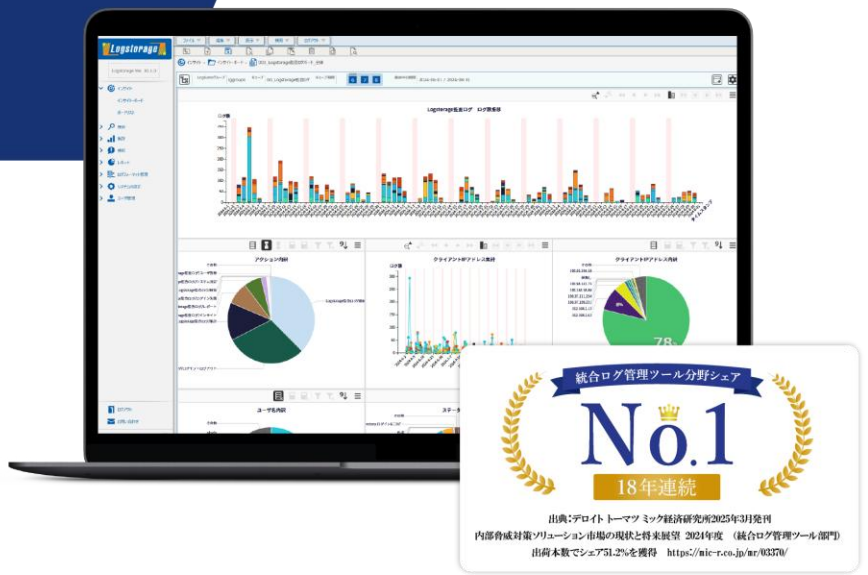
Logstorage VER.10

統合ログ管理システム「ログストレージ」

Logstorage Box 連携パック
参考資料



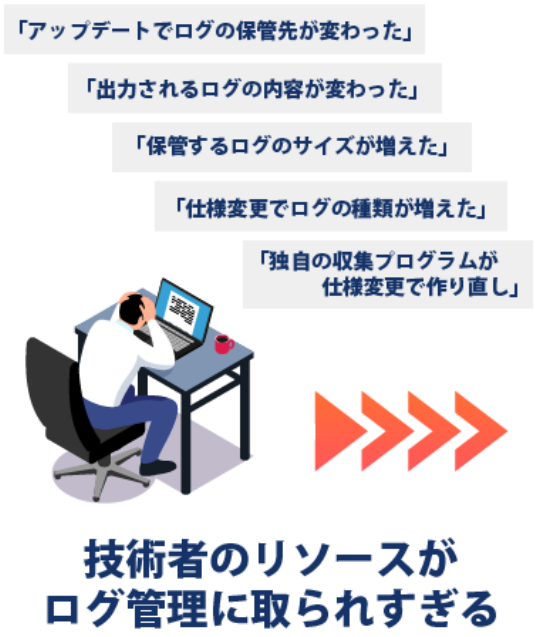
Infoscience
インフォサイエンス株式会社　Infoscience Corporation　www.infoscience.co.jp
プロダクト事業部　Product division　https://logstorage.com　info@logstorage.com　／　Tel: 03-5427-3503　／　Fax: 03-5427-3889

Logstorage 連携パックとは

連携パックは、各分野で人気の製品と連携して開発した「ログの収集・分析がすぐにスタートできる」Logstorageのオプション製品です。

連携パックを導入することで、各連携製品のログ管理のセットアップを簡略化できるほか、運用中に、収集対象のログの

フォーマット(並び順や表示の仕方)や出力方法に変更があっても、各連携パックのバージョンアップで、変更を反映できます。



パッケージ内容

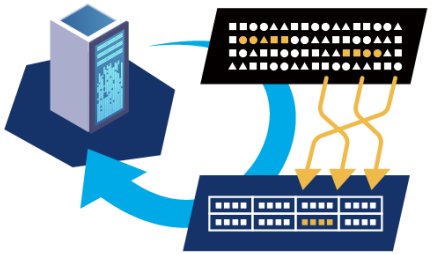
Logstorage 連携パックには、専用のログ収集モジュール・ログフォーマット定義ファイル・分析テンプレートが含まれます。

