス」などの監視が可能です。

詳細なログを表示

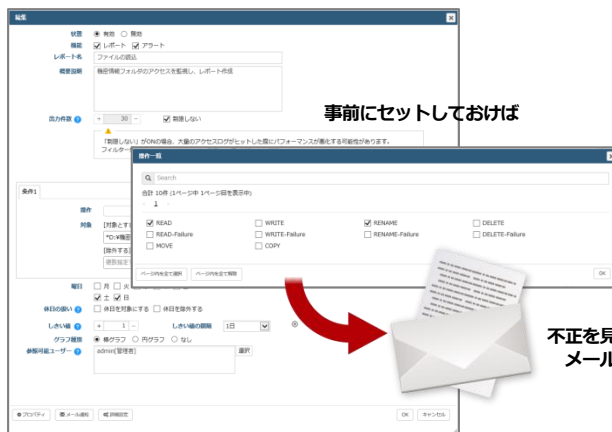
詳細なログから不審な操作をトレースできます。

SMASHは 運用も かんたん



保管

ログは自動的にCSVファイルに書き出され、毎日に圧縮して保管されるので、運用の手間は最小限。もちろん過去のCSVファイルをSMASH本体にインポートすることもできます。



メール通知

事前に監視したい操作をあらかじめ定義しておけば、条件に合致するログが見つかった時に、アラートメールを送ったり、日次でレポートメールを送ったりすることが可能です。

動作環境

対応OS： Windows Server 2016 / 2019 / 2022 / 2025

Windows Storage Server 2016

Windows Server IoT 2019 / 2022

※32bit版OSには対応していません

※各OS のサービスパック (SP) に対応

※各エディション (Standard / Enterprise / Datacenter) に対応

※仮想環境 (VMWare, Hyper-V, Citrix XenServer) に対応

※ ALog SMASH最新バージョンでの動作環境となります。

CPU： Quad Core 以上

メモリ： 16GB 以上

ディスク容量： 100GB以上の空き容量

※SSD推奨

※アクセスログの保管期間の長さによって別途必要となります。

ソフトウェア： .NET Framework 4.8以上

以下のいずれかのWebブラウザ：

Firefox バージョン68以上

Google Chrome バージョン76以上

Microsoft Edge

動作条件

・ファイルアクセスログの出力対象となるドライブがNTFSフォーマットであること (FATフォーマットには対応していません)。

ログ出力ボリューム試算例

100人の環境でSMASHを利用し、CSVファイル (ZIP圧縮) と検索用DBファイルをそれぞれ1年間保管したときの試算例です。

(ユーザー1人あたり1日分のログデータ量を5MBとします)

CSVファイル : $2.5\text{KB} \times 100\text{人} \times 300\text{日}$
= **75MB/年**

検索用DBファイル : $37.5\text{KB} \times 100\text{人} \times 300\text{日}$
= **1125MB/年**

合計：1.2GB/年

SMASHは300ユーザ以下の環境でのファイルアクセスログの取得を目的とした製品です。300ユーザーを超える環境や、ファイルアクセスログ以外のログをご希望の場合は、エンタープライズ向け製品のALog ConVerter for Windowsをご利用ください。

価格/保守サポートについて

■ サブスクリプション価格

品名	月（年間契約）	型番
ALog SMASH 1サーバライセンス	¥9,000	R-AL-SMS-NL

※サブスクリプションには保守が含まれておりますので、別途保守へのご加入は不要です。

※年間での契約となります。

■ 保守サポート



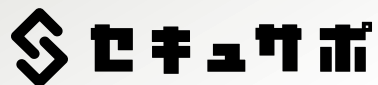
● テクニカルサポート

- メールによるお問い合わせ。
年末年始を除く平日の9時～17時
- お電話によるお問合せ、ご訪問による対応は含まれません

● パッチ版（ログ変換プログラム）の無償利用

● メジャーバージョンアップ版の無償利用

CSIRT部隊のアウトソースなら



セキュサポは、サイバー攻撃や内部不正の検知、対応支援から、日ごろのセキュリティ相談の窓口、攻撃の入り口となる脆弱性の診断まで、社外のCSIRTとして企業のセキュリティ対策・強化をトータルにサポートするサービスです。



サイバー攻撃
対策



インシデント
レスポンス支援



内部不正
対策



サイバー保険



強化レポート

セキュサポはSOCサービスだけでなく、**攻撃の予防**もサポート



脆弱性
対策



セキュリティ
相談窓口

情報システム部門のアウトソースなら

クラウド情シスサービス



ランサポは、ITシステムのパラメータシート作成やトラブル対応、設定変更など、社外の情報システムとして企業のITシステム運用をトータルにサポートするサービスです。



サーバ、ネットワークの
運用/監視業務



年間計画
の作成支援



障害/トラブル
対応



BCP関連
支援



定型業務
代行



クラウド移行
支援



PCマスター
イメージ作成



セキュリティ対策
支援