



マルチクラウドテンプレート レポート集

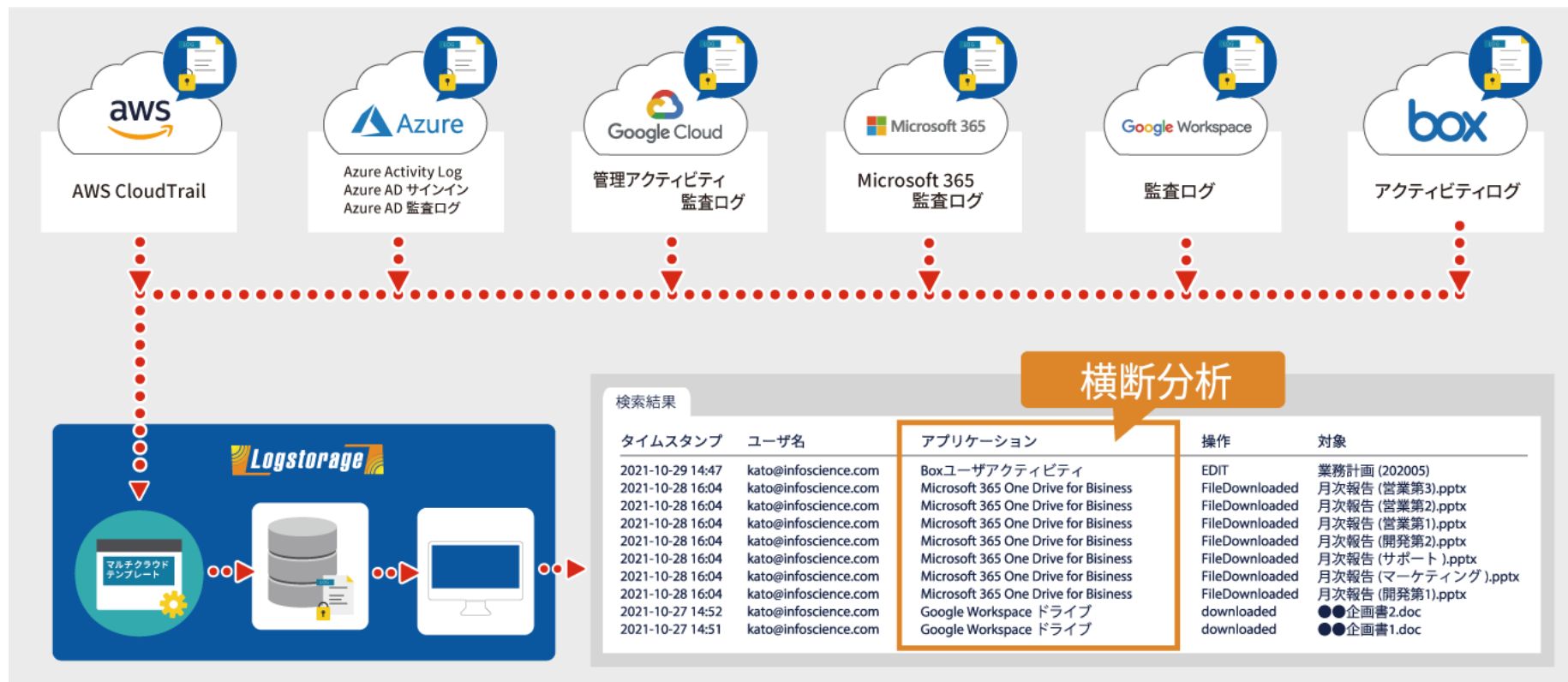
Infoscience

インフォサイエンス株式会社
プロダクト事業部

Infoscience Corporation
www.infoscience.co.jp info@logstorage.com
Tel: 03-5427-3503 Fax: 03-5427-3889