ログ収集モジュール

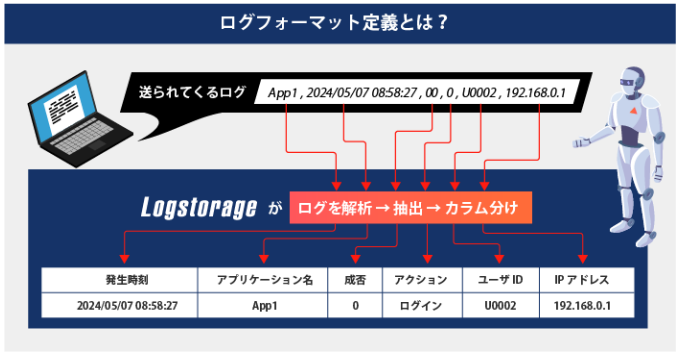
製品ごとにログの出力方法や出力先は異なります。各製品のログにあわせたログ収集モジュールをご用意しております。

※製品によっては収集モジュールが不要の場合もございます。
その場合、パッケージに含まれませんので、ご了承ください。

ログフォーマット定義ファイル



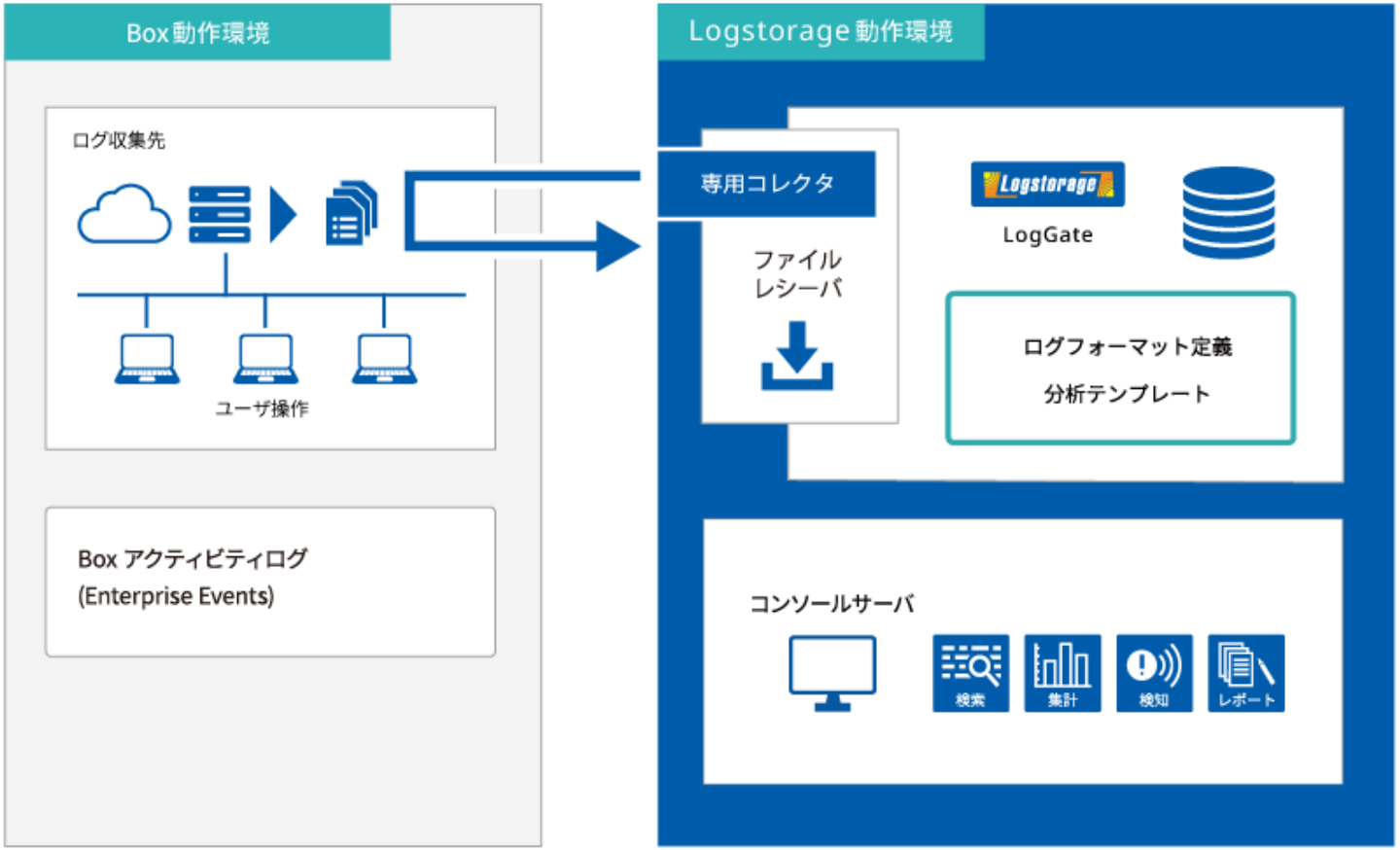
連携している製品のログフォーマット（並び順や表示の仕方）を分析し、ログを項目ごとに抽出します。



