

Logstorage to

統合ログ管理システム「ログストレージ」

Logstorage Google Workspace 連携パック 参考資料



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。



「出力されるログの内容が変わった」

「保管するログのサイズが増えた」

「仕様変更でログの種類が増えた」

「独自の収集プログラムが 仕様変更で作り直し」





技術者のリソースが ログ管理に取られすぎる



「技術者のリソースがログ管理に取られすぎる課題」を解決

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。

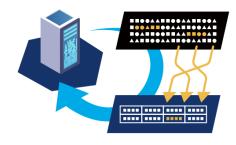
ログ収集モジュール



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。

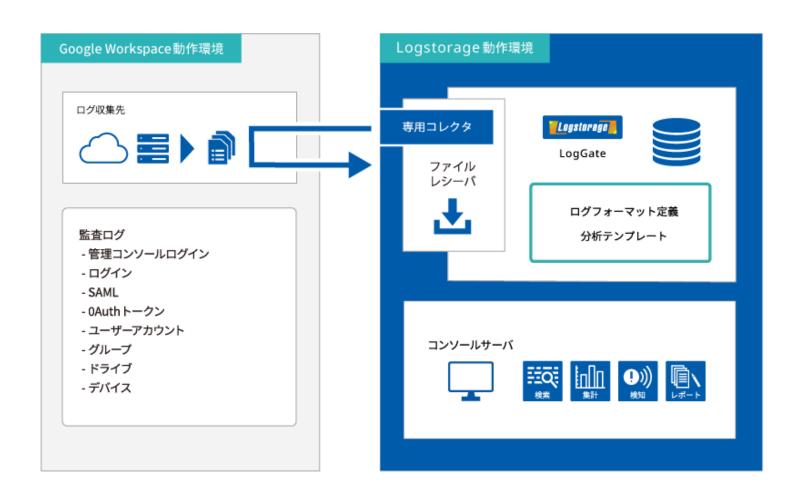


分析テンプレート



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・集計テンプレート一覧

Logstorage Google Workspace 連携パック の検索・集計テンプレートは以下の通りです。

検索・集計条件テンプレート名	概要
Google Workspace OAuth トークン イベント一覧	-
Google Workspace SAML イベント一覧	-
Google Workspace グループ イベント一覧	-
Google Workspace デバイス イベント一覧	-
Google Workspace ドライブ イベント一覧	-
Google Workspace ドライブ イベント一覧 ※プライマリーイベントのみ	-
Google Workspace ドライブ イベント一覧 【レポート用】共有権限設定の変更	「ユーザーの共有権限の変更」or「リンク共有のアクセスタイプの変更」or「リンク共有の公開設定の変更」で抽出
Google Workspace ユーザーアカウント イベント一覧	-
Google Workspace ログイン イベント一覧	-
Google Workspace 管理コンソール イベント一覧	-
Google Workspace OAuth トークン イベント一覧	-
Google Workspace SAML イベント一覧	-
Google Workspace グループ イベント一覧	-
Google Workspace デバイス イベント一覧	-
Google Workspace ドライブ イベント一覧	-

レポートテンプレート一覧

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

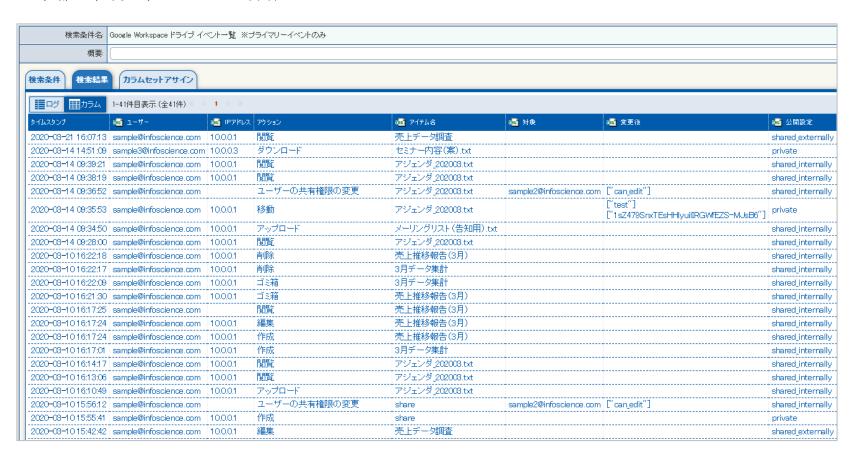
レポート条件テンプレート名	概要
Google Workspace ドライブ アクセス頻度の高いフォルダ・ファイル	「アップロード」or「ダウンロード」or「コピー」or「プレビュー」or「編集」 or「移動」or「閲覧」で抽出 ※100件以上のフィルター条件あり
Google Workspace ドライブ アップロードの頻度が高いユーザー	「アップロード」の操作を1日あたり100件以上したユーザーを抽出
Google Workspace ドライブ ダウンロードの頻度が高いユーザー	「ダウンロード」の操作を1日あたり100件以上したユーザーを抽出
Google Workspace ドライブ 共有権限設定の変更	「ユーザーの共有権限の変更」or「リンク共有のアクセスタイプの変更」or「リンク共有の公開設定の変更」で抽出
Google Workspace ドライブ 業務時間外にファイルアクセスしているユーザー	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「閲覧」をしたユーザーを抽出
Google Workspace ドライブ 組織外からアクセスされたフォルダ・ファイル	※抽出条件の「@infoscience¥.co¥.jp」は自ドメインに変更してください。
Google Workspace ログイン失敗	-
Google Workspace ログイン失敗(OAuth トークン)	-
Google Workspace ログイン失敗(SAML)	-
Google Workspace ログイン成功	-
Google Workspace ログイン成功(OAuth トークン)	-
Google Workspace ログイン成功(SAML)	-