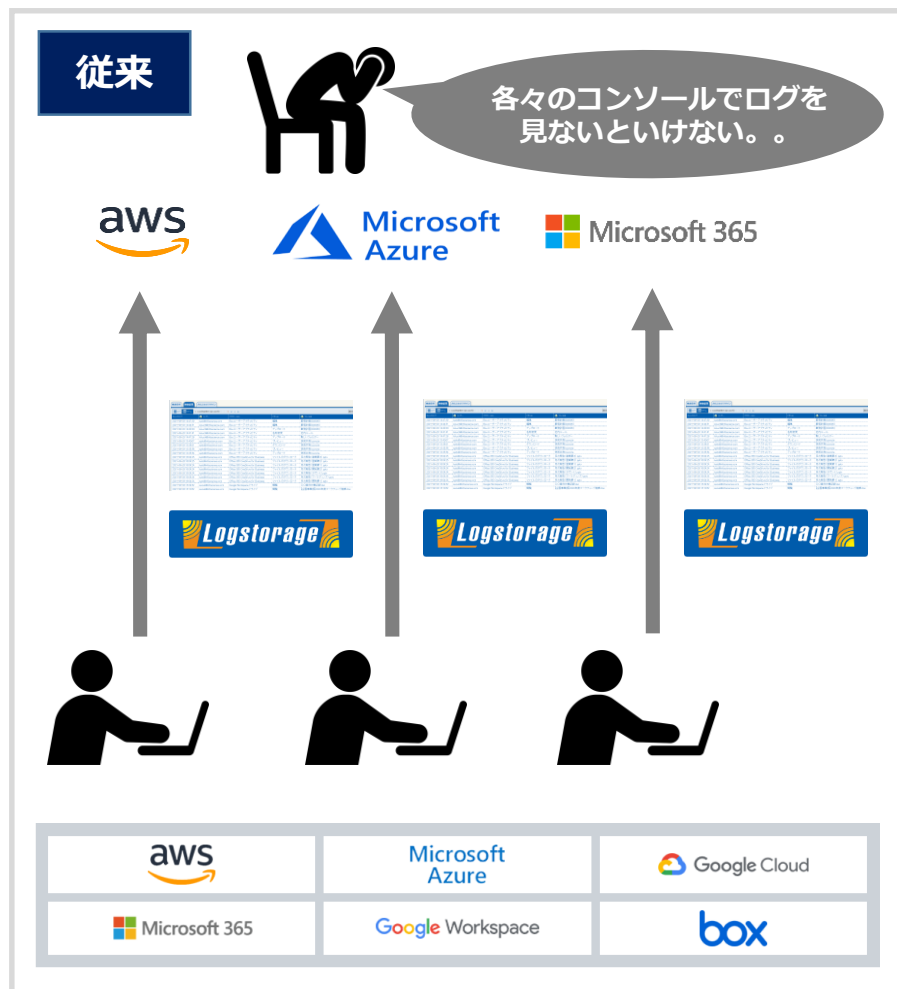
Logstorage で収集したクラウドサービスログを横断的に分析・レポート

Logstorage Cloud Solutions に含まれる連携製品を横断分析できるテンプレートです。



対応しているLogstorage Cloud Solutions 連携パックを2つ以上ご購入の方に

無償提供いたします。



各クラウドサービスのログを横断的に分析することが可能に！

■ 検索

- ・マルチクラウド イベント一覧
- ・マルチクラウド イベント一覧(SaaSのみ)
- ・マルチクラウド ファイル操作(SaaSのみ)
- ・マルチクラウド ログイン一覧

■ 集計

- ・マルチクラウド アクセス頻度の高いファイル(SaaSのみ)
- ・マルチクラウド アップロードの頻度が高いユーザー(SaaSのみ)
- ・マルチクラウド ダウンロードの頻度が高いユーザー(SaaSのみ)
- ・マルチクラウド ユーザー別アクセス集計[日別]
- ・マルチクラウド ユーザー別アクセス集計[時間別]
- ・マルチクラウド ログイン失敗
- ・マルチクラウド ログイン成功
- ・マルチクラウド 業務時間外にファイルアクセスしているユーザー(SaaSのみ)
- ・マルチクラウド 組織外からアクセスされたファイル(SaaSのみ)

■ レポート

- ・マルチクラウド アクセス頻度の高いファイル(SaaSのみ)
- ・マルチクラウド アップロードの頻度が高いユーザー(SaaSのみ)
- ・マルチクラウド ダウンロードの頻度が高いユーザー(SaaSのみ)
- ・マルチクラウド ユーザー別アクセス集計[日別]
- ・マルチクラウド ユーザー別アクセス集計[時間別]
- ・マルチクラウド ログイン失敗
- ・マルチクラウド ログイン成功
- ・マルチクラウド 業務時間外にファイルアクセスしているユーザー(SaaSのみ)
- ・マルチクラウド 組織外からアクセスされたファイル(SaaSのみ)

各クラウドサービスの監査ログを横断的に分析することができます。

検索条件名: マルチクラウド イベント一覧					
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		1-100件目表示 (2,000件以上) < 1 2 3 4 5 6 7 8 9 10 > >> [表示]			
タイムスタンプ	ユーザー	アプリケーション	操作	対象	接続元IP
2022-10-29 13:36:01	saito@infoscience.com	Boxユーザーアクティビティ	ITEM_OPEN	技術共有.boxnote	100.10.132.102
2022-10-29 13:36:01	saito@infoscience.com	Boxユーザーアクティビティ	DOWNLOAD	技術共有.boxnote	100.10.132.102
2022-10-29 13:35:56	saito@infoscience.com	Boxユーザーアクティビティ	PREVIEW	技術共有.boxnote	100.10.132.102
2022-10-29 13:35:54	saito@infoscience.com	Boxユーザーアクティビティ	UPLOAD	技術共有.boxnote	100.10.132.102
2022-10-29 13:35:34	saito@infoscience.com	Boxユーザーアクティビティ	LOGIN	saito@infoscience.com	100.10.132.102
2022-10-29 13:35:34	saito@infoscience.com	Boxユーザーアクティビティ	ADD_LOGIN_ACTIVITY_DEVICE	saito@infoscience.com	100.10.132.102
2022-10-29 13:35:29	kato	AWS CloudTrail	ConsoleLogin		100.10.0.1
2022-10-29 13:31:26	hayashi@infoscience.com	Azure Active Directory サインイン			100.20.0.1
2022-10-29 13:29:52	tuchida@infoscience.com	Azure Active Directory サインイン			100.20.0.1
2022-10-28 16:06:00	suzuki@infoscience.com	Google Workspace ドライブ	trash	△△案件作業記録.doc	54.0.0.1
2022-10-28 16:05:59	suzuki@infoscience.com	Google Workspace ドライブ	trash	○×案件作業記録.doc	54.0.0.1
2022-10-28 16:05:58	suzuki@infoscience.com	Google Workspace ドライブ	trash	××案件作業記録.doc	54.0.0.1
2022-10-28 16:05:57	suzuki@infoscience.com	Google Workspace ドライブ	trash	○△案件作業記録.doc	54.0.0.1
2022-10-28 16:05:56	suzuki@infoscience.com	Google Workspace ドライブ	trash	○○案件作業記録.doc	54.0.0.1
2022-10-28 16:04:25	kato@infoscience.com	Microsoft 365 OneDrive for Business	FileDownloaded	月次報告(営業第3).pptx	100.10.0.1
2022-10-28 16:04:25	kato@infoscience.com	Microsoft 365 OneDrive for Business	FileDownloaded	月次報告(営業第2).pptx	100.10.0.1
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	FileDownloaded	月次報告(営業第1).pptx	100.10.0.1
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	FileDownloaded	月次報告(開発第2).pptx	100.10.0.1
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	FileDownloaded	月次報告(サポート).pptx	100.10.0.1
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	FileDownloaded	月次報告(マーケティング).pptx	100.10.0.1
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	FileDownloaded	月次報告(開発第1).pptx	100.10.0.1
2022-10-28 15:58:49	watanabe	AWS CloudTrail	ConsoleLogin		100.10.0.1
2022-10-28 15:39:52	suzuki@infoscience.com	Google Workspace ドライブ	view	○○案件作業記録.doc	54.0.0.1
2022-10-28 15:27:14	user1@infoscience.com	GCP 管理アクティビティ監査ログ	v1.compute.instances.start	projects/gcp-test/zones/asia-northeast1-b/instances/instance-ws	100.10.0.1
2022-10-28 15:12:56	suzuki@infoscience.com	Google Workspace ドライブ	trash	【企画事業部】2022年度マーケティング施策.doc	54.0.0.1