分析テンプレート

各製品から出力される多数のログの中から、どのログを検索すればよいのか・何を集計したらよいのか・どんなレポートを出力すればよいのか、ログ分析をサポートする分析テンプレートをご提供いたします。

システム構成



検索テンプレート一覧

検索-1

Logstorage Box 連携パック の検索テンプレートは以下の通りです。

検索条件テンプレート名
Boxユーザーアクティビティ 全ログ検索
Boxユーザーアクティビティ 全ログ検索（パス・ロール設定有り）
Boxユーザーアクティビティ OAuth アクセストークンの作成
Boxユーザーアクティビティ アイテムの修正
Boxユーザーアクティビティ アクセス付与
Boxユーザーアクティビティ アクセス無効
Boxユーザーアクティビティ アップロード
Boxユーザーアクティビティ アプリ作成
Boxユーザーアクティビティ アプリ公開キー削除
Boxユーザーアクティビティ アプリ公開キー追加
Boxユーザーアクティビティ ウィルスの検出
Boxユーザーアクティビティ グループからアイテム削除
Boxユーザーアクティビティ グループからユーザ削除
Boxユーザーアクティビティ グループにアイテム追加
Boxユーザーアクティビティ グループにユーザ追加
Boxユーザーアクティビティ グループ作成
Boxユーザーアクティビティ グループ削除
Boxユーザーアクティビティ グループ編集
Boxユーザーアクティビティ コピー
Boxユーザーアクティビティ コメント作成
Boxユーザーアクティビティ コメント削除
Boxユーザーアクティビティ タスクの作成
Boxユーザーアクティビティ タスク割当の作成

検索テンプレート一覧

検索-2

検索条件テンプレート名
Boxユーザーアクティビティ タスク割当の削除
Boxユーザーアクティビティ タスク割当の更新
Boxユーザーアクティビティ ダウンロード
Boxユーザーアクティビティ デバイスの関連付けを削除
Boxユーザーアクティビティ デバイスの関連付けを追加
Boxユーザーアクティビティ デバイストラストの失敗
Boxユーザーアクティビティ ファイルから透かしを削除
Boxユーザーアクティビティ ファイルに透かしを追加
Boxユーザーアクティビティ ファイルのオープン
Boxユーザーアクティビティ ファイル自動削除の設定
Boxユーザーアクティビティ フォルダーアクセス許可の変更
Boxユーザーアクティビティ プレビュー
Boxユーザーアクティビティ メタデータインスタンスの作成
Boxユーザーアクティビティ メタデータインスタンスの削除
Boxユーザーアクティビティ メタデータインスタンスの更新
Boxユーザーアクティビティ メタデータテンプレートの作成
Boxユーザーアクティビティ メタデータテンプレートの削除
Boxユーザーアクティビティ メタデータテンプレートの更新
Boxユーザーアクティビティ メールエイリアスの作成
Boxユーザーアクティビティ メールエイリアスの削除
Boxユーザーアクティビティ ユーザーセッションの無効
Boxユーザーアクティビティ ユーザ作成
Boxユーザーアクティビティ ユーザ削除
Boxユーザーアクティビティ ユーザ編集