検索例

ドライブ上のフォルダ・ファイルのアクセス履歴を確認できます。

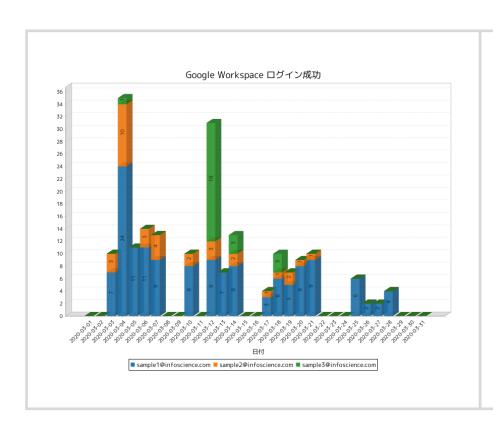
Google Workspaceユーザーのアクセス履歴を可視化

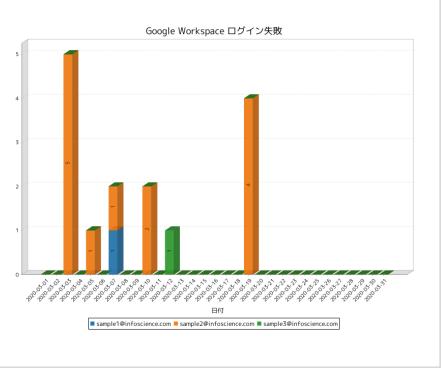
→いつ、誰が、何を、どのように操作したか?



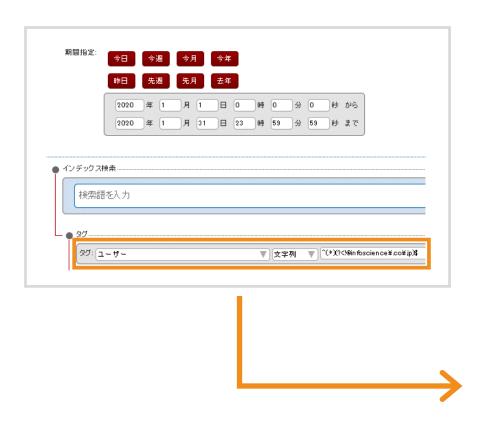
Google Workspaceのログイン履歴を確認することで、

Google Workspaceの利用状況不審なアクセスがないかを把握できます。



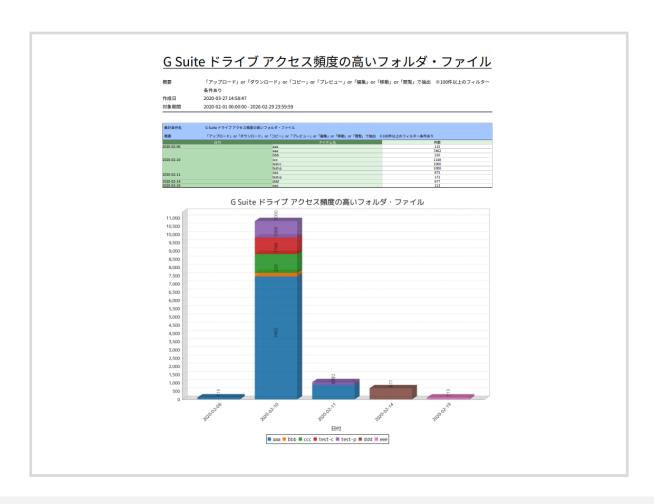


組織外のユーザーからアクセスされたフォルダ・ファイルの一覧が確認できます。





定期的に監査したいイベントをレポート出力することで、ログのモニタリングにかかる運用負荷を軽減します。





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。



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