参照したいユーザーをクリック（＝トラッキング）することで、ユーザーの行動追跡をすることができます。

検索条件名:	マルチクラウド ファイル操作(SaaSのみ)			
概要:	「アップロード」or「ダウンロード」or「コピー」or「プレビュー」or「編集」or「移動」or「名前変更」or「ロック」or「ロック解除」...で抽出			
検索条件	検索結果	カラムセットアサイン		
ログ	カラム	1-100件目表示 (全1,802件) < < 1 2 3 4 5 6 7 8 9 10 > >>		
タイムスタンプ	ユーザー	アプリケーション	アクション	ファイル名
2022-10-29 14:47:39	kato@infoscience.com	Boxユーザーアクティビティ	編集	業務計画(202205)
2022-10-29 14:44:51	kikuchi@infoscience.com	Boxユーザーアクティビティ	編集	業務計画(202205)
2022-10-29 14:42:00	kikuchi@infoscience.com	Boxユーザーアクティビティ	アップロード	業務計画(202205)

検索条件名:	マルチクラウド ファイル操作(SaaSのみ)			
概要:	「アップロード」or「ダウンロード」or「コピー」or「プレビュー」or「編集」or「移動」or「名前変更」or「ロック」or「ロック解除」...で抽出			
検索条件	検索結果	カラムセットアサイン		
ログ	カラム	1-43件目表示 (全43件) < < > >>		
タイムスタンプ	ユーザー	アプリケーション	アクション	ファイル名
2022-10-29 14:47:39	kato@infoscience.com	Boxユーザーアクティビティ	編集	業務計画(202205)
2022-10-28 16:04:25	kato@infoscience.com	Microsoft 365 OneDrive for Business	ファイルのダウンロード	月次報告(営業第3).pptx
2022-10-28 16:04:25	kato@infoscience.com	Microsoft 365 OneDrive for Business	ファイルのダウンロード	月次報告(営業第2).pptx
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	ファイルのダウンロード	月次報告(営業第1).pptx
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	ファイルのダウンロード	月次報告(開発第2).pptx
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	ファイルのダウンロード	月次報告(サポート).pptx
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	ファイルのダウンロード	月次報告(マーケティング).pptx
2022-10-28 16:04:24	kato@infoscience.com	Microsoft 365 OneDrive for Business	ファイルのダウンロード	月次報告(開発第1).pptx
2022-10-27 14:52:12	kato@infoscience.com	Google Workspace ドライブ	ダウンロード	●●企画書2.doc
2022-10-27 14:51:09	kato@infoscience.com	Google Workspace ドライブ	ダウンロード	●●企画書.doc
2022-10-27 11:33:52	kato@infoscience.com	Microsoft 365 SharePoint	ファイルの削除	〇〇案件議事録.doc