検索テンプレート一覧

検索-3

検索条件テンプレート名
Boxユーザーアクティビティ リテンションの作成
Boxユーザーアクティビティ リテンションの削除
Boxユーザーアクティビティ リテンションポリシー割当の追加
Boxユーザーアクティビティ ログイン
Boxユーザーアクティビティ ログイン失敗
Boxユーザーアクティビティ ログイン追加
Boxユーザーアクティビティ ロック
Boxユーザーアクティビティ ロック解除
Boxユーザーアクティビティ ワークフローのアップロード違反
Boxユーザーアクティビティ ワークフローの不正ダウンロード
Boxユーザーアクティビティ ワークフローの共有ポリシー違反
Boxユーザーアクティビティ ワークフローの自動化を削除
Boxユーザーアクティビティ ワークフローの自動化を追加
Boxユーザーアクティビティ ワークフローポリシーを追加
Boxユーザーアクティビティ 共有
Boxユーザーアクティビティ 共有停止
Boxユーザーアクティビティ 共有有効期限
Boxユーザーアクティビティ 共有期限更新
Boxユーザーアクティビティ 共有項目更新
Boxユーザーアクティビティ 利用規約に同意
Boxユーザーアクティビティ 利用規約を拒否
Boxユーザーアクティビティ 削除
Boxユーザーアクティビティ 削除取り消し
Boxユーザーアクティビティ 名称変更

検索テンプレート一覧

検索-4

検索条件テンプレート名
Boxユーザーアクティビティ 外部共有ロール変更
Boxユーザーアクティビティ 外部共有削除
Boxユーザーアクティビティ 外部共有招待
Boxユーザーアクティビティ 外部共有有効期限延長
Boxユーザーアクティビティ 外部共有有効期限更新
Boxユーザーアクティビティ 外部共有許可
Boxユーザーアクティビティ 移動
Boxユーザーアクティビティ 管理者ログイン
Boxユーザーアクティビティ 管理者ロール変更
Boxユーザーアクティビティ 編集
Boxユーザーアクティビティ 訴訟ホールドから削除する
Boxユーザーアクティビティ 訴訟ホールドポリシーの作成
Boxユーザーアクティビティ 訴訟ホールドポリシーの削除
Boxユーザーアクティビティ 訴訟ホールドポリシーの更新
Boxユーザーアクティビティ 訴訟ホールド対象にする
Boxユーザーアクティビティ 透かし付きファイルのダウンロード
Boxユーザーアクティビティ 項目同期
Boxユーザーアクティビティ 項目同期停止

集計テンプレート一覧

集計

Logstorage Box 連携パックの集計テンプレートは以下の通りです。

集計条件テンプレート名	概要
Boxユーザーアクティビティ アクセス頻度の高いフォルダ・ファイル	「アップロード」or「コピー」or「ダウンロード」or「プレビュー」で抽出　※10件以上のフィルター条件あり
Boxユーザーアクティビティ アップロード/ダウンロードの頻度が高いユーザー	「アップロード」or「ダウンロード」の操作を1日あたり、10件以上したユーザー名を抽出
Boxユーザーアクティビティ オープンリンク/コラボレートの頻度が高いユーザー	「有効化された共有リンク」or「コラボレータの招待」の操作を1日あたり、10件以上したユーザー名を抽出
Boxユーザーアクティビティ フォルダ・ファイル操作 集計	「アップロード」or「コピー」or「ダウンロード」で抽出
Boxユーザーアクティビティ ログイン失敗 集計	-
Boxユーザーアクティビティ ログイン成功 集計	-
Boxユーザーアクティビティ 日別ダウンロードデータ量	-
Boxユーザーアクティビティ 時間別ダウンロードデータ量	-
Boxユーザーアクティビティ 業務時間外にアップロード/ダウンロードしているユーザー	「アップロード」or「ダウンロード」を、22:00～翌6:00（仮）の間に1日あたり、10件以上したユーザー名を抽出
Boxユーザーアクティビティ 組織外（フリーメールアドレス含む）からアクセスされたフォルダ・ファイル	「アップロード」or「ダウンロード」or「プレビュー」or「ファイルオープン」で抽出　※抽出条件の「@infoscience¥.co¥.jp」は自ドメインに変更してください。
Boxユーザーアクティビティ アクセス頻度の高いフォルダ・ファイル	「アップロード」or「コピー」or「ダウンロード」or「プレビュー」で抽出　※10件以上のフィルター条件あり
Boxユーザーアクティビティ アップロード/ダウンロードの頻度が高いユーザー	「アップロード」or「ダウンロード」の操作を1日あたり、10件以上したユーザー名を抽出
Boxユーザーアクティビティ オープンリンク/コラボレートの頻度が高いユーザー	「有効化された共有リンク」or「コラボレータの招待」の操作を1日あたり、10件以上したユーザー名を抽出
Boxユーザーアクティビティ フォルダ・ファイル操作 集計	「アップロード」or「コピー」or「ダウンロード」で抽出
Boxユーザーアクティビティ ログイン失敗 集計	-
Boxユーザーアクティビティ ログイン成功 集計	-

レポートテンプレート一覧

レポート

Logstorage Box 連携パック のレポートテンプレートは以下の通りです。

レポート条件テンプレート名	概要
Boxユーザーアクティビティ アップロード/ダウンロードの頻度が高いユーザー 日次集計レポート	集計条件 Box アップロード/ダウンロードの頻度が高いユーザー で抽出
Boxユーザーアクティビティ オープンリンク/コラボレートの頻度が高いユーザー 日次集計レポート	集計条件 Box オープンリンク/コラボレートの頻度が高いユーザー で抽出
Boxユーザーアクティビティ グループ登録・編集・削除 日次レポート	検索条件： Box グループ作成／Box グループ編集／Box グループ削除 で抽出
Boxユーザーアクティビティ フォルダ・ファイル操作 日別集計レポート	集計条件： Box フォルダ・ファイル操作 集計 で抽出
Boxユーザーアクティビティ ユーザ登録・編集・削除 日次レポート	検索条件： Box ユーザ作成／Box ユーザ編集／Box ユーザ削除 で抽出
Boxユーザーアクティビティ ログイン失敗 日別集計レポート	集計条件： Box ログイン失敗 集計 で抽出
Boxユーザーアクティビティ ログイン成功 日別集計レポート	集計条件： Box ログイン成功 集計 で抽出
Boxユーザーアクティビティ 日別ダウンロードデータ量 日別集計レポート	集計条件 Box日別ダウンロードデータ量 で抽出
Boxユーザーアクティビティ 時間別ダウンロードデータ量 時間別集計レポート	集計条件 Box時間別ダウンロードデータ量 で抽出
Boxユーザーアクティビティ 業務時間外にアップロード/ダウンロードしているユーザー 日次集計レポート	集計条件 Box 業務時間外にアップロード/ダウンロードしているユーザー で抽出
Boxユーザーアクティビティ 組織外（フリーメールアドレス含む）からアクセスされたフォルダ・ファイル 日別集計レポート	集計条件 Box組織外（フリーメールアドレス含む）からアクセスされたフォルダ・ファイル で抽出

検索例

Box上のアクセス履歴を確認できます。

Box利用ユーザの操作履歴を可視化 → **いつ、誰が、何を、どのように操作したか？**

検索条件名: Box 全ログ検索

概要:

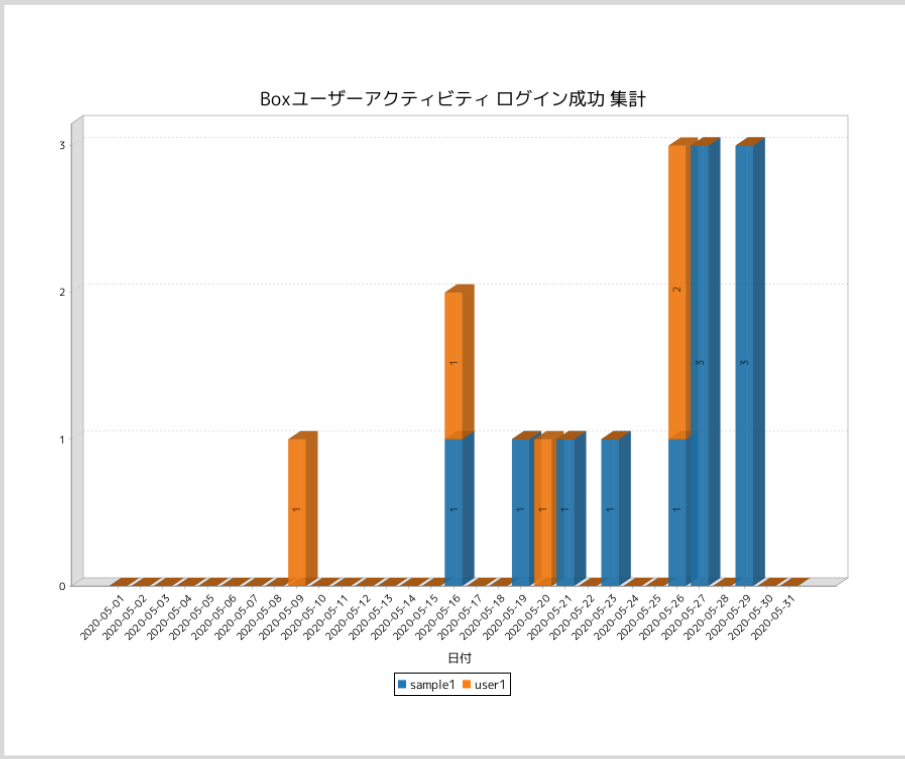
検索条件 | 検索結果 | カラムセットアサイン

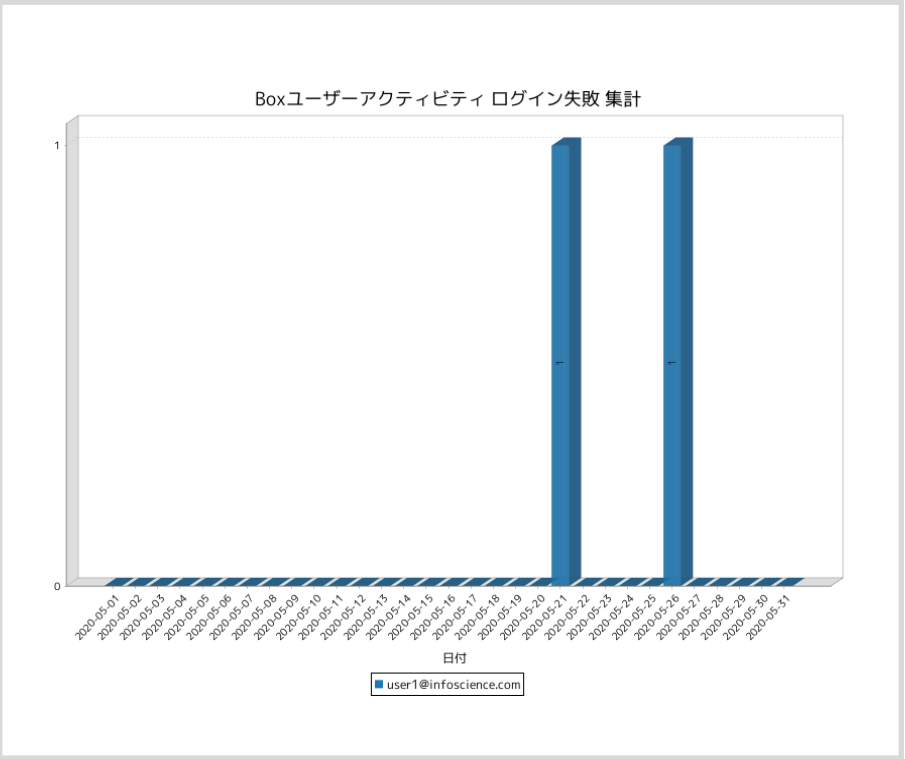
ログ | カラム　1-50件目 表示（全69件）　1 2 > >>　[表示数: 100件]　拡張トラッキング　ログを折り込

タイムスタンプ	作成名	作成ログイン	アクション	ソース_項目名(フォルダ・ファイル名)	ソース_親名	IPアドレス	ソース_ログイン
2019-07-15 10:32:34	suzuki	suzuki@infoscience.co.jp	ログイン			192.168.0.123	suzuki@infoscience.co.jp
2019-07-15 10:33:18	suzuki	suzuki@infoscience.co.jp	プレビュー	7月売上情報.xls	売上情報	192.168.0.123	
2019-07-15 10:34:08	suzuki	suzuki@infoscience.co.jp	プレビュー	顧客名簿.doc	顧客情報	192.168.0.123	
2019-07-15 10:35:09	suzuki	suzuki@infoscience.co.jp	ダウンロード	顧客名簿.doc	顧客情報	192.168.0.123	
2019-07-17 17:11:54	Unknown User		ログイン失敗			192.100.0.1	inoue@aaa.co.jp
2019-07-17 17:12:10	inoue	inoue@aaa.co.jp	ログイン			192.100.0.1	inoue@aaa.co.jp
2019-07-17 17:13:57	inoue	inoue@aaa.co.jp	アップロード	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-17 17:13:58	inoue	inoue@aaa.co.jp	外部共有招待	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-17 17:16:26	inoue	inoue@aaa.co.jp	共有	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-17 17:16:35	inoue	inoue@aaa.co.jp	共有項目更新	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-17 17:18:44	inoue	inoue@aaa.co.jp	ログイン追加			192.100.0.1	inoue@aaa.co.jp
2019-07-17 17:22:48	inoue	inoue@aaa.co.jp	アップロード	会議資料.docx	20190718_A社様向け打ち合わせ資料	192.100.0.1	
2019-07-17 17:23:50	Unknown User		ダウンロード	会議資料.docx	20190718_A社様向け打ち合わせ資料	192.100.0.1	
2019-07-17 17:26:44	inoue	inoue@aaa.co.jp	アップロード	案件共有情報.xlsx	20190718_A社様向け打ち合わせ資料	192.100.0.1	
2019-07-17 17:27:11	inoue	inoue@aaa.co.jp	ダウンロード	案件共有情報.xlsx	20190718_A社様向け打ち合わせ資料	192.100.0.1	
2019-07-17 17:33:50	inoue	inoue@aaa.co.jp	外部共有招待	20190718_A社様向け打ち合わせ資料	すべてのファイル	192.100.0.1	
2019-07-18 08:42:24	kimura	kimura-k@gmail.com	ダウンロード	会議資料.docx	20190718_A社様向け打ち合わせ資料	10.66.0.1	
2019-07-18 08:42:24	kimura	kimura-k@gmail.com	ダウンロード	案件共有情報.xlsx	20190718_A社様向け打ち合わせ資料	10.66.0.1	
2019-07-18 08:42:27	kimura	kimura-k@gmail.com	プレビュー	会議資料.docx	20190718_A社様向け打ち合わせ資料	10.66.0.1	
2019-07-18 08:42:46	kimura	kimura-k@gmail.com	アップロード	無題のメモ 2019-07-18 08:42:44.boxnote	20190718_A社様向け打ち合わせ資料	10.66.0.1	