設定件数以上（以下）のアクセスがあるファイルを抽出し、確認することができます。

フィルター設定（グループ 2）

合計値フィルター

☒ 条件1

100

以上

☐ 条件2

10

より小さい

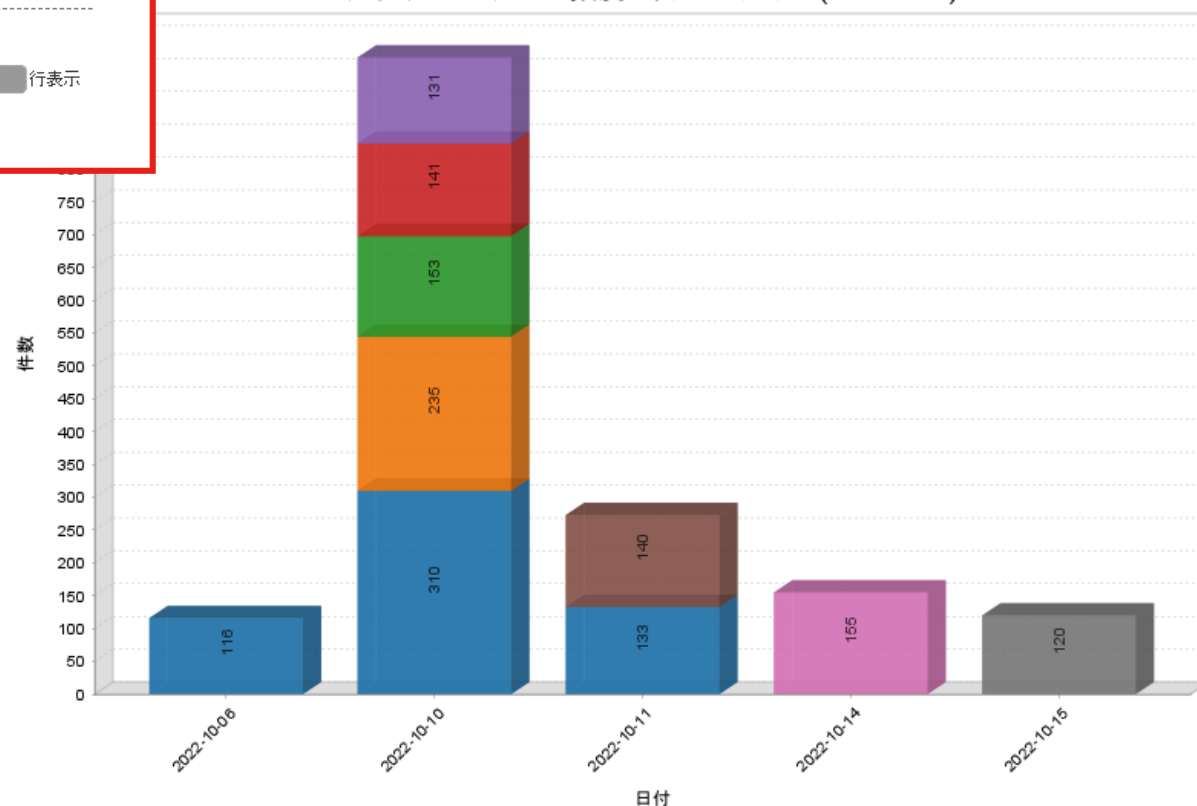
グループ行数フィルター

☐ グループ行数

10

行表示

マルチクラウド アクセス頻度の高いファイル(SaaSのみ)



■ 社内規定.doc ■ 2022年度予算.xlsx ■ 【営業部】休暇予定.doc ■ 売上報告書（2022年1月）.doc ■ 月次報告書（2022年11月）.doc
■ 【企画事業部】2022年度マーケティング施策.doc ■ 新規プロダクト開発計画.doc ■ O×案件概要.doc

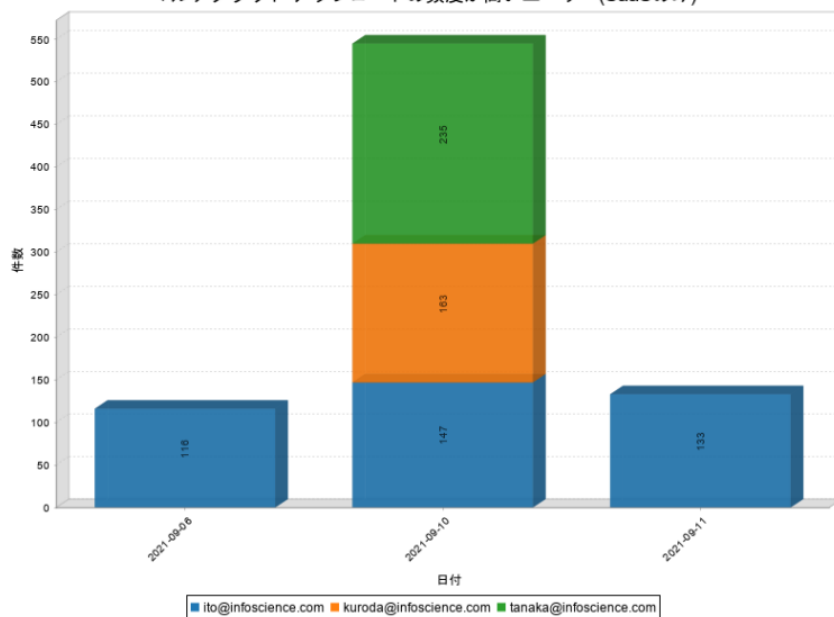
集計・レポート： アップロード、ダウンロードの頻度が高いユーザー

マルチクラウド アップロードの 頻度が高いユーザー(SaaSのみ)

概要
作成日 2021-09-16 14:47:37
対象期間 2021-09-01 00:00:00 - 2021-09-30 23:59:59

集計条件名 マルチクラウド アップロードの頻度が高いユーザー(SaaSのみ)			
概要 「アップロード」の操作を1日あたり100件以上したユーザーを抽出			
日付	ユーザー	件数	日付
2021-09-06	ito@infoscience.com	116	
	ito@infoscience.com	147	
2021-09-10	kuroda@infoscience.com	163	
	tanaka@infoscience.com	235	
2021-09-11	ito@infoscience.com	133	

マルチクラウド アップロードの頻度が高いユーザー(SaaSのみ)