レポート例 1

Boxのログイン履歴を確認することで、
Boxの利用状況や不審なアクセスがないかを把握できます。





レポート例 2

定期的にレポート出力し、ファイル操作履歴を確認することができます。

Box フォルダ・ファイル操作 日別集計レポート

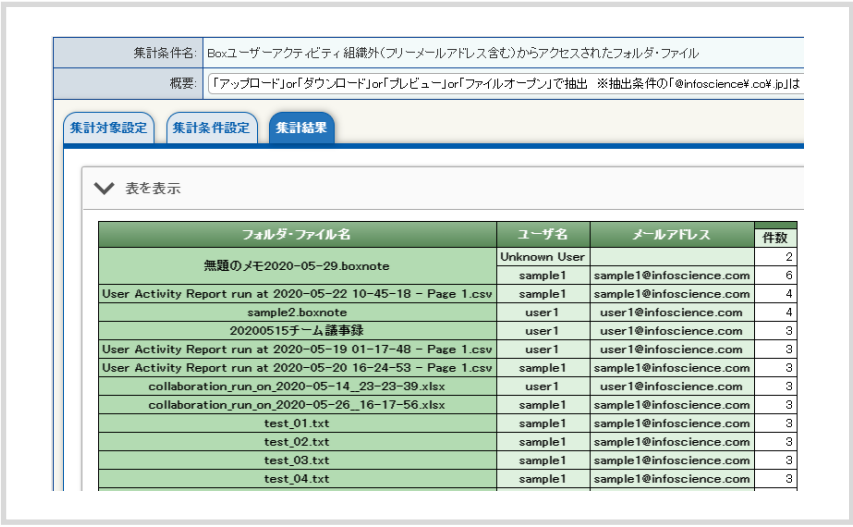
概要　集計条件: Box フォルダ・ファイル操作 集計 で抽出
作成日　2016-08-03 15:56:24
対象期間　2016-07-01 00:00:00 - 2016-07-31 23:59:59

集計条件名　Box フォルダ・ファイル操作 集計
概要　アクション: アップロード／コピー／ダウンロード で抽出

日付	ユーザ	操作	操作対象	件数
2016-07-15	[redacted]	UPLOAD	見積書	1
2016-07-19	[redacted]	DOWNLOAD	外部ファイル	14
	[redacted]	DOWNLOAD	test1.txt	5
		UPLOAD	test1.txt	6
			サンプル.docx	1
			セールスチーム用フォルダ	2
			社内ルール.docx	1
2016-07-20	[redacted]	UPLOAD	Box Reports	1
			folder_tree_run_on_2016-07-19__19-59-35.xlsx	1
	[redacted]	UPLOAD	test001.txt	1
2016-07-22	[redacted]	UPLOAD	test001.txt	1
			テスト共有	1
2016-07-26	[redacted]	DOWNLOAD	外部ファイル	1
		UPLOAD	公開用フォルダ	1
2016-07-27	[redacted]	UPLOAD	test	1
			test2	1
2016-07-28	[redacted]	DOWNLOAD	usage_log_run_on_2016-07-27__21-48-20.xlsx	1
			外部ファイル	1
		UPLOAD	usage_log_run_on_2016-07-27__21-48-20.xlsx	1
2016-07-29	[redacted]	DOWNLOAD	サンプル.docx	1
			社内ルール.docx	2
		UPLOAD	サンプル.docx	1
			セールスチーム用フォルダ	1
			社内ルール.docx	1

レポート例3

組織外のユーザーからアクセスされたフォルダ・ファイルの一覧が確認できます。



フォルダ・ファイル名	ユーザ名	メールアドレス	件数
無題のメモ2020-05-29.boxnote	Unknown User		2
	sample1	sample1@infoscience.com	6
User Activity Report run at 2020-05-22 10-45-18 - Page 1.csv	sample1	sample1@infoscience.com	4
sample2.boxnote	user1	user1@infoscience.com	4
20200515チーム議事録	user1	user1@infoscience.com	3
User Activity Report run at 2020-05-19 01-17-48 - Page 1.csv	user1	user1@infoscience.com	3
User Activity Report run at 2020-05-20 16-24-53 - Page 1.csv	sample1	sample1@infoscience.com	3
collaboration_run_on_2020-05-14_23-23-39.xlsx	user1	user1@infoscience.com	3
collaboration_run_on_2020-05-26_16-17-56.xlsx	sample1	sample1@infoscience.com	3
test_01.txt	sample1	sample1@infoscience.com	3
test_02.txt	sample1	sample1@infoscience.com	3
test_03.txt	sample1	sample1@infoscience.com	3
test_04.txt	sample1	sample1@infoscience.com	3

お問い合わせ

ご不明点、ご相談につきましては、下記お問い合わせ先からご連絡ください。

電話でのお問い合わせ

03-5427-3503

【受付】平日 9:00～17:30

メールでのお問い合わせ

info@logstorage.com

会社名・氏名・メールアドレス・電話番号を
ご記入の上、お問い合わせください

当社のホームページでも資料請求・お問い合わせができます。
https://logstorage.com