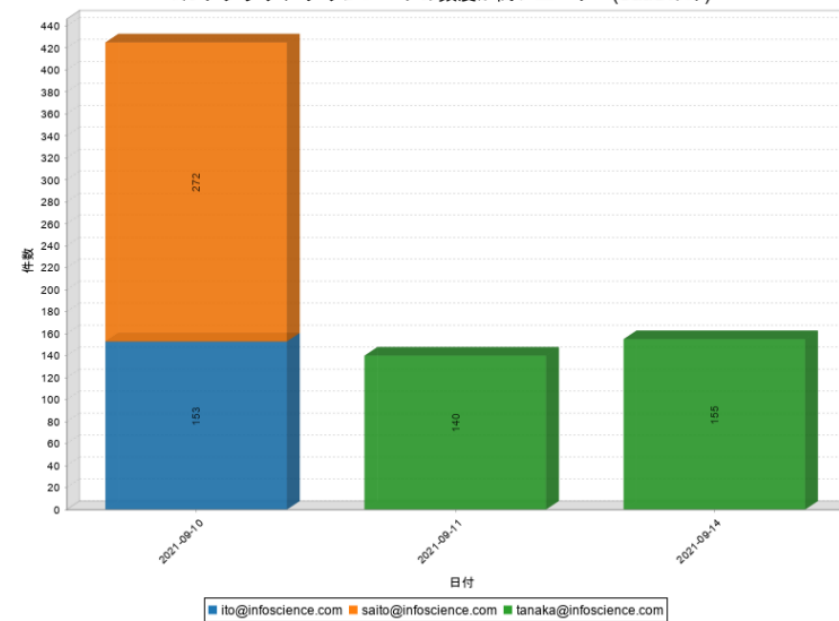


マルチクラウド ダウンロードの 頻度が高いユーザー(SaaSのみ)

概要
作成日 2021-09-16 14:47:45
対象期間 2021-09-01 00:00:00 - 2021-09-30 23:59:59

集計条件名 マルチクラウド ダウンロードの頻度が高いユーザー(SaaSのみ)			
概要 「ダウンロード」の操作を1日あたり100件以上したユーザーを抽出			
日付	ユーザー	件数	日付
2021-09-10	ito@infoscience.com	153	
	saito@infoscience.com	272	
2021-09-11	tanaka@infoscience.com	140	
2021-09-14	tanaka@infoscience.com	155	

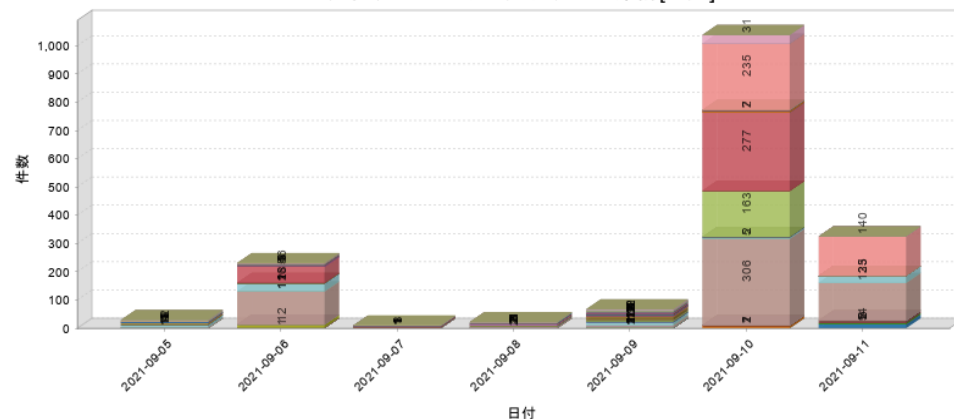
マルチクラウド ダウンロードの頻度が高いユーザー(SaaSのみ)



集計・レポート： ユーザー別アクセス集計（日別、時間別）

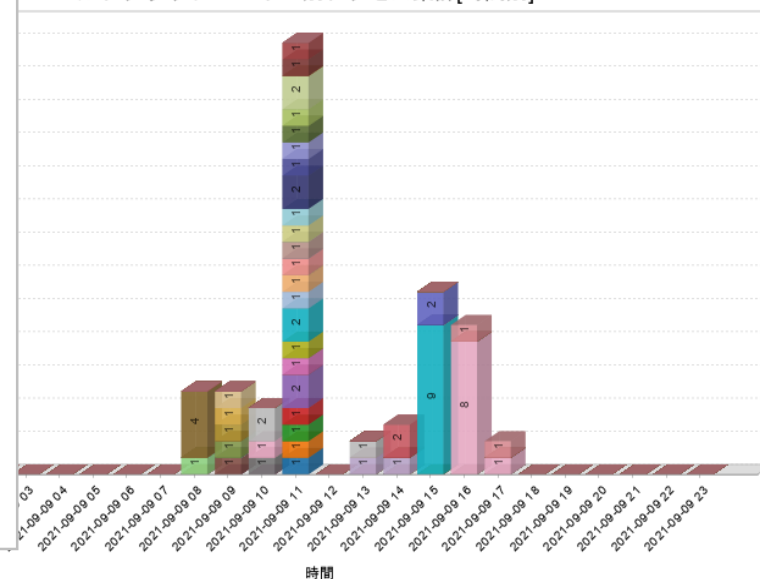
各クラウドサービスの利用状況を確認することができます。

マルチクラウド ユーザー別アクセス集計[日別]



58f0442a-18b1-43ba-8495-73b8ec3bf63a NT AUTHORITY\SYSTEM (Microsoft.Exchange.ServiceHost) NT AUTHORITY\SYSTEM (w3wp)
 ServicePrincipal_ae3d8957-5d87-45ec-823a-f7c51d11160d ServicePrincipal_be73648a-b922-4d0e-8951-a0af8366f411
 ServicePrincipal_d57f46d-8293-450f-b5a6-2ddf42350ba4 aiba@f.co.jp anonymous app@sharepoint fukase@i.co.jp
 futami@k.co.jp hayashi hayashi@bbb.com inoue ito ito@infoscience.com kasahara@a.co.jp kato kato@b.co.jp
 kato@infoscience.com kikuchi@infoscience.com kimura@aaa.com kitagawa kiyota@h.co.jp kobayashi kurita@m.co.jp
 kuroda@infoscience.com matumoto@e.co.jp mori morita muto@c.co.jp nakamura oohira@infoscience.com saito
 saito@infoscience.com sakaguchi@i.co.jp sakata@bbb.com sakurai@d.co.jp sample33@infoscience.com
 sample54@infoscience.com sasaki sasaki-s@infoscience.com sasaki@g.co.jp sasamura@i.co.jp sato segawa@i.co.jp
 suzuki@aaa.com suzuki@infoscience.com takahashi takeuchi tamura tanaka tanaka@a.co.jp tanaka@infoscience.com
 tazaki@n.co.jp urn:spo:anon#8292fb10ae8602cb894b105a41a1cab425c97e6fd05a86963e7b5f4510f5db70 user1@infoscience.com
 yamada yamaguchi

マルチクラウド ユーザー別アクセス集計[時間別]

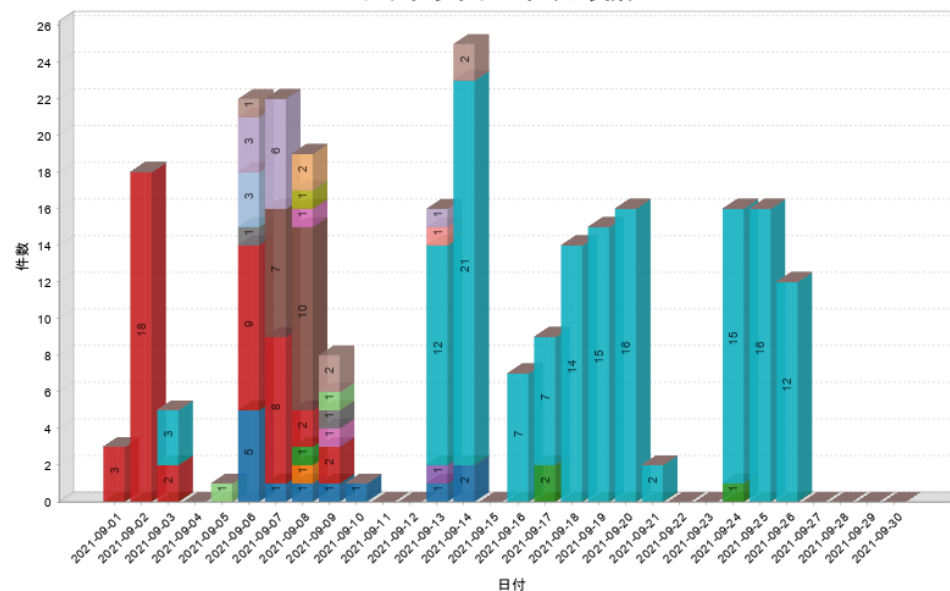


aiba@f.co.jp fukase@i.co.jp futami@k.co.jp hayashi@bbb.com inoue kasahara@a.co.jp kato kato@b.co.jp
 kato@infoscience.com kimura@aaa.com kiyota@h.co.jp kobayashi kurita@m.co.jp kuroda@infoscience.com
 matumoto@e.co.jp mori morita muto@c.co.jp sakaguchi@i.co.jp sakata@bbb.com sakurai@d.co.jp sasaki
 sasaki@g.co.jp sasamura@i.co.jp sato segawa@i.co.jp suzuki@aaa.com suzuki@infoscience.com takahashi tamura
 tanaka tanaka@a.co.jp tazaki@n.co.jp user1@infoscience.com yamada

集計・レポート： ログイン失敗、ログイン成功

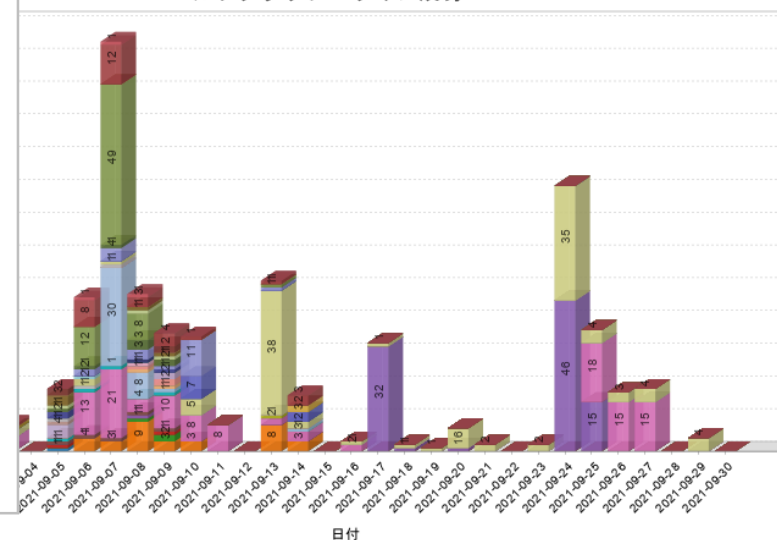
不審なログイン情報を確認することができます。

マルチクラウド ログイン失敗



hayashi@infoscience.com inoue ito@infoscience.com kato@infoscience.com kimura@infoscience.com
 kobayashi@infoscience.com kuroda@infoscience.com morita oohira@infoscience.com saito@infoscience.com
 sample33@infoscience.com sample54@infoscience.com sasaka sasaki@infoscience.com sato@infoscience.com
 yamada@infoscience.com

マルチクラウド ログイン成功



hayashi hayashi@infoscience.com inoue ito ito@infoscience.com kimura kimura@infoscience.com
 kobayashi kobayashi@infoscience.com kuroda kuroda@infoscience.com miura miura@infoscience.com mori
 morita nakamura oohira@infoscience.com saito saito@infoscience.com sample33@infoscience.com
 sample54@infoscience.com sasaka sasaki-s@infoscience.com sasaki@infoscience.com sato sato@infoscience.com
 tamura tanaka tanaka@infoscience.com tuchida@infoscience.com watanabe yamada yamada@infoscience.com
 yamaguchi

集計・レポート： 業務時間外にファイルアクセスしているユーザー

業務時間外でのファイルアクセス状況を定期的に把握することができます。

レポート作成条件名: マルチクラウド 業務時間外にファイルアクセスしているユーザー(SaaSのみ)

概要:

起動タイミング レポート内容 出力 保存期間設定

起動タイミング: 定期

範囲: 毎日

実行時間: 8 時 0 分

対象期間: 1 日間前の 22 時 0 分 0 秒 から 8 時間

プレビュー:

次の実行時間: 2021-09-17(金) 08:00:00

次の実行の対象期間: 2021-09-16(木) 22:00:00 から 2021-09-17(金) 05:59:59 まで

マルチクラウド 業務時間外にファイル アクセスしているユーザー(SaaSのみ)

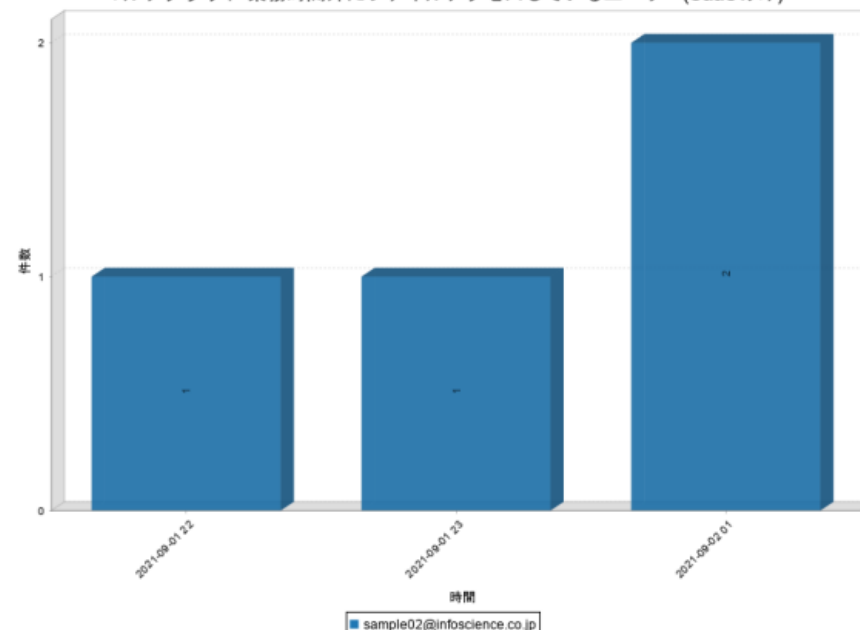
概要

作成日 2021-09-16 16:13:47

対象期間 2021-09-01 22:00:00 - 2021-09-02 05:59:59

集計条件名 マルチクラウド 業務時間外にファイルアクセスしているユーザー(SaaSのみ)			
概要 22:00～翌6:00 (仮) の間に、「アップロード」or「ダウンロード」or「コピー」or「プレビュー」or「編集」or「移動」or「名前変更」or「ロック」or「ロック解除」...で抽出			
時間	ユーザー	件数	
2021-09-01 22	sample02@infoscience.co.jp	1	
2021-09-01 23	sample02@infoscience.co.jp	1	
2021-09-02 01	sample02@infoscience.co.jp	2	

マルチクラウド 業務時間外にファイルアクセスしているユーザー(SaaSのみ)



集計・レポート： 組織外からアクセスされたファイル

組織外の利用者からアクセスされたファイルの一覧を確認することができます。

集計条件名: マルチクラウド 組織外からアクセスされたファイル(SaaSのみ)

概要: ※抽出条件の「@infoscience¥.co¥.jp」は自ドメインに変更してください。

集計対象設定
集計条件設定
集計結果

LogGateグループ: lgroup1

検索条件からコピー: 検索条件選択

期間指定:

今日
今週
今月
今年

昨日
先週
先月
去年

2021 年 9 月 1 日 0 時 0 分 0 秒 から
2021 年 9 月 30 日 23 時 59 分 59 秒 まで

インデックス検索

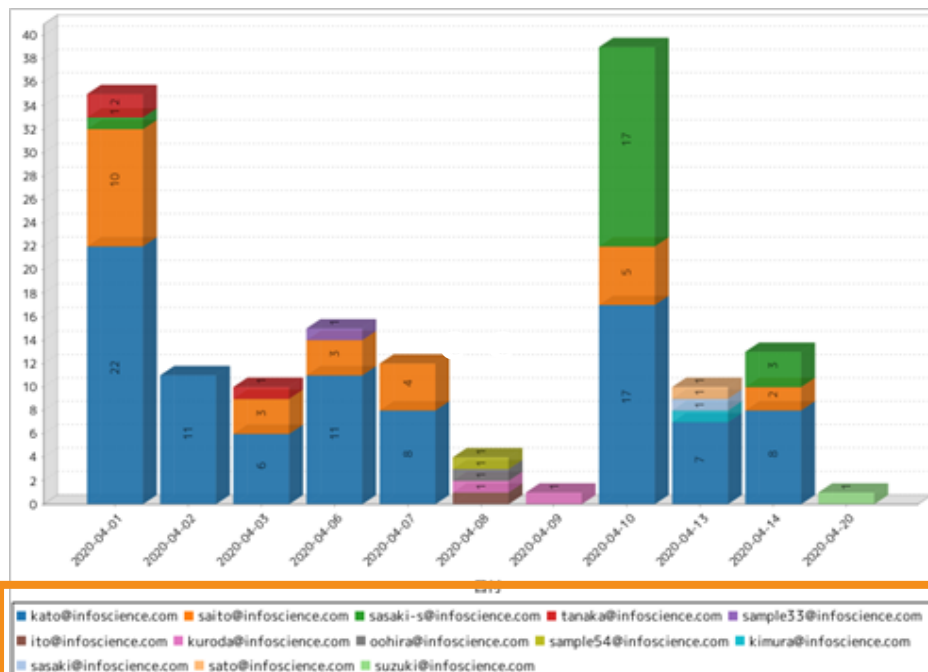
検索語を入力

タグ: ユーザー 文字列 (.*)(?<@infoscience¥.com)\$ 正規表現

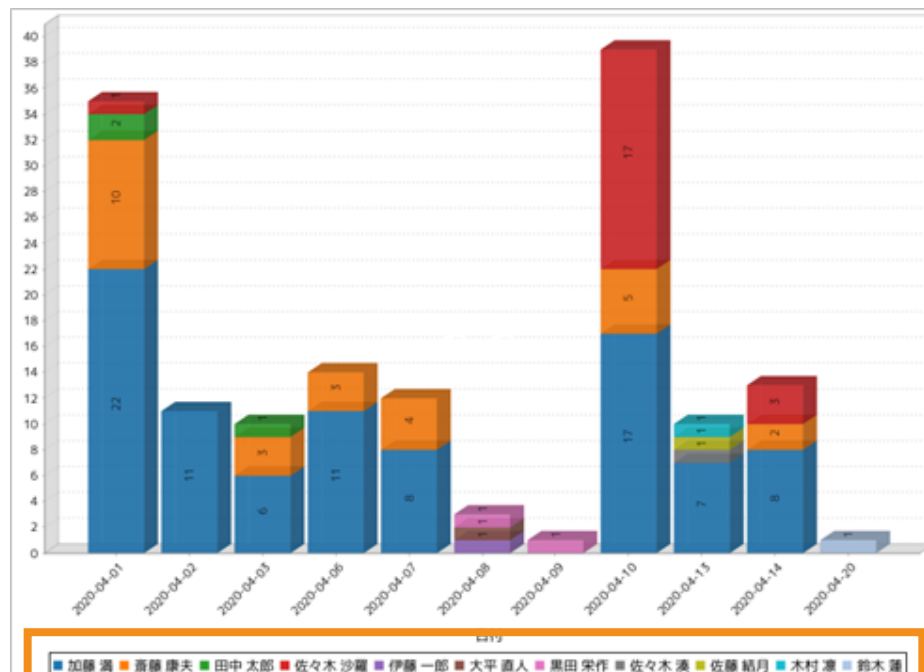
日付	ファイル名	ユーザー	件数
2021-09-02	20201201_〇〇案件打ち合わせ議事録.doc	hayashi@bbb.com	1
		kimura@aaa.com	1
		maeda@bbb.com	2
		miyata@bbb.com	1
		sakata@bbb.com	1
		suzuki@aaa.com	2
	□△QA表.doc	sakata@bbb.com	1
2021-09-06	△△QA表.doc	sakata@bbb.com	1
	〇△QA表.doc	sakata@bbb.com	1
	〇〇稟議申請.docx	app@sharepoint	1
	【ウェビナー】ログ管理の必要性.mp4	app@sharepoint	1
	【ウェビナー】製品紹介.mp4	app@sharepoint	1
	サポート調査.xlsx	app@sharepoint	1
	補足説明.xlsx	app@sharepoint	1
2021-09-09	パートナー様向け説明会資料.pdf	aiba@f.co.jp	1
		fukase@l.co.jp	1
		futami@k.co.jp	1
		hayashi@bbb.com	1
		kasahara@a.co.jp	1
		kato@b.co.jp	1
		kimura@aaa.com	1
		kiyoto@h.co.jp	1
		kurita@m.co.jp	1
		matumoto@e.co.jp	1
		muto@c.co.jp	1
		sakaguchi@j.co.jp	1
		sakata@bbb.com	2
		sakurai@d.co.jp	1
		sasaki@g.co.jp	1
		sasamura@j.co.jp	1
		segawa@i.co.jp	1
		suzuki@aaa.com	2
		tanaka@a.co.jp	1
		tazaki@n.co.jp	1

マスタ連携機能を利用することで、ログの可読性を更に向上することができます。

【マスタ連携なし】



【マスタ連携あり】



開発元

インフォサイエンス株式会社

〒108-0023

東京都港区芝浦2-4-1 インフォサイエンスビル

<https://www.infoscience.co.jp/>

お問い合わせ先

インフォサイエンス株式会社

プロダクト事業部

TEL 03-5427-3503 FAX 03-5427-3889

<https://logstorage.com/>

mail : info@logstorage